Комплексные решения для построения сетей

WB-10P/WB-11P

Руководство по эксплуатации, версия 1.2.0 (08.2018)

Терминал беспроводного доступа (2G/3G/4G)

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

Версия документа	Дата выпуска	Содержание изменений
Версия 1.4	08.2018	Добавлено: 3.5.2.3 Подменю «L2TP» 3.5.2.4 Подменю «Open VPN»
Версия 1.3	12.2017	Добавлено: 3.5.2.4 Подменю «DHCP Relay» 3.5.2.15 Подменю «Резервирование»
Версия 1.2	09.2017	Третья публикация
Версия 1.1	02.2017	Вторая публикация
Версия 1.0	12.2016	Первая публикация
Версия программного обеспечения	Версия ПО: 1.2.0.329 Версия Web-интерфейса: 1.2.83	

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

Обозначение	Описание
Полужирный шрифт	Полужирным шрифтом выделены примечания и предупреждения, название глав, заголовков, заголовков таблиц.
Курсивом Calibri	Курсивом Calibri указывается информация, требующая особого внимания.
	Устройство WB-10P/WB-11P
	Компьютер
	Цифровая телевизионная приставка STB
	Беспроводное соединение

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

СОДЕРЖАНИЕ 4
1 ВВЕДЕНИЕ 6
2 ОПИСАНИЕ ИЗДЕЛИЯ 7
2.1 Назначение 7
2.2 Варианты исполнения 7
2.3 Характеристики устройств 7
2.4 Структура и принцип работы изделия 11
2.5 Основные технические параметры 11
2.6 Конструктивное исполнение 12
2.7 Световая индикация 13
2.8 Сброс к заводским настройкам 14
2.9 Комплект поставки 14
3 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР 15
3.1 Начало работы 15
3.2 Пользователи 16
3.3 Применение конфигурации и отмена изменений 16
3.4 Настройки 17
3.4.1 Основные элементы Web-интерфейса 17
3.4.2 Меню «Сеть» 18
3.4.2.1 Подменю «Интернет» 18
3.4.2.2 Подменю «GRE» 22
3.4.2.3 Подменю «L2TP» 24
3.4.2.4 Подменю «OpenVPN» 25
3.4.2.5 Подменю «IPv6» 27
3.4.2.6 Подменю «DHCP Relay» 29
3.4.2.7 Подменю «QoS» 29
3.4.2.8 Подменю «Шейпинг трафика» 30
3.4.2.9 Подменю «DHCP-сервер» 31
3.4.2.10 Подменю «Локальный DNS» 32
3.4.2.11 Подменю «NAT и проброс портов» 33
3.4.2.12 Подменю «Сетевой экран» 35
3.4.2.13 Подменю «Фильтр MAC» 37
3.4.2.14 Подменю «Маршрутизация» 38
3.4.2.15 Подменю «Динамический DNS» 40
3.4.2.16 Подменю «SNMP» 41
3.4.2.17 Подменю «Контроль связи» 42
3.4.3 Меню «Система» 43
3.4.3.1 Подменю «Время» 43
3.4.3.2 Подменю «Доступ» 44
3.4.3.3 Подменю «Журнал» 46
3.4.3.4 Подменю «Пароли» 49
3.4.3.5 Подменю «Управление конфигурацией» 50
3.4.3.6 Подменю «Обновление ПО» 50
3.4.3.7 Подменю «Перезагрузка» 51
3.4.3.8 Подменю «Автоконфигурирование» 52
3.4.3.9 Подменю «Интерфейс управления» 55
3.4.3.10 Подменю «wiSLA» 56
3.4.3.11 Подменю «Дополнительные настройки» 57
3.5 Мониторинг системы 58
3.5.1 Подменю «Интернет» 58
3.5.2 Подменю «Ethernet-порты» 61

3.5.3 Подменю «USB модемы» 62
3.5.4 Подменю «DHCP» 64
3.5.5 Подменю «ARP» 64
3.5.6 Подменю «Устройство» 65
3.5.7 Подменю «Conntrack» 66
3.5.8 Подменю «Маршрутизация» 67
4 АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP 71
5 ПРОЦЕДУРА ВОССТАНОВЛЕНИЯ СИСТЕМЫ ПОСЛЕ СБОЯ ПРИ ОБНОВЛЕНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ 74
ПРИЛОЖЕНИЕ А. ЗАПУСК ПРОИЗВОЛЬНОГО СКРИПТА ПРИ СТАРТЕ СИСТЕМЫ 75
ПРИЛОЖЕНИЕ Б. ИЗМЕНЕНИЕ НАСТРОЕК ПО УМОЛЧАНИЮ ДЛЯ ОПЕРАТОРОВ ПРИ АВТОМАТИЧЕСКОМ ОПРЕДЕЛЕНИИ ОПЕРАТОРА 76
ПРИЛОЖЕНИЕ В. ИСПОЛЬЗОВАНИЕ COMMAND LINE INTERFACE (CLI) ДЛЯ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА 77
ПРИЛОЖЕНИЕ Г. ИНСТРУКЦИЯ ПО УСТАНОВКЕ УСТРОЙСТВА 89

1 ВВЕДЕНИЕ

Современные тенденции развития связи диктуют операторам необходимость поиска оптимальных технологий, позволяющих удовлетворить стремительно возрастающие потребности абонентов, сохраняя при этом преемственность бизнес-процессов, гибкость развития и сокращение затрат на предоставление различных сервисов. Беспроводные технологии в короткое время прошли огромный путь от нестабильных низкоскоростных сетей связи малого радиуса до сетей ШПД, сопоставимых по скорости с проводными сетями с высокими требованиями к качеству предоставления услуг.

Терминал беспроводного доступа WB-10P/WB-11P (далее «устройство») предназначен для использования вне помещений и представляет собой единую точку доступа ко всем интерактивным сервисам по беспроводным сетям операторов сотовой связи. Устройство имеет 1 порт Gigabit Ethernet для организации питания (PoE 48В) и подключения проводных сетей передачи данных.

Подключение к сетям 2G/3G/4G производится посредством одного или двух установленных на плату устройства USB-модема, работающих в режиме резервирования или агрегации каналов и поддерживающих соответствующие стандарты.

В настоящем руководстве по эксплуатации изложено назначение, основные технические характеристики, правила конфигурирования, мониторинга и смены программного обеспечения терминалов беспроводного доступа WB-10P/WB-11P.

Эксплуатация устройства должна производиться только с внешними, подключенными к USB-модемам, антеннами.

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

WB-10P и WB-11P – высокопроизводительные двухканальные 2G/3G/4G терминалы для подключения сетевого оборудования к сети Internet или ведомственным/корпоративным сетям, с поддержкой функции резервирования/агрегации каналов.

2.2 Варианты исполнения

В настоящий момент устройства выпускаются в следующих модификациях:

Таблица 1 – Варианты исполнения

Наименование модели	Интерфейс Ethernet	Порт USB	Количество портов USB	Спецификация USB
WB-10P	RJ-45	Тип A	2	2.0
WB-11P	RJ-45	Тип A	2	2.0

Устройство рассчитано на работу в широком диапазоне температур от «минус» 40°C до «плюс» 55°C. Запуск устройства в условиях пониженной температуры окружающей среды производится в два этапа:

1. После подключения кабеля Ethernet, на вход устройства подается питание. Включившийся в работу термостат отслеживает текущую температуру платы. Если температура ниже «минус» 5°C, то питание на CPU не подается, а подключается нагревательный элемент, который нагревает плату до рабочей температуры.

2. При достижении температуры выше «минус» 5°C, питание подается на CPU и производится запуск устройства. Нагревательный элемент продолжает работать. При превышении температуры платы 0°C, нагревательный элемент отключается.

2.3 Характеристики устройств

Интерфейсы:

- Ethernet: 1 порт Ethernet RJ-45 10/100/1000BASE-T;
- USB: 2 порта USB2.0 для подключения USB-модемов с внешними антеннами. Подключение внешних антенн через разъемы CRC9 или TS9 (тип разъема зависит от конструктивных особенностей USB-модема).

Питание шлюза осуществляется через витую пару сети Ethernet постоянным током напряжением 48В (PoE)**.** Устройства WB-10P и WB-11P функционально идентичны. Отличие заключается в размерах и типе герметичного корпуса, а так же в типе внешних антенн и способе их подключения.

Функции:

- сетевые функции:
  - работа в режиме «моста» или «маршрутизатора»;

  - поддержка статического адреса и DHCP (DHCP-клиент на стороне порта Ethernet);
  - поддержка VLAN;
  - поддержка GRE;
  - поддержка OpenVPN
  - поддержка L2TP
  - поддержка DNS;
  - поддержка DynDNS;
  - поддержка NAT;
  - поддержка DHCP Relay;
  - сетевой экран;
  - поддержка NTP;
  - фильтрация по MAC (черные и белые списки);
  - IPv6.

- обновление ПО через Web-интерфейс;
- поддержка резервной версии ПО;
- поддержка DHCP-based autoprovisioning;
- TR-069;
- удаленный мониторинг, конфигурирование и настройка: Web-интерфейс, Telnet, SNMP;
- возможность создания отдельного изолированного туннеля для управления;
- поддержка взаимодействия с платформой мониторинга и управления качеством услуг связи wiSLA.
- возможность настройки устройства через CLI.

На рисунке 1 показаны схемы применения оборудования *WB-10P/WB-11P*.

Схема 1

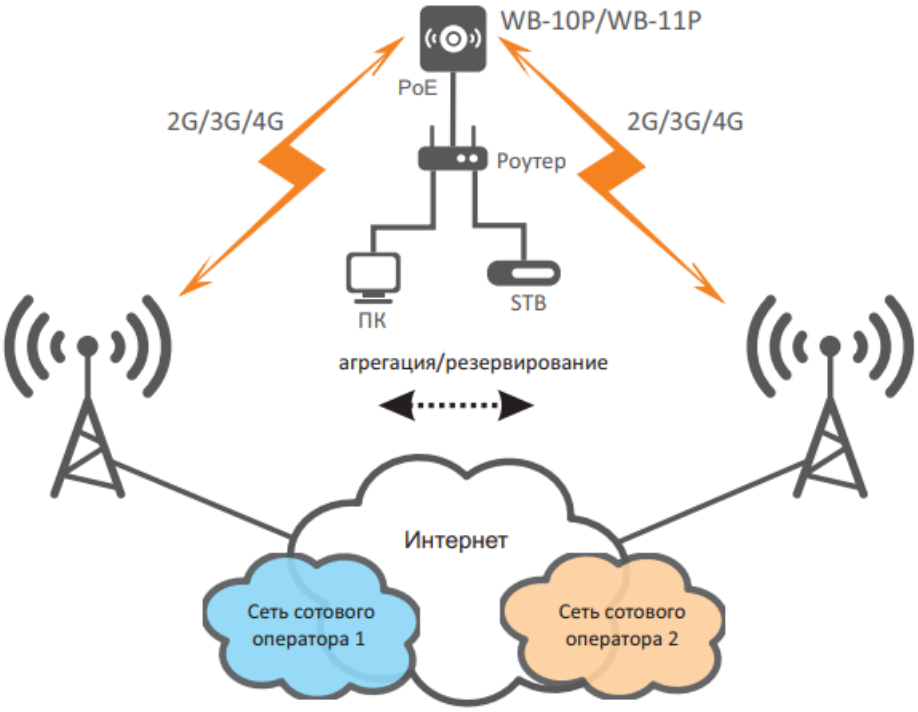


Схема 2

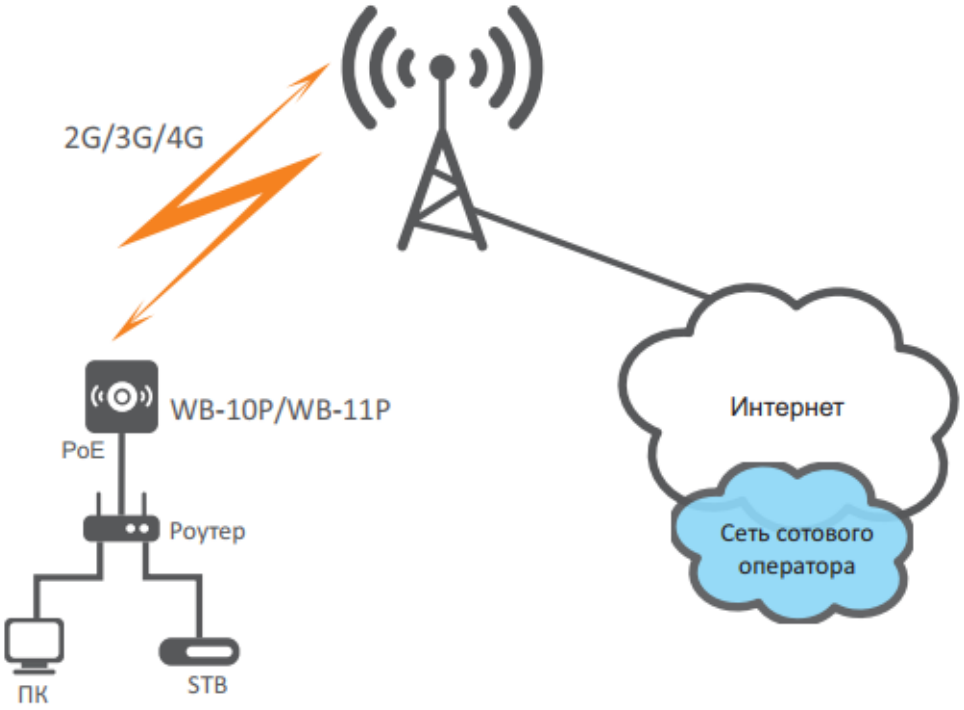


Схема 3

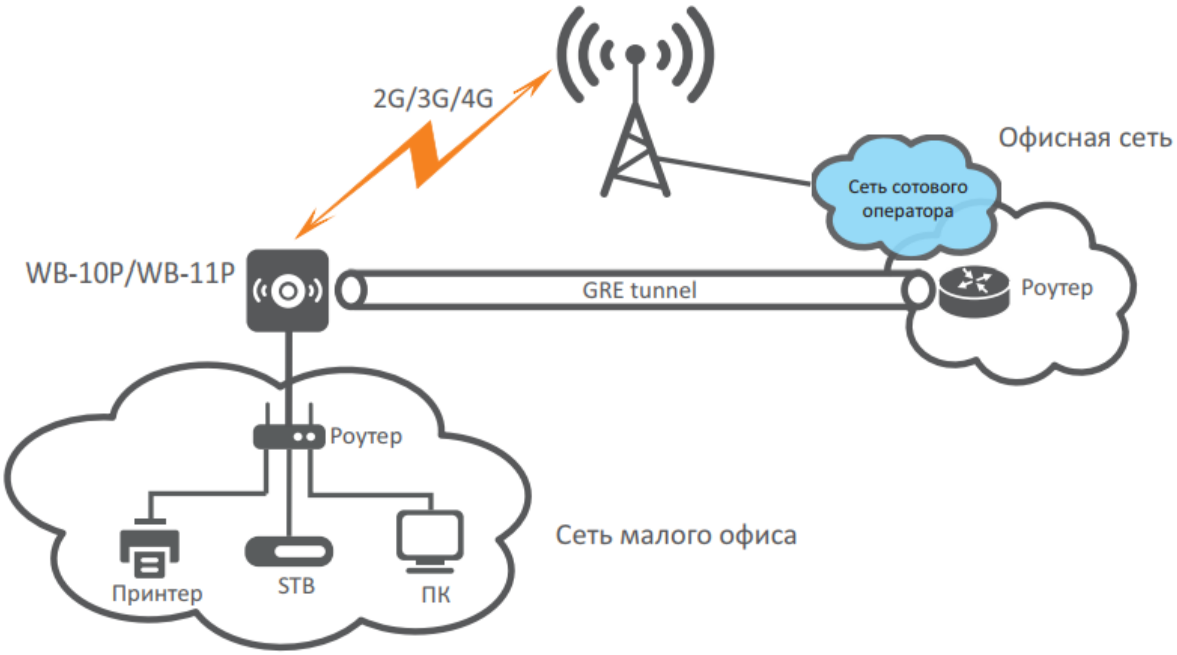


Схема 4

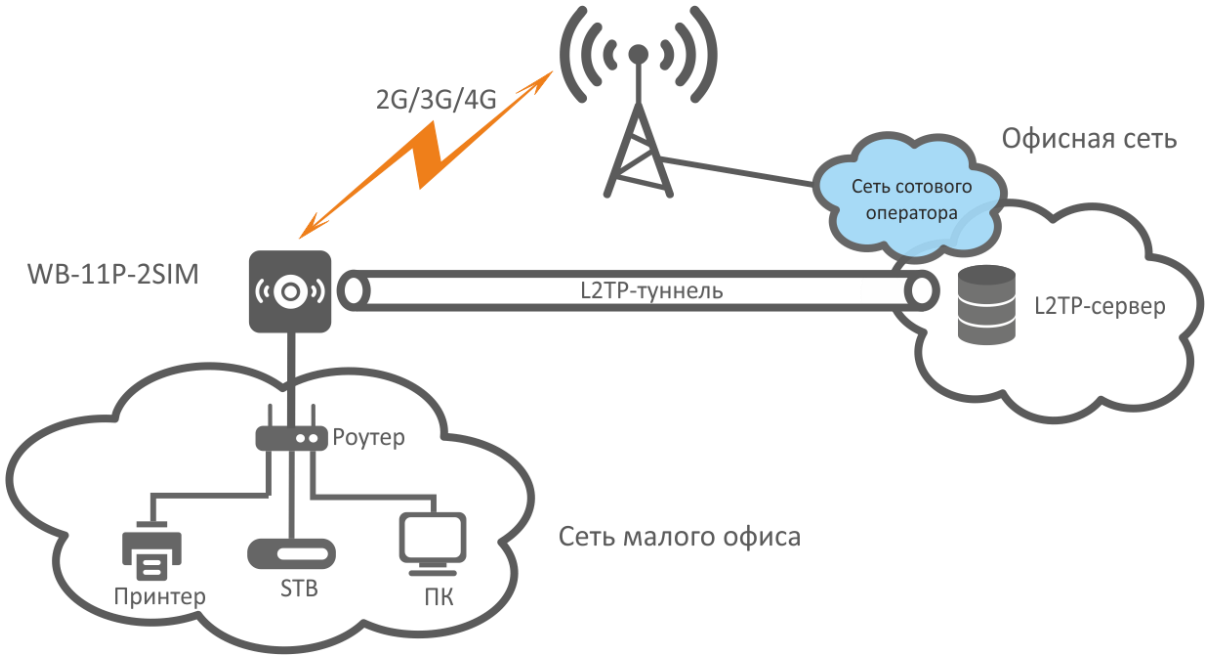


Схема 5

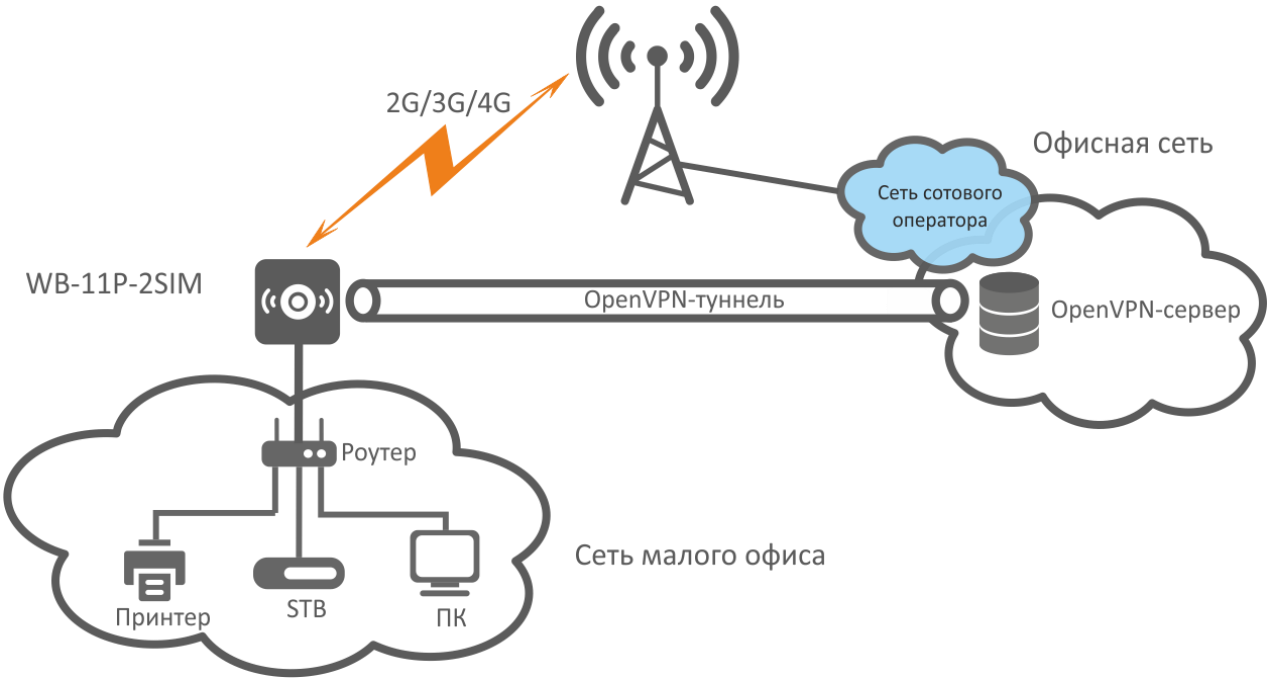


Рисунок 1 – Функциональные схемы применения WB-10P/WB-11P

2.4 Структура и принцип работы изделия

Терминал *WB-10P/WB-11P* состоит из следующих подсистем:

- CPU, в состав которого входит:
  - Высокоинтегрированная система на кристалле (System-on-a-Chip – SoC) Realtek RTL8954ES, включающая в себя процессор, гигабитный коммутатор со встроенными PHY, аппаратную акселерацию трафика L2/L3/L4, USB 2.0 порты, PCI-E контроллеры;
  - Flash-память – 32MB;
  - Оперативная память – 128MB (DDR3);
- Ethernet-модуль: 10/100/1000BASE-T;
- 2 USB Host порта.

Структурная схема устройств приведена на рисунке 2.

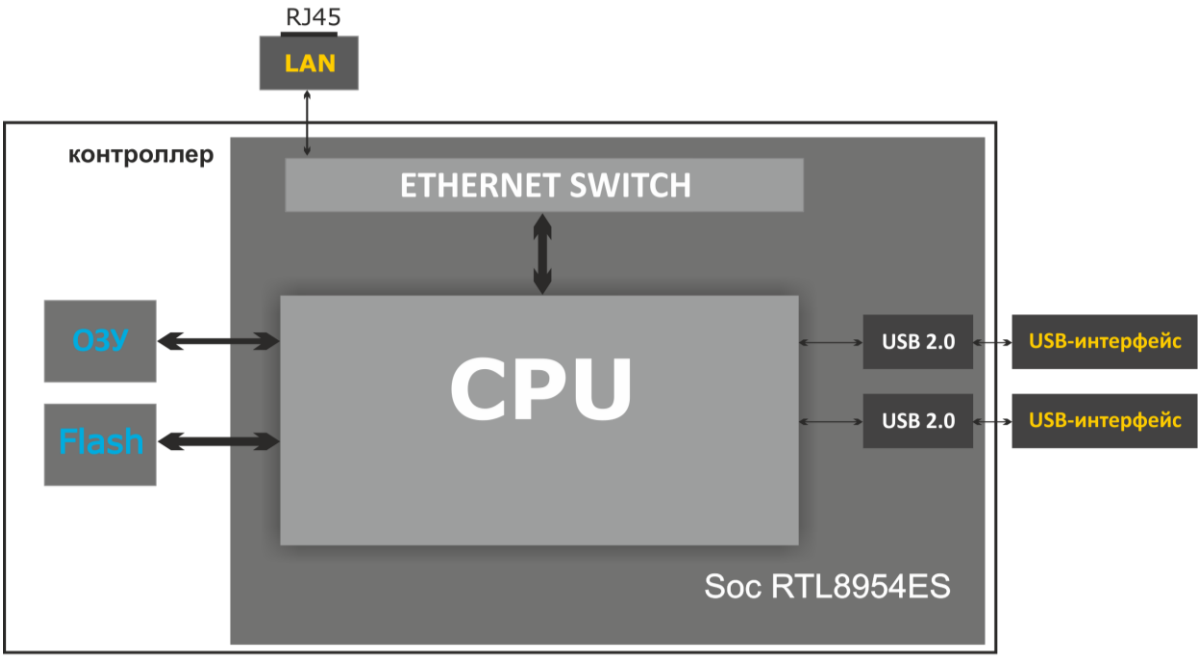


Рисунок 2 – Структурная схема WB-10P/WB-11P

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

2.5 Основные технические параметры

Основные технические параметры устройств приведены в таблице 2.

Таблица 2 – Основные технические параметры

Параметры интерфейса Ethernet	
Количество портов	1
Электрический разъем	RJ-45

Скорость передачи, Мбит/с	10/100/1000, автоопределение
Поддержка стандартов	BASE-T

Управление

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

Общие параметры

Питание		PoE 48В, Class 4.
Потребляемая мощность		не более 20 Вт
Рабочий диапазон температур		от -40 до +55°С
Относительная влажность при температуре 25°С		до 80%
Габариты	WB-10P	194x144x84 мм
	WB-11P	200x226x48 мм
Масса	WB-10P	0,65 кг
	WB-11P	0,90 кг

2.6 Конструктивное исполнение

Устройства имеют герметичный корпус класса защиты IP55 (WB-10P) и IP67 (WB-11P), обеспечивающий защиту от пыли и влаги.

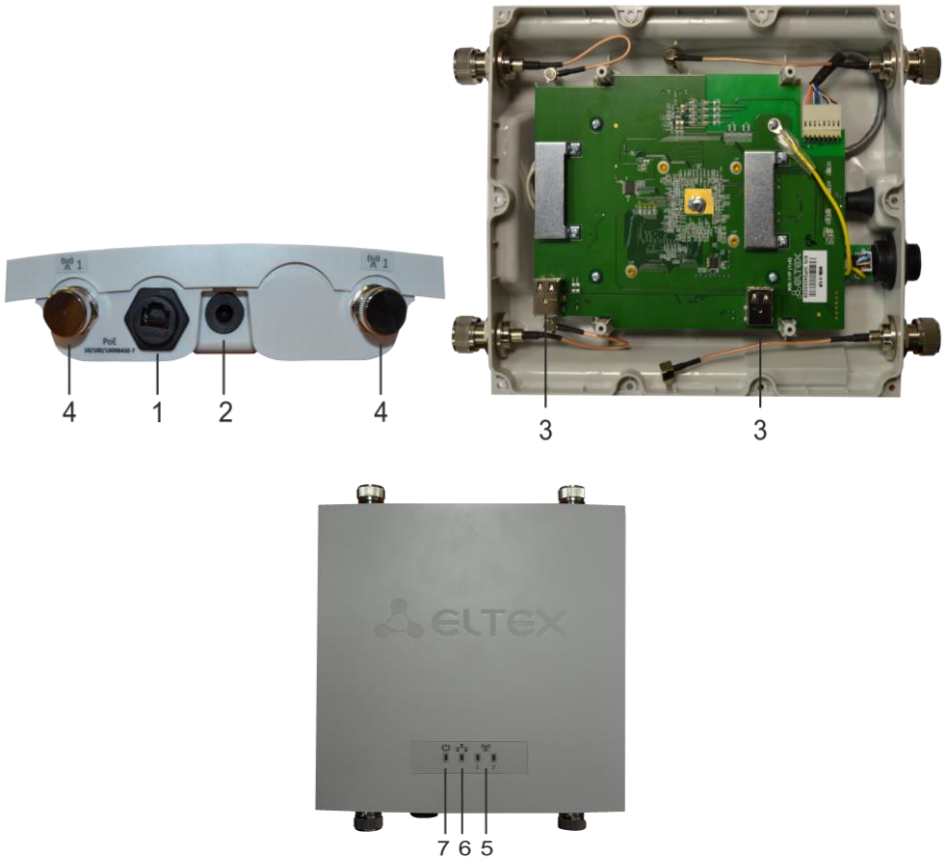


Рисунок 3 – Интерфейсы устройства WB-11P

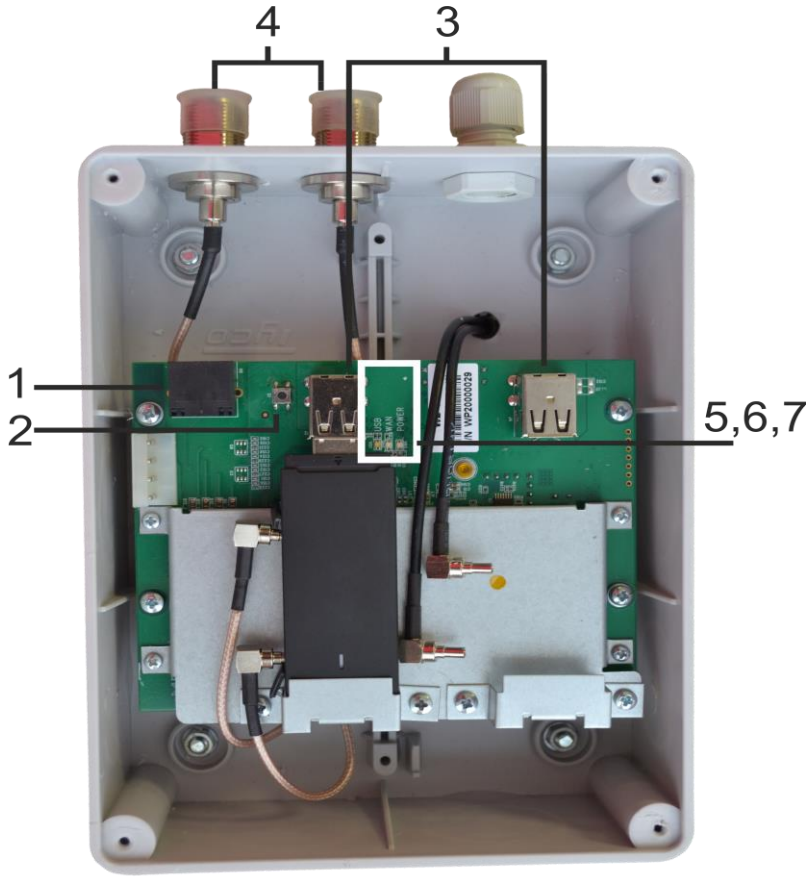


Рисунок 4 – Интерфейсы устройства WB-10P

На плате расположены следующие интерфейсы и световые индикаторы, таблица 3.

Таблица 3 – Описание интерфейсов и индикаторов платы

Элемент передней панели		Описание
1	Порт Ethernet. PoE (разъем X6)	Получение питания по фантомным цепям. Подключение к сети Ethernet.
2	Кнопка S1	Функциональная кнопка. Для перезагрузки устройства или сброса к заводским настройкам.
3	Порт USB1/USB2 (разъемы J3/J4)	Для подключения USB-модемов
4	Разъемы Cable N (female)	Для подключения внешних антенн
5	Индикатор USB	Индикатор подключенного USB модема
6	Индикатор WAN	Индикатор режимов работы порта Ethernet
7	Индикатор Power	Индикатор питания и статуса работы устройства

2.7 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов, расположенных на передней панели. Перечень состояний индикаторов приведен в таблице 4.

Таблица 4 – Световая индикация состояния устройств серии WB-10P/WB-11P

Индикатор	Состояние индикатора	Состояние устройства
WAN	горит зеленым (10, 100Mbps)/ оранжевым (1000 Mbps)	установлено соединение между станционным терминалом и абонентским устройством на

		скорости 10/100 или 1000 Мбит/с соответственно
	Мигает	процесс пакетной передачи данных через порт Ethernet
USB	зеленый, горит	Хотя бы один из USB-модемов подключен
	не горит	Отключены все USB-модемы
1[1]	зеленый, горит	В USB-порт 1 установлен USB-модем
	не горит	В USB-порт 1 не установлен USB-модем
2[1]	зеленый, горит	В USB-порт 2 установлен USB-модем
	не горит	В USB-порт 2 не установлен USB-модем
Power	зеленый, горит постоянно	включено питание устройства, нормальная работа
	оранжевый, горит постоянно	отсутствует выход в Интернет
	красный, горит постоянно	загрузка устройства, сброс устройства к заводским настройкам
	синий[1]	Включен нагревательный элемент

2.8 Сброс к заводским настройкам

Для запуска устройства с заводскими настройками необходимо в загруженном состоянии нажать и удерживать функциональную кнопку «S1» (расположена в нижней части корпуса правее ethernet интерфейса за герметичной резиновой вставкой. Для нажатия кнопки используйте любой тупоконечный предмет подходящего диаметра и длины и надавите им на дно резиновой вставки до характерного щелчка кнопки), пока индикатор «Power» не загорится красным цветом. Произойдет автоматическая перезагрузка устройства. При заводских установках устройство доступно через порт Ethernet по адресу *192.168.1.1,* маска подсети – *255.255.255.0*; имя пользователя/пароль для доступа через Web-интерфейс: admin/password. По умолчанию на проводном интерфейсе включен DHCP сервер.

2.9 Комплект поставки

В базовый комплект поставки устройства входят:

- терминал WB-10P/WB-11P;
- руководство по установке и настройке.

[1] Только для устройств WB-11P

3 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

Конфигурирование устройств показано на примере WB-11P. Конфигурирование устройства WB-10P производится аналогично.

3.1 Начало работы

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

1. Откройте Web-браузер (программу-просмотрщик гипертекстовых документов), например, Firefox, Opera, Chrome.

2. Введите в адресной строке браузера IP-адрес устройства, предварительно настроив статический IP-адрес на ПК из подсети 192.168.1.0/24 или убедившись, что ПК получил по DHCP IP-адрес из подсети 192.168.1.0/24;

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

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

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

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

3.2 Пользователи

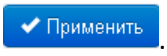
На устройстве существует только один пользователь - **admin**. Пользователь **admin** (пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек и полный мониторинг состояния устройства.

Для выхода пользователя из системы, нажмите на кнопку «*Выход*». Текущая сессия пользователя будет завершена, отобразится окно авторизации:

3.3 Применение конфигурации и отмена изменений

1. Применение конфигурации

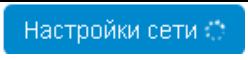
По нажатию на кнопку «Применить» происходит сохранение конфигурации во flash-память устройства и применение новых настроек. Все настройки вступают в силу без перезагрузки устройства.

Кнопка «Применить» в меню расширенных настроек имеет вид: 

.

В Web-интерфейсе реализована визуальная индикация текущего состояния процесса применения настроек, таблица 5.

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».

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

2. Отмена изменений

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

Кнопка отмены изменений в меню расширенных настроек имеет вид: Отмена.

3.4 Настройки

3.4.1 Основные элементы Web-интерфейса

На рисунке 5 представлены элементы навигации Web-конфигуратора в режиме настроек.

Рисунок 5 – Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса разделено на семь областей:

1. Имя пользователя, под которым был осуществлен вход в систему, а также кнопка завершения сеанса работы в Web-интерфейсе (*«Выход»*) под данным пользователем.
2. Вкладки меню группируют вкладки подменю по категориям: Мониторинг, Сеть, Система.
3. Вкладки подменю служат для управления полем настроек.
4. Поле настроек устройства, которое базируется на выборе пользователя, предназначено для просмотра настроек устройства и ввода конфигурационных данных.
5. Кнопки управления конфигурацией.

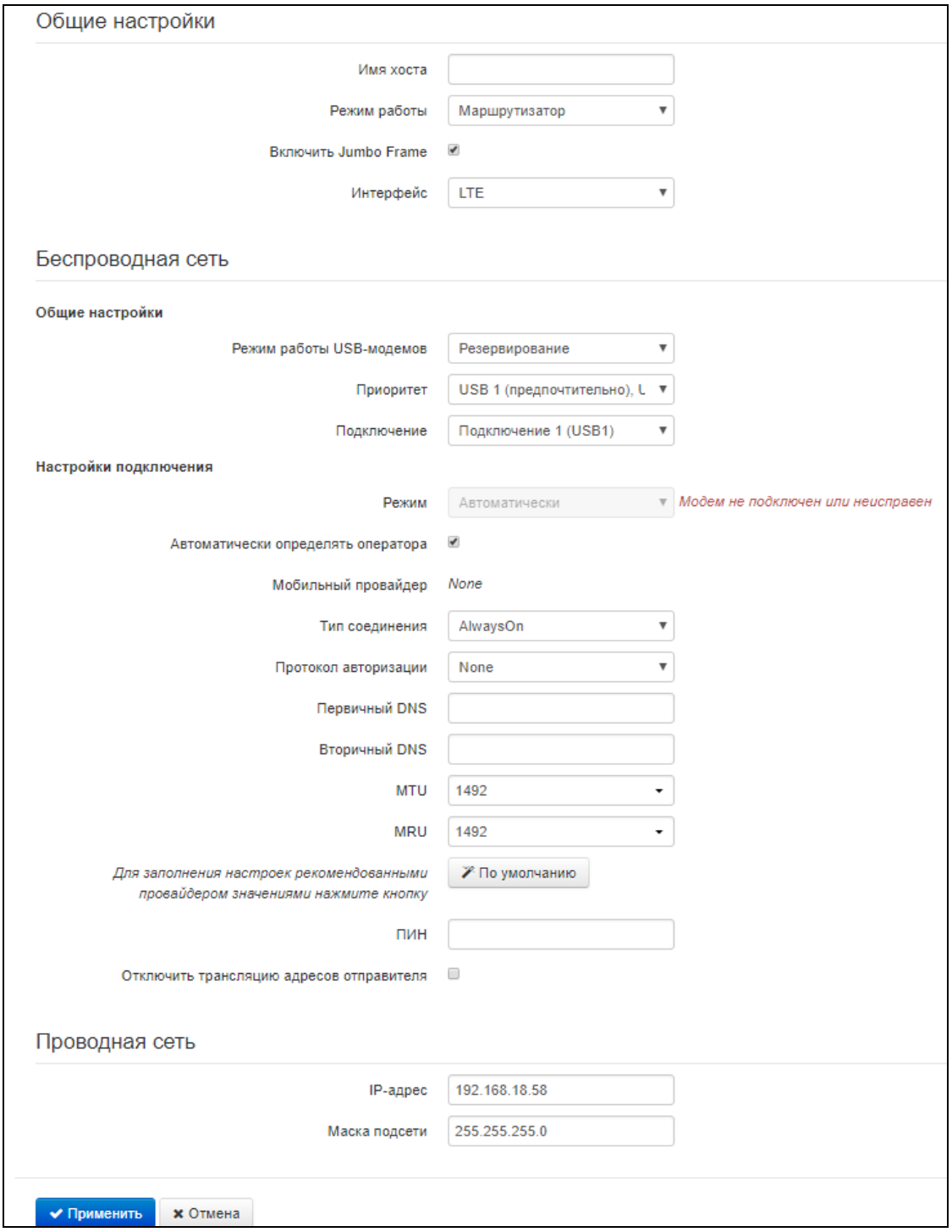
6. Информационное поле, в котором отображается версия ПО, версия Web-интерфейса.

3.4.2 Меню «Сеть»

В меню «Сеть» выполняются все основные сетевые настройки устройства.

3.4.2.1 Подменю «Интернет»

В подменю «Интернет» выполняется конфигурирование подключения к беспроводной сети передачи данных операторов сотовой связи и локальной сети со статической или динамической (в режиме моста) настройкой IP-адреса.



Общие настройки

- *Имя хоста* – сетевое имя устройства.
- *Режим работы* – режим работы устройства:
  - Маршрутизатор – между проводным и беспроводным интерфейсами устанавливается режим маршрутизатора;
  - Мост – между проводным и беспроводным интерфейсами устанавливается режим моста: данные передаются прозрачно из проводной в беспроводную сеть и обратно по протоколу GRE (настройка GRE описана в разделе 3.4.2.2 Подменю «GRE»).

  При выборе режима работы «Маршрутизатор» IP-адрес интерфейса проводной сети будет иметь статические настройки; в режиме «Мост» - статические или по протоколу DHCP.
- *Включить Jumbo Frame* – при выбранном флаге включена поддержка больших кадров;
- *Интерфейс* – интерфейс, через который будет происходить передача трафика из проводной сети в беспроводную в режиме «Маршрутизатор».

Беспроводная сеть

- Режим работы USB-модемов – позволяет настроить режим работы с USB-модемами для обеспечения защиты от неработоспособного беспроводного канала или объединения беспроводных каналов с целью увеличения общей пропускной способности:
  - *Резервирование* – режим работы, при котором выбирается основной и резервный USB-модем согласно приоритету. Переход на резервный модем осуществляется при прекращении связи по основному модему:
    - *Приоритет* – выбор приоритетного модема, который подключен к порту USB1 или USB2:
      - *USB1 (предпочтительно), USB2* – если подключены оба модема, то первым соединение устанавливает модем, подключенный к порту USB1, а при отсутствии связи через него или если он был извлечен/не установлен, соединение устанавливается через модем, подключенный к порту USB2;
      - *USB2 (предпочтительно), USB1* – если подключены оба модема, то первым соединение устанавливает модем, подключенный к порту USB2, а при отсутствии связи через него или если он был извлечен/не установлен, соединение устанавливается через модем, подключенный к порту USB1.
  - *Агрегация* – режим работы при котором одновременно активны оба USB-модема для увеличения общей пропускной способности в беспроводной сети. Данные через них передаются согласно весу подключения:
    - *Вес подключения через USB1/2* – коэффициент, условно определяющий количество пакетов из общего потока данных, которые будут передаваться через модем, подключенный к порту USB1 и USB2.
  - *Подключение* – номер подключения (в скобках указан номер порта USB с подключенным модемом, соответствующий выбранному подключению), для которого производится настройка подключения (USB1 — разъем J3, USB2 — разъем J4).

Настройки подключения

- *Режим* – настройка режима работы USB-модема (2G/3G/4G/Автоматически). Настройка является частью конфигурации USB-модема и при установке другого модема будет считана из его конфигурации автоматически при следующем открытии страницы или ее обновлении:

  - *2G/3G/4G* – модем будет производить попытку установления подключения к сети оператора используя только технологию 2G, 3G или 4G, соответственно;
  - *Автоматически* – модем автоматически определяет оптимальную технологию для подключения из поддерживаемых им или доступных в сети оператора. Со временем используемая технология может изменяться автоматически.

Если модем не поддерживает одну или несколько технологий из списка, то выбор этого режима подключения будет недоступен.

- *Автоматически определять оператора* – при выбранном флаге оператор, SIM-карта которого установлена в модем, будет определяться автоматически и для него будут установлены настройки по умолчанию. (Смена настроек по умолчанию для операторов описана в ПРИЛОЖЕНИИ Б)

- *Мобильный провайдер* – имя провайдера, предоставляющего доступ к сети 2G/3G/4G. Из списка Вы можете выбрать одного из шести мобильных операторов (стандартные настройки каждого из них хранятся в памяти устройства), присутствующих на территории Российской Федерации: Мегафон, Билайн, МТС, Скайлинк, Теле2, Yota. Нажав на кнопку «По умолчанию» произойдёт заполнение настроек подключения параметрами выбранного провайдера. Если настройки провайдера в Вашем регионе отличаются от предложенных, отредактируйте их в соответствии с необходимыми значениями.

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

  Если стоит флаг «Автоматически определять оператора», в поле отображается провайдер, который определился для установленной SIM-карты.

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

- *Тип соединения* – в зависимости от выбранного значения PPP-сессия поднята всегда (AlwaysOn), сессия инициируется при необходимости передачи трафика (OnDemand).

- *Таймаут неактивности, с* – промежуток времени, по истечению которого происходит разрыв PPP-сессии по неактивности в режиме OnDemand;

- *Протокол авторизации* – протокол, который будет использоваться для идентификации при подключении к беспроводной сети;

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

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

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

- *Дополнительные параметры инициализации* – параметры для подключения к сети мобильной связи (пример: AT+CGDCONT=1,IP). В этой строке нельзя использовать кавычки;

- *APN* – имя точки доступа, используется для подключения к сети мобильной связи (пример*:* Internet – для Мегафон);

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

- *MTU/MRU* – максимальный размер блока данных, передаваемых/принимаемых по сети, рекомендуемое значение – 1492;

- *ПИН* – для ввода PIN-кода SIM-карты, установленной в USB-модем, если требуется. По умолчанию у большинства операторов сотовой связи проверка PIN-кода SIM-карты отключена. В таком случае поле следует оставить пустым;

- *Отключить трансляцию адресов отправителя* – при установленном флаге отключена подмена адреса источника отправителя пакета из локальной подсети (отключение masquerading). Поле доступно при выбранном режиме работы «Маршрутизатор».

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

Проводная сеть

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

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

    - IP-адрес – установка IP-адреса проводного интерфейса устройства;
    - Маска подсети – маска внешней подсети.

  - *DHCP* – режим работы, при котором IP-адрес и маска подсети будут получены от DHCP-сервера автоматически.

    Поддерживаемые опции:

    - 1 – маска сети;
    - 12 – сетевое имя устройства;
    - 15 – доменное имя;
    - 33 – статические маршруты;
    - 42 – адрес NTP-сервера;
    - 43 – специфичная информация производителя;
    - 66 – адрес TFTP-сервера;
    - 67 – имя файла программного обеспечения для загрузки по TFTP с сервера из опции 66;
    - 121 – бесклассовые статические маршруты.

Для протокола DHCP имеется возможность задать необходимое значение опции 60.

- *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля *Vendor ID (опция 60).* При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.
  Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат: **[VENDOR:**производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**][SN:**серийный номер**][MAC:**MAC-адрес интерфейса Ethernet**][VERSION:**версия программного обеспечения**]**

Пример:

[VENDOR:Eltex][DEVICE:WB-10P][HW:1.0][SN:WP20000032][MAC:A8:F9:4B:16:0E:60][VERSION:1.0.0.251]

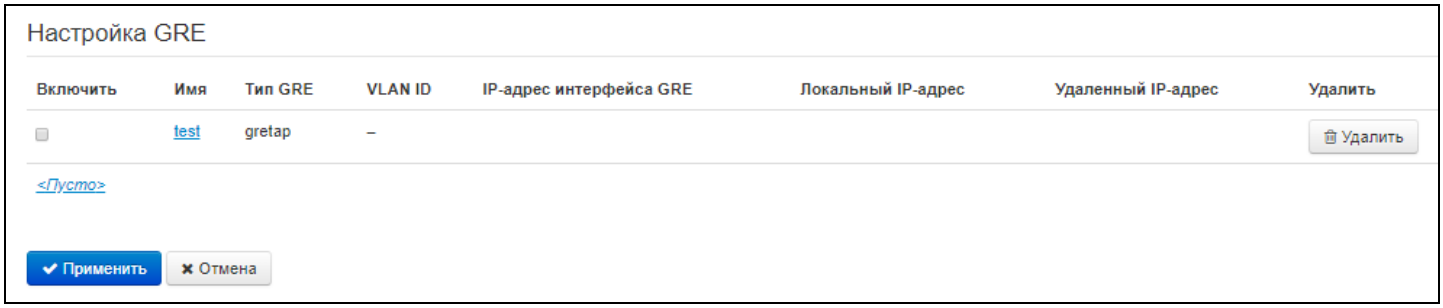
В режиме работы устройства «Маршрутизатор» доступен только протокол Static.

3.4.2.2 Подменю «GRE»

В данном разделе производится настройка протокола GRE для туннелирования данных локальных подсетей через корпоративную сеть или сеть интернет.

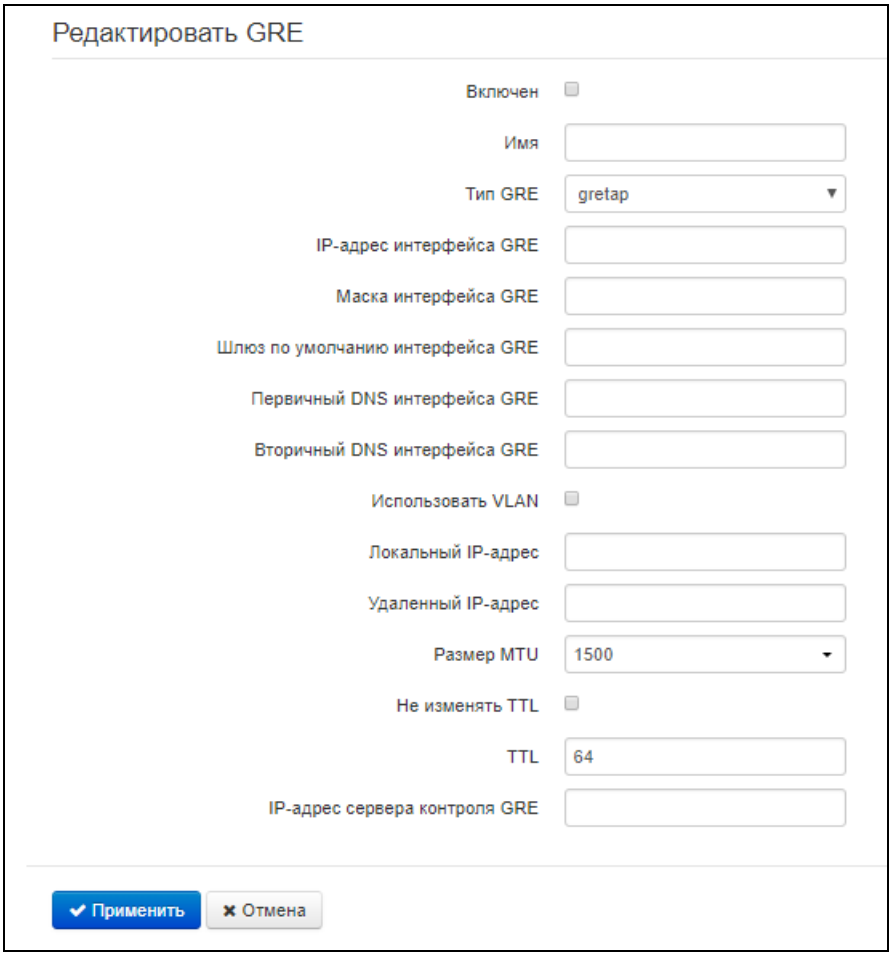
Чтобы включить или выключить туннели, следует отметить нужную конфигурацию в графе «Включить» и нажать кнопку «Применить».

С помощью кнопки «Удалить» можно удалять существующие туннели.



Настройка GRE

Для добавления нового туннеля нажмите на поле «Пусто» (либо нажмите на название существующего туннеля для его редактирования) и заполните следующие поля в появившемся окне:



- *Включен* – флаг, который активирует использование туннеля;
- *Имя* – имя интерфейса;
- *Тип GRE* – позволяет настроить тип GRE туннеля;
- *IP-адрес интерфейса GRE* – установка IP-адреса устройства в туннеле;
- *Маска интерфейса GRE* – маска подсети интерфейса GRE;
- *Шлюз по умолчанию интерфейса GRE* – IP-адрес дефолтного шлюза интерфейса GRE;
- *Первичный DNS интерфейса GRE, Вторичный DNS интерфейса GRE* – адреса серверов доменных имён (используется для определения IP-адреса устройства по его доменному имени) для интерфейса GRE. Данные поля можно оставить пустыми, если в них нет необходимости.
- *Использовать VLAN* – при установленном флаге разрешается передавать данные 802.1q;
- *VLAN ID* – идентификационный номер VLAN, принимает значения от 1 до 4095; не должен совпадать с идентификаторами VLAN других сервисов;
- *Локальный IP-адрес* – собственный IP-адрес устройства, полученный на беспроводном интерфейсе;

- *Удаленный IP-адрес* – IP-адрес встречного устройства, на котором будет терминироваться туннель GRE;
- *Размер MTU* – максимальный размер блока данных, передаваемых через туннель;
- *Не изменять TTL* – при установленном флаге значение заголовка TTL, передаваемого по протоколу GRE, не инкрементируется;
- *TTL* – позволяет задать желаемое значение заголовка TTL передаваемого пакета GRE;
- *IP-адрес сервера для контроля GRE* – IP-адрес, на который будут отправляться запросы для проверки активности туннеля. Если поле пустое – контроль GRE не используется.

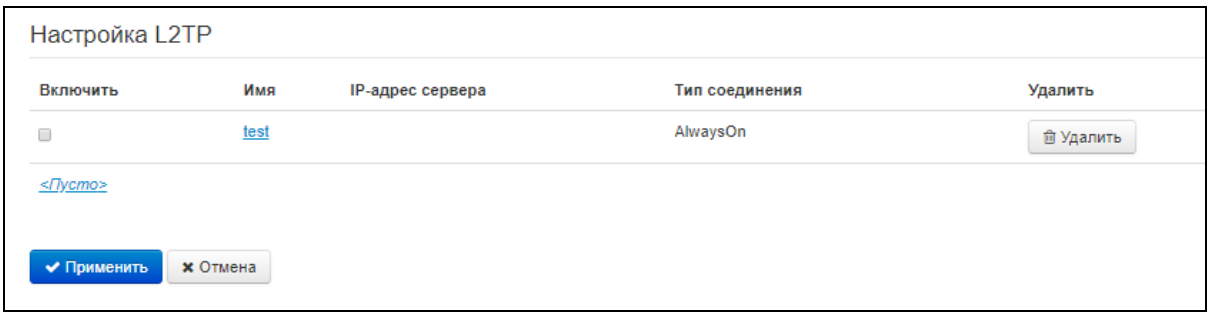
Для записи настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

3.4.2.3 Подменю «L2TP»

В данном разделе производится настройка L2TP-туннелей.

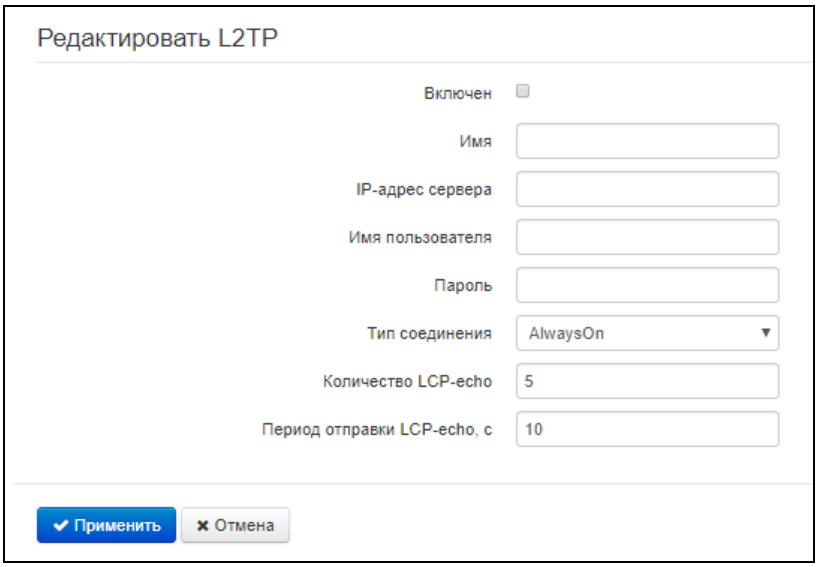
Чтобы включить или выключить туннели, нужно отметить нужную конфигурацию в графе «Включить» и нажать кнопку «Применить».

С помощью кнопки «Удалить» можно удалять существующие туннели.



Настройка L2TP

Для добавления нового туннеля нажмите на поле «Пусто» (либо нажмите на название существующего туннеля для его редактирования) и заполните следующие поля в появившемся окне:



- *Включен* – флаг, который активирует использование туннеля;
- *Имя* – имя интерфейса;
- *IP-адрес сервера* – установка IP-адреса сервера L2TP;
- *Имя пользователя* – имя пользователя для авторизации на сервере L2TP;
- *Пароль* – пароль для авторизации на сервере L2TP;
- *Тип соединения* – в зависимости от выбранного значения L2TP-сессия поднята всегда (AlwaysOn), сессия инициируется при необходимости передачи трафика (OnDemand) или сессия инициализируется вручную при помощи кнопки «Connect» в таблице настройки туннелей (Manual);
- *Таймаут неактивности, с* – промежуток времени, по истечению которого происходит разрыв L2TP -сессии по неактивности в режиме OnDemand;
- *Количество LCP-echo* – количество неотвеченных LCP-запросов, после которых происходит разрыв L2TP -сессии;
- *Период отправки LCP-echo*, с – период отправки LCP-запросов.

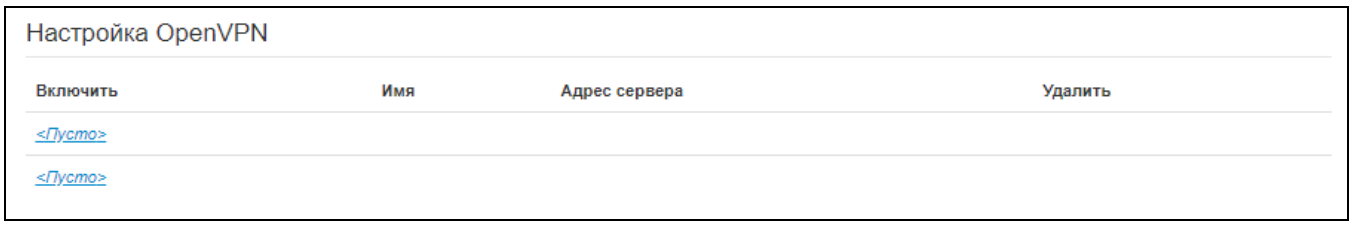
Для записи настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

3.4.2.4 Подменю «OpenVPN»

В данном разделе производится настройка OpenVPN-туннелей.

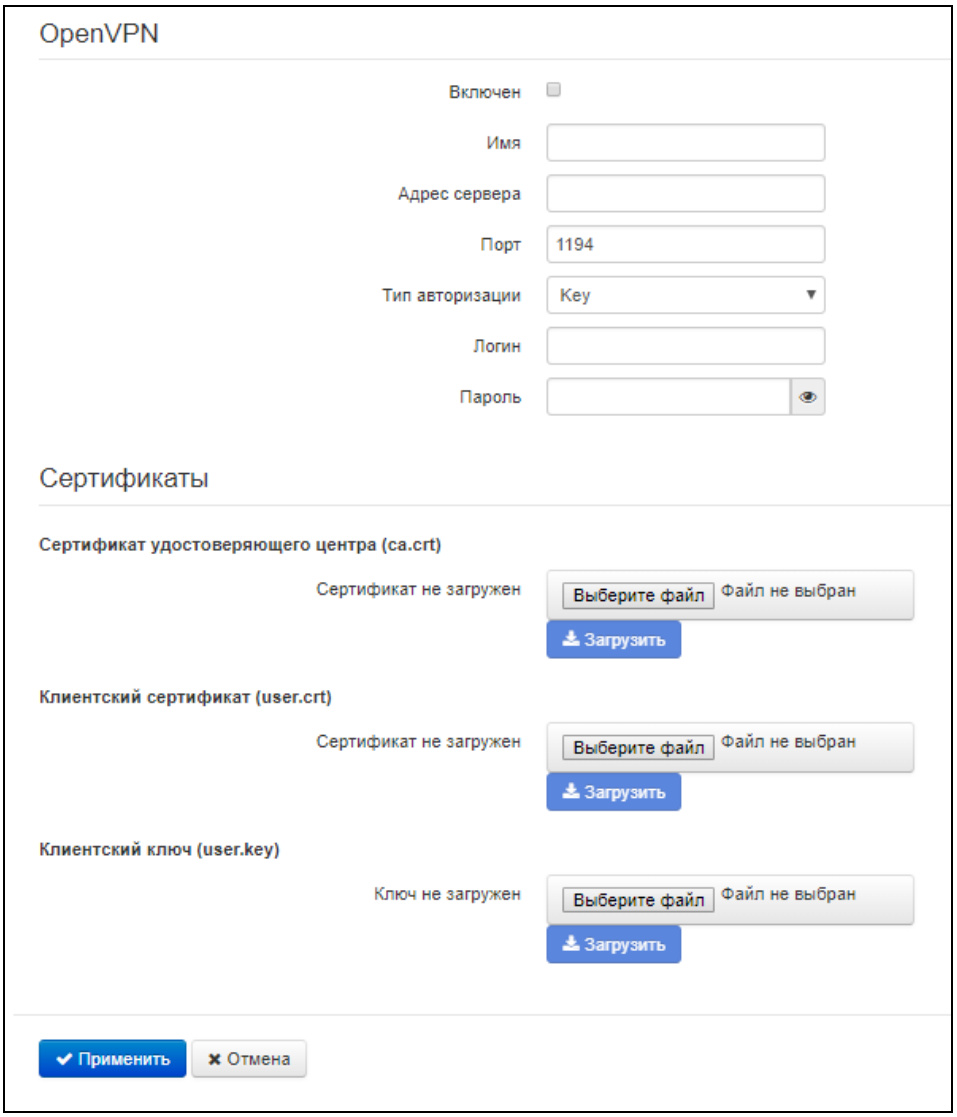
Чтобы включить или выключить туннели, нужно отметить нужную конфигурацию в графе «Включить» и нажать кнопку «Применить».

С помощью кнопки «Удалить» можно удалять существующие туннели.



Настройка OpenVPN

Для добавления нового туннеля нажмите на поле «Пусто» (либо нажмите на название существующего туннеля для его редактирования) и заполните следующие поля в появившемся окне:



- *Включен* – флаг, который активирует использование туннеля;
- *Имя* – имя интерфейса;
- *Адрес сервера* – установка IP-адреса сервера OpenVPN;
- *Порт* – порт, на который будут отправляться запросы;
- *Тип авторизации* – в зависимости от выбранного значения авторизация будет проходить при помощи связки логин-пароль и сертификата удостоверяющего центра (User), либо при помощи двух сертификатов и клиентского ключа (Key);
- *Логин* – имя пользователя для авторизации на сервере OpenVPN;
- *Пароль* – пароль для авторизации на сервере OpenVPN;
- *Сертификат удостоверяющего центра* – для загрузки сертификата необходимо нажать на кнопку *«Выберите файл»*, выбрать файл на локальном компьютере и нажать кнопку *«Загрузить»*;

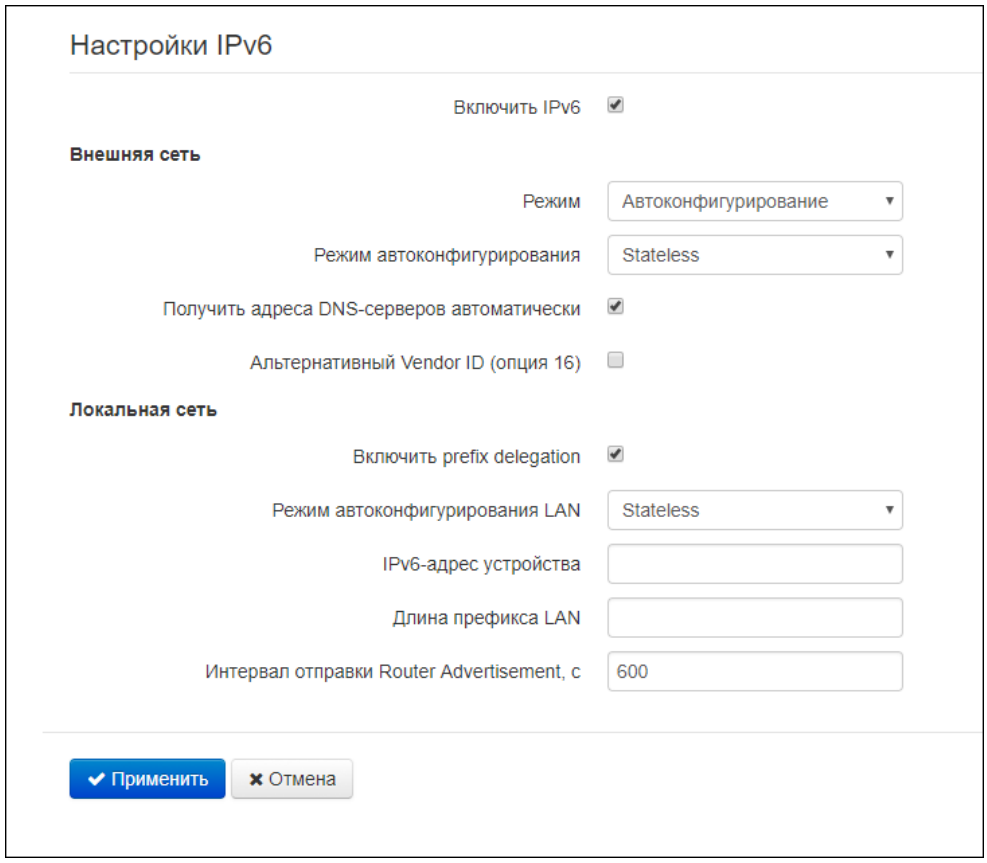
- *Клиентский сертификат* – для загрузки сертификата необходимо нажать на кнопку *«Выберите файл»*, выбрать файл на локальном компьютере и нажать кнопку *«Загрузить»*;
- *Клиентский ключ* – для загрузки сертификата необходимо нажать на кнопку *«Выберите файл»*, выбрать файл на локальном компьютере и нажать кнопку *«Загрузить»*;

После загрузки сертификатов их можно просмотреть, нажав на кнопку *«Просмотр»*.

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

3.4.2.5 Подменю «IPv6»[1]

В подменю «IPv6» выполняется конфигурирование подключения к внешней сети и локальной сети по протоколу IPv6.



Настройки IPv6

- *Включить IPv6* – позволяет включить или отключить использование протокола IPv6.

Внешняя сеть

- *Режим* – способ подключения устройства к внешней сети:
  - *Static* – подключение к сети Интернет через протокол IPv6 осуществляется по настройкам, заданным пользователем;

[1] В текущей версии программного обеспечения IPv6 не поддерживается.

- *Автоконфигурирование* – подключение к сети Интернет через протокол IPv6 осуществляется по настройкам, полученным через один из режимов автоконфигурирования: SLAAC, Stateless, Stateful.

Настройки подключения к внешней сети

1. При выборе режима **«Static»** будут доступны следующие настройки:

- *Внешний IPv6-адрес устройства* – статический IPv6-адрес устройства, с которым будет осуществляться доступ к сети Интернет;
- *Длина префикса* – аналог маски подсети в IPv4. Определяет, какая часть адреса определяет подсеть, а какая хост. Максимальное значение длины префикса – 128, в настоящее время чаще всего используется префикс 64;
- *IPv6-Шлюз по умолчанию* – IPv6-адрес шлюза, используемого по умолчанию;
- *IPv6*-Первичный DNS – IPv6-адрес первичного DNS-сервера;
- *IPv6*-Вторичный DNS – IPv6-адрес вторичного DNS-сервера.

2. При выборе режима **«Автоконфигурирование»** будут доступны следующие настройки:

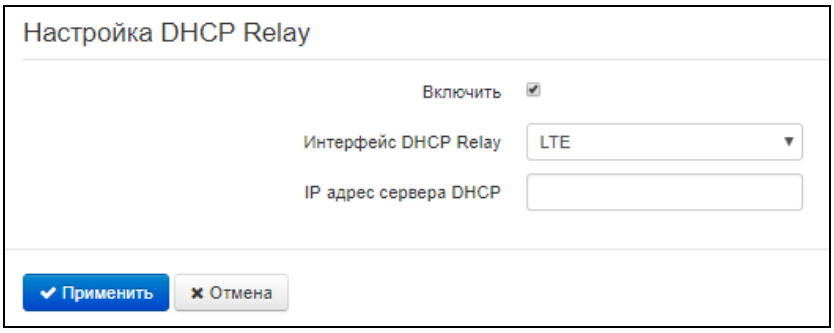
- *Режим автоконфигурирования* – способ получения настроек подключения устройства к внешней сети:
  - *SLAAC* – получение настроек IPv6 через сообщение «Router Advertisement» протокола ICMPv6;
  - *Stateless* – получение настроек IPv6 через сообщение «Router Advertisement (RA)» протокола ICMPv6, запрос недостающих параметров через DHCPv6;
  - *Stateful* – получение настроек IPv6 через протокол DHCPv6.
- *Получить адреса DNS-серверов автоматически* – способ получения адреса DNS-серверов: автоматически или ввести самостоятельно, как при выбранном режиме «Static»;
- *Альтернативный Vendor ID (опция 16)* – настройка аналогична настройке в IPv4 (см. пункт 3.4.2.1 Подменю «Интернет»), доступна при выбранном режиме автоконфигурирования «Stateless» или «Stateful» или включенной настройки «Разрешить prefix delegation».

Локальная сеть

- *Разрешить prefix delegation* – разрешить выдачу хостам локальной сети IPv6-адресов из подсети, полученной через автоконфигурирование во внешней сети;
- *Режим автоконфигурирования LAN* – выбор способа получения настроек подключения хостов к локальной сети:
  - *SLAAC* – получение настроек IPv6 через сообщение «Router Advertisement» протокола ICMPv6;
  - *Stateless* – получение настроек IPv6 через сообщение «Router Advertisement (RA)» протокола ICMPv6, запрос недостающих параметров через DHCPv6;
  - *Stateful* – получение настроек IPv6 через протокол DHCPv6;
  - *Off* – автоконфигурирование отключено, сетевые настройки IPv6 нужно задавать на хостах в ручную.
- *IPv6-адрес устройства* – IPv6-адрес устройства в локальной сети;

- *Длина префикса LAN* – определяет длину префикса локальной сети;
- *Интервал отправки Router Advertisement, с* – интервал времени, в течение которого устройства отправляется сообщение RA протокола ICMPv6 с настройками сети для хостов.

3.4.2.6 Подменю «DHCP Relay»

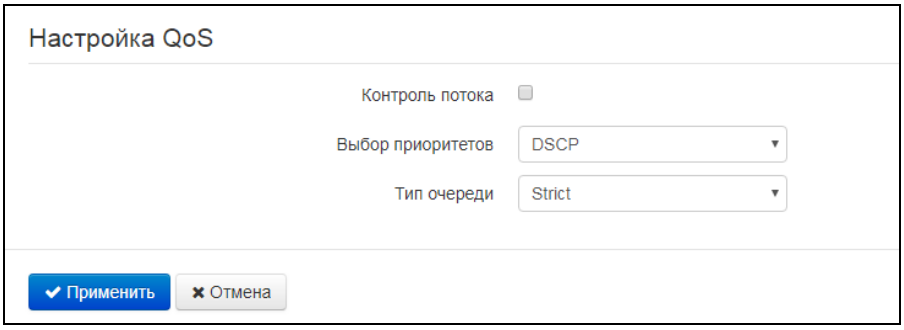


Настройка DHCP Relay

- *Включить* – позволяет включить или отключить использование настройки DHCP Relay.
- *Интерфейс DHCP Relay* – позволяет выбрать интерфейс, через который будет осуществляться ретрансляция DHCP-пакетов.
- *IP-адрес сервера DHCP* – позволяет задать адрес хоста, на котором запущен сервер DHCP.

3.4.2.7 Подменю «QoS»

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



Настройка QoS

- *Контроль потока* – включение/выключение контроля скорости, с которой потоки определенного вида трафика передаются во внешнюю сеть;

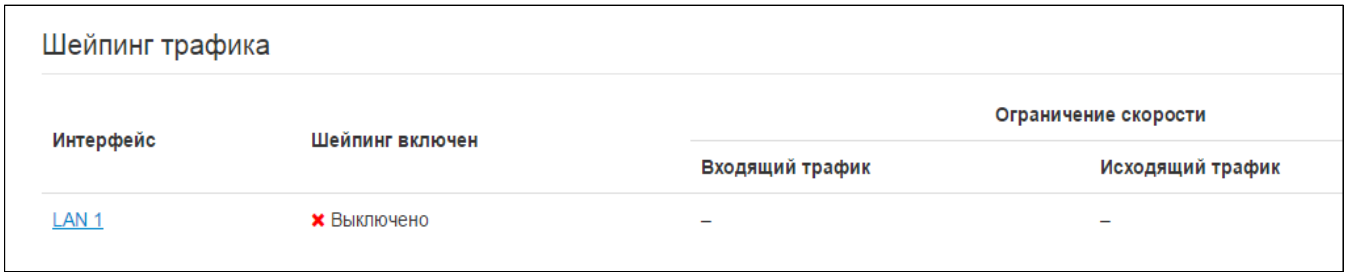
При включенном контроле потока настройки приоритетов недоступны

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

- *Тип очереди* – выбор дисциплины обслуживании 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.

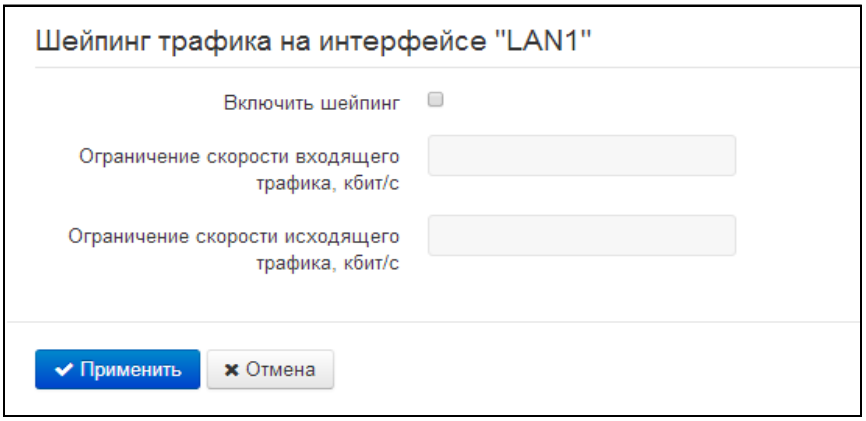
3.4.2.8 Подменю «Шейпинг трафика»

В подменю «Шейпинг трафика» можно ограничить входящую и исходящую скорости трафика на проводном интерфейсе.



Шейпинг трафика

Данное подменю представлено в виде таблицы, в которой напротив имени интерфейса указан статус шейпинга на нем и значения максимально разрешенных скоростей входящего и исходящего трафика. Для того чтобы перейти к настройкам определенного интерфейса, нажмите на его название.



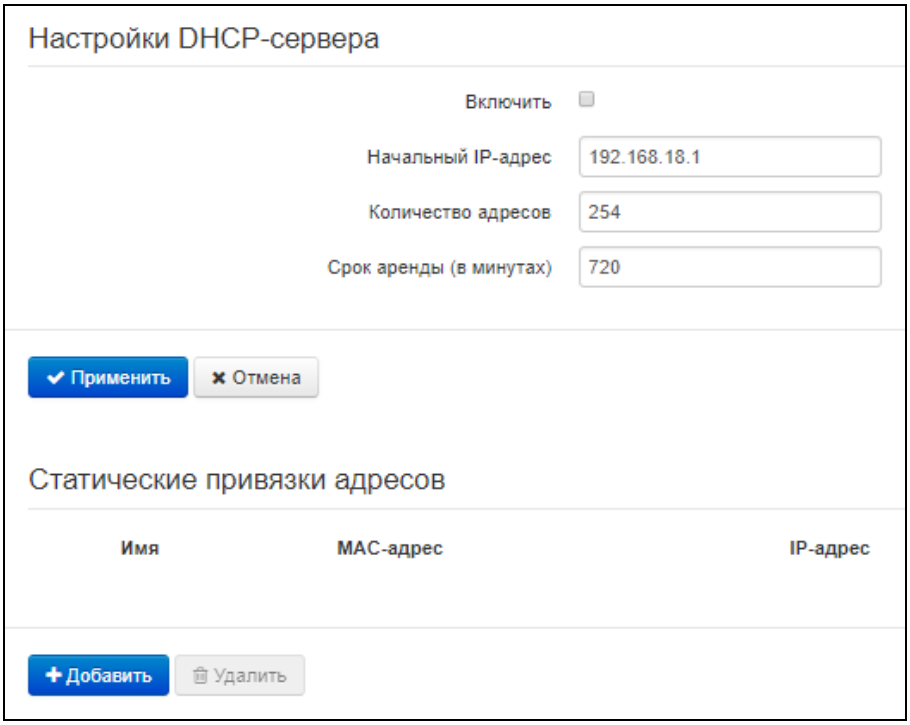
Шейпинг трафика на интерфейсе

- *Включить шейпинг* – при установленном флаге включено ограничение скорости входящего, исходящего трафика;
  - *Ограничение скорости входящего/исходящего трафика, кбит/с* – максимальная скорость входящего/исходящего трафика в кбит/с в диапазоне от 0 до 1048576 кбит/с, шаг изменения скорости входящего трафика составляет 16 кбит/с, а исходящего 64 кбит/с.

3.4.2.9 Подменю «DHCP-сервер»

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

Устройства *WB-10P* и *WB-11P* имеют возможность посредством протокола динамического конфигурирования (DHCP – Dynamic Host Configuration Protocol) автоматически назначать IP-адреса и необходимые для выхода в Интернет параметры компьютерам, подключенным к LAN-интерфейсу. Его использование позволяет избежать ограничений ручной настройки протокола TCP/IP. DHCP-сервер доступен для конфигурирования, только если сервис Интернет настроен в режиме маршрутизатора.



Настройки DHCP-сервера

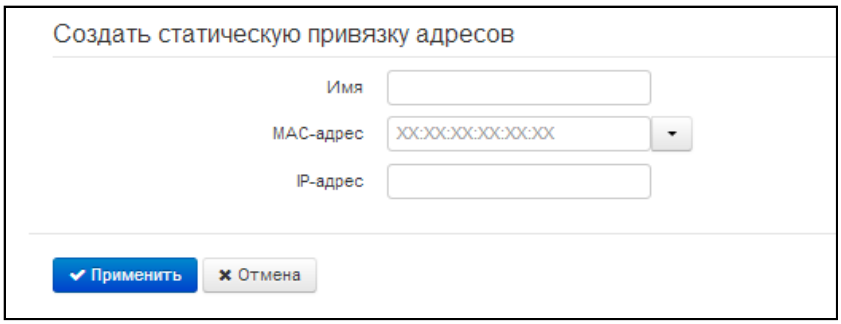
- *Включить* – при установленном флаге включить локальный DHCP-сервер;
- *Начальный IP-адрес* – начальный адрес пула IP-адресов;
- *Количество адресов* – количество адресов в пуле;
- *Срок аренды (в минутах)* – установка максимального времени использования подключенным устройством IP-адреса, назначенного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

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

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

Статические привязки адресов

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



- Имя – 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»*.

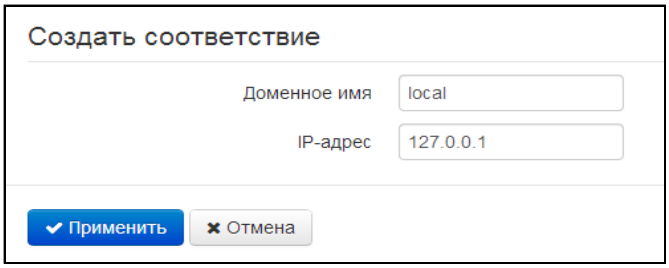
3.4.2.10 Подменю «Локальный DNS»

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

Локальный DNS позволяет шлюзу получить IP-адрес взаимодействующего устройства по его сетевому имени (хосту). В случае отсутствия сервера DNS в сегменте сети, которому принадлежит терминал, но при необходимости маршрутизации по сетевым именам, можно использовать «Локальный DNS». При этом необходимо знать установленные соответствия между именами узлов (хостов) и их IP-адресами.

Настройка узлов

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



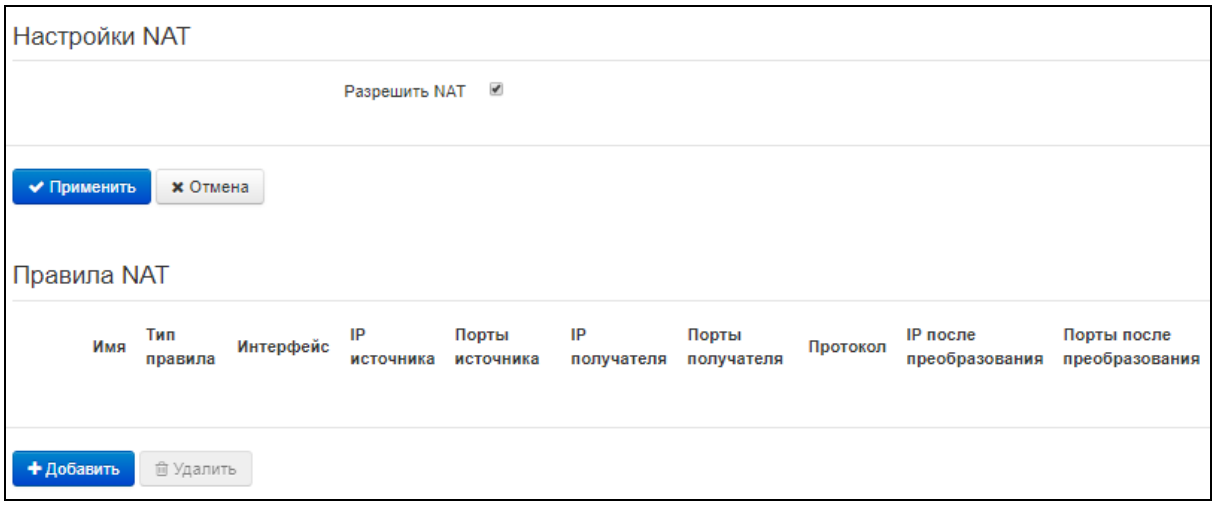
- Доменное имя – имя узла;
- IP-адрес – IP-адрес узла.

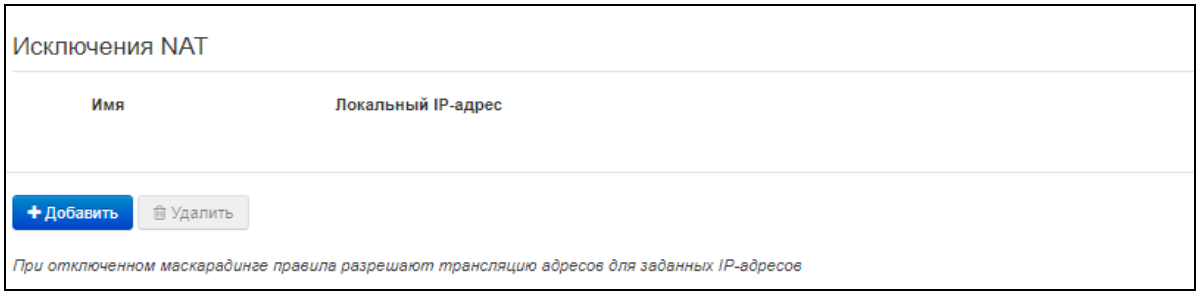
Нажмите кнопку *«Применить»* для создания соответствия IP-адрес – доменное имя. Для отмены изменений нажмите кнопку *«Отмена»*. Для удаления записи из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку *«Удалить»*.

3.4.2.11 Подменю «NAT и проброс портов»

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

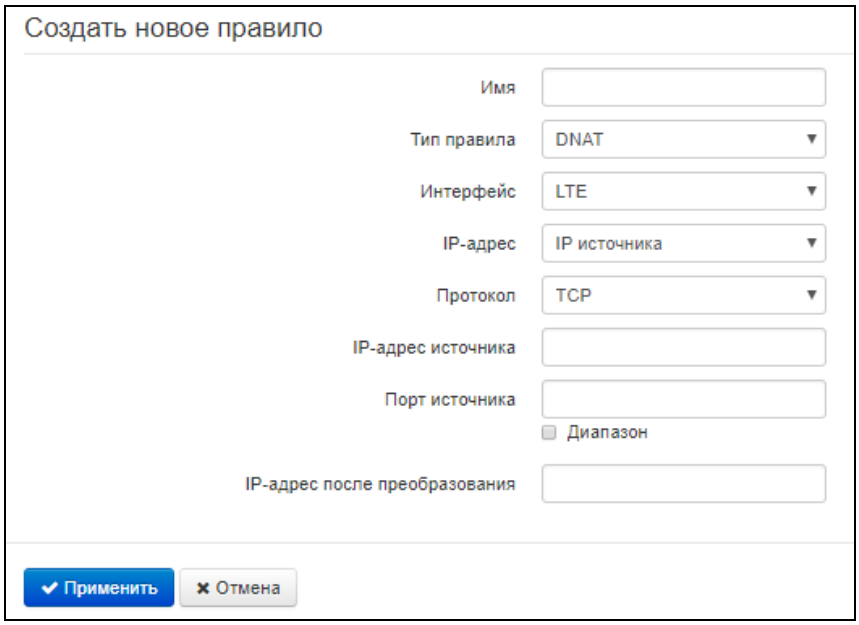
NAT – (Network Address Translation) режим трансляции сетевых адресов – позволяет преобразовывать IP-адреса и сетевые порты IP-пакетов. Проброс сетевых портов необходим, когда TCP/UDP-соединение с локальным (подключенным к LAN-интерфейсу) компьютером устанавливается из внешней сети. Данное меню настроек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





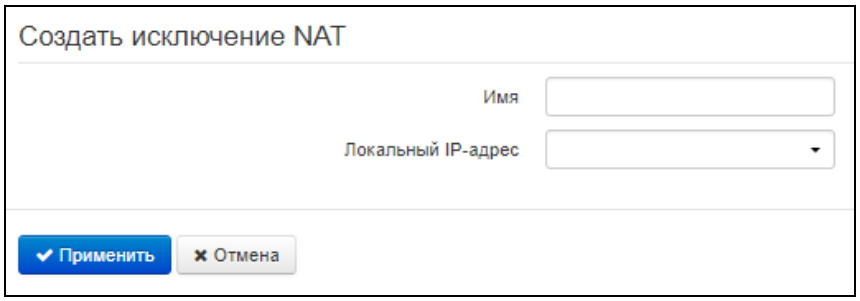
Настройка правила NAT

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



- *Имя* – название правила (поле обязательно для заполнения);
- *Тип правила* – выбор типа правила: SNAT, DNAT, MASQUERADE;
- *Интерфейс* – выбор интерфейса, на котором будет работать правило;
- *IP-адрес* – позволяет выбрать, по каким адресам будет определяться, что пакет попадает под данное правило;
- *Протокол* – выбор протокола пакета, попадающего под данное правило: TCP, UDP, TCP/UDP;
- *IP-адрес источника/IP-адрес получателя* – в зависимости от режима, выбранного в поле *«IP-адрес»*, можно указать адреса, по которым будет определяться, что пакет попадает под данное правило;
- *Порт источника/Порт получателя* – в зависимости от режима, выбранного в поле *«IP-адрес»*, можно указать порты, по которым будет определяться, что пакет попадает под данное правило;
- *Диапазон* – при установке данного флага, вместо одного порта можно задать диапазон;
- *IP-адрес после преобразования* – адрес, на который будет заменён адрес отправителя или адрес получателя, в зависимости от значения поля *«Тип правила»*.

Настройка исключения NAT



Для добавления нового исключения NAT нажмите кнопку *«Добавить»* и в открывшемся окне «Создать исключение NAT» заполните следующие поля:

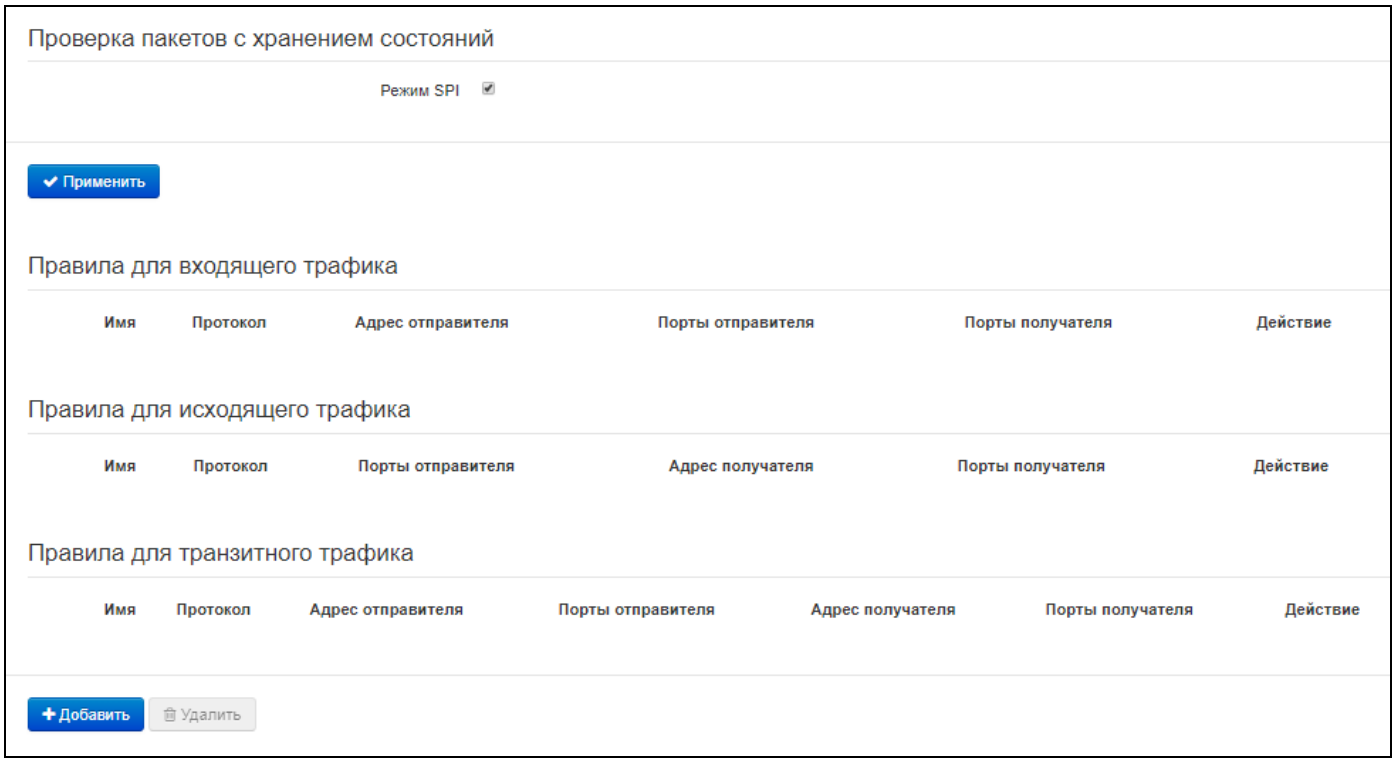
- Имя – название правила (поле обязательно для заполнения);
- Локальный IP-адрес – адрес из локальной подсети, для которого будет работать текущее исключение. Можно выбрать адрес из выпадающего меню, где отображаются IP-адреса, добавленные в ARP-таблицу.

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

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

3.4.2.12 Подменю «Сетевой экран»

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

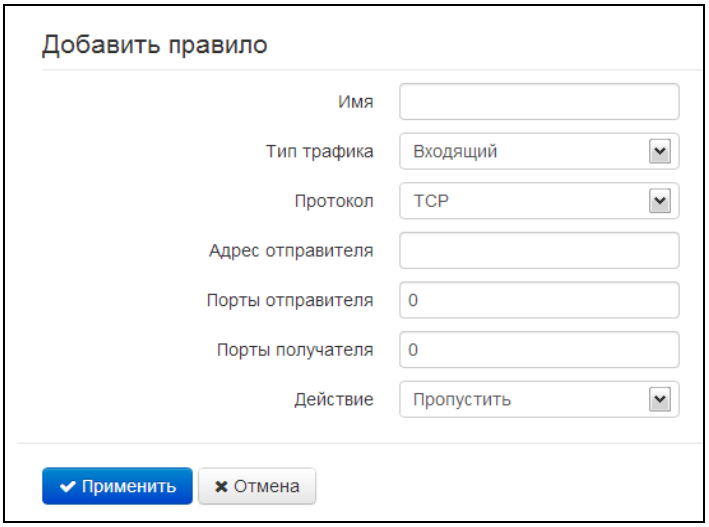


Проверка пакетов с хранением состояний

В данном пункте возможно включение/отключение проверки пакетов с хранением состояний (SPI).

Настройка правил сетевого экрана

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



- *Имя* – название правила;
- *Тип трафика* – выбор типа трафика, на который распространяется действие данного правила:
  - *Входящий* – входящий на устройство трафик (получателем является непосредственно один из сетевых интерфейсов устройства). При выборе данного типа трафика для редактирования станут доступны следующие поля:
    - *Адрес отправителя* – задает начальный IP-адрес отправителя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.16.0/24 или 192.168.16.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов (запись маски в виде /24 соответствует записи /255.255.255.0);
  - *Исходящий* – исходящий с устройства трафик (трафик, генерируемый локально устройством с одного из сетевых интерфейсов). При выборе данного типа трафика для редактирования станут доступны следующие поля:
    - *Адрес получателя* – задает IP-адрес получателя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.18.0/24 или 192.168.18.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;
  - *Транзитный* – транзитный трафик (трафик, проходящий между двумя сетевыми интерфейсами, когда отправителем и получателем являются внешние устройства). При выборе данного типа трафика для редактирования станут доступны следующие поля:

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

- *Протокол* – протокол пакета, на который распространяется действие данного правила: TCP, UDP, TCP/UDP, ICMP, любой.

- *Действие* – действие, совершаемое над пакетами (отбросить/пропустить).

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

- *Порты отправителя* – список портов отправителя, пакеты которого будут попадать под данное правило (допускается указывать либо одиночный порт, либо через “-“ диапазон портов); для указания всех портов введите диапазон «0-65535»;

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

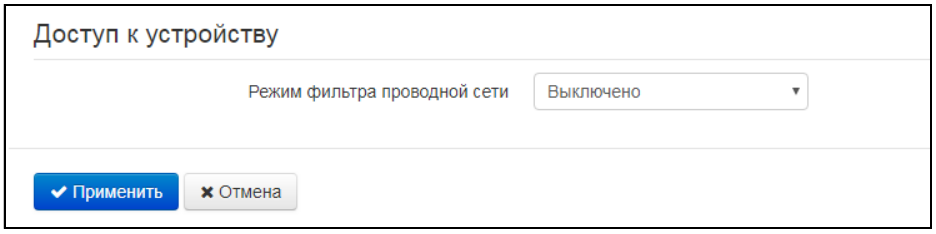
При выборе протокола ICMP для редактирования будут доступны настройки:

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

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

3.4.2.13 Подменю «Фильтр MAC»

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



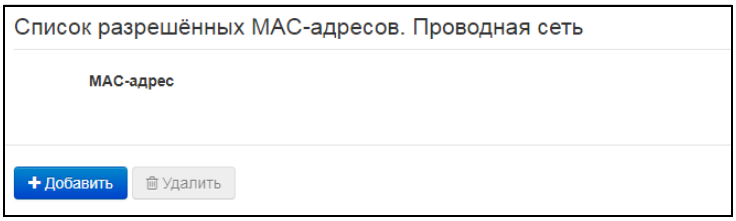
Настройки ограничения доступа

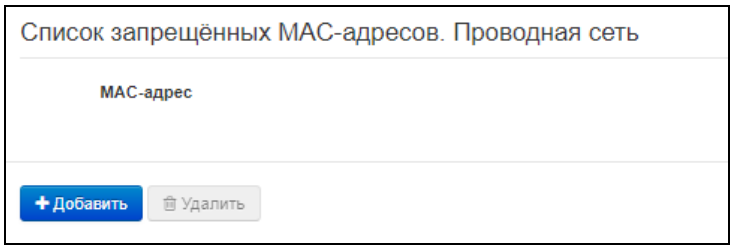
- *Режим фильтра проводной сети* — определяет политику доступа к устройству через проводной интерфейс Ethernet:
  - *Выключено* – фильтрация по MAC-адресам отключена – всем клиентам разрешен доступ к устройству;
  - *Чёрный список* – в данном режиме работы фильтра клиентам, MAC-адреса которых указаны в «Списке MAC-адресов», запрещено подключаться к устройству. Клиентам, MAC-адреса которых не указаны в списке, доступ к устройству разрешен;

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

Список MAC-адресов

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



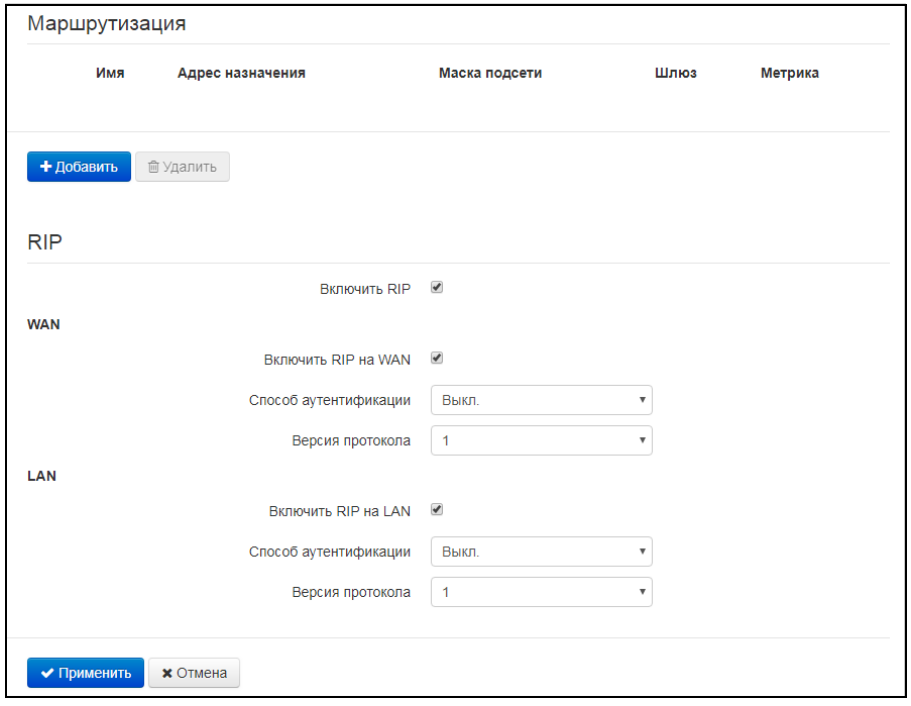


Для добавления нового клиента в список нажмите кнопку *«Добавить»* и введите его MAC-адрес или выберите MAC-адрес хоста, подключенного к устройству.

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

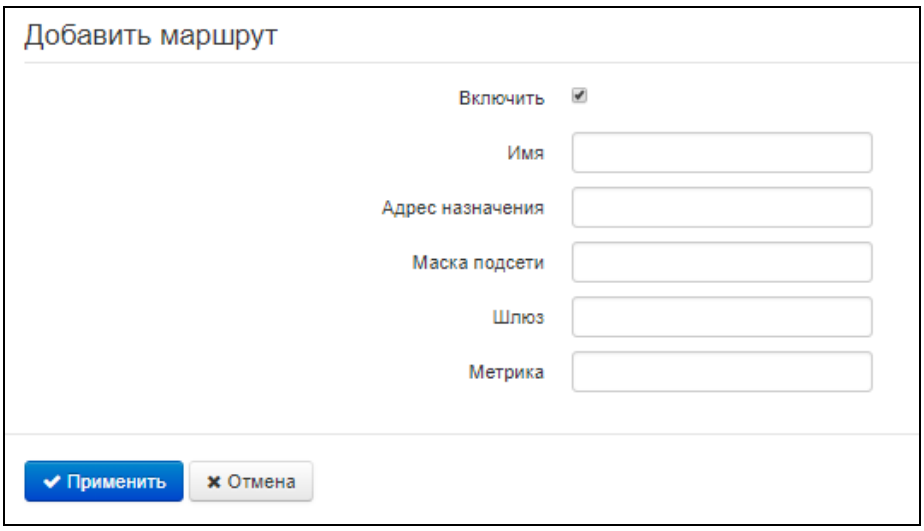
3.4.2.14 Подменю «Маршрутизация»

В подменю «Маршрутизация» устанавливаются статические маршруты устройства.



Маршрутизация

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



- *Включить* – при включенном флаге маршрут активен;
- *Имя* – название маршрута, используется для удобства восприятия человеком;
- *Адрес назначения* – IP-адрес хоста или подсети назначения, до которых необходимо установить маршрут;
- *Маска подсети* – маска подсети. Для хоста маска подсети устанавливается в значение 255.255.255.255, для подсети – в зависимости от её размера;
- *Шлюз* – IP-адрес шлюза, через который осуществляется выход на *«Адрес назначения»;*
- *Метрика* – позволяет задать число переходов («хопов») для выбора оптимального маршрута.

RIP

Для включения протокола RIP следует активировать параметр «Включить RIP». Это включит анонсирование маршрутов проводного интерфейса:

- *Способ аутентификации* – выбрать способ аутентификации перед обменом маршрутами с соседним маршрутизатором: выкл/Текст/MD5X;
- *Пароль для аутентификации* – пароль, используемый при аутентификации с соседним маршрутизатором;
- *Версия протокола* – используемая версия протокола RIP: RIPv1, RIPv2, RIPv1+RIPv2.

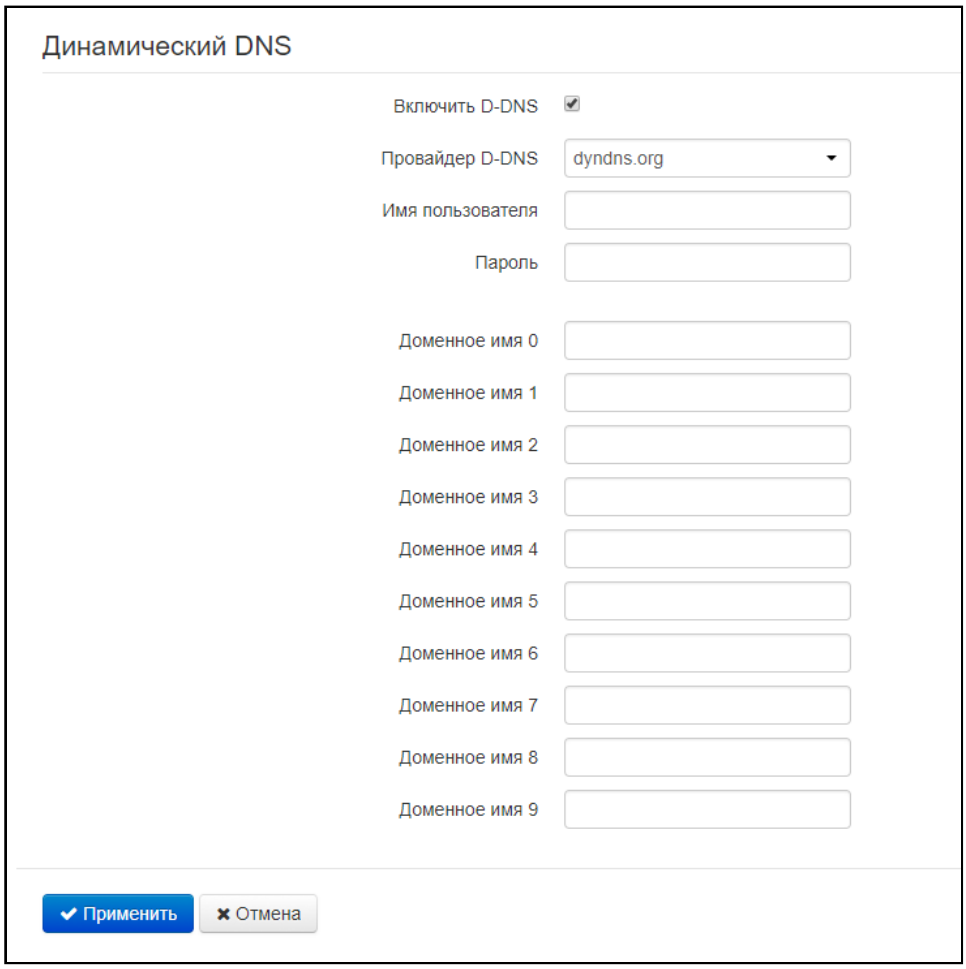
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

3.4.2.15 Подменю «Динамический DNS»

В подменю «Динамический DNS» выполняется настройка соответствующего сервиса.

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

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

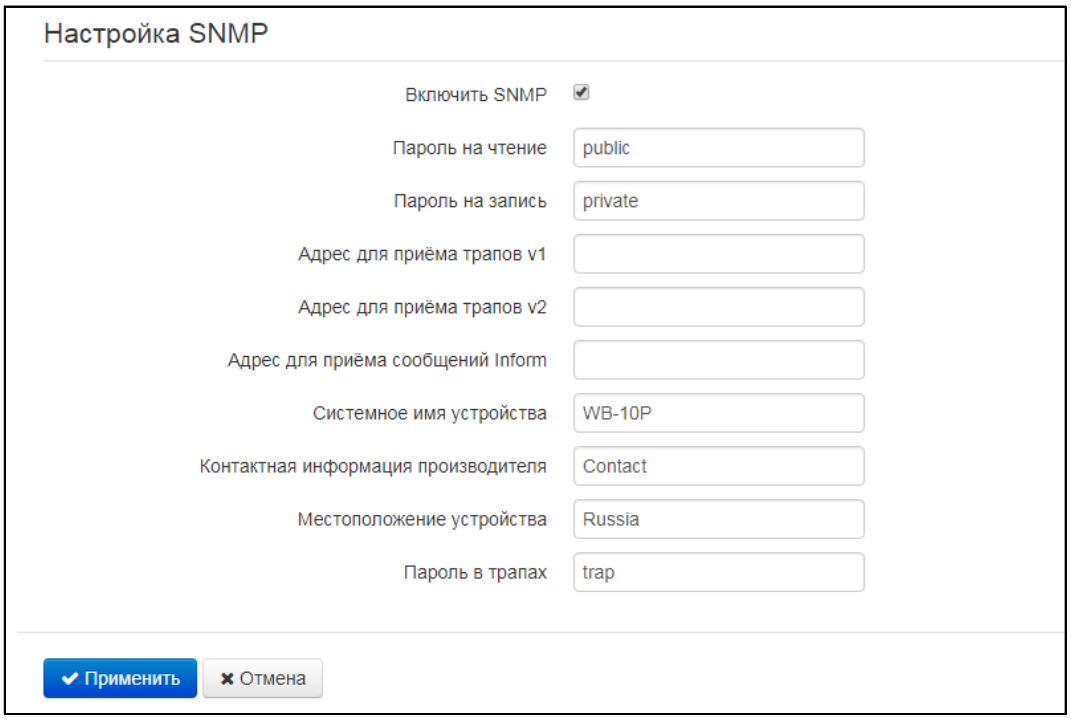


- *Включить D-DNS* – при установленном флаге сервис D-DNS активен и для редактирования доступны следующие настройки:
- *Провайдер D-DNS* – название провайдера D-DNS – выберите одного провайдера из списка доступных;
- *Имя пользователя* – имя пользователя для доступа к учетной записи сервиса D-DNS;
- *Пароль* – пароль для доступа к учетной записи сервиса D-DNS;
- *Доменное имя (0..9)* – можно зарегистрировать до десяти доменных имён устройства (обычно требуется лишь одно). Обновление информации об IP-адресе устройства на сервере провайдера происходит периодически через 60 секунд.

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

3.4.2.16 Подменю «SNMP»

Программное обеспечение WB-10P позволяет проводить конфигурирование и мониторинг состояния устройства, используя протокол SNMP. В подменю «SNMP» выполняются настройки параметров SNMP-агента. Устройство поддерживает протоколы версий SNMPv1, SNMPv2c, SNMPv3.

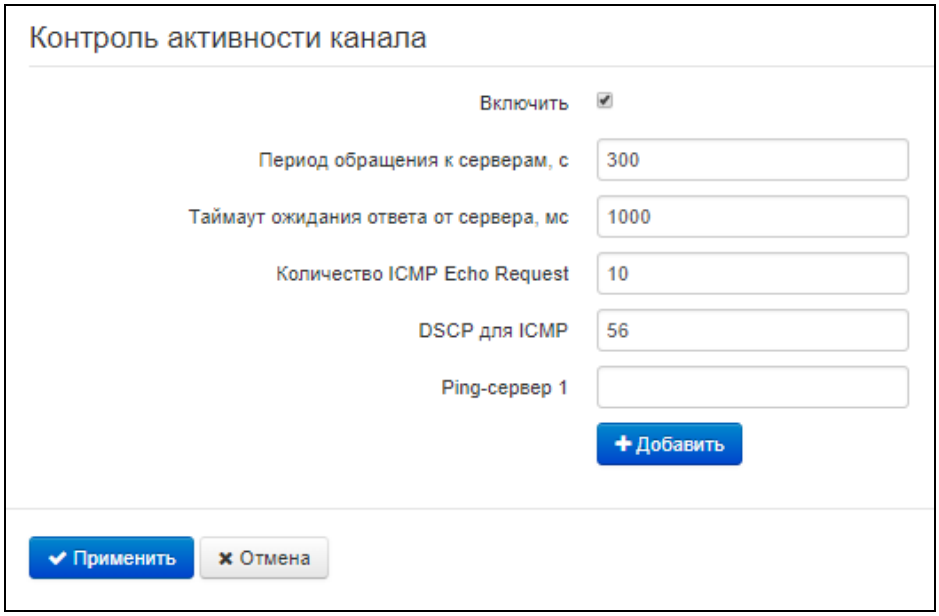


- *Включить SNMP* – при установленном флаге разрешено использование протокол SNMP;
- *Пароль на чтение* – пароль на чтение параметров (общепринятый: *public*);
- *Пароль на запись* – пароль на запись параметров (общепринятый: *private*);
- *Адрес для приёма трапов v1* – IP-адрес или доменное имя приемника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

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

3.4.2.17 Подменю «Контроль связи»

В данном подменю можно настроить пороговые значения параметров определения качества основного подключения (USB1 или USB2), при превышении которых будет осуществлено переключение на резервное подключение (USB1 или USB2).



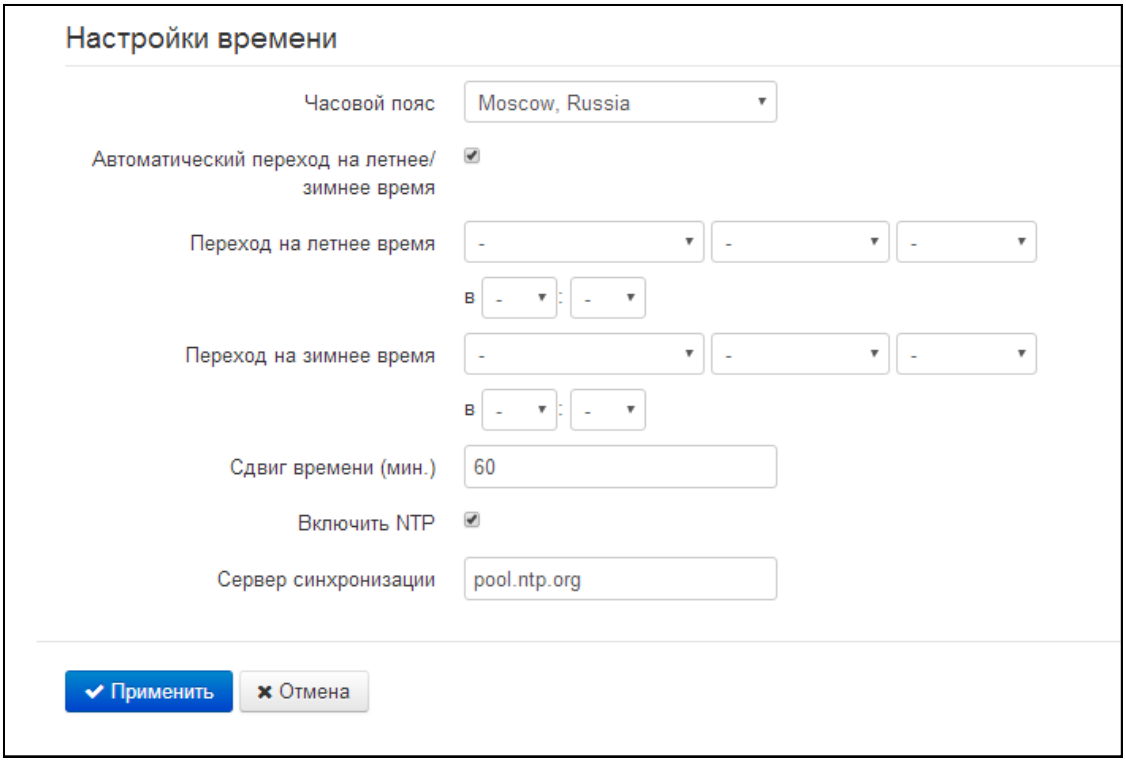
- *Включить* – при установленном флаге становятся доступны следующие настройки:
- *Период обращения серверам, с* – интервал отправки периодических сообщений в секундах с целью проверки доступности сервера контроля качества соединения;
- *Таймаут ожидания ответа от сервера, мс* – если не будет ответа от сервера, то по истечении данного интервала времени будет произведена повторная отправка пакетов;
- *Количество ICMP Echo Request* – количество пакетов, которое будет отправляться на сервер для проверки качества связи;
- *DSCP для ICMP* – значение поля DSCP-заголовка IP-пакета для ICMP-пакета с заданным портом источника;
- *Ping-сервер 1..5* – IP-адрес, на который будут отправляться запросы для проверки активности соединения.

3.4.3 Меню «Система»

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

3.4.3.1 Подменю «Время»

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



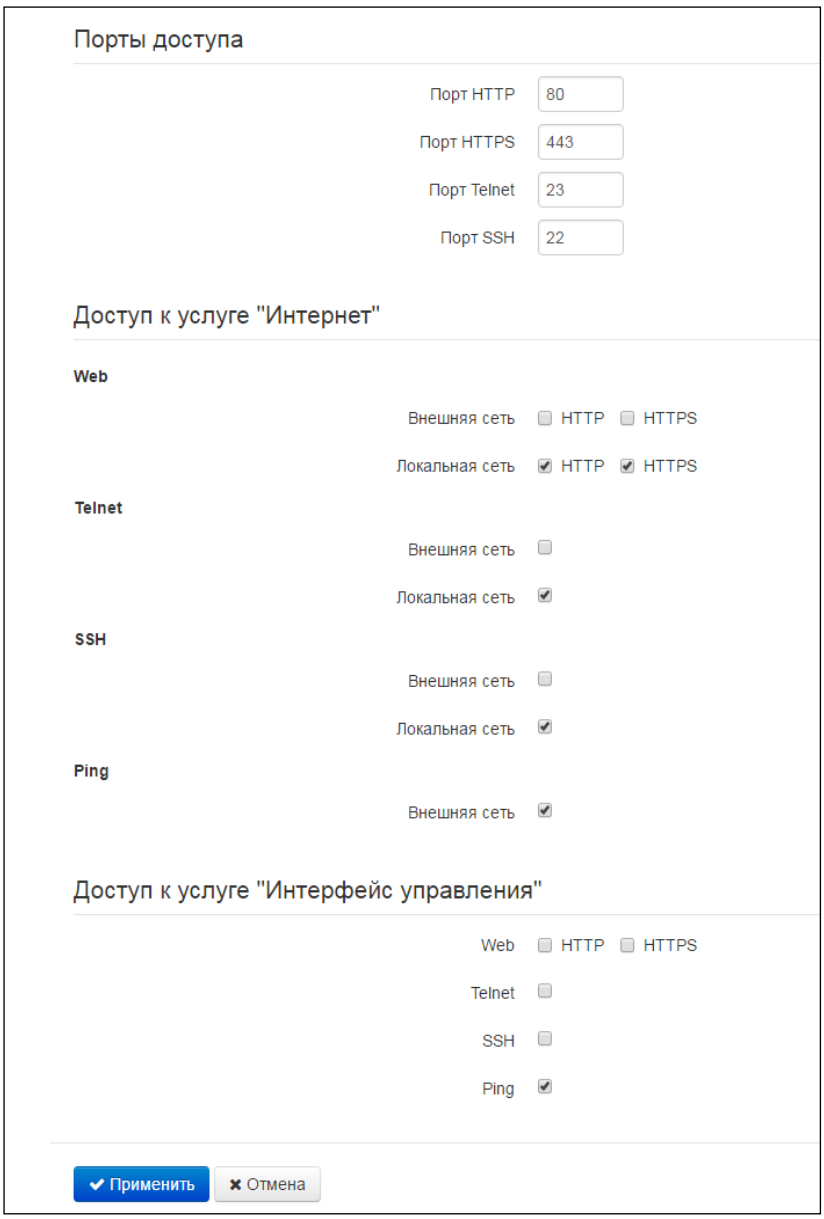
Настройки времени

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

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

3.4.3.2 Подменю «Доступ»

В подменю *«Доступ»* настраивается доступ к устройству посредством Web-интерфейса, Telnet и SSH.



Порты доступа

В данном разделе выполняется настройка TCP-портов для сервисов HTTP, HTTPS, Telnet, SSH.

- *Порт HTTP* – номер порта для доступа к Web-интерфейсу устройства по протоколу *HTTP*, по умолчанию – 80;
- *Порт HTTPS* – номер порта для доступа к Web-интерфейсу устройства по протоколу *HTTPS* (*HTTP Secure* – безопасное подключение), по умолчанию – 443;
- *Порт Telnet* – номер порта для доступа к устройству по протоколу *Telnet*, по умолчанию – 23;
- *Порт SSH* – номер порта для доступа к устройству по протоколу *SSH*, по умолчанию – 22.

По протоколам *Telnet* и *SSH* осуществляется доступ к командной строке (консоль linux).

Доступ к услуге "Интернет"

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

Web, Внешняя сеть:

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

Web, Локальная сеть:

- *HTTP* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через порт Ethernet по протоколу HTTP (небезопасное подключение);
- *HTTPS* – при установленном флаге разрешено подключение к Web-конфигуратору устройства через порт Ethernet 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 беспроводную сеть) или внутренней (через порт Ethernet) сети установите соответствующие флаги.

SSH:

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

Для разрешения доступа к устройству по протоколу SSH из внешней (через беспроводную сеть) или внутренней (через порт Ethernet) сети установите соответствующие флаги.

Ping:

ICMP-ping – механизм, реализованный в протоколе ICMPv4 и v6 для контроля доступности сетевых устройств.

Для разрешения ответа на входящие ICMP-echo сообщения установите соответствующий флаг.

Доступ к услуге Интерфейс управления:

Раздел позволяет настроить доступ к интерфейсу управления устройством, используя протоколы HTTP, HTTPS, Telnet, SSH, а так же доступность по протоколу ICMP. Настройка интерфейса производится на странице **Система – Интерфейс управления**. Для разрешения доступа по какому-либо из указанных протоколов установите соответствующие флаги.

Доступ через GRE туннели:

Если в системе настроены GRE-туннели, для каждого туннеля будет доступен раздел *Доступ через «Имя туннеля»*.

Раздел позволяет настроить доступ к устройству через туннели GRE используя протоколы HTTP, HTTPS, Telnet, SSH, а так же доступность по протоколу ICMP. Настройка GRE-туннелей производится на странице **Сеть – GRE**. Для разрешения доступа по какому-либо из указанных протоколов установите соответствующие флаги.

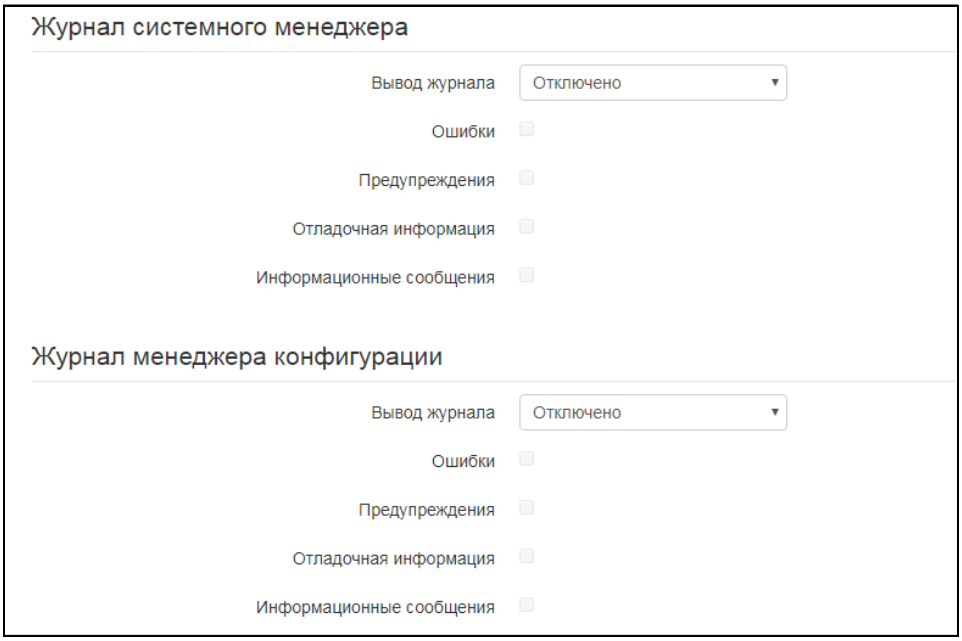
Для авторизации по протоколам Telnet и SSH по умолчанию используются имя пользователя *admin*, пароль – *password*. После авторизации станет доступен интерфейс для конфигурирования CLI.

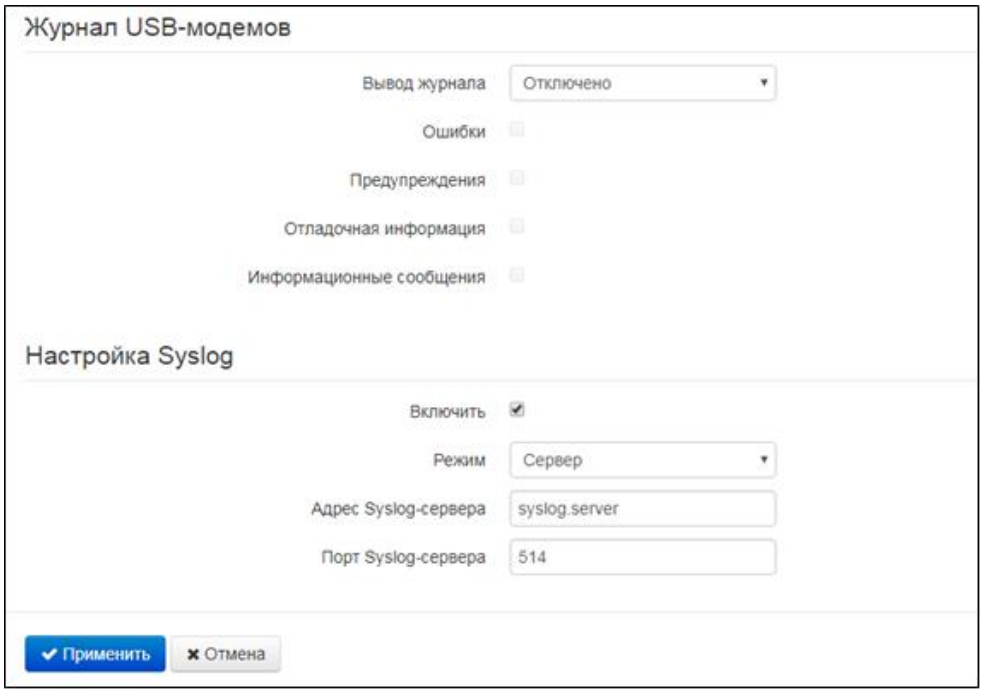
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена»*.

3.4.3.3 Подменю «Журнал»

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

- Системный менеджер – отвечает за настройку устройства согласно файлу конфигурации.
- Менеджер конфигурации – отвечает за работу с файлом конфигурации (чтение и запись в файл конфигурации из различных источников) и сбор информации мониторинга устройства.
- Журнал USB-модемов – отвечает за взаимодействие с USB-модемами.





Журнал системного менеджера

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

Ниже настраивается тип сообщений, выводимых в журнал системного менеджера:

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

Журнал менеджера конфигурации

- *Вывод журнала* – направление вывода сообщений журнала:
  - *Отключено* – журнал отключен;
  - *Syslog* – сообщения выводятся по протоколу syslog на удаленный сервер либо в локальный файл (настройка протокола осуществляется ниже);

- *Консоль* – сообщения выводятся в консоль устройства (необходимо подключение через переходник COM-порта);
- *Телнет* – сообщения выводятся в telnet-сессию; для этого сначала необходимо создать подключение по протоколу telnet.

Ниже настраивается тип сообщений, выводимых в журнал менеджера конфигурации:

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

Журнал USB-модемов

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

Ниже настраивается тип сообщений, выводимых в журнал системного менеджера:

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

Настройка Syslog

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

- *Включить* – при установленном флаге запущен Syslog-агент;
- *Режим* – режим работы Syslog-агента:

- *Сервер* – информация журналов отправляется на удаленный Syslog-сервер (этот режим называется «удаленный журнал»);
- *Локальный файл* – информация журналов сохраняется в локальном файле;
- *Сервер и файл* – информация журналов отправляется на удаленный Syslog-сервер и сохраняется в локальном файле.

Далее в зависимости от режима Syslog-агента доступны настройки:

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

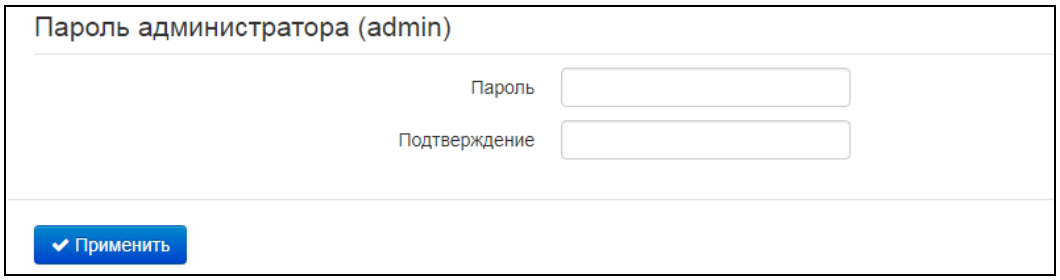
3.4.3.4 Подменю «Пароли»

В подменю «Пароли» устанавливаются пароли доступа привилегированного пользователя администратор.

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

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

Логин администратора: admin

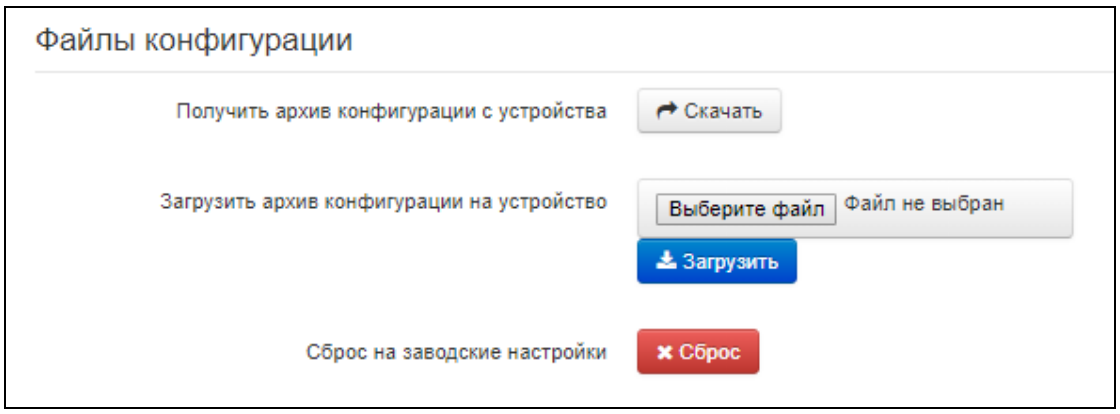


- *Пароль администратора* – в соответствующие поля введите пароль администратора и подтвердите его;

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

3.4.3.5 Подменю «Управление конфигурацией»

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



Получение конфигурации

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

Обновление конфигурации

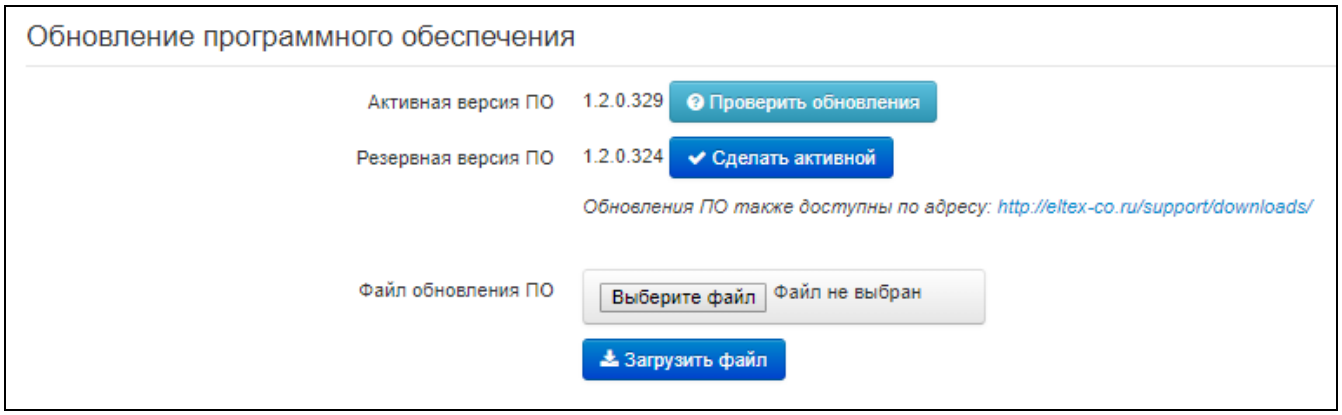
- *Загрузить архив конфигурации на устройство* – выбор сохраненного на локальном компьютере файла конфигурации. Для обновления конфигурации устройства нажмите кнопку «Выберите файл», укажите файл (в формате .tar.gz) и нажмите кнопку «Загрузить». Загруженная конфигурация применяется автоматически без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

Сброс на заводские настройки

Для сброса устройства к настройкам по умолчанию нажмите кнопку «Сброс».

3.4.3.6 Подменю «Обновление ПО»

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



- *Активная версия ПО* – версия программного обеспечения, установленного на устройстве, работающая в данный момент;

- *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;
- *Резервная версия ПО* – версия программного обеспечения, установленного на устройстве, на которую можно перейти в случае проблем с активной версией ПО;
- *Сделать активной* – кнопка, позволяющая сделать резервную версию ПО активной, для этого потребуется перезагрузка устройства. Активная версия ПО в этом случае станет резервной.

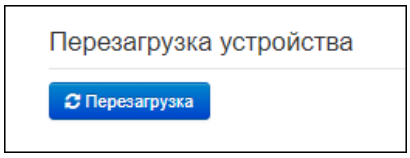
Для работы функции проверки обновления необходимо наличие выхода в Интернет.

Обновить программное обеспечение устройства можно также вручную, предварительно загрузив файл ПО с сайта http://eltex-co.ru/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. Если не удалось этого избежать и загружаемый образ ПО был записан не полностью, в результате чего запуск этого ПО становится невозможным, шлюз автоматически попытается запустить резервный образ ПО (при его наличии).

3.4.3.7 Подменю «Перезагрузка»

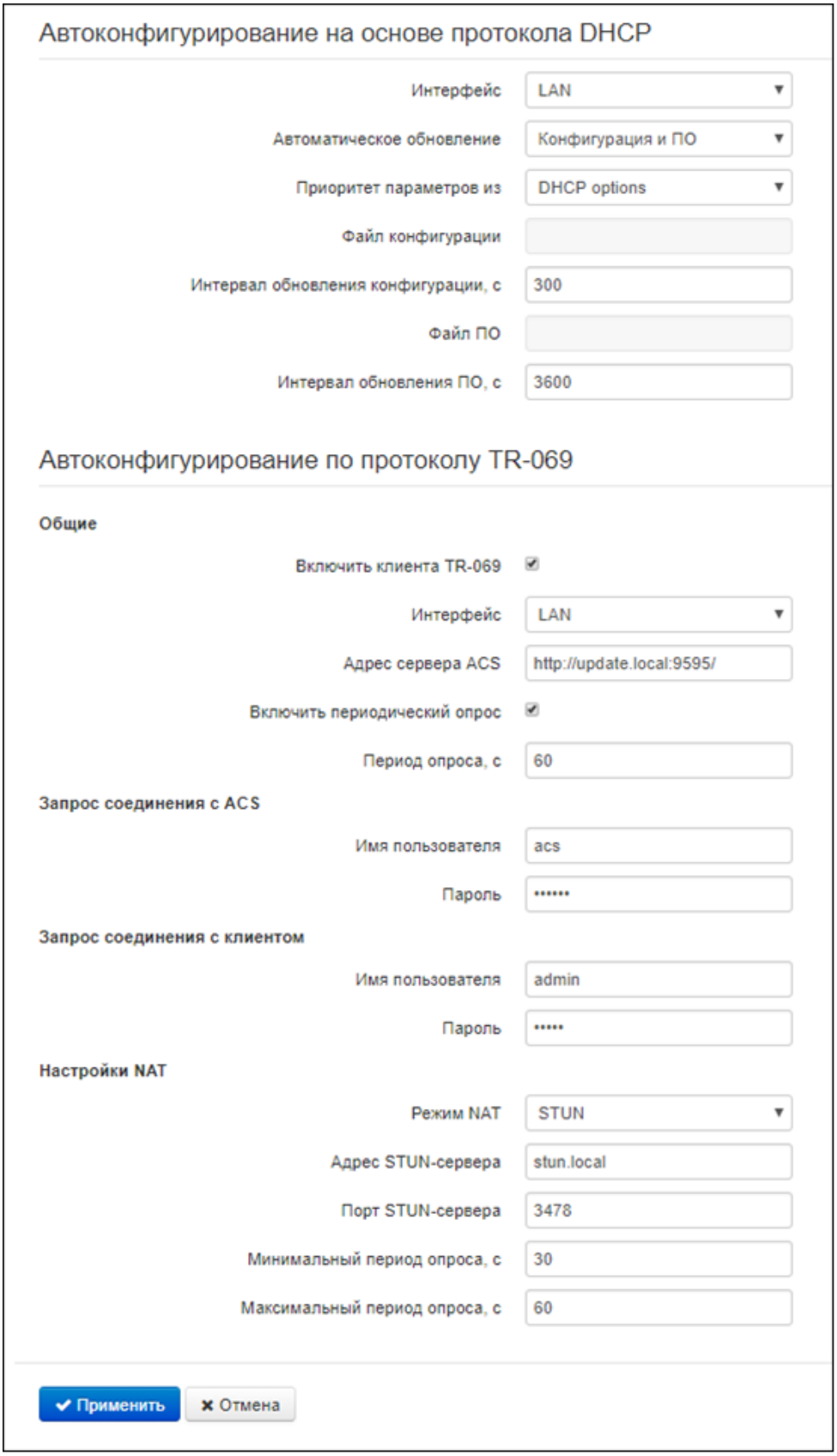


В подменю «Перезагрузка» выполняется перезапуск устройства.

Для перезагрузки устройства нажмите на кнопку «Перезагрузить». Процесс перезагрузки устройства занимает примерно 2 минуты.

3.4.3.8 Подменю «Автоконфигурирование»

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



Автоконфигурирование на основе протокола DHCP:

- *Интерфейс* – выбор интерфейса для автоконфигурирования по протоколу DHCP*;*
- *Автоматическое обновление* – выбор режима обновления устройства; возможно несколько вариантов:
  - *Выключено* – автоматическое обновление конфигурации и программного обеспечения устройства отключено;
  - *Конфигурация и ПО* – разрешено периодическое обновление конфигурации и программного обеспечения устройства;
  - *Только конфигурация* – разрешено периодическое обновление только конфигурации устройства;
  - *Только ПО* – разрешено периодическое обновление только программного обеспечения устройства.
- *Приоритет параметров из* – данный параметр определяет, откуда необходимо взять названия и расположение файлов конфигурации и программного обеспечения:
  - *Static settings* – пути к файлам конфигурации и программного обеспечения определяются соответственно из параметров «*Файл конфигурации»* и «*Файл ПО»*; подробнее работу алгоритма смотрите в **разделе 4** Алгоритм работы автоматического обновления устройства на основе протокола DHCP;
  - *DHCP options* – пути к файлам конфигурации и программного обеспечения определяются из DHCP опций 43 и 66 (для этого необходимо для услуги Интернет выбрать протокол DHCP); подробнее работу алгоритма смотрите в **разделе 4** Алгоритм работы автоматического обновления устройства на основе протокола DHCP;
- *Файл конфигурации* – полный путь к файлу конфигурации – задаётся в формате URL (на данный момент возможна загрузка файла конфигурации по протоколам TFTP и HTTP):

  tftp://<server address>/<full path to cfg file>
  http://<server address>/<full path to cfg file>
  где < server address > – адрес HTTP- или TFTP-сервера (доменное имя или IPv4),
  < full path to cfg file > – полный путь к файлу конфигурации на сервере;
- *Интервал обновления конфигурации, с* – промежуток времени в секундах, через который осуществляется периодическое обновление конфигурации устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;
- *Файл ПО* – полный путь к файлу программного обеспечения – задаётся в формате URL (на данный момент возможна загрузка файла ПО по протоколам TFTP и HTTP):

  tftp://<server address>/<full path to firmware file>
  http://<server address>/<full path to firmware file>
  где < server address > – адрес HTTP- или TFTP-сервера (доменное имя или IPv4),
  < full path to firmware file > – полный путь к файлу ПО на сервере;
- *Интервал обновления ПО, с* – промежуток времени в секундах, через который осуществляется периодическое обновление программного обеспечения устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;
- *Имя пользователя/пароль FTP* – задает имя пользователя и пароль при авторизации на сервере ftp при скачивании файлов конфигурации или ПО.

Детальное описание алгоритма автоматического обновления на основе протокола DHCP смотрите в разделе **4** Алгоритм работы автоматического обновления устройства на основе протокола DHCP;

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 управления*, то данный интерфейс автоматически будет использоваться для работы по протоколу TR-069. Настройка выбора интерфейса будет заблокирована;
- *Адрес сервера ACS* – адрес сервера автоконфигурирования. Адрес необходимо вводить в формате http://<address>:<port> или https://<address>:<port> (<address> – IP-адрес или доменное имя ACS-сервера, <port> – порт сервера ACS, по умолчанию порт 10301). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS;
- *Включить периодический опрос* – при установленном флаге встроенный клиент TR-069 осуществляет периодический опрос сервера ACS с интервалом, равным *«Периоду опроса»*, в секундах. Цель опроса - обнаружить возможные изменения в конфигурации устройства.

Запрос соединения с ACS:

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

Запрос соединения с клиентом:

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

Настройки NAT:

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

- *Режим NAT* – определяет, каким образом клиент должен получить информацию о своем публичном адресе. Возможны следующие режимы:
  - *STUN* – использовать протокол STUN для определения публичного адреса;
  - *Manual* – ручной режим, когда публичный адрес задается явно в конфигурации; в этом режиме на устройстве, выполняющем функции NAT, необходимо добавить правило проброса TCP-порта, используемого клиентом TR-069;
  - *Off* – NAT не используется – данный режим рекомендуется использовать, только когда устройство подключено к серверу ACS напрямую, без преобразования сетевых адресов. В этом случае публичный адрес совпадает с локальным адресом клиента.

При выборе режима *STUN* необходимо задать следующие настройки:

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

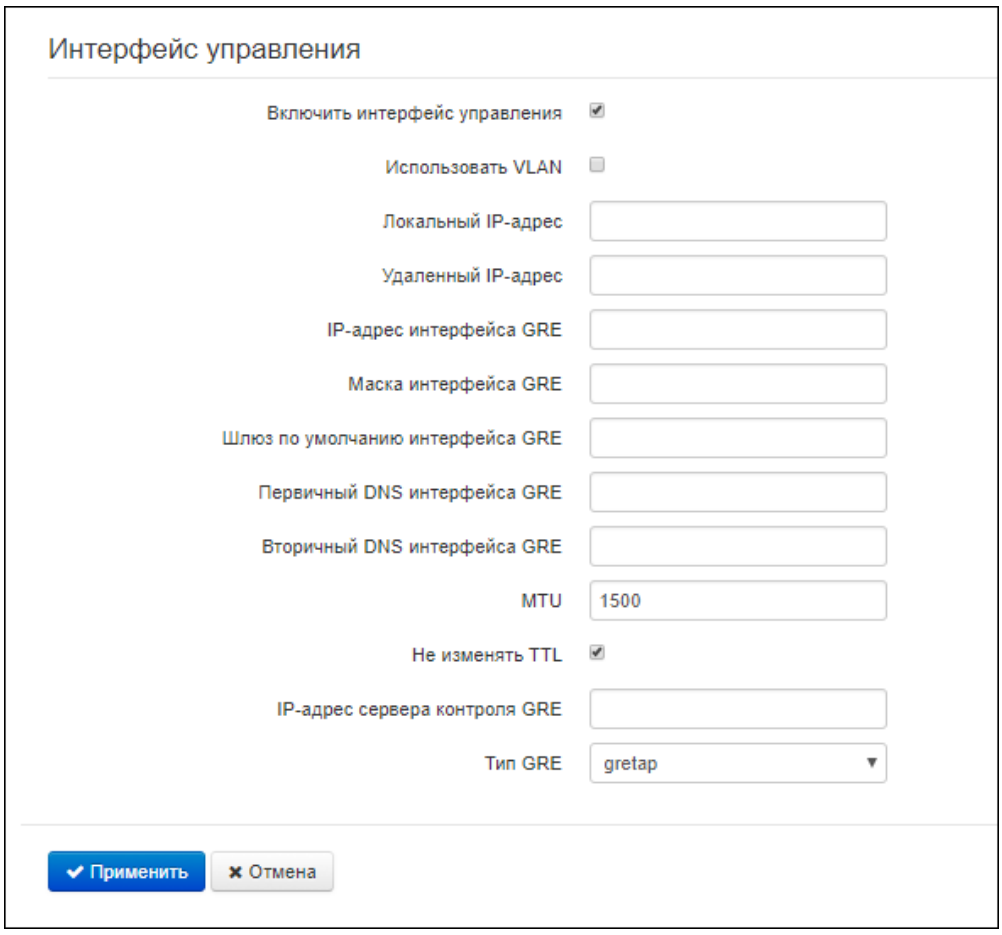
При выборе режима *Manual* публичный адрес клиента задается вручную через параметр *Адрес NAT* (адрес необходимо вводить в формате IPv4).

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

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

3.4.3.9 Подменю «Интерфейс управления»

Меню позволяет настроить GRE туннель для удалённого управления устройством с использованием протоколов HTTP, HTTPS, Telnet и SSH.

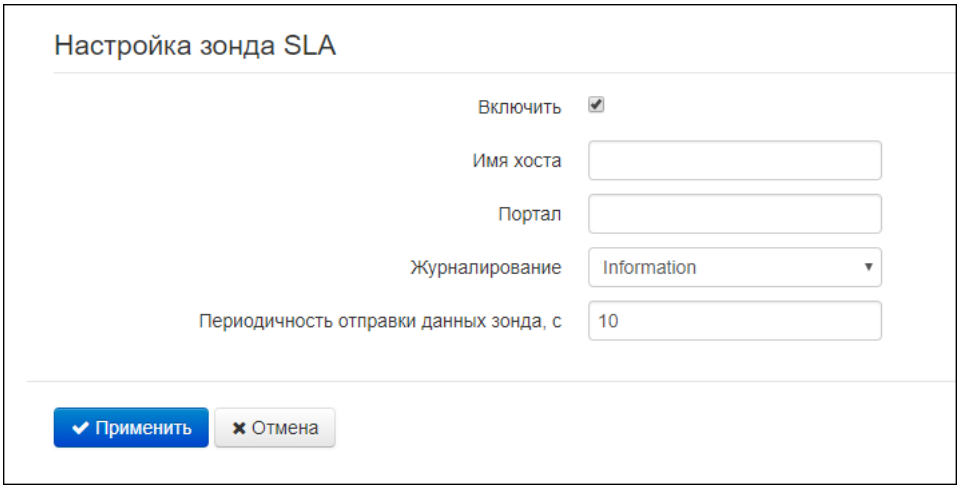


- Включить интерфейс управления – флаг активирует GRE-туннель для удалённого управления устройством;
- Использовать VLAN – при установленном флаге управление устройством может производиться в выделенной VLAN, номер которой указан в поле «VLAN ID»;
- Локальный IP-адрес – собственный IP-адрес устройства, полученный на беспроводном интерфейсе;
- Удаленный IP-адрес – IP-адрес встречного устройства, на котором будет терминироваться туннель GRE для интерфейса управления;
- IP-адрес интерфейса GRE – установка IP-адреса устройства в туннеле;
- Маска интерфейса GRE – маска подсети интерфейса GRE;
- Шлюз по умолчанию интерфейса GRE – IP-адрес дефолтного шлюза интерфейса GRE;
- Первичный DNS интерфейса GRE, Вторичный DNS интерфейса GRE – адреса серверов доменных имён (используется для определения IP-адреса устройства по его доменному имени) для интерфейса GRE. Данные поля можно оставить пустыми, если в них нет необходимости.
- MTU – максимальный размер блока данных, передаваемых через туннель
- Не изменять TTL – при установленном флаге значение заголовка TTL, передаваемого по протоколу GRE, не инкрементируется;
- TTL – позволяет задать желаемое значение заголовка TTL передаваемого пакета GRE.
- IP-адрес сервера для контроля GRE – IP-адрес, на который будут отправляться запросы для проверки активности туннеля. Если поле пустое – контроль GRE не используется.
- Тип GRE – позволяет настроить тип GRE-туннеля;

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

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

3.4.3.10 Подменю «wiSLA»



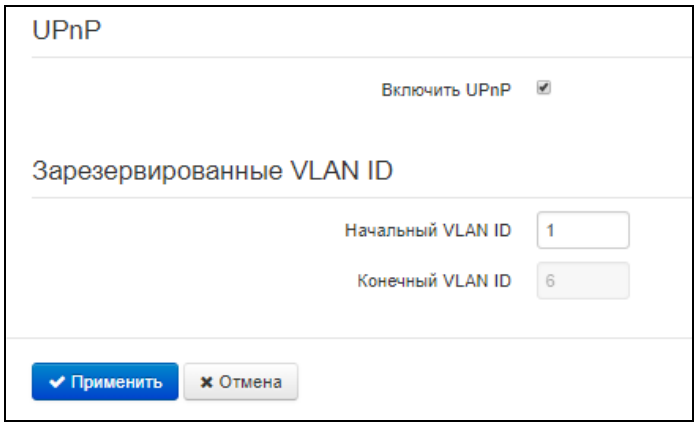
Настройка зонда SLA

В этом разделе производится настройка взаимодействия с платформой мониторинга и управления качеством услуг связи wiSLA.

- *Включить* – при установленном флаге запущена отправка данных на портал wiSLA;
- *Имя хоста* – имя устройства при взаимодействии с порталом wiSLA;
- *Портал* – URL портала, на который зонд будет отправлять собираемые данные;
- *Журналирование* – позволяет выбрать уровень отладки в сообщениях, отправляемых зондом;
- *Периодичность отправки данных зонда, с* – время в секундах, через которое данные отправляются зондом на портал.

3.4.3.11 Подменю «Дополнительные настройки»

В подменю «Дополнительные настройки» можно включить UPnP.



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

Зарезервированные VLAN ID

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

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

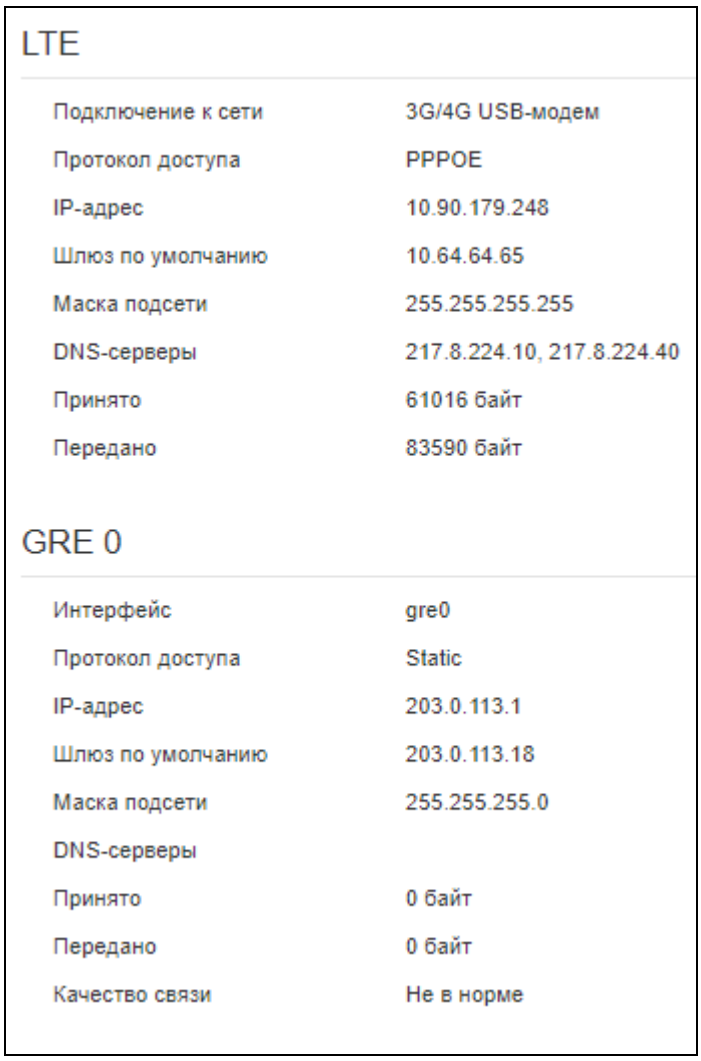
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

3.5 Мониторинг системы

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

3.5.1 Подменю «Интернет»

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



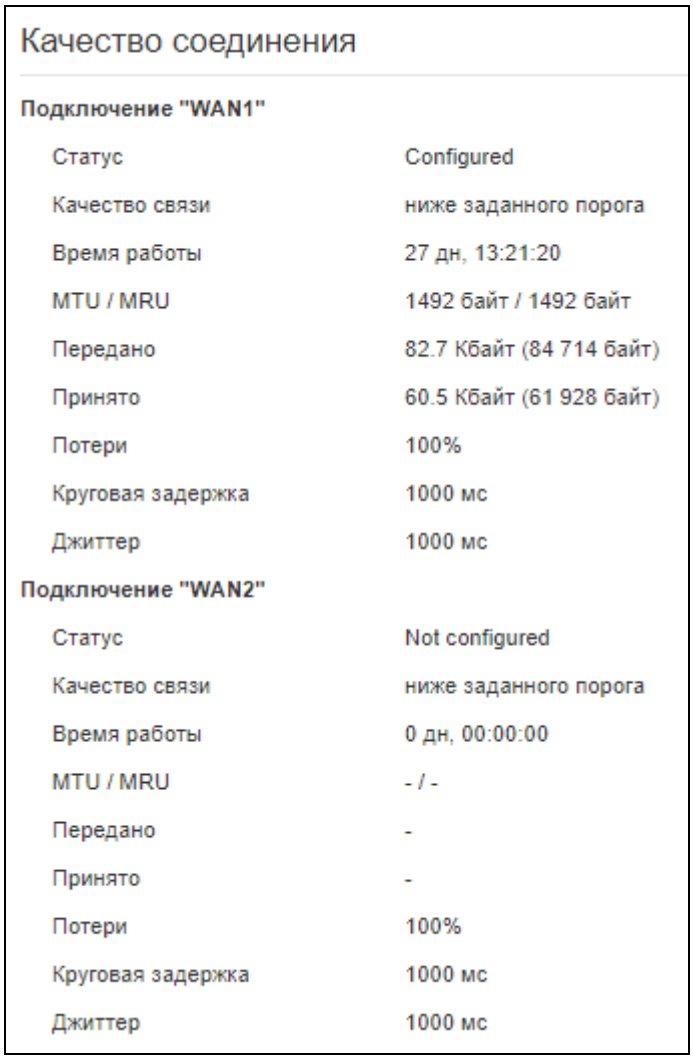
LTE

- *Подключение к сети* – способ подключения к сети провайдера осуществляется через 3G/4G USB-модем, подключенный к портам USB;
- *Протокол доступа* – протокол, используемый для доступа к сети Интернет;
- *IP-адрес* – IP-адрес устройства во внешней сети, полученный через USB-модем;
- *Шлюз по умолчанию* – IP-адрес сетевого шлюза по умолчанию, полученный через USB-модем;
- *Маска подсети* – маска подсети сетевого интерфейса полученная через USB-модем;

- *DNS-серверы* – список IP-адресов DNS-серверов, полученных через USB-модем;
- *Принято* – количество байт, принятых на интерфейсе LTE;
- *Передано* – количество байт, переданных с интерфейса LTE.

GRE0/GRE1

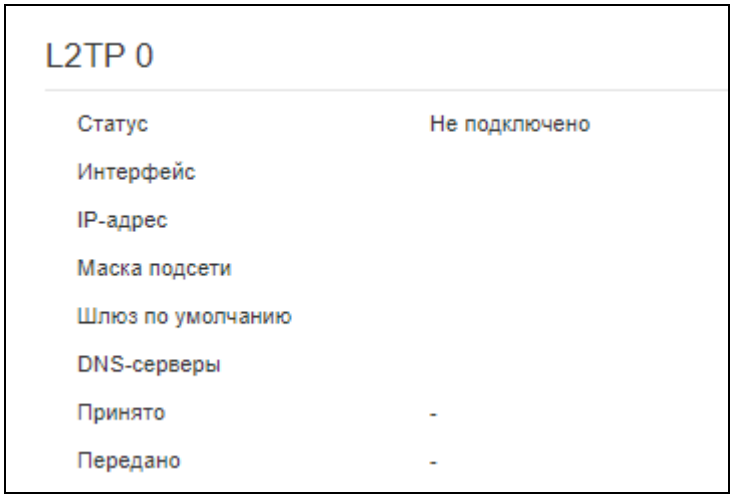
- *Интерфейс* – имя интерфейса, настроенное в конфигурации;
- *Протокол доступа* – протокол, используемый для доступа к сети Интернет;
- *IP-адрес* – IP-адрес устройства в туннеле;
- *Шлюз по умолчанию* – IP-адрес сетевого шлюза по умолчанию, настроенный на интерфейсе GRE;
- *Маска подсети* – маска подсети сетевого интерфейса GRE;
- *DNS-серверы* – список IP-адресов DNS-серверов, настроенных на интерфейсе GRE;
- *Принято* – количество байт, принятых на интерфейсе GRE;
- *Передано* – количество байт, переданных с интерфейса GRE;
- *Качество связи* – показывает доступность сервера контроля GRE.



Качество соединения

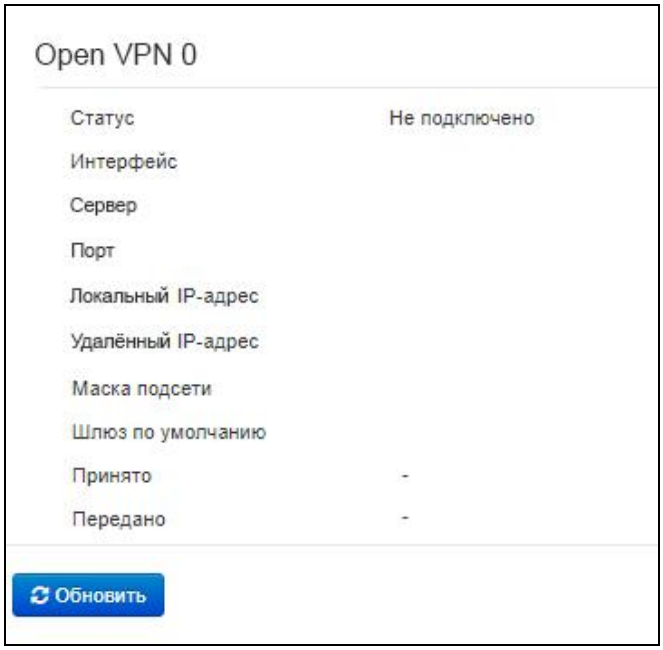
Подключение "WAN1"/Подключение "WAN2"

- *Статус* – состояние подключения USB-модема к устройству;
- *Качество связи* – показывает доступность сервера контроля качества связи;
- *Время работы* – время работы с момента последнего подключения модема к устройству;
- *MTU/MRU* – максимальный размер блока данных, передаваемых/принимаемых по сети;
- *Передано* – количество байт, переданных через WAN интерфейс;
- *Принято* – количество байт, принятых на WAN интерфейс;
- *Потери* – процент потерь с WAN интерфейса;
- *Круговая задержка* – время, затраченное на передачу пакета icmp и прием ответа на него;
- *Джиттер* – неравномерность времени, отведенного на доставку пакета.



L2TP0/L2TP1

- *Статус* – отображает состояние подключения;
- *Интерфейс* – имя интерфейса, настроенное в конфигурации;
- *IP-адрес* – IP-адрес устройства в туннеле;
- *Маска подсети* – маска подсети сетевого интерфейса GRE;
- *Шлюз по умолчанию* – IP-адрес сетевого шлюза по умолчанию, настроенный на интерфейсе GRE;
- *DNS-серверы* – список IP-адресов DNS-серверов, настроенных на интерфейсе GRE;
- *Принято* – количество байт, принятых на интерфейсе GRE;
- *Передано* – количество байт, переданных с интерфейса GRE.



Open VPN 0/Open VPN 1

- *Статус* – отображает состояние подключения;
- *Интерфейс* – имя интерфейса, настроенное в конфигурации;
- *Сервер* – IP-адрес сервера Open VPN;
- *Порт* – Порт, на который будут отсылаться запросы на подключение к серверу;
- *Локальный IP-адрес* – IP-адрес устройства в туннеле;
- *Удалённый IP-адрес* – IP-адрес удалённого конца туннеля;
- *Маска подсети* – маска подсети сетевого интерфейса GRE;
- *Шлюз по умолчанию* – IP-адрес сетевого шлюза по умолчанию, настроенный на интерфейсе GRE;
- *Принято* – количество байт, принятых на интерфейсе GRE;
- *Передано* – количество байт, переданных с интерфейса GRE.

3.5.2 Подменю «Ethernet-порты»

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

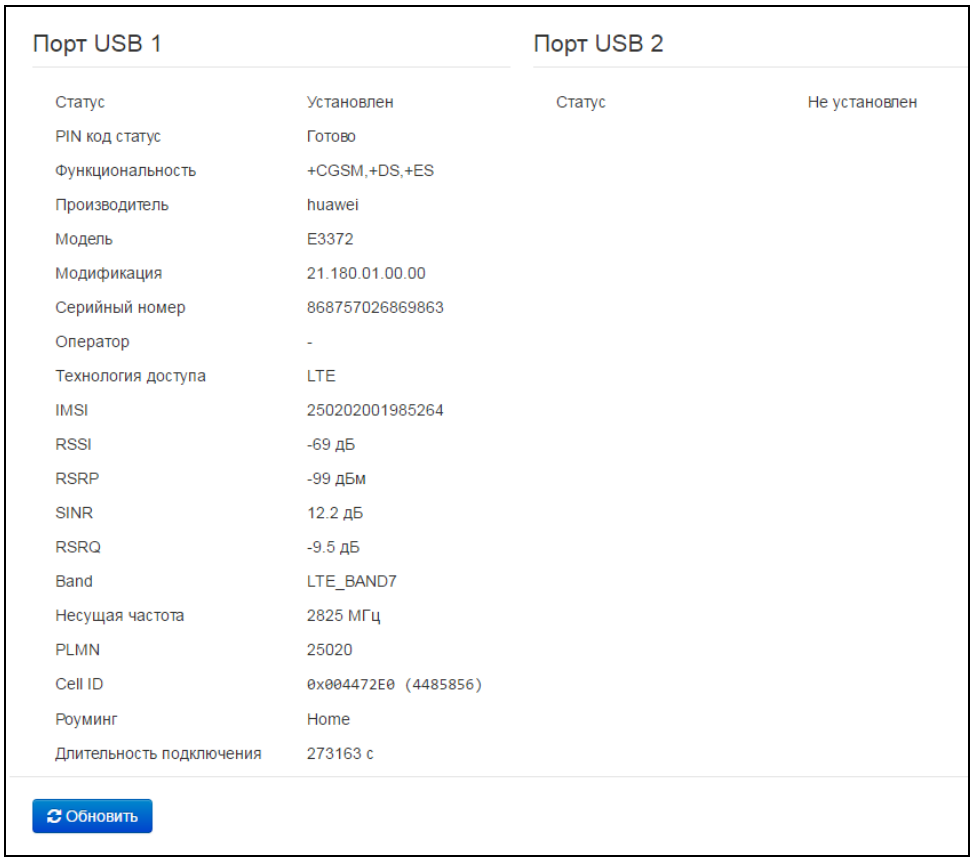
Состояние Ethernet-портов

- *Порт* – название порта:
  - LAN 1 – Ethernet порт локальной подсети.
- *Подключение* – состояние подключения к данному порту:
  - *Вкл.* – к порту подключено сетевое устройство (линк активен);
  - *Выкл.* – к порту не подключено сетевое устройство (линк не активен).
- *Скорость* – скорость подключения внешнего сетевого устройства к порту (10/100/1000 Мбит/с);
- *Режим* – режим передачи данных:
  - *Full-duplex* – полный дуплекс;
  - *Half-duplex* – полудуплекс.
- *Передано* – количество переданных байт с порта;
- *Принято* – количество принятых байт портом.

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

3.5.3 Подменю «USB модемы»

Подменю «USB модемы» позволяет получить информацию о статусе подключения USB-модемов к устройству, а так же текущую информацию о модемах и подключению к базовой станции.



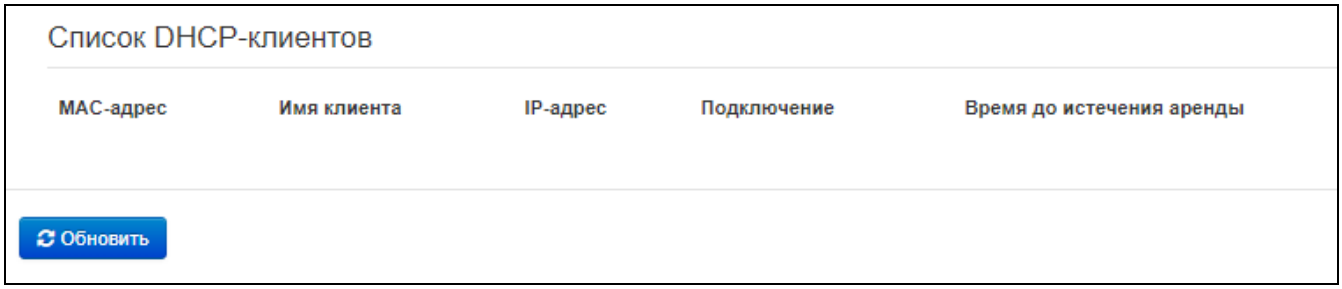
- *Статус* – состояние подключения USB модема к устройству;
- *PIN код статус* – состояние использования/проверки кода PIN SIM карты, установленной в USB модем:
  - *Готово* – PIN код из конфигурации прошел проверку.
  - *PIN код отсутствует в конфигурации* – требуется PIN код. PIN код в конфигурации не обнаружен;
  - *Ошибка SIM-карты* – вероятно не рабочая карта SIM (попробуйте извлечь SIM из модема и установить заново);
  - *Неправильный PIN код* – PIN код из конфигурации не прошел проверку;
  - *Модем не обнаружен* – устройство занято или не отвечает;
  - *Неизвестная ошибка* – не известная ошибка. Устройство вернуло соответствующий код, либо не отвечает.
- *Функциональность* – описывает текущие возможности USB-модема;
- *Производитель* – название производителя USB-модема;
- *Модель* – модель USB-модема;
- *Модификация* – версия программного обеспечения USB-модема;
- *Серийный номер* – номер USB-модема, присвоенный ему заводом изготовителем;
- *Оператор* – название оператора мобильной связи, к которому произведено подключение в данный момент;
- *Технология доступа* – технология, по которой было произведено подключения к оператору для передачи данных модемом (2G – GSM, 3G –WCDMA, 4G – LTE);
- *IMSI (International Mobile Subscriber Identity)* – международный идентификатор мобильного абонента (индивидуальный номер абонента), ассоциированный с каждым пользователем мобильной связи (идентификационный номер SIM-карты);
- *RSSI (Received Signal Strength Indicator)* – среднее значение мощности принимаемого пилотного сигнала;
- *RSRP (Reference Signal Received Power)* – уровень принимаемого сигнала с Базовой Станции.
- *SINR (Signal Interface + Noise Ratio)* – отношение уровня полезного сигнала к уровню шума в точке приема;
- *RSRQ (Reference Signal Received Quality)* – характеризует качество пронятых пилотных сигналов;
- *Band* – рабочий частотный диапазон;
- *Несущая частота* – несущая частота диапазона;
- *PLMN (Public Land Mobile Network ID)* – индекс сетевого кода мобильного оператора связи;
- *Cell ID* – идентификатор соты. Этот уникальный параметр присваивается оператором каждому сектору каждой БС и служит для его идентификации;
- *Роуминг* – принадлежность к зоне роуминга:
  - Home – вне зоны роуминга;

- Roaming – в зоне роуминга.

- *Длительность подключения* – продолжительность текущего подключения к сети оператора сотовой связи

3.5.4 Подменю «DHCP»

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



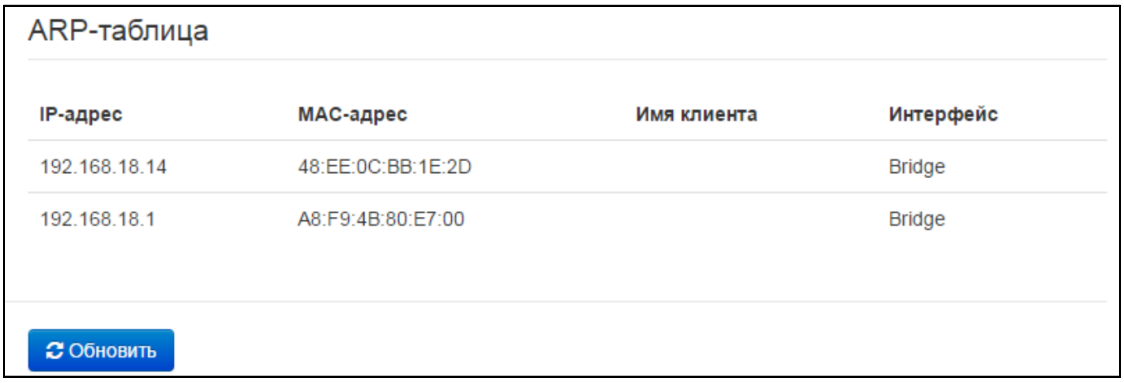
Активные DHCP-аренды

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

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

3.5.5 Подменю «ARP»

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



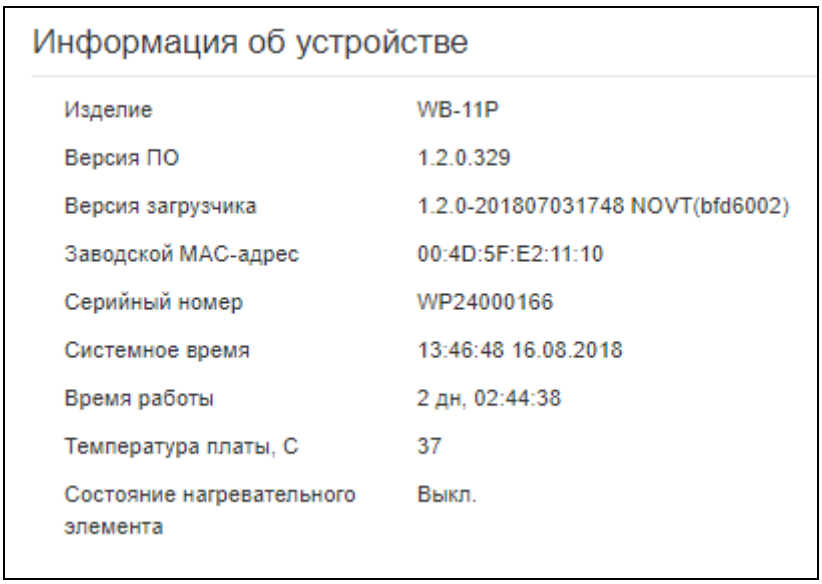
ARP-таблица

- *IP-адрес* – IP-адрес устройства;
- *MAC-адрес* – MAC-адрес устройства;

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

Для получения текущей информации нажмите кнопку «Обновить».

3.5.6 Подменю «Устройство»

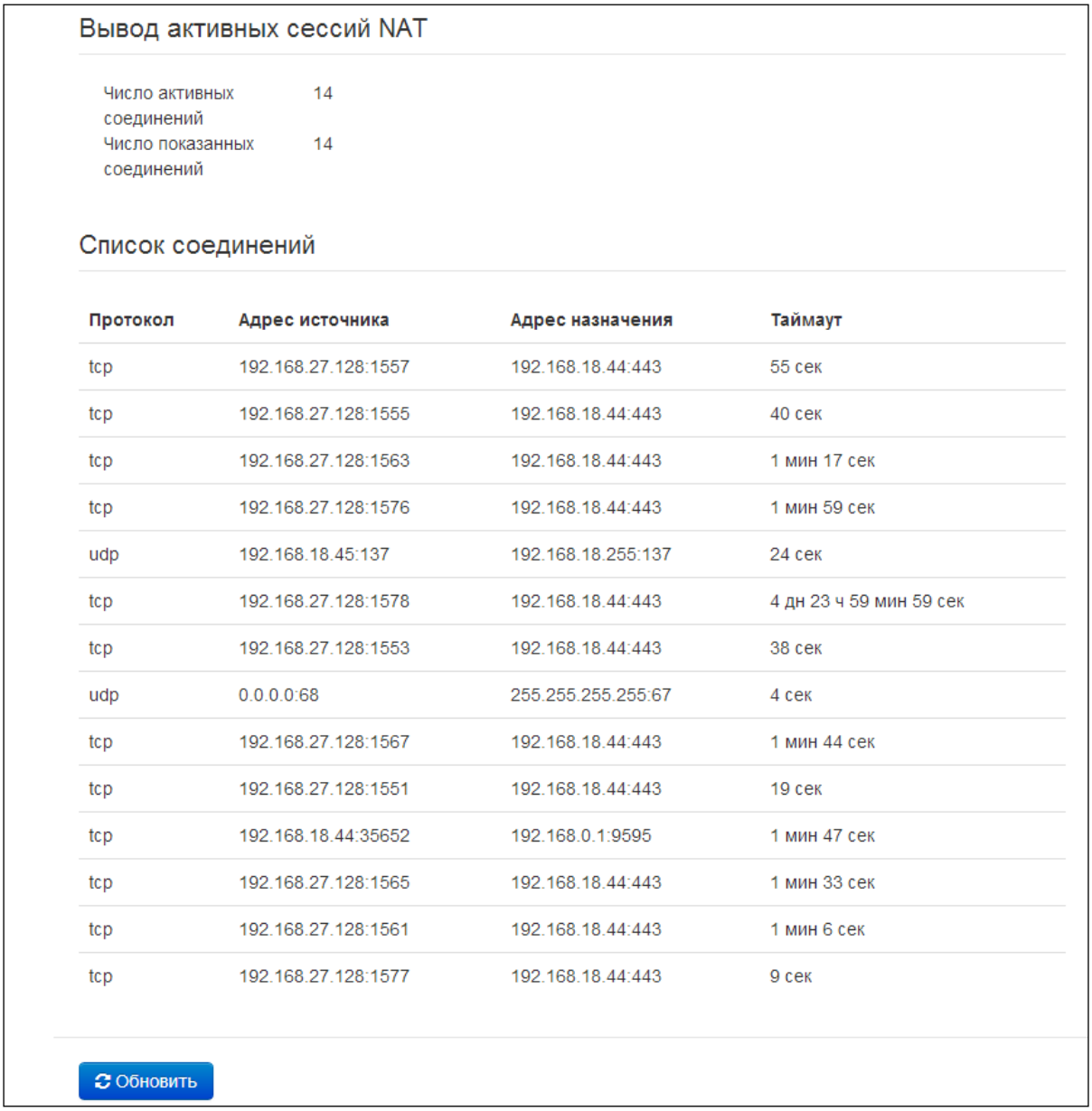


В подменю «Устройство» приведена общая информация об устройстве.

Информация об устройстве

- *Изделие* – наименование модели устройства;
- *Версия ПО* – версия программного обеспечения устройства;
- *Версия загрузчика* – версия программы загрузчика основной программы;
- *Заводской MAC-адрес* – MAC-адрес WAN-интерфейса устройства, установленный заводом-изготовителем;
- *Серийный номер* – серийный номер устройства, установленный заводом-изготовителем.
- *Системное время* – текущие время и дата, установленные в системе;
- *Время работы* – время работы с момента последнего включения или перезагрузки устройства;
- *Температура платы, С* – текущая температура датчика, который находится на плате;
- *Состояние нагревательного элемента* – состояние элемента, который нагревает устройство при низкой температуре окружающей среды.

3.5.7 Подменю «Conntrack»



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

Вывод активных сессий NAT

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

Список соединений

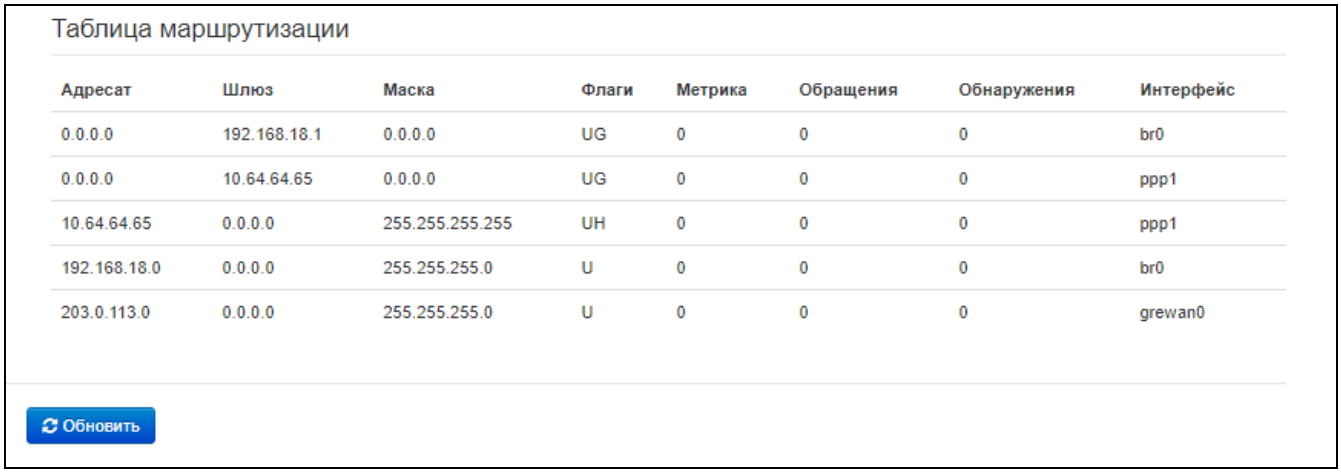
- *Протокол* – протокол, по которому установлено соединение;
- *Адрес источника* – IP-адрес и номер порта инициатора соединения;

- *Адрес назначения* – IP-адрес и номер порта адресата соединения;
- *Таймаут* – период времени до уничтожения соединения.

Для получения текущей информации нажмите кнопку «Обновить».

3.5.8 Подменю «Маршрутизация»

В подменю «Маршрутизация» отображается таблица маршрутизации устройства.



- *Адресат* – IP-адрес хоста или подсети назначения, до которых установлен маршрут;
- *Шлюз* – IP-адрес шлюза, через который осуществляется выход на адресата;
- *Маска* – маска подсети;
- *Флаги* – определенные характеристики данного маршрута. Существуют следующие значения *флагов*:
  - **U –** указывает, что маршрут создан и является проходимым;
  - **H –** указывает на маршрут к определенном узлу;
  - **G –** указывает, что маршрут пролегает через внешний шлюз. Сетевой интерфейс системы предоставляет маршруты в сети с прямым подключением. Все прочие маршруты проходят через внешние шлюзы. Флагом G отмечаются все маршруты, кроме маршрутов в сети с прямым подключением;
  - **R –** указывает, что маршрут, скорее всего, был создан динамическим протоколом маршрутизации, работающим на локальной системе, посредством параметра reinstate;
  - **D –** указывает, что маршрут был добавлен в результате получения сообщения перенаправления ICMP (ICMP Redirect Message). Когда система узнает о маршруте из сообщения ICMP Redirect, маршрут включается в таблицу маршрутизации, чтобы исключить перенаправление для последующих пакетов, предназначенных тому же адресату.
  - **M –** указывает, что маршрут подвергся изменению - вероятно, в результате работы динамического протокола маршрутизации на локальной системе и применения параметра mod;
  - **A –** указывает на буферизованный маршрут, которому соответствует запись в таблице ARP.
  - **C –** указывает, что источником маршрута является буфер маршрутизации ядра;

- **L –** указывает, что пунктом назначения маршрута является один из адресов данного компьютера. Такие «локальные маршруты» существуют только в буфере маршрутизации;
- **B –** указывает, что конечным пунктом маршрута является широковещательный адрес. Такие «широковещательные маршруты» существуют только в буфере маршрутизации;
- **I –** указывает, что маршрут связан с кольцевым (loopback) интерфейсом с целью иной, нежели обращение к кольцевой сети. Такие «внутренние маршруты» существуют только в буфере маршрутизации;
- **! –** указывает, что дейтаграммы, направляемые по этому адресу, будут отвергаться системой.

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

Для получения текущей информации нажмите кнопку «Обновить».

Пример настройки

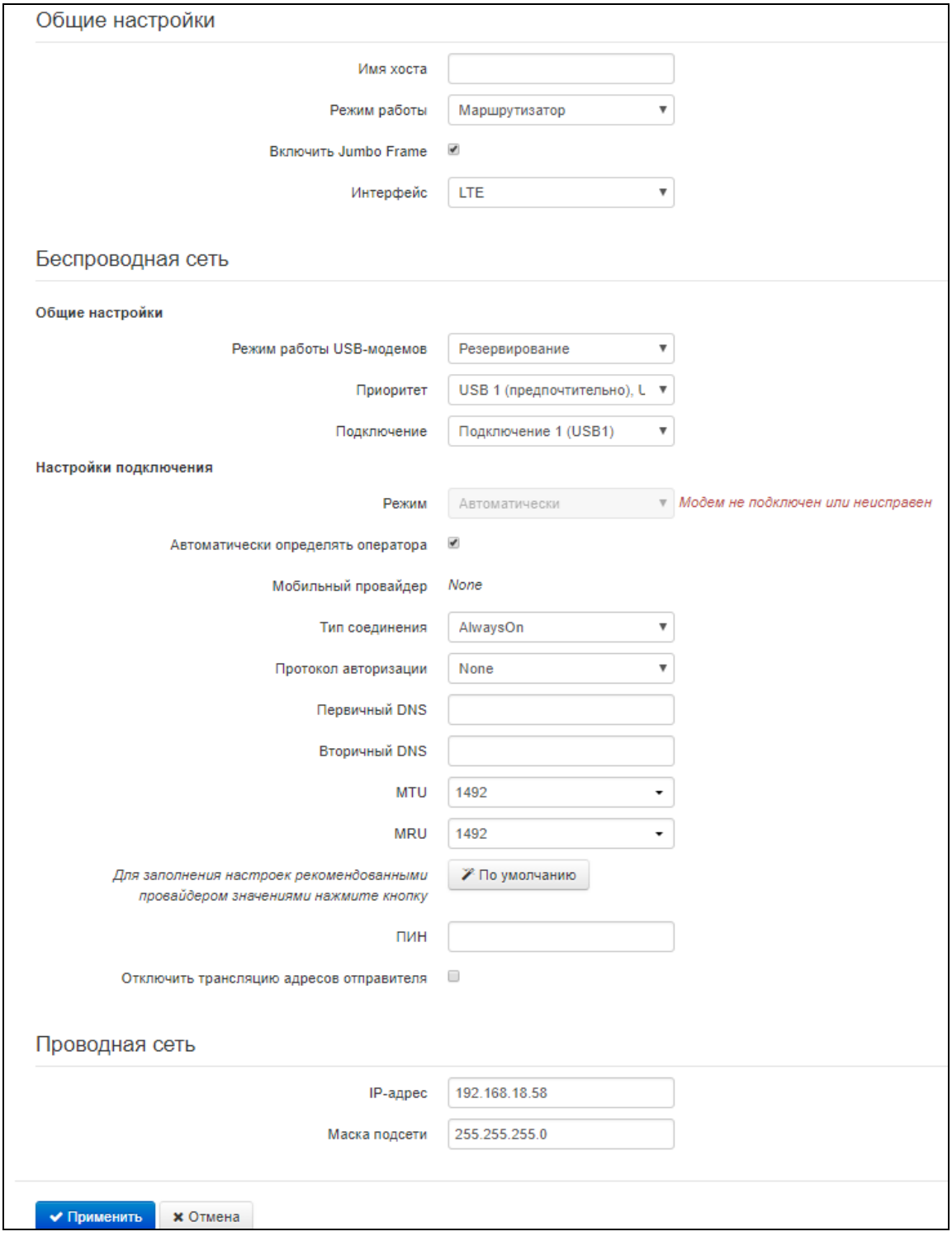
1. Подключите ПК к Ethernet порту устройства напрямую через инжектор PoE или другое сетевое оборудование выполняющее функцию PoE.

2. В адресной строке браузера введите IP-адрес устройства (по умолчанию 192.168.1.1), предварительно настроив статический IP-адрес на ПК из подсети 192.168.1.0/24 или получив сетевые настройки по протоколу DHCP.

3. При успешном подключении к устройству появится окно с запросом логина и пароля.

Укажите *Логин* – admin, *Пароль* – password. Нажмите кнопку «Войти».

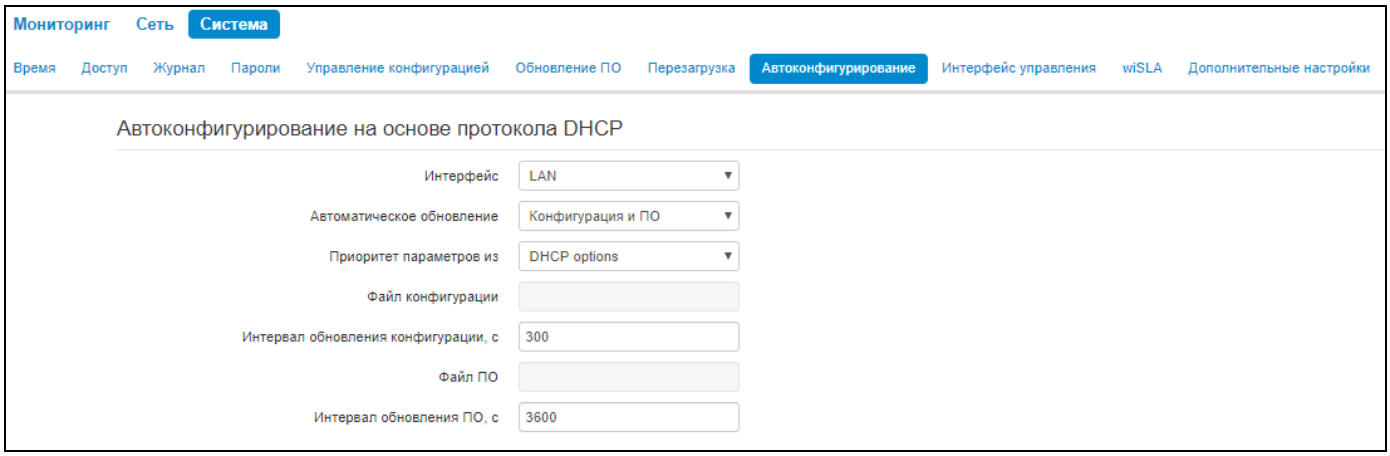
4. Для настройки внешнего соединения на верхней панели web-конфигуратора выберите меню «Сеть». На странице «Интернет» в поле «Подключение» выберите «Подключение 1», «Режим работы» - «Маршрутизатор». В поле «Режим» автоматически отобразится текущие режим для подключения, настроенный на USB модеме. Если в селекторе какой-то режим недоступен, значит он не поддерживается установленным USB модемом. Рекомендуется использовать режим «Автоматически». В заводской конфигурации оператор определяется автоматически, и для него используются настройки по умолчанию. Если нужно использовать специфические настройки, уберите флаг «Автоматически определять оператора». В поле «Мобильный провайдер» выберите одного из доступных провайдеров и нажмите кнопку «По умолчанию». Это приведет к автоматическому заполнению настроек подключения для выбранного провайдера. Если требуемого провайдера нет в списке, то выберите «Другой» и произведите настройку вручную. В поле «ПИН» введите PIN-код SIM-карты (если требуется).



5. Для настройки проводной части сетевого подключения, задайте IP-адрес и маску подсети в разделе «Проводная сеть».

6. Для сохранения и применения настроек нажмите кнопку «Применить».

4 АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP



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

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

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

- <protocol> – протокол, используемый для загрузки соответствующего файла с сервера (поддерживаются протоколы HTTP и TFTP);
- <server address> – адрес сервера, с которого необходимо загрузить файл (доменное имя или IPv4);
- <path to file> – путь к файлу на сервере.

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

- *$MA* – MAC address – вместо данного макроса в URL файла устройство подставляет собственный MAC-адрес;
- *$SN* – Serial number – вместо данного макроса в URL файла устройство подставляет собственный серийный номер;
- *$PN* – Product name – вместо данного макроса в URL файла устройство подставляет название модели (например, WB-10P);
- *$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/WB-10P/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_wb10p.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: wb10p.cfg;
- для имени файла программного обеспечения: wb10p.fw.

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

tftp://update.local/wb10p.cfg,

а URL файла ПО:

tftp://update.local/wb10p.fw.

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

   - для протокола: tftp;
   - для адреса сервера: update.local;
   - для имени файла конфигурации: wb10p.cfg;
   - для имени файла программного обеспечения: wb10p.fw.

Формат опции 43 (Vendor specific info)

1|<acs_url>|2|<pcode>|3|<username>|4|<password>|5|<server_url>|6|<config.file>|7|<firmware.file>|8|<vlan_tag>

1 - код адреса сервера автоконфигурирования по протоколу TR-069;
2 - код для указания параметра Provisioning code;
3 - код имени пользователя для авторизации на сервере TR-069;
4 - код пароля для авторизации на сервере TR-069;
5 - код адреса сервера; адрес сервера задается в формате URL: tftp://address или http://address. В первом варианте указан адрес сервера TFTP, во втором – HTTP;
6 - код имени файла конфигурации;
7 - код имени файла ПО;
8 - код тега VLAN для управления.
"|" - обязательный разделительный символ между кодами и значениями подопций.

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

1. Инициализация DHCP-обмена

После загрузки устройство инициирует DHCP-обмен.

2. Анализ опции 43

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

3. Анализ опции 66

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

Особенности обновления конфигурации.

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

Особенности обновления программного обеспечения.

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

Если текущая версия программного обеспечения совпадает с версией файла, полученного по протоколу DHCP, обновление ПО производиться не будет. Обновление производится только в случае несовпадения версий. О запущенном процессе записи образа программного обеспечения во flash-память устройства свидетельствует поочередное циклическое мигание индикатора «Power» зеленым, оранжевым и красным цветом.

Не отключайте питание и не перегружайте устройство во время записи образа во flash-память. Данные действия приведут к частичной записи ПО, что равноценно порче загрузочного раздела устройства. Дальнейшая работа устройства будет невозможна. Для восстановления работоспособности устройства воспользуйтесь инструкцией, которая приведена в разделе 5 «Процедура восстановления системы после сбоя при обновлении программного обеспечения**».**

5 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) и резервная версия ПО на шлюзе отсутствует или повреждена, в результате чего дальнейшая работа устройства стала невозможной (индикатор «Power» постоянно горит красным цветом), воспользуйтесь следующим алгоритмом восстановления работоспособности устройства:

- Распакуйте архив с файлом программного обеспечения.
- Подключите ПК к порту WAN устройства, установите на сетевом интерфейсе адрес из подсети 192.168.1.0/24.
- Запустите на ПК TFTP-клиента (для Windows рекомендуется использовать программу Tftpd32), в качестве адреса удалённого хоста укажите 192.168.1.6, а для передачи выберите файл linux.bin из распакованного архива программного обеспечения.
- Запустите команду отправки файла на удаленный хост (команда **Put**). Должен запуститься процесс передачи файла на устройство.
- Если процесс передачи файла начался – дождитесь его окончания, после чего WB-10P произведет запись программного обеспечения в память и автоматически выполнит запуск системы. Время записи составляет около 5 минут. Об успешном восстановлении устройства свидетельствует оранжевый или зеленый цвет индикатора «Power». При этом на устройстве сохраняется конфигурация, которая была до сбоя. Если подключиться к устройству не удаётся – произведите сброс на заводские настройки.
- Если процесс передачи файла не начался, убедитесь в корректности сетевых настроек компьютера и попробуйте еще раз. В случае неудачи – устройство необходимо отправить в ремонт либо выполнить восстановление, подключившись к устройству по COM-порту через специальный адаптер (при его наличии).

ПРИЛОЖЕНИЕ А. ЗАПУСК ПРОИЗВОЛЬНОГО СКРИПТА ПРИ СТАРТЕ СИСТЕМЫ

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

Для запуска произвольного скрипта в файле конфигурации создана секция настроек:

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

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

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

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

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

ПРИЛОЖЕНИЕ Б. ИЗМЕНЕНИЕ НАСТРОЕК ПО УМОЛЧАНИЮ ДЛЯ ОПЕРАТОРОВ ПРИ АВТОМАТИЧЕСКОМ ОПРЕДЕЛЕНИИ ОПЕРАТОРА

В ходе работы с устройством может потребоваться изменение настроек для отдельных операторов при автоматическом определении SIM-карты. Для этого настройки операторов хранятся в файле конфигурации на устройстве в секции:

```
 OperatorDefaultSettings:
Operator0:
  Name: "megafon"
  Username: ""
  Password: ""
  PhoneNumber: "*99#"
  AdditionalParams: "AT+CGDCONT=1,IP,internet"
Operator1:
  Name: "mts"
  Username: "mts"
  Password: "mts"
  PhoneNumber: "*99#"
  AdditionalParams: "AT+CGDCONT=1,IP,internet.mts.ru"
Operator2:
  Name: "beeline"
  Username: "beeline"
  Password: "beeline"
  PhoneNumber: "*99#"
  AdditionalParams: "AT+CGDCONT=1,IP,internet.beeline.ru"
    ...
```

В этой секции для каждого указанного оператора можно настроить свои параметры, которые будут использоваться при автоопределении.

ПРИЛОЖЕНИЕ В. ИСПОЛЬЗОВАНИЕ COMMAND LINE INTERFACE (CLI) ДЛЯ КОНФИГУРИРОВАНИЯ И МОНИТОРИНГА

Изменения в конфигурации, произведенные через CLI применяются без перезагрузки устройства.

Для сохранения изменений в энергонезависимую память устройства необходимо выполнить последовательно команды **commit** и **confirm.**

CLI предусматривает только привилегированный режим.

Команды **do**, **exit**, **help**, **history** и **top** доступны для большинства подменю, их назначение описано в таблице команд CLI в разделе **config** – **network**.

Перечень команд CLI:

Таблица В1 – Команды CLI

Команда									Значение	Описание	Функция команды no
logout									-	Завершить текущую сессию CLI	-
reboot									-	Перезагрузка устройства	
help									-	Вывести подсказки синтаксиса CLI	-
configure									(dir)	Режим конфигурирования устройства	-
	network								(dir)	Настройка сетевых параметров	-
		jumboframes	enable						-	Включить поддержку больших кадров	Выключить поддержку больших кадров
		router	<options>							Настройки режима маршрутизатора	-
			enable						-	Включает режим роутера на устройстве	-
			ip	<options>					-	Конфигурирование сетевого интерфейса	-
				address	<value>				IP-address	IP-адрес в локальной сети	--
				mask	<value>				netmask	Маска локальной сети	-
			masquerade	<options>					-	Настройка маскарадинга	-
				enable					-	Включить трансляцию адресов локальной подсети	-
				disable					-	Отключить трансляцию адресов локальной подсети	-
			interface	<value>					lte | gre0 | gre1	Интерфейс для интернета	-
		bridge	<options>						-	Настройка режима моста	-
			enable						-	Включает режим моста на устройстве	-

			mode	<value>					static | dhcp	Режим получения ip-адреса на локальном интерфейсе	-
			ip	<options>					-	Настройки сетевого интерфейса, который будет использоваться при выборе mode – static	-
				address	<value>				IP-address	IP-адрес в локальной сети, который используется при выборе mode – static	-
				mask	<value>				netmask	Маска локальной сети, который используется при выборе mode – static	-
		traffic-shape	<options>						-	Настройки шейпинга трафика	-
			egress	<value>					int: 0..1048576	Ограничение скорости исходящего трафика	-
			ingress	<value>					int: 0..1048576	Ограничение скорости входящего трафика	-
			mode	<value>					enable | disable	Настройка включения/выключения шейпинга трафика	
		do							-	Позволяет выполнять команды корневого режима из любого другого режима командного интерфейса.	-
		exit							-	Переход на уровень выше в структуре команд CLI	-
		help							-	Вывести подсказки синтаксиса CLI	-
		history							-	Просмотр истории команд CLI	-
		no	<command>						Результат использования команды no с различными командами указан в столбце «Функция команды no»	Использование отрицательной команды	-
		top							-	Возвращает в корневой режим	-
	autoprovision	<options>							-	Настройки автоконфигурирования	-
		cwmp							(dir)	Настройки автоконфигурирования по протоколу TR-069	-
			acs	<options>					-	Настройки авторизации на сервере автоконфигурирования	-

				authname	<value>				string	Логин для авторизации на сервере автоконфигурирования	-
				password	<value>				string	Пароль для авторизации на сервере автоконфигурирования	-
			client	<options>					-	Настройки авторизации для входящих запросов с сервера	-
				authname	<value>				string	Логин для авторизации входящих запросов с сервера	-
				password	<value>				string	Логин для авторизации входящих запросов с сервера	-
			enable						-	Включить автоконфигурирование по протоколу TR-069	Выключить автоконфигурирование по протоколу TR-069
			interface	<value>					lan | lte | gre0 | gre1	Интерфейс, на котором будет запущено автоконфигурирование по протоколу TR-069	-
			nat	mode	<options>				-	Настройки режима NAT	-
					disable				-	Не используется NAT	-
					stun	<options>			-	Настройки использования STUN сервера для определения типа NAT	-
						enable			-	Использовать STUN сервер для определения типа NAT	Не использовать STUN сервер для определения типа NAT
						address	<value>		IP-address	Адрес STUN-сервера	-
						port	<value>		int: 1..65535	Порт STUN-сервера	-
						keepalive	<options>		-	Параметры опроса сервера	-
							min	<value>	int: 10..2147483647	Минимальный период опроса	-
							max	<value>	int: 10..2147483647	Максимальный период опроса	-
					manual	<options>			-	Настройки ручного задания параметров NAT	-
						enable			-	Включить ручное задание параметров NAT	Выключить ручное задание параметров NAT
						address	<value>		IP-address	Публичный адрес	-
			periodic	<options>					-	Настройки периодического опроса ACS сервера	-
				enable					-	Включить периодический опрос ACS сервера	Выключить периодический опрос ACS сервера
				interval	<value>				-	Период опроса сервера	-
			url	<value>					string	Адрес сервера автоконфигурирования	-
		dhcpbased							(dir)	Настройки автоконфигурирования по	-

										протоколу DHCP	
			cfg_file	<value>					string	Имя файла конфигурации	-
			cfg_interval	<value>					int: 0..1000000	Интервал обновления конфигурации	-
			fw_file	<value>					string	Имя файла прошивки	-
			fw_interval	<value>					int: 0..1000000	Интервал обновления прошивки	-
			interface	<value>					lan | lte | gre0 | gre1	Выбор интерфейса для автоконфигурирования по протоколу DHCP	-
			mode	<value>					disable | cfg_only | cfg_and_fw | fw_only	Режим автоконфигурирования по протоколу DHCP	-
			priority	<value>					dhcp | static	Настройка приоритета параметров из опций DHCP или из статических настроек	-
	clock	<options>							-	Настройки системного времени	-
		auto	time	<value>					enable | disable	Включение автоматического перехода на летнее/зимнее время	Установить параметры по умолчанию
		timezone	<value>						int: -12..+12	Настройка часового пояса	Установить часовой пояс по умолчанию
	hostname	<value>							string	Задание сетевого имени устройства	Установить сетевое имя устройства по умолчанию
	ip	set							(dir)	Сетевые настройки устройства	-
			http	port	<value>				int: 1..65535	Назначение порта для доступа по протоколу http	Установка порта для доступа по протоколу http в значение по умолчанию
			https	port	<value>				int: 1..65535	Назначение порта для доступа по протоколу https	Установка порта для доступа по протоколу https в значение по умолчанию
			ssh	port	<value>				int: 1..65535	Назначение порта для доступа по протоколу ssh	Установка порта для доступа по протоколу ssh в значение по умолчанию
			telnet	port	<value>				int: 1..65535	Назначение порта для доступа по протоколу telnet	Установка порта для доступа по протоколу telnet в значение по умолчанию
			route	<value>					int: 1..30	Настройка статических маршрутов	-
					enable				-	Включить текущий статический маршрут	-
					name				string	Название маршрута	
					destination	ip	<value>		IP-address	IP-адрес назначения	-
					gateway	<value>			IP-address	Шлюз для текущего маршрута	-
					mask	<value>			netmask	Маска подсети назначения	-
					metric	<value>			metric	Метрика	-
				add							Создание нового маршрута

				del	<value>				int: 1..30		Удаление маршрута
				show	<options>						-
					all						Вывести информацию обо всех маршрутах
					<value>				int: 1..30		Вывести информацию об одном маршруте
	log								(dir)	Настройки логирования	-
		configd							(dir)	Настройки логирования конфигурации	-
			debug	enable					-	Включить вывод отладочных сообщений	Выключить вывод отладочных сообщений
			errors	enable					-	Включить вывод сообщений об ошибках	Выключить вывод сообщений об ошибках
			info	enable					-	Включить вывод информационных сообщений	Выключить вывод информационных сообщений
			warnings	enable					-	Включить вывод предупреждений	Выключить вывод предупреждений
			output	<value>					disable | console | telnet | syslog	Выбор места вывода логов	Установить место вывода логов в значение по умолчанию
		networkd							(dir)	Настройки логирования сетевой службы	
			debug	enable					-	Включить вывод отладочных сообщений	Выключить вывод отладочных сообщений
			errors	enable					-	Включить вывод сообщений об ошибках	Выключить вывод сообщений об ошибках
			info	enable					-	Включить вывод информационных сообщений	Выключить вывод информационных сообщений
			warnings	enable					-	Включить вывод предупреждений	Выключить вывод предупреждений
			output	<value>					disable | console | telnet | syslog	Выбор места вывода логов	Установить место вывода логов в значение по умолчанию
		usb-modems							(dir)	Настройки логирования USB-модемов	
			debug	enable					-	Включить вывод отладочных сообщений	Выключить вывод отладочных сообщений
			errors	enable					-	Включить вывод сообщений об ошибках	Выключить вывод сообщений об ошибках
			info	enable					-	Включить вывод информационных сообщений	Выключить вывод информационных сообщений
			warnings	enable					-	Включить вывод предупреждений	Выключить вывод предупреждений
			output	<value>					disable | console | telnet | syslog	Выбор места вывода логов	Установить место вывода логов в значение по умолчанию
		syslog							(dir)	Настройки Syslog	-
			enable						-	Включить Syslog	Выключить Syslog
			mode	<value>					server | local | server/local	Режим вывода Syslog	Установить режим вывода Syslog в значение по умолчанию
			server	<options>					-	Настройки сервера Syslog	-
				ip	<value>				IP-address	IP-адрес сервера Syslog	Установить IP-адрес сервера Syslog в значение по умолчанию
				port	<value>				int: 1..65535	Порт сервера Syslog	Установить порт сервера Syslog в значение по умолчанию

	ntp	<options>							-	Параметры синхронизации времени по NTP	-
		mode	<value>						enable | disable	Включение синхронизации времени по протоколу NTP	Установить параметр в значение по умолчанию
		remote	peer	<value>					IP-address	Адрес сервера NTP	Установить адрес сервера NTP в значение по умолчанию
	qos								(dir)	Настройки качества обслуживания	
		flow	control	<value>					enable | disable	Включение и выключение контроля потока	Установить контроль потока в значение по умолчанию
		priority	decision	<value>					DSCP | 802.1p	Настройка выбора приоритетов	Установить выбор приоритетов в значение по умолчанию
		queue	type	<value>					STRICT | WFQ	Выбор типа очереди	Установить тип очереди в значение по умолчанию
	security								(dir)	Настройки безопасности	-
		firewall	rule	<value>					int: 1..30 (dir)	Редактирование правил сетевого экрана	-
					action	<value>			ACCEPT | DROP	Действие, совершаемое с пакетом, подходящим под текущее правило	Установить действие по умолчанию
					destination	<options>			-	Параметры получателя	-
						ip	<value>		IP-address	IP-адрес получателя	Установить IP-адрес получателя по умолчанию
						port	<value>		int: 1..65535	Порт получателя	Установить порт получателя по умолчанию
					enable				-	Включить текущее правило	Выключить правило
					name	<value>			string	Название правила	Удалить название правила
					protocol	<value>			tcp | udp | tcp/udp | icmp | any	Выбор протокола	Установить протокол в значение по умолчанию
					source	<options>			-	Параметры отправителя	-
						ip	<value>		IP-address	IP-адрес отправителя	Установить IP-адрес отправителя по умолчанию
						port	<value>		int: 1..65535	Порт отправителя	Установить порт отправителя по умолчанию
					type	<value>			Input | Output | Forward	Тип правила сетевого экрана	Установить тип правила в значение по умолчанию
		mac	filter	<options>					-	Настройка фильтра MAC-адресов	-
				client	<value>	address	<value>		int: || MAC-address	Задание MAC адреса, который будет находится в выбранном списке	Удалить выбранный MAC из списка
				mode	<value>				disabled | allow | deny	Режим фильтра	Установить режим фильтра в значение по умолчанию
		nat	rule	<value>					int: 1..10 (dir)	Настройки проброса портов	-
					destination	<options>			-	Параметры получателя	-
						ip	<value>		IP-address	IP-адрес получателя	Установить IP-адрес получателя в значение по умолчанию

						port	<value>		int: 1..65535	Порт получателя	Установить порт получателя в значение по умолчанию
					enable				-	Включить текущее правило	Выключить текущее правило
					ip	address	<value>		IP-address	Выбор IP-адресов, предназначенных для замены	Установить IP-адреса по умолчанию
					name	<value>			string	Название правила	Удалить название правила
					protocol	<value>			tcp | udp | tcp/udp | any	Протокол, для которого действует текущее правило	Установить значение протокола
					source	<options>			-	Параметры отправителя	-
						ip	<value>		IP-address	IP-адрес отправителя	Установить значение IP-отправителя в значение по умолчанию
						port	<value>		int: 1..65535	Порт отправителя	Установить порт отправителя в значение по умолчанию
					target	ip	<value>		IP-address	IP-адрес после преобразования	Установить IP-адрес после преобразования в значение по умолчанию
					type	<value>			dnat | snat | masquerade	Тип правила	Установить тип правила в значение по умолчанию
		ping	wireless	<value>					enable | disable	Включить или выключить возможность доступа к устройству по протоколу ICMP	Выключить возможность доступа к устройству по протоколу ICMP
		ssh	<options>						-	Настройки доступа к устройству по протоколу SSH	-
			wired	<value>					enable | disable	Включить или выключить доступ к устройству через проводной интерфейс	Выключить доступ к устройству через проводной интерфейс
			wireless	<value>					enable | disable	Включить или выключить доступ к устройству через беспроводной интерфейс	Выключить доступ к устройству через беспроводной интерфейс
		telnet	<options>						-	Настройки доступа к устройству по протоколу Telnet	
			wired	<value>					enable | disable	Включить или выключить доступ к устройству через проводной интерфейс	Выключить доступ к устройству через проводной интерфейс
			wireless	<value>					enable | disable	Включить или выключить доступ к устройству через беспроводной интерфейс	Выключить доступ к устройству через беспроводной интерфейс
		web	<options>						-	Настройки доступа к устройству по протоколу HTTP	
			wired	<value>					enable | disable	Включить или выключить доступ к устройству через проводной	Выключить доступ к устройству через проводной интерфейс

										интерфейс	
			wireless	<value>					enable | disable	Включить или выключить доступ к устройству через беспроводной интерфейс	Выключить доступ к устройству через беспроводной интерфейс
	snmp								-	Настройка мониторинга устройства по протоколу SNMP	-
		enable							-	Включить SNMP	Выключить SNMP
		informsink	<value>						string	Адрес для приёма сообщений Inform	Установить адрес для приёма сообщений Inform в значение по умолчанию
		rocommunity	<value>						string	Пароль на чтение	Установить пароль на чтение в значение по умолчанию
		rwcommynity	<value>						string	Пароль на запись	Установить пароль на запись в значение по умолчанию
		syscontact	<value>						string	Контактная информация производителя	Установить контактную информацию производителя в значение по умолчанию
		syslocation	<value>						string	Местоположение устройства	Установить местоположение устройства в значение по умолчанию
		sysname	<value>						string	Системное имя устройства	Установить системное имя устройства в значение по умолчанию
		trap2sink	<value>						string	Адрес приёма трапов v2	Установить адрес приёма трапов v2 в значение по умолчанию
		trapcommunity	<value>						string	Пароль в трапах	Установить пароль в трапах в значение по умолчанию
		trapsink	<value>						string	Адрес приёма трапов v1	Установить адрес приёма трапов v1 в значение по умолчанию
	tunnel	gre	<value>						0 | 1 (dir)	Настройки GRE-туннелей	-
				ip	<options>				-		-
					address	<value>			IP-address	IP-адрес интерфейса GRE	-
					mask	<value>			netmask	Маска интерфейса GRE	-
					gateway	<value>			IP-address	Шлюз по умолчанию интерфейса GRE	-
					dns	<value>	<value>		IP-address	Адрес сервера DNS интерфейса GRE	-
				enable					-	Включить текущий интерфейс GRE	Выключить текущий интерфейс GRE
				keepalive	<value>				IP-address	IP-адрес сервера контроля GRE	Выключить контроль GRE
				localaddr	<value>				IP-address	Локальный IP-адрес	-
				mtu	<value>				int:	Размер MTU для интерфейса GRE	Установить MTU в значение по умолчанию
				name	<value>				string	Имя интерфейса GRE	-
				remoteaddr	<value>				IP-address	Удалённый IP-адрес	-

				ttl	<value>				int: 0..255	Переопределить TTL для интерфейса GRE	Установить TTLв значение по умолчанию
				type	<value>				gre, gretap	Выбор типа GRE	-
		l2tp	<value>						0 | 1 (dir)	Настройки L2TP-туннелей	
				connection	type					Настройка типа соединения	
						alwayson				Соединение активно всегда	
						ondemand				Соединение активно только когда происходит передача трафика	
						manual				Запрос на установление соединения отправляется по нажатии кнопки в WEB-конфигураторе	
				enable					-	Включить текущий интерфейс L2TP	Выключить текущий интерфейс L2TP
				name	<value>				string	Имя интерфейса L2TP	-
				username	<value>				string	Имя пользователя для авторизации на сервера L2TP	
				password	<value>				string	Пароль для авторизации на сервера L2TP	
				server					IP-address	IP-адрес сервера L2TP	
				timers	<option>					Настройка таймеров для туннеля	
					echofailure					Количество потерянных LCP-echo запросов, нужное для отключения туннеля	
					echointerval					Период отправки LCP-echo запросов	
					idle					Таймаут неактивности	
				mtu	<value>				int:	Размер MTU для интерфейса GRE	Установить MTU в значение по умолчанию
		openvpn	<value>						0 | 1 (dir)	Настройки OpenVPN-туннелей	
				name	<value>				string	Имя интерфейса Open VPN	-
				authtype						Тип авторизации	
					User					Авторизация при помощи связки логин/пароль	
					Key					Авторизация при помощи сертификатов и ключей	
				enable					-	Включить текущий интерфейс L2TP	Выключить текущий интерфейс L2TP
				username	<value>				string	Имя пользователя для авторизации на сервера Open VPN	
				password	<value>				string	Пароль для авторизации на сервера Open VPN	
				server					IP-address	IP-адрес сервера Open VPN	

				port					int 1..65535	Порт, на который будут отправляться запросы для подключения к серверу Open VPN	
				auth	<value>				string	Алгоритм, используемый при авторизации	-
				cipher	<value>				string	Используемый алгоритм шифрования	-
				download					-	-	-
					ca	<value>			URL	Ссылка для скачивания сертификата удостоверяющего центра	-
					client				-	-	-
						cert			-	Ссылка для скачивания клиентского сертификата	-
						key			-	Ссылка для скачивания клиентского ключа	-
	usb-modem	<options>							-	Настройки USB-модемов	-
		priority	<value>						USB1 | USB2	Выбор приоритетного подключения	Установить приоритетное подключение в значение по умолчанию
		mode	<value>						reservation | aggregation	Режим работы USB-модемов	Установить режим работы модемов в значение по умолчанию
		connection	<value>						1 | 2 (dir)	Настройки подключения	
				additional_ parametres					string	Дополнительные параметры инициализации	Установить дополнительные параметры инициализации в значение по умолчанию
				login					string	Имя пользователя для подключения	Установить имя пользователя в значение по умолчанию
				mode					2G | 3G | 4G | auto	Выбор режима работы модемов	Установить режим работы модема в значение по умолчанию
				mru					int: 68..1500	Настройка MRU для интерфейса	Установить MRU в значение по умолчанию
				mtu					int: 68..1500	Настройка MTU для интерфейса	Установить MTU в значение по умолчанию
				number					string	Номер дозвона	Установить номер дозвона в значение по умолчанию
				password					string	Пароль для подключения	Удалить пароль для подключения
				pin					string	ПИН-код сим-карты	Удалить ПИН-код
				ppptype					alwayson | ondemand	Тип соединения	Установить тип соединения в значение по умолчанию
				usb-port					USB1 | USB2	Порт USB	Установить порт USB в значение по умолчанию
	username	admin	password	<value>					string	Изменения пароля администратора	Установить пароль администратора в значение по умолчанию

	management										
		destination	<value>						IP-address	Удалённый адрес для создания туннеля GRE управления	
		source	<value>						IP-address	Локальный адрес для создания туннеля GRE управления	
		enable								Включить интерфейс управления	Выключить интерфейс управления
		keepalive	<value>						IP-address	IP-адрес ping-сервера для проверки активности туннеля	
		mtu	<value>						int:	Размер MTU для интерфейса GRE управления	Установить MTU в значение по умолчанию
		ttl	<value>						int: 0..255	Переопределить TTL для интерфейса GRE управления	Установить TTL в значение по умолчанию
		type	<value>						gre | gretap	Установить тип GRE управления	
		vlan	<vlaue>						int: 1..4096	Задать метку VLAN для интерфейса управления	Убрать метку VLAN для интерфейса управления
	wisla								-	Настройки wiSLA	-
		enable							-	Включить сервис wiSLA	Выключить сервис wiSLA
		host	<value>						string	Установить имя клиента wiSLA	-
		logging	<value>						error | warning | notice | information | debug | trace	Установить уровень логирования	-
		portal	<value>						string | IP-address	Установить адрес портала wiSLA	-
		sendperiod	<value>						-	Установить период отправки сообщений	-
debug									-	Вход в режим отладки	-
	ps								-	Ввод списка процессов, выполняемых на устройстве	-
	reboot								-	Перезагрузка устройства	-
arp	<options>	<value>							-a | -i | -d | -s | -v | -n | -p | -H || IP-address	Использование утилиты arp	-
at	<value>	<options>							int 1..2	Команда для использования утилиты AT, для взаимодействия с USB-модемами	-
		get							-	Получение списка доступных режимов работы модема	-
		set	<value>						2G | 3G | 4G | auto	Установка режима работы модема	-
		pin	<value>						status | enable | disable	Настройка работы с ПИН-кодом	-
backup	<value>	<value>							host || string	Выгрузка конфигурации с устройства	-
boot	system	<value>							bank1 | bank2	Смена образа для загрузки системы	-
commit									-	Подтверждение применения изменений	-

confirm									-	Сохранение изменений в энергонезависимую память	-
monitor	<value>	<value>	<options>						loopback | lan | ppp1 | ppp2 | gre1 | gre2 || int: 1..65535 || <tcpdump_options>	Использование утилиты tcpdump	-
restore	<value>	<value>							host || string	Загрузка конфигурации на устройство	-
rollback									-	Сброс устройства к заводским настройкам	-
shell									-	Переход в консоль linux	-
show	<options>								-	Команда для вывода информации о системе	-
	bootvar								-	Выводит информацию об образах программного обеспечения, которые загружены в системе	-
	interfaces								-	Выводит список сетевых интерфейсов и информацию о них	-
	ip	<options>								-	
		route							<route_options>	Выводит информацию о маршрутах в системе	-
		static-route							-	Выводит информацию о настроенных в системе статических маршрутах	-
	tunnels								-	Выводит информацию о настроенных туннелях	-
		gre								Выводит информацию о настроенных туннелях GRE	
		l2tp								Выводит информацию о настроенных туннелях L2TP	
		openvpn								Выводит информацию о настроенных туннелях OpenVPN	
upgrade	image	<value>	<value>						host || string	Обновление программного обеспечения	-
uptime									-	Выводит информацию о времени работы устройства с последней перезагрузки	-

ПРИЛОЖЕНИЕ Г. ИНСТРУКЦИЯ ПО УСТАНОВКЕ УСТРОЙСТВА

Рекомендации по установке

1. Рекомендуемое устанавливаемое положение: крепление на трубостойку/столб или стену.
2. Перед установкой и включением устройства необходимо проверить устройство на наличие видимых механических повреждений. В случае наличия повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику.
3. Устройство должно быть установлено на трубостойку/столб или стену таким образом, чтобы LAN-порт был направлен вниз.
4. Незадействованные антенные разъемы требуется закрыть защитной крышкой, которая входит в комплект поставки устройства.
5. Не производите установку данного устройства во время грозы. Может существовать риск удара молнией.
6. Необходимо соблюдать требования по напряжению, току и частоте, указанные в данной инструкции.
7. Перед подключением к устройству измерительных приборов и компьютера, их необходимо предварительно заземлить. Разность потенциалов между корпусами оборудования и измерительных приоров не должна превышать 1В.
8. Перед включением устройства убедиться в целостности кабелей и их надежном креплении к разъемам.
9. Во время монтажа устройства на высотных конструкциях следует выполнять установленные нормы и требования при высотных работах.
10. Эксплуатация устройства должна производиться инженерно-техническим персоналом, прошедшим специальную подготовку.
11. Подключать к устройству только годное к применению вспомогательное оборудование.

Устройство крепится на трубостойку/столб или стену, соблюдая инструкции по технике безопасности и рекомендации, приведенные выше.

В комплект поставки устройства входит необходимый комплект крепежа устройства на трубостойку/столб и стену.

Порядок установки устройства

1. Крепление кронштейнов к устройству;
2. Крепление устройства на трубостойку/столб или стену;
3. Подключение кабелей к разъемам устройства;
4. Установка антенн.

Порядок крепления кронштейнов к устройству

При монтаже устройства на разъемы антенн обязательно должны быть установлены пылезащитные (герметичные) колпачки, которые входят в комплект поставки устройства. Снимать колпачки нужно непосредственно перед подключением к антенным разъемам.

1. Соберите кронштейн для крепления на трубостойку:

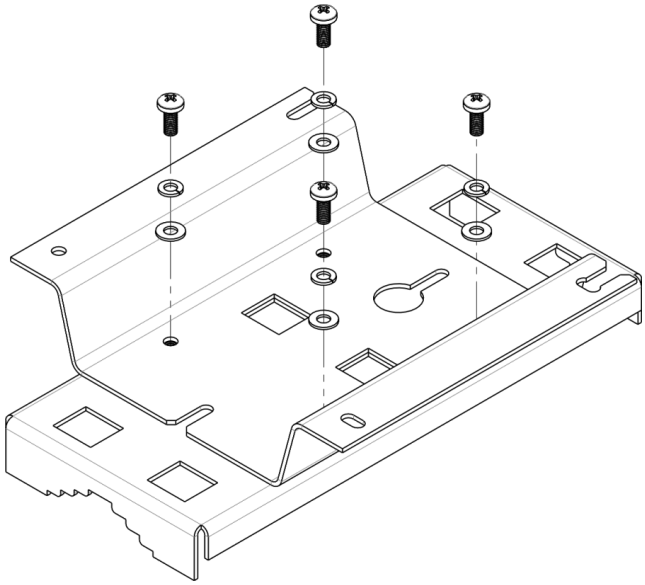


Рисунок Г1 – Кронштейн для крепления на трубостойку

a) Соедините кронштейн, который будет крепиться на трубостойку, с кронштейном, который будет крепиться к устройству, как показано на рисунке Г1.

b) Совместите два отверстия для винтов на обоих кронштейнах. С помощью отвертки прикрепите кронштейны друг к другу.

2. Закрепите кронштейн на трубостойке:

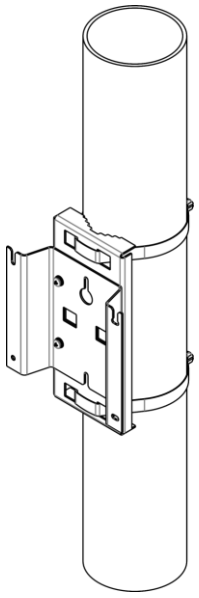


Рисунок Г2 – Крепление кронштейна на трубостойку

a) При помощи хомутов закрепите кронштейн на трубостойку, рисунок Г2.

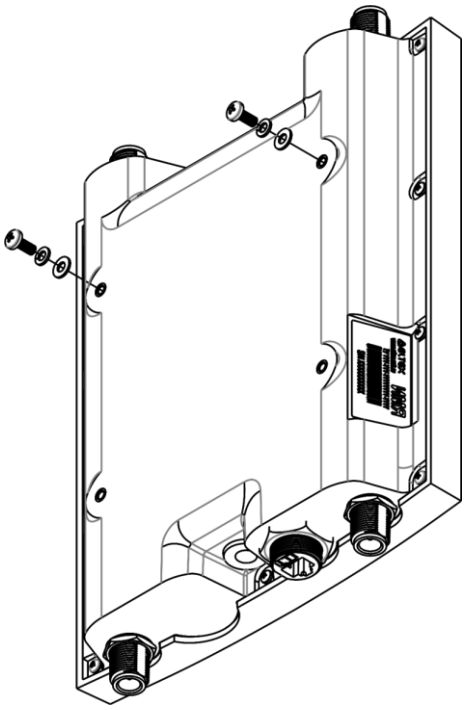


Рисунок Г3 – Крепление винтов к устройству

b) В верхние крепежные отверстия на корпусе WOP-2ac установите шайбы и винты DIN7985 M6. Винты не нужно закручивать до конца, оставьте зазор минимум 3 мм, рисунок Г3.

3. Закрепите устройство на трубостойке:

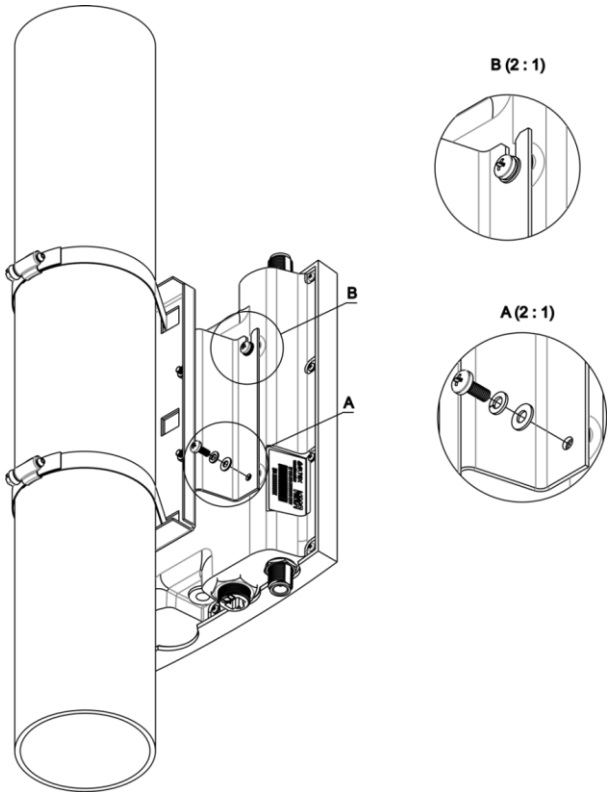


Рисунок Г4 – Крепление устройства на трубостойке

a) Установите устройство на незакрученные верхние винты кронштейна, который прикреплен к трубостойке, рисунок Г4.

b) В нижние отверстия крепления установите винты, рисунок Г4.

c) С помощью отвертки затяните верхние и нижние винты.

Порядок крепления устройства на стену

1. Установите кронштейн (входит в комплект поставки) для крепления на стене:

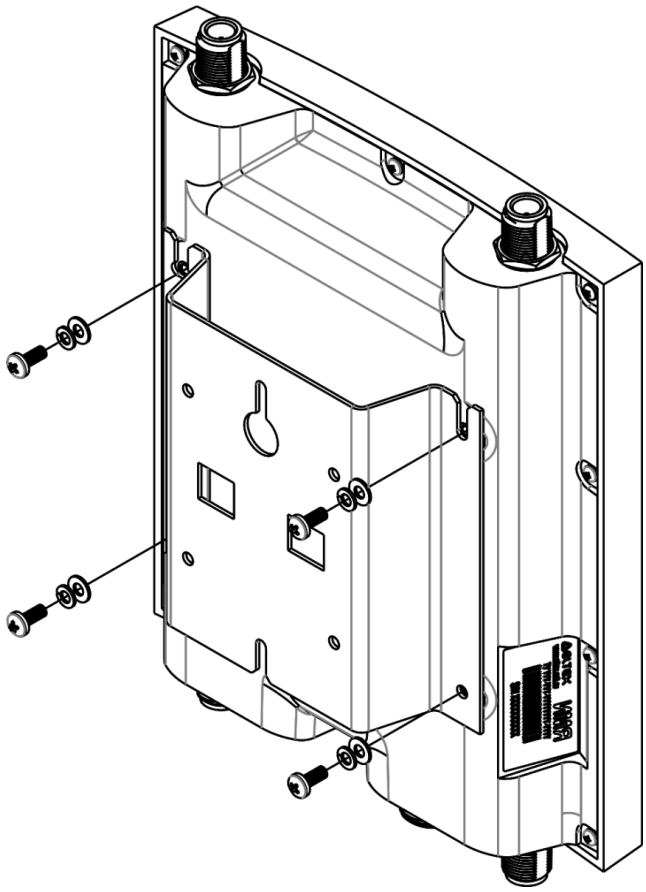


Рисунок Г5 – Крепление кронштейна

a) Расположение кронштейна на устройстве показано на рисунке Г5.

b) Совместите четыре отверстия для винтов на кронштейне с такими же отверстиями на устройстве. С помощью отвертки прикрепите кронштейн винтами к устройству.

2. Установите шурупы на стене на расстоянии 100 мм друг от друга как показано на рисунке Г6.

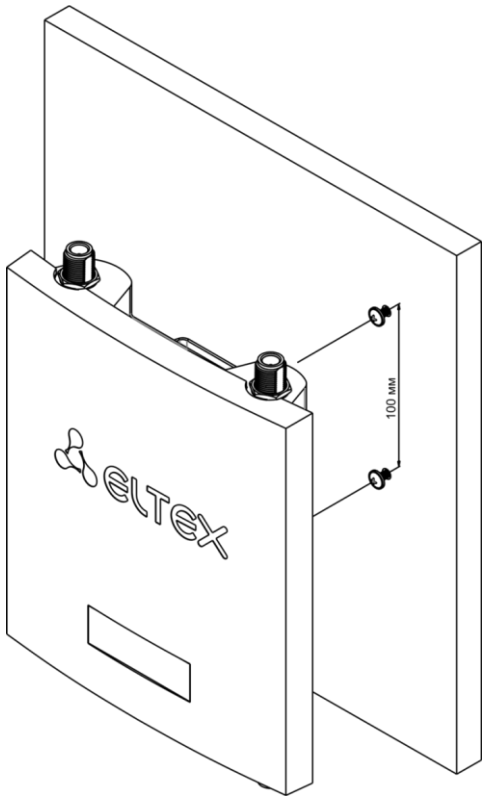


Рисунок Г6 – Крепление устройства на стене

3. Закрепите устройство на стене. Габариты устройства после установки относительно крепежных отверстий представлены на рисунке Г7.

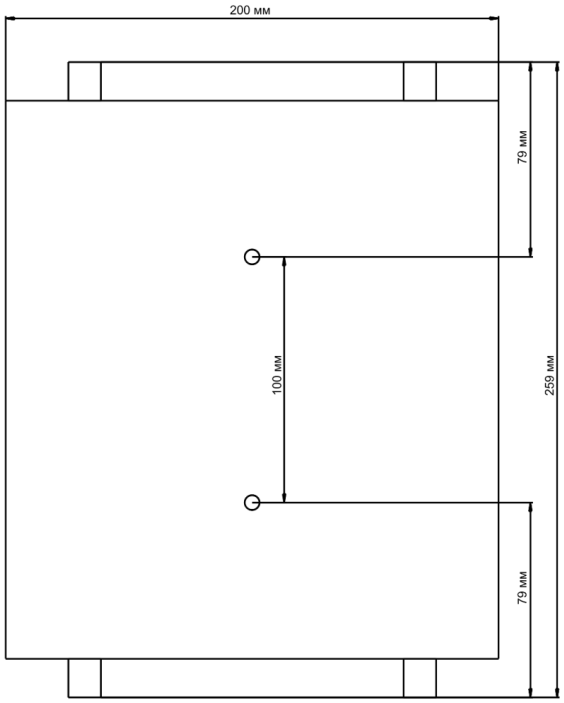


Рисунок Г7 – Габариты устройства относительно крепежных отверстий

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-co.ru
На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ООО «Предприятие «ЭЛТЕКС», обратиться к в базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра на техническом форуме:

http://www.eltex-co.ru/support/downloads/
http://eltex-co.ru/forum/
http://www.eltex-co.ru/support/knowledge/