Research Laboratory of Design Automation
НИЛ автоматизации проектирования
Сделано в России
Тел.: (495) 26-66-700, e-mail: info@reallab.ru, www.reallab.ru

Серия шлюзов RealLab! NLS-Gateway

Работа со шлюзами RealLab! серии NLS-Gateway, настройка Chirpstack, Zigbee2MQTT и основных параметров ОС RealLab! Raspbian Linux

Программное обеспечение шлюзов RealLab! серии NLS-Gateway

Руководство пользователя

© НИЛ АП, 2026

Версия от 1 июня 2026 г.

Одной проблемой стало меньше!

Уважаемый покупатель!

Научно-исследовательская лаборатория автоматизации проектирования (НИЛ АП) благодарит Вас за покупку и просит сообщать нам свои пожелания по улучшению этого руководства или описанной в нем продукции. Направляйте Ваши пожелания по адресу или телефону:

НИЛ АП, пер. Биржевой Спуск, 8, Таганрог, 347900,

Тел. (495) 26-66-700,

e-mail: info@reallab.ru • www.reallab.ru.

Вы можете также получить консультации по применению нашей продукции, воспользовавшись указанными выше координатами.

Пожалуйста, внимательно изучите настоящее руководство. Это позволит вам быстро и эффективно приступить к использованию приобретенного изделия.

Авторские права на настоящее руководство принадлежат НИЛ АП.

Оглавление

1. Вводная часть 5

1.1. Первый запуск 5

2. Веб-конфигуратор RealLab! 6

2.1. Описание веб-конфигуратора RealLab! 6

2.2. Навигация по веб-интерфейсу конфигуратора RealLab! 6

2.3. Начальная настройка веб-конфигуратора RealLab! 7

2.3.1. Смена пароля 7

2.4. Получение Gateway ID концентратора LoRaWAN 8

2.5. Настройки веб-конфигуратора 9

2.6. Главная страница веб-конфигуратора 12

2.7. Страница «Инфо» 14

2.8. Страница «Процессы» 15

2.9. Настройка часов реального времени (RTC) 16

2.9.1. Настройка даты и времени 17

2.9.2. Настройка часового пояса 18

2.9.3. Синхронизация и настройка NTP 19

2.10. Настройка параметров сети 20

2.10.1. Ethernet 21

2.10.2. Настройка Wi-Fi 24

2.10.3. Bluetooth 28

2.10.4. Настройка CAN 32

2.10.5. LoRaWAN 37

2.10.6. MQTT 48

2.10.7. Zigbee 53

3. Chirpstack 55

3.1. Описание ПО Chirpstack....55
3.2. Шлюзы RealLab с поддержкой Chirpstack....55
3.3. Вход в веб-интерфейс Chirpstack....55
3.4. Добавление LoRaWAN-концентратора в Chirpstack....56
3.5. Добавление датчиков LoRaWAN в Chirpstack....59
3.6. Передача данных с датчика в MQTT-брокер....65
4. Zigbee2MQTT....68
4.1. Описание ПО Zigbee2MQTT....68
4.2. Шлюзы RealLab с поддержкой Zigbee2MQTT....68
4.3. Вход в веб-интерфейс Zigbee2MQTT....68
4.4. Добавление датчиков и маршрутизаторов....69
4.5. Просмотр информации о датчиках....71
4.6. Управление датчиками из интерфейса Zigbee2MQTT....73
4.7. Карта сети....74
4.8. Настройка подключения к MQTT-брокеру с использованием шифрования TLS....75
4.9. Просмотр логов службы Zigbee2MQTT....77
Лист регистрации изменений....78

1. Вводная часть

Данный документ содержит инструкции по работе с программным обеспечением Reallab! Web-Config, Chirpstack и Zigbee2MQTT для шлюзов RealLab! серии NLS-Gateway.

При первом запуске шлюза обратитесь к п. 1.1 для воспроизведения корректной конфигурации устройства.

1.1. Первый запуск

Чтобы начать работу с Chirpstack, необходимо подключить шлюз RealLab! к источнику питания и локальной сети по Ethernet. Дождитесь его полной загрузки (20-25 секунд), шлюз получит динамический IP-адрес по DHCP.

Чтобы узнать динамический IP-адрес по DHCP, используйте ПО RealLab! Scanner PLCs или поиск через BLE-сканер (см. п. 2.10.3.1).

После получения IP-адреса появится возможность зайти в веб-конфигуратор RealLab! WebConfig для настройки шлюза и его интерфейсов, подключиться к шлюзу по SSH или зайти в веб-интерфейс Chirpstack, либо Zigbee2MQTT. Конфигуратор доступен локально на ПЛК на порте «8000», – чтобы его открыть, введите в адресную строку браузера IP-адрес: 8000.

Пример записи: 192.168.10.143:8000

Также станут доступны веб-интерфейсы Chirpstack и Zigbee2MQTT в зависимости от модификации шлюза.

Работа с веб-интерфейсами подробнее описана в разделах 2–4.

2. Веб-конфигуратор RealLab!

2.1. Описание веб-конфигуратора RealLab!

Веб-конфигуратор RealLab! является программным обеспечением, предназначенным для конфигурации параметров ОС шлюза RealLab! NLS-Gateway через браузер. Веб-конфигуратор автоматически запускается локально на шлюзе.

Возможности веб-конфигуратора RealLab!:

- настройка подключения к сети по Wi-Fi и Ethernet;
- просмотр информации о шлюзе и его состоянии (нагрузка, состояние интерфейсов);
- управление процессами, запущенными на ПЛК;
- управление параметрами интерфейса CAN;
- настройка параметров LoRaWAN-концентратора и Zigbee-координатора;
- настройка часов реального времени (RTC);
- конфигуратор CAN.

2.2. Навигация по веб-интерфейсу конфигуратора RealLab!

Навигация реализована с помощью кнопок в шапке веб-интерфейса. Для перехода в нужный раздел нажмите соответствующую кнопку.

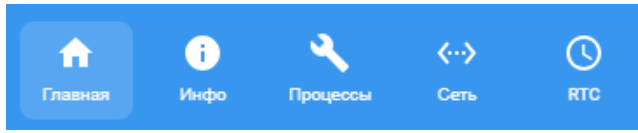


Рис. 2.1. Меню навигации при ширине окна браузера более 900 пикселей

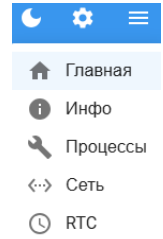


Рис. 2.2. Меню навигации при ширине окна браузера менее 900 пикселей

2.3. Начальная настройка веб-конфигуратора RealLab!

Для получения доступа ко входу в веб-конфигуратор RealLab! необходимо, чтобы устройство находилось в одной сети с устройством, с которого происходит подключение к конфигуратору.

В адресную строку браузера введите: «IP-адрес-шлюза:8000» (пример: 192.168.10.223:8000).

Откроется главная страница веб-конфигуратора, поверх нее отобразится окно авторизации (см. рис. 2.3).

Стандартные данные для входа в учетную запись веб-конфигуратора (эти данные не связаны с данными для подключения по SSH):

Имя пользователя: *pi*

Пароль: *12345678*

ВАЖНО! Пароль рекомендуется заменить на пользовательский.

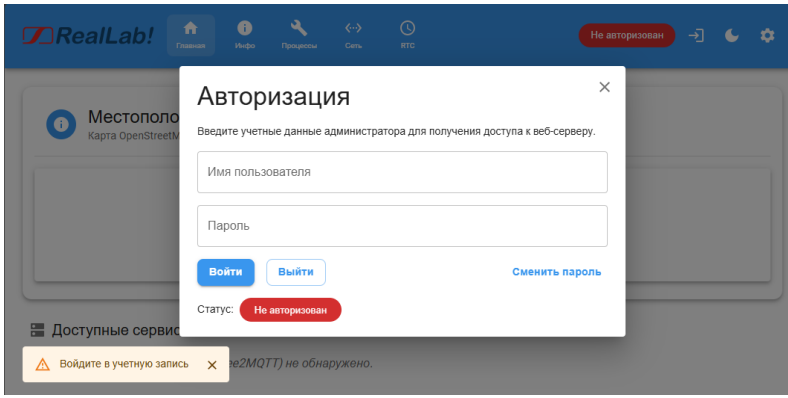


Рис. 2.3. Окно авторизации веб-конфигуратора RealLab!

2.3.1. Смена пароля

Для смены пароля в шапке веб-конфигуратора нажмите на кнопку авторизации:

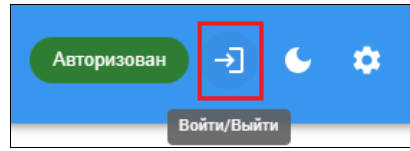


Рис. 2.4. Кнопка авторизации

В появившемся окне авторизации (см. рис. 2.3) нажмите на кнопку «Сменить пароль». Далее введите текущий пароль в поле «Старый пароль», а новый пароль в поле «Новый пароль» (см. рис. 2.5).

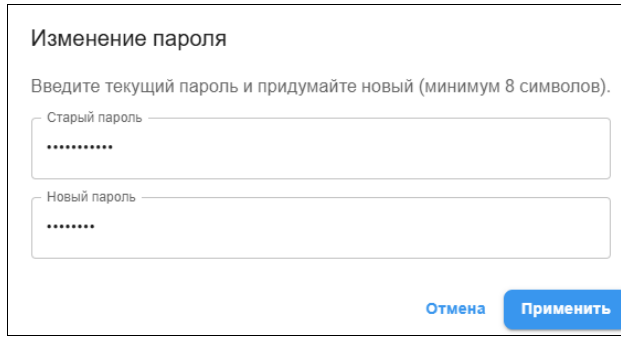


Рис. 2.5. Окно смены пароля

При успешной смене пароля появится уведомление (см. рис. 2.6).

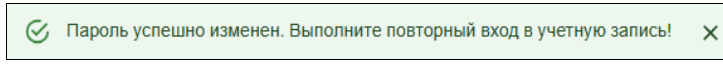


Рис. 2.6. Уведомление об успешной смене пароля

Выполните повторный вход в учетную запись с новым паролем, после этого доступ к серверу будет получен на 60 минут. Через 60 минут нужно будет выполнить вход повторно. Изменить период доступ к веб-интерфейсу можно в настройках сервера (п. 2.5.2).

2.4. Получение Gateway ID концентратора LoRaWAN

Перейдите на вкладку «Сеть» с помощью кнопки в шапке веб-интерфейса, после этого откроются сетевые настройки шлюза и появится список внутренних вкладок. Выберите вкладку LoRaWAN (рис. 2.7).

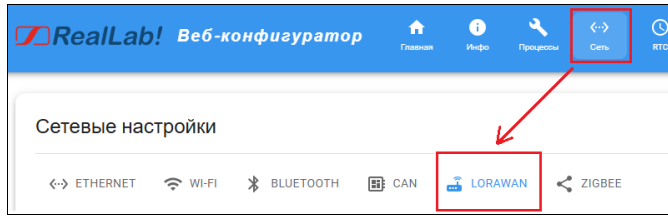


Рис. 2.7. Переход на вкладку Сеть – LoRaWAN

На странице отобразятся текущие параметры конфигурации LoRaWAN-концентратора и его идентификационный номер – Gateway ID (см. рис. 2.8).

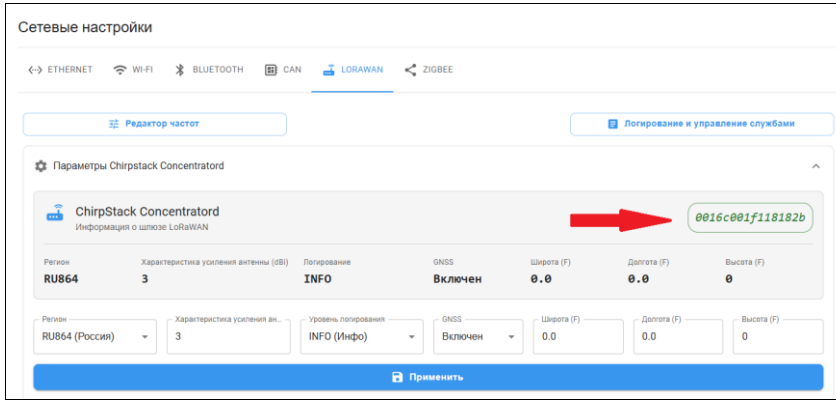


Рис. 2.8. Gateway ID на странице Сеть – LoRaWAN

2.5. Настройки веб-конфигуратора

Для входа в настройки веб-конфигуратора необходимо выполнить вход в учетную запись. После успешной попытки авторизации нажмите на значок в шапке веб-интерфейса, откроется окно с настройками (см. рис. 2.9).

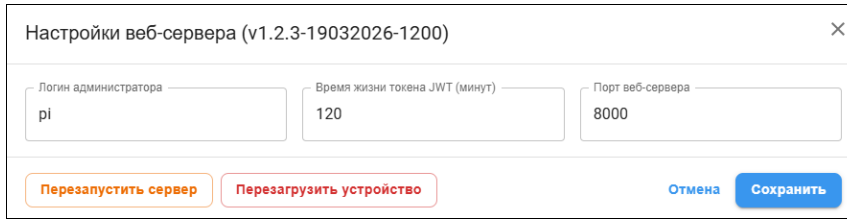


Рис. 2.9. Настройки веб-конфигуратора RealLab!

В заголовке окна в скобках указана текущая версия веб-конфигуратора RealLab! (v1.2.3-19032026-1200 на рис. 2.9).

Доступные настройки для изменения:

- логин администратора – имя учетной записи;
- время жизни JWT токена в минутах – после успешной авторизации выход из учетной записи автоматически произойдет через указанное количество минут;

- порт веб-конфигуратора – по умолчанию используется порт 8000, но его можно изменить на любой другой, кроме тех, что уже заняты другими сервисами.

2.5.1. Логин администратора

Для смены логина администратора измените его в поле «Логин администратора». Появится предупреждение о сбросе пароля. Нажмите кнопку «Сохранить».

ВАЖНО! При изменении логина администратора необходимо также сменить пароль.

Появится два окна (см. рис. 2.10): с временным паролем и окно авторизации. Закройте окно авторизации и скопируйте временный пароль в буфер обмена (см. рис. 2.11).

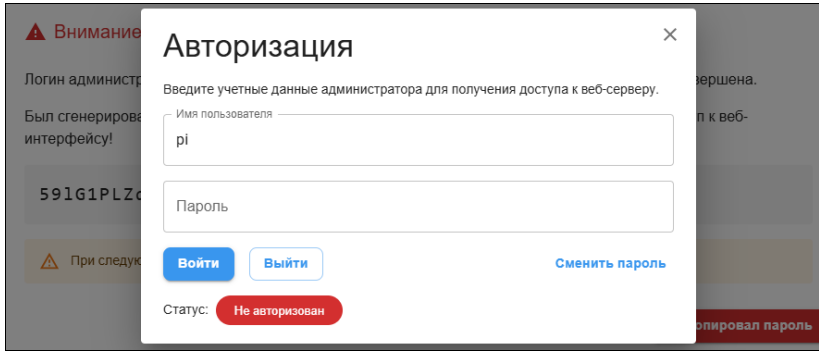


Рис. 2.10. Два окна после изменения логина

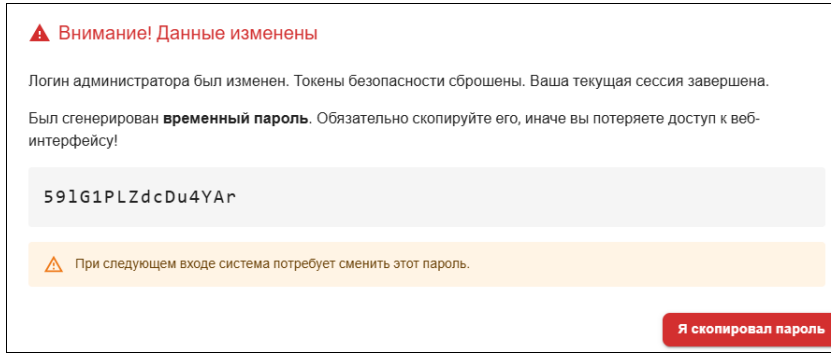


Рис. 2.11. Окно, содержащее временный пароль

Войдите в учетную запись под новым логином и паролем, нажмите значок в шапке веб-интерфейса для отображения окна авторизации и введите новый логин и временный пароль. После входа выполните смену пароля, как это описано в п. 2.3.1.

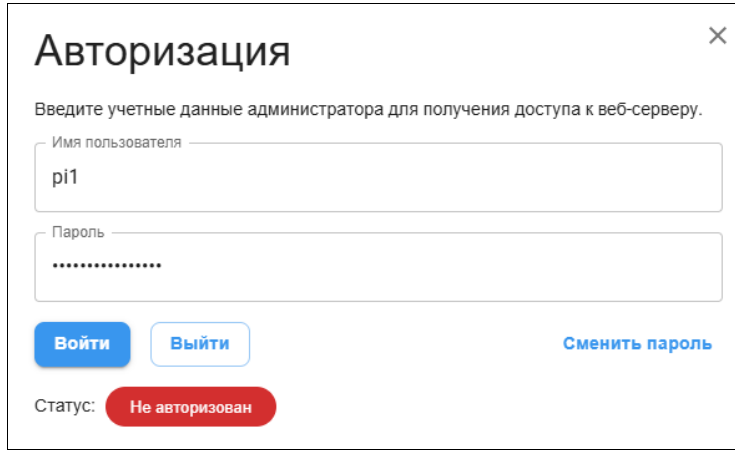


Рис. 2.12. Вход в учетную запись под новым логином

2.5.2. Время жизни токена JWT

При необходимости увеличения или уменьшения времени одной сессии, после авторизации в веб-конфигураторе RealLab! измените данный параметр. Например, значение 60 означает, что через 60 минут после авторизации токен будет считаться истекшим и придется заново входить в учетную запись (см. рис. 2.9).

После изменения значения, нажмите кнопку «Сохранить» и заново войдите в учетную запись для применения изменений, форма авторизации появится автоматически.

2.5.3. Порт веб-конфигуратора

Веб-конфигуратор по умолчанию использует порт 8000, но его можно изменить на любой другой, кроме тех, которые уже заняты другими сервисами.

После изменения номера порта, нажмите кнопку «Сохранить». Браузер отобразит запрос для подтверждения действия (см. рис. 2.13), нажмите «ОК».

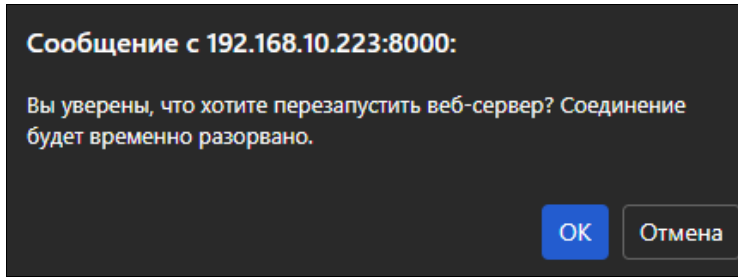


Рис. 2.13. Запрос на подтверждение изменения порта веб-конфигуратора

Через несколько секунд, при успешном изменении порта, произойдет автоматическое перенаправление на другой порт (см. рис. 2.14).

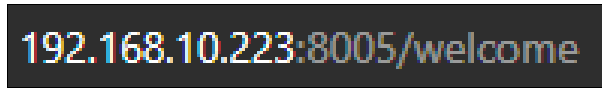


Рис. 2.14. Адресная строка после изменения порта

2.5.4. Действия

В настройках сервера есть возможность перезапустить сервер и перезапустить устройство (шлюз).

Перезапуск сервера – перезапуск службы веб-конфигуратора RealLab!

Перезапуск устройства (шлюза) – перезагрузка командой «sudo reboot».

При вызове действия браузер запросит подтверждение.

2.6. Главная страница веб-конфигуратора

На главной странице располагается карта с отображением текущего местоположения устройства (см. рис. 2.15). В нижней части страницы отображаются ссылки на активные веб-интерфейсы Chirpstack и Zigbee2MQTT. Если служба Chirpstack либо Zigbee2MQTT не запущена, либо не может быть запущена из-за ошибки, то ссылка отображаться не будет.

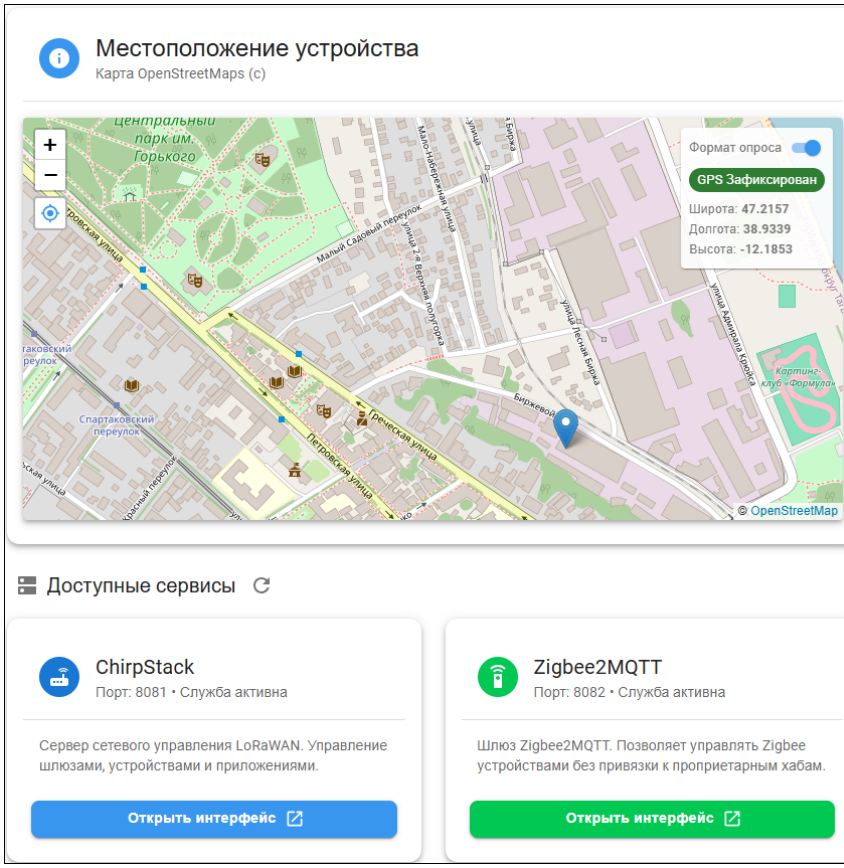


Рис. 2.15. Главная страница веб-конфигуратора RealLab!

Для перехода в веб-интерфейс Chirpstack или Zigbee2MQTT нажмите на кнопку «Открыть интерфейс» на карточке отображенного сервиса.

Местоположение устройства запрашивается каждые 3 секунды. Чтобы отключить постоянные запросы к API, переведите переключатель «формат опроса» в верхнем правом углу карты в выключенное положение (см. рис. 2.16). Так GPS будет запрашиваться только один раз – при переходе на главную страницу.

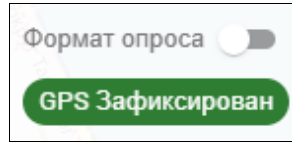


Рис. 2.16. Формат опроса GPS – одиночный

ВАЖНО! GPS-модуль установлен не на всех модификациях! В случае отсутствия модуля интерфейс карты позволит установить координаты вручную (см. рис. 2.17).

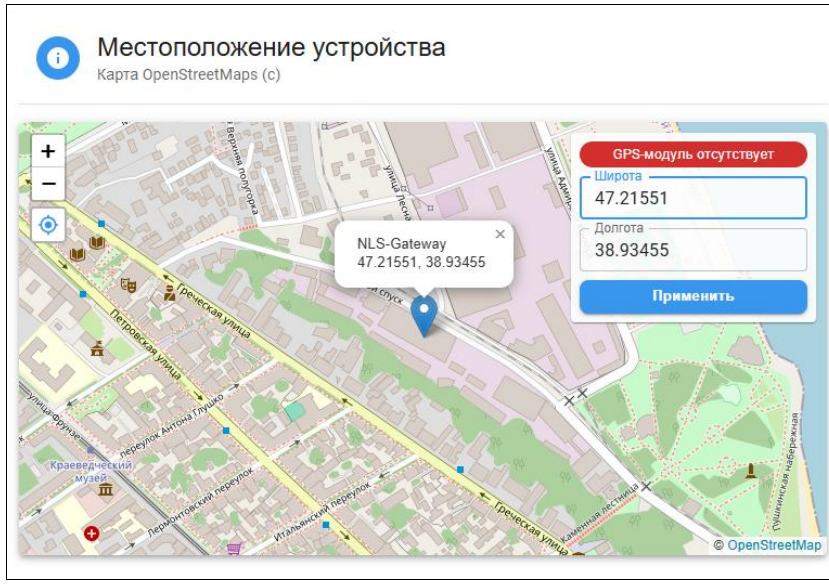


Рис. 2.17. Интерфейс карты при отсутствии модуля GPS

2.7. Страница «Инфо»

На странице «Инфо» можно просмотреть информацию о шлюзе, системе, нагрузке на ядра процессора, а также уровень заполнения постоянной и оперативной памяти.

По умолчанию включен автоматический запрос текущего состояния системы каждые 3 секунды – данная функция работает только когда открыт соответствующий функционал (см. рис. 2.18).

Рис. 2.18. Информация о системе

Рис. 2.19. Информация об интерфейсах

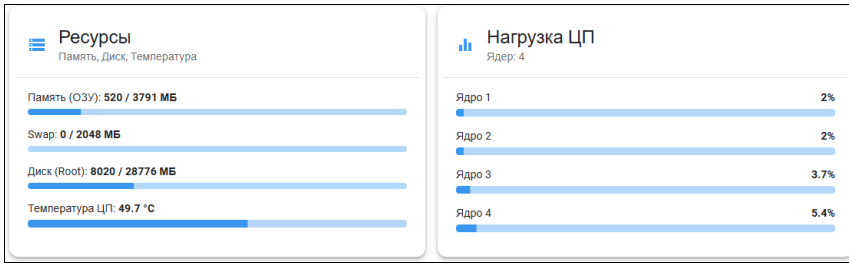


Рис. 2.20. Информация об используемых ресурсах

2.8. Страница «Процессы»

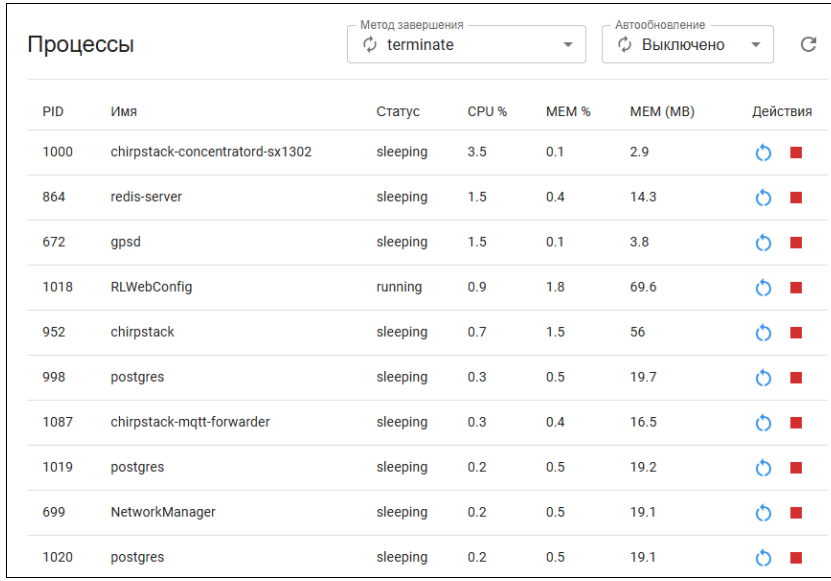
На данной странице отображается список запущенных процессов на устройстве.

Каждый процесс имеет свой идентификатор (PID) и имя. Также в таблице отображается нагрузка процесса на процессор (CPU в процентах) и память (MEM в процентах и мегабайтах) (см. рис. 2.21). Процессы отсортированы по убыванию нагрузки на процессор.

В колонке «Действия» можно перезапустить или остановить любой процесс из таблицы. Завершить процесс можно двумя методами: «terminate» или «killall -9». Используйте «killall -9» для принудительного завершения процесса, если при завершении процесса с помощью

“terminate” возникает ошибка. Метод можно выбрать в верхней части страницы из выпадающего списка.

По умолчанию автообновление списка процессов отключено, его можно включить в верхней части страницы, выбрав из выпадающего списка значение 3, 5, или 10 секунд. Для единичного обновления списка процессов кликните на кнопку .



PID	Имя	Статус	CPU %	MEM %	MEM (MB)	Действия
1000	chirpstack-concentratord-sx1302	sleeping	3.5	0.1	2.9	
864	redis-server	sleeping	1.5	0.4	14.3	
672	gpsd	sleeping	1.5	0.1	3.8	
1018	RLWebConfig	running	0.9	1.8	69.6	
952	chirpstack	sleeping	0.7	1.5	56	
998	postgres	sleeping	0.3	0.5	19.7	
1087	chirpstack-mqtt-forwarder	sleeping	0.3	0.4	16.5	
1019	postgres	sleeping	0.2	0.5	19.2	
699	NetworkManager	sleeping	0.2	0.5	19.1	
1020	postgres	sleeping	0.2	0.5	19.1	

Рис. 2.21. Таблица запущенных процессов на шлюзе NLS-Gateway

2.9. Настройка часов реального времени (RTC)

Перейдите на страницу настройки параметров часов реального времени (RTC). В верхней части страницы отображаются текущие значения параметров (см. рис. 2.22):

- системное время;
- время в модуле RTC;
- часовой пояс;
- состояние сервиса NTP;
- состояние синхронизации.

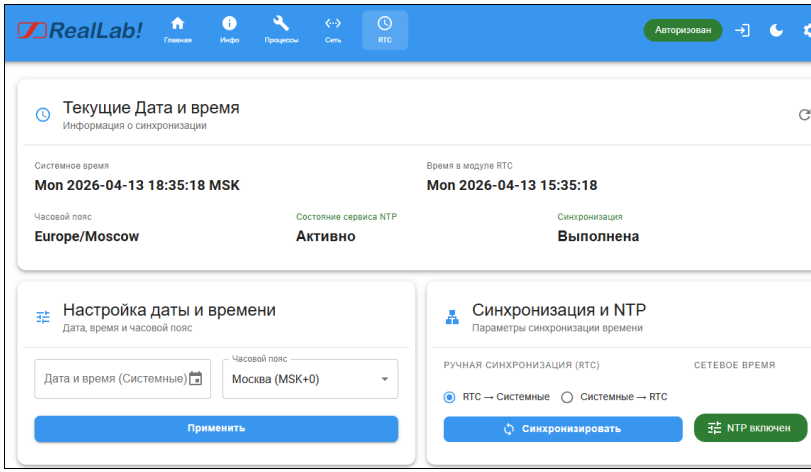


Рис. 2.22. Страница настройки RTC

2.9.1. Настройка даты и времени

Для изменения текущей даты и времени введите их вручную в формате «ДД/ММ/ГГГГ чч:мм» (пример: 30/03/2026, 12:35), либо выберите с помощью мышки (см. рис. 2.23). Далее нажмите «OK», затем «Применить».

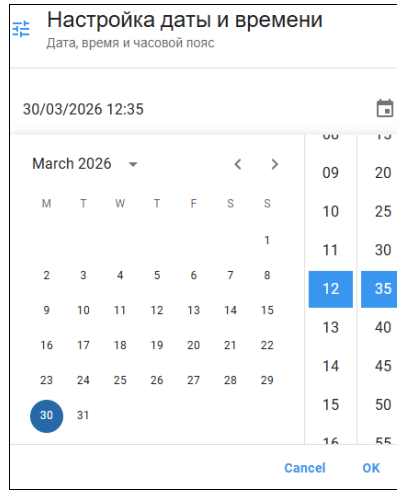


Рис. 2.23. Настройка даты и времени

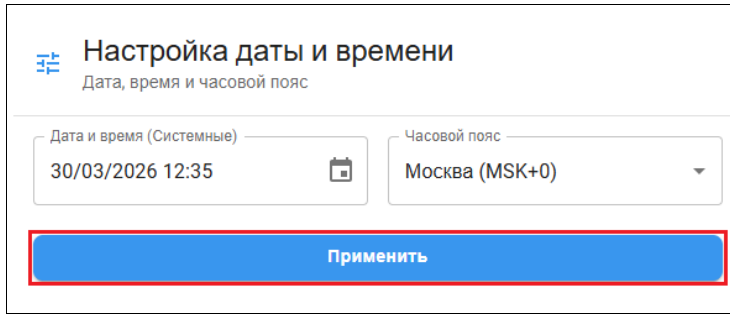


Рис. 2.24. Применение изменения даты и времени

2.9.2. Настройка часового пояса

Для изменения часового пояса выберите из выпадающего списка «Часовой пояс», а поле для ввода даты и времени оставьте пустым.

Выберите нужное значение (см. рис. 2.25) и нажмите «Применить» (см. рис. 2.26).

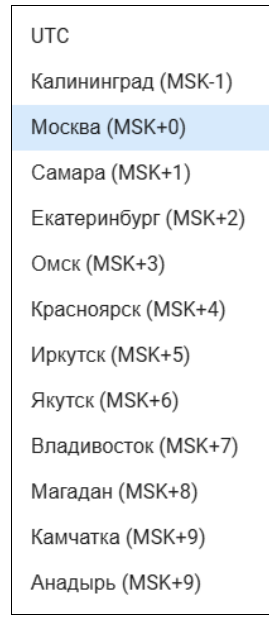


Рис. 2.25. Список часовых поясов

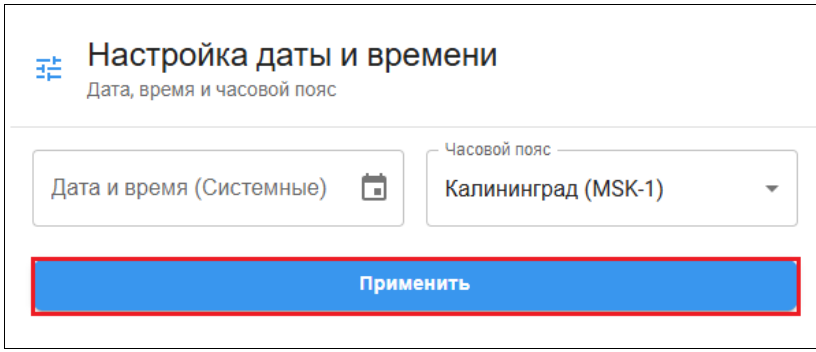


Рис. 2.26. Применение изменения часового пояса

2.9.3. Синхронизация и настройка NTP

Синхронизация времени:

- RTC → системные: системное время принимает значение, настроенное в модуле часов реального времени (RTC);
- Системные → RTC: в модуль часов реального времени (RTC) записывается системное время;

Для выполнения синхронизации выберите нужный режим и нажмите на кнопку «Синхронизировать» (см. рис. 2.27).

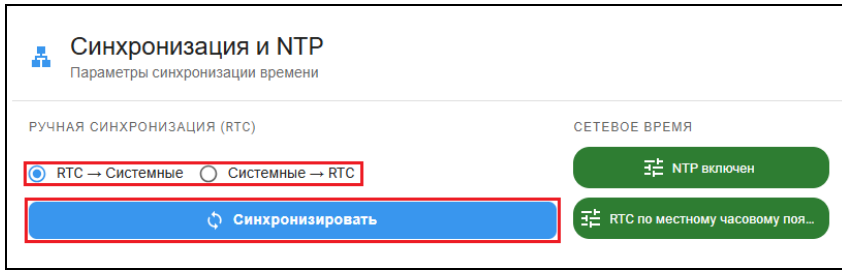


Рис. 2.27. Выбор режима синхронизации и ее выполнение

Для изменения состояния NTP нажмите на кнопку «NTP включен (выключен)» (см. рис. 2.28).

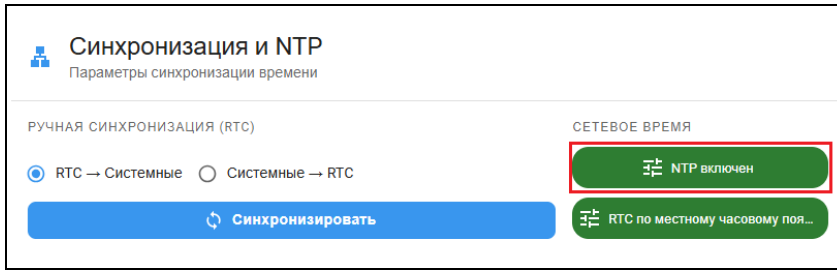


Рис. 2.28. Изменение состояния NTP

Для синхронизации времени RTC с местным часовым поясом должна быть включена функция «RTC по местному часовому поясу». Если она будет выключено, время RTC будет использовать время по Гринвичу (см. рис. 2.29).

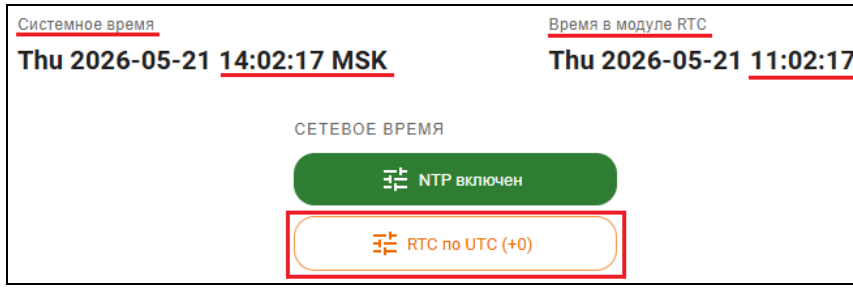


Рис. 2.29. Изменение режима RTC (по местному часовому поясу или по UTC+0)

2.10. Настройка параметров сети

Перейдите на страницу «Сеть», она содержит вкладки, каждая из которых соответствует настраиваемому подключению (см. рис. 2.30).

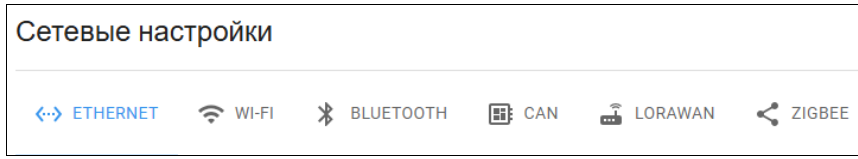


Рис. 2.30. Вкладки на странице «Сеть»

2.10.1. Ethernet

Данная вкладка открыта по умолчанию при переходе на страницу «Сеть».

Функции:

- сканер IP-адресов (занятых и свободных);
- настройка статического или динамического IP-адреса.

2.10.1.1. Сканер IP-адресов

Нажмите кнопку «Сканер IP-адресов» в верхней части страницы (см. рис. 2.31).

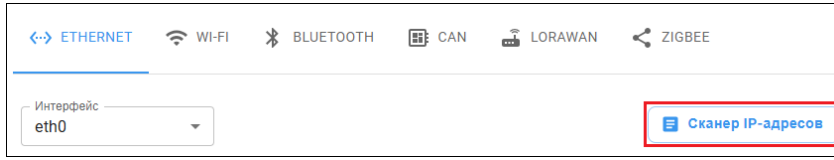


Рис. 2.31. Кнопка «Сканер IP-адресов»

Откроется окно поверх страницы (см. рис. 2.32). Выберите тип вывода списка IP-адресов:

- занятые: использовать для просмотра списка занятых IP-адресов конкретными устройствами (выводится IP-адрес, MAC-адрес и наименование производителя);
- свободные: использовать для поиска свободных IP-адресов для назначения статического IP-адреса шлюзу (выводится список свободных IP-адресов, доступных для использования).

Далее нажмите на кнопку сканирования (обозначена стрелкой на рис. 2.32).

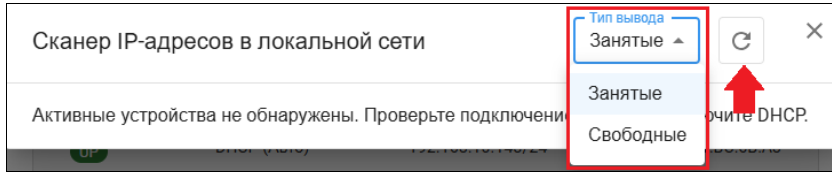


Рис. 2.32. Выбор типа вывода списка IP-адресов

Рис. 2.33. Пример вывода занятых IP-адресов

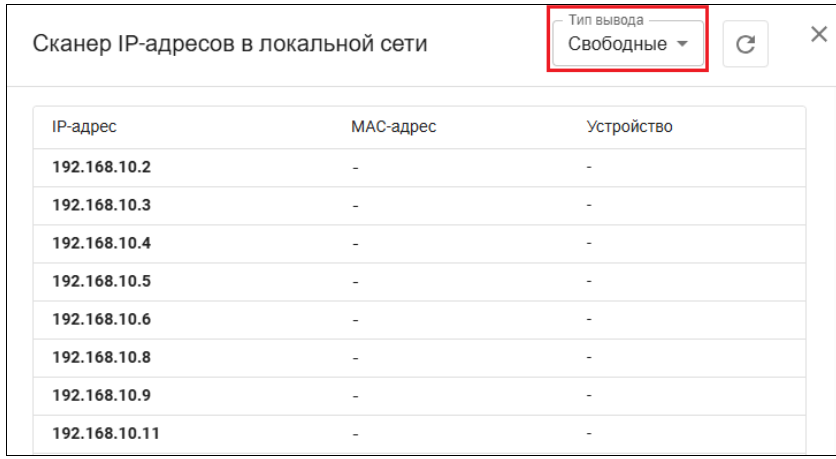


Рис. 2.34. Пример вывода свободных IP-адресов

2.10.1.2. Настройка статического IP-адреса

Воспользуйтесь сканером IP-адресов для поиска свободного IP-адреса (п. 2.10.1.1).

После выбора и копирования IP-адреса, который будет присвоен шлюзу, в нижней части страницы выберите Режим IP «Static (Вручную)» из выпадающего списка и вставьте новый IP-адрес в поле «IP-адрес (CIDR)» (см. рис. 2.35). После IP-адреса обязательно указывайте маску через «/». *Пример: 192.168.10.223/24.*

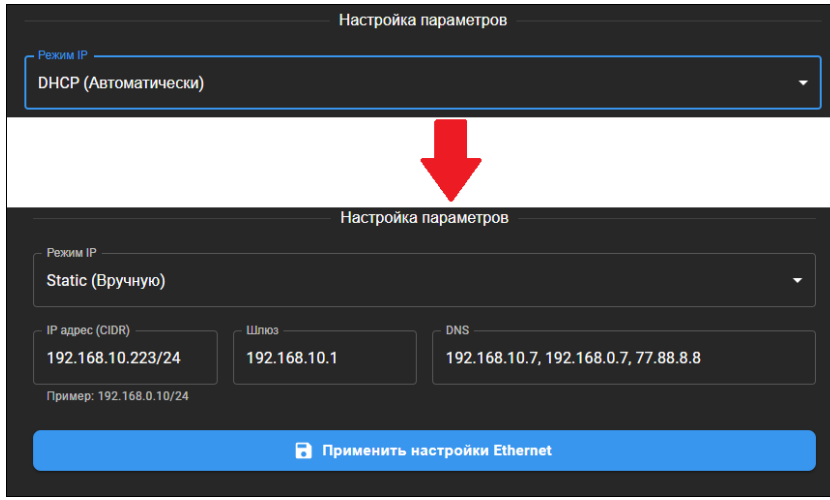


Рис. 2.35. Установка статического IP-адреса

Для применения новых параметров нажмите кнопку «Применить настройки Ethernet». В нижней части страницы появится уведомление об успешной смене IP-адреса и произойдет автоматический переход по новому адресу. После перехода по новому IP-адресу потребуется заново войти в учетную запись.

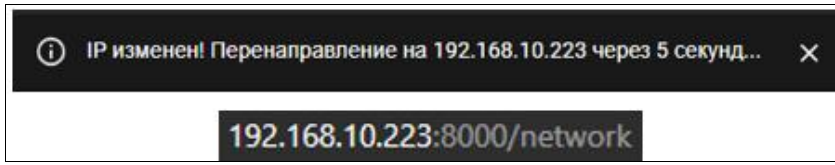


Рис. 2.36. Уведомление и адрес в адресной строке браузера

2.10.1.3. Настройка динамического IP-адреса

В нижней части страницы Настройки Ethernet измените параметр «Режим IP» с «Static (вручную)» на «DHCP (Автоматически)» (см. рис. 2.37).

Нажмите кнопку «Применить настройки Ethernet». После этого определите новый адрес шлюза с помощью ПО RealLab Scanner PLCs либо Advanced IP Scanner.

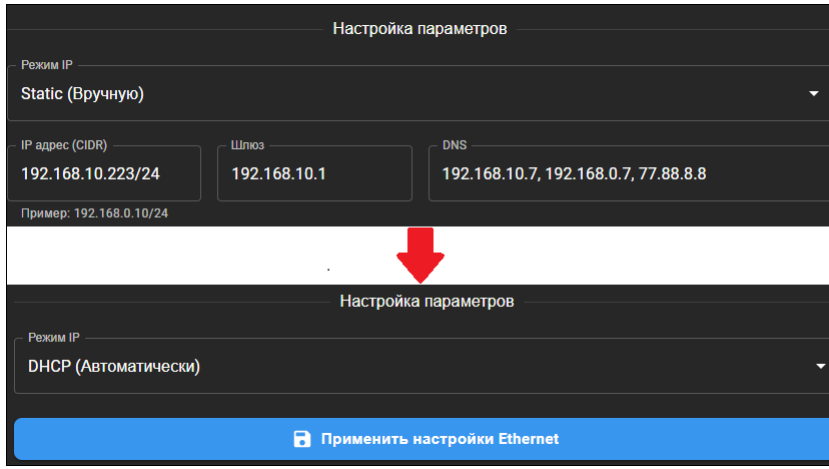


Рис. 2.37. Изменение режима получения IP-адреса на автоматический (DHCP)

2.10.2. Настройка Wi-Fi

При переходе на вкладку «Wi-Fi» выполняется автоматическое сканирование сети, при включенном Wi-Fi это занимает несколько секунд. В верхней части расположен переключатель Wi-Fi. Кликните по нему для изменения состояния модуля Wi-Fi (подписан как «Вкл/Выкл» на рис. 2.43).

Рядом с переключателем отображается MAC-адрес Wi-Fi модуля.

На вкладке Wi-Fi в веб-интерфейсе также находятся кнопки действий:

- сканировать: выполняет сканирование сети (примерно 3-5 сек.);
- сохраненные: открывает список сохраненных Wi-Fi-сетей с возможностью их удаления. Для удаления необходимо нажать на значок напротив удаляемой сети (см. рис. 2.44).

Для подключения к сети Wi-Fi выполните сканирование сети, если это необходимо, и кликните по строке с названием сети, к которой необходимо подключиться.

Если сеть не защищена паролем, отобразиться окно с двумя кнопками: «Отмена» и «Подключиться» (см. рис. 2.38).

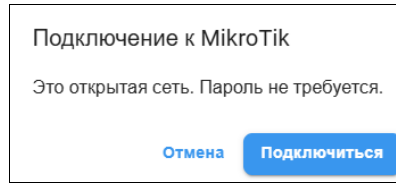


Рис. 2.38. Подключение к сети без пароля

Введите пароль, если подключаетесь к этой защищенной сети впервые и ее нет в списке сохраненных. Нажмите «Подключиться» после ввода пароля (см. рис. 2.39).

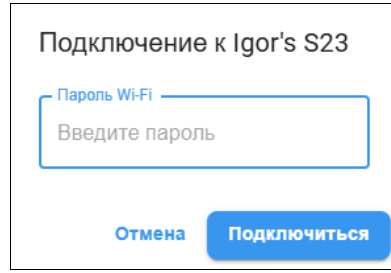


Рис. 2.39. Подключение к защищенной сети

Если пароль будет введен верно, в нижней части экрана появится соответствующее уведомление. В противном случае, появится ошибка.

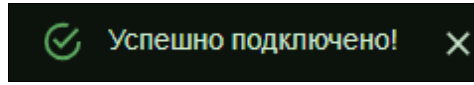


Рис. 2.40. Уведомление об успешном подключении к сети

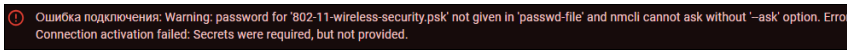


Рис. 2.41. Сообщение при неправильно введенном пароле

При попытке подключиться к сети, к которой ранее выполнялось подключение (она находится в списке сохраненных), достаточно нажать «Подключиться» без ввода пароля (см. рис. 2.42).

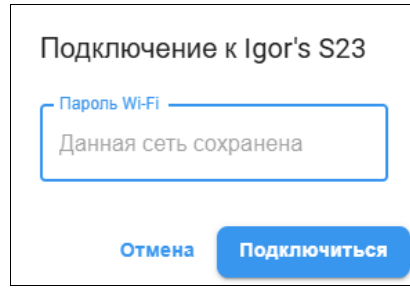


Рис. 2.42. Подключение к сохраненной сети

Справа от MAC-адреса отображается имя сети, к которой подключен шлюз по Wi-Fi. Также в списке обнаруженных Wi-Fi-сетей, напротив имени сети, к которой шлюз подключен, отображается надпись «Подключено». Для отключения от точки доступа Wi-Fi, к которой на данный момент подключен шлюз, необходимо нажать на значок справа от ее названия.

После перезагрузки шлюз автоматически подключается к последней подключенной точке доступа Wi-Fi.

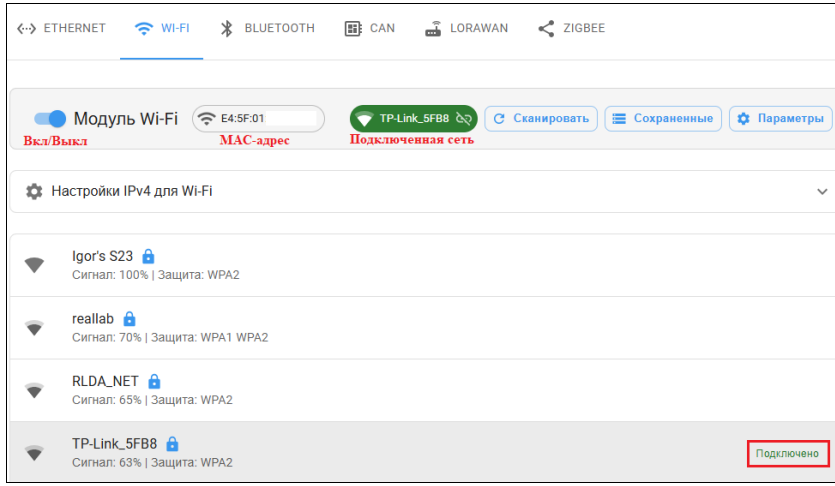


Рис. 2.43. Вкладка Wi-Fi

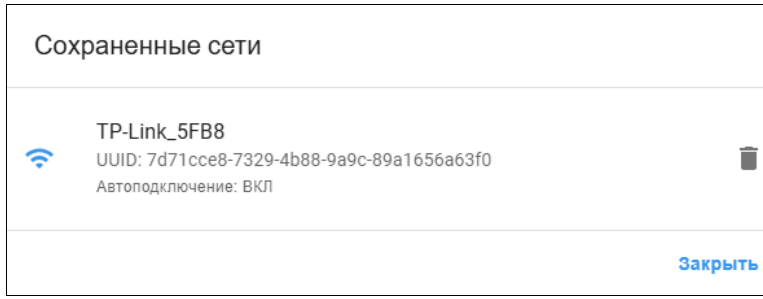


Рис. 2.44. Список сохраненных сетей

2.10.2.1. Настройки IPv4 для Wi-FI

На вкладке Wi-Fi есть дополнительные параметры для настройки соединения по Wi-Fi, вкладка «Настройки IPv4 для Wi-Fi» (см. рис. 2.45).

Кликните по списку «Настройки IPv4 для Wi-Fi», чтобы открыть их. Внутри отображаются данные об активном подключении к сети: метод получения IP-адреса, IP-адрес, маска, MAC-адрес, список DNS-серверов, адрес шлюза.

Также есть возможность настройки статического/динамического IP, аналогично п. 2.10.1.2.

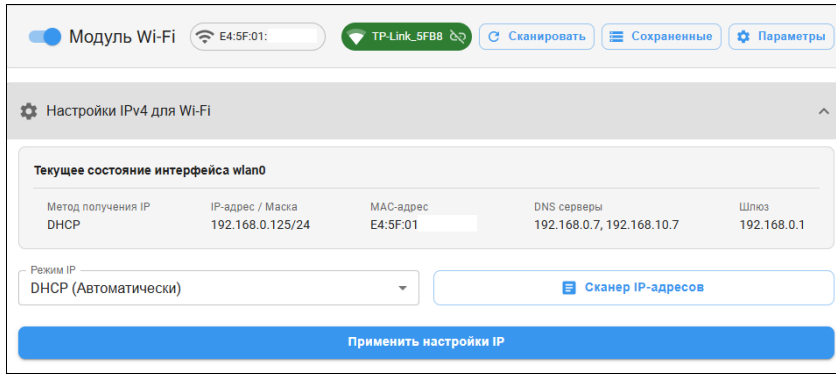


Рис. 2.45. Настройки IPv4 для Wi-Fi

2.10.2.2. Параметры Wi-Fi

Кнопка диалога «Параметры» находится в верхней части вкладки «Wi-Fi».

Параметры позволяют выбрать используемую антенну (внутреннюю или внешнюю) и выбрать режим Wi-Fi (стандартный или режим точки

доступа) *(временно недоступно)* (см. рис. 2.46). Для сохранения параметров нажмите кнопку применить.

ВАЖНО! Для применения параметров используемой антенны требуется перезагрузка устройства.

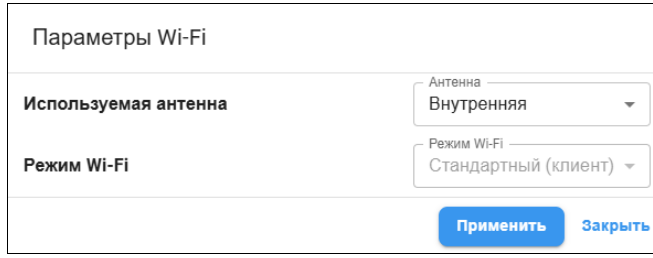


Рис. 2.46. Параметры Wi-Fi

2.10.3. Bluetooth

На вкладке Bluetooth можно выполнить Bluetooth-сканирование и просмотреть список сопряженных устройств.

Включенный по умолчанию BLE-Server позволяет удаленно считывать IP-адрес и имя хоста шлюза. Для этого используется программа-сканер nRF Connect или ее аналоги на любом Bluetooth-устройстве.

2.10.3.1. Определение IP-адреса шлюза с помощью BLE

Откройте программу nRF Connect, например, на смартфоне и найдите шлюз по его имени хоста (NLS-Gateway-*), нажмите «Подключиться/Connect» (см. рис. 2.47). Для упрощения поиска используйте фильтр по названию устройства – «NLS».

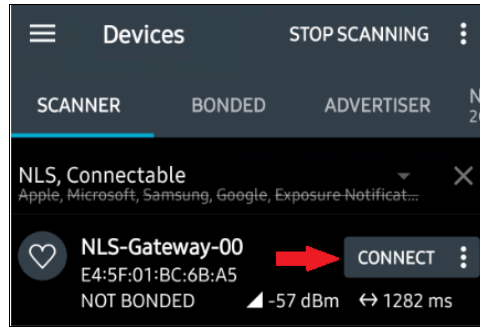


Рис. 2.47. Подключение к BLE-серверу

Далее выберите из списка пункт с UUID «12345678-1234-5678-1234-567812345678», появится 2 параметра, которые можно считать. Первый – IP-адрес, второй – имя хоста. Нажмите на кнопку «Считать (Read)» для получения данных (см. рис. 2.48).

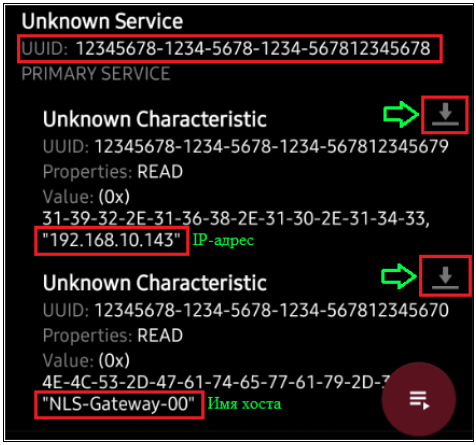


Рис. 2.48. Чтение IP-адреса и имени хоста

2.10.3.2. Сканирование и сопряжение устройств

Перейдите на вкладку «Сеть», выберите Bluetooth в веб-конфигураторе шлюза. Включите Bluetooth, если он отключен. Нажмите кнопку «Сканировать» (см. рис. 2.49).

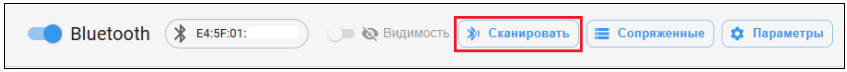


Рис. 2.49. Сканирование Bluetooth-устройств

В течение 10 секунд появится список обнаруженных устройств. Нажмите на кнопку «Сопряжение» напротив имени необходимого устройства (см. рис. 2.50).

Рис. 2.50. Сопряжение с устройством

На подключаемом устройстве и в веб-конфигураторе появится 6-значный код. Нажмите «Установить сопряжение» (см. рис. 2.51).

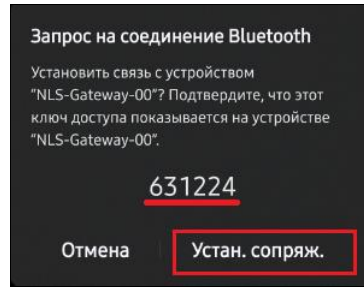


Рис. 2.51. Код на устройстве

Рис. 2.52. Код в веб-конфигураторе

В результате устройство появится в списках сопряженных устройств (см. рис. 2.53, рис. 2.54). Для удаления из списка сопряженных устройств, нажмите на значок удаления в веб-конфигураторе напротив названия устройства, с которым хотите разорвать подключение (см. рис. 2.54).

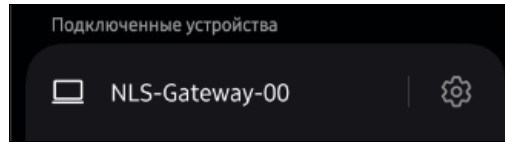


Рис. 2.53. Шлюз в списке сопряженных устройств

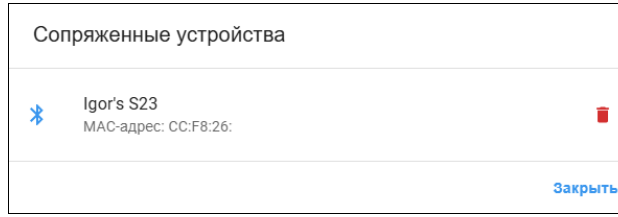


Рис. 2.54. Список сопряженных устройств в веб-конфигураторе

2.10.3.3. Изменение параметров Bluetooth

Нажмите кнопку «Параметры» в верхней части вкладки Bluetooth (см. рис. 2.49), появится окно управления BLE-сервером (см. рис. 2.55).

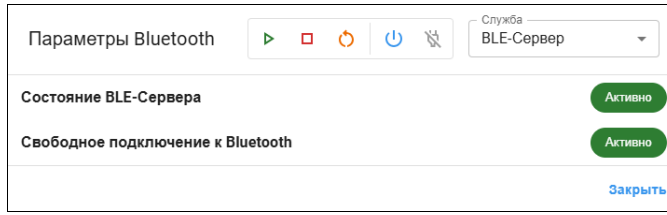


Рис. 2.55. Окно параметров Bluetooth

В шапке диалога доступен выбор настраиваемой службы «BLE-сервер» или «Свободное подключение». Слева от выпадающего списка доступны кнопки действий для выбранной службы (старт, стоп, перезапуск, включение и отключение автозапуска).

По умолчанию обе службы активны и находятся в автозапуске.

BLE-Сервер позволяет узнать IP-адрес и имя хоста устройства с любого устройства с поддержкой Bluetooth (подробнее в п. 2.10.3.1). Чтобы отключить его, остановите службу «BLE-сервер» и отключите ее автозапуск.

Рис. 2.56. Остановка и отключение автозапуска BLE-сервера

Свободное подключение к Bluetooth позволяет другим устройствам сопрягаться со шлюзом по Bluetooth без подтверждения кода доступа на самом шлюзе. Если отключить данную службу, то попытка сопряжения со шлюзом с другого устройства будет отклоняться и будет работать только сопряжение, запрос на которое будет отправлен с самого шлюза.

ВАЖНО! Состояние службы свободного подключения к Bluetooth **не влияет** на подключение к BLE-серверу через nRF Connect и подобные приложения.

Для запуска службы и ее добавления в автозапуск, выберите нужную службу, нажмите кнопки «Запустить» и «Включить автозапуск» (см. рис. 2.57).

Рис. 2.57. Запуск службы и добавление в автозапуск

2.10.4. Настройка CAN

Страница настройки CAN-интерфейсов разделена на две части.

Первая часть позволяет настроить сам CAN-интерфейс, а вторая – сконфигурировать его по протоколам SDO, NMT, LSS. В верхней части страницы отображается блок с информацией о текущем состоянии выбранного CAN-интерфейса.

Рис. 2.58. Отображение состояния выбранного интерфейса

2.10.4.1. Изменение параметров CAN-интерфейса

Для изменения состояния выбранного интерфейса укажите его режим (включен или выключен), введите скорость в битах в секунду (например, 125000), укажите время восстановления в миллисекундах (по умолчанию 1000) и нажмите кнопку «Применить» (см. рис. 2.59).

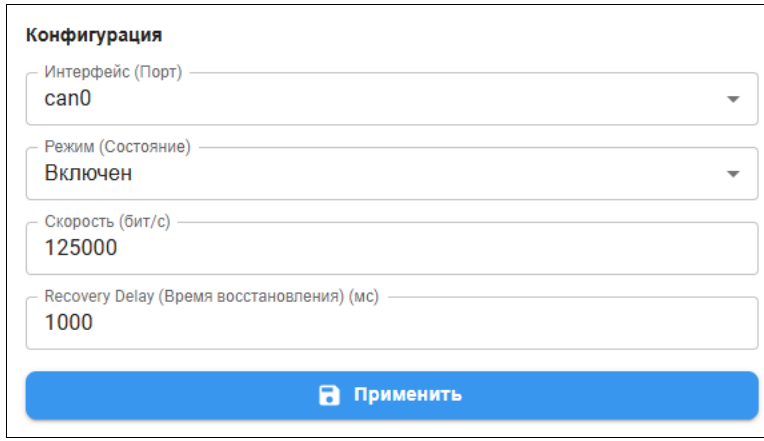


Рис. 2.59. Раздел конфигурации CAN-интерфейсов

Для отключения интерфейса установите режим «Выключен» (см. рис. 2.59) и нажмите кнопку «Применить».

2.10.4.2. Изменение параметров CAN-модуля (NMT, LSS, SDO)

Настройте интерфейс can0, установите режим «Включен» и скорость, соответствующую скорости модуля. Время восстановления оставьте равным 1000 мс.

ВАЖНО! Рекомендуется настраивать каждый модуль отдельно в режиме подключения «точка-точка».

На вкладке «CAN» страницы «Сеть» ниже раздела конфигурации находится форма для ввода ID настраиваемого модуля и раздел конфигурации состояния модуля по протоколу NMT (см. рис. 2.62).

Включите отладку через candump, на этой же странице находится окно «CAN Monitor». Нажмите кнопку «Старт» для начала отладки конфигурации CAN-модуля (см. рис. 2.60).

Подключите настраиваемый CAN-модуль к порту *can0*, в окне отладки появится кадр BootUp (см. рис. 2.60).

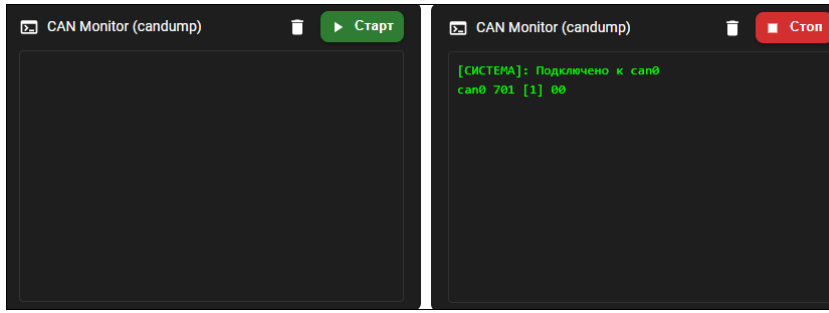


Рис. 2.60. Окно отладки конфигурации CAN-модуля

Введите ID настраиваемого модуля (см. рис. 2.62). Если ID неизвестен, воспользуйтесь окном отладки. При правильно выбранной скорости передачи данных после подключения в окне отладки появляется кадр BootUp (см. рис. 2.61).

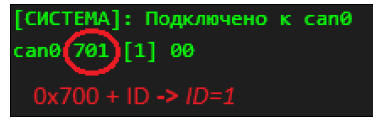


Рис. 2.61. ID-модуля в отладочном окне

С помощью протокола NMT можно перевести модуль в состояния «Работа», «Остановка» и «Конфигурация», также можно выполнить сброс узла («СбросУ») или сброс подключения к модулю («СбросП»).

Для настройки параметров модуля CAN переведите его в состояние конфигурации, для этого нажмите кнопку «Конфиг» в разделе конфигурации NMT (см. рис. 2.62).

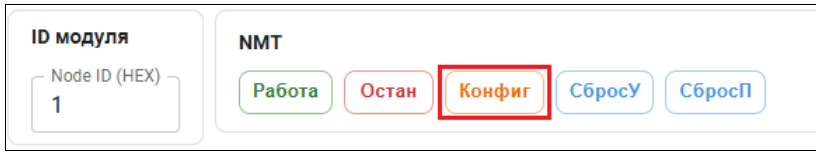


Рис. 2.62. Разделы ввода ID и конфигурации по NMT

Конфигурация по SDO позволяет изменить параметры SDO настраиваемого модуля.

ВАЖНО! Для настройки SDO модуль должен находиться в состоянии конфигурации (Pre-Operational).

Пример – настройка Heartbeat. Для этого в разделе SDO введите индекс 1017, суб-индекс 00, значение 0 и прочитайте текущее значение Heartbeat кнопкой «Чтение (R)» (см. рис. 2.63).

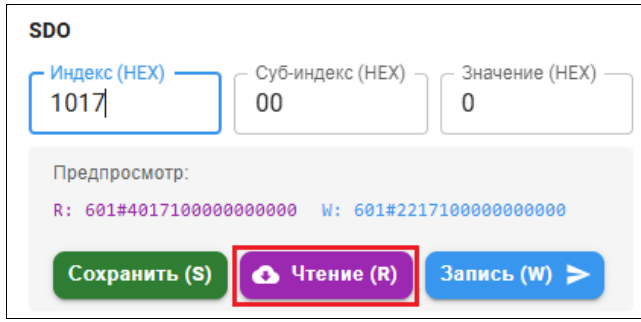


Рис. 2.63. Ввод параметров SDO для чтения Heartbeat

В окне отладки отобразится отправленная команда и ответ модуля. В данном случае значение Heartbeat на модуле равно 0 мс, Heartbeat выключен (см. рис. 2.64).

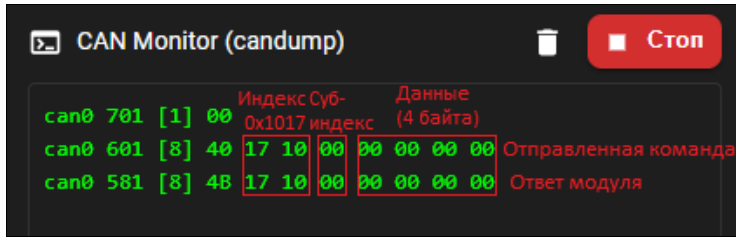


Рис. 2.64. Чтение Heartbeat модуля

Для настройки Heartbeat на отправку каждые 500 мс введите «1F4» (500 в шестнадцатеричном виде) в поле «Значение» и нажмите кнопку «Отправить (W)». После того как модуль ответит на отправленную команду, нажмите «Сохранить» (см. рис. 2.65). После сохранения модуль перезагрузится.

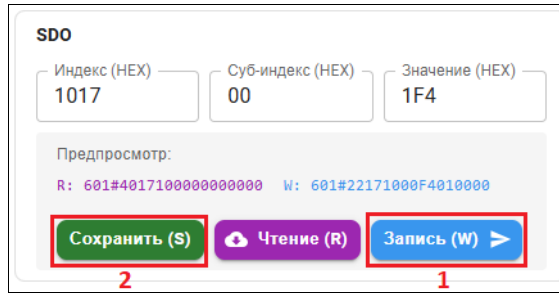


Рис. 2.65. Запись значения

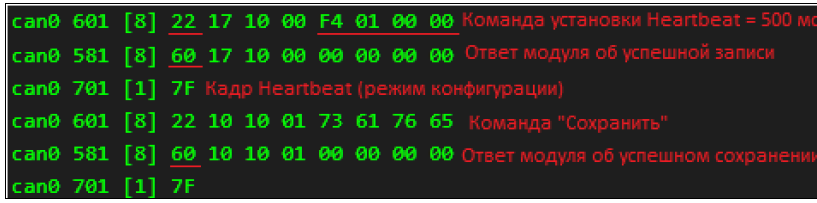


Рис. 2.66. Окно отладки во время сохранения нового значения Heartbeat

Если после включения Heartbeat перевести модуль в режим работы через NMT, то в отладочном окне появятся кадры «05», что означает отправку Heartbeat в рабочем режиме (см. рис. 2.67).

```
can0 701 [1] 7F Heartbeat - режим конфигурации
can0 000 [2] 01 01 Переход в рабочий режим
can0 701 [1] 05 Heartbeat - рабочий режим
can0 701 [1] 05
```

Рис. 2.67. Отправка Heartbeat в рабочем режиме

Конфигурация по LSS позволяет настроить ID и скорость модуля.

ВАЖНО! Для настройки по протоколу LSS модуль должен находиться в состоянии конфигурации (Pre-Operational). Если модуль находится в рабочем состоянии по NMT, то в режим конфигурации LSS он перейти не сможет. Перед этим переведите модуль в режим конфигурации по NMT.

Для изменения параметров модуль необходимо перевести в режим конфигурации LSS, для этого нажмите кнопку «Конфиг» в разделе LSS.

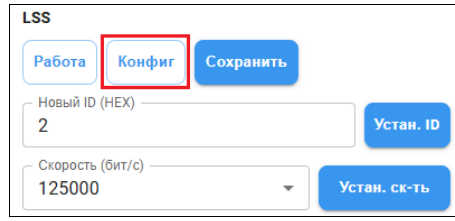


Рис. 2.68. Раздел конфигурации LSS

Установите желаемые параметры ID и (или) скорости. Нажмите на кнопку установки соответствующего параметра, затем нажмите «Сохранить». Модуль автоматически перейдет в рабочий режим LSS.

Для изменения ID модуля необходимо перевести модуль в режим конфигурации LSS, ввести новое значение ID в шестнадцатеричном формате, нажать кнопку «Устан. ID», затем нажать кнопку «Сохранить» (см. рис. 2.69).

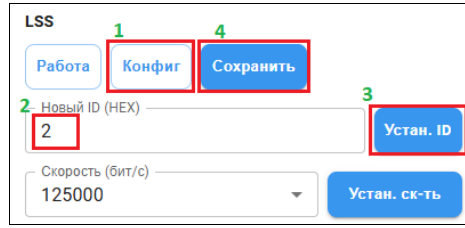


Рис. 2.69. Пример установки ID модуля

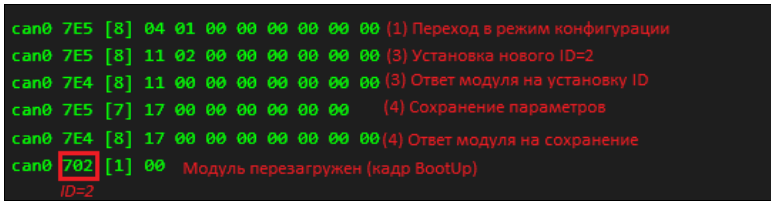


Рис. 2.70. Отладочное окно в процессе установки ID

2.10.5. LoRaWAN

Вкладка LoRaWAN предназначена для настройки взаимодействия ПО Chirpstack с LoRaWAN-концентратором в части параметров, отсутствующих в веб-интерфейсе.

В верхней части страницы находятся кнопки «Редактор частот» и «Логирование и управление службами» (см. рис. 2.71).

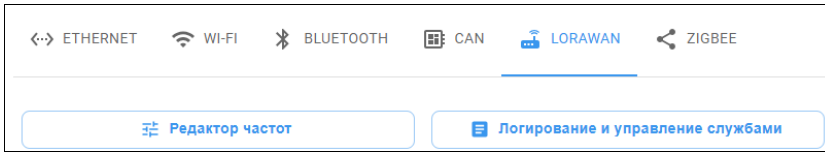


Рис. 2.71. Верхняя часть вкладки LoRaWAN

Отдельно настраиваются общие параметры:

- Chirpstack ConcentratorD (регион, характеристика усиления антенны, уровень логирования, использование GNSS и т.д., см. рис. 2.72);
- Chirpstack Network Server (порт веб-интерфейса, максимальное время декодирования для парсинга пакетов, формат передаваемых данных и т.д., см. рис. 2.73);
- Chirpstack MQTT Forwarder – ретранслятор пакетов LoRa на MQTT-брокер (уровень логирования, формат данных, сокеты получения данных, см. рис. 2.74).
- Chirpstack Gateway Mesh для определения роли шлюза, Ретранслятор/Граничный.

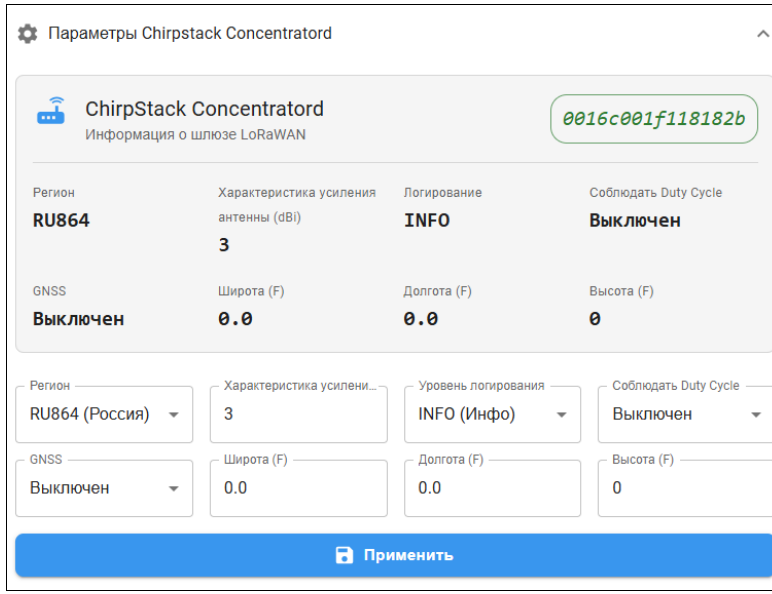


Рис. 2.72. Параметры концентратора LoRaWAN

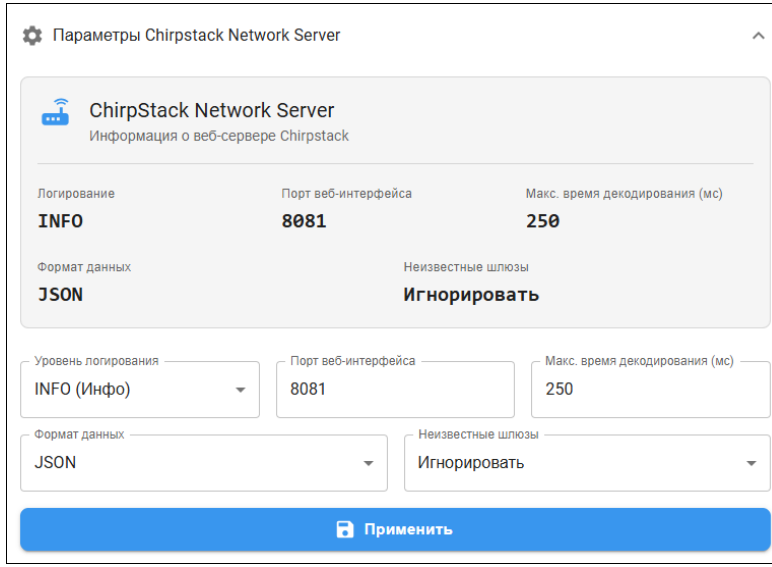


Рис. 2.73. Параметры сервера Chirpstack

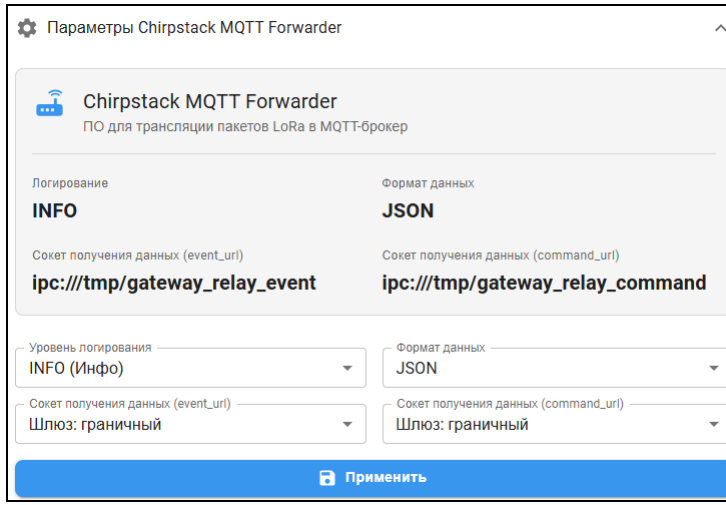


Рис. 2.74. Параметры Chirpstack MQTT Forwarder

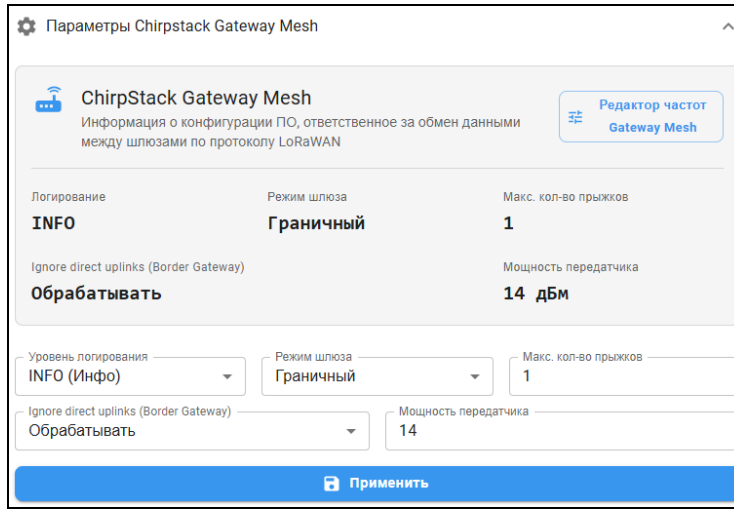


Рис. 2.75. Параметры Chirpstack Gateway Mesh

2.10.5.1. Описание основных параметров Chirpstack Concentratord

Параметр **Регион** изменяет частотный план в соответствии с выбранным значением (см. рис. 2.76).

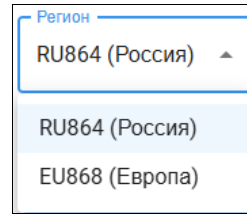


Рис. 2.76. Выпадающий список «Регион»

Параметр **Характеристика усиления антенны (dBi)** влияет на регулировку мощности передатчика: чем больше значение данного параметра, тем меньше мощность передатчика (регулировка происходит автоматически). Укажите подлинное значение характеристики усиления антенны. Значение можно найти в документации к приобретенной антенне.

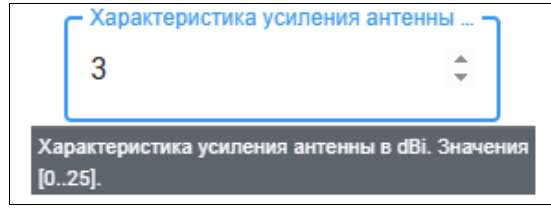


Рис. 2.77. Характеристика усиления антенны (dBi)

Параметр **GNSS** предназначен для использования модуля GPS. Если значение параметра «Включен», то будут использоваться координаты местоположения, получаемые с модуля GPS. В противном случае будут использоваться координаты, введенные вручную (параметры **Широта(F), Долгота(F), Высота(F)**) (см. рис. 2.78).

ВАЖНО! Не используйте данный параметр в случае отсутствия модуля GPS в приобретенной модификации устройства.

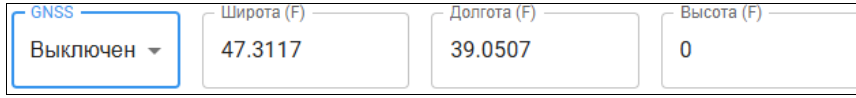


Рис. 2.78. Параметры GNSS

Данные параметры транслируются в конфигурационный файл Chirpstack и влияют на отображение местоположения модуля только в веб-интерфейсе Chirpstack (см. рис. 2.79). Координаты для примера были выбраны случайно.

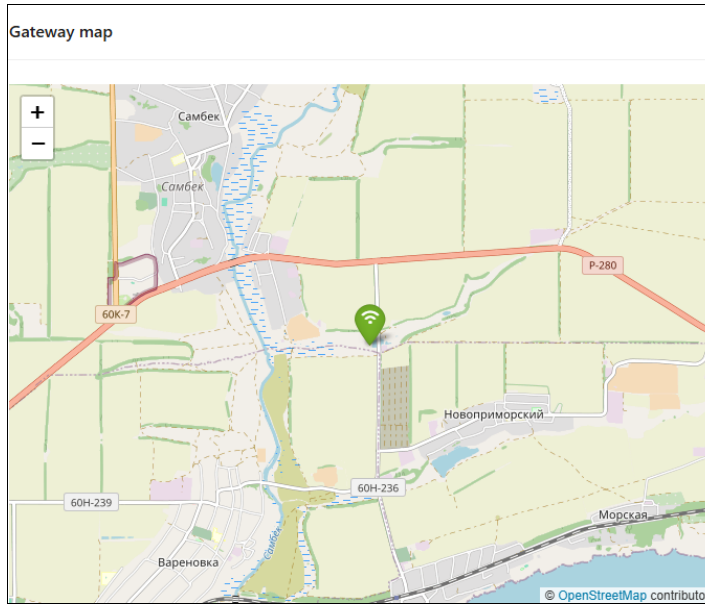


Рис. 2.79. Карта в Chirpstack - Dashboard

Параметр **Соблюдать Duty Cycle** отвечает за соблюдение ограничения на использование частот по времени, если он включен, то контроль за превышением Duty Cycle осуществляется. При отключенном значении данного параметра осуществляется только отслеживание использования Duty Cycle без блокировки пакетов при его превышении.

ВАЖНО! На данный момент поддерживается соблюдение DC только для региона EU868.

2.10.5.2. Описание основных параметров Chirpstack (Network Server)

Порт веб-сервера позволяет изменить порт, на котором запущен веб-конфигуратор Chirpstack. Значение по умолчанию: 8081.

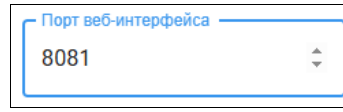


Рис. 2.80. Порт веб-сервера Chirpstack

Макс. время декодирования – максимальное время декодирования для парсинга пакетов LoRa. Алгоритм парсинга пакета записывается в

«Device Profiles» – «Имя_устройства» – вкладка «Payload codec» в веб-интерфейсе Chirpstack.

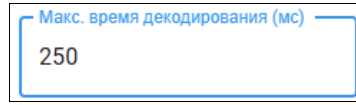


Рис. 2.81. Максимальное время декодирования пакета

Формат данных – формат передаваемых данных: JSON либо Protobuf.

Неизвестные шлюзы – при установленном значении «Игнорировать» кадры от неизвестных шлюзов будут проигнорированы. В противном случае, данный шлюз будет их обрабатывать.

2.10.5.3. Описание основных параметров Chirpstack MQTT Forwarder

Формат данных – формат передаваемых данных: JSON либо Protobuf.

Сокеты получения данных – сокеты, по которым MQTT Forwarder получает данные для их отправки в MQTT-брокер. Сокеты должны выбираться в соответствии с выбранным режимом шлюза в параметрах Gateway Mesh.

Рис. 2.82. Сокеты получения данных

2.10.5.4. Описание основных параметров Chirpstack Gateway Mesh

ПО Chirpstack Gateway Mesh отвечает за обмен данными между шлюзами по протоколу LoRaWAN и позволяет выбрать режим шлюза:

- граничный – шлюз собирает данные с датчиков и передает в MQTT-брокер (на верхний уровень);
- ретранслятор – шлюз передает данные другим шлюзам на выбранных частотах и на выбранное количество «прыжков» (кол-во пересылок) по протоколу LoRaWAN.

ВАЖНО! При изменении режима шлюза также измените параметры сокетов в параметрах Chirpstack MQTT Forwarder! Если шлюз в режиме ретранслятора, MQTT Forwarder рекомендуется отключить. Сделать это можно через диалог «Логирования и управления службами». Остановите службу и исключите ее из автозагрузки. Более подробно см. п. 2.10.5.6.

Изменение частот, на которых производится обмен данными между шлюзами, выполняется в диалоге, вызываемом кнопкой «Редактор Частот Gateway Mesh» (см. рис. 2.85).

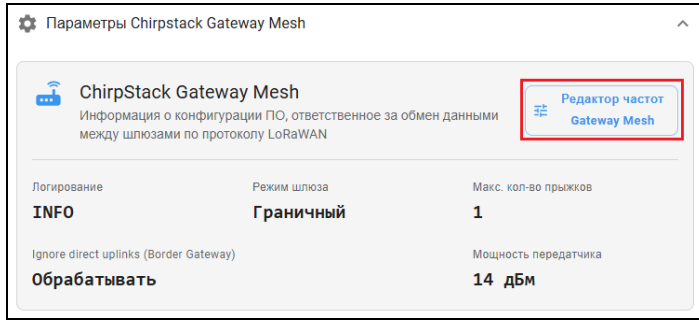


Рис. 2.83. Кнопка вызова редактора частот Gateway Mesh

В редакторе можно добавить или удалить частоты, через которые будет происходить обмен данными между шлюзами. После изменения частот нажмите «Готово» и примените изменения кнопкой «Применить» в секции «Параметры Chirpstack Gateway Mesh». Частоты регулируются в файле выбранного в секции параметров Chirpstack Concentratord региона.

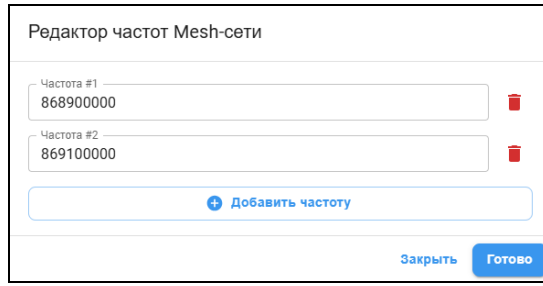


Рис. 2.84. Редактор частот Gateway Mesh

2.10.5.5. Изменение параметров частотного плана

Для редактирования частот, входящих в выбранный частотный план (параметр «Регион» во вкладке параметров Chirpstack Concentratord) нажмите кнопку «Редактор частот» в верхней части вкладки LoRaWAN.

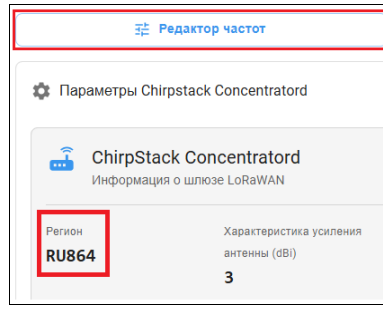


Рис. 2.85. Кнопка “Редактор частот”

В редакторе частот находится следующие вкладки:

- общие параметры региона для настройки мощности передатчика и параметра ADR;
- параметры стандартных каналов, по которым шлюз принимает данные;
- специальные каналы (LoRa Std, FSK);
- маяки времени (параметры класса Б) для дополнительных параметров для устройств LoRaWAN класса Б (для работы с устройствами этого класса требуется модификация шлюза с GPS-модулем).

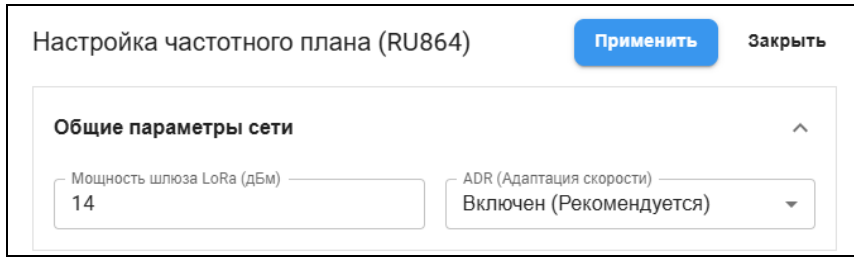


Рис. 2.86. Окно редактора частот

Параметры частотного плана позволяют настроить дополнительные частоты, параметры Data Rate и Spreading Factor, ширины канала, модуляции. Всего может быть добавлено 8 каналов: 2 основных (всегда активны) и 6 дополнительных.

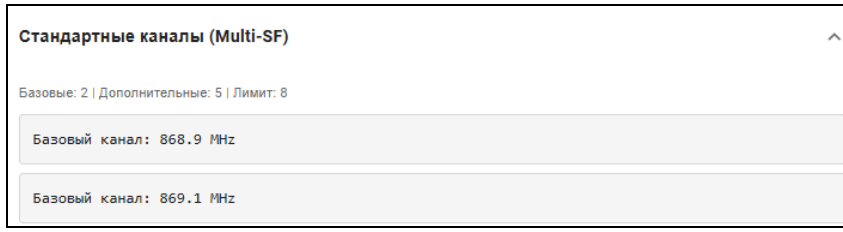


Рис. 2.87. Основные каналы частотного плана RU864

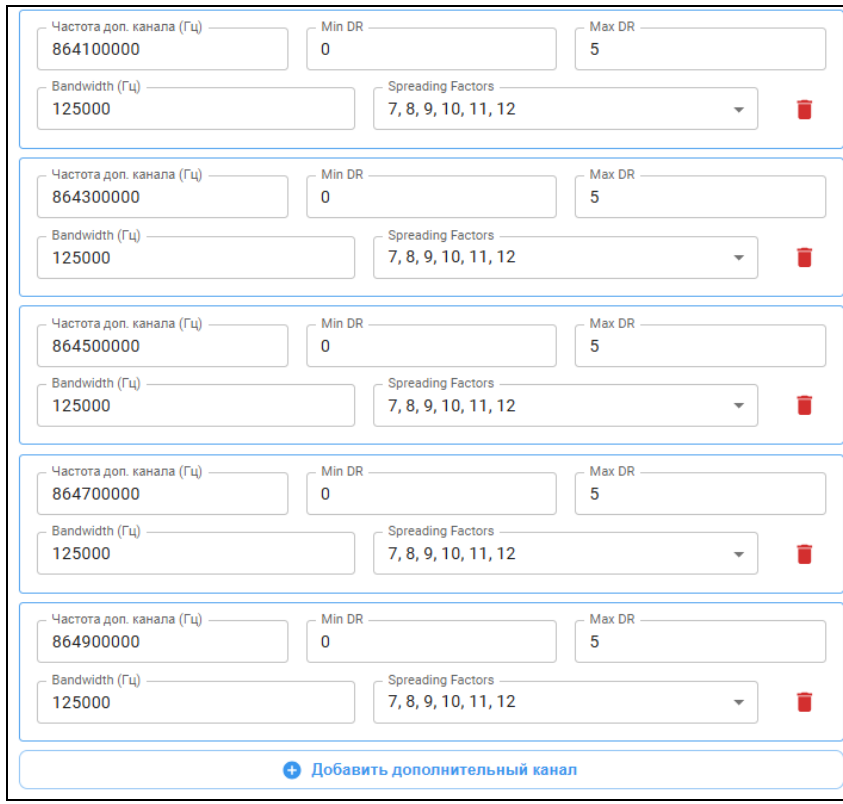


Рис. 2.88. Дополнительные каналы частотного плана RU864

Для удаления канала используйте кнопку , для создания нового канала – кнопку «Добавить дополнительный канал» в нижней части вкладки. Укажите частоту доп. канала в Гц. Без необходимости не изменяйте значения остальных параметров канала, установленных по умолчанию.

Также присутствует настройка специальных каналов – LoRa Standard и FSK (Frequency Shift Keying). По умолчанию она настроена в параметрах региона EU868 (см. рис. 2.89), настройка специальных каналов в параметрах региона RU864 необязательна.

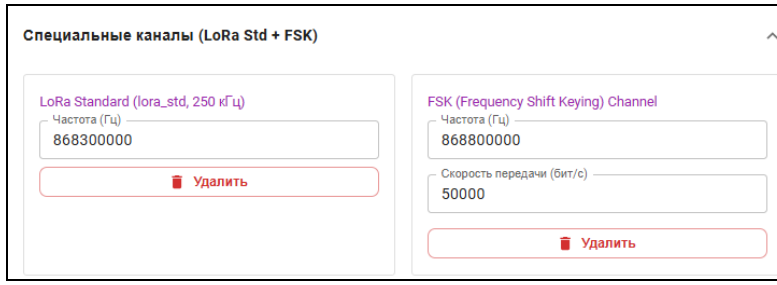


Рис. 2.89. Параметры специальных каналов для региона EU868

После изменения любых параметров – каналов, частот или мощности передатчика, выполните сохранение, нажав на кнопку «Применить» (см. рис. 2.90).

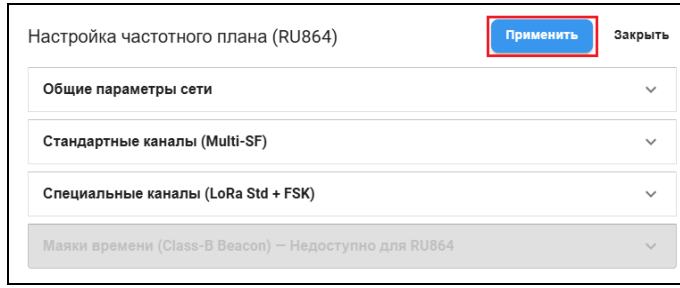


Рис. 2.90. Сохранение параметров

2.10.5.6. Логирование и управление службами Chirpstack

Для открытия меню логирования и управления службами Chirpstack необходимо кликнуть на кнопку «Логирование и управление службами». Откроется окно поверх страницы (см. рис. 2.91).

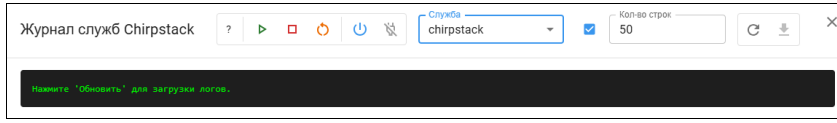


Рис. 2.91. Окно логирования и управления службами Chirpstack

В шапке окна журнала служб Chirpstack выберите службу, для которой нужно посмотреть логи или изменить ее состояние.

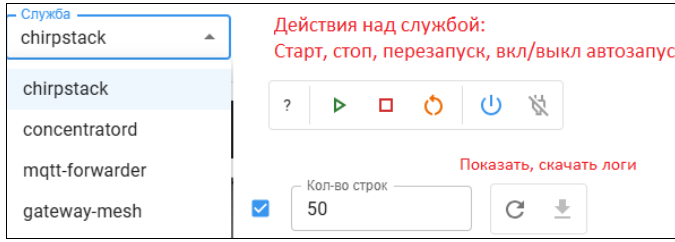


Рис. 2.92. Подробное описание окна логирования и управления службами Chirpstack

При необходимости, настройте ограничение на вывод и скачивания логов: укажите количество строк с конца файла, которые будут отображены или скачаны (см. рис. 2.93). Для скачивания всех логов выбранной службы, снимите галочку возле формы ввода количества строк.

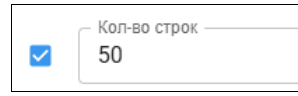


Рис. 2.93. Ограничение вывода логов

После выбора службы для просмотра логов нажмите кнопку в правой части шапки окна. После этого логи отобразятся в основной части открытого окна (см. рис. 2.94).

```
Apr 17 17:51:47 raspberrypi chirpstack[936]: 2026-04-17T14:51:47.505985Z  INFO
stats{gateway_id=0016c001f118182b}: chirpstack::storage::metrics: Metrics saved
name=gw:0016c001f118182b aggregation=MONTH
Apr 17 17:52:03 raspberrypi chirpstack[936]: 2026-04-17T14:52:03.651986Z  INFO
chirpstack::gateway::backend::mqtt: Message received from gateway region_id="ru864"
topic=ru864/gateway/0016c001f118182b/event/up qos=AtMostOnce json=true
Apr 17 17:52:03 raspberrypi chirpstack[936]: 2026-04-17T14:52:03.829088Z  INFO
chirpstack::gateway::backend::mqtt: Message received from gateway region_id="ru864"
topic=ru864/gateway/0016c001f118182b/event/up qos=AtMostOnce json=true
Apr 17 17:52:03 raspberrypi chirpstack[936]: 2026-04-17T14:52:03.861590Z  INFO
up{deduplication_id=6a429cc6-57d8-478c-a5c6-e9c35dd9911f}: chirpstack::uplink: Uplink
received f_type=UnconfirmedDataUp
```

Рис. 2.94. Логи Chirpstack

ВАЖНО! Перед скачиванием логов отобразите их с помощью нажатия на кнопку отображения ( ).

Для скачивания логов нажмите на кнопку , после этого файл с логами будет сохранен в загрузки устройства, с которого выполнен вход в веб-конфигуратор RealLab! (см. рис. 2.95).

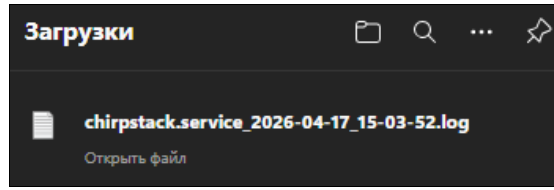


Рис. 2.95. Результат скачивания логов

2.10.6. MQTT

Вкладка настройки параметров MQTT содержит секции настройки параметров брокера MQTT (Mosquitto) и параметров MQTT для ПО Chirpstack.

2.10.6.1. Параметры брокера MQTT (Mosquitto)

Секция настройки параметров брокера MQTT позволяет изменить следующие параметры:

- базовые настройки (порт брокера);
- параметры безопасности (разрешение анонимного входа, авторизация, логи и пароль);
- параметры шифрования трафика и перевыпуск сертификатов.

Данная секция содержит кнопки обновления состояния текущих параметров и открытия диалога логирования и управления службой брокера MQTT (см. рис. 2.96).

Рис. 2.96. Кнопки обновления параметров и открытия диалога логирования

Основной функционал:

Порт брокера – MQTT-брокер будет развернут на выбранном порте. Значение по умолчанию: 1883.

Разрешить анонимный вход – значение «Разрешить» разрешает подключение к брокеру без параметров авторизации (логина и пароля). При включении авторизации данный параметр принимает значение «Запретить».

Авторизация – при включении данного параметра требуется задать имя пользователя и пароль для подключения к брокеру. При включении данного параметра анонимная авторизация станет невозможной до его отключения. После задания логина и пароля для подключения к брокеру MQTT поле ввода пароля всегда будет пустым. Если требуется изменить параметры брокера, введите старый пароль, который задавали ранее, или введите новый.

Шифрование трафика – данный параметр включает шифрование по протоколу TLS с использованием сертификатов.

Перевыпуск сертификатов – при подтверждении перевыпуска сертификатов, они генерируются сроком на 365 дней по путям: /etc/mosquitto/certs/ и /etc/mosquitto/ca_certificates/. После генерации сертификатов нажмите кнопку «Обновить» и включите параметр «Включить защищенное соединение», чтобы увидеть период действительности сертификатов.

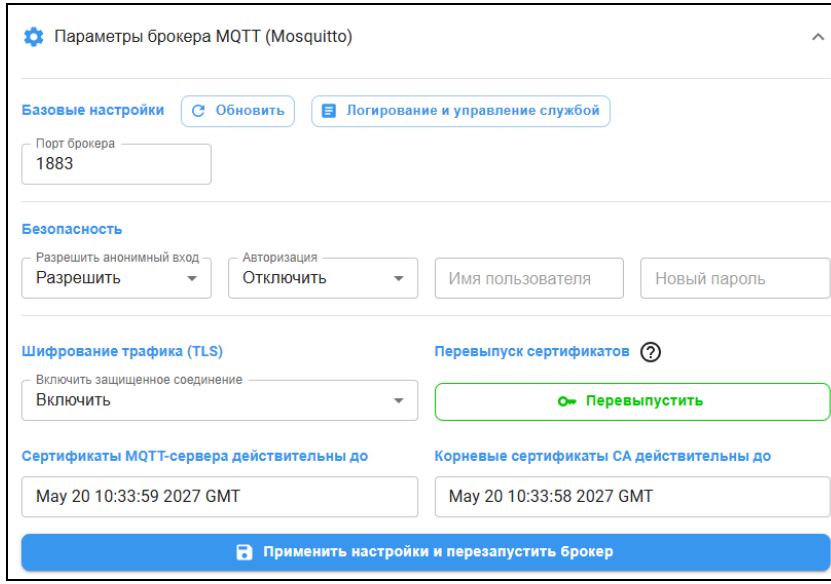


Рис. 2.97. Параметры брокера MQTT

После внесения изменений в параметры брокера нажмите кнопку «Применить настройки и перезапустить брокер». Служба брокера Mosquitto будет перезапущена.

2.10.6.2. Логирование и управление службой брокера MQTT (Mosquitto)

Для отображения диалога управления службой брокера MQTT, нажмите на кнопку «Логирование и управление службой» (см. рис. 2.96).

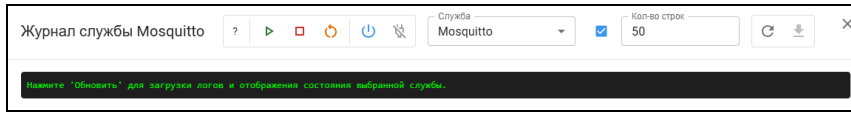


Рис. 2.98. Журнал службы Mosquitto

Кнопки управления службой позволяют запустить, остановить, перезапустить выбранную службу. Кнопки включения и отключения автозагрузки позволяют включить или отключить автоматический запуск службы после загрузки устройства. При наведении курсора на кнопку появится подсказка о действии кнопки (см. рис. 2.99).

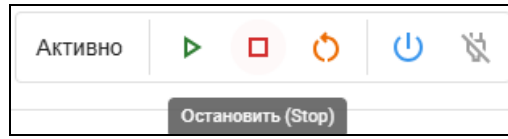


Рис. 2.99. Кнопки управления службой

Для отображения журнала выбранной службы укажите количество выводимых строк с конца, либо снимите галочку ограничения на вывод строк. В таком случае будет выведен весь журнал службы с момента последней загрузки устройства. Нажмите кнопку «Обновить» ( ).

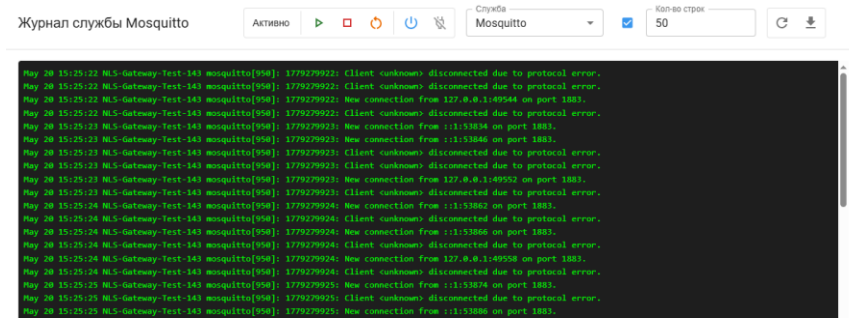


Рис. 2.100. Отображение журнала службы Mosquitto

Для скачивания логов нажмите на кнопку «Выгрузить в файл» ( ).

2.10.6.3. Параметры MQTT для Chirpstack

Секция настройки параметров MQTT для Chirpstack позволяет изменить следующие параметры:

- параметры MQTT для Chirpstack NS;
- параметры region-файлов Chirpstack NS;
- параметры Chirpstack MQTT Forwarder.

Описание общих параметров MQTT для ПО Chirpstack:

- keep Alive Interval – соединение между клиентом и сервером будет считаться разорванным, если за указанное значение параметра (время) не происходил обмен данными;
- QoS – параметр отвечает за надежность передачи данных по протоколу MQTT: 0 (максимум один раз), 1 (минимум один раз), 2 (ровно один раз). Чем выше уровень, тем медленнее скорость передачи, но выше надежность;
- адрес брокера – адрес брокера, с которого или которому отправляются данные по протоколу MQTT. При наведении на поле ввода появится подсказка о методе обмена данными с брокером, адрес которого вводится. Также доступен выбор протокола передачи данных (tcp/ssl): если подключение защищено с помощью сертификатов (включено шифрование), то используйте протокол SSL;
- имя пользователя и пароль – параметры для подключения к MQTT-брокеру. Пароль после задания и повторного обновления страницы отображаться не будет. Для внесения изменений введите пароль заново.

Описание параметров MQTT для Chirpstack NS:

- command-топик – в данный топик MQTT-брокера отправляются команды для конечных устройств;
- event-топик – в данный топик MQTT-брокера отправляются данные о событиях от конечных устройств.

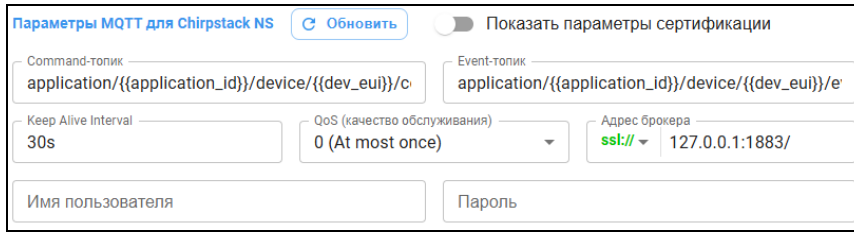


Рис. 2.101. Параметры MQTT для Chirpstack NS

Описание параметров MQTT для region-файлов Chirpstack NS:

- Clean Session – параметр определяет, должен ли MQTT-брокер запоминать состояние сессии клиента при разрыве соединения.

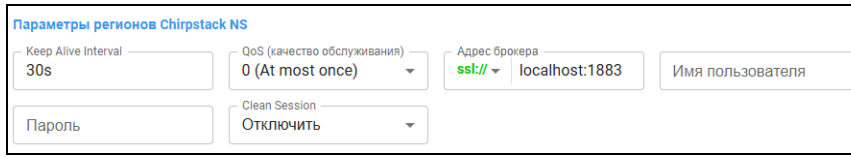


Рис. 2.102. Параметры MQTT для регионов Chirpstack NS

Описание параметров MQTT для Chirpstack MQTT Forwarder:

- интервал переподключения – каждое указанное время будет происходить попытка Chirpstack MQTT Forwarder подключиться к MQTT-брокеру в случае возникновения ошибки при прошлом подключении.

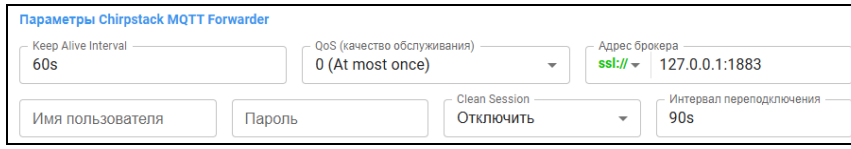


Рис. 2.103. Параметры MQTT для Chirpstack MQTT Forwarder

Также поддерживается настройка параметров сертификатов для ПО Chirpstack. Чтобы отобразить параметры сертификатов Chirpstack, нажмите на переключатель «Показать параметры сертификации» (см. рис. 2.104)

Рис. 2.104. Переключатель отображения параметров сертификации

Пример заполнения параметров сертификатов отображен на рис. 2.105.

Рис. 2.105. Параметры сертификатов ПО Chirpstack

Для применения параметров нажмите кнопку «Применить настройки и перезапустить службы Chirpstack». После применения параметров службы Chirpstack будут перезапущены.

2.10.7. Zigbee

Вкладка Zigbee на странице «Сеть» позволяет настроить основные параметры Zigbee и посмотреть журнал службы Zigbee2MQTT.

Описание параметров Zigbee, доступных для настройки:

- уровень логирования – подробность информации в журнале службы Zigbee2MQTT. Доступны значения: Debug, Info, Warning, Error;
- порт веб-интерфейса – порт, на котором запущен веб-интерфейс Zigbee2MQTT;
- веб-интерфейс Z2M – позволяет включить или отключить веб-интерфейс Zigbee2MQTT;
- интеграция с Home Assistant – при включении отправляет данные в топик «homeassistant» MQTT-брокера;
- адрес брокера MQTT – устанавливает адрес брокера MQTT, в который передаются данные с конечных устройств Zigbee;
- мощность передатчика – изменяет усиление мощности передатчика Zigbee в диапазоне -20..20 дБм.

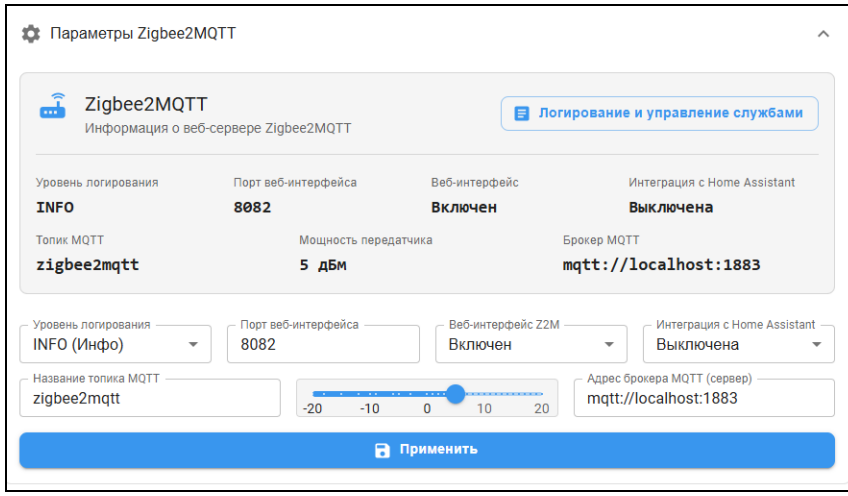


Рис. 2.106. Параметры Zigbee

После изменения параметров нажмите кнопку «Применить». Служба Zigbee2MQTT будет перезапущена. Процесс применения параметров может занять до 20 секунд.

Также есть возможность управления службой и просмотром ее журнала. Для отображения окна управления службой нажмите кнопку «Логирование и управление службами» ().

Рис. 2.107. Кнопка «Логирование и управление службами»

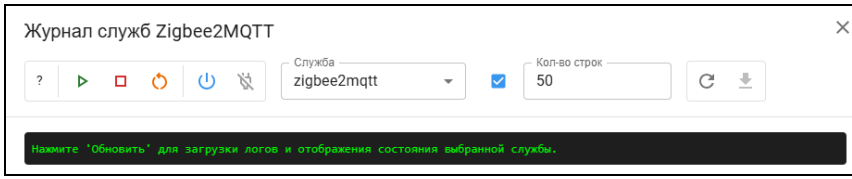


Рис. 2.108. Диалог «Логирование и управление службами»

Управление службой и просмотр журнала аналогичны п. 2.10.6.2.

3. Chirpstack

3.1. Описание ПО Chirpstack

ChirpStack – это сетевой сервер LoRaWAN с открытым исходным кодом, который можно использовать для настройки сетей LoRaWAN. ChirpStack предоставляет веб-интерфейс для управления шлюзами, устройствами и арендаторами для настройки данных интеграции с основными облачными провайдерами, базами данных и сервисами обычно используется для обработки данных устройств. ChirpStack предоставляет gRPC API, который может использоваться для интеграции или расширения ChirpStack.

Возможности Chirpstack:

- поддержка устройств классов A и C;
- поддержка адаптивной скорости передачи данных (ADR);
- логирование кадров LoRaWAN в реальном времени;
- поддержка настройки частотных диапазонов для обмена данными;
- поддержка Mesh-сети с Chirpstack Gateway Mesh;
- поддержка версий 1.0.0-1.1.0 протокола LoRaWAN;
- интеграция с MQTT.

3.2. Шлюзы RealLab с поддержкой Chirpstack

Ниже приведен список шлюзов RealLab, поддерживающих обмен данными по протоколу LoRaWAN с использованием ПО Chirpstack.

- NLS-Gateway-LoRa-2RS;
- NLS-Gateway-LoRa-2RS-PoE;
- NLS-Gateway-LoRa-1RS-1CAN;
- NLS-Gateway-LoRa-1RS-1CAN-PoE.

3.3. Вход в веб-интерфейс Chirpstack

Перейти в веб-интерфейс Chirpstack можно двумя способами:

- ввести в строку браузера IP-адрес-шлюза и порт 8081. Пример: 192.168.1.234:8081;
- перейти через веб-конфигуратор RealLab!.

Для перехода через веб-конфигуратор, откройте веб-интерфейс RealLab! и войдите в учетную запись. На главной странице будет отображена карточка с информацией о сервисе Chirpstack, нажмите кнопку «Открыть интерфейс» (см. рис. 3.1). Более подробное описание главной страницы веб-конфигуратора находится в п. 2.6.

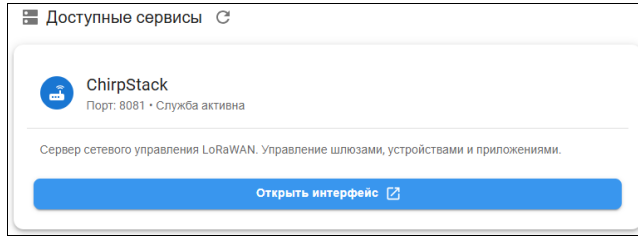


Рис. 3.1. Карточка сервиса Chirpstack

После перехода в веб-интерфейс Chirpstack, необходимо ввести имя учетной записи и пароль (см. рис. 3.2). Далее нажмите кнопку «Submit».

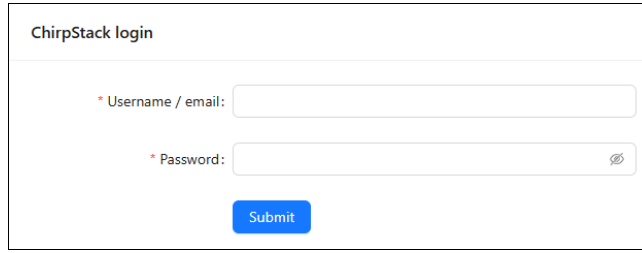


Рис. 3.2. Страница входа в учетную запись Chirpstack

Данные для входа по умолчанию:

Имя пользователя: *admin*

Пароль: *admin*

3.4. Добавление LoRaWAN-концентратора в Chirpstack

Выполните начальную настройку шлюза в веб-конфигураторе RealLab! если она не выполнялась ранее (п. 2.3).

Далее перейдите в веб-интерфейс Chirpstack (п. 3.3). В боковом меню выберите «Gateways» (см. рис. 3.3). Появится таблица добавленных LoRaWAN-концентраторов.

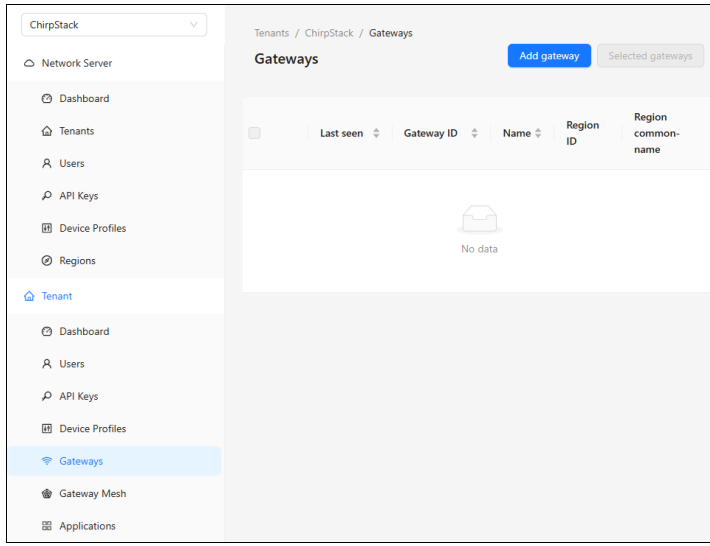


Рис. 3.3. Переход на вкладку Gateways в веб-интерфейсе Chirpstack

Нажмите кнопку «Add gateway» для открытия меню добавления концентратора. Скопируйте Gateway ID со вкладки «Сеть» LoRaWAN веб-интерфейса RealLab! (п. 2.4) и вставьте в форму «Gateway ID (EUI64)» (см. рис. 3.4). Пролистайте страницу до конца и нажмите кнопку «Submit».

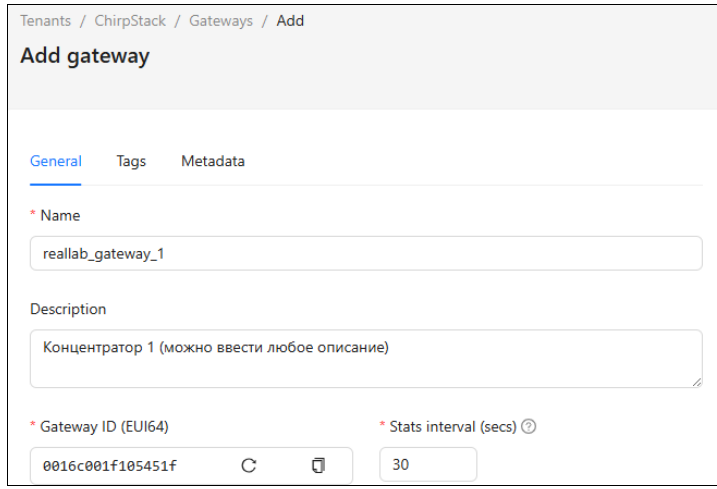


Рис. 3.4. Добавление концентратора в Chirpstack

Через 30-60 секунд обновите страницу. На странице появится дата последнего появления в сети, код частотного плана и местоположение на карте при условии, что GPS-модуль успешно подключился к спутникам (см. рис. 3.6). В нижней части страницы можно увидеть статистику отправки и приема пакетов (см. рис. 3.5).

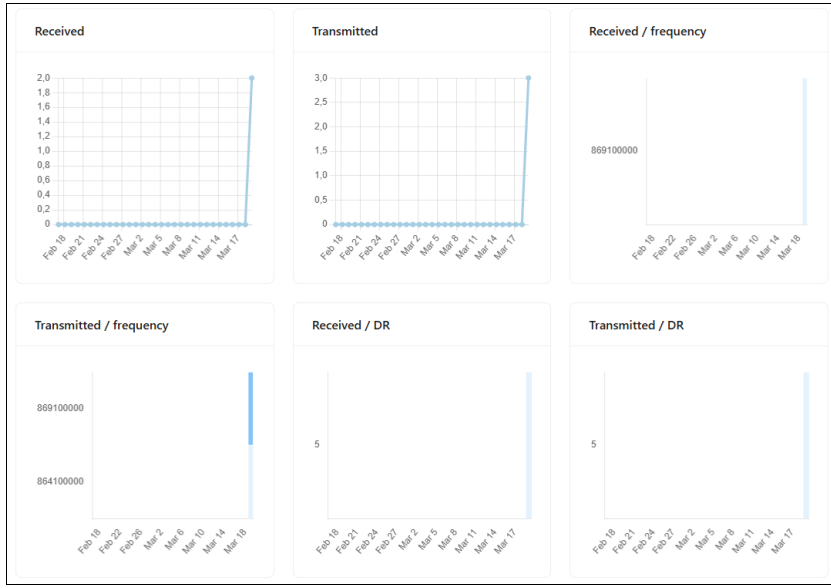


Рис. 3.5. Статистика приема и передачи пакетов по протоколу LoRaWAN

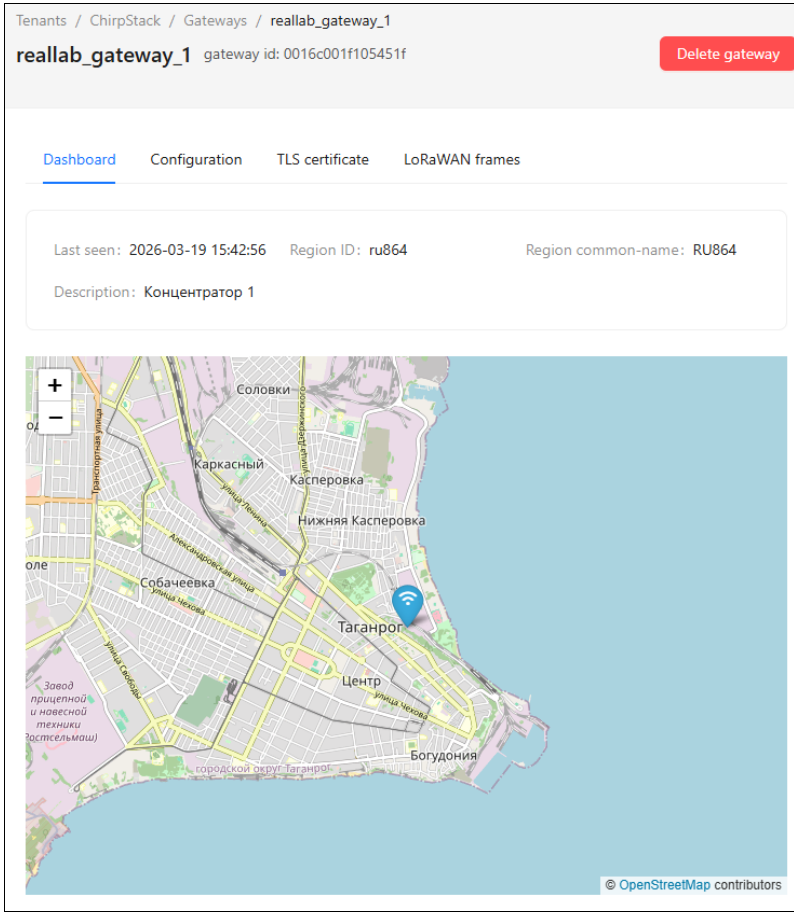


Рис. 3.6. Страница информации о добавленном концентраторе в Chirpstack

3.5. Добавление датчиков LoRaWAN в Chirpstack

Для добавления датчика LoRaWAN в Chirpstack откройте веб-интерфейс Chirpstack и перейдите на вкладку «Device Profiles» (профили устройств).

Для добавления нового датчика нажмите кнопку добавления профиля устройства «Add device profile» (см. рис. 3.7).

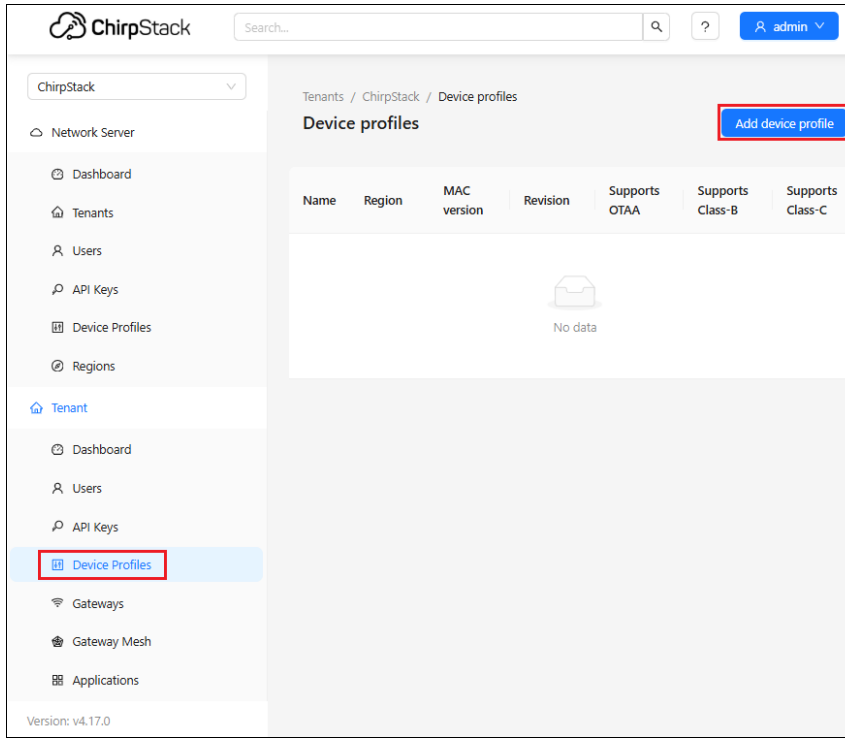


Рис. 3.7. Вкладка профилей устройств

Введите имя датчика и его описание. Укажите частотный план (Region), по которому работает датчик и его конфигурацию (Region Configuration).

Версию LoRaWAN, ревизию региональных параметров, задержку «RX1 Delay» на подключение устройства к сети и список поддерживаемых скоростей передачи (Supported data-rates) указывайте в соответствии с характеристиками датчика. Пример конфигурации показан на рис. 3.8.

ВАЖНО! Если значение параметра RX1 Delay в Chirpstack не соответствует значению данного параметра в конфигурации датчика, то возможно возникновение проблем с подключением датчика к шлюзу.

ВАЖНО! После создания профиля устройства в Chirpstack, вы можете его использовать для всех добавляемых датчиков, соответствующих данному профилю. Например, если вы используете 5 датчиков Вега ТД-11, то достаточно использовать один и тот же профиль устройства для них. Нет необходимости создавать несколько одинаковых профилей.

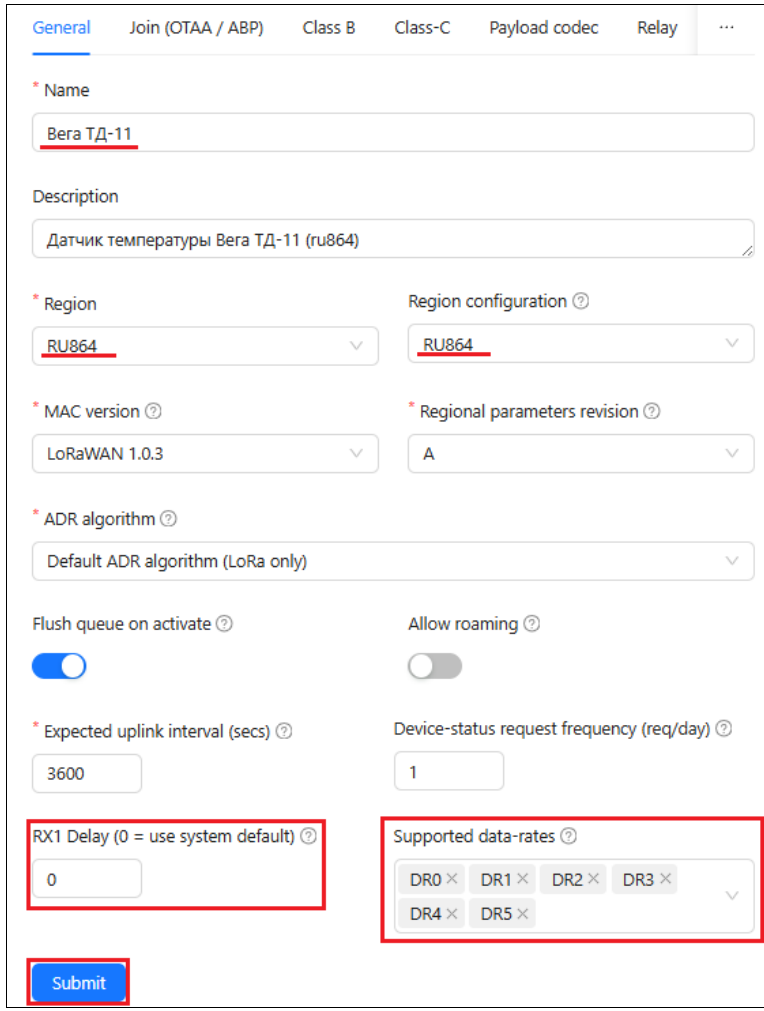


Рис. 3.8. Параметры добавления датчика LoRaWAN

Далее перейдите во вкладку Applications и создайте приложение с помощью кнопки «Add Application» (см. рис. 3.9).

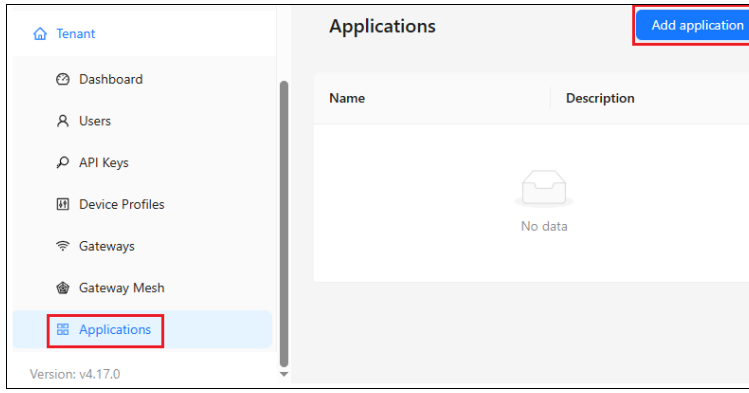


Рис. 3.9. Вкладка «Applications»

Введите название приложения и нажмите кнопку «Submit» (см. рис. 3.10).

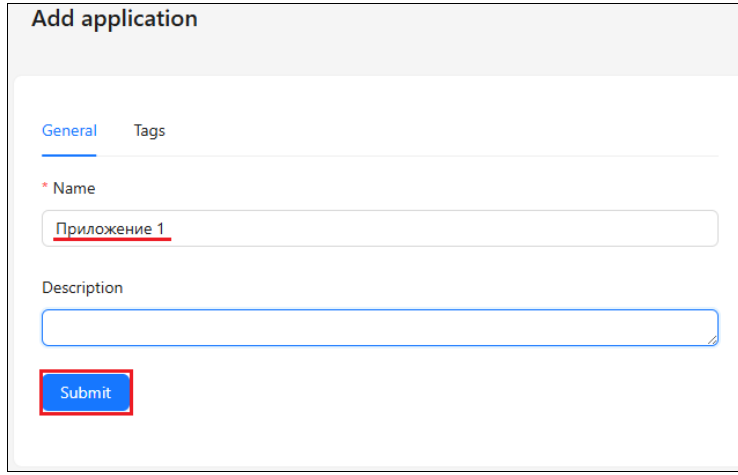


Рис. 3.10. Создание приложения

В приложение можно добавить неограниченное количество датчиков. Для добавления датчика нажмите кнопку «Add device».

На открывшейся странице заполните следующие поля: имя, Device EUI, Join EUI и Device Profile. В поле Device Profile выберите «Tenant» и ранее созданный профиль устройства (см. рис. 3.11). В нижней части окна нажмите «Submit».

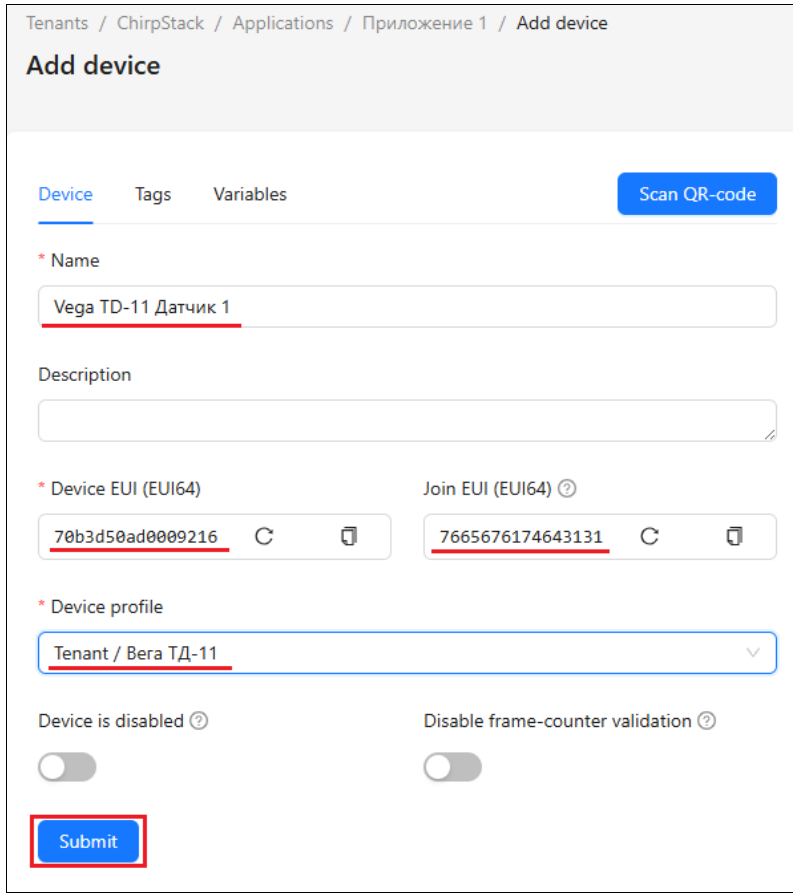


Рис. 3.11. Создание устройства

Далее необходимо ввести Application Key для привязки датчика к шлюзу по OTAA (см. рис. 3.12).

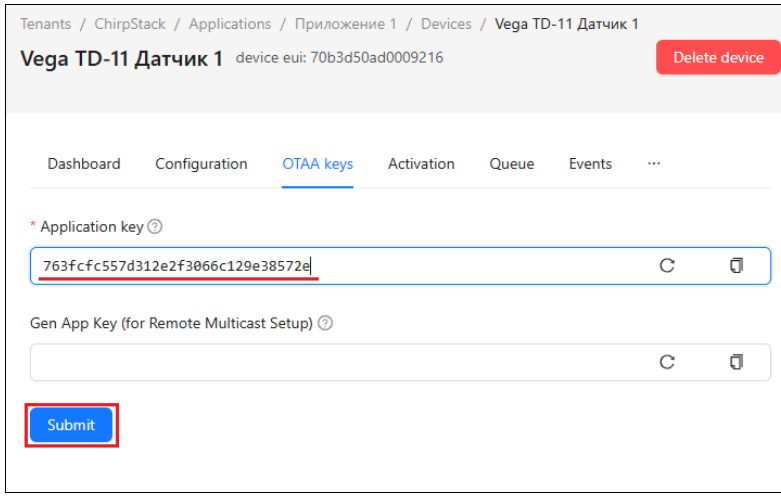


Рис. 3.12. Добавление Application Key

Далее нажмите «Submit». Откроется страница добавленного устройства, в верхней части выберите вкладку «LoRaWAN Frames» (см. рис. 3.13).

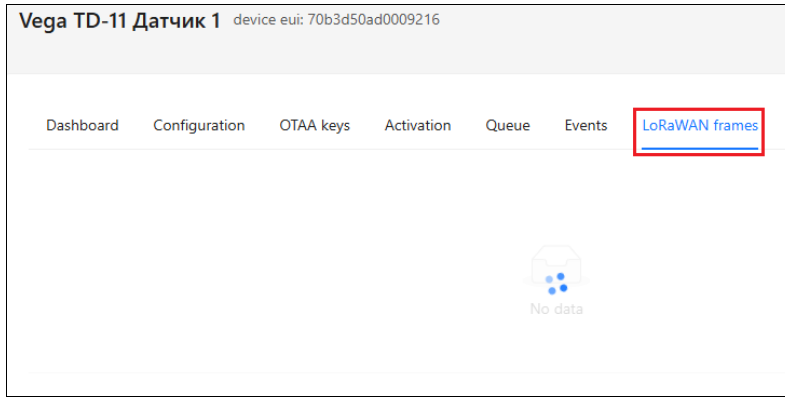


Рис. 3.13. Вкладка LoRaWAN Frames

После этого нажмите на датчике кнопку активации и ожидайте подключения.

При успешном подключении появляются записи в таблице: JoinRequest (запрос на подключение) и JoinAccept (запрос на подключение принят). Далее будут появляться данные с состояниями ConfirmedDataUp и UnconfirmedDataDown (см. рис. 3.14).

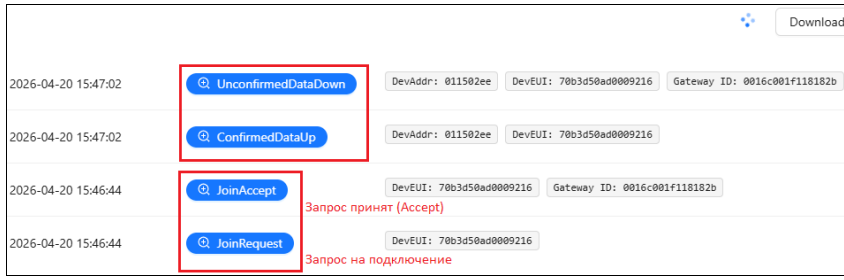


Рис. 3.14. Процесс подключения датчика и отправки данных на шлюз

Если перейти на вкладку «Events» (события), то можно увидеть передаваемые данные (строка «Data» на рис. 3.15).

Рис. 3.15. Событие передачи данных с датчика на шлюз

3.6. Передача данных с датчика в MQTT-брокер

По умолчанию Chirpstack передает данные в топик события application/{{application_id}}/device/{{dev_eui}}/event/{{event}}.

Сам датчик передает данные в виде строки байт, структура которой описана в руководстве к используемому датчику. Данные в «сыром» виде не передаются в топик MQTT-брокера.

Чтобы преобразовать данные в JSON и передать их в MQTT-брокер, необходимо зайти в веб-интерфейс Chirpstack и открыть профиль настраиваемого датчика и выбрать вкладку «Payload Codec» (см. рис. 3.16).

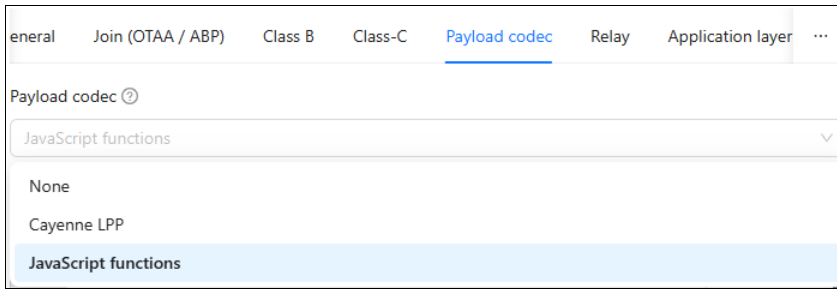


Рис. 3.16. Выбор Payload codec

Затем выберите JavaScript и вставьте туда код, предоставляемый производителем, или напишите код вручную, опираясь на описание

формата кадра передаваемых данных (frame_payload). После написания кода нажмите «Submit», чтобы применить изменения.

Пример кода на JavaScript показан на рис. 3.17.

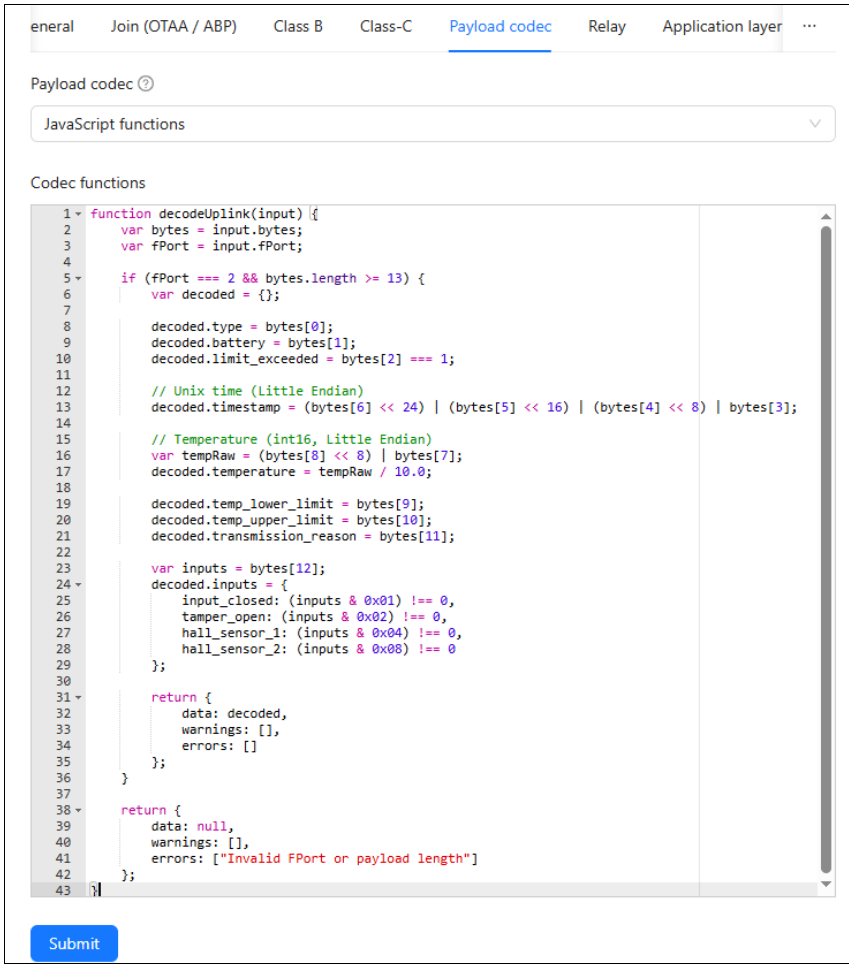


Рис. 3.17. Пример кода на JavaScript для датчика Вега ТД-11

Ниже показан пример отображения данных в MQTT Explorer.

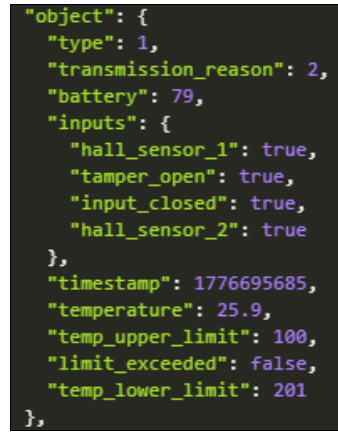


Рис. 3.18. Пример отображения данных в MQTT Explorer после преобразования

Также данные можно посмотреть в Chirpstack –> Applications –> <Имя приложения> –> <Датчик> –> Events. Выберите любое событие «Up» с кадром передачи данных Data как на рис. 3.15 и нажмите на кнопку «Up».

В правой части веб-интерфейса отобразятся переданные данные.

Обработанные данные находятся в объекте «object» (см. рис. 3.19).

Рис. 3.19. Данные после обработки в Chirpstack

4. Zigbee2MQTT

4.1. Описание ПО Zigbee2MQTT

Zigbee2MQTT является программным обеспечением, объединяющим Zigbee-устройства разных производителей в единую Mesh-сеть и делающим их управляемыми через протокол MQTT. Zigbee2MQTT предоставляет веб-интерфейс для подключения Zigbee-устройств к шлюзу и управления ими.

Возможности Zigbee2MQTT:

- создание привязок устройств;
- управление группами устройств;
- интеграция с Home Assistant;
- большое количество поддерживаемых конечных устройств;
- поддержка Mesh-сети Zigbee;
- логирование и отчетная информация об изменении значений датчиков;
- интеграция с MQTT.

4.2. Шлюзы RealLab с поддержкой Zigbee2MQTT

Ниже приведен список шлюзов RealLab, поддерживающих обмен данными по протоколу Zigbee с использованием ПО Zigbee2MQTT.

- NLS-Gateway-Zigbee-2RS;
- NLS-Gateway- Zigbee-2RS-PoE;
- NLS-Gateway- Zigbee-1RS-1CAN;
- NLS-Gateway- Zigbee-1RS-1CAN-PoE.

4.3. Вход в веб-интерфейс Zigbee2MQTT

Перейти в веб-интерфейс Zigbee2MQTT можно двумя способами:

- ввести в строку браузера IP-адрес-шлюза и порт 8082. *Пример: 192.168.10.234:8082;*
- перейти через веб-конфигуратор RealLab! (см. 2.6, рис. 2.15).

4.4. Добавление датчиков и маршрутизаторов

В веб-интерфейсе на любой из страниц слева находится панель, содержащая навигационное меню и кнопку разрешения подключения датчиков Zigbee к координатору.

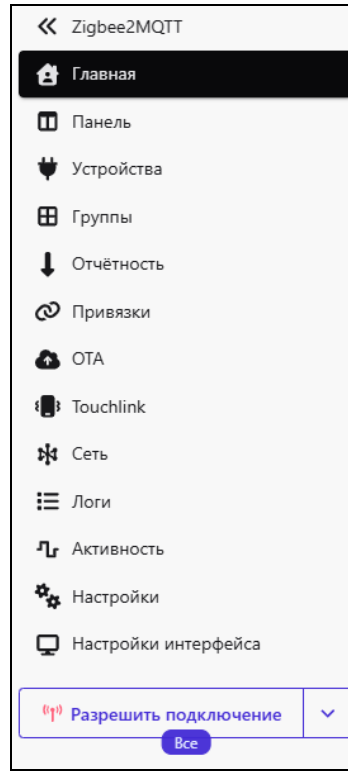
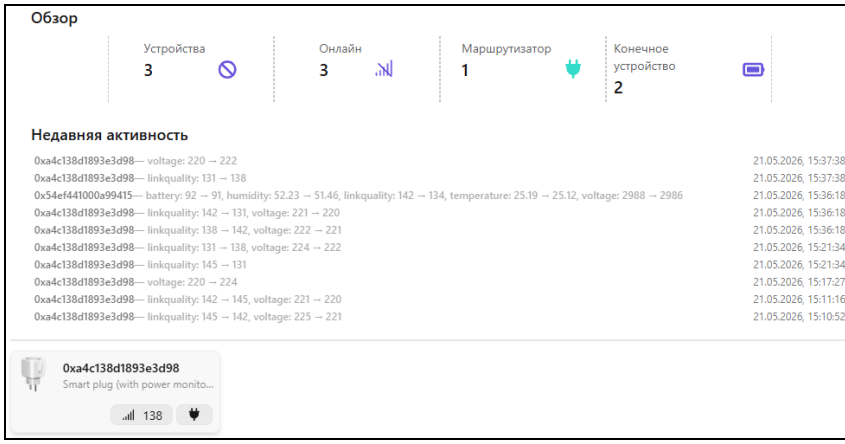


Рис. 4.1. Панель навигации и кнопка разрешения подключения

На основной части страницы находятся секции «Обзор» и «Последняя активность».

Секция «Обзор» отображает количество добавленных и активных устройств, а также разбивает их на категории – «маршрутизаторы» и «конечные устройства».

Секция «Недавняя активность» отображает изменение показаний, поступающих с датчиков.



Нажмите кнопку «Разрешить подключение» в боковой панели навигации интерфейса Zigbee2MQTT (см. рис. 4.2).

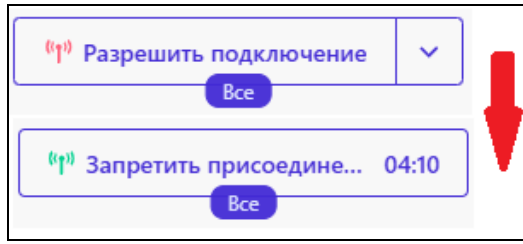


Рис. 4.2. Кнопка разрешения подключения

Откройте вкладку «Устройства» в Zigbee2MQTT.

Далее на устройстве, которое хотите привязать к шлюзу, зажмите кнопку подключения на 5 секунд – устройство перейдет в режим подключения и спустя некоторое время появится в списке веб-интерфейса Zigbee2MQTT.

Если таким способом подключить устройство не удалось, то обратитесь к инструкции по работе с подключаемым устройством.

На рис. 4.3. отображен список подключенных устройств и их данные – имя (можно изменить в параметрах), адрес, модель, качество сигнала (LQI), доступность, а также кнопки действий.

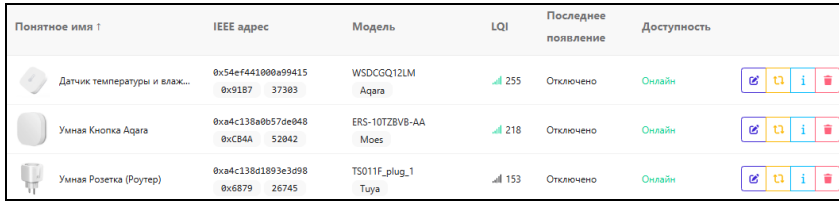


Рис. 4.3. Список подключенных устройств

4.5. Просмотр информации о датчиках

Со страницы устройств можно перейти в свойства любого из добавленных датчиков. Для этого необходимо нажать на имя устройства, свойства которого нужно открыть.

Свойства выбранного устройства содержат вкладки:

- информация – подробная информация об устройстве (тип, адрес, сетевой адрес, модель Zigbee, определение, ID прошивки, недавняя активность, топик MQTT);

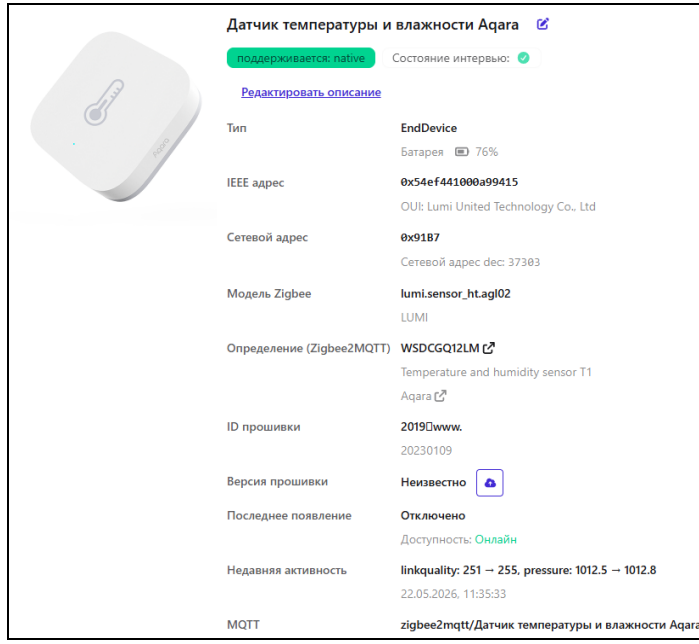


Рис. 4.4. Информация о датчике температуры и влажности

- свойства – информация о текущих показаниях датчика (температура, влажность, давление и т.д.);

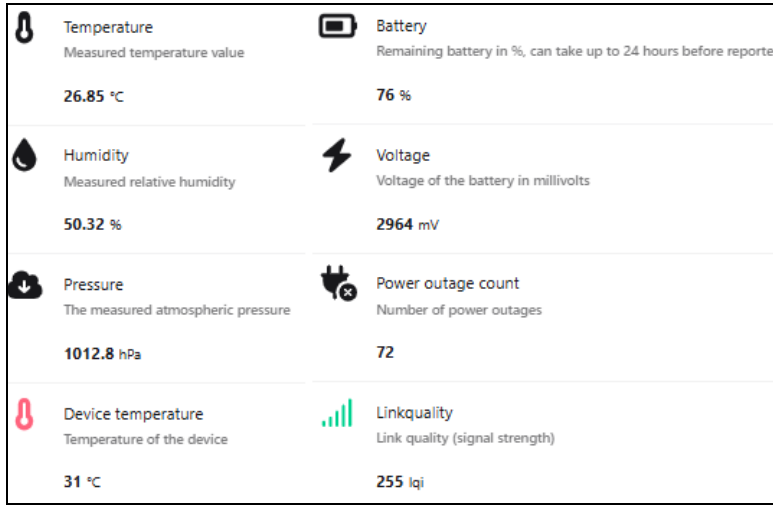


Рис. 4.5. Показания датчика температуры и влажности

- настройки – позволяет настроить некоторые параметры самого датчика;
- привязки – привязка позволяет устройствам напрямую управлять друг-другом без вмешательства Zigbee2MQTT или любого программного обеспечения для домашней автоматизации. Если устройства не подходят для привязки друг к другу, настройте взаимодействие между ними через стороннее ПО (Home Assistant, Node-RED и т.д.);
- отчетность – функция, с помощью которой Zigbee-устройство (например, датчик температуры) само отправляет свои данные координатору без постоянного опроса с его стороны.

Для настройки отчетности нажмите кнопку «Добавить», выберите кластер и атрибут, укажите интервалы отправки отчета в секундах и условие отправки отчета «Мин. изменение отчета». Значение «10» равно изменению температуры на 1 градус.

ВАЖНО! Для того, чтобы изменения применились без ошибок, сразу после нажатия на кнопку применения изменений нажмите на кнопку RESET на самом датчике, он будет переведен в рабочий режим.

ВАЖНО! Некоторые устройства используют свои правила для отправки данных на координатор и автоматически добавляют их в Chirpstack.

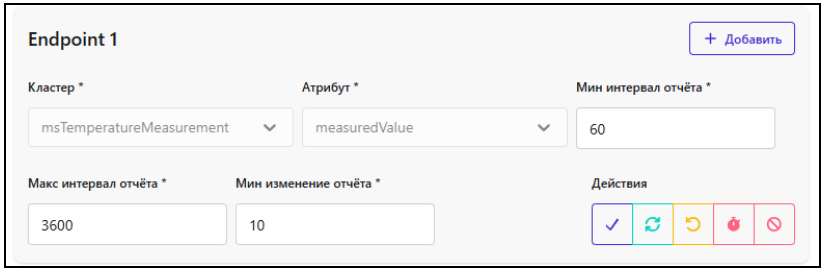


Рис. 4.6. Параметры отчетности датчика об изменении температуры

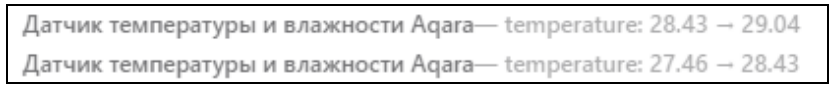


Рис. 4.7. Получение данных в секции «недавняя активность» главной страницы веб-интерфейса

4.6. Управление датчиками из интерфейса Zigbee2MQTT

Откройте вкладку «Панель» с помощью боковой панели навигации.

Датчики, с которых можно только считывать информацию, будут ее отображать. Устройства, которыми можно управлять, предоставляют элементы интерфейса для управления их состоянием.

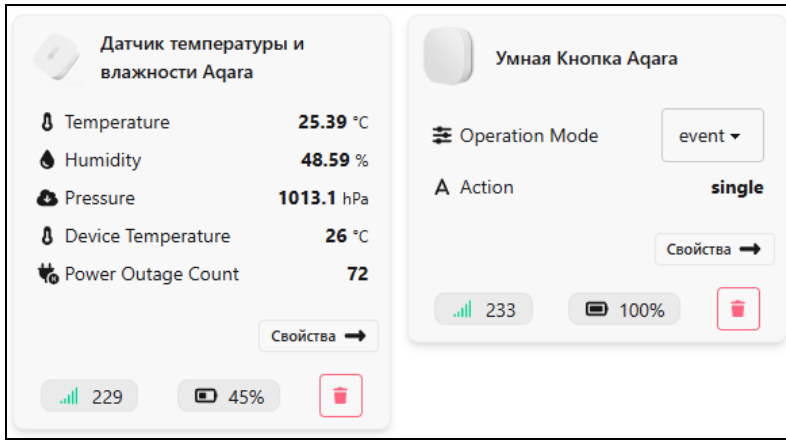


Рис. 4.8. Показания датчиков в панели веб-интерфейса

На рис. 4.9 выделены элементы управления умной розеткой: состоянием, таймером автоматического отключения, режимом защиты от детей.

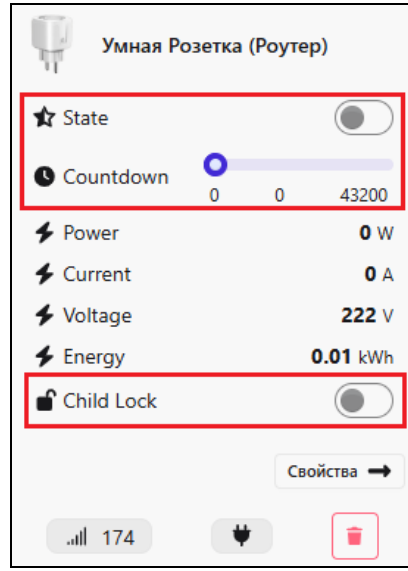


Рис. 4.9. Элементы управления умной розеткой через панель веб-интерфейса

4.7. Карта сети

Откройте вкладку «Сеть» с помощью боковой панели навигации.

В основной части окна появится интерфейс генерации карты сети. Выберите тип отображения «Карта» и нажмите кнопку «Сформировать».

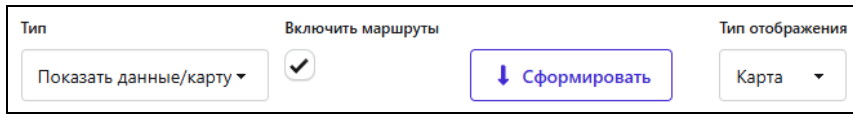


Рис. 4.10. Генерация карты сети

На карте отображены связи между устройствами и координатором.

К координатору подключены умная кнопка, датчик температуры и влажности. Умная розетка выступает в роли маршрутизатора, к ней можно подключить датчики. Стрелка «Tx» с уровнем сигнала 130 означает качество сигнала при передаче данных с координатора на умную розетку

(маршрутизатор). На качество сигнала при передаче влияет мощность передатчика, регулируемая в веб-конфигураторе RealLab! (см. п. 2.10.7).

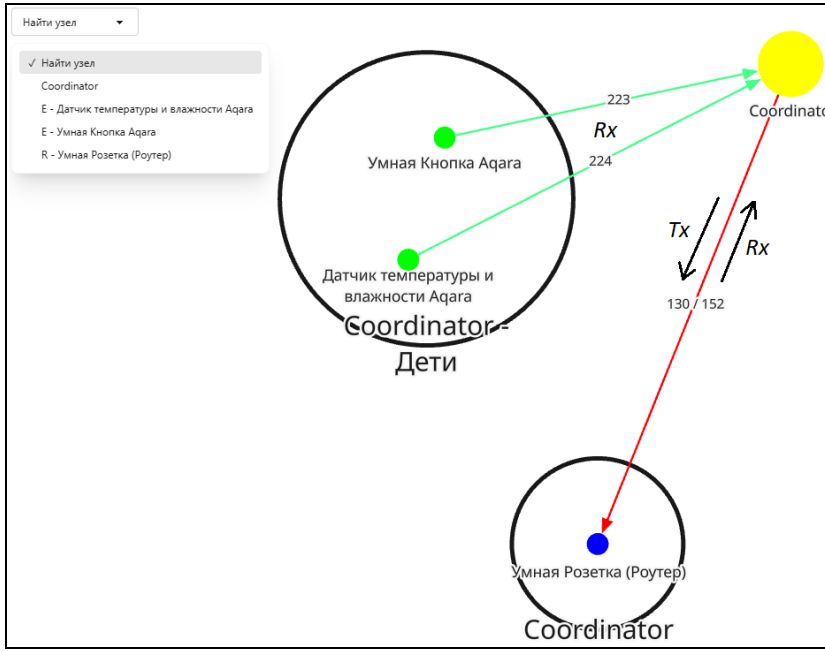


Рис. 4.11. Карта сети

4.8. Настройка подключения к MQTT-брокеру с использованием шифрования TLS

Для настройки защищенного обмена данными между Zigbee2MQTT и MQTT-брокером выполните следующие действия:

Включите защищенное соединение для брокера Mosquitto через веб-конфигуратор RealLab! (см. п. 2.10.6.1) и сгенерируйте сертификаты.

Перейдите в настройки Zigbee2MQTT с помощью боковой панели навигации. В верхней части окна выберите вкладку «Настройки». Выберите вложенную вкладку «MQTT».

Заполните поля «ca», «cert», «key», как на рис. 4.12, указав корректные пути, по которым находятся сертификаты.

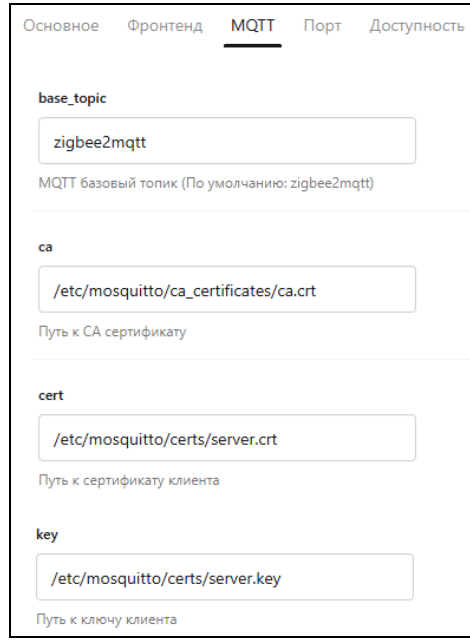


Рис. 4.12. Параметры сертификатов Zigbee2MQTT

Если используется авторизация для доступа к MQTT-брокеру, также введите имя пользователя и пароля в поля «user» и «password» соответственно.

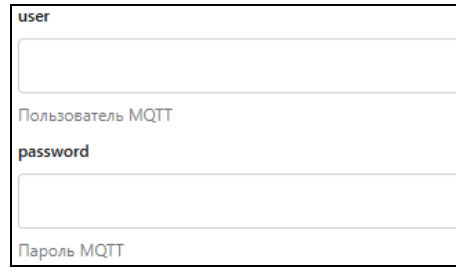


Рис. 4.13. Параметры авторизации MQTT-брокера в Zigbee2MQTT

ВАЖНО! После изменения параметров требуется перезапустить службу Zigbee2MQTT для применения изменений. Перезапустить службу можно кнопкой «Перезапуск» в диалоге логирования и управления службами во вкладке «Zigbee» страницы «Сеть» веб-конфигуратора RealLab! (см. рис. 2.108).

4.9. Просмотр логов службы Zigbee2MQTT

Логи можно посмотреть двумя способами:

- через веб-интерфейс RealLab! (см. п. 2.10.7);
- через веб-интерфейс Zigbee2MQTT.

Откройте вкладку «Логи» с помощью боковой панели навигации. Выберите, в каком количестве и какого уровня логи нужно отобразить.

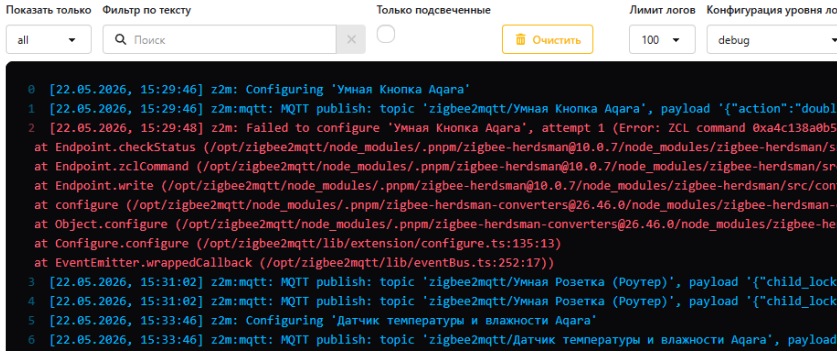


Рис. 4.14. Логи Zigbee2MQTT

Лист регистрации изменений

Дата изменения	Описание изменения	Примечание
22.05.2026	*Изменен п. 2.10, добавлен п. 4 (информация о Zigbee2MQTT)*	