Абонентская станция

WB-2P-LR5

Руководство по эксплуатации

Версия ПО 2.4.6

IP-адрес: 192.168.1.1

Username: admin

Password: password

Содержание

1 Введение ... 4

1.1 Аннотация ... 4

1.2 Условные обозначения ... 4

2 Описание изделия ... 5

2.1 Назначение ... 5

2.2 Характеристики устройства ... 5

2.3 Основные технические параметры ... 8

2.4 Конструктивное исполнение ... 10

2.5 Световая индикация ... 11

2.6 Сброс к заводским настройкам ... 12

2.7 Комплект поставки ... 12

3 Порядок установки ... 13

3.1 Инструкции по технике безопасности ... 13

3.2 Рекомендации по установке ... 13

3.3 Монтаж устройства WB-2P-LR5 ... 14

3.3.1 Предварительная настройка ... 14

3.3.2 Порядок монтажа ... 14

3.4 Включение устройства ... 16

3.5 Юстировка антенны Wi-Fi ... 16

4 Управление устройством через web-конфигуратор ... 17

4.1 Начало работы ... 17

4.2 Смена пользователей ... 18

4.3 Применение конфигурации и отмена изменений ... 19

4.4 Тестовый режим ... 20

5 Основные элементы web-интерфейса ... 21

5.1 Меню «Мониторинг» ... 22

5.1.1 Подменю «Интернет» ... 22

5.1.2 Подменю «WDS» ... 24

5.1.3 Подменю «Ethernet-порты» ... 25

5.1.4 Подменю «DHCP» ... 25

5.1.5 Подменю «ARP» ... 26

5.1.6 Подменю «PPPoE Relay» ... 26

5.1.7 Подменю «PPPoE Client» ... 27

5.1.8 Подменю «Устройство» ... 27

5.1.9 Подменю «Conntrack» ... 28
5.1.10 Подменю «Маршрутизация» ... 29
5.2 Меню «Сеть» ... 30
5.2.1 Подменю «Интернет» ... 30
5.2.2 Подменю «Радиоинтерфейс» ... 40
5.2.3 Подменю «Локальная сеть» ... 42
5.2.4 Подменю «Настройка MAC-адресов» ... 43
5.2.5 Подменю «Локальный DNS» ... 44
5.2.6 Подменю «NAT и проброс портов» ... 45
5.2.7 Подменю «Сетевой экран» ... 47
5.2.8 Подменю «Маршрутизация» ... 49
5.2.9 Подменю «Динамический DNS» ... 50
5.2.10 Подменю «SNMP» ... 51
5.3 Меню «IP-телевидение» ... 52
5.3.1 Подменю «IPTV» ... 52
5.4 Меню «Система» ... 54
5.4.1 Подменю «Время» ... 54
5.4.2 Подменю «Доступ» ... 55
5.4.3 Подменю «Журнал» ... 56
5.4.4 Подменю «Пароли» ... 58
5.4.5 Подменю «Управление конфигурацией» ... 59
5.4.6 Подменю «Обновление ПО» ... 60
5.4.7 Подменю «Перезагрузка» ... 61
5.4.8 Подменю «Автоконфигурирование» ... 61
5.4.9 Подменю «Дополнительные настройки» ... 64
6 Пример настройки ... 66
7 Спектроанализатор ... 68
8 Алгоритм работы автоматического обновления устройства на основе протокола DHCP ... 69
9 Процедура восстановления системы после сбоя при обновлении программного обеспечения ... 72
10 Приложение А. Запуск произвольного скрипта при старте системы ... 73
11 Приложение Б. Диаграмма направленности ... 74
12 Список изменений ... 76

1 Введение

1.1 Аннотация

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

WB-2P-LR5 – это абонентская станция, основное предназначение которой - подключение к беспроводной сети доступа Wi-Fi. Сеть может быть построена с использованием базовых станций. Конструкция WB-2P-LR5 имеет герметичный корпус, что предполагает установку устройства преимущественно на открытой территории в различных климатических условиях.

В настоящем руководстве по эксплуатации изложены назначение, основные технические характеристики, конструктивное исполнение, порядок установки, правила конфигурирования, мониторинга и смены программного обеспечения абонентской станции WB-2P-LR5.

1.2 Условные обозначения

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

Абонентская станция WB-2P-LR5 (далее «устройство») разработана для предоставления доступа к высокоскоростной безопасной беспроводной сети.

Устройство WB-2P-LR5 обеспечивает доступ к современным интерактивным сервисам: Интернет, IPTV, VoIP.

WB-2P-LR5 подключается к базовой станции по технологии Wi-Fi и работает в диапазоне 5 и 6 ГГц (частотный диапазон 5830 - 6150 МГц поддержан на устройствах WB-2P-LR5 rev.B и WB-2P-LR5 rev.C). Предполагается использование совместно с WOP-2ac-LR5. Также может использоваться для организации беспроводного моста между устройствами.

WB-2P-LR5 поддерживает современные требования к качеству сервисов и позволяет передавать наиболее важный трафик в приоритетных очередях. Обеспечение приоритизации происходит на основе технологий QoS: CoS (специальные метки в поле VLAN-пакета) и ToS (метки в поле IP-пакета).

Устройство может работать в широком диапазоне рабочих температур и высокой влажности (парки, заводы, стадионы и т.д.).

Питание устройства осуществляется по технологии Passive PoE 24 В.

2.2 Характеристики устройства

Интерфейсы:

- 1 порт Ethernet 10/100/1000BASE-T (RJ-45);
- Wi-Fi 5-6 ГГц IEEE 802.11a/n/ac;
- Технологический Wi-Fi 2.4 ГГц 802.11b/g/n (интерфейс малого радиуса действия для юстировки и настройки устройства в период инсталляции).[1]

Питание устройства осуществляется через PoE-инжектор 24 В от сети 220 В.

При питании устройства инжектором напряжения отличного от 24 В устройство выйдет из строя!

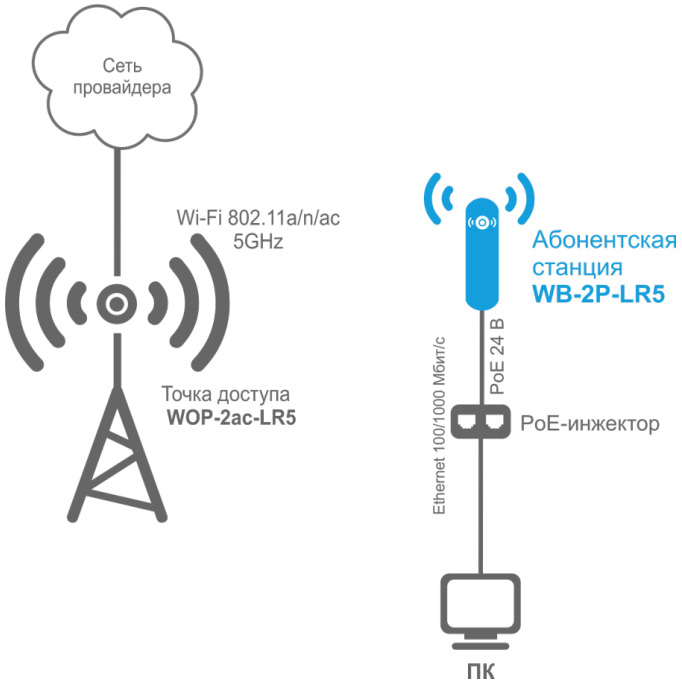
[1]Для WB-2P-LR5 rev.C.

Сетевые функции:

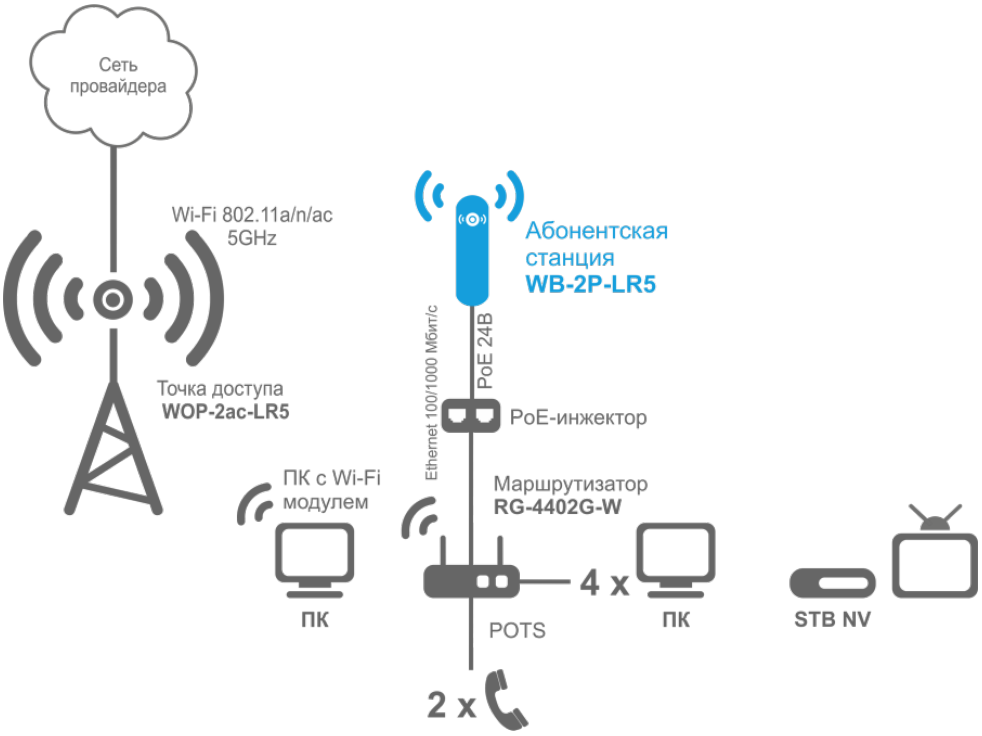
- работа в режиме «моста» или «маршрутизатора»;
- работа в режиме устройства «Wi-Fi Клиент» и «Беспроводной мост»;
- поддержка режима VLAN Trunk;
- поддержка Management VLAN;
- поддержка General VLAN;
- поддержка Transparent Mode;
- статическая маршрутизация;
- поддержка функции Беспроводной прозрачный мост;
- поддержка PPPoE-клиента;
- синхронизация времени по NTP;
- поддержка статического адреса и DHCP (DHCP-клиент на стороне WAN, DHCP-сервер на стороне LAN);
- поддержка DNS;
- поддержка D-DNS;
- поддержка NAT;
- поддержка UPnP;

- сетевой экран;
- поддержка клонирования MAC-адреса на WAN-интерфейсе;
- 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;
- поддержка TR-069;
- удаленный мониторинг, конфигурирование и настройка: SNMP, web-интерфейс, Telnet, SSH.

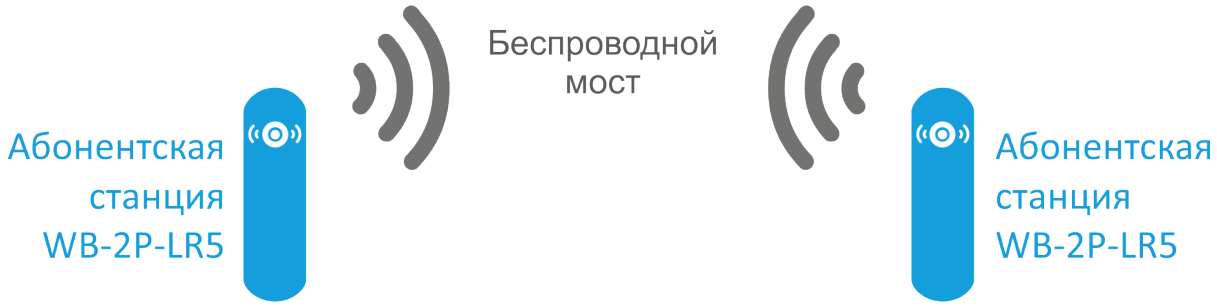
На рисунках ниже приведены схемы применения оборудования WB-2P-LR5.



Функциональная схема использования WB-2P-LR5 без маршрутизатора



Функциональная схема использования WB-2P-LR5 с маршрутизатором



Функциональная схема использования WB-2P-LR5 для организации беспроводного моста

2.3 Основные технические параметры

Основные технические параметры устройства приведены в таблице 1.

Таблица 1 – Основные технические параметры

Параметры LAN-интерфейса Ethernet	
Количество портов	1
Электрический разъем	RJ-45
Скорость передачи, Мбит/с	10/100/1000, автоопределение
Поддержка стандартов	BASE-T
Параметры беспроводного интерфейса	
Стандарты	802.11a/n/ac
Частотный диапазон, МГц	5180–5825 МГц 5180-6150 МГц (для устройств WB-2P-LR5 rev.B, WB-2P-LR5 rev.C)
Модуляция	BPSK, QPSK, 16QAM, 64QAM, 256QAM
Скорость передачи данных, Мбит/с	**802.11a:** до 54 Мбит/с **802.11n:** до 300 Мбит/с **802.11ac:** до 867 Мбит/с
Максимальная выходная мощность передатчика	**5–6 ГГц:** 24 дБм (для устройств WB-2P-LR5, WB-2P-LR5 rev.B) 28 дБм (для устройств WB-2P-LR5 rev.C)
Чувствительность приемника	**5–6 ГГц:** -94 дБм
Безопасность	64/128/152-битное WEP-шифрование данных, WPA/WPA2,централизованная авторизация через RADIUS-сервер (WPA/WPA2 Enterprise)
Характеристики антенны	
Усиление	2x12 дБи

Поляризация	двухполяризационная антенна
Угол излучения (горизонтальная поляризация)	60°
Угол излучения (вертикальная поляризация)	15°
КСВ	2.0:1
Импеданс	50 Ом
Коэффициент обратного излучения	> 20 дБ
Управление	
Удаленное управление	web-интерфейс, Telnet, SSH, SNMP (мониторинг), TR-069
Ограничение доступа	по паролю
Общие параметры	
Процессор	Realtek RTL8197FS 1ГГц
RAM	128 МБ
Flash	32 МБ
Питание	Passive PoE 24 В
Потребляемая мощность	не более 8 Вт
Рабочий диапазон температур	от -45 до +65°C
Относительная влажность	до 95%
Степень защиты	IP54
Габариты	80x66x282 мм
Масса	0,35 кг

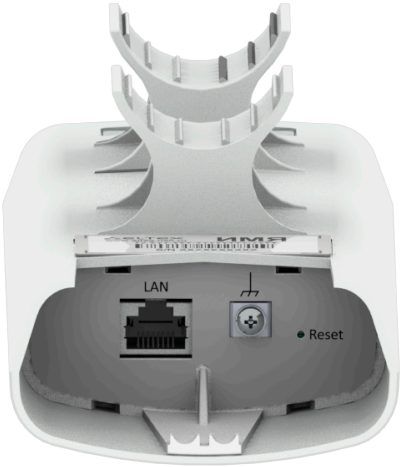
2.4 Конструктивное исполнение

Устройство WB-2P-LR5 имеет пластиковый корпус в промышленном исполнении. Размер устройства 80x66x282 мм.

Внешний вид устройства WB-2P-LR5 приведен на рисунке ниже.

Внешний вид устройства WB-2P-LR5

На нижней панели устройства WB-2P-LR5 расположены LAN-порт 10/100/1000Base-T (разъем RJ-45) для подключения к внутренней сети и питанию PoE, клемма заземления (в устройствах WB-2P-LR5 rev.C) и кнопка сброса к заводским настройкам («Reset»).



Разъемы нижней панели WB-2P-LR5

2.5 Световая индикация

Внешний вид панели индикации WB-2P-LR5 приведен на рисунке ниже.

Внешний вид панели индикации WB-2P-LR5

Текущее состояние устройства отображается при помощи индикаторов, расположенных на задней панели устройства WB-2P-LR5. Перечень индикаторов и их описание приведены в таблице 2.

Таблица 2 – Описание индикаторов задней панели

	Индикатор	Состояние индикатора	Описание
	Power – индикатор питания и статуса работы устройства	зеленый, горит постоянно	питание подключено, нормальная работа
		оранжевый, горит постоянно	устройство не получило адрес по DHCP
		красный, горит постоянно	загрузка устройства
	LAN – индикатор порта LAN-интерфейса	горит зеленым (10, 100 Мбит/с)/ оранжевым (1000 Мбит/с)	канал между LAN-интерфейсом WB- 2P-LR5 и подключенным устройством активен
		мигает	процесс пакетной передачи данных между LAN-интерфейсом WB-2P-LR5 и подключенным устройством

	Индикатор	Состояние индикатора	Описание
	WLAN – индикаторы уровня сигнала от базовой станции (RSSI)	красный, горит	Устройство подключено к базовой станции. Уровень сигнала от БС больше -94 дБм
		желтый, горит	Устройство подключено к базовой станции. Уровень сигнала от БС больше -80 дБм.
		зеленый, горит	Устройство подключено к базовой станции. Уровень сигнала от БС больше -70 дБм.
		зеленый, горит	Устройство подключено к базовой станции. Уровень сигнала от БС больше -60 дБм.
		ни один индикатор не горит	Устройство не подключено к базовой станции

2.6 Сброс к заводским настройкам

Существует два способа сброса устройства к заводским настройкам.

1. Через кнопку «Reset» на устройстве. Необходимо в загруженном состоянии устройства нажать и удерживать кнопку «Reset» (около 10-15 секунд), которая находится на нижней панели устройства, пока индикатор «Power» не замигает оранжевым цветом.
2. Через PoE-инжектор, поставляемый с устройством. Необходимо в загруженном состоянии устройства нажать и удерживать кнопку «RST» на инжекторе около 10-15 секунд (индикатор «Power» на устройстве будет мигать оранжевым цветом).

   Произойдет автоматическая перезагрузка устройства. При заводских установках будет запущен DHCP-клиент. В случае если адрес не будет получен по DHCP, то у устройства будет адрес - *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-2P-LR5 входят:

- Абонентская станция WB-2P-LR5;
- Комплект крепежа: хомуты для крепления, 2 шт.;
- Инжектор PoE 24 В;
- Патч-корд RJ-45, 5е кат., 1.5м;
- Шнур питания евровилка - C13-F-1.8м;
- Вкладыш с описанием индикации;
- Сертификат соответствия;
- Паспорт.

По запросу в комплект может входить кронштейн крепления с возможностью регулировки по горизонтали и вертикали.

3 Порядок установки

В данном разделе описаны инструкции по технике безопасности, рекомендации по установке, процедура установки и порядок включения устройства WB-2P-LR5.

3.1 Инструкции по технике безопасности

1. Не вскрывайте корпус устройства. Внутри устройства нет элементов, предназначенных для обслуживания пользователем.
2. Не производите установку данного устройства во время грозы. Есть риск удара молнией.
3. Необходимо соблюдать требования по напряжению, току и частоте, указанные в данной инструкции.
4. Перед подключением к устройству измерительных приборов и компьютера, их необходимо предварительно заземлить. Разность потенциалов между корпусами оборудования и измерительных приборов не должна превышать 1 В.
5. Перед включением устройства убедитесь в целостности кабелей и их надежном креплении к разъемам.
6. Во время монтажа устройства на высотных конструкциях следует выполнять установленные нормы и требования при высотных работах.
7. Эксплуатация устройства должна производиться инженерно-техническим персоналом, прошедшим специальную подготовку.
8. Подключать к устройству только годное к применению вспомогательное оборудование.

3.2 Рекомендации по установке

1. Рекомендуемое устанавливаемое положение: крепление на трубостойку/столб.
2. Перед установкой и включением устройства необходимо проверить устройство на наличие видимых механических повреждений. В случае наличия повреждений следует прекратить установку устройства, составить соответствующий акт и обратиться к поставщику.
3. Устройство должно быть установлено вертикально на трубостойку/столб, при этом LAN-порт должен быть направлен вниз.
4. Для обеспечения наилучшего уровня сигнала секторная антенна базовой станции должна находиться в зоне прямой видимости WB-2P-LR5. Наибольший уровень сигнала можно получить юстировкой антенны с помощью индикаторов RSSI.
5. С обратной стороны от места крепления кронштейна расположена передающая часть антенны. Именно эту плоскость следует направлять на секторную антенну базовой станции.

После юстировки убедитесь, что сигнал от станции не ниже допустимого уровня -65 ÷ -70 дБм. Возможно уменьшение данного показателя до -75 дБм, если не предполагается использование VoIP, потокового видеовещания и другого чувствительного к потерям трафика в беспроводной сети.

Размещайте устройство WB-2P-LR5 на трубостойке/столбе таким образом, чтобы оно было максимально направлено на секторную антенну базовой станции. При этом обязательно должна быть обеспечена прямая видимость до базовой станции.

3.3 Монтаж устройства WB-2P-LR5

3.3.1 Предварительная настройка

Перед установкой проведите предварительную настройку устройства (пример настройки в разделе Пример настройки). Для этого подключите питание (пункты 2-7 в разделе Порядок монтажа) и следуйте алгоритму из раздела Пример настройки. Удостоверьтесь, что абонентская станция подключается к нужной беспроводной сети: должны гореть индикаторы уровня сигнала.

3.3.2 Порядок монтажа

1. Установите устройство LAN-портом вниз на трубостойку так, как показано на рисунке ниже и закрепите его хомутами, идущими в комплекте с устройством. Соблюдайте инструкции по технике безопасности и рекомендации, приведенные в разделах Инструкция по технике безопасности и Рекомендации по установке.

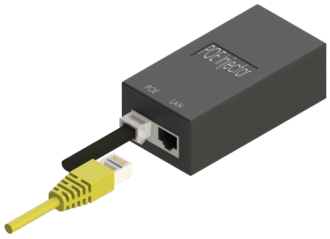
2. Снимите крышку, закрывающую LAN-порт на нижней панели устройства. Выполните заземление устройства через специальную клемму (для WB-2P-LR5 rev.C),

3.Подключите Ethernet-кабель к LAN-порту.

4. Закройте крышку нижней панели.

5. Подключите Ethernet-кабель, идущий от WB-2P-LR5, к PoE-порту инжектора.

6. Подключите Ethernet-кабель Вашей LAN-сети или ПК к LAN-порту PoE-инжектора.



7. Подключите PoE-инжектор к розетке 220 В с помощью сетевого шнура.

8. Отрегулируйте положение устройства для получения наилучшего сигнала. Уровень сигнала можно отследить с помощью индикации на задней панели.

9. Затяните хомуты.

3.4 Включение устройства

1. Включите инжектор в розетку 220 В. К LAN-порту инжектора подключите ПК.
2. Устройство WB-2P-LR5 после включения питания загрузится в течение минуты. Подключитесь с помощью браузера к web-конфигуратору WB-2P-LR5.

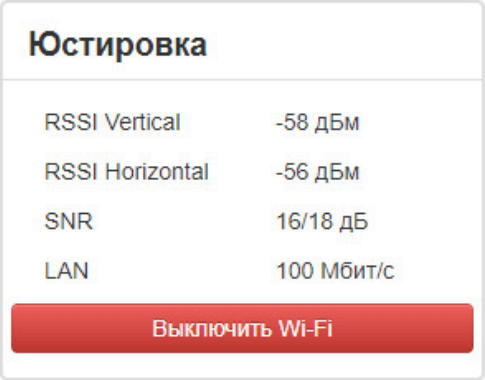
   IP-адрес по умолчанию: 192.168.1.1.
   Логин: *admin*, пароль: *password*.

3. Настройка сети описана в разделе 5.1 Меню "Сеть".

3.5 Юстировка антенны Wi-Fi

Для удобства юстировки антенны на устройстве реализован Технологический Wi-Fi (доступен только для WB-2P-LR5 rev.C). Он дает возможность подключиться беспроводным клиентом к открытому SSID «EltexWiFi» (диапазон частот 2.4 ГГц) и выполнить юстировку, используя данные мониторинга параметров соединения абонентской станции WB-2P-LR5 с базовой станцией в WEB-интерфейсе.

1. Подключите смартфон к сети Wi-Fi с SSID «EltexWiFi».
2. Задайте следующие настройки соединения на смартфоне: статический IP-адрес – **192.0.2.X** ; маска сети – **255.255.255.0** ; шлюз – **192.0.2.1** .
3. Откройте браузер и введите адрес **192.0.2.1:8080.** Откроется окно юстировки, где в реальном времени отображается уровень сигнала от станции, к которой подключена WB-2P-LR5:



4. Выполните юстировку, добившись максимального RSSI.
5. После юстировки необходимо отключить Технологический Wi-Fi.

Включение/выключение Технологического Wi-Fi выполняется через web-конфигуратор устройства, описание приведено в разделе «Подменю «Дополнительные настройки» .

4 Управление устройством через web-конфигуратор

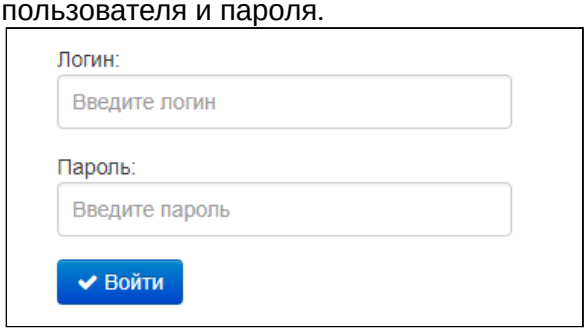
4.1 Начало работы

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.

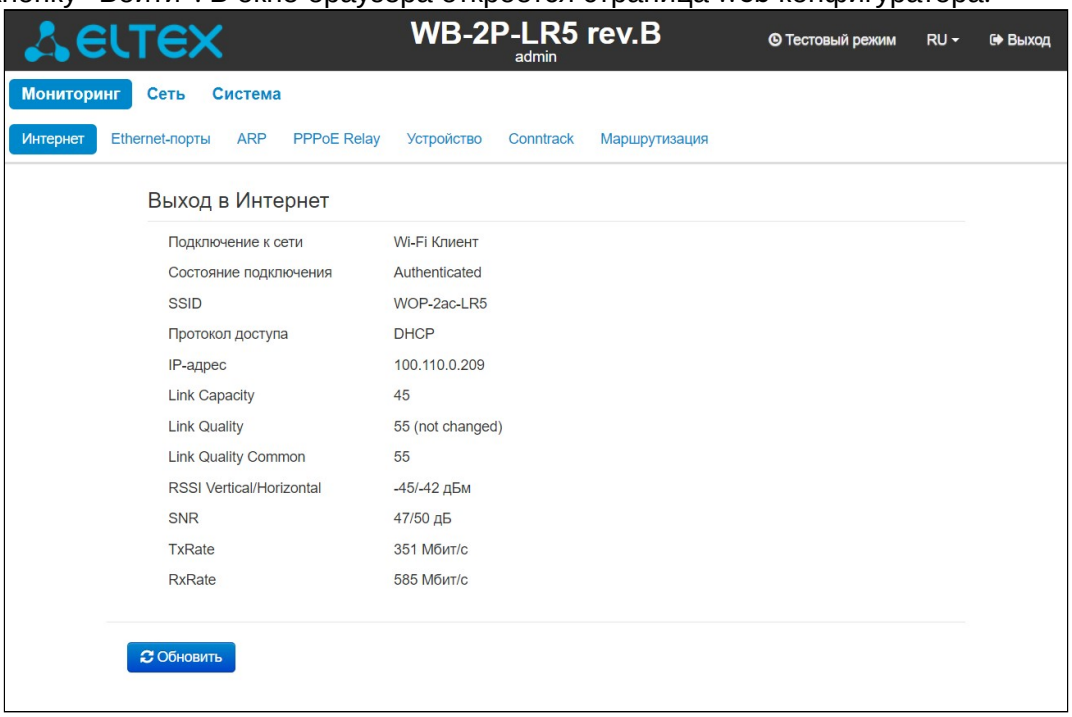
   Заводской IP-адрес устройства: 192.168.1.1, маска подсети: 255.255.255.0. По умолчанию устройство может получить адрес по DHCP.

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

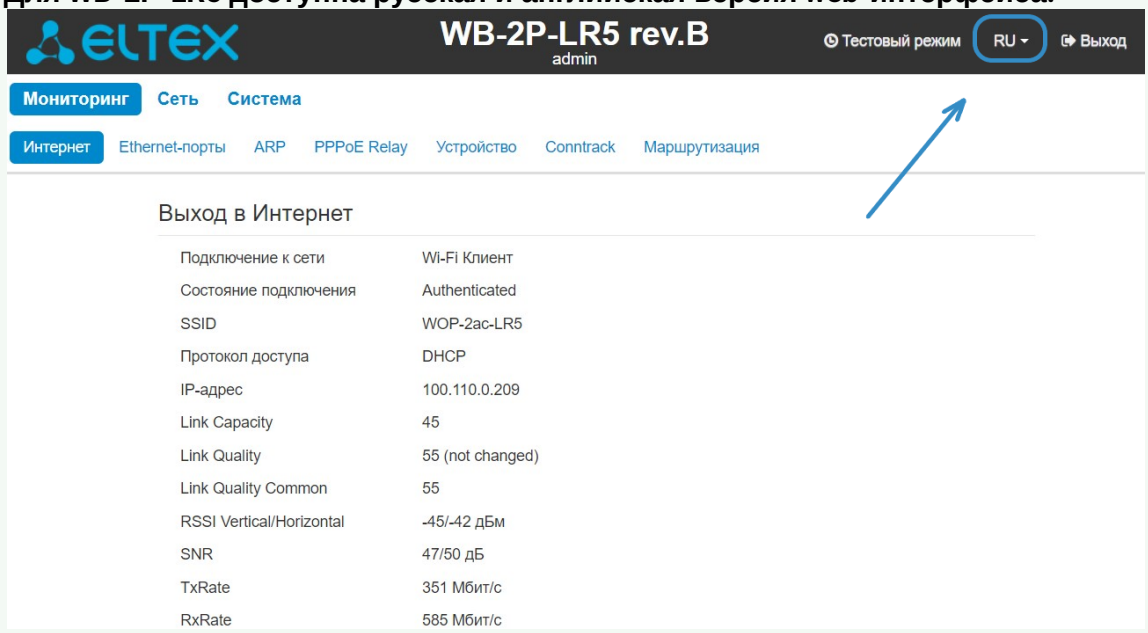


   Заводские установки: логин: *admin*, пароль: *password*.

3. Введите имя пользователя в строке «Логин» и пароль в строке «Пароль».
   Нажмите кнопку «Войти». В окне браузера откроется страница web-конфигуратора.



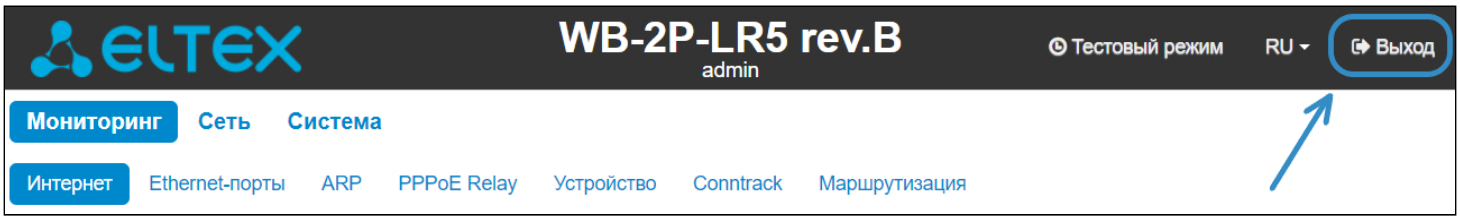
На верхней панели web-интерфейса можно переключить язык отображения информации. Для WB-2P-LR5 доступна русская и английская версия web-интерфейса.



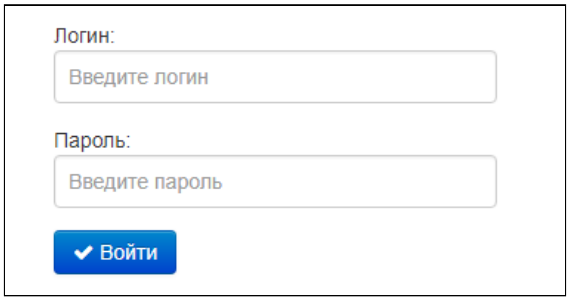
4.2 Смена пользователей

На устройстве существует два типа пользователей: **admin** и **viewer**:

- **admin** (пароль по умолчанию: **password**) имеет полный доступ к устройству: чтение и запись любых настроек, полный мониторинг состояния устройства.
- **viewer** имеет право только просматривать всю конфигурацию устройства без возможности что-либо редактировать, мониторинг состояния устройства 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 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.**

В web-интерфейсе реализована визуальная индикация текущего состояния процесса применения настроек.
Визуальная индикация текущего состояния процесса применения настроек:

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

Кнопка «Применить» в меню Применить.

2. Отмена изменений

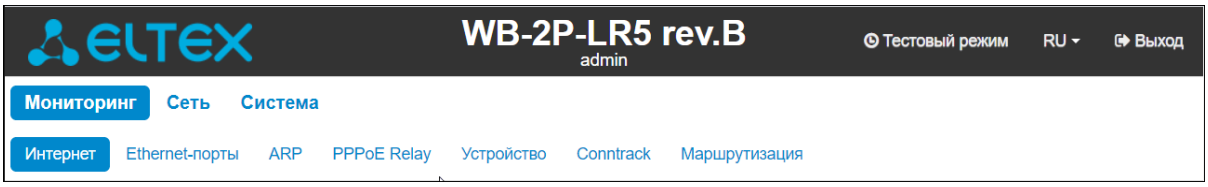
> **Отмена изменений производится только до нажатия на кнопку «Применить». При нажатии на кнопку «Применить» изменённые на странице параметры будут обновлены на текущие значения и сохранены в память устройства. После нажатия на кнопку «Применить» возврат к предыдущим настройкам будет невозможен.**

Кнопка отмены изменений имеет вид: Отмена.

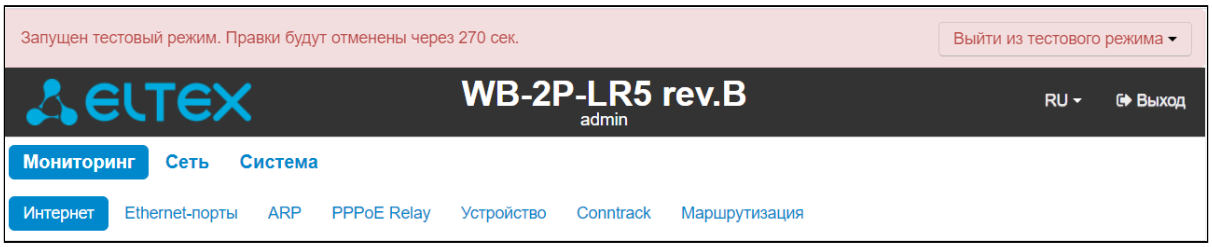
4.4 Тестовый режим

На устройстве реализован тестовый режим для пробного применения конфигурации.

Чтобы его активировать, нажмите кнопку «Тестовый режим» на верхней панели web-интерфейса.



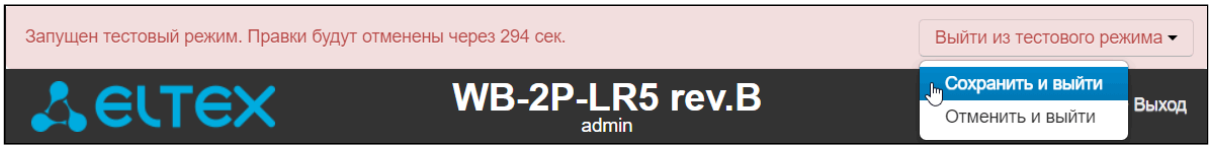
Время работы тестового режима - 300 секунд (5 минут). В течение этого времени можно перемещаться по вкладкам web-конфигуратора и производить какие-либо изменения, применяя их на каждой странице с помощью кнопки «Применить».



После проверки необходимой конфигурации нажмите кнопку «Выйти из тестового режима» и выберите нужное действие:

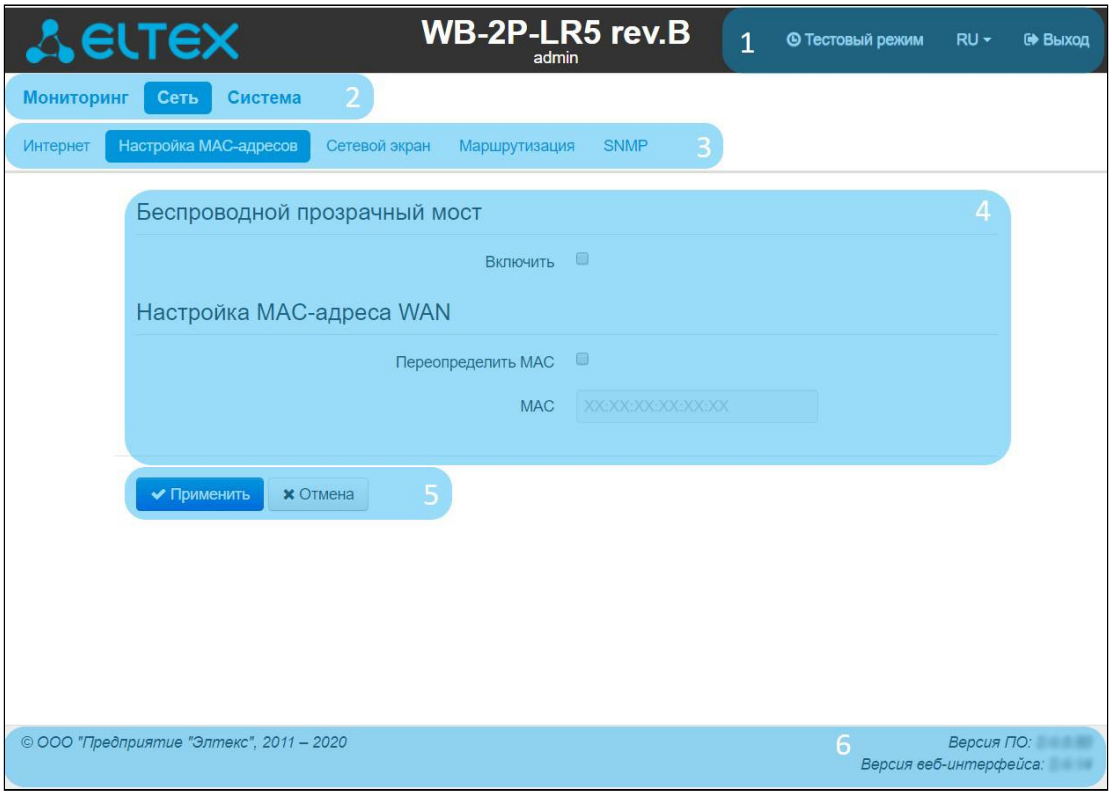
- «Сохранить и выйти» - при нажатии произойдет выход из тестового режима и сохранение в энергонезависимую память всех изменений в конфигурации, которые были сделаны и применены в этом режиме. Отменить изменения, выполненные в тестовом режиме, будет невозможно.
- «Отменить и выйти» - при нажатии произойдет выход из тестового режима и отмена всех изменений, выполненных в этом режиме. Будет восстановлена конфигурация, действующая на устройстве до активации тестового режима.

Если в течение 300 секунд администратором не будет произведен выход из тестового режима, это произойдет автоматически вместе с откатом всех изменений, которые были сделаны в данном режиме. По истечению указанного времени конфигурация восстановится, даже если в результате сделанных изменений был потерян доступ до устройства.



5 Основные элементы web-интерфейса

На рисунке ниже представлены элементы навигации web-конфигуратора.



Окно пользовательского интерфейса разделено на семь областей:

1. Имя пользователя, под которым был осуществлен вход в систему, а также кнопка завершения сеанса работы в web-интерфейсе (*выход*) под данным пользователем.
2. Вкладки меню группируют вкладки подменю по категориям: **Мониторинг, Сеть** , **IPTV(доступно только в режиме маршрутизатора), Система** .
3. Вкладки подменю служат для управления полем настроек.
4. Поле настроек устройства, которое базируется на выборе пользователя, предназначено для просмотра настроек устройства и ввода конфигурационных данных.
5. Кнопки управления конфигурацией, подробная информация приведена в разделе Применение конфигурации и отмена изменений.
6. Информационное поле, в котором отображается версия ПО, версия web-интерфейса.

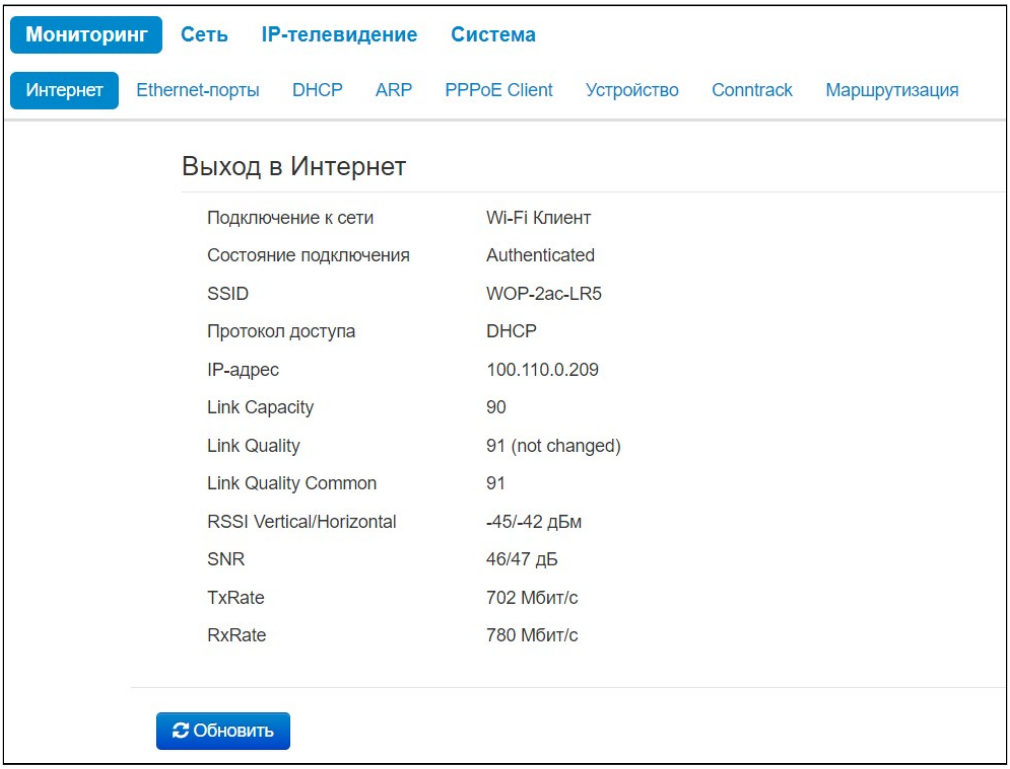
5.1 Меню «Мониторинг»

В данном меню доступен мониторинг устройства.

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

5.1.1 Подменю «Интернет»

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



Выход в Интернет

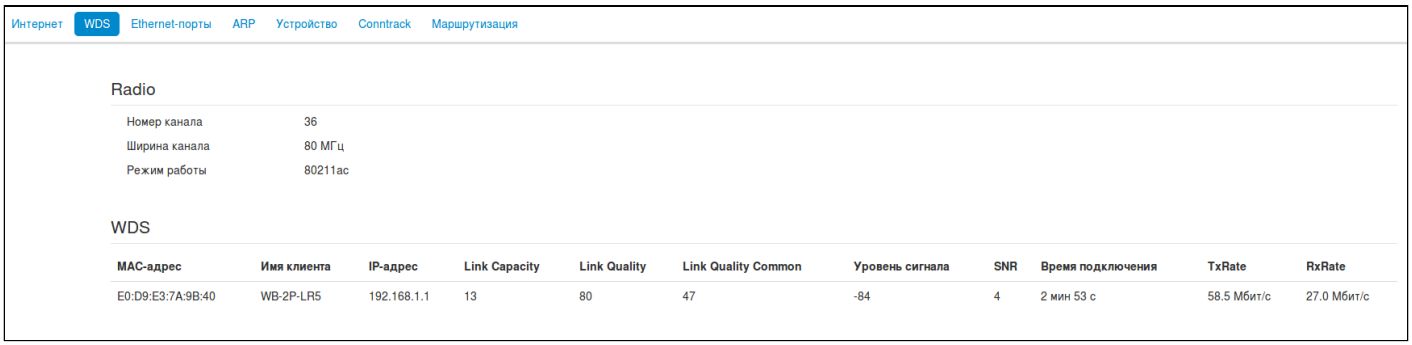
- *Подключение к сети* – показывает тип подключения к внешней сети;
- *Состояние подключения* – показывает состояние подключения к внешней сети;
- *Идентификатор сети (SSID)* – имя беспроводной сети, к которой подключено устройство;
- *Протокол доступа* – протокол, используемый для доступа к сети;
- *IP-адрес* – IP-адрес устройства во внешней сети;
- *Link Capacity* – параметр, который отображает эффективность использования устройством модуляции на передачу. Рассчитывается исходя из количества пакетов, переданных на каждой модуляции, и понижающих коэффициентов. Максимальное значение- 100% (означает, что все пакеты передаются на максимальной модуляции для максимального типа nss, поддерживаемого устройством). Минимальное значение- 2% (в случае, когда пакеты передаются на модуляции nss1mcs0 для устройства с поддержкой MIMO 3x3). Значение параметра рассчитывается за последние 10 с;
- *Link Quality* – параметр, который отображает состояние линка, рассчитанный на основании количества отправленных ретрансмитов пакетов. Максимальное значение — 100% (все переданные пакеты отправились с первой попытки), минимальное значение – 0% (ни один пакет не был успешно отправлен). Значение параметра рассчитывается за последние 10 с;
- *Link Quality Common* – параметр, который отображает состояние линка, рассчитанный на основании количества отправленных ретрансмитов пакетов. Максимальное значение — 100% (все переданные пакеты отправились с первой попытки), минимальное значение – 0% (ни один пакет не был успешно отправлен). Значение параметра рассчитывается за все время подключения;
- *RSSI Vertical/Horizontal* – уровень сигнала от базовой станции, дБм;
- *SNR* – отношение сигнал/шум, дБ;
- *TxRate* - канальная скорость передачи, Мбит/с;
- *RxRate* - канальная скорость приема, Мбит/с.

Для обновления информации на странице нажмите кнопку «Обновить».

5.1.2 Подменю «WDS»

Подменю «WDS» доступно только в режиме «Беспроводной мост»

В подменю «WDS» осуществляется просмотр настроек радиоинтерфейса и состояние Беспроводного моста.



Radio:

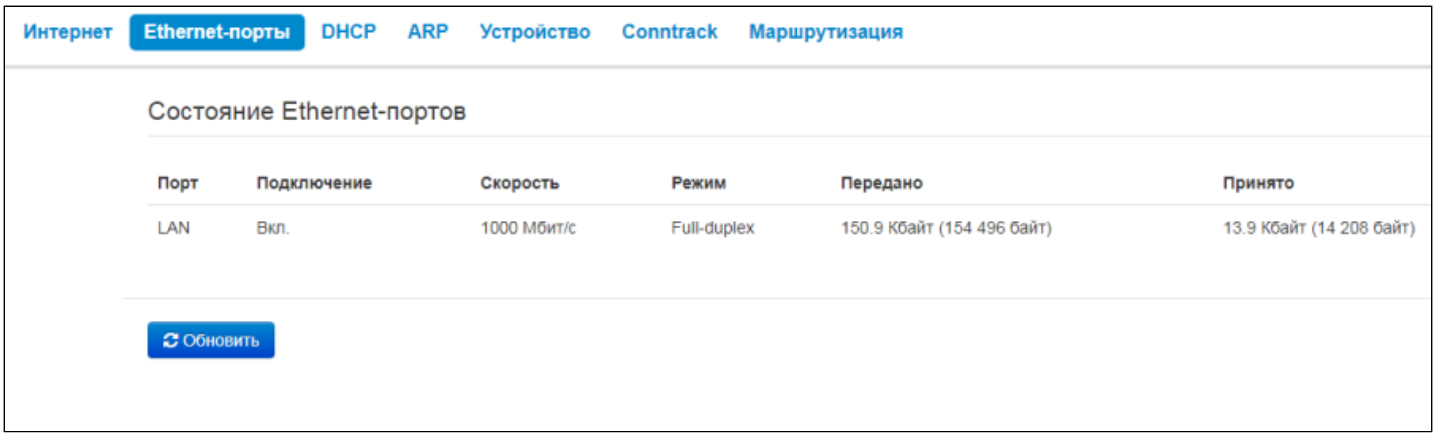
- *Номер канала* – канал, на котором установлен беспроводной мост;
- *Ширина канала* – используемая ширина канала для беспроводного моста;
- *Режим работы* – текущий режим работы радиоинтерфейса устройства.

WDS:

- *MAC-адрес* – MAC-адрес встречного устройства;
- *Имя клиента* – сетевое имя встречного устройства;
- *IP-адрес* – IP-адрес встречного устройства;
- *Link Capacity* – параметр, который отображает эффективность использования модуляции на передачу. Рассчитывается исходя из количества пакетов, переданных на каждой модуляции, и понижающих коэффициентов. Максимальное значение- 100% (все пакеты передаются на максимальной модуляции для максимального типа nss, поддерживаемого устройством). Минимальное значение- 2% (в случае, когда пакеты передаются на модуляции nss1mcs0 для устройства с поддержкой MIMO 3x3). Значение рассчитывается за последние 10 с;
- *Link Quality* – параметр, который отображает состояние линка, рассчитанный на основании количества отправленных ретрансмитов пакетов. Максимальное значение — 100% (все пакеты отправились с первой попытки), минимальное значение – 0% (ни один пакет не был успешно отправлен). Значение рассчитывается за последние 10 с;
- *Link Quality Common* – параметр, который отображает состояние линка, рассчитанный на основании количества отправленных ретрансмитов пакетов. Максимальное значение — 100% (все пакеты отправились с первой попытки), минимальное значение – 0% (ни один пакет не был успешно отправлен). Значение рассчитывается за все время подключения;
- *Уровень сигнала* – уровень принимаемого сигнала от встречного устройства, дБм;
- *SNR* – отношение сигнал/шум, дБ;
- *Время подключения* – время, в течение которого активен беспроводной мост;
- *TxRate* – канальная скорость передачи, Мбит/с;
- *RxRate* – канальная скорость приема, Мбит/с.

5.1.3 Подменю «Ethernet-порты»

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



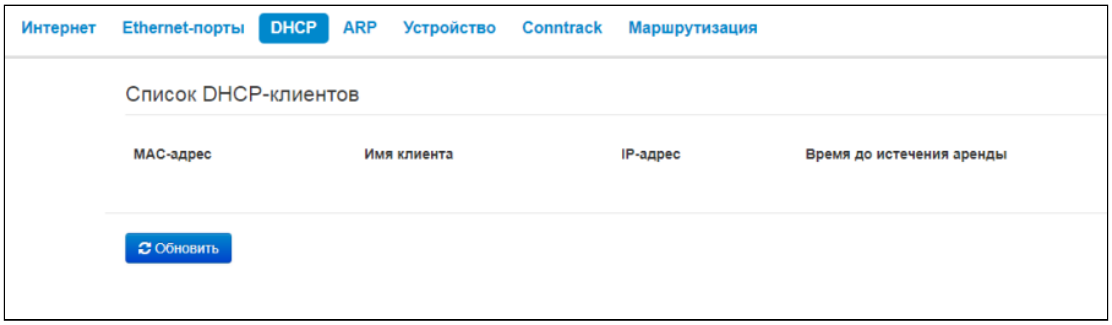
Состояние Ethernet-портов

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

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

5.1.4 Подменю «DHCP»

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



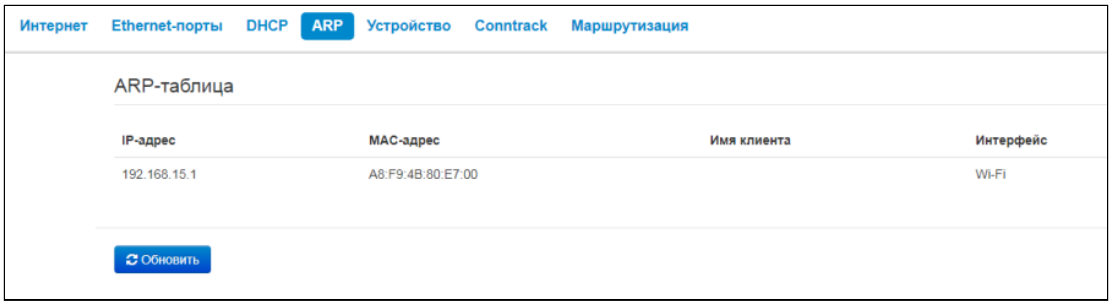
Список DHCP-клиентов

- *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».

5.1.5 Подменю «ARP»

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



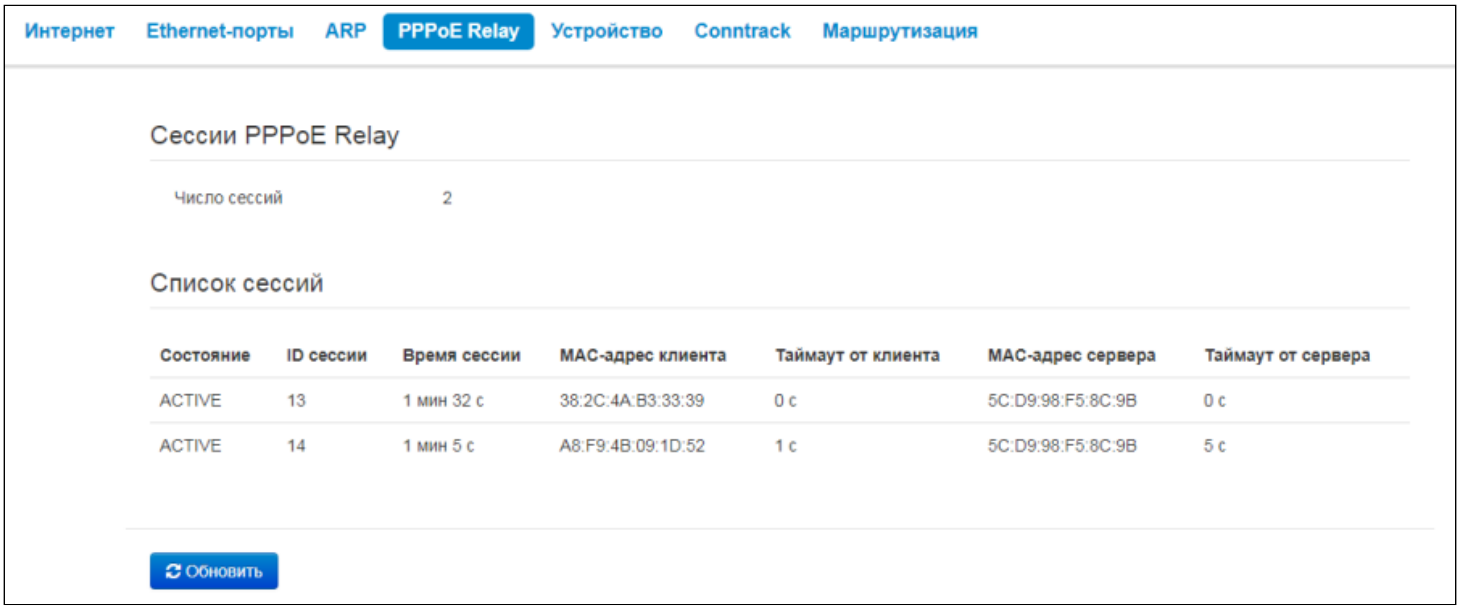
ARP-таблица

- *IP-адрес* – IP-адрес устройства;
- *MAC-адрес* – MAC-адрес устройства;
- *Имя клиента* - hostname устройства (если имеется);
- *Интерфейс* – интерфейс, со стороны которого активно устройство: LAN, Wi-Fi, Bridge .

Для получения текущей информации нажмите кнопку «Обновить».

5.1.6 Подменю «PPPoE Relay»

Подменю «PPPoE Relay» доступно только в режиме устройства «Wi-Fi Клиент» в режиме работы «Мост»



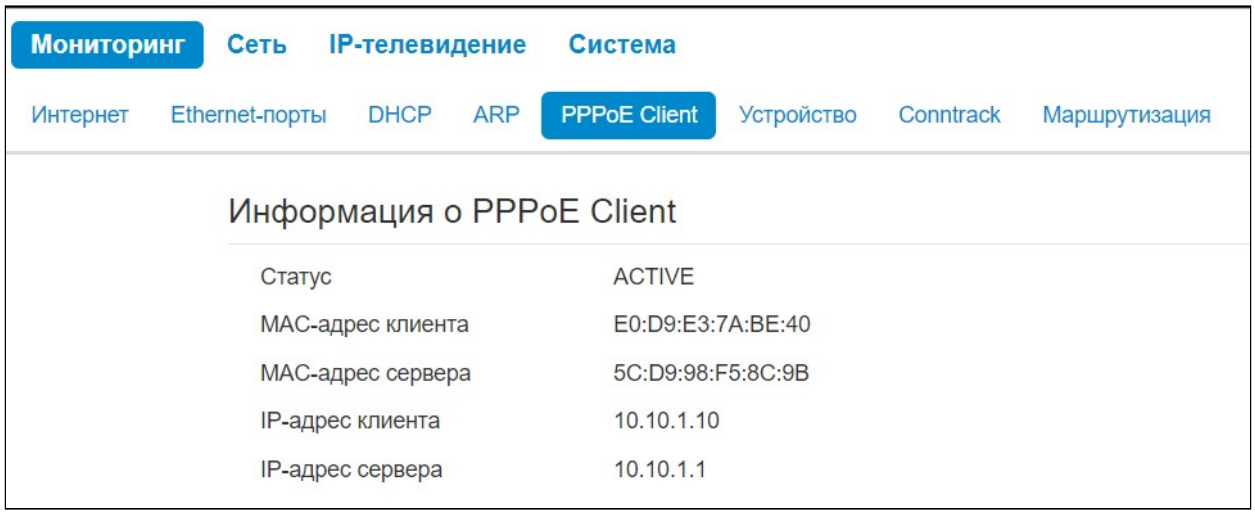
- *Число сессий* – число PPPoE-сессий, поднятых через устройство. Максимальное значение – 64.
- *Состояние* – активная либо неактивная сессия.
- *ID сессии* – номер сессии.
- *Время сессии* – аптайм сессии.
- *Таймаут от клиента* – время с момента принятия последнего пакета от клиента.
- *Таймаут от сервера* – время с момента принятия последнего пакета от сервера.

Так же можно увидеть информацию об MAC-адресе клиента и сервера.

5.1.7 Подменю «PPPoE Client»

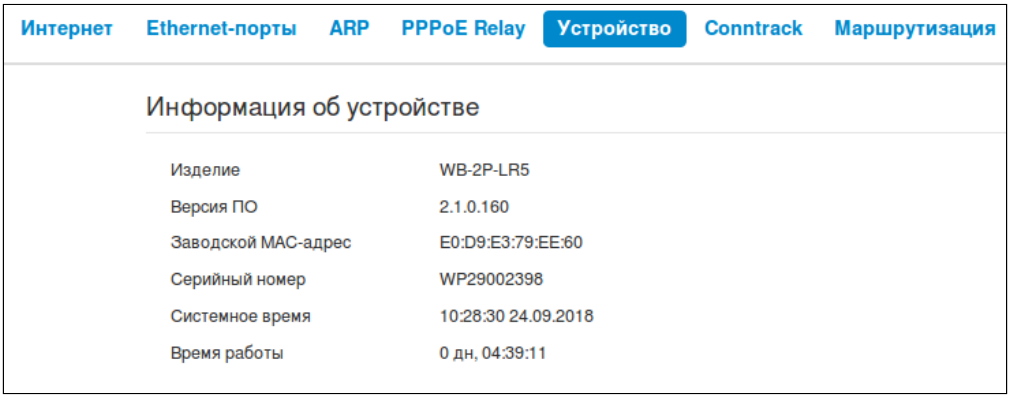
Подменю «PPPoE Client» доступно только в режиме работы «Маршрутизатор»

На странице можно увидеть информацию о MAC-адресе и IP-адресе клиента и сервера. Параметр "Статус" отображает состояние сессии - активная либо неактивная сессия.



5.1.8 Подменю «Устройство»

В подменю «Устройство» приведена общая информация об устройстве.

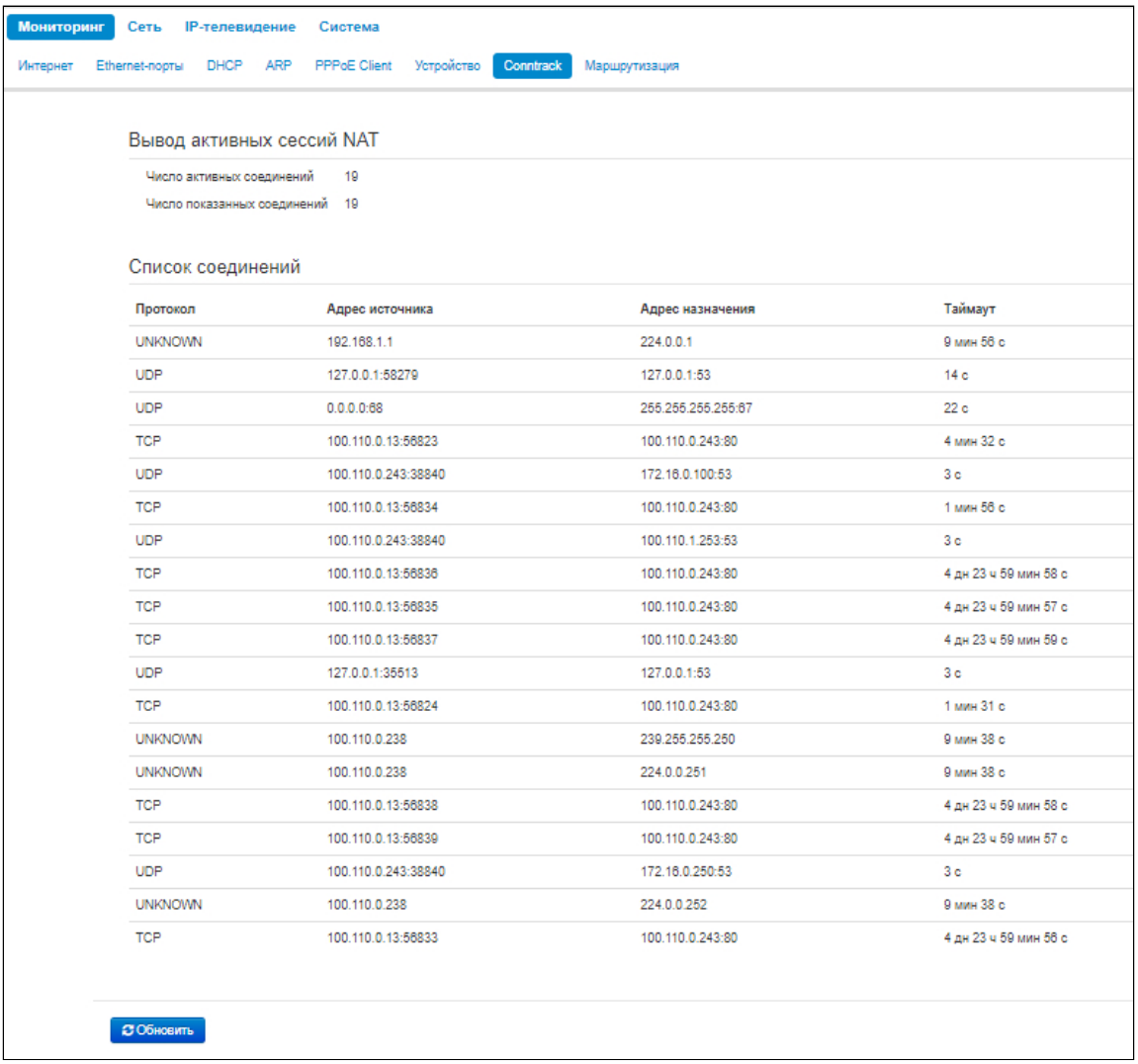


Информация об устройстве

- *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.

5.1.9 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 консоль устройства.

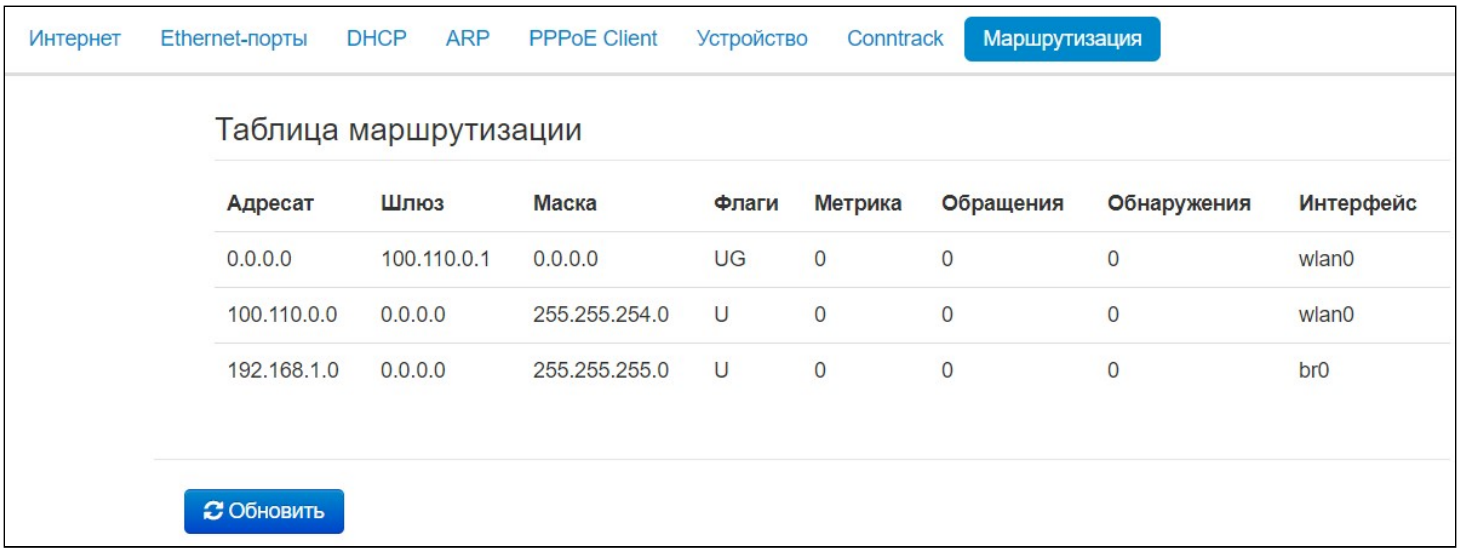
Список соединений

- *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 разрыва соединения.

Для получения текущей информации нажмите кнопку «Обновить».

5.1.10 Подменю «Маршрутизация»

В подменю «Маршрутизация» отображается таблица маршрутизации устройства.



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

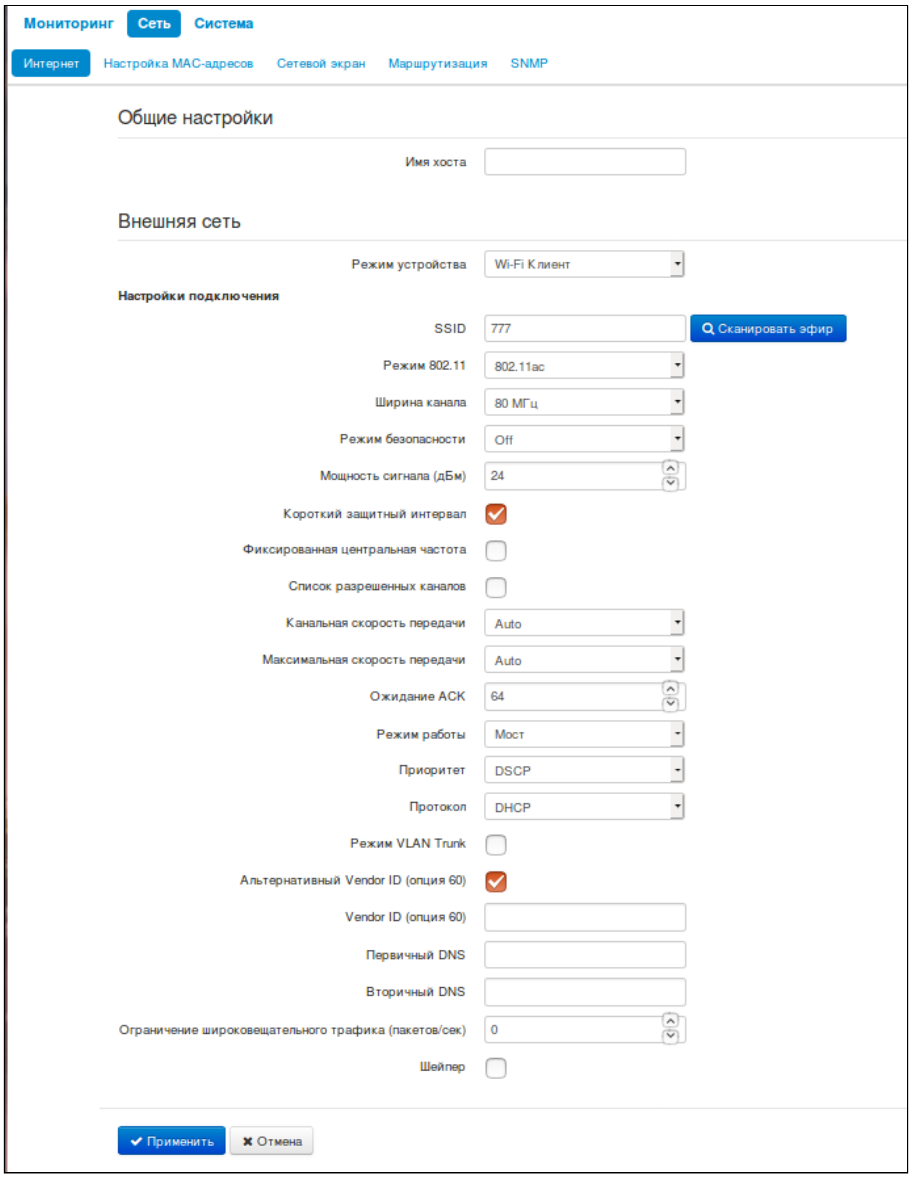
5.2 Меню «Сеть»

В меню «Сеть» выполняются основные сетевые настройки устройства.

5.2.1 Подменю «Интернет»

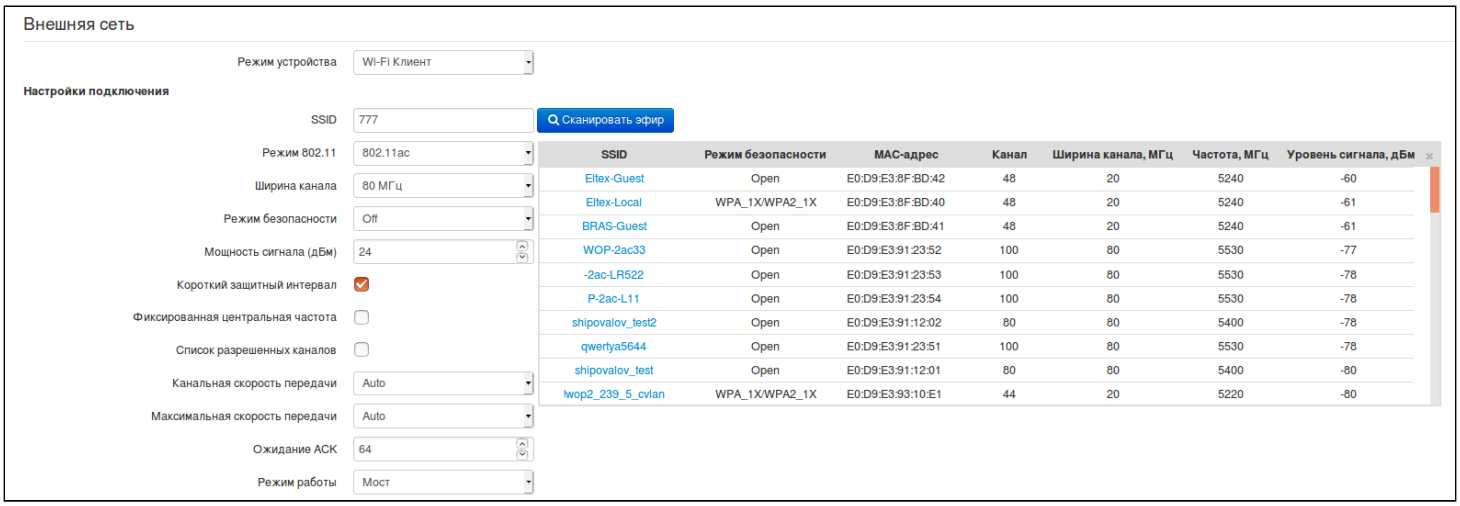
В подменю «Интернет» выполняется настройка параметров для подключения к базовой станции по Wi-Fi и выбор режима подключения устройства.

Режим устройства Wi-Fi Клиент



- *Имя хоста* – имя, назначенное сетевому устройству;
- *Режим устройства* – режим подключения устройства;
- *SSID (Идентификатор сети)* – имя беспроводной сети, используется для подключения к базовой станции. 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.

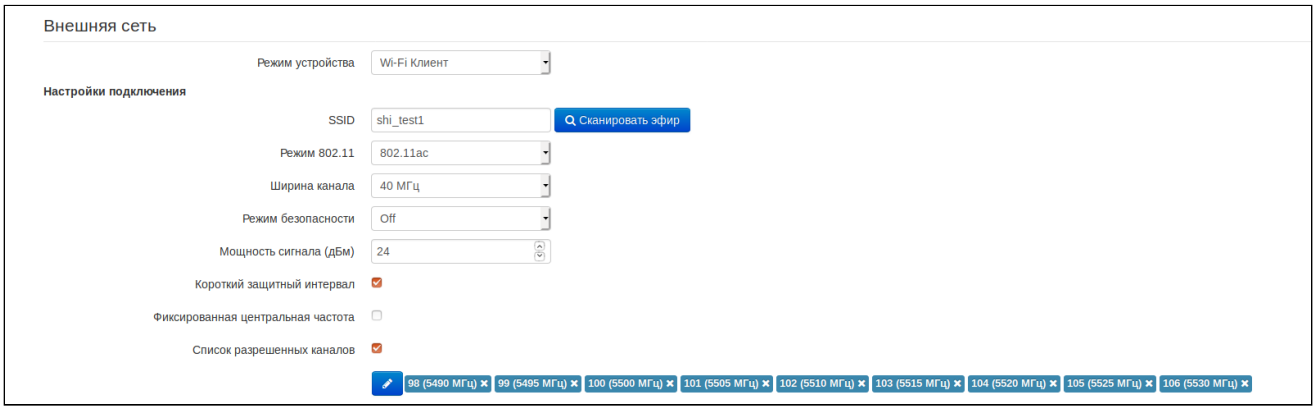
- *Сканировать эфир* – по нажатию кнопки начнется сканирование радиоэфира в заданном диапазоне. После сканирования появится список найденных точек доступа. Список будет состоять из семи столбцов: SSID, режим безопасности, MAC-адрес точки доступа, канал, ширина канала, частота, уровень сигнала. При выборе одной из найденных точек будет автоматически заполнено поле SSID, выбран соответствующий режим безопасности.



- *Режим 802.11* – выбор режима работы беспроводного интерфейса:
  - *802.11a* – данный стандарт предусматривает максимальную скорость до 54 Мбит/с;
  - *802.11n* – данный стандарт предусматривает максимальную скорость до 300 Мбит/с;
  - *802*.11ac - данный стандарт предусматривает максимальную скорость до 866.7 Мбит/с.
- *Ширина канала* – ширина полосы частот канала, на котором работает Wi-Fi клиент, принимает значения 5, 10, 20, 40 и 80 МГц. Стоит отметить, что ширина канала в 80 МГц будет работать только в стандарте 802.11ac. Если на базовой станции установлена ширина канала 5 или 10 МГц, то на абонентской станции необходимо выбрать аналогичную полосу.
- *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, ~!@#$%^&*()_-+=) и иметь длину 5 или 13 символов. Данный режим скрыт в web-интерфейсе.
  - *WPA, WPA2* – шифрование WPA и WPA2. Длина ключа составляет от 8 до 63 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:|/?.,<>"`' 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 передатчика Wi-Fi в дБм.
- *Короткий защитный интервал* – поддержка укороченного защитного интервала. Используется 400 нс защитный интервал (вместо 800 нс);
- *Фиксированная центральная частота* – при активации флага весь трафик (пакеты данных и управления) будет передаваться на указанной центральной частоте канала с заданной шириной полосы (40 или 80 МГц). Функция является проприетарной, передача ведется не по стандартам IEEE 802.11, где предполагается использование разных центральных частот для трафика данных и управления при ширине канала 40/80 МГц. При работе WB-2P-LR5 с устройствами WOP-2ac-LR5, на которых включена фиксированная центральная частота, активация на абонентской станции не требуется, т.к. происходит автоматически в момент подключения к базовой станции.
- *Список разрешенных каналов (Limit Channels)* – список частот, на которых производится сканирование эфира для подключения к базовой станции.

  Если, например, на БС выставлен канал 100L (5490-5530 МГц) с шириной полосы 40 МГц, то в списке разрешенных каналов на абонентской станции должны быть выбраны *все каналы, находящиеся в этом частотном диапазоне*: 98 - 106 канал включительно. При такой

настройке WB-2P-LR5 будет сканировать только частотный диапазон 5490 - 5530 МГц и успешно подключится к БС на канале 100L/40.



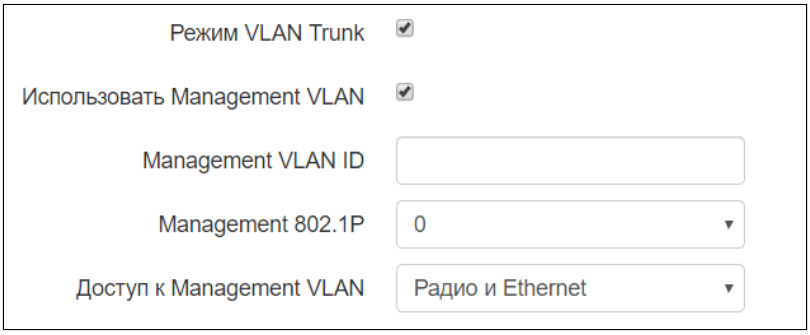
- *Канальная скорость передачи* – фиксированная скорость беспроводной передачи данных, определяемая спецификациями стандартов IEEE 802.11a/n/ac;
- *Максимальная скорость передачи* – максимальная допустимая скорость беспроводной передачи данных, определяемая спецификациями стандартов IEEE 802.11a/n/ac;
- *Ожидание ACK* – таймаут ожидания подтверждения пакета. При больших расстояниях (более 2,5 км) параметр следует увеличить, подобрав оптимальное значение;
- *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 моста между беспроводным и проводным интерфейсами устройства.
- Приоритет – выбор способа приоритизации. Определяет поле, на основании которого трафик, передающийся в радио интерфейс будет распределяться по очередям WMM:
  - *DSCP* – будет анализироваться приоритет из поля DSCP заголовка IP-пакета;
  - *802.1p* – будет анализироваться приоритет из поля CoS (Class of Service) тегированных пакетов.
- *Протокол* – определяет режим работы интерфейса, через который будет осуществляться подключение 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* – установка маски подсети WAN-интерфейса устройства в сети провайдера;
    - *Шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
  - *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. До тех пор, пока адрес по DHCP не получен, доступ к устройству будет по адресу из поля IP-адрес.
    - *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-2P-LR5][HW:1.2][SN:WP29000038] [WAN:E0:D9:E3:75:55:60] [LAN:E0:D9:E3:75:55:60][VERSION:2.0.0.161]

- *PPPoE (доступно в режиме маршрутизатора)* – 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;
  - *Размер MTU* – максимальный размер пакета, который может быть передан через PPP-сессию без фрагментации;
  - *Имя сервиса* – имя сервиса провайдера. Значение тега Service-Name в сообщении PADI для инициализации PPPoE-соединения (использование данной опции не является обязательным, этот параметр настраивается только по требованию провайдера);
  - *Вторичный доступ* – определяет способ установки IP-адреса на интерфейсе для доступа к устройству, если не используется VLAN управления.
    - *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;
    - *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* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
      - *Маска подсети* – установка маски подсети WAN-интерфейса устройства в сети провайдера;
      - *Шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
      - *Первичный DNS, Вторичный DNS* – IP-адреса DNS-серверов;
- *Отключить трансляцию адресов отправителя (доступно в режиме маршрутизатора)* – опция позволяет отключить трансляцию адресов отправителей (masquerade);
- *Ограничение широковещательного трафика (пакетов/сек)* – устанавливает ограничение на передачу широковещательного трафика во внешнюю сеть Wi-Fi;
- *Шейпер* – ограничение скорости в направлениях Downlink и Uplink. Максимальное ограничение 200 Мбит/с.

VLAN Trunk в режиме моста

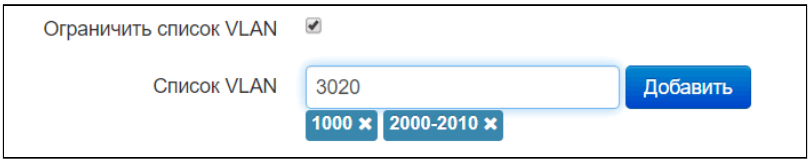
- *Режим VLAN trunk* – при установленном флаге активируется транковый порт. Устройство будет прозрачно передавать все VLAN (с учетом опции "Ограничить список VLAN"), которые получены от базовой станции, на проводных клиентов и в обратном направлении. При этом прохождение нетегированного трафика зависит от опции "Прозрачный режим";
  - *Использовать Management VLAN* – при установленном флаге включается доступ к устройству через VLAN управления:



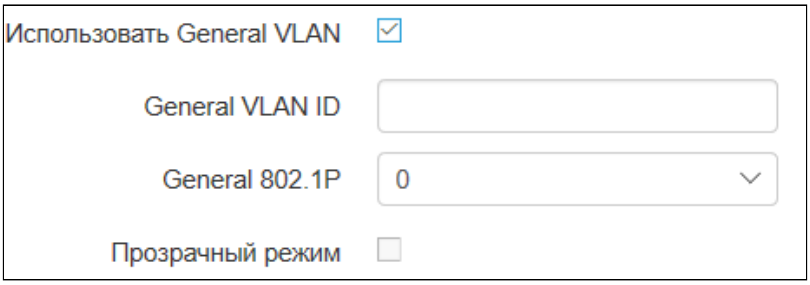
    - *Management VLAN ID* – идентификатор VLAN, используемый для доступа к устройству;
    - *Management 802.1P* – признак 802.1P (другое название CoS – Class of Service), устанавливаемый на пакеты, исходящие с данного интерфейса. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет);
    - *Доступ к Management VLAN* – ограничение доступа к сети управления. Возможные значения:
      - *Радио и Ethernet* – доступ в сеть управления возможен со стороны радиоинтерфейса и интерфейса Ethernet;
      - *Радио* – доступ в сеть управления возможен только со стороны радиоинтерфейса.

При включении флага «Использовать Management VLAN» и неправильной настройке Management VLAN возможна потеря доступа к устройству. При подключении через Ethernet у стройство будет доступно по адресу 192.0.3.1.

  - *Ограничить список VLAN* – при установленном флаге устройство в режиме VLAN trunk будет пропускать только ограниченное количество VLAN, которые указаны в поле "Список VLAN":
    - *Список VLAN* – содержит идентификаторы VLAN, которые разрешены для передачи. Принимает значения от 1 до 4094, возможно указать диапазон, например "2000-2010".

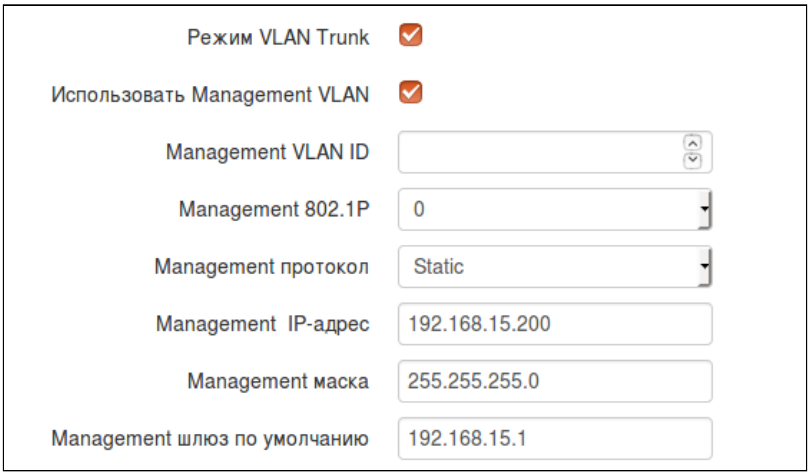


  - *Использовать General VLAN* – при установленном флаге с одного VLAN, указанного в поле *General VLAN ID* будет сниматься метка и трафик этого VLAN пройдет на клиента без тега. При прохождении трафика в о братную сторону на нетегированный трафик будет навешиваться метка General VLAN ID:
    - *General VLAN ID* – идентификатор VLAN;
    - *General 802.1P* – признак 802.1P (другое название CoS – Class of Service), устанавливаемый на пакеты, исходящие с данного интерфейса. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).
  - Прозрачный режим - при установленном флаге устройство будет пропускать нетегированный трафик в режиме VLAN trunk.

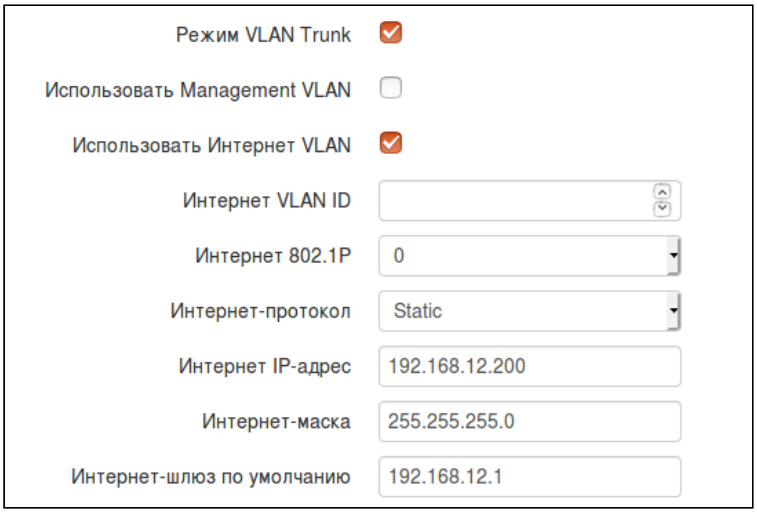


VLAN Trunk в режиме маршрутизатора

- *Режим VLAN Trunk* – при установленном флаге активируется транковый порт для возможности использования Management VLAN и Internet VLAN:

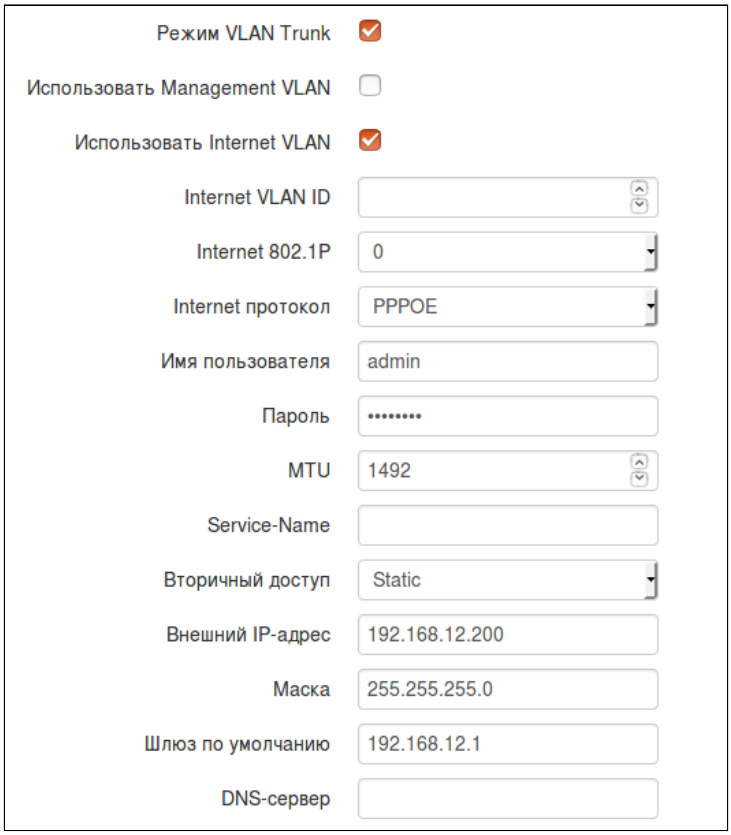


- *Использовать Management VLAN* – при установленном флаге включается доступ к устройству через VLAN управления :
  - *Management VLAN ID* – идентификатор VLAN, используемый для доступа к устройству;
  - *Management 802.1P* – признак 802.1P (другое название CoS – Class of Service), устанавливаемый на пакеты, исходящие с данного интерфейса. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).
  - *Management-протокол* – определяет режим работы интерфейса управления.
    - *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.
    - *Static* – режим работы, при котором IP-адрес и все необходимые параметры на интерфейс назначаются статически. При выборе типа «Static» для редактирования станут доступны следующие параметры:
      - *Management IP-адрес* – установка IP-адреса интерфейса устройства в сети управления;
      - *Management маска подсети* – установка маски подсети интерфейса устройства в сети управления;
      - *Management шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;



- *Использовать Internet VLAN* – при установленном флаге включается поддержка VLAN , для передачи пользовательского трафика.
  - *Internet VLAN ID* – идентификатор VLAN;
  - *Internet 802.1P* – признак 802.1P (другое название CoS – Class of Service), устанавливаемый на пакеты, исходящие с данного интерфейса. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет).
  - *Internet протокол* – выбор режима работы интерфейса устройства, используемого для передачи пользовательского трафика в отдельном VLAN.
    - *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.
    - *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:
      - *Internet IP-адрес* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
      - *Internet маска подсети* – установка маски подсети WAN-интерфейса устройства в сети провайдера;
      - *Internet шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации.

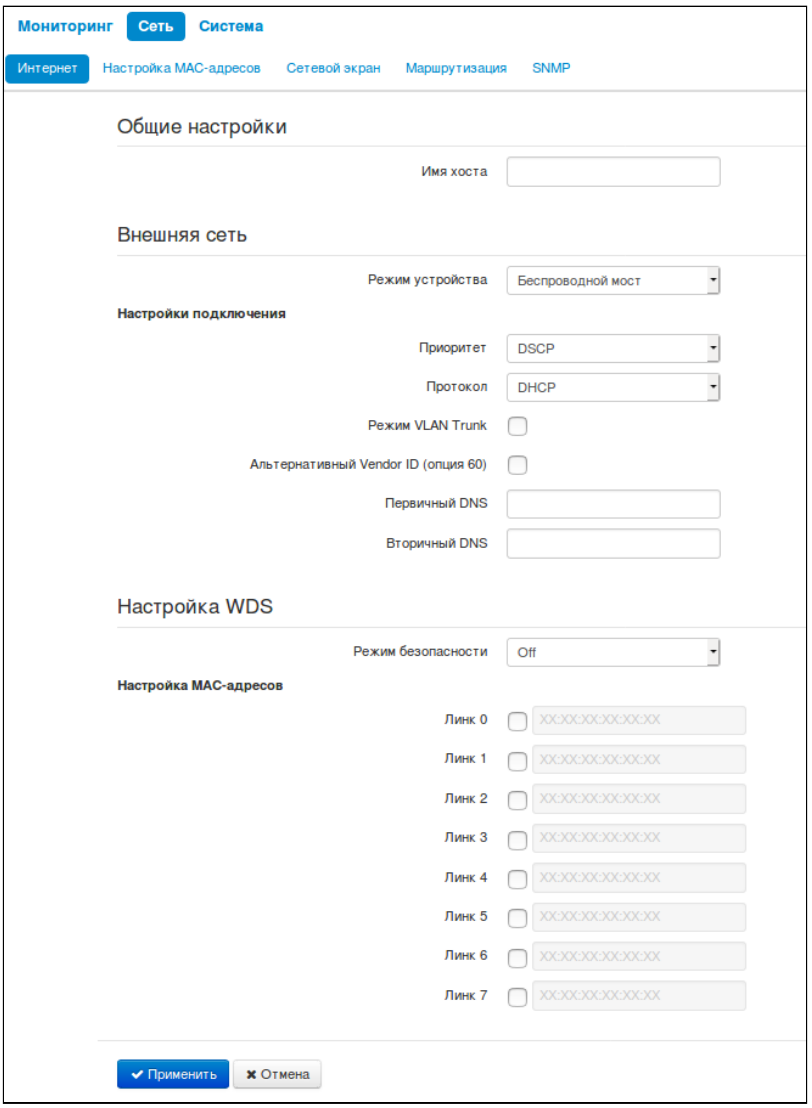
Если в качестве Internet протокола выбран *PPPoE,* то появляется возможность задать настройки вторичного доступа:



- *Вторичный доступ* – определяет способ установки IP-адреса на интерфейсе для доступа к устройству, если не используется VLAN управления.
  - *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.
  - *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* – установка IP-адреса WAN-интерфейса устройства в сети провайдера;
    - *Маска подсети* – установка маски подсети WAN-интерфейса устройства в сети провайдера;
    - *Ш люз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
    - *DNS-сервер* – адрес сервера доменных имён (используются для определения IP-адреса устройства по его доменному имени).

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.

Режим устройства Беспроводной мост

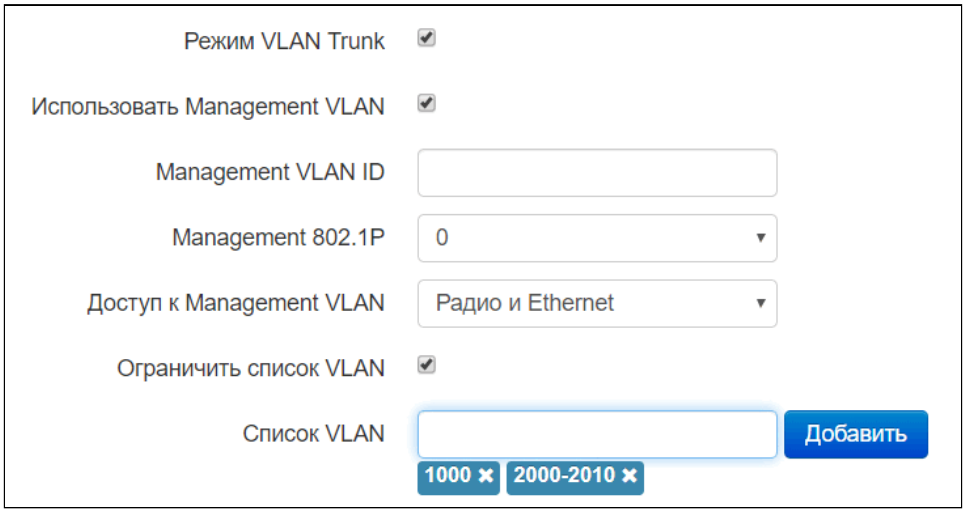


Внешняя сеть

- *Имя хоста* – имя, назначенное сетевому устройству;
- *Режим устройства* – режим подключения устройства;
- Приоритет – выбор способа приоритизации. Определяет поле, на основании которого трафик, передающийся в радио интерфейс будет распределяться по очередям WMM:
  - *DSCP* – будет анализироваться приоритет из поля DSCP заголовка IP-пакета;
  - *802.1p* – будет анализироваться приоритет из поля CoS (Class of Service) тегированных пакетов.
- *Протокол* – определяет режим работы интерфейса, через который будет осуществляться подключение 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* – установка маски подсети WAN-интерфейса устройства в сети провайдера;
    - *Шлюз по умолчанию* – адрес, на который отправляется пакет, если для него не найден маршрут в таблице маршрутизации;
  - *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. До тех пор, пока адрес по DHCP не получен, доступ к устройству будет по адресу из поля IP-адрес.

- *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-2P-LR5][HW:1.2][SN:WP29000038] [WAN:E0:D9:E3:75:55:60] [LAN:E0:D9:E3:75:55:60][VERSION:2.0.0.161]

- *Первичный DNS, Вторичный DNS* – IP-адреса DNS-серверов;
- *Режим VLAN trunk* – при установленном флаге активируется транковый порт с возможностью использования Management VLAN:
  - *Использовать Management VLAN* – при установленном флаге включается доступ к устройству через VLAN управления:
    - *Management VLAN ID* – идентификатор VLAN, используемый для доступа к устройству;
    - *Management 802.1P* – признак 802.1P (другое название CoS – Class of Service), устанавливаемый на пакеты, исходящие с данного интерфейса. Принимает значения от 0 (низший приоритет) до 7 (наивысший приоритет);
    - *Доступ к Management VLAN* – ограничение доступа к сети управления. Возможные значения:
      - *Радио и Ethernet* – доступ в сеть управления возможен со стороны радиоинтерфейса и интерфейса Ethernet;
      - *Радио* – доступ в сеть управления возможен только со стороны радиоинтерфейса.
  - *Ограничить список VLAN* – при установленном флаге устройство в режиме VLAN trunk будет пропускать только ограниченное количество VLAN, которые указаны в поле "Список VLAN":
    - *Список VLAN* – содержит идентификаторы VLAN, которые разрешены для передачи. Принимает значения от 1 до 4094, возможно указать диапазон, например "2000-2010".



Настройка WDS

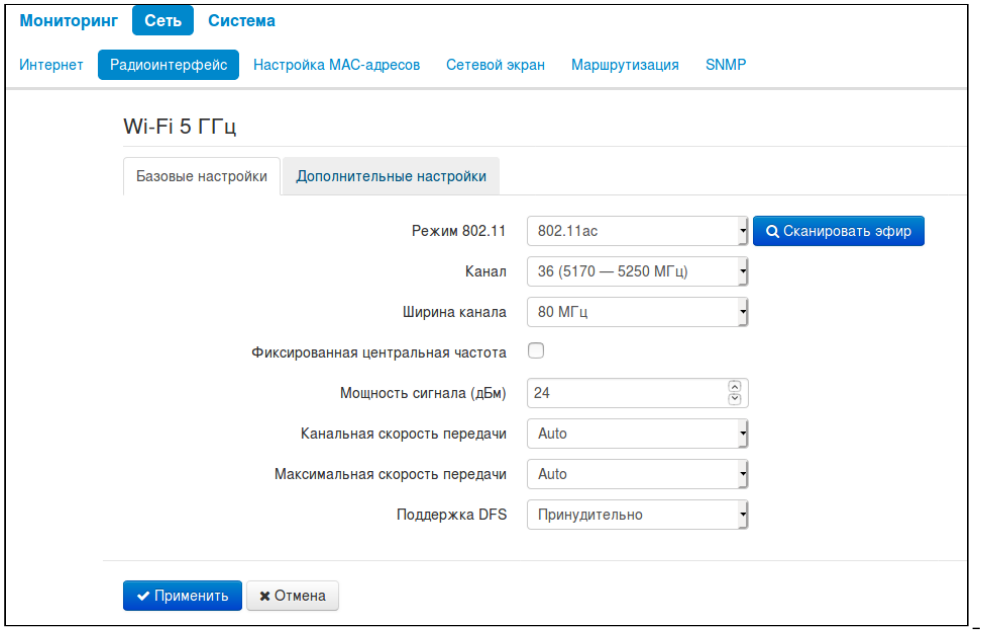
- *Режим безопасности* – выбор режима безопасности беспроводного моста:
  - *Off* – отключено шифрование беспроводной сети, низкий уровень безопасности;
  - *WPA2* – аутентификация WPA2. Длина ключа составляет от 8 до 11 символов. Разрешается использовать только символы: a-z, A-Z, 0-9, ~!@#$%^&*()_-+=;:|/?.,<>"`' или пробел.
- *Линк X (где X=0..7)* – включение линков беспроводного моста. В соответствующем поле необходимо вписать MAC-адрес встречного устройства, до которого настраивается беспроводной мост.

5.2.2 Подменю «Радиоинтерфейс»

Подменю «Радиоинтерфейс» доступно только в режиме «Беспроводной мост».

В подменю «Радиоинтерфейс» осуществляются настройки радиоинтерфейса для организации беспроводного моста.

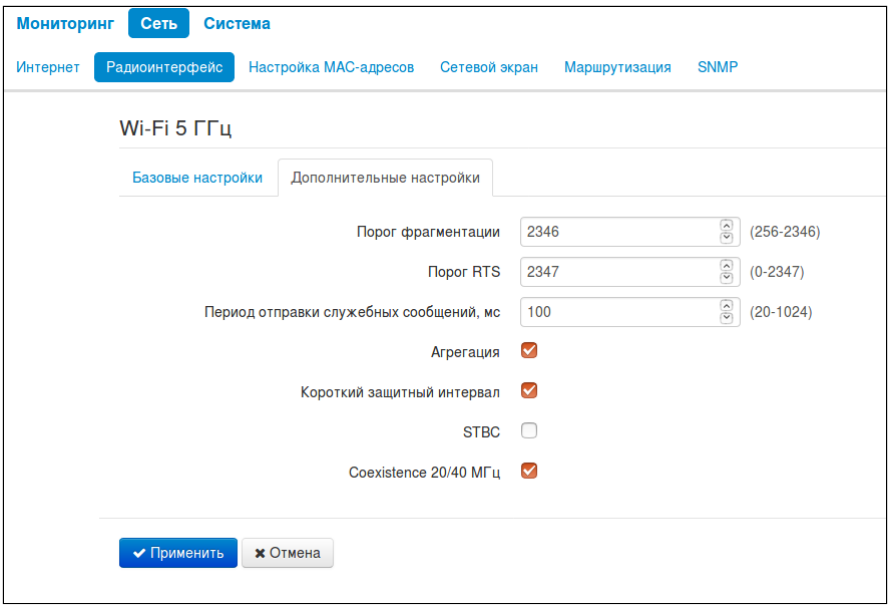
Базовые настройки:



- *Сканировать эфир* – по нажатию кнопки начнется сканирование радиоэфира в заданном диапазоне. После сканирования появится список найденных точек доступа. Список будет состоять из семи столбцов: SSID точки доступа, режим безопасности, MAC-адрес точки доступа, канал, ширина канала, частота, уровень сигнала.
- *Режим* – режим работы радиоинтерфейса согласно стандартам:
  - *802.11a* – данный стандарт предусматривает максимальную скорость 54 Мбит/с;
  - *802.11n* – данный стандарт предусматривает максимальную скорость 300 Мбит/с;
  - *802*.11ac – данный стандарт предусматривает максимальную скорость 866,7 Мбит/с.
- *Канал* – выбор канала передачи данных;
- *Ширина канала* – ширина полосы частот канала, на котором работает радиоинтерфейс устройства, принимает значения 5, 10, 20, 40 и 80 МГц, в зависимости от выбранного режима работы радиоинтерфейса;
- *Фиксированная центральная частота* – при активации флага весь трафик (пакеты данных и управления) будет передаваться на указанной центральной частоте канала с заданной шириной полосы (40 или 80 МГц). Функция является проприетарной, передача ведется не по стандартам IEEE 802.11, где предполагается использование разных центральных частот для трафика данных и управления при ширине канала 40/80 МГц;
- *Мощность сигнала, дБм* – регулировка мощности сигнала передатчика Wi-Fi в дБм;

- *Канальная скорость передачи* – фиксированная скорость беспроводной передачи данных, определяемая спецификациями стандартов IEEE 802.11a/n/ac;
- *Максимальная скорость передачи* – максимальная допустимая скорость беспроводной передачи данных, определяемая спецификациями стандартов IEEE 802.11a/n/ac;
- *Поддержка DFS* – механизм динамического выбора частоты. Требует от беспроводных устройств сканировать радиоэфир и избегать использования каналов, совпадающих с каналами, на которых работают радиолокационные системы в 5 ГГц диапазоне:
  - Выключено – механизм выключен. DFS-каналы не доступны для выбора;
  - Включено – механизм включен;
  - Принудительно – механизм выключен. DFS-каналы доступны для выбора.

Дополнительные настройки:



- *Порог фрагментации* – порог фрагментации фрейма, в байтах. Принимает значения 256-2346, по умолчанию – 2346.
- *Порог RTS* – число байт, через которое посылается запрос на передачу (Request to Send). Уменьшение данного значения может улучшить работу точки доступа при большом количестве подключенных клиентов, однако это уменьшает общую пропускную способность беспроводной сети. Принимает значения 0-2347, по умолчанию – 2347.
- *Период отправки служебных сообщений* – период посылки маячковых фреймов. Фреймы передаются для обнаружения точки доступа в эфире, принимает значения 20-2000 мс, по умолчанию - 100 мс.
- *Агрегация* – включение поддержки AMPDU/AMSDU.
- *Короткий защитный интервал* – поддержка укороченного защитного интервала. При передаче данных используется 400 нс защитный интервал (вместо 800 нс).
- *STBC* – метод пространственно-временного блочного кодирования, направленный на повышение надежности передачи данных. При установленном флаге устройство передает один поток данных через несколько антенн. Если флаг не установлен, устройство не передает один и тот же поток данных через несколько антенн.
- Coexistence 20/40 МГц – режим автоматической смены ширины канала при загруженном радиоэфире.

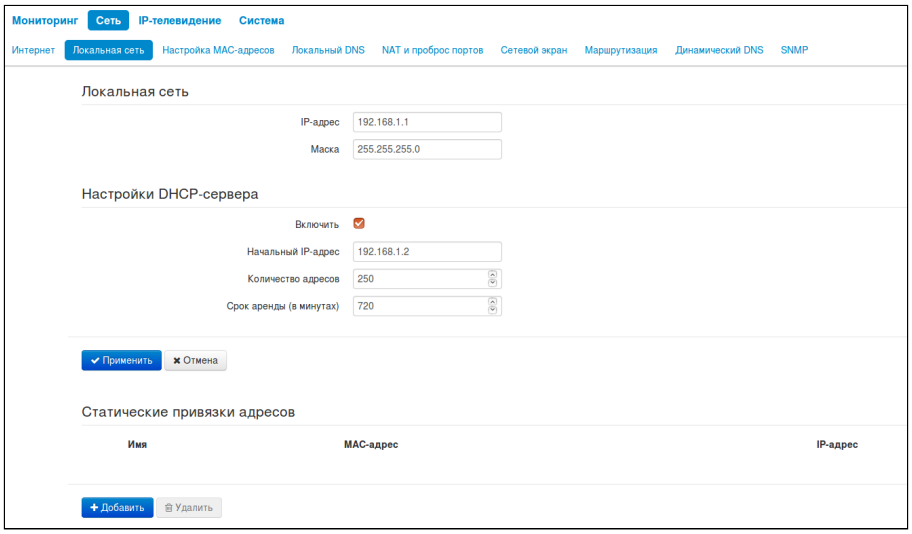
Для работы беспроводного моста необходимо, чтобы настройки радиоинтерфейса были идентичны на всех устройствах.

5.2.3 Подменю «Локальная сеть»

Подменю «Локальная сеть» доступно только в режиме «Маршрутизатор».

В подменю «Локальная сеть» выполняются настройки локальной сети, DHCP-сервера, устанавливаются статические привязки адресов.

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



Локальная сеть:

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

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 (в минутах)* – установка максимального времени использования подключенным устройством IP-адреса, назначенного DHCP-сервером, в минутах.

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 пула DHCP на адрес из другой подсети по отношению к подсети интерфейса LAN – происходит автоматическая установка пула в соответствии с заданной локальной подсетью.

Статические привязки адресов

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

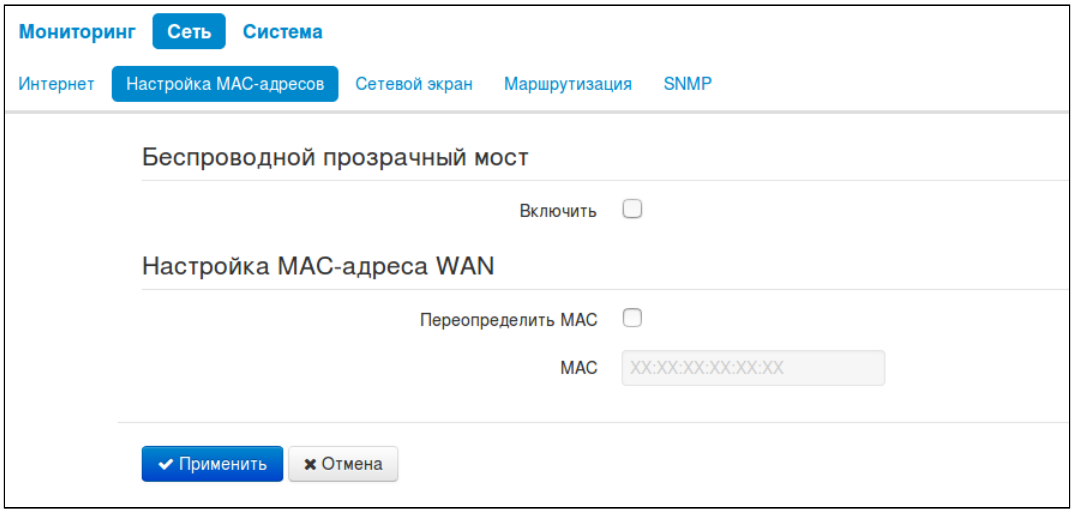
- *Имя* – название привязки;
- *MAC-адрес* – установка статического MAC-адреса. Задается в формате XX:XX:XX:XX:XX:XX;
- *IP-адрес* – установка статического IP-адреса для указанного MAC-адреса.

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»*.

5.2.4 Подменю «Настройка MAC-адресов»

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



Беспроводной прозрачный мост

> **Для режима работы Wi-Fi клиента «Мост» доступна настройка «Беспроводной прозрачный мост».**

При включении функции «Беспроводной прозрачный мост» WB-2P-LR5 не будет подменять клиентские MAC-адреса из LAN-сети на свой MAC-адрес. Ограничение – 15 MAC-адресов без подмены, при превышении ограничения клиентские MAC-адреса будут подменяться. На базовой станции в разделе подключенных клиентов, кроме MAC-адреса абонентской станции, будут отображены MAC-адреса клиентских устройств из LAN-сети.

Настройка MAC-адреса WAN

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

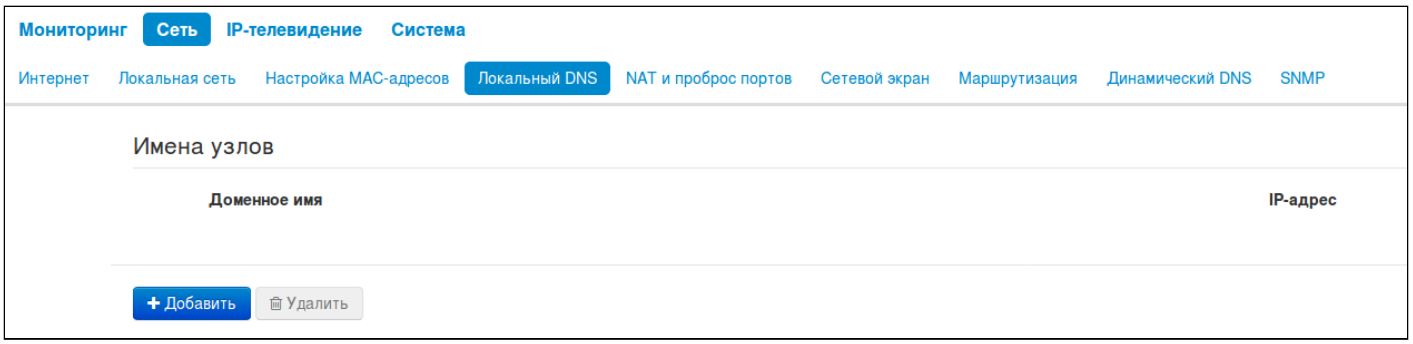
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.2.5 Подменю «Локальный DNS»

Подменю «Локальный DNS» доступно только в режиме «Маршрутизатор».

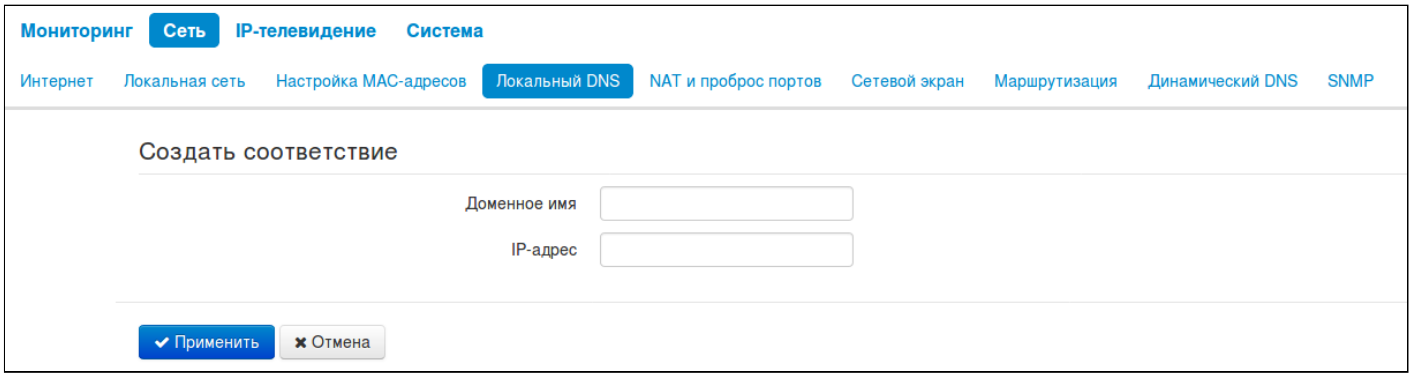
В подменю «Локальный DNS» производится конфигурирование локального DNS-сервера устройства путем добавления в базу пар IP-адрес – доменное имя.

Локальный DNS позволяет получить IP-адрес устройства по его доменному имени (хосту) в случае отсутствия сервера DNS в сегменте сети. 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:



В

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

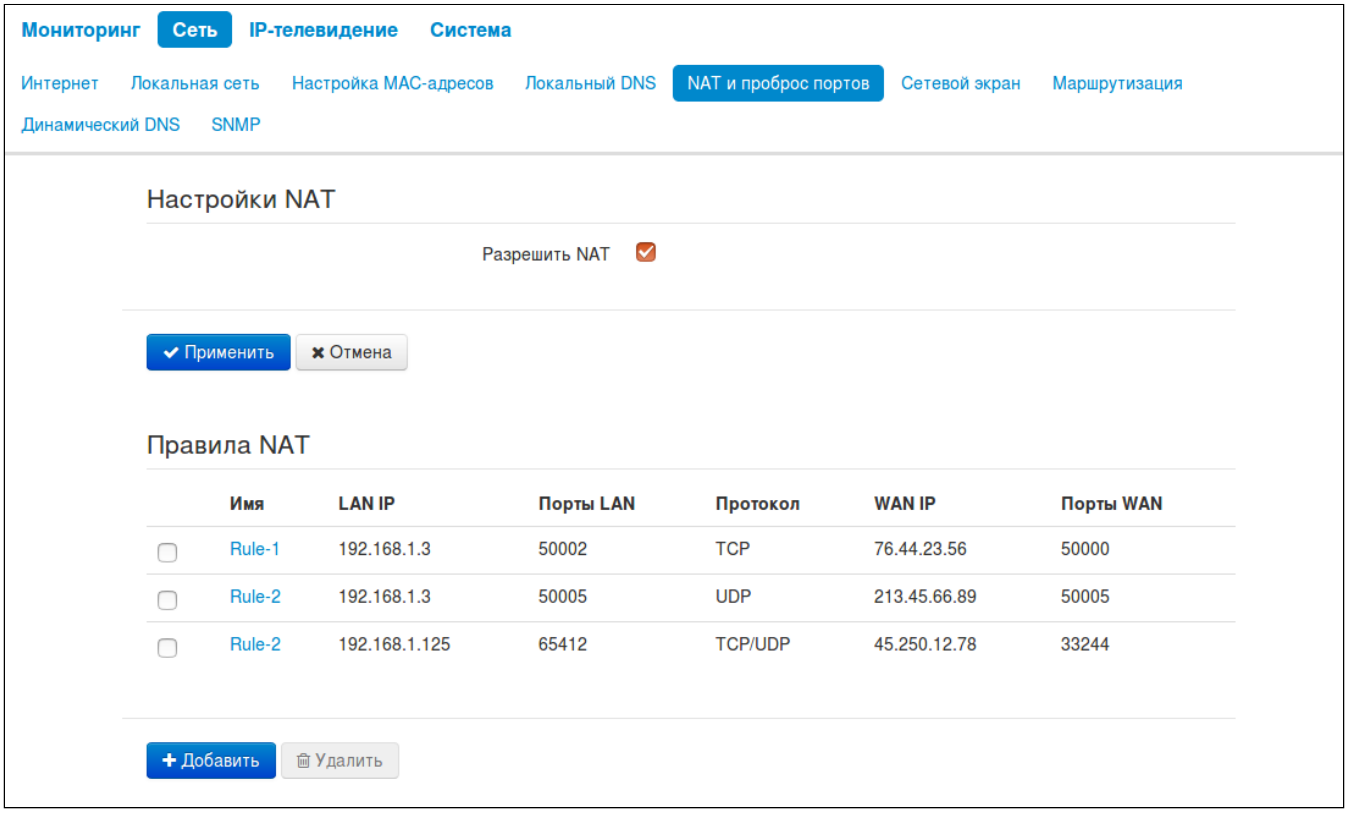
Нажмите кнопку *«Применить»* для создания соответствия IP-адрес – доменное имя. Для отмены изменений нажмите кнопку *«Отмена»*. Для удаления записи из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку *«Удалить»*.

5.2.6 Подменю «NAT и проброс портов»

Подменю «NAT и проброс портов» доступно только в режиме «Маршрутизатор».

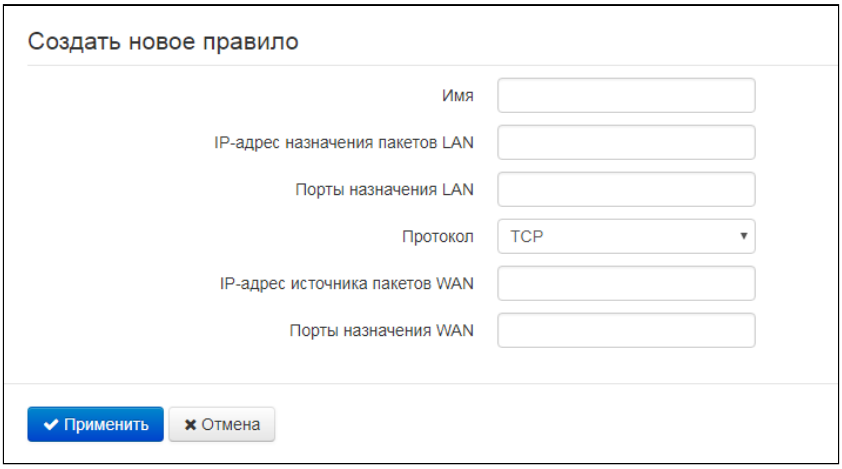
В подменю «NAT и проброс портов» выполняется настройка проброса портов (ports forwarding) из WAN-интерфейса в LAN-интерфейс.

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



Настройка правила NAT

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



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

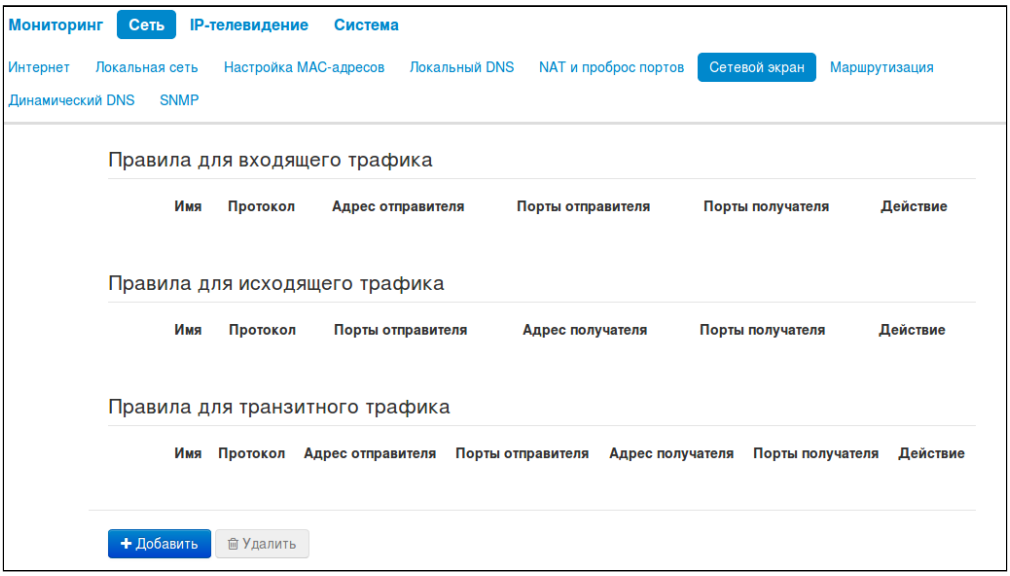
Правило проброса портов работает следующим образом. У пакета, приходящего на адрес WAN-интерфейса устройства по протоколу *«Протокол»* на порт из диапазона *«Порты назначения WAN»* и имеющего адрес источника *«IP-адрес источника пакетов WAN»* (если это параметр оставить пустым – адрес источника не анализируется),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

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

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

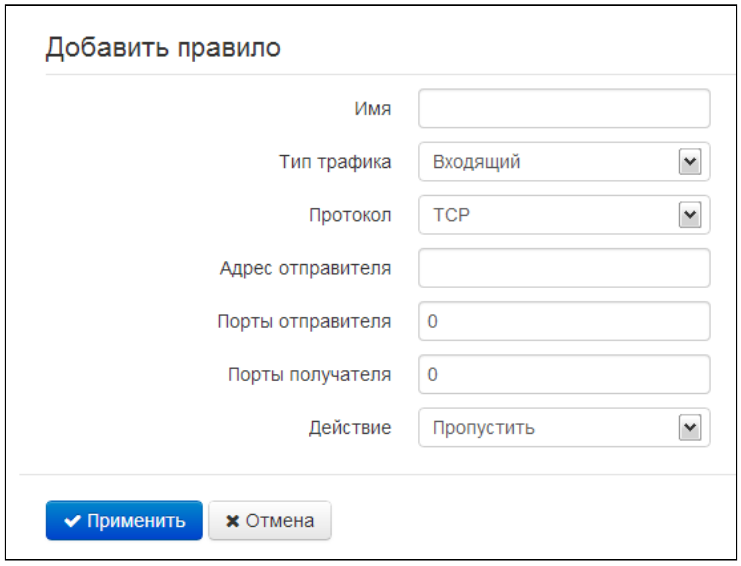
5.2.7 Подменю «Сетевой экран»

В подменю *«Сетевой экран»* устанавливаются правила прохождения входящего, исходящего и транзитного трафика. Имеется возможность ограничивать прохождение трафика разного типа (входящий, исходящий, транзитный) в зависимости от протокола, IP-адресов источника и назначения, TCP/UDP-портов источника и назначения (для 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;
- *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 один 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 один порт, либо через "-" диапазон портов); для указания всех портов введите диапазон «0-65535»;.

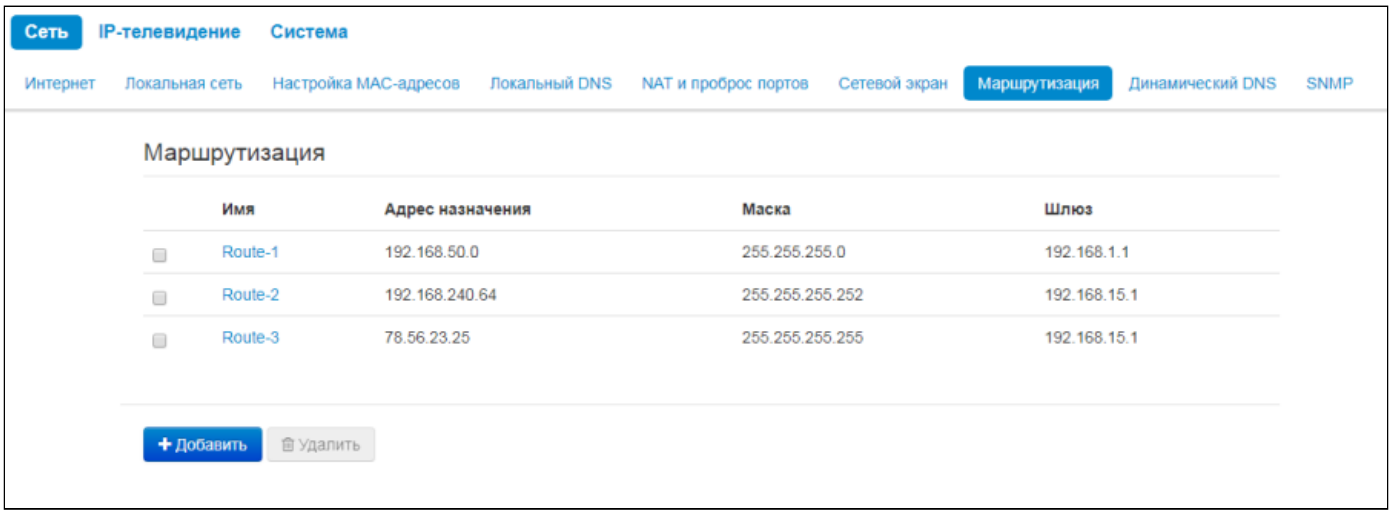
При выборе протокола ICMP для редактирования будут доступны настройки:

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

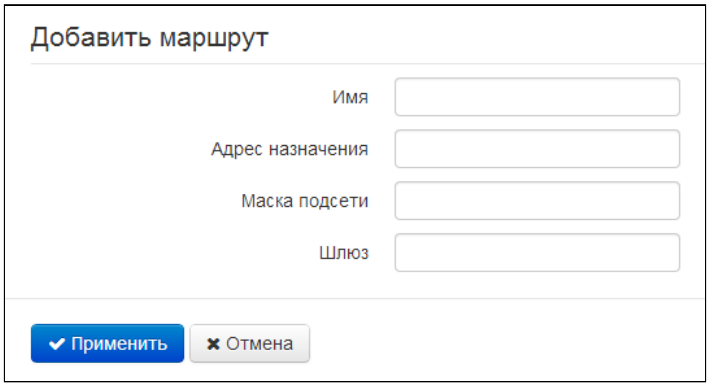
Нажмите кнопку «Применить» для добавления нового правила. Для отмены изменений нажмите кнопку «Отмена». Для удаления записи из списка необходимо установить флаг напротив соответствующей записи и нажать на кнопку «Удалить».

5.2.8 Подменю «Маршрутизация»

В подменю «Маршрутизация» устанавливаются статические маршруты.



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



- *Имя* – название маршрута.
- *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»*.

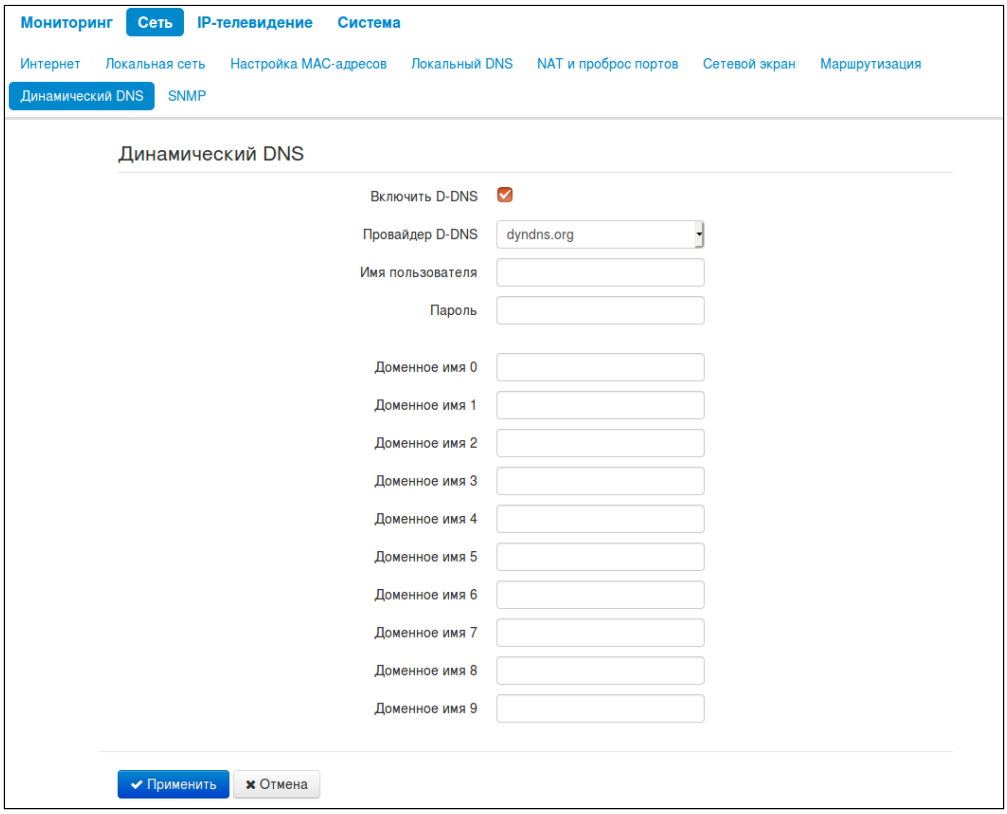
5.2.9 Подменю «Динамический DNS»

Подменю «Динамический DNS» доступно только в режиме «Маршрутизатор».

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.

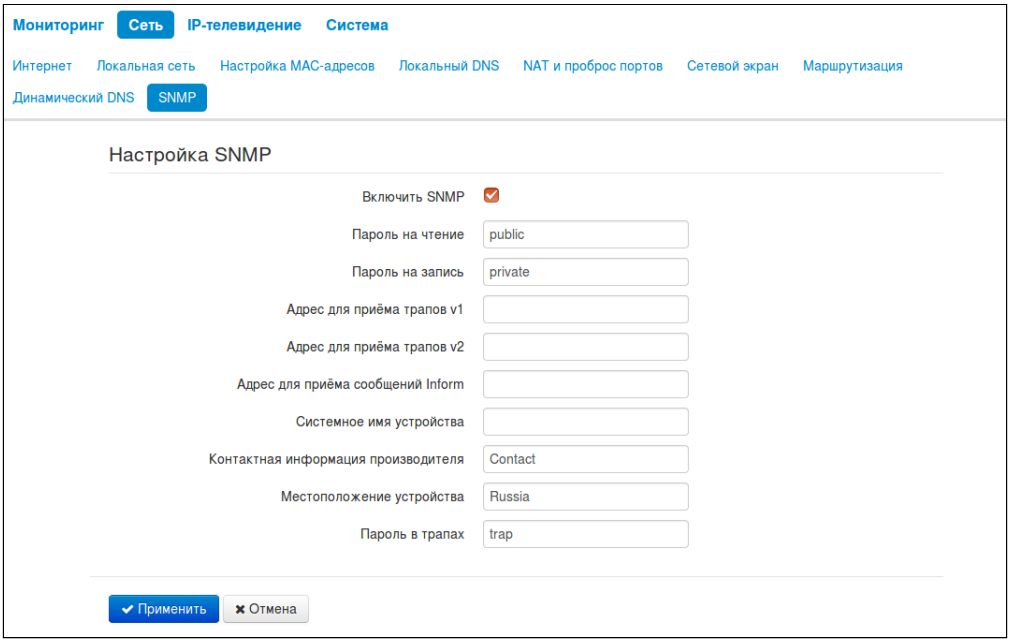


- *Включить D-DNS* – при установленном флаге сервис D-DNS активен и для редактирования доступны следующие настройки:
  - *Провайдер D-DNS* – название провайдера D-DNS – выберите одного провайдера из списка доступных;
  - *Имя пользователя* – имя пользователя для доступа к учетной записи сервиса D-DNS;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

5.2.10 Подменю «SNMP»

Программное обеспечение *WB-2P-LR5* 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.



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

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

- eltexLtd.1.164.1 – мониторинг параметров WB-2P-LR5
- eltexLtd.1.166.1 – мониторинг параметров WB-2P-LR5 rev.B
- eltexLtd.1.167.1 – мониторинг параметров WB-2P-LR5 rev.C

где eltexLtd – 1.3.6.1.4.1.35265 - идентификатор предприятия ЭЛТЕКС.

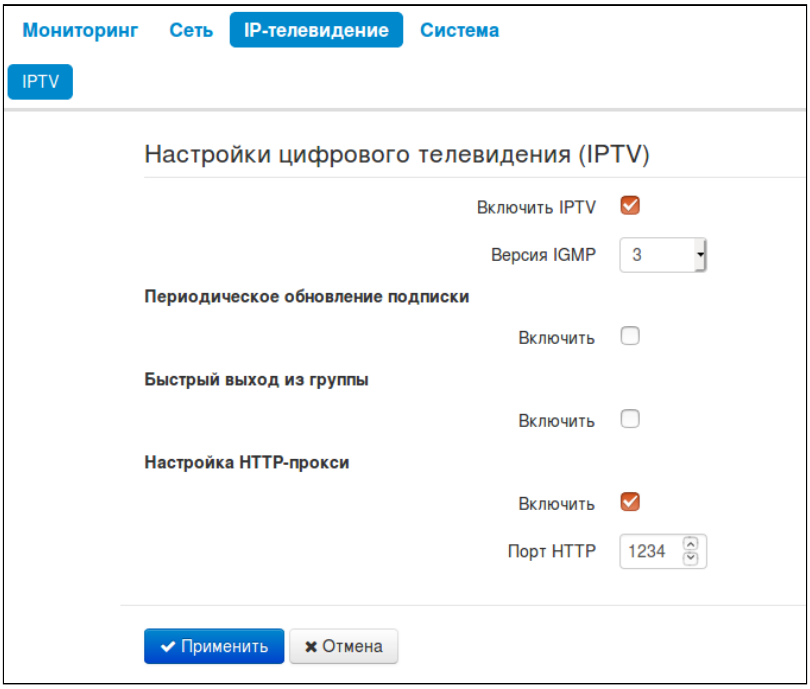
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку «Применить». Для отмены изменений нажмите кнопку «Отмена».

5.3 Меню «IP-телевидение»

Меню доступно только в режиме работы «Маршрутизатор»

5.3.1 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;
- *Версия IGMP* – версия протокола IGMP для отправки IGMP-сообщений с WAN-интерфейса (сообщений активации или деактивации подписки на каналы IP-телевидения). Поддерживаются версии 2 и 3.

Периодическое обновление подписки

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

Быстрый выход из группы

- *Включить* – при включенной опции происходит быстрый выход из мультикастовой группы. Данную функцию не рекомендуется включать, если используется более одного приемника мультикастового трафика.

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 устройство имеет на LAN-интерфейсе адрес 192.168.0.1, для порта прокси-сервера выбрано значение 1234, и необходимо воспроизвести канал 227.50.50.100, транслирующийся на UDP-порт 9000 – для программы VLC адрес потока нужно задать в виде: http://@192.168.0.1:1234/udp/227.50.50.100:9000.

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

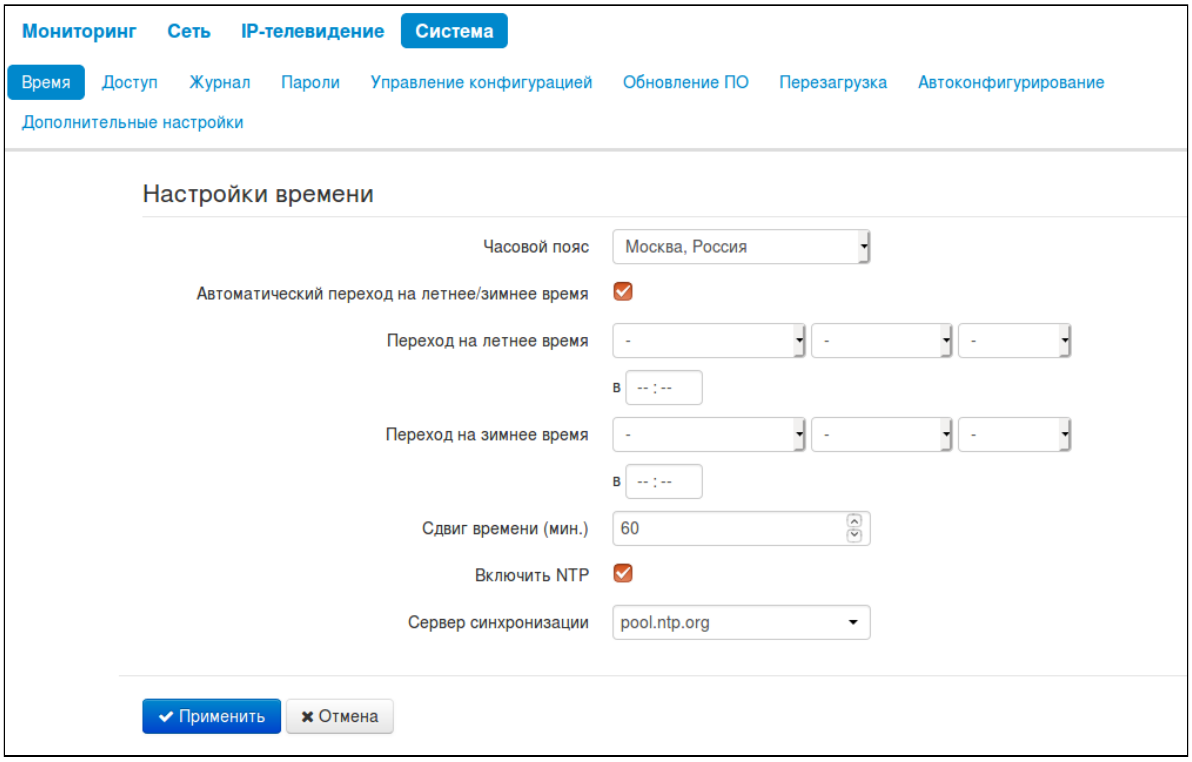
5.4 Меню «Система»

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

5.4.1 Подменю «Время»

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

Настройки времени

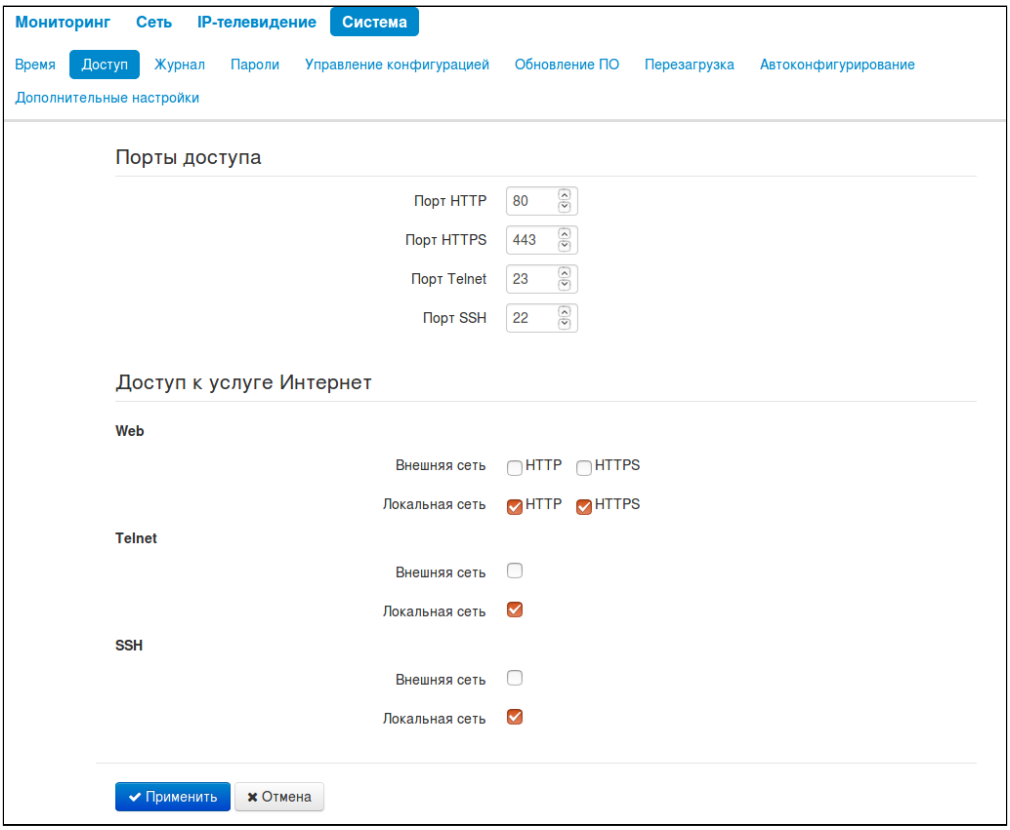


- *Часовой пояс* – позволяет установить часовой пояс в соответствии с ближайшим городом в Вашем регионе из заданного списка;
- *Автоматический переход на летнее/зимнее время* – при установленном флаге переход на летнее/зимнее время будет выполняться автоматически в заданный период времени:
  - *Переход на летнее время* – день и время, когда выполнять переход на летнее время;
  - *Переход на зимнее время* – день и время, 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»*.

5.4.2 Подменю «Доступ»

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



Порты доступа

В данном разделе выполняется настройка TCP-портов для доступа к устройству по 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

В данном разделе разрешается или запрещается доступ к устройству отдельными правилами для локальной и внешней сети (режим маршрутизатора). Для этого необходимо установить соответствующие флаги:

Web:

- *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).

Telnet:

Telnet – протокол, предназначенный для удаленного управления устройствами. Позволяет подключиться к устройству по сети для настройки и управления.
Для разрешения доступа к устройству по протоколу Telnet установите соответствующий флаг.

SSH:

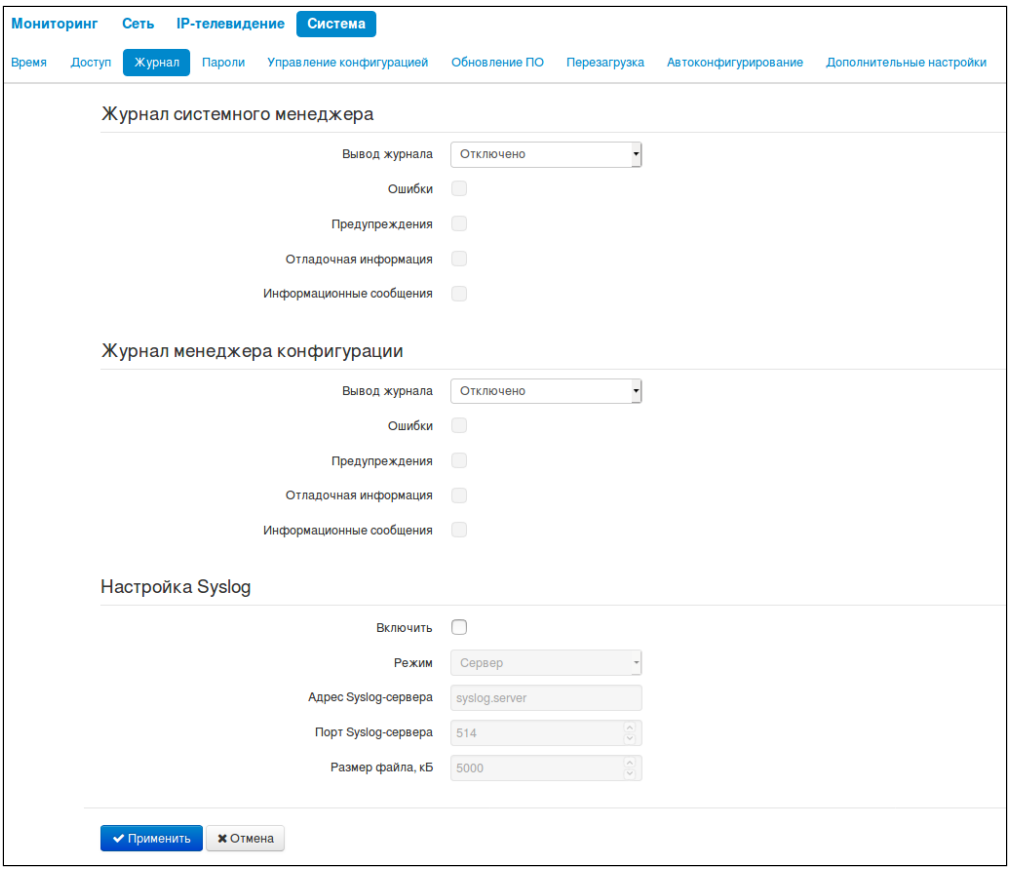
SSH – безопасный протокол удаленного управления устройствами. В отличие от Telnet протокол SSH шифрует весь трафик, включая передаваемые пароли.
Для разрешения доступа к устройству по протоколу SSH установите соответствующий флаг.

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

5.4.3 Подменю «Журнал»

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

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



Журнал системного менеджера

- *Вывод журнала* – направление вывода сообщений журнала:
  - *Отключено* – вывод 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* – вывод 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 (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;
    - *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 режимов «Сервер», «Сервер и файл»);
- *Порт Syslog-сервера* – порт для входящих сообщений Syslog-сервера (по умолчанию 514, необходимо для режимов «Сервер», «Сервер и файл»);
- *Имя файла* – имя файла для хранения журнала в формате Syslog (необходимо для режимов «Локальный файл», «Сервер и файл»). При нажатии на ссылку «Показать журнал» откроется страница с содержимым файла Syslog;
- *Размер файла, кБ* – максимальный размер файла журнала (необходимо для режимов «Локальный файл», «Сервер и файл»).

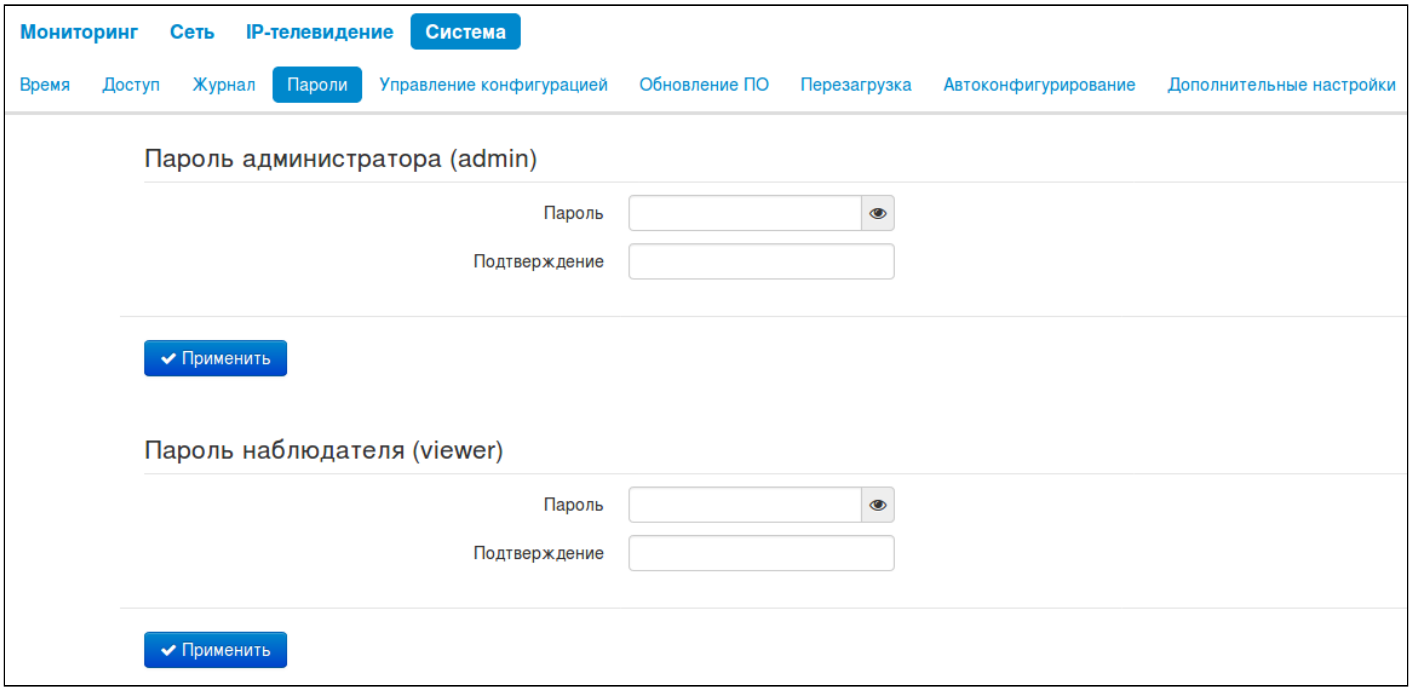
5.4.4 Подменю «Пароли»

В подменю «Пароли» устанавливаются пароли доступа администратора 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. Наблюдатель (пароль по умолчанию: **viewer**) имеет возможность только просматривать конфигурацию и данные мониторинга устройства без возможности вносить какие-либо изменения.

Логин администратора: admin
Логин наблюдателя: viewer



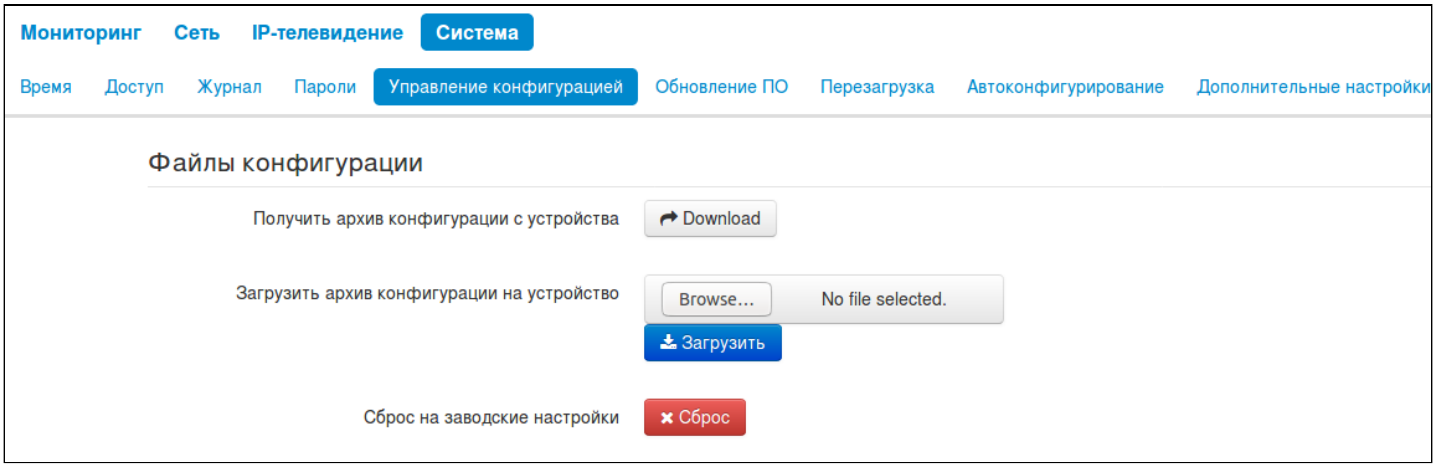
- *Пароль администратора* – в соответствующие поля введите пароль администратора и подтвердите его;
- *Пароль наблюдателя (viewer)* – в соответствующие поля введите пароль наблюдателя и подтвердите его.

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

5.4.5 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 «Download».

Обновление конфигурации

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

Обратите внимание, все пароли в конфигурации устройства шифруются ключом, который зависит от MAC-адреса устройства. Перед загрузкой конфигурации с одного устройства на другие предварительно нужно поменять пароли в файле конфигурации.

Для изменения паролей необходимо открыть файл конфигурации в текстовом редакторе и изменить пароли. Далее сохранить изменения в архиве конфигурации. Пример изменения паролей приведен ниже:

```
    Passwords:
        AdminPassword: "encrypted:7C607178736B7465"
        ViewerPassword: "encrypted:7A68677C6176"

изменяется на

    Passwords:
        AdminPassword: "password"
        ViewerPassword: "password"
```

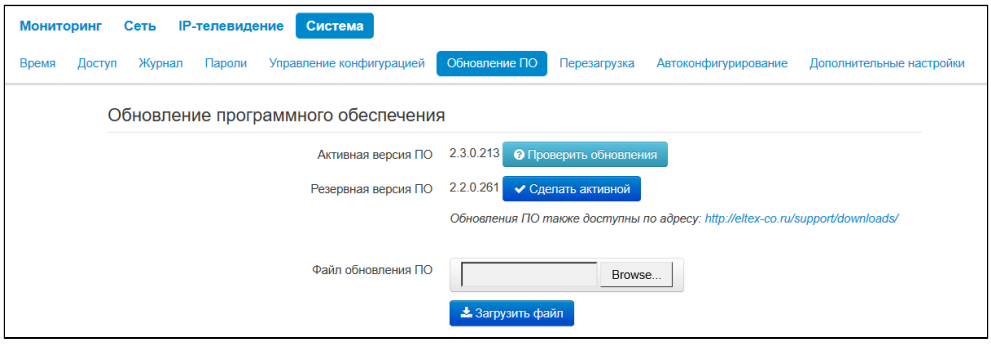
Сброс устройства на заводские настройки

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

5.4.6 Подменю «Обновление ПО»

Подменю «Обновление ПО» предназначено для обновления программного обеспечения устройства.

Обновление ПО для устройств WB-2P-LR5:



- *Активная версия ПО* – версия программного обеспечения, установленного на устройстве, работающая в данный момент;
- *Резервная версия ПО* – версия программного обеспечения, установленного на устройстве, на которую можно переключиться без загрузки файла ПО;
- *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;
- *Сделать активной* – кнопка, позволяющая сделать резервную версию ПО активной, для этого потребуется перезагрузка устройства. Активная версия ПО в этом случае станет резервной.

Для работы функции проверки обновления необходимо наличие выхода в Интернет.

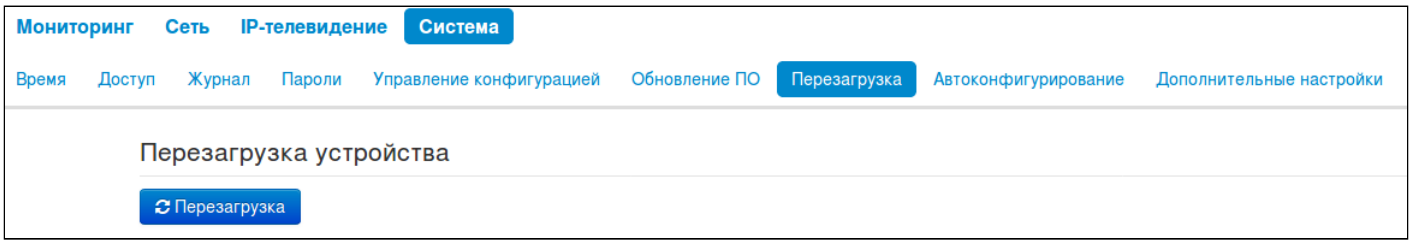
Обновить программное обеспечение устройства можно также вручную, предварительно загрузив файл ПО с сайта https://eltex-co.ru/support/downloads/ и сохранив его на компьютере. Для этого нажмите кнопку «Выберите файл» в поле *Файл обновления ПО* и укажите путь к файлу в формате .tar.gz.

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. В случае обновления с версии ПО 2.0.0 на версию ПО 2.1.0 после обновления необходимо осуществить сброс устройства к заводским настройкам и повторно сконфигурировать в соответствии со схемой использования, либо предварительно настроить значение мощности сигнала в меню Сеть - Интернет не менее 16 дБм.

5.4.7 Подменю «Перезагрузка»

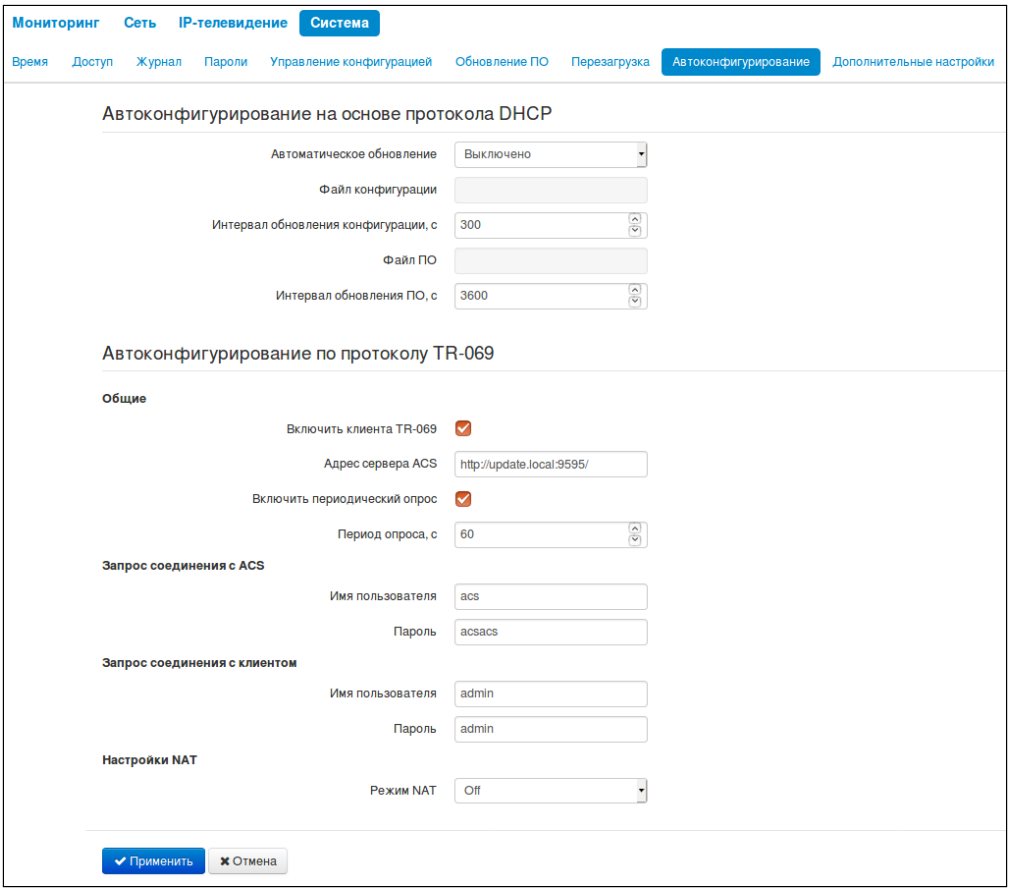
В подменю «Перезагрузка» выполняется перезапуск устройства.



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

5.4.8 Подменю «Автоконфигурирование»

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



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 Алгоритм работы автоматического обновления устройства на основе протокола DHCP;
  - *DHCP options* – пути к файлам конфигурации и программного обеспечения определяются из DHCP опций 43 и 66 (для этого необходимо для услуги Интернет выбрать протокол DHCP); подробнее работу алгоритма смотрите в разделе Алгоритм работы автоматического обновления устройства на основе протокола DHCP;
- *Файл конфигурации* – полный путь к файлу конфигурации – задаётся в формате URL (на данный момент возможна загрузка файла конфигурации по протоколу TFTP):

  tftp://<server address>/<full path to cfg file>
  где < server address > – адрес 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 протоколу TFTP):

  tftp://<server address>/<full path to firmware file>
  где < server address > – адрес 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 Алгоритм работы автоматического обновления устройства на основе протокола DHCP.

Автоконфигурирование по протоколу TR-069:

Общие:

- *Включить клиента TR-069* – при установленном флаге разрешена работа встроенного клиента протокола TR-069, 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 9595). Во втором случае клиент будет использовать безопасный протокол HTTPS для обмена информацией с сервером ACS.
- *Включить периодический опрос* – при установленном флаге встроенный клиент TR-069 осуществляет периодический опрос сервера ACS с интервалом, равным *«Периоду опроса»*, в секундах. Цель опроса - обнаружить возможные изменения в конфигурации устройства.

Запрос соединения с ACS:

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

Запрос соединения с клиентом:

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

Настройки NAT:

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

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

При выборе режима *STUN* необходимо задать следующие настройки:

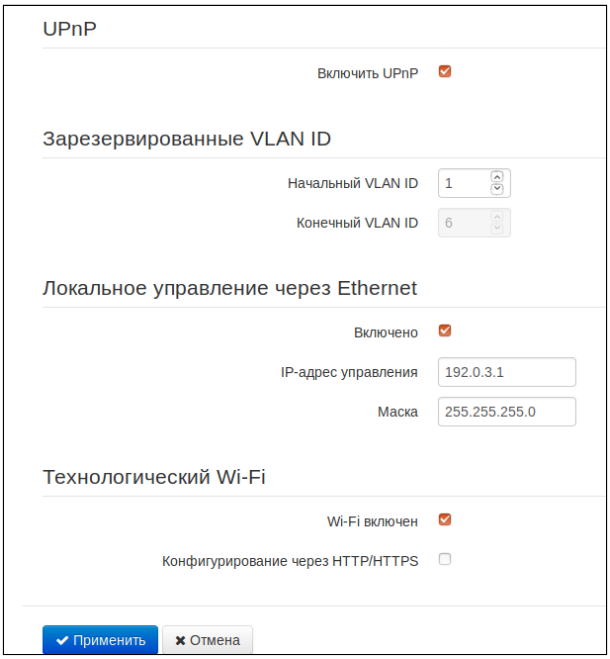
- *Адрес STUN-сервера* − IP-адрес или доменное имя STUN-сервера;
- *Порт STUN-сервера* − UDP-порт STUN-сервера (по умолчанию значение 3478);
- *Минимальный период опроса, с* и *Максимальный период опроса, с* − определяют интервал времени в секундах для отправки периодических сообщений на STUN-сервер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

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

По протоколу TR-069 возможно произвести основное конфигурирование устройства, обновление программного обеспечения, чтение информации об устройстве (версия ПО, модель, серийный номер и т.д.), загрузку и выгрузку целого файла конфигурации, удаленную перезагрузку устройства (поддержаны спецификации TR-069, TR-098).
Для вступления в силу новой конфигурации и занесения настроек в энергонезависимую память нажмите кнопку *«Применить»*. Для отмены изменений нажмите кнопку *«Отмена»*.

5.4.9 Подменю «Дополнительные настройки»

В подменю «Дополнительные настройки» можно включить UPnP, указать зарезервированные VLAN ID, включить/выключить Технологический Wi-Fi.



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.

- *Включить UPnP* – при установленном флаге протокол UPnP включен, иначе – выключен.

Зарезервированные VLAN ID

Зарезервированные VLAN ID – список служебных VLAN, используемых устройством для внутренних целей.

- *Начальный VLAN ID* – начальный номер VLAN;
- *Конечный VLAN ID* – конечный номер VLAN.

При включении флага «Использовать Management VLAN» и неправильной настройке Management VLAN возможна потеря доступа к устройству. При подключении через Ethernet у стройство будет доступно по адресу 192.0.3.1.

Технологический Wi-Fi

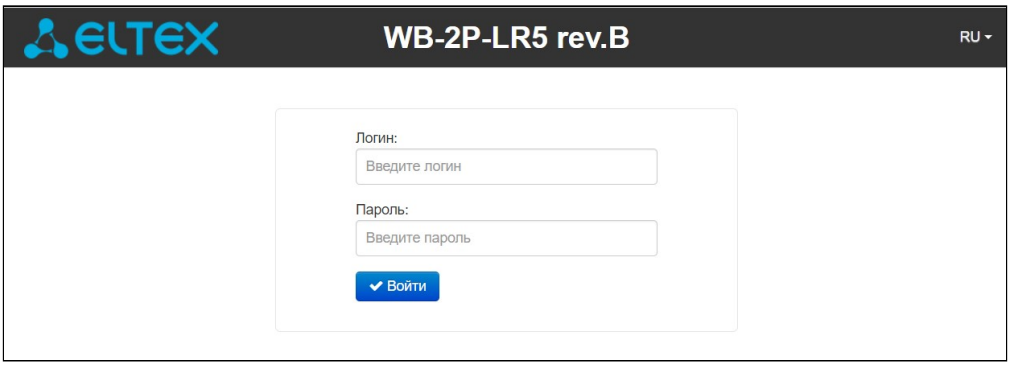
- Технологический Wi-Fi (доступен только на WB-2P-LR5 rev.C) используется при юстировке Wi-Fi (пункт 3.5 Юстировка антенны Wi-Fi). При включенном Технологическом Wi-Fi к устройству можно подключиться Wi-Fi клиентом через открытую сеть с SSID «EltexWiFi» (диапазон частот 2.4 ГГц).
  - *Wi-Fi включен* – при установленном флаге Технологический Wi-Fi включен, иначе – выключен. По умолчанию Технологический Wi-Fi включен.
  - *Конфигурирование через HTTP/HTTPS* – при установленном флаге доступна возможность конфигурирования устройства через Технологический Wi-Fi. По умолчанию конфигурирование через HTTP/HTTPS выключено.

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

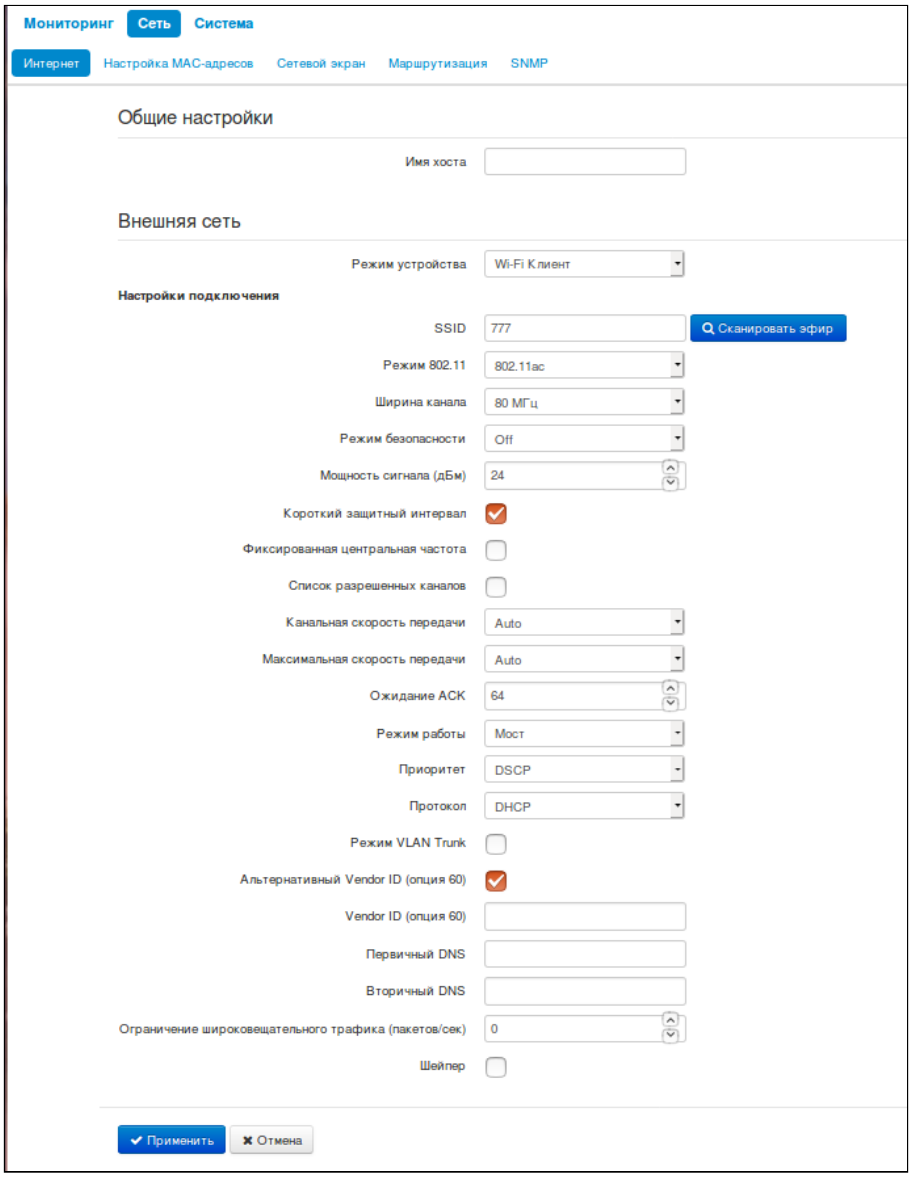
Во избежание несанкционированного доступа к устройству после юстировки Wi-Fi необходимо выключить Технологический Wi-Fi

6 Пример настройки

1. Подключите ПК к LAN-порту инжектора;
2. В адресной строке браузера введите IP-адрес устройства (по умолчанию 192.168.1.1, если устройство не получило адрес по DHCP). 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 ПК находится в одной сети с устройством.



На странице «Интернет» в меню «Сеть» настраивается внешнее соединение. В поле «Режим работы» выберите нужный режим работы: Мост или Маршрутизатор. Если для подключения к сети провайдера используются статические настройки, то в поле «Протокол» нужно выбрать значение «Static», заполнить поля «IP-адрес», «Маска подсети», «Шлюз по умолчанию», «Первичный DNS» и «Вторичный DNS» – значения параметров предоставляются провайдером.
Необходимо настроить подключение к базовой станции. В поле «SSID» укажите идентификатор беспроводной сети, к которой необходимо произвести подключение. В поле «Режим безопасности» выберите режим безопасности, по которому осуществляется аутентификация в данной сети и задайте ключ, если используется сеть с шифрованием. После нажатия на кнопку «Применить», абонентская станция выполнит поиск указанного SSID в эфире и при обнаружении выполнит попытку подключения к базовой станции с указанными параметрами. Если параметры указаны корректно и уровень сигнала достаточный, произойдет успешное подключение.

7 Спектроанализатор

Чтобы воспользоваться встроенным спектроанализатором на WB-2P-LR5 необходимо зайти на устройство по telnet или ssh.

Запуск производится командой: **spectrum-analyzer**.

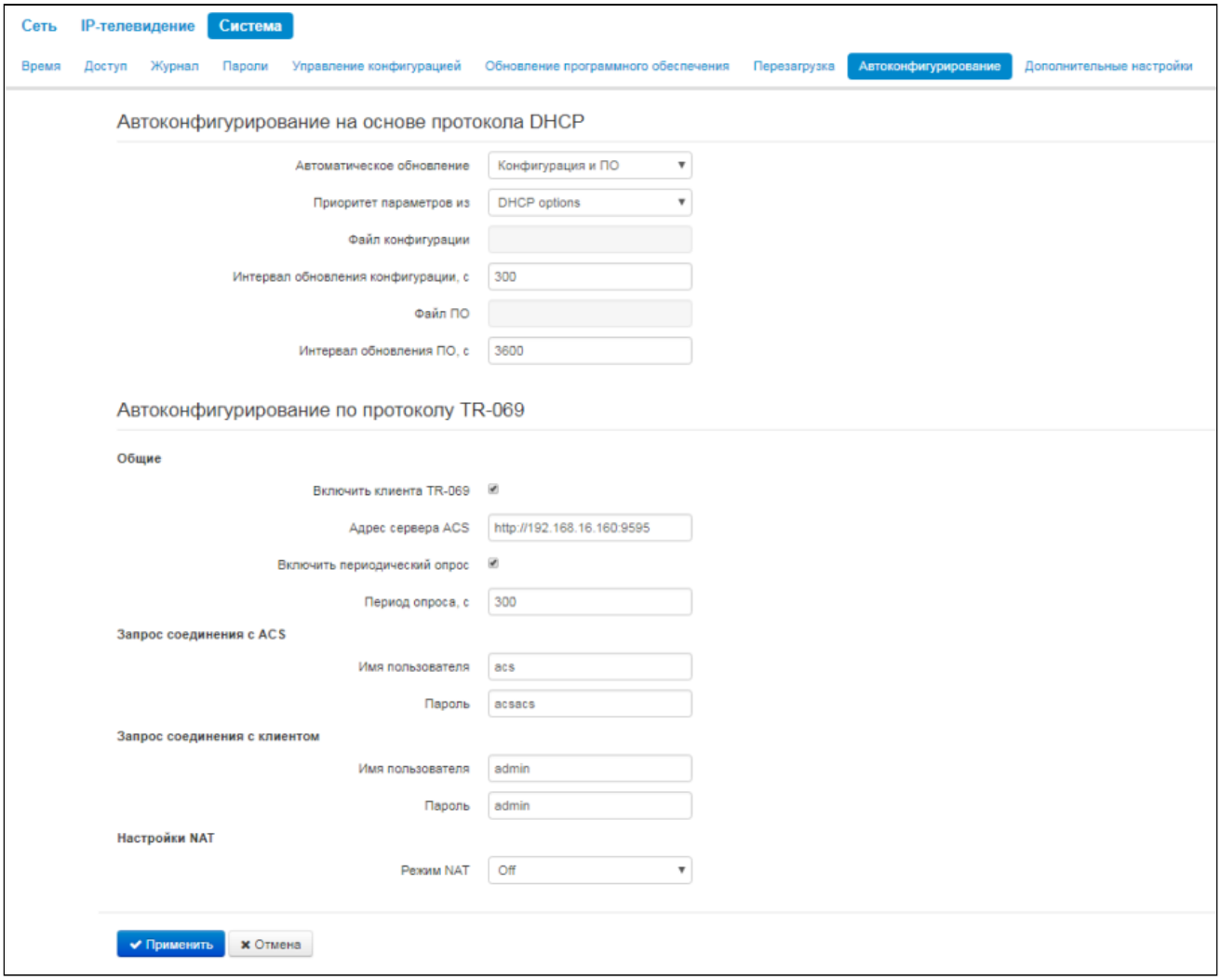
Время анализа всех радиоканалов диапазона составляет примерно 5 минут.

Обратите внимание, что на время работы спектроанализатора произойдет отключение от базовой станции до тех пор, пока спектроанализатор не прекратит свою работу.

Результат можно получить с помощью команды **spectrum-analyzer-result**. В консоль будет выдана информация о загрузке каждого радиоканала (в процентах):

```
root@WB-2P-LR5:~$ spectrum-analyzer
Spectrum analyzer scanning in progress
root@WB-2P-LR5:~$
root@WB-2P-LR5:~$ spectrum-analyzer-result
=================start dump config================
node: Monitoring.Network.SpectrumAnalyzer
        name: 36, value: 5
        name: 37, value: 5
        name: 38, value: 0
        name: 39, value: 3
        name: 40, value: 1
        name: 41, value: 3
        name: 42, value: 0
        name: 43, value: 3
        name: 44, value: 3
        name: 45, value: 3
        name: 46, value: 0
        name: 47, value: 4
        name: 48, value: 2
        ...
```

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

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

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

   - *$MA* – MAC address – вместо данного макроса в URL файла устройство подставляет собственный MAC-адрес;
   - *$SN* – Serial number – вместо данного макроса в URL файла устройство подставляет собственный серийный номер;
   - *$PN* – Product name – вместо данного макроса в URL файла устройство подставляет название модели (например, WB-2P-LR5).

MAC-адрес, серийный номер и название модели можно посмотреть в режиме мониторинга на странице меню «Устройство».
Примеры URL:

tftp://download.server.loc/firmware.file, http://192.168.25.34/configs/WB-2P-LR5//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_wb.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: wb-2p-lr5.cfg;
- для имени файла программного обеспечения: wb-2p-lr5.fw.

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

tftp://update.local/wb-2p-lr5.cfg,
а URL файла ПО:
tftp://update.local/wb-2p-lr5.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: wb-2p-lr5.cfg;
- для имени файла программного обеспечения: wb-2p-lr5.fw.

Формат опции 43 (Vendor specific info)

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

1 – код адреса сервера автоконфигурирования по протоколу TR-069;

2 – код для указания параметра Provisioning Code.

3 – код имени пользователя для авторизации на сервере TR-069;

4 – код пароля для авторизации на сервере TR-069;

5 – код адреса сервера; адрес сервера задается в формате URL: tftp://address или http://address . В первом варианте указан адрес сервера TFTP, во втором – HTTP;

6 – код имени файла конфигурации;

7 – код имени файла ПО;

8 – код тега VLAN для управления;

«|» - обязательный разделительный символ между кодами и значениями подопций.

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

1. Инициализация DHCP-обмена
   После загрузки устройство инициирует DHCP-обмен.
2. Анализ опции 43
   При получении опции 43 анализируется подопция 8 (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 во вкладке «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 Процедура восстановления системы после сбоя при обновлении программного обеспечения .

9 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 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 устройство произведет запись программного обеспечения в память и автоматически выполнит запуск системы. Время записи составляет около 8 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).

10 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 cfg.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*.

11 Приложение Б. Диаграмма направленности

Диаграмма направленности антенны вертикальной поляризации в H-плоскости:

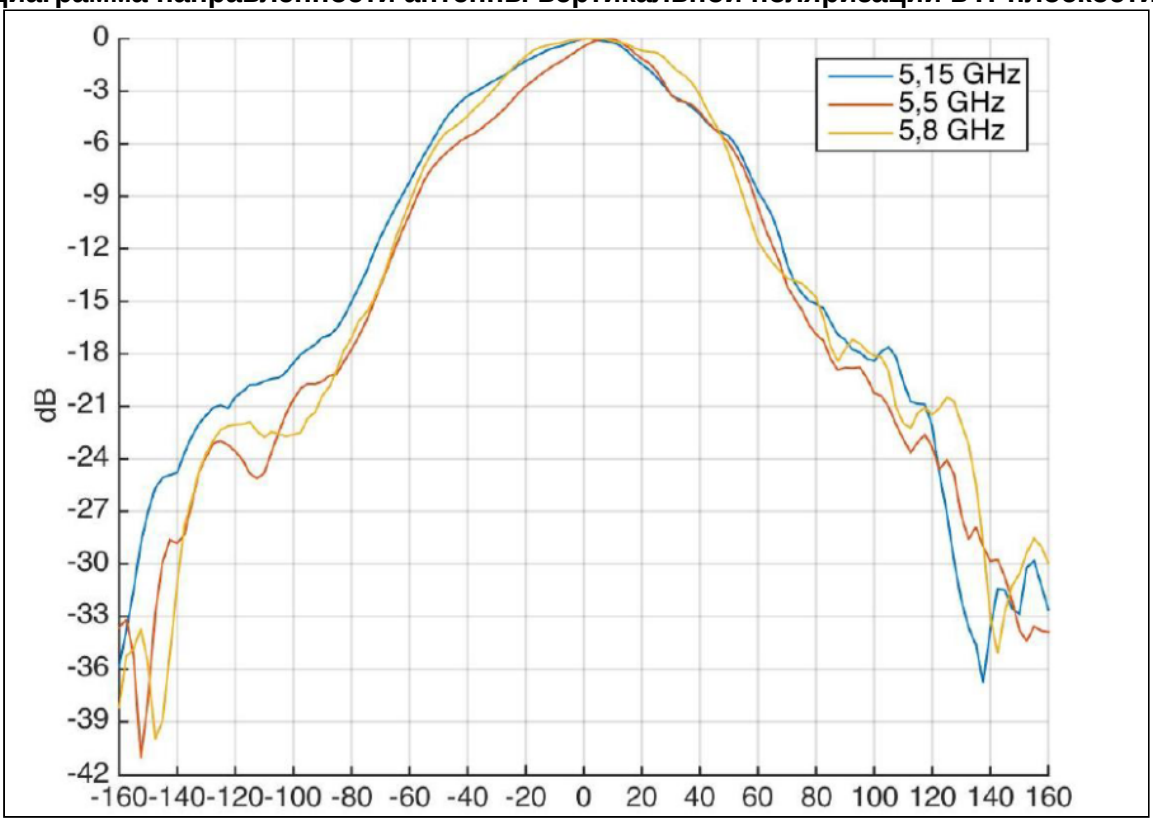


Диаграмма направленности антенны вертикальной поляризации в E-плоскости:

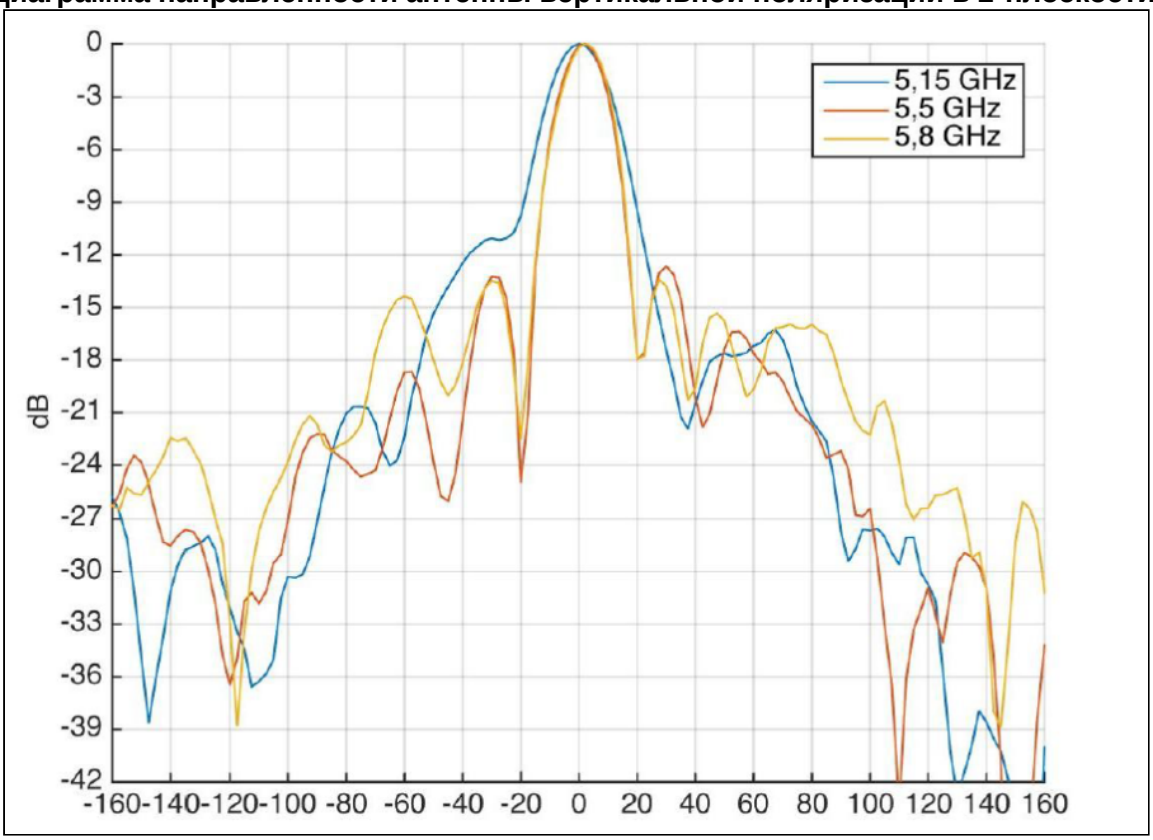


Диаграмма направленности антенны горизонтальной поляризации в H-плоскости:

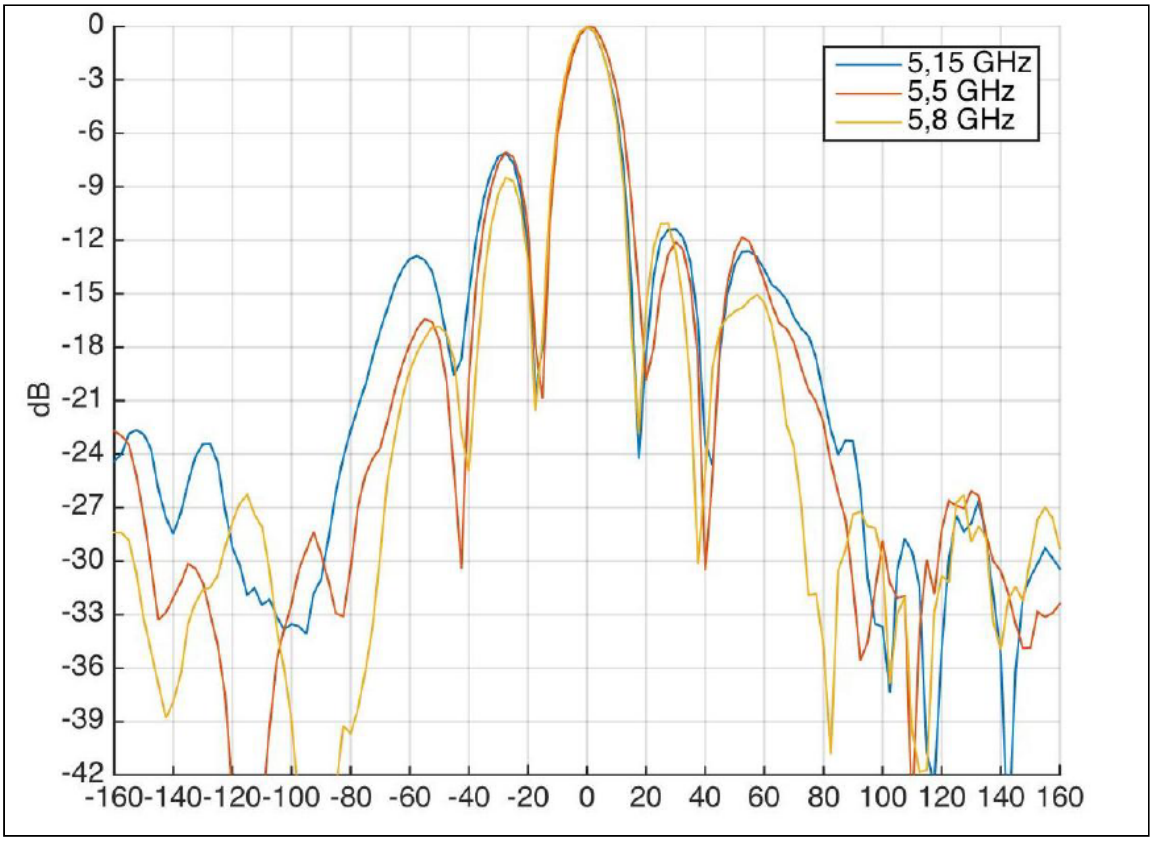
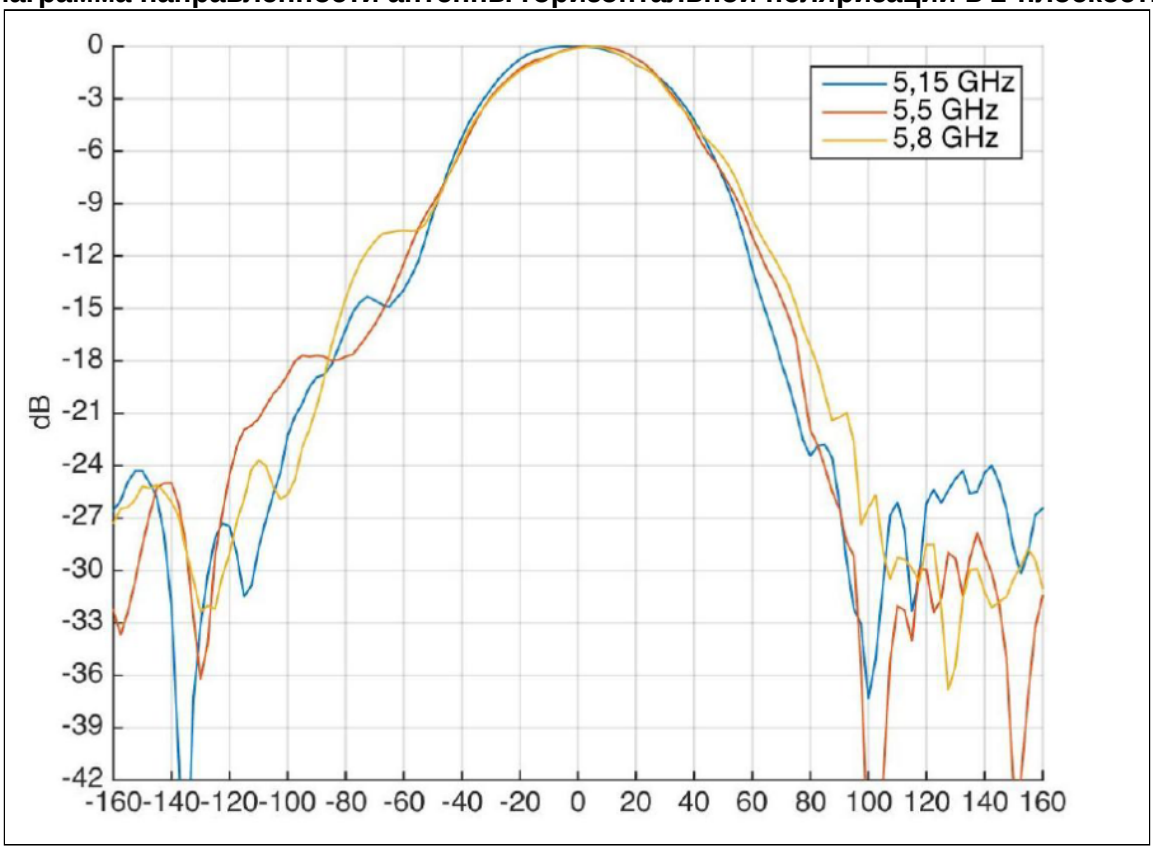


Диаграмма направленности антенны горизонтальной поляризации в Е-плоскости:



12 Список изменений

Версия документа	Дата выпуска	Содержание изменений
Версия 5.2	25.06.2021	Синхронизация с версией ПО 2.4.6
Версия 5.1	22.12.2020	Синхронизация с версией ПО 2.4.1
Версия 5.0	06.04.2020	Синхронизация с версией ПО 2.4.0 Добавлено: 4.4 Тестовый режим Изменено: 5.2.1 Меню «Сеть/Интернет»
Версия 4.0	06.11.2019	Синхронизация с версией ПО 2.3.0 Изменено: • Технические параметры • Конструктивное исполнение • Порядок монтажа • Юстировка антенны Wi-Fi • Меню «Сеть/Интернет» • Подменю «Локальная сеть» • Меню «Сеть/SNMP» • Меню «Мониторинг» • Подменю «PPPoE Relay»
Версия 3.0	28.06.2019	Синхронизация с версией ПО 2.2.0 Добавлено: • Юстировка антенны Wi-Fi

Версия документа	Дата выпуска	Содержание изменений
Версия 2.0	31.10.2018	Добавлено: 4.5.3 Беспроводной мост 4.6.4 Подменю «WDS» 4.6.5 Подменю «Радиоинтерфейс» 4.7.2 Подменю «WDS» Изменено: 2.2 Характеристики устройства 4.6.3 Подменю «Интернет» 4.6.7 Подменю «Настройка MAC-адресов»
Версия 1.0	24.11.2017	Первая публикация
Версия программного обеспечения		2.4.6

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

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

Форма обратной связи на сайте: https://eltex-co.ru/support/

Servicedesk: https://servicedesk.eltex-co.ru

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

Официальный сайт компании: https://eltex-co.ru/

Технический форум: https://eltex-co.ru/forum

База знаний: https://docs.eltex-co.ru/display/EKB/Eltex+Knowledge+Base

Центр загрузок: https://eltex-co.ru/support/downloads