TAU-24.IP TAU-16.IP

Operation Manual
Version 2.13.1 (November 2015)

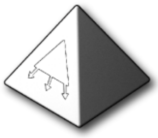
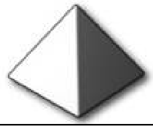
Universal Network Terminal

Firmware version: 2.13.1
Linux version: 291 Wed Mar 4 15:33:57 NOVT 2015
Firmware version: v10_23_03_15
BPU version: v20150703 date: 2015 Jul 3 time 18:56:10

Factory default IP address 192.168.1.2
username: admin
password: rootpasswd

Document version	Issue date	Revisions
Version 1.0	10 November 2015	First issue.

SYMBOLS

Symbol	Description
Bold font face	Notes, warnings, chapter headings, titles, 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 data are written in Courier New semibold.
<KEY>	Keyboard keys are written in upper-case and enclosed in angle brackets.
	Analogue phone unit icon
	Gatekeeper icon
	TAU Universal Network Terminal icon
	MES3124F 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 are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.**

TARGET AUDIENCE

This operation 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.

CONTENTS

1 INTRODUCTION

TAU-24.IP/TAU-16.IP Universal Network Terminal allows to connect analogue phone units to packed-based data networks accessible through copper-wire or optical Ethernet interfaces.

TAU-24.IP/TAU-16.IP could be used as a subscriber access point utilizing SIP/SIP-T and H.323 protocols and provides a perfect telephone communication solution for underpopulated areas, offices, dwellings and geographically dispersed facilities.

This operation manual describes intended use, key specifications, configuration, and firmware update methods for TAU-24.IP/TAU-16.IP network terminal (hereinafter the "device").

2 PRODUCT DESCRIPTION

2.1 Purpose

TAU-24.IP/TAU-16.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.

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.

Interface types:

- 24 or 16 Analogue ports FXS;
- two Ethernet 10/100/1000BaseT electrical interfaces.
- one Mini-Gbic (SFP) Ethernet 1000BaseX optical interfaces.

Device features:

- Integrated Layer 2 Ethernet switch.
- VoIP protocols: H.323, SIP/SIP-T[1].
- Static address and DHCP support.
- Echo cancellation (G.168 recommendation).
- Packet loss concealment (PLC).
- Voice activity detector (VAD).
- Silence suppression.
- DTMF tone detection and generation.
- Fax transmission: upspeed/pass-through; T.38 UDP Real-Time Fax.
- Cisco NSE support.
- V.152 support.
- Flexible numbering scheme.
- Operation with and without external gatekeeper (H.323/RAS).
- Operation with multiple SIP servers in various SIP profiles.
- Support for VoIP operation in the switch in case of SIP server connection loss.
- Active session support for SIP protocol operations through NAT.
- Transmission of cpc-rus subscriber category via SIP protocol.
- 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.
- STP support.
- LLDP support.
- iptables network-level firewall.
- STUN support.
- Service (simulation service) management using IMS (3GPP TS 24.623).
- Remote monitoring, configuration and setup:
  - Web interface.

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

- telnet.
- SSH.
- SNMP.
- TR-069.
- User authentication with RADIUS server.

Supported supplementary services:

- Call Hold/Retrieve.
- Call Transfer.
- Call Waiting notification.
- 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.

SIP, supported recommendations:

- 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 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;
- SIP OPTIONS Keep-Alive (SIP Busy Out);
- NAT support.

2.2 Typical Application Diagrams

This manual covers the following TAU connection methods:

1. ***Subscriber access point*** In this case, the device acts as a gateway between analogue phone units and remote PBX, see Fig. 1. Gateway subscriber ports are registered at the software switch—Softswitch. Supplementary services in this method are provided by the software switch.

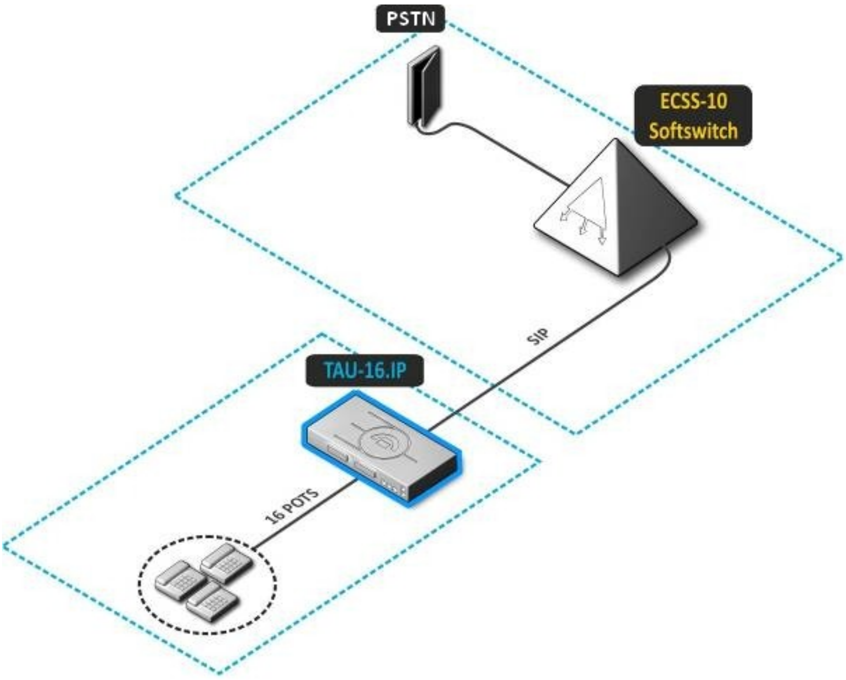


Fig. 1— TAU-24.IP/TAU-16.IP subscriber access point

2. Distributed mini-PABX mode In this case, the device acts as a mini-PABX that is able to access other gateways (TAU-32M.IP, TAU-72.IP, etc.) and Softswitch using SIP/H.323 protocols. The device allows for unassisted processing of supplementary services, call routing, see Fig. 2.

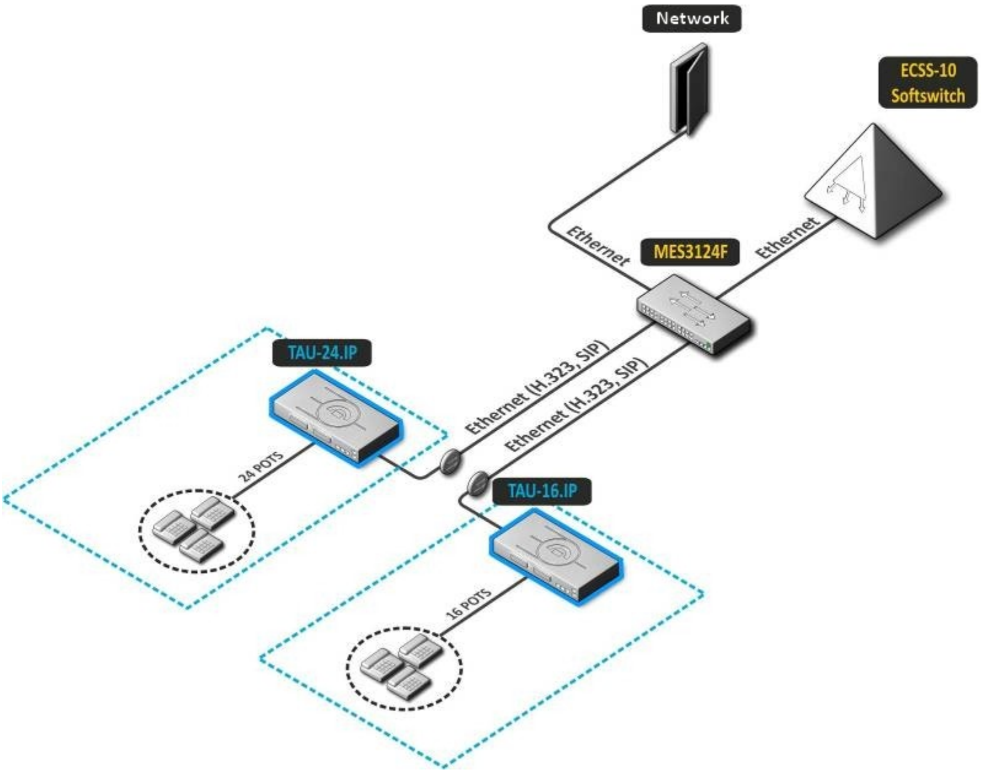


Fig. 2— TAU-24.IP/TAU-16.IP distributed mini-PABX

2.3 Product 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.

Fig. 3 shows TAU-24.IP/TAU-16.IP functional chart.

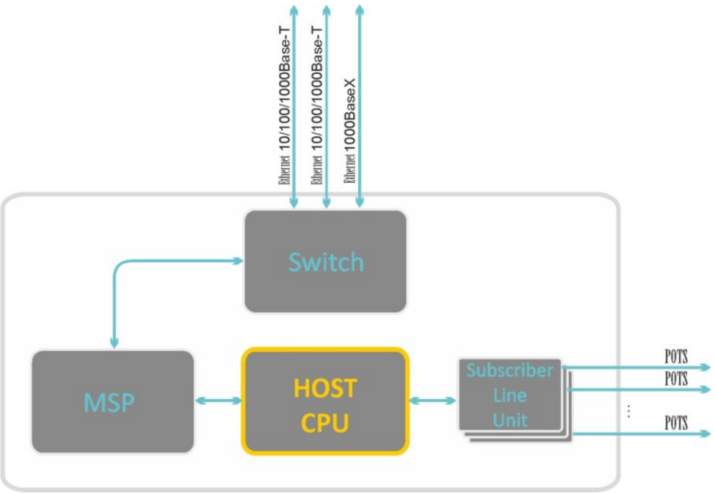


Fig. 3—TAU functional chart

2.4 Main Specifications

Table 1 lists main specifications of the terminal.

Table 1—Main specifications of the terminal

Protocols and Standards

Protocol stack	ITU-T H.323 v3/v4/v5
Communication protocol for session initiation, monitoring and cancellation	SIP
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)

Voice codecs

Voice codecs	G.729AB G.711(A/U) G.723.1 (6.3 Kbps, 5.3 Kbps) G.726 32 kBps (for SIP only)

Parameters of electrical Ethernet interface

No. of ports:	2
Electrical connector	RJ-45
Transfer rate, Mbit / s	Autonegotiation, 10/100/1000 Mbps/s duplex
Standards support	10/100/1000Base-T

Parameters of the optical Ethernet interface

No. of ports:	1
Optical connector	Mini-Gbic (SFP): 1) full-duplex, two-fiber with 1310 nm (Single-Mode), 1000BaseX (LC connector), the supply voltage - 3.3V 2) duplex, single fiber with wavelengths in the transmission/reception 1310/1550 nm, 1000BaseX (SC connector), the supply voltage - 3.3V
Transfer rate, Mbit / s	1000 Mb/s, duplex
Standards support	1000Base-X

Analogue interfaces

No. of ports:	TAU-24.IP	24
	TAU-16.IP	16
Loop resistance:	up to 3.4kΩ	
Dialling reception	pulse/frequency (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 surge linear side cross must be equipped with a three-pole arresters voltage 230V operation. Recommended arresters company KRONE "MK, 230 V" with heat protection spring.**	
Remote measurement of parameters of the subscriber line	yes	
Parameters set	programmable	

Console

RS-232 Serial port	
Data rate, Mbit / s	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

Power voltage	DC: -36..-60B AC: ~150-250B 50 Гц **When using a small unvented closet (access setting) load capacity structure-one to Earl 0.4 / port.** **If you use of forced-tional ventilation cabinet to operate at heavy load.**
Power consumption without active subscribers	30 W
Current consumption of active subscriber set	30 mA
Operating temperature range	From 0 to 40°C
Relative humidity	Up to 80 %
Dimensions (W x H x D)	420x45x134 mm, 19" form-factor, 1U size
Weight	3kg

2.5 Design

TAU-24.IP/TAU-16.IP network terminal has a metal case available for 19” form-factor rack-mount 1U shelf installation.

The front panel of the device mains AC is shown in Fig. 4a-b.

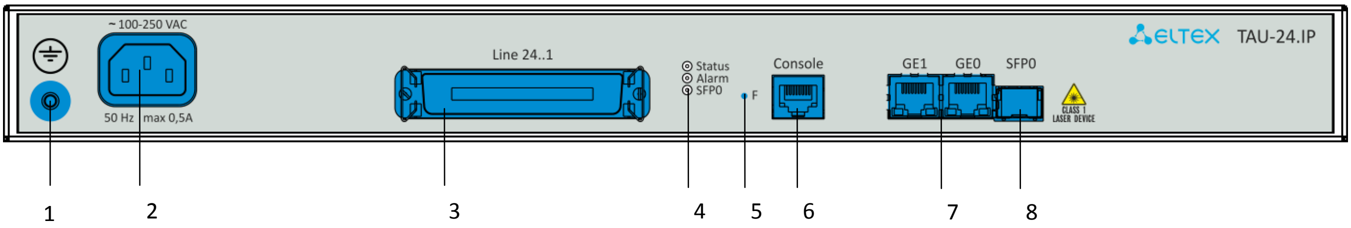


Fig. 4a— TAU-24.IP front panel appearance mains AC

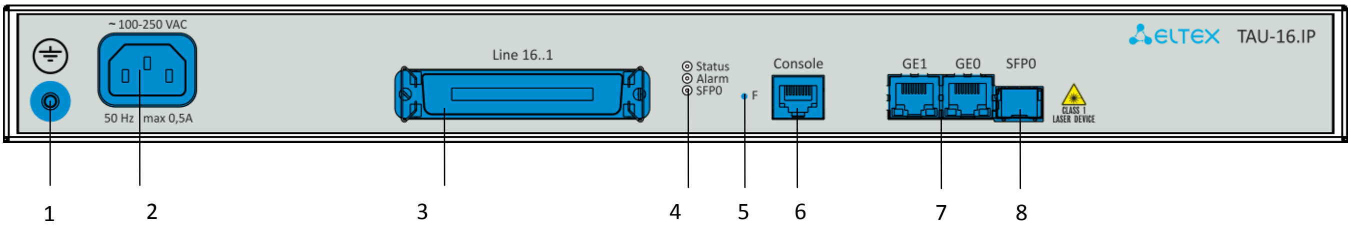


Fig. 4b— TAU-16.IP front panel appearance mains AC

The front panel of the device mains DC is shown in Fig. 4c (as an example TAU-24.IP.).

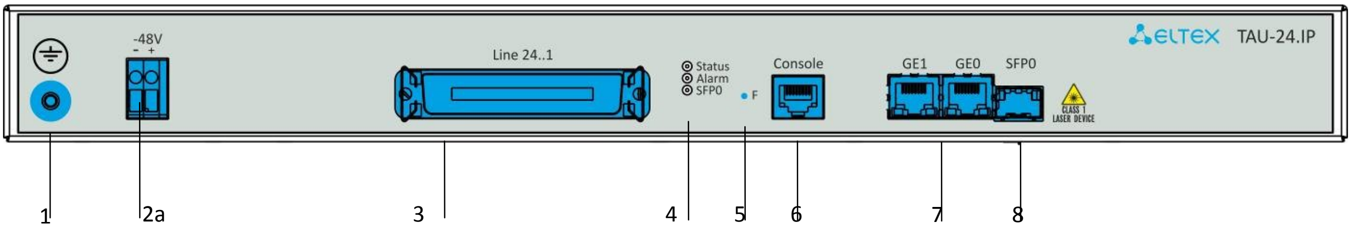


Fig. 4c— TAU-24.IP front panel appearance mains DC

Connectors, LEDs and controls located on the front panel of the device are listed in Table 2.

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

№	Front panel elements	Description
1	⏚	An earthing bolt
2	*~150 – 250 VAC, 50 Hz max 2A*	Connector for AC power supply with voltage 150–250VAC, 50Hz (depending on the order)
2a	*-48V*	Connector for DC power supply with rated voltage -48VDC (permissible voltage from -36VDC to -60VDC)
3	*Line 24(16)..1*	CENC-50M connectors (for contact pin assignment, see Appendix A)
4	*Status*	Device operation indicator
	Alarm	Alarm indicator Shows three types of alarms
	SFP0	SFP optical interface activity indicator
3	*F*	Function button
7	*Console*	RS-232 console port for local control of the device
6	*GE1/GE0*	2 x RJ-45 ports of Ethernet 10/100/1000 Base-T interfaces
8	*SFP0*	Chassis for optical SFP modules of 1000Base-X Gigabit uplink interface used for IP network connection

The rear panel of the device contains no connectors, indicators and controls.

For contact pin assignment, see Appendix A.

2.6 LED Indication

Alarm, Status, SFP0 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
Status	solid red	operating system is not loaded (together with LED Alarm)
		main application is not running (together with LED Alarm, flashing mode *Fatal*)
	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 loaded, board type identified
	flashes red, yellow, and green	factory **Safemode** (together with LED Alarm, flashing mode *Fatal*)
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 200ms)	Fatal (critical failure)—connection of the main application to subscriber ports is lost
	off	normal state
SFP0	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

LED/Status		**LED/Status**
Yellow LED 10/100/1000	**Green LED 10/100/1000**	
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

2.7 'F' Function Button Operation

To reboot the operating device, press and hold 'F' button located on the front panel of the device for 5 seconds. ***Alarm*** LED will become solid red. Also, this button allows you to reset the device to factory settings when you forget or don't know device IP address or password used for login. To do this, turn the device on while holding 'F' button. Hold the button until ***Status*** LED begins to flash yellow, green and red alternatively, and ***Alarm*** LED becomes solid red. After that, you can access the device by IP address ***192.168.1.2.*** When connecting with web configurator, default password for ***admin*** user is ***rootpasswd***.

For detailed description of the factory reset procedure, see Section 6.5 'Reset to factory settings in protected mode'.

2.8 Delivery Package

TAU-24/16.IP standard delivery package includes:

- TAU universal network terminal.
- CENC-50M connector—1pcs.
- Earthing cable.
- A mounting set for 19'' rack.
- Operation manual on CD-disk.
- Declaration of conformity.
- Passport.

For devices power **DC**:

- PVS cable 2x1,5 – 2m.

For devices power **AC**:

- Power cable Europlug.

If ordered, delivery package may also include:

- 1000Base-T/Mini-Gbic (SFP) optical interface—1 pcs.

3 INSTALLATION ORDER AND SEFETY MEASURES

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

3.1 Safety instruction

3.1.1 General Guidelines

Any operations with the equipment should comply to the Safety Rules for Operation of Customers' 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 functioning supplementary equipment.

3 TAU-24.IP/TAU-16.IP terminal 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 6,0x10*4 to 10,7x10*4 Pa (from 450 to 800 mm Hg).

4 The device should be not be exposed to mechanical shock, vibration, smoke, dust, water, and chemicals.

5 To avoid components overheating which may result in device malfunction, do not block air vents or place objects on the equipment.

3.1.2 Electrical Safety Requirements

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

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.

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

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

3.1.3 Electrostatic Discharge Safety Measures

In order to avoid failures caused by electrostatic discharge, we strongly recommend to wear ESD belt, shoes and wrist strap which prevent electrostatic charge accumulation (for wrist strap, make sure that it has a secure fit against the skin) and connect the cable to earthing prior to operation.

3.2 TAU-24.IP/TAU-16.IP Installation

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.

If the device was exposed to low temperatures for a long time before installation, leave it for 2 hours at ambient 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.

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.

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

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 left bottom corner of the front panel, see Fig. 4.

3.3 Startup sequence

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

For subscriber unit overvoltage protection, the linear side of the distribution cross should be equipped with triple pole arresters with trip voltage 230V. We recommend to use KRONE arresters—MK, 230V—with a thermal protection spring.

Connect the power supply cable to the device. Depending on the provided sources, the device could be powered from grounded power outlet 220/110VAC, 50/60Hz, or from -38...-72VDC power supply. To connect the device to 220VAC 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.

If a PC is supposed to be connected to TAU-24.IP/TAU-16.IP console port, connect TAU-24.IP/TAU-16.IP COM port to PC COM port. PC should be powered off and grounded at the same point with the switch.

Ensure that all cables are undamaged and securely connected.

Turn the device on and check the front panel LEDs to make sure the terminal is in normal operating conditions.

3.4 Support brackets mounting

The delivery package includes support brackets for rack installation and mounting screws to fix the device case on the brackets.

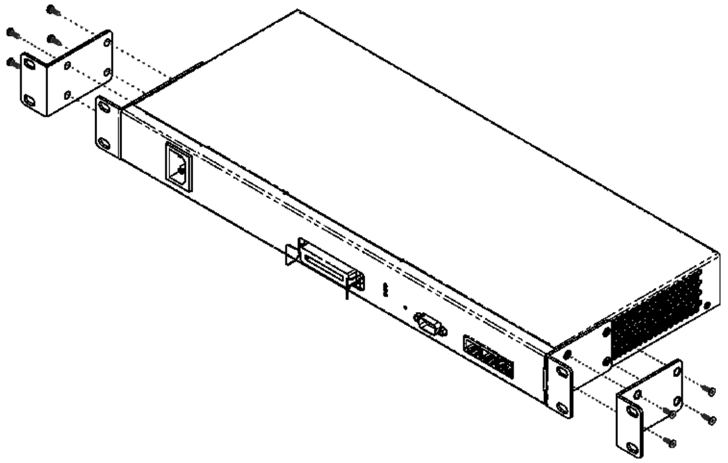


Fig. 5—Support brackets mounting

To install the support brackets:

6 Align four mounting holes in the support bracket with the corresponding holes in the side panel of the device, see Fig. 5.

7 Use a screwdriver to screw the support bracket to the case.

Repeat steps 1 and 2 for the second support bracket.

3.5 Device rack installation

To install the device to the rack:

1. Attach the device to the vertical guides of the rack.
2. Align mounting holes in the support bracket with the corresponding holes in the rack guides. Use the holes of the same level on both sides of the guides to ensure the device horizontal installation.
3. Use a screwdriver to screw the device to the rack.

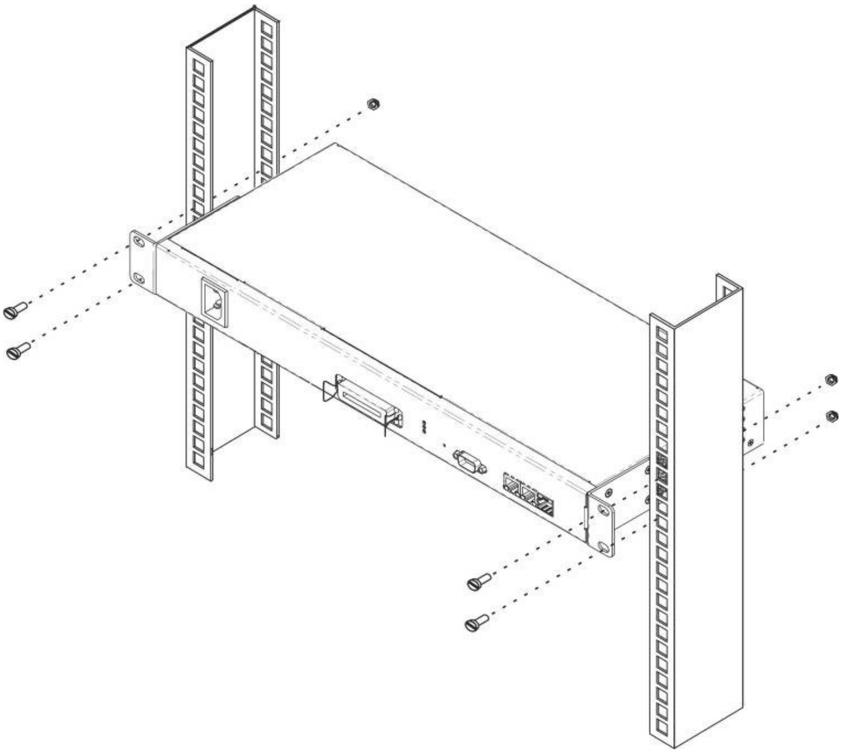


Fig. 6—Device rack installation

4 GENERAL SWITCH 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 to set password for access via telnet and ssh (password is not defined by default), and also change administrator, operator and non-privileged user passwords to access the web interface. For setting password for access via telnet and ssh, see Section 6.4 'Setting password for 'admin' user' For setting password for access via web interface, see Section 5.1.6.6 'Password'. We recommend to write down and store defined passwords in a safe place, inaccessible by intruders.

In order to prevent device configuration data loss, e.g. after reset to factory settings, we recommend making configuration backup copies and storing them on a PC each time significant changes are made.

5 DEVICE CONFIGURATION

You can connect to the device using the following methods: via web interface, via telnet/ssh protocols, or using RS-232 cable.

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 ~ is configured configured by the user, and in the / etc directory factory configuration of the device).

Configuration files can be edited, are connected via the RS-232 or telnet via built-in text editor joe.

To save the contents of the directory / etc ~ non-volatile memory device, you must execute the save. The changes take effect after rebooting the device.

5.1 TAU-24.IP/TAU-16.IP configuration via WEB Interface. Administrator Access[1]

To configure the device, establish connection in the *web browser*, e.g. Firefox, Internet Explorer, etc. Enter device IP address into address bar of web browser.

TAU-24.IP/TAU-16.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 gateway will be forced to end the session. This restriction is not effective in cases when you leave 'Monitoring' or 'System info' pages open, 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's recommended to change password (see Section *5.1.6.6*).

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

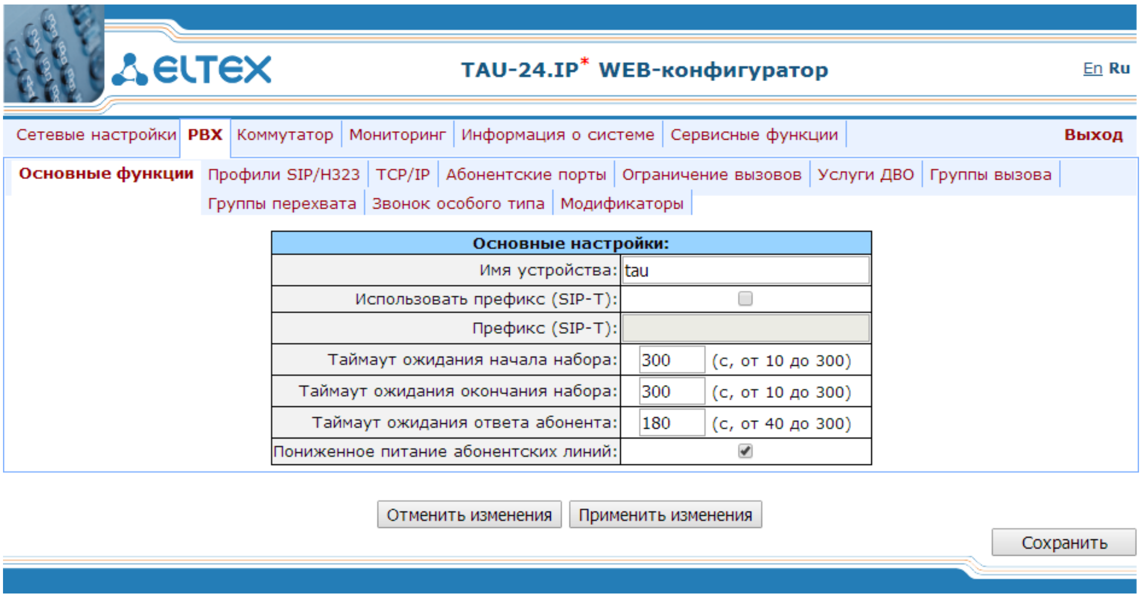
Web Configurator Language

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

Firmware version '-ru' postfix means that the default interface language is Russian, and '-en' postfix stands for English. To change the interface language, select the respective link in the web configurator header bar (on the right side).

[1] The description is an example of the configurator for TAU-24.IP device. For TAU-16.IP device settings are the same, the number of configurable ports - 16

Example of web configurator menu in Russian:



TAU-24.IP* WEB-конфигуратор

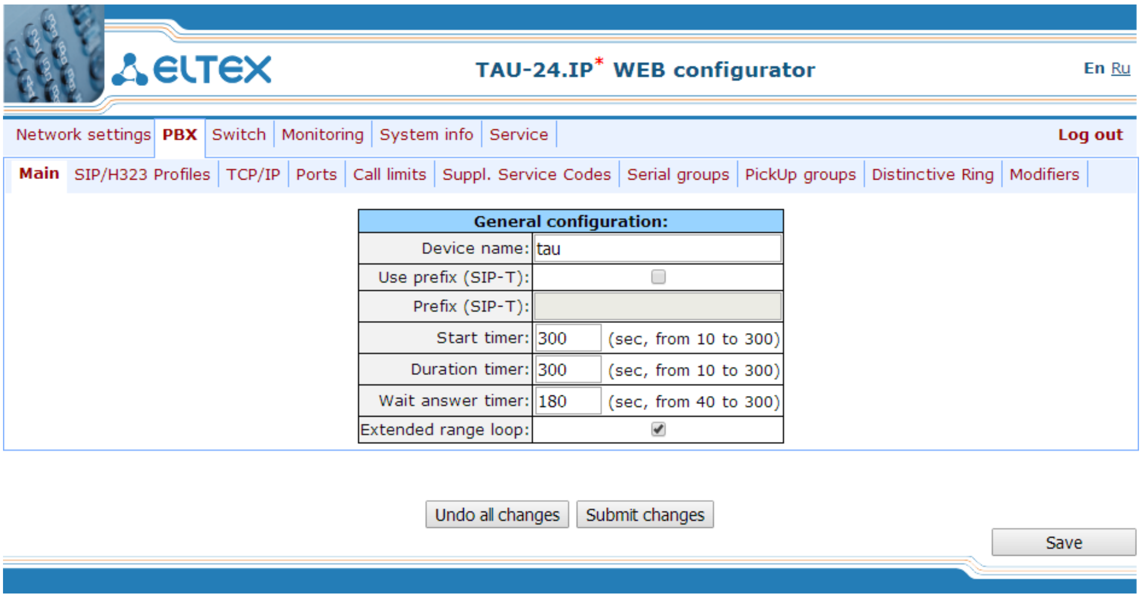
En Ru

Сетевые настройки | PBX | Коммутатор | Мониторинг | Информация о системе | Сервисные функции | Выход
Основные функции | Профили SIP/H323 | TCP/IP | Абонентские порты | Ограничение вызовов | Услуги ДВО | Группы вызова | Группы перехвата | Звонок особого типа | Модификаторы

Основные настройки:	
Имя устройства:	tau
Использовать префикс (SIP-T):	□
Префикс (SIP-T):	
Таймаут ожидания начала набора:	300 (с, от 10 до 300)
Таймаут ожидания окончания набора:	300 (с, от 10 до 300)
Таймаут ожидания ответа абонента:	180 (с, от 40 до 300)
Пониженное питание абонентских линий:	☑

Отменить изменения
Применить изменения
Сохранить

Example of web configurator menu in English:


ELTEX
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Main | SIP/H323 Profiles | TCP/IP | Ports | Call limits | Suppl. Service Codes | Serial groups | PickUp groups | Distinctive Ring | Modifiers
Undo all changes
Submit changes
Save

General configuration:		
Device name:	tau	
Use prefix (SIP-T):	☐	
Prefix (SIP-T):		
Start timer:	300	(sec, from 10 to 300)
Duration timer:	300	(sec, from 10 to 300)
Wait answer timer:	180	(sec, from 40 to 300)
Extended range loop:	☑	

Indication of Changes in Web Configurator

Web configurator supports indication of configuration changes, that is shown in the header bar of configuration interface (TAU-24.IP/TAU-16.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 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.

Table 6 lists description of configuration menu windows.

Table 6 – Description of configuration menu, administrator access

Menu (engl)	Description	Section
Network settings	**Adjustment of the device network settings**	**5.1.1**
Network	Configuration of network settings	5.1.1.1
VLAN conf	VLAN configuration	5.1.1.2
Route	Static route configuration for WAN and VLAN interfaces	5.1.1.3
Hosts	Local DNS server configuration	5.1.1.4
SNMP	SNMP agent configuration	5.1.1.5
Syslog	Syslog server configuration	5.1.1.6
Firewall	Configuration of denied/allowed IP server addresses	5.1.1.7
NTP	NTP configuration	5.1.1.8
ACS	TR-069 monitoring and management protocol settings	5.1.1.9
Uatoupdate	Automatic update configuration	5.1.1.10

PBX	**VoIP (Voice over IP) configuration**	**5.1.2**
Main	Device basic settings	5.1.2.1
SIP/H323 Profiles	Configuration of SIP/H323 profiles	5.1.2.2
SIP Common	SIP common settings	5.1.2.2.1
H323	H323 protocol settings (works in profile 1 only)	5.1.2.2.2
Profile 1..8	Profile configuration	5.1.2.2.3
SIP Custom	SIP custom settings for a profile	5.1.2.2.3
Codecs	Codec settings for a profile	5.1.2.2.4
Dialplan	Routing settings for a profile	5.1.2.2.5
Alert-Info	Configuration of a distinctive ring, formed by Alert-Info value	5.1.2.2.6
TCP/IP	Configuration of network port range for various protocols	5.1.2.3
Ports	Configuration of device subscriber ports and subscriber profiles	5.1.2.4
Call limits	Configuration of simultaneous call limits	5.1.2.5
Suppl. Service Codes	Configuration of supplementary service codes	5.1.2.6
Serial groups	Configuration of serial groups	5.1.2.7
PickUp groups	Configuration of pickup groups	5.1.2.8
Distinctive ring	'Distinctive ring' service administration	5.1.2.9
Modifiers	Configuration of number modifiers	5.1.2.10
Switch	**Configuration of switch settings**	**5.1.3**
Switch ports settings	Configuration of integrated Ethernet switch ports	5.1.3.1
802.1q	Configuration of packet routing rules for switch operation in 802.1q mode	5.1.3.3
QoS & Bandwidth control	Quality of service functions and bandwidth limits configuration	5.1.3.4
Monitoring	**Device monitoring**	**5.1.4**
Port	Device subscriber ports status information	5.1.4.1
Status	Gateway hardware platform status information—voltages, temperature sensors, fans, SFP data	5.1.4.2
Switch	Switch port state monitoring	5.1.4.3
Suppl. Service	Information on the current status of supplementary services on subscriber port	5.1.4.4
IMS SS status	Monitoring of services, software controlled switch with support for IMS	5.1.4.5
Serial groups	Monitoring of registration serial groups	5.1.4.6
System info	**System information**	**5.1.5**
Device info	View the device and network settings information	5.1.5.1
Route	Routing table configuration	5.1.5.2
ARP	ARP table configuration	5.1.5.3
Service	**Firmware update, configuration file operations, rebooting device, setting/changing passwords**	**5.1.6**
Firmware upgrade	Firmware update of subscriber units	5.1.6.1
Backup/Restore	Download/upload configuration files to/from PC	5.1.6.1
Reboot	Rebooting device	5.1.6.3
Security	Encryption feature	5.1.6.4
MOH	Download/upload audio file for call hold service	5.1.6.5
Password	Management of passwords used to access the device via web interface	5.1.6.6
Logout	**Finish the device administration session for the current user**	**5.1.6.7**

5.1.1 Network settings

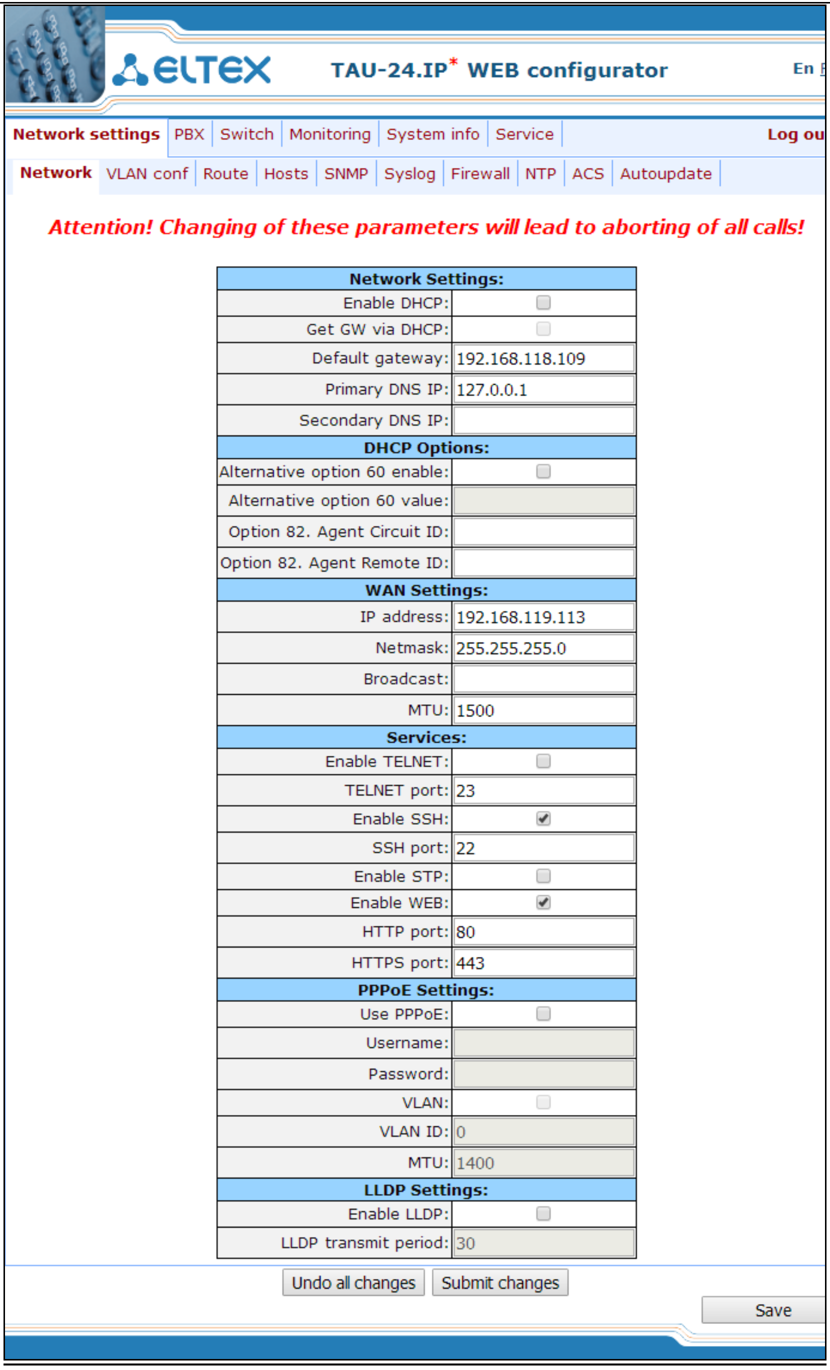
In **Network settings** menu, you can define network settings of the device.

5.1.1.1 Network

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. Allows the gateway to obtain all necessary network settings from DHCP server.
- **SNMP** is a simple network management protocol. 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. 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. 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** is a network protocol that allows the client located behind a network address translation server (NAT) to discover its external IP address.

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



Attention! Changing of these parameters will lead to aborting of all calls!

Network Settings:	
Enable DHCP:	□
Get GW via DHCP:	□
Default gateway:	192.168.118.109
Primary DNS IP:	127.0.0.1
Secondary DNS IP:	
DHCP Options:	
Alternative option 60 enable:	□
Alternative option 60 value:	
Option 82. Agent Circuit ID:	
Option 82. Agent Remote ID:	
WAN Settings:	
IP address:	192.168.119.113
Netmask:	255.255.255.0
Broadcast:	
MTU:	1500
Services:	
Enable TELNET:	□
TELNET port:	23
Enable SSH:	☑
SSH port:	22
Enable STP:	□
Enable WEB:	☑
HTTP port:	80
HTTPS port:	443
PPPoE Settings:	
Use PPPoE:	□
Username:	
Password:	
VLAN:	□
VLAN ID:	0
MTU:	1400
LLDP Settings:	
Enable LLDP:	□
LLDP transmit period:	30

Network settings:

– *Enable DHCP* –when checked, use DHCP protocol to obtain device network settings, otherwise fixed settings (WAN settings) will be used.

Supported options:

- 1—network mask.
- 3—default network gateway address.
- 6—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 **5.1.2.2.3**).
- 121—classless static routes (for option usage, see Section **5.1.1.3**).

– *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.

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 (5.3.2) of the web interface.

Example:

```
[VENDOR:Eltex][DEVICE:TAU24][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 ID* – allows to add Option 82, Suboption 1 — Agent Circuit ID, into DHCP request.

– *Option 82. Agent Remote ID* – allows to add Option 82, Suboption 2 — Agent Remote ID, into DHCP request.

<u>*WAN Settings:*</u>

- *IP address*—device IP address.
- *Netmask*—device network mask.
- *Broadcast address*—device subnet broadcast address.
- *MTU*—maximum transmission unit, that could be transferred through WAN interface without fragmentation.

<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.
- *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.

<u>*Connection Settings:*</u>

- *Use PPPoE*—when checked, enable PPPoE connection.
- *Username*—username for PPP server authentication.
- *Password*—password for PPP server authentication.
- *VLAN*—when checked, use separate VLAN for PPPoE access.
- *VLAN ID*—VLAN identifier.
- MTU—maximum transmission unit, that could be transferred through PPP interface without fragmentation.

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/signaling/control traffic transmission via PPPoE', and then apply configuration changes using *'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 *'Submit Changes'* button. To discard all changes made to configuration, click *'Undo All Changes'* button.

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

5.1.1.2 VLAN conf

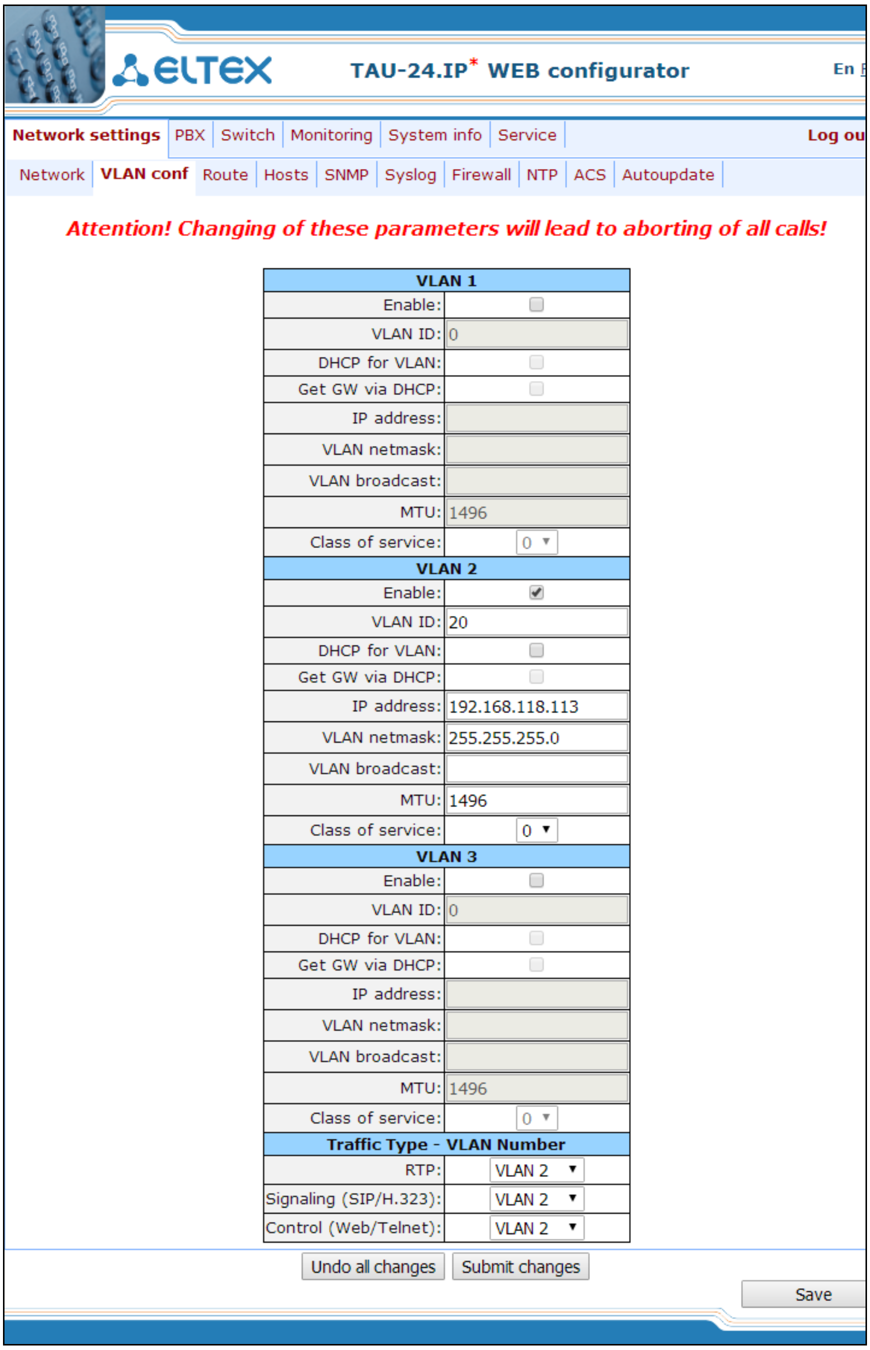
In 'VLAN conf' submenu, you will be able to configure VLAN network settings and transmission of signals and voice traffic, and also set up device management through various VLAN networks.

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



Attention! Changing of these parameters will lead to aborting of all calls!

VLAN 1	
Enable:	□
VLAN ID:	0
DHCP for VLAN:	□
Get GW via DHCP:	□
IP address:	
VLAN netmask:	
VLAN broadcast:	
MTU:	1496
Class of service:	0
VLAN 2	
Enable:	☑
VLAN ID:	20
DHCP for VLAN:	□
Get GW via DHCP:	□
IP address:	192.168.118.113
VLAN netmask:	255.255.255.0
VLAN broadcast:	
MTU:	1496
Class of service:	0
VLAN 3	
Enable:	□
VLAN ID:	0
DHCP for VLAN:	□
Get GW via DHCP:	□
IP address:	
VLAN netmask:	
VLAN broadcast:	
MTU:	1496
Class of service:	0
Traffic Type - VLAN Number	
RTP:	VLAN 2
Signaling (SIP/H.323):	VLAN 2
Control (Web/Telnet):	VLAN 2

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 protocol.
- *IP address—VLAN interface IP address.*
- *VLAN netmask—network mask used for VLAN interface.*
- *VLAN broadcast—subnet broadcast address of VLAN interface.*
- *MTU*—maximum transmission unit, that could be transferred through VLAN interface without fragmentation.
- *Class of service (802.1p)*—802.1p priority for the current VLAN.

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 assignment for SIP/H323 signal traffic.
- *Control (Web/Telnet)*—VLAN, PPPoE assignment for gateway management via web interface, telnet, and SSH.

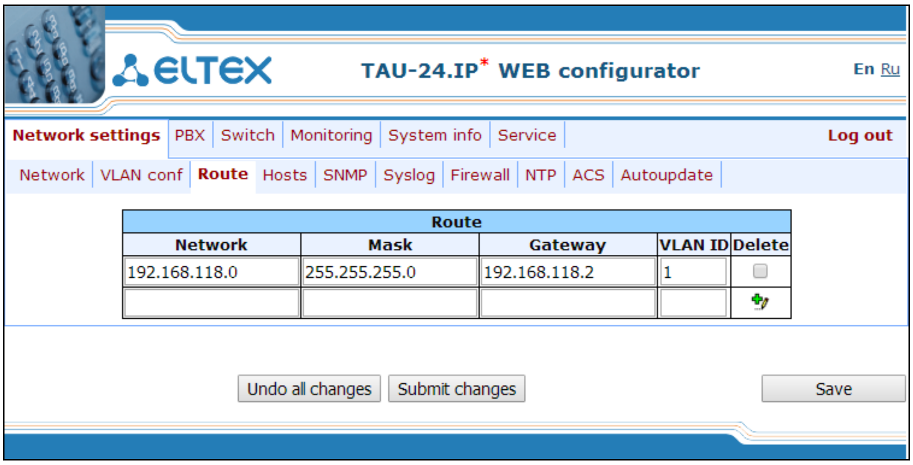
Voice traffic will be transmitted via PPPoE only after the device is restarted!

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

5.1.1.3 Static Route

In *'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.


eltex
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Network | VLAN conf | Route | Hosts | SNMP | Syslog | Firewall | NTP | ACS | Autoupdate
Undo all changes
Submit changes
Save

Route

Network	Mask	Gateway	VLAN ID	Delete
192.168.118.0	255.255.255.0	192.168.118.2	1	□
				+

- 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 *'Submit Changes'* button. To remove the route, select 'Delete' checkbox and click *'Submit Changes'* button.

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

5.1.1.4 Local DNS (Hosts)

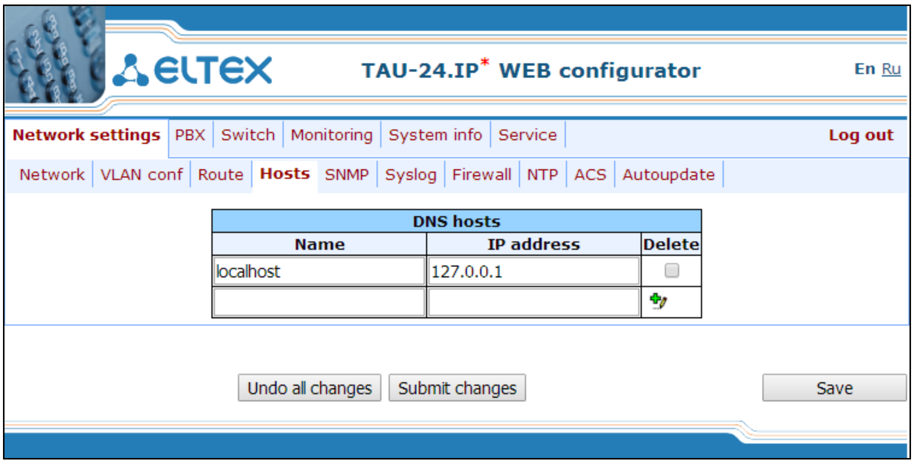
In 'Hosts' submenu, you can configure settings required for local DNS operation.

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

Local DNS – allows the gateway to obtain IP address of the communicating device by its network name (hostname). You may use local DNS in cases when DNS server is missing from the network segment that the gateway belongs to, and you need to establish routing using network names, or when you have to use SIP server network name as its address. Although, you have to know matches between hostnames 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.



DNS hosts		
Name	IP address	Delete
localhost	127.0.0.1	□
		✚

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

- *Name*—name of a host.
- *IP-address*—IP address of a host.

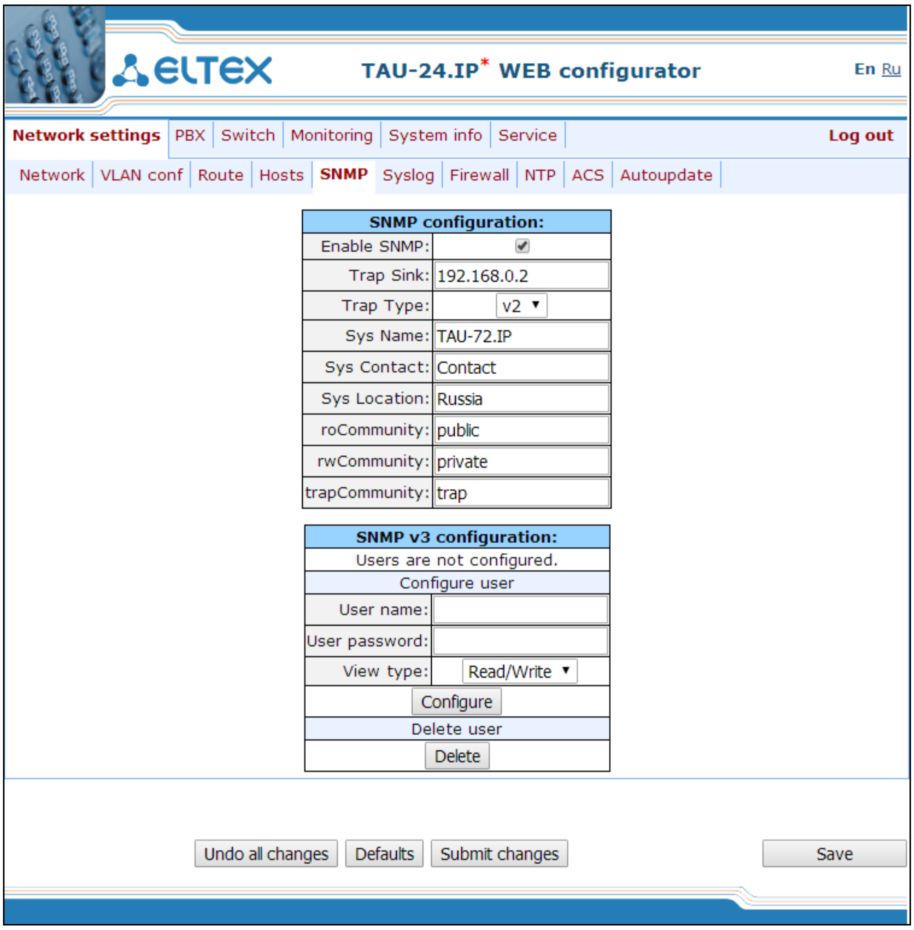
To add/apply a new route, enter the data in the field with ✚ icon, and click *'Submit Changes'* button. To remove the route, select 'Delete' checkbox and click *'Submit Changes'* button.

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

5.1.1.5 SNMP protocol configuration

TAU-24.IP/TAU-16.IP software allows to monitor status of the device and its sensors 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.


TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Network | VLAN conf | Route | Hosts | SNMP | Syslog | Firewall | NTP | ACS | Autoupdate
Configure
Delete
Undo all changes
Defaults
Submit changes
Save

SNMP configuration:	
Enable SNMP:	☑
Trap Sink:	192.168.0.2
Trap Type:	v2
Sys Name:	TAU-72.IP
Sys Contact:	Contact
Sys Location:	Russia
roCommunity:	public
rwCommunity:	private
trapCommunity:	trap

SNMP v3 configuration:	
Users are not configured.	
Configure user	
User name:	
User password:	
View type:	Read/Write
Delete user	

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

SNMP configuration:

- *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.

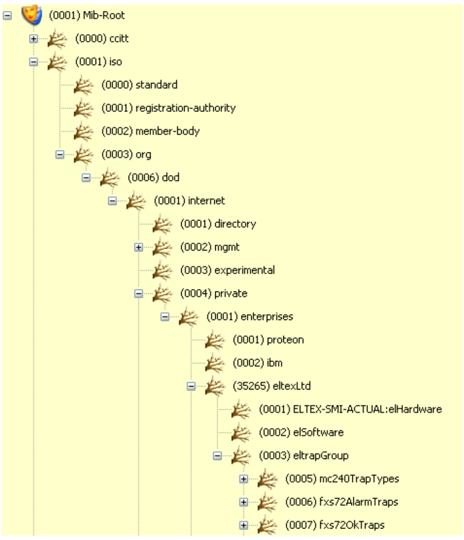
- *User name*—account username.
- *User password*—access password Password should contain 8 characters or more.
- *View type*—account access mode selection:
  - *Read/Write*—read/write mode.
  - *Read only*—read-only mode.

- *Delete*—click this button to delete all accounts for access via SNMP v3.

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

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

MIB Tree



```
⊟ (0001) Mib-Root
    ⊞ (0000) ccitt
    ⊟ (0001) iso
        (0000) standard
        (0001) registration-authority
        (0002) member-body
        ⊟ (0003) org
            ⊟ (0006) dod
                ⊟ (0001) internet
                    (0001) directory
                    ⊞ (0002) mgmt
                    (0003) experimental
                    ⊟ (0004) private
                        ⊟ (0001) enterprises
                            (0001) proteon
                            (0002) ibm
                            ⊟ (35265) eltexLtd
                                (0001) ELTEX-SMI-ACTUAL:elHardware
                                (0002) elSoftware
                                ⊟ (0003) eltrapGroup
                                    ⊞ (0005) mc240TrapTypes
                                    ⊞ (0006) fxs72AlarmTraps
                                    ⊞ (0007) fxs72OkTraps
```

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:*
  - *Board power supply voltage should fall within the limits: 38V<Vbat<72V.*
  - *Ringing voltage shall be within: 100V <Ring1 <120V and 100V <Vring2 <120V;*
  - *Temperature on a sensor should not exceed 90°C.*
- *Successful/unsuccessful firmware update.*
- *Successful/unsuccessful configuration download/upload.*

5.1.1.5.1 SNMP monitoring

The gateway supports monitoring of the following parameters via SNMP.

General Gateway Data

Object identifier enterprises.35265.1.9.

fxsDevName	Gateway name
fxsDevType	Gateway type
fxsDevCfgBuild	Firmware version
fxsFreeSpace	Free disk space
fxsFreeRam	Free RAM
fxsCpuUsage	CPU utilization (%)

Object identifier enterprises.35265.4.

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

Platform Sensor Parameters

Object identifier enterprises.35265.1.9.10.

fxsMonitoringVMode	subscriber sets power mode
fxsMonitoringVBat	voltage primary network, V
fxsMonitoringVRing1	voltage generated by inductor kit 1-24, V
fxsMonitoringTemp1	Temperature measured by submodule 1 sensor
fxsMonitoringTemp2	Temperature measured by submodule 2 sensor
fxsMonitoringTemp3	Temperature measured by submodule 3 sensor
fxsMonitoringTemp4	Temperature measured by submodule 4 sensor
fxsMonitoringFanState	Fan status (on or off)
fxsMonitoringFan1Rotate	Fan health 1, if it's on
fxsMonitoringFan2Rotate	Fan health 2, if it's on
fxsMonitoringDevicePower	Type of power supply installed

List of the possible modes of supply of subscriber sets:

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

Call Monitoring

Object identifier enterprises.35265.1.9.12.1.1.

fxsPortPhoneNumber	Subscriber number
fxsPortState	Port status
fxsPortUserName	Subscriber name
fxsPortTalkingNum	Number(s) of the remote subscriber or two subscribers in conference mode
fxsPortTalkingStartTime	Call start time
fxsPortSipConnected	Last known successful registration on SIP server
fxsPortH323Connected	Gatekeeper registration time
fxsPortSipConnecteNext	Amount of time until next SIP server registration
fxsPortSipConnecteState	SIP server registration status
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.

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

5.1.1.5.2 Device Configuration via SNMP

Gateway supports data readout and configuration via SNMP for the following settings.

Custom Settings for FXS Ports

Object identifier enterprises.35265.1.9.12.2.1.

fxsPortConfigPhone	Phone (up to 20 characters)
fxsPortConfigUserName	User Name (up to 20 characters)
fxsPortConfigAuthName	Authentication name (up to 20 characters)
fxsPortConfigAuthPass	Authentication password (up to 20 characters)
fxsPortConfigCustom	Custom
fxsPortConfigPlaymoh	Play music on hold
fxsPortConfigAON	CallerID
fxsPortConfigAONHideDate	Hide date
fxsPortConfigAONHideName	Hide Name
fxsPortConfigTaxophone	Taxophone—operation in payphone mode
fxsPortConfigMinFlashtime	Min Flashtime (70 to 1000)
fxsPortConfigMaxFlashtime	Max Flashtime (minflashtime to 1000)
fxsPortConfigGainr	Gain receive (-230 to 20)
fxsPortConfigGaint	Gain transmit (-170 to 60)
fxsPortConfigCategory	SS7 category (SIP-T)
fxsPortConfigCallTransfer	Process flash
fxsPortConfigCallWaiting	Call Waiting
fxsPortConfigHotLine	Hot Line
fxsPortConfigHotNumber	Hot Number (up to 20 characters)
fxsPortConfigHotTimeout	Hot Timeout (0 to 300)
fxsPortConfigDisabled	Disabled
fxsPortConfigCtBusy	CF Busy
fxsPortConfigCtUnconditional	CF Unconditional
fxsPortConfigCtNoanswer	CF No answer
fxsPortConfigCtTimeout	CFNR Timeout (0 to 300)
fxsPortConfigClir	CLIR
fxsPortConfigStopDial	Stop dial at #
fxsPortConfigAltNumber	Alt.Number (up to 20 characters)
fxsPortConfigUseAltNumber	Use Alt.Number
fxsPortConfigPickUp	Membership in PickUp groups (up to 86 characters)
fxsPortConfigSipPort	SIP Port (0 to 65535)
fxsPortConfigCfgPriOverCw	CFB has priority over CW
fxsPortConfigRowStatus	Row status (required in SNMP SET). Value for storing data in a file: 1
fxsPortConfigDvoCwEn	Call waiting enable
fxsPortConfigDvoCtAttendedEn	Call transfer attended enable
fxsPortConfigDvoCtUnattendedEn	Call transfer unattended enable
fxsPortConfigDvoUnconditionalEn	Call forward unconditional enable
fxsPortConfigDvoCfBusyEn	Call forward on busy enable
fxsPortConfigDvoCfAnswerEn	Call forward on no answer enable
fxsPortConfigDvoCfServiceEn	Call forward on out of service enable
fxsPortConfigDvoDoDisturbEn	Do not disturb enable
fxsPortConfigCtOutofservice	CF Out Of Service
fxsPortConfigCfuNumber	CF Unconditional Number (up to 20 characters)
fxsPortConfigCfbNumber	CF Busy Number (up to 20 characters)
fxsPortConfigCfnrNumber	CF No Reply Number (up to 20 characters)
fxsPortConfigCfoosNumber	CF Out Of Service Number (up to 20 characters)
fxsPortConfigDnd	DND
fxsPortConfigEnableCpc	CPC
fxsPortConfigCpcTime	CPC time(ms)
fxsPortConfigSipProfileID	SIP/H323 profile
fxsPortConfigPortProfileID	Subscriber profile
fxsPortConfigUseAltNumberAsContact	Use alternative number as contact (only for serial groups members)
fxsPortConfigCpcRus	Category
fxsPortConfigModifier	Modifier
fxsPortConfigMwiDialtone	MWI

fxsPortConfigRowStatus	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.

FXS settings of subscriber profiles

Object identifier *enterprises.35265.1.9.30.3.1.1.*

profilePortsPlaymoh	Play music on hold
profilePortsAON	CallerID
profilePortsAONHideDate	Hide date
profilePortsAONHideName	Hide Name
profilePortsTaxophone	Taxophone
profilePortsMinFlashtime	Min Flashtime (70 to 1000)
profilePortsMaxFlashtime	Max Flashtime (minflashtime to 1000)
profilePortsGainr	Gain receive (-230 to 20)
profilePortsGaint	Gain transmit (-170 to 60)
profilePortsCategory	SS7 category (SIP-T)
profilePortsCfgPriOverCw	CFB has priority over CW
profilePortsEnableCpc	CPC enable
profilePortsCpcTime	CPC time
profilePortsRowStatus	Row status This parameter is mandatory for SNMP SET. To store data in a file, set '1' as value.
profilePortsCpcRus	CPC-RUS

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.

sipCommonEnablesip	Enable SIP
sipCommonShortmode	Short mode
sipCommonTransport	Transport
sipCommonSipMtu	SIP UDP MTU
sipCommonInviteTotalT	Invite total timeout (1000 to 39000)
sipCommonInviteInitT	Invite initial timeout (100 to 1000)
sipCommonPortRegistrationDelay	Port registration delay (ms)
stunEnable	Use STUN
stunServer	STUN server
stunInterval	STUN interval
sipPublicIp	PublicIP

Configuration of common SIP parameters

Object identifier enterprises.35265.1.9.30.1.1.

sipCommonEnablesip	Enable SIP
sipCommonShortmode	Short mode
sipCommonTransport	Transport
sipCommonSipMtu	SIP UDP MTU
sipCommonInviteTotalT	Invite total timeout (1000 to 39000)
sipCommonInviteInitT	Invite initial timeout (100 to 1000)
sipCommonPortRegistrationDelay	Port registration delay (ms)
stunEnable	Use STUN
stunServer	STUN server
stunInterval	STUN interval

sipPublicIp	PublicIP

These settings match ones described in Section 5.1.2.2.1.

Configuration of common parameters

Object identifier enterprises.35265.1.9.37.

fansForceEnable	Fans force enable
fansThresholdTemperature	Fans threshold temperature
deviceName	Device name
startTimer	Start timer
durationTimer	Duration timer
waitAnswerTimer	Wait answer timer
siptUsePrefix	Use prefix (SIP-T)
siptPrefix	Prefix (SIP-T)

Configuration of port TCP/UDP parameters

Object identifier enterprises.35265.1.9.45.

rtpSipMin	RTP SIP min
rtpSipMax	RTP SIP max
interceptPortMin	Intercept port min
interceptPortMax	Intercept port max
diffservForSip	Diffserv for SIP
diffservForRtp	Diffserv for RTP
verifyRemoteMediaAddress	Verify remote media address

Configuration of call limits

Object identifier enterprises.35265.1.9.46.1.

clType	Host of neighbour gateway radiobutton
clHostOfNeighbourGateway	Host of neighbour gateway area
clSimultaneousCallsCount	Simultaneous calls count
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 ringing service configuration

Object identifier enterprises.35265.1.9.47.1.

drRule	Rule
drRing	Ring, msec
drPause	Pause, msec
drSubscriberProfiles	Subscriber profiles
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 service record, set value 1, to add a record—value 4, to remove a record—value 2.

Automatic update configuration

Object identifier enterprises.35265.1.9.35.

fxsEnableAutoupdate	Enable autoupdate
fxsSource	Source
fxsTFTPServer	Autoupdate server

fxsConfigurationFile	Configuration file
fxsFirmwareVersion	Firmware versions file
fxsConfigurationUpdateInterval	Configuration update interval
fxsFirmwareUpdateInterval	Firmware update interval
autoupdateProtocol	Autoupdate protocol
autoupdateAuth	Autoupdate auth
autoupdateUser	Username
autoupdatePassword	Password

System Log Configuration

Object identifier enterprises.35265.1.9.38.

runSyslog	Run syslog on startup
syslogAddr	Syslog server
syslogPort	Syslog port
appErr	Error
appWarn	Warning
appInfo	Info
appDbg	Debug
sipLevel	SIP Log Level
h323Level	H323 Log Level
vapiEnabled	Enabled
vapiLibLevel	Lib Level
vapiAppLevel	App Level
appAlarm	App Alarm

These settings match ones described in Section 5.1.1.6.

Specific SIP parameters' configuration

Object identifier enterprises.35265.1.9.30.1.3.1.

sipProfileObtimeout	Dial timeout (0 to 300)
sipProfileMode	Proxy mode
sipProfileOptions	Home server test
sipProfileKeepalivet	Keepalive time (10000 to 3600000), ms
sipProfileDomainToReg	Use domain to Register
sipProfileDomain	SIP-Domain (up to 20 characters)
sipProfileRegisterRetryInterval	Registration Retry Interval (10 to 3600)
sipProfileOutbound	Outbound
sipProfileInboundProxy	Inbound
sipProfileExpires	Expires (10 to 345600)
sipProfileAuthentication	Authentication
sipProfileUsername	Username (up to 20 characters)
sipProfilePassword	Password (up to 20 characters)
sipProfileDtmfmime	DTMF MIME Type
sipProfileHfmime	Hook flash MIME Type
sipProfileCtWithReplaces	CT with replaces
sipProfile100Rel	100rel
sipProfileUserPhone	User=Phone
sipProfileUriEscapeHash	Escape hash uri
sipProfileCwRingback	Ringback at callwaiting
sipProfileRingbackSdp	Remote ringback
sipProfileRingback	Ringback at answer 183
sipProfileProxy0	Proxy (up to 40 characters)
sipProfileProxy1	
sipProfileProxy2	

sipProfileProxy3	
sipProfileProxy4	
sipProfileRegrar0	Registrar (up to 40 characters)
sipProfileRegrar1	
sipProfileRegrar2	
sipProfileRegrar3	
sipProfileRegrar4	
sipProfileRegistration0	Use registration
sipProfileRegistration1	
sipProfileRegistration2	
sipProfileRegistration3	
sipProfileRegistration4	
sipProfilePRTPstat	P-RTP-Stat
sipProfileRowStatus	Row status This parameter is mandatory for SNMP SET. To store data in a file, set '1' as value.
sipProfileKeepAliveInterval	NAT Keep Alive Interval (s)
sipProfileKeepAliveMode	NAT Keep Alive Msg
sipProfileConferenceMode	Conference mode
sipProfileConferenceServer	Conference server
sipProfileEnableIMS	Enable IMS
sipProfileXCAPNameForThreePartyConference	XCAP name for three-party conference
sipProfileXCAPNameForHotline	XCAP name for hotline
sipProfileXCAPNameForCallWaiting	XCAP name for call waiting
sipProfileXCAPNameForCallHold	XCAP name for call hold
sipProfileXCAPNameForExplicitCallTransfer	XCAP name for explicit call transfer
sipProfileUseAlertInfo	Alert-Info
sipProfileFullRuriCompliance	Full RURI compliance
sipProfileChangeover	Changeover

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.*

cadenceNumber	Rule number
cadenceName	Alert-Info string
cadenceRingRule	Distinctive Ring rule
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 service 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.

useG711A	Use G.711U
useG711U	Use G.711A
useG726to32	Use G.726-32
useG723	Use G.723
useG729B	Use G.729B
useG729A	Use G.729A
g711Ptime	G.711 Ptime
g729Ptime	G.729 Ptime
g723Ptime	G.723 Ptime
g726to32Ptime	G.726-32 Ptime
g726to32PT	G.726-32 PT
dtmfTransfer	DTMF Transfer

flashTransfer	Flash Transfer
faxDetectDirection	Fax Detect Direction
faxTransferCodec	Fax Transfer Codec
slaveFaxTransferCodec	Slave Fax Transfer Codec
modemTransfer	Modem Transfer
rfc2833PT	rfc2833 PT
silenceSuppression	Silence suppression
echoCanceller	Echo canceller
nlpDisable	NLP disable
comfortNoise	Comfort noise
rtcpTimer	RTCP timer
rtcpControlPeriod	RTCP control period
ciscoNsePT	NSE PT
t38MaxDatagramSize	Max Datagram Size
t38Bitrate	Bitrate
modemFaxDelay	Delay (modem/fax)
voiceMode	Mode
voiceDelayMin	Delay
voiceDelayMax	Delay max
voiceDeletionThreshold	Deletion threshold
voiceDeletionMode	Deletion mode
profilesCodecsRowStatus	Row status This parameter is mandatory for SNMP SET. To store data in a file, set '1' as value.
rfc3264PtCommon	Decoding rfc2833 with PT from answer SDP
rtcpXR	RTCP-XR

✓ **These settings match ones described in Section 5.1.2.2.4.**

Configuration of routing and pickup groups

Object identifier enterprises. *35265.1.9.30.5.1.1.*

Data readout performed for enterprises.35265.1.9.30.5.1.1.fxsDialPlanNext.n identifier allows you to get the number of the next free record in SIP profile routing table. You can configure up to 300 records in total.

profileDialPlanHost	IP address (up to 40 characters)
profileDialPlanDigits	Prefix (up to 20 characters)
profileDialPlanTimeout	Timeout (0 to 20)
profileDialPlanMinDigits	Min Digits (up to 20)
profileDialPlanType	Protocol&Target
profileDialPlanAccessMask	Ingress (up to 108 characters)
profileDialPlanDialtone	Dial tone
profileDialPlanModifier	Modifier (up to 8 characters)
profileDialPlanDelnum	Number of digits to delete (0 to quantity of digits in a number)
profileDialPlanPtime	Ptime (0, 10, 20,… 90)
profileDialPlanRowStatus	Row status This parameter is mandatory for SNMP SET. To store data in a file, its value should be as follows: to change the dialplan record, set value 1, to add a record—value 4, to remove a record—value 2.

✓ **These settings match ones described in Section 5.1.2.2.5.**

Configuration of a Routing Plan Based on Regular Expressions

Object identifier enterprises.35265.1.9.30.5.3.1.

profileRegExpDialOn	Regular expression dialplan

profileRegExpDialProtocol	Protocol
profileRegExpDialText	Expressions
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.

fxsSerialGroupsPhone	Phone (up to 20 characters)
fxsSerialGroupsEnabled	Enabled
fxsSerialGroupsSerialType	Type
fxsSerialGroupsBusyType	Busy
fxsSerialGroupsTimeout	Timeout (0 to 99)
fxsSerialGroupsSipPort	SIP Port (0 to 65535)
fxsSerialGroupsAuthName	Group name (up to 20 characters)
fxsSerialGroupsAuthPass	Password (up to 20 characters)
fxsSerialGroupsPorts	Ports (up to 48 characters)
fxsSerialGroupsSipProfile	Sip Profile
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 0.

SNMP Settings Configuration

Object identifier enterprises.35265.1.9.31.

tauTrapSink	Trap Sink
tauTrapType	Trap Type
tauSysName	Sys Name
tauSysContact	Sys Contact
tauSysLocation	Sys Location
tauRoCommunity	roCommunity
tauRwCommunity	rwCommunity
tauTrapCommunity	trapCommunity
tauUserV3Name	User name
tauUserV3Password	User password
tauViewV3Type	View type
tauRestartSnmp	Allows to restart SNMP client.

These settings match ones described in Section 5.1.1.5.

Configuration of Supplementary Service Codes

Object identifier enterprises.35265.1.9.20.

tauVoipDvoCallwaiting	Call waiting

tauVoipDvoCtAttended	Call transfer attended
tauVoipDvoCtUnattended	Call transfer unattended
tauVoipDvoCfUnconditional	Call forward unconditional
tauVoipDvoCfBusy	Call forward on busy
tauVoipDvoCfNoanswer	Call forward on no answer
tauVoipDvoCfService	Call forward on out of service
tauVoipDvoDoDisturb	Do not disturb

***These settings match ones described in Section 5.1.2.6*.**

Firewall Settings Configuration

Object identifier enterprises.35265.1.9.44.

startingSourceIpAddress	Starting source IP address
numberOfSourceIpAddresses	Number of source IP addresses
allSourceIpAddresses	All source IP addresses
ruleprotocol	Protocol
typeOfMessageICMP	Type of message (ICMP)
startingSourcePort	Starting source port
numberOfSourcePorts	Number of source ports
allSourcePorts	All source ports
startingDestinationPort	Starting destination port
numberOfDestinationPorts	Number of destination ports
allDestinationPorts	All destination ports
ruleTarget	Target
ruleMoveTo	Moves the rule in the table; specify a row to move the rule into (1 to 30).
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.
firewallApply	Apply rules
firewallConfirm	Confirm applied rules

These settings match ones described in Section 5.1.1.7.

Service features

Object identifier enterprises.35265.1.9.

fxsConfigSave	Save configuration into non-volatile memory
fxsReboot	Reboot gateway

5.1.1.5.3 Device Firmware Update

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

Request format: <TFTP server IP address> <Firmware file name>

Example: 192.168.16.44 firmware.img24

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

5.1.1.5.4 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

Request format: <TFTP server IP address> <Configuration file name> upload.

Example: 192.168.16.44 cfgTau24.crypt upload

Device configuration upload

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

Request format: <TFTP server IP address> <Configuration file name> download

Example: 192.168.16.44 cfgTau24.crypt download

Apply loaded changes

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

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

Example: 192.168.16.44 cfgTau24.crypt apply

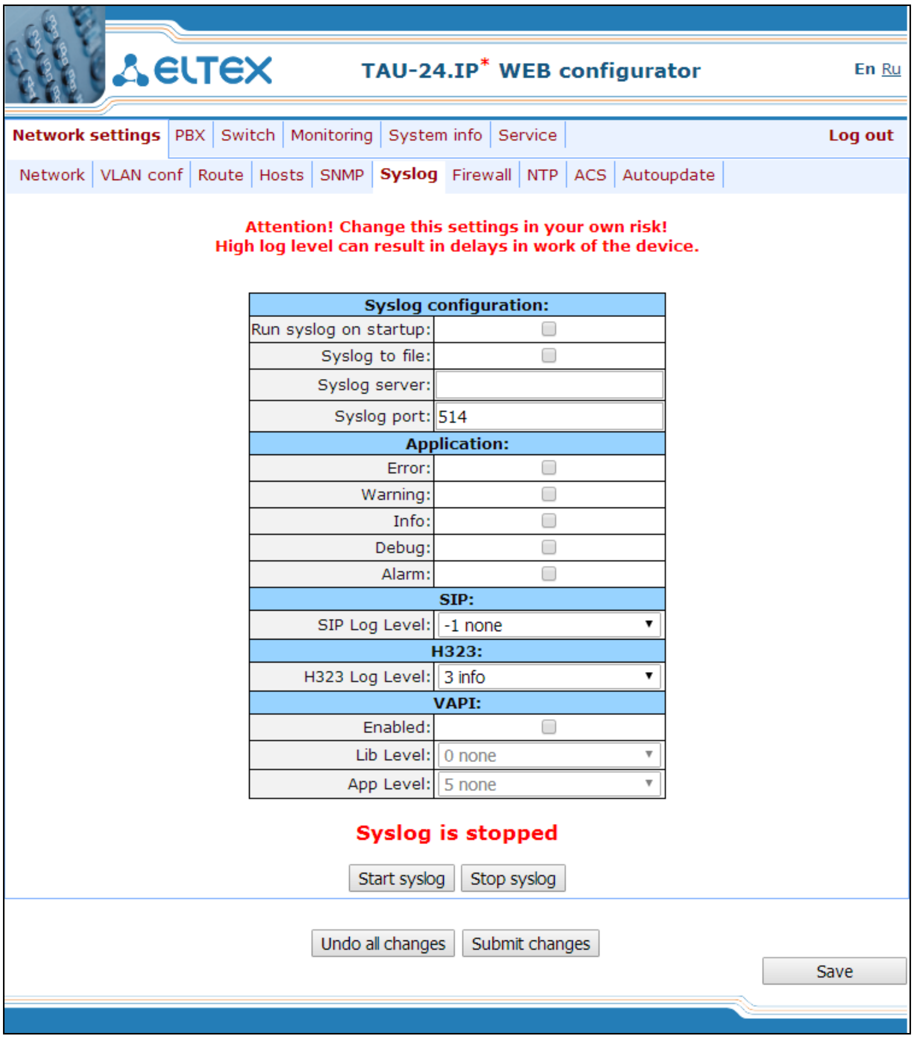
5.1.1.6 Syslog Protocol Configuration

In *'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 without due cause.

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 a Eltex Service Centre Specialist.



Attention! Change this settings in your own risk!
High log level can result in delays in work of the device.

Syslog configuration:	
Run syslog on startup:	□
Syslog to file:	□
Syslog server:	
Syslog port:	514
Application:	
Error:	□
Warning:	□
Info:	□
Debug:	□
Alarm:	□
SIP:	
SIP Log Level:	-1 none
H323:	
H323 Log Level:	3 info
VAPI:	
Enabled:	□
Lib Level:	0 none
App Level:	5 none

Syslog is stopped

<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).

Record type (APPLICATION):

- *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 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.

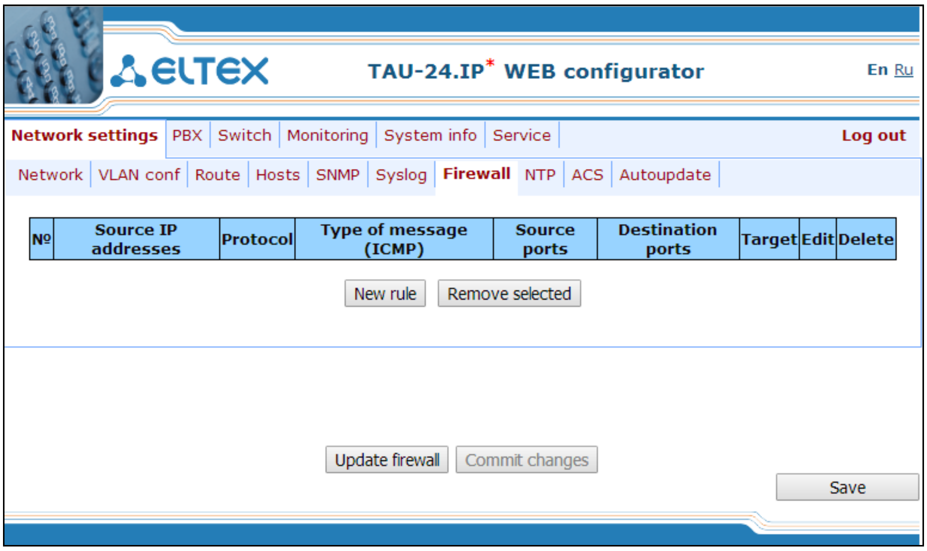
Use *'Start'* and *'Stop'* buttons to start and stop the output of logging information to the system log.

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 *'Undo All Changes'* button. To apply changes, click *'Submit Changes'* button.

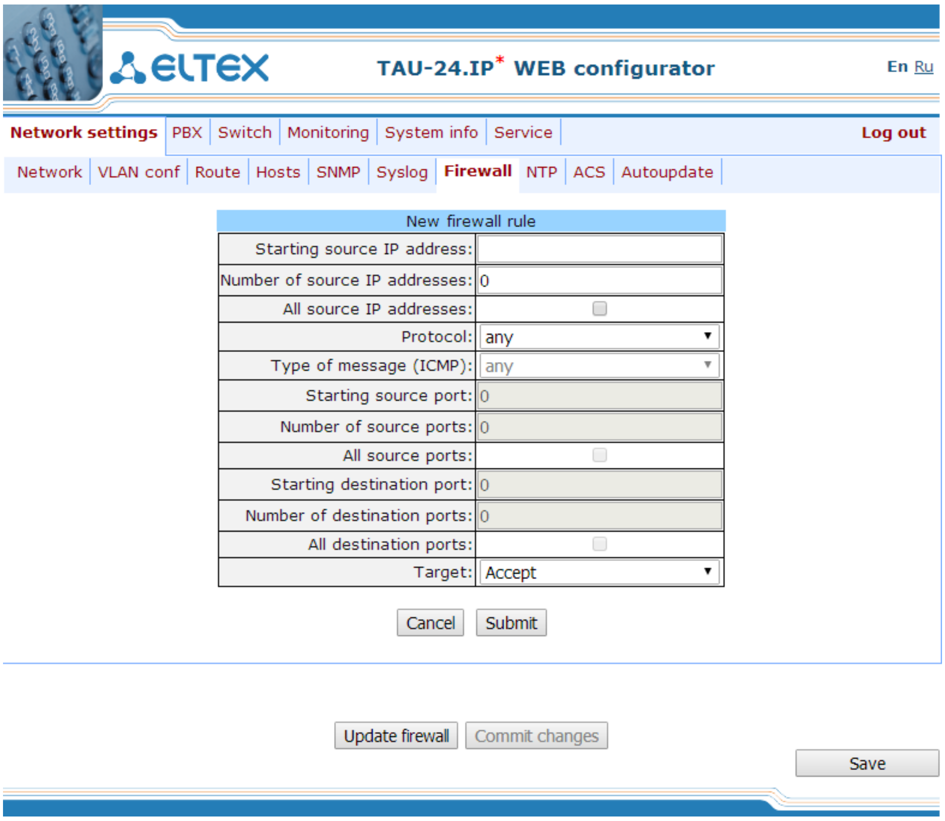
5.1.1.7 Firewall configuration

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



№	Source IP addresses	Protocol	Type of message (ICMP)	Source ports	Destination ports	Target	Edit	Delete

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


ELTEX
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service | Log out
Network | VLAN conf | Route | Hosts | SNMP | Syslog | Firewall | NTP | ACS | Autoupdate
Cancel
Submit
Update firewall
Commit changes
Save

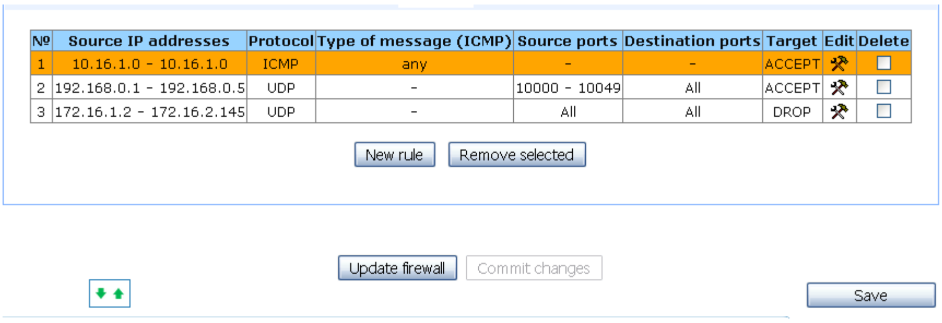
New firewall rule	
Starting source IP address:	
Number of source IP addresses:	0
All source IP addresses:	□
Protocol:	any
Type of message (ICMP):	any
Starting source port:	0
Number of source ports:	0
All source ports:	□
Starting destination port:	0
Number of destination ports:	0
All destination ports:	□
Target:	Accept

New firewall rule:

- *Starting source IP address*—starting IP address of the range of packet sources.
- *Number of source IP addresses*—number of IP addresses in the range of packet sources.
- *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 *'Submit'* button.



№	Source IP addresses	Protocol	Type of message (ICMP)	Source ports	Destination ports	Target	Edit	Delete
1	10.16.1.0 - 10.16.1.0	ICMP	any	-	-	ACCEPT	⚒	□
2	192.168.0.1 - 192.168.0.5	UDP	-	10000 - 10049	All	ACCEPT	⚒	□
3	172.16.1.2 - 172.16.2.145	UDP	-	All	All	DROP	⚒	□

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

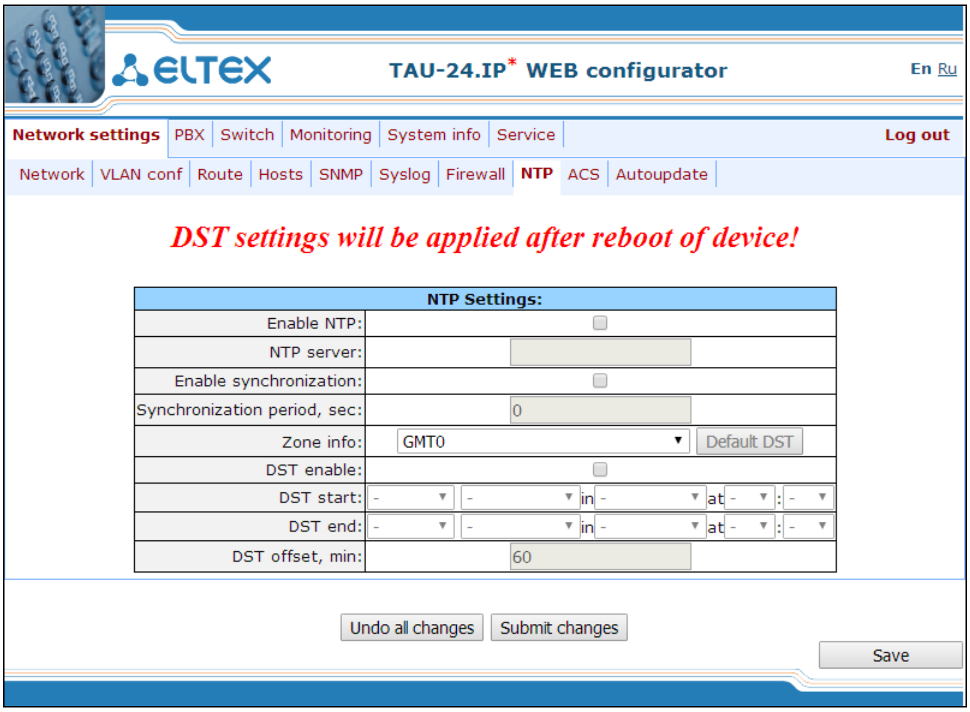
To change the rule sequence, select the necessary rule and move it to the desired position with ⬇⬆ buttons.

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

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

5.1.1.8 NTP Configuration

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.



DST settings will be applied after reboot of device!

NTP Settings:	
Enable NTP:	□
NTP server:	
Enable synchronization:	□
Synchronization period, sec:	0
Zone info:	GMT0 ▾ Default DST
DST enable:	□
DST start:	- ▾ - ▾ in - ▾ at - ▾ : - ▾
DST end:	- ▾ - ▾ in - ▾ at - ▾ : - ▾
DST offset, min:	60

– *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 K**.

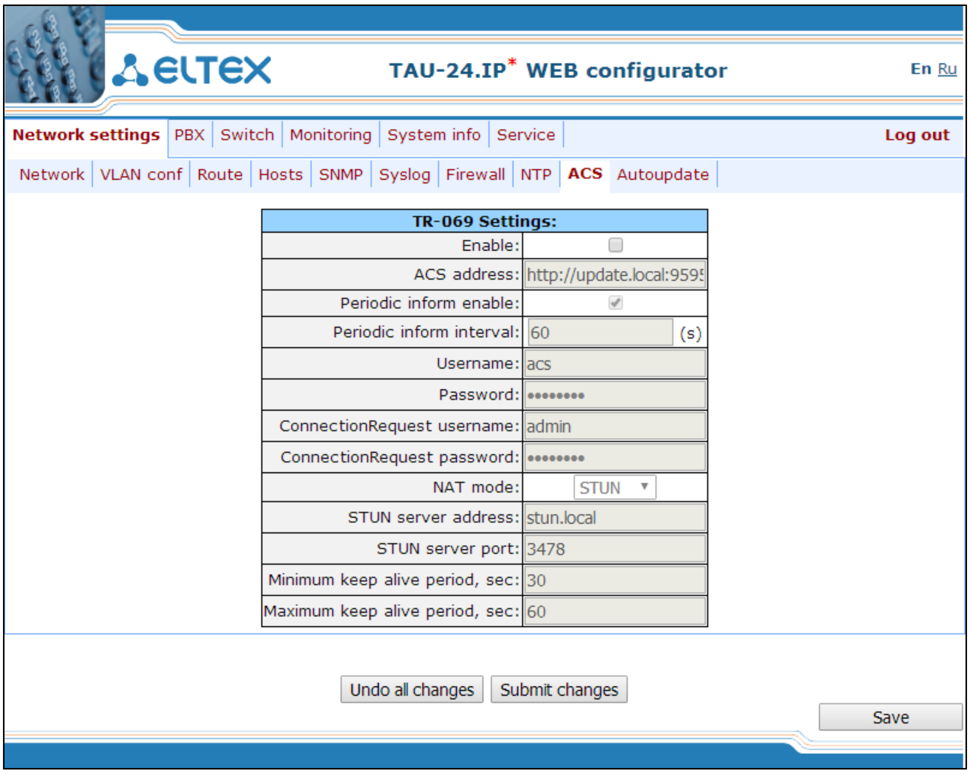
Exclamation mark symbol means that DST settings are not used for this timezone!

DST settings will be applied only after the device is restarted!

- *DST enable*—when checked, device will perform daylight saving change and the set back process.
- *Default DST*—allows to set standard DST periods for the current timezone.
- *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 *'Undo All Changes'* button. To apply changes, click *'Submit Changes'* button.

5.1.1.9 TR-069 Monitoring and Management Protocol Configuration (ACS)



TR-069 Settings:	
Enable:	□
ACS address:	http://update.local:959
Periodic inform enable:	☑
Periodic inform interval:	60 (s)
Username:	acs
Password:	••••••••
ConnectionRequest username:	admin
ConnectionRequest password:	••••••••
NAT mode:	STUN
STUN server address:	stun.local
STUN server port:	3478
Minimum keep alive period, sec:	30
Maximum keep alive period, sec:	60

TR-069 Monitoring and Management Protocol Settings (TR-069 Settings):

- *Enable*—when checked, enable device management via TR-069 protocol.
- *ACS address*—ACS server address. Enter address in the following format: http://<address>:<port> (<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 password*—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:

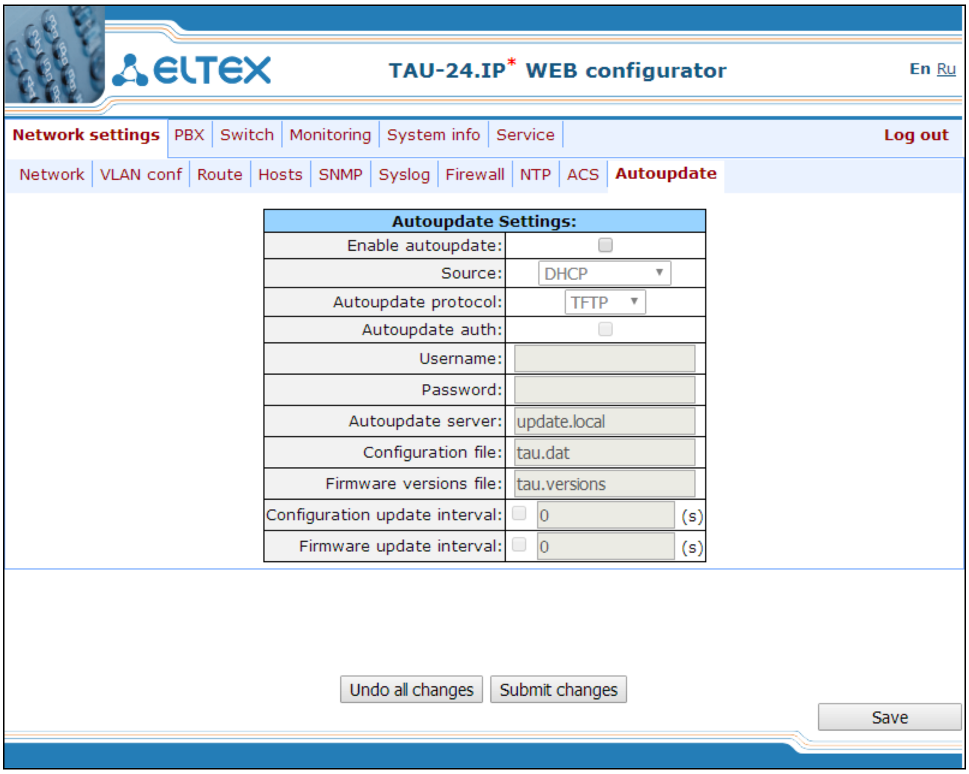
  - *STUN*—use STUN protocol for public address identification. When choosing STUN client operation mode, you should define the following settings:
    - *STUN server address*—STUN server IP address or domain name.
    - *STUN server port*—STUN server UDP port (3478 by default).
    - *Minimum keep alive 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 *'Undo All Changes'* button. To apply changes, click *'Submit Changes'* button.

5.1.1.10 Automatic update configuration (Autoupdate)



Autoupdate Settings:

Enable autoupdate:	□
Source:	DHCP
Autoupdate protocol:	TFTP
Autoupdate auth:	□
Username:	
Password:	
Autoupdate server:	update.local
Configuration file:	tau.dat
Firmware versions file:	tau.versions
Configuration update interval:	□ 0 (s)
Firmware update interval:	□ 0 (s)

Automatic update settings (Autoupdate)

- *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 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 update interval* —when checked, automatically update configuration with the specified period in seconds.
- *Firmware update interval* —when checked, automatically update firmware with the specified period in seconds.

For autoupdate system operating procedure, see **Appendix F**. **Automatic Configuration Procedure and Gateway Firmware Version Check.**

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

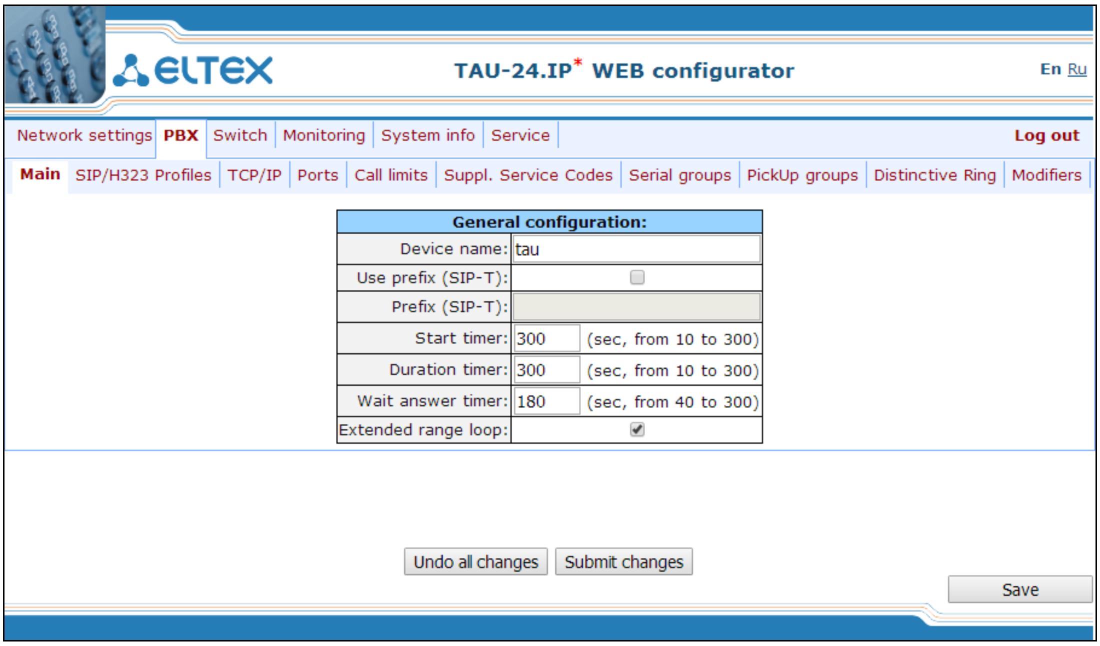
03—Login suboption value.
03—length, 3bytes.
61:63:73—suboption value (acs).
04—Password suboption value.
06—length, 6bytes.
61:63:73:61:63:73—suboption value (acsacs).

5.1.2 VoIP Configuration (*PBX)*

In '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 Basic Configuration (Main)

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



General configuration:		
Device name:	tau	
Use prefix (SIP-T):	☐	
Prefix (SIP-T):		
Start timer:	300	(sec, from 10 to 300)
Duration timer:	300	(sec, from 10 to 300)
Wait answer timer:	180	(sec, from 40 to 300)
Extended range loop:	☑	

<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).**

— *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.

– *Duration timer*—complete number dialling timeout. Takes effect after the first digit of a number has been dialled, 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.

– *Extended range loop*—enable extended range mode. If 'Extended range loop' option is not set, power supply voltage of subscriber units equals to 34V, current in a closed loop—22mA. Maximum loop resistance is 1.5kΩ. Fans will start only when submodule sensor temperature exceeds 95°C (ambient temperature 43-46°C), also they will start at their minimum speed. If 'Extended range loop' option is set, power supply voltage of subscriber units equals to 54V, current in a closed loop—25mA. Maximum loop resistance is 2.1kΩ. In this mode, fans will start using the following algorithm:

  - When temperature of any submodule exceeds the threshold value ('Fans threshold temperature'), fans will start at 1/2 speed.
  - When temperature of any submodule exceeds the threshold value by 5°C, fans will start at 5/8 speed.
  - When temperature of any submodule exceeds the threshold value by 10°C, fans will start at 6/8 speed.
  - When temperature of any submodule exceeds the threshold value by 15°C, fans will start at 7/8 speed.
  - When temperature of any submodule exceeds the threshold value by 20°C, fans will start at maximum speed.

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

5.1.2.2 *SIP/H323 Profiles*

In '*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 *SIP Common Parameters (SIP Common)*

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

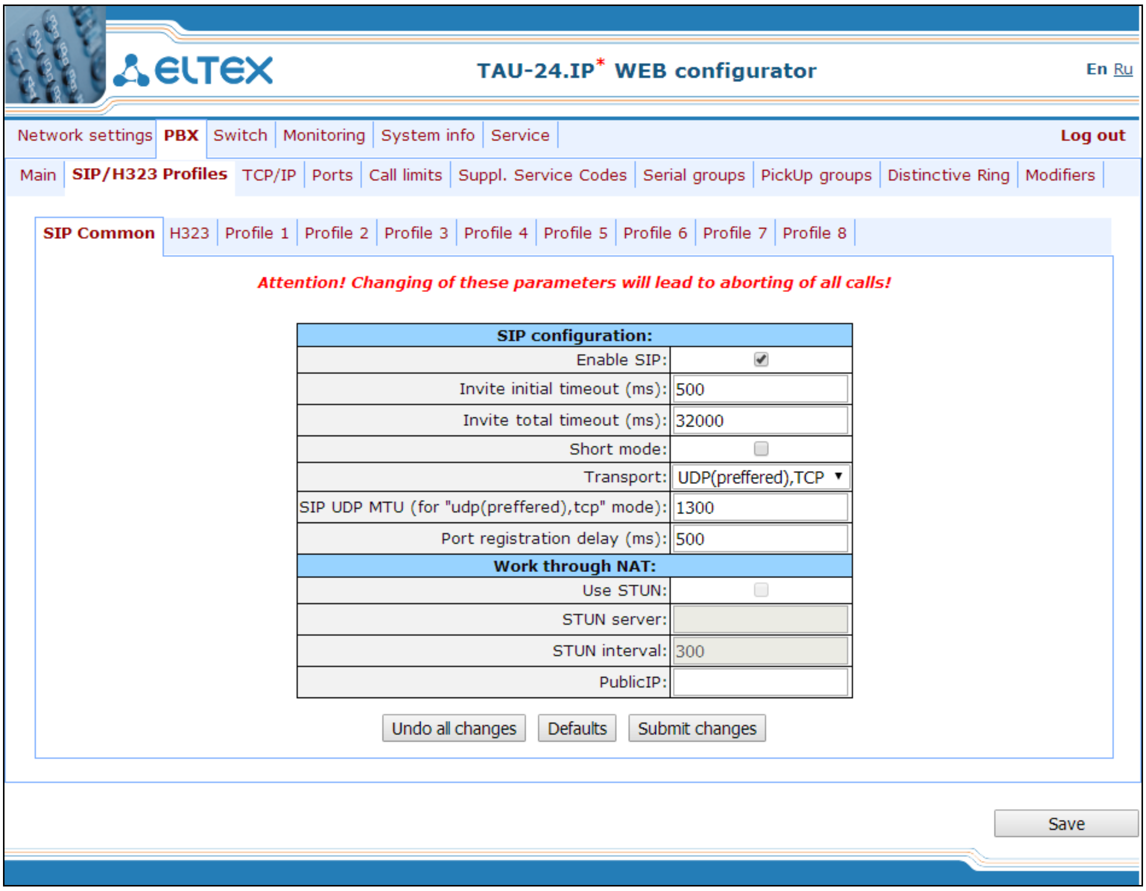
SIP (Session Initiation Protocol) is a signalling protocol, used in IP telephony. It performs basic call management tasks such as starting and finishing session.

Addressing in SIP network based on SIP URI scheme:

sip:user@host:port;uri-parameters

where:
user—number of a SIP subscriber.
@—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 will not clear-back calls, if SIP subscriber's number contains the following characters: '+', ';', '=', '?'.



Attention! Changing of these parameters will lead to aborting of all calls!

SIP configuration:	
Enable SIP:	☑
Invite initial timeout (ms):	500
Invite total timeout (ms):	32000
Short mode:	☐
Transport:	UDP(preffered),TCP ▼
SIP UDP MTU (for "udp(preffered),tcp" mode):	1300
Port registration delay (ms):	500
Work through NAT:	
Use STUN:	☐
STUN server:	
STUN interval:	300
PublicIP:	

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

SIP configuration:

- *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).
- *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:

$$\textit{Invite total timeout} = 100 + \sum_{n=0}^{N-1} (2^n)\cdot \text{Invite\_initial\_timeout}$$

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

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

5.1.2.2.1.1. SIP-T Protocol Configuration

Configure the following parameters to utilize SIP-T protocol:

- 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 Basic Configuration (Main);**

- 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**;

- 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 Ports**;
- To receive international calls with '+' symbol preceding the number, you should configure 'User=Phone' option, see Section **5.1.2.2.3 SIP Custom Parameters (Profile *N* SIP *Custom*)**.

5.1.2.2.2 H.323 Protocol

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.

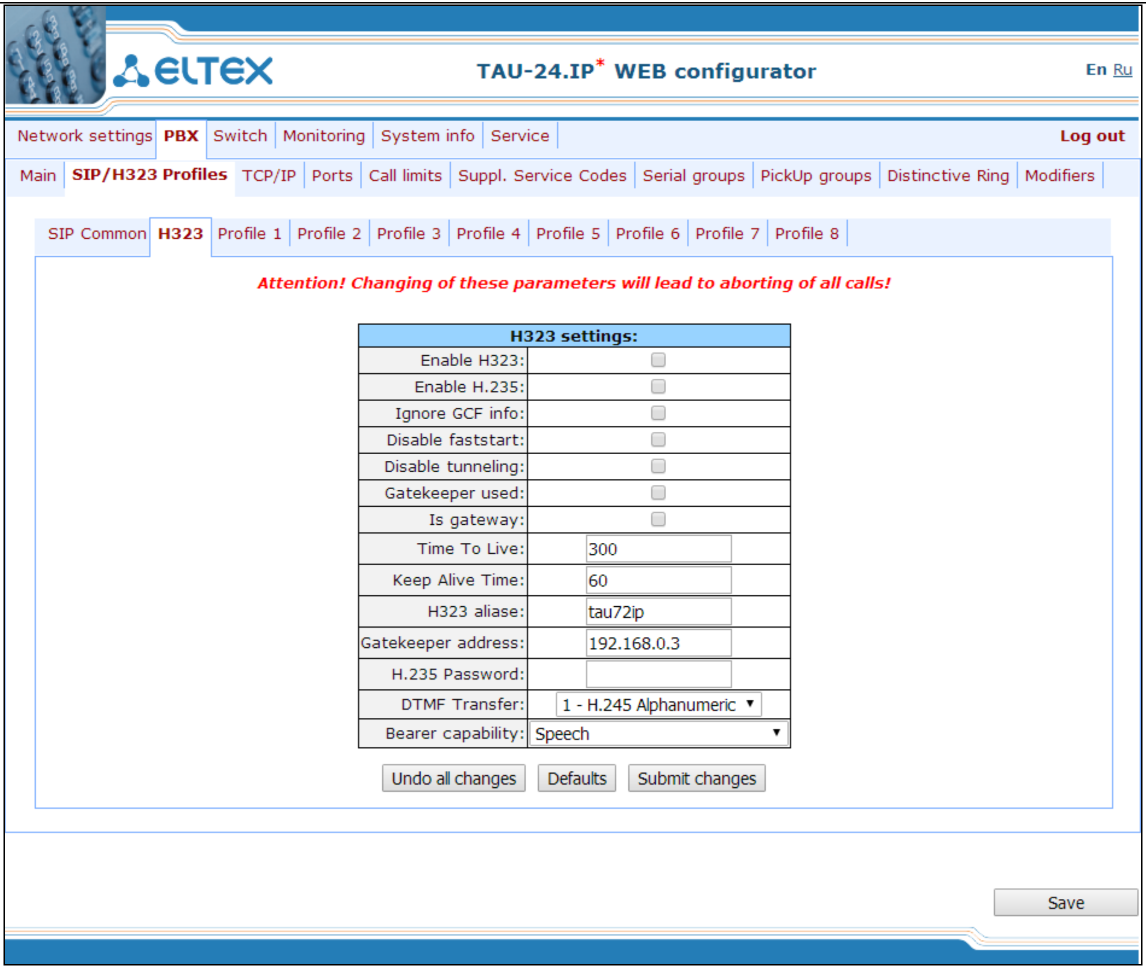
H.323 stack of TAU gateway supports the following protocols:

- *H.245*—allows 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.


ELTEX
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service | Log out
Main | SIP/H323 Profiles | TCP/IP | Ports | Call limits | Suppl. Service Codes | Serial groups | PickUp groups | Distinctive Ring | Modifiers
SIP Common | H323 | Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 | Profile 7 | Profile 8
Undo all changes
Defaults
Submit changes
Save

Attention! Changing of these parameters will lead to aborting of all calls!

H323 settings:	
Enable H323:	☐
Enable H.235:	☐
Ignore GCF info:	☐
Disable faststart:	☐
Disable tunneling:	☐
Gatekeeper used:	☐
Is gateway:	☐
Time To Live:	300
Keep Alive Time:	60
H323 aliase:	tau72ip
Gatekeeper address:	192.168.0.3
H.235 Password:	
DTMF Transfer:	1 - H.245 Alphanumeric
Bearer capability:	Speech

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

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

H323 settings:

- *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 tunnelling 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*.

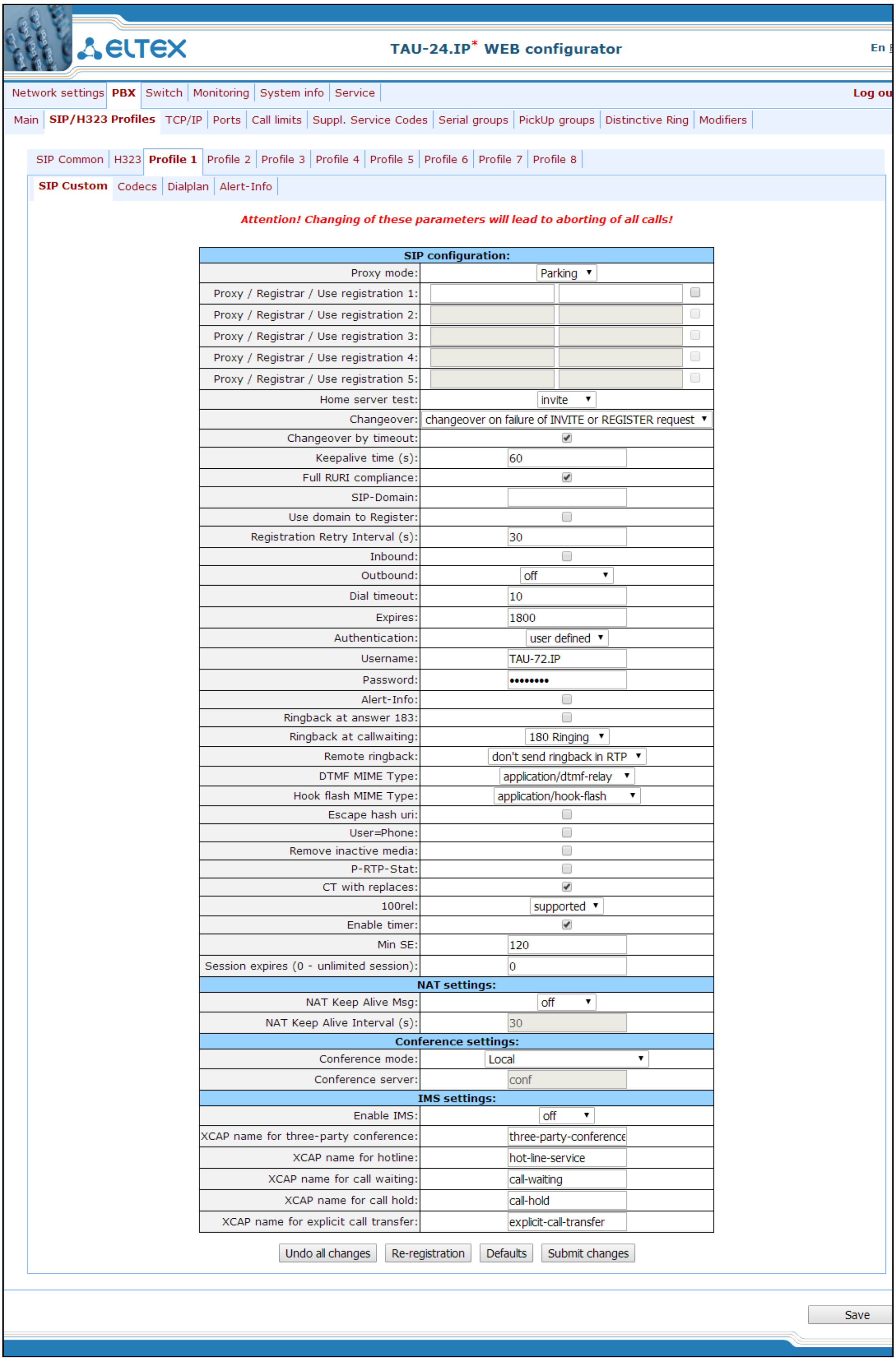
To ensure the successful renewal of device registration on gatekeeper, specify *Keep Alive Time* renewal period equal to 2/3 of *Time To Live* registration period. Moreover, for *Time To Live* parameter, we recommend specifying the same value as for the gatekeeper, so the registration renewal period—*Keep 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.

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

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.



ELTEX
TAU-24.IP* WEB configurator
En
Network settings | PBX | Switch | Monitoring | System info | Service
Log ou
Main | SIP/H323 Profiles | TCP/IP | Ports | Call limits | Suppl. Service Codes | Serial groups | PickUp groups | Distinctive Ring | Modifiers
SIP Common | H323 | Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 | Profile 7 | Profile 8
SIP Custom | Codecs | Dialplan | Alert-Info

Attention! Changing of these parameters will lead to aborting of all calls!

SIP configuration:	
Proxy mode:	Parking
Proxy / Registrar / Use registration 1:	☐
Proxy / Registrar / Use registration 2:	☐
Proxy / Registrar / Use registration 3:	☐
Proxy / Registrar / Use registration 4:	☐
Proxy / Registrar / Use registration 5:	☐
Home server test:	invite
Changeover:	changeover on failure of INVITE or REGISTER request
Changeover by timeout:	☑
Keepalive time (s):	60
Full RURI compliance:	☑
SIP-Domain:	
Use domain to Register:	☐
Registration Retry Interval (s):	30
Inbound:	☐
Outbound:	off
Dial timeout:	10
Expires:	1800
Authentication:	user defined
Username:	TAU-72.IP
Password:	••••••••
Alert-Info:	☐
Ringback at answer 183:	☐
Ringback at callwaiting:	180 Ringing
Remote ringback:	don't send ringback in RTP
DTMF MIME Type:	application/dtmf-relay
Hook flash MIME Type:	application/hook-flash
Escape hash uri:	☐
User=Phone:	☐
Remove inactive media:	☐
P-RTP-Stat:	☐
CT with replaces:	☑
100rel:	supported
Enable timer:	☑
Min SE:	120
Session expires (0 - unlimited session):	0
NAT settings:	
NAT Keep Alive Msg:	off
NAT Keep Alive Interval (s):	30
Conference settings:	
Conference mode:	Local
Conference server:	conf
IMS settings:	
Enable IMS:	off
XCAP name for three-party conference:	three-party-conference
XCAP name for hotline:	hot-line-service
XCAP name for call waiting:	call-waiting
XCAP name for call hold:	call-hold
XCAP name for explicit call transfer:	explicit-call-transfer

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:

- 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:
- 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.

SIP configuration:

- *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.
- *Change-over*—this setting defines the request transmission error that will be used for redundant proxy changeover: INVITE and REGISTER, INVITE only or REGISTER only.
- *Changeover by timeout*—when enabled, redundant proxy changeover will be performed when response 408 is received, in addition to standard responses 503 and 505.
- *Keepalive time (s)*—period of time between OPTIONS or REGISTER management message transfers, in seconds.
- *Full RURI compliance*—when checked, all URI elements (*user, 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 Register*—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 routing plan.
  - *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' *settings.*
- *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*—when an incoming call is received, the gateway will not generate a ringback tone.
  - *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 '183progress' 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 I.

- *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'* setting.
- *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.

Conference settings:

- *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.

IMS settings:

- *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 *Re-registration* button.

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

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

Setting operation for outgoing communications:

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

Setting operation for incoming communications:

- supported, required—when the following tag is received in 'INVITE' request—supported: 100rel, or required: 100rel—perform reliable transfer of provisional replies. If there is no supported: 100rel tag in INVITE request, the gateway will perform unreliable transfer of provisional replies.
- 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 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.

SIP domain configuration order for 'n' profile:

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

TAU 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.

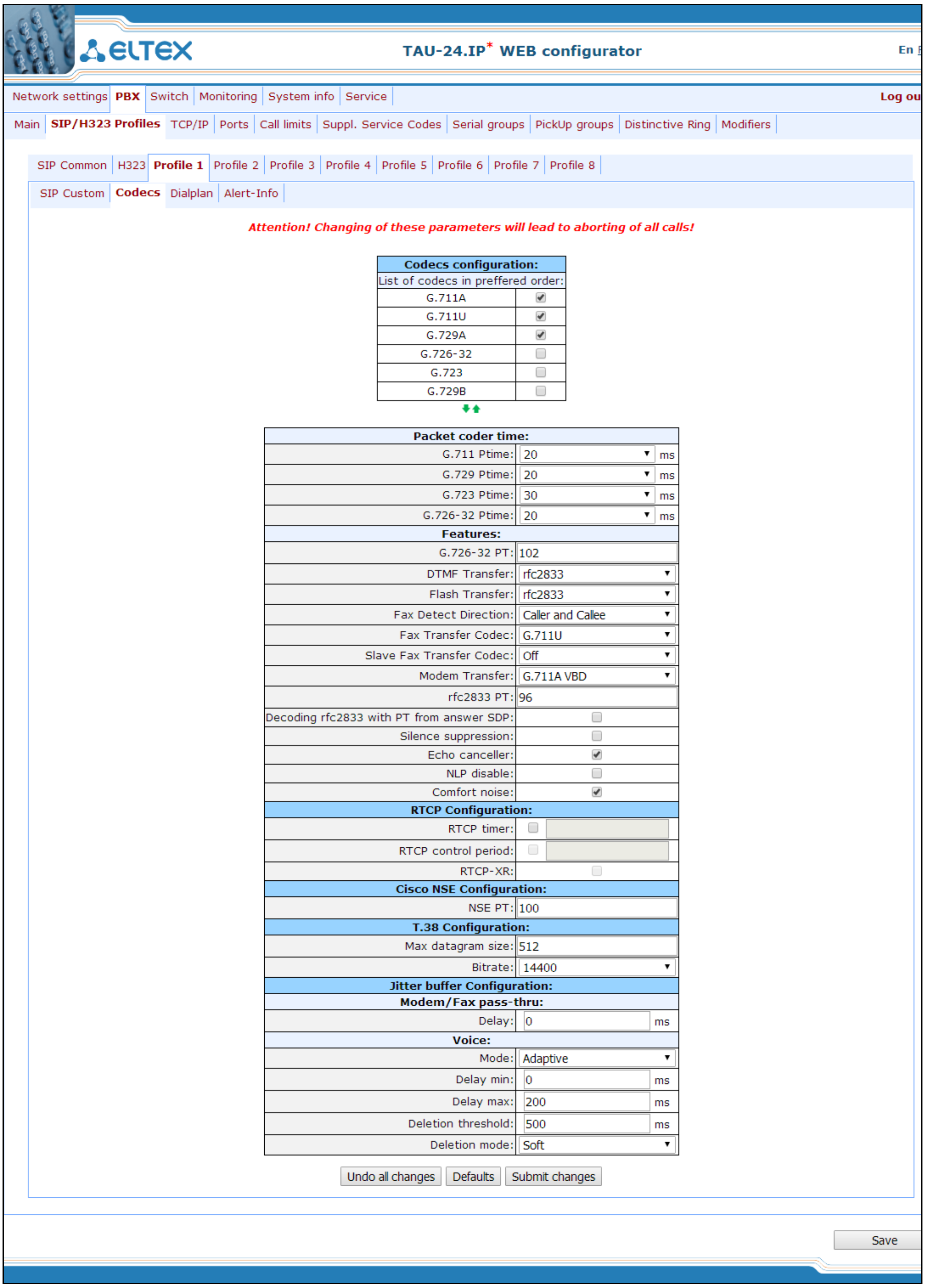
! **You don't have to reboot the gateway in order to apply codec settings. When applying settings, all current calls will be terminated!!!**

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.


ELTEX
TAU-24.IP* WEB configurator
En
Network settings | PBX | Switch | Monitoring | System info | Service
Log ou
Main | SIP/H323 Profiles | TCP/IP | Ports | Call limits | Suppl. Service Codes | Serial groups | PickUp groups | Distinctive Ring | Modifiers
SIP Common | H323 | Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 | Profile 7 | Profile 8
SIP Custom | Codecs | Dialplan | Alert-Info
Undo all changes
Defaults
Submit changes
Save

Attention! Changing of these parameters will lead to aborting of all calls!

Codecs configuration:	
List of codecs in preffered order:	
G.711A	☑
G.711U	☑
G.729A	☑
G.726-32	☐
G.723	☐
G.729B	☐

Packet coder time:		
G.711 Ptime:	20	ms
G.729 Ptime:	20	ms
G.723 Ptime:	30	ms
G.726-32 Ptime:	20	ms
Features:		
G.726-32 PT:	102	
DTMF Transfer:	rfc2833	
Flash Transfer:	rfc2833	
Fax Detect Direction:	Caller and Callee	
Fax Transfer Codec:	G.711U	
Slave Fax Transfer Codec:	Off	
Modem Transfer:	G.711A VBD	
rfc2833 PT:	96	
Decoding rfc2833 with PT from answer SDP:	☐	
Silence suppression:	☐	
Echo canceller:	☑	
NLP disable:	☐	
Comfort noise:	☑	
RTCP Configuration:		
RTCP timer:	☐	
RTCP control period:	☐	
RTCP-XR:	☐	
Cisco NSE Configuration:		
NSE PT:	100	
T.38 Configuration:		
Max datagram size:	512	
Bitrate:	14400	
Jitter buffer Configuration:		
Modem/Fax pass-thru:		
Delay:	0	ms
Voice:		
Mode:	Adaptive	
Delay min:	0	ms
Delay max:	200	ms
Deletion threshold:	500	ms
Deletion mode:	Soft	

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 Ptime*—for G.726-32 codec (permitted values: 10, 20, 30).
- *G.726-32 PT*—G.726-32 codec payload type (permitted values: 96 to 127).

In *'Features'* section:

- *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 **5.1.2.4**).
  - *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 tones 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).
- *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 ***'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 is 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.

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 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.

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.

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

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

5.1.2.2.5 Routing and Pickup Code Configuration *(Profile N Dialplan)*

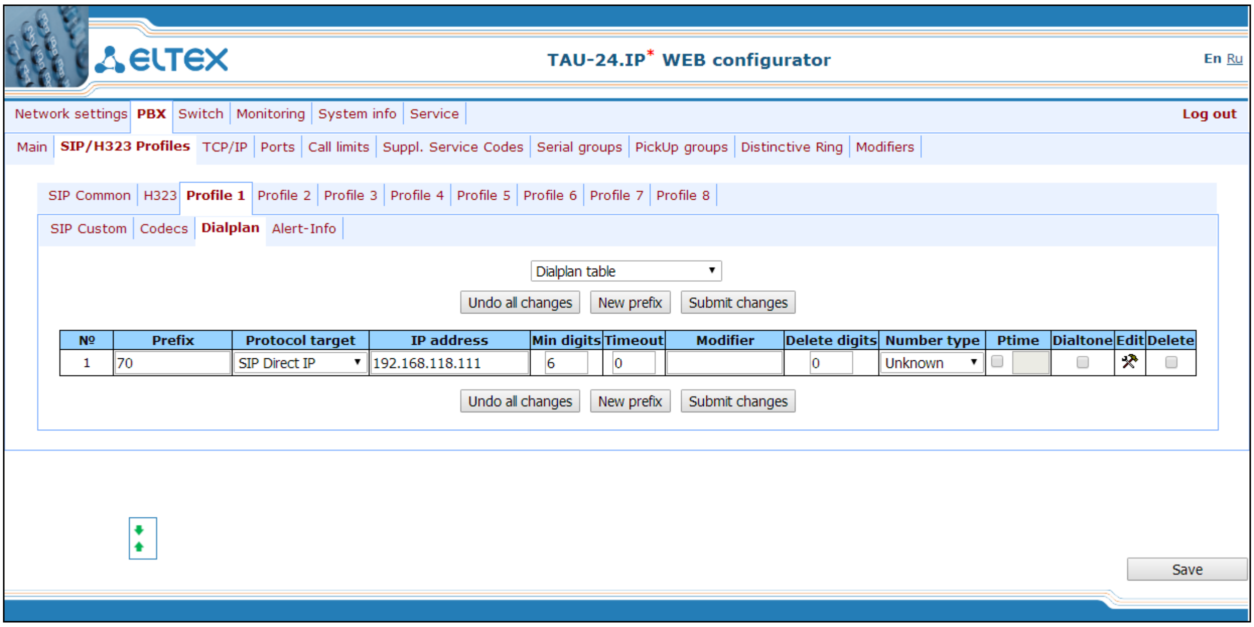
In *'Profile n/Dialplan'* submenu, you may configure prefixes for routing and pickup groups for each profile.

TAU-32M.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 dialled number and the dialling timeout, it comprises the routing rule. If a number dialled by the subscriber falls within the scope of a single rule, the call will be routed by this rule. If a dialled number falls within the scope of multiple rules, the call will be routed by the rule with the highest priority. When dialled 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 dialled number is not limited, and the end of dialling occurs on the expiration of 'outbound' timer, or on '#' button pressed. 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 Routing and Pickup Code Configuration *(Profile N Dialplan)***.



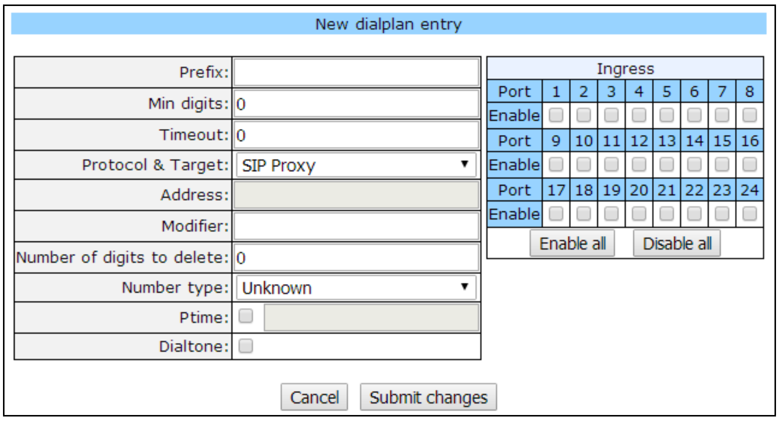
ELTEX
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Main | SIP/H323 Profiles | TCP/IP | Ports | Call limits | Suppl. Service Codes | Serial groups | PickUp groups | Distinctive Ring | Modifiers
SIP Common | H323 | Profile 1 | Profile 2 | Profile 3 | Profile 4 | Profile 5 | Profile 6 | Profile 7 | Profile 8
SIP Custom | Codecs | Dialplan | Alert-Info
Dialplan table
Undo all changes
New prefix
Submit changes
Save

Nº	Prefix	Protocol target	IP address	Min digits	Timeout	Modifier	Delete digits	Number type	Ptime	Dialtone	Edit	Delete
1	70	SIP Direct IP	192.168.118.111	6	0		0	Unknown	□	□	🛠	□

5.1.2.2.5.1 Dialplan 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 *'New prefix'* button:



New dialplan entry

Prefix:	
Min digits:	0
Timeout:	0
Protocol & Target:	SIP Proxy ▾
Address:	
Modifier:	
Number of digits to delete:	0
Number type:	Unknown ▾
Ptime:	□
Dialtone:	□

Ingress

Port	1	2	3	4	5	6	7	8
Enable	□	□	□	□	□	□	□	□
Port	9	10	11	12	13	14	15	16
Enable	□	□	□	□	□	□	□	□
Port	17	18	19	20	21	22	23	24
Enable	□	□	□	□	□	□	□	□

- *Prefix.*
- *Min digits*—minimum length of a number dialled by the prefix.
- *Timeout*—dialling timeout for the next digit of a number, in seconds. Begins operation, when the minimum length of a number dialled by the prefix is achieved. If the minimum length of a dialled number is already achieved, and no digits have been dialled 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 dialled number.
- *Number of digits to delete*—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).

  When outgoing call is performed using a prefix, the digit deletion modifier ('Number of digits to delete') is applied first to the dialled 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 dialled. 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 '*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 *'Undo All Changes'* button. To apply changes, click *'Submit Changes'* button. To store changes to non-volatile memory of the device, click *'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:

4 In *'Min digits'* field, enter a minimum quantity of digits for routing with this prefix.

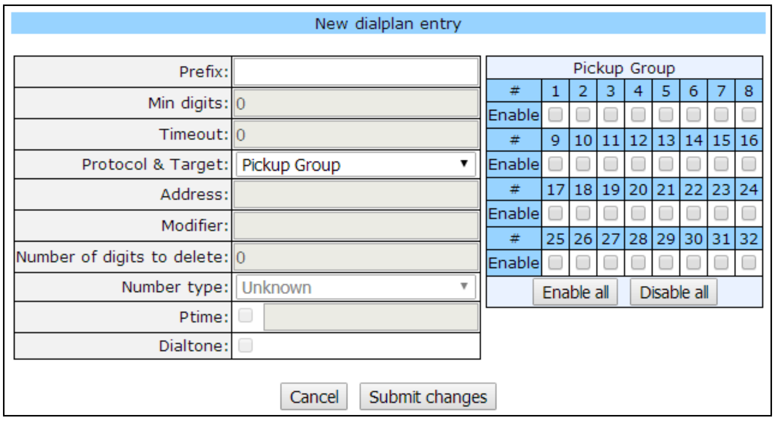
5 In 'Timeout' field, dialling timeout for the next digit of a number should be greater than zero. In this case, when user dials the number with length that matches the minimum quantity of digits, gateway will wait for the next digit dialling during the specified timeout. If the digit is not dialled,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

6 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.

7 *'Stop* dial *at #'* function allows to perform a call after the necessary quantity of digits are dialled without the wait for a timeout. It may be configured separately for each port in *'PBX/Ports/Edit/Custom'* tab. 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:



New dialplan entry

Prefix:	
Min digits:	0
Timeout:	0
Protocol & Target:	Pickup Group ▾
Address:	
Modifier:	
Number of digits to delete:	0
Number type:	Unknown ▾
Ptime:	□
Dialtone:	□

Pickup Group

#	1	2	3	4	5	6	7	8
Enable	□	□	□	□	□	□	□	□
#	9	10	11	12	13	14	15	16
Enable	□	□	□	□	□	□	□	□
#	17	18	19	20	21	22	23	24
Enable	□	□	□	□	□	□	□	□
#	25	26	27	28	29	30	31	32
Enable	□	□	□	□	□	□	□	□

Configuration of pickup groups affects the following settings:

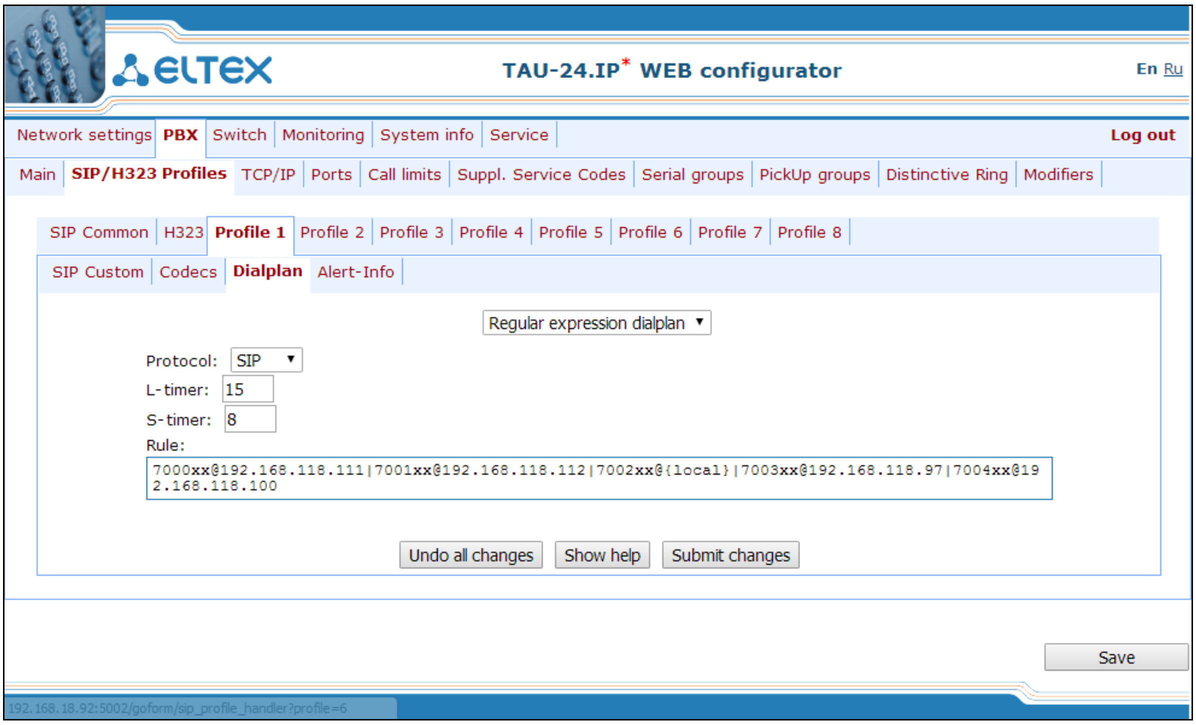
- *Prefix*—pickup code. Sequence of digits (for example, *8) that, when dialled, allows any subscriber of the group to pickup the call received by another subscriber of the group.
- *Protocol&Target*—it's necessary to select a pickup group—PickUp.
- *PickUp Group*—defines the list of groups, that will 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 *'Enable all'* button. To disable this pickup code for all groups, click *'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.



Regular expression dialplan

Protocol: SIP

L-timer: 15

S-timer: 8

Rule:

```
7000xx@192.168.118.111|7001xx@192.168.118.112|7002xx@{local}|7003xx@192.168.118.97|7004xx@19
2.168.118.100
```

- *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

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)

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.
- *****—* 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}—'5' could be dialled 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.

- **'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 dialled 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).

Timers

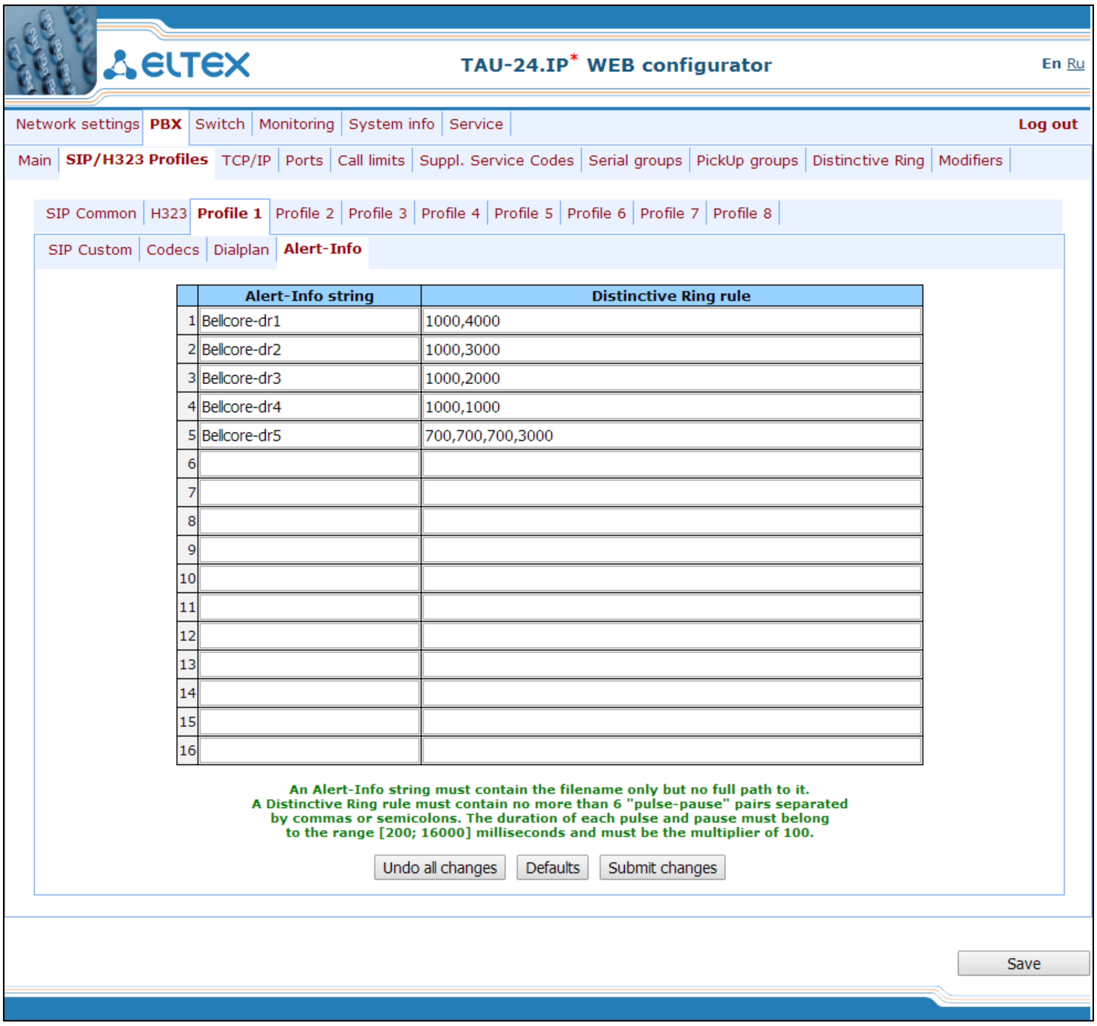
- **S-timer—**activates, when the dialling complies with one of the rules, but it is possible that further dialling will achieve compliance with another rule.
- **L-timer**—activates, when the gateway detects the necessity of dialling of at least one more digit in order to achieve the compliance with 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
L20 8,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 *'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	Distinctive Ring rule
1	Bellcore-dr1	1000,4000
2	Bellcore-dr2	1000,3000
3	Bellcore-dr3	1000,2000
4	Bellcore-dr4	1000,1000
5	Bellcore-dr5	700,700,700,3000
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

An Alert-Info string must contain the filename only but no full path to it.
A Distinctive Ring rule must contain no more than 6 "pulse-pause" pairs separated by commas or semicolons. The duration of each pulse and pause must belong to the range [200; 16000] milliseconds and must be the multiplier of 100.

- *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.

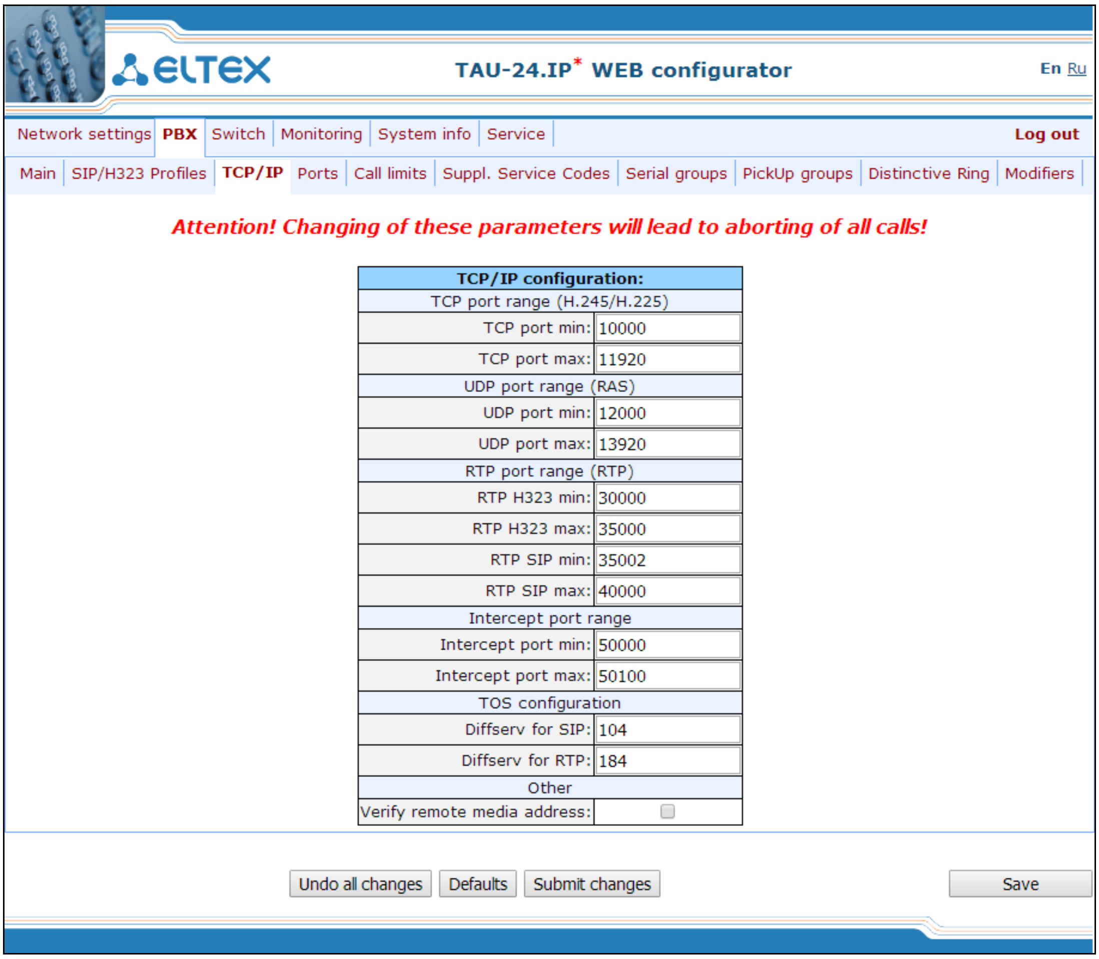
The rule includes up to 6 pairs of impulse/pause values; all values are comma-separated. Each value must be divisible by 100 and fall within the range from 200 to 16000ms.

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 Configuration of network ports (TCP/IP)

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.



Attention! Changing of these parameters will lead to aborting of all calls!

TCP/IP configuration:	
TCP port range (H.245/H.225)	
TCP port min:	10000
TCP port max:	11920
UDP port range (RAS)	
UDP port min:	12000
UDP port max:	13920
RTP port range (RTP)	
RTP H323 min:	30000
RTP H323 max:	35000
RTP SIP min:	35002
RTP SIP max:	40000
Intercept port range	
Intercept port min:	50000
Intercept port max:	50100
TOS configuration	
Diffserv for SIP:	104
Diffserv for RTP:	184
Other	
Verify remote media address:	□

<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—configuration of Diffserv:

- *Diffserv for SIP*—type of service for SIP packets. You may configure all 8-bit Diffserv fields (DSCP bits—6 high bits) sent in IP protocol header; parameter value should be specified decimally. For utilized values, see Table 7.
- *Diffserv for RTP*—type of service for RTP packets. You may configure all 8-bit Diffserv fields (DSCP bits—6 high bits) sent in IP protocol header; parameter value should be specified decimally. For utilized values, see Table 7.

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 7—'Type of service for RTP packets' (Diffserv) field value:

Diffserv field value	Description
0 (0x00)	(DSCP 0x00) – Best effort – default value
32 (0x20)	(DSCP 0x08) – Class 1
40 (0x28)	(DSCP 0x0A)– assured forwarding, low drop precedence (Class1, AF11)
48 (0x30)	(DSCP 0x0C)– assured forwarding, medium drop precedence (Class1, AF12)
56 (0x38)	(DSCP 0x0E)– assured forwarding, high drop precedence (Class1, AF13)
64 (0x40)	(DSCP 0x10) – Class 2
72 (0x48)	(DSCP 0x12)– assured forwarding, low drop precedence (Class2, AF21)
80 (0x50)	(DSCP 0x14)– assured forwarding, medium drop precedence (Class2, AF22)
88 (0x58)	(DSCP 0x16)– assured forwarding, high drop precedence (Class2, AF23)
96 (0x60)	(DSCP 0x18) – Class 3
104 (0x68)	(DSCP 0x1A)– assured forwarding, low drop precedence (Class3, AF31)
112 (0x70)	(DSCP 0x1C)– assured forwarding, medium drop precedence (Class3, AF32)
120 (0x78)	(DSCP 0x1E)– assured forwarding, high drop precedence (Class3, AF33)
128 (0x80)	(DSCP 0x20) – Class 4
136 (0x88)	(DSCP 0x22)– assured forwarding, low drop precedence (Class4, AF41)
144 (0x90)	(DSCP 0x24)– assured forwarding, medium drop precedence (Class4, AF42)
152 (0x98)	(DSCP 0x26)– assured forwarding, high drop precedence (Class4, AF43)
160 (0xA0)	(DSCP 0x28) – Class 5

184 (0xB8)	(DSCP 0x2E) – expedited forwarding (Class5, Expedited Forwarding)
IP Precedence:	
0 (0x00)	IPP0 (Routine)
32 (0x20)	IPP1 (Priority)
64 (0x40)	IPP2 (Immediate)
96 (0x60)	IPP3 (Flash)
128 (0x80)	IPP4 (Flash Override)
160 (0xA0)	IPP5 (Critical)
192 (0xC0)	IPP6 (Internetwork Control)
224 (0xE0)	IPP7 (Network Control)

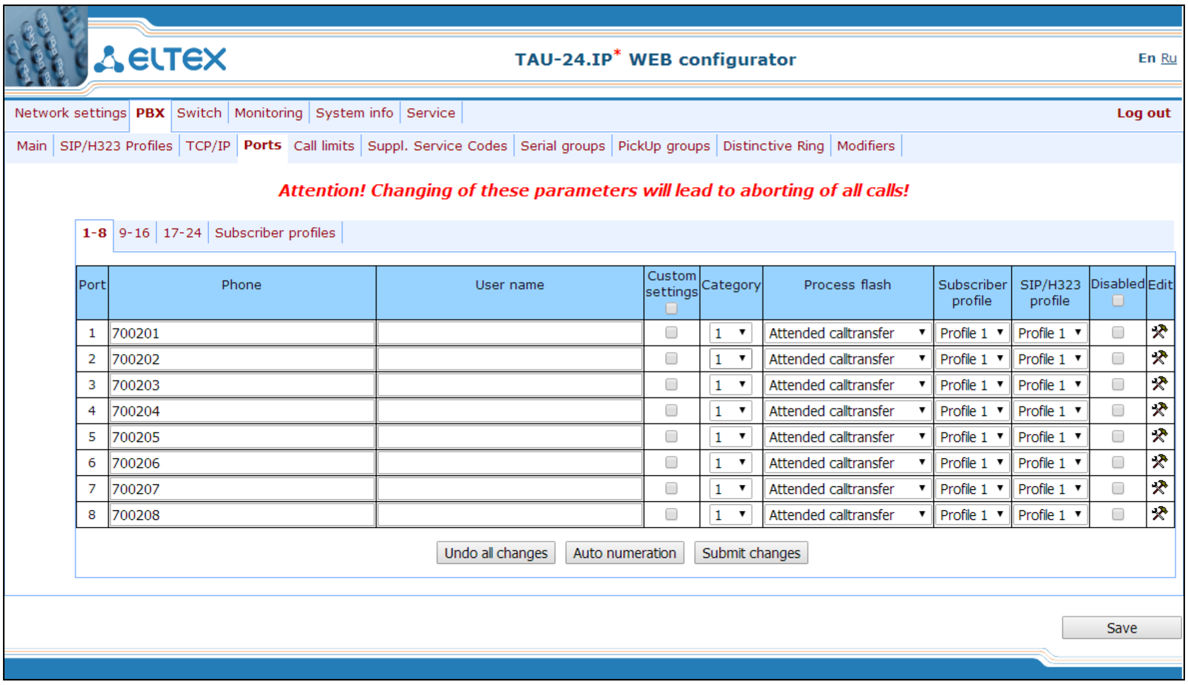
To discard all changes made to configuration, click *'Undo All Changes'* button. To set default parameters, click *'Defaults'* button (the figure below shows default values). To apply changes, click *'Submit Changes'* button.

5.1.2.4 PortsConfiguration of Subscriber Ports (Ports)

In *'Ports'* menu, 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.


ELTEX
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Main | SIP/H323 Profiles | TCP/IP | Ports | Call limits | Suppl. Service Codes | Serial groups | PickUp groups | Distinctive Ring | Modifiers

Attention! Changing of these parameters will lead to aborting of all calls!

1-8 | 9-16 | 17-24 | Subscriber profiles

Port	Phone	User name	Custom settings □	Category	Process flash	Subscriber profile	SIP/H323 profile	Disabled □	Edit
1	700201		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
2	700202		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
3	700203		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
4	700204		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
5	700205		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
6	700206		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
7	700207		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒
8	700208		□	1	Attended calltransfer	Profile 1	Profile 1	□	⚒

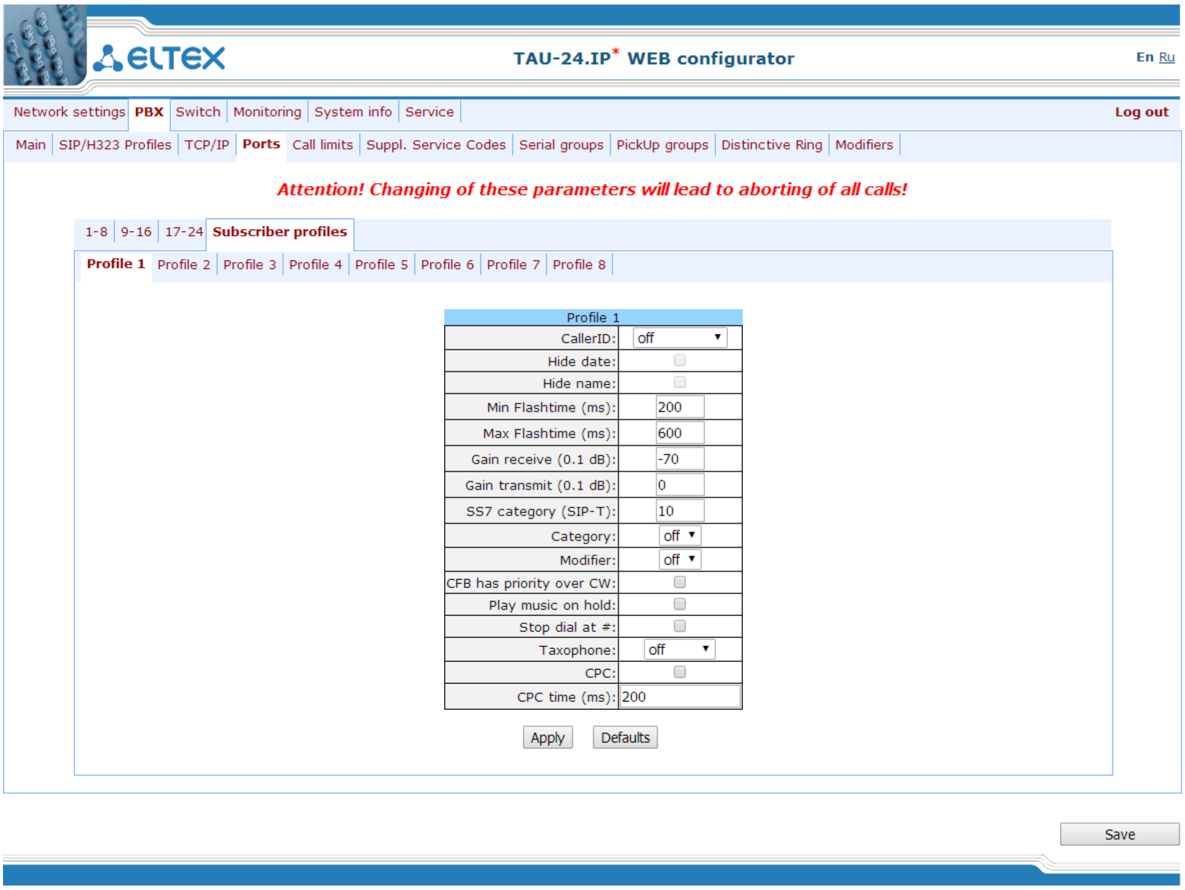
Configuration of ports

– *Port*—port number.

- *Phone*—subscriber's number.
- *User name*—subscriber's name.
- *Custom*—when checked, use common settings for this port (configured by clicking '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 '*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:*



Attention! Changing of these parameters will lead to aborting of all calls!

Profile 1	
CallerID:	off
Hide date:	□
Hide name:	□
Min Flashtime (ms):	200
Max Flashtime (ms):	600
Gain receive (0.1 dB):	-70
Gain transmit (0.1 dB):	0
SS7 category (SIP-T):	10
Category:	off
Modifier:	off
CFB has priority over CW:	□
Play music on hold:	□
Stop dial at #:	□
Taxophone:	off
CPC:	□
CPC time (ms):	200

- *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 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-32M.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 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 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'.

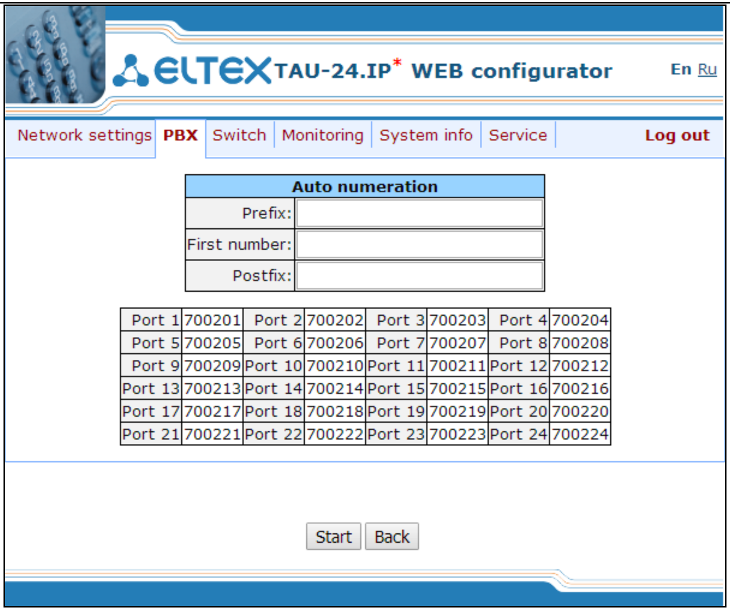
- *Modifier*—modifier table number, used for the current port.
- *CFB has priority over CW*—defines the priority between CFB (Forward on busy) and CW (Call wait) services. When checked, CFB service has a priority over CW, and vice versa.
- *Play music on hold*—use 'Play music on hold' service. When 'Hold' 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.

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

Automatic enumeration

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



Auto numeration	
Prefix:	
First number:	
Postfix:	

Port 1	700201	Port 2	700202	Port 3	700203	Port 4	700204
Port 5	700205	Port 6	700206	Port 7	700207	Port 8	700208
Port 9	700209	Port 10	700210	Port 11	700211	Port 12	700212
Port 13	700213	Port 14	700214	Port 15	700215	Port 16	700216
Port 17	700217	Port 18	700218	Port 19	700219	Port 20	700220
Port 21	700221	Port 22	700222	Port 23	700223	Port 24	700224

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.

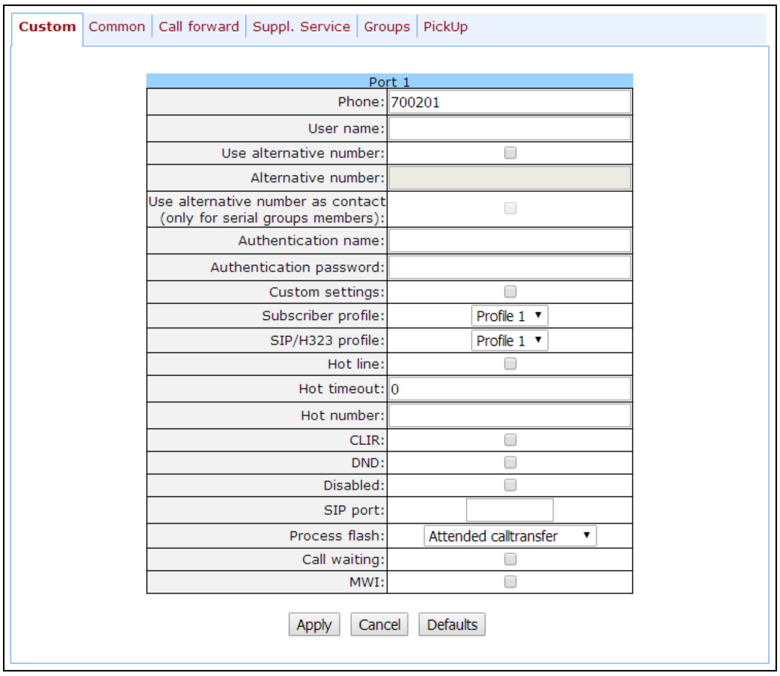
Prefix and postfix—constant parts, added in the beginning and in the end of a number.

To start enumeration, click *'Start'* button. To return to *'Ports'* menu, click *'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:



Port 1	
Phone:	700201
User name:	
Use alternative number:	☐
Alternative number:	
Use alternative number as contact (only for serial groups members):	☐
Authentication name:	
Authentication password:	
Custom settings:	☐
Subscriber profile:	Profile 1
SIP/H323 profile:	Profile 1
Hot line:	☐
Hot timeout:	0
Hot number:	
CLIR:	☐
DND:	☐
Disabled:	☐
SIP port:	
Process flash:	Attended calltransfer
Call waiting:	☐
MWI:	☐

- *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 settings*—when checked, use common settings for this port (configured by clicking '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.
- *Hot line*—when checked, '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*—when checked, calling line identification restriction service—CLIR—is enabled.
- *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 calltransfer*—'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 calltransfer*—'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.

For 'Calltransfer' service operation principles, see Section 7.1 Calltransfer.

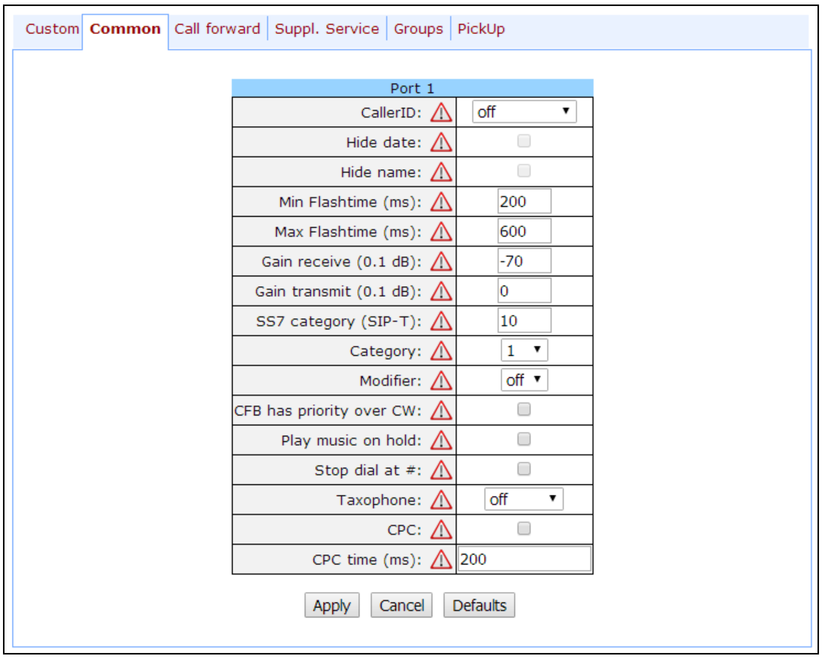
This setting will not work, if 'IMS mode'—'Enable IMS' parameter in SIP profile settings—is enabled on the device.

— *Call waiting*—when checked, 'Call waiting service' will be enabled (service is available in flash function operation mode—call transfer).

— *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.

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

'Common' tab—FXS type port common settings:



Port 1	
CallerID:	off ▾
Hide date:	☐
Hide name:	☐
Min Flashtime (ms):	200
Max Flashtime (ms):	600
Gain receive (0.1 dB):	-70
Gain transmit (0.1 dB):	0
SS7 category (SIP-T):	10
Category:	1 ▾
Modifier:	off ▾
CFB has priority over CW:	☐
Play music on hold:	☐
Stop dial at #:	☐
Taxophone:	off ▾
CPC:	☐
CPC time (ms):	200

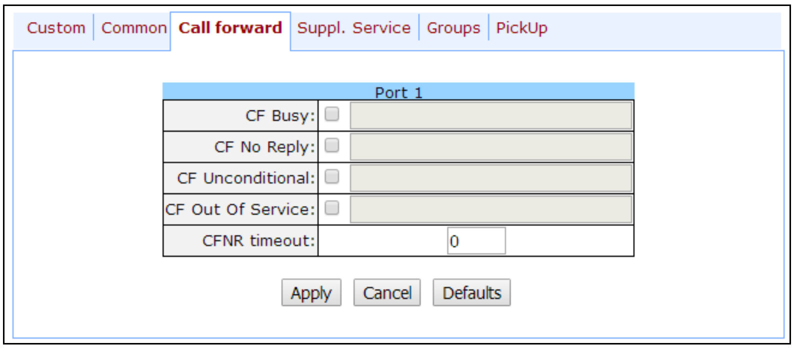
Description of fields is equivalent to *'PBX/Ports/Subscriber profiles'* tab fields shown above.

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:



Custom | Common | **Call forward** | Suppl. Service | Groups | PickUp

Port 1		
CF Busy:	□	
CF No Reply:	□	
CF Unconditional:	□	
CF Out Of Service:	□	
CFNR timeout:		0

Apply | Cancel | Defaults

- *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, OOS service is enabled—forward the call, when the subscriber is out of service.

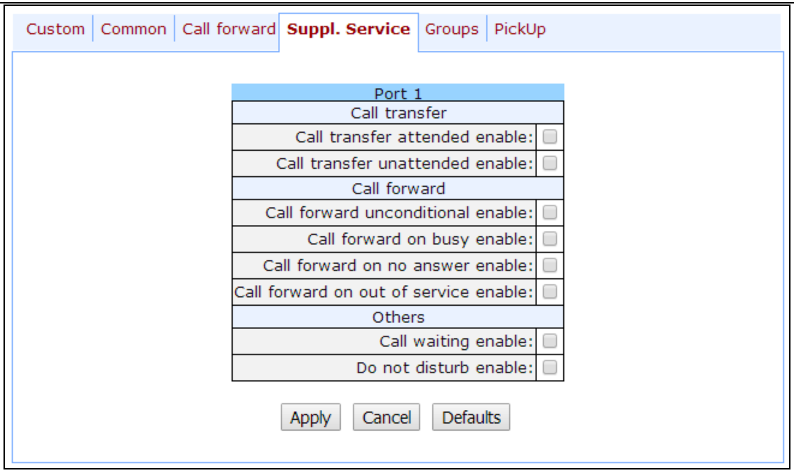
—

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.

Against each service, there is a number that the call will be forwarded to.

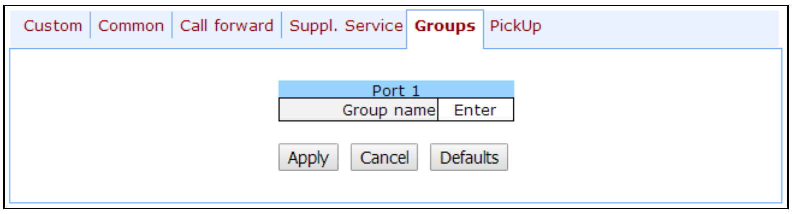
«Suppl. Service tab allows you to enable/disable supplementary services. For detailed description of supplementary service operations, see Section **5.1.2.6.**



Port 1	
Call transfer	
Call transfer attended enable:	□
Call transfer unattended enable:	□
Call forward	
Call forward unconditional enable:	□
Call forward on busy enable:	□
Call forward on no answer enable:	□
Call forward on out of service enable:	□
Others	
Call waiting enable:	□
Do not disturb enable:	□

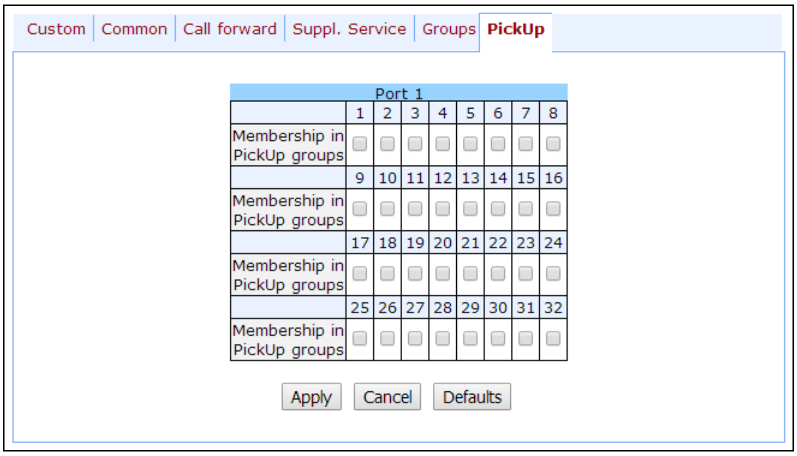
*'**Groups**' tab allows you to add/remove ports to/from serial groups. For detailed description of serial discovery group operations, see Section* **5.1.2.7.**

In ***'Groups'*** tab, you may see a 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:



Port 1	
Group name	Enter

'PickUp' tab — add/remove ports to/from the pickup groups. For detailed description of pickup group operations, see Section **5.1.2.8.**



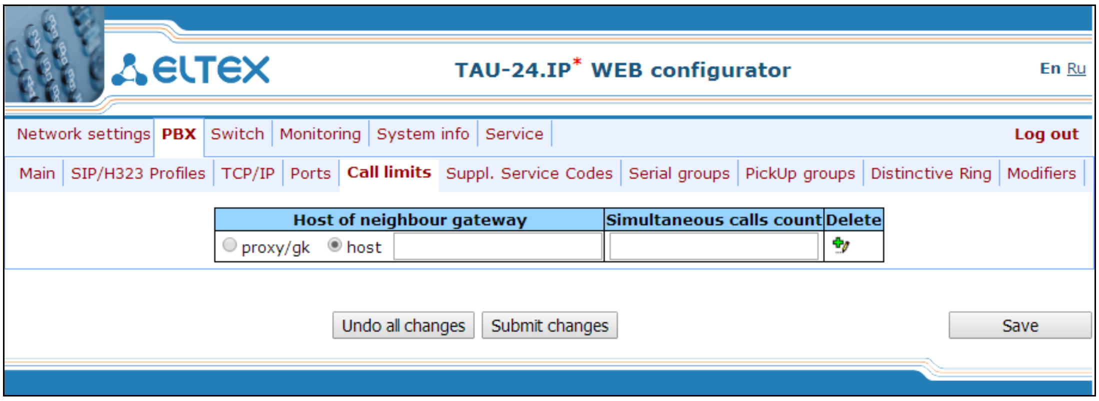
Port 1								
	1	2	3	4	5	6	7	8
Membership in PickUp groups	□	□	□	□	□	□	□	□
	9	10	11	12	13	14	15	16
Membership in PickUp groups	□	□	□	□	□	□	□	□
	17	18	19	20	21	22	23	24
Membership in PickUp groups	□	□	□	□	□	□	□	□
	25	26	27	28	29	30	31	32
Membership in PickUp groups	□	□	□	□	□	□	□	□

– 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 *'Apply'* button. To reset settings to default values, click *'Defaults'* button.

5.1.2.5 Simultaneous Call Limits (Call limits)

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



Host of neighbour gateway		Simultaneous calls count	Delete
○ proxy/gk ● 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 discard all changes made to configuration, click *'Undo All Changes'* button. To store changes to non-volatile memory of the device, click *'Save'* button.

5.1.2.6 Configuration of Supplementary Service Codes (Suppl. Service Codes)

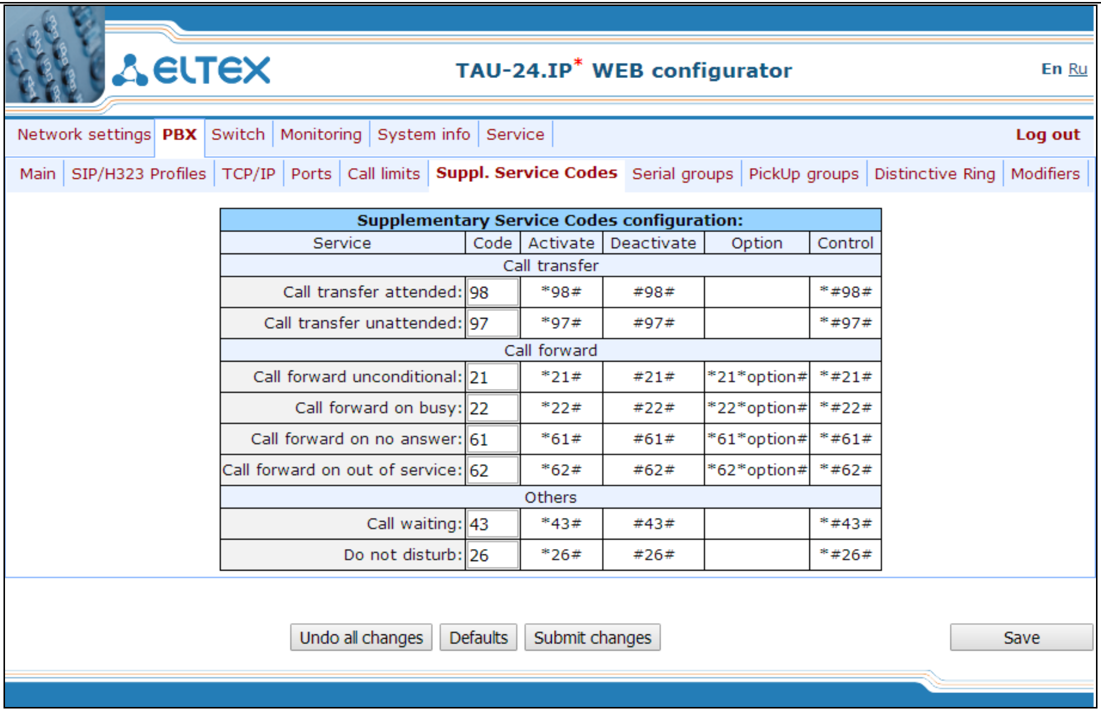
Supplementary services are provided to each subscriber, but in order to use a specific service, the subscriber must enable it first at the service provider. Service providers may create their own service plans containing several supplementary services. To do this, in **5.1.2.4** section, on ***Suppl. 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#

Supplementary Service Codes configuration:

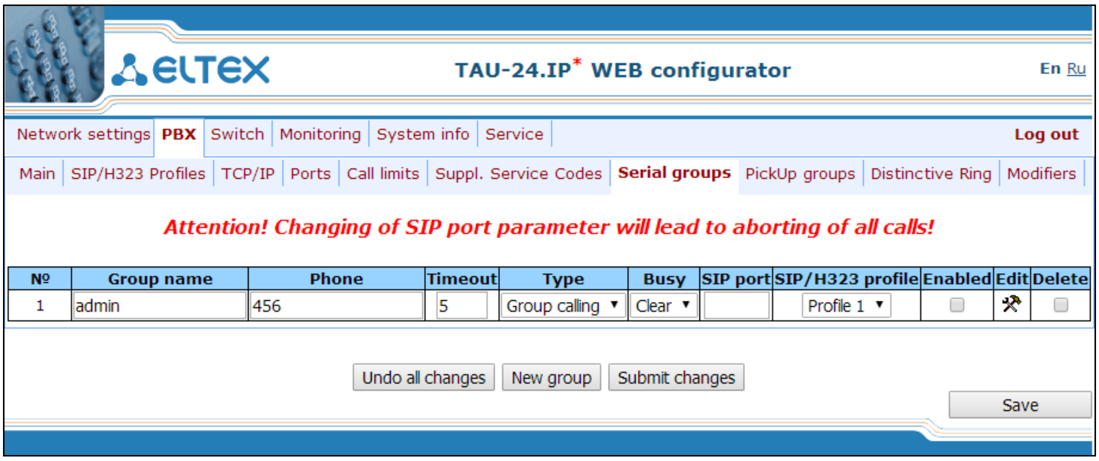
- *Service—type of supplementary service:*
  - *Call transfer attended*—'Call transfer' service with the wait for response of the subscriber, the call is being forwarded to.
  - *Call transfer unattended*—'Call transfer' service without the wait for response of the subscriber, the call is being forwarded 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.
- *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 *'Undo All Changes'* button. To set the default values, click *'Defaults'* button. To apply changes, click *'Submit Changes'* button. To store changes to non-volatile memory of the device, click *'Save'* button.

5.1.2.7 *Serial groups*

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

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!!!

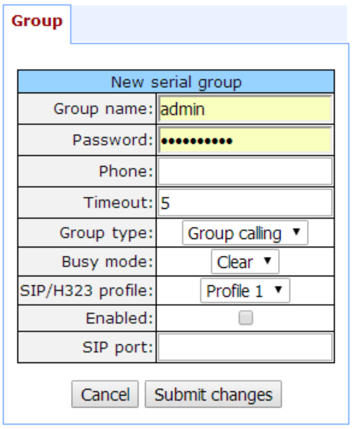


Attention! Changing of SIP port parameter will lead to aborting of all calls!

№	Group name	Phone	Timeout	Type	Busy	SIP port	SIP/H323 profile	Enabled	Edit	Delete
1	admin	456	5	Group calling ▾	Clear ▾		Profile 1 ▾	□	⚒	□

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, and so on. 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 *'New group'* button:



New serial group

Group name:	admin
Password:	••••••••••
Phone:	
Timeout:	5
Group type:	Group calling ▾
Busy mode:	Clear ▾
SIP/H323 profile:	Profile 1 ▾
Enabled:	□
SIP port:	

- *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.

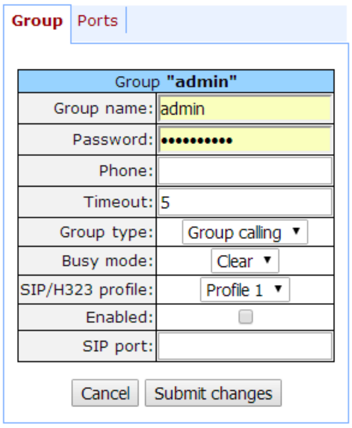
– *Enabled*—when checked, the call group is enabled.

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:



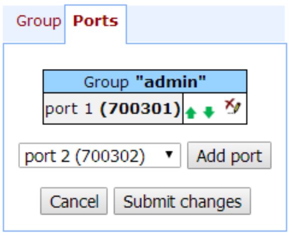
Group | Ports

Group "admin"	
Group name:	admin
Password:	••••••••••
Phone:	
Timeout:	5
Group type:	Group calling ▾
Busy mode:	Clear ▾
SIP/H323 profile:	Profile 1 ▾
Enabled:	□
SIP port:	

Cancel | Submit changes

For description of menu fields, see above.

'Ports'—group ports:



Group | Ports

Group "admin"	
port 1 (700301)	↑ ↓ ☒

port 2 (700302) ▾ | Add port

Cancel | Submit changes

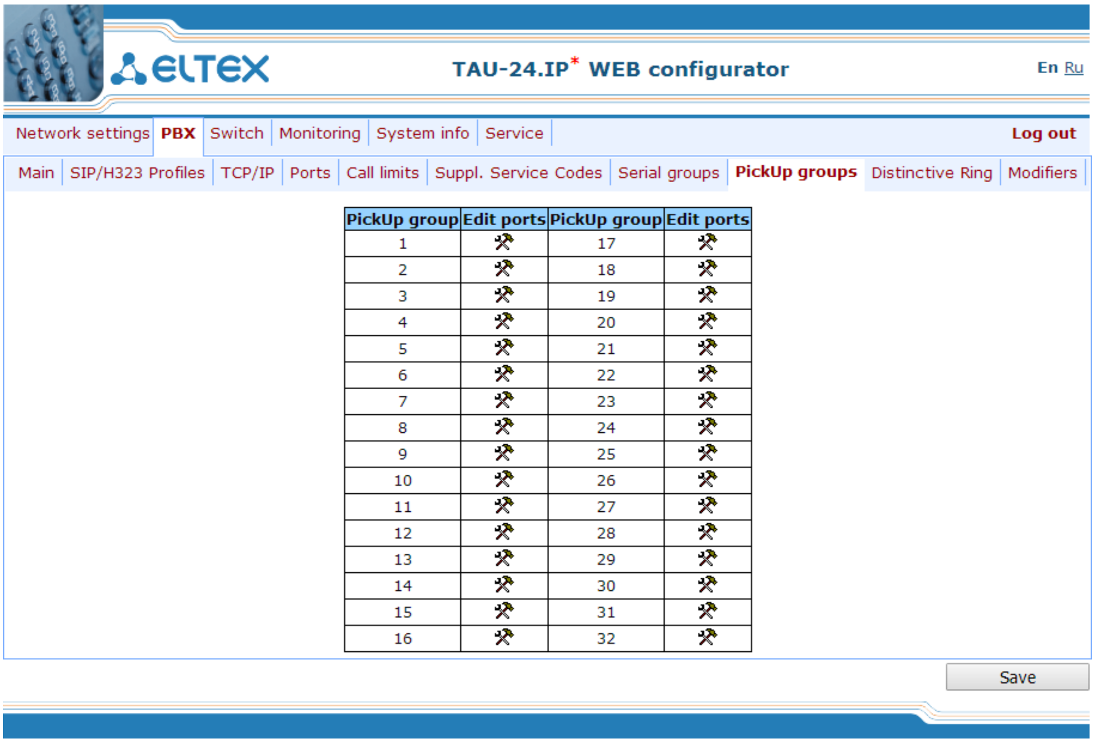
To add a port to a group, select the desired port from the drop-down list and click *'Add port'* button.

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 Pickup Group Configuration (Pickup Groups)

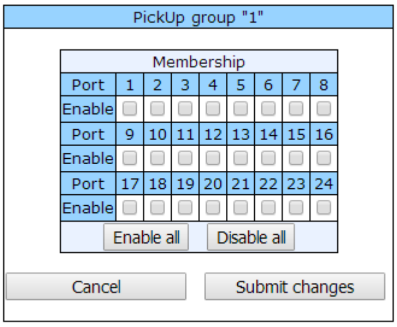
In *'PickUp groups'* submenu, you may configure pickup groups. You may configure up to 32 different pickup groups in total.

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.**



PickUp group	Edit ports	PickUp group	Edit ports
1	⚒	17	⚒
2	⚒	18	⚒
3	⚒	19	⚒
4	⚒	20	⚒
5	⚒	21	⚒
6	⚒	22	⚒
7	⚒	23	⚒
8	⚒	24	⚒
9	⚒	25	⚒
10	⚒	26	⚒
11	⚒	27	⚒
12	⚒	28	⚒
13	⚒	29	⚒
14	⚒	30	⚒
15	⚒	31	⚒
16	⚒	32	⚒

- *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:



Membership

Port	1	2	3	4	5	6	7	8
Enable	□	□	□	□	□	□	□	□
Port	9	10	11	12	13	14	15	16
Enable	□	□	□	□	□	□	□	□
Port	17	18	19	20	21	22	23	24
Enable	□	□	□	□	□	□	□	□

- *Port*—subscriber port number.
- *Enable*—when checked, the port belongs to the pickup group; otherwise, it does not belong to this group.

When *'Enable'* checkbox is selected against the subscriber port, this port is included into the pickup group; otherwise, it is excluded from this group. To set permissions for all subscriber ports, click *'Enable all'* button. To deselect checkboxes for all subscriber ports, click *'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 'Cancel' button. To save changes, click *'Submit Changes'* button. To store changes to non-volatile memory of the device, click *'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.

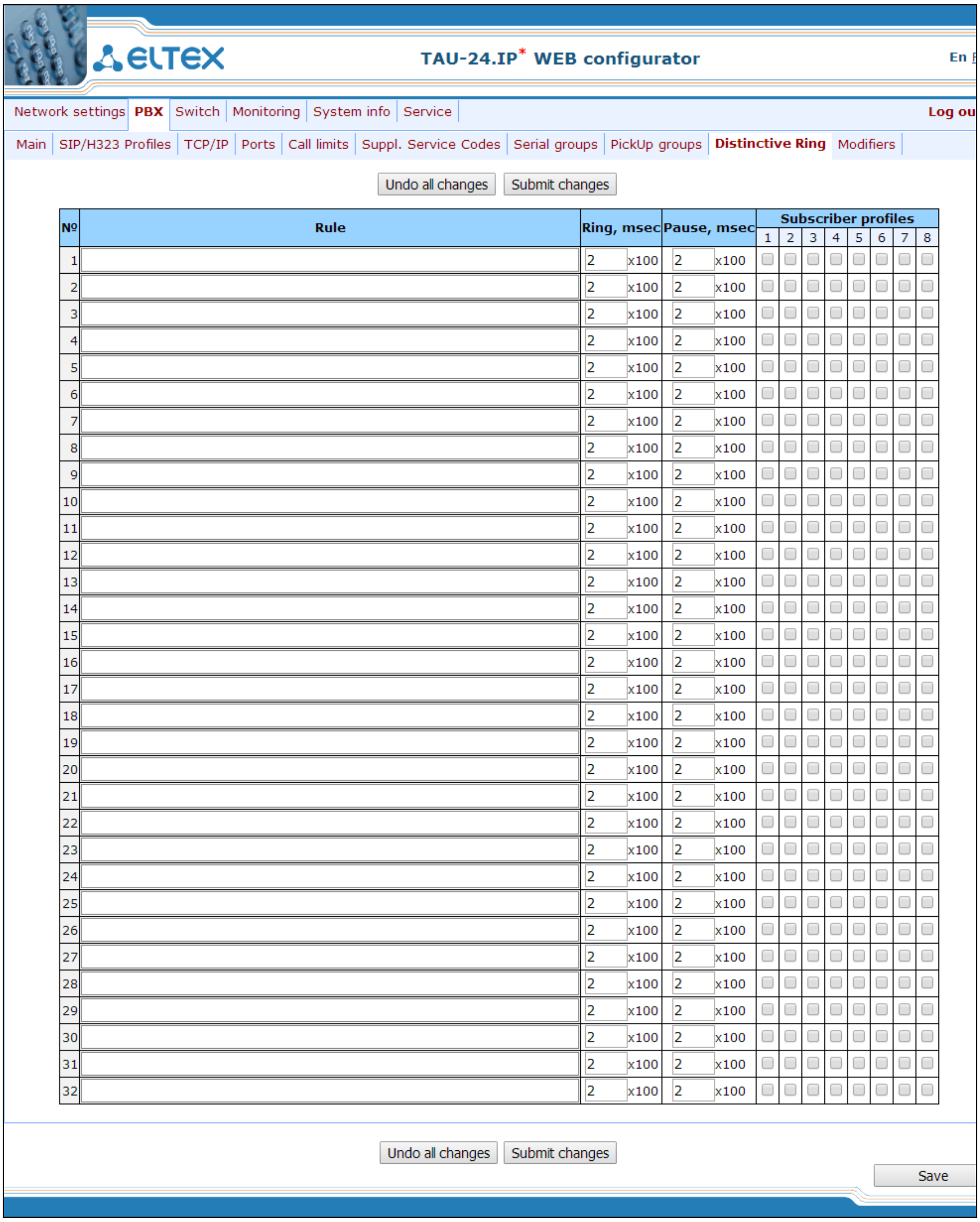
Pickup group may be used in combination with a call group; in this case, all ports that belong to a call group should belong to the pickup group as well. Thus, each port that belong to a call group will be able to pickup an incoming call to a group number.

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 tunnelling.)

5.1.2.9 'Distinctive Ring' Service Configuration

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		2 x100	2 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		2 x100	2 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.}.

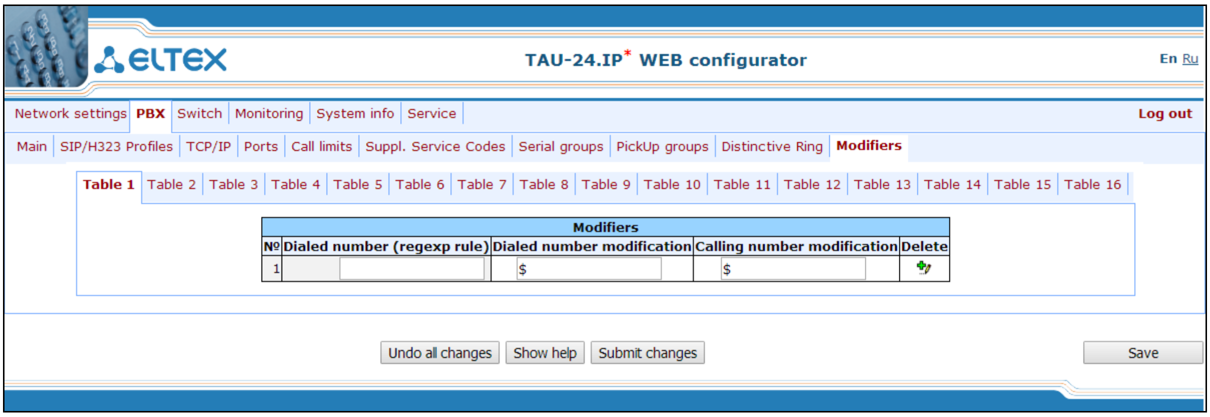
  Example:
  5{2,5}—caller's number may be equal to 55, 555, 5555, or 55555.
- **.** – 'dot' special symbol means that a preceding digit, range, or '*', '#' characters may be repeated from one to infinity times. Equivalent to a record {0,}.

  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 *Modifiers*

This setting allows for the modification of the associated and dialled numbers depending on the call direction. Modifiers are used in outgoing calls.

Modifiers work only when routing rules are used, described with regular expressions (5.1.2.2.5.4); at that, in number modification routing rules, <:> characters should not be used.



Modifiers

№	Dialed number (regexp rule)	Dialed number modification	Calling number modification	Delete
1		$	$	

The gateway allows you to configure 16 modifier groups, each group contains one or several modification rules:

- *Dialed number (regexp rule)*—dialled number mask.
- *Dialed number modification*—dialled number modification rule.
- *Calling number modification*—modification rule for TAU subscriber's number (caller's number).

Dialled 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}—dialled 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.
  Dialled 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$

5.1.3 *Switch*

In *'Switch'* menu, you may configure switch ports.

5.1.3.1 Switch ports settings

In *'Switch ports settings'* submenu, you may configure parameters of integrated Ethernet switch ports.

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 records.

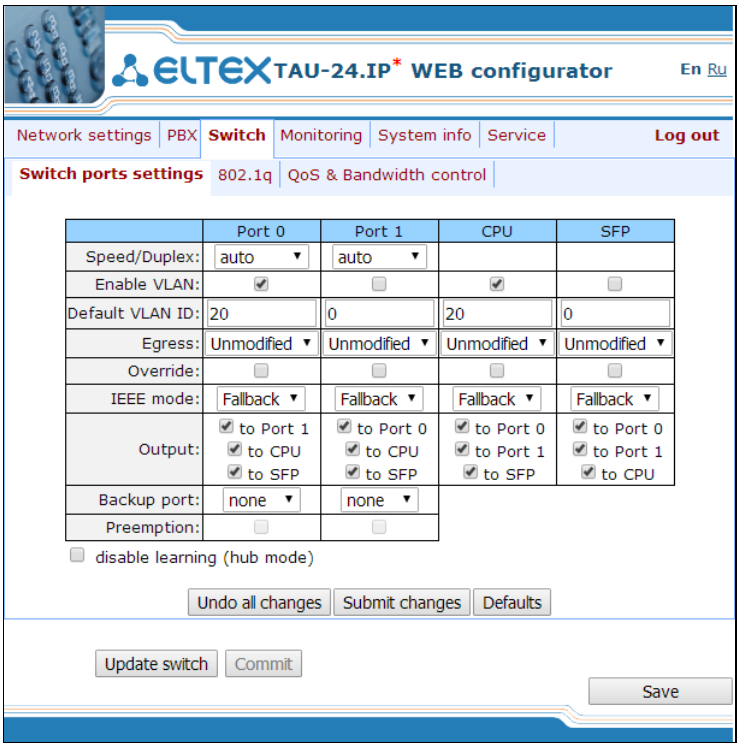
2. ***Port based VLAN***—to use this mode, *'IEEE Mode'* value should be set to *'Fallback'* for all ports, mutual availability of data ports should be set to *'Output'* with the respective checkboxes. For VLAN operation, use *'Enable VLAN', 'Default VLAN ID', 'Egress',* and *'Override'* settings. '802.1q'

routing table in '*802.1q*' tab should not contain any records.

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'* settings. 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'* settings. 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**.**



	Port 0	Port 1	CPU	SFP
Speed/Duplex:	auto	auto		
Enable VLAN:	☑	□	☑	□
Default VLAN ID:	20	0	20	0
Egress:	Unmodified	Unmodified	Unmodified	Unmodified
Override:	□	□	□	□
IEEE mode:	Fallback	Fallback	Fallback	Fallback
Output:	☑ to Port 1 ☑ to CPU ☑ to SFP	☑ to Port 0 ☑ to CPU ☑ to SFP	☑ to Port 0 ☑ to Port 1 ☑ to SFP	☑ to Port 0 ☑ to Port 1 ☑ to CPU
Backup port:	none	none		
Preemption:	□	□		

□ disable learning (hub mode)

Gateway switch is equipped with 3 x electrical Ethernet ports and 1 x port for CPU interactions:

— *port0, port1*—electrical Ethernet ports of the device.

— *CPU*—internal port linked to the device CPU.

— *SFP0*—optical (SFP) Ethernet ports of the device.

Switch settings:

- *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'* row. 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 rejected. 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.
- *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 switch when switch settings are applied. Click* '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 *'Defaults'* button to set default parameters (the figure below shows default values).

5.1.3.2 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.

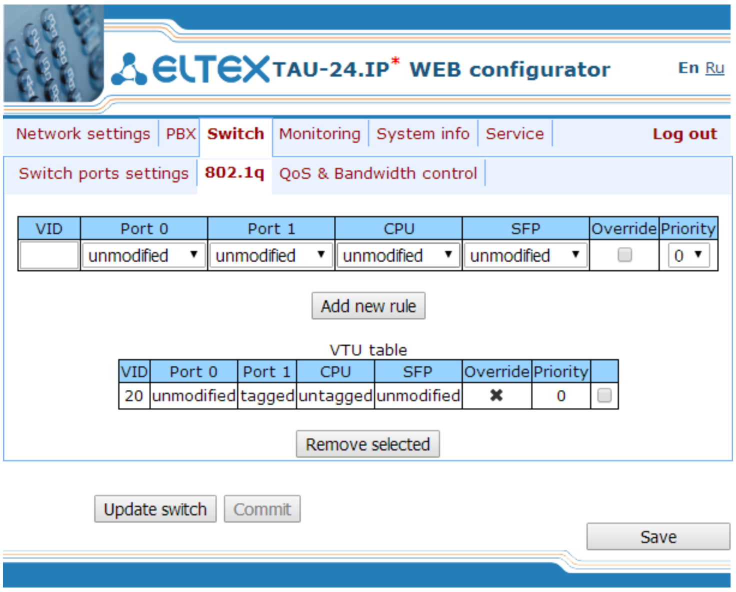
2 Connect a PC to perform the tracing directly to TAU Ethernet port.

3 Run the application on the PC that captures network traffic. In the application, select Ethernet interface connected to TAU as a traffic capture interface.

4 After tracing, save captured traffic into a file.

5.1.3.3 802.1q

In '802.1q' submenu, you may define the configuration of packet routing rules for switch operation in 802.1q mode.



VID	Port 0	Port 1	CPU	SFP	Override	Priority
	unmodified	unmodified	unmodified	unmodified	□	0

VTU table

VID	Port 0	Port 1	CPU	SFP	Override	Priority	
20	unmodified	tagged	untagged	unmodified	✖	0	□

Gateway switch is equipped with 3 x electrical Ethernet ports and 1 x port for CPU interactions:

- *port0, port1*—electrical Ethernet ports of the device.
- *CPU*—internal port linked to the device CPU.
- *SFP0*—optical (SFP) Ethernet ports of the device TAU-24.IP/TAU-16.IP.

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.

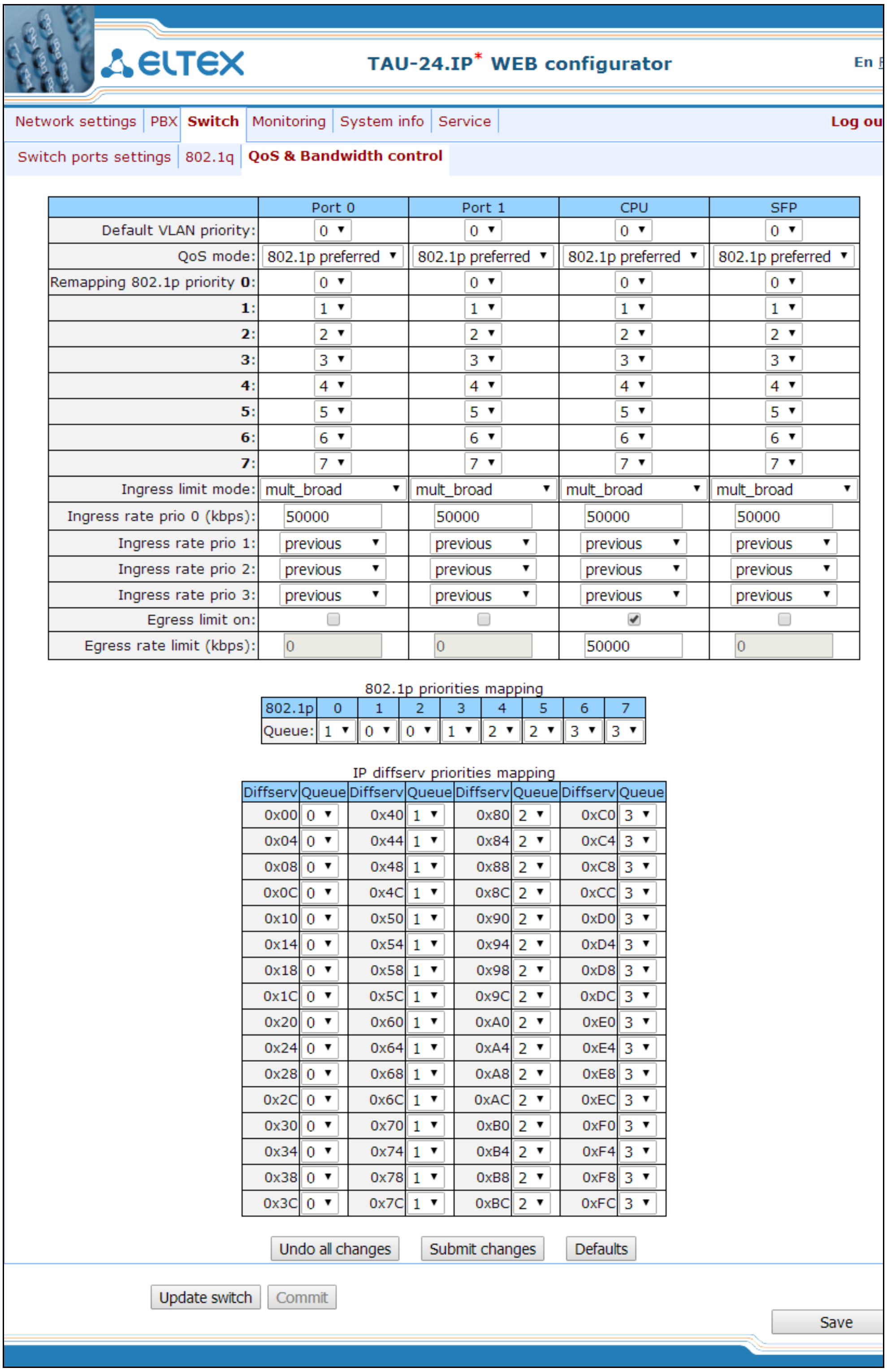
- *unmodified*—packets will be sent by the port without any changes (i.e. as they have been received).
- *untagged*—packets will always be sent without VLAN tag by this port.
- tagged—packets will always be sent with VLAN tag by this port.
- *not member*—packets with specified VID will not be sent by 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 *'Add New Rule'* button.
To remove records, select checkboxes for the rows to be removed and click *'Remove selected'* button.

✓ **'Update Switch'** *and* **'Commit'** *buttons allow to retain access to the switch when switch settings are applied.* ***Click*** **'Commit'** ***button in 30 seconds interval to confirm newly applied settings, or the previous settings will be restored.***

5.1.3.4 QoS & Bandwidth control

In *'QoS & Bandwidth control'* submenu, you may configure Quality of Service functions and bandwidth restrictions.



	Port 0	Port 1	CPU	SFP
Default VLAN priority:	0	0	0	0
QoS mode:	802.1p preferred	802.1p preferred	802.1p preferred	802.1p preferred
Remapping 802.1p priority **0**:	0	0	0	0
1:	1	1	1	1
2:	2	2	2	2
3:	3	3	3	3
4:	4	4	4	4
5:	5	5	5	5
6:	6	6	6	6
7:	7	7	7	7
Ingress limit mode:	mult_broad	mult_broad	mult_broad	mult_broad
Ingress rate prio 0 (kbps):	50000	50000	50000	50000
Ingress rate prio 1:	previous	previous	previous	previous
Ingress rate prio 2:	previous	previous	previous	previous
Ingress rate prio 3:	previous	previous	previous	previous
Egress limit on:	□	□	☑	□
Egress rate limit (kbps):	0	0	50000	0

802.1p priorities mapping

802.1p	0	1	2	3	4	5	6	7
Queue:	1	0	0	1	2	2	3	3

IP diffserv priorities mapping

Diffserv	Queue	Diffserv	Queue	Diffserv	Queue	Diffserv	Queue
0x00	0	0x40	1	0x80	2	0xC0	3
0x04	0	0x44	1	0x84	2	0xC4	3
0x08	0	0x48	1	0x88	2	0xC8	3
0x0C	0	0x4C	1	0x8C	2	0xCC	3
0x10	0	0x50	1	0x90	2	0xD0	3
0x14	0	0x54	1	0x94	2	0xD4	3
0x18	0	0x58	1	0x98	2	0xD8	3
0x1C	0	0x5C	1	0x9C	2	0xDC	3
0x20	0	0x60	1	0xA0	2	0xE0	3
0x24	0	0x64	1	0xA4	2	0xE4	3
0x28	0	0x68	1	0xA8	2	0xE8	3
0x2C	0	0x6C	1	0xAC	2	0xEC	3
0x30	0	0x70	1	0xB0	2	0xF0	3
0x34	0	0x74	1	0xB4	2	0xF4	3
0x38	0	0x78	1	0xB8	2	0xF8	3
0x3C	0	0x7C	1	0xBC	2	0xFC	3

– *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.

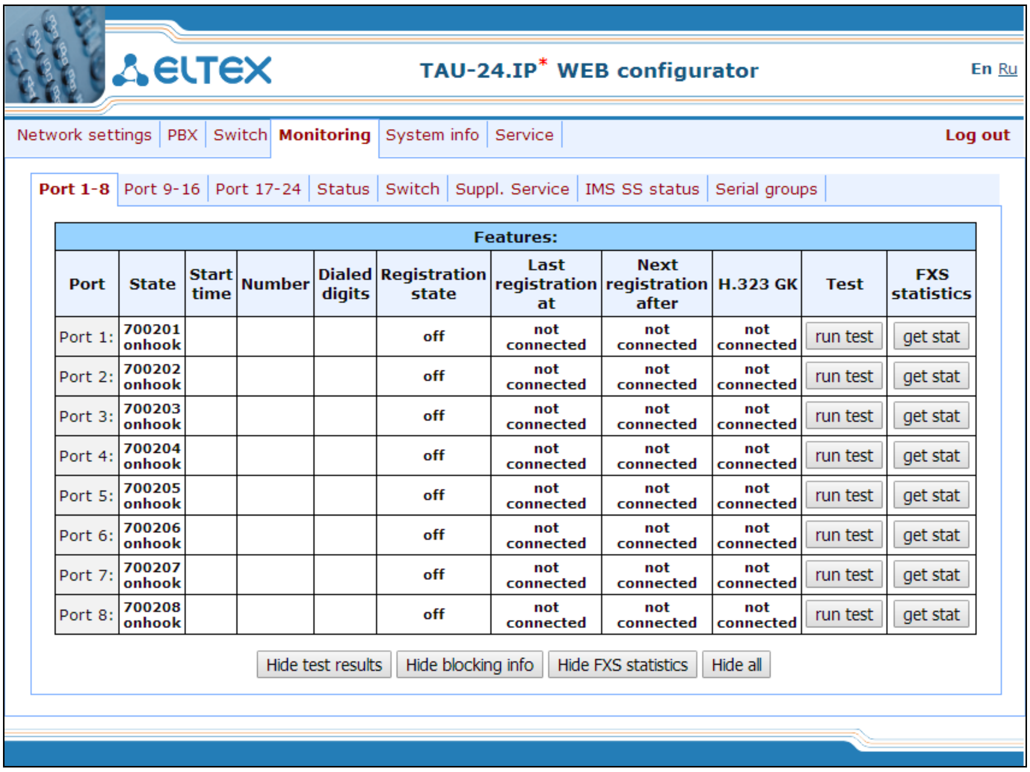
Queue 3 has the highest priority, queue 0—the lowest priority. Weighted packet distribution to outgoing queues 3/2/1/0 is as follows: 8/4/2/1.

5.1.4 *Monitoring*

In *'Monitoring'* menu, you may monitor the device status.

5.1.4.1 Subscriber Port Monitoring (Port)

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:	700201 onhook				off	not connected	not connected	not connected	run test	get stat
Port 2:	700202 onhook				off	not connected	not connected	not connected	run test	get stat
Port 3:	700203 onhook				off	not connected	not connected	not connected	run test	get stat
Port 4:	700204 onhook				off	not connected	not connected	not connected	run test	get stat
Port 5:	700205 onhook				off	not connected	not connected	not connected	run test	get stat
Port 6:	700206 onhook				off	not connected	not connected	not connected	run test	get stat
Port 7:	700207 onhook				off	not connected	not connected	not connected	run test	get stat
Port 8:	700208 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:
  - onhook—phone is onhook.
  - offhook—phone is offhook.
  - dial—dialling number.
  - ringback—sending 'ringback' tone.
  - ringing—sending '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 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):

- *leakadge 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.

’Hide blocking info’ deletes the results of tests of all types.

‘Hide all’ button removed the results of tests of all types.

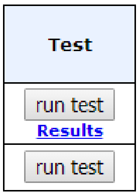
If the port is already in *'blocked'* state, and the *'Last block cause'* link is inactive, it means that the port was blocked when the phone is offhook. This blocking will be performed after the 'busy' tone is played to the subscriber's phone for two minutes. Upon the expiry of two-minute interval, 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 *'Save'* button.

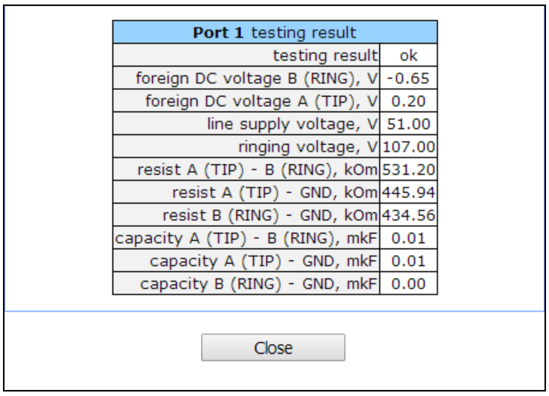
When you click on ‘Hide blocking info’ button information on blocking will be removed.

When you click ‘Hide all’ button are removed the results of tests of all types.

Port test



'Run test' button, located against each port, allow s 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 1 testing result	
testing result	ok
foreign DC voltage B (RING), V	-0.65
foreign DC voltage A (TIP), V	0.20
line supply voltage, V	51.00
ringing voltage, V	107.00
resist A (TIP) - B (RING), kOm	531.20
resist A (TIP) - GND, kOm	445.94
resist B (RING) - GND, kOm	434.56
capacity A (TIP) - B (RING), mkF	0.01
capacity A (TIP) - GND, mkF	0.01
capacity B (RING) - GND, mkF	0.00

Description of '*Port test results*' informational window:

- *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.

Do not launch the test for multiple ports simultaneously. Port test cannot be interrupted!

Test results description:

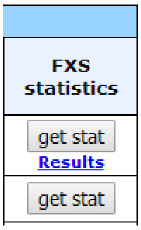
- *OK*—line test has been completed successfully.
- *TEST FAILURE*—invalid operand values were calculated during measurement. For example, division by zero has occurred. This error may appear in line resistance and capacity measurements upon the expiry of capacity measurement timeout.
- *STATE FAILURE*—occurs 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.

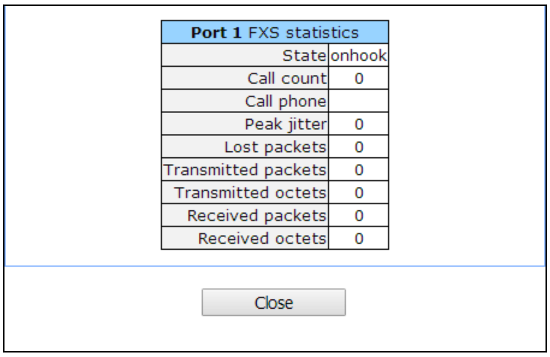
Click *'Hide test result'* button to remove test result information.

When you click *'Hide all'* button, all results for conducted tests of all types will be deleted.

Performed Call Statistics



'Get stat' button located against each port allows to get the statistics on performed calls for the specific port. To see the statistics, hover the mouse cursor over the *'result'* link located against the respective port, or open the test results window by clicking the link:



Port 1 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

Description of 'Port FXS statistics' informational window:

- *State*—current port status:
  - *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.
  - *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.

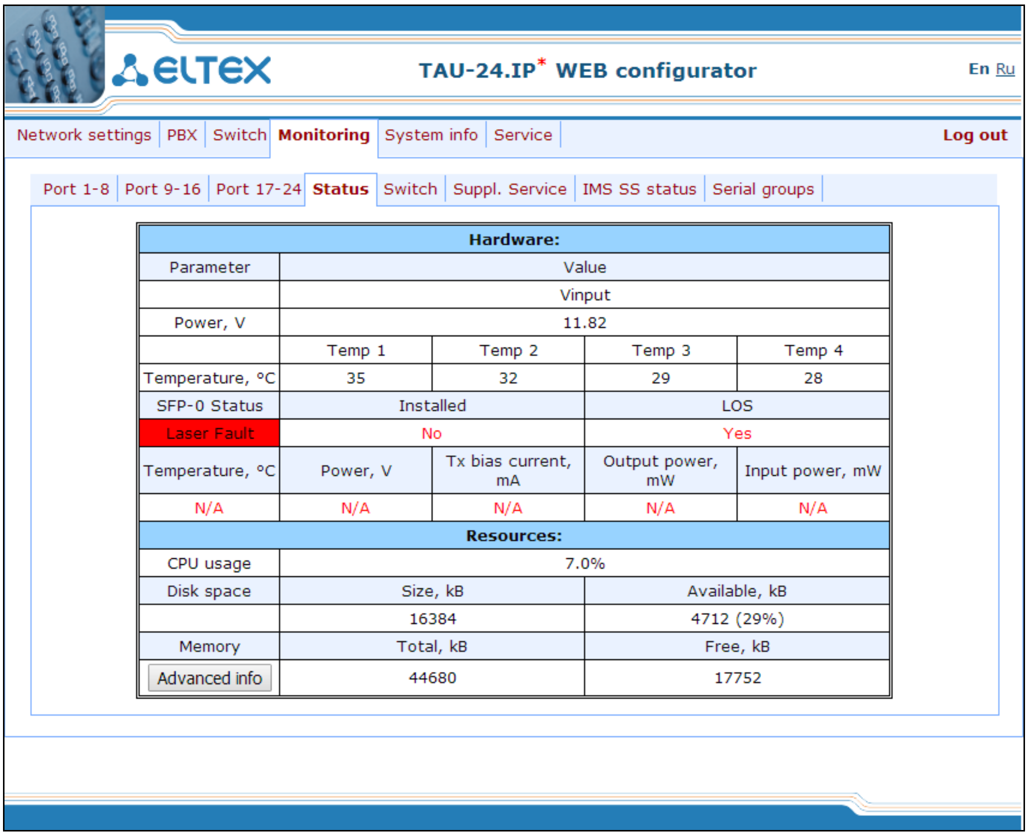
'Hide test results', 'Hide blocking info, 'Hide FXS/FXO statistics', 'Hide all' buttons allow to hide line test data, blocking data, FXS/FXO statistics, and all listed data respectively.

When you click *'Hide FXS statistics'* button, generated statistics on performed calls on this port will be deleted.

When you click *'Hide all'* button, all results for conducted tests of all types will be deleted.

5.1.4.2 Board Parameter Status Monitoring (Status)

In *'Status'* submenu, you can monitor physical parameters of the board and SFP modules supporting DDM (digital diagnostics monitoring) function.



Hardware:				
Parameter	Value			
	Vinput			
Power, V	11.82			
	Temp 1	Temp 2	Temp 3	Temp 4
Temperature, °C	35	32	29	28
SFP-0 Status	Installed		LOS	
Laser Fault	No		Yes	
Temperature, °C	Power, V	Tx bias current, mA	Output power, mW	Input power, mW
N/A	N/A	N/A	N/A	N/A
Resources:				
CPU usage	7.0%			
Disk space	Size, kB		Available, kB	
	16384		4712 (29%)	
Memory	Total, kB		Free, kB	
Advanced info	44680		17752	

Table ***'Hardware'—platform sensor parameters****:*

'Parameter'—controlled parameters and *'Value'*—controlled parameters' values:

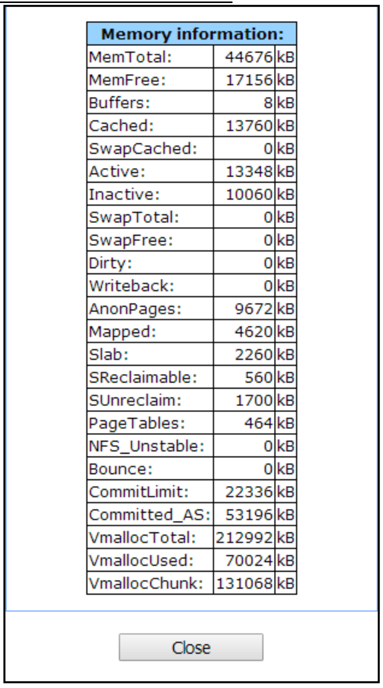
– *Power, V* - voltage generated by inductor 2 V. The device comprises a source of magneto ringing: working with sets of 1-24.

– *Temperature, °C*—temperature measured by sensors (each submodule has its own temperature sensor).

Fans will turn on automatically when the temperature exceeds 55°C, and turned off when the temperature falls below 45°C.

- *SFP-0 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.
- *Resources*—monitoring of system resources:
  - *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 *'Advanced info'* button to open the window with advanced information on RAM utilization.



Memory information:		
MemTotal:	44676	kB
MemFree:	17156	kB
Buffers:	8	kB
Cached:	13760	kB
SwapCached:	0	kB
Active:	13348	kB
Inactive:	10060	kB
SwapTotal:	0	kB
SwapFree:	0	kB
Dirty:	0	kB
Writeback:	0	kB
AnonPages:	9672	kB
Mapped:	4620	kB
Slab:	2260	kB
SReclaimable:	560	kB
SUnreclaim:	1700	kB
PageTables:	464	kB
NFS_Unstable:	0	kB
Bounce:	0	kB
CommitLimit:	22336	kB
Committed_AS:	53196	kB
VmallocTotal:	212992	kB
VmallocUsed:	70024	kB
VmallocChunk:	131068	kB

Permitted parameter values:

- Board power supply voltage should fall within the limits: 38V<Vbat<72V.
- Ringing voltage shall be within: 100V <Ring1 <120V and 100V <Vring2 <120V.
- 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.

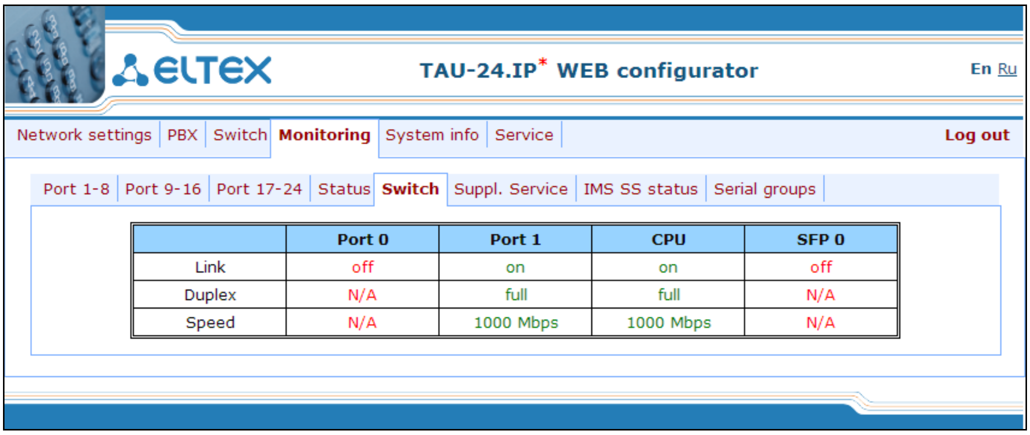
Description of Resources informational window (system resource monitoring):

- *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*—RAM.
  - *Total*—total amount of RAM in kbytes.
  - *Free*—free amount of RAM in kbytes.

5.1.4.3 Switch Port Status Monitoring (*Switch)*

In *'Switch'* menu, you may view status of integrated Ethernet switch ports.

The switch is equipped with 2 x Gigabit Ethernet electrical ports (Port 0, Port 1), 1 x optical ports (SFP 0), designed for connection to data networks and additional Ethernet devices, and 1 x internal CPU port for connection to TAU HOST processor.



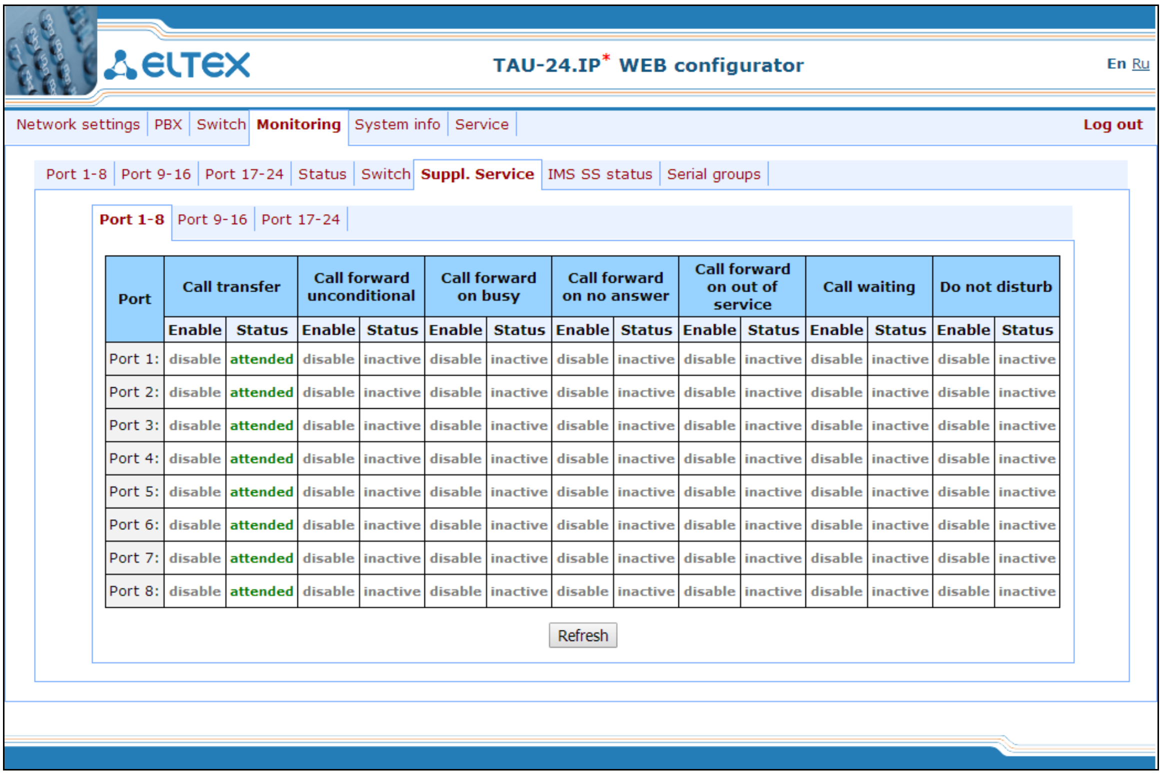
	Port 0	Port 1	CPU	SFP 0
Link	off	on	on	off
Duplex	N/A	full	full	N/A
Speed	N/A	1000 Mbps	1000 Mbps	N/A

Description of informational window:

- *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:
  - N/A—value is not available, as the link is inactive.
  - 10 Mb, 100 Mb, 1000 Mb.

5.1.4.4 Supplementary Service Status Monitoring (Suppl.Service)

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	
	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
Port 2:	disable	attended	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
Port 4:	disable	attended	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
Port 6:	disable	attended	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
Port 8:	disable	attended	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive	disable	inactive

Description of informational window:

- *Port*—subscriber port number.
- *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 with the wait for response of the subscriber, the call is being forwarded to.
- *Unattended*—'Call transfer' service is enabled, without the wait for response of the subscriber, the call is being forwarded to.
- *Off*—'Call transfer' service is disabled.

Status for other services:

- *Active*—active.
- *Inactive*—inactive.

For *'Call forward'* service, define the number configured for the call forwarding in the status field.

Services:

- *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.

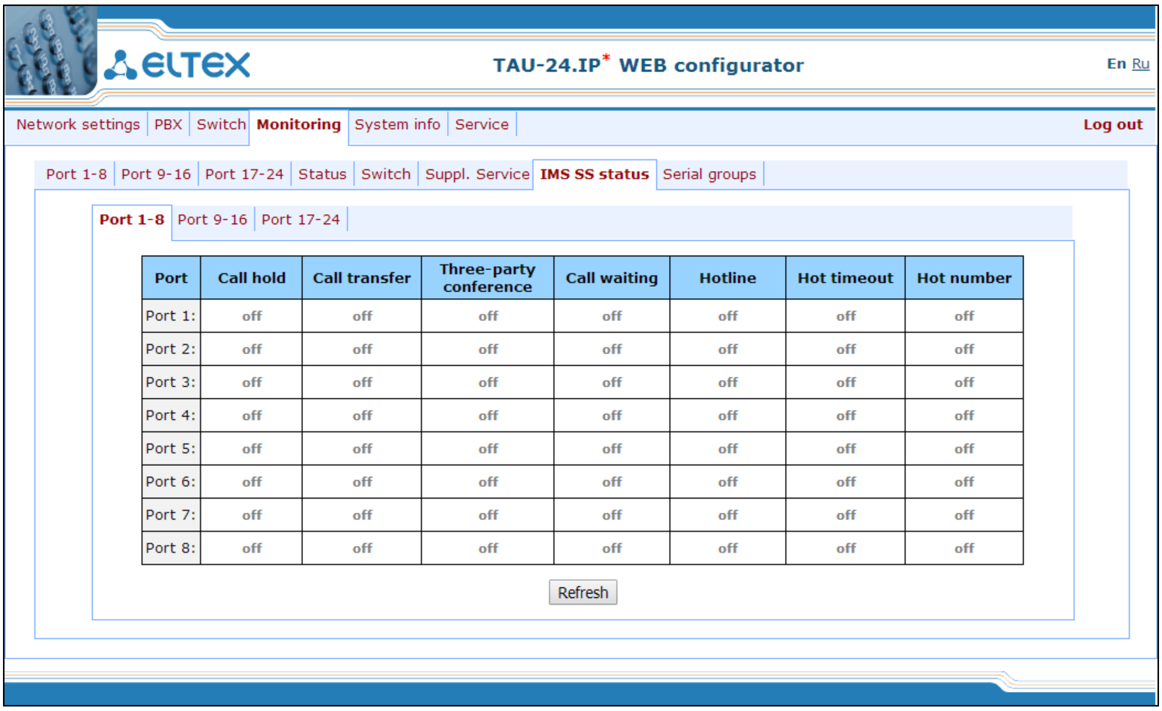
— *Call waiting*—'Call waiting' service.

— *Do not disturb*—'Do not disturb' service.

Use *'Refresh'* button to refresh table data.

5.1.4.5 IMS SS status Monitoring

In *'IMS SS status'* menu, you may view the current state of services managed by the Softswitch with IMS support.


ELTEX
TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Port 1-8 | Port 9-16 | Port 17-24 | Status | Switch | Suppl. Service | IMS SS status | Serial groups
Port 1-8 | Port 9-16 | Port 17-24
Refresh

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*—subscriber port number.

Services:

— *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.

Service statuses:

— *Off*—IMS management is disabled.

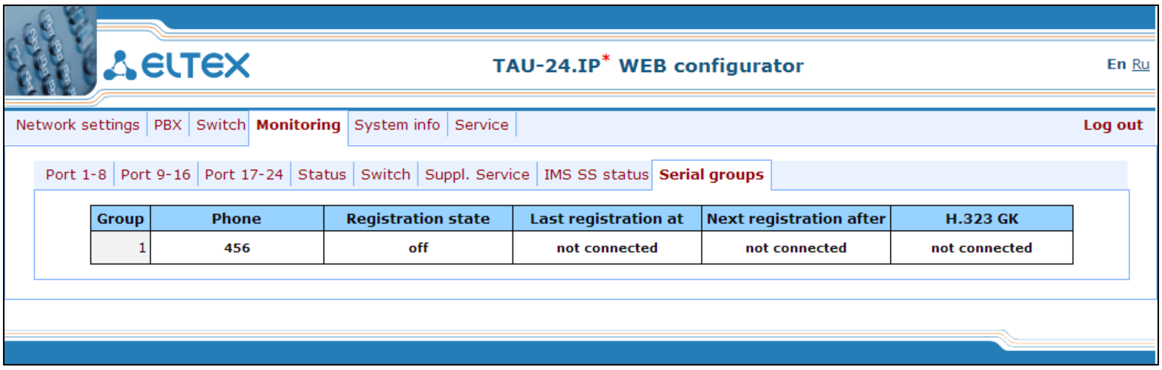
— *Disable*—service is disabled.

- *Enable*—service is enabled.

Use *'Refresh'* button to refresh table data.

5.1.4.6 Serial Group Registration Status Monitoring

In *'Serial groups'* menu, you may view the current state of serial group registration.


TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service
Log out
Port 1-8 | Port 9-16 | Port 17-24 | Status | Switch | Suppl. Service | IMS SS status | Serial groups

Group	Phone	Registration state	Last registration at	Next registration after	H.323 GK
1	456	off	not connected	not connected	not connected

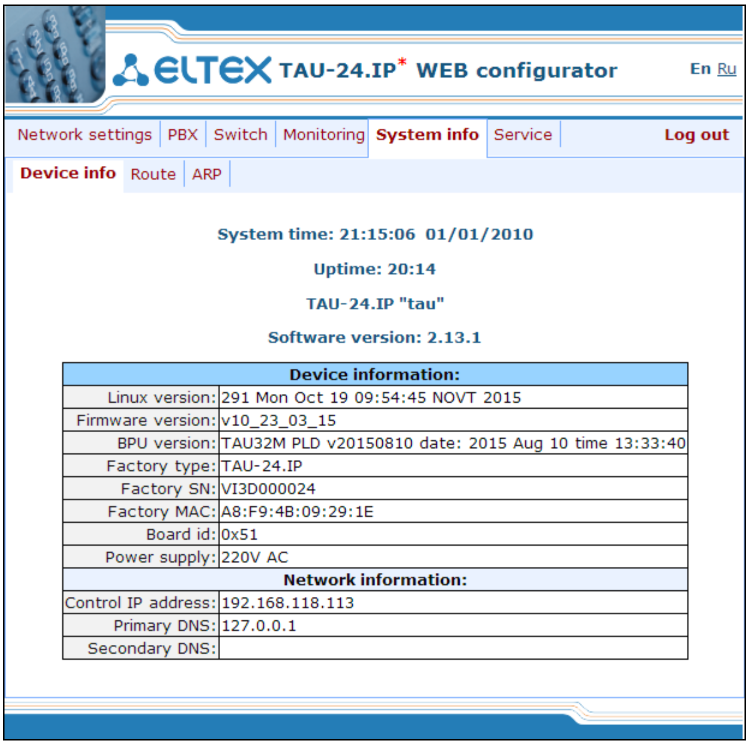
Description of informational window:

- *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 System Information *(System info)*

5.1.5.1 Service Status Monitoring (Device info)

In *'System info'* menu, you can view the system information.



System time: 21:15:06 01/01/2010

Uptime: 20:14

TAU-24.IP "tau"

Software version: 2.13.1

Device information:	
Linux version:	291 Mon Oct 19 09:54:45 NOVT 2015
Firmware version:	v10_23_03_15
BPU version:	TAU32M PLD v20150810 date: 2015 Aug 10 time 13:33:40
Factory type:	TAU-24.IP
Factory SN:	VI3D000024
Factory MAC:	A8:F9:4B:09:29:1E
Board id:	0x51
Power supply:	220V AC
Network information:	
Control IP address:	192.168.118.113
Primary DNS:	127.0.0.1
Secondary DNS:	

Description of informational window:

- *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-24.IP/TAU-16.IP —firmware version.
- *Software Version*—device firmware version.

Device information

- *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).

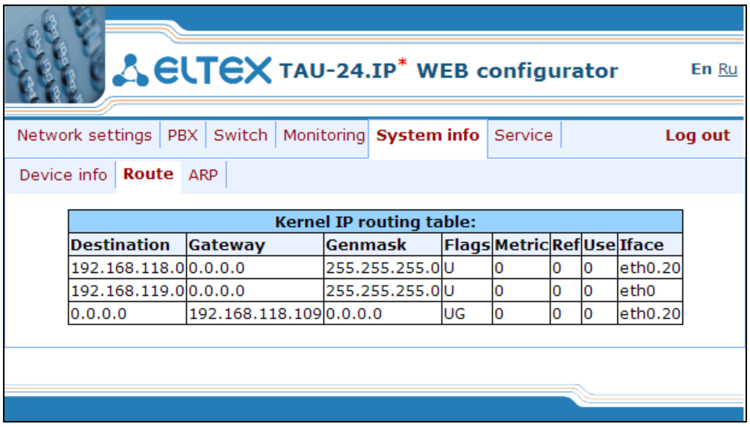
Network information

- *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 *Route*

In *'Route'* menu, you can view the current routing table.



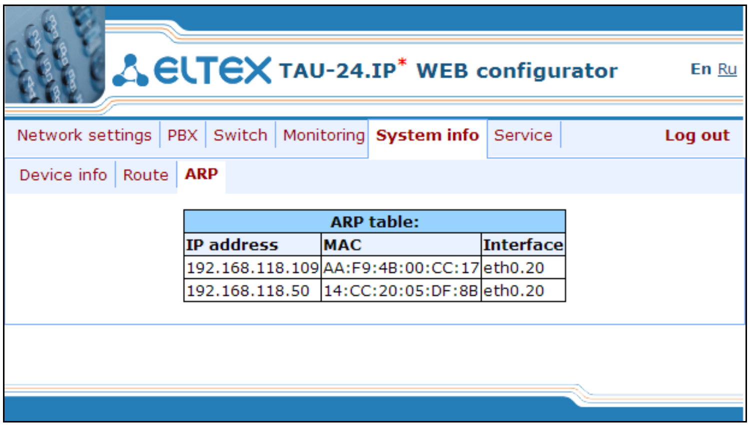
Kernel IP routing table:							
Destination	**Gateway**	**Genmask**	**Flags**	**Metric**	**Ref**	**Use**	**Iface**
192.168.118.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0.20
192.168.119.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	192.168.118.109	0.0.0.0	UG	0	0	0	eth0.20

<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 ARP

In *ARP* menu, you can view the device ARP table.



ARP table:		
IP address	MAC	Interface
192.168.118.109	AA:F9:4B:00:CC:17	eth0.20
192.168.118.50	14:CC:20:05:DF:8B	eth0.20

<u>*ARP table:*</u>

- *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 *Service*

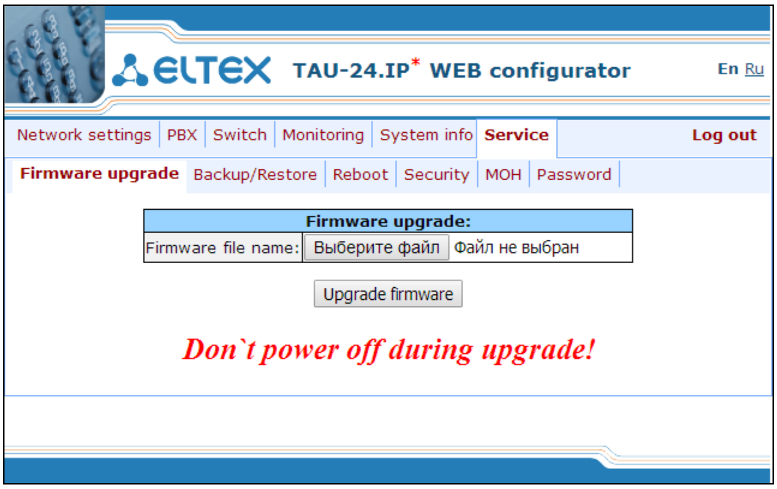
In *'Service'* menu, you may update the firmware, work with configuration files and other service features.

5.1.6.1 *Firmware upgrade*

In *'Firmware upgrade'* submenu, you may update the firmware of the subscriber units.

If the firmware version has been issued prior to September 2010, it is forbidden to update the file system and Linux kernel from a single archive!

Firmware versions prior to 1.11.x should be updated according to the instructions listed in the beginning of this operation manual.



Firmware upgrade:

Firmware file name: Выберите файл Файл не выбран

Don`t power off during upgrade!

In *'Firmware upgrade'* section, you can update the TAU firmware (firmware file is an image named ***firmware.img***).

In the opened window, specify the path to the firmware file by clicking *'Select File'* button and click

'*Upgrade firmware*' button.

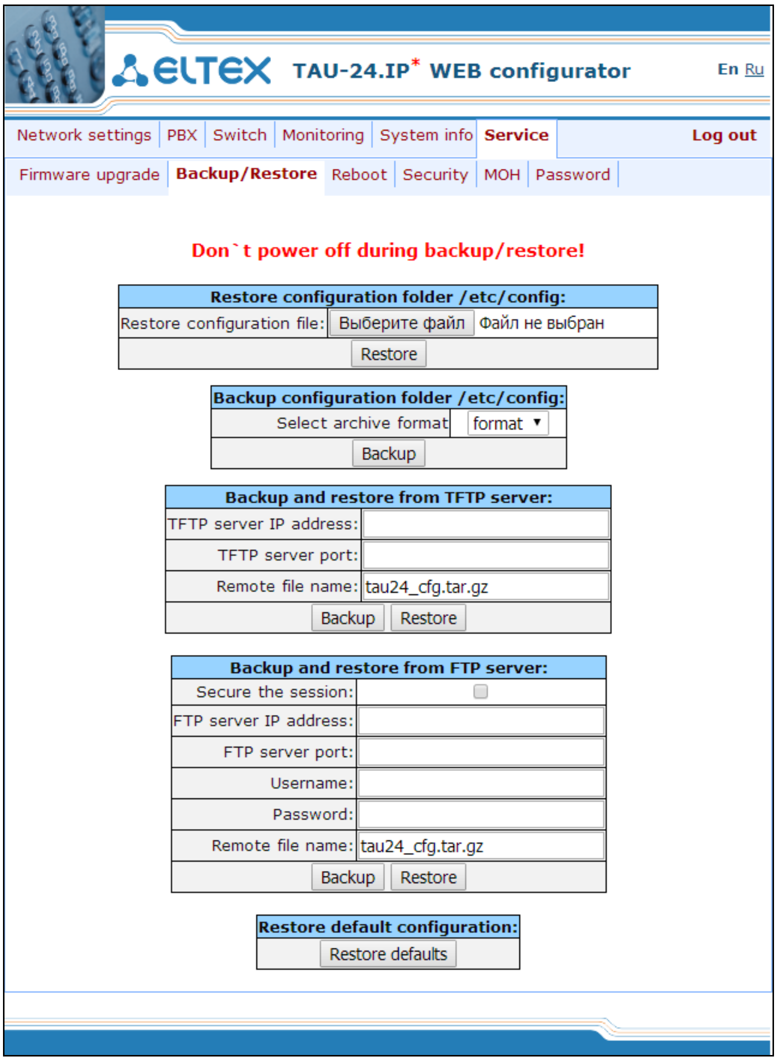
5.1.6.2 Download/Upload Configuration *(Backup/Restore)*

In *'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.



TAU-24.IP* WEB configurator En Ru

Network settings | PBX | Switch | Monitoring | System info | Service | Log out

Firmware upgrade | Backup/Restore | Reboot | Security | MOH | Password

Don`t power off during backup/restore!

Restore configuration folder /etc/config:	
Restore configuration file:	Выберите файл Файл не выбран
Restore	

Backup configuration folder /etc/config:	
Select archive format	format ▾
Backup	

Backup and restore from TFTP server:	
TFTP server IP address:	
TFTP server port:	
Remote file name:	tau24_cfg.tar.gz
Backup Restore	

Backup and restore from FTP server:	
Secure the session:	□
FTP server IP address:	
FTP server port:	
Username:	
Password:	
Remote file name:	tau24_cfg.tar.gz
Backup Restore	

Restore default configuration:

Restore defaults

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 *'Restore configuration file'* field using *'Select file'* button (file name should be as follows: tau24_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 tau24_cfg.tar, or tau24_cfg.tar.gz depending on the selected format).

To download configuration files or other folders to a PC, click *'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 *'Restore'* button, to upload configuration files from TFTP server to device. Click *'Backup'* button to download files from device to TFTP server.

3. Download/upload files using FTP server

Backup/Restore from FTP server:

- *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 *'Restore'* button, to upload configuration files to device. Click *'Backup'* button, to download configuration files from device.

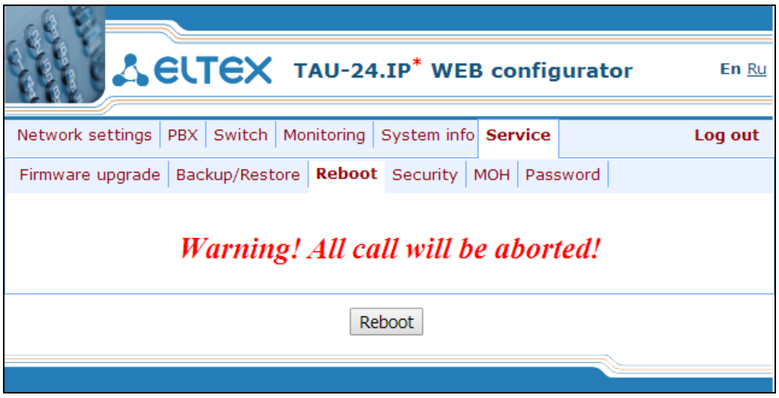
Click *'Restore default'* button to reset the configuration to factory defaults.

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 *'Reboot'* button in the *'Reboot'* submenu.

5.1.6.3 *Reboot*

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


ELTEX TAU-24.IP* WEB configurator
En Ru
Network settings | PBX | Switch | Monitoring | System info | Service | Log out
Firmware upgrade | Backup/Restore | Reboot | Security | MOH | Password

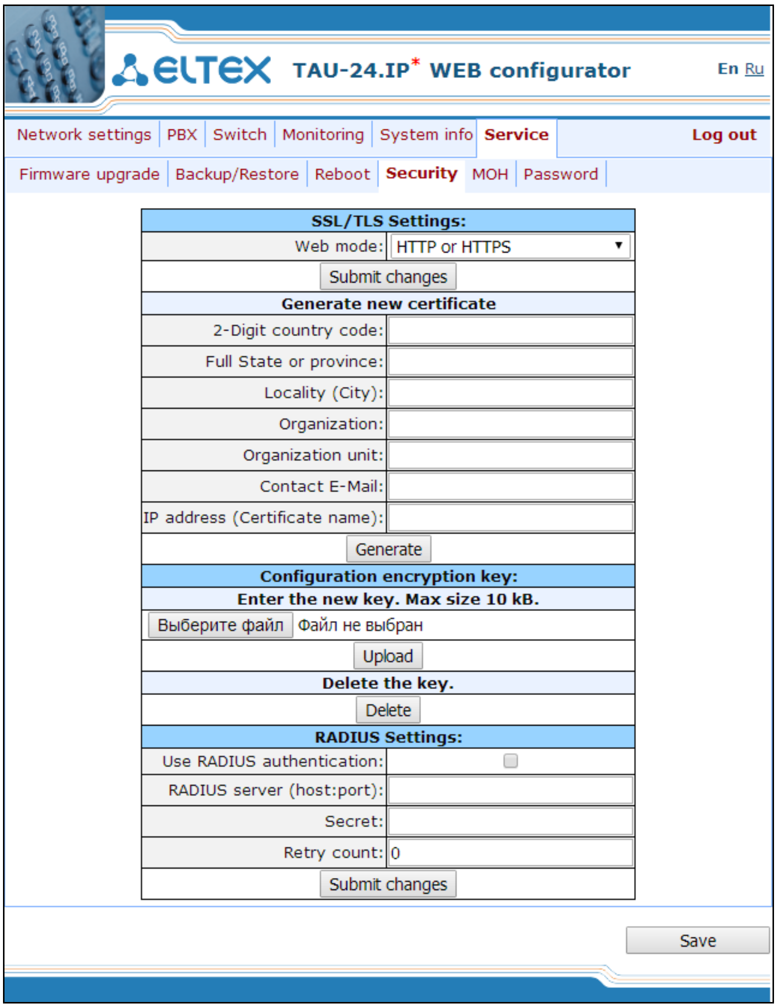
Warning! All call will be aborted!

To reboot the device, click *'Reboot'* button.

Before performing a reboot, make sure that all changes are saved, otherwise they will be lost!

5.1.6.4 Encryption Features (Security)

In *'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.



SSL/TLS Settings:	
Web mode:	HTTP or HTTPS
Generate new certificate	
2-Digit country code:	
Full State or province:	
Locality (City):	
Organization:	
Organization unit:	
Contact E-Mail:	
IP address (Certificate name):	
Configuration encryption key:	
Enter the new key. Max size 10 kB.	
Delete the key.	
RADIUS Settings:	
Use RADIUS authentication:	□
RADIUS server (host:port):	
Secret:	
Retry count:	0

— *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.

When you change connection mode in WEB configurator, click *'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 *'Generate'* button to generate self-signed certificate.

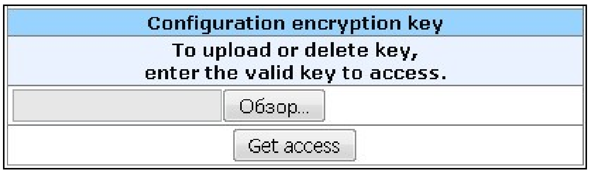
Configuration encryption key:

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'*, specify path to file to be uploaded to the device using *'Select file'* button and click *'Upload'.*


Configuration encryption key

To upload or delete key,
enter the valid key to access.

RADIUS Settings:

- *Use RADIUS authentication*—use RADIUS server for authentication of users administering the device via WEB, telnet, SSH.
- *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

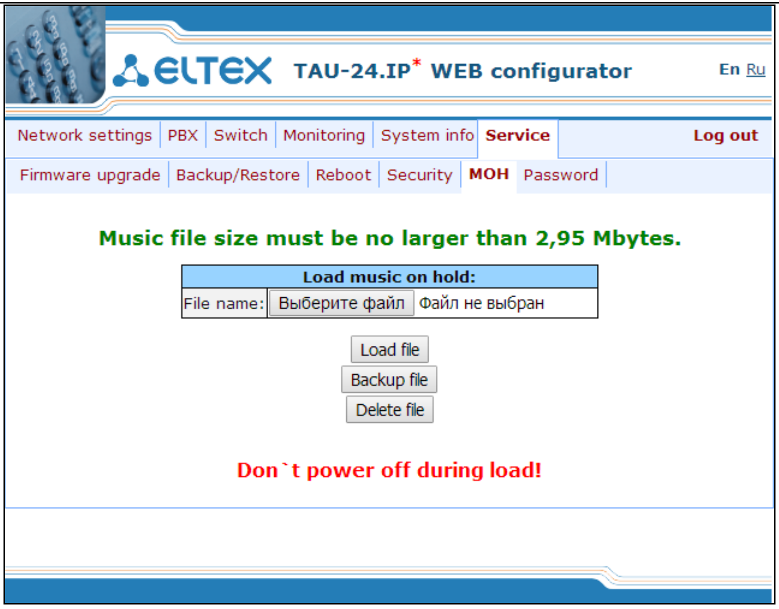
To delete or change previously uploaded key, specify the path to the encryption key using 'Browse' button and then click *'Get access'*.

To save changes, click *'Save'* button.

5.1.6.5 'Music on Hold' service configuration (MOH)

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.

Correct operation of the service is guaranteed only for connections that use G.711A and G.711U codecs!



Music file size must be no larger than 2,95 Mbytes.

Load music on hold:

File name: Выберите файл Файл не выбран

Don`t power off during load!

— *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:

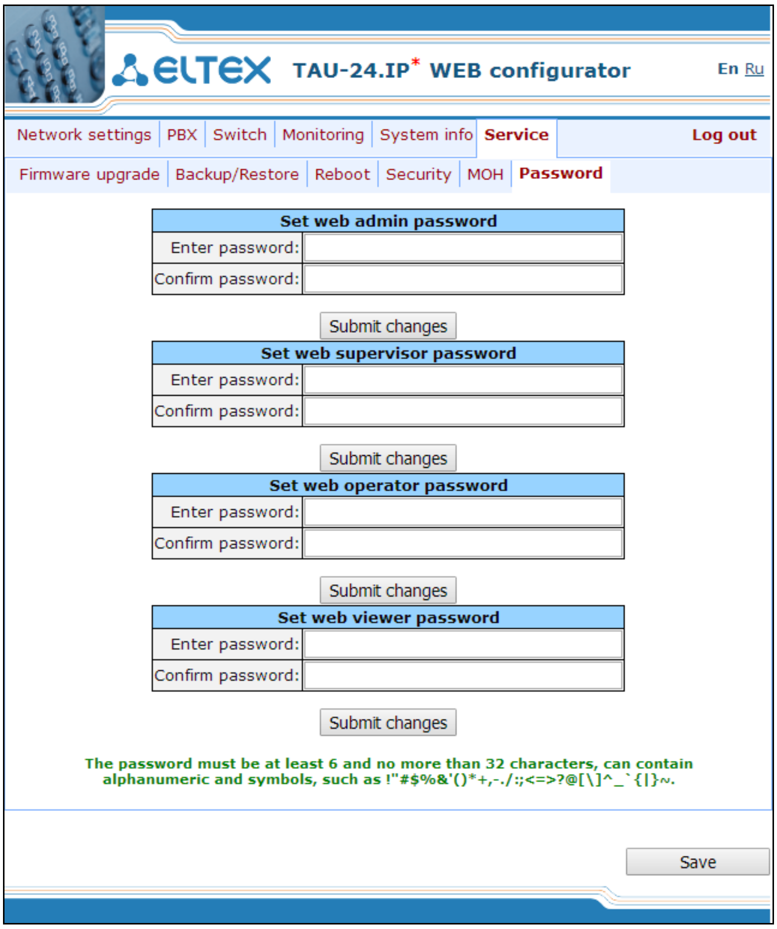
ffmpeg -fs <X>M -i <inputfilename> -ar 8000 -acodec pcm_alaw -ac 1 <outputfilename>.

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 Changing Access Passwords using Web Configurator (Password)

In *'Passwords'* submenu, you may work with passwords for device access via web interface.



Set web admin password

Enter password:

Confirm password:

Set web supervisor password

Enter password:

Confirm password:

Set web operator password

Enter password:

Confirm password:

Set web viewer password

Enter password:

Confirm password:

The password must be at least 6 and no more than 32 characters, can contain alphanumeric and symbols, such as !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~.

Access passwords operations:

- *Set web admin password*—administrator password for device access via web interface (*admin* user).
- *Set supervisor password*—supervisor password for device access via web interface (*supervisor* user).
- Set operator password—operator password for device access via web interface (*operator* user).
- *Set viewer password*—viewer password for device access via web interface (*viewer* user).

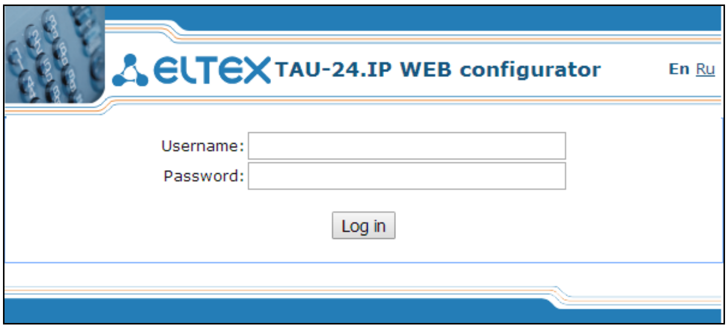
User rights:

- *supervisor*—will be able to access all device parameters in read-only mode.
- *admin*—has full access to the device.
- *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 'Submit Changes' button. To save changes, click *'Save'* button.

5.1.6.7 Change user

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 *Log in'* button. To exit configuration program, click *'Cancel'* button.

5.2 TAU-24.IP/TAU-16.IP Configuration via web Interface Operator Access

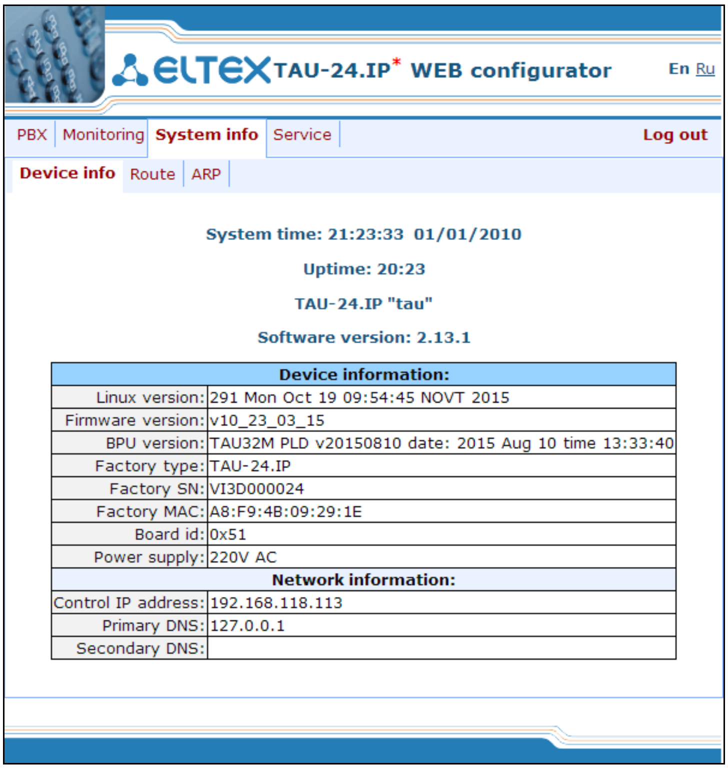
To configure the device, establish connection in the *web browser*, e.g. Firefox, Internet Explorer, etc. Enter device IP address into address bar of web browser.

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

TAU factory default IP address—192.168.1.2, network mask—255.255.255.0

Initial startup username: *operator*
password: specified by admin.

The following menu will appear on the operator's terminal:



System time: 21:23:33 01/01/2010

Uptime: 20:23

TAU-24.IP "tau"

Software version: 2.13.1

Device information:	
Linux version:	291 Mon Oct 19 09:54:45 NOVT 2015
Firmware version:	v10_23_03_15
BPU version:	TAU32M PLD v20150810 date: 2015 Aug 10 time 13:33:40
Factory type:	TAU-24.IP
Factory SN:	VI3D000024
Factory MAC:	A8:F9:4B:09:29:1E
Board id:	0x51
Power supply:	220V AC
Network information:	
Control IP address:	192.168.118.113
Primary DNS:	127.0.0.1
Secondary DNS:	

Web configurator supports indication of configuration changes, that is shown in the header bar of configuration interface (TAU-24.IP/TAU-16.IP WEB configurator.) Table 5 lists indicator states ('*' character in the header bar of configuration interface).

In all tabs, '*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.

Table 8 lists web configurator menu tabs available to the operator. For detailed web configurator description, see Section 5.1 of this document.

Table 8 - Description of configuration menu, operator access

Menu (en)	Description	Section
PBX	**VoIP (Voice over IP) configuration**	**5.1.2**
Main	Device basic settings	5.1.2.1
SIP/H323 Profiles	Configuration of SIP/H323 profiles	5.1.2.2
SIP Common	SIP common settings	5.1.2.2.1
H323	H323 protocol settings (works in profile 1 only)	5.1.2.2.2
Profile 1..8	Profile configuration	5.1.2.2.3
SIP Custom	SIP custom settings for a profile	5.1.2.2.3
Codecs	Codec settings for a profile	5.1.2.2.4
Dialplan	Routing settings for a profile	5.1.2.2.5
Alert-Info	Configuration of a distinctive ring, formed by Alert-Info value	5.1.2.2.6
TCP/IP	Configuration of network port range for various protocols	5.1.2.3
Ports	Configuration of Subscriber Ports	5.1.2.4
Call limits	Configuration of simultaneous call limits	5.1.2.5
Suppl. Service Codes	Configuration of Supplementary Service Codes	5.1.2.6
Serial groups	Configuration of serial groups	5.1.2.7
PickUp groups	Configuration of call pickup group	5.1.2.8
Distinctive ring	'Distinctive ring' service administration	5.1.2.9
Modifiers	Configuration of number modifiers	5.1.2.10
Monitoring	Device monitoring	**5.1.4**
Port	Device subscriber ports status information	5.1.4.1
Status	Gateway hardware platform status information—voltages, temperature sensors, fans, SFP data	5.1.4.2
Switch	Switch port state monitoring	5.1.4.3
Suppl. Service	Information on the current status of supplementary services on subscriber port	5.1.4.4
IMS SS status	State monitoring of services managed by the software switch with IMS function support	5.1.4.5
Serial groups	Serial group registration status monitoring	5.1.4.6
System info	**System information**	**5.1.5**
Device info	View the device and network settings information	5.1.5.1
Route	Routing table configuration	5.1.5.2
ARP	ARP table configuration	5.1.5.3
Service	**Firmware update, configuration file operations, rebooting device, setting/changing passwords**	**5.1.6**
Reboot	Rebooting device	5.1.6.3
Logout	**Finish the device administration session for the current user**	**5.1.6.7**

5.3 Non-privileged user access for device monitoring

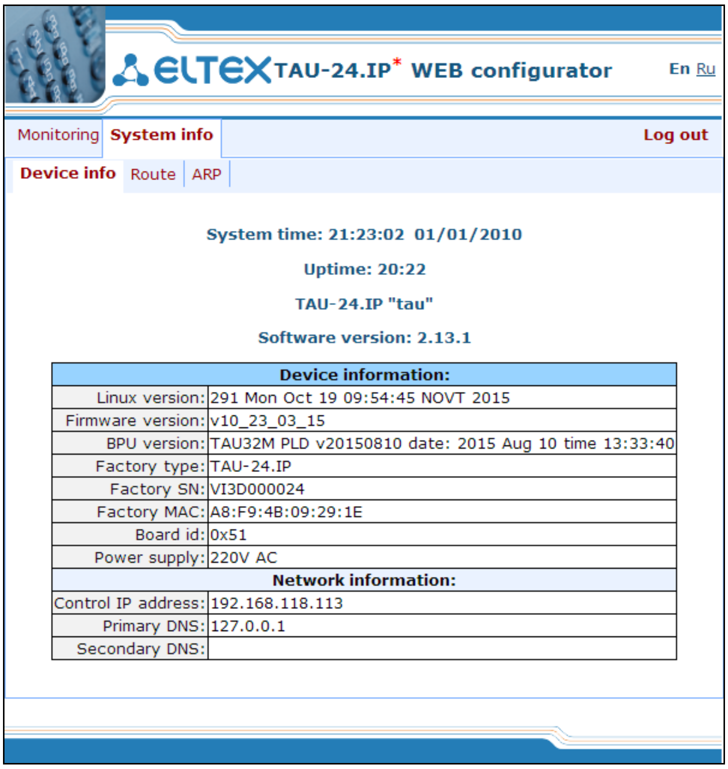
To monitor the device, establish connection in the *web browser* (hypertext document viewer), such as Firefox, Internet Explorer. Enter device IP address into address bar of web browser.

TAU 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:



System time: 21:23:02 01/01/2010

Uptime: 20:22

TAU-24.IP "tau"

Software version: 2.13.1

Device information:	
Linux version:	291 Mon Oct 19 09:54:45 NOVT 2015
Firmware version:	v10_23_03_15
BPU version:	TAU32M PLD v20150810 date: 2015 Aug 10 time 13:33:40
Factory type:	TAU-24.IP
Factory SN:	VI3D000024
Factory MAC:	A8:F9:4B:09:29:1E
Board id:	0x51
Power supply:	220V AC
Network information:	
Control IP address:	192.168.118.113
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 *Monitoring*

For detailed tabs description, see ***Section 5.1.4*** of this document.

5.3.2 *System info*

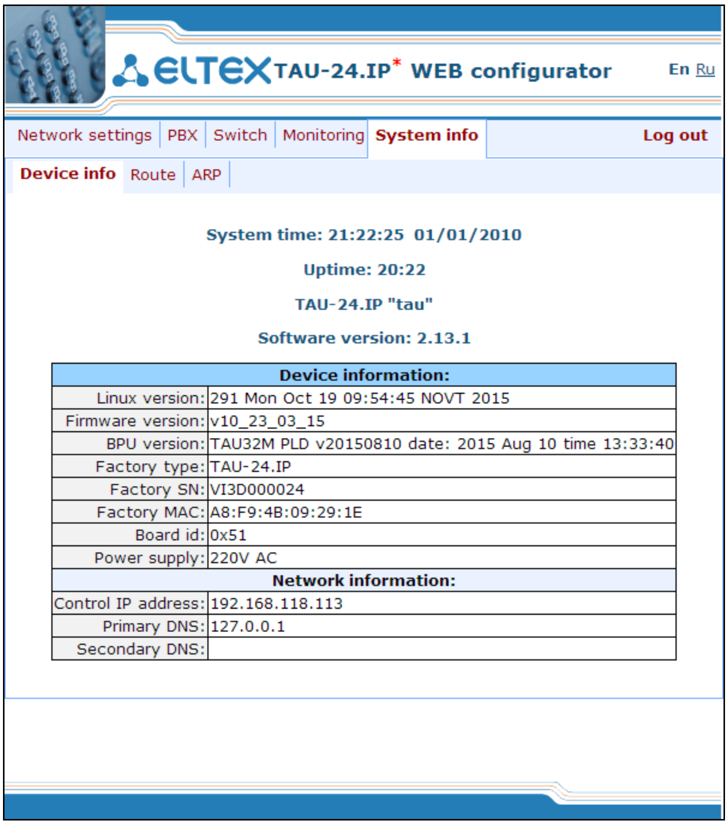
For detailed menu description, see ***Section 5.1.5*** of this document.

5.4 Supervisor Access

To login to the device, establish connection in the *web browser* (hypertext document viewer), such as Firefox, Internet Explorer. Enter device IP address into address bar of web browser (factory default 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.

The following menu will appear on the operator's terminal:



System time: 21:22:25 01/01/2010

Uptime: 20:22

TAU-24.IP "tau"

Software version: 2.13.1

Device information:	
Linux version:	291 Mon Oct 19 09:54:45 NOVT 2015
Firmware version:	v10_23_03_15
BPU version:	TAU32M PLD v20150810 date: 2015 Aug 10 time 13:33:40
Factory type:	TAU-24.IP
Factory SN:	VI3D000024
Factory MAC:	A8:F9:4B:09:29:1E
Board id:	0x51
Power supply:	220V AC
Network information:	
Control IP address:	192.168.118.113
Primary DNS:	127.0.0.1
Secondary DNS:	

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.

Table 9—List of available commands

Command	Description
`config`	Enter the configuration mode
`?`	Show the list of available commands
`help`	Show help on CLI operation
`quit, logout, exit`	Exit the command line mode
`history`	Show the list of previously entered commands
`passwd`	Change password for 'admin' user
`ps`	Show information on the current processes
`reboot`	Reboot gateway
`route`	Show/configure the routing table
`save`	Save configuration into non-volatile memory
`shell`	Go to Linux console
`show hwaddr`	Show MAC address
`show ipaddr`	Show IP address
`show netmask`	Show network mask
`system`	Show firmware version
`traceroute`	Trace the route to host
`ping`	Send echo (ping) request
Application operation commands	
`pbx restart`	Command that allows to restart the main application
`pbx registration <n>`	SIP server registration renewal for ports working in a single SIP profile, where <n> is a number of SIP profile
Statistics operation commands	
`pbx history`	View the current call statistics
`pbx statistic <n>`	View the port-specific statistics, where <n> is a port number
Automatic configuration commands	
`update cfg <A.B.C.D> <filename>`	Configuration update: A.B.C.D. – IP address of a computer, that runs TFTP server, pointing to the folder with the file. filename—configuration file name
`update img <A.B.C.D> <filename>`	Software update: A.B.C.D. – IP address of a computer, that runs TFTP server, pointing to the folder with the file. filename—firmware file name
Configuration mode commands (use 'config' command to enter this mode). You may configure the device name in the configuration mode	
`?`	Show the list of available commands
`help`	Show help on CLI operation
`quit`	Exit the command line mode
`exit`	Exit the configuration mode
`history`	Show the list of previously entered commands
`mac set <AA:BB:CC:DD:EE:FF>`	Set the user MAC address
`mac clear`	Remove the user MAC address
`mac get`	Show the user MAC address
`reset <static | dhcp>`	Reset configuration to factory defaults (and set static or dynamic method to obtain network settings)
`save`	Save configuration into non-volatile memory

`set autoupdate <par1> <par2>`	Automatic update configuration par1: cfg—configuration file name fw—firmware versions' file name interval_cfg—configuration update period interval_fw—firmware update period src—autoupdate mode tftp—autoupdate server address usage—autoupdate utilization par2: par1 parameter value
`set <dhcp|dhcp_gateway> <on|off>`	Configure DHCP parameters for the main network: dhcp—use DHCP dhcp_gateway—use the gateway, received via DHCP

`set ntp interval`
`set ntp <interval| ipaddr| timecorrect| usage>`
	Configure NTP server operation parameters:
	interval—time resynchronization period
	ipaddr—NTP server IP address
	timecorrect—time zone
	usage—NTP protocol usage

`set <broadcast|gateway| ipaddr| netmask| dns> <A.B.C.D>`	Configure broadcast address, gateway, IP address, mask, DNS server address
`set pppoe <par1> <par2>`	PPPoE settings par1: password—password usage—PPPoE usage user—user name vid—identifier of VLAN network, used by PPPoE operations vlan—VLAN subnet utilization par2: par1 parameter value
`set <control|rtp|signaling> <no_vlan| vlan1| vlan2| vlan3| pppoe>`	Define the interface for control, voice traffic (RTP), and signalling no_vlan—main network without VLAN vlan1,vlan2,vlan3—corresponding VLAN network pppoe—PPPoE interface
`set <snmp| ssh| telnet> <on|off>`	Configuration of SNMP, SSH, TELNET protocols for gateway management
`set <vlan1| vlan2| vlan3> <par1> <par2>`	VLAN subnet configuration vlan1,vlan2,vlan3—VLAN subnet number par1: broadcast—broadcast address cos—802.1p priority dhcp—use DHCP dhcp_gateway—use the gateway, received via DHCP id—VLAN network identifier ipaddr—IP address netmask—network mask usage—VLAN subnet usage par2: par1 parameter value
`show`	Show network and autoconfiguration parameters
`version`	View configuration file version

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. Use CLI command to enter this mode.

To view the current call statistics, use `pbx 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 10—Call statistics record format.

Record	Description
No	Sequence number of the record
Local	TAU 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 11—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 subscriber put a remote subscriber on hold
holded	TAU 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-32M.IP subscriber put the phone offhook, didn't perform a call and put the phone back onhook
local busy	TAU-32M.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-32M.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-32M.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
Pickuper failed	'Call pickup' failed
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 **shell** command. 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@fxs24 /root]$ cd /tmp
[root@fxs24 /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.

To view the port-specific statistics, use the following command: `pbx statistic <n>`, where <n>—port number.

Table 12—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 `shell` command. 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@fxs24 /admin]$cd /
[admin@fxs24 /]$tar -cf conf.tar /etc/
[admin@fxs24 /]$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@fxs24 /admin]$cd /
[admin@fxs24 /]$tftp -gl conf.tar server ip-address
[admin@fxs24 /]$tar -xf conf.tar
```

Save settings using `'save'` command.
Restart the gateway using `'reboot -f'` command.

6.4 Setting password for 'admin' user

Given that it is possible to remotely connect to TAU gateway via Telnet, in order to prevent an unauthorized access, we recommend to set password for *admin* user (admin user is not protected by password in factory settings). To set the password, 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 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).

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-24 FXS Gateway   *
**************************

fxs24 login:
```

Enter `admin`; for factory settings, the password is not required.

5 Enter `passwd` command. The following text will appear on screen:

```
> passwd
Changing password for admin
New password:
```

6 Enter password, press <ENTER>, confirm password, press <ENTER>:

```
> passwd
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
```

7 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 `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.`

8 Save settings using `'save'` command.

9 Restart the gateway using `'reboot -f'` command.

6.5 Reset to Factory Defaults

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 'Status' indicator flashes (flashed green and red rapidly), then release the button to avoid another reboot of the device. TAU will begin its operation in '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/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).

To save factory configuration via WEB interface, click 'save' button in any tab.

Warning!!! In legacy firmware versions, this function may lead to situations when device always starts up in 'safemode'. To restore the normal operation, you should reset device configuration to factory defaults via console or Telnet/SSH.

Reset configuration to factory defaults, Telnet/SSH:

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-24 FXS Gateway   *
**************************

fxs24 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
> config reset static
```

or, if you have to define the dynamic
obtaining of network settings in factory configuration (via DHCP protocol):

```
> enable
> config reset dhcp
```

b. To reset settings in CLI mode and delete the console password, execute the following commands:

```
> shell
 reset2defaults static
```

or, if you have to define the dynamic obtaining of network settings in factory configuration (via DHCP protocol):

```
> shell
 reset2defaults dhcp
```

7 SUPPLEMENTARY SERVICES USAGE

7.1 Calltransfer

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 calltransfer', 'Unattended calltransfer', or 'Local CT' in 'Flash transfer' field, see Section 5.1.2.4.

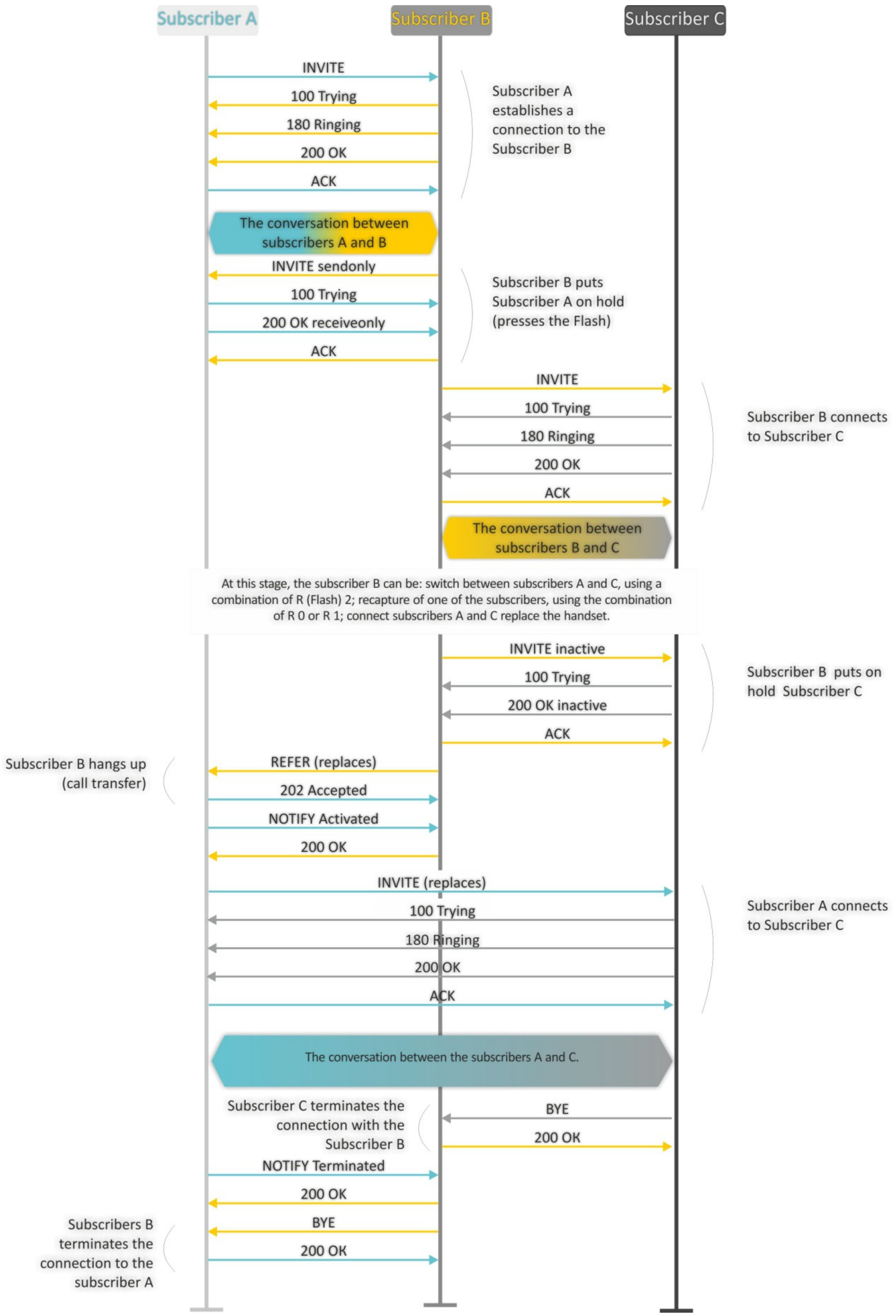
'*Attended calltransfer*' service allows you to temporarily disconnect an online subscriber (Subscriber A), establish connection with another subscriber (Subscriber C) and return to the previous connection without dialling or transfer the call while disconnecting Subscriber B (a subscriber that performs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

'*Attended calltransfer*' 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.
- R 4—call transfer. Voice connection will be established between Subscribers A and C.
- clearback—call transfer. Voice connection will be established between Subscribers A and C.

Fig. 7 shows an algorithm of '*Attended calltransfer*' service performed by Subscriber B via SIP protocol.



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

Fig. 7—Algorithm of '*Attended calltransfer*' service performed by Subscriber B via SIP protocol

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

Fig. 8 shows an algorithm of '*Unattended calltransfer*' service performed by Subscriber B via SIP protocol.

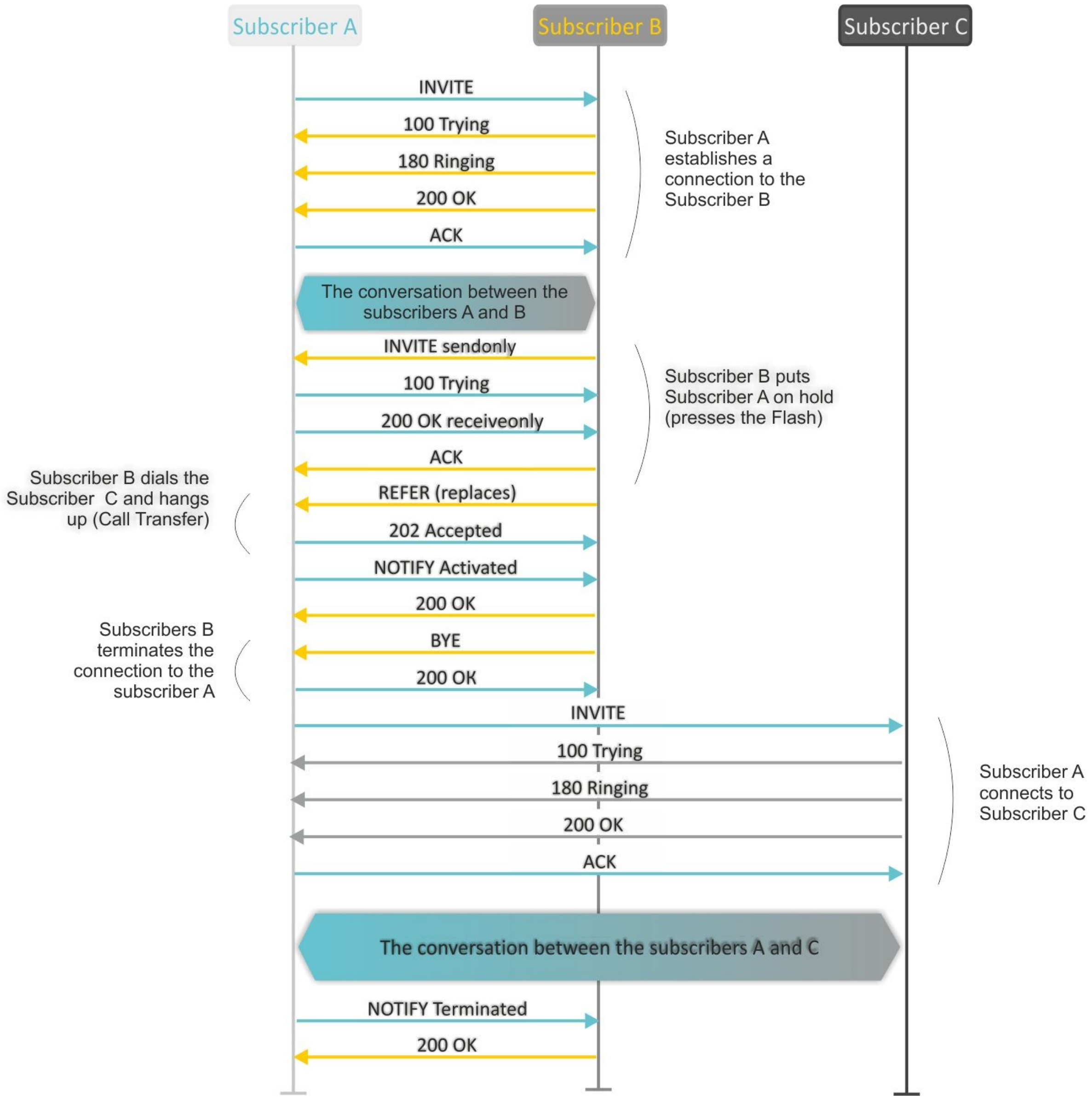

Subscriber A
Subscriber B
Subscriber C
INVITE
100 Trying
180 Ringing
200 OK
ACK
Subscriber A establishes a connection to the Subscriber B
The conversation between the subscribers A and B
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Subscriber B puts Subscriber A on hold (presses the Flash)
REFER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

Fig. 8—Algorithm of '*Unattended calltransfer*' service performed by Subscriber B via SIP protocol

7.2 Call Waiting

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 calltransfer', 'Unattended calltransfer', 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.
- R – short clearback (flash).

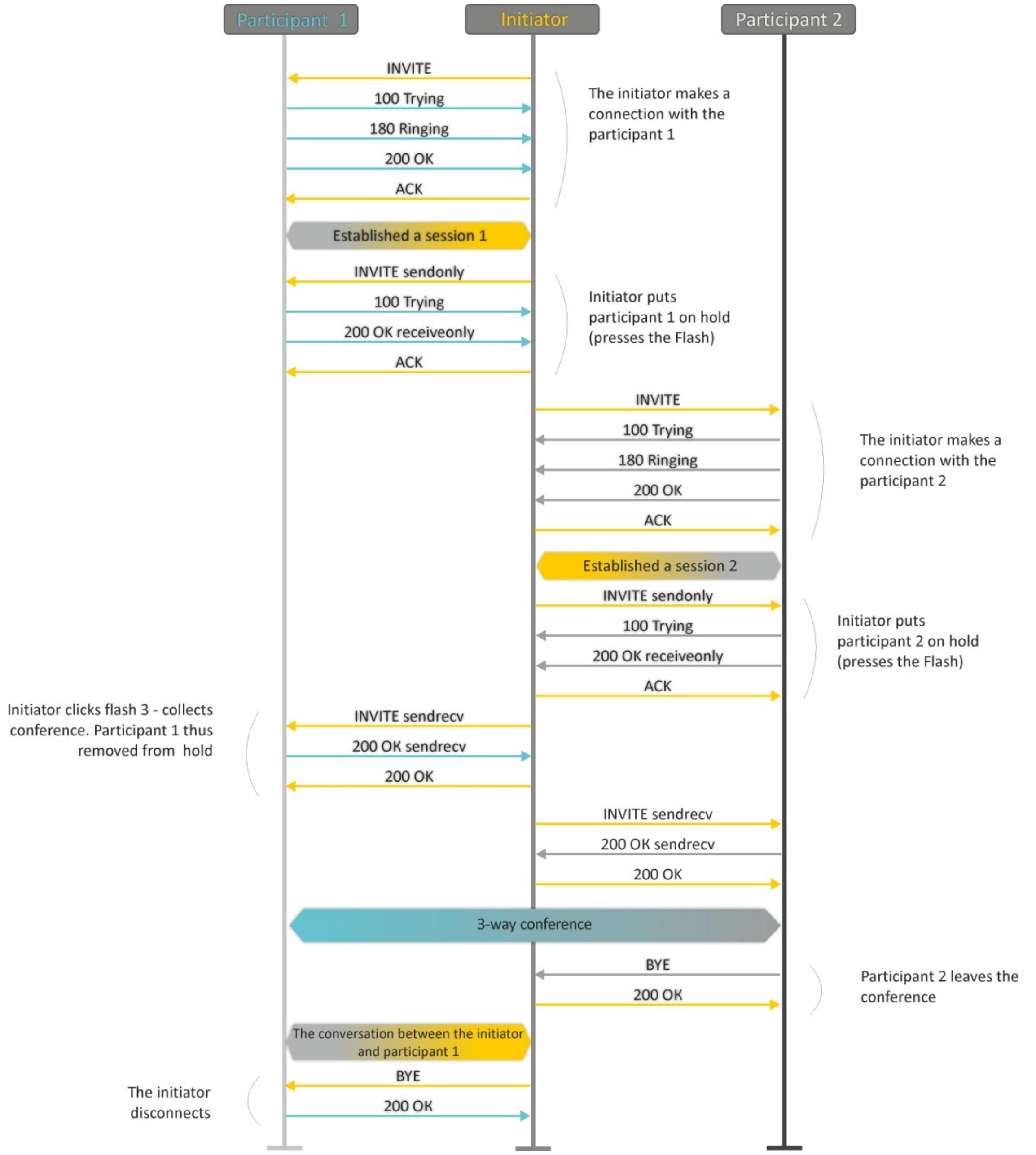
7.3 3-way conference

Three-way conference is a service, that enables simultaneous phone communication for 3 subscribers. For entering conference mode, see Section 7.1.

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.

Fig. 9 shows an algorithm of '3-way conference' service performed locally on the device via SIP protocol.



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

Fig. 9—Algorithm of '3-way conference' service performed locally on the device via SIP protocol

Fig. 10 shows an algorithm of '3-way conference' service performed at the conference server via SIP protocol ('REFER to focus' option).

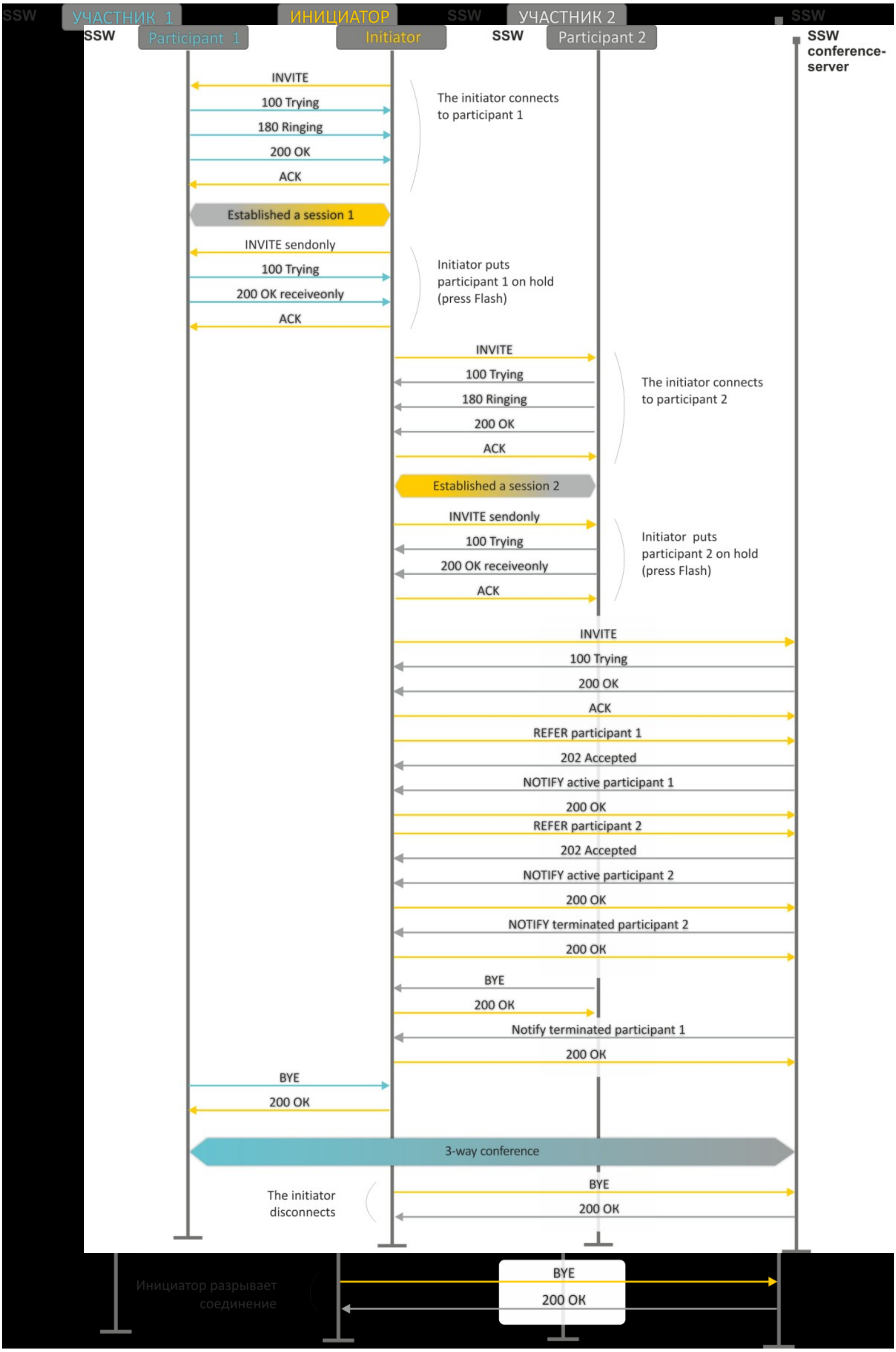


Fig. 10—Algorithm of '3-way conference' service performed at the conference server via SIP protocol (REFER to focus)

Fig. 11 shows an algorithm of '3-way conference' service performed at the conference server via SIP protocol ('REFER to user' option).

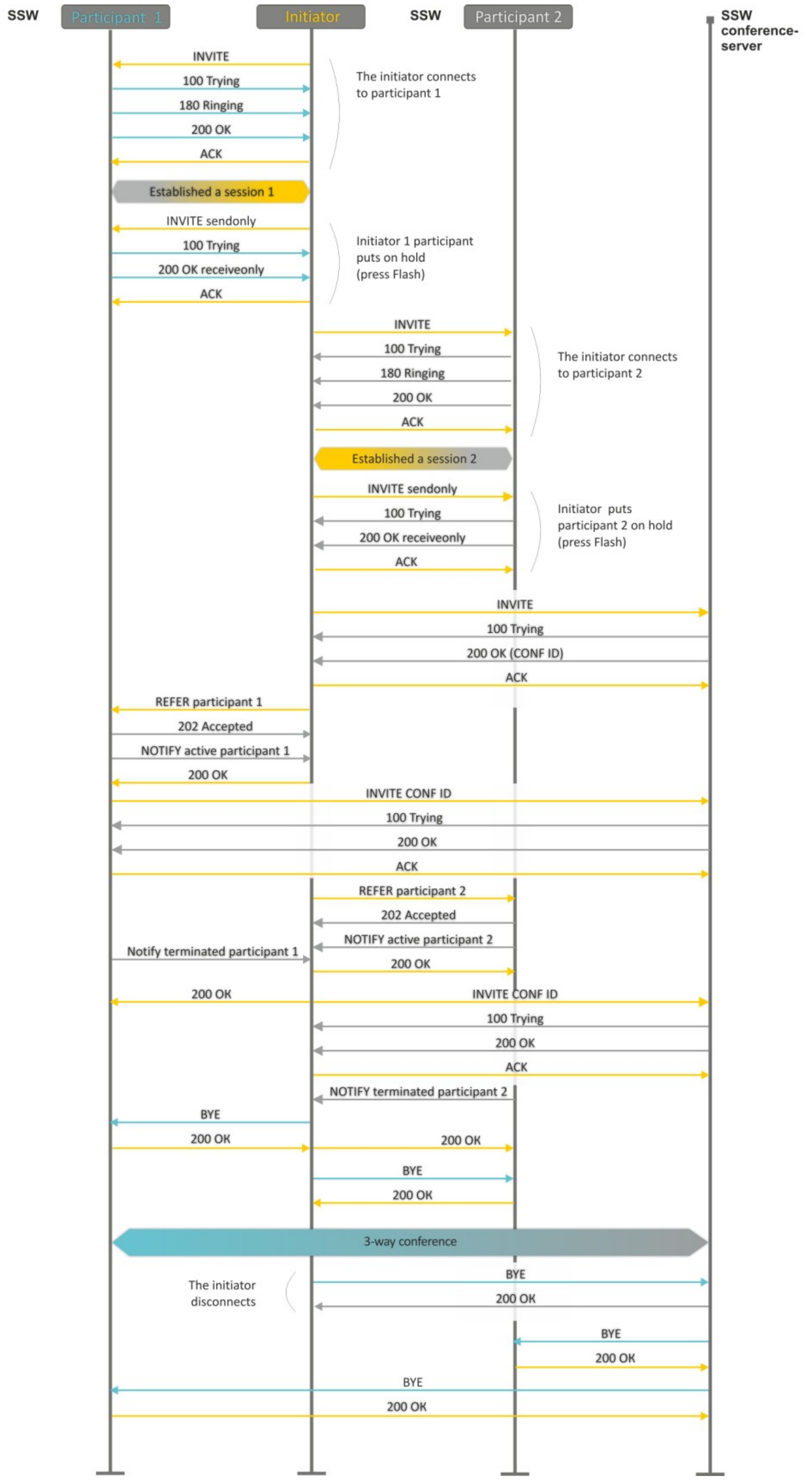


Fig. 11—Algorithm of '3-way conference' service performed at the conference server via SIP protocol (REFER to user)

8 CONNECTION ESTABLISHMENT ALCORITHMS

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.

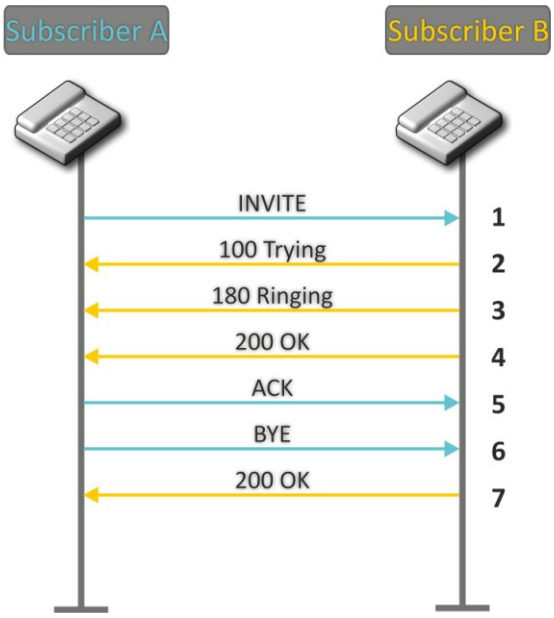


Fig. 12—SIP call algorithm

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.

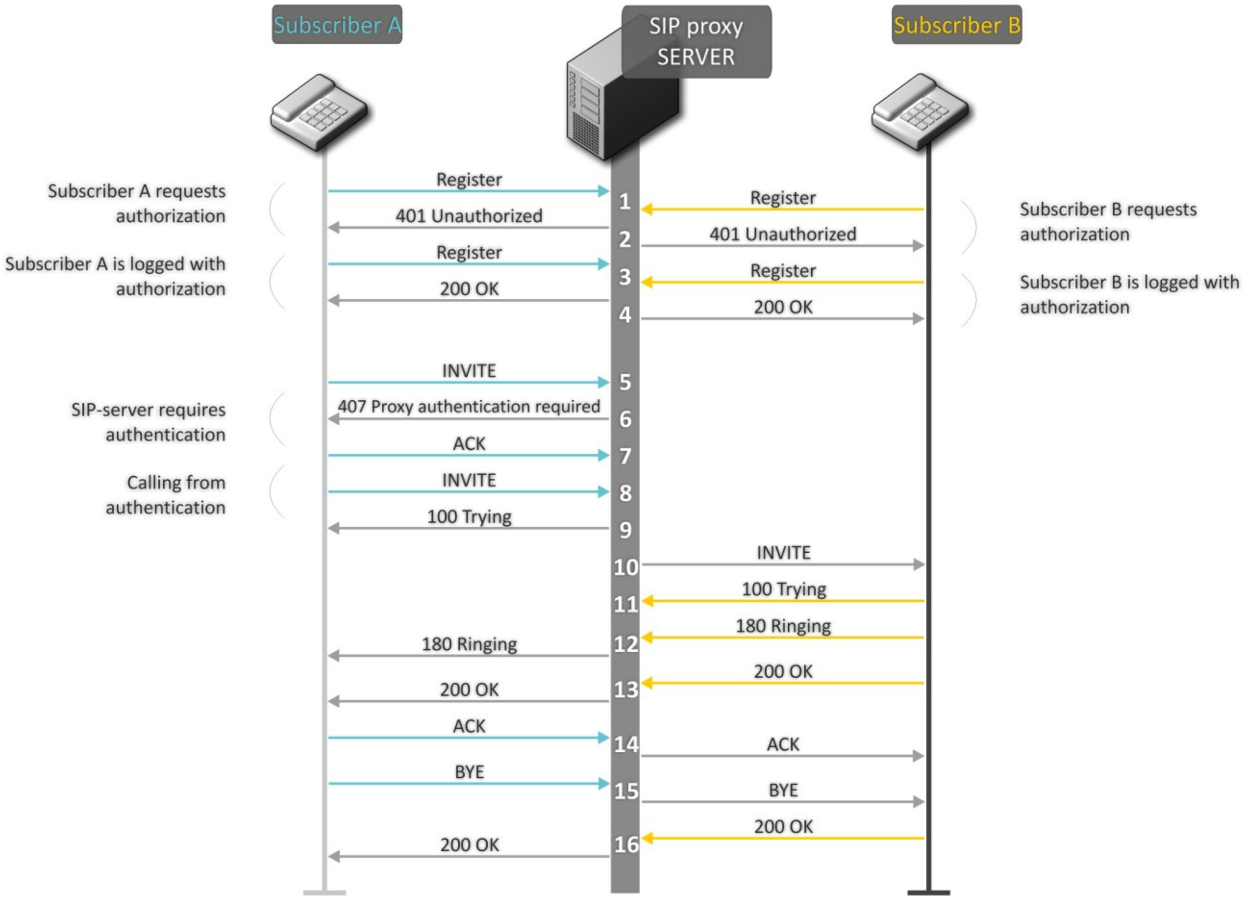

Subscriber A
SIP proxy SERVER
Subscriber B
Subscriber A requests authorization
Subscriber A is logged with authorization
SIP-server requires authentication
Calling from authentication
Subscriber B requests authorization
Subscriber B is logged with authorization
Register
401 Unauthorized
Register
200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

Fig. 13—Call algorithm involving SIP proxy server

Algorithm description:

1 Subscriber A and Subscriber B register at SIP server.

2 SIP server prompts for authorization.

3 Subscriber A and Subscriber B register at SIP server with authorization.

4 SIP server responses on successful registration.

5 Subscriber A rings up Subscriber B.

6 SIP server requests authentication.

7 Subscriber A gateway confirms received authorization request command.

8 Subscriber A rings up Subscriber B.

9 SIP server receives the command for processing.

10 SIP server translates Subscriber A call request directed at Subscriber B.

11 Subscriber B gateway receives the command for processing.

12 Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone to Subscriber A phone.

13 Subscriber B answers the call.

14 Subscriber A gateway confirms session establishment.

15 Subscriber A clears back, 'busy' audio tone is sent to the Subscriber B.

16 Subscriber B gateway confirms received clearback command.

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.

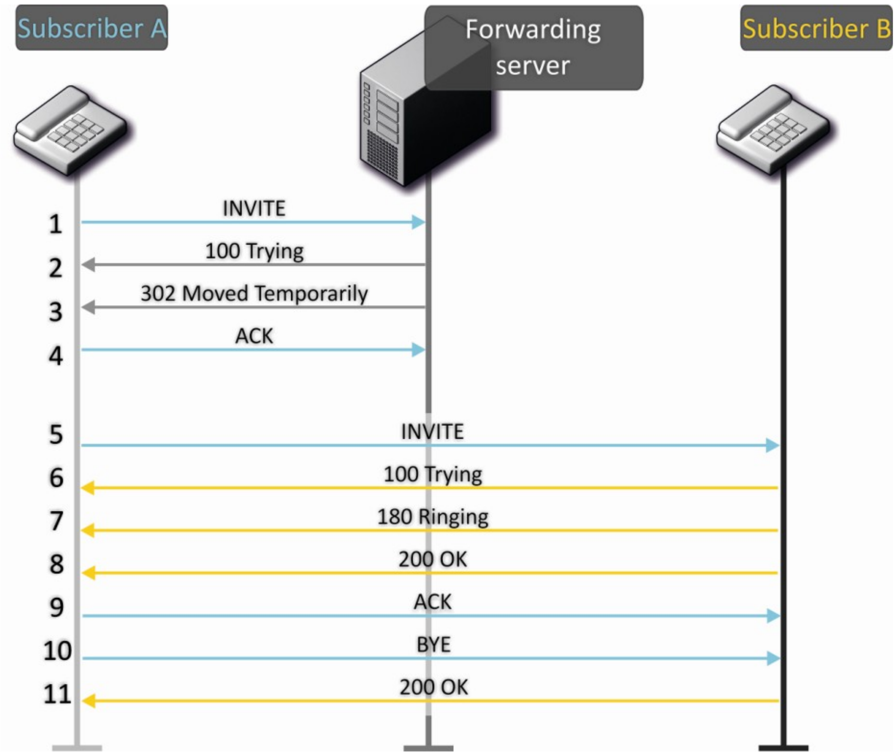


Fig. 14—Call algorithm involving forwarding server

Algorithm description:

1 Subscriber A rings up Subscriber B. Call is sent to the forwarding server with the callee address information.

2 Forwarding server receives the command for processing.

3 Forwarding server requests the information on the Subscriber B current address from the location server. Received information (the callee current address and the list of callee registered addresses) is sent to Subscriber A in '302 moved temporarily' message.

4 Subscriber A gateway confirms the reception of reply from the forwarding server.

5 Subscriber A rings up Subscriber B directly.

6 Subscriber B gateway receives the command for processing.

7 Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone to Subscriber A phone.

8 Subscriber B answers the call.

9 Subscriber A gateway confirms session establishment.

10 Subscriber A clears back, 'busy' audio tone is sent to the Subscriber B.

11 Subscriber B gateway confirms received clearback command.

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.

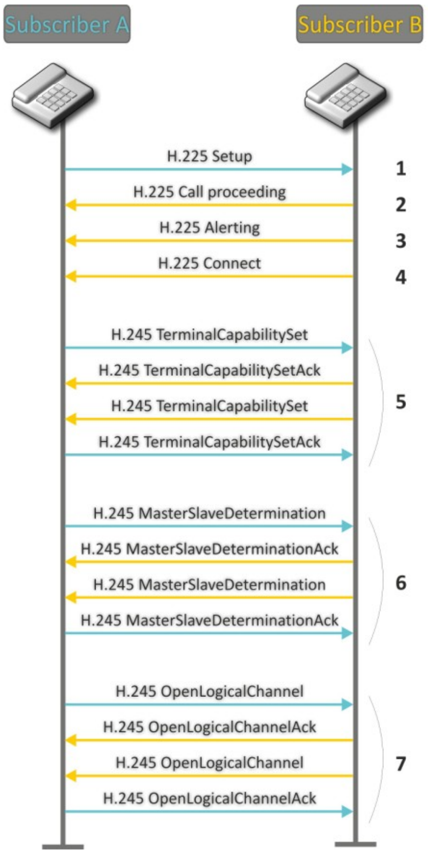

Subscriber A
Subscriber B
H.225 Setup
1
H.225 Call proceeding
2
H.225 Alerting
3
H.225 Connect
4
H.245 TerminalCapabilitySet
H.245 TerminalCapabilitySetAck
H.245 TerminalCapabilitySet
H.245 TerminalCapabilitySetAck
5
H.245 MasterSlaveDetermination
H.245 MasterSlaveDeterminationAck
H.245 MasterSlaveDetermination
H.245 MasterSlaveDeterminationAck
6
H.245 OpenLogicalChannel
H.245 OpenLogicalChannelAck
H.245 OpenLogicalChannel
H.245 OpenLogicalChannelAck
7

Fig. 15—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.

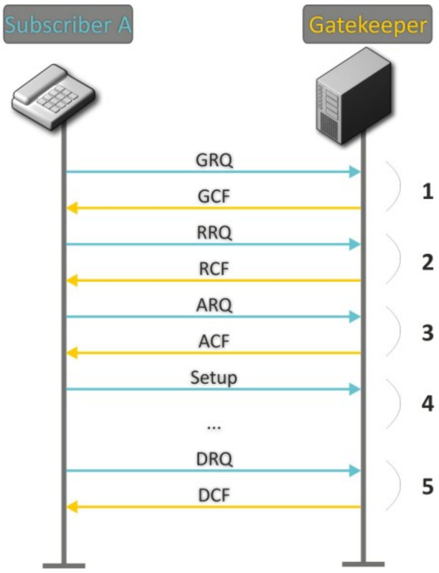


Fig. 16—Gatekeeper call algorithm

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 13—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 feature	0—faststart enabled 1—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 1—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
diffserv	Type of service for RTP packets (for utilized values, see Table 7)	0-255
sip_diffserv	Type of service for SIP packets (for utilized values, see Table 7)	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
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
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
publicip	IP address of a public NAT	A.B.C.D
shortmode	Use shortened field names in SIP protocol header	0–disable 1–enable
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	Subscriber's response timeout	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—configuration of Syslog parameters		
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_alarm	Send alarm event messages to Syslog server	0–disable 1–enable
app_dbg	Send application debug 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
limits—call limits		
limit_0 to 19	Call restriction rules Examples: limit_0: [proxy] 5 limit_1: 192.168.16.53 8	A.B.C.D or FQDN or [proxy] N 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 Warning!!! 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
cadence—'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!!! Example: '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	|—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)
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.	For syntax, see Section **5.1.2.10 Modifiers**
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—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. 2—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 '183progress' message transmission via SIP protocol.
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')
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. 1—Remote—conference assembly is performed at the conference 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. '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–enable
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
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
only_register_ changeover	Type of requests used for changeover to redundant proxy	0 – INVITE, REGISTER 1 – REGISTER 2 – INVITE
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	G.726-32 codec payload type	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 (Flash transmission by the subscriber's port via IP network is possible only when 'Transmit flash' is configured on this port)	0—Flash transmission disabled 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
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
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. - It is recommended, that 'Delay threshold' was greater than 'Delay max' for at least of 50ms.	jb_vo_delay_max-500
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
rfc3264_pt_common	When performing outgoing call, receive DTMF tones in rfc2833 format with payload type proposed by a communicating gateway; otherwise, 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
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 protocol h323—H.323 protocol (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 **Enumeration of pickup groups, used in a file, is less by 1 than enumeration, used in web interface!!!**
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 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 Value: 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. Value: - 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) Value: 0 – unknown; 1 – subscriber; 2 – national; 3 – international. d9—play 'PBX response' tone when the first prefix digit is dialled. Value: 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, "+" – allowed, portN,..portM—comma-separated list of ports. Example: +0,32—access is allowed for ports 1 and 33. Warning!!! 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. Value: 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
name	Signal received in alert-Info header	
ports—configuration of device subscriber ports and subscriber profiles		
port_def 0..7—subscriber profile settings		
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; when this setting is enabled, the category will be sent in 'from' field, and 'tel uri' will be used instead of 'sip uri'	0—disable categories 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
port_0..23—port 0..23 custom settings		
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 a file corresponds to 'port 1' in WEB interface and on the device housing.**		
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	Authentication username	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' service is enabled	String, 20 digits max. or ""—parameter is not defined
custom	Use port custom settings	0—use common settings from common configuration for all ports 1—use custom settings specified for this port
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 the line with 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	200-600ms
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 digits max. or ""—parameter is not defined
cfb_number	Number, that the call is forwarded to when the subscriber is busy	String, 20 digits max. or ""—parameter is not defined
cfu_number	Number for 'Call forward unconditional'	String, 20 digits max. or ""—parameter is not defined
cfoos_number	Number, that the call is forwarded to when the subscriber is out of service	String, 20 digits 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 1 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
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 digits 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 is enabled 1—port is disabled
cpc_rus	Subscriber category; when this setting is enabled, the category will be sent in 'from' field, and 'tel uri' will be used instead of 'sip uri'	0—disable categories 1-10—subscriber category
modifier	Modifier group used by this profile	0-15
mwi_dialtone	'Message waiting indicator' service	0–disable 1–enable
pstn_rb_detect_timeout	Ringback tone detection in the subscriber line Allows to avoid establishment of voice connection in IP networks prior to the answer of a subscriber, or prior to detection of the specific number of rings. If there is no ringback tone within the specified value, it is considered that the callee has responded (reply '200 OK' is sent via SIP)	1-60
fxo_detect_line_presence	Detection of subscriber's line connection to FXO for the line status view in monitoring	0–disable 1–enable
fxo_block_line_presence	Block FXO set, if the subscriber's line is not connected to it	0–disable 1–enable

9.1.2 Device network settings

Table 14—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.

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
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	VLAN1, 2, 3 usage	0–disable 1–enable
v1ipaddr	VLAN1,2,3 interface IP address	A.B.C.D
v2ipaddr	Net mask, used for VLAN1,2,3 interface	A.B.C.D
v3ipaddr	Broadcast address in VLAN1,2,3 interface subnet	A.B.C.D
v1netmask	VLAN 1, 2, 3 identifier	1-4095
v2netmask	802.1p priority for VLAN1, 2, 3	0-7
v3netmask	VLAN assignment for voice traffic	0–disable 1 – VLAN1 2 – VLAN2 3 – VLAN3 4 – PPPoE
v1broadcast	VLAN destination for SIP/H323 signalling traffic	0–disable 1 – VLAN1 2 – VLAN2 3 – VLAN3 4 – PPPoE
v2broadcast	VLAN destination for gateway management via WEB interface, telnet, ssh	0–disable 1 – VLAN1 2 – VLAN2 3 – VLAN3 4 – PPPoE
v3broadcast	DNS server IP address	A.B.C.D
vid 1,2,3	Device time synchronization with an external server via NTP	0–disable 1–enable
v1mtu	Maximum transmission unit (VLAN 1)	86-1496
v2mtu	Maximum transmission unit (VLAN 2)	86-1496
v3mtu	Maximum transmission unit (VLAN 3)	86-1496
cos 1,2,3	NTP server address	A.B.C.D
rtp_vlan	RTP transfer interface	0—use the main interface for RTP transfer 1-3—use VLAN interface for RTP transfer 4—use PPPOE interface for RTP transfer
sig_vlan	Signalling transfer interface	0—use the main interface for signalling transfer 1-3—use VLAN interface for signalling transfer 4—use PPPOE interface for signalling transfer

ctl_vlan	Management interface	0—use the main interface for management 1-3—use VLAN interface for management 4—use PPPOE interface for management
telnet_en	Device access via Telnet protocol	0–disable 1–enable
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
ntpen	NTP protocol	0–disable 1–enable
ntpip	NTP server IP address	A.B.C.D
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
cfg_interval	Configuration file version check interval	1 - 99999
fw_interval	Software version check interval	1 - 99999
dnsip	Primary DNS server IP address	A.B.C.D
reserved_dnsip	Secondary DNS server IP address	A.B.C.D
telnet_port	TCP port for TELNET protocol operation	1-65535, 23 by default
ssh_port	TCP port for SSH protocol operation	1-65535, 22 by default
web_port	WEB server port number for HTTP protocol operation	1-65535, 80 by default
https_port	WEB server port number for HTTPS protocol operation	1-65535, 443 by default
web_en	Device access via web interface	0–disable 1–enable
radius_enable	Use RADIUS server for authentication of users administering the device via WEB, telnet, SSH	0–disable 1–enable
radius_server	RADIUS server address	A.B.C.D
radius_secret	Password to access the RADIUS server	String, 50 characters max.
radius_retry	Number of retries during the access to RADIUS server	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

TR-069—configuration of TR-069 monitoring and management protocol settings		
Enable	TR-069 device management process	0–disable 1–enable
URL	ACS server address	http://<address>:<port>, where <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. Goal of the polling is to identify possible changes in the device configuration	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	User 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; identifies the method, that will be used by client for obtaining its public address information	STUN Manual Off See description on page 36.
NATAddress	STUN server IP address or domain name	
STUNEnable	use STUN protocol for public address identification	0–disable 1–enable
STUNServerAddress	STUN server IP address or domain name	
STUNServerPort	STUN server UDP port	1-65535, 3478 by default
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
snmp—snmp protocol configuration		
agentproto	Transport protocol	udp
agentport	Transport port used by agent	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	(server manager or proxy agent) A.B.C.D
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 are written comma-separated in one string Access mode: - rw—read/write - ro—read

9.1.3 Switch port settings

Table 15–Switch port settings (Switch)

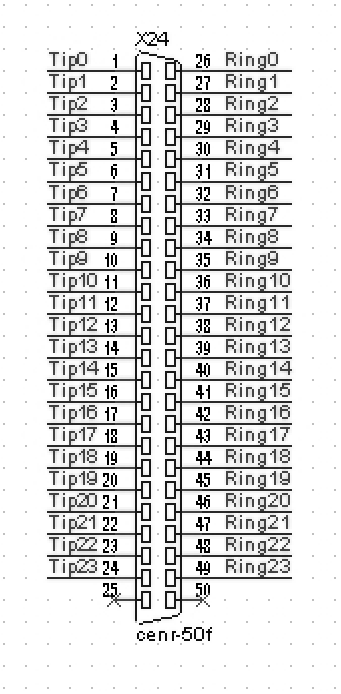
Field name	***Description***	***Values***
vlan—example of switch configuration using VLAN		
hubmode	Ethernet switch operation in hub mode	0–disable 1–enable
Port mapping: 0—GE0 (GE2) port 1—GE1 (GE1) port 2—GE2 (GE0) port 3—CPU port (CPU) 4—SFP0 port (SFP0) 5—SFP1 port (SFP1) In models of with one SFP port is used only SFP 0		
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 ID	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 In models of with one SFP port is used only SFP 0	
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 A—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: 0x1C, low for: 0x18 C—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-24.IP/TAU-16.IP NETWORK TERMINAL CONTACT PIN ASSIGNMENT



Ring[X] and Tip[X] contacts are designed for the phone unit connection.

Wire colour and terminal contact correspondence table (Nexans 25×2×24 c. 5+ cable)

Twisted pair	Wire	Terminal contact	Twisted pair	Wire	Terminal contact
Yellow-brown	**Yellow**	**1**	White-brown	**White**	**13**
	Brown	26		Brown	38
Black-green	**Black**	**2**	Red-green	**Red**	**14**
	Green	27		Green	39
White-gray	**White**	**3**	Purple -gray	**Purple**	**15**
	Gray	28		Gray	40
Red-blue	**Red**	**4**	Yellow-blue	**Yellow**	**16**
	Blue	29		Blue	41
Purple-orange	**Purple**	**5**	Black-orange	**Black**	**17**
	Orange	30		Orange	42
Yellow-gray	**Yellow**	**6**	White -green	**White**	**18**
	Gray	31		Green	43
Black-brown	**Black**	**7**	Red -brown	**Red**	**19**
	Brown	32		Brown	44
White-orange	**White**	**8**	Purple -blue	**Purple**	**20**
	Orange	33		Blue	45
Red-gray	**Red**	**9**	Yellow-green	**Yellow**	**21**
	Gray	34		Green	46
Purple-green	**Purple**	**10**	Black -gray	**Black**	**22**
	Green	35		Gray	47
Yellow-orange	**Yellow**	**11**	White -blue	**White**	**23**
	Orange	36		Blue	48
Black-blue	**Black**	**12**	Red -orange	**Red**	**24**
	Blue	37		Orange	49
			Purple-brown	**Purple**	**25**
				Brown	50

Wire colour and terminal contact correspondence table (Teldor 25×2×24 c. 5 cable)

Colour	Terminal contact	Colour	Terminal contact
Black-blue	**1**	**Purple-green**	**13**
Blue-Black	26	Green-purple	38
Black-orange	**2**	**Purple-brown**	**14**
Orange-Black	27	Brown-purple	39
Black-green	**3**	**Purple-gray**	**15**
Green- black	28	Gray-purple	40
Black-brown	**4**	**Red-blue**	**16**
Brown-black	29	Blue-red	41
Black-gray	**5**	**Red-orange**	**17**
Gray-black	30	Orange-red	42
Yellow-blue	**6**	**Red-green**	**18**
Blue-yellow	31	Green-red	43
Yellow-orange	**7**	**Red-brown**	**19**
Orange-yellow	32	Brown-red	44
Yellow-green	**8**	**Red-gray**	**20**
Green-yellow	33	Grey-red	45
Yellow brown	**9**	**White-blue**	**21**
Brown-yellow	34	Blue-white	46
Yellow-gray	**10**	**White-orange**	**22**
Gray-yellow	35	Orange-white	47
Purple-blue	**11**	**White-green**	**23**
Blue-purple	36	Green-white	48
Purple-orange	**12**	**White-brown**	**24**
Orange-purple	37	Brown-white	49
		White-gray	**25**
		Gray-white	50

Wire colour and terminal contact correspondence table (NENSHI NSPC-7019-25 cable)

Colour	Terminal contact	Colour	Terminal contact
White-blue	**1**	**Black-green**	**13**
Blue	26	Green	38
White-orange	**2**	**Black-brown**	**14**
Orange	27	Brown	39
White-green	**3**	**Black-gray**	**15**
Green	28	Gray	40
White-brown	**4**	**Yellow-blue**	**16**
Brown	29	Blue	41
White-gray	**5**	**Yellow-orange**	**17**
Gray	30	Orange	42
Red-blue	**6**	**Yellow-green**	**18**
Blue	31	Green	43
Red-orange	**7**	**Yellow-brown**	**19**
Orange	32	Brown	44
Red-green	**8**	**Yellow-gray**	**20**
Green	33	Gray	45
Red-brown	**9**	**Purple-blue**	**21**
Brown	34	Blue	46
Red-gray	**10**	**Purple-orange**	**22**
Gray	35	Orange	47
Black-blue	**11**	**Purple-green**	**23**
Blue	36	Green	48
Black-orange	**12**	**Purple-brown**	**24**
Orange	37	Brown	49
		Purple-gray	**25**
		Gray	50

APPENDIX B. ALTERNATIVE FIRMWARE UPDATE METHOD

When you cannot update the firmware via web interface or the console (telnet, RS-232), you may use an alternative firmware update method via 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-24>>
```

7. Enter `set ipaddr` {device ip address} <ENTER> (for example: `set ipaddr 192.168.16.112`).
8. Enter `set netmask` {device network mask} <ENTER> (for example: `set netmask 255.255.255.0`).
9. Enter `set serverip` {IP address of a computer, that runs TFTP server} <ENTER> (for example: `set serverip 192.168.16.44`).
10. To activate the network interface, execute `mii i` <ENTER> command:

```
=> mii i
Init switch 0: ..Ok!
Init switch 1: ..Ok!
Init phy 1: ..Ok!
Init phy 2: ..Ok!
=>
```

11. To update linux kernel, use `run updatecsp` command:

```
FXS-24>> 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-24>>
```

12. To update the media processor firmware, use `run updatemsp` command:

```
FXS-24>> 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-24>>
```

13. To update the file system, use `run updatefs` command:

```
FXS-24>> 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-24>>
```

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.

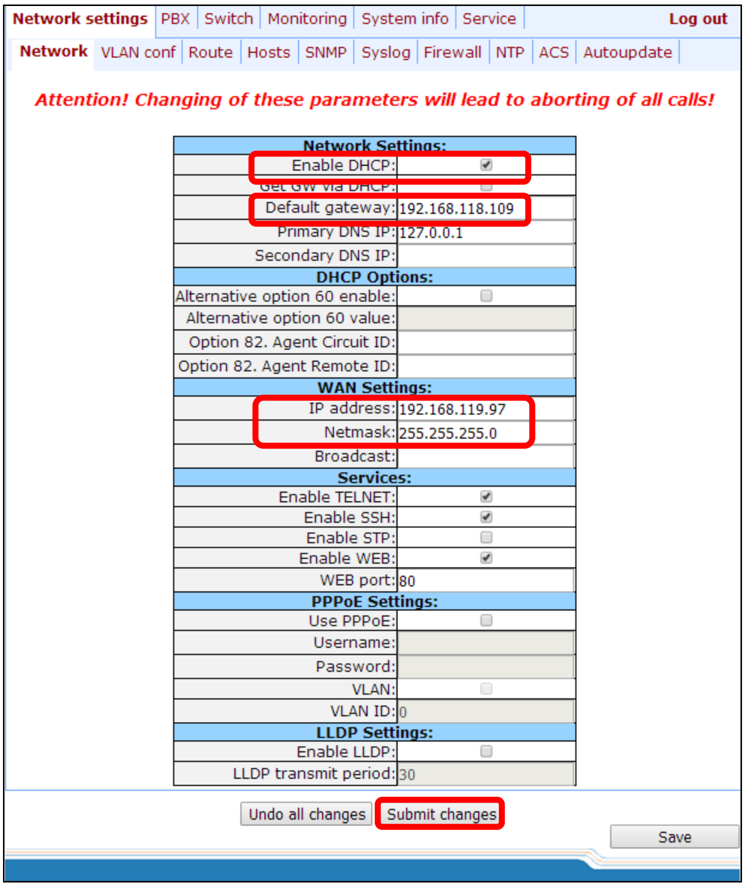
2. Device configuration is performed via WEB interface (see Paragraph **5.1** of this manual) using a web browser (e.g. Internet Explorer, Mozilla Firefox, Opera, Google Chrome). Initial connection to the gateway is performed by IP address, specified by the manufacturer (TAU factory default IP address—192.168.1.2, network mask—255.255.255.0).

   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 as a DHCP server client in order to obtain IP address automatically: '*Network settings -> Network*' menu section, select '*Use DHCP*' checkbox.

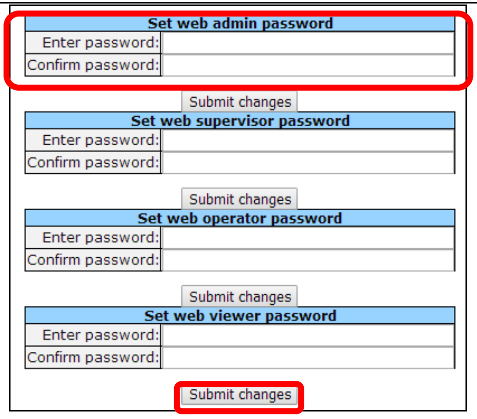
Make sure to apply changes with 'Submit Changes' button, located in the bottom of the page.



Attention! Changing of these parameters will lead to aborting of all calls!

Network Settings:	
Enable DHCP:	☑
Get GW via DHCP:	□
Default gateway:	192.168.118.109
Primary DNS IP:	127.0.0.1
Secondary DNS IP:	
DHCP Options:	
Alternative option 60 enable:	□
Alternative option 60 value:	
Option 82. Agent Circuit ID:	
Option 82. Agent Remote ID:	
WAN Settings:	
IP address:	192.168.119.97
Netmask:	255.255.255.0
Broadcast:	
Services:	
Enable TELNET:	☑
Enable SSH:	☑
Enable STP:	□
Enable WEB:	☑
WEB port:	80
PPPoE Settings:	
Use PPPoE:	□
Username:	
Password:	
VLAN:	□
VLAN ID:	0
LLDP Settings:	
Enable LLDP:	□
LLDP transmit period:	30

3. We highly recommend changing default password after device installation in '*Service ->Password*' menu section:



Set web admin password

Enter password:	
Confirm password:	

Submit changes

Set web supervisor password

Enter password:	
Confirm password:	

Submit changes

Set web operator password

Enter password:	
Confirm password:	

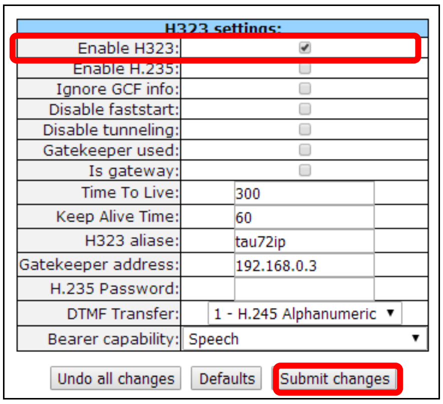
Submit changes

Set web viewer password

Enter password:	
Confirm password:	

Submit changes

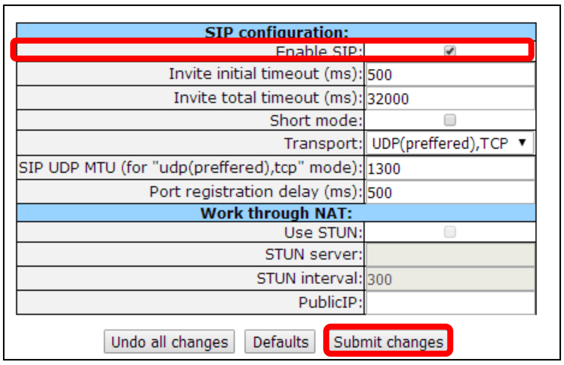
4. When the respective protocol (*SIP/H.323*) is used in *'PBX -> SIP/H323 Profiles -> SIP Common'* and *'PBX -> SIP/H323 Profiles -> H323'* menu sections, you should activate operation via these protocols by selecting *'Enable SIP'*, *'Enable H323'* checkboxes.



H323 settings:

Enable H323:	☑
Enable H.235:	□
Ignore GCF info:	□
Disable faststart:	□
Disable tunneling:	□
Gatekeeper used:	□
Is gateway:	□
Time To Live:	300
Keep Alive Time:	60
H323 aliase:	tau72ip
Gatekeeper address:	192.168.0.3
H.235 Password:	
DTMF Transfer:	1 - H.245 Alphanumeric ▾
Bearer capability:	Speech ▾

Undo all changes | Defaults | Submit changes

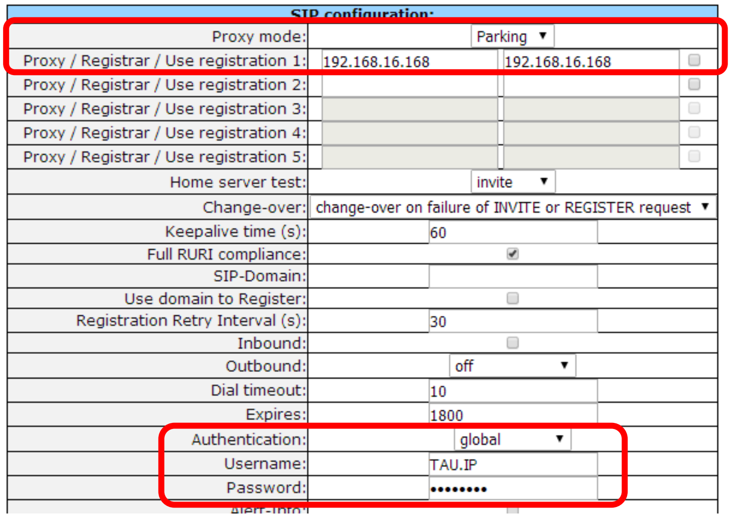


SIP configuration:

Enable SIP:	☑
Invite initial timeout (ms):	500
Invite total timeout (ms):	32000
Short mode:	□
Transport:	UDP(preffered),TCP ▾
SIP UDP MTU (for "udp(preffered),tcp" mode):	1300
Port registration delay (ms):	500
Work through NAT:	
Use STUN:	□
STUN server:	
STUN interval:	300
PublicIP:	

Undo all changes | Defaults | Submit changes

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.



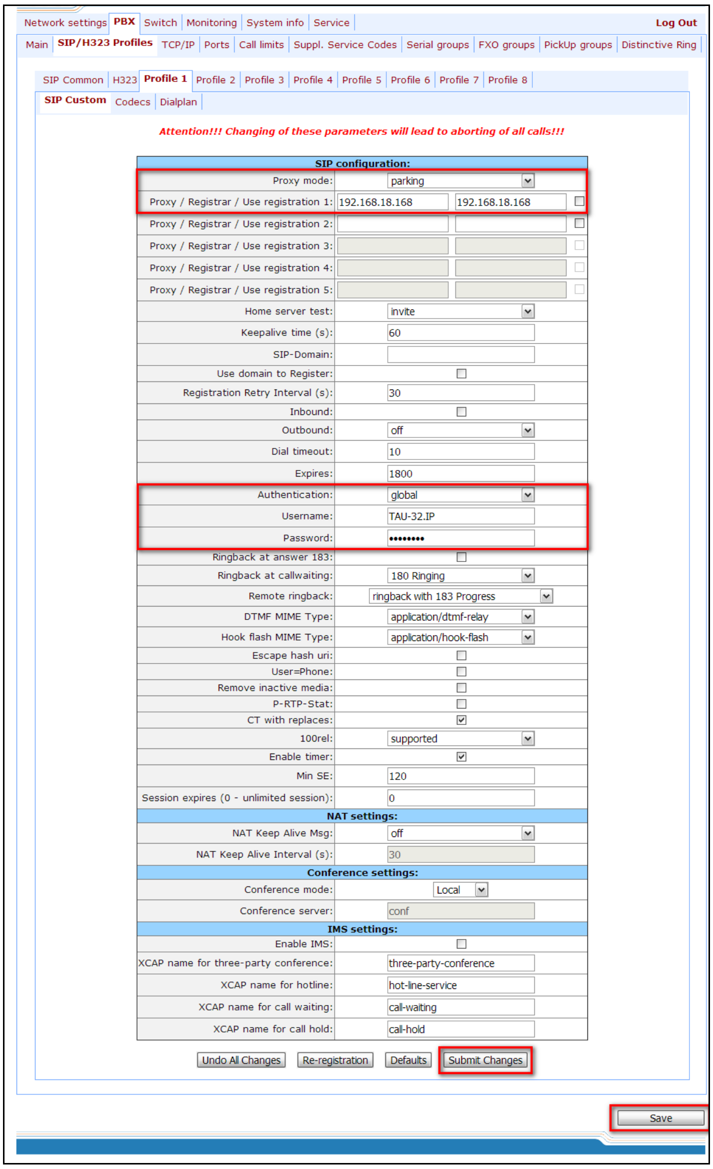
SIP configuration:

Proxy mode:	Parking ▾		
Proxy / Registrar / Use registration 1:	192.168.16.168	192.168.16.168	□
Proxy / Registrar / Use registration 2:			□
Proxy / Registrar / Use registration 3:			□
Proxy / Registrar / Use registration 4:			□
Proxy / Registrar / Use registration 5:			□
Home server test:	invite ▾		
Change-over:	change-over on failure of INVITE or REGISTER request ▾		
Keepalive time (s):	60		
Full RURI compliance:	☑		
SIP-Domain:			
Use domain to Register:	□		
Registration Retry Interval (s):	30		
Inbound:	□		
Outbound:	off ▾		
Dial timeout:	10		
Expires:	1800		
Authentication:	global ▾		
Username:	TAU.IP		
Password:	••••••••		
Alert-Info:	□		

In '*PBX -> SIP/H323 Profiles -> Profile n -> SIP Custom*' tab, perform the following settings:

- To be able to register device ports on the registration server, you should define a reservation mode in 'Proxy mode' menu item.
- 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; in this case, SIP-proxy server (Proxy) address is the same as for the registration server (Registrar).
- To enable port authorization, you should set the following value for 'Authentication' parameter: 'global' or 'user defined'.

a) 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.

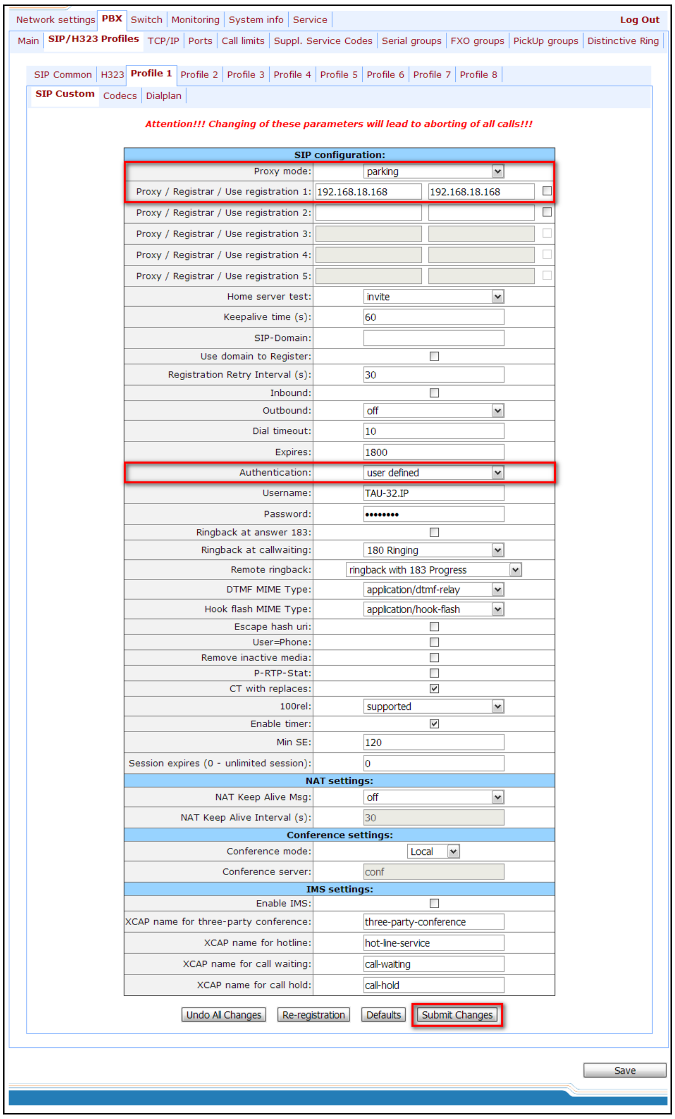


Attention!!! Changing of these parameters will lead to aborting of all calls!!!

SIP configuration:			
Proxy mode:	parking		
Proxy / Registrar / Use registration 1:	192.168.18.168	192.168.18.168	□
Proxy / Registrar / Use registration 2:			□
Proxy / Registrar / Use registration 3:			□
Proxy / Registrar / Use registration 4:			□
Proxy / Registrar / Use registration 5:			□
Home server test:	invite		
Keepalive time (s):	60		
SIP-Domain:			
Use domain to Register:	□		
Registration Retry Interval (s):	30		
Inbound:	□		
Outbound:	off		
Dial timeout:	10		
Expires:	1800		
Authentication:	global		
Username:	TAU-32.IP		
Password:	••••••••		
Ringback at answer 183:	□		
Ringback at callwaiting:	180 Ringing		
Remote ringback:	ringback with 183 Progress		
DTMF MIME Type:	application/dtmf-relay		
Hook flash MIME Type:	application/hook-flash		
Escape hash uri:	□		
User=Phone:	□		
Remove inactive media:	□		
P-RTP-Stat:	□		
CT with replaces:	☑		
100rel:	supported		
Enable timer:	☑		
Min SE:	120		
Session expires (0 - unlimited session):	0		
NAT settings:			
NAT Keep Alive Msg:	off		
NAT Keep Alive Interval (s):	30		
Conference settings:			
Conference mode:	Local		
Conference server:	conf		
IMS settings:			
Enable IMS:	□		
XCAP name for three-party conference:	three-party-conference		
XCAP name for hotline:	hot-line-service		
XCAP name for call waiting:	call-waiting		
XCAP name for call hold:	call-hold		

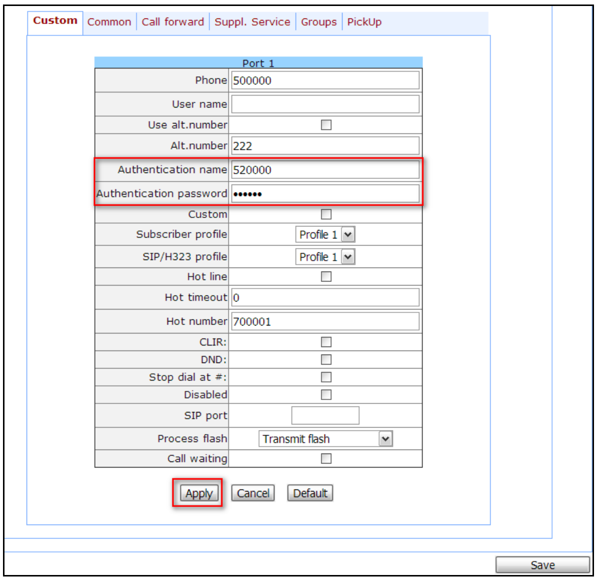
b) When 'user defined' value is used, each port will be authorized with its own name and password, in this case authorization name and password should be specified in 'PBX ->

Ports -> Edit -> Custom' section, 'Authentication name' and 'Authentication password' fields respectively.



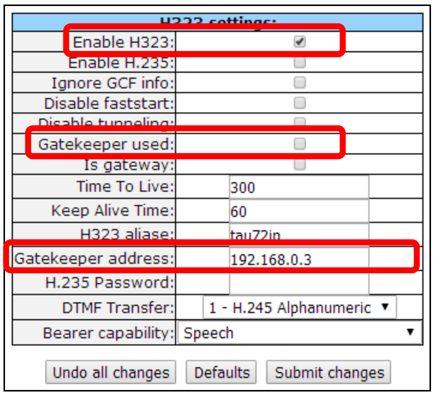
Attention!!! Changing of these parameters will lead to aborting of all calls!!!

SIP configuration:			
Proxy mode:	parking		
Proxy / Registrar / Use registration 1:	192.168.18.168	192.168.18.168	□
Proxy / Registrar / Use registration 2:			□
Proxy / Registrar / Use registration 3:			□
Proxy / Registrar / Use registration 4:			□
Proxy / Registrar / Use registration 5:			□
Home server test:	invite		
Keepalive time (s):	60		
SIP-Domain:			
Use domain to Register:	□		
Registration Retry Interval (s):	30		
Inbound:	□		
Outbound:	off		
Dial timeout:	10		
Expires:	1800		
Authentication:	user defined		
Username:	TAU-32.IP		
Password:	••••••••		
Ringback at answer 183:	□		
Ringback at callwaiting:	180 Ringing		
Remote ringback:	ringback with 183 Progress		
DTMF MIME Type:	application/dtmf-relay		
Hook flash MIME Type:	application/hook-flash		
Escape hash uri:	□		
User=Phone:	□		
Remove inactive media:	□		
P-RTP-Stat:	□		
CT with replaces:	☑		
100rel:	supported		
Enable timer:	☑		
Min SE:	120		
Session expires (0 - unlimited session):	0		
NAT settings:			
NAT Keep Alive Msg:	off		
NAT Keep Alive Interval (s):	30		
Conference settings:			
Conference mode:	Local		
Conference server:	conf		
IMS settings:			
Enable IMS:	□		
XCAP name for three-party conference:	three-party-conference		
XCAP name for hotline:	hot-line-service		
XCAP name for call waiting:	call-waiting		
XCAP name for call hold:	call-hold		



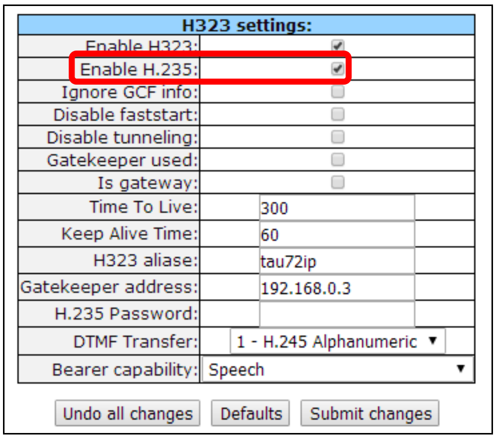
Port 1	
Phone	500000
User name	
Use alt.number	□
Alt.number	222
Authentication name	520000
Authentication password	••••••
Custom	□
Subscriber profile	Profile 1
SIP/H323 profile	Profile 1
Hot line	□
Hot timeout	0
Hot number	700001
CLIR:	□
DND:	□
Stop dial at #:	□
Disabled	□
SIP port	
Process flash	Transmit flash
Call waiting	□

6. 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.



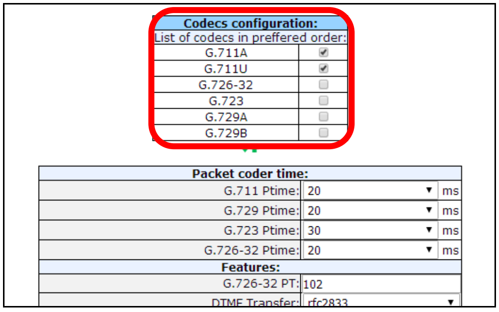
H323 settings:	
Enable H323:	☑
Enable H.235:	□
Ignore GCF info:	□
Disable faststart:	□
Disable tunneling:	□
Gatekeeper used:	□
Is gateway:	□
Time To Live:	300
Keep Alive Time:	60
H323 aliase:	tau72ip
Gatekeeper address:	192.168.0.3
H.235 Password:	
DTMF Transfer:	1 - H.245 Alphanumeric
Bearer capability:	Speech

7. 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.



H323 settings:	
Enable H323:	☑
Enable H.235:	☑
Ignore GCF info:	□
Disable faststart:	□
Disable tunneling:	□
Gatekeeper used:	□
Is gateway:	□
Time To Live:	300
Keep Alive Time:	60
H323 aliase:	tau72ip
Gatekeeper address:	192.168.0.3
H.235 Password:	
DTMF Transfer:	1 - H.245 Alphanumeric ▾
Bearer capability:	Speech ▾

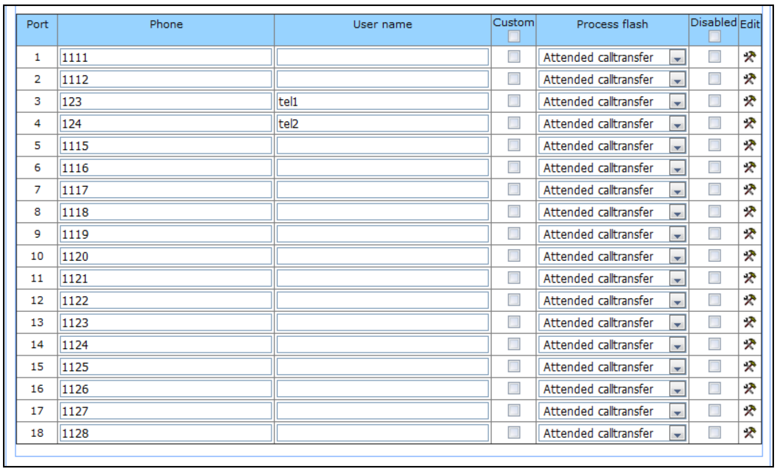
8. In '*PBX -> SIP/H323 Profiles -> Profile **n** -> Codecs*' section, select utilized codecs and define their selection priority. During H.323 protocol operation, all settings should be configured in Profile 1.



Codecs configuration:	
List of codecs in preffered order:	
G.711A	☑
G.711U	☑
G.726-32	□
G.723	□
G.729A	□
G.729B	□

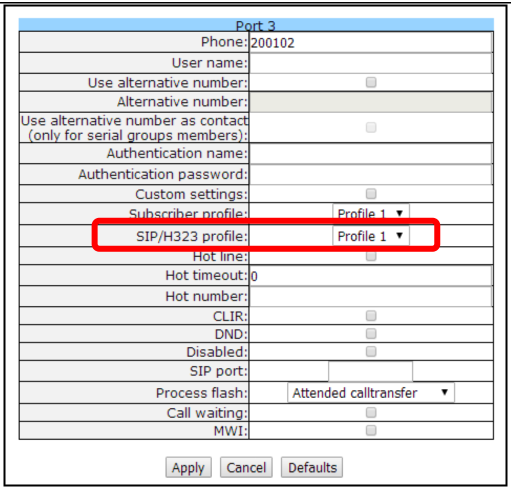
Packet coder time:		
G.711 Ptime:	20 ▾	ms
G.729 Ptime:	20 ▾	ms
G.723 Ptime:	30 ▾	ms
G.726-32 Ptime:	20 ▾	ms
Features:		
G.726-32 PT:	102	
DTMF Transfer:	rfc2833 ▾	

9. In *'PBX -> Ports'* section, assign phone numbers to device ports.



Port	Phone	User name	Custom □	Process flash	Disabled □	Edit
1	1111		□	Attended calltransfer	□	⚒
2	1112		□	Attended calltransfer	□	⚒
3	123	tel1	□	Attended calltransfer	□	⚒
4	124	tel2	□	Attended calltransfer	□	⚒
5	1115		□	Attended calltransfer	□	⚒
6	1116		□	Attended calltransfer	□	⚒
7	1117		□	Attended calltransfer	□	⚒
8	1118		□	Attended calltransfer	□	⚒
9	1119		□	Attended calltransfer	□	⚒
10	1120		□	Attended calltransfer	□	⚒
11	1121		□	Attended calltransfer	□	⚒
12	1122		□	Attended calltransfer	□	⚒
13	1123		□	Attended calltransfer	□	⚒
14	1124		□	Attended calltransfer	□	⚒
15	1125		□	Attended calltransfer	□	⚒
16	1126		□	Attended calltransfer	□	⚒
17	1127		□	Attended calltransfer	□	⚒
18	1128		□	Attended calltransfer	□	⚒

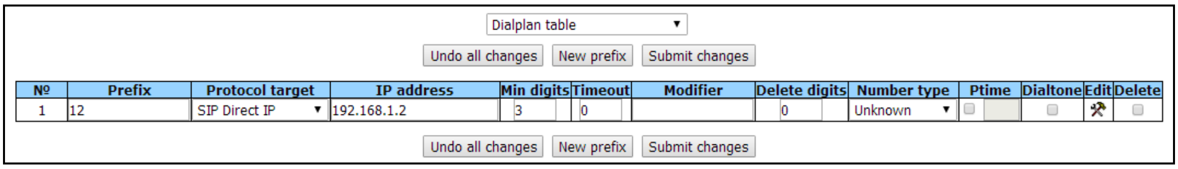
10. In subscriber port settings ('*PBX -> Ports -> Edit -> Custom*'), specify an active SIP profile number in '*SIP/H323 profile*' (by default, Profile 1 is defined for all subscriber ports).



Port 3

Phone:	200102
User name:	
Use alternative number:	□
Alternative number:	
Use alternative number as contact (only for serial groups members):	□
Authentication name:	
Authentication password:	
Custom settings:	□
Subscriber profile:	Profile 1 ▾
SIP/H323 profile:	Profile 1 ▾
Hot line:	□
Hot timeout:	0
Hot number:	
CLIR:	□
DND:	□
Disabled:	□
SIP port:	
Process flash:	Attended calltransfer ▾
Call waiting:	□
MWI:	□

11. 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.



Dialplan table ▾

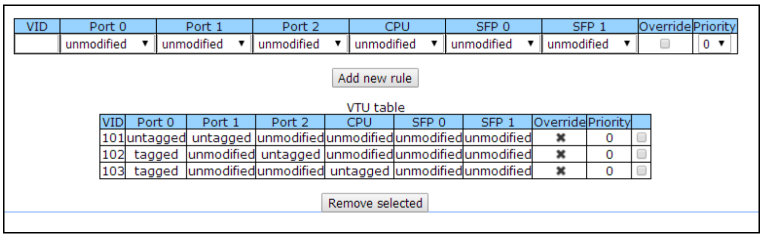
№	Prefix	Protocol target	IP address	Min digits	Timeout	Modifier	Delete digits	Number type	Ptime	Dialtone	Edit	Delete
1	12	SIP Direct IP ▾	192.168.1.2	3	0		0	Unknown ▾	□	□	⚒	□

12. 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 port 1, packets with VLAN ID=102 should be sent tagged to 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—'*VTU table*'—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 (see Section 5.1.3.2).

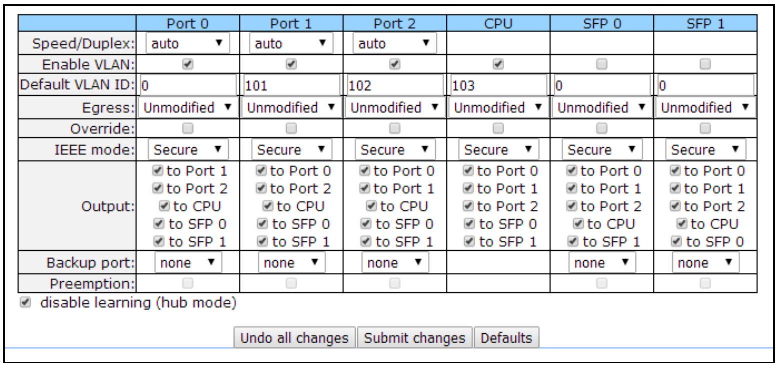


VID	Port 0	Port 1	Port 2	CPU	SFP 0	SFP 1	Override	Priority
	unmodified ▾	unmodified ▾	unmodified ▾	unmodified ▾	unmodified ▾	unmodified ▾	□	0 ▾

VTU table

VID	Port 0	Port 1	Port 2	CPU	SFP 0	SFP 1	Override	Priority	
101	untagged	untagged	unmodified	unmodified	unmodified	unmodified	✖	0	□
102	tagged	unmodified	untagged	unmodified	unmodified	unmodified	✖	0	□
103	tagged	unmodified	unmodified	untagged	unmodified	unmodified	✖	0	□

3. For switch ports, you should configure '*VTU table*' 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, that allow to use 'Default VLAN ID' settings (see Section 5.1.3.1).



	Port 0	Port 1	Port 2	CPU	SFP 0	SFP 1
Speed/Duplex:	auto ▾	auto ▾	auto ▾			
Enable VLAN:	☑	☑	☑	☑	□	□
Default VLAN ID:	0	101	102	103	0	0
Egress:	Unmodified ▾	Unmodified ▾	Unmodified ▾	Unmodified ▾	Unmodified ▾	Unmodified ▾
Override:	□	□	□	□	□	□
IEEE mode:	Secure ▾	Secure ▾	Secure ▾	Secure ▾	Secure ▾	Secure ▾
Output:	☑ to Port 1 ☑ to Port 2 ☑ to CPU ☑ to SFP 0 ☑ to SFP 1	☑ to Port 0 ☑ to Port 2 ☑ to CPU ☑ to SFP 0 ☑ to SFP 1	☑ to Port 0 ☑ to Port 1 ☑ to CPU ☑ to SFP 0 ☑ to SFP 1	☑ to Port 0 ☑ to Port 1 ☑ to Port 2 ☑ to SFP 0 ☑ to SFP 1	☑ to Port 0 ☑ to Port 1 ☑ to Port 2 ☑ to CPU ☑ to SFP 1	☑ to Port 0 ☑ to Port 1 ☑ to Port 2 ☑ to CPU ☑ to SFP 0
Backup port:	none ▾	none ▾	none ▾		none ▾	none ▾
Preemption:	□	□	□		□	□

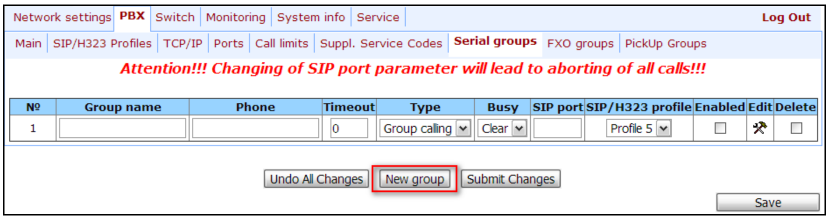
☑ disable learning (hub mode)

4. Click '*Update switch*' button to apply settings. Connect to the device using 103 VLAN and confirm applied settings with *'Commit'* button. After that, modified switch settings could be saved in the non-volatile memory with '*Save*' button.

APPENDIX E. EXAMPLE OF PABX CONFIGURATION WITH TAU-24.IP/TAU-16.IP

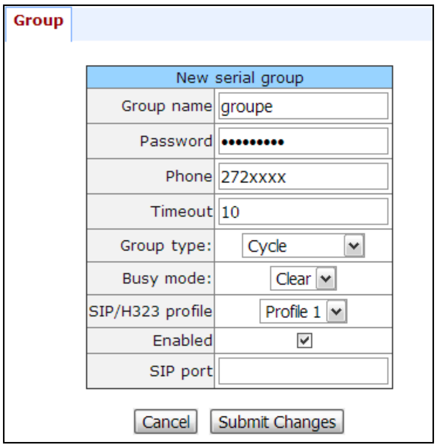
Objective: You have to build PABX with 4 subscriber numbers. A single number is allocated to PABX by a local exchange network—272xxxx. When a call comes to this number, it should be transferred to all 4 x PABX subscriber ports in turns. Ringing time for each number is 10 seconds.

1. Using Ethernet cable, connect gateway Ethernet port to your local area network. Connect to the device using WEB configurator.
2. As a rule, 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:



Attention!!! Changing of SIP port parameter will lead to aborting of all calls!!!

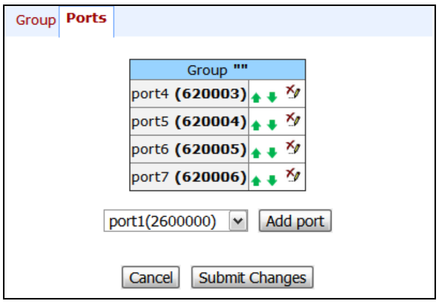
№	Group name	Phone	Timeout	Type	Busy	SIP port	SIP/H323 profile	Enabled	Edit	Delete
1			0	Group calling	Clear		Profile 5	□	⚒	□



New serial group	
Group name	groupe
Password	•••••••••
Phone	272xxxx
Timeout	10
Group type:	Cycle
Busy mode:	Clear
SIP/H323 profile	Profile 1
Enabled	☑
SIP port	

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.

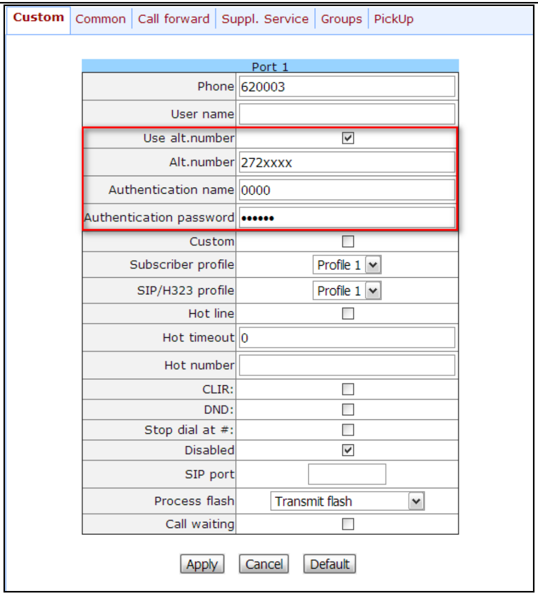
3. In group port settings ('*PBX -> Serial groups -> Edit*'), add ports into a call group (see Section 5.1.2.7).



Group ""
port4 **(620003)**
port5 **(620004)**
port6 **(620005)**
port7 **(620006)**

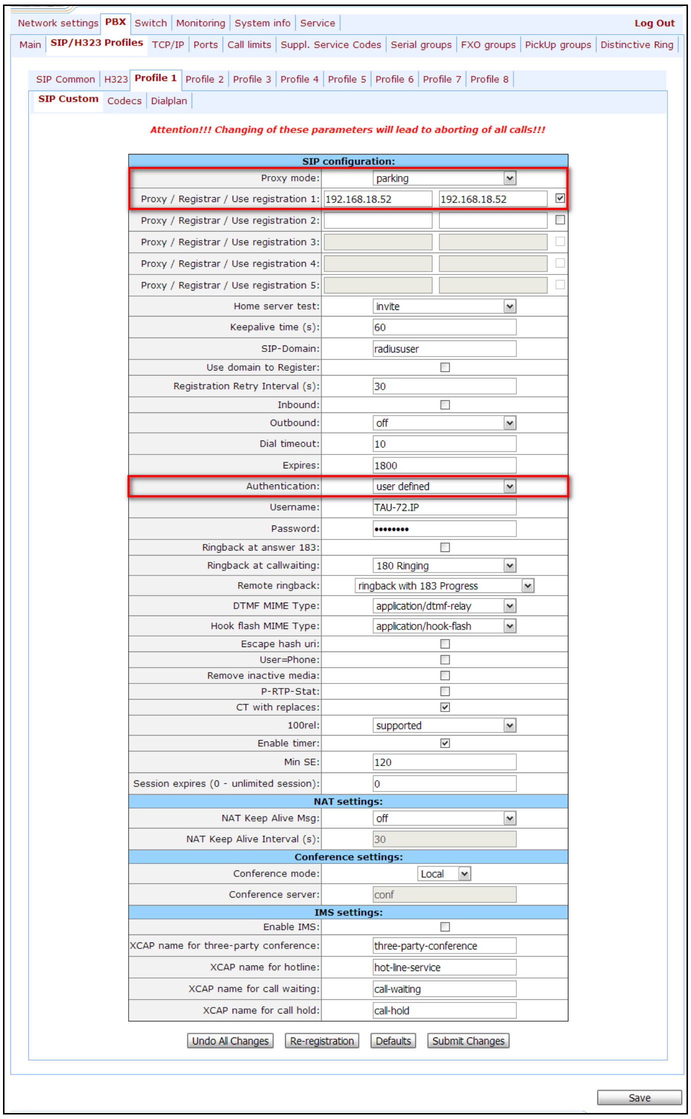
port1(2600000)

4. In subscriber port settings—*PBX -> PORTS -> Edit -> Custom tab*, define the internal subscriber enumeration. 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.



Port 1	
Phone	620003
User name	
Use alt.number	☑
Alt.number	272xxxx
Authentication name	0000
Authentication password	••••••
Custom	☐
Subscriber profile	Profile 1
SIP/H323 profile	Profile 1
Hot line	☐
Hot timeout	0
Hot number	
CLIR:	☐
DND:	☐
Stop dial at #:	☐
Disabled	☑
SIP port	
Process flash	Transmit flash
Call waiting	☐

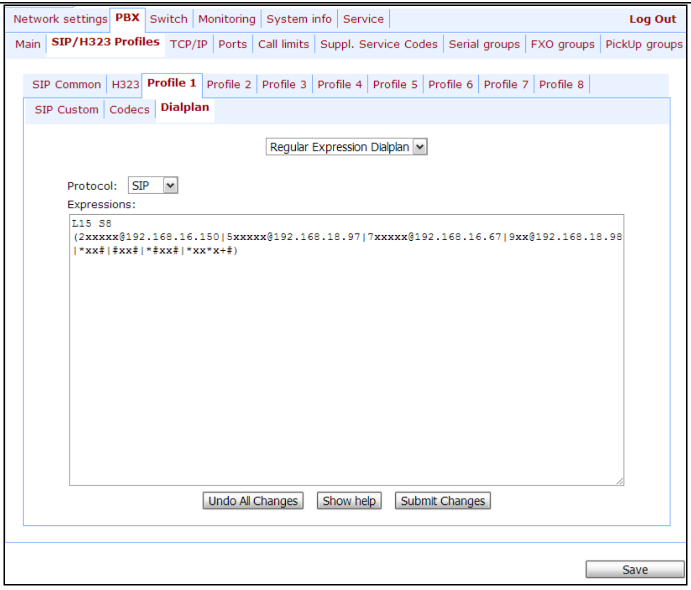
5. Next, configure SIP/H.323 profile assigned to the call group *(PBX -> SIP/H323 Profiles -> Profile n -> SIP Custom).* Define SIP server address and allow registration and authentication on SIP server.



Attention!!! Changing of these parameters will lead to aborting of all calls!!!

SIP configuration:			
Proxy mode:	parking		
Proxy / Registrar / Use registration 1:	192.168.18.52	192.168.18.52	☑
Proxy / Registrar / Use registration 2:			☐
Proxy / Registrar / Use registration 3:			☐
Proxy / Registrar / Use registration 4:			☐
Proxy / Registrar / Use registration 5:			☐
Home server test:	invite		
Keepalive time (s):	60		
SIP-Domain:	radiususer		
Use domain to Register:	☐		
Registration Retry Interval (s):	30		
Inbound:	☐		
Outbound:	off		
Dial timeout:	10		
Expires:	1800		
Authentication:	user defined		
Username:	TAU-72.IP		
Password:	•••••••••		
Ringback at answer 183:	☐		
Ringback at callwaiting:	180 Ringing		
Remote ringback:	ringback with 183 Progress		
DTMF MIME Type:	application/dtmf-relay		
Hook flash MIME Type:	application/hook-flash		
Escape hash uri:	☐		
User=Phone:	☐		
Remove inactive media:	☐		
P-RTP-Stat:	☐		
CT with replaces:	☑		
100rel:	supported		
Enable timer:	☑		
Min SE:	120		
Session expires (0 - unlimited session):	0		
NAT settings:			
NAT Keep Alive Msg:	off		
NAT Keep Alive Interval (s):	30		
Conference settings:			
Conference mode:	Local		
Conference server:	conf		
IMS settings:			
Enable IMS:	☐		
XCAP name for three-party conference:	three-party-conference		
XCAP name for hotline:	hot-line-service		
XCAP name for call waiting:	call-waiting		
XCAP name for call hold:	call-hold		

6. For outgoing calls routing, configure addressed dial peers in the respective SIP/H.323 profile ('PBX -> SIP-H323 Profiles -> Profile n -> Dialplan' menu section).



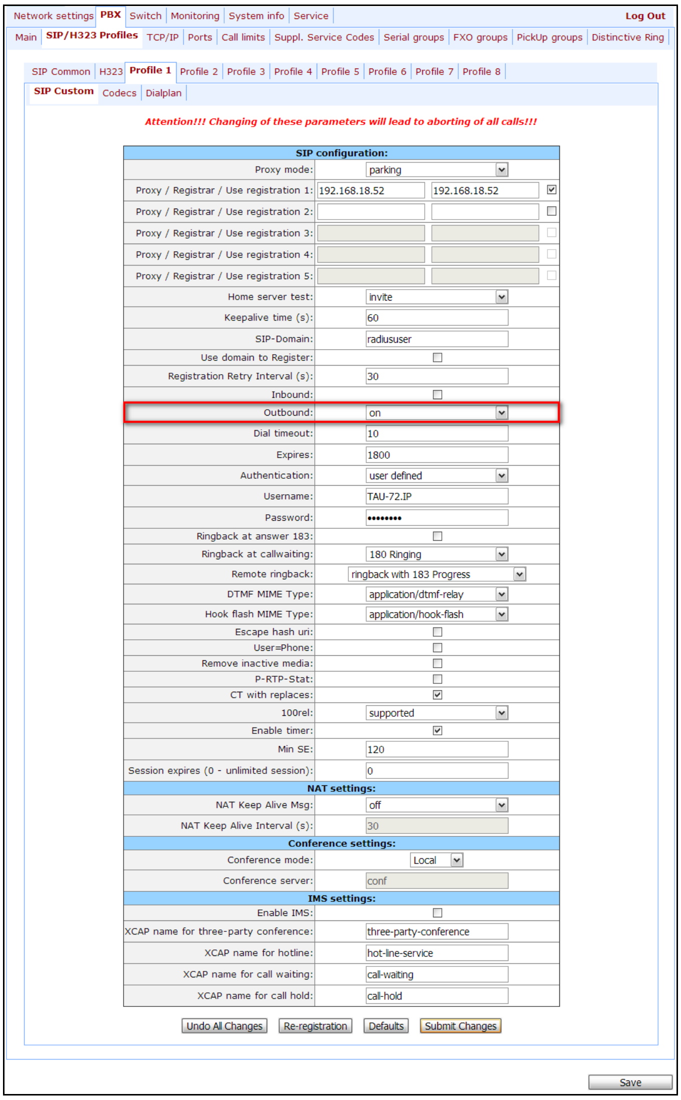
Regular Expression Dialplan

Protocol: SIP

Expressions:

```
L15 S8
(2xxxxx@192.168.16.150|5xxxxx@192.168.18.97|7xxxxx@192.168.16.67|9xx@192.168.18.98
|*xx#|#xx#|*#xx#|*xx*x+#)
```

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.



Attention!!! Changing of these parameters will lead to aborting of all calls!!!

SIP configuration:			
Proxy mode:	parking		
Proxy / Registrar / Use registration 1:	192.168.18.52	192.168.18.52	☑
Proxy / Registrar / Use registration 2:			☐
Proxy / Registrar / Use registration 3:			☐
Proxy / Registrar / Use registration 4:			☐
Proxy / Registrar / Use registration 5:			☐
Home server test:	invite		
Keepalive time (s):	60		
SIP-Domain:	radiususer		
Use domain to Register:	☐		
Registration Retry Interval (s):	30		
Inbound:	☐		
Outbound:	on		
Dial timeout:	10		
Expires:	1800		
Authentication:	user defined		
Username:	TAU-72.IP		
Password:	••••••••		
Ringback at answer 183:	☐		
Ringback at callwaiting:	180 Ringing		
Remote ringback:	ringback with 183 Progress		
DTMF MIME Type:	application/dtmf-relay		
Hook flash MIME Type:	application/hook-flash		
Escape hash uri:	☐		
User=Phone:	☐		
Remove inactive media:	☐		
P-RTP-Stat:	☐		
CT with replaces:	☑		
100rel:	supported		
Enable timer:	☑		
Min SE:	120		
Session expires (0 - unlimited session):	0		
NAT settings:			
NAT Keep Alive Msg:	off		
NAT Keep Alive Interval (s):	30		
Conference settings:			
Conference mode:	Local		
Conference server:	conf		
IMS settings:			
Enable IMS:	☐		
XCAP name for three-party conference:	three-party-conference		
XCAP name for hotline:	hot-line-service		
XCAP name for call waiting:	call-waiting		
XCAP name for call hold:	call-hold		

APPENDIX F. CALCULATION OF PHONE LINE LENGTH

Table 16—Electrical resistance/cable type relationship for 1km of DC subscriber cable lines at 20°C ambient temperature.[1]

Cable grade for subscriber lines of local exchange network	**Core diameter**	**Electrical resistance of 1km circuit, Ω, max.**	**Line length (other phone units), extended range mode enabled, km**	**Line length (other phone units), extended range mode disabled, km**
TPP, TPPep, TPPZ, TPPepZ, TPPB,TPP epB, TPPZB, TPPBG, TPPepBG, TPPBbShp, TPPepBbShp, TPPZBbShp, TPPZepBbShp, TPPt	0.32	458.0	1.638	0.983
	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
	0.64	116.0	6.466	3.879
	0.70	96.0	7.813	4.688
TPV, TPZBG	0.32	458.0	1.638	0.983
	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
	0.64	116.0	6.466	3.879
	0.70	96.0	7.813	4.688
TG, TB, TBG, TK	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
	0.64	116.0	6.466	3.879
	0.70	96.0	7.813	4.688
TStShp, TAShp	0.50	192.0	3.906	2.344
	0.70	96.0	7.813	4.688
TSV	0.40	296.0	2.534	1.520
	0.50	192.0	3.906	2.344
KSPZP	0.64	116.0	6.466	3.879
KSPP, KSPZP, KSPPB, KSPZPB, KSPPt, KSPZPt, KSPZPK	0.90	56.8	13.204	7.923

Phone line length calculation for different types of cable[2]:

1. Cable resistance at 20°C

   Rcab = Lcab*Rsp20;

   where

   Rsp20 [Ω/km] specific DC cable resistance at 20°C, table in Appendix 3.

2. Cable length

   Lcab = Rcab/Rsp20 [km]

3. Loop resistance at 20°C

[1] Line length values for 'Rus' phone unit will be lower than specified in the table.

[2] Calculation is taken from http://izmer-ls.ru/shle.html

Lloop = 2*Lcab
Rloop = Lloop*Rsp20 = 2*Lcab*Rsp20;

Lloop = Rloop/Rsp20.

In case of phone lines, loop resistance includes phone unit resistance: 600Ω

If the extended range mode is enabled, ('Extended range loop' setting, see Section 5.1.2.1), equipment manufactured by Eltex provides maximum loop resistance of 2100Ω. Subsequently, loop resistance excluding the phone unit equals to 1500Ω. Thus, maximum loop length is calculated by the equation:

Lloop = 1500/Rsp20 [km].

4. Line length is calculated by the equation:

Lline = Lcab = Lloop/2 = 1500/(2*Rsp20) = 750/Rsp20 [km].

5. If you have to consider the cable temperature, the cable line length will be calculated with an adjustment:

Lline = 750/(Rsp20*(1-a*(T-20)))

where

a—is a temperature factor (table value)

T—cable temperature

'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.

TAU automatic configuration and configuration file version check operation algorithm

For each TAU, a reference configuration file is created; in **/etc/config/cfg.yaml** configuration file, specify its current version #ConfigFileVersion=YYYYMMDDHHMM:

```
#!version 1.0
#tau-24 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: tau24
```

During TAU 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, 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 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. After restart, TAU 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.

Fig. 17 shows TAU automatic configuration and configuration file version check operation algorithm.

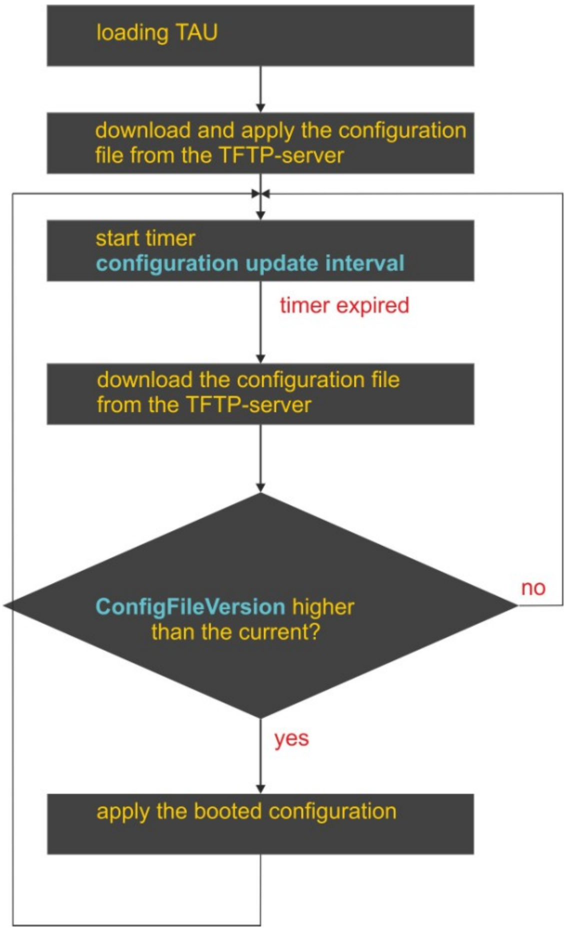

loading TAU
download and apply the configuration file from the TFTP-server
start timer
configuration update interval
timer expired
download the configuration file from the TFTP-server
ConfigFileVersion higher than the current?
no
yes
apply the booted configuration

Fig. 17—TAU automatic configuration and configuration file version check operation algorithm

Autoupdate and firmware version check operation algorithm

During TAU startup, and upon the expiry of *'Firmware update interval'* timeout, the gateway checks for the version description file (tau.versions) at the specified path on TFTP server. If the configuration file is present, TAU 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 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.

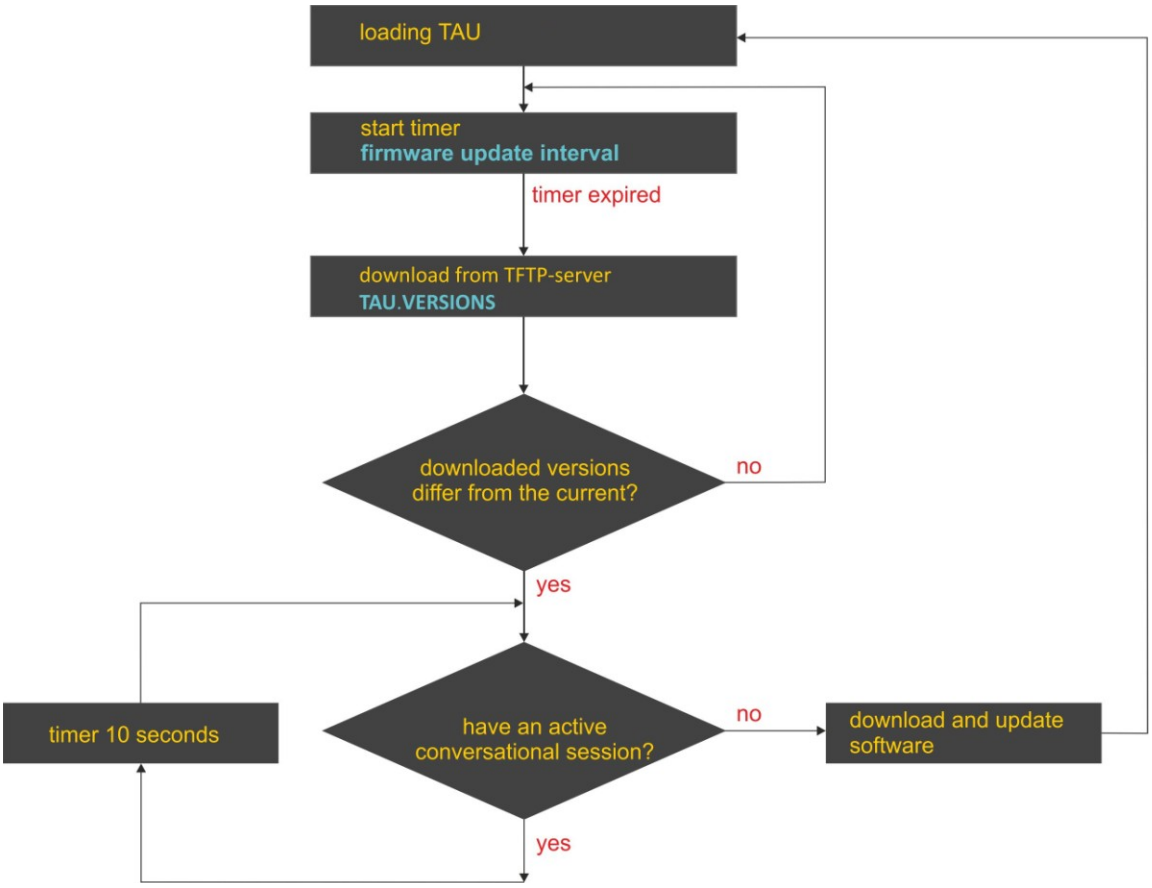


Fig. 18—Autoupdate and firmware version check operation algorithm

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	***Tau24_<MAC>.dat***

Tau24_<MAC>.dat—configuration file name When such name is received, gateway substitutes **<MAC>** with its own MAC address.
Example: Example: Transferred name of a configuration file is tau24_<MAC>.dat. When this name is received, the gateway generates availability request for tau24_ A8F94B887D27.dat file on TFTP server.

Configuration file is downloaded to PC via WEB interface in tau24_cfg.tar.gz format; to use it in autoconfiguration procedure, rename it to tau24_<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 tau24_<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. If Option 43 is missing, Options 66 and 67 will be processed. 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:6B:6D:67
```

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.img).

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/tau24_<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 “/tau24ip/firmware/tau.versions;/tau24ip/conf/tau24_<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.

tau.versions file 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:

- FS—file system with working application [1].
- CSP—gateway operating system[1].
- MSP—media processor software[1].
- *IMG*—complete software image, includes FS, CSP, MSP, and ARM.
- ARM—platform software[1].

Software file name format:

- *filenameFS*—tau24.fs.{software version number}.
- *filenameCSP*—tau24.csp.{software version number}.
- *filenameMSP*—tau24.msp.{software version number}.
- *filenameIMG*—tau24.img.{software version number}.
- *filenameARM*—tau24.arm.{software version number}.

tau.versions file contents example:

```
FS=1.8.0 fs/tau24.fs.1.8.0
CSP=209 csp/tau24.csp.209
MSP=GA_10_23_02_03 msp/tau24.msp. GA_10_23_02_03
IMG=2.1.0 tau24ip/firmware/img/tau24.img.2.1.0
ARM=20111117 arm/tau24.arm.20111117
```

[1] Not used in the current firmware version.

APPENDIX H. DEVICE FIREWALL CONFIGURATION—IPTABLES

Table 17—Device firewall configuration commands

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
   ```

   r) view all tables:

   ```
   iptables -L
   ```

6. Save created rules with **`'iptables-save'`** command.

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 K. DESCRIPTION EVENTS SENT TO THE MESSAGE TRAP, TRAP V2, INFORM

1. The format of the values used in the messages Trap, Trap V2, Inform

The format of the transmitted values consists of two parts:% $ X and Y, where X% - the number parameter according to the structure of the ladder, Y $ - type output value.

The structure of information transmitted in messages Trap, Trap V2, Inform

Name	OID	Description
mcTrapExState	1.3.6.1.4.1.35265.3.5.1	Condition
mcTrapLParam1	1.3.6.1.4.1.35265.3.5.2	Parameter 1
mcTrapLParam2	1.3.6.1.4.1.35265.3.5.3	Parameter 2
mcTrapLParam3	1.3.6.1.4.1.35265.3.5.4	Parameter 3
mcTrapID	1.3.6.1.4.1.35265.3.5.5	Identifier
mcTrapDescr	1.3.6.1.4.1.35265.3.5.6	Description
mcTrapRestoredAlarmID	1.3.6.1.4.1.35265.3.5.7	If this event recovery, whereas here the identifier of the accident. If this is an emergency event, then here it is transmitted to 0.
mcTrapSyncType	1.3.6.1.4.1.35265.3.5.8	Type: 0 - Normal; 1 - inactive accident; 2 - active accident
mcReservedFlag	1.3.6.1.4.1.35265.3.5.9	Reserve

The value of variable% x contained in the description of the alarm corresponds to the structure of the following descriptions:
%1 –param1
%2 –param2
%3 –param3
%5 –description

Value Types of $Y:
$d – integer
$s – string

2. Description of the messages transmitted TAU

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	Option 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	Option 1: voltage Option 2: the number of the inductor (1 or 2)
fxs72TemperatureAlarmTrap	MAJOR	The temperature sensor% 2 $ d =% 1 $ d greater than the maximum value (90°C)	1.3.6.1.4.1.35265.3.6.3	Option 1: The temperature Option 2: The number of the temperature sensor (1-4)
fxs72FanAlarmTrap	MAJOR	Fan% 1 $ d is on, but does not rotate	1.3.6.1.4.1.35265.3.6.4	Option 1: The number of fan
fxs72SSwAlarmTrap	MAJOR	No registration on the 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	Option 1: The port number
fxs72VbatOkTrap	CLEAR	The voltage Vbat OK	1.3.6.1.4.1.35265.3.7.1	
fxs72VringOkTrap	CLEAR	The voltage Vring% 2 $ d OK	1.3.6.1.4.1.35265.3.7.2	Option 2: the number of the inductor (1 or 2)
fxs72TemperatureOkTrap	CLEAR	The temperature sensor% 2 $ d OK	1.3.6.1.4.1.35265.3.7.3	Option 2: The number of the temperature sensor (1-4)
fxs72FanOkTrap	CLEAR	Fan% 1 $ d is operating normally	1.3.6.1.4.1.35265.3.7.4	Option 1: The number of fan
fxs72SSwOkTrap	CLEAR	There is a registration MGC/SSW	1.3.6.1.4.1.35265.3.7.5	It is used for software version - Megaco
fxs72PortOkTrap	CLEAR	Port% 1 $ per unlocked	1.3.6.1.4.1.35265.3.7.6	Option 1: The port number
fxs72VmodeSwitchTrap	INFO	Diet changed -% 1 $ a in	1.3.6.1.4.1.35265.3.7.10	Option 1: the new regime: 1 - 60 V 2 – 48 V
fxs72FansSwitchTrap	INFO	Fan status changed	1.3.6.1.4.1.35265.3.7.11	Option 1: 0 - included 1 - included
fxs72updateFwFail	MINOR	Error while updating software	1.3.6.1.4.1.35265.3.6.20	Option 1: The type of error
fxs72updateFwOk	INFO	Updated Software	1.3.6.1.4.1.35265.3.7.20	
fxs72BpuAlarmTrap	CRITICAL	No communication with the BPU	1.3.6.1.4.1.35265.3.6.12	
fxs72BpuOkTrap	CLEAR	Contact Bending restored	1.3.6.1.4.1.35265.3.7.12	

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) Novosibirsk NOVT-6 Asia/Novosibirsk
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) 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+12) Anadyr ANAT-12 Asia/Anadyr
New Zealand (UTC+12) Auckland, Wellington NZST-12NZDT,M10.1.0,M3.3.0/3 Pacific/Auckland

Tonga (UTC+13) Nuku'alofa TOT-13 Tonga/Nuku'alofa

Kiribati (UTC+14) Caroline Island LINT-14 Kiribati/Caroline Island

TECHNICAL SUPPORT

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

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

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

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