TAU-1M.IP

Operation Manual
v 1.5 (05.2016)

VoIP Gateway

Document version	Issue date	Revisions
Version 1.5	23 May 2016	Updated according to firmware version 1.13.1
Version 1.4	03 February 2016	Updated according to firmware version 1.13.0 Added: - 3.6.2.7 MAC Filter submenu Changed: -- 3.5.1 Internet - 3.5.3 IPTV - 3.6.1 WEB interface basic elements - 3.6.2.1 'Internet' submenu - 3.6.2.2 'MAC address configuration' submenu - 3.6.2.3 'DHCP server' submenu - 3.6.3.2 'Line configuration' submenu - 3.6.3.3 'Profiles' submenu - 3.6.6.1 'Time' submenu - 3.6.6.8 'Autoconfiguration' submenu - 3.7.2 'VoIP' submenu - 3.7.5 'ARP' submenu - 4.1 Call transfer
Version 1.3	20 November 2015	Updated according to firmware version 1.12.2
Version 1.2	18 March 2015	Updated according to firmware version 1.12 Added: - 3.6.3.7 'Call history' menu - 3.6.6.9 'VLAN management' submenu - 3.7.9 'Call history' submenu - Appendix B. Running user-defined script upon system startup Changed: - 3.5.1 Internet - 3.6.2.1 'Internet' submenu - 3.6.2.5 'NAT and port forwarding' submenu - 3.6.3.1 'Network configuration' submenu - 3.6.3.2 'Line configuration' submenu - 3.6.3.3 'Profiles' submenu - 3.6.3.5 'VAS management prefixes' submenu - 3.6.6.2 'Access' submenu - 3.6.6.5 'Configuration management' submenu - 3.6.6.8 'Autoconfiguration' submenu - 3.6.6.10 'Additional settings' submenu - 3.7.1 'Internet' submenu - 3.7.2 'VoIP' submenu - 6 Device automatic update algorithm based on DHCP
Version 1.1	10 November 2014	Updated according to firmware version 1.10.1 Added: - 3.6.2.10 'User VLAN' submenu - 3.6.3.6 'Call signal' submenu - 3.6.5.1 'Function' submenu Changed: - 3.5 Quick configuration menu - 3.6.3.1 'Network configuration' submenu - 3.6.2.1 'Internet' submenu - 3.6.3.3 'Profiles' submenu - 3.6.4.2 'STB' submenu - 3.6.6.1 'Time' submenu
Version 1.0	26 February 2014	First issue
Firmware version	Firmware version: 1.13.1 Web interface version: 1.13.80	

SYMBOLS

Symbol	Description
Bold font face	Notes, warnings, chapter headings, titles, table titles are written in bold.
Calibri Italic	Important information is written in Calibri Italic.

Notes and warnings

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

Warnings are used to inform the user about harmful situations for the device and the user alike, which could cause malfunction or data loss.

CONTENTS

1 INTRODUCTION

Today, VoIP is one of the most rapidly evolving communication services. *TAU-1M.IP* series gateways (hereinafter the "device") are designed to provide VoIP services to the network clients.

TAU-1M.IP VoIP gateway with an integrated router allows to connect an analog phone to packed-based data networks accessible via Ethernet.
The device is intended for operation in home or small office (SMB) environment.

This operation manual describes intended use, key specifications, configuration, monitoring, and firmware update for *TAU-1M.IP* VoIP gateways.

2 PRODUCT DESCRIPTION

2.1 Purpose

TAU-1M.IP is a high-performance VoIP gateway with the full set of features which allow users to leverage VoIP functionality.

TAU-1M.IP gateway allows to connect an analog phone or a fax modem to IP networks. With built-in router, the device enables connection of local network equipment to broadband access network. Device may be connected up to 2 PCs that will be able to access the Internet through integrated NAT/DHCP server features. USB port allows for the external storage device, 3G/4G USB modem or Wi-Fi-adapter connection[1].

2.2 Device Specifications

Interfaces:

- FXS: 1 x RJ-11 port
- LAN: 2 x Ethernet RJ-45 10/100BASE-T ports
- WAN: 1 x Ethernet RJ-45 10/100BASE-T port
- USB: 1 x USB 2.0 port

Gateway is powered by external 12 V DC adapter for 220 V 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 features support
- VoIP protocols: SIP
- Echo cancellation (G.168 recommendations)
- Voice activity detection (VAD)
- Comfort noise generator
- DTMF signals detection and generation
- DTMF transmission (INBAND, rfc2833, SIP INFO)
- Fax transmission:

---

[1]Wi-Fi adapters are not supported in the current firmware version.

– G.711A/G.711U
– T.38

- Operation w/ and w/o SIP server

- *Value Added Services:*

    – Call Hold
    – Call Transfer
    – Call Waiting
    – Call Forward at Busy
    – Call Forward at No answer
    – Call Forward Unconditional
    – DND
    – Caller ID: FSK, DTMF
    – Hotline
    – Group call
    – Call Pickup
    – Three-way conference call
    – Flexible numbering scheme

- Firmware update via web interface

- DHCP-based auto provisioning support

- TR-069
- Remote monitoring, configuration and setup: Web interface, Telnet.

Fig.1 shows *TAU-1M.IP* connection diagram.
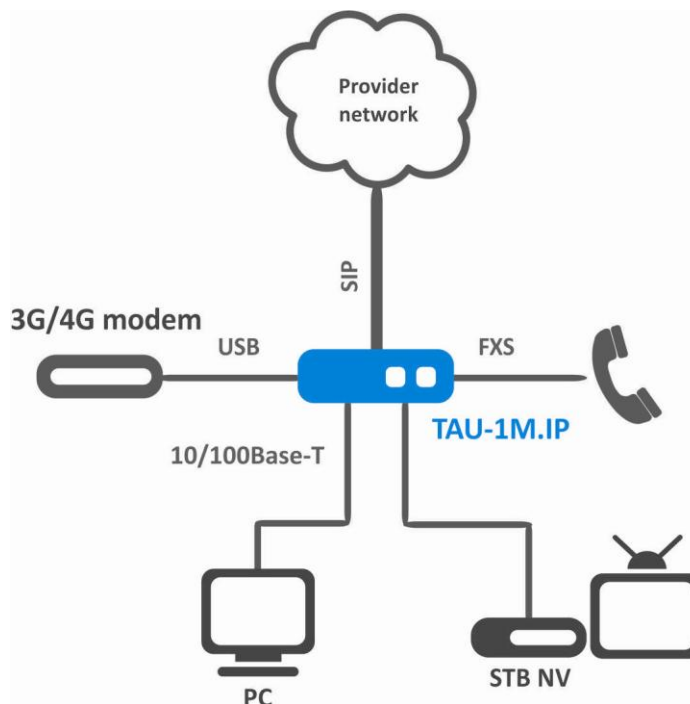
Fig.1—TAU-1M.IP operation diagram

2.3 Device Design and Operating Principle

TAU-1M.IP terminal include the following subsystems:

– Controller featuring:

  ▪ RealtekRTL8972C highly-integrated System-on-a-Chip (SoC), including a CPU, 100Mbit switch with a built-in PHY, hardware L2/L3/L4 traffic acceleration, USB 2.0 ports, PCI-E controllers, and 8 PCM channels for VoIP applications
  ▪ Flash memory: 8Mb
  ▪ SDRAM: 128MB

– SLIC subscriber unit
– RJ-45 10/100BASE-T Ethernet switch w/ 2 ports for LAN
– WAN Ethernet module: RJ-45 10/100BASE-T
– USB Host port

For device design diagram, see Fig. 2.
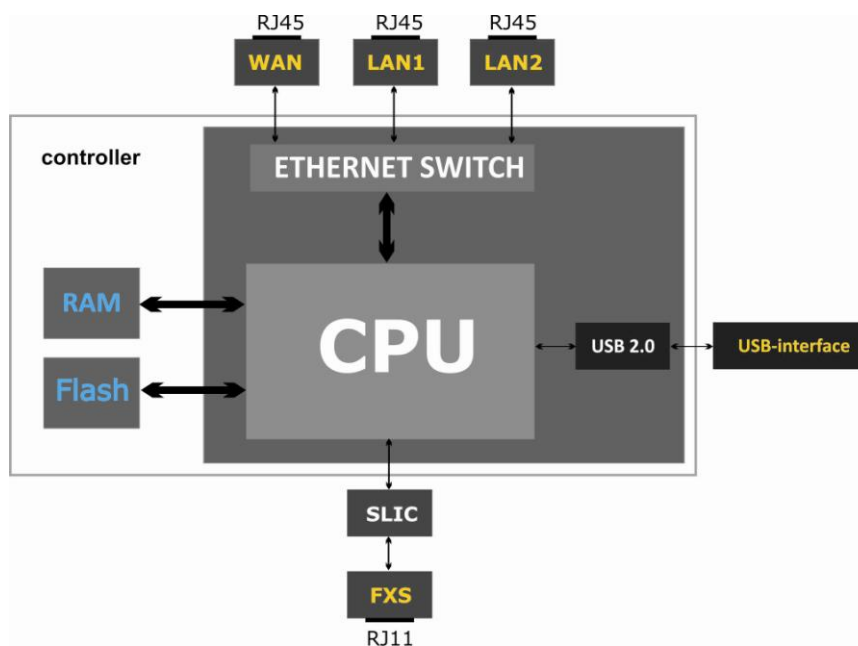
Fig.2—TAU-1M.IP design diagram

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

The device may functionally be divided into four block:

– 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 configuration, can process both tagged and untagged frames. 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 SLIC subscriber unit module to be digitized. 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 features' support.

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

Fig. 3 shows TAU-1M.IP functional diagram.
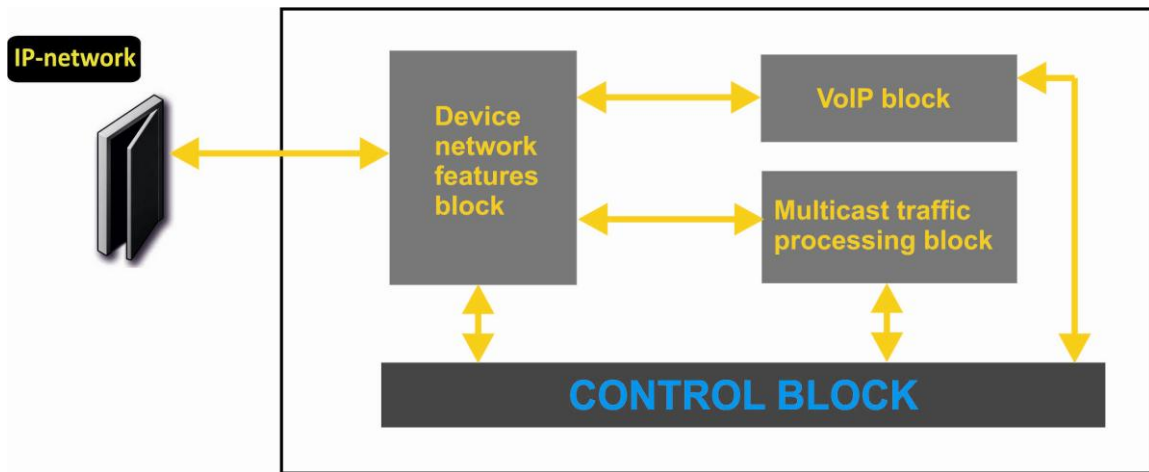
Fig.3—TAU-1M.IP series functional diagram

2.4 Main Specifications

Table 2 lists main specifications of the device.

Table 1—Main specifications

VoIP Protocols

Supported protocols	SIP

Audio codecs

Codecs	G.729, annex A, annex B G.711a, G.711u, G.723.1 Modem transmission: G.711a, G.711u Fax transmission: G.711a, G.711u, T.38

Ethernet WAN interface specifications

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

Ethernet LAN interface specifications

No. of interfaces	2
Electric port	RJ-45
Data rate, Mbps	10/100, autodetection
Supported standards	BASE-T

Analogue user ports example

Number of ports	1
Loop resistance (phone resistance excluded)	Up to 80Ω
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 12 V DC 1.5 A
Power consumption	6 W max (max. current consumption 0.5 A)
Operating temperature range	from +5 to 40°C
Relative humidity at 25°C	up to 80 %
Dimensions	122x96x33 mm
Weight	0.15 kg max

2.5 Design

TAU-1M.IP terminal is enclosed into 122x96x33 mm plastic housing.

2.5.1 Top panel of the device

Fig. 4 shows TAU-1M.IP top panel layout.
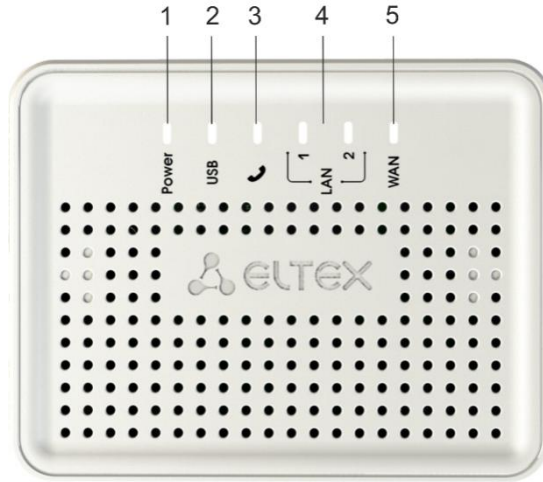
Fig.4—TAU-1M.IP top panel layout

TAU-1M.IP top panel is equipped with LED indicators, see Table 2.

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

Front panel elements		Description
1	Power	Device power and activity status indicator
2	USB	External USB device activity indicator (USB flash, external HDD, 3G/4G USB modem)
3	✆	Analog phone indicator
4	LAN	LAN interface port indicators
5	WAN	WAN interface indicator

2.5.2 Rear panel of the device

Fig.5 shows *TAU-1M.IP* rear panel layout.
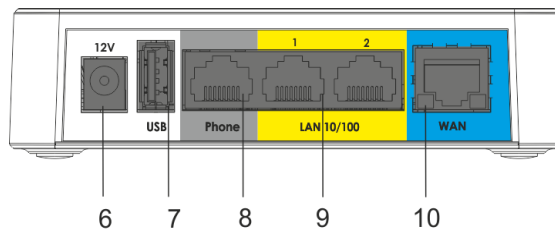
Fig.5—TAU-1M.IP rear panel layout

TAU-1M.IP rear panel is equipped with the following connectors and controls, see Table 3.

Table 3—Description of LEDs and controls located on *TAU-1M.IP* rear panel

Rear panel element		Description
6	12V	Connector for power adapter
7	USB	USB port for external USB device connection (USB flash, HDD, 3G/4G USB modem)
8	Phone	RJ-11 port for analog phone unit connection
9	LAN	2 x 10/100BASE-T Ethernet (RJ-45) ports for local network device connection
10	WAN	10/100BASE-T Ethernet (RJ-45) port for external network connection

2.6 Light Indication

WAN, LAN, Phone, Power indicators located on *TAU-1M.IP* top panel show the device current status. Table 5 lists possible states of the LEDs.

Table 4—Light indication of *TAU-1M.IP* series status

LED	LED State	Device State
WAN	Solid (green—10 Mbps, orange—100 Mbps)	Connection between station-side terminal and subscriber-side device is established
	Flashes	Transferring data packets via WAN interface
LAN	Solid (green—10 Mbps, orange—100 Mbps)	Connection to the network device is established
	Flashes	Transferring data packets via LAN interface
☎	Green, solid	Phone is off-hook (line is active)
	Off	Phone is on-hook, normal operation
	Green, flashes with 20 Hz frequency for 1 second, then 4 second pause	Incoming call is on the phone port
	Green, flashes slowly in periods	Subscriber port is not registered at SIP proxy server
	Green, double short flashes in 3 second intervals	Line test is in progress
USB	Green, solid	USB device is connected
	Off	USB device is disconnected
Power	Green, solid	Device power is on, normal operation
	Orange, solid	Internet is not accessible
	Red, solid	Device starts up
	Flashes red and green intermittently in periods	Device is being reset to factory defaults

2.7 Reset to Factory Defaults

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 in periods. 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.

2.8 Delivery Package

TAU-1M.IP series standard delivery package includes:

- Multi-purpose terminal;
- 220/12 V 1.5 A power adapter;
- Installation and configuration guide.

3 DEVICE MANAGEMENT VIA WEB CONFIGURATOR

3.1 Getting Started
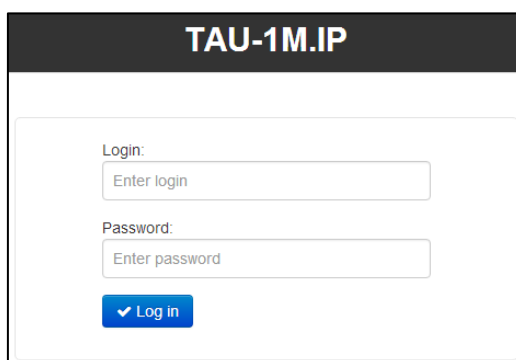
In order to start the operation, you should connect to the device via LAN interface using a web browser.

1. Open a web browser (hypertext document viewer) such as Firefox, Opera, or Chrome.
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'* field and password into *'Password'* field.
   Factory settings: login: *admin*, password: *password*.
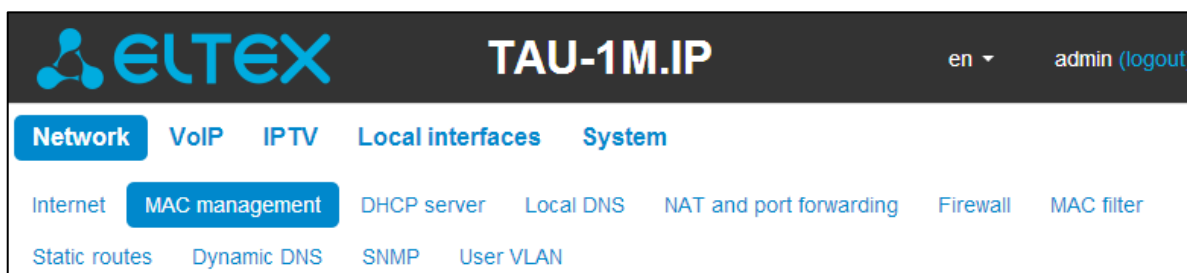
4. Click *'Log in'* button. Quick configuration menu will be shown in the browser window, see Fig. 6.

3.2 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 and configure Wi-Fi, 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 *'Logout'* button, the current user session will be terminated; login window will be displayed.
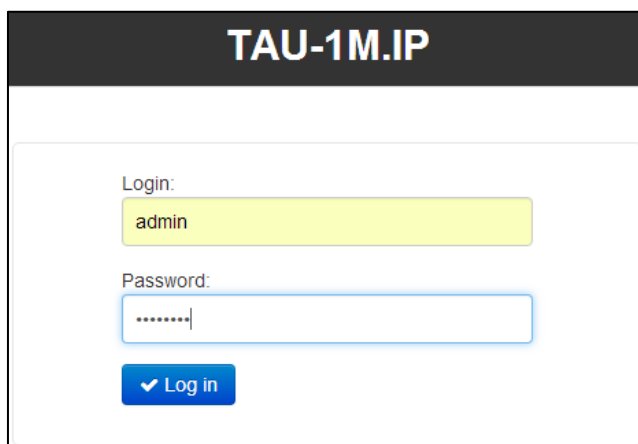
To change the access, you should specify the corresponding username and password and click *'Log in'* button.

3.3 WEB Interface Operation Modes

TAU-1M.IP web interface may operate in three modes:

- **Monitoring**—system monitoring mode—allows to view various device operation information: Internet connection activity, phone port status, amount of received/sent data via network interfaces, etc.
- **Tiles**—quick system configuration mode—each tile contains settings grouped by their function: Internet, VoIP, IPTV, and System. A tile only displays basic parameters that allow for 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 mouse cursor on it.
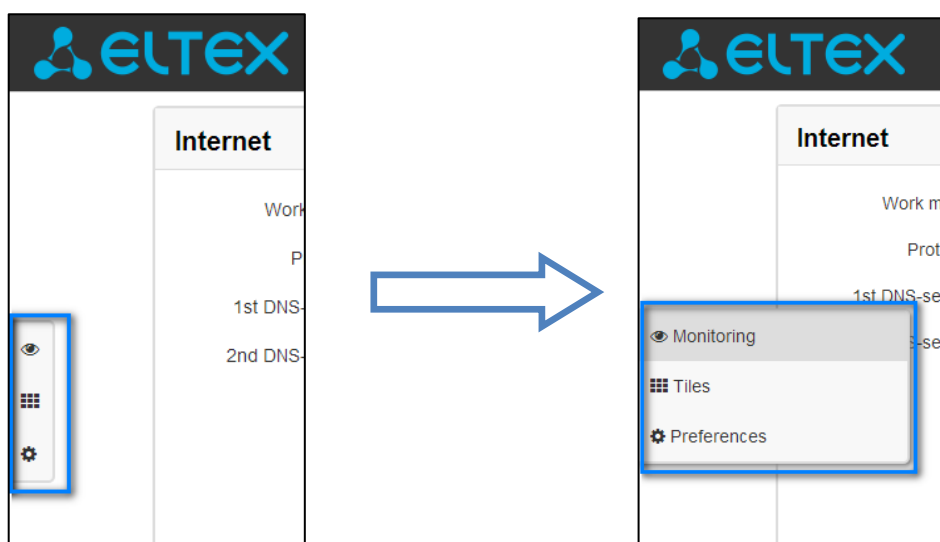
To proceed from 'Tiles' mode into 'Settings', you may also click 'Details' link in the tile.

3.4 Applying and Discarding Changes Made to Configuration

3.4.1 Applying configuration

Click 'Apply' button to save the configuration into the device flash memory and apply new settings. All settings will take effect without device restart.

'Apply' button in the quick configuration menu and the advanced settings menu will appear as follows: ; .

WEB interface features visual indication of the current status of the settings application process, see Table 5.

Table 5—Visual indication of the current status of the settings application process

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

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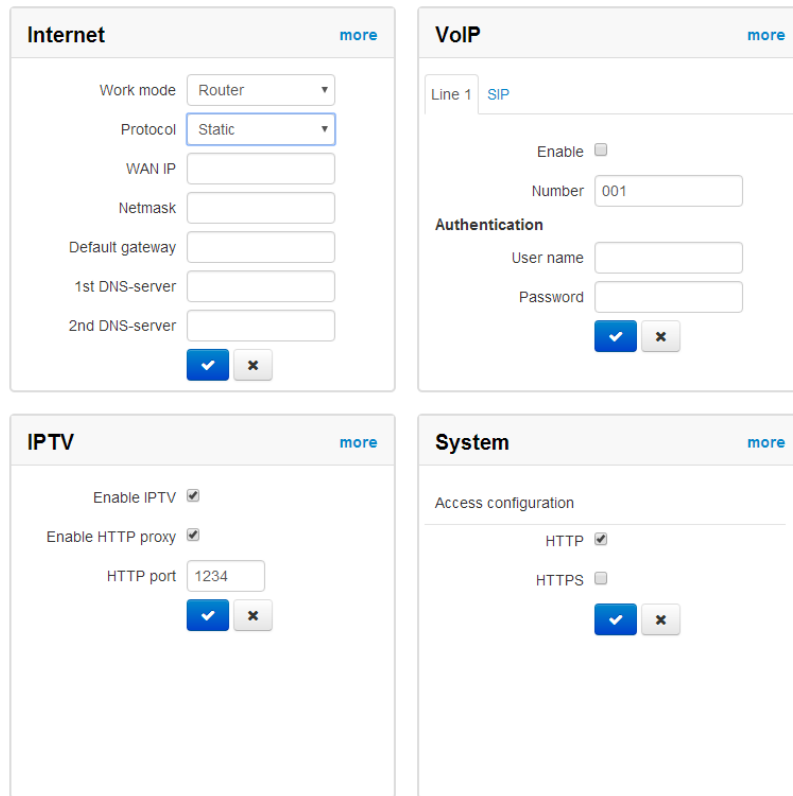
You may discard changes only until 'Apply' button is clicked. In this case, edited parameters on the page will be updated with the values currently stored in the device memory. After you click 'Apply', you will not be able to restore previous settings.

Discard changes button in the quick configuration menu and the advanced settings menu will appear as follows: ; .

3.5 Quick Configuration Menu

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

Fig.6—Quick configuration menu

Settings are divided into the following categories:

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

3.5.1 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 'Details' link.

- *Work mode*—device operation mode:
    - *Router*—router mode is established between LAN and WAN interfaces (LAN is isolated from WAN);
    - *Bridge*—bridge mode is established between LAN and WAN interfaces: data is transferred 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:

- *External IP address*—specify device WAN interface IP address in the provider network;
- *Subnet mask*—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 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 DHCP server. Supported options:

- 1—network mask
- 3—default network gateway address
- 6—DNS address
- 12—device network name
- 28—network broadcast address
- 33—static routes
- 42—NTP server address
- 43—specific vendor information
- 60—alternative Vendor ID
- 66—TFTP server address
- 67—firmware file name (to download via TFTP from the server specified in Option 66)
- 121—classless static routes

In Option 60 DHCP request, the device will send vendor information in the following format:

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

Example:
[VENDOR:Eltex][DEVICE:TAU-1M.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]
[LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0],

– *Primary DNS,Secondary DNS*—DNS IP addresses—if DNS addresses are not obtained automatically 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:

- *Username*—username for authorization on PPP server;
- *Password*—password for authorization on PPP server;
- *Service-Name*—'Service-Name' tag value in PADI message for PPPoE connection initialization (this parameter is optional, and configured only on the provider's request);
- *Secondary access*—type of access to local area network resources.
  You may select 2 options:
  DHCP—dynamic access when IP address and 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 special channel—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);
    - *Username*—username for authorization on PPTP server;
    - *Password*—password for authorization on PPTP server;
    - *Secondary access*—type of access to local area network resources and PPTP server.
    You may select 2 options:
    DHCP—dynamic access when IP address and 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;
      - *Subnet mask*—subnet mask for static access;
      - *DNS*—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 viaa 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);
    - *Username*—username for authorization on L2TP server;
    - *Password*—password for authorization on L2TP server;
    - *Secondary access*—type of access to local area network resources and L2TP server.
    You may select 2 options:
    DHCP—dynamic access when IP address and 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;
      - *Subnet mask*—subnet mask for static access;
      - *DNS*—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 to establish 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[1] 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 ☑ button. To discard changes, click ✖ button.

---

[1]IPSec is not supported in the current firmware version.

To connect the device to the provider network, you should request the network settings from the provider. If you use the 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.

3.5.2 VoIP

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

In the 'Line 1' and 'Line 2' tabs you may configure the device phone ports respectively:

– *Enable*—when selected, the current line is active;
– *Number*—subscriber number, assigned for this phone line;
– *Username*—username 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).

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

3.5.3 IPTV

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

– Enable IPTV—when selected, enable IPTV packet transmission from *TAU-1M.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 non-volatile memory, click ✔ button. To discard changes, click ✖ button.

3.5.4 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 'Details' link.

Access to Web via WAN:

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

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

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

3.6 Advanced Settings

To proceed to the advanced settings mode, click 'Details' link in any tile name or select 'Settings' item on the left panel.

3.6.1 WEB interface basic elements

Fig. 7 shows WEB configurator basic navigation elements in the advanced settings mode.
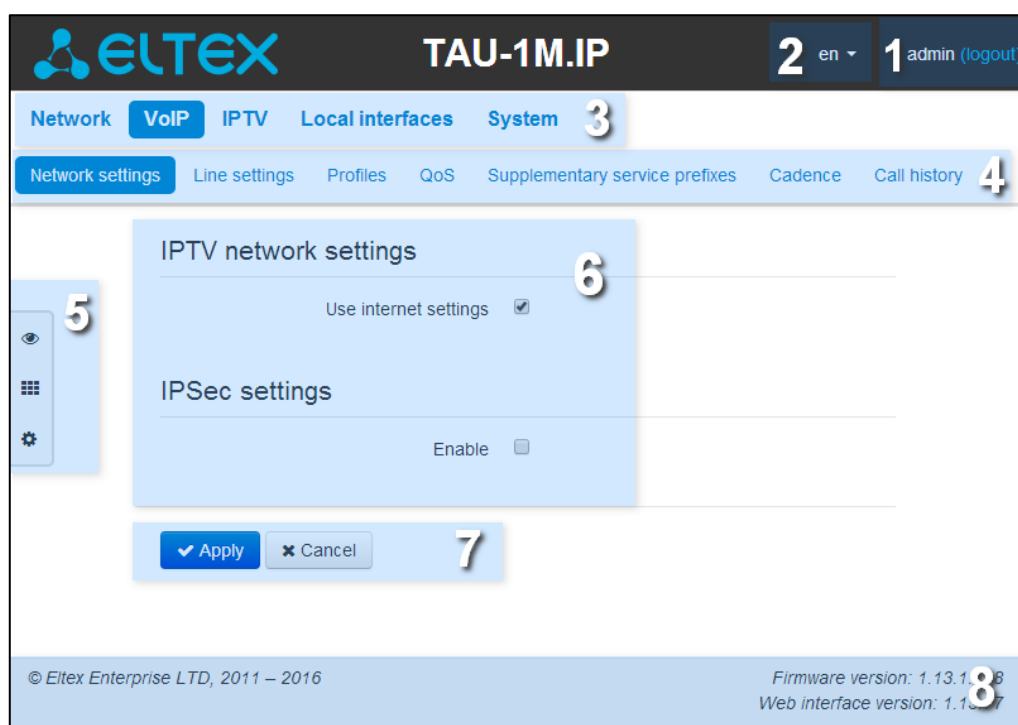
Fig.7—Web configurator navigation elements

User interface window is divided into 7 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 a category: **Network**, **VoIP**, **IPTV**, **Local Interfaces, System**.
4. Submenu tabs allow for settings field management.
5. WEB configurator mode changing panel (for description, see Section 3.3 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 3.4 Applying and Discarding Changes Made to Configuration .

    − *Apply*—apply and save the current configuration into non-volatile memory of the device;
    − *Discard*—discard changes (effective only until '*Apply*' button is clicked).

8. Informational field showing firmware version and WEB interface version.

3.6.2 'Network' menu

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

3.6.2.1 '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

    −   *Hostname*—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 only;
- *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.

— *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 Full*—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*—device operation mode:

- *Router*—router mode is established between LAN and WAN interfaces (LAN is isolated from WAN);
- *Bridge*—bridge mode is established between LAN and WAN interfaces: data is transferred transparently from LAN to WAN and back—in fact, the device operates in the router 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:
  - *Device external IP address*—specify device WAN interface IP address in the provider network;
  - *Subnet mask*—external subnet mask;
  - *Default gateway*—address that the packet will be sent to, when route for it is not found in the routing table;
  - *1st DNS, 2nd DNS* —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 DHCP server. Supported options:
    - 1—network mask
    - 3—default network gateway address
    - 6—DNS address
    - 12—device network name

- 28—network broadcast address
- 33—static routes
- 42—NTP server address
- 43—specific vendor information
- 60—alternative Vendor ID
- 66—TFTP server address
- 67—firmware file name (to download via TFTP from the server specified in Option 66)
- 121—classless static routes

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)* field value 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:device vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**software version**]**

  Example:
  [VENDOR:Eltex][DEVICE:TAU-1M.IP][HW:1.0][SN:VI23000118]
  [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

- *Primary DNS, Secondary DNS*—DNS IP addresses—if DNS addresses are not obtained automatically 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:
  - *Username*—username for authorization on PPP server;
  - *Password*—password for authorization;
  - *MTU*—maximum block size for data transmitted via the network (1492 is recommended);
  - *Service-Name*—Service-Name tag value in PADI message (this field is optional);
  - *Secondary access*—type of access to local area network resources;
    You may select 2 options:
    DHCP—dynamic access when IP address and 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);
  - *Hardware traffic 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 special channel—a tunnel—using PPTP. When *'PPTP'* is selected, the following parameters will be available for editing:
  - *PPTP server*—PPTP server IP address;
  - *Username*—username 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);
- Secondary access—type of access to local area network resources and PPTP server.
You may select 2 options:
DHCP—dynamic access when IP address and 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;
- Subnet mask—subnet mask for static access;
- DNS—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).

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

- L2TP—operation mode when the Internet access is established via a special channel—a tunnel—using L2TP. When 'L2TP' is selected, the following parameters will be available for editing:
    - L2TP server—L2TP server IP address;
    - Username—username 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);
    - Secondary access—type of access to local area network resources and L2TP server;
    You may select 2 options:
    DHCP—dynamic access when IP address and 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—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).

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

PPTP and L2TP allow to establish 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[1] allows for the higher security level compared to PPTP and guarantees the higher level of protection for business-critical data.

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

- *Use VLAN in external network*—when selected, use VLAN identifier specified in 'VLAN ID' field for the Internet access.

    - *VLAN ID*—VLAN identifier used for the service.
    - *802.1P*—802.1P marker (another name: *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—virtual local area network. VLAN consist of a group of hosts combined into a single network regardless of their location. Devices grouped into a single VLAN will have the same VLAN-ID.

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

When you choose 'Bridge' 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:

        - *IP address*—specify device WAN interface IP address in the provider network.
        - *Subnet mask*—external subnet mask;
        - *Default gateway*—address that 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 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)* field value 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:device vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**software version**]**

            Example:
            [VENDOR:Eltex][DEVICE:TAU-1M.IP][HW:1.0][SN:VI23000118]
            [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

---

[1]IPSec is not supported in the current firmware version.

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

When '3G/4G USB modem' connection method is selected, the following field will become available for configuration:

- *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;
- *Username*—username used for authentication in the wireless network;
- *Password*—password used for authentication in the wireless network;
- *Called number*—dial-up number for wireless network connection (e.g. *99***1#).
- *Additional parameters*—parameters for wireless 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).

'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.

Local area network:

- *Device IP address*—device IP address in LAN;
- *Netmask*—subnet mask in LAN.

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

IPSec configuration:

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 encryption algorithm	des ▾
Diffie Hellman group	1 ▾
IKE SA lifetime, s	86400

Phase 2

IKE authentication algorithm	hmac_md5 ▾
IKE encryption algorithm	des ▾
Diffie Hellman group	1 ▾
IPSec SA lifetime, s	3600

- *Enable*—enable IPSec protocol utilization 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 address* together with *Remote netmask* define a remote subnet address used for IPSec-encrypted communication. If the mask value is 255.255.255.255, communication is performed with a single host. Mask that differs from 255.255.255.255 allows you to define a whole subnet. Thus, device features allow you to establish 4 network topologies that utilize IPSec traffic encryption: Point-to-Point, Network-to-Point, Point-to-Network, Network-to-Network;
- *Remote gateway*—gateway used for remote network access;
- *NAT-T mode*—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 activated only when NAT is detected on the way to the destination host;
  - *Force*—use NAT-T in any case;
  - *Off*—disable NAT-T on connection establishment.

    The following NAT-T settings are available:
  - *NAT-T UDP port*—UDP port for packets for IPSec message encapsulation. Default value is 4500;
  - *NAT-T keepalive packet transmission interval, seconds*—periodic message transmission interval for UDP connection keepalive on the device performing NAT functions.
- *Aggressive mode*—phase 1 operation mode when all the necessary information is exchanged using three unencrypted packets. In the main mode, the exchange process involves six unencrypted packets;
- *Identifier type*—device identifier type: address, fqdn, keyed, user_fqdn, asn1dn;
- *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. Also, they 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* —selectan 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;
- *Phase 1 lifetime, seconds*—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;
- *Phase 2 lifetime, seconds ('IPSec SA lifetime')*—time that should pass for data encryption key changeover (other name 'IPSec SA lifetime'). Default value is 60 minutes (3600 seconds).
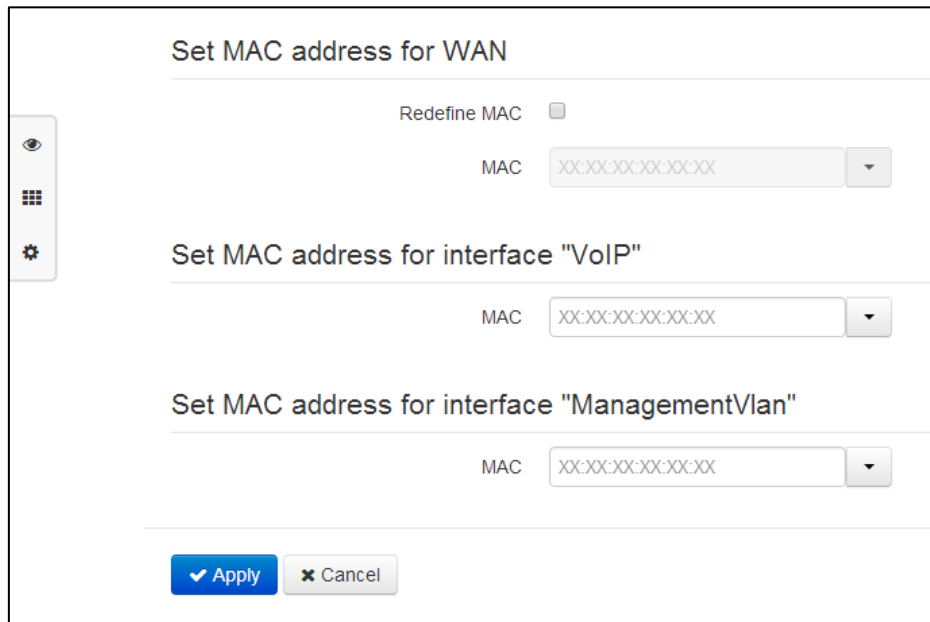
To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

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

3.6.2.2 'MAC address configuration' submenu

In the 'MAC address configuration' 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. This may be helpful, when your ISP network employs MAC address tethering. In this case, if you are planning to use *TAU-1M.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 'VLAN management' interface, see sections 'MAC address configuration for *'VoIP'* interface' or 'MAC address configuration for *'VLAN management'* interface'.

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

3.6.2.3 '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-1M.IP* may automatically assign IP addresses and parameters required for the Internet access to computers connected to the LAN interface and wireless Wi-Fi access point. 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.

Settings of DHCP server

- – *Enabled*—when selected, enable local DHCP server;
- – *Start IP address*—starting 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 *'Apply'* button. To discard changes, click *'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.**

Creating of static lease

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

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

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

3.6.2.4 'Local DNS' submenu

In '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 hostnames (domains) and their IP addresses.
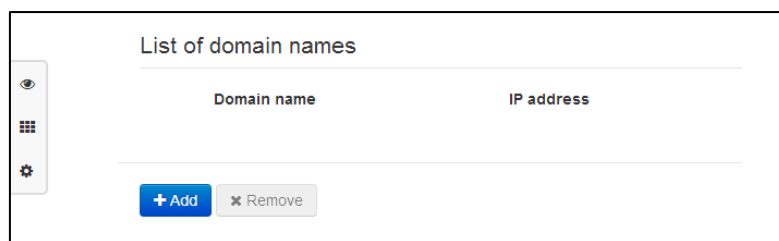
Configuration of hosts

To add the address into the list, click *'Add'* button in the 'Create match' window and fill in the following fields:
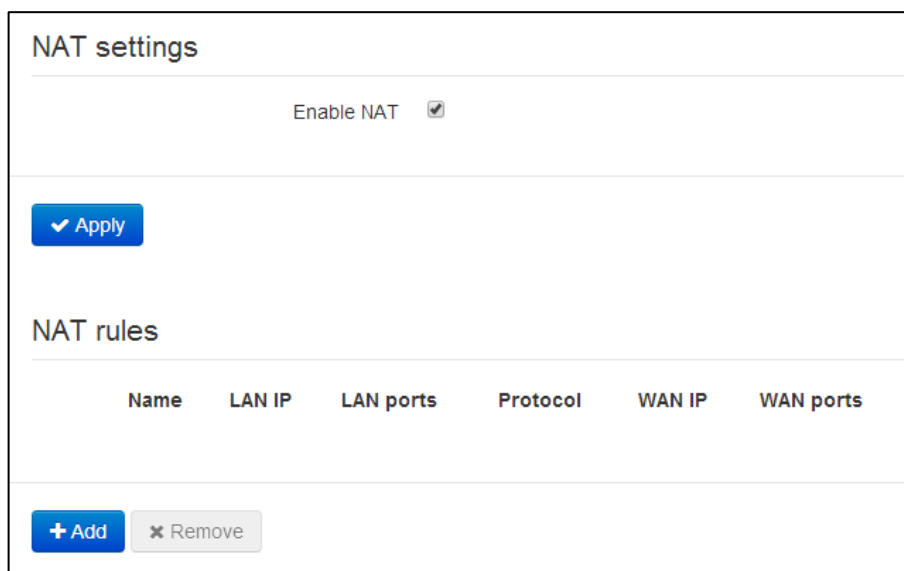
- *Domain name*—host name.
- *IP address*—host IP address.

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

3.6.2.5 '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 for IP packet address and network port translation. Port forwarding is required when TCP/UDP connection to a local computer (connected to LAN interface) is established from the external network. In this settings menu, you may define the rules allowing packets to pass from the external network to the specified address in the local network and thus enabling connection. In general, port forwarding is necessary for torrent and P2P service operation. For this purpose, you should identify TCP/UDP ports used by a torrent or p2p client in their settings and assign the respective forwarding rules for your computer IP address.

NAT settings

Enable NAT ☑

✔ Apply

NAT rules

Name	LAN IP	LAN ports	Protocol	WAN IP	WAN ports

+ Add   ✖ Remove

Configuration of NAT rules

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

Add a new rule

Name	
LAN IP address	
Destination ports of LAN	
Protocol	TCP ▼
WAN IP address	
Destination ports of WAN	

✔ Apply   ✖ Cancel

–   *Name*—name of the rule (this field is mandatory);
–   *LAN packet destination IP address (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 in the external network that cause the packet to fall under this rule (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 analysed), its destination address and port are substituted with values from *'LAN IP address'* and *'LAN ports'* fields.

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

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

3.6.2.6 '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 (incoming, outgoing, transit) 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).
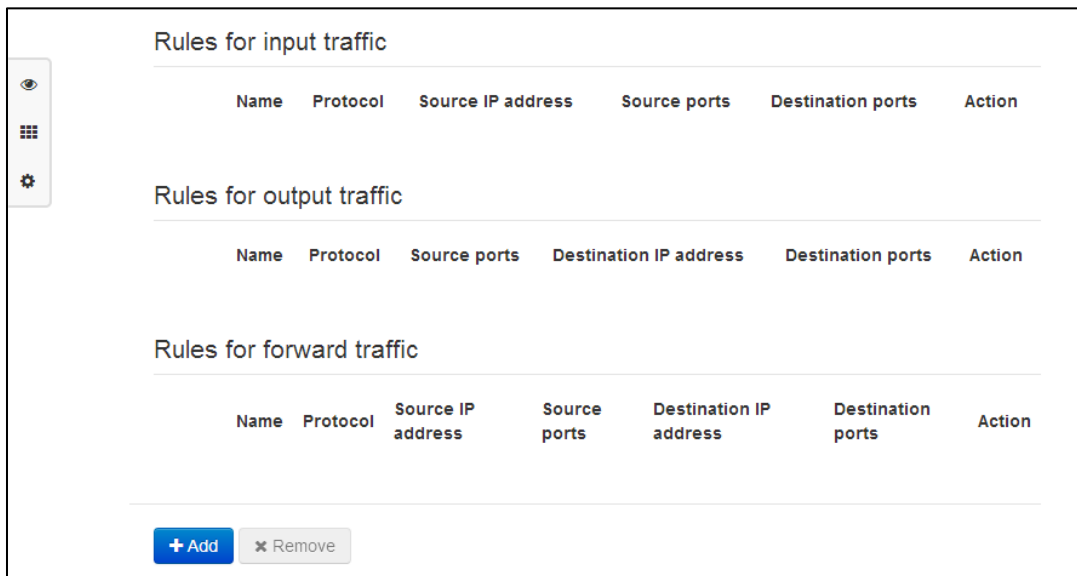
Configuration of firewall rules

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

Add a new rule

Name	
Traffic type	Input ▼
Protocol	TCP ▼
Source IP address	
Source ports	0
Destination ports	0
Action	Accept ▼

✔ 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).

    - ▪ *Outgoing*—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.

    - ▪ *Transit*—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 (a single port or port range delimited by '-' is permitted);
- – *Destination ports*—list of destination ports (a single port or port range delimited by '-' is permitted).

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

- – *Message type*—you may create a rule for the specific ICMP message type only or for all ICMP message types.

Click 'Apply' button to add a new rule. To discard changes, click *'Cancel'* button. To remove the record from the list, select the checkbox next to the respective record and click 'Delete'.
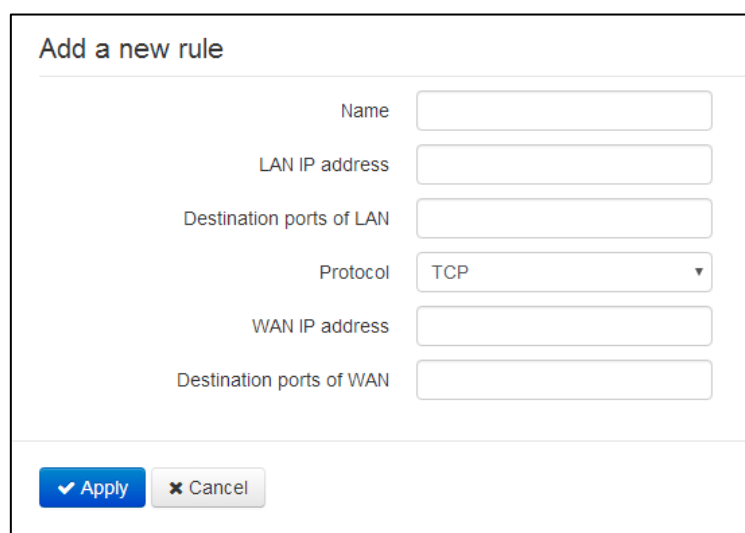
3.6.2.7 MAC filter submenu

In the 'MAC filter' submenu, you may configure access filtering by client's MAC address.
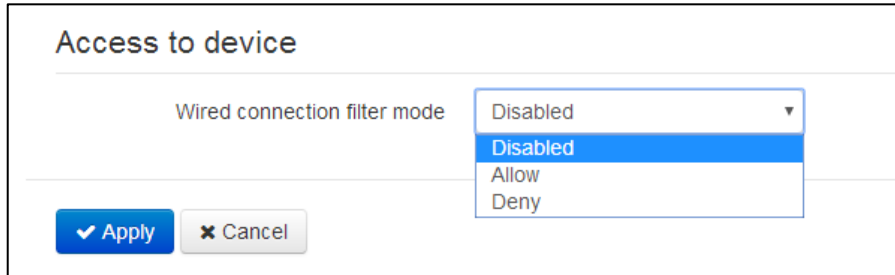
– *Filter mode*—define one of the three filter operation modes depending on the client's MAC address:

- *Disable*—MAC address filtering is disabled, all clients are allowed to connect to the access point;
- *Deny*—in this filter operation mode, clients with MAC addresses from the 'MAC address list' are denied to connect to the access point. Subscribers with unlisted MAC addresses are allowed to connect to the AP;
- *Allow*—in this filter operation mode, clients with MAC addresses from the 'MAC address list' are allowed to connect to the access point. Subscribers with unlisted MAC addresses are denied to connect to the AP.

MAC Address List

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

To add a new client to the list, click *'Add'* button and enter its MAC address, or click drop-down menu button and select the MAC of the device connected to the wired or Wi-Fi network.

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

3.6.2.8 'Routing' submenu

In the 'Routing' submenu, you may configure device static routes.
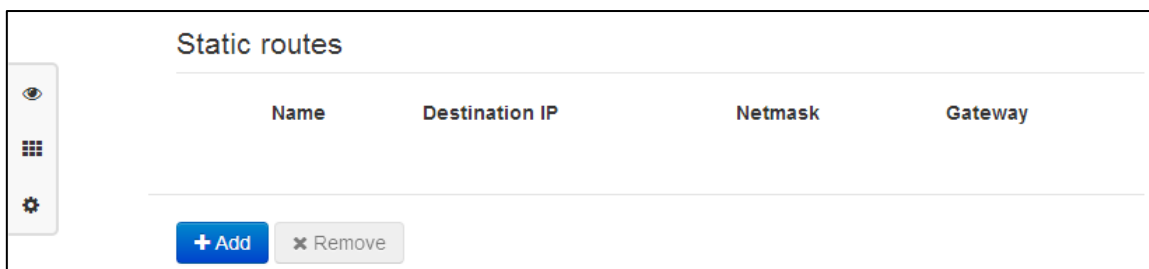
To add a new route, click *'Add'* button and fill in the following fields:

- — *Name*—route name, used for human perception convenience. You may leave this field empty;
- — *Destination address*—IP address of destination host or subnet that the route should be established to;
- — *Netmask* – 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 address'*.

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

3.6.2.9 'Dynamic DNS' submenu

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

Dynamic DNS (D-DNS) allows DNS server information to be updated in real time and (optionally) in automatic mode. It's used for assigning a fixed domain name to a device (to a computer or router) with a dynamic IP address.
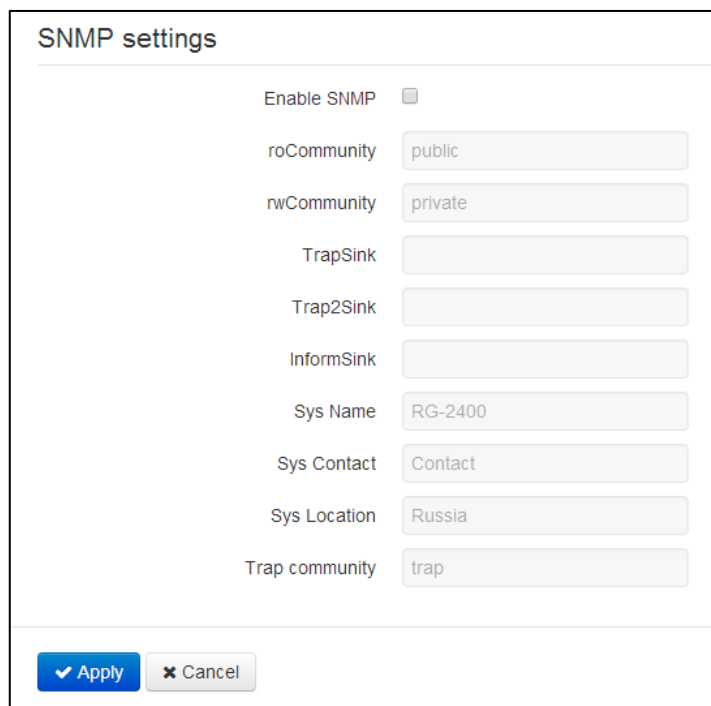
Dynamic DNS is frequently used in local networks, where clients are obtaining IP addresses through DHCP and then registering their names on local DNS-server.

– *Enable D-DNS*—when selected, D-DNS service is enabled; the following settings will become available for editing:
– *D-DNS provider*—D-DNS provider name, select a provider from the list of available providers;
– *Username*—user name used to access D-DNS service account;
– *Password*—password used to access D-DNS service account;
– *Domain name (0..9)*—you may register up to 10 device domain names (in general, only one name is required). 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 *'Apply'* button. To discard changes, click *'Cancel'* button.

3.6.2.10 'SNMP' submenu.

TAU-1M.IP software allows to monitor status of the device and configure it via SNMP protocol. In SNMP submenu, you can configure settings of SNMP agent. Device supports SNMPv1, SNMPv2c protocol versions.

SNMP settings

Enable SNMP	☐
roCommunity	public
rwCommunity	private
TrapSink	
Trap2Sink	
InformSink	
Sys Name	RG-2400
Sys Contact	Contact
Sys Location	Russia
Trap community	trap

✔ Apply   ✖ Cancel

– *Enable SNMP*—when selected, SNMP will be enabled for utilization;
– *Read password (roCommunity)*—password for parameter reading (common: '*public*');
– *Write password (rwCommunity)*—password for parameter writing (common: '*private*');
– *TrapSink (Trap v1 reception address)*—IP address or domain name of SNMPv1-trap message recipient in HOST [COMMUNITY [PORT]] format;
– *Trap2Sink (Trap v2 reception address)*—IP address or domain name of SNMPv2-trap message recipient in HOST [COMMUNITY [PORT]] format;
– *InformSink (inform message reception address)*—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 an 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.1.5—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 *'Apply'* button. To discard changes, click *'Cancel'* button.

3.6.2.11 'User VLAN' submenu

User VLAN is described by VLAN identifier which network traffic is transferred transparently from the device WAN interface to LAN with the consequent tag removal in LAN. I.e. when the user VLAN is enabled, the device initializes a network bridge between WAN port and specific LAN ports; at that, on the WAN side the traffic is sent/received with the specified VLAN identifier which is removed on the LAN side.

– *Status*—shows the current VLAN status (enabled/disabled);
– *Service name*—user VLAN name;
– *VLAN ID*—VLAN identifier;
– *Interfaces*—list of LAN ports mapped to the current user VLAN.

The device allows you to configure up to 4 uses VLANs. To open VLAN settings for editing, click one of the links *VLAN0…VLAN3*:

- *Enable*—when selected, user VLAN is enabled. If you try to disable a user VLAN with one or multiple LAN ports mapped to it, these LAN ports will be mapped to the Internet service;
- *Service name*—arbitrary name, associated with the current user VLAN;
- *VLAN ID*—VLAN identification number, may take values from 1 to 4095; should not match VLAN identifiers for other services;
- *Interfaces*—list of interfaces mapped to the current user VLAN. Non-editable field. To map the device LAN ports to user VLAN, go to the 'Local interfaces' tile.

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

3.6.3 'VoIP' Menu

In the 'VoIP' menu, you may configure VoIP (Voice over IP): SIP protocol configuration, FXS interface configuration, installation of codecs, numbering schedule, fax and modem data transfer mode.

3.6.3.1 'Network configuration' submenu

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

- *Use Internet settings*—when selected, use network settings specified in the *'Network' -> 'Internet'* menu, otherwise use settings specified in this menu;
- *Use VLAN*[1]—when selected, VoIP service will use a dedicated interface in a separate VLAN for its operation, with VLAN number specified in *'VLAN ID'* field.
  - *802.1P*—802.1P marker (another name: *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:

---

[1] In the firmware version 1.9.1, you may specify custom settings for VoIP service only in the dedicated VLAN.

- ▪ *Static*—operation mode where IP address and all the necessary settings 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 Option 60.
  - ⁻ *Alternative Vendor ID (Option 60)*—when selected, the device transmits *Vendor ID (Option 60)* field value 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:device vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**software version**]**

  Example:

  [VENDOR:Eltex][DEVICE:TAU-1M.IP][HW:1.0][SN:VI23000118]
  [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

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.

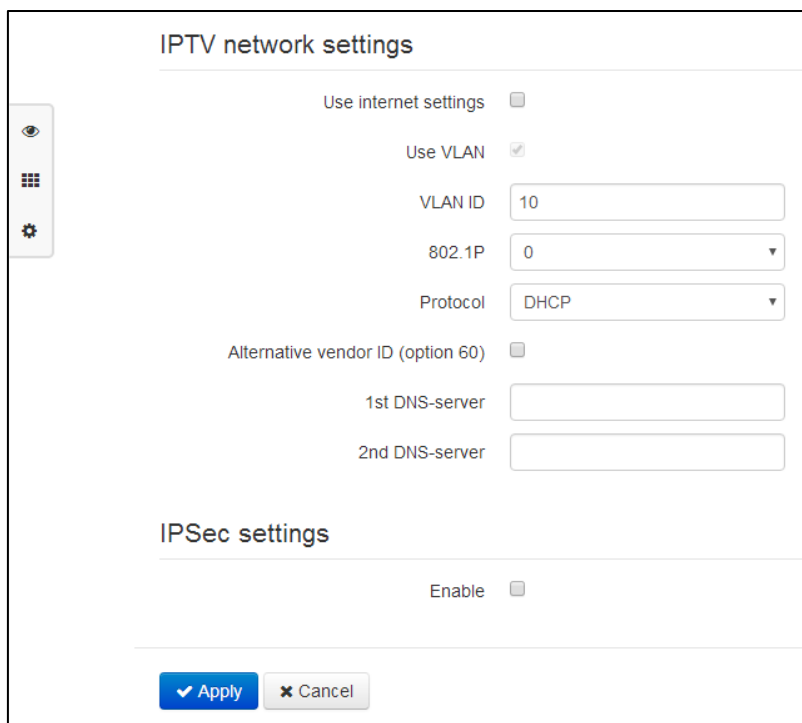For detailed *IPSec* settings, see Section .

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

3.6.3.2 'Line configuration' submenu

In the *'Line configuration'* submenu, you may configure the phone port.

To edit settings, press and hold the left mouse button on the link with the line number (1) to configure and fill in the following fields in the 'Edit line' window:

Account settings

- _Enable_—when selected, the port is active;
- _Profile_—select SIP profile from the list of available profiles. To configure profiles, use _'VoIP' -> 'Profiles'_ menu;
- _Phone_—subscriber number, assigned to this phone port;
- _Username_—username 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);
- _SIP port_—UDP port for incoming SIP message reception for this account, and for outgoing SIP message transmission from this account. It may take values from 1 to 65535 (default value: 5060);
- _Calling party category_—Subscriber category—enables transmission of outgoing messages in the 'From' header; the latter is transmitted in Tel-URI format (see RFC3966);
- _Authentication login and password_—username and password used for subscriber authentication on SIP server (and on registration server).

Supplementary service

- _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 dialling will be processed locally by the device (call transfer will be performed when the connection with the third party is established). For the 'Attended calltransfer' detailed operation algorithm, see Section _4.1'Call Transfer'_;
  - _Unattended calltransfer_— flash dialling will be processed locally by the device (call transfer will be performed when the subscriber finishes dialling a third party number). For the 'Unattended calltransfer' detailed operation algorithm, see Section _4.1'Call Transfer'_;

- *Call transfer mode*—this setting is available for the 'Attended calltransfer' mode only and governs call transfer service activation mode:

  - Mixed—call transfer is activated on clearback and pressing R 4;
  - Flash+4—call transfer is activated on pressing R 4;
  - On clearback—call transfer is activated on clearback.

- *Direct number*—when the phone goes offhook, dial the defined number immediately;
- *Call waiting*—when selected, 'Call waiting' service will be enabled (this service is available in 'flash—call transfer' function operation mode);
- *Call waiting ID*—Deliver calling party phone number during call waiting—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 to establish an outgoing connection automatically without dialling the number after the phone handset is picked up with the defined delay (in seconds). When checked, fill in the following fields:

  - *Hotline/warmline number*—phone number that will be used for connection establishment upon 'Delay timeout' expiration after the phone handset is picked up (in SIP profile being used, a prefix for this direction should be defined in the numbering schedule);
  - *Delay timeout, seconds*—time interval that will be used for connection establishment with the opposite subscriber, in seconds.

- *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:

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

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

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

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

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

- *Disabled*—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 (Configuration of physical parameters)

– Deliver calling party phone number—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.

– *Hangup timeout, seconds*—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, seconds*—'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, seconds*—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 onhook time, ms*—minimal clearback detection time, in milliseconds. At that, this parameter represents the maximum flash detection time;
– *Min flash* time—minimal flash detection time, (80–1000) ms;
– *Gain receive, 0.1 dB*—received signal gain (transmitted into the phone handset), measurement unit—0.1 dB;
– *Gain transmit, 0.1 dB*—transmitted signal gain (received by the phone handset microphone), measurement unit—0.1 dB;
– *Min pulse, ms*—configuration is required for pulse dialling mode, (10-150) ms;
– *Interdigit, ms*—configuration is required for pulse dialling mode, (150-20000) ms;
– *Polarity reversal*—when this option is enabled, line voltage polarity reversal occurs right after the callee responses to the outgoing call. After the clearback, the voltage polarity returns to its original state. This option is essential for payphone operation (polarity reversal indicates the start of the paid time interval).

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

3.6.3.3 'Profiles' submenu

In the 'Profiles' submenu, you may configure device SIP profiles. For each SIP profile, you may assign custom SIP and registration server addresses, voice and fax/modem codecs, custom numbering schedule and other parameters. Different SIP profiles are needed when different subscriber ports operate via different communication directions (different SIP servers). At that, for each subscriber port, you may assign only one SIP profile (*'VoIP' -> 'Line configuration'* menu setting).

To edit profile settings, left-click the link of the profile to be configured. In the 'Edit profile:' window, fill in the following fields:

Edit profile: SIP parameters

Profile includes	Line 1
Profile name	1st profile
Proxy mode	Homing ▾
Proxy server	
Registration	☐
Registration server	
Home server check method	Invite ▾
Home server keepalive timeout, s	30

Reserved proxy

[**+ Add**] [✖ Remove]

SIP domain	
Use domain to register	☐
Outbound mode	Off ▾
Expires	1800
Registration Retry Interval	30
Public IP address	
Use SIP Display Name in register	☐
Ringback at 183 Progress	☐
User call	180 Ringing ▾
100rel	Supported ▾
Timer enable	☑
Min SE, s	120
Session expires, s	1800
Keepalive NAT sessions mode	Off ▾
Use Alert-Info header	☐
Check RURI user part only	☐
Send IP address in Call-ID header	☐

Three-party conference

Mode   Local

Conference server   conf

IMS settings

IMS mode   Off

XCAP name for call hold   call-hold

XCAP name for call waiting   call-waiting

XCAP name for three-party conference   three-party-conference

XCAP name for hotline   hot-line-service

XCAP name for call transfer   explicit-call-transfer

Dialplan

Dialplan configuration   S5, L5 ([xABCD*#].S)

Voice codecs configuration

Codec 1   G.711a

Codec 2   G.711u

Codec 3   G.729

Codec 4   G.723

G.711 packet time, ms   20

G.729 packet time, ms   20

G.723 packet time, ms   30

Dispersion time, ms   32

Jitter Buffer

Min delay, ms   40

Max delay, ms   130

Deletion Threshold (DT)   500

Jitter factor   7

SIP parameters

- – *Profile contents*—list of subscriber ports that the profile is assigned to; this field cannot be changed;
- – *Profile name*—custom name of the configured profile;
- – *SIP proxy operation mode* – select SIP server operation mode form the drop-down list:

  - ▪ Disable;
  - ▪ Parking—SIP-proxy redundancy mode without main SIP-proxy management;
  - ▪ Homing—SIP-proxy redundancy mode with main SIP-proxy management.

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

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

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

2   In the 'homing' mode, three types of the main SIP-proxy management are available: periodic transmission of OPTIONS messages to its address, periodic transmission of REGISTER messages to its address, or transmission of INVITE request when performing outgoing call. First of all, INVITE request is sent to the main SIP-proxy, and if it is unavailable, then to the next redundant one, etc. Regardless of the management type, when the main SIP-proxy operation is restored, gateway will use it to renew its registration. The gateway will 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, register ports that utilize this profile on 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 UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name. As a rule, registration server is physically co-located with SIP proxy server (they have the same address);
- *Primary server control method*—select availability control method for the primary SIP server in 'Homing' mode:

  - *Invite*—transmission of INVITE request to its address when performing an outgoing call;
  - *Register*—periodic transmission of REGISTER messages to its address;
  - *Options*—periodic transmission of OPTIONS messages to its address.

- Primary server control period—periodic message transmission interval in seconds; used for primary SIP server availability check.

Redundant SIP proxies

To add a redundant SIP proxy, click 'Add' button and enter the following settings:

- *SIP proxy server*—network address of redundant SIP server. 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*—network address of redundant registration server (specify UDP port after the colon, default value is 5060). You may specify IP address as well as the domain name. If the *'Registration server'* checkbox is selected, the redundant server registration is enabled.

To remove the redundant SIP proxy, select the checkbox next to the specified address and click 'Delete' button.

- *SIP domain*—domain where the device is located (fill in, if required);
- *Apply SIP Domain for registration*—when selected, apply SIP Domain for registration (SIP domain will be inserted into the 'Request-Line' of 'Register' requests);
- *Outbound mode*—'Outbound' mode:
  - *Disabled*—calls will be routed according to the numbering schedule;
  - *Outbound*—numbering schedule is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, PBX response will be sent to the subscriber in order to enable subscriber service management (VAS management);

- Outbound with 'Busy' tone—numbering schedule is required for outgoing communications; however, all calls will be routed via SIP server; if there is no registration, VoIP will be unavailable: error tone will be transmitted to the phone headset.

- *Registration renewal time period*—time for subscriber port registration on SIP server. At the average, port registration renewal will be performed after 2/3 of the specified period;
- *Registration retry interval*—when the registration is unsuccessful, time period between SIP server registration attempts;
- *Public address*—this parameter is used as an external address of the device when it operates behind the NAT (gateway). As a public address, you may specify an external address (WAN) of a gateway (NAT) that *TAU-1M.IP* operates through. At that, on the gateway (NAT), you should forward the corresponding SIP and RTP ports used by the device;
- *Use SIP Display Name during registration*—when selected, use username in 'SIP Display Info' field of the 'Register' message;
- *Ringback on 183 Progress*—when selected, 'ringback' tone will be sent upon receiving '183 Progress' message (w/o enclosed SDP).

- *Calling subscriber*—provisional response sent by the device to the caller equipment during the incoming call:

  - *180 Ringing*—caller equipment will receive response 180; upon receiving this message, caller equipment should send a local ringback tone into the line;
  - *183 Progress with SDP*—caller equipment will receive response 183+SDP—used for voice frequency path forwarding before the answer of the callee. In this case, *TAU-1M.IP* will send a ringback tone remotely to the caller.
- *100rel*—use reliable provisional responses (RFC3262):
  - *supported*—reliable provisional responses are supported;
  - *required*—reliable provisional responses are mandatory;
  - *off*—reliable provisional responses are disabled.

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

Setting operation for outgoing communications:

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

Setting operation for incoming communications:

- *Supported, required*—when the following tag is received in 'INVITE' request—supported: 100rel, or required: 100rel—perform reliable transfer of provisional replies. If there is no supported: 100rel tag in INVITE request, the gateway will perform unreliable transfer of provisional replies;
- *Disabled*—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 selected, the 'timer' (RFC 4028) extension support is enabled. When connection is established, and both sides support 'timer' extension, one of them periodically sends re-INVITE requests for connection monitoring purposes (if both sides support UPDATE method, wherefore it should be specified in the 'Allow' header, the session update is performed by periodic transmission of UPDATE messages);
- *Minimal session time, sec*—minimal time interval for connection health checks (90 to 1800s, 120s by default);
- *Session time, seconds*—period of time in seconds that should pass before the forced session termination if the session is not renewed in time (90 to 80000s, recommended value—1800s, 0—unlimited session);
- *Periodic SIP server polling*—select SIP server polling method:
  - *Disabled*—SIP server will not be polled;
  - *Options*—SIP server polling with OPTIONS messages;
  - *Notify*—SIP server polling with NOTIFY messages;
  - *CLRF*—SIP server polling with an empty UDP packet.
- *Polling interval*—SIP server polling time period, in seconds;
- *Process Alert-Info header*—process INVITE request 'Alert-Info' header to send a non-standard ringing to the subscriber port;
- *Check username only in RURI*—when selected, only subscriber number (user) will be analysed, and if the number matches, the call will be assigned to the subscriber port. When unselected, all URI elements (user, host and port—subscriber number, IP address and UDP/TCP port) will be analysed 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 selected, during outgoing communications, device custom IP address will be used in 'Call-ID' header in 'localid@host' format.

Three-way conference call

- *Mode*—three-way conference call operation mode. Two modes are possible:

  - *Local*—conference assembly is performed locally by the device after pressing 'flash+3';
  - *Remote (RFC4579)*—conference assembly is performed at the remote server; after pressing 'flash+3', 'Invite' message will be sent to the server using number specified in the *'Conference server'* field. In this case, conference operation complies with the algorithm described in RFC4579. For detailed algorithm description, see Paragraph 4.3.2.

- *Conference server*—in general, address of the server that establishes conference using algorithm described in RFC4579. Address is specified in the following format SIP-URI: user@address:port. You may specify the 'user' URI part only—in this case, 'Invite' message will be sent to the SIP proxy address;

IMS configuration

– _Enable VAS management using IMS_—you may manage some service types using IMS (IP Multimedia Subsystem) server. In this case, 'Three-way conference call' (complies with RFC4579 algorithm), 'Call hold', 'Call waiting', 'Hotline' services (regardless of whether they were enabled in the configuration or not) will be enabled remotely by IMS server that sends 'Notify' messages containing enable/disable commands in XCAP format (in fact, XML, RFC4825).

  ▪ _Disabled_—IMS will not be used;
  ▪ _Without subscription_—you may manage some service types using IMS (IP Multimedia Subsystem) server. In this case, 'Three-way conference call' (complies with RFC4579 algorithm), 'Call hold', 'Call waiting', 'Hotline' services (regardless of whether they were enabled in the configuration or not) will be enabled remotely by IMS server that sends 'Notify' messages containing enable/disable commands in XCAP format (in fact, XML, RFC4825). In this case, when the gateway finishes subscriber registration, SUBSCRIBE requests will not be sent, only NOTIFY requests received from IMS and used for service management will be processed;
  ▪ _With subscription_—you may manage some service types using IMS (IP Multimedia Subsystem) server. In this case, 'Three-way conference call' (complies with RFC4579 algorithm), 'Call hold', 'Call waiting', 'Hotline' services (regardless of whether they were enabled in the configuration or not) will be enabled remotely by IMS server that sends 'Notify' messages containing enable/disable commands in XCAP format (in fact, XML, RFC4825). In this case, when the gateway finishes subscriber registration, it sends SUBSCRIBE requests, and if the subscription is successfully completed, it will process NOTIFY requests received from IMS and used for service management.

– _'Call hold' service name_—name of the XML element located in the 'Notify' message body that is used for transmission of 'Call hold' enabling/disabling commands. For example, if the service name value is 'call-hold', enabling command will be as follows:

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

  Disabling command:

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

– _'Call waiting' service name_—name of the XML element located in the 'Notify' message body that is used for transmission of 'Call waiting' enabling/disabling commands. For example, if the service name value is 'call-waiting', enabling command will be as follows:

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

  Disabling command:

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

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

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

  Disabling command:

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

– _'Hotline' service name_—name of the XML element located in the 'Notify' message body that is used for transmission of 'Hotline' enabling command. In the enabling command, you should pass the hotline number and the call timeout. For example, if the service name value is 'hot-line-service' and you should call the number 30001 in 6 seconds after the phone handset is picked up, the enabling command will be as follows:

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

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

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

By default, if the enabling command is not received, all the services mentioned above are disabled.

Numbering plan

To define the numbering schedule, use regular expressions in the 'Numbering schedule configuration' field.

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

Structure of regular expressions

Sxx, Lxx ( ),
where
xx—arbitrary values of S and L timers
()—numbering schedule margins.

- Basis is the designations used for the dialled digit sequence recording. Digit sequence is recorded using several designations—digits dialled from the phone keypad: 0, 1, 2, 3, …, 9, #, and *. **If you use # in the dialplan, you may block the dialling completion using this key!**
- Digit sequence enclosed in square brackets corresponds to any character enclosed in these brackets.

  - Example: ([1239])—corresponds to any digit—1, 2, 3, or 9.

- Use a hyphen to define a range of characters. Mostly used inside square brackets.

  - Example 1: (1–5)—any digit from 1 to 5;
  - Example 2: ([1-39])—example listed above in the different entry format.

- 'X' character corresponds to any digit from 0 to 9.

  - Example: (1XX)—any 3-digit number that begins with 1.

- '.' —repeat previous character from 0 ad infinitum;
- «+»—repeat previous character from 1 ad infinitum;
- {a,b}—repeat previous character from 'a' to 'b' times;
- {a,}—repeat previous character more than 'a' times;
- {,b}—repeat previous character less than 'b' times.

  - Example: (810X.) —international number with any quantity of digits.

Settings affecting dialplan configuration:

- *Interdigit Long Timer ('L' character in numbering schedule record)*—entry timeout for the next digit, if there are no templates that correspond to the dialled combination;
- *Interdigit Short Timer ('S')*—entry timeout for the next digit, if the dialled combination fully matches at least one template and if there is at least one template that requires an extension dialling for the full match.

Additional features:

1. Dialled sequence replacement

Syntax: *<arg1:arg2>*

This feature allows you to replace the dialled sequence with any dialled character sequence. At that, the second argument should be defined with the specific value, both arguments may be empty.

- Example: (<83812:> XXXXXX)—this record will correspond to dialled digits 83812, but this sequence will be skipped and will not be sent to the SIP server.

2. Tone insertion to dialling

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

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

3. Dialling restriction.

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

- Example: (8 10Xxxxxxxx ! | 8 xxx xxxxxxx)—expression allows long-distance dialling only and denies outgoing international calls.

4. Replacement of dialling timer values

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

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

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

- Example: (S48XXX. | XXX) or ([1-5] XX S0)—record will trigger an instant call transfer, when the 3-digit number beginning with 1,2, … , 5 is dialled.

5. Direct address dialling (IP Dialing)

'@' placed after the number defines that the dialled call will be sent to the subsequent server address. We recommend using 'IP Dialing', as well as call reception and transmission without registration *(«Call Without Reg», «Answer Without Reg»)*. This may help when the server fails.
Also, IP Dialling address format may be used for numbers intended for the call forwarding.

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

Voice codec configuration

The signal processor of the device 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.711 is a PCM codec that does not employ a compression of voice data. This codec must be supported by all VoIP equipment manufacturers. G.711A and G.711U codecs differ from each other in encoding law (A-law is a linear encoding and U-law is non-linear). The U-law encoding is used in North America, and the A-law encoding—in Europe.

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

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

- *Codec 1..4*—you may select a codec and the .and an order of their usage. The highest priority codec should be specified in the 'Codec 1' field. For operation, you should specify at least one codec:

    - *Disabled*—codec will not be 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 codec.

- *Packetization time*—amount of voice data in milliseconds (ms) transmitted in a single RTP packet for the corresponding codec (G.711, G.729, G.723);
- *Dispersion time, ms*—parameter that cancels an echo caused by the voice signal dispersion. Parameter values may be specified in the interval from 2ms to 128ms.

NOTE! You may specify alternative voice codecs for the selected direction. For each direction, you may specify the preferred codec for voice communication in the numbering schedule. Configuration is performed in the numbering schedule. For each direction, an additional codec configuration may be specified in parentheses after the 'codecs:' word.

If you have to use multiple codecs, you may separate them with a comma ','. Multiple parameters may be specified for a single direction. In this case, separate them with a semicolon ';'— (param1:subparam1,subparam2;param2:subparam1,subparam2). subparamX permitted values: 'g711a', 'g711u', 'g729', 'g723'.

param1 and param2 permitted values—'codecs' and 'rfc2833_PT' respectively.

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

Jitter buffer

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 features the following jitter buffer settings:

- *Minimum delay, ms*—minimum expected IP package network propagation delay;
- *Maximum delay, ms*—maximum expected IP package network propagation delay;
- *Threshold for immediate packet deletion, ms*—maximum amount of time for voice package removal from the buffer. The parameter value should be greater or equal to maximum delay.
- *Buffer optimization factor*—parameter used for jitter buffer size optimization. Recommended value is 0.

Fax and modem transmission

Fax may be transmitted using 711 voice codec or T.38 specialized 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 to perform reliable fax transmissions through unstable channels.

- *Modem transmission*—select a codec to be used for data transmission when the gateway detects modem signals:

  - Disabled—modem signals will not be detected;
  - G.711a VBD—use G.711A codec in VBD mode;
  - G.711u VBD—use G.711U codec in VBD mode.

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

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

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

  - *Disabled*—codec will not be used;
  - G.711a—use G.711A codec;
  - G.711u—use G.711U codec;
  - T.38—use T.38 protocol.

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

- *Accept transition to T.38*—when selected, incoming *re-invite* to T.38 from the opposite gateway will be enabled;
- *T.38 Redundancy size*—add redundancy to T.38 packets; the value corresponds to the number of previous packets which is duplicated in each new T.38 packet. Such redundancy method is intended for packet loss during transmission.

Additional parameters

- *DTMF Transfer*—DTMF tone transmission method:

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

- *Flash transmission*—Flash transmission method:

    - *SIP info* (Hookflash)—send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/ Hook Flash* extension as *'signal=hf'*;
    - *SIP info (DTMF Relay)*—send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/dtmf-relay* extension as *'signal=hf'*;
    - *SIP info (Broadsoft)*—send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/Broadsoft* extension as *'event flashhook'*;
    - *SIP info (SSCC)*—send messages to the opposite side via SIP in INFO requests. *flash* event is sent in *Application/sscc* extension as *'event flashhook'*.

> **In the current firmware version, flash transmission is possible via SIP only.**

- *Payload type for RFC2833 packets*—payload type for packet transmission via RFC2833 (permitted values: from 96 to 127);
- *Same payload type for transmission and reception*—option is used in outgoing calls for payload type negotiation of events sent via RFC2833 (DTMF and Flash). When selected, event transmission and reception via RFC2833 is performed using the payload from 200Ok message sent by the opposite side. When unselected, event transmission is performed via RFC2833 using the payload from 200Ok being received, and reception—using the payload type from its own configuration (specified in the outgoing Invite);
- *Use voice activity detector*—when selected, enable voice activity detector;
- *Use echo cancellation*—when selected, use echo cancellation;
- *Use RTCP*—when selected, use RTCP for voice link monitoring.

    - *Transmission period*—RTCP packet transmission period, in seconds;
    - *Reception period*—RTCP message reception period measured in transmission period units; if there is not a single RTCP packet received until the reception period expires, *TAU-1M.IP* will terminate the connection.

SIP profile basic settings
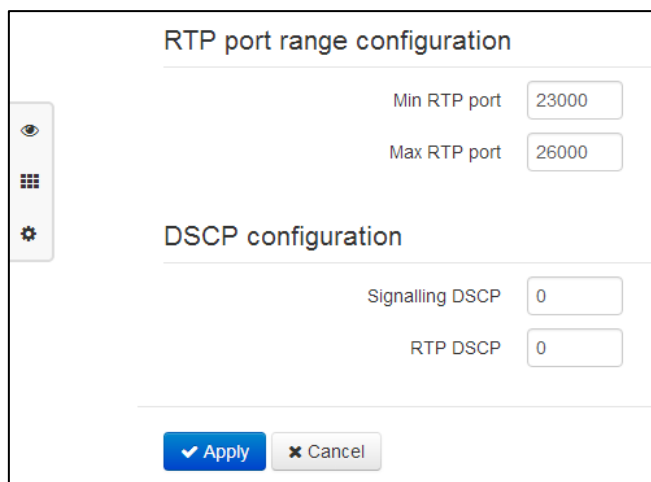
- *Use STUN*—when selected, use STUN (Session Traversal Utilities for NAT) protocol in order to define device public address (external NAT address). We recommend using this protocol for device operation through NAT;
- *STUN server address*—STUN server IP address or domain name; specify an alternative server port after the colon (default value is 3478);
- *STUN server polling period, seconds*—time period that defines transmission of a request to STUN server. The less the polling period, the faster the response to the public address changes;

—　*Transport*—select the protocol for SIP message transmission.

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

3.6.3.4 'QoS' submenu

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

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

—　*Signalling DSCP*—DSCP field value of IP packet header for signalling traffic (should be specified decimally, may take values from 0 to 63).
—　*RTP DSCP* —DSCP field value of IP packet header for voice traffic (should be specified decimally, may take values from 0 to 63).

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

3.6.3.5 'VAS management prefixes' submenu

In the 'VAS management prefixes' submenu, you may configure codes dialled from the phone unit in order to enable or disable VAS.

Subscribers may manage state of services from their phone units. The following functions are available:
—　Service activation—* service_code #;
—　Service activity check—*# service_code #;
—　Service cancellation—# service_code #.

In order to activate 'Call forward unconditional', 'Call forward on busy', 'Call forward on no answer', or 'Hotline/warmline' service, you should specify a phone number:

* service_code * phone_number #

When the activation code is entered or the service is cancelled, subscriber may hear a 'confirmation' tone (3 short tones) which means that the service has been activated or cancelled successfully.

After service confirmation code entry, the subscriber may hear either 'PBX response' tone (continuous) or a 'busy' tone (intermittent). 'PBX response' tone means that the service has been enabled and activated, 'busy' tone—that this service is disabled.

Subscriber service management

- VAS—VAS list

    - *CFU (Call forward unconditional)*—when active, all incoming calls will be forwarded to the specified number;
    - *CFB (Call forward on busy)*—when active, all incoming calls will be forwarded to the specified number, if the subscriber is busy;
    - *CFNR (Call forward on no answer)*—when active, all incoming calls will be forwarded to the specified number, if there is no answer from the subscriber;
    - *Permit to pickup incoming calls*—when activated by the subscriber, incoming calls may be picked up by other subscribers from the same pickup group;
    - Hotline/warmline—when active, the defined phone number will be dialled upon expiration of the specific time period after the phone handset will have been picked up;
    - *Call waiting*—when active, the subscriber will receive notifications on incoming calls while being in a call state. Subscriber may accept, reject or ignore waiting call;
    - *DND (Do not disturb)*—this service allows the subscriber to put temporary restriction on all incoming calls.
  - *Activation code*—service activation code;
  - *Deactivation code*—service deactivation code;
  - *Service status check code*—service activity check code.

Deactivation code and service status check code are generated automatically based on the activation code.

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

3.6.3.6 'Call signal' submenu

In the 'Call signal' submenu, you may configure an alternative call control signal (cadence) depending on the caller number or 'Alert-Info' header value in the incoming 'Invite'. Cadence value for each call signal is represented by the sequence of alternating pulses and pauses delimited by ', ' or ';'. Pulse/pause duration should be defined in milliseconds and divisible by 100. Minimum pulse/pause duration is 200 ms, maximum is 8,000 ms.

To map a specific cadence to 'Alert-Info' header value in the incoming 'Invite', you should select the *'Process Alert-Info header'* checkbox in the respective SIP profile, and define the signal name in 'Signal name' field in cadence settings (e.g. Example-cadence). When 'Alert-Info' header value in the incoming 'Invite' is <http://127.0.0.1/Example-cadence>, cadence will be output into the line.

If the cadence is not found by the 'Alert-Info' header, attempt to find the cadence by the caller number will be taken. If the latter is absent, the standard call signal with the cadence '1000, 4000' will be output.

Cadence table

	Cadence name	Cadence
☐	Bellcore-dr1	1000,4000
☐	Bellcore-dr2	1000,3000
☐	Bellcore-dr3	1000,2000
☐	Bellcore-dr4	1000,1000
☐	Bellcore-dr5	700,700,700,3000

+ Add   **✖ Remove**

To edit the specific signal, click the respective link in the *'Cadence name'* column.

To add a signal, click 'Add' button and enter the following settings:

Edit cadence

Cadence name	Bellcore-dr1
Cadence	1000,4000

✔ Apply   **✖ Cancel**
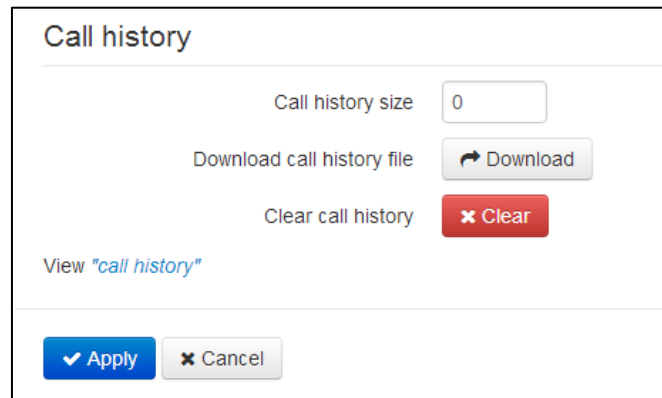
- *Cadence name*—name of the signal;
- *Cadence*—duration of the call voltage application to the phone unit, both values should be divisible by 100 ms, minimum value is 200 ms, maximum is 8,000 ms.

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

3.6.3.7 'Call history' menu

In the call history submenu, you may configure call history logging.

- – *Call history size*—maximum number of log records, may take values from 0 to 10,000 strings. Enter '0' value to disable call history logging. When the defined log limit is reached, each consequent record will delete the oldest record in the beginning of the log.
- – *Download call history file*—to save 'voip_history' file on a local PC, click 'Download' button.
- – *Clear call history*—to clear call history, click 'Clear' button.

To view the call history, follow the *'View call history'* link. For parameter monitoring description, see Section.

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

3.6.4 'IPTV' menu

3.6.4.1 'IPTV' submenu

In the 'IPTV' submenu, you may configure the IPTV service.

- – *Enable IPTV*—when selected, enable IPTV signal transmission from *TAU-1M.IP* WAN interface (from the provider network) to the devices connected to LAN interface.
- – *IGMP version*—IGMP version used for IGMP message transmission from the WAN interface (IPTV channel subscription activation or deactivation messages). Versions 2 and 3 are supported.

Renew subscription

- – *Enable*—when chosen, periodic transmission of messages containing a list of active IPTV channels is performed from WAN interface to the upstream server broadcasting IPTV signals. Disabling the periodic subscription update function is required if the upstream server disables IPTV channel broadcasting after the definite time period.
- – *Renew subscription interval, seconds*—transmission interval for messages containing a list of active IPTV channels, in seconds. Define the update rate value less than the uplink server signal broadcasting timeout.

Fast leave mode

- – Enable—when selected, enable quick group leave mode. This function minimizes the multicast stream switching delay (stream disconnects right after receiving 'Leave Group' message from the

client without an additional acknowledgement request). Avoid using this mode, when there are multiple IPTV recipients connected to a single LAN port.

VLAN IPTV

    – *Use VLAN*—when selected, use dedicated VLAN for IPTV service (VLAN number may be the same as for the Internet service or STB), otherwise IPTV will use the Internet service interface. This setting allows to configure the interface for IPTV signal reception from the external network.
    – *VLAN ID*—VLAN identifier for IPTV signal reception.
    – *802.1P*—802.1P marker (another name: *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). Utilized by QoS algorithms.

HTTP proxy settings

    – *Enable*—when selected, enable HTTP proxy feature. HTTP proxy transforms UDP stream into HTTP stream utilizing TCP (reliable packet 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-1M.IP*.

      For example, if *TAU-1M.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 *'Apply'* button.To discard changes, click *'Cancel'* button.

3.6.4.2 'STB' submenu

In the 'STB' submenu, you may configure dedicated VLAN for STB operation.

    – *Enable STB*—when selected, STB mode will be enabled for the respective ports specified in 'Local interfaces' section.

– *Use VLAN*—when selected, use dedicated VLAN for STB (VLAN number may be the same as for the Internet service or STB), otherwise STB will operate without VLAN tag in the external network.

– *VLAN ID*—VLAN number to be used for STB service traffic transmission from the device WAN interface.

– *802.1P*—802.1P marker (another name: *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). Utilized by QoS algorithms.
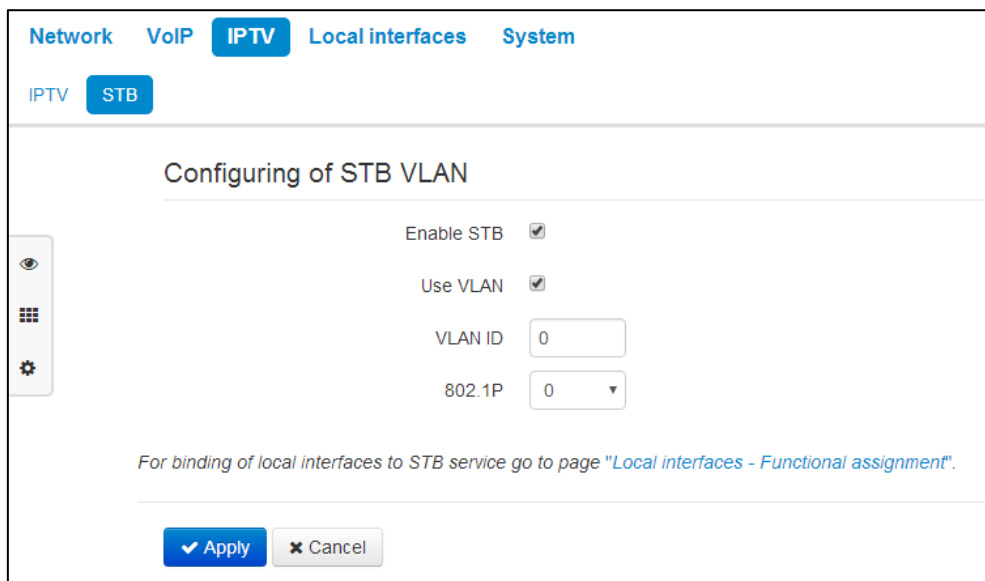
To add LAN ports to STB service, use *'Ports'* tile from the quick device configuration mode. It should be noted, that when *'Use VLAN'* option is enabled, traffic will be transferred from WAN interface and received with configured VLAN tag, but on LAN interface (WLAN) the traffic will be untagged (the tag will be removed).
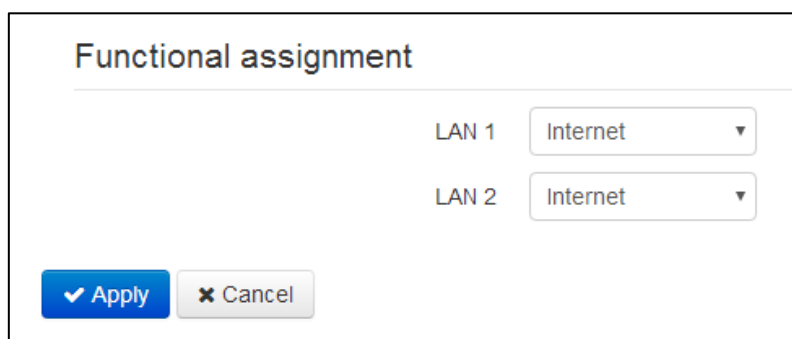
To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.6.5 'Local interfaces' menu

In the 'Local interfaces' menu, you may establish functions for each interface.

3.6.5.1 'Function' submenu

In the 'Function' submenu, you may establish service types for each LAN port.

In the current firmware version, you may select the Internet, STB and user VLAN service types for local interfaces. At that, IPTV signal broadcasting is enabled for each local interface with active IPTV function.

Internet service type means that the current LAN port will be used for Internet access; STB service type means that it will be used for STB connection. At that, the Internet port is connected to WAN interface of the respective service by routing, and STB port is connected to STB service WAN interface by bridge (traffic is transferred transparently from LAN to WAN and back).

For STB service WAN interface configuration, see Section 3.6.4.2 'STB' submenu.

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

3.6.6 'System' menu

In the 'System' menu, you may configure settings for system, time and access to the device via various protocols, change the device password and update the device firmware.

3.6.6.1 'Time' submenu

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

Time Settings

- *Time zone*—allows you to set a timezone from the list according to the nearest city in your region.
- *Daylight saving time enable*—when selected, automatic daylight saving change will be performed automatically within the defined time period.
  - *DST start*—daylight saving change starting day.
  - *DST end*—daylight saving change ending day.
  - *DST offset (minutes)*—time shift period in minutes.
- *Enable NTP*—select this checkbox to enable device system time synchronization with the particular NTP server.
- *NTP server*—time synchronization server IP address/domain name. You may enter server address manually or select it from the list.
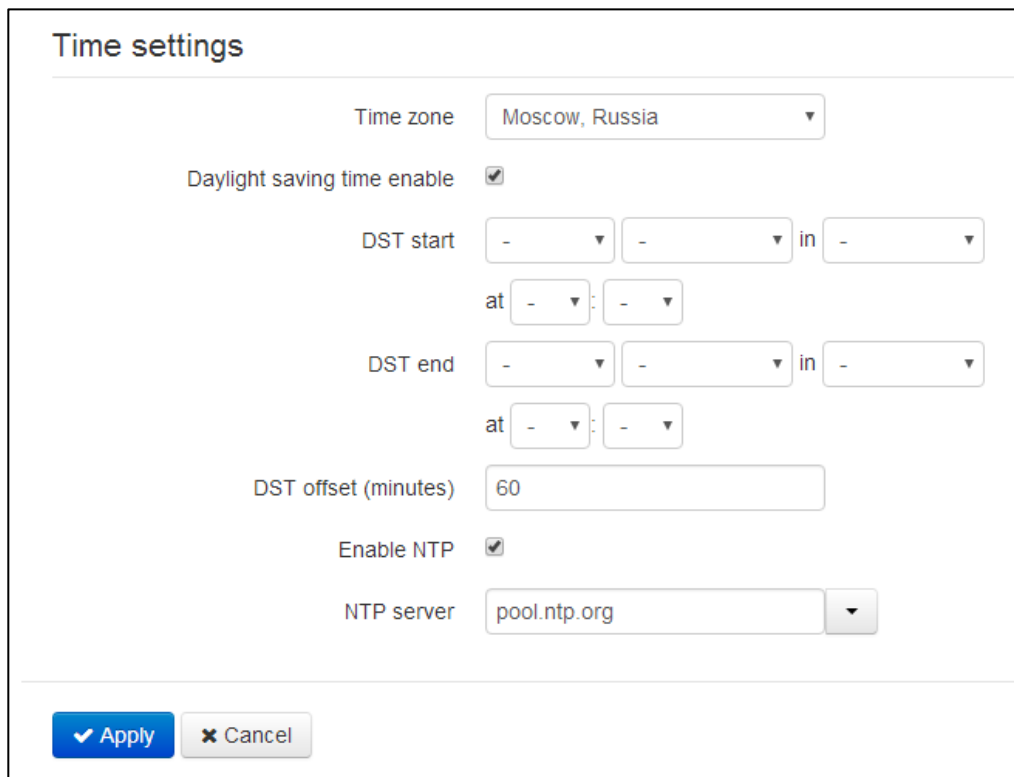
To apply a new configuration and store settings into the non-volatile memory, click *'Apply'* button. To discard changes, click *'Cancel'* button.

3.6.6.2 'Access' submenu

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

Access ports

HTTP port	80
HTTPS port	443
Telnet port	23
SSH port	22

Access to service Internet

Web
- WAN ☑ HTTP ☐ HTTPS
- LAN ☑ HTTP ☑ HTTPS

Telnet
- WAN ☐
- LAN ☑

SSH
- WAN ☐
- LAN ☑

Access to service VoIP
- Web ☐ HTTP ☐ HTTPS
- Telnet ☐
- SSH ☐

Access to service Management VLAN
- Web ☐ HTTP ☐ HTTPS
- Telnet ☐
- SSH ☐

Access to USB
- WAN ☐
- LAN ☑
- Allow access to anonymous user ☑
- Allow write permission to anonymous user ☐

✔ Apply   ✖ Cancel

Access ports

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

- *HTTP port*—number of the port that allows for the device WEB interface access via *HTTP*, default value is 80.
- *HTTPS port*—number of the port that allows for the device WEB interface access via *HTTPS* (secure connection), default value is 443.
- *Telnet port*—number of the port that allows for the device WEB interface access via *Telnet*, default value is 23.
- *SSH port*—number of the port that allows for the device WEB interface access via *SSH*, default value is 22.

You may use *Telnet* and *SSH* protocols in order to access the command line (Linux console). Username/password for console connection: admin/password.

Access to service Internet

To gain device access from the Internet service interfaces, set the following permissions:

Web, external network:

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

Web, internal network:

- *HTTP*—when selected, LAN port (or Wi-Fi wireless access point) connection to the device web configurator is enabled via HTTP (insecure connection);
- *HTTPS*—when selected, LAN port (or Wi-Fi wireless access point) connection to the device web configurator is enabled via HTTPS (secure connection).

Telnet:

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

To enable the device access via Telnet protocol from the external (via WAN port) or internal (via LAN port or Wi-Fi wireless access point) network, select the appropriate checkboxes.

SSH:

SSH is a secure device remote control protocol. However, as opposed to Telnet, SSH encrypts all traffic, including passwords being transferred.

To enable the device access via SSH protocol from the external (via WAN port) or internal (via LAN port or Wi-Fi wireless access point) network, select the appropriate checkboxes.

Access to service VoIP:

In this section, you may configure access to VoIP service interface (to configure VoIP service interface, use IP—VoIP—Network configuration) through the WEB (HTTP or HTTPS), and also via Telnet and SSH protocols. To enable access to any protocols listed above, select the appropriate checkboxes.

Access to service Management VLAN:

Use this section to configure access to the management VLAN interface that allows for device management via HTTP, HTTPS, Telnet or SSH protocols. To configure the interface, use **System—Management VLAN** page. To enable access to any protocols listed above, select the appropriate checkboxes.

> **For Telnet and SSH protocol authorization, you may use default username *admin* and password *password*. After authorization, Linux console will become available that supports basic commands of the 'shell' command interpreter.**

Access to USB:

In this section, you may configure FTP access to the USB storage device.

To enable the access to the connected USB device via FTP protocol from the external (via WAN port) or internal (via LAN port or Wi-Fi wireless access point) network, select the appropriate checkboxes.

To allow the anonymous user access to the USB device, select the 'Allow anonymous user access' checkbox.

To allow the anonymous user to write data to USB device, select the 'Allow anonymous user writes' checkbox.

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

3.6.6.3 'Log' submenu

In the 'Log' submenu, you may configure output for various debug messages intended for device troubleshooting. Debug information is provided by the following device software modules:

- VoIP manager—deals with VoIP functions operations.
- System manager—deals with the device configuration according to the configuration file.
- Configuration manager—deals with the configuration file operations (config file reads and writes from various sources) and the device monitoring information collection.

VoIP log

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

Given below is the configuration of VoIP log message types:

— *Errors*—select this checkbox, if you want to collect 'Error' type messages;
— *Warnin*—select this checkbox, if you want to collect 'Warning' type messages;
— *Debug*—select this checkbox, if you want to collect debug messages;
— *Info*—select this checkbox, if you want to collect information messages;
— *SIP trace level*– defines output level of VoIP SIP manager stack messages.

Networkd log

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

Given below is the configuration of system manager log message types:

- *Errors*—select this checkbox, if you want to collect 'Error' type messages;
- *Warning* —select this checkbox, if you want to collect 'Warning' type messages;
- *Debug* —select this checkbox, if you want to collect debug messages;
- *Info* —select this checkbox, if you want to collect information messages.

Configd log (Configuration manager log)

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

Given below is the configuration of configuration manager log message types:

- *Errors*—select this checkbox, if you want to collect 'Error' type messages;
- *Warnings*—select this checkbox, if you want to collect 'Warning' type messages;
- *Debug*—select this checkbox, if you want to collect debug messages;
- *Info*—select this checkbox, if you want to collect information messages.

Syslog settings

If there is at least a single log (VoIP manager, system manager or configuration manager) is configured for Syslog output, you should enable Syslog agent that will intercept debug messages from the respective manager and send them to remote server or save them to a local file in Syslog format.

- *Enable*—when selected, user Syslog agent is launched.
- *Mode*—Syslog agent operation mode:
  - *Server*—log information will be sent to the remote Syslog server (this is the 'remote log' mode);
  - *Local file*—log information will be saved to the local file;
  - *Server and file*—log information will be sent to the remote Syslog server and saved to the local file.

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

- *Syslog server address*—Syslog server IP address or domain name (required for 'Server' mode);
- *Syslog server port*—port for Syslog server incoming messages (default value is 514; required for 'Server' mode);

— *File name*—name of the file to store log in Syslog format (required for 'File' mode);
— *File size, KB*—maximum log file size (required for 'File' mode).

3.6.6.4 'Passwords' submenu

In the 'Passwords' submenu, you may define passwords for administrator, non-privileged user, and viewer access.

Defined passwords allow for the device access via WEB interface and also via Telnet and SSH protocols.

When signing into WEB interface, administrator (default password: **password**) has the full access to the device: read/write any settings, full device status monitoring. Non-privileged user (default password: **user**) may configure network settings (except for the Internet connection settings), may access the device status monitoring. Viewer (default password: **viewer**) may view the configuration and the device monitoring data only, without any editing permissions.

> ✓ **Administrator login: admin**
> **Non-privileged user login: user**
> **Viewer login: viewer**

— *Administrator password*—enter administrator password in the respective fields and confirm it.
— *User password*—enter non-privileged user password in the respective fields and confirm it.
— *Viewer password*—enter viewer password in the respective fields and confirm it.

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

3.6.6.5 'Configuration management' submenu

In the 'Configuration management' submenu, you may save and update the current configuration.
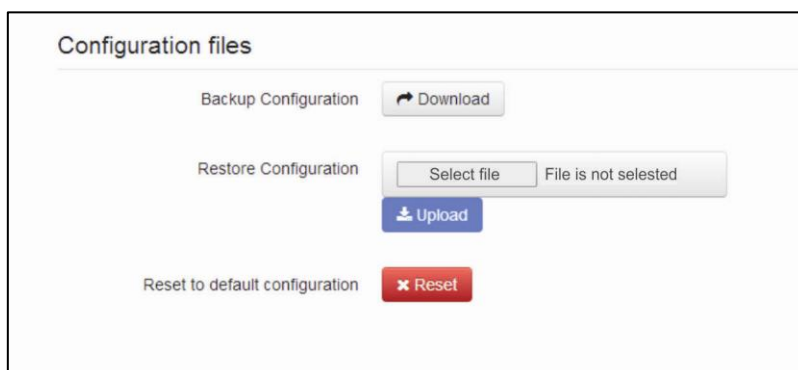
Buckup configuration

To save the current device configuration to a local PC, click 'Download' button.

Restore configuration

Upload configuration archive to device—select configuration file stored on a local PC. To update the device configuration, click *'Select file'* button, specify a file (in .tar.gz format) and click *'Upload'* button. Uploaded configuration will be applied automatically and does not require device reboot.

– *Reset to default configuration*—to reset the device to default factory settings, click *'Reset'* button.

3.6.6.6 'Firmware upgrade' submenu

In 'Firmware upgrade' submenu, you may update the firmware of the device.
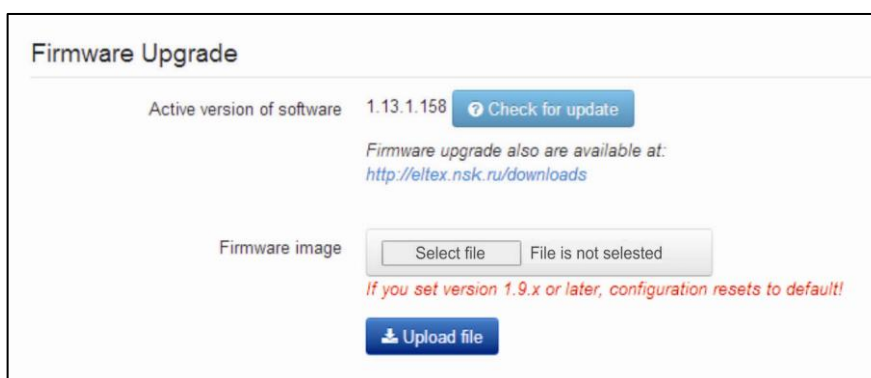
– *Firmware version*—installed firmware version.
– *Check for updates*—click this button to check the availability of the latest firmware version. With this function, you may quickly check the latest firmware version and update the firmware, if necessary.

Firmware update check function requires Internet access.

You may update the device firmware manually by downloading the firmware file from the web site *http://eltex.nsk.ru/downloads* and saving it on the computer. To do this, click the 'Select file' button in the *'Firmware image'* field, and specify path to firmware .tar.gz format file.

To launch the update process, click 'Upload file' button. The process may take several minutes (its current status will be shown on the page). The device will be automatically rebooted when the update is completed.

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

3.6.6.7 'Reboot' submenu

In the 'Reboot' submenu, you may reboot the device.
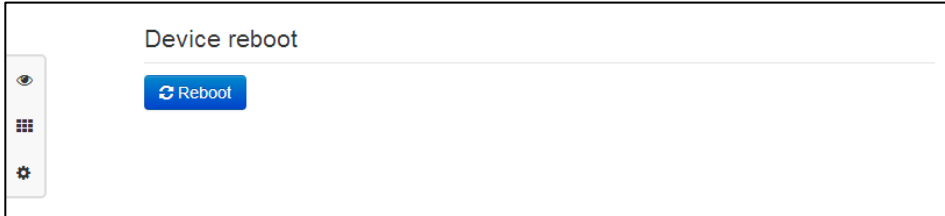
Click the 'Reboot' button to reboot the device. Device reboot process takes approximately 1 minute to complete.

3.6.6.8 'Autoconfiguration' submenu

In the 'Autoconfiguration' submenu, you may configure DHCP-based autoprovisioning algorithm and TR-069 subscriber device automatic configuration protocol.

DHCP-based autoprovisioning

- *Provisioning mode*—select the device update mode; there are several options available:

  - *Disabled*—automatic updates of the device configuration and firmware are disabled;
  - *Configuration and firmtware*—periodic updates of the device configuration and firmware are enabled;
  - *Configuration only*—only periodic updates of the device configuration are enabled;
  - *Firmware only*—only periodic updates of the device firmware are enabled.

- *Priority from*—this parameter manages names and locations of configuration and firmware files:

  - *Static settings*—paths to configuration and firmware files are defined by the *'Configuration file'* and *'Firmware file'* settings accordingly; for detailed algorithm operation, see Section 6;
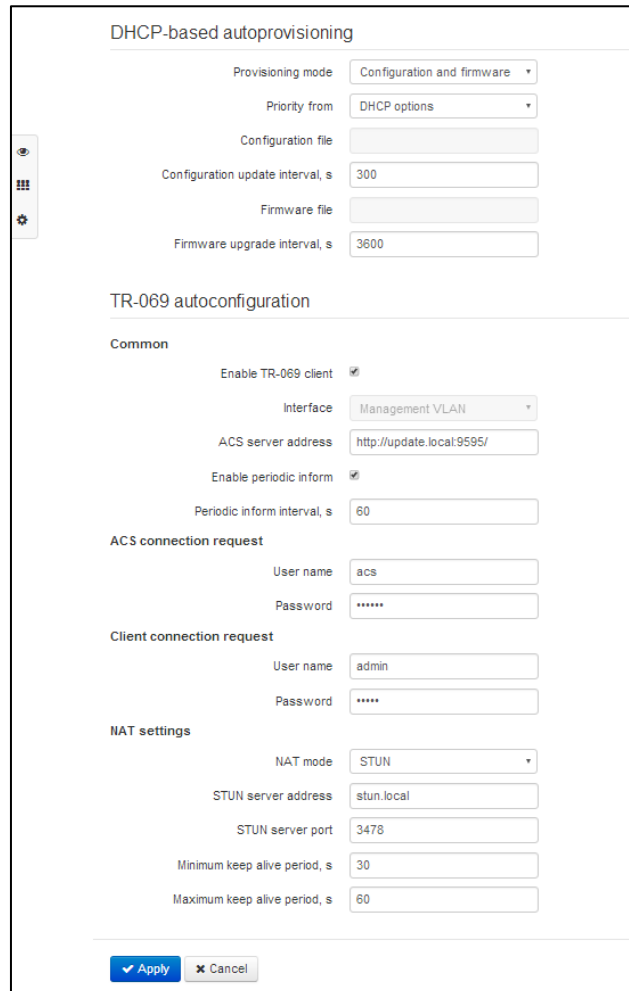 - *DHCP options*—paths to configuration and firmware files are defined by the DHCP Option 43, 66, and 67 (to do this, you should select DHCP for the Internet service); for detailed algorithm operation, see Section 6.

- *Configuration file*—full path to configuration file—defined in URL format (at this time, you may upload configuration files via TFTP and HTTP protocols):

  tftp://<server address>/<full path to cfg file>
  http://<server address>/<full path to cfg file>
  where< server address > is HTTP or TFTP server address (domain name or IPv4).
  <full path to cfg file >—full path to configuration file on server.

- *Configuration update interval, seconds*—time period in seconds that will be used for periodic device configuration update; if 0 is selected, device will be updated only once—immediately after startup.
- *Firmware file*—full path to firmware file—defined in URL format (at this time, you may upload firmware files via TFTP and HTTP protocols):

  tftp://<server address>/<full path to firmware file>
  http://<server address>/<full path to firmware file>
  where< server address > is HTTP or TFTP server address (domain name or IPv4).
  <full path to firmware file >—full path to firmware file on server.

- *Firmware update interval, seconds*—time period in seconds that will be used for periodic device firmware update; if 0 is selected, device will be updated only once—immediately after startup.

For detailed DHCP-based automatic update algorithm, see Section 6 Device automatic update algorithm based on DHCP.

TR-069 autoconfiguration:

Common:

- *Enable TR-069 client*—when selected, integrated TR-069 protocol client will be enabled;
- *Interface*—select the interface for TR-069 protocol operation. If *'Management VLAN'* interface is enabled on the gateway, this VLAN will be used for TR-069 protocol operation automatically. Interface selection setting will be disabled;
- *Interface*—an interface, that will be used for the device autoconfiguration;
- *ACS server address*—autoconfiguration server address. Enter address in the following format: http://<address>:<port> or https://<address>:<port> (<address> –ACS server IP address or domain name, <port>—ACS server port, default value is 80). Alternatively, the client will exchange the data

---

with ACS server via the secure protocol—HTTPS. By default, ACS server produced by Eltex utilizes port 9595 for communication;

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

ACS connection request:

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

Client connection request:

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

NAT settings

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

– *NAT mode*—identifies the method, that will be used by client for obtaining its public address information. The following modes are possible:

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

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

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

When *Manual* mode is selected, client public address should be entered manually with *NAT address* setting (in IPv4 format).
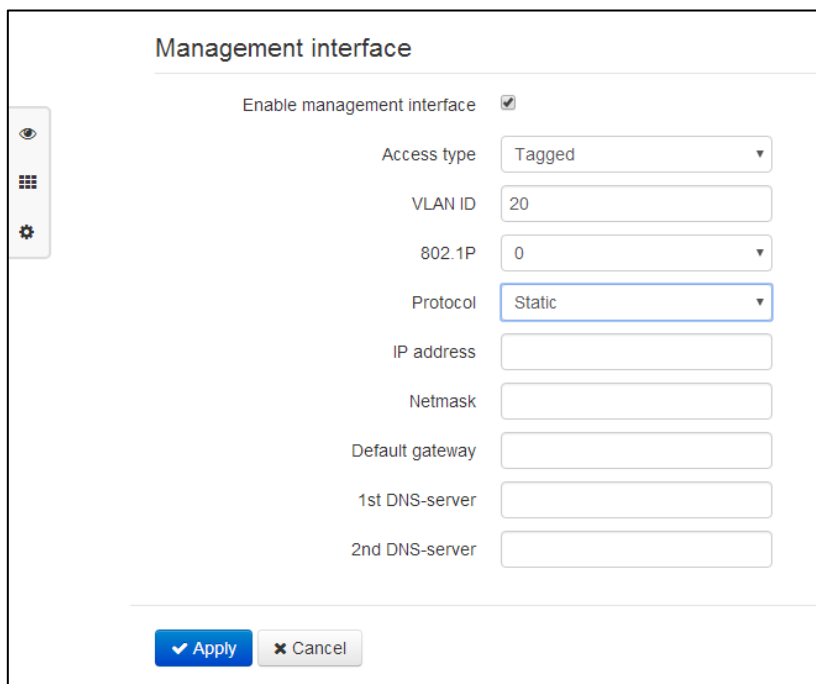
> **For correct ACS server operation behind the NAT, STUN server minimum polling period should be less than maximum session time provided by the NAT device.**

TR-069 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 '*Apply*' button. To discard changes, click '*Cancel*' button.

3.6.6.9 'Management interface' submenu

Use this menu to configure the network interface and establish the device network management via HTTP, HTTPS, Telnet or SSH protocols.

Management interface

Enable management interface	☑
Access type	Tagged ▼
VLAN ID	20
802.1P	0 ▼
Protocol	Static ▼
IP address	
Netmask	
Default gateway	
1st DNS-server	
2nd DNS-server	

✔ Apply   ✖ Cancel

- *Enable management interface*—when selected, device management will be performed via this interface.

- *Access type*—defines interface operation mode.

  - *Tagged*—data is transferred by the interface with the defined VLAN ID.

  - *Untagged*—data is transferred by the interface without VLAN.

VLAN ID—*identifier for interface definition into virtual local area network.*
- *802.1P*—802.1P marker (another name: *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 settings 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 the management interface.
    - *Netmask*—subnet mask for the management interface.
    - *Default gateway*—default gateway IP address for the management interface.
    - *1st DNS-server, 2nd DNS-server*—DNS server IP addresses required for the gateway autoconfiguration protocols' operation; to configure protocols, use **System**—**Autoconfiguration** page.

  - *DHCP*—operation mode where IP address, subnet mask, DNS address and other necessary settings for the 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)* field value 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:device vendor**][DEVICE:**device type**][HW:**hardware version**] [SN:**serial number**][WAN:**WAN interface MAC address**][LAN:**LAN interface MAC address**][VERSION:**software version**]**
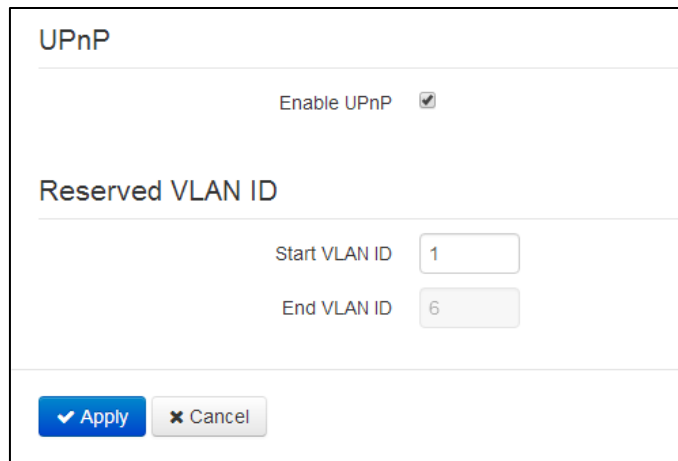
  Example:
  [VENDOR:Eltex][DEVICE:TAU-1M.IP][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]
  [LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

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

3.6.6.10 'Additional settings' submenu

In 'Additional settings' submenu, you may enable UPnP.

- *Enable UPnP*—when selected, UPnP will be active. UPnP is used by some applications (for example, DC clients, such as FlylinkDC++) for automatic creation of forwarding rules for TCP/UDP ports used by these applications on the uplink router. We recommend turning UPnP on in order to enable file sharing services within the network.

Reserved VLAN ID

Reserved VLAN IDs are required for solving intrasystem tasks of the gateway and may be changed depending on the VLAN ID being used for the system:

- *Start VLAN ID*—starting VLAN ID value in the reserved range, may take values in range [1-4090];
- *End VLAN ID*—ending VLAN ID value in the reserved range. This setting is unavailable for editing and calculated automatically.

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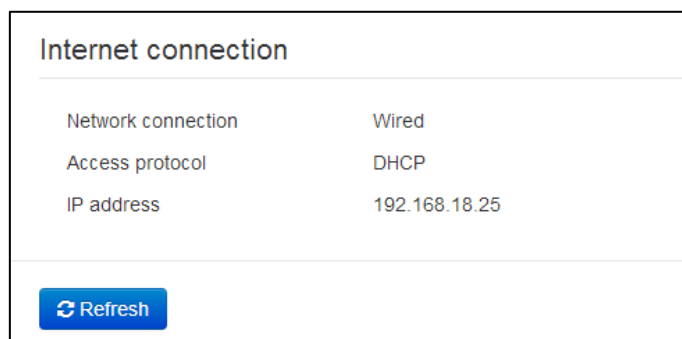
3.7 System monitoring

To enter the 'System monitoring' mode, select 'Monitoring' from the left-hand side panel.

Some pages does not feature automatic update of the device monitoring data. To obtain the current information from the device, click ⟳ Refresh **button.**

3.7.1 'Internet' submenu

In the 'Internet' submenu, you may view basic network settings of the device.

Internet connection	
Network connection	Wired
Access protocol	DHCP
IP address	192.168.18.25

⟳ Refresh

Internet access

- — _Network connection_—method of connection to data network. To configure the connection, use **Network—Internet** section.

    - ▪ _Wired_—connection to the provider network is established through the WAN port using copper-wire or optical patch cord.
    - ▪ _3G/4G USB modem_—connection to the provider network is established using 3G/4G USB modem connected to USB port on the device rear panel.

- — _Access protocol_—protocol used for the Internet access.
- — _IP address_—device IP address in the external network.
- — _IP address in the internal provider network_—IP address used within the internal provider network for access to local network resources of the provider.

3.7.2 'VoIP' submenu

In 'VoIP' submenu, you may view VoIP network interface status, monitor subscriber units, test lines, and monitor IMS.

Status of VoIP network interface

IP address   0.0.0.0

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
☐	1	001	None			Disabled					Test

⊘ Register   ⊗ Unregister

IMS monitoring

Line	1
IMS management	Off
Three-party conference	–
Call hold	–
Call Waiting	–
Hotline	–
Hotline number	–
Hotline timeout, s	–
XCAP name for call transfer	–

VoIP network interface status

– *IP address*—IP address for VoIP service network interface.

Monitoring of subscriber units

– *Line*—device subscriber unit number.
– *Local number*—subscriber phone number assigned to this subscriber port.
– *Registration*—state of registration on proxy server for the group phone number:
  - *Disabled*—SIP server registration function is disabled in SIP profile settings;
  - *Error*—registration was unsuccessful;
  - *Completed*—registration on SIP server successfully completed.
– *Expires in*—expiration time of subscriber port registration on SIP server.
– *Server address*—address of the server that the subscriber line has been registered at for the last time.
– *Line state*—physical line status. The line may have one of the following states:
  - *Inactive*—the phone handset is on-hook (or subscriber port is disabled), normal operation;

- *Active*—the phone handset is off-hook; 'PBX response' tone, ringback tone, or error tone is transmitted into the line, or the line is in the call state;
- *Ringing tone*—ringing tone is supplied to the phone headset (during the incoming call).
- *Test*—line testing started.

– *Call state 1, 2*—each subscriber port may support up to 2 communication sessions simultaneously. In this field you may see the state of the call with the respective remote subscriber. The call may have one of the following states:

- *Dialling number*—call is being dialled from the phone unit;
- *Busy*—call has cleared back for some reason, busy tone is transmitted into the line;
- *Outgoing call*—remote subscriber is being dialled, ringback tone is transmitted into the line;
- *Incoming call*—incoming call is being received at the phone port, ringing tone is transmitted into the line;
- *Conversation*—voice connection is established with the remote subscriber;
- *Opposite on hold*—remote subscriber is on hold;
- *Local on hold*—local subscriber has been put on hold by the remote subscriber;
- *Error, put phone onhook*—error tone is transmitted into the line. As a rule, error tone is played on the busy signal timeout expiration (configured separately for each line), when the subscriber doesn't put the phone onhook.

– *Remote user 1, 2*—remote subscriber phone number for each communication session.
– *Line test*—click the 'Test' button to launch the subscriber line testing. Process status is represented by a countdown timer (in the 'Line state' column) indicating the remaining test time. You cannon run the test for multiple lines simultaneously. Test duration—80 seconds. Subscriber unit is blocked for the time of the test—it will not be able to make or receive calls.

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
☐	1	001	None			Testing (74 s)					⟳

To see the results when the test finishes, click 🔍 button in the 'Line test' column. Results are represented in the table mode and contain the following data:

- *Test date*
- *TIP wire constant extraneous voltage*
- *RING wire constant extraneous voltage*
- *Line power voltage*
- *Voltage between TIP and RING wires*
- *Voltage between TIP wire and ground*
- *Voltage between RING wire and ground*
- *Capacity between TIP and RING wires*
- *Capacity between TIP wire and ground*
- *Capacity between RING wire and ground*

Line 1 test result example:

Test result: Line 1	✖
Test date	07:08:15 01.01.1970
Foreign DC voltage A (TIP)	0.141025 U
Foreign DC voltage B (RING)	0.179273 U
Line supply voltage	-49.408009 U
Resistance A (TIP) - B (RING)	1225.932983 kΩ
Resistance A (TIP) - Ground	592.529297 kΩ
Resistance B (RING) - Ground	371.247986 kΩ
Capacity A (TIP) - B (RING)	50 nF
Capacity A (TIP) - Ground	50 nF
Capacity B (RING) - Ground	50 nF

🗑 Remove   ✖ Close

Under the Subscriber set monitoring table, you may find buttons for forced registration or de-registration of the selected lines.

IMS monitoring

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

– *Management from IMS*—shows whether the subscriber line service remote control from IMS server is enabled (configured in SIP profile, see *'Profiles'* submenu).
– *Three-way conference*—shows whether the 'Three-way conference' service activation command is received from IMS server.
– *Call hold*—shows whether the 'Call hold' service activation command is received from IMS server.
– *Call waiting*—shows whether the 'Call waiting' service activation command is received from IMS server.
– *Hotline*—shows whether the 'Hotline' service activation command is received from IMS server.
– *Hotline number*—show the 'Hotline' service phone number in the activation command from IMS server.
– *Hotline timeout, seconds*—show the dialling timeout for the 'Hotline' service in the activation command from IMS server.

– *'Call transfer' service name*—shows the defined name of the 'Call transfer' service.

✔ —service is active.
✖ —service is inactive.

3.7.3 'Ethernet ports' submenu

In the 'Ethernet ports' submenu, you may view the device Ethernet port state.

Ethernet port status

- *Port*—name of the port.
    - *WAN*—external network port.
    - *LAN 1..2*—local area network port.
- *Connection*—status of the connection to this port:
    - *Enabled*—network device is connected to the port (link is active);
    - *Disabled*—network device is not connected to the port (link is inactive).
- *Speed*—data rate of the external network device connected to the port (10/100/1000Mbps).
- *Mode*—data transfer mode:
    - *Full-duplex*—full duplex;
    - *Half-duplex*—half-duplex.
- *Transmitted* —quantity of bytes sent from the port.
- *Received*—quantity of bytes received by the port.

To obtain actual information on the Ethernet port state, click 'Update' button.

3.7.4 'DHCP' submenu

In the 'DHCP' submenu, you may view the list of network devices connected to the LAN interface, that were assigned IP addresses by a local DHCP server, and also the IP address lease expiration time.
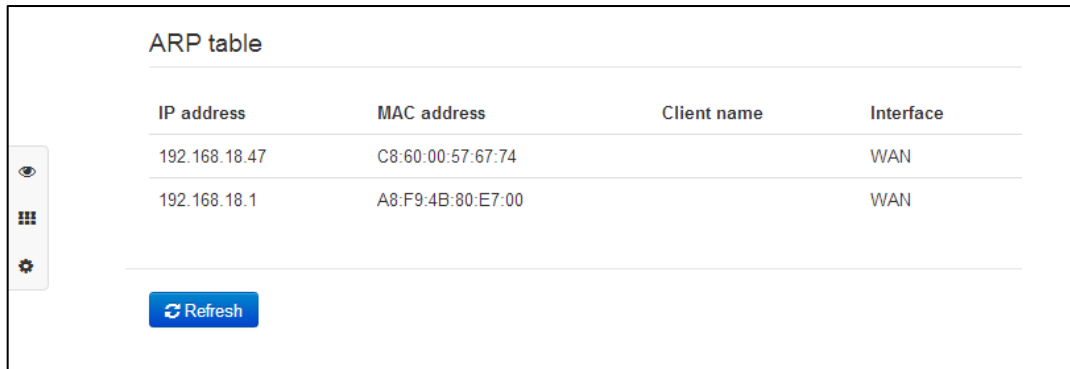
Active DHCP leases

- MAC address—connected device MAC address.
- *Client name*—connected device network name.
- *IP address*—IP address assigned to the client from the address pool.
- *Lease expires*—remaining time of the assigned address lease.

To obtain actual information on DHCP clients, click 'Update' button.

3.7.5 'ARP' submenu

In the 'ARP' submenu, you may view an ARP table. In ARP table, you may find information on IP and MAC address correspondence for neighbouring network devices.
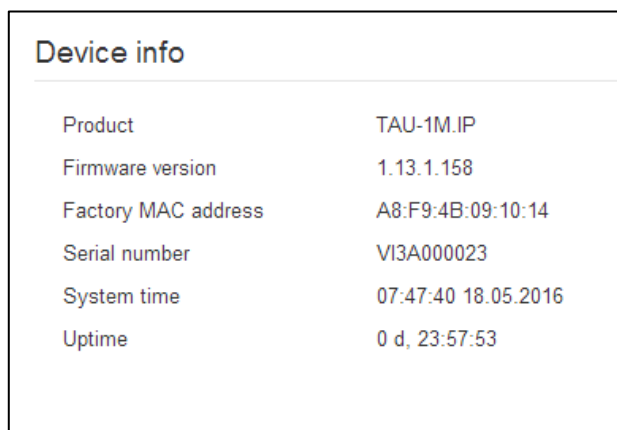

ARP table

- IP address—device IP address.
- MAC address—device MAC address.
- *Client name*—connected device network name.
- *Interface*—interface of the device active side: WAN, LAN, Bridge.

To obtain actual information, click 'Update' button.

3.7.6 'Device' submenu

In the 'Device' submenu, you may find general device information.

Device Information

- − *Product*—device model name.
- − *Firmware version*—device firmware version.
- − *Factory MAC address* —device WAN interface MAC address defined by the manufacturer.
- − *Serial number*—device serial number defined by the manufacturer.
- − *System time*—current date and time defined in the system.
- − *Uptime*—time of operation since the last startup or reboot of the device.

3.7.7 'Conntrack' submenu

In the 'Conntrack' submenu, you may find the current active network connections of the device.

Active NAT session

- − *Count of active connections*—total number of active network connections.
- − *Count of shown connections*—number of connections shown in the WEB interface. In order to maintain high performance of the WEB interface, maximum number of connections shown is limited to 1024. You may view other connections with the device command console (*cat /proc/net/nf_conntrack*).

List of connections

- − *Protocol*—protocol that the connection is being established through.
- − *Source address*—connection initiator IP address and port number.
- − *Destination IP*—connection destination IP address and port number.
- − *Timeout*—time period until the connection termination.

To obtain actual information, click 'Update' button.

3.7.8 'Routing' submenu

In the 'Routing' submenu, you may view the device routing table.

Route table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Interface
192.168.18.0	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
172.20.0.0	192.168.18.1	255.255.255.0	UG	0	0	0	eth1
10.100.101.0	192.168.18.1	255.255.255.0	UG	0	0	0	eth1
172.16.0.0	192.168.18.1	255.255.252.0	UG	0	0	0	eth1
192.168.0.0	192.168.18.1	255.255.0.0	UG	0	0	0	eth1
0.0.0.0	192.168.18.1	0.0.0.0	UG	0	0	0	eth1

↻ Refresh

- − *Destination*—IP address of destination host or subnet that the route is established to.
- − *Gateway*—gateway IP address that allows for the access to the 'Destination'.
- − *Genmask* – subnet mask.
- − *Flags*—specific route attributes. The following flag values exist:

  - ▪ **U**—means that the route is created and passable;
  - ▪ **H**—identifies the route to the specific host;
  - ▪ **G**—means that the route lies through the external gateway. System network interface provides routes in the network with direct connection. All other routes lie through the external gateways. 'G' flag is user for all routes except for the routes in the direct connection networks;
  - ▪ **R**—means that the route most likely was created by a dynamic routing protocol running on a local system with the 'reinstate' parameter;
  - ▪ **D**—means that the route was added on reception of the ICMP Redirect Message. When the system learns the route from the ICMP Redirect message, the route will be added into the routing table in order to exclude redirection of the following packets intended for the same destination. Such routes are marked with the 'D' flag;
  - ▪ **M**—means that the route was modified—likely by a dynamic routing protocol running on a local system with the 'mod' parameter applied;
  - ▪ **A**—means buffered route with corresponding record in the ARP table;
  - ▪ **C**—means that the route source in the core routing buffer;
  - ▪ **L**—means that the route destination is an address of this PC. Such 'local routes' exist in the routing buffer only;

- **B**—means that the route destination is a broadcasting address. Such 'broadcast routes' exist in the routing buffer only;
- **I**—means that the route is related to the loopback interface with a goal that differs from the access to the ring network. Such 'internal routes' exist in the routing buffer only;
- **!** means that datagrams sent to this address will be rejected by the system.

– *Metric*—defines route cost. Metrics allows you to sort the duplicate routes, if they are exist in the table.
– *Ref*—identified number of references to the route for connection establishment (not used by the system).
– *Use*—number of route detections performed by IP protocol.
– *Interface*—name of the network interface that the route lies through.

To obtain actual information, click 'Update' button.

3.7.9 'Call history' submenu

In the 'Call history' submenu, you may view the list of performed phone calls and the summary for each call.

The device RAM may store up to 10,000 records for performed calls. If the record number exceeds 10,000, the oldest records (at the top of the table) will be removed, and new ones will be added at the end of the file.

Log statistics will not be collected, when the history size is zero.

Filter (show)

Change call history settings

No	Line	Local	Remote	Remote host	Start call time	Start talk time	Talk duration	State	Type	TxPack	TxBytes	RxPack	RxBytes
1	1	1026	1025	192.168.18.34	03:47:30 01.01.1970	03:47:39 01.01.1970	31s	remote clear	outgoing	97	9211	1499	257828
2	1	1026	1025	192.168.18.34	03:48:58 01.01.1970	-	-	remote busy	outgoing	0	0	0	0

« ‹ › »

20 ▾ records per page

Page 1 from 1

'Call history' table field description:

– *№*—sequence number of the record in the table;
– *Line*—device subscriber port number;
– *Local*—subscriber number assigned to this subscriber port;
– *Remote*—remote subscriber number that the phone connection has been established with;
– *Remote host*—remote subscriber IP address that the phone connection has been established with;
– *Start call time*—call received/performed time and date;
– *Start talk time*—Call start time and date;
– *Talk duration*—call duration in seconds;
– *State*—transient state or reason for call clearing; description becomes available, when you hover the cursor over the call state record;

- *Type*—call type: outgoing or incoming;
- *TxPack*—number of RTP packets sent during the call;
- *TxBytes*—number of bytes sent during the call;
- *RxPack*—number of RTP packets received during the call;
- *RxBytes*—number of bytes received during the call.

In the call history table, you may search records by different parameters; to do this, click the 'Filter (Show)' link. Filtering may performed by the subscriber line address, local or remote number, opposite side IP address, call received time, call start time, call state and call type. For filtering parameter description, see call history table field description above.

Call received time from/to or *Call start time from/to*—call received/performed time period or call start time period in the 'hh:mm:ss dd.mm.yyyy' format.

To hide the table record filtration parameter settings, click the *'Hide filter'* link.

To configure call history parameters, click 'Configure call history parameters' link.

- Click ◀◀ button to proceed to the table showing the first record.
- Click ◀ button to proceed to the previous page with the call history table.
- Click ▶ button to proceed to the next page with the call history table.
- Click ▶▶ button to proceed to the table showing the last record.

Use 'Records on page' selector to configure the number of table records displayed on a single page.

3.8 Configuration example

1. Connect a PC to one of the device LAN ports, connect provider network cable to the WAN port.
2. Enter the gateway IP address in the browser address bar (default value: 192.168.1.1).
3. When the device connection is successfully established, you will see the login and password request window. Fill in the fields and click 'Sign in' button (default login: admin, default password: password).

If this field is not visible, make sure that the automatic IP address obtaining feature is enabled in the network connection settings on your PC.

4. In the 'Internet' tile, you may configure an external connection. If *TAU-1M.IP*is intended to be used as a router—select the 'Router' value in the 'Operation mode' field of the 'Internet' tile. In 'Protocol' field, select the protocol used by your ISP and enter all the necessary data according to the provider's instructions. If you are required to use static settings in order to connect to the provider network, select 'Static' value in the 'Protocol' field and fill the 'Device external IP address', 'Subnet mask', 'Default gateway', 'Primary DNS', and 'Secondary

DNS' fields—parameter values should be obtained from the provider. To save and apply settings, click [✔] button.

To specify additional parameters, go to advanced settings mode by clicking the 'Details' link (see Section 3.6.2.1 'Internet' submenu).

5. When your ISP network employs MAC address tethering, click 'Details' button in the 'Internet' tile and open the 'MAC address configuration' submenu. In the 'WAN MAC address configuration' section, select the

'Redefine MAC' checkbox and enter MAC address of the device previously connected to the Internet into the 'MAC' field. To save and apply settings, click 'Apply' button.
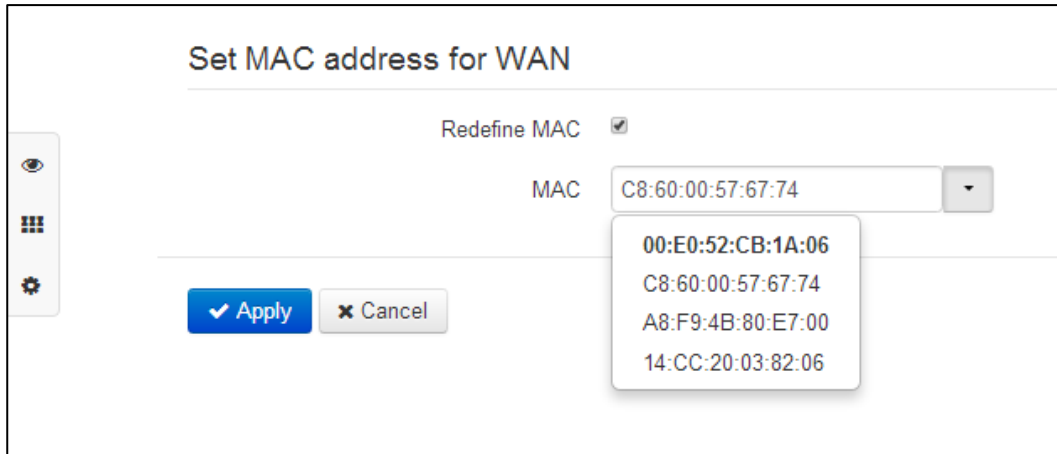
If *TAU-1M.IP* is intended to be used as a 3-port switch—select the 'Bridge' value in the 'Operation mode' field of the 'Internet' tile. In *'IP address'* field, specify an address that will be used for the device access. Define subnet mask (default: 255.255.255.0). To save and apply settings, click [✓] button.
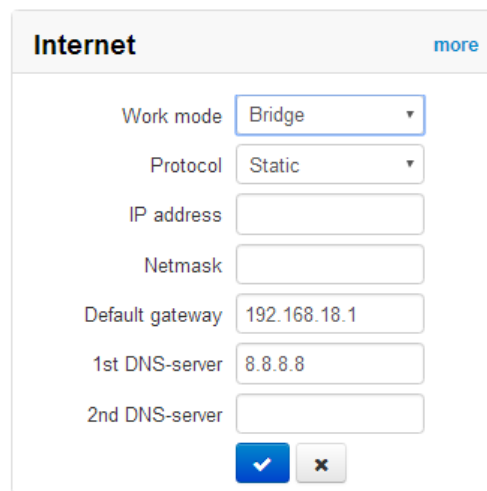
In the *'Bridge'* mode, the gateway will not assign IP addresses automatically using DHCP to devices connected to the LAN interface.

6. In the 'VoIP' tile, you may perform quick configuration of the subscriber line for operation via SIP. To do this, select 'Line 1' tab. Select 'Enable' checkbox, enter the phone number for this line, and login and password for SIP server authorization. To save and apply settings, click [✓] button.

7. Select 'SIP' tab in the 'VoIP' tile to configure SIP parameters. Specify IP address or domain name of the SIP server and registration server (if necessary) in the corresponding fields. If ports used by servers differ from 5060, specify alternative ports after the colon. Specify SIP domain, if necessary. Select 'Registration' checkbox, if the subscriber is required to register on SIP server for VoIP operation (as a rule, registration is required). To save and apply settings, click [✔] button.



To specify additional parameters, go to advanced settings mode by clicking the 'Details' link (see Section 3.6.3 'VoIP' Menu).

8. If you are planning to use IPTV, select 'Enable IPTV' in the 'IPTV' tile. To enable transmission of IPTV streams via HTTP, select 'Enable HTTP proxy' checkbox. In the 'HTTP port' field, specify the port that will be used for connection of external devices to a local HTTP proxy. To save and apply settings, click [✔] button.

IPTV   more

Enable IPTV ☑

Enable HTTP proxy ☑

HTTP port   1234

If IPTV service require a dedicated VLAN, go to advanced settings mode by clicking the 'Details' link and specify VLAN ID in the respective field (see Section 3.6.4 'IPTV' menu).

4 VALUE ADDED SERVICES USAGE

4.1 Call transfer

Call transfer service may be performed locally using gateway resources, or remotely using resources of a communicating device. If the service is performed using resources of a communicating device, the access to 'Call transfer' service is established via subscriber port settings menu—*'VoIP' -> 'Line configuration'*—by selecting *'Transmit Flash'* value in *'Flash operation mode'* field. Service process logics in this case will be defined by the communicating device.

When *'Call transfer'* service is performed locally using gateway resources, the access to this service is established via subscriber port settings menu—*'VoIP' -> 'Line configuration'*—by selecting *'Attended calltransfer'* or *'Unattended calltransfer'* in *'Flash operation 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.

'Attended calltransfer' service usage:

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

- R 0—disconnect a subscriber on hold, connect to online subscriber;
- R 1—disconnect an online subscriber, connect to subscriber on hold;
- R 2—switch to another subscriber (change a subscriber);
- R 3—conference. R 4—call transfer; voice connection will be established between Subscribers A and C;
- 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 *'Attended calltransfer'* service operation algorithm.

Subscriber A — **Subscriber B** — **Subscriber C**

Message	Direction	Description
INVITE	A → B	Subscriber A establishes a connection to the Subscriber B
100 Trying	B → A	
180 Ringing	B → A	
200 OK	B → A	
ACK	A → B	

The conversation between subscribers A and B

Message	Direction	Description
INVITE sendonly	B → A	Subscriber B puts Subscriber A on hold (presses the Flash)
100 Trying	A → B	
200 OK receiveonly	A → B	
ACK	B → A	

Message	Direction	Description
INVITE	B → C	Subscriber B connects to Subscriber C
100 Trying	C → B	
180 Ringing	C → B	
200 OK	C → B	
ACK	B → C	

The conversation between subscribers B and C

At this stage, the subscriber B can be: switch between subscribers A and C, using a combination of R (Flash) 2; recapture of one of the subscribers, using the combination of R 0 or R 1; connect subscribers A and C replace the handset.

Message	Direction	Description
INVITE inactive	B → C	Subscriber B puts on hold Subscriber C
100 Trying	C → B	
200 OK inactive	C → B	
ACK	B → C	

Message	Direction	Description
REFER (replaces)	B → A	Subscriber B hangs up (call transfer)
202 Accepted	A → B	
NOTIFY Activated	A → B	
200 OK	B → A	

Message	Direction	Description
INVITE (replaces)	A → C	Subscriber A connects to Subscriber C
100 Trying	C → A	
180 Ringing	C → A	
200 OK	C → A	
ACK	A → C	

The conversation between the subscribers A and C.

Message	Direction	Description
BYE	C → B	Subscriber C terminates the connection with the Subscriber B
200 OK	B → C	
NOTIFY Terminated	B → A	
200 OK	A → B	
BYE	B → A	Subscribers B terminates the connection to the subscriber A
200 OK	A → B	

'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 *'Unattended calltransfer'* service operation algorithm.
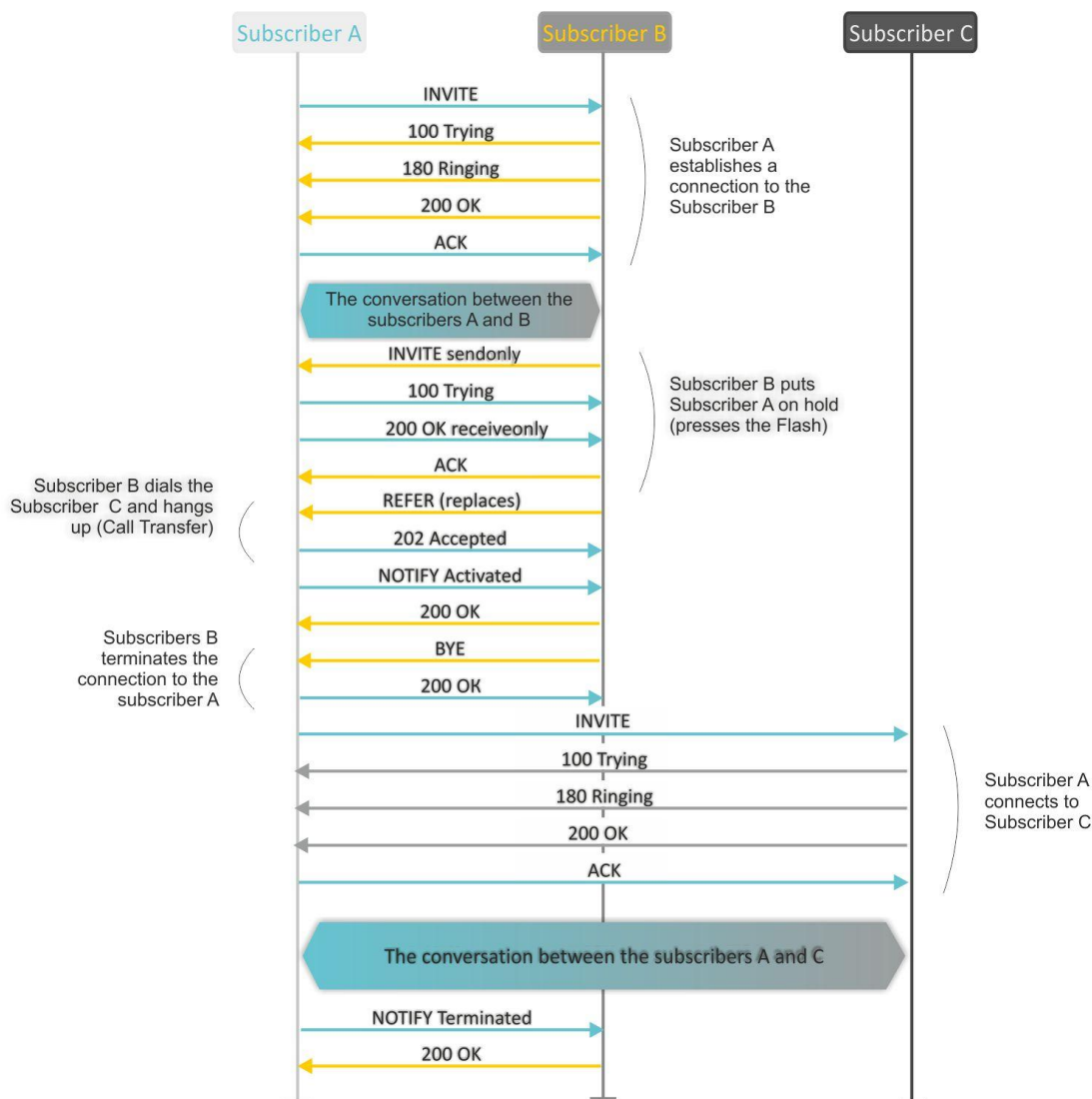
4.2 Call Waiting

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

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

Access to this service is established via subscriber line settings menu by selecting *'Attended calltransfer'*, or *'Unattended calltransfer'* in the *'flash operation 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 a new call (change a subscriber);
    — R—short clearback (flash).

4.3 Three-way conference call

Three-way conference is a service, that enables simultaneous phone communication for 3 subscribers. Press R 3 keys to enter the conference mode (see Section *4.1 Call transfer*).

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

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

4.3.1 Local conference

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

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

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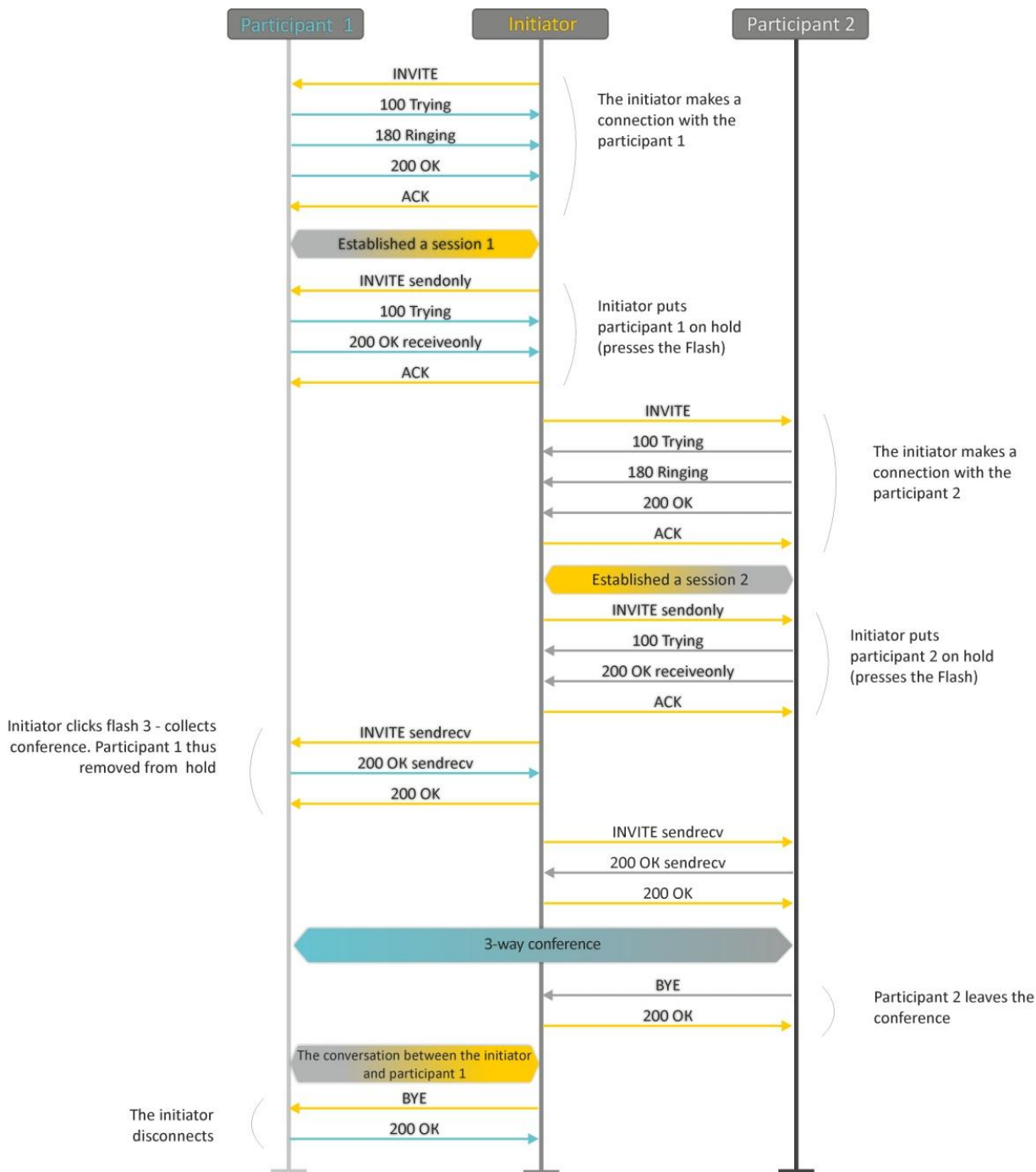
4.3.2 Remote conference

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

TAU-1M.IP Gateway
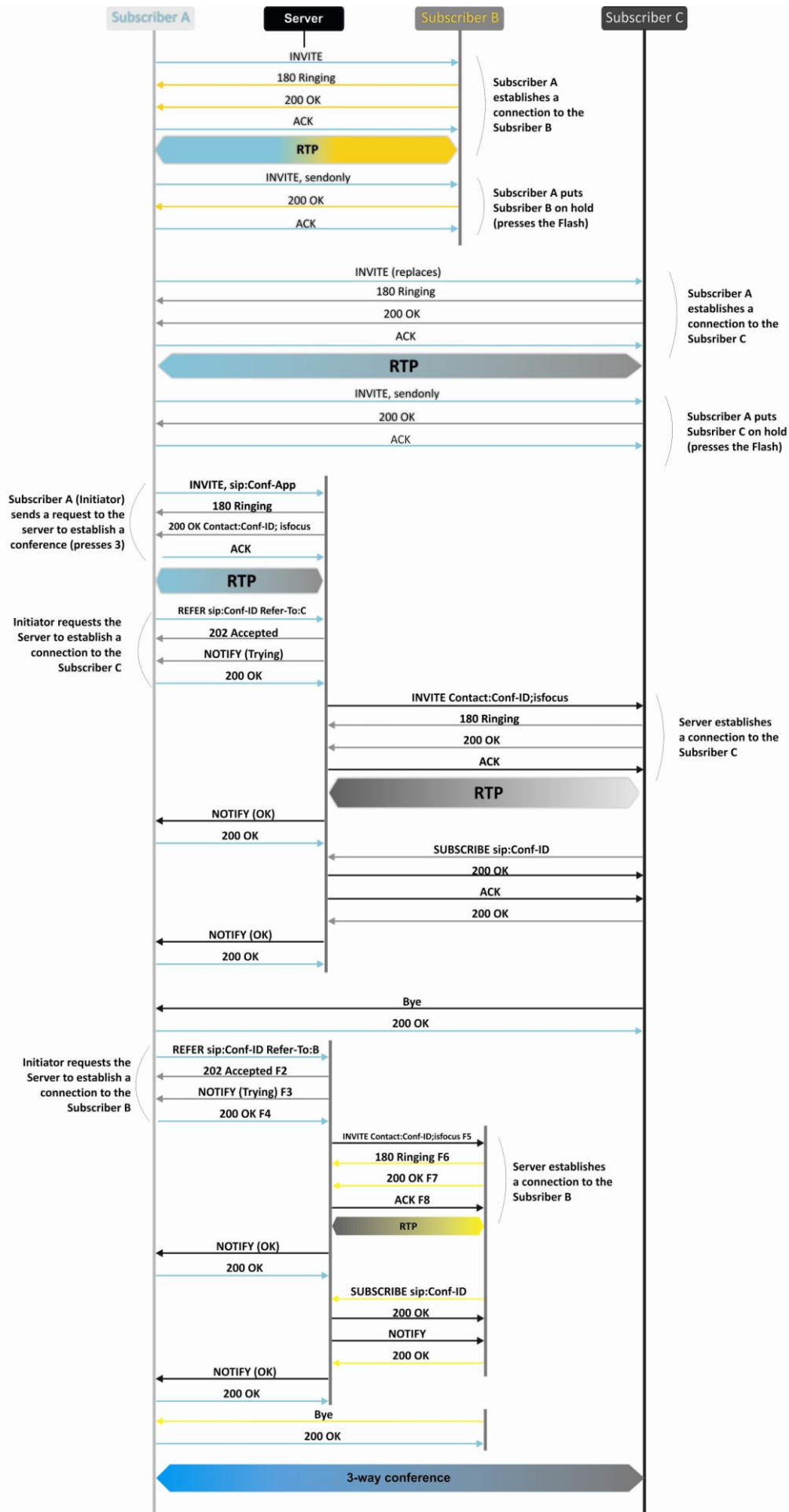
5 CONNECTION ESTABLISHMENT ALGORITHMS

5.1 Algorithm of a Successful Call via SIP Protocol

SIP (Session Initiation Protocol) 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 IETFRFC 3665. This section describes an example of a connection initiation scenario via SIP between two gateways, that know each other IP addresses in advance.
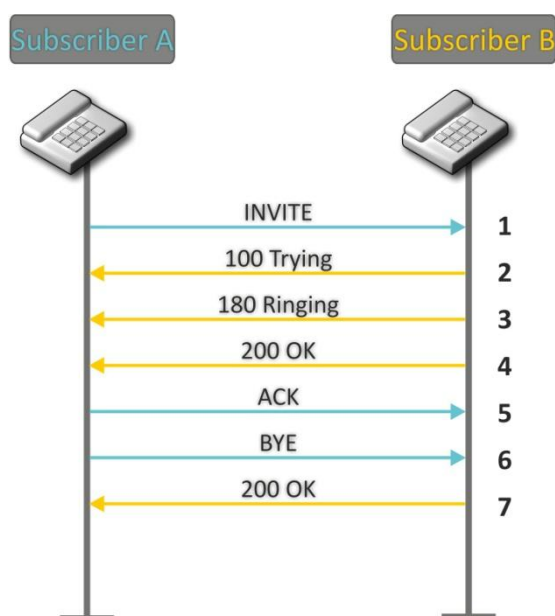
Algorithm description:

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.

5.2 Call Algorithm Involving SIP Proxy Server

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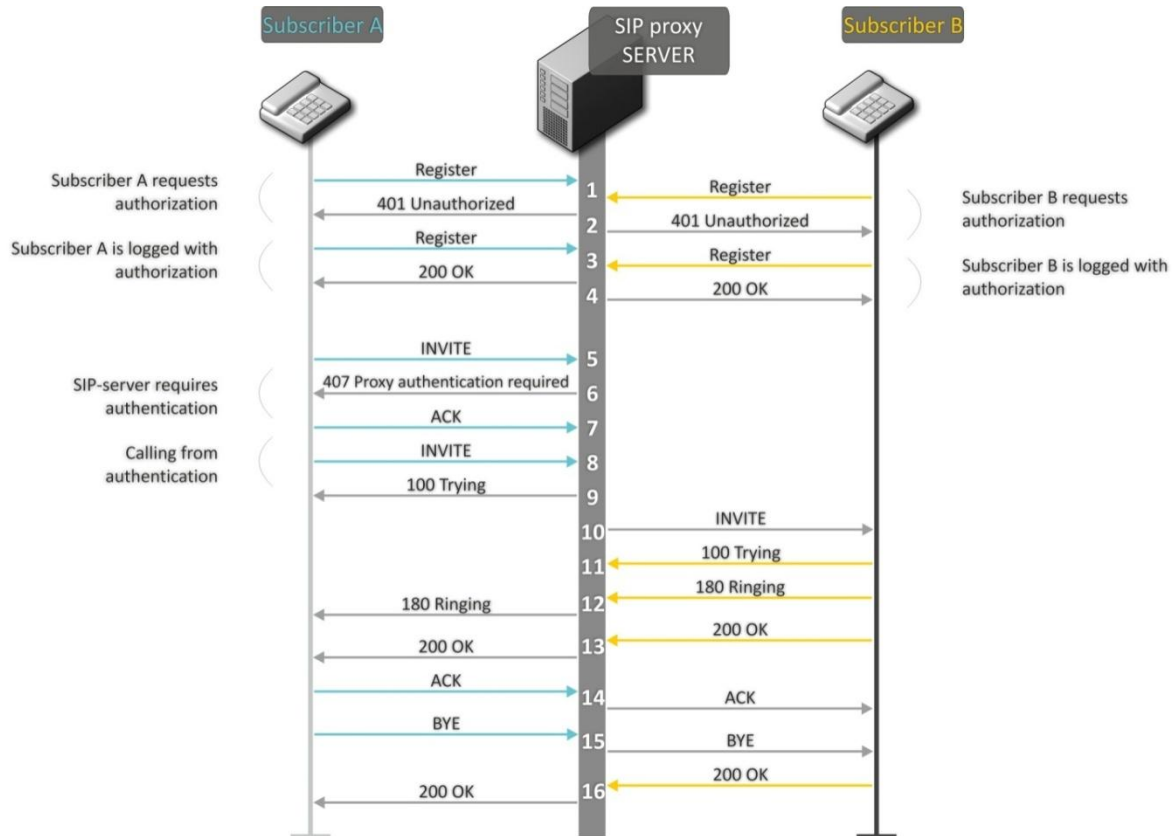
Algorithm description:

Registration at the 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.
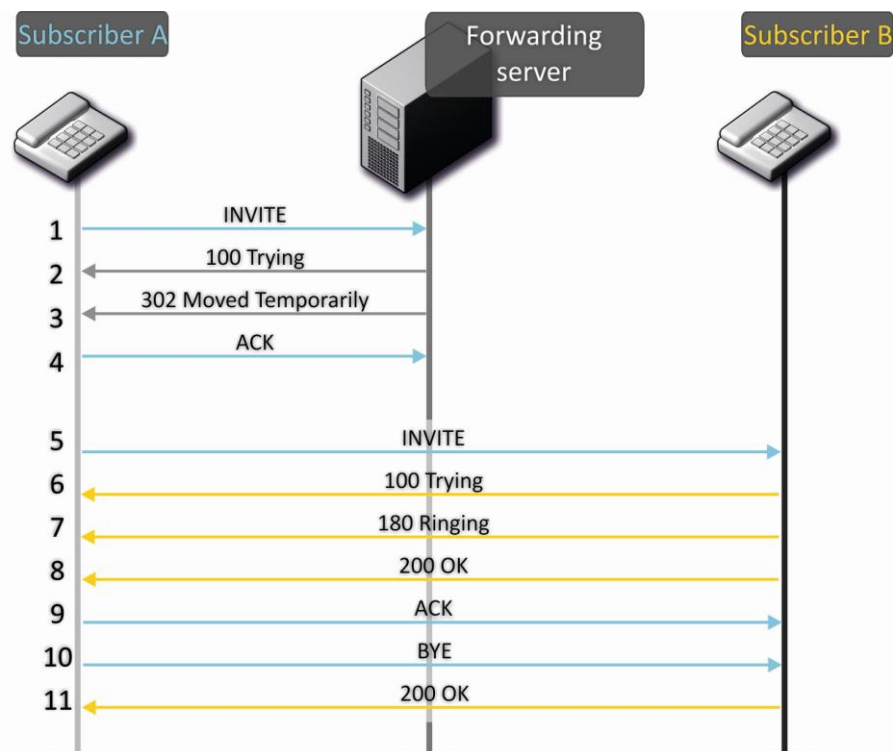9. SIP server receives the command for processing.
10. SIP server translates Subscriber A call request directed at Subscriber B.
11. Subscriber B gateway receives the command for processing.
12. Subscriber B is free. In this moment, 'ringing' tone is sent to the Subscriber B phone, and 'ringback' tone 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.

5.3 Call Algorithm Involving Forwarding Server

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

Algorithm description:

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

6 DEVICE AUTOMATIC UPDATE ALGORITHM BASED ON DHCP

Device automatic update algorithm is defined by the *'Parameter priority from'* value.

1. If the *'Static settings'* value is selected, then the full path (including access protocol and server address) to configuration file and firmware file will be defined by *'Configuration file'* and *'Firmware file'* parameters. Full path should be specified in URL format (HTTP and TFTP are supported):

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

    – <protocol>—protocol used for downloading corresponding files from the server (HTTP and TFTP are supported).
    – <server address>—address of the server with a file to be downloaded (domain name or IPv4).
    – <path to file>—path to file on the server.

    You may use the following wildcards in URL (reserved words substituted with the specific values):

    – *$MA*—MAC address—this wildcard in file URL is substituted by the native device MAC address;
    – *$SN*—Serial number—this wildcard in file URL is substituted by the native device serial number;
    – *$PN*—Product name—this wildcard in file URL is substituted by the model name (e.g. TAU-1M.IP);
    – *$SWVER*—Software version—this wildcard in file URL is substituted by the firmware version number;
    – *$HWVER*—Hardware version—this wildcard in file URL is substituted by the device hardware version number.

For MAC address, serial number and model name, see 'Device' section on the monitoring page.

URL examples:

tftp://download.server.loc/firmware.file,
http://192.168.25.34/configs/tau1m/my.cfg,
tftp://server.tftp/$PN/config/$SN.cfg,
http://server.http/$PN/firmware/$MA.frm, etc.

At that, some URL parameters may be omitted. For example, configuration file may be specified in the following format:

http://192.168.18.6
or
config_tau1m.cfg

If the system is unable to extract the necessary file downloading parameters (protocol, server address or path to file on server) from configuration file or firmware file URL, it will attempt to extract an unknown parameter from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), when address obtaining via DHCP is enabled for the Internet service (DHCP option format and analysis will be provided below). If the system is unable to extract missing parameter from DHCP options, default value will be used.

- Protocol: tftp
- Server address: update.local
- Configuration file name: tau1m.cfg
- Firmware file name: tau1m.fw

Thus, if you leave *'Configuration file'* and *'Firmware file'* fields empty, and Options 43 or 66, 67 with file locations are not obtained via DHCP, configuration file URL will be as follows:

tftp://update.local/tau1m.cfg

and the firmware file URL:

tftp://update.local/tau1m.fw

2. If 'DHCP options' value is selected, configuration file and firmware file URLs will be extracted from DHCP Option 43 (Vendor specific info) or 66 (TFTP server) and 67 (Boot file name), wherefore address obtaining via DHCP should be enabled for the Internet service (DHCP option format and analysis will be provided below). If DHCP options fail to provide some of the URL parameters, default parameter value will be used.

- Protocol: tftp
- Server address: update.local
- Configuration file name: tau1m.cfg
- Firmware file name: tau1m.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>|8|<vlan_tag>

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

Algorithm of identification of configuration file and firmware file URL parameters from DHCP Options 43 and 66, 67.

1. DHCP exchange initialization

Device initializes DHCP exchange after the startup.

2. Option 43 analysis

When Option 43 is received, codes 5, 6, and 7 suboptions are analyzed in order to identify the server address and the configuration and firmware file names.

3.   Option 66 analysis

If Option 43 is not received from DHCP server or it is received but the system fails to extract the server address, Option 66 will be discovered. If the system fails to obtain the firmware file name, Option 67 will be discovered. They are used for TFTP server address and the firmware file path extraction respectively. Next, configuration and firmware files will be downloaded from Option 66 address via TFTP.

Special aspects of configuration updates.

Configuration file should be in**.tar.gz** format (this format is used when configuration is saved from the web interface in the 'System' - 'Configuration management' tab). Configuration downloaded from the server will be applied automatically and does not require device reboot.

Special aspects of firmware updates.

Firmware file should be in.tar.gz format. When the firmware file is loaded, the device unpacks it and checks its version (using 'version' file in tar.gz archive).

If the current firmware version matches the version of the file obtained via DHCP, firmware will not be updated. Update is performed only when firmware versions are mismatched. When the firmware image is written into the device flash memory, the Power indicator will flash green, orange and red in succession.

Do not power off or reboot the device, when the firmware image is written into the flash memory. These actions will interrupt the firmware update, that will lead to the device boot partition corruption. The device will become inoperable. To restore the device operation, use the instruction provided in Section 7.

7 SYSTEM RECOVERY AFTER FIRMWARE UPDATE FAILURE

If the failure occurred during the firmware update (via Web interface or DHCP-based automatic update)—for example, you have pressed power button by accident—and the device became inoperable (Power LED is solid red), use the following device recovery algorithm:

- Extract the contents of the firmware archive.
- Connect your PC to the device WAN port and specify the address for the network interface from 192.168.1.0/24 subnet.
- Launch TFTP client on the PC (for Windows, we recommend using Tftpd32), specify 192.168.1.6 as the remote host address and select linux.bin file from the extracted firmware archive.
- Run the command to send the file to the remote host (**Put** command). File transfer to *TAU-1M.IP* should start.
- If the file transfer process is started, wait until it finishes, after that *TAU-1M.IP* will write the firmware into the memory and launch the system automatically. Write time is approximately 5 minutes. When the device is successfully restored, the Power LED will be orange or green. Device will retain the configuration that was used before the failure. If the device is unreachable, reset the device to default settings.
- If the file transfer is not initiated, check the PC network settings for errors and try again. If you are unable to restore the device, send it to the service centre for repairs or connect it to the device via COM port using special adapter (if available).

APPENDIX A. CALCULATION OF PHONE LINE LENGTH

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

Cable grade for subscriber lines of local exchange network	Core diameter, mm	Electrical resistance of 1 km circuit, Ω, max.	Line length (other phone units), km	Line length ('Rus' phone units), km
TPP, TPPep, TPPZ, TPPepZ, TPPB,TPPepB, 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
KSPP, KSPZP, KSPPB, KSPZPB, KSPPt, KSPZPt, KSPZPK	0.90	56.8	28.521	12.324

APPENDIX B. RUNNING USER-DEFINED SCRIPT UPON SYSTEM STARTUP

Sometimes, it is necessary to perform specific actions on the device startup, that may not be specified in the configuration file settings. For this purpose, TAU-1M.IP allows you to set the user-defined script in the configuration file. This script may feature any desired sequence of commands.

For user-defined script execution, use the following settings section in the configuration file:

UserScript:
    Enable: "0"
    URL: ""

'Enable' option allows (if the value is 1) or denies (if the value is 0) execution of the script which path is specified in the URL parameter.

Executed script may be located on the remote server or on the device itself. The script may be downloaded from the remote server via HTTP or TFTP. Consider configuration file examples for user-defined script execution from various sources.

1. Execution from HTTP server
To execute the script from HTTP server, you should specify full path to file in HTTP-URL format within URL parameter:
URL: "http://192.168.0.250/user-script/script.sh"
After the device startup, script.sh file located in the 'user-script' folder at 192.168.0.250 will be downloaded automatically via HTTP from the server and executed afterwards.
2. Execution from TFTP server
To execute the script from TFTP server, you should specify full path to file in TFTP-URL format within URL parameter:
URL: "tftp://192.168.0.250/user-script/script.sh"
After the device startup, script.sh file located in the 'user-script' folder at 192.168.0.250 will be downloaded automatically via TFTP from the server and executed afterwards.
3. Local script execution
Due to file system specifics, local script should be located in the /etc/config folder only, as the contents of this folder are the only one that remain after the device reboot. Script in /etc/config folder may be created either with vi editor, or downloaded from the external TFTP server (using 'tftp –gluser.sh<TFTP-server address>' command). After creation of the script, you should set execution permissions with 'chmod 777 /etc/config/user.sh' command.
In the configuration file, local script execution URL should be as follows:
URL: "File://etc/config/user.sh"

It is important to note, that the user script should begin with the '#!/bin/sh' directive.

TECHNICAL SUPPORT

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

9 Ibragimova street, Almaty, Republic of Kazakhstan, 050032,
Phone:
+7(727) 320-18-40
+7(727) 320-18-38
E-mail: info@eltexalatau.kz

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

http://www.eltexalatau.kz/en