

IP-телефон

VP-12(P)

Руководство по эксплуатации

версия ПО 1.2.1

имя пользователя: **admin**
пароль: **password**

Версия документа	Дата выпуска	Содержание изменений
Версия 1.2	13.11.2017	Синхронизация с версией ПО 1.2.1.
Версия 1.1	10.10.2017	Синхронизация с версией ПО 1.2.0.
Версия 1.0	27.07.2017	Первая публикация
Версия программного обеспечения	Версия ПО: 1.2.1. Версия Web-интерфейса: 1.1. 7	

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

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

Примечания и предупреждения



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



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

СОДЕРЖАНИЕ

Введение	5
1 ОПИСАНИЕ ИЗДЕЛИЯ	6
1.1 Назначение	6
1.2 Характеристика устройства	6
1.3 Структура и принцип работы изделия.....	7
1.4 Основные технические параметры.....	8
1.5 Конструктивное исполнение	9
1.5.1 Верхняя панель устройства	9
1.5.2 Задняя панель устройства	10
1.5.3 Световая индикация	10
1.5.4 Индикация состояния на графическом дисплее	11
1.5.5 Сброс к заводским настройкам	12
1.6 Комплект поставки	12
2 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР	13
2.1 Начало работы.....	13
2.2 Режимы работы WEB-интерфейса	13
2.3 Применение конфигурации и отмена изменений	14
2.3.1 Применение конфигурации	14
2.3.2 Отмена изменений	14
2.4 Расширенные настройки	14
2.4.1 Основные элементы WEB-интерфейса	14
2.4.2 Меню «Сеть»	15
2.4.3 Меню «IP-телефония»	33
2.4.4 Меню «Система».....	52
2.5 Мониторинг системы	66
2.5.1 Подменю «Интернет».....	66
2.5.2 Подменю «IP-телефония»	67
2.6 Пример настройки.....	74
ПРИЛОЖЕНИЕ А. АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP	74
ПРИЛОЖЕНИЕ Б. ПРОЦЕДУРА ВОССТАНОВЛЕНИЯ СИСТЕМЫ ПОСЛЕ СБОЯ ПРИ ОБНОВЛЕНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.....	81
ПРИЛОЖЕНИЕ В. ЗАПУСК ПРОИЗВОЛЬНОГО СКРИПТА ПРИ СТАРТЕ СИСТЕМЫ	82
Приложение Г. НАСТРОЙКА dhcp клиентов в мультисервисном режиме.....	83

ВВЕДЕНИЕ

В настоящее время IP-телефония это одна из наиболее быстро развивающихся телекоммуникационных услуг. Для возможности предоставления VoIP-услуг абонентам сети разработаны IP-телефоны серии *VP-12(P)* (далее «устройство»).

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 *IP-телефонов серии VP-12(P)*.

1 ОПИСАНИЕ ИЗДЕЛИЯ

1.1 Назначение

VP-12P – IP-телефон, предназначенный для предоставления голосовых услуг и подключения персонального компьютера в IP-сеть по одному кабелю. Устройство обладает передовым функционалом, имеет поддержку технологии PoE, высокое качество и универсальный стиль.

VP-12P подойдет для организаций с высокими требованиями к качеству передаваемой голосовой информации, надежности и удобству использования.

1.2 Характеристика устройства

Интерфейсы:

- LAN: 1 порт Ethernet RJ-45 10/100BASE-T;
- PC: 1 порт Ethernet RJ-45 10/100BASE-T;
- Headset: 1 разъем для подключения гарнитуры.

Питание шлюза осуществляется через внешний адаптер 5 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 LAN, DHCP-сервер на стороне PC);
 - поддержка DNS;
 - поддержка NAT;
 - сетевой экран;
 - поддержка NTP;
 - поддержка механизмов качества обслуживания QoS (QoS по DSCP и 802.1P);
- 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);
- 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 on Busy;
 - переадресация по неответу – Call Forward on No response;
 - безусловная переадресация – Call Forward Unconditional;
 - не беспокоить – DND;
 - горячая линия – Hotline;

- трехсторонняя конференция;
- гибкий план нумерации;
- обновление ПО через web-интерфейс;
- поддержка DHCP-based autoprovisioning;
- TR-069;
- удаленный мониторинг, конфигурирование и настройка: Web-интерфейс, Telnet.

На рисунке 1.1 приведена схема включения VP-12(P).

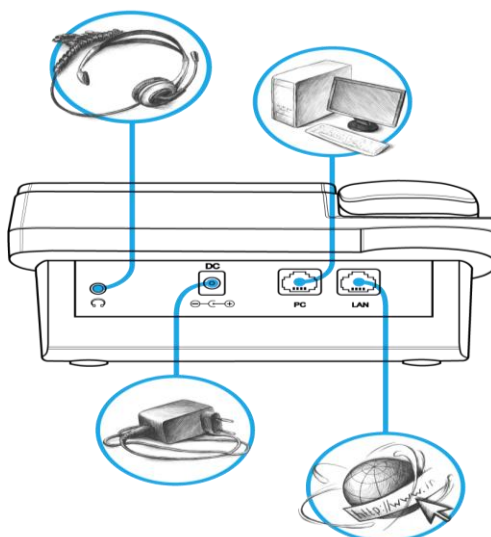


Рисунок 1– Функциональная схема использования VP-12(P)

1.3 Структура и принцип работы изделия

Структура и принцип работы изделия IP-телефон VP-12(P) состоит из следующих подсистем:

- контроллер, в состав которого входит:
 - высокоинтегрированная система на кристалле (System-on-a-Chip – SoC) Realtek RTL8972C, включающая в себя процессор, 100-мбитный коммутатор со встроенными PHY, аппаратную акселерацию трафика L2/L3/L4;
 - flash-память – 16MB;
 - оперативная память SDRAM – 128MB;
 - 1 кодек (ADC/DAC);
- 1 порт LAN: RJ-45 10/100BASE-T;
- 1 порт PC: RJ-45 10/100BASE-T.

Структурная схема устройства приведена на рисунке 1.2.

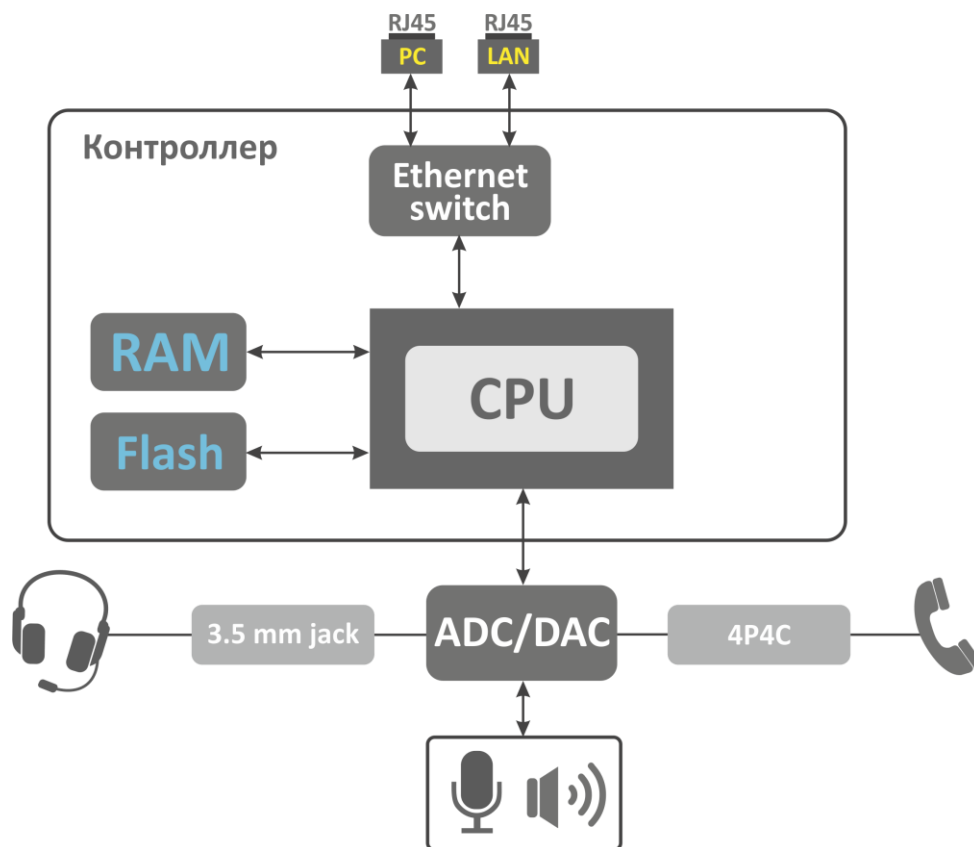


Рисунок 2 – Структурная схема VP-12(P)

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

1.4 Основные технические параметры

Основные технические параметры устройства приведены в таблице 1.

Таблица 1 – Основные технические параметры

Протоколы VoIP

Поддерживаемые протоколы	SIP
--------------------------	-----

Аудиокодеки

Кодеки	G.729, annex A, annex B G.711a, G.711u, G.723.1, G.726-24, G.726-32
--------	---

Параметры LAN-интерфейса Ethernet

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

Параметры PC-интерфейса Ethernet

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

Управление

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

Общие параметры

Питание	адаптер питания 5V DC, 2 А.
Потребляемая мощность	не более 6 Вт (максимальный потребляемый ток 1 А)
Рабочий диапазон температур	от +5 до +40°С
Относительная влажность при температуре 25°С	до 80%
Габариты	180x110x225 мм
Масса	не более 0,15 кг.

1.5 Конструктивное исполнение

IP-телефон *VP-12(P)* выполнен в пластиковом корпусе размерами 180x110x225 мм

1.5.1 Верхняя панель устройства

Внешний вид верхней панели устройства *VP-12(P)* приведен на рисунке 1.3.

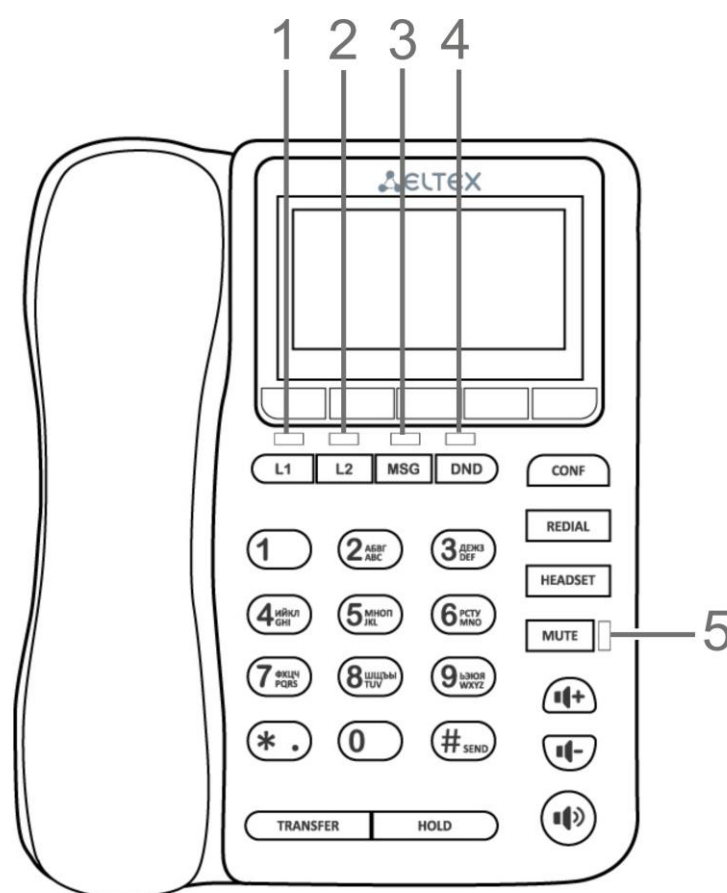


Рисунок 3 – Внешний вид верхней панели *VP-12(P)*

На верхней панели устройства *VP-12(P)* расположены следующие световые индикаторы:

Таблица 2 – Описание индикаторов и органов управления передней панели

Элемент передней панели		Описание
1	L1	Индикатор состояния первой линии
2	L2	Индикатор состояния второй линии
3	MSG	Индикатор наличия сообщений в голосовой почте
4	DND	Индикатор состояния услуги DND
5	MUTE	Индикатор отключенного микрофона

1.5.2 Задняя панель устройства

Внешний вид задней панели устройства *VP-12(P)* приведен на рисунке 1.4.

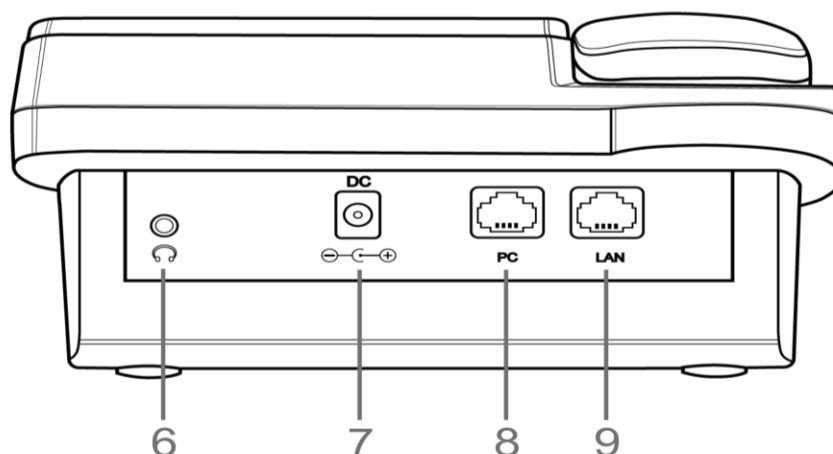


Рисунок 4 – Внешний вид задней панели *VP-12(P)*

На задней панели устройства *VP-12(P)* расположены следующие разъемы и органы управления, таблица 3.

Таблица 3 – Описание индикаторов и органов управления задней панели *VP-12(P)*

Элемент задней панели		Описание
6	Headset	Разъем 3.5 mm для подключения гарнитуры
7	DC	разъем для подключения адаптера питания, 5V 2A
8	PC	порт 10/100BASE-T Ethernet (разъем RJ-45) для подключения ПК
9	LAN	порт 10/100BASE-T Ethernet (разъем RJ-45) для подключения к локальной сети

1.5.3 Световая индикация

Текущее состояние устройства *VP-12(P)* отображается при помощи индикаторов L1, L2, MSG, DND, MUTE – расположенных на верхней панели, а также при помощи графического дисплея. Перечень состояний индикаторов приведен в таблице 4.

Таблица 4 – Световая индикация состояния устройства серии VP-12(P)

Индикатор	Состояние индикатора	Состояние устройства
L1, L2	не горит	Аккаунт зарегистрирован и находится в режиме ожидания входящего/исходящего вызова.
	горит зеленым	Аккаунт активен и находится в режиме разговора или набора номера.
	мигает зеленым (в режиме ожидания)	Аккаунт в процессе регистрации
	мигает зеленым во время разговора	Второй входящий вызов, входящий вызов на второй линии, один или более вызовов на удержании
	мигает зеленым во время входящего вызова	Входящий вызов
	горит красным	Ошибка регистрации
	горит оранжевым	Аккаунт находится в режиме DND (не беспокоить)
DND	горит красным	Как минимум на одном аккаунте активирован режим DND
	не горит	Режим DND не активирован
Mute	горит зеленым	Активирован режим mute для текущего разговора
	не горит	Режим mute не активирован

1.5.4 Индикация состояния на графическом дисплее

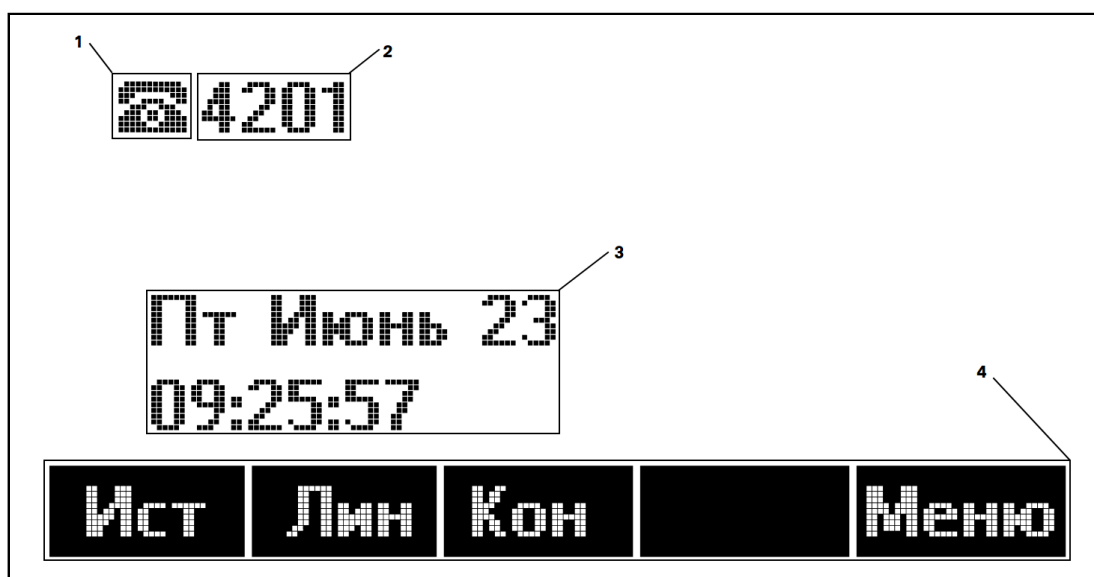





Рисунок 5 - Индикация состояния на графическом дисплее

1 Индикатор положения тел. Трубки / состояния спикерфона:

-  - телефонная трубка поднята;
-  - телефонная трубка положена;
-  - спикерфон активирован.

2 Телефонный номер текущего аккаунта

3 Текущее время и дата

4 Действия выполняемые при нажатии софт-клавиш

1.5.5 Сброс к заводским настройкам

Для запуска устройства с заводскими настройками необходимо в загруженном состоянии при помощи экранного выполнить сброс настроек:

Меню -> 3. Настройки -> 2. Система -> 3. Сброс настроек -> Да

Произойдет автоматическая перезагрузка устройства.

При заводских установках устройство работает в режиме моста с автоматическим получением IP адреса от DHCP сервера; имя пользователя/пароль для доступа через web-интерфейс: admin/password.

1.6 Комплект поставки

В базовый комплект поставки устройства серии *VP-12(P)* входят:

- Терминал абонентский универсальный;
- Адаптер питания 220/5В 2А;
- Кабель RJ-45;
- Краткое руководство пользователя.

2 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

2.1 Начало работы

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

1. Откройте Web-браузер, например, Firefox, Опера, Chrome.
2. Введите в адресной строке браузера IP-адрес устройства.



По умолчанию IP-телефон получает IP-адрес и другие параметры сети по протоколу DHCP.

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



Рисунок 6 - Окно аутентификации для входа в web-интерфейс



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

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

Нажмите кнопку «Войти». В окне браузера откроется панель мониторинга.

2.2 Режимы работы WEB-интерфейса

WEB-интерфейс устройства VP-12(P) может работать в двух режимах:

- **Настройки** – режим конфигурирования системы (режим полного конфигурирования) – позволяет выполнить полное конфигурирование устройства. Данному режиму соответствуют три вкладки «Сеть», «IP-телефония» и «Система»;
- **Мониторинг** – режим мониторинга системы – используется для просмотра различного рода информации, которая касается работы устройства: активность Интернет-соединения, состояние телефонного порта, объем принятых/переданных данных по сетевым интерфейсам и так далее. Режиму мониторинга соответствует одноименная вкладка «Мониторинг»

2.3 Применение конфигурации и отмена изменений

2.3.1 Применение конфигурации

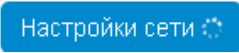



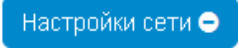



По нажатию на кнопку «Применить» происходит сохранение конфигурации во flash-память устройства и применение новых настроек. Все настройки вступают в силу без перезагрузки устройства.

Кнопка «Применить» имеет вид: .

В WEB-интерфейсе реализована визуальная индикация текущего состояния процесса применения настроек:

Таблица 5 – 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, то после нажатия на кнопку «Применить» появится соответствующее сообщение с указанием причины, а в названии вкладки отобразится значок  .

2.3.2 Отмена изменений



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

Кнопка отмены изменений имеет вид: .

2.4 Расширенные настройки

Для перехода в режим конфигурирования устройства перейдите на одну из трех вкладок «Сеть», «IP-телефония» или «Система» в зависимости от цели конфигурирования.

2.4.1 Основные элементы WEB-интерфейса

На рисунке 2.2 представлены элементы навигации WEB-конфигуратора в режиме расширенных настроек.

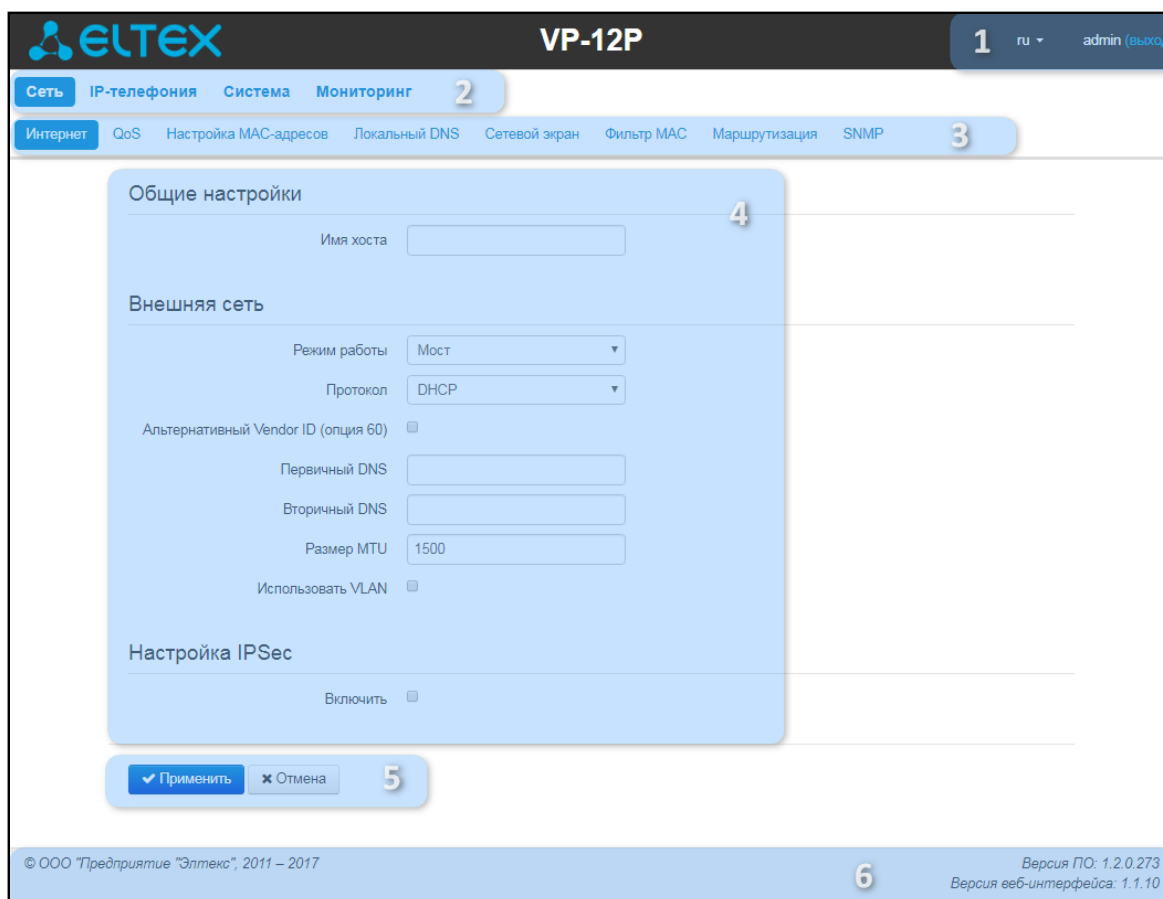


Рисунок 7 – Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса разделено на семь областей:

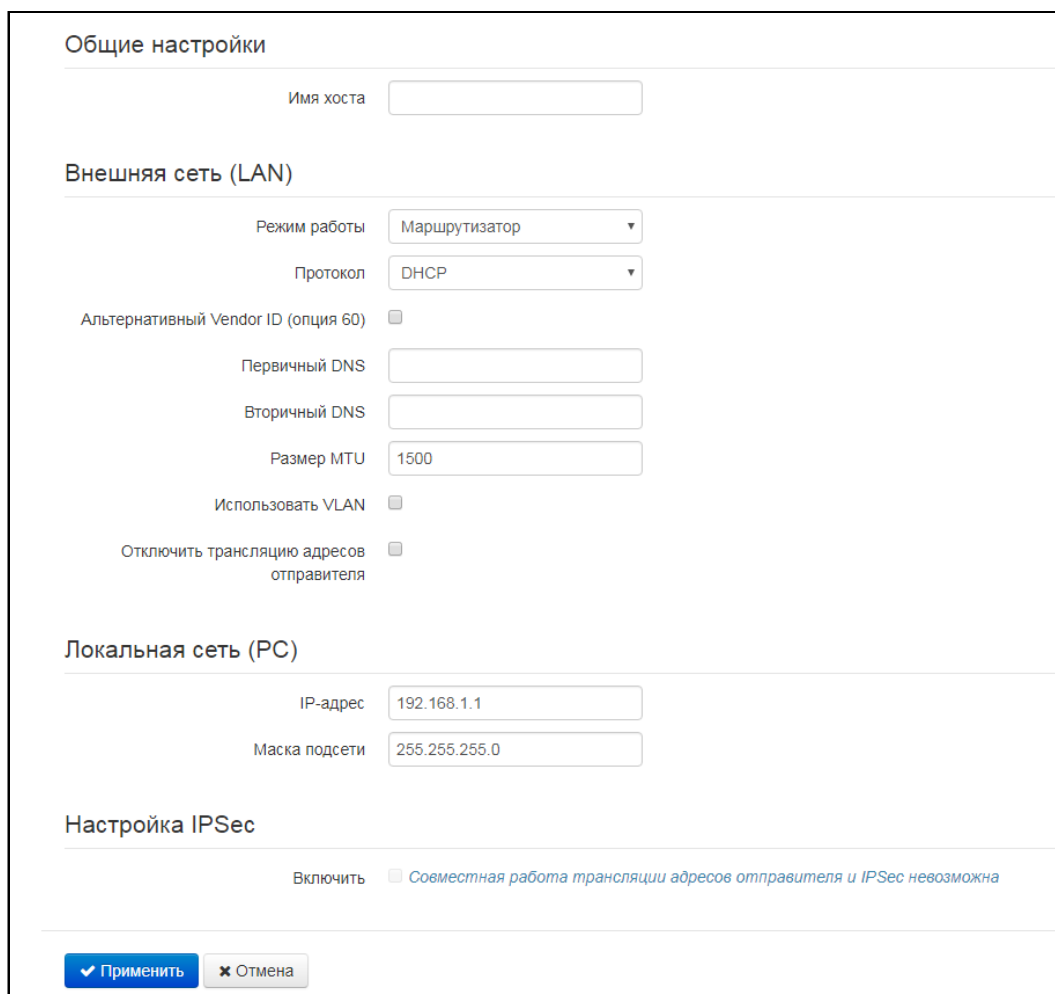
- 1 Имя пользователя, под которым был осуществлен вход в систему, кнопка завершения сеанса работы в WEB-интерфейсе (*выход*) под данным пользователем и выпадающее меню выбора языка web-интерфейса.
- 2 Вкладки меню группируют вкладки подменю по категориям: **Сеть**, **IP-телефония**, **Система**, **Мониторинг**.
- 3 Вкладки подменю служат для управления полем настроек.2.2
- 4 Поле настроек устройства, которое базируется на выборе пользователя, предназначено для просмотра настроек устройства и ввода конфигурационных данных.
- 5 Кнопки управления конфигурацией, подробная информация приведена в разделе 2.3.
 - *Применить* – применить и сохранить текущую конфигурацию в энергонезависимую память устройства;
 - *Отмена* – отмена изменений (возможна только до нажатия на кнопку «*Применить*»).
- 6 Информационное поле, в котором отображается версия программного обеспечения, версия WEB-интерфейса.

2.4.2 Меню «Сеть»

В меню «Сеть» выполняется конфигурирование сетевых настроек устройства.

2.4.2.1 Подменю «Интернет»

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



Общие настройки

Имя хоста

Внешняя сеть (LAN)

Режим работы

Протокол

Альтернативный Vendor ID (опция 60)

Первичный DNS

Вторичный DNS

Размер MTU

Использовать VLAN

Отключить трансляцию адресов отправителя

Локальная сеть (PC)

IP-адрес

Маска подсети

Настройка IPSec

Включить Совместная работа трансляции адресов отправителя и IPSec невозможна

Рисунок 8 - Подменю «Интернет»

Общие настройки

- Имя хоста – сетевое имя устройства.

Внешняя сеть

- Режим работы – режим работы устройства:
 - *Маршрутизатор* – между LAN- и PC-интерфейсами устанавливается режим маршрутизатора (PC изолирован от LAN);
 - *Мост* – между PC и LAN-интерфейсами устанавливается режим моста: данные передаются прозрачно из LAN в PC 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 LAN-интерфейса устройства к сети предоставления услуг провайдера:

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

Поддерживаемые опции:

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

Для протокола DHCP имеется возможность задать необходимое значение 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:VP-12(P)][HW:1.0][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:DO][LAN:02:20:80:a8:f9:4b][VERSION:#1.1.0]
 - *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 LAN-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, Шлюз*;

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

- *PPTP* – режим, при котором на LAN-интерфейсе поднимается 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 локальным сетевым ресурсам и PPTP-серверу. Можно выбрать 2 варианта:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;

Static – статический, в этом случае необходимые для доступа к PPTP-серверу параметры задаются вручную:

- *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
- *Маска подсети* – при статическом доступе маска подсети;
- *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
- *Шлюз* – при статическом доступе шлюз для доступа к PPTP-серверу (если необходим).
- *Использовать второй доступ для VoIP* – опция доступна, если для сервиса IP-телефонии не настроен выделенный интерфейс (установлен флаг «Использовать настройки Internet»). При снятом флаге (по умолчанию) сервис IP-телефонии

использует для своей работы интерфейс PPP, при установленном – интерфейс второго доступа (IPoE).

Аппаратное ускорение трафика работает только для интерфейса второго доступа (IPoE - IP over Ethernet).

– *L2TP* – режим, при котором на LAN-интерфейсе поднимается 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 локальным сетевым ресурсам и L2TP-серверу. Можно выбрать 2 варианта:

DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;

Static – статический, в этом случае необходимые для доступа к L2TP-серверу параметры задаются вручную:

- *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
- *Маска подсети* – при статическом доступе маска подсети;
- *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
- *Шлюз* – при статическом доступе шлюз для доступа к L2TP-серверу (если необходим);
- *Использовать второй доступ для VoIP* – опция доступна, если для сервиса IP-телефонии не настроен выделенный интерфейс (установлен флаг «*Использовать настройки Internet*»). При снятом флаге (по умолчанию) сервис IP-телефонии использует для своей работы интерфейс PPP, при установленном – интерфейс второго доступа (IPoE).

Аппаратное ускорение трафика работает только для интерфейса второго доступа (IPoE - IP over Ethernet).

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 IPsec¹ предлагает больше уровней безопасности, чем PPTP, и гарантирует высокую степень безопасности важных для организации данных.

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

¹ Для корректной работы IPsec следует отключить трансляцию адресов отправителя.

- *Использовать VLAN во внешней сети* – при установленном флаге использовать идентификатор VLAN, указанный в поле «VLAN ID».
 - *VLAN ID* – идентификатор VLAN, используемый для данной услуги;
 - *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).

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

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

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

- *Протокол* – выбор протокола, по которому будет осуществляться подключение LAN-интерфейса устройства к сети предоставления услуг провайдера:

- *Static* – режим работы, при котором IP-адрес и все необходимые параметры на LAN-интерфейсе назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:

- *IP-адрес* – установка IP-адреса LAN-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:VP-12P][HW:1.0][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.1.0]

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

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 (Сеть – DHCP-сервер).

Настройка IPSec:

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

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

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

Настройка IPSec

Включить

Интерфейс

Локальный IP-адрес

Адрес локальной подсети

Маска локальной подсети

Адрес удаленной подсети

Маска удаленной подсети

Удаленный шлюз

Режим NAT-T

Агрессивный режим

Тип идентификатора

Идентификатор

Фаза 1

Заранее заданный ключ

Алгоритм аутентификации

Алгоритм шифрования

Группа Диффи-Хеллмана

Время жизни фазы 1, сек

Фаза 2

Алгоритм аутентификации

Алгоритм шифрования

Группа Диффи-Хеллмана

Время жизни фазы 2, сек

Рисунок 9 - Настройка IPSec

- *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*».



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

2.4.2.2 Подменю «QoS»

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

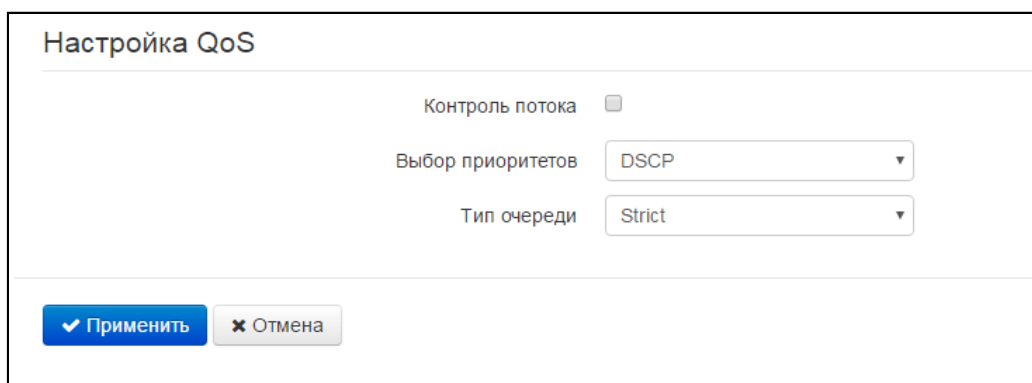


Рисунок 10 - Настройка QoS

Настройка QoS

- *Контроль потока* – включение/выключение механизма управления потоком передачи данных по протоколу TCP;

- **Выбор приоритетов** – выбор способа приоритезации трафика:
 - *DSCP* – механизм классификации, управления трафиком и обеспечения качества обслуживания посредством приоритетов;
 - *802.1p* – признак (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).



При включенном контроле потока настройки приоритетов недоступны.

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

2.4.2.3 Подменю «Настройка MAC-адресов»

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

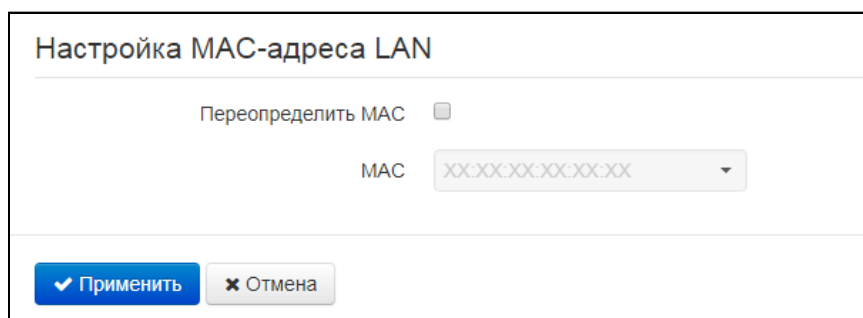


Рисунок 11 - Подменю «Настройка MAC-адресов»

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

При нажатии на кнопку выпадающего меню в поле «*MAC*» возможно записать MAC-адрес компьютера, с которого Вы подключены к WEB-конфигуратору. Эта функция будет полезна, если на сети вашего Интернет-провайдера используется привязка по MAC-адресу. В этом случае, если Вам необходимо использовать устройство *VP-12(P)* в качестве маршрутизатора, на LAN-интерфейсе устройства необходимо назначить MAC-адрес Вашего компьютера (который ранее был подключен к сети Интернет).

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

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

2.4.2.4 Подменю «DHCP-сервер»

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

Устройство VP-12(P) 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 PC-интерфейсу. Его использование позволяет избежать ограничений ручной настройки протокола TCP/IP. DHCP-сервер доступен для конфигурирования, только если сервис Интернет настроен в режиме маршрутизатора.




Рисунок 12 - Подменю «DHCP-сервер»

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 PC – 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:

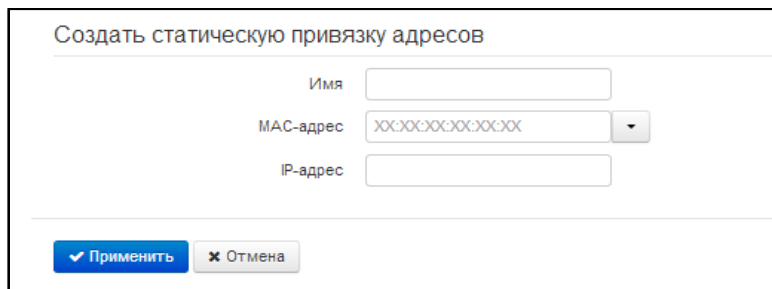


Рисунок 13 - Создание статической привязки адреса

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

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

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

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

2.4.2.5 Подменю «Локальный DNS»

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

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



Доменное имя	IP-адрес
<input type="checkbox"/> test.ru	192.168.12.12

Рисунок 14 - Создание статической привязки адреса

Настройка узлов

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

Рисунок 15 - Настройка узлов

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

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

2.4.2.6 Подменю «NAT и проброс портов»

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

NAT – (Network Address Translation) режим трансляции сетевых адресов – позволяет преобразовывать IP-адреса и сетевые порты IP-пакетов. Проброс сетевых портов необходим, когда TCP/UDP-соединение с локальным (подключенным к PC-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.

Имя	PC IP	Порты PC	Протокол	LAN IP	Порты LAN
+ Добавить Удалить					

Рисунок 16 - Подменю «NAT и проброс портов»

Настройка правила NAT

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

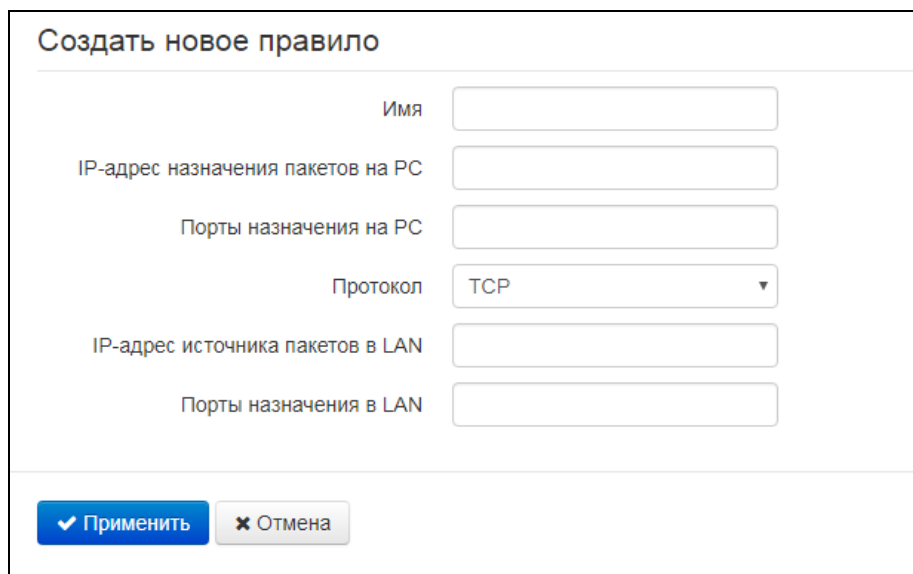


Рисунок 17 - Настройки правила NAT

- *Имя* – название правила (поле обязательно для заполнения);
- *IP-адрес назначения пакетов на PC* – IP-адрес хоста подключенного к порту PC, на который осуществляется трансляция пакетов, попадающих под данное правило;
- *Порты назначения на PC* – значения TCP/UDP-портов получателя подключенного к порту PC, на которые будут транслироваться пакеты (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 в LAN* – IP-адрес отправителя пакета во внешней сети, попадающего под данное правило;
- *Порты назначения в LAN* – значения TCP/UDP-портов 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 LAN-интерфейса устройства по протоколу «Протокол» на порт из диапазона «Порты назначения в LAN» и имеющего адрес источника «IP-адрес источника пакетов в LAN» (если это параметр оставить пустым – адрес источника не анализируется), осуществляется подмена адреса и порта назначений на значения соответственно из полей «IP-адрес назначения пакетов на PC» и «Порты назначения на PC».

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

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

2.4.2.7 Подменю «Сетевой экран»

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

Правила для входящего трафика						
Имя	Протокол	Адрес отправителя	Порты отправителя	Порты получателя	Действие	
Правила для исходящего трафика						
Имя	Протокол	Порты отправителя	Адрес получателя	Порты получателя	Действие	
Правила для транзитного трафика						
Имя	Протокол	Адрес отправителя	Порты отправителя	Адрес получателя	Порты получателя	Действие

Рисунок 18 - Подменю «Сетевой экран»

Настройка правил сетевого экрана

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

Создать новое правило

Имя	<input type="text"/>
Тип трафика	<input type="text" value="Входящий"/>
Протокол	<input type="text" value="TCP"/>
Адрес отправителя	<input type="text"/>
Порты отправителя	<input type="text" value="0"/>
Порты получателя	<input type="text" value="0"/>
Действие	<input type="text" value="Пропустить"/>

Рисунок 19 - Создание правила для сетевого экрана

- *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);
- *Порты получателя* – список портов получателя, пакеты которого будут попадать под данное правило (допускается указывать либо одиночный порт, либо через “-” диапазон портов).
- При выборе протокола ICMP для редактирования будут доступны настройки:
- *Тип сообщения* – можно создать правило только для определенного типа ICMP-сообщения либо для всех.

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

2.4.2.8 Подменю «Фильтр MAC»

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

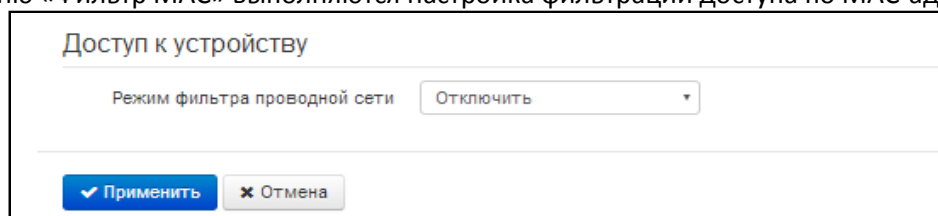


Рисунок 20 - Подменю «Фильтр MAC»

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

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

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

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

2.4.2.9 Подменю «Маршрутизация»

В подменю «Маршрутизация» настраиваются статические маршруты устройства.

Имя	Адрес назначения	Маска подсети	Шлюз
<input type="checkbox"/> route1	192.168.23.0	255.255.255.0	192.168.0.254

Buttons: + Добавить, x Удалить

Рисунок 21 - Подменю «Маршрутизация»

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

Добавить маршрут

Имя:

Адрес назначения:

Маска подсети:

Шлюз:

Buttons: ✓ Применить, x Отмена

Рисунок 22 - Добавление нового маршрута

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

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

2.4.2.10 Подменю «SNMP»

Программное обеспечение *VP-12(P)* позволяет проводить мониторинг состояния устройства и его конфигурирование, используя протокол SNMP. В подменю «SNMP» выполняются настройки параметров SNMP-агента. Устройство поддерживает протоколы версий SNMPv1, SNMPv2c.



Рисунок 23 - Подменю «SNMP»

- *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).

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

2.4.3 Меню «IP-телефония»

В меню «IP-телефония» выполняются настройки VoIP (Voice over IP): настройка протокола SIP, конфигурация аккаунтов, установка кодеков, ДВО и плана нумерации.

2.4.3.1 Подменю «Настройки сети»

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

Рисунок 24 - Подменю «Настройки сети»

- *Использовать настройки Internet* – при установленном флаге использовать настройки сети, установленные в меню «Сеть» -> «Интернет», иначе – настройки, установленные в текущем меню;
- *Использовать VLAN²* – при установленном флаге сервис IP-телефонии будет использовать для своей работы выделенный интерфейс в отдельной VLAN, номер которой указан в поле «VLAN ID» .
- *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).
- *Протокол* – выбор протокола назначения адреса на интерфейс услуги VoIP:
 - *Static* – режим работы, при котором IP-адрес и все необходимые настройки на LAN-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;
 - *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-

² В версии ПО 1.9.1 разрешается задавать индивидуальные сетевые настройки услуги VoIP только в выделенной VLAN.

сервера, сервера регистрации), будут получены от DHCP-сервера автоматически. Если от провайдера не удастся 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:VP-12P][HW:1.0][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]
```

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

Настройка IPSec:

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

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

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

Подробное описание настроек *IPSec* приведено в разделе 2.4.2.1 в графе Настройка IPSec.

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

2.4.3.2 Подменю «SIP аккаунты»

Выбрать аккаунт для редактирования можно в выпадающем меню «аккаунт».

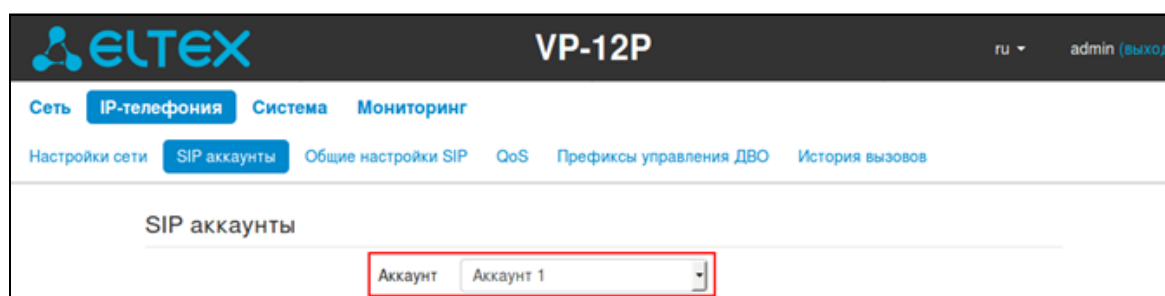


Рисунок 25 - Подменю «SIP аккаунты»

За каждым аккаунтом можно назначить собственные адреса SIP-сервера и сервера регистрации, голосовые кодеки, индивидуальный план нумерации и другие параметры.

Вкладка основные настройки:

Рисунок 26 - Вкладка «Основные настройки»

- *Включить* – при установленном флаге аккаунт активен;
- *Номер телефона* – абонентский номер, закрепленный за аккаунтом;
- *Имя пользователя* – имя пользователя, сопоставленное с аккаунтом (отображается в поле DisplayName заголовка From в исходящих сообщениях SIP);
- *Использовать альтернативный номер* – при установленном флаге в заголовок «From» сообщений SIP, отправляемых с данного аккаунта, будет подставляться альтернативный номер (в частности, чтобы маскировать свой реальный номер от системы АОН вызываемого абонента);
- *Подставлять заголовок в Contact* – альтернативный номер, присвоенный телефонному порту, будет заменен на указанный номер в заголовке Contact сообщения SIP;
- *SIP порт* – UDP-порт для приёма входящих сообщений SIP на данный аккаунт, а также для отправки исходящих SIP-сообщений с данного аккаунта. Принимает значения 1-65535 (по умолчанию 5060);
- *Категория абонента* – категория вызывающего абонента (calling party category) – используется для передачи в заголовке «From» исходящих сообщений; последний при этом передается в формате Tel-URI (см. RFC3966);

Аутентификация

Рисунок 27 - Аутентификация

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

Параметры SIP

В секции «Параметры SIP» выполняются настройки SIP-параметров аккаунта.

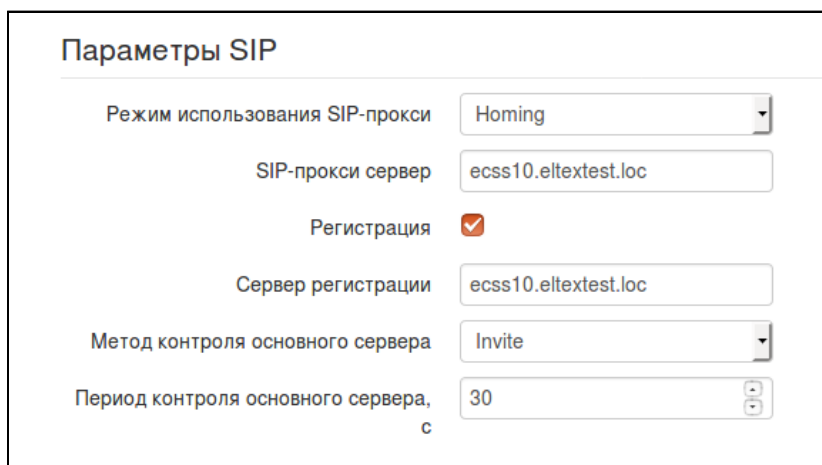


Рисунок 28 - Параметры SIP

- *Режим использования SIP-прокси* – в ниспадающем списке можно выбрать режим работы с SIP-сервером:
 - Не использовать;
 - Parking – режим резервирования SIP-прокси без контроля основного SIP-прокси;
 - Homing – режим резервирования SIP-прокси с контролем основного SIP-прокси.

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

При наличии резервных SIP-прокси работа в режимах *Parking* и *Homing* осуществляется следующим образом. При совершении исходящего вызова телефон отправляет сообщение INVITE на адрес основного SIP-прокси или при попытке регистрации – сообщение REGISTER. В случае если по истечении времени *Invite total timeout* от основного SIP-прокси не приходит ответ либо приходит ответ 408 или 503 – телефон 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:

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

В режиме homing доступно три вида контроля основного SIP-прокси: посредством периодической передачи на его адрес сообщений OPTIONS, посредством периодической передачи на его адрес сообщений REGISTER либо посредством передачи запроса INVITE при совершении исходящего вызова. Запрос INVITE сначала передается на основной SIP-прокси, а

затем, в случае его недоступности, на текущий резервный и т.д. Независимо от вида контроля, если обнаружено, что основной SIP-прокси восстановился – происходит перерегистрация на нем. Телефон 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 аккаунт, 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;
1. *Период контроля основного сервера* – интервал отправки периодических сообщений в секундах с целью проверки доступности основного SIP-сервера.

Резервные SIP-прокси

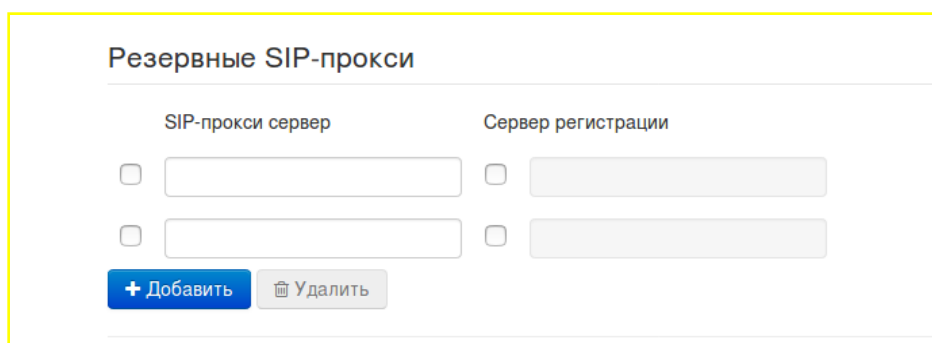


Рисунок 29 - Резервные SIP-прокси

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»

Дополнительные параметры SIP

Дополнительные параметры SIP

SIP-домен	<input type="text" value="eltextest.loc"/>
Применить SIP Domain для регистрации	<input checked="" type="checkbox"/>
Режим Outbound	<input type="text" value="Выключен"/>
Период времени перерегистрации	<input type="text" value="1800"/>
Интервал повтора регистрации	<input type="text" value="30"/>
Публичный адрес	<input type="text"/>
Использовать SIP Display Name при регистрации	<input type="checkbox"/>
Выдача КПВ при получении 183 Progress	<input type="checkbox"/>
Вызов абонента	<input type="text" value="180 Ringing"/>
100rel	<input type="text" value="Supported"/>
Разрешить Timer	<input checked="" type="checkbox"/>
Минимальное время сессии, с	<input type="text" value="120"/>
Время сессии, с	<input type="text" value="1800"/>
Периодический опрос SIP-сервера	<input type="text" value="Отключен"/>
Обрабатывать заголовок Alert-Info	<input type="checkbox"/>
Проверять только имя пользователя в RURI	<input type="checkbox"/>
Передавать IP-адрес в заголовке Call-ID	<input type="checkbox"/>

Рисунок 30 - Дополнительные параметры SIP

- *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.
1. *Период времени перерегистрации* – время, в течение которого действительна регистрация абонентского порта на SIP-сервере. Перерегистрация порта осуществляется в среднем через 2/3 указанного периода;
 2. *Интервал повтора регистрации* – промежуток времени между попытками зарегистрироваться на SIP-сервере в случае неуспешной регистрации;

3. *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 VP-12(P). При этом на самом шлюзе (NAT) необходимо сделать проброс соответствующих SIP- и RTP-портов, используемых устройством;
4. *Использовать SIP Display Name при регистрации* – при установленном флаге передавать имя пользователя в поле SIP Display Info сообщения Register;
5. *Выдача «КПВ» при получении 183 Progress* – при установленном флаге выдавать сигнал «Контроль посылки вызова» при приеме сообщения «183 Progress» (без вложенного SDP);
6. *Вызов абонента* – предварительный ответ, который отправляется устройством вызываемому оборудованию при входящем звонке:
 - *180 Ringing* – вызываемому оборудованию отправляется ответ 180; получив это сообщение, вызываемое оборудование должно выдать в линию локальный сигнал КПВ;
 - *183 Progress with SDP* – вызываемому оборудованию отправляется ответ 183+SDP – используется для проключения разговорного тракта до ответа вызываемого. В данном случае VP-12(P) будет удалено выдавать вызываемому абоненту сигнал КПВ.
7. *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 обе стороны поддерживают метод UPDATE, для чего он должен быть указан в заголовке Allow – обновление сессии осуществляется посредством периодической отправки сообщений UPDATE);
- *Минимальное время сессии, с* – минимальный интервал проверки работоспособности соединения (от 90 до 1800 с, по умолчанию 120 с.);
- *Время сессии, с* – период времени в секундах, по истечении которого произойдет принудительное завершение сессии, в случае если сессия не будет вовремя обновлена (от 90 до 80000 с., рекомендуемое значение - 1800 с, 0 – время сессии не ограничено);
- *Периодический опрос SIP-сервера* – выбор способа опроса SIP-сервера:
 - *Отключен* – SIP-сервер не опрашивается;
 - *Options* – опрос SIP-сервера при помощи сообщений OPTIONS;
 - *Notify* – опрос SIP-сервера при помощи сообщений NOTIFY;
 - *CLRF* – опрос SIP-сервера пустым UDP-пакетом;
- 1. *Интервал опроса* – период времени в секундах, через который выполняется опрос SIP-сервера;
- 2. *Обрабатывать заголовок Alert-Info* – обрабатывать заголовок Alert-Info в запросе INVITE для выдачи на абонентский порт отличной от стандартной посылки вызова;
- 3. *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.
- 4. *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.

Вкладка «Кодеки»

Основные настройки
Кодеки
Настройки сервисов
Дополнительные параметры
План нумерации

Приоритет кодеков

Кодек 1	<input type="text" value="G.711a"/>
Кодек 2	<input type="text" value="G.729"/>
Кодек 3	<input type="text" value="G.711u"/>
Кодек 4	<input type="text" value="G.723"/>
Кодек 5	<input type="text" value="G.726-24"/>
Кодек 6	<input type="text" value="G.726-32"/>
Кодек 7	<input type="text" value="G.722"/>

Время пакетизации

Время пакетизации G.711, мс	<input type="text" value="20"/>
Время пакетизации G.729, мс	<input type="text" value="20"/>
Время пакетизации G.723, мс	<input type="text" value="30"/>
Время пакетизации G.726-24, мс	<input type="text" value="20"/>
Время пакетизации G.726-32, мс	<input type="text" value="20"/>

Тип нагрузки

Тип нагрузки G.726-24	<input type="text" value="103"/>
Тип нагрузки G.726-32	<input type="text" value="104"/>

Рисунок 31 - Вкладка «Кодеки»

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

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

- 2. *Тип нагрузки* - тип динамической нагрузки для кодека G.726-24 или G.726-32 (разрешенные для использования значения – от 96 до 127).

Вкладка настройка сервисов

Рисунок 32 - Вкладка настройка сервисов

- *Не беспокоить* – при установленном флаге устанавливается временный запрет входящей связи (услуга DND – Don't Disturb).
 - *Остановка набора при #* – при установленном флаге использовать кнопку '#' на телефонном аппарате для окончания набора, иначе '#' набранная с телефонного аппарата, используется как часть номера;
 - *CLIR* – ограничение идентификации номера вызывающего абонента
 - *Выкл* – услуга CLIR отключена;
 - *SIP:From* – в заголовке From сообщений протокола SIP будет передаваться *Anonymous sip:anonymous@unknown.host*
 - *SIP:From* и *SIP:Contact* – в заголовках *From* и *Contact* сообщений протокола SIP будет передаваться *Anonymous sip:anonymous@unknown.host*
1. *Горячая/теплая линия* – при установленном флаге разрешена услуга «горячая/теплая линия». Услуга позволяет автоматически установить исходящее соединение при подъеме 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;

Блок параметров «Переадресация»

Рисунок 33 - Блок параметров «Переадресация»

- **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);
- 1. **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);
- 2. **Переадресация по неответу** – при установленном флаге разрешена услуга CFNA (Call Forward at No Answer) – переадресация вызова при неответе абонента. При установленном флаге заполните следующие поля:
 - *Номер переадресации по неответу* – номер, на который перенаправляются входящие вызовы при неответе абонента при включенной услуге «Переадресация по неответу» (в плане нумерации используемого SIP-профиля должен быть префикс на данное направление);
 - *Таймаут неответа, с* – интервал времени, через который будет производиться переадресация вызова в случае неответа абонента, в секундах;

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

- CFU;
- DND;
- CFB, CFNA.

Трехсторонняя конференция

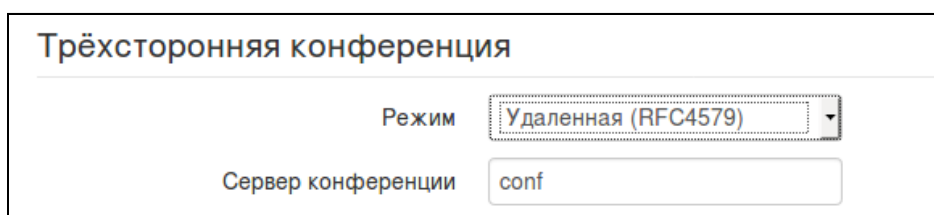


Рисунок 34 - Трехсторонняя конференция

- **Режим** – режим работы трехсторонней конференции. Возможно два режима:
 - *Локальная* – конференция собирается локально устройством после нажатия комбинации «flash+3»;
 - *Удаленная (RFC4579)* – конференция собирается на удаленном сервере, для чего после нажатия «flash+3» на сервер отправляется сообщение Invite на номер, указанный в поле «Сервер конференции». В этом случае конференция работает по алгоритму, описанному в RFC4579.
- 1. **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.

Вкладка «Дополнительные параметры»

Основные настройки	Кодеки	Настройки сервисов	Дополнительные параметры	План нумерации
Тип нагрузки для пакетов RFC 2833			96	
Одинаковый тип нагрузки для приёма и передачи			<input type="checkbox"/>	
Использовать обнаружение тишины			<input checked="" type="checkbox"/>	
Использовать эхоподавление			<input checked="" type="checkbox"/>	
RTCP			<input checked="" type="checkbox"/>	
Передача DTMF			RFC 2833	
Интервал передачи			5	
Период приёма			5	
RTCP-XR			<input checked="" type="checkbox"/>	

Рисунок 35 - Вкладка «Дополнительные параметры»

- *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;
 - *Время дисперсии, мс* – параметр, позволяющий бороться с эхом, вызванным дисперсией речевого сигнала. Значения параметра изменяются в промежутке от 2 до 128 мс.
 - *Использовать RTCP* – при установленном флаге использовать протокол RTCP для контроля за разговорным каналом:
 - *Интервал передачи* – интервал передачи пакетов RTCP, сек;
 - *Период приёма* – период приёма сообщения RTCP измеряется в единицах интервала передачи; если по истечении периода приёма от встречной стороны не будет получено ни одного RTCP-пакета – устройство разрывает соединение.
1. *RTCP-XR* – при установленном флаге будут отправляться пакеты RTCP Extended Reports в соответствии с RFC 3611.
 2. *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.

Блок параметров «Джиттер-буфер»



Джиттер-буфер	
Минимальная задержка, мс	40
Максимальная задержка, мс	130
Порог немедленного удаления пакетов, мс	500
Фактор оптимизации буфера	7
Время дисперсии, мс	32

Рисунок 36 - Блок параметров «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;
- *Порог немедленного удаления пакетов, мс* – максимальный промежуток времени, через который происходит удаление речевых пакетов из буфера. Значение данного параметра больше или равно максимальной задержке;
- *Фактор оптимизации буфера* – параметр, используемый для оптимизации размера джиттер-буфера. Рекомендуется выставлять его значение в 0.

Блок настройки физических параметров

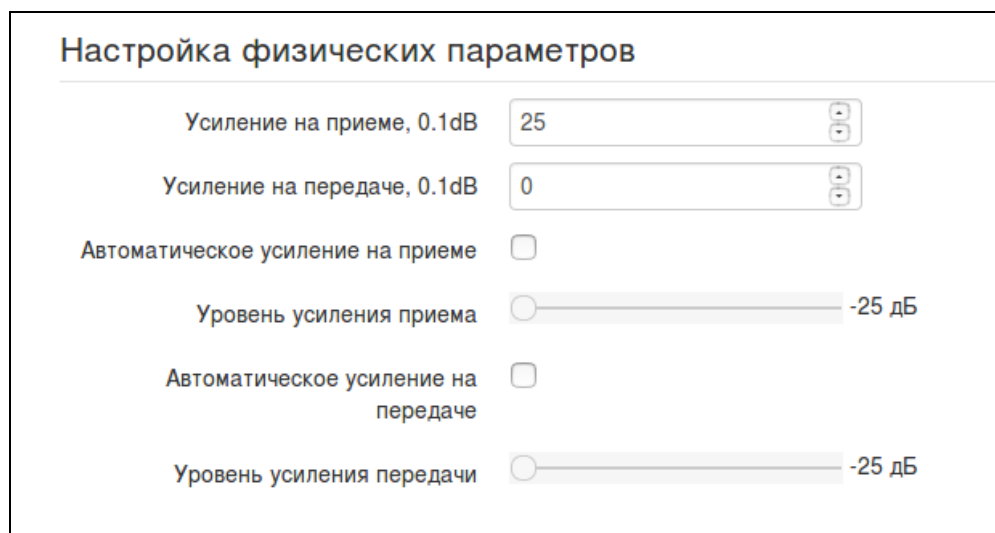


Рисунок 37 - Блок настройки физических параметров

- *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;
- *Автоматическое усиление на приёме* – если флаг установлен, то принимаемый сигнал будет усилен до заданного уровня (максимальное усиление сигнала +/- 15дБ), иначе – усиление производиться не будет;
- *Уровень усиления приёма* – определяет значение уровня, до которого будет усиливаться аналоговый сигнал при приеме (допустимы значения -25, -22, -19, -16, -13, -10, -7, -4, -1 дБ);
- *Автоматическое усиление на передаче* – если флаг установлен, то передаваемый сигнал будет усилен до заданного уровня (максимальное усиление сигнала +/- 15дБ), иначе – усиление производиться не будет;
- *Уровень усиления передачи* – определяет значение уровня, до которого будет усиливаться аналоговый сигнал при передаче (допустимы значения -25, -22, -19, -16, -13, -10, -7, -4, -1 дБ).

План нумерации

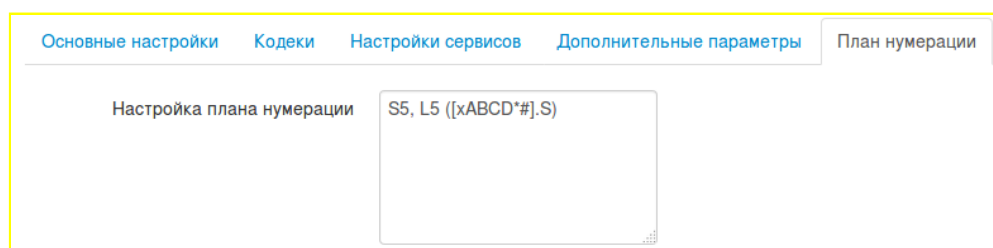


Рисунок 38 - Настройка плана нумерации

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

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

Структура регулярного выражения:

Sxx, Lxx (),

где

xx – произвольные значения таймеров S и L;

() – границы плана нумерации.

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

- Последовательность цифр, заключённая в квадратные скобки, соответствует любому из заключённых в скобки символу.
 - Пример: ([1239]) – соответствует любой из цифр 1, 2, 3 или 9.
- 1. 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.
- 2. Символ X соответствует любой цифре от 0 до 9.
 - Пример: (1XX) - любой трёхзначный номер, начинающийся на 1.
- 3. «.» - повторение предыдущего символа от 0 до бесконечности раз.
- 4. «+» - повторение предыдущего символа от 1 до бесконечности раз.
- 5. {a,b} – повторение предыдущего символа от a до b раз;
- 6. {a,} – повторение предыдущего символа не меньше a раз;
- 7. {,b} – повторение предыдущего символа не больше b раз.
 - Пример: (810X.) - международный номер с любым количеством цифр.

Настройки, влияющие на обработку плана нумерации:

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

Дополнительные возможности:

1. Замена набранной последовательности

Синтаксис: `<arg1:arg2>`

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

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

2. Вставка тона в набор

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

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

3. Запрет набора номера.

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

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

4. Замена значений таймеров набора номера

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

- Пример: S4 (8XXX.) или S4,L8 (XXX)

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

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

5. Набор по прямому адресу (IP Dialing)

Символ «@», поставленный после номера, означает, что далее будет указан адрес сервера, на который будет отправлен вызов на набранный номер. Рекомендуется использовать «*IP Dialing*», а также приём и передачу вызовов без регистрации («*Call Without Reg*», «*Answer Without Reg*»). Это может помочь в случае отказа сервера.

Кроме того, формат адреса с IP Dialing может быть использован в номерах, предназначенных для переадресации звонков.

- Пример 1: (8 xxx xxxxxxx) - 11-значный номер, начинающийся на 8.
- Пример 2: (8 xxx xxxxxxx | <:8495> xxxxxxx) - 11-значный номер, начинающийся на 8, если введён 7-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 план нумерации позволяет набрать любой номер, состоящий из цифр, а если ничего не введено в течение 5 секунд, вызвать номер 1000 (допустим, это секретарь).
- Пример 6: (*5x*xxx*x#|*2x*xxxxxxxxxx#|#xx#[2-7]xxxx|8, [2-9]xxxxxxxx|8, 10x.|1xx<:@10.110.60.51:5060>).
- Пример 7: (1xx|0[1-9]|00[1-8]|*5x*xxx*x#|*2x*xxxxxxxxxx#|#xx#[2-7]xxxx|8, [2-9]xxxxxxxx|8, 10x.).

Общие настройки профилей SIP

Рисунок 39 - Общие настройки 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.
 - *Таймер T1, мс* – интервал между посылкой первого INVITE и второго при отсутствии ответа на первый в мс, для последующих INVITE (третьего, четвертого и т.д.) данный интервал увеличивается вдвое (например, при значении 300 мс, второй INVITE будет передан через 300 мс, третий – через 600 мс, четвертый – через 1200 мс и т.д.);
 - *Таймер T2, мс* – максимальный интервал для перепосылки не-INVITE запросов и ответов на INVITE запросы;
 - *Таймер B, мс* – общий таймаут передачи сообщений INVITE в мс. По истечении данного таймаута определяется, что направление недоступно. Используется для ограничения ретрансляций сообщений INVITE, в том числе для определения доступности
- 1. *Транспорт* – выбор протокола для транспортировки сообщений протокола SIP
- 2. *Спецификация тонов* - выбор страны, для определения используемого набора тонов.

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

2.4.3.3 Подменю «QoS»

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

Настройка диапазона RTP-портов

Минимальный RTP-порт

Максимальный RTP-порт

Настройка DSCP для сигнализации (SIP)

SIP-порт	DSCP
<input type="button" value="+ Добавить"/>	<input type="button" value="Удалить"/>

Рисунок 40 - Подменю «QoS»

Настройка диапазона RTP-портов

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

Настройка DSCP для сигнализации (SIP)

Добавить

SIP-порт

DSCP

Рисунок 41 - Настройка правила QoS

Настройка правила QoS

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

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

2.4.3.4 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.

Префиксы управления ДВО			
Услуги ДВО	Код активации	Код деактивации	Код проверки статуса услуги
Безусловная переадресация	* <input type="text"/> #	-	-
Переадресация вызова по занятости	* <input type="text"/> #	-	-
Переадресация по неответу	* <input type="text"/> #	-	-
Разрешить перехват вызова на порт	* <input type="text"/> #	-	-
Горячая/теплая линия	* <input type="text"/> #	-	-
Ожидание вызова	* <input type="text"/> #	-	-
Не беспокоить	* <input type="text"/> #	-	-

Рисунок 42 - Префиксы управления ДВО

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.

1. *Код активации* – код для активации услуги;
2. *Код деактивации* – код для деактивации услуги;
3. *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*».

Меню «История вызовов»

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

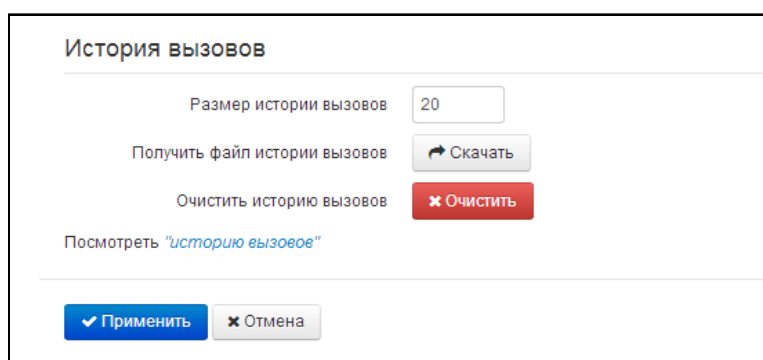


Рисунок 43 - Меню «История вызовов»

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

Для просмотра истории вызовов перейдите по ссылке «*Посмотреть “историю вызовов”*». Описание мониторинга параметров приведено в разделе 2.5.2.7 Подменю «История вызовов».

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

2.4.4 Меню «Система»

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

2.4.4.1 Подменю «Время»

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

Рисунок 44 - Подменю «Время»

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.
- *Сервер синхронизации* – IP-адрес/доменное имя сервера синхронизации времени. Возможен ручной ввод адреса сервера или выбор из списка.

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

2.4.4.2 Подменю «Доступ»

В подменю «Доступ» настраивается доступ к устройству посредством WEB-интерфейса и Telnet.

Порты доступа

Порт HTTP

Порт HTTPS

Порт Telnet

Доступ к услуге "Интернет"

Web

Внешняя сеть (LAN) HTTP HTTPS

Локальная сеть (PC) HTTP HTTPS

Telnet

Внешняя сеть (LAN)

Локальная сеть (PC)

Доступ к услуге "VoIP"

Web HTTP HTTPS

Telnet

Доступ к услуге "Интерфейс управления"

Web HTTP HTTPS

Telnet

Рисунок 45 - Подменю «Доступ»

Порты доступа

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

- *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;

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

Доступ к услуге Интернет

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

Web, Внешняя сеть:

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

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

Web, Локальная сеть:

- *HTTP* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через LAN-порт (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 LAN-порт) или внутренней (через PC-порт) сети установите соответствующие флаги.

Доступ к услуге VoIP:

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

Доступ к услуге *Интерфейс управления*:

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



Для авторизации по протоколу Telnet по умолчанию используются имя пользователя *admin*, пароль – *password*. После авторизации станет доступна консоль операционной системы Linux с возможностью использования основных команд командного интерпретатора shell.

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

2.4.4.3 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.

- Менеджер интерфейсов – отвечает за работу интерфейсов взаимодействия устройства с пользователем (таких как клавиатура, дисплей, спикерфон, телефонная трубка и т.д.).

Журнал телефонии

Вывод журнала

Ошибки

Предупреждения

Отладочная информация

Информационные сообщения

Уровень трассировки SIP

Журнал системного менеджера

Вывод журнала

Ошибки

Предупреждения

Отладочная информация

Информационные сообщения

Журнал менеджера конфигурации

Вывод журнала

Ошибки

Предупреждения

Отладочная информация

Информационные сообщения

Журнал менеджера интерфейсов

Вывод журнала

Ошибки

Предупреждения

Отладочная информация

Информационные сообщения

Настройка Syslog

Включить

Режим

Адрес Syslog-сервера

Порт Syslog-сервера

Рисунок 46 - Подменю «Журнал»

Журнал телефонии

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

Ниже настраивается тип сообщений, выводимых в журнал телефонии:

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

Журнал системного менеджера, менеджера конфигурации, менеджера интерфейсов

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

Ниже настраивается тип сообщений, выводимых в журнал:

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

Настройка Syslog

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

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

Далее в зависимости от режима Syslog-агента доступны настройки:

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

2.4.4.4 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 протоколу Telnet.

При входе через WEB-интерфейс администратор (пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек, полный мониторинг состояния устройства.



Логин администратора: admin

Пароль администратора (admin)

Пароль

Подтверждение

Рисунок 47 - Подменю «Пароли»

- *Пароль администратора* – в соответствующие поля введите пароль администратора и подтвердите его;

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

2.4.4.5 Подменю «Управление конфигурацией»

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

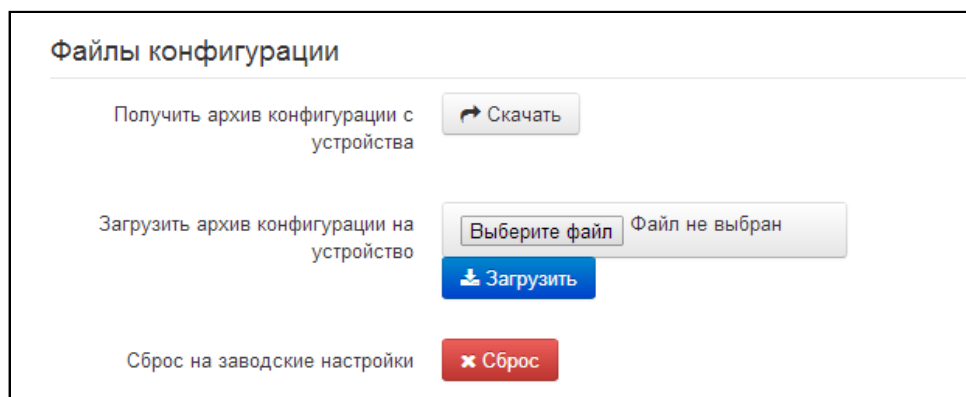


Рисунок 48 - Подменю «Файлы конфигурации»

Получение конфигурации

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

Обновление конфигурации

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

2.4.4.6 Подменю «Обновление ПО»

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

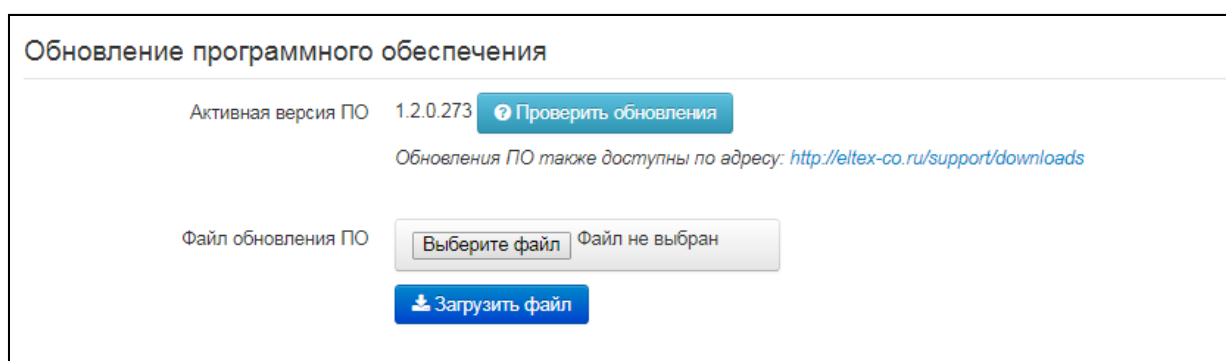


Рисунок 49 - Подменю «Обновление ПО»

- *Активная 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-co.ru/support/downloads/> и сохранив его на компьютере. Для этого нажмите кнопку «Выберите файл» в поле *Файл обновления ПО* и укажите путь к файлу управляющей программы в формате .tar.gz.

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



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

2.4.4.7 Подменю «Перезагрузка»

В подменю «Перезагрузка» выполняется перезапуск устройства.



Рисунок 50 - Подменю «Перезагрузка»

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

2.4.4.8 Подменю «Автоконфигурирование»

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

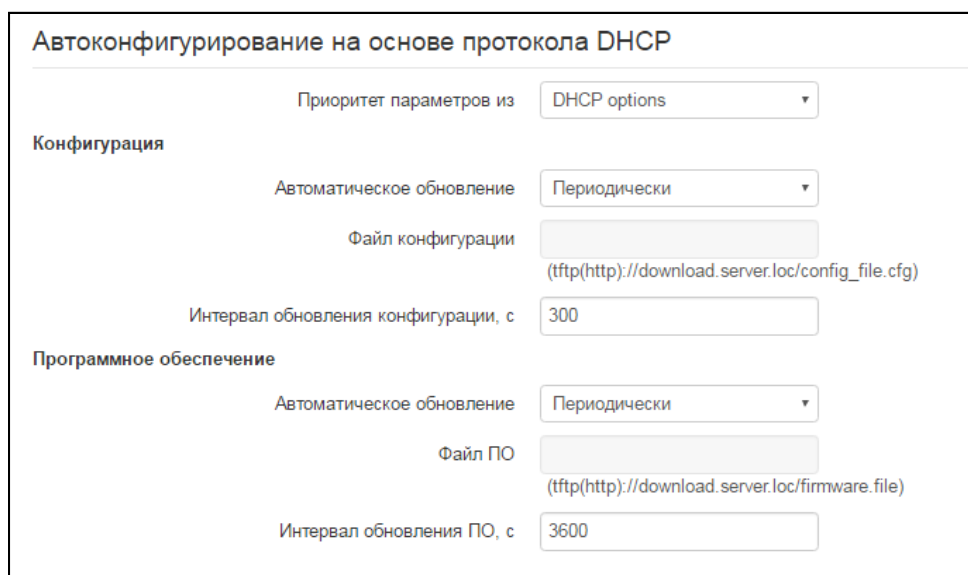


Рисунок 51 - Автоконфигурирование на основе протокола DHCP

Автоконфигурирование по протоколу TR-069

Общие

Включить клиента TR-069

Интерфейс:

Адрес сервера ACS:

Включить периодический опрос

Период опроса, с:

Запрос соединения с ACS

Имя пользователя:

Пароль:

Запрос соединения с клиентом

Имя пользователя:

Пароль:

Настройки NAT

Режим NAT:

Адрес STUN-сервера:

Порт STUN-сервера:

Минимальный период опроса, с:

Максимальный период опроса, с:

Рисунок 52 - Автоконфигурирование по протоколу TR-069

Автоконфигурирование на основе протокола DHCP:

- *Приоритет параметров из* – данный параметр определяет, откуда необходимо взять названия и расположение файлов конфигурации и программного обеспечения:
 - *Static settings* – пути к файлам конфигурации и программного обеспечения определяются соответственно из параметров «*Файл конфигурации*» и «*Файл ПО*»; подробнее работу алгоритма смотрите в разделе 0;
 - *DHCP options* – пути к файлам конфигурации и программного обеспечения определяются из DHCP опций 43, 66 и 67 (для этого необходимо для услуги Интернет выбрать протокол DHCP); подробнее работу алгоритма смотрите в разделе 0;
- 1. *Автоматическое обновление*—для обновления конфигурации ПО отдельно можно задать один из нескольких режимов обновления:
 - *Выключено* - автоматическое обновление конфигурации или программного обеспечения устройства отключено;
 - *Периодически* - автообновление конфигурации или программного обеспечения устройства будет производиться через заданный промежуток времени;

- По расписанию - автообновление конфигурации или программного обеспечения устройства будет производиться в заданное время, в указанные дни недели.

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

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

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

где < server address > – адрес HTTP- или TFTP-сервера (доменное имя или IPv4),

< full path to cfg file > – полный путь к файлу конфигурации на сервере;

- *Интервал обновления конфигурации, с* – промежуток времени в секундах, через который осуществляется периодическое обновление конфигурации устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;
- *Время обновления файла конфигурации* - время в 24-часовом формате, в которое будет производиться автообновление конфигурации;
- *Дни обновления конфигурации* - дни недели, в которые в заданное время будет производиться автообновление конфигурации.
- *Файл ПО* – полный путь к файлу программного обеспечения – задаётся в формате URL (на данный момент возможна загрузка файла ПО по протоколам TFTP и HTTP):

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

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

где < server address > – адрес HTTP- или TFTP-сервера (доменное имя или IPv4),

< full path to firmware file > – полный путь к файлу ПО на сервере;

- *Интервал обновления ПО, с* – промежуток времени в секундах, через который осуществляется периодическое обновление программного обеспечения устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;
- *Время обновления ПО* - время в 24-часовом формате, в которое будет производиться автообновление программного обеспечения;
- *Дни обновления ПО* - дни недели, в которые в заданное время будет производиться автообновление программного обеспечения.

Детальное описание алгоритма автоматического обновления на основе протокола DHCP смотрите в разделе 0.

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 80). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS. ACS-сервер фирмы Eltex по умолчанию использует для связи порт 9595;

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

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).



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

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

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

2.4.4.9 Подменю «Интерфейс управления»

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

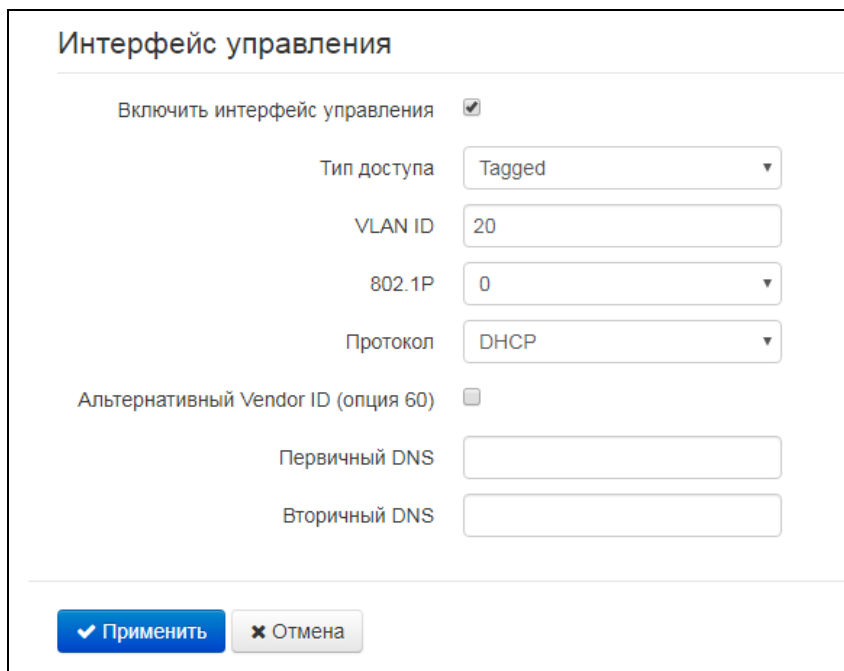


Рисунок 53 - Подменю «Интерфейс управления»

- *Включить интерфейс управления* – при установленном флаге управление устройством производится через данный интерфейс;
 - *Тип доступа* – задает режим работы интерфейса:
 - *Tagged* – данные передаются интерфейсом с использованием заданного VLAN ID;
 - *Untagged* – данные передаются интерфейсом без использования VLAN.
 - 1. *VLAN ID* – идентификатор для выделения интерфейса в виртуальную локальную сеть;
 - 2. *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);
 - 3. *Протокол* – выбор протокола назначения адреса на интерфейс:
 - *Static* – режим работы, при котором IP-адрес и все необходимые настройки на LAN-интерфейсе 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:VP-12P][HW:1.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]
[LAN:02:20:80:a8:f9:4b][VERSION:#1.12.0]


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

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

2.5 Мониторинг системы

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



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

2.5.1 Подменю «Интернет»

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

Выход в Интернет

Подключение к сети	Проводное
Протокол доступа	Static
IP-адрес	192.168.18.123

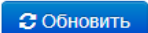


Рисунок 54 - Подменю «Интернет»

Выход в Интернет

- *Подключение к сети* – способ подключения к сети передачи данных. Настройка подключения производится в разделе **Сеть – Интернет**:
 - *Проводное* – подключение к сети провайдера осуществляется посредством соединения медным или оптическим патч-кордом с портом LAN;
- 1. *Протокол доступа* – протокол, используемый для доступа к сети Интернет;
- 2. *IP-адрес* – IP-адрес устройства во внешней сети;

2.5.2 Подменю «IP-телефония»

В подменю «IP-телефония» осуществляется просмотр состояния сетевого интерфейса VoIP и мониторинг аккаунтов.

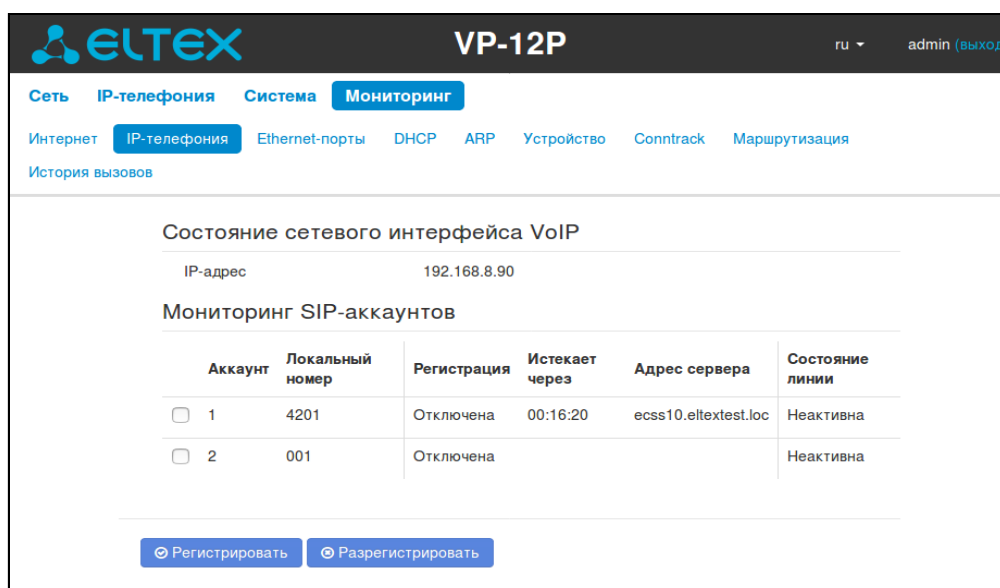


Рисунок 55 - Подменю «IP-телефония»

Состояние сетевого интерфейса VoIP

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

Мониторинг SIP-аккаунтов

- *Аккаунт* – номер аккаунта;
- *Локальный номер* – номер телефона абонента, закрепленный за данным аккаунтом;
- *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.
- 1. *Истекает через* – время до истечения регистрации аккаунта на SIP-сервере;
- 2. *Адрес сервера* – адрес сервера, на котором последний раз прошла регистрацию абонентская линия;
- 3. *Состояние линии* – состояние физической линии. Линия может находиться в одном из следующих состояний:

- *Не активна* – телефонная трубка положена (либо аккаунт выключен), нормальная работа;
- *Активна* – линия находится в состоянии разговора;
- *Посылка вызова* – на телефон подается вызывной сигнал (при поступлении входящего звонка);
- *Исходящий вызов* – подается сигнал КПВ (при совершении исходящего звонка);
- *На удержании* – вызов находится на удержании.

2.5.2.1 Подменю «Ethernet-порты»

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

Состояние Ethernet-портов					
Порт	Подключение	Скорость	Режим	Передано	Принято
LAN	Вкл.	100 Мбит/с	Full-duplex	1.8 Мбайт (1 903 024 байт)	857.8 Кбайт (878 341 байт)
PC	Выкл.				

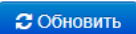


Рисунок 56 - Подменю «Ethernet-порты»

Состояние Ethernet-портов

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

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

2.5.2.2 Подменю «DHCP»

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

Список DHCP-клиентов			
MAC-адрес	Имя клиента	IP-адрес	Время до истечения аренды
<div style="background-color: #0070C0; color: white; padding: 2px 5px; display: inline-block;">  Обновить </div>			

Рисунок 57 - Подменю «DHCP»

Активные DHCP-аренды

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

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

2.5.2.3 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	MAC-адрес	Имя клиента	Интерфейс
192.168.18.1	A8:F9:4B:80:E7:00		Bridge

[Обновить](#)

Рисунок 58 - Подменю «ARP»

ARP-таблица

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

Для получения текущей информации нажмите кнопку «Обновить».

2.5.2.4 Подменю «Устройство»

В подменю «Устройство» приведена общая информация об устройстве.

Информация об устройстве	
Изделие	VP-12P
Версия ПО	1.2.0.273
Заводской MAC-адрес	A8:F9:4B:2A:92:5A
Серийный номер	V14B000039
Системное время	07:28:00 29.08.2017
Время работы	4 дн, 01:09:13

Рисунок 59 - Подменю «Устройство»

Информация об устройстве

- *Изделие* – наименование модели устройства;
- *Версия ПО* – версия программного обеспечения устройства;
- *Заводской MAC-адрес* – MAC-адрес устройства, установленный заводом-изготовителем;
- *Серийный номер* – серийный номер устройства, установленный заводом-изготовителем;
- *Системное время* – текущие время и дата, установленные в системе;

- *Время работы* – время работы с момента последнего включения или перезагрузки устройства.

2.5.2.5 Подменю «Conntrack»

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

Вывод активных сессий NAT			
Число активных соединений	11		
Число показанных соединений	11		
Список соединений			
Протокол	Адрес источника	Адрес назначения	Таймаут
TCP	192.168.27.86:50158	192.168.18.37:80	1 мин 25 с
UDP	192.168.18.10:49328	255.255.255.255:138	23 с
TCP	192.168.27.86:50164	192.168.18.37:80	1 мин 59 с
UDP	192.168.18.24:137	192.168.18.255:137	27 с
UDP	192.168.23.25:5070	192.168.18.37:5062	27 с
UDP	192.168.18.10:137	192.168.18.255:137	23 с
TCP	192.168.27.86:50166	192.168.18.37:80	4 дн 23 ч 59 мин 59 с
UDP	192.168.18.32:17500	192.168.18.255:17500	4 с
UDP	192.168.23.42:5063	192.168.18.37:5062	26 с
UDP	192.168.18.32:17500	255.255.255.255:17500	4 с
TCP	192.168.27.86:50161	192.168.18.37:80	1 мин 42 с

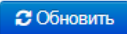


Рисунок 60 - Подменю «Conntrack»

Вывод активных сессий NAT

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

Список соединений

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

Для получения текущей информации нажмите кнопку «Обновить».

2.5.2.6 Подменю «Маршрутизация»

В подменю «Маршрутизация» отображается таблица маршрутизации устройства.

Таблица маршрутизации							
Адресат	Шлюз	Маска	Флаги	Метрика	Обращения	Обнаружения	Интерфейс
192.168.18.0	0.0.0.0	255.255.255.0	U	0	0	0	br0
172.20.0.0	192.168.18.1	255.255.255.0	UG	0	0	0	br0
10.100.101.0	192.168.18.1	255.255.255.0	UG	0	0	0	br0
172.16.0.0	192.168.18.1	255.255.252.0	UG	0	0	0	br0
192.168.0.0	192.168.18.1	255.255.0.0	UG	0	0	0	br0
0.0.0.0	192.168.18.1	0.0.0.0	UG	0	0	0	br0



Рисунок 61 - Подменю «Маршрутизация»

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

Для получения текущей информации нажмите кнопку «Обновить».

2.5.2.7 Подменю «История вызовов»

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

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

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

Фильтр (показать)

[Настроить параметры истории вызовов](#)

#	Линия	Локальный номер	Удаленный номер	IP-адрес встречной стороны	Время поступления вызова	Время начала разговора	Длительность разговора	Состояние вызова	Тип вызова	Передано пакетов	Передано байт	Принято пакетов	Принято байт
1	2	008	-	-	03:04:14 01.01.1970	-	-	local	входящий	0	0	0	0
2	1	007	-	-	03:04:16 01.01.1970	-	-	local	входящий	0	0	0	0

записей на странице

Страница 1 из 1

Рисунок 62 - Подменю «История вызовов»

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 0 **Меню «История вызовов»**.

- При нажатии на кнопку  произойдет переход к таблице, начиная с первой записи.
- При нажатии на кнопку  произойдет переход к предыдущей странице с таблицей истории вызовов.
- При нажатии на кнопку  произойдет переход к следующей странице с таблицей истории вызовов.
- При нажатии на кнопку  произойдет переход к таблице, заканчивая последней записью.

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

2.6 Пример настройки

На ПК откройте Web-браузер, например, Firefox, Opera, Chrome.

В адресной строке браузера введите IP-адрес устройства.



По умолчанию устройство получает IP-адрес и другие параметры сети по протоколу DHCP. Для дальнейшей работы необходимо узнать IP-адрес который получил IP-телефон от DHCP сервера. Сделать это можно при помощи экранного меню, для этого:

Нажмите софт-клавишу меню, далее в разделе «статус» посмотрите какой IP-адрес получил телефон.

Если IP-адрес установлен в значение 0.0.0.0, то это значит IP-телефон не получил его от DHCP сервера. В таком случае необходимо настроить сетевые параметры вручную при помощи экранного меню. Настройка устройства с помощью экранного меню описана в следующем разделе.

При успешном подключении к устройству появится окно с запросом логина и пароля. Заполните поля и нажмите кнопку «Войти».

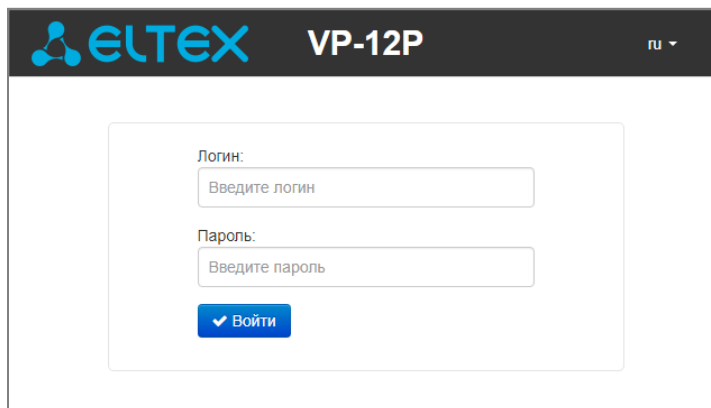


Рисунок 63 – Страница авторизации пользователя



По умолчанию логин: admin, пароль: password.

В верхнем правом углу, при необходимости, возможно сменить язык WEB-интерфейса на нужный:



Рисунок 64 – Переключатель языка WEB-интерфейса

При успешной авторизации откроется страница с мониторингом текущего состояния устройства:

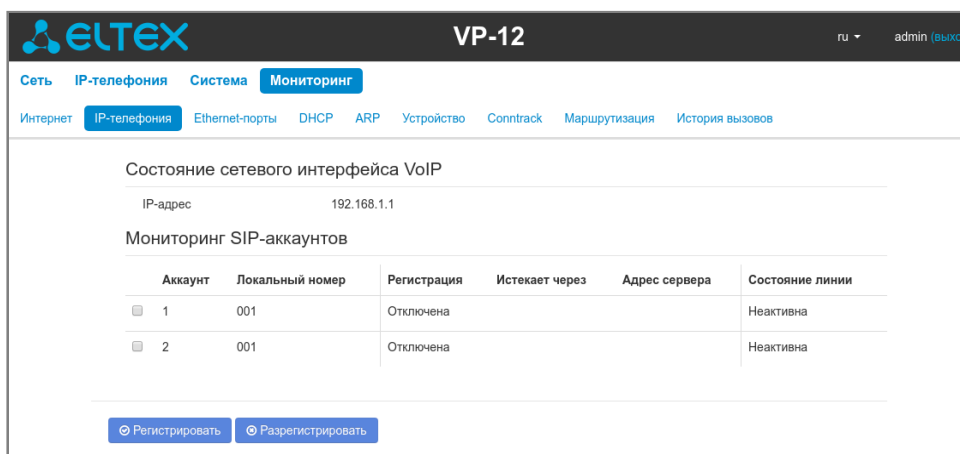
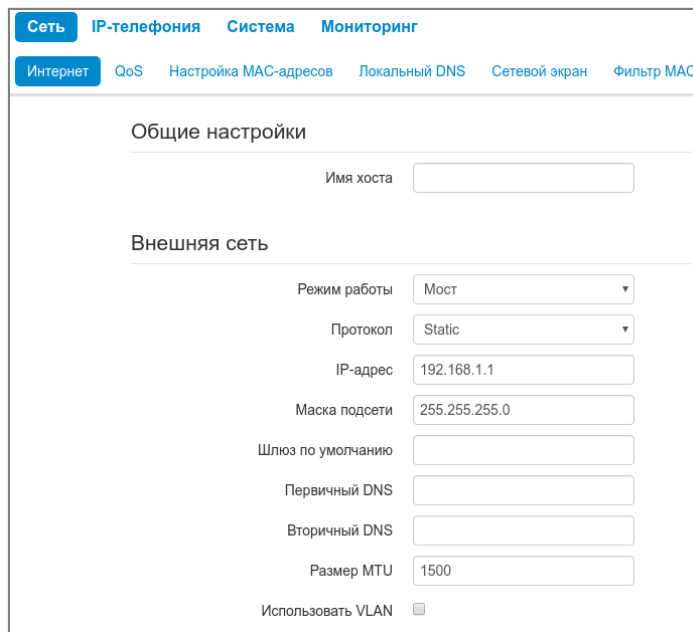


Рисунок 65 – Домашняя страница WEB-интерфейса

Для изменения сетевых настроек устройства перейдите в раздел «Сеть - Интернет».


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.

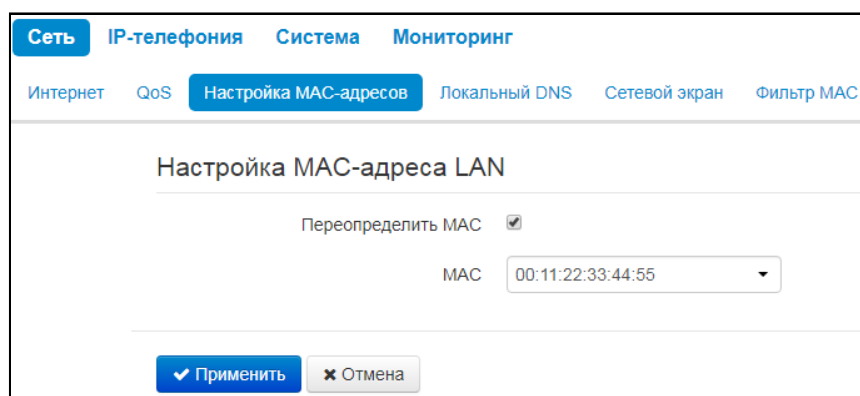
Для сохранения и применения настроек нажмите кнопку .



The screenshot shows the 'Сеть' (Network) configuration page. The 'Интернет' (Internet) tab is selected. Under 'Общие настройки' (General settings), there is a field for 'Имя хоста' (Host name). Under 'Внешняя сеть' (External network), there are fields for 'Режим работы' (Operation mode) set to 'Мост' (Bridge), 'Протокол' (Protocol) set to 'Static', 'IP-адрес' (IP address) set to '192.168.1.1', 'Маска подсети' (Subnet mask) set to '255.255.255.0', 'Шлюз по умолчанию' (Default gateway), 'Первичный DNS' (Primary DNS), 'Вторичный DNS' (Secondary DNS), and 'Размер MTU' (MTU size) set to '1500'. There is also a checkbox for 'Использовать VLAN' (Use VLAN) which is currently unchecked.

Рисунок 66 – Настройка сетевых параметров

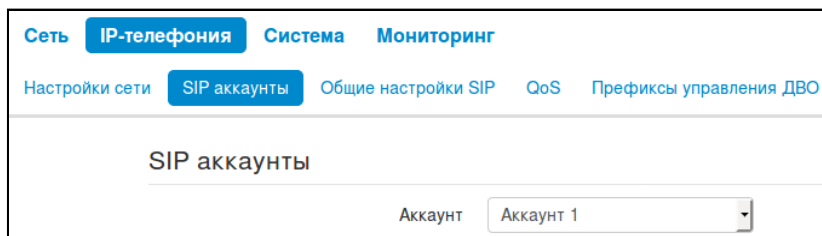
Если в сети вашего Интернет-провайдера используется привязка к MAC-адресу, откройте вкладку «Сеть - > Настройка MAC-адресов». В разделе «Настройка MAC-адреса LAN» установите флаг «Переопределить MAC» и введите в поле «MAC» необходимый MAC-адрес устройства. Для сохранения и применения настроек нажмите кнопку .



The screenshot shows the 'Настройка MAC-адреса LAN' (LAN MAC address configuration) page. The 'Настройка MAC-адресов' (MAC address configuration) tab is selected. There is a checkbox for 'Переопределить MAC' (Override MAC) which is checked. Below it is a dropdown menu for 'MAC' with the value '00:11:22:33:44:55'. At the bottom, there are two buttons: 'Применить' (Apply) and 'Отмена' (Cancel).

Рисунок 67 – Настройка MAC-адреса LAN

Во вкладке «IP-телефония -> SIP аккаунты» выполняется настройка аккаунтов для работы по протоколу SIP. Для этого выберите в выпадающем списке «Аккаунт», который необходимо настроить.



The screenshot shows the 'SIP аккаунты' (SIP accounts) page. The 'SIP аккаунты' (SIP accounts) tab is selected. There is a dropdown menu for 'Аккаунт' (Account) with the value 'Аккаунт 1' (Account 1).

Рисунок 68 – Выбор SIP-аккаунта

Отметьте пункт «Включить», введите номер телефона, который будет назначен данному аккаунту, а также укажите логин и пароль для авторизации на SIP-сервере.

Включить	<input checked="" type="checkbox"/>
Номер телефона	<input type="text" value="4201"/>
Имя пользователя	<input type="text" value="4201"/>
Использовать альтернативный номер	<input type="checkbox"/>
SIP-порт	<input type="text" value="5060"/>
Категория абонента	<input type="text" value="Не использовать"/>

Рисунок 69 – Настройка SIP-аккаунта

Аутентификация	
Логин	<input type="text" value="4201"/>
Пароль	<input type="password" value="****"/>

Рисунок 70 – Настройка логина и пароля

Ниже на вкладке 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. Установите флаг «Регистрация», если для работы телефонии необходима регистрация абонентов на SIP-сервере (обычно, регистрация необходима).

Параметры SIP	
Режим использования SIP-прокси	<input type="text" value="Homing"/>
SIP-прокси сервер	<input type="text" value="192.168.8.235"/>
Регистрация	<input checked="" type="checkbox"/>
Сервер регистрации	<input type="text" value="ecss10.eltextest.loc:5065"/>
Метод контроля основного сервера	<input type="text" value="Invite"/>
Период контроля основного сервера, с	<input type="text" value="30"/>

Рисунок 71 – Параметры SIP

Укажите SIP домен (при необходимости) в блоке параметров «Дополнительные параметры SIP». При необходимости использования доменного имени при регистрации, установите SIP-домен в разделе «Дополнительные параметры SIP»:

Дополнительные параметры SIP	
SIP-домен	<input type="text" value="eltextest.loc"/>
Применить SIP Domain для регистрации	<input checked="" type="checkbox"/>
Режим Outbound	<input type="text" value="Выключен"/>
Период времени перерегистрации	<input type="text" value="1800"/>
Интервал повтора регистрации	<input type="text" value="30"/>
Публичный адрес	<input type="text"/>

Рисунок 72 – Дополнительные параметры SIP

Для сохранения и применения настроек нажмите кнопку .

ПРИЛОЖЕНИЕ А. АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP

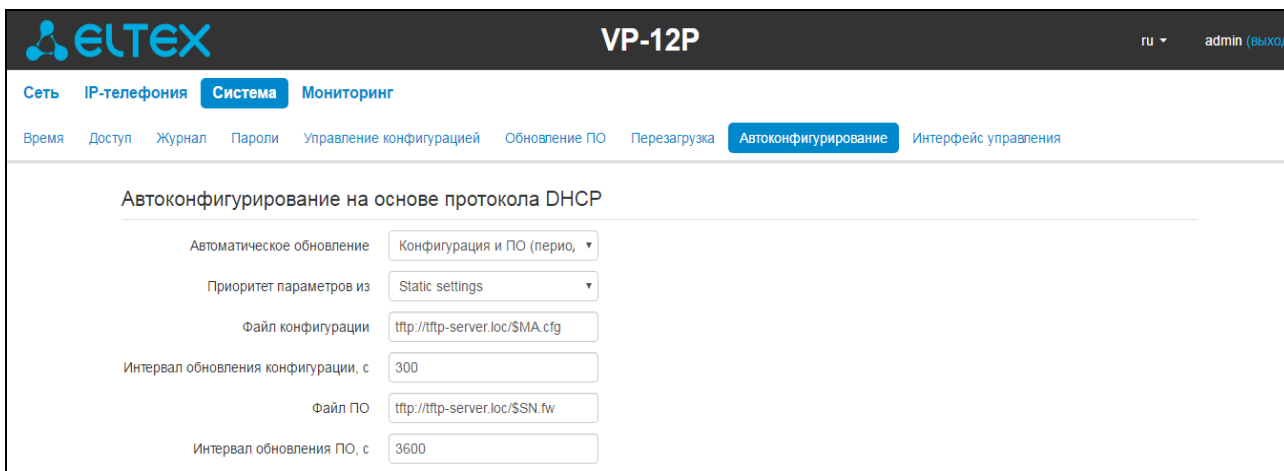


Рисунок - Вкладка «Автоконфигурирование»

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

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

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

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

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

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

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

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

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

\$PN – Product name – вместо данного макроса в URL файла устройство подставляет название модели (например, VP-12P);

\$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/vp-12(p)/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_vp12.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: \$MAC.cfg;
- для имени файла программного обеспечения: vp12.fw.

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

```
tftp://update.local/A8.F9.4B.00.11.22.cfg,
```

а URL файла ПО:

```
tftp://update.local/vp12.fw.
```

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

- для протокола: tftp;
- для адреса сервера: update.local;
- для имени файла конфигурации: \$MAC .cfg;
- для имени файла программного обеспечения: vp12.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.

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.

ПРИЛОЖЕНИЕ Б. 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 удаленного 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 *VP-12(P)*.
- Если процесс передачи файла начался – дождитесь его окончания, после чего *VP-12(P)* 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 В. 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 VP-12(P) предусмотрена возможность через конфигурационный файл настроить запуск произвольного скрипта, в который можно поместить любую желаемую последовательность команд.

Для запуска произвольного скрипта в файле конфигурации создана секция настроек:

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

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

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

1. Запуск с HTTP-сервера

Для запуска скрипта с HTTP-сервера необходимо в параметре URL указать полный путь к файлу в формате HTTP-URL:

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

В этом случае после старта устройства файл script.sh, хранящийся в каталоге user-script по адресу 192.168.0.250, автоматически загрузится по протоколу HTTP с указанного сервера, после чего будет произведён его запуск.

2. Запуск с TFTP-сервера

Для запуска скрипта с TFTP-сервера необходимо в параметре URL указать полный путь к файлу в формате TFTP-URL:

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

В этом случае после старта устройства файл script.sh, хранящийся в каталоге user-script по адресу 192.168.0.250, автоматически загрузится по протоколу TFTP с указанного сервера, после чего будет произведён его запуск.

3. Запуск локального скрипта

Ввиду особенностей файловой системы локальный скрипт должен располагаться только в каталоге /etc/config, так как только содержимое этого каталога сохраняется после перезагрузки устройства. Скрипт в каталоге /etc/config можно создать либо с помощью редактора vi, либо загрузить его с внешнего TFTP-сервера (командой tftp -gl user.sh <TFTP-server address>). После создания скрипта ему необходимо назначить права на запуск командой chmod 777 /etc/config/user.sh.

В файле конфигурации URL для запуска локального скрипта имеет вид:

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

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

ПРИЛОЖЕНИЕ Г. НАСТРОЙКА DHCP КЛИЕНТОВ В МУЛЬТИСЕРВИСНОМ РЕЖИМЕ.

На устройствах VP-12(P) имеется возможность настраивать опции, получаемые DHCP клиентами на разных интерфейсах.

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

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

Конфигурацию списка запрашиваемых опций можно изменять и хранится она как и все остальные настройки в конфигурационном файле: `/etc/config/cfg.yaml`. По умолчанию списки опций не прописаны (в конфигурации следующая запись `DHCPOptionList: ""`), это значит что опции запрашиваются и применяются согласно приведённой выше таблице.

Способы редактирования конфигурации

I. С помощью редактора vi.

1. Список опций для интерфейса Internet задаётся в параметре `DHCPOptionList` секции `Internet=>Network`.

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

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

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



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

II. С помощью команды setconf

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

Пример 1. Необходимо получить значение DHCPOptionList:

для интерфейса Internet

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

для интерфейса VoIP

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

для интерфейса Management

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

Пример 2. Необходимо назначить некоторый список опций:

для интерфейса Internet

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

для интерфейса VoIP (назначаем список опций по умолчанию)

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

для интерфейса Management

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

III. Конфигурирование на персональном компьютере

Предварительно скачивается конфигурация с устройства на ПК (через web интерфейс), далее с помощью любого текстового редактора меняются значения, сохраняются изменения. Завершающим этапом является загрузка измененной конфигурации в устройство. !!! Данный метод не рекомендуется!!!

Правила редактирования DHCPOptionList

1. Валидные значения: 3,6,12,15,26,28,33, 42,43,66,67,120,121,249;
2. Опции в параметре DHCPOptionList указываются через запятую и без пробелов между опциями, пример DHCPOptionList: "3,6,12,15,26,120,121";

3. Порядок следования опций в DHCPOptionList не важен;
4. Каждая из опций 12, 15, 42, 43, 66, 67, 120 может быть запрошена и применены только с одного интерфейса;
5. Опции 1, 3, 6, 26, 28, 33, 121, 249 могут запрашиваться dhcp клиентами для каждого субинтерфейса;
6. Опции 66 и 67 должны быть указаны на одном и том же интерфейсе;
7. Если в DHCPOptionList ничего не указано, то тогда список запрашиваемых опций по умолчанию (учетом пункта 8);
8. Если DHCPOptionList указаны опции (из пункта 4), которые по умолчанию запрашиваются с другого интерфейса (на котором DHCPOptionList не заполнен), то тогда опции будут запрашиваться с первого интерфейса, а на втором из списка по умолчанию данные опции будут исключены *;
9. Если для интерфейса в DHCPOptionList указан список опций, то будут запрашиваться только эти опции;
10. Опцию 1 в DHCPOptionList нельзя указывать, она запрашивается и применяется всегда и со всех интерфейсов независимо от прочих настроек;

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

*** Пример к пункту 8:**

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

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

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

В итоге будут следующие списки:

значение параметра: Internet.Network.DHCPOptionList: "3, 6, 26, 28, 33, 121, 249, 12" запрашиваемый список опций: 1, 3, 6, 26, 28, 33, 121, 249, 12 значение параметра: System.ManagementVLAN.DHCPOptionList: "" запрашиваемый список опций: 1, 3, 6, 15, 26, 28, 33, 42, 43, 66, 67, 121, 249



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

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

Российская Федерация, 630020, г. Новосибирск, ул. Окружная, дом 29В.

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 базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

Официальный сайт компании: <http://eltex-co.ru>

Технический форум: <http://eltex-co.ru/forum>

База знаний: <http://eltex-co.ru/support/knowledge>

Центр загрузок: <http://eltex-co.ru/support/downloads>