VoIP Gateways

TAU-4.IP, TAU-8.IP, TAU-8.IP-W

Operation Manual

User name: **admin**

Password: **password**

Document version	Release date	Revisions
Version 1.18	01.12.2020	Updated according to firmware version 2.6.5 Changed: Unique OIDs for TAU-4.IP and TAU-8.IP
Version 1.17	28.08.2019	Updated according to firmware version 2.6.3 Added: 3.3.4 The PCAP Traces submenu Changed: 3.3 The Traces menu
Version 1.16	27.06.2019	Updated according to firmware version 2.6.2 Added: – CPC (Calling Party Control) Fixed: – TR-069 client crashes and restarts – Problems with setting parameters through TR-069 – Problems of using DNS servers received via DHCP in the 'Internet' and 'IP telephony' services – VoIP crashes – Memory leaks when requesting a parameter tree via TR-069 – Hang up the call with the cause 'Internal media error' when changing the 'Owner/Creator' field in SDP
Version 1.15	07.12.2018	Updated according to firmware version 2.6.0 Changed: 2.1 Configuration procedure. Administrator Access 2.1.1.2 The WEB Authentication submenu 2.1.1.5 The Upgrade submenu 2.1.1.7 The Network submenu, the Internet service 2.1.3.4 The Line acoustic signals submenu 2.1.3.2 The QoS submenu 2.1.3.3 The FXS submenu 2.1.3.4 The Line acoustic signals submenu 3.2.8 The VoIP submenu APPENDIX C. THE USE OF COMMAND LINE INTERFACE (CLI) FOR CONFIGURATION AND MONITORING
Version 1.14	10.07.18	Updated according to firmware version 2.5.0 Changed: 2.1.1.1 The Settings submenu 2.1.1.2 The WEB Authentication submenu 2.1.1.6 The Network settings submenu 2.1.4.2 The Firewall Rules submenu APPENDIX C. THE USE OF COMMAND LINE INTERFACE (CLI) FOR CONFIGURATION AND MONITORING
Version 1.13	12.03.2018	Added: – DHCP Relay (option 82)
Version 1.12	01.11.2017	Added: – The possibility to specify the name of FXS profile; – The possibility to specify the second DNS. Fixed: – Displaying the DNS received from DHCP.
Version 1.11	23.03.2017	Added: – the possibility to transfer # - symbol without coding; – option of PTE autonegotiation
Version 1.10	14.02.2017	Added: – support for 726 codecs; – TAU-4.IP support. Fixed: – TR-069. Updating firmware and configuration via ACS; – obtaining gateway from DHCP by default.
Version 1.9	22.06.2016	Added: – MAC-address filtering; – Automatic control of signal amplification; – support for profiles for different call directions; – Echo suppression; – Copy of codec settings for each call; – Adaptive jitter buffer;

		– Uploading the user pitches for analogue lines; – T1 and T2 timers settings for SIP; – Anonymous call support; – TR-069. New parameters are added. Fixed: – Timezone for Yekaterinburg; – Minimum time for detection of disconnection is decreased up to 200 ms; – Voice menu playing interrupting.
Version 1.8	11.08.2015	Added: – Wizard is implemented; – Voice menu is implemented; – Method for address getting of the default configuration from Static to DHCP is changed; – Improved operation with FXS-profiles by using custom-settings; – Corrected VoIP operation with secondary DNS-servers; – Corrected problem of blocking a gateway operation when FXS-port is defected; – TR-069. Operation process with Set/Get Parameter Attributes is corrected; – Opportunity to use regular expressions is added for call signal setting.
Version 1.7	27.05.2015	Added: – Display system information on the 'Information/System' page; – Access port settings via FTP protocol. Fixed: – Operation of the series selection groups by using STUN; – Problem of configuration upload; – VoIP operation is corrected for 3G/4G changeover; – Ringback tone problem during a call to a call group or a serial selection group; – vlan_priority configuration problem; – problem of traceroute information unloading; – Problem of VoIP application high-overload; – Problem of setting reset for print- server after rebooting a gateway.
Version 1.6	01.10.2014	Added: – Settings of day-light saving time are added into NTP; – Order of autoconfiguration settings is changed via DHCP; – The following options are added in the SIP-profile settings: – Process Alert-Info header; – Check only username in RURI; – Periodically polling a SIP-server; – Upgraded ring cadence; – Configuration speed/duplex.
Version 1.5	23.01.2014	Added: – Configuration of the device access ports; – NAT setting for TR-069; – SIP-server reservation setting; – Session time settings; – IMS settings; – Support of two mode of three-way conference; – line polarity reversal;
Version 1.4	21.05.2013	Added: – encryption based on IPSec technology; – Configuration serial selection groups.
Version 1.3	31.01.2013	Added: – Autoconfiguration via DHCP; – Setup of the VoIP logging; – Setup of IGMP logging; – Specific menu to set up SIP profiles; – Specific menu to set up FXS profiles.
Version 1.2	09.02.2012	Added: – Call history, setup of a history log; – Call groups monitoring; – Setup of Caller ID type; – Local call transfer;

		– Setup of the primary network for PPPoE.
Version 1.1	09.12.2011	Added: – Call groups settings; – Web-interface language selection (Russian/English);
Version 1.0	02.06.2011	First issue
Current firmware version: 2.6.5		

SYMBOLS

Symbol	Description
Bold font face	Notes, warnings, section headings, titles and table titles are written in bold.
Calibri Italic	Important information is written in Calibri Italic
	Analogue phone
	SIP server
	TAU-4/8.IP customer gateway
	Computer
	Digital set-top box (STB)
	Network connection
	Wireless network

NOTES AND WARNINGS

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

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

CONTENTS

INTRODUCTION 8
1 PRODUCT DESCRIPTION 9
1.1 Purpose 9
1.2 Design 9
1.3 Device specification 9
1.4 Product design and operating principle 12
1.5 Main specifications 14
1.6 Design 16
1.6.1 Front panel of the device 16
1.6.2 Back panel of the device 16
1.7 Light indication 17
1.8 Reset the device to the factory settings 18
1.9 Delivery Package 18
2 DEVICE CONFIGURATION VIA WEB-INTERFACE. ADMINISTRATOR ACCESS 19
2.1 The 'System' menu 21
2.1.1 The 'Settings' submenu 22
2.1.2 The 'WEB Authentication' submenu 23
2.1.3 The 'Autoprovisioning' submenu 25
2.1.4 The 'Configuration' submenu 28
2.1.5 The 'Upgrade' submenu 29
2.2 The 'Network' menu 29
2.2.1 The 'Network settings' submenu 29
2.2.2 The 'IPSec' submenu 41
2.2.3 The 'Hosts' submenu 49
2.2.4 The 'Static routes' submenu 51
2.2.5 The 'SNMP' submenu 53
2.3 The 'Print Server' menu 54
2.4 The 'PBX' menu 55
2.4.1 The 'SIP' submenu 55
2.4.3 The 'FXS' submenu 75
2.4.4 The 'Line acoustic signals' submenu 83
2.4.5 The 'Hunt groups' submenu 86
2.4.6 The 'Pickup groups' submenu 88
2.4.7 The 'Serial groups' submenu 89
2.4.8 The 'Subscriber service control' submenu 91
2.4.9 The 'Cadence' submenu 92
2.4.10 The 'Call History' submenu 93
2.5 The 'Security' submenu 93
2.5.1 The 'General' submenu 93
2.5.2 The 'Firewall Rules' submenu 94
2.5.3 The 'MAC filter' submenu 96
3 DEVICE MONITORING VIA WEB-INTERFACE. ADMINISTRATOR ACCESS 98
3.1 The 'Info' menu 98
3.1.1 The 'System' submenu 98
3.1.2 The 'USB' submenu 99
3.2 The 'Status' menu 99
3.2.1 The 'System' submenu 99
3.2.2 The 'Processes' submenu 100
3.2.3 The 'Interfaces' submenu 101
3.2.4 The 'WLAN' submenu 102
3.2.5 The 'Netstat' submenu 103
3.2.6 The 'IPtables' submenu 104

3.2.7 The ‘Diagnostic’ submenu 105
3.2.8 The ‘VoIP’ submenu 105
3.2.9 The ‘Call History’ submenu 109
3.3 The ‘Traces’ menu 113
3.3.1 The ‘Syslog Settings’ submenu 113
3.3.2 The ‘Syslog’ submenu 114
3.3.3 The ‘Kernel’ submenu 115
3.3.4 The ‘PCAP Traces’ submenu 115
3.4 The ‘Reboot’ menu 117
4 VALUE ADDED SERVICES 118
4.1 Call transfer 118
4.2 Call Waiting 120
4.3 Three-way conference call 121
4.3.1 Local conference 121
4.3.2 Remote conference 122
5 DHCP AUTOPROVISIONING OPERATION ALGORITHM 124
APPENDIX A. THE USE OF VOICE MENU FOR GATEWAY SETTINGS 127
APPENDIX B. THE USE OF WIZARD MENU 128
APPENDIX C. THE USE OF COMMAND LINE INTERFACE (CLI) FOR CONFIGURATION AND MONITORING 131
Basic commands 148
Configuration level commands 164
Network settings level commands 167
Port and port profiles settings level commands 175
SIP profiles configuration level commands 181

INTRODUCTION

Today, VoIP is one of the most rapidly evolving telecommunication services. *TAU-4.IP* and *TAU-8.IP* series gateways (hereinafter the “devices”) are designed to provide VoIP services to the network subscribers. The devices are produced in various modifications. They differ in a set of interfaces and functionality.

VoIP subscriber gateways *TAU-4.IP* and *TAU-8.IP* allow connecting up to 4 or 8 analogue phones to packet-based data networks accessible via Ethernet interfaces.

The devices target home users and small offices. They are a perfect solution to provide sparsely populated areas with telephony.

This operation manual describes intended use, main specifications and rules of configuring, monitoring and updating of VoIP customer gateways *TAU-4.IP* and *TAU-8.IP*.

1 PRODUCT DESCRIPTION

1.1 Purpose

TAU-4.IP and *TAU-8.IP* are the high-performance VoIP customer gateways with the full set of options allowing consumers to use VoIP advantages.

The devices are designed to connect analogue phones and fax-modems to the IP network.

The devices and connection wires for subscriber device connection are specified for unmanned day-and-night service in close heated spaces with ambient temperature from +5° to +40°C and relative humidity from 20% to 80%. The devices do not include built-in protection of subscriber terminals from voltage and current overloads.

220 V external adapter provides power supply.

1.2 Design

There are three types of the device design that differ in the set of interfaces and functionality (see Table 1).

Table 1 – Models

Model name	Presence of WAN Interface	Number of FXS ports	Presence of Wi-Fi
TAU-4.IP	+	4	-
TAU-8.IP	+	8	-
TAU-8.IP-W	+	8	+

TAU-8.IP-W devices have a built-in Wi-Fi adapter capable to connect up to 2 external antennas. The built-in Wi-Fi adapter supports 802.11n technology that allows providing data transmission service via the wireless network with QoS higher than for devices supporting 802.11g and 802.11b. In addition, the device remains backward compatible with 802.11g and 802.11b devices.

1.3 Device specification

Device is equipped with the following interfaces:

4×RJ-11 ports to connect analogue phones (TAU-4.IP);
8×RJ-11 ports to connect analogue phones (TAU-8.IP);
1 Ethernet RJ-45 10/100BASE-T WAN port;
WLAN 802.11n[1];
USB2.0 port to connect storage devices, USB-modem or printer.

[1] Only for TAU-8.IP-W

The gateway is powered via an external 12V DC adapter at 220V.

The device supports the following functions:

- Network functions:
  - *PPPoE support (PAP, CHAP, MSCHAP authorization, PPPoE compression[2]);*
  - *PPTP/L2TP support;*
  - *Static address support and DHCP (DHCP-client on WAN);*
  - *DNS support;*
  - *NAT support;*
  - *NTP support;*
  - *SNMP support;*
  - *QoS mechanisms support;*
- VoIP protocols: SIP
- ToS for RTP packets, SIP;
- echo cancellation (G.164 and G.165 guidelines);
- silence detector (VAD);
- Comfort noise generation;
- DTMF signals detection and generation;
- DTMF transmission (INBAND, rfc2833, SIP INFO);
- Fax transmission:
  - *G.711a, G.711u;*
  - *upspeed/pass-through;*
  - *T.38.*
- Operation with several SIP servers;

[2] Not available in the current version

- Value Added Services (VAS):
  - *Call Hold;*
  - *Call Transfer;*
  - *Call Waiting;*
  - *Call Forward Busy;*
  - *Call Forward No Answer;*
  - *Call Forward Unconditional;*
  - *DND (Do not disturb);*
  - *Call Pickup;*
  - *Caller ID: V.23, Bell202, DTMF, Russian Caller ID;*
  - *Hotline;*
  - *CLIR – caller ID service restriction. 'AntiAON' service;*
  - *Value added service control via phone;*
  - *Conference call.*
- Firmware update via web-interface
- Remote monitoring, configuration and setup: Web interface, Telnet, FTP, SSH, SNMP, TR-069;
- Express setting menu;
- Voice menu support;
- Support for MAC address filtering;
- Support for automatic gain control on analogue lines;
- Support for profiles for different call directions;
- Loading user pitches for analogue lines.

Figure 1 shows application diagram of the equipment via TAU-8.IP-W example.

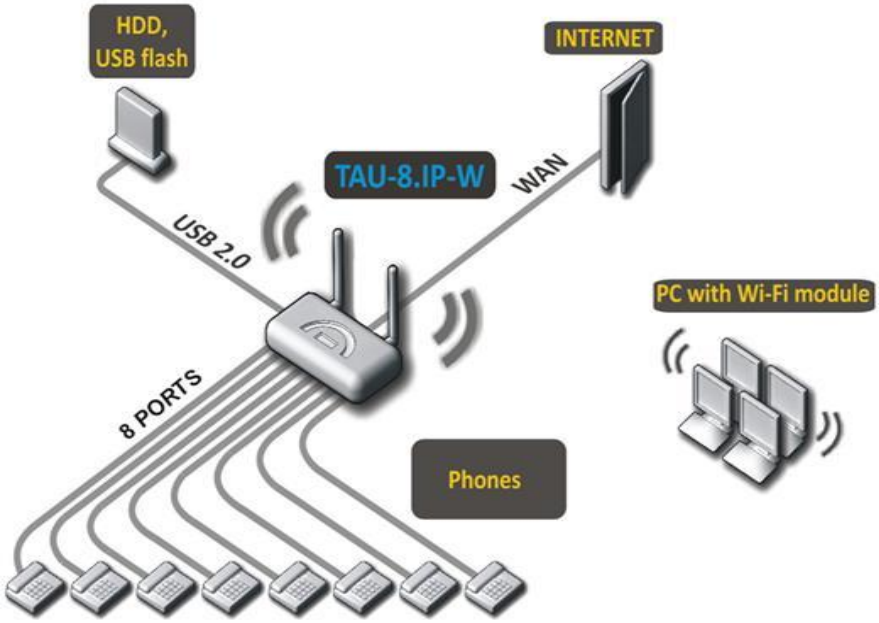


Fig. 1 – TAU-8.IP-W Functional diagram

1.4 Product design and operating principle

TAU-4.IP/TAU-8.IP/TAU-8.IP-W subscriber terminal consists of the following subsystems:

- Controller featuring:
  - Mindspeed digital signal processor;
  - flash memory – 32MB;
  - SDRAM – 256MB;
- SLIC subscriber unit module (4 or 8 FXS ports);
- Ethernet-module RJ-45 10/100BASE-T WAN;
- Wi-Fi adapter (only for TAU-8.IP-W);
- USB-module.

Fig. 2 shows the device architecture diagram.

TAU-4.IP and TAU-8.IP architecture diagrams differ by the number of ports and presence of Wi-Fi module in the TAU-8.IP-W.

The device runs under Linux operating system. Mindspeed digital signal processor performs basic control functions. It enables IP-packets routing, IP-telephony operation, group traffic proxying etc.

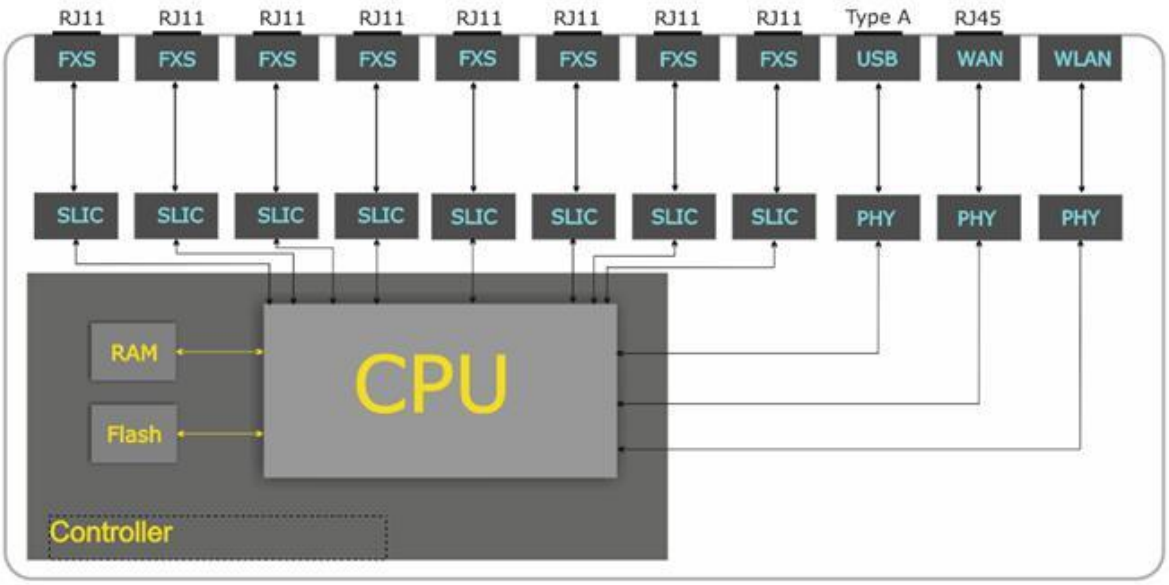


Figure 2 – TAU-8.IP structure diagram

The device may be functionally divided into four blocks:

- Device network features block;
- VoIP block;
- Multicast traffic processing block;
- Control block (Linux operating system).

Device network features block enables IP packet passing and switching according to the device routing table. Depending on the network interface, this block can process both tagged and untagged packets. Supports DHCP, PPPoE, PPTP.

VoIP block enables SIP operation for transmission of voice signals through the network that features packet switching. The subscriber's voice signal is transferred to the SLIC subscriber unit module, where it is converted into digital form. The digitized signal is transferred to VoIP block to be encoded using one of the selected standards and is transferred further in the form of digital packets to the controller via the intrasystem backbone. In addition to voice signals, digital packets contain control and interaction signals.

Multicast traffic processing block is designed to process multicast traffic with the aim of VoIP function support.

Control block based on Linux operating system monitors operation of all the other blocks and subsystems and manages their interaction.

Figure 3 shows TAU-8.IP functional diagram.

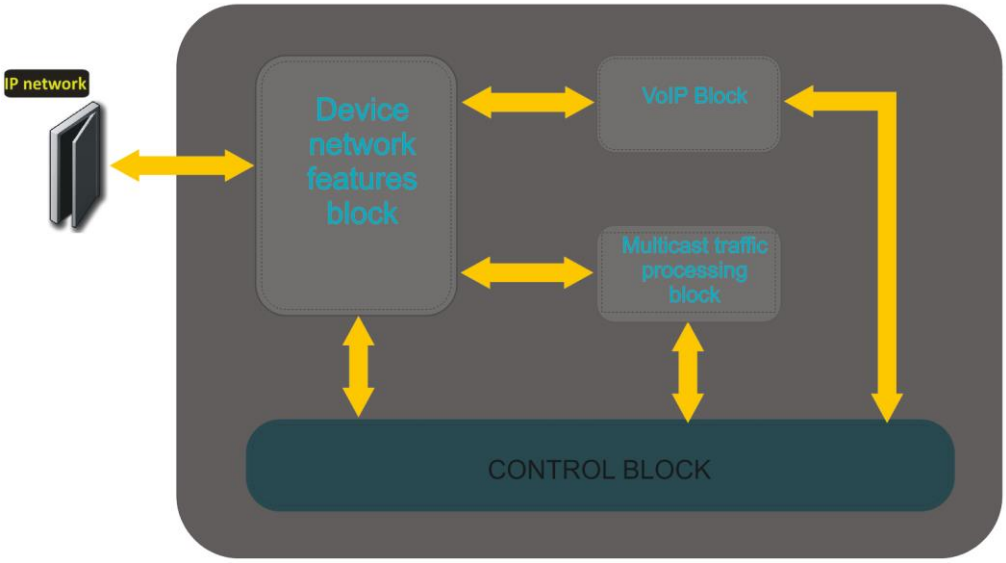


Figure 3 - TAU-8.IP functional diagram

1.5 Main specifications

Table 2 shows main specifications of the device:

Table 2 — Main specifications

VoIP protocols		
Supported protocols		SIP
Fax support		T.38 Real-Time Fax pass-thru (G.711A/U)
Modem support		V.152
Voice standards		VAD AEC (echo cancellation, G.165 recommendation) CNG (comfort noise generator)
Audio codecs		
Codecs		G.729, annex A, annex B G.726 G.711a, G.711u G.723 Fax transmission: G.711a, G.711u, T.38 Modem transmission: G.711a, G.711u
Ethernet WAN interface specifications:		
Number of ports		1
Electric port		RJ-45;
Data rate, Mbps		autodetection, 10/100 Mbps, duplex/half-duplex
Supported standards		10BASE-T/100BASE-TX
Analogue user port specifications		
Number of ports	TAU-4.IP	4
	TAU-8.IP/TAU-8.IP-W	8
Loop resistance		up to 1.5 kΩ
Dialling		pulse/frequency (DTMF)
Caller ID display		FSK V23,FSK Bell202, DTMF

Wireless interface parameters[3]		
Standards		802.11 b/g/n
Frequency range, MHz		2400 ~ 2483,5
Modulation		BPSK, QPSK, 16 QAM, 64 QAM, DBPSK, DQPSK, CCK
Data transfer rate, Mbps		**802.11b(CCK):** 1, 2, 5.5 ,11 **802.11g(OFDM):** 6, 9, 12 , 18, 24, 36, 48, 54 **811n (HT20, 800ns GI):** 130, 117, 104, 78, 52, 39, 26, 13 **802.11n (HT40, 400ns GI):** 300, 270, 240, 180, 120, 90, 60, 30 **802.11n (HT40, 800ns GI):** 270, 243, 216, 162, 108, 81, 54, 27
Maximum transmitter output power		**802.11b:** 16 dBm **802.11g:** 11dBm **802.11n(20MHz MCS0/8):** 19 dBm **802.11n(20MHz MCS7/15):** 12 dBm **802.11n(40MHz MCS0/8):** 19 dBm **802.11n(40MHz MCS7/15):** 11 dBm
Receiver sensitivity		**802.11b:** -83 dBm **802.11g:** -70 dBm **802.11n(20MHz MCS7):** -67 dBm **802.11n(20MHz MCS15):** -66 dBm **802.11n(40MHz MCS7):** -65 dBm
Data protection		64/128/152-bit WEP data encryption; WEP, TKIP and AES
Control		
Remote control		Web interface, Telnet, SSH, SNMP, TR-069
Access restriction		password
General parameters		
Power supply		12V DC power adapter
Power consumption	TAU-4.IP	max 11 W
	TAU-8.IP	max 16 W
	TAU-8.IP-W	max 16.5 W
Operation temperature range		from +5 to +40°C
Relative humidity at 25°C		up to 80%
Dimensions		218x49x220 mm
Weight		up to 0.3 kg

[3] For TAU-8.IP-W only

1.6 Design

TAU-4.IP and TAU-8.IP subscriber terminals are enclosed into 218x49x120 mm plastic housing.

1.6.1 Front panel of the device

The front panel of device is shown in Fig. 4.

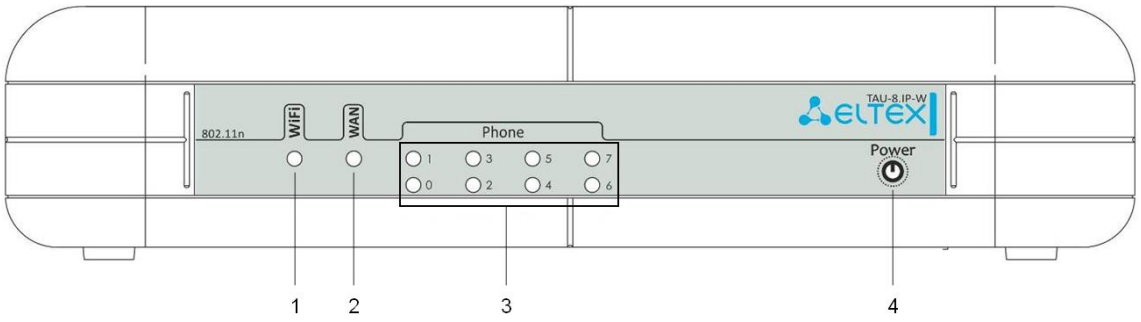


Fig. 4 - TAU-8.IP-W front panel

LEDs and controls located on the front panel are listed in Table 3.

Table 3 – Description of LEDs and controls located on the front panel

Rear panel element		Description
1	WiFi[4]	Operation indicator for wireless network
2	WAN	WAN interface indicator
3	Phone	Analogue phone indicator
4	Power	Device power and activity status indicator

1.6.2 Back panel of the device

The back panel layout of the device is shown in Figure 5.

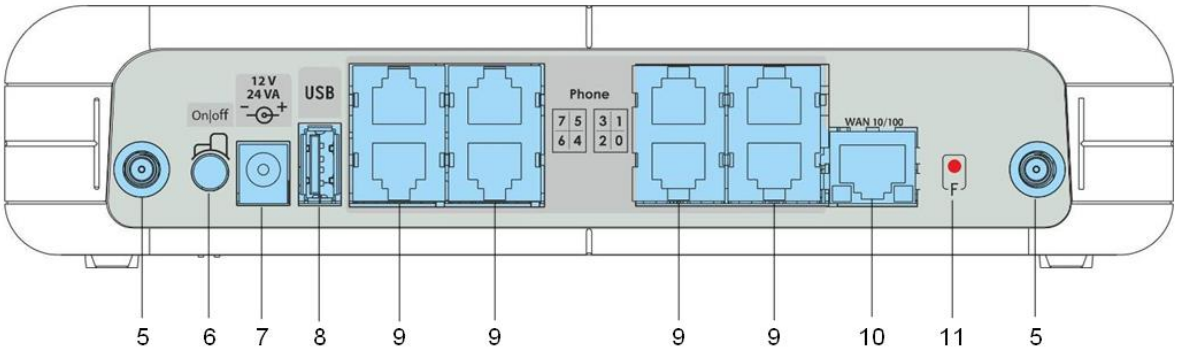


Fig. 5 - TAU-8.IP-W back panel appearance

[4] For TAU-8.IP-W only

The following connectors and controls are located on the back panel (Table 4).

Table 4 – Description of the connectors and controls on the back panel

Rear panel element		Description
5		Connector for Wi-Fi-antennas connection[5]
6	On/Off	ON/OFF switch
7	12V	Power adapter connector
8	USB	USB connector for external memory connection
9	Phone	8×RJ-11 connectors for analogue phone connection
10	WAN	10/100BASE-T port, 100BASE-TX (RJ-45 connector) for connection to external network (WAN)
11	F	A functional key to reboot the device and reset it to factory settings

1.7 Light indication

Wi-Fi, **WAN, Phone** and **Power** LEDs display current state of the device located on the front panel.

Status list of indicators is shown in Table 5 and 6.

Table 5 – Light indication of the device

LED	LED state	Device state
Wi-Fi[6]	solid green	Wi-Fi network is active
	flashes	transmitting data via Wi-Fi
WAN	solid green (10 Mbps)or orange (100 Mbps)	connection between station terminal and subscriber device is established
	flashes	packet data transmission via WAN interface
Phone	solid green	the phone is off-hook
	off	phone is on-hook, normal operation
	flashes during with 20 Hz frequency for 1 second, then 4 seconds pause	incoming call is on the phone port
	green, flashes slowly in periods	subscriber port registration is absent at SIP-proxy server
Power	solid green	power is on, normal operation
	flashes green	reset the device to the factory settings
	orange	internet is not accessible
	red	device starts up

[5] For TAU-8.IP-W only
[6] For TAU-8.IP-W only

Table 6 – Light indication of Ethernet 10/100 interface

LED	LED state	Device state
Green LED	solid on	10 Mbps connection with the external device is established
	Flashes	10 Mbps data transmission
Orange LED	solid on	100 Mbps connection with the external device is established
	Flashes	100 Mbps data transmission

1.8 Reset the device to the factory settings

To reset the device to default settings, press and hold 'F' button until 'Power' indicator begins to flash green. Indicator will flash before rebooting the device. The device will be rebooted automatically. Gateway will receive IP-address automatically by using DHCP protocol in the default configuration (beginning with software version 2.0.0). Voice menu provides control of the received IP-address (See Appendix A for more details).

1.9 Delivery Package

The standard delivery package of TAU-4.IP /TAU-8.IP includes:

- universal TAU-4.IP /TAU-8.IP subscriber terminal;
- 220/12 V, 2 A power adapter;
- removable antenna (only for TAU-8.IP-W);
- information leaflet;
- operation manual on a CD (optional).

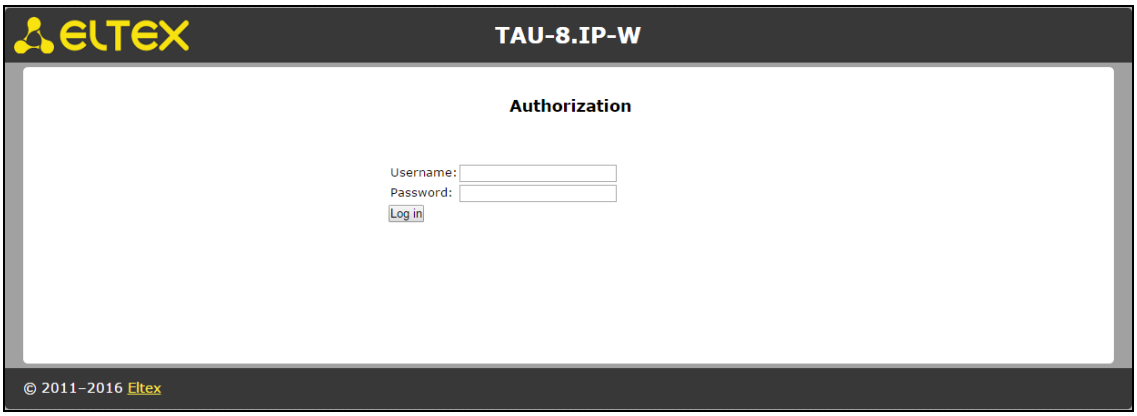
2 DEVICE CONFIGURATION VIA WEB-INTERFACE. ADMINISTRATOR ACCESS

The device configuration is shown by example of TAU-8.IP-W. Configuration of TAU-4.IP and TAU-8.IP is performed in a similar way.

Connect to the device via WAN interface by using web-browser (explorer for hypertext document) such as Firefox, Opera and Chrome. Enter IP-address of the device into the browser string.

The default IP-address of the device - 192.168.1.2, subnet mask - 255.255.255.0. Gateway will receive IP-address automatically by using DHCP protocol in the default configuration (beginning with software version 2.0.0). Voice menu provides control of the received IP-address (See Appendix A for more details).

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



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

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

The *'Information'* menu of the *'System'* submenu will open after getting access to the web-configurator. Navigation elements of the WEB-configurator are shown in Fig. 6.

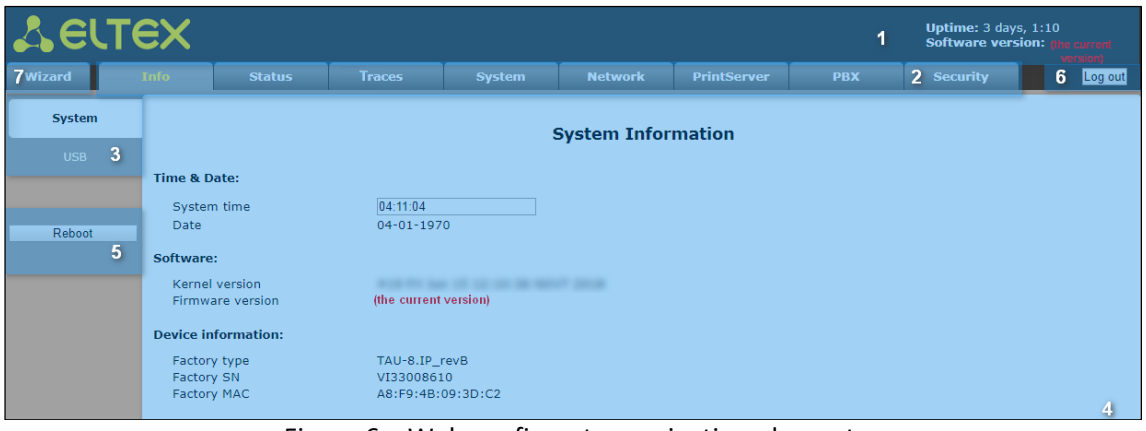


Figure 6 – Web configurator navigation elements

User interface window is divided into seven general areas:

1. *Information space displays the device name, software version, operation time after loading.*
2. *Menu to control field of settings*
3. *Submenu options to control field of settings.*
4. *Settings field of the device based on the user choice. It is destined for viewing the device settings and configuration data entry.*

To save changes into non-volatile memory, click *'Save changes' button.* In this case, settings for *'Traces', 'PBX'* and *'Safety' tabs are applied automatically.* Reboot the device to apply changes for *'System', 'Network'* and *'Print Server'* tabs. Notice about restart behavior will appear in dialog window and *'Reboot'* button will change color to red.

5. Control buttons:

- *Reboot – device reboot menu.*

6. *Button to end the session to access the device - **Log out (** admin **).***

TAU-8.IP includes two types of the users: **admin**, **user** and **viewer**. User **admin** (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring. User user (default password: user) may access device status monitoring without reading and recording configuration data. User **viewer** (spectator, default password: **viewer**) may only view full device configuration without editing privileges; may access full device status monitoring.

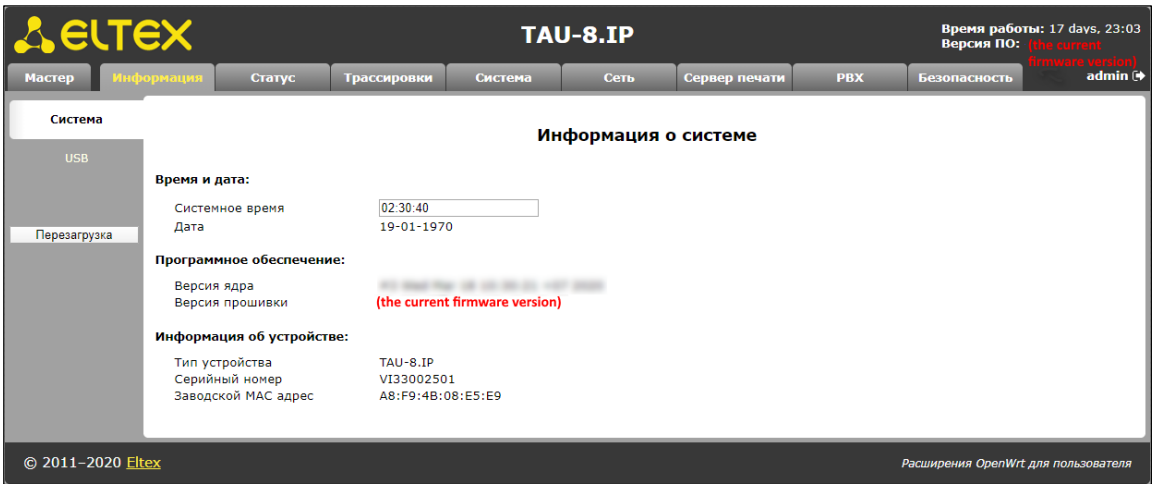
7. 'Wizard' tab for the device rapid configuration (see APPENDIX B for the detailed description).

Web Configurator Language:

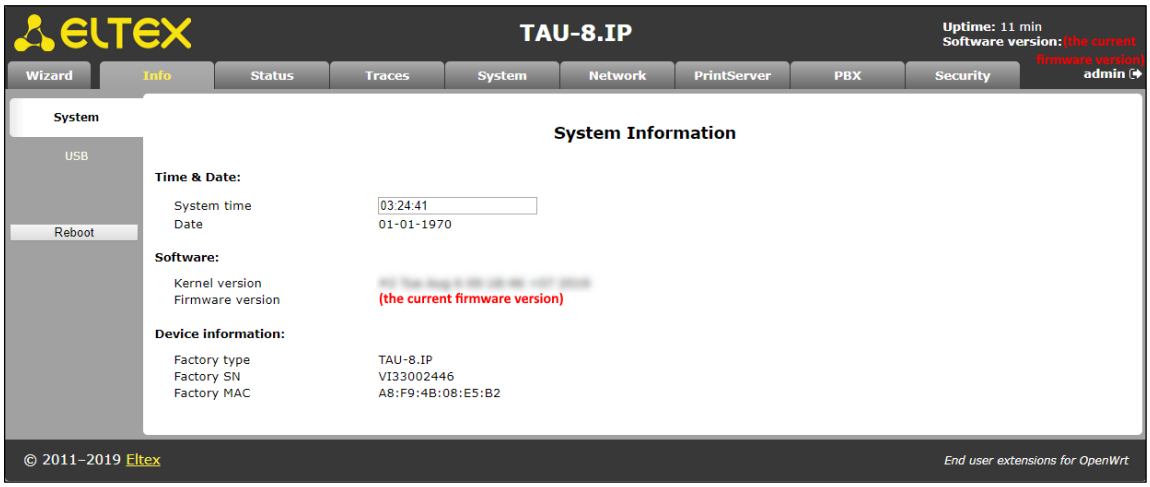
Web configurator allows selecting from two interface languages: *Russian* and *English*.

By default, interface language for firmware version is specified as '-ru' for Russian language and '-en' for English language. Enter in the menu 'System', select the desired interface language in Settings worksheet, click 'Save Changes' button and after click 'Apply' button.

Example of web configurator menu in Russian:

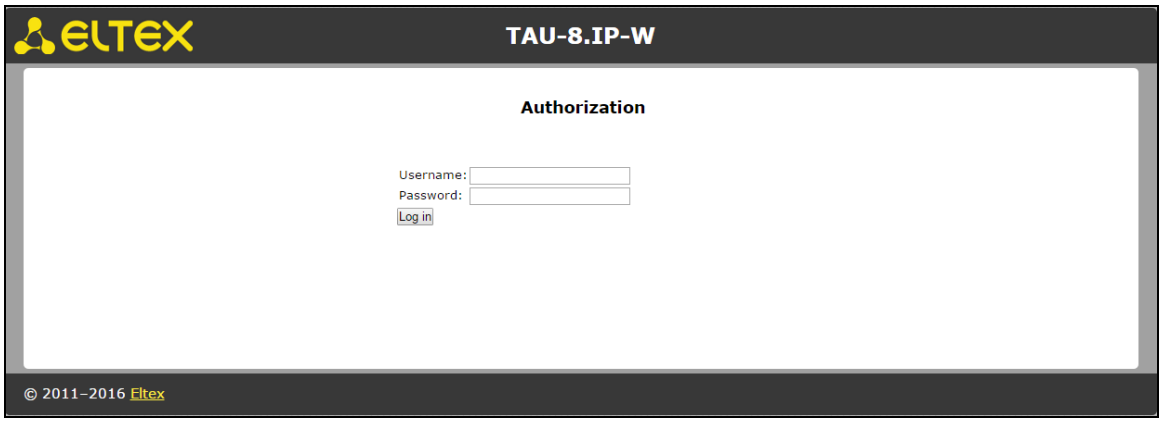


Example of web configurator menu in English:



Changing users:

After clicking the *'Log out'* button, the current user session will be finished and authorization window will appear:



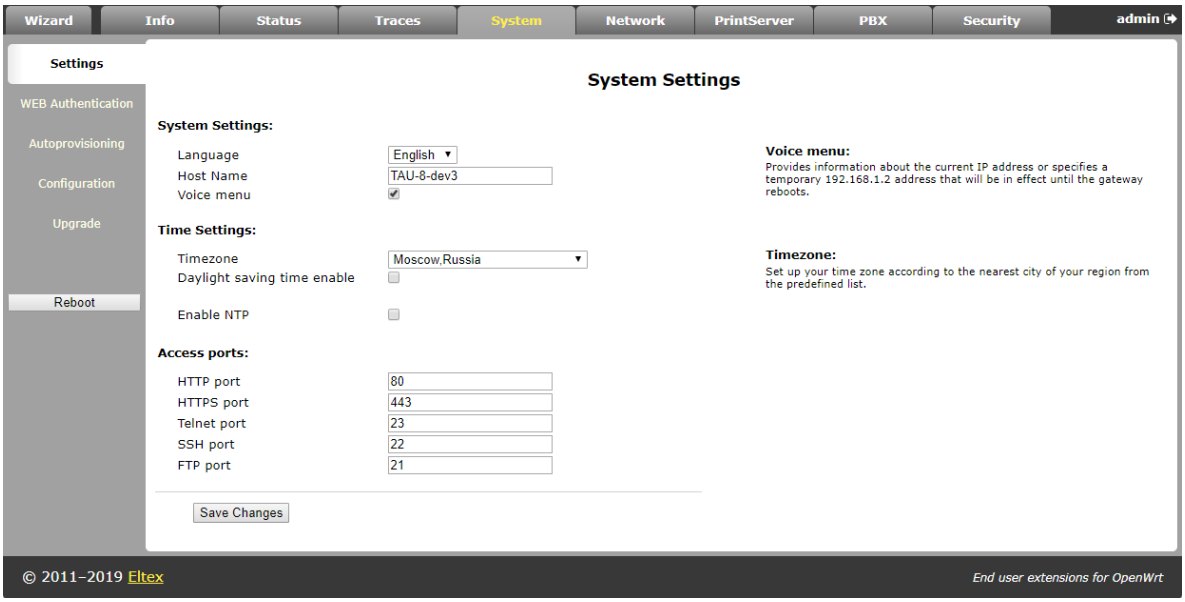
To change user, assign user name and password and click *'Log in'* button.

2.1 The 'System' menu

The *'System'* menu provides configuration of the system, time and access to the device via Web, Telnet, SSH and FTP and it allows you to change password, work with configuration files and the device software update.

2.1.1 The 'Settings' submenu

Use the submenu to configure system and time.

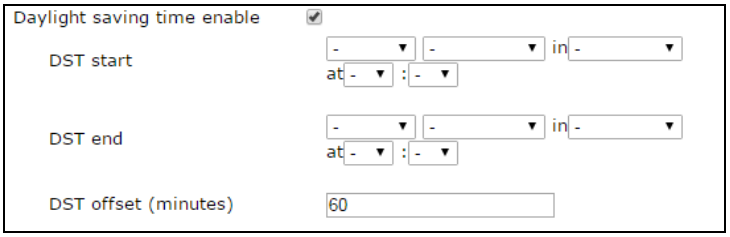


System settings:

- *Language* – language selection for the Web-configurator from two variants: Russian and English;
- *Host Name* – host name (OpenWrt is set up by default) can be used for device identification;
- *Voice menu* — when checked, the setting allows you to get information about the current device IP and to specify a temporary IP address – 192.168.1.2 (will be in effect until the reboot of gateway). To access to the voice menu, dial *** on the phone. To set a temporary IP address, dial 0 in the voice menu mode.

Time Settings:

- *Timezone* – allows you to pick a timezone from the list in accordance with the closest city of your region;
- *Daylight saving time enable* – when checked, settings of the automatic daylight saving time are available:



- *Daylight saving (DST start) – setting of the moment and time of daylight saving by the format of 'week number, day, hour, minutes', for example the last Sunday of July at half night;*

- *DST end – you can set date and time of daylight saving time (DST) in the format 'week number, week day, month, hours, minutes', for example, the second Sunday of October, 00 hours 00 minutes;*

- *DST offset (minutes) – set the time shift value, in minutes;*

- *Enable NTP* – set the flag to enable synchronization of the device system time from specified NTP server.

- *Get the NTP server address automatically* – set the flag to get NTP server address from DHCP server (option 42) automatically.

- *NTP Server* – IP-address/domain of NTP-server.

Access Ports:

- *HTTP port* – specify a port for access via HTTP protocol;

- *HTTPS port* – specify a port for access via HTTPS protocol;

- *Telnet port* – specify a port for access via Telnet protocol;

- *SSH port* – specify a port for access via SSH protocol*;*

- *FTP port* – specify a port for access via FTP protocol.

To store changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

2.1.2 The 'WEB Authentication' submenu

Use the submenu to assign passwords for administrator and unprivileged user.

TAU-8.IP implies two types of the users: admin and user. User admin (default password: password) has full access to the device: read/write any settings, full device status monitoring. User user (default password: user) may access device status monitoring without reading and recording configuration data. V**iewer** (**spectator**, default password: **viewer**) may only view full device configuration without editing privileges and access full device status monitoring.

Administrator password is used for administrator access via Web-interface, Telnet and SSH protocols. User password is used for unprivileged user access via Web, Telnet, SSH and FTP. Viewer password is used to view the device settings via Web, Telnet, SSH and FTP.

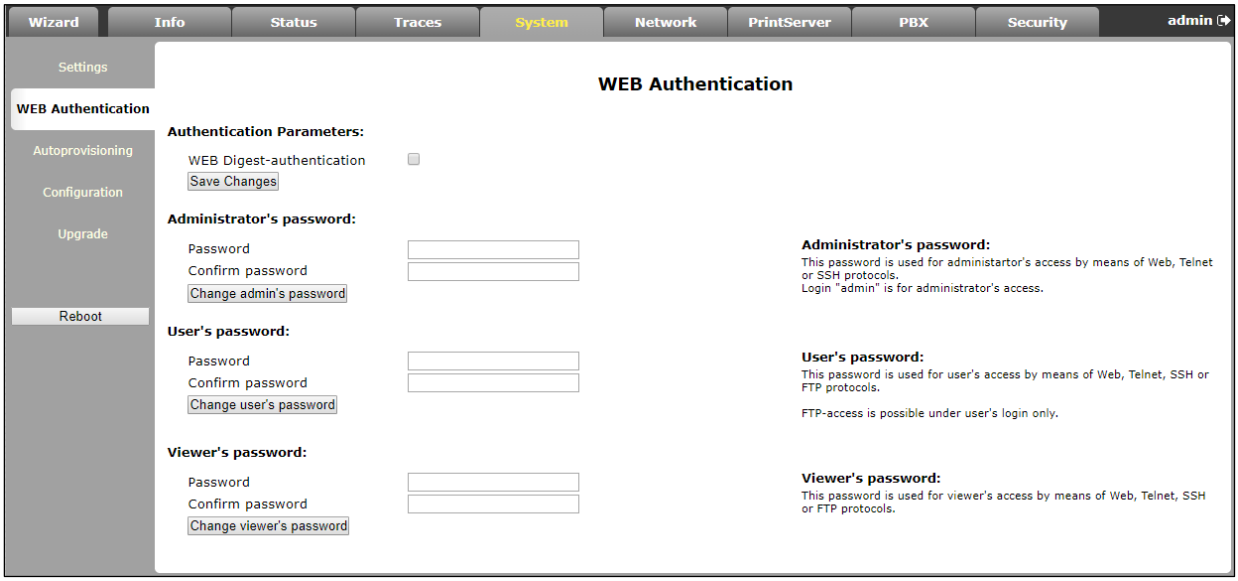
Administrator login for access via Web-interface: *admin.*

Administrator login for access via Telnet and SSH protocols: admin. *After successful authorization, CLI will be started. To access to shell, enter enable and shell sequentially.*

Unprivileged user login for access via Web-interface, Telnet, SSH, FTP: *user.*

Viewer login for access via WEB interface, Telnet, SSH and FTP: viewer.

Access via FTP is available only for USER.



Authentication Parameters:

WEB Digest-authentication — when checked, user authentication is performed in accordance with digest algorithm. When unchecked, basic method is used.

Access passwords settings:

- *Password* – field for entering a password;
- *Confirm Password* – field for confirming a password.

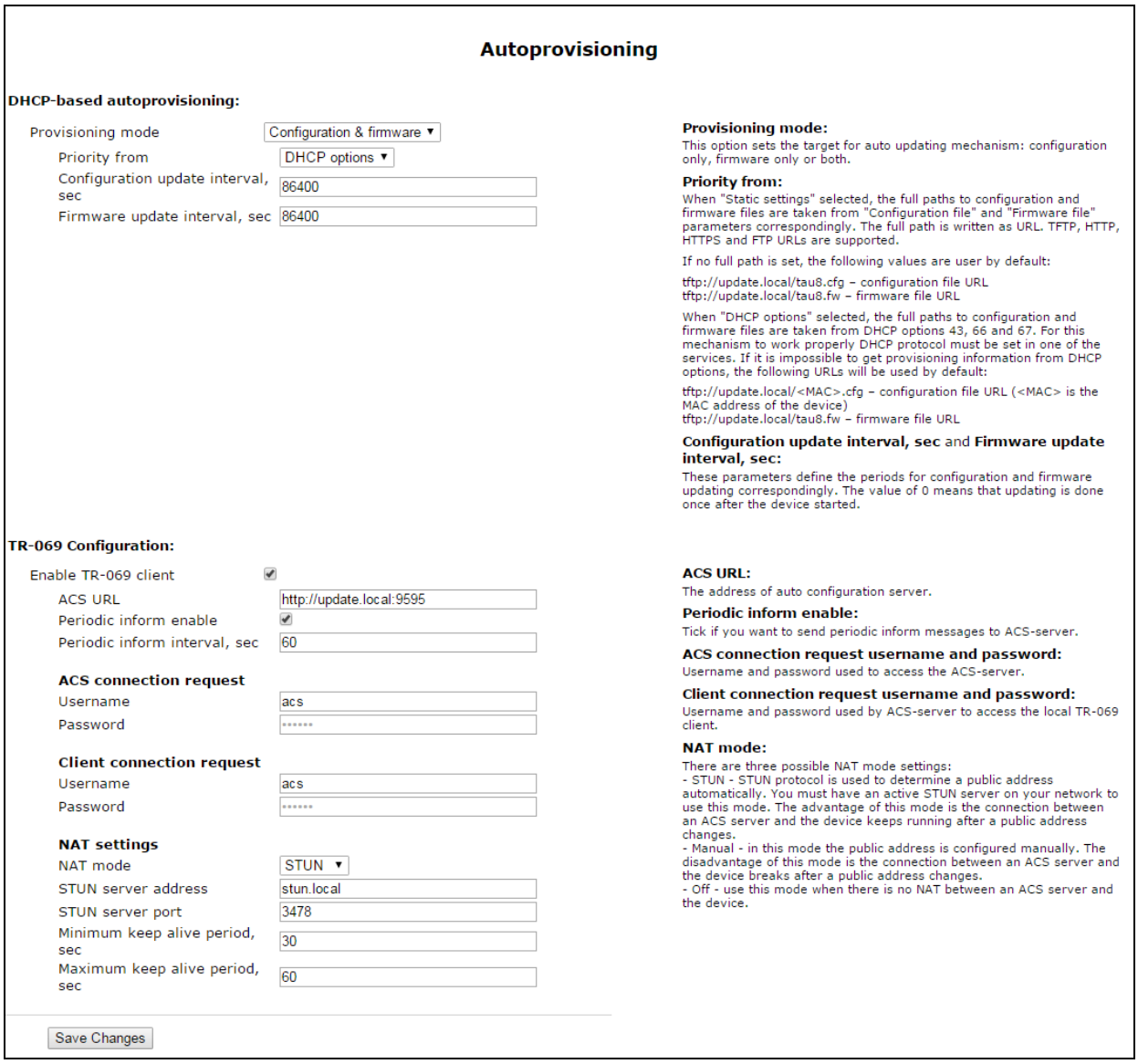
Click *'Change admin's password'*, *'Change user's password'* or *'Change viewer's password'* button to apply or change administrator, user or viewer passwords correspondingly.

2.1.3 The 'Autoprovisioning' submenu

The submenu provides settings of the built-in client for TR-069 autoprovisioning protocol of subscriber device by using DHCP protocol.

DHCP-based autoprovisioning:

The device after loading will try to get information about autoprovisioning server address and names of firmware and configuration files by using DHCP.



- Autoupdate (Provisioning mode) – *type selection of autoupdate:*
  - *Disabled – autoupdate is disabled;*
  - *Configuration & firmware – performed autoupdate of configuration and firmware;*
  - *Configuration only – provides only autoupdate of configuration;*
  - *Firmware only – provides only firmware autoupdate.*

- *Priority from* – priority selection of file determination for autoprovisioning:

  · *DHCP options – when this priority is selected, URL of configuration file and firmware are determined by using 43, 66 and 67 DHCP-options for that purpose one of the services should have address getting configured via DHCP.*

If you couldn't eject autoupdate parameters the following URL parameters will be used by default:
tftp://update.local/<MAC>.cfg - URL of the configuration file (where <MAC> is MAC-address of the device, and symbol '.' is byte-separator)
tftp://update.local/tau8.fw is URL of firmware file.

  · *Configuration update interval, sec – determinates configuration update interval. 0 value means that update will be applied only once when the device is launched;*

  · *Firmware update interval, sec – determinates firmware update interval. 0 value means update will be applied only once during the device start.*

  · *Static settings – when this priority is selected, you should specify file location to update configuration and firmware;*

If the path to a file is absent, the following values will be used by default:
tftp://update.local/tau8.cfg - URL of configuration file;
tftp://update.local/tau8.fw- URL of firmware file.

  · *Configuration file – full configuration pathname in the URL format (TFTP-, HTTP-, HTTPS- and FTP-URLs are supported, for example, tftp://update-server.loc/tau8.conf);*

  · *Firmware update interval, sec – determines configuration update interval. 0 value means that update will be applied only once when the device is launched;*

  · *Firmware file – pathname of firmware in the URL format (TFTP-, HTTP-, HTTPS- and FTP-URLs are supported, for example, tftp://update-server.loc/tau8.conf);*

  · *Configuration update interval, sec – determines firmware update interval. 0 value means update will be applied only once during the device start.*

See a detailed description of DHCP-based autoprovisioning operation algorithm in the section 5**.**

TR-069 Configuration:

- *Enable TR-069 client* – when checked, integrated TR-069 protocol client will be enabled;

- *ACS URL* – autoconfiguration server address. Enter address in the following format: http://ip address>:<port> (<ip address> – ACS server IP-address or domain name, <port> – ACS server port);

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

ACS connection request:

- *Username, Password* – username and password used by client to access ACS server.

Client connection request:

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

Software updating, changing and reading a current configuration, rebooting and resetting to the default settings can be implemented via TR-069 protocol.

NAT settings:

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

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

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

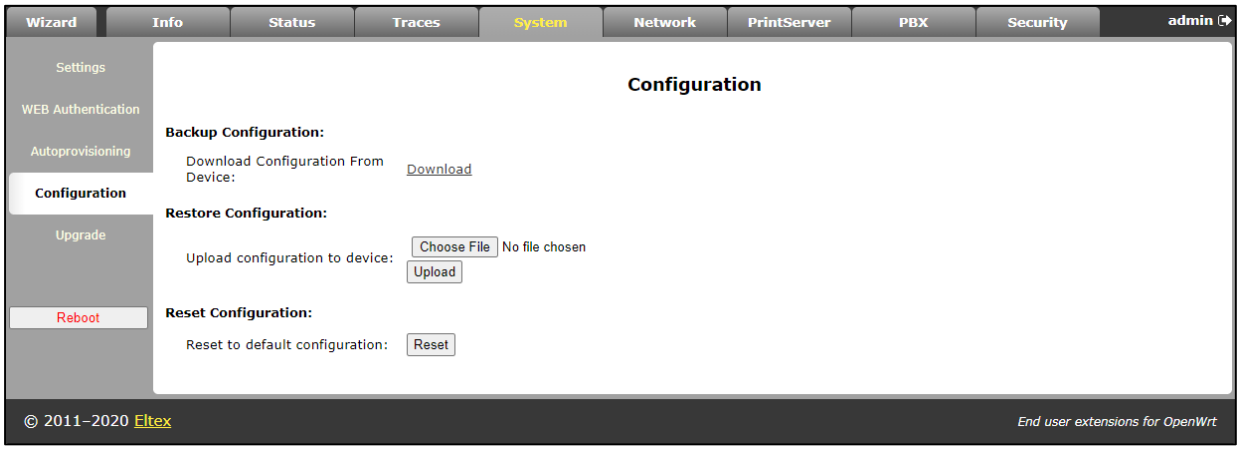
- *STUN server address* – STUN server IP address or domain name;
- *STUN server port* – STUN server UDP port (3478 by default);
- *Minimum keep alive period, seconds and Maximum keep alive period, seconds* – define the time interval in seconds for periodic transmission of messages to STUN server in order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

If *Manual* mode is selected, the client's public address is set manually via the *NAT Address* parameter (the address must be entered in IPv4 format).

To save changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

2.1.4 The 'Configuration' submenu

In the 'Configuration' submenu, you may save the current configuration, restore and reset it to the default settings.



Backup Configuration:

- To save the current configuration of the device to a local PC, click *'Backup'* button.

Restore Configuration:

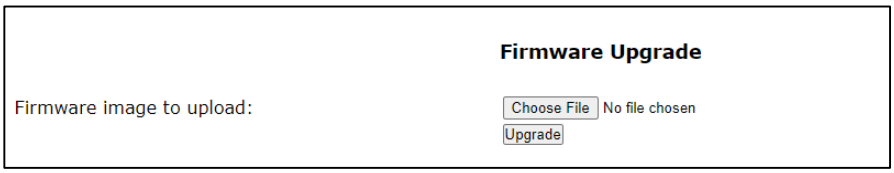
- *Saved config.tgz file* – configuration file selection. To restore previous established configuration, click *'Restore'* button.

Reset to default configuration – reset to the default configuration via pressing *'Reset'* button.

After the reset, the access to the device is possible via IP address getting from DHCP interface. If DHCP server is absent, use gateway voice menu. In order to do that, connect phones to any FXS port and dial '*' first, then dial '0'. 192.168.1.2 - IP address will be assigned to the device automatically. This address will be available until the first reboot of the gateway.**

2.1.5 The 'Upgrade' submenu

Use the submenu to update the device control program.



- *Firmware image to upload:* – firmware file selection – you should select *.tgz. archive file.

Select firmware file and click *'Upgrade' button to upgrade firmware of the device.* The process of upgrading a firmware can take a few minutes, after that the device will automatically reboot.

Do not switch off or reboot the device during the software update.

When returning to firmware version 2.4.2 and later, reset the device to the default configuration for the device proper operation.

2.2 The 'Network' menu

Use the *'Network'* menu to configure VLAN, WAN interface, SNMP client and wireless Wi-Fi access point; install MAC-addresses, NAT rules (for the device with Wi-Fi module) and operate with routing table.

2.2.1 The 'Network settings' submenu

Use the menu to specify the network interface configuration and configure the access to the device via various protocols.

To connect the device to the provider's network, you should to check the network settings with operator. When static settings are used, in the field *'Protocol for address getting on WAN'* you should select *'Static'* value and full *'WAN IP Address', 'WAN subnet mask', '1st DNS', '2nd DNS'* and *'The default gateway'* fields by values received from providers. If the devices on the provider network receive network settings via DHCP, PPPoE, L2TP or PPTP protocol, you should select corresponding protocols from *'Protocol for address getting on WAN'* box and use provider instructions for correct device configuration.

Network model is based on the service connections. You can configure maximum three services: **Internet, VoIP** and **Management**. Their division is implemented using VLAN identifiers. By default, key service **(Internet)** is set up, and other services are disabled.

When VoIP service is enabled, **VoIP** application will use VoIP service configuration for its operation. If VoIP service is disabled then VoIP application use Internet network configuration for operation.

Management service name does not mean that it can be used only for device management. The service can be used for various user needs. However, if TR-069 client is run up on the device, it will use **Management** service configuration for its operation. If the service is disabled, TR-069 client uses Internet configuration for its operation.

Internet – key service, it cannot be disabled. The rest of the services are additional and can be disabled.

To configure or check service settings, click corresponding button at the top of *'Network settings'* page.

It is important to know that you cannot use the same VLAN IDs for different services.

It is important to avoid the presence of the same subnet IP addresses (within one service as well as several services) on different network interfaces.

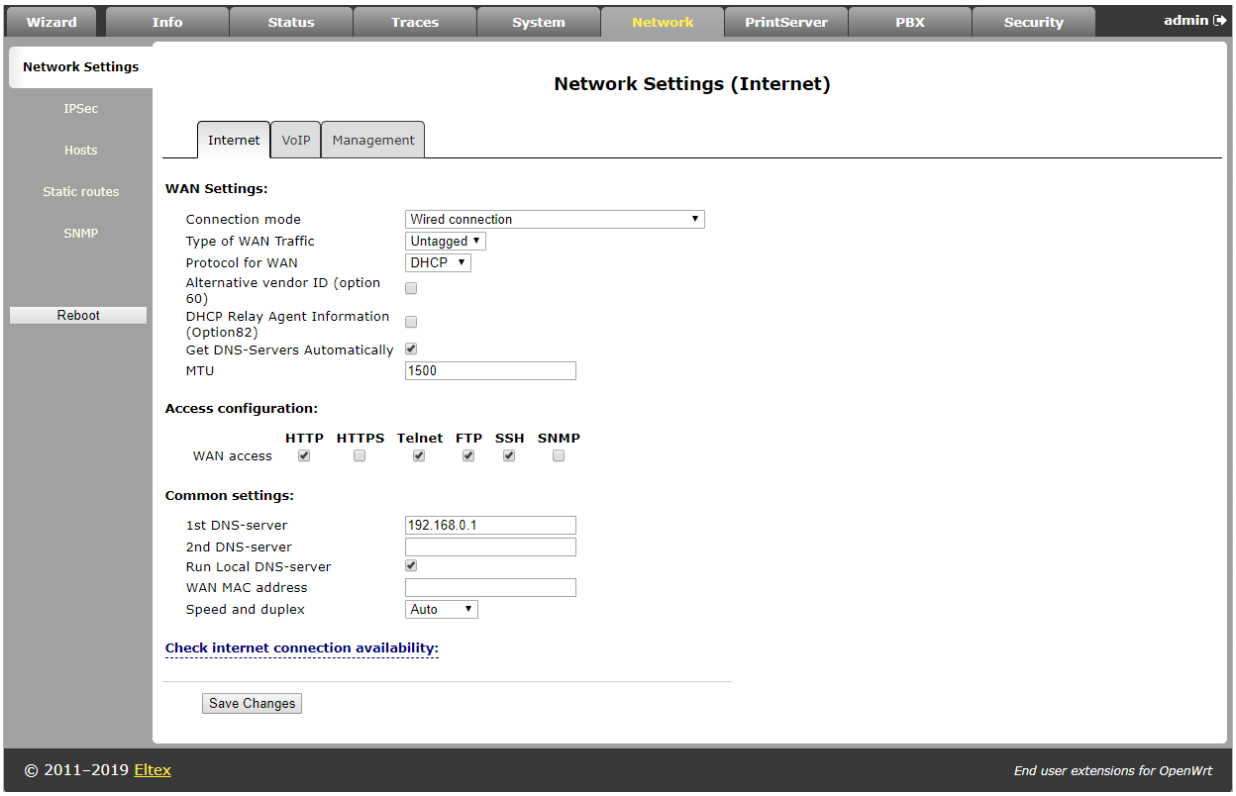
The 'Network settings' submenu. Internet service

WAN settings – use this field for WAN interface settings.

Connection mode – select connection method to WAN from the drop down list (option is available for configuration only in Internet):

- *Wired connection – Internet connection is performed only through Ethernet-cable by using WAN port;*
- *Wireless connection only (3G/4G) – Internet connection is performed via wireless USB 3G/4G modem (via mobile telephone network). To configure modem, you should click link 'Setup 3G/4G USB modem';*
- *Switch to reserve channel automatically – Internet connection is performed via key channel (it is assigned in the main submenu in the 'Preferred channel' field) and automatic transfer will be performed via backup channel in case of vanishing the Internet access via main channel.*

To configure USB-modem, click the *'Setup 3G/4G USB modem'* link.

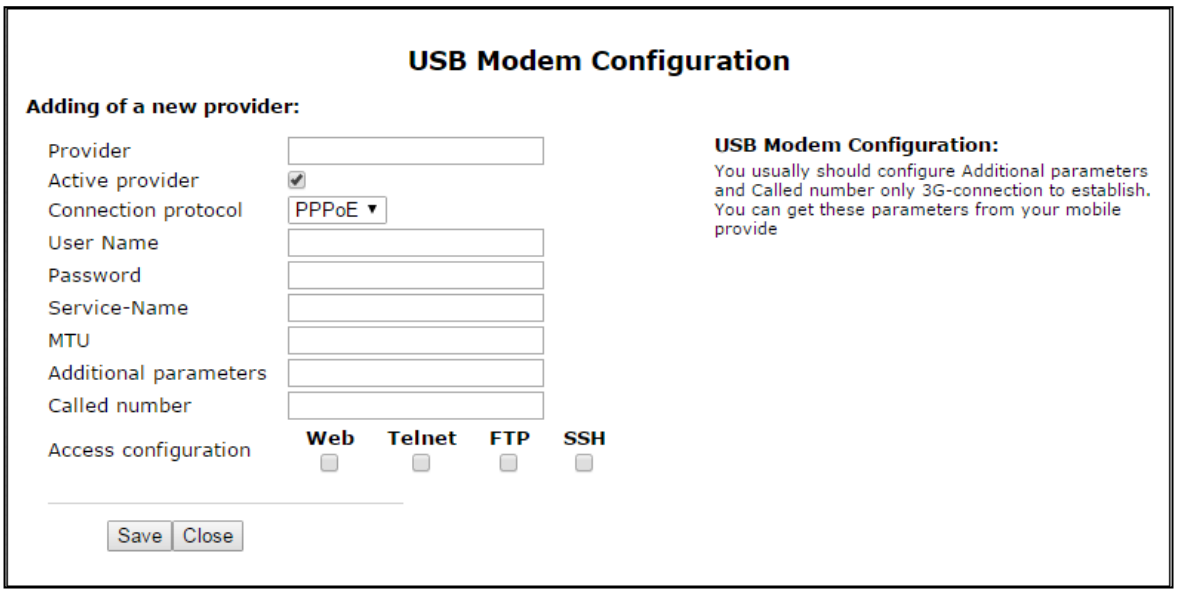


Determination of Internet connection availability is performed by transmitting the ICMP Echo-Requests via key channel to the service addresses specified in section *'Check internet connection availability'*. If the response to echo-test is received then decision about Internet connection availability via main channel is taken otherwise decision about transition to backup channel is taken. After transition to backup channel, the device continues to poll ping-servers via the preferred channel and if even one server gets answer the device returns back to the preferred channel.

When you select connection mode, *'Only wireless'* or *'Go on to the backup channel automatically'* you will see the link for switching to the 3G modem settings on the right side (**it is available only for Internet service**):

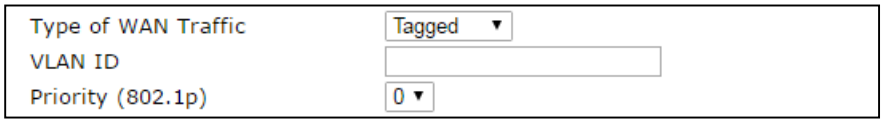
- *Provider* – provider name (arbitrary);
- *Active provider* – when checked, provider is active;
- *Connection protocol* – when 3G-modems are used, select PPPoE protocol; when 4G-modems are used, select DHCP protocol;
- *User Name* – user name for authentication (fill in, if required);
- *Password* – password for authentication (fill in, if required);
- *Service-Name* – 'Service-Name' tag is used during establishing PPP connection (full if it is required);
- *MTU* – maximum size of data block, by default it is 1500;

- *Additional parameters* – additional parameters of initialization (given by provider; for example Megafon mobile operator CGDCONT=1,IP,internet);
- *Called number* – it is given by provider (for example the Megafon *99***1#);
- *Access configuration* – if necessary, set flags under required protocol.



When *'Switch to backup channel'* connection mode is selected, selection of preferred channel becomes available (but only for Internet):

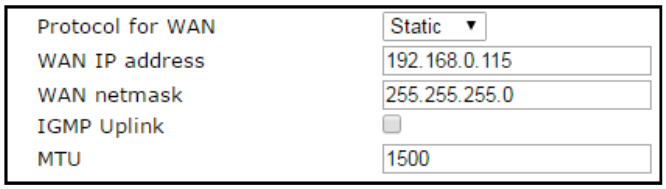
- *Preferred channel* – select the type of preferred channel from drop down list:
  - *Wired – channel via Ethernet WAN port of the device.*
  - *Wireless – channel via mobile communication network through USB-modem.*
- *Type of WAN Traffic* – selection of traffic type (Untagged and Tagged);



  - *VLAN ID – VLAN ID used for the service;*
  - *Priority (802.1p) – 1p priority settings for the VLAN ID;*

- *Protocol for WAN* – protocol selection for establishing a connection:

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



  - *WAN IP-Address – WAN IP-address settings;*

  - *WAN Netmask – WAN subnet mask;*

  - *IGMP Uplink – option is available only for TAU-8.IP-W devices – when checked, multicast traffic will be received from WAN interface of the service. Option can be included only in one service. WAN-interface of the service, where IGMP Uplink flag is set, will be used for signal reception of IPTV;*

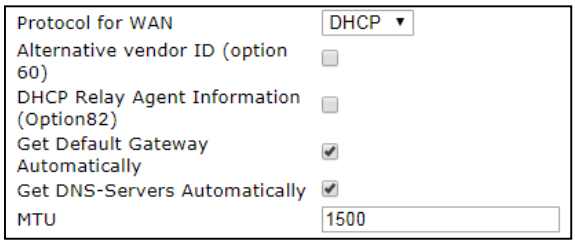
  - *MTU – maximum block size for data transmitted via the network (MTU=1500 for Ethernet protocol). This field is optional. Default value: 1500. The field is active only when the bridge mode is disabled.*

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

Supported options:

- 1 – subnet mask;
- 3 – default network gateway address;
- 6 – DNS address;
- 12 – device network name;
- 15 – domain name:
- 28 – network broadcast address;
- 33 – static routes;
- 42 – NTP server address;
- 43 – specific vendor information;
- 66 – TFTP server address;
- 67 – firmware file name (to download via TFTP from the server specified in Option 66);
- 82 – DHCP Relay agent information;
- 120 – SIP server outbound;
- 121 – classless static routes;

When 'DHCP' type is selected, the following parameters will be available for editing:



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

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

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

Example:

[VENDOR:Eltex][DEVICE:TAU-8.IP][HW:1.6][SN:VI33007740]
[WAN:A8:F9:4B:09:31:B0][VERSION:#current Firmware version]

- *DHCP Relay Agent information (Option 82)* – when selected, you can add to DHCP request the following data:

  Agent circuit ID – allows you to add suboption 1 - Agent Circuit ID;

  Agent Remote ID (Suboption 2) – allows adding option 82 to the DHCP request.

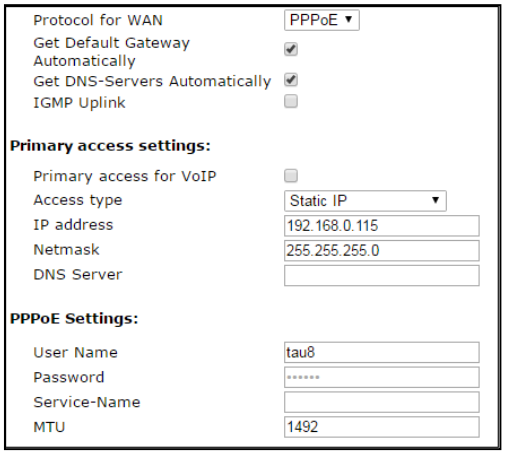
- *Get DNS-Servers Automatically* – when checked, *DNS*-server address (from DHCP-option 6) will be gotten automatically from DHCP-server (this flag can be set only in several services);

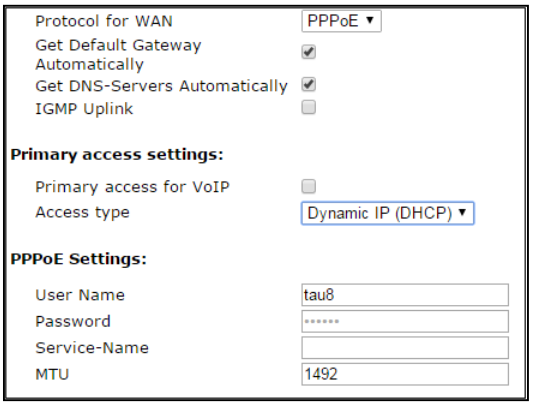
- *IGMP Uplink* – option is available only for TAU-8.IP-W devices – when checked, multicast traffic will be received from WAN interface of the service. Option can be included only in one service. Option can be included only in one service. WAN interface of the service, for which *IGMP Uplink* flag is set, will be used for IPTV signal reception;

- *MTU* – maximum size of data block transmitted by network (for Ethernet protocol MTU is 1500). This field is optional. Default value: 1500 The field is active only when the bridge mode is disabled.

PPPoE – operation mode, at which PPP-session is established on WAN-interface via PPPoE protocol.

When 'PPPoE' is selected, the following parameters are available for modification:





- *Get DNS-Servers Automatically* – when checked, DNS-server address (from DHCP-option 6) will be gotten automatically from DHCP-server (this flag can be set only in several services);

- *IGMP Uplink* – option is available only for TAU-8.IP-W devices – when checked, multicast traffic will be received from WAN interface of the service. Option can be included only in one service. Option can be included only in one service. WAN-interface of the service, where IGMP Uplink flag is set, will be used for signal reception of IPTV;

Primary access settings:

- *Primary access for VoIP* – when checked, interface of primary access will be used for operation of VoIP application; It is active only when VoIP service is disabled;

- *Access type* – access type selection:

  - *Dynamic IP (DHCP) – dynamic access, IP-address and all necessary parameters (subnet mask, address of DNS server) are received via DHCP;*

  - *Static IP – static access. When this access type is chosen, parameters necessary for operation in primary network (IP address, subnet mask and DNS-server) are assigned manually:*

  - *IP Address – address for access to local network recourses of provider;*

  - *Netmask – subnet mask in the primary access network;*

  - *DNS Server – server of the domain names used in local provider network.*

PPPoE Settings:

- *User Name* – user name for authorization on PPP server;
- *Password* – password for authorization on PPP-server;
- *Service-Name* – Service-Name tag value in PADI message for PPPoE connection initialization (this field is optional: set the parameter if it is required by provider);
- *MTU size* – maximum block size for data transmitted via the network. 1492 is recommended;

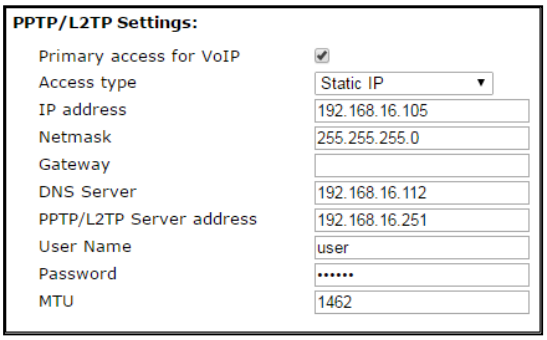
PPTP – operation mode when the Internet access is established via a special channel—a tunnel—using VPN;

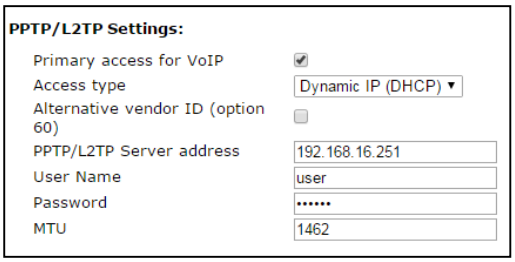
L2TP – protocol for VPN implementation.

PPTP and L2TP allow establishing secure communication link over the Internet between the remote user's computer and organization's private network. PPTP and L2TP are based on Point-to-Point Protocol (PPP) and act as its extension. First, the OSI model higher level data is encapsulated into PPP, and then into PPTP or L2TP for tunnel transmission via public data networks. PPTP and L2TP functionality differs. L2TP may be used not only in IP networks, service messages for tunnel creation and data transfer use the same format and protocols. PPTP may be used only in IP networks, it requires a dedicated TCP connection for tunnel creation and usage. L2TP over IPSec[7] allows for the higher security level compared to PPTP and provides the higher level of protection for business-critical data.

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

During the selection PPTP or L2TP, the following parameters will be available for changing:





- Primary access for VoIP – when checked, interface of the primary access will be used for operation VoIP application; flag is active only when VoIP is disabled;
- Access type – access type to PPTP-server. Two variant is possible: dynamic access, when IP-address and other required parameters are obtained via DHCP protocol and static

[7] IPSec support has been implemented in firmware version 1.6.0 and higher

access in this case IP address, subnet mask, DNS server, gateway and other required parameters for access to PPTP server are assigned manually;

- IP Address – when the static access is used, VPN server will be accessed from this address;
- Netmask – subnet mask for static access;
- Gateway – gateway IP address for static access, it is used for access to VPN-server (if VPN server is located in other subnet);
- DNS Server – server of names for static access, that is used in provider local network;
- PPTP/L2TP Server address – IP-address or domain name of VPN server;
- User Name – user name for authorization on VPN server;
- Password – password for authorization on VPN server;
- MTU – maximum size of data block transmitted through the network. 1462 is recommended value for PPPTP protocols and L2TP.

IGMP Uplink – option is available only for TAU-8.IP-W devices – when checked, multicast traffic will be received from WAN interface of the service. Option can be included only in one service. WAN-interface of the service, where *IGMP Uplink* flag is set, will be used for signal reception of IPTV.

Wi-Fi – use this section to set the parameters of the wireless interface. The section is available only for TAU-8.IP-W devices.

- *Wi-Fi access mode* – determine operation mode for wireless interface in the service:
  - *Off – access to the service via wireless interface is disabled;*
  - *Tagged – access to the service is performed via tagged wireless interface (VLAN ID is specified in the field 'VLAN identifier' – see above);*
  - *Untagged – access to the service is performed via untagged wireless interface;*
- *Bridge mode* – when checked, the device operates in the bridge mode (network traffic pass between WAN and Wi-Fi interfaces transparently). In bridge mode it is available via IP address of WAN interface;
- *SSID* – wireless network name (max length of the name is 32 symbols), entering with case-sensitive of keyboard. The parameter can include digits, Latin letters and the next symbols: "-", "_", ".", "!", ";", "#" (take into account that "!", ";" and "#" symbols can't be placed first). ***Please note that the field is obligatory;***
- *WLAN IP-Address* – IP-address of wireless access point;
- *WLAN Netmask* – subnet mask of wireless access point;
- *Enable WLAN DHCP-server (Local DHCP-server)* – when checked, host connecting via Wi-Fi to TAU-8.IP-W can get IP address, subnet mask and other parameters (that are required for work in network) from a built-in DHCP server automatically.

Access configuration – use this section to set permission for access to the device via Web-interface and via Telnet, FTP and SSH protocols.

- *WAN access* – to enable access to the device from external network, you should set the flag opposite to the required connection: Web, Telnet, FTP, SSH and SNMP;

- *WLAN access* – only for TAU-8.IP-W devices – to enable access to the device from wireless network, you should set the flag opposite to the required connection: Web, Telnet, FTP, SSH и SNMP.

Common settings – use this section to set parameters that are applied to all the services configured on the device.

- *1st DNS server, 2nd DNS server* – server addresses of domain names (it is used for host IP address determination by using its domain name). These fields can be empty, if they are not required;

- *Run Local DNS-server* – when checked, local DNS server is enabled otherwise it is disabled. Option is applied only to the TAU-8.IP-W devices. Local DNS server operates on the side of the device wireless interface. When option is enable, local DHCP server as a DNS address get WLAN interface address to the users. It is recommended to leave this option on;

- *IGMP Proxy* – when checked, IGMP Proxy is enabled (necessary for IPTV operation). Option is available only for TAU-8.IP-W devices;

By default, gateway is used only for static installation method of IP address on WAN interface.

- WAN MAC address – MAC address of WAN interface;

- Speed and duplex – selection of speed and operation mode for duplex.

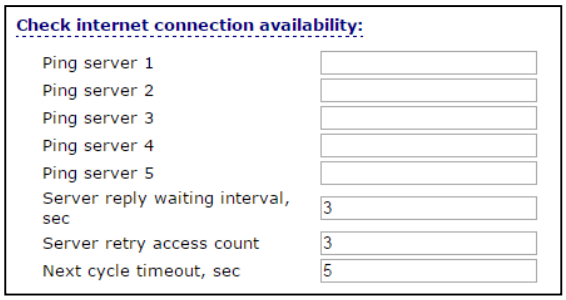
In case of using a gateway in private network, it is recommended to set IP address from allowed RFC1918 range for this type of networks:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Check internet connection availability: these settings are used for checking the activity of preferred channel during the selection of automatic switch to the backup channel in Internet service. Activity of the preferred channel is determined by having access at least one of the specified ping-servers during the assigned time interval.



- *Ping server 1..5* – host addresses to check access to Internet (transmission of the simple command 'ping' to specified node);

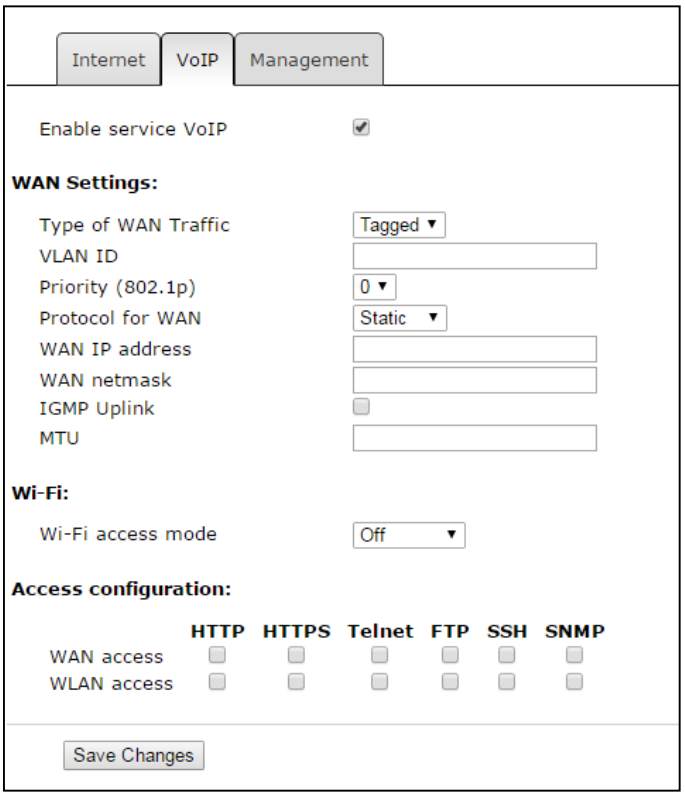
- *Server reply waiting interval, sec* – time interval during which the device will wait reply from ping-server;

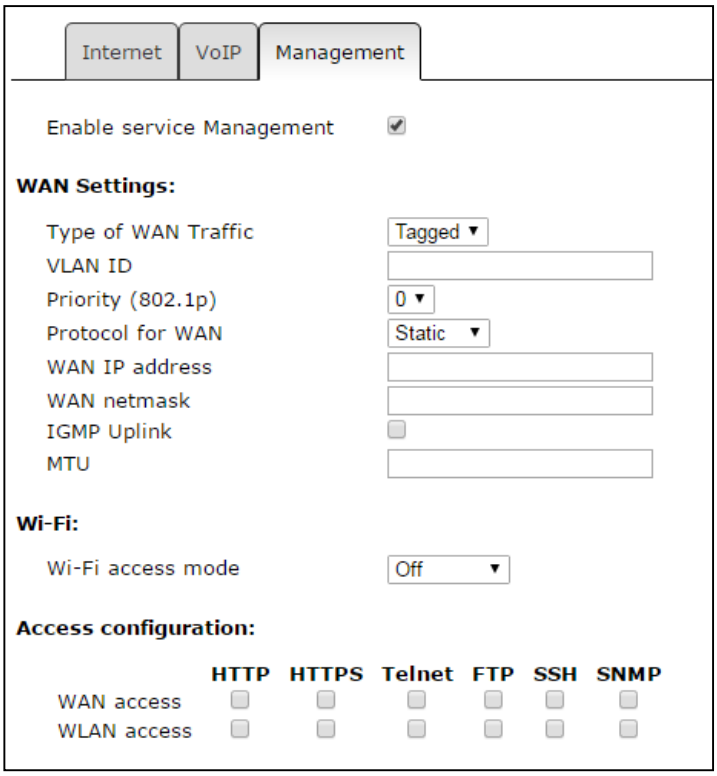
- *Server retry access count* – max count of the server retries in case of absence of response from ping-server during specified time (*Server reply waiting interval*);

- *Next cycle timeout, sec* – time interval between checks of access to the ping-servers.

To save changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

The 'Network settings' submenu, VoIP and Management services





When '*Add VLAN for VoIP*' flag is set, VoIP services will be made available via **'VoIP' service.** If the checkbox is disabled, VoIP services will be made available via **'Internet'** service.

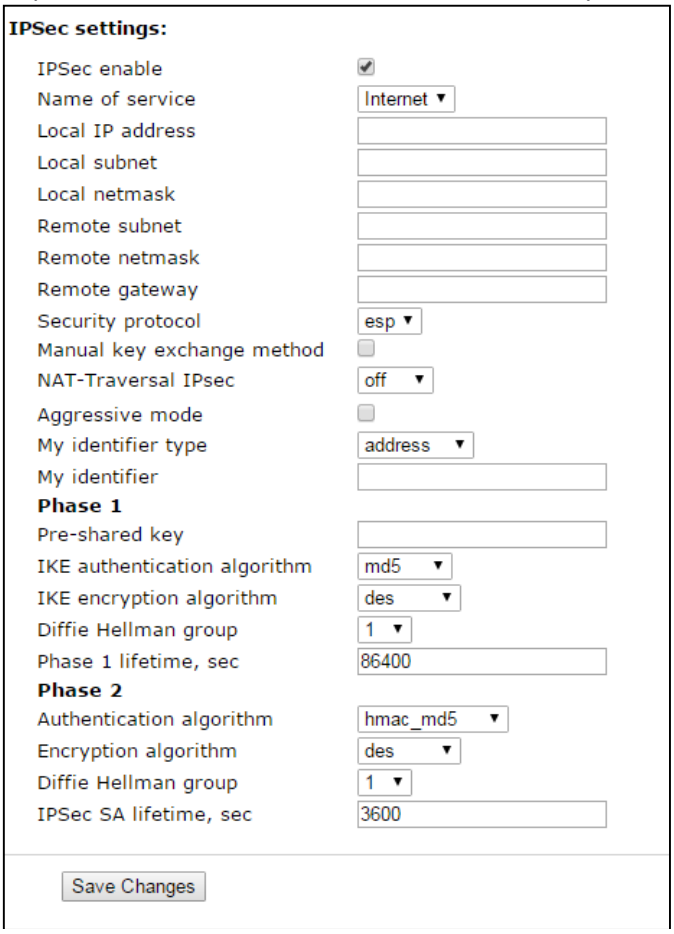
When *'Add VLAN for Management'* is set, configuring by using DHCP and TR-069 protocol will be available through **'Management' service.** If the checkbox is disabled, configuring by using DHCP and TR-069 protocol will be available through **'Internet'**.

Description of fields (accessible to configure) are described in the section 2.2.1 The 'Network settings' submenu.

To save changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

2.2.2 The 'IPSec' submenu

In this submenu, you may configure IPSec encryption (IP Security). IPSec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPsec also includes secure Internet Key Exchange protocols.



IPSec settings:

- *IPSec enable* – permit to use IPSec protocol for data encryption;
- *Name of service* – service selection where encryption via IPSec protocol will be used;
- *Local IP address* – the device address for operation via IPSec protocol;
- *Local subnet* in cooperation with *Local netmask* determine local subnet for creation network-to-network or network-to-point topology;
- *Remote subnet* in cooperation with *Remote netmask* determine address of remote subnet for connection with using encryption via IPSec protocol. If the mask value is 255.255.255.255, communication is performed with a single host. Mask that differs from 255.255.255.255 allows defining a whole subnet. Thus, functionality of the device allows you to organize the following 4 network topologies with using encryption traffic via IPSec protocol: point-to-point, network-to-point, point-to-network, network-to-network;
- *Remote gateway* – gateway used for remote network access;

- *Security protocol* – there are two key protocols: AH (Authentication header) and EPS (Encapsulating Security Payload). The first provides data authentication except data encryption; the second provides both operations. The device supports only the ESP protocol. IPSec can operate in one of the two modes: 'transport' or 'tunnel'. In the first case, contents of IP-packet (payload) is encrypted and/or authenticated except the header. In the second case, contents of initial IP-packet is encrypted and/or authenticated totally and new header is added to it. TAU-8.IP device operates only in the tunnel mode;

- *Manual key exchange method* – when manual mode is set, authentication and encryption keys are specified manually. This mode is not recommended to use. The following settings are available when the mode is disabled:

  · *NAT-Traversal IPSec - NAT-T mode selection. NAT-T (NAT Traversal) encapsulates IPSec traffic and simultaneously creates UDP packets to be sent correctly by a NAT device. For this purpose, NAT-T adds an additional UDP header before IPSec packet so it would be processed as an ordinary UDP packet and the recipient host would not perform any integrity checks. When the packet arrives to the destination, UDP header is removed and the packet goes further as an encapsulated IPSec packet. With NAT-T technique, you may establish communication between IPSec clients in secured networks and public IPSec hosts via firewalls. You can choose one of the three NAT-T operation modes:*

  · *on – NAT-T mode is activated only when NAT is detected on the way to the destination host;*

  · *force – use NAT-T in any case;*

  · *off – disable NAT-T on connection establishment.*

The following NAT-T settings are available:

· *UDP port NAT-T – UDP port for packets used for IPSec message encapsulation. Default value is 4500;*

· *NAT-T keepalive packet transmission interval, sec – periodic message transmission interval for UDP connection keepalive on the device performing NAT functions.*

· *Aggressive mode – phase 1 operation mode, when all the necessary data is exchanged using three unencrypted packets. In the main mode, the exchange process involves six unencrypted packets.*

· *My identifier type – identifier type of the device: address, fqdn, user_fqdn, asn1dn;*

· *My identifier – device identifier used for identification during phase 1 (fill in, if required). Identifier format depends on the type.*

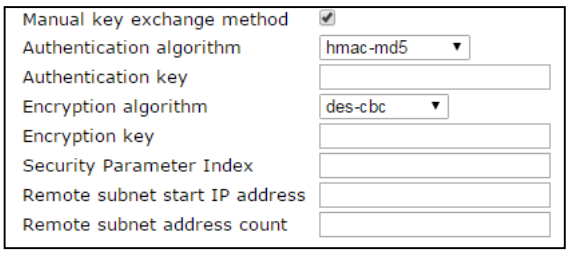
Phase 1 During the first step (phase), two hosts negotiate on the identification method, encryption algorithm, hash algorithm and Diffie Hellman group. In addition, they identify each other. For phase 1, there are the following settings.

- *Pre-shared key;*
- *Authentication algorithm – select an authentication algorithm from the list: MD5, SHA1, SHA256, SHA384, SHA512;*
- *Encryption algorithm – select an encryption algorithm from the list: DES, 3DES, Blowfish, Cast128, AES;*
- *Diffie Hellman group – select Diffie-Hellman group;*
- *Phase 1 lifetime, sec – time that should pass for hosts' mutual re-identification and policy comparison (other name IKE SA lifetime). Default value is 24 hours (86400 seconds).*

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

- *Authentication algorithm – select an authentication algorithm from the list: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512;*
- *Encryption algorithm – select an encryption algorithm from the list: DES, 3DES, Blowfish, Twofish, Cast128, AES;*
- *Diffie Hellman group – select Diffie-Hellman group;*
- *Phase 2 lifetime, sec – time that should pass for data encryption key changeover (other name IPSec SA lifetime). Default value is 60 minutes (3600 seconds).*

During the activation of manual mode of key exchange, the following settings will be available:



- *Authentication algorithm* – select an authentication algorithm from the list: HMAC-MD5, NMAC-SHA1, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512;
- *Authentication key* – key authentication is assigned in dependence on selected algorithm;

- *Encryption algorithm* – select an encryption algorithm from the list: DES-CBC, 3DES-CBC, Blowfish-CBC, Cast128-CBC;

- *Encryption key* – encryption key is assigned in dependence on selected algorithm;

- *Security Parameter Index* – identifying tag added to IPSec header. It helps to the hub to differ two data streams involving different encryption algorithms;

- *Remote subnet start IP address* in cooperation with *'Remote subnet address count'* determines address list to establish IPSec tunnel. Addresses should locate in subnet determined by 'Remote subnet' and 'Remote subnet mask' parameters.

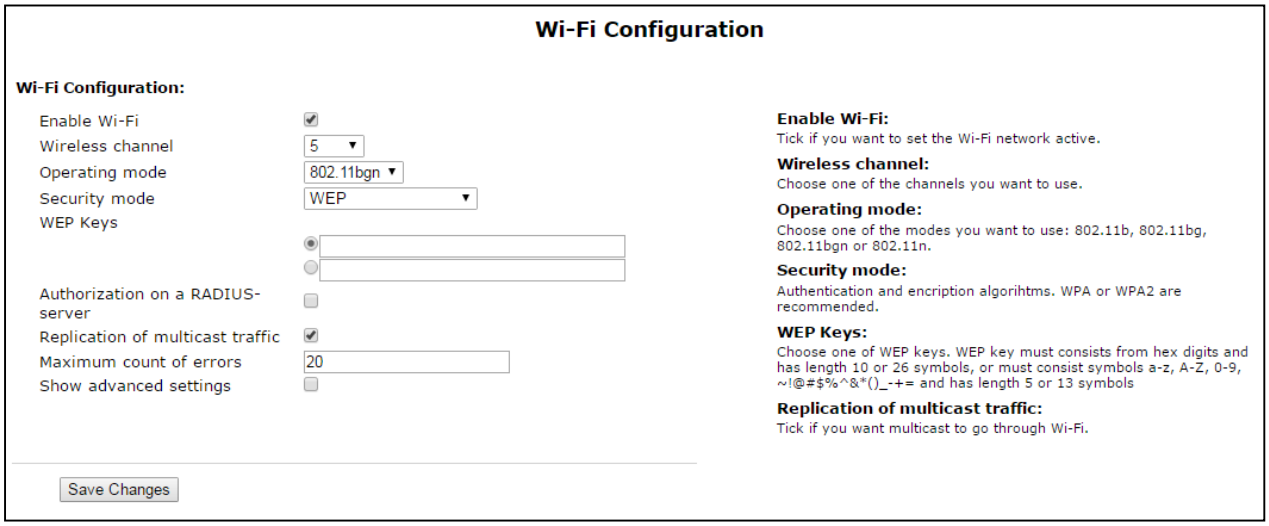
The 'Wi-Fi' submenu

The submenu is available only for TAU-8.IP-W devices.
Use the submenu to configure wireless network.

Wi-Fi Configuration:

- Enable Wi-Fi – when checked, option of wireless access to the device is enabled;

Wireless network name (SSID) is set in the 'Network' menu (tab 'Network settings') separately for each service. SSID field becomes active if you select the Tagged/Untagged of 'Access mode via Wi-Fi'. These settings will be applied to all the configured access points.



- Channel number for Wi-Fi – channel number for wireless network operation**;**

- *Operating mode* – wireless interface operation mode:

  - *802.11b – if all the Wi-Fi clients support standard 802.11b;*

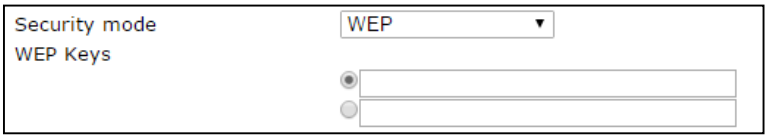
  - *802.11bg – if network has Wi-Fi clients with 802.11b and 802.11g support;*

- *802.11bgn – if the network has Wi-Fi clients with 802.11b, 802.11g and 802.11n support.*

- *Security options* – select security mode of wireless network:

  - *Off – disable encryption to transmit data (low security level);*

  - *WEP – WEP algorithm – when this type of authentication is selected, you must enter security keys:*



WEP Keys – You can enter up to two different keys of 10 or 26 hexadecimal digits, or 5 or 13 ASCII8. To select a key, check the corresponding box. Using WEP is not recommended due to security flaws related primarily to its encryption weakness and lack of any user authentication mechanisms. The key problem of WEP is that it uses highly similar keys for different data packages;

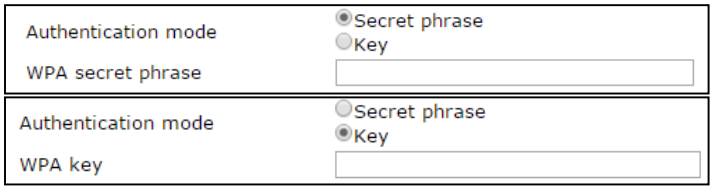
  - *Use WPA only – use only WPA standard. WPA uses TKIP, MIC and 802.1X algorithms, it significantly increases security of the standard in relation to WEP;*

  - *Use WPA2 only – use only WPA2 standard. CCMP and AES are implemented in WPA2 thereby WPA2 became more secured in opposite to WPA. Take into account that it is recommended to use this secure algorithm;*

  - *Use WPA and WPA2 – use security algorithm WPA and WPA2.*

When any type of WPA authentication is selected, the following settings will be available for editing:

- *Authentication mode* – select authentication method – secret phrase (password) or key access:

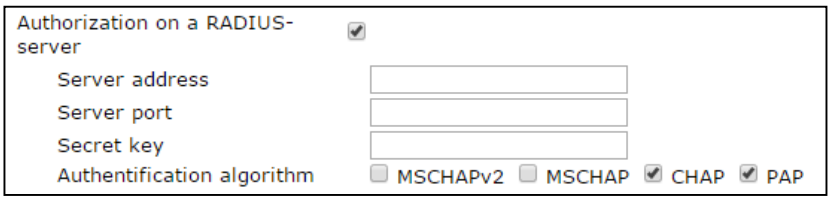


  - *Secret phrase – encryption key is a string with length from 8 to 63 ASCII symbols;*

  - *Secret WPA key (Key) – set key with 64 characters of hexadecimal number system;*

[8] ASCII is a set of 128 characters for machine representation of capital and lower case Latin characters, digits, punctuation marks, and special symbols.

- *Authorization on a RADIUS-server* – when checked, use authorization on a RADIUS-server. When the parameter is selected, the following settings will be available for editing:



  - *Server Address – domain name or IPv4 address of authorization server;*
  - *Server Port – server port for authorization;*
  - *Secret key – secret key for access to server of authorization;*
  - *Authentication algorithm – select authorization algorithm (MSCHAPv2, MSCHAP, CHAP, PAP).*

Username for client authentication on RADIUS server is equal to its MAC address (lowercase letter without separator symbols between bytes) and key of RADIUS server is used as password.

- *Replication of multicast traffic* – enable replication mode for multicast traffic. When this parameter is selected, the following configuration will be available:
  - *Maximum count of errors – max count of transmission errors upon the exceeding of which it is considered that the user out of network range. It is used to disable users in the replication mode of multicast traffic;*
- *Show advanced settings* – when checked, configuring the addition settings are available from the following list:
  - *HT40+ – when checked, merge mode of two 20 MHz channels into 40 MHz channel is enabled (the first channel is over the second, it operates only for 1-9 channels);*
  - *HT40- – when checked , merge mode of two 20 MHz channels into 40 MHz channel (the second is over the first, it operates only for 5-11 channels);*
  - *LDPC support – when checked, support of coding with low-density parity-check code is enabled;*
  - *SMPS - Static – when checked, Spatial Multiplexing Power Save Static method is available;*
  - *SMPS - Dynamic – when checked, Spatial Multiplexing Power Save Dynamic method is available;*

- *Green Field – when checked, compatibility with IEEE 802.11b/g;*
- *Delayed Block Ack – when checked, delayed data block acknowledgment mode is enabled, otherwise immediate acknowledgment is used;*
- *Set A-MSDU to 7935 octets – when checked, max size of A-MSDU is 7935 bytes otherwise it is 3839 bytes;*
- *DSSS/CCK mode (for 40 MHz) – when checked, DSSS/CCK modulation operation mode is used;*
- *PSMP support – when checked, Power Save Multi-Poll will be used for down town;*
- *L-SIG TXOP support – when checked, L-SIG TXOP method of combined protection for data transmission (802.11n) is used;*
- *STBC support at reception (1 stream) (RX-STBC1), STBC support at reception (up to 2 streams) (RX-STBC2), STBC support at reception (up to 3 streams) (RX-STBC123) – when checked, signal reception with supporting STBC (space time block codes) encryption is enabled;*
- *TX-STBC – when checked, data encryption is used to improve signal-to-noise ratio;*
- *Short guard interval (20 MHz) (SHORT-GI-20) – when checked, guard interval for 20 MHz operation mode is equal to 400 ns (data speed is up to 150 Mbps), otherwise-800 ns (data speed is up to 130 Mbps);*
- *Short guard interval (40 MHz) (SHORT-GI-40) – when checked, guard interval for 40 MHz operation mode is equal to 400 ns (data speed is up to 300 Mbps), otherwise-800 ns (data speed is up to 270 Mbps);*
- *WMM – Wi-Fi Multimedia (WMM) operation mode setting. This operation mode allows you to transmit audio- and video content simultaneously with data transmission quickly and efficiently.*

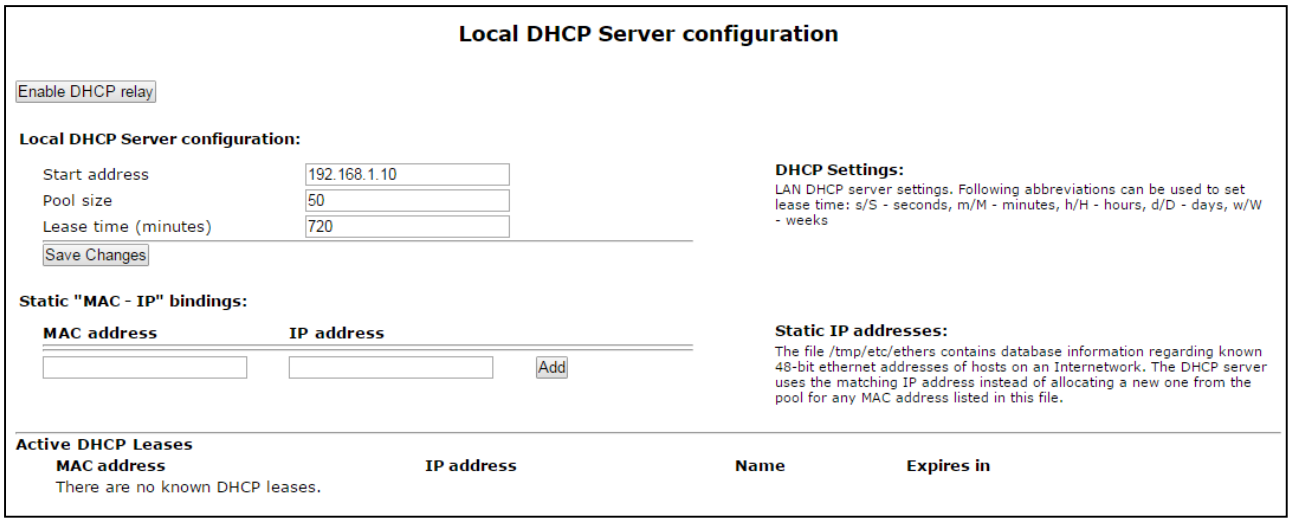
To save changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

The 'DHCP Server' submenu

The submenu is available only for TAU-8.IP-W devices.

In the DHCP server submenu, you may configure a local DHCP server.

DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses to the computers. DHCP eliminates limitations associated with the manual TCP/IP protocol configuration.



Local DHCP Server configuration:

- Start Address – starting address in the IP address pool;
- Pool size – number of addresses in the pool;
- Lease time (minutes) – set the maximum time for IP address lease issued by DHCP server to the connected device, in minutes.

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

Static IP address configuration allows you rigidly tie IP address (transmitted by DHCP server) to client's MAC address.

To add new static IP address, click *'Add'* button and fill in the following fields:

- *MAC Address* – set static MAC-address. It is assigned in XX:XX:XX:XX:XX:XX format;
- *IP Address* – set static IP address for assigned MAC address.

Click *Add* button to enter the IP address into the static IP address list for DHCP server.

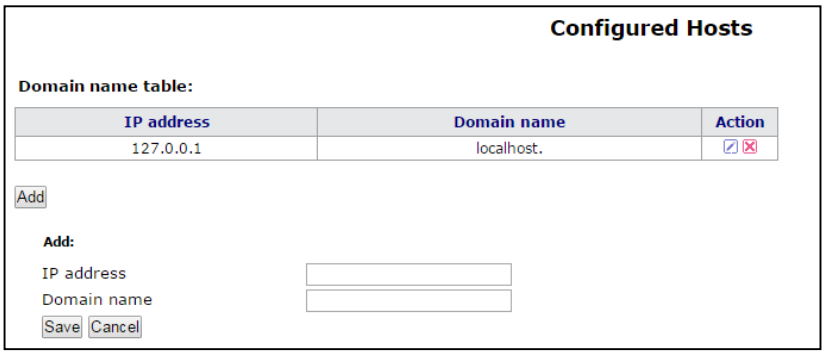
To remove an address from the list, click the *'Delete'* link next to the selected address.

Client's Mac address, IP address extracted from the pool, client name and lease duration of the address are specified in the table **Active DHCP Leases**.

When you press *'Enable/disable DHCP Relay'* button, DHCP agent-repeater will be turned off/on. To save changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply changes* button.

2.2.3 The 'Hosts' submenu

In the submenu, a local DNS server can be configured by adding 'IP address—domain name' pairs into the database.



Configuration of domain names

To add the address into the list, fill in the described below fields and click *'Add'* button:

- *IP address* – IPv4-address of host corresponding to the name specified in the *'Domain name'* field;
- *Domain name* – host domain name for access to it.

To remove an address from the list, click the *'Delete'* link next to the selected address.

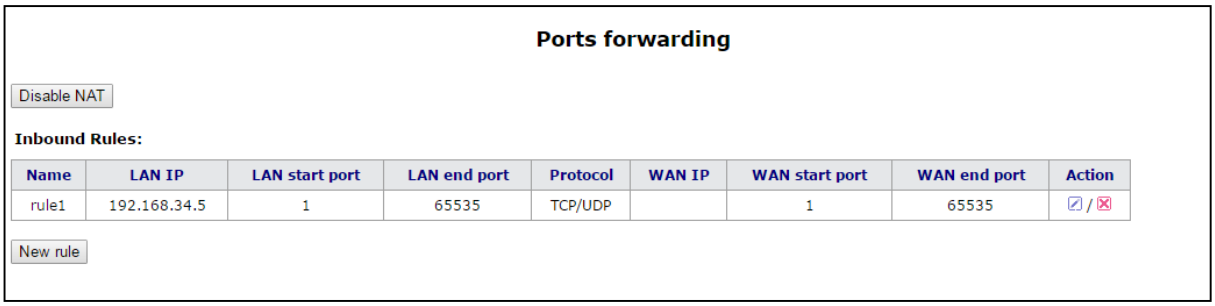
To save changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply* button.

The 'Ports Forwarding' submenu

The submenu is available only for TAU-8.IP-W devices.

In the submenu, you may configure port forwarding from WAN interface to WLAN interface.

NAT (Network Address Translation) allows for IP packet address and network port translation. Port forwarding is required when TCP/UDP connection to a local computer (connected to LAN interface) is established from the external network. In this settings menu, you may define the rules allowing packets to pass from the external network to the specified address in the local network and thus establishing connection. Port forwarding is required when torrent and p2p servers are used. For this purpose, you should identify TCP/UDP ports used by a torrent or p2p client in their settings and assign the respective forwarding rules for your computer IP address.



Configuration of NAT rules:

Network Address Translation (NAT) mode is enabled by default. To disable NAT, click *'Disable NAT'* button.

To add new NAT rule, click *'New rule'* button and fill in the following fields:

- *Name* – service name (this field is required);
- *LAN IP Address* – internal destination IP address – IP address of the host in LAN used for packet translation falling under this rule;
- *Traffic type* – traffic type selection. When *'Any'* value is set, internal destination IP address (*LAN IP address*) is used for all incoming traffic. When you select type *'Specify'*, you may get opportunity to specify some parameters of incoming traffic:
  - *Start port, End port – these two parameters determine the range of port destination on an external network. Received to WAN interface packet will fall under this rule if its destination port locates in specified range;*
  - *Local start port – determine start port of the destination port range in local network for packet retranslation. Terminal port of the range is automatically calculated in the context of range size for the destination ports in external network (defined by the difference between Terminal port and Start port);*
  - *Protocol – selection of the packet protocol falling under this rule: TCP, UDP, TCP/UDP;*
- *WAN IP* – selection of source IP address that sends packets into external networks. When 'Any' value is set, packet translation will be permitted (packets are transmitted from any IP address of external network). When 'specify' type is selected, the packet translation will be permitted into local network (source IP address of packets are equal to value from *IP address* field).

Port forwarding rule will work as follows: If the packet destination port (coming to the device WAN interface) belongs to the range from *'Start port'* to *'Terminal port'*, source IP address is equal to address assigned in *'WAN IP address'* field (if this address is specified). Packet protocol is equal to value from *'Protocol'* field. The packet will be retransmitted to interface's LAN with destination address spoofing to the *LAN IP address* and with destination port spoofing to a value of LAN port range (the start value of the range is determined by *'Start LAN port'* parameter).

To add rule in the table, click *'Save changes' button.* To store settings into the non-volatile memory, click *Apply* button.

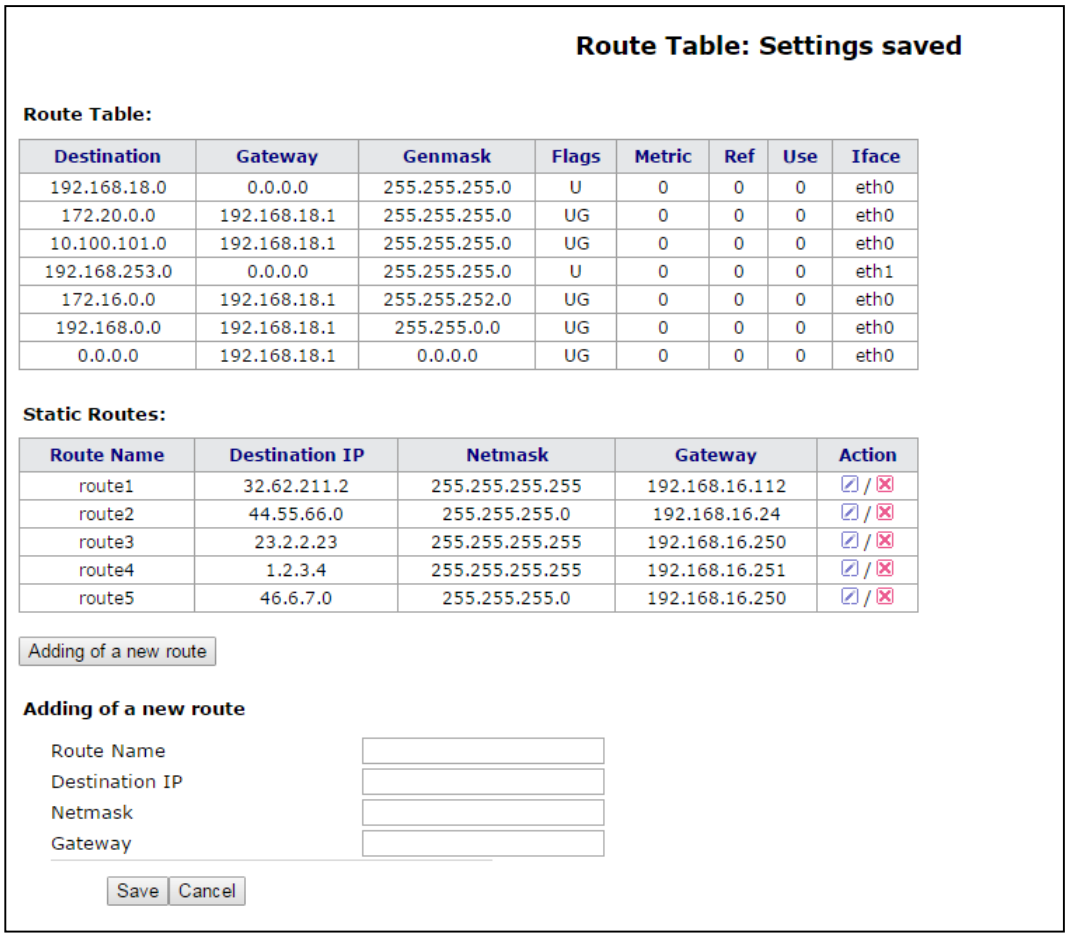
The changes in the submenu are effective immediately after clicking 'Apply Changes' button. Device reboot is not required.

2.2.4 The 'Static routes' submenu

Use the menu to set up static device routs and display current routing table.

Routing table description:

- **Destination** – IP-address of destination network;
- **Gateway** – IP-address of gateway for connection to destination network;
- **Genmask** – subnet mask of destination network;
- **Flags** – route flag:
  - ***G*** *– route uses a gateway;*
  - ***U*** *– route is active;*
  - ***H****—the destination is a separate host;*
  - ***D****—the route was created after receiving a redirected ICMP message;*
  - ***M****—the route was changed by a redirected ICMP message;*
  - ***!****—an inactive route, packets will be rejected;*
- **Metric** – number of steps (hops) to destination place;
- **Ref** – maximum number of data which the system will be able to receive in one packet from the remote computer;
- **Detection (Use)** – specify the value that is used for establishing a connection;
- **Interface (Ifase)** – network interface that the routs lie through.



To add new rout, click ‘Add’ and fill the following fields:

- *Route Name* – rout name (it is used for convenience);
- *Destination IP* – destination address by which rout is established. Destination IP is specified in the IPv4 format (can be subnet address or host address);
- *Netmask* – subnet mask to which rout is created– used in cooperation with destination IP and together they determine network address or host, if mask has value 255.255.255.255);
- *Gateway* – device IP address for connection to the destination network.

To add route in the table, click *‘Save’* button.

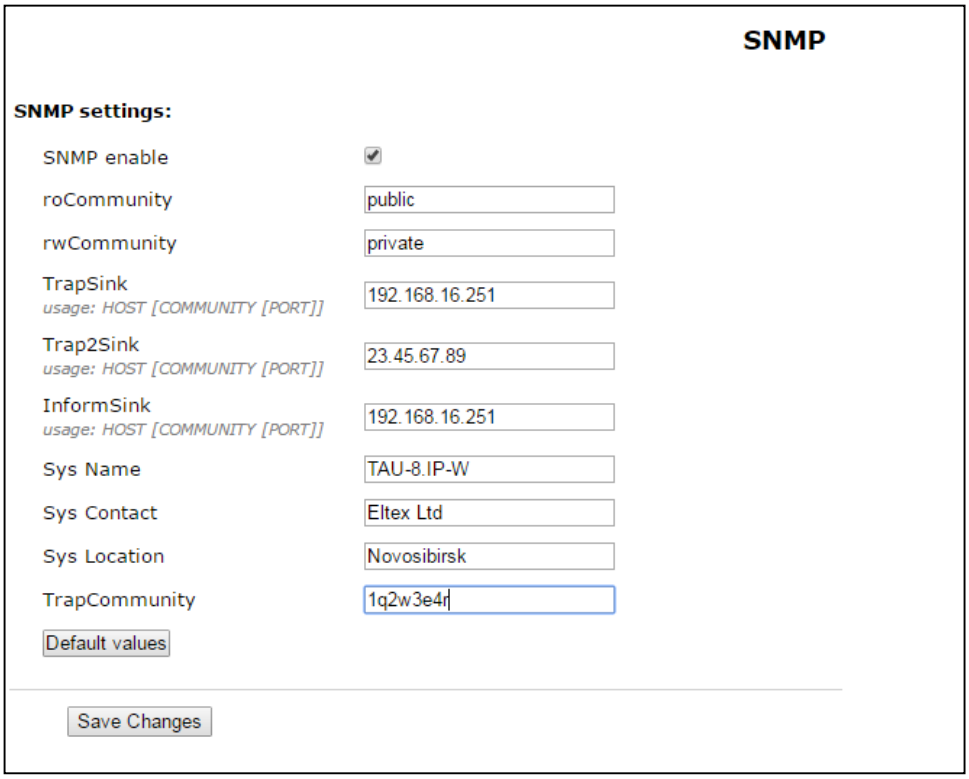
To edit route in the table ‘Static routs’ in the *‘Action’* column, click . To delete - on the icon .

To store changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

2.2.5 The 'SNMP' submenu

Terminal software allows you to monitor status of the device and its detectors, configure and read some settings by using SNMP. In *'SNMP'* menu, you can configure settings of SNMP agent. The device supports SNMPv1 and SNMPv2 protocol version.



SNMP settings:

- *Enable SNMP* – when checked, SNMP will be enabled for utilization;
- *Password on reading (roCommunity)* – password for parameter reading (common: *public*);
- *Password on recording (rwCommunity)* – password for parameter writing (common: *private*);
- *TrapSink* – IP address of SNMPv1-trap message recipient in the format HOST [COMMUNITY [PORT]];
- *Trap2Sink* – IP address SNMPv2-trap message recipient in the format HOST [COMMUNITY [PORT]];
- *Inform(InformSink) (address for receiving of messages)* – IP address of Inform message recipient in the format HOST [COMMUNITY [PORT]];
- Sys Name – *device name;*
- Sys Contact – *contact details of the device vendor;*

- Sys Location – *the device location information;*

- *TrapCommunity* – password enclosed in traps (by default: trap).

In the current firmware version by using SNMP, you may get the device specific statistical information about its network interfaces trough OID 1.3.6.1.2.1.2: network interface list, IP and MAC addresses specified to network interfaces, number of received and transmitted packets, number of received and transmitted bytes, count of errors, losses etc.

The list of objects, that may be read and configured via SNMP, is given below:

- Enterprise.1.3.1 – SIP profile basic settings

- Enterprise.1.3.2.1 – SIP profile settings

- Enterprise.1.1.2.1 – FXS port settings

- Enterprise.1.2.1.1 – FXS profile settings

- Enterprise.1.4.1.1 – call group settings

- Enterprise.1.5 – VAS activation codes for the phone unit

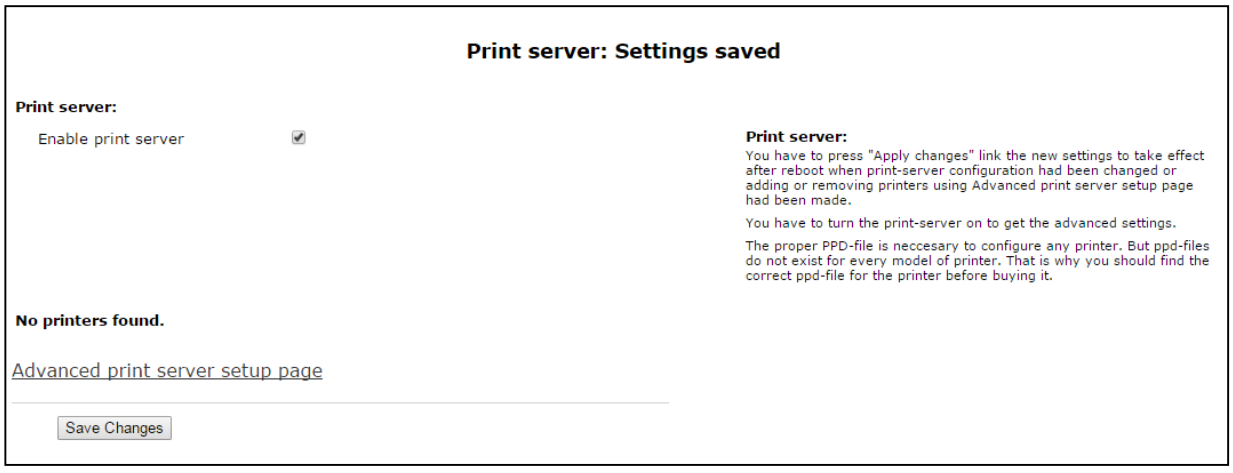
- Enterprise.2.1 – SNMP settings

- Enterprise.3.1 – system log settings. Where Enterprise – 1.3.6.1.4.1.35265.1.55.1 is the TAU-4.IP device identifier and 1.3.6.1.4.1.35265.1.55.2 is the TAU-8.IP device identifier.

To save changes to the RAM of the device, click the *Save Changes* button. To save settings to the non-volatile memory, click *Apply* button.

2.3 The ‘Print Server’ menu

Use the *‘Print server’* menu to configure the print server.



- *Enable print server* – when checked, print server is enabled.

When the printer is connected to the USB port, it should be determined automatically. To configure printer, specify gateway path to the ppd file with detailed information about printer functionality. You may find this ppd file in the web site of printer vendor.

Printer configuration in Windows:

The following steps are required to configure printer in Windows:

Go to ‘Start menu -> ‘Printers and faxes’ and select **‘Installation of new printer’ -> Network printer or printer connected to another PC’ -> ‘Connect to a printer via Internet, home network or intranet’** and enter the URL: *http://server:631/printers/model*

In address, ‘Model’ parameter should be identical to printer name that is displayed on the print page of print server.

Select preferred driver by using installation disk.

Installation is finished.

Advanced printer settings menu can be accessed by clicking the corresponding button.

On the page of advanced settings, you can group printers, control tasks, change printer settings and print text pages. All the necessary information and help with print server settings may be found on the www.cups.org web site.

To save changes to the non-volatile memory, click ‘Apply’ button.

2.4 The ‘PBX’ menu

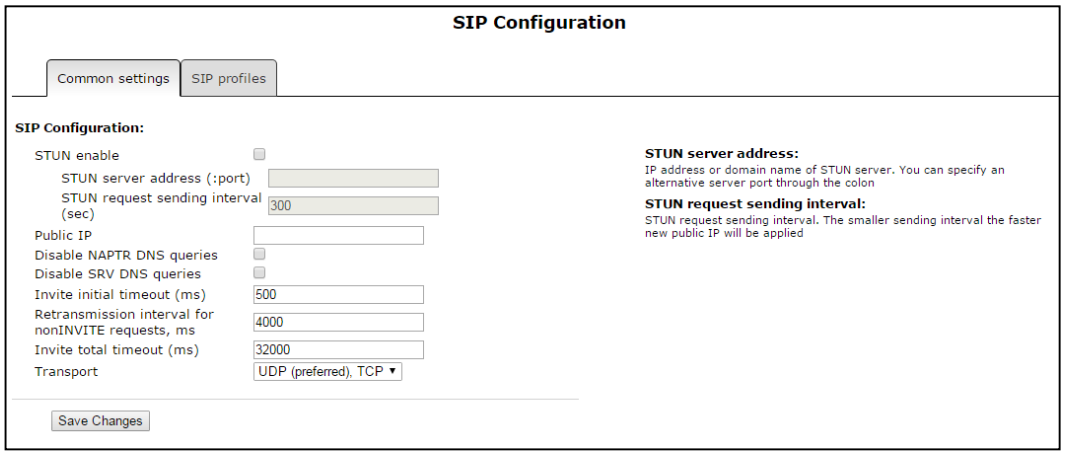
Use ‘PBX’ menu to configure VoIP (Voice over IP): SIP protocol configuration, QoS (Quality of Service) settings, FXS interface configuration, acoustic signal setting of line, setting of call groups and groups of call intercepting, installation of codecs and dial plan.

2.4.1 The ‘SIP’ submenu

Use the menu to configure the device for operation via SIP protocol.

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

Common settings



SIP configuration:

- *STUN enable* – STUN (Session Traversal Utilities for NAT) is used during initialization of STUN server in the network to determine public address (the device external gateway address);

  - *STUN server address (:port) – IP address or domain name of STUN server. Alternative server port can be assigned after colon (the default value is 3478);*

  - STUN request sending interval (sec) – *STUN request sending interval. The less polling interval then higher speed of reaction on the public address changes;*

- *Public IP* – the parameter is used as external device address during work on NAT (on gateway). This parameter is used as a public address of gateway (NAT) WAN interface on which TAU-8.IP is set up. At that, SIP and RTP port forwarding is required (these ports are used by TAU-8.IP);

- *Disable NAPTR DNS queries* – in some cases, when DNS operates incorrectly, NAPTR queries (Naming authority pointer) may cause negative result. When flag is set, these queries will be disabled;

- *Disable SRV DNS queries* – in some cases, when DNS server operates incorrectly, SRV requires may cause negative result. When flag is set, automatic queries will be disabled;

- *Invite initial timeout (ms)* – time interval (in milliseconds) between the first INVITE message transfer and the second INVITE message transfer when the first message is unanswered. This interval will be doubled for the next INVITEs (third, fourth and etc.).(For example, if the second INVITE will be transferred after 300 ms, the third will be transmitted after 600 ms, the fourth - after 1200 ms and etc.);

- *Retransmission interval for nonINVITE requests (ms)* – time interval in milliseconds between the first nonINVITE message transfer and the second nonINVITE message transfer when the first message is unanswered. This interval will be doubled for the next

message transfers (third, fourth etc.).(For example, if the second nonINVITE will be transferred after 300 ms, the third will be transmitted after 600 ms, the fourth - after 1200 ms and etc., up to value of INVITE initial timeout);

- *Invite total timeout (ms)* – total timeout of INVITE message transmission, in milliseconds. Upon timeout of INVITE message transmission (in milliseconds), the selected direction will be not available. It is used to limit INVITE message retranslation including determination of SIP-proxy accessibility*;*

- *Transport* – selecting a transport layer protocol that is used to receive and transmit SIP messages:

  - *UDP (preferred), TCP– receiving via UDP and TCP. TCP is used for packet sending with size more than 1300 bytes, UDP- for packets with size up to 1300 bytes;*

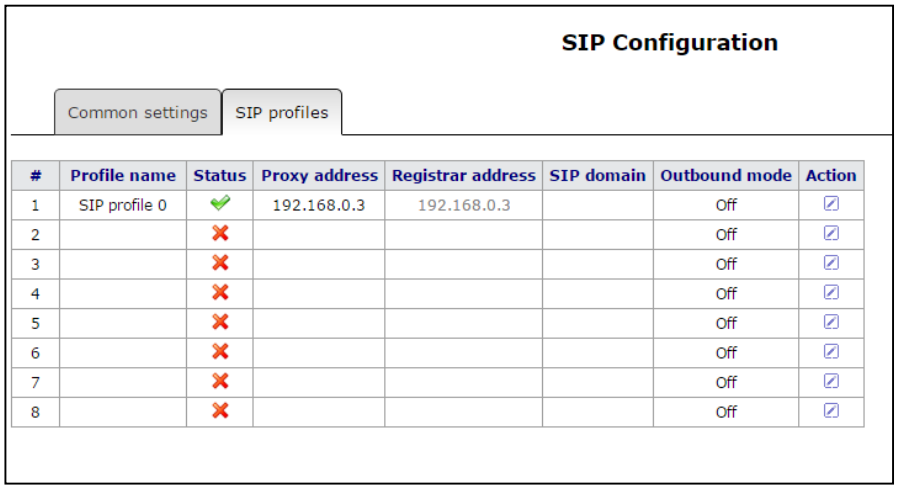
  - *TCP (preferred), UDP – reception via UDP and TCP. Transmission via TCP. If connection is not established via TCP, the transmission will be performed via UDP;*

  - *only UDP – use only UDP protocol;*

  - *only TCP – use only TCP protocol.*

To save changes into the device RAM, click *'Save Changes'* button.

SIP profiles



To edit profile, click button in the column *'Action'* of the *'SIP profiles'* table.

SIP Configuration

Common settings | SIP profiles

#	Profile name	Status	Proxy address	Registrar address	SIP domain	Outbound mode	Action
1	SIP profile 0	✔	192.168.0.3	192.168.0.3		Off	☑
2		✘				Off	☑
3		✘				Off	☑
4		✘				Off	☑
5		✘				Off	☑
6		✘				Off	☑
7		✘				Off	☑
8		✘				Off	☑

Profile:

Profile name: SIP profile 0
Activate profile: ☑

You can not deactivate the profile. It is used by by FXS-ports FXS0, FXS1, FXS2, FXS3, FXS4, FXS5, FXS6 and FXS7

SIP Configuration:

Proxy mode: Homing mode
Proxy address (:port): 192.168.0.3
Registration: ☑
Registrar address (:port): 192.168.0.3
Reserved SIP proxy:
Add
Home server check:
Check method: Invite
Keepalive timeout (s): 35
SIP domain:
Use domain to register: ☐
Outbound mode: Off
Expires: 1800
Registration Retry Interval:
User call (SIP): ◉ 180 Ringing ○ 183 Progress (Early media)
Use SIP Display info in Register: ☐
Ringback at 183 Progress: ☐
Use Alert-Info header: ☐
Remove rejected media: ☐
Check RURI user part only: ☐
100rel: supported
Timer enable: ☑
Min SE, sec: 120
Session expires, sec: 1800
Keep alive NAT sessions:
Mode: Off
Keepalive timeout, s: 30
Three-party conference:
Mode: Local
Conference server: conf
IMS settings:
IMS mode: Off
XCAP name for call hold: call-hold
XCAP name for call waiting: call-waiting
XCAP name for three-party conference: three-party-conference
XCAP name for hotline: hot-line-service
XCAP name for call transfer: explicit-call-transfer

Proxy mode:
"Proxy mode" is the mechanism of working with SIP server.
When "No proxy" mode is selected it is forbidden to make calls or send messages through the SIP server.
When "Homing" mode is selected the device moves to the first reserved SIP server if the home server is not available. After that the device contols the home server periodically with one of the "Check method".
In "Parking" mode the device moves to the first reserved SIP server if the home server is not available without further control of the home server.

Check method:
"Check method" defines one of the three methods used to control availability of the home server in the homing mode. The control may be done by means of sending periodical OPTIONS messages, by means of sending periodical REGISTER meassages or by means of sending INVITE meassage before an outgoing call is made.

Keepalive timeout (s):
"Keepalive timeout" defines the time interval between sending either REGISTER or OPTIONS messages, in seconds.

Outbound mode:
When the mode "**Off**" is chosen, dialplan will be used for call routing. Both "**Outbound**" and "**Outbound with busy**" modes use dialplan for call routing, but all the calls go through a SIP server. The difference between theese two modes is as follows. As for the "**Outbound**" mode, if there is no registration on a SIP server, you will have the oportunity to set some additional services from your phone.
When you choose "**Outbound with busy**" mode, you will not be able to do anything without registration.

Registration Retry Interval:
When the device loses registration it will try to register with the proxy every <Registration Retry Interval> seconds.

Ringback at 183 Progress:
Send ringback to FXS at receiving 183 Progress

Use Alert-Info header:
When enabled, an Alert-Info header field is used to create an alternative cadence for ringing. See page "PBX" - "Cadence" for details.

Remove rejected media:
Tick this option if you want to remove inactive media from the offer SDP despite of RFC3264 requirements. It is recommended to turn this option on when using Iskratel softswitch.

Check RURI user part only:
When activated, an incoming call is accepted when a user part only of Request-URI match detected.
When deactivated, an incoming call is accepted when all the parts of Request-URI (user, host, port) match detected.

100rel:
Off - option 100rel is not supported; Supported - extension 100rel is inserted in Required-header of 1xx-answers only if this extension is supported by a counterparty of a call;
Required - extension 100rel is inserted in Required-header of both Invite message and any 1xx-answers if this extension is supported by a counterparty of a call.

Keep alive NAT sessions:
Keep alive NAT sessions mechanism allows to keep UDP sessions alive when the device is behind the NAT. When using this mechanism you do not need to configure ports forwarding in an external router. UDP sessions keep alive by means of periodical sending one of the followinfg type of a message to a SIP server: OPTIONS, NOTIFY or CLRF.

List of codecs in preferred order:

Dialplan Configuration:

Save | Cancel

Profile:

- *Profile name* – username of configurable profile;
- *Activate profile* – when checked, the profile is active otherwise it is passive;

SIP configuration:

- *Proxy mode* – the device has provided redundancy mechanism of SIP-proxy server (and registration server) since firmware version 1.8.0 thereby you may work through the redundant servers if connection with the main server was lost. You may select one of three SIP server operation modes in the dropdown list:
  - *Disable;*
  - *Parking – SIP-proxy redundancy mode without main SIP-proxy management;*
  - *Homing – SIP-proxy redundancy mode with main SIP-proxy management.*

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

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

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

1. In the 'parking' mode, the main SIP-proxy management is absent, and the gateway will continue operation with the redundant SIP-proxy even when the main proxy operation is restored. If the connection to the current SIP-proxy is lost, querying of the subsequent SIP-proxies will be continued using the algorithm described above. If the last redundant SIP-proxy is not available, the querying will continue in a cycle, beginning from the main SIP-proxy.
2. In the 'homing' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing

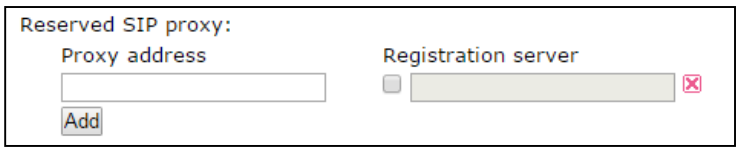
outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then to the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, gateway will renew its registration. Gateway begin operation with the main SIP-proxy.

- *Proxy Address (:port)* – network address of a SIP server—device that manages access to provider's phone network for all subscribers. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060.

- *Registration* – when checked, register ports that utilize this profile on registration server;

- *Registrar address (:port)* – network address of a device that is used for registration of all phone network subscribers in order to provide them with the communication services (specify registration server UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name. Usually, registration server is physically co-located with SIP proxy server (they have the same address);

Reserved SIP proxy – addition reserved SIP-proxy addresses:



- *Proxy address* – network address of the reserved SIP-server;

- *Registration server* – to specify registration server you should set flag before the field and enter a registration server address of a reserved proxy;

To add reserved SIP server, click *'Add'* button. To delete it, click ☒ button opposite to server.

- *Home server check* – check availability of the main SIP server in the Homing mode;

- *Check method* – method selection to check availability of the main SIP server in the 'Homing' mode:

  - *Invite – transmission of INVITE request to its address when performing an outgoing call;*

  - *Register – periodic transmission of REGISTER messages to its address;*

  - *Options - control by periodic sending OPTIONS messages to its address;*

- *Keepalive timeout (s)* – periodic message transmission interval in seconds; used for primary SIP server availability check;

- *SIP domain* – domain where the device is located (fill in if required);

- *Use domain to register* – use the domain during registration. In this case, domain will be transmitted into Request URI of ‘REGISTER’ request;

- Outbound proxy – ‘Outbound’ mode:

  - *Off - route the calls according the dialplan;*

  - *Outbound - dialplan is needed for outgoing connection, but all calls will be routed by SIP-server; in case of registration absence subscriber will get station reply, to manage subscriber service (Supply services management);*

  - *With busy tone - dialplan is needed for outgoing connection, but all calls will be routed by SIP-server; in case of registration absence VOIP will be unavailable: error tone will be output in the phone. 'Outbound’ mode is analogue to the device operation with dialing plan (x.);*

- *Registration renewal time period (Expires)* – time for subscriber port registration on SIP server. At the average, port registration renewal will be performed after 2/3 of the specified period;

- *Registration Retry Interval* – when the registration is unsuccessful, time period between SIP server registration attempts;

- *User call (SIP):*

  - *180 Ringing - 180 reply is sending to caller equipment; caller equipment should output local ringback tone in line after getting this message;*

  - *183 Progress with SDP - 183+SDP reply is sending to caller equipment; used for frequency path forwarding to callee reply. In this case, TAU-8.IP will remote send ringback tone to caller.*

- *Use SIP Display info in Register* – when checked, use username in 'SIP Display Info' field of the 'Register' message;

- *Ringback at 183 Progress* – when checked, 'ringback' tone will be sent upon receiving '183 Progress' message (w/o enclosed SDP);

- *Use Alert-Info header* – 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 the section 2.4.9 The ‘Cadence’ submenu;

- *Remove rejected media* – when option is enabled, passive media will be excepted from offer-SDP against the RFC3264 advice. Enable the option for coordination with Iskratel equipment;

- *Check RURI user name only* - when checked, only subscriber number (user) will be analyzed, and if the number matches, the call will be assigned to the subscriber port. If

unchecked, 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.

- *Transmit symbol '#' as %23* – when checked, send hash symbol (#) in SIP URI as escape sequence '%23', otherwise–as '#' symbol.

- 100rel – utilization of reliable provisional responses (RFC3262):

  - *Supported – reliable provisional responses are supported;*

  - *Required – reliable provisional responses are mandatory;*

  - *Disabled — reliable provisional responses are disabled;*

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.

- *Enable timer* – when checked, enables support of SIP session timers (RFC 4028). After connection establishment, if both sides are supporting timer, one of them periodically send re-INVITE queries for connection control (if both sides are supporting UPDATE method (it should be pointed in 'Allow' header) session update is being processed by periodical UPDATE messages sending); The following settings are available for configuring:

  · *Minimal session time (Min SE, sec) – minimal time interval for connection health checks (90 to 1800s, 120s by default). The value shouldn't be more then value specified in the field 'Session time';*

  · *Session expires, s – period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 80000s, recommended value–1800s, 0–unlimited session);*

- *Periodic SIP server polling (Keepalive NAT sessions)* – allows you to support active UDP-session when you work on NAT. It obviates the necessity to create the rules of port forwarding on the external router. Session activity is supported by periodical sending one of the message types to SIP server: OPTIONS, NOTIFY or CLRF.

  · *Mode – message type selection for sending to SIP server (OPTIONS, NOTIFY or CLRF), Off – disable SIP server polling;*

  · *Keepalive timeout, s – SIP server polling time period to support active UDP connection;*

- *Three-party conference* – service provides establishing connection between three subscribers;

  Mode – selection of three-party operation mode:

  · *Local – conference assembly is performed locally by the TAU-8.IP device after pressing 'flash+3'; operation mode algorithm is described in the section 4.3.1;*

  · *Remote (RFC4579) - conference is intended on remote server. Then, after pressing 'flash+3' combination Invite message sending on server to number, pointed in the 'Conference server' field. In this case conference processing by algorithm, described in RFC4579. For detailed description, see section 4.3.2.*

- *Conference server* - conference connection establishment server address processed by algorithm, described in RFC4579. Address sets in SIP-URI format: user@address:port. It is available to set only user part URI - in this case Invite message will be sent to SIP proxy address.

- IMS settings:

- *IMS mode* – service control configuration:

  - *Service (simulation service) management using IMS (3GPP TS 24.623)*

  - *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.*

- *'Call Hold' service name* - XML element name in Notify message body, used for transmission of commands to activate/deactivate 'Call Hold' service. Example: if service name has 'call-hold' value, activation command will appear as:

  <call-hold active="true"/>,

  and deactivation command:

  <call-hold active="false"/>

- *'Call Hold' service name* - XML element name in Notify message body, used for transmission of commands to activate/deactivate 'Call Hold' service. Example: if service name has 'call-waiting' value, activation command will appear as:

  <call-waiting active="true"/>

  and deactivation command:

  <call-waiting active="false"/>

- *'3-way Conference' service name* - XML element name in Notify message body, used for transmission of commands to activate/deactivate '3-way Conference' service. Example: if service name has 'three-party-conference' value, activation command will appear as:

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

  and deactivation command:

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

- *'Hot Line' service name* - XML element name in Notify message body, used for transmission of commands to activate/deactivate 'Hot Line' service. Activation command sending Hotline phone number and call timeout. Example: if service name has

'hot-line-service' value and it is needed to perform a call to number 30001 after 6 seconds after on-hook, activation command will appear as:

<hot-line-service>

<addr>30001</addr>

<timeout>6</timeout>

</hot-line-service>

If activation command is not received 'Hot Line' service will be disabled.

- *'Call Hold' service name* - XML element name in Notify message body, used for transmission of commands to activate/deactivate 'Call Hold' service. Example: if service name has *'call-transfer'* value, activation command will appear as:

  < call transfer active="true"/>,

  and deactivation command:

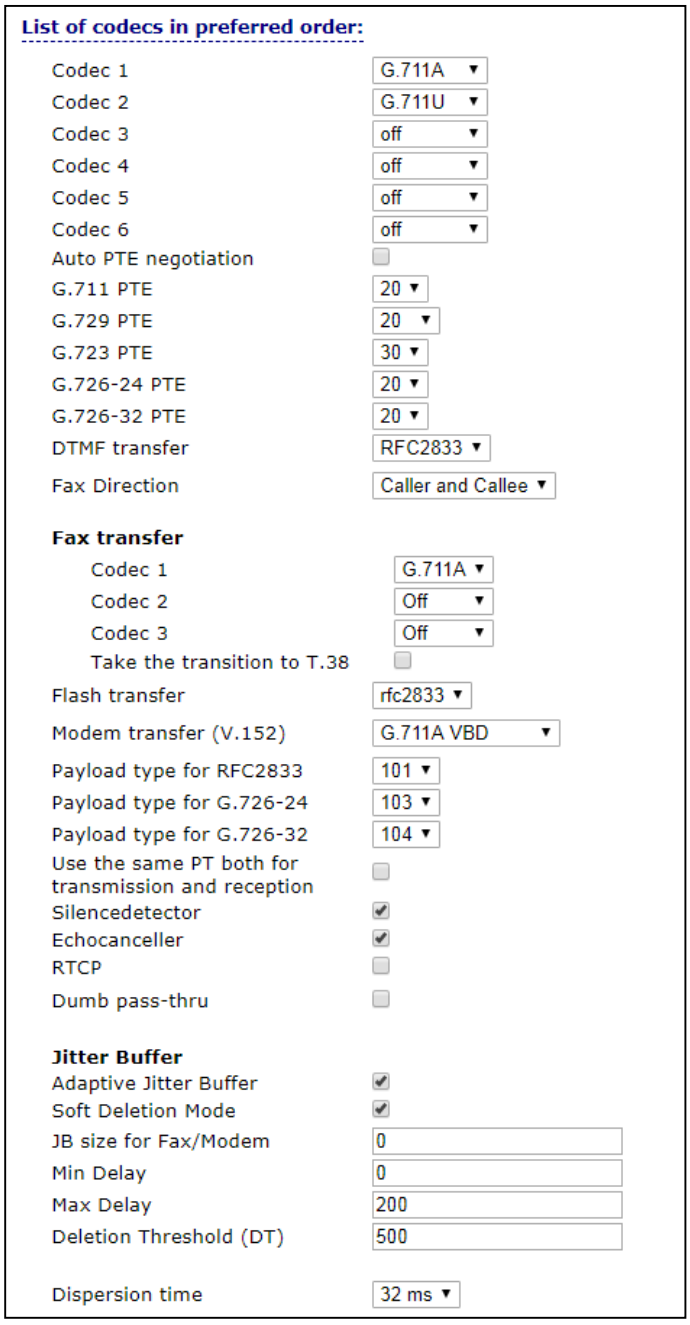
  < call transfer active="false"/>

To save changes into the RAM of the device, click *'Save'* button. To exit from editing mode without saving, click *'Cancel'* button.

List of codecs in order of preference:

- *Codec 1..6* - you may select a codec and an order of their usage when connection is established. The highest priority codec should be specified in the 'Codec 1' field. For operation, you should specify at least one codec: In the drop-down list of this field, the codec is selected:
  - *G.711A;*
  - *G.711U;*
  - *G.723;*
  - *G.729;*
  - *G.729A;*
  - *G.729B;*
  - *G.726-24;*
  - *G.726-32;*

- *off - codec is not used.*



- *Autonegotiation of packetization time* – when checked, packetization time adjusts to RTP stream packetization time of counter side;

- *Packetization time for G.711/G.729/G.723/G.726-24/G.726-32, ms* – count of ms in one RTP packet for G.711A, G.711U, G.729, G.723, G.726-24 and G.726-32 codecs correspondingly;

- *DTMF transfer* – DTMF signal transmission method:

  - *Inband – inband transmission;*

- *RFC2833–according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;*
- *SIP Info - transmission of the messages via SIP in INFO queries.*
  - 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).

- *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 – 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;*
  - *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;*

Fax transmission may be implemented using voice codec 711 or special codec for facsimile codec t/38 messages transmission.

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.

- *Fax transfer codec 1...3* - allows you to select codecs and an order of their usage. Codec with the highest priority should be placed in 'Fax codec 1' field. For processing it is necessary to point at least one codec:
  - *Off - codec is not using.*
  - *G.711A–use G.711A codec;*
  - *G.711U–use G.711U codec;*
  - *T.38 - use T.38 protocol.*

All fax codecs should be different! In addition when selecting G.711a or G.711u relevant codec should be active in the list of device voice codecs.

- *Take the transition to T.38* – when checked, incoming *re-invite* to T.38 from the opposite gateway otherwise it will be enabled;

- *Flash transfer* – Flash transmission way:

  - *off — Flash transmission disabled;*

  - *RFC2833 – Flash transmission is performed according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;*

  - *info – transfer 'flash' via SIP protocol. INFO messages are used for SIP protocol and flash signal view will depend on MIME expansion type;*

When choosing the option 'Transmit Flash: info' with 'Type of flash message': dtmf-relay' when generating SIP INFO for flash, the extension specified for DTMF transmission of SIP INFO messages is used

- *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 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.*

The chosen codec should be active in voice codecs list too.

- *Payload type for RFC2833 packets* – payload type for packets transmission via RFC2833 (permitted values: 96 to 127);

- *Use the same PT both for transmission and reception* – when checked, use the same type of payload for transmission and reception;

- *Silencedetector* – when checked, use silence detector otherwise do not use it;

- *Echocanceller* – when checked, use echo canceller otherwise do not use it;

- *RTCP* - when checked use RTCP for voice channel control: The following parameters are available for editing:

  - *Sending interval – interval of message transmission via RTCP protocol, in seconds;*

  - *Receiving period – RTCP packet receiving period. Assigned in the units of transmission period. The device breaks connection if no one packet will be received via RTCP protocol from the opposite site during the receiving period;*

- *Dumb pass-thru:*

  - *VBD codec – codec selection (G.711A or G.711U) to transmit data in voice channel;*

  - *Payload type – payload type of voice channel data transmission (acceptable values for use are 0, 8, and the range from 96 to 127). Setting is used for modem data transmission when codec and payload type of RTP opposite side are changed during transition to modem.*

Jitter Buffer compensates jitter effect. Received packets on the reception side will be not reproduced immediately; they will be reproduced with the delay, which is unnoticed by man. However, this delay allows you to improve quality of voice transmission in case of jitter.

- *Adaptive Jitter Buffer* – when checked, buffer size will change from minimum to maximum automatically. Otherwise, buffer size will be fixed and equal to maximum size of adaptive jitter buffer;

- *Soft Deletion Mode* – when checked, to improve the quality of voice transmission the packets are not dropped immediately when they achieve maximum value of jitter buffer. They will be dropped in the period of deletion threshold expiration. Otherwise the packets will be deleted immediately after achieving max value of jitter buffer;

- *JB size for Fax/Modem* – time interval of packet collecting during fax/modem transmission (available values are from 0 to 200 ms);

- *Min Delay, ms* – minimum size of jitter buffer (acceptable value range is from 0 to 200 ms, but no more than max value of jitter buffer);

- *Max Delay, ms* – upper limit (maximum size) of jitter buffer (acceptable value range is from 0 to 200 ms);

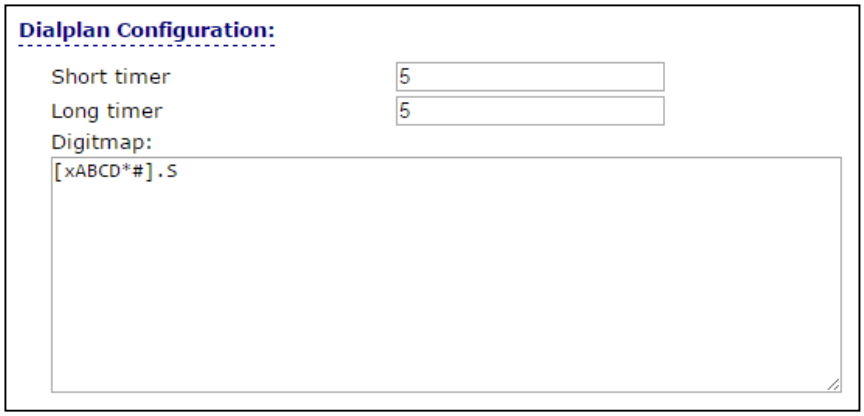
- *Deletion Threshold (DT)* – time period, after that, in 'Soft' mode, all packets will be deleted immediately (acceptable value range is from 0 to 500 but no less then max value of jitter buffer);

- *Dispersion time* – parameter to determine time after which reflected signal will achieve initial source of the signal (available values are 8, 16, 32, 48, 64 ms).

To save changes into the RAM of the device, click *'Save'* button. To exit from editing mode without saving, click *'Cancel'* button.

Dialplan Configuration:

Dialplan of the device is configured in the block shown below.



Dialplan is assigned by regular expressions. Structure and format of regular expressions providing various capabilities of dial number are shown below.

To save changes into the RAM of the device, click *'Save'* button. To exit from editing mode without saving, click *'Cancel'* button.

Regular expression structure:

Regular expression on TAU-8.IP may be described by digits and special symbols as well as their combination.

- The basis is the designations for recording a sequence of dialed digits. Dialed digits sequence is recording using several designations: digits dialed from the phone keypad: 0, 1, 2, 3, …, 9, #, and *. 0, 1, 2, 3, …, 9, # and *.

Symbol '#' usage in dialplan can block end of dial by this key!

- Digit sequence enclosed in square brackets corresponds to any of the characters enclosed in brackets.

  · *Example: ([1239]) - corresponds to any of these digits: 1, 2, 3 and 9.*

- Symbol range may be set through the dash. Most often used inside square brackets.
  - *Example 1: (1-5) - any digit from 1 to 5.*
  - *Example 2: ([1-39]) - example from previous paragraph with other record format.*
- Symbol 'X' corresponds to any digit from 0 to 9.
  - *Example: (1XX) - any three-digit number, starting at 1.*
- '.' - Previous symbol repeating from 0 to infinity.
- '+' - Previous symbol repeating from 1 to infinity.
- {a,b} - Previous symbol repeating from 'a' to 'b' times;
- {a,} - Previous symbol repeating less than 'a' times;
- {,b} - Previous symbol repeating less than 'b' times.
  - *Example: (810X.) – international number with any digits amount.*

Settings that affect dialplan processing:

- *Interdigit Long Timer* – entry timeout for the next digit, if there are no templates that correspond to the dialed combination;
- *Interdigit Short Timer* – entry timeout for the next digit. If the dialed combination fully corresponds to at least one template and if there is at least one template that requires an extension dialing for the full matching.

Additional features:

1. Dialed sequence replacement

Syntax: ***<arg1:arg2>***

This ability allows replacing the dialed sequence with any dialed symbols sequence. In doing so, the second argument should be set as a defined value. Both arguments can be empty.

- *Example1: (<83812:> XXXXXX) - this record will comply with dialed digits 83812, but this sequence will be omitted and will not be transmitted to SIP server.*
- *Example2: (<8:7>123) – this record will correspond to dialed digits 8123, however 7123 sequence will be transmitted to the SIP server.*

2. Tone insert into dial

   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.

   - *Example: (8, 770) - after digit 8 a continuous tone will output when dialing number 8770.*

3. Number dialling deny.

   If at the end of pattern add symbol '!' the dialling of numbers corresponding to the template will be blocked.

   - *Example: (8 10X xxxxxxx ! | 8 xxx xxxxxxx) - expression allows dialling only intercity numbers and exclude international calls.*

4. Replacement of number dialling timers values

   Timer values may be specified for a complete dialplan, as well as for the specific pattern. Character 'S' is responsible for *'Interdigit Short Timer'* setting and 'L' for *'Interdigit Long Timer'*. Timer values may be specified for all templates in a dialplan if values are listed before the opening parenthesis.

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

   If these values are listed in one sequence only, they are effective only for this sequence. In this case, a colon should not be set between timeout key and value; a value can be placed in any part of pattern.

   - *Example: (S4 8XXX. | XXX) uлu ([1-5] XX S0) - entry will call instant call transmission when three-digit number starting at 1, 2, ..., 5 is dialed.*

5. Direct address dial (IP Dialling)

   Symbol '@', setted after number, means that server address, where call will be transmitted will be setted next. We recommend to use *'IP Dialling'* and receive and transmission of call without registration *('Call Without Reg', 'Answer Without Reg')*. It may help in case of server failure.

   Moreover, IP Dialing address format can be used in numbers intended for call forwarding.

   - *Example 1: (8 xxx xxxxxxx) - 11-digit number, starting at 8.*

   - *Example 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) - 11-digit number, starting at 8; add 8495 to transmitting number if 7-digit number is entered.*

- *Example 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) - the emergency services and some intercity numbers dialing.*

- *Example 4: (S0 <:82125551234>) - specified number speed dial, 'Hotline' mode analogue on another gateways.*

- *Example 5: (S5 <:1000> | xxxx) - this dialplan allows to dial any number, that consists of digits, and if nothing input during 5 seconds call number 1000 (e.g. it's a receptionist).*

- *Example 6: (*5x*xxxx*x#|*2x*xxxxxxxxxx#|#xx#|[2-7]xxxxx|8,*

- *[2-9]xxxxxxxxx|8, 10x.|1xx<:@10.110.60.51:5060>).*

- *Example 7: (1xx|0[1-9]|00[1-8]|*5x*xxxx*x#|*2x*xxxxxxxxxx#|#xx#|[2-7]xxxxx|8,*

- *[2-9]xxxxxxxxx|8, 10x.).*

Sometimes it is needed to perform calls locally within the device. In so doing, if device IP address is unknown or periodically changing, it is convenient to use reserved '{local}' word as server address; it means that device will transmit related number sequence to own device address.

- *Example: (123@{local}) - Call on number 123 will be locally processed within the device.*

6. Configuration of pickup codes

   Using this command, you are able to set pickup code for assigned group.

   Syntax: ***ABC@{pickup:X}***

   where *ABC – pickup code (e.g. *8)*;

   X - pickup group number (enumeration from 0).

   - *Example: 112@{pickup:0} - subscribers A and B are belong to one pickup group with index 0. In case when subscriber A receiving incoming call, subscriber B can pickup the call using digit combination 112.*

7. Codec assigning for directions

   In dependence on call direction, you may use different codecs. This setting is more priority than common codec settings (see section 2.4.1 The 'SIP' submenu).

   Syntax: ***'call direction' (codecs: codec1, codec2, codec3, codec4)***

where codec1, codec2, codec3, codec4 – codecs used on assigned direction in priority order

- *Example: XXXX@10.16.24.5 (codecs: g723, g711u, g711a, g729a) – g.723 (in this case priority is highest) g.711u, g.711a and g.729a (codec is assigned as final, priority is lowest) codecs will be used for calls to XXXX@10.16.24.5. You should also not forget that you cannot use more than one version of the g.729 codec at the same time.*

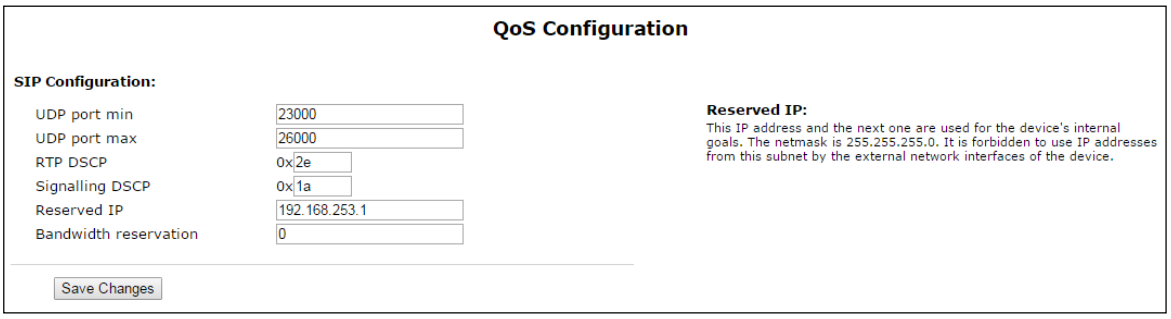
To save changes into the RAM of the device, click *'Save'* button. To exit from editing mode without saving, click *'Cancel'* button.

To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

2.4.2 The 'QoS' submenu

Use this menu to configure QoS parameters.



QoS Configuration

- *Minimal port number for UDP connections (UDP port min)* – the lower limit of the RTP port range used for voice traffic transmission;
- *Maximal port number for UDP connection (UDP port max)* – the upper limit of the RTP port range used for voice traffic transmission;
- *RTP DSCP* – DSCP field value of IP packet header for voice traffic (it is set for hexadecimal number system);
- *Signalling DSCP* – DSCP field value of IP packet header for signal traffic (it is set for hexadecimal number system);
- *Reserved IP* – this IP address and the next IP will be reserved for internal the device requirements. 255.255.0 is subnet mask. It is not recommended to assign IP addresses from the subnet on external network interface;

To store changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

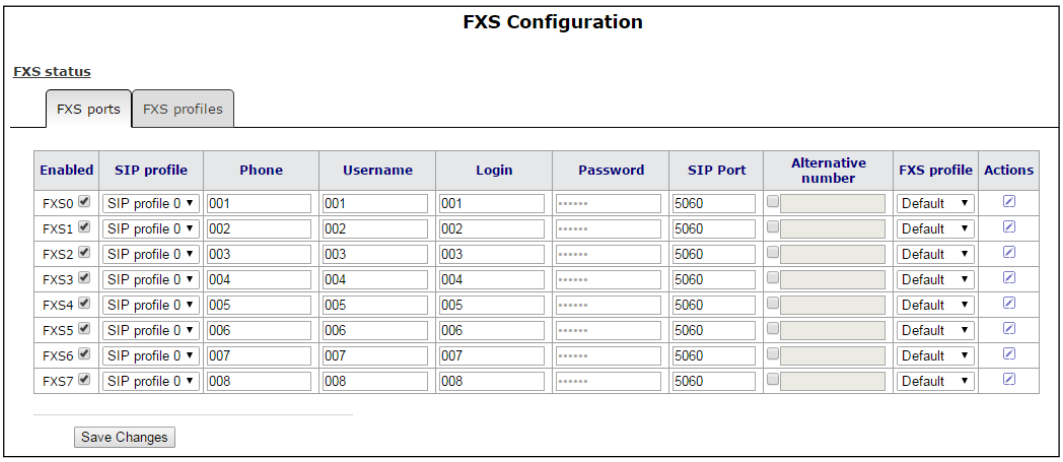
2.4.3 The 'FXS' submenu

Use the menu to configure subscriber line unit of the device.

For physical line parameters, you may create separated FXS profiles. It is handy tool for device configuration when customer units have the same parameters. In this case, it is sufficient to configure one FXS profile with required line parameters after that specify this profile to each FXS port.

FXS ports

For fast transition to *'Status/Telephony'* submenu, click *'FXS status'* (section 3.2.8) where monitoring statistic of customer unit status, call groups and series selection groups are available.

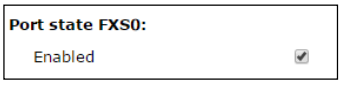


- *FXS profile* – when *'No profile'* value is set – line physical parameters are assigned for all FXS port individually otherwise configuration of one from assigned FXS port is used for customer unit physical parameters (section **FXS profiles**).

To edit customer unit settings, click button in *'Action'* colon of common table.

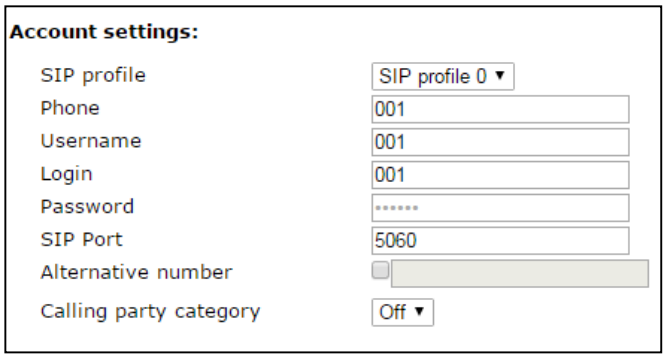
Full list of customer port parameters is shown below.

Port status:



- *Enabled* – when checked, port is enabled otherwise-disabled;

Account settings:

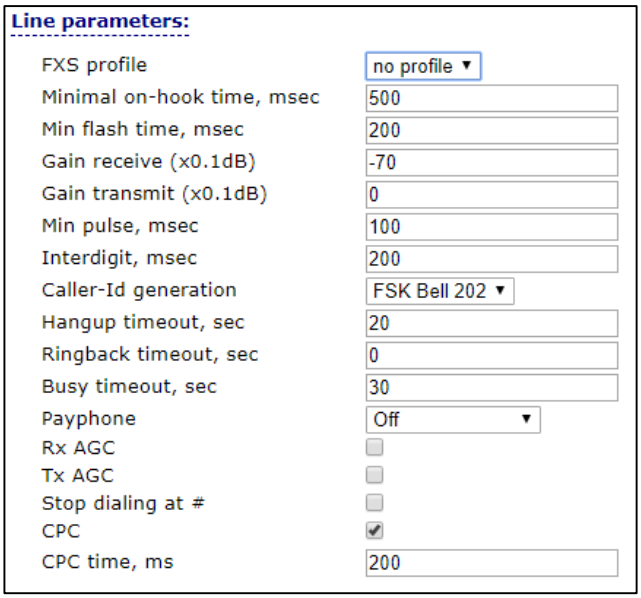


- *SIP profile* – selecting SIP profile from the list of available profile (you may configure SIP profile in the *'PBX/SIP'* menu);
- *Phone* – subscriber number assigned to the phone port.
- *Username* – username associated with port;
- *Login* – username for authentication on SIP server (and on registration server);
- *Password* – password for authentication on SIP server (and on registration server);
- *SIP port* – UDP port to receive SIP incoming messages by account and transmit output SIP messages from the account. May take values from 1 to 65535. The default value is 5060;
- *Alternative number* – user alternative number (when flag is set on the left side of field, parameter is active). 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);
- *Calling party category* – set the number identifying blocker category of subscriber (1-10), category is not used by default.

Line parameters:

- *FXS profile* – selecting user profile for subscriber line parameters. You can configure group of parameters in the *'FXS profiles'* tab.

The selector value *'No profile'* includes individual FXS port settings:



- *Minimal on-hook time* – min clearback detection time, in milliseconds. At that, this parameter represents the max flash detection time.

- *Min flash time* – min time of flash detection, in ms;

- *Gain receive (x0.1dB)* – received signal gain (transmitted into the phone handset), measurement unit—0.1dB;

- *Gain transmit (x0.1dB)* – transmitted signal gain (received by the phone handset microphone), measurement unit—0.1dB;

- *Min pulse* – configuration is required for pulse dialling mode;

- *Interdigit* – configuration is required for pulse dialling mode;

- *Caller-ID generation* – select mode for Caller ID generation. For Caller ID operation, subscriber's phone unit must support the selected method.

  - *Off - Caller ID is disabled;*

  - *Dtmf–DTMF Caller ID method. Issuing a number is made after each call on the line with dual-frequency DTMF signals;*

  - *FSK BELL 202, FSK V.23 – FSK Caller ID method (using BELL 202 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.*

  - *Rus AON–'Russian Caller ID' method. A number is issued by 'Caller ID' request signal of callee phone;*

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

In FSK BELL 202 and FSK V.23 modes, Caller ID information is sent in SDMF format: time/data and number.

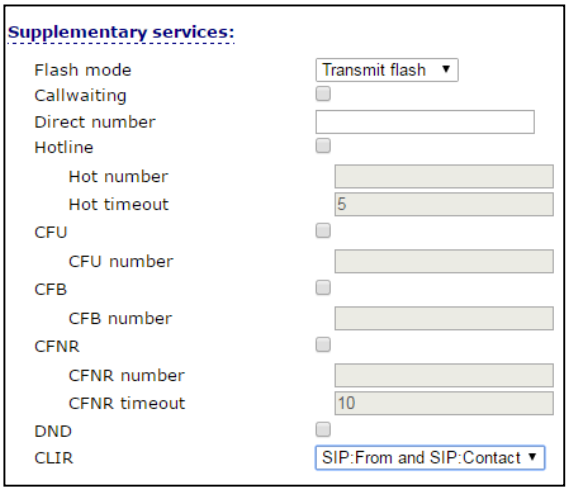
- *Hangup timeout, sec* – dialing timeout for the first digit of a number. When there is no dialing during the specified time, 'busy' tone will be sent to the subscriber, and the dialing will end;
- *Ringback timeout, sec* – 'busy' tone timeout for the subscriber. If the subscriber doesn't put the phone onhook until the timeout expires, an error tone will be sent into the line.
- *Busy timeout, sec* – launches when an incoming call is received and defines the maximum call response time. When the defined timeout expires, busy tone will be sent to the remote subscriber.
- *Payphone* – port operates in payphone mode:
  - *Off – normal mode, payphone is disabled;*
  - *Polarity reversal – payphone operation mode with polarity reversal. Perform line power polarity reversal on subscriber's response, and return it to original state on;*
  - *12 kHz – when there is an outgoing call, tariff pulse with 12 kHz frequency will be sent in the line one time per second[9];*
  - *16 kHz – when there is an outgoing call, tariff pulse with 16 kHz frequency will be sent in the line one time per second[10];*
- *Rx AGC* – when selected, a received signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise—the amplification will not be carried out.
- *Rx AGC Level* – determines the value of the level to which an analogue signal will be amplified when receiving (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).
- *Tx AGC* – when selected, a transmitted signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise—the amplification will not be carried out;
- *Tx AGC Level* – determines the value of the level to which an analogue signal will be amplified when transmitting (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).
- *Stop dialing #* – when selected, use # button on the phone unit to end the dialling, otherwise # will be recognized as a part of the number.

[9] Available only in previous versions of TAU-4/8(W).IP
[10] Available only in previous versions of TAU-4/8(W).IP

- *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 short-term subscriber loop rupture (range from 200 to 3000 ms);

Supplementary services:



- *Flash mode* – flash function operation mode (short clearback):

  · *Transmit flash – transmit flash into the channel using one of the methods described in 'Profiles' tab, 'Flash transmission' parameter);*

  · *Attended calltransfer – flash dialing will be processed locally by the device (call transfer will be performed when the connection with the third party is established). For the 'Attended calltransfer' detailed operation algorithm see in the section 4.1;*

  · *Unattended call transfer – flash will be processed locally by the device (call transfer will be performed when the subscriber finishes dialling a third party number). For the Unattended call transfer detailed operation algorithm, see the section 4.1;*

  · *Local call transfer - call transmission within device, without REFER message sending. For the Local call transfer detailed operation algorithm, see the section 4.1.*

- *Callwaiting* – when checked, *'Call waiting'* service will be enabled otherwise - disabled (this service is available in 'flash—call transfer' function operation mode);

- *Hotline/warmline* – when checked, *'Hotline/warm line'* service is enabled. This service allows establishing an outgoing connection automatically without dialling the number after the phone handset is picked up with the defined delay (in seconds). When checked, fill in the following fields:

  · *Hotline/warmline number – phone number that will be used for connection establishment upon Delay timeout expiration after the phone handset is picked up*

(in SIP profile being used, a prefix for this direction should be defined in the numbering schedule).

- *Delay timeout, seconds – time interval that will be used for connection establishment with the opposite subscriber, in seconds. When set to 0, the connection will be established immediately.*

- *Call forward unconditional* – when selected, CFU (Call Forward Unconditional) service is enabled—all incoming calls will be forwarded to the specified call forward unconditional number. When checked, fill in the following fields:

  - *Call forward unconditional number – number that all incoming calls will be forwarded to when Call forward unconditional service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule).*

- *Call forward on busy* – when selected, CFB (Call Forward on Busy) service is enabled—forward the call to the specified number, when the subscriber is busy. When checked, fill in the following fields:

  - *Call forward on busy number – number that all incoming calls will be forwarded to when the subscriber is busy (in SIP profile being used, a prefix for the specific direction should be defined in the numbering schedule).*

- *Call forward on no answer* – when selected, CFBNA (Call Forward on no Answer) service is enabled—forward the call when there is no answer from the subscriber. When checked, fill in the following fields:

  - *Call forward on no answer – number that incoming calls will be forwarded to when there is no answer from the subscriber and Call forward on no answer service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule)*

  - *No answer timeout, seconds – time interval that will be used for call forwarding when there is no answer from the subscriber, in seconds.*

- *Do not disturb* – when selected, temporary restriction is placed for incoming calls (DND service).

- *CLIR* – caller ID service restriction:

  - *Disable – CLIR service is disabled;*

  - *SIP:From – 'anonymous' will be sent in the 'From' header of 'SIP' message;*

  - *SIP:From and SIP:Contact – «anonymous» will be sent in the 'From' and 'Contact' headers of SIP messages.*

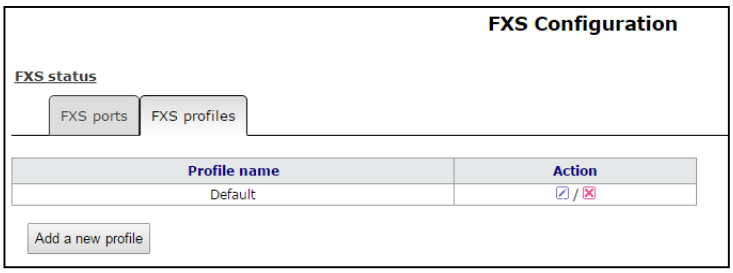
When multiple services are enabled simultaneously, the priority will be as follows (in the descending order):

- CFU;
- DND;
- CFB, CFNA.

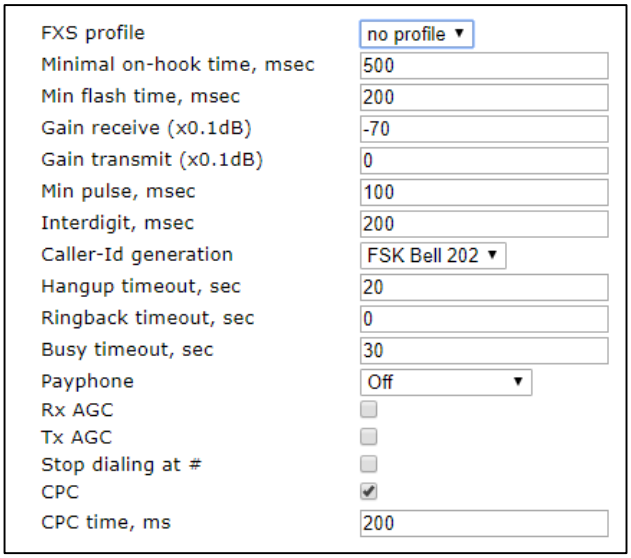
FXS profiles

For fast transition to *'Status/Telephony'* submenu, click *'FXS status'* (section 3.2.8) where monitoring statistic of customer unit status, call groups and series selection groups are available.

Delete profile is not recommended, if it is used by only one port.



Click button in *'Action'* column of 'FXS profiles' table to edit profile. To delete - on the icon . To add new profile, click *'Add new profile'* button. The list of FXS profile settings is shown below.



- *Profile name* – user-friendly profile name;
- *Minimal on-hook time, sec* – minimal clearback detection time, in milliseconds. At that, this parameter represents the maximum flash detection time;
- *Min flash time* – min time of flash detection, in ms;
- *Gain receive (x0.1dB)* – received signal gain (transmitted into the phone handset), measurement unit—0.1dB;

- *Gain transmit (x0.1dB)* – transmitted signal gain (received by the phone handset microphone), measurement unit—0.1dB;

- *Min pulse* – configuration is required for pulse dialling mode;

- *Interdigit* – configuration is required for pulse dialling mode;

- *Caller-ID generation* – select mode for Caller ID generation. For Caller ID operation, subscriber's phone unit must support the selected method.

  - *Off - Caller ID is disabled;*

  - *Dtmf–DTMF Caller ID method. Issuing a number is made after each call on the line with dual-frequency DTMF signals;*

  - *FSK BELL 202, FSK V.23 – FSK Caller ID method (using BELL 202 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.*

  - *Rus AON–'Russian Caller ID' method. A number is issued by 'Caller ID' request signal of callee phone;*

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

In FSK BELL 202 and FSK V.23 modes, Caller ID information is sent in SDMF format: time/data and number.

- Hangup timeout, sec – dialing timeout for the first digit of a number. When there is no dialing during the specified time, 'busy' tone will be sent to the subscriber, and the dialing will end;

- Busy timeout, sec – launches when an incoming call is received and defines the maximum call response time. When the defined timeout expires, busy tone will be sent to the remote subscriber.

- Ringback timeout, sec – 'busy' tone timeout for the subscriber. If the subscriber doesn't put the phone on-hook until the timeout expires, an error tone will be sent into the line.

- *Payphone* – port operates in payphone mode:

  - *Off – normal mode, paypnone is disabled;*

  - *Polarity reversal – payphone operation mode with polarity reversal. Perform line power polarity reversal on subscriber's response, and return it to original state on;*

- *12 kHz – when there is an outgoing call, tariff pulse with 12 kHz frequency will be sent in the line one time per second[11];*
- *16 kHz – when there is an outgoing call, tariff pulse with 16 kHz frequency will be sent in the line one time per second[12];*

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

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

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

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

- *Stop dialing #* – when selected, use # button on the phone unit to end the dialling, otherwise # will be recognized as a part of the number. To assign the required FXS profile for subscriber port, select this port from the port settings or open port settings in the edit mode and select required profile from the configured profile list for *'FXS profile'* parameter in the *'Line profile'* section.

- *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 short-term subscriber loop rupture (range from 200 to 3000 ms);

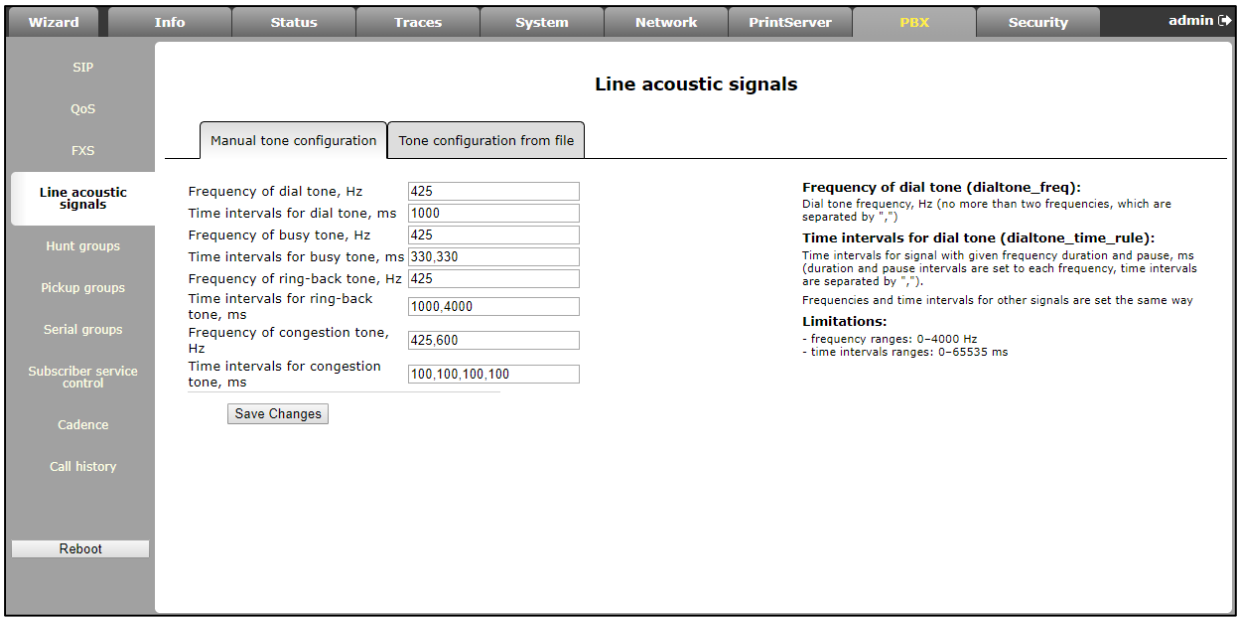
To store changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

2.4.4 The 'Line acoustic signals' submenu

This setting allows for the modification of information acoustic signals parameters as well as for the upload of ready files with the tones settings.

[11] Available only in previous versions of TAU-4/8(W).IP
[12] Available only in previous versions of TAU-4/8(W).IP

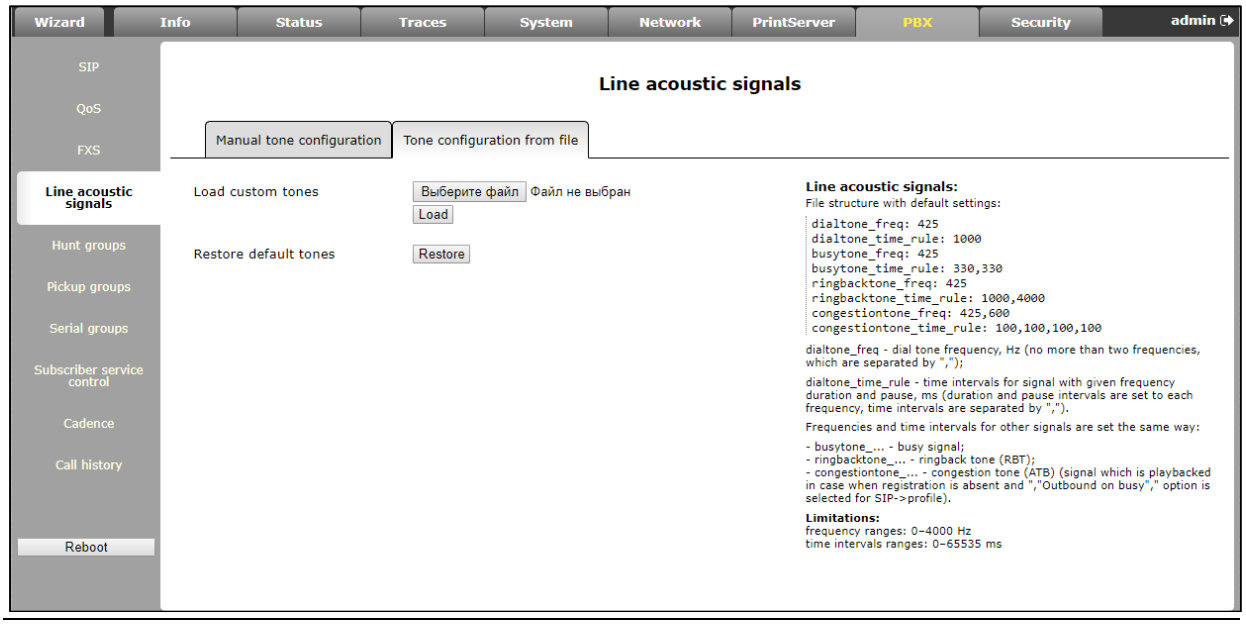


To set the parameters of acoustic signals manually, use ‘Manual tone configuration’. You can set frequencies and signal cadences listed below:

- 'Station reply' tone frequency, Hz
- 'Station reply' tone cadences, ms
- 'Busy' tone frequency, Hz
- 'Station reply' tone cadences, ms
- 'Ringback' tone frequency, Hz
- 'Ringback' tone cadences, ms
- 'Congestion' tone frequency, Hz
- 'Congestion' tone cadences, ms

Value limits:

- the range for frequencies: 0 – 4000 Hz;
- the range for time intervals: 0 – 65535 ms.



To load tone settings, click *'Select file'* and select configuration file in the «Configure tone from file». After, click *'Load'* button.

The requirements for the structure of tones configuration file are the following (the example contains standard frequency and time interval values):

```
dialtone_freq: 425
dialtone_time_rule: 1000
busytone_freq: 425
busytone_time_rule: 330.330
ringbacktone_freq: 425
ringbacktone_time_rule: 1000.4000
congestiontone_freq: 425.600
congestiontone_time_rule: 100,100,100,100
```

where

dialtone_freq – 'Dial tone' frequencies, Hz (no more than 2 frequencies, the frequencies are separated with comma ',');

dialtone_time_rule – time intervals of duration and pause of a signal with given frequency, ms (for each frequency pause and signal length intervals are specified, time intervals are separated with comma ',').

Likewise, frequencies and time intervals are setting for other signals:

- *busytone* – 'busy' tone;
- *ringbacktone* – 'ringback' tone;
- *congestiontone* – signal when there is no registration and 'Outbound on busy' mode of SIP profile is disabled.

Value limits:

- the range for frequencies: 0 – 4000 Hz;
- the range for time intervals: 0 – 65535 ms.

To reset tone settings (restore default tones) to the factory default settings, click *'Restore'* button.

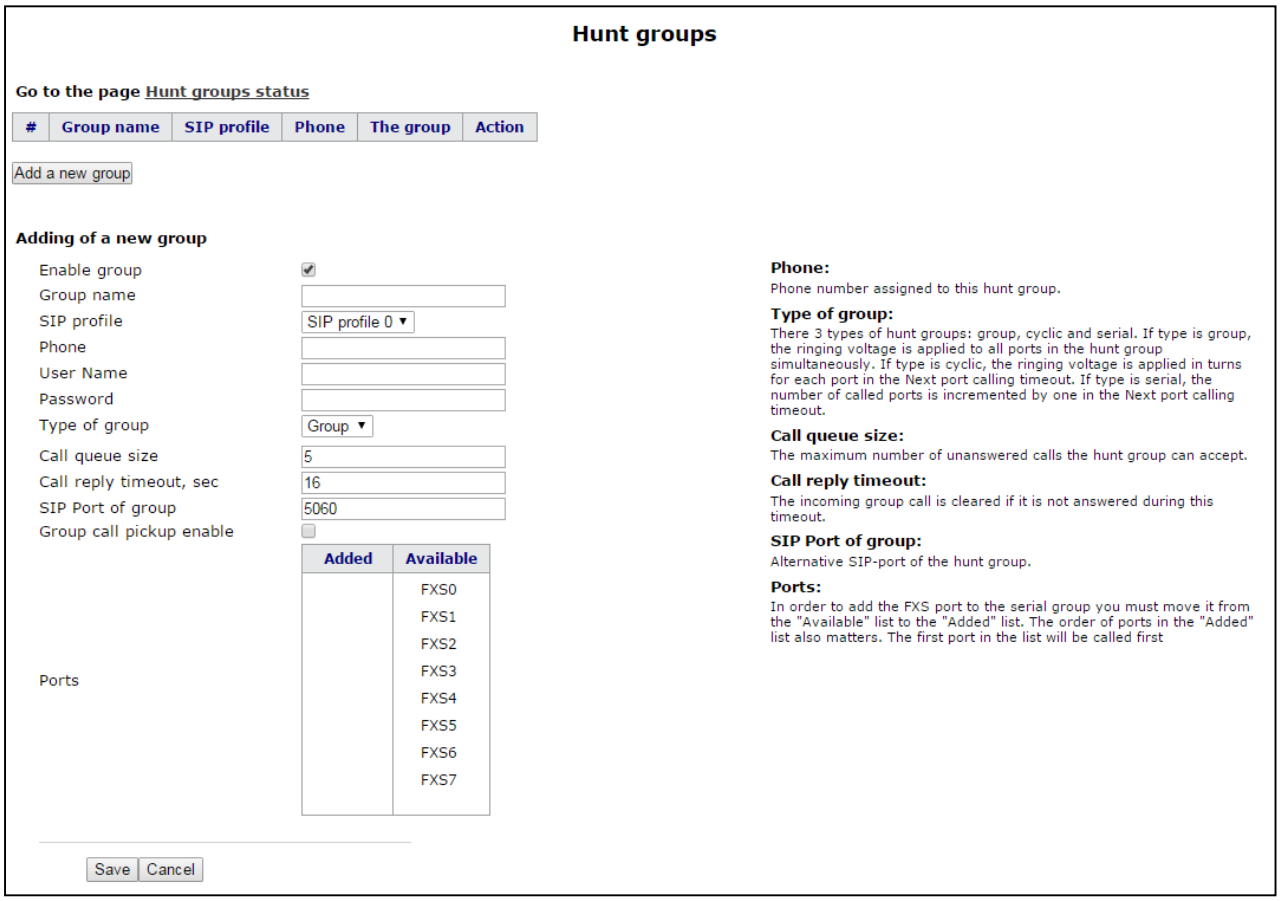
To store changes to the RAM of the device, click the *Save Changes button.* To store settings into the non-volatile memory, click *Apply* button.

2.4.5 The 'Hunt groups' submenu

Use the menu to run call groups (hunt groups).

For fast transition to *'Status/Telephony'* submenu, click *'FXS status'* (section 3.2.8) where monitoring statistic of customer unit status, call groups and series selection groups are available.

Call groups allow performing call center features. Device supports 3 call group modes: group, serial and cyclic.



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

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

In *'cycle'* mode the free participant of the group is searched by timeout. Thus, cyclical calls each after each will be sent to all the free group ports.

Adding a new group

- *Enable group* – when checked, call group is enabled otherwise call group is disabled;
- *Group name* – identification group name;

- *SIP profile* – SIP profile used by call group;
- *Phone* – phone number assigned to the group;
- *User Name* – username for authentication on SIP server;
- *Password* – password for authentication on SIP server;
- *Type of group* – call group type:
  - *Group - the call comes in to all free ports of the group simultaneously;*
  - *Serial - amount of ports on which the call signal is coming; increased by 1 after Next port calling timeout expires;*
  - *Cyclic – cadence through the interval, that is equal to timeout of the next port calling, will be transmitted to each port of group cyclically;*
- *Next port calling timeout, sec* – option is used by 'serial' and 'cyclic' group types and option assigns time interval to switch a call to following port(s);
- *Call queue size* – setting allows you to limit maximum number of unanswered calls to call group queue. If the group has free port and unanswered calls, incoming call is not put on the queue.
- *Call reply timeout, sec* – if group call is not answered, it will be dropped after timeout expiration (calling subscriber receives 'busy' signal);
- *SIP Port of group* – alternative SIP port of group (the default value is 5060);
- *Group call pickup enable* – when checked, group call interception is permitted. Call interception is available only if call group subscribers belong to the same group SIP profile;
- *Ports* – to add port into serial group, click the preferred port in the *'Available'* list and drag it to the *'Added' list.* Take into account that the order of ports is important because of searching free port will be performed from the top of the list downwards (the top port of the list will be called as first).

To add new group, click *'Save'*. To cancel adding a new group, click *'Cancel'* button.

To edit record in *'Action'* column of *'Hunt group'* table, click button. To delete - on the icon .

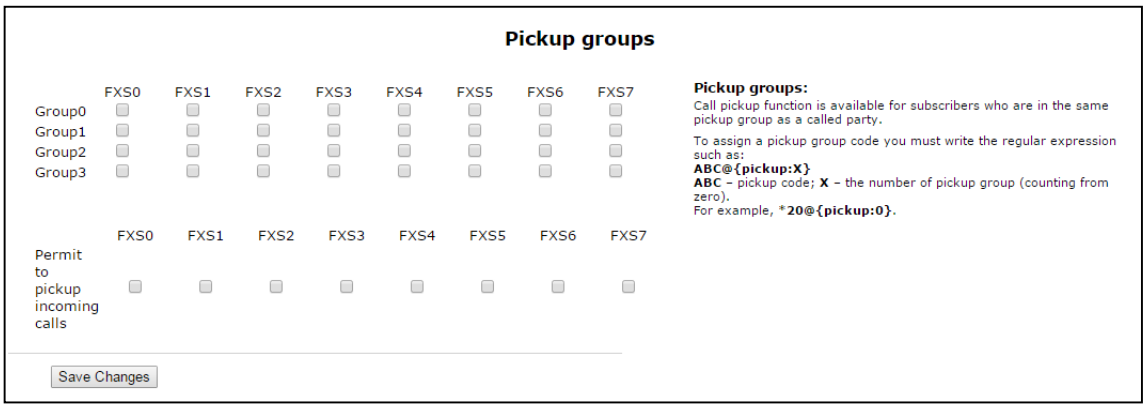
To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the 'Apply' button. Device reboot is not required.

2.4.6 The 'Pickup groups' submenu

Use the menu to configure pickup groups. You may configure only 4 different pickup groups.

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. Use the Dialplan configuration tab to configure a pickup code. For detailed information, see Dialplan Configuration.



- *Group 0..3* – sequential number of pickup group;
- *FXS 0..7* – FXS port number;
- *Permit to pickup incoming calls* – when checked, you may pick up incoming calls.

To add port to pickup group, select the checkbox next to the respective port.

Service usage:

The call comes in to the phone unit of a subscriber that belongs to the pickup group. If subscriber can not answer the call, another subscriber that belongs to that group and that uses the same SIP profile may answer the incoming call. To do this, they should dial a pickup code, and the connection with the caller will be established after that.

Pay attention that call pickup is possible only if called and pickup subscribers using the same SIP profile.

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. 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.

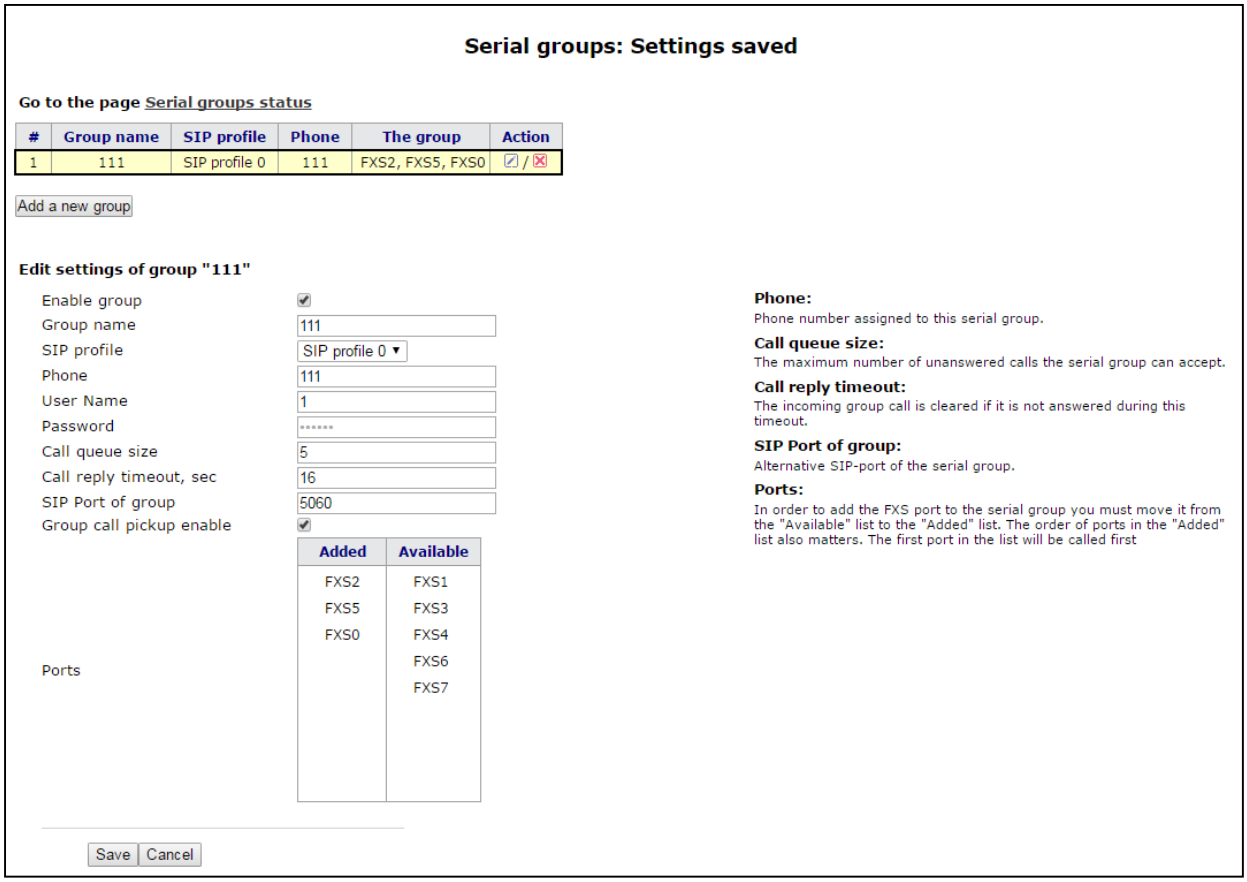
Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

To store changes to the RAM of the device, click the Save Changes button. To store settings into the non-volatile memory, click Apply button.

2.4.7 The 'Serial groups' submenu

In the serial group each new call occupies first free port thereby implementing the 'multichannel phone' mode. In 'multichannel phone' mode, a call occupies one port. When all the ports are busy, new call will be put in queue if queue has free ports (otherwise call will be broken up). When port will be free, the first port of queue will be sent to this free port. Thus, maximum number of calls, which can be sent to the serial group, is determined by sum of port number in the group and by size of call queue. Throughout its existence, each individual call is transmitted only to the one port that it occupied initially. It is the main difference from call group where the first received call occupies all the ports (call is transmitted to these ports in accordance with selected group type) and the next call is put in free place of queue (if queue does not have free place, the call is broken up). At that, maximum number of incoming calls are determined as 'size of queue + 1'.

Click *'Go to the page Serial groups status'* button for the rapid transition to the 'Status/Telephony' submenu (see section 3.2.8), where monitoring statistic of status for customer unit, call group and series selection is available.



To add group click the *'Add a new group' button.* After that, the form for editing a serial group will be opened:

- *Enable group* – when checked, serial group is enabled otherwise call to the serial group is impossible;
- *Group name* – identification group name*;*
- *SIP profile* – SIP profile used by serial group;
- *Phone* – group phone number;
- *User Name* – user name for authentication on SIP server;
- *Password* – password for authentication on SIP server;
- *Call queue size* – setting allows you to limit maximum number of unanswered calls in call group. Incoming calls will be put in queue if it has free ports and if serial group does not have free ports.
- *Call reply timeout, sec* – if group call is not answered, it will be dropped after timeout expiration (calling subscriber receives 'busy' signal);
- *SIP Port of group* – alternative SIP port of group (the default value is 5060);
- *Group call pickup enable* – when checked, group call interception is permitted. Call interception is available only if call group subscribers belong to the same group SIP profile;
- *Ports* – to add port into serial group, click the preferred port in the 'Available' list and drag it to the 'Added' list. Take into account that the order of ports is important because of searching free port will be performed from the top of the list downwards (the top port of the list will be called as first).

To add new group, click *'Save'*. To cancel adding a new group, click *'Cancel'* button.

To edit record in *'Action'* column of 'Hunt group' table, click button. To delete - on the icon .

To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

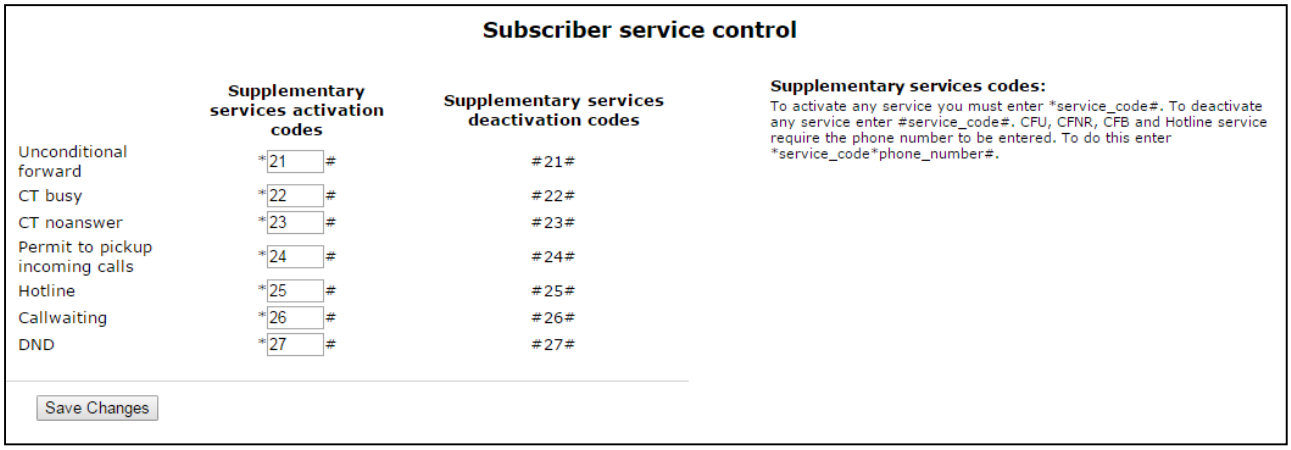
2.4.8 The 'Subscriber service control' submenu

Use the submenu to set activation code of VAD (value added service).

Use the dialing number in the following format to activate/deactivate services:

- Supplementary services activation codes: *** code_services #**
- Supplementary services deactivation codes: **# code_services #**
- Check service activity: ***# code_services #**

To activate 'CFU' (unconditional forwarding), 'CFB' (forwarding on busy), 'CFNA' (conditional forwarding on ring no answer) and 'hot/warm line' services, enter the code in the following format: ***service_code* phone_number#**



When the activation code is entered or the service is cancelled subscriber will hear a 'Confirmation' tone (3 short tones), that means that service is successfully activated or cancelled.

After entering the service confirmation code, 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.

To store changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

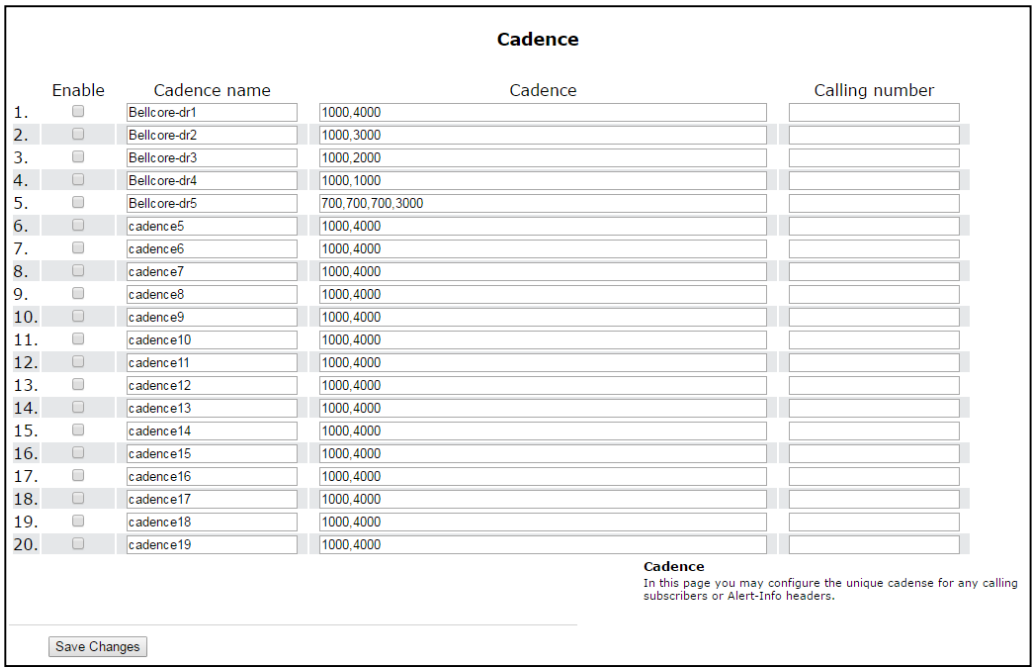
2.4.9 The 'Cadence' submenu

Use this submenu to configure alternative call control signal (cadence) in accordance with caller number or 'Alter-Info' header value of the incoming 'Invite' message. Cadence value for each call signal is represented by sequence of interleaved pulses and pauses delimited by ',' or ';'. Value of pulse/pause duration is specified in milliseconds and should be divisible by 100. Minimum pulse/pause duration is 200 ms, maximum-8000 ms.

To assign cadence to Alert-Info header value in incoming Invite you should activate the *'Use Alert-Info header'* flag in assigned SIP profile (2.4 The 'PBX' menu) and set signal name in the 'Signal Name' field (e.g. Example-cadence) in cadence settings. Cadence will playback to line if incoming Invite will content Alert-Info header with value <http://127.0.0.1/Example-cadence>.

If cadence is not found by Alert-Info header, there will be an attempt to find the cadence by caller number. If this cadence is not found the standard signal with cadence '1000', '4000' output.

You may configure up to 20 different signals in total.



- *Enable* – when checked, call transmission is enabled.
- *Cadence name* – text signal description received from 'Alert-Info' header of 'INVITE' message;
- *Cadence* - length of the ringing voltage sending to a subscriber set and length of the pause between call signals, both values should be multiple to 100 ms, min value is 200 ms, max is 8000 ms;
- *Calling number* – number of caller party for which distinctive signal of call transmission is adjusted;

Changes in this submenu take effect immediately after clicking the *'Apply'* button. Device reboot is not required.

To store changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply* button.

2.4.10 The 'Call History' submenu

For detailed description of parameter settings, see 2.4.10 The 'Call History' submenu**.**

Call history saving

To save ***'voip_history'*** history file on local PC, click *'Download call history file'* button.

Viewing call history

Click 'View call history' button to view call log of 'Status/Call history' section.

Call history size – maximum number of log records, may take values from 0 to 20,000 strings. Enter '0' value to disable call history logging.

To clear call history, click ' Clean history' button.

To save changes to the RAM of the device, click the Save Changes button. To store settings into the non-volatile memory, click Apply button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

2.5 The 'Security' submenu

Use 'Security' menu to configure firewall (install security level and limit of transit traffic). Menu is available for TAU-8.IP-W.

2.5.1 The 'General' submenu

Use this submenu to provide required protection level. The changes of the submenu will be applied without reboot.

Security Level:

- *No Security* – incoming traffic is permitted (from WAN to WLAN), outputting traffic (from WLAN to WAN) is permitted;
- *Inbound Security* – incoming traffic (from WAN to WLAN) is forbidden, outputting traffic (from WLAN to WAN) is permitted;

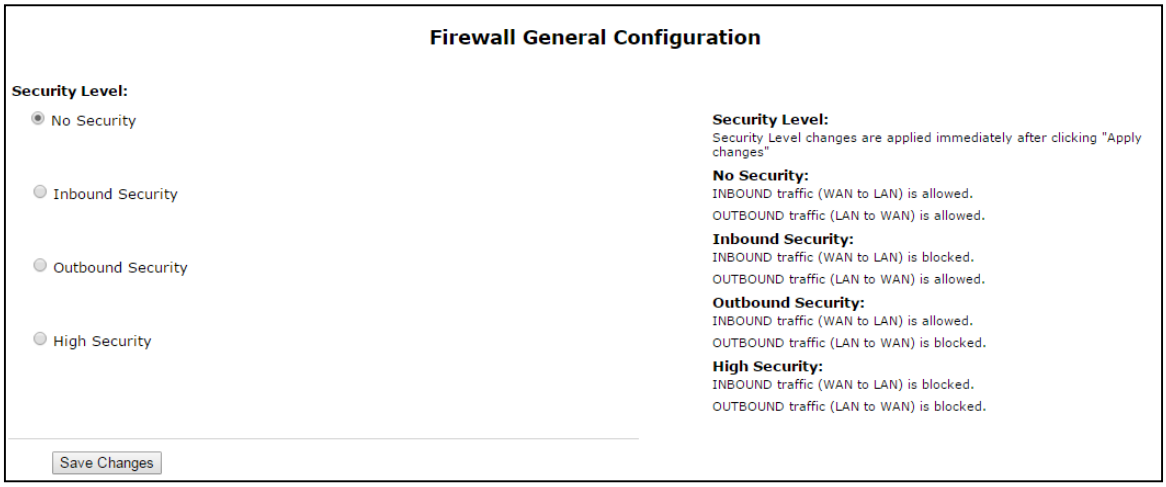
- *Outbound Security* – incoming traffic is permitted (from WAN to WLAN), outputting traffic (from WLAN in WAN) forbidden;

- *High Security* – incoming traffic is forbidden (from WAN to WLAN), outputting traffic (from WLAN in WAN) is forbidden.

You may set the rules permitting reception/transmission traffic to specific address in the *'Firewall rules'* submenu.

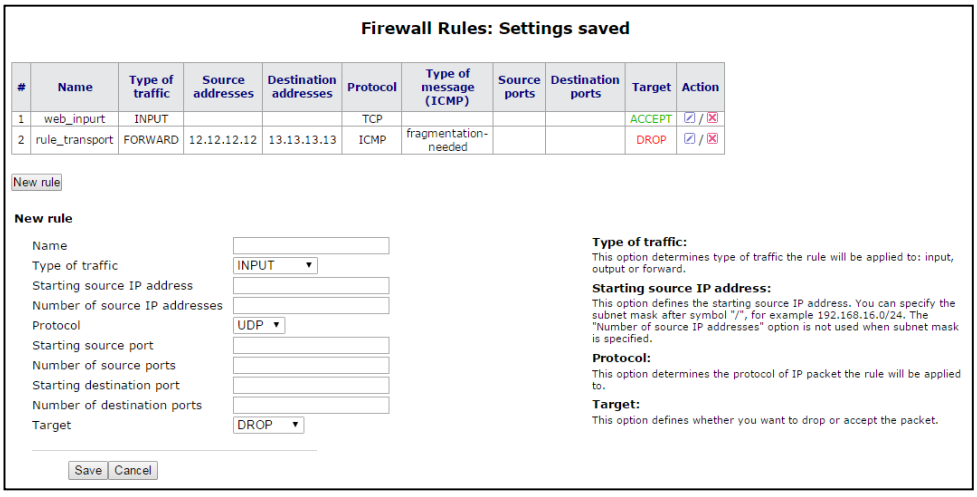
To save changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.



2.5.2 The 'Firewall Rules' submenu

Use the submenu to set transit traffic rules.



Description of 'Firewall rules' table.

Firewall rule configuration:

To add new rule, click ‘Add’ and fill the following fields:

- *Name* – user-friendly character name of rule;
- *Traffic type* –type selection of traffic that satisfies this rule:
  - *INPUT – incoming traffic. When this traffic type is chosen, the following fields will become available:*
    - *Starting source IP address* – assigns start IP address of the transmitter. After ‘/’ symbol you may assign subnet mask (for example, 192.168.18.0/24) to extract all the range of addresses. When mask is assigned, ‘Destination address number’ is not taken into account;
    - *Number of source IP addresses* – use the field to specify address range of source, if address mask of source is not specified;
  - *OUTPUT – outgoing traffic. When this traffic type is chosen, the following fields will become available:*
    - *Starting destination IP address* – assign start IP address of receiver. After ‘/’ symbol you may assign subnet mask (for example, 192.168.18.0/24) to extract all the range of addresses. When mask is assigned, ‘Destination address number’ is not taken into account;
    - *Number of destination IP addresses* – field is used to assign destination address range if the subnet mask of source is not specified;
  - *FORWARD – transit traffic. When this traffic type is chosen, the following fields will become available:*
    - *Starting source IP address* – assigns start IP address of the transmitter. After ‘/’ symbol you may assign subnet mask (for example, 192.168.18.0/24) to extract all the range of addresses. When mask is assigned, ‘Destination address number’ is not taken into account;
    - *Number of source IP addresses* – use the field to specify address range of source, if address mask of source is not specified;
    - *Starting destination IP address* – assign start IP address of receiver. After ‘/’ symbol you may assign subnet mask (for example, 192.168.18.0/24) to extract all the range of addresses. When mask is assigned, ‘Destination address number’ is not taken into account;
    - *Number of destination IP addresses* – field is used to assign destination address range if the subnet mask of source is not specified;

- *Protocol* – protocol of packet is subject of the rule (TCP, UDP, ICMP, ANY). When the ANY value is selected the rule created in the protocol field will cover all packets of TCP, UDP, ICMP.

- *Target* – take action on the packets (drop/omit).

When TCP or UDP are selected the following settings will be available for editing:

- *Starting source port* – start port of sender when packet is object of this rule;

- *Number of source ports* – used to determine port range of sender;

- *Starting destination port* – start port of receiver when packet will be object of this rule;

- *Number of destination ports* – used to determine port range of sender.

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

- *Type of message* – you may create rule for determined ICMP message type or for all the ICMP messages.

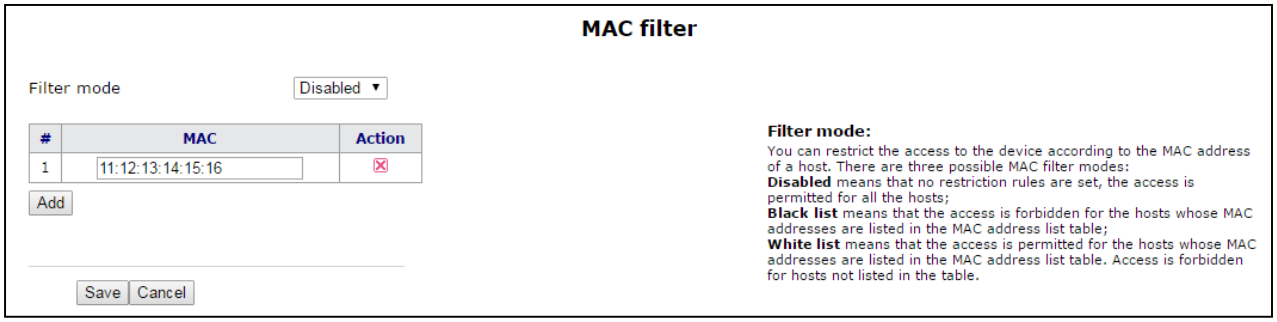
To add rule to the table, click *'Save'* button. To discard settings, click *'Cancel'* button. To edit record in *'Action'* column of *'Firewall Rules'* table, click button. To delete a record, click button.

To store settings into the non-volatile memory, click *Apply* button.

Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

2.5.3 The 'MAC filter' submenu

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



- *Filter mode* – three operation modes are available:

  - *Disabled– MAC address filtering is disabled;*

- *Black list – access is forbidden for devices with MAC addresses from the 'MAC address list'. Access for devices with unlisted MAC addresses is permitted;*
- *White list – access is permitted for devices with MAC addresses from the 'MAC addresses list'. Access for devices with unlisted MAC addresses is forbidden;*

- # – numerical order of rule;
- *MAC address* — MAC addresses list for which an action will be performed in accordance with the filter mode.

To add rule to the table, click *'Save'* button. To discard settings, click *'Cancel'* button. To delete a record, click ☒ button.

To store settings into the non-volatile memory, click *Apply* button.

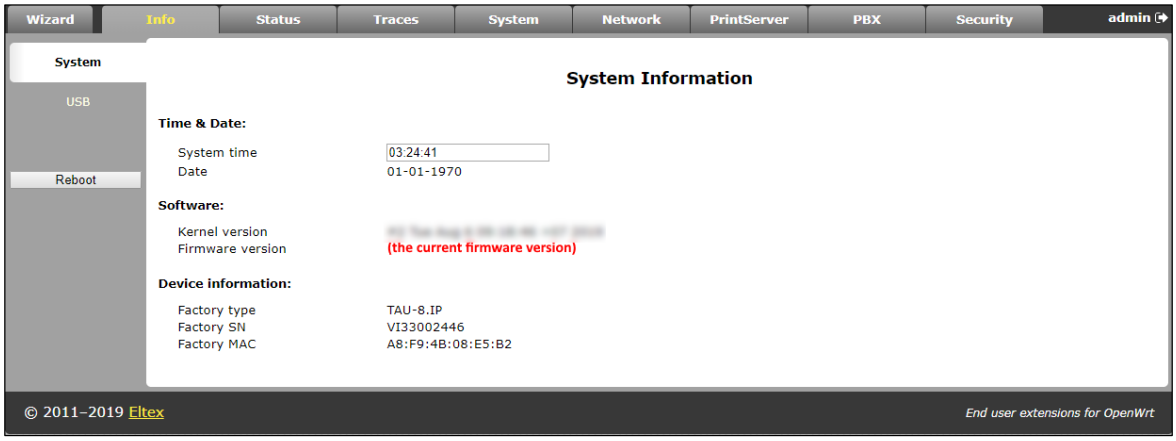
Changes in this submenu take effect immediately after clicking the *'Apply' button.* Device reboot is not required.

3 DEVICE MONITORING VIA WEB-INTERFACE. ADMINISTRATOR ACCESS

3.1 The 'Info' menu

3.1.1 The 'System' submenu

Information about system parameters such as firmware version and system time is available in the submenu.



- Time & Date – system time and date:
  - *System time – time in the format hh:mm:ss;*
  - *Date – date in dd:mm:yy format;*
- Software:
  - *Kernel version – kernel release;*
  - *Firmware version – version of file system.*
- Device information:
  - *Factory type – the device type specified by vendor;*
  - *Factory SN – the factory device serial number;*
  - *Factory MAC – physical device address.*

3.1.2 The ‘USB’ submenu

The submenu displays information about connected USB device.

To check catalog list of connected USB device, click *‘Connect via FTP’*. Browser will request username and password.

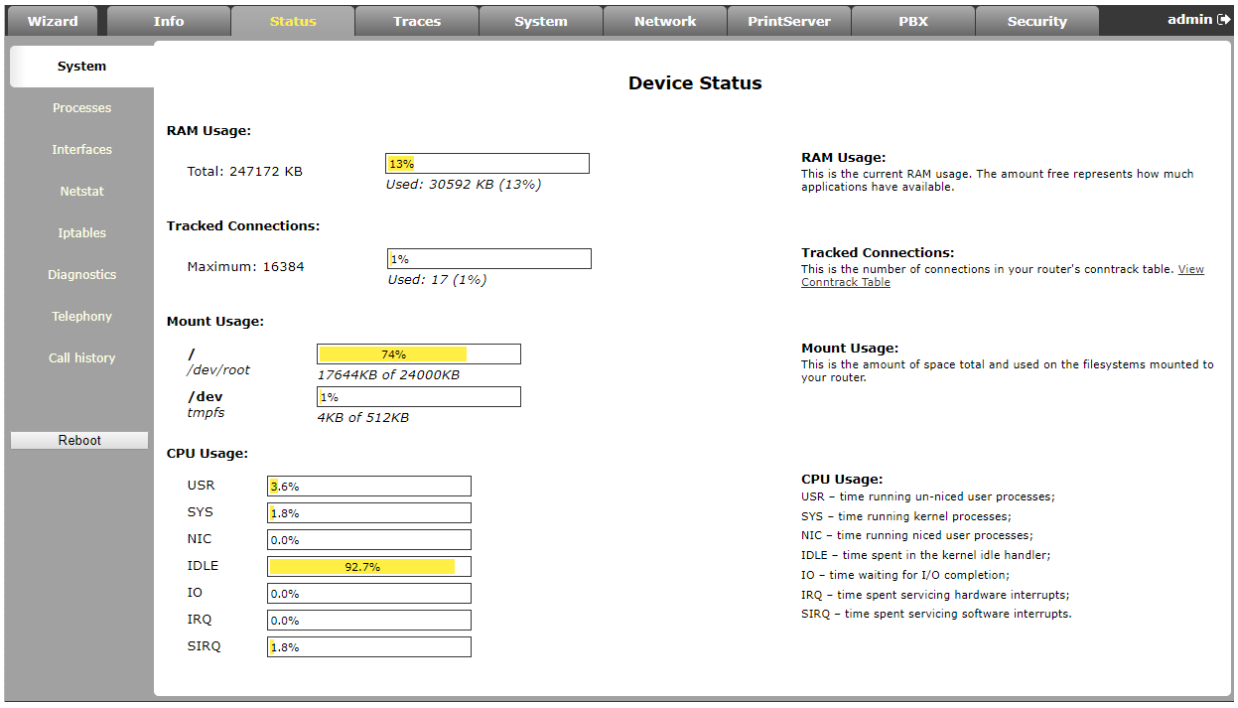
Click ‘Dismount’ button before disconnecting a USB device.

3.2 The ‘Status’ menu

Use the menu to monitor all the device systems.

3.2.1 The ‘System’ submenu

Use the submenu to display RAM usage (connection number in ‘conntrack’ table) size of file space.



The device status

- *RAM Usage* – current RAM usage, in percents of the maximum disk space;
- *Tracked Connection* – connection number in ‘conntrack’ table of router, in percents of maximum;

- *Filespace* (*Mount Usage*) – common filespace size and disk space usage of the device installed system, as a percentage of maximum disk space;

- *CPU Usage* – processor utilization.

3.2.2 The 'Processes' submenu

Use this submenu to monitor active process. By default, the table will be updated every 20 seconds.

Running Processes

Stop Refreshing Interval: 20 (in seconds)

For more information about fields see the legend...

Processes Status

PID	Uid	VmSize	Stat	Command
1	root	440	S	init
2	root		SW	[kthreadd]
3	root		SW	[ksoftirqd/0]
4	root		SW	[events/0]
5	root		SW	[khelper]
8	root		SW	[async/mgr]
113	root		SW	[sync_supers]
115	root		SW	[bdi-default]
117	root		SW	[kblockd/0]
125	root		SW	[ksuspend_usbd]
130	root		SW	[khubd]
146	root		SW	[rpciod/0]
156	root		SW	[kswapd0]
157	root		SW	[aio/0]
158	root		SW	[nfsiod]
159	root		SW<	[kslowd000]
160	root		SW<	[kslowd001]
162	root		SW	[crypto/0]
236	root		SW	[scsi_tgtd/0]
243	root		SW	[mtdblockd]
335	root		SW	[kondemand/0]
336	root		SW	[kconservative/0]
881	root		SW	[cfg80211]
891	root		SW	[phy0]
906	root	568	S	-ash --login
1038	root	340	S	klogd -c1
1052	root	208	S	/sbin/hotplug2 --persistent --max-children 1
1491	root	244	S	/sbin/fbtn
1492	root	244	S	/sbin/imonitor_loop
1537	root	3036	S	rawsock
1613	root	1348	S	/usr/bin/lighttpd -f /tmp/lighttpd-ssl.conf
1645	nobody	336	S	dnsmasq
1653	root	200	S	vsftpd
1679	root	2312	S	cupsd -C /etc/cups/cupsd.conf
1858	root	204	S	udhcpc -t 0 -i eth0 -s /usr/sbin/dhcpc.script -b -V V
1986	root	516	S	/bin/sh /sbin/voip_loop
2036	root	208	S	/usr/sbin/interface-control
2042	root	256	S	/usr/sbin/telnetd -l /bin/login -p 23 &
2602	root	216	S	/sbin/run_update_fw 86400 /usr/sbin/provision_fw.scri
2636	root	204	S	udhcpc -t 0 -i eth0 -s /usr/sbin/dhcpc.script -b -V V
2637	root	216	S	/sbin/run_update_cfg 86400 /usr/sbin/provision_cfg.sc
2795	root	280	S	/usr/sbin/dropbear -d /tmp/etc/key.dss -r /tmp/etc/ke
2823	root	2572	S	/sbin/voip
2824	root	2572	S	/sbin/voip
2825	root	2572	S	/sbin/voip
2826	root	2572	S	/sbin/voip
2827	root	2572	S	/sbin/voip
2828	root	2572	S	/sbin/voip
2829	root	2572	S	/sbin/voip
2830	root	2572	S	/sbin/voip
2831	root	2572	S	/sbin/voip
2832	root	2572	S	/sbin/voip
8920	root	252	S	/usr/bin/webif-page /www/cgi-bin/webif/admin/status-p
8921	root	448	S	sh -c /usr/bin/haserl /www/cgi-bin/webif/admin/status
8922	root	236	S	/usr/bin/haserl /www/cgi-bin/webif/admin/status-proce
8923	root	556	S	/bin/sh
9006	root		Z	[sh]
9007	root		Z	[sed]

Legend:
Memory sizes are in kB units.
Stat shortcuts meaning: A=Active, I=Idle (waiting for startup), O=Nonexistent, R=Running, S=Sleeping, T=Stopped, W=Swapped, Z=Canceled.
Commands enclosed in "[...]" are kernel threads.
For more information see the ps command description.

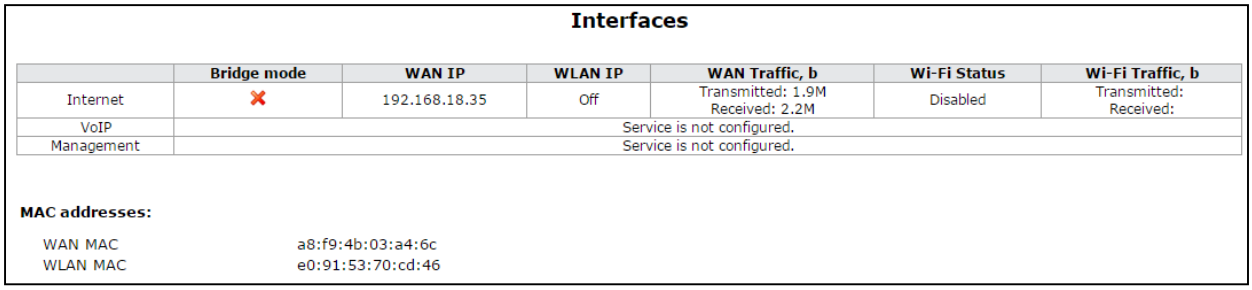
To stop update, click ‘Stop update’ button.

To restore auto refresh, select *‘Interval’* (3-59 seconds) and click *‘Auto refresh’* button.

To view information of *‘Process status’* table fields click *‘See the most used signal descriptions’ button.*

3.2.3 The ‘Interfaces’ submenu

Use the menu to monitoring such external network parameters of interfaces as IP address, number of received and transmitted packets. For TAU-8.IP-W is available monitoring of Wi-Fi parameters.



Interfaces

	Bridge mode	WAN IP	WLAN IP	WAN Traffic, b	Wi-Fi Status	Wi-Fi Traffic, b
Internet	✖	192.168.18.35	Off	Transmitted: 1.9M Received: 2.2M	Disabled	Transmitted: Received:
VoIP	Service is not configured.					
Management	Service is not configured.					

MAC addresses:

WAN MAC	a8:f9:4b:03:a4:6c
WLAN MAC	e0:91:53:70:cd:46

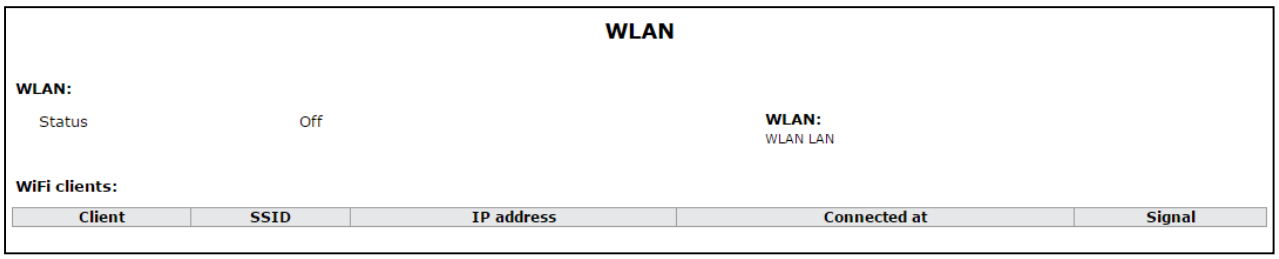
The following information about active services will be displayed in the table:

- *Bridge mode* – you can check enabled or disabled bridge mode in the service;
- *WAN IP* – IP address of the service WAN interface (when bridge mode is enabled, you can see IP address specified to the bridge);
- *WLAN IP* – WLAN status (enabled/disabled);
- *WAN Traffic, b* – shows received and transmitted traffic through WAN interface;

Wi-Fi information is displayed for TAU-8.IP:

- *Wi-Fi Status* – shows current status of wireless network for this service:
  - *Error of address getting – Wi-Fi configuration file is not read or PC board is not checked for Wi-Fi;*
  - *Disabled – Wi-Fi is disabled in configuration;*
  - *Enabled – Wi-Fi is enabled and active;*
  - *Error of initialization – Wi-Fi is disabled in configuration but is not active because of error;*
  - *Unknown – status is not known;*
- *Wi-Fi Traffic, b* – display amount of data received and transmitted through the wireless interface.

3.2.4 The 'WLAN' submenu[13]



Wireless network:

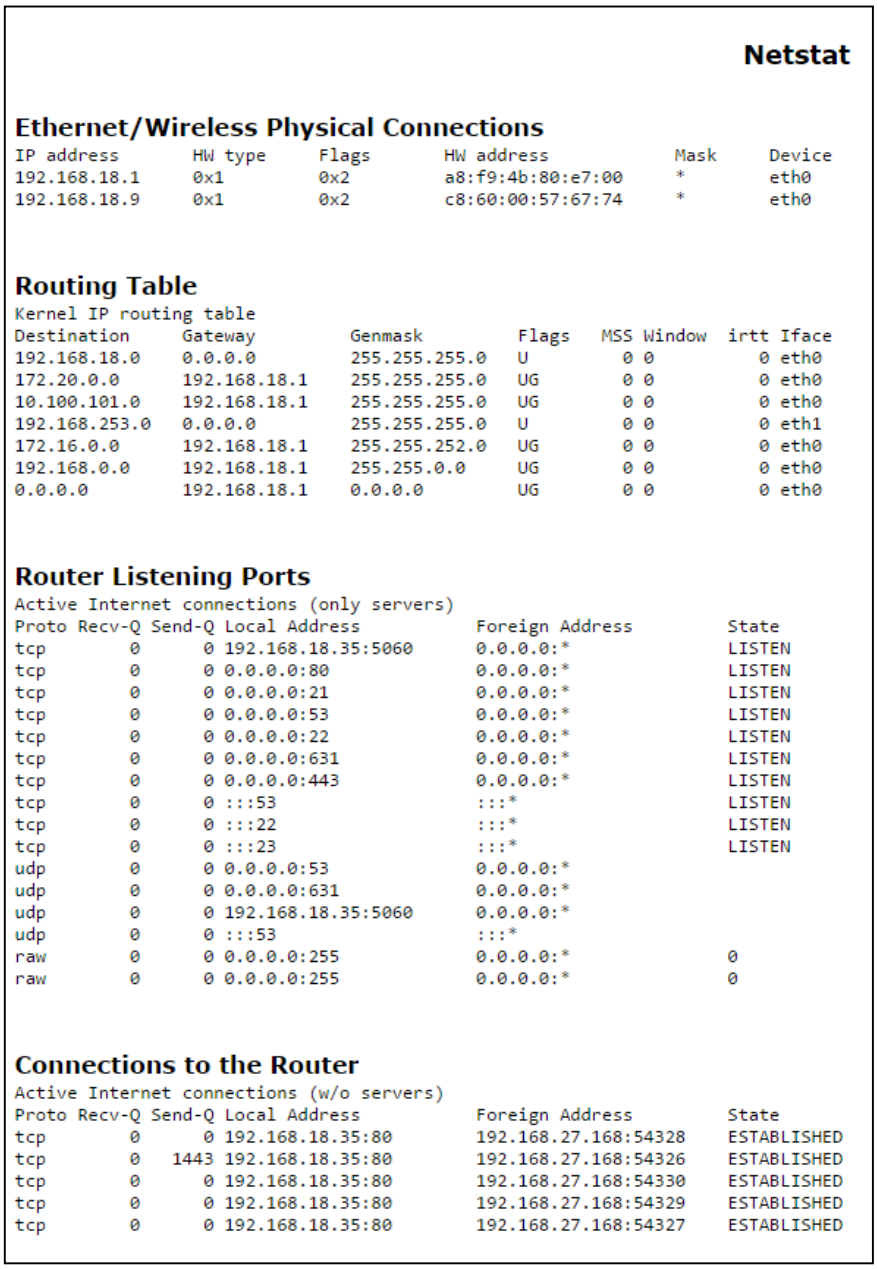
- *Status* – status of WLAN operation (on/off);
- *Channel number for Wi-Fi* – channel number for operation of wireless network**;**
- *Security options* – secure mode of wireless network:
  - *Off – low security level, data is transmitted in the unencrypted form;*
  - *WEP – WEP authentication;*
  - *WPA–WPA authentication;*
  - *WPA2 –WPA2 authentication;*
  - *WPA and WPA2– WPA and WPA2 authentication.*

The list of connected clients is displayed in the *'Wi-Fi clients'* table.

[13] Configuring the submenu is available only for TAU-8.IP-W

3.2.5 The 'Netstat' submenu

Use the submenu to monitor status of network connections and routings.



Netstat

Ethernet/Wireless Physical Connections

```
IP address       HW type     Flags       HW address            Mask     Device
192.168.18.1     0x1         0x2         a8:f9:4b:80:e7:00     *        eth0
192.168.18.9     0x1         0x2         c8:60:00:57:67:74     *        eth0
```

Routing Table

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.18.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
172.20.0.0      192.168.18.1    255.255.255.0   UG        0 0          0 eth0
10.100.101.0    192.168.18.1    255.255.255.0   UG        0 0          0 eth0
192.168.253.0   0.0.0.0         255.255.255.0   U         0 0          0 eth1
172.16.0.0      192.168.18.1    255.255.252.0   UG        0 0          0 eth0
192.168.0.0     192.168.18.1    255.255.0.0     UG        0 0          0 eth0
0.0.0.0         192.168.18.1    0.0.0.0         UG        0 0          0 eth0
```

Router Listening Ports

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.18.35:5060      0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:21              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:53              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:631             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 :::53                   :::*                    LISTEN
tcp        0      0 :::22                   :::*                    LISTEN
tcp        0      0 :::23                   :::*                    LISTEN
udp        0      0 0.0.0.0:53              0.0.0.0:*
udp        0      0 0.0.0.0:631             0.0.0.0:*
udp        0      0 192.168.18.35:5060      0.0.0.0:*
udp        0      0 :::53                   :::*
raw        0      0 0.0.0.0:255             0.0.0.0:*               0
raw        0      0 0.0.0.0:255             0.0.0.0:*               0
```

Connections to the Router

```
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.18.35:80        192.168.27.168:54328    ESTABLISHED
tcp        0   1443 192.168.18.35:80        192.168.27.168:54326    ESTABLISHED
tcp        0      0 192.168.18.35:80        192.168.27.168:54330    ESTABLISHED
tcp        0      0 192.168.18.35:80        192.168.27.168:54329    ESTABLISHED
tcp        0      0 192.168.18.35:80        192.168.27.168:54327    ESTABLISHED
```

3.2.6 The 'IPtables' submenu

Use the menu to view operation of the installed network filters.

Iptables status

Target Filter

Chain INPUT (policy ACCEPT 1145 packets, 111K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options
1	4455	603K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
2	0	0	REJECT	udp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	udp dpt:53 reject-with icmp-port-unreachable
3	289	15532	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:80
4	0	0	REJECT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:443 reject-with icmp-port-unreachable
5	0	0	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:23
6	0	0	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:22
7	0	0	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:21
8	0	0	ACCEPT	tcp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp dpt:20
9	152	10962	REJECT	udp	--	eth0	*	0.0.0.0/0	0.0.0.0/0	udp dpt:161 reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options
1	0	0	TCPMSS	tcp	--	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x06/0x02 TCPMSS clamp to PMTU
2	0	0	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 1516 packets, 835K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options
1	3398	1227K	ACCEPT	all	--	*	*	0.0.0.0/0	0.0.0.0/0	state RELATED,ESTABLISHED
2	0	0	REJECT	udp	--	*	eth0	0.0.0.0/0	0.0.0.0/0	udp dpt:162 reject-with icmp-port-unreachable

Target NAT

Chain PREROUTING (policy ACCEPT 8459 packets, 782K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Chain POSTROUTING (policy ACCEPT 34 packets, 2291 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Chain OUTPUT (policy ACCEPT 34 packets, 2291 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Target Mangle

Chain PREROUTING (policy ACCEPT 13659 packets, 1445K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Chain INPUT (policy ACCEPT 6077 packets, 744K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Chain OUTPUT (policy ACCEPT 4952 packets, 2071K bytes)

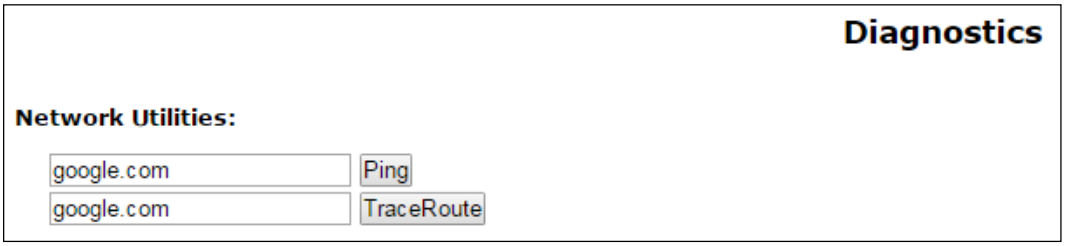
num	pkts	bytes	target	prot	opt	in	out	source	destination	options

Chain POSTROUTING (policy ACCEPT 4952 packets, 2071K bytes)

num	pkts	bytes	target	prot	opt	in	out	source	destination	options

3.2.7 The 'Diagnostic' submenu

Use the submenu to check accessibility of the net node and determine data route.

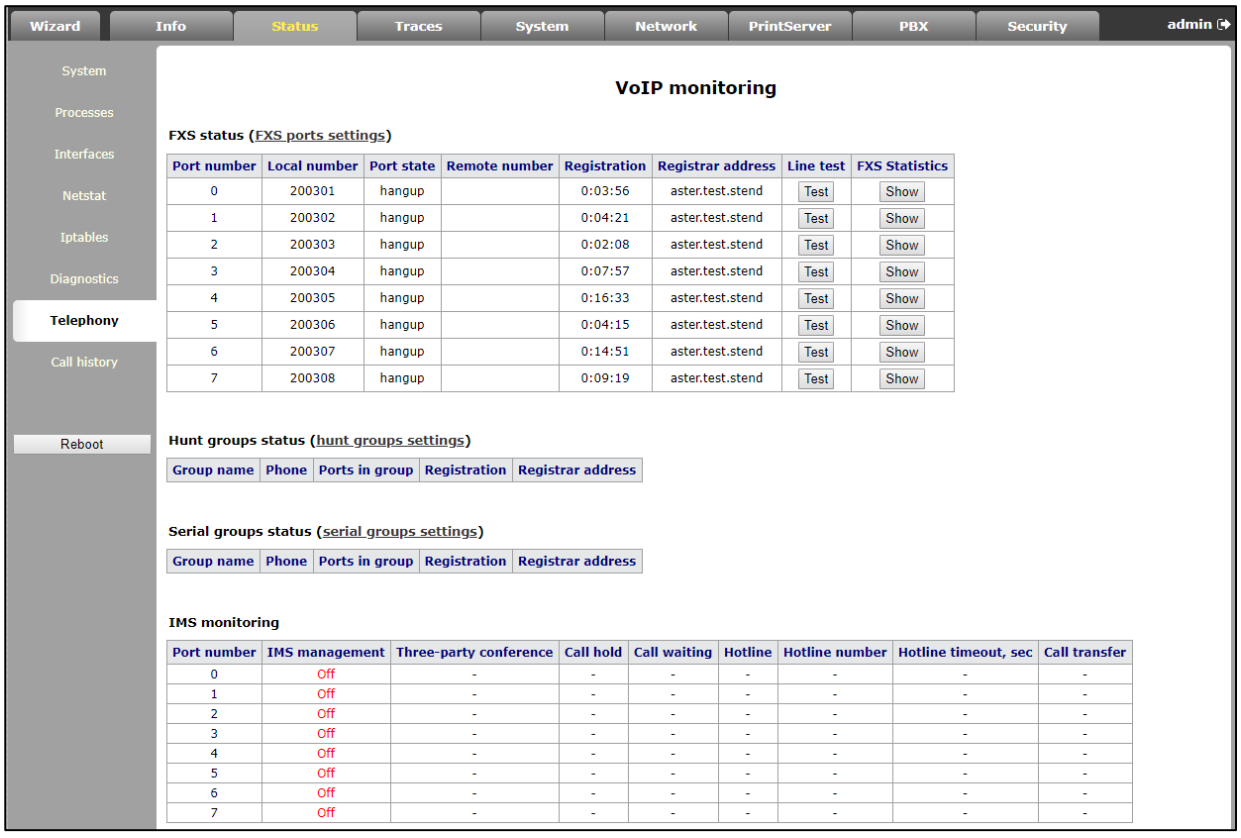


Network Utilities:

- *Ping* – utility to check net connections on the base of TCP/IP;
- *TraceRoute* – utility to determine data routs in TCP/IP networks.

3.2.8 The 'VoIP' submenu

Use this submenu to monitor status of customer units, call groups and serial groups.



FXS status – the *'FXS status'* table displays status of the device subscriber units and registration status on SIP proxy server. Click *'FXS port settings'* to go to the section of *'PBX/FXS'* subscriber port settings (The detailed information about configured parameters can be found in section 2.4.3 The 'FXS' submenu).

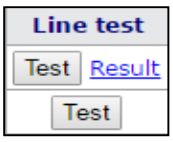
- *Port number* – port number assigned to the subscriber unit;
- *Local number* – phone number, assigned to the subscriber unit;
- *Port state* – subscriber unit status.

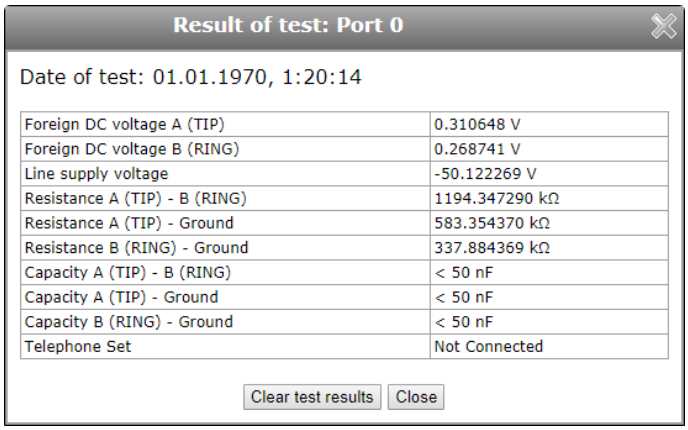
  The list of possible state:

  - *hangup – handset is hung up;*
  - *hangdown – handset is hung down;*
  - *dial – dialing a phone number of callee;*
  - *calling – call to the remote side (attempt to establish connection);*
  - *ringback – ringback tone will be sent into the line (for outcoming call);*
  - *talking – connection is established from the remote side;*
  - *ringing – ring voltage is transmitted to the line (when incoming call is received);*
  - *holding – remote subscriber is put on hold;*
  - *holded – port is put on hold by remote side;*
  - *3way call – three-way conference;*
  - *testing – test of subscriber line.*
- *Remote number* – when connection is established, this field displays the number of opposite subscriber;
- *Registration* – when registration on SIP server is successful, this field displays registration time. If registration is failed, the field will display 'No registered' record;
- *Registrar address* – SIP server address of registered subscriber;
- *Line test* – start parameter test corresponding to the subscriber line port.

Port test

'Test' button opposite each of ports allows you to test parameters corresponding subscriber line port. Click this button to begin test (test continues about 1 minutes). When test is finished, you may click the *'Result'* button to view test results that contain the following information:

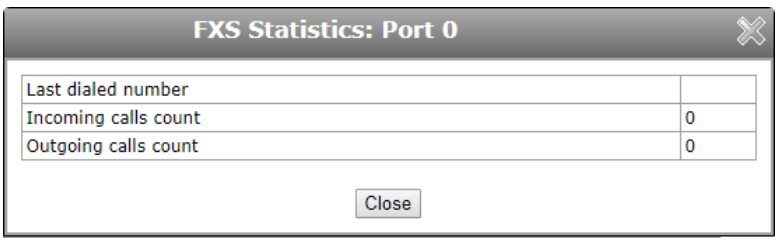




- *Date of test;*
- *Foreign DC voltage A (TIP);*
- *Foreign DC voltage B (RING);*
- *Line supply voltage;*
- *Resistance A (TIP) – B (RING);*
- *Resistance A (TIP) – Ground;*
- *Resistance B (RING) – Ground;*
- *Capacity A (TIP) – B (RING);*
- *Capacity A (TIP) – Ground;*
- *Capacity B (RING) – Ground*
- *Telephone Set — on/off phone status monitoring.*

FXS Statistics

FXS statistics display number of incoming and outgoing calls as well as the last dialed number.



Hunt groups status – this table displays registration status of configured hunt groups. Click the *'Hunt groups settings'* link to switch to the '*PBX*/*Hunt groups*' section of hunt group settings (see 2.4.5 The 'Hunt groups' submenu).

- *Group name* – identification group name;
- *Phone* – phone number assigned to the group;
- *Ports in group* – list of the device port included in the call group;
- *Registration* – when registration on SIP server is successful, this field displays registration time. If registration is failed, the field will display *'Not registered'* record;
- *Registrar address* – address of SIP server where call group is registered.

Serial group status – shows registration status of configured serial groups. Click the *'Serial groups settings'* link to forward to the '*PBX*/*Serial groups*' configuration section (see 2.4.7 The 'Serial groups' submenu for detailed description).

- *Group name* – identification group name;
- *Phone* – phone number assigned to the group;
- *Ports in group* – list of the device port included in the hunt group;
- *Registration* – when registration on SIP server is successful, this field displays registration time. If registration is failed, the field will display *'Not registered'* record;
- *Registrar address* – address of SIP server where the call group is registered.

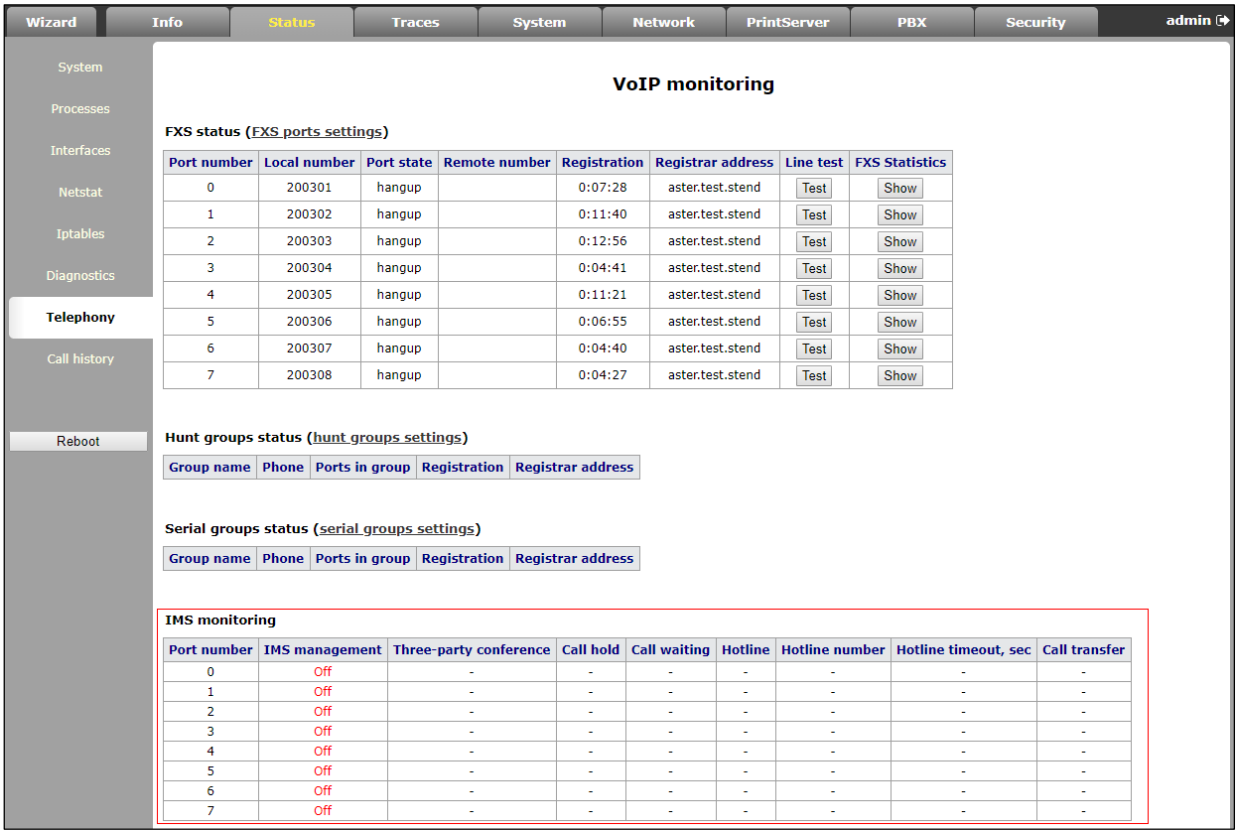
IMS monitoring

IMS monitoring shows the status of some services (activated or not activated) on each subscriber line, if this line allows remote control from the IMS server (IP Multimedia Subsystem).

- *IMS management* – shows whether the subscriber line service remote control from IMS server is enabled;
- *Three-party conference* – shows whether the 'Three-party conference' service activation command is received from IMS server;
- *Call hold* – shows whether the 'Call hold' service activation command is received from IMS server;
- *Call waiting* – shows whether the 'Call waiting' service activation command is received from IMS server;
- *Hotline* – shows whether the 'Hotline' service activation command is received from IMS server;
- *Hotline number* – shows phone number of 'Hot line' service activation command from IMS server;

- *Hotline timeout, sec* – shows the dialing timeout for the 'Hotline' service in the activation command from IMS server;

- *Call transfer* – shows whether the 'Call transfer' service activation command is received from IMS server.

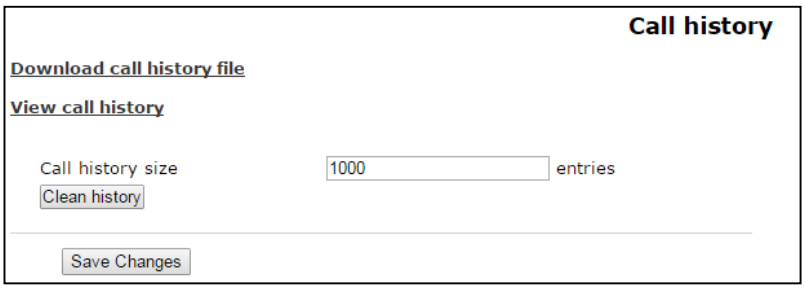


3.2.9 The 'Call History' submenu

Device RAM may store up to 20000 performed calls records. When the number of records exceeds 20000, the oldest records will be deleted, and the new ones will be added at the end of the file.

Statistics are not recorded in the call log at zero history size.

Click the 'Change call history settings' link to switch to the 'PBX/Call History' section of subscriber port settings (For detailed parameter configuration description, see 2.4.10 The 'Call History' submenu).



For mandatory cleaning a history, click the *'Clean history'* button.

Call history saving

To save history file on local PC, click the *'Download call history file'* link.

Call history view

Click the 'View call history' *link to switch to a call log:*

Call history

Change call history settings

Filter (show/hide)

#	FXS port	Local number	Remote number	Remote host IP address	Start call time	Start talk time	Talk duration	Call state	Call type	Transmitted packets	Transmitted bytes	Received packets	Received bytes
1	1	002	001	192.168.18.35	Thu Jan 1 03:03:42 1970	-	-	local clear	outgoing	0	0	0	0
2	0	001	002	192.168.18.35	Thu Jan 1 03:03:42 1970	-	-	remote clear	incoming	0	0	0	0
3	1	002	003	192.168.18.35	Thu Jan 1 03:03:51 1970	-	-	local clear	outgoing	0	0	0	0
4	2	003	002	192.168.18.35	Thu Jan 1 03:03:51 1970	-	-	remote clear	incoming	0	0	0	0
5	1	002	-	-	Thu Jan 1 03:04:03 1970	-	-	local	outgoing	0	0	0	0
6	0	001	002	192.168.18.35	Thu Jan 1 03:04:05 1970	Thu Jan 1 03:04:06 1970	8s	remote clear	outgoing	283	45973	267	40995
7	1	002	001	192.168.18.35	Thu Jan 1 03:04:05 1970	Thu Jan 1 03:04:06 1970	8s	local clear	incoming	236	37253	258	42468
8	0	001	002	192.168.18.35	Thu Jan 1 03:04:18 1970	-	-	remote busy	outgoing	0	0	0	0
9	1	002	001	192.168.18.35	Thu Jan 1 03:04:18 1970	-	-	local busy	incoming	0	0	0	0
10	0	001	009	192.168.18.35	Thu Jan 1 03:04:28 1970	-	-	no route	outgoing	0	0	0	0
11	1	002	-	-	Thu Jan 1 03:04:31 1970	-	-	local	outgoing	0	0	0	0
12	0	001	002	192.168.18.35	Thu Jan 1 03:05:33 1970	Thu Jan 1 03:05:34 1970	7s	local clear	outgoing	185	27845	190	31726
13	1	002	001	192.168.18.35	Thu Jan 1 03:05:33 1970	Thu Jan 1 03:05:34 1970	7s	remote clear	incoming	139	22954	154	23308
14	0	001	002	192.168.18.35	Thu Jan 1 03:05:44 1970	-	-	remote busy	outgoing	0	0	0	0
15	1	002	001	192.168.18.35	Thu Jan 1 03:05:44 1970	-	-	local busy	incoming	0	0	0	0
16	0	001	-	-	Thu Jan 1 03:05:49 1970	-	-	local	outgoing	0	0	0	0
17	1	002	003	192.168.18.35	Thu Jan 1 03:05:51 1970	-	-	local clear	outgoing	0	0	0	0
18	2	003	002	192.168.18.35	Thu Jan 1 03:05:51 1970	-	-	remote clear	incoming	0	0	0	0
19	1	002	002	192.168.18.35	Thu Jan 1 03:06:04 1970	-	-	remote busy	outgoing	0	0	0	0
20	1	002	002	192.168.18.35	Thu Jan 1 03:06:04 1970	-	-	local busy	incoming	0	0	0	0

1 view all *Page 1 of 2* Records 1-20 of 21 Entries per page: 20

The parameters of statistic record in call log:

- *#* – sequence number of the record;
- *FXS port* – the device FXS port number;
- *Local number* – TAU subscriber number for which record is created;
- *Remote number* – remote subscriber number;
- Opposite side IP address (Remote host) – *remote host IP address;*
- *Start call time* – call received/performed time;
- *Start talk time* – call start time;
- *Call Duration* – call duration in seconds;
- *State* – transient state or reason for call clearing;

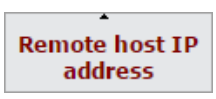
- *Type* – call type (outgoing, incoming);
- *Transmitted packets* – number of RTP packets transmitted during the call;
- *Transmitted bytes* – number of bytes transmitted during the call;
- *Received packets* – number of RTP packets received during the call;
- *Received bytes* – number of bytes received during the call.

Table 3.1 – Transient states and reasons for call clearing output into statistics

Transient states	**Description**
Size	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
Reasons for call clearing	**Description**
Local	TAU subscriber put the phone offhook, didn't perform a call and put the phone back on hook
local busy	TAU 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 subscriber clearback
remote clear	Remote subscriber clearback
local fail	Local or remote failure that has occurred during the connection establishment. Possible error reasons: mismatch codecs, reboot, source lack (band pass) and etc.
remote fail	
remote redirection	Redirecting (before the call – CFB, CFNA, CFU or during the call-CT) is performed by a remote subscriber
local redirection	Redirecting (before the call – CFB, CFNA, CFU or during the call-CT) is performed by TAU subscriber
Replaced	Subscriber status, when the 'Call Transfer' service is performed

Ranking of records

Table records can be gradated by any parameter if click on the arrow of column header by left mouse button. The direction of ranking is specified next to the header that is highlighted in red color and can be changed by pressing the left button of mouse.



- put in order of increasing;

- put in order of decreasing.

Record filtering

Call history records can be filtered by one or several parameters.

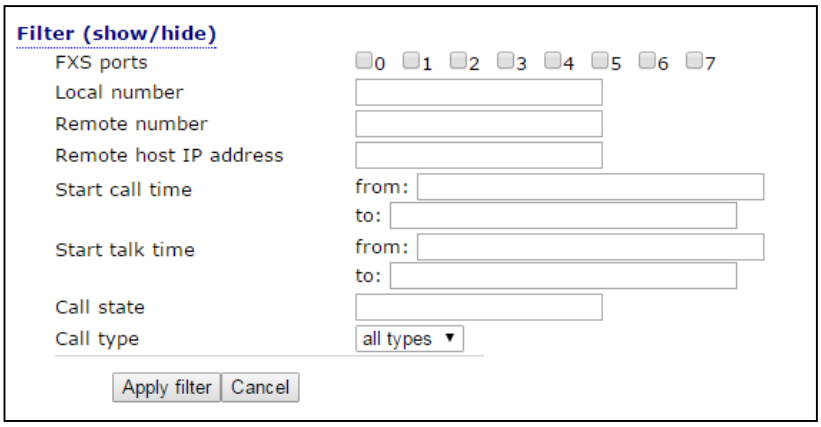
Filter list:

- *FXS ports* – FXS port number of the device;
- *Local number* – TAU subscriber number;
- *Remote number* – remote subscriber number;
- *Opposite side IP address* – IP address of a remote host;
- *Call received time from/to* – call received/performed time period in the 'hh:mm:ss dd.mm.yyyy' format (for example, for 22 February 2012 at 6:31 p.m.): '*18:31 02/22/2012*', '*22 feb 2012 18:31:00*', '*6:31:00 pm 22 February 2012*' etc.
- *Call start time from/to* – call start time period in the 'hh:mm:ss dd.mm.yyyy' format (for example, for 22 February 2012 at 6:31 p.m.): '*18:31 02/22/2012*', '*22 feb 2012 18:31:00*', '*6:31:00 pm 22 February 2012*' etc.

If the assigned data is not found, it will be highlighted in red color.

- *Call status* - transient state or a reason of call termination;
- *Call type* – call type (all types), outgoing and incoming.

To filter log by assigned parameters, click the *'Apply filter'* button. To translate all filter values back to initial state, click the *'Cancel'* button.

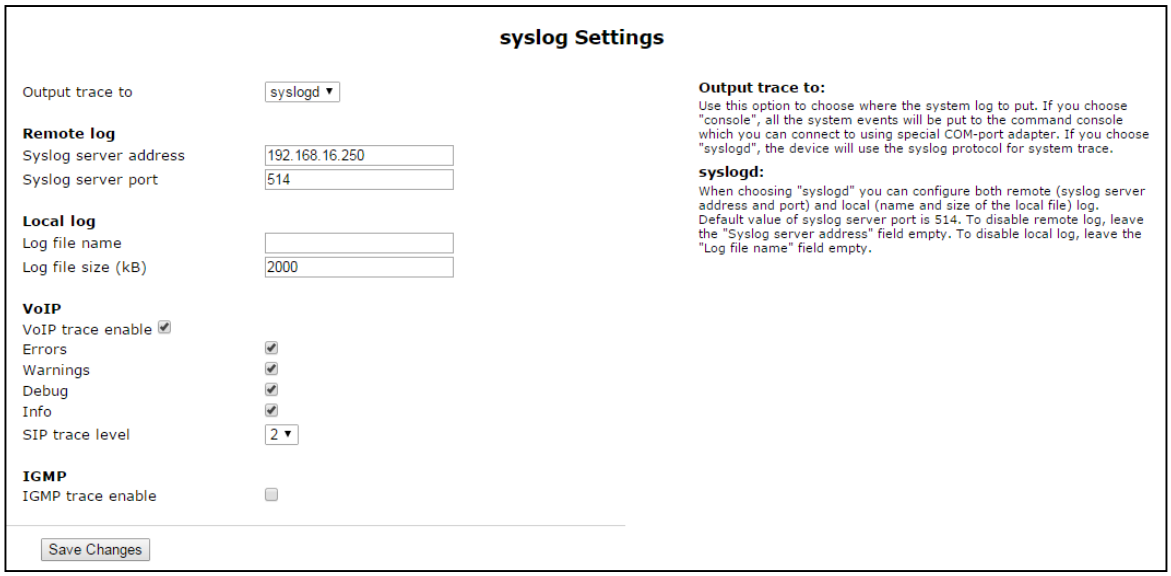


3.3 The ‘Traces’ menu

Access to the *‘Traces’* menu is performed on the administrator privileges.

3.3.1 The ‘Syslog Settings’ submenu

Use this submenu to perform parameter settings for output of remote/local log.



Syslog Settings:

- Output trace to – mode of syslog output:
  - *console – display log into continuous console of the device (continuous console is connected via COM port by using special adapter; connection parameters are 115200, 8, n, 1 and n);*
  - *syslogd – trace is displayed into remote and local log;*
  - *disable – trace is disabled;*
  - *telnet session 0 (1, 2, …) – if the device is connected via Telnet protocol you may display trace in the of active Telnet-session.*

Remote log:

- *Syslog server address* – IP address or domain name of remote log server; empty field means that the remote log is not used;
- *Syslog server port* – server port to record remote log (the default value is 514).

Local Log:

- *Log file name* – fill in this field by file name (file will be recorded into catalog /var/log;
- *Log file size (kB)* – file size in kB.

VoIP:

- *VoIP trace enable* – when checked, VoIP trace is enabled otherwise VoIP trace is disabled. Set the following flags to enter messages with determined type:
  - *Errors;*
  - *Warnings;*
  - *Debug;*
  - *Info;*
  - *SIP trace level – from 1 to 9.*

IGMP:

- *IGMP trace enable* – when checked, logging the messages of IGMP protocol is enabled.

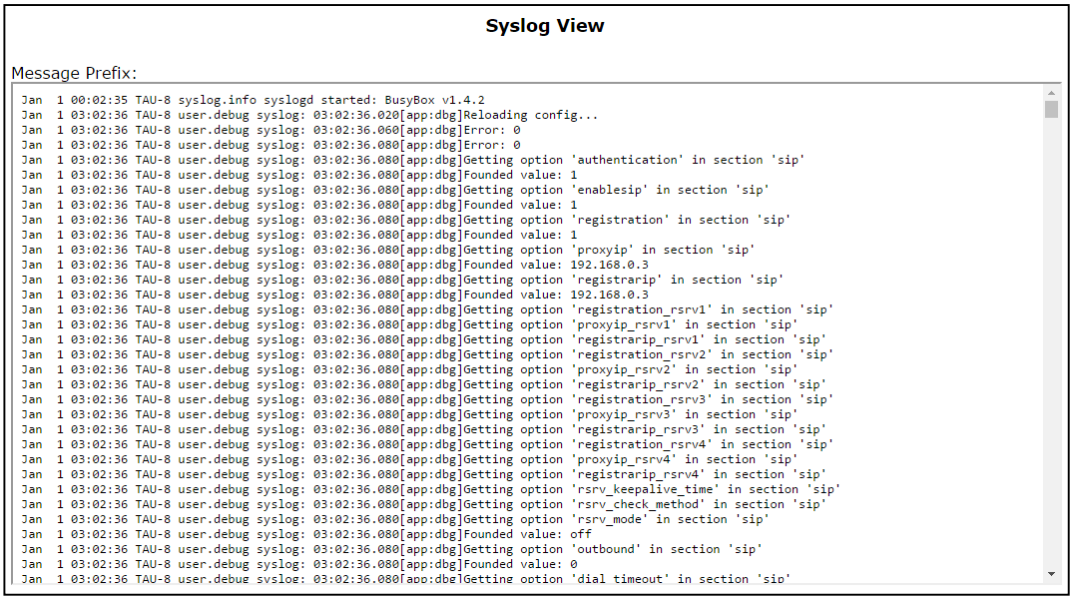
When you reboot the device, log file saved in the file system will be lost!

Changes in this menu will be applied immediately after pressing *'Apply' button.* Device reboot is not required.

To save changes to the RAM of the device, click the *Save Changes* button. To store settings into the non-volatile memory, click *Apply* button.

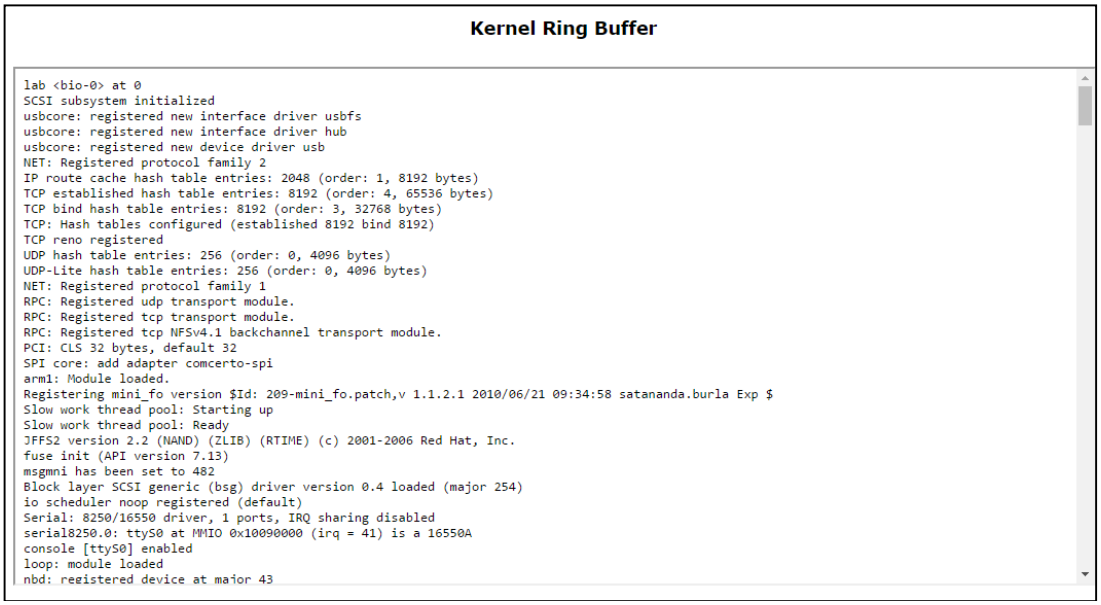
3.3.2 The 'Syslog' submenu

Use the menu to view the local log file. This service will be available if you select trace in syslogd and determine name and size of local log file.



3.3.3 The ‘Kernel’ submenu

Use the submenu to view circular kernel buffer.



3.3.4 The ‘PCAP Traces’ submenu

The submenu makes it possible to capture network traffic from active interfaces of a device.

The *‘Start traces’* section*:*

- *Interface* — a selector field used for assigning the interface for network traffic capturing (only active interfaces are displayed);
- *Filter* — network traffic filtering rules;
- The *‘Start’* button — a button to start network traffic capturing. If traffic capturing has been started successfully, the following message is displayed: «TCP-dump for interface `<ifacename>` is started. Otherwise, the message will be like: «Can't start tcpdump». In most cases this is due to entering an incorrect filter into the *‘Filter’* field;
- The ‘*Stop’* button — a button to stop network traffic capturing.

The ‘*Dump files’* section contains the list of files that can be unloaded by pressing the file name in the ‘*Name’* field. Unnecessary files can be removed by pressing *‘Remove’*.

Filter expression structure:

Each expression that specifies a filter includes one or more primitives that consist of one or more object identifiers and classifiers preceding them. Object’s name or number can serve as identifier.

Object classifiers:

1. *type* – specifies the type of the object assigned by the identifier. The *type* may accept the following values:

- *host*
- *net*
- *port.*

If the *type* is not defined, *host* value is meant.

2. *dir* – specifies the direction relative to the object. The classifier accepts the following values:

- *src (the object is a sender)*
- *dst (the object is a recipient)*
- *src or dst (a sender or a recipient)*
- *src and dst (a sender and a recipient).*

If the *dir* is not defined, *src* or *dst* is meant. To enable the mode for capturing traffic from *any* interface, *inbound* and *outbound* classifiers can be used.

3. *proto* – specifies the protocol according to which packets are structured. The classifier accepts the following values:

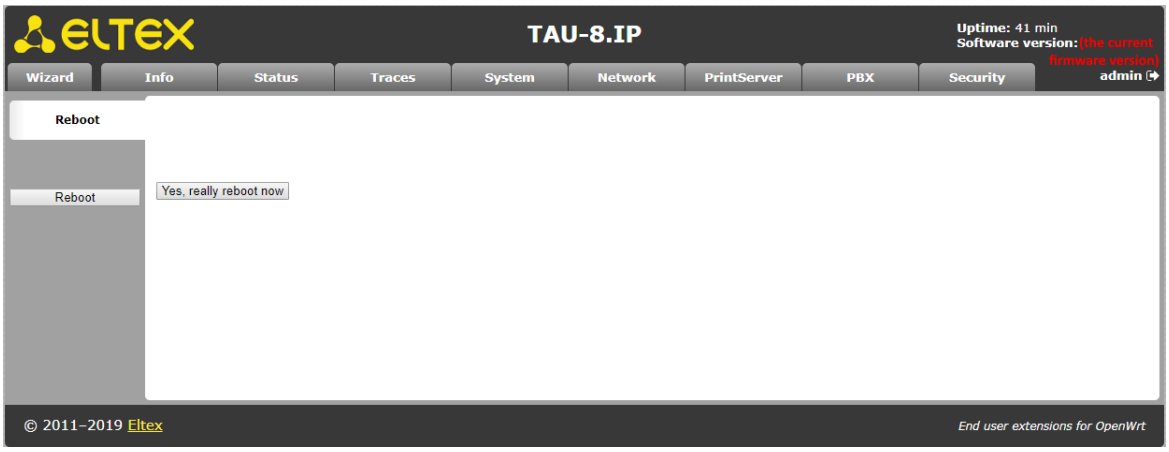
- *ether*
- *ip*
- *arp*
- *decnet*
- *tcp*
- *udp.*

If the primitive does not contain protocol classifiers, it is expected that all protocols compatible with object type match the filter.

Maximum traffic dump size is 60MB. At exceeding of the threshold, new files will be written instead of outdated ones.

3.4 The ‘Reboot’ menu

To reboot the device, click *‘Reboot’* button on the left panel of Web configurator. After that, confirm it by clicking *‘Yes, really reboot now’*. The device rebooting may continue about one minute.



4 VALUE ADDED SERVICES

4.1 Call transfer

Access to the *'Call transfer'* service is established via subscriber port settings menu – *'Ports conf.'* - by selecting *'Attended calltransfer'* value or *'Unattended calltransfer'* in the *'Flash transfer'* field.

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

'Attended calltransfer' service usage:

While being in a call state with a Subscriber B, 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* – 3-Way Call;
- *R clearback* — call transfer. Voice connection will be established between Subscribers B and C.

Fig. below shows an algorithm of *'Attended calltransfer'* service operation.

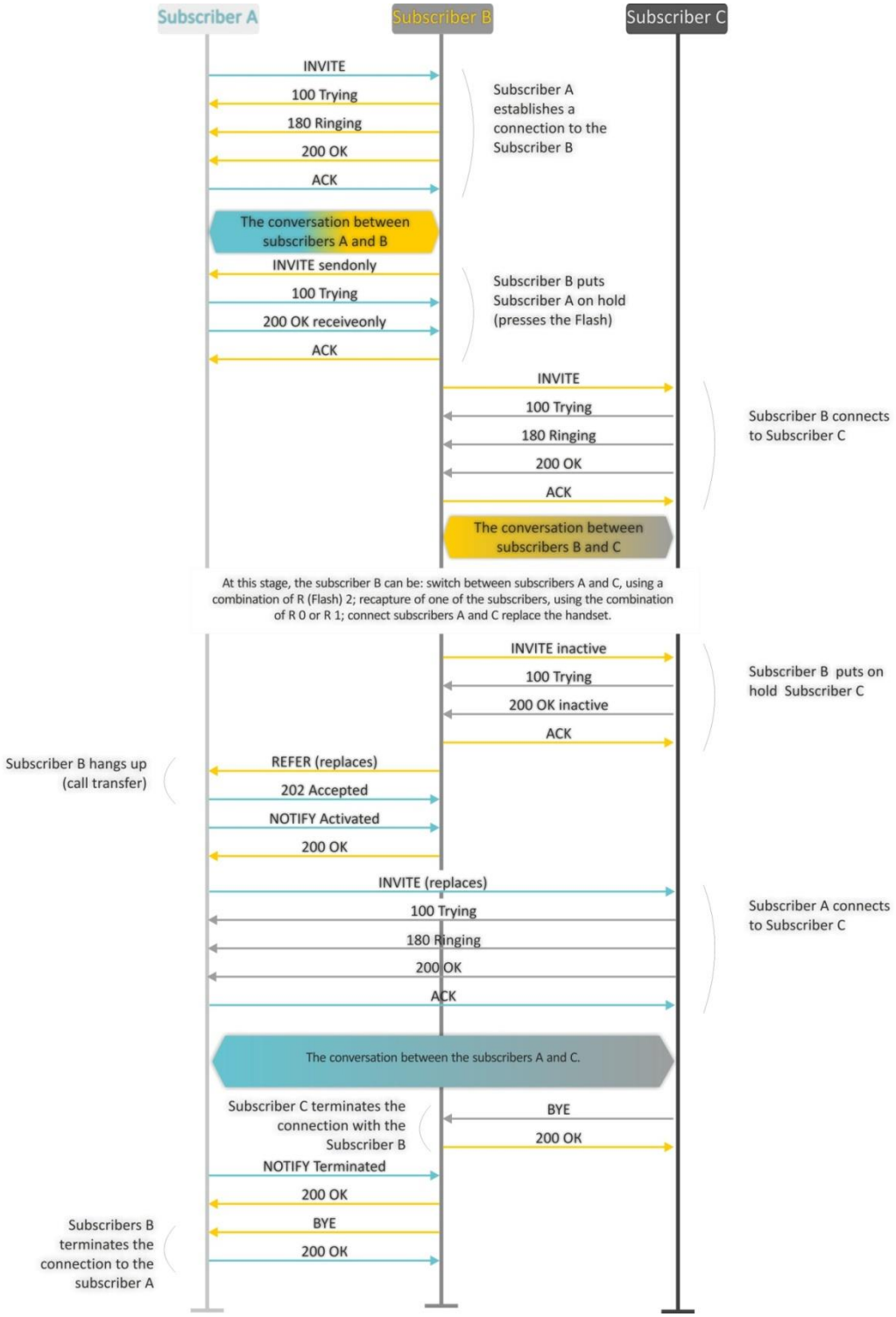


Fig. 6 - 'Attended calltransfer' service operation algorithm

'Unattended calltransfer' service allows to put an online subscriber (Subscriber B) 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.

Figure below shows an algorithm of 'Unattended calltransfer' service operation.

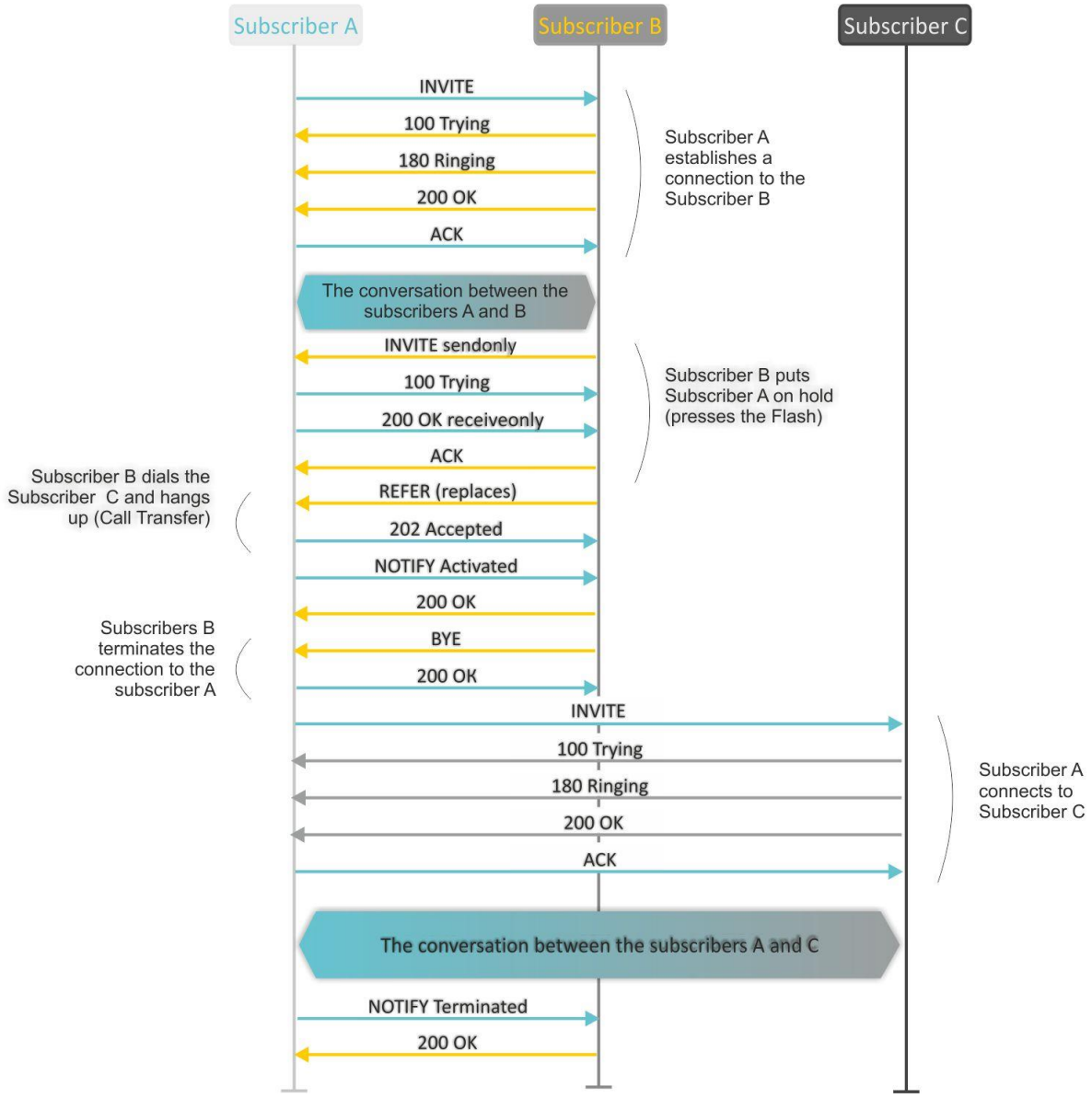


Fig. 7 - 'Unattended calltransfer' service operation algorithm

'Local Calltransfer' service allows to transfer the call within the gateway without external REFER message sending in case when Subscriber C is local TAU subscriber and call was made directly, without proxy server. If subscriber C is an external subscriber or local one that has been dialed using proxy server, *'Local Calltransfer'* service performs as *'Attended Calltransfer'*, i.e. call transfer is carried out by sending the REFER message to subscriber B.

4.2 Call Waiting

This service allows informing 'busy' users about new incoming calls with a special signal.

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

Access to this service is established via subscriber port settings menu *'FXS'* by selecting *'Attended calltransfer'*, *'Unattended calltransfer'*, or *'Local Calltransfer'* 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;
- R 2 — switch to a new call;
- R – short clearback (flash).

4.3 Three-way conference call

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

Subscriber that started the conference seems to be its initiator; two other subscribers are the participants.

Two modes are available: local and remote; in the first mode, the conference is established locally by the initiator subscriber; in the second, the conference is established using a remote server, the so-called conference server.

4.3.1 Local conference

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

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

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

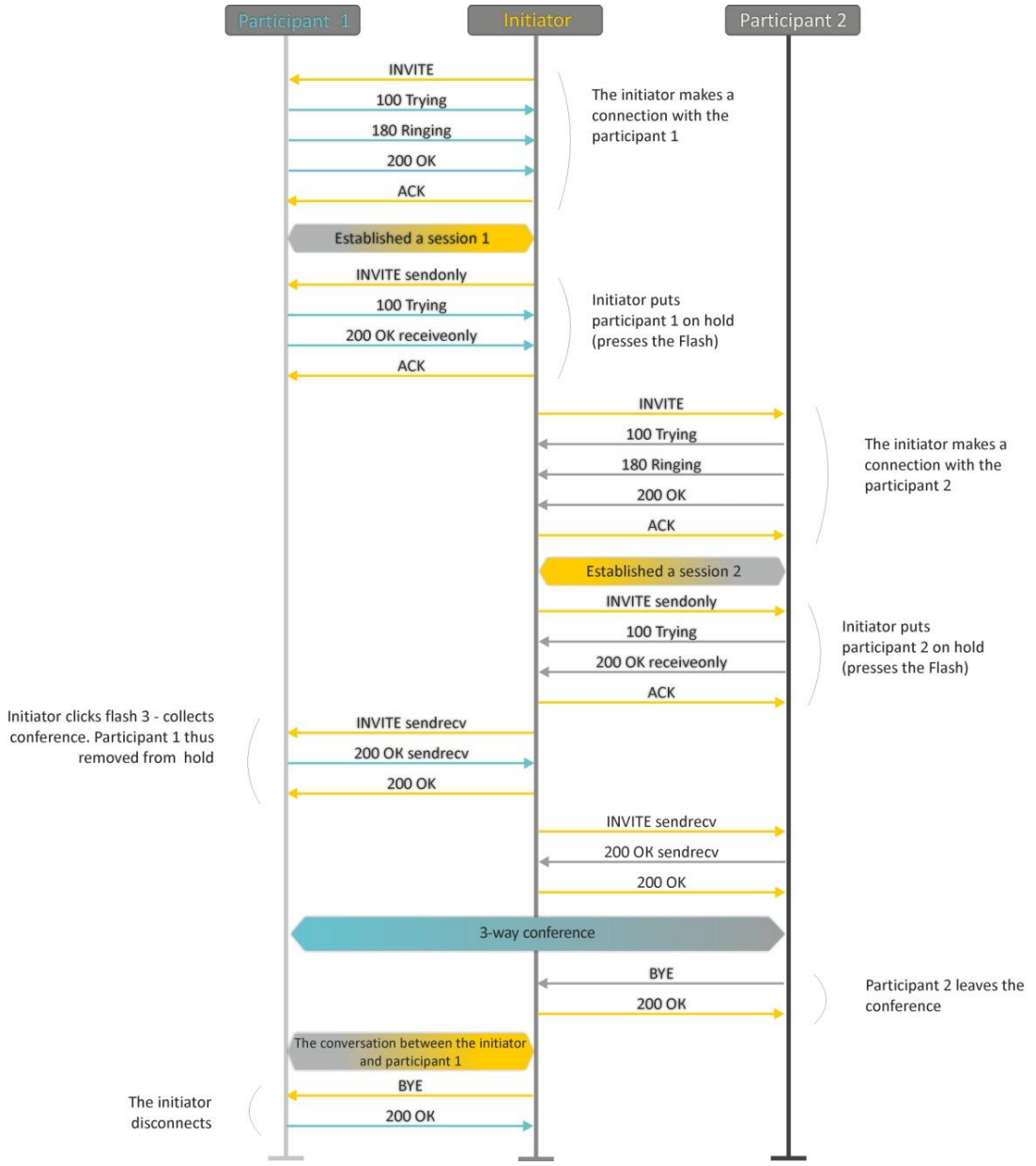


Fig. 8 - '3-way conference' service operation algorithm

4.3.2 Remote conference

Remote conference processing by algorithm, described in RFC4579. The feature of the algorithm is that the initiator subscriber establishes a connection with the conference server (also called a focus) by pressing flash + 3, and then requests for focus to establish a connection with two other conference participants. The figure below shows detailed operation algorithm.

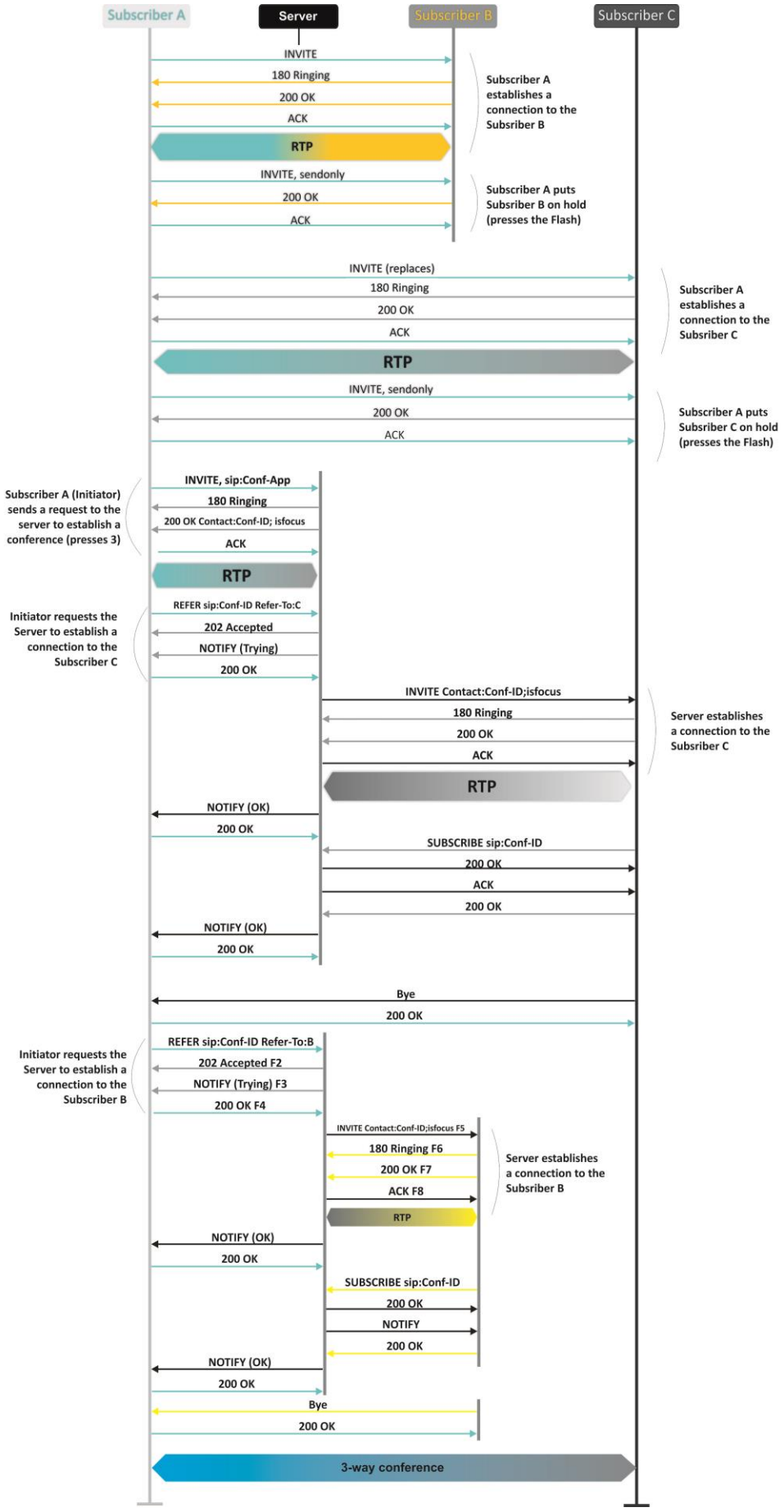


Fig. 9 - 'Remote conference' service operation algorithm

5 DHCP AUTOPROVISIONING OPERATION ALGORITHM

If the packet exchange is performed via DHCP, the device checks DHCP reply messages for existence of Option 43 (Vendor-Specific Info). If 'DHCP options' value is detected; server URL, firmware file names and configurations will be extracted from DHCP Option 43. After that, the reboot process will be start by using the received information. If DHCP option is not detected the device searching Option 66 (TFTP server) and 67 (Boot file name). If the searching is successful, firmware and configuration files will be loaded from specified server.

Option 43 format (Vendor-Specific Info):

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

1 – autoconfiguration by TR-069 protocol server address code;

2 – Provisioning code suboption number;

3 – username for authorization on TR-069 server code;

4 – password for authorization on TR-069 server code;

5 – server address code; server address is specified in URL format: tftp://address or http://address. In the first option, the address of the TFTP server is specified, in the second - HTTP;

6 – configuration file name code;

7 – firmware file name code;

8 – VLAN tag code for management.

'|' – mandatory separation symbol between codes and suboption values.

Autoconfiguration procedure algorithm:

1. DHCP sharing initialization

After loading, the device initiates a DHCP sharing.

2. Option 43 analysis

When Option 43 is received, Suboption 8 is analyzed (vlan tag):

- Suboption exists and differs from current VLAN tag (DHCP exchange is initiated in new VLAN);
- Suboption is absent or present and does not differ from the current VLAN tag: first of all, option is checked for presence of suboptions with 1, 2, 3 and 4 codes. If these suboptions are present, the device stops the analysis of the other options and establishes connection to ACS server to apply autoconfiguration via TR-069 protocol. If these options are absent, suboptions with 5, 6 and 7 codes will be analyzed to determine URL of server, configuration file names and firmware. If suboptions 6 and 7 are absent, the configuration update procedure and software are not performed.

3. Analysis of 66 and 67 options

If 43 Option from DHCP server is not received, client searches for Option 66 and extracts TFTP server address. If Option 66 was received with Option 67, the firmware name will be extracted from Option 67. If 67 Option is not received, both the firmware file name and configuration file will be extracted from configuration (these parameters are displayed on the WEB-interface's page in the *'Firmware file name'* fields (for Option 66 analysis) of the '*System/Autoconfiguration* and *Configuration file name*' menu). If these fields are empty, the attempt to load the files will be performed:

MAC_ADDRESS.cfg

MAC_ADDRESS.fw

Where MAC_ADDRESS is MAC address of the device WAN interface written by uppercase letters after dot '.' (for example, A8.F9.4B.02.20.9A.cfg и A8.F9.4B.02.20.9A.fw).

4. Configuration Update

New configuration will be applied only if its MD5-hash differs from MD5 of current configuration.

5. Checking a firmware and mounting a disk image

After loading a firmware file, its version is checked by using 'version' file in tar.gz archive).

If the current firmware version corresponds to version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. The running process of recording a firmware image to the flash memory of the device is indicated by the alternating cyclical blinking of the 'Power' indicator in green, orange and red.

The functions of password encryption (if PPPoE, PPTP, L2TP protocols are used) and SIP client encryption for authentication on SIP server have been added since firmware version 1.8.0. 'config.file' file. When you prepare the config.file or *.cfg file for autoconfiguring with changing passwords you should substitute option *'auth_pass_encrypted' 'encrypted password'* to option *'auth_pass' 'password'* line for each account in the '*/etc/config/pbx*' file. To change authentication password using PPPoE, PPTP, L2TP, you should substitute in the */etc/config/network* file

option 'pppoe_psw_encrypted' ' encrypted password'

option 'pptp_password_encrypted' ' encrypted password''

to:

option 'pppoe_psw' 'password'

option 'pptp_password' 'password''

Do not turn off the power or overload the device while writing the image to flash-memory. These actions will lead to a partial recording of firmware, which is equivalent to damage to the boot partition of the device. The device will become inoperable. You may restore the device operation only trough RS-232 by using a special COM port adapter for connection to computer.

As from FW version 2.6.0, password encryption function was added to all device configuration files. If you need to change a password for web or for connection to the device via telnet or ssh when you prepare config.file or *.cfg for autoconfiguration, delete *'encrypted'* and *specify user password* in */etc/config/passwd* file. For example, to change password of admin user you must replace *option 'adm_password_encrypted' '2B5141626956D541' with option 'adm_password' '*new password*'*.

APPENDIX A. THE USE OF VOICE MENU FOR GATEWAY SETTINGS

Voice menu allows getting information about current IP address or assigning temporary address 192.168.1.2 that will be used before the gateway reboot.

Voice menu includes two options:

- When you dial the **'***'** combination, user will be forwarded to the first node of voice menu where client will hear current IP address received by eth0 interface. This IP address can be used to connect to a gateway with the purpose of its setting and monitoring;
- When you dial the **'0'** digit, 192.168.1.2 IP forcing at the eth0 interface will be performed immediately after listening current IP address or at the moment of issuing IP address. After that, new IP address will be pronounced. This IP address will be present at the interface until gateway restarts or until expiration time of IP address lease if the settings on interface were obtained via DHCP protocol.

After each new IP address setting on eth0 interface, VoIP application will be rebooted and all the current VoIP connections will be aborted.

APPENDIX B. THE USE OF WIZARD MENU

Wizard menu allows users to configure the gateway without large number of advanced setting parameters that are usually installed by default.

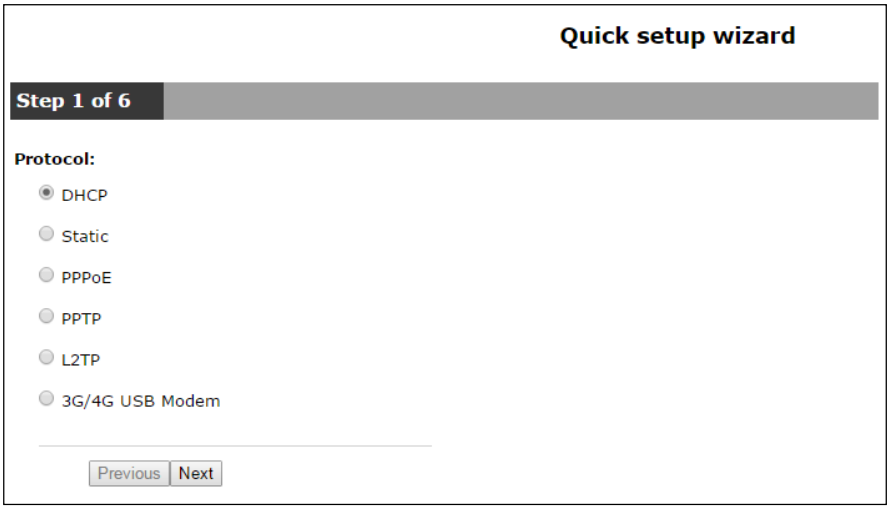
The system automatically directs a user to the *'Wizard'* menu at the first run.

You can use the quick settings by using the *'Wizard'* menu or browse to the more detailed gateway configuration by selecting the other tab on the current page of web-configurator.

The menu consists of several configuration steps. To pass to the next step, click *'Next'* button. To return to the previous step, click *'Previous'* button. After checking data entered, you should apply configuration by clicking *'Apply'* button.

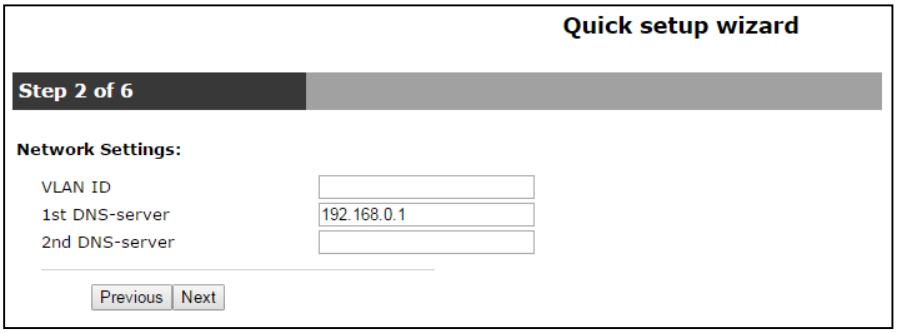
Step 1. Protocol

Selecting the used protocol for connection via TCP/IP - *DHCP, Static, PPPoE, PPTP, L2TP, 3G/4G USB modem*. Configuration of all the ports is described above in this user manual.



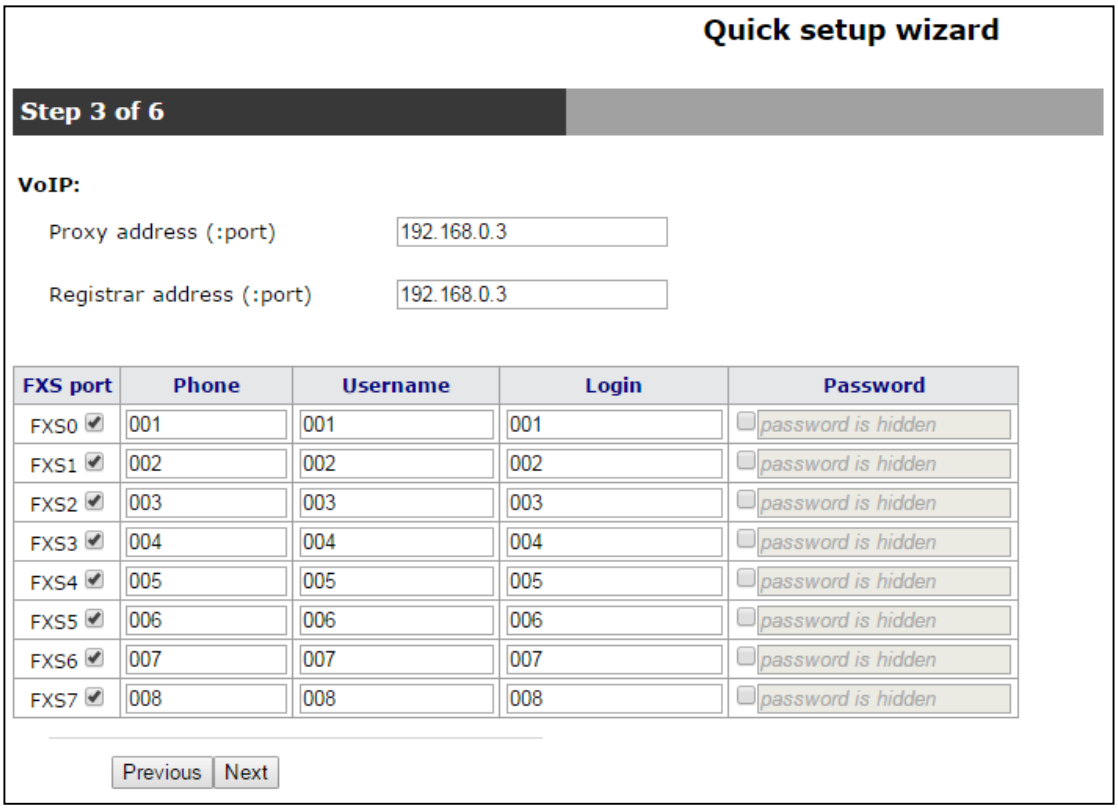
Step 2. Network Settings

In dependence to selected protocol, the following parameters must be set up: VLAN ID, WAN IP address, WAN netmask, 1st DNS-server, 2nd DNS-server, Default Gateway, PPTP/L2TP Server address and others. The more detailed description of the options is given above.



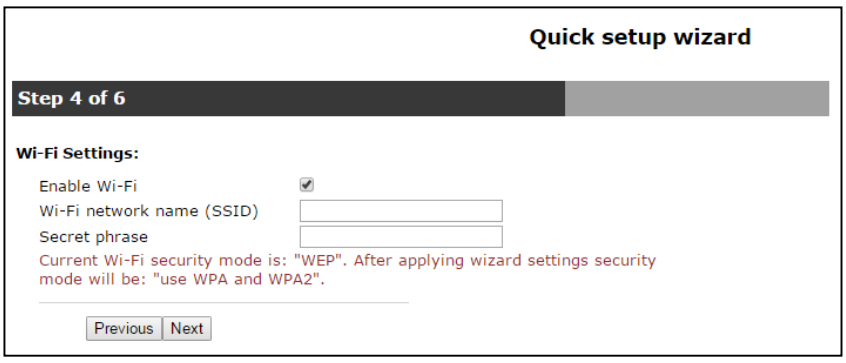
Step 3. VoIP

The page includes the key set of options for VoIP operation: Proxy address (:port) and Registrar address (:port); FXS-sets: Phone number, Username, Login and Password for authentication on a server.



Step 4. Wi-Fi settings[14]

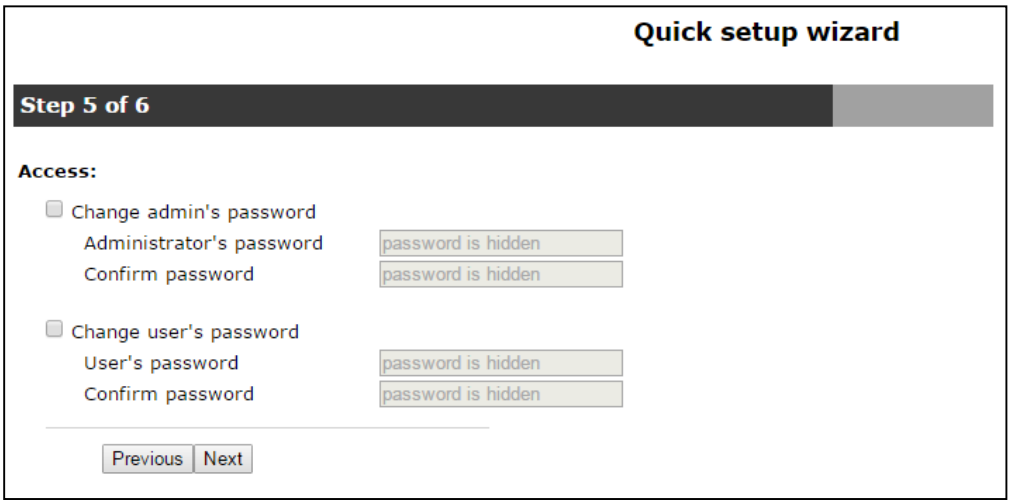
The page is used to activate and configure access via Wi-Fi by assigning a Wi-Fi network name (SSID) and Secret phrase.



[14] For TAU-8.IP-W only

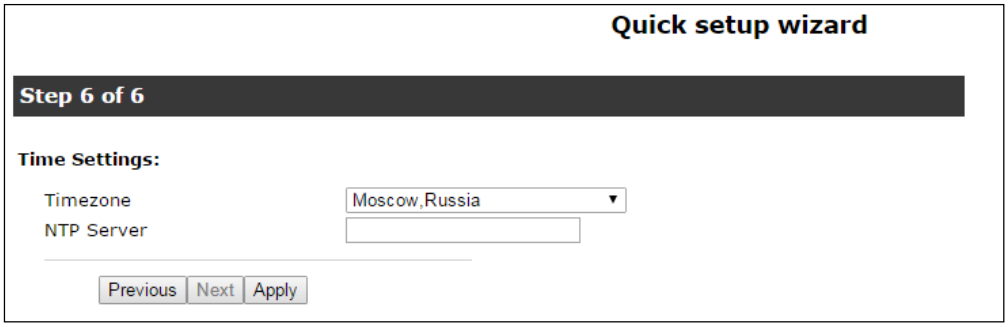
Step 5. Access

Use the page to change password for ‘admin’ and ‘user ’users. Proceeding to the next configuration step is blocked, if *‘Password’* and *‘Confirm password’* fields are empty or filled incorrectly.



Step 6. Time Settings

The page allows you to select Time zone from the list in accordance with the nearest city of your region.



APPENDIX C. THE USE OF COMMAND LINE INTERFACE (CLI) FOR CONFIGURATION AND MONITORING

Configuration changes, performed by CLI, will be applied after device **reboot** (except for IPTV settings). To apply changes, restart PBX (**pbx restart**). All the current calls will be dropped.

To save changes into the device non-volatile memory, execute the **save** command.

CLI has two modes:

- privileged — available for 'admin' profile. The mode allows you to get full access to the device configuring, trouble-shooting and monitoring;
- unprivileged – available for 'admin' and 'user' profiles. The mode provides narrow set of the options for the device monitoring and trouble-shooting.

Table C.1 — CLI commands

Command							Value	Privilegy	Description	No command function
quit							-	none	Completes the current CLI session	-
help							-	none	Displays CLI command prompts	-
ping	<options>		<value>				IP address	none		-
	repeat	<value>					int:1-4294967295	none	The number of outgoing icmp echo requests (default: 5) 5)	-
	payload	<value>					int:0-65535	none	Size of data block (in bytes) transmitted by one icmp packets as payload data (default:56)	-
	df-bit						-	none	don't fragment bit setting (default: not set)	-

	tos	<value>					int:0-63	none	Type-of-service tag with which icmp packet will be transmitted (default: 0)	-
	timeout	<value>					int:1-60	none	Waiting time for response to transmitted icmp echo request, seconds (default: 2)	-
traceroute	<options>			<value>			IP address	none		-
	df-bit						-	none	don't fragment bit setting (default: not set)	-
	repeat	<value>					int: 1-8	none	The number of transmitted packets with unchangeable ttl (default: 2)	-
	timeout	<value>					int:0-10	none	Waiting time for response to outgoing udp/icmp packet, in seconds (default: 2)	-
	ttl	<value>					int:1-255	none	Maximum hop number on the route(default: 255)	-
	tos	<value>					int:0-63	none	Type-of-service tag with which udp/icmp packet will be transmitted (default: 0)	-
	icmp						-	none	Use ICMP echo request instead of UDP datagrams (default: not use)	-

	port	<value>					int:1-65535	none	UDP port number for UDP datagram transmission (default: 33434)	
	size	<value>					int:40-32768	none	Overall length of traceroute packets, in bytes (default:100)	-
show	..						..	none		-
	system						-	none	Displays the Firmware version	-
	hwaddr						-	none	Displays the current MAC address	-
	ipaddr						-	none	Displays the current IP address	-
	netmask						-	none	Displays the current netmask	-
	network						-	none	Displays network interface configurations	-
	version						-	none	Displays the device configuration versions	-
	voiceport	..					..	none		-
		status		<value>			int:1-8	none	Displays FXS port status	-
		configuration		<value>			int:1-8	priv	Displays FXS port configuration	-
enable							-	none	Enables privileged mode	-
	disable						-	priv	Disables privileged	-

									mode	
	passwd							priv	Set a password for admin/user profiles (password is valid only for access via terminal and WEB).	
		admin	<value>					none	Set password for 'admin' profile	-
		user	<value>					none	Set password for 'user' profile	
	pbx	..					..	priv		-
		restart					-	priv	Restarts PBX application (all the current voice connections will be dropped)	-
	reset	<value>					-	priv	Resets to the default settings (the device will be rebooted automatically)	-
	backup	<value1> <value2>					IP address str:64 sym	priv	Saves backup configuration on the remote tftp server	-
	restore	<value1> <value2>					IP address str:64 sym	priv	Restores backup configuration from the remote tftp server	-
	test	..					..	priv		-
		voiceport	<value>				int:1-8	priv	Runs subscriber line testing	-
	reboot							priv	Device reboot	-
	route	<value>					-n/-e/-A/add/del/delete	priv	Management of the routing table	-
	save						-	priv	Saves configuration	-

									into non-volatile memory	
	shell						-	priv	Go to shell mode	-
	show	..						..	none	-
		system					-	none	Displays the Firmware version	-
		hwaddr					-	none	Displays the current MAC address	-
		ipaddr					-	none	Displays the current IP address	-
		netmask					-	none	Displays the current netmask	-
		network					-	none	Displays network interface configurations	-
		version					-	none	Displays the device configuration versions	-
		configuration					-	priv	Displays full device configuration	-
		voiceport	..				..	none		-
			status	<value>			int:1-8	none	Displays FXS port status	-
			configuration	<value>			int:1-8	priv	Displays FXS port configuration	-
		voiceprofile	<value>				int:1-8	priv	Displays FXS profile information	-
		switch					-	none	Displays Ethernet port status	-
		call	..				..	none		-
			active					none	Displays active calls	-
			history					none	Displays call history	-

									(for configuring, see section 3.2.9).	
		proc					-	priv	Displays the list of running processes	-
		history					-	priv	Displays CLI history	-
	upgrade	..					..	priv		-
		image	<value1> <value2>				IP address str:64 sym	priv	Firmware update of the device	-
	configure						(dir)	priv	The device configuration mode	-
		do					-	priv	Allows to execute root mode commands from any other command-line interface mode	-
		exit					-	priv	Exit the device configuration mode	-
		no	<command>				-	priv	The use of a negative form (no) of the command	-
		network					(dir)	priv	Network interface configuration	-
			do				-	priv	allows to execute root mode commands from any other command-line interface mode	-
			no	<command>			-	priv	The use of a negative form (no) of the command	-
			exit				-	priv	Exit from the network interface configuration	-
			dhcp				-	priv	Network interface	Use the Static protocol

									configuration is performed via DHCP	on the WAN port
			dhcp_gateway				-	priv	Apply DHCP option 3 received from DHCP	Do not apply DHCP option 3 received from DHCP
			dhcp_dns				-	priv	Apply DHCP option 6 received from DHCP	Do not apply DHCP option 6 received from DHCP
			dns	<value>			IP address	priv	Configures IP address of the first external DNS	Set the default DNS address (Default: 192.168.1.1)
			dns2	<value>			IP address	priv	Configures IP address of the second external DNS	Set the default second DNS address (Default: 192.168.1.1)
			dscp	..			..			
				signaling	<value>		int:0-63	priv	Set DSCP tag for SIP message transmission	Set the default DSCP tag value (default: 26)
				media	<value>		int:0-63	priv	Set DSCP tag for RTP/RTCP traffic transmission	Set the default DSCP tag value (default: 46)
			gateway	<value>			IP address	priv	Set the default gateway address	Set the default gateway address (Default: 192.168.1.1)
			ipaddr	<value>			IP address	priv	Set network interface IP address	Set the default IP address of network interface (Default: 192.168.1.2)
			netmask	<value>			netmask	priv	Set the subnet mask	Set the default value of subnet mask (default: 255.255.255.0)
			ntp	..			..	priv		
				enable			-	priv	Enables NTP	Disables NTP
				ipaddr	<value>		address	priv	Set a remote server	Set the default value of

									for time synchronization	NTP server address (Default: 0.pool.ntp.org)
				timezone	<value>		-12..+12	priv	Time zone setting	Set the default value for time zone (Default: GMT0)
			snmp	..			..	priv		-
				enable			-	priv	Enables SNMP	Disables SNMP
				trapsink	<value>		IP address	priv	Destination address of SNMPv1-trap	Set the default value of trap destination address (Default: address is not set)
				trapsink_v2	<value>		IP address	priv	Destination address of SNMPv2-trap	Set the default value of trap destination address (Default: address is not set)
				rocomm	<value>		str:96 sym	priv	Password for reading the parameters	Set the default value of password to read parameters (Default: public)
				rwcomm	<value>		str:96 sym	priv	Password for parameter writing	Set the default password value to read and record the parameters (Default: private)
				trapcomm	<value>		str:96 sym	priv	Password contained in traps	Set the default value for password contained in traps (Default: trap)
			telnet				-	priv	Allow the access to the device via telnet protocol	Deny the access to the device via telnet protocol
			ssh				-	priv	Allow the access to the device via SSHv2 protocol	Deny the access to the device via SSHv2 protocol
			web	..			..	priv		-

				enable			-	priv	Allow the access to the device via HTTP and HTTPS protocols	Deny the access to the device via HTTP and HTTPS protocols
		devname	<value>				str:96 sym	priv	Device name	Specify the default device name (default: TAU-8)
		sip	..				..	priv		-
			profile N				int:1-8	priv	Configuration mode of SIP profile N	-
				do			-	priv	Allows to execute root mode commands from any other command-line interface mode	-
				no	<command>		-	priv	The use of a negative form (no) of the command	-
				exit			-	priv	Exit the configuration mode of SIP profile N	-
				proxy	..		..	priv		-
					mode	<value>	none|park|home	priv	Set operation mode for SIP proxy server	Set the default factory operation mode for SIP proxy server (Default: none)
					address	<value1> <value2>	int:1-5 address[:port]	priv	SIP proxy server address	Set the default SIP proxy server (Default: no address)
				regristrar	..		..	priv		-
					address	<value1> <value2>	int:1-5 address[:port]	priv	SIP registrar server address	Set the registrar SIP proxy server (Default: no address)
					enable	<value>	int:1-5	priv	Allows registration on SIP server	Deny registration on SIP server

					interval	<value>	int:10-3600	priv	Set registration time, in seconds	Set the default reregistration time(default: 300)
				domain	<value>			priv	Set SIP domain	Do not use SIP domain
				domain_to_reg				priv	Allow the use of SIP domain during registration on SIP server	Deny the use of SIP domain during registration on SIP server
				expires	<value>			priv	Set reregistration time on SIP server, in seconds	Set the default reregistration time on SIP server (default: 1800)
				codec	..		..	priv		-
					list	<value>	The list of voice codecs separated by 'space' character g729a, g729b, g729x, g711a, g711u, g723, g726_24, g726_32	priv	Voice codec list by priority	-
					ptime	<value1> <value2>	Value1: g729, g711, g723, g726_24, g726_32 value2: 10-120	priv	Set packetization time for voice codecs (ms)	Set the default packetization time (default: g729 – 20ms, g711 – 20ms, g723 – 30ms, g726_24 – 20ms, g726_32 – 20ms)
				dtmfmode	..			priv		Set the default dialing signaling method (Default: Inband)
					inband			priv	Use inband digit transfer of extension dialing in RTP voice packets	-
					rfc2833			priv	Use digit transfer of extension dialing according to RFC2833 as	-

									dedicated load in RTP voice packets	
					info	<value>	dtmf-relay|dtmf|audio	priv	Set transfer method for extension dialing symbols	-
				fax	..		..	priv		-
					detect	<value>	none|caller|callee|both	priv	Set the fax signal detection mode	Disable the fax signal detection mode
					codec	<value>	g711a|g711u|t38|none	priv	Set codec to transmit fax messages	Set the default codec to transmit fax messages (Default: g711a)
					enable_in_t38			priv	Allow the proceeding to T.38	Deny the proceeding to T.38
				name	<value>		str:96 sym	priv	Set the name of SIP profile N	Set the default name of SIP profile N. (Default: SIP_profile_N)
				ecan	..		..	priv		-
					enable		-	priv	Enable echo cancellation function	Disable echo cancellation function
					tail	<value>	8|16|32|48|64	priv	Set the time of a reflected signal dispersion, ms	Set the default time of a reflected signal dispersion, ms (Default: 64)
				enable				priv	Allow SIP profile usage	Deny SIP profile usage
				vad			-	priv	Enable voice activity detector	Disable voice activity detector
				dialplan	..		..	priv		-
					ltimer	<value>	int:1-30	priv	Set L-timer value	Set the default L-timer value (Default: 15)
					stimer	<value>	int:1-10	priv	Set S-timer value	Set the default S-timer value (Default: 8)
					rule	<value>	str:1000 sym	priv	Set dialplan	Set the default dialplan

										(Default: [xABCD*#].S)
		udp	..				..	priv		-
			rtpport	..			..	priv		-
				sip	..		..	priv		-
					min	<value>	int:1024-65535	priv	Set the lower range value of UDP ports for RTP transmission	Set the lower range value of UDP ports for RTP transmission by default (default: 16384)
					max	<value>	int:1024-65535	priv	Set the upper range value of UDP ports for RTP transmission	Set the upper range value of UDP ports for RTP transmission by default (default: 32767)
		voice port N					int:1-8	priv	Configuration mode for FXS N port	-
			do				-	priv	Allows to execute root mode commands from any other command-line interface mode	-
			no	<command>			-	priv	The use of a negative form (no) of the command	-
			exit				-	priv	Exit configuration mode of FXS N port	-
			username	<value>			str:96 sym	priv	Specify user name	Specify user name by default (Default: 00N)
			authname	<value>			str:96 sym	priv	Specify user name for authentication	Set the default user name for authentication (Default: 00N)
			password	<value>			str:96 sym	priv	Set the password for authentication	Reset authentication password
			phone	<value>				priv	Set the subscriber port number	Set the subscriber port number by default

										(Default: 00N)
			profile	..			..	priv		-
				sip	<value>		int:1-8	priv	Set the SIP profile parameters for FXS port	Set FXS port parameters of SIP profile 0
				voice	<value>		int:1-8	priv	The command is intended for assigning voice profile to port.	-
			disable				-	priv	Disable FXS port	Enable FXS port
									hi	
			callerid	<value>			fsk_bell|fsk_v23||dtmf	priv	Specify caller identification method	Disable caller identification
			flash	..			..	priv		-
				min	<value>		int:70-2000	priv	Set the lower range value of flash event detection, ms	Set the lower range value of flash event detection by default, ms (Default: 200)
				max	<value>		int:min-200	priv	Set the upper range value of flash event detection, ms	Set the upper range value of flash event detection by default, ms (Default: 600)
			hybrid	..			..	priv		-
				rx	<value>		int:-230-20	priv	Set a gain factor value of terminating set at the reception, dB	Set the default value (default: -70)
				tx	<value>		int:-170-60	priv	Set a gain factor value of terminating set at the transmission, dB	Set the default value (default: 0)
			stopdial				-	priv	Enable option that completes dialing by	Disable option that completes dialing by

									entering # character	entering # character
			timer	..						
				duration	<value>		int: 0-60		Set a timer value for dialing, ms	Set the default timer value for dialing, ms (default: 30)
				waitanswer	<value>		int: 0-120		Set an answer timer value	Set the default answer timer value, ms (Default: 30)
			profile name		<value>				Set a command name for FXS profile.	Deletes the name specified to FXS profile.
		voice profile N					int:1-8	priv	Configuration mode of FXS profile N	-
			do				-	priv	Allows to execute root mode commands from any other command-line interface mode	-
			no	<command>			-	priv	The use of a negative form (no) of the command	-
			exit				-	priv	Exit configuration mode of FXS profile N	-
			callerid	<value>			fsk_bell|fsk_v23||dtmf	priv	Specify caller identification method	Disable caller identification
			flash	..			..	priv		-
				min	<value>		int:70-2000	priv	Set the lower range value of flash event detection, ms	Set the lower range value of flash event detection by default, ms (Default: 200)
				max	<value>		int:min-200	priv	Set the upper range value of flash event detection, ms	Set the upper range value of flash event detection by default,

										ms (Default: 600)
			hybrid	..			..	priv	Set hybrid parameters	-
				rx	<value>		int:-230-20	priv	Set a gain factor value of terminating set at the reception, dB	Set the default value (default: -70)
				tx	<value>		int:-170-60	priv	Set a gain factor value of terminating set at the transmission, dB	Set the default value (default: 0)
			profile	..				priv		
				name	<value>		str:96 sym	priv	Set FXS profile name	Set the default FXS profile name (Default: Default)
			stopdial				-	priv	Enable option that completes dialing by entering # character	Disable option that completes dialing by entering # character
			timer	...						
				duration	<value>		Int:0-60		Set a timer value for dialing, ms	Set the default timer value for dialing, ms (default: 30)
				waitanswer	<value>		Int:0-120		Set an answer timer value	Set the default answer timer value, ms (Default: 30)
tunnel	<value>						0 - Internet 1 = VoIP 2 - Management			
		do							Allows to execute root mode commands from any other command-line interface mode	
		exit							Exit configuration	

									mode of tunnel profile	
		l2tp							Configuration mode of l2tp tunnel	
			do						Allows to execute root mode commands from any other command-line interface mode	
			exit						Exit configuration mode of tunnel-l2tp2 profile	
			timers	…						
				echointerval	<value>			Int: 0-20	Set the value of LCP echo interval to control PPP connection state	
		pppoe								
			do						Allows to execute root mode commands from any other command-line interface mode	
			exit						Exit configuration mode of tunnel-ppoe profile	
			timers	…						
				echointerval	<value>				Set the value of LCP echo interval to control PPP connection state	
		pptp								
			do						Allows to execute root mode	

									commands from any other command-line interface mode	
			exit						Exit configuration mode of tunnel-pppo profile	
			timers	…						
				echointerval	<value>				Set the value of LCP echo interval to control PPP connection state	
				echofailure	<value>			Int: 0-20	Set the value of error number for LCP echo interval to control PPP connections.	

Basic commands

do

Allows to execute root mode commands from any other command-line interface mode

Syntax

do <command>

Parameters

command – EXEC level command

Privilegy

priv

Command mode

CONFIG, CONFIG-NETWORK, CONFIG-SIP, CONFIG-VOICEPORT,CONFIG-VOICEPROFILE

Example

```
tau-8(config)# do show ipaddr
IP address: 192.168.118.119
```

exit

Command is designed to exit the configuration mode

Syntax

exit

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG, CONFIG-NETWORK, CONFIG-SIP, CONFIG-VOICEPORT,CONFIG-VOICEPROFILE

no

Negotiation command.

Syntax

no <command>

Parameters

<command> - command. Executes for command negotiation or default value setting

Privilegy

priv

Command mode

CONFIG, CONFIG-NETWORK, CONFIG-SIP, CONFIG-VOICEPORT,CONFIG-VOICEPROFILE

Example

```
tau-8(config)# no timer duration
```

Top level commands (exec)

quit

CLI session exit command.

Syntax

quit

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

help

CLI syntax tip command.

Syntax

help

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

ping

Ping utility.

Syntax

ping [repeat <value>] [payload <value>] [df-bit do|dont|want] [tos <value>] [timeout <value>] destination

Parameters

<repeat> is the number of icmp echo requests (5 by default);

<payload> is the size of the data unit to be sent in a single icmp packet as a payload (in bytes) (56 by default);

<df-bit> enables “don’t fragment bit” (disabled by default);

<tos> is a type-of-service tag in the icmp packet to be sent (default: 0);

<timeout> is a timeout in seconds for response to a sent icmp echo request (default: 2);

destination – destination host address.

<value> – parameter value:

for repeat: 1-4294967295

for payload: 0-65535;

for df-bit

do – set;

dont – don't set;

want – don't set for packets exceed MTU

for tos: 0-63;

for timeout: 1-60.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> ping 192.168.118.46
PING 192.168.118.46 (192.168.118.46) 56(84) bytes of data.
64 bytes from 192.168.118.46: icmp_seq=1 ttl=64 time=9.31 ms
64 bytes from 192.168.118.46: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 192.168.118.46: icmp_seq=3 ttl=64 time=1.29 ms
64 bytes from 192.168.118.46: icmp_seq=4 ttl=64 time=1.30 ms
64 bytes from 192.168.118.46: icmp_seq=5 ttl=64 time=1.34 ms

--- 192.168.118.46 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4009ms
rtt min/avg/max/mdev = 1.019/2.854/9.311/3.230 ms
```

traceroute

TraceRoute utility.

Syntax

tracerout [df-bit][repeat <value>][timeout <value>][ttl <value>][tos <value>][icmp] [port<value>][size <value>] destination

Parameters

df-bit – set «don't fragment bit» (not set by default);

<repeat> is the number of sent packets with unchanged “ttl” (default: 2);

<timeout> is a timeout in seconds for response to a sent udp/icmp packet (default: 2);

<ttl> is the hop limit for a route (default: 255);

<tos> is a type-of-service tag in the udp/icmp packet to be sent (default: 0);

<icmp> enables the use of ICMP ECHO instead of UDP datagrams (disabled by default);

<port> is the number of UDP port, which is used to send UDP datagrams (default: 33434);

<size> is the full length of a traceroute packet in bytes (100 by default);

destination – destination host address.

< value > – parameter value:

for repeat: 1-8;

for timeout: 0-10;

for ttl: 1-255;

for tos: 0-63;

for port: 1-65535;

for size: 40-32768.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> traceroute 192.168.118.46
traceroute to 192.168.118.46 (192.168.118.46), 255 hops max, 100 byte packets
 1 192.168.118.46 (192.168.118.46) 1.510 ms 1.053 ms
```

show system

The command is intended for viewing firmware version.

Syntax

show system

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show system
firmware version: #2.4.1.118-ru
```

show hwaddr

The command is intended for viewing current MAC address.

Syntax

show hwaddr

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show hwaddr
MAC address: A8:F9:4B:08:E3:EE
```

show ipaddr

The command is intended for viewing current IP address.

Syntax

show ipaddr

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show ipaddr
IP address: 192.168.1.2
```

show netmask

The command is intended for viewing network mask.

Syntax

show netmask

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show netmask
Netmask: 255.255.255.0
```

show network

The command is intended for viewing network interfaces configuration.

Syntax

show network

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show network
network.common_settings=common_settings
network.common_settings.1stdns=192.168.0.1
network.common_settings.run_localdns=1
network.common_settings.run_igmpproxy=0
network.common_settings.network_mode=advanced
network.common_settings.wan_speedduplex=Auto
network.service0=service
network.service0.service_name=Internet
network.service0.wan_type=Untagged
network.service0.connection=wired
network.service0.wan_protocol=DHCP
network.service0.get_gw=1
network.service0.get_dns=1
network.service0.wan_ip=192.168.1.2
network.service0.wan_netmask=255.255.255.0
network.service0.default_gw=192.168.1.1
network.service0.pppoe_user=user
network.service0.pppoe_mtu=1500
network.service0.web_from_wan=1
network.service0.webhttps_from_wan=0
network.service0.telnet_from_wan=1
network.service0.ftp_from_wan=1
network.service0.ssh_from_wan=1
network.service0.wifi_mode=Off
```

```
network.service0.use_vendor_info=0
network.service0.pppoe_psw_encrypted=7A627F75746F796B
ntp_client.ntp=ntp_client
ntp_client.ntp.enable=0
```

show version

The command is intended for viewing device configuration version.

Syntax

show version

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show version
Config version: 8
```

show configuration

The command is intended for viewing full device configuration.

Syntax

show configuration

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# show configuration
network.common_settings=common_settings
network.common_settings.1stdns=192.168.0.1
network.common_settings.run_localdns=1
network.common_settings.run_igmpproxy=0
network.common_settings.network_mode=advanced
network.common_settings.wan_speedduplex=Auto
| Press any key to continue | Press 'q' to exit |
```

show voiceport status

The command is intended for viewing FXS port status.

Syntax

show voiceport status <value>

Parameters

< value > – parameter 1-8 value.

Privilegy

none

Command mode

EXEC

Example

```
tau-8# show voiceport status 1
Phone: 001
Status: hangup
Registration time: 0
Server registration:
```

show voiceport configuration

The command is intended for viewing FXS port configuration.

Syntax

show voiceport configuration <value>

Parameters

< value > – parameter 1-8 value

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# show voiceport configuration 1
pbx.fxs1=config
pbx.fxs1.custom=0
pbx.fxs1.profile=Default
pbx.fxs1.phone=001
pbx.fxs1.username=001
pbx.fxs1.disabled=0
pbx.fxs1.minonhooktime=500
pbx.fxs1.gainr=-70
pbx.fxs1.gaint=0
 ...
| Press any key to continue | Press 'q' to exit |
```

show voiceprofile

The command is intended for viewing FXS profile information.

Syntax

show voiceprofile <value>

Parameters

<value> – parameter value: 1-8

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# show voiceprofile 1
fxs_profiles.profile0=profile
fxs_profiles.profile0.profile_name=Default
fxs_profiles.profile0.minonhooktime=500
fxs_profiles.profile0.gainr=-70
fxs_profiles.profile0.gaint=0
| Press any key to continue | Press 'q' to exit |
```

show switch

The command is intended for viewing Ethernet port status.

Syntax

show switch

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8# show switch
Link: on
Duplex: full
Speed: 100Mbps
```

show call active

Shows information on active calls.

Syntax

show call active

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8# show call active
PBX call history:
no info
```

show call history

Displays call history (for configuring, see section 3.2.9).

Syntax

show call history

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> show call history
PBX call history:
|No|      local|      remote|   remote host|       start call time|       start talk time|         talk duration|         state|    type|
|00|     855101|          -|          -| Sun Jan  3 23:02:00 2010|                 -|                 -| local| outgoing|
|01|     855101|          -|          -| Sun Jan  3 23:02:02 2010|                 -|                 -| local| outgoing|
```

show proc

The command is intended for viewing running processes list.

Syntax

show proc

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# show proc
  PID USER      VSZ STAT COMMAND
    1 admin    1504 S    init [
    2 admin       0 SW<  [kthreadd]
    3 admin       0 SWN  [ksoftirqd/0]
    4 admin       0 SW<  [watchdog/0]
    5 admin       0 SW<  [events/0]
...
```

show history

The command is intended for viewing CLI commands history.

Syntax

show history

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# show history
   4  show voiceport statistic
   8  show voiceport statistic 1
   9  show voiceport status 1
  11  show voiceport configuration 1
  12  show voiceprofile 1
```

enable

The command is intended to enable the privilege mode.

Syntax

enable

Parameters

Command contains no arguments.

Privilegy

none

Command mode

EXEC

Example

```
tau-8> enable
```

```
tau-8#
```

disable

The command is intended to disable the privilege mode.

Syntax

disable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# disable
tau-8>
```

passwd user

Set a password for admin/user profiles (password is valid only for access via terminal. A password for WEB access can be set in System → Access Passwords).

Syntax

passwd user <value>

Parameters

<value> – password;

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# passwd user
Changing password for admin
New password:
Bad password: too short
Retype password:
Password for admin changed by admin
```

pbx restart

Restarts PBX application (all the current voice connections will be dropped).

Syntax

pbx restart

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# pbx restart
Restart voip...
```

reset

Resets the device to factory settings (the device reboots automatically).

Syntax

reset <value>

Parameters

<value> – parameter value:

dhcp – network settings in reset configuration will be setted dynamically;

static – network settings in reset configuration will be static (IP address 192.168.1.2).

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# reset static
Do you really want to reset configuration and restart device? (yes/no)
```

backup

Saves a configuration backup to a remote TFTP server.

Syntax

backup <value1><value2>

Parameters

<value 1> – TFTP server IP address where configuration will be uploaded;

<value 2> – configuration file name (string: 64 characters)

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# backup 192.168.118.46 config.tar.gz
tau-8#
```

restore

Restores a configuration backup from a remote TFTP server.

Syntax

restore <value1><value2>

Parameters

<value 1> – TFTP server IP address where configuration will be downloaded from;

<value 2> – configuration file name (string: 64 characters)

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# restore 192.168.118.46 configtau.tar.gz
update_tftp_cfg.sh: set TFTP IP to 192.168.118.46
update_tftp_cfg.sh: CFG filename: configtau.tar.gz
tau-8#
```

test voiceport

Runs subscriber line testing.

Syntax

test voiceport <value>

Parameters

<value>-number:1-8

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# test voiceport 2
waiting result...
RING ext -0.37, V, TIP ext -0.37, V
Vbat. -31.45, V, Vring1.   nan, V, Vring2   nan, V
res T-R. 950.41, kOm; res T-G. 471.79, kOm; res R-G 670.24, kOm
cap T-R.  0.00, mkF; cap T-G.  0.00, mkF; cap R-G  0.00, mkF
end testing, result '0'
```

reboot

The command is intended for rebooting the device.

Syntax

reboot <confirm>

Parameters

<confirm> – yes/no

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# reboot
Do you really want to restart device? (yes/no)
```

route add

The command is intended for adding the route rule.

Syntax

route add <value1> netmask <value2> gateway <value3>

Parameters

<value1> – IP address;
<value2> – mask address;
<value3> – default gateway IP address.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# route add 192.168.1.0 netmask 255.255.255.0 gateway 192.168.118.77
tau-8#
```

route del

The command is intended for deleting route rule.

Syntax

route del <value1> netmask <value2>

Parameters

<value1> – IP address;
<value2> – mask address;

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# route del 192.168.1.0 netmask 255.255.255.0
tau-8#
```

save

The command is intended for saving configuration to the volatile memory of the device.

Syntax

save

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# save
save config
Image 0: Flag 0, Image 1: Flag 1
tar: removing leading '/' from member names
compressed 126485 bytes to device 0
```

shell

The command is intended for enter the shell mode.

Syntax

shell

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# shell
BusyBox v1.15.3 (2017-09-05 14:59:00 +07) built-in shell (ash)
Enter 'help' for a list of built-in commands.
[admin@tau:/root]
```

upgrade image

The command is intended for updating the firmware.

Syntax

upgrade image <value1><value2>

Parameters

<value1> - TFTP server IP address where the firmware will be downloaded from;

<value2> - firmware file name (string: 64 characters)

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# upgrade image 192.168.118.46 tau24.img
update_tftp_fw.sh: set TFTP IP to 192.168.118.46
rm: cannot remove '/tmp/syslog.trace': No such file or directory
update_tftp_fw.sh: downloading IMG filename:
update_tftp_fw.sh: Copy bin files in /tmp/bin
tau-8#
```

configure

The command is intended for enter the configuration mode.

Syntax

configure

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

EXEC

Example

```
tau-8# configure
tau-8(config)#
```

Configuration level commands

network

The command is intended for enter the network interface configuration mode.

Syntax

network

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG

Example

```
tau-8(config)# network
tau-8(config-net)#
```

devname

The command is intended for setting the device name.

Syntax

devname <value>

Parameters

<value> - string: 96 characters

Privilegy

priv

Command mode

CONFIG

Negotiation function 'no' command

Set the default device name (default: TAU-8).

Example

```
tau-8(config)# devname tau8_hub
```

sip profile 1..8

The command is intended for enter the SIP profile N configuration mode.

Syntax

sip profile 1..8

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG

Example

```
tau-8(config)# sip profile 1
tau-8(config-sip-profile)#
```

udp rtpport sip min

Sets the minimum value of the range of UDP ports which are used to transmit RTP.

Syntax

udp rtpport sip min <value>

Parameters

<value> - number: 1024-65535

Privilegy

priv

Command mode

CONFIG

Negotiation function 'no' command

Sets the default minimum value of the range of UDP ports which are used to transmit RTP (default: 16384).

Example

```
tau-8(config)# udp rtpport sip min 10000
```

udp rtpport sip max

Sets the maximum value of the range of UDP ports which are used to transmit RTP.

Syntax

udp rtpport sip max <value>

Parameters

<value> - number: 1024-65535

Privilegy

priv

Command mode

CONFIG

Negotiation function 'no' command

Sets the default maximum value of the range of UDP ports which are used to transmit RTP (default: 32767).

Example

```
tau-8(config)# udp rtpport sip max 12000
```

voice port 1..8

The command is intended for enter the voiceports configuration mode.

Syntax

voice port 1..8

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG

Example

```
tau-8(config)# voice port 1
tau-8(config-voice-port)#
```

voice profile 1..8

The command is intended for enter the voice profiles configuration mode.

Syntax

voice profile 1..8

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG

Example

```
tau-8(config)# voice profile 2
tau-8(config-voice-profile)#
```

Network settings level commands

dhcp

Enables network interface configuration via DHCP.

Syntax

dhcp

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set static network setting configuration receiving mode

Example

```
tau-8(config-net)# dhcp
```

dhcp_gateway

The command is intended for using default gateway received via DHCP (default: don't use).

Syntax

dhcp_gateway

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Use default gateway, set in the device configuration

Example

```
tau-8(config-net)# dhcp_gateway
```

dhcp_dns

Enables the use of the DNS server received via DHCP (default: don't use).

Syntax

dhcp_dns

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Enables the use of the DNS server, which is set in the device configuration.

Example

```
tau-8(config-net)# dhcp_dns
tau-8(config-net)#
```

dns

Sets the IP address of the first external DNS server.

Syntax

dns <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default DNS server address (default: 192.168.1.1).

Example

```
tau-8(config-net)# dns 8.8.8.8
```

dns2

Sets the IP address of the second external DNS server.

Syntax

dns <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default DNS server address (default: 192.168.1.1).

Example

```
tau-8(config-net)# dns 54.34.23.6
```

dscp signaling

Sets the DSCP tag for transmission of SIP messages.

Syntax

dscp signaling <value>

Parameters

<value> - number:0-63

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default DSCP tag value (default: 26).

Example

```
tau-8(config-net)# dscp signaling 33
```

dscp media

Sets the DSCP tag for transmission of RTP/RTCP traffic.

Syntax

dscp media <value>

Parameters

<value> - number: 0-63

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default DSCP tag value (default: 46).

Example

```
tau-24(config-net)# dscp media 3
```

gateway

The command is intended for setting default gateway address.

Syntax

gateway <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the default factory IP address of the gateway (default: 192.168.1.1).

Example

```
tau-8(config-net)# gateway 192.168.118.99
```

ipaddr

Sets the IP address of network interface.

Syntax

ipaddr <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the factory IP address of network interface (default: 192.168.1.2).

Example

```
tau-8(config-net)# ipaddr 192.168.118.9
```

netmask

Sets a subnet.

Syntax

netmask <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the factory settings of subnet mask (default: 255.255.255.0).

Example

```
tau-8(config-net)# netmask 255.255.255.0
```

ntp enable

Enables the NTP protocol (default: disabled).

Syntax

ntp enable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable NTP.

Example

```
tau-8(config-net)# ntp enable
```

ntp ipaddr

The command is intended for setting remote time synchronization server address.

Syntax

ntp ipaddr <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default value of NTP server address (Default: 0.pool.ntp.org)

Example

```
tau-8(config-net)# ntp ipaddr 192.168.11.1
```

ntp timezone

The command is intended for setting the timezone.

Syntax

ntp timezone <value>

Parameters

<value> : -12..+12

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the factory settings of time zone (default: GMT0).

Example

```
tau-8(config-net)# ntp timezone +1
```

snmp enable

The command is intended for enabling SNMP.

Syntax

snmp enable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Disable SNMP.

Example

```
tau-8(config-net)# snmp enable
```

snmp trapsink

Sets the address of the SNMPv1-trap traps receiver.

Syntax

snmp trapsink<value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default trap destination address value (default: address is not set)

Example

```
tau-8(config-net)# snmp trapsink 192.168.118.7
```

snmp trapsink_v2

Sets the address of the SNMPv2-trap traps receiver.

Syntax

snmp trapsink_v2 <value>

Parameters

<value> - IP address

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Set the default trap destination address value (default: address is not set)

Example

```
tau-8(config-net)# snmp trapsink_v2 192.168.118.9
```

snmp rocomm

Sets a password to protect Settings reading.

Syntax

snmp rocomm <value>

Parameters

<value> - string:96 characters

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the factory password to protect Settings reading (default: public).

Example

```
tau-8(config-net)# snmp rocomm test
```

snmp rwcomm

Sets a password to protect Settings writing.

Syntax

snmp rwcomm <value>

Parameters

<value> - string:96 characters

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the factory password to protect Settings reading and writing (default: private).

Example

```
tau-8(config-net)# snmp rwcomm priv
```

snmp trapcomm

Sets a password contained in traps.

Syntax

snmp trapcomm <value>

Parameters

<value> - string:96 characters

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Sets the factory value for the password contained in traps (default: trap).

Example

```
tau-8(config-net)# snmp trapcomm testtrap
```

telnet

Enables access to the device via the telnet protocol.

Syntax

telnet

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Deny the access to the device via telnet protocol.

Example

```
tau-8(config-net)# telnet 192.168.1.7
```

ssh

Enables access to the device via the SSHv2 protocol.

Syntax

ssh

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Deny the access to the device via SSHv2 protocol.

Example

```
tau-8(config-net)# ssh 192.57.2.6
```

web enable

Enables access to the device via HTTP and HTTPS.

Syntax

web enable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-NETWORK

Negotiation function 'no' command

Deny the access to the device via HTTP and HTTPS.

Example

```
tau-8(config-net)# web enable
```

Port and port profiles settings level commands

username

The command is intended for setting username.

Syntax

username <value>

Parameters

<value> - string: 96 characters

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Set the default username (default: 00N).

Example

```
tau-8(config-voice-port)# username 772001
```

authname

Sets a user name for authentication.

Syntax

authname <value>

Parameters

<value> - string: 96 characters

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Sets the default user name for authentication (default: 00N).

Example

```
tau-8(config-voice-port)# authname 772001
```

password

The command is intended for setting authentication password.

Syntax

password <value>

Parameters

<value> - string: 96 characters

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Reset authentication password.

Example

```
tau-8(config-voice-port)# password 7U7r2tt1u
```

phone

The command is intended for setting suscriber port number.

Syntax

phone <value>

Parameters

<value> string: 96 characters

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Set the subscriber port number by default (default: 00N).

Example

```
tau-8(config-voice-port)# phone 1
tau-8(config-voice-port)#
```

profile sip

Sets Settings of the SIP profile for the FXS port.

Syntax

profile sip <value>

Parameters

<value> - number:1-8

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Set FXS port parameters of SIP profile 0.

Example

```
tau-8(config-voice-port)# profile sip 1
```

profile voice

The command is intended for assigning voice profile to port.

Syntax

profile voice <value>

Parameters

<value> - number:1-8 (default: 1)

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Example

```
tau-8(config-voice-port)# profile voice 1
```

disable

The command is intended for disabling FXS port.

Syntax

disable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Enable FXS port.

Example

```
tau-8(config-voice-port)# disable
tau-8(config-voice-port)#
```

custom

The command is intended for disabling voice profile settings usage.

Syntax

custom

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-VOICE-PORT

Negotiation function 'no' command

Enable voice profile settings usage.

Example

```
tau-8(config-voice-port)# custom
```

callerid

Sets a caller identification method.

Syntax

callerid<value>

Parameters

<value> - fsk_bell|fsk_v23||dtmf

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Disables caller identification.

Example

```
tau-8(config-voice-port)# callerid fsk
```

flash min

Sets the minimum value (ms) of the range of flash event detection.

Syntax

flash min <value>

Parameters

<value> - number:70-2000

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Set the lower range value of flash event detection by default, ms (default: 200).

Example

```
tau-8(config-voice-port)# flash min 70
```

flash max

Sets the maximum value (ms) of the range of flash event detection.

Syntax

flash max <value>

Parameters

<value> - number: 70-2000

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Set the upper range value of flash event detection by default, ms (default: 600).

Example

```
tau-8(config-voice-port)# flash max 700
```

hybrid rx

Sets the gain value (dB) for signals received in the differential system.

Syntax

hybrid rx <value>

Parameters

<value> - number: -230...-20

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Set the default value (default: -70).

Example

```
tau-8(config-voice-port)# hybrid rx -20
```

hybrid tx

Sets the gain value (dB) for signals transmitted in the differential system.

Syntax

hybrid tx <value>

Parameters

<value> - number: -170...-60

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Set the default value (default: 0).

Example

```
tau-8(config-voice-port)# hybrid tx 20
```

stopdial

The command is intended for enabling dial stop using # character.

Syntax

stopdial

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Disables option that stops dialing by entering # character.

Example

```
tau-8(config-voice-profile)# stopdial
tau-8(config-voice-profile)#
```

timer duration

Sets a value of the dialling timer (ms).

Syntax

timer duration<value>

Parameters

<value> - number: 0-60

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Sets the default value of the dialling timer (ms) (default: 30).

Example

```
tau-8(config-voice-port)# timer duration 6
tau-8(config-voice-port)#
```

timer waitanswer

The command is intended for setting reply waiting timer value.

Syntax

timer waitanswer <value>

Parameters

<value> - number: 0-120

Privilegy

priv

Command mode

CONFIG-VOICE-PORT, CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Set the default reply timer value, ms (default: 30).

Example

```
tau-8(config-voice-port)# timer waitanswer 55
tau-8(config-voice-port)#
```

profile name

Set a command name for FXS profile.

Syntax

profile name <value>

Parameters

<value> - string, 64 characters max

Privilegy

priv

Command mode

CONFIG-VOICE-PROFILE

Negotiation function 'no' command

Deletes the name specified to FXS profile.

Example

```
tau-8(config-voice-profile)# profile name ss9
tau-8(config-voice-profile)#
```

SIP profiles configuration level commands

proxy mode

Sets the mode of operation with SIP proxy server ('none' — do not use proxy server; 'park' — the parking mode; 'home' — the homing mode).

Syntax

proxy mode <value>

Parameters

<value> - none-don't use proxy;
-park – parking mode;
-home – homing mode.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default factory operation mode for SIP proxy server (default: none).

Example

```
tau-8(config-sip-profile)# proxy mode home
```

proxy address

Sets the address of the SIP proxy server.

Syntax

proxy address <value1><value2>

Parameters

<value1> - number: 1-5;

<value2> - address[:port]

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Sets the default address of the SIP proxy server (default: no address).

Example

```
tau-8(config-sip-profile)# proxy address 1 route.com:5063
```

registrar address

Sets the address of the SIP registrar server.

Syntax

registrar address <value1><value2>

Parameters

<value1> - number: 1-5;

<value2> - address[:port]

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Sets the default address of the SIP registrar server (default: no address).

Example

```
tau-8(config-sip-profile)# registrar address 1 route.com:5063
```

registrar enable

Enables registration on the SIP server.

Syntax

registrar enable <value>

Parameters

<value> - number: 1-5

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Deny registration on SIP server.

Example

```
tau-8(config-sip-profile)# registrar enable 1
```

registrar interval

The command is intended for setting reregistration interval value, sec.

Syntax

registrar interval <value>

Parameters

<value> - number: 10-3600

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Sets the default interval between repeated registrations (default: 300).

Example

```
tau-8(config-sip-profile)# registrar interval 400
```

domain

The command is intended for setting SIP domain.

Syntax

domain <value>

Parameters

<value> - string:96 characters

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Do not use SIP domain.

Example

```
tau-8(config-sip-profile)# domain voip.local
```

domain_to_reg

Enables the use of SIP domain for registration on the SIP server.

Syntax

domain_to_reg

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Deny the use of SIP domain during registration on SIP server.

Example

```
tau-8(config-sip-profile)# domain_to_reg
tau-8(config-sip-profile)#
```

expires

Sets the time of repeated registration on the SIP server (s).

Syntax

expires <value>

Parameters

<value> - number: 0-2147483647 (default: 1800)

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default reregistration time on SIP server (default: 1800).

Example

```
tau-8(config-sip-profile)# expires 3600
```

codec list

Configures the list of supported codecs (listed in the order of priority from the highest to the lowest one) (default: g711a, g711u).

Syntax

codec list <value>

Parameters

<value> - list of voice codecs separated by ‘space’ character g729a, g729b, g729x, g711a, g711u, g723, g726_24, g726_32.

Privilegy

priv

Command mode

CONFIG-SIP

Example

```
tau-8(config-sip-profile)# codec list g723
tau-8(config-sip-profile)#
```

codec ptime

This command is intended for setting voice codec packetization time, ms.

Syntax

codec ptime <value1><value2>

Parameters

<value1> - g729|g711|g723| g726_24 |g726_32;

<value2> - 5-120

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default packetization value (default: g729 – 20ms, g711 – 20ms, g723 – 30ms, g726_24 – 20ms, g726_32 – 20ms).

Example

```
tau-8(config-sip-profile)# codec ptime g726_24 30
tau-8(config-sip-profile)#
```

dtmfmode inband

Enables inband transmission of digits for extension dialling in RTP voice packets.

Syntax

dtmfmode inband

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default dialing signaling method (default: Inband).

Example

```
tau-8(config-sip-profile)# dtmfmode inband
tau-8(config-sip-profile)#
```

dtmfmode rfc2833

Use digit transfer of extension dialing according to RFC2833 as dedicated load in RTP voice packets.

Syntax

dtmfmode rfc2833

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default dialing signaling method (default: Inband).

Example

```
tau-8(config-sip-profile)# dtmfmode rfc2833
tau-8(config-sip-profile)#
```

dtmfmode info

Sets the transmission mode for digits of extension dialling.

Syntax

dtmfmode info <value>

Parameters

<value> - dtmf-relay|dtmf|audio

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default dialing signaling method (default: Inband).

Example

```
tau-8(config-sip-profile)# dtmfmode info dtmf
tau-8(config-sip-profile)#
```

fax detect

The command is intended for setting fax detection mode.

Syntax

fax detect <value>

Parameters

< value > – parameter value:
none - detection is disabled;
caller - detection on transmitting side;
callee - detection on receiving side;
both-detection on both sides (default).

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Disable the fax signal detection mode

Example

```
tau-8(config-sip-profile)# fax detect both
```

fax codec

Sets a codec for fax transmissions.

Syntax

fax codec <value>

Parameters

<value> - g711a|g711u|t38|none

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default codec to transmit fax messages (default: g711a).

Example

```
tau-8(config-sip-profile)# fax codec t38
```

fax enable_in_t38

Enables switching to T.38.

Syntax

fax enable_in_t38

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Deny the proceeding to T.38.

Example

```
tau-8(config-sip-profile)# fax enable_in_t38
tau-8(config-sip-profile)#
```

name

Sets the name of SIP profile N.

Syntax

name<value>

Parameters

<value> - string: 96 characters

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default name of SIP profile N. (Default: SIP_profile_N).

Example

```
tau-8(config-sip-profile)# name art
tau-8(config-sip-profile)#
```

ecan enable

The command is intended for enabling echocancellation feature.

Syntax

ecan enable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Disable echocancellation feature.

Example

```
tau-8(config-sip-profile)# ecan enable
```

ecan tail

Sets the dispersion time for reflected signals (ms).

Syntax

ecan tail <value>

Parameters

<value> - 8|16|32|48|64

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default time of a reflected signal dispersion, ms (default: 64).

Example

```
tau-8(config-sip-profile)# ecan tail 128
```

enable

Enables the use of SIP profile.

Syntax

enable

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Disables the use of SIP profile.

Example

```
tau-8(config-sip-profile)# enable
tau-8(config-sip-profile)#
```

vad

Enables voice activity detector.

Syntax

vad

Parameters

Command contains no arguments.

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Disables voice activity detector.

Example

```
tau-8(config-sip-profile)# vad
```

dialplan ltimer

The command is intended for setting L-timer value.

Syntax

dialplan ltimer <value>

Parameters

<value> - number: 1-30

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default L-timer value (default: 15).

Example

```
tau-8(config-sip-profile)# dialplan ltimer 10
```

dialplan stimer

The command is intended for setting S-timer value.

Syntax

dialplan ltimer <value>

Parameters

<value> - number: 1-10

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default L-timer value (default: 8).

Example

```
tau-8(config-sip-profile)# dialplan stimer 5
```

dialplan rule

The command is intended for setting the dial plan.

Syntax

dialplan rule <value>

Parameters

<value> - string: 1000 characters

Privilegy

priv

Command mode

CONFIG-SIP

Negotiation function 'no' command

Set the default dial plan (default: [xABCD*#].S)

Example

```
tau-8(config-sip-profile)# dialplan rule "S5 L15 xxxxxx|xxxxxxx"
```

TECHNICAL SUPPORT

For technical assistance in issues related to operation of ELTEX Enterprise Ltd. equipment, please contact our Service Center:

Feedback form on the website: **https://eltex-co.ru/support/**
Servicedesk: **https://servicedesk.eltex-co.ru/**

Visit ELTEX official website to get the relevant technical documentation and software, benefit from our knowledge base, send us an online request or consult with a Service Center specialist at our technical forum:

Official website: **https://eltex-co.ru/**
Technical forum: **https://eltex-co.ru/forum**
Knowledge base: **https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base**
Download center: **https://eltex-co.ru/support/downloads**