

VoIP Gateway

TAU-8N.IP

User Manual
Firmware version 1.8.1

MGMT IP address: 192.168.1.1

Username: admin

Password: password

Contents

1	Introduction	6
2	Product Description	7
2.1	Purpose	7
2.2	Device Specification	7
2.3	Device Design and Operating Principle	8
2.4	Main Specifications	10
2.5	Design.....	12
2.5.1	Front Panel of the Device	12
2.5.2	Rear Panel of the Device	13
2.6	Light Indication	14
2.7	Reset to Factory Settings	15
2.8	Delivery Package.....	15
3	Device Management via Web Configurator.....	16
3.1	Getting Started	16
3.2	User Change	17
3.3	Web Interface Operation Modes	17
3.4	Applying and Discarding Changes Made to Configuration	18
3.4.1	Applying Configuration.....	18
3.4.2	Discarding Changes.....	19
3.5	Quick Configuration Menu.....	19
3.5.1	Internet	19
3.5.2	VoIP	21
3.5.3	System.....	22
3.6	Advanced Settings.....	22
3.6.1	Web Interface Basic Elements	22
3.6.2	"Network" Menu	24
3.6.2.1	"Internet" Submenu	24
3.6.2.2	"MAC Management" Submenu.....	33
3.6.2.3	"Firewall" Submenu	33
3.6.2.4	Configuration of firewall rules.....	34
3.6.2.5	"ACL" Submenu	35
3.6.2.6	Limitations on MAC Addresses	35
3.6.2.7	Time Limits on Schedule	35

3.6.2.8	"MAC Filter" Submenu	36
3.6.2.9	"Routes" Submenu	37
3.6.2.10	"SNMP" Submenu	38
3.6.2.11	"TACACS" Submenu.....	39
3.6.3	"VoIP" Menu.....	40
3.6.3.1	"Network Settings" Submenu	40
3.6.3.2	"QoS" Submenu	42
3.6.3.3	"Line Settings" Submenu	43
3.6.3.4	"SIP profiles" Submenu	48
3.6.3.5	"Dialplan Profiles" Submenu.....	64
3.6.3.6	" Hunt Groups" Submenu.....	67
3.6.3.7	"Pickup Groups" Submenu	69
3.6.3.8	"Supplementary Service Prefixes" Submenu.....	70
3.6.3.9	"Cadence" Submenu	71
3.6.3.10	"Call History" Submenu.....	72
3.6.4	"System" Menu	73
3.6.4.1	"Time" Submenu.....	73
3.6.4.2	"Access" Submenu.....	74
3.6.4.3	"Log" Submenu.....	76
3.6.4.4	"WEB Authentication" Submenu.....	78
3.6.4.5	"Configuration Management" Submenu	79
3.6.4.6	"Firmware Upgrade" Submenu	79
3.6.4.7	"Reboot" Submenu	80
3.6.4.8	The "Autoprovisioning" Submenu	81
3.6.4.9	"Certificates" Submenu.....	84
3.7	System Monitoring.....	88
3.7.1	"Internet" Menu.....	88
3.7.2	"VoIP" Menu.....	89
3.7.3	Ethernet ports menu	92
3.7.4	"ARP" Menu	94
3.7.5	"Device" Menu	94
3.7.6	"CPU" Menu	95
3.7.7	"Routes" Menu.....	96
3.7.8	"Call History" Menu	97
3.7.9	"Diagnostics" Menu.....	98

3.8	Example of device configuration	99
4	Supplementary Service Usage	101
4.1	Call Transfer	101
4.2	Call Waiting	104
4.3	Three-party Conference	105
4.3.1	Local Conference	105
4.3.2	Remote Conference	106
5	Connection Establishment Algorithms.....	107
5.1	Algorithm of a Successful Call via SIP Protocol	107
5.2	Call Algorithm Involving SIP Proxy Server	108
5.3	Call Algorithm Involving Forwarding Server	109
5.4	DHCP-based Autoprovisioning Algorithm	110
6	System recovery after a firmware update failure.....	114
7	APPENDIX A. CALCULATION OF PHONE LINE LENGTH.....	115
8	APPENDIX B. RUNNING USER-DEFINED SCRIPT UPON SYSTEM STARTUP	116
9	APPENDIX C. DHCP CLIENTS CONFIGURATION IN MULTISERVICE MODE.....	117
10	APPENDIX D. USING THE COMMAND LINE INTERFACE (CLI) FOR CONFIGURATION AND MONITORING.....	120


Document version	Issue date	Revisions
Version 5.0	05.11.2024	Fifth issue
Version 4.0	28.04.2023	Fourth issue
Version 3.0	30.09.2022	Third issue
Version 2.0	10.06.2022	Second issue
Version 1.0	18.12.2020	First issue
Firmware version	1.8.1	


NOTATIONAL CONVENTIONS

Symbol	Description
Bold font face	Notes, warnings, section headings, titles and table titles are written in bold.
<i>Calibri Italic</i>	Important information is written in Calibri Italic.

NOTES AND WARNINGS

 **Tips provide additional information on device operation and setup.**

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

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

1 Introduction

Today, VoIP is one of the most rapidly evolving telecommunication services. TAU-8N.IP series gateways (hereinafter the "device") are designed to provide VoIP services to the network clients.

TAU-8N.IP VoIP gateway allows connecting analogue phones to packet-based data networks accessible via Ethernet. The device is intended for operation in home or small offices (SMB).

This operation manual describes intended use, key specifications, configuration, monitoring, and firmware update for TAU-8N.IP VoIP gateways.

2 Product Description

2.1 Purpose

TAU-8N.IP is a high-performance VoIP gateway with the full set of features that allow users to take advantage of VoIP functionality. TAU-8N.IP gateway allows connecting an analogue phone or a fax modem to IP networks.

The devices 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 built in voltage and current protection for subscriber terminations.

2.2 Device Specification

Interfaces:

- FXS: 8 × RJ-11 ports;
- WAN: 1 × RJ-45 10/100BASE-T Ethernet port;
- MGMT: 1 × RJ-45 10/100BASE-T Ethernet port;
- USB: 1 × USB 2.0 port.

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

Functions:

- network functions:
 - PPPoE support (PAP/SPAP- and CHAP/MSCHAP-V2-authorization, PPPoE-compression);
 - L2TP support;
 - static address and DHCP support;
 - SNMP support;
 - network screen.
- VoIP protocols: SIP;
- echo cancellation (G.168 recommendations);
- voice activity detection (VAD);
- comfort noise generation;
- DTMF signals detection and generation;
- DTMF transmission (INBAND, rfc2833, SIP INFO);
- fax transmission:
 - G.711A/G.711U;
 - T.38.
- modem transmission;
- operation w/ and w/o a SIP server;
- Supplementary Services:
 - Call Hold;
 - Call Transfer;
 - Call Waiting;
 - Call Forward at Busy;
 - Call Forward at No Answer;
 - Call Forward Unconditional;
 - DND (Do Not Disturb);
 - Caller ID: FSK, DTMF;
 - Hotline;
 - Group call;

- Call Pickup;
- Three-party Conference;
- Flexible dialplan.
- firmware update via web interface;
- DHCP-based auto provisioning support;
- remote monitoring, configuration and setup: web interface, Telnet, SSH, TR-069.

Figure 1 shows TAU-8N.IP connection diagram.

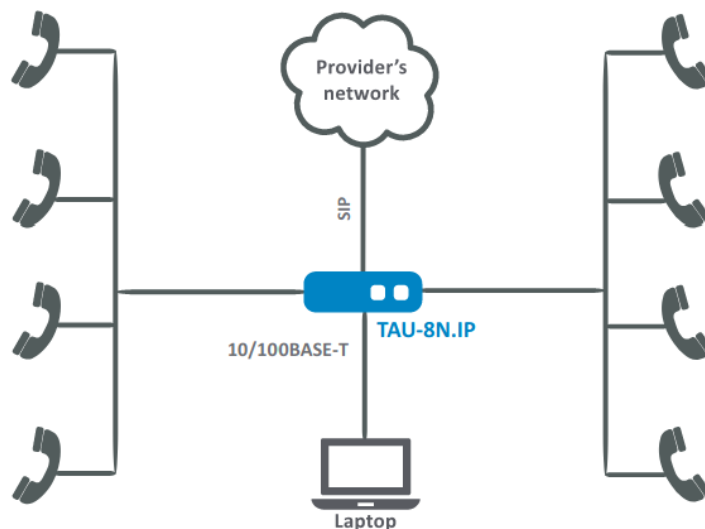


Figure 1 – TAU-8N.IP connection diagram

2.3 Device Design and Operating Principle

TAU-8N.IP terminal consists of the following subsystems:

- controller that includes:
 - processor, including a 100 Mbps switch with a built-in PHY, USB 2.0 ports, PCI-E controllers, 8 PCM channels for VoIP applications;
 - flash memory – 512 MB;
 - SDRAM RAM – 512 MB.
- 8 × subscriber units;
- Ethernet module MGMT: RJ-45 10/100BASE-T;
- Ethernet WAN module: RJ-45 10/100BASE-T;
- USB Host port.

Block diagram of the device is shown in [Figure 2](#).

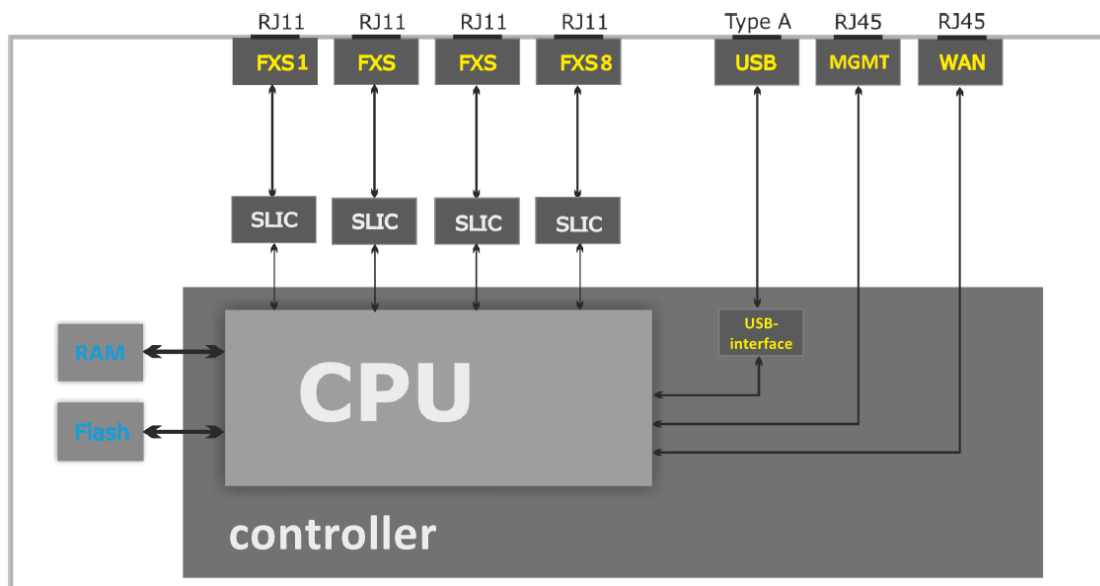


Figure 2 – TAU-8N.IP block diagram

The device is running the Linux operating system. Basic control functions are performed by a processor which enables IP packet routing, VoIP operation, etc.

Functionally the device may be divided into 3 blocks:

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

Device network features block enables IP packet passing according to the device routing table. Depending on the network interface configuration, this block can process both tagged and untagged packets. Supports DHCP, PPPoE, L2TP protocols.

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

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

Figure 3 shows TAU-8N.IP functional diagram.

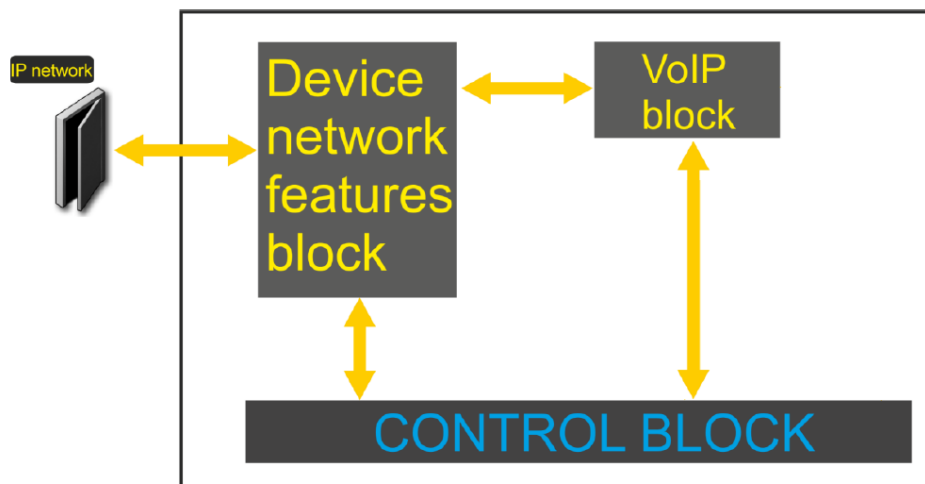


Figure 3 – TAU-8N.IP functional diagram

2.4 Main Specifications

The table shows main device specifications.

Table 1 – Main specifications

VoIP protocols	
Supported protocols	SIP
Voice codecs	
Codecs	G.729, annex A, annex B, G.711a, G.711u, G.723.1, G.726-16, G.726-24, G.726-32, G.726-40, AAL2-G.726-16, AAL2-G.726-24, AAL2-G.726-32, AAL2-G.726-40, modem transmission: G.711a, G.711u, fax transmission: G.711 a, G.711u, T.38
Ethernet WAN interface specifications	
Number of ports	1
Electrical connector	RJ-45
Data rate	10/100 Mbps, autodetection
Supported standards	BASE-T

Ethernet MGMT interface specifications	
Number of interfaces	1
Electrical connector	RJ-45
Data rate	10/100 Mbps, autodetection
Supported standards	BASE-T
Analogue user port specifications	
Number of ports	8
Loop resistance (phone resistance included)	up to 1800 Ω
Dialing reception	pulse/frequency (DTMF)
Caller ID broadcasting	FSK BELL 202/FSK V.23/DTMF
Control	
Remote control	web interface, Telnet, SSH, TR-069
Access restriction	by password and by IP address
General parameters	
Power supply	power adapter 12 B DC, 2.0 A
Power consumption	up to 19 W (max. current consumption is 1.58 A)
Operating temperature	from +0 to +40 °C
Relative humidity at 25 °C	up to 80 %
Dimensions (W × H × D)	208 × 38 × 115 mm
Weight	0.3 kg
Service life	no less than 5 years

2.5 Design

TAU-8N.IP subscriber gateway is enclosed into 208 × 38 × 115 mm plastic housing.

2.5.1 Front Panel of the Device

The TAU-8N.IP front panel is shown in [Figure 4](#).

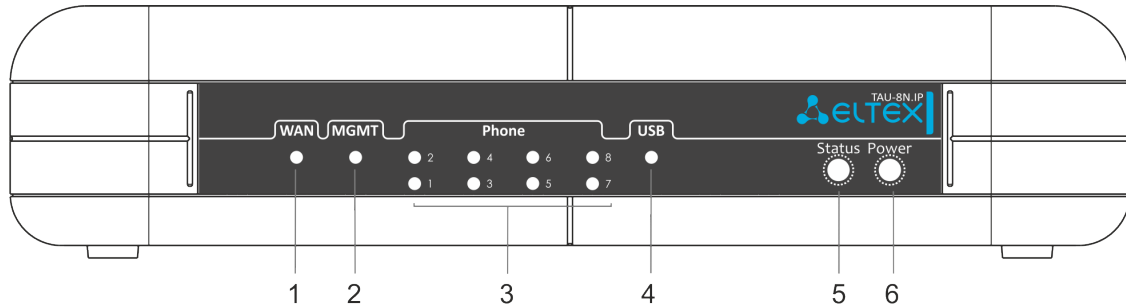


Figure 4 – TAU-8N.IP front panel appearance

Table 2 – Description of the front panel indicators and controls

Front panel element		Description
1	WAN	WAN interface indicator
2	MGMT	MGMT interface indicator
3	Phone	analogue phone indicator
4	USB	external USB device operation indicator (USB flash, external HDD)
5	Status	device operation status indicator
6	Power	device power and activity status indicator

2.5.2 Rear Panel of the Device

The TAU-8N.IP rear panel appearance is shown in [Figure 5](#).

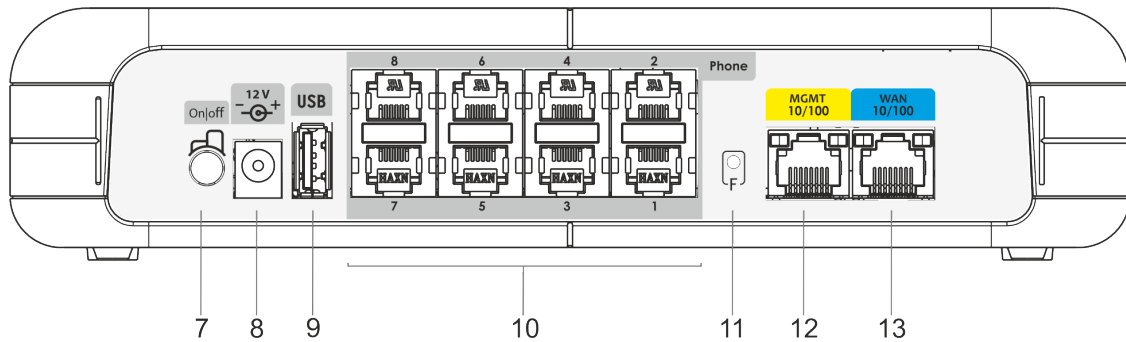


Figure 5 – TAU-8N.IP rear panel appearance

Table 3 – Description of the rear panel indicators and controls

Rear panel element		Description
7	ON/OFF	ON/OFF switch
8	12V	Power adapter connector
9	USB	USB port for external USB device connection (USB flash, HDD)
10	Phone	8 × RJ-11 ports for analogue phone connection
11	F	A functional key that reboots the device and resets it to factory settings
12	MGMT	10/100BASE-T Ethernet (RJ-45) port for device network management
13	WAN	10/100BASE-T (RJ-45) port for external network connection

2.6 Light Indication

WAN, MGMT, Phone, USB, Power, Status indicators located on TAU-8N.IP front panel show the device current status. The list of possible states of the LEDs is shown in the table below.

Table 4 – Light indication of TAU-8N.IP states

Indicator	Indicator state	Device status
WAN	solid (green – 10 Mbps, orange – 100 Mbps)	connection between station terminal and subscriber device is established
	flashes	packet data transmission via WAN interface
MGMT	solid (green – 10 Mbps, orange – 100 Mbps)	connection to the network device is established
	flashes	packet data transmission via MGMT interface
Phone	green, solid	phone is off-hook (line is active)
	off	phone is on-hook, normal operation
	green, flashes at 20 Hz frequency for a second, then 4 seconds pause	incoming call is on the phone port
	green, flashes slowly in period	subscriber port is not registered at SIP proxy server
	green, double short flashes in 3 seconds intervals	line test is in progress
USB	green, solid	USB device is connected
	off	USB device is not connected
Status	red, solid	failed start attempts are over the limit
	green, solid	system loaded, the Internet is accessible
	red, continuous flashing at 10 Hz frequency	bootloader is missing
	green, flashes at 1 Hz frequency	system loaded, the Internet is not accessible
	green, red, intermittent flashing	reset to factory settings
	off	device power supply is off
Power	green, solid	device power supply is on, normal operation
	red, solid	device starts up

2.7 Reset to Factory Settings

In order to reset the device to factory settings, press the "F" button located on the device back panel when the device is powered up and hold it until the "Status" indicator begins to flash red and green intermittently. The device will be rebooted automatically.

Factory settings:

- DHCP client is launched on WAN interface;
- MGMT interface address – 192.168.1.1;
- subnet mask – 255.255.255.0;
- user name/password for web interface access: admin/password.

2.8 Delivery Package

TAU-8N.IP standard delivery package includes:

- TAU-8N.IP VoIP gateway;
- 220/12 V, 2.0 A power adapter;
- Installation and configuration guide.

3 Device Management via Web Configurator

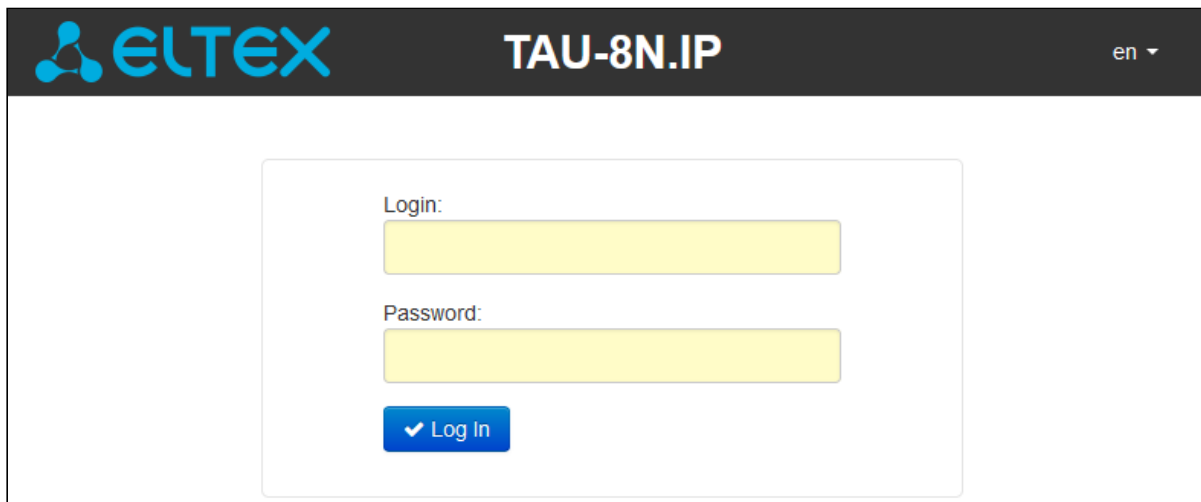
3.1 Getting Started

In order to start the operation, connect to the device via MGMT interface using a web browser:

1. Open a web browser (hypertext document viewer), for example, Firefox, Opera, Chrome.
2. Enter the device IP address in the browser address bar.

⚠ Default IP address of the device – **192.168.1.1**; subnet mask – **255.255.255.0**.

When the device is successfully detected, username and password request page will be shown in the browser window.



3. Enter your username into "Login" and password into "Password" field.

⚠ Factory settings: **login – admin**; **password – password**.

4. Click the "Log in" button. The quick configuration menu will be shown in the browser window.

⚠ Change the default user password to avoid unauthorized access to the device. For setting password for access via web interface, see "[WEB Authentication](#)" Submenu. It is recommended to write down and store the set passwords in a safe place which is inaccessible for intruders. Device management must be inaccessible from public networks. Management allocation in a separate VLAN is described in "[Network Settings](#)" Submenu. Disabling of unused protocol for management and standard ports changing are described in "[Access](#)" Submenu.

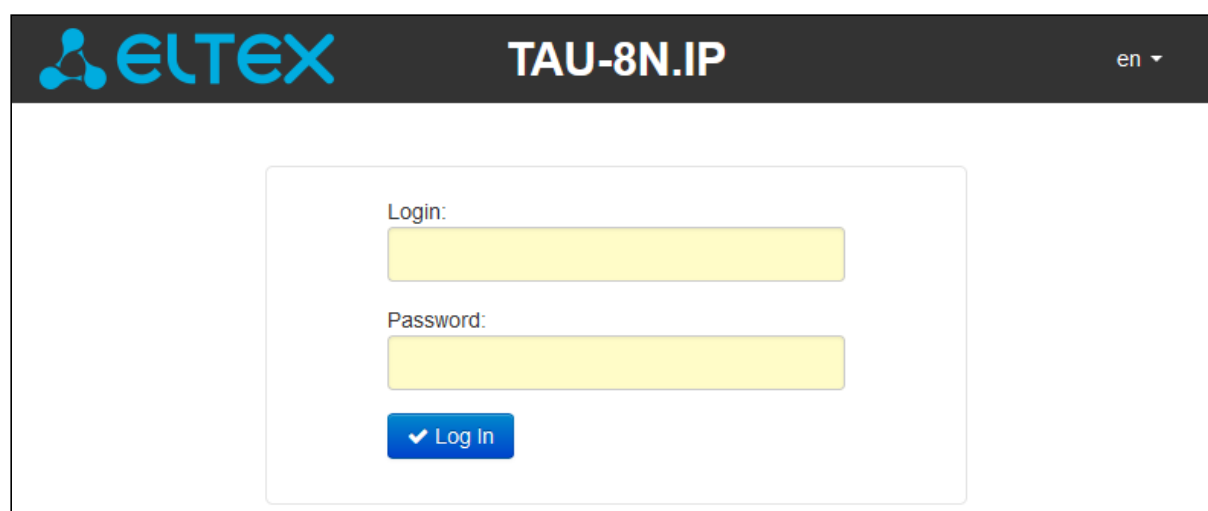
✓ Before working with the device, it is recommended to upgrade the firmware to the current version (see the "[Firmware Upgrade](#)" Submenu). The current version of the firmware can be obtained on the [Download Center](#) page on the official website of the company or by contacting the ELTEX Service Center. For technical support contacts and useful links, see the Technical Support section on the last page of this manual.

3.2 User Change

There are three user types for the device: **admin**, **user** and **viewer**. **Admin (administrator)**, default password: **password** has the full access to the device: reading and writing any settings, full device status monitoring. **User (non-privileged user)**, default password: **user** may change their password and configure PPPoE in order to connect to the Internet, may not access the device status monitoring. **Viewer** (default password: **viewer**) may view full device configuration, may change only their password, may access full device status monitoring.



When you click the "logout" button, the current user session will be terminated; login window will be displayed:



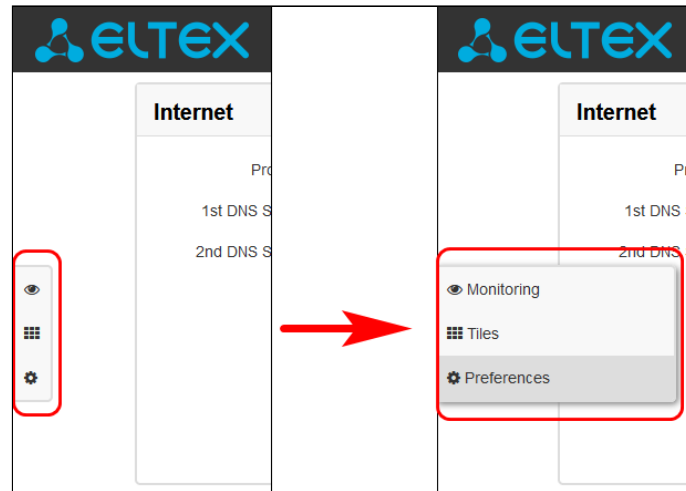
To change the access, you should specify the corresponding username and password and click the "Log in" button.

3.3 Web Interface Operation Modes

TAU-8N.IP web interface can operate in three modes:

- **Monitoring** – system monitoring mode that is used to view device operation information: network connection availability, phone port state, amount of data received/transferred via network interfaces, etc.;
- **Tiles** – quick system configuration mode. Each tile contains settings grouped by their functions: Internet, VoIP and System. A tile only displays basic parameters that enable the quickest possible configuration of a specific device function;
- **Preferences** – advanced system configuration mode (full configuration mode) that enables full device configuration.

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



To proceed from the "Tiles" mode into "Preferences", you may also click "more" link in the tile heading.

3.4 Applying and Discarding Changes Made to Configuration

3.4.1 Applying Configuration







⚠ Click the "Apply" button to save the configuration into the device flash memory and apply new settings. All settings will be applied without device restart.

The "Apply" button in the quick configuration menu and the advanced settings menu will appear as follows:



Web interface visual indication of the current status of the setting application process is described in the following table:

Visual indication of the current status of the setting application process

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

3.4.2 Discarding Changes

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

The "Cancel" button in the quick configuration menu and the advanced settings menu will appear as follows:



3.5 Quick Configuration Menu

In the quick configuration menu, basic device settings are displayed, see [Figure 6](#).

Figure 6 – Quick configuration menu

Settings are divided into the following tiles:

- *Internet* – quick Internet access configuration;
- *VoIP* – quick VoIP configuration;
- *System* – configuration of access to web interface via WAN port.

3.5.1 Internet

In order to access the Internet, basic settings should be specified in the "Internet" tile. To specify additional parameters, go to advanced settings mode by clicking the "more" link.

- *Protocol* – select the protocol that will be used for device WAN interface connection to provider network:
 - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. When "Static" type is selected, the following parameters will be available for editing:
 - *WAN IP* – specify device WAN interface IP address in the provider network;
 - *Netmask* – external subnet mask;
 - *Default Gateway* – address where the packet will be sent to, when route for it is not found in the routing table;
 - *1st DNS Server, 2nd DNS Server* – domain name server addresses (allow to identify the IP address of the device by its domain name). You may leave these fields empty, if they are not required.
 - *DHCP* – operation mode where IP address, netmask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.

Supported options:

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

In Option 60 DHCP request, the device will send vendor information in the following format: **[VENDOR:vendor][DEVICE:device type][HW:hardware version][SN:serial number]**

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

Example:

[VENDOR:Eltex][DEVICE:TAU-8N.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0][VERSION:1.8.1]

The list of DHCP options used on each network interface (Internet, VoIP, Management) can be set manually. See the list setup information in the [Appendix C](#).

PPPoE – operation mode when PPP session is established on WAN interface. When "PPPoE" is selected, the following parameters are available for editing:

- *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 (this parameter is optional, and configured only on the provider's request);
- *Secondary Access* – type of access to local network resources.

There are 2 options to select:

- *DHCP* – dynamic access when IP address and all other required parameters are obtained via DHCP;
- *Static* – in this case, it is necessary to manually specify access settings: IP address, Netmask, DNS Server.

L2TP – operation mode when the Internet access is established via a tunnel, using L2TP. When "L2TP" is selected, the following parameters will be available for editing:



- *L2TP Server* – L2TP server address (domain name or IP address in IPv4 format);
- *User Name* – user name for authorization on L2TP server;
- *Password* – password for authorization on L2TP server;
- *Secondary access* – type of access to local network resources and L2TP server.

You may select 2 options:

- *DHCP* – dynamic access when IP address and all other required parameters are obtained via DHCP;
- *Static* – in this case, L2TP server access settings should be specified manually:
 - *IP Address* – when the static access is used, L2TP server will be accessed from this address;
 - *Netmask* – when the static access is used, subnet mask;
 - *DNS Server* – when the static access is used, local area network DNS;
 - *Gateway* – when the static access is used, gateway for L2TP server access (if necessary).

L2TP allows establishing secure communication link over the Internet between the remote user's computer and organization's private network. L2TP is based on Point-to-Point Protocol (PPP) and acts as its extension. First, the OSI model higher level data is encapsulated into PPP, and then into L2TP for tunnel transmission via public data networks. L2TP may be used not only in IP networks, service messages for tunnel creation and data transfer use the same format and protocols.

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

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

To connect the device to the provider network, it is necessary to request the network settings from the provider. If you use the static settings, select "Static" value in the "Protocol" field and fill the "WAN IP", "Netmask", "Default Gateway", "1st DNS Server", and "2nd DNS Server" fields with the corresponding values obtained from the provider. If devices in the provider network obtain network settings via DHCP, PPPoE, or L2TP – select the corresponding protocol in the "Protocol" field and refer to provider's instructions to achieve complete and correct device configuration.

3.5.2 VoIP



For VoIP operation, you should specify settings in the "VoIP" tile. To specify additional parameters, go to advanced settings mode by clicking the "more" link.

In the tabs "Line 1" – "Line 8" you may configure the device phone ports "Phone 1" – "Phone 8" respectively:

- *Enable* – when checked, the current line is active;
- *Number* – subscriber number assigned for the phone line;
- *User Name* – user name for authentication on SIP server;
- *Password* – password for authentication on SIP server.

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

- *Proxy Server* – network address of a SIP server – device that manages access to provider's phone network for all subscribers. You may specify IP address as well as the domain name (specify an alternative SIP server UDP port after the colon (:), default value is 5060);
- *Registration* – when checked, subscriber port registration will be enabled on the registration server;
- *Registration Server* – network address of a device that is used for registration of all phone network subscribers in order to provide them with the communication services (specify an alternative registration server port after the colon (:), default value is 5060). You may specify IP address as well as the domain name. Usually, registration server is physically co-located with SIP proxy server (they have the same address);
- *SIP Domain* – domain where the device is located (fill in if required), is assigned automatically when receiving DHCP option 15 or specified manually. A manually specified domain takes precedence over the DHCP configuration.

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



3.5.3 System

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

Access to web via WAN:

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

⚠ By default, access to the device web interface is enabled only for MGMT interface.

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

3.6 Advanced Settings

To proceed to the advanced settings mode, click "more" link in any title heading or select "Preferences" on the left panel.

3.6.1 Web Interface Basic Elements

Figure 7 shows web configurator basic navigation elements in the advanced settings mode.

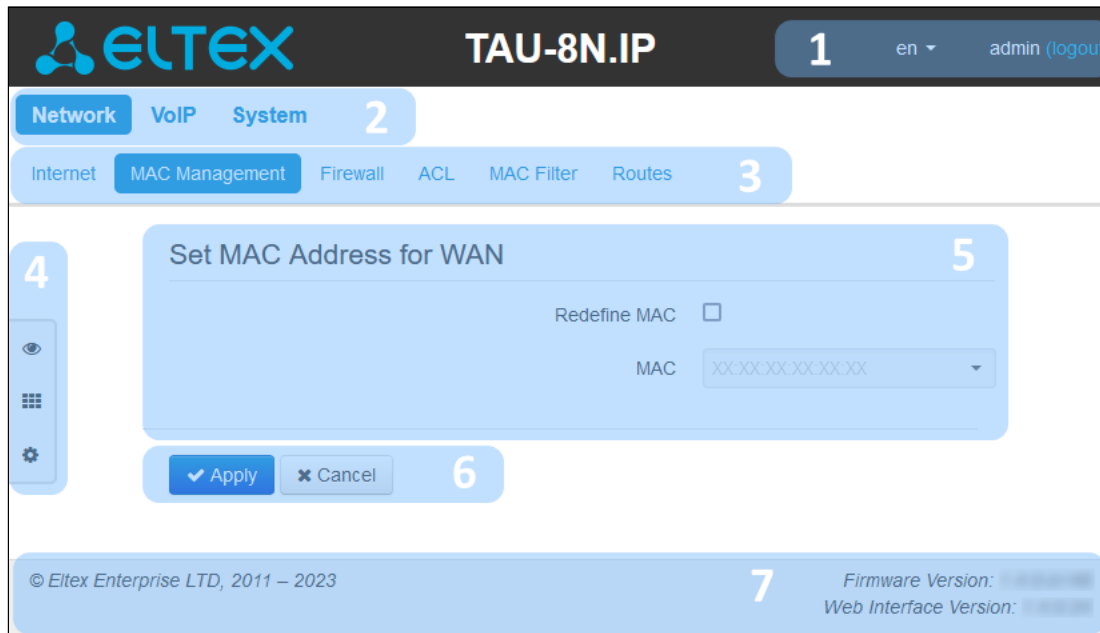


Figure 7 – Web configurator navigation elements

User interface window is divided into seven areas:

1. Logged in user name, session termination button in the web interface (*logout*) for the current user and drop-down menu for setting language.
2. Menu tabs include submenu tabs grouped by category: **Network, VoIP, System**.
3. Submenu tabs allow you to control settings field.
4. Web configurator mode changing panel (for more details, see Section "[Web Interface Operation Modes](#)").
5. Device settings field based on the user selection; allows you to view device settings and enter configuration data.
6. Configuration management buttons (for more details, see Section "[Applying and Discarding Changes Made to Configuration](#)"):
 - *Apply* – apply and save the current configuration into the device non-volatile memory;
 - *Cancel* – discard changes (you can discard changes only until "*Apply*" button is clicked).
7. Informational field showing firmware version and Web interface version.

3.6.2 "Network" Menu

In the "Network" menu, you may configure the device network settings.

3.6.2.1 "Internet" Submenu

In the "Internet" submenu, you may configure an external network (via PPPoE, DHCP, L2TP and statically) and management interface.

Common Settings

- *Hostname* – device network name.

WAN

- *Internet Connection* – external network connection method for the device:
 - *Wired connection* – connection to the Internet is established using only Ethernet cable via WAN port;
 - *3G/4G USB Modem* – connection to the Internet is established using 3G/4G USB modem (via cellular data network), connected to the USB port of the device;

- *Automatically Switch to Reserve Channel* – connection to the Internet is established via the primary channel (defined below in the "*Primary Channel*" field), and in case of loss of access to the Internet via the main channel, an automatic transition to the reserve channel will be made.
- *Speed and duplex* – specify data rate and duplex mode for WAN Ethernet port of the gateway:
 - *Auto* – automatic speed and duplex negotiations;
 - *100 Half* – 100 Mbps data transfer rate with half-duplex mode is supported;
 - *100 Full* – 100 Mbps data transfer rate with duplex mode is supported;
 - *10 Half* – 10 Mbps data transfer rate with half-duplex mode is supported;
 - *10 Full* – 10 Mbps data transfer rate with duplex mode is supported;

Connection Settings:

- *Protocol* – select the protocol that will be used for device WAN interface connection to provider network:
 - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned statically. When "*Static*" type is selected, the following parameters will be available for editing:
 - *WAN IP Address* – specify device WAN interface IP address in the provider network;
 - *Netmask* – external subnet mask;
 - *Default Gateway* – address where the packet will be sent to, when route for it is not found in the routing table;
 - *1st DNS Server, 2nd DNS Server* – domain name server addresses (allow to identify the IP address of the device by its domain name). You may leave these fields empty, if they are not required;
 - *MTU* – maximum size of data block transmitted through the network;
 - *Use VLAN* – when the box is checked, use identifier type VLAN specified in the "*VLAN ID*" field for Internet connection:
 - *VLAN ID* – VLAN identifier used for the service;
 - *802.1P* – 802.1P marker (another name is CoS (Class of Service)), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority).
 - *DHCP* – operation mode where IP address, netmask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.

Supported options:

- 1 – network mask;
- 3 – the default network gateway address;
- 6 – DNS address;
- 12 – device network name;
- 15 – domain name;
- 26 – MTU size;
- 28 – network broadcast address;
- 33 – static routes;
- 42 – NTP server address;
- 43 – specific vendor information;
- 60 – alternative vendor ID;
- 66 – TFTP server address;
- 67 – firmware file name (to download via TFTP from the server specified in Option 66);
- 82 – DHCP Relay agent information;
- 120 – SIP server outbound;
- 121 – classless static routes;
- 249 – Private/Classless Static Route (MS).

For DHCP, you may specify the required value for Options 60 and 82.

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

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

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

Example:

```
[VENDOR:Eltex][DEVICE:TAU-8N.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0][VERSION:1.8.1]
```

- *DHCP Relay Agent information (Option 82)* – when checked, you can add the following data to DHCP request:
 - *Agent circuit ID (Option 82)* – allows adding suboption 1 – Agent Circuit ID into DHCP request;
 - *Agent Remote ID (Option 82)* – allows adding suboption 2 – Agent Remote ID into DHCP request.

The list of DHCP options used on each network interface (Internet, VoIP) can be set manually. You will find the list setup information in the Appendix C.

- *1st DNS Server, 2nd DNS Server* – DNS IP address – if DNS addresses are not automatically assigned via DHCP, define them manually. Manually defined addresses will take precedence over DNS addresses obtained via DHCP;
- *MTU* – maximum size of data block transmitted through the network;
- *Use VLAN* – when the box is checked, use identifier type VLAN specified in the "VLAN ID" field for Internet connection:
 - *VLAN ID* – VLAN identifier used for the service;
 - *802.1P* – 802.1P marker (another name is CoS (Class of Service)), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority).
- *PPPoE* – operation mode when PPP session is established on WAN interface. When:
 - *User Name* – user name for authorization on PPP server;
 - *Password* – password for authorization;
 - *MTU* – maximum block size for data transmitted via the network (1492 is recommended value);
 - *Service-Name* – Service-Name tag value in PADI message (this parameter is optional);
 - *Connection Type* – depending on the value chosen, a PPPoE session is always established (*AlwaysOn*), initiated when traffic should be transmitted (*OnDemand*) or established/terminated manually using the buttons "Connect tunnel/Disconnect tunnel" (*Manual*);
 - *Idle, s* – the period of time after which a PPPoE session is terminated due to inactivity in *OnDemand* mode;
 - *LCP echo interval, s* – LCP request period;
 - *LCP echo failure* – the number of unanswered LCP requests, after which a PPPoE session is terminated;
 - *Secondary Access* – type of access to local network resources. You may select 2 options:
 - *DHCP* – dynamic access when IP address and all other required parameters are obtained via DHCP;
 - *Static* – in this case, you should specify access settings manually: *IP address, Netmask, DNS Server, Gateway*.
 - *Use the Secondary Access for VoIP* – this option is available, if there are no dedicated interfaces for VoIP service ("Use Internet Settings" checkbox is selected). When the checkbox is not selected (default value), VoIP service uses PPP interface for its operation; when selected – secondary access interface (IPoE);
 - *Use VLAN* – when the checkbox is selected, use identifier type VLAN specified in the "VLAN ID" field for Internet connection:

- *VLAN ID* – VLAN identifier used for the service;
- *802.1P* – 802.1P marker (another name is CoS (Class of Service)), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority).
- *L2TP* – operation mode when the Internet access is established via a tunnel, using L2TP. When "*L2TP*" is selected, the following parameters will be available for editing:
 - *L2TP Server* – L2TP server IP address;
 - *User Name* – user name for authorization on L2TP server;
 - *Password* – password for authorization on L2TP server;
 - *MTU* – maximum block size for data transmitted via the network (1462 is recommended value);
 - *Secondary access* – type of access to local network resources and L2TP server.

You may select 2 options:

- *DHCP* – dynamic access when IP address and all other required parameters are obtained via DHCP;
- *Static* – in this case, L2TP server access settings should be specified manually:
 - *IP Address* – when the static access is used, L2TP server will be accessed from this address;
 - *Netmask* – when the static access is used, subnet mask;
 - *DNS Server* – when the static access is used, local area network DNS;
 - *Gateway* – when the static access is used, gateway for L2TP server access (if necessary);
 - *Use secondary access for VoIP* – this option is available, if there are no dedicated interfaces for VoIP service ("*Use Internet Settings*" checkbox is selected). When the checkbox is not selected (default value), VoIP service uses PPP interface for its operation; when selected – secondary access interface (IPoE).

L2TP allows establishing secure communication link over the Internet between the remote user's computer and organization's private network. L2TP is based on Point-to-Point Protocol (PPP) and acts as its extension. First, the OSI model higher level data is encapsulated into PPP, and then into L2TP for tunnel transmission via public data networks. L2TP may be used not only in IP networks, service messages for tunnel creation and data transfer use the same format and protocols.

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

- *Use VLAN* – when the checkbox is selected, use VLAN ID specified in the "*VLAN ID*" field for Internet connection:
 - *VLAN ID* – VLAN identifier used for the service;
 - *802.1P* – 802.1P marker (another name is CoS (Class of Service)), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority).

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

When "3G/4G USB Modem" connection method is selected, the following fields will be available for configuration:

The screenshot shows a configuration window titled "WAN". Under the heading "Connection Settings", there are several fields:

- Internet Connection:** A dropdown menu currently set to "3G/4G USB Modem".
- Mobile Provider:** A dropdown menu currently set to "Megafon".
- User Name:** An empty text input field.
- Password:** A text input field with ten dots representing masked characters.
- Called Number:** An empty text input field.
- Additional Parameters:** An empty text input field.
- MTU:** A dropdown menu currently set to "1492".

At the bottom of the form, there is a button labeled "By Default" with a pencil icon. Below the button, there is a note: "Click the button to fill in the recommended by your ISP values of the settings".

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

If your provider is missing from the list, select "Other" and enter your service provider settings into fields.

- *Protocol* – this field is available only when "Other" is selected in the mobile service providers list. For most cases, mobile service providers establish network access using *PPPoE*, however some modems may require *DHCP* for proper operation;
- *User Name* – username for authentication in the wireless network;
- *Password* – password for authentication in the wireless network;
- *Called Number* – dial-up number for wireless network connection (e.g.: *99***1#);
- *Additional Parameters* – parameters for mobile network connection (e.g.: AT+CGDCONT=1,IP,internet– for Megafon); do not use quotation marks in this string;
- *MTU* – maximum block size for data transmitted via the network (1492 is recommended value).

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

When "Automatically Switch to Reserve Channel" connection method is selected, the following settings will be available for configuration:

WAN

Internet Connection Automatically Switch to Reservi ▾

[Checking the Access to the Internet](#)

Primary Channel Wired ▾

Speed and Duplex Auto ▾

Wired Connection Settings

Protocol DHCP ▾

Alternative Vendor ID (option 60)

DHCP Relay Agent Information (Option82)

1st DNS Server

2nd DNS Server

MTU 1500

Use VLAN

Wireless Connection Settings

Mobile Provider Other ▾

Protocol PPPOE ▾

User Name

Password

Called Number *99#

Additional Parameters AT+CGDCONT=1,IP,internet

MTU 1492 ▾

- *Primary channel* – select the type of the primary channel from the drop-down list:
 - *Wired* – channel via the Ethernet WAN port of the device;
 - *Wireless* – channel via a mobile network through the wireless USB modem.

Wired Connection settings:

The settings are identical to settings for "Wired Connection" method.

Wireless connection settings:

The settings are identical to settings for "3G/4G USB modem" connection method.

Checking the Access to the Internet

Checking the Access to the Internet

Server Response Timeout, ms	<input type="text" value="1000"/>	↓↑
Number of Attempts to Access the Server	<input type="text" value="10"/>	↓↑
Interval Between Server Polling Cycles, s	<input type="text" value="240"/>	↓↑
Ping Server 1	<input type="text" value="8.8.8.8"/>	
Ping Server 2	<input type="text" value="8.8.4.4"/>	<input type="button" value="🗑"/>
	<input type="button" value="+"/>	

- *Server Response Timeout, ms* – time during which a response from the PING server is expected;
- *Number of Attempts to Access the Server* – maximum amount of attempts to access a PING server, after which it will be decided to switch to the redundant channel;
- *Interval Between Server Polling Cycles, s* – time interval after which a new PING server poll cycle starts;
- *Ping Server 1..5* – IP address or domain name of a PING server. Fields for entering PING servers 2..5. appear after a previous field filled.

MGMT Management Interface

- *IP address* – IP address of the device for the management interface;
- *Netmask* – management interface subnet mask.

IPSec Settings

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

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

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

IPSec Settings

Enable

Interface Ethernet ▾

Local IP Address

Local Subnet

Local Netmask

Remote Subnet

Remote Netmask

Remote Gateway

NAT-Traversal IPsec Off ▾

Aggressive Mode

My Identifier Type address ▾

My Identifier

Phase 1

Pre-shared Key

IKE Authentication Algorithm md5 ▾

IKE Anryption Algorithm des ▾

Diffie Hellman Group 1 ▾

IKE SA Lifetime, s 86400 ▾

Phase 2

IKE Authentication Algorithm hmac_md5 ▾

IKE Anryption Algorithm des ▾

Diffie Hellman Group 1 ▾

IPSec SA Lifetime, s 3600 ▾

- *Enable* – allow using IPSec for data encryption;
- *Interface* – this setting takes effect only when PPPoE, PPTP or L2TP are selected for the Internet, and defines the interface that will be accessed with IPSec: Ethernet (secondary access interface) or PPP (primary access interface); When DHCP or Static protocol is selected, there is only a single interface (Ethernet) active for the service that may be accessed with IPSec only;
- *Local IP Address* – device address for IPSec operation;
- *Local subnet* address together with *Local Netmask* define a local subnet for creation of network-to-network or network-to-point topologies;

- *Remote subnet* address together with *Remote Netmask* define a remote subnet address used for IPSec encrypted communication. If the mask value is 255.255.255.255 communication is performed with a single host. Mask that differs from 255.255.255.255 allows defining a whole subnet. Thus, functionality of the device allows organizing the following 4 network topologies with using encryption traffic via IPSec protocol: point-to-point, network-to-point, point-to-network, network-to-network;
- *Remote Gateway* – gateway used for remote network access;
- *NAT-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:
 - *On* – NAT-T mode is enabled only when NAT is detected on the way to the destination host;
 - *Force* – use NAT-T in any case;
 - *Off* – disable NAT-T on connection establishment.
 The following NAT-T settings are available:
 - *NAT-T UDP Port* – UDP port for packets used for IPSec message encapsulation. Default value is 4500;
 - *Interval Between Sending NAT-T Keepalive Packets, s* – periodic message transmission interval for UDP connection keepalive on the device performing NAT functions;
 - *Aggressive Mode* – phase 1 operation mode, when all the necessary data is exchanged using three unencrypted packets. In the main mode, the exchange process involves six unencrypted packets;
 - *My Identifier Type* – device identifier type: *address, fqdn, keyed, user_fqdn, asn1dn*;
 - *My Identifier* – device identifier used for identification during phase 1 (fill in, if required). Identifier format depends on the type.

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

- *Pre-shared Key* – a secret key used by authentication algorithm in phase 1. A string from 8 to 63 characters long;
- *IKE Authentication Algorithm* – select an authentication algorithm from the list: *md5, sha1*;
- *IKE Encryption Algorithm* – select an encryption algorithm from the list: *des, 3des, blowfish*;
- *Diffie Hellman Group* – select Diffie-Hellman group;
- *IKE SA Lifetime, s* – 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:

- *IKE Authentication Algorithm* – select an authentication algorithm from the list: *hmac-md5, hmac-sha1, des, 3des*;
- *IKE Encryption Algorithm* – select an encryption algorithm from the list: *des, 3des, blowfish*;
- *Diffie Hellman Group* – select Diffie-Hellman group;
- *IPSec SA Lifetime, s* – time that should pass for data encryption key changeover. Default value is 60 minutes (3600 seconds).

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

3.6.2.2 "MAC Management" Submenu

In the "MAC management" submenu, you may change the device WAN interface MAC address.

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

To redefine MAC on the WAN interface, enter the required MAC address in the MAC field.

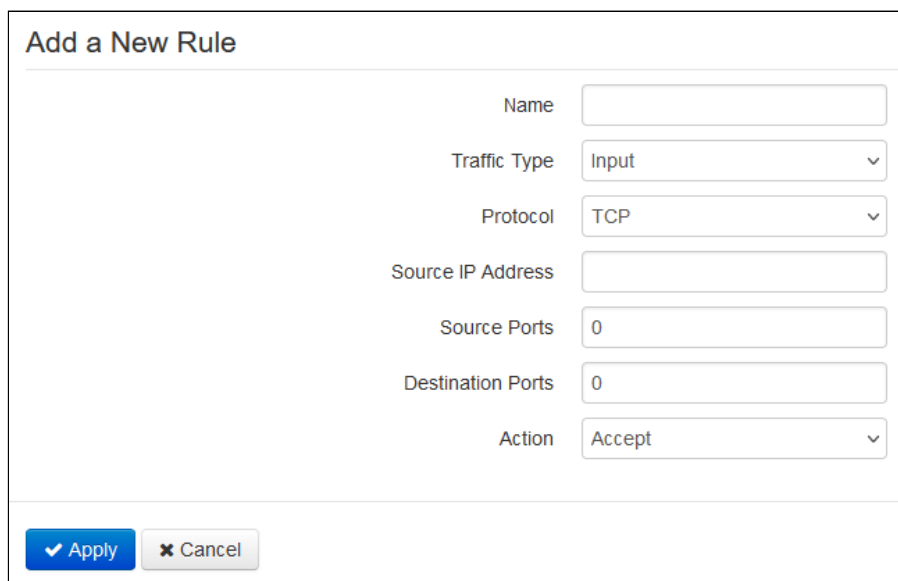
To apply a new configuration and store settings into the non-volatile memory, click the "Apply" button. To discard changes, click the "Cancel" button.

3.6.2.3 "Firewall" Submenu

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

3.6.2.4 Configuration of firewall rules

To add a new rule, click the "Add" button and fill in the following fields in the "Add a New Rule" window:



- *Name* – rule name;
- *Traffic Type* – select the traffic type that will fall under this rule:
 - *Input* – incoming device traffic (recipient is one of the device network interfaces). When this traffic type is chosen, the following fields will be available for editing:
 - *Source IP Address* – define starting source IP address. Use "/" symbol to define a subnet mask in "xxx.xxx.xxx.xxx" or "xx" format, e.g. 192.168.16.0/24 or 192.168.16.0/255.255.255.0, when you need to highlight an address range (/24 mask record corresponds to /255.255.255.0);
 - *Output* – outgoing device traffic (traffic generated locally by the device from one of the network interfaces). When this traffic type is chosen, the following fields will be available for editing:
 - *Destination IP Address* – define destination IP address. Use "/" symbol to define a mask in "xxx.xxx.xxx.xxx" or "xx" format, e.g. 192.168.18.0/24 or 192.168.18.0/255.255.255.0, when you need to highlight an address range;
- *Protocol* – packet protocol that will fall under this rule: *TCP, UDP, TCP/UDP, ICMP, any*;
- *Action* – action to be performed on packets (*Accept/Drop*).

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

- *Source Ports* – list of source ports falling under the rule (a single port or port range delimited by "-" is permitted);
- *Destination Ports* – list of destination ports falling under the rule (a single port or port range delimited by "-" is permitted).

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

- *Type of ICMP Message* – you can create the rule for the specific ICMP message type or for all ICMP message types.

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

3.6.2.5 "ACL" Submenu

In the "ACL" submenu you may configure access lists. ACL (Access Control List) contains rules that determine traffic flow through the interface.

3.6.2.6 Limitations on MAC Addresses

Add a New Rule

Enable

Interface

MAC Address

Access

✔ Apply
✘ Cancel

- *Enable* – when checked, MAC filtering rule is enabled;
- *Interface* – interface for which the created rule will be valid (*wan/mgmt*);
- *MAC Address* – MAC address of a device for which the created rule will be valid;
- *Access* – Allow/Deny access for a given device..

3.6.2.7 Time Limits on Schedule

Add a New Rule

Enable

Interface

Traffic Type

Begin At

Stop At

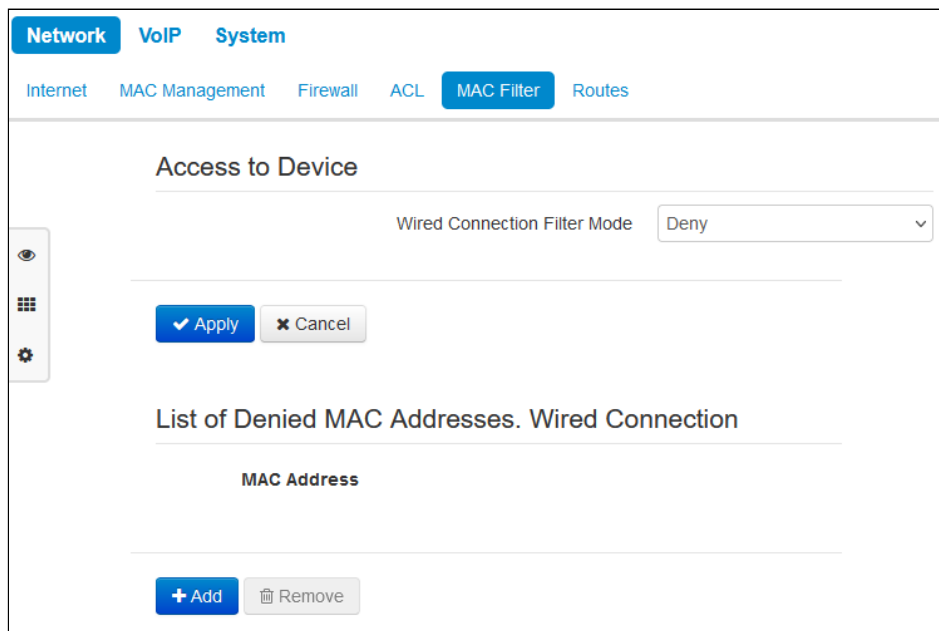
Access

✔ Apply
✘ Cancel

- *Enable* – when checked, a filtering rule is enabled and disabled at the scheduled time;
- *Interface* – interface for which the created rule will be valid (*wan/mgmt*);
- *Traffic type* – the traffic for which the created rule will be valid (*Input/Output*);
- *Begin at* – time in the 24-hour clock (hh:mm), from which the created rule will be valid;
- *Stop at* – time in the 24-hour clock (hh:mm), up to which the created rule will be valid;
- *Access* – Allow/Deny access for a given device.

3.6.2.8 "MAC Filter" Submenu

In the "MAC filter" submenu, you may configure access filtering by client's MAC address.



- **Wired Connection Filter Mode** – defines one of the three filter operation modes depending on the client's MAC address:
 - *Disabled* – MAC address filtering is disabled; all clients are able to connect to the device;
 - *Deny* – access is forbidden for devices with MAC addresses from the "List of Denied MAC Addresses. Wired Connection". Access for devices with unlisted MAC addresses is permitted;
 - *Allow* – access is permitted for devices with MAC addresses from the "List of Allowed MAC Addresses. Wired Connection" in this operation mode. Access for devices with unlisted MAC addresses is forbidden.

List of MAC Addresses

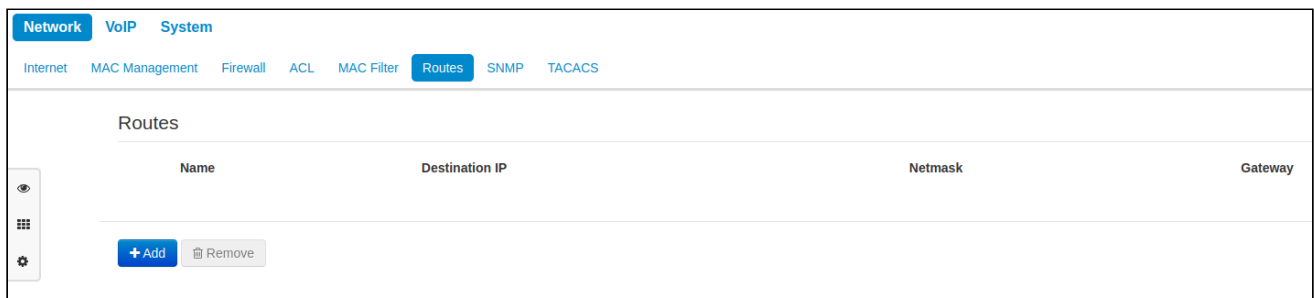
You may enter up to 30 client MAC addresses which may access the device in accordance with the specified filtering mode.

To add a new client to the list, click the "Add" button and enter its MAC address.

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

3.6.2.9 "Routes" Submenu

In the "Routes" submenu, you may configure device static routes.



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

Add Route

Name

Destination IP

Netmask

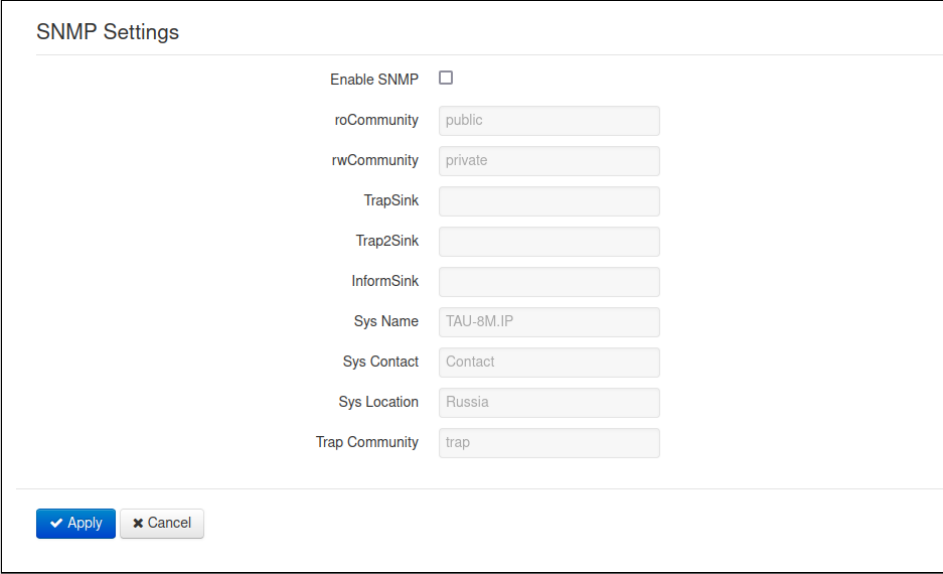
Gateway

- *Name* – route name, used for human perception convenience. You may leave this field empty;
- *Destination IP* – IP address of destination host or subnet that the route should be established to;
- *Netmask* – a subnet mask. Netmask for host should be 255.255.255.255, for subnet – depending on its size;
- *Gateway* – gateway IP address that allows for the access to the "Destination IP".

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

3.6.2.10 "SNMP" Submenu

The TAU-8N.IP software allows monitoring the device status using the SNMP protocol. In the "SNMP" submenu the parameters of the SNMP agent are configured. The device supports protocol versions SNMPv1, SNMPv2c.



- *Enable SNMP* – if this flag is set, the use of SNMP protocol is allowed;
- *Read password* – password for reading parameters (common: public);
- *Write password* – password for writing parameters (common: private);
- *Address for receiving v1 traps* – IP address or domain name of the SNMPv1-trap message receiver in HOST [COMMUNITY [PORT]] format;
- *Address for receiving v2 traps* – IP address or domain name of the SNMPv2-trap message receiver in HOST [COMMUNITY [PORT]] format;
- *Address to receive Inform messages* – IP address or domain name of the Inform message receiver in HOST [COMMUNITY [PORT]] format;
- *Device System Name* – the name of the device;
- *Manufacturer Contact Information* – contact information of the device manufacturer;
- *Device Location* – information about the location of the device;
- *Password in traps* – password contained in traps (default: trap).

A list of objects supported for reading and configuration via SNMP:

- *Enterprise.1.3.1* – general SIP profile settings;
- *Enterprise.1.3.2.1* – SIP profile settings;
- *Enterprise.1.1.2.1* – FXS port settings;
- *Enterprise.1.1.4.1.1* – call group settings;
- *Enterprise.1.1.5* – codes for activating VAS from the telephone set;
- *Enterprise.2.1* – SNMP settings;
- *Enterprise.3.1* – system log settings,

where Enterprise is 1.3.6.1.4.1.35265.1.289.1 device ID.

To write the settings to the non-volatile memory, press the "Apply" button. To cancel the changes, press the "Cancel" button.

3.6.2.11 "TACACS" Submenu

This section configures the use of the TACACS+ protocol. The TACACS+ protocol provides a centralized security system to verify users accessing the device.

TACACS Settings

Enable TACACS

Authentication Priority: TACACS -> Local v

Check Interval for TACACS-server: 5

Primary Server

Server:

Secret Key: *****

Reserve Server

Server:

Secret Key: *****

✓ Apply
✕ Cancel

- *Enable TACACS* – if this flag is checked, the use of the TACACS protocol is enabled;
- *Authentication Priority* – TACACS protocol usage mode:
 - *TACACS* – users are authenticated only against a list of TACACS servers;
 - *Local -> TACACS* – user authentication is performed first using the local user base, then using the list of TACACS servers;
 - *TACACS -> Local* – user authentication is performed first by the list of TACACS servers, then by the local user base.
- *TACACS Server Availability Check Interval* – the interval after which the device considers that the TACACS server is unavailable;
- *Primary Server:*
 - *Server* – network address of the main TACACS server. Both IP address and domain name (specify an alternative TACACS server port after the colon (:), default value is 49);
 - *The secret key* is the password for authentication to the primary TACACS server.
- *Backup Server:*
 - *Server* – network address of the backup TACACS server. Both IP address and domain name can be specified (specify an alternative TACACS server port after the colon (:), default value is 49);
 - *The secret key* is the password for authentication to the backup TACACS server.

⚠ TACACS and Digest authentication cannot be used simultaneously.

3.6.3 "VoIP" Menu

In the "VoIP" menu, you may configure VoIP (Voice over IP): SIP configuration, FXS interface configuration, installation of codecs, dialplan, fax and modem data transfer methods.

3.6.3.1 "Network Settings" Submenu

In the "Network Settings" submenu, it is an option to set your own network settings for the VoIP service.

- *Use Internet Settings* – when checked, use network settings specified in the "Network → Internet" menu, otherwise use settings specified in this menu;
- *Use VLAN* – when checked, VoIP service will use a dedicated interface in a separate VLAN, with VLAN number specified in the "VLAN ID";
- *VLAN ID* – VLAN identifier used for the service;
- *802.1P* – 802.1P marker (another name is CoS (Class of Service)), assigned to the outgoing IP packets from this interface. It may take values from 0 (the lowest priority) to 7 (the highest priority);
- *Protocol* – select address assigning protocol for the VoIP service interface:
 - *Static* – operation mode where IP address and all the necessary parameters for WAN interface are assigned manually. When "Static" type is selected, the following parameters will be available for editing:
 - *IP address* – specify the IP address for VoIP service interface;
 - *Netmask* – subnet mask of the VoIP service interface;
 - *Default gateway* – IP address for VoIP service interface default gateway;
 - *1st DNS Server, 2nd DNS Server* – DNS server IP addresses required for VoIP service operations.
 - *DHCP* – operation mode where IP address, netmask, DNS address and other necessary settings for service operation (e.g. SIP and registration server static routes) are automatically obtained from DHCP server. If you are unable to obtain DNS server addresses from the provider, you may

specify them manually using "1st DNS Server" and "2nd DNS Server" fields. Manually defined addresses will take precedence over DNS addresses obtained via DHCP.

For DHCP, you may specify the required value for Options 60 and 82.

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

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

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

Example:

[VENDOR:Eltex][DEVICE:TAU-8N.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0][VERSION:1.8.1]

- *DHCP Relay Agent information (Option 82)* – when checked, you can add the following data to DHCP request:
 - *Agent circuit ID (Option 82)* – enables adding suboption 1 – Agent Circuit ID into DHCP request;
 - *Agent Remote ID (Option 82)* – enables adding suboption 2 – Agent Remote ID into DHCP request.

The list of DHCP options used on each network interface (Internet, VoIP) can be set manually. You will find the list setup information in the Appendix C.

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

3.6.3.2 "QoS" Submenu

In the "QoS" submenu, you may configure Quality of Service (QoS) functions.

The screenshot displays the QoS configuration interface. At the top, there are tabs for "Network", "VoIP", and "System". Below these are sub-tabs for "Network Settings", "QoS", "Line Settings", "SIP Profiles", "Dialplan Profiles", "Hunt Groups", and "Pickup Groups". Further down, there are links for "Supplementary Service Prefixes", "Cadence", and "Call History".

The main content area is divided into two sections:

- RTP Port Range Configuration:** This section contains two input fields: "Min RTP Port" with a value of 23000 and "Max RTP Port" with a value of 26000. Below these fields are "Apply" and "Cancel" buttons.
- DSCP Configuration:** This section features a table with two columns: "SIP Port" and "DSCP". Below the table are "+ Add" and "Remove" buttons.

RTP Port Range Configuration

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

DSCP Configuration

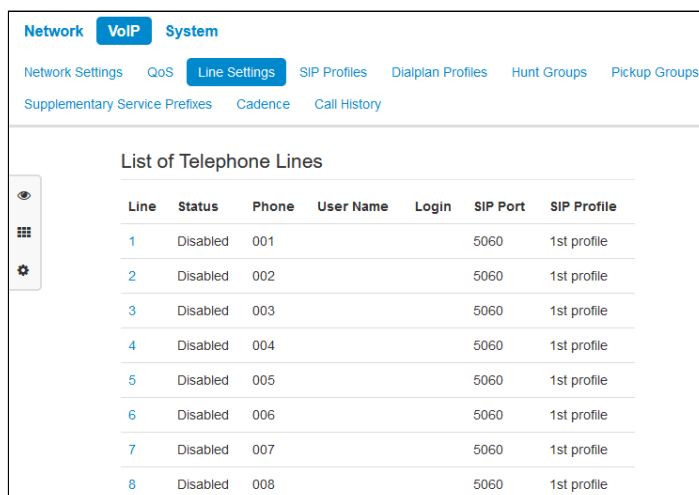
The screenshot shows the "Add" configuration dialog. It contains two input fields: "SIP Port" with a value of 0 and "DSCP" with a value of 0. Below these fields are "Apply" and "Cancel" buttons.

- *SIP Port* – the value of a source port for outgoing voice traffic to be marked by the specified DSCP code;
- *DSCP* – DSCP field value of IP packet header for voice traffic with the specified source port.

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

3.6.3.3 "Line Settings" Submenu

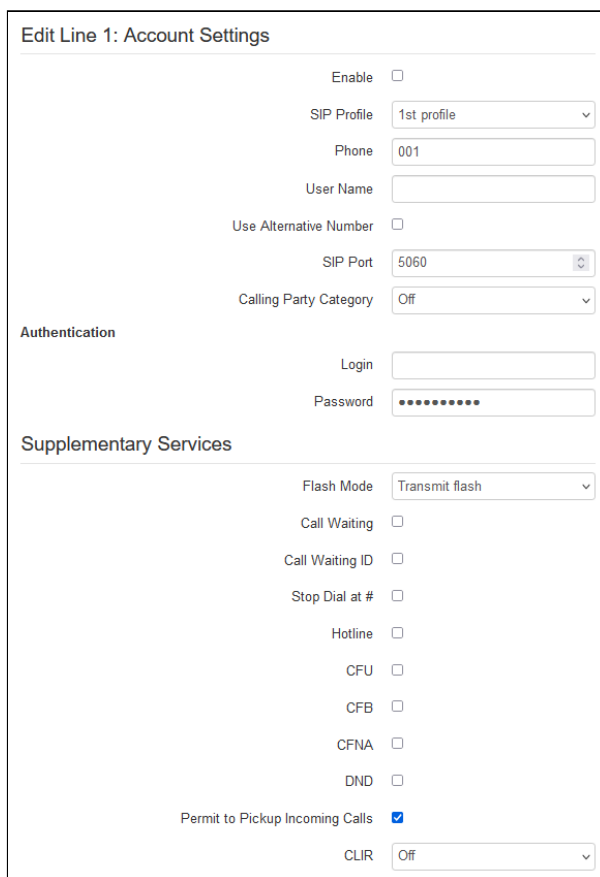
In the "Line settings" submenu, you may configure the phone ports Phone 1–8.



The screenshot shows the 'Line Settings' submenu with a navigation bar at the top containing 'Network', 'VoIP', and 'System'. Below the navigation bar are several sub-menus: 'Network Settings', 'QoS', 'Line Settings' (highlighted), 'SIP Profiles', 'Dialplan Profiles', 'Hunt Groups', 'Pickup Groups', 'Supplementary Service Prefixes', 'Cadence', and 'Call History'. The main content area is titled 'List of Telephone Lines' and contains a table with the following data:

Line	Status	Phone	User Name	Login	SIP Port	SIP Profile
1	Disabled	001			5060	1st profile
2	Disabled	002			5060	1st profile
3	Disabled	003			5060	1st profile
4	Disabled	004			5060	1st profile
5	Disabled	005			5060	1st profile
6	Disabled	006			5060	1st profile
7	Disabled	007			5060	1st profile
8	Disabled	008			5060	1st profile

To edit settings, press the left mouse button on the link with the number of adjustable line and fill the following fields in the appeared "Edit Line" window:



The screenshot shows the 'Edit Line 1: Account Settings' window with the following fields and options:

- Enable:
- SIP Profile: 1st profile (dropdown)
- Phone: 001 (text input)
- User Name: (text input)
- Use Alternative Number:
- SIP Port: 5060 (dropdown)
- Calling Party Category: Off (dropdown)
- Authentication**
 - Login: (text input)
 - Password: (password input)
- Supplementary Services**
 - Flash Mode: Transmit flash (dropdown)
 - Call Waiting:
 - Call Waiting ID:
 - Stop Dial at #:
 - Hotline:
 - CFU:
 - CFB:
 - CFNA:
 - DND:
 - Permit to Pickup Incoming Calls:
 - CLIR: Off (dropdown)

Account Settings

- *Enable* – when checked, port is active;
- *SIP profile* – select SIP profile from the list of available profiles. To configure profiles, use the "VoIP" → "Profiles";
- *Phone* – subscriber number assigned to the phone port;
- *User Name* – user name associated with the port (shown in "Display-Name" field of the "From" header in the outgoing SIP messages);

- *Use Alternative Number* – when checked, an *Alternative Number* will be inserted into the "From" header of SIP messages sent from this port (particularly, in order to hide the real number from the Caller ID system of the callee);
- *Use as a Contact Header* – alternative number assigned to a phone port will be changed to specified number and inserted into "Contact" header of SIP message. The setting is used only for ports located in a call group;
- *SIP Port* – UDP port used to receive incoming SIP messages on the account and to transmit outgoing SIP messages from the account. It may take values from 1 to 65535 (the default value is 5060);
- *Calling Party Category* – enables transmission of outgoing messages in the "From" header; the latter is transmitted in Tel-URI format (see RFC3966);
- *Login and Password* – user name and password used for subscriber authentication on SIP server (and on registration server).

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 Section "Call Transfer";
 - *Unattended calltransfer* – flash will be processed locally by the device (call transfer will be performed when the subscriber finishes dialing a third party number). For the "Unattended calltransfer" detailed operation algorithm see Section "Call Transfer";
 - *Local calltransfer* – call transmission within device, without REFER message sending. For the "Local calltransfer" detailed operation algorithm see Section "Call Transfer".
- *Call transfer mode* – this setting is available for the *Attended calltransfer* and *Local calltransfer* modes only and governs call transfer service activation mode:
 - *Combined* – call transfer is enabled on clearback and pressing R4;
 - *Flash +4* – call transfer is activated on pressing R4;
 - *Flash +4 with callback* – call transfer is activated after pressing R4. When the call is disconnected, the call is ended only with the subscriber who was in contact, with the subscriber on hold a callback is established;
 - *On Release* – the call transfer is activated after the call is released.
- *Call Resumption* – available only for *Attended calltransfer* and *Local calltransfer*, this setting is responsible for the mode of returning to the call with the caller on hold, provided that the oncoming caller is the first to end the call:
 - *Via CallBack* – Call resumption occurs after the call is disconnected via CallBack;
 - *Automatically* – the call with the caller on hold is resumed automatically with the speech path being switched on.
- *Call Waiting* – when checked, "Call waiting" service will be enabled (this service is available in flash – call transfer function operation mode);
- *Call Waiting ID* – when checked, the subscriber number is delivered for the call waiting service;
- *Stop Dial at #* – when checked, use # button on the phone unit to end the dialing, otherwise # will be recognized as a part of the number;
- *Hotline* – when checked, "Hotline" service is enabled. This service allows establishing 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 "Hot Timeout" expiration after the phone handset is picked up (in SIP profile being used, a prefix for this direction should be defined in the dialplan);
 - *Hot timeout, s* – time interval that will be used for connection establishment with the opposite subscriber, in seconds.
- *CFU (Call Forward Unconditional)* – when checked, CFU service is enabled – all incoming calls will be forwarded to the specified call forward unconditional number. When checked, fill in the following fields:

- *CFU Number* – number that all incoming calls will be forwarded to when Call forward unconditional service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan).
- *CFB (Call Forward on Busy)* – when checked, CFB service is enabled – forward the call to the specified number, when the subscriber is busy. When checked, fill in the following fields:
 - *CFB Number* – number that all incoming calls will be forwarded to when the subscriber is busy (in SIP profile being used, a prefix for the specific direction should be defined in the dialplan).
- *CFNA (Call Forward on No Answer)* – when checked, CFNA service is enabled – forward the call when there is no answer from the subscriber. When checked, fill in the following fields:
 - *CFNA Number* – number that incoming calls will be forwarded to when there is no answer from the subscriber and CFNA service is enabled (in SIP profile being used, a prefix for this direction should be defined in the dialplan);
 - *CFNA Timeout, s* – time interval that will be used for call forwarding when there is no answer from the subscriber, in seconds.
- *DND (Do Not Disturb)* – when checked, temporary barring on incoming calls is set. When multiple services are enabled simultaneously, the priority will be as follows (in the descending order):
 - *CFU*;
 - *DND*;
 - *CFB, CFNA*.
- *Permit to Pickup Incoming Calls* – when this option is enabled, incoming calls pickup is enabled for the port (call pickup is allowed only within a single pickup group when ports use the same SIP profile);
- *CLIR* – caller ID service restriction:
 - *Off* – caller ID is disabled;
 - *SIP:From* – anonymous *sip:anonymous@unknown.host* will be sent in the "From" header of SIP messages;
 - *SIP:From* and *SIP>Contact* – anonymous *sip:anonymous@unknown.host* will be sent in the "From" and "Contact" headers of SIP messages.
- *Special Tone* – when flagged, a special station response will be played on this port in case of established local forwardings.

⚠ If "IMS mode" (implicit or explicit) is enabled in the settings of the selected SIP profile, the "Special tone" parameter will be ignored.

Line Parameters

Line Parameters	
Caller ID Generation	Off
Hangup Timeout, s	0
Busy Timeout, s	120
Ringback Timeout, s	0
Minimal On-hook Time, ms	500
Min Flash Time, ms	200
Gain Receive, 0.1 dB	-70
Gain Transmit, 0.1 dB	0
Speaker Voice Level, dB	0
Microphone Voice Level, dB	0
Min Pulse, ms	100
Interdigit, ms	120
Payphone	Off
Network Settings	
DSCP	0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **Caller ID generation** – select the Caller ID mode. For Caller ID operation, subscriber`s phone unit must support the selected method:
 - *Off* – Caller ID is disabled;
 - *FSK V.23, FSK Bell 202* – FSK Caller ID method (using Bell202 standard, or ITU-T V.23). The number is served between the first and second ringing tones by a stream of data with a frequency modulation;
 - *DTMF* – DTMF Caller ID method. The number is served between the first and second ringing tones by double frequency DTMF ringings.
- **Hangup Timeout, s** – dialing timeout for the first digit of a number, in seconds. When there is no dialing during the specified time, busy tone will be sent to the subscriber, and the dialing will end;
- **Busy Timeout, s** – busy tone timeout for the subscriber, in seconds. If the subscriber does not put the phone onhook until the timeout expires, an error tone will be sent into the line;
- **Ringback timeout, s** – launches when an incoming call is received and defines the maximum call response time, in seconds. When the defined timeout expires, busy tone will be sent to the remote subscriber;
- **Minimal On-hook Time, ms** – min clearback detection time, in milliseconds. At that, this parameter represents the maximum flash detection time;
- **Min Flash Time, ms** – min flash detection time, 80–1000 ms;
- **Gain Receive, 0.1dB** – received signal gain (signal transmitted into the phone handset), measurement unit is 0.1dB. The range of values is between -200 and 200dB;
- **Gain Transmit, 0.1dB** – transmitted signal gain (signal received by the phone handset microphone), measurement unit is 0.1dB. The range of values is between -200 and 200dB;
- **Speaker Voice Level, dB** – configuration of voice signal level directed towards a subscriber. The range of values is between -31 and 31 dB;
- **Microphone Voice Level, dB** – configuration of voice signal level directed from a subscriber. The range of values is between -31 and 31dB;
- **Min Pulse, ms** – configuration is required for pulse dialing mode. The range of values is between 10 and 150ms;
- **Interdigit, ms** – configuration is required for pulse dialing mode. The range of values is between 150 and 20000 ms.
- **Payphone** – line settings when the payphone is connected:
 - *Off* – standard mode, the payphone is not connected;

- *Polarity Reversal* – voltage polarity reversal during an outgoing call after a called subscriber's response;
- *12 kHz* – a 12 kHz tariff pulse is delivered to the line every second during an outgoing call;
- *16 kHz* – a 16 kHz tariff pulse is delivered to the line every second during an outgoing call.

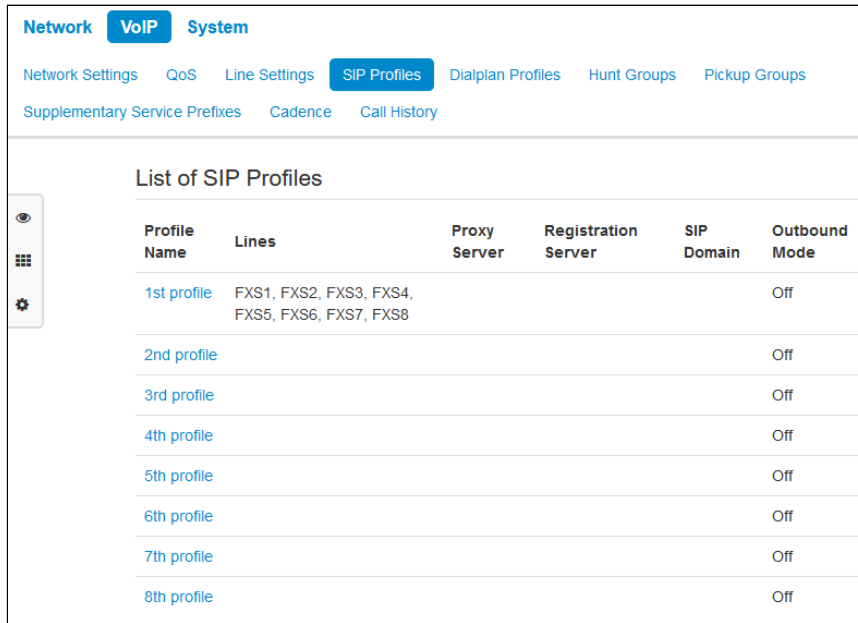
Network Settings

- *DSCP* – DSCP field value of IP packet header for voice traffic from the specified line.

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

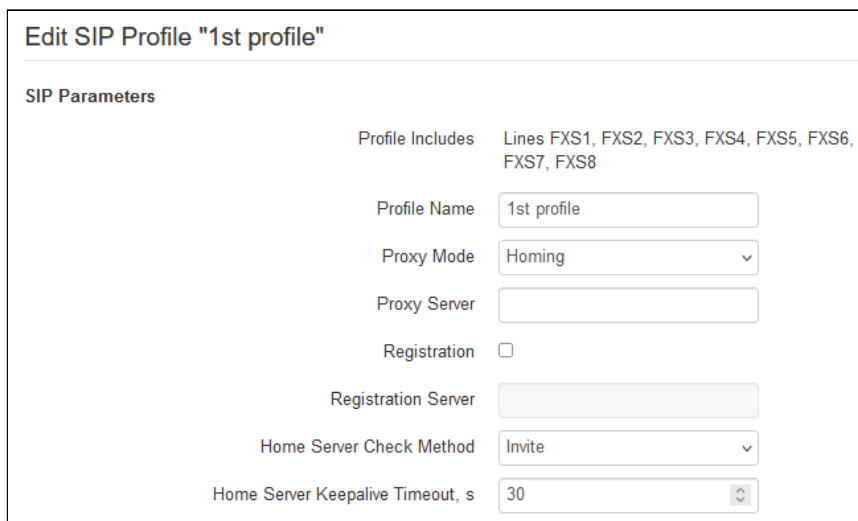
3.6.3.4 "SIP profiles" Submenu

In the "SIP Profiles" submenu, you may configure device SIP profiles. You can assign custom SIP and registration server addresses, voice, fax codecs, individual dialplan and other parameters for every SIP profile. Various SIP profiles usage is needed when various subscriber ports operating via various connection directions (SIP servers). At this time only one SIP profile can be assigned to every subscriber port (configuration in the "VoIP" → "Line Settings" menu).



Profile Name	Lines	Proxy Server	Registration Server	SIP Domain	Outbound Mode
1st profile	FXS1, FXS2, FXS3, FXS4, FXS5, FXS6, FXS7, FXS8				Off
2nd profile					Off
3rd profile					Off
4th profile					Off
5th profile					Off
6th profile					Off
7th profile					Off
8th profile					Off

Left-click the configurable profile link to configure the profile. An "Edit SIP Profile" window will be opened. Fill in the following fields:



Edit SIP Profile "1st profile"

SIP Parameters

Profile Includes Lines FXS1, FXS2, FXS3, FXS4, FXS5, FXS6, FXS7, FXS8

Profile Name

Proxy Mode

Proxy Server

Registration

Registration Server

Home Server Check Method

Home Server Keepalive Timeout, s

SIP Parameters

- *Profile Includes* – list of subscriber ports, which assigned with profile; field is non-editable;
- *Profile Name* – custom name of the configurable profile;
- *Proxy Mode* – select SIP server (SIP-proxy) operation mode form the drop-down list:
 - *Off* – SIP proxy server is not used, all INVITE queries are sent to address, specified after "@" symbol in the dialplan mask entry;
 - *Parking* – SIP proxy redundancy mode without main SIP proxy management;
 - *Homing* – SIP proxy redundancy mode with main SIP proxy management.

The gateway may operate with a single main SIP proxy and up to 4 redundant SIP proxies. For exclusive operation 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 operation 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, or 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:

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

In the "*Homing*" mode, three types of the main SIP proxy management are available: periodic transmission of OPTIONS messages to its address; periodic transmission of REGISTER messages to its address; transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP proxy, and then, if it is unavailable, to the current redundant one, etc. Regardless of the management type, when the main SIP proxy operation is restored, gateway will renew its registration. The gateway starts operation with the main SIP proxy.

- *Proxy Server* – network address of a SIP server – device that manages access to provider`s phone network for all subscribers. You may specify IP address as well as the domain name (specify an alternative SIP server UDP port after the colon (:), default value is 5060);
- *Registration* – when checked, subscriber port registration will be enabled on the registration server;
- *Registration Server* – network address of a device that is used for registration of all phone network subscribers in order to provide them with the communication services (specify registration server port after the colon (:), default value is 5060). You may specify IP address as well as the domain name. Usually, registration server is physically co-located with SIP proxy server (they have the same address);
- *Home Server Check Method* – selecting of the main SIP server availability control method when server is in "*Homing*" mode:
 - *Invite* – control by sending INVITE request to its address when performing outgoing call;
 - *Register* – control by periodic sending REGISTER messages to its address;
 - *Options* – control by periodic sending OPTIONS messages to its address;
- *Home Server Keepalive Timeout, s* – periodic messages sending interval (in seconds), in order to check if the main SIP server is available.

Redundant SIP proxies

Reserved Proxy

Proxy Server	Registration Server
<input type="checkbox"/> <input style="width: 150px;" type="text"/>	<input type="checkbox"/> <input style="width: 150px;" type="text"/>
<input type="button" value="+ Add"/>	<input type="button" value="Remove"/>

SIP Domain

Use Domain to Register

Outbound Mode

Expires

Registration Retry Interval

Public IP Address

Use SIP Display Name in Register

Ringback at 183 Progress

Remove inactive media

User Call

Escape Hash Uri

100rel

Timer Enable

Min SE, s

Session Expires, s

Keepalive NAT Sessions Mode

Use Alert-Info Header

Check RURI User Part Only

Send IP Address in Call-ID Header

Click the "Add" button to add the redundant SIP proxy and execute the following settings:

- *Proxy Server* – redundant SIP server network address. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon (:), default value is 5060);
- *Registration Server* – redundant registration server network address (specify UDP port after the colon (:), default value is 5060). You may specify IP address as well as the domain name. Registration on the redundant server is enabled when "Registration Server" field is selected.

To delete the redundant SIP proxy, select the checkbox next to the respective address and click the button "Remove".

- *SIP Domain* – domain where the device is located (fill in, if required), is assigned automatically when receiving DHCP option 15 or specified manually. A manually specified domain takes precedence over the DHCP configuration;
- *Use Domain to Register* – when selected SIP domain is used for registration (will be inputted in Register query Request-Line);
- *Outbound Mode*:
 - *Off* – route the calls according the dialplan;

- *Outbound* – dialplan is needed for outgoing connection, but all calls will be routed by SIP server; in case of registration absence subscriber will get station reply, to manage subscriber service (Supplementary services management);
- *Outbound with Busy* – dialplan is needed for outgoing connection, but all calls will be routed by SIP server; in case of registration absence VOIP will be unavailable: error tone will be output in the phone.
- *Expires* – time for subscriber port registration on SIP server. Average, port registration renewal is carried out after 2/3 of specified period;
- *Registration Retry Interval* – when the registration is unsuccessful, time period between SIP server registration attempts;
- *Public IP Address* – this parameter is used as device`s external address while working on NAT (on gateway). This parameter is used as a public address of gateway (NAT) WAN interface on which TAU-8N.IP is set up. Wherein it is needed to traverse corresponding SIP and RTP ports, used by device, on the gateway (NAT);
- *Use SIP Display Name in Register* – when selected user name is transmitted in the SIP Display Info field of Register message;
- *Ringback at 183 Progress* – when checked, "ringback" tone will be sent upon receiving "183 Progress" message (without attached SDP);
- *Remove inactive media* – when checked, remove inactive media streams during SDP session modification. Enables interaction with gateways that incorrectly handle rfc3264 recommendation (according to recommendation, the number of streams should not decrease during session modifications);
- *User Call* – preliminary answer, transmitted by the device to caller equipment during incoming call:
 - *180 Ringing* – 180 reply is sent to caller equipment; caller equipment should output local ringback tone in line after getting this message;
 - *183 Progress with SDP* - 183+SDP reply is sent to caller equipment; used for frequency path forwarding to callee reply. In this case TAU-8N.IP will remote send ringback tone to caller.
- *Escape Hash Uri* – when checked, pass the pound key in SIP URI as an escape sequence "%23", otherwise as "#" symbol.
- *100rel* – utilization of reliable provisional responses (RFC3262):
 - *Supported* – reliable provisional responses are supported;
 - *Required* – reliable provisional responses are mandatory;
 - *Off* – reliable provisional responses are disabled.

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

Setting operation for outgoing communications:

Supported – send the following tag in "INVITE" request – supported: 100rel. In this case, communicating gateway may transfer provisional responses reliably or unreliably – as it deems fit;

Required – send the following tags in "INVITE" request – supported: 100rel and required: 100rel. In this case, communicating gateway should perform reliable transfer of provisional replies. If communicating gateway does not support reliable provisional responses, it should reject the request with message 420 and provide the following tag – unsupported: 100rel. In this case, the second INVITE request will be sent without the following tag – required: 100rel;

Off – do not send any of the following tags in "INVITE" request – supported: 100rel and required: 100rel. In this case, the interacting gateway will transmit preliminary responses unreliably.

Setting operation for incoming communications:

Supported, Required – when the following tag is received in "INVITE" request – supported: 100rel, or required: 100rel, perform reliable transfer of provisional replies. If there is no supported: 100rel tag in INVITE request, the gateway will perform unreliable transfer of provisional replies;

Off – when the following tag is received in "INVITE" request – required: 100rel, reject the request with message 420 and provide the following tag – unsupported: 100rel. Otherwise, perform unreliable transfer of provisional replies.

- *Timer Enable* – when checked, support of SIP session timer (RFC 4028) is enabled. After connection establishment, if both sides support timer, one of them periodically sends re-INVITE queries for connection control (if both sides support UPDATE method (it should be pointed in "Allow" header) session update is being processed by periodical UPDATE messages sending);
- *Min SE, s* – minimal time interval for connection health checks (90 to 1800 s, 120 s by default);
- *Session Expires, s* – period of time in seconds that should pass before the forced session termination, if the session is not renewed in time (90 to 80000 s, recommended value – 1800 s, 0 – unlimited session);
- *Keepalive NAT Sessions Mode* – SIP server poll method selecting:
 - *Off* – SIP server is not polling;
 - *Options* – SIP server poll, with OPTIONS messages;
 - *Notify* – SIP server poll, with NOTIFY messages;
 - *CLRF* – SIP server poll with empty UDP packet.
- *Keepalive timeout, s* – time interval in seconds, after which SIP server poll is processing;
- *Use Alert-Info Header* – process INVITE request "Alert-Info" header to send a non-standard ringing to the subscriber port.
- *Check RURI User Part Only* – when checked, only subscriber number (user) will be analyzed, and if the number matches, the call will be assigned to the subscriber port. If unchecked, all URI elements (user, host and port – subscriber number, IP address and UDP/TCP port) will be analyzed upon receiving an incoming call. If all URI elements match, the call will be assigned to the subscriber port.
- *Send IP Address in Call-ID Header* – when checked, Call-ID header use local device IP address in *localid@host* format when outgoing connection is processing.

Three-party Conference:

- *Mode* – 3-way conference operation mode. Two modes are available:
 - *Local* – conference is gathered locally by the device after pressing «flash+3» combination;
 - *Remote (RFC4579)* – conference is gathered on remote server. Then, after pressing "flash+3" combination Invite message is sent on server to number, pointed in the "Conference Server" In this case conference is processed by algorithm, described in RFC4579. For detailed description see Section "[Remote Conference](#)".
- *Conference Server* – conference connection establishment server address processed by algorithm, described in RFC4579. Address is set in SIP-URI format: *user@address:port*. It is available to set only user part URI, in this case Invite message will be sent to SIP proxy address.

IMS Configuration

- *IMS mode* – mode of operation with IMS. Three modes are possible:
 - *Disabled* – IMS is not in use;
 - *Unsubscribed* – some types of services are allowed to be managed from the IMS (IP Multimedia Subsystem) server. In this case activation of "Three-way Conference" (works only according to RFC4579 algorithm), "Call Hold", "Call Waiting", "Hotline", "Call Transfer" services (regardless of whether they are enabled or not in the configuration) is performed remotely by the IMS server by sending Notify messages, in the body of which commands for activation/deactivation of services in XCAP format (actually – XML, RFC4825) are transmitted. In this case SUBSCRIBE requests are not sent by the gateway after subscriber registration, only NOTIFY-requests received from the IMS, by means of which the services are managed, are processed;
 - *With subscription* – some types of services are allowed to be managed from the IMS (IP Multimedia Subsystem) server. In this case, activation of "Three-Way Conference" (works only according to RFC4579 algorithm), "Call Hold", "Call Waiting", "Hotline", "Call Transfer" services (regardless of whether they are enabled or not in the configuration) is performed remotely by the IMS server through sending messages to the dispatcher. Call Transfer" (regardless of whether they are enabled or not in the configuration) is performed remotely by the IMS server by sending Notify messages, in the body of which commands for activation/deactivation of services in XCAP format (actually – XML, RFC4825) are sent. In this case, the gateway sends SUBSCRIBE requests after subscriber registration and, upon successful subscription, processes NOTIFY requests received from the IMS, through which services are managed.
- *Call Hold service name* is the name of the XML element in the body of the Notify message used to send the activation/deactivation command for the Call Hold service. For example, if the service name is "call-hold", the activation command will look the following way:


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

 and the deactivation command:


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

- The name of the Call Waiting service is the name of the XML element in the body of the Notify message used to send the activation/deactivation command for the Call Waiting service. For example, if the service name has the value *"call-waiting"*, the activation command will look the following way: `<call-waiting active="true"/>`

and the deactivation command:

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

- "Three-party conference" service name is the name of the XML element in the body of the Notify message used to send the activation/deactivation command for the "Three-party conference" service. For example, if the service name has the value *"three-party-conference"*, the activation command will look the following way: `<three-party-conference active="true"/>`

- and the deactivation command:

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

- Hotline service name - the name of the XML element in the body of the Notify message used to send the activation command for the Hotline service. In the activation command, the hotline phone number and the call timeout are transmitted. For example, if the service name has the value *"hot-line-service"* and it is necessary to make a call to the number 30001 in 6 seconds after lifting the handset - the activation command will look the following way:

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

If the activation command is not received, the Hotline service will be deactivated.

- Call-transfer service name is the name of the XML element in the body of the Notify message used to send the activation/deactivation command for the Call-transfer service. For example, if the service name is *"call-transfer"*, the activation command will look the following way:

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

- and the deactivation command:

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

By default, if no activation command is received - all the above services are deactivated.

Dialplan

Dialplan	
Dialplan Configuration	S5, L5 ([xABCD*#].S)
Voice Codecs Configuration	
Codec 1	G.711a
Codec 2	G.711u
Codec 3	G.723.1
Codec 4	G.729
Codec 5	Off
G.711 Packet Time, ms	20
G.723.1 Packet Time, ms	30
G.729 Packet Time, ms	20

Dialplan is set with regular expressions in the "Dialplan Configuration" field.

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

Regular expression structure:

Sxx, Lxx (),

where:

xx – random values of S and L timers;

() – dialplan limits.

The basis is the designations for recording a sequence of dialed digits. Dialed digits sequence is recorded using several designations: digits, dialed by phone keyboard: 0, 1, 2, 3, ..., 9, # and *.

⚠ Symbol "#" in dialplan can block end of dial by this key!

- Digit sequence enclosed in square brackets corresponds to any of the characters enclosed in brackets, for example:
 - ([1239]) – corresponds to any of this digits: 1, 2, 3 or 9.
- Symbol range may be set through the hyphen. It is most often used inside square brackets, for example:
 - (1-5) – any digit from 1 to 5;
 - ([1-39]) – example from previous paragraph with other record format. Corresponds to any of this digits: 1, 2, 3 or 9.
- Symbol "X" corresponds to any digit from 0 to 9, for example:
 - (1XX) – any three-digit number, starting at 1.
- "." – previous symbol repeating from 0 to infinite number of times, for example: (810X.) – international number with any digits amount;
- "+ – previous symbol repeating from 1 to infinite number of times;
- {a,b} – previous symbol repeating from "a" to "b" times;
- {a,} – previous symbol repeating equal to or more than "a" times;
- {b} – previous symbol repeating equal to "b" times;
- {,b} – previous symbol repeating equal to or less than "b" times;
- {,b} – previous symbol repeating less than "b" times;
 - (810X.) – international number with any digits amount.

Settings that affect dialplan processing:

- *Interdigit Long Timer ("L" digit in dialplan entry)* – entry timeout for the next digit, if there are no templates that correspond to the dialed combination;
- *Interdigit Short Timer ("S" digit in dialplan entry)* – 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 replacing the dialed sequence to any dialed symbols sequence. In doing so, the second argument should be set as a defined value, both arguments can be empty

- Example: (<83812:> XXXXXX) – this record will comply to dialed digits 83812, but this sequence will be omitted and will not be transmitted to SIP server.

2. Tone insert into dial

For long-distance access (for city access in case of office PBX), it is possible to send "PBX response" tone after certain digits entry. The signal will be sent after those digits in the mask line of which there is a comma after these digits

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

3. Number dialing deny

If you add symbol "!" at the end of pattern, the dialing of numbers corresponding to the pattern will be blocked.

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

4. Replacement of number dialing timer`s values

Timer values may be specified for a complete dialplan, as well as for the specific pattern. Character "S" stands for "Interdigit Short Timer" setting and "L" for "Interdigit Long Timer". Timer values can be specified for all patterns in the dialplan if the values are listed before the opening parenthesis.

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

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

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

5. Dialing by direct address (IP Dialing)

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

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

- Example 1: (8 xxx xxxxxxx) is an 11-digit number starting at 8.
- Example 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) is an 11-digit number starting at 8 if entered 7-digit, then add to the transmitted number 8495.
- Example 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) – a set of emergency numbers, as well as some long-distance number.
- Example 4: (S0 <:82125551234>) is a specified number speed dial, "Hotline" mode analogue on another gateway.

- Example 5: (S5 <:1000> | xxxx) – this dialplan allows to dial any number, that consists of digits, and if nothing input during 5 seconds call number 1000 (e.g. receptionist).
- 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 it is needed to perform calls locally within the device. In so doing, if device IP address is unknown or periodically changing, it is convenient to use reserved "{local}" word as server address; it means that device will transmit related number sequence to own device address.

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

6. Configuration of pickup codes

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

Syntax: ABC@{pickup:X}, where

ABC – pickup code (e.g. *8),

X – pickup group number (pickup group enumeration from 0).

- Example: 112@{pickup:0} – subscribers A and B belong to one pickup group with index 0. If subscriber A receives an incoming call, subscriber B can pickup the call by dialing digit combination 112.

Voice Codecs Configuration

Dialplan	
Dialplan Configuration	S5, L5 ([xABCD*#].S)
Voice Codecs Configuration	
Codec 1	G.711a
Codec 2	G.711u
Codec 3	G.723.1
Codec 4	G.729
Codec 5	Off
G.711 Packet Time, ms	20
G.723.1 Packet Time, ms	30
G.729 Packet Time, ms	20

Devices signal processor encodes analogue voice traffic and fax data into digital signal and performs its reverse decoding. The gateway supports the following voice codecs: G.711A, G.711U, G.729, G.723.1.

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

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

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

G.726-16, G.726-24, G.726-32, G.726-40 – codecs with voice data compression according to the ADIKM algorithm and a transfer rate of 16, 24, 32 or 40 kbps, which have a standard byte storage order (G726) –little endian, and the alternative (AAL2-G726) is big endian.

- *Codec 1..7* – allows you to select codecs and the order in which they will be used. Codec with the highest priority should be placed in "*Codec 1*" field. For operation, you should specify at least one codec:
 - *Off* – the codec is not used;
 - *G.711a* – use G.711a codec;
 - *G.711u* – use G.711u codec;
 - *G.723.1* – use G codec.723.1;
 - *G.729* – use G.729 codec;
 - *G.729a* – use G.729a codec;
 - *G.729b* – use G.729b codec.
 - *G.726-16* – use G.726-16 codec;
 - *G.726-24* – use G.726-24 codec;
 - *G.726-32* – use G.726-32 codec;
 - *G.726-40* – use G.726-40 codec;
 - *AAL2-G.726-16* – use AAL2-G.726-16 codec;
 - *AAL2-G.726-24* – use AAL2-G.726-24 codec;

- AAL2-G.726-32 – use AAL2-G.726-32 codec;
- AAL2-G.726-40 – use AAL2-G.726-40 codec.
- *Packet Time, ms* – the amount of voice data in milliseconds (ms), transmitted in a single RTP protocol voice packet.

⚠ Alternative voice codecs can be set for the selected direction. There is ability of preferred codec setting for voice transmission for every direction in dialplan. Configuration is made in dialplan. Additional codec settings are indicated in parentheses after the word «codecs:» for every direction.

If it is necessary to use several codecs, they must be listed with symbol "," between them. It is possible to set several parameters for direction. In this case they must be divided by symbol ";" – (param1:subparam1,subparam2;param2:subparam1,subparam2). Acceptable values of subparamX subparameters: g711a, g711u, g729, g723.

Allowed subparameters values: param1 – codecs; param2 – rfc2833_PT.

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

Jitter Buffer

Jitter Buffer	
Min Delay, ms	40
Max Delay, ms	130
Deletion Threshold (DT)	500
Jitter Factor	7

Jitter is the irregularity of the time periods allowed for packet delivery. The delay in packet delivery and jitter is calculated in milliseconds. Jitter is of great importance when transmitting real-time information (e.g. voice or video).

In the RTP protocol, also called the "media stream protocol", there is a field to mark the exact time of transmission relative to the entire RTP stream. According to this information, the receiving party clarifies how parameters should be set to mask potential network problems, such as delays and jitter. If expected time for packet delivery from sender to receiver during whole call is strictly equal to definite value (e.g. 50 ms) we can approve that this network contains no jitter. But often packets are delayed in the network and delivery time interval could fluctuate in a fairly large (in terms of critical to time traffic) time range. If application-receiver of this sound or video will playback it in time order in which the packets are coming, we will get noticeable voice (or video) quality degradation. Example: when it comes to voice – we will hear voice interruption and other interference.

The device has the following jitter buffer settings:

- *Min Delay, ms* – minimum expected time of IP packet spread through network;
- *Max Delay, ms* – maximum expected time of IP packet spread through network;
- *Deletion Threshold (DT)* – maximum time interval through which deleting of voice packets from buffer id processing. The parameter value is greater than or equal to maximum delay;
- *Jitter Factor* – parameter, used for jitter buffer size optimization. It is recommended to set its value to 0.

Fax and modem transmission

Fax Transfer	
Fax Codec 1	G.711a
Fax Codec 2	G.711u
Fax Codec 3	Off
Fax Detect Direction	Caller and Callee
Take the Transition to T.38	<input type="checkbox"/>

- *Modem Transmission* – selection of the codec to be used for data transmission when modem signals are detected by the gateway:
 - *G.711a VBD* – use G.711a codec in VBD mode;
 - *G.711u VBD* – use G.711u codec in VBD mode;
 - *G.711a VBD+EC* – use G.711a codec in VBD+EC mode.
 - *G.711u VBD+EC* – use G.711u codec in VBD+EC mode;
 - *G.711a RFC3108* – RFC3108 support, G.711A codec is used when transmitting data over a modem connection;
 - *G.711u RFC3108* – RFC3108 support, G.711U codec is used when transmitting data over a modem connection;
 - *Disabled* – do not detect modem signals.

In VBD (Voice Band Data) mode, the gateway turns off the Voice Activity Detector (VAD), Comfort Noise Generator (CNG) and echo compensators, which is necessary when establishing a modem connection.

⚠ The difference between VBD+EC mode and VBD mode is the formation of SDP:

For VBD+EC mode:

a=gpmde:8 vbd=yes;ecan=off

For VBD mode:

a=gpmde:8 vbd=yes

⚠ The selected codec must also be active in the list of voice codecs.

Fax transfer may be carried out using G.711A and G.711U voice codecs or a special codec for T.38 messages transmission.

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

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

⚠ The selected codec must also be active in the list of voice codecs.

- *Fax Codec 1..3* – allows you to select codecs and an order of their usage. Codec with the highest priority should be placed in "Fax Codec 1" field. For operation, you should specify at least one codec:
 - *Off* – the 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 must be different! In addition, when choosing G.711a or G.711u the selected codec must also be active in the list of voice codecs.

- *Fax Detect Direction* – defines the call direction for fax tone detection and subsequent switching to fax codec:
 - *No Detect Fax* – disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite gateway);
 - Both sides are CED signaling detection for both incoming and outgoing calls;
 - *Calling* – detecting CED signals only on an outgoing call;
 - *Called* – detecting CED tones only when there is an incoming call.
- *Take the Transition to T.38* – when checked, incoming re-invite to T.38 from oncoming gateway is allowed;
- *T.38 Redundancy Count* – adding the redundancy into T.38 packets; value is corresponding to amount of previous packets, which is doubling in every new T.38 packet. This redundancy method is intended for case when the packets are lost in the transfer.

Additional Parameters

Additional Parameters

DTMF Transfer RFC 2833

Flash Transfer SIP Info (Hookflash)

RFC2833 Payload Type 96

Echocanceller Simple

Use the Same PT Both for Transmission and Reception

Silencedetector

RTCP

Dispersion Time, ms 125

SRTCP

- *DTMF Transfer* – DTMF tone transmission method:
 - *Inband* – inband transmission;
 - *RFC 2833* – according to RFC2833 recommendations, as a dedicated load in RTP voice packets;
 - *SIP Info* – transmission of the messages via SIP in INFO queries.
- *Flash Transfer* – flash transfer type:
 - *SIP Info (Hookflash)* – transmission of the messages to the interoperable side via SIP in INFO queries. Flash event is sent in Application/Hook Flash extension as "signal=hf";
 - *SIP Info (DTMF Relay)* – transmission of the messages to the interoperable side via SIP in INFO queries. Flash event is sent in Application/dtmf-relay as "signal=hf";
 - *SIP Info (Broadsoft)* – transmission of the messages to the interoperable side via SIP in INFO queries. Flash event is sent in Application/Broadsoft extension as "event flashhook";
 - *SIP Info (SSCC)* – transmission of the messages to the interoperable side via SIP in INFO queries. Flash event is sent in Application/sscc extension as "event flashhook".

⚠ In current firmware version Flash transmit is available only via SIP.

- *RFC2833 Payload Type* – payload type for packets transmission via RFC2833 (permitted values: 96 to 127);
- *Echocanceller* – determines the mode of using echo cancellation (*Simple, Speex and WebRTC*);
- *Use the Same PT Both for Transmission and Reception* – option is intended for alignment of events, transmitted via RFC2833 (DTMF and Flash) when outgoing call is processing. When checked, transmission and reception of events via RFC2833 is processing with payload from received by oncoming side of message 200Ok. When unchecked transmission of events via RFC2833 is processing with payload from received 200Ok, reception – with payload type from its own configuration (sets in outgoing Invite);
- *Silencedetector* – use silence detector when enabled;
- *RTCP* – when checked, use RTCP for voice channel control:
 - *Sending Interval* – RTCP packets sending interval, sec;
 - *Receiving Period* – RTCP message receiving period is measured in sending interval units; if receiving period expires and there is no any RTCP packet received from oncoming side – TAU-8N.IP cuts the connection off;
 - *RTCP-XR* – when checked, sending "RTCP Extended Reports" control packets according to RFC 3611.

- *Dispersion Time, ms* – parameter, that allows to deal with echo, caused by voice signal dispersion. The parameter values are changing in the range from 2 to 128 ms;
- *SRTP* – when checked, RTP stream encryption will be used. In this case the RTP/SAVP profile will be specified in the SDP of outgoing INVITE requests. Also, an RTP/SAVP profile will be searched in the SDP of incoming requests. If RTP/SAVP-profile is not found, the call will be rejected;
- *Crypto Suite 1-2* – allows you to select the encryption and hashing algorithms to be used. The crypto suite with the highest priority must be registered in the field "*Crypto Suite 1*". For operation, you should specify at least one crypto suite:
 - *AES_80* – corresponds to AES_CM_128_HMAC_SHA1_80;
 - *AES_32* – corresponds to AES_CM_128_HMAC_SHA1_32.

To save the changes click the "Save" button. To discard changes, click the button "Cancel".

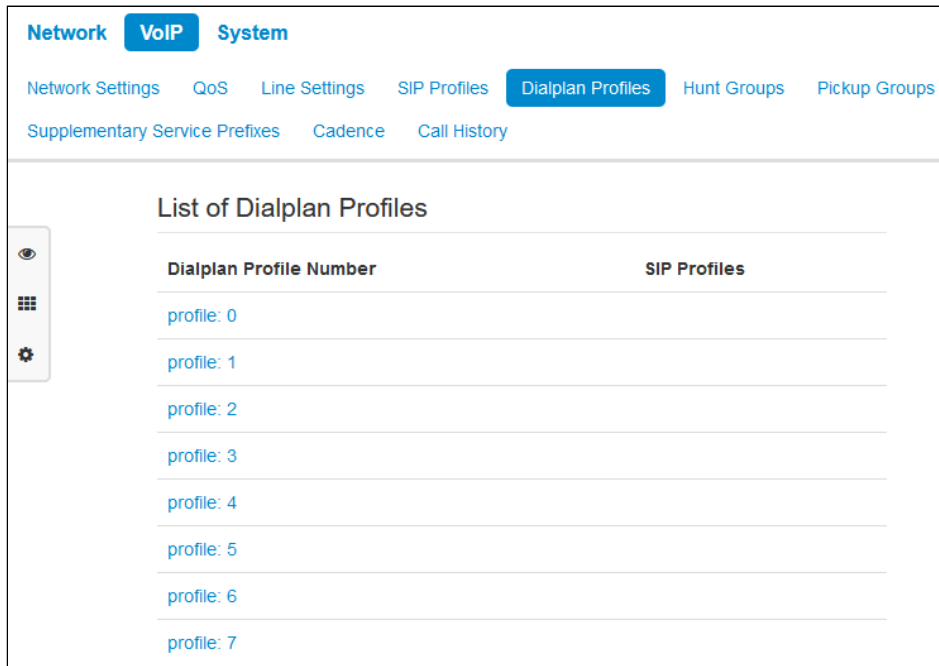
SIP Profile Common Settings

- *STUN Enable* – when checked, STUN protocol (Session Traversal Utilities for NAT) is used to identify device public address (external NAT address). It is recommended to use this protocol when the device is operating via NAT;
- *STUN Server Address* – STUN server or domain name of IP address, specify an alternative server port after the colon (default value is 3478);
- *STUN Request Sending Interval, s* – interval, after which sending the request to the STUN server. The fewer request interval the higher reaction to public address change.
 - *Timer T1, ms* – time interval between first and second INVITEs, when there is no response to the first one, in ms; the interval will be doubled for subsequent INVITEs (third, fourth, etc.) (e.g. for 300 ms, the second INVITE will be sent in 300 ms, the third is in 600 ms, the fourth is in 1200 ms, etc.);
 - *Timer T2, ms* – maximum time interval for retransmission of non-INVITE requests and replies to INVITE requests;
 - *Timer B, ms* – total timeout for INVITE message transmission, in milliseconds. When this timeout expires, the direction is deemed to be unavailable. Allows to limit INVITE message retransmission, including messages used for availability identification.
- *Transport* – selecting the protocol for SIP messages transportation;
- *Tones Specification* – selecting the country for specification used tone set.

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

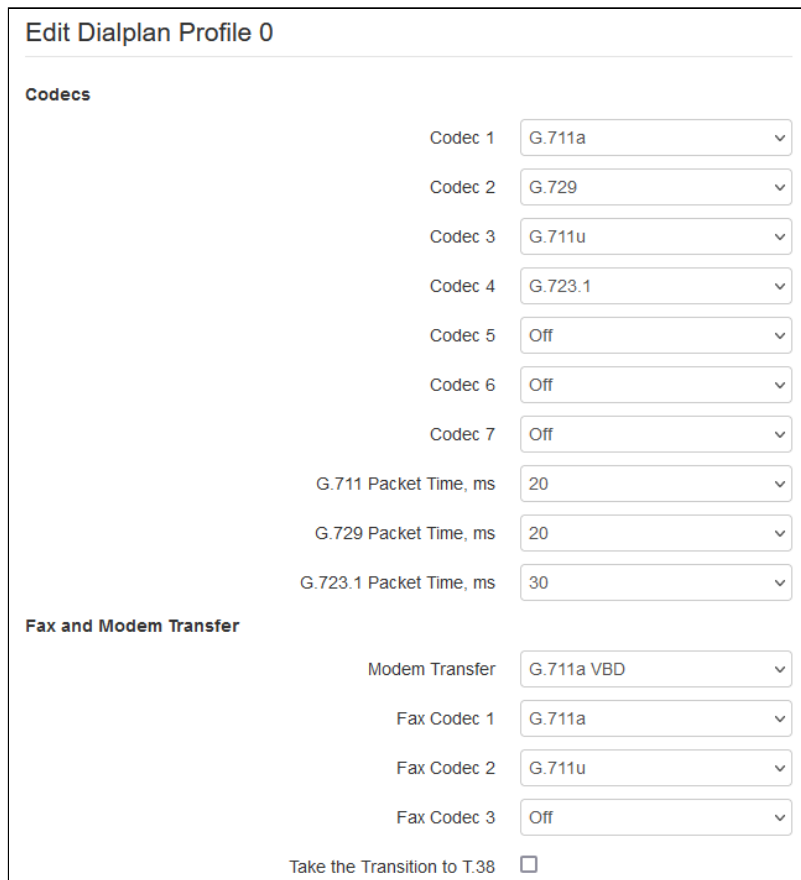
3.6.3.5 "Dialplan Profiles" Submenu

In this submenu you can set call profiles for using in different directions.



You can configure up to 8 dialplan profiles.

Edit Dialplan Profile



Codecs:

- *Codec 1...7* – enables you to select codecs and an order of their usage. Codec with the highest priority should be placed in "Codec 1" field. For operation, you should specify at least one codec:
 - *Off* – the codec is not used;
 - *G.711a* – use G.711a codec;
 - *G.711u* – use G.711u codec;
 - *G.723.1* – use G.723.1 codec;
 - *G.729* – use G.729 codec;
 - *G.729a* – use G.729a codec;
 - *G.729b* – use G.729b codec;
 - *G.726-16* – use G.726-16 codec;
 - *G.726-24* – use G.726-24 codec;
 - *G.726-32* – use G.726-32 codec;
 - *G.726-40* – use G.726-40 codec;
 - *AAL2-G.726-16* – use AAL2-G.726-16 codec;
 - *AAL2-G.726-24* – use AAL2-G.726-24 codec;
 - *AAL2-G.726-32* – use AAL2-G.726-32 codec;
 - *AAL2-G.726-40* – use AAL2-G.726-40 codec.
- *Packet Time* – voice milliseconds amount in one RTP packet (for codecs G.711a, G.711u, G.729, G.723.1).

Fax and Modem Transfer:

- *Modem Transfer* – selection of the codec, that will be used for data transmission when modem signals detecting by the gateway:
 - *G.711a VBD* – use G.711a codec in VBD mode;
 - *G.711u VBD* – use G.711u codec in VBD mode;
 - *G.711a VBD+EC* – use G.711a codec in VBD+EC mode;
 - *G.711u VBD+EC* – use G.711u codec in VBD+EC mode;
 - *G.711a RFC3108* – RFC3108 support, G.711A codec is used for data transmission via modem connection;
 - *G.711u RFC3108* – RFC3108 support, G.711U codec is used for data transmission via modem connection;
 - *Off* – disable modem signal detection.

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

⚠ The difference between VBD+EC mode and VBD mode is the formation of SDP:

For VBD+EC mode:

a=gpmde:8 vbd=yes;ecan=off

For VBD mode:

a=gpmde:8 vbd=yes

⚠ The selected codec must also be active in the list of voice codecs.

- *Fax Codec 1...3* – allows you to select codecs and an order of their usage. Codec with the highest priority should be placed in "Fax Codec 1" field. For operation, you should specify at least one codec:
 - *Off* – the 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 must be different! In addition, when choosing G.711a or G.711u the selected codec must also be active in the list of voice codecs.

- *Take the Transition to T.38* – when checked, incoming re-invite to T.38 from oncoming gateway is allowed;
- *38 Redundancy Count* – adding the redundancy into T.38 packets; value is corresponding to amount of previous packets, which is doubling in every new T.38 packet. This redundancy method is necessary in case of packet loss during transmission.

Additional Parameters:

Additional Parameters	
DTMF Transfer	RFC 2833
RFC2833 Payload Type	96
Echocanceller	Simple
Silencedetector	<input checked="" type="checkbox"/>
Dispersion Time, ms	125
Max Call Number	12

- *DTMF Transfer* – DTMF tone transmission method:
- *Inband* – inband transmission;
- *RFC 2833* – according to RFC2833 recommendations, as a dedicated load in RTP voice packets;
- *SIP Info* – transmission of the messages via SIP in INFO queries.
- *RFC2833 Payload Type* – payload type for packets transmission via RFC2833 (permitted values: 96 to 127);
- *Echocanceller* – determines the mode of using echo cancellation (*Off, Speex, Simple and WebRTC*);
- *Silencedetector* – use silence detector when enabled;
- *Dispersion Time, ms* – parameter, that allows to deal with echo, caused by voice signal dispersion. The parameter values are changing in the range from 2 to 128 ms;
- *Max Call Number* – this parameter allows to restrict simultaneous calls on one direction amount.

Jitter Buffer:

- *Min Delay, ms* – minimum expected time of IP packet spread through network;
- *Max Delay, ms* – maximum expected time of IP packet spread through network;
- *Jitter Factor* – parameter, used for jitter buffer size optimization. It is recommended to set its value to 0.
- *Deletion Threshold (DT)* – max time interval through which deleting of voice packets from buffer id processing. The parameter value is greater than or equal to max delay (permitted values from 0 to 500, but at least max jitter buffer value);
- *Use the Same PT Both for Transmission and Reception* – when checked, use the same payload type for Rx and Tx;
- *Rx AGC* – when checked, a received signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise – the amplification will not be carried out;
- *Rx AGC Level* – determines the value of the level to which an analogue signal will be amplified when receiving (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB);

- *Tx AGC* – when checked, a transmitted signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise – the amplification will not be carried out;
- *Tx AGC Level* – determines the value of the level to which an analogue signal will be amplified when transmitting (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).

Jitter Buffer

Min Delay, ms

Max Delay, ms

Jitter Factor

Deletion Threshold (DT)

Use the Same PT Both for Transmission and Reception

Rx AGC

Rx AGC Level -25 dB

Tx AGC

Tx AGC Level -25 dB

To save the changes click the "Apply" button. To discard changes, click the "Cancel" button.

3.6.3.6 "Hunt Groups" Submenu

In the "Hunt groups" submenu you can control hunt groups.

Hunt groups allow to perform call center features. The device supports 3 call group modes:

- *Group* – in the group mode, the call comes in to all free ports of the group simultaneously. When one of the group members answers, call transmission to other ports stops.
- *Cyclic* – in the cyclic mode, the gateway after timeout (*Next Port Calling Timeout, s*) continuously searches for a free group member, and the call is transferred to their number.
- *Serial* – in the serial group mode, the call comes in to the first free port in the group list, and then, after the specific time interval (Timeout of next port call), the next free port in the list will be added to the main one, etc. When one of the group members answers, call transmission to other ports stops.

Network **VoIP** **System**

Network Settings QoS Line Settings SIP Profiles Dialplan Profiles **Hunt Groups** Pickup Groups

Supplementary Service Prefixes Cadence Call History

Hunt Groups

Group Name	Status	SIP Profile	Phone	List of the Ports
Group1	✘	1st profile		

- *Group Name* – the name of the hunt group.
- *Status* – the status of the hunt group: enabled/ disabled;
- *SIP Profile* – SIP profile, used by the hunt group;
- *Phone* – hunt group phone number;
- *List of the Ports* – line (ports) list, that includes hunt group.

To configure the hunt group, click on the corresponding link in the "Group Name" column.

Edit Group

Enable

SIP Profile

Group Name

Phone

Username

Password

SIP Port

Group Type

Call Queue Size, s

Call Reply Timeout, s

Group Call Pickup Enable

List of the Ports

Line FXS1	<input checked="" type="checkbox"/>
Line FXS2	<input checked="" type="checkbox"/>
Line FXS3	<input checked="" type="checkbox"/>
Line FXS4	<input checked="" type="checkbox"/>
Line FXS5	<input type="checkbox"/>
Line FXS6	<input type="checkbox"/>
Line FXS7	<input type="checkbox"/>
Line FXS8	<input type="checkbox"/>

- *Enable* – use the group when checked;
- *SIP Profile* – SIP profile, assigned to hunt group. Profile settings are performed in the section "VoIP → SIP Profiles";
- *Group Name* – identification name of the group;
- *Phone* – hunt group phone number;
- *Username* – user name for authentication on SIP server;
- *Password* – password for authentication on SIP server;
- *SIP Port* – alternative SIP port for group (default is 5060);
- *Group Type* – the type of the hunt group:
 - *Group* – the call comes in to all free ports of the group simultaneously;
 - *Serial* – the number of ports to which the call signal comes in increases by one after the next port call timeout expires;
 - *Cyclic* – the call signal comes in to each port in the group in turn after an interval equal to the Next Port Calling Timeout. When last port in group is reached, ring-round continues from the first port;
- *Next Port Calling Timeout, s* – is used by "Serial" and "Cyclic" type groups and set time interval in seconds after which next port(s) are called;
- *Call Queue Size, s* – allows to restrict max missed calls amount in call group queue. Received call is not set in queue if there are free ports in group;

- *Call Reply Timeout, s* – if there will be no answer to hunt call, the call resets after this time interval;
- *Group Call Pickup Enable* – when checked, group call pickup is allowed. Call pickup is possible only if call group subscribers belong to one pickup group (see "[Pickup Groups](#)" Submenu).

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

3.6.3.7 "Pickup Groups" Submenu

The "Pickup Groups" submenu is intended for call pickup groups configuration.

Pickup Group – subscriber group, authorized to receive (or pickup) any calls directed at another subscriber of the group. i.e. each subscriber that belongs to the group will be able to pickup the call received on any other port of this group by dialing a pickup code. Pickup code configuration is carried out in the "Dialplan" point in the "SIP Profiles" submenu.

	Line 1	Line 2	Line 3	Line 4	Line 5	Line 6	Line 7	Line 8
Group 1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Group 8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

To add/delete the line in group check/uncheck this group.

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

Service usage:

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

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

Pickup group may be used in combination with a hunt group; in this case, all ports that belong to a hunt group should belong to the pickup group as well. In this case, each port that belong to a pickup 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 or phone port, they will hear "busy" tone.

3.6.3.8 "Supplementary Service Prefixes" Submenu

In the "Supplementary Service Prefixes" submenu codes dialed from the telephone set are configured to activate or deactivate supplementary services.

Subscribers can manage the status of supplementary services from their telephone set. The following options are available:

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

To activate "Call Forward Unconditional" (CFU), "Call Forward on Busy" (CFB), "Call Forward on No Answer" (CFNA), "Hotline/Warmline" services you should enter the phone number:

- service_code * phone_number #

After service activation or deactivating code entry subscriber will hear a "Confirmation" tone (3 short tones), that means that service is successfully activated or deactivated.

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

Supplementary Services	Activation Code	Deactivation Code	Check Code
CFU	* 00 #	#00#	*#00#
CFB	* #	-	-
CFNA	* #	-	-
Permit to Pickup Incoming Calls	* #	-	-
Hotline	* #	-	-
Call Waiting	* #	-	-
DND	* #	-	-

Subscriber service management

- *Supplementary Services* – list of supplementary services:
- *CFU* – forwards all subscriber`s incoming calls to specified number;
- *CFB* – forwards all subscriber`s incoming calls to specified number when they are busy;
- *CFNA* – forwards all subscriber`s incoming calls to specified number after specified time if subscriber does not reply;
- *Permit to Pickup Incoming Calls* – all incoming to subscriber calls can be picked up by other subscribers from this pickup group;
- *Hotline* – a specified number is automatically dialed in set interval after lifting the handset;

- *Call Waiting* – allows subscriber to get the notification about new incoming call in call state. Subscriber can accept, decline or ignore the waiting call;
- *DND (Do Not Disturb)* – allows subscriber to temporarily restrict all incoming calls.
- *Activation Code* – code for service activation;
- *Deactivation Code* – code for service deactivation;
- *Check Code* – code for service activity control;

Deactivation and check codes filled automatically based on activation code.

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

3.6.3.9 "Cadence" Submenu

In the "Cadence" submenu you can set alternative cadence signal according to Alert-Info header in incoming Invite. Cadence value for each call signal is represented by sequence of interchangeable pulses and pauses delimited by ";" or ",". Value of pulse/pause duration is specified in milliseconds and should be divisible by 100. Minimum pulse/pause duration is 200 ms, maximum – 8000 ms.

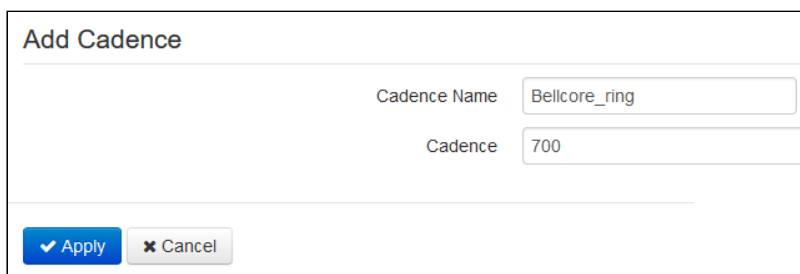
To assign cadence to Alert-Info header value in incoming Invite, you should check the "Use Alert-Info Header" box in assigned SIP profile and set signal name in the "Cadence Name" field (e.g. Example-cadence) in cadence settings. Cadence will playback to line if incoming Invite will content Alert-Info header with value <http://127.0.0.1/Example-cadence>.

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

	Cadence Name	Cadence
<input type="checkbox"/>	Bellcore-dr1	1000,4000
<input type="checkbox"/>	Bellcore-dr2	1000,3000
<input type="checkbox"/>	Bellcore-dr3	1000,2000
<input type="checkbox"/>	Bellcore-dr4	1000,1000
<input type="checkbox"/>	Bellcore-dr5	700,700,700,3000

To edit the specified signal, click on assigned link in "Cadence Name" column.

To add a signal, click the "Add" button and execute the following settings:

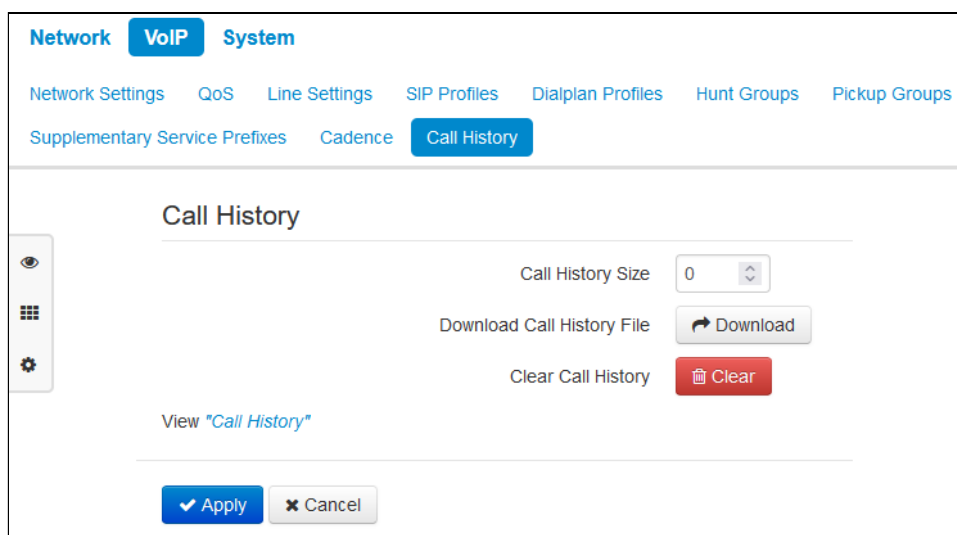


- *Cadence Name*;
- *Cadence* – length of the ringing voltage sending to a subscriber set and length of the pause between call signals, both values should be divisible by 100, min value is 200 ms, max is 8000 ms.

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

3.6.3.10 "Call History" Submenu

In the "Call History" submenu you can configure call logging chronology.



- *Call History Size* – max log entries size, gets values from 0 to 10000 lines. Value "0" disable call logging. In reaching set restriction in log every next entry will delete the oldest entry in log.
- *Download Call History File* – to save the "voip_history" file on local PC click the "Download" button;
- *Clear Call History* – to clear the call history click the "Clear" button.

To view the call history, click the "View Call History" link. A description of parameter monitoring is given in the "Call History" Menu.

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

3.6.4 "System" Menu

In the "System" menu you can configure system, time, device access via different protocols, change password and update device firmware.

3.6.4.1 "Time" Submenu

In the "Time" submenu you can configure time synchronization protocol (NTP).

The screenshot displays the 'Time Settings' configuration interface. At the top, there are tabs for 'Network', 'VoIP', and 'System', with 'System' being the active tab. Below these are sub-tabs: 'Time', 'Access', 'Log', 'WEB authentication', 'Configuration Management', 'Firmware Upgrade', and 'Reboot'. The 'Time' sub-tab is selected. The main content area is titled 'Time Settings' and contains the following fields:

- Time Zone:** A dropdown menu set to 'Moscow'.
- Daylight Saving Time Enable:** A checked checkbox.
- DST Start:** A date and time selector (month, day, year, and time) followed by 'in'.
- DST End:** A date and time selector (month, day, year, and time) followed by 'in'.
- DST Offset (minutes):** A numeric input field set to '60'.
- Enable NTP:** A checked checkbox.
- NTP Server:** A dropdown menu set to 'pool.ntp.org'.

At the bottom of the form, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

Time Settings

- *Time Zone* – allows setting the timezone according to the nearest city for your region from the list;
- *Daylight Saving Time Enable* – when checked, daylight saving time will be performed automatically in specified time period:
 - *DST Start* – day and time, when daylight saving time is starting;
 - *DST End* – day and time, when daylight saving time is ending;
 - *DST Offset (minutes)* – time period in minutes, on which time offset is performed.
- *Enable NTP* – check if it is needed to enable device system time synchronization from a certain NTP server;
- *NTP Server* – time synchronization server IP address / domain name. It is possible to input server address manually or select it from the list.

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

3.6.4.2 "Access" Submenu

In the "Access" submenu you can configure the access to device via web interface, Telnet and SSH.

The screenshot shows the 'Access' submenu configuration page. At the top, there are tabs for 'Network', 'VoIP', and 'System', with 'System' selected. Below the tabs are links for 'Time', 'Access', 'Log', 'WEB authentication', 'Configuration Management', 'Firmware Upgrade', and 'Reboot'. There are also links for 'Autoprovisioning' and 'Certificates'. The main content area is titled 'Access Ports' and contains four input fields: 'HTTP Port' (80), 'HTTPS Port' (443), 'Telnet Port' (23), and 'SSH Port' (22). Below this is the 'Access to "Internet" Service' section, which has three sub-sections: 'Web', 'Telnet', and 'SSH'. Each sub-section has checkboxes for 'WAN' and 'MGMT (Management Interface)' for 'HTTP' and 'HTTPS'. The 'Web' section has 'WAN' checked for HTTP and unselected for HTTPS, and 'MGMT (Management Interface)' checked for both HTTP and HTTPS. The 'Telnet' section has 'WAN' unselected and 'MGMT (Management Interface)' checked. The 'SSH' section has 'WAN' unselected and 'MGMT (Management Interface)' checked. At the bottom of the page are 'Apply' and 'Cancel' buttons.

Access Ports

In this section you can configure TCP ports for access to the device via HTTP, HTTPS, Telnet, SSH.

- *HTTP Port* – number of port for access to web interface via HTTP, default is 80;
- *HTTPS Port* – number of port for access to web interface via HTTPS (HTTP Secure – secure connection), default is 443;
- *Telnet Port* – number of port for access to web interface via Telnet, default is 23;
- *SSH Port* – number of port for access to web interface via SSH, default is 22.

Access to the command line (Linux console) is carried out via Telnet and SSH protocols. Username/password for connection to the console: *admin/password*.

Access to "Internet" Service

To access the device via Internet service interfaces set the following permissions:

Web:

External network and Management interface:

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

Telnet:

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

To grant the access to device using Telnet protocol from external network (via WAN port) and management interface (via *MGMT* port) set the corresponding flags.

SSH:

SSH – secure protocol of device remote control. Unlike Telnet, SSH protocol encrypts whole traffic, including transmitted passwords.

To grant the access to device using SSH protocol from external network (via WAN port) and management interface (via *MGMT* port) set the corresponding flags.

Access to "VoIP" Service:

In this section you can configure the access to VoIP service interface (VoIP service interface is configured in the "*VoIP* → *Network Settings*" section) via web (*HTTP* and *HTTPS*) and also via *Telnet* and *SSH* protocols. To grant the access by any of specified protocols set the corresponding flags.

⚠ For authorization via Telnet and SSH protocols use default username: admin, password: password. After authentication Linux OS console with possibility to use main command interpreter "*shell*" commands will be available.

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

3.6.4.3 "Log" Submenu

The "Log" submenu is intended for configuring the output of various kinds of debug messages of the system in order to detect the causes of problems in the device operation. Debug information may be obtained from the following software modules of the device:

- VoIP manager is responsible for VoIP features operation.
- System manager is responsible for device configuration according to configuration file.
- Configuration manager is responsible for operations with configuration file (reading and writing to the configuration file from different sources) and device monitoring information gathering.

The screenshot displays the 'Log' submenu within the 'System' configuration page. The 'Syslog Settings' section includes an 'Enable' checkbox (checked), a 'Mode' dropdown menu (set to 'Server'), a 'Syslog Server Address' text input field (containing 'syslog.server'), and a 'Syslog Server Port' dropdown menu (set to '514'). The 'VoIP Log' section features four checkboxes for 'Error', 'Warning', 'Debug', and 'Info', all of which are currently unchecked. Below these are two dropdown menus for 'SIP Trace Level' (set to '0: fatal errors, panic') and 'Media Trace Level' (set to '0: fatal error').

Syslog Settings

- *Enable* – when checked, it is possible to set your own settings for the output of debug messages.
- *Mode* – log messages output direction:
 - *Server* – log information is sent to remote Syslog server (this mode is called "remote log");
 - *Local file* – log information is saved to local file;
 - *Server and file* – messages are output via the Syslog protocol to a remote server in file (the protocol is configured below);
 - *Console* – messages are output to device console (connection via COM port adapter is needed);
 - *Remote terminal* – messages are output to the session of the connected terminal via remote access protocols (Telnet/SSH);
 - *USB* – output of messages to a file created on a connected USB device.

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

- *Syslog Server Address* – Syslog server IP address or domain name (required for the "Server" mode);
- *Syslog Server Port* – port for Syslog server incoming messages (514 by default; required for the "Server" mode);
- *File Name* – file name for storage of log in Syslog format (required for the "Local File" mode);
- *File Size, KiB* – log file max size (required for "Local File" mode).

VoIP Log

Type of messages that output to VoIP log is configured below:

- *Error* – check the box if it is needed to output "Error" type messages;
- *Warning* – check the box if it is needed to output "Warning" type messages;
- *Debug* – check the box if it is needed to output "Debug" type messages;
- *Info* – check the box if it is needed to output "Info" type messages;
- *SIP Trace Level* – sets the VoIP SIP manager stack messages output level. Each of the levels (0, 1, 2, 3, 5, 7, 9) has its own interpretation, specified in the drop-down list;
- *Media Trace Level* – sets the output level of media messages. Each of the levels (0, 1, 2, 3, 4, 5, 6) has its own interpretation, specified in the drop-down list.

Networkd Log

Type of messages that output to Network log is configured below:

- *Error* – check the box if it is needed to output "Error" type messages;
- *Warning* – check the box if it is needed to output "Warning" type messages;
- *Debug* – check the box if it is needed to output "Debug" type messages;
- *Info* – check the box if it is needed to output "Info" type messages.

Config Log

Type of messages that output to Config log is configured below:

- *Error* – check the box if it is needed to output "Error" type messages;
- *Warning* – check the box if it is needed to output "Warning" type messages;
- *Debug* – check the box if it is needed to output "Debug" type messages;
- *Info* – check the box if it is needed to output "Info" type messages.

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

3.6.4.4 "WEB Authentication" Submenu

In the "WEB Authentication" submenu you can set passwords for access by administrator, unprivileged user and viewer.

Set passwords are used for device access via web interface and also via Telnet and SSH protocols.

Admin (administrator, default password: password) has the full access to the device: reading/writing any settings, full device status monitoring. **User (non-privileged user, default password: user)** may change their password and configure PPPoE in order to connect to the Internet, may not access the device status monitoring. **Viewer (default password: viewer)** may view full device configuration, may change only their password, may access full device status monitoring.

- ⚠ User name of Administrator: **admin**.
 User name of Unprivileged user: **user**.
 User name of Viewer: **viewer**.

The screenshot shows the 'WEB authentication' configuration page. At the top, there are navigation tabs: Network, VoIP, and System (selected). Below the tabs are links for Time, Access, Log, WEB authentication (selected), Configuration Management, Firmware Upgrade, Reboot, Autoprovisioning, and Certificates. The main content area is titled 'Authentication Parameters' and includes a checkbox for 'WEB digest-authentication' which is checked. Below this, there are three sections for password configuration: 'Administrator Password', 'User Password', and 'Viewer Password'. Each section has a 'Password' input field with a toggle icon, a 'Confirm' input field, and a 'Change Password' button. At the top of the password sections, there are 'Apply' and 'Cancel' buttons.

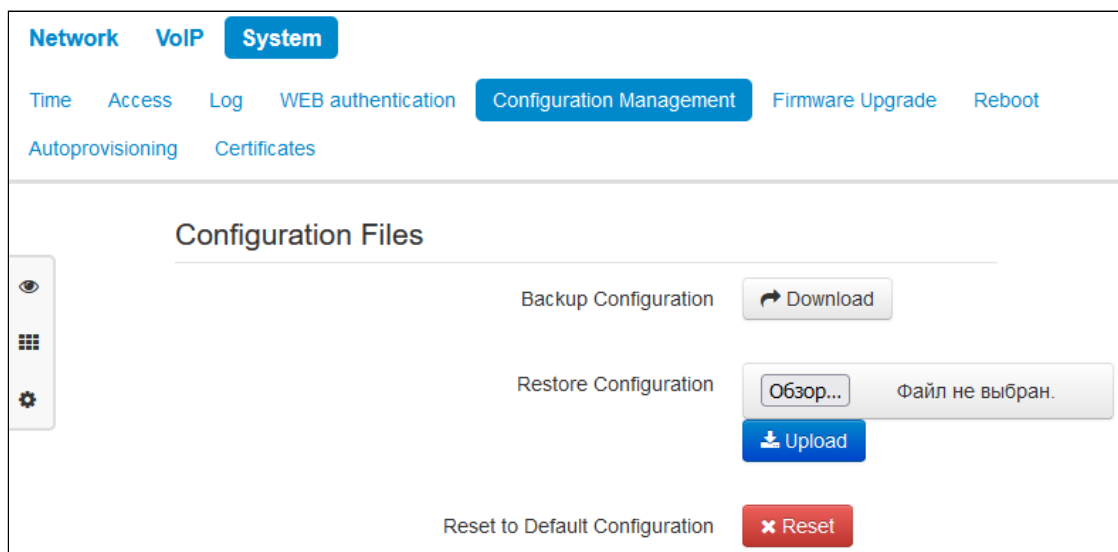
- *WEB Digest-authentication* – when checked, user authentication is performed in accordance with digest algorithm;
- *Administrator Password* – enter the administrator password and confirmation in corresponding fields;
- *User Password* – enter the unprivileged user password and confirmation in corresponding fields;
- *Viewer Password* – enter the viewer password and confirmation in corresponding fields.

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

- ⚠ **TACACS and Digest authentication cannot be used simultaneously.**

3.6.4.5 "Configuration Management" Submenu

In the "Configuration Management" submenu you can save and update current configuration.



Backup Configuration

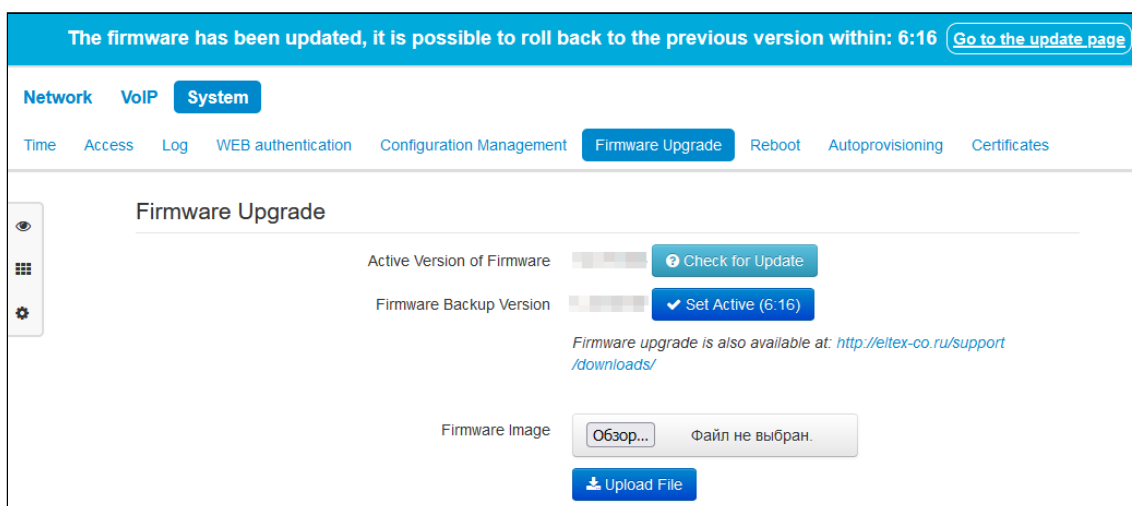
To save the current device configuration to a local computer click the "Download"

Restore Configuration

- *Download the configuration archive to the device* – selection of configuration file saved on local computer. To update the device configuration click the "Select file" button, specify a file (in .tar.gz format) and click the "Upload" Uploaded configuration will be applied automatically without device rebooting.
- *Reset to Default Configuration* – to reset the device to factory default settings click the "Reset"

3.6.4.6 "Firmware Upgrade" Submenu

The "Firmware Upgrade" submenu is intended for the device firmware upgrade.



- *Active Version of Firmware* – version of the firmware that is installed on the device;
- *Check for Update* – the button for firmware version check. Using this function, it is easy to check availability of new firmware version and update it if it is needed;
- *Firmware Backup Version* – firmware version installed on the device, which can be accessed in case of problems with the active firmware version;
- *Set Active* – a button that allows you to make a backup version of the firmware active, this will require a reboot of the device. In this case active firmware version will become a backup one.

⚠ If the ID of the active firmware version and the backup version are different, the system will automatically overwrite the backup version with the active firmware version after 10 minutes. Up to this point, the firmware versions can be switched between each other.

⚠ Internet access is required for the update check function to work.

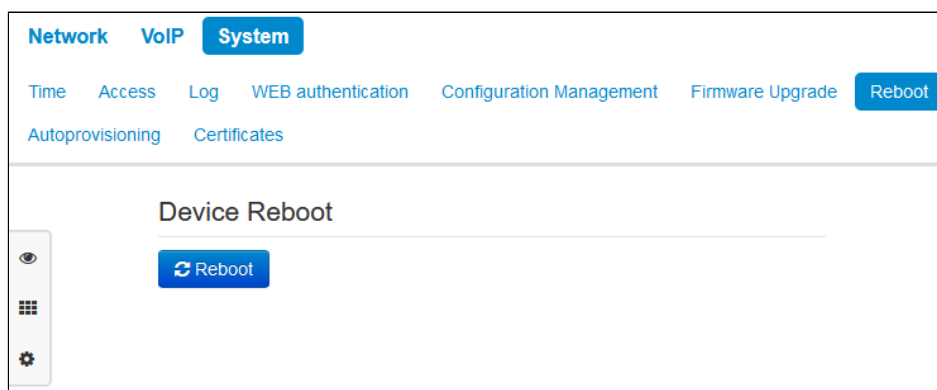
You can also update the device firmware manually by downloading the firmware file from our site <http://eltex-co.ru/support/downloads> and saving it on your computer. To do this, click the "Select file" button in the "Firmware Image" field and specify the path to the control program file in .tar.gz format.

To start the update process, click the "Upload File" button. The update process will take several minutes (its current status will be indicated on the page), after which the device will automatically reboot.

⚠ Do not turn off the power or reboot the device during the firmware update process.

3.6.4.7 "Reboot" Submenu

In the "Reboot" submenu you can reboot the device.



To reboot the device, click the "Reboot" button. The device reboot process takes about 30 seconds.

3.6.4.8 The "Autoprovisioning" Submenu

The "Autoprovisioning" submenu configures the DHCP-based autoprovisioning algorithm and the automatic configuration protocol of the subscriber devices TR-069.

Port	Connection	Speed	Mode	Transmitted	Received
MGMT	Off				
WAN	On	100 Mbit/s	Full-duplex	9.7 MiB (10 214 300 bytes)	9.1 MiB (9 554 851 bytes)

DHCP-based Autoprovisioning

- *Parameters Priority from* – this parameter determines where you need to get the names and location of configuration files and firmware:
 - *Static settings* – the paths to the configuration files and firmware are determined respectively from the "Configuration File" and "Firmware File" parameters; for more algorithm details see Section [DHCP-based Autoprovisioning Algorithm](#);
 - *DHCP options* – the paths to the configuration and firmware files are determined from the DHCP options 43, 66 and 67 (it is necessary to select the DHCP protocol for the Internet service); for more algorithm details see Section [DHCP-based Autoprovisioning Algorithm](#);
- *Provisioning Mode* – to update the firmware configuration separately, you can specify one of the following update modes:
 - *Disabled* – automatic update of device configuration or firmware is disabled;
 - *Periodically* – automatic update of the configuration or firmware of the device will be performed at a specified time interval;
 - *Scheduled* – the device will automatically update its configuration or firmware at a specified time, on specified days of the week.
- *Configuration File* – the full path to the firmware file is specified in the URL format (at the moment it is possible to download the software file using TFTP and HTTP):


```
tftp://<server address>/<full path to cfg file>
```

```
http://<server address>/<full path to cfg file>
```

where <server address> is HTTP or TFTP server address (domain name or IPv4),
 <full path to cfg file> is full path to configuration file on server;
- *Configuration Update Interval, s* – the time interval in seconds after which the device configuration is periodically updated; selecting 0 means a one-time update only just after the device is loaded;
- *Time of Configuration Update* – time in 24-hour format at which the configuration will be automatically updated;
- *Days of Configuration Update* – days of the week on which the configuration will be updated automatically at the specified time.
- *Firmware File* – the full path to the firmware file is specified in the URL format (at the moment it is possible to download the software file using TFTP and HTTP):


```
tftp://<server address>/<full path to firmware file>
```

```
http://<server address>/<full path to firmware file>
```

where <server address> is HTTP or TFTP server address (domain name or IPv4),
 <full path to firmware file> is full path to firmware file on server;

- *Manifest File* – the full path to the manifest file is specified in the URL format (at the moment it is possible to download the file using TFTP and HTTP): The use of the manifest file is due to the large size of the firmware file, which is downloaded periodically according to the firmware automatic update algorithm. To reduce the heavy load on the network in such cases, it is recommended to use the manifest file.

The file structure is a string that specifies the ID of the firmware version available for download and update. For example, the contents of the manifest file may be as follows: "1.3.0-b12".

An optional feature has been added in the current version to control the integrity of the manifest file data: a line with an MD5 checksum added to the file. If the manifest file is specified, but an error occurred with it during transmission over the network and an incorrect checksum was received, then an attempt will be made to retrieve the manifest file again after the timeout specified in the configuration. In this case, the contents of the manifest file can be as follows:

1.3.0-b12

e1edcfce14cffe655d5f28d95e3f88e

- *Firmware Update Interval, s* – the time interval in seconds after which the device firmware is periodically updated; selecting 0 means a one-time update only immediately after the device is loaded;
- *Time of Firmware Update* – time in 24-hour format in which the firmware will be automatically updated;
- *Days of Firmware Update* – days of the week on which the firmware will be updated automatically at the specified time.

For a detailed description of the automatic DHCP-based update algorithm, see Section [DHCP-based Autoprovisioning Algorithm](#).

TR-069 Autoconfiguration

TR-069 Autoconfiguration

Common

Enable TR-069 Client

Interface

ACS Server Address

Enable Periodic Inform

Periodic Inform Interval, s

ACS Connection Request

User Name

Password

Client Connection Request

User Name

Password

NAT Settings

NAT Mode

STUN Server Address

STUN Server Port

Minimum Keep Alive Period, s

Maximum Keep Alive Period, s

Common:

- *Enable TR-069 Client* – when checked, TR-069 internal client operation is enabled;
- *Interface* – selection of the interface through which the device will be automatically configured for operation using the TR-069 protocol;
- *ACS Server Address* – autoconfiguration server address. The address must be entered in the format `http://<address>:<port>` or `https://<address>:<port>` (<address> is ACS server IP address or domain name, <port> is ACS server port, the default port is 80). In the second case, the client will use the secure HTTPS protocol to exchange information with the ACS server. Eltex ACS server defaults to port 9595 for communication;
- *Enable Periodic Inform* – when checked, internal TR-069 client performs periodic ACS server polling with an interval equal to the "Periodic Inform Interval" in seconds. Goal of the polling is to identify possible changes in the device configuration;
- *Periodic Inform Interval, s* – 2 PERIODIC messages sending interval.

ACS Connection Request:

User Name, Password – user name and password for client access to the ACS server.

Client Connection Request:

User Name, Password – user name and password for the ACS server access to TR-069 client.

NAT Settings:

If there is a NAT (network address translation) between the client and ACS server, ACS server may not be able to establish the connection to client without specific technologies intended to prevent such situations.

- *NAT Mode* – determines how the client should receive information about their public address. Available modes:
- *STUN* – use STUN protocol for public address identification;

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

When selecting STUN mode, the following settings must be set:

- *STUN Server Address* – STUN server IP address or domain name;
- *STUN Server Port* – STUN server UDP port (3478 by default);
- *Minimum Keep Alive Period, s* and *Maximum Keep Alive Period, s* – define the time interval in seconds for periodic transmission of messages to STUN server for public address modification discovery.

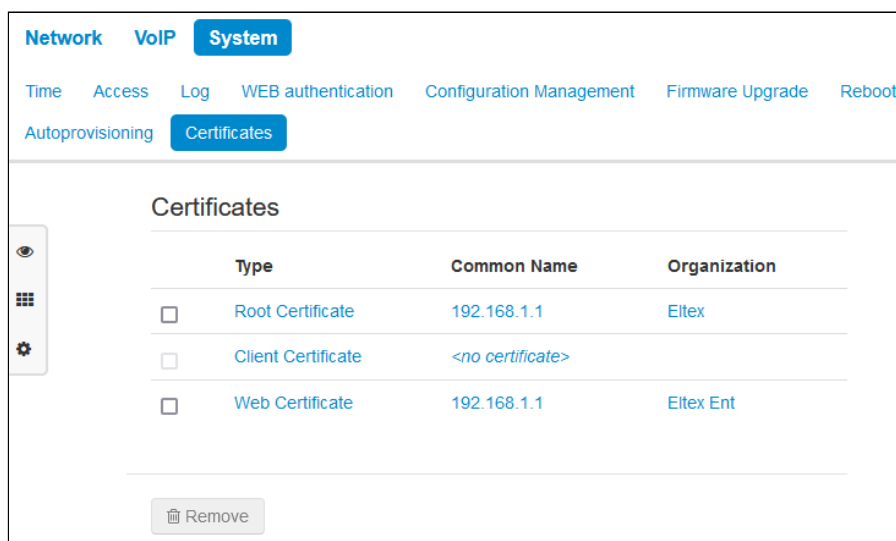
When the *Manual* mode is selected, the client's public address is set manually via the *NAT Address* parameter (the address must be entered in IPv4 format).

⚠ To work correctly with an ACS server behind NAT, the minimum polling period of a STUN server must be less than the maximum save time of the session by the NAT device.

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

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

3.6.4.9 "Certificates" Submenu



The "Certificates" submenu allows to view, download and upload the certificates for use in secure TLS connections in the device.

Root Certificate

The root certificate is used to authenticate certificates for incoming connections. This certificate must be signed by the authorization center.

The screenshot shows a web interface for configuring a Root Certificate. The page is titled "Root Certificate" and is part of a "System" configuration menu. The interface includes a navigation bar with tabs for "Network", "VoIP", and "System", and a sub-menu for "Certificates". The main content area displays the following information:

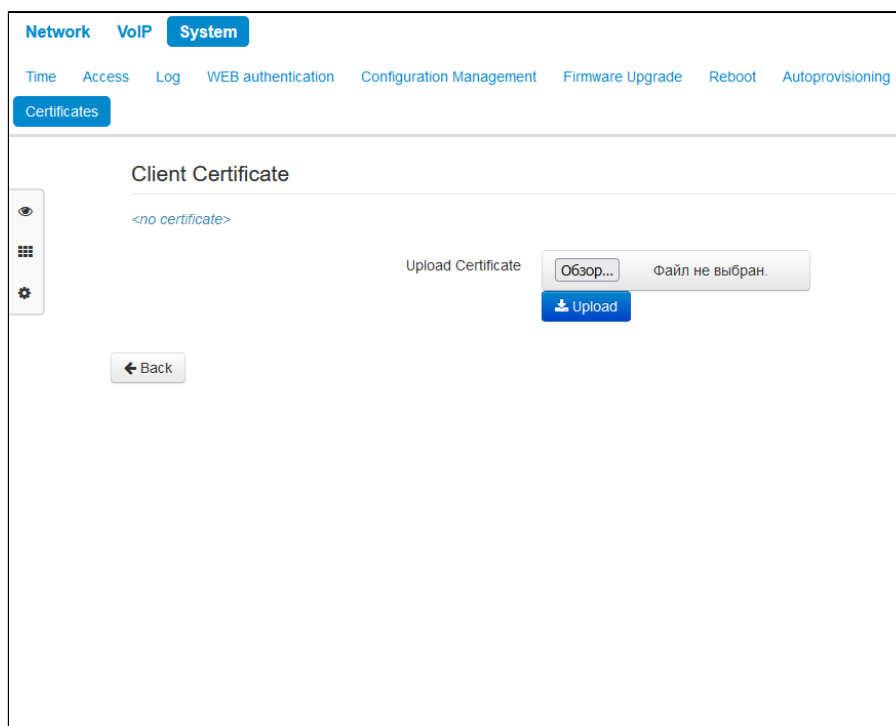
- Certificate:**
 - Serial Number: 76:57:8F:9B:90:D4:A8:01:62:3A:49:48:D5:3B:F3:E0:0B:2C:4E:D5
 - Not valid before: [blurred]
 - Not valid after: [blurred]
- Subject:**
 - Common Name: 192.168.1.1
 - Organization: Eitex
 - Subject Alternative Name: -
- Name of the certification authority:**
 - Common Name: 192.168.1.1
 - Organization: Eitex

Below the certificate details, there is a section titled "Operation With Certificate" containing two buttons: "Download Certificate" with a "Download" button, and "Upload Certificate" with a file selection button labeled "Обзор..." and "Файл не выбран.", and an "Upload" button. A "Back" button is located at the bottom left of the page.

- *Serial Number* – serial number of the chosen certificate;
- *Not valid before* – certificate start date;
- *Not valid after* – certificate end date;
- Information about the certificate receiver (*Common Name, Organization, Subject Alternative Name*).
- Data about the authorization center (*Common Name, Organization*).

Client Certificate

The client certificate is used for outgoing SIP connections using TLS.



- *Serial Number* – serial number of the chosen certificate;
- *Not valid before* – certificate start date;
- *Not valid after* – certificate end date.
- Information about the certificate receiver (*Common Name, Organization, Subject Alternative Name*);
- Data about the authorization center (*Common Name, Organization*).

Web Certificate

The web certificate is used when accessing the device`s web configurator via the HTTPS protocol.

The screenshot shows the 'Web Certificate' configuration page. At the top, there are navigation tabs for 'Network', 'VoIP', and 'System', with 'System' selected. Below these are sub-tabs: 'Time', 'Access', 'Log', 'WEB authentication', 'Configuration Management', 'Firmware Upgrade', 'Reboot', and 'Autoprovisioning'. The 'Certificates' sub-tab is active. The main content area is titled 'Web Certificate' and contains the following information:

- Certificate**
 - Serial Number: 4E:0B:4D:7E:49:A5:3F:E1:E3:59:30:CA:8A:F0:3A:DC:F2:E1:24:66
 - Not valid before: 05.12.2023
 - Not valid after: 18.01.2038
- Subject**
 - Common Name: 192.168.1.1
 - Organization: Eitex Ent
 - Subject Alternative Name: -
- Name of the certification authority**
 - Common Name: 192.168.1.1
 - Organization: Eitex Ent

At the bottom, there is an 'Operation With Certificate' section with two actions:

- Download Certificate**: A button labeled 'Download' with a download icon.
- Upload Certificate**: A file selection interface with a button labeled 'Обзор...' (Browse...), a status message 'Файл не выбран.' (File not selected.), and a blue 'Upload' button with an upload icon.

A 'Back' button is located at the bottom left of the page.

- *Serial Number* – serial number of the chosen certificate;
- *Not valid before* – certificate start date;
- *Not valid after* – certificate end date.
- Information about the certificate receiver (*Common Name, Organization, Subject Alternative Name*);
- Data about the authorization center (*Common Name, Organization*).

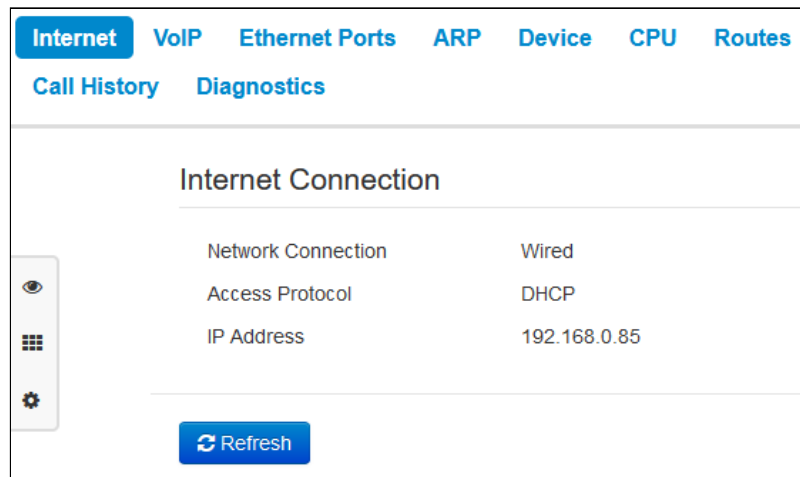
3.7 System Monitoring

To switch to the "System Monitoring" mode select "Monitoring" on the left panel.

⚠ Some pages do not automatically update device monitoring data. To get current information, click the "Refresh" button.

3.7.1 "Internet" Menu

In the "Internet" menu you can view common network settings of the device.



Internet connection

- *Network Connection* – type of network connection;
- *Access Protocol* – protocol, used for Internet access;
- *IP Address* – device IP address in external network.

3.7.2 "VoIP" Menu

In the "VoIP" menu you can view the state of the VoIP network interface, monitor subscriber sets and hunt group registration status, test lines.

Status of VoIP Network Interface

IP Address 192.168.0.113

FXS Status

Line	Local Number	Registration	Expires In	Server Address	Line State	Call State 1	Remote User 1	Call State 2	Remote User 2	Line Test	FXS statistics
<input type="checkbox"/> FXS1	1	Ok	00:26:49	192.168.0.1	Testing (57 s)						Show
<input type="checkbox"/> FXS2	2	Ok	00:21:19	192.168.0.1	Ringing	Ringing	3			Test	Show
<input type="checkbox"/> FXS3	3	Ok	00:21:24	192.168.0.1	Active	Ringback	2			Test	Show
<input type="checkbox"/> FXS4	4	Ok	00:21:32	192.168.0.1	Inactive					Test	Show
<input type="checkbox"/> FXS5	5	Ok	00:21:38	192.168.0.1	Inactive					Test	Show
<input type="checkbox"/> FXS6	6	Ok	00:21:44	192.168.0.1	Inactive					Test	Show
<input type="checkbox"/> FXS7	7	Ok	00:21:50	192.168.0.1	Inactive					Test	Show
<input type="checkbox"/> FXS8	8	Ok	00:21:56	192.168.0.1	Inactive					Test	Show

[Register](#) [Unregister](#)

Hunt Groups Status


Group Name	State	Phone	Line List	Registration	Expires In	Server Address
Group1	Enabled	17005	FXS1, FXS2, FXS3, FXS6, FXS7	Ok	00:29:24	192.168.0.1
Group2	Disabled			None		
Group3	Disabled			None		
Group4	Disabled			None		
Group5	Disabled			None		
Group6	Disabled			None		
Group7	Disabled			None		
Group8	Disabled			None		


Status of VoIP Network Interface

- *IP Address* – IP address for VoIP service network interface.

FXS Status

- *Line* – number of device`s subscriber set;
- *Local Number* – subscriber`s phone number, assigned to this subscriber port;
- *Registration* – state of group phone number registration on proxy server:
 - *None* – registration on SIP server function is disabled in SIP profile configuration;
 - *Error* – registration failed;
 - *Ok* – registration on SIP server is successful;
- *Expires In* – time before the registration expiration of the subscriber port on SIP server;
- *Server Address* – address of the server where the subscriber line was last registered;
- *Line State* – physical line state. The line can be in one of the following states:
 - *Inactive* – the handset is off hook (or subscriber port is disabled), normal work;
 - *Active* – the handset is on hook; a station response signal is output to the line, either a ringback tone or an error signal, or the line is in a conversation state;
 - *Ringing* – the phone rings (when an incoming call is received);
 - *Testing* – line testing process is launched.
- *Call State 1, 2* – every subscriber port support up to 2 simultaneous communication sessions. This field displays the status of the call with the corresponding remote subscriber. The call can be in one of the following states:
 - *Dial* – dialing from a telephone set;
 - *Busy* – the call for some reason is cleared, a busy signal is output to the line;
 - *Outgoing Call* – the remote subscriber is being called; a ringback tone is output to the line;
 - *Incoming Call* – an incoming call arrives at the phone port, a ringing tone is output to the line;
 - *Conversation* – a conversation connection with the remote subscriber is established;
 - *Oncoming on Hold* – remote subscriber is on hold;
 - *Local on Hold* – local subscriber is put on hold;
 - *Error, Hang up* – error tone is output to the line. The error tone is output after the expiration of the busy tone timeout (configured separately for each line) when you forgot to hang up the phone.
- *Remote User 1, 2* – phone number of the remote subscriber of each communication session.
- *FXS statistics* – displays number of incoming and outgoing calls as well as the last dialed number.
- *Line Test* – the subscriber line testing process is starting after clicking the "Test" The status of the process is indicated by a reverse timer (in the "Line State" column), which indicates the remaining test time. You cannot run the test on multiple lines at the same time. The test duration is 80 seconds. During the test, the subscriber set is blocked – it will be impossible to make and receive calls.

Line	Local Number	Registration	Expires In	Server Address	Line State	Call State 1	Remote User 1	Call State 2	Remote User 2	Line Test	FXS statistics
<input checked="" type="checkbox"/>	FXS1 001	None			Testing (77 s)						Show

At the end of the test, the result can be viewed by clicking the button  in the "Test Line" column. The result is presented in the form of a table and contains the following data:

- *Test Date*;
- *Foreign DC Voltage A (TIP)*;
- *Foreign DC Voltage B (RING)*;
- *Foreign AC Voltage A (TIP)*;
- *Foreign AC Voltage B (RING)*;
- *Line Supply Voltage*;
- *Cross Current*;
- *Longitudinal Current*;
- *Resistance A (TIP) – B (RING)*;
- *Resistance A (TIP) – Ground*;
- *Resistance B (RING) – Ground*;
- *Resistance A (TIP) – B (RING)*;
- *Capacity A (TIP) – Ground*;

- *Capacity B (RING) – Ground*;
- *Telephone set* – information about the TS connection.

Example of Line 1 test result:

Test Result: Line FXS1 ✕	
Test Date	17:35:17 07.12.2023
Foreign DC Voltage A (TIP)	0.099774 U
Foreign DC Voltage B (RING)	0.041903 U
Foreign AC Voltage A (TIP)	0.040325 U
Foreign AC Voltage B (RING)	0.028888 U
Line Supply Voltage	-55.851212 U
Cross Current	0.281639 mA
Longitudinal Current	-0.095401 mA
Resistance A (TIP) - B (RING)	503.466339 kΩ
Resistance A (TIP) - Ground	472.445129 kΩ
Resistance B (RING) - Ground	402.959167 kΩ
Capacity A (TIP) - B (RING)	50 nF
Capacity A (TIP) - Ground	50 nF
Capacity B (RING) - Ground	50 nF
Telephone Set	Not connected

Under the FXS Status table there are buttons for compulsory registration or unregistration of selected lines.

Hunt Groups Status

- *Group Name* – the name of the hunt group.
- *State* – the status of the hunt group: enabled or disabled;
- *Phone* – hunt group phone number;
- *Line List* – line (port) list, that are included in the hunt group;
- *Registration* – state of group phone number registration on proxy server:
 - *None* – registration on SIP server function is disabled in SIP profile configuration;
 - *Error* – registration failed;
 - *Ok* – registration on SIP server is successful;
- *Expires In* – time before the expiration of registration of the hunt group on SIP server;
- *Server Address* – address of the server where the hunt group was last registered.

IMS Monitoring

IMS monitoring shows the status of some services (activated or not activated) on each subscriber line, provided that remote management from the IMS (IP Multimedia Subsystem) server is enabled on that line.

IMS Monitoring								
Line	FXS1	FXS2	FXS3	FXS4	FXS5	FXS6	FXS7	FXS8
IMS Management	Off	Off	Off	Off	Off	Off	Off	Off
Three-party Conference	-	-	-	-	-	-	-	-
Call Hold	-	-	-	-	-	-	-	-
Call Waiting	-	-	-	-	-	-	-	-
Hotline	-	-	-	-	-	-	-	-
Hotline Number	-	-	-	-	-	-	-	-
Hotline Timeout, s	-	-	-	-	-	-	-	-
Call Transfer	-	-	-	-	-	-	-	-
Special condition tone	-	-	-	-	-	-	-	-

- *IMS Management*— shows whether or not remote management of subscriber line services from the IMS server is enabled (configurable in the SIP profile, see the "[SIP Profiles](#)" Submenu);
- *Three-way conference* – shows whether or not the command to activate the "Three-way conference" service has been received from the IMS server;
- *Call Hold* – shows whether or not a command to activate the Call Hold service has been received from the IMS server;
- *Call Waiting* – shows whether or not a command to activate the Call Waiting service has been received from the IMS server;
- *Hotline* – shows whether or not the command to activate the Hotline service has come from the IMS server;
- *Hotline Number* – shows the phone number for the Hotline service in the activation command from the IMS server;
- *Hotline Timeout, s* – shows the dialing timeout for the Hotline service in the activation command from the IMS server;
- *Call Transfer* – shows whether or not a command to activate the Call Transfer service has been received from the IMS server;
- *Special Station Reply* – shows whether or not the command to activate the "Special Station Reply" service has been received from the IMS server.

- ✓ – service is activated;
- ✗ – service is not activated.

3.7.3 Ethernet ports menu

In the "Ethernet Ports" menu, you can view the state of the device Ethernet ports.

Internet VoIP Ethernet Ports ARP Device CPU Routes Call History Diagnostics						
State of Ethernet Ports						
Port	Connection	Speed	Mode	Transmitted	Received	
MGMT	Off					
WAN	On	100 Mbit/s	Full-duplex	9.7 MiB (10 214 300 bytes)	9.1 MiB (9 554 851 bytes)	

Refresh

State of Ethernet ports

- *Port* – port name:
 - *WAN* – external network port;
 - *MGMT* – a port for device management.
- *Connection* – state of connection to this port:
 - *On* – network device is connected to the port (link is active);
 - *Off* – network device is not connected to the port (link is inactive).
- *Speed* – speed of the external network device connection to this port (10/100/1000 Mbit/s);
- *Mode* – data transmission mode:
 - *Full-duplex*;
 - *Half-duplex*.
- *Transmitted* – amount of transmitted bytes from port;
- *Received* – amount of received bytes from port.

To get current information about the state of Ethernet ports, click the "*Refresh*" button.

3.7.4 "ARP" Menu

In the "ARP" menu, you can view the device ARP table. The ARP table contains information about the alignment between the IP and MAC addresses of neighboring network devices.

IP Address	MAC Address	Client Name	Interface
192.168.0.1	50:3E:AA:03:23:EC		WAN
192.168.0.160	E8:DE:27:A8:93:94		WAN

ARP Table

- *IP Address* – the device IP address;
- *MAC Address* – the device MAC address;
- *Client Name* – network name of the connected device;
- *Interface* – the interface from which the device is active: *WAN*, *MGMT*.

To get current information, click the "Refresh" button.

3.7.5 "Device" Menu

The "Device" menu contains common information about the device.

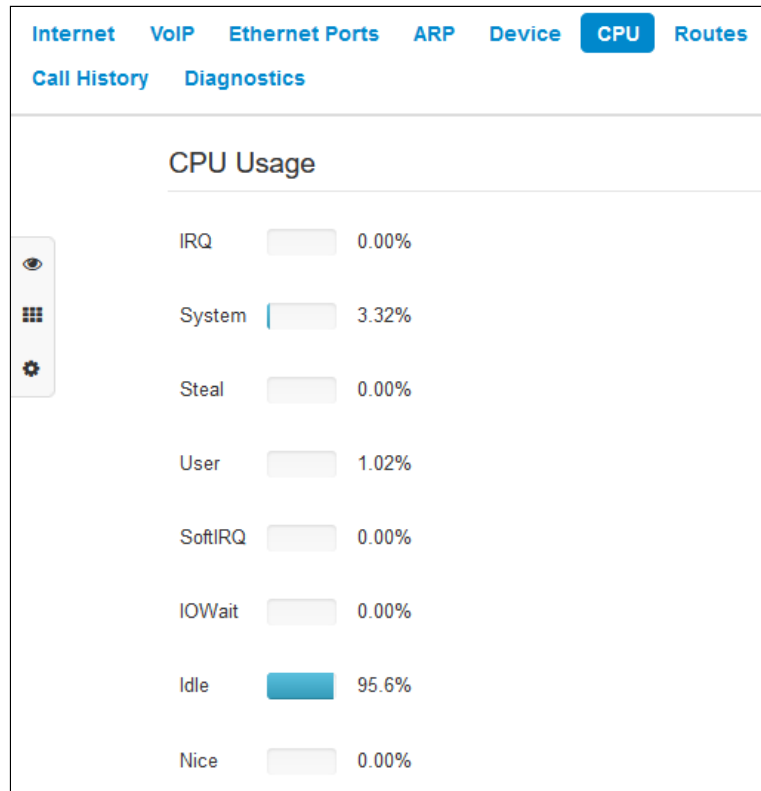
Product	TAU-8N.IP
Firmware Version	1.0.0.0
Factory MAC Address	50:3E:AA:03:23:EC
Serial Number	123456789
System Time	05:58:52 08.12.2023
Uptime	23:13:10

Device Info

- *Product* – device model name;
- *Firmware Version* – device firmware version;
- *Factory MAC Address* – device WAN interface MAC address, set by manufacturer;
- *Serial Number* – device serial number, set by manufacturer;
- *System Time* – current time and date, set in the system;
- *Uptime* – the time since the last device switching or rebooting.

3.7.6 "CPU" Menu

The "CPU" menu displays data on CPU usage.



CPU Usage

- *IRQ* – percentage of CPU time spent on processing of hardware interruptions;
- *System* – percentage of CPU time utilization by core processes;
- *Steal* – percentage of CPU time during which the device does not receive processor resources for its execution;
- *User* – percentage of CPU time utilization by user applications;
- *SoftSIRQ* – percentage of CPU time spent on processing of firmware interruptions;
- *IOWait* – percentage of CPU time spent on input operations;
- *Idle* – percentage of unused CPU resources;
- *Nice* – percentage of CPU time utilization by applications with a modified priority.

3.7.7 "Routes" Menu

In the "Routes" menu, you can view the device routing table.

Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
0.0.0.0	192.168.0.1	0.0.0.0	UG	0	0	0	wan
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	wan
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	mgmt

- *Destination* – IP address of destination host or subnet that the route is established to;
- *Gateway* – gateway IP address that allows for the access to the Destination;
- *Netmask* – a subnet mask;
- *Flags* – certain route characteristics. There are the following flag values:
 - **U** – shows that the route is created and is passable;
 - **H** – indicates the route to a particular node;
 - **G** – shows that the route goes through an external gateway. The network interface of the system provides routes on the network with a direct connection. All other routes pass through external gateways. The G flag marks all routes except those on the network with a direct connection;
 - **R** – shows that the route was most likely created by a dynamic routing protocol running on the local system using the reinstate parameter;
 - **D** – shows that the route was added as a result of receiving an ICMP Redirect Message. When the system learns about the route from the ICMP Redirect message, the route is included in the routing table to avoid redirection for subsequent packets destined to the same destination. Such routes are marked with the D flag;
 - **M** – shows that the route has changed – probably as a result of running a dynamic routing protocol on the local system and using the mod parameter;
 - **A** – indicates a buffered route to which an entry in the ARP table corresponds;
 - **C** – shows that the source of the route is the core routing buffer;
 - **L** – shows that the destination of the route is one of the addresses of this computer. Such "local routes" exist only in the routing buffer;
 - **B** – shows that the destination of the route is a broadcast address. Such "broadcast routes" exist only in the routing buffer;
 - **I** – shows that the route is connected to a loopback interface for a purpose other than to access the ring network. Such "internal routes" exist only in the routing buffer;
 - **!** – shows that datagrams sent to this address will be rejected by the system.
- *Metric* – determines route "cost". The metric is used to sort duplicate routes, if any exist in the table;
- *Ref* – fixed number of calls to the route to create a connection (not used in the system);
- *Use* – the number of route detections made by IP;
- *Interface* – the name of the network interface through which this route runs.

To get current information, click the "Refresh" button.

3.7.8 "Call History" Menu

In the "Call History" menu, you can view a list of completed phone calls, as well as a summary of each call.

Device RAM may store up to 10 000 performed calls records. When the number of records exceeds 10 000, the oldest records will be deleted, and the new ones will be added at the end of the file.

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

Filter (show)

[Change Call History Settings](#)

No	Line	Local	Remote	Remote Host	Start Call Time	Start Talk Time	Talk Duration	State	Type	TxPack	TxBytes	RxPack	RxBytes
1	1	80100	80101	192.168.0.160	09:57:30 08.12.2023	09:57:32 08.12.2023	6s	local clear	outgoing	105	24722	111	25923
2	2	80101	80100	192.168.0.160	09:57:30 08.12.2023	09:57:32 08.12.2023	6s	remote clear	incoming	1	240	0	0
3	2	80101	80100	192.168.0.160	09:57:46 08.12.2023	-	-	local clear	outgoing	0	0	0	0
4	1	80100	80101	192.168.0.160	09:57:46 08.12.2023	-	-	remote clear	incoming	0	0	0	0
5	1	80100	85430000	192.168.0.160	09:58:22 08.12.2023	09:58:22 08.12.2023	25s	local clear	outgoing	327	24817	536	128640
6	2	80101	85430001	192.168.0.160	09:58:27 08.12.2023	09:58:27 08.12.2023	15s	local clear	outgoing	507	39217	104	24960
7	1	80100	7100005	192.168.0.160	09:59:24 08.12.2023	-	-	no route	outgoing	0	0	0	0

20 records per page

Page 1 from 1

Description of the "Call History" table fields:


- *No* – sequence number of the record in the table;
- *Line* – device subscriber port number;
- *Local* – subscriber number assigned to the current subscriber port;
- *Remote* – remote subscriber number that the phone connection has been established with;
- *Remote Host* – IP address of the remote subscriber with whom a telephone connection was established;
- *Start Call Time* – received/performed call time and date;
- *Start Talk Time* – call start time and date;
- *Talk Duration* – talk duration in seconds;
- *State* – intermediate state or reason for call clearing; description becomes available, when you hover the cursor over the call state record;
- *Type* – call type: outgoing or incoming;
- *TxPack* – number of RTP packets transmitted during the call;
- *TxBytes* – number of bytes transmitted during the call;
- *RxPack* – number of RTP packets received during the call;
- *RxBytes* – number of bytes received during the call.


In the call history table, you may search records by different parameters. To do this, click the "Filter (show)" link. Filtering can be performed by subscriber line number, local or remote number, remote IP, call start time, talk start time, call state and call type. For filtering parameter description, see call history table field description above.


Start Call Time, from/to or *Start Talk Time, from/to* – call received/performed time period or talk start time period in the "hh:mm:ss dd.mm.yyyy" format.


To hide the settings for filtering records, click the "*Filter (hide)*" link.

To configure call history parameters, click "*Change Call History Settings*" link. For detailed parameter configuration description, see "[Call History](#)" Submenu.

Click  button to proceed to the first record of the call history table.

Click  button to proceed to the previous page of the call history table.

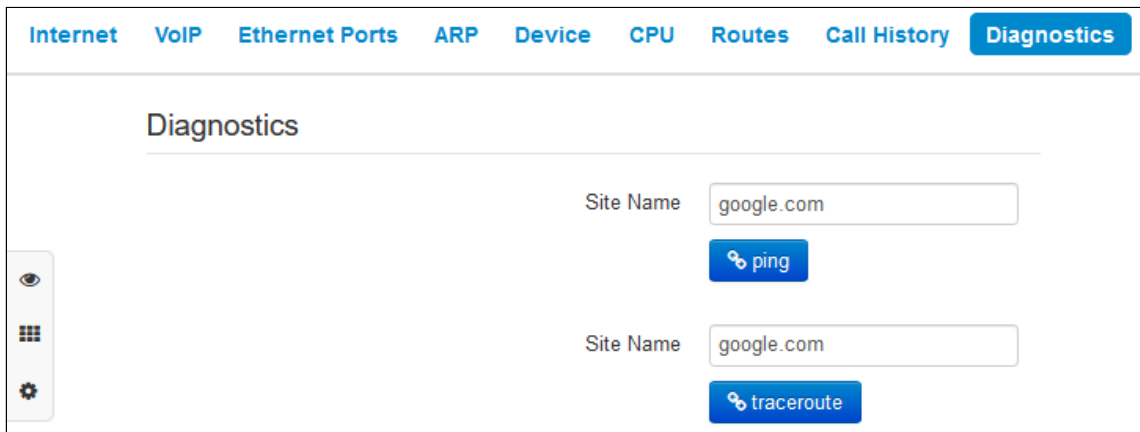
Click  button to proceed to the next page of the call history table.

Click  button to proceed to the last record of the call history table.

Selecting "*records per page*" enables you to customize the number of displayed table records on a single page.

3.7.9 "Diagnostics" Menu

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



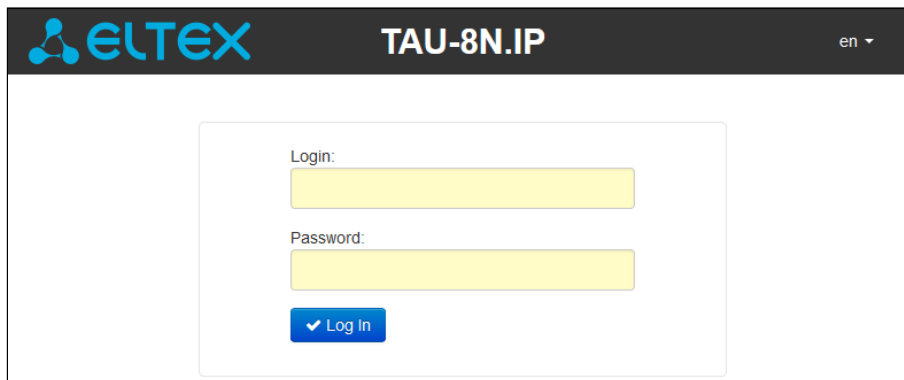
Network Utilities:

- *Ping* – utility for checking connections in TCP/IP-based networks;
- *Traceroute* – utility to determine data routes in TCP/IP networks.

3.8 Example of device configuration


Connect the PC to the device`s MGMT port, connect the wire from the provider`s network to the WAN port;
Enter the IP address of the gateway in the browser address bar (by default 192.168.1.1);

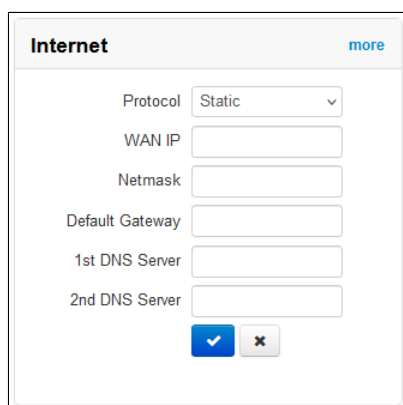
When the device is connected, a window will appear asking for your login and password. Fill in the fields and click "Log in" (by default login: admin, password: password).



If this window does not appear, make sure that the automatic connection to obtain an IP address is set in the network connection settings on your PC.


In the "Internet" tile you can configure external connection. In the "Protocol" field, select the protocol used by your Internet service provider and enter the required data according to the provider`s instructions. If you use the static settings, select Static value in the "Protocol" field and fill the "WAN IP", "Netmask", "Default Gateway," "1st DNS Server", and "2nd DNS Server" fields with the corresponding values obtained from service provider. To

save and apply settings, click .




To specify additional parameters, go to advanced settings mode by clicking the "more" link (see the "Internet Submenu").

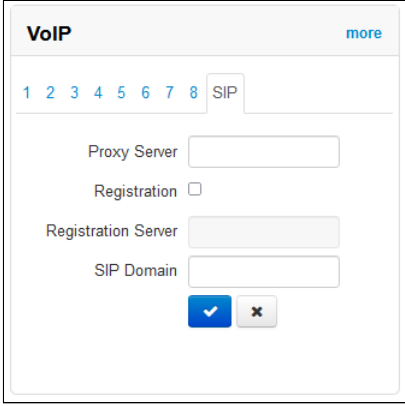
In the "VoIP" tile subscriber lines are quickly configured for operation via SIP. To do this, select "Line" number required for configuring. Check the "Enable" box, enter phone number assigned to the current line, user name and password for SIP server authorization.

To save and apply settings, click .

The subscriber lines in another "Line" tabs are configured the same way.

Select the "SIP" tab in the "VoIP" tile to configure the SIP settings. Enter the SIP and registration servers IP addresses or domain name (if necessary) in the corresponding fields. If port numbers used on servers are different than 5060, specify alternative port colon separated. Specify the SIP Domain if necessary. Check the "Registration" box if SIP server subscriber registration is required for VoIP operation (usually registration is required).

To save and apply settings, click .



The screenshot shows a configuration window titled "VoIP" with a "more" link in the top right corner. Below the title is a horizontal menu with tabs numbered 1 through 8, and the "SIP" tab is selected. The main content area contains the following fields and controls:

- Proxy Server: A text input field.
- Registration: A checkbox, currently unchecked.
- Registration Server: A text input field.
- SIP Domain: A text input field.
- At the bottom, there are two buttons: a blue button with a white checkmark and a grey button with a white 'x'.

To specify additional parameters, go to advanced settings mode by clicking the "more" link (see the "VoIP Menu").

4 Supplementary Service Usage

4.1 Call Transfer

"Call transfer" service may be performed locally using gateway resources, or remotely using resources of a communicating device. If the service is performed using resources of a communicating device, the access to "Call transfer" service is established via subscriber port settings menu – "VoIP → Line Settings" by selecting "Transmit flash" value in "Flash Mode" field. Service process logics in this case will be defined by the communicating device.

When "Call transfer" service is performed locally using gateway resources, the access to this service is established via subscriber port settings menu – "VoIP → Line Settings" – by selecting "Attended calltransfer", "Unattended calltransfer", or "Local calltransfer" in "Flash Mode" field.

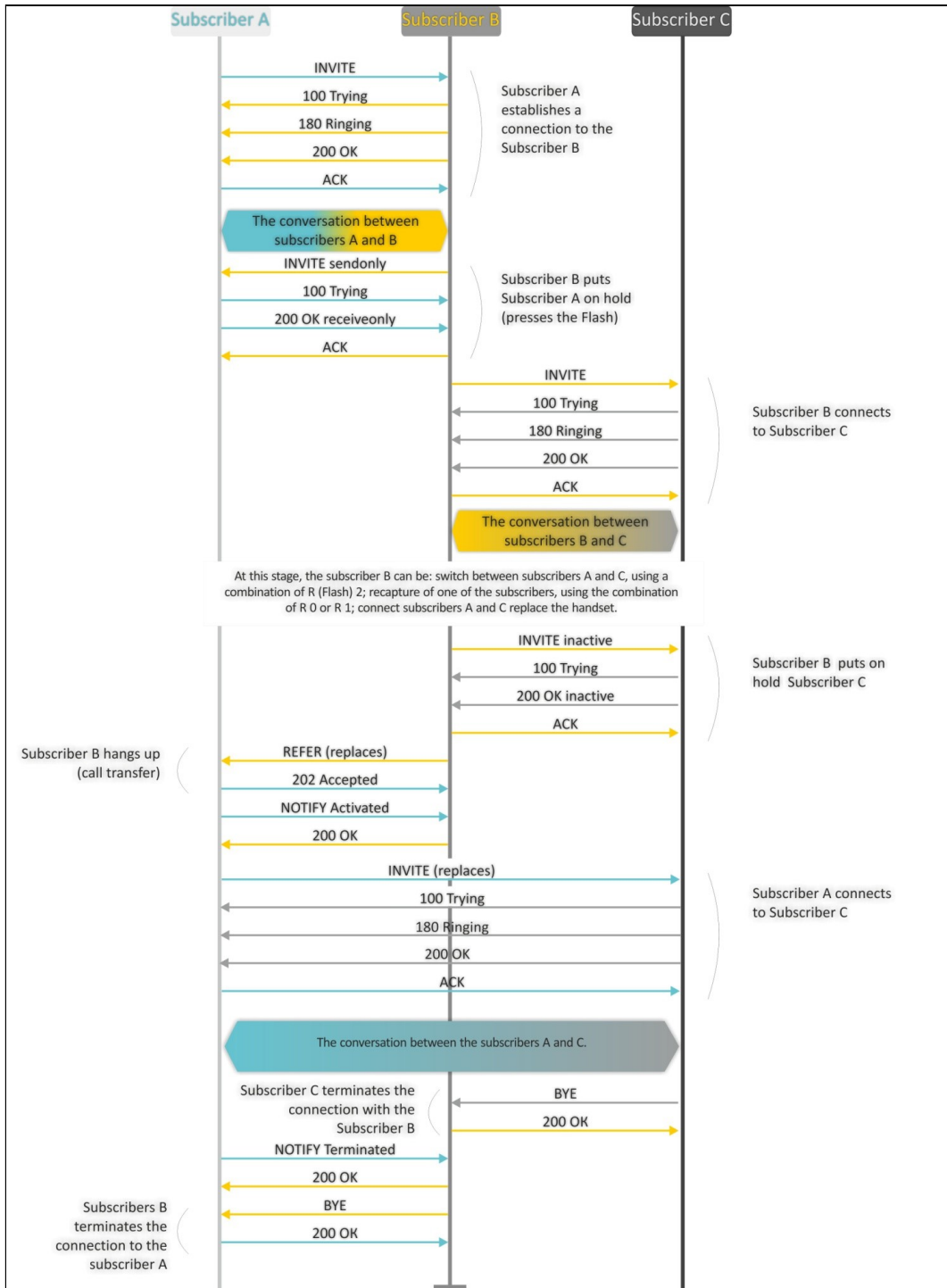
"Attended calltransfer" service enables temporary disconnection of an online subscriber (Subscriber A), connection establishing with another subscriber (Subscriber C) and return to the previous connection without dialing or transfer the call while disconnecting Subscriber B.

"Attended calltransfer" service usage:

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

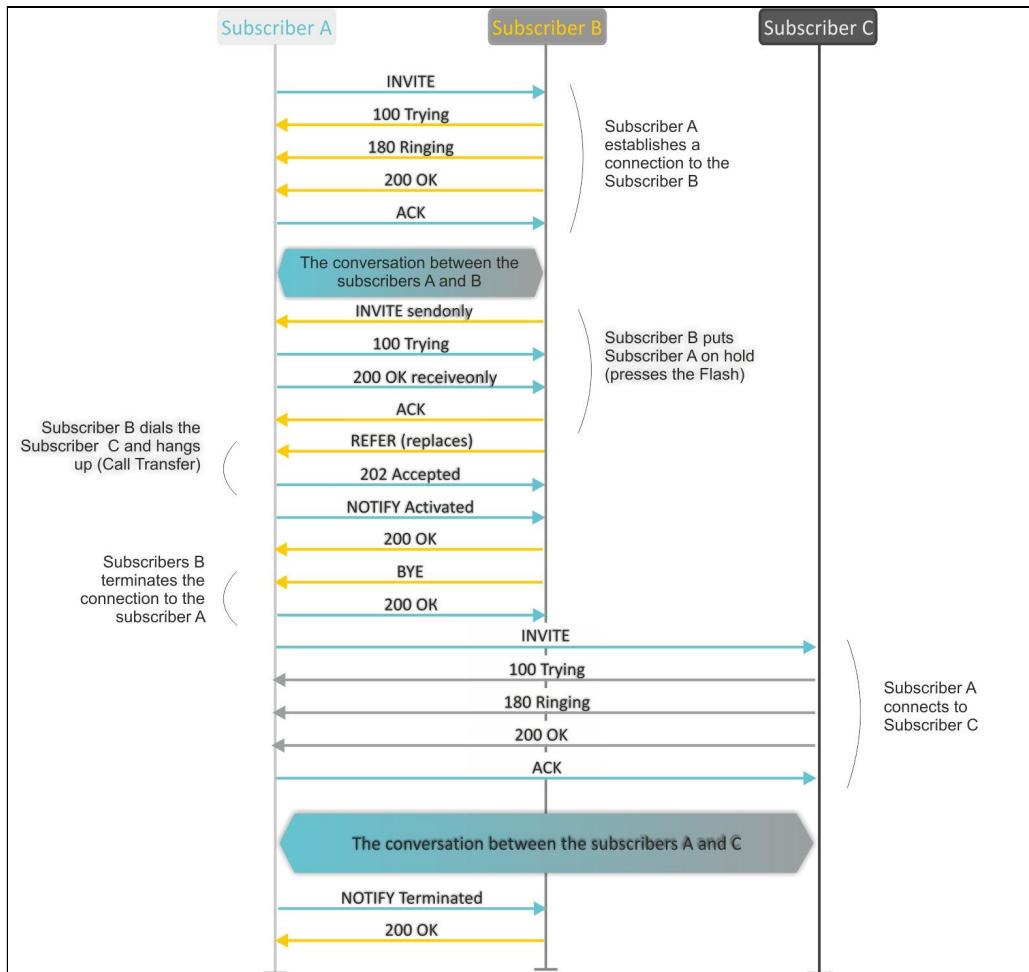
- *R0* – disconnect a subscriber on hold, connect to online subscriber;
- *R1* – disconnect an online subscriber, connect to subscriber on hold;
- *R2* – switch to another subscriber (subscriber change);
- *R3* – conference;
- *R4* – call transfer. Voice connection will be established between Subscribers A and C;
- *R clearback* – call transfer. Voice connection will be established between Subscribers A and C.

The figure below shows an algorithm of "Attended calltransfer" service operation:



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

The figure below shows an algorithm of "Unattended calltransfer" service operation:



"Local Calltransfer" service allows to transfer the call within the gateway without external REFER message sending in case when Subscriber C is local TAU-8N.IP subscriber and call was made directly, without proxy server. If subscriber C is external or local subscriber, but has been called using proxy server, "Local Calltransfer" service works the same way as "Attended Calltransfer", i.e. call transfer is carried out by sending the REFER message to subscriber B.

4.2 Call Waiting

This service allows to inform "busy" users about new incoming calls with a special signal. Upon receiving this notification, user can answer or reject a waiting call.

Access to this service is established via subscriber "Line Settings" menu by selecting "*Attended calltransfer*", "*Unattended calltransfer*", or "*Local Calltransfer*" in "*Flash Mode*" field and checking the "*Call Waiting*".

Service usage:

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

- *R0* – reject new call;
- *R1* – answer the waiting call;
- *R2* – switch to new call (subscriber change);
- *R* – short clearback (flash).

4.3 Three-party Conference

Three-party conference is a service, that enables simultaneous phone communication for 3 subscribers. For entering conference mode press R3 (see Section "Call Transfer").

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

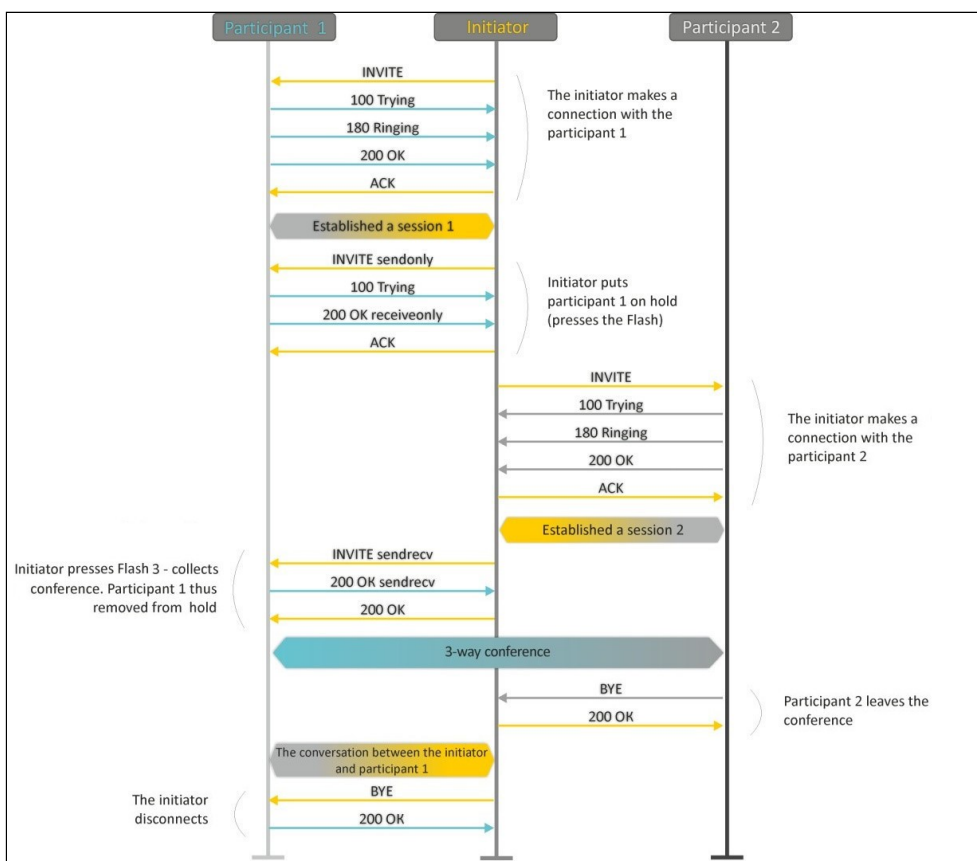
Local conference is the one mode of three-party conference operation. In this mode, the conference is collected locally by the initiator subscriber.

4.3.1 Local Conference

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

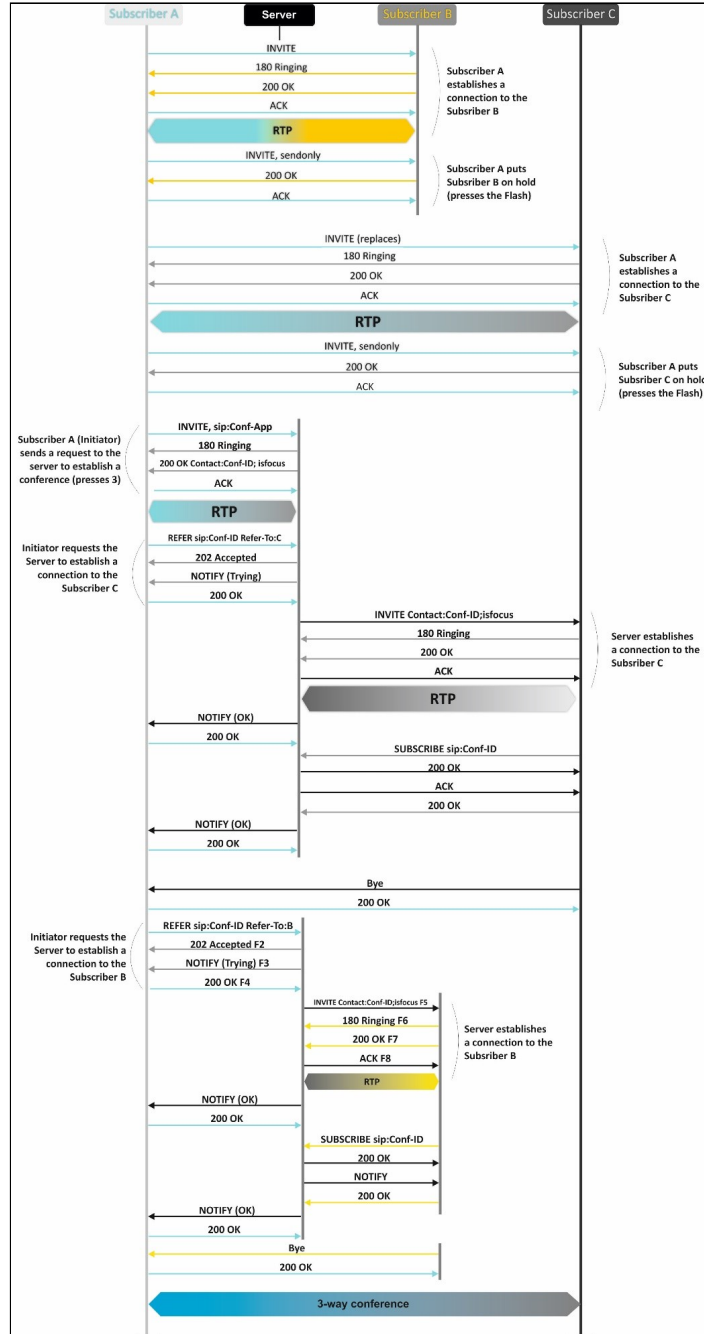
The conference terminates, when initiator leaves; in this case, both participants will receive clearback message. If one of the participants leaves the conference, the initiator and the second participant will switch into a standard two-party call. A short clearback flash is processed as described in the sections "Call Transfer" and "Call Waiting".

The figure below shows an algorithm of "Three-party conference" service performed locally by subscriber B via SIP protocol.



4.3.2 Remote Conference

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

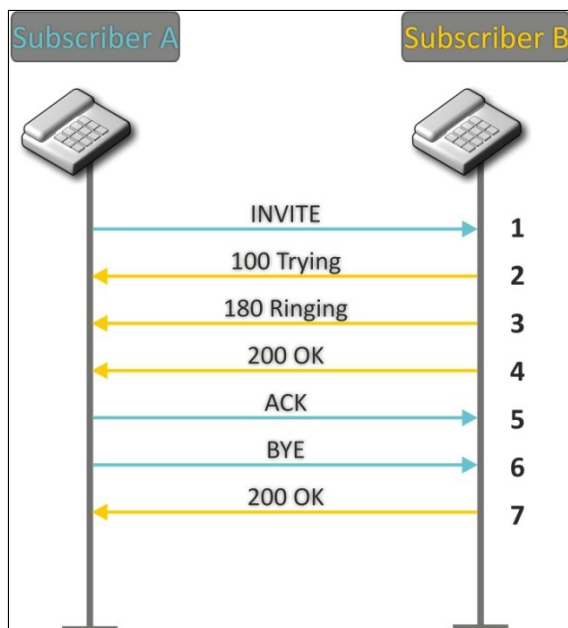


5 Connection Establishment Algorithms

5.1 Algorithm of a Successful Call via SIP Protocol

SIP is a session initiation protocol, that performs basic call management tasks such as starting and finishing session.

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

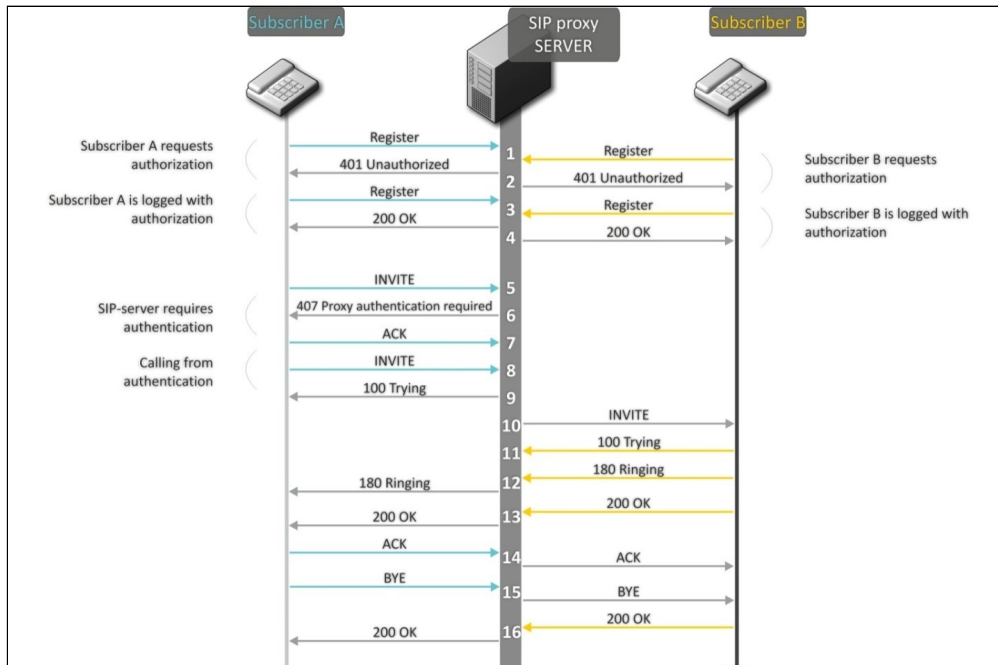


Algorithm description:

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

5.2 Call Algorithm Involving SIP Proxy Server

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

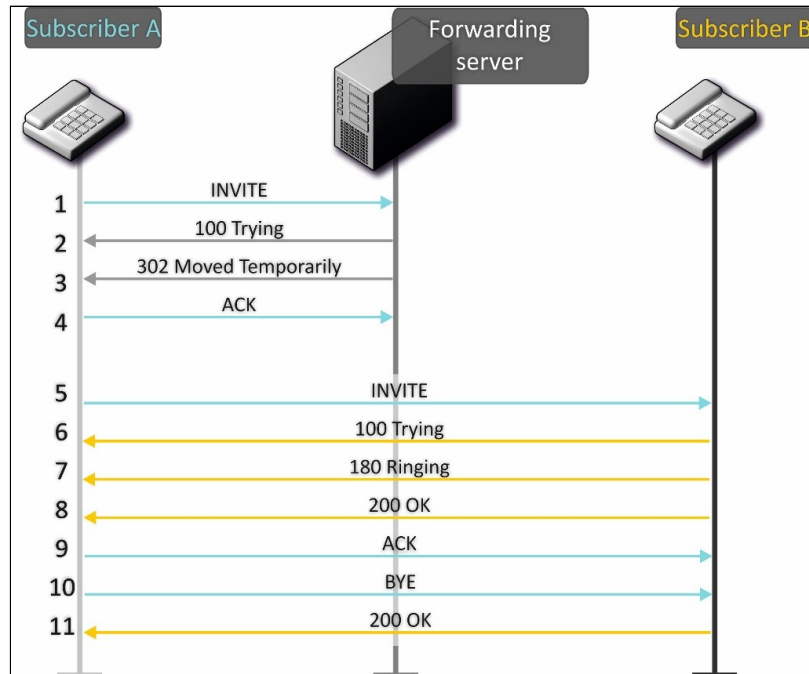


Algorithm description:

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

5.3 Call Algorithm Involving Forwarding Server

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



Algorithm description:

- Subscriber A rings up Subscriber B. The call is sent to forwarding server with the callee address information;
- Forwarding server receives the command for processing;
- Forwarding server requests the information on the Subscriber B current address from the location server; Received information (the callee current address and the list of callee registered addresses) is sent to Subscriber A in "302 moved temporarily" message;
- Subscriber A gateway confirms the reception of reply from the forwarding server;
- Subscriber A rings up Subscriber B directly;
- Subscriber B gateway receives the command for processing;
- Subscriber B is free. At this moment, "ringing" tone is sent to the Subscriber B phone, and "ringback" tone is sent to Subscriber A phone;
- Subscriber B answers the call;
- Subscriber A gateway confirms session establishment;
- Subscriber A clears back, "busy" audio tone is sent to Subscriber B;
- Subscriber B gateway confirms received clearback command.

5.4 DHCP-based Autoprovisioning Algorithm

Device autoprovisioning procedure algorithm is determined by the "Parameters Priority from" parameter value ("System → Autoprovisioning").

If "Static settings" value is selected, then the full path (including the access protocol and server address) to the configuration files and firmware is determined from the "Configuration File" and "Firmware File" parameters. The full path is specified in the URL format (HTTP and TFTP are supported):

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

- <protocol> is protocol that used for downloading the corresponding file from server (supports HTTP and TFTP);
- <server address> is address of the server from which the file should be downloaded (domain name or IPv4);
- <path to file> is path to file on server.

The following macros are allowed in the URL (reserved words, instead of which the device substitutes certain values):

- \$MA – MAC address – instead of this macro, the device inserts its own MAC address in the file URL;
- \$SN – Serial number – instead of this macro, the device inserts its own serial number in the file URL;
- \$PN – Product name – instead of this macro, the device inserts its product name (e.g. TAU-8N.IP) in the file URL;
- \$SWVER – Software version – instead of this macro, the device inserts its software version number in the file URL;
- \$HWVER – Hardware version – instead of this macro, the device inserts its hardware version number in the file URL.

The MAC address, serial number and model name can be found on the monitoring page in the "Device" tab.

URL examples:

tftp://download.server.loc/firmware.file,

http://192.168.25.34/configs/tau8n/my.cfg,
 tftp://server.tftp/\$PN/config/\$SN.cfg,
 http://server.http/\$PN/firmware/\$MA.frm etc.

It is allowed to omit some URL parameters. For example, the configuration file can be specified in this format:

http://192.168.18.6/

or

config_tau8n.cfg

If it is impossible to extract all the parameters required for downloading the file from the configuration or firmware URL file (protocol, server address or path to the file on the server), an attempt to extract an unknown parameter from DHCP option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name) will be made, in case when Internet service is set to receive an address using DHCP (the format and analysis of the DHCP options will be given below). If it is impossible to extract the missing parameter from the DHCP options, the default value will be used:

- For protocol: tftp;
- For server address: update.local;
- For configuration file name: tau8n.cfg;
- For firmware file name: tau8n.fw.

Thus, if the "*Configuration File*" and "*Firmware File*" fields are left empty, options 43 or 66, 67 with the location of these files will not be received via DHCP – the URL of the configuration file will look this way:

tftp://update.local/tau8n.cfg,

and the URL of the firmware file:

tftp://update.local/tau8n.fw.

If "*DHCP options*" value is selected, URL of configuration and firmware files are extracted from DHCP options 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), for which the Internet service must be set to receive the address via DHCP (format and analysis of DHCP options will be given below). If it is not possible to determine any URL parameter from the DHCP options, the default value is used for it:

- For protocol: tftp;
- For server address: update.local;
- For configuration file name: tau8n.cfg;
- For firmware file name: tau8n.fw.

Option 43 format (Vendor specific info)

1|<acs_url>|2|<pcode>|3|<username>|4|<password>|5|<server_url>|6|<config.file>|7|<firmware.file>|9|<manifest.file>

- 1 – autoconfiguration by TR-069 protocol server address code;
 - 2 – code for "Provisioning code" parameter;
 - 3 – code for username for authorization on TR-069 server code;
 - 4 – password for authorization on TR-069 server code;
 - 5 – server address code; server address is specified in URL format: tftp://address or http://address. In the first option, the address of the TFTP server is specified, in the second option HTTP address is specified;
 - 6 – configuration file name code;
 - 7 – firmware file name code;
 - 9 – code of the file name with the description of the firmware version of the device on the server for updating;
- "|" – mandatory separation symbol between codes and suboption values.

⚠ For TR-069 autoconfiguration, suboptions 1, 3 and 4 will be used when the priority from the DHCP options is selected in the "DHCP-based Autoprovisioning" section. Algorithm for determining configuration file URL parameters and firmware from DHCP options 43 and 66.

1. DHCP sharing initialization:

After loading, the device initiates a DHCP sharing.

2. Option 43 analysis:

When option 43 is received, suboptions with codes 5, 6, 7 and 9 are analyzed to determine the server address and the names of the configuration files and firmware.

3. Option 66 analysis:

If option 43 from the DHCP server was not received or received, but the server address could not be retrieved from it, option 66 search is performed. If the firmware file name also failed to get – option 67 search is performed. The TFTP server address and the path to the firmware file are retrieved from them, respectively. Then the configuration and firmware files will be downloaded from the address from option 66 via TFTP.

Configuration update features

The configuration file must be in the .tar.gz format (in this format the configuration is saved via the Web interface in the "System" → "Configuration Management" tab). The configuration downloaded from the server is applied automatically without rebooting the device.

Firmware update features

Manifest file must be in text file format, consisting one line with identifier of firmware version available for download from the auto-update server.

The firmware file must be in the .tar.gz format. After downloading the firmware file, it is unpacked and a version is checked (based on the contents of the version file in the tar.gz archive).

If there is a URL for downloading manifest file in configuration, the firmware file will not be downloaded to check if the version is up to date. Downloading will start only if the firmware version ID in manifest file differs from the current firmware version ID on the device.

If there is no manifest file URL, then the firmware version is checked by downloading the firmware file.

⚠ Do not turn off the power or overload the device while saving the image to flash-memory. These actions will lead to a partial recording of firmware, which is equivalent to damage to the boot partition of the device. If this happens, restore the device power, and it boot from the backup firmware image. To restore the second firmware image, wait 10 minutes and the device will automatically copy the operating firmware image to the backup memory. If the backup area of firmware was also damaged at the update time, then restoring the device`s operability is possible only in a specialized service center.

Do not start device firmware update if the backup area of firmware is damaged. Wait 10 minutes from the moment of successful device startup to restore the backup area and only after that perform the update.

6 System recovery after a firmware update failure

If the firmware update procedure (via Web interface or via DHCP-based autoprovisioning mechanism) fails (for example, due to an accidental power outage), as a result, further device operation became impossible (the "Power" indicator is solid red), use the following device recovery algorithm:

1. Unpack the firmware file;
2. Connect the PC to the device's WAN port, set the address from the 192.168.1.0/24 subnet on the network interface;
3. Run the TFTP client on the PC (it is recommended to use the Tftpd32 for Windows), specify 192.168.1.6 as the remote host address, and select the linux.bin file from the unpacked firmware archive for transfer;
4. Run the command to send a file to a remote host (the Put command). The process of transferring the file to the TAU-8N.IP device should start;
5. If the file transfer process has begun – wait for it to finish, after which the TAU-8N.IP will record the firmware to the memory and automatically start the system. The recording time is about 5 minutes. The successful recovery of the device is indicated by the orange or green color of the "Power" indicator. The device saves the configuration that was before the failure. If you cannot connect to the device, reset to factory settings;
6. If the file transfer process has not started, make sure that computer's network settings are correct and try again. In case of failure the device must be sent for repair or to perform a recovery by connecting to the device via the COM port via a special adapter (if available).

7 APPENDIX A. CALCULATION OF PHONE LINE LENGTH

Table A1 – Electrical resistance/cable core diameter relationship for 1 km of DC subscriber cable lines at ambient temperature +20 °C.

Core diameter, mm	Electrical resistance of 1 km circuit, Ω, max.	Line length (another telephone set), km
0,32	458,0	3,537
0,40	296,0	5,473
0,50	192,0	8,438
0,64	116,0	13,966
0,70	96,0	16,875
0,90	56,8	28,521

8 APPENDIX B. RUNNING USER-DEFINED SCRIPT UPON SYSTEM STARTUP

Periodically, it is necessary to perform certain actions at device startup, which cannot be performed by specifying certain settings via the configuration file. For this case, TAU-8N.IP device provides the ability to configure the startup of a user-defined script through the configuration file, in which you can put any desired sequence of commands.

To run a user-defined script, a settings section has been created in the configuration file:

```
UserScript:
```

```
Enable: "0"
```

```
URL: ""
```

The "Enable" option allows (if the value is 1) or denies (if the value is 0) the script startup, the path to which is specified in the URL parameter.

The script can be located both on remote server and on the device itself. The script can be downloaded via HTTP or TFTP from remote server. Consider the examples of the configuration file to run a custom script from different sources.

1. Run from HTTP server

To run the script from the HTTP server, it is necessary to specify the full path to the file in the format of the HTTP URL in the URL parameter:

```
URL: "http://192.168.0.250/user-script/script.sh"
```

In this case, after the device starts, the script.sh file stored in the user-script directory at 192.168.0.250 will be automatically downloaded via HTTP from the specified server, after which it will be launched.

2. Run from TFTP server

To run the script from the TFTP server, it is necessary to specify the full path to the file in the format of the TFTP URL in the URL parameter:

```
URL: "tftp://192.168.0.250/user-script/script.sh"
```

In this case, after the device starts, the script.sh file stored in the user-script directory at 192.168.0.250 will be automatically downloaded via TFTP from the specified server, after which it will be launched.

3. Running a local script

Due to the file system features, the local script should be located only in the /etc/config directory, since only the contents of this directory are saved after the device is rebooted. The script in the /etc/config directory can be created either using the "vi" editor, or download it from an external TFTP server (using the `tftp -gl user.sh <TFTP-server address>` command). After creating the script, it needs to assign launch permissions with command `chmod 777 /etc/config/ user.sh`.

In the configuration file, the URL to run a local script is:

```
URL: "File://etc/config/user.sh"
```

It is important to note that the user script must begin with the directive `#!/bin/sh`.

9 APPENDIX C. DHCP CLIENTS CONFIGURATION IN MULTISERVICE MODE

On TAU-8N.IP devices it is possible to configure the options received by DHCP clients on different interfaces.

Option	Только интерфейс Internet	Internet + VoIP	
		Internet	VoIP
1 = Subnet Mask	+	+	+
3 = Router	+	+	+
6 = Domain Name Server	+	+	+
12 = Host Name	+	+	-
15 = Domain Name	+	+	-
26 = Interface MTU	+	+	+
28 = Broadcast Address	+	+	+
33 = Static Route	+	+	+
40 = Network Information Service Domain	+	+	-
41 = Network Information Service Servers	+	+	-
42 = Network Time Protocol Servers	+	+	-
43 = Vendor-Specific Information	+	+	-
66 = TFTP Server Name	+	+	-
67 = Bootfile name	+	+	-
120 = SIP Servers	+	-	+
121 = Classless Static Route	+	+	+
249 = Private/Classless Static Route (Microsoft)	+	+	+

According to the table, options 1, 3, 6, 26, 28, 33, 121, 249 can be requested by DHCP clients for each subinterface. Accordingly, these options will be individually applied for each subinterface. Options 12, 15, 40, 41, 42, 43, 66, 67, 120 can be requested and used only for one DHCP client, since they are system-wide, that is, they do not lead to the network interface configuration. The requested options list configuration can be changed and it is stored like all other settings in the configuration file: /etc/config/cfg.yaml. By default, the option lists are not specified (the configuration contains the following entry: DHCPOptionList: ""), this means that the options are requested and applied according to the table above.

Configuration editing methods

Using the vi editor

1. The list of options for the Internet interface is specified in the DHCPOptionList parameter of the "*Internet* → *Network*" section.
2. The list of options for the VoIP interface is specified in the DHCPOptionList parameter of the "*VoIP* → *Network*" section.

After editing and saving in the vi editor, it is necessary to run the following commands:

reloadcfg – apply the modified configuration to work, the result of the command should be "Configuration accepted";

save – save the changed configuration in non-volatile memory.

⚠ The save command can only be executed if the previous command is successful. If the result was "Configuration not accepted" when executing the reloadcfg command, save is forbidden.

Using setconf command

✔ This method is recommended. It also eliminates the necessity to execute the reloadcfg and save commands. getconf (display current configuration) and setconf (set parameter value).

Example 1. To get the DHCPOptionList value:

for Internet interface

```
getconf Internet.Network | grep DHCPOptionList
```

for VoIP interface

```
getconf Voip.Network | grep DHCPOptionList
```

Example 2. To assign some list of options:

for Internet interface

```
setconf Internet.Network DHCPOptionList "3,6,26,28,33,121,249,12"
```

for VoIP interface (assign the default list of options)

```
setconf Voip.Network DHCPOptionList ""
```

Configuration on PC

The configuration is to be pre-downloaded from the device to the PC (via the web interface), then with the help of any text editor the values are to be changed and saved. The final step is to upload the changed configuration to the device.

⚠ This method is not recommended!

DHCPOptionList Editing Rules

Permitted parameter values: 3,6,12,15,26,28,33,40,41,42,43,66,67,120,121,249;

The options in the DHCPOptionList parameter are separated by commas and no spaces between the options, an example of a DHCPOptionList: "3,6,12,15,26,120,121";

The order of options in DHCPOptionList is not important;

Each of the options 12, 15, 40, 41, 42, 43, 66, 67, 120 can be requested and applied from only one interface;

Options 1, 3, 6, 26, 28, 33, 121, 249 can be requested by DHCP clients for each subinterface; Options 66 and 67 must be specified on the same interface;

Options 66 and 67 must be specified on the same interface;

If nothing is specified in the DHCPOptionList, then the list of requested options will be default (subject to step 8);

If the DHCPOptionList specifies the options (from step 4), which by default are requested from another interface (on which the DHCPOptionList is empty), then the options will be requested from the first interface, and on the second from the default list these options will be excluded;

If a list of options is specified for the interface in the DHCPOptionList, then only these options will be requested;

Option 1 cannot be specified in the DHCPOptionList, it is requested and applied always and from all interfaces regardless of other settings.

⚠ After editing the DHCPOptionList, device reboot is recommended. Correct device operation is not guaranteed before reboot.

10 APPENDIX D. USING THE COMMAND LINE INTERFACE (CLI) FOR CONFIGURATION AND MONITORING

Information on using the CLI for configuration and monitoring is available at this [link](#).

TECHNICAL SUPPORT

For technical assistance in issues related to handling Eltex Ltd. equipment, please, address to Service Center of the company:

<https://eltex-co.com/support/>

You are welcome to visit Eltex official website to get the relevant technical documentation and software, to use our knowledge base or consult a Service Center Specialist.

<http://www.eltex-co.com/>

<http://www.eltex-co.com/support/downloads/>