

# TAU-4M.IP

## Operation Manual

Firmware version 2.3.1

---

VoIP Gateway

IP address: **http://192.168.1.1**  
Username: **admin**  
Password: **password**

Document version	Issue data	Revisions
Version 1.3	30.04.2020	Updated according to firmware version 2.3.1
Version 1.2	31.01.2020	Updated according to firmware version 2.3.0
Version 1.1	28.05.2018	Updated according to firmware version 2.1.0
Version 1.0	15.01.2018	First issue
<b>Firmware version</b>	Firmware version: 2.3.1.4 Web-interface version: 2.3.0.54	

## SYMBOLS

Symbol	Description
<b>Bold font face</b>	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



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.

## TABLE OF CONTENTS

INTRODUCTION .....	6
1 PRODUCT DESCRIPTION .....	7
1.1 Purpose.....	7
1.2 Device specification .....	7
1.3 Device Design and Operating Principle .....	9
1.4 Main Specifications.....	11
1.5 Design .....	12
1.5.1 Top panel of the device .....	12
1.5.2 Rear panel of the device .....	13
1.6 Light indication .....	13
1.7 Reset to factory settings.....	14
1.8 Delivery Package.....	14
2 DEVICE MANAGEMENT VIA WEB CONFIGURATOR.....	15
2.1 Getting started.....	15
2.2 Changing users.....	15
2.3 WEB interface operation modes .....	16
2.4 Applying and discarding changes made to configuration .....	17
2.4.1 Applying configuration.....	17
2.4.2 Discarding changes .....	17
2.5 'Quick configuration' menu .....	18
2.5.1 Internet .....	18
2.5.2 VoIP .....	21
2.5.3 IPTV .....	22
2.5.4 System.....	22
2.6 Advanced settings.....	23
2.6.1 WEB interface basic elements .....	23
2.6.2 'Network' menu .....	23
2.6.3 'VoIP' menu .....	45
2.6.4 'IPTV' menu .....	74
2.6.5 'System' menu.....	75
2.7 System Monitoring .....	94
2.7.1 'Internet' submenu .....	94
2.7.2 'VoIP' submenu .....	95
2.7.3 'Ethernet Ports' submenu .....	98
2.7.4 'DHCP' submenu .....	99
2.7.5 'ARP' submenu .....	99
2.7.6 'Device' submenu.....	100
2.7.7 'CPU' submenu .....	100
2.7.8 'Conntrack' submenu .....	101
2.7.9 'Routes' submenu .....	102
2.7.10 'Call History' submenu .....	103
2.7.11 'Diagnostics' submenu .....	104
2.8 Configuration example .....	105
3 VALUE ADDED SERVICES USAGE .....	108
3.1 Call Transfer .....	108
3.2 Call Waiting.....	111
3.3 Three-way conference.....	111
3.3.1 Local conference .....	111
3.3.2 Remote conference .....	113
4 CONNECTION ESTABLISHMENT ALGORITHMS.....	114
4.1 Algorithm of a Successful Call via SIP Protocol.....	114
4.2 Call Algorithm Involving SIP Proxy Server.....	115

---

4.3 Call Algorithm Involving Forwarding Server .....	116
5 DEVICE AUTOMATIC UPDATE ALGORITHM BASED ON DHCP .....	117
6 SYSTEM RECOVERY AFTER A FIRMWARE UPDATE FAILURE.....	120
APPENDIX A. CALCULATION OF PHONE LINE LENGTH .....	121
APPENDIX B. RUNNING USER-DEFINED SCRIPT UPON SYSTEM STARTUP.....	122
APPENDIX C. DHCP CLIENTS CONFIGURATION IN MULTISERVICE MODE .....	123

## INTRODUCTION

Today, VoIP is one of the most rapidly evolving telecommunication services. *TAU-4M.IP* series gateways (hereinafter the "device") are designed to provide VoIP services to the network clients.

*TAU-4M.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-4M.IP* VoIP gateways.

## 1 PRODUCT DESCRIPTION

### 1.1 Purpose

*TAU-4M.IP* is a high-performance VoIP gateway with the full set of features that allow users to take advantage of VoIP functionality.

*TAU-4M.IP* gateway allows connecting an analogue phone or a fax modem to IP networks. With a built-in router, the device enables connection of local network equipment to a broadband access network. It is possible to connect one PC that will be able to access the Internet using integrated NAT/DHCP server features. The USB port is used to connect external drive, 3G/4G USB modem.

### 1.2 Device specification

#### **Interfaces:**

- FXS: 4 x RJ-11 ports
- LAN: 1 x Ethernet RJ-45 10/100BASE-T port
- WAN: 1 x Ethernet RJ-45 10/100BASE-T port
- USB: 1 x USB2.0 port

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

#### **Functions:**

- Network functions:
  - Operation in 'bridge' or 'router' mode;
  - PPPoE support (PAP, SPAP and CHAP authorization, PPPoE compression);
  - PPTP support;
  - L2TP support;
  - Static IP address and DHCP support (DHCP client on WAN side, DHCP server on LAN side);
  - DNS support;
  - NAT support;
  - Firewall;
  - NTP support;
  - QoS support (QoS via DSCP and 802.1P);
- IPTV function support;
- 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;
- Operation w/ and w/o a SIP server;
- Value Added Services (VAS):
  - 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-way conference call;
  - Flexible dial plan;
- Firmware update via web interface;
- DHCP-based auto provisioning support;
- TR-069;
- Remote monitoring, configuration and setup: web-interface, Telnet.

Figure1 shows *TAU-4M.IP* connection diagram.

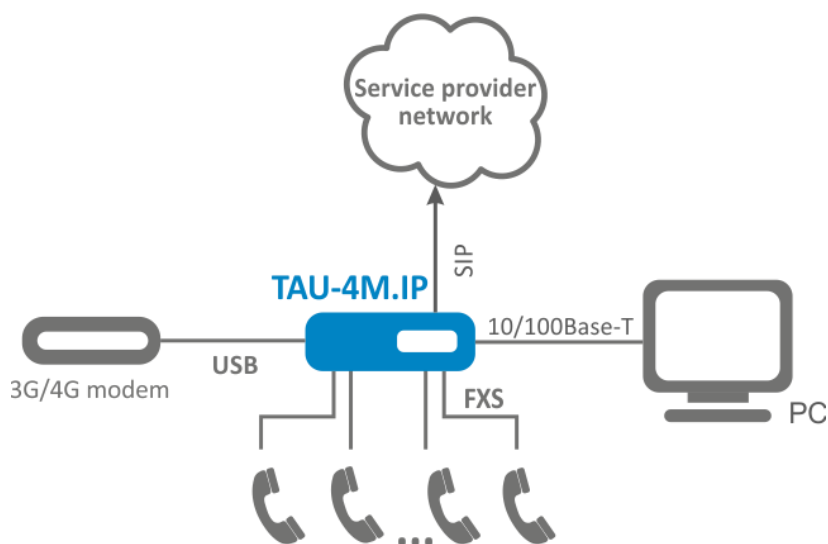


Figure 1 – *TAU- 4M.IP* operation diagram



### 1.3 Device Design and Operating Principle

TAU-4M.IP terminal consists of the following subsystems:

- Controller that includes:
  - Flash memory – 8MB;
  - SDRAM – 128MB.
- 4 x SLIC subscriber units;
- 1 x LAN port RJ-45 10/100BASE-T;
- WAN Ethernet module: RJ-45 10/100BASE-T;
- USB Host port.

Block diagram for the device is shown in Figure2.

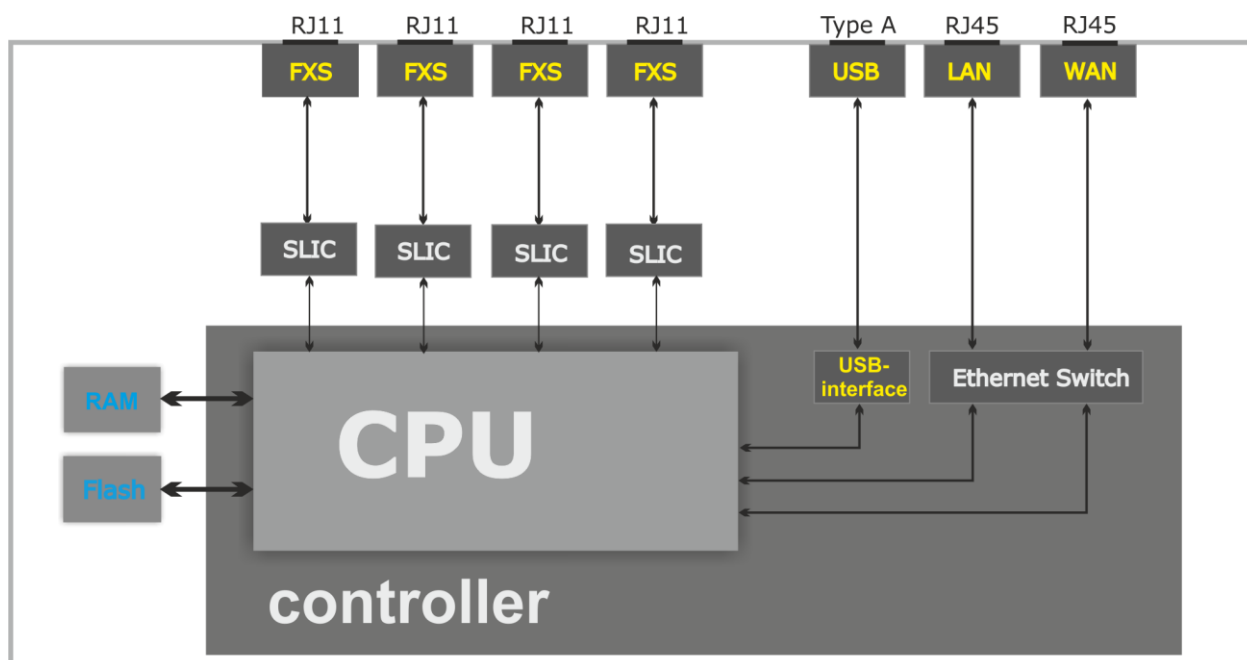


Figure 2 – TAU- 4M.IP design diagram

The device runs under Linux operating system. Basic control functions are performed by Realtek processor which enables IP packet routing, VoIP operation, group traffic proxying and etc.

The device may functionally be divided into four blocks:

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

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

**VoIP block** enables SIP protocol 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.

**Multicast traffic processing block** enables processing of IGMP messages and multicast traffic for IPTV functions support.

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

Fig 3 shows *TAU-4M.IP* functional diagram.

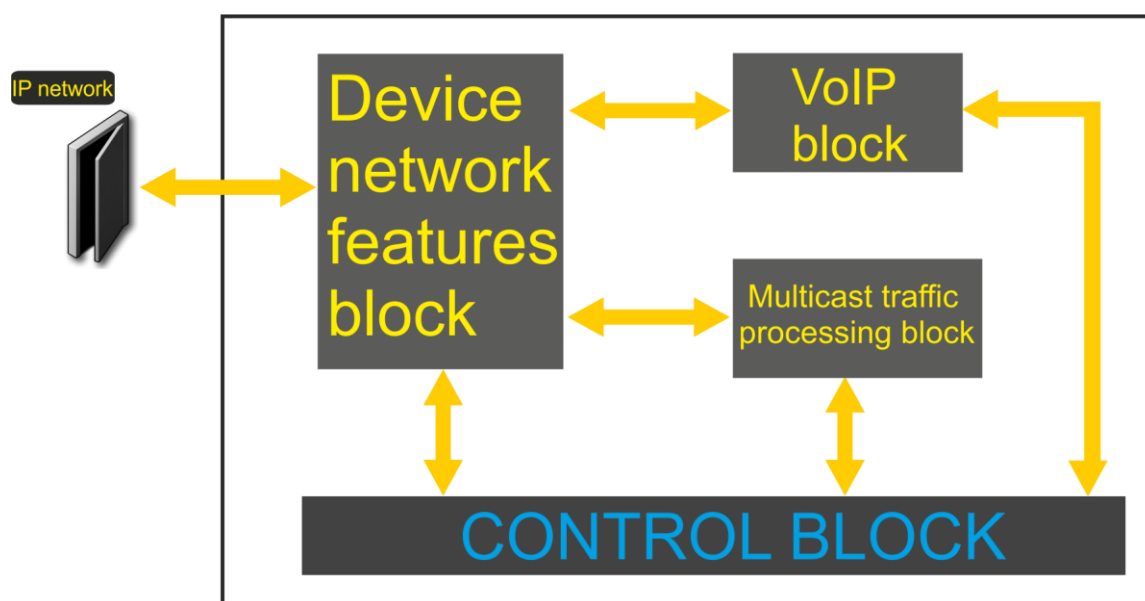


Figure 3 – *TAU- 4M.IP* functional diagram

## 1.4 Main Specifications

Table 1 contains 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.722, G.726-24, G.726-32 Modem transmission: G.711a, G.711u Fax transmission: G.711a, G.711u, T.38
--------	------------------------------------------------------------------------------------------------------------------------------------------------------------------

### Ethernet WAN interface specifications:

Number of ports	1
Electrical connector	RJ-45
Data rate, Mbps	10/100, autodetection
Supported standards	BASE-T

### Ethernet LAN interface specifications:

Number of interfaces	1
Electrical connector	RJ-45
Data rate, Mbps	10/100, autodetection
Supported standards	BASE-T

### Analogue user port specifications

Number of ports	4
Loop resistance (phone resistance excluded)	up to 800 $\Omega$
Dialling reception	pulse/frequency (DTMF)
Subscriber terminal protection	current and voltage
Caller ID broadcasting	FSK BELL202/FSK V.23/DTMF

### Control

Remote control	web interface, Telnet, SSH, SNMP, TR-069
Access restriction	password

### General parameters

Power supply	power adapter 12V DC, 2.0 A.
Power consumption	up to 12.5 W (max. current consumption is 1.1A)
Operation temperature range	from +5 to +40°C
Relative humidity at 25°C	up to 80%
Dimensions	187x120x32.5 mm
Weight	0.25 kg

## 1.5 Design

*TAU-4M.IP* subscriber terminal is enclosed into 187x120x32.5 mm plastic housing.

### 1.5.1 Top panel of the device

The *TAU-4M.IP* top panel appearance is shown in Figure 4.

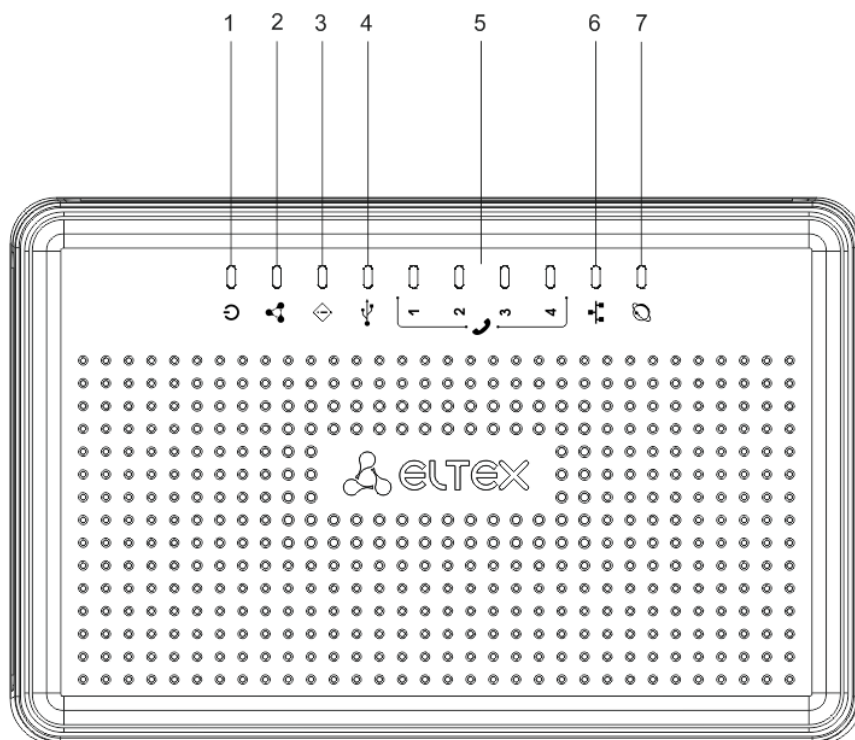



Figure 4 - *TAU-4M.IP* top panel appearance

Connectors, LEDs and controls located on *TAU-4M.IP* top panel are described in Table 2:

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

Top panel of the device		Description
1	Power	Device power and operation status indicator
2	Status	Device operation status indicator
3	Alarm	Device alarm indicator (indicator is disabled in the firmware version 2.3.1)
4	USB	External USB device operation indicator (USB flash, external HDD, 3G/4G USB modem)
5		Analogue phone indicators
6	LAN	LAN interface indicator
7	WAN	WAN interface indicator

## 1.5.2 Rear panel of the device

The *TAU-4M.IP* rear panel appearance is shown in Figure 5.

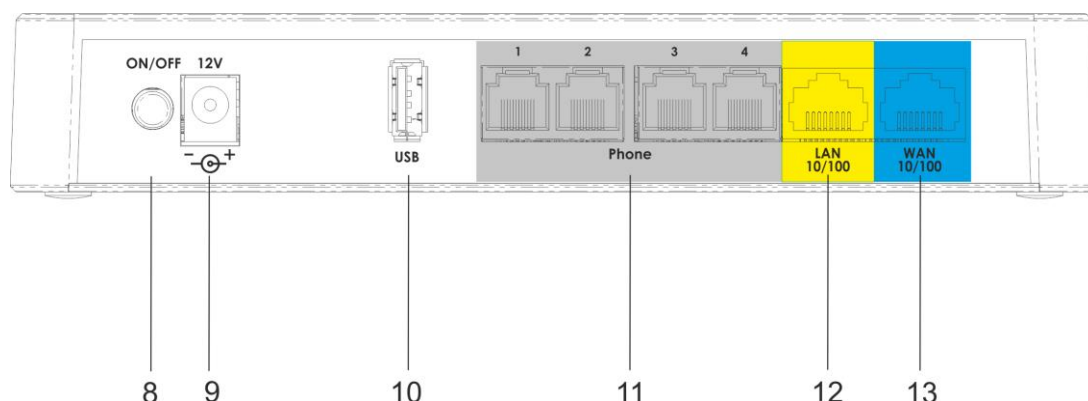


Figure 5 - *TAU-4M.IP* rear panel appearance

Connectors and controls located on *TAU-4M.IP* rear panel are described in Table 3.

Table 3 – Description of connectors and controls located on *TAU-4M.IP* rear panel

Rear panel element		Description
8	ON/OFF	ON/OFF switch
9	12V	Power adapter connector
10	USB	USB port for external USB device connection (USB flash, external HDD, 3G/4G USB modem)
11	Phone	4 x RJ-11 ports for analogue phone connection
12	LAN	10/100BASE-T Ethernet (RJ-45) port for local network device connection
13	WAN	10/100BASE-T Ethernet (RJ-45) port for external network connection

## 1.6 Light indication

**WAN, LAN, Phone, Power** indicators located on *TAU-4M.IP* top panel show the device current status. Table 4 lists possible states of the LEDs.

Table 4 - Light indication of *TAU-4M.IP* states

Indicator	Indicator State	Device state
WAN	Solid (green - 10 Mbps, orange - 100Mbps)	Connection between station terminal and subscriber device is established
	Flashes	Packet data transmission via WAN interface
LAN	Solid (green - 10 Mbps, orange - 100Mbps)	Connection to the network device is established
	Flashes	Packet data transmission via LAN interface
	Green, solid	Phone is off-hook (line is active)
	Off	Phone is on-hook, normal operation
	Green, flashes with 20Hz frequency for second, then 4seconds 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
Alarm	Off	Indication is not available in the firmware version 2.3.1
Status	Green, solid	Normal device operation
	Green, solid	Internet is not accessible
	Red, solid	Device starts up
	Flashes red and green intermittently in periods	Device is being reset to factory settings
Power	Red	Device power supply is on

## 1.7 Reset to factory settings

In order to reset the device to factory settings, press the 'F' button located on the device side panel when the device is powered up and hold it until the 'Power' indicator begins to flash red and green intermittently. Device will be rebooted automatically. Factory settings: DHCP client is launched on WAN interface, LAN interface address—192.168.1.1, subnet mask—255.255.255.0; username/password for web interface access: admin/password.

## 1.8 Delivery Package

*TAU-4M.IP* standard delivery package includes:

- Multi-purpose subscriber terminal;
- 220/12 V, 2 A power adapter;
- Installation and configuration guide.

## 2 DEVICE MANAGEMENT VIA WEB CONFIGURATOR

### 2.1 Getting started

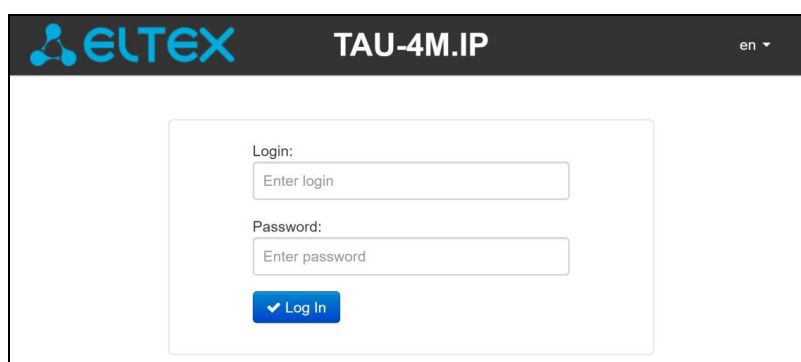
In order to start the operation, you should connect to the device via LAN interface using a web browser:

1. Open a web browser (hypertext document viewer).
2. Enter the device IP address in the browser address bar.



**Factory default IP address: 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*.**

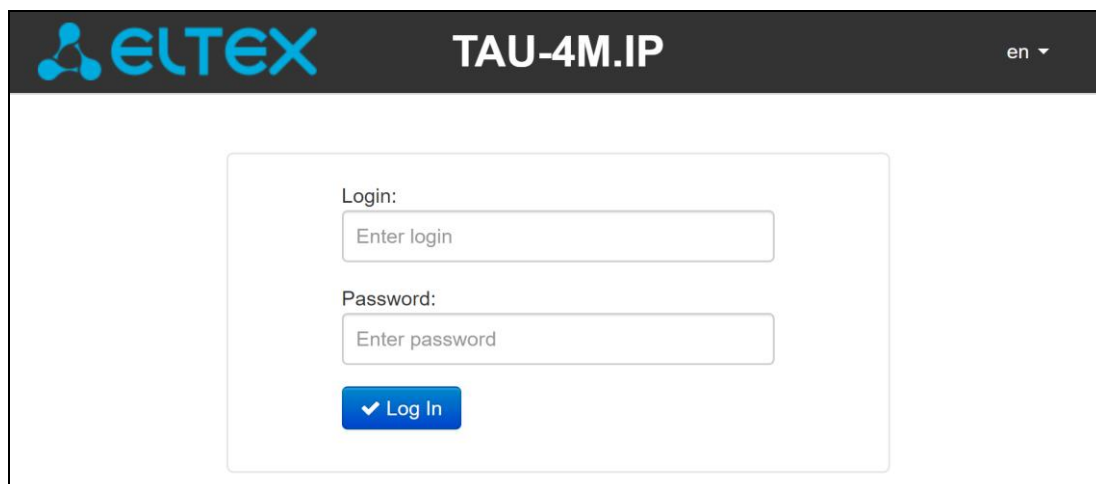
4. Click the 'Log in' button. The quick configuration menu will be shown in the browser window, see Figure 6.

### 2.2 Changing users

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



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



The login page for TAU-4M.IP features a dark header with the ELTEX logo and the text 'TAU-4M.IP'. A language dropdown menu is set to 'en'. The main content area contains a login form with the following elements:

- Login:** A text input field with the placeholder 'Enter login'.
- Password:** A text input field with the placeholder 'Enter password'.
- Log In:** A blue button with a white checkmark icon and the text 'Log In'.

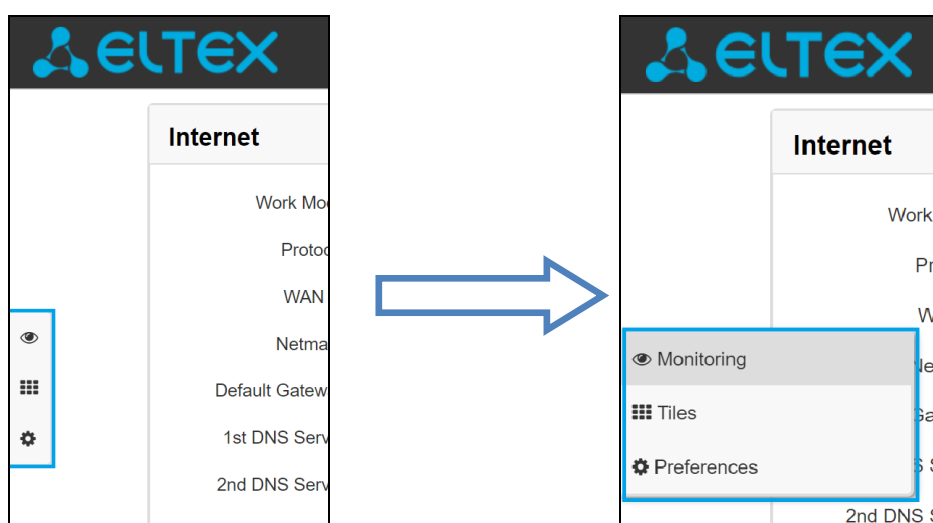
To change the access, you should specify the corresponding username and password and click the *Log in* button.

## 2.3 WEB interface operation modes

TAU-4M.IP WEB interface can operate in three modes:

- **Monitoring** – system monitoring mode – allows viewing 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, IPTV and etc. A tile only displays basic parameters that allow the quickest possible configuration of a specific device function.
- **Settings** – advanced system configuration mode (full configuration mode) – 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 move a mouse cursor on it.



To proceed from the Tiles mode into Settings, you may also click 'more' link in the tile.



## 2.4 Applying and discarding changes made to configuration

### 2.4.1 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.

'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 Table 5.

Table 5 – Visual indication of the current status of the setting application process

Appearance	Description
	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.
	Successful settings saving and application are indicated by  icon in the tab name.
	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.

### 2.4.2 Discarding changes



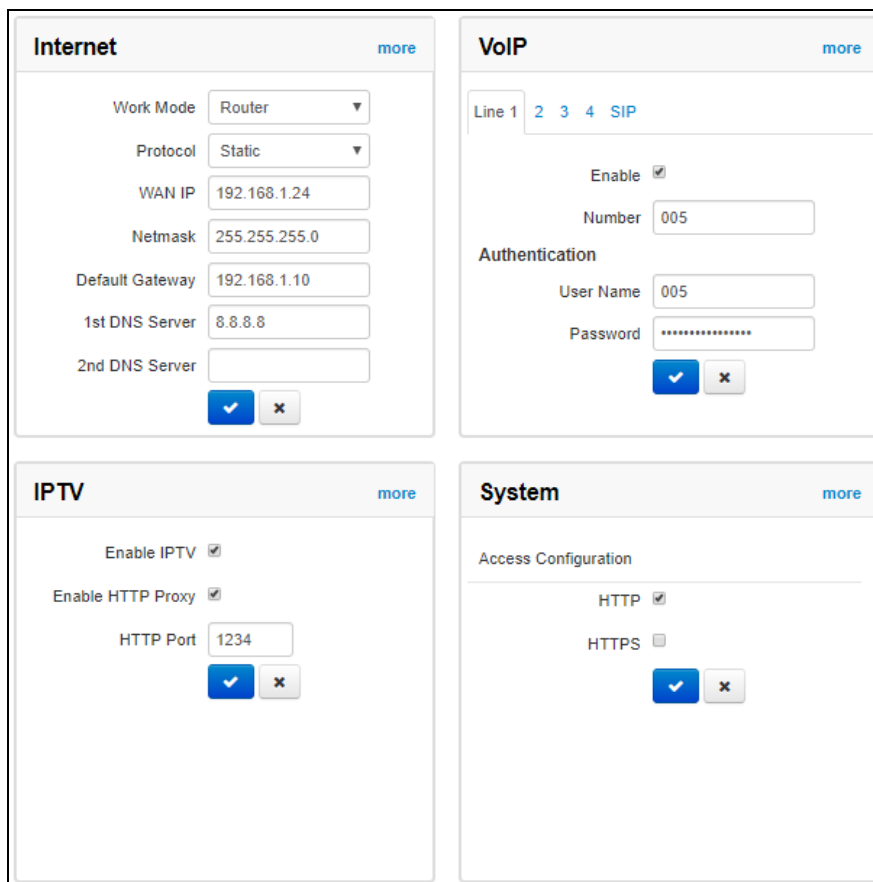
You may discard changes only until 'Apply' button is clicked. In this case, edited parameters on the page will be updated with the values currently stored in the device memory. After you click 'Apply', you will not be able to restore previous settings.

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



## 2.5 'Quick configuration' menu

In the quick configuration menu, you will find basic device settings, see Figure 6.



The screenshot displays the 'Quick configuration' menu with four main sections, each with a 'more' link in the top right corner:

- Internet:** Contains fields for Work Mode (Router), Protocol (Static), WAN IP (192.168.1.24), Netmask (255.255.255.0), Default Gateway (192.168.1.10), 1st DNS Server (8.8.8.8), and 2nd DNS Server (empty). At the bottom are blue checkmark and red X buttons.
- VoIP:** Features a 'Line 1' tab with sub-tabs 2, 3, 4, and SIP. It includes an 'Enable' checkbox (checked), a 'Number' field (005), an 'Authentication' section with 'User Name' (005) and 'Password' (masked with dots), and blue checkmark and red X buttons at the bottom.
- IPTV:** Includes 'Enable IPTV' (checked), 'Enable HTTP Proxy' (checked), and an 'HTTP Port' field (1234). At the bottom are blue checkmark and red X buttons.
- System:** Shows 'Access Configuration' with 'HTTP' (checked) and 'HTTPS' (unchecked) options. At the bottom are blue checkmark and red X buttons.

Figure 6 – Quick configuration menu

Settings are divided into the following categories:

- *Internet* – quick Internet access configuration;
- *VoIP* – quick VoIP configuration;
- *IPTV* – device configuration to support IPTV features;
- *System* – configure access to web interface via WAN port.

### 2.5.1 Internet

In order to access the Internet, you should specify basic settings in the Internet section. To specify additional parameters, go to advanced settings mode by clicking the 'more' link.

- *Work mode* — the device operation mode:
  - *Router* — router mode is established between LAN and WAN (LAN is isolated from WAN);
  - *Bridge* — bridge mode is established between WAN and LAN interfaces: data is transmitted transparently from LAN to WAN and back.
- *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 (allows identifying 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, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.

Supported options:

- 1 – network mask;
- 3 – default network gateway address;
- 6 – DNS address;
- 12 – device network name;
- 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:serialnumber][WAN:WAN interface MAC address][LAN:LAN interface MAC address][VERSION:firmware version]**

Example:

[VENDOR:Eltex][DEVICE:TAU-4M.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]  
[LAN:02:20:80:a8:f9:4b][VERSION:#2.3.1]

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

- *PPPoE* – operation mode when PPP session is established on WAN interface. When PPPoE is selected, the following parameters will be 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.  
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, Subnet mask, DNS, Gateway*.

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

- *PPTP Server* – PPTP server address (domain name or IP address in IPv4 format);
- *User name* – user name for authorization on PPTP server;
- *Password* – password for authorization on PPTP server;
- *Secondary access* — type of access to local network resources and PPTP 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, you should specify PPTP server access settings manually:

- *IP address* – when the static access is used, PPTP server will be accessed from this address;
- *Netmask* – subnet mask for static access;
- *DNS server* – when the static access is used, local area network DNS;
- *Gateway* – when the static access is used, gateway for PPTP server access (if necessary).

- *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, you should specify L2TP server access settings manually:

- *IP address* – when the static access is used, PPTP server will be accessed from this address;
- *Netmask* – subnet mask for static access;
- *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).

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

creation and usage. L2TP over IPSec<sup>1</sup> allows for the higher security level compared to PPTP and provides the higher level of protection for business-critical data.

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

To apply a new configuration and store settings into the flash memory, click . To discard changes click



To connect the device to the provider network, you should request the network settings from the provider. If you use static settings, select 'Static' value in the Protocol field and fill the External IP address, Subnet mask, Default gateway, Primary DNS and Secondary DNS fields with the corresponding values obtained from the provider. If devices in the provider network obtain network settings via DHCP, PPPoE, PPTP, or L2TP — select the corresponding protocol in the Protocol field and refer to provider's instructions to achieve complete and correct device configuration.

## 2.5.2 VoIP


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

In the tabs Line 1, Line 2, Line 3, and Line 4 you may configure the device phone ports Phone1, Phone2, Phone3, and Phone4 respectively:

- *Enable* – when selected, 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:

- *SIP 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 selected, 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 flash memory, click . To discard changes click




<sup>1</sup>Disable sender address translation for correct IPSec operation.

### 2.5.3 IPTV

For IPTV operation, you should specify settings in IPTV section. To specify additional parameters, go to advanced settings mode by clicking the *more* link.

- *Enable IPTV* – when selected, enable IPTV signal transmission from *TAU-4M.IP* WAN interface (from the provider network) to the devices connected to LAN interface.
- *Enable HTTP proxy* – when selected, use HTTP proxy. HTTP proxy transforms UDP stream into HTTP stream in order to improve stream image quality, when the quality of the communication link in local area network is low.
- *HTTP Port* – HTTP proxy port number that will be used for video streaming. Use this port to connect to IPTV streams being broadcast by the device.

For example, if the device address on LAN interface is 192.168.0.1, proxy server port is 2354, and the desired channel 227.50.50.100 is being broadcast to UDP port 1234, you should specify the following stream address for VLC application: `http://@192.168.0.1:2345/udp/227.50.50.100:1234`.

To apply a new configuration and store settings into the flash memory, click . To discard changes click



### 2.5.4 System


In the System section, 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 selected, the WAN port connection to the device WEB configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when selected, the WAN port connection to the device WEB configurator is enabled via HTTPS (insecure connection);



**By default, access to the device WEB interface is enabled only for LAN interface.**

To apply a new configuration and store settings into the flash memory, click . To discard changes click



## 2.6 Advanced settings

To proceed to the advanced settings mode, click *more* link in any tile or select Preferences item on the left panel.

### 2.6.1 WEB interface basic elements

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

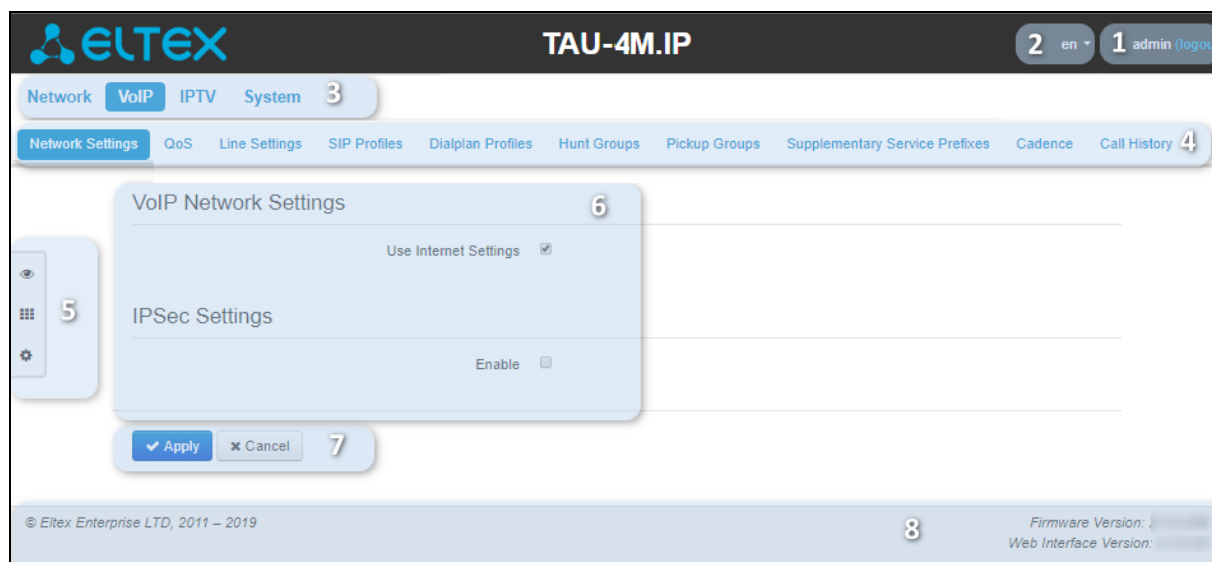


Figure 7 – Web configurator navigation elements

User interface window is divided into eight general areas:

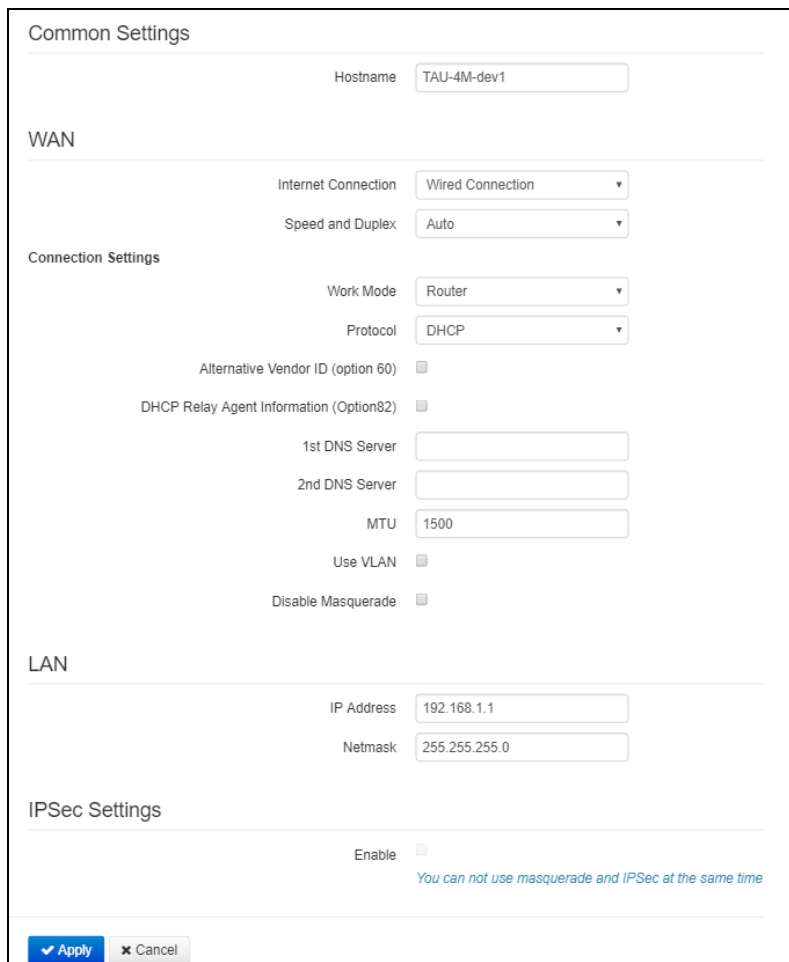
1. Logged in user name and session termination button in the web interface ('Sign Out') for the current user.
2. Changing the user interface language. One of two languages is available: Russian (ru) or English (eng).
3. Menu tabs include submenu tabs grouped by category: **Network, VoIP, IPTV, System**.
4. Submenu tabs allow you to control settings field.
5. WEB configurator mode changing panel (to get more details, see Section **2.3 WEB interface operation modes**).
6. Device settings field based on the user selection; allows you to view device settings and enter configuration data.
7. Configuration management buttons; for detailed description, see Section **2.4 Applying and discarding changes made to configuration**.
  - *Apply* — apply and save the current configuration into flash memory of the device;
  - *Discard* — discard changes (effective only until 'Apply' button is clicked).
8. Informational field showing firmware version and WEB interface version.

### 2.6.2 'Network' menu

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

### 2.6.2.1 'Internet' submenu

In the 'Internet' submenu, you may configure an external network (via PPPoE, DHCP, PPTP, L2TP, statically, in the router or bridge mode) and LAN.



#### Common settings

- Host name – device network name.

#### WAN

- *Internet connection* – external network connection method for the device:
  - *Wired connection* – connection to the Internet is established using 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 the backup channel* – the connection to the Internet is carried out 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 backup 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* – 100Mbps data transfer rate with half-duplex mode is supported;



- *100 Half* – 100Mbps data transfer rate with duplex mode is supported;
- *10 Half* – 10Mbps data transfer rate with half-duplex mode is supported;
- *10 Full* – 10Mbps data transfer rate with duplex mode is supported;

### Connection settings

When you choose **Wired connection** method, the following connection settings will become available:

- **Work mode** — the device operation mode:
  - *Router* — router mode is established between LAN and WAN (LAN is isolated from WAN);
  - *Bridge* — bridge mode is established between WAN and LAN interfaces: data is transferred transparently from LAN to WAN and back—in fact, the device operates in the switch mode.

When you choose *Router* operation mode, the following connection settings will become available:

- **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 (allows identifying 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, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from DHCP server.

Supported options:

- 1 – network mask;
- 3 – default network gateway address;
- 6 – DNS address;
- 12 – device network name;
- 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;

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

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

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

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

Example:

[VENDOR:Eltex][DEVICE:TAU-4M.IP][HW:1.0][SN:VI23000118]  
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.3.1]

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

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

- *1st DNS Server, 2nd DNS Server* – DNS Ip address – if DNS addresses are not automatically assigned via DHCP, you should defined them manually. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.
- *PPPoE* – operation mode when PPP session is established on WAN interface. When PPPoE is selected, the following parameters will be available for editing:
  - *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 button “Connect tunnel”;
  - *Idle* – the period of time after which a PPPoE session is terminated;
  - *LCP echo interval* – LCP request period;
  - *LCP echo failure* – the number of missed LCP requests after which a PPPoE session is terminated;
  - *Secondary access* – type of access to local network resources. You may select from 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, Subnet mask, DNS, Gateway*;

- *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);

- *Traffic hardware acceleration* – increase device bandwidth for PPP traffic (if *PPP* is selected) or IPoE traffic (if *Ethernet* is selected) transmission depending on the selected value.
- *PPTP* – operation mode when the Internet access is established via a tunnel, using PPTP. When *PPTP* is selected, the following parameters will be available for editing:
  - *PPTP Server* – PPTP server IP address;
  - *User name* – user name for authorization on PPTP server;
  - *Password* – password for authorization on PPTP server;
  - *MTU* – maximum block size for data transmitted via the network (1462 is recommended);
  - *Connection Type* – depending on the value chosen, a PPTP session is always established (AlwaysOn), initiated when traffic should be transmitted (OnDemand) or established/terminated manually using the button “Connect tunnel”;
  - *Idle* – the period of time after which a PPTP session is terminated;
  - *LCP echo interval* – LCP request period;
  - *LCP echo failure* – the number of missed LCP requests after which a PPTP session is terminated;
  - *Secondary access* — type of access to local network resources and PPTP 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, you should specify PPTP server access settings manually:

- *IP address* – when the static access is used, PPTP server will be accessed from this address;
- *Netmask* – subnet mask for static access;
- *DNS server* – when the static access is used, local area network DNS;
- *Gateway* – when the static access is used, gateway for PPTP 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) is used;

Hardware traffic acceleration – works only for secondary access interface (IPoE).

- *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);
  - *Connection Type* – depending on the value chosen, a PPTP session is always established (AlwaysOn), initiated when traffic should be transmitted (OnDemand) or established/terminated manually using the button “Connect tunnel”;
  - *Idle* – the period of time after which a L2TP session is terminated;
  - *LCP echo interval* – LCP request period;
  - *LCP echo failure* – the number of missed LCP requests after which a L2TP session is terminated;
  - *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, you should specify L2TP server access settings manually:

- *IP address* – when the static access is used, PPTP server will be accessed from this address;
- *Netmask* – subnet mask for static access;
- *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) is used;

Hardware traffic acceleration – works only for secondary access interface (IPoE).

PPTP and L2TP allow establishing secure communication link over the Internet between the remote user's computer and organization's private network. PPTP and L2TP are based on Point-to-Point Protocol (PPP) and act as its extension. First, the OSI model higher level data is encapsulated into PPP, and then into PPTP or L2TP for tunnel transmission via public data networks. PPTP and L2TP functionality differs. L2TP may be used not only in IP networks, service messages for tunnel creation and data transfer use the same format and protocols. PPTP may be used only in IP networks, it requires a dedicated TCP connection for tunnel creation and usage. L2TP over IPSec<sup>2</sup> allows for the higher security level compared to PPTP and provides the higher level of protection for business-critical data.

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

- *Use VLAN* – when the checkbox is selected, use VLAN ID specified in the 'VLAN ID' field for Internet connection.
  - *VLAN ID* – VLAN ID 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.

- *Disable Masquerade* – when selected, disable source address substitution for packets sent from LAN (disables masquerading).

When you choose '*Bridge*' operation mode, the following connection settings will be available:

- *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:
    - *IP address* – specify device WAN interface IP address in the provider network;
    - *Netmask* – external subnet mask;

<sup>2</sup> Disable sender address translation for correct IPSec operation.

- *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 (allows 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, subnet mask, DNS address, default gateway and other necessary settings for network operation are automatically obtained from
  - *Alternative Vendor ID (Option 60)* — when selected, the device transmits *Vendor ID (Option 60)* in *Option 60 DHCP messages (Vendor class ID)*. If the field is empty, Option 60 will not be transmitted in DHCP messages.

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

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

Example:

[VENDOR:Eltex][DEVICE:TAU-4M.IP][HW:1.0][SN:VI23000118]  
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.3.1]

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

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

*1st DNS Server, 2nd DNS Server*— DNS Ip address — if DNS addresses are not automatically assigned via DHCP, you should define them manually. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.

- *PPPoE* — operation mode when PPP session is established on WAN interface. When PPPoE is selected, the following parameters will be available for editing:
  - *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);
  - *LCP echo interval* — LCP request period;
  - *LCP echo failure* — the number of missed LCP requests after which a PPPoE session is terminated;

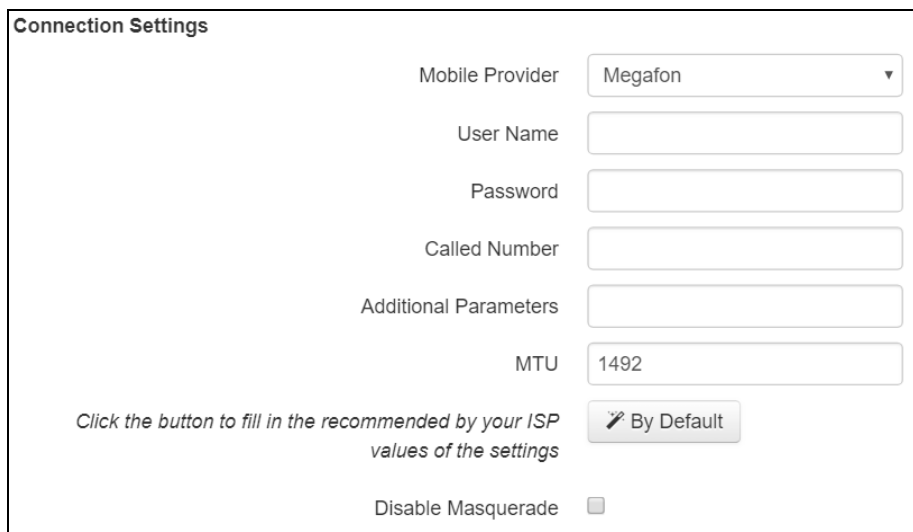


**When PPPoE is selected in bridge mode, the connection type will always be AlwaysOn.**

- *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* – 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;
  - *Primary DNS, Secondary DNS* – domain name server addresses (allows identifying the IP address of the device by its domain name). You may leave these fields empty, if they are not required.

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



**Connection Settings**

Mobile Provider: Megafon

User Name:

Password:

Called Number:

Additional Parameters:

MTU: 1492

Click the button to fill in the recommended by your ISP values of the settings

Disable Masquerade: ☐

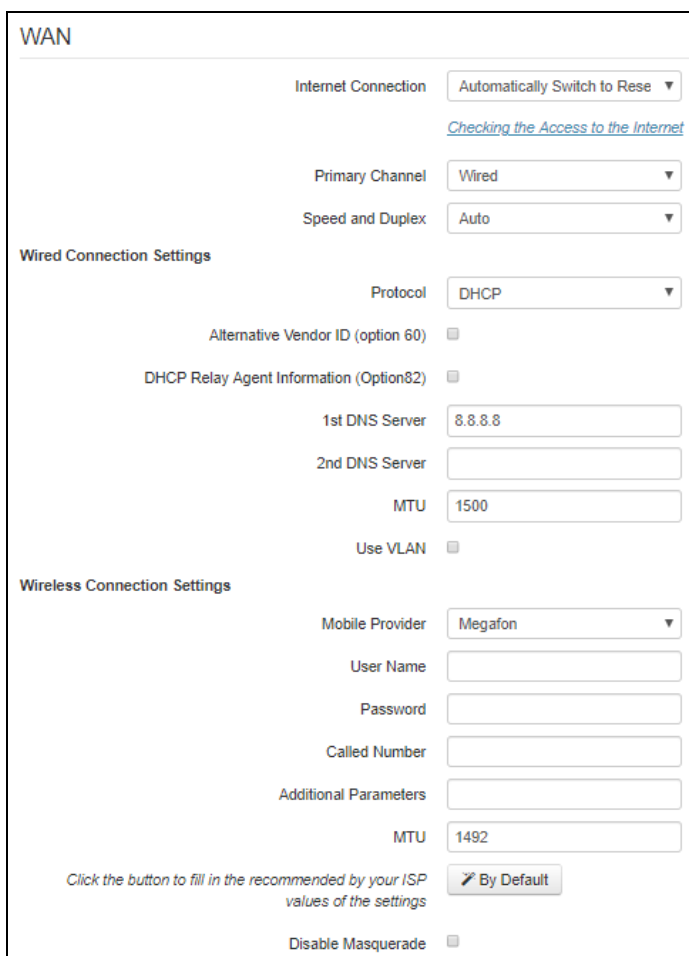
- *Mobile provider* – 3G/4G service provider name. You may select one of the six mobile service providers operating in Russian Federation (their settings are stored in the device memory): Megafon, Beeline, MTS, Skylink, Tele2, Yota. Click Default button to fill in the connection settings with the selected 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 Redundant Channel** connection method is selected, the following settings will be available for configuration:



The image shows a 'WAN' configuration window. At the top, 'Internet Connection' is set to 'Automatically Switch to Rese' (likely Redundant). Below it is a link 'Checking the Access to the Internet'. The 'Primary Channel' is set to 'Wired' and 'Speed and Duplex' is 'Auto'. Under 'Wired Connection Settings', the 'Protocol' is 'DHCP'. There are checkboxes for 'Alternative Vendor ID (option 60)' and 'DHCP Relay Agent Information (Option82)'. The '1st DNS Server' is '8.8.8.8', '2nd DNS Server' is empty, and 'MTU' is '1500'. There is a 'Use VLAN' checkbox. Under 'Wireless Connection Settings', 'Mobile Provider' is 'Megafon', and 'User Name', 'Password', 'Called Number', and 'Additional Parameters' are empty. The 'MTU' is '1492'. At the bottom, there is a 'By Default' button with a pencil icon and a 'Disable Masquerade' checkbox.

- *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.

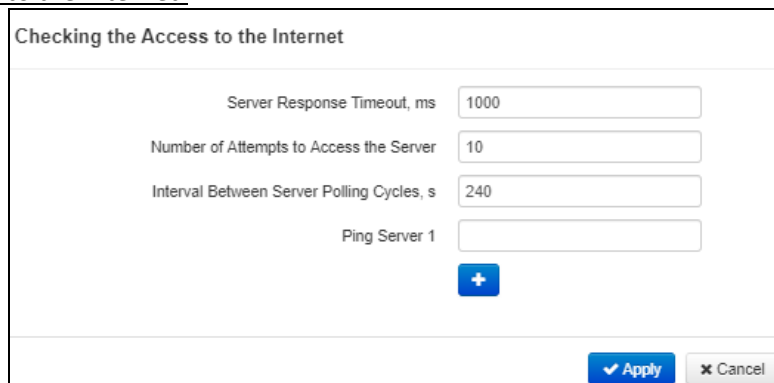
#### Wired connection settings:

The settings are identical **'Wireless connection'** with **'Router'** mode selected.

#### Wireless connection settings:

The settings are identical with settings for **'3G/4G USB modem'** connection method.

#### Checking the Access to the Internet:



The image shows a 'Checking the Access to the Internet' dialog box. It contains four input fields: 'Server Response Timeout, ms' (1000), 'Number of Attempts to Access the Server' (10), 'Interval Between Server Polling Cycles, s' (240), and 'Ping Server 1' (empty). Below the 'Ping Server 1' field is a blue button with a plus sign. At the bottom right are 'Apply' and 'Cancel' buttons.

- *Server Response Timeout, s* – time during which a response from the PING server is expected;
- *Number of Attempts to Access the Server, s* – 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.

#### LAN:

- *IP address* – device IP address in LAN;
- *Subnet mask* – subnet mask in LAN.



**LAN setting is disabled in the Bridge operation mode.**



**the local subnet address is changed, the local DHCP server address pool (Network—DHCP Server) will be changed automatically.**

#### IPSec Settings:

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

IPSec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPSec also includes secure Internet Key Exchange protocols.

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 Ancryption Algorithm 

des

Diffie Hellman Group 

1

IKE SA Lifetime, s 

86400

Phase 2

IKE Authentication Algorithm 

hmac\_md5

IKE Ancryption 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* together with *Local Netmask* define a local subnet for creation of network-to-network or network-to-point topologies;
- *Remote Subnet* 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 you to organize the following 4 network topologies with using encryption traffic via IPSec protocol: point-to-point, network-to-point, point-to-network, network-to-network;
- *Remote gateway* – gateway used for remote network access;
- *NAT-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.

- *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 (other name IPSec SA lifetime). Default value is 60 minutes (3600 seconds).

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



**This IPSec implementation works only when the sender address translation is disabled, as the client IP address is involved in the key formation.**

### 2.6.2.2 'QoS' submenu

In the 'QoS' submenu you may configure traffic processing priorities and queues type.

**QoS Settings**

Flow Control ☐  
Priority Decision DSCP ▼  
Queue Type Strict ▼

✓ Apply
✕ Cancel

#### QoS configuration

- *Flow control* – enabling/disabling of TCP Flow Control mechanism;
- *Priority decision* – choice of the traffic prioritization method:
  - *DSCP* – mechanism of classification, traffic control and QoS support through priorities;
  - *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).

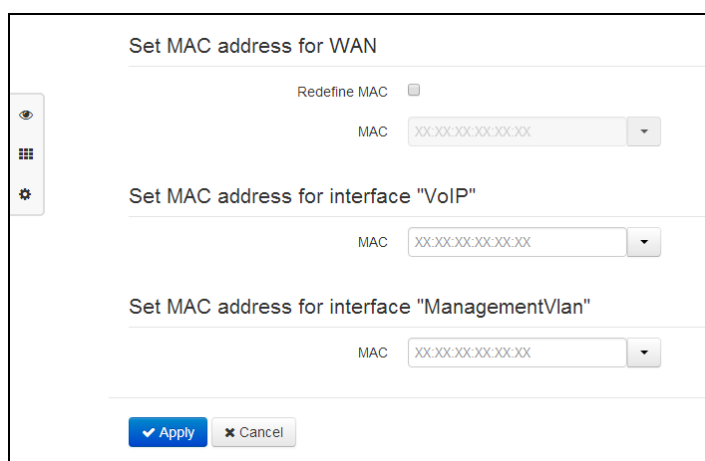


**With flow control is enabled, priority settings are not available.**

- *Queue type* – choice of queue service procedure:
  - *Strict* – service procedure when low-priority traffic is sent only when a higher-priority queue has been already sent;
  - *WRQ* – service procedure when an available broadband is shared between queues in proportion to priorities.
  - *Weight 0..5* – priority weight is determined in the range from 1 to 127, the more weight, the more priority of traffic.

### 2.6.2.3 'MAC management' submenu

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



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

When you click a drop-down menu button in the '*MAC*' field, you may specify MAC address of the computer connected to WEB configurator. The option may be helpful, when your ISP (Internet service provider) network employs MAC address tethering. In this case, if you are planning to use *TAU-4M.IP* as a router, MAC address of your computer (previously connected to the Internet) should be assigned to the WAN interface of the device.

To redefine MAC for '*VoIP*' or '*Management*' interfaces, see sections '*Set MAC address for interface 'VOIP'*' or '*Set MAC address for interface 'ManagementVlan'*'.

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

### 2.6.2.4 'DHCP server' submenu

In the 'DHCP server' submenu, you may configure a local DHCP server and define static address bindings.

With DHCP (Dynamic Host Configuration Protocol), *TAU-4M.IP* may automatically assign IP addresses and parameters required for the Internet access to computers connected to the LAN interface. DHCP eliminates limitations associated with the manual TCP/IP protocol configuration. DHCP server is available for configuration only when the Internet service is configured in the router mode.

### DHCP Server Settings

Enable ☒

Start IP Address

Pool Size

Lease Time (min)

✓ Apply

✗ Cancel

### Static Leases

Name	MAC Address	IP Address
<div> <div>+ Add</div> <div>✗ Remove</div> </div>		

### DHCP server settings

- *Enable* – when selected, enable local DHCP server;
- *Start IP address* – initial address in the IP address pool;
- *Pool size* – number of addresses in the pool;
- *Lease time (min)* – set the maximum time for IP address lease issued by DHCP server to the connected device, in minutes.

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



**When you change a starting address to a value from another subnet in relation to the LAN interface subnet, the pool will be automatically adjusted in accordance to the current local subnet address value.**

### Static leases

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

### Creating of Static Lease

Name

MAC Address

IP Address

✓ Apply

✗ Cancel

- *Name* – current static binding name.
- *MAC address* – specify a static MAC address. Format: XX:XX:XX:XX:XX:XX, you may select connected device addresses from the pop-up menu.
- *IP address* – define a static IP address for the specific MAC address.

Static binding configuration may become useful, if you have to assign a specific IP address to the specific PC connected to the device LAN interface.

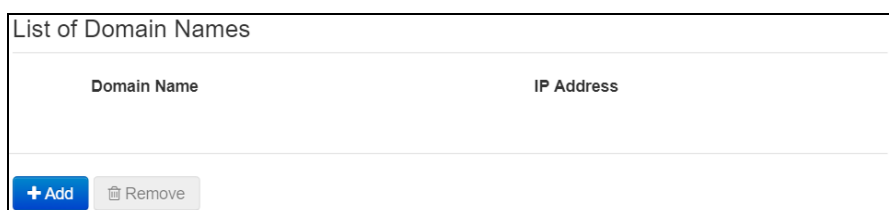
Click the *'Apply'* button to enter the IP address into the static IP address list for DHCP server. To discard changes click the *'Cancel'* button.

To delete the address from the list, select the checkbox next to the respective record and click *'Delete'*.

### 2.6.2.5 'Local DNS' submenu

In the 'Local DNS' submenu, you may configure a local DNS server by adding 'IP address—domain name' pairs into the database.

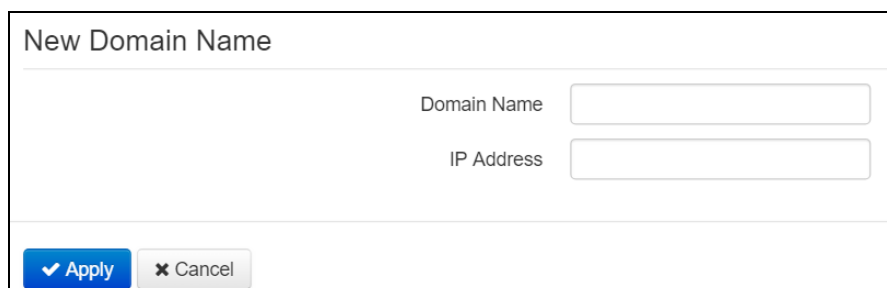
Local DNS—allows the gateway to obtain IP address of the communicating device by its domain name. You may use Local DNS in cases when DNS server is missing from the network segment that the gateway belongs to, and you need to establish routing using network names, or when you have to use SIP server network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



Domain Name	IP Address
<div> <span>+ Add</span> <span>Remove</span> </div>	

#### Adding a domain

To add the address into the list, click the *'Add'* button in the *'New domain name'* window and fill in the following fields:



New Domain Name

Domain Name

IP Address

✓ Apply

✗ Cancel

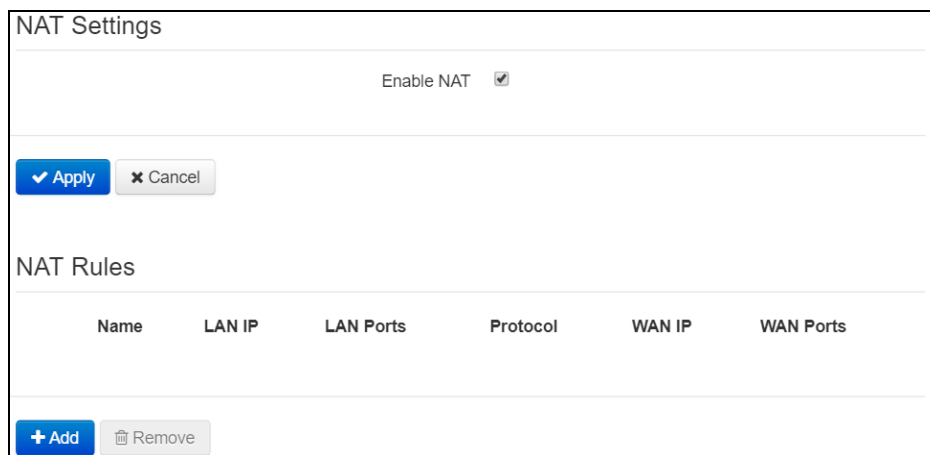
- Domain name – host name;
- IP address – host IP address.

Click *'Apply'* to create 'IP address—domain name' pair. To discard changes click the *'Cancel'* button. To delete the record from the list, select the checkbox next to the respective record and click *'Delete'*.

### 2.6.2.6 'NAT and port forwarding' submenu

In the 'NAT and port forwarding' submenu, you may configure port forwarding from WAN interface to LAN interface. This submenu is available only when the Internet service is configured in the router mode.

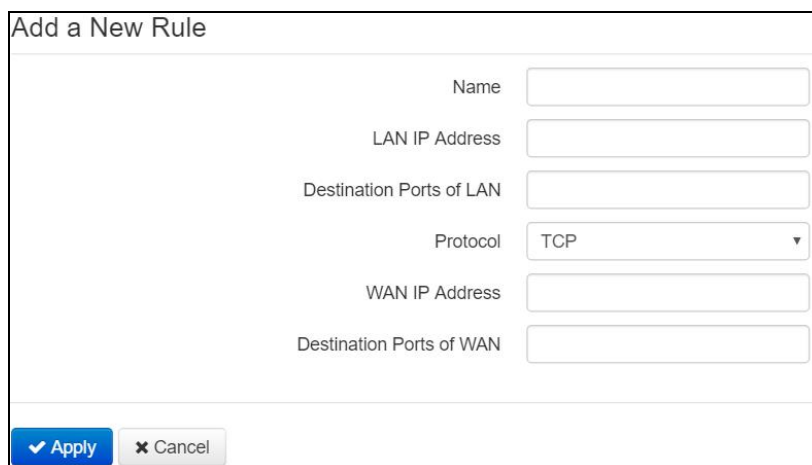
NAT (Network Address Translation) allows translating IP packet addresses and network ports. Port forwarding is required when TCP/UDP connection to a local computer (connected to LAN interface) is established from the WAN. In this settings menu, you may define the rules allowing packets to pass from the external network to the specified address in the local network and thus establishing connection. Port forwarding is required when torrent and P2P services are used. For this purpose, you should identify TCP/UDP ports used by a torrent or P2P client in their settings and assign the respective forwarding rules for your computer IP address.



The NAT Settings window has a title bar 'NAT Settings'. Below the title bar, there is a section with the text 'Enable NAT' followed by a checked checkbox. Below this, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon). Below these buttons is a section titled 'NAT Rules'. This section contains a table with the following headers: 'Name', 'LAN IP', 'LAN Ports', 'Protocol', 'WAN IP', and 'WAN Ports'. Below the table, there are two buttons: '+ Add' and 'Remove' (with a trash can icon).

### Configuration of NAT rules

To add a new NAT rule, click the 'Add' button and fill in the following fields in the 'Add a new rule' window:



The 'Add a New Rule' window has a title bar 'Add a New Rule'. Below the title bar, there are six input fields arranged vertically: 'Name', 'LAN IP Address', 'Destination Ports of LAN', 'Protocol' (a dropdown menu with 'TCP' selected), 'WAN IP Address', and 'Destination Ports of WAN'. At the bottom of the window, there are two buttons: 'Apply' (with a checkmark icon) and 'Cancel' (with an 'x' icon).

- *Name* – name of the rule (this field is mandatory);
- *LAN IP address* – IP address of the host in LAN used for packet translation falling under this rule;
- *Destination ports of LAN* – recipient TCP/UDP port values that will be used for packet translation into LAN (a single port or port range delimited by '-' is permitted);
- *Protocol* – selection of the packet protocol falling under this rule: TCP, UDP, TCP/UDP;
- *WAN IP address* – source IP address that sends packets into external networks falling under this rule;
- *Destination ports of WAN* – recipient TCP/UDP port values that will be used for packet translation into LAN (a single port or port range delimited by '-' is permitted).

Port forwarding rule will work as follows: For the packet that comes to device WAN interface address via '*Protocol*' to the port from '*WAN ports*' range and has a '*WAN IP address*' source address (if this parameter is empty, source address will not be analyzed), its destination address and port are substituted with values from '*LAN IP address*' and '*Destination ports of LAN*' fields.

Click the '*Apply*' button to add a new rule. To discard changes, click the '*Cancel*' button.

To delete the record from the list, select the checkbox next to the respective record and click 'Delete'.

### 2.6.2.7 '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, forward) 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).

Rules for Input Traffic						
Name	Protocol	Source IP Address	Source Ports	Destination Ports	Action	
Rules for Output Traffic						
Name	Protocol	Source Ports	Destination IP Address	Destination Ports	Action	
Rules for Forward Traffic						
Name	Protocol	Source IP Address	Source Ports	Destination IP Address	Destination Ports	Action

+ Add
Remove

#### Configuration of firewall rules

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

#### Add a New Rule

Name

Traffic Type

Protocol

Source IP Address

Source Ports

Destination Ports

Action

✓ Apply
✗ Cancel

- *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 become available:
  - *Source address* – define starting source IP address. Use '/' symbol to define a 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 become available:
  - *Destination 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.
- *Forward* – transit traffic (traffic being transferred between two network interfaces when the source and destination are external devices). When this traffic type is chosen, the following fields will become available:
  - *Source IP address* – define source IP address. Use '/' symbol to define a 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.
  - *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 (reject/skip).

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 'Cancel' button. To delete the record from the list, select the checkbox next to the respective record and click 'Delete'.



### 2.6.2.8 'ACL' submenu

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

Limitations on MAC Addresses

#	Status	MAC Address	Access	Speed Limit
<div>+ Add Remove</div>				

Limitations on URL Addresses

#	Status	URL
<div>+ Add Remove</div>		

Time Limits on Schedule

#	Status	Begin At	Stop At	Access	Speed Limit
<div>+ Add Remove</div>					

#### Limitations on MAC addresses

Add a New Rule

Enable ☐

MAC Address

Deny Access ☐

Speed Limit, kbit/s

✓ Apply

✗ Cancel

- *Enable* – when selected, MAC filtering rule is enabled;
- *MAC address* – MAC address of a device for which the created rule will be valid;
- *Deny access* – when selected, the access and transfer of transit traffic from a given device will be totally prohibited. If the option is disabled, the data transmission rate will be limited by a specified value.
- *Speed limit, kbps* – maximum data stream rate for the device with the specified MAC address (0 kbps — is equivalent to the absence of a data rate limit).

#### Limitations on URL addresses

Add a New Rule

Enable ☐

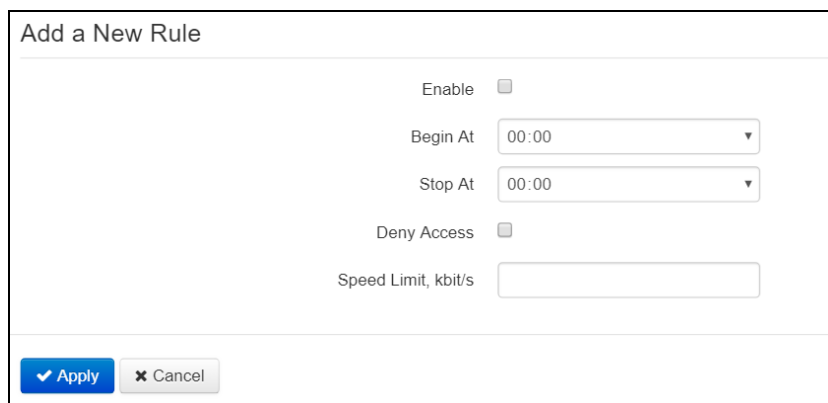
URL

✓ Apply

✗ Cancel

- *Enable* – when selected, URL filtering rule is enabled;
- *URL* – URL of a device for which the created rule will be valid;

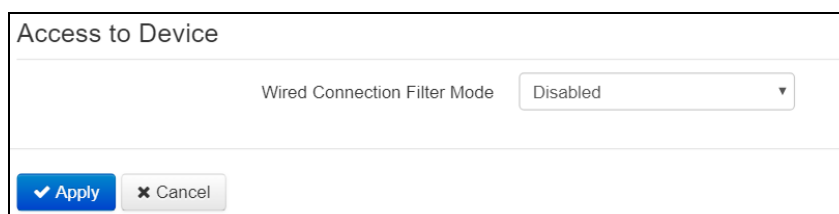
#### Time limits on schedule



- *Enable* – when selected, a filtering rule is enabled and disabled at the scheduled time;
- *Begin at* – time in the 24-hour number format (hh: mm), from which the created rule will be valid;
- *Stop at* – time in the 24-hour number format (hh: mm), up to which the created rule will be valid;
- *Deny access* – when selected, the access and transfer of transit traffic from a given device will be totally prohibited. If the option is disabled, the data transmission rate will be limited by a specified value.
- *Speed limit, kbps* – during a specified time period, the rate will be limited to the specified value (0 kbps is equivalent to the absence of a data rate limit).

#### 2.6.2.9 'MAC filter' submenu

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



- *Wired connection filter mode* – define 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;
  - *Allow* – access is forbidden for devices with MAC addresses from the 'MAC address list' in this operation mode. Access for devices with unlisted MAC addresses is permitted;
  - *Deny* – access is permitted for devices with MAC addresses from the 'MAC address list' in this operation mode. Access for devices with unlisted MAC addresses is forbidden.

#### **MAC address list**

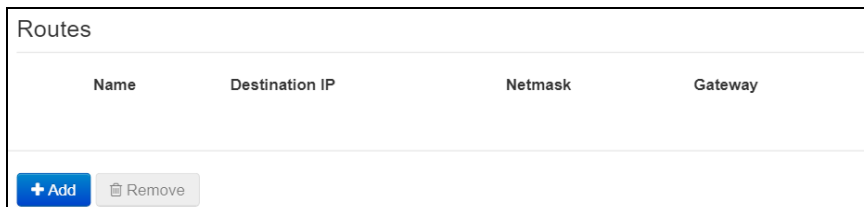
You may enter up to 30 client MAC addresses which may access the device in accordance with the specified filtering mode.

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.

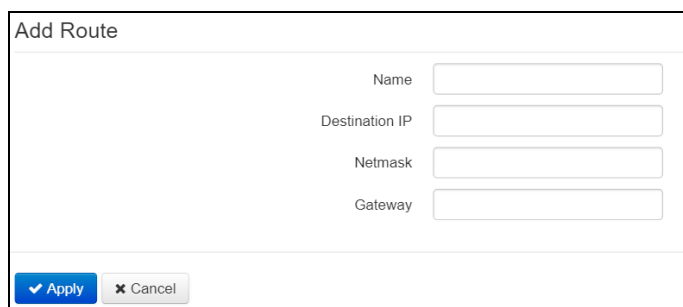
### 2.6.2.10 'Routes' submenu

In the 'Static routes' submenu, you may configure device static routes.



Name	Destination IP	Netmask	Gateway
<div> <span>+ Add</span> <span>Remove</span> </div>			

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



#### Add Route

Name

Destination IP

Netmask

Gateway

✓ Apply
✗ Cancel

- *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;
- *Subnet mask* — a subnet mask. Subnet mask 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*'.

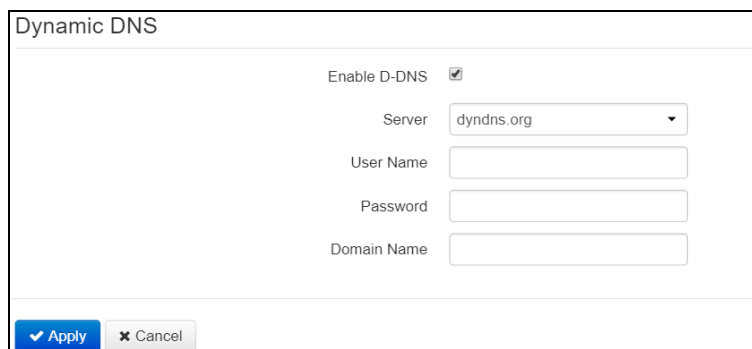
To apply a new configuration and store settings into the non-volatile memory, click the '*Apply*' button. To discard changes, click the '*Cancel*' button.

### 2.6.2.11 'Dynamic DNS' submenu

In the 'Dynamic DNS' submenu, you may configure the respective service.

*Dynamic DNS (D-DNS)* allows updating DNS server information in real time and in automatic mode. It is used for assigning a fixed domain name to a device (to a computer or router) with a dynamic IP address.

Dynamic DNS is frequently used in local networks, where clients are obtaining IP addresses through DHCP and then registering their names on local DNS-server.



#### Dynamic DNS

Enable D-DNS
☒

Server

User Name

Password

Domain Name

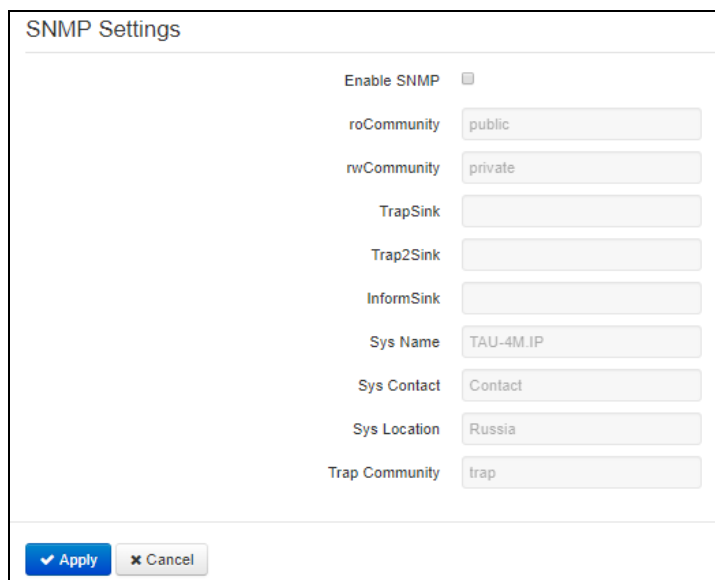
✓ Apply
✗ Cancel

- *Enable D-DNS* – when selected, D-DNS service is enabled; the following settings will be available for editing:
  - *D-DNS provider* – D-DNS provider address, select a provider from the list of available providers or enter provider's address manually;
  - *User name* – user name used to access D-DNS server account;
  - *Password* – password used to access D-DNS service account;
  - *Domain name* – registered domain name on D-DNS server. Device IP address information is updated on the provider server periodically in 60 seconds.

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

### 2.6.2.12 'SNMP' submenu

*TAU-4M.IP* software allows monitoring status of the device and configuring it via SNMP. In SNMP submenu, you can configure settings of SNMP agent. Device supports SNMPv1, SNMPv2c protocol versions.



The image shows a web-based configuration window titled "SNMP Settings". It contains the following fields and controls:

- Enable SNMP**: A checkbox that is currently checked.
- roCommunity**: A text input field with the value "public".
- rwCommunity**: A text input field with the value "private".
- TrapSink**: An empty text input field.
- Trap2Sink**: An empty text input field.
- InformSink**: An empty text input field.
- Sys Name**: A text input field with the value "TAU-4M.IP".
- Sys Contact**: A text input field with the value "Contact".
- Sys Location**: A text input field with the value "Russia".
- Trap Community**: A text input field with the value "trap".
- At the bottom, there are two buttons: a blue "Apply" button with a checkmark icon and a grey "Cancel" button with an 'X' icon.

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

- *Sys location* – device location information;
- *Trap community* – password enclosed in traps (default value: trap).

In the current firmware version, you may configure specific device parameters via SNMP: SIP basic settings, SIP profile settings, FXS port settings, call group settings, VAS management codes dialled from the phone unit, SNMP settings, system log settings.

Given below is the list of objects that may be read and configured via SNMP:

- Enterprise.1.3.1 – SIP profile basic settings;
- Enterprise.1.3.2.1 – SIP profile settings;
- Enterprise.1.1.2.1 – FXS port settings;
- Enterprise.1.4.1.1 – Call group settings;
- Enterprise.1.5 – VAS activation codes for the phone unit;
- Enterprise.2.1 – SNMP settings;
- Enterprise.3.1 – system log settings.

where Enterprise – 1.3.6.1.4.1.35265.1.56 is the device identifier.

To store settings into the non-volatile memory, click the '*Apply*' button. To discard changes, click the '*Cancel*' button.

### 2.6.3 '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.

#### 2.6.3.1 'Network settings' submenu

In the 'Network settings' submenu, you may specify custom network settings for VoIP service are specified.

VoIP Network Settings

Use Internet Settings

☐

Use VLAN

☒

VLAN ID

802.1P

Protocol

Alternative Vendor ID (option 60)

☐

DHCP Relay Agent Information (Option82)

☐

1st DNS Server

2nd DNS Server

IPSec Settings

Enable

☐

- *Use Internet settings* – when selected, use network settings specified in the 'Network -> Internet' menu, otherwise use settings specified in this menu;
- *Use VLAN<sup>3</sup>* – when selected, VoIP service will use a dedicated interface in a separate VLAN for its operation, with VLAN number specified in the 'VLAN ID' field.
- *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;
    - *Subnet mask* – subnet mask for VoIP service interface;
    - *Default gateway* – IP address for VoIP service interface default gateway;
    - *1st DNS, 2nd DNS*—DNS server IP addresses required for VoIP service operations.
  - *DHCP* – operation mode where IP address, subnet mask, 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 'Primary DNS' and 'Secondary DNS' fields. Manually defined addresses will have a priority 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 selected, the device transmits *Vendor ID (Option 60) in Option 60 DHCP messages (Vendor class ID)*. If the field is empty, Option 60 will not be transmitted in DHCP messages.

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

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

Example:

[VENDOR:Eltex][DEVICE:TAU-4M.IP][HW:1.0][SN:VI23000118]  
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#2.3.1]

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

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

<sup>3</sup> In the firmware version 1.9.1, you may specify custom settings for VoIP service only in the dedicated VLAN.

### IPSec settings:

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

IPSec is a set of protocols used for protection of data transmitted via Internet Protocol that enables authentication, integrity check and/or encryption of IP packets. IPSec also includes secure Internet Key Exchange protocols.

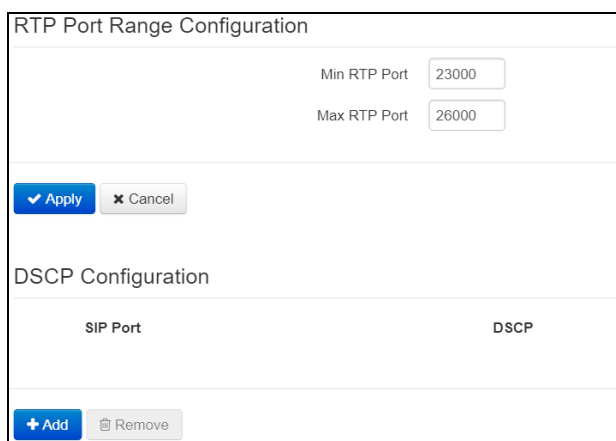
In the current firmware version, you may only access the device management interfaces (Web, Telnet, SSH) using IPSec.

For detailed *IPSec* description, see Section 2.6.2.1 of the '*IPSec settings*' 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.

### **2.6.3.2 'QoS' submenu**

In the 'QoS' submenu, you may configure Quality of Service functions.

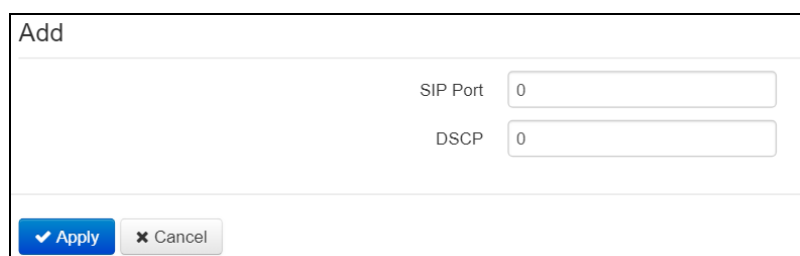


The screenshot shows the 'QoS' configuration interface. It has two main sections: 'RTP Port Range Configuration' and 'DSCP Configuration'. The 'RTP Port Range Configuration' section has two input fields: 'Min RTP Port' with the value '23000' and 'Max RTP Port' with the value '26000'. Below these fields are two buttons: a blue 'Apply' button with a checkmark icon and a grey 'Cancel' button with an 'X' icon. The 'DSCP Configuration' section has two columns: 'SIP Port' and 'DSCP'. Below these columns are two buttons: a blue '+ Add' button and a grey 'Remove' button with a trash icon.

### 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 for alarm (SIP)



The screenshot shows the 'Add' configuration window. It has two input fields: 'SIP Port' with the value '0' and 'DSCP' with the value '0'. Below these fields are two buttons: a blue 'Apply' button with a checkmark icon and a grey 'Cancel' button with an 'X' icon.

### Configuration of QoS rules

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

### 2.6.3.3 'Line settings' submenu

In the 'Line settings' submenu, you may configure the phone ports *Phone1*, *Phone2*, *Phone 3*, *Phone 4*.

List of Telephone Lines						
Line	Status	Phone	User Name	Login	SIP Port	SIP Profile
1	Enabled	210101	210101	210101	5060	1st profile
2	Enabled	210102	210102	210102	5060	1st profile
3	Enabled	210103	210103	210103	5060	1st profile
4	Enabled	210104	210104	210104	5060	1st profile

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

Edit Line 1: Account Settings

Enable ☒

SIP Profile 1st profile

Phone

User Name

Use Alternative Number ☐

SIP Port

Calling Party Category Off

Authentication

Login

Password

Supplementary Services

Flash Mode Transmit flash

Direct Number

Call Waiting ☐

Call Waiting ID ☐

Stop Dial at # ☐

Hotline ☐

CFU ☐

CFB ☐

CFNR ☐

DND ☐

Permit to Pickup Incoming Calls ☒

CLIR Off



Line Parameters

Caller ID Generation

Off

Hangup Timeout, s

0

Busy Timeout, s

120

Ringback Timeout, s

0

Minimal On-hook Time, ms

800

Min Flash Time, ms

100

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

200

Payphone

Off

Network Settings

DSCP

0

Apply

Cancel

### Account settings

- *Enable* – when selected, a port is active;
- *SIP profile* – select SIP profile from the list of available profiles. To configure profiles, use the 'VoIP -> Profiles' menu.
- *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 selected, 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).
- *Authentication 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 will be processed locally by the device (call transfer will be performed when the connection with the third party is established). For the 'Attended call transfer' detailed operation algorithm, see Section 3.13.1 Call Transfer;

- *Unattended calltransfer* – flash will be processed locally by the device (call transfer will be performed when the subscriber finishes dialling a third party number). For the Unattended call transfer detailed operation algorithm, see Section 3.13.1 Call Transfer;
  - *Local calltransfer* – call transmission within device, without REFER message sending. For the Local call transfer detailed operation algorithm, see Section 3.13.1 Call Transfer.
- *Call transfer mode* – this setting is available for the Attended call transfer and Local call transfer modes only and governs call transfer service activation mode:
  - Combined – call transfer is enabled on clearback and pressing R 4;
  - Flash+4 – call transfer is enabled on pressing R 4;
  - Onhook – call transfer is enabled on clearback.
- *Call waiting* – when selected, 'Call waiting' service will be enabled (this service is available in flash—call transfer function operation mode);
- *Call waiting ID* – when selected, the subscriber number is delivered for the call waiting service;
- *Stop dial at #* – when selected, use # button on the phone unit to end the dialling, otherwise # will be recognized as a part of the number;
- *Hotline* – when selected, 'Hotline/warmline' service is enabled. This service allows establishing an outgoing connection automatically without dialling the number after the phone handset is picked up with the defined delay (in seconds). When checked, fill in the following fields:
  - *'Hot number* – phone number that will be used for connection establishment upon Delay timeout expiration after the phone handset is picked up (in SIP profile being used, a prefix for this direction should be defined in the dialplan);
  - *Hot timeout, s* – time interval that will be used for connection establishment with the opposite subscriber, in seconds;
- *CFU (Call forward unconditional)* – when selected, CFU (Call Forward Unconditional) service is enabled—all incoming calls will be forwarded to the specified call forward unconditional number. When checked, fill in the following fields:
  - *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 selected, 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 selected, 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 Call forward on no answer 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 selected, temporary restriction is placed for incoming calls (DND service).

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* – CLIR service 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.

#### Line parameters

- *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 Bell 202, FSK V.23* – 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;
  - *Rus AON* — calling line identification using “Russian AON”. A number is identified at the signal «AON request» from a called subscriber's phone;
- *Hangup timeout, s* – dialling timeout for the first digit of a number. When there is no dialling during the specified time, busy tone will be sent to the subscriber, and the dialling will end;
- *Busy timeout, s* – 'busy' tone timeout for the subscriber. If the subscriber doesn't put the phone onhook until the timeout expires, an error tone will be sent into the line;
- *Ringback timeout, s* – launches when an incoming call is received and defines the maximum call response time. When the defined timeout expires, busy tone will be sent to the remote subscriber.
- *Minimal on-hook time, ms* – min clearback detection time, in milliseconds. At that, this parameter represents the max 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 to 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 to 200dB;
- *Speak voice level, dB* – configuration of voice signal level directed towards a subscriber. The range of values is between -31 to 31 dB;

- *Microphone voice level, dB* - configuration of voice signal level directed from a subscriber. The range of values is between -31 to 31dB;
- *Min pulse, ms* – configuration is required for pulse dialling mode. The range of values is between 10 to 150 ms;
- *Interdigit, ms* – configuration is required for pulse dialling mode. The range of values is between 150 to 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.

### 2.6.3.4 '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/modem 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).

List of SIP Profiles

Profile Name	Lines	Proxy Server	Registration Server	SIP Domain	Outbound Mode
<a href="#">1st profile</a>	1, 2, 3, 4	192.168.21.160	192.168.21.160		Outbound
<a href="#">2nd profile</a>					Off
<a href="#">3rd profile</a>					Off
<a href="#">4th profile</a>					Off
<a href="#">5th profile</a>					Off

Common Settings

STUN Enable

☐

Timer T1, ms

(100-1000)

Timer T2, ms

(1000-32000)

Timer B, ms

(1000-39000)

Click the button to fill in the SIP timer settings with recommended values

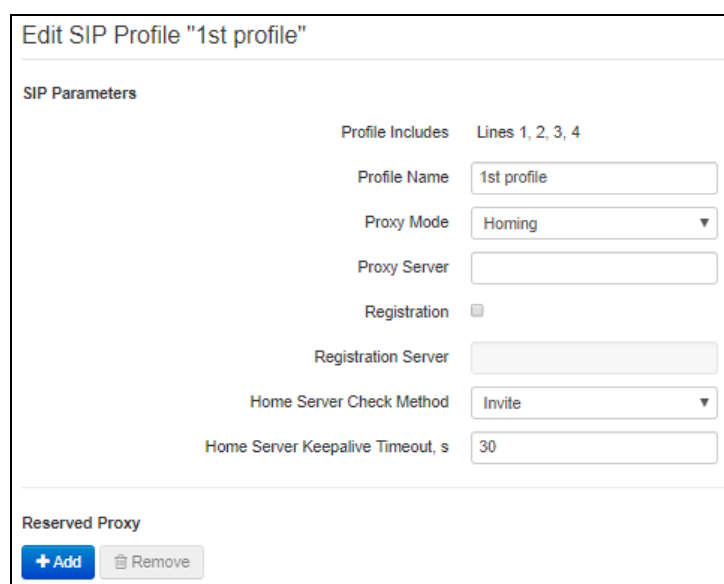
Transport

▼

Tones Specification

▼

Click the configurable profile link by the left mouse button to configure the profile. An 'Edit profile' window will be opened. Fill in the following fields:



### 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 not using, all INVITE queries are sending to address, pointed 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 four redundant SIP-proxies. For exclusive operations with the main SIP-proxy, 'Parking' and 'Homing' modes are identical. In this case, if the main SIP-proxy fails, it will take time to restore its operational status.

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

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

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

In the 'homing' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then to the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, gateway will renew its registration. Gateway begin operation with the main SIP-proxy.

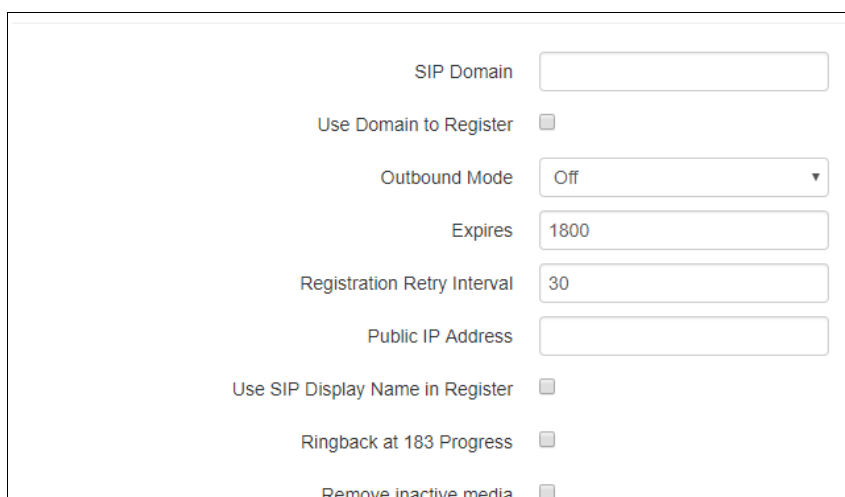
- *SIP proxy server* – network address of a SIP server—device that manages access to provider's phone network for all subscribers. You may specify IP address as well as the domain name (specify SIP server UDP port after the colon, default value is 5060);
- *Registration* – when selected, subscriber port 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* - periodic messages sending interval (in seconds), in order to check if the main SIP server is available.

### Reserved proxy

Click the 'Add' button to add the redundant SIP proxy and execute 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 'Remove'.



The screenshot shows a configuration window for a SIP proxy. It contains the following fields and controls:

- SIP Domain**: A text input field.
- Use Domain to Register**: A checkbox.
- Outbound Mode**: A dropdown menu currently set to "Off".
- Expires**: A text input field with the value "1800".
- Registration Retry Interval**: A text input field with the value "30".
- Public IP Address**: A text input field.
- Use SIP Display Name in Register**: A checkbox.
- Ringback at 183 Progress**: A checkbox.
- Remove inactive media**: A checkbox.

User Call	180 Ringing
Escape Hash Uri	<input type="checkbox"/>
100rel	Supported
Timer Enable	<input checked="" type="checkbox"/>
Min SE, s	120
Session Expires, s	1800
Keepalive NAT Sessions Mode	Off
Use Alert-Info Header	<input type="checkbox"/>
Check RURI User Part Only	<input type="checkbox"/>
Send IP Address in Call-ID Header	<input type="checkbox"/>

- *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 for registration is applying (SIP domain will be inputted in Register query Request-Line);
- *Outbound mode* - outbound mode:
  - *Off* - route the calls according the dialplan;
  - *Outbound* - dialplan is needed for outgoing connection, but all calls will be routed by SIP-server; in case of registration absence subscriber will get station reply, to manage subscriber service (Supply services management);
  - *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* - remaining time for SIP server registration renewal. 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 behind NAT (behind gateway). External (WAN) gateway interface (NAT) address behind which *TAU-4M.IP* is set is used as public address. Wherein it is needed to traverse corresponding SIP and RTP ports, used by device, on the gateway;
- *Use SIP Display Name in register* - when selected transmitting user name 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 when incoming call exists:

- *180 Ringing* - 180 reply is sending to caller equipment; caller equipment should output local ringback tone in line after getting this message;
- *183 Progress with SDP* - 183+SDP reply is sending to caller equipment; used for frequency path forwarding to callee reply. In this case *TAU-4M.IP* will remote send ringback tone to caller.
- *Escape Hash Uri*—when selected, 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;

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

#### *Setting operation for outgoing communications:*

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

#### *Setting operation for incoming communications:*

- *Supported, Required* – when the following tag is received in 'INVITE' request—supported: 100rel, or required: 100rel, perform reliable transfer of provisional replies. If there is no supported: 100rel tag in INVITE request, the gateway will perform unreliable transfer of provisional replies;
- *Off*—when the following tag is received in 'INVITE' request—required: 100rel, reject the request with message 420 and provide the following tag—unsupported: 100rel. Otherwise, perform unreliable transfer of provisional replies.
- *Enable timer* – when checked, enables support of SIP session timers (RFC 4028). After connection establishment, if both sides are supporting timer, one of them periodically send re-INVITE queries for connection control (if both sides are supporting UPDATE method (it should be pointed in 'Allow' header) session update is being processed by periodical UPDATE messages sending);
- *Min SE, s* – minimal time interval for connection health checks (90 to 1800s, 120s 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 80000s, recommended value–1800s, 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

Three-party Conference

Mode

Local ▼

Conference Server

conf

- *Mode* - 3-way-conference operation mode. Two modes are available;
  - *Local* - conference is intended locally by the device after pressing 'flash+3' combination;
  - *Remote (RFC4579)* - conference is intended on remote server. Then, after pressing 'flash+3' combination Invite message sending on server to number, pointed in the 'Conference server' field. In this case conference processing by algorithm, described in RFC4579. For detailed description see section 3.3.2.
- *Conference server* - conference connection establishment server address processed by algorithm, described in RFC4579. Address sets in SIP-URI format: user@address:port. It is available to set only user part URI - in this case Invite message will be sent to SIP proxy address.

### IMS settings

IMS Settings

IMS Mode

Off ▼

- *IMS mode* - IMS processing mode. Three modes are available;
  - *Off* - IMS is not using;
  - *Implicit* - Allow management of certain types of services by the IMS (IP Multimedia Subsystem) server. In this case enabling the '3-way Conference' (works only by the algorithm RFC4579), 'Call Hold', 'Call Waiting', 'Hot line' (regardless of whether they are

enabled or not in the configuration) services is performed remotely by the IMS server by sending Notify messages, the body of which sends commands to enable/disable services in XCAP format (in fact, XML, RFC4825). In this subscription option, gateway will not send SUBSCRIBE requests after subscriber registration, and will only process NOTIFY requests received from IMS, which are used for service management;

- *Explicit* - Allow management of certain types of services by the IMS (IP Multimedia Subsystem) server. In this case enabling the '3-way Conference' (works only by the algorithm RFC4579), 'Call Hold', 'Call Waiting', 'Hot line' (regardless of whether they are enabled or not in the configuration) services is performed remotely by the IMS server by sending Notify messages, the body of which sends commands to enable/disable services in XCAP format (in fact, XML, RFC4825). In this subscription option, gateway will send SUBSCRIBE requests after subscriber registration, and upon successful subscription, will process NOTIFY requests received from IMS, which are used for service management.
- *XCAP name for Call Hold* - XML element name in Notify message body, used for transmission of commands to enable/disable 'Call Hold' service. Example: if service name has 'call-hold' value, activation command will appear as:

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

and deactivation command:

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

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

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

and deactivation command:

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

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

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

and deactivation command:

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

- *XCAP name for Hotline* - XML element name in Notify message body, used for transmission of commands to enable/disable 'Hot Line' service. Activation command sending Hot Line phone number and call timeout. Example: if service name has 'three-party-conference' value and it is needed to perform a call to number 30001 after 6 seconds after onhook, activation command will appear as:

`<hot-line-service>`

`<addr>30001</addr>`

`<timeout>6</timeout>`

`</hot-line-service>`

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

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

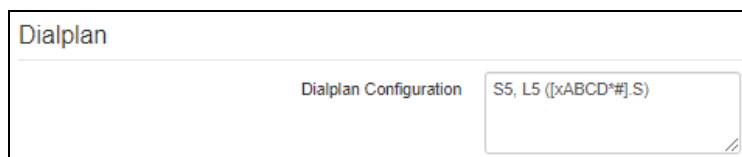
```
< call-transfer active="true"/>
```

and deactivation command:

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

If activation command is not received all listed above services will be deactivated by default.

### Dialplan



To define the numbering schedule, use regular expressions in the 'Dialplan Configuration' field. The structure and format of regular expressions that enable different dialling 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 recording using several designations: digits, dialed by phone keyboard: 0, 1, 2, 3, ..., 9, # and \*. **Symbol '#' usage in dialplan can block end of dial by this key!**

- Digit sequence enclosed in square brackets corresponds to any of the characters enclosed in brackets.
  - Example: ([1239]) - corresponds to any of this digits: 1, 2, 3 and 9.
- Symbol range may be set through the dash. Most often used inside square brackets.
  - Example 1: (1-5) - any digit from 1 to 5.
  - Example 2: ([1-39]) - example from previous paragraph with other record format.
- Symbol 'X' corresponds to any digit from 0 to 9.
  - Example: (1XX) - any three-digit number, starting at 1.
- '.' - Previous symbol repeating from 0 to infinity.
- '+' - Previous symbol repeating from 1 to infinity.
- {a,b} - Previous symbol repeating from 'a' to 'b' times;
- {a,} - Previous symbol repeating less than 'a' times;
- {,b} - Previous symbol repeating less than 'b' times.
  - Example: (810X.) - international number with any digits amount.

Settings that affect dialplan processing:

- *Interdigit Long Timer ('L' digit in dialplan entry)* - next digit input waiting time, if there are no patterns that appropriate for dialed combination;

- *Interdigit Short Timer ('S' digit in dialplan entry)* - next digit input waiting time, if there is at least one pattern that appropriate for dialed combination, and at least one more that needs extension dialing.

Additional features:

1. Dialed sequence replacement

Syntax: `<arg1:arg2>`

This ability allows to replace 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 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 common to hear a ringback, that may be implemented by inserting comma in a sequence of digits.

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

3. Number dialling deny.

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

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

4. Replacement of number dialling timers values

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

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

If these values are listed in one sequence only, they are effective only for this sequence. 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. Direct address dial (IP Dialling)

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

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

- Example 1: `( 8 xxx xxxxxxx )` - 11-digit number, starting at 8.
- Example 2: `( 8 xxx xxxxxxx | <:8495> xxxxxxx )` - 11-digit number, starting at 8; add 8495 to transmitting number if 7-digit number is entered.
- Example 3: `(0[123] | 8 [2-9]xx [2-9]xxxxx)` - the emergency services and some intercity numbers dialling.
- Example 4: `(S0 <:82125551234>)` - specified number speed dial, 'Hotline' mode analogue on another gateways.

- Example 5: (S5 <:1000> | xxxx) - this dialplan allows to dial any number, that consists of digits, and if nothing input during 5 seconds call number 1000 (e.g. it's a receptionist).
- Example 6: (\*5x\*xxxx\*x#|\*2x\*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8, [2-9]xxxxxxxxx|8, 10x.|1xx<:@10.110.60.51:5060>).
- Example 7: (1xx|0[1-9]|00[1-8]|\*5x\*xxxx\*x#|\*2x\*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8, [2-9]xxxxxxxxx|8, 10x.).

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

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

## 6. Configuration of pickup codes

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

Syntax: ABC@{pickup:X}, where

ABC – pickup code (e.g. \*8),

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

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

### Dialplan profiles setting

For every direction you may choose no more than 1 dialplan profile, that will define call parameters on this direction. Profile configuration is described in 'Dialplan profiles' section. For every direction alternative profile setting is specified in parenthesis after the word 'profile:'.

**Example:** ([23]xxx(profile:0)

### Voice codecs configuration

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.729 Packet Time, ms	20 ▼
G.723.1 Packet Time, ms	30 ▼

Devices signal processor encodes analogue voice traffic and fax/modem data into digital signal and performs its reverse decoding. Gateway supports the following voice codecs: G.711A, G.711U, G.729, G723.1, G.726, G.722.

G.711 is PCM codec that does not employ a compression of voice data. This codec must be supported by all VoIP equipment manufacturers. G.711A and G.711U codecs differ from each other in encoding law (A-law is a

linear encoding and U-law is non-linear). The U-law encoding is used in North America, and the A-law encoding—in Europe.

G.722 is a broadband codec that uses ADPCM compression algorithm with range division at the rate of 48, 56 and 64 kbps.

G.723.1 is a voice data compression codec, allows for two operation modes: 6.3kbps and 5.3kbps. G.723.1 codec has a voice activity detector and performs comfort noise generation at the remote end during period of silence (Annex A).

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

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

- *Codec 1...7* - allows you to select codecs and the order of their usage. Codec with the highest priority should be placed in 'Codec 1' field. For processing it is necessary to point at least one codec:
  - *Off* – codec is not used;
  - G.711A – use G.711A codec;
  - G.711U – use G.711U codec;
  - G.723 – use G.723.1 codec;
  - G.729 (A,B) – use G.729 annexA or G.729B codec;
  - G.726 – 24–use G.726 codec with 24 kbps speed;
  - G.726 – 32–use G.726-32 codec with 32 kbps speed;
  - G.722 – use G.722 codec;
- *Packet time* - voice milliseconds amount in one RTP packet (for codecs G.711, G.729, G.723 and G.726);
- *Payload type*—dynamic load type for G.726-24 or G.726-32 codecs (allowed values – from 95 to 127).



**Alternative voice codecs may be specified for chosen direction. There is ability of preferred codec setting for voice transmission for every direction in dialplan. Configuration is processing in dialplan. For every direction codec settings are pointed in parenthesis after word 'codecs:'.**

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). Allowed subparamX subparameters values: g711a, g711u, g729, g723.

Allowed param1 - codecs and param2 - rfc2833\_PT subparameters values:

**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 ▼

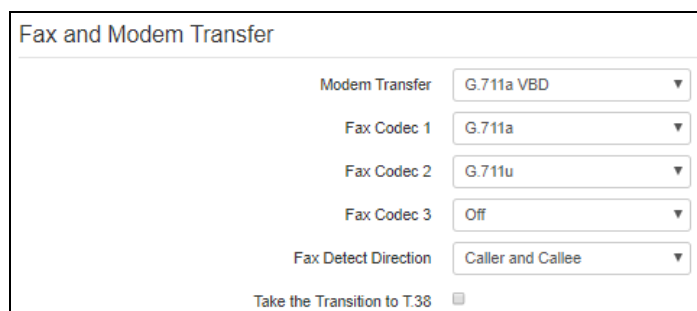
Jitter is a deviation of time periods dedicated to packet delivery. Packet delivery delay and jitter are measured in milliseconds. Jitter value is higher for real time data transfers (e.g. voice or video data).

In RTP, also known as 'media stream protocol', there is a field for precision transmission time tag related to the whole RTP stream. Receiving device uses these time tags to learn when to expect the packet and whether the packet order has been observed. On the basis of this information, the receiving side will learn how to configure its settings in order to evade potential network problems such as delays and jitter. If the expected time for packet delivery from the source to the destination for the whole call period corresponds to the defined value, e.g. 50ms, it is fair to say that there is no jitter in such a network. But packets are delayed in the network frequently, and the delivery time period may fluctuate significantly (in the context of time-critical traffic). If the audio or video recipient application will play packets in the order of their reception time, voice (or video) quality will deteriorate significantly. For example, if the voice data is being transferred, there will be interruptions and interference in the voice.

The device have the following jitter buffer settings:

- *Min delay, ms* - min expecting time of IP packet spread through network;
- *Max delay, ms* - max expecting time of IP packet spread through network;
- *Deletion threshold (DT)* - max time interval through which deleting of voice packets from buffer id processing. Parameter value greater than or equal to max delay;
- *Jitter factor* - parameter, used for jitter buffer size optimization. Recommended value is 0.

#### Fax and modem transfer



Fax may be transmitted using 711 voice codec or T.38 special codec for sending facsimile messages.

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

- *Modem transfer* - selecting of codec, that will be used for data transmission when modem signals detecting by the gateway:
  - Off — disable modem signal detection;
  - G.711a VBD — use G.711A codec in VBD mode;
  - G.711u VBD — use G.711U codec in VBD mode.

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



**Selected codec should also be enabled in voice codec list.**

- *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 processing it is necessary to point at least one codec:

- *Off* – codec is not using.
- G.711A – use G.711A codec;
- G.711U – use G.711U codec;
- T.38 – use T.38 protocol.



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

- *Fax Detect Direction*—defines the call direction for fax tone detection and subsequent switching to fax codec:
  - *No detect fax*—disables fax tone detection, but will not affect fax transmission (switching to fax codec will not be initiated, but such operation still may be performed by the opposite gateway);
  - *Caller and Callee*—tones are detected during both fax transmission and receiving. During fax transmission, CNG FAX signal is detected from the subscriber's line. During fax receiving, V.21 signal is detected from the subscriber's line;
  - *Caller*—tones are detected only during fax transmission. During fax transmission, CNG FAX signal is detected from the subscriber's line;
  - *Callee*—tones are detected only during fax receiving. During fax receiving, V.21 signal is detected from the subscriber's line;
- *Take the transition to T.38* - when checked incoming re-invite on T.38 on oncoming gateway is enabled;
- *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

Use the Same PT Both for Transmission and Reception ☐

Silencedetector ☒

Echocanceller ☒

RTCP ☐

Dispersion Time, ms 32

✔ Apply
✖ Cancel

- *DTMF Transfer*—DTMF tone transmission method:
  - *Inband*;
  - *RFC2833*—according to RFC2833 recommendation, as a dedicated payload 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 transmission is available only via SIP.**

- *RFC2833 payload type* - payload type for packets transmission via RFC2833 (permitted values: 96 to 127);
- *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 Tx and Rx of events via RFC2833 is processing with payload from received by oncoming side of message 200Ok. When unchecked Tx of events via RFC2833 is processing with payload from received 200Ok, Rx - with payload type from its own configuration (sets in outgoing Invite);
- *Silencedetector* - use silence detector when enabled;
- *Echocanceller* - when checked - use echocanceller;
- *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-4M.IP* cuts the connection off.
  - *RTCP-XR* – when checked, sending 'RTCP Extended Reports' control packets according to RFC 3611.
- *Dispersion time, ms* - parameter that cancels an echo caused by the voice signal dispersion. Parameter values may be specified in the interval from 2 ms to 128 ms.

### SIP common settings

**Common Settings**

STUN Enable ☒

STUN Server Address

STUN Request Sending Interval, s

Timer T1, ms  (100-1000)

Timer T2, ms  (1000-32000)

Timer B, ms  (1000-39000)

Click the button to fill in the SIP timer settings with recommended values

Transport

Tones Specification

- *STUN Enable* - when checked, STUN protocol is used to identify device public address (external NAT address). It is recommended to use this protocol while device working through NAT;
- *STUN server Address* - STUN server IP address or domain name, 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 300ms, the second INVITE will be sent in 300ms, the third is in 600ms, the fourth is in 1200ms, 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.

### 2.6.3.5 'Dialplan Profiles' submenu

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

List of Dialplan Profiles	
Dialplan Profile Number	SIP Profiles
<a href="#">profile: 0</a>	
<a href="#">profile: 1</a>	
<a href="#">profile: 2</a>	
<a href="#">profile: 3</a>	

You can configure up to 4 dialplan profiles.

#### Dialplan profile editing

### Edit Dialplan Profile 0

Codecs

Codec 1	G.711a
Codec 2	G.729
Codec 3	G.711u
Codec 4	G.723
Codec 5	G.726-24
Codec 6	G.726-32
Codec 7	G.722

G.711 Packet Time, ms	20
G.729 Packet Time, ms	20
G.723 Packet Time, ms	30
G.726-24 Packet Time, ms	20
G.726-32 Packet Time, ms	20
G.726-24 Payload Type	103
G.726-32 Payload Type	104

Fax and Modem Transfer

Modem Transfer

G.711a VBD

Fax Codec 1

G.711a

Fax Codec 2

G.711u

Fax Codec 3

Off

Take the Transition to T.38

☐

Additional Parameters

DTMF Transfer

RFC 2833

RFC2833 Payload Type

96

Silencedetector

☒

Echocanceller

☒

Dispersion Time, ms

32

Max Call Number

12

Jitter Buffer

Min Delay, ms

40

Max Delay, ms

130

Jitter Factor

7

Deletion Threshold (DT)

500

Use the Same PT Both for Transmission and Reception

☐

Rx AGC

☐

Rx AGC Level

-25 dB

Tx AGC

☐

Tx AGC Level

-25 dB

Apply

Cancel

### Codecs

- *Codec 1...7* - allows you to select codecs and an order of their usage. Codec with the highest priority should be placed in 'Codec 1' field. For processing it is necessary to point at least one codec:
  - Off – codec is not used.
  - G.711A – use G.711A codec;
  - G.711U – use G.711U codec;
  - G.723 – use G.723.1 codec;
  - G.729 – use G.729 annexA or G.729B codec.
  - G.726 – 24–use G.726 codec with 24 kbps speed
  - G.726 – 32–use G.726-32 codec with 32 kbps speed
  - G.722 – use G.722 codec
- *Packet Time* - voice milliseconds amount in one RTP packet (for codecs G.711A, G.729, G.723 and G.726).

- *Payload Type* - dynamic payload type for codecs G.726-24 or G.726-32 (permitted values - from 96 to 127).

#### Fax and Modem Transfer

- *Modem transfer* - selecting of codec, that will be used for data transmission when modem signals detecting by the gateway:
  - Off — disable modem signal detection;
  - G.711a VBD — use G.711A codec in VBD mode;
  - G.711u VBD — use G.711U codec in VBD mode.

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



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

- *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 processing it is necessary to point at least one codec:
  - Off — codec is not used.
  - G.711A — use G.711A codec;
  - G.711U — use G.711U codec;
  - T.38 — use T.38 protocol.



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

- *Take the Transition to T.38* - when checked incoming *re-invite* to T.38 from 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

- *DTMF Transfer*—DTMF tone transmission method:
  - *Inband*;
  - *RFC2833*—according to RFC2833 recommendation, as a dedicated payload in RTP voice packets;
  - *SIP Info* - transmission of the messages via SIP in INFO queries.
- *Payload type for RFC2833 packets* - payload type for packets transmission via RFC2833 (permitted values: 96 to 127);
- *Silencedetector* — use silence detector when enabled;
- *Echocanceller* — use echocanceller when checked;
- *Dispersion time, ms* - parameter, that allows to fight with echo, caused by voice signal dispersion. 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* - min expecting time of IP packet spread through network;
- *Max delay, ms* - max expecting time of IP packet spread through network;
- *Deletion Threshold, ms* - max time interval through which deleting of voice packets from buffer id processing. Parameter value greater than or equal to max delay (permitted values from 0 to 500, but at least max jitter buffer value);
- *Buffer optimization factor* - parameter, used for jitter buffer size optimization. It is recommended to set its value into 0;
- *Use the Same PT Both for Transmission and Reception* - when checked use same payload type for Rx and Tx;
- *Rx AGC*—when selected, a received signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise—the amplification will not be carried out;
- *Rx AGC Level*—determines the value of the level to which an analogue signal will be amplified when receiving (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB);
- *Tx AGC*—when selected, a transmitted signal will be amplified to the specified level (maximum signal amplification is +/- 15 dB), otherwise—the amplification will not be carried out;
- *Tx AGC Level*—determines the value of the level to which an analogue signal will be amplified when transmitting (allowed values: -25, -22, -19, -16, -13, -10, -7, -4, -1 dB).

### 2.6.3.6 'Hunt Groups' submenu

In the 'Hunt groups' submenu you can control call groups.

Call groups allow to perform call center features. Device supports 3 call group modes:

- *Group* - mode, when 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.
- *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.
- *Cyclic* - in the cyclic mode, the gateway after timeout (*Timeout of next port call*) continuously searches for a free group member, and the call is transferred to their number.

Hunt Groups				
Group Name	Status	SIP Profile	Phone	List of the Ports
Group1	✖	1st profile		
Group2	✖	1st profile		
Group3	✖	1st profile		
Group4	✖	1st profile		
Group5	✖	1st profile		

- *Group name* - Call group name;
- *Status* - call group state: enabled, disabled;
- *SIP Profile* - SIP profile, used by call group;

- *Phone* - call group phone number;
- *List of the Ports* - line (ports) list that includes call group.

To configure the call group, click on the corresponding link in the '*Group Name*' column.

Edit Group

Enable
☐

SIP Profile
1st profile

Group Name
Group1

Phone

Username

Password

SIP Port
5060

Group Type
Group

Call Queue Size, s
10

Call Reply Timeout, s
20

Group Call Pickup Enable
☒

List of the Ports

Line 1☐

Line 2☐

Line 3☐

Line 4☐

✓ Apply

✗ Cancel

- *Enable* - use the group when checked;
- *SIP Profile* - SIP profile, assigned to call group. Profile configured in the '*VOIP->Profiles*';
- *Group name* - identification group name;
- *Phone* - call 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* - call group type:
  - *Group* - the call comes in to all free ports of the group simultaneously;
  - *Serial* - amount of ports on which the call signal is coming; increased by 1 after Next port calling timeout expires;
  - *Cyclic* - call signal after interval In reaching last port in group ring-round continue from the first port;
- *Next port calling timeout, s* - option is used by serial and cyclic type groups and set time interval in seconds, through which executes call of next port;
- *Call Queue Size, s* - setting allows restricting max missed calls amount in call group queue. Received call do not set in queue if there a free ports in group;

- *Call reply timeout, s* - if there will be no answer to group 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 are belong one pickup group (see Section 2.6.3.1 The 'Pickup Groups' submenu).
- *List of the Ports* - when checked, a line (port) will be included into this call 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.

### 2.6.3.7 'Pickup Groups' submenu

The '*Pickup groups*' submenu is intended for call pickup groups configuration.

Pickup group—subscriber group, authorized to receive (or intercept) 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 dialling a pickup code. Pickup code configuration is carried out in the '*Dialplan*' point in the '*Profiles*' submenu.

Pickup Groups				
	Line 1	Line 2	Line 3	Line 4
Group 1	<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"/>
Group 3	<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"/>

To add/delete the line in group, select/deselect the checkbox next to the respective 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 that uses the same SIP profile may answer the incoming call. To do this, they should dial a pickup code, and the connection with the caller will be established after that.

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

Pickup group may be used in combination with a call group; in this case, all ports that belong to a call group should belong to the pickup group 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, 'Busy' tone will be transmitted to subscriber.

### 2.6.3.8 'Supplementary Service Prefixes' submenu

In the 'Supplementary Service Prefixes' submenu

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

- service activation - \* service\_code #;
- service activity check - \*# service\_code #;
- service cancellation - # service\_code #;

To enable 'Call Forward Unconditional' (CFU), 'Call Forward on Busy' (CFB), 'Call Forward on No Reply' (CFNR), 'Hotline/Warmline' services you should enter the phone number:

\* service\_code \* phone\_number #

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

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

Supplementary Service Prefixes			
Supplementary Services	Activation Code	Deactivation Code	Check Code
CFU	* <input type="text"/> #	-	-
CFB	* <input type="text"/> #	-	-
CFNR	* <input type="text"/> #	-	-
Permit to Pickup Incoming Calls	* <input type="text"/> #	-	-
Hotline	* <input type="text"/> #	-	-
Call Waiting	* <input type="text"/> #	-	-
DND	* <input type="text"/> #	-	-

#### Subscriber service management

- *Supplementary services* - list of Supplementary services:
  - *CFU* - service that forwards all subscriber's incoming calls to specified number;
  - *CFB* - service that forwards all subscriber's incoming calls to specified number when he is busy;
  - *CFNR* - service that forwards all subscriber's incoming calls to specified number after specified time if subscriber do not reply;
  - *Permit to Pickup Incoming Calls* - if subscriber enabled the service all incoming to him calls can be pickuped by other subscribers from this pickup group;
  - *Hotline* - when enabled, the defined phone number will be dialled upon expiration of a specified time period after the phone handset will have been picked up;
  - *Call waiting* - service allows a subscriber to get the notification about new incoming call in call state. Subscriber can accept, decline or ignore waiting call;



– *DND (Do not Disturb)* - service allows subscriber temporarily restrict all incoming calls.

- *Activation Code* - code for service enabling;
- *Deactivation Code* - code for service disabling;
- *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.

### 2.6.3.9 'Cadence' submenu

In the '*Cadence*' submenu you can set alternative cadence signal according to Alert-Info header in incoming Invite. Cadence value for every call signal sets as a sequence of rolling impulse and pause lengths divided by symbol ',' or ';'. Impulse/pause length value sets in milliseconds and must be multiple to 100. Min impulse/pause length is 200 ms, max - 8000 ms.

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

If cadence 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' output.

Cadence Name	Cadence
 <a href="#">Bellcore-dr1</a>	1000,4000
 <a href="#">Bellcore-dr2</a>	1000,3000
 <a href="#">Bellcore-dr3</a>	1000,2000
 <a href="#">Bellcore-dr4</a>	1000,1000
 <a href="#">Bellcore-dr5</a>	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 following settings:

Add Cadence

Cadence Name

Cadence

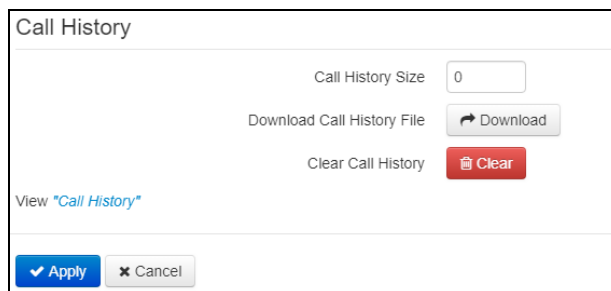
 

- *Cadence name* - cadence name;
- *Cadence* - length of the ringing voltage sending to a subscriber set and length of the pause between call signals, both values should be multiple to 100 ms, min value is 200 ms, max is 8000 ms;

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

### 2.6.3.10 'Call History' submenu

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



- *Call History size* - max log entries size, get values from 0 to 10000 strings. 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;

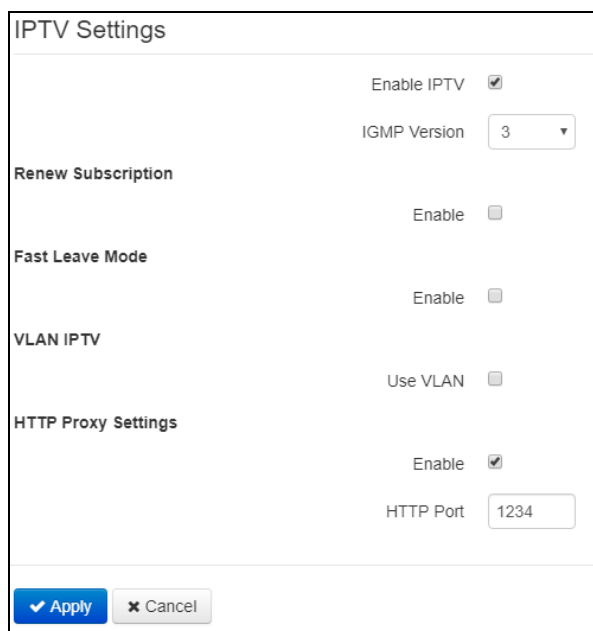
To view the call history, click the 'View Call History' link. Parameters monitoring is shown in Section 2.7.10 'Call History' submenu .

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

## 2.6.4 'IPTV' menu

### 2.6.4.1 The 'IPTV' submenu

In the 'IPTV' submenu you can configure the IPTV service.



- *Enable IPTV* – when selected, enables IPTV signal transmission from *TAU-4M.IP* WAN interface (from the provider network) to the devices connected to LAN interface.

- *IGMP version* - IGMP version for IGMP messages sending from WAN interface (IPTV channel subscription enabling/disabling messages). Supports versions 2 and 3.

#### Renew Subscription

- *Enable* - when option is enabled messages with active IPTV channel list are periodically sending from the WAN interface to higher server, that translating IPTV signals. Enabling the periodic subscription renewal function is necessary if higher server disabling IPTV channel translation after specified time interval.
  - *Renew Subscription Interval, s* - active IPTV channel list messages sending period, in seconds. Set the renewal period value less than IPTV channel translation disabling by higher server timeout.

#### Fast Leave Mode

- *Enable* - when checked fast group leave mode is enabled. This function reduces device's delay for switching between multicast streams (stream disconnection is processing after receiving 'Leave Group' message from subscriber without additional rerequest). It is not recommended to use this mode when more than one IPTV receiver connected to one LAN port.

#### VLAN IPTV

- *Use VLAN* - when checked, use dedicated VLAN for IPTV service (VLAN number may coincide with VLAN number for Internet or STB service), otherwise IPTV will use Internet service interface. This setting allows to determine the interface for UPTV signals receiving from external network;
  - *VLAN ID* - VLAN identifier for IPTV signals receiving;
  - *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). Used for QoS algorithms processing.

#### HTTP proxy settings

- *Enable* - when checked HTTP proxy service is enabled. HTTP proxy transforms UDP stream into HTTP stream, that using TCP (reliable packets delivery protocol) in order to improve stream image quality, when the quality of the communication link in local area network is low;
  - *HTTP Port* – HTTP proxy port number that will be used for video streaming. Use this port to connect to IPTV streams being broadcast by *TAU-4M.IP*.

For example, if *TAU-4M.IP* address on LAN interface is 192.168.0.1, proxy server port is 2354, and the desired channel 227.50.50.100 is being broadcast to UDP port 1234, you should specify the following stream address for VLC application:  
 http://@192.168.0.1:2345/udp/227.50.50.100:1234.

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

## 2.6.5 'System' menu

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

### 2.6.5.1 'Time' submenu

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

Time Settings

Time Zone

Moscow, Russia

Daylight Saving Time Enable

☒

DST Start

-

-

in

-

at

--:--

DST End

-

-

in

-

at

--:--

DST Offset (minutes)

60

Enable NTP

☒

NTP Server

pool.ntp.org

✓ Apply

✗ Cancel

#### Time settings

- *Time Zone* - allows to set 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, when daylight saving time is starting;
  - *DST End* - day, when daylight saving time is ending;
  - *DST Offset (minutes)* - time period in minutes, on which time offset is performing.
- *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.

### 2.6.5.2 'Access' submenu

In the 'Access' submenu, you can configure the access to device via WEB interface, Telnet and SSH and also access to the USB storages via FTP.

#### Access Ports

HTTP Port	<input type="text" value="80"/>
HTTPS Port	<input type="text" value="443"/>
Telnet Port	<input type="text" value="23"/>
SSH Port	<input type="text" value="22"/>

#### Access to "Internet" Service

##### Web

WAN	<input checked="" type="checkbox"/> HTTP	<input type="checkbox"/> HTTPS
LAN	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> HTTPS

##### Telnet

WAN	<input checked="" type="checkbox"/>
LAN	<input checked="" type="checkbox"/>

##### SSH

WAN	<input type="checkbox"/>
LAN	<input checked="" type="checkbox"/>

#### Access to "VoIP" Service

Web	<input type="checkbox"/> HTTP	<input type="checkbox"/> HTTPS
Telnet	<input type="checkbox"/>	
SSH	<input type="checkbox"/>	

#### Access to "Management Interface" Service

Web	<input type="checkbox"/> HTTP	<input type="checkbox"/> HTTPS
Telnet	<input type="checkbox"/>	
SSH	<input type="checkbox"/>	

#### Access to USB

WAN	<input type="checkbox"/>
LAN	<input checked="" type="checkbox"/>
Allow Anonymous User Access	<input checked="" type="checkbox"/>
Allow Anonymous User Write Permission	<input type="checkbox"/>

## 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 get access to the device via Internet service interfaces set the following permissions:

Web, external network:

- *HTTP* – when selected, the WAN port connection to the device WEB configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when selected, the WAN port connection to the device WEB configurator is enabled via HTTPS (insecure connection);

Web, Local network:

- *HTTP* – when selected, the LAN port connection to the device Web configurator is enabled via HTTP (insecure connection);
- *HTTPS* – when selected, the LAN port connection to the device Web configurator is enabled via HTTPS (insecure connection);

Telnet:

**Telnet** is a protocol that allows establishing mechanisms of control over the network. It allows you to establish remote connection to the gateway from a computer for configuration and management purposes.

To grant the access to device using Telnet protocol from external (via WAN port) or internal (via LAN port) network set the following flags.

SSH:

**SSH** - secure protocol of device remote control. In opposite from Telnet, SSH encrypting whole traffic, including transmitting passwords.

To grant the access to device using SSH protocol from external (via WAN port) or internal (via LAN port) network set the following flags.

## Access to 'VoIP' service:

In this section you can configure the access to VoIP service interface (VoIP service interface is configuring 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.

### Access to 'Management Interface' Service:

This section allows to configure the access to device management via HTTP, HTTPS Telnet or SSH. Interface configuration is performing on the '**System- > Management Interface**' page. To grant the access by any of specified protocols set the corresponding flags.



**For authentication via Telnet and SSH protocols username - *admin* and password - *password* are default. After authentication Linux OS console with possibility to use main command interpreter 'shell' commands will be available.**

### Access to USB:

In this section, you can configure the access to device that connected to USB port via FTP.

To grant the access to USB device using FTP from external (via WAN port) or internal (via LAN port) network set the following flags.

To grant anonymous user the access to connected USB device set the 'Allow Anonymous User Access' flag.

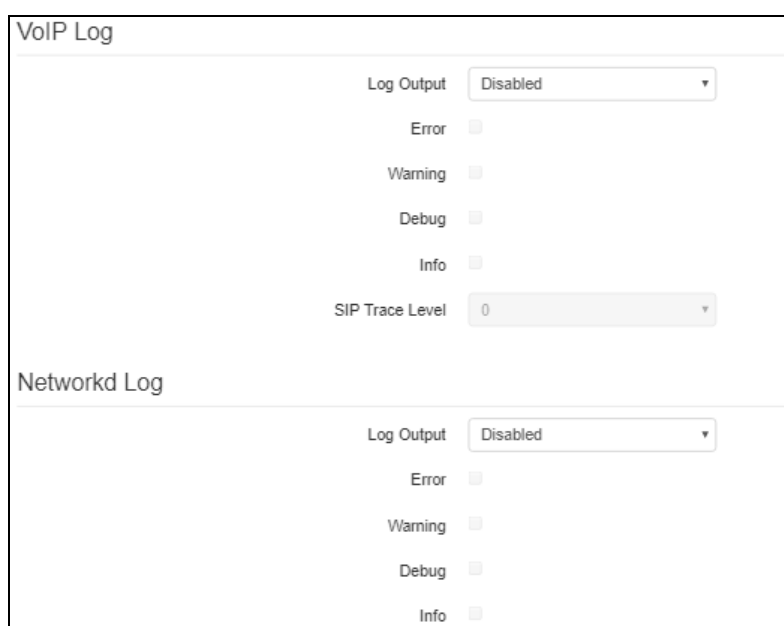
To grant anonymous user the rights to record data to the USB device set the 'Allow Anonymous User Write Permission' flag.

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

### **2.6.5.3 'Log' submenu**

The '*Log*' submenu is intended for configuring the output of various kinds of debugging messages of the system in order to detect the causes of problems in the device operation. Debug information may be obtained from 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 a configuration window titled 'Log'. It is divided into two main sections: 'VoIP Log' and 'Networkd Log'. Each section contains a 'Log Output' dropdown menu set to 'Disabled', and four checkboxes for 'Error', 'Warning', 'Debug', and 'Info', all of which are currently unchecked. Additionally, the 'VoIP Log' section includes a 'SIP Trace Level' dropdown menu set to '0'.

### Configd Log

Log Output

Disabled

Error
☐

Warning
☐

Debug
☐

Info
☐

### Syslog Settings

Enable
☐

Mode

Server

Syslog Server Address

syslog.server

Syslog Server Port

514

✓ Apply

✗ Cancel

### VoIP Log

- *Log Output* - log messages output direction:
  - *Disabled* - log is disabled;
  - *Syslog* - messages are output to the remote server or local file via syslog protocol (protocol configuration is carried out below);
  - *Console* - messages are output to device console (connection via COM port adapter is needed);
  - *Telnet* - messages are output to the telnet session; for this create the connection via telnet protocol first.

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

- *Error* - check if it is needed to output 'Error' type messages;
- *Warning* - check if it is needed to output 'Warning' type messages;
- *Debug* - check if it is needed to output 'Debug' type messages;
- *Info* - check if it is needed to output 'Info' type messages;
- *SIP Trace Level* - sets the VoIP SIP manager stack messages output level.

### Networkd Log

- *Log Output* - log messages output direction:
  - *Disabled* - log is disabled;
  - *Syslog* - messages are output to the remote server or local file via syslog protocol (protocol configuration is carried out below);
  - *Console* - messages are output to device console (connection via COM port adapter is needed);
  - *Telnet* - messages are output to the telnet session; for this create the connection via telnet protocol first.



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

- *Error* - check if it is needed to output 'Error' type messages;
- *Warning* - check if it is needed to output 'Warning' type messages;
- *Debug* - check if it is needed to output 'Debug' type messages;
- *Info* - check if it is needed to output 'Info' type messages;

### Config Log

- *Log Output* - log messages output direction:
  - *Disabled* - log is disabled;
  - *Syslog* - messages are output to the remote server or local file via syslog protocol (protocol configuration is carried out below);
  - *Console* - messages are output to device console (connection via COM port adapter is needed);
  - *Telnet* - messages are output to the telnet session; for this create the connection via telnet protocol first.

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

- *Error* - check if it is needed to output 'Error' type messages;
- *Warning* - check if it is needed to output 'Warning' type messages;
- *Debug* - check if it is needed to output 'Debug' type messages;
- *Info* - check if it is needed to output 'Info' type messages;

### Syslog Settings

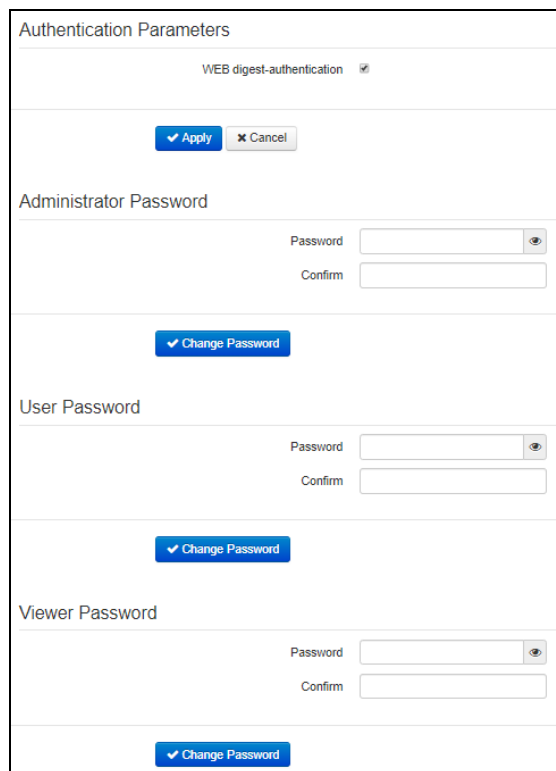
If at least one of logs (VoIP manager, System manager or configuration manager) is configured to output in Syslog it is needed to enable the Syslog agent, that will intercept debug messages from corresponding manager and send them to remote server or save to local file in Syslog format.

- *Enable* - when checked syslog agent is running;
- *Mode* - Syslog agent operation mode:
  - *Server* - log information is sending to remote Syslog server (this mode calls 'remote log');
  - *Local file* - log information is saving to local file;
  - *Server and file* - log information is sending to remote Syslog server and saving to local file.

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

- *Syslog Server Address* - Syslog server IP address or domain name (needed for 'Server' mode);
- *Syslog Server Port* - incoming Syslog server messages port (default is 514, needed for 'Server' mode);
- *File Name* - log storage file name in Syslog format (needed for 'Local File' mode);
- *File Size, KB* - log file max size (needed for 'Local File' mode).

## 2.6.5.4 'WEB authentication' submenu



In the '*WEB authentication*' submenu, you can set passwords for access by administrator, unprivileged user and viewer.

*WEB digest-authentication* — when selected, user authentication is performed in accordance with digest algorithms.

The passwords specified are used for device access via WEB interface and also VIA Telnet and SSH protocols.

When logging in via WEB interface administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring. Unprivileged user (default password: **user**) may perform only network configuration (except Internet connection), Have the access to device status monitoring. Viewer (default password: **viewer**) have access only to viewing the configuration and device monitoring data without ability to implement any changes.



**Administrator login: admin**  
**Unprivileged user login: user**  
**Viewer login: viewer**

- *Administrator Password* - type administrator password and confirmation in corresponding fields;
- *User Password* - type unprivileged user password and confirmation in corresponding fields;
- *Viewer Password* - type 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.



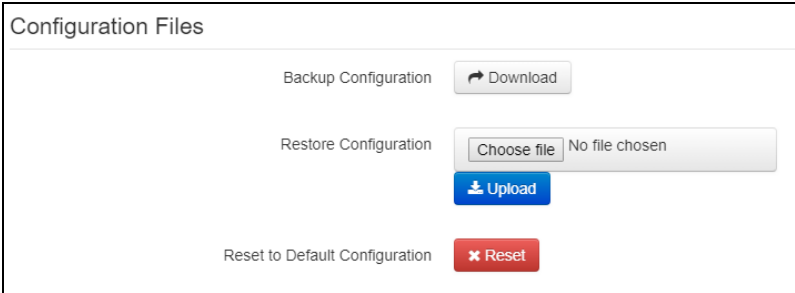
When upgrading to version 2.3.0, all passwords will be encrypted. When returning to version 2.1.0 and below, reset the device to factory configuration.



Beginning with version 2.3.0, a function of password encryption in the configuration file is added. If one of the device passwords should be changed, it is necessary to delete 'encrypted' and specify a new password when preparing the cfg.yaml file for automatic configuration. For example, to change a password of 'admin', delete "encrypted:" from "AdminPassword". Then specify a '\*new password\*' in "new password".

### 2.6.5.5 'Configuration Management' submenu

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



The screenshot shows a web interface titled "Configuration Files". It contains three main sections:
 

- Backup Configuration:** A button labeled "Download" with a download icon.
- Restore Configuration:** A "Choose file" button next to the text "No file chosen", followed by a blue "Upload" button with an upload icon.
- Reset to Default Configuration:** A red button labeled "Reset" with a red 'x' icon.

#### Backup Configuration

To save current device configuration to local computer click on the 'Download' button.

#### Restore Configuration

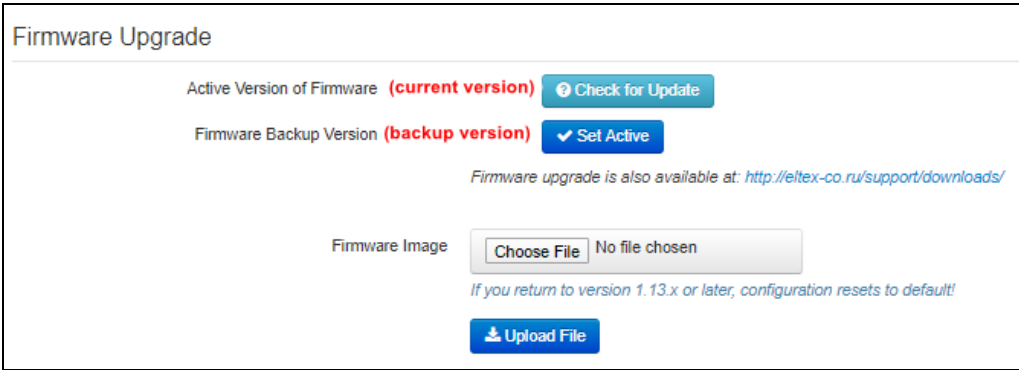
*Upload configuration archive to the device* - selection of configuration file saved on local computer. To update the device configuration click the 'Choose file' button, specify a file (in .tar.gz format) and click the 'Upload' button. Uploaded configuration will be applied automatically without device rebooting.

#### Reset to default configuration

To reset the device to factory default settings, click the 'Reset' button.

### 2.6.5.6 'Firmware Upgrade' submenu

The 'Firmware Upgrade' submenu is intended for upgrading the device's firmware.



The screenshot shows a web interface titled "Firmware Upgrade". It contains the following elements:
 

- Active Version of Firmware:** Labeled "(current version)" in red, with a blue "Check for Update" button.
- Firmware Backup Version:** Labeled "(backup version)" in red, with a blue "Set Active" button.
- Link:** Text stating "Firmware upgrade is also available at: <http://eltex-co.ru/support/downloads/>".
- Firmware Image:** A "Choose File" button next to the text "No file chosen", followed by a blue "Upload File" button with an upload icon.
- Warning:** Text below the upload button: "If you return to version 1.13.x or later, configuration resets to default!".

- *Active Version of Firmware* - version of the firmware that is installed on the device;
- *Check for Update* - the button for firmware version actuality check. Using this function you can fast check availability of new firmware version and if it is needed update it.
- *Firmware Image* - the version of the firmware installed on the device, which can be accessed in case of problems with the active version of the firmware.
- *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 reserve.



**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 <http://eltex-co.com/support/downloads> and saving it to your computer. To do this, click the 'Select file' button in the *Software update file* field and specify the path to the control program file in .tar.gz format.

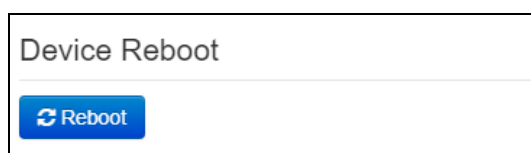
To start the update process, click the 'Upload file' button. The update process will take several minutes (its current status will be indicated on the page), after which the device will automatically reboot.



**Do not turn off the power or reboot the device during the software update process.**

#### 2.6.5.7 'Reboot' submenu

In the '*Reboot*' submenu you can reboot the device.



To reboot the device, click on the 'Reboot' button. The device reboot process takes about 1 minute.

#### 2.6.5.8 'Autoprovisioning' submenu

The '*Autoprovisioning*' submenu configures the DHCP-based autoprovisioning algorithm (autoconfiguration based on the DHCP protocol) and the automatic configuration protocol of the subscriber devices TR-069.

DHCP-based Autoprovisioning

Parameters Priority from

DHCP options

Configuration

Provisioning Mode

Periodically

Configuration File

(tftp(http://download.server.loc/config\_file.cfg))

Configuration Update Interval, s

300

Firmware

Provisioning Mode

Periodically

Firmware File

(tftp(http://download.server.loc/firmware.file))

Firmware Upgrade Interval, s

3600

TR-069 Autoconfiguration

Common

Enable TR-069 Client
☒

Interface
Internet

ACS Server Address
http://192.168.21.160:9595/

Enable Periodic Inform
☒

Periodic Inform Interval, s
60

ACS Connection Request

User Name
acs

Password
\*\*\*\*\*

Client Connection Request

User Name
admin

Password
\*\*\*\*\*

NAT Settings

NAT Mode
STUN

STUN Server Address
stun.local

STUN Server Port
3478

Minimum Keep Alive Period, s
30

Maximum Keep Alive Period, s
60

### 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 5;
  - DHCP options** - the paths to the configuration and firmware files are determined from the DHCP options 43, 66 and 67 (to do this, select the DHCP protocol for the Internet service); for more algorithm details see Section 5;
- Provisioning Mode** - to update the firmware configuration separately, you can specify one of several 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 configuration file is specified in the URL format (in this moment it is possible to download the configuration file using TFTP and HTTP):

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

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

where < server address > – HTTP or TFTP server address (domain name or IPv4),

< full path to cfg file > – 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 an one-time update only immediately after the device is loaded;
- *Time of Configuration Update* - time in 24-hour format in 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 > – HTTP or TFTP server address (domain name or IPv4),

< full path to firmware file > – full path to firmware file on server;

- *Firmware Update Interval, s* - the time interval in seconds after which the device firmware is periodically updated; selecting 0 means an 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 5.

### TR-069 Autoconfiguration

#### **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. If the *management interface* is enabled on the gateway, then this VLAN will automatically be used to work using the TR-069 protocol. Interface selecting setting will be locked;
- *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* - username and password for client access to the ACS server.

#### Client Connection Request:

*User Name, Password* - username 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. These technologies allow the client to identify its so called public address (NAT address or in other words external address of a gateway, that covers the client.) When public address is identified, the client reports it to the server that uses this public address for establishing connection to the client in the future.

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

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

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

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



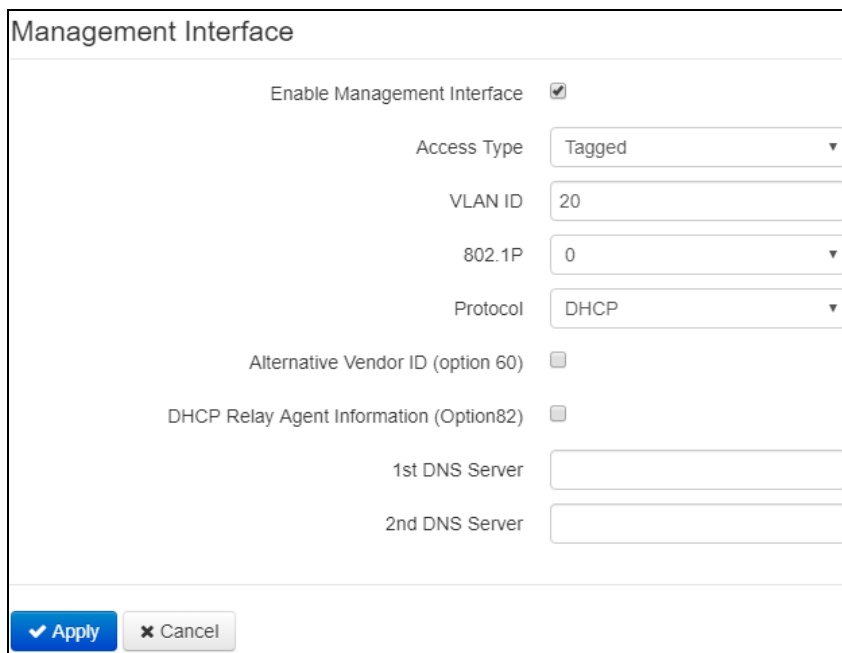
**To work correctly with an ACS server behind NAT, the minimum polling period of a STUN server must be less than the maximum save time of the session by the NAT device.**

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

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

### 2.6.5.9 'Management Interface' submenu

This submenu allows to configure the network interface to organize network device management via HTTP, HTTPS Telnet and SSH.



- *Enable Management Interface* - when checked the device is controlled via this interface;
- *Access Type* - sets interface operating mode:
  - *Tagged* - data is transmitted by the interface using the specified VLAN ID;
  - *Untagged* - data is transmitted by the interface without VLAN ID usage;
- *VLAN ID* - identifier for allocating an interface to a virtual local area network;
- *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 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* - setting the management interface IP address;
    - *Netmask* - management interface subnet mask;
    - *Default Gateway* - default management interface network gateway IP address;
    - *1st DNS server, 2nd DNS server* — DNS server IP addresses required for the autoconfiguration protocols of the gateway that are configured on the **System-Autoprovisioning** page.
  - *DHCP* – operation mode where IP address, subnet mask, DNS address and other necessary settings for interface operation (e.g. 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 '*Primary DNS*' and '*Secondary DNS*' fields. Manually defined addresses will have a priority over DNS addresses obtained via DHCP.



For DHCP, you may specify the required value for Option 60.

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

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

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

Example:

[VENDOR:Eltex][DEVICE:TAU-4M.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]  
[LAN:02:20:80:a8:f9:4b][VERSION:#2.3.1]

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

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

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

## 2.6.5.10 'Certificates' submenu

Certificates			
	Type	Common Name	Organization
<input type="checkbox"/>	Root Certificate	192.168.1.1	Eltex
<input type="checkbox"/>	Client Certificate	<no certificate>	
<input type="checkbox"/>	Web Certificate	192.168.1.1	Eltex Ent
<input type="button" value="Remove"/>			

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.

#### Root Certificate

Certificate

Serial Number

9A:95:D9:1C:51:C5:CD:DF

Not valid before

1/1/1970

Not valid after

12/31/1975

Subject

Common Name

192.168.1.1

Organization

Eltex

Subject Alternative Name

—

Name of the certification authority

Common Name

192.168.1.1

Organization

Eltex

Operation With Certificate

Download Certificate

Upload Certificate

No file chosen

- *Serial Number* — serial number of the chosen certificate;
- *Not valid before* — certificate start date;
- *Not valid after* — certificate end date;
- *Subject* — information about the certificate recipient (common name, organization, subject alternative name);
- *Name of the certification authority* — information about the certification authority (common name, organization).

## Client Certificate

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

Client Certificate

Certificate

Serial Number

Not valid before 29.03.2018

Not valid after 29.03.2019

Subject

Common Name Eltex

Organization Eltex

Subject Alternative Name –

Name of the certification authority (self-signed certificate)

Common Name Eltex

Organization Eltex

Operation With Certificate

Download Certificate

Download

Upload Certificate

Choose File

No file chosen

Upload

Back

- *Serial Number* - serial number of the chosen certificate;
- *Not valid before* - certificate start date;
- *Not valid after* - certificate end date;
- *Subject* - information about the certificate receiver (Common Name, Organization, Additional domain addresses);
- *Name of the certification authority* - authorization center information (Common name, Organization).

## WEB Certificate

The WEB certificate is used when accessing the device's WEB configurator via the HTTPS protocol.

Web Certificate

Certificate

Serial Number
FB:60:9A:A5:63:56:D9:9D

Not valid before
01/01/1970

Not valid after
18/01/2038

Subject

Common Name
192.168.1.1

Organization
Eltex Ent

Subject Alternative Name
—

Name of the certification authority (self-signed certificate)

Common Name
192.168.1.1

Organization
Eltex Ent

Operation With Certificate

Download Certificate
Download

Upload Certificate
Choose file No file chosen
Upload

Back

- *Serial Number* — serial number of the chosen certificate;
- *Not valid before* — certificate start date;
- *Not valid after* — certificate end date;
- *Subject* — information about the certificate recipient (common name, organization, subject alternative name);
- *Name of the certification authority* — information about the certification authority.

### 2.6.5.11 'Advanced' submenu

In the 'Advanced' submenu you can enable UPnP.

UPnP

Enable UPnP ☒

Reserved VLAN ID

Start VLAN ID
1

End VLAN ID
6

Apply Cancel

- *Enable UPnP* - when checked UPnP will be active. UPnP is used by some applications (for example, DC clients, such as FlylinkDC ++) to automatically create TCP / UDP port forwarding rules used by these applications on the upstream router. It is recommended to enable UPnP to enable file sharing services on the network.

#### Reserved VLAN ID

Reserved VLAN IDs are required for the gateway's internal system needs and can be changed depending on the VLAN ID used on the network:


- *Start VLAN ID* - the initial value of the VLAN identifier in the reserved range, may take values [1-4090];
- *End VLAN ID* - the final value of the VLAN identifier in the reserved range. This setting is not editable and is calculated automatically.

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

## 2.7 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 obtain current information from the device, click the  button.

### 2.7.1 'Internet' submenu

In the '*Internet*' submenu you can view common network settings of the device.

#### Internet Connection

Network Connection	Wired
Access Protocol	DHCP
IP Address	192.168.21.1



#### Internet Connection

- *Network Connection* - type of network connection. You can configure the connection in the '**Network** -> **Internet**' section:
  - *Wired* - connection to the provider's network is made by connecting a copper or optical patch cord to the WAN port;
  - *3G/4G USB modem* - connection to the provider's network via 3G/4G USB modem connected to the USB port on the back of the device.
- *Access Protocol* - protocol, used for Internet access;
- *IP address* – device IP address in external network;
- *Internal IP address* - the IP address that is used in the provider's internal network to access the local network resources of the provider.

When **Automatically Switch to Redundant Channel** connection method is selected, the following fields will be available for configuration:

- *Connection Availability* - shows ping server availability through this connection;
- *Activity* - shows that interface is used for user data transmission.

## 2.7.2 'VoIP' submenu

In the 'VoIP' submenu, you can view the state of the VoIP network interface, monitor subscriber sets and call group registration status, test lines, IMS.

Status of VoIP Network Interface

IP Address

192.168.1.24

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"/> 1	001	None			Inactive					<button>Test</button>	<button>Show</button>
<input type="checkbox"/> 2	002	None			Inactive					<button>Test</button>	<button>Show</button>
<input type="checkbox"/> 3	003	None			Inactive					<button>Test</button>	<button>Show</button>
<input type="checkbox"/> 4	004	None			Inactive					<button>Test</button>	<button>Show</button>

Register

Unregister

Hunt Groups Status

Group Name	State	Phone	Line List	Registration	Expires In	Server Address
Group1	Disabled			None		
Group2	Disabled			None		
Group3	Disabled			None		
Group4	Disabled			None		
Group5	Disabled			None		

IMS Monitoring

Line	1	2	3	4
IMS Management	Off	Off	Off	Off
Three-party Conference	-	-	-	-
Call Hold	-	-	-	-
Call Waiting	-	-	-	-
Hotline	-	-	-	-
Hotline Number	-	-	-	-
Hotline Timeout, s	-	-	-	-
XCAP Name for Call Transfer	-	-	-	-


### 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:
  - *Disabled* - registration on SIP server function is disabled in SIP profile configuration;
  - *Failed* - registration failed;
  - *Ok* - registration on SIP server is successful.
- *Expires In* - time before the expiration of registration 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. Line can be in following states:
  - *Inactive* - the handset is offhook (or subscriber port is disabled), normal work;
  - *Active* - the handset is onhook; 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. Call can be in following states:
  - *Dial* - dialing from a telephone set;
  - *Busy* - the call for some reason is strayed, 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 usually issued 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.
- *Line Test* - the subscriber line testing process is starting after clicking on the 'Test' button. The status of the process is indicated by a reverse timer (in the 'Line State' column), which indicates the remaining test time. Do not launch the test for multiple ports simultaneously. 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
<input type="checkbox"/> 1	210101	Ok	00:19:28	192.168.21.160	Testing (78 s)					

At the end of the test, the result can be viewed by clicking on 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;*
- *Capacity A (TIP) - B (RING);*
- *Capacity A (TIP) - Ground;*
- *Capacity B (RING) - Ground;*
- *Telephone set* — information on telephone availability.



Line 1 test result example:

Test Result: Line 1	
Test Date	04:14:51 02.01.1970
Foreign DC Voltage A (TIP)	0.094453 U
Foreign DC Voltage B (RING)	0.063521 U
Foreign AC Voltage A (TIP)	0.025163 U
Foreign AC Voltage B (RING)	0.022896 U
Line Supply Voltage	-51.930691 U
Cross Current	0.414878 mA
Longitudinal Current	0.405639 mA
Resistance A (TIP) - B (RING)	1009.705566 kΩ
Resistance A (TIP) - Ground	504.494354 kΩ
Resistance B (RING) - Ground	283.437805 kΩ
Capacity A (TIP) - B (RING)	50 nF
Capacity A (TIP) - Ground	50 nF
Capacity B (RING) - Ground	50 nF
Telephone Set	Not connected
<div> <div>Remove</div> <div>Close</div> </div>	

- *FXS statistics* - the number of incoming and outgoing calls received on the port and the last number dialed.

FXS statistics: Line 1	
Last Call Number	6001
Incoming Calls Count	1
Outcoming Calls Count	2
<div> <div>Close</div> <div>Reset statistics</div> </div>	

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

### Hunt Groups Status

- *Group name* - call group name;
- *State* - call group state: enabled or disabled;
- *Phone* – phone number assigned to the call group;
- *Line List* - line (ports) list that includes call group.
- *Registration* - state of group phone number registration on proxy server:

- *Disabled* - 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 call group on SIP server;
  - *Server Address* - address of the server where the call group was last registered.

### IMS Monitoring


IMS monitoring shows the status of some services (enabled or disabled) on each subscriber line, provided that this line allows remote control from the IMS server (IP Multimedia Subsystem).

- *IMS Management* - indicates whether or not remote control of subscriber line services is enabled from the IMS server (configured in the SIP profile, see the 'SIP Profiles' submenu);
- *Three-party Conference* - indicates whether or not the team to enable the 'Three-party Conference' service from the IMS server has arrived;
- *Call Hold* - indicates whether or not the 'Call Hold' service enabling command came from the IMS server;
- *Call Waiting* - indicates whether or not the 'Call Waiting' service enabling command came from the IMS server;
- *Hotline* - indicates whether or not the 'Hotline' service enabling command came from the IMS server;
- *Hotline Number* - shows the phone number for the 'Hotline' service in the enabling command from the IMS server;
- *Hotline Timeout, s* - shows the timeout for the 'Hotline' service in the enabling command from the IMS server.
- *XCAP Name for Call Transfer* - shows the specified 'Call Transfer' service name.

- ✓ - on
- ✗ - off

### 2.7.3 'Ethernet Ports' submenu

In the '*Ethernet Ports*' submenu, you can view the status of the device Ethernet ports.

State of Ethernet Ports					
Port	Connection	Speed	Mode	Transmitted	Received
WAN	On	100 Mbit/s	Full-duplex	4.4 M (4 621 224 B)	23.3 M (24 443 293 B)
LAN	Off				
 Refresh					

### State of Ethernet Ports


- *Port* – port name:
  - *WAN* - external network port;
  - *LAN* - local network port.
- *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* - full duplex;
  - *Half-duplex* - half duplex;
- *Transmitted* - amount of transmitted bytes from port;
- *Received* - amount of received bytes from port.

To get current information about the status of Ethernet ports, click the Refresh button.

#### 2.7.4 'DHCP' submenu

In the '*DHCP*' submenu you can view a list of network devices connected to the LAN interface, which were assigned IP addresses by the local DHCP server, as well as the time until IP address lease expires.

List of DHCP Clients			
MAC Address	Client Name	IP Address	Lease Expires
			


##### List of DHCP Clients

- *MAC Address* - MAC address of the connected device;
- *Client Name* - network name of the connected device;
- *IP Address* - IP address assigned to client from address pool;
- *Lease Expires* - the period after which the lease of the dedicated address expires.

To get current information about the DHCP clients, click the '*Refresh*' button.

#### 2.7.5 'ARP' submenu

In the '*ARP*' submenu, 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.

ARP Table			
IP Address	MAC Address	Client Name	Interface
192.168.21.160	52:54:00:67:2E:6F		WAN
			

## ARP Table

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

To get current information, click the '*Refresh*' button.

## 2.7.6 'Device' submenu

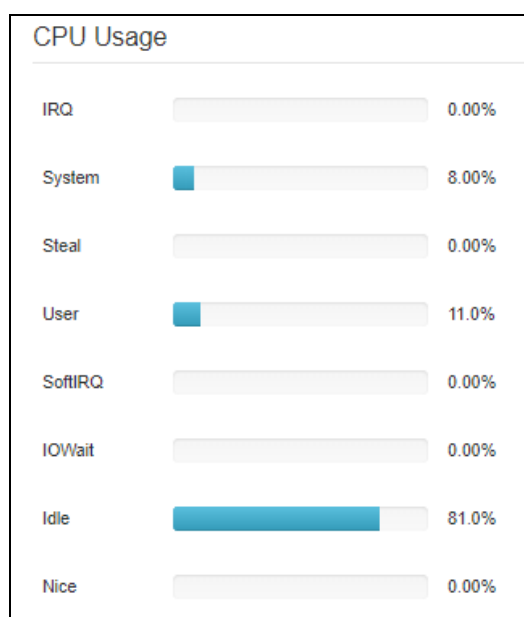
The '*Device*' submenu contains common information about the device.

Device Info	
Product	TAU-4M.IP
Firmware Version	
Factory MAC Address	A8:F9:4B:2A:93:4E
Serial Number	VI4D000045
System Time	11:03:07 05.03.2020
Uptime	1 d, 20:03:03

## 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 time the device was switched on or rebooted.

## 2.7.7 'CPU' submenu



## CPU Usage

- *IRQ* – percentage of CPU time spent on hardware interrupts processing;
- *System* – percentage of CPU time spent by kernel processes;
- *User* – percentage of CPU time spent by user programs;
- *SoftIRQ* – percentage of CPU time spent on software interrupts processing;
- *IOWait* – percentage of CPU time spent on input/output operations;
- *Idle* – idle CPU resources percentage;
- *Nice* – percentage of CPU time spent by programs with changed priority.

## 2.7.8 'Conntrack' submenu

In the 'Conntrack' submenu you can view current active network connections of the device.

Active NAT Session

Active Connections Count

12

Shown Connections Count

12

List of Connections

Protocol	Source Address	Destination IP	Timeout
UDP	192.168.1.1:35139	239.255.255.250:1900	8 s
TCP	192.168.27.136:65184	192.168.21.1:80	17 s
IGMP	192.168.1.1	224.0.0.1	9 min 59 s
TCP	192.168.27.136:65286	192.168.21.1:80	1 min 55 s
TCP	192.168.27.136:65244	192.168.21.1:80	1 min 4 s
UDP	192.168.21.160:5060	192.168.21.1:5060	2 min 48 s
TCP	192.168.27.136:65272	192.168.21.1:80	1 min 38 s
TCP	192.168.27.136:65301	192.168.21.1:80	4 d 23 h 59 min 59 s
TCP	192.168.27.136:65257	192.168.21.1:80	1 min 21 s
TCP	192.168.27.136:65183	192.168.21.1:80	17 s
TCP	192.168.27.136:65217	192.168.21.1:80	49 s
IGMP	0.0.0.0	224.0.0.22	7 min 14 s

Refresh

## Active NAT Session

- *Active Connections Count* - total number of active network connections;
- *Shown Connections Count* - number of connections shown in WEB interface. In order not to reduce the performance of the WEB-interface, the maximum number of shown connections is limited to 1024. All another connections you can view in device's command console (command `cat /proc/net/nf_conntrack`).

### List of Connections


- *Protocol* - protocol by which the connection has been established;
- *Source Address* - connection initiator IP address and port number;
- *Destination IP* - connection destination IP address and port number;
- *Timeout* - time period before the disconnection.

To get current information, click the '*Refresh*' button.

## 2.7.9 'Routes' submenu

In the '*Routes*' submenu, you can view the device routing table.

Routes							
Destination	Gateway	Netmask	Flags	Metric	Ref	Use	Interface
192.168.21.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
224.0.0.0	0.0.0.0	240.0.0.0	U	0	0	0	eth1
0.0.0.0	192.168.21.160	0.0.0.0	UG	0	0	0	eth1



- *Destination* – IP address of destination host or subnet that the route should be established to.
- *Gateway* – gateway IP address that allows for the access to the Destination.
- *Netmask* — a subnet mask;
- *Flags* – certain route characteristics. The following *flag* values exist:
  - **U** - shows that route is created and is passable;
  - **H** - points to the route to a particular node;
  - **G** - indicates 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** - indicates that the route was most likely created by a dynamic routing protocol running on the local system using the *reinstall* parameter;
  - **D** - indicates 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. This routes marked with flag D;
  - **M** - indicates 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** - points to a buffered route to which an entry in the ARP table corresponds.
  - **C** - indicates that the source of the route is the core routing buffer;

- get current information, click the 'Refresh' button.

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

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

Description of the 'call history' table fields:

- 
- |                              |     |
|------------------------------|-----|
| TAU-4M.IP Subscriber gateway | 103 |
|------------------------------|-----|





- *Type* - call type: incoming or outgoing;
- *TxPack* - the number of RTP packets transmitted during a call;
- *TxBytes* - amount of transmitted bytes during the conversation;
- *RxPack* - the number of RTP packets received during a call;
- *RxBytes* - amount of received bytes during the conversation;

In the call history table, you can select records by various parameters. To do this, click the 'Filter (show)' link. Filtering can be done by subscriber line number, local or remote number, counter party's IP address, call arrival time, call start time, call status and call type. The description of the filtering parameters is listed in the description of the fields in the call history table above.

*Start Call Time, from/to or Start Talk Time, from/to* - the time frame for receiving/making a call or beginning a conversation in the format 'hh:mm:ss dd.mm.yyyy'.

To hide the settings for filtering records in a table, click the *Filter (hide)* link.

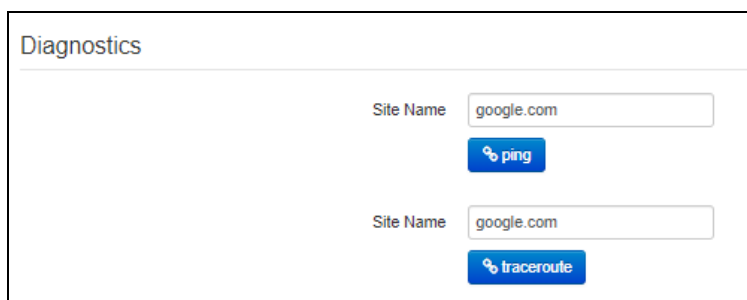
To set up call history settings, click on the 'Change Call History Settings' link. For detailed description of parameter settings see Section 2.6.3.10 'Call History' submenu .

- |                 |                                                                                     |                                                                    |
|-----------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Clicking on the |    | button will switch to the table, starting from the first entry.    |
| Clicking on the |    | button will move to the previous page with the call history table. |
| Clicking on the |    | button will move to the next page with the call history table.     |
| Clicking on the |  | button will switch to the table, ending with the last entry.       |

Selecting 'records per page' allows you to customize the number of displayed table entries on a single page.

### 2.7.11 'Diagnostics' submenu

The submenu can be used to check the accessibility of a node in the network and determine a data transfer route.



Network utilities:

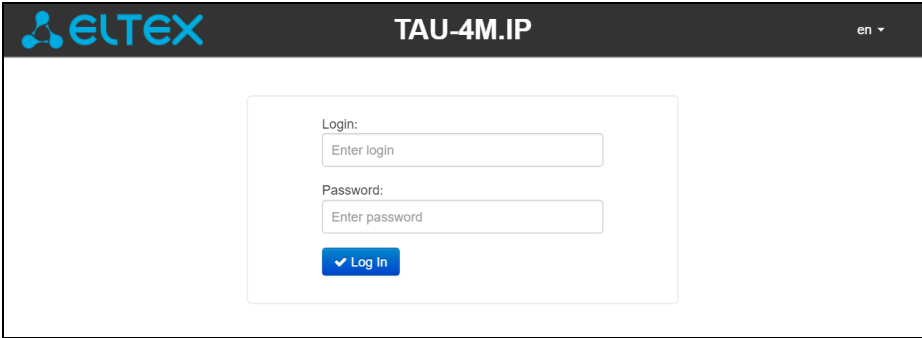
- *Ping* — the utility used to test hosts on TCP/IP networks for reachability.
- *Traceroute* — the utility used to determine the route according to which packets move.




## 2.8 Configuration example

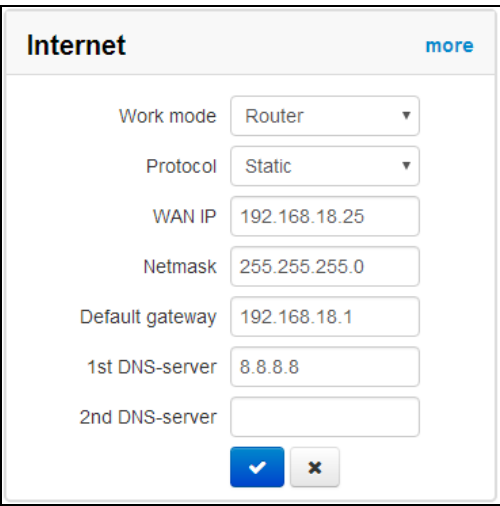
Connect the PC to one of the device's LAN ports, connect the wire from the provider's network to the WAN port;

- In the address bar of the browser, enter the IP address of the gateway (by default 192.168.1.1);
- When the device connection is established, a window will appear asking for your login and password. Fill in the fields and click the 'Log In' button (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.

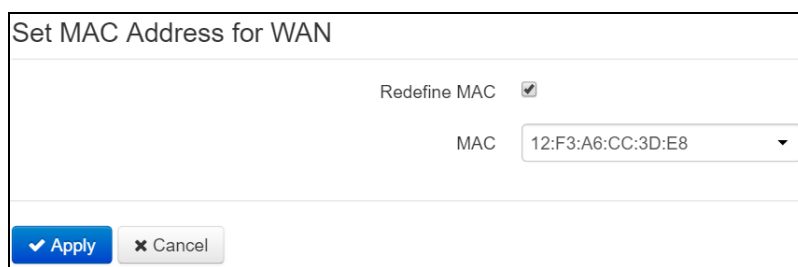
- In the 'Internet' tile you can configure external connection. If *TAU-4M.IP* will be used as a router - select the value of the 'Work mode' field - the router in the 'Internet' tile. In the 'Protocol' field, select the protocol used by your internet service provider and enter the required data according 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 the provider. To save and apply changes, click .



To specify additional parameters, go to advanced settings mode by clicking the 'more' link (see Section 2.6.2.1 'Internet' submenu).

- If your Internet provider's network uses binding to the MAC address, click the 'more' in the 'Internet' tile and open the 'MAC management' submenu. In the 'Set MAC address for WAN' section, check the 'Redefine MAC' flag and enter the MAC address of the device that was

previously connected to the Internet in the MAC field. To save and apply changes click the 'Apply' button.




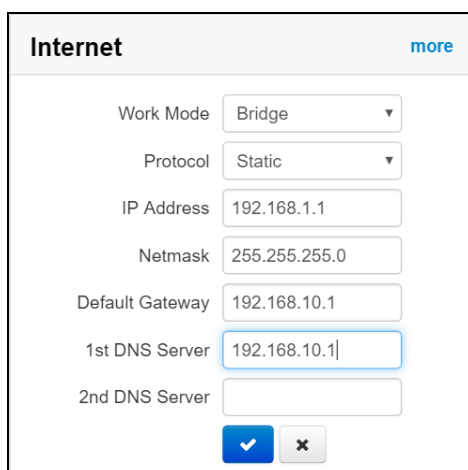
Set MAC Address for WAN

Redefine MAC ☒

MAC 12:F3:A6:CC:3D:E8

✓ Apply ✕ Cancel

If *TAU-4M.IP* will be used as a 2-port switch - select the value of the 'Work mode' field - the bridge in the 'Internet' tile. In the 'IP-address' field, specify the address that will be assigned to the device to access it. Enter the subnet mask (default: 255.255.255.0) To save and apply changes click .



**Internet** [more](#)

Work Mode Bridge

Protocol Static

IP Address 192.168.1.1

Netmask 255.255.255.0


Default Gateway 192.168.10.1

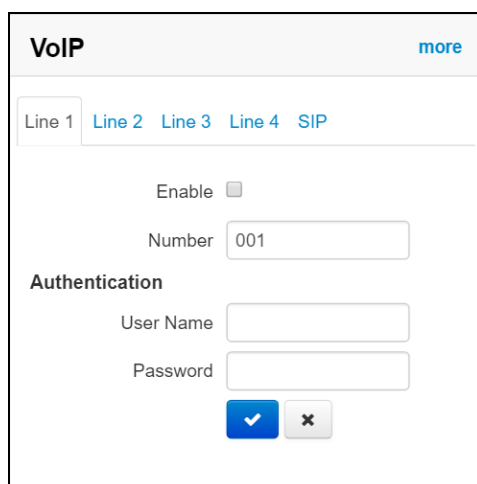
1st DNS Server 192.168.10.1

2nd DNS Server

✓ ✕

In the 'Bridge' mode gateway will not automatically output IP addresses via DHCP to devices that connected to the LAN interface.

- In the 'VoIP' tile, you can perform quick configuration of subscriber lines for operating with SIP. For this select the 'Line' tab with number of the line that should be configured. Select the 'Enable' checkbox, input the number of the phone that will be on this line, user name and password for SIP server authorization. To save and apply changes, click .



**VoIP** [more](#)

Line 1 **Line 2** Line 3 Line 4 SIP

Enable ☐

Number 001


**Authentication**

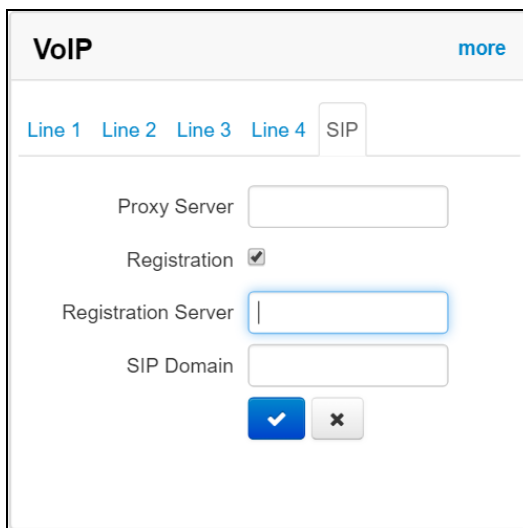
User Name

Password

✓ ✕


The subscriber line in another 'Line' tab is configured the same way.

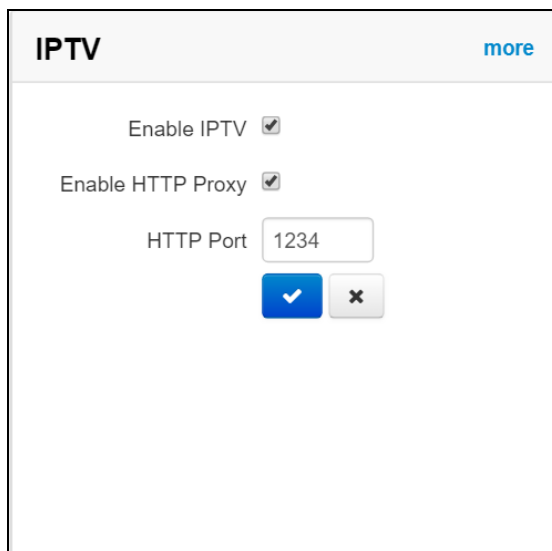
- Select the SIP tab in the 'VoIP' tile to configure the SIP settings. Enter the SIP and registration servers IP address or domain name (if necessary) in the corresponding fields. If servers use port numbers other than 5060, then set alternate ports after a colon. Specify the SIP domain if necessary. Select the 'Registration' checkbox if you need to register subscribers on a SIP server for telephony to work (usually, registration is required). To save and apply changes click .



The image shows the 'VoIP' configuration interface. At the top, there's a header with 'VoIP' and a 'more' link. Below the header, there are tabs for 'Line 1', 'Line 2', 'Line 3', 'Line 4', and 'SIP'. The 'SIP' tab is selected. The configuration fields include: 'Proxy Server' (text input), 'Registration' (checkbox, checked), 'Registration Server' (text input), and 'SIP Domain' (text input). At the bottom, there are two buttons: a blue checkmark button and a grey 'x' button.

To specify additional parameters, go to advanced settings mode by clicking the 'more' link (see Section 2.6.3 'VoIP' menu).

- If you intend to use IPTV - check the 'Enable IPTV' unit in the 'IPTV' tile. To enable the IPTV streams transmission over HTTP, check the 'Enable HTTP proxy' unit. In the 'HTTP port' field, specify the port that will be used to connect external devices to the local HTTP proxy. To save and apply changes, click .



The image shows the 'IPTV' configuration interface. At the top, there's a header with 'IPTV' and a 'more' link. Below the header, there are checkboxes for 'Enable IPTV' and 'Enable HTTP Proxy', both of which are checked. Below these, there is an 'HTTP Port' field with the value '1234'. At the bottom, there are two buttons: a blue checkmark button and a grey 'x' button.

If a separate VLAN is used for the IPTV service, switch to the advanced settings mode by clicking the 'more' link and enter the VLAN ID in the corresponding field.

## 3 VALUE ADDED SERVICES USAGE

### 3.1 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 -> Lines Settings'—by selecting 'Attended calltransfer' or 'Unattended calltransfer' in 'Flash mode' field.

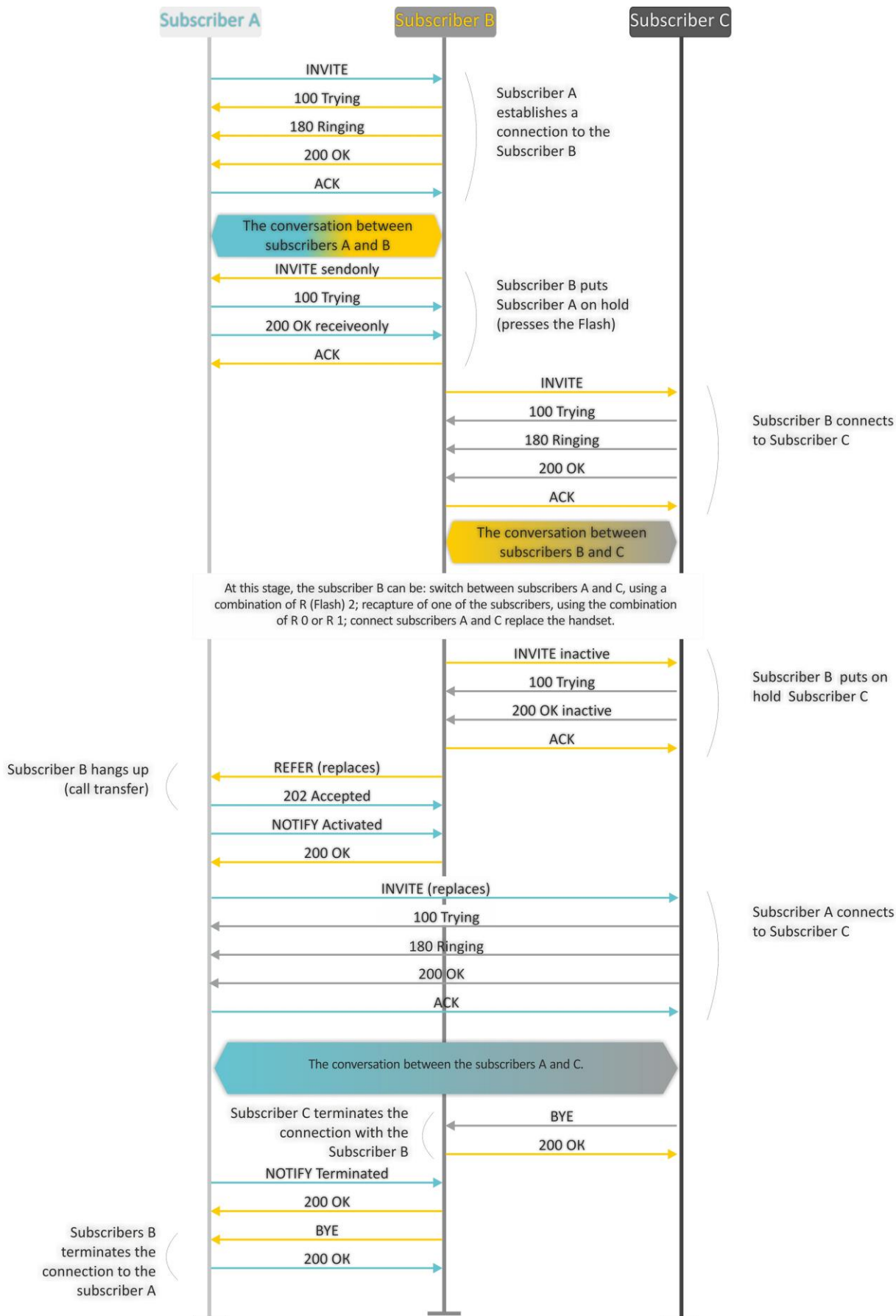
'Attended calltransfer' service allows you to temporarily disconnect an online subscriber (Subscriber A), establish connection with another subscriber (Subscriber C) and return to the previous connection without dialling or transfer the call while disconnecting Subscriber B (a subscriber that performs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

'Attended calltransfer' service usage:

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

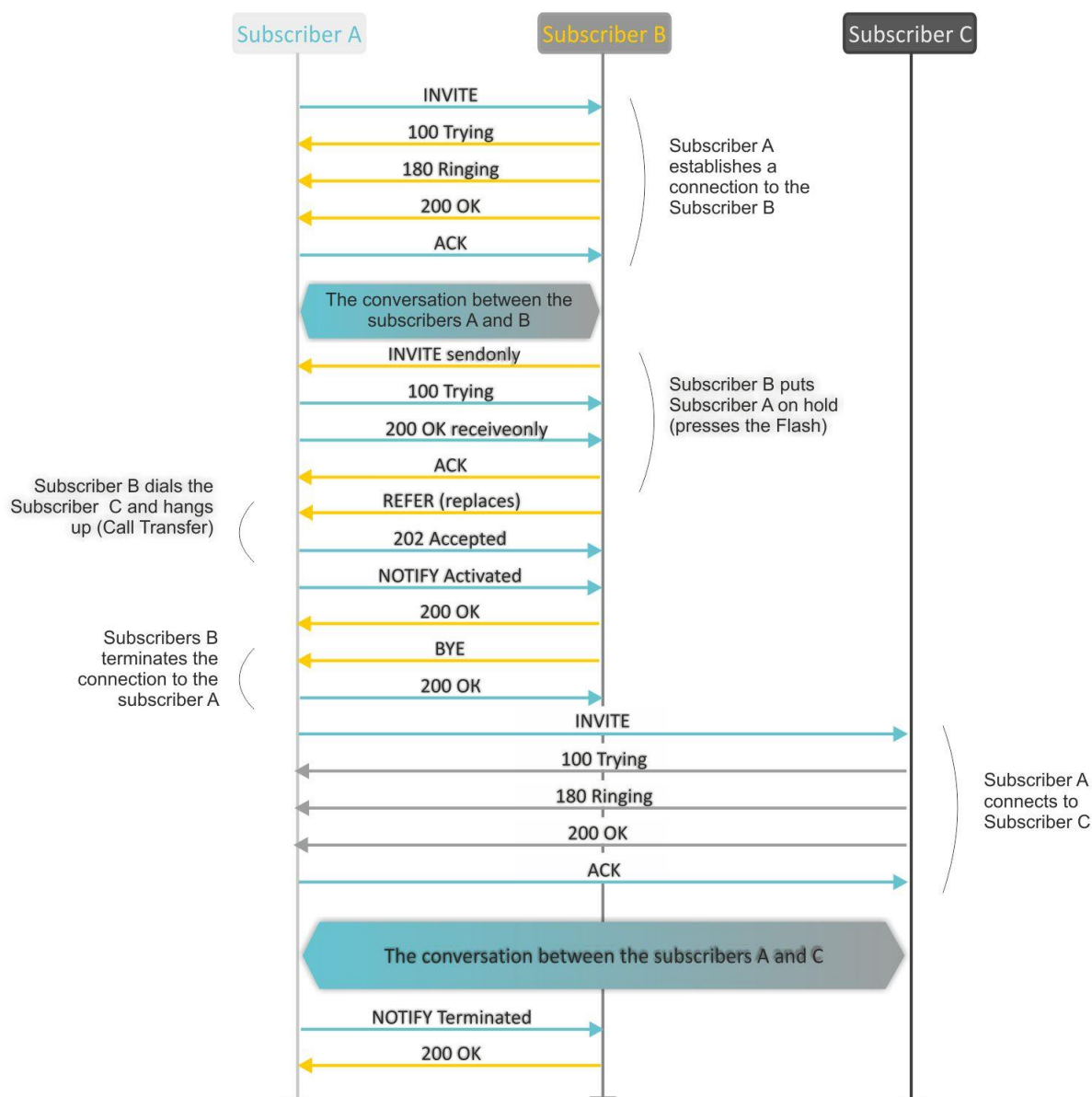
- R 0—disconnect a subscriber on hold, connect to online subscriber;
- R 1—disconnect an online subscriber, connect to subscriber on hold;
- R 2—switch to another subscriber (change a subscriber);
- R 3—conference;
- R 4—call transfer. Voice connection will be established between Subscribers A and C.
- R clearback—call transfer. Voice connection will be established between Subscribers A and C.

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 dialling the number.

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-4M.IP*, subscriber and call was made directly, without proxy server. If subscriber C is external subscriber or local, but has been dialed using proxy server, 'Local Calltransfer' service processing as 'Attended Calltransfer', ie call transfer is carried out by sending the REFER message to subscriber B.

## 3.2 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 selecting '*Call waiting*' checkbox.

Service usage:

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

- R 0—reject a new call;
- R 1—answer the waiting call;
- R 2—switch to new call (change a subscriber);
- R – short clearback (flash).

## 3.3 Three-way conference

Three-way conference is a service, that enables simultaneous phone communication for 3 subscribers. For entering conference mode, see Section 3.1 Call Transfer.

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

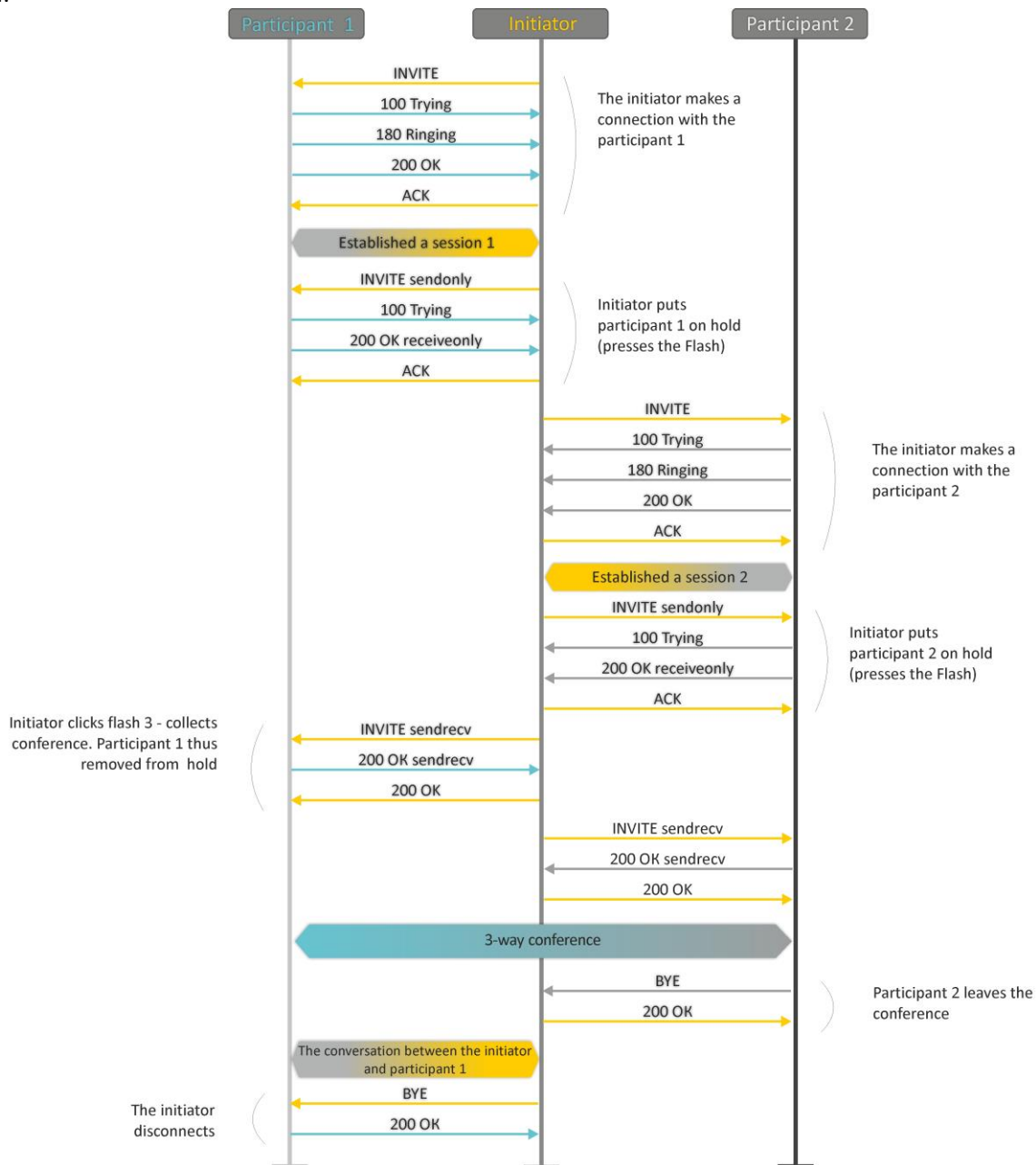
Two modes are available: local and remote. In the first mode, the conference is assembling locally by the initiator subscriber; in the second, the conference is established using a remote server, the so-called conference server.

### 3.3.1 Local conference

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

The conference terminates, when initiator leaves; in this case, both participants will receive clearback message. If one of the participants leaves the conference, the initiator and the second participant will switch into a standard two-party call. Short flash clearback is processed as described in Sections 3.1 Call Transfer and 3.2 Call Waiting.

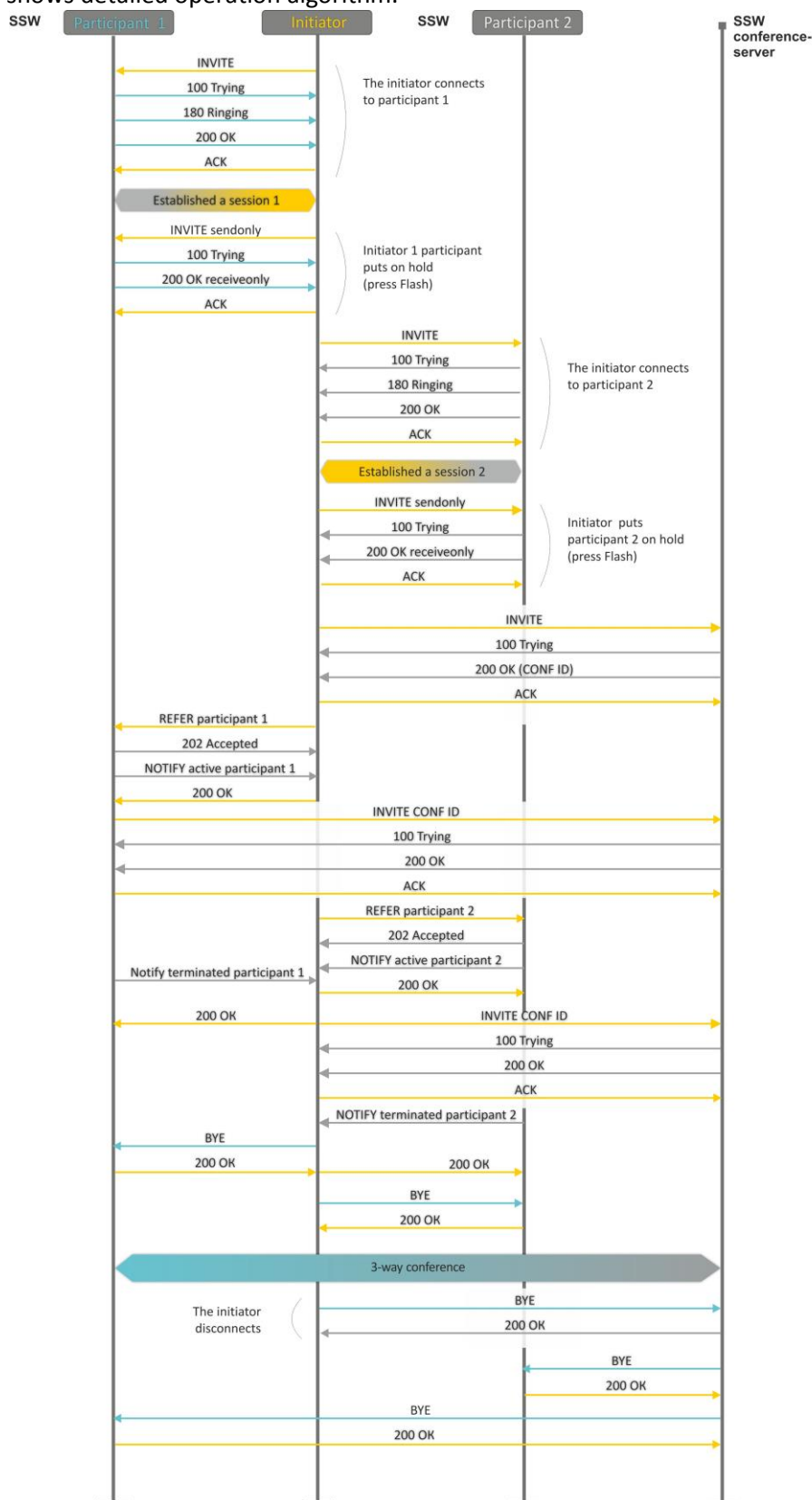
Figure below shows an algorithm of '3-way conference' service performed locally by subscriber B via SIP protocol.





### 3.3.2 Remote conference

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

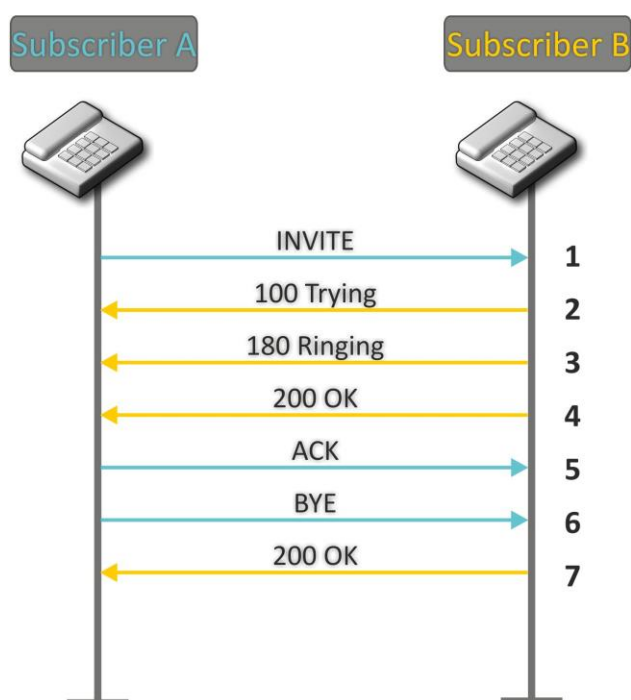


## 4 CONNECTION ESTABLISHMENT ALGORITHMS

### 4.1 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.

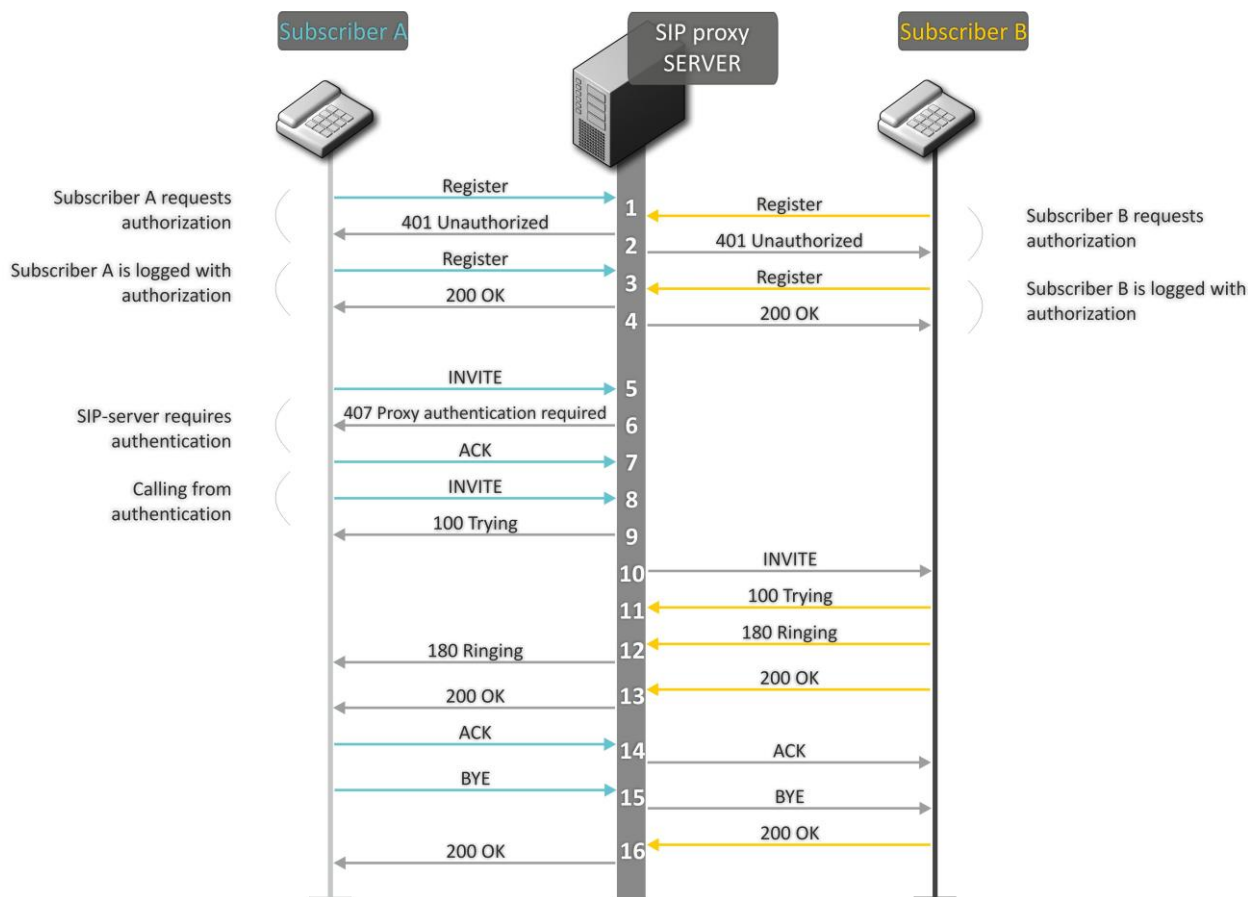


Algorithm description:

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

## 4.2 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.



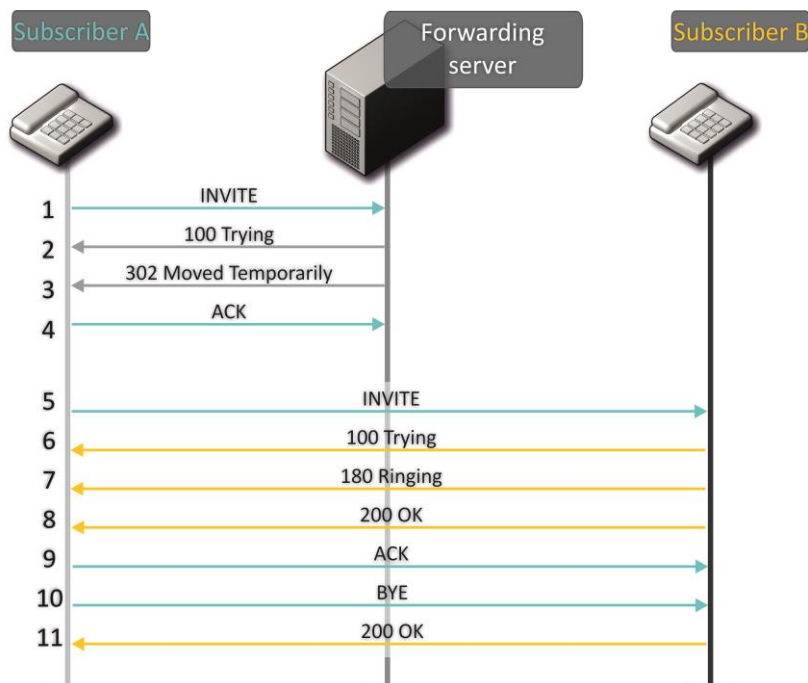
Algorithm description:

Subscriber A and Subscriber B register at SIP server.

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

### 4.3 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:

1. Subscriber A rings up Subscriber B. Forwarding server receives the command for processing.
2. Forwarding server receives the command for processing.
3. Forwarding server requests the information on the Subscriber B current address from the location server. Received information (the callee current address and the list of callee registered addresses) is sent to Subscriber A in '302 moved temporarily' message.
4. Subscriber A gateway confirms the reception of reply from the forwarding server.
5. Subscriber A rings up Subscriber B directly.
6. Subscriber B gateway receives the command for processing.
7. Subscriber B is free. Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone to Subscriber A phone.
8. Subscriber B answers the call.
9. Subscriber A gateway confirms session establishment.
10. Subscriber A clears back, 'busy' audio tone is sent to the Subscriber B.
11. Subscriber B gateway confirms received clearback command.

## 5 DEVICE AUTOMATIC UPDATE ALGORITHM BASED ON DHCP

### DHCP-based Autoprovisioning

Parameters Priority from

DHCP options

Configuration

Provisioning Mode

Periodically

Configuration File

(tftp(http://download.server.loc/config\_file.cfg))

Configuration Update Interval, s

300

Firmware

Provisioning Mode

Periodically

Firmware File

(tftp(http://download.server.loc/firmware.file))

Firmware Upgrade Interval, s

3600

Automatic device update procedure algorithm is determined by the '*Parameters priority from*' parameter value.

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> – protocol that used for downloading the corresponding file from server (supports HTTP and TFTP);

<server address> – address of the server from which the file should be downloaded (domain name or IPv4);

<path to file> – 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-4M.IP) in the file URL;

\$SWVER – Software version – instead of this macro, the device inserts its firmware 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' section.

URL examples:

```
tftp://download.server.loc/firmware.file,
http://192.168.25.34/configs/tau4m/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_tau4m.cfg
```

If it is impossible to extract all the parameters required for downloading the file from the configuration or software 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 a server address: update.local;
- For a configuration file name tau4m.cfg;
- For a firmware file name tau4m.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 like:

```
tftp://update.local/tau4m.cfg,
```

and the URL of the firmware file:

```
tftp://update.local/tau4m.fw.
```

If 'DHCP options' value is selected, URLs 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 a server address: update.local;
- For a configuration file name tau4m.cfg;
- For a firmware file name tau4m.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>
```

>

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

2—Provisioning code suboption number;

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

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

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

- 6 - configuration file name code;
- 7 - firmware file name code;

'|' - 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 'Autoconfiguration based on the DHCP' section.**

**Algorithm for determining the parameters of the URL configuration files and software from the 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, and 7 are analyzed to determine the server address and the names of the configuration files and software.

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 is searched. 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 extracted 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.**

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

If the current firmware version matches the version of the file received via DHCP, the firmware will not be updated. Updating is performed only in case of a version mismatch. The running process of recording a firmware image to the flash memory of the device is indicated by the alternating cyclical blinking of the 'Power' indicator in green, orange and red.



**Do not turn off the power or overload the device while writing the image to flash-memory. These actions will lead to a partial recording of firmware, which is equivalent to damage to the boot partition of the device. Further operation of the device will be impossible. To restore the device, use the instructions provided in the section 6.**

## 6 SYSTEM RECOVERY AFTER A FIRMWARE UPDATE FAILURE

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

- Unpack the firmware file.
- Connect the PC to the device's WAN port, set the address from the 192.168.1.0/24 subnet on the network interface.
- Run the TFTP client on the PC (for Windows, it is recommended to use the Tftpd32), specify 192.168.1.6 as the remote host address, and select the linux.bin file from the unpacked software archive for transfer.
- Run the command to send a file to a remote host (the **Put** command). The process of transferring the file to the *TAU-4M.IP* device should start.
- If the file transfer process has begun - wait for it to finish, after which the *TAU-4M.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. At the same time, the device saves the configuration that was before the failure. If you can not connect to the device - reset to factory settings.
- 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).



## APPENDIX A. CALCULATION OF PHONE LINE LENGTH

Table - Electrical resistance/cable type relationship for 1km of DC subscriber cable lines.

Cable grade for subscriber lines of local exchange network	Core diameter, mm	Electrical resistance of 1km circuit, $\Omega$ , max	Line length (another TA), km	Line length (TA Rus), km
TPP, TPPEp, TPPZ, TPPEpZ, TPPB, TPP epB, TPPZB, TPPBG, TPPEpBG, TPPBbShp, TPPEpBbShp, TPPZBbShp, TPPZepBbShp, TPPT	0.32	458.0	3.537	1.528
	0.40	296.0	5.473	2.365
	0.50	192.0	8.438	3.646
	0.64	116.0	13.966	6.034
	0.70	96.0	16.875	7.292
TPV, TPZBG	0.32	458.0	3.537	1.528
	0.40	296.0	5.473	2.365
	0.50	192.0	8.438	3.646
	0.64	116.0	13.966	6.034
	0.70	96.0	16.875	7.292
TG, TB, TBG, TK	0.40	296.0	5.473	2.365
	0.50	192.0	8.438	3.646
	0.64	116.0	13.966	6.034
	0.70	96.0	16.875	7.292
TStShp, TASHp	0.50	192.0	8.438	3.646
	0.70	96.0	16.875	7.292
TSV	0.40	296.0	5.473	2.365
	0.50	192.0	8.438	3.646
KSPZP	0.64	116.0	13.966	6.034
KSP, KSPZ, KSPPB, KSPZPB, KSPPt, KSPZPt, KSPZPK	0.90	56.8	28.521	12.324

## 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-4M.IP device provides the ability to configure the launch of an arbitrary script through the configuration file, in which you can put any desired sequence of commands.

For user-defined script execution, use the following settings section 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 launch, the path to which is specified in the URL parameter.

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

### 1. Launch from HTTP server

To run the script from the HTTP server, you must 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. Launch from TFTP server

To run the script from the TFTP server, you must 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. Local script launch

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 the `chmod 777` command /etc/config/user.sh.

In the configuration file, the URL for launching 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`.

## APPENDIX C. DHCP CLIENTS CONFIGURATION IN MULTISERVICE MODE

On *TAU-4M.IP* devices, starting with version 1.14.1, it is possible to configure the options received by DHCP clients on different interfaces.

Option	Only Internet interface	Internet + VoIP		Internet + VoIP + Managment		
		Internet	VoIP	Internet	VoIP	MNG
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 DHCPOptionList entry: ""), this means that the options are requested and applied according to the table above.

## Configuration editing methods

### I. 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.
3. The list of options for the Management interface is specified in the DHCPOptionList parameter of the System => ManagementVLAN section.

After editing and saving in the vi editor, you must 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' execution is not allowed.

### II. 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:** You need to get the DHCPOptionList value:

for Internet interface

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

for VoIP interface

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

for Management interface

```
getconf System.ManagementVLAN | grep DHCPOptionList
```

**Example 2:** You need 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 ""
```

for Management interface

```
setconf System.ManagementVLAN DHCPOptionList "3,6,26,28,33,42,43,66,67,121,249"
```

### III. Using PC

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



**This method is not recommended!**

### DHCPOptionList Editing Rules

1. Valid values: 3,6,12,15,26,28,33,40,41,42,43,66,67,120,121,249;
2. 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';
3. The order of options in DHCPOptionList is not important;
4. Each of the options 12, 15, 40, 41, 42, 43, 66, 67, 120 can be requested and applied from only one interface;
5. Options 1, 3, 6, 26, 28, 33, 121, 249 may be requested by DHCP clients for each subinterface;
6. Options 66 and 67 must be specified on the same interface;
7. If nothing is specified in the DHCPOptionList, then the list of requested options will be default (subject to clause 8);
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 \*;
9. If a list of options is specified for the interface in the DHCPOptionList, then only these options will be requested;
10. Option 1 in the DHCPOptionList can not be specified, it is requested and applied always and from all interfaces regardless of other settings;

If any of the items is breached, then when applying the configuration, the 'Configuration not accepted' message will be displayed. You can find out the configuration error if you enable the configd logs, then when applying the configuration, the reason for which the configuration is not applied will be indicated in detail.

#### \* Example for item 8:

Suppose the following list of options is specified for the Internet interface: Internet.Network.DHCPOptionList: '3, 6, 26, 28, 33, 121, 249, 12'

And for the management interface nothing is specified: System.ManagementVLAN.DHCPOptionList: ""

then, according to unit 7, the default option list should be 3, 6, 12, 15, 26, 28, 33, 40, 41, 42, 43, 66, 67, 121, 249, but since option 12 is explicitly specified on the Internet interface, it will be excluded from this list.

Finally the following lists will appear:

parameter value: Internet.Network.DHCPOptionList: '3, 6, 26, 28, 33, 121, 249, 12' requested list of options: 1, 3, 6, 26, 28, 33, 121, 249, 12 parameter value: System.ManagementVLAN.DHCPOptionList: "" requested list of options: 1, 3, 6, 15, 26, 28, 33, 40, 41, 42, 43, 66, 67, 121, 249



**After editing the DHCPOptionList, device reboot is recommended. Correct device operation is not guaranteed until the device is rebooted.**

## TECHNICAL SUPPORT

Contact Eltex Service Center to get technical support regarding our products:

29v Okružnaya st., Novosibirsk, Russian Federation, 630020

E-mail: [eltex@eltex-co.ru](mailto:eltex@eltex-co.ru)

Visit Eltex official website to get the relevant technical documentation and software or send us online request.

Official website: <https://eltex-co.com/>

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