Комплексные решения для построения сетей

WB-2

Руководство по эксплуатации, версия 1.1 (09.2015)

Точка доступа с интегрированным маршрутизатором

IP-адрес: http://192.168.1.1

имя пользователя: admin

пароль: password

Версия документа	Дата выпуска	Содержание изменений
Версия 1.1	09.09.2015	Синхронизация с версией ПО 1.12.0 Изменения: - 4.5 Меню быстрого конфигурирования - 4.6.2.2 Подменю «Настройка MAC-адресов» - 4.6.5.2 Подменю «Доступ» - 4.6.5.3 Подменю «Журнал» - 4.6.5.9 Подменю «Дополнительные настройки» - 4.7.1 Подменю «Интернет» - 5 Алгоритм работы автоматического обновления устройства на основе протокола DHCP
Версия 1.0	14.10.2014	Первая публикация
Версия программного обеспечения	Версия ПО: 1.12.0 Версия веб-интерфейса: 1.13.39	

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Аннотация

Современные тенденции развития связи диктуют операторам необходимость поиска наиболее 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 все больше набирают обороты и к данному моменту в короткое время прошли огромный путь от нестабильных низкоскоростных сетей связи малого радиуса до сетей ШПД, сопоставимых по скорости с проводными сетями с высокими критериями к качеству предоставления услуг.

Устройство WB-2 является точкой доступа Wi-Fi с интегрированным маршрутизатором. Основное предназначение WB-2: установка внутри зданий в качестве точки доступа к различным ресурсам беспроводной сети.

Устройство ориентировано на домашних пользователей и небольшие офисы.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, конструктивное исполнение, порядок установки, правила конфигурирования, мониторинга и смены программного обеспечения точки доступа WB-2.

1.2 Условные обозначения

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

Примечания и предупреждения

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

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

2 ОПИСАНИЕ ИЗДЕЛИЯ

2.1 Назначение

Для возможности предоставления доступа пользователей к высокоскоростной, безопасной беспроводной сети разработана беспроводная точка доступа WB-2 (далее «устройство»).

Устройство WB-2 – единая точка доступа к современным интерактивным сервисам: Интернет и Full HD IPTV.

Точка доступа WB-2 предназначена для подключения устройств к проводной и беспроводной сети стандартов 802.11 a/b/g/n/ac. WB-2 подключается к проводной сети с помощью 10/100/1000M Ethernet-интерфейса, и с помощью радиоинтерфейса создает беспроводной высокоскоростной доступ для устройств, поддерживающих технологию Wi-Fi в диапазоне 2,4 и 5ГГц. К устройству можно подключить до двух устройств проводной сети. USB-разъем используется для подключения внешних накопителей или 3G/4G USB-модема.

WB-2 поддерживает современные требования к качеству сервисов и позволяет передавать наиболее важный трафик в более приоритетных очередях по сравнению с обычным. Обеспечение приоритезации происходит на основе основных технологий QoS: CoS (Специальные метки в поле VLAN пакета) и ToS (метки в поле IP пакета).

2.2 Характеристика устройства

Интерфейсы:

- LAN: 2 порта Ethernet RJ-45 10/100BASE-T;
- WAN: 1 порт Ethernet RJ-45 10/100/1000BASE-T;
- WLAN: IEEE 802.11 a/b/g/n/ac;
- USB: 1 порт USB2.0.

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

Функции:

- *сетевые функции:*
  - работа в режиме «моста» или «маршрутизатора»;
  - поддержка PPPoE (PAP, SPAP и CHAP авторизация, PPPoE компрессия);
  - поддержка PPTP;
  - поддержка L2TP;
  - поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
  - поддержка DNS;
  - D-DNS;
  - поддержка NAT;
  - UPnP;
  - сетевой экран;
  - клонирование MAC-адреса на WAN-интерфейсе;
  - поддержка NTP;

- поддержка механизмов качества обслуживания QoS (QoS по DSCP и 802.1P);

- поддержка функций IPTV (IGMP-proxy, UDP-to-HTTP proxy);
- обновление ПО через web-интерфейс;
- поддержка DHCP-based autoprovisioning;
- TR-069;
- удаленный мониторинг, конфигурирование и настройка: Web-интерфейс, Telnet, SSH.

На рисунке 1 приведена схема применения оборудования WB-2.

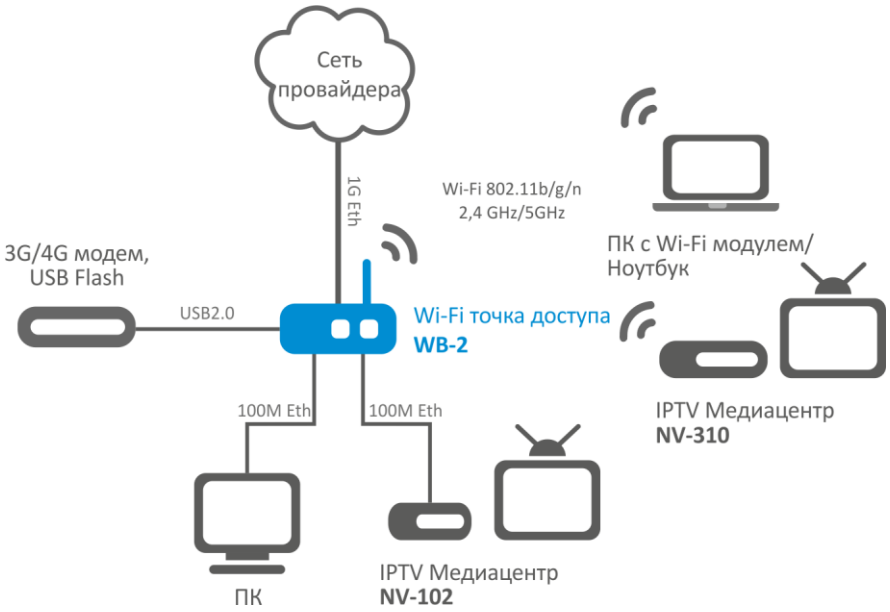


Рисунок 1 – Функциональная схема использования WB-2

2.3 Основные технические параметры

Основные технические параметры устройства приведены в таблице 2.

Таблица 1 – Основные технические параметры

Параметры WAN-интерфейса Ethernet

Количество портов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100/1000, автоопределение
Поддержка стандартов	BASE-T

Параметры LAN-интерфейса Ethernet

Количество интерфейсов	2
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100, автоопределение
Поддержка стандартов	BASE-T

Параметры беспроводного интерфейса

Стандарты	802.11 a/b/g/n/ac
Частотный диапазон, МГц	2.4 ~ 2.4835 ГГц, 5.15 ~ 5.35 ГГц, 5.65 ~ 5.73ГГц, 5.735 ~ 5.835 ГГц
Модуляция	BPSK, QPSK, 16 QAM, 64 QAM, DBPSK, DQPSK, CCK
Скорость передачи данных, Мбит/с	**802.11b(CCK):** 1, 2, 5.5 ,11 **802.11g(OFDM):** 6, 9, 12 , 18, 24, 36, 48, 54 **811n (HT20, 800ns GI):** 13, 26, 39, 78, 104, 117, 130 **802.11n (HT40, 400ns GI):** 30, 60, 90, 120, 180, 240, 270, 300 **802.11n (HT40, 800ns GI):** 27, 54, 81, 108, 162, 216, 243, 270
Максимальная выходная мощность передатчика	**2,4 ГГц (802.11 b/g/n): до 15 dBm** **5 ГГц (802.11 a/n/ac): до 17 dBm**
Чувствительность приемника	2,4 ГГц: **802.11n(MCS0):** -90 dBm **802.11n(MCS4):** -79 dBm **802.11n(MCS7):** -72 dBm 5 ГГц: **802.11ac (MCS0):** -92 dBm **802.11ac (MCS4):** -82 dBm **802.11ac (MCS7):** -76 dBm
Безопасность	64/128/152-битное WEP-шифрование данных; WEP, TKIP и AES

Управление

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

Общие параметры

Питание	адаптер питания 12V DC, 1,5 А.
Потребляемая мощность	Не более 5 Вт
Рабочий диапазон температур	от +5 до +40°С
Относительная влажность при температуре 25°С	до 80%
Габариты	122x96x33 мм
Масса	не более 0,15 кг.

2.4 Конструктивное исполнение

Точка доступа WB-2 выполнена в пластиковом корпусе размерами 122x96x33 мм.

2.4.1 Передняя панель устройства

Внешний вид верхней панели устройства WB-2 приведен на рисунке 2.

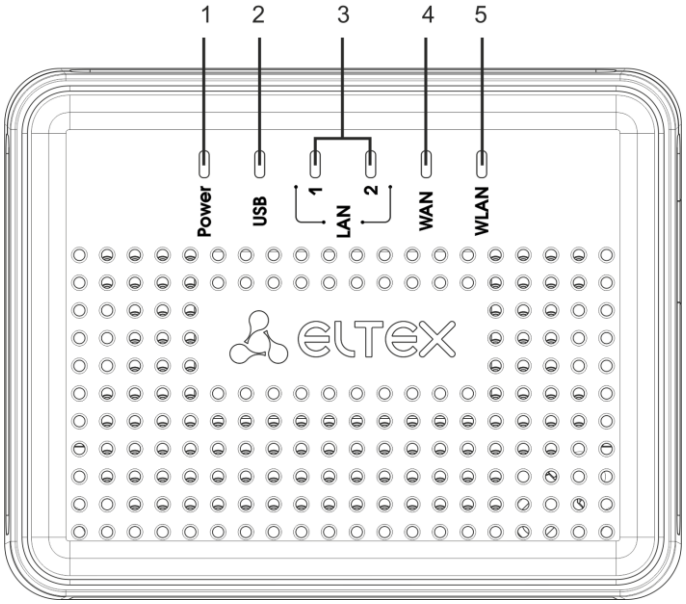


Рисунок 2 – Внешний вид передней панели WB-2

На верхней панели устройства *WB-2* расположены следующие световые индикаторы, таблица 2.

Таблица 2 – Описание индикаторов верхней панели

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

2.4.2 Задняя панель устройства

Внешний вид задней панели устройства WB-2 приведен на рисунке 3.

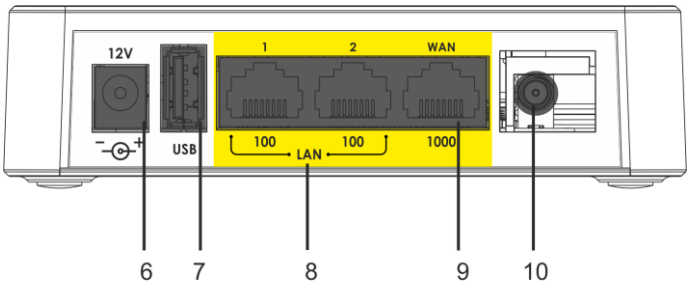


Рисунок 3 – Внешний вид задней панели WB-2

На задней панели устройства WB-2 расположены следующие разъемы и органы управления, таблица 3.

Таблица 3 – Описание индикаторов и органов управления задней панели *RG2400*

Элемент задней панели		**Описание**
6	12V	разъем для подключения адаптера питания
7	USB	разъем USB для подключения внешнего USB-устройства (USB flash, жесткий диск, 3G/4G USB-модем)
8	LAN	2 порта 10/100BASE-T Ethernet (разъем RJ-45) для подключения сетевых устройств
9	WAN	порт 10/100/1000BASE-T (разъем RJ-45) для подключения к внешней сети
10		разъем для подключения WiFi-антенны

2.5 Световая индикация

Текущее состояние устройства отображается при помощи индикаторов **WLAN, WAN, LAN, USB, Power** – расположенных на верхней панели. Перечень состояний индикаторов приведен в таблице 5.

Таблица 4 – Световая индикация состояния устройства WB-2

Индикатор	**Состояние индикатора**	**Состояние устройства**
WLAN	зеленый, горит постоянно	сеть Wi-Fi-активна
	зеленый, мигает	процесс передачи данных по беспроводной сети
WAN	горит зеленым (10, 100Mbps)/ оранжевым (1000 Mbps)	установлено соединение между станционным терминалом и абонентским устройством
	мигает	процесс пакетной передачи данных по WAN-интерфейсу
LAN	горит зеленым (10, 100 Mbps)/ оранжевым (1000 Mbps)	установлено соединение с подключенным сетевым устройством
	мигает	процесс пакетной передачи данных по LAN-интерфейсу
USB	зеленый, горит	USB-устройство подключено
	не горит	USB-устройство отключено
Power	зеленый, горит постоянно	включено питание устройства, нормальная работа
	оранжевый, горит постоянно	отсутствует выход в Интернет
	красный, горит постоянно	загрузка устройства, сброс устройства к заводским настройкам

2.6 Сброс к заводским настройкам

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

2.7 Комплект поставки

В базовый комплект поставки устройства WB-2 входят:

- точка доступа;
- адаптер питания 220/12В 1,5 А;
- 1 съемная антенна;
- руководство по установке и настройке.

3 ПОРЯДОК УСТАНОВКИ

3.1 Инструкции по технике безопасности

1. Не устанавливайте устройство рядом с источниками тепла и в помещениях с температурой ниже 5°С или выше 40°С.
2. Не используйте устройство в помещениях с высокой влажностью. Не подвергайте устройство воздействию дыма, пыли, воды, механических колебаний или ударов.
3. Не вскрывайте корпус устройства. Внутри устройства нет элементов, предназначенных для обслуживания пользователем.

Во избежание перегрева компонентов устройства и нарушения его работы запрещается закрывать вентиляционные отверстия посторонними предметами и размещать предметы на поверхности оборудования.

3.2 Рекомендации по установке

1. 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.
2. Если устройство находилось длительное время при низкой температуре, перед началом работы следует выдержать его в течение двух часов при комнатной температуре. После длительного пребывания устройства в условиях повышенной влажности перед включением выдержать в нормальных условиях не менее 12 часов.
3. Устройство устанавливается в горизонтальном положении, соблюдая инструкции по технике безопасности.
4. При размещении устройства для обеспечения зоны покрытия сети Wi-Fi с наилучшими характеристиками учитывайте следующие правила:
    a. Устанавливайте устройство в центре беспроводной сети;
    b. Минимизируйте число преград (стены, потолки, мебель и другое) между WB-2 и другими беспроводными сетевыми устройствами;
    c. Не устанавливайте устройство вблизи (порядка 2 м.) электрических, радио устройств;
    d. Не рекомендуется использовать радиотелефоны и другое оборудование, работающее на частоте 2,4 ГГц, 5ГГц, в радиусе действия беспроводной сети Wi-Fi;
    e. Препятствия в виде стеклянных/металлических конструкций, кирпичных/бетонных стен, а также емкости с водой и зеркала могут значительно уменьшить радиус действия Wi-Fi сети.

3.3 Порядок включения

1. Установите антенну (поставляется вместе с устройством) в SMA-разъем, рисунок 3.
2. Подключите сетевой Ethernet-кабель, проведённый вашим интернет-провайдером, к разъему **WAN** точки доступа WB-2, рисунок 3.
3. Если точка доступа будет использоваться в качестве домашнего проводного маршрутизатора, то подключите сетевой Ethernet-кабель к разъемам **LAN** точки доступа WB-2 и вашего сетевого устройства (компьютер, принтер, телевизионная приставка и другое).
4. Подключите шнур адаптера питания к разъему питания устройства **12V**. Далее подключите адаптер к источнику питания, рисунок 3.
5. После подключения точки доступа к сети питания дождитесь полной загрузки устройства (это может занять около минуты).

4 УПРАВЛЕНИЕ УСТРОЙСТВОМ ЧЕРЕЗ WEB-КОНФИГУРАТОР

4.1 Начало работы

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

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

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

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

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

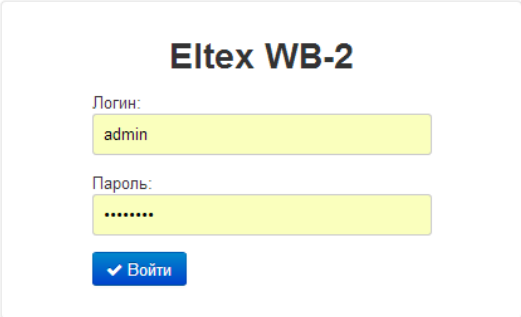
Заводские установки: логин: *admin*, пароль: *password*.

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

4.2 Смена пользователей

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

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



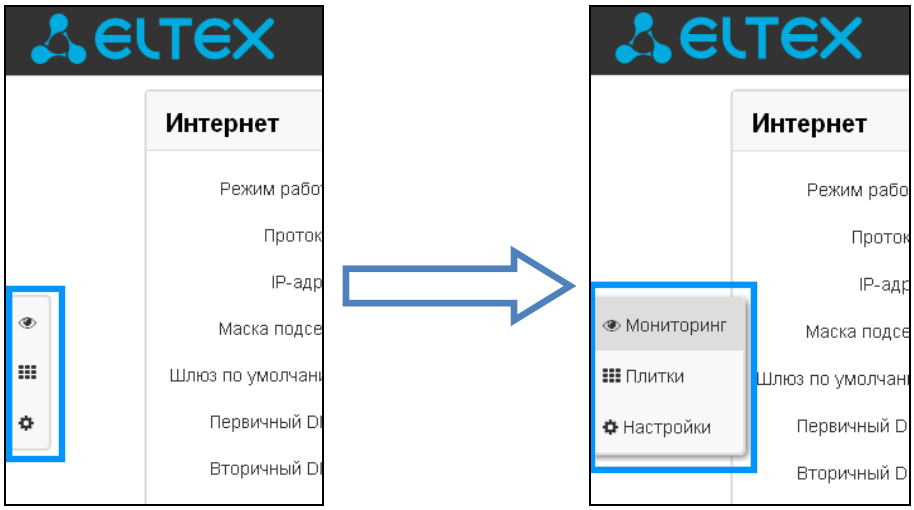
Для смены доступа необходимо указать соответствующие имя пользователя и пароль, нажать кнопку *«Войти».*

4.3 Режимы работы WEB-интерфейса

WEB-интерфейс устройства WB-2 может работать в трех режимах:

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

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

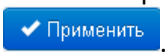


Из режима «Плитки» в режим «Настройки» переход возможен также через ссылку «подробнее» в названии плитки.

4.4 Применение конфигурации и отмена изменений

1. Применение конфигурации

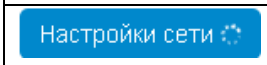
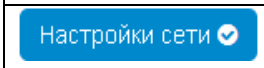
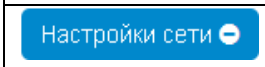
По нажатию на кнопку «Применить» происходит сохранение конфигурации во flash-память устройства и применение новых настроек. Все настройки вступают в силу без перезагрузки устройства.

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

.

В WEB-интерфейсе реализована визуальная индикация текущего состояния процесса применения настроек, таблица 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».
	Об успешном сохранении и применении настроек информирует значок в названии вкладки.
	Если значение параметра было указано с ошибкой – после нажатия на кнопку «Применить» появится соответствующее сообщение об ошибке с указанием причины, а в названии вкладки отобразится значок .

2. Отмена изменений

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

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

.

4.5 Меню быстрого конфигурирования

В меню быстрого конфигурирования отображаются основные настройки устройства, рисунок 4.

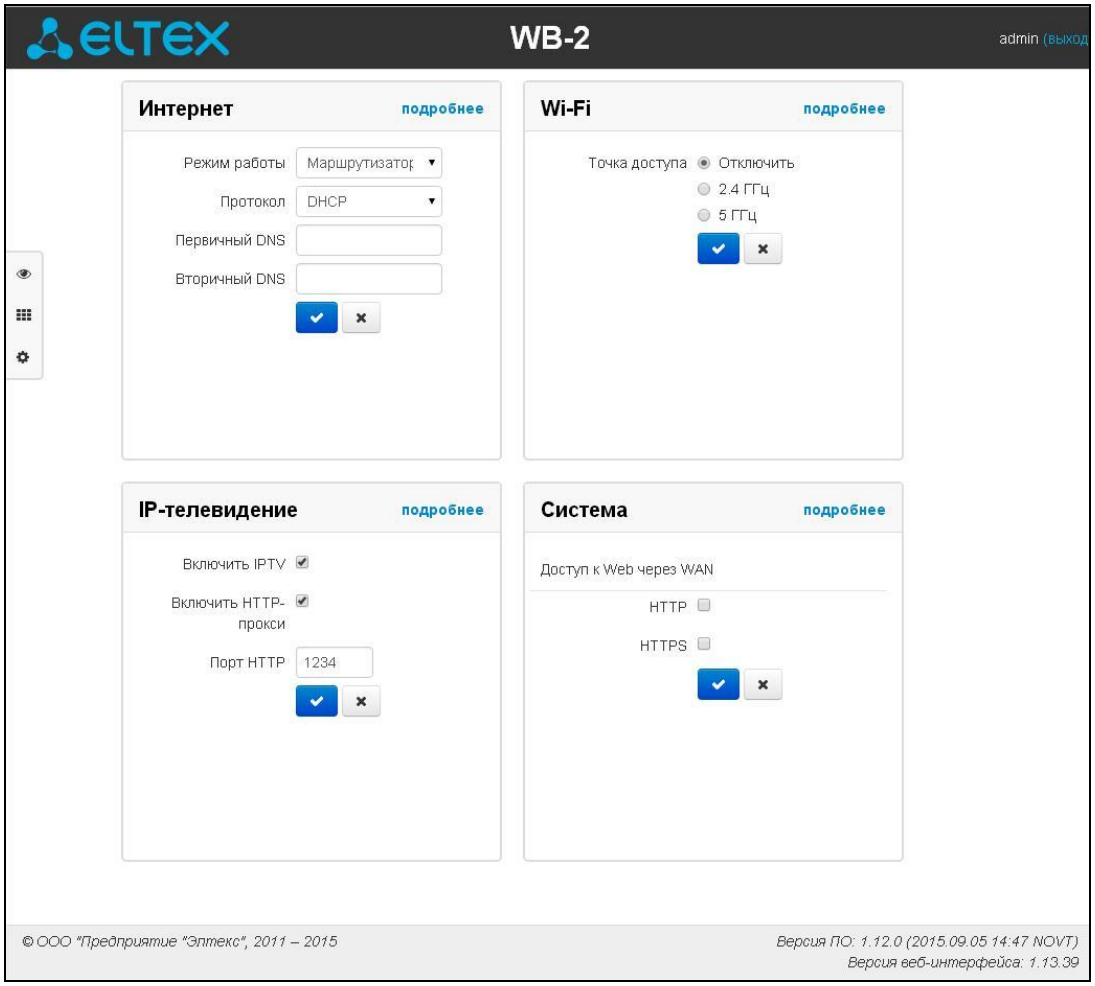


Рисунок 4 – Меню быстрого конфигурирования

Настройки разделены по следующим категориям:

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

4.5.1 Интернет

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

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

    Поддерживаемые опции:
    - 1 – маска сети;
    - 3 – адрес сетевого шлюза по умолчанию;
    - 6 – адрес DNS-сервера;
    - 12 – сетевое имя устройства;
    - 28 – широковещательный адрес сети;
    - 33 - статические маршруты;
    - 42 – адрес NTP-сервера;
    - 43 – специфичная информация производителя;
    - 66 – адрес TFTP сервера;
    - 121 – бесклассовые статические маршруты.

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

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

    Пример:
    [VENDOR:Eltex][DEVICE:WB-2][HW:2.0][SN:VI23000118][WAN:A8:F9:4B:03:2A:D0]
    [LAN:02:20:80:a8:f9:4b][VERSION:#1.5.0]
  - *PPPoE* – режим работы, при котором на WAN-интерфейсе поднимается PPP-сессия. При выборе «PPPoE» для редактирования станут доступны следующие параметры:
    - *Имя пользователя* – имя пользователя для авторизации на PPP-сервере;

- *Пароль* – пароль для авторизации на PPP-сервере;
- *Service-Name* – имя услуги – значение тега Service-Name в сообщении PADI для инициализации PPPoE-соединения (использование данной опции не является обязательным, этот параметр настраивается только по требованию провайдера);
- *Второй доступ* – тип доступа к локальным сетевым ресурсам.
  Можно выбрать 2 варианта:
  DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
  Static – статический – в этом случае необходимые для доступа параметры нужно указать вручную: *IP-адрес*, *Маска подсети, DNS-сервер.*

- *PPTP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол PPTP. При выборе «*PPTP*» для редактирования станут доступны следующие параметры:
  - *PPTP-Сервер* – адрес сервера PPTP (доменное имя или IP-адрес в формате IPv4);
  - *Имя пользователя* – имя пользователя для авторизации на PPTP-сервере;
  - *Пароль* – пароль для авторизации на PPTP-сервере;
  - *Второй доступ* – тип доступа к локальный сетевым ресурсам и PPTP-серверу.
    Можно выбрать 2 варианта:
    DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
    Static – статический, в этом случае необходимые для доступа к PPTP-серверу параметры задаются вручную:
    - *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
    - *Маска подсети* – при статическом доступе маска подсети;
    - *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
    - *Шлюз* – при статическом доступе шлюз для доступа к PPTP-серверу (если необходим).

- *L2TP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол L2TP. При выборе «*L2TP*» для редактирования станут доступны следующие параметры:
  - *L2TP-Сервер* – адрес сервера L2TP (доменное имя или IP-адрес в формате IPv4);
  - *Имя пользователя* – имя пользователя для авторизации на L2TP-сервере;
  - *Пароль* – пароль для авторизации на L2TP-сервере;
  - *Второй доступ* – тип доступа к локальный сетевым ресурсам и L2TP-серверу.
    Можно выбрать 2 варианта:
    DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
    Static – статический, в этом случае необходимые для доступа к L2TP-серверу параметры задаются вручную:
    - *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
    - *Маска подсети* – при статическом доступе маска подсети;
    - *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
    - *Шлюз* – при статическом доступе шлюз для доступа к L2TP-серверу (если необходим).

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

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

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

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

4.5.2 Wi-Fi

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

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

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

4.5.3 IP-телевидение

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

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

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

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

4.5.4 Система

В разделе «Система» выполняются настройки доступа к web-конфигуратору устройства. Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее».

Доступ к Web через WAN:

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

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

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

4.6 Расширенные настройки

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

4.6.1 Основные элементы WEB-интерфейса

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

Рисунок 5 – Элементы навигации Web-конфигуратора

Окно пользовательского интерфейса разделено на семь областей:

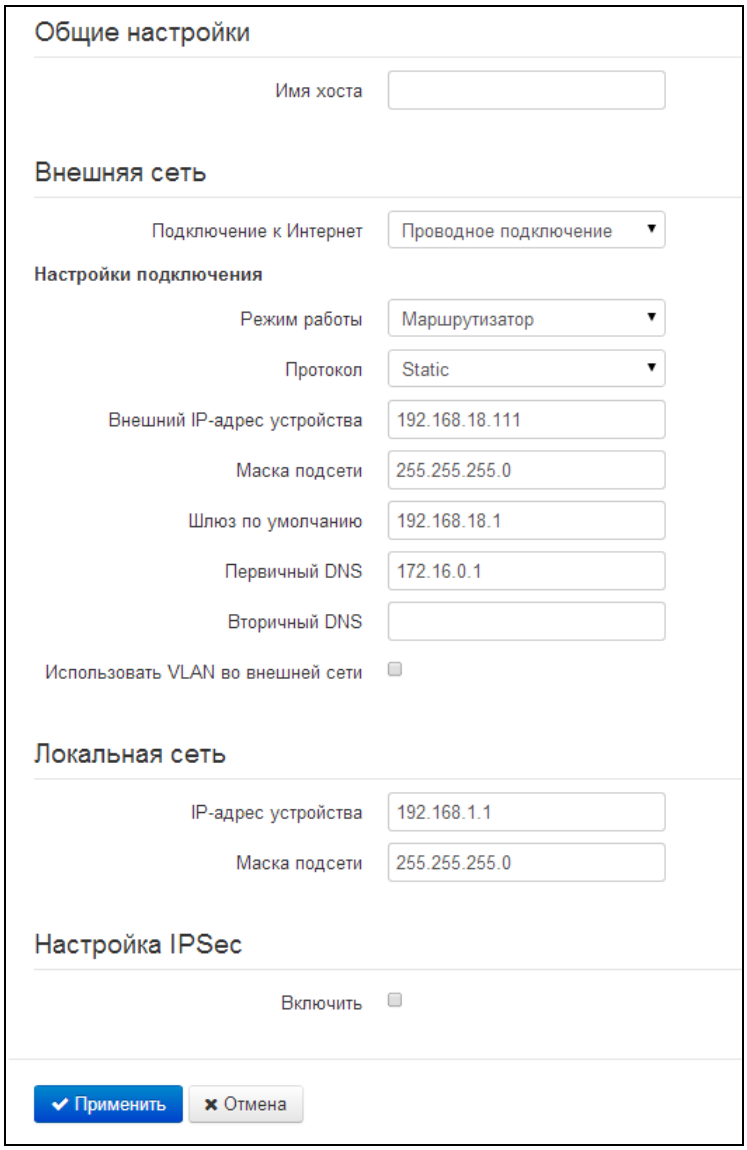
1. Имя пользователя, под которым был осуществлен вход в систему, а также кнопка завершения сеанса работы в WEB-интерфейсе (*выход*) под данным пользователем.
2. Вкладки меню группируют вкладки подменю по категориям: **Сеть**, **IP-телефония**, **IP-телевидение**, **Система**.
3. Вкладки подменю служат для управления полем настроек.
4. Панель смены режима WEB-конфигуратора (описание в разделе 3.3)
5. Поле настроек устройства, которое базируется на выборе пользователя, предназначено для просмотра настроек устройства и ввода конфигурационных данных.
6. Кнопки управления конфигурацией, подробная информация приведена в разделе 3.4:
7. Информационное поле, в котором отображается версия ПО, версия WEB-интерфейса.

4.6.2 Меню «Сеть»

В меню «Сеть» выполняются основные сетевые настройки устройства.

4.6.2.1 Подменю «Интернет»

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



Общие настройки

- *Имя хоста – сетевое имя устройства.*

Внешняя сеть

- *Подключение к Интернет* – способ подключения устройства к внешней сети:
  - *Проводное подключение* – подключение к сети Интернет осуществляется только по Ethernet-кабелю через порт WAN;

- *3G/4G USB-модем* – подключение к сети Интернет осуществляется через беспроводной USB-модем 3G/4G (через сеть мобильной связи), подключенный к USB-порту устройства;
- *Wi-Fi подключение* – подключение к сети Интернет осуществляется через беспроводную сеть Wi-Fi.

Настройки подключения

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

– *Режим работы* – режим работы устройства:

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

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

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

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

- *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от DHCP-сервера автоматически.
  Поддерживаемые опции:
  - 1 – маска сети;
  - 3 – адрес сетевого шлюза по умолчанию;
  - 6 – адрес DNS-сервера;
  - 12 – сетевое имя устройства;
  - 28 – широковещательный адрес сети;
  - 33 - статические маршруты;
  - 42 – адрес NTP-сервера;
  - 43 – специфичная информация производителя;
  - 66 – адрес TFTP-сервера;
  - 121 – бесклассовые статические маршруты.

Для протокола DHCP имеется возможность задать необходимое значение опции 60.

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

  Пример:
  [VENDOR:Eltex][DEVICE:WB-2][HW:2.0][SN:VI23000118]
  [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.9.3]
- *Первичный DNS, Вторичный DNS* – IP-адреса DNS-серверов – если адреса DNS-серверов не назначаются автоматически по протоколу DHCP, при необходимости задайте их вручную.

- *PPPoE* – режим работы, при котором на WAN-интерфейсе поднимается PPP-сессия. При выборе «PPPoE» для редактирования станут доступны следующие параметры:
  - *Имя пользователя* – имя пользователя для авторизации на PPP-сервере;
  - *Пароль* – пароль для авторизации;
  - *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1492);
  - *Service-Name* – имя услуги – значение тэга Service-Name в сообщении PADI (поле не обязательно для заполнения);
  - *Второй доступ* – тип доступа к локальным сетевым ресурсам.
    Можно выбрать 2 варианта:
    DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
    Static – статический – в этом случае необходимые для доступа параметры задаются вручную:
    IP-адрес, Маска подсети, DNS-сервер;
  - *Аппаратное ускорение трафика* – в зависимости от выбранного значения достигается увеличение пропускной способности устройства при передаче трафика PPP (при выборе *PPP*) или IPoE (при выборе *Ethernet*).
- *PPTP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол PPTP. При выборе «*PPTP*» для редактирования станут доступны следующие параметры:
  - *PPTP-Сервер* – IP-адрес сервера PPTP;
  - *Имя пользователя* – имя пользователя для авторизации на PPTP-сервере;
  - *Пароль* – пароль для авторизации на PPTP-сервере;
  - *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1462);
  - *Второй доступ* – тип доступа к локальный сетевым ресурсам и PPTP-серверу.
    Можно выбрать 2 варианта:
    DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
    Static – статический, в этом случае необходимые для доступа к PPTP-серверу параметры задаются вручную:
  - *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
  - *Маска подсети* – при статическом доступе маска подсети;

- *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
- *Шлюз* – при статическом доступе шлюз для доступа к PPTP-серверу (если необходим).

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

- *L2TP* – режим, при котором выход в Интернет осуществляется через специальный канал, туннель, используя протокол L2TP. При выборе «*L2TP*» для редактирования станут доступны следующие параметры:
  - *L2TP-Сервер* – IP-адрес сервера L2TP;
  - *Имя пользователя* – имя пользователя для авторизации на L2TP-сервере;
  - *Пароль* – пароль для авторизации на L2TP-сервере;
  - *MTU* – максимальный размер блока данных, передаваемых по сети (рекомендуемое значение – 1462);
  - *Второй доступ* – тип доступа к локальный сетевым ресурсам и L2TP-серверу.
    Можно выбрать 2 варианта:
    DHCP – динамический доступ, когда IP-адрес и все необходимые параметры получаются по протоколу DHCP;
    Static – статический, в этом случае необходимые для доступа к L2TP-серверу параметры задаются вручную:
  - *IP-адрес* – при статическом доступе с этого адреса осуществляется доступ до PPTP-сервера;
  - *Маска подсети* – при статическом доступе маска подсети;
  - *DNS-сервер* – при статическом доступе сервер DNS, используемый в локальной сети;
  - *Шлюз* – при статическом доступе шлюз для доступа к L2TP-серверу (если необходим).

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

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

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

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

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

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

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

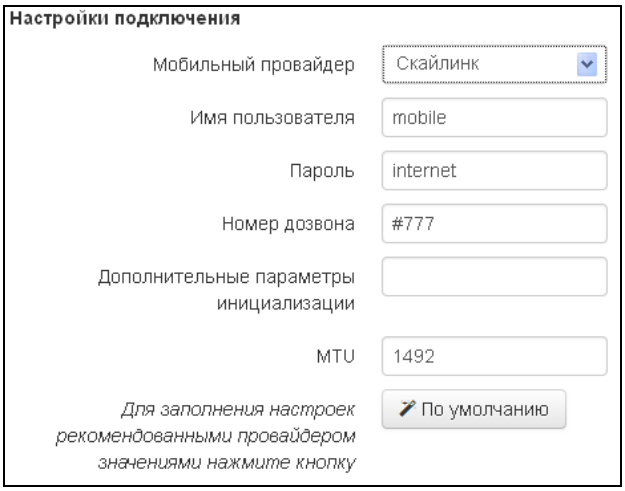
  - *Static* – режим работы, при котором IP-адрес и все необходимые параметры на WAN-интерфейс назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:

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

  - *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от
    - *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля *Vendor ID (опция 60).* При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.
      Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат:
      [VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**] [SN:**серийный номер**][WAN:**MAC-адрес интерфейса WAN**][LAN:**MAC-адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

      Пример:
      [VENDOR:Eltex][DEVICE:WB-2][HW:2.0][SN:VI23000118]
      [WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.9.3]
    - *Первичный DNS, Вторичный DNS* – IP-адреса DNS-серверов – если адреса DNS-серверов не назначаются автоматически по протоколу DHCP, при необходимости задайте их вручную.

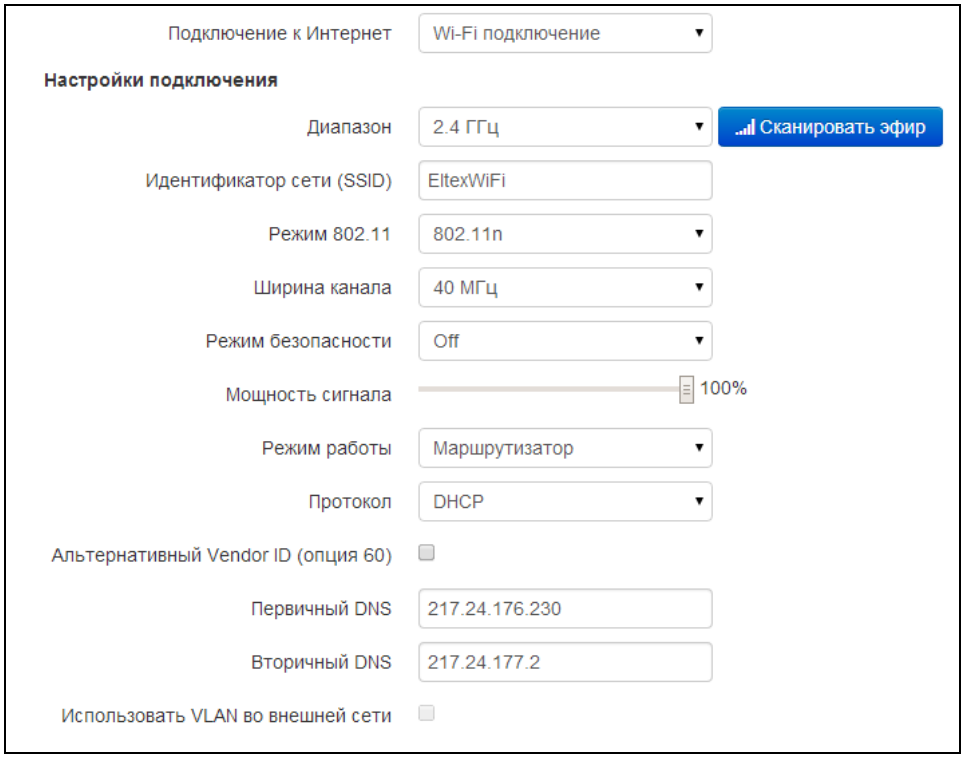
2. При выборе способа подключения **«3G/4G USB-модем»** для настройки будут доступны следующие поля:



- *Мобильный провайдер* – имя провайдера, предоставляющего доступ к сети 3G/4G. Из списка Вы можете выбрать одного из шести мобильных операторов (настройки каждого из них хранятся в памяти устройства), присутствующих на территории Российской Федерации: Мегафон, Билайн, МТС, Скайлинк, Теле2, Yota. Нажав на кнопку «По умолчанию» произойдёт заполнение настроек подключения параметрами выбранного провайдера. Если настройки провайдера в Вашем регионе отличаются от предложенных, отредактируйте их в соответствии с необходимыми значениями.
  Если Вашего провайдера нет в списке – выберите значение «Другой» и заполните все поля в соответствии с настройками Вашего провайдера;
- *Протокол* – поле доступно только при выборе значения «Другой» из списка мобильных провайдеров. В большинстве случаев мобильные операторы используют протокол PPPoE для доступа к своей сети, однако для работы с модемами некоторых провайдеров может потребоваться выбор протокола DHCP;
- *Имя пользователя* – имя пользователя для идентификации при подключении к беспроводной сети;
- *Пароль* – пароль для идентификации при подключении к беспроводной сети;
- Номер дозвона – номер дозвона для подключения к беспроводной сети (пример: *99***1#);
- *Дополнительные параметры* – параметры для подключения к сети мобильной связи (пример: AT+CGDCONT=1,IP,internet – для Мегафон); в данной строке нельзя использовать кавычки;
- *MTU* – максимальный размер блока данных, передаваемых по сети, рекомендуемое значение – 1492.

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

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



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

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

– *Идентификатор сети (SSID)* – имя беспроводной сети, используется для подключения к устройству. Максимальная длина имени – 32 символа, ввод с учетом регистра клавиатуры. Данный параметр может состоять из цифр, латинских букв, а также символов "-", "_", ".", "!", ";", "#" и пробела, при этом символы "!", ";", "#" и пробел не могут стоять первыми;
– *Режим 802.11* – выбор режима работы беспроводного интерфейса.
Для 2.4 ГГц:
  - *802.11b* – если все беспроводные клиенты поддерживают стандарт 802.11b, по данному стандарту максимальная скорость составляет 11 Мбит/с;
  - *802.11bg* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b и 802.11g, по стандарту 802.11g максимальная скорость составляет 54 Мбит/с;
  - *802.11bgn* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b, 802.11g и 802.11n;
  - *802.11n* – данный стандарт предусматривает максимальную скорость до 150 Мбит/с.

Для 5 ГГц:
  - *802.11a* – максимальная скорость составляет 54 Мбит/с;
  - *802.11n* – данный стандарт предусматривает максимальную скорость до 150 Мбит/с.
  - *802*.11ac - данный стандарт предусматривает максимальную скорость до 433 Мбит/с.

- *Ширина канала* – ширина полосы частот канала, на котором работает Wi-Fi клиент, принимает значения 20, 40 и 80 МГц. Ширина канала в 80 МГц по факту будет работать только на стандарте 802.11ac.
- *Режим безопасности* – выбор режима безопасности беспроводной сети:

  - *Off* – отключено шифрование беспроводной сети, низкий уровень безопасности;
  - *WEP* – шифрование WEP. WEP-ключ должен состоять из шестнадцатеричных цифр и иметь длину 10 или 26 символов, либо должен быть строкой (символы a-z, A-Z, 0-9, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов.
  - *WPA, WPA2* – шифрование WPA и WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:\\|/?.,<>"`' или пробел. Рекомендуется использовать режимы шифрования WPA и WPA2 как наиболее безопасные на данный момент;
  - *WPA-Enterprise, WPA2-Enterprise* – шифрование WPA и WPA2 с аутентификацией клиента по 802.1x. В качестве авторизационных данных необходимо ввести имя пользователя и пароль.

- *Мощность сигнала* – регулировка мощности сигнала приемо-передатчика Wi-Fi в процентах от максимального уровня.
- *Режим работы* – режим работы устройства:

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

- *Протокол* – выбор протокола, по которому будет осуществляться подключение по Wi-Fi интерфейсу устройства к сети предоставления услуг провайдера:

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

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

  - *DHCP* – режим работы, при котором IP-адрес, маска подсети, адрес DNS-сервера, шлюз по умолчанию и другие параметры, необходимые для работы в сети, будут получены от
    - *Альтернативный Vendor ID (опция 60)* – при установленном флаге устройство передаёт в DHCP-сообщениях в опции 60 (Vendor class ID) значение из поля *Vendor ID (опция 60).* При пустом поле опция 60 в сообщениях протокола DHCP не передаётся.
      Если флаг *Альтернативный Vendor ID (опция 60)* не установлен – в опции 60 передается значение по умолчанию, которое имеет следующий формат:
      [VENDOR:производитель**][DEVICE:**тип устройства**][HW:**аппаратная версия**] [SN:**серийный номер**][WAN:**MAC-адрес интерфейса WAN**][LAN:**MAC-адрес интерфейса LAN**][VERSION:**версия программного обеспечения**]**

      Пример:

[VENDOR:Eltex][DEVICE:WB-2][HW:2.0][SN:VI23000118]
[WAN:A8:F9:4B:03:2A:D0][LAN:02:20:80:a8:f9:4b][VERSION:#1.9.3]

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

Локальная сеть:

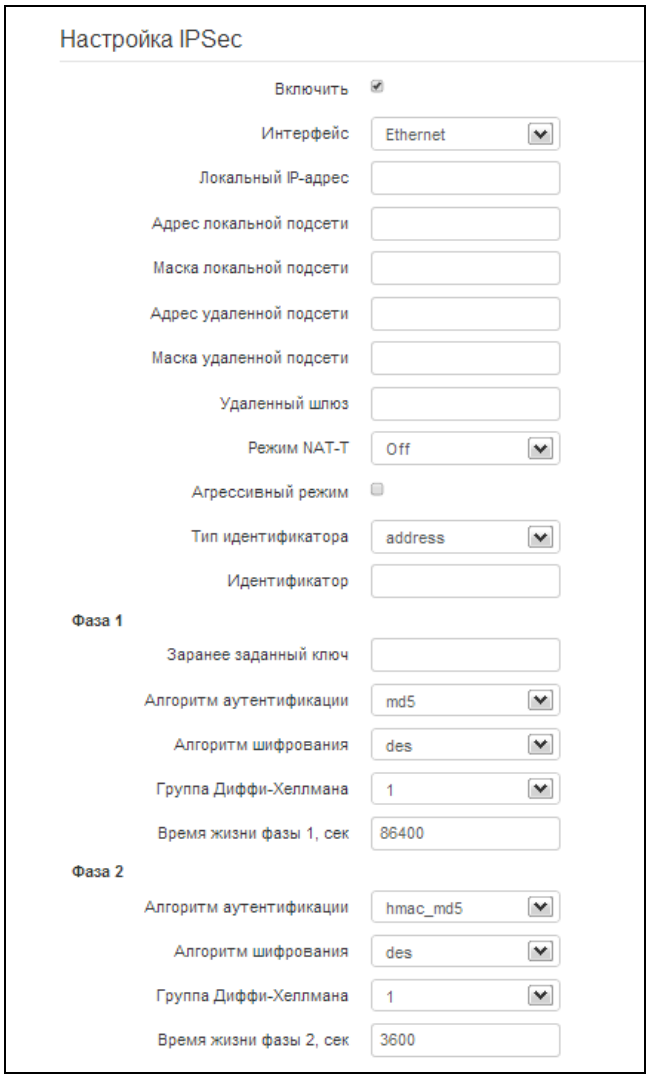
- *IP-адрес устройства* – IP-адрес устройства в локальной сети;
- *Маска подсети* – маска подсети в локальной сети.

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

Настройка IPSec:

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

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



- *Включить* – разрешить использование протокола IPSec для шифрования данных;
- *Интерфейс* – настройка имеет силу только при выборе для Интернета протоколов PPPoE, PPTP или L2TP и определяет, для доступа по какому интерфейсу использовать IPSec: Ethernet (интерфейс второго доступа) или PPP (интерфейс первого доступа). При выборе протоколов DHCP или Static в услуге активен только один интерфейс (Ethernet), по которому возможен доступ только посредством IPSec.
- *Локальный IP-адрес* – адрес устройства для работы по протоколу IPSec;
- *Адрес локальной подсети* совместно с *Маской локальной подсети* определяют локальную подсеть для создания топологий сеть-сеть или сеть-точка;
- *Адрес удаленной подсети* совместно с *Маской удаленной подсети* определяют адрес удаленной подсети для связи с использованием шифрования по протоколу IPSec. Если маска имеет значение 255.255.255.255 – связь осуществляется с единственным хостом. Маска, отличная от 255.255.255.255, позволяет задать целую подсеть. Таким образом, функциональные возможности устройства позволяют организовать 4 топологии сети с использованием шифрования трафика по протоколу IPSec: точка-точка, сеть-точка, точка-сеть, сеть-сеть;
- *Удаленный шлюз* – шлюз, через который осуществляется доступ к удаленной подсети;
- *Режим NAT-T* – выбор режима NAT-T. NAT-T (NAT Traversal) инкапсулирует трафик IPSec и одновременно создает пакеты UDP, которые устройство NAT корректно пересылает. Для этого NAT-T помещает дополнительный заголовок UDP перед пакетом IPSec, чтобы он во всей сети обрабатывался как обычный пакет UDP, и хост получателя не проводил никаких проверок целостности. После поступления пакета к месту назначения заголовок UDP удаляется, и пакет данных продолжает свой дальнейший путь как инкапсулированный пакет IPSec. С помощью техники NAT-T возможно установление связи между клиентами IPSec в защищённых сетях и общедоступными хостами IPSec через межсетевые экраны. Режимы работы NAT-T:
  - *on* – режим NAT-T активируется только при обнаружении NAT на пути к хосту назначения;
  - *force* – в любом случае использовать NAT-T;
  - *off* – не использовать NAT-T при установлении соединения.

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

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

- *Заранее заданный ключ* – секретный ключ, используемый в алгоритме аутентификации на фазе 1. Представляет собой строку от 8 до 63 символов;
- *Алгоритм аутентификации* – выбор одного из списка алгоритмов аутентификации: MD5, SHA1;

- *Алгоритм шифрования* – выбор одного из списка алгоритмов шифрования: DES, 3DES, Blowfish;
- *Группа Диффи-Хеллмана* – выбор группы Diffie-Hellman;
- *Время жизни фазы 1, сек* – время, по истечении которого узлам необходимо переидентифицировать друг друга и сравнить политику (другое название IKE SA lifetime). По умолчанию 24 часа (86400 секунд).

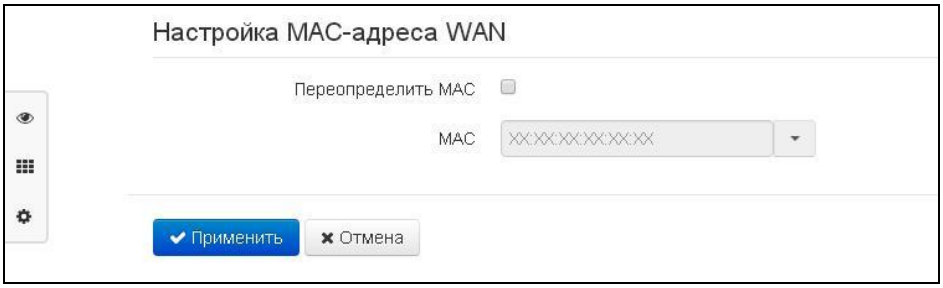
Фаза 2. На втором этапе генерируются данные ключей, узлы «договариваются» об используемой политике. Этот режим, также называемый быстрым режимом (quick mode), отличается от первой фазы тем, что может установиться только после первого этапа, когда все пакеты второй фазы шифруются.

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

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

4.6.2.2 Подменю «Настройка MAC-адресов»

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



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

При нажатии на кнопку выпадающего списка в правом конце поля «*MAC*» появится список MAC-адресов устройств, подключенных к WB-2. Первым из них будет адрес компьютера, с которого Вы подключены к WEB-конфигуратору.

Эта функция будет полезна, если на сети Вашего Интернет-провайдера используется привязка по MAC-адресу. В этом случае если Вам необходимо использовать устройство в качестве маршрутизатора, на WAN-интерфейс устройства необходимо назначить MAC-адрес Вашего компьютера (который ранее был подключен к сети Интернет).

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

4.6.2.3 Подменю «DHCP-сервер»

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

Устройство имеет возможность посредством протокола динамического конфигурирования (DHCP – Dynamic Host Configuration Protocol) автоматически назначать IP-адреса и необходимые для выхода в Интернет параметры компьютерам, подключенным к LAN-интерфейсу и беспроводной Wi-Fi точке доступа. Его использование позволяет избежать ограничений ручной настройки протокола TCP/IP.

Настройки DHCP-сервера

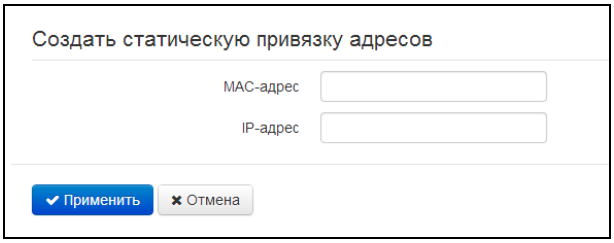
- *Включен* – при установленном флаге включить локальный DHCP-сервер, иначе – не включать;
- *Начальный IP-адрес* – начальный адрес пула IP-адресов;
- *Количество адресов* – количество адресов в пуле;
- *Срок аренды* – установка максимального времени использования подключенным устройством IP-адреса,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

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

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

Статические привязки адресов

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



- *MAC-адрес* – установка статического MAC-адреса. Задается в формате XX:XX:XX:XX:XX:XX;
- *IP-адрес* – установка статического IP-адреса для указанного MAC-адреса.

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

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

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

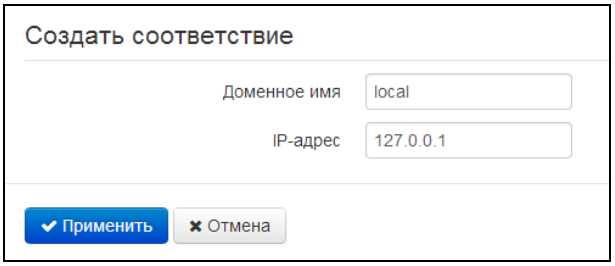
4.6.2.4 Подменю «Локальный DNS»

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

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

Настройка узлов

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



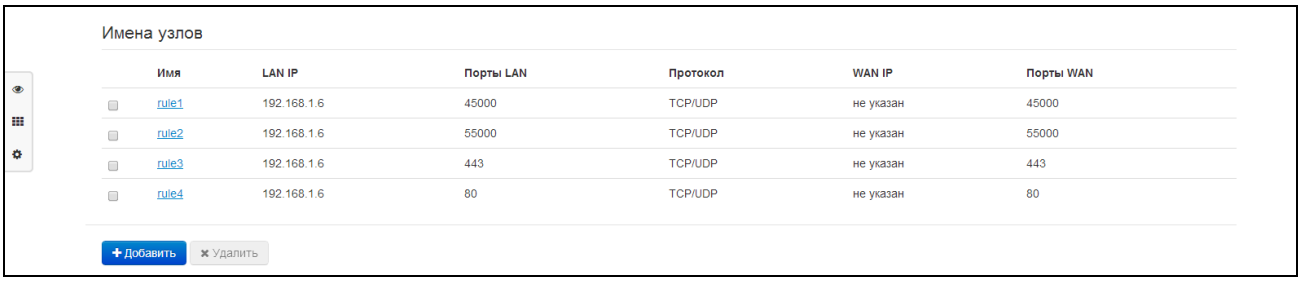
- *Доменное имя* – имя узла;
- *IP-адрес* – IP-адрес узла.

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

4.6.2.5 Подменю «NAT и проброс портов»

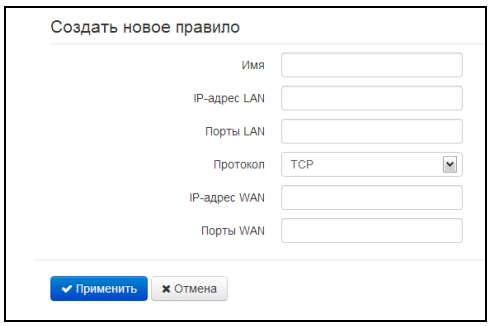
В подменю «NAT и проброс портов» выполняется настройка проброса портов (ports forwarding) из WAN-интерфейса в LAN-интерфейс.

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



Настройка правила NAT

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



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

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

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

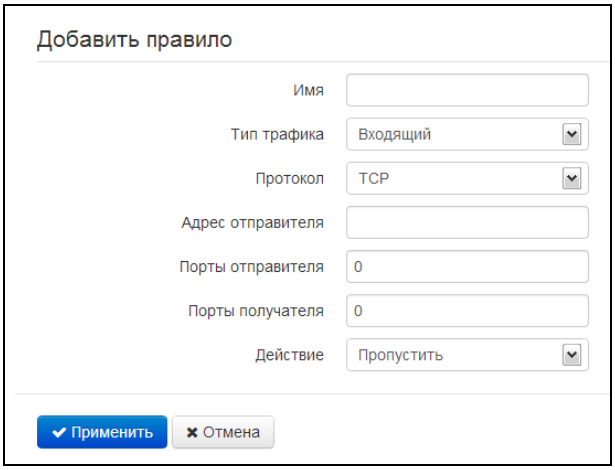
Для удаления правила из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку «Удалить».

4.6.2.6 Подменю «Сетевой экран»

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

Настройка правил сетевого экрана

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



- *Имя* – название правила;
- *Тип трафика* – выбор типа трафика, на который распространяется действие данного правила:

- *Входящий* – входящий на устройство трафик (получателем является непосредственно один из сетевых интерфейсов устройства). При выборе данного типа трафика для редактирования станут доступны следующие поля:

  Адрес отправителя – задает начальный IP-адрес отправителя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.16.0/24 или 192.168.16.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов (запись маски в виде /24 соответствует записи /255.255.255.0);

- *Исходящий* – исходящий с устройства трафик (трафик, генерируемый локально устройством с одного из сетевых интерфейсов). При выборе данного типа трафика для редактирования станут доступны следующие поля:
  - *Адрес получателя* – задает IP-адрес получателя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.18.0/24 или 192.168.18.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;

- *Транзитный* – транзитный трафик (трафик, проходящий между двумя сетевыми интерфейсами, когда отправителем и получателем являются внешние устройства). При выборе данного типа трафика для редактирования станут доступны следующие поля:
  - *Адрес отправителя* – задает IP-адрес отправителя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.16.0/24 или 192.168.16.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;
  - *Адрес получателя* – задает IP-адрес получателя. Через символ "/" можно указать маску подсети в форматах xxx.xxx.xxx.xxx или xx, например, 192.168.18.0/24 или 192.168.18.0/255.255.255.0, чтобы выделить сразу целый диапазон адресов;

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

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

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

При выборе протокола ICMP для редактирования будут доступны настройки:

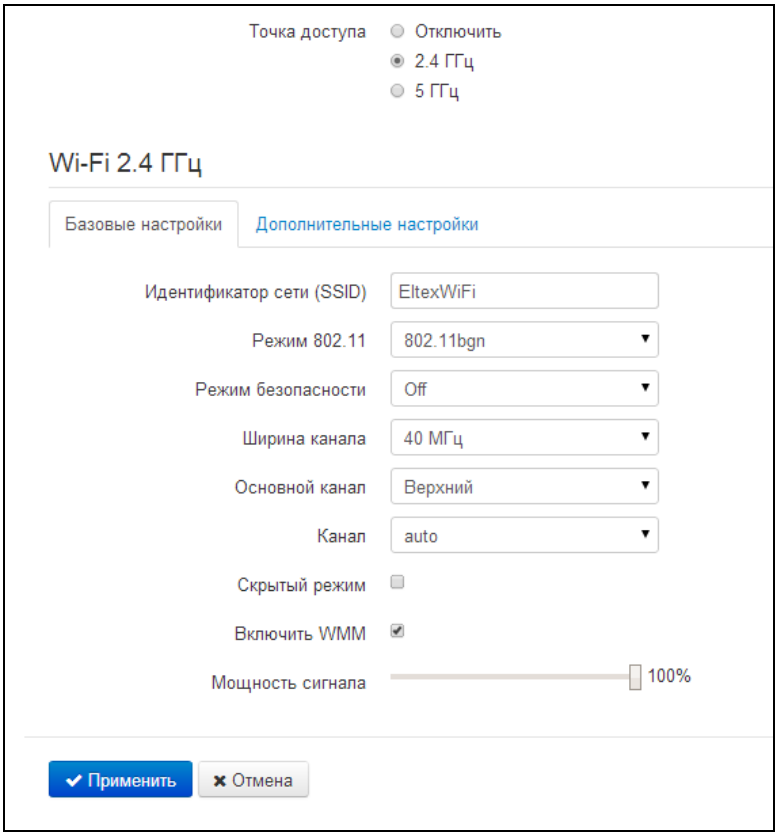
- *Тип сообщения* – можно создать правило только для определенного типа ICMP-сообщения либо для всех.

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

4.6.2.7 Подменю «Wi-Fi»

В подменю «Wi-Fi» выполняются настройки беспроводной Wi-Fi сети. Настройки выполняются для сети Wi-Fi на частоте 2.4 ГГц или 5 ГГц. Устройство не поддерживает работу одновременно в двух диапазонах частот.

Все настройки разделены на базовые и дополнительные.



Базовые настройки

- *Точка доступа* – выбор диапазона работы (2.4 ГГЦ или 5 ГГц) беспроводной точки доступа в соответствующем диапазоне частот, иначе – точка доступа отключена;
- *Идентификатор сети (SSID)* – имя беспроводной сети, используется для подключения к устройству. Максимальная длина имени – 32 символа, ввод с учетом регистра клавиатуры. Данный параметр может состоять из цифр, латинских букв, пробелов, а также символов "-", "_", ".", "!", ";", "#", при этом символы "!", ";" , "#" и пробел не могут стоять первыми;
- *Режим 802.11* – выбор режима работы беспроводного интерфейса.
  Для 2.4 ГГц:
  - *802.11b* – если все беспроводные клиенты поддерживают стандарт 802.11b, по данному стандарту максимальная скорость составляет 11 Мбит/с;
  - *802.11bg* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b и 802.11g, по стандарту 802.11g максимальная скорость составляет 54 Мбит/с;
  - *802.11bgn* – если в сети присутствуют беспроводные клиенты с поддержкой 802.11b, 802.11g и 802.11n;
  - *802.11n* – данный стандарт предусматривает максимальную скорость до 150 Мбит/с.

  Для 5 ГГц:
  - *802.11a* – максимальная скорость составляет 54 Мбит/с;
  - *802.11n* – данный стандарт предусматривает максимальную скорость до 150 Мбит/с.

- *802.11ac* - данный стандарт предусматривает максимальную скорость до 433 Мбит/с. Клиенты, поддерживающие стандарт 802.11n, так-же могут работать с точкой доступа в данном режиме.

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

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

Рекомендуется использовать режимы безопасности WPA и WPA2 как наиболее безопасные.

– *Использовать авторизацию через RADIUS* – при установленном флаге точка доступа будет авторизовывать клиентов по 802.1x (WPA/WPA2-Enterprise) с использованием RADIUS-сервера. Опция доступна при использовании режимов безопасности WPA или WPA2;
– *IP-адрес RADIUS сервера* – адрес RADIUS-сервера;
– *Порт RADIUS сервера* – номер UDP-порта для обмена данными между устройством и RADIUS-сервером (по умолчанию 1812);
– *Пароль RADIUS сервера* – пароль доступа к RADIUS-серверу;
– *Использовать аккаунтинг через RADIUS* – при установленном флаге точка доступа будет использовать аккаунтинг сервер RADIUS для учета авторизованных пользователей на RADIUS;
– *IP-адрес RADIUS сервера для аккаунтинга* – адрес RADIUS аккаунтинга сервера (обычно совпадает с адресом RADIUS-сервера);
– *Порт RADIUS сервера для аккаунтинга* – номер UDP-порта для обмена данными между устройством и RADIUS аккаунтинг сервером (по умолчанию 1813);
– *Пароль RADIUS сервера для аккаунтинга* – пароль доступа к RADIUS аккаунтинг серверу;
– *Ширина канала* – ширина полосы частот канала, на котором работает беспроводная точка доступа, принимает значения 20, 40 или 80 МГц;
– *Основной канал* – основной канал точки доступа. Настройка доступна при выборе ширины канала в 40 МГц – в этом случае суммарный канал 40 МГц образуется из двух соседних частотных каналов по 20 МГц. Выбор основного канала определяется положением относительно дополнительного:

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

– *Канал* – номер канала для работы беспроводной сети. При выборе значения «auto» автоматически определяется канал с меньшим уровнем помех;
– *Скрытый режим* – при установленном флаге точка доступа будет скрыта в эфире. Подключиться к ней можно, только заранее зная её SSID;
– *Включить WMM* – при установленном флаге включена функция WiFi Multimedia, которая позволяет оптимизировать передачу мультимедийного трафика по беспроводной среде;
– *Мощность сигнала* – регулировка мощности сигнала точки доступа в процентах от максимального уровня.

Дополнительные настройки

- *Порог фрагментации (Fragmentation Threshold)* – максимальный размер непрерывного блока данных для передачи по беспроводной сети. Данные большего размера будут разбиты на части — фрагментированы; принимает значения от 0 до 2346;
- *Порог RTS (RTS Threshold)* – максимальный запрашиваемый размер блока данных для передачи. В технологии CSMA/CA пакеты RTS (request to send) посылаются базовой станции до передачи реальных данных. При наличии свободного окна база отвечает пакетом CTS (clear to send) и клиент отсылает пакет запрошенного размера. Чем меньше размер RTS, тем больше вероятность получить разрешение от базовой станции, тем быстрее восстанавливается сеть после коллизий, но тем меньше производительность сети в целом. Принимает значения от 0 до 2347;
- *Период отправки служебных сообщений, мс (Beacon Interval)* – промежуток времени между служебными сообщениями в беспроводной сети. Служебные сообщения передают параметры частот, протоколов, безопасности, мощности передатчиков, задержек и т. д. Принимает значения от 20 до 1024;
- *Тип преамбулы (Preample Length)* – размер преамбулы показывает длину служебного поля в каждом пакете. Длинная преамбула состоит из 128 бит, короткая – из 56 бит. Короткий размер преамбулы повышает общее быстродействие системы, используется для мультимедиа-приложений;
- *Включить IAPP* – протокол IAPP (Inter-Access Point Protocol) позволяет использовать роуминг клиентов между несколькими точками доступа внутри одного сегмента сети;
- *Отключить защиту (Wi-Fi Protection)* – это специальный механизм для сетей 802.11 b/g. Включение механизма гарантирует возможность работы медленных устройств стандарта b в среде с большим количеством высокоскоростных устройств стандарта g. Это достигается увеличением времени обслуживания старых клиентов, заданием для них меньшего размера окна RTS, снижением общего быстродействия сети;
- *Агрегация (Aggregation)* – включает возможность объединения нескольких маленьких пакетов для передачи в одном большом;
- *Короткий защитный интерва (Short GI)* – средство снижения ошибок при взаимодействии радио устройств — пустой промежуток между передаваемыми шестнадцатеричными символами (0,1,...E,F). Стандартный длинный защитный интервал (Long GI) имеет продолжительность 800нс. Считается, что за это время сигнал полностью доходит до приемника с учетом всех задержек и отражений. По истечении этого интервала, передается следующий символ. Short GI длится 400нс. Использование Short GI повышает общую производительность беспроводной сети примерно на 11%, но иногда ведет к увеличению ошибок приема/передачи;
- *Изоляция клиентов (WLAN Partition)* – включение запрета взаимодействия беспроводных клиентов между собой;
- *Включить STBC* – включение механизма Space Time Block Coding (STBC), используется в беспроводных сетях для передачи копий потока данных через несколько антенн и для обеспечения приёма разных версий блока данных в целях повышения надежности обмена данными. Известно, что радиосигнал распространяется в среде по достаточно сложным траекториям и подвержен влиянию отражения, рефракции, рассеивания, а также искажается воздействием теплового шума приёмника, что в конечном счете приводит к тому, что одни копии переданного сигнала могут оказаться значительно лучше (менее искажены) других. Эта избыточность повышает вероятность корректно декодировать сигнал из нескольких его копий на приёмной стороне. Технология STBC объединяет все копии принятого блока данных оптимальным образом для извлечения максимального количества информации из каждой из них.
- *Сосуществование 20/40МГц (20/40MHz Coexist)* – включенная опция приводит к тому, что если в радиусе действия нашей точки доступа будут обнаружены другие точки на аналогичных частотных каналах или все каналы будут сильно загружены – наша точка доступа отключит использование частотного диапазона 40МГц, чтобы не мешать соседям;

– *Адаптивная диаграмма направленности (Beamforming)* – технология, подразумевающая формирование электромагнитного поля антенны базовой станции в дальней зоне в виде узконаправленного главного лепестка, ориентированного в сторону абонентского устройства с возможностью изменения направленных свойств при изменении положения этого оборудования.

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

4.6.2.8 Подменю «Фильтр MAC»

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

Настройки ограничения доступа по Wi-Fi

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

Список MAC-адресов

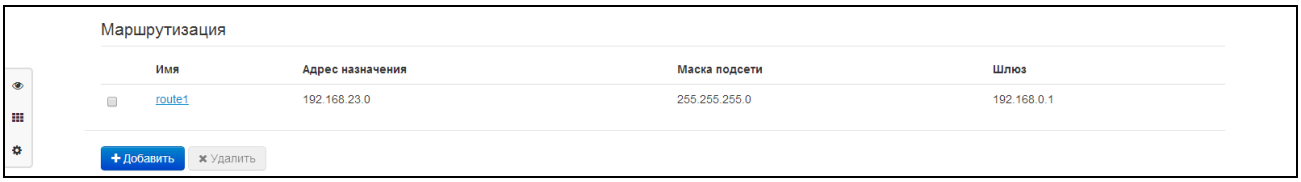
Задается отдельно для каждого диапазона. В список можно внести до тридцати MAC-адресов клиентов, доступ которым к точке доступа регулируется настройкой режима фильтра соответствующего диапазона частот.

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

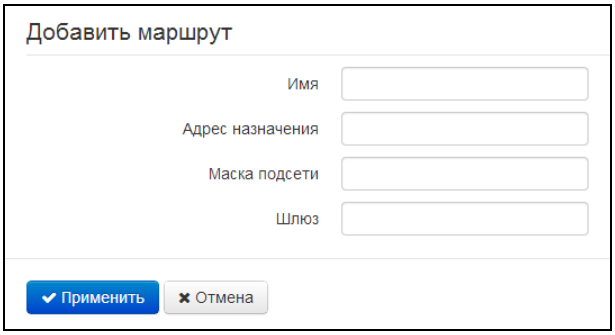
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

4.6.2.9 Подменю «Маршрутизация»

В подменю «Маршрутизация» устанавливаются статические маршруты устройства.



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



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

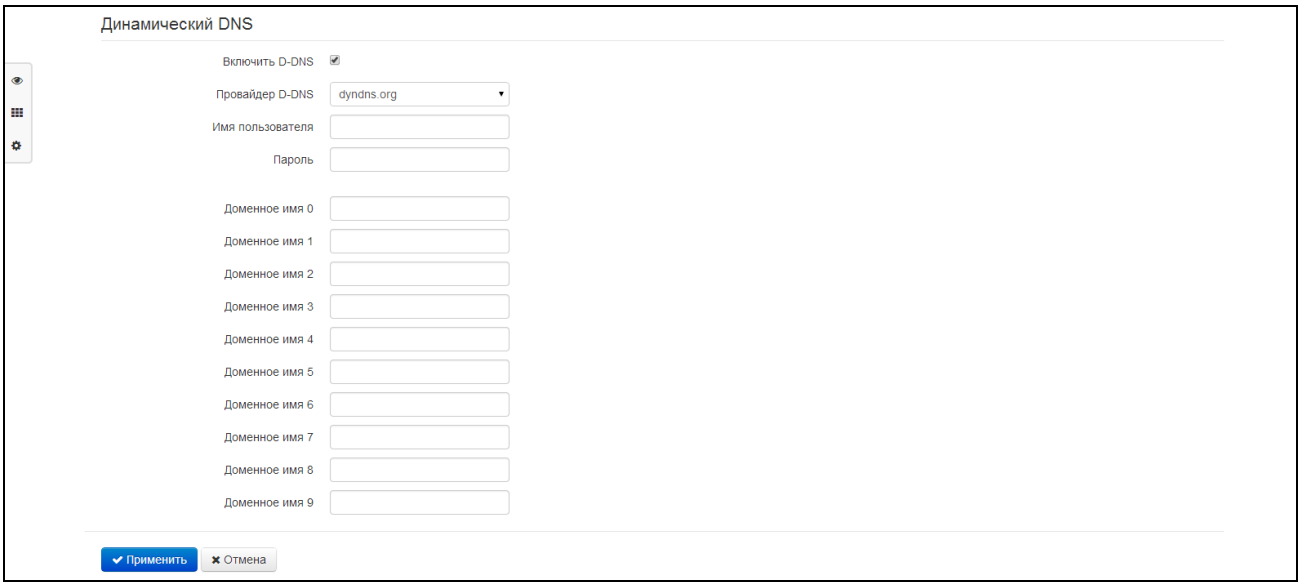
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

4.6.2.10 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.

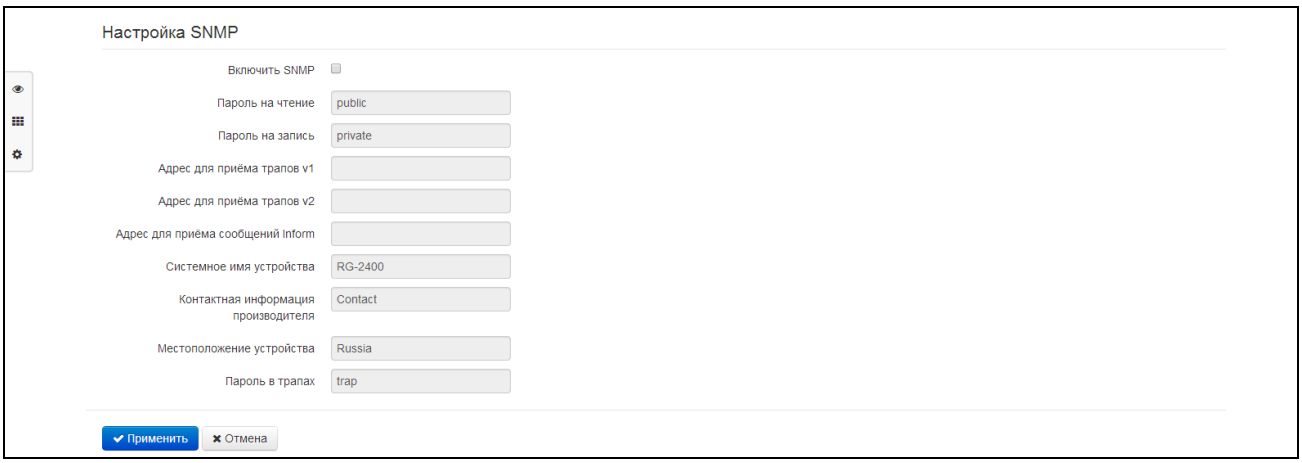


- *Включить D-DNS* – при установленном флаге сервис D-DNS активен и для редактирования доступны следующие настройки:
- *Провайдер D-DNS* – название провайдера D-DNS – выберите одного провайдера из списка доступных;
- *Имя пользователя* – имя пользователя для доступа к учетной записи сервиса D-DNS;
- *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».*

4.6.2.11 Подменю «Настройка SNMP»

Программное обеспечение *WB-2* позволяет проводить мониторинг состояния устройства и его датчиков, используя протокол SNMP. В подменю «SNMP» выполняются настройки параметров SNMP-агента. Устройство поддерживает протоколы версий SNMPv1, SNMPv2c, SNMPv3.



- *Включить SNMP* – при установленном флаге разрешено использование протокол SNMP;
- *Пароль на чтение* – пароль на чтение параметров (общепринятый: *public*);
- *Пароль на запись* – пароль на запись параметров (общепринятый: *private*);

- *Адрес для приёма трапов v1* – IP-адрес или доменное имя приемника сообщений SNMPv1-trap в формате HOST [COMMUNITY [PORT]];
- *Адрес для приёма трапов v2* – IP-адрес или доменное имя приемника сообщений SNMPv2-trap в формате HOST [COMMUNITY [PORT]];
- *Адрес для приёма сообщений Inform* – IP-адрес или доменное имя приемника сообщений Inform в формате HOST [COMMUNITY [PORT]];
- *Системное имя устройства* – имя устройства;
- *Контактная информация производителя* – контактная информация производителя устройства;
- *Местоположение устройства* – информация о местоположении устройства;
- *Пароль в трапах* – пароль, содержащийся в трапах (по умолчанию: trap).

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

- Enterprise.2.1 – настройки SNMP
- Enterprise.3.1 – настройки системного журнала

где Enterprise – 1.3.6.1.4.1.35265.1.56 идентификатор предприятия Элтекс.

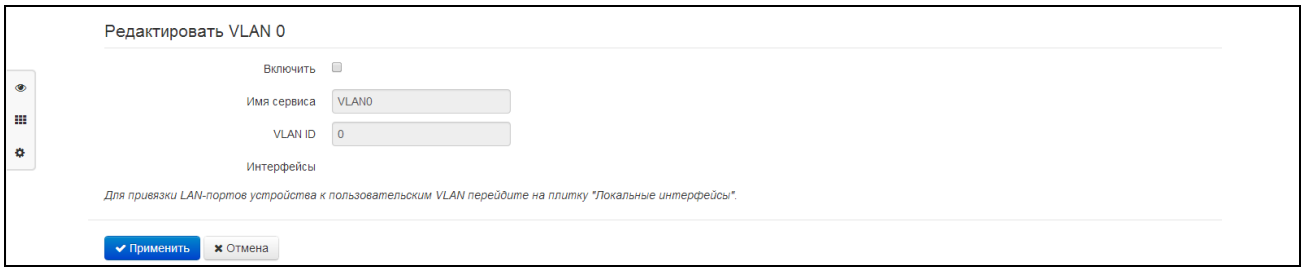
Для сохранения изменений в оперативную память устройства нажать кнопку *«Сохранить изменения» («Save Changes»)*. Для записи настроек в энергонезависимую память нажмите кнопку *«Применить» («Apply»)*.

4.6.2.12 Подменю «Пользовательские VLAN»

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

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

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



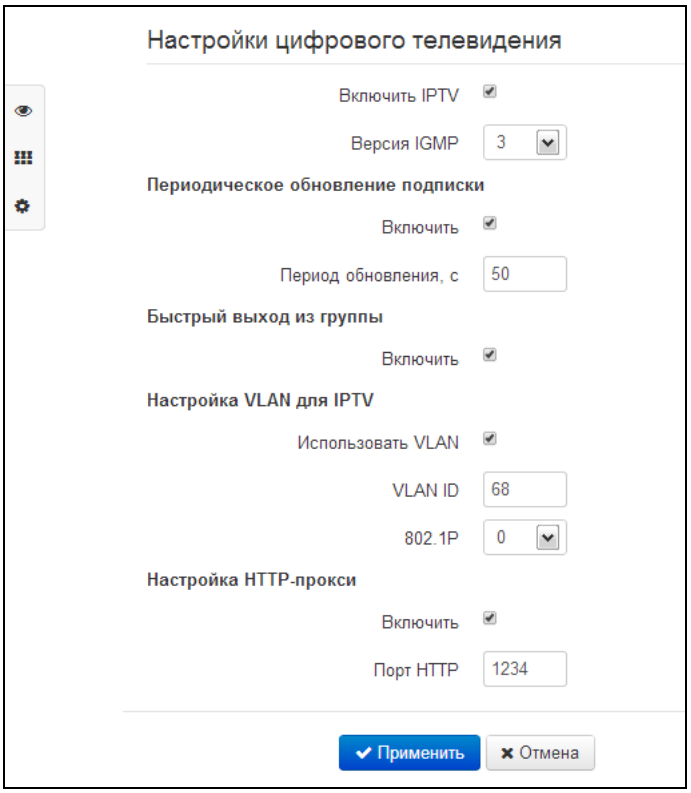
- *Включить* – при установленном флаге пользовательская VLAN включена. При попытке отключить пользовательский VLAN, к которому привязаны один или несколько LAN-портов, эти LAN-порты привяжутся к сервису Интернет;
- *Имя сервиса* – произвольное имя, сопоставляемое с данным пользовательским VLAN;
- *VLAN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

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

4.6.3 Меню «IP-телевидение»

4.6.3.1 Подменю «IPTV»

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



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

Переодическое обновление подписки

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

Настройка VLAN для IPTV

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

Настройка HTTP-прокси

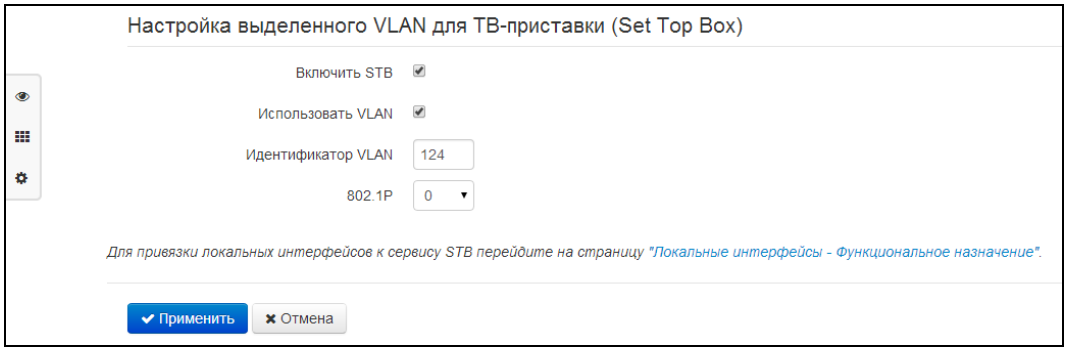
- *Включить* – при установленном флаге включена функция HTTP-прокси. HTTP-прокси осуществляет преобразование UDP-потока в поток HTTP, использующий протокол TCP (протокол надежной доставки пакетов), что позволяет улучшить качество транслируемого изображения при плохом качестве канала связи в локальной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

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

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

4.6.3.2 Подменю «STB»

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



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

- *Идентификатор VLAN* – номер VLAN, который будет использоваться для передачи трафика сервиса STB с интерфейса WAN устройства;
- *802.1P* – признак 802.1P (другое название *CoS – Class of Service*), устанавливаемый на исходящие с данного интерфейса IP-пакеты. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет). Используется в работе алгоритмов обеспечения качества сервиса (QoS).

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

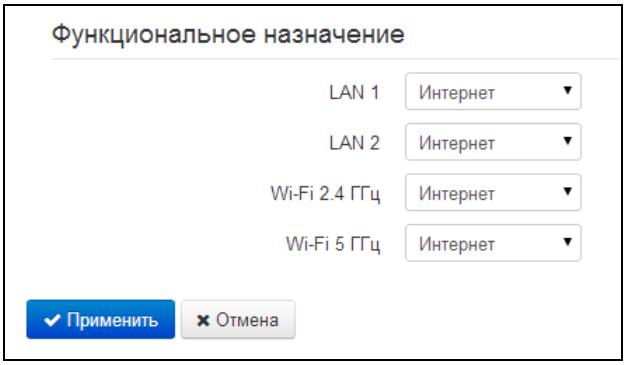
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить».* Для отмены изменений нажмите кнопку *«Отмена».*

4.6.4 Меню «Локальные интерфейсы»

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

4.6.4.1 Подменю «Функциональное назначение»

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



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

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

WAN-интерфейс услуги STB настраивается в разделе 4.6.3.2.

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

Таким образом, устройство обеспечивает возможность выхода в Интернет и подключения телевизионной приставки как по проводному каналу, так и через беспроводную точку доступа Wi-Fi в любом диапазоне частот.

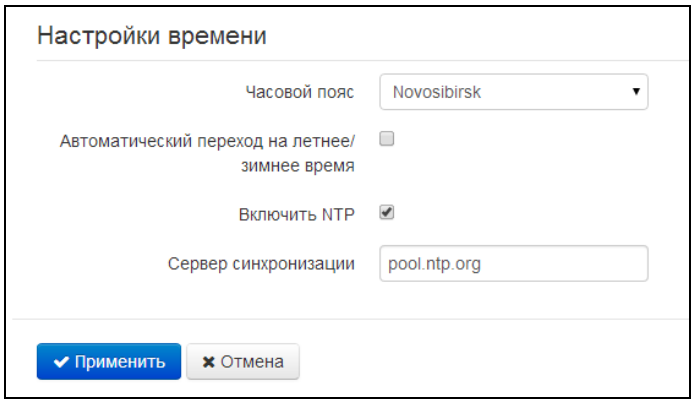
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

4.6.5 Меню «Система»

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

4.6.5.1 Подменю «Время»

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



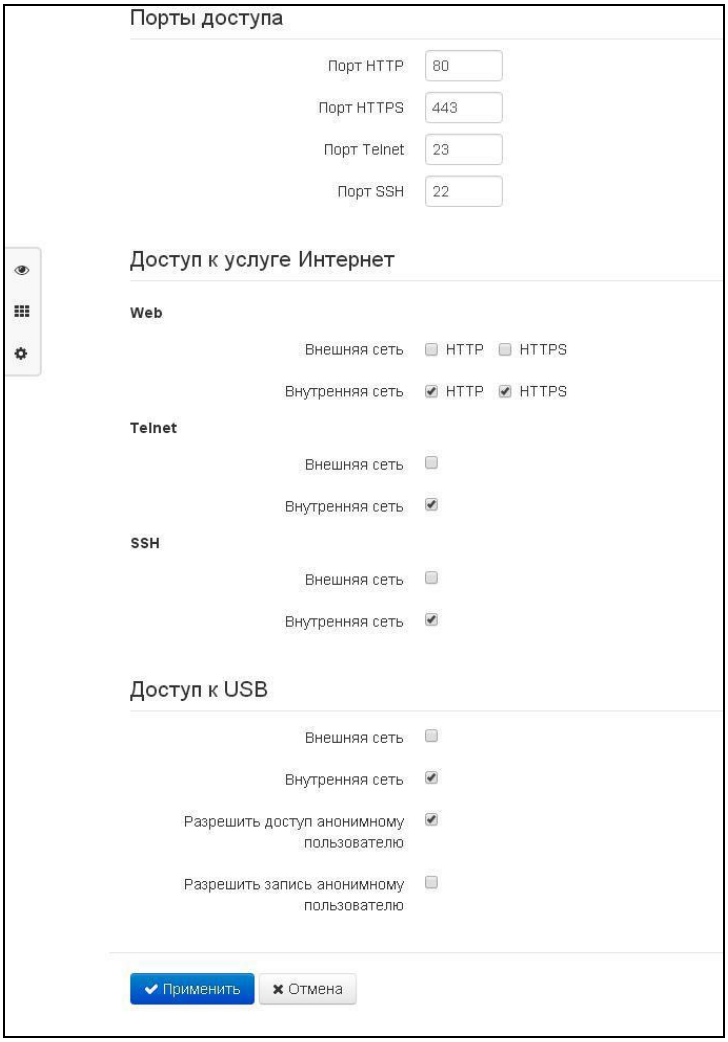
Настройки времени

- *Часовой пояс* – позволяет установить часовой пояс в соответствии с ближайшим городом в Вашем регионе из заданного списка;
- *Автоматический переход на летнее/зимнее время* – при установленном флаге 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»*.

4.6.5.2 Подменю «Доступ»

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



Порты доступа

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

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

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

Доступ к услуге Интернет

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

Web, Внешняя сеть:

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

Web, Внутренняя сеть:

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

Telnet:

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

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

SSH:

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

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

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

Доступ к USB:

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

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

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

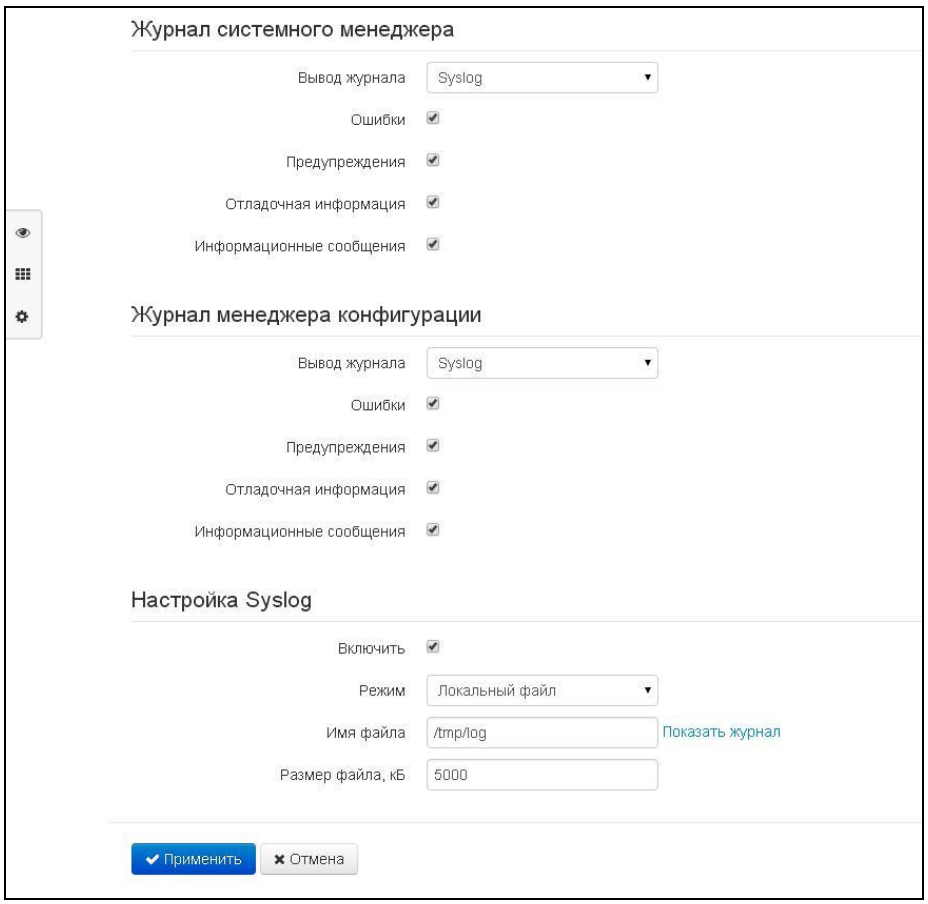
Для разрешения записи данных на USB-устройство анонимному пользователю установите флаг «Разрешить запись анонимному пользователю».

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

4.6.5.3 Подменю «Журнал»

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

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



Журнал системного менеджера

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

Ниже настраивается тип сообщений, выводимых в журнал системного менеджера:

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

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

Журнал менеджера конфигурации

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

Ниже настраивается тип сообщений, выводимых в журнал менеджера конфигурации:

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

Настройка Syslog

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

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

Далее в зависимости от режима Syslog-агента доступны настройки:

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

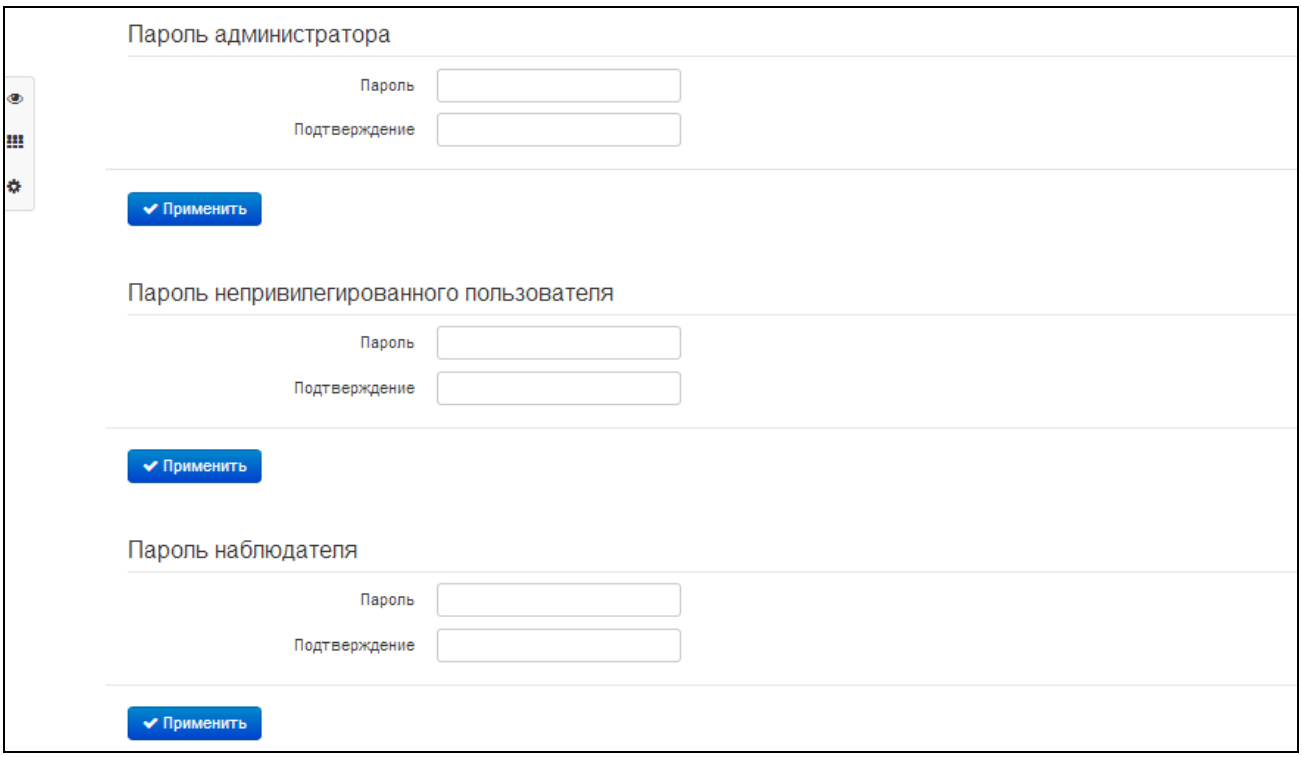
4.6.5.4 Подменю «Пароли»

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

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

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

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

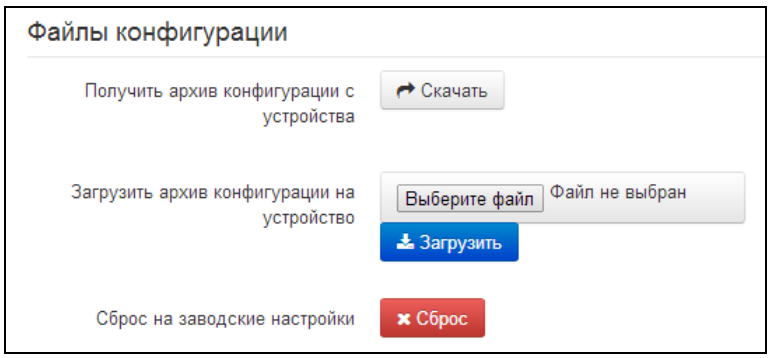


- *Пароль администратора* – в соответствующие поля введите пароль администратора и подтвердите его;
- *Подтверждение пароля* – в соответствующие поля введите пароль непривилегированного пользователя и подтвердите его.

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

4.6.5.5 Подменю «Управление конфигурацией»

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



Получение конфигурации

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

Обновление конфигурации

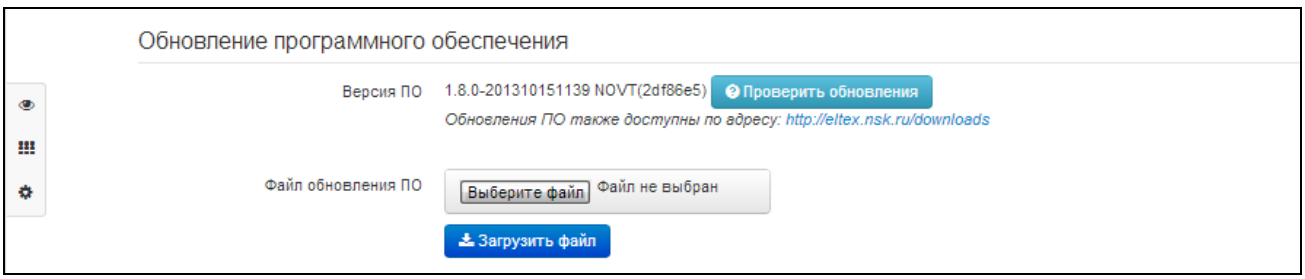
– *Архив конфигурации* – выбор сохраненного на локальном компьютере файла конфигурации. Для обновления конфигурации устройства нажмите кнопку «Обзор», укажите файл (в формате .tar.gz) и нажмите кнопку «Загрузить». Загруженная конфигурация применяется автоматически без перезагрузки устройства.

Сброс устройства на заводские настройки

Чтобы сделать сброс всех настроек устройства на стандартные заводские установки, нажмите кнопку «Сброс».

4.6.5.6 Подменю «Обновление ПО»

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



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

Для работы функции проверки обновления необходимо наличие выхода в Интернет.

Обновить программное обеспечение устройства можно также вручную, предварительно загрузив файл ПО с сайта *http://eltex.nsk.ru/downloads* и сохранив его на компьютере. Для этого нажмите кнопку «Выберите файл» в поле *Файл обновления ПО* и укажите путь к файлу управляющей программы в формате .tar.gz.

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

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

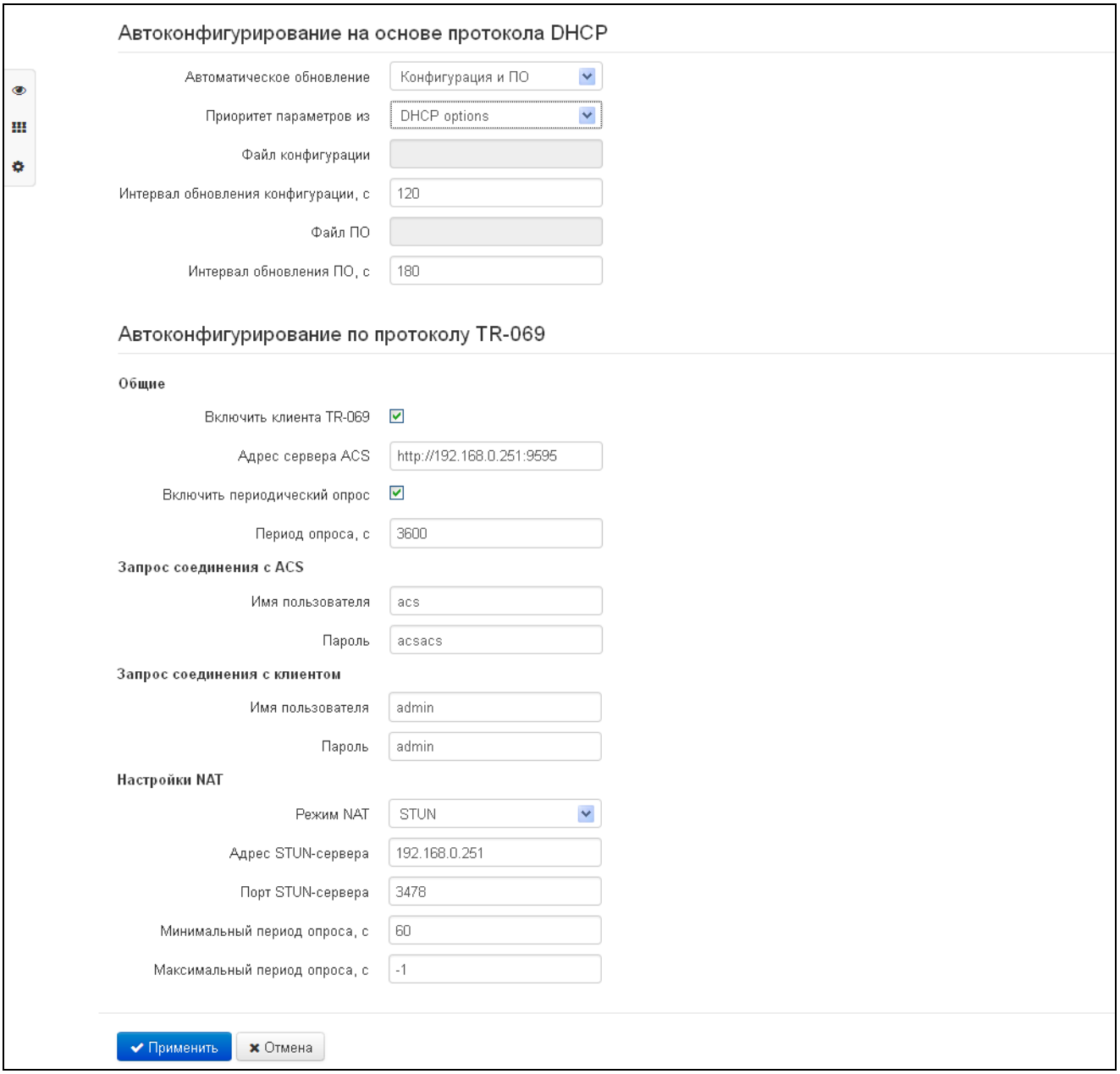
4.6.5.7 Подменю «Перезагрузка»

В подменю «Перезагрузка» выполняется перезапуск устройства.

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

4.6.5.8 Подменю «Автоконфигурирование»

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



Автоконфигурирование на основе протокола DHCP:

- *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 5*;
- *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 5*;

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

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

– *Интервал обновления конфигурации, с* – промежуток времени в секундах, через который осуществляется периодическое обновление конфигурации устройства; выбор значения 0 означает однократное обновление только сразу после загрузки устройства;
– *Файл ПО* – полный путь к файлу программного обеспечения – задаётся в формате URL (на данный момент возможна загрузка файла ПО по протоколам TFTP и HTTP):

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

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

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

Автоконфигурирование по протоколу TR-069:

Общие:

– *Включить клиента TR-069* – при установленном флаге разрешена работа встроенного клиента протокола TR-069, иначе – запрещена;
– *Адрес сервера ACS* – адрес сервера автоконфигурирования. Адрес необходимо вводить в формате http://<address>:<port> или https://<address>:<port> (<address> – IP-адрес или доменное имя ACS-сервера, <port> – порт сервера ACS, по умолчанию порт 10301). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS;
– *Включить периодический опрос* – при установленном флаге встроенный клиент TR-069 осуществляет периодический опрос сервера ACS с интервалом, равным *«Периоду опроса»*, в секундах. Цель опроса - обнаружить возможные изменения в конфигурации устройства.

Запрос соединения с ACS:

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

Запрос соединения с клиентом:

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

Настройки NAT:

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

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

При выборе режима *STUN* необходимо задать следующие настройки:

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

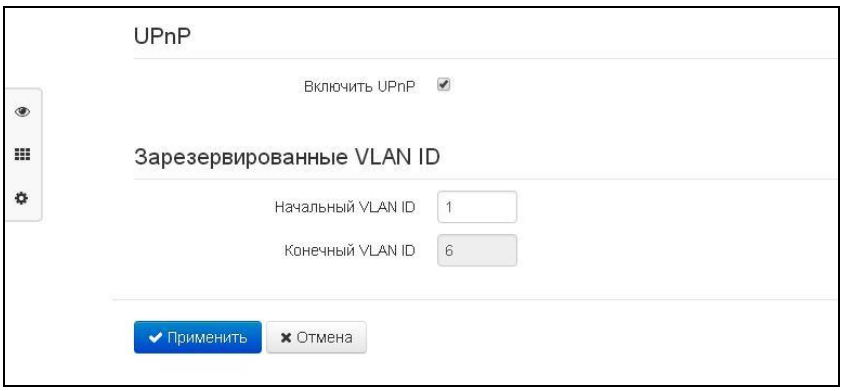
При выборе режима *Manual* публичный адрес клиента задается вручную через параметр *Адрес NAT* (адрес необходимо вводить в формате IPv4).

В версии ПО 1.9.0 по протоколу TR-069 возможно произвести полное конфигурирование устройства, обновление программного обеспечения, чтение информации об устройстве (версия ПО, модель, серийный номер и т.д), загрузку и выгрузку целого файла конфигурации, удаленную перезагрузку устройства (поддержаны спецификации TR-069, TR-098, TR-104).

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

4.6.5.9 Подменю «Дополнительные настройки»

В подменю «Дополнительные настройки» можно включить UPnP и задать резервирование VLAN ID..



UPnP

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.

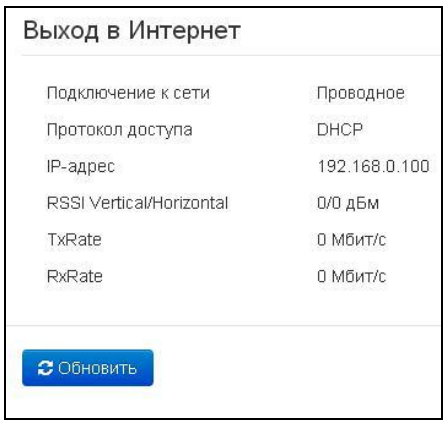
4.7 Мониторинг системы

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

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

4.7.1 Подменю «Интернет»

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



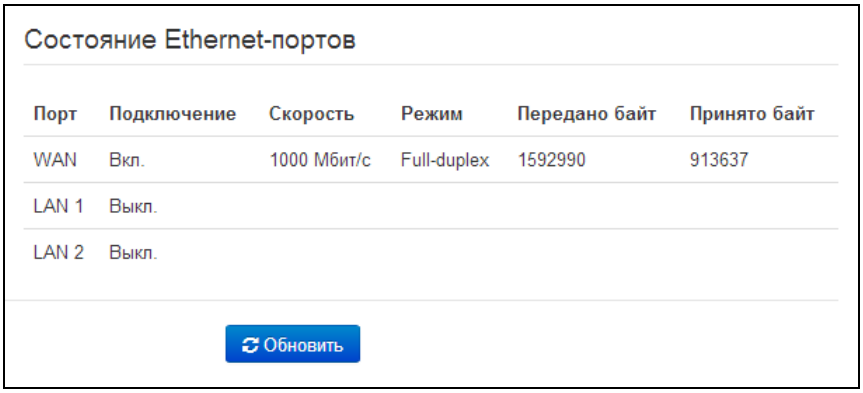
Выход в Internet

- *Подключение к сети* – показывает тип подключения к внешней сети Интернет;
- *Протокол доступа* – протокол, используемый для доступа к сети Интернет;
- *IP-адрес* – IP-адрес устройства во внешней сети;
- *RSSI Vertical/Horizontal* – уровень мощности Wi-Fi сигнала при использовании устройства в режиме клиента;
- *TxRate* – скорость передачи данных от устройства в режиме Wi-Fi клиента;
- *RxRate* – скорость приема данных устройством в режиме Wi-Fi клиента.

Для обновления информации на странице нажмите кнопку «Обновить».

4.7.2 Подменю «Ethernet-порты»

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



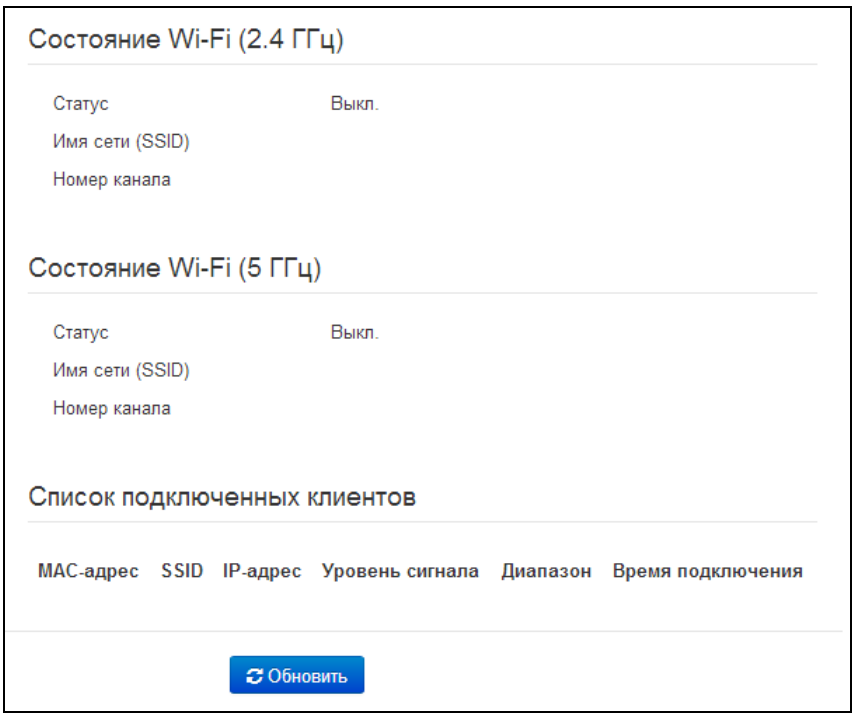
Состояние Ethernet-портов

- *Порт* – название порта:
  - *WAN* – порт внешней сети;
  - *LAN 1..2* – порт локальной сети.
- *Подключение* – состояние подключения к данному порту:
  - *Вкл.* – к порту подключено сетевое устройство (линк активен);
  - *Выкл.* – к порту не подключено сетевое устройство (линк не активен).
- *Скорость* – скорость подключения внешнего сетевого устройства к порту (10/100/1000 Мбит/с);
- *Режим* – режим передачи данных:
  - *Full-duplex* – полный дуплекс;
  - *Half-duplex* – полудуплекс;
- *Передано байт* – количество переданных байт с порта;
- *Принято байт* – количество принятых байт портом.

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

4.7.3 Подменю «Wi-Fi»

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



Состояние Wi-Fi

- *Статус* – состояние сети Wi-Fi:
  - *Выкл.* – сеть Wi-Fi выключена;
  - *Вкл.* – сеть Wi-Fi включена.
- *Имя сети (SSID)* – имя точки доступа Wi-Fi в соответствующем диапазоне частот;

– *Номер канала* – текущий номер канала, используемый точкой доступа в соответствующем диапазоне частот.

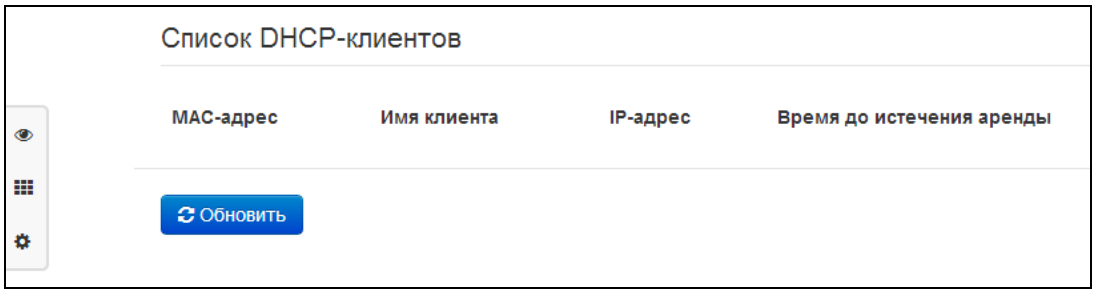
Список подключеных клиентов

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

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

4.7.4 Подменю «DHCP»

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



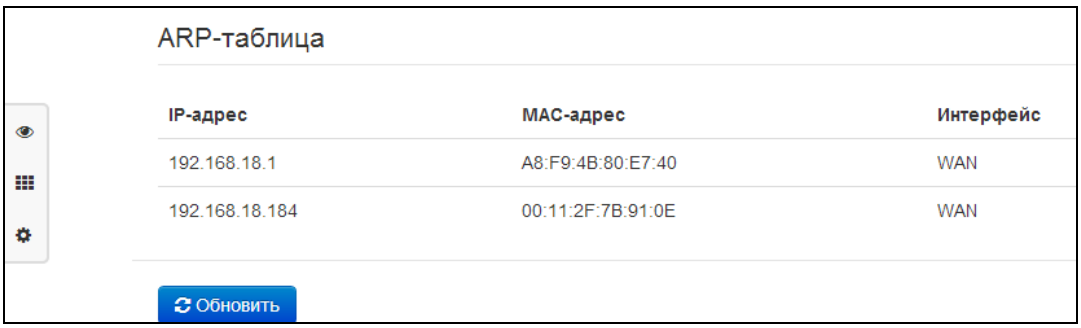
Активные DHCP-аренды

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

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

4.7.5 Подменю «ARP»

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



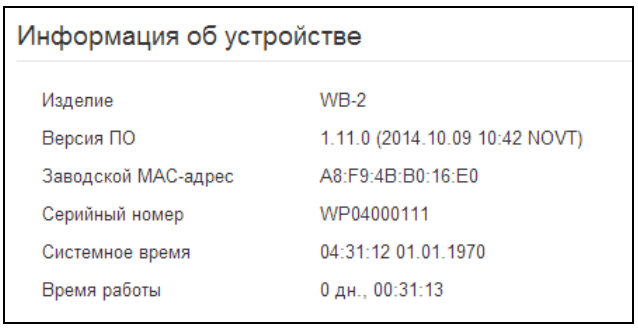
ARP-таблица

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

Для получения текущей информации нажмите кнопку «Обновить».

4.7.6 Подменю «Устройство»

В подменю «Устройство» приведена общая информация об устройстве.

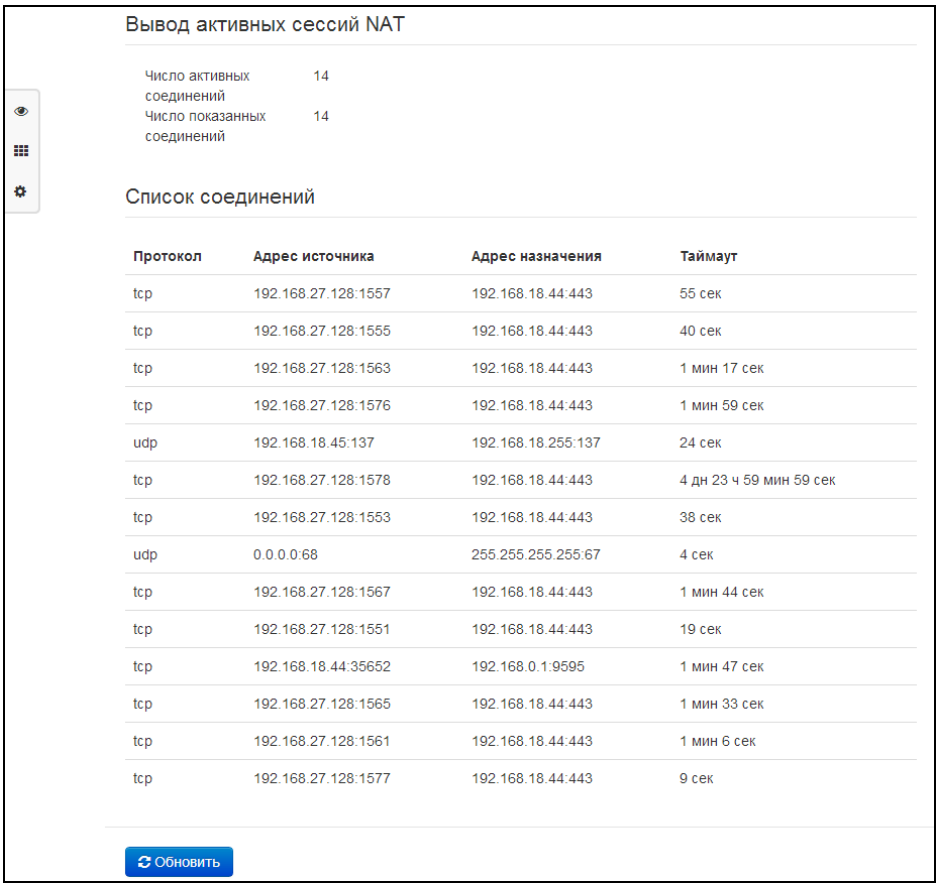


Информация об устройстве

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

4.7.7 Подменю «Conntrack»

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



Вывод активных сессий NAT

- *Число активных соединений* – общее число активных сетевых соединений;
- *Число показанных соединений* – число соединений, выведенных в WEB-интерфейс. Чтобы не снижать производительность работы WEB-интерфейса, максимальное число показанных соединений ограничено значением 1024. Остальные соединения можно посмотреть через командную консоль устройства.

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».

4.7.8 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 подсети* – маска подсети;
- *Флаги* – определенные характеристики данного маршрута. Существуют следующие значения *флагов*:

  - **U -** указывает, что маршрут создан и является проходимым;
  - **H -** указывает на маршрут к определенном узлу;
  - **G -** указывает, что маршрут пролегает через внешний шлюз. Сетевой интерфейс системы предоставляет маршруты в сети с прямым подключением. Все прочие маршруты проходят через внешние шлюзы. Флагом G отмечаются все маршруты, кроме маршрутов в сети с прямым подключением;
  - **R -** указывает, что маршрут, скорее всего, был создан динамическим протоколом маршрутизации, работающим на локальной системе, посредством параметра reinstate;
  - **D -** указывает, что маршрут был добавлен в результате получения сообщения перенаправления ICMP (ICMP Redirect Message). Когда система узнает о маршруте из сообщения ICMP Redirect, маршрут включается в таблицу маршрутизации, чтобы исключить перенаправление для последующих пакетов, предназначенных тому же адресату. Такие маршруты отмечены флагом D;
  - **M -** указывает, что маршрут подвергся изменению - вероятно, в результате работы динамического протокола маршрутизации на локальной системе и применения параметра mod;
  - **A -** указывает на буферизованный маршрут, которому соответствует запись в таблице ARP.
  - **C -** указывает, что источником маршрута является буфер маршрутизации ядра;
  - **L -** указывает, что пунктом назначения маршрута является один из адресов данного компьютера. Такие «локальные маршруты» существуют только в буфере маршрутизации;
  - **B -** указывает, что конечным пунктом маршрута является широковещательный адрес. Такие «широковещательные маршруты» существуют только в буфере маршрутизации;
  - **I -** указывает, что маршрут связан с кольцевым (loopback) интерфейсом с целью иной, нежели обращение к кольцевой сети. Такие «внутренние маршруты» существуют только в буфере маршрутизации;
  - **!** - указывает, что дейтаграммы, направляемые по этому адресу, будут отвергаться системой;

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

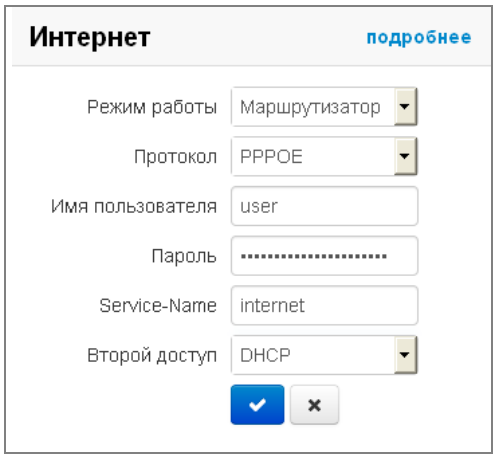
Для получения текущей информации нажмите кнопку «Обновить».

4.8 Пример настройки

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

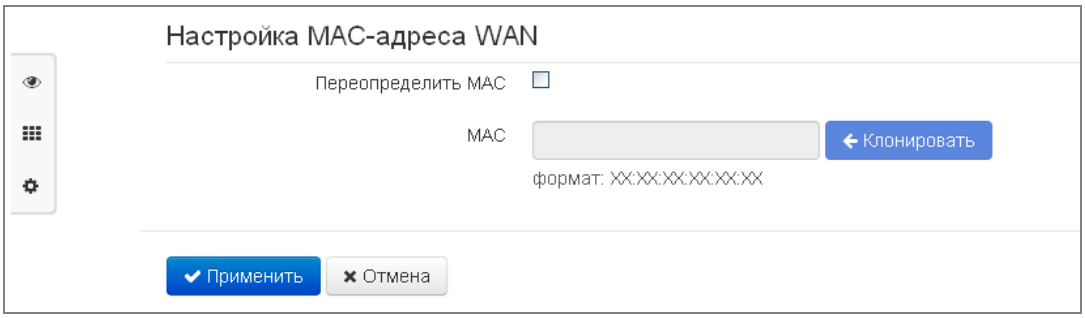
Если это окно не появилось, убедитесь, что в настройках сетевого подключение на вашем ПК установлено автоматическое получение IP-адреса.

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

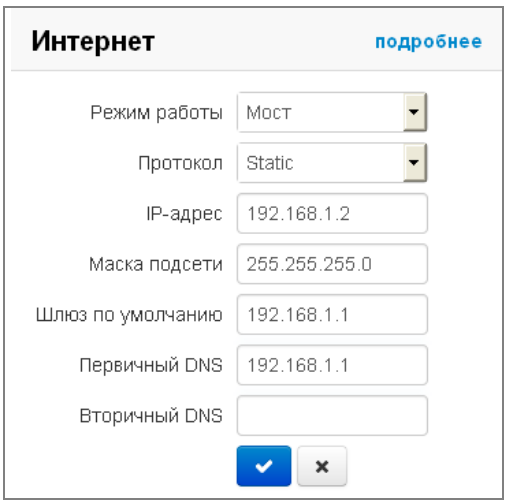


Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее» (смотрите раздел *4.6.2.1* Подменю «Интернет»).

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

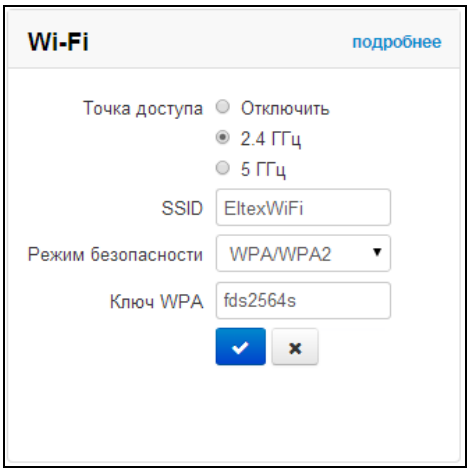


Если *устройство* будет использоваться в качестве 3-портового коммутатора, в плитке «Интернет» выберите значение поля «Режим работы» *Мост*. В поле «IP-адрес» укажите адрес, который будет назначен устройству для доступа к нему. Введите маску подсети (по умолчанию 255.255.255.0) и при необходимости шлюз по умолчанию и адрес DNS-сервера. Для сохранения и применения настроек нажмите кнопку .



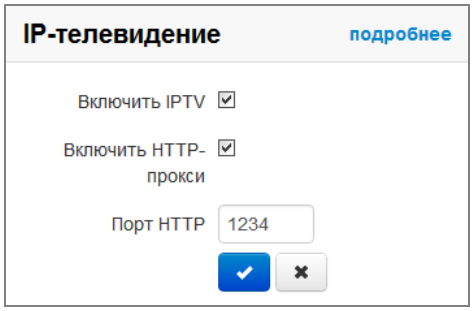
В режиме *Мост* шлюз не будет автоматически выдавать IP-адреса по протоколу DHCP устройствам, подключенным к интерфейсу LAN.

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



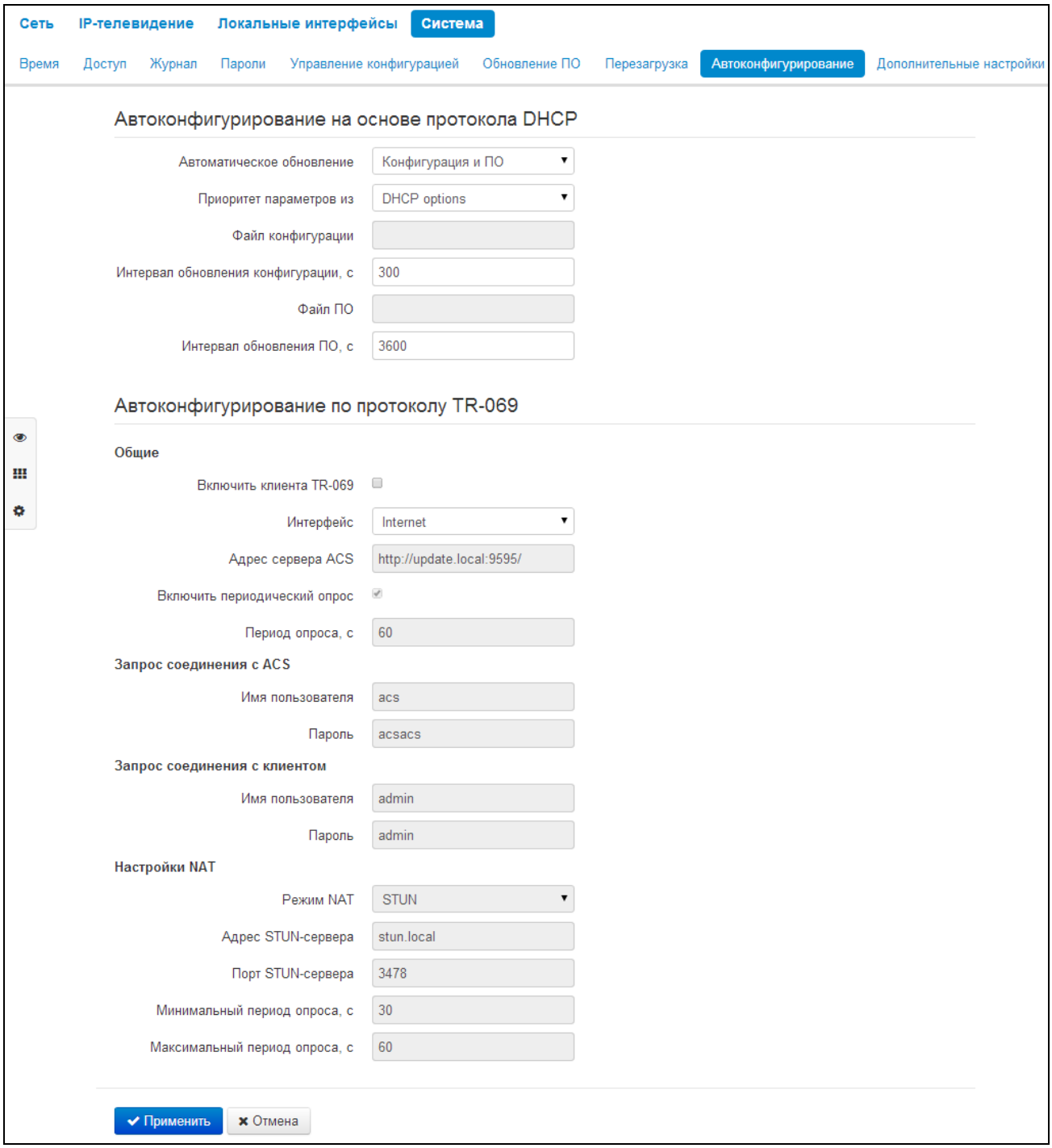
Для указания дополнительных параметров перейдите в режим расширенных настроек, нажав ссылку «подробнее» (смотрите раздел 4.6.2.7 Подменю «Wi-Fi»).

7. Если предполагается использование IP-телевидения – в плитке «IP-телевидение» отметьте пункт «Включить IPTV». Для включения возможности передачи IPTV потоков по HTTP отметьте пункт «Включить HTTP-прокси». В поле «Порт HTTP» укажите порт, который будет использоваться для подключения внешних устройств к локальному HTTP-прокси. Рекомендуется использовать HTTP-прокси при просмотре IP-телевидения через беспроводную сеть Wi-Fi (в целях улучшения качества транслируемого в эфире изображения). Для сохранения и применения настроек нажмите кнопку  .



Если для услуги IPTV используется отдельный VLAN, перейдите в режим расширенных настроек, нажав ссылку «подробнее» и укажите ID VLAN в соответствующем поле (смотрите раздел 4.6.3 Меню «IP-телевидение»).

5 АЛГОРИТМ РАБОТЫ АВТОМАТИЧЕСКОГО ОБНОВЛЕНИЯ УСТРОЙСТВА НА ОСНОВЕ ПРОТОКОЛА DHCP



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

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

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

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

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

- *$MA* – MAC address – вместо данного макроса в URL файла устройство подставляет собственный MAC-адрес;
- *$SN* – Serial number – вместо данного макроса в URL файла устройство подставляет собственный серийный номер;
- *$PN* – Product name – вместо данного макроса в URL файла устройство подставляет название модели (например, RG-2402G-W).

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-2/my.cfg,
tftp://server.tftp/$PN/config/$SN.cfg,
http://server.http/$PN/firmware/$MA.frm и т.д.

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

http://192.168.18.6
или
config_rg24.cfg

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

- для протокола: tftp;
- для адреса сервера: update.local;
- для имени файла конфигурации: <MAC>.cfg;
- для имени файла программного обеспечения: wb2.fw.

В имени файла конфигурации вместо <MAC> будет указан MAC-адрес порта WAN, он состоит из 6-ти октетов, разделенных точками. Пример имени файла конфигурации по умолчанию: A8.F9.4B.B2.1E.46.cfg. 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/ A8.F9.4B.B2.1E.46.cfg ,

а URL файла ПО:

tftp://update.local/wb2.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: <MAC>.cfg;
   - для имени файла программного обеспечения: wb2.fw.

Формат опции 43 (Vendor specific info)

1|< acs_url >|2|< opcode >|3|<login_acs>|4|<password_acs>|5|<server_url>|6|< config.file >|7|< password >|8|< vlan_tag>

- 1 – код адреса сервера автоконфигурирования по протоколу TR-069;
- 2 – код для указания параметра Provisioning Code[1].
- 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 анализируется подопция 4 (vlan_tag):

- подопция присутствует и отличается от текущего тега VLAN – инициируется DHCP-обмен в новом VLAN;
- подопция отсутствует либо присутствует и не отличается от текущего тега VLAN: выполняется анализ подопций с кодами 1, 2 и 3 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 6.

6 ПРОЦЕДУРА ВОССТАНОВЛЕНИЯ СИСТЕМЫ ПОСЛЕ СБОЯ ПРИ ОБНОВЛЕНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

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

- Распакуйте архив с файлом программного обеспечения.
- Подключите ПК к порту WAN устройства, установите на сетевом интерфейсе адрес из подсети 192.168.1.0/24.
- Запустите на ПК TFTP-клиента (для Windows рекомендуется использовать программу Tftpd32), в качестве адреса удалённого хоста укажите 192.168.1.6, а для передачи выберите файл linux.bin из распакованного архива программного обеспечения.
- Запустите команду отправки файла на удаленный хост (команда **Put**). Должен запуститься процесс передачи файла на устройство.
- Если процесс передачи файла начался – дождитесь его окончания, после чего 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

Периодически 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 config.yaml создана секция настроек:

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

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

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

1. Запуск с HTTP-сервера

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

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

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

2. Запуск с TFTP-сервера

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

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

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

3. Запуск локального скрипта

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

   chmod 777 /etc/config/user.sh

   В файле конфигурации URL для запуска локального скрипта имеет вид:

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

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

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Для получения технической консультации по вопросам эксплуатации оборудования ТОО «ЭлтексАлатау» Вы можете обратиться в Сервисный центр компании:

050032, Республика Казахстан, г. Алматы, мкр-н. Алатау, ул. Ибрагимова 9
Телефоны центра технической поддержки:
+7 (727) 320-18-40
E-mail: info@eltexalatau.kz
На официальном сайте компании Вы можете найти техническую документацию и программное обеспечение для продукции ТОО «ЭлтексАлатау», обратиться к в базе знаний, оставить интерактивную заявку или проконсультироваться у инженеров Сервисного центра :

www.eltexalatau.kz