Комплексные решения для построения сетей

TAU-4M.IP

Руководство по эксплуатации, версия ПО 2.3.1

Абонентский шлюз IP-телефонии

IP-адрес: **http://192.168.1.1**
имя пользователя: **admin**
пароль: **password**

http://eltex-co.ru/support/downloads/

Версия документа	Дата выпуска	Содержание изменений
Версия 1.3	30.04.2020	Синхронизация с версией ПО 2.3.1
Версия 1.2	31.01.2020	Синхронизация с версией ПО 2.3.0 Добавлено: - 2.7.7 Подменю «CPU» - 2.7.11 Подменю «Диагностика» Изменено: - 2.6.2.1 Подменю «Интернет» - 2.6.3.3 Подменю «Настройка линий» - 2.6.3.4 Подменю «Профили SIP» - 2.6.5.4 Подменю «Аутентификация WEB» - 2.7.2 Подменю «IP-телефония»
Версия 1.1	28.05.2018	Синхронизация с версией ПО 2.1.0
Версия 1.0	15.01.2018	Первая публикация
Версия программного обеспечения	Версия ПО: 2.3.1.4 Версия веб-интерфейса: 2.3.0.54	

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Описание
Полужирный шрифт	Полужирным шрифтом выделены примечания и предупреждения, название глав, заголовков, заголовков таблиц.
Курсив Calibri	Курсивом Calibri указывается информация, требующая особого внимания.

Примечания и предупреждения

Примечания содержат важную информацию, советы или рекомендации по использованию и настройке устройства.

Предупреждения информируют пользователя о ситуациях, которые могут нанести вред устройству или человеку, привести к некорректной работе устройства или потере данных.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ....6
1 ОПИСАНИЕ ИЗДЕЛИЯ....7
1.1 Назначение....7
1.2 Характеристика устройства....7
1.3 Структура и принцип работы изделия....9
1.4 Основные технические параметры....11
1.5 Конструктивное исполнение....12
1.5.1 Верхняя панель устройства....12
1.5.2 Задняя панель устройства....13
1.6 Световая индикация....13
1.7 Сброс к заводским настройкам....14
1.8 Комплект поставки....14
2 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР....15
2.1 Начало работы....15
2.2 Смена пользователей....15
2.3 Режимы работы Web-интерфейса....16
2.4 Применение конфигурации и отмена изменений....17
2.4.1 Применение конфигурации....17
2.4.2 Отмена изменений....18
2.5 Меню быстрого конфигурирования....18
2.5.1 Интернет....19
2.5.2 IP-телефония....21
2.5.3 IP-телевидение....22
2.5.4 Система....22
2.6 Расширенные настройки....23
2.6.1 Основные элементы Web-интерфейса....23
2.6.2 Меню «Сеть»....24
2.6.3 Меню «IP-телефония»....49
2.6.4 Меню «IP-телевидение»....81
2.6.5 Меню «Система»....83
2.7 Мониторинг системы....101
2.7.1 Подменю «Интернет»....101
2.7.2 Подменю «IP-телефония»....102
2.7.3 Подменю «Ethernet-порты»....107
2.7.4 Подменю «DHCP»....107
2.7.5 Подменю «ARP»....108
2.7.6 Подменю «Устройство»....108
2.7.7 Подменю «CPU»....109
2.7.8 Подменю «Conntrack»....110
2.7.9 Подменю «Маршрутизация»....111
2.7.10 Подменю «История вызовов»....112
2.7.11 Подменю «Диагностика»....114
2.8 Пример настройки....114
3 ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ....118
3.1 Передача вызова....118
3.2 Уведомление о поступлении нового вызова – Call Waiting....120
3.3 Трехсторонняя конференция....121
3.3.1 Локальная конференция....121
3.3.2 Удаленная конференция....122
4 АЛГОРИТМЫ УСТАНОВЛЕНИЯ СОЕДИНЕНИЯ....125
4.1 Алгоритм успешного вызова по протоколу SIP....125
4.2 Алгоритм вызова с участием SIP прокси-сервера....125

4.3 Алгоритм вызова с участием сервера переадресации 126
5 АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP 128
6 ПРОЦЕДУРА ВОССТАНОВЛЕНИЯ СИСТЕМЫ ПОСЛЕ СБОЯ ПРИ ОБНОВЛЕНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 132
ПРИЛОЖЕНИЕ А. РАСЧЕТ ДЛИНЫ ТЕЛЕФОННОЙ ЛИНИИ..... 133
ПРИЛОЖЕНИЕ Б. ЗАПУСК ПРОИЗВОЛЬНОГО СКРИПТА ПРИ СТАРТЕ СИСТЕМЫ 134
ПРИЛОЖЕНИЕ В. НАСТРОЙКА DHCP-КЛИЕНТОВ В МУЛЬТИСЕРВИСНОМ РЕЖИМЕ 135

ВВЕДЕНИЕ

В настоящее время IP-телефония является одной из наиболее быстро развивающихся телекоммуникационных услуг. Для возможности предоставления VoIP-услуг абонентам сети разработаны абонентские шлюзы серии *TAU-4M.IP* (далее — устройство).

Абонентский шлюз IP-телефонии *TAU-4M.IP* используется для подключения аналоговых телефонных аппаратов к сетям пакетной передачи данных, выход на которые осуществляется через интерфейс Ethernet.

Устройство ориентировано на домашних пользователей и небольшие офисы.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения абонентских шлюзов IP-телефонии *TAU-4M.IP.*

1 ОПИСАНИЕ ИЗДЕЛИЯ

1.1 Назначение

Устройство *TAU-4M.IP* – высокопроизводительный абонентский шлюз IP-телефонии с полным набором функций, позволяющих потребителю использовать преимущества IP-телефонии.

Абонентский шлюз *TAU-4M.IP* предназначен для подключения аналоговых телефонных аппаратов и факс-модемов к IP-сети. Благодаря встроенному маршрутизатору устройство обеспечивает возможность подключения оборудования локальной сети к сети широкополосного доступа. К устройству можно подключить один компьютер, доступ в интернет для которого возможен с помощью встроенных функций NAT/DHCP-сервера. USB-разъем используется для подключения внешнего накопителя, 3G/4G USB-модема.

1.2 Характеристика устройства

Интерфейсы:

- FXS: 4 порта RJ-11;
- LAN: 1 порт Ethernet RJ-45 10/100BASE-T;
- WAN: 1 порт Ethernet RJ-45 10/100BASE-T;
- USB: 1 порт USB2.0.

Питание шлюза осуществляется через внешний адаптер 12 В постоянного тока от сети 220 В.

Функции:

- сетевые функции:
  - работа в режиме «моста» или «маршрутизатора»;
  - поддержка PPPoE (PAP-, SPAP- и CHAP-авторизация, PPPoE-компрессия);
  - поддержка PPTP;
  - поддержка L2TP;
  - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
  - поддержка DNS;
  - поддержка NAT;
  - сетевой экран;
  - поддержка NTP;
  - поддержка механизмов качества обслуживания QoS (QoS по DSCP и 802.1P);
- поддержка функций IPTV;
- протоколы IP-телефонии: SIP;
- эхокомпенсация (рекомендации G.168);
- детектор активности речи (VAD);
- генератор комфортного шума;
- обнаружение и генерирование сигналов DTMF;

- передача DTMF (INBAND, rfc2833, SIP INFO);
- передача факса:
  - G.711A/G.711U;
  - T.38;
- работа с SIP-сервером и без него;
- функции ДВО:
  - удержание вызова – Call Hold;
  - передача вызова – Call Transfer;
  - уведомление о поступлении нового вызова – Call Waiting;
  - переадресация по занятости – Call Forward at Busy;
  - переадресация по неответу – Call Forward at No answer;
  - безусловная переадресация – Call Forward Unconditional;
  - не беспокоить – DND;
  - Caller ID: FSK, DTMF;
  - горячая линия – Hotline;
  - групповой вызов;
  - перехват вызова – Call Pickup;
  - трехсторонняя конференция;
  - гибкий план нумерации;
- обновление ПО через Web-интерфейс;
- поддержка DHCP-based autoprovisioning;
- TR-069;
- удаленный мониторинг, конфигурирование и настройка: Web-интерфейс, Telnet.

На рисунке 1 приведена схема включения *TAU-4M.IP*.

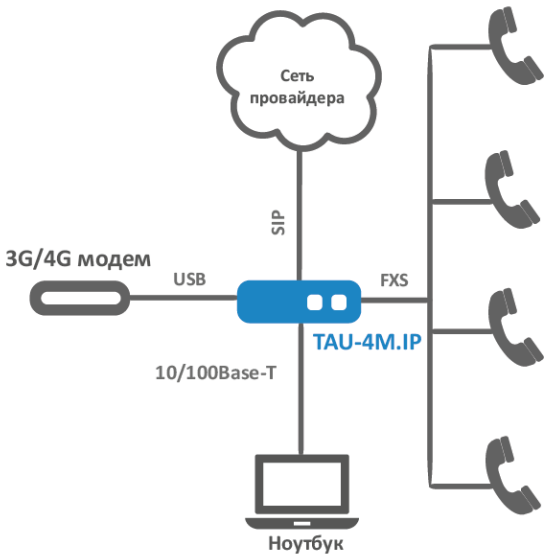


Рисунок 1 – Функциональная схема использования *TAU-4M.IP*

1.3 Структура и принцип работы изделия

Абонентский терминал *TAU-4M.IP* состоит из следующих подсистем:

- контроллер, в состав которого входит:
  - высокоинтегрированная система на кристалле (System-on-a-Chip – SoC) Realtek RTL8972C, включающая в себя процессор, 100-мегабитный коммутатор со встроенными PHY, аппаратную акселерацию трафика L2/L3/L4, USB 2.0 порты, PCI-E контроллеры, 8 каналов PCM для работы приложений VoIP;
  - flash-память – 8MB;
  - оперативная память SDRAM – 128MB;
- 4 абонентских комплекта SLIC;
- 1 порт LAN: RJ-45 10/100BASE-T;
- Ethernet-модуль WAN: RJ-45 10/100BASE-T;
- USB Host-порт.

Структурная схема устройства приведена на рисунке 2.

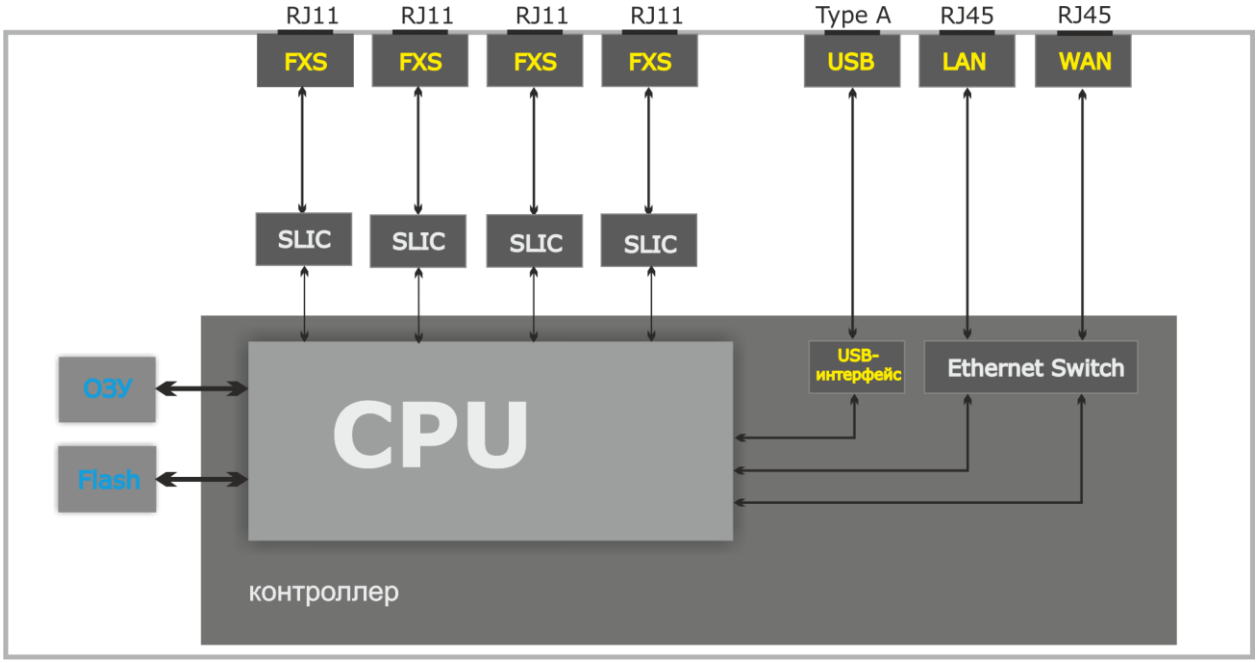


Рисунок 2 – Структурная схема TAU-4M.IP

Устройство работает под управлением операционной системы Linux. Основные функции управления сосредоточены в процессоре Realtek, который осуществляет маршрутизацию IP-пакетов, обеспечивает работу IP-телефонии, проксирование группового трафика и т.д.

Функционально устройство можно разделить на 4 блока:

- Блок поддержки сетевых функций устройства;
- Блок IP-телефонии;
- Блок обработки multicast-трафика;
- Блок управления (операционная система Linux).

Блок поддержки сетевых функций устройства обеспечивает прохождение и коммутацию IP-пакетов в соответствии с таблицей маршрутизации устройства, может обрабатывать как нетегированные, так и тегированные пакеты в зависимости от настройки сетевых интерфейсов. Поддерживает протоколы DHCP, PPPoE, PPTP, L2TP.

Блок IP-телефонии обеспечивает работу устройства по протоколу SIP для передачи речевых сигналов по сети с коммутацией пакетов. Речевой сигнал абонента поступает на модуль абонентских комплектов SLIC, где преобразовывается в цифровой вид. Оцифрованный сигнал направляется в блок IP-телефонии, где кодируется по одному из выбранных стандартов и в виде цифровых пакетов поступает в контроллер через внутрисистемную магистраль. Цифровые пакеты содержат, кроме речевых, сигналы управления и взаимодействия.

Блок обработки multicast-трафика предназначен для обработки IGMP-сообщений и multicast-трафика с целью поддержки функций IP-телевидения.

Блок управления на базе операционной системы Linux контролирует работу всех остальных блоков и подсистем устройства и обеспечивает их взаимодействие.

Функциональная схема устройства *TAU-4M.IP* представлена на рисунке 3.

Рисунок 3 – Функциональная схема устройства серии *TAU-4M.IP*

1.4 Основные технические параметры

Основные технические параметры устройства приведены в таблице 1.

Таблица 1 – Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP

Аудиокодеки

Кодеки	G.729, annex A, annex B G.711a, G.711u, G.723.1, G.722, G.726-24, G.726-32 Передача модема: G.711a, G.711u Передача факса: G.711a, G.711u, T.38

Параметры WAN-интерфейса Ethernet

Количество портов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100, автоопределение
Поддержка стандартов	BASE-T

Параметры LAN-интерфейса Ethernet

Количество интерфейсов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100, автоопределение
Поддержка стандартов	BASE-T

Параметры аналоговых абонентских портов

Количество портов	4
Сопротивление шлейфа (без учета сопротивления ТА)	до 800 Ом
Прием набора	импульсный/частотный (DTMF)
Защита абонентских окончаний	по току и по напряжению
Выдача Caller ID	FSK BELL202/FSK V.23/DTMF

Управление

Удаленное управление	Web-интерфейс, Telnet, SSH, SNMP, TR-069
Ограничение доступа	по паролю

Общие параметры

Питание	адаптер питания 12 В постоянного тока, 2 А.
Потребляемая мощность	не более 12,5 Вт (максимальный потребляемый ток 1,1 А)
Рабочий диапазон температур	от +5 до +40°С
Относительная влажность при температуре 25°С	до 80%
Габариты	187x120x32.5 мм
Масса	не более 0,25 кг

1.5 Конструктивное исполнение

Абонентский терминал *TAU-4M.IP* выполнен в пластиковом корпусе размерами 187x120x32,5 мм.

1.5.1 Верхняя панель устройства

Внешний вид верхней панели устройства *TAU-4M.IP* приведен на рисунке 4.

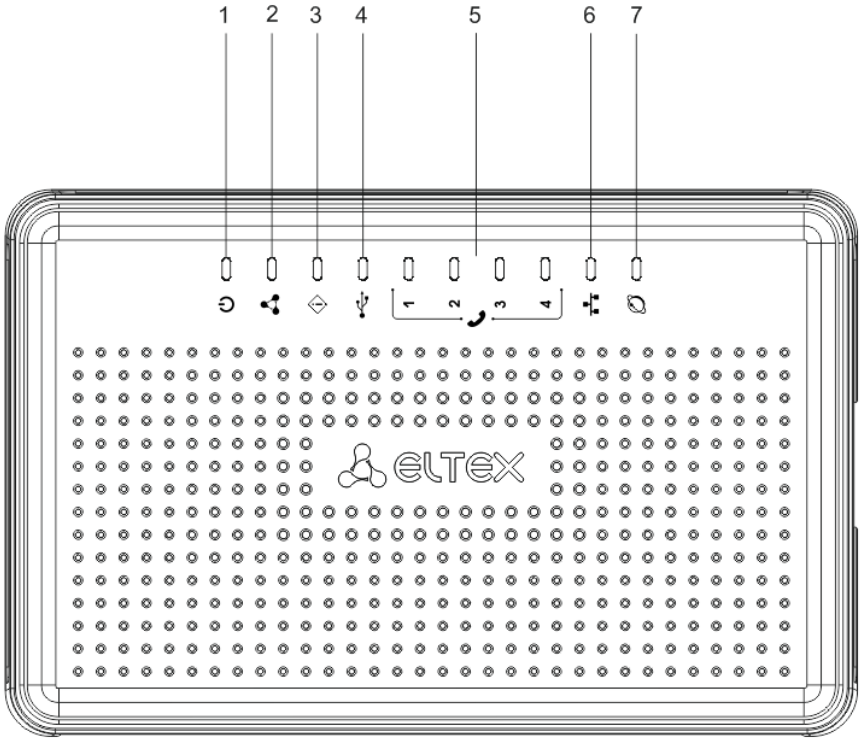


Рисунок 4 – Внешний вид верхней панели *TAU-4M.IP*

На верхней панели устройства *TAU-4M.IP* расположены следующие световые индикаторы:

Таблица 2 – Описание индикаторов и органов управления передней панели

Элемент передней панели		Описание
1	Power	индикатор питания и статуса работы устройства
2	Status	индикатор статуса работы устройства
3	Alarm	индикатор аварий на устройстве (неактивен в версиях ПО 2.3.0 и выше)
4	USB	индикатор работы внешнего USB-устройства (USB flash, внешний жесткий диск, 3G/4G USB-модем)
5		индикаторы работы аналоговых телефонных портов
6	LAN	индикатор LAN-интерфейса
7	WAN	индикатор WAN-интерфейса

1.5.2 Задняя панель устройства

Внешний вид задней панели устройства *TAU-4M.IP* приведен на рисунке 5.

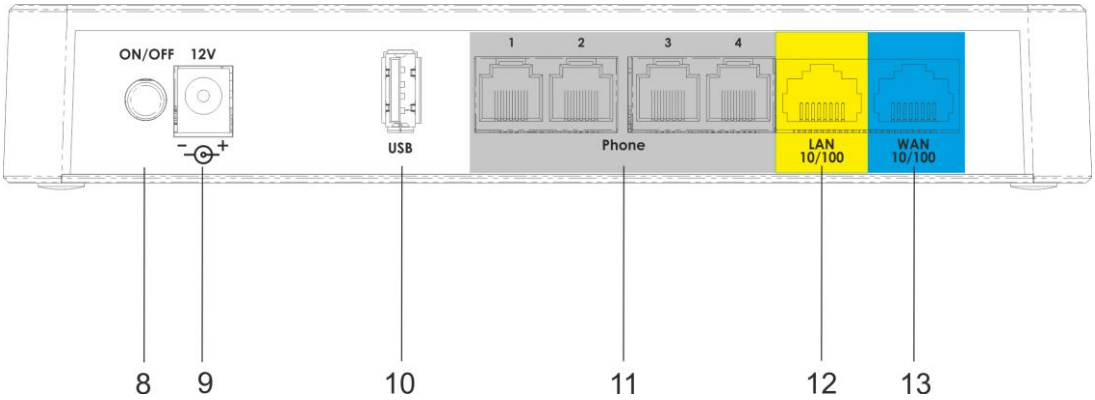


Рисунок 5 – Внешний вид задней панели *TAU-4M.IP*

На задней панели устройства *TAU-4M.IP* расположены разъемы и органы управления, представленные в таблице 3.

Таблица 3 – Описание индикаторов и органов управления задней панели *TAU-4M.IP*

Элемент задней панели		Описание
8	ON/OFF	тумблер включения/выключения устройства
9	12V	разъем для подключения адаптера питания
10	USB	разъем USB для подключения внешнего USB-устройства (USB flash, жесткий диск, 3G/4G USB-модем)
11	Phone	4 разъема RJ-11 для подключения аналоговых телефонных аппаратов
12	LAN	порт 10/100BASE-T Ethernet (разъем RJ-45) для подключения локального сетевого устройства
13	WAN	порт 10/100BASE-T (разъем RJ-45) для подключения к внешней сети

1.6 Световая индикация

Текущее состояние устройства *TAU-4M.IP* отображается при помощи индикаторов **WAN, LAN, Phone, Power** – расположенных на верхней панели. Перечень состояний индикаторов приведен в таблице 4.

Таблица 4 – Световая индикация состояния устройства серии *TAU-4M.IP*

Индикатор	Состояние индикатора	Состояние устройства
WAN	горит (зеленым – 10 Mbps, оранжевым – 100Mbps)	установлено соединение между станционным терминалом и абонентским устройством
	мигает	процесс пакетной передачи данных по WAN-интерфейсу
LAN	горит (зеленым – 10 Mbps, оранжевым – 100Mbps	установлено соединение с подключенным сетевым устройством
	мигает	процесс пакетной передачи данных по LAN-интерфейсу

	зеленый, горит постоянно	телефонная трубка поднята (линия активна)
	не горит	трубка положена, нормальная работа
	зеленый, в течение секунды мигает с частотой 20 Гц, затем 4 секунды пауза	на телефонный порт поступает входящий вызов
	зеленый, периодическое редкое мигание	отсутствует регистрация абонентского порта на SIP-прокси сервере
	зеленый, двойные короткие мигания с интервалом в 3 секунды	идет тест линии
USB	зеленый, горит	USB-устройство подключено
	не горит	USB-устройство не подключено
Alarm	не горит	недоступен в версиях ПО 2.3.0 и выше
Status	зеленый, горит постоянно	нормальная работа устройства
	оранжевый, горит постоянно	отсутствует выход в Интернет
	красный, горит постоянно	загрузка устройства
	периодическое попеременное мигание красным и зеленым цветами	сброс устройства к заводским настройкам
Power	красный	включено питание устройства

1.7 Сброс к заводским настройкам

Для запуска устройства с заводскими настройками необходимо в загруженном состоянии нажать и удерживать кнопку «F», которая находится на боковой панели устройства, пока индикатор «Power» начнет периодически мигать попеременно красным и зеленым цветами. Произойдет автоматическая перезагрузка устройства. При заводских установках на WAN-интерфейсе запущен DHCP-клиент, адрес интерфейса LAN - *192.168.1.1,* маска подсети – *255.255.255.0*; имя пользователя/пароль для доступа через Web-интерфейс: admin/password.

1.8 Комплект поставки

В базовый комплект поставки устройства серии *TAU-4M.IP* входят:

- терминал абонентский универсальный;
- адаптер питания 220/12В, 2 А;
- руководство по установке и настройке.

2 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

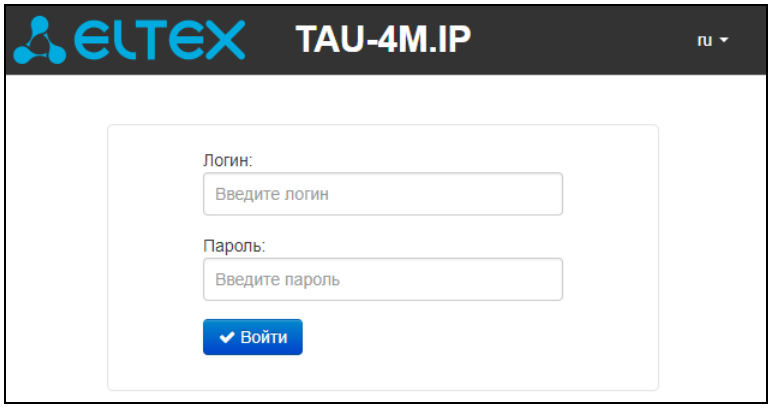
2.1 Начало работы

Для начала работы нужно подключиться к устройству по интерфейсу LAN через Web-браузер:

1. Откройте Web-браузер (программу-просмотрщик гипертекстовых документов), например, Firefox, Opera, Chrome.
2. Введите в адресной строке браузера IP-адрес устройства.

Заводской IP-адрес устройства: 192.168.1.1, маска подсети: 255.255.255.0

При успешном обнаружении устройства в окне браузера отобразится страница с запросом имени пользователя и пароля.



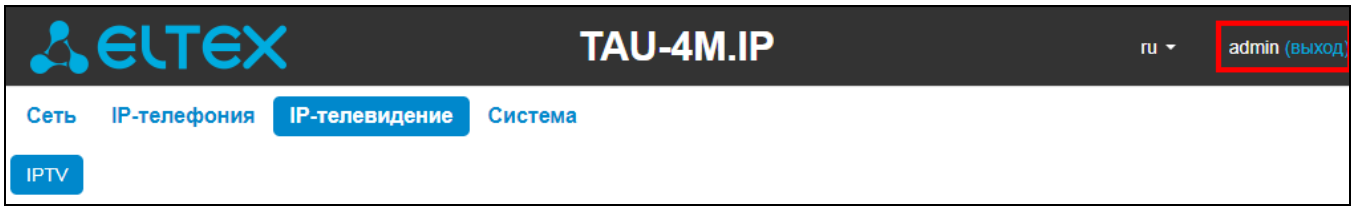
3. Введите имя пользователя в строке «Логин» и пароль в строке «Пароль».

Заводские установки: логин: *admin*, пароль: *password*.

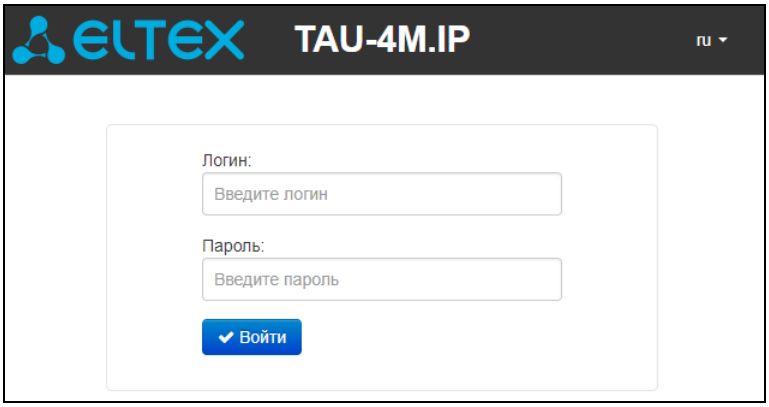
4. Нажмите кнопку «Войти». В окне браузера откроется меню быстрого конфигурирования, рисунок 6.

2.2 Смена пользователей

На устройстве существует три типа пользователей: **admin**, **user** и **viewer**. Пользователь **admin** (**администратор**, пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек, полный мониторинг состояния устройства. Пользователь **user** (**непривилегированный пользователь**, пароль по умолчанию: **user**) имеет возможность выполнить только настройку PPPoE для подключения к Интернет, не имеет доступа к мониторингу состояния устройства. Пользователь **viewer** (**наблюдатель**, пароль по умолчанию: viewer) имеет право только просматривать всю конфигурацию устройства без возможности что-либо редактировать, мониторинг состояния устройства ему доступен в полном объеме.



При нажатии на кнопку «*выход*» текущая сессия пользователя будет завершена, отобразится окно авторизации:



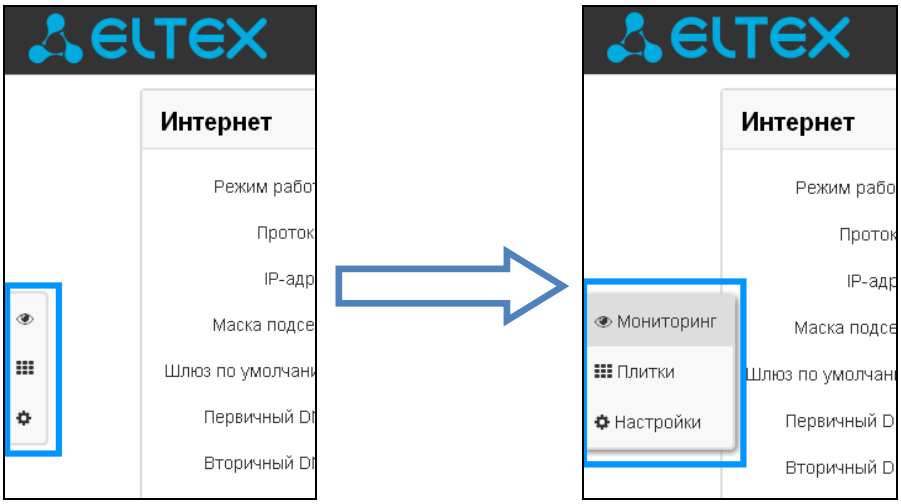
Для смены доступа необходимо указать соответствующие имя пользователя и пароль, нажать кнопку *«Войти».*

2.3 Режимы работы Web-интерфейса

Web-интерфейс устройства *TAU-4M.IP* может работать в трех режимах:

- **Мониторинг** – режим мониторинга системы – используется для просмотра различного рода информации, которая касается работы устройства: активность Интернет-соединения, состояние телефонного порта, объем принятых/переданных данных по сетевым интерфейсам и так далее;
- **Плитки** – режим быстрого конфигурирования системы – в каждой плитке сгруппированы настройки по их функциональному назначению: Интернет, IP-телефония, IP-телевидение и другие. В плитку выведены только основные параметры, позволяющие максимально быстро настроить определенную функцию устройства;
- **Настройки** – расширенный режим конфигурирования системы (режим полного конфигурирования) – позволяет выполнить полное конфигурирование устройства.

Для навигации между режимами Web-интерфейса служит панель, которая находится с левой стороны Web-интерфейса. При наведении указателя мыши панель раскрывается:



Из режима «Плитки» в режим «Настройки» переход возможен также через ссылку *«подробнее»* в названии плитки.

2.4 Применение конфигурации и отмена изменений

2.4.1 Применение конфигурации

По нажатию на кнопку «Применить» происходит сохранение конфигурации во flash-память устройства и применение новых настроек. Все настройки вступают в силу без перезагрузки устройства.

Кнопка «Применить» в меню быстрого конфигурирования и в меню расширенных настроек соответственно имеет вид: ; Применить.

В Web-интерфейсе реализована визуальная индикация текущего состояния процесса применения настроек, описанная в Таблица 5:

Таблица 5 – Визуальная индикация текущего состояния процесса применения настроек

Внешний вид	Описание состояния
Настройки сети	После нажатия на кнопку «Применить» происходит процесс применения и записи настроек в память устройства. Об этом информирует значок в названии вкладки и на кнопке «Применить».
Настройки сети	Об успешном сохранении и применении настроек информирует значок в названии вкладки.
Настройки сети	Если значение параметра было указано с ошибкой, то после нажатия на кнопку «Применить» появится соответствующее сообщение с указанием причины, а в названии вкладки отобразится значок .

2.4.2 Отмена изменений

Отмена изменений производится только до нажатия на кнопку «Применить». В этом случае отредактированные на странице параметры обновятся текущими значениями, записанными в памяти устройства. После нажатия на кнопку «Применить» возврат к предыдущим настройкам будет невозможен.

Кнопка отмены изменений в меню быстрого конфигурирования и в меню расширенных настроек соответственно имеет вид: ✖; ✖ Отмена.

2.5 Меню быстрого конфигурирования

В меню быстрого конфигурирования отображаются основные настройки устройства, Рисунок 6.

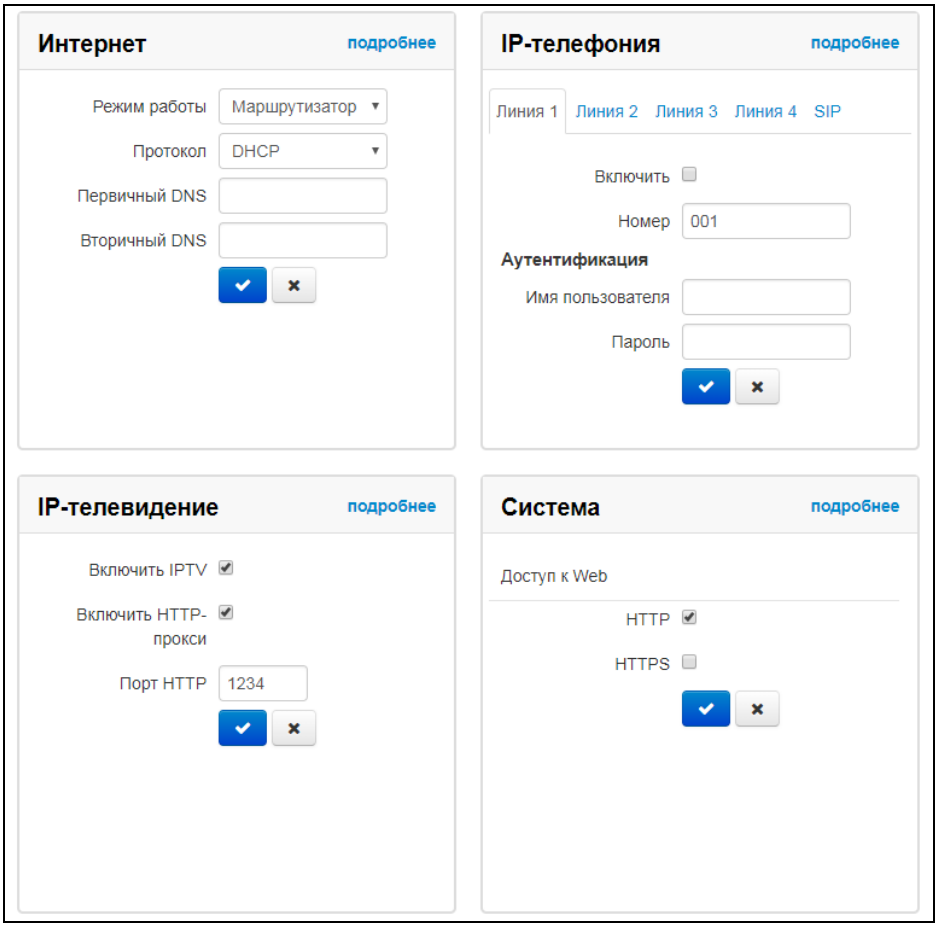


Рисунок 6 – Меню быстрого конфигурирования

Настройки разделены по следующим категориям:

- *Интернет* – быстрая настройка выхода в сеть Интернет;
- *IP-телефония* – быстрая настройка телефонии;
- *IP-телевидение* – конфигурирование устройства для поддержки функций IPTV;
- *Система* – настройка доступа к Web-интерфейсу через WAN-порт.

2.5.1 Интернет

Для доступа к сети Интернет необходимо установить основные настройки в разделе «Интернет». Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «*подробнее*».

- *Режим работы* – режим работы устройства:
  - *Маршрутизатор* – между LAN и WAN-интерфейсом устанавливается режим маршрутизатора (LAN изолирован от WAN);
  - *Мост* – между WAN и LAN-интерфейсом устанавливается режим моста: данные передаются прозрачно из LAN в WAN и обратно;

- *Протокол* – выбор протокола, по которому будет осуществляться подключение WAN-интерфейса устройства к сети провайдера:
  - *Static* – режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static» для редактирования будут доступны следующие параметры:
    - *Внешний IP-адрес* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
    - *Маска подсети* – маска внешней подсети;
    - *Шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
    - *Первичный DNS, Вторичный DNS* – адреса серверов доменных имён (используются для определения IP-адреса устройства по его доменному имени). Данные поля можно не заполнять, если в них нет необходимости.
  - *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от DHCP-сервера автоматически.

    Поддерживаемые опции:

    - 1 – маска сети;
    - 3 – адрес сетевого шлюза по умолчанию;
    - 6 – адрес DNS-сервера;
    - 12 – сетевое имя устройства;
    - 15 – доменное имя:
    - 26 – размер MTU;
    - 28 – широковещательный адрес сети;
    - 33 - статические маршруты;
    - 42 – адрес NTP-сервера;
    - 43 – специфичная информация производителя;
    - 60 – альтернативный Vendor ID;
    - 66 – адрес TFTP-сервера;
    - 67 – имя файла ПО (для загрузки по TFTP с сервера из опции 66);
    - 82 - информация агента DHCP Relay;
    - 120 – outbound SIP-сервера;
    - 121 – бесклассовые статические маршруты.

В DHCP-запросе в опции 60 устройство передает следующую информацию производителя в формате:

[VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**] [SN:**серийный номер**][WAN:**MAC- адрес интерфейса WAN**][LAN:**MAC- адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

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

Список используемых DHCP-опций на каждом сетевом интерфейсе (Internet, VoIP, Management) можно задавать вручную. Информация по настройке списка представлена в приложении В.

– *PPPoE* – режим работы, при котором на WAN-интерфейсе поднимается PPP-сессия. При выборе «PPPoE» для редактирования станут доступны следующие параметры:

· *Имя пользователя* – имя пользователя для авторизации на PPP-сервере;
· *Пароль* – пароль для авторизации на PPP-сервере;
· *Service-Name* – имя услуги – значение тега Service-Name в сообщении PADI для инициализации PPPoE-соединения (использование данной опции не является обязательным, этот параметр настраивается только по требованию провайдера);
· *Второй доступ* – тип доступа к локальным сетевым ресурсам. Можно выбрать 2 варианта:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
Static – статический – в этом случае необходимые для доступа параметры нужно указать вручную: *IP-адрес*, *Маска подсети, DNS-сервер, Шлюз.*

– *PPTP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол PPTP. При выборе «*PPTP*» для редактирования станут доступны следующие параметры:

· *PPTP-Сервер* – адрес сервера PPTP (доменное имя или IP-адрес в формате IPv4);
· *Имя пользователя* – имя пользователя для авторизации на PPTP-сервере;
· *Пароль* – пароль для авторизации на PPTP-сервере;
· *Второй доступ* – тип доступа к локальным сетевым ресурсам и PPTP-серверу. Можно выбрать 2 варианта:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
Static – статический, в этом случае необходимые для доступа к PPTP-серверу параметры задаются вручную:

▪ *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
▪ *Маска подсети* – при статическом доступе маска подсети;
▪ *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
▪ *Шлюз* – при статическом доступе шлюз для доступа к PPTP-серверу (если необходим).

– *L2TP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол L2TP. При выборе «*L2TP*» для редактирования станут доступны следующие параметры:

· *L2TP-сервер* – адрес сервера L2TP (доменное имя или IP-адрес в формате IPv4);

- *Имя пользователя* – имя пользователя для авторизации на L2TP-сервере;
- *Пароль* – пароль для авторизации на L2TP-сервере;
- *Второй доступ* – тип доступа к локальным сетевым ресурсам и L2TP-серверу. Можно выбрать 2 варианта:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
Static – статический, в этом случае необходимые для доступа к L2TP-серверу параметры задаются вручную:

- *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
- *Маска подсети* – при статическом доступе маска подсети;
- *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
- *Шлюз* – при статическом доступе шлюз для доступа к L2TP-серверу (если необходим).

Протоколы PPTP и L2TP используются для создания защищенного канала связи через Internet между компьютером удаленного пользователя и частной сетью его организации. PPTP и L2TP основываются на протоколе Point-to-Point Protocol (PPP) и являются его расширениями. Данные верхних уровней модели OSI сначала инкапсулируются в PPP, а затем в PPTP или L2TP для туннельной передачи через сети общего доступа. Функциональные возможности PPTP и L2TP различны. L2TP может использоваться не только в IP-сетях, служебные сообщения для создания туннеля и пересылки по нему данных используют одинаковый формат и протоколы. PPTP может применяться только в IP-сетях, и ему необходимо отдельное соединение TCP для создания и использования туннеля. L2TP поверх IPSec[1] предлагает больше уровней безопасности, чем PPTP, и имеет высокую степень защищенности важных для организации данных.

Особенности L2TP делают его очень перспективным протоколом для построения виртуальных сетей.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку . Для отмены изменений нажмите кнопку .

Чтобы подключить устройство к сети провайдера, необходимо уточнить у оператора сетевые настройки. При использовании статических настроек в поле «Протокол» нужно выбрать значение «Static», заполнить поля «Внешний IP-адрес», «Маска подсети», «Шлюз по умолчанию», «Первичный DNS» и «Вторичный DNS» предоставленными провайдером соответствующими значениями. Если устройства в сети провайдера получают сетевые настройки по протоколам DHCP, PPPoE, PPTP или L2TP – в поле «Протокол» выберите соответствующий протокол и воспользуйтесь инструкциями провайдера для полной и правильной настройки устройства.

2.5.2 IP-телефония

Для работы IP-телефонии необходимо установить настройки в разделе «IP-телефония». Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку *«подробнее»*.

Во вкладках «Линия 1», «Линия 2», «Линия 3», «Линия 4» выполняются основные настройки телефонных портов устройства «Phone1», «Phone2», «Phone3», «Phone4» соответственно:

- *Включить* – при установленном флаге данная линия активна;
- *Номер* – абонентский номер, закрепленный за телефонной линией;
- *Имя пользователя* – имя пользователя для аутентификации на SIP-сервере;
- *Пароль* – пароль для аутентификации на SIP-сервере.

[1] Для корректной работы IPSec следует отключить трансляцию адресов отправителя.

Во вкладке «SIP» выполняются основные настройки для SIP-прокси сервера:

- *SIP-прокси сервер* – сетевой адрес SIP-сервера – устройства, осуществляющего контроль доступа всех абонентов к телефонной сети провайдера. Можно указать как IP-адрес, так и доменное имя (через двоеточие можно задать альтернативный UDP-порт SIP-сервера, по умолчанию 5060);
- *Регистрация* – при установленном флаге разрешена регистрация абонентских портов на сервере регистрации;
- *Сервер регистрации* – сетевой адрес устройства, на котором осуществляется регистрация всех абонентов телефонной сети с целью предоставления им права пользоваться услугами связи (через двоеточие можно указать альтернативный порт сервера регистрации, по умолчанию 5060). Можно указать как IP-адрес, так и доменное имя. Обычно сервер регистрации физически совмещен с SIP-прокси сервером (они имеют одинаковый адрес);
- *SIP domain* – домен, в котором находится устройство (заполнять при необходимости), назначается автоматически из 15 опции протокола DHCP или задается вручную. Домен, заданный вручную имеет приоритет над настройкой, полученной по DHCP.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку . Для отмены изменений нажмите кнопку .

2.5.3 IP-телевидение

Для работы функции IPTV нужно выполнить основные настройки в разделе «IP-телевидение». Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку *«подробнее»*.

- *Включить IPTV* – при установленном флаге разрешена трансляция сигналов IP-телевидения с WAN-интерфейса *TAU-4M.IP* (из сети провайдера) на устройства, подключенные к LAN-интерфейсу;
- *Включить HTTP-прокси* – при установленном флаге использовать HTTP-прокси. HTTP-прокси осуществляет преобразование UDP-потока в поток HTTP, что позволяет улучшить качество транслируемого изображения при плохом качестве канала связи в локальной сети.
- *Порт HTTP* – номер порта HTTP-прокси, с которого будет осуществляться транслирование видео-потока. Используйте этот порт для подключения к транслируемым устройством потокам IPTV.

Например, если устройство имеет на LAN-интерфейсе адрес 192.168.0.1, для порта прокси-сервера выбрано значение 2345, и необходимо воспроизвести канал 227.50.50.100, транслирующийся на UDP-порт 1234 – для программы VLC адрес потока нужно задать в виде: http://@192.168.0.1:2345/udp/227.50.50.100:1234.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку . Для отмены изменений нажмите кнопку .

2.5.4 Система

В разделе «Система» выполняется настройка доступа к Web-конфигуратору устройства. Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку *«подробнее»*.

Доступ к Web через WAN:

- *HTTP* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через WAN-порт по протоколу HTTP (небезопасное подключение);
- *HTTPS* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через WAN-порт по протоколу HTTPS (безопасное подключение).

По умолчанию доступ к Web-интерфейсу устройства разрешен только через LAN-интерфейс.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку . Для отмены изменений нажмите кнопку .

2.6 Расширенные настройки

Для перехода в режим расширенных настроек устройства нажмите ссылку *«подробнее»* в названии любой плитки или выберите пункт «Настройки» на панели слева.

2.6.1 Основные элементы Web-интерфейса

На рисунке 7 представлены элементы навигации Web-конфигуратора в режиме расширенных настроек.

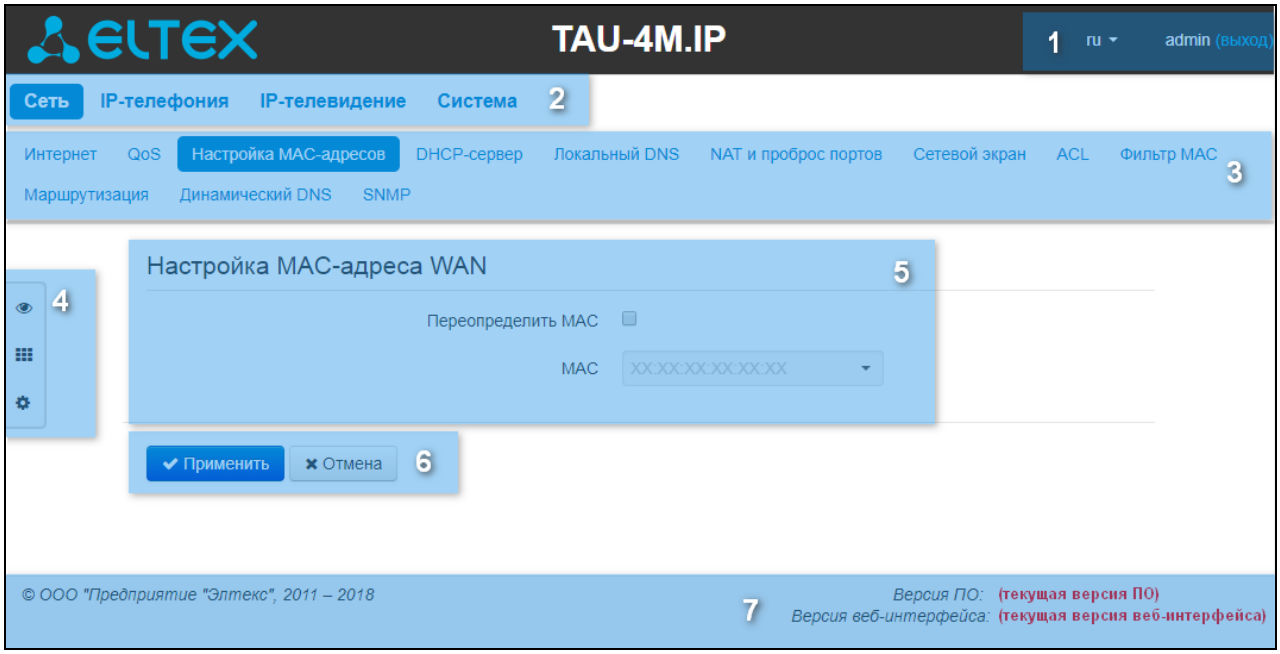


Рисунок 7 – Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса разделено на семь областей:

1 Имя пользователя, под которым был осуществлен вход в систему, кнопка завершения сеанса работы в Web-интерфейсе (*выход*) под данным пользователем и выпадающее меню выбора языка Web-интерфейса.

2 Вкладки меню группируют вкладки подменю по категориям: **Сеть**, **IP-телефония**, **IP-телевидение**, **Система**.

3 Вкладки подменю служат для управления полем настроек.

4 Панель смены режима Web-конфигуратора (описание в разделе 2.3).

5 Поле настроек устройства, которое базируется на выборе пользователя, предназначено для просмотра настроек устройства и ввода конфигурационных данных.

6 Кнопки управления конфигурацией, подробная информация приведена в разделе 2.4.

- *Применить* – применить и сохранить текущую конфигурацию в энергонезависимую память устройства;
- *Отмена* – отмена изменений (возможна только до нажатия на кнопку «*Применить*»).

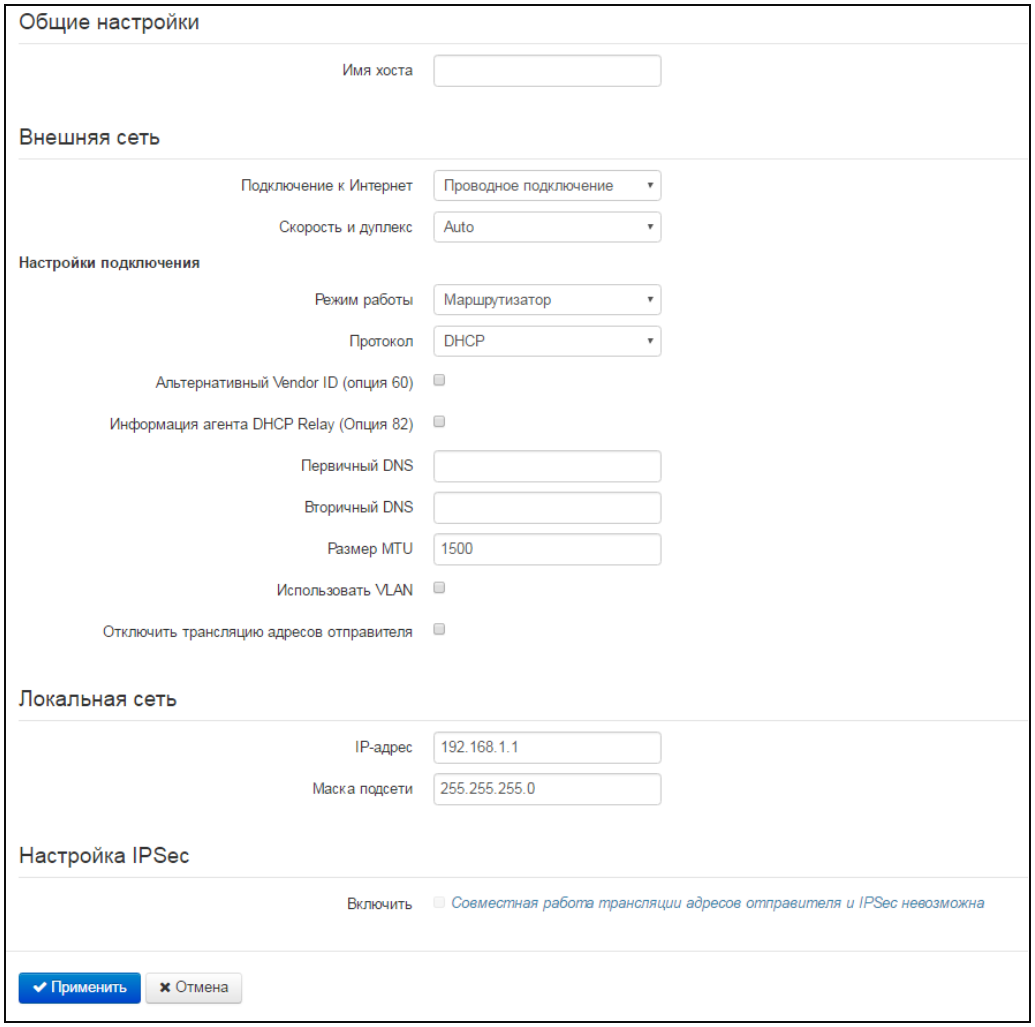
7 Информационное поле, в котором отображается версия программного обеспечения, версия Web-интерфейса.

2.6.2 Меню «Сеть»

В меню «Сеть» выполняется конфигурирование сетевых настроек устройства.

2.6.2.1 Подменю «Интернет»

В подменю «Интернет» выполняется конфигурирование внешней сети (по протоколам PPPoE, DHCP, PPTP, L2TP, статически, в режиме маршрутизатора и моста) и локальной сети.



Общие настройки

- Имя хоста – сетевое имя устройства.

Внешняя сеть

- *Подключение к Интернет* – способ подключения устройства к внешней сети:
  - *Проводное подключение* – подключение к сети Интернет осуществляется только по Ethernet-кабелю через порт WAN;
  - *3G/4G USB-модем* – подключение к сети Интернет осуществляется через беспроводной USB-модем 3G/4G (через сеть мобильной связи), подключенный к USB-порту устройства.
  - *Автоматически переходить на резервный канал* – подключение к сети Интернет осуществляется по основному каналу (задается ниже в поле «Основной канал»), и в случае пропадания доступа к Интернет по основному каналу будет произведен автоматический переход на резервный канал.
- Скорость и дуплекс – установка скорости передачи данных и режима работы дуплекса на Ethernet-порту WAN абонентского шлюза:
  - *Auto* – автоматическое согласование скорости и дуплекса;
  - *100 Half* – поддерживается скорость 100 Мбит/с с полудуплексный режимом;
  - *100 Full* – поддерживается скорость 100 Мбит/с с дуплексным режимом;
  - *10 Half* – поддерживается скорость 10 Мбит/с с полудуплексным режимом;
  - *10 Full* – поддерживается скорость 10 Мбит/с с дуплексным режимом.

Настройки подключения

При выборе способа подключения **«Проводное подключение»** будут доступны следующие настройки подключения:

- Режим работы – режим работы устройства:
  - *Маршрутизатор* – между LAN и WAN-интерфейсами устанавливается режим маршрутизатора (LAN изолирован от WAN);
  - *Мост* – между WAN и LAN-интерфейсами устанавливается режим моста: данные передаются прозрачно из LAN в WAN и обратно – фактически устройство работает в режиме коммутатора.

При выборе режима работы *«Маршрутизатор»* будут доступны следующие настройки подключения:

- *Протокол* – выбор протокола, по которому будет осуществляться подключение WAN-интерфейса устройства к сети предоставления услуг провайдера:
  - *Static* – режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:
    - *Внешний IP-адрес устройств* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
    - *Маска подсети* – маска внешней подсети;
    - *Шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;

- *Первичный DNS, Вторичный DNS* – адреса серверов доменных имён (используются для определения IP-адреса устройства по его доменному имени). Данные поля можно оставить пустыми, если в них нет необходимости.

– *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от DHCP-сервера автоматически.

Поддерживаемые опции:

- 1 – маска сети;
- 3 – адрес сетевого шлюза по умолчанию;
- 6 – адрес DNS-сервера;
- 12 – сетевое имя устройства;
- 15 – доменное имя;
- 26 – размер MTU;
- 28 – широковещательный адрес сети;
- 33 - статические маршруты;
- 42 – адрес NTP-сервера;
- 43 – специфичная информация производителя;
- 60 – альтернативный Vendor ID;
- 66 – адрес TFTP-сервера;
- 67 – имя файла ПО (для загрузки по TFTP с сервера из опции 66);
- 82 - информация агента DHCP Relay;
- 120 – outbound SIP-сервера;
- 121 – бесклассовые статические маршруты.

Для протокола DHCP имеется возможность задать необходимое значение опций 60 и 82.

- *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля *Vendor ID (опция 60).* При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.

Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат:
[VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**] [SN:**серийный номер**][WAN:**MAC-адрес интерфейса WAN**][LAN:**MAC-адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

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

- Информация агента DHCP Relay (опция 82) – при установленном флаге позволяет добавить в DHCP-запрос:

▪ *Идентификатор цепи агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 1 - Agent Circuit ID;
▪ *Идентификатор удаленного агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 2 - Agent Remote ID.

Список используемых DHCP-опций на каждом сетевом интерфейсе (Internet, VoIP, Management) можно задавать вручную. Информация по настройке списка представлена в приложении B.

- *Первичный DNS*, *Вторичный DNS* – IP-адреса DNS-серверов – если адреса DNS-серверов не назначаются автоматически по протоколу DHCP, при необходимости задайте их вручную. Адреса, заданные вручную, будут иметь приоритет над адресами DNS-серверов, полученными по протоколу DHCP.

– *PPPoE* – режим работы, при котором на WAN-интерфейсе поднимается PPP-сессия. При выборе «PPPoE» для редактирования станут доступны следующие параметры:

- *Имя пользователя* – имя пользователя для авторизации на PPP-сервере;
- *Пароль* – пароль для авторизации;
- *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1492);
- *Service-Name* – имя услуги – значение тега Service-Name в сообщении PADI (поле не обязательно для заполнения);
- *Тип соединения* – в зависимости от выбранного значения PPPoE-сессия поднята всегда (*AlwaysOn*), инициируется при необходимости передачи трафика (*OnDemand*) или инициируется и терминируется вручную при помощи кнопок «*Включить туннель/Выключить туннель*» (*Manual*);
- *Таймаут неактивности, с* – промежуток времени, по истечении которого происходит разрыв PPPoE-сессии по неактивности в режиме *OnDemand*;
- *LCP echo интервал, с* – период отправки LCP-запросов;
- *Количество ошибок LCP echo* – количество неотвеченных LCP-запросов, после которых происходит разрыв PPPoE-сессии;
- *Второй доступ* – тип доступа к локальным сетевым ресурсам. Можно выбрать один из двух вариантов:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры назначаются по протоколу DHCP;
Static – статический – в этом случае необходимые для доступа параметры задаются вручную: *IP-адрес*, *Маска подсети, DNS-сервер, Шлюз;*

- *Использовать второй доступ для VoIP* – опция доступна, если для сервиса IP-телефонии не настроен выделенный интерфейс (установлен флаг *«Использовать настройки Internet»*). При снятом флаге (по умолчанию) сервис IP-телефонии использует для своей работы интерфейс PPP, при установленном – интерфейс второго доступа (IPoE);
- *Аппаратное ускорение трафика* – в зависимости от выбранного значения достигается увеличение пропускной способности устройства при передаче трафика PPP (при выборе *PPP*) или IPoE (при выборе *Ethernet*).

– *PPTP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол PPTP. При выборе «*PPTP*» для редактирования станут доступны следующие параметры:

- *PPTP-сервер* – IP-адрес сервера PPTP;
- *Имя пользователя* – имя пользователя для авторизации на PPTP-сервере;
- *Пароль* – пароль для авторизации на PPTP-сервере;
- *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1462);
- *Тип соединения* – в зависимости от выбранного значения PPTP-сессия поднята всегда (*AlwaysOn*), инициируется при необходимости передачи трафика (*OnDemand*) или инициируется и терминируется вручную при помощи кнопок «*Включить туннель/Выключить туннель*» (*Manual*);

- *Таймаут неактивности, с* – промежуток времени, по истечении которого происходит разрыв PPTP-сессии по неактивности в режиме *OnDemand*;
- *LCP echo интервал, с* – период отправки LCP-запросов;
- *Количество ошибок LCP echo* – количество неотвеченных LCP-запросов, после которых происходит разрыв PPTP-сессии;
- *Второй доступ* – тип доступа к локальным сетевым ресурсам и PPTP-серверу. Можно выбрать один из двух вариантов:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры назначаются по протоколу DHCP;
Static – статический, в этом случае необходимые для доступа к PPTP-серверу параметры задаются вручную:

- *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
- *Маска подсети* – при статическом доступе маска подсети;
- *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
- *Шлюз* – при статическом доступе шлюз для доступа к PPTP-серверу (если необходим).

- *Использовать второй доступ для VoIP* – опция доступна, если для сервиса IP-телефонии не настроен выделенный интерфейс (установлен флаг *«Использовать настройки Internet»*). При снятом флаге (по умолчанию) сервис IP-телефонии использует для своей работы интерфейс PPP, при установленном – интерфейс второго доступа (IPoE).

Аппаратное ускорение трафика работает только для интерфейса второго доступа (IPoE).

– *L2TP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол L2TP. При выборе «*L2TP*» для редактирования станут доступны следующие параметры:

- *L2TP-сервер* – IP-адрес сервера L2TP;
- *Имя пользователя* – имя пользователя для авторизации на L2TP-сервере;
- *Пароль* – пароль для авторизации на L2TP-сервере;
- *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1462);
- *Тип соединения* – в зависимости от выбранного значения PPTP-сессия поднята всегда (*AlwaysOn*), инициируется при необходимости передачи трафика (*OnDemand*) или инициируется и терминируется вручную при помощи кнопок «*Включить туннель/Выключить туннель*» (*Manual*);
- *Таймаут неактивности, с* – промежуток времени, по истечении которого происходит разрыв L2TP-сессии по неактивности в режиме *OnDemand*;
- *LCP echo интервал, с* – период отправки LCP-запросов;
- *Количество ошибок LCP echo* – количество неотвеченных LCP-запросов, после которых происходит разрыв L2TP-сессии;
- *Второй доступ* – тип доступа к локальный сетевым ресурсам и L2TP-серверу. Можно выбрать один из двух вариантов:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры назначаются по протоколу DHCP;
Static – статический, в этом случае необходимые для доступа к L2TP-серверу параметры задаются вручную:

- *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
- *Маска подсети* – при статическом доступе маска подсети;
- *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
- *Шлюз* – при статическом доступе шлюз для доступа к L2TP-серверу (если необходим);

- *Использовать второй доступ для VoIP* – опция доступна, если для сервиса IP-телефонии не настроен выделенный интерфейс (установлен флаг *«Использовать настройки Internet»*). При снятом флаге (по умолчанию) сервис IP-телефонии использует для своей работы интерфейс PPP, при установленном – интерфейс второго доступа (IPoE).

  Аппаратное ускорение трафика работает только для интерфейса второго доступа (IPoE).

Протоколы PPTP и L2TP используются для создания защищенного канала связи через Internet между компьютером удаленного пользователя и частной сетью его организации. PPTP и L2TP основываются на протоколе Point-to-Point Protocol (PPP) и являются его расширениями. Данные верхних уровней модели OSI сначала инкапсулируются в PPP, а затем в PPTP или L2TP для туннельной передачи через сети общего доступа. Функциональные возможности PPTP и L2TP различны. L2TP может использоваться не только в IP-сетях, служебные сообщения для создания туннеля и пересылки по нему данных используют одинаковый формат и протоколы. PPTP может применяться только в IP-сетях, и ему необходимо отдельное соединение TCP для создания и использования туннеля.

L2TP поверх IPSec[2] предлагает больше уровней безопасности, чем PPTP, и гарантировать высокую степень безопасность важных для организации данных. Особенности L2TP делают его очень перспективным протоколом для построения виртуальных сетей.

Использовать VLAN во внешней сети – при установленном флаге использовать для выхода в Интернет идентификатор VLAN, указанный в поле «VLAN ID».

- *VLAN ID* – идентификатор VLAN, используемый для данной услуги;
- *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).

VLAN – виртуальная локальная сеть. Представляет собой группу хостов, объединенных в одну сеть независимо от их физического местонахождения. Устройства, сгруппированные в одну виртуальную сеть VLAN, имеют одинаковый идентификатор VLAN-ID.

- *Отключить трансляцию адресов отправителя* – при установленном флаге отключена подмена адреса источника отправителя пакета из локальной подсети (отключение masquerading).

При выборе режима работы *«Мост»* будут доступны следующие настройки подключения:

- *Протокол* – выбор протокола, по которому будет осуществляться подключение WAN-интерфейса устройства к сети предоставления услуг провайдера:
  - *Static* – режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:
    - *IP-адрес* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
    - *Маска подсети* – маска внешней подсети;
    - *Шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
    - *Первичный DNS, Вторичный DNS* – адреса серверов доменных имён (используются для определения IP-адреса устройства по его доменному имени). Данные поля можно оставить пустыми, если в них нет необходимости.

[2] Для корректной работы IPSec следует отключить трансляцию адресов отправителя.

– *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, назначаются по протоколу DHCP;

· *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля *Vendor ID (опция 60).* При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.

Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат:
[VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**] [SN:**серийный номер**][WAN:**MAC-адрес интерфейса WAN**][LAN:**MAC-адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

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

· Информация агента DHCP Relay (опция 82) – при установленном флаге позволяет добавить в DHCP-запрос:

- *Идентификатор цепи агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 1 - Agent Circuit ID;
- *Идентификатор удаленного агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 2 - Agent Remote ID.

Список используемых DHCP-опций на каждом сетевом интерфейсе (Internet, VoIP, Management) можно задавать вручную. Информация по настройке списка представлена в приложении B.

Первичный DNS, *Вторичный DNS* – IP-адреса DNS-серверов – если адреса DNS-серверов не назначаются автоматически по протоколу DHCP, при необходимости задайте их вручную. Адреса, заданные вручную, будут иметь приоритет над адресами DNS-серверов, полученными по протоколу DHCP.

- *PPPoE* – режим работы, при котором на WAN-интерфейсе поднимается PPP-сессия. При выборе «PPPoE» для редактирования станут доступны следующие параметры:

· *Имя пользователя* – имя пользователя для авторизации на PPP-сервере;
· *Пароль* – пароль для авторизации;
· *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1492);
· *Service-Name* – имя услуги – значение тега Service-Name в сообщении PADI (поле не обязательно для заполнения);
· *LCP echo интервал, с* – период отправки LCP-запросов;
· *Количество ошибок LCP echo* – количество неотвеченных LCP-запросов, после которых происходит разрыв PPPoE-сессии;

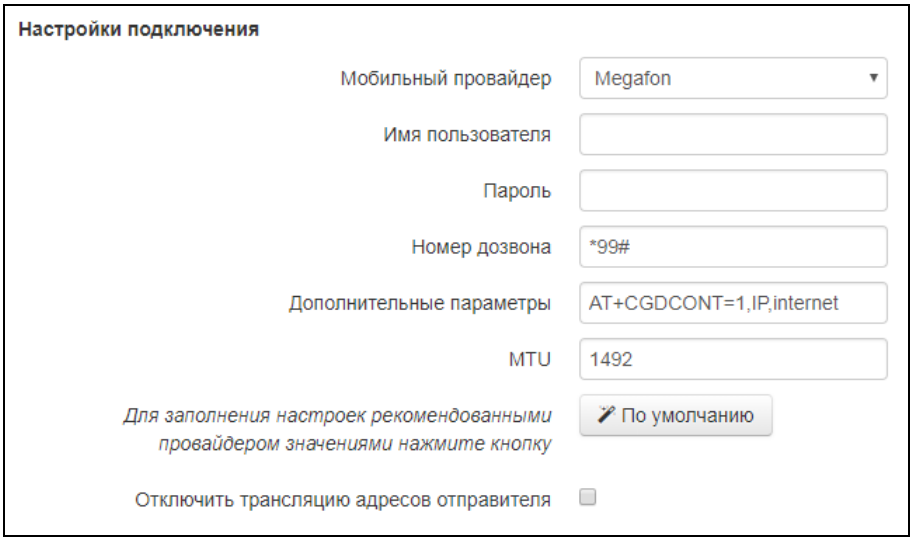
При выборе PPPoE в режиме моста тип соединения всегда будет AlwaysOn.

· *Второй доступ* – тип доступа к локальным сетевым ресурсам. Можно выбрать один из двух вариантов:

– *DHCP* – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
– *Static* – статический – в этом случае необходимые для доступа параметры задаются вручную:

  - *IP-адрес* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
  - *Маска подсети* – маска внешней подсети;
  - Шлюз по умолчанию – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
  - *Первичный DNS, Вторичный DNS* – адреса серверов доменных имён (используются для определения IP-адреса устройства по его доменному имени). Данные поля можно оставить пустыми, если в них нет необходимости.

При выборе способа подключения **«3G/4G USB-модем»** для настройки будут доступны следующие поля:



- *Мобильный провайдер* – имя провайдера, предоставляющего доступ к сети 3G/4G. Из списка Вы можете выбрать одного из шести мобильных операторов (настройки каждого из них хранятся в памяти устройства), присутствующих на территории Российской Федерации: Мегафон, Билайн, МТС, Скайлинк, Теле2, Yota. При нажатии на кнопку «По умолчанию» произойдёт заполнение настроек подключения параметрами выбранного провайдера. Если настройки провайдера в Вашем регионе отличаются от предложенных, отредактируйте их в соответствии с необходимыми значениями.

Если Вашего провайдера нет в списке – выберите значение «Другой» и заполните все поля в соответствии с настройками Вашего провайдера;

- *Протокол* – поле доступно только при выборе значения «Другой» из списка мобильных провайдеров. В большинстве случаев мобильные операторы используют протокол PPPoE для доступа к своей сети, однако для работы с модемами некоторых провайдеров может потребоваться выбор протокола DHCP;

- *Имя пользователя* – имя пользователя для идентификации при подключении к беспроводной сети;

- *Пароль* – пароль для идентификации при подключении к беспроводной сети;

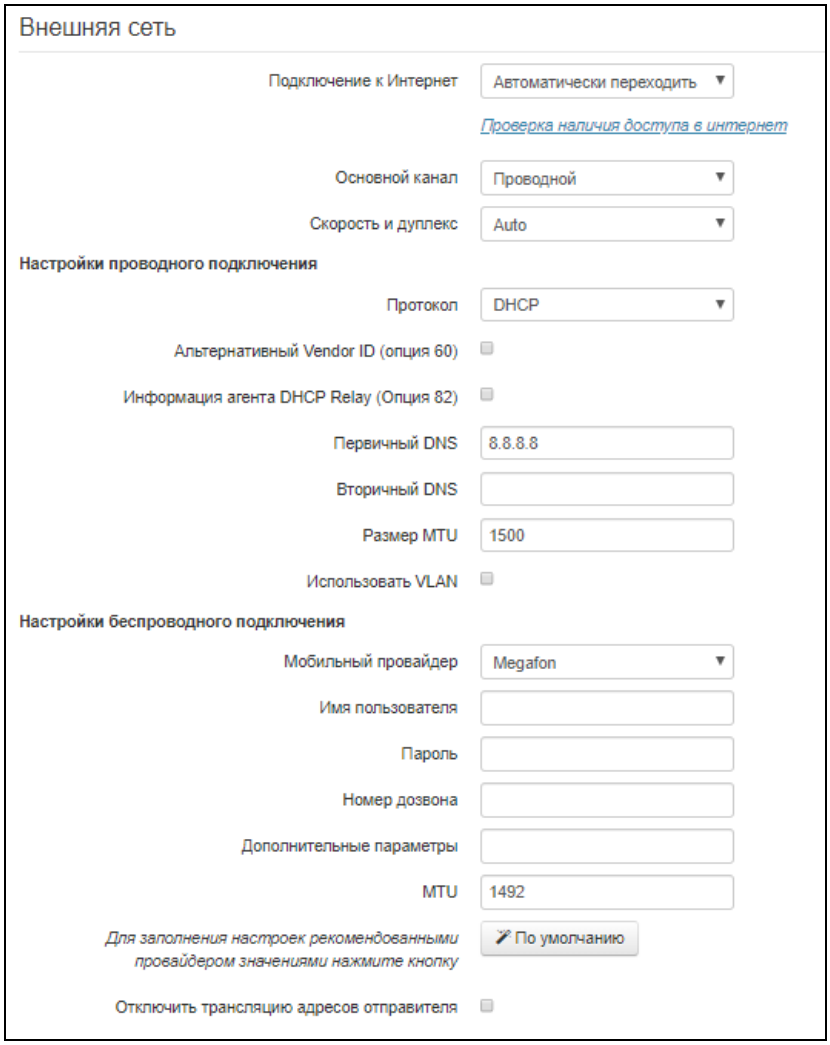
- *Номер дозвона* – номер дозвона для подключения к беспроводной сети (пример: *99***1#);

- *Дополнительные параметры* – параметры для подключения к сети мобильной связи (пример: AT+CGDCONT=1,IP,internet – для Мегафон); в данной строке нельзя использовать кавычки;

- *MTU* – максимальный размер блока данных, передаваемых по сети, рекомендуемое значение – 1492.

Кнопка *«По умолчанию»* предназначена для заполнения настроек провайдера заранее предустановленными значениями, хранимыми в памяти устройства, тем самым избавляя пользователя от необходимости искать эти настройки в Интернете.

При выборе способа подключения **«Автоматически переходить на резервный канал»** будут доступны следующие настройки:



- *Основной канал (Preferred channel)* – из выпадающего списка нужно выбрать тип основного канала:

  – *Проводной (Wired)* – канал через Ethernet WAN порт устройства.

  – *Беспроводной (Wireless)* – канал через сеть мобильной связи посредством беспроводного USB-модема.

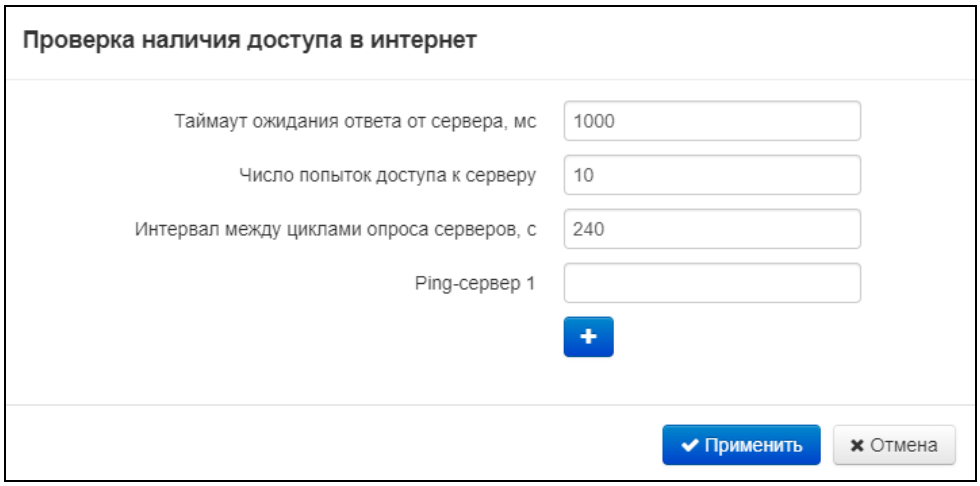
Настройки проводного подключения:

Настройки идентичны настройкам для способа подключения **«Проводное подключение»** с выбранным режимом **«Маршрутизатор»**.

Настройки беспроводного подключения:

Настройки идентичны настройкам для способа подключения **«3G/4G USB-модем».**

Проверка наличия доступа в интернет:



- *Таймаут ожидания ответа от сервера, с* – время, в течение которого ожидается ответ от PING-сервера;
- *Число попыток доступа к серверу, с* – максимальное число попыток доступа к PING-серверу, после чего будет принято решение о переходе на резервный канал;
- *Интервал между циклами опроса серверов, с* – промежуток времени, по истечении которого начинается новый цикл опроса PING-серверов.
- *Ping-сервер 1..5* – IP-адрес или доменное имя PING-сервера. Поля для ввода PING-серверов 2..5 появляются после заполнения предыдущего поля.

Локальная сеть:

- *IP-адрес устройства* – IP-адрес устройства в локальной сети;
- *Маска подсети* – маска подсети в локальной сети.
- *Отключить трансляцию адресов отправителя* – при установленном флаге отключена подмена адреса источника отправителя пакета из локальной подсети (отключение masquerading).

Настройка локальной сети в режиме работы устройства «Мост» недоступна.

При изменении адреса локальной подсети происходит автоматическая смена пула адресов локального DHCP-сервера (Сеть – DHCP-сервер).

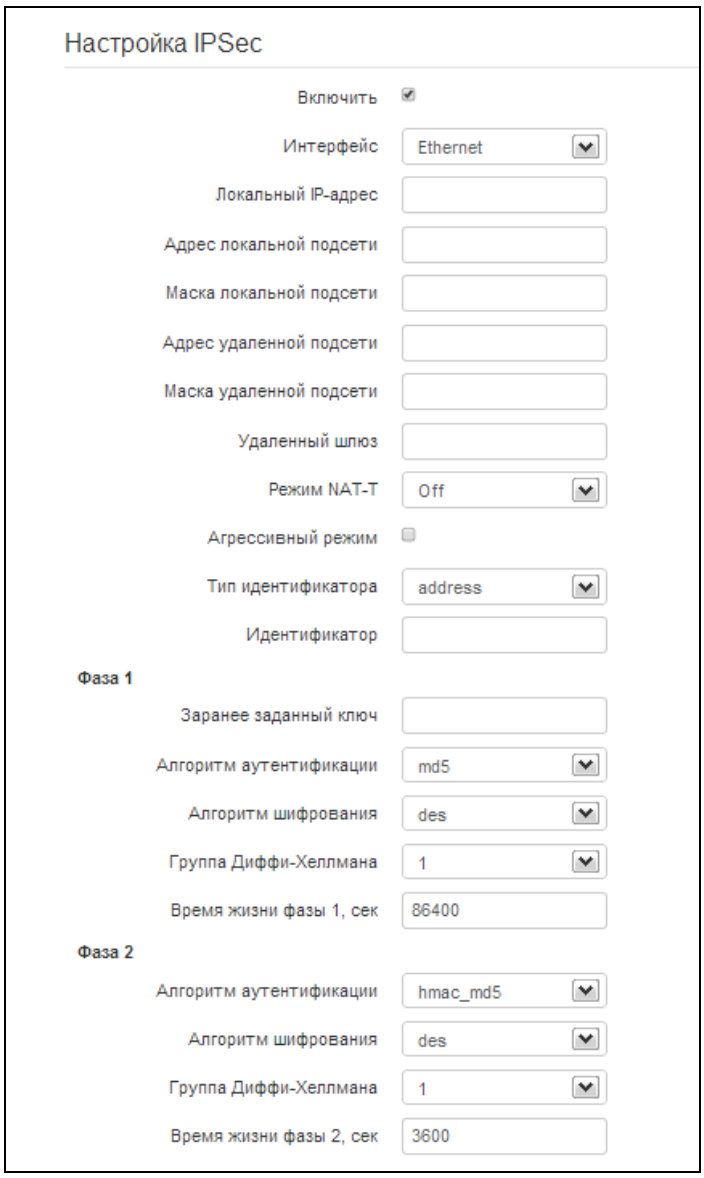
Настройка IPSec:

В данном разделе осуществляется настройка шифрования по технологии IPSec (IP Security).

IPSec – это набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяющий осуществлять подтверждение подлинности (аутентификацию), проверку

целостности и/или шифрование IP-пакетов. IPSec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

В текущей версии программного обеспечения посредством IPSec можно осуществлять только доступ к интерфейсам управления устройством (Web, Telnet, SSH).



- *Включить* – разрешить использование протокола IPSec для шифрования данных;
- *Интерфейс* – настройка имеет силу только при выборе для Интернета протоколов PPPoE, PPTP или L2TP и определяет, для доступа по какому интерфейсу использовать IPSec: Ethernet (интерфейс второго доступа) или PPP (интерфейс первого доступа). При выборе протоколов DHCP или Static в услуге активен только один интерфейс (Ethernet), по которому возможен доступ только посредством IPSec;
- *Локальный IP-адрес* – адрес устройства для работы по протоколу IPSec;
- *Адрес локальной подсети* совместно с *Маской локальной подсети* определяют локальную подсеть для создания топологий сеть-сеть или сеть-точка;
- *Адрес удаленной подсети* совместно с *Маской удаленной подсети* определяют адрес удаленной подсети для связи с использованием шифрования по протоколу IPSec. Если маска имеет значение 255.255.255.255 – связь осуществляется с единственным хостом. Маска,

отличная от 255.255.255.255, позволяет задать целую подсеть. Таким образом, функциональные возможности устройства позволяют организовать 4 топологии сети с использованием шифрования трафика по протоколу IPSec: точка-точка, сеть-точка, точка-сеть, сеть-сеть;

- *Удаленный шлюз* – шлюз, через который осуществляется доступ к удаленной подсети;
- *Режим NAT-T* – выбор режима NAT-T. NAT-T (NAT Traversal) инкапсулирует трафик IPSec и одновременно создает пакеты UDP, которые устройство NAT корректно пересылает. Для этого NAT-T помещает дополнительный заголовок UDP перед пакетом IPSec, чтобы он во всей сети обрабатывался как обычный пакет UDP, и хост получателя не проводил никаких проверок целостности. После поступления пакета к месту назначения заголовок UDP удаляется, и пакет данных продолжает свой дальнейший путь как инкапсулированный пакет IPSec. С помощью техники NAT-T возможно установление связи между клиентами IPSec в защищённых сетях и общедоступными хостами IPSec через межсетевые экраны. Режимы работы NAT-T:
  - *On* – режим NAT-T активируется только при обнаружении NAT на пути к хосту назначения;
  - *Force* – в любом случае использовать NAT-T;
  - *Off* – не использовать NAT-T при установлении соединения.

  Доступны следующие настройки NAT-T:

  - *UDP-порт NAT-T* – UDP-порт пакетов, в которые осуществляется инкапсуляция сообщений IPSec. По умолчанию 4500.
  - *Интервал отправки пакетов NAT-T keepalive, сек* – интервал отправки периодических сообщений для поддержания активного состояния UDP-соединения на устройстве, выполняющего функции NAT.
- *Агрессивный режим* – режим работы на фазе 1, когда обмен всей необходимой информацией осуществляется тремя нешифрованными пакетами. В стандартном режиме (main mode) обмен осуществляется шестью нешифрованными пакетами;
- *Тип идентификатора* – тип идентификатора устройства: address, fqdn, keyed, user_fqdn, asn1dn;
- *Идентификатор* – идентификатор устройства, используемый для идентификации на фазе 1 (заполнять при необходимости). Формат идентификатора зависит от типа.

Фаза 1. На первом этапе (фазе) два узла «договариваются» о методе идентификации, алгоритме шифрования, хеш-алгоритме и группе Diffie Hellman. Они также идентифицируют друг друга. Для фазы 1 имеются следующие настройки:

- *Заранее заданный ключ* – секретный ключ, используемый в алгоритме аутентификации на фазе 1. Представляет собой строку от 8 до 63 символов;
- *Алгоритм аутентификации* – выбор одного из списка алгоритмов аутентификации: MD5, SHA1;
- *Алгоритм шифрования* – выбор одного из списка алгоритмов шифрования: DES, 3DES, Blowfish;
- *Группа Диффи-Хеллмана* – выбор группы Diffie-Hellman;

- *Время жизни фазы 1, сек* – время, по истечении которого узлам необходимо переидентифицировать друг друга и сравнить политику (другое название IKE SA lifetime). По умолчанию 24 часа (86400 секунд).

Фаза 2. На втором этапе генерируются данные ключей, узлы «договариваются» об используемой политике. Этот режим, также называемый быстрым режимом (quick mode), отличается от первой фазы тем, что может установиться только после первого этапа, когда все пакеты второй фазы шифруются.

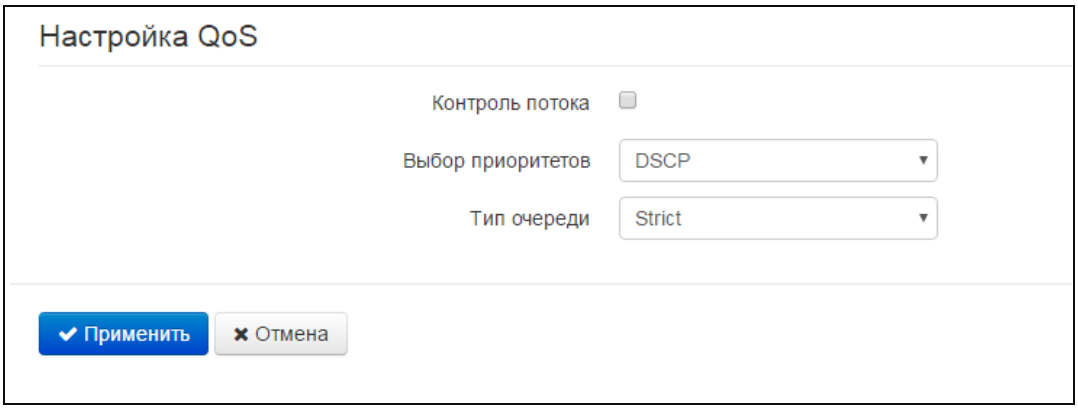
- *Алгоритм аутентификации* – выбор одного из списка алгоритмов аутентификации: HMAC - MD5, HMAC-SHA1, DES, 3DES;
- *Алгоритм шифрования* – выбор одного из списка алгоритмов шифрования: DES, 3DES, Blowfish;
- *Группа Диффи-Хеллмана* – выбор группы Diffie-Hellman;
- *Время жизни фазы 2, сек* – время, через которое происходит смена ключа шифрования данных (другое название IPSec SA lifetime). По умолчанию 60 минут (3600 секунд).

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

Данная реализация IPSec работает только при отключенной трансляции адресов отправителя, так как IP-адрес клиента участвует в формировании шифра.

2.6.2.2 Подменю «QoS»

В подменю «QoS» осуществляется настройка приоритетов обработки трафика и типа очередей.



Настройка QoS

- *Контроль потока* – включение/выключение механизма управления потоком передачи данных по протоколу TCP;
- *Выбор приоритетов* – выбор способа приоритизации трафика:
  - *DSCP* – механизм классификации, управления трафиком и обеспечения качества обслуживания посредством приоритетов;

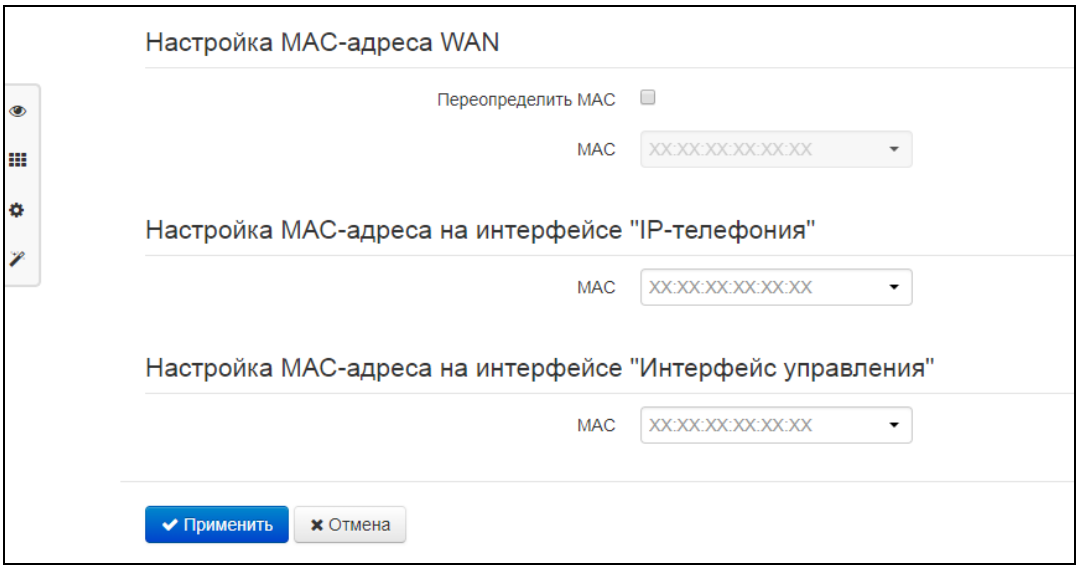
– *802.1p* – признак (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).

При включенном контроле потока настройки приоритетов недоступны.

- *Тип очереди* – выбор дисциплины обслуживания очередей:
  - *Strict* – дисциплина обслуживания очередей, при которой трафик с более низким приоритетом передается, только когда уже передана очередь с более высоким приоритетом;
  - *WRQ* – дисциплина обслуживания очередей, при которой доступная полоса пропускания делится между очередями пропорционально приоритету.
    - *Приоритет 0..5* – определяется вес приоритета в диапазоне от 1 до 127, чем выше вес, тем приоритетнее трафик.

2.6.2.3 Подменю «Настройка MAC-адресов»

В подменю «Настройка MAC-адресов» можно изменить MAC-адрес WAN-интерфейса устройства.



- *Переопределить MAC* – при установленном флаге на интерфейсе Интернет используется MAC-адрес из поля *MAC*.

При нажатии на кнопку выпадающего меню в поле «*MAC*» *возможно* записать MAC-адрес компьютера, с которого Вы подключены к Web-конфигуратору. Эта функция будет полезна, если на сети вашего Интернет-провайдера используется привязка по MAC-адресу. В этом случае, если Вам необходимо использовать устройство *TAU-4M.IP* в качестве маршрутизатора, на WAN-интерфейс устройства необходимо назначить MAC-адрес Вашего компьютера (который ранее был подключен к сети Интернет).

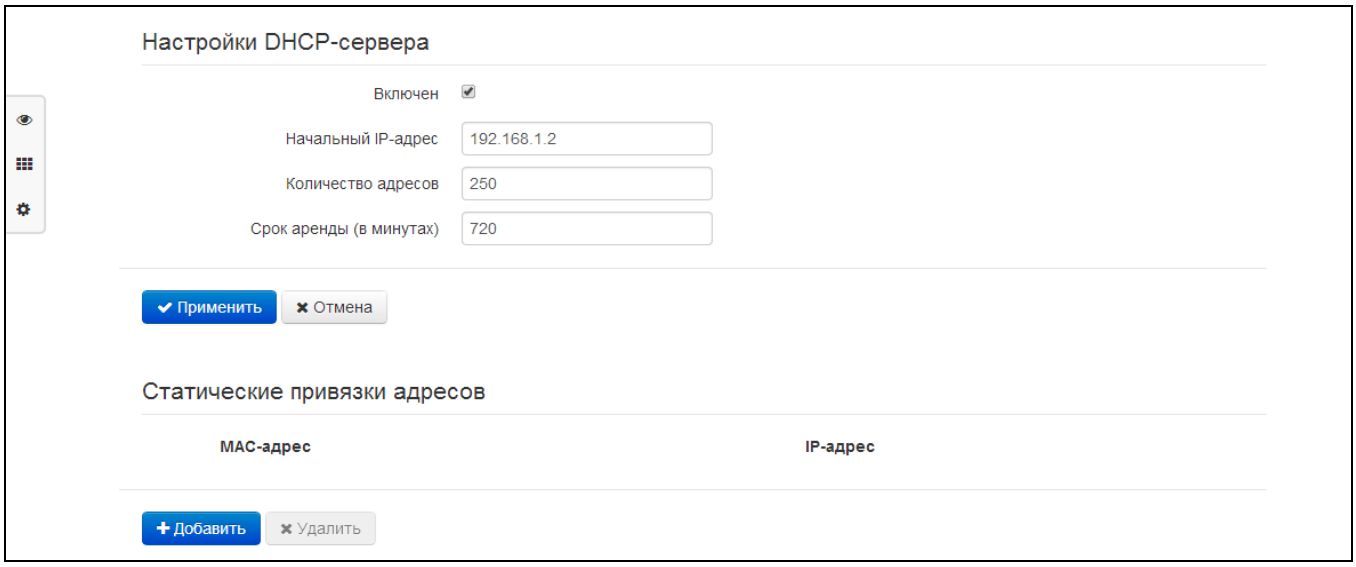
Для переопределения MAC на интерфейсе «IP-телефония» или «Интерфейс управления» воспользуйтесь разделами «Настройка MAC-адреса на интерфейсе "*IP-телефония*"» или «Настройка MAC-адреса на интерфейсе "*Интерфейс управления*"».

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.2.4 Подменю «DHCP-сервер»

В подменю «DHCP-сервер» выполняются настройки локального DHCP-сервера, устанавливаются статические привязки адресов.

Устройство *TAU-4M.IP* имеет возможность посредством протокола динамического конфигурирования (DHCP – Dynamic Host Configuration Protocol) автоматически назначать IP-адреса и необходимые для выхода в Интернет параметры компьютерам, подключенным к LAN-интерфейсу. Его использование позволяет избежать ограничений ручной настройки протокола TCP/IP. DHCP-сервер доступен для конфигурирования, только если сервис Интернет настроен в режиме маршрутизатора.



Настройки DHCP-сервера

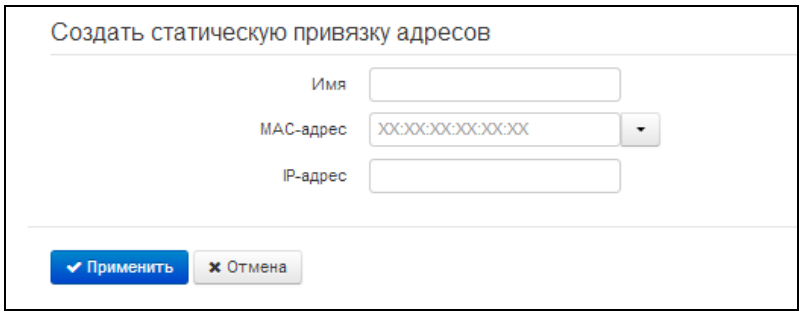
- *Включен* – при установленном флаге включить локальный DHCP-сервер;
- *Начальный IP-адрес* – начальный адрес пула IP-адресов;
- *Количество адресов* – количество адресов в пуле;
- *Срок аренды, мин* – установка максимального времени использования подключенным устройством IP-адреса, назначенного DHCP-сервером.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

При попытке изменить начальный адрес на значение из другой подсети по отношению к подсети интерфейса LAN происходит автоматическая установка пула под текущее значение адреса локальной подсети.

Статические привязки адресов

Для добавления новой статической привязки нажмите кнопку *«Добавить»* и заполните следующие поля:



- Имя текущей статической привязки;
- MAC-адрес – установка статического MAC-адреса. Задается в формате XX:XX:XX:XX:XX:XX, возможен выбор адреса подключенных устройств из всплывающего меню;
- IP-адрес – установка статического IP-адреса для указанного MAC-адреса.

Конфигурирование статических привязок полезно, если Вам необходимо, чтобы определенному компьютеру, подключенному к LAN-интерфейсу устройства, всегда назначался определенный IP-адрес.

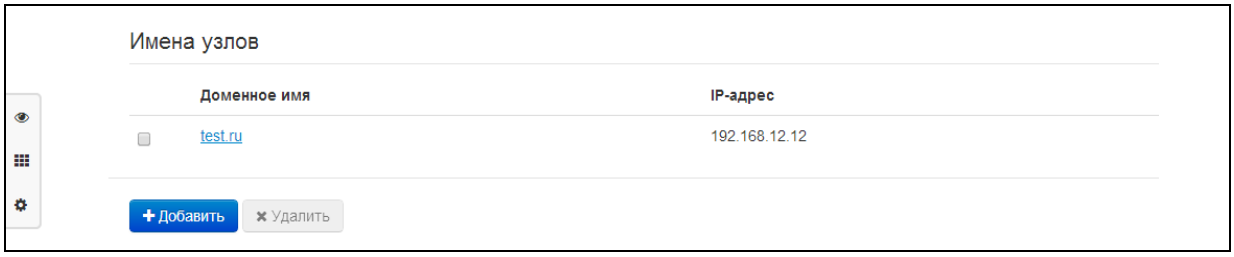
Нажмите кнопку *«Применить»* для внесения IP-адреса в список статических IP-адресов для DHCP-сервера. Для отмены изменений нажмите кнопку *«Отмена».*

Для удаления адреса из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку *«Удалить»*.

2.6.2.5 Подменю «Локальный DNS»

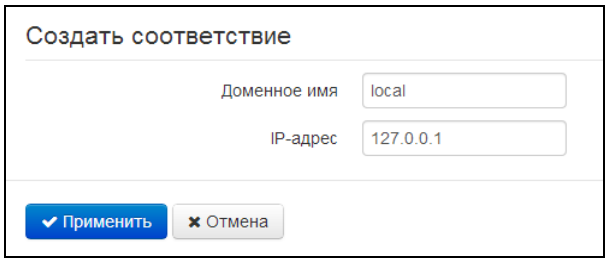
В подменю «Локальный DNS» производится конфигурирование локального DNS-сервера устройства путем добавления в базу пар IP-адрес – доменное имя.

Локальный DNS позволяет шлюзу получить IP-адрес взаимодействующего устройства по его доменному имени. В случае отсутствия сервера DNS в сегменте сети, которому принадлежит шлюз, но при необходимости маршрутизации по сетевым именам либо использования в качестве адреса SIP-сервера его сетевого имени, можно использовать «Локальный DNS». При этом необходимо знать установленные соответствия между именами узлов (доменами) и их IP-адресами.



<u>Настройка узлов</u>

Для добавления адреса в список необходимо нажать кнопку *«Добавить»* и в окне *«Создать соответствие»* заполнить следующие поля:



- Доменное имя – имя узла;
- IP-адрес – IP-адрес узла.

Нажмите кнопку *«Применить»* для создания соответствия IP-адрес – доменное имя. Для отмены изменений нажмите кнопку *«Отмена».* Для удаления записи из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку *«Удалить»*.

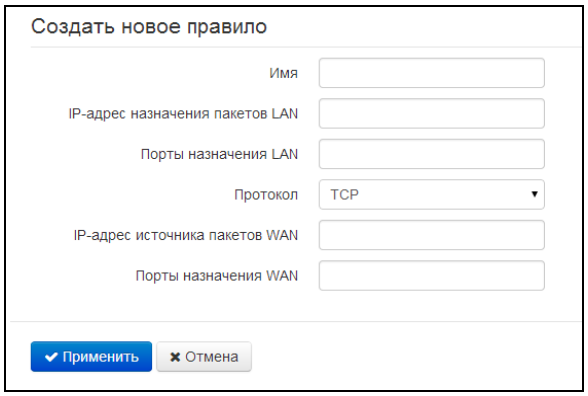
2.6.2.6 Подменю «NAT и проброс портов»

В подменю «NAT и проброс портов» выполняется настройка проброса портов (ports forwarding) из WAN-интерфейса в LAN-интерфейс. Подменю доступно, только если сервис Интернет настроен в режиме маршрутизатора.

NAT – (Network Address Translation) режим трансляции сетевых адресов – позволяет преобразовывать IP-адреса и сетевые порты IP-пакетов. Проброс сетевых портов необходим, когда TCP/UDP-соединение с локальным (подключенным к LAN-интерфейсу) компьютером устанавливается из внешней сети. Данное меню настроек позволяет задать правила, разрешающие прохождение пакетов из внешней сети на указанный адрес в локальной сети, тем самым делая возможным установление соединения. Проброс портов главным образом необходим при использовании torrent- и p2p-сервисов. Для этого в настройках torrent- или p2p-клиента нужно посмотреть используемые им TCP/UDP-порты и задать для этих портов соответствующие правила проброса на IP-адрес Вашего компьютера.

Настройка правила NAT

Для добавления нового правила NAT нажмите кнопку *«Добавить»* и в открывшемся окне «Создать новое правило» заполните следующие поля:



- *Имя* – название правила (поле обязательно для заполнения);
- *IP-адрес назначения пакетов LAN* – IP-адрес хоста в локальной сети, на который осуществляется трансляция пакетов, подпадающих под данное правило;
- *Порты назначения LAN* – значения TCP/UDP-портов получателя, на которые будут транслироваться пакеты в локальную сеть (допускается указывать либо одиночный порт, либо через “-“ диапазон портов);
- *Протокол* – выбор протокола пакета, подпадающего под данное правило: TCP, UDP, TCP/UDP;
- *IP-адрес источника пакетов WAN* – IP-адрес отправителя пакета во внешней сети, подпадающего под данное правило;
- *Порты назначения WAN* – значения TCP/UDP-портов получателя пакета во внешней сети, при которых пакет подпадает под данное правило (допускается указывать либо одиночный порт, либо через “-“ диапазон портов).

Правило проброса портов работает следующим образом. У пакета, приходящего на адрес WAN-интерфейса устройства по протоколу *«Протокол»,* на порт из диапазона *«Порты WAN»* и имеющего адрес источника *«IP-адрес WAN»* (если этот параметр оставить пустым – адрес источника не анализируется), осуществляется подмена адреса и порта назначения на содержимое полей *«IP-адрес LAN»* и *«Порты LAN»* соответственно.

Нажмите кнопку *«Применить»* для добавления нового правила. Для отмены изменений нажмите кнопку *«Отмена»*.

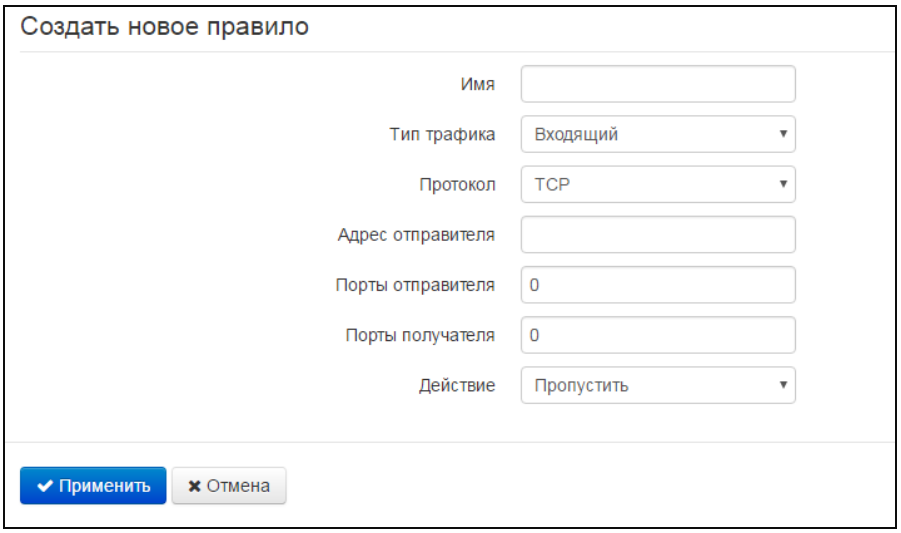
Для удаления правила из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку «Удалить».

2.6.2.7 Подменю «Сетевой экран»

В подменю *«Сетевой экран»* устанавливаются правила прохождения входящего, исходящего и транзитного трафика. Имеется возможность ограничивать прохождение трафика разного типа (входящий, исходящий, транзитный) в зависимости от протокола, IP-адресов источника и назначения, TCP/UDP-портов источника и назначения (для сообщений протоколов TCP или UDP), типа сообщения ICMP (для сообщений протокола ICMP).

Настройка правил сетевого экрана

Для добавления нового правила нажмите кнопку *«Добавить»* и в открывшемся окне «Создать новое правило» заполните следующие поля:



- *Имя* – название правила;
- *Тип трафика* – выбор типа трафика, на который распространяется действие данного правила:
  - *Входящий* – входящий на устройство трафик (получателем является непосредственно один из сетевых интерфейсов устройства). При выборе данного типа трафика для редактирования станут доступны следующие поля:
    - *Адрес отправителя* – задает начальный IP-адрес отправителя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.16.0/24 или 192.168.16.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов (запись маски в виде /24 соответствует записи /255.255.255.0);
  - *Исходящий* – исходящий с устройства трафик (трафик, генерируемый локально устройством с одного из сетевых интерфейсов). При выборе данного типа трафика для редактирования станут доступны следующие поля:

- *Адрес получателя* – задает IP-адрес получателя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.18.0/24 или 192.168.18.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;

– *Транзитный* – транзитный трафик (трафик, проходящий между двумя сетевыми интерфейсами, когда отправителем и получателем являются внешние устройства). При выборе данного типа трафика для редактирования станут доступны следующие поля:

- *Адрес отправителя* – задает IP-адрес отправителя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.16.0/24 или 192.168.16.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;
- *Адрес получателя* – задает IP-адрес получателя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.18.0/24 или 192.168.18.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;

- *Протокол* – протокол пакета, на который распространяется действие данного правила: TCP, UDP, TCP/UDP, ICMP, любой;
- *Действие* – действие, совершаемое над пакетами (отбросить/пропустить);

При выборе протоколов TCP, UDP, TCP/UDP для редактирования будут доступны настройки:

- *Порты отправителя* – список портов отправителя, пакеты которого будут подпадать под данное правило (допускается указывать либо одиночный порт, либо через “-“ диапазон портов);
- *Порты получателя* – список портов получателя, пакеты которого будут попадать под данное правило (допускается указывать либо одиночный порт, либо через “-“ диапазон портов);

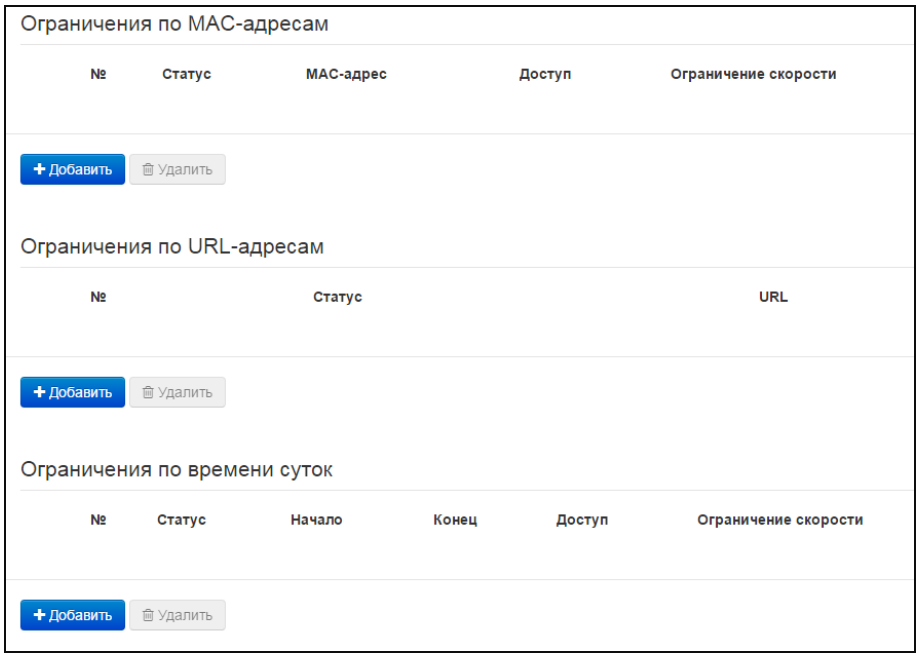
При выборе протокола ICMP для редактирования будут доступны настройки:

- *Тип сообщения* – можно создать правило только для определенного типа ICMP-сообщения либо для всех.

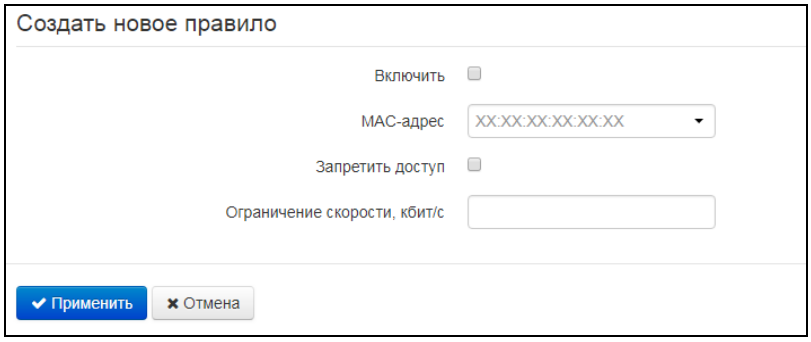
Нажмите кнопку «Применить» для добавления нового правила. Для отмены изменений нажмите кнопку «Отмена». Для удаления записи из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку «Удалить».

2.6.2.8 Подменю «ACL»

В подменю «ACL» выполняются настройки списков доступа. Access Control List или ACL — список контроля доступа, который содержит правила, определяющие прохождение трафика через интерфейс.

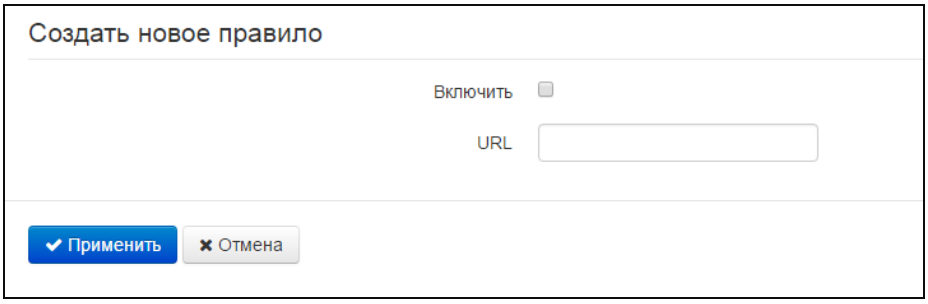


Ограничения по MAC-адресам



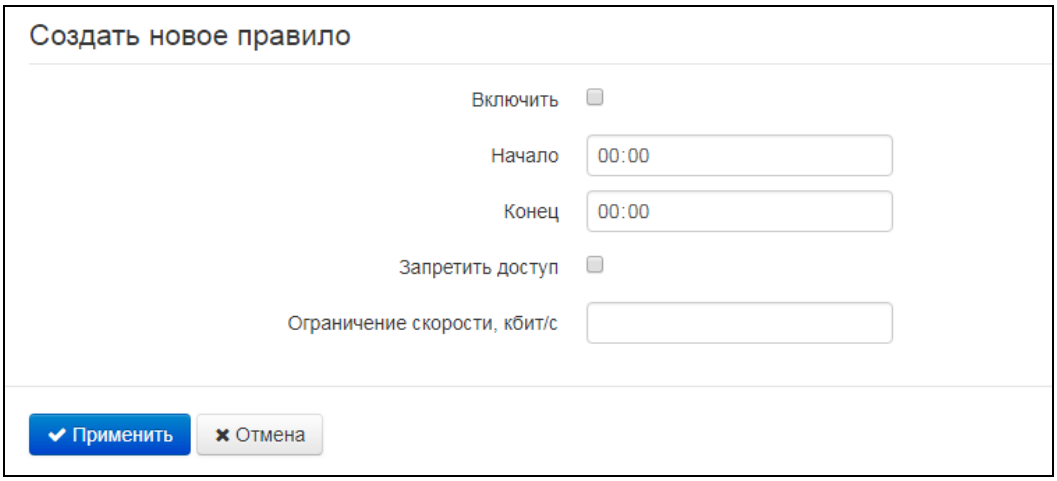
- *Включить* – при установленном флаге активируется правило фильтрации по MAC;
- *MAC-адрес* – MAC-адрес устройства, для которого будет действовать созданное правило;
- *Запретить доступ* – при установленном флаге с заданного устройства будет полностью запрещён доступ и передача транзитного трафика. Если флаг не установлен, скорость будет ограничена до указанного значения;
- *Ограничение скорости, кбит/с* – максимальная скорость потока данных для устройства с указанным MAC-адресом (0 кбит/с — эквивалентно отсутствию ограничения скорости потока данных);

Ограничения по URL-адресам



- *Включить* – при установленном флаге активируется правило фильтрации по URL;
- *URL* – URL-адрес устройства, для которого будет действовать созданное правило;

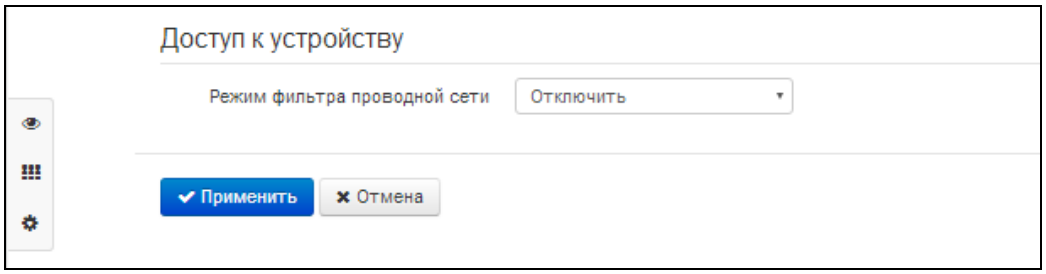
Ограничения по времени суток



- *Включить* – при установленном флаге правило фильтрации активируется и деактивируется в назначенное время;
- *Начало* – время в 24-часовом формате счисления (чч:мм), с которого будет действовать созданное правило;
- *Конец* – время в 24-часовом формате счисления (чч:мм), до которого будет действовать созданное правило;
- *Запретить доступ* – при установленном флаге будет полностью запрещён доступ и передача транзитного трафика. Если флаг не установлен, скорость будет ограничена до указанного значения;
- *Ограничение скорости, кбит/с* – в течение заданного интервала времени скорость будет ограничена до указанного значения (0 кбит/с — эквивалентно отсутствию ограничения скорости потока данных).

2.6.2.9 Подменю «Фильтр MAC»

В подменю «Фильтр MAC» выполняются настройка фильтрации доступа по MAC-адресу клиента.



- Режим фильтра – определяет один из трех алгоритмов работы фильтра в зависимости от MAC-адреса клиента:
  - *Отключить* – фильтрация по MAC-адресам отключена – всем клиентам разрешено подключаться к устройству;

– *Чёрный список* – в данном режиме работы фильтра клиентам, MAC-адреса которых указаны в «Списке MAC-адресов», запрещено подключаться к устройству. Абонентам, MAC-адреса которых не указаны в списке, подключение разрешено;
– *Белый список* – в данном режиме работы фильтра клиентам, MAC-адреса которых указаны в «Списке MAC-адресов», разрешено подключаться к устройству. Абонентам, MAC-адреса которых в списке не указаны, подключение запрещено.

Список MAC-адресов

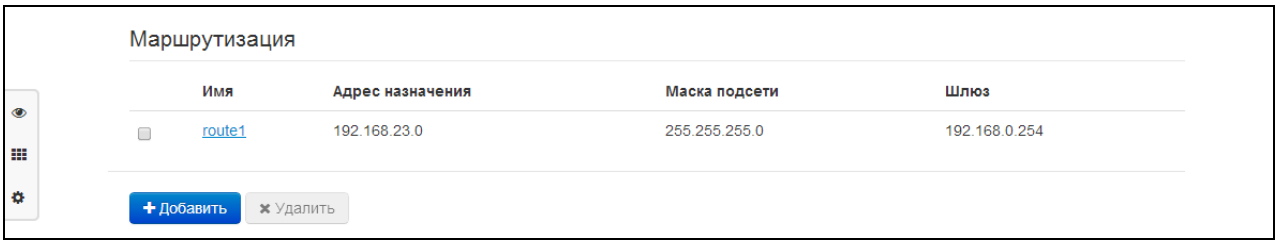
В список можно внести до тридцати MAC-адресов клиентов, доступ которым к устройству регулируется настройкой режима фильтра.

Для добавления нового клиента в список нажмите кнопку *«Добавить»* и введите его MAC-адрес.

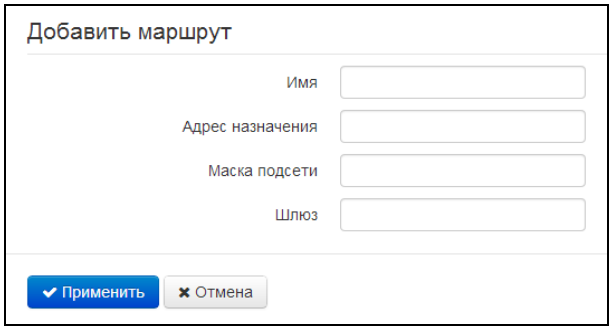
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.2.10 Подменю «Маршрутизация»

В подменю «Маршрутизация» настраиваются статические маршруты устройства.



Для добавления нового маршрута нажмите на кнопку «Добавить» и заполните следующие поля:



- *Имя* – название маршрута, используется для удобства восприятия человеком. Поле можно оставить пустым;
- *Адрес назначения* – IP-адрес хоста или подсети назначения, до которых необходимо установить маршрут;
- *Маска подсети* – маска подсети. Для хоста маска подсети устанавливается в значение 255.255.255.255, для подсети – в зависимости от её размера;
- *Шлюз* – IP-адрес шлюза, через который осуществляется выход на *«Адрес назначения»*.

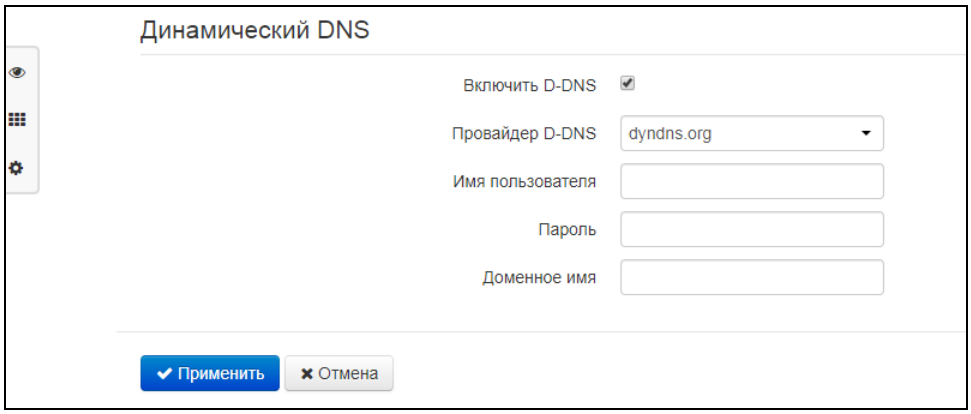
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.2.11 Подменю «Динамический DNS»

В подменю «Динамический DNS» выполняется настройка соответствующего сервиса.

Динамический DNS (D-DNS) позволяет информации на DNS-сервере обновляться в реальном времени в автоматическом режиме. Применяется для назначения постоянного доменного имени устройству (компьютеру, роутеру) с динамическим IP-адресом.

Динамический DNS часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена на локальном DNS-сервере.

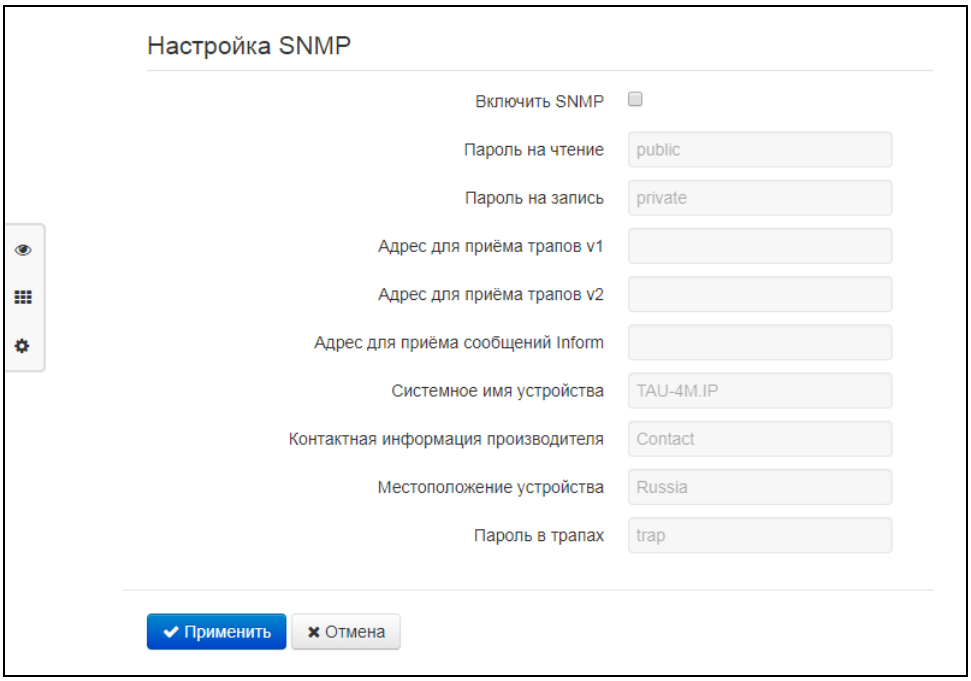


- *Включить D-DNS* – при установленном флаге сервис D-DNS активен, и для редактирования доступны следующие настройки:
- *Провайдер D-DNS* – адрес провайдера D-DNS – выберите одного провайдера из списка доступных или введите его адрес вручную;
- *Имя пользователя* – имя пользователя для доступа к учетной записи сервиса D-DNS;
- *Пароль* – пароль для доступа к учетной записи сервиса D-DNS;
- *Доменное имя* – регистрируемое доменное имя на D-DNS сервере. Обновление информации об IP-адресе устройства на сервере провайдера происходит периодически через 60 секунд.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.2.12 Подменю «SNMP»

Программное обеспечение *TAU-4M.IP* позволяет проводить мониторинг состояния устройства и его конфигурирование, используя протокол SNMP. В подменю «SNMP» выполняются настройки параметров SNMP-агента. Устройство поддерживает протоколы версий SNMPv1, SNMPv2c.



- *Включить SNMP* – при установленном флаге разрешено использование протокола SNMP;
- *Пароль на чтение* – пароль на чтение параметров (общепринятый: *public*);
- *Пароль на запись* – пароль на запись параметров (общепринятый: *private*);
- *Адрес для приёма трапов v1* – IP-адрес или доменное имя приемника сообщений SNMPv1-trap в формате HOST [COMMUNITY [PORT]];
- *Адрес для приёма трапов v2* – IP-адрес или доменное имя приемника сообщений SNMPv2-trap в формате HOST [COMMUNITY [PORT]];
- *Адрес для приёма сообщений Inform* – IP-адрес или доменное имя приемника сообщений Inform в формате HOST [COMMUNITY [PORT]];
- *Системное имя устройства* – имя устройства;
- *Контактная информация производителя* – контактная информация производителя устройства;
- *Местоположение устройства* – информация о местоположении устройства;
- *Пароль в трапах* – пароль, содержащийся в трапах (по умолчанию: trap).

В текущей версии программного обеспечения по протоколу SNMP имеется возможность конфигурировать отдельные параметры устройства: общие настройки SIP, настройки SIP-профилей, настройки FXS-порта, настройки групп вызова, настройки кодов управления ДВО с телефонного аппарата, настройки SNMP, настройки системного журнала.

Ниже приведен список объектов, поддерживаемых для чтения и конфигурирования посредством протокола SNMP:

- Enterprise.1.3.1 – общие настройки SIP-профилей;
- Enterprise.1.3.2.1 – настройки SIP-профилей;
- Enterprise.1.1.2.1 – настройки FXS-порта;
- Enterprise.1.4.1.1 – настройки групп вызова;
- Enterprise.1.5 – коды активации ДВО с телефонного аппарата;
- Enterprise.2.1 – настройки SNMP;
- Enterprise.3.1 – настройки системного журнала.

где Enterprise – 1.3.6.1.4.1.35265.1.56 идентификатор устройства.

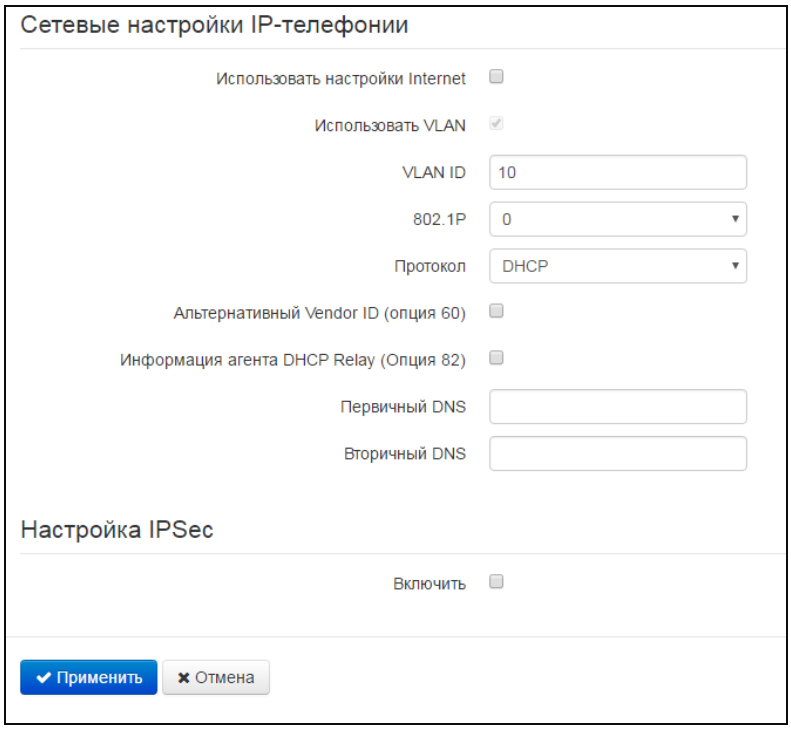
Для записи настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.3 Меню «IP-телефония»

В меню «IP-телефония» выполняются настройки VoIP (Voice over IP): настройка протокола SIP, конфигурация интерфейсов FXS, установка кодеков, плана нумерации, методов передачи факса и модема.

2.6.3.1 Подменю «Настройки сети»

В подменю «Настройки сети» имеется возможность задать собственные сетевые настройки для услуги VoIP.



- *Использовать настройки Internet* – при установленном флаге использовать настройки сети, установленные в меню *«Сеть» -> «Интернет»*, иначе – настройки, установленные в текущем меню;
- *Использовать VLAN*[3] – при установленном флаге сервис IP-телефонии будет использовать для своей работы выделенный интерфейс в отдельной VLAN, номер которой указан в поле *«VLAN ID»;*
- *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет);
- *Протокол* – выбор протокола назначения адреса на интерфейс услуги VoIP:
  - *Static* – режим работы, при котором IP-адрес и все необходимые настройки на WAN-интерфейс назначаются вручную. При выборе типа «Static» для редактирования станут доступны следующие параметры:

[3] В версии ПО 1.9.1 разрешается задавать индивидуальные сетевые настройки услуги VoIP только в выделенной VLAN.

- *IP-адрес* – установка IP-адреса интерфейса услуги VoIP;
- *Маска подсети* – маска подсети интерфейса услуги VoIP;
- *Шлюз по умолчанию* – IP-адрес дефолтного шлюза интерфейса услуги VoIP;
- *Первичный DNS*, *Вторичный DNS* – IP-адреса DNS-серверов, необходимых для работы услуги VoIP.

– *DHCP* – режим работы, при котором IP-адрес, маска подсети, адреса DNS-серверов и другие параметры, необходимые для работы услуги (например, статические маршруты до SIP-сервера, сервера регистрации), будут получены от DHCP-сервера автоматически. Если от провайдера не удаётся получить адреса DNS-серверов, Вы можете назначить их вручную в полях *«Первичный DNS»* и *«Вторичный DNS»*. Адреса, заданные вручную, будут иметь приоритет над адресами DNS-серверов, полученными по протоколу DHCP.

Для протокола DHCP имеется возможность задать необходимое значение опций 60 и 82.

- *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля *Vendor ID (опция 60).* При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.

Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат:
[VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**]** **[SN:**серийный номер**][WAN:**MAC-адрес интерфейса WAN**][LAN:**MAC-адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

Пример:

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

- Информация агента DHCP Relay (опция 82) – при установленном флаге позволяет добавить в DHCP-запрос:

▪ *Идентификатор цепи агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 1 - Agent Circuit ID;
▪ *Идентификатор удаленного агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 2 - Agent Remote ID.

Список используемых DHCP-опций на каждом сетевом интерфейсе (Internet, VoIP, Management) можно задавать вручную. Информация по настройке списка представлена в приложении В.

Настройка IPSec:

В данном разделе осуществляется настройка шифрования по технологии IPSec (IP Security).

IPSec – это набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, позволяющий осуществлять подтверждение подлинности (аутентификацию), проверку целостности и/или шифрование IP-пакетов. IPSec также включает в себя протоколы для защищённого обмена ключами в сети Интернет.

В текущей версии программного обеспечения посредством IPSec можно осуществлять только доступ к интерфейсам управления устройством (Web, Telnet, SSH).

Подробное описание настроек *IPSec* приведено в разделе 2.6.2.1 в графе *Настройка IPSec*.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

2.6.3.2 Подменю «QoS»

В подменю «QoS» настраиваются функции обеспечения качества обслуживания (Quality of Service).

Настройка диапазона RTP-портов

- *Минимальный RTP-порт* - нижняя граница диапазона RTP-портов, используемых для передачи разговорного трафика;
- *Максимальный RTP-порт* - верхняя граница диапазона RTP-портов, используемых для передачи разговорного трафика.

Настройка DSCP для сигнализации (SIP)

Настройка правила QoS

- *SIP-порт* – значение порта источника для исходящего голосового трафика, который будет маркироваться заданным кодом DSCP;
- *DSCP* – значение поля DSCP заголовка IP-пакета для голосового трафика с заданным портом источника.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

2.6.3.3 Подменю «Настройка линий»

В подменю *«Настройка линий»* выполняются настройки телефонных портов *Phone1, Phone2, Phone3, Phone4*.

Список телефонных линий

Линия	Статус	Номер телефона	Имя пользователя	Логин	SIP-порт	Профиль SIP
1	Выключен	001			5060	1st profile
2	Выключен	002			5060	1st profile
3	Выключен	003			5060	1st profile
4	Выключен	004			5060	1st profile

Для редактирования настроек нажмите левой кнопкой мыши по ссылке с номером настраиваемой линии и в открывшемся окне «Редактировать линию:» заполните следующие поля:

Редактировать линию 1: Настройка аккаунта

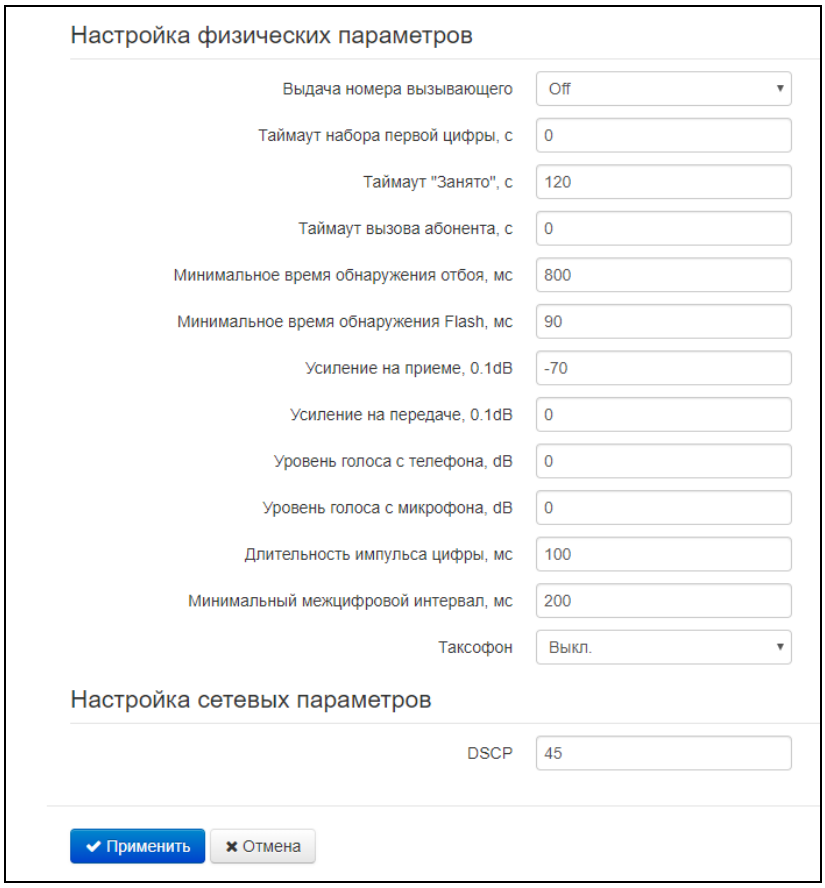
Включить ☐
Профиль SIP: 1st profile
Номер телефона: 001
Имя пользователя:
Использовать альтернативный номер ☐
SIP-порт: 5060
Категория абонента: Не использовать

Аутентификация

Логин:
Пароль:

Услуги ДВО

Режим использования Flash: Transmit flash
Прямой номер:
Ожидание вызова ☐
Выдача номера вызывающего абонента при ожидании вызова ☐
Остановка набора при # ☐
Горячая/теплая линия ☐
Безусловная переадресация ☐
Переадресация по занятости ☐
Переадресация по неответу ☐
Не беспокоить ☐
Разрешить перехват вызова на порт ☑
CLIR: Выкл.



Настройка аккаунта

- *Включить* – при установленном флаге порт активен;
- *Профиль SIP* – выбор SIP-профиля из перечня доступных. Настройка профилей производится в меню *«IP-телефония» -> «Профили»*;
- *Номер телефона* – абонентский номер, закрепленный за телефонным портом;
- *Имя пользователя* – имя пользователя, сопоставленное с портом (отображается в поле Display-Name заголовка From в исходящих сообщениях SIP);
- *Использовать альтернативный номер* – при установленном флаге в заголовок «From» сообщений SIP, отправляемых с данного порта, будет подставляться альтернативный номер (в частности, чтобы маскировать свой реальный номер от системы АОН вызываемого абонента);
- *Подставлять заголовок в Contact* – альтернативный номер, присвоенный телефонному порту, будет заменен на указанный номер в заголовке Contact сообщения SIP. Данная настройка используется только для портов, находящихся в группе вызова;
- *SIP-порт* – UDP-порт для приёма входящих сообщений SIP на данный аккаунт, а также для отправки исходящих SIP-сообщений с данного аккаунта. Принимает значения 1-65535 (по умолчанию 5060);
- *Категория абонента* – категория вызывающего абонента (calling party category) – используется для передачи в заголовке «From» исходящих сообщений; последний при этом передается в формате Tel-URI (см. RFC3966);

- *Логин и пароль для аутентификации* – имя пользователя и пароль, используемые для аутентификации абонента на SIP-сервере (и сервере регистрации);

<u>*Услуги ДВО*</u>

- *Режим использования flash* – режим использования функции flash (короткий отбой):
  - *Transmit flash* – передача flash в канал (одним из методов, настроенных во вкладке «Профили» в параметре *Передача Flash*);
  - *Attended calltransfer* – flash обрабатывается локально устройством (передача вызова осуществляется после установления соединения с третьим абонентом). Подробное описание алгоритма работы «Attended calltransfer» смотрите в разделе 3.1 Передача вызова;
  - *Unattended calltransfer* – flash обрабатывается локально устройством (передача вызова осуществляется по окончанию набора номера третьего абонента). Подробное описание алгоритма работы «Unattended calltransfer» смотрите в разделе 3.1 Передача вызова;
  - *Local calltransfer* – передача вызова внутри устройства, без отправки сообщения REFER. Подробное описание алгоритма работы «Local calltransfer» смотрите в разделе 3.1 Передача вызова.

- *Режим передачи вызова* – настройка доступна только для Attended calltransfer и Local calltransfer и отвечает за режим активации услуги передачи вызова:
  - Комбинированный – передача вызова активируется по отбою и по нажатию R 4;
  - Flash+4 –передача вызова активируется после нажатия R 4;
  - По отбою – передача вызова активируется после отбоя.

- *Ожидание вызова* – при установленном флаге разрешена услуга «*Ожидание вызова*» (услуга доступна в режиме использования функции flash – call transfer);

- *Выдача номера вызывающего абонента при ожидании вызова* – при установленном флаге происходит выдача номера абонента для услуги ожидания вызова;

- *Остановка набора при #* – при установленном флаге использовать кнопку ‘#’ на телефонном аппарате для окончания набора, иначе ‘#’, набранная с телефонного аппарата, используется как часть номера;

- *Горячая/теплая линия* – при установленном флаге разрешена услуга «*горячая/теплая линия*». Услуга позволяет автоматически установить исходящее соединение при подъёме трубки телефона без набора номера с заданной задержкой (в секундах). При установленном флаге заполните следующие поля:
  - *Номер услуги "горячая/теплая линия"* – номер телефона, с которым будет устанавливаться соединение через время, равное «Таймауту задержки», после поднятия трубки телефона (в плане нумерации используемого SIP-профиля должен быть префикс на данное направление);
  - *Таймаут задержки, с* – интервал времени, через который будет устанавливаться соединение с встречным абонентом, в секундах;

- *Безусловная переадресация* – при установленном флаге разрешена услуга CFU (Call Forward Unconditional) – все входящие вызовы перенаправляются на указанный номер безусловной переадресации. При установленном флаге заполните следующие поля:
  - *Номер безусловной переадресации* – номер, на который перенаправляются все входящие вызовы при включенной услуге «Безусловная переадресация» (в плане

нумерации используемого SIP-профиля должен быть префикс на данное направление);

- *Переадресация по занятости* – при установленном флаге разрешена услуга CFB (Call Forward at Busy) – переадресация вызова при занятости абонента на указанный номер. При установленном флаге заполните следующие поля:
  - *Номер переадресации по занятости* – номер, на который перенаправляются входящие вызовы при занятости абонента при включенной услуге «Переадресация по занятости» (в плане нумерации используемого SIP-профиля должен быть префикс на данное направление);
- *Переадресация по неответу* – при установленном флаге разрешена услуга CFNA (Call Forward at No Answer) – переадресация вызова при неответе абонента. При установленном флаге заполните следующие поля:
  - *Номер переадресации по неответу* – номер, на который перенаправляются входящие вызовы при неответе абонента при включенной услуге «Переадресация по неответу» (в плане нумерации используемого SIP-профиля должен быть префикс на данное направление);
  - *Таймаут неответа, с* – интервал времени, через который будет производиться переадресация вызова в случае неответа абонента;
- *Не беспокоить* – при установленном флаге устанавливается временный запрет входящей связи (услуга DND – Don’t Disturb).

При включении одновременно нескольких услуг приоритет следующий (в порядке снижения):

- CFU;
- DND;
- CFB, CFNA.

- *Разрешить перехват вызова на порт* – при включенной опции разрешен перехват входящих на порт вызовов (перехват разрешается только в пределах одной группы перехвата и при условии использования портами одного SIP-профиля);
- *CLIR* – ограничение идентификации номера вызывающего абонента:
  - *Выкл* – услуга CLIR отключена;
  - *SIP:From* – в заголовке From сообщений протокола SIP будет передаваться *Anonymous sip:anonymous@unknown.host*
  - *SIP:From и SIP:Contact – в заголовках From и Contact* сообщений протокола SIP будет передаваться *Anonymous sip:anonymous@unknown.host*

<u>*Настройка физических параметров*</u>

- *Выдача номера вызывающего* – выберите режим определения номера вызывающего абонента (Caller ID). Для работы Caller ID необходимо, чтобы телефонный аппарат абонента поддерживал установленный метод:
  - *Off* – определение номера вызывающего абонента выключено;
  - *FSK Bell 202, FSK V.23* – определение номера и имени вызывающего абонента методом FSK (по стандарту Bell202, или ITU-T V.23). Выдача номера в линию осуществляется между первым и вторым сигналом посылки вызова потоком данных с частотной модуляцией;

  - *DTMF* - определение номера вызывающего абонента методом DTMF. Выдача номера в линию осуществляется между первым и вторым сигналом посылки вызова двухчастотными DTMF-посылками;
  - *RUS AON* – идентификация линии вызывающего абонента методом «Русский АОН». Номер определяется по сигналу «Запрос АОН», выдаваемому телефоном вызываемого абонента;

- *Таймаут набора первой цифры, с* – таймер ожидания набора первой цифры номера. При отсутствии набора в течение установленного времени абоненту будет выдан сигнал «занято», а прием набора номера будет прекращен;
- *Таймаут «Занято», с* – таймер выдачи абоненту сигнала «занято». Если по истечении установленного таймаута абонент не положит трубку телефона – в линию будет выдан сигнал ошибки;
- *Таймаут вызова абонента, с* – запускается при поступлении входящего вызова и определяет максимальное время ответа на вызов. По истечении установленного таймаута удаленному абоненту будет отправлен сигнал занятости.
- *Минимальное время обнаружения отбоя, мс* – минимальное время обнаружения отбоя. Одновременно с этим, данный параметр является максимальным временем детектирования короткого отбоя (flash).
- *Минимальное время обнаружения flash* – минимальное время обнаружения короткого отбоя, (80-1000) мс;
- *Усиление на прием, 0.1dB* – усиление сигнала на приём (сигнал, который выдается в трубку телефона), (-200..200) единица измерения – 0,1 дБ;
- *Усиление на передаче, 0.1dB* – усиление сигнала на передачу (сигнала, поступающего в микрофон телефонной трубки), (-200..200) единица измерения – 0,1 дБ;
- *Уровень голоса с телефона, dB* - настройка уровня речевого сигнала к абоненту, (-31..31) dB;
- *Уровень голоса с микрофона, dB* - настройка уровня речевого сигнала от абонента, (-31..31) dB;
- *Длительность импульса цифры, мс* – настройка необходима при импульсном режиме набора номера, (10-150) мс;
- *Минимальный межцифровой интервал* – настройка необходима при импульсном режиме набора номера, (150-20000) мс;
- *Таксофон (Payphone)* – настройка режима работы линии при подключении таксофона:
  - *Выкл. (Off)* – обычный режим, таксофон не подключен;
  - *Переполюсовка (Polarity reversal)* – изменение полярности напряжения питания линии при исходящем вызове после ответа встречного абонента;
  - *Импульсы 12 кГц (12 kHz)* – при исходящем вызове в линию один раз в секунду выдается тарифный импульс частотой 12 кГц;
  - *Импульсы 16 кГц (16 kHz)* – при исходящем вызове в линию один раз в секунду выдается тарифный импульс частотой 16 кГц.

Настройка сетевых параметров

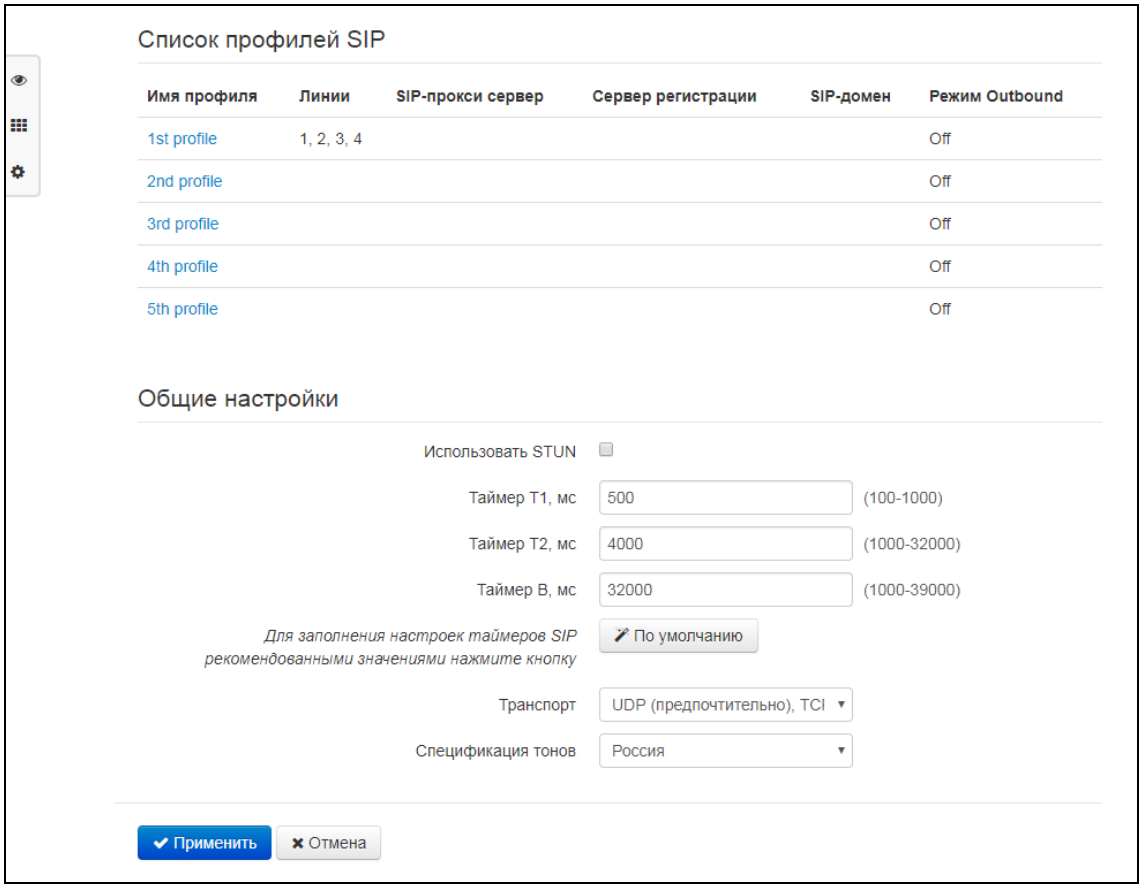
- *DSCP* - значение поля DSCP-заголовка IP-пакета для голосового трафика с настраиваемой линии.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

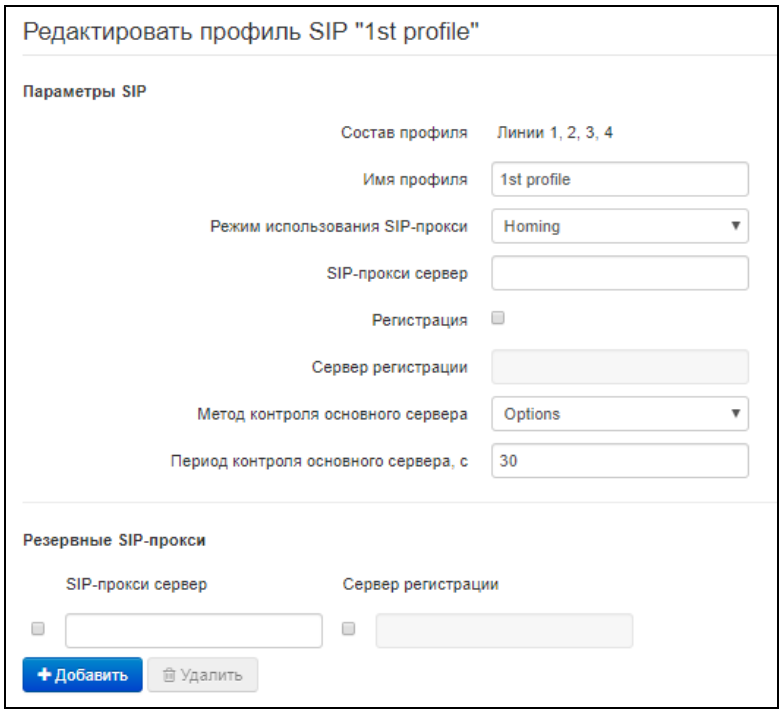
2.6.3.4 Подменю «Профили SIP»

В подменю «*Профили SIP*» выполняются настройки SIP-профилей устройства. За каждым SIP-профилем можно назначить собственные адреса SIP-сервера и сервера регистрации, голосовые кодеки и кодеки факса/модема, индивидуальный план нумерации и другие параметры. Необходимость

использования разных SIP-профилей возникает, когда разные абонентские порты работают через разные направления связи (разные SIP-серверы). При этом за каждым абонентским портом может быть закреплен только один SIP-профиль (настройка в меню *«IP-телефония» -> «Настройка линий»*).



Для редактирования настроек профиля нажмите левой кнопкой мыши по ссылке настраиваемого профиля. В открывшемся окне «Редактировать профиль:» заполните следующие поля:



Параметры SIP

- *Состав профиля* – список абонентских портов, которым назначен профиль, поле не редактируемое;
- *Имя профиля* – пользовательское имя настраиваемого профиля;
- *Режим использования SIP-прокси* – в выпадающем списке можно выбрать режим работы с SIP-сервером:
  - Не использовать – режим, при котором SIP-прокси сервер не используется, а все запросы INVITE отправляются на адрес, указанный после символа «@» в записи масок плана нумерации;
  - Parking – режим резервирования SIP-прокси без контроля основного SIP-прокси;
  - Homing – режим резервирования SIP-прокси с контролем основного SIP-прокси.

Шлюз может работать с одним основным и максимум четырьмя резервными SIP-прокси. При работе только с основным SIP-прокси, режимы Parking и Homing ничем друг от друга не отличаются. В этом случае при отказе основного SIP-прокси потребуется его восстановление для обеспечения работоспособности.

При наличии резервных SIP-прокси работа в режимах *Parking* и *Homing* осуществляется следующим образом. При совершении исходящего вызова шлюз отправляет сообщение INVITE на адрес основного SIP-прокси или при попытке регистрации – сообщение REGISTER. В случае если по истечении времени *Invite total timeout* от основного SIP-прокси не приходит ответ, либо приходит ответ 408 или 503 – шлюз отправляет INVITE (либо REGISTER) на адрес первого резервного SIP-прокси. Если он тоже недоступен, запрос переправляется на следующий резервный SIP-прокси и т.д. Как только доступный резервный SIP-прокси будет найден, произойдет перерегистрация на нем.

Далее, в зависимости от выбранного режима резервирования, действия следующие:

В режиме parking нет контроля основного SIP-прокси, и шлюз продолжает работать с резервным SIP-прокси, даже если основной восстановлен. При потере связи с текущим SIP-прокси будет продолжен опрос последующих резервных SIP-прокси по описанному выше алгоритму. При недоступности последнего резервного SIP-прокси опрос продолжится по кругу, начиная с основного.

В режиме homing доступно три вида контроля основного SIP-прокси: посредством периодической передачи на его адрес сообщений OPTIONS, посредством периодической передачи на его адрес сообщений REGISTER либо посредством передачи запроса INVITE при совершении исходящего вызова. Запрос INVITE сначала передается на основной SIP-прокси, а затем, в случае его недоступности, на текущий резервный и т.д. Независимо от вида контроля, если обнаружено, что основной SIP-прокси восстановился – происходит перерегистрация на нем. Шлюз начинает работать с основным SIP-прокси.

- *SIP-прокси сервер* – сетевой адрес SIP-сервера – устройства, осуществляющего контроль доступа всех абонентов к телефонной сети провайдера. Можно указать как IP-адрес, так и доменное имя (через двоеточие можно задать UDP-порт SIP-сервера, по умолчанию 5060);
- *Регистрация* – при установленном флаге регистрировать порты, использующие данный профиль, на сервере регистрации;
- *Сервер регистрации* – сетевой адрес устройства, на котором осуществляется регистрация всех абонентов телефонной сети с целью предоставления им права пользоваться услугами связи (через двоеточие можно указать UDP-порт сервера регистрации, по умолчанию 5060). Можно указать как IP-адрес, так и доменное имя. Обычно сервер регистрации физически совмещен с SIP-прокси сервером (они имеют одинаковые адреса);
- *Метод контроля основного сервера* – выбор метода контроля доступности основного SIP-сервера в режиме Homing:
  - *Invite* – контроль посредством передачи на его адрес запроса INVITE при совершении исходящего вызова;

- *Register* – контроль посредством периодической передачи на его адрес сообщений REGISTER;
- *Options* – контроль посредством периодической передачи на его адрес сообщений OPTIONS;

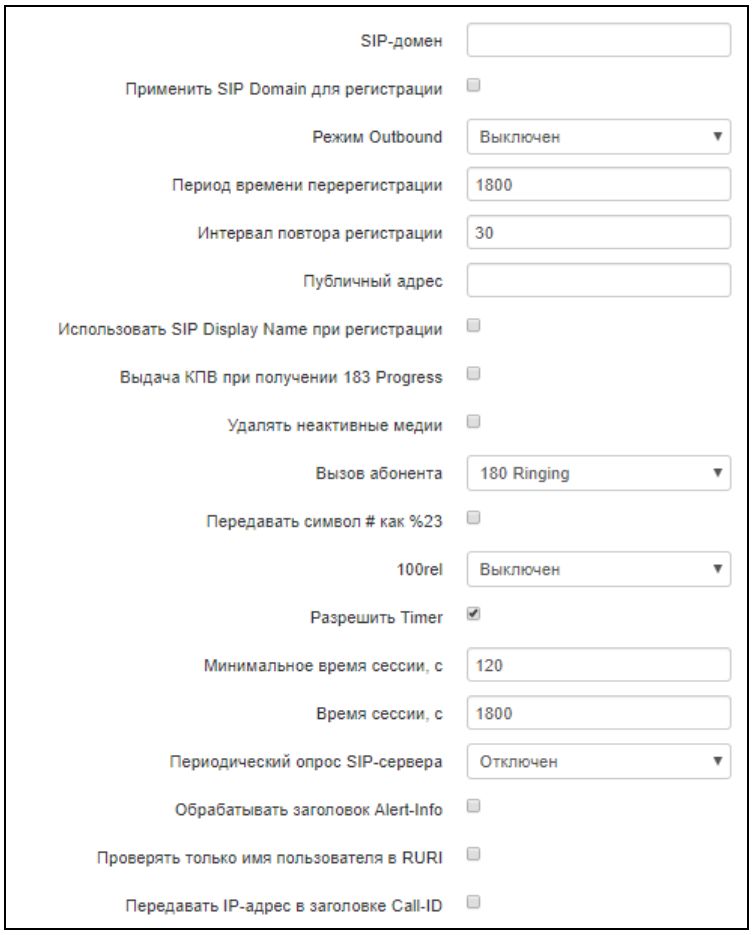
- *Период контроля основного сервера* – интервал отправки периодических сообщений в секундах с целью проверки доступности основного SIP-сервера.

Резервные SIP-прокси

Для добавления резервного SIP-прокси нажмите кнопку «Добавить» и выполните следующие настройки:

- *SIP-прокси сервер* – сетевой адрес резервного SIP-сервера. Можно указать как IP-адрес, так и доменное имя (через двоеточие можно задать UDP-порт SIP-сервера, по умолчанию 5060);
- *Сервер регистрации* – сетевой адрес резервного сервера регистрации (через двоеточие можно указать UDP-порт, по умолчанию 5060). Можно указать как IP-адрес, так и доменное имя. Если установлен флаг перед полем *Сервера регистрации*, то включена регистрация на резервном сервере.

Для удаления резервного SIP-прокси установите флаг напротив заданного адреса и нажмите кнопку «Удалить».



- *SIP domain* – домен, в котором находится устройство (заполнять при необходимости), назначается автоматически из 15 опции протокола DHCP или задается вручную. Домен, заданный вручную, имеет приоритет над настройкой, полученной по DHCP;

- *Применить SIP Domain для регистрации* – при установленном флаге применить SIP Domain для регистрации (SIP-домен будет подставляться в Request-Line запросов Register);

- *Режим Outbound* – режим Outbound:

- *Выключен* – маршрутизировать вызовы согласно плана нумерации;
- *Outbound* – для работы исходящей связи необходим план нумерации, однако все вызовы будут маршрутизироваться через SIP-сервер; в случае отсутствия регистрации абоненту выдается ответ станции, чтобы можно было осуществлять управление абонентским сервисом (управление ДВО);
- *Outbound с выдачей «занято»* – для работы исходящей связи необходим план нумерации, однако все вызовы будут маршрутизироваться через SIP-сервер; при отсутствии регистрации воспользоваться телефонией будет невозможно: в трубку выдается сигнал ошибки;

- *Период времени перерегистрации* – время, в течение которого действительна регистрация абонентского порта на SIP-сервере. Перерегистрация порта осуществляется в среднем через 2/3 указанного периода;

- *Интервал повтора регистрации* – промежуток времени между попытками зарегистрироваться на SIP-сервере в случае неуспешной регистрации;

- *Публичный адрес* – данный параметр используется в качестве внешнего адреса устройства при работе за NAT (за шлюзом). В качестве публичного адреса прописывается адрес внешнего (WAN) интерфейса шлюза (NAT), за которым установлен *TAU-4M.IP*. При этом на самом шлюзе (NAT) необходимо сделать проброс соответствующих SIP- и RTP-портов, используемых устройством;

- *Использовать SIP Display Name при регистрации* – при установленном флаге передавать имя пользователя в поле SIP Display Info сообщения Register;

- *Выдача «КПВ» при получении 183 Progress* – при установленном флаге выдавать сигнал «Контроль посылки вызова» при приеме сообщения «183 Progress» (без вложенного SDP);

- *Удалять неактивные медии* - при установленном флаге удалять неактивные медиа потоки при модификации SDP-сессии. Используется для взаимодействия со шлюзами, некорректно поддерживающими рекомендацию rfc3264 (по рекомендации количество потоков при модификациях сессии не должно уменьшаться);

- *Вызов абонента* – предварительный ответ, который отправляется устройством вызывающему оборудованию при входящем звонке:

  - *180 Ringing* – вызывающему оборудованию отправляется ответ 180; получив это сообщение, вызывающее оборудование должно выдать в линию локальный сигнал КПВ;
  - *183 Progress with SDP* – вызывающему оборудованию отправляется ответ 183+SDP – используется для проключения разговорного тракта до ответа вызываемого. В данном случае *TAU-4M.IP* будет удаленно выдавать вызывающему абоненту сигнал КПВ.
  - *Передавать символ # как %23* — при установленном флаге передавать знак фунта ("решетку") в SIP URI как escape-последовательность "%23", иначе - как символ "#".

- *100rel* – использование надежных предварительных ответов (RFC3262):

  - *Supported* – поддержка использования надежных предварительных ответов;
  - *Required* – требование использовать надежные предварительные ответы;
  - *Выключен* – не использовать надежные предварительные ответы.

Протоколом SIP определено два типа ответов на запрос, инициирующий соединение (INVITE) – предварительные и окончательные. Ответы класса 2xx, 3xx, 4xx, 5xx и 6xx являются окончательными и передаются надежно – с подтверждением их сообщением АСК. Ответы

класса 1xx, за исключением ответа *100 Trying*, являются предварительными и передаются ненадежно – без подтверждения (RFC3261). Эти ответы содержат информацию о текущей стадии обработки запроса INVITE, вследствие чего потеря таких ответов нежелательна. Использование надежных предварительных ответов также предусмотрено протоколом SIP (RFC 3262) и определяется наличием тега *100rel* в инициирующем запросе, в этом случае предварительные ответы подтверждаются сообщением PRACK.

Работа настройки при исходящей связи:

- *Supported* – передавать в запросе INVITE тег supported: 100rel. В этом случае взаимодействующий шлюз по своему усмотрению может передавать предварительные ответы либо надежно, либо нет;
- *Required* – передавать в запросе INVITE теги supported: 100rel и required: 100rel. В этом случае взаимодействующий шлюз должен передавать предварительные ответы надежно. Если взаимодействующий шлюз не поддерживает надежные предварительные ответы, то он должен отклонить запрос сообщением 420 с указанием неподдерживаемого тега unsupported: 100rel, в этом случае будет отправлен повторный запрос INVITE без тега required: 100rel;
- *Выключен* – не передавать в запросе INVITE ни один из тегов supported: 100rel и required: 100rel. В этом случае взаимодействующий шлюз будет передавать предварительные ответы ненадежно.

Работа настройки при входящей связи:

- *Supported, Required* – при приеме в запросе INVITE тега supported: 100rel, либо тега required: 100rel, передавать предварительные ответы надежно. Если тега supported: 100rel в запросе INVITE нет, то передавать предварительные ответы ненадежно;
- *Выключен* – при приеме в запросе INVITE тега required: 100rel, отклонить запрос сообщением 420 с указанием неподдерживаемого тега unsupported: 100rel. В остальных случаях передавать предварительные ответы ненадежно.

- *Разрешить timer* – при установленном флаге включена поддержка расширения timer (RFC 4028). После установления соединения, если обе стороны поддерживают timer, одна из них периодически отправляет запросы re-INVITE для контроля соединения (если обе стороны поддерживают метод UPDATE, для чего он должен быть указан в заголовке Allow – обновление сессии осуществляется посредством периодической отправки сообщений UPDATE);

- *Минимальное время сессии*, с – минимальный интервал проверки работоспособности соединения (от 90 до 1800 с, по умолчанию 120 с.);

- *Время сессии, с* – период времени в секундах, по истечении которого произойдет принудительное завершение сессии, в случае если сессия не будет вовремя обновлена (от 90 до 80000 с., рекомендуемое значение - 1800 с, 0 – время сессии не ограничено);

- *Периодический опрос SIP-сервера* – выбор способа опроса SIP-сервера:

  - *Отключен* – SIP-сервер не опрашивается;
  - *Options* – опрос SIP-сервера при помощи сообщений OPTIONS;
  - *Notify* – опрос SIP-сервера при помощи сообщений NOTIFY;
  - *CLRF* – опрос SIP-сервера пустым UDP-пакетом;

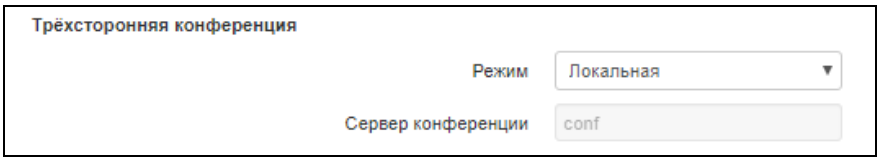
- *Интервал опроса* – период времени в секундах, через который выполняется опрос SIP-сервера;

- *Обрабатывать заголовок Alert-Info* – обрабатывать заголовок Alert-Info в запросе INVITE для выдачи на абонентский порт отличной от стандартной посылки вызова;

- *Проверять только имя пользователя в RURI* – если флаг установлен, то анализируется только абонентский номер (user), при совпадении которого вызов будет назначен на абонентский порт. Если флаг снят, то при поступлении входящего вызова производится анализ всех элементов URI (user, host и port – абонентский номер, IP-адрес и UDP/TCP-порт). При совпадении всех элементов URI вызов будет назначен на абонентский порт.

- *Передавать IP-адрес в заголовке Call-ID* – если флаг установлен, то в заголовке Call-ID при исходящей связи используется собственный IP-адрес устройства в формате localid@host.

Трехсторонняя конференция



- *Режим* – режим работы трехсторонней конференции. Возможно два режима:

  – *Локальная* – конференция собирается локально устройством после нажатия комбинации «flash+3»;
  – *Удаленная (RFC4579)* – конференция собирается на удаленном сервере, для чего после нажатия «flash+3» на сервер отправляется сообщение Invite на номер, указанный в поле «*Сервер конференции*». В этом случае конференция работает по алгоритму, описанному в RFC4579. Подробно данный алгоритм описан в пункте 3.3.2.

- *Сервер конференции* – в общем случае адрес сервера, осуществляющего установление конференции по алгоритму, описанному в RFC4579. Адрес задается в формате SIP-URI: user@address:port. Можно указать только пользовательскую часть URI (user) – в этом случае сообщение Invite отправится на адрес SIP-прокси.

Настройка IMS

- *Режим IMS* – режим работы с IMS. Возможно три режима:

  – Выключен – IMS не используется;
  – Без подписки - разрешено управление некоторыми видами услуг с сервера IMS (IP Multimedia Subsystem). В этом случае включение услуг «Трехсторонняя конференция» (работает только по алгоритму RFC4579), «Удержание вызова», «Ожидание вызова», «Горячая линия» (независимо от того, включены они или нет в конфигурации) производит удаленно сервер IMS посредством отправки сообщений Notify, в теле которых передаются команды на активацию/деактивацию услуг в формате XCAP (фактически – XML, RFC4825). При таком варианте запросы SUBSCRIBE после регистрации абонентов шлюзом не отправляются, обрабатываются только NOTIFY-запросы, принятые от IMS, с помощью которых происходит управление услугами;
  – С подпиской - разрешено управление некоторыми видами услуг с сервера IMS (IP Multimedia Subsystem). В этом случае включение услуг «Трехсторонняя конференция» (работает только по алгоритму RFC4579), «Удержание вызова»,

«Ожидание вызова», «Горячая линия» (независимо от того, включены они или нет в конфигурации) производит удаленно сервер IMS посредством отправки сообщений Notify, в теле которых передаются команды на активацию/деактивацию услуг в формате XCAP (фактически – XML, RFC4825). При таком варианте шлюз отправляет запросы SUBSCRIBE после регистрации абонентов и при успешной подписке обрабатывает NOTIFY-запросы, принятые от IMS, с помощью которых происходит управление услугами.

- *Имя услуги "Удержание вызова"* – название элемента XML в теле сообщения Notify, используемого для передачи команды активации/деактивации услуги «Удержание вызова». Например, если имя услуги имеет значение «call-hold», то команда активации будет выглядеть так:

  <call-hold active="true"/>

  а команда деактивации:

  <call-hold active="false"/>

- *Имя услуги "Ожидание вызова"* – название элемента XML в теле сообщения Notify, используемого для передачи команды активации/деактивации услуги «Ожидание вызова». Например, если имя услуги имеет значение «call-waiting», то команда активации будет выглядеть так:

  <call-waiting active="true"/>

  а команда деактивации:

  <call-waiting active="false"/>

- *Имя услуги "Трехсторонняя конференция"* – название элемента XML в теле сообщения Notify, используемого для передачи команды активации/деактивации услуги «Трехсторонняя конференция». Например, если имя услуги имеет значение «three-party-conference», то команда активации будет выглядеть так:

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

  а команда деактивации:

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

- *Имя услуги "Горячая линия"* – название элемента XML в теле сообщения Notify, используемого для передачи команды активации услуги «Горячая линия». В команде активации передаются номер телефона горячей линии и таймаут вызова. Например, если имя услуги имеет значение «hot-line-service», и необходимо совершать вызов на номер 30001 через 6 секунд после подъема трубки телефона - команда активации будет выглядеть так:

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

  Если команда активации не получена, услуга «Горячая линия» будет выключена.

- Имя *услуги "Передача вызова"* – название элемента XML в теле сообщения Notify, используемого для передачи команды активации/деактивации услуги «Трехсторонняя

конференция». Например, если имя услуги имеет значение «call-transfer», то команда активации будет выглядеть так:

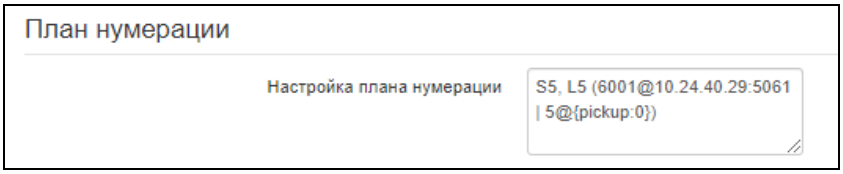
< call-transfer active="true"/>

а команда деактивации:

< call-transfer active="false"/>

По умолчанию если не пришла команда на активацию – все вышеперечисленные услуги деактивированы.

План нумерации



План нумерации задается при помощи регулярных выражений в поле «Настройка плана нумерации».

Ниже приводится структура и формат регулярных выражений, обеспечивающих различные возможности набора номера.

Структура регулярного выражения:

Sxx, Lxx ( ),
где
xx – произвольные значения таймеров S и L;
() – границы плана нумерации.

Основой являются обозначения для записи последовательности набранных цифр. Последовательность цифр записывается с помощью нескольких обозначений: цифры, набираемые с клавиатуры телефона: 0, 1, 2, 3, …, 9, # и *. **Использование символа # в плане нумерации может блокировать завершение набора с помощью этой клавиши!**

- Последовательность цифр, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символов.
  - Пример: ([1239]) – соответствует любой из цифр 1, 2, 3 или 9.
- Через тире может быть указан диапазон символов. Чаще всего используется внутри квадратных скобок.
  - Пример 1: (1-5) - любая цифра от 1 до 5.
  - Пример 2:([1-39]) - пример из предыдущего пункта с иной формой записи.
- Символ X соответствует любой цифре от 0 до 9.
  - Пример: (1XX) - любой трёхзначный номер, начинающийся на 1.
- «.» - повторение предыдущего символа от 0 до бесконечности раз.
- «+» - повторение предыдущего символа от 1 до бесконечности раз.

- {a,b} – повторение предыдущего символа от a до b раз;
- {a,} – повторение предыдущего символа не меньше a раз;
- {,b} – повторение предыдущего символа не больше b раз.
    - Пример: (810X.) - международный номер с любым количеством цифр.

Настройки, влияющие на обработку плана нумерации:

- *Interdigit Long Timer (буква «L» в записи плана нумерации)* - время ожидания ввода следующей цифры в том случае, если нет шаблонов, подходящих под набранную комбинацию;
- *Interdigit Short Timer (буква «S» в записи плана нумерации)* - время ожидания ввода следующей цифры, если с набранной комбинацией полностью совпадает хотя бы один шаблон, и при этом имеется еще хотя бы один шаблон, до полного совпадения с которым необходимо осуществить донабор номера.

Дополнительные возможности:

1. Замена набранной последовательности

Синтаксис: *<arg1:arg2>*

Данная возможность позволяет заменить набранную последовательность на любую последовательность набираемых символов. При этом второй аргумент должен быть указан определённым значением, оба аргумента могут быть пустыми.

- Пример: (<83812:> XXXXXX) - данная запись будет соответствовать набранным цифрам 83812, но эта последовательность будет опущена и не будет передана на SIP-сервер.

2. Вставка тона в набор

При выходе на межгород (в офисных станциях - на город) привычно слышать ответ станции, что можно реализовать вставкой запятой в нужную позицию последовательности цифр.

- Пример: (8, 770) - при наборе номера 8770 после цифры 8 будет выдан непрерывный тон.

3. Запрет набора номера.

Если в конце шаблона номера добавить восклицательный знак '!', то набор номеров, соответствующих шаблону, будет заблокирован.

- Пример: (8 10X xxxxxxx ! | 8 xxx xxxxxxx) – выражение разрешает набор только междугородних номеров и исключает международные вызовы.

4. Замена значений таймеров набора номера

Значения таймеров могут быть назначены как для всего плана нумерации, так и для определённого шаблона. Буква «S» отвечает за установку *«Interdigit Short Timer»*, а «L» - за *«Interdigit Long Timer»*. Значения таймеров могут быть указаны для всех шаблонов в плане нумерации, если значения перечислены до открывающейся круглой скобки.

- Пример: S4 (8XXX.) или S4,L8 (XXX)

Если эти значения указаны только в одной из последовательностей, то действуют только для неё. Также в этом случае не надо ставить двоеточие между ключом и значением таймаута, значение может быть расположено в любом месте шаблона.

- Пример: (S4 8XXX. | XXX) или ([1-5] XX S0) – запись вызовет мгновенную передачу вызова при наборе трехзначного номера, начинающегося на 1,2, … , 5.

5. Набор по прямому адресу (IP Dialing)

Символ «@», поставленный после номера, означает, что далее будет указан адрес сервера, на который будет отправлен вызов на набранный номер. Рекомендуется использовать *«IP Dialing»*, а также приём и передачу вызовов без регистрации *(«Call Without Reg», «Answer Without Reg»*). Это может помочь в случае отказа сервера.
Кроме того, формат адреса с IP Dialing может быть использован в номерах, предназначенных для переадресации звонков.

- Пример 1: (8 xxx xxxxxxx) - 11-значный номер, начинающийся на 8.
- Пример 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) - 11-значный номер, начинающийся на 8, если введён 7- значный, то добавить к передаваемому номеру 8495.
- Пример 3: (0[123] | 8 [2-9]xx [2-9]xxxxxx) - набор номеров экстренных служб, а так же некоторых междугородних номеров.
- Пример 4: (S0 <:82125551234>) - быстрый набор указанного номера, аналог режима «Hotline» на других шлюзах.
- Пример 5: (S5 <:1000> | xxxx) - данный план нумерации позволяет набрать любой номер, состоящий из цифр, а если ничего не введено в течение 5 секунд, вызвать номер 1000 (допустим, это секретарь).
- Пример 6: (*5x*xxxx*x#|*2x*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8, [2-9]xxxxxxxxx|8, 10x.|1xx<:@10.110.60.51:5060>).
- Пример 7: (1xx|0[1-9]|00[1-8]|*5x*xxxx*x#|*2x*xxxxxxxxxxx#|#xx#|[2-7]xxxxx|8, [2-9]xxxxxxxxx|8, 10x.).

Иногда может потребоваться совершать звонки локально внутри устройства. При этом если IP-адрес устройства не известен или периодически изменяется, удобно использовать в качестве адреса сервера зарезервированное слово «{local}», что означает отправку соответствующей последовательности цифр на собственный адрес устройства.

- Пример: (123@{local}) – вызов на номер 123 будет обработан локально внутри устройства.

6. Настройка кода перехвата

При помощи данной команды можно установить код перехвата для заданной группы.

Синтаксис: ABC@{pickup:X}, где

ABC – код перехвата (например *8),

X – номер группы перехвата (нумерация групп перехвата с 0).

- Пример: 112@{pickup:0} – абоненты А и Б состоят в одной группе перехвата с индексом 0. В случае если абоненту А поступает входящий вызов, то абонент Б может перехватить вызов, набрав комбинацию цифр 112.

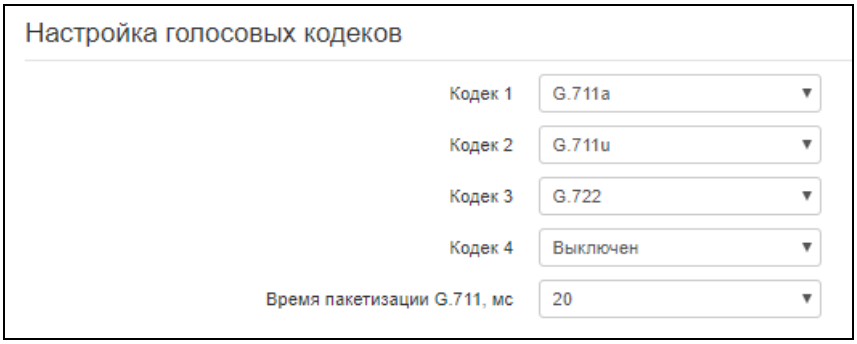
Установка профилей dialplan

Для каждого направления можно выбрать не более одного профиля dialplan, который будет определять параметры вызовов на этом направлении. Настройки профилей производятся в разделе

«Профили dialplan». Для каждого направления настройка альтернативного профиля указывается в круглых скобках после слова «profile:».

Пример:([23]xxx(profile:0)

Настройка голосовых кодеков



Сигнальный процессор устройства выполняет функции кодирования аналогового речевого трафика, данных факса/модема в цифровые сигналы, а также обратного декодирования. Шлюз поддерживает следующие голосовые кодеки: G.711A, G.711U, G.729, G723.1, G.726, G.722.

G.711 – представляет собой ИКМ-кодирование без сжатия речевой информации. Данный кодек должен быть обязательно поддержан всеми производителями VoIP-оборудования. Кодеки G.711A и G.711U отличаются друг от друга законом кодирования (A-закон – линейное кодирование и U-закон - нелинейное). Кодирование по U-закону применяется в Северной Америке, по A-закону – в Европе.

G.722 — широкополосный кодек, использующий АДИКМ с разделением на поддиапазоны и работающий со скоростью 48, 56 и 64 кбит/с.

G.723.1 – кодек со сжатием речевой информации, предусматривает два режима работы: 6.3 Кбит/с и 5.3 Кбит/с. Кодек G.723.1 имеет детектор речевой активности и обеспечивает генерацию комфортного шума на удаленном конце в период молчания.

G.726-24, G.726-32 - кодек со сжатием речевой информации по алгоритму АДИКМ и скоростью передачи 24 или 32 Кбит/с.

G.729 – также является кодеком со сжатием речевой информации и обеспечивает скорость передачи 8 Кбит/с. Аналогично кодеку G.723.1, кодек G.729 поддерживает детектор речевой активности и обеспечивает генерацию комфортного шума.

- *Кодек 1..7*– позволяет выбрать кодеки и порядок, в котором они будут использоваться. Кодек с наивысшим приоритетом нужно прописать в поле «Кодек 1». Для работы необходимо указать хотя бы один кодек:
  - *Выключен* - кодек не используется.
  - G.711a – использовать кодек G.711A;
  - G.711u – использовать кодек G.711U;
  - G.723 – использовать кодек G.723.1;
  - G.729(A, B) – использовать кодек G.729 annexA или G.729B;
  - G.726-24 - использовать кодек G.726 со скоростью 24 Кбит/с;
  - G.726-32 - использовать кодек G.726 со скоростью 32 Кбит/с;
  - G.722 - использовать кодек G.722.

- *Время пакетизации* – число миллисекунд речи в одном RTP-пакете (для кодеков G.711, G.729, G.723 и G.726).

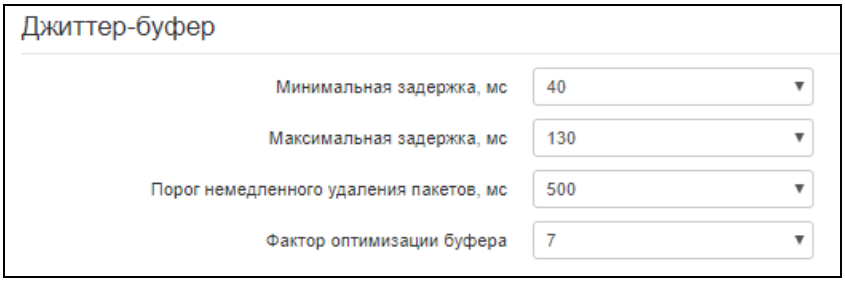
Могут быть заданы альтернативные голосовые кодеки для выбранного направления. Для каждого из направлений в плане нумерации есть возможность задания предпочтительного кодека для передачи речи. Для каждого направления дополнительные настройки кодеков указываются в круглых скобках после слова «codecs:».

Если необходимо использование нескольких кодеков, то их перечисляют через символ «,». Можно указывать несколько параметров для направления. В таком случае они должны быть разделены символом «;» - (param1:subparam1,subparam2;param2:subparam1,subparam2). Допустимые значения субпараметров subparamX: g711a, g711u, g729, g723.

Допустимые значения параметров param1 и param2 — codecs и rfc2833_PT соответственно.

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

Джиттер-буфер



Джиттер (jitter) — это неравномерность периодов времени, отведенных на доставку пакета. Задержка в доставке пакета и джиттер исчисляются в миллисекундах. Величина джиттера имеет большое значение при передаче информации в режиме реального времени (например, голос или видео).

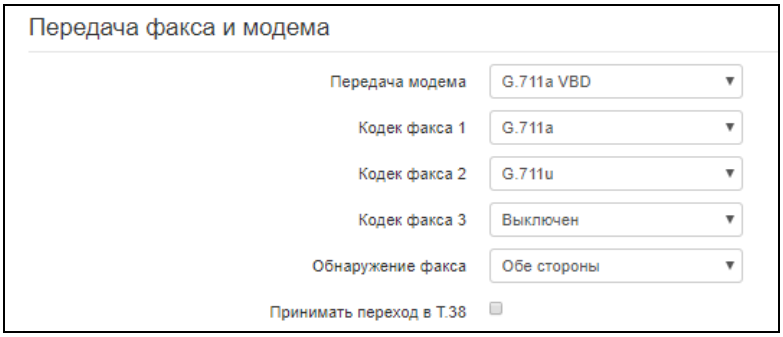
В протоколе RTP, который еще называют «протоколом потока передающей среды» (media stream), есть поле для метки точного времени передачи относительно всего RTP-потока. Принимающее устройство использует эти временные метки для выяснения того, когда следует ожидать пакет, соблюден ли порядок пакетов. Исходя из этой информации, приемная сторона выясняет, как следует настроить свои параметры, чтобы замаскировать потенциальные сетевые проблемы, такие как задержки и джиттер. Если ожидаемое время на доставку пакета от отправителя к приемнику на протяжении всего периода разговора строго равно определенному значению, например 50 мс, можно утверждать, что в такой сети джиттера нет. Но зачастую пакеты задерживаются в сети, и временной интервал доставки может колебаться в довольно большом (с точки зрения трафика, критичного ко времени) временном диапазоне. В случае если приложение-приемник такого звука или видео будет воспроизводить его в том временном порядке, в котором приходят пакеты, мы получим заметное ухудшения качества голоса (или видео). Например, если это касается голоса, то мы услышим прерывание в голосе и другие помехи.

Устройство имеет следующие настройки джиттер-буфера:

- *Минимальная задержка, мс* – минимальное ожидаемое время задержки распространения IP-пакета по сети;
- *Максимальная задержка, мс* – максимальное ожидаемое время задержки распространения IP-пакета по сети;

- *Порог немедленного удаления пакетов, мс* – максимальный промежуток времени, через который происходит удаление речевых пакетов из буфера. Значение данного параметра больше или равно максимальной задержке;
- *Фактор оптимизации буфера* – параметр, используемый для оптимизации размера джиттер-буфера. Рекомендуется выставлять его значение в 0.

Передача факса и модема



Передача факса может осуществляться с использованием речевого кодека 711 или специального кодека для передачи факсимильных сообщений T.38.

T.38 – стандарт, описывающий передачу факсимильных сообщений в реальном времени через IP-сети. Сигналы и данные, передаваемые факсимильным аппаратом, кодируются в пакеты протокола T.38. В формируемые пакеты может вводиться избыточность – данные из предыдущих пакетов, что позволяет осуществлять надежную передачу факса по нестабильным каналам.

- *Передача модема* – выбор кодека, который будет использоваться для передачи данных при детектировании шлюзом сигналов модема:
  - Выключен – не детектировать сигналы модема;
  - G.711a VBD – использовать кодек G.711A в режиме VBD;
  - G.711u VBD – использовать кодек G.711U в режиме VBD.

В режиме VBD (Voice Band Data) шлюз выключает детектор активности речи (VAD), генератор комфортного шума (CNG) и эхокомпенсаторы, что необходимо при установлении модемного соединения.

Выбранный кодек должен быть также активен в списке разговорных кодеков.

- *Кодек факса 1..3* – позволяет выбрать кодеки и порядок, в котором они будут использоваться. Кодек с наивысшим приоритетом нужно прописать в поле «Кодек факса 1». Для работы необходимо указать хотя бы один кодек:
  - *Выключен* – кодек не используется.
  - G.711a – использовать кодек G.711A;
  - G.711u – использовать кодек G.711A;
  - T.38 – использовать протокол T.38.

Все кодеки факса должны быть разными! Кроме этого при выборе G.711a или G.711u соответствующий кодек должен быть активен в списке разговорных кодеков устройства.

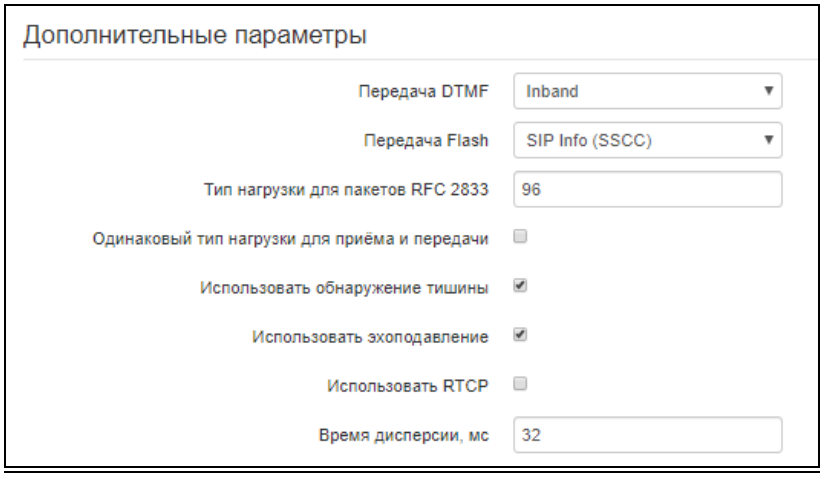
- *Обнаружение факса* – определяет направление вызова, при котором разрешено детектировать тоны факса, после чего будет осуществлять переход на кодек факса:

- *Не детектировать тоны факса* – отключает детектирование тонов факса, но не запрещает передачу факса (не будет инициироваться переход на кодек факса, но данный переход может быть сделан встречным шлюзом);
- *Обе стороны* – детектируются тоны как при передаче факса, так и при приеме. При передаче факса детектируется сигнал CNG FAX с абонентской линии. При приеме факса детектируется сигнал V.21 с абонентской линии;
- *Вызывающая* – детектируются тоны только при передаче факса. При передаче факса детектируется сигнал CNG FAX с абонентской линии;
- *Вызываемая* – детектируются тоны только при приеме факса. При приеме факса детектируется сигнал V.21 с абонентской линии.

- *Принимать переход в T.38* – при установленном флаге разрешен входящий re-invite на T.38 от встречного шлюза;

- *Размер избыточности T.38 Redundancy* – добавление избыточности в пакеты T.38, значение соответствует количеству предыдущих пакетов, которое дублируется в каждом новом пакете T.38. Такой способ избыточности используется в случае потери пакетов при передаче.

Дополнительные параметры



- *Передача DTMF* – способ передачи сигналов DTMF:

  - *Inband* – внутриполосная передача;
  - *RFC2833* – согласно рекомендации RFC2833 в качестве выделенной нагрузки в речевых пакетах RTP;
  - *SIP info* – передача сообщений по протоколу SIP в запросах INFO.

- *Передача Flash* – способ передачи Flash:

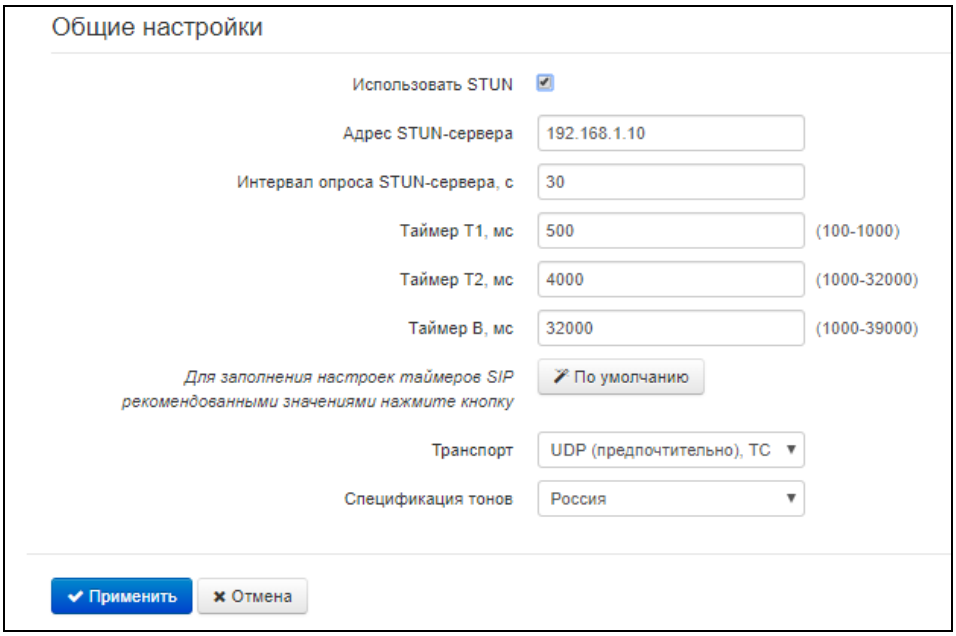
  - *SIP info* (Hookflash) – передача сообщений на взаимодействующую сторону по протоколу SIP в запросах INFO. Событие *flash* передается в расширении *Application/Hook Flash* как *signal=hf*;
  - *SIP info (DTMF Relay)* – передача сообщений на взаимодействующую сторону по протоколу SIP в запросах INFO. Событие *flash* передается в расширении *Application/dtmf-relay* как *signal=hf;*
  - *SIP info (Broadsoft)* – передача сообщений на взаимодействующую сторону по протоколу SIP в запросах INFO. Событие *flash* передается в расширении *Application/Broadsoft* как *event flashhook*;
  - SIP info (SSCC) – передача сообщений на взаимодействующую сторону по протоколу SIP в запросах INFO. Событие *flash* передается в расширении *Application/sscc* как *event flashhook*.

В текущей версии ПО передача Flash возможна только по протоколу SIP.

- *Тип нагрузки для пакетов RFC2833* – тип нагрузки для передачи пакетов по RFC2833 (разрешенные для использования значения – от 96 до 127);
- *Одинаковый тип нагрузки для приёма и передачи* – опция используется при исходящем вызове для согласования типа нагрузки событий, передаваемых по RFC2833 (DTMF и Flash). При установленном флаге передача и прием событий по RFC2833 осуществляется с нагрузкой из принятого от встречной стороны сообщения 200Ok. При снятом флаге передача событий по RFC2833 осуществляется с нагрузкой из принятого 200Ok, а приём – с типом нагрузки из собственной конфигурации (указывается в исходящем Invite);
- *Использовать обнаружение тишины* – при установленном флаге использовать детектор тишины;
- *Использовать эхоподавление* – при установленном флаге использовать эхоподавление;
- *Использовать RTCP* – при установленном флаге использовать протокол RTCP для контроля за разговорным каналом:
  - *Интервал передачи* – интервал передачи пакетов RTCP, сек;
  - *Период приема* – период приёма сообщения RTCP измеряется в единицах интервала передачи; если по истечении периода приёма от встречной стороны не будет получено ни одного RTCP-пакета – *TAU-4M.IP* разрывает соединение.
  - *RTCP-XR* — при установленном флаге будут отправляться пакеты RTCP Extended Reports в соответствии с RFC 3611.
- *Время дисперсии, мс* – параметр, позволяющий бороться с эхом, вызванным дисперсией речевого сигнала. Значения параметра изменяются в промежутке от 2 до 128 мс.

Для сохранения изменений нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

Общие настройки профилей SIP



- *Использовать STUN* – при установленном флаге используется протокол STUN (Session Traversal Utilities for NAT) для определения публичного адреса устройства (внешнего адреса NAT). Рекомендуется использовать данный протокол при работе устройства через NAT;

- *Адрес STUN-сервера* – IP-адрес или доменное имя сервера STUN, через двоеточие можно ввести альтернативный порт сервера (по умолчанию 3478);

- *Интервал опроса STUN-сервера, с* – интервал, по истечении которого отправляется запрос на сервер STUN. Чем меньше интервал опроса, тем выше скорость реакции на изменение публичного адреса.

  – *Таймер T1, мс* – интервал между посылкой первого INVITE и второго при отсутствии ответа на первый в мс, для последующих INVITE (третьего, четвертого и т.д.) данный интервал увеличивается вдвое (например, при значении 300 мс второй INVITE будет передан через 300 мс, третий – через 600 мс, четвертый – через 1200 мс и т.д.);
  – *Таймер T2, мс* — максимальный интервал для перепосылки не-INVITE запросов и ответов на INVITE-запросы;
  – *Таймер B, мс* – общий таймаут передачи сообщений INVITE в мс. По истечении данного таймаута определяется, что направление недоступно. Используется для ограничения ретрансляций сообщений INVITE, в том числе для определения доступности;

- *Транспорт* – выбор протокола для транспортировки сообщений протокола SIP;

- *Спецификация тонов* - выбор страны для определения используемого набора тонов.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.3.5 Подменю «Профили dialplan»

В этом подменю можно настроить профили вызова для использования на различных направлениях.

Всего можно настроить 4 профиля dialplan.

Редактирование профиля dialplan

Редактирование профиля dialplan 0

Кодеки

Кодек 1	G.711a
Кодек 2	G.729
Кодек 3	G.711u
Кодек 4	G.723
Кодек 5	G.726-24
Кодек 6	G.726-32
Кодек 7	G.722
Время пакетизации G.711, мс	20
Время пакетизации G.729, мс	20
Время пакетизации G.723, мс	30
Время пакетизации G.726-24, мс	20
Время пакетизации G.726-32, мс	20
Тип нагрузки G.726-24	103
Тип нагрузки G.726-32	104

Передача факса и модема

Передача модема	G.711a VBD
Кодек факса 1	G.711a
Кодек факса 2	G.711u
Кодек факса 3	Выключен
Принимать переход в T.38	☐

Дополнительные параметры

Передача DTMF	RFC 2833
Тип нагрузки для пакетов RFC 2833	96
Использовать обнаружение тишины	☑
Использовать эхоподавление	☑
Время дисперсии, мс	32
Максимальное количество вызовов	12

Джиттер-буфер

Минимальная задержка, мс	40
Максимальная задержка, мс	130
Фактор оптимизации буфера	7
Порог немедленного удаления пакетов, мс	500
Одинаковый тип нагрузки для приёма и передачи	☐
Автоматическое усиление на приеме	☐
Уровень усиления приема	-25 дБ
Автоматическое усиление на передаче	☐
Уровень усиления передачи	-25 дБ

✔ Применить ✖ Отмена

Кодеки

- *Кодек 1..7* – позволяет выбрать кодеки и порядок, в котором они будут использоваться. Кодек с наивысшим приоритетом нужно прописать в поле «Кодек 1». Для работы необходимо указать хотя бы один кодек:
  - Выключен - кодек не используется.
  - G.711a – использовать кодек G.711A;
  - G.711u – использовать кодек G.711U;
  - G.723 – использовать кодек G.723.1;
  - G.729(A, B) – использовать кодек G.729 annexA или G.729B;
  - G.726-24 - использовать кодек G.726 со скоростью 24 Кбит/с;
  - G.726-32 - использовать кодек G.726 со скоростью 32 Кбит/с;
  - G.722 - использовать кодек G.722.
- *Время пакетизации* – число миллисекунд речи в одном RTP-пакете (для кодеков G.711A, , G.729, G.723 и G.726).
- *Тип нагрузки* - тип динамической нагрузки для кодека G.726-24 или G.726-32 (разрешенные для использования значения – от 96 до 127).

Передача факса и модема

- *Передача модема* – выбор кодека, который будет использоваться для передачи данных при детектировании шлюзом сигналов модема:
  - Выключен – не детектировать сигналы модема;
  - G.711a VBD – использовать кодек G.711A в режиме VBD;
  - G.711u VBD – использовать кодек G.711U в режиме VBD.

В режиме VBD (Voice Band Data) шлюз выключает детектор активности речи (VAD), генератор комфортного шума (CNG) и эхокомпенсаторы, что необходимо при установлении модемного соединения.

Выбранный кодек должен быть также активен в списке разговорных кодеков.

- *Кодек факса 1..3* – позволяет выбрать кодеки и порядок, в котором они будут использоваться. Кодек с наивысшим приоритетом нужно прописать в поле «Кодек факса 1». Для работы необходимо указать хотя бы один кодек:
  - Выключен – кодек не используется.
  - G.711a – использовать кодек G.711A;
  - G.711u – использовать кодек G.711A;
  - T.38 – использовать протокол T.38.

Все кодеки факса должны быть разными! Кроме этого, при выборе G.711a или G.711u соответствующий кодек должен быть активен в списке разговорных кодеков устройства.

- *Принимать переход в T.38* – при установленном флаге разрешен входящий *re-invite* на T.38 от встречного шлюза;
- *Размер избыточности T.38 Redundancy* – добавление избыточности в пакеты T.38, значение соответствует количеству предыдущих пакетов, которое дублируется в каждом новом *пакете T.38.* Такой способ избыточности необходим в случае потери пакетов при передаче.

Дополнительные параметры

- *Передача DTMF* – способ передачи сигналов DTMF:
  - *Inband* – внутриполосная передача;
  - *RFC2833* – согласно рекомендации RFC2833 в качестве выделенной нагрузки в речевых пакетах RTP;
  - *SIP info* – передача сообщений по протоколу SIP в запросах INFO.
- *Тип нагрузки для пакетов RFC2833* – тип нагрузки для передачи пакетов по RFC2833 (разрешенные для использования значения – от 96 до 127);
- *Использовать обнаружение тишины* – при установленном флаге использовать детектор тишины;
- *Использовать эхоподавление* – при установленном флаге использовать эхоподавление;
- *Время дисперсии, мс* – параметр, позволяющий бороться с эхом, вызванным дисперсией речевого сигнала. Значения параметра изменяются в промежутке от 2 до 128 мс.
- *Максимальное количество вызовов* — этот параметр позволяет установить ограничение на количество одновременных вызовов на направлении.

Джиттер-буфер

- *Минимальная задержка, мс* – минимальное ожидаемое время задержки распространения IP-пакета по сети;
- *Максимальная задержка, мс* – максимальное ожидаемое время задержки распространения IP-пакета по сети;
- *Порог немедленного удаления пакетов, мс* – максимальный промежуток времени, через который происходит удаление речевых пакетов из буфера. Значение данного параметра больше или равно максимальной задержке (допустимые значения от 0 до 500, но не менее значения максимального буфера джиттера);
- *Фактор оптимизации буфера* – параметр, используемый для оптимизации размера джиттер-буфера. Рекомендуется выставлять его значение в 0;
- *Одинаковый тип нагрузки для приёма и передачи* – при установленном флаге использовать одинаковый тип нагрузки для приема и передачи;
- *Автоматическое усиление на приёме* – если флаг установлен, то принимаемый сигнал будет усилен до заданного уровня (максимальное усиление сигнала +/- 15дБ), иначе усиление производиться не будет;
- *Уровень усиления приёма* – определяет значение уровня, до которого будет усиливаться аналоговый сигнал при приеме (допустимы значения -25, -22, -19, -16, -13, -10, -7, -4, -1 дБ);
- *Автоматическое усиление на передаче* – если флаг установлен, то передаваемый сигнал будет усилен до заданного уровня (максимальное усиление сигнала +/- 15дБ), иначе усиление производиться не будет;
- *Уровень усиления передачи* – определяет значение уровня, до которого будет усиливаться аналоговый сигнал при передаче (допустимы значения -25, -22, -19, -16, -13, -10, -7, -4, -1 дБ).

2.6.3.6 Подменю «Группы вызова»

В подменю «Группы вызова» выполняется управление группами вызовов.

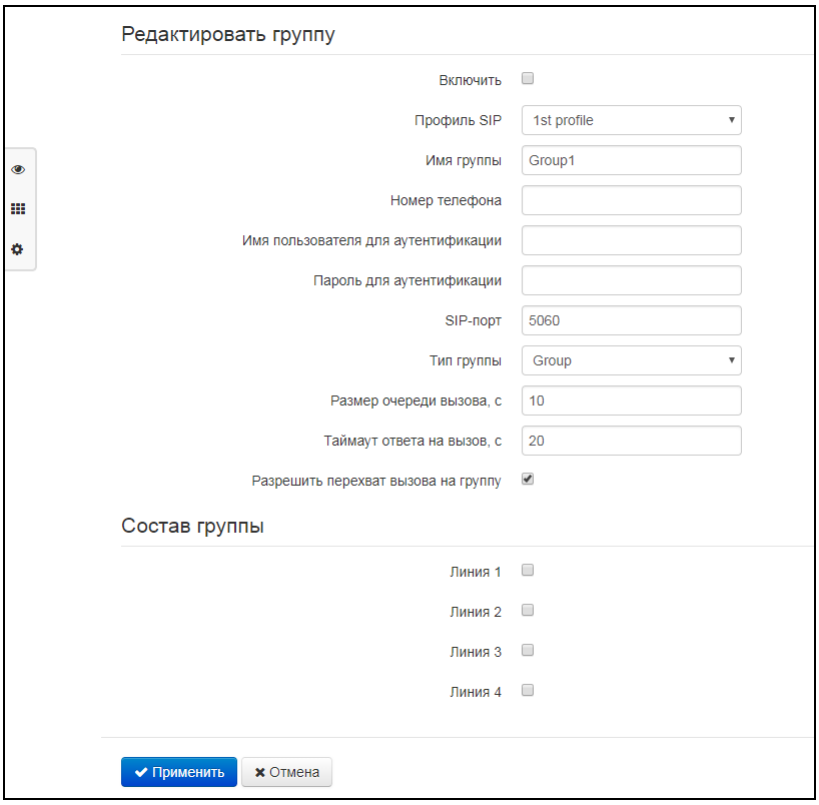
Группы вызова предназначены для выполнения функций центра обработки вызовов. Устройством поддерживается 3 режима работы групп вызова:

- *Групповой (Group)* – режим, при котором вызов поступает на все свободные порты группы одновременно. При ответе одного из участников группы вызов на остальные порты прекращается;

- *Задержанный групповой (Serial)* – режим, при котором вызов поступает на первый свободный в списке группы порт, затем, через определенный промежуток времени (*Таймаут вызова следующего порта*), к основному добавляется следующий свободный в списке порт и т.д. При ответе одного из участников группы, вызов на остальные порты прекращается;
- *Поисковый (Cyclic)* – режим, при котором по таймауту (*Таймаут вызова следующего порта*) последовательно выбирается свободный участник из состава группы, и на этот номер переходит вызов.

- *Имя группы* – название группы вызова;
- *Статус* – состояние группы вызова: включен, выключен;
- *Профиль* – SIP-профиль, используемый группой вызова;
- *Номер телефона* – номер телефона группы вызова;
- *Состав группы* – список линий (портов), которые входят в группу вызова.

Для выполнения настроек группы вызова нажмите на соответствующую ссылку в колонке «*Имя группы*»:



- *Включить* – при установленном флаге использовать группу;

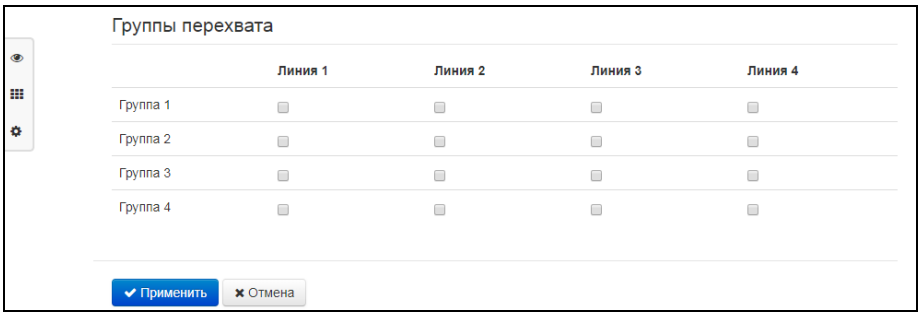
- *Профиль* – SIP-профиль, назначенный группе вызова. Настройки профиля выполняются в разделе «*IP-телефония -> Профили»*;
- *Имя группы* – идентификационное имя группы;
- *Номер телефона* – телефонный номер группы вызова;
- *Имя пользователя для аутентификации* – имя пользователя, которое используется для аутентификации на SIP-сервере;
- *Пароль для аутентификации* – пароль для аутентификации на SIP-сервере;
- *SIP порт* – альтернативный SIP-порт группы (по умолчанию 5060);
- *Тип группы* – тип группы вызова:
  - *Group* – сигнал вызова подается на все порты в группе одновременно;
  - *Serial* – количество портов, на которые подается вызывной сигнал, увеличивается на один по истечении таймаута вызова следующего порта;
  - *Cyclic* – сигнал вызова через интервал, равный таймауту вызова следующего порта, подается по очереди на каждый порт в группе. При достижении последнего порта в группе обзвон продолжается вновь с первого порта;
- *Таймаут вызова следующего порта, с* – опция используется группами типа «serial» и «cyclic» и задает интервал времени в секундах, через который осуществляется вызов следующего/следующих портов;
- *Размер очереди вызовов* – настройка позволяет ограничить максимальное число неотвеченных вызовов в очереди группы вызова. Поступивший вызов не ставится в очередь, если в группе есть свободные порты;
- *Таймаут ответа на вызов, с* – если не будет ответа на групповой вызов по истечении данного интервала времени, вызов сбрасывается;
- *Разрешить перехват вызова на группу* – при установленном флаге разрешен перехват вызова, поступившего на группу. Перехват вызова возможен, только если абоненты группы вызова принадлежат одной группе перехвата (2.6.3.1 Подменю «Группы перехвата»);
- *Состав группы* – при установленном флаге линия (порт) будет входить в состав данной группы вызова.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

2.6.3.7 Подменю «Группы перехвата»

Подменю «*Группы перехвата*» служит для настройки групп перехвата вызова.

Группа перехвата вызова – группа абонентов, уполномоченных принимать (перехватывать) любой вызов, направленный на другого абонента, входящего в группу. То есть, каждый абонент, принадлежащий группе, может перехватить вызов, поступивший на любого другого абонента данной группы путем набора кода перехвата. Настройка кода перехвата осуществляется в пункте *«План нумерации»* подменю *«Профили»*.



Для добавления/удаления линии установите/снимите флаг напротив заданной группы.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

Использование услуги:

На телефонный аппарат абонента, принадлежащего группе перехвата, поступает вызов. Если абонент не может ответить на вызов – другой абонент, также принадлежащий этой группе и использующий тот же профиль SIP, может перехватить поступивший вызов. Для этого он должен набрать код перехвата, после чего произойдет соединение с вызывающим абонентом.

Обратите внимание, что перехват вызова возможен только в том случае, если вызываемый и перехватывающий вызов абоненты используют один и тот же SIP-профиль.

Группа перехвата может использоваться совместно с группой вызова, для этого все порты, принадлежащие группе вызова, должны принадлежать группе перехвата. В этом случае любой порт, принадлежащий группе перехвата, может перехватить вызов, поступивший на групповой номер.

Если абонент набирает код перехвата в момент, когда на группу или телефонный порт не поступает ни одного вызова – абоненту будет выдан сигнал «Занято».

2.6.3.8 Подменю «Префиксы управления ДВО»

В подменю «Префиксы управления ДВО» настраиваются коды, набираемые с телефонного аппарата, для активации или деактивации услуг ДВО.

Абонент может управлять состоянием услуг со своего телефонного аппарата. Доступны следующие функции:

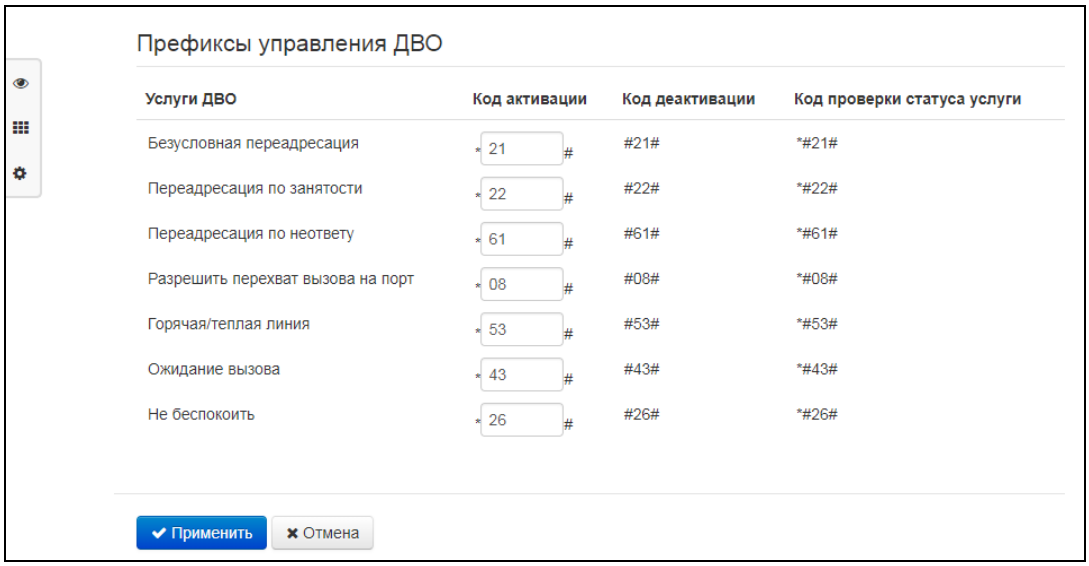
- активация услуги – * код_услуги #;
- проверка активности услуги – *# код_услуги #;
- отмена услуги - # код_услуги #;

Для активации услуг «Безусловная переадресация», «Переадресация вызова по занятости», «Переадресация по неответу», «Горячая/теплая линия» требуется ввести номер телефона:

* код_услуги * номер_телефона #

После ввода кода активации или отмены услуги абонент услышит сигнал «Подтверждение» (3 коротких сигнала), который говорит о том, что услуга успешно активирована или отменена.

После ввода кода проверки услуги абонент может услышать либо сигнал «Ответ станции» (непрерывный сигнал), либо сигнал «Занято» (короткие гудки). Сигнал «Ответ станции» говорит о том, что услуга включена и активирована, сигнал «Занято» – услуга выключена.



Управление абонентским сервисом

- *Услуги ДВО* – список услуг ДВО:
  - *Безусловная переадресация* – услуга, при активации которой все вызовы, поступившие абоненту, перенаправляются на заданный номер;
  - *Переадресация вызова по занятости* – услуга, при активации которой все вызовы, поступившие абоненту, в случае его занятости перенаправляются на заданный номер;
  - *Переадресация по неответу* – услуга, при активации которой все вызовы, поступившие абоненту, перенаправляются на заданный номер при неответе абонента в течение определенного времени;
  - *Разрешить перехват вызова на порт* – если услуга активирована абонентом – поступившие на него вызовы могут быть перехвачены другими абонентами из той же группы перехвата;
  - Горячая/теплая линия – при активации услуги, после поднятия трубки через установленный интервал времени происходит автоматический набор заданного номера;
  - *Ожидание вызова* – активация услуги позволяет абоненту в состоянии разговора получать уведомление о новом поступившем вызове. Абонент может принять, отклонить или игнорировать ожидающий вызов;
  - *Не беспокоить* – услуга позволяет абоненту временно ограничить все входящие вызовы.

- *Код активации* – код для активации услуги;
- *Код деактивации* – код для деактивации услуги;
- *Код проверки статуса услуги* – код для контроля активности услуги;

Код деактивации и код проверки статуса услуги заполняются автоматически на основании кода активации.

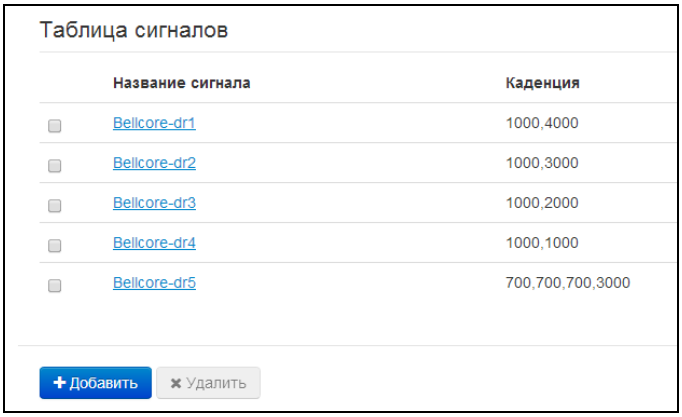
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.3.9 Подменю «Сигналы вызова»

В подменю «*Сигнал вызова*» осуществляется настройка альтернативного сигнала посылки вызова (каденции) в зависимости от значения заголовка Alert-Info во входящем Invite. Значение каденции для каждого сигнала вызова задаётся в виде последовательности чередующихся длительностей импульса и пауз, разделенных символом "," или ";". Значение длительности импульса/паузы задается в миллисекундах и должно быть кратно 100. Минимальная длительность импульса/паузы составляет 200мс, максимальная - 8000 мс.

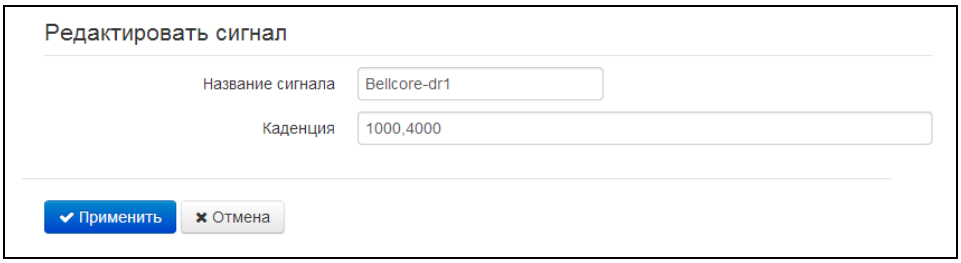
Для того чтобы привязать определённую каденцию к значению заголовка Alert-Info во входящем Invite, необходимо в соответствующем профиле SIP активировать флаг *«Обрабатывать заголовок Alert-Info»*, а в настройках каденции указать название сигнала в поле «Название сигнала» (например, Example-cadence). Каденция будет проиграна в линию, если во входящем Invite заголовок Alert-Info будет иметь значение <http://127.0.0.1/Example-cadence>.

Если каденция по заголовку Alert-Info не найдена, будет произведена попытка найти каденцию по номеру вызывающего абонента. При отсутствии последней выдается стандартный сигнал вызова с каденцией "1000,4000".



Для редактирования определенного сигнала нажмите на соответствующую ссылку в колонке «*Название сигнала*».

Для добавления сигнала нажмите кнопку «*Добавить*» и выполните следующие настройки:

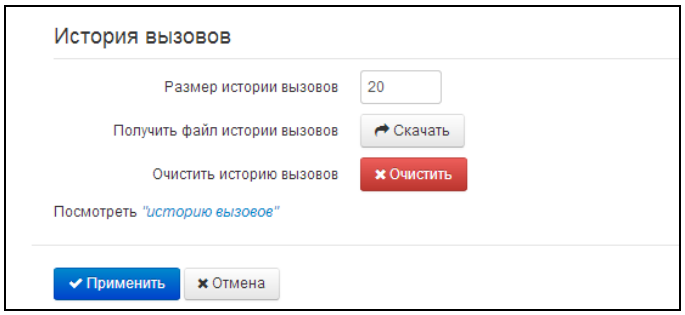


- Название сигнала – имя сигнала;
- Каденция – длительность подачи вызывного напряжения на телефонный аппарат и (через запятую/точку с запятой) длительность паузы между сигналами вызова, оба значения должны быть кратны 100 мс, минимальное значение 200мс, максимальное – 8000 мс;

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.3.10 Подменю «История вызовов»

В подменю «*История вызовов*» производится настройка ведения хронологии вызовов.



- *Размер истории вызовов* – максимальное количество записей в журнале, принимает значения от 0 до 10000 строк. Значение «0» отключает ведение истории вызовов. При достижении установленного ограничения в журнале каждая последующая запись удалит самую старую запись в начале журнала;
- *Получить файл истории вызовов* – для сохранения файла «voip_history» на локальном ПК нажмите на кнопку «Скачать»;
- *Очистить историю вызовов* – для очистки истории вызовов нажмите на кнопку «Очистить»;

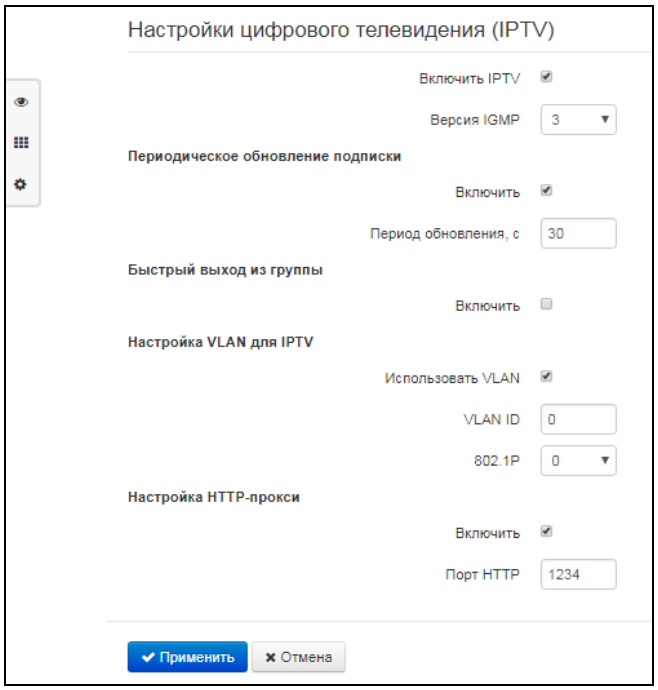
Для просмотра истории вызовов перейдите по ссылке *«Посмотреть “историю вызовов”»*. Описание мониторинга параметров приведено в разделе 2.7.10 Подменю «История вызовов».

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.4 Меню «IP-телевидение»

2.6.4.1 Подменю «IPTV»

В подменю «*IPTV*» выполняются настройки для работы сервиса «IP-телевидение».



- *Включить IPTV* – при установленном флаге разрешена трансляция сигналов IP-телевидения с WAN-интерфейса *TAU-4M.IP* (из сети провайдера) на устройства, подключенные к LAN-интерфейсу;
- *Версия IGMP* – версия протокола IGMP для отправки IGMP-сообщений с WAN-интерфейса (сообщений активации или деактивации подписки на каналы IP-телевидения). Поддерживаются версии 2 и 3.

Периодическое обновление подписки

- *Включить* – при включенной опции происходит периодическая отправка с WAN-интерфейса сообщений со списком активных IPTV-каналов на вышестоящий сервер, осуществляющий трансляцию сигналов IP-телевидения. Включение функции периодического обновления подписки необходимо, если вышестоящий сервер отключает трансляцию IPTV-каналов через определенный интервал времени;
  - *Период обновления, с* – период отправки сообщений со списком активных IPTV-каналов, в секундах. Установите величину периода обновления в значение, меньшее, чем таймаут отключения трансляции сигнала вышестоящим сервером.

Быстрый выход из группы

- *Включить* – при установленном флаге включен режим быстрого выхода из группы. Данная функция уменьшает задержку устройства на переключение между многоадресными потоками (отключение потока происходит сразу после получения от клиента сообщения «Leave Group» без дополнительного переспроса). Не рекомендуется использовать данный режим, когда к одному порту LAN подключено более одного приёмника IPTV.

Настройка VLAN для IPTV

- *Использовать VLAN* – при установленном флаге использовать для услуги IPTV выделенный VLAN (номер VLAN может совпадать с номером VLAN для услуги Интернет или STB), иначе для IPTV будет использоваться интерфейс услуги Интернет. Эта настройка позволяет определить интерфейс для приёма IPTV-сигналов из внешней сети;
  - *VLAN ID* – идентификационный номер VLAN для приёма сигналов IP-телевидения;
  - *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет). Используется в работе алгоритмов обеспечения качества сервиса (QoS).

Настройка HTTP-прокси

- *Включить* – при установленном флаге включена функция HTTP-прокси. HTTP-прокси осуществляет преобразование UDP-потока в поток HTTP, использующий протокол TCP (протокол надежной доставки пакетов), что позволяет улучшить качество транслируемого изображения при плохом качестве канала связи в локальной сети;
- *Порт HTTP* – номер порта HTTP-прокси, с которого будет осуществляться транслирование видео-потока. Используйте этот порт для подключения к транслируемым устройством *TAU-4M.IP* потокам IPTV.

Например, если *TAU-4M.IP* имеет на LAN-интерфейсе адрес 192.168.0.1, для порта прокси-сервера выбрано значение 2345, и необходимо воспроизвести канал 227.50.50.100, транслирующийся на UDP-порт 1234 – для программы VLC адрес потока нужно задать в виде: http://@192.168.0.1:2345/udp/227.50.50.100:1234.

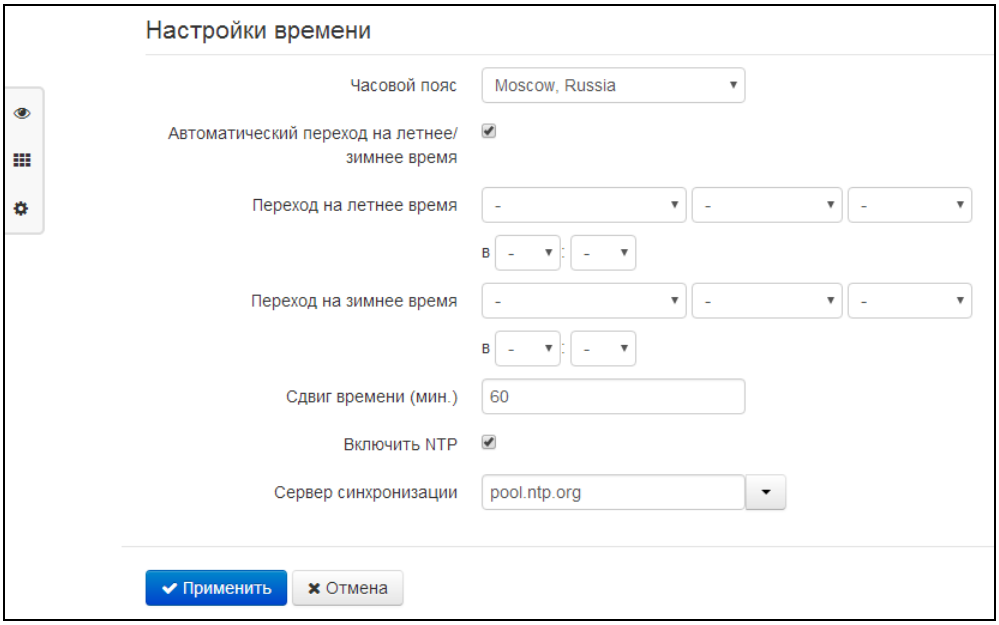
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.5 Меню «Система»

В меню «*Система*» выполняются настройки системы, времени, доступа к устройству по различным протоколам, производится смена пароля и обновление программного обеспечения устройства.

2.6.5.1 Подменю «Время»

В подменю «*Настройки времени*» выполняется настройка протокола синхронизации времени (NTP).



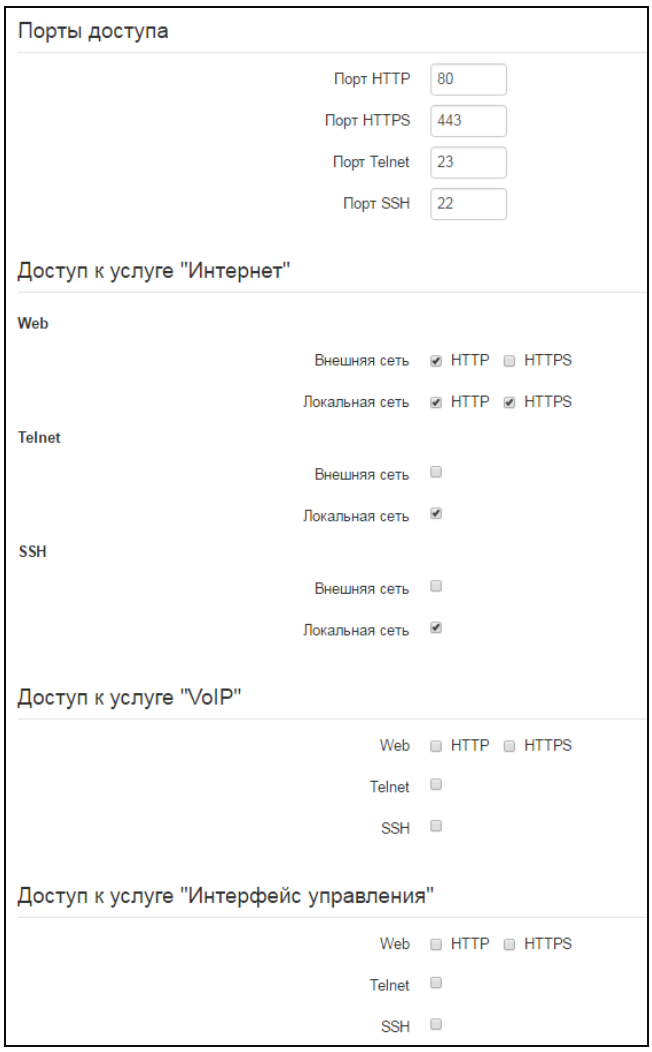
Настройки времени

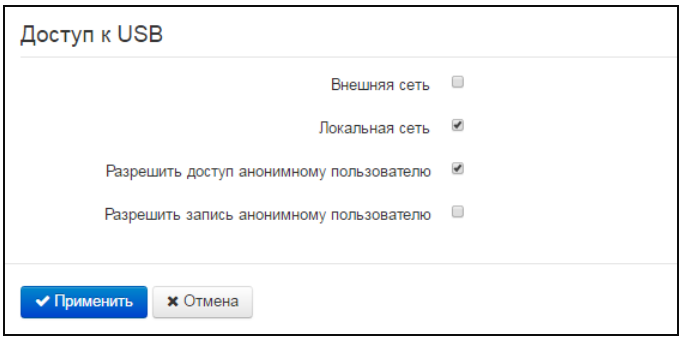
- *Часовой пояс* – позволяет установить часовой пояс в соответствии с ближайшим городом в Вашем регионе из заданного списка;
- *Автоматический переход на летнее/зимнее время* – при установленном флаге переход на летнее/зимнее время будет выполняться автоматически в заданный период времени:
  - *Переход на летнее время* – день, когда будет выполняться переход на летнее время;
  - *Переход на зимнее время* – день, когда будет выполняться переход на зимнее время;
  - *Сдвиг времени (мин.)* – период времени в минутах, на который выполняется сдвиг времени.
- *Включить NTP* – установите флаг, если необходимо включить синхронизацию системного времени устройства с определенного сервера NTP;
- *Сервер синхронизации* – IP-адрес/доменное имя сервера синхронизации времени. Возможен ручной ввод адреса сервера или выбор из списка.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.5.2 Подменю «Доступ»

В подменю «*Доступ*» настраивается доступ к устройству посредством Web-интерфейса, Telnet и SSH, а также доступ по протоколу FTP к накопителю, подключенному к порту USB.





Порты доступа

В данном разделе выполняется настройка TCP-портов для доступа к устройству по протоколам HTTP, HTTPS, Telnet, SSH.

- *Порт HTTP* – номер порта для доступа к Web-интерфейсу устройства по протоколу *HTTP*, по умолчанию – 80;
- *Порт HTTPS* – номер порта для доступа к Web-интерфейсу устройства по протоколу *HTTPS* (*HTTP Secure* – безопасное подключение), по умолчанию – 443;

- *Порт Telnet* – номер порта для доступа к устройству по протоколу *Telnet*, по умолчанию – 23;
- *Порт SSH* – номер порта для доступа к устройству по протоколу *SSH*, по умолчанию – 22.

По протоколам *Telnet* и *SSH* осуществляется доступ к командной строке (консоль linux). Имя пользователя/пароль для подключения к консоли: admin/password.

Доступ к услуге Интернет

Для получения доступа к устройству с интерфейсов услуги Интернет установите соответствующие разрешения:

Web, Внешняя сеть:

- *HTTP* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через WAN-порт по протоколу HTTP (небезопасное подключение);
- *HTTPS* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через WAN-порт по протоколу HTTPS (безопасное подключение).

Web, Локальная сеть:

- *HTTP* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через LAN-порт по протоколу HTTP (небезопасное подключение);
- *HTTPS* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через LAN-порт по протоколу HTTPS (безопасное подключение).

Telnet:

Telnet – протокол, предназначенный для организации управления по сети. Позволяет удаленно подключиться к шлюзу с компьютера для настройки и управления.

Для разрешения доступа к устройству по протоколу Telnet из внешней (через WAN-порт) или внутренней (через LAN-порт) сети установите соответствующие флаги.

SSH:

SSH – безопасный протокол удаленного управления устройствами. В отличие от Telnet, протокол SSH шифрует весь трафик, включая передаваемые пароли.

Для разрешения доступа к устройству по протоколу SSH из внешней (через WAN-порт) или внутренней (через LAN-порт) сети установите соответствующие флаги.

Доступ к услуге *VoIP*:

В данном разделе осуществляется настройка доступа к интерфейсу услуги VoIP (интерфейс услуги VoIP настраивается на странице IP-телефония – Настройка сети) через Web (протоколы HTTP или HTTPS), а также по протоколам Telnet и SSH. Для разрешения доступа по какому-либо из указанных протоколов установите соответствующие флаги.

Доступ к услуге *Интерфейс управления*:

Раздел позволяет настроить доступ для управления устройством, используя протоколы HTTP, HTTPS, Telnet или SSH. Настройка интерфейса производится на странице **Система** – **VLAN управления**. Для разрешения доступа по какому-либо из указанных протоколов установите соответствующие флаги.

Для авторизации по протоколам Telnet и SSH по умолчанию используются имя пользователя *admin* и пароль *password*. После авторизации становится доступна консоль операционной системы Linux с возможностью использования основных команд командного интерпретатора shell.

Доступ к USB:

В данном разделе осуществляется настройка доступа к устройству, подключенному к USB-порту, по протоколу FTP.

Для разрешения доступа к подключенному USB-устройству по протоколу FTP из внешней (через WAN-порт) или внутренней (через LAN-порт) сети установите соответствующие флаги.

Для разрешения доступа к подключенному USB-устройству анонимному пользователю установите флаг «Разрешить доступ анонимному пользователю».

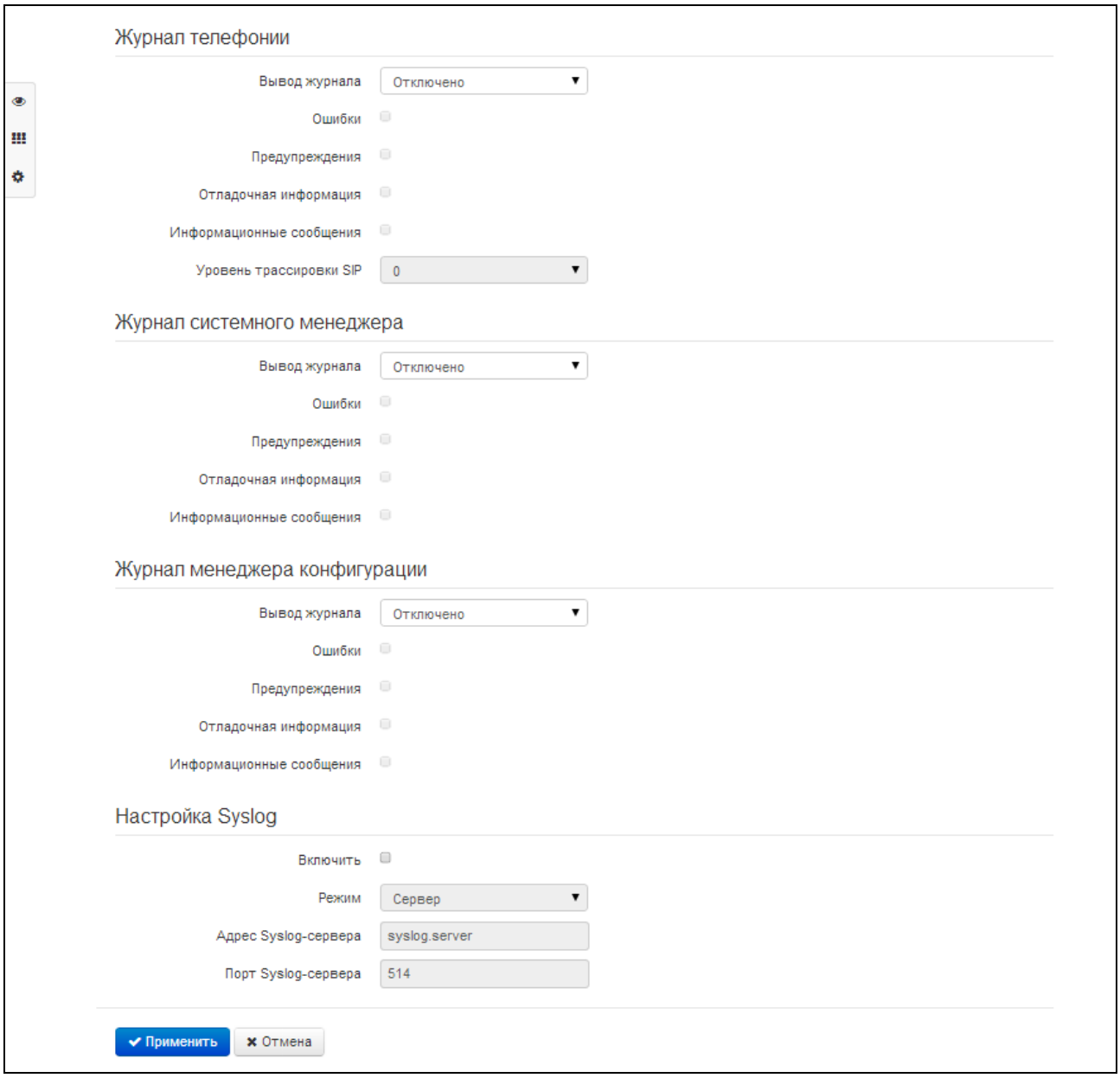
Для разрешения записи данных на USB-устройство анонимному пользователю установите флаг «Разрешить запись анонимному пользователю».

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

2.6.5.3 Подменю «Журнал»

Подменю «*Журнал*» предназначено для настройки вывода разного рода отладочных сообщений системы в целях обнаружения причин проблем в работе устройства. Отладочную информацию возможно получить от следующих программных модулей устройства:

- Менеджер телефонии – отвечает за работу функций IP-телефонии.
- Системный менеджер – отвечает за настройку устройства согласно файлу конфигурации.
- Менеджер конфигурации – отвечает за работу с файлом конфигурации (чтение и запись в конфигурационный файл из различных источников) и сбор информации мониторинга устройства.



Журнал телефонии

- *Вывод журнала* – направление вывода сообщений журнала:
  - *Отключено* – журнал отключен;
  - *Syslog* – сообщения выводятся по протоколу syslog на удаленный сервер либо в локальный файл (настройка протокола осуществляется ниже);
  - *Консоль* – сообщения выводятся в консоль устройства (необходимо подключение через переходник COM-порта);
  - *Telnet* – сообщения выводятся в telnet-сессию; для этого сначала необходимо создать подключение по протоколу telnet.

Ниже настраивается тип сообщений, выводимых в журнал телефонии:

- *Ошибки* – установите флаг, если необходимо выводить сообщения типа «Ошибки»;
- *Предупреждения* – установите флаг, если необходимо выводить сообщения типа «*Предупреждения*»;

- *Отладочная информация* – установите флаг, если необходимо выводить отладочные сообщения;
- *Информационные сообщения* – установите флаг, если необходимо выводить информационные сообщения;
- *Уровень трассировки SIP* – задаёт уровень вывода сообщений стека SIP-менеджера телефонии.

Журнал системного менеджера

- *Вывод журнала* – направление вывода сообщений журнала:
  - *Отключено* – журнал отключен;
  - *Syslog* – сообщения выводятся по протоколу syslog на удаленный сервер либо в локальный файл (настройка протокола осуществляется ниже);
  - *Консоль* – сообщения выводятся в консоль устройства (необходимо подключение через переходник COM-порта);
  - *Telnet* – сообщения выводятся в telnet-сессию; для этого сначала необходимо создать подключение по протоколу telnet.

Ниже настраивается тип сообщений, выводимых в журнал системного менеджера:

- *Ошибки* – установите флаг, если необходимо выводить сообщения типа «Ошибки»;
- *Предупреждения* – установите флаг, если необходимо выводить сообщения типа «*Предупреждения*»;
- *Отладочная информация* – установите флаг, если необходимо выводить отладочные сообщения;
- *Информационные сообщения* – установите флаг, если необходимо выводить информационные сообщения;

Журнал менеджера конфигурации

- *Вывод журнала* – направление вывода сообщений журнала:
  - *Отключено* – журнал отключен;
  - *Syslog* – сообщения выводятся по протоколу syslog на удаленный сервер либо в локальный файл (настройка протокола осуществляется ниже);
  - *Консоль* – сообщения выводятся в консоль устройства (необходимо подключение через переходник COM-порта);
  - *Telnet* – сообщения выводятся в telnet-сессию; для этого сначала необходимо создать подключение по протоколу telnet.

Ниже настраивается тип сообщений, выводимых в журнал менеджера конфигурации:

- *Ошибки* – установите флаг, если необходимо выводить сообщения типа «Ошибки»;
- *Предупреждения* – установите флаг, если необходимо выводить сообщения типа «*Предупреждения*»;
- *Отладочная информация* – установите флаг, если необходимо выводить отладочные сообщения;
- *Информационные сообщения* – установите флаг, если необходимо выводить информационные сообщения.

Настройка Syslog

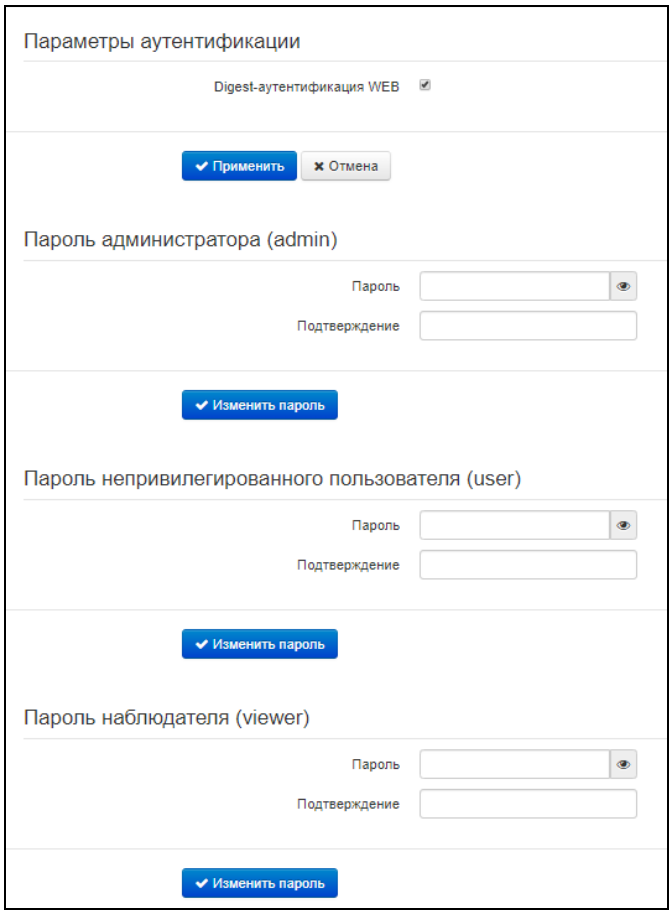
Если хотя бы один из журналов (менеджера телефонии, системного менеджера или менеджера конфигурации) настроен для вывода в Syslog, необходимо включить Syslog-агента, который будет перехватывать отладочные сообщения от соответствующего менеджера и отправлять их либо на удаленный сервер, либо сохранять в локальный файл в формате Syslog.

- *Включить* – при установленном флаге запущен Syslog-агент;
- *Режим* – режим работы Syslog-агента:
  - *Сервер* – информация журналов отправляется на удаленный Syslog-сервер (этот режим называется «удаленный журнал»);
  - *Локальный файл* – информация журналов сохраняется в локальном файле;
  - *Сервер и файл* – информация журналов отправляется на удаленный Syslog-сервер и сохраняется в локальном файле.

Далее, в зависимости от режима Syslog-агента, доступны настройки:

- *Адрес Syslog-сервера* – IP-адрес или доменное имя Syslog-сервера (необходимо для режима «Сервер»);
- *Порт Syslog-сервера* – порт для входящих сообщений Syslog-сервера (по умолчанию 514, необходимо для режима «Сервер»);
- *Имя файла* – имя файла для хранения журнала в формате Syslog (необходимо для режима «Файл»;
- *Размер файла, кБ* – максимальный размер файла журнала (необходимо для режима «Файл»).

2.6.5.4 Подменю «Аутентификация WEB»



В подменю «Аутентификация WEB» устанавливаются пароли доступа администратора, непривилегированного пользователя и наблюдателя.

Digest-аутентификация WEB (WEB Digest-authentication) – при установленном флаге аутентификация пользователей осуществляется в соответствии с алгоритмами digest.

Установленные пароли используются для доступа к устройству через Web-интерфейс, а также по протоколам Telnet и SSH.

При входе через Web-интерфейс администратор (пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек, полный мониторинг состояния устройства. Непривилегированный пользователь (пароль по умолчанию: **user**) имеет возможность выполнить только сетевые настройки (кроме настроек подключения к Интернет), имеет доступ к мониторингу состояния устройства. Наблюдатель (пароль по умолчанию: **viewer**) имеет возможность только просматривать конфигурацию и данные мониторинга устройства без возможности вносить какие-либо изменения.

Логин администратора: admin
Логин непривилегированного пользователя: user
Логин наблюдателя: viewer

- *Пароль администратора* – в соответствующие поля введите пароль администратора и подтвердите его;
- *Пароль непривилегированного пользователя* – в соответствующие поля введите пароль непривилегированного пользователя и подтвердите его;
- *Пароль наблюдателя* – в соответствующие поля введите пароль наблюдателя и подтвердите его.

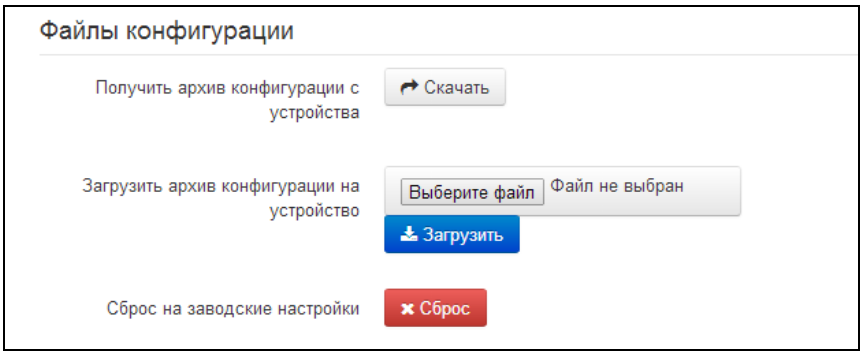
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

При обновлении версии до 2.3.0 и выше все пароли будут зашифрованы. При возврате на версию 2.1.0 и ниже требуется сбросить конфигурацию устройства до заводской.

Начиная с версии ПО 2.3.0 доступна функция шифрования паролей в файле конфигурации устройства. При подготовке файла cfg.yaml для автоматического конфигурирования, если требуется изменить один из паролей на устройстве, необходимо убрать ‘encrypted’ и задать пароль. Например, чтобы изменить пароль для пользователя admin, нужно в значении «AdminPassword» стереть ‘encrypted’ и задать новый пароль ‘*новый пароль*’.

2.6.5.5 Подменю «Управление конфигурацией»

В подменю «*Управление конфигурацией*» выполняется сохранение и обновление текущей конфигурации.



Получение конфигурации

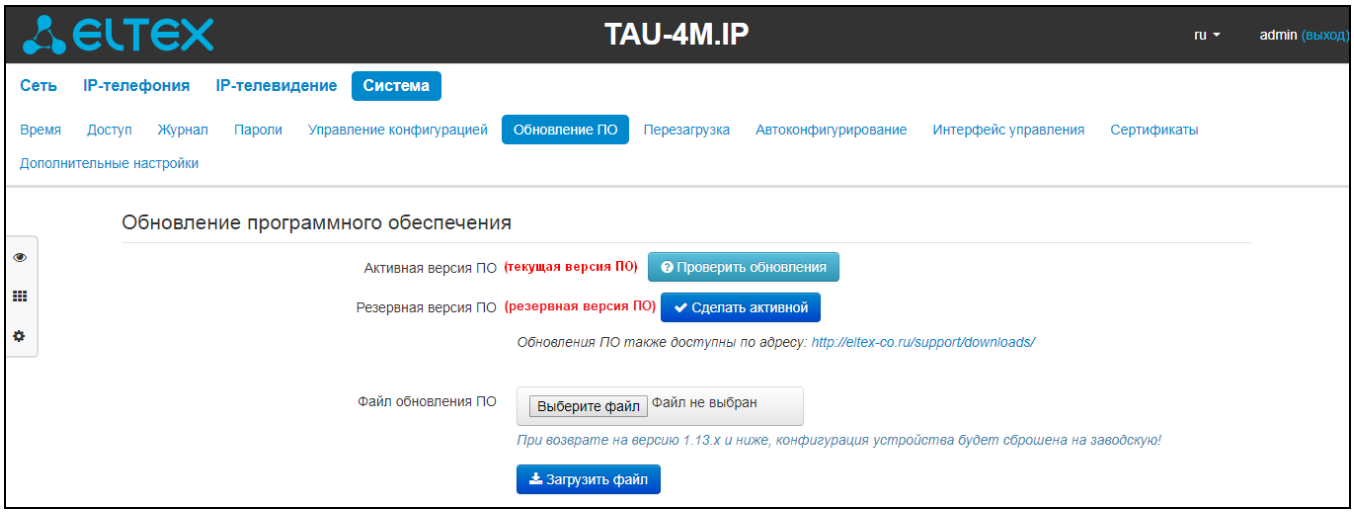
Чтобы сохранить текущую конфигурацию устройства на локальный компьютер, нажмите кнопку «Скачать».

Обновление конфигурации

- *Загрузить архив конфигурации на устройство* – выбор сохраненного на локальном компьютере файла конфигурации. Для обновления конфигурации устройства нажмите кнопку «Выберите файл», укажите файл (в формате .tar.gz) и нажмите кнопку «Загрузить». Загруженная конфигурация применяется автоматически без перезагрузки устройства.
- *Сброс на заводские настройки* – для сброса устройства к настройкам по умолчанию нажмите кнопку *«Сброс»*.

2.6.5.6 Подменю «Обновление ПО»

Подменю «*Обновление ПО*» предназначено для обновления управляющей микропрограммы устройства.



- *Активная версия ПО* – версия программного обеспечения, установленного на устройстве;
- *Проверить обновления* – кнопка для проверки актуальности версии программного обеспечения. С помощью этой функции Вы можете быстро проверить наличие новой версии программного обеспечения и, в случае необходимости, выполнить его обновление.
- *Резервная версия ПО* – версия программного обеспечения, установленного на устройстве, на которую можно перейти в случае проблем с активной версией ПО;
- *Сделать активной* – кнопка, позволяющая сделать резервную версию ПО активной, для этого потребуется перезагрузка устройства. Активная версия ПО в этом случае станет резервной.

Для работы функции проверки обновления необходимо наличие выхода в Интернет.

Обновить программное обеспечение устройства можно также вручную, предварительно загрузив файл ПО с сайта *http://eltex-co.ru/support/downloads* и сохранив его на компьютере. Для этого нажмите

кнопку «Выберите файл» в поле *Файл обновления ПО* и укажите путь к файлу управляющей программы в формате .tar.gz.

Для запуска процесса обновления необходимо нажать кнопку «Загрузить файл». Процесс обновления займет несколько минут (о его текущем статусе будет указано на странице), после чего устройство автоматически перезагрузится.

Не отключайте питание устройства и не выполняйте его перезагрузку в процессе обновления ПО.

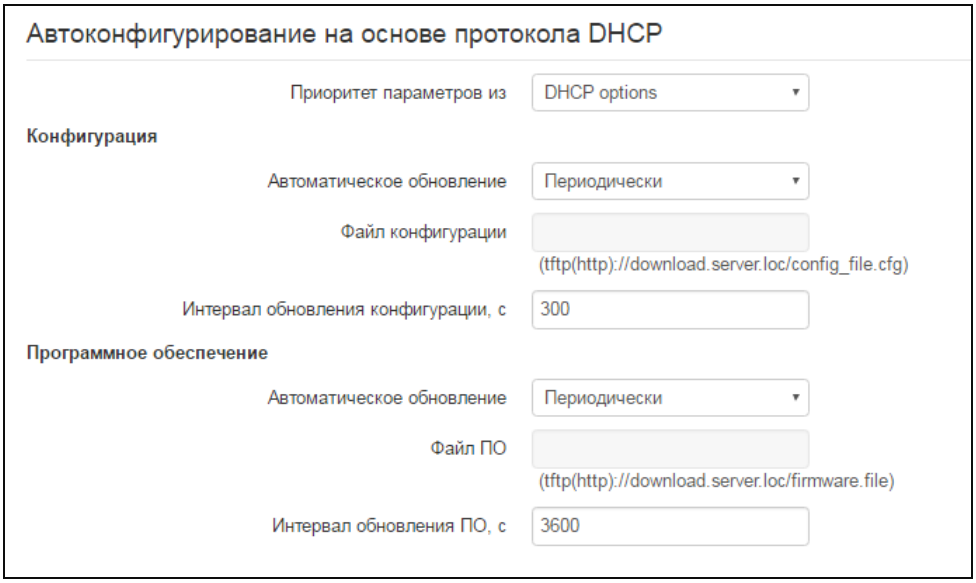
2.6.5.7 Подменю «Перезагрузка»

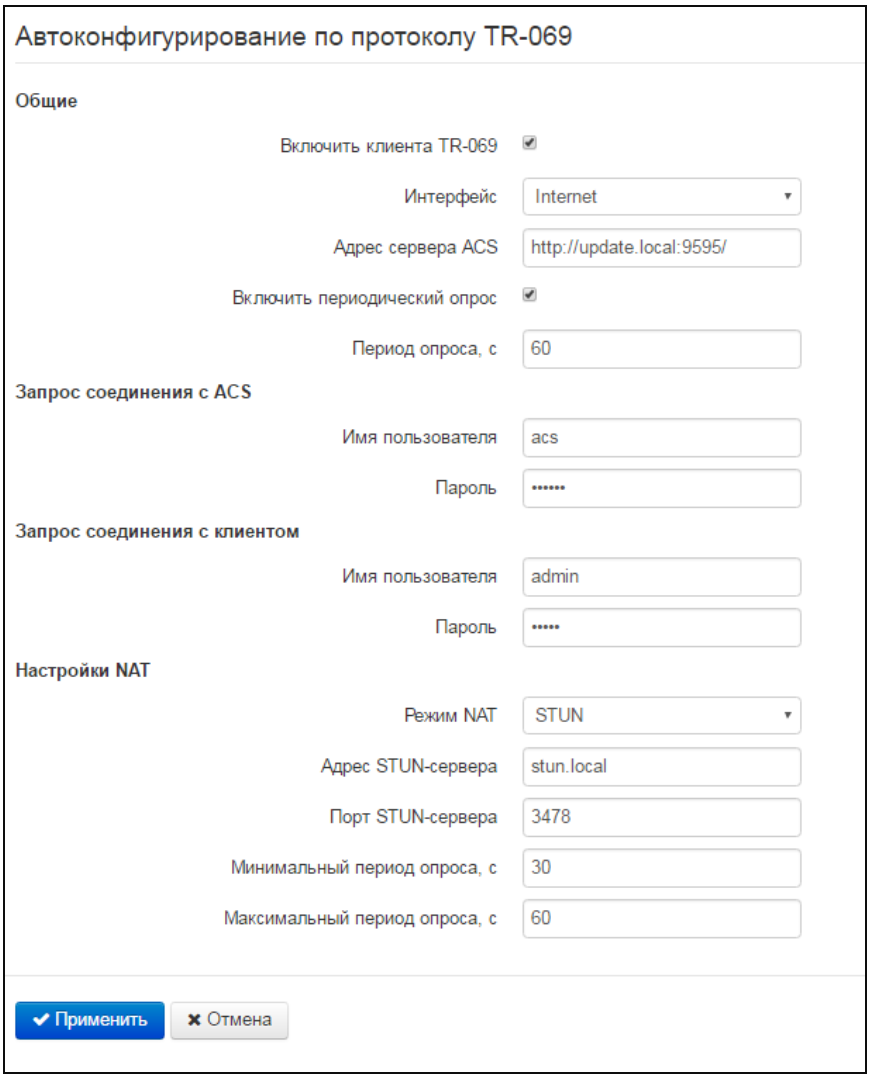
В подменю «*Перезагрузка*» выполняется перезапуск устройства.

Для перезагрузки устройства нажмите на кнопку «Перезагрузить». Процесс перезагрузки устройства занимает примерно 1 минуту.

2.6.5.8 Подменю «Автоконфигурирование»

В подменю «*Автоконфигурирование*» выполняется настройка алгоритма DHCP-based autoprovisioning (автоконфигурирование на основе протокола DHCP) и протокола автоматического конфигурирования абонентских устройств TR-069.





Автоконфигурирование на основе протокола DHCP:

- *Приоритет параметров из* – данный параметр определяет, откуда необходимо взять названия и расположение файлов конфигурации и программного обеспечения:
  - *Static settings* – пути к файлам конфигурации и программного обеспечения определяются соответственно из параметров «*Файл конфигурации*» и «*Файл ПО*»; подробнее о работе алгоритма смотрите в разделе 5;
  - *DHCP options* – пути к файлам конфигурации и программного обеспечения определяются из DHCP-опций 43, 66 и 67 (для этого необходимо для услуги Интернет выбрать протокол DHCP); подробнее о работе алгоритма смотрите в разделе 5;
- *Автоматическое обновление* – для обновления конфигурации ПО отдельно можно задать один из нескольких режимов обновления:
  - *Выключено* – автоматическое обновление конфигурации или программного обеспечения устройства отключено;
  - *Периодически* – автообновление конфигурации или программного обеспечения устройства будет производится через заданный промежуток времени;
  - *По расписанию* – автообновление конфигурации или программного обеспечения устройства будет производиться в заданное время, в указанные дни недели.

- *Файл конфигурации* – полный путь к файлу конфигурации – задаётся в формате URL (на данный момент возможна загрузка файла конфигурации по протоколам TFTP и HTTP):

  tftp://<server address>/<full path to cfg file>
  http://<server address>/<full path to cfg file>
  где < server address > – адрес HTTP- или TFTP-сервера (доменное имя или IPv4),
  < full path to cfg file > – полный путь к файлу конфигурации на сервере;

- *Интервал обновления конфигурации, с* – промежуток времени в секундах, через который осуществляется периодическое обновление конфигурации устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;

- *Время обновления файла конфигурации* - время в 24-часовом формате, в которое будет производится автообновление конфигурации;

- *Дни обновления конфигурации* - дни недели, в которые в заданное время будет производиться автообновление конфигурации.

- *Файл ПО* – полный путь к файлу программного обеспечения – задаётся в формате URL (на данный момент возможна загрузка файла ПО по протоколам TFTP и HTTP):

  tftp://<server address>/<full path to firmware file>
  http://<server address>/<full path to firmware file>,
  где < server address > – адрес HTTP- или TFTP-сервера (доменное имя или IPv4),
  < full path to firmware file > – полный путь к файлу ПО на сервере;

- *Интервал обновления ПО, с* – промежуток времени в секундах, через который осуществляется периодическое обновление программного обеспечения устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;

- *Время обновления ПО* - время в 24-часовом формате, в которое будет производится автообновление программного обеспечения;

- *Дни обновления ПО* - дни недели, в которые в заданное время будет производиться автообновление программного обеспечения.

Детальное описание алгоритма автоматического обновления на основе протокола DHCP представлено в разделе 5.

Автоконфигурирование по протоколу TR-069:

Общие:

- *Включить клиента TR-069* – при установленном флаге разрешена работа встроенного клиента протокола TR-069;

- *Интерфейс* – выбор интерфейса, через который будет выполняться автоконфигурирование устройства для работы по протоколу TR-069. Если на шлюзе включен *интерфейс управления*, то данная VLAN автоматически будет использоваться для работы по протоколу TR-069. Настройка выбора интерфейса будет заблокирована;

- *Адрес сервера ACS* – адрес сервера автоконфигурирования. Адрес необходимо вводить в формате http://<address>:<port> или https://<address>:<port> (<address> – IP-адрес или доменное имя ACS-сервера, <port> – порт сервера ACS, по умолчанию порт 80). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS. ACS-сервер фирмы Eltex по умолчанию использует для связи порт 9595;

- *Включить периодический опрос* – при установленном флаге встроенный клиент TR-069 осуществляет периодический опрос сервера ACS с интервалом, равным *«Периоду опроса»*, в секундах. Цель опроса - обнаружить возможные изменения в конфигурации устройства.

- *Период опроса* – интервал отправки сообщений 2 PERIODIC.

Запрос соединения с ACS:

Имя пользователя, Пароль – имя пользователя и пароль для доступа клиента к ACS-серверу.

Запрос соединения с клиентом:

Имя пользователя, Пароль – имя пользователя и пароль для доступа ACS-сервера к клиенту TR-069.

Настройки NAT:

Если на пути между клиентом и сервером ACS имеет место преобразование сетевых адресов (NAT – network address translation) – сервер ACS может не иметь возможности установить соединение с клиентом, если не использовать определенные технологии, позволяющие этого избежать. Эти технологии сводятся к определению клиентом своего, так называемого публичного адреса (адреса NAT или по-другому – внешнего адреса шлюза, за которым установлен клиент). Определив свой публичный адрес, клиент сообщает его серверу, и сервер в дальнейшем для установления соединения с клиентом использует уже не его локальный адрес, а публичный.

- *Режим NAT* – определяет, каким образом клиент должен получить информацию о своем публичном адресе. Возможны следующие режимы:

  - *STUN* – использовать протокол STUN для определения публичного адреса;
  - *Manual* – ручной режим, когда публичный адрес задается явно в конфигурации; в этом режиме на устройстве, выполняющем функции NAT, необходимо добавить правило проброса TCP-порта, используемого клиентом TR-069;
  - *Off* – NAT не используется – данный режим рекомендуется использовать только когда устройство подключено к серверу ACS напрямую, без преобразования сетевых адресов. В этом случае публичный адрес совпадает с локальным адресом клиента.

При выборе режима *STUN* необходимо задать следующие настройки:

- *Адрес STUN-сервера* – IP-адрес или доменное имя STUN-сервера;
- *Порт STUN-сервера* – UDP-порт STUN-сервера (по умолчанию значение 3478);
- *Минимальный период опроса, с* и *Максимальный период опроса, с* – определяют интервал времени в секундах для отправки периодических сообщений на STUN-сервер с целью обнаружения изменения публичного адреса.

При выборе режима *Manual* публичный адрес клиента задается вручную через параметр *Адрес NAT* (адрес необходимо вводить в формате IPv4).

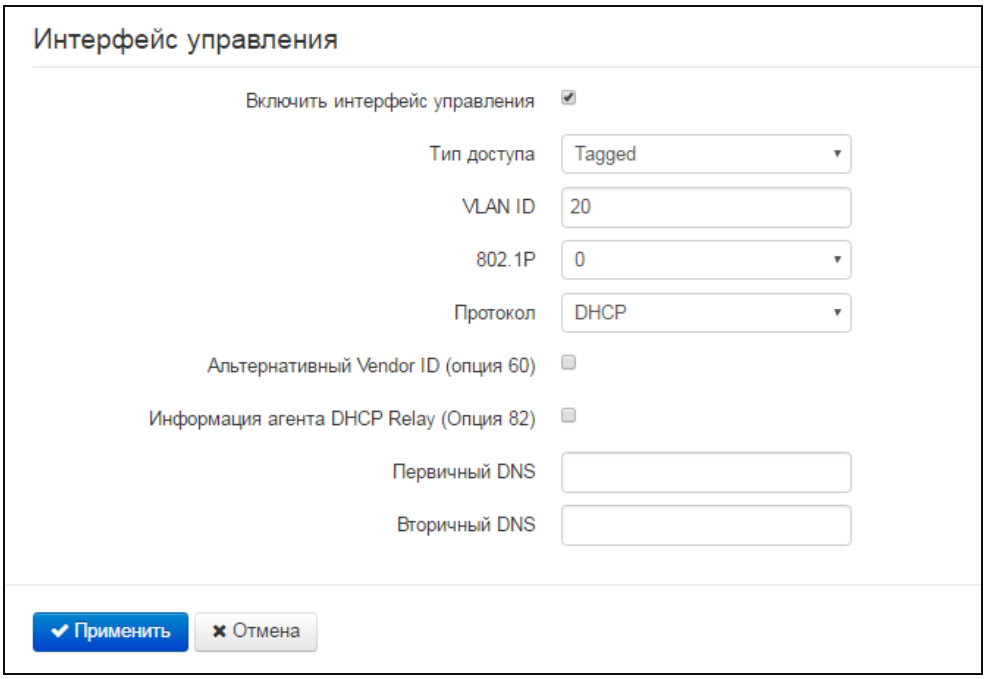
Для корректной работы с ACS-сервером за NAT минимальный период опроса STUN-сервера должен быть меньше, чем максимальное время сохранения сессии NAT-устройством.

По протоколу TR-069 возможно произвести полное конфигурирование устройства, обновление программного обеспечения, чтение информации об устройстве (версия ПО, модель, серийный номер и т.д), загрузку и выгрузку целого файла конфигурации, удаленную перезагрузку устройства (поддержаны спецификации TR-069, TR-098, TR-104).

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.6.5.9 Подменю «Интерфейс управления»

Меню позволяет настроить сетевой интерфейс для организации сетевого управления устройством, используя протоколы HTTP, HTTPS, Telnet и SSH.



- *Включить интерфейс управления* – при установленном флаге управление устройством производится через данный интерфейс*;*
- *Тип доступа* — задает режим работы интерфейса:
  - *Tagged* — данные передаются интерфейсом с использованием заданного VLAN ID;
  - *Untagged* — данные передаются интерфейсом без использования VLAN.
- *VLAN ID* — идентификатор для выделения интерфейса в виртуальную локальную сеть*;*
- *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет);
- *Протокол* – выбор протокола назначения адреса на интерфейс:
  - *Static* – режим работы, при котором IP-адрес и все необходимые настройки на WAN-интерфейс назначаются вручную. При выборе типа «Static» для редактирования станут доступны следующие параметры:
    - *IP-адрес* – установка IP-адреса интерфейса управления;
    - *Маска подсети* – маска подсети интерфейса управления;
    - *Шлюз по умолчанию* – IP-адрес сетевого шлюза по умолчанию интерфейса управления;
    - *Первичный DNS, Вторичный DNS* – IP-адреса DNS-серверов, необходимых для работы протоколов автоконфигурирования шлюза, настройка которых производится на странице **Система – Автоконфигурирование.**

– *DHCP* – режим работы, при котором IP-адрес, маска подсети, адреса DNS-серверов и другие параметры, необходимые для работы интерфейса (например, статические маршруты), будут получены от DHCP-сервера автоматически. Если от провайдера не удаётся получить адреса DNS-серверов, Вы можете назначить их вручную в полях *«Первичный DNS»* и *«Вторичный DNS»*. Адреса, заданные вручную, будут иметь приоритет над адресами DNS-серверов, полученными по протоколу DHCP.

Для протокола DHCP имеется возможность задать необходимое значение опции 60.

- *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля Vendor ID (опция 60). При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.

  Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат:
  [VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**][SN:**серийный номер**][WAN:**MAC-адрес интерфейса WAN**][LAN:**MAC-адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

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

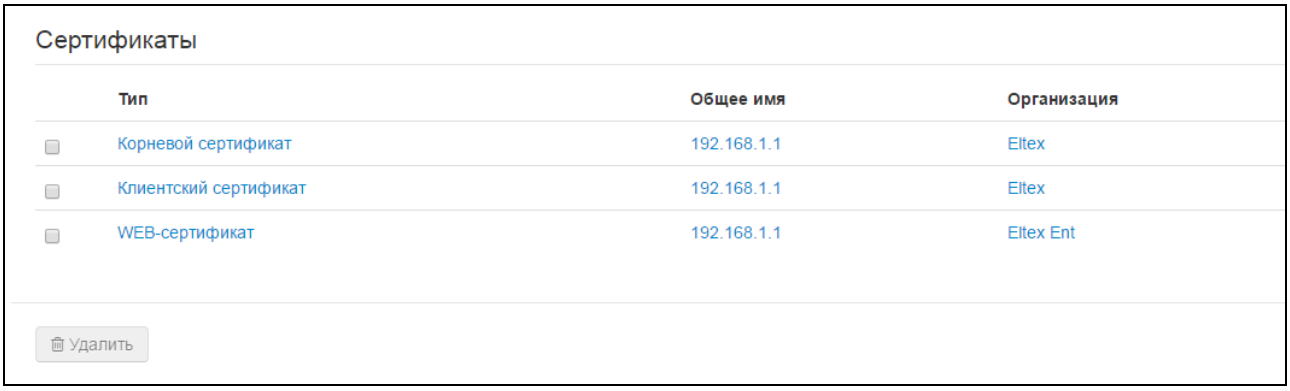
- *Информация агента DHCP Relay (опция 82)* – при установленном флаге позволяет добавить в DHCP-запрос:

  – *Идентификатор цепи агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 1 - Agent Circuit ID;
  – *Идентификатор удаленного агента (Опция82)* – позволяет добавить в DHCP-запрос опцию 82, подопцию 2 - Agent Remote ID.

  Список используемых DHCP-опций на каждом сетевом интерфейсе (Internet, VoIP, Management) можно задавать вручную. Информация по настройке списка представлена в приложении В.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

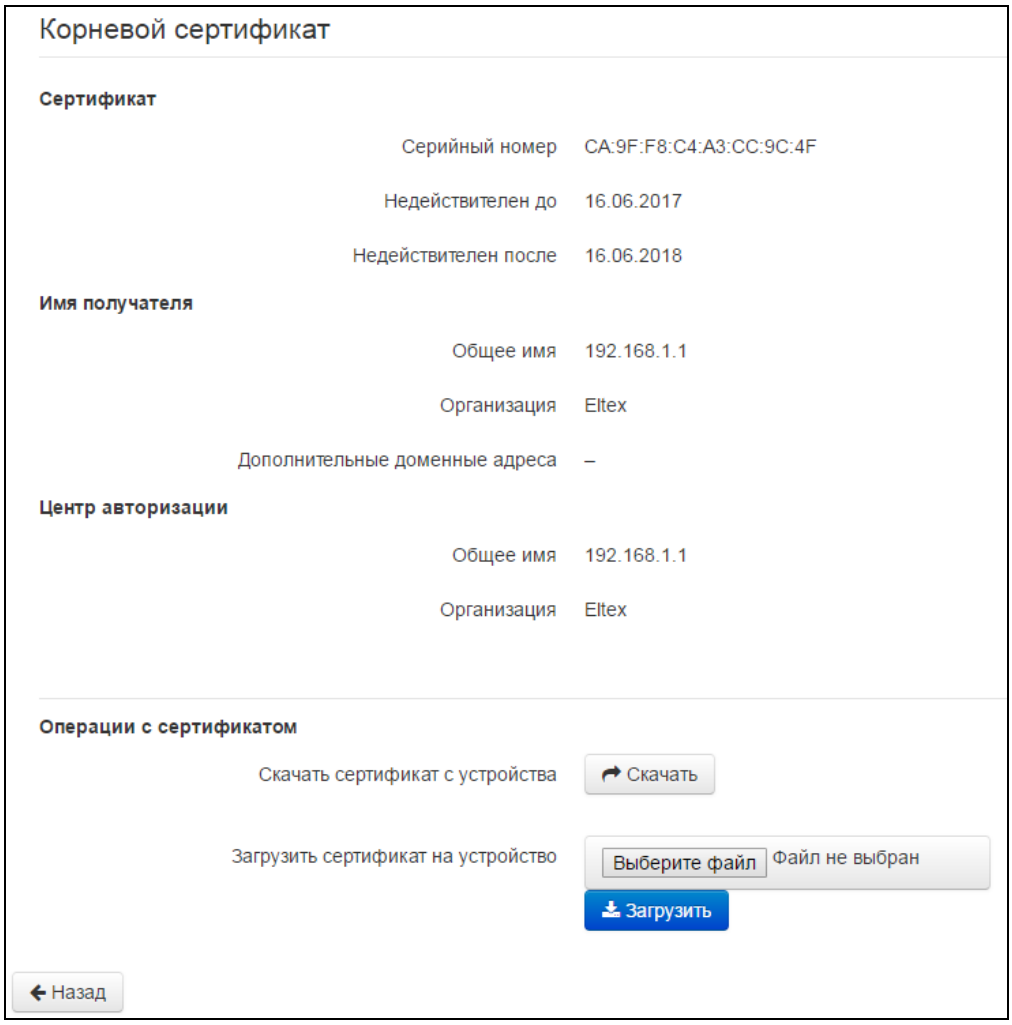
2.6.5.10 Подменю «Сертификаты»



Подменю «*Сертификаты*» позволяет просматривать, скачивать и загружать на устройство сертификаты для использования в защищённых соединениях TLS.

Корневой сертификат

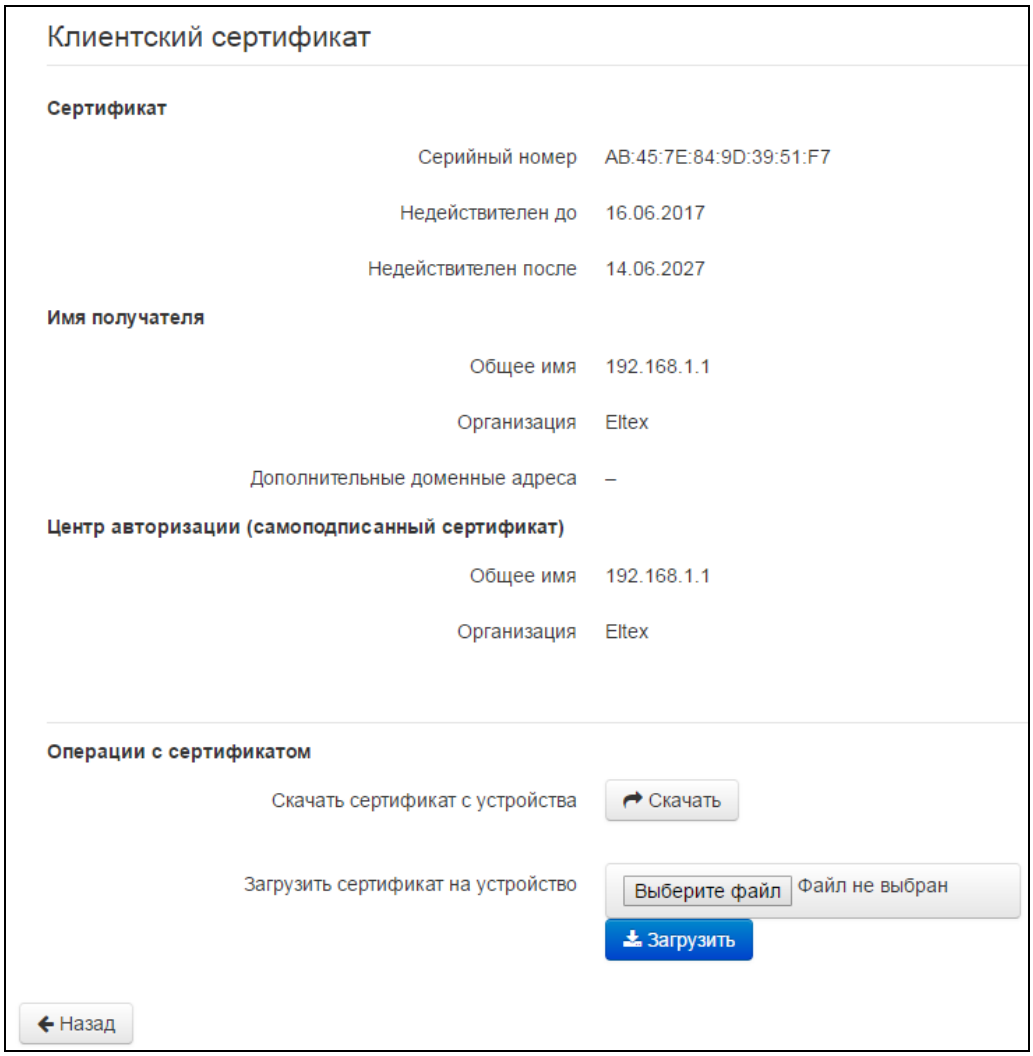
Корневой сертификат используется для проверки подлинности сертификатов при входящих соединениях. Этот сертификат должен быть подписан центром авторизации.



- *Серийный номер* — серийный номер выбранного сертификата;
- *Недействителен до* – дата начала действия сертификата;
- *Недействителен после* – дата окончания действия сертификата;
- *Имя получателя* – данные о получателе сертификата (Общее имя, Организация, Дополнительные доменные адреса);
- *Центр авторизации* – данные о центре авторизации (Общее имя, Организация).

Клиентский сертификат

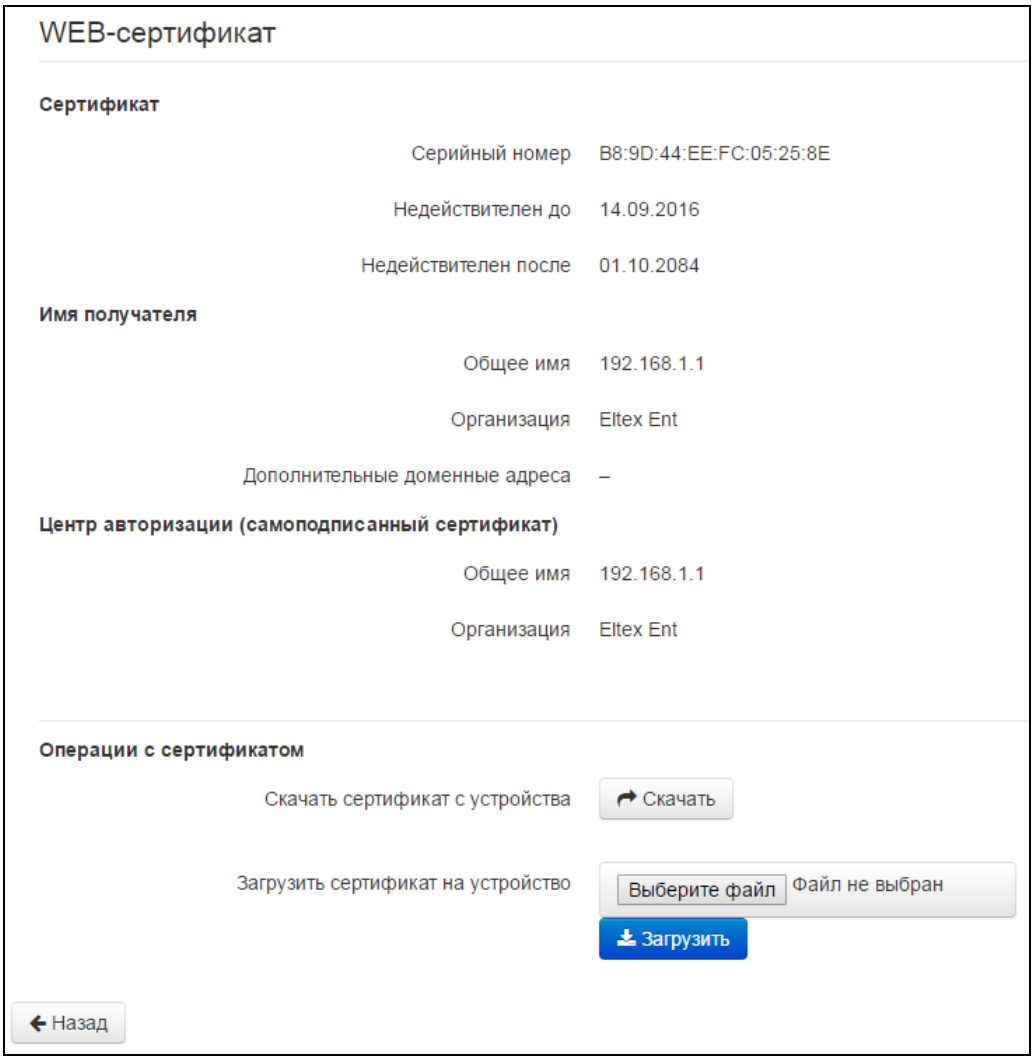
Клиентский сертификат используется при исходящих соединениях по протоколу SIP с использованием TLS.



- *Серийный номер* — серийный номер выбранного сертификата;
- *Недействителен до* – дата начала действия сертификата;
- *Недействителен после* – дата окончания действия сертификата;
- *Имя получателя* – данные о получателе сертификата (Общее имя, Организация, Дополнительные доменные адреса);
- *Центр авторизации* – данные о центре авторизации (Общее имя, Организация).

WEB-сертификат

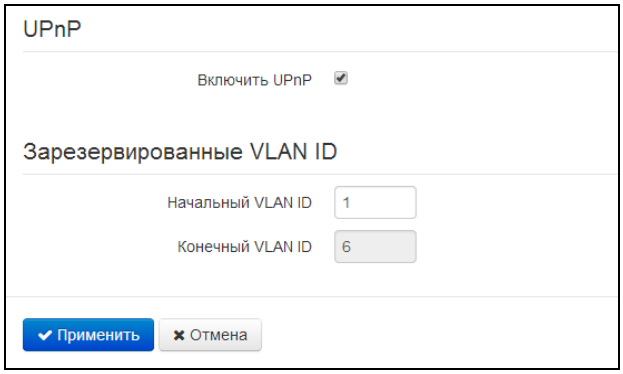
WEB-сертификат используется при доступе к Web-конфигуратору устройства по протоколу HTTPS.



- *Серийный номер* — серийный номер выбранного сертификата;
- *Недействителен до* – дата начала действия сертификата;
- *Недействителен после* – дата окончания действия сертификата;
- *Имя получателя* – данные о получателе сертификата (Общее имя, Организация, Дополнительные доменные адреса);
- *Центр авторизации* – данные о центре авторизации (Общее имя, Организация).

2.6.5.11 Подменю «Дополнительные настройки»

В подменю «*Дополнительные настройки*» можно включить UPnP.



- *Включить UPnP* – при установленном флаге протокол UPnP будет активен. Протокол UPnP используется некоторыми приложениями (например, DC-клиентами, такими как FlylinkDC++) для автоматического создания правил проброса TCP/UDP-портов, используемых этими приложениями, на вышестоящем маршрутизаторе. Рекомендуется включить UPnP для обеспечения работы сервисов обмена файлами в сети.

Зарезервированные VLAN ID

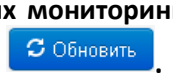
Зарезервированные VLAN ID необходимы для внутрисистемных нужд шлюза и могут быть изменены в зависимости от используемого на сети VLAN ID:

- Начальный VLAN ID – начальное значение идентификатора VLAN в зарезервированном диапазоне, принимает значения [1-4090];
- Конечный VLAN ID – начальное значение идентификатора VLAN в зарезервированном диапазоне. Данная настройка недоступна для редактирования и рассчитывается автоматически.

Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

2.7 Мониторинг системы

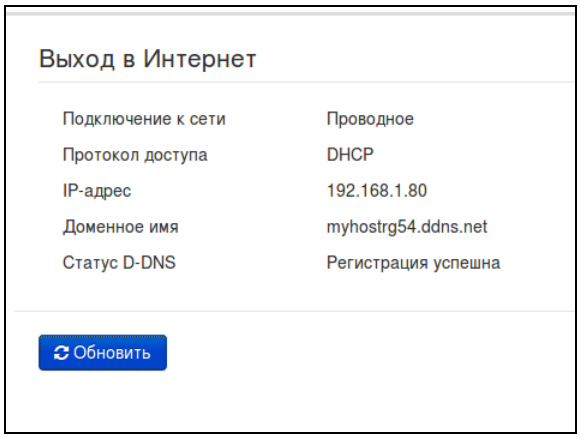
Для перехода в режим "мониторинг системы" на панели слева выберите пункт «*Мониторинг*».

На некоторых страницах не реализовано автоматические обновление данных мониторинга устройства. Для получения текущей информации с устройства нажмите кнопку 

.

2.7.1 Подменю «Интернет»

В подменю «*Интернет*» осуществляется просмотр основных сетевых настроек устройства.



Выход в Интернет

- *Подключение к сети* – способ подключения к сети передачи данных. Настройка подключения производится в разделе **Сеть** – **Интернет**:
  - *Проводное* – подключение к сети провайдера осуществляется посредством соединения медным или оптическим патч-кордом с портом WAN;
  - *3G/4G USB-модем* – подключение к сети провайдера осуществляется через 3G/4G USB-модем, подключенный к порту USB на задней панели устройства.
- *Протокол доступа* – протокол, используемый для доступа к сети Интернет;
- *IP-адрес* – IP-адрес устройства во внешней сети;
- *IP-адрес во внутренней сети провайдера* – IP-адрес, который используется во внутренней сети провайдера для доступа к локальным сетевым ресурсам провайдера.

Если выбран способ подключения **«Автоматически переходить на резервный канал»**, отображается два подключения, для которых дополнительно выводятся следующие поля:

- *Наличие связи* — показывает доступность ping-сервера через данное подключение;
- *Активность* — показывает, что интерфейс используется для передачи пользовательских данных.

2.7.2 Подменю «IP-телефония»

В подменю «*IP-телефония*» осуществляется просмотр состояния сетевого интерфейса VoIP, мониторинг абонентских комплектов и состояния регистрации групп вызова, тестирование линий, мониторинг IMS.

Состояние сетевого интерфейса VoIP

IP-адрес 192.168.1.20

Мониторинг абонентских комплектов

Линия	Локальный номер	Регистрация	Истекает через	Адрес сервера	Состояние линии	Состояние вызова 1	Удаленный абонент 1	Состояние вызова 2	Удаленный абонент 2	Тест линии	Статистика FXS
1	001	Отключена			Неактивна					Тест	Показать
2	002	Отключена			Неактивна					Тест	Показать
3	003	Отключена			Неактивна					Тест	Показать
4	004	Отключена			Неактивна					Тест	Показать

Регистрировать Разрегистрировать

Мониторинг групп вызова

Имя группы	Состояние	Номер телефона	Список линий	Регистрация	Истекает через	Адрес сервера
Group1	Включена	005	1, 3, 4	Отключена		
Group2	Выключена			Отключена		
Group3	Выключена			Отключена		
Group4	Выключена			Отключена		
Group5	Выключена			Отключена		

Мониторинг IMS

Линия	1	2	3	4
Управление с IMS	Выключено	Выключено	Выключено	Выключено
Трёхсторонняя конференция	–	–	–	–
Удержание вызова	–	–	–	–
Ожидание вызова	–	–	–	–
Горячая/теплая линия	–	–	–	–
Номер горячей линии	–	–	–	–
Таймаут горячей линии, с	–	–	–	–
Имя услуги "Передача вызова"	–	–	–	–

Состояние сетевого интерфейса VoIP

- *IP-адрес* – IP-адрес сетевого интерфейса услуги VoIP.

Мониторинг абонентских комплектов

- *Линия* – номер абонентского комплекта устройства;
- *Локальный номер* – номер телефона абонента, закрепленный за данным абонентским портом;
- *Регистрация* – состояние регистрации телефонного номера группы на прокси-сервере:
  - *Отключена* – функция регистрации на SIP-сервере выключена в настройках профиля SIP;
  - *Ошибка* – процедура регистрации закончилась неудачей;
  - *Выполнена* – процедура регистрации на SIP-сервере выполнена успешно.

- *Истекает через* – время до истечения регистрации абонентского порта на SIP-сервере;
- *Адрес сервера* – адрес сервера, на котором последний раз прошла регистрацию абонентская линия;
- *Состояние линии* – состояние физической линии. Линия может находиться в одном из следующих состояний:
  - *Не активна* – телефонная трубка положена (либо абонентский порт выключен), нормальная работа;
  - *Активна* – телефонная трубка поднята; в линию выдается сигнал ответа станции, либо сигнал КПВ, либо сигнал ошибки, либо линия находится в состоянии разговора;
  - *Посылка вызова* – на телефон подается вызывной сигнал (при поступлении входящего звонка);
  - *Тестирование* – запущен процесс тестирования линии.
- *Состояние вызова 1, 2* – каждый абонентский порт может одновременно поддерживать до двух сеансов связи. В данном поле отображается состояние вызова с соответствующим удаленным абонентом. Вызов может находиться в одном из следующих состояний:
  - *Набор номера* – осуществляется набор номера с телефонного аппарата;
  - *Занято* – вызов по каким-либо причинам отбился, в линию выдается сигнал «занято»;
  - *Исходящий вызов* – осуществляется вызов удаленного абонента, в линию выдаётся сигнал КПВ;
  - *Входящий вызов* – на телефонный порт поступает входящий вызов, в линию выдается вызывной сигнал;
  - *Разговор* – установлено разговорное соединение с удаленным абонентом;
  - *Встречный на удержании* – удаленный абонент поставлен на удержание;
  - *Локальный на удержании* – локальный абонент поставлен удаленным на удержание;
  - *Ошибка, положите трубку* – в линию выдается сигнал ошибки. Сигнал ошибки обычно выдается по истечении таймаута выдачи сигнала «занято» (настраивается отдельно для каждой линии), когда забыли положить трубку телефона.
- *Удаленный абонент 1, 2* – номер телефона удаленного абонента каждого сеанса связи.
- *Тест линии* – по кнопке Тест запускается процесс тестирования абонентской линии. О статусе процесса свидетельствует обратный таймер (в столбце «Состояние линии»), сигнализирующий об оставшемся времени теста. Нельзя запустить тест одновременно на нескольких линиях. Продолжительность теста – 80 секунд. На время теста абонентский комплект блокируется – совершать и принимать звонки будет невозможно.

Линия	Локальный номер	Регистрация	Истекает через	Адрес сервера	Состояние линии	Состояние вызова 1	Удаленный абонент 1	Состояние вызова 2	Удаленный абонент 2	Тест линии
1	20000	Есть	00:06:12	192.168.16.250	Тестирование (75)					

По окончании теста результат можно посмотреть, нажав на кнопку в столбце «Тест линии». Результат представляется в виде таблицы и содержит следующие данные:

- Дата теста
- Постоянное стороннее напряжение на проводе A (TIP)
- Постоянное стороннее напряжение на проводе B (RING)
- Переменное стороннее напряжение на проводе A (TIP)
- Переменное стороннее напряжение на проводе B (RING)

- Напряжение питания линии
- Поперечный ток (Ток в линии)
- Продольный ток (Ток утечки)
- Сопротивление между проводами A (TIP) и B (RING)
- Сопротивление между проводом A (TIP) и землёй
- Сопротивление между проводом B (RING) и землёй
- Ёмкость между проводами A (TIP) и B (RING)
- Ёмкость между проводом A (TIP) и землёй
- Ёмкость между проводом B (RING) и землёй
- Телефонный аппарат — информация о наличии подключения ТА (телефонного аппарата).

Пример результата теста линии 1:

Результат теста: Линия 1

Дата теста	12:03:35 24.12.2019
Постоянное стороннее напряжение на проводе A (TIP)	0.114408 В
Постоянное стороннее напряжение на проводе B (RING)	0.110085 В
Переменное стороннее напряжение на проводе A (TIP)	0.029830 В
Переменное стороннее напряжение на проводе B (RING)	0.024119 В
Напряжение питания линии	-51.755463 В
Поперечный ток	0.415014 мА
Продольный ток	0.383402 мА
Сопротивление между проводами A (TIP) и B (RING)	1168.946167 кОм
Сопротивление между проводом A (TIP) и землёй	545.660583 кОм
Сопротивление между проводом B (RING) и землёй	392.071228 кОм
Ёмкость между проводами A (TIP) и B (RING)	50 нФ
Ёмкость между проводом A (TIP) и землёй	50 нФ
Ёмкость между проводом B (RING) и землёй	50 нФ
Телефонный аппарат	Не подключен

Удалить Закрыть

- *Статистика FXS* – отображает количество входящих и исходящих звонков, поступивших на порт, а также последний набранный номер.

Статистика FXS: Линия 1

Последний набранный номер	6001
Количество входящих звонков	1
Количество исходящих звонков	2

Закрыть Сброс статистики

Под таблицей Мониторинга абонентских комплектов находятся кнопки для принудительной регистрации или отмены регистрации выбранных линий.

Мониторинг групп вызова

- *Имя группы* – название группы вызова;
- *Состояние* – состояние группы вызова: включена или выключена;
- *Номер телефона* – номер телефона, закрепленный за группой вызова;
- *Список линий* – список линий (портов), которые входят в группу;
- *Регистрация* – состояние регистрации телефонного номера группы на прокси-сервере:
  - *Отключена* – функция регистрации на SIP-сервере выключена в настройках *профиля SIP*;
  - *Ошибка* – процедура регистрации закончилась неудачей;
  - *Выполнена* – процедура регистрации на SIP-сервере выполнена успешно;
- *Истекает через* – время до истечения регистрации группы вызова на SIP-сервере;
- *Адрес сервера* – адрес сервера, на котором последний раз прошла регистрацию группа вызова.

Мониторинг IMS

Мониторинг IMS показывает состояние некоторых услуг (активирована или не активирована) на каждой абонентской линии, при условии, что на этой линии разрешено удаленное управление с сервера IMS (IP Multimedia Subsystem).

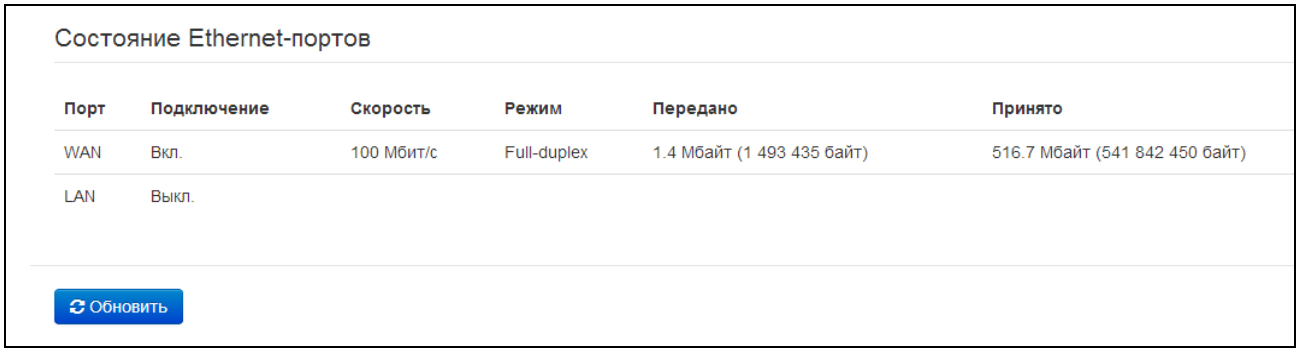
- *Управление с IMS* – показывает, включено или нет удаленное управление услугами абонентской линии с сервера IMS (настраивается в профиле SIP, см. подменю «Профили SIP»);
- *Трёхсторонняя конференция* – показывает, пришла или нет команда на активацию услуги «Трёхсторонняя конференция» с сервера IMS;
- *Удержание вызова* – показывает, пришла или нет команда на активацию услуги «Удержание вызова» с сервера IMS;
- *Ожидание вызова* – показывает, пришла или нет команда на активацию услуги «Ожидание вызова» с сервера IMS;
- *Горячая линия* – показывает, пришла или нет команда на активацию услуги «Горячая линия» с сервера IMS;
- *Номер горячей линии* – показывает номер телефона для услуги «Горячая линия» в команде активации от сервера IMS;
- *Таймаут горячей линии, с* – показывает таймаут набора для услуги «Горячая линия» в команде активации от сервера IMS.
- *Имя услуги «Передача вызова»* - показывает заданное имя услуги «Передача вызова».

✔ – услуга активирована;

✖ – услуга не активирована.

2.7.3 Подменю «Ethernet-порты»

В подменю «*Ethernet-порты*» выполняется просмотр состояния Ethernet-портов устройства.



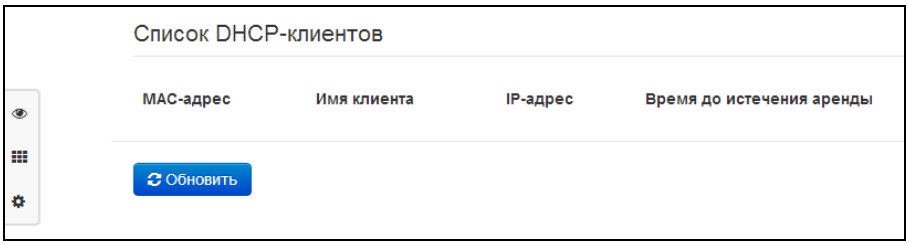
Состояние Ethernet-портов

- *Порт* – название порта:
  - *WAN* – порт внешней сети;
  - *LAN* – порт локальной сети.
- *Подключение* – состояние подключения к данному порту:
  - *Вкл.* – к порту подключено сетевое устройство (линк активен);
  - *Выкл.* – к порту не подключено сетевое устройство (линк не активен).
- *Скорость* – скорость подключения внешнего сетевого устройства к порту (10/100/1000 Мбит/с);
- *Режим* – режим передачи данных:
  - *Full-duplex* – полный дуплекс;
  - *Half-duplex* – полудуплекс;
- *Передано* – количество переданных байт с порта;
- *Принято* – количество принятых байт портом.

Для получения текущей информации о состоянии Ethernet-портов нажмите кнопку «Обновить».

2.7.4 Подменю «DHCP»

В подменю «*DHCP*» можно посмотреть список подключенных к LAN-интерфейсу сетевых устройств, которым были назначены IP-адреса локальным DHCP-сервером, а также время до истечения аренды IP-адреса.



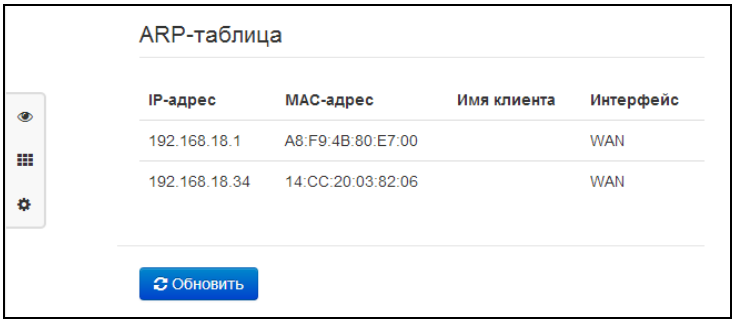
Активные DHCP-аренды

- *MAC-адрес* – MAC-адрес подключенного устройства;
- *Имя клиента* – сетевое имя подключенного устройства;
- *IP-адрес* – IP-адрес, назначенный клиенту из пула адресов;
- *Время до истечения аренды* – срок, через который истекает аренда выделенного адреса.

Для получения текущей информации о DHCP-клиентах нажмите кнопку «*Обновить*».

2.7.5 Подменю «ARP»

В подменю «*ARP*» выполняется просмотр ARP-таблицы. В ARP-таблице содержится информация о соответствии IP- и MAC- адресов соседних сетевых устройств.



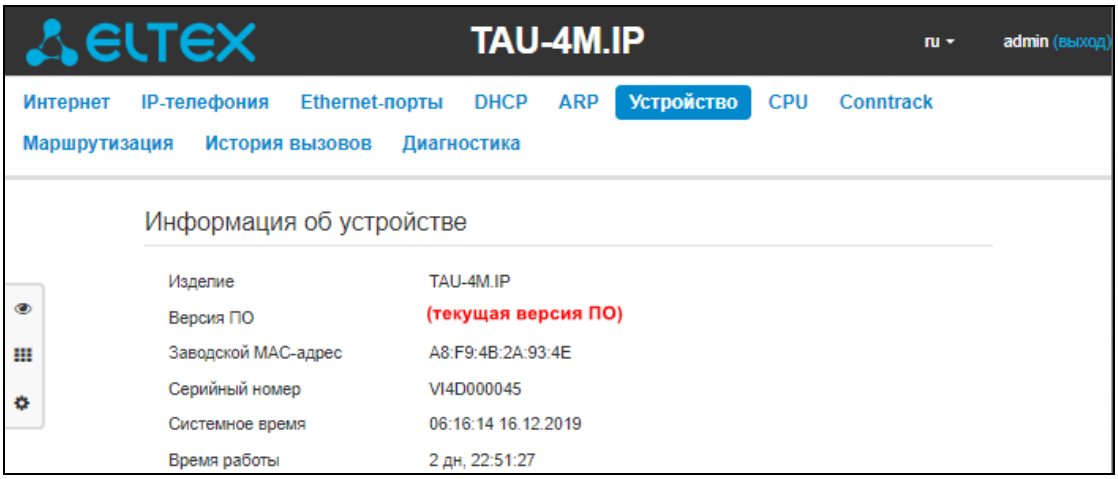
ARP-таблица

- *IP-адрес* – IP-адрес устройства;
- *MAC-адрес* – MAC-адрес устройства;
- *Имя клиента* – сетевое имя подключенного устройства;
- *Интерфейс* – интерфейс, со стороны которого активно устройство: WAN, LAN, Bridge.

Для получения текущей информации нажмите кнопку «*Обновить*».

2.7.6 Подменю «Устройство»

В подменю «*Устройство*» приведена общая информация об устройстве.

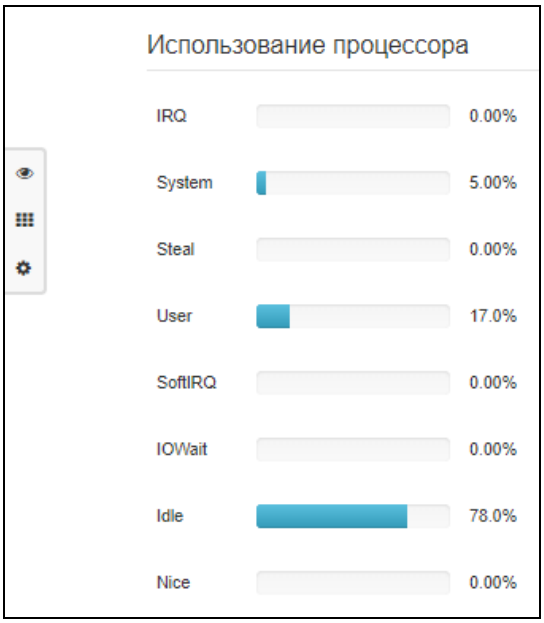


Информация об устройстве

- *Изделие* – наименование модели устройства;
- *Версия ПО* – версия программного обеспечения устройства;
- *Заводской MAC-адрес* – MAC-адрес WAN-интерфейса устройства, установленный заводом-изготовителем;
- *Серийный номер* – серийный номер устройства, установленный заводом-изготовителем;
- *Системное время* – текущие время и дата, установленные в системе;
- *Время работы* – время работы с момента последнего включения или перезагрузки устройства.

2.7.7 Подменю «CPU»

В подменю «*CPU*» отображаются данные по использованию процессора.



Использование процессора

- *IRQ* – процент процессорного времени, потраченного на обработку аппаратных прерываний;
- *System* – процент использования процессорного времени процессами ядра;
- *User* – процент использования процессорного времени пользовательскими программами;
- *SoftIRQ* – процент процессорного времени, потраченного на обработку программных прерываний;
- *IOWait* – процент процессорного времени, потраченного на операции ввода;
- *Idle* – процент незадействованных процессорных ресурсов;
- *Nice* – процент использования процессорного времени программами с измененным приоритетом.

2.7.8 Подменю «Conntrack»

В подменю «*Conntrack*» отображаются текущие активные сетевые соединения устройства.

Вывод активных сессий NAT

Число активных соединений 18

Число показанных соединений 18

Список соединений

Протокол	Адрес источника	Адрес назначения	Таймаут
TCP	192.168.27.168:60975	192.168.8.77:80	24 с
TCP	192.168.27.168:61004	192.168.8.77:80	1 мин 54 с
TCP	192.168.27.168:60995	192.168.8.77:80	1 мин 24 с
TCP	192.168.27.168:60998	192.168.8.77:80	1 мин 34 с
TCP	192.168.27.168:60981	192.168.8.77:80	44 с
TCP	192.168.27.168:60984	192.168.8.77:80	54 с
TCP	192.168.27.168:61001	192.168.8.77:80	1 мин 44 с
TCP	192.168.27.168:60993	192.168.8.77:80	1 мин 24 с
TCP	192.168.27.168:60978	192.168.8.77:80	34 с
TCP	192.168.27.168:61007	192.168.8.77:80	4 дн 23 ч 59 мин 59 с
TCP	192.168.27.168:60994	192.168.8.77:80	1 мин 14 с
TCP	192.168.27.168:60987	192.168.8.77:80	1 мин 4 с
TCP	192.168.27.168:60969	192.168.8.77:80	4 с
IGMP	0.0.0.0	224.0.0.22	6 мин 31 с
UDP	192.168.1.1:41959	239.255.255.250:1900	16 с
TCP	192.168.27.168:60990	192.168.8.77:80	1 мин 14 с
TCP	192.168.27.168:60972	192.168.8.77:80	14 с
IGMP	192.168.1.1	224.0.0.1	9 мин 45 с

Обновить

Вывод активных сессий NAT

- *Число активных соединений* – общее число активных сетевых соединений;
- *Число показанных соединений* – число соединений, выведенных в Web-интерфейс. Чтобы не снижать производительность работы Web-интерфейса, максимальное число показанных соединений ограничено значением 1024. Остальные соединения можно посмотреть через командную консоль устройства (команда *cat /proc/net/nf_conntrack*).

Список соединений

- *Протокол* – протокол, по которому установлено соединение;
- *Адрес источника* – IP-адрес и номер порта инициатора соединения;
- *Адрес назначения* – IP-адрес и номер порта адресата соединения;
- *Таймаут* – период времени до уничтожения соединения.

Для получения текущей информации нажмите кнопку «*Обновить*».

2.7.9 Подменю «Маршрутизация»

В подменю «*Маршрутизация*» отображается таблица маршрутизации устройства.

Адресат	Шлюз	Маска	Флаги	Метрика	Обращения	Обнаружения	Интерфейс
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
0.0.0.0	192.168.10.1	0.0.0.0	UG	0	0	0	eth1

- *Адресат* – IP-адрес хоста или подсети назначения, до которых установлен маршрут;
- *Шлюз* – IP-адрес шлюза, через который осуществляется выход на адресата;
- *Маска подсети* – маска подсети;
- *Флаги* – определенные характеристики данного маршрута. Существуют следующие значения *флагов*:
  - **U -** указывает, что маршрут создан и является проходимым;
  - **H -** указывает на маршрут к определенном узлу;
  - **G -** указывает, что маршрут пролегает через внешний шлюз. Сетевой интерфейс системы предоставляет маршруты в сети с прямым подключением. Все прочие маршруты проходят через внешние шлюзы. Флагом G отмечаются все маршруты, кроме маршрутов в сети с прямым подключением;
  - **R -** указывает, что маршрут, скорее всего, был создан динамическим протоколом маршрутизации, работающим на локальной системе, посредством параметра reinstate;
  - **D -** указывает, что маршрут был добавлен в результате получения сообщения перенаправления ICMP (ICMP Redirect Message). Когда система узнает о маршруте из сообщения ICMP Redirect, маршрут включается в таблицу маршрутизации, чтобы

исключить перенаправление для последующих пакетов, предназначенных тому же адресату. Такие маршруты отмечены флагом D;

- **M -** указывает, что маршрут подвергся изменению - вероятно, в результате работы динамического протокола маршрутизации на локальной системе и применения параметра mod;
- **A -** указывает на буферизованный маршрут, которому соответствует запись в таблице ARP.
- **C -** указывает, что источником маршрута является буфер маршрутизации ядра;
- **L -** указывает, что пунктом назначения маршрута является один из адресов данного компьютера. Такие «локальные маршруты» существуют только в буфере маршрутизации;
- **B -** указывает, что конечным пунктом маршрута является широковещательный адрес. Такие «широковещательные маршруты» существуют только в буфере маршрутизации;
- **I -** указывает, что маршрут связан с кольцевым (loopback) интерфейсом с целью иной, нежели обращение к кольцевой сети. Такие «внутренние маршруты» существуют только в буфере маршрутизации;
- **!** - указывает, что дейтаграммы, направляемые по этому адресу, будут отвергаться системой;

- *Метрика* – определяет «стоимость» маршрута. Метрика используется для сортировки дублирующих маршрутов, если таковые присутствуют в таблице;
- *Обращения* – зафиксированное число обращений к маршруту с целью создания соединения (не используется в системе);
- *Обнаружения* – число обнаружений маршрута, выполненных протоколом IP;
- *Интерфейс* – имя сетевого интерфейса, через который пролегает данный маршрут.

Для получения текущей информации нажмите кнопку «Обновить».

2.7.10 Подменю «История вызовов»

В подменю «*История вызовов*» можно просмотреть список совершенных телефонных вызовов, а также сводную информацию по каждому вызову.

В оперативной памяти устройства можно сохранить до 10 000 записей о совершенных вызовах. При количестве записей более 10 000 самые старые (вверху таблицы) удаляются, и в конец файла добавляются новые.

Запись статистики в журнале вызовов не ведется при нулевом размере истории.

Фильтр (показать)

Настроить параметры истории вызовов

#	Ли-ния	Локальный номер	Удаленный номер	IP-адрес встречной стороны	Время поступления вызова	Время начала разговора	Длительность разговора	Состояние вызова	Тип вызо-ва	Передано пакетов	Передано байт	Принято пакетов	Принято байт
1	4	225	222	192.168.1.18	09:45:08 17.01.2018	09:45:10 17.01.2018	5с	remote clear	исходящий	232	39904	68	10901
2	1	222	225	example.org	09:45:08 17.01.2018	09:45:10 17.01.2018	5с	local clear	входящий	63	10200	206	35432
3	1	222	sip	192.168.1.10	09:45:21 17.01.2018	09:45:23 17.01.2018	3с	local clear	входящий	64	10213	173	29452
4	4	225	sip	192.168.1.10	09:45:58 17.01.2018	09:46:00 17.01.2018	2с	local clear	входящий	98	16697	110	18616

20 записей на странице

Страница 1 из 1

Описание полей таблицы «история вызовов»:

- *#* - порядковый номер записи в таблице;
- *Линия* – номер абонентского порта устройства;
- *Локальный номер* – номер абонента, закрепленный за данным абонентским портом;
- *Удаленный номер* – номер удаленного абонента, с которым было установлено телефонное соединение;
- *IP-адрес встречной стороны* – IP-адрес удаленного абонента, с которым было установлено телефонное соединение;
- *Время поступления вызова* – время и дата поступления/совершения вызова;
- *Время начала разговора* – время и дата начала разговора;
- *Длительность разговора* – длительность разговора в секундах;
- *Состояние вызова* – промежуточное состояние либо причина завершения вызова; описание становится доступным при наведении курсора на запись состояния вызова;
- *Тип вызова* – тип вызова: исходящий или входящий;
- *Передано пакетов* – количество переданных RTP-пакетов за время разговора;
- *Передано байт* – количество переданных байт за время разговора;
- *Принято пакетов* – количество принятых RTP-пакетов за время разговора;
- *Принято байт* – количество принятых байт за время разговора.

В таблице истории звонков можно произвести отбор записей по различным параметрам. Для этого нажмите ссылку «Фильтр (показать)». Фильтрация может производиться по номеру абонентской линии, локальному или удаленному номеру, IP-адресу встречной стороны, времени поступления вызова, времени начала разговора, состоянию вызова и типу звонка. Описание параметров фильтрации указано в описании полей таблицы истории вызовов выше.

Время поступления вызова от/до или *Время начала разговора от/до* – временные рамки поступления/совершения вызова или начала разговора в формате «чч:мм:сс дд.мм.гггг».

Для скрытия настройки параметров фильтрации записей в таблице нажмите на ссылку *Фильтр «скрыть»*.

Для настройки параметров истории звонков нажмите на ссылку «Настроить параметры истории вызовов». Подробное описание настройки параметров приведено в разделе 2.6.3.10 Подменю «История вызовов».

При нажатии на кнопку произойдет переход к таблице, начиная с первой записи.

При нажатии на кнопку произойдет переход к предыдущей странице с таблицей истории вызовов.

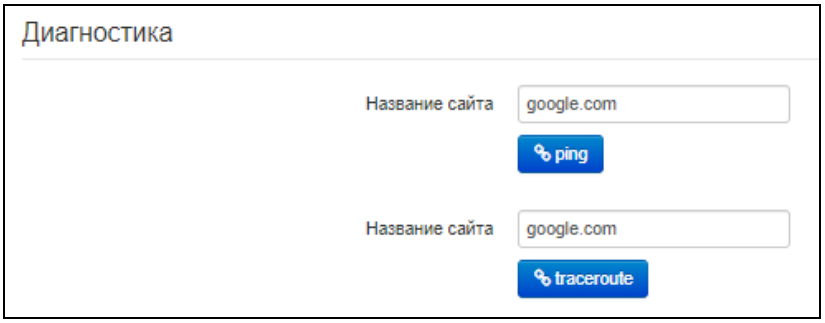
При нажатии на кнопку произойдет переход к следующей странице с таблицей истории вызовов.

При нажатии на кнопку произойдет переход к таблице, заканчивая последней записью.

Селектор «записей на странице» позволяет настроить количество выводимых записей таблицы на одной странице.

2.7.11 Подменю «Диагностика»

В подменю можно выполнить проверку доступности узла в сети и определить маршрут следования данных.

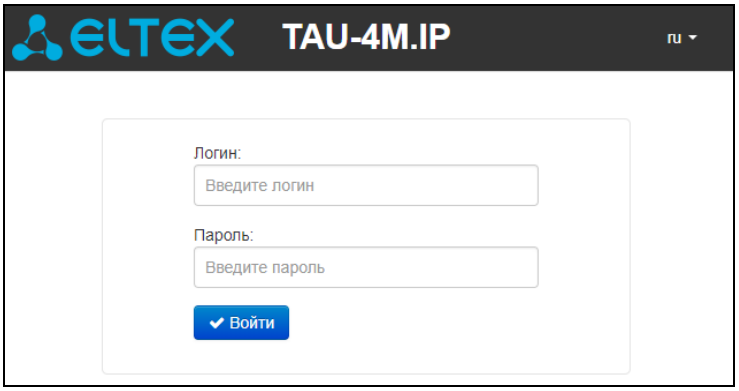


Сетевые утилиты:

- *Ping* – утилита для проверки соединений в сетях на основе TCP/IP;
- *Traceroute* – утилита для определения маршрутов следования данных в сетях TCP/IP.

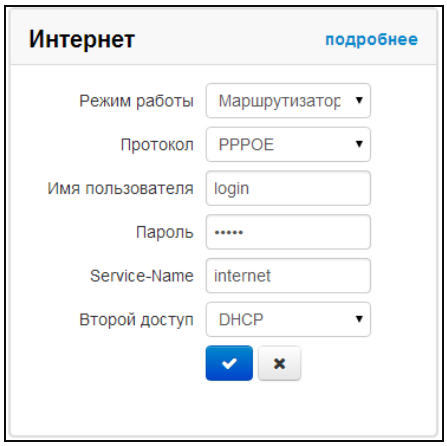
2.8 Пример настройки

- Подключите ПК к одному из LAN-портов устройства, провод от сети провайдера подключите к порту WAN;
- В адресной строке браузера введите IP-адрес шлюза (по умолчанию 192.168.1.1);
- При успешном подключении к устройству появится окно с запросом логина и пароля. Заполните поля и нажмите кнопку «Войти» (По умолчанию логин:admin, пароль:password).



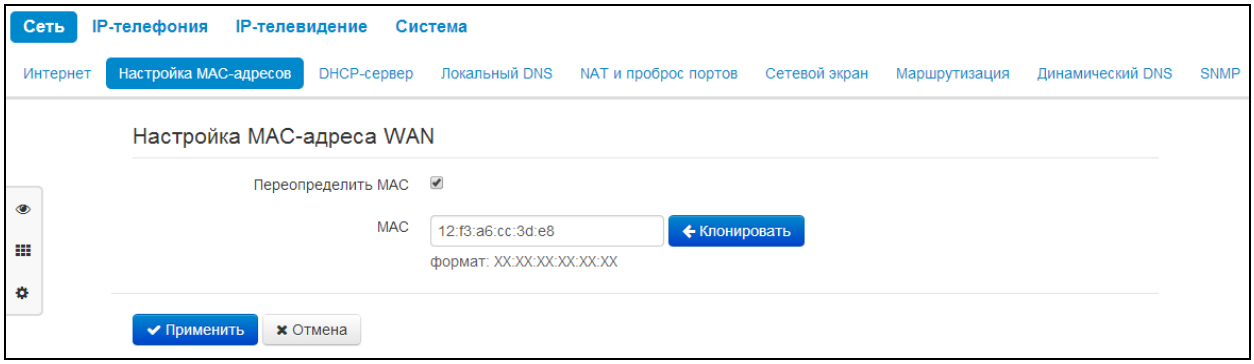
Если это окно не появилось, убедитесь, что в настройках сетевого подключения на вашем ПК установлено автоматическое получение IP-адреса.

- В плитке «Интернет» настраивается внешнее соединение. Если *TAU-4M.IP* будет использоваться в качестве маршрутизатора – в плитке «Интернет» выберите значение поля «Режим работы» - маршрутизатор. В поле «Протокол» выберите протокол, используемый вашим поставщиком услуг Интернет, и введите необходимые данные согласно инструкциям провайдера. Если для подключения к сети провайдера используются статические настройки, то в поле «Протокол» нужно выбрать значение «*Static*», заполнить поля «Внешний IP-адрес устройства», «Маска подсети», «Шлюз по умолчанию», «Первичный DNS» и «Вторичный DNS» - значения параметров предоставляются провайдером. Для сохранения и применения настроек нажмите кнопку .

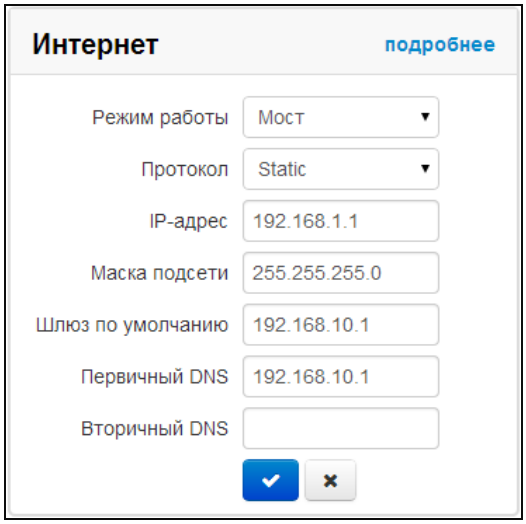


Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее» (смотрите раздел 2.6.2.1 Подменю «Интернет»).

- Если в сети вашего Интернет-провайдера используется привязка к MAC-адресу, нажмите кнопку «подробнее» в плитке «Интернет» и откройте подменю «Настройка MAC-адресов». В разделе «Настройка MAC-адреса WAN» установите флаг «Переопределить MAC» и введите в поле «MAC» MAC-адрес устройства, который ранее был подключен к сети Интернет. Если был подключен ПК, с которого производится в данный момент настройка устройства, то достаточно нажать на кнопку «*Клонировать»,* чтобы назначить шлюзу MAC-адрес вашего ПК. Для сохранения и применения настроек нажмите кнопку «Применить».

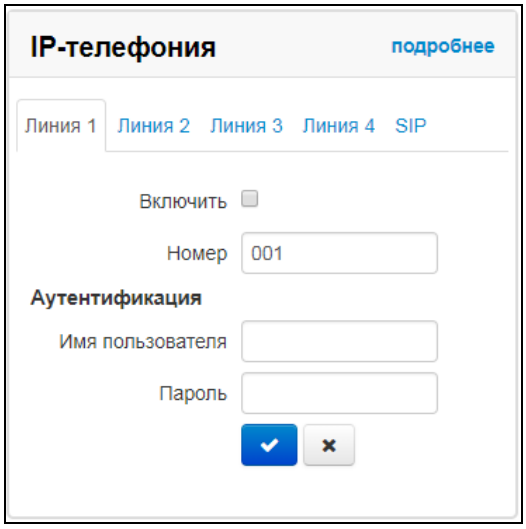


Если *TAU-4M.IP* будет использоваться в качестве 2-портового коммутатора, то в плитке «Интернет» выберите значение поля «Режим работы» - мост. В поле «IP-адрес» укажите адрес, который будет назначен устройству для доступа к нему. Введите маску подсети (по умолчанию 255.255.255.0). Для сохранения и применения настроек нажмите кнопку .



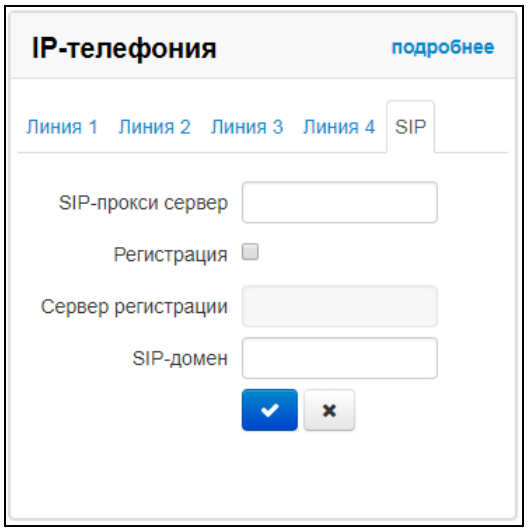
В режиме *моста* шлюз не будет автоматически выдавать IP-адреса по протоколу DHCP устройствам, подключенным к интерфейсу LAN.

- В плитке «IP-телефония» выполняется быстрая настройка абонентских линий для работы по протоколу SIP. Для этого выберите вкладку «Линия» с номером линии, которую необходимо настроить. Отметьте пункт «Включить», введите номер телефона, который будет на данной линии, логин и пароль для авторизации на SIP-сервере. Для сохранения и применения настроек нажмите кнопку .



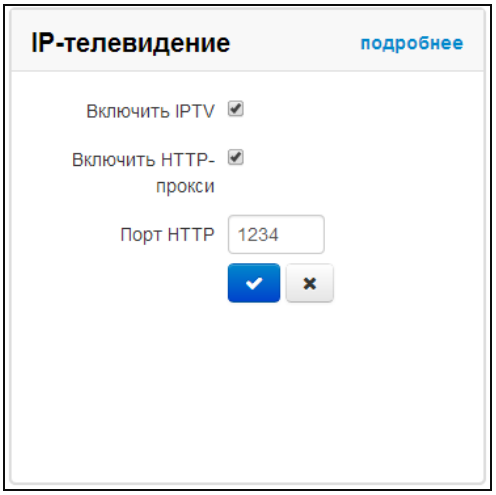
Таким же образом настраивается абонентская линия в другой вкладке «Линия».

- Выберите вкладку «SIP» в плитке «IP-телефония» для настройки параметров SIP. Укажите IP-адрес или доменное имя SIP-сервера и сервера регистрации (при необходимости) в соответствующих полях. Если на серверах используются номера портов, отличные от 5060, то через двоеточие укажите альтернативные порты. Укажите SIP-домен при необходимости. Установите флаг «Регистрация», если для работы телефонии необходима регистрация абонентов на SIP-сервере (обычно, регистрация необходима). Для сохранения и применения настроек нажмите кнопку .



Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее» (смотрите раздел 2.6.3 *Меню «IP-телефония»*).

- Если предполагается использование IP-телевидения – в плитке «IP-телевидение» отметьте пункт «Включить IPTV». Для включения возможности передачи IPTV-потоков по HTTP отметьте пункт «Включить HTTP-прокси». В поле «Порт HTTP» укажите порт, который будет использоваться для подключения внешних устройств к локальному HTTP-прокси. Для сохранения и применения настроек нажмите кнопку .



Если для услуги IPTV используется отдельный VLAN, перейдите в режим расширенных настроек, нажав ссылку «подробнее», и укажите ID VLAN в соответствующем поле.

3 ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ

3.1 Передача вызова

Услуга «Передача вызова» может выполняться локально средствами шлюза либо средствами взаимодействующего устройства. Если услуга осуществляется средствами взаимодействующего устройства, то доступ к услуге «Передача вызова» устанавливается через меню настроек абонентского порта *«IP-телефония» -> «Настройка линий»* путем выбора значения *«Transmit flash»* в поле *«Режим использования flash»*. В этом случае логику выполнения услуги определяет взаимодействующее устройство.

При выполнении услуги *«Передача вызова»* локально средствами шлюза доступ к ней устанавливается через меню настроек абонентского порта *«IP-телефония» ->* «*Настройка линий*» путем выбора значения *«Attended calltransfer*», «*Unattended calltransfer*» либо «*Local calltransfer*» в поле «*Режим использования flash*».

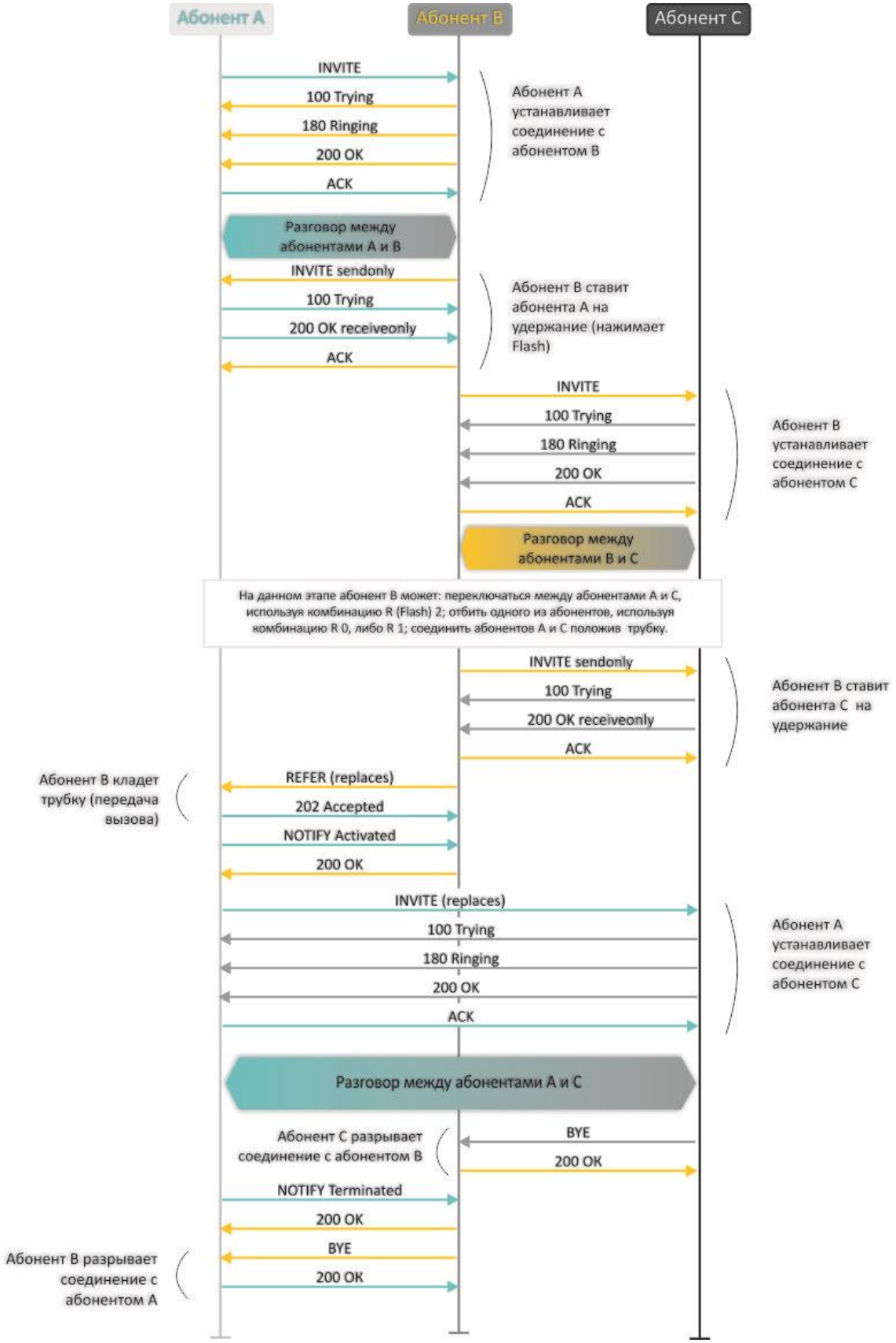
Услуга *«Attended calltransfer*» позволяет временно разорвать соединение с абонентом, находящимся на связи (абонент А), установить соединение с другим абонентом (абонент С), а затем вернуться к прежнему соединению без набора номера либо передать вызов с отключением абонента В.

Использование услуги «*Attended calltransfer*»:

Находясь в состоянии разговора с абонентом А, установить его на удержание с помощью короткого отбоя flash (R), дождаться сигнала «ответ станции» и набрать номер абонента С. После ответа абонента С возможно выполнение следующих операций:

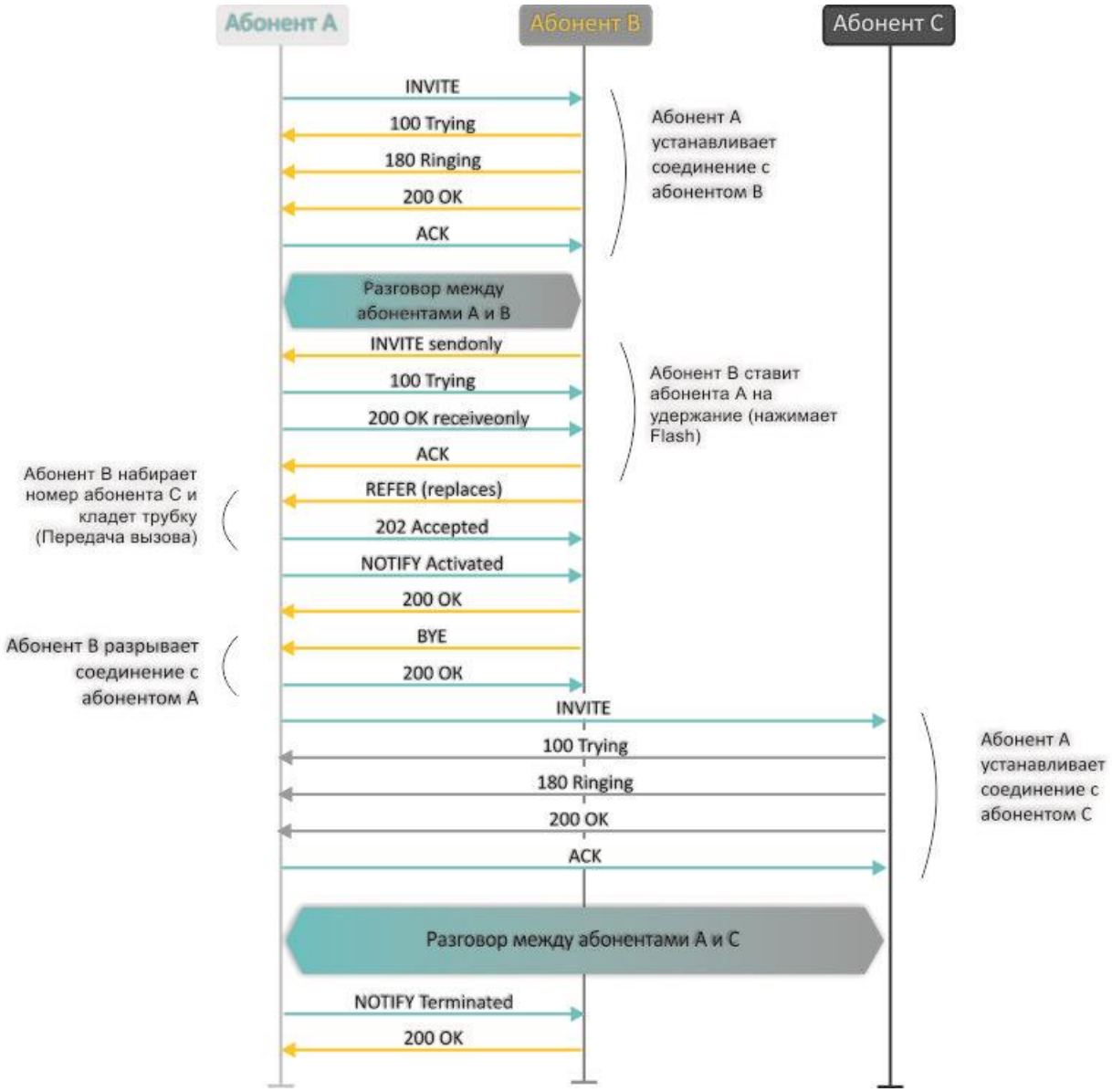
- R 0 – отключение абонента, находящегося на удержании, соединение с абонентом, находившимся на связи;
- R 1 – отключение абонента, находящегося на связи, соединение с абонентом, находившимся на удержании;
- R 2 – переключение на другого абонента (смена абонента);
- R 3 – конференция;
- R 4 - передача вызова, устанавливается разговорное соединение между абонентами А и С;
- R отбой – передача вызова, устанавливается разговорное соединение между абонентами А и С.

Ниже на рисунке представлен алгоритм работы услуги «*Attended calltransfer*»:


Абонент A
Абонент B
Абонент C
INVITE
100 Trying
180 Ringing
200 OK
ACK
Абонент A устанавливает соединение с абонентом B
Разговор между абонентами A и B
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Абонент B ставит абонента A на удержание (нажимает Flash)
INVITE
100 Trying
180 Ringing
200 OK
ACK
Абонент B устанавливает соединение с абонентом C
Разговор между абонентами B и C
На данном этапе абонент B может: переключаться между абонентами A и C, используя комбинацию R (Flash) 2; отбить одного из абонентов, используя комбинацию R 0, либо R 1; соединить абонентов A и C положив трубку.
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Абонент B ставит абонента C на удержание
Абонент B кладет трубку (передача вызова)
REFER (replaces)
202 Accepted
NOTIFY Activated
200 OK
INVITE (replaces)
100 Trying
180 Ringing
200 OK
ACK
Абонент A устанавливает соединение с абонентом C
Разговор между абонентами A и C
Абонент C разрывает соединение с абонентом B
BYE
200 OK
NOTIFY Terminated
200 OK
Абонент B разрывает соединение с абонентом A
BYE
200 OK

Услуга «*Unattended calltransfer*» позволяет поставить на удержание абонента, находящегося на связи (абонент А), с помощью короткого отбоя flash и осуществить набор номера другого абонента (абонента С). Передача вызова осуществляется автоматически по окончанию набора номера абонентом В.

Ниже на рисунке представлен алгоритм работы услуги «*Unattended calltransfer*»:



Услуга *«Local calltransfer»* позволяет сделать передачу вызова внутри шлюза без отправки внешнего сообщения REFER в том случае, если абонент С является локальным абонентом *TAU-4M.IP,* и вызов его был произведен напрямую в обход прокси-сервера. Если же абонент С является внешним абонентом либо локальным, но он был вызван через прокси-сервер, услуга *«Local calltransfer»* работает так же, как *Attended calltransfer*», то есть передача вызова осуществляется посредством отправки абоненту В сообщения REFER.

3.2 Уведомление о поступлении нового вызова – Call Waiting

Услуга позволяет абоненту, при занятости его телефонным разговором, с помощью определенного сигнала получить оповещение о новом входящем вызове.

Пользователь, при получении оповещения о новом вызове, может принять или отклонить ожидающий вызов.

Доступ к услуге устанавливается через меню настроек абонентской линии путем выбора значения «*Attended calltransfer*», «*Unattended calltransfer*» либо «*Local calltransfer»* в поле «*Режим использования flash*» и установки флага «*Ожидание вызова*».

Использование услуги:

В состоянии разговора и получения индикации о поступлении нового вызова возможно выполнение следующих операций:

- R 0 – отказ от нового вызова;
- R 1 – принять ожидающий вызов;
- R 2 – переключение на новый вызов (смена абонента);
- R – короткий отбой (flash).

3.3 Трехсторонняя конференция

Трехсторонняя конференция – услуга, обеспечивающая возможность одновременного установления телефонного соединения между тремя абонентами. Переход в режим конференции осуществляется по нажатию клавиш R 3 (описано в разделе 3.1 Передача вызова).

Абонент, собравший конференцию, является ее инициатором, другие два абонента – ее участниками.

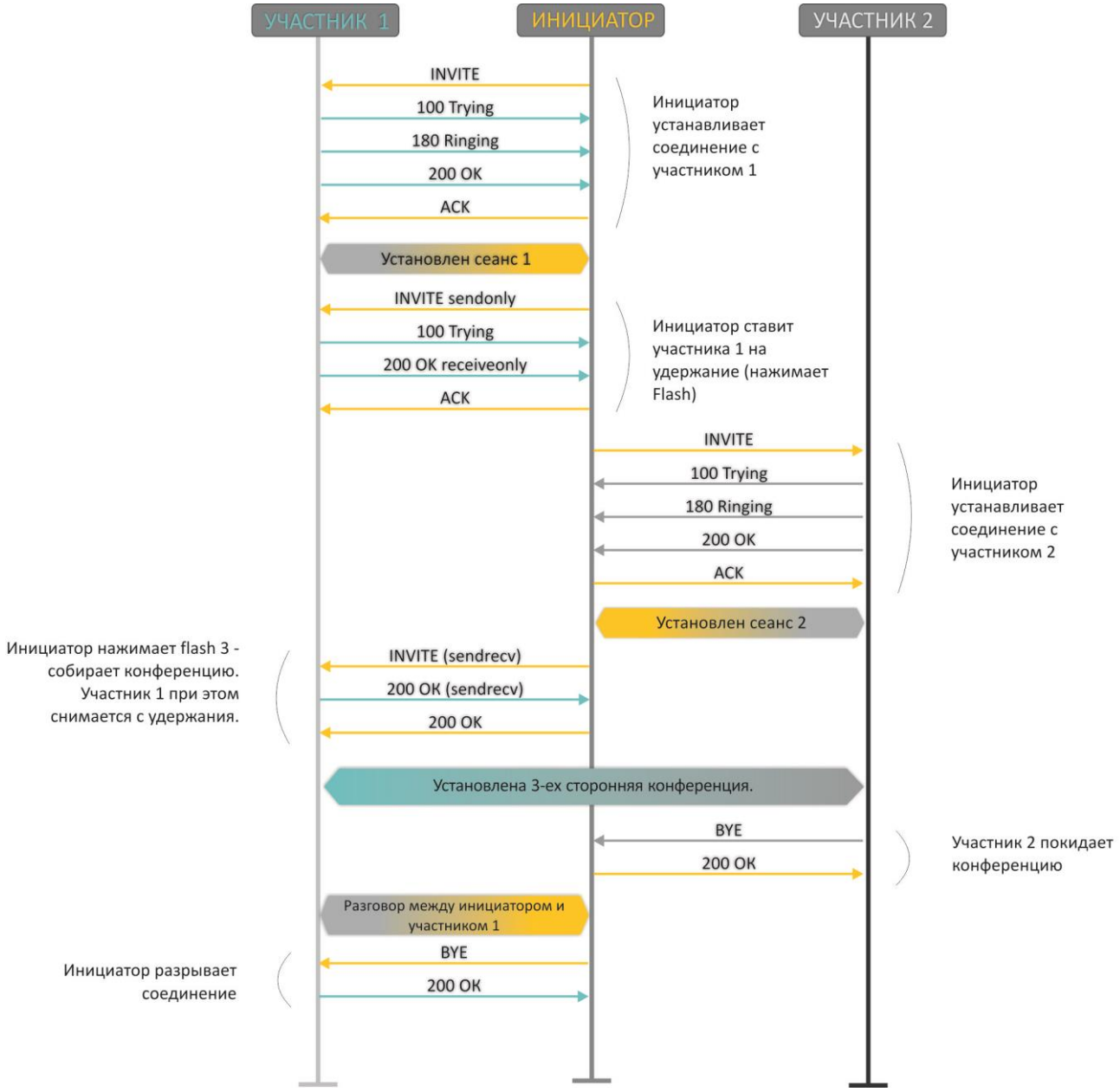
Возможно два режима работы трехсторонней конференции: локальный и удаленный. В первом режиме конференция собирается локально абонентом-инициатором, во втором – конференция устанавливается с помощью удаленного сервера, так называемого сервера конференции.

3.3.1 Локальная конференция

В режиме конференции нажатие короткого отбоя flash инициатором игнорируется. Сообщения протокола сигнализации, принятые от участников и переводящие сторону инициатора в режим удержания, приводят к выводу этого участника из конференции, при этом инициатор и второй участник переключатся в состояние обычного двустороннего разговора.

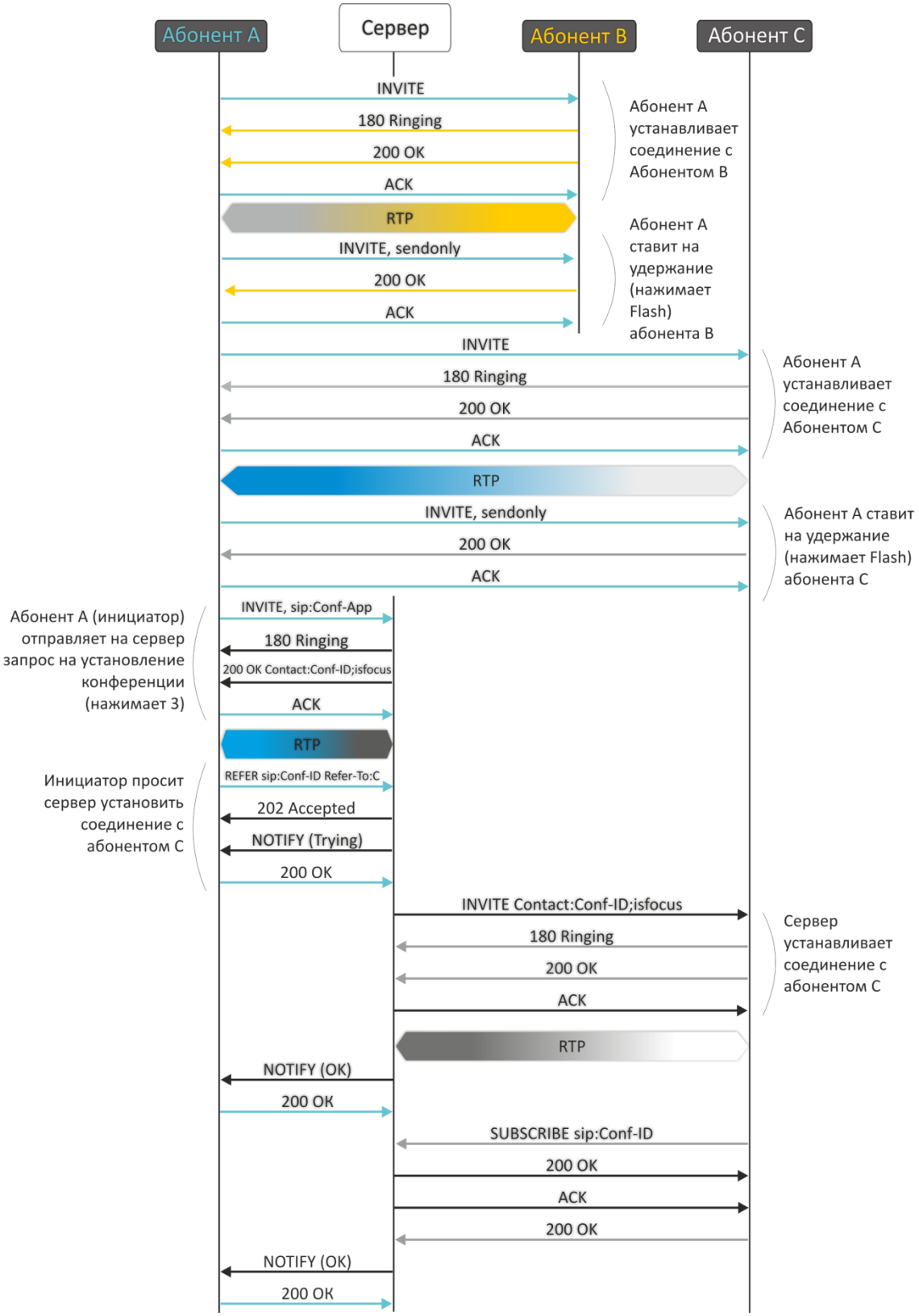
Конференция разрушается, если ее покидает инициатор, обоим участникам при этом будет передано сообщение отбоя. Если конференцию покидает любой из участников, то ее инициатор и второй участник переключатся в состояние обычного двустороннего разговора. Короткий отбой flash при этом обрабатывается как описано в разделах 3.1 Передача вызова и 3.2 Уведомление о поступлении нового вызова – Call Waiting.

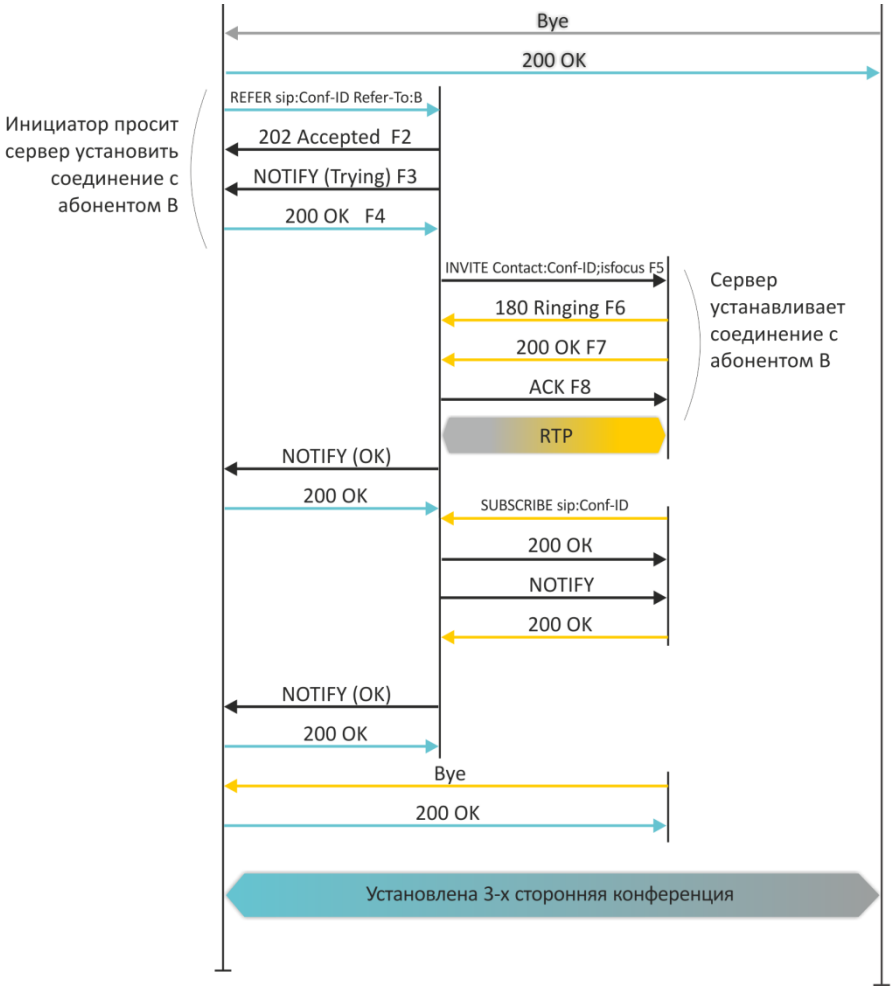
На рисунке ниже представлен алгоритм выполнения услуги «3-way conference» локально абонентом B по протоколу SIP.



3.3.2 Удаленная конференция

Удаленная конференция работает по алгоритму, описанному в RFC4579. Особенность алгоритма состоит в том, что по нажатию flash+3 абонент-инициатор устанавливает соединение с сервером конференции (называемым также фокусом), после чего просит фокус установить соединение с двумя другими участниками конференции. Ниже на рисунке детально изображен алгоритм работы.


Абонент A
Сервер
Абонент B
Абонент C
INVITE
180 Ringing
200 OK
ACK
RTP
INVITE, sendonly
200 OK
ACK
Абонент A устанавливает соединение с Абонентом B
Абонент A ставит на удержание (нажимает Flash) абонента B
INVITE
180 Ringing
200 OK
ACK
RTP
INVITE, sendonly
200 OK
ACK
Абонент A устанавливает соединение с Абонентом C
Абонент A ставит на удержание (нажимает Flash) абонента C
Абонент A (инициатор) отправляет на сервер запрос на установление конференции (нажимает 3)
INVITE, sip:Conf-App
180 Ringing
200 OK Contact:Conf-ID;isfocus
ACK
RTP
Инициатор просит сервер установить соединение с абонентом C
REFER sip:Conf-ID Refer-To:C
202 Accepted
NOTIFY (Trying)
200 OK
INVITE Contact:Conf-ID;isfocus
180 Ringing
200 OK
ACK
RTP
Сервер устанавливает соединение с абонентом C
NOTIFY (OK)
200 OK
SUBSCRIBE sip:Conf-ID
200 OK
ACK
200 OK
NOTIFY (OK)
200 OK

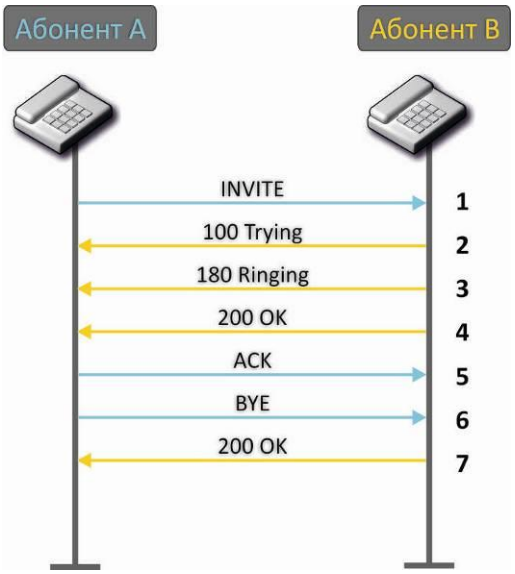

Bye
200 OK
REFER sip:Conf-ID Refer-To:B
Инициатор просит сервер установить соединение с абонентом B
202 Accepted F2
NOTIFY (Trying) F3
200 OK F4
INVITE Contact:Conf-ID;isfocus F5
Сервер устанавливает соединение с абонентом B
180 Ringing F6
200 OK F7
ACK F8
RTP
NOTIFY (OK)
200 OK
SUBSCRIBE sip:Conf-ID
200 OK
NOTIFY
200 OK
NOTIFY (OK)
200 OK
Bye
200 OK
Установлена 3-х сторонняя конференция

4 АЛГОРИТМЫ УСТАНОВЛЕНИЯ СОЕДИНЕНИЯ

4.1 Алгоритм успешного вызова по протоколу SIP

Протокол SIP (Session Initiation Protocol) – протокол установления сеанса обеспечивает выполнение базовых задач управления вызовом, таких как открытие и завершение сеанса.

Протокол SIP определяет 3 основных сценария установления соединения: между пользователями, с участием прокси-сервера, с участием сервера переадресации. Основные алгоритмы установления соединения описаны в документе IETF RFC 3665. В данном разделе приведен пример сценария установления соединения по протоколу SIP между двумя шлюзами, которым заранее известны IP-адреса друг друга.

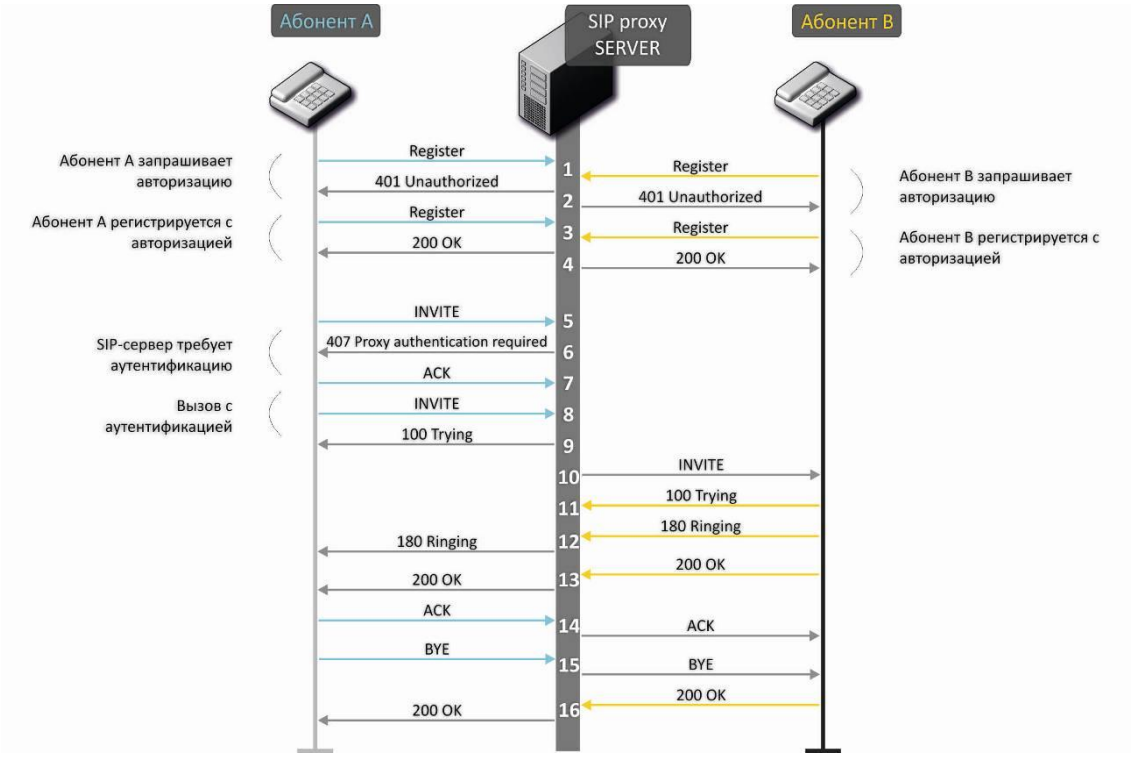


Описание алгоритма:

1. Абонент «A» вызывает абонента «B».
2. Шлюз абонента «B» принял команду на обработку.
3. Абонент «B» свободен. В этот момент на аппарат абонента «B» выдается «Посылка вызова», а абоненту «A» — «Контроль посылки вызова».
4. Абонент «B» отвечает на вызов.
5. Шлюз абонента «A» подтверждает установление сессии.
6. Отбой абонента «A», абоненту «B» выдается акустический сигнал «Занято».
7. Шлюз абонента «B» подтверждает принятую команду отбоя.

4.2 Алгоритм вызова с участием SIP прокси-сервера

В данном разделе описывается сценарий установления соединения между двумя шлюзами с участием SIP прокси-сервера. В этом случае вызывающий шлюз (абонент A) должен знать постоянный адрес абонента и IP-адрес прокси-сервера. SIP прокси-сервер обрабатывает сообщения, полученные от «абонента A», выполняет поиск «абонента B», приглашает к сеансу связи и выполняет функции маршрутизатора между двумя шлюзами.



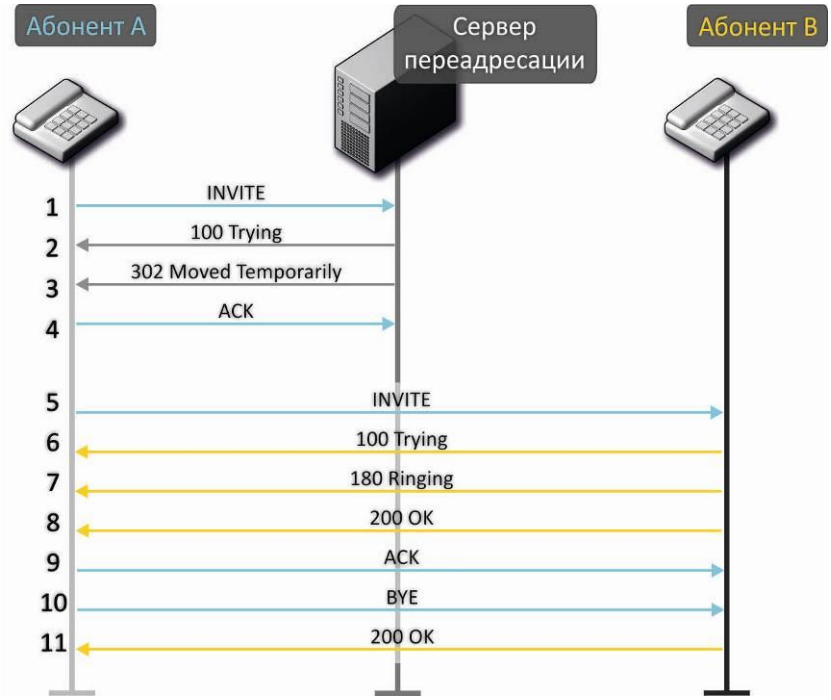
Описание алгоритма:

Регистрация на SIP-сервере.

1. Абонент «A» и абонент «B» регистрируются на SIP-сервере.
2. SIP-сервер запрашивает авторизацию.
3. Абонент «A» и абонент «B» регистрируются на SIP-сервере с авторизацией.
4. Ответ SIP-сервера об успешной регистрации.
5. Абонент «A» вызывает абонента «B».
6. Запрос аутентификации от SIP-сервера.
7. Шлюз абонента «A» подтверждает принятую команду на запрос авторизации.
8. Абонент «A» вызывает абонента «B».
9. SIP-сервер принял команду на обработку.
10. SIP-сервер транслирует запрос вызова абонентом «A» абонента «B».
11. Шлюз абонента «B» принял команду на обработку.
12. Абонент «B» свободен. В этот момент на аппарат абонента «B» выдается «Посылка вызова», а абоненту «A» — «Контроль посылки вызова».
13. Абонент «B» отвечает на вызов.
14. Шлюз абонента «A» подтверждает установление сессии.
15. Отбой абонента «A», абоненту «B» выдается акустический сигнал «Занято».
16. Шлюз абонента «B» подтверждает принятую команду отбоя.

4.3 Алгоритм вызова с участием сервера переадресации

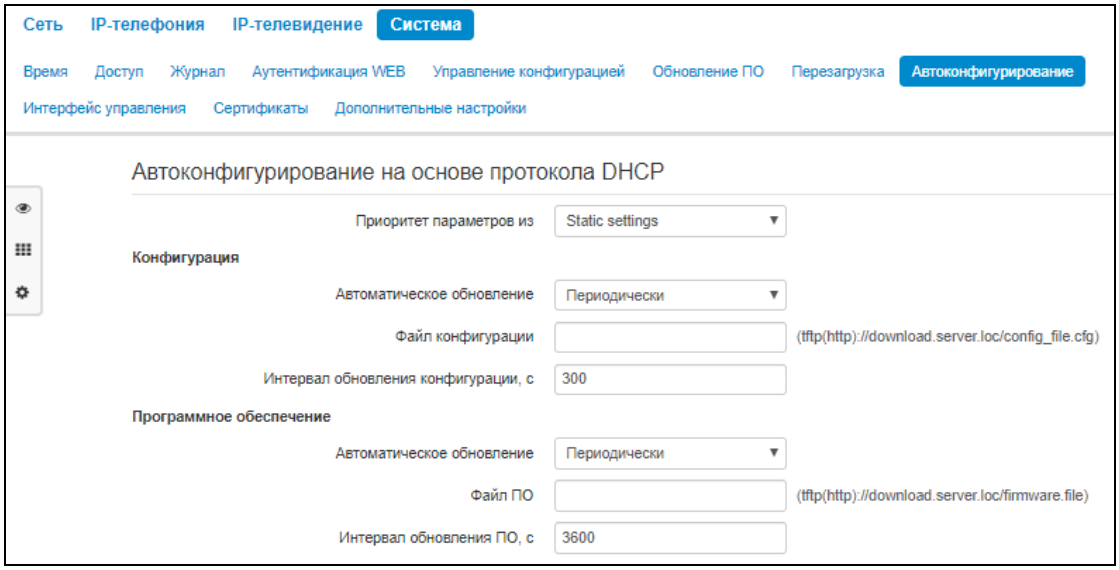
В данном разделе описывается сценарий установления соединения между двумя шлюзами с участием сервера переадресации. В этом случае вызывающий шлюз (абонент A) самостоятельно устанавливает соединение, а сервер переадресации лишь реализует преобразование постоянного адреса вызываемого абонента в его текущий адрес. Адрес сервера переадресации абонент получает от администратора сети.



Описание алгоритма:

1. Абонент «A» вызывает абонента «B». Вызов направляется на сервер переадресации с информацией об адресе вызываемого абонента.
2. Сервер переадресации принял команду на обработку.
3. Сервер переадресации запросил информацию о текущем адресе абонента «B» у сервера местоположения. Полученная информация (текущий адрес вызываемого пользователя или список зарегистрированных адресов вызываемого пользователя) передается в сообщении «302 moved temporarily» абоненту «A».
4. Шлюз абонента «A» подтверждает прием ответа от сервера переадресации.
5. Абонент «A» напрямую вызывает абонента «B».
6. Шлюз абонента «B» принял команду на обработку.
7. Абонент «B» свободен. В этот момент на аппарат абонента «B» выдается «Посылка вызова», а абоненту «A» — «Контроль посылки вызова».
8. Абонент «B» отвечает на вызов.
9. Шлюз абонента «A» подтверждает установление сессии.
10. Отбой абонента «A», абоненту «B» выдается акустический сигнал «Занято».
11. Шлюз абонента «B» подтверждает принятую команду отбоя.

5 АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP



Алгоритм работы процедуры автоматического обновления устройства определяется значением параметра *«Приоритет параметров из»*.

Если выбрано значение «*Static settings*», то из параметров *«Файл конфигурации»* и *«Файл ПО»* определяется полный путь (включая протокол доступа и адрес сервера) к файлам конфигурации и программного обеспечения. Полный путь указывается в формате URL (поддерживаются протоколы HTTP и TFTP):

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

<protocol> – протокол, используемый для загрузки соответствующего файла с сервера (поддерживаются протоколы HTTP и TFTP);

<server address> – адрес сервера, с которого необходимо загрузить файл (доменное имя или IPv4);

<path to file> – путь к файлу на сервере.

В URL допускается использование следующих макросов (зарезервированные слова, вместо которых устройство подставляет определенные значения):

$MA – MAC address – вместо данного макроса в URL файла устройство подставляет собственный MAC-адрес;

$SN – Serial number – вместо данного макроса в URL файла устройство подставляет собственный серийный номер;

$PN – Product name – вместо данного макроса в URL файла устройство подставляет название модели (например, TAU-4M.IP);

$SWVER – Software version – вместо данного макроса в URL файла устройство подставляет номер версии программного обеспечения;

$HWVER – Hardware version – вместо данного макроса в URL файла устройство подставляет номер аппаратной версии устройства.

MAC-адрес, серийный номер и название модели можно узнать на странице мониторинга в разделе «Устройство».

Примеры URL:

tftp://download.server.loc/firmware.file,
http://192.168.25.34/configs/tau4m/my.cfg,
tftp://server.tftp/$PN/config/$SN.cfg,
http://server.http/$PN/firmware/$MA.frm и т.д.

При этом допускается опускать некоторые параметры URL. Например, файл конфигурации можно задать в таком формате:

http://192.168.18.6
или
config_tau4m.cfg

Если из URL-файла конфигурации или программного обеспечения не удаётся извлечь все необходимые для загрузки файла параметры (протокол, адрес сервера или путь к файлу на сервере), будет произведена попытка извлечь неизвестный параметр из DHCP-опций 43 (Vendor specific info) или 66 (TFTP server) и 67 (Boot file name), в случае если в услуге Интернет установлено получение адреса по протоколу DHCP (формат и анализ DHCP-опций будет приведён ниже). Если из DHCP-опций не получается извлечь недостающий параметр, будет использоваться заданное значение по умолчанию:

- для протокола: tftp;
- для адреса сервера: update.local;
- для имени файла конфигурации: tau4m.cfg;
- для имени файла программного обеспечения: tau4m.fw.

Таким образом, если поля *«Файл конфигурации»* и «*Файл ПО»* оставить пустыми, и по протоколу DHCP не будет получены опции 43 или 66, 67 с указанием местоположения этих файлов – URL файла конфигурации будет иметь вид:

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

а URL файла ПО:

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

Если выбрано значение «DHCP options», URL файлов конфигурации и программного обеспечения извлекаются из DHCP-опций 43 (Vendor specific info) или 66 (TFTP server) и 67 (Boot file name), для чего в услуге Интернет должно быть установлено получение адреса по протоколу DHCP (формат и анализ DHCP-опций будет приведён ниже). Если из DHCP-опций не удается определить какой-нибудь параметр URL – для него используется заданное значение по умолчанию:

- для протокола: tftp;
- для адреса сервера: update.local;

- для имени файла конфигурации: tau4m.cfg;
- для имени файла программного обеспечения: tau4m.fw.

Формат опции 43 (Vendor specific info)

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

1 - код адреса сервера автоконфигурирования по протоколу TR-069;
2 - код для указания параметра Provisioning code;
3 - код имени пользователя для авторизации на сервере TR-069;
4 - код пароля для авторизации на сервере TR-069;
5 - код адреса сервера; адрес сервера задается в формате URL: tftp://address или http://address. В первом варианте указан адрес сервера TFTP, во втором – HTTP;
6 - код имени файла конфигурации;
7 - код имени файла ПО;

"|" - обязательный разделительный символ между кодами и значениями подопций.

Для автоконфигурирования по протоколу TR-069 подопции 1, 3 и 4 будут применяться, когда в разделе автоконфигурирования на основе протокола DHCP будет выбран приоритет из DHCP-опций.

Алгоритм определения параметров URL файлов конфигурации и программного обеспечения из DHCP-опций 43 и 66

1. Инициализация DHCP-обмена

После загрузки устройство инициирует DHCP-обмен.

2. Анализ опции 43

При получении опции 43 выполняется анализ подопций с кодами 5, 6 и 7 с целью определения адреса сервера и имён файлов конфигурации и программного обеспечения.

3. Анализ опции 66

Если опция 43 от DHCP-сервера не получена либо получена, но из неё не удалось извлечь адрес сервера – осуществляется поиск опции 66. Если имя файла ПО также не удалось получить – осуществляется поиск опции 67. Из них извлекаются соответственно адрес сервера TFTP и путь к файлу ПО. Далее файлы конфигурации и программного обеспечения будут загружаться с адреса из опции 66 по протоколу TFTP.

Особенности обновления конфигурации

Файл конфигурации должен иметь формат **.tar.gz** (в данном формате происходит сохранение конфигурации через Web-интерфейс в закладке «Система» - «Управление конфигурацией»). Загруженная с сервера конфигурация применяется автоматически без перезагрузки устройства.

Особенности обновления программного обеспечения

Файл программного обеспечения должен иметь формат .tar.gz. После загрузки файла ПО осуществляется его распаковка и проверка версии (по содержимому файла version в tar.gz-архиве).

Если текущая версия программного обеспечения совпадает с версией файла, полученного по протоколу DHCP, обновление ПО производиться не будет. Обновление производится только в случае

несовпадения версий. О запущенном процессе записи образа программного обеспечения во flash-память устройства свидетельствует поочередное циклическое мигание индикатора «Power» зеленым, оранжевым и красным цветом.

Не отключайте питание и не перезагружайте устройство во время записи образа во flash-память. Данные действия приведут к частичной записи ПО, что равноценно порче загрузочного раздела устройства. Дальнейшая работа устройства будет невозможна. Для восстановления работоспособности устройства воспользуйтесь инструкцией, которая приведена в разделе 6.

6 ПРОЦЕДУРА ВОССТАНОВЛЕНИЯ СИСТЕМЫ ПОСЛЕ СБОЯ ПРИ ОБНОВЛЕНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Если при выполнении процедуры обновления программного обеспечения (через Web-интерфейс или через механизм автоматического обновления на основе протокола DHCP) произошел сбой (например, из-за случайного отключения питания), в результате чего дальнейшая работа устройства стала невозможной (индикатор «Power» постоянно горит красным цветом), воспользуйтесь следующим алгоритмом восстановления работоспособности устройства:

- Распакуйте архив с файлом программного обеспечения.
- Подключите ПК к порту WAN устройства, установите на сетевом интерфейсе адрес из подсети 192.168.1.0/24.
- Запустите на ПК TFTP-клиента (для Windows рекомендуется использовать программу Tftpd32), в качестве адреса удалённого хоста укажите 192.168.1.6, а для передачи выберите файл linux.bin из распакованного архива программного обеспечения.
- Запустите команду отправки файла на удаленный хост (команда **Put**). Должен запуститься процесс передачи файла на устройство *TAU-4M.IP*.
- Если процесс передачи файла начался – дождитесь его окончания, после чего *TAU-4M.IP* произведет запись программного обеспечения в память и автоматически выполнит запуск системы. Время записи составляет около 5 минут. Об успешном восстановлении устройства свидетельствует оранжевый или зеленый цвет индикатора «Power». При этом на устройстве сохраняется конфигурация, которая была до сбоя. Если подключиться к устройству не удаётся – произведите сброс до заводских настроек.
- Если процесс передачи файла не начался, убедитесь в корректности сетевых настроек компьютера и попробуйте еще раз. В случае неудачи устройство необходимо отправить в ремонт либо выполнить восстановление, подключившись к устройству по COM-порту через специальный адаптер (при его наличии).

ПРИЛОЖЕНИЕ А. РАСЧЕТ ДЛИНЫ ТЕЛЕФОННОЙ ЛИНИИ

Таблица 6 – Зависимость электрического сопротивления 1 км цепей абонентских кабельных линий постоянному току при температуре окружающей среды 20°С от применяемого кабеля.

Марка кабеля для АЛГТС	**Диаметр жилы, мм**	**Электрическое сопротивление 1 км цепи, Ом, не более**	**Длина линии (другие ТА), км**	**Длина линии (ТА Русь), км**
ТПП, ТППэп, ТППЗ, ТППэпЗ, ТППБ, ТПП эпБ, ТППЗБ, ТППБГ, ТППэпБГ, ТППББШп, ТППэпББШп, ТППЗББШп, ТППЗэпББШп, ТППт	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
ТПВ, ТПЗБГ	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
ТГ, ТБ, ТБГ, ТК	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
ТСтШп, ТАШп	0,50	192,0	8,438	3,646
	0,70	96,0	16,875	7,292
ТСВ	0,40	296,0	5,473	2,365
	0,50	192,0	8,438	3,646
КСПЗП	0,64	116,0	13,966	6,034
КСПП, КСПЗП, КСППБ, КСПЗПБ, КСППт, КСПЗПт, КСПЗПК	0,90	56,8	28,521	12,324

ПРИЛОЖЕНИЕ Б. ЗАПУСК ПРОИЗВОЛЬНОГО СКРИПТА ПРИ СТАРТЕ СИСТЕМЫ

Периодически возникает необходимость при старте устройства выполнять определённые действия, которые нельзя осуществить заданием определенных настроек через файл конфигурации. Для этого случая в устройстве *TAU-4M.IP* предусмотрена возможность через конфигурационный файл настроить запуск произвольного скрипта, в который можно поместить любую желаемую последовательность команд.

Для запуска произвольного скрипта в файле конфигурации создана секция настроек:

```
UserScript:
Enable: "0"
URL: ""
```

Опция «Enable» разрешает (если значение 1) или запрещает (если значение 0) запуск скрипта, путь к которому указан в параметре URL.

Запускаемый скрипт может располагаться как на удалённом сервере, так и на самом устройстве. С удалённого сервера скрипт может быть загружен посредством протоколов HTTP или TFTP. Рассмотрим примеры файла конфигурации для запуска пользовательского скрипта с разных источников.

1. Запуск с HTTP-сервера
   Для запуска скрипта с HTTP-сервера необходимо в параметре URL указать полный путь к файлу в формате HTTP-URL:
   URL: “http://192.168.0.250/user-script/script.sh”
   В этом случае после старта устройства файл script.sh, хранящийся в каталоге user-script по адресу 192.168.0.250, автоматически загрузится по протоколу HTTP с указанного сервера, после чего будет произведён его запуск.
2. Запуск с TFTP-сервера
   Для запуска скрипта с TFTP-сервера необходимо в параметре URL указать полный путь к файлу в формате TFTP-URL:
   URL: “tftp://192.168.0.250/user-script/script.sh”
   В этом случае после старта устройства файл script.sh, хранящийся в каталоге user-script по адресу 192.168.0.250, автоматически загрузится по протоколу TFTP с указанного сервера, после чего будет произведён его запуск.
3. Запуск локального скрипта
   Ввиду особенностей файловой системы локальный скрипт должен располагаться только в каталоге /etc/config, так как только содержимое этого каталога сохраняется после перезагрузки устройства. Скрипт в каталоге /etc/config можно создать либо с помощью редактора vi, либо загрузить его с внешнего TFTP-сервера (командой tftp –gl user.sh <TFTP-server address>). После создания скрипта ему необходимо назначить права на запуск командой chmod 777 /etc/config/user.sh.
   В файле конфигурации URL для запуска локального скрипта имеет вид:
   URL: “File://etc/config/user.sh”

Важно отметить, что пользовательский скрипт должен начинаться с директивы #!/bin/sh.

ПРИЛОЖЕНИЕ В. НАСТРОЙКА DHCP-КЛИЕНТОВ В МУЛЬТИСЕРВИСНОМ РЕЖИМЕ

На устройствах TAU-4M.IP, начиная с версии 1.14.1, имеется возможность настраивать опции, получаемые DHCP-клиентами на разных интерфейсах.

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

Согласно приведенной таблице, опции 1, 3, 6, 26, 28, 33, 121, 249 могут запрашиваться DHCP-клиентами для каждого сабинтерфейса. Соответственно, данные опции будут индивидуально применены для каждого сабинтерфейса. Опции 12, 15, 40, 41, 42, 43, 66, 67, 120 могут запрашиваться и применяться только для одного DHCP-клиента, так как они общесистемные, т.е., не приводят к настройке сетевого интерфейса.

Конфигурацию списка запрашиваемых опций можно изменять, и хранится она, как и все остальные настройки, в конфигурационном файле: **/etc/config/cfg.yaml.** По умолчанию списки опций не

прописаны (в конфигурации — следующая запись: DHCPOptionList: ""), это значит, что опции запрашиваются и применяются согласно приведённой выше таблице.

Способы редактирования конфигурации

I. С помощью редактора *vi*

1. Список опций для интерфейса Internet задаётся в параметре DHCPOptionList секции Internet=>Network.
2. Список опций для интерфейса VoIP задаётся в параметре DHCPOptionList секции Voip=>Network.
3. Список опций для интерфейса Management задаётся в параметре DHCPOptionList секции System=>ManagementVLAN.

После редактирования и сохранения в редакторе *vi* необходимо выполнить следующие команды:

- ***reloadcfg*** - применяем измененную конфигурацию в работу, результат выполнения команды должен быть "Configuration accepted";
- ***save*** - сохраняем измененную конфигурация в энергонезависимую память.

Команду *save* можно выполнять только в случае успешного выполнения предыдущей команды. Если при выполнении команды *reloadcfg* результат был "Configuration not accepted", *save* выполнять запрещено.

II. С помощью команды *setconf*

Данный метод — рекомендуемый. Также он избавляет от необходимости выполнения команд reloadcfg и save. **getconf** (вывести на экран текущую конфигурацию) и **setconf** (установить значение параметра).

Пример 1. Необходимо получить значение DHCPOptionList:

для интерфейса Internet

getconf Internet.Network | grep DHCPOptionList

для интерфейса VoIP

getconf Voip.Network | grep DHCPOptionList

для интерфейса Management

getconf System.ManagementVLAN | grep DHCPOptionList

Пример 2. Необходимо назначить некоторый список опций:

для интерфейса Internet

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

для интерфейса VoIP (назначаем список опций по умолчанию)

setconf Voip.Network DHCPOptionList ""

для интерфейса Management

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

III. Конфигурирование на персональном компьютере

Предварительно скачивается конфигурация с устройства на ПК (через Web-интерфейс), далее с помощью любого текстового редактора меняются значения, сохраняются изменения. Завершающим этапом является загрузка измененной конфигурации в устройство.

Использование данного метода не рекомендуется!

Правила редактирования DHCPOptionList

1. Допустимые значения: 3,6,12,15,26,28,33,40,41,42,43,66,67,120,121,249;
2. Опции в параметре DHCPOptionList указываются через запятую и без пробелов между опциями, пример DHCPOptionList: "3,6,12,15,26,120,121";
3. Порядок следования опций в DHCPOptionList неважен;
4. Каждая из опций 12, 15, 40, 41, 42, 43, 66, 67, 120 может быть запрошена и применена только с одного интерфейса;
5. Опции 1, 3, 6, 26, 28, 33, 121, 249 могут запрашиваться DHCP-клиентами для каждого сабинтерфейса;
6. Опции 66 и 67 должны быть указаны на одном и том же интерфейсе;
7. Если в DHCPOptionList ничего не указано, то тогда список запрашиваемых опций — по умолчанию (с учетом пункта 8);
8. Если в DHCPOptionList указаны опции (из пункта 4), которые по умолчанию запрашиваются с другого интерфейса (на котором DHCPOptionList не заполнен), то тогда опции будут запрашиваться с первого интерфейса, а на втором — данные опции будут исключены из списка по умолчанию *;
9. Если для интерфейса в DHCPOptionList указан список опций, то будут запрашиваться только эти опции;
10. Опцию 1 в DHCPOptionList нельзя указывать, она запрашивается и применяется всегда и со всех интерфейсов независимо от прочих настроек.

Если какой-либо из пунктов нарушен, то при применении конфигурации будет выведено сообщение "Configuration not accepted". Ошибку в конфигурации можно узнать, если включить логи configd, тогда при применении конфигурации будет подробно указана причина, по которой конфигурация не применена.

*** Пример к пункту 8:**

Допустим, для интерфейса Internet указан следующий список опций: Internet.Network.DHCPOptionList: "3, 6, 26, 28, 33, 121, 249, 12"

А для интерфейса management ничего не указано: System.ManagementVLAN.DHCPOptionList: ""

тогда, согласно пункту 7, должен быть запрошен список опций по умолчанию 3, 6, 12, 15, 26, 28, 33, 40, 41, 42, 43, 66, 67, 121, 249, но так как опция 12 указана явно на интерфейсе Internet, то из этого списка она будет исключена.

В итоге списки будут выглядеть следующим образом:

значение параметра: Internet.Network.DHCPOptionList: "3, 6, 26, 28, 33, 121, 249, 12"

запрашиваемый список опций: 1, 3, 6, 26, 28, 33, 121, 249, 12

значение параметра: System.ManagementVLAN.DHCPOptionList: ""
запрашиваемый список опций: 1, 3, 6, 15, 26, 28, 33, 40, 41, 42, 43, 66, 67, 121, 249

После редактирования DHCPOptionList рекомендуется перезагрузка устройства. До перезагрузки корректная работа устройства не гарантируется.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ООО «Предприятие «ЭЛТЕКС» Вы можете обратиться в Сервисный центр компании:

Российская Федерация ,630020, г. Новосибирск, ул. Окружная, дом 29в.
E-mail: techsupp@eltex.nsk.ru
На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к в базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: http://eltex-co.ru/
Технический форум: http://forum.eltex-co.ru/
База знаний: http://kcs.eltex.nsk.ru/
Центр загрузок: http://eltex-co.ru/support/downloads/