Комплексные решения для построения сетей

RG-2400/RG-4400

RG-2402G, RG-2404G, RG-2402G-W, RG-2404G-W
RG-4402G-W, RG-4402GF-W

Руководство по эксплуатации, версия 1.5 (03.2015)

Абонентский шлюз IP-телефонии

IP-адрес: http://192.168.1.1

имя пользователя: admin

пароль: password

http://www.элтекс.рф/dokumentatsiya
http://www.eltex.nsk.ru/dokumentatsiya

Версия документа	Дата выпуска	Содержание изменений
Версия 1.5	16.03.2015	Добавлено описание RG-4402GF-W. Синхронизация с версией ПО 1.12.0 Добавлено: - 3.6.3.9 Подменю «История вызовов» - 3.6.6.9 Подменю «VLAN управления» - 3.7.10 Подменю «История вызовов» Изменения: - 2 Описание изделия - 3.5.1 Интернет - 3.6.2.1 Подменю «Интернет» - 3.6.2.5 Подменю «NAT и проброс портов» - 3.6.3.1 Подменю «Настройки сети» - 3.6.3.2 Подменю «Настройка линий» - 3.6.3.3 Подменю «Профили» - 3.6.6.2 Подменю «Доступ» - 3.6.6.5 Подменю «Управление конфигурацией» - 3.6.6.6 Подменю «Обновление ПО» - 3.6.6.8 Подменю «Автоконфигурирование» - 3.6.6.10 Подменю «Дополнительные настройки» - 3.7.1 Подменю «Интернет» - 3.7.2 Подменю «IP-телефония» - 6 Алгоритм работы автоматического обновления устройства на основе протокола DHCP
Версия 1.4	06.11.2014	Добавлено описание RG-4402G-W. Синхронизация с версией ПО 1.10.1 Добавлено: - 3.6.3.8 Подменю «Сигнал вызова» - 3.6.5 Меню «Локальные интерфейсы» Изменения: - 3.5.1 Интернет - 3.5.2 IP-телефония - 3.6.2.1 Подменю «Интернет» - 3.6.3.1 Подменю «Настройки сети» - 3.6.3.3 Подменю «Профили» - 3.6.4.2 Подменю «STB» - 3.6.6.1 Подменю «Время»
Версия 1.3	11.04.2014	Синхронизация с версией ПО 1.9.0 Добавлено: -3.6.1.13 Подменю «Пользовательские VLAN» - Приложение Б. Запуск произвольного скрипта при старте системы Изменения: - 3.6.1.1 Подменю «Настройки сети» - 3.6.1.7 Подменю «Wi-Fi»
Версия 1.2	15.11.2013	Синхронизация с версией ПО 1.8.0
Версия 1.1	11.07.2013	Добавлено: - «Система» – «Время» - «Система» – «Доступ» Изменения: - «Выход в Интернет» – «Сетевые настройки» - «Система» – «Обновление ПО»
Версия 1.0	04.06.2013	Первая публикация
Версия программного обеспечения	Версия ПО: 1.12.0 Версия веб-интерфейса: 1.12.33	

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Описание
Полужирный шрифт	Полужирным шрифтом выделены примечания и предупреждения, название глав, заголовков, заголовков таблиц.
Курсивом Calibri	Курсивом Calibri указывается информация, требующая особого внимания.
	Аналоговый телефонный аппарат
	SIP-сервер
	Устройство семейства RG-2400/RG-4400
	Компьютер
	Цифровая телевизионная приставка STB
	«Подключение к сети»
	Беспроводная сеть

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

1 ВВЕДЕНИЕ

В настоящее время IP-телефония это одна из наиболее быстро развивающихся телекоммуникационных услуг. Для возможности предоставления VoIP-услуг абонентам сети разработаны абонентские шлюзы серии *RG-2400/RG-4400* (далее «устройство»): RG-2402G, RG-2404G, RG-2402G-W, RG-2404G-W, RG-4402G-W, RG4402GF-W.

Устройства выпускаются в различных модификациях, отличаются набором интерфейсов и функциональными возможностями.

Абонентские шлюзы IP-телефонии серии *RG-2400/RG-4400* обеспечивают подключение аналоговых телефонных аппаратов к сетям пакетной передачи данных, выход на которые осуществляется через интерфейсы 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 серии *RG-2400/RG-4400.*

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Устройство серии *RG-2400/RG-4400* – высокопроизводительный абонентский шлюз IP-телефонии с полным набором функций, позволяющих потребителю использовать преимущества IP-телефонии.

Абонентский шлюз серии *RG-2400/RG-4400* 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 до четырех компьютеров, доступ в интернет для которых возможен с помощью встроенных функций NAT/DHCP-сервера. USB-разъем используется для подключения внешних накопителей или 3G/4G USB-модема.

2.2 Варианты исполнения

Устройство выпускается в следующих модификациях, таблица 1:

Таблица 1 – Варианты исполнения

Наименование модели	Интерфейс WAN	Количество портов интерфейса LAN	Количество портов FXS	Наличие Wi-Fi
RG-2402G	RJ-45	4 Gigabit Ethernet	2	-
RG-2404G	RJ-45	4 Gigabit Ethernet	4	-
RG-2402G-W	RJ-45	4 Gigabit Ethernet	2	+
RG-2404G-W	RJ-45	4 Gigabit Ethernet	4	+
RG-4402G-W	RJ-45	4 Gigabit Ethernet	2	+
RG-4402GF-W	SFP	4 Gigabit Ethernet	2	+

Устройства RG-2402G-W, RG-2404G-W имеют встроенный адаптер Wi-Fi. Модели RG-2402G-W и RG-2404G-W обеспечивают возможность подключения до двух внешних антенн. Модели RG-4402G-W и RG-4402GF-W имеют две внутренние антенны. Встроенный адаптер Wi-Fi поддерживает технологию 802.11n, что позволяет предоставлять услуги передачи данных по беспроводной сети с более высоким качеством сервиса по сравнению с устройствами, поддерживающими стандарт 802.11g, оставаясь при этом обратно совместимым с устройствами 802.11g и 802.11b. Кроме этого поддерживается работа одновременно в двух диапазонах частот: 2.4 и 5 ГГц.

2.3 Характеристика устройства

Интерфейсы:

- FXS: 2 или 4[1] порта RJ-11;
- LAN: 4 порта Ethernet RJ-45 10/100/1000BASE-T;
- WAN: 1 порт Ethernet (RJ-45 10/100/1000BASE-T) или SFP 1000 BASE-X[3];
- WLAN: IEEE 802.11 a/b/g/n[2];
- 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;
- эхо компенсация (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 Response;

[1] только для моделей RG-2404G, RG-2404G-W
[2] только для моделей RG-2402G-W, RG-2404G-W, RG-4402G-W, RG-4402GF-W
[3] только для модели RG-4402GF-W

- безусловная переадресация – Call Forward Unconditional;
- не беспокоить – DND;
- Caller ID: FSK, DTMF;
- горячая линия – Hotline;
- групповой вызов;
- перехват вызова – Call Pickup;
- гибкий план нумерации;

- обновление ПО через web-интерфейс;
- поддержка DHCP-based autoprovisioning;
- TR-069;
- удаленный мониторинг, конфигурирование и настройка: Web-интерфейс, Telnet, SNMP.

На рисунке 1 приведена схема применения оборудования серии *RG-2400/RG-4400* на примере RG-2404G-W.

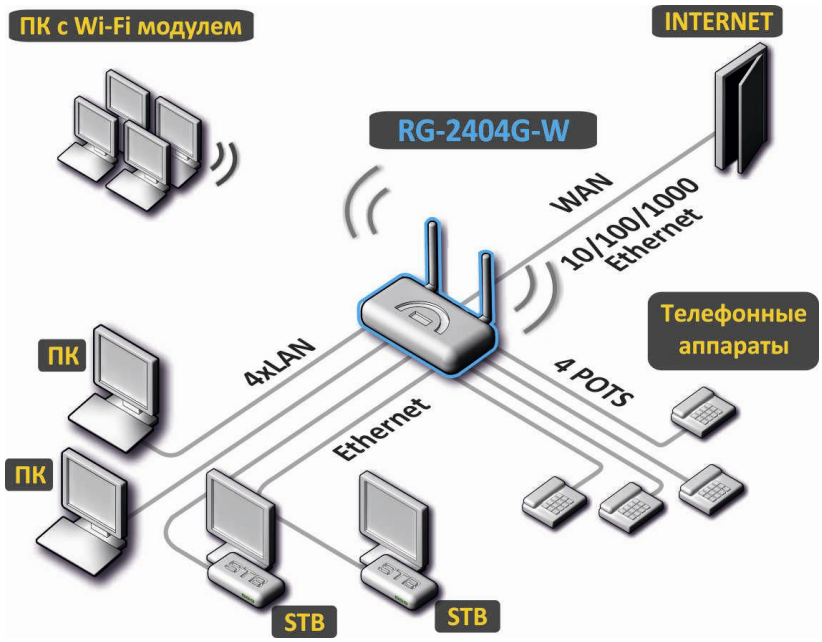


Рисунок 1 – Функциональная схема использования RG-2404G-W

2.4 Структура и принцип работы изделия

Абонентский терминал серии *RG-2400/RG-4400* состоит из следующих подсистем:

- контроллер, в состав которого входит:
  - высокоинтегрированная система на кристалле (System-on-a-Chip – SoC) Realtek RTL8954C, включающая в себя процессор, гигабитный 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;
- абонентские комплекты SLIC (2 или 4 порта FXS);
- Ethernet-коммутатор RJ-45 10/100/1000BASE-T на 4 порта – LAN;
- Ethernet-модуль WAN: RJ-45 10/100/1000BASE-T/SFP 1000 BASE-X[1];
- 802.11n dual-band Wi-Fi адаптер (только для моделей RG-2402G-W, RG-2404G-W, RG-4402G-W);
- USB Host порт.

Структурная схема устройства приведена на рисунке 2.

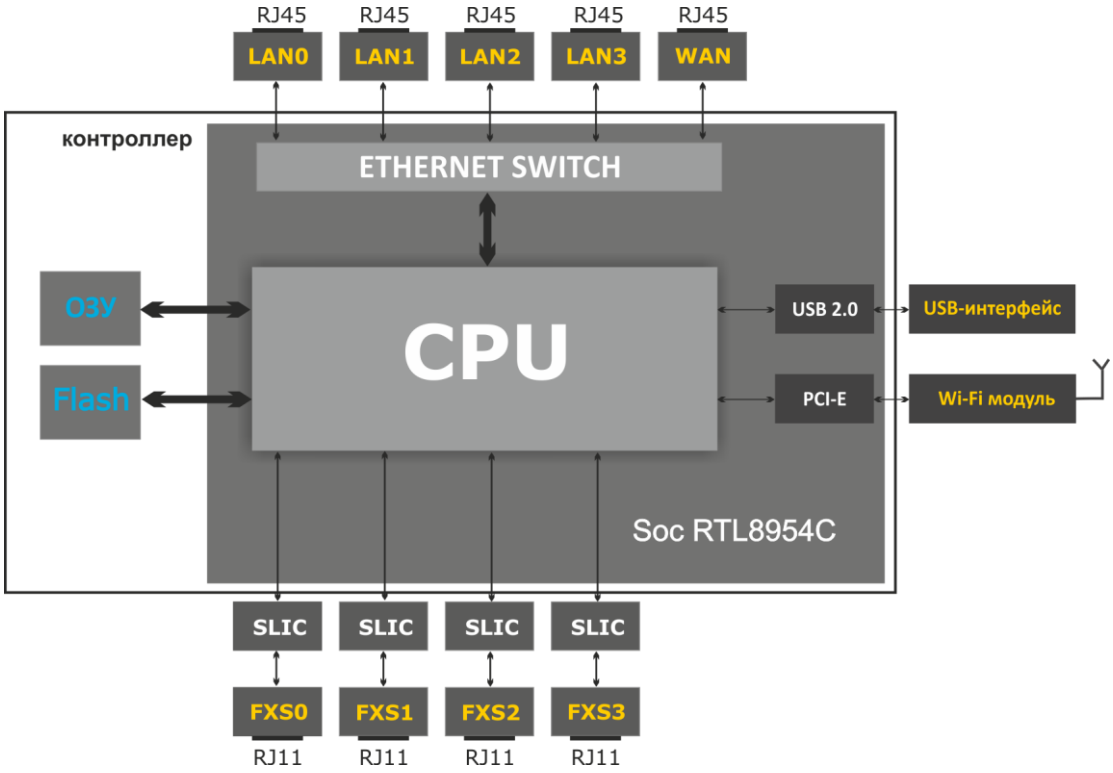


Рисунок 2 – Структурная схема RG-2404G-W

Структурная схема других устройств серии *RG-2400/RG-4400* отличается количеством портов FXS и отсутствием модуля Wi-Fi.

[1] только для модели RG-4402GF-W

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 серии *RG-2400/RG-4400* представлена на рисунке 3.

Рисунок 3 – Функциональная схема устройства серии *RG-2400/RG-4400*

2.5 Основные технические параметры

Основные технические параметры устройства приведены в таблице 2.

Таблица 2 – Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP

Аудиокодеки

Кодеки	G.729, annex A, annex B, G.711a, G.711u, G.723.1 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	10/100/1000, автоопределение
Поддержка стандартов	BASE-T, 1000 BASE-X[1]

Параметры LAN-интерфейса Ethernet

Количество интерфейсов	4
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100/1000, автоопределение
Поддержка стандартов	BASE-T

Параметры аналоговых абонентских портов

Количество портов:	RG-2402G, RG-2402G-W, RG-4402G-W, RG-4402GF-W	2
	RG-2404G, RG-2404G-W	4
Сопротивление шлейфа		до 2 кОм
Прием набора		импульсный/частотный (DTMF)
Защита абонентских окончаний		по току и по напряжению
Выдача Caller ID		FSK BELL202/FSK V.23/DTMF
Параметры беспроводного интерфейса[2]		
Стандарты		802.11 a/b/g/n
Частотный диапазон, МГц		2.4 ~ 2.4835 ГГц, 5.15 ~ 5.35 ГГц
Модуляция		BPSK, QPSK, 16 QAM, 64 QAM, DBPSK, DQPSK, CCK
Скорость передачи данных, Мбит/с		**802.11b(CCK):** 1, 2, 5.5 ,11 **802.11g(OFDM):** 6, 9, 12 , 18, 24, 36, 48, 54 **811n (HT20, 800ns GI):** 13, 26, 39, 78, 104, 117, 130 **802.11n (HT40, 400ns GI):** 30, 60, 90, 120, 180, 240, 270, 300 **802.11n (HT40, 800ns GI):** 27, 54, 81, 108, 162, 216, 243, 270
Максимальная выходная мощность передатчика		**802.11b: 16dBm** **802.11g: 11dBm** **802.11n(20MHz MCS0/8):** 19 dBm **802.11n(20MHz MCS7/15):** 12 dBm **802.11n(40MHz MCS0/8):** 19 dBm **802.11n(40MHz MCS7/15):** 11 dBm
Чувствительность приемника		**802.11b:** -83 dBm **802.11g:** -70 dBm **802.11n(20MHz MCS7):** -67 dBm **802.11n(20MHz MCS15):** -66 dBm **802.11n(40MHz MCS7):** -65 dBm

[1] только для модели RG-4402GF-W

[2] Только для моделей RG-2402G-W, RG-2404G-W

Безопасность		64/128/152-битное WEP-шифрование данных; WEP, TKIP и AES
Управление		
Удаленное управление		Web-интерфейс, Telnet, SNMP
Ограничение доступа		по паролю
Общие параметры		
Питание		адаптер питания 12V DC, 2 A.
Потребляемая мощность	RG-2404G	не более 10 Вт
	RG-2404G-W	не более 12 Вт
	RG-2402G	не более 7.5 Вт
	RG-2402G-W	не более 9 Вт
	RG-4402G-W	не более 10 Вт
	RG-4402GF-W	не более 11,5 Вт
Рабочий диапазон температур		от +5 до +40°C
Относительная влажность при температуре 25°C		до 80%
Габариты	серия RG-2400	218x120x49 мм
	серия RG-4400	187x125x32 мм
Масса		не более 0,3 кг.

2.6 Конструктивное исполнение

Абонентский терминал серии RG-2400/RG-4400 выполнен в пластиковом корпусе размерами 218x120x49 мм.

2.6.1 Передняя панель устройства

Внешний вид передней панели устройства RG-2404G-W приведен на рисунке 4.

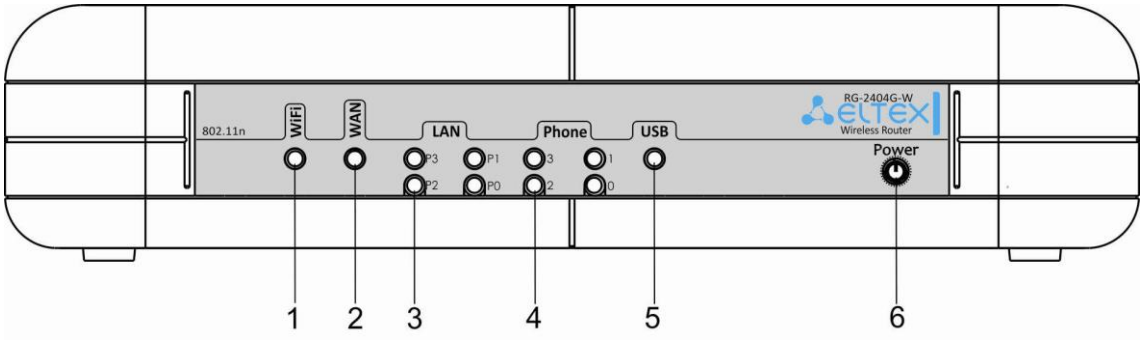


Рисунок 4 – Внешний вид передней панели RG-2404G-W

На передней панели устройства серии *RG-2400/RG-4400* расположены следующие световые индикаторы и органы управления, таблица 3.

Таблица 3 – Описание индикаторов и органов управления передней панели

Элемент передней панели		Описание
1	WiFi[1]	индикатор работы беспроводной сети
2	WAN	индикатор WAN-интерфейса
3	LAN	индикаторы портов LAN-интерфейса
4	Phone	индикаторы работы аналоговых телефонных аппаратов
5	USB	индикатор работы внешнего USB-устройства (USB flash, внешний жесткий диск, 3G/4G USB-модем)
6	Power	индикатор питания и статуса работы устройства

[1] Только для моделей RG-2402G-W, RG-2404G-W, RG4402G-W, RG-4402GF-W

2.6.2 Задняя панель устройства

Внешний вид задней панели устройства RG-2404G-W приведен на рисунке 5.

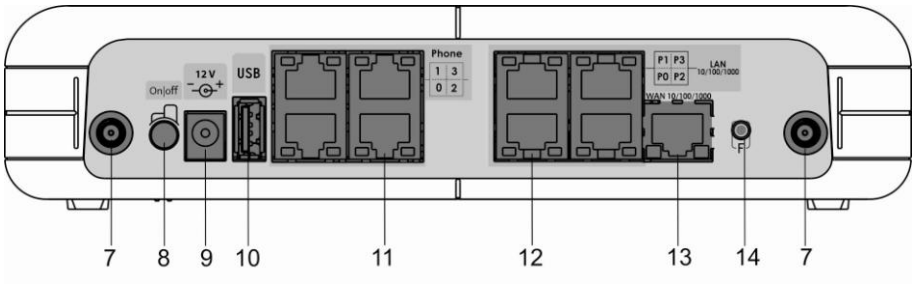


Рисунок 5 – Внешний вид задней панели RG-2404G-W

На задней панели устройства серии *RG-2400* расположены следующие разъемы и органы управления, таблица 4.

Таблица 4 – Описание индикаторов и органов управления задней панели *RG2400*

Элемент задней панели		Описание
7		разъем для подключения WiFi-антенны[1]
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	разъем RJ-11 для подключения аналоговых телефонных аппаратов: - для устройств RG-2402G, RG-2402G-W: 2; - для устройств RG-2404G, RG-2404G-W: 4.
12	LAN	4 порта 10/100/1000BASE-T Ethernet (разъем RJ-45) для подключения сетевых устройств
13	WAN	порт 10/100/1000BASE-T (разъем RJ-45) для подключения к внешней сети
14	F	функциональная кнопка для перезагрузки устройства и сброса к заводским настройкам

Внешний вид задней панели устройства RG-4402G-W приведен на рисунке 6. Внешний вид задней панели устройства RG-4402GF-W приведен на рисунке 7.

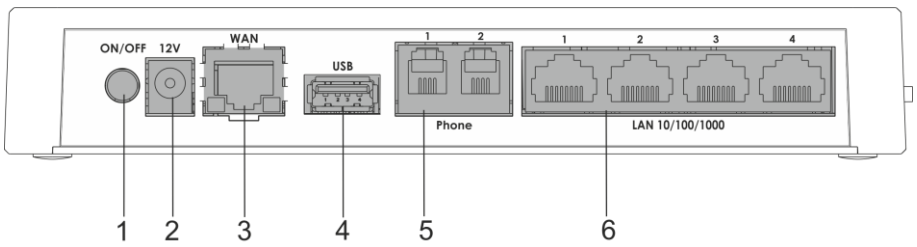


Рисунок 6 – Внешний вид задней панели RG-4402G-W

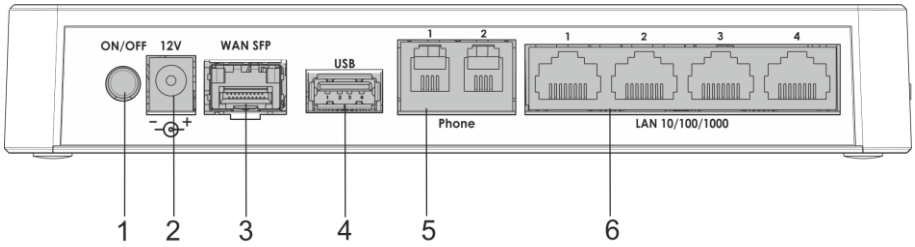


Рисунок 7 – Внешний вид задней панели RG-4402GF-W

На задней панели устройства серии *RG-4400* расположены следующие разъемы и органы управления, таблица 5.

Таблица 5 – Описание индикаторов и органов управления задней панели *RG-4400*

Элемент задней панели			**Описание**
1	On/Off		тумблер включения/выключения устройства
2	12V		разъем для подключения адаптера питания
3	для RG-4402G-W	WAN	порт 10/100/1000BASE-T (разъем RJ-45)
	для RG-4402GF-W	WAN SFP	1000 BASE-X (шасси для SFP)
4	USB		разъем USB для подключения внешнего USB-устройства (USB flash, жесткий диск, 3G/4G USB-модем)
5	Phone		разъем RJ-11 для подключения аналоговых телефонных аппаратов
6	LAN 10/100/1000		4 порта 10/100/1000BASE-T Ethernet (разъем RJ-45) для подключения сетевых устройств

2.7 Световая индикация

Текущее состояние устройства *RG-2400/RG-4400* отображается при помощи индикаторов **Wi-Fi[1], WAN, LAN, Phone, Power** – расположенных на передней панели. Перечень состояний индикаторов приведен в таблице 5.

Таблица 6 – Световая индикация состояния устройства серии *RG-2400/RG-4400*

Индикатор	Состояние индикатора	Состояние устройства
Wi-Fi[1]	зеленый, горит постоянно	сеть Wi-Fi-активна
	зеленый, мигает	процесс передачи данных по беспроводной сети
WAN	горит зеленым (10, 100Mbps)/ оранжевым (1000 Mbps)	установлено соединение между станционным терминалом и абонентским устройством
	мигает	процесс пакетной передачи данных по WAN-интерфейсу
LAN	горит зеленым (10, 100 Mbps)/ оранжевым (1000 Mbps)	установлено соединение с подключенным сетевым устройством
	мигает	процесс пакетной передачи данных по LAN-интерфейсу
Phone0 Phone1 Phone2[2] Phone3[2]	зеленый, горит постоянно	телефонная трубка поднята (линия активна)
	не горит	трубка положена, нормальная работа
	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-proxy сервере
	двойные короткие мигания с интервалом в 3 секунды	идет тест линии
USB	зеленый, горит	USB-устройство подключено
	не горит	USB-устройство отключено
Power	зеленый, горит постоянно	включено питание устройства, нормальная работа
	оранжевый, горит постоянно	отсутствует выход в Интернет
	красный, горит постоянно	загрузка устройства, сброс устройства к заводским настройкам

2.8 Сброс к заводским настройкам

Для запуска устройства с заводскими настройками необходимо в загруженном состоянии нажать и удерживать кнопку «F», пока индикатор «Power» не загорится красным цветом. 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] Только для моделей RG-2402G-W, RG-2404G-W, RG4402G-W, RG4402GF-W

[2] Только для моделей RG-2404G, RG-2404G-W

2.9 Комплект поставки

В базовый комплект поставки устройства серии *RG-2400/RG-4400* входят:

- терминал абонентский универсальный;
- адаптер питания 220/12В 2 А;
- 2 съемные антенны (только для устройств RG-2402G-W, RG-2404G-W; устройства RG-4402G-W и RG4402GF-W имеют внутренние антенны);
- руководство по установке и настройке.

3 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

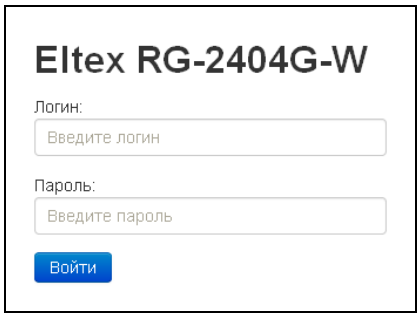
3.1 Начало работы

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.



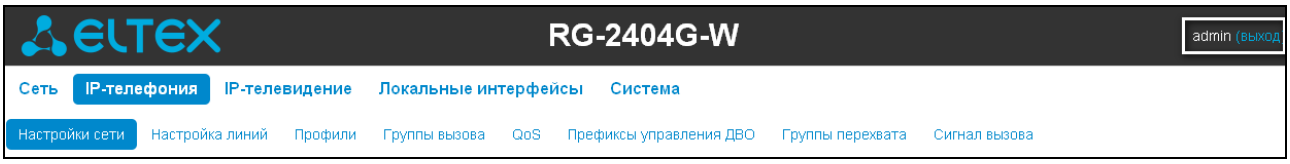
3. Введите имя пользователя в строке «Логин» и пароль в строке «Пароль».

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

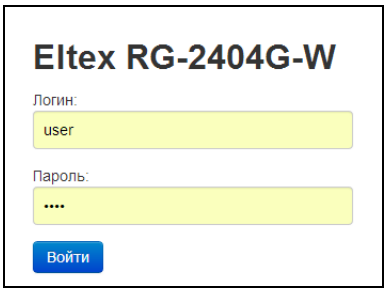
4. Нажмите кнопку «Войти». В окне браузера откроется меню быстрого конфигурирования, рисунок 8.

3.2 Смена пользователей

На устройстве существует три типа пользователей: **admin**, **user** и **viewer**. Пользователь **admin** (пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек, полный мониторинг состояния устройства. Пользователь **user** (пароль по умолчанию: **user**) имеет возможность выполнить только настройку PPPoE для подключения к Интернет и настройку Wi-Fi, не имеет доступа к мониторингу состояния устройства. Пользователь **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:



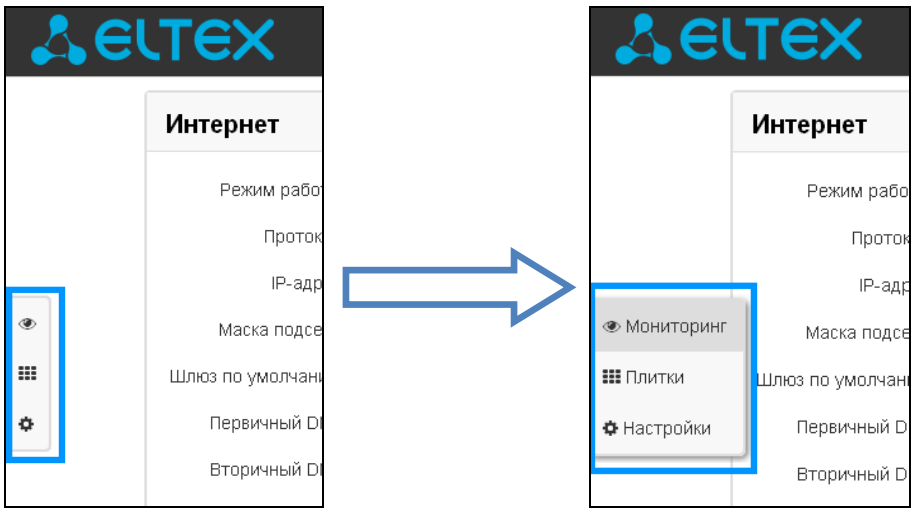
Для смены доступа необходимо указать соответствующие имя пользователя и пароль, нажать кнопку *«Войти»*.

3.3 Режимы работы WEB-интерфейса

WEB-интерфейс устройства серии *RG-2400/RG-4400* 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 т.д.;
- **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 используется панель, которая находится с левой стороны WEB-интерфейса. При наведении указателя мыши панель раскрывается:

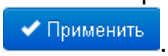


Из режима «Плитки» в режим «Настройки» переход возможен также через ссылку «подробнее» в названии плитки.

3.4 Применение конфигурации и отмена изменений

1. Применение конфигурации

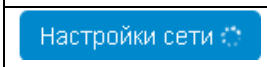
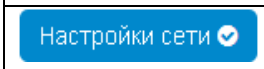
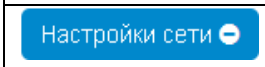
По нажатию на кнопку «Применить» происходит сохранение конфигурации во flash-память устройства и применение новых настроек. Все настройки вступают в силу без перезагрузки устройства.

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

.

В WEB-интерфейсе реализована визуальная индикация текущего состояния процесса применения настроек, таблица 7.

Таблица 7 – Визуальная индикация текущего состояния процесса применения настроек

Внешний вид	Описание состояния
	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».
	Об успешном сохранении и применении настроек информирует значок в названии вкладки.
	Если значение параметра было указано с ошибкой – после нажатия на кнопку «Применить» появится соответствующее сообщение об ошибке с указанием причины, а в названии вкладки отобразится значок .

2. Отмена изменений

Отмена изменений производится только до нажатия на кнопку «Применить». В этом случае изменённые 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:  ; 

.

3.5 Меню быстрого конфигурирования

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

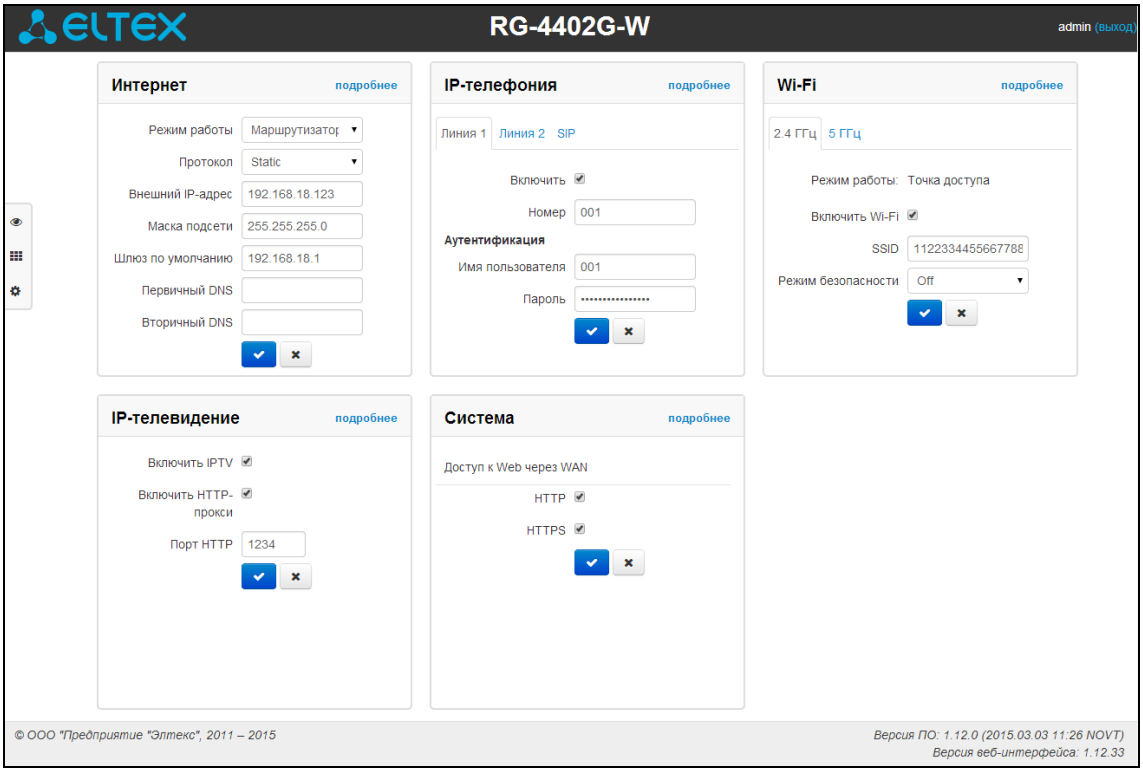


Рисунок 8 – Меню быстрого конфигурирования

Настройки разделены по следующим категориям:

- *Интернет* – быстрая настройка выхода в сеть Интернет;
- *IP-телефония* – быстрая настройка телефонии;
- *Wi-Fi* – настройка беспроводной точки доступа;
- *IP-телевидение* – конфигурирование устройства для поддержки функций IPTV;
- *Система* – настройка системных параметров (доступ к устройству, синхронизация времени и пр.).

3.5.1 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 – фактически устройство работает в режиме коммутатора.

- *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 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 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;
  - 28 – широковещательный адрес сети;
  - 33 - статические маршруты;
  - 42 – адрес NTP-сервера;
  - 43 – специфичная информация производителя;
  - 66 – адрес TFTP сервера;
  - 67 – имя файла программного обеспечения для загрузки по TFTP с сервера из опции 66;
  - 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:RG-2404G-W][HW:1.4][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]
  [LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

- *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.*

- *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 локальный 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 локальный 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 безопасности важных для организации данных.
Особенности L2TP делают его очень перспективным протоколом для построения виртуальных сетей.

- *Bridge*[2] – устройство работает в режиме моста (5-портовый коммутатор), для доступа к устройству установите параметры:
  - *IP-адрес* – IP-адрес моста;
  - *Маска подсети* – маска подсети моста.

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 устройства», «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.

3.5.2 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 0» .. «Линия 3»[3] выполняются основные настройки телефонных портов устройства «Phone0».. «Phone3» 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.

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

[1] В текущей версии программного обеспечения IPSec не поддерживается.
[2] В версии ПО 1.5.0 нельзя создать мост в тегированном режиме.
[3] Для моделей RG-2402G, RG-2402G-W, RG-4402G-W, RG-4402GF-W для настройки доступны только вкладки «Линия 0», «Линия 1»

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).

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

3.5.3 Wi-Fi[1]

Для работы устройства по сети Wi-Fi нужно указать основные настройки в разделе «Wi-Fi». Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее».

Во вкладке «2.4 ГГц» выполняются настройки для сети Wi-Fi на частоте 2.4 ГГц, во вкладке «5 ГГц» выполняются настройки для сети Wi-Fi на частоте 5 ГГц:

- *Включить Wi-Fi* – при установленном флаге активирована беспроводная точка доступа в соответствующем диапазоне частот (2.4 ГГЦ или 5 ГГц), при снятом флаге – точка доступа отключена;
- *SSID* – имя беспроводной сети, используется для подключения к устройству. Максимальная длина имени – 32 символа, ввод с учетом регистра клавиатуры. Данный параметр может состоять из цифр, латинских букв, а также символов "-", "_", ".", "!", ";", "#", при этом символы "!", ";" и "#" не могут стоять первыми;
- *Режим безопасности* – выбор режима безопасности беспроводной сети:
  - *Off* – отключено шифрование беспроводной сети, низкий уровень безопасности;
  - *WEP* – аутентификация WEP. WEP-ключ должен состоять из шестнадцатеричных цифр и иметь длину 10 или 26 символов, либо должен быть строкой (символы a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов.
  - *WPA, WPA2* – аутентификация WPA и WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' или пробел.

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

3.5.4 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 *RG-2400/RG-4400* (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. Функция полезна при просмотре IPTV через беспроводный канал Wi-Fi;

[1] Плитка Wi-Fi доступна только для моделей RG-2402G-W, RG-2404G-W, RG-4402G-W, RG-4402GF-W

– *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 .

3.5.5 Система

В разделе «Система» выполняются настройки 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 .

3.6 Расширенные настройки

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

3.6.1 Основные элементы WEB-интерфейса

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

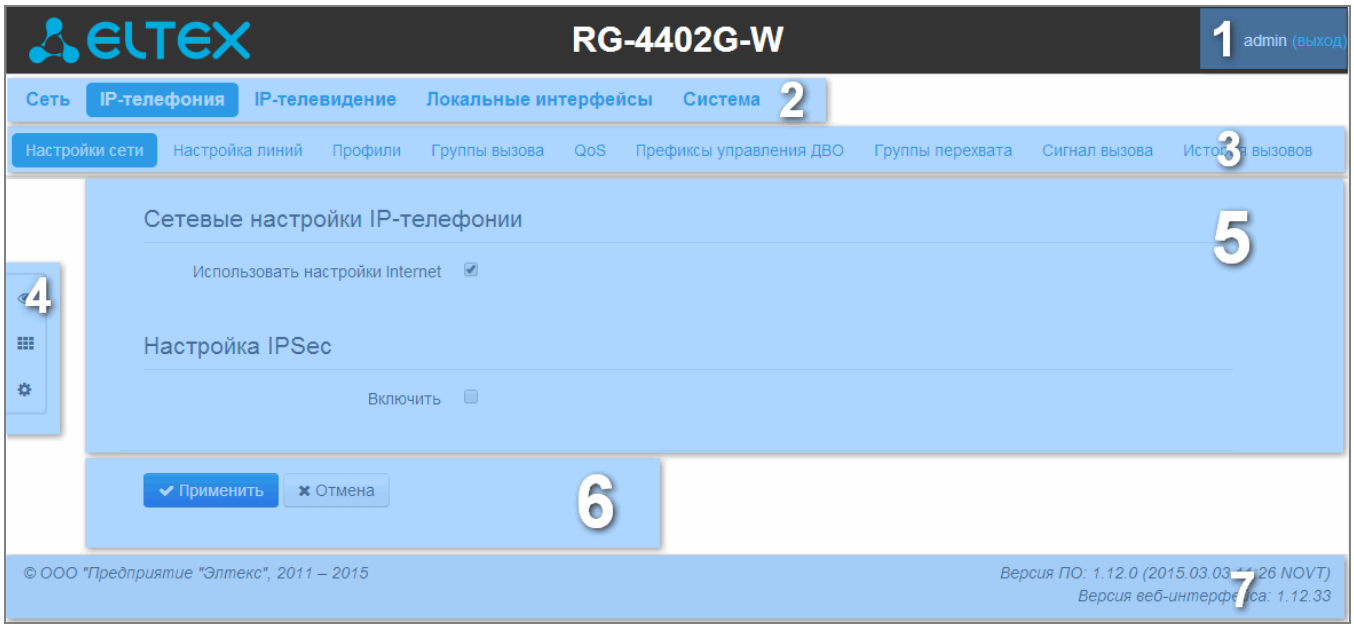


Рисунок 9 – Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса разделено на семь областей:

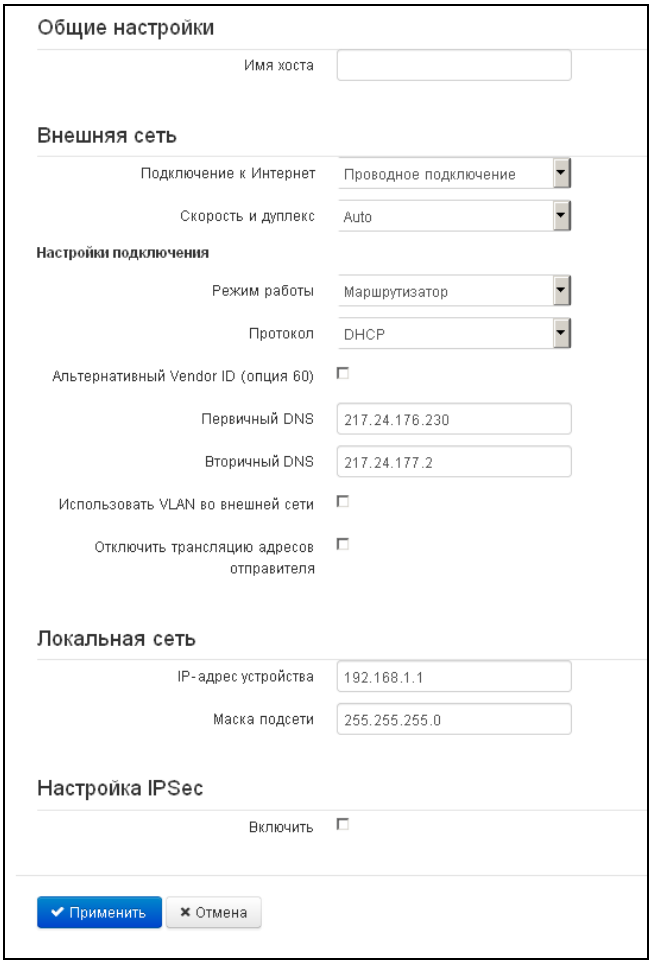
1. Имя пользователя, под которым был осуществлен вход в систему, а также кнопка завершения сеанса работы в WEB-интерфейсе (*выход*) под данным пользователем.
2. Вкладки меню группируют вкладки подменю по категориям: **Сеть**, **IP-телефония**, **IP-телевидение**, **Локальные интерфейсы, Система**.
3. Вкладки подменю служат для управления полем настроек.
4. Панель смены режима WEB-конфигуратора (описание в разделе 3.3)
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 3.4:
7. Информационное поле, в котором отображается версия ПО, версия WEB-интерфейса.

3.6.2 Меню «Сеть»

В меню «Сеть» выполняются основные сетевые настройки устройства.

3.6.2.1 Подменю «Интернет»

В подменю «Интернет» выполняется конфигурирование подключения к 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;
  - *Wi-Fi подключение* – подключение к сети Интернет осуществляется через беспроводную сеть Wi-Fi.

- *Скорость и дуплекс* – установка скорости передачи данных и режима работы дуплекса на Ethernet-порту WAN абонентского шлюза:

  - *Auto* – автоматическое согласование скорости и дуплекса;
  - *1000 Full* – поддерживается скорость 1000 Мбит/с с дуплексным режимом;
  - *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

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

- *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;
    - 28 – широковещательный адрес сети;
    - 33 - статические маршруты;
    - 42 – адрес NTP-сервера;

- 43 – специфичная информация производителя;
- 66 – адрес TFTP-сервера;
- 67 – имя файла программного обеспечения для загрузки по TFTP с сервера из опции 66;
- 121 – бесклассовые статические маршруты.

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:RG-2404G-W][HW:1.4][SN:VI23000118]
  [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

- *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 тэга Service-Name в сообщении PADI (поле не обязательно для заполнения);
  - *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 задаются вручную:
    IP-адрес, Маска подсети, DNS-сервер;
  - *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);

- *Второй доступ* – тип доступа к локальный 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).

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);
  - *Второй доступ* – тип доступа к локальный 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).

  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[1] предлагает больше уровней

[1] В текущей версии программного обеспечения IPSec не поддерживается.

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, прописанный 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 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.

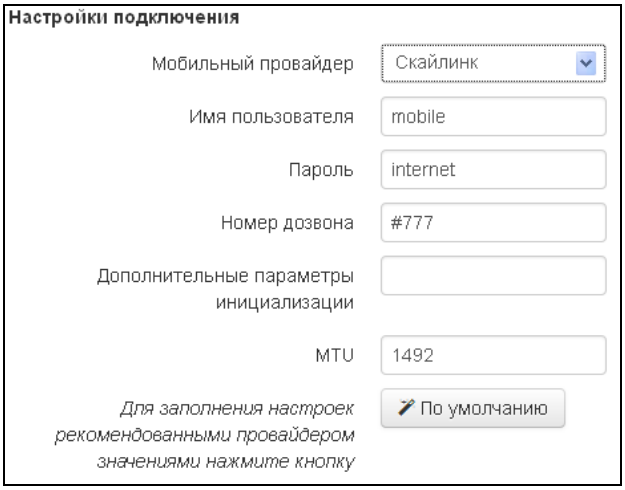
  - *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от
    - *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class 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:RG-2404G-W][HW:1.4][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

- *Первичный DNS, Вторичный DNS* – IP-адреса DNS-серверов – если адреса DNS-серверов не назначаются автоматически по протоколу DHCP, при необходимости задайте их вручную.

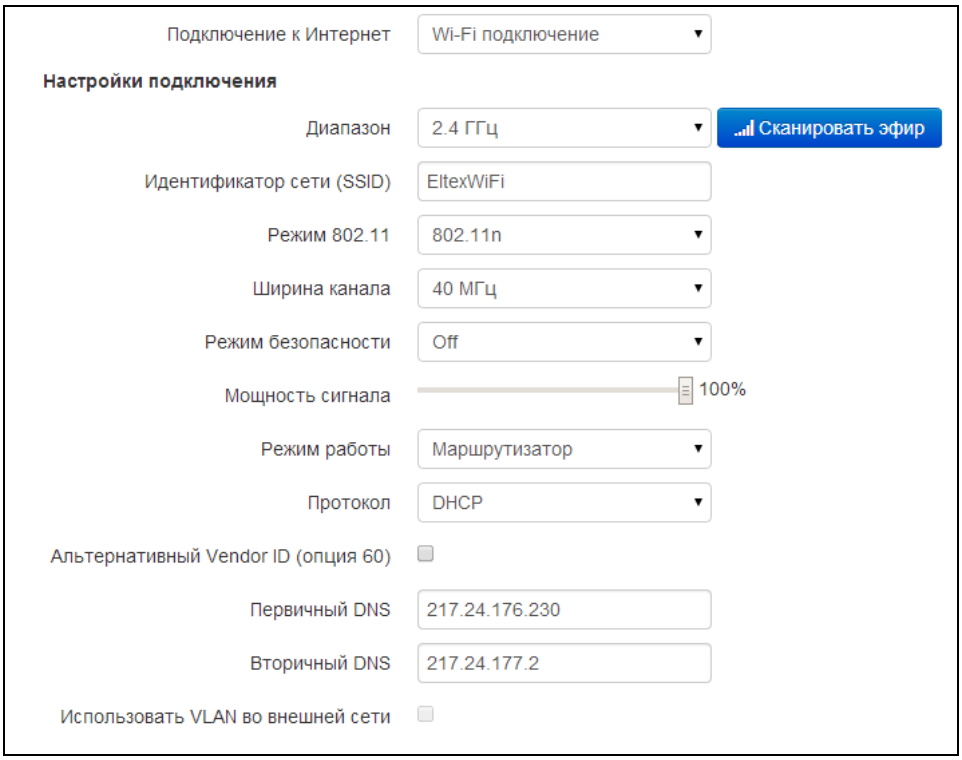
2. При выборе способа подключения **«3G/4G USB-модем»** для настройки будут доступны следующие поля:



- *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. Нажав 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.

3. При выборе способа подключения **«Wi-Fi подключение»** будут доступны следующие настройки:



– *Диапазон* – выбор рабочего диапазона: 2.4 ГГц или 5 ГГц;

При использовании режима «Wi-Fi подключение» точка доступа Wi-Fi будет недоступна в выбранном диапазоне подключения.

– *Идентификатор сети (SSID)* – имя беспроводной сети, используется для подключения к устройству. Максимальная длина имени – 32 символа, ввод с учетом регистра клавиатуры. Данный параметр может состоять из цифр, латинских букв, а также символов "-", "_", ".", "!", ";", "#" и пробела, при этом символы "!", ";", "#" и пробел не могут стоять первыми;
– *Режим 802.11* – выбор режима работы беспроводного интерфейса.
Для 2.4 ГГц:
  - *802.11b* – если все беспроводные клиенты поддерживают стандарт 802.11b, по данному стандарту максимальная скорость составляет 11 Мбит/с;
  - *802.11bg* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b и 802.11g, по стандарту 802.11g максимальная скорость составляет 54 Мбит/с;
  - *802.11bgn* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b, 802.11g и 802.11n;
  - *802.11n* – данный стандарт предусматривает максимальную скорость 300 Мбит/с. 802.11n использует технологию MIMO (несколько входов, несколько выходов), обработку сигналов и технологию интеллектуальной антенны для передачи нескольких потоков данных через несколько антенн. Это даёт пятикратное увеличение производительности и двукратное увеличение диапазона по сравнению с предыдущим стандартом 802.11g.

Для 5 ГГц:

- *802.11a* – максимальная скорость составляет 54 Мбит/с;
- *802.11n* – данный стандарт предусматривает максимальную скорость 300 Мбит/с. 802.11n использует технологию MIMO (несколько входов, несколько выходов), обработку сигналов и технологию интеллектуальной антенны для передачи нескольких потоков данных через несколько антенн;

– *Ширина канала* – ширина полосы частот канала, на котором работает Wi-Fi клиент, принимает значения 20 и 40 МГц;
– *Режим безопасности* – выбор режима безопасности беспроводной сети:

- *Off* – отключено шифрование беспроводной сети, низкий уровень безопасности;
- *WEP* – шифрование WEP. WEP-ключ должен состоять из шестнадцатеричных цифр и иметь длину 10 или 26 символов, либо должен быть строкой (символы a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов.
- *WPA, WPA2* – шифрование WPA и WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' или пробел. Рекомендуется использовать режимы шифрования WPA и WPA2 как наиболее безопасные на данный момент.

– *Мощность сигнала* – регулировка мощности сигнала приемопередатчика Wi-Fi в процентах от максимального уровня;
– *Режим работы* – режим работы устройства:

- *Маршрутизатор* – между LAN- и WAN-интерфейсами (WAN-интерфейсом становится беспроводной интерфейс Wi-Fi) устанавливается режим маршрутизатора (LAN изолирован от WAN);
- *Мост* – устанавливается режим беспроводного моста к подключенной сети Wi-Fi.

– *Протокол* – выбор протокола, по которому будет осуществляться подключение по Wi-Fi интерфейсу 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 устройства* – установка IP-адреса W-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
  - *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:RG-2404G-W][HW:1.4][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

- *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.

Локальная сеть:

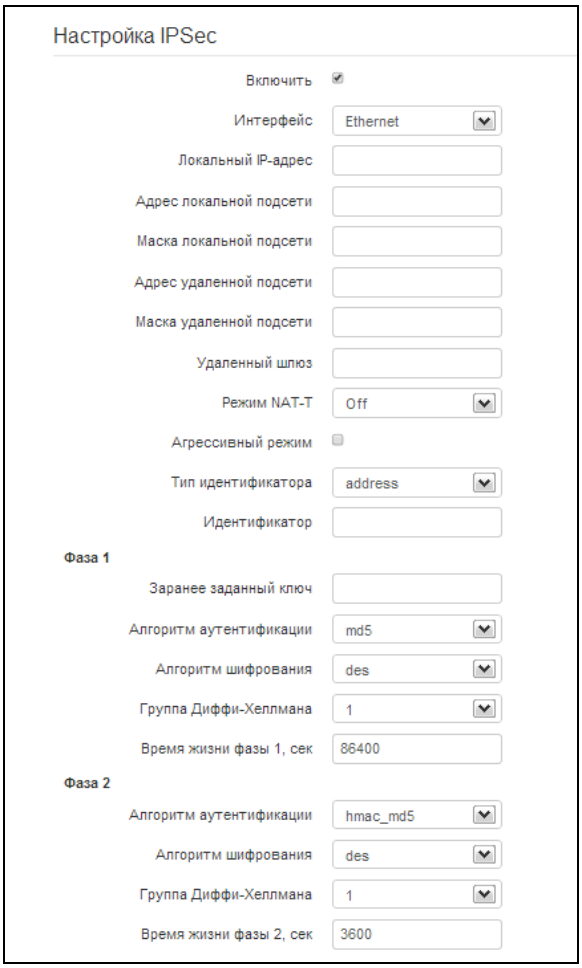
- *IP-адрес устройства* – IP-адрес устройства в локальной сети;
- *Маска подсети* – маска подсети в локальной сети.

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



- *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, хэш 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).

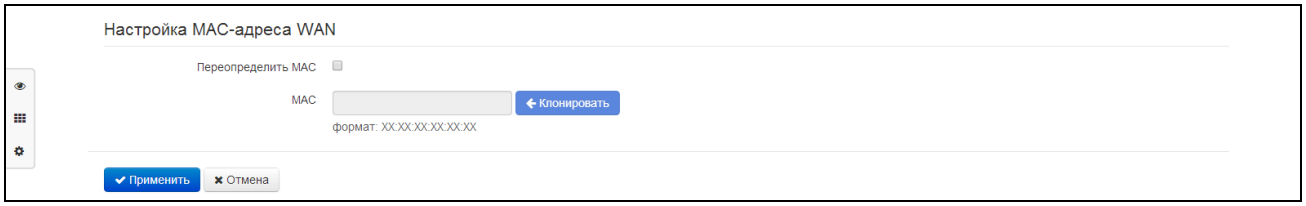
Фаза 2. На втором этапе генерируются данные ключей, узлы «договариваются» об используемой политике. Этот режим, также называемый быстрым режимом (quick mode), отличается от первой фазы тем, что может установиться только после первого этапа, когда все пакеты второй фазы шифруются.

- *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».*

3.6.2.2 Подменю «Настройка MAC-адресов»

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



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

При нажатии на кнопку «*Клонировать*» в поле «*MAC*» записывается 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 *RG-2400/RG-4400* в качестве маршрутизатора, на WAN-интерфейс устройства необходимо назначить MAC-адрес Вашего компьютера (который ранее был подключен к сети Интернет). Для этого достаточно подключиться к WEB-конфигуратору устройства по LAN-интерфейсу и нажать кнопку «*Клонировать*».

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

3.6.2.3 Подменю «DHCP-сервер»

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

Устройство *RG-2400/RG-4400* 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 и беспроводной Wi-Fi точке доступа. Его использование позволяет избежать ограничений ручной настройки протокола TCP/IP.

Настройки DHCP-сервера

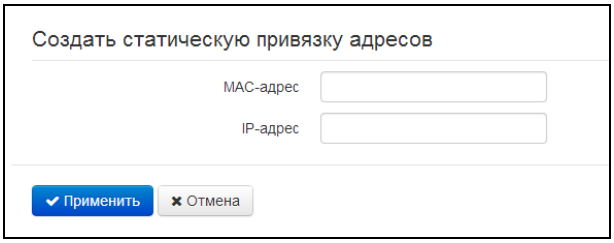
- *Включен* – при установленном флаге включить локальный DHCP-сервер;
- *Начальный IP-адрес* – начальный адрес пула IP-адресов;
- *Количество адресов* – количество адресов в пуле;
- *Срок аренды* – установка максимального времени использования подключенным устройством IP-адреса, назначенного DHCP-сервером,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

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:



– *MAC-адрес* – установка статического MAC-адреса. Задается в формате XX:XX:XX:XX:XX:XX;
– *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»*.

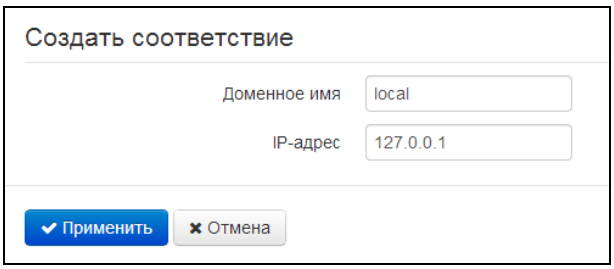
3.6.2.4 Подменю «Локальный DNS»

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 сетевому имени (хосту). 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 (хостов) и их IP-адресами.

Настройка узлов

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



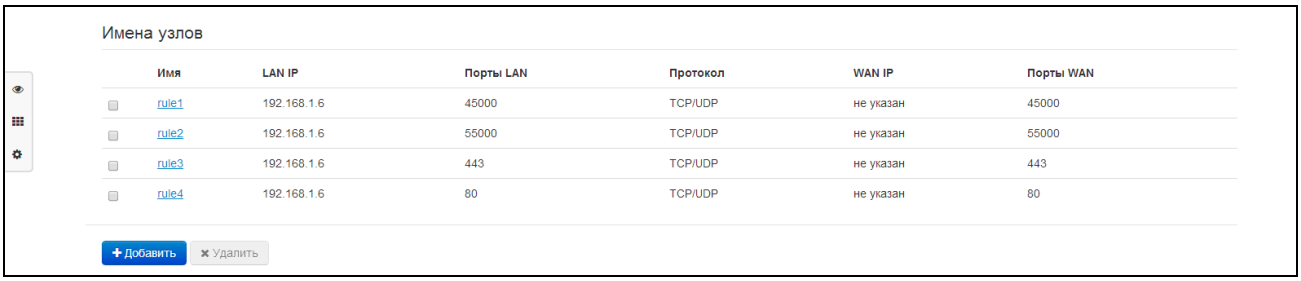
– *Доменное имя* – имя узла;
– *IP-адрес* – IP-адрес узла.

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»*.

3.6.2.5 Подменю «NAT и проброс портов»

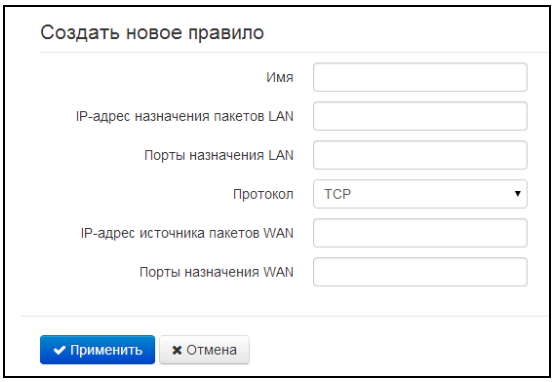
В подменю «NAT и проброс портов» выполняется настройка проброса портов (ports forwarding) из WAN-интерфейса в LAN-интерфейс.

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, попадающих под данное правило;
- *Порты назначения LAN* – TCP/UDP-порты получателя, на которые будут транслироваться пакеты в локальную сеть (допускается указывать либо одиночный порт, либо через “-“ диапазон портов);
- *Протокол* – выбор протокола пакета, попадающего под данное правило: TCP, UDP, TCP/UDP;
- *IP-адрес источника пакетов WAN* – IP-адрес отправителя пакета во внешней сети, попадающего под данное правило;
- *Порты назначения WAN* – TCP/UDP-порты получателя пакета во внешней сети, при которых пакет попадает 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 назначения WAN»* и имеющего адрес источника *«IP-адрес источника пакетов WAN»* (если это параметр оставить пустым – адрес источника не анализируется), осуществляется подмена адреса и порта назначений на значения соответственно из полей *«IP-адрес назначения пакетов LAN»* и *«Порты назначения LAN»*.

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

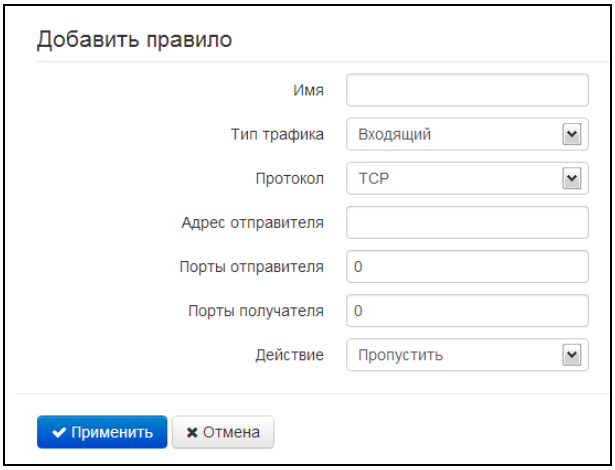
Для удаления правила из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку «Удалить».

3.6.2.6 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 протокола TCP или UDP), типа сообщения 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 попадать под данное правило (допускается указывать либо одиночный порт, либо через “-“ диапазон портов); для указания всех портов введите диапазон «0-65535»;
- *Порты получателя* – список портов получателя, пакеты которого будут попадать под данное правило (допускается указывать либо одиночный порт, либо через “-“ диапазон портов); для указания всех портов введите диапазон «0-65535»;.

При выборе протокола ICMP для редактирования будут доступны настройки:

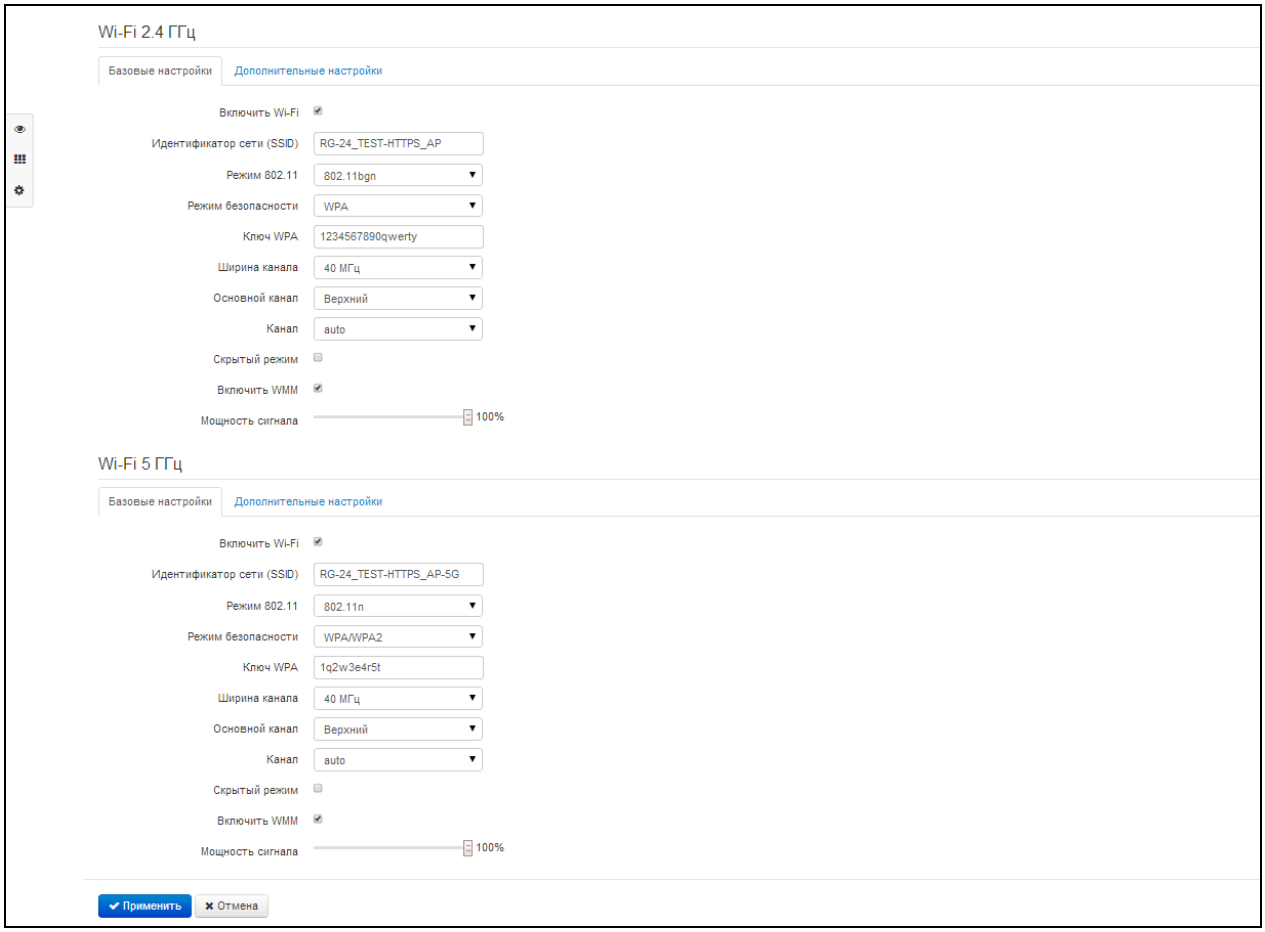
- *Тип сообщения* – можно создать правило только для определенного типа ICMP-сообщения либо для всех.

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».

3.6.2.7 Подменю «Wi-Fi»

В подменю «Wi-Fi» выполняются настройки беспроводной Wi-Fi сети. Подменю доступно только для моделей RG-2402G-W, RG-2404G-W, RG-4402G-W, RG-4402GF-W. Настройки выполняются для сети Wi-Fi на частоте 2.4 ГГц и 5 ГГц. Устройство поддерживает работу одновременно в двух диапазонах частот.

Все настройки разделены на базовые и дополнительные.



Базовые настройки

- *Включить Wi-Fi* – при установленном флаге включена беспроводная точка доступа в соответствующем диапазоне частот;
- *Идентификатор сети (SSID)* – имя беспроводной сети, используется для подключения к устройству. Максимальная длина имени – 32 символа, ввод с учетом регистра клавиатуры. Данный параметр может состоять из цифр, латинских букв, пробелов, а также символов "-", "_", ".", "!", ";", "#", при этом символы "!", ";" , "#" и пробел не могут стоять первыми;
- *Режим 802.11* – выбор режима работы беспроводного интерфейса.
  Для 2.4 ГГц:
  - *802.11b* – если все беспроводные клиенты поддерживают стандарт 802.11b, по данному стандарту максимальная скорость составляет 11 Мбит/с;
  - *802.11bg* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b и 802.11g, по стандарту 802.11g максимальная скорость составляет 54 Мбит/с;
  - *802.11bgn* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b, 802.11g и 802.11n;
  - *802.11n* – данный стандарт предусматривает максимальную скорость 300 Мбит/с. 802.11n использует технологию MIMO (несколько входов, несколько выходов), обработку сигналов и технологию интеллектуальной антенны для передачи

нескольких потоков данных через несколько антенн. Это даёт пятикратное увеличение производительности и двукратное увеличение диапазона по сравнению с предыдущим стандартом 802.11g.

Для 5 ГГц:

- *802.11a* – максимальная скорость составляет 54 Мбит/с;
- *802.11n* – данный стандарт предусматривает максимальную скорость 300 Мбит/с. 802.11n использует технологию MIMO (несколько входов, несколько выходов), обработку сигналов и технологию интеллектуальной антенны для передачи нескольких потоков данных через несколько антенн.

– *Режим безопасности* – выбор режима безопасности беспроводной сети:

- *Off* – отключено шифрование беспроводной сети, низкий уровень безопасности;
- *WEP* – шифрование WEP. WEP-ключ должен состоять из шестнадцатеричных цифр и иметь длину 10 или 26 символов, либо должен быть строкой (символы a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов.
- *WPA, WPA2* – шифрование WPA и WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' или пробел. Рекомендуется использовать режимы шифрования WPA и WPA2 как наиболее безопасные на данный момент.

Рекомендуется использовать режимы безопасности WPA и WPA2 как наиболее безопасные.

– *Ширина канала* – ширина полосы частот канала, на котором работает беспроводная точка доступа, принимает значения 20 и 40 МГц;

– *Основной канал* – основной канал точки доступа. Настройка доступна при выборе ширины канала в 40 МГц – в этом случае суммарный канал 40 МГц образуется из двух соседних частотных каналов по 20 МГц. Выбор основного канала определяется положением относительно дополнительного:

- Верхний – частота основного канала выше частоты дополнительного;
- Нижний – частота основного канала ниже частоты дополнительного.

– *Канал* – номер канала для работы беспроводной сети. При выборе значения «auto» автоматически определяется канал с меньшим уровнем помех;

– *Скрытый режим* – при установленном флаге точка доступа будет скрыта в эфире. Подключиться к ней можно, только заранее зная её SSID;

– *Включить WMM* – при установленном флаге включена функция WiFi Multimedia, которая позволяет оптимизировать передачу мультимедийного трафика по беспроводной среде;

– *Мощность сигнала* – регулировка мощности сигнала точки доступа в процентах от максимального уровня.

Дополнительные настройки

– *Порог фрагментации (Fragmentation Threshold)* – максимальный размер непрерывного блока данных для передачи по беспроводной сети. Данные большего размера будут разбиты на части — фрагментированы; принимает значения от 0 до 2346;

– *Порог RTS (RTS Threshold)* – максимальный запрашиваемый размер блока данных для передачи. В технологии CSMA/CA пакеты RTS (request to send) посылаются базовой станции до передачи реальных данных. При наличии свободного окна база отвечает пакетом CTS (clear to send) и клиент отсылает пакет запрошенного размера. Чем меньше размер RTS, тем больше вероятность получить разрешение от базовой станции, тем быстрее восстанавливается сеть после коллизий, но тем меньше производительность сети в целом. Принимает значения от 0 до 2347;

- *Период отправки служебных сообщений, мс (Beacon Interval)* – промежуток времени между служебными сообщениями в беспроводной сети. Служебные сообщения передают параметры частот, протоколов, безопасности, мощности передатчиков, задержек и т. д. Принимает значения от 20 до 1024;
- *Тип преамбулы (Preample Length)* – размер преамбулы показывает длину служебного поля в каждом пакете. Длинная преамбула состоит из 128 бит, короткая – из 56 бит. Короткий размер преамбулы повышает общее быстродействие системы, используется для мультимедия-приложений;
- *Включить IAPP* – протокол IAPP (Inter-Access Point Protocol) позволяет использовать роуминг клиентов между несколькими точками доступа внутри одного сегмента сети;
- *Отключить защиту (Wi-Fi Protection)* – это специальный механизм для сетей 802.11 b/g. Включение механизма гарантирует возможность работы медленных устройств стандарта b в среде с большим количеством высокоскоростных устройств стандарта g. Это достигается увеличением времени обслуживания старых клиентов, заданием для них меньшего размера окна RTS, снижением общего быстродействия сети;
- *Агрегация (Aggregation)* – включает возможность объединения нескольких маленьких пакетов для передачи в одном большом;
- *Короткий защитный интерва (Short GI)* – средство снижения ошибок при взаимодействии радио устройств — пустой промежуток между передаваемыми шестнадцатеричными символами (0,1,...E,F). Стандартный длинный защитный интервал (Long GI) имеет продолжительность 800нс. Считается, что за это время сигнал полностью доходит до приемника с учетом всех задержек и отражений. По истечении этого интервала, передается следующий символ. Short GI длится 400нс. Использование Short GI повышает общую производительность беспроводной сети примерно на 11%, но иногда ведет к увеличению ошибок приема/передачи;
- *Изоляция клиентов (WLAN Partition)* – включение запрета взаимодействия беспроводных клиентов между собой;
- *Включить STBC* – включение механизма Space Time Block Coding (STBC), используется в беспроводных сетях для передачи копий потока данных через несколько антенн и для обеспечения приёма разных версий блока данных в целях повышения надежности обмена данными. Известно, что радиосигнал распространяется в среде по достаточно сложным траекториям и подвержен влиянию отражения, рефракции, рассеивания, а также искажается воздействием теплового шума приёмника, что в конечном счете приводит к тому, что одни копии переданного сигнала могут оказаться значительно лучше (менее искажены) других. Эта избыточность повышает вероятность корректно декодировать сигнал из нескольких его копий на приёмной стороне. Технология STBC объединяет все копии принятого блока данных оптимальным образом для извлечения максимального количества информации из каждой из них.
- *Сосуществование 20/40МГц (20/40MHz Coexist)* – включенная опция приводит к тому, что если в радиусе действия нашей точки доступа будут обнаружены другие точки на аналогичных частотных каналах или все каналы будут сильно загружены – наша точка доступа отключит использование частотного диапазона 40МГц, чтобы не мешать соседям;
- *Адаптивная диаграмма направленности (Beamforming)* – технология, подразумевающая формирование электромагнитного поля антенны базовой станции в дальней зоне в виде узконаправленного главного лепестка, ориентированного в сторону абонентского устройства с возможностью изменения направленных свойств при изменении положения этого оборудования.

Если устройство работает в двух диапазонах частот (одновременно включены «Wi-Fi 2.4ГГц» и «Wi-Fi 5ГГц») – максимальная скорость передачи для каждого диапазона уменьшиться до 150 Мбит/с ввиду отключения технологии MIMO.

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

3.6.2.8 Подменю «Фильтр MAC»

В подменю «Фильтр MAC» выполняются настройка фильтрация доступа по WiFi и MAC-адресу клиента.

Настройки ограничения доступа по Wi-Fi

- *Режим фильтра* – задается отдельно для диапазонов 2.4 и 5 ГГц и определяет один из трех алгоритмов работы фильтра в зависимости от MAC-адреса клиента:
  - *Отключить* – фильтрация по MAC-адресам отключена – всем клиентам разрешено подключаться к точке доступа;
  - *Чёрный список* – в данном режиме работы фильтра клиентам, MAC-адреса которых указаны в «Списке MAC-адресов», запрещено подключаться к точке доступа. 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 точке доступа. Абонентам, MAC-адреса которых в списке не указаны, подключение запрещено.

Список MAC-адресов

Задается отдельно для каждого диапазона. В список можно внести до тридцати MAC-адресов клиентов, доступ которым к точке доступа регулируется настройкой режима фильтра соответствующего диапазона частот.

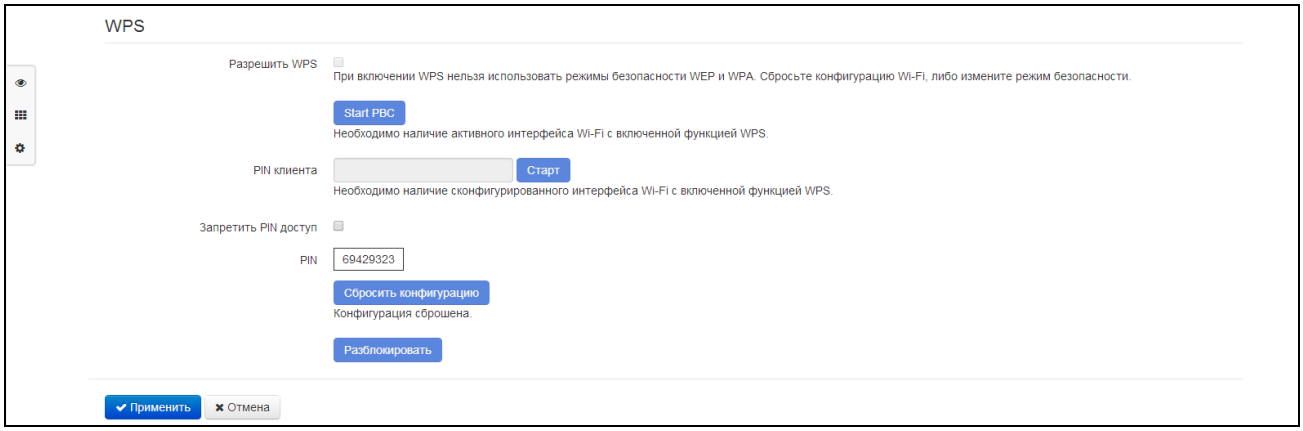
Для добавления нового клиента в список нажмите кнопку *«Добавить»* и введите его MAC-адрес.

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

3.6.2.9 Подменю «WPS»

В подменю «WPS» выполняется настройка протокола WPS (Wi-Fi Protected Setup).

WPS – стандарт полуавтоматического создания беспроводной сети Wi-Fi. Целью протокола WPS является упрощение процесса настройки беспроводной сети. WPS автоматически обозначает имя сети и задает шифрование для защиты от несанкционированного доступа в сеть, при этом нет необходимости вручную задавать все параметры.



Функция WPS активируется (деактивируется) сразу на обоих диапазонах частот.

Используя терминологию WPS, устройство может находиться в двух состояниях:

- *Configured* – точка доступа (хотя бы в одном диапазоне частот) сконфигурирована – это значит, что настроены имя сети, параметры шифрования и другие параметры;
- *Unconfigured* – точка доступа в обоих диапазонах частот не сконфигурирована – это значит, что все параметры Wi-Fi имеют настройки по умолчанию.

В зависимости от состояния точки доступа некоторые функции WPS могут быть заблокированы.

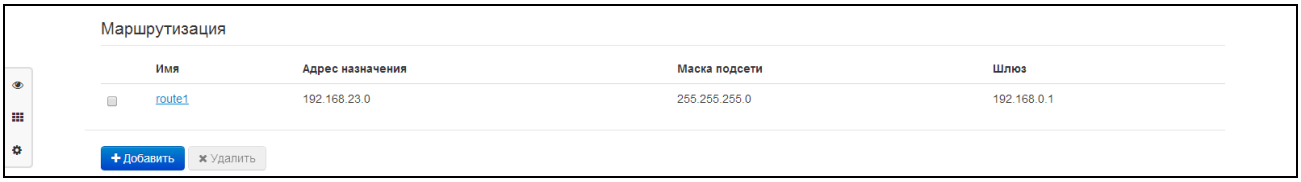
- *Разрешить WPS* – при установленном флаге разрешено использовать протокол WPS для автоматической настройки беспроводной сети; функция WPS активируется сразу в обоих диапазонах частот. Функцию WPS нельзя включить, если хотя бы в одном диапазоне частот настроен режим шифрования WEP или WPA.
- *Start PBC* – программная кнопка PBC (Push Button Configuration) – выполняет функции кнопки WPS на корпусе устройства. Подключение клиента происходит автоматически после нажатия на данную кнопку. Подключение клиента по кнопке PBC возможно как из состояния «Unconfigured» (точка доступа не сконфигурирована), так и из состояния «Configured» (точка доступа сконфигурирована). При подключении из состояния «Configured» клиент получает настроенные на устройстве имя сети и параметры шифрования. При подключении из состояния «Unconfigured» устройство автоматически генерирует и назначает клиенту имя сети и параметры шифрования. После нажатия на кнопку PBC функция WPS активна в течение двух минут.
- *PIN клиента* – используется для подключения клиента по его PIN-коду (только когда точка доступа находится в состоянии «Configured». Для подключения клиента введите его PIN в поле ввода и нажмите кнопку «Старт». Функция активна в течение двух минут после нажатия на кнопку «Старт».
- *Запретить PIN доступа* – запрет подключения к точке доступа по PIN-коду (PIN-код устройства указан в поле *PIN*). Настройка имеет силу, когда точка доступа находится в состоянии «Unconfigured», и осуществляется попытка Wi-Fi-клиента подключиться к ней по PIN-коду.

- *Сбросить конфигурацию* – для принудительного перевода точки доступа из состояния «Configured» в состояние «Unconfigured» нажмите кнопку «*Сбросить конфигурацию*» - установятся настройки Wi-Fi по умолчанию.
- *Разблокировать* – если Wi-Fi-клиент 10 раз подряд введет неверный PIN-код точки доступа (при попытке подключиться к ней по PIN-коду, когда она находится в состоянии Unconfigured) – функция WPS заблокируется. Для принудительного разблокирования функции WPS нажмите кнопку «*Разблокировать*».

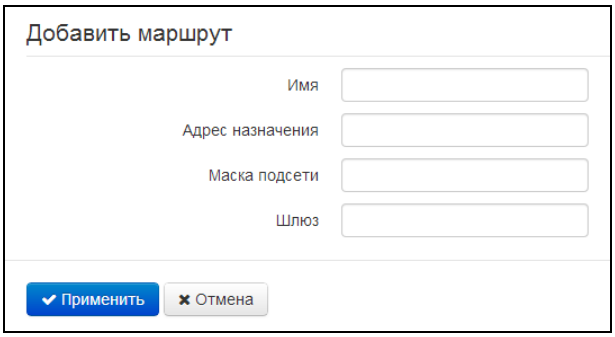
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

3.6.2.10 Подменю «Маршрутизация»

В подменю «Маршрутизация» устанавливаются статические маршруты устройства.



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



- *Имя* – название маршрута, используется для удобства восприятия человеком;
- *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».*

3.6.2.11 Подменю «Динамический DNS»

В подменю «Динамический DNS» выполняется настройка соответствующего сервиса.

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

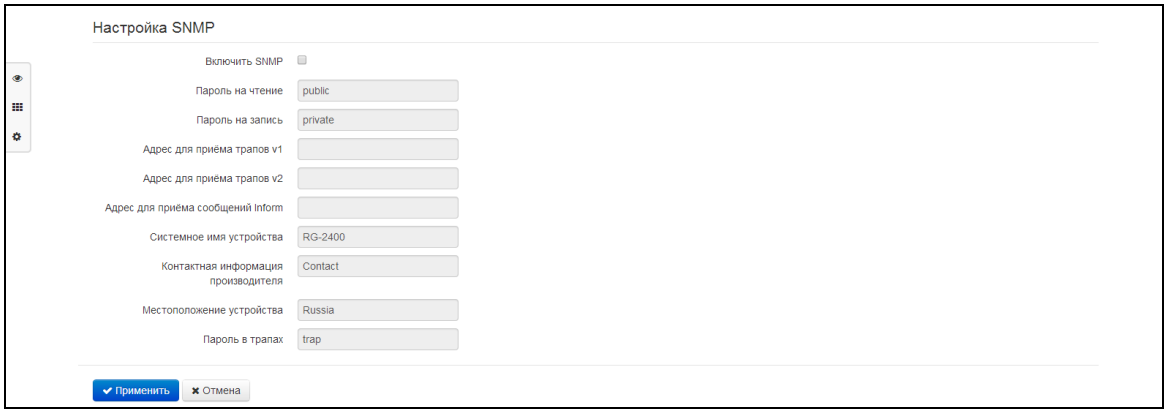
Динамический DNS часто применяется в локальных сетях, где клиенты получают IP-адрес по DHCP, а потом регистрируют свои имена на локальном DNS-сервере.

- *Включить D-DNS* – при установленном флаге сервис D-DNS активен и для редактирования доступны следующие настройки:
- *Провайдер D-DNS* – название провайдера D-DNS – выберите одного провайдера из списка доступных;
- *Имя пользователя* – имя пользователя для доступа к учетной записи сервиса D-DNS;
- *Пароль* – пароль для доступа к учетной записи сервиса D-DNS;
- *Доменное имя (0..9)* – можно зарегистрировать до десяти доменных имён устройства (обычно требуется лишь одно). 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»*.

3.6.2.12 Подменю «Настройка SNMP»

Программное обеспечение *RG-2400/RG-4400* позволяет проводить конфигурирование и мониторинг состояния устройства и его датчиков, используя протокол SNMP. В подменю «SNMP» выполняются настройки параметров SNMP-агента. Устройство поддерживает протоколы версий SNMPv1, SNMPv2c, SNMPv3.



- *Включить SNMP* – при установленном флаге разрешено использование протокол 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-портов, 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-портов
- 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 предприятия Элтекс.

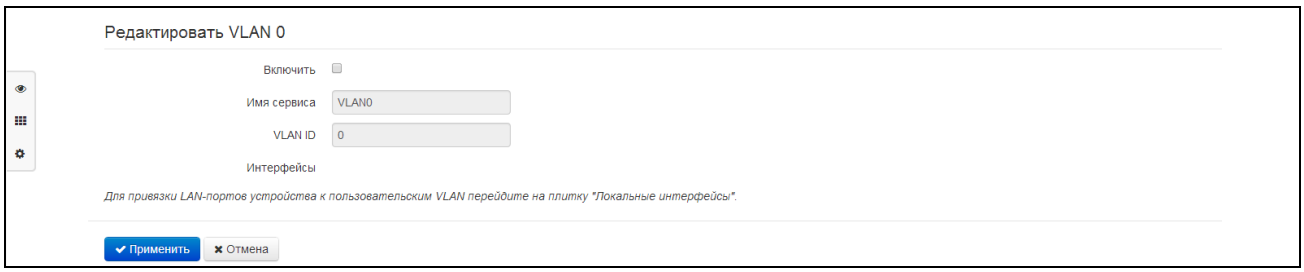
Для сохранения изменений в оперативную память устройства нажать кнопку *«Сохранить изменения» («Save Changes»)*. Для записи настроек в энергонезависимую память нажмите кнопку *«Применить» («Apply»).*

3.6.2.13 Подменю «Пользовательские VLAN»

Пользовательская VLAN определяется идентификатором VLAN, сетевой трафик в пределах которого проходит прозрачно с WAN-интерфейса устройства на LAN с последующим снятием тэга в локальной сети. То есть фактически при включении пользовательской VLAN в устройстве инициализируется сетевой мост между WAN-портом и определенными LAN-портами, при этом на стороне WAN трафик передаётся/принимается с заданным идентификатором VLAN, а на стороне LAN тэг снимается.

- *Статус* – отображается состояние данного VLAN (включен/выключен);
- *Имя сервиса* – имя пользовательской VLAN;
- *VLAN ID* – идентификатор VLAN;
- *Интерфейсы* – список портов LAN, привязанных к данной пользовательской VLAN.

В устройстве можно сконфигурировать до четырёх пользовательских VLAN. Чтобы открыть настройки VLAN для редактирования, кликните по одной из ссылок *VLAN0…VLAN3*:



- *Включить* – при установленном флаге пользовательская VLAN включена. При попытке отключить пользовательский VLAN, к которому привязаны один или несколько LAN-портов, эти LAN-порты привяжутся к сервису Интернет;
- *Имя сервиса* – произвольное имя, сопоставляемое с данным пользовательским VLAN;
- *VLAN ID* – идентификационный номер VLAN, принимает значения от 1 до 4095; не должен совпадать с идентификаторами VLAN других сервисов;
- *Интерфейсы* – список интерфейсов, которые привязаны к данному пользовательскому VLAN. Нередактируемое поле. Для привязки LAN-портов устройства к пользовательской VLAN перейдите на плитку "Локальные интерфейсы".

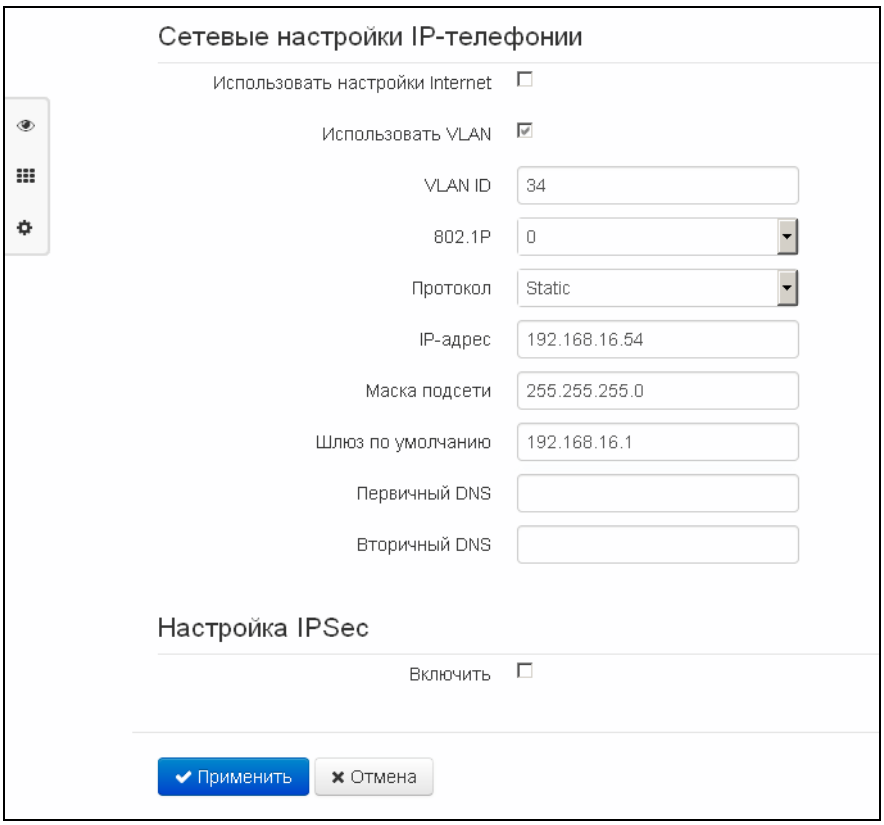
Для записи настроек в энергонезависимую память нажмите кнопку *«Применить» («Apply»).* Для отмены изменений нажмите кнопку *«Отмена».*

3.6.3 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.

3.6.3.1 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 *«Интернет» -> «Настройки сети»*, иначе – настройки, установленные в текущем меню;
- *Использовать VLAN*[1] – при установленном флаге услуга VoIP будет работать в выделенной 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 назначается вручную. При выборе типа «Static» для редактирования станут доступны следующие параметры:
    - *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;

[1] Разрешается задавать индивидуальные сетевые настройки услуги VoIP только в выделенной VLAN.

- *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 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:RG-2404G-W][HW:1.4][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

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).

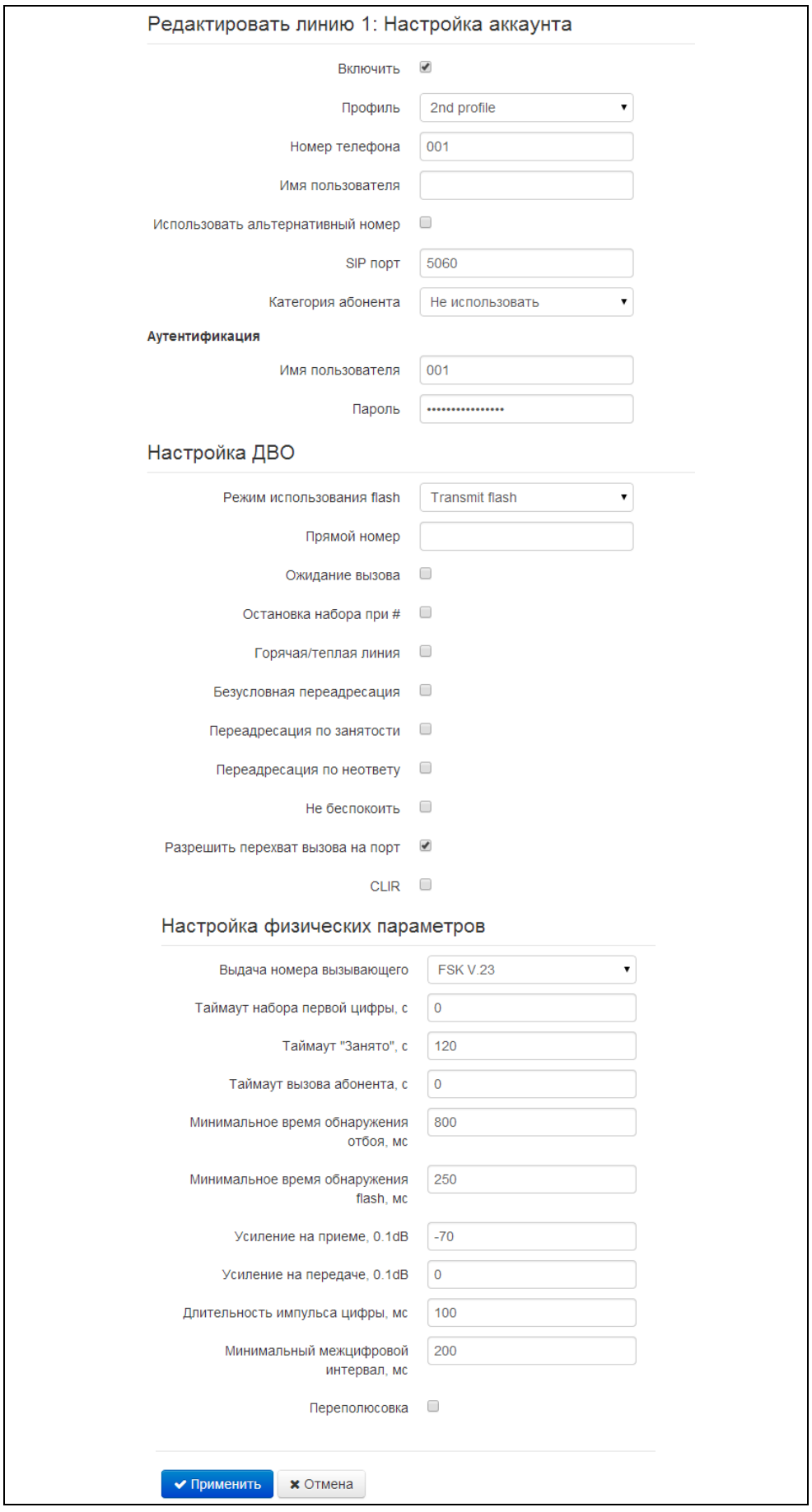
Подробное описание настроек *IPSec* приведено в разделе 3.6.2.1.

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

3.6.3.2 Подменю «Настройка линий»

В подменю *«Настройка линий»* выполняются настройки телефонных портов Phone0 .. Phone3 соответственно.

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



Настройка аккаунта

- *Включить* – при установленном флаге данный порт активен;
- *Профиль* – выбор SIP-профиля из перечня доступных. Настройка профилей производится в меню *«IP-телефония» -> «Профили»*.
- *Номер телефона* – абонентский номер, присвоенный телефонному порту;
- *Имя пользователя* – имя пользователя, сопоставленное с данным 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);
- *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 исходящий сообщений; последний при этом передается в формате Tel-URI (см. RFC3966);
- *Имя пользователя и пароль для аутентификации* – имя пользователя и пароль, используемые для аутентификации абонента на SIP-сервере (и сервере регистрации);

Настройка ДВО

- *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 4.1 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 4.1 Передача вызова;
  - *Local calltransfer* – передача вызова внутри устройства, без отправки сообщения REFER. Подробное описание алгоритма работы «Local calltransfer» смотрите в разделе 4.1 Передача вызова.

- *Прямой номер* – при подъеме трубки телефона сразу осуществляется вызов на указанный номер;
- *Ожидание вызова* – при установленном флаге разрешена услуга «*Ожидание вызова*» (услуга доступна в режиме использования функции flash – call transfer);
- *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 услуги «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 CFNR (Call Forward at No Response) – 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, в секундах;

– *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. При установленном флаге в заголовке *From* сообщений по протоколу SIP будет передаваться *Anonymous <sip:anonymous@unknown.host>* .

Настройка физических параметров

- *Выдача номера вызывающего* – выберите режим определения номера вызывающего абонента (Caller ID). Для работы Caller ID необходимо, чтобы телефонный аппарат абонента поддерживал установленный метод:

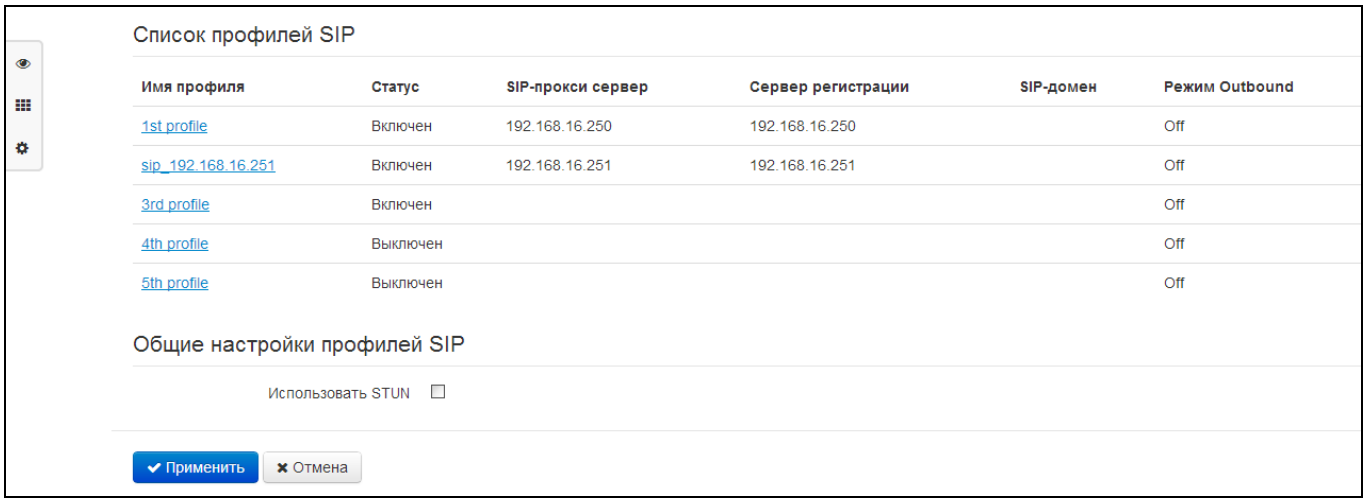
  - *Off* – определение номера вызывающего абонента выключено;
  - *FSK Bell 202, FSK V.23* – определение номера и имени вызывающего абонента методом FSK (по стандарту Bell202, или ITU-T V.23). Выдача номера в линию осуществляется между первым и вторым сигналом посылки вызова потоком данных с частотной модуляцией;
  - *DTMF* – определение номера вызывающего абонента методом DTMF. Выдача номера в линию осуществляется между первым и вторым сигналом посылки вызова двухчастотными DTMF посылками;

- *Таймаут набора первой цифры, с* – таймер ожидания набора первой цифры номера. При отсутствии набора в течение установленного времени, абоненту будет выдан сигнал «занято» и прекращен прием набора номера;
- *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 незанятости абонентского комплекта, мс* – минимальное время обнаружения отбоя, в миллисекундах. Одновременно с этим, данный параметр является максимальным временем детектирования короткого отбоя (flash).
- *Минимальное время flash* – минимальное время обнаружения короткого отбоя, (80-1000) мс;
- *Усиление на прием, 0.1dB* – усиление сигнала на приём (сигнал, который выдается в трубку телефона), единица измерения – 0,1 дБ;
- *Усиление на передаче, 0.1dB* – усиление сигнала на передачу (сигнала, поступающего в микрофон телефонной трубки), единица измерения – 0,1 дБ;
- *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;
- *Переполюсовка* – при включенной опции при исходящем вызове происходит изменение полярности напряжения питания в линии сразу после ответа вызываемого абонента. После отбоя полярность напряжения питания возвращается в исходное значение. Опция необходима для работы таксофона (изменение полярности напряжения питания сигнализирует о начале платного интервала времени).

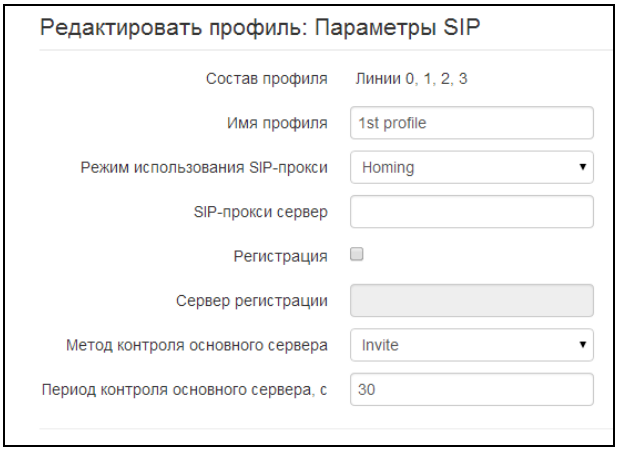
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

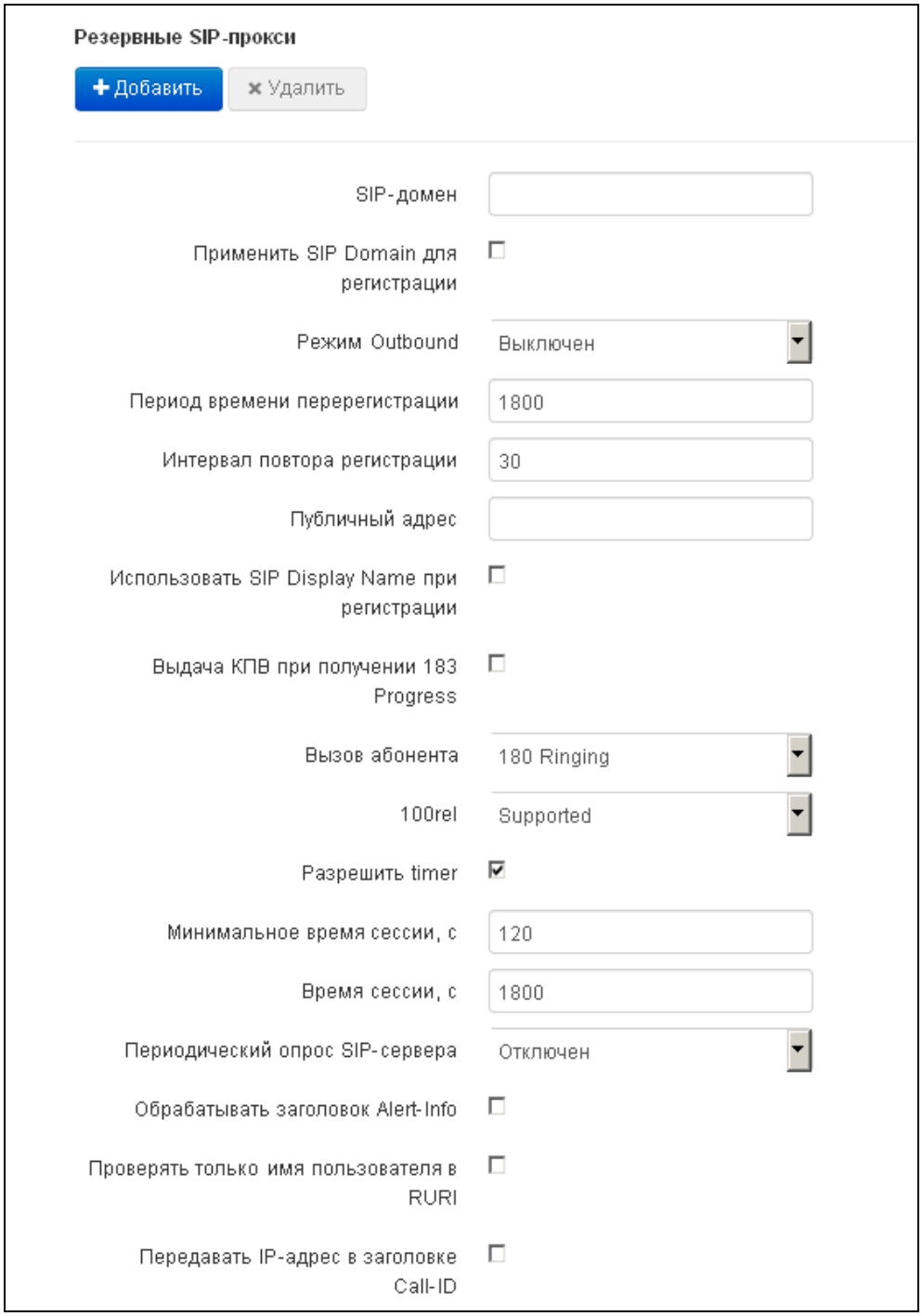
3.6.3.3 Подменю «Профили»

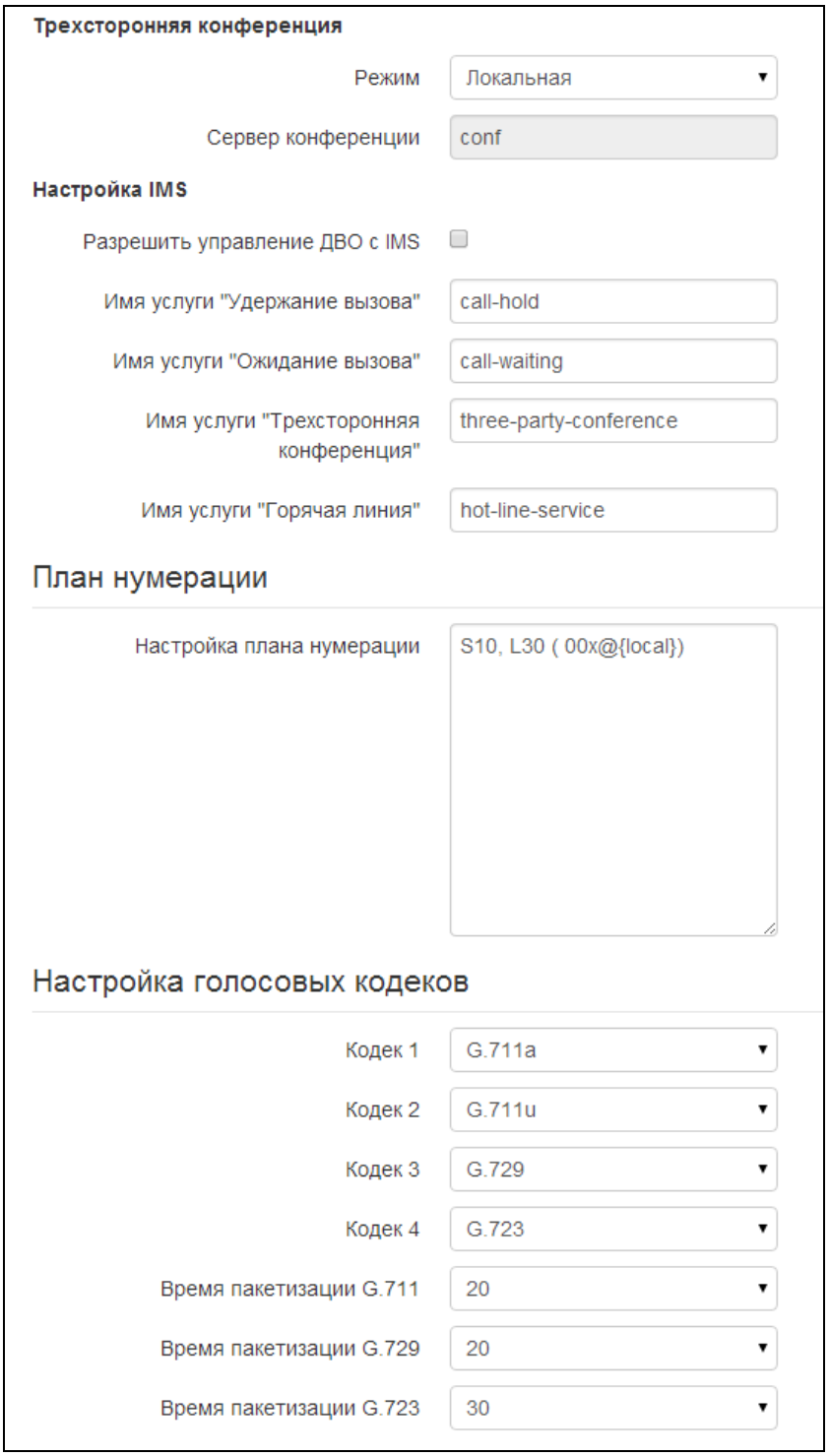
В подменю «Профили» выполняются настройки SIP-профилей устройства. За каждым SIP-профилем можно назначить собственные адреса SIP-сервера и сервера регистрации, голосовые кодеки и кодеки факса/модема, индивидуальный план нумерации и другие параметры. Необходимость использования разных SIP-профилей возникает,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

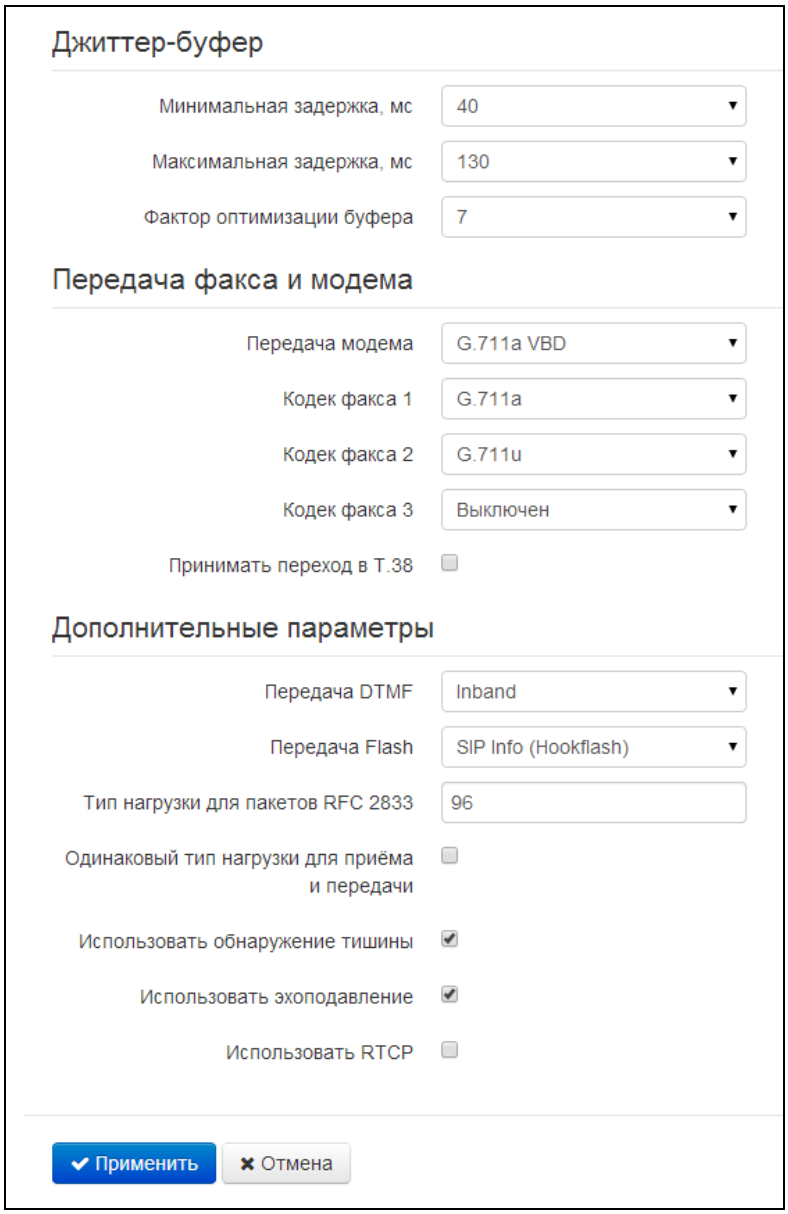


Для редактирования настроек профиля нажмите левой кнопкой мыши по ссылке настраиваемого профиля. В открывшемся окне «Редактировать профиль:» заполните следующие поля:




Резервные SIP-прокси
+ Добавить
× Удалить
SIP-домен
Применить SIP Domain для регистрации
Режим Outbound
Выключен
Период времени перерегистрации
1800
Интервал повтора регистрации
30
Публичный адрес
Использовать SIP Display Name при регистрации
Выдача КПВ при получении 183 Progress
Вызов абонента
180 Ringing
100rel
Supported
Разрешить timer
Минимальное время сессии, с
120
Время сессии, с
1800
Периодический опрос SIP-сервера
Отключен
Обрабатывать заголовок Alert-Info
Проверять только имя пользователя в RURI
Передавать IP-адрес в заголовке Call-ID


Трехсторонняя конференция
Режим
Локальная
Сервер конференции
conf
Настройка IMS
Разрешить управление ДВО с IMS
Имя услуги "Удержание вызова"
call-hold
Имя услуги "Ожидание вызова"
call-waiting
Имя услуги "Трехсторонняя конференция"
three-party-conference
Имя услуги "Горячая линия"
hot-line-service
План нумерации
Настройка плана нумерации
S10, L30 (00x@{local})
Настройка голосовых кодеков
Кодек 1
G.711a
Кодек 2
G.711u
Кодек 3
G.729
Кодек 4
G.723
Время пакетизации G.711
20
Время пакетизации G.729
20
Время пакетизации G.723
30



Параметры SIP

- *Состав профиля* – список абонентских портов, которым назначен профиль, поле не редактируемое;
- *Имя профиля* – пользовательское имя настраиваемого профиля;
- *Режим использования SIP-прокси* – в ниспадающем списке можно выбрать режим работы с SIP-сервером:

  - Не использовать;
  - Parking – режим резервирования SIP-proxy без контроля основного SIP-proxy;
  - Homing – режим резервирования SIP-proxy с контролем основного SIP-proxy.

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

  При наличии резервных SIP-proxy работа в режимах *Parking* и *Homing* осуществляется следующим образом. При совершении исходящего вызова шлюз отправляет сообщение

INVITE на адрес основного SIP-proxy 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 не доступен, 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:

1 В режиме parking нет контроля основного SIP-proxy 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.

2 В режиме homing доступно три вида контроля основного SIP-proxy: 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-proxy 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, с* – 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);
- *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 *RG-2400/RG-4400*. При этом на самом шлюзе (NAT) необходимо сделать проброс соответствующих SIP- и RTP-портов, используемых устройством серии *RG-2400/RG-4400*;
- *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);

- *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 *RG-2400/RG-4400* будет удалено выдавать вызывающему абоненту сигнал КПВ.
- *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 ACK. 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 встречная сторона поддерживает 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,* с – 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* – 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 4.3.2.

- *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

- *Разрешить управление ДВО с IMS* – при установленном флаге 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);
- *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.

По умолчанию если не пришла команда на активацию – все выше перечисленные 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 диалплане может блокировать завершение набора с помощью этой клавиши!**
- Последовательность цифр, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символу.
    - 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 диалплана:

- *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 диалплана, так и для определённого шаблона. Буква «S» отвечает за установку *«Interdigit Short Timer»*, а «L» - за *«Interdigit Long Timer»*. Значения таймеров может быть указано для всех шаблонов в диалплане, 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-ми 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 некоторого странного набора междугородних номеров.
- Пример 4: (S0 <:82125551234>) - быстрый набор указанного номера, аналог режима «Hotline» на других шлюзах.
- Пример 5: (S5 <:1000> | xxxx) - данный диалплан 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.

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.

Настройка голосовых кодеков

Сигнальный процессор *RG-2400/RG-4400* 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.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.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.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..4* – 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 – использовать кодек G.729.

- *Время пакетизации* – число миллисекунд речи в одном RTP-пакете (для кодеков G.711A и G.711U).

Джиттер-буфер

Джиттер (jitter) — это неравномерность периодов времени, отведенных на доставку пакета. Задержка в доставке пакета и джиттер исчисляется 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;
- *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.

– *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 предназначен 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 пакета – RG-2400/RG-4400 разрывает соединение.

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

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

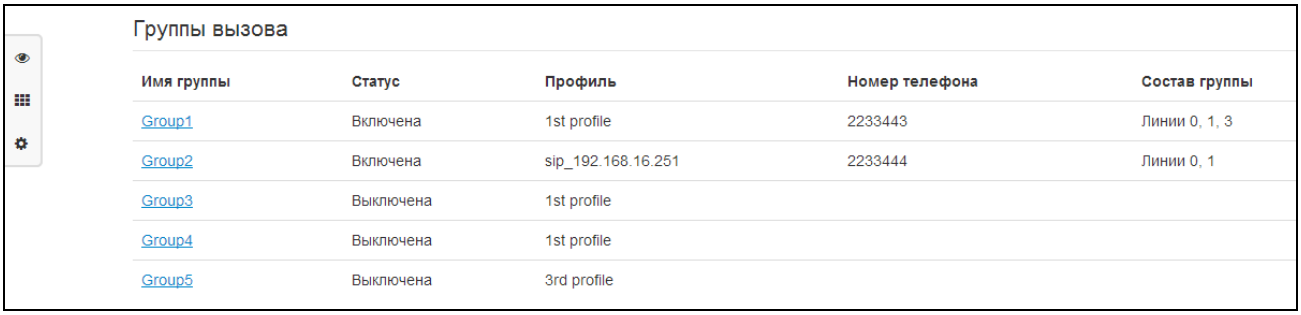
3.6.3.4 Подменю «Группы вызова»

В подменю «Группы вызова» выполняется управление группами вызовов.

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

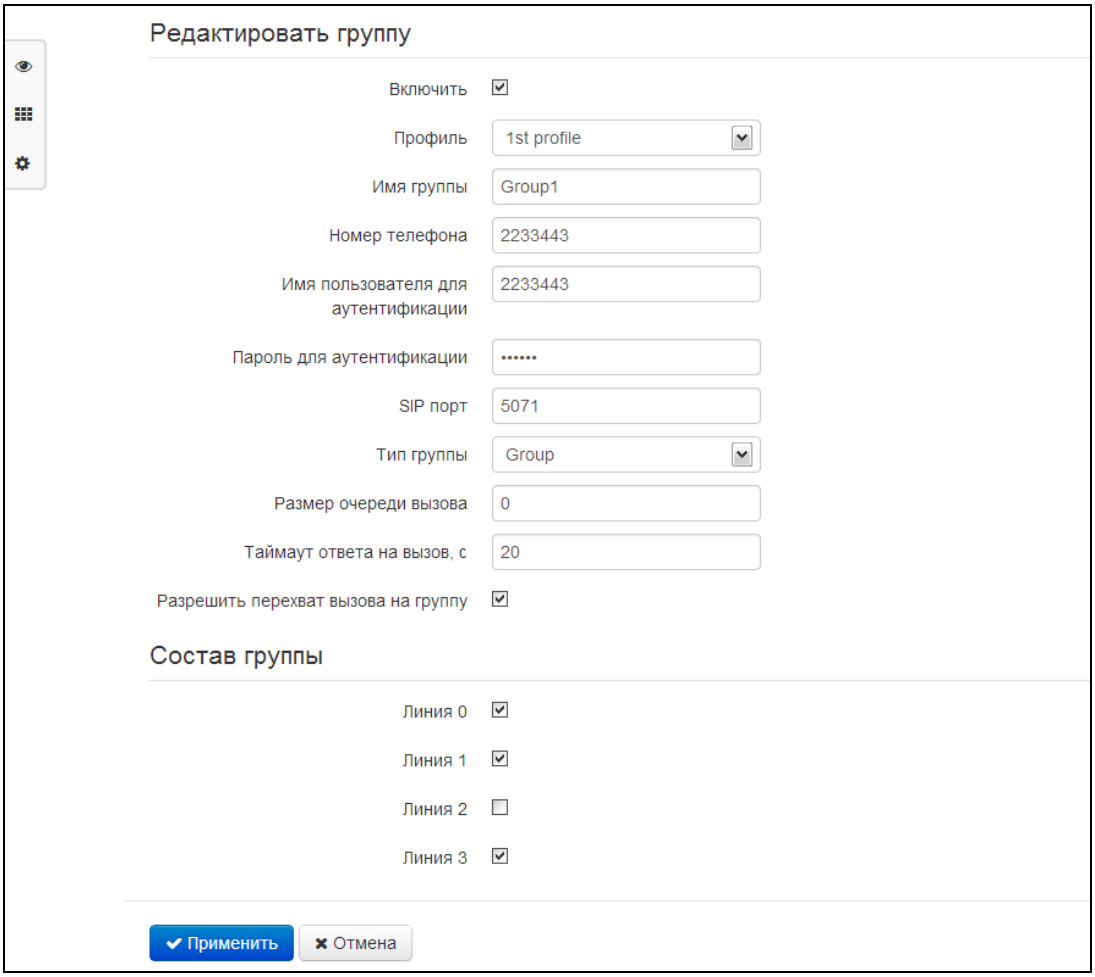
- *Групповой (Group)* – режим, при котором вызов поступает на все свободные порты группы одновременно. При ответе одного из участников группы, вызов на остальные порты прекращается;
- *Задержанный групповой (Serial)* – режим, при котором вызов поступает на первый свободный в списке группы порт, затем 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, назначенный группе вызова
– *Номер телефона* – номер телефона группы вызова;
– *Состав группы* – список линий (портов), которые входят в группу вызова.

Для выполнения настроек группы вызова нажмите на соответсвующую 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:

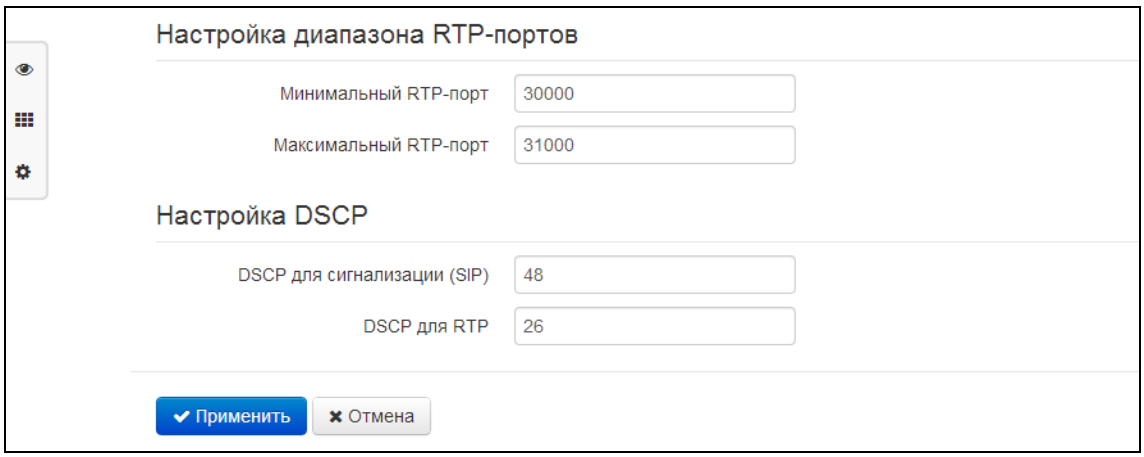
  - *Group* – сигнал вызова подается на все порты в группе одновременно;
  - *Serial* – количество портов, на которые подается вызывной сигнал, увеличивается на один по истечении таймаута вызова следующего порта;
  - *Cyclic* – сигнал вызова через интервал, равный таймауту вызова следующего порта, подается 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 одой группе перехвата (смотрите в разделе *3.6.3.7* 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»*.

3.6.3.5 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

- *DSCP для сигнализации (SIP)* – значение поля DSCP заголовка IP-пакета для сигнального трафика (устанавливается в десятичной системе счисления, принимает значения от 0 до 63);
- *DSCP для RTP* – значение поля DSCP заголовка IP-пакета для голосового трафика (устанавливается в десятичной системе счисления, принимает значения от 0 до 63).

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

3.6.3.6 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.

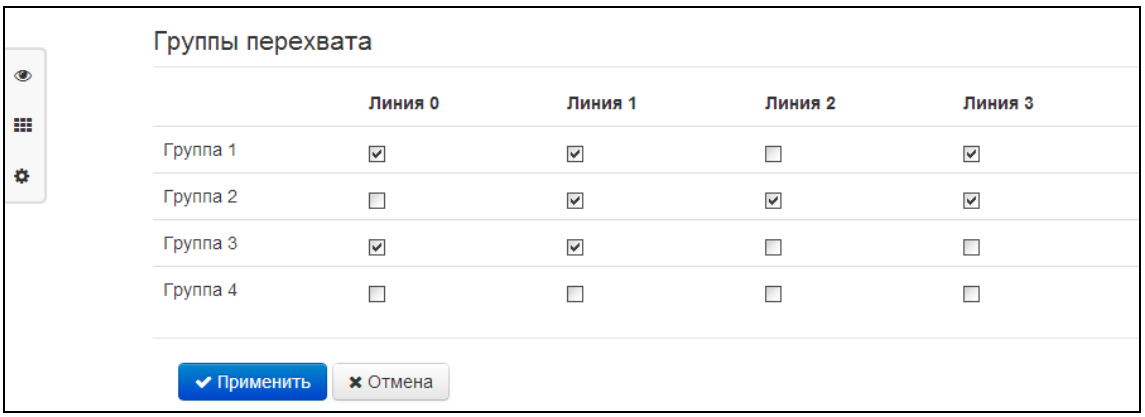
Код деактивации и код проверки статуса услуги заполняются автоматически на основании кода активации.

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

3.6.3.7 Подменю «Группы перехвата»

Подменю «*Группа перехвата*» служит для настройки перехвата входящего на порт или группу портов вызова. Всего может быть сконфигурировано до 4 различных групп перехвата.

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 в определенную группу установите/снимите флаг на против 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, то другой абонент, также принадлежащий этой группе и использующий такой же профиль SIP, может перехватить поступивший вызов. Для этого он должен после подъема трубки 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 вызова может перехватить вызов, поступивший на групповой номер.

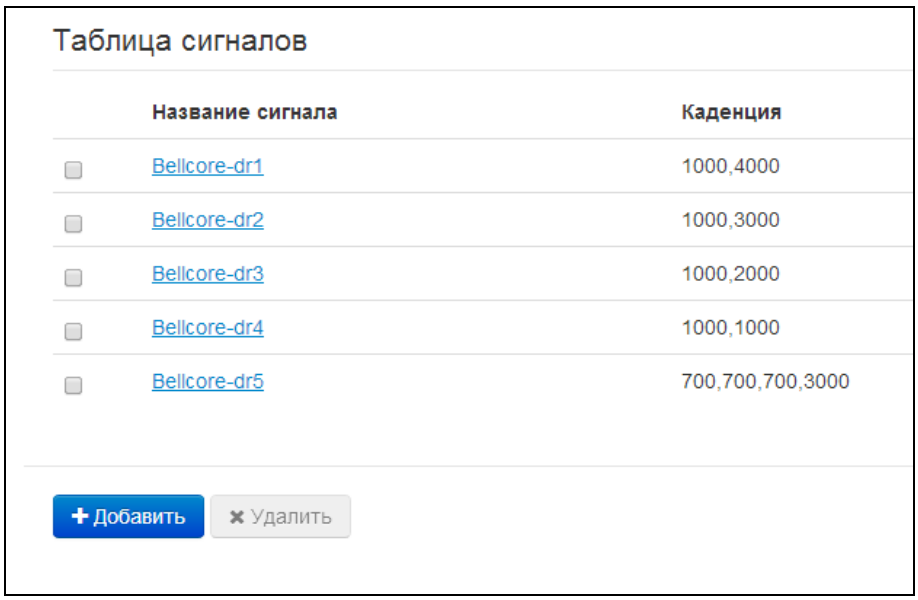
Если абонент набирает код перехвата в момент, когда на группу не поступает ни одного вызова, то абоненту будет выдан сигнал «Занято».

3.6.3.8 Подменю «Сигнал вызова»

В подменю «Сигнал вызова» осуществляется настройка альтернативного сигнала посылки вызова (каденции) в зависимости от номера вызывающего абонента либо 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.

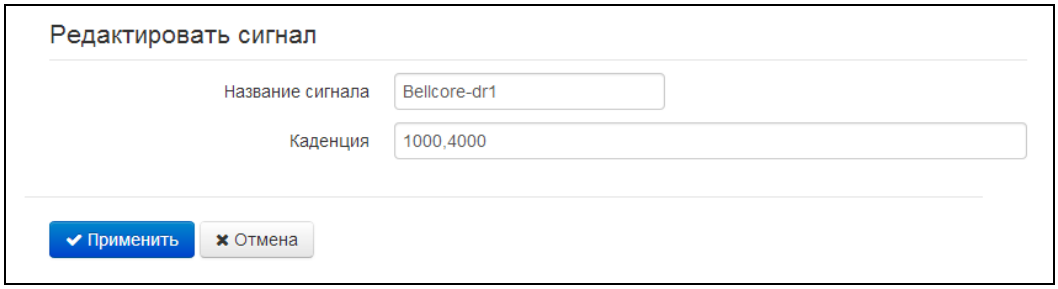
Для того чтобы привязать определённую каденцию к значению заголовка Alert-Info во входящем Invite, необходимо в соответствующем профиле SIP активировать флаг *«Обрабатывать заголовок Alert-Info»*, а в настройках каденции указать название сигнала в поле «Название сигнала» (например, Example-cadence). 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 соответсвующую ссылку в колонке «*Название сигнала*».

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



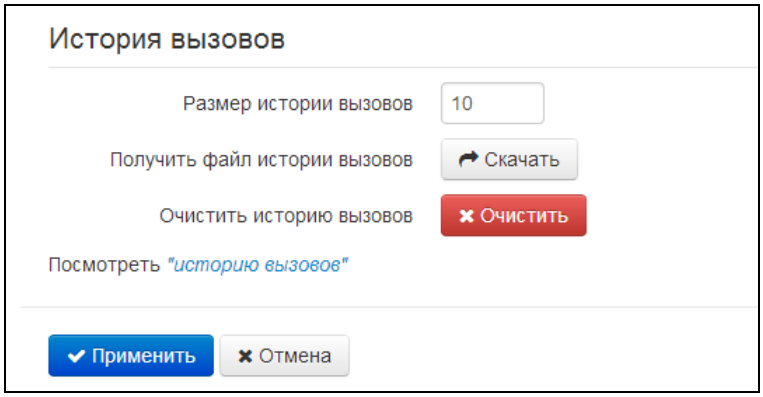
– *Название сигнала* – имя сигнала;

- *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»*.

3.6.3.9 Подменю «История вызовов»

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



- *Размер истории вызовов* – максимальное количество записей в журнале. Диапазон допустимых значений от 0 до 10000 строк. Значение 0 отключает ведение истории вызовов. При достижении установленного ограничения в журнале каждая последующая запись удалит самую струю 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»*.

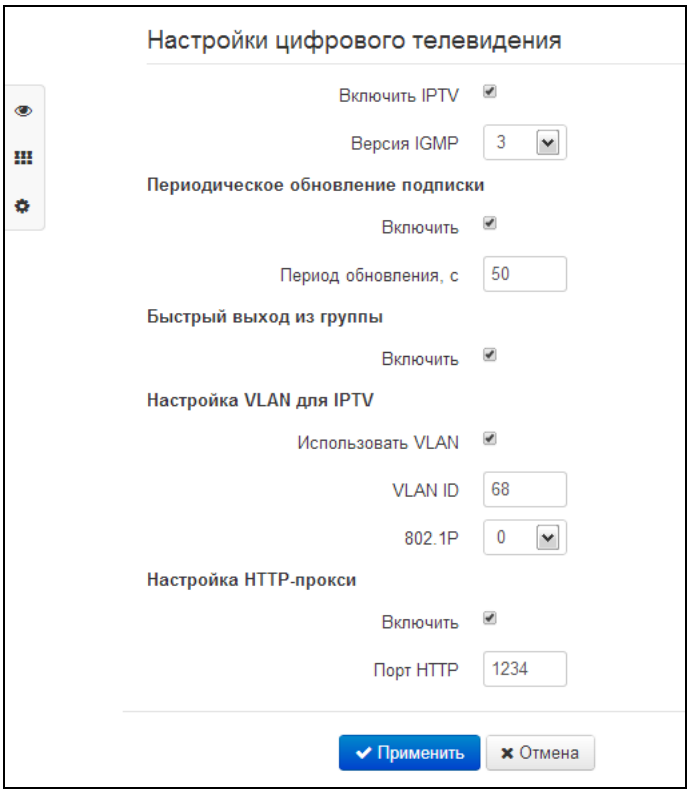
Для просмотра истории вызовов перейдите по ссылке «Посмотреть *“историю вызовов”*» (описание мониторинга параметров приведено в разделе *3.7.10 Подменю «История вызовов».*

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

3.6.4 Меню «IP-телевидение»

3.6.4.1 Подменю «IPTV»

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



- *Включить IPTV* – при установленном флаге разрешена трансляция сигналов IP-телевидения с WAN-интерфейса *RG-2400/RG-4400* (из сети провайдера) на устройства, подключенные к LAN-интерфейсу (по Ethernet или Wi-Fi);
- *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.

Переодическое 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.

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 группового трафика;
- *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

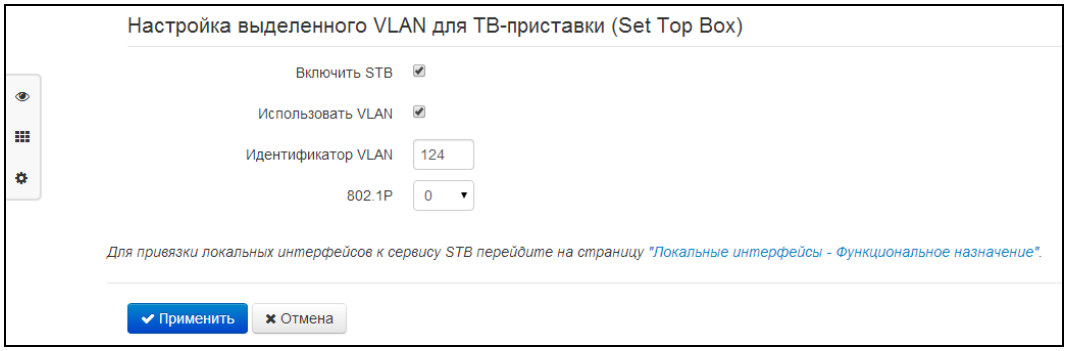
- *Включить* – при установленном флаге включена функция HTTP-прокси. HTTP-прокси осуществляет преобразование UDP-потока в поток HTTP, использующий протокол TCP (протокол надежной доставки пакетов), что позволяет улучшить качество транслируемого изображения при плохом качестве канала связи в локальной сети. Функция полезна при просмотре IPTV через беспроводный канал Wi-Fi;
- *Порт HTTP* – номер порта HTTP-прокси, с которого будет осуществляться транслирование видео-потока. Используйте этот порт для подключения к транслируемым устройством *RG-2400/RG-4400* потокам IPTV.

  Например, если *RG-2400/RG-4400* 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»*.

3.6.4.2 Подменю «STB»

В подменю «STB» выполняются настройки выделенной VLAN для работы цифровой телевизионной приставки (Set-Top Box).



- *Включить STB* – при установленном флаге будет включен режим STB для соответствующих портов в разделе «Локальные интерфейсы»;
- *Использовать VLAN* – при установленном флаге использовать для ТВ-приставки выделенный VLAN (номер VLAN может совпадать с номером VLAN для услуги Интернет или IPTV), иначе будет осуществляется работа STB без тега VLAN во внешней сети;

- *Идентификатор VLAN* – номер VLAN, который будет использоваться для передачи трафика сервиса STB с интерфейса WAN устройства;
- *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).

Добавление портов LAN в сервис STB производится в плитке *«Локальные интерфейсы»* из режима быстрого конфигурирования устройства. Для устройств с Wi-Fi в сервис STB также можно добавить точку доступа 2.4 или 5 ГГц (или обе сразу). При этом между WAN и LAN (WLAN)-интерфейсом сервиса STB создаётся мост для прозрачного прохождения пакетов от ТВ-приставки через устройство и обратно. Следует отметить, что в случае включенной опции «Использовать VLAN» с интерфейса WAN трафик уходит и принимается с настроенным тегом VLAN, а на интерфейсе LAN (WLAN) – трафик нетегированный (тег снимается).

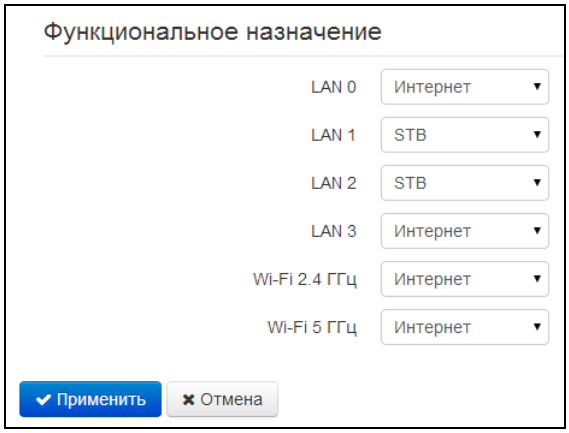
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

3.6.5 Меню «Локальные интерфейсы»

В меню «Локальные интерфейсы» для каждого интерфейса устанавливается функциональное назначение.

3.6.5.1 Подменю «Функциональное назначение»

В подменю «Функциональное назначение» для каждого порта и Wi-Fi интерфейса устанавливается тип предоставляемой услуги.



В текущей версии ПО для локальных интерфейсов можно выбрать тип сервиса Интернет, STB или пользовательские VLAN. При этом на каждый локальный интерфейс разрешается трансляция сигналов IP-телевидения при включенной функции IPTV.

Тип сервиса Интернет означает, что с данного LAN-порта будет осуществляться выход в сеть Интернет; тип сервиса STB – данный LAN-порт предназначен для подключения телевизионной приставки (Set-Top-Box). При этом порт Интернет соединен с WAN-интерфейсом одноименной услуги через маршрутизацию, а порт STB соединен с WAN-интерфейсом услуги STB через мост (трафик проходит прозрачно с WAN на LAN и обратно).

WAN-интерфейс услуги STB настраивается в разделе 3.6.4.2.

На устройствах RG-2402G-W, RG-2404G-W, RG-4404G-W и RG4402GF-W тип сервиса задаётся также для интерфейсов Wi-Fi – отдельно для 2.4 и 5 ГГц. Тип сервиса Интернет означает, что с данного Wi-Fi-интерфейса через маршрутизацию осуществляется доступ в Интернет; тип сервиса STB – данный Wi-Fi-интерфейс включен в мост STB и прозрачно соединён с WAN-интерфейсом этой услуги.

Таким образом, устройство серии *RG-2400/RG-4400* обеспечивает возможность выхода в Интернет и подключения телевизионной приставки как по проводному каналу, так и через беспроводное подключение по Wi-Fi в любом диапазоне частот.

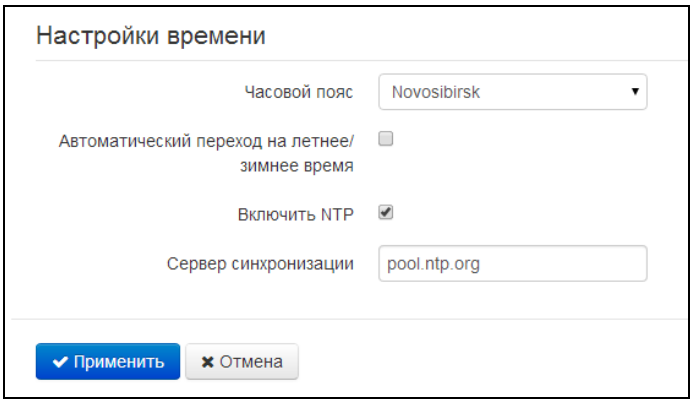
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

3.6.6 Меню «Система»

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

3.6.6.1 Подменю «Время»

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



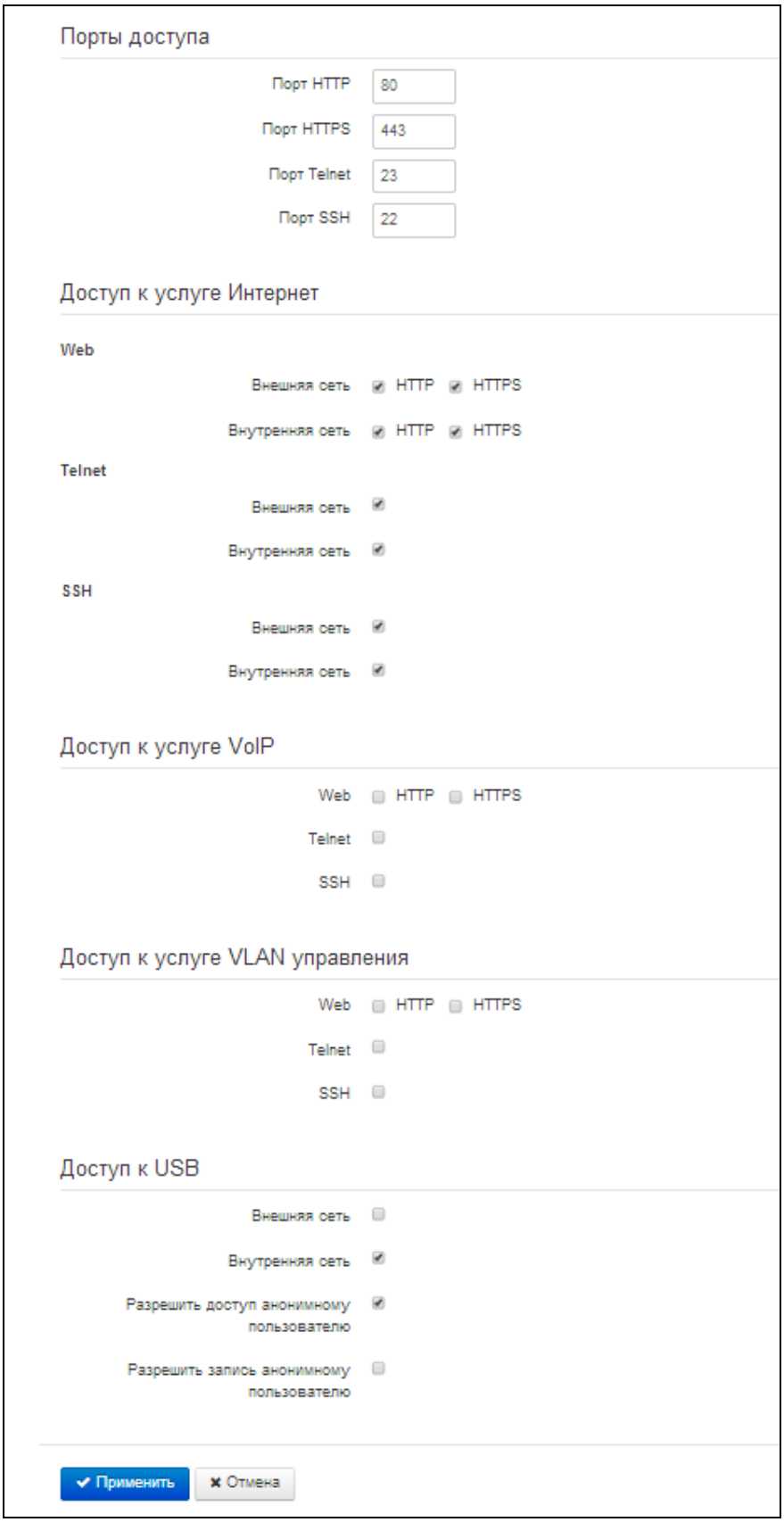
Настройки времени

- *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 будет переход на летнее/зимнее время будет выполняться автоматически в заданный период времени:
  - *Переход на летнее время* – день, когда выполнять переход на летнее время;
  - *Переход на зимнее время* – день, когда выполнять 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.

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

3.6.6.2 Подменю «Доступ»

В подменю «Доступ» настраивается доступ к устройству посредством WEB-интерфейса, Telnet и SSH, а также доступ к USB-носителю.



Порты доступа

В данном разделе выполняется настройка TCP-портов для сервисов 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).

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, Внутренняя сеть:

- *HTTP* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через LAN-порт (или через беспроводную точку доступа Wi-Fi) по протоколу HTTP (небезопасное подключение);
- *HTTPS* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через LAN-порт (или через беспроводную точку доступа Wi-Fi) 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 или беспроводную точку доступа Wi-Fi) 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 или беспроводную точку доступа Wi-Fi) 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 VLAN управления:

Раздел позволяет настроить доступ к интерфейсу managementVLAN 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*, пароль – *password*. После авторизации станет 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 или беспроводную точку доступа Wi-Fi) сети установите соответствующие флаги.

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

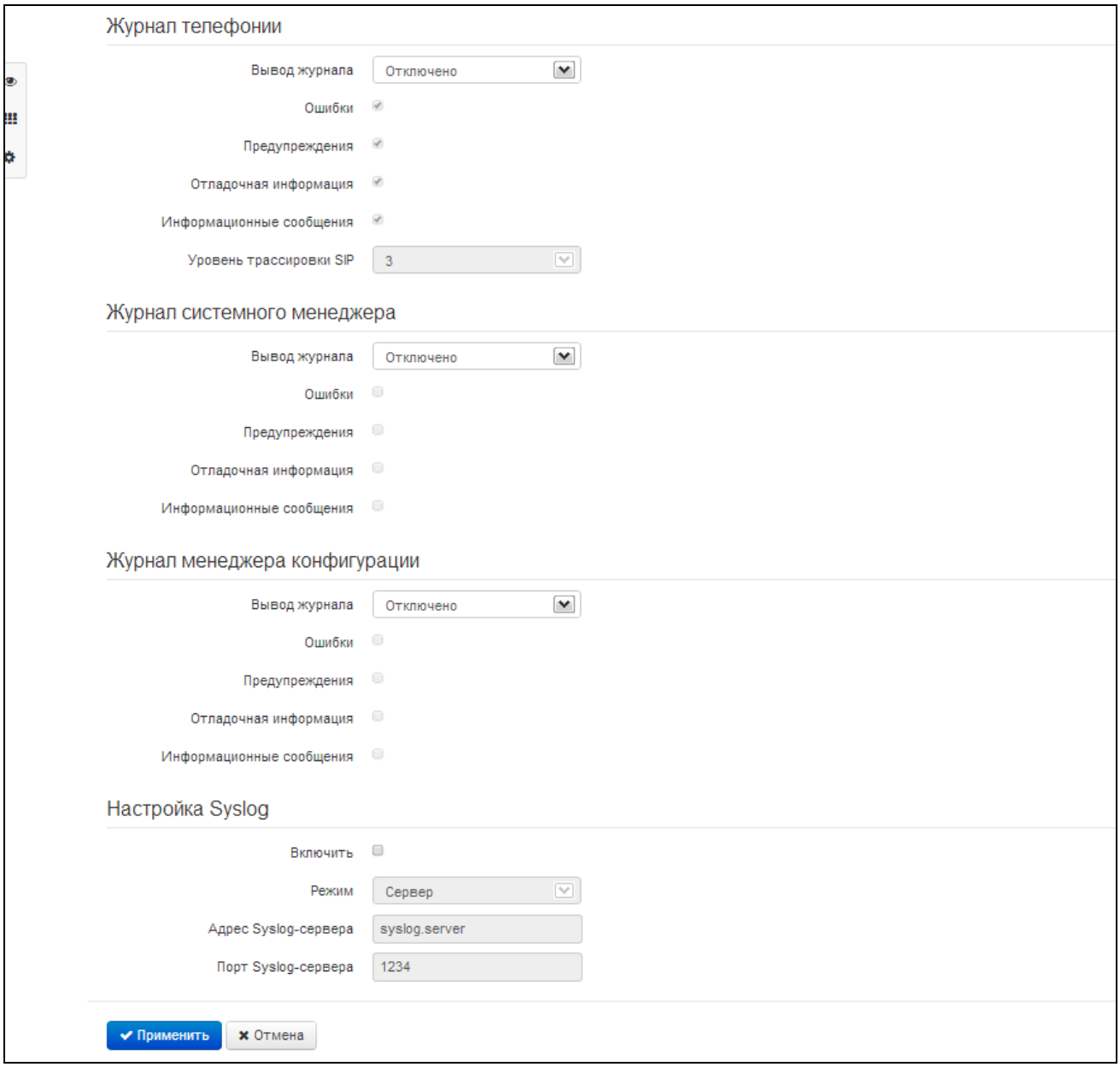
Для разрешения записи данных на USB-устройство анонимному пользователю установите флаг «Разрешить запись анонимному пользователю».

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

3.6.6.3 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 конфиг-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);
  - *Телнет* – 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);
  - *Телнет* – 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);
  - *Телнет* – 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»).

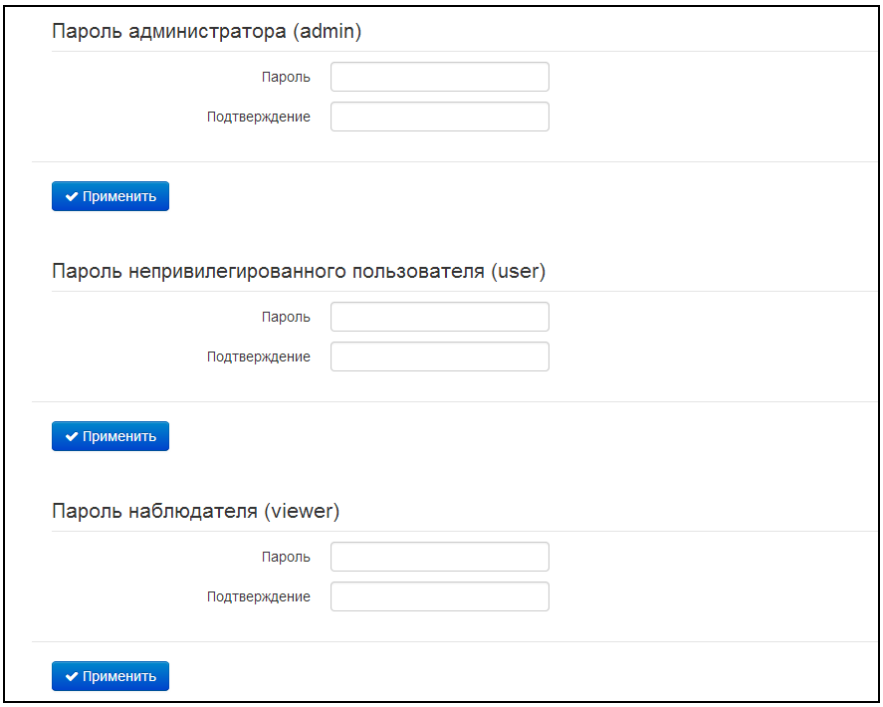
3.6.6.4 Подменю «Пароли»

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

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) и настройки Wi-Fi, 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

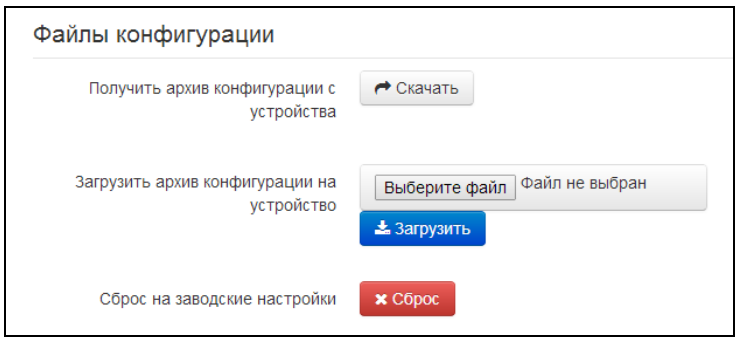


- *Пароль администратора* – в соответствующие поля введите пароль администратора и подтвердите его;
- *Подтверждение пароля* – в соответствующие поля введите пароль непривилегированного пользователя и подтвердите его.

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

3.6.6.5 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

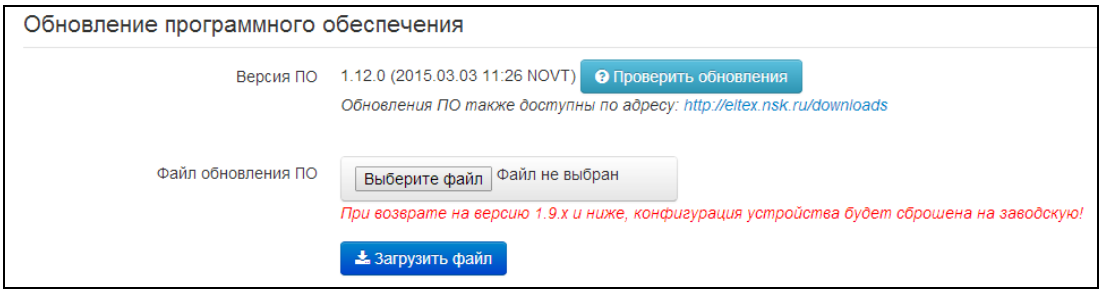
- *Загрузить архив конфигурации на устройство* – выбор сохраненного на локальном компьютере файла конфигурации. Для обновления конфигурации устройства нажмите

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».

3.6.6.6 Подменю «Обновление ПО»

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



- *Версия ПО* – версия программного обеспечения, установленного на устройстве;
- *Проверить обновления* – кнопка для проверки последней версии программного обеспечения. С помощью этой функции Вы можете быстро проверить наличие новой версии программного обеспечения и в случае необходимости выполнить его обновление.

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.nsk.ru/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, не выполняйте его перезагрузку в процессе обновления ПО.

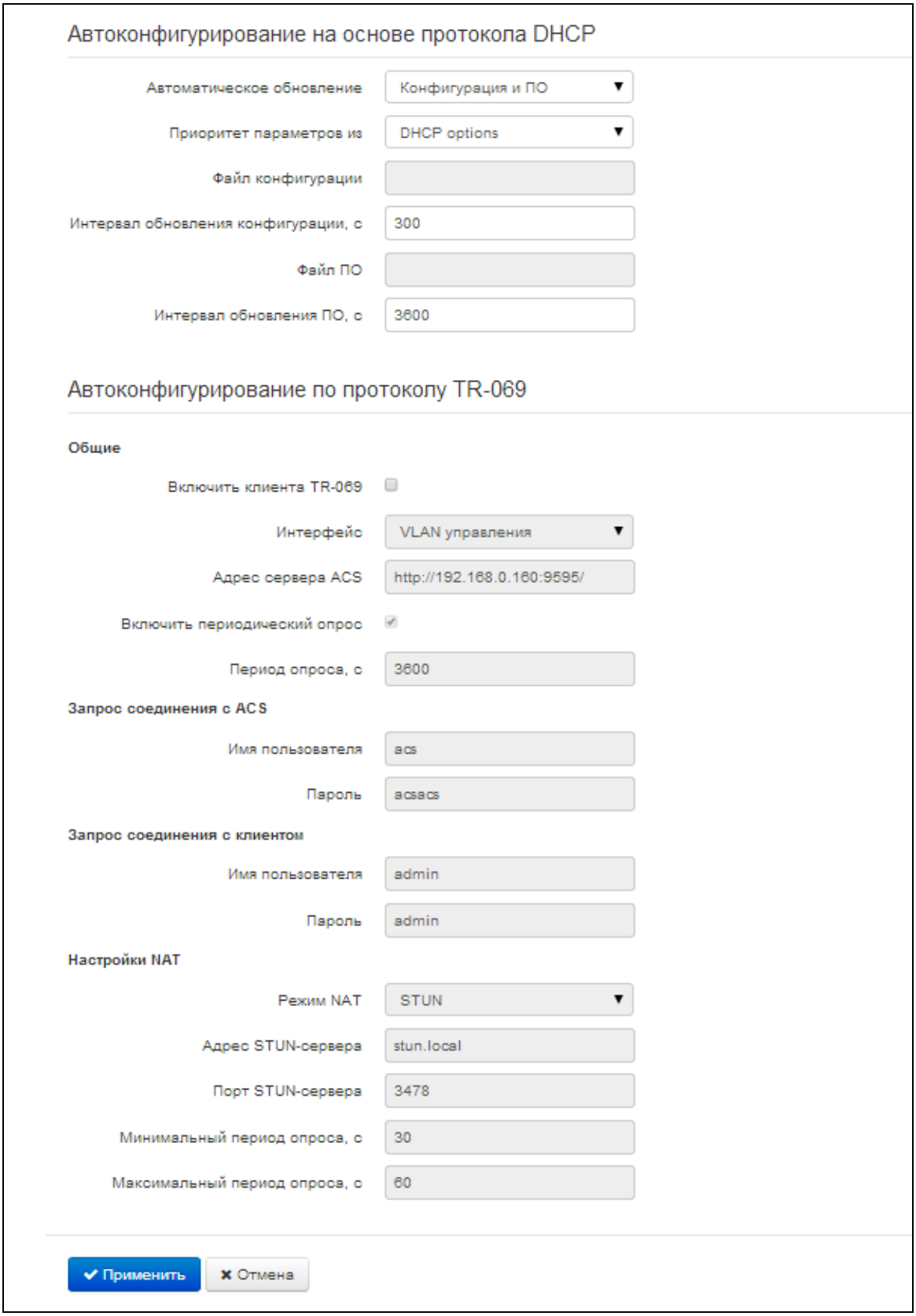
3.6.6.7 Подменю «Перезагрузка»

В подменю «Перезагрузка» выполняется перезапуск устройства.

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

3.6.6.8 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:

- *Автоматическое обновление* – выбор режима обновления устройства; возможно несколько вариантов:
  - *Выключено* – автоматическое обновление конфигурации и программного обеспечения устройства отключено;
  - *Конфигурация и ПО* – разрешено периодическое обновление конфигурации и программного обеспечения устройства;
  - *Только конфигурация* – разрешено периодическое обновление только конфигурации устройства;
  - *Только ПО* – разрешено периодическое обновление только программного обеспечения устройства.
- *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 работу алгоритма смотрите в разделе 6;
  - *DHCP options* – пути к файлам конфигурации и программного обеспечения определяются из DHCP опций 43 и 66 (для этого необходимо для услуги Интернет выбрать протокол DHCP); подробнее работу алгоритма смотрите в разделе 6;
- *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;
- *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.

Детальное описание алгоритма автоматического обновления на основе протокола DHCP смотрите в разделе 6.

Автоконфигурирование по протоколу TR-069:

Общие:

- *Включить клиента TR-069* – при установленном флаге разрешена работа встроенного клиента протокола TR-069;
- *Интерфейс* – выбор интерфейса для работы по протоколу TR-069. Если на шлюзе включен интерфейс *VLAN 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 10301). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS;
- *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.

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 возможность 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.

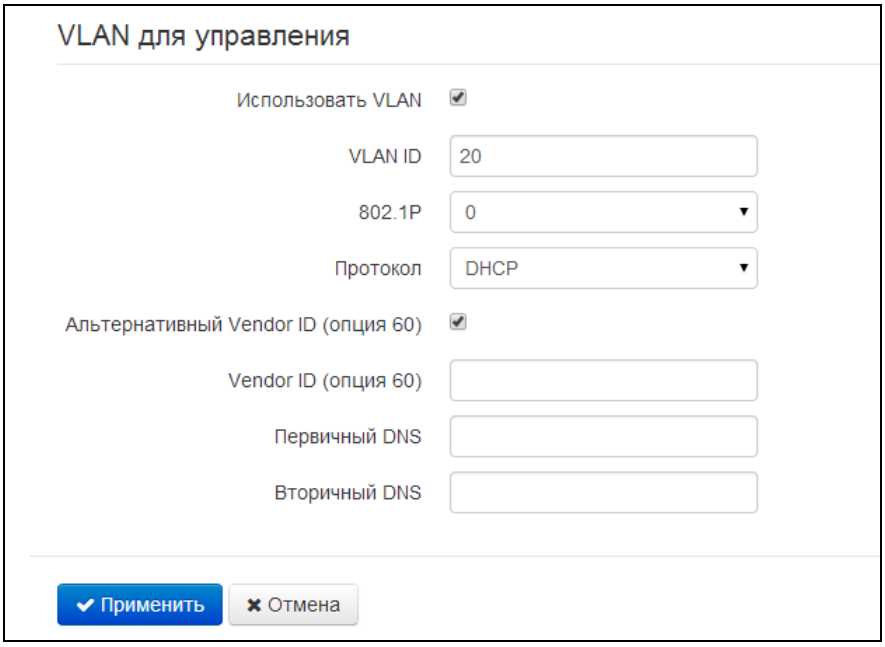
При выборе режима *Manual* публичный адрес клиента задается вручную через параметр *Адрес NAT* (адрес необходимо вводить в формате IPv4).

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».*

3.6.6.9 Подменю «VLAN управления»

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



- *Использовать VLAN* – при установленном флаге управление устройством может производиться в выделенной 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:

- *Static* – режим работы, при котором IP-адрес и все необходимые настройки на WAN-интерфейс назначается 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**]**

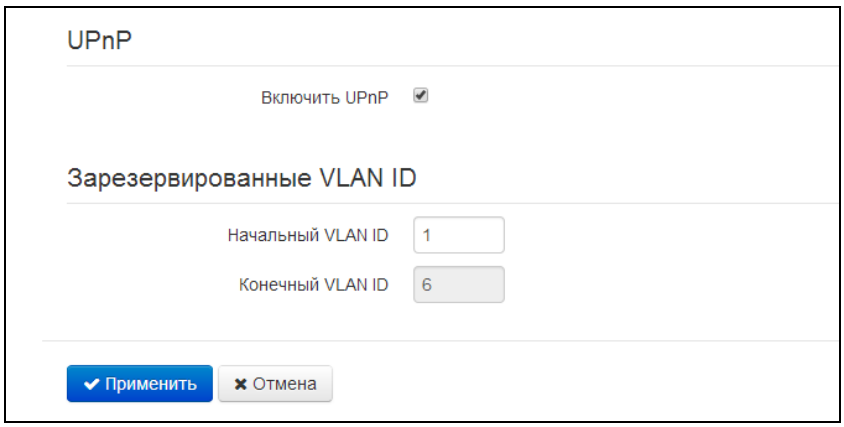
Пример:

[VENDOR:Eltex][DEVICE:RG-2404G-W][HW:1.4][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]

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

3.6.6.10 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, используемыми 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».*

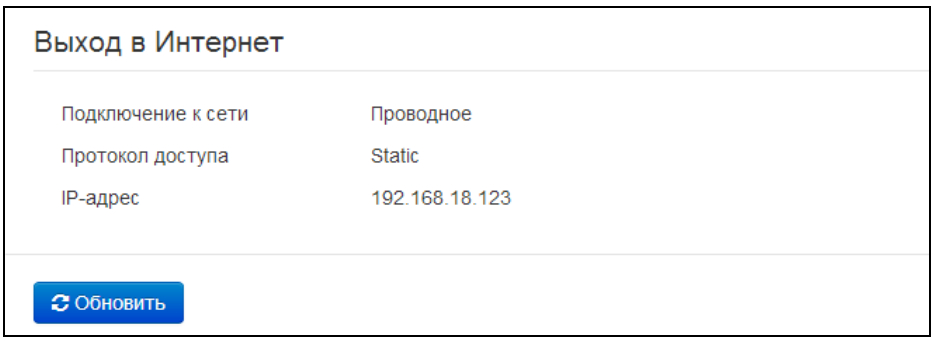
3.7 Мониторинг системы

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 Обновить**.**

3.7.1 Подменю «Интернет»

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

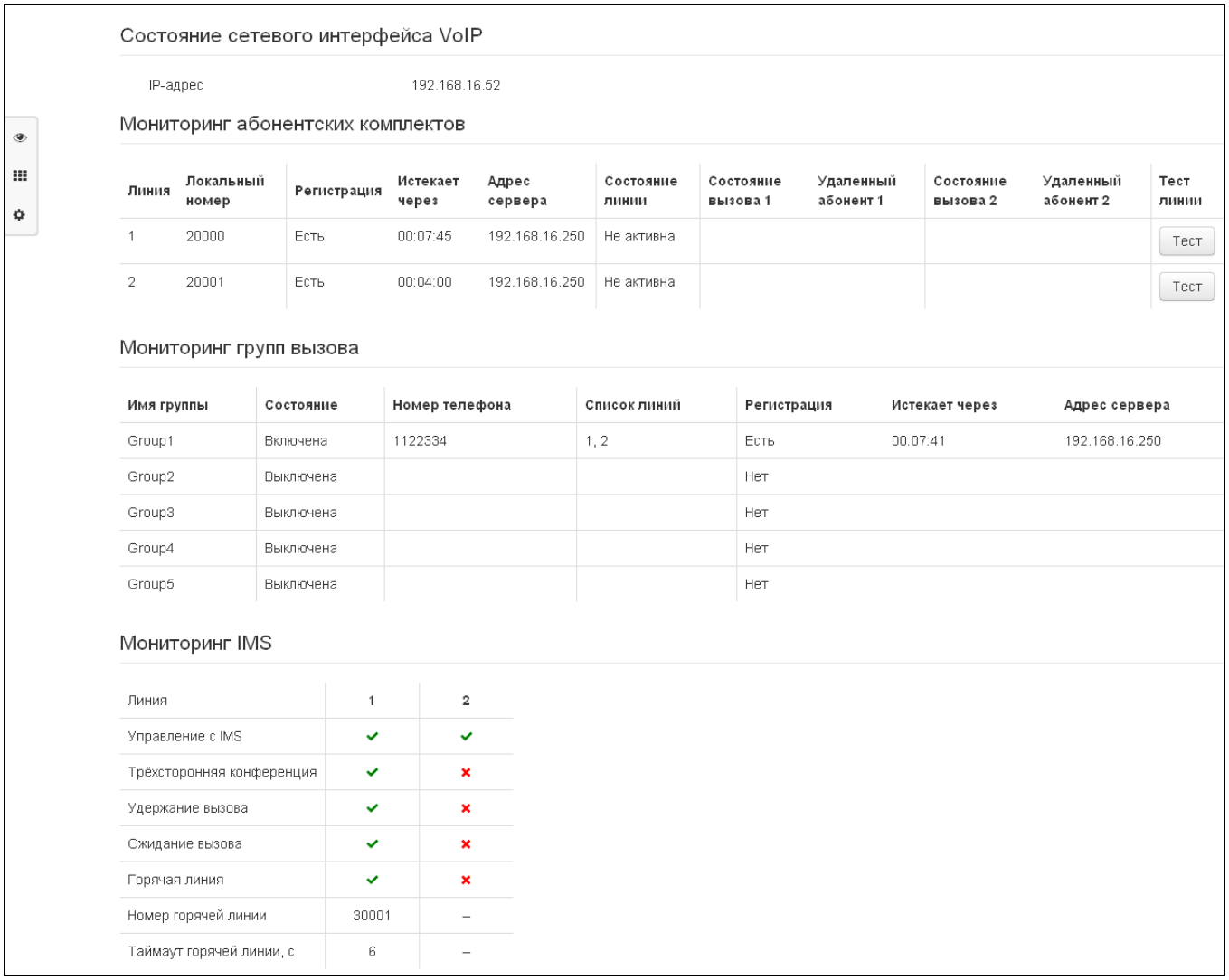


Выход в Internet

- *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;
  - *Wi-Fi-клиент* – подключение к сети провайдера осуществляется через активную точку доступа Wi-Fi. При этом RG-2400/RG-4400 выступает в роли Wi-Fi-клиента.
- *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.

3.7.2 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* – 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 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.

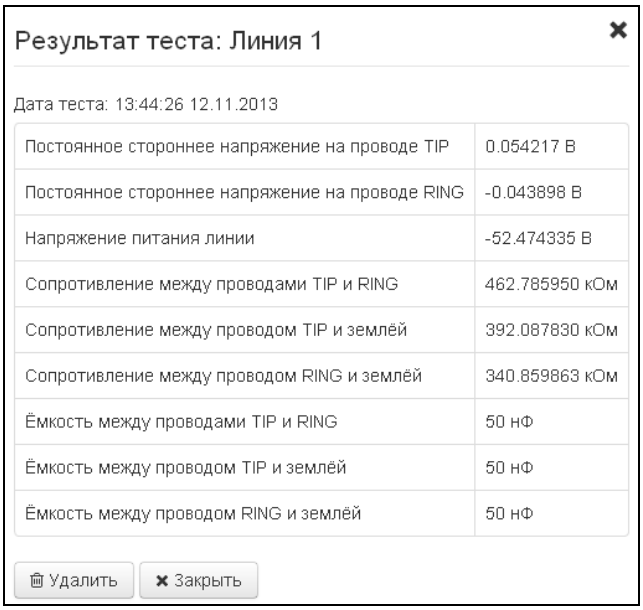
Линия	Локальный номер	Регистрация	Истекает через	Адрес сервера	Состояние линии	Состояние вызова 1	Удаленный абонент 1	Состояние вызова 2	Удаленный абонент 2	Тест линии
1	20000	Есть	00:06:12	192.168.16.250	Тестирование (75)					

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 TIP*
- *Постоянное стороннее напряжение на проводе RING*
- *Напряжение питания линии*
- *Сопротивление между проводами TIP и RING*
- *Сопротивление между проводом TIP и землёй*
- *Сопротивление между проводом RING и землёй*

- *Ёмкость между проводами TIP и RING*
- *Ёмкость между проводом TIP и землёй*
- *Ёмкость между проводом RING и землёй*

Пример результата теста линии 1:



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).

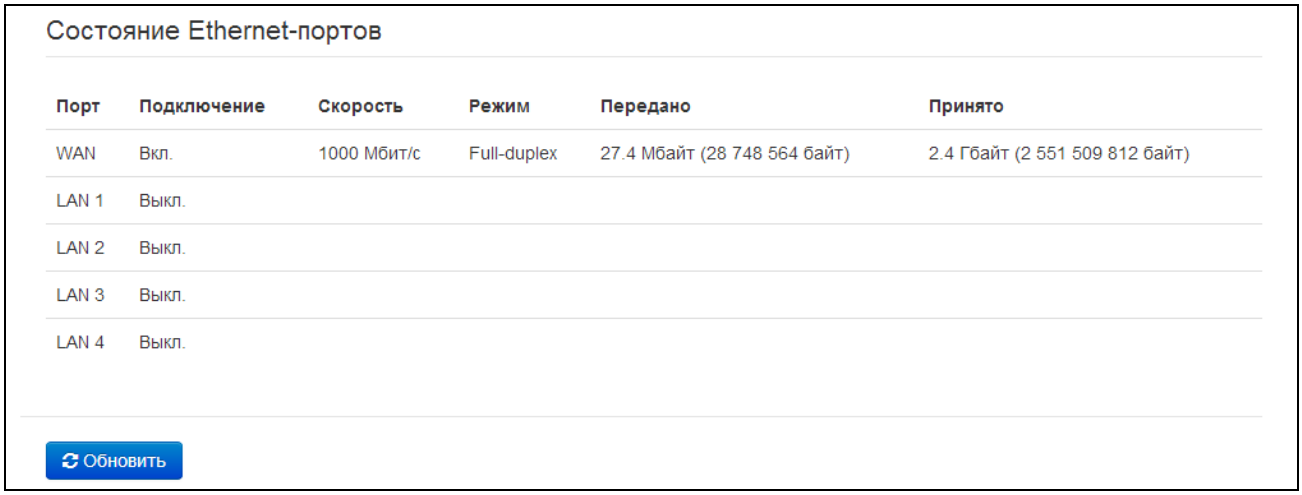
- *Управление с IMS* – показывает, включено или нет удаленное управление услугами абонентской линии с сервера IMS (настраивается в профиле SIP, см. подменю «Профили»);
- *Трёхсторонняя конференция* – показывает, пришла или нет команда на активацию услуги «Трёхсторонняя конференция» с сервера IMS;
- *Удержание 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.

✔ – услуга активирована;
✖ – услуга не активирована.

3.7.3 Подменю «Ethernet-порты»

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



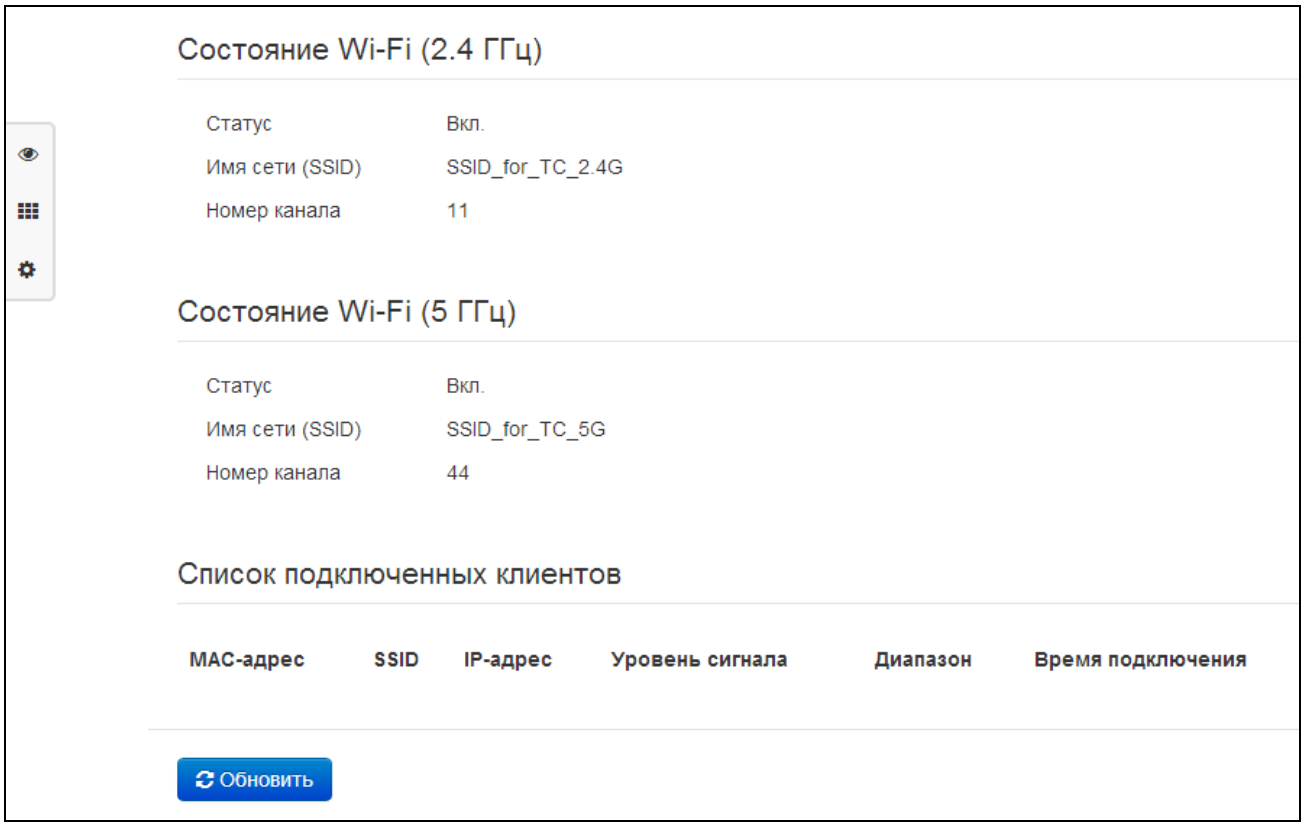
Состояние Ethernet-портов

- *Порт* – название порта:
  - *WAN* – порт внешней сети;
  - *LAN 0..3* – 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».

3.7.4 Подменю «Wi-Fi»

В подменю «Wi-Fi» осуществляется просмотр информации о подключенных клиентах к беспроводной точке доступа Wi-Fi.



Состояние Wi-Fi

- *Статус* – состояние сети Wi-Fi:
  - *Выкл.* – сеть Wi-Fi выключена;
  - *Вкл.* – сеть Wi-Fi включена.
- *Имя сети (SSID)* – имя точки доступа Wi-Fi в соответствующем диапазоне частот;
- *Номер канала* – текущий номер канала, используемый точкой доступа в соответствующем диапазоне частот.

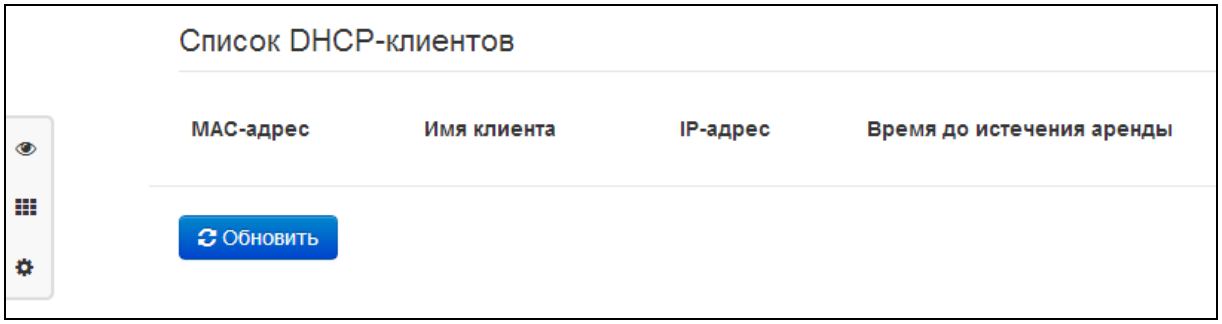
Список подключеных клиентов

- *MAC-адрес* – MAC-адрес клиента, который подключен к устройству по сети Wi-Fi;
- *SSID* – имя точки доступа, к которой подключен клиент;
- *IP-адрес* – IP-адрес, назначенный клиенту;
- *Уровень сигнала* – уровень сигнала от клиента;
- *Диапазон* – диапазон частот, в котором подключен клиент (2.4 или 5 ГГц);
- *Время подключения* – время подключения клиента к точке доступа.

Для получения текущей информации о подключенных Wi-Fi-клиентах нажмите кнопку «Обновить».

3.7.5 Подменю «DHCP»

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



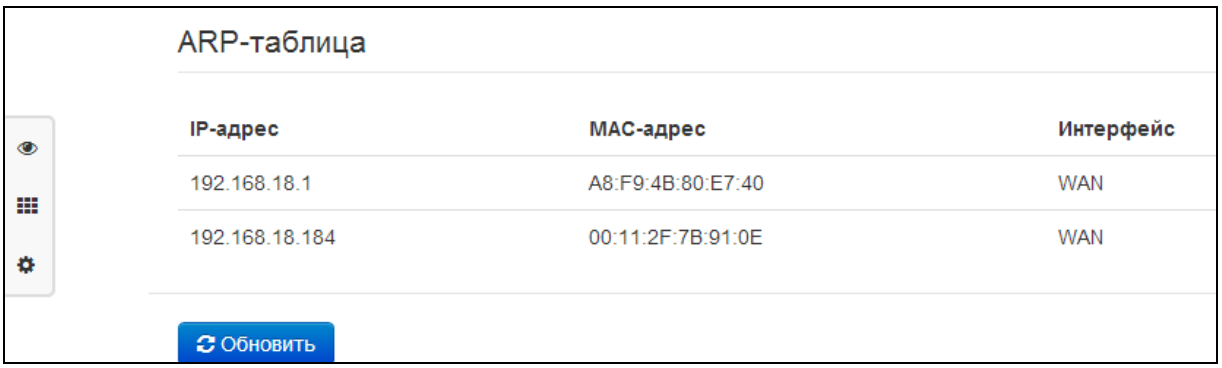
Активные DHCP-аренды

- *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».

3.7.6 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;
- *Интерфейс* – интерфейс, со стороны которого активно устройство: WAN, LAN, Bridge.

Для получения текущей информации нажмите кнопку «Обновить».

3.7.7 Подменю «Устройство»

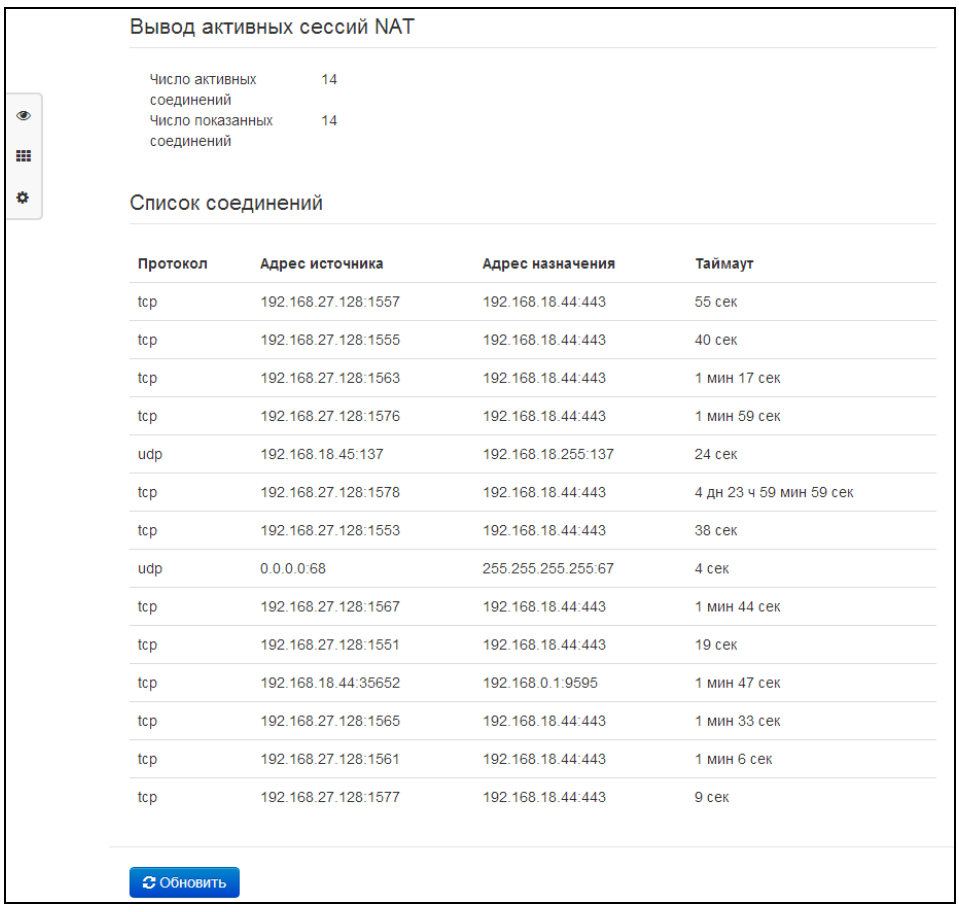
В подменю «Устройство» приведена общая информация об устройстве.

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.

3.7.8 Подменю «Conntrack»

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



Вывод активных сессий NAT

- *Число активных соединений* – общее количество активных сетевых соединений;
- *Число показанных соединений* – количество 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».

3.7.9 Подменю «Маршрутизация»

В подменю «Маршрутизация» отображается таблица маршрутизации устройства.

- *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.

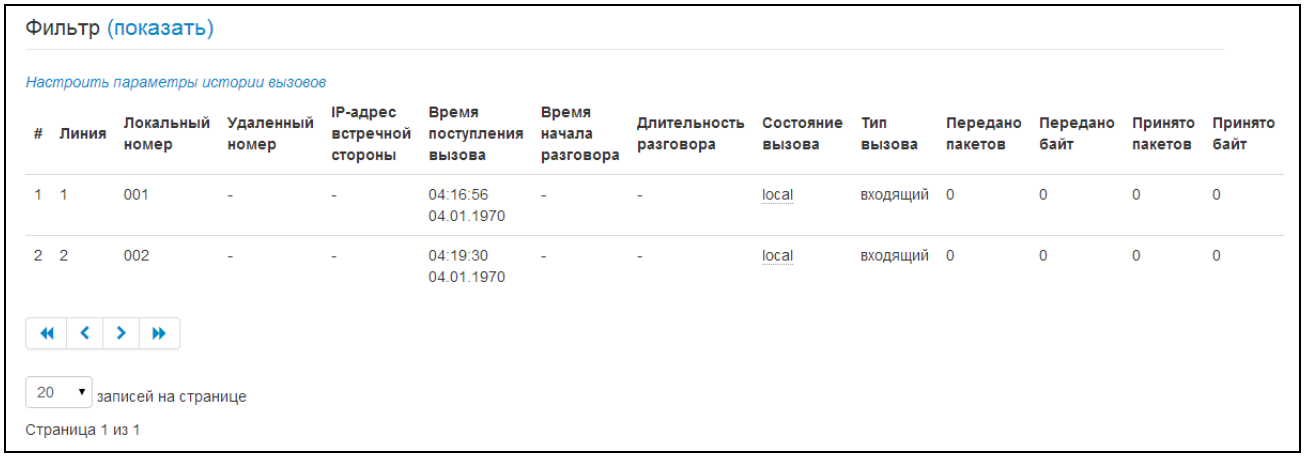
Для получения текущей информации нажмите кнопку «Обновить».

3.7.10 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.



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 *3.6.3.9 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.

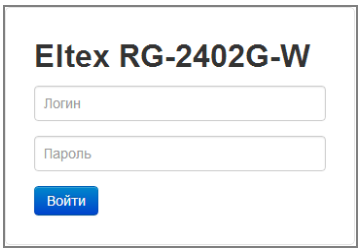
При нажатии на кнопку  произойдет переход к следующей странице с таблицей истории вызовов.

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

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

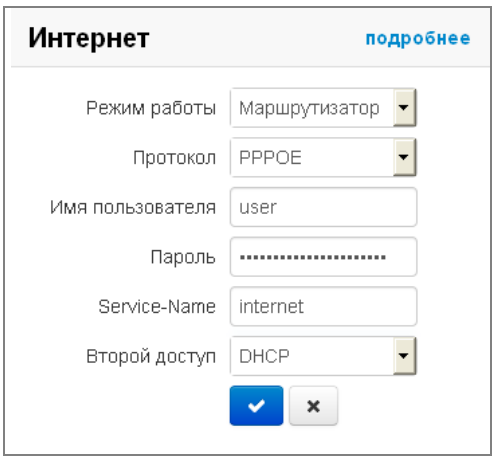
3.8 Пример настройки

1. Подключите ПК к одному из LAN-портов устройства, провод от сети провайдера подключите к порту WAN;
2. В адресной строке браузера введите IP-адрес шлюза (по умолчанию 192.168.1.1);
3. При успешном подключении к устройству появится окно с запросом логина и пароля. Укажите *Логин* – admin, Пароль – password. Нажмите кнопку «Войти».



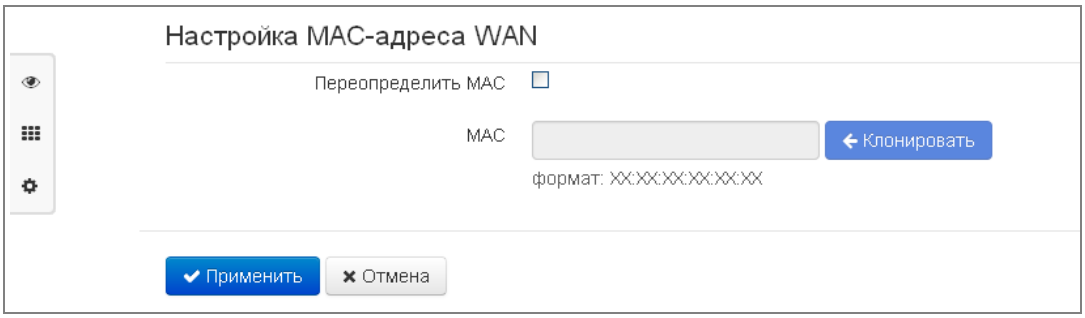
Если это окно не появилось, убедитесь, что в настройках сетевого подключение на вашем ПК установлено автоматическое получение IP-адреса.

4. В плитке «Интернет» настраивается внешнее соединение. 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  .

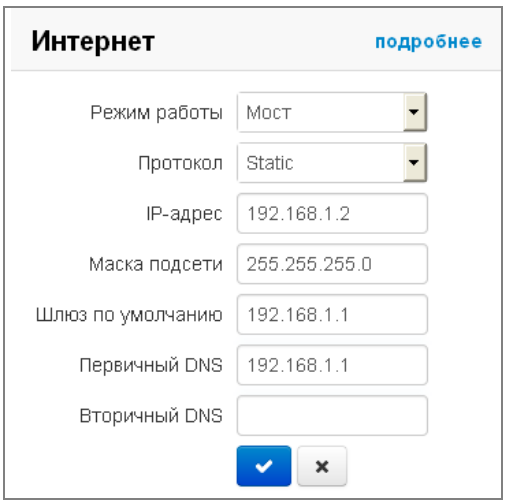


Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее» (смотрите раздел *3.6.2.1 Подменю «Интернет»*).

5. 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».

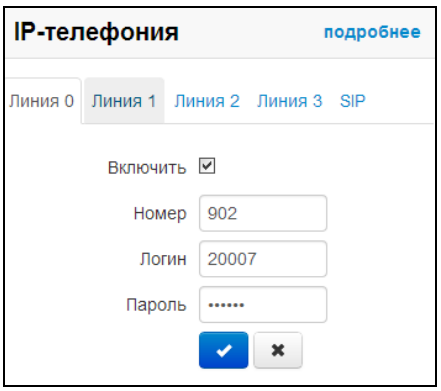


Если *RG-2400/RG-4400* будет использоваться в качестве 5-портового коммутатора, в плитке «Интернет» выберите значение поля «Режим работы» *Мост*. В поле «IP-адрес» укажите адрес, который будет назначен устройству для доступа к нему. Введите маску подсети (по умолчанию 255.255.255.0) и при необходимости шлюз по умолчанию и адрес DNS-сервера. Для сохранения и применения настроек нажмите кнопку .



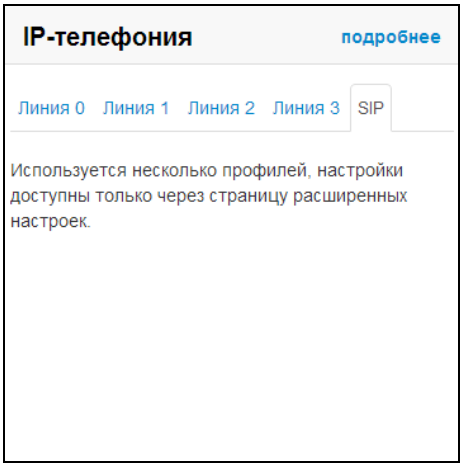
В режиме *Мост* шлюз не будет автоматически выдавать IP-адреса по протоколу DHCP устройствам, подключенным к интерфейсу LAN.

6. 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 .



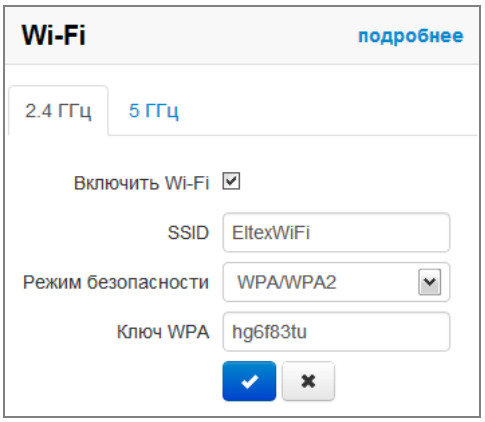
Таким же образом настройте остальные абонентские линии в других вкладках «Линия».

7. 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 *3.6.3 Меню «IP-телефония»*).

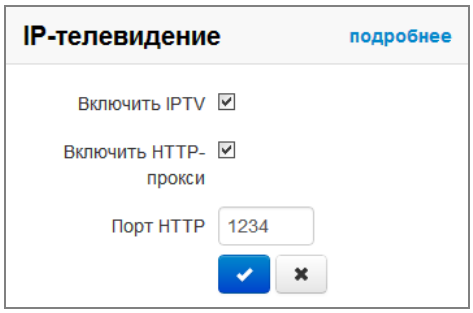
8. В плитке «Wi-Fi» настраиваются параметры сети Wi-Fi. Выберите необходимый частотный диапазон 2.4ГГц или 5ГГц. Для включения сети Wi-Fi установите флаг «Включить Wi-Fi». В поле «SSID» задается имя точки доступа. При выборе режима безопасности *«off»* для подключения к сети Wi-Fi не будет требоваться ключ доступа. Для того чтобы ограничить доступ к сети Wi-Fi в поле «Режим безопасности» выберите «WEP», «WPA» или «WPA2» и укажите ключ, который будет использоваться для подключения к сети. Длина ключа для WEP должна быть 5 или 13 символов, для WPA и WPA2 – от 8 до 64 символов. Чтобы сделать Wi-Fi сеть наиболее защищённой используйте режим WPA или WPA2. Для сохранения и применения настроек нажмите кнопку .



Существует возможность использовать одновременно два диапазона частот. Для этого настройте аналогичным образом точку доступа в другой вкладке.

Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее» (смотрите раздел *3.6.2.7 Подменю «Wi-Fi»*).

9. 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. Рекомендуется использовать HTTP-прокси при просмотре IP-телевидения через беспроводную сеть Wi-Fi (в целях улучшения качества транслируемого в эфире изображения). 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 (смотрите раздел *3.5.4 Меню «IP-телевидение»*).

4 ИСПОЛЬЗОВАНИЕ ДОПОЛНИТЕЛЬНЫХ УСЛУГ

4.1 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*».

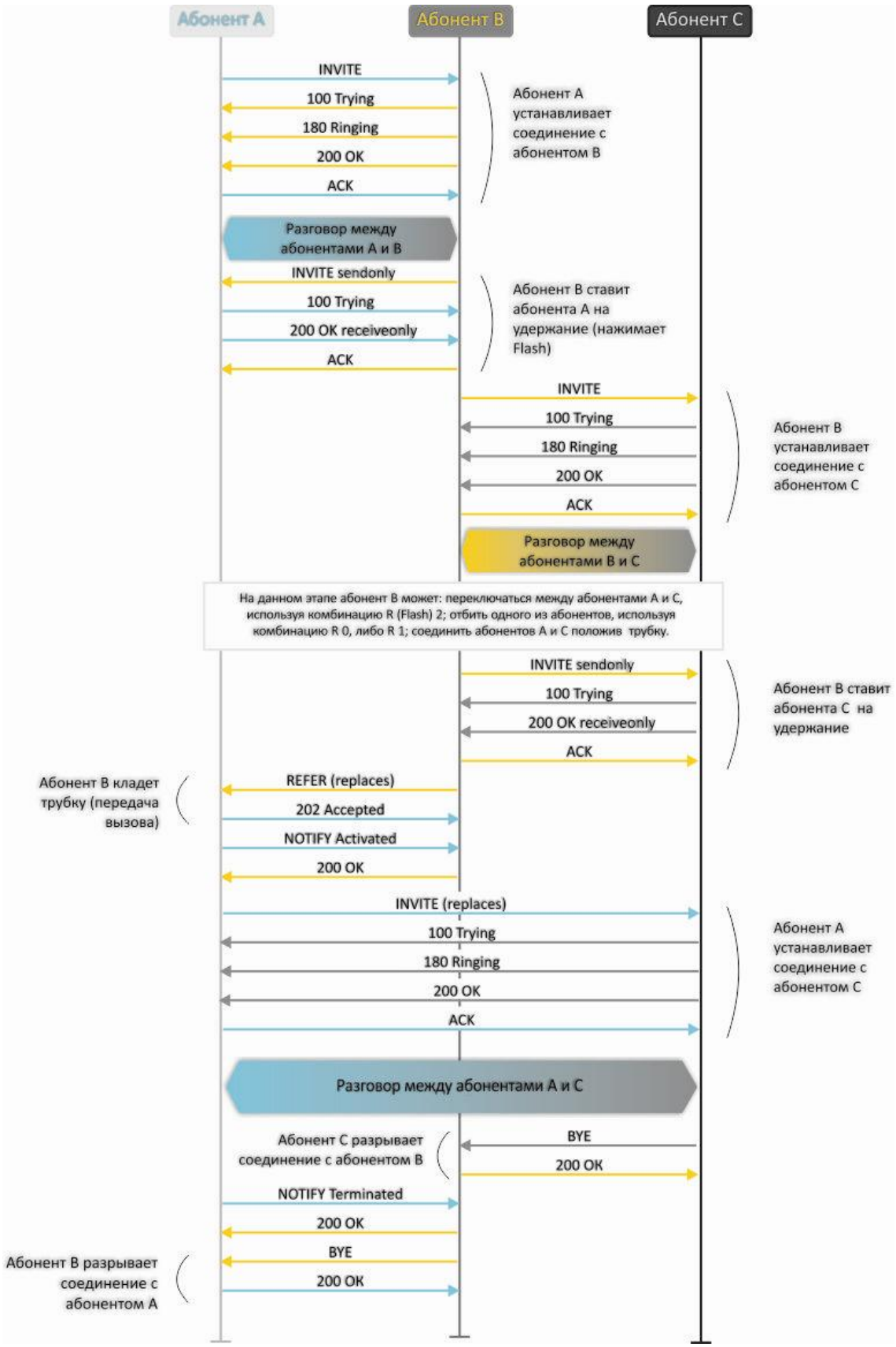
Услуга *«Attended calltransfer*» позволяет временно разорвать соединение с абонентом, находящимся на связи (абонент А), установить соединение с другим абонентом (абонент С), а затем вернуться к прежнему соединению без набора номера либо передать вызов с отключением абонента В.

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:

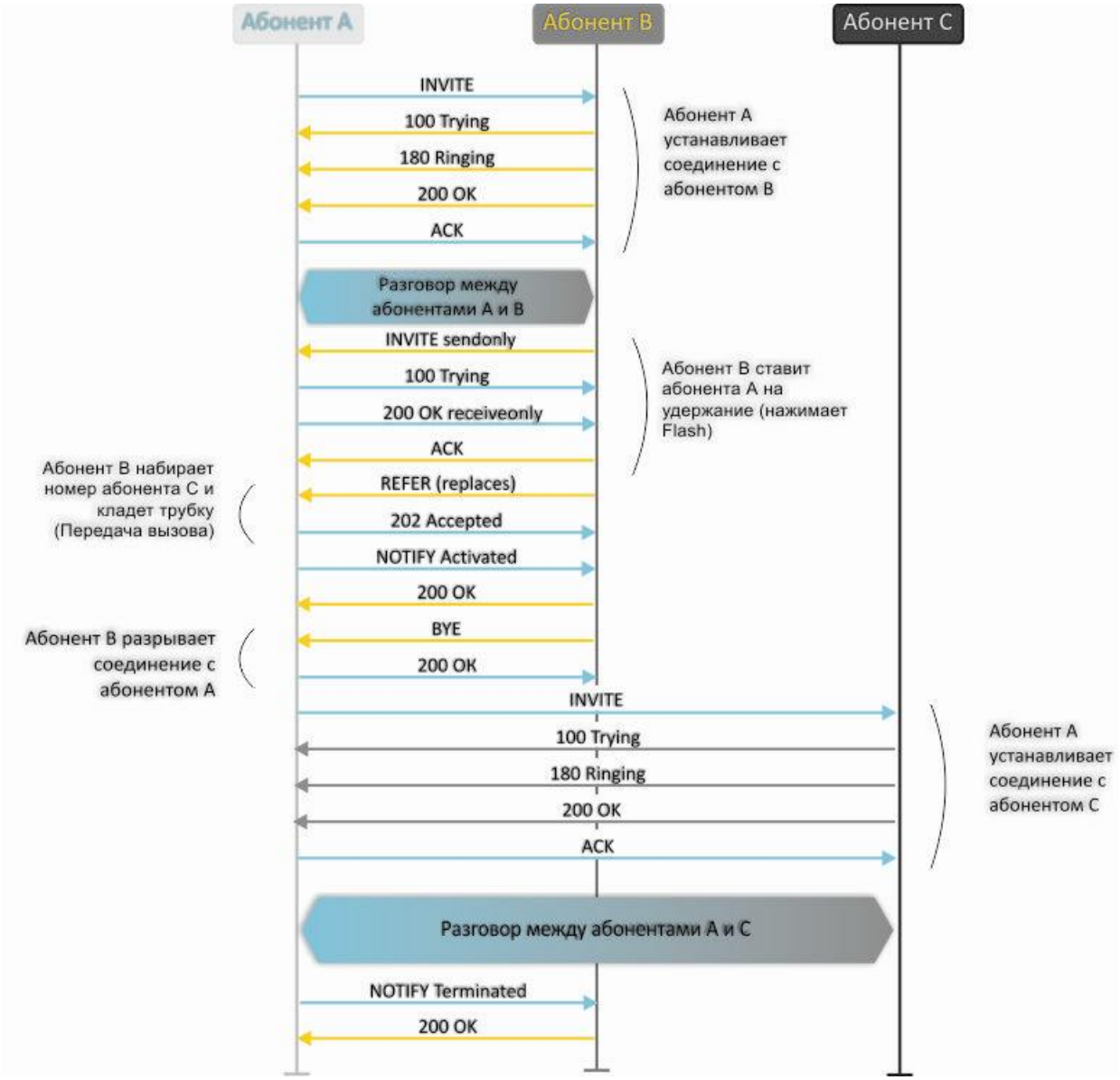
- R 0 – отключение абонента, находящегося на удержании, соединение с абонентом, находившимся на связи;
- R 1 – отключение абонента, находящегося на связи, соединение с абонентом, находившимся на удержании;
- R 2 – переключение на другого абонента (смена абонента);
- R 3 – конференция;
- R отбой – передача 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 *RG-2400/RG-4400* 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.

4.2 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*», либо «*Unattended calltransfer*», либо *«Local calltransfer»* в поле «*Режим использования flash*» и установки флага «*Ожидание вызова*».

Использование услуги:

Находясь в состоянии разговора и получении 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).

4.3 Трехсторонняя конференция

Трехсторонняя конференция – услуга, обеспечивающая возможность одновременного телефонного общения трех абонентов. Переход в режим конференции осуществляется по нажатию клавиш R 3 (описано в разделе **4.1 Передача вызова**).

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

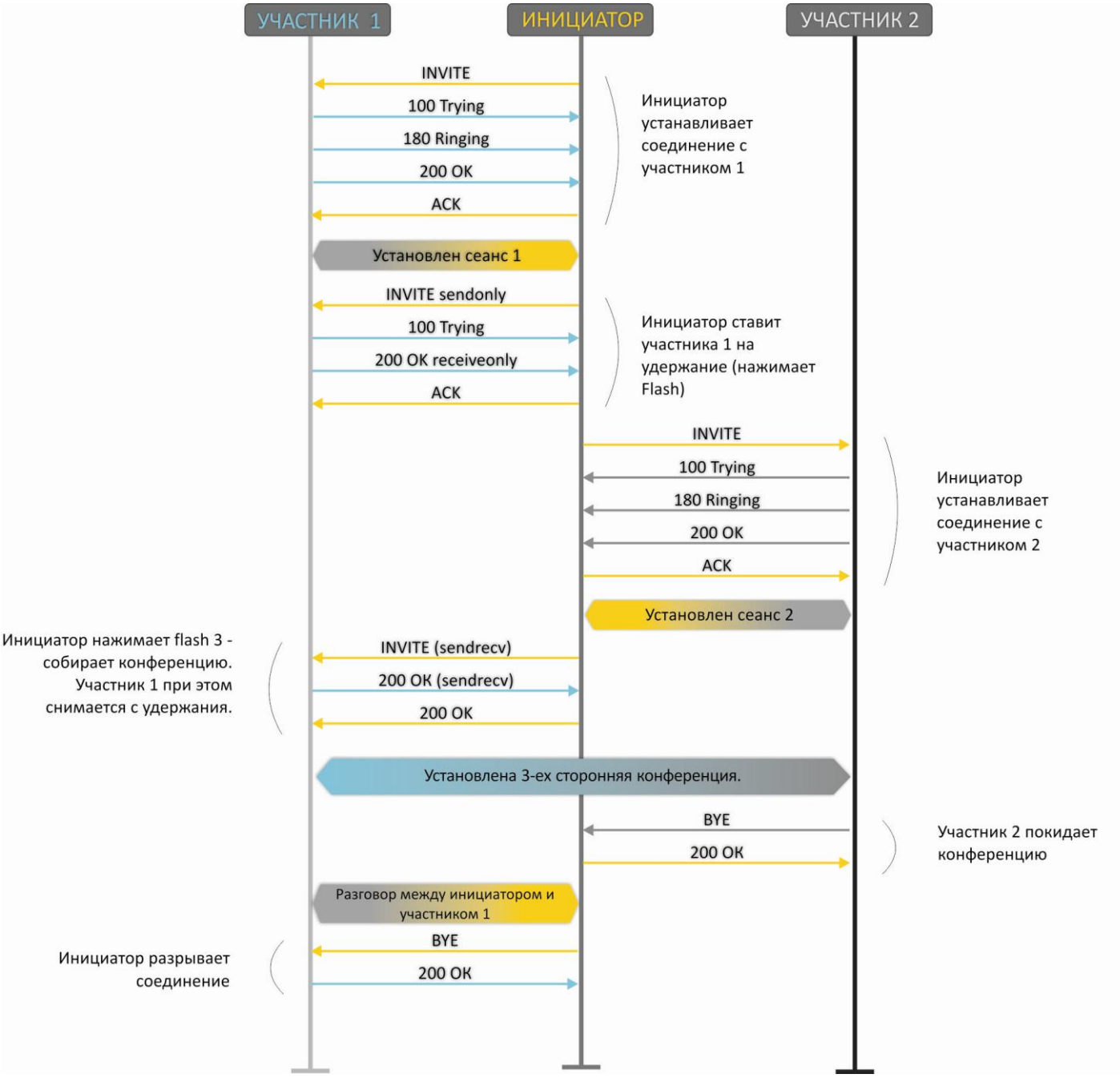
Возможно два режима работы трехсторонней конференции: локальный и удаленный. В первом режиме конференция собирается локально абонентом-инициатором, во втором – конференция устанавливается с помощью удаленного сервера, так называемого сервера конференции.

4.3.1 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.

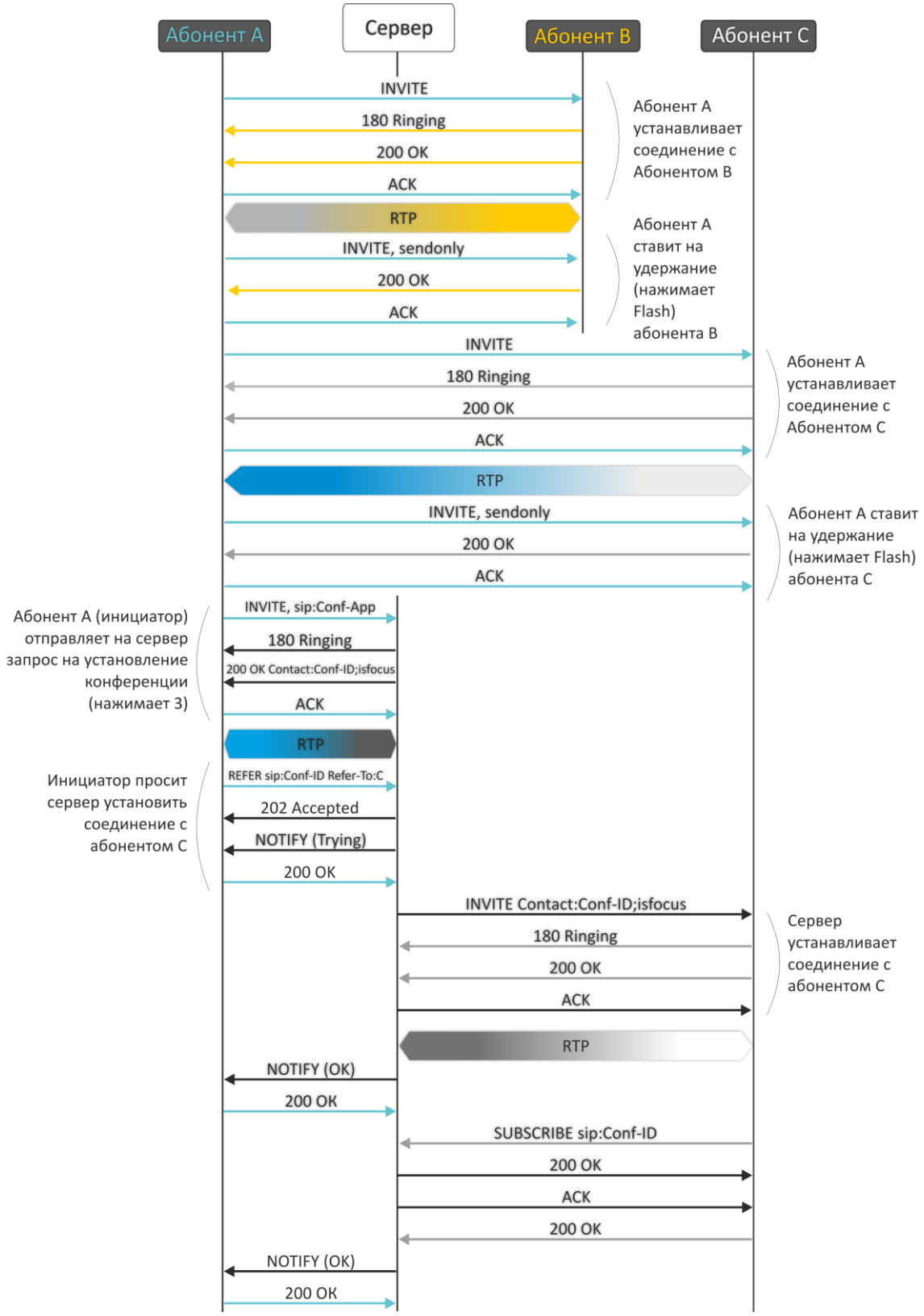
Конференция разрушается, если ее покидает инициатор, обоим участникам при этом будет передано сообщение отбоя. Если конференцию покидает любой из участников, то ее инициатор и второй участник переключатся в состояние обычного двустороннего разговора. Короткий отбой flash при этом обрабатывается как описано в разделах **4.1 Передача вызова** и **4.2 Уведомление о поступлении нового вызова**.

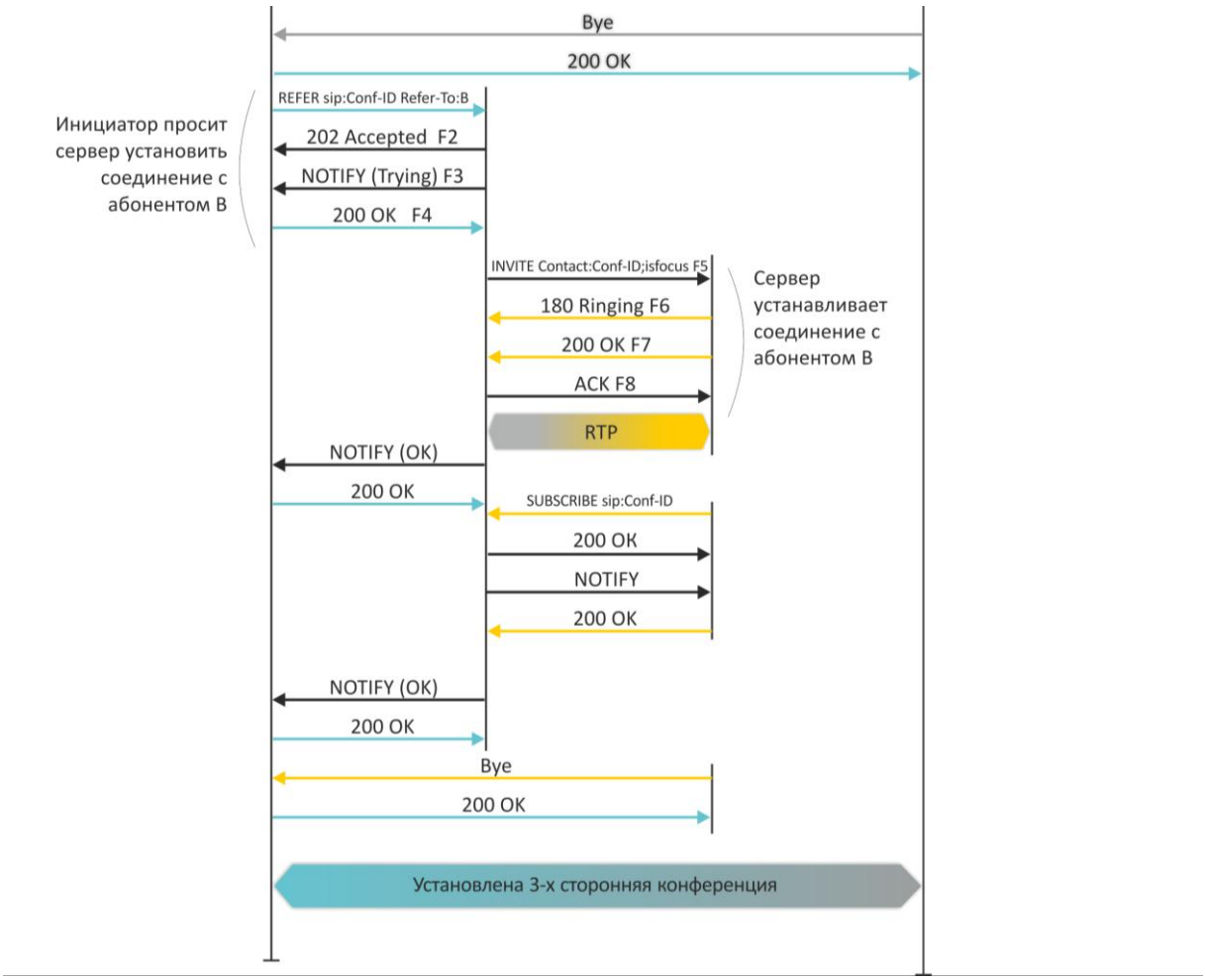
На рисунке ниже представлен алгоритм выполнения услуги «3-way conference» локально абонентом B по протоколу SIP.


УЧАСТНИК 1
ИНИЦИАТОР
УЧАСТНИК 2
INVITE
100 Trying
180 Ringing
200 OK
ACK
Инициатор устанавливает соединение с участником 1
Установлен сеанс 1
INVITE sendonly
100 Trying
200 OK receiveonly
ACK
Инициатор ставит участника 1 на удержание (нажимает Flash)
INVITE
100 Trying
180 Ringing
200 OK
ACK
Инициатор устанавливает соединение с участником 2
Установлен сеанс 2
Инициатор нажимает flash 3 - собирает конференцию. Участник 1 при этом снимается с удержания.
INVITE (sendrecv)
200 OK (sendrecv)
200 OK
Установлена 3-ех сторонняя конференция.
BYE
200 OK
Участник 2 покидает конференцию
Разговор между инициатором и участником 1
Инициатор разрывает соединение
BYE
200 OK

4.3.2 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.



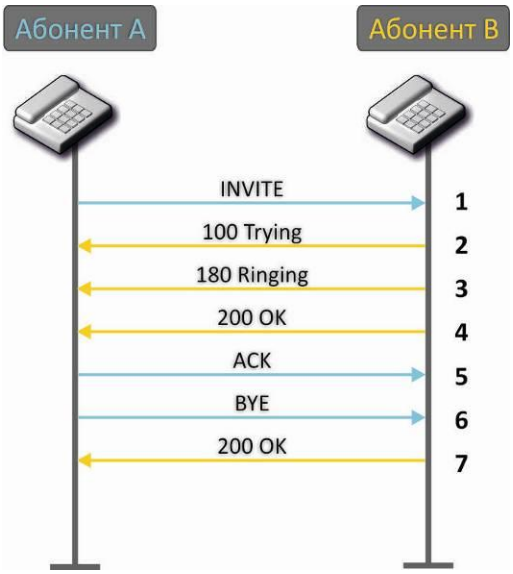

Bye
200 OK
REFER sip:Conf-ID Refer-To:B
Инициатор просит сервер установить соединение с абонентом B
202 Accepted F2
NOTIFY (Trying) F3
200 OK F4
INVITE Contact:Conf-ID;isfocus F5
Сервер устанавливает соединение с абонентом B
180 Ringing F6
200 OK F7
ACK F8
RTP
NOTIFY (OK)
200 OK
SUBSCRIBE sip:Conf-ID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

5 АЛГОРИТМЫ УСТАНОВЛЕНИЯ СОЕДИНЕНИЯ

5.1 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 proxy-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.

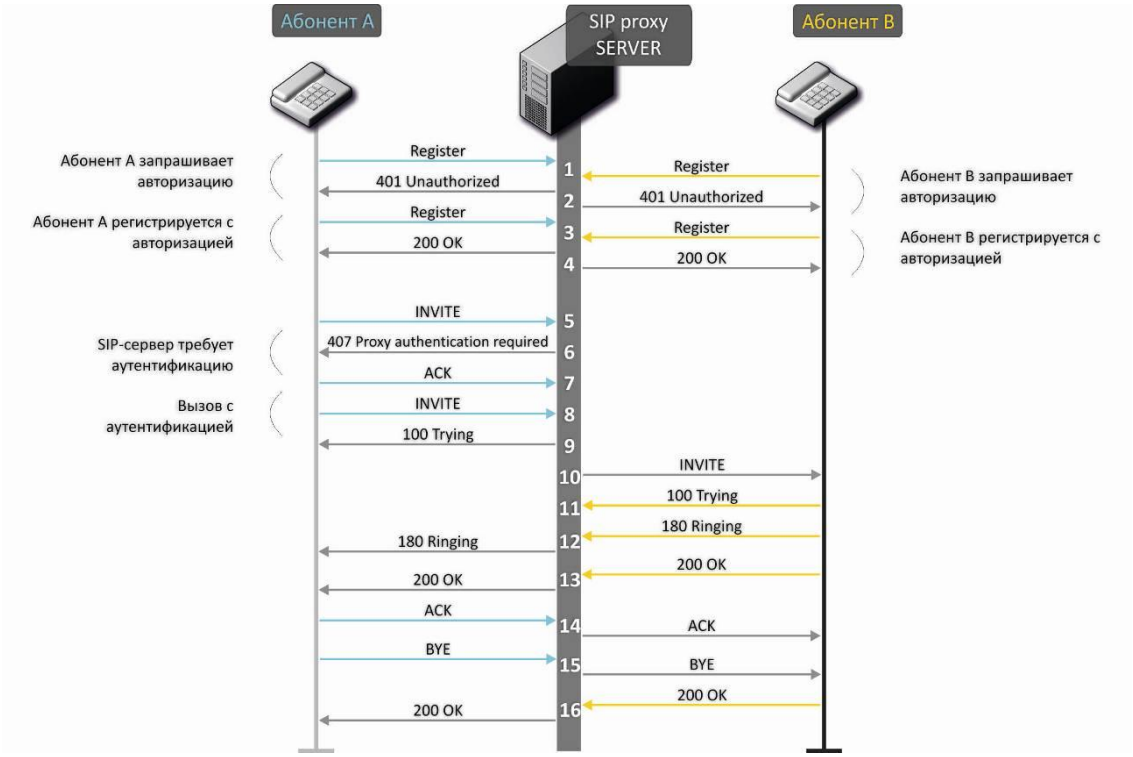


Описание алгоритма:

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

5.2 Алгоритм вызова с участием SIP proxy-сервера

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



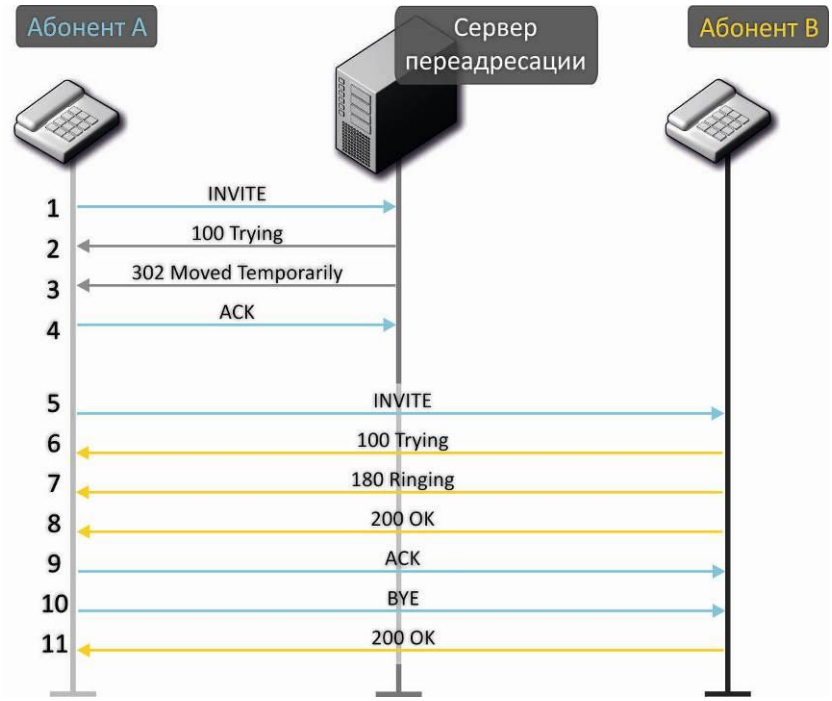
Описание алгоритма:

Регистрация на SIP-сервере.

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

5.3 Алгоритм вызова с участием сервера переадресации

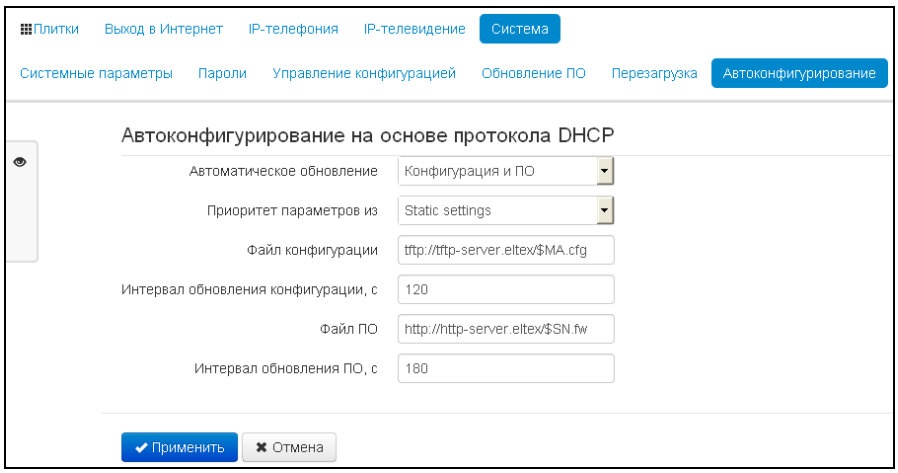
В данном разделе описывается сценарий установления соединения между двумя шлюзами с участием сервера переадресации. В этом случае вызывающий шлюз (абонент А) самостоятельно устанавливает соединение, а сервер переадресации лишь реализует преобразование постоянного адреса вызываемого абонента в его текущий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



Описание алгоритма:

1. Абонент «А» вызывает абонента «В». 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 «В» у сервера местоположения. Полученная информация (текущий адрес вызываемого пользователя или список зарегистрированных адресов вызываемого пользователя) передается в сообщении «302 moved temporarily» абоненту «А».
4. Шлюз абонента «А» подтверждает прием ответа от сервера переадресации.
5. Абонент «А» напрямую вызывает абонента «В».
6. Шлюз абонента «В» принял команду на обработку.
7. Абонент «В» свободен. В этот момент на аппарат абонента «В» выдается «Посылка вызова», а абоненту «А» «Контроль посылки вызова».
8. Абонент «В» отвечает на вызов.
9. Шлюз абонента «А» подтверждает установление сессии.
10. Отбой абонентка «А», абоненту «В» выдается акустический сигнал «Занято».
11. Шлюз абонента «В» подтверждает принятую команду отбоя.

6 АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP



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

1. 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;
- *$PN* – Product name – вместо данного макроса в URL файла устройство подставляет название модели (например, RG-2402G-W);
- *$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/RG-2400/RG-4400/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_rg24.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: rg24.cfg;
- для имени файла программного обеспечения: rg24.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/rg24.cfg,

а URL файла ПО:

tftp://update.local/rg24.fw.

2. 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: rg24.cfg;
   - для имени файла программного обеспечения: rg24.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>|8|<vlan_tag>

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;

8 - код тега VLAN для управления.

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

Алгоритм определения параметров URL файлов конфигурации и программного обеспечения из DHCP опций 43 и 66, 67.

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 перегружайте 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 7.

7 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 *RG-2400/RG-4400*.
- Если процесс передачи файла начался – дождитесь его окончания, после чего *RG-2400/RG-4400* 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 на заводские настройки.
- 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 – 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, ТППэпББбШп, ТППЗББбШп, ТППЗэпББбШп, 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 серии *RG-2400/RG-4400* 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, т.к. 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*.

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.
Телефоны центра технической поддержки:
+7(383) 274-47-87,
+7(383) 272-83-31,
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:

http://eltex-media.ru
http://eltex.nsk.ru/support/documentations
http://eltex.nsk.ru/forum
http://eltex.nsk.ru/interaktivnyi-zapros
http://eltex.nsk.ru/database