



ELTEXALATAU

Complete solutions for networking

TAU-8.IP

TAU-8.IP-W

User manual, version 1.9 (22.06.2015)

IP-telephony Customer gateway








Username: admin
Password: password

www.eltexalatau.kz

Software version	Kernel release	#39 Wed Jun 9 14:29:16 NOVT 2016
	Firmware version	#2.1.0.132
Document version	Issue date	Contents of changes
Version 1.9	09.09.2015	<p>Added:</p> <ul style="list-style-type: none"> – MAC-address filtration; – Automatic control of signal amplification; – Support of profiles for different call direction; – Echo suppressing; – 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. <p>Corrected:</p> <ul style="list-style-type: none"> – Timezone for Yekaterinburg; – Minimum time for detection of disconnection is decreased up to 200 ms; – Interrupting voice menu playing
Version 1.8	11.08.2015	<p>Added:</p> <ul style="list-style-type: none"> – Wizard is realized; – Voice menu is realized; – 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 for using regular expressions is added for call signal setting.
Version 1.7	27.05.2015	<p>Added:</p> <ul style="list-style-type: none"> – Display system information on the 'Information/System' page; – Access port settings via FTP protocol. <p>Corrected:</p> <ul style="list-style-type: none"> – Operation of the series selection groups by using STUN; – Problem of configuration upload; – VoIP operation is corrected for 3G/4G changeover; – Ring back tone problem during a call to a call group or a serial selection group; – vlan_priority configuration problem; – problem of <i>traceroute</i> 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	<p>Added:</p> <ul style="list-style-type: none"> – 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	<p>Added:</p> <ul style="list-style-type: none"> – Configuration of the device access ports; – NAT setting for TR-069; – SIP-server reservation setting; – Session time settings; – IMS settings; – Supporting two mode of three-way conference; – line reversal
Version 1.4	21.05.2013	<p>Added:</p> <ul style="list-style-type: none"> – Code setting based on IPSec technology; – Configuration serial selection groups
Version 1.3	31.01.2013	<p>Added:</p> <ul style="list-style-type: none"> – Autoconfiguration via DHCP; – Setup of the VoIP logging; – Setup of IGMP logging;

		<ul style="list-style-type: none">- Specific menu to set up SIP profiles ;- Specific menu to set up FXS profiles
Version 1.2	09.02.2012	Added: <ul style="list-style-type: none">- 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: <ul style="list-style-type: none">- Call groups settings;- Web-interface language selection (Russian/English);
Version 1.0	02.06.2011	First issue

SYMBOLS

Symbol	Description
Semibold font	Notes, warnings, chapter titles, headers and table titles are written in semibold font.
<i>Calibri Italic</i>	Important information is written by Calibri Italic.
	Analogue phone
	SIP-server
	TAU-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 are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.

CONTENTS

1 INTRODUCTION.....	7
2 DEVICE DESCRIPTION	8
2.1 Purpose	8
2.2 Design.....	8
2.3 Device characteristics.....	8
2.4 Architecture and the device operation principle	11
2.5 Key specifications.....	13
2.6 Design.....	14
2.6.1 The device front panel	14
2.6.2 Rear panel of the device	15
2.7 Light indication.....	15
2.8 Reset to the default settings.....	16
2.9 Delivery package	16
3 THE DEVICE CONFIGURATION VIA WEB-INTERFACE.....	17
3.1 Configuration order. Administrator access	17
3.1.1 System configuration. System menu.....	20
3.1.1.1 'Settings' submenu.....	20
3.1.1.2 'Access passwords' submenu	21
3.1.1.3 Autoprovisioning submenu	22
3.1.1.4 'Configuration' submenu	25
3.1.1.5 'Upgrade' submenu.....	25
3.1.2 Configure networking parameters of the device. 'Network' menu	26
3.1.2.1 'Network settings' submenu	26
3.1.2.1.1 'Network settings' submenu. 'Internet' service.....	27
3.1.2.1.2 'IPSec' submenu	34
3.1.2.1.3 'Wi-Fi' submenu	36
3.1.2.1.4 DHCP-Server submenu	38
3.1.2.1.5 'Local DNS' ('Hosts') submenu	39
3.1.2.1.6 'NAT rules' ('Port Forwarding') submenu	40
3.1.2.1.7 'Static routes' submenu	41
3.1.2.1.8 'SNMP' menu	43
3.1.3 'Print Server' menu	44
3.1.4 'PBX' menu	45
3.1.4.1 'SIP' submenu.....	45
3.1.4.1.1. Common settings.....	46
3.1.4.1.2. SIP profiles	47
3.1.4.2 'QoS' submenu	58
3.1.4.3 'FXS' submenu	59
3.1.4.3.1 FXS ports	59
3.1.4.3.2 FXS profiles.....	63
3.1.4.4 'Line acoustic signals' submenu	65
3.1.4.5 ' Hunt groups' submenu.....	66
3.1.4.6 'Pickup groups' submenu	68
3.1.4.7 'Serial groups' submenu.....	69
3.1.4.8 'Subscriber service control' submenu	70
3.1.4.9 'Cadence' submenu.....	71
3.1.4.10 'Call History' submenu	72
3.1.5 'Security' menu	72
3.1.5.1 'General' submenu	72
3.1.5.2 'Firewall Rules' submenu	73
3.1.5.3 MAC filter submenu	75
4 DEVICE MONITORING VIA WEB INTERFACE. ADMINISTRATOR ACCESS	76
4.1 'Info' menu.....	76
4.1.1 'System' submenu	76
4.1.2 'USB' submenu	76
4.2 'Status' menu	77
4.2.1 'System' subsystem.....	77
4.2.2 'Processes' submenu.....	78
4.2.3 'Interfaces' submenu	79

4.2.4 'WLAN' submenu	79
4.2.5 'Netstat' submenu	80
4.2.6 'IPtables' submenu	81
4.2.7 'Diagnostic' submenu	81
4.2.8 'Telephony' submenu	82
4.2.9 'Call History' submenu	84
4.3 'Log' menu	87
4.3.1 'Syslog Settings' submenu	87
4.3.2 'Syslog' submenu	88
4.3.3 'Kernel' submenu	89
4.4 Reboot of the device. 'Reboot' menu	89
5 ADDED SERVICE USAGE	90
5.1 Call transfer	90
5.2 Call Waiting	92
5.3 Three-way conference call	93
5.3.1 Local conference	94
5.3.2 Remote conference	95
6 AUTOPROVISIONING PROCEDURE OPERATION ALGORITHM VIA DHCP	96
APPENDIX 1. VOICE MENU USAGE FOR GATEWAY SETTINGS	98
APPENDIX 2. USAGE OF WIZARD MENU	99
ACCEPTANCE CERTIFICATE AND WARRANTY	102

1 INTRODUCTION

At the present time, IP-telephony is the most progressive telecommunication service. TAU-8.IP consumer gateways are developed (the device) to provide subscribers by VoIP services. The devices are produced in various modifications. They differs by set of interfaces and functionality.

TAU-8.IP VoIP consumer gateways allow you to connect up to 8 analogue phones to the packet-based data networks accessible via Ethernet interfaces.

The devices are oriented to the home users and small offices. It is perfect solution to provide underoccupied objects.

This operation manual describes intended use, main specification, rules of configuring, monitoring and firmware update for *TAU-8.IP* VoIP consumer gateways.

2 DEVICE DESCRIPTION

2.1 Purpose

TAU-8.IP device is high-performance VoIP consumer gateway with the full set of options which allow consumers to use VoIP advantages.

TAU-8.IP is designed to connection analogue phones and fax-modems to the IP network.

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

220 V External mains adapter provides power supply.

2.2 Design

There are two types of the device design distinguishing by set of interfaces and functionality (see Table 1).

Table 1 – Models

Module name	Presence of WAN interface	Number of FXS	Presence of Wi-Fi
TAU-8.IP	+	8	-
TAU-8.IP-W	+	8	+

TAU-8.IP-W devices have a built-in Wi-Fi adapter with capable to connect up to 2 external antennas. Built-in Wi-Fi adapter supports 802.11n technology, it allows you to provide data transmission service of the wireless network with superior QoS in contrast with the device supported 802.11g and 802.11b. In addition, the device stays backward compatible with the 802.11g and 802.11b devices.

2.3 Device characteristics

The device has the following interfaces:

- 8×RJ-11 ports to connect analogue phones;
- 1 Ethernet RJ-45 10/100BASE-T WAN port;
- WLAN 802.11n¹;
- USB2.0 port to connect bulk memory, USB – modem or printer.

Gateway is powered by external 12V DC adapter for 220V electrical networks.

¹ Only for TAU-8.IP-W

The device supports the next functions:

- *Network functions:*
 - PPPoE support (PAP, CHAP, MSCHAP authorization, PPPoE compression¹);
 - PPTP/L2TP support;
 - Static address support and DHCP (DHCP-client on WAN);
 - DNS support;
 - NAT support;
 - NTP support;
 - SNMP support;
 - QoS support;
- IP-telephony protocol: SIP;
- ToS for RTP, SIP packets;
- Echo cancellation (G.164, G.165 guidelines);
- Silence detector (VAD);
- Comfortable noise generator;
- 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;
- *Value added service:*
 - Call Hold;
 - Call Transfer;
 - Call Waiting;
 - Call FWD Busy;
 - Call FWD No answer;
 - Call FWD Unconditional;
 - DND (Do not disturb);
 - Call Pickup;
 - Caller ID: V.23, Bell202, DTMF;
 - Hotline;
 - CLIR – caller identity restriction;
 - Value added service control via phone;
 - Conference call;
- Firmware update via web-interface;
- Remote monitoring, configuring and settings: Web-interface, Telnet, FTP, SSH, SNMP, TR-069;
- Express setting menu;
- Voice menu support;
- Supporting MAC address filtration;
- Supporting automatic gain control on analogue lines;
- Loading user pitches for analogue lines.

¹It is not available in the current version

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

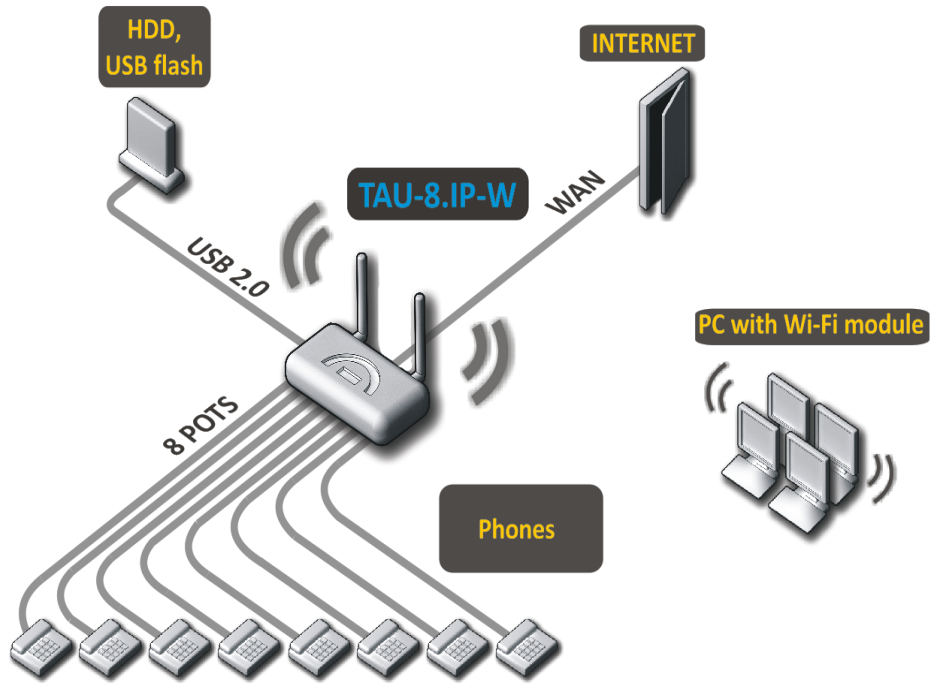


Fig. 1 – TAU-8.IP-W Functional diagram

2.4 Architecture and the device operation principle

TAU-8.IP/TAU-8.IP-W subscriber terminal consist of the following subsystem:

- Controller includes:
 - Mindspeed digital signal processor;
 - flash memory – 16MB;
 - SDRAM Operating storage – 256MB;
- SLIC Subscriber complex (8×FXS ports);
- Ethernet-module RJ-45 10/100/1000BASE-T WAN;
- Wi-Fi adapter (only for TAU-8.IP-W);
- USB-module.

Fig. 2 shows the device architecture diagram.

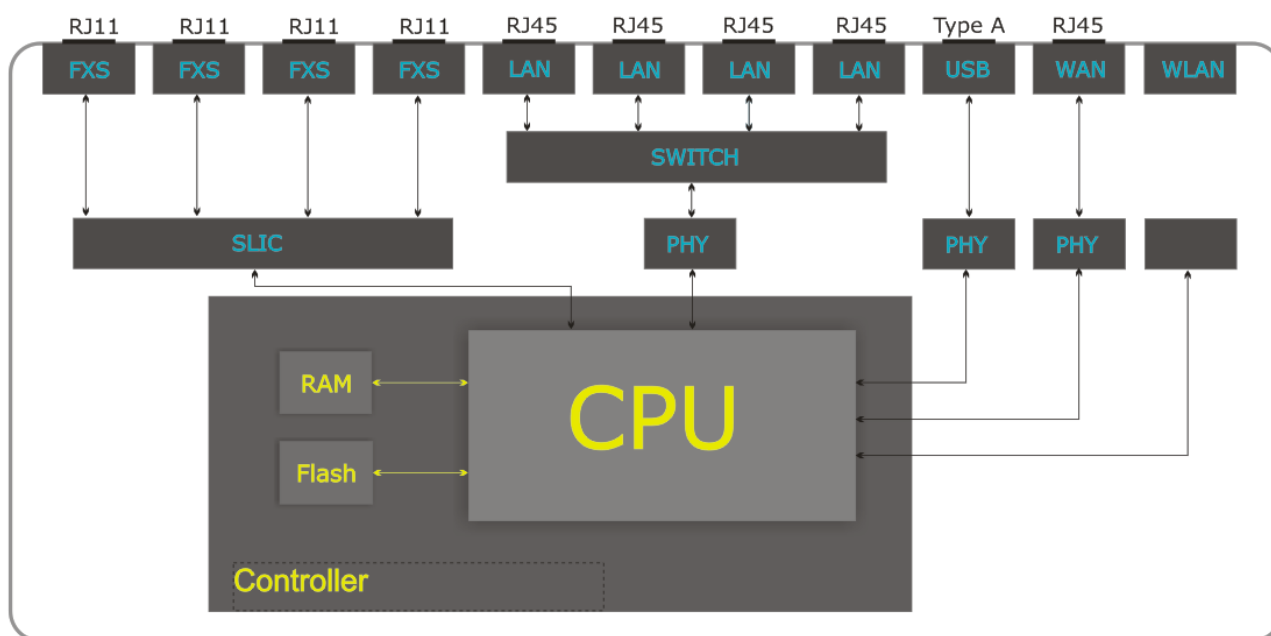


Fig. 2 – TAU-8.IP architecture diagram

TAU-8.IP architecture diagram differs by absence of Wi-Fi module.

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

The device can be divided into 4 blocks by functionality:

- Device network features block;
- VoIP block;
- Processing block of multicast traffic;
- Control block (Linux operation system).

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

VoIP block provides the device operation via SIP protocol to transmit voice signal through packet-switched network. Subscriber's voice signal is transmitted to the SLIC subscriber line module to be digitized.

Sampled signal is directed to VoIP block to be encoded in accordance with selected standards and is transmitted further in the form of digital packets to the controller via the intrasystem backbone. In addition to voice signals, digital packets contain control and interaction signals.

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

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

Fig. 3 shows TAU-8.IP function diagram.

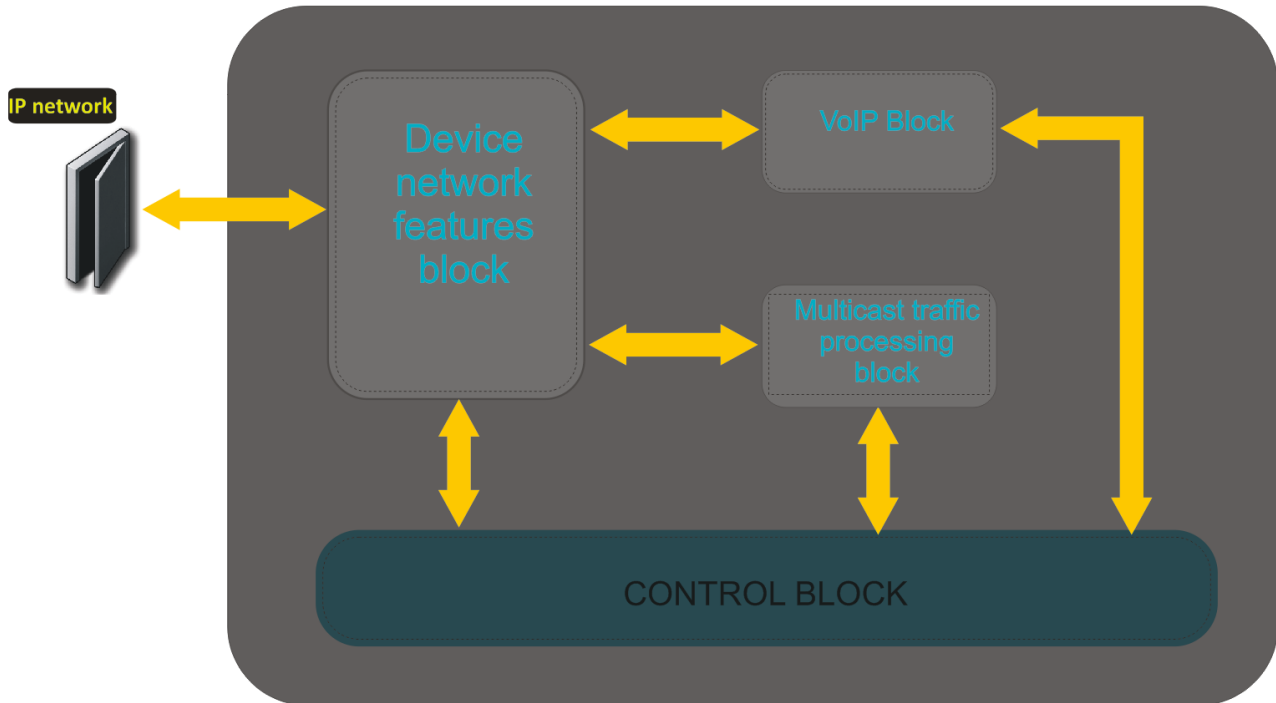


Fig. 3 – TAU-8.IP function diagram

2.5 Key specifications

Table 2 lists key specification of the device:

Table 2 – Key specifications

VoIP Protocols

Supported protocols	SIP
Fax support	T.38 UDP Real-Time Fax pass-thru (G.711A/U)
Modem support	V.152
Voice standards	VAD (silence suppression) AEC (echo cancellation, guideline G.165) CNG (comfortable noise generation)

Audio codecs

Codecs	G.729, annex A, annex B G.711a, G.711u G.723 Fax transmission: G.711a, G.711u, T.38 Modem transmission: G.711a, G.711u
--------	--

WAN-interface parameters for Ethernet

Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	autodetection, 10/100 Mbps, duplex/half-duplex
Standard	10Base-T/100Base-TX

Analogue subscriber ports parameters

Number of ports	8
Line loop resistance	Up to 1.5 kOhm
Typesetting reception	pulse/frequency (DTMF)
Caller ID getting	FSK V23, FSK Bell202, DTMF

Wireless¹ interface parameters

Standards	802.11 b/g/n
Frequency range, MHz	2400 ~ 2483,5
Modulation	BPSK, QPSK, 16 QAM, 64 QAM, DBPSK, DQPSK, CCK
Data bit rate, Mbps	802.11b(CCK): 1, 2, 5.5, 11 802.11g(OFDM): 6, 9, 12, 18, 24, 36, 48, 54 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: 16dBm 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
Security	64/128/152 bits WEP-data encryption; WEP, TKIP and AES

¹ Only for TAU-8.IP-W

Control

Remote control	Web-interface, Telnet, SSH, FTP, SNMP, TR-069.
Access restriction	By password

General Parameters

Power Supply	12V DC Power supply adapter	
Maximum power consumption:	TAU-8.IP	26,4 W
	TAU-8.IP-W	27,6 W
Operating temperature range	from +5 to +40°C	
Operation relative humidity when temperature is 25°C	up to 80%	
Dimensions	218x120x49 mm	
Weight	0,3 kg max	

2.6 Design

TAU-8.IP subscriber terminal enclosed into 218x120x49 mm plastic housing.

2.6.1 The device front panel

Fig. 4 shows front panel layout of the device

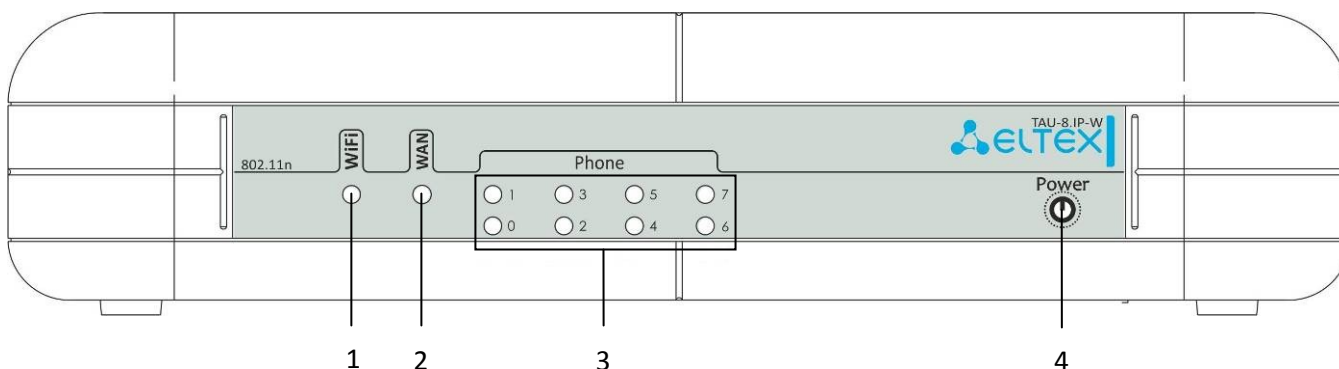


Fig. 4 – TAU-8.IP-W, front panel

Network indicators and controls are located on the front panel, table 3.

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

Front panel element		Description
1	WiFi	Operation indicator for wireless network
2	WAN	WAN-interface indicator
3	Phone	Analogue phones operation indicators
4	Power	Indicator of power supply and the device operation status

2.6.2 Rear panel of the device

The rear panel layout of the device is depicted in Fig. 5.

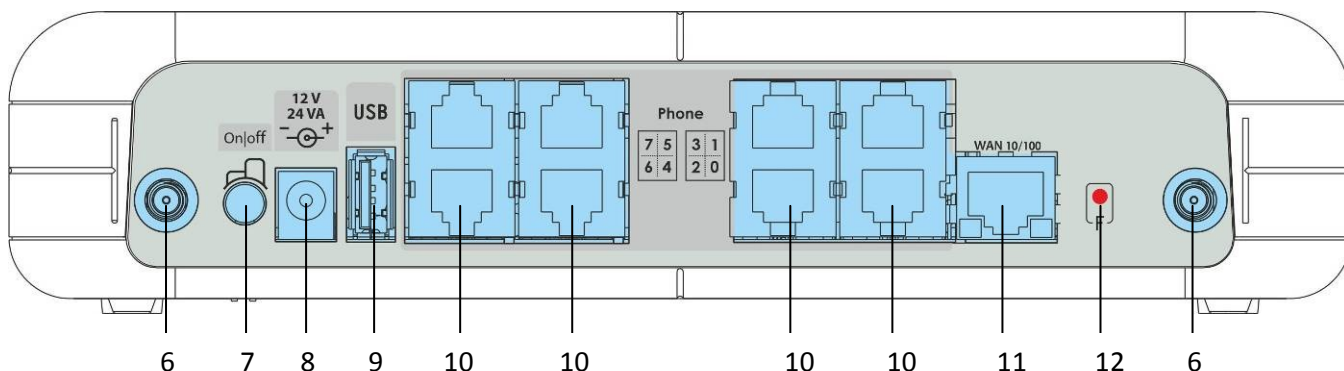


Fig. 5 – TAU-8.IP-W rear panel

The following connectors and controls are located on the rear panel, Table 4.

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

Front panel element		Description
6		Connector for Wi-Fi-antennas ¹ connection
7	On/Off	On-off main switch
8	12V	Connector to connect power adaptor
9	USB	USB connector for external memory connection
10	Phone	8×RJ-11 connectors for analogue phone connection
11	WAN	10/100BASE-T port, 100BASE-TX (RJ-45 connector) for connection to external network (WAN)
12	F	Functional button to reboot and reset the device settings to the default

2.7 Light indication

Wi-Fi¹, 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

Indicator	Indicator state	The device state
Wi-Fi ¹	Green	Wi-Fi- network is active
	Flashes	Data transfer process by using wireless network
WAN	Green (10 Mbps) or orange (100 Mbps)	Connection is established between station terminal and subscriber terminal
	Flashes	Packet data transmission process by using

¹ Only for TAU-8.IP-W

		WAN-interface
Phone	Green	The phone is off-hook
	Solid off	The phone is on-hook, normal operation
	Flashes during with 20 Hz frequency for 1 second, then 4 seconds pause	Incoming call is on the phone port
	Green, flashes slowly in periods	Subscriber port registration is absent at SIP-proxy server
Power	Green	Device power is enabled, normal operation
	Green	Reset the device to default settings
	Orange	No internet access available
	Red	The device loading

Table 6 – Light indication of Ethernet 100/10 interface

Indicator	Indicator status	The device status
Green	Solid on	10 Mbps connection with the external device is established
	Flashes	10 Mbps data transmission
Orange	Solid on	100 Mbps connection with the external device is established
	Flashes	100 Mbps data transmission

2.8 Reset to the default settings

In order 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 1** for more details).

2.9 Delivery package

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

- Universal TAU-8.IP subscriber terminal;
- power adaptor with 220/12V 2 A supply;
- 2 removable antenna (only for TAU-8.IP-W);
- Operation manual.

3 THE DEVICE CONFIGURATION VIA WEB-INTERFACE

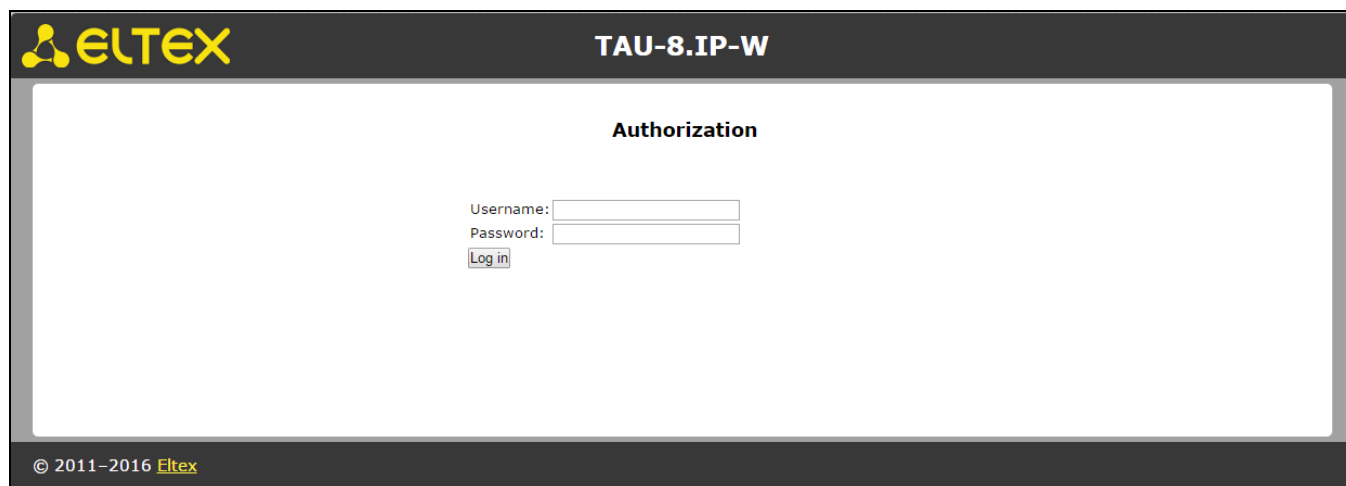
3.1 Configuration order. Administrator access

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 (since firmware version 2.0.0). Voice menu provides control of the received IP-address (See Appendix 1 for more details).

The device requires username and password after entering an IP-address.



The screenshot shows the ELTEX logo in the top left corner and the title 'TAU-8.IP-W' in the top right. The main content area is titled 'Authorization' and contains two input fields: 'Username:' and 'Password:'. Below these fields is a 'Log in' button. At the bottom left of the page, there is a copyright notice: '© 2011–2016 Eltex'.



For the first program start up, user name – *admin*, and password – *password*.

'Information' menu of the 'System' submenu will open after getting access to the web-configurator. Navigation elements of the WEB- configurator are depicted on Fig. 6.

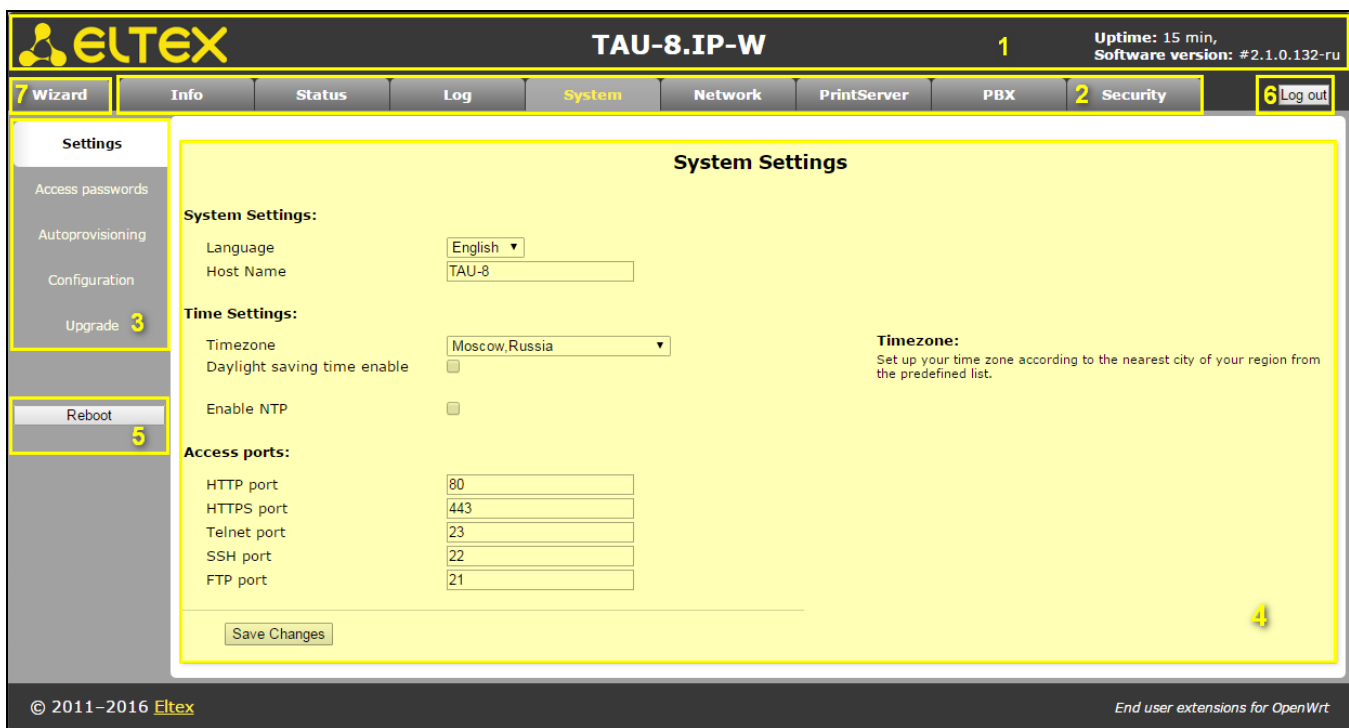


Fig. 6 – Web-configurator guidance elements

User interface window is divided into four 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 'Apply' button. In this case, settings for 'Log', '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. Configuration control buttons:
 - *Apply* – save the current configuration into non-volatile memory of the device and apply it;
 - *Cancel* – reset the device configuration to the settings saved into non-volatile memory;
 - *Reboot* – device reboot menu.
6. **Log out** is session termination button of the device access. TAU-8.IP includes two types of the users: **admin** and **user**. **Admin** (by default, password is **password**) has the full access to the device (read and write any settings, full device status monitoring). **User** (default password is **user**) may access device status monitoring without reading and recording configuration data.
7. **'Wizard'** tab for the device rapid configuration (see Appendix 2 for the detailed description).

Web-configuration language:

Web-configurator allows you to select one of the 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 Web- configurator on Russian language:

The screenshot shows the 'Информация о системе' (System Information) page in Russian. The interface includes a top navigation bar with tabs like 'Мастер', 'Информация', 'Статус', 'Журнал', 'Система', 'Сеть', 'Сервер печати', 'PBX', 'Безопасность', and 'Выход'. The main content area displays the following information:

Время и дата:	
Системное время	01:17:01
Дата	03-01-1970
Программное обеспечение:	
Версия ядра	#6 Thu Aug 6 15:25:37 NOV 2015
Версия прошивки	#2.0.0-ru
Информация об устройстве:	
Тип устройства	TAU-8.IP-W
Серийный номер	VI09000257
Заводской MAC адрес	A8:F9:4B:03:A4:6A

At the bottom, it shows '© 2011–2015 Eltex' and 'Расширения OpenWrt для пользователя'.

Example Web- configurator on English language:

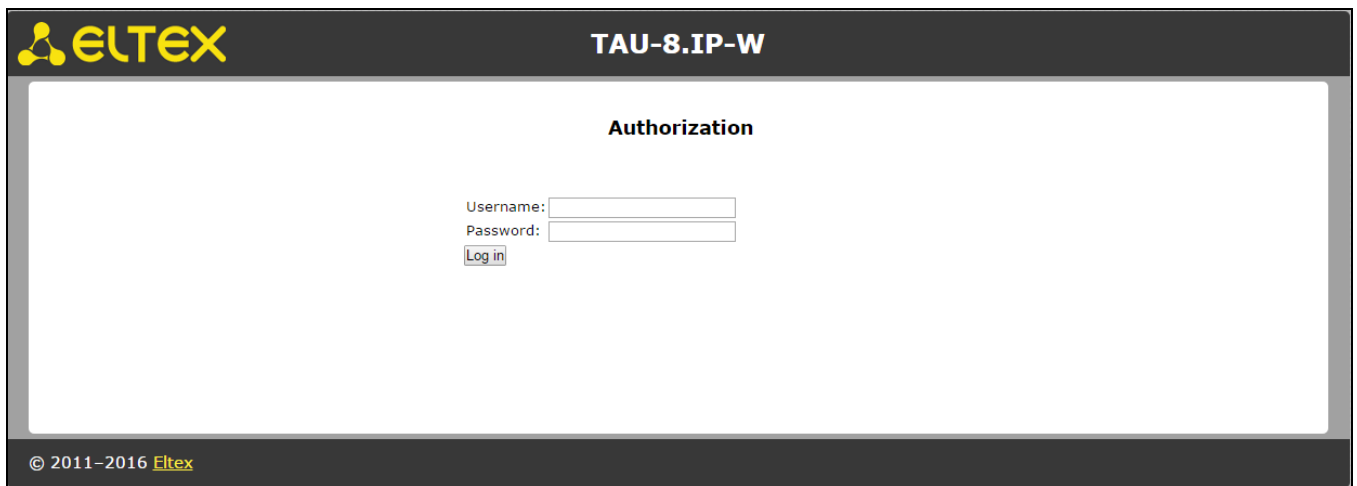
The screenshot shows the 'System Information' page in English. The interface includes a top navigation bar with tabs like 'Wizard', 'Info', 'Status', 'Log', 'System', 'Network', 'PrintServer', 'PBX', 'Security', and 'Log out'. The main content area displays the following information:

Time & Date:	
System time	01:15:31
Date	03-01-1970
Software:	
Kernel version	#6 Thu Aug 6 15:25:37 NOV 2015
Firmware version	#2.0.0-ru
Device information:	
Factory type	TAU-8.IP-W
Factory SN	VI09000257
Factory MAC	A8:F9:4B:03:A4:6A

At the bottom, it shows '© 2011–2015 Eltex' and 'End user extensions for OpenWrt'.

User change:

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



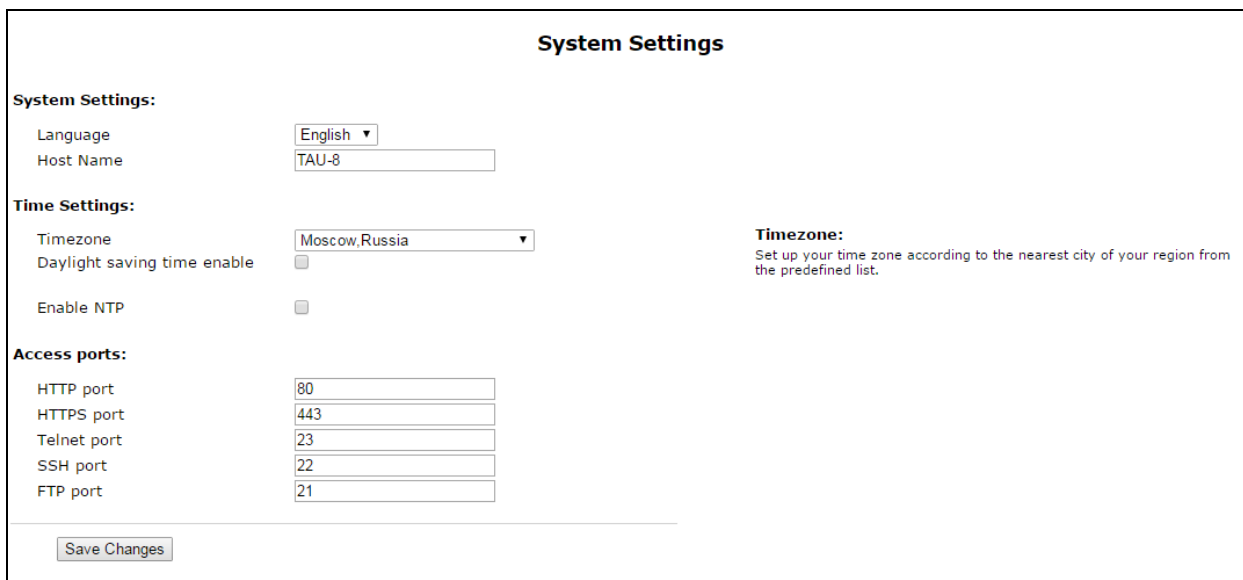
To change user, assign user name and password and click 'Log in' button.

3.1.1 System configuration. System menu

'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.

3.1.1.1 '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;

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

Access Ports:

- *HTTP port* – specify port for access via HTTP protocol;
- *HTTPS port* – specify port for access via HTTPS protocol;
- *Telnet port* – specify port for access via Telnet protocol;
- *SSH port* – specify port for access via SSH protocol;
- *FTP port* – specify port for access via FTP protocol.

To save changes into non-volatile memory of the device, click ‘Save Changes’ button. To record settings into non-volatile memory, click ‘Apply’ button.

3.1.1.2 ‘Access passwords’ submenu

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

TAU-8.IP includes two types of the users: **admin** and **user**. **Admin** (by default, password is **password**) has the full access to the device (read and write any settings, full device status monitoring). **User** (default password is user) may access device status monitoring without reading and recording configuration data.

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.



- Administrator login for access via Web-interface: *admin*.**
- Administrator login for access via Telnet and SSH protocols: *root*.**
- Unprivileged user login for access via Web-interface, Telnet, SSH, FTP: *user*.**



Access via FTP is available only for USER user.

Access passwords settings:

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

Click *'Change admin's password'* button to apply administrator password and *'Change user's password'* button to change password of unprivileged user.

3.1.1.3 Autoprovisioning submenu

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

Autoprovisioning

DHCP-based autoprovisioning:

Provisioning mode	<input type="text" value="Configuration & firmware"/>	<p>Provisioning mode: This option sets the target for auto updating mechanism: configuration only, firmware only or both.</p> <p>Priority from: When "Static settings" selected, the full paths to configuration and firmware files are taken from "Configuration file" and "Firmware file" parameters correspondingly. The full path is written as URL. TFTP, HTTP, HTTPS and FTP URLs are supported.</p> <p>If no full path is set, the following values are user by default: tftp://update.local/tau8.cfg – configuration file URL tftp://update.local/tau8.fw – firmware file URL</p> <p>When "DHCP options" selected, the full paths to configuration and firmware files are taken from DHCP options 43, 66 and 67. For this mechanism to work properly DHCP protocol must be set in one of the services. If it is impossible to get provisioning information from DHCP options, the following URLs will be used by default: tftp://update.local/<MAC>.<MAC>.cfg – configuration file URL (<MAC> is the MAC address of the device) tftp://update.local/tau8.fw – firmware file URL</p> <p>Configuration update interval, sec and Firmware update interval, sec: These parameters define the periods for configuration and firmware updating correspondingly. The value of 0 means that updating is done once after the device started.</p>
Priority from	<input type="text" value="DHCP options"/>	
Configuration update interval, sec	<input type="text" value="86400"/>	
Firmware update interval, sec	<input type="text" value="86400"/>	

TR-069 Configuration:

Enable TR-069 client	<input checked="" type="checkbox"/>	<p>ACS URL: The address of auto configuration server.</p> <p>Periodic inform enable: Tick if you want to send periodic inform messages to ACS-server.</p> <p>ACS connection request username and password: Username and password used to access the ACS-server.</p> <p>Client connection request username and password: Username and password used by ACS-server to access the local TR-069 client.</p> <p>NAT mode: There are three possible NAT mode settings: - STUN - STUN protocol is used to determine a public address automatically. You must have an active STUN server on your network to use this mode. The advantage of this mode is the connection between an ACS server and the device keeps running after a public address changes. - Manual - in this mode the public address is configured manually. The disadvantage of this mode is the connection between an ACS server and the device breaks after a public address changes. - Off - use this mode when there is no NAT between an ACS server and the device.</p>
ACS URL	<input type="text" value="http://update.local:9595"/>	
Periodic inform enable	<input checked="" type="checkbox"/>	
Periodic inform interval, sec	<input type="text" value="60"/>	

ACS connection request	
Username	<input type="text" value="acs"/>
Password	<input type="password" value="*****"/>

Client connection request	
Username	<input type="text" value="acs"/>
Password	<input type="password" value="*****"/>

NAT settings	
NAT mode	<input type="text" value="STUN"/>
STUN server address	<input type="text" value="stun.local"/>
STUN server port	<input type="text" value="3478"/>
Minimum keep alive period, sec	<input type="text" value="30"/>
Maximum keep alive period, sec	<input type="text" value="60"/>

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 autoprovigioning:
 - *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.1



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 when the device is launched.
- *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 update will be applied only once during the device start;
- *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 autoprovigioning operation algorithm in the chapter 6 **Autoprovigioning procedure operation algorithm via DHCP** .

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://x.x.x.x:10301 (x.x.x.x – ACS server IP-address or domain name, 10301 – ACS server port by default);

- *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 realized 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* – identifies the method that will be used by client for obtaining its public address information. The following modes are possible:
 - *STUN* – use STUN protocol for public address determination;
 - *Manual* – manual mode, when public address is explicit in configuration; in this mode, you should add a forwarding rule on a device that acts as a NAT for TCP port used by TR-069 client;
 - *Off* – *NAT will not be used*—this mode is recommended only when the device is directly connected to ACS server without network address translation. In this case public address will match local client address.

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

- *STUN server address* – STUN server IP address or domain name;
- *STUN server port* – STUN server UDP port (default value is 3478);
- *Minimum keep alive period, 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.

When *Manual* mode is selected, client public address should be entered with *NAT address* setting (in IPv4 format).

To save changes into operative memory, click '*Save Changes*' button. To store settings into the non-volatile memory, click '*Apply*' button.

3.1.1.4 'Configuration' submenu

In the 'Configuration' submenu, you may save 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 active to the first reboot of the gateway.

3.1.1.5 '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.

3.1.2 Configure networking parameters of the device. '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.

3.1.2.1 'Network settings' submenu

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

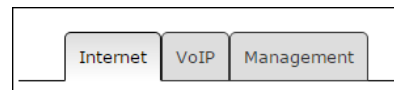
To connect the device to the provider's network, you should to check the network settings with operator. When static settings are used, in the field '*Protocol for address getting on WAN*' you should select '*Static*' value and full 'WAN IP Address', 'WAN subnet mask', '1st DNS', '2nd DNS' and 'The default 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 realized by 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.

3.1.2.1.1 'Network settings' submenu. 'Internet' service

Network Settings (Internet)

Internet
VoIP
Management

WAN Settings:

Connection mode:

Type of WAN Traffic:

Protocol for WAN:

Alternative vendor ID (option 60):

Vendor ID (option 60):

Get Default Gateway Automatically:

Get DNS-Servers Automatically:

IGMP Uplink:

MTU:

Wi-Fi:

Wi-Fi access mode:

Access configuration:

	HTTP	HTTPS	Telnet	FTP	SSH	SNMP
WAN access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
WLAN access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Common settings:

1st DNS-server:

2nd DNS-server:

Run Local DNS-server:

IGMP Proxy:

Default Gateway:

WAN MAC address:

Speed and duplex:

[Check internet connection availability:](#)

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 link '*Setup 3G/4G USB modem*'.

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.

USB Modem Configuration

Adding of a new provider:

Provider

Active provider

Connection protocol

User Name

Password

Service-Name

MTU

Additional parameters

Called number

Access configuration **Web** **Telnet** **FTP** **SSH**

USB Modem Configuration:
 You usually should configure Additional parameters and Called number only 3G-connection to establish. You can get these parameters from your mobile provide

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 server):

- *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);

Type of WAN Traffic

VLAN ID

Priority (802.1p)

- *VLAN ID* – VLAN ID used for the service;
- *Priority (802.1p)* – 802.1p 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:

Protocol for WAN	Static ▾
WAN IP address	192.168.0.115
WAN netmask	255.255.255.0
IGMP Uplink	<input type="checkbox"/>
MTU	1500

- *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. The default value is 1500. The field is active only when 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 – network mask;
- 3 – default network gateway address;
- 6 – DNS address;
- 12 – device network name;
- 28 – network broadcast address;
- 33 – static routes;
- 42 – NTP server address;
- 43 – specific vendor information;
- 66 – TFTP server address;
- 67 – firmware file name (for download via TFTP from the server specified in Option 66);
- 121 – classless static routes.

After selecting «DHCP» type, the following settings will be available for editing:

Protocol for WAN	DHCP ▾
Alternative vendor ID (option 60)	<input checked="" type="checkbox"/>
Vendor ID (option 60)	VOIP-Eltex-TAU-8.IP
Get Default Gateway Automatically	<input type="checkbox"/>
Get DNS-Servers Automatically	<input checked="" type="checkbox"/>
IGMP Uplink	<input type="checkbox"/>
MTU	1500

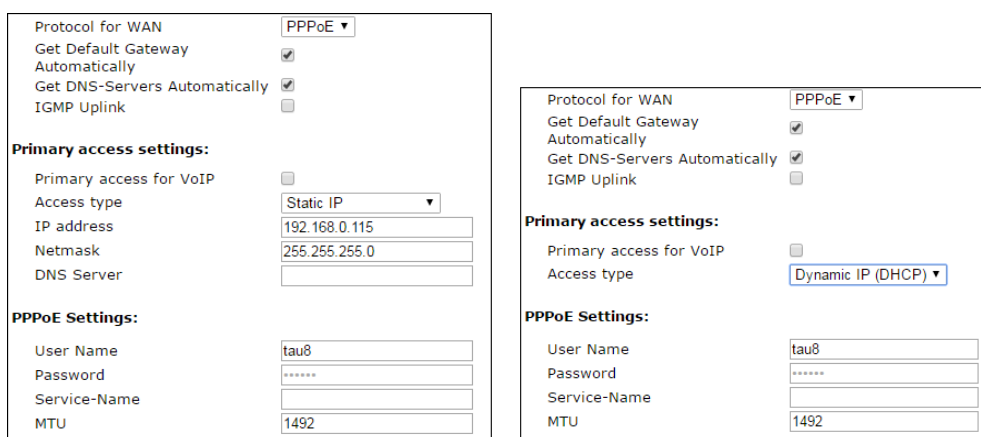
- *Alternative vendor ID (option 60)* – when checked, the device transmits *Vendor ID* (option 60) value of 'Vendor class ID' field by DHCP-messages of option 60. When the field is empty, the 60 option is not transmitted by DHCP protocol messages. If *Alternative Vendor ID (option 60)* is not set – the default value is transmitted by option 60. This value has the following format:
[VENDOR:manufacturer][DEVICE:device type][HW:hardware] [SN:serial number]
[WAN:MAC address of WAN interface][LAN:MAC address of LAN interface][VERSION:firmware version]

Example:

[VENDOR:Eltex][DEVICE:TAU-8.IP][HW:1.6][SN:VI33007740]
 [WAN:A8:F9:4B:09:31:B0][LAN:02:20:80:a8:f9:4b][VERSION:#2.1.0.132]

- *Get Default Gateway Automatically* – when checked, by default, gateway option (from DHCP option 3) will be automatically accepted from DHCP server. The flag can be set only in one service;

- *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 device. When flag is set, multicast traffic will be received from WAN-interface of the service. Option can be enabled 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. The default value is 1500. The field is active when the bridge mode is disabled.
- **PPPoE** – operation mode, at which PPP-session is established on WAN-interface via PPPoE protocol. When 'PPPoE' is chosen, the following parameters will become available for editing:



The image shows two side-by-side screenshots of a configuration interface for PPPoE. Both screenshots have 'Protocol for WAN' set to 'PPPoE'. The left screenshot shows 'Get Default Gateway Automatically' and 'Get DNS-Servers Automatically' checked, and 'IGMP Uplink' unchecked. Under 'Primary access settings', 'Primary access for VoIP' is unchecked, and 'Access type' is 'Static IP'. The IP address is 192.168.0.115 and the netmask is 255.255.255.0. Under 'PPPoE Settings', the User Name is 'tau8', Password is masked with asterisks, Service-Name is empty, and MTU is 1492. The right screenshot shows the same top options, but 'Access type' is 'Dynamic IP (DHCP)'. The 'PPPoE Settings' are identical to the left screenshot.

- *Get Default Gateway Automatically* – when checked, gateway, by default, will be gotten from PPP server automatically (this flag can be set only in one service);
- *Get DNS-Servers Automatically* – when checked, DNS-server addresses will be gotten from PPP-server automatically (this flag can be set in several services);
- *IGMP Uplink* – option is available only for TAU-8.IP-W device. When flag is set, multicast traffic will be received from WAN-interface of the service. Option can be enabled only in one service. WAN interface of the service, for which *IGMP Uplink* flag is set, will be used for IPTV signal reception;

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 realization.

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 IPSec¹ allows for the higher security level compared to PPTP and guarantees the higher level of protection for business-critical data.

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

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

PPTP/L2TP Settings:	
Primary access for VoIP	<input checked="" type="checkbox"/>
Access type	Static IP ▾
IP address	192.168.16.105
Netmask	255.255.255.0
Gateway	
DNS Server	192.168.16.112
PPTP/L2TP Server address	192.168.16.251
User Name	user
Password	*****
MTU	1462

PPTP/L2TP Settings:	
Primary access for VoIP	<input checked="" type="checkbox"/>
Access type	Dynamic IP (DHCP) ▾
Alternative vendor ID (option 60)	<input type="checkbox"/>
PPTP/L2TP Server address	192.168.16.251
User Name	user
Password	*****
MTU	1462

- *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 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 PPTP protocols and L2TP.

¹IPSec is not supported in the current firmware version.

- *IGMP Uplink* – option is available for TAU-8.IP-W device – when checked; the multicast traffic will be received from WAN interface of the service. Option can be enabled only in one service. WAN interface of the service, where *IGMP Uplink* is set, will be used to receive IPTV signals.

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 should be filled 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 and 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;
- *Default Gateway* – network gateway address by default. All traffic, which does not correspond to none routing static rule, will transmitted to this address.



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.

Check internet connection availability:	
Ping server 1	<input type="text"/>
Ping server 2	<input type="text"/>
Ping server 3	<input type="text"/>
Ping server 4	<input type="text"/>
Ping server 5	<input type="text"/>
Server reply waiting interval, sec	<input type="text" value="3"/>
Server retry access count	<input type="text" value="3"/>
Next cycle timeout, sec	<input type="text" value="5"/>

- *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 into the device operative memory, click ‘Save Changes’ button. To write settings into non-volatile memory, click ‘Apply’ button.

3.1.2.1.2 ‘Network settings’ submenu, VoIP services and Management

Internet	VoIP	Management				
Enable service VoIP <input checked="" type="checkbox"/>						
WAN Settings:						
Type of WAN Traffic	Tagged ▾					
VLAN ID	<input type="text"/>					
Priority (802.1p)	0 ▾					
Protocol for WAN	Static ▾					
WAN IP address	<input type="text"/>					
WAN netmask	<input type="text"/>					
IGMP Uplink	<input type="checkbox"/>					
MTU	<input type="text"/>					
Wi-Fi:						
Wi-Fi access mode	Off ▾					
Access configuration:						
	HTTP	HTTPS	Telnet	FTP	SSH	SNMP
WAN access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WLAN access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Save Changes"/>						

Internet	VoIP	Management				
Enable service Management <input checked="" type="checkbox"/>						
WAN Settings:						
Type of WAN Traffic	Tagged ▾					
VLAN ID	<input type="text"/>					
Priority (802.1p)	0 ▾					
Protocol for WAN	Static ▾					
WAN IP address	<input type="text"/>					
WAN netmask	<input type="text"/>					
IGMP Uplink	<input type="checkbox"/>					
MTU	<input type="text"/>					
Wi-Fi:						
Wi-Fi access mode	Off ▾					
Access configuration:						
	HTTP	HTTPS	Telnet	FTP	SSH	SNMP
WAN access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WLAN access	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 section 3.1.2.1.1. 'Network settings' submenu, 'Internet' service.

To save changes into operative memory of the device, click 'Save changes' button. To write settings into non-volatile memory, click 'Apply' button.

3.1.2.2 'IPSec' submenu

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

IPSec settings:

IPSec enable

Name of service Internet ▼

Local IP address

Local subnet

Local netmask

Remote subnet

Remote netmask

Remote gateway

Security protocol esp ▼

Manual key exchange method

NAT-Traversal IPsec off ▼

Aggressive mode

My identifier type address ▼

My identifier

Phase 1

Pre-shared key

IKE authentication algorithm md5 ▼

IKE encryption algorithm des ▼

Diffie Hellman group 1 ▼

Phase 1 lifetime, sec

Phase 2

Authentication algorithm hmac_md5 ▼

Encryption algorithm des ▼

Diffie Hellman group 1 ▼

IPSec SA lifetime, sec

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* determines address of remote subnet for connection with using encryption via IPSec protocol. If mask has value 255.255.255.255 then connection is established with a single host. Mask (distinct from 255.255.255.255) allows you to specify 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 providing access to the remote subnet;
- *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. 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. NAT-T operation modes.

You can choose one of the three NAT-T operation modes:

- *on* – NAT-T mode is activated only if 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:

- *NAT-T UDP port* – UDP-port of packets for IPSec message encapsulation. Default value is 4500;
- *NAT-T keepalive, sec (Interval between sending NAT-T keepalive packets, sec)* – periodic messages transmission interval for UDP connection keepalive on the device performing NAT function;
- *Aggressive mode* – phase 1 operation mode when all the necessary information is exchanged by 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 type.

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

- *Pre-shared key*;
- *IKE authentication algorithm* – select an authentication algorithm from the list: MD5, SHA1, SHA256, SHA384, SHA512;
- *IKE 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 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, se (IPSec SA lifetime)* – 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:

Manual key exchange method	<input checked="" type="checkbox"/>
Authentication algorithm	hmac-md5
Authentication key	<input type="text"/>
Encryption algorithm	des-cbc
Encryption key	<input type="text"/>
Security Parameter Index	<input type="text"/>
Remote subnet start IP address	<input type="text"/>
Remote subnet address count	<input type="text"/>

- *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.

3.1.2.3 'Wi-Fi' submenu

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

Wi-Fi Configuration

Wi-Fi Configuration:

<p>Enable Wi-Fi <input checked="" type="checkbox"/></p> <p>Wireless channel <input type="text" value="5"/></p> <p>Operating mode <input type="text" value="802.11bgn"/></p> <p>Security mode <input type="text" value="WEP"/></p> <p>WEP Keys</p> <p><input checked="" type="radio"/> <input type="text"/></p> <p><input type="radio"/> <input type="text"/></p> <p>Authorization on a RADIUS-server <input type="checkbox"/></p> <p>Replication of multicast traffic <input checked="" type="checkbox"/></p> <p>Maximum count of errors <input type="text" value="20"/></p> <p>Show advanced settings <input type="checkbox"/></p>	<p>Enable Wi-Fi: Tick if you want to set the Wi-Fi network active.</p> <p>Wireless channel: Choose one of the channels you want to use.</p> <p>Operating mode: Choose one of the modes you want to use: 802.11b, 802.11bg, 802.11bgn or 802.11n.</p> <p>Security mode: Authentication and encryption algorithms. WPA or WPA2 are recommended.</p> <p>WEP Keys: Choose one of WEP keys. WEP key must consists from hex digits and has length 10 or 26 symbols, or must consist symbols a-z, A-Z, 0-9, ~!@#%&^&*()_+ = and has length 5 or 13 symbols</p> <p>Replication of multicast traffic: Tick if you want multicast to go through Wi-Fi.</p>
---	--

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 ASCII¹ characters. 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 realized 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 you select any type of WPA authentication 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;
- *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.

¹ ASCII is a set of 128 characters for machine representation of capital and lower case Latin characters, digits, punctuation marks, and special symbols.

- *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);
 - *Enable WMM* – Wi-Fi Multimedia (WMM) operation mode setting. This operation mode allows you to quickly and efficiently transmit audio- and video content simultaneously with data transmission.

To save changes into the device operative memory click ‘*Save changes*’ button. To store settings into non-volatile memory, click ‘*Apply*’ button.

3.1.2.4 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

Enable DHCP relay

Local DHCP Server configuration:

Start address

Pool size

Lease time (minutes)

Static "MAC - IP" bindings:

MAC address	IP address	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add"/>

Static IP addresses:
The file /tmp/etc/ethers contains database information regarding known 48-bit ethernet addresses of hosts on an Internetwork. The DHCP server uses the matching IP address instead of allocating a new one from the pool for any MAC address listed in this file.

Active DHCP Leases

MAC address	IP address	Name	Expires in
There are no known DHCP leases.			

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.

To add IP address into the list with the static IP addresses for DHCP server, click 'Add' button.

To delete address from the list, click 'Delete' link against 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 into the device operative memory, click 'Save Changes' button. To record into non-volatile memory, click 'Apply Changes'.

3.1.2.5 'Local DNS' ('Hosts') submenu

Use the submenu to configure local DNS server of the device by adding 'IP address-domain name' pairs into the database.

Configured Hosts

Domain name table:

IP address	Domain name	Action
127.0.0.1	localhost.	<input type="checkbox"/> <input type="checkbox"/>

Add:

IP address

Domain name

Host configuration

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 the address from the list, select the checkbox next to the respective address and click 'Delete'.

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

3.1.2.6 'NAT rules' ('Port Forwarding') submenu

This 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, enabling connection. In general, port forwarding is necessary for torrent and P2P service operation. For this purpose, you should identify TCP/UDP ports used by a torrent or p2p client in their settings and assign the respective forwarding rules for your computer IP address.

Ports forwarding

Inbound Rules:

Name	LAN IP	LAN start port	LAN end port	Protocol	WAN IP	WAN start port	WAN end port	Action
rule1	192.168.34.5	1	65535	TCP/UDP		1	65535	<input type="checkbox"/> <input type="checkbox"/>

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:

Adding of a new rule

Type	Inbound	<p>Ports forwarding: Ports forwarding are applied immediately after clicking "Apply changes"</p> <p>LAN IP: IP address in internal network</p> <p>WAN IP: IP address in external network</p> <p>Start port, end port: Range of ports, rule will be applied to</p>
Name	<input type="text"/>	
LAN IP address	<input type="text"/>	
Traffic type	<input type="text" value="Any"/>	
WAN IP	<input type="checkbox"/>	

- *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 add record into non-volatile memory, click ‘*Apply*’ button.



The changes in the submenu are effective immediately after clicking ‘Apply Changes’ button. Reboot is not required.

3.1.2.7 ‘Static routes’ submenu

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

Route Table: Settings saved

Route Table:

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	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

Static Routes:

Route Name	Destination IP	Netmask	Gateway	Action
route1	32.62.211.2	255.255.255.255	192.168.16.112	<input type="checkbox"/> / <input type="checkbox"/>
route2	44.55.66.0	255.255.255.0	192.168.16.24	<input type="checkbox"/> / <input type="checkbox"/>
route3	23.2.2.23	255.255.255.255	192.168.16.250	<input type="checkbox"/> / <input type="checkbox"/>
route4	1.2.3.4	255.255.255.255	192.168.16.251	<input type="checkbox"/> / <input type="checkbox"/>
route5	46.6.7.0	255.255.255.0	192.168.16.250	<input type="checkbox"/> / <input type="checkbox"/>

Adding of a new route

Adding of a new route

Route Name

Destination IP

Netmask

Gateway



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* – path flag:
 - *G* – path uses a gateway;
 - *U* – path is active;
 - *H* – destination address is individual host;
 - *D* – set if the path was created after receiving a redirected ICMP message;
 - *M* – set if the path was modified by redirected ICMP message;
 - *!* – unoperated rout, packets will be dropped;
- *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 in 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 rout in the table, click 'Save' button.

To edit rout in the table 'Static routs' in the 'Action' column, click . To delete rout, click  button.

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



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

3.1.2.8 'SNMP' menu

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

SNMP settings:

SNMP enable

roCommunity

rwCommunity

TrapSink
usage: HOST [COMMUNITY [PORT]]

Trap2Sink
usage: HOST [COMMUNITY [PORT]]

InformSink
usage: HOST [COMMUNITY [PORT]]

Sys Name

Sys Contact

Sys Location

TrapCommunity

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 through 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 and 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,

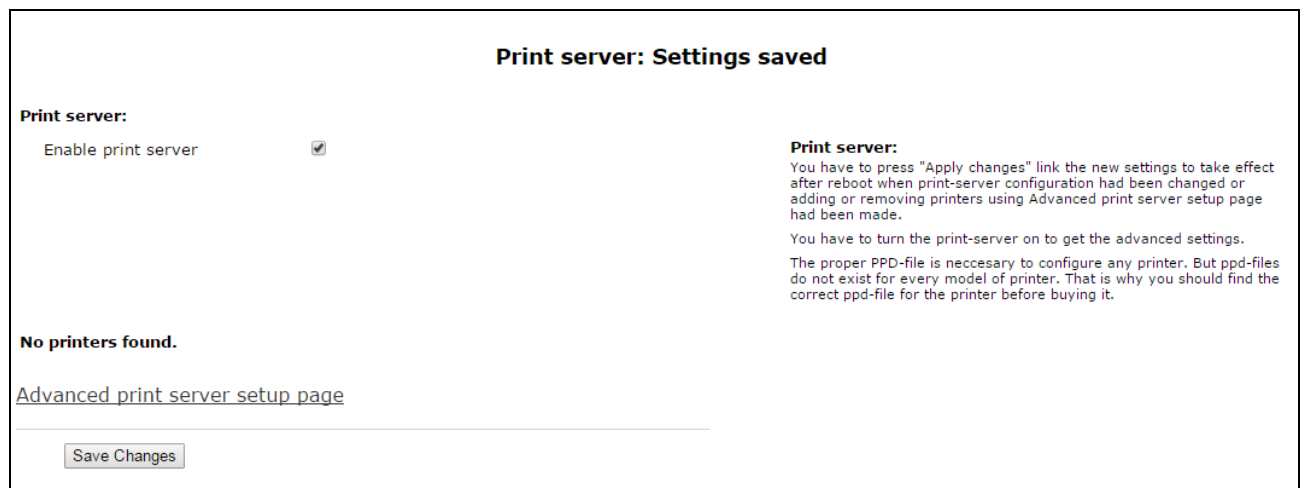
- Enterprise.3.1 – system log settings.

Where Enterprise – 1.3.6.1.4.1.35265.1.55 is the TAU-8.IP device identifier.

To save changes into the device operative memory, click ‘*Save Changes*’ button. To record settings into the non-volatile memory, click ‘*Apply*’ button.

3.1.3 ‘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:

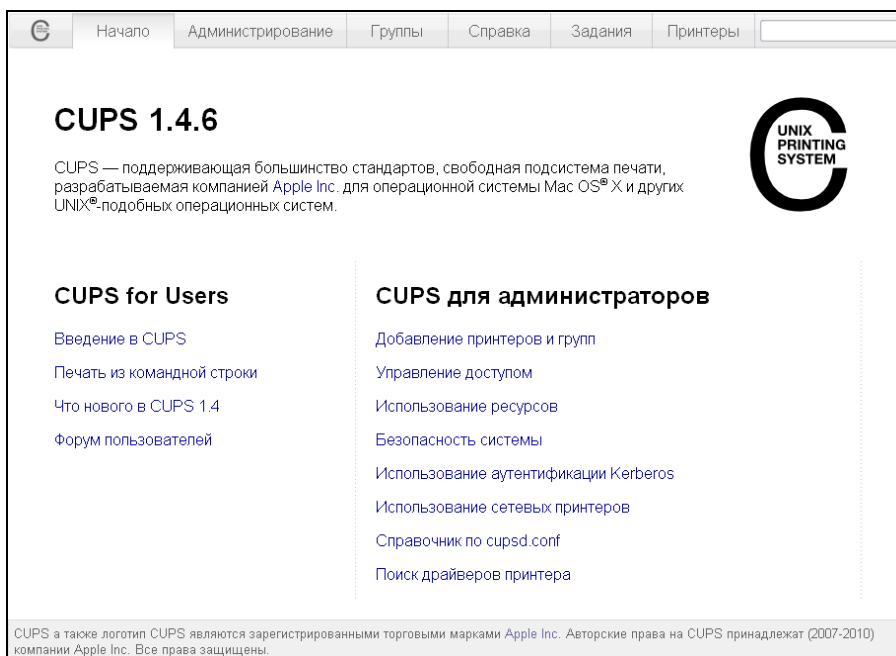
1. Go to ‘**Start menu → Printers and faxes**’ and select ‘**Installation of new printer → Network printer or printer connected to another PC → Connect to a printer via Internet, home network or intranet** and enter string with *URL*: <http://server:631/printers/model>.



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

2. Select preferred driver by using installation disk.
3. Installation is finished.

Also you may use page of advanced printer settings by clicking on the corresponding button. Page view is shown below:



On the page of advanced settings you may combine printers into groups, 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 record changes into the non-volatile memory, click '*Apply*' button.

3.1.4 '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.

3.1.4.1 '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 provides basic tasks for call control (for example session start and finish).

3.1.4.1.1. Common settings

SIP Configuration

Common settings
SIP profiles

SIP Configuration:

STUN enable	<input type="checkbox"/>	
STUN server address (:port)	<input type="text"/>	STUN server address: <small>IP address or domain name of STUN server. You can specify an alternative server port through the colon</small>
STUN request sending interval (sec)	<input type="text" value="300"/>	STUN request sending interval: <small>STUN request sending interval. The smaller sending interval the faster new public IP will be applied</small>
Public IP	<input type="text"/>	
Disable NAPTR DNS queries	<input type="checkbox"/>	
Disable SRV DNS queries	<input type="checkbox"/>	
Invite initial timeout (ms)	<input type="text" value="500"/>	
Retransmission interval for nonINVITE requests, ms	<input type="text" value="4000"/>	
Invite total timeout (ms)	<input type="text" value="32000"/>	
Transport	<input type="text" value="UDP (preferred), TCP"/>	









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 requests (STUN request sending interval)* – 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 and 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 operative memory, click ‘*Save Changes*’ button.

3.1.4.1.2. SIP profiles

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	

To edit profile, click  button in the colon ‘*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:

Activate profile:

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

SIP Configuration:

Proxy mode:

Proxy address (:port):

Registration:

Registrar address (:port):

Reserved SIP proxy:

Home server check:

Check method:

Keepalive timeout (s):

SIP domain:

Use domain to register:

Outbound mode:

Expires:

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:

Timer enable:

Min SE, sec:

Session expires, sec:

Keep alive NAT sessions:

Mode:

Keepalive timeout, s:

Three-party conference:

Mode:

Conference server:

IMS settings:

IMS mode:

XCAP name for call hold:

XCAP name for call waiting:

XCAP name for three-party conference:

XCAP name for hotline:

XCAP name for 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 controls 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 messages or by means of sending INVITE message 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 these two modes is as follows: As for the "Outbound" mode, if there is no registration on a SIP server, you will have the opportunity 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 "B3K" - "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 Ikratel 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 following 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.

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

For operations with redundant SIP-proxies, 'Parking' and 'Homing' modes will work as follows: the gateway sends INVITE message to the main SIP-proxy address when performing

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

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

- 1 In the 'parking' mode, the main SIP-proxy management is absent, and the gateway will continue operation with the redundant SIP-proxy even when the main proxy operation is restored. If the connection to the current SIP-proxy is lost, querying of the subsequent SIP-proxies will be continued using the algorithm described above. If the last redundant SIP-proxy is not available, the querying will continue in a cycle, beginning from the main SIP-proxy.
- 2 In the 'homing' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then to the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, gateway will use it to renew its registration. The gateway will begin operation with the main SIP-proxy.

- *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. As a rule, registration server is physically co-located with SIP proxy server (they have the same address);

Reserved SIP proxy – addition reserved SIP-proxy addresses:

Reserved SIP proxy:

Proxy address	Registration server
<input style="width: 90%;" type="text"/>	<input style="width: 90%;" type="text"/> <input type="checkbox"/>
<input type="button" value="Add"/>	<input type="button" value="X"/>

- *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* – periodic transmission of 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:
 - *Disable* – call will be routed according to the numbering schedule;
 - *Outbound* – numbering schedule is required for outgoing communications, however, all calls will be routed via SIP server; if there is no registration PBX response will be sent to the subscriber in order to enable subscriber service management (VAS management);
 - *Outbound with busy* – numbering schedule is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, VoIP will be unavailable: error tone will be transmitted to the phone headset. '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* caller equipment will receive response 180; upon receiving this message, caller equipment should send a local ringback tone into the line;
 - *183 Progress (Early media)* – caller equipment will receive response 183+SDP—used for voice frequency path forwarding before the answer of the callee. In this case, TAU-8.IP will send a ringback tone remotely to the 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 **3.1.4.9**;
- *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 username only in RURI*—when checked, only subscriber number (user) will be analyzed, and if the number matches, the call will be assigned to the subscriber port. When 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;
- *100rel* – use reliable provisional responses (RFC3262):
 - *Supported* – reliable provisional responses are supported;
 - *Required* – reliable provisional responses are mandatory;
 - *Off* – reliable provisional responses are disabled.

SIP protocol defines two types of responses for connection initiating request (INVITE)—provisional and final. 2xx, 3xx, 4xx, 5xx 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*;
- *Disabled* – do not send any of the following tags in INVITE request—*supported: 100rel* and *required: 100rel*. In this case, communicating gateway will perform unreliable transfer of provisional replies.

Setting operation for incoming communications:

- *Supported, Required* – when the following tag is received in 'INVITE' request—*supported: 100rel*, or *required: 100rel*—perform reliable transfer of provisional replies. If there is no 'supported: 100rel' tag in 'INVITE' request, the gateway will perform unreliable transfer of provisional replies;
 - *Disable* – 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, the 'timer' (RFC 4028) extension support is enabled. When connection is established, and both sides support 'timer' extension, one of them periodically sends re-INVITE requests for connection monitoring purposes (if both sides support UPDATE method, wherefore it should be specified in the 'Allow' header, the session update is performed by periodic transmission of UPDATE messages). 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 time, sec (Session expires, sec)* – 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 5.3.1;
 - *Remote* – conference assembly is performed at the remote server; after pressing 'flash+3', 'Invite' message will be sent to the server using number specified in the 'Conference server' field. In this case, conference operation complies with the algorithm described in RFC4579. For detailed algorithm description, see 5.3.2;
 - *Conference server* – in general, address of the server that establishes conference using algorithm described in RFC4579. Address is specified in the following format SIP-URI: user@address:port. You may specify the 'user' URI part only—in this case, 'Invite' message will be sent to the SIP proxy address;
- *IMS settings:*
 - *IMS mode* – service control configuration:
 - *Off* – simulation services by using IMS (3GPP TS 24.623) is disabled;
 - *Implicit* – implicit IMS subscription. Under this option, the gateway does not send SUBSCRIBE requests after subscriber registration, processing only NOTIFY requests received from IMS and used to manage subscriptions;
 - *Explicit* – explicit IMS subscription. Under this option, the gateway does not send SUBSCRIBE requests after subscriber registration, processing only NOTIFY requests received from IMS and used to manage subscriptions;
 - *XCAP name for call hold* – name of the XML element located in the 'Notify' message body that is used for transmission of 'Call hold' enabling/disabling commands. For example, if the service name value is 'call-hold', enabling command will be as follows:


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

 Disabling command:


```
<call-hold active="false"/>
```
 - *XCAP name for call waiting* – name of the XML element located in the 'Notify' message body that is used for transmission of 'Call waiting' enabling/disabling commands. For example, if the service name value is 'call-waiting', enabling command will be as follows:


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

 Disabling command:


```
<call-waiting active="false"/>
```
 - *XCAP name for three-party conference* – name of the XML element located in the 'Notify' message body that is used for transmission of 'Three-way conference call' enabling/disabling commands. For example, if the service name value is 'three-party-conference', enabling command will be as follows:


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

 Disabling command:


```
< three-party-conference active="false"/>
```
 - *XCAP name for hotline* – name of the XML element located in the 'Notify' message body that is used for transmission of 'Hotline' enabling command. In the enabling command, you should pass the hotline number and the call timeout. For example, if the service name value is 'hot-line-service' and you should call the number 30001 in 6 seconds after the phone handset is picked up, the enabling command will be as follows:


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

<timeout>6</timeout>

</hot-line-service>

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

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

< call transfer active="true"/>

Disabling command:

< call transfer active="false"/>

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

List of codecs in preferred order:

- *Codec 1..4* – 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:

- *G.711A*;
- *G.711U*;
- *G.723*;
- *G.729*;
- *G.729A*;
- *G.729B*;
- *off* – codec will not be used.

- *Packetization time, ms (G.711 PTE)* – count of ms in one RTP packet (for G.711A, G.711U and G.723 codecs);

- *DTMF transfer* – DTMF signal transmission method:

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

List of codecs in preferred order:

Codec 1	G.711A ▼
Codec 2	G.711U ▼
Codec 3	off ▼
Codec 4	off ▼
G.711 PTE	20 ▼
G.729 PTE	20 ▼
G.723 PTE	30 ▼
DTMF transfer	RFC2833 ▼
Fax Direction	Caller and Callee ▼

Fax transfer

Codec 1	G.711A ▼
Codec 2	Off ▼
Codec 3	Off ▼
Take the transition to T.38	<input checked="" type="checkbox"/>

Flash transfer rfc2833 ▼

Modem transfer (V.152) G.711A VBD ▼

Payload type for RFC2833 101 ▼

Use the same PT both for transmission and reception

Silencedetector

Echocanceller

RTCP

Dumb pass-thru

Jitter Buffer

Adaptive Jitter Buffer

Soft Deletion Mode

JB size for Fax/Modem 0

Min Delay 0

Max Delay 200

Deletion Threshold (DT) 500

Dispersion time 32 ms ▼

- *Fax Direction* – determine call direction for which fax tone detection is permitted. After that the transition to the fax codec will be performed:

- *No detect fax* – disable fax tone detection with saving fax transmission (transition to the fax codec will be not initiated, but the transition will be performed by opposite gateway);
- *Caller* – tones are detected only during fax transmission. During the fax transmission, CNG FAX signal is detected from the subscriber line;
- *Callee* – tones are detected only during fax reception. During the fax reception, V.21 signal is detected from the subscriber line;
- *Caller and Callee* – tones are detected during the transmission as well as reception. During the fax transmission, CNG FAX signal is detected from the subscriber line and V.21 signal during the fax reception;

Fax transfer can be realized by using G. 711 voice codec or special codec to transmit T.38 facsimile messages.

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

- *Fax transfer Codec 1..3* – you may select a codec and the .and an order of their usage. The highest priority codec should be specified in the 'Fax codec 1' field. For operation, you should specify at least one codec:

- *off* – codec is not used.
- *G.711a* – use G.711A codec;
- *G.711u* – use G.711U codec;
- *T.38* – use T.38 protocol.



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

- *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 is disabled;
 - *RFC2833* – flash transmission is provided in accordance with RFC2833 recommendation as a dedicated payload in RTP¹ 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;
- *Modem Transfer (V.152)* – determine the transfer in the 'Voice band data' (V.152 is recommended). Gateway disables voice activity detector (VAD) and generator comfort noise (CNG). It is necessary when modem connection is established;
 - *Off* – modem signal is not detected;
 - *G.711A VBD* –use G.711A codec for data transmission via modem connection. Switching to G.711A codec in the VBD mode is realized via CED tone detection;
 - *G.711U VBD* – use G.711U codec for data transmission via modem connection. Switching to the G.711U codec in the VBD mode is realized via CED tone detection;
 - *G.711A NSE* –CISCO NSE support. If data is transmitted via modem connection, G.711A codec is used;
 - *G.711U NSE* – CISCO NSE support. G.711U codec is used for data transmission via modem connection.



Selected codec should be enabled in voice codec list.

- *Payload type for RFC2833 packet transfer (Payload)* – payload type for packet transmission via RFC2833 (acceptable values for use are from 96 to 127);
- *Use the same PT both for transmission and reception* – when checked, use the same type of payload for transmission and reception;

¹ Flash transmission via RFC2833 is not available for firmware version 1.1.

- *Silencedetector* – when checked, use silence detector otherwise do not use it;
- *Echocanceller* – when checked, use echo canceller otherwise do not use it;
- *Use RTCP (RTCP)* – when checked, use RTCP protocol to control a voice channel. 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. But 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 device operative memory, click ‘Save’ button. To leave the edit mode without saving changes, click ‘Cancel’.

Dialplan Configuration:

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

Dialplan Configuration:

Short timer

Long timer

Digitmap:

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 operative memory of the device, click 'Save'. To leave the edit mode without saving changes, 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.

- Basis is the designations used for the dialed digit sequence recording. Digit sequence is recorded using several designations—digits dialed from the phone keypad: 0, 1, 2, 3, ..., 9, #, and *. **If you use # in the dialplan, you may block the dialing completion using this key!**
- Digit sequence enclosed in square brackets corresponds to any character enclosed in these brackets.
 - *Example: ([1239]) – corresponds to any digits 1, 2, 3 or 9*
- Use a hyphen to define a range of characters. Mostly used inside square brackets.
 - *Example 1: (1-5) – any digit from 1 to 5,*
 - *Example 2:([1-39]) – example listed above in the different entry format.*
- 'X' character corresponds to any digit from 0 to 9.
 - *Example: (1XX) – any 3-digit number that begins with 1.*
- «.» – repeat previous character from 0 ad infinitum..
- «+» – repeat previous character from 1 ad infinitum.
- {a,b} – repeat previous character from 'a' to 'b' times.
- {a,} – repeat previous character more than 'a' times.
- {,b} – repeat previous character less than 'b' times.
 - *Example: (810X.) – international number with any quantity of digits.*

Settings affecting dialplan configuration:

- *Interdigit Long Timer* – 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 feature allows you to replace the dialed sequence with any dialed character sequence. At that, the second argument should be defined with the specific value, both arguments may be empty.

- *Example1: (<83812:> XXXXXX) – this record will correspond to dialed digits 83812, but this sequence will be skipped and will not be sent to the 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 insertion to dialing

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

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

3. Dialing restriction

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

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

4. Replacement of dialing timer values

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

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

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

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

5. Direct address dialing (IP Dialing)

'@' placed after the number defines that the dialed call will be sent to the subsequent server address. We recommend using 'IP Dialing', as well as call reception and transmission without registration («Call Without Reg», «Answer Without Reg»). This may help when the server fails.

Also, IP Dialling address format may be used for numbers intended for the call forwarding.

- *Example 1: (8 xxx xxxxxxx) – 11-digit number beginning with 8.*
- *Example 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) – 11-digit number beginning with 8; if 7-digit number is dialed, add 8495 to number being sent.*
- *Example 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) – dialing of emergency call numbers and unusual sets of long-distance numbers.*
- *Example 4: (S0 <:82125551234>) – quickly dial the specified number, similar to 'Hotline' mode on other gateways.*
- *Example 5: (S5 <:1000> | xxxx) – this dialplan allows you to dial any number that contains digits, and if there was no entry in 5 seconds dial number '1000' (for example, it belongs to a secretary).*
- *Example 6: (*5x*xxxx*x#|*2x*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8,[2-9]xxxxxxxx|8, 10x.|1xx<:@10.110.60.51:5060>).*
- *Example 7: (1xx|0[1-9]|00[1-8]|*5x*xxxx*x#|*2x*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8,[2-9]xxxxxxxx|8, 10x.).*

Sometimes, you may need to make calls locally inside of the device. If IP address is unknown or periodically changing, you may use the reserved word «{local}». It means sending of the corresponding digit sequence to the own device address.

- Example: (123@{local}) – call to the 123 number will be locally processed inside of the device.

6. Pickup code configuration

You may set a pickup code for assigned group by using this command.

- Syntax: `ABC@{pickup:X}`

where `ABC` – pickup code (for example `*8`);

`X` – pickup group number (numbering from zero).

- Example: `112@{pickup:0}` – A and B subscribers are involved by one pickup group with index 0. If A subscriber receives the incoming call then B subscriber can pick up call by dialing 112 digit combination.

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 3.1.4.1.2).

- 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`.

To save changes into the device operative memory, click 'Save' button. To exit the editing mode without changes, click 'Cancel' button.

To record settings into the non-volatile memory, click 'Apply' button.



Changes in this menu will be applied immediately after pressing the 'Apply' button. Reboot is not required.

3.1.4.2 'QoS' submenu

Use this menu to configure QoS parameters.

QoS Configuration

SIP Configuration:		Reserved IP: <small>This IP address and the next one are used for the device's internal goals. The netmask is 255.255.255.0. It is forbidden to use IP addresses from this subnet by the external network interfaces of the device.</small>
UDP port min	<input style="width: 100%;" type="text" value="23000"/>	
UDP port max	<input style="width: 100%;" type="text" value="26000"/>	
RTP DSCP	<input style="width: 100%;" type="text" value="0x2e"/>	
Signalling DSCP	<input style="width: 100%;" type="text" value="0x1a"/>	
Reserved IP	<input style="width: 100%;" type="text" value="192.168.253.1"/>	
Bandwidth reservation	<input style="width: 100%;" type="text" value="0"/>	
<input type="button" value="Save Changes"/>		

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. 255.255.255.0 is subnet mask. It is not recommended to assign IP addresses from the subnet on external network interface;

To save changes into operative memory of the device, click 'Save changes' button. To record settings into the non-volatile memory, click 'Apply' button.



Changes in this submenu will be applied immediately after pressing the 'Apply' button. Reboot is not required.

3.1.4.3 '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.

3.1.4.3.1 FXS ports

For fast transition to 'Status/Telephony' submenu, click 'FXS status' (section 4.2.8) where monitoring statistic of customer unit status, call groups and series selection groups are available.

FXS Configuration

FXS status

Enabled	SIP profile	Phone	Username	Login	Password	SIP Port	Alternative number	FXS profile	Actions
FXS0 <input checked="" type="checkbox"/>	SIP profile 0 ▼	001	001	001	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS1 <input checked="" type="checkbox"/>	SIP profile 0 ▼	002	002	002	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS2 <input checked="" type="checkbox"/>	SIP profile 0 ▼	003	003	003	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS3 <input checked="" type="checkbox"/>	SIP profile 0 ▼	004	004	004	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS4 <input checked="" type="checkbox"/>	SIP profile 0 ▼	005	005	005	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS5 <input checked="" type="checkbox"/>	SIP profile 0 ▼	006	006	006	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS6 <input checked="" type="checkbox"/>	SIP profile 0 ▼	007	007	007	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>
FXS7 <input checked="" type="checkbox"/>	SIP profile 0 ▼	008	008	008	*****	5060	<input type="checkbox"/>	Default ▼	<input checked="" type="checkbox"/>

- *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 3.1.4.3.2 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:

<p>Port state FXS0:</p> <p>Enabled <input checked="" type="checkbox"/></p>

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

Account settings:

Account settings:	
SIP profile	SIP profile 0 ▼
Phone	001
Username	001
Login	001
Password	*****
SIP Port	5060
Alternative number	<input type="checkbox"/> <input type="text"/>
Calling party category	Off ▼

- 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 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. Receive value 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:

Line parameters:	
FXS profile	no profile ▼
Minimal on-hook time, msec	500
Min flash time, msec	200
Gain receive (x0.1dB)	-70
Gain transmit (x0.1dB)	0
Min pulse, msec	100
Interdigit, msec	200
Caller-Id generation	FSK Bell 202 ▼
Hangup timeout, sec	0
Ringback timeout, sec	0
Busy timeout, sec	120
Payphone	Off ▼
Rx AGC	<input type="checkbox"/>
Tx AGC	<input type="checkbox"/>
Stop dialing at #	<input type="checkbox"/>

- *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. Subscriber phone should support competent method for Caller ID operation:
 - *Off* – Caller ID is disabled;
 - *DTMF* – DTMF Caller ID method. The number is served between the first and second calls on the line by dual-frequency DTMF;
 - *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 data stream with a frequency modulation;



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

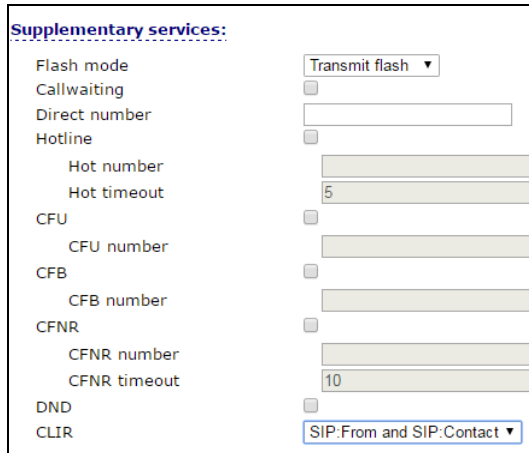


In FSK BELL 202 and FSK V.23 modes, Caller ID information is sent in SDMF format: time/data and number.

- *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;
 - *16 kHz* – when there is an outgoing call, tariff pulse with 16 kHz frequency will be sent in the line one time per second;
- *Automatic gain at the reception (Rx AGC)* – when checked, received signal will be amplified up to specified level (max gain is +/- 15 dB), otherwise gain is not enabled;
 - *Retrain margin of signal reception (Rx AGC level)* – identify retrain margin for received analogue signal gain (available values are -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).
- *Automatic gain at the transmission (Tx AGC)* – when flag is set, transmitted signal will be amplified up to specified level (max gain is +/-15dB), otherwise gain is not applied;
 - *Retrain margin of signal transmission (Tx AGC level)* – identify retrain margin to amplify analogue signal of transmission (available values are -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).

- *Stop dialing at #* – when checked, use ‘#’ button on the phone unit to end the dialing, otherwise ‘#’ will be recognized as a part of the number.

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 section **5 Added service usage**;
 - *Unattended calltransfer* – flash dialing will be processed locally by the device (call transfer will be performed when the subscriber finishes dialing a third party number). For 'Unattended calltransfer' detailed operation algorithm, see Section **5 Added service usage**;
 - *Local calltransfer* – call transfer inside the device without sending a message REFER. For 'Local calltransfer' detailed operation algorithm, see Section **5 Added service usage**;
- *Callwaiting* – when checked, 'Call waiting' service will be enabled otherwise – disabled (this service is available in 'flash—call transfer' function operation mode);
- *Direct number* – when the phone goes offhook, dial the defined number immediately;
- *Hotline/warmline* – when checked, 'Hotline/warm line' service is enabled. This service allows you to establish an outgoing connection automatically without dialing the number after the phone handset is picked up with the defined delay (in seconds). When checked, fill in the following fields:
 - *Hot 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.);
 - *Hot timeout, sec* – time interval that will be used for connection establishment with the opposite subscriber, in seconds;
- *Call forward unconditional (CFU)* – when active, all incoming calls will be forwarded to the specified number. When flag is set fill in the following fields:
 - *Call forward unconditional number (CFU number)* – number that all incoming calls will be forwarded to if 'CFU' service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule.);
- *Call forward on busy (CFB)* – when active, all incoming calls will be forwarded to the specified number, if the subscriber is busy. When flag is set fill in the following fields:

- *Call forward on busy number (CFB number)* – number that incoming calls will be forwarded to when the subscriber is busy and *Call forward on busy* service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule.);
- *Call forward on no answer (CFNA)* – when active, all incoming calls will be forwarded to the specified number, if there is no answer from the subscriber. When flag is set, fill in the following fields:
 - *Call forward on no answer (CFNA number)* – number that incoming calls will be forwarded to when there is no answer from the subscriber and *Call forward on no answer* service is enabled (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule.);
 - *CFNA timeout, sec* – time interval that will be used for call forwarding when there is no answer from the subscriber, in seconds;
- *Do not disturb (DND)* – when checked, temporary restriction is placed for incoming calls (DND service – Don't Disturb);
- *CLIR – caller ID service restriction:*
 - Off – 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.

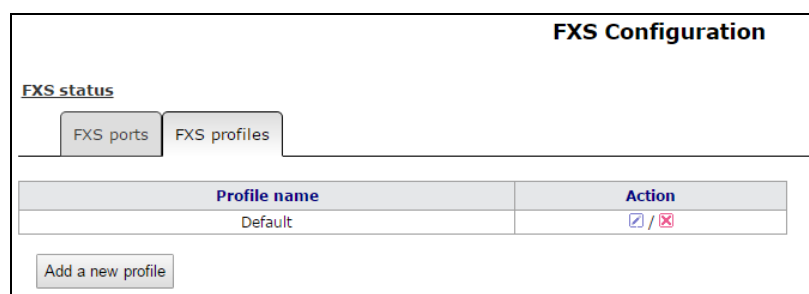
When multiple services are enabled simultaneously, the priority will be as follows (in the descending order):

- CFU;
- DND;
- CFB, CFNA.

3.1.4.3.2 FXS profiles

Click '*FXS status*' button for fast transition to the '*Status/Telephony*' submenu (section 4.2.8), where monitoring statistic of subscriber line unit, call group and serial group is 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 it, click button. To add new profile, click 'Add new profile' button. The list of FXS profile settings is shown below.

FXS profile:	
Profile name	<input type="text"/>
Minimal on-hook time, msec	<input type="text" value="800"/>
Min flash time, msec	<input type="text" value="200"/>
Gain receive (x0.1dB)	<input type="text" value="-70"/>
Gain transmit (x0.1dB)	<input type="text" value="0"/>
Min pulse, msec	<input type="text" value="100"/>
Interdigit, msec	<input type="text" value="200"/>
Caller-Id generation	<input type="text" value="FSK Bell 202"/>
Hangup timeout, sec	<input type="text" value="30"/>
Ringback timeout, sec	<input type="text" value="30"/>
Busy timeout, sec	<input type="text" value="60"/>
Payphone	<input type="text" value="Off"/>
Rx AGC	<input checked="" type="checkbox"/>
Rx AGC level	<input type="text" value="-25 dB"/>
Tx AGC	<input type="checkbox"/>
Stop dialing at #	<input type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- *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, ms* – minimal flash detection time, in milliseconds;
- *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, ms* – configuration is required for pulse dialing mode;
- *Min interdigit interval (Interdigit), in milliseconds* – configuration is required for pulse dialing mode;
- *Caller ID generation* – select mode for Caller ID generation. Subscriber phone should support competent method for Caller ID operation:
 - *Off* – number identification of calling subscriber is disabled;
 - *DTMF* – DTMF Caller ID method. The number is served between the first and second calls on the line by dual-frequency DTMF;
 - *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 data stream with a frequency modulation;



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* – 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;
- *Busy 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;
- *Payphone* – operation line settings for payphone connection:
 - *Off* – normal mode, payphone is disabled;
 - *Polarity reversal* – when this option is enabled, line voltage polarity reversal occurs right after the callee responses to the outgoing call;

- 12 kHz – when there is an outgoing call, tariff pulse with 12 kHz frequency will be sent in the line one time per second;
- 16 kHz – when there is an outgoing call, tariff pulse with 16 kHz frequency will be sent in the line one time per second;
- Automatic gain at the reception (Rx AGC) – when the flag is set, received signal will be amplified up to assigned level (max gain is +/- 15 dB), otherwise gain is not enabled;
 - Retrain margin of signal reception (Rx AGC level) – identify retrain margin for received analogue signal gain (available values are -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).
- Automatic gain at the transmission (Tx AGC) – when flag is set, transmitted signal will be amplified up to specified level (maximal gain is +/- 15 dB) otherwise gain is not applied;
 - Retrain margin of signal transmission (Tx AGC level) – identify retrain margin for analogue signal gain of signal transmission (available values are -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).
- Stop dialing at # – when checked, use '#' button on the phone unit to end the dialing, 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.

To save changes into the device operative memory, click 'Save changes' button. To record settings into non-volatile memory, click 'Apply' button.



Changes will be applied immediately after pressing 'Apply' button. Reboot is not required.

3.1.4.4 'Line acoustic signals' submenu

Use this submenu to load files with tone settings and restore the default tone settings.

Line acoustic signals

Load custom tones Выберите файл Файл не выбран

Restore default tones

Line acoustic signals:
File structure with default settings:

```
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
```

dialtone_freq - dial tone frequency, Hz (no more than two frequencies, which are separated by ",");
dialtone_time_rule - time intervals for signal with given frequency duration and pause, ms (duration and pause intervals are set to each frequency, time intervals are separated by ",").
Frequencies and time intervals for other signals are set the same way:
...-busytone - busy signal;
...-ringbacktone - ringback tone (RBT);
...-congestiontone - congestion tone (ATB) (signal which is played back in case when registration is absent and "Outbound on busy" option is selected for SIP->profile).

Limitations:
frequency ranges: 0 - 4000 Hz
time intervals ranges: 0 - 65535 ms

To load tone settings, click 'Select file' and select configuration file. After, click 'Load' button.

The tone configuration file should satisfy the following requirements (shown example presents 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 – frequencies of ‘Station response’ signal, Hz (up to two frequencies, frequencies are separated by comma ‘,’);

dialtone_time_rule – duration time intervals and signal pause with assigned frequency, in milliseconds (signal and pause durations are specified for each frequency, the time intervals are separated by comma ‘,’).

Frequencies and time intervals for other signals are specified analogically:

- *busytone* – ‘busy’ signal;
- *ringbacktone* – ‘Ring back tone’ (RBT) signal;
- *congestiontone* – signal when there is no registration and ‘Outbound on busy’ mode of SIP profile is disabled.

Value limit:

- frequency range: 0 – 4000 Hz
- time interval range: 0 – 65535 ms

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

To save changes into the device operative memory, click ‘Save changes’ button. To record settings into non-volatile memory, click ‘Apply’ button.

3.1.4.5 ‘Hunt groups’ submenu

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

Click ‘Go to the page Hunt groups status’ button to switch to the ‘Status/Telephony’ submenu (section 4.2.8), where monitoring statistic of customer unit status, hunt groups and series selection groups are available.

Hunt groups

[Go to the page Hunt groups status](#)

#	Group name	SIP profile	Phone	The group	Action
Add a new group					

Adding of a new group

Enable group

Group name

SIP profile

Phone

User Name

Password

Type of group

Call queue size

Call reply timeout, sec

SIP Port of group

Group call pickup enable

Phone:
Phone number assigned to this hunt group.

Type of group:
There 3 types of hunt groups: group, cyclic and serial. If type is group, the ringing voltage is applied to all ports in the hunt group simultaneously. If type is cyclic, the ringing voltage is applied in turns for each port in the Next port calling timeout. If type is serial, the number of called ports is incremented by one in the Next port calling timeout.

Call queue size:
The maximum number of unanswered calls the hunt group can accept.

Call reply timeout:
The incoming group call is cleared if it is not answered during this timeout.

SIP Port of group:
Alternative SIP-port of the hunt group.

Ports:
In order to add the FXS port to the serial group you must move it from the "Available" list to the "Added" list. The order of ports in the "Added" list also matters. The first port in the list will be called first

Added	Available
	FXS0
	FXS1
	FXS2
	FXS3
	FXS4
	FXS5
	FXS6
	FXS7

Ports

Save Cancel

Hunt groups provides functions of call processing center. The device is supported by 3 operation mode of hunt groups: group, serial and cyclic.

In *'group'* mode, the call will be sent to all the free group ports simultaneously. If one participant of call group answers, the call to other ports is stopped.



In *'serial'* mode call will be sent to the first free port in the list and, after specified timeout, the next free port from the list will be added to the main port. When one of the group participants answers, the call to the other free ports will be finished.

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 of 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* – call group signal will be sent to all the ports of group simultaneously;
 - *Serial* – port number, that call will be forwarded to, will be increased by one when zero value is defined for call timeout of the next port;
 - *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 record, click  button.

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



Changes in this submenu will be applied immediately after pressing *'Apply'* button. Reboot is not required.

3.1.4.6 '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 any calls directed at another subscriber of the group. In other words, each subscriber inside that belongs to the group may pick up the call received on any other port of the group by dialing pickup code. Use the Section 3.1.4.1.2 to configure a pickup code. For detailed information see section '*Dialplan Configuration*'.

Pickup groups

	FXS0	FXS1	FXS2	FXS3	FXS4	FXS5	FXS6	FXS7
Group0	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Permit to pickup incoming calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Pickup groups:
 Call pickup function is available for subscribers who are in the same pickup group as a called party.
 To assign a pickup group code you must write the regular expression such as:
ABC@{pickup:X}
 ABC – pickup code; X – the number of pickup group (counting from zero).
 For example, ***20@{pickup:0}**.

- *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 is transmitted to the subscriber phone unit covered by pickup group. If the subscriber can't answer to a call – another subscriber, that belongs to the pickup group and use the same SIP profile, can pick up incoming call. To do it, user should dial intercept code and after that connection with the calling user will be established.

Pay attention that the call interception is possible only when called client and picking up client use 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 belongs 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.

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



In the submenu, changes will be applied immediately after pressing '*Apply*' button. Reboot of the device is not required.

3.1.4.7 'Serial groups' submenu

In the serial group each new call occupies first free port thereby realizing 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 which 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 (section 4.2.8), where monitoring statistic of status for customer unit, call group and series selection is available.

Serial groups: Settings saved

Go to the page [Serial groups status](#)

#	Group name	SIP profile	Phone	The group	Action
1	111	SIP profile 0	111	FXS2, FXS5, FXS0	↗ / ↘

[Add a new group](#)

Edit settings of group "111"

Enable group	<input checked="" type="checkbox"/>		
Group name	<input type="text" value="111"/>		
SIP profile	<input type="text" value="SIP profile 0"/>		
Phone	<input type="text" value="111"/>		
User Name	<input type="text" value="1"/>		
Password	<input type="password" value="*****"/>		
Call queue size	<input type="text" value="5"/>		
Call reply timeout, sec	<input type="text" value="16"/>		
SIP Port of group	<input type="text" value="5060"/>		
Group call pickup enable	<input checked="" type="checkbox"/>		

Added	Available
FXS2	FXS1
FXS5	FXS3
FXS0	FXS4
	FXS6
	FXS7

Phone:
Phone number assigned to this serial group.

Call queue size:
The maximum number of unanswered calls the serial group can accept.

Call reply timeout:
The incoming group call is cleared if it is not answered during this timeout.

SIP Port of group:
Alternative SIP-port of the serial group.

Ports:
In order to add the FXS port to the serial group you must move it from the "Available" list to the "Added" list. The order of ports in the "Added" list also matters. The first port in the list will be called first

To add group click the 'Add a new group' button. After 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 doesn't have free ports.
- *Call reply timeout, sec* – if group call is not answered, it will be dropped after timeout expiration (calling subscriber is received 'busy' signal);
- *SIP Port of group* – alternative SIP port of serial group (the default value is 5060);

- *Group call pickup enable* – when checked, incoming call of the serial group may be picked up by other subscribers from the same pickup group (with the same 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 free port search 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’ button. To cancel adding a new group, click ‘Cancel’ button.

To edit record in ‘Action’ column of ‘Serial groups’ table, click button. To delete record, click button.

To store settings into non-volatile memory, click ‘Apply’ button.



The changes will be applied immediately after pressing ‘Apply’ button. Reboot is not required.

3.1.4.8 ‘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#**

Subscriber service control			
	Supplementary services activation codes	Supplementary services deactivation codes	Supplementary services codes:
Unconditional forward	*21#	#21#	To activate any service you must enter *service_code#. To deactivate any service enter #service_code#. CFU, CFNR, CFB and Hotline service require the phone number to be entered. To do this enter *service_code*phone_number#.
CT busy	*22#	#22#	
CT noanswer	*23#	#23#	
Permit to pickup incoming calls	*24#	#24#	
Hotline	*25#	#25#	
Callwaiting	*26#	#26#	
DND	*27#	#27#	
<input type="button" value="Save Changes"/>			

After entering an activation code or canceling a service, the subscriber will hear ‘Confirmation’ signal (tree short signals) that means successful service activation or cancelation.

After entering a check code of the subscriber service, the subscriber can hear ‘Station response’ signal (long signal) or ‘Busy’ signal (short signals). ‘Station response’ signal means that service is enabled and activated, ‘Busy’ – service is disabled.

To save changes into operative memory, click ‘Save changes’ button. To store settings into non-volatile memory, click ‘Apply’ button.



In this submenu, changes are applied immediately after pressing the ‘Apply’ button. Reboot is not required.

3.1.4.9 'Cadence' submenu

Use this submenu to configure alternative call control signal (cadence) in accordance with caller number or 'Alert-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 map a specific cadence to the 'Alert-Info' header of incoming 'Invite' message, you should select 'Use Alert-Info header' checkbox in the respective SIP profile (see section 3.1.4.1.2 SIP profiles) and specify signal name (for example, Example-cadence) in the 'Signal name' field. Cadence will be transmitted to the line if 'Alert-Info' header of incoming 'Invite' message has <http://127.0.0.1/Example-cadence> value.

If cadence is not found by 'Alert-Info' header, attempt to find the cadence by the caller number will be taken. If cadence is not found by calling subscriber number, "1000, 4000" standard call with cadence will be sent.

You can configure only 20 various signals.

Cadence

	Enable	Cadence name	Cadence	Calling number
1.	<input type="checkbox"/>	Bellcore-dr1	1000,4000	
2.	<input type="checkbox"/>	Bellcore-dr2	1000,3000	
3.	<input type="checkbox"/>	Bellcore-dr3	1000,2000	
4.	<input type="checkbox"/>	Bellcore-dr4	1000,1000	
5.	<input type="checkbox"/>	Bellcore-dr5	700,700,700,3000	
6.	<input type="checkbox"/>	cadence5	1000,4000	
7.	<input type="checkbox"/>	cadence6	1000,4000	
8.	<input type="checkbox"/>	cadence7	1000,4000	
9.	<input type="checkbox"/>	cadence8	1000,4000	
10.	<input type="checkbox"/>	cadence9	1000,4000	
11.	<input type="checkbox"/>	cadence10	1000,4000	
12.	<input type="checkbox"/>	cadence11	1000,4000	
13.	<input type="checkbox"/>	cadence12	1000,4000	
14.	<input type="checkbox"/>	cadence13	1000,4000	
15.	<input type="checkbox"/>	cadence14	1000,4000	
16.	<input type="checkbox"/>	cadence15	1000,4000	
17.	<input type="checkbox"/>	cadence16	1000,4000	
18.	<input type="checkbox"/>	cadence17	1000,4000	
19.	<input type="checkbox"/>	cadence18	1000,4000	
20.	<input type="checkbox"/>	cadence19	1000,4000	

Cadence
In this page you may configure the unique cadence for any calling subscribers or Alert-Info headers.

- *Enable* – when checked, call transmission is enabled.
- *Cadence name* – text signal description received from 'Alert-Info' header of 'INVITE' message;
- *Cadence* – duration of call voltage application to the phone unit and, after comma/semicolon, duration of pause between call signals. Both values should be divisible by 100 ms (minimum value is 200 ms, maximum is 8000 ms);
- *Calling number* – number of caller party for which distinctive signal of call transmission is adjusted;

To save changes into operative memory click 'Save changes' button. To store settings into non-volatile memory, click 'Apply' button.



In this submenu, changes are applied immediately after pressing the 'Apply' button. Reboot is not required.

3.1.4.10 'Call History' submenu

For detailed description of parameter monitoring, see section 4.2.9.

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 into the device operative memory, click '*Save changes*' button. To store settings into non-volatile memory, click 'Apply' button.



In this submenu, changes are applied immediately after pressing the 'Apply' button. Reboot is not required.

3.1.5 'Security' menu

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

3.1.5.1 'General' submenu

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

Firewall General Configuration

Security Level:

No Security

Inbound Security

Outbound Security

High Security

Security Level:
Security Level changes are applied immediately after clicking "Apply changes"

No Security:
INBOUND traffic (WAN to LAN) is allowed.
OUTBOUND traffic (LAN to WAN) is allowed.

Inbound Security:
INBOUND traffic (WAN to LAN) is blocked.
OUTBOUND traffic (LAN to WAN) is allowed.

Outbound Security:
INBOUND traffic (WAN to LAN) is allowed.
OUTBOUND traffic (LAN to WAN) is blocked.

High Security:
INBOUND traffic (WAN to LAN) is blocked.
OUTBOUND traffic (LAN to WAN) is blocked.

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 into the device operative memory, click *'Save changes'* button. To record settings into the non-volatile memory, click *'Apply'* button.



Changes in the submenu will be applied immediately after pressing *'Apply'* button. Reboot is not required.

3.1.5.2 'Firewall Rules' submenu

Use the submenu to set transit traffic rules.

Firewall Rules: Settings saved

#	Name	Type of traffic	Source addresses	Destination addresses	Protocol	Type of message (ICMP)	Source ports	Destination ports	Target	Action
1	web_inport	INPUT			TCP				ACCEPT	<input type="checkbox"/> <input type="checkbox"/>
2	rule_transport	FORWARD	12.12.12.12	13.13.13.13	ICMP	fragmentation-needed			DROP	<input type="checkbox"/> <input type="checkbox"/>

New rule

Name:

Type of traffic:

Starting source IP address:

Number of source IP addresses:

Protocol:

Starting source port:

Number of source ports:

Starting destination port:

Number of destination ports:

Target:

Type of traffic:
This option determines type of traffic the rule will be applied to: input, output or forward.

Starting source IP address:
This option defines the starting source IP address. You can specify the subnet mask after symbol "/", for example 192.168.16.0/24. The "Number of source IP addresses" option is not used when subnet mask is specified.

Protocol:
This option determines the protocol of IP packet the rule will be applied to.

Target:
This option defines whether you want to drop or accept the packet.

Description of 'Firewall rules' table.

Firewall rule configuration:

To add new rule, click 'Add' button and fill in 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 selected, the following fields will be available for editing:
 - *Starting source IP address* – specify start IP address of source. You may assign subnet mask after '/' symbol (for example 192.168.16.0/24) to extract all the address range. When 'Address number of source' parameter is not taken into;
 - *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 checked, the following fields will be available to edit:
 - *Starting destination IP address* – specify destination IP address. After '/' 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* – use this field to assign address range of receiver if receiver mask is not specified;



- *FORWARD* – transit traffic. When checked, the following fields will be available for editing:
 - *Starting source IP address* – assign 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* – field is used to assign address range of the transmitter if the subnet 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);
 - *Action* – take action under 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 protocol is selected, the following settings will be 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 non-volatile memory, click '*Apply*' button.



Changes in the submenu will be applied immediately after pressing '*Apply*' button. Reboot is not required.

3.7.1.3 MAC filter submenu

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

MAC filter

Filter mode Disabled ▾

#	MAC	Action
1	11:12:13:14:15:16	⊗

Filter mode:
 You can restrict the access to the device according to the MAC address of a host. There are three possible MAC filter modes:
Disabled means that no restriction rules are set, the access is permitted for all the hosts;
Black list means that the access is forbidden for the hosts whose MAC addresses are listed in the MAC address list table;
White list means that the access is permitted for the hosts whose MAC addresses are listed in the MAC address list table. Access is forbidden for hosts not listed in the table.

- *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 non-volatile memory, click 'Apply' button.



Changes in the submenu will be applied immediately after pressing 'Apply' button. Reboot is not required.

4 DEVICE MONITORING VIA WEB INTERFACE. ADMINISTRATOR ACCESS

4.1 'Info' menu

4.1.1 'System' submenu

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

System Information	
Time & Date:	
System time	<input type="text" value="04:11:30"/>
Date	01-01-1970
Software:	
Kernel version	#39 Wed Jun 22 14:29:16 NOVT 2016
Firmware version	#2.1.0.132-ru
Device information:	
Factory type	TAU-8.IP-W
Factory SN	VI09000259
Factory MAC	A8:F9:4B:03:A4:6C

- *Time & Date* – system time and date:
 - *System time* – time in the format hh:mm:ss;
 - *Date* – data in format dd:mm:yy;
- *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.

4.1.2 'USB' submenu

The submenu displays information about connected USB device.

USB Devices					
All connected devices (excluding system hubs)					
Bus	Device	Product	Manufacturer	VendorID:ProdID	USB version
01	2	HP LaserJet P2015 Series	Hewlett-Packard	03f0:3817	2.00

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



By default, user name : *user*
password: *user*

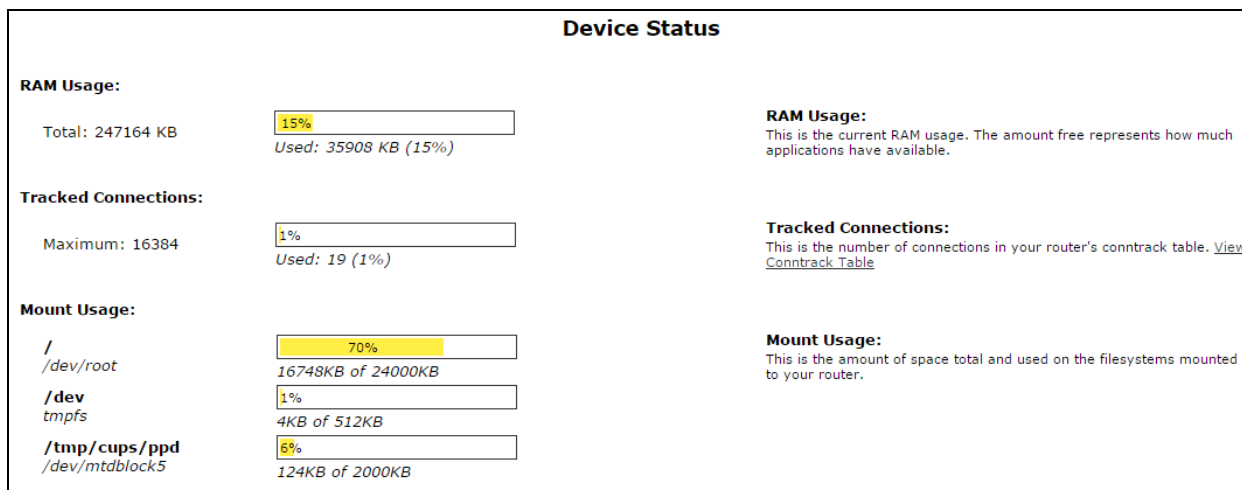
Click 'Dismount' button before disconnecting a USB device.

4.2 'Status' menu

Use the menu to monitor all the device systems.

4.2.1 'System' subsystem

Use the submenu to display RAM usage (connection number in 'contrack' 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 'contrack' table of router, in percents of maximum;
- *Filespace (Mount Usage)* – common filesystem size and disk space usage of the device installed system, in percents of maximum disk space.

4.2.2 'Processes' submenu

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

Running Processes

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/fbtpn
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.

4.2.3 '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.

4.2.4 'WLAN¹' submenu

WLAN				
WLAN:				
Status	Off	WLAN: WLAN LAN		
WiFi clients:				
Client	SSID	IP address	Connected at	Signal

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:

¹ Configuring the submenu is available only for TAU-8.IP-W

- *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.

4.2.5 '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:*              LISTEN
udp    0      0  0.0.0.0:631           0.0.0.0:*              LISTEN
udp    0      0  192.168.18.35:5060    0.0.0.0:*              LISTEN
udp    0      0  :::53                 :::*                    LISTEN
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

```


4.2.6 '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

4.2.7 'Diagnostic' submenu

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

Diagnostics

Network Utilities:

Network Utilities:

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

4.2.8 'Telephony' submenu

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

VoIP monitoring								
FXS status (FXS ports settings)								
Port number	Local number	Port state	Remote number	Registration	Registrar address	Line test		
0	001	hangup		not registered		<input type="button" value="Test"/>		
1	002	hangup		not registered		<input type="button" value="Test"/>		
2	003	hangup		not registered		<input type="button" value="Test"/>		
3	004	hangup		not registered		<input type="button" value="Test"/>		
4	005	hangup		not registered		<input type="button" value="Test"/>		
5	006	hangup		not registered		<input type="button" value="Test"/>		
6	007	hangup		not registered		<input type="button" value="Test"/>		
7	008	hangup		not registered		<input type="button" value="Test"/>		
Hunt groups status (hunt groups settings)								
Group name	Phone	Ports in group	Registration	Registrar address				
Serial groups status (serial groups settings)								
Group name	Phone	Ports in group	Registration	Registrar address				
IMS monitoring								
Port number	IMS management	Three-party conference	Call hold	Call waiting	Hotline	Hotline number	Hotline timeout, sec	Call transfer
0	Off	-	-	-	-	-	-	-
1	Off	-	-	-	-	-	-	-
2	Off	-	-	-	-	-	-	-
3	Off	-	-	-	-	-	-	-
4	Off	-	-	-	-	-	-	-
5	Off	-	-	-	-	-	-	-
6	Off	-	-	-	-	-	-	-
7	Off	-	-	-	-	-	-	-

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 see section 3.1.4.3).

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

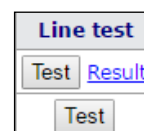
The list of possible state:

- *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 outgoing 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.

Test of ports

‘**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 ‘**Result**’ button to view test results which contains the following information:



Result of test: Port 0	
Date of test: 01.01.1970, 1:40:03	
Foreign DC voltage A (TIP)	0.086812 V
Foreign DC voltage B (RING)	0.097122 V
Line supply voltage	-53.627094 V
Resistance A (TIP) - B (RING)	495.165070 kΩ
Resistance A (TIP) - Ground	360.010132 kΩ
Resistance B (RING) - Ground	376.831970 kΩ
Capacity A (TIP) - B (RING)	< 50 nF
Capacity A (TIP) - Ground	< 50 nF
Capacity B (RING) - Ground	< 50 nF

- *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*.

Hunt groups status – this table displays registration status of configured hunt groups. Click ‘**Hunt groups settings**’ to switch to the ‘**PBX/Hunt groups**’ section of hunt group settings (see **3.1.4.4**).

- *Group name* – group identifier name;
- *Phone* – phone number assigned to the group;
- *Ports in group* – list of the device port included in the hunt group;
- *Registration* – registration status of group phone number on SIP server (if a phone number is registered you will see registration time otherwise you will see the record ‘*Not registered*’).

Serial groups status – shows registration status of configured serial groups. Click ‘**Serial groups settings**’ button to forward to the ‘**PBX/Serial groups**’ configuration section (see section **3.1.4.7** 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* – registration status of group phone number on SIP server (if a phone number is registered you will see registration time otherwise you will see the record ‘*Not registered*’).

IMS monitoring

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

4.2.9 'Call History' submenu

The device RAM may store up to 20 000 records for performed calls. If the record number exceeds 20 000, the oldest records (at the top of the table) will be removed, and new ones will be added at the end of the file. Log statistics will not be collected, when the history size is zero.

Click '*Change call history settings*' to switch to the '*PBX/Call History*' section of subscriber port settings (For detailed parameter configuration description, see Section **3.1.4.10**).



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

Call history saving

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

Call history view

Click '*View call history*' 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

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 – Intermediate state and reason of call that are clearing output into statistic

Intermediate state	Description
Size	Inbound or outbound holding
Talking	Talking subscriber
Holding	TAU subscriber held on the remote subscriber
Held	TAU subscriber is held on by remote subscriber
Call termination reasons	Description
Local	TAU subscriber pick up the phone without a call and put the phone down
local busy	TAU subscriber is busy
remote busy	Remote subscriber is busy
invalid number	Wrong number
no answer	Subscriber does not answer
no local user	Inbound call to non-existent number
no remote user	Outbound call to non-existent number

no route	Call to inaccessible direction
local clear	Call release of TAU subscriber
remote clear	Call release of remote subscriber
local fail	Local or remote error arisen under establishing a connection. The error source may be: mismatch codecs, reboot, source luck (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" and 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" and etc.

Filter (show/hide)

FXS ports 0 1 2 3 4 5 6 7

Local number

Remote number

Remote host IP address

Start call time from: to:

Start talk time from: to:

Call state

Call type



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 'Apply filter' button. To translate all filter values back to initial state, click 'Cancel' button.

4.3 'Log' menu

Access to the 'Log' menu is performed on the administrator privileges.

4.3.1 'Syslog Settings' submenu

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

syslog Settings

Output trace to syslogd ▾

Remote log

Syslog server address

Syslog server port

Local log

Log file name

Log file size (kB)

VoIP

VoIP trace enable

Errors

Warnings

Debug

Info

SIP trace level

IGMP

IGMP trace enable

Output trace to:
Use this option to choose where the system log to put. If you choose "console", all the system events will be put to the command console which you can connect to using special COM-port adapter. If you choose "syslogd", the device will use the syslog protocol for system trace.

syslogd:
When choosing "syslogd" you can configure both remote (syslog server address and port) and local (name and size of the local file) log. Default value of syslog server port is 514. To disable remote log, leave the "Syslog server address" field empty. To disable local log, leave the "Log file name" field empty.

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!

To save changes into the operative memory, click ‘*Save changes*’ button. To store settings into non-volatile memory, click ‘*Apply*’ button.



Changes in this menu will be applied immediately after pressing ‘*Apply*’ button. Reboot is not required.

4.3.2 ‘Syslog’ submenu

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

Syslog View

Message Prefix:

```

Jan 1 00:02:35 TAU-8 syslog.info syslogd started: BusyBox v1.4.2
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.020[app:dbg]Reloading config...
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.060[app:dbg]Error: 0
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Error: 0
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'authentication' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: 1
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'enablesip' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: 1
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registration' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: 1
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'proxyip' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: 192.168.0.3
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registrariip' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: 192.168.0.3
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registration_rsrv1' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'proxyip_rsrv1' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registrariip_rsrv1' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registration_rsrv2' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'proxyip_rsrv2' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registrariip_rsrv2' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registration_rsrv3' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'proxyip_rsrv3' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registrariip_rsrv3' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registration_rsrv4' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'proxyip_rsrv4' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'registrariip_rsrv4' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'rsrv_keepalive_time' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'rsrv_check_method' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'rsrv_mode' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: off
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'outbound' in section 'sip'
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Founded value: 0
Jan 1 03:02:36 TAU-8 user.debug syslog: 03:02:36.080[app:dbg]Getting option 'dial timeout' in section 'sip'
    
```


4.3.3 'Kernel' submenu

Use the submenu to view circular kernel buffer.

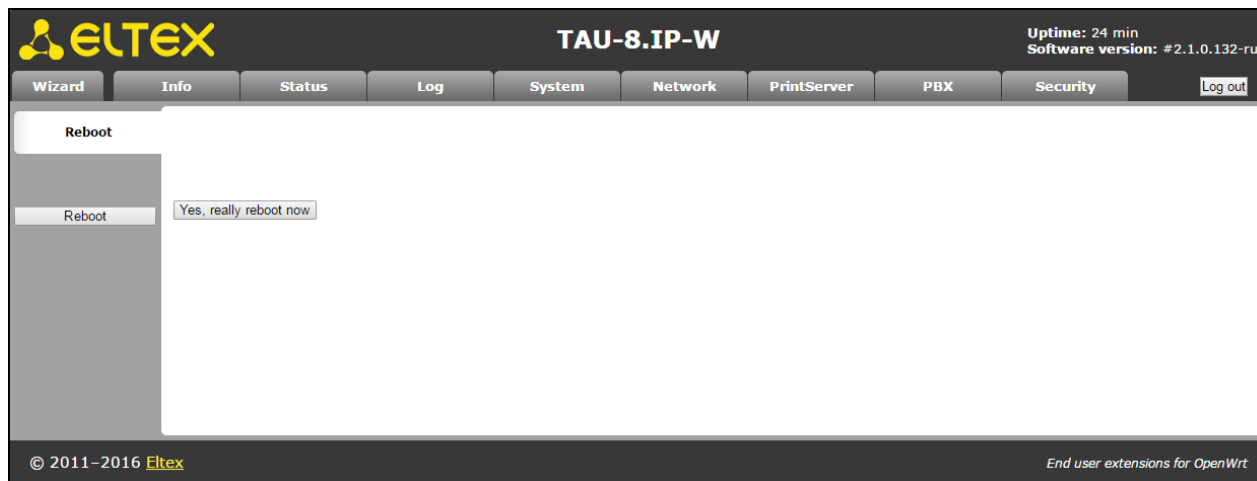
```

Kernel Ring Buffer

lab <bio-0> at 0
SCSI subsystem initialized
usbcore: registered new interface driver usbfs
usbcore: registered new interface driver hub
usbcore: registered new device driver usb
NET: Registered protocol family 2
IP route cache hash table entries: 2048 (order: 1, 8192 bytes)
TCP established hash table entries: 8192 (order: 4, 65536 bytes)
TCP bind hash table entries: 8192 (order: 3, 32768 bytes)
TCP: Hash tables configured (established 8192 bind 8192)
TCP reno registered
UDP hash table entries: 256 (order: 0, 4096 bytes)
UDP-Lite hash table entries: 256 (order: 0, 4096 bytes)
NET: Registered protocol family 1
RPC: Registered udp transport module.
RPC: Registered tcp transport module.
RPC: Registered tcp NFSv4.1 backchannel transport module.
PCI: CLS 32 bytes, default 32
SPI core: add adapter concerto-spi
arm1: Module loaded.
Registering mini_fo version $Id: 209-mini_fo.patch,v 1.1.2.1 2010/06/21 09:34:58 satananda.burla Exp $
Slow work thread pool: Starting up
Slow work thread pool: Ready
JFFS2 version 2.2 (NAND) (ZLIB) (RTIME) (c) 2001-2006 Red Hat, Inc.
fuse init (API version 7.13)
msgmni has been set to 482
Block layer SCSI generic (bsg) driver version 0.4 loaded (major 254)
io scheduler noop registered (default)
Serial: 8250/16550 driver, 1 ports, IRQ sharing disabled
serial8250.0: ttyS0 at MMIO 0x10090000 (irq = 41) is a 16550A
console [ttyS0] enabled
loop: module loaded
nbd: registered device at major 43
    
```

4.4 Reboot of the device. '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.



5 ADDED SERVICE USAGE

5.1 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.

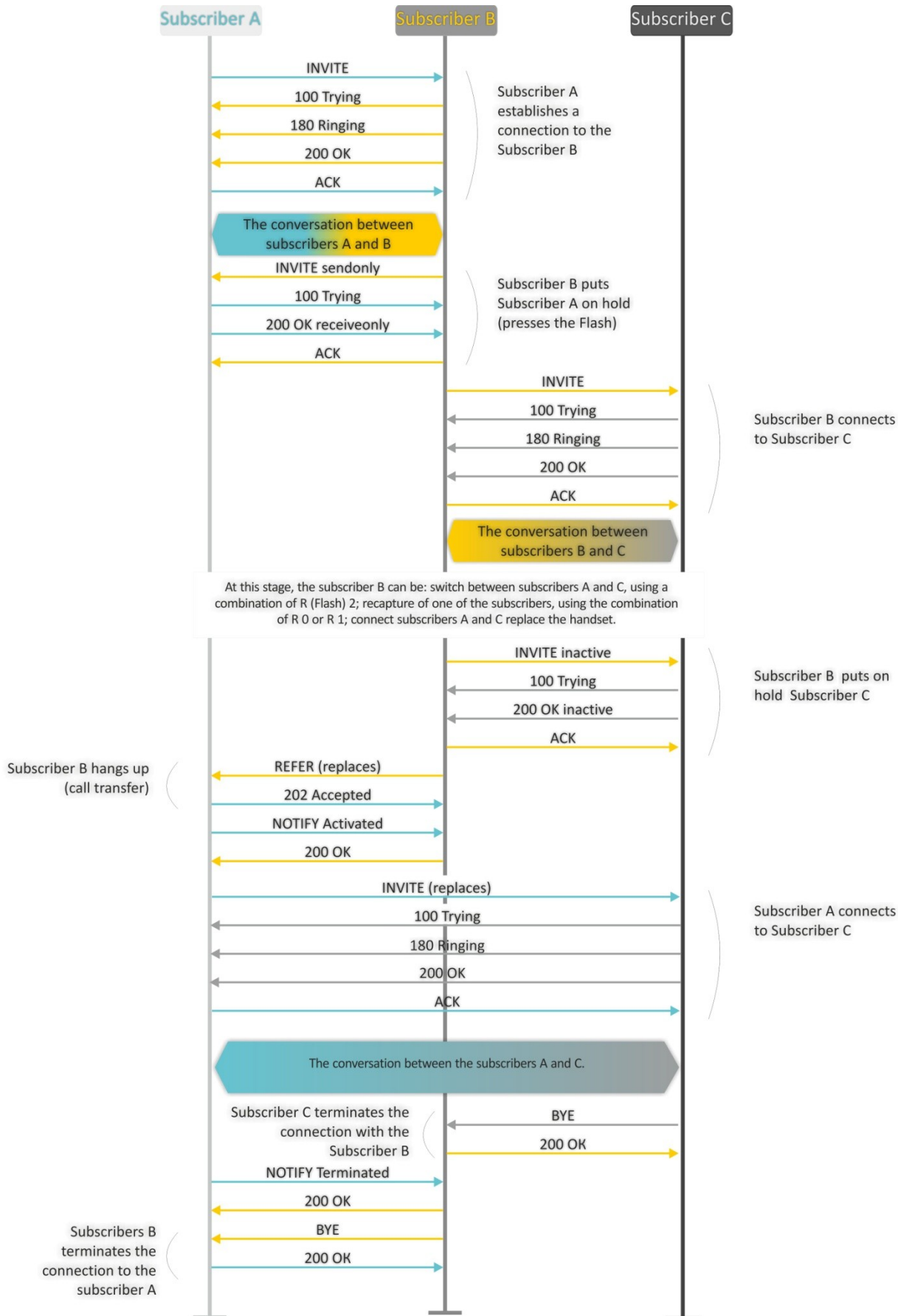
'Attended calltransfer' service allows you to temporarily disconnect an online subscriber (Subscriber A), establish connection with another subscriber (Subscriber C) and return to the previous connection without dialling or transfer the call while disconnecting Subscriber B.

'Attended calltransfer' service usage:

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

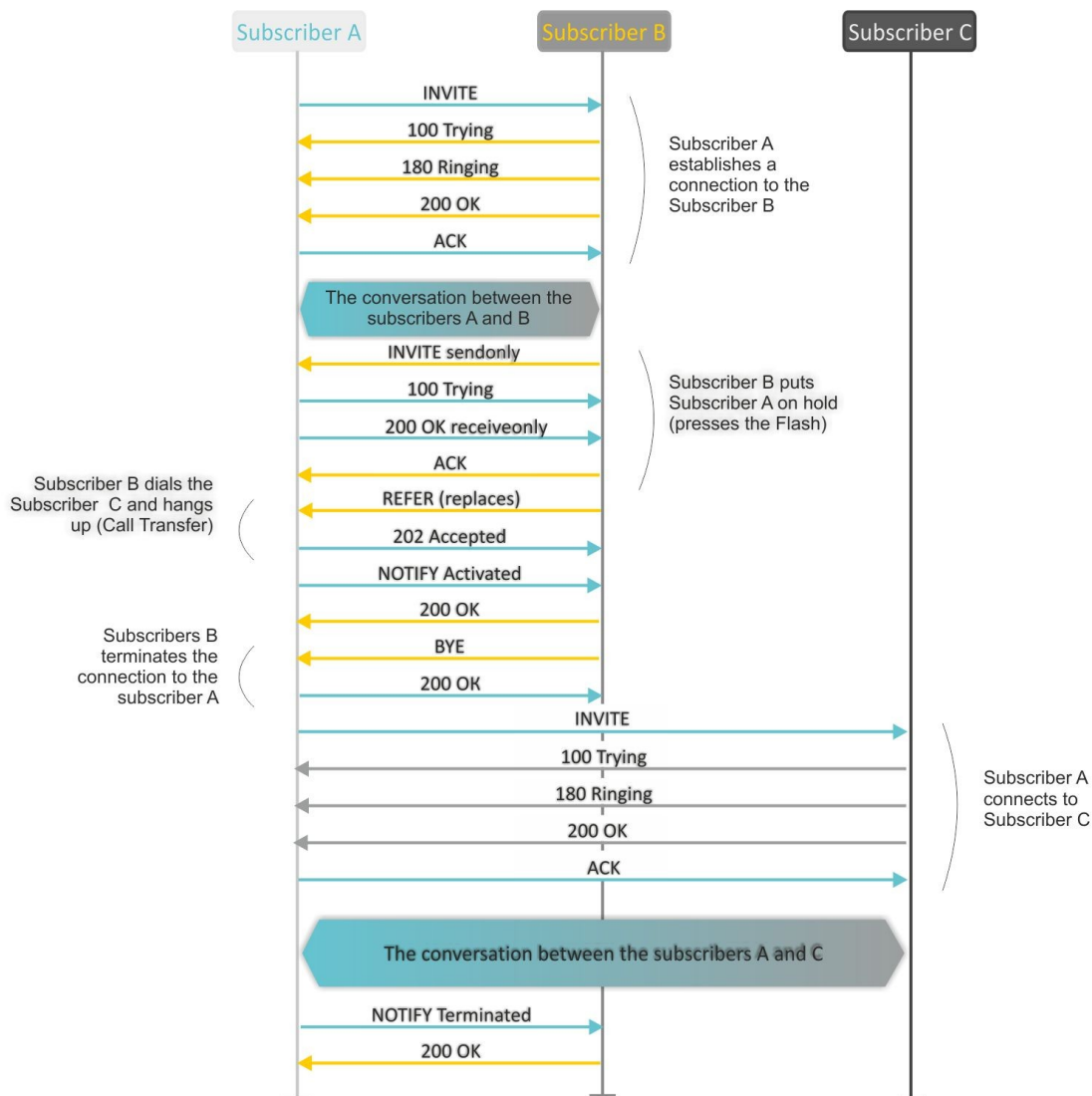
- R 0 – disconnect a subscriber on hold, connect to online subscriber;
- R 1 – disconnect an online subscriber, connect to subscriber on hold;
- R 2 – switch to another subscriber (change a subscriber);
- R 3 – 3-Way Call;
- R clearback – call transfer; voice connection will be established between Subscribers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

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



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

Figure below shows 'Unattended calltransfer' service operation algorithm:



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

5.2 Call Waiting

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

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

Access to this service is established via subscriber line settings menu by selecting 'Attended calltransfer', 'Unattended calltransfer' or 'Local calltransfer' in the '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).

5.3 Three-way conference call

Three-way conference is a service that enables simultaneous phone communication for 3 subscribers. For detailed three-way conference mode information see Section **5.1 Call transfer**.

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

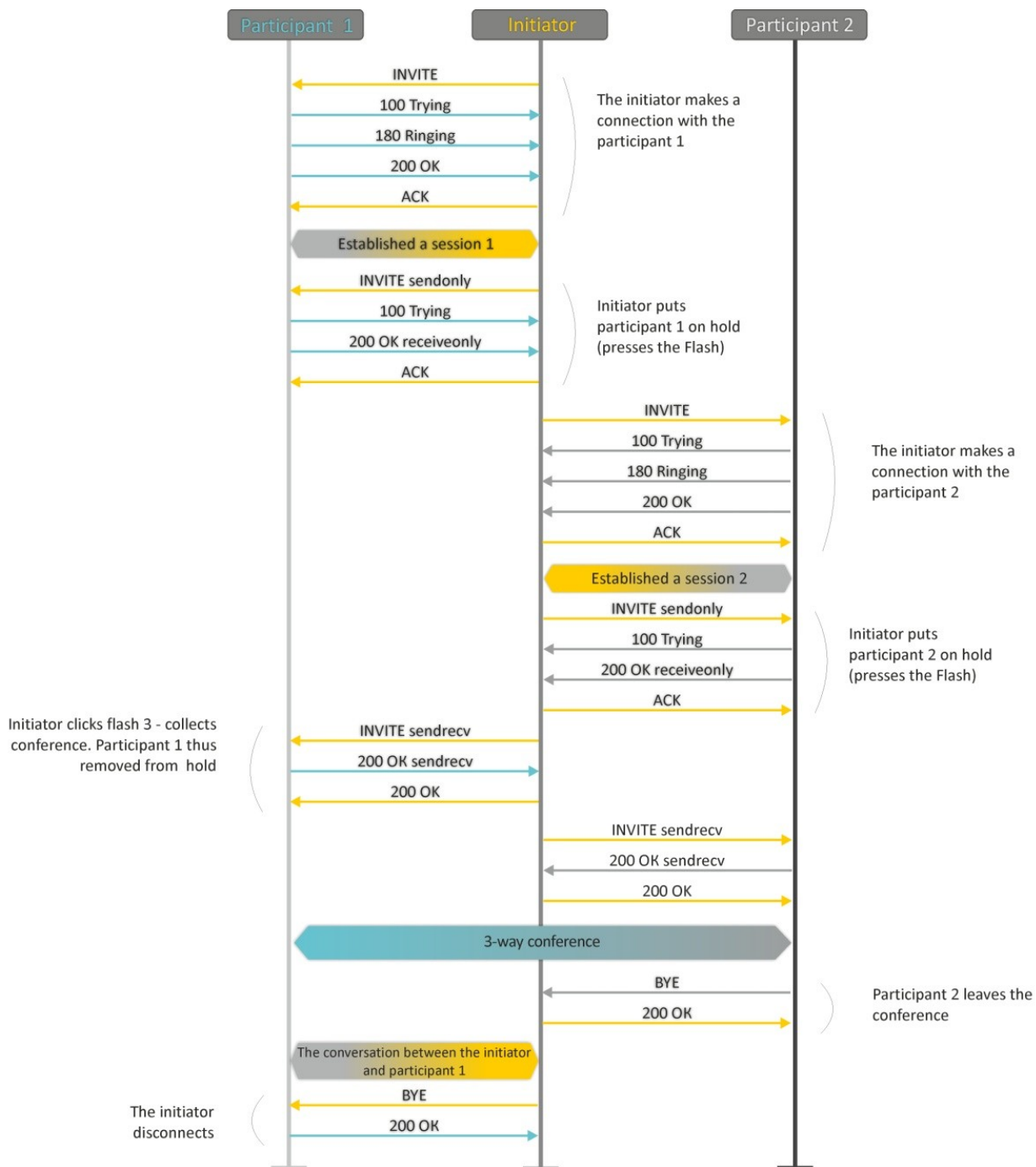
There are two operation modes for a three-way conference: local mode and remote mode. In the first mode, the conference is assembled locally by the initiating subscriber; in the second mode, the conference is established remotely by a remote server, also known as the conference server.

5.3.1 Local conference

In conference mode, pressing 'flash' is ignored by initiator. Messages of signaling protocol, received from the participants and intended to put the initiator side in hold mode, force this participant to leave the conference. At that, the initiator and the second participant will switch to the ordinary two-party call mode.

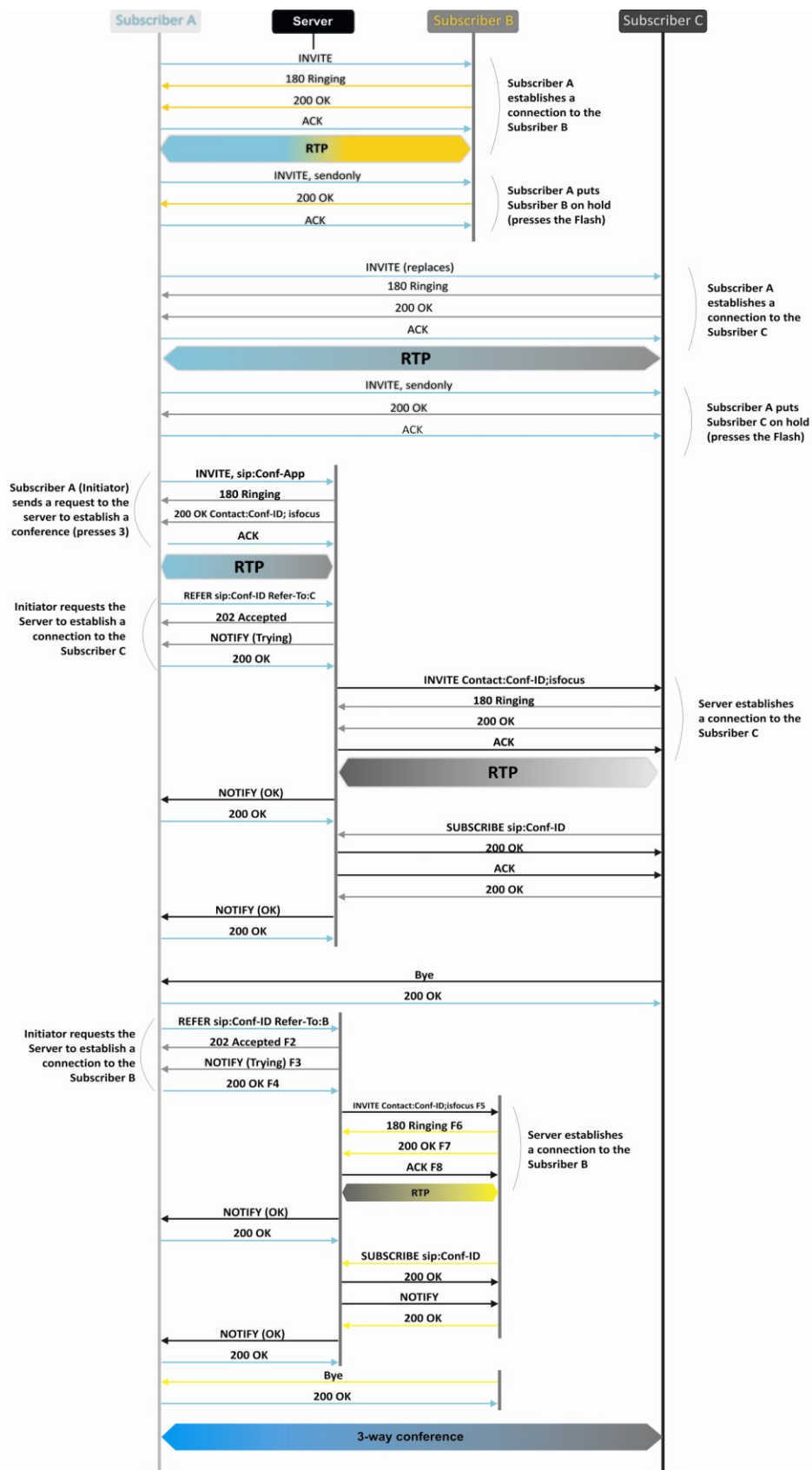
The conference terminates, when initiator leaves; in this case, both participants will receive clearback message. If one of the participants leaves the conference, the initiator and the second participant will switch to a standard two party call. Flash is processed as described in Sections 5.1 Call transfer and 5.2 Call Waiting.

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



5.3.2 Remote conference

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



6 AUTOPROVISIONING PROCEDURE OPERATION ALGORITHM VIA DHCP

If the packet exchange is performed through 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 started by using the received information. If DHCP option is not detected the device searches Option 66 (TFTP server) and 67 (Boot file name). If the searching is successful, firmware and configuration files will be loaded from specified server.

Format of option 43 (Vendor-Specific Info):

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

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

Autoconfiguration procedure algorithm:

1. DHCP exchange initialization

Device initializes DHCP exchange after the startup.

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 suboption 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 and 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. When the firmware image is written into the device flash memory, the Power indicator will flash green, orange and red in succession.



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 ***option 'pppoe_psw_encrypted' 'encrypted password'***
option 'pptp_password_encrypted' 'encrypted password''
to
option 'pppoe_psw' 'password'
option 'pptp_password' 'password'' in the *'/etc/config/network'* file.



Do not power off or reboot the device, when the firmware image is written into the flash memory. These actions will interrupt the firmware update, that will lead to the device boot partition corruption. The device will become inoperable. You may restore the device operation only trough RS-232 by using a special COM port adapter for connection to computer.

APPENDIX 1. VOICE MENU USAGE FOR GATEWAY SETTINGS

Voice menu allows you to get information about current IP address or assign temporary address 192.168.1.2, that will be used before the gateway reboot.

Voice menu includes two options:

- When you dial of ‘***’ 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 ‘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 setting a new IP address for eth0 interface VoIP application will be rebooted and all the current VoIP connections will be broken.

APPENDIX 2. USAGE OF WIZARD MENU

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

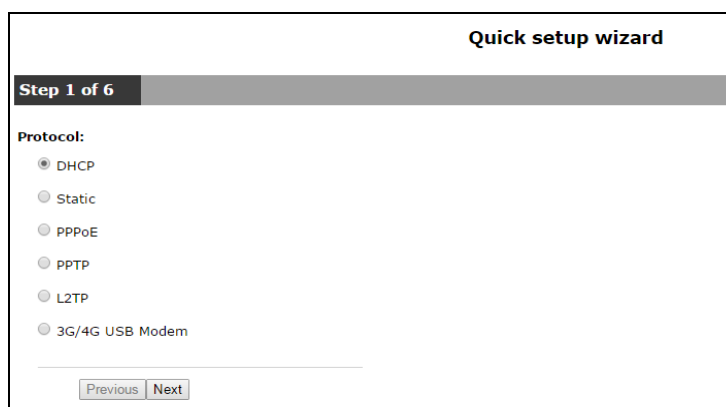
The system automatically directs a user to the 'Wizard' menu at the first run.

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.

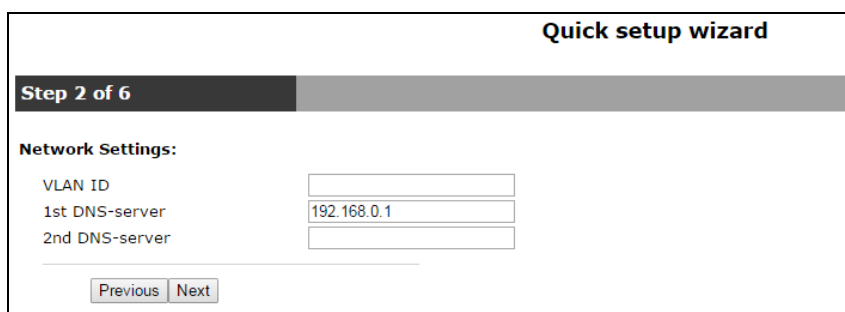
Step 1. Protocol

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.

Quick setup wizard

Step 3 of 6

VoIP:

Proxy address (:port)

Registrar address (:port)

FXS port	Phone	Username	Login	Password
FXS0 <input checked="" type="checkbox"/>	<input type="text" value="001"/>	<input type="text" value="001"/>	<input type="text" value="001"/>	<input type="checkbox"/> password is hidden
FXS1 <input checked="" type="checkbox"/>	<input type="text" value="002"/>	<input type="text" value="002"/>	<input type="text" value="002"/>	<input type="checkbox"/> password is hidden
FXS2 <input checked="" type="checkbox"/>	<input type="text" value="003"/>	<input type="text" value="003"/>	<input type="text" value="003"/>	<input type="checkbox"/> password is hidden
FXS3 <input checked="" type="checkbox"/>	<input type="text" value="004"/>	<input type="text" value="004"/>	<input type="text" value="004"/>	<input type="checkbox"/> password is hidden
FXS4 <input checked="" type="checkbox"/>	<input type="text" value="005"/>	<input type="text" value="005"/>	<input type="text" value="005"/>	<input type="checkbox"/> password is hidden
FXS5 <input checked="" type="checkbox"/>	<input type="text" value="006"/>	<input type="text" value="006"/>	<input type="text" value="006"/>	<input type="checkbox"/> password is hidden
FXS6 <input checked="" type="checkbox"/>	<input type="text" value="007"/>	<input type="text" value="007"/>	<input type="text" value="007"/>	<input type="checkbox"/> password is hidden
FXS7 <input checked="" type="checkbox"/>	<input type="text" value="008"/>	<input type="text" value="008"/>	<input type="text" value="008"/>	<input type="checkbox"/> password is hidden

Step 4. Wi-Fi settings¹

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

Quick setup wizard

Step 4 of 6

Wi-Fi Settings:

Enable Wi-Fi

Wi-Fi network name (SSID)

Secret phrase

Current Wi-Fi security mode is: "WEP". After applying wizard settings security mode will be: "use WPA and WPA2".

¹ Only for TAU-8.IP-W

Step 5. Access

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

Quick setup wizard

Step 5 of 6

Access:

Change admin's password

Administrator's password

Confirm password

Change user's password

User's password

Confirm password

Step 6. Time Settings

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

Quick setup wizard

Step 6 of 6

Time Settings:

Timezone ▼

NTP Server

ACCEPTANCE CERTIFICATE AND WARRANTY

TAU-8.IP _____ VoIP gateway with serial number _____ meets the requirements of technical specification TU 6650-068-33433783-2011 and is classified as fit for operation.

The manufacturer, Eltex Enterprise LLC, guarantees that the TAU-8.IP subscriber gateway meets the requirements of technical specification TU 6650-068-33433783-2011 provided its operation conditions correspond to the ones set forth in this Manual.

Transportation of equipment should correspond to condition 5 and storage of equipment should correspond to condition 1 in accordance with Russian government standard 15150.

The warranty period is 1 year. Production data is specified on the package.

The device does not contain precious materials.

Director

_____ A. N. Chernikov
signature full name

Head of the Quality Control Department

_____ S. I. Igonin.
signature full name

Vendor:
29v Okruzhnaya Street
Novosibirsk, 630020
E-mail: eltex@eltex.nsk.ru

Made in Russia

