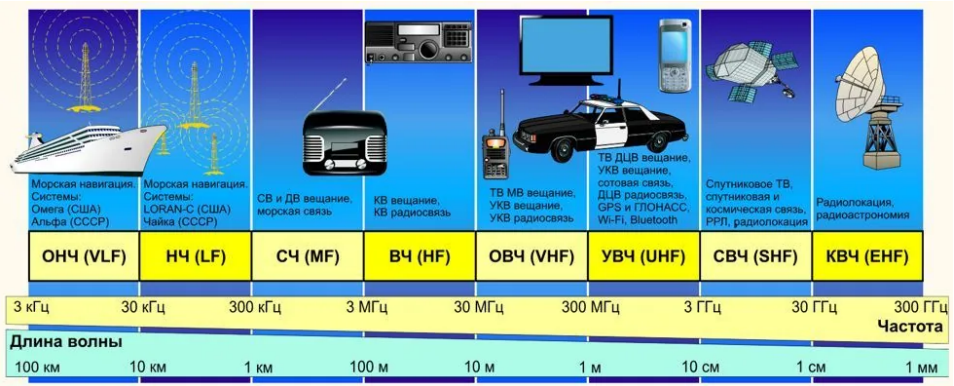
Аппаратное обеспечение IoT/CPS
Лекция 6

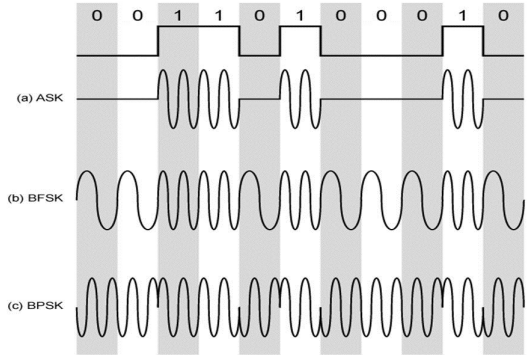
А. А. Подшивалов
apodshivalov@miem.hse.ru

Основы цифровой радиосвязи и фундаментальные ограничения


Морская навигация.
Системы:
Омега (США)
Альфа (СССР)
Морская навигация.
Системы:
LORAN-C (США)
Чайка (СССР)
СВ и ДВ вещание,
морская связь
КВ вещание,
КВ радиосвязь
ТВ МВ вещание,
УКВ вещание,
УКВ радиосвязь
ТВ ДЦВ вещание,
УКВ вещание,
сотовая связь,
ДЦВ радиосвязь,
GPS и ГЛОНАСС,
Wi-Fi, Bluetooth
Спутниковое ТВ,
спутниковая и
космическая связь,
РРЛ, радиолокация
Радиолокация,
радиоастрономия
ОНЧ (VLF)
НЧ (LF)
СЧ (MF)
ВЧ (HF)
ОВЧ (VHF)
УВЧ (UHF)
СВЧ (SHF)
КВЧ (EHF)
3 кГц
30 кГц
300 кГц
3 МГц
30 МГц
300 МГц
3 ГГц
30 ГГц
300 ГГц
Частота
Длина волны
100 км
10 км
1 км
100 м
10 м
1 м
10 см
1 см
1 мм

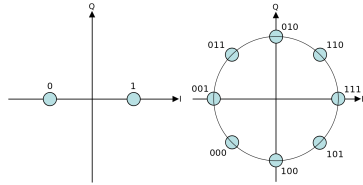
Модуляция радиосигнала

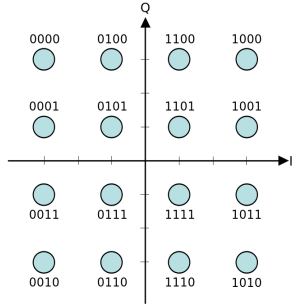
- Изменение параметров несущего сигнала в зависимости от модулирующего сигнала
  - Амплитудная (AM)
  - Частотная (FM)
  - Фазовая (PM)
- Цифровая манипуляция
  - ASK — Amplitude shifted keying
  - FSK — Frequency shifted keying
  - PSK — Phase shifted keying
  - ...



Цифровая манипуляция

- Передаем одним символом несколько бит
  - n-PSK
  - QAM
- OFDM — одновременно передается несколько поднесущих
- DSSS
  - Одному биту («символу») соответствует целая последовательность 0 и 1 («chips») в передаваемых данных (PSK или FSK)
  - CDMA
- CSS — Chirp Spread Spectrum





Предел Шеннона

- Теорема Шеннона-Хартли

$$C = B \log_2 \left(1 + \frac{S}{N}\right),$$

где:

  - C (capacity) — максимальная пропускная способность канала, бит/с
  - B (bandwidth) — полоса пропускания канала, Гц
  - S (signal) — полная мощность сигнала, Вт
  - N (noise) — мощность шума, Вт
  - $\frac{S}{N}$ — отношение сигнал/шум, SNR

- При $\frac{S}{N} \gg 1$:

$$C = B \log_2 \left(1 + \frac{S}{N}\right) \approx B \log_2 \frac{S}{N} = \frac{\ln 10}{\ln 2} B \log_{10} \frac{S}{N} \approx 3,32 \times B \times \log_{10} \frac{S}{N} = 0,332 \times B \times SNR^{[dB]}$$

- При $\frac{S}{N} \ll 1$:

$$C = B \log_2 \left(1 + \frac{S}{N}\right) \approx B \frac{1}{\ln 2} \frac{S}{N} \approx 1,44 \frac{S}{N_0},$$

где N_0 — спектральная плотность шума, $N = BN_0$

- Тепловой шум: $N = k_B T B$, где $k_B = 1,380649 \times 10^{-23}$ Дж × К — постоянная Больцмана, T — температура (в градусах Кельвина)

Формула Фрииса

- Выражает мощность сигнала на приемнике в зависимости от расстояния (free-space pathloss)

$$\frac{P_r}{P_t} = G_r G_t \left(\frac{\lambda}{4\pi R}\right)^2,$$

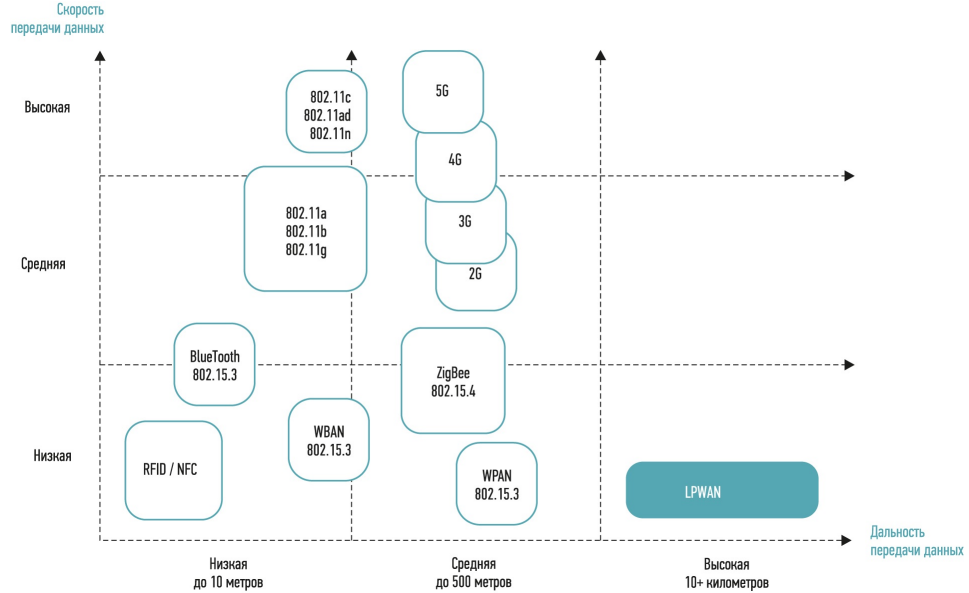
где:

  - P_r, P_t (power) — мощность сигнала на приемнике (receiver) и передатчике (transmitter)
  - G_r, G_t (gain) — коэффициент усиления антенн приемника и передатчика
  - R — расстояние между приемником и передатчиком
  - λ — длина волны

- Она же в дБ:

$$P_r^{[dBm]} = P_t^{[dBm]} + G_t^{[dBi]} + G_r^{[dBi]} + 20\log_{10}\frac{\lambda}{4\pi R}$$

Фундаментальные ограничения и реальные технологии



Два класса технологий IoT

- LPWAN, Low-power Wide Area Network
  - Скорость передачи не важна (сотни, редко тысячи бит/с), требуется большая зона покрытия
  - UNB-сети (Sigfox, NB-Fi и подобные), LoRa/LoRaWAN, в некоторой степени — NB-IoT
  - Частотный диапазон Sub 1-GHz (433 или 868/915 МГц)
- LR-WPAN, Low-rate Wireless Personal Area Network
  - Скорость передачи относительно мала (до 250 кбит/с), зона покрытия — до десятков метров, интересно энергосбережение
  - IEEE 802.15.4, BLE, IEEE 802.11ah
  - Частотный диапазон ISM (2,4 ГГц) или Sub 1-GHz
- «Вне зачета» — традиционные беспроводные технологии: WiFi (IEEE 802.11), Bluetooth, Bluetooth Low Energy, сотовая связь

Мокнет одинокая свинья @Mos_art1 · Apr 7

В истребителе главное — мотор. Обычно авиаписарчуки тут заводят свою заклепидорскую волынку про воздушное и водяное охлаждение, какие плюсы и минусы: это всё хуйня.

Двигатели делятся на:

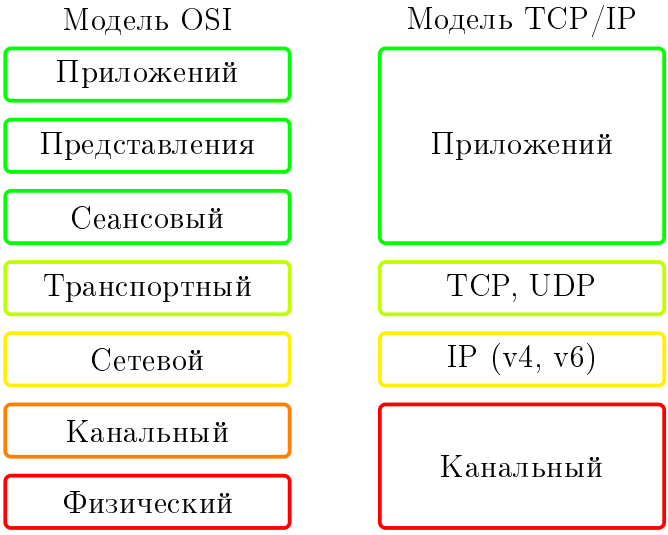
- серийные.
- перспективные.
- экспериментальные.

6 2 43

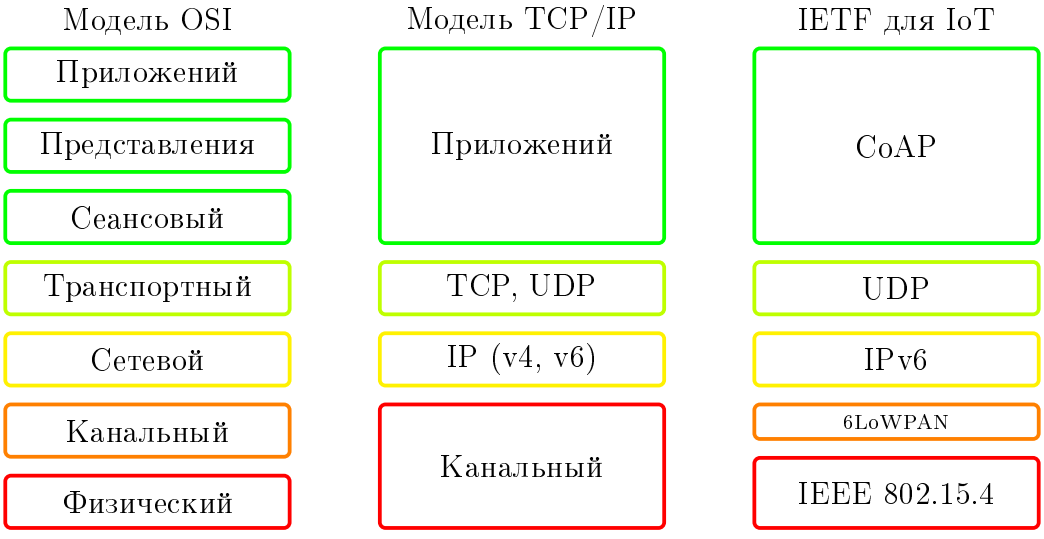
Конкретные примеры: WPAN и mesh-сети

Модели сетевого взаимодействия

Модели сетевого взаимодействия



Модели сетевого взаимодействия

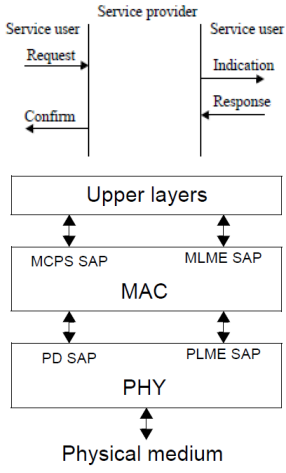


Канальный уровень

- Формирование кадров (MPDU)
- MAC — Medium Access Control, управление доступом к среде передачи
  - Очередность доступа, особенно в случае TDMA
  - Разрешение коллизий
  - Адресация
- LLC — Logical Link Control, управление связью
  - Установление и разрыв соединения
  - Подтверждение передачи, повторная отправка кадров
- Защита информации

Стандарт IEEE 802.15.4

- Описывает физический (PHY) и MAC-уровни беспроводных персональных сетей (WPAN, wireless personal-area network) и интерфейсы между ними
- Несколько разных вариантов PHY, скорость передачи данных от 10 до 1000 кбит/с, размер пакета — 127 байт
  - GFSK, 50 кбит/с, 868/915 МГЦ; типичная чувствительность приемника (CC1310) — -110 дБм
  - Q-PSK DSSS, 250 кбит/с, 2,4 ГГц; типичная чувствительность приемника (CC2630) — -100 дБм



MAC-уровень 802.15.4

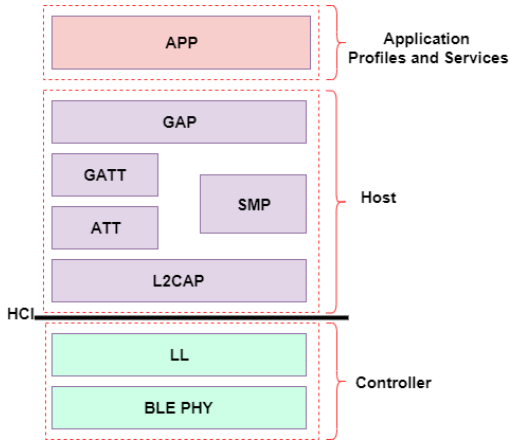
- Структура кадров, различные их типы (beacon, data frame, acknowledgement, MAC command)
- Алгоритмы доступа к каналу
- Адресация с помощью 6- и 2-байтовых адресов (6-байтовый адрес — это EUI-48)
- Топология сети — «звезда» или mesh
- Ассоциация и деассоциация
- Подтверждение приема данных
- Защита информации

6LoWPAN

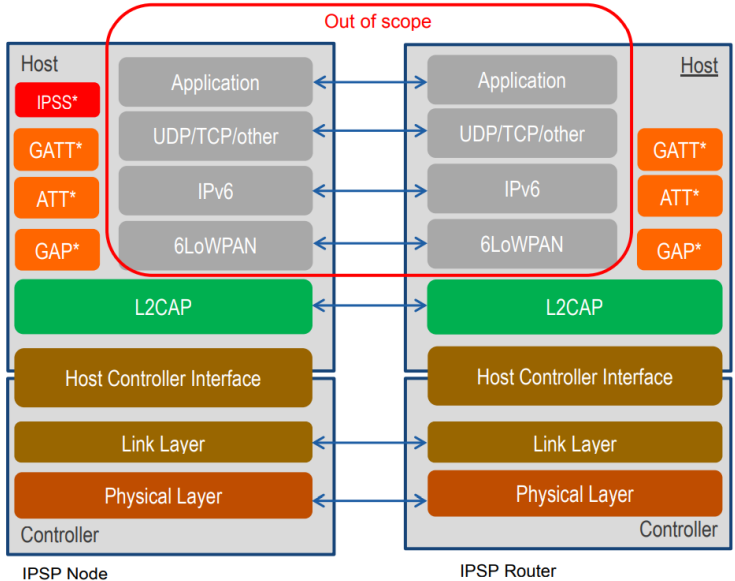
- Стандарт передачи пакетов IPv6 в сетях IEEE 802.15.4, IPv6 over Low-Power Wireless Personal Area Networks (RFC 4944)
- Сжатие заголовков (обновлено в RFC 6282)
- Фрагментация пакетов
- Маршрутизация, два основных подхода:
  - mesh-under (LOAD, LOADng — принят как стандарт ITU-T G.9903)
  - route-over, каждый узел может выступать IP-маршрутизатором (RPL, RFC 6550 — стандарт IETF)
- Автоматическое конфигурирование адресов (с помощью ICMPv6)

Bluetooth Low Energy

- Стандарт для небольших персональных сетей
- 40 каналов в диапазоне 2,4 ГГц, расстояние между соседними каналами 2 МГц, модуляция GFSK, 1 Мбит/с
- Ведущее и ведомое устройство обмениваются данными с некоторой периодичностью
- L2CAP — Logical Link Control and Adaptation Protocol, одна из функций — фрагментация пакетов



6LoWPAN поверх BLE



Защита информации в радиосети

Угрозы в радиосети

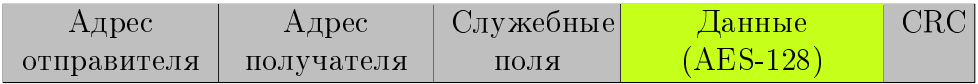
- Кто угодно может слушать эфир на любой частоте
- В лицензируемом диапазоне любой желающий может передавать в эфир что угодно, пока не придет Роскомнадзор
- В безлицензионном диапазоне любой желающий может передавать в эфир что хочет
- Большинство IoT-систем работает в безлицензионных диапазонах (433 МГц, 868 МГц, 2,4 ГГц)
- Угрозы (далеко не исчерпывающий список)
  - Перехват данных
  - Передача фальсифицированных данных
  - Косвенное определение состояния устройства

Наивный протокол

Адрес отправителя	Адрес получателя	Служебные поля	Данные	CRC

- Целостность пакета проверяется контрольной суммой (CRC)
- Данные не зашифрованы
- Кто угодно может прочитать данные
- Кто угодно может сфальсифицировать данные

Наивный протокол+шифрование

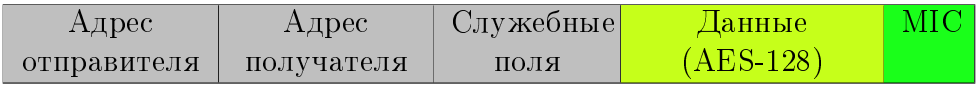


- Целостность пакета проверяется контрольной суммой (CRC)
- Данные зашифрованы, например, AES-128
- Посторонний не может прочитать данные
- Посторонний не может сфальсифицировать данные

Подмена данных MAC-уровня

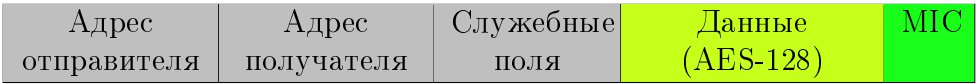
- Получаем из эфира чужой пакет
- Меняем что угодно, кроме зашифрованных данных
- Пересчитываем контрольную сумму
- Те же данные, но от другого отправителя, или к другому получателю, или...

Добавляем имитовставку (MIC)



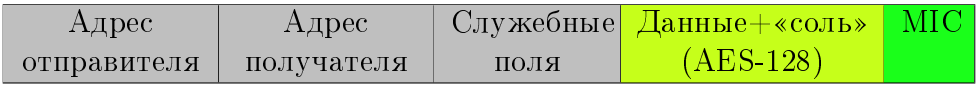
- Шифрование всего пакета слишком ресурсоемко
- Вместо (или вместе с) контрольной суммы используем MIC (Message Integrity Code, имитовставка) — зависящую от ключа однонаправленную хеш-функцию
- AES-CMAC и другие подобные алгоритмы

Определение состояния устройства



- Шифрование AES-ECB: каждый раз один и тот же ключ
- Зашифрованный блок меняется, только если меняются исходные данные
- Даже не расшифровывая блок данных, можно понять, изменились ли они
- Если показания водосчетчика не менялись уже неделю — в квартире никого нет

Добавляем «соль»



- 2 или 4 случайных байта
- При приеме и расшифровке «соль» отбрасывается
- Одни и те же данные, но разная «соль» — разные зашифрованные блоки

Атака повтором

Адрес отправителя	Адрес получателя	Служебные поля	Данные+«соль» (AES-128)	MIC

- Прослушиваем эфир, записываем нужный пакет
- В нужный нам момент времени воспроизводим его
- Пример: охранная сигнализация, датчик вскрытия окна

Защита от атаки повтором

- Добавляем счетчик или nonce (number used once)
- Счетчик может только возрастать, nonce не должен повторяться
- Сброс счетчика в 0 — отдельная и редкая процедура

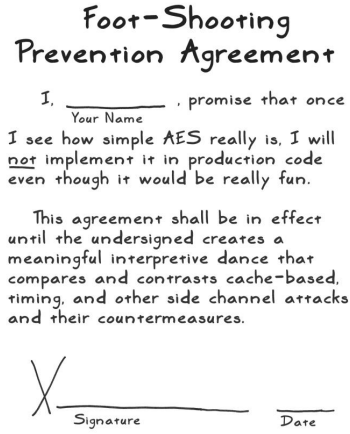
Активная атака повтором

- Записываем пакет с номером n и одновременно «глушим» его на приемнике
- Записываем пакет с номером $n + 1$ и одновременно «глушим» его на приемнике
- Воспроизводим пакет с номером n (пользователь считает, что это — пакет с номером $n + 1$)
- Затем воспроизводим пакет с номером $n + 1$

Немного о криптографии и генераторах случайных чисел

Три главных правила криптографии

1. Не изобретайте свой алгоритм
2. Если вам кажется, что авторы известных алгоритмов что-то сделали неправильно, но про это не написано у Брюса Шнайера — вам кажется
3. Ни при каких обстоятельствах не изобретайте свой алгоритм



Foot-Shooting Prevention Agreement

I, _____ , promise that once
Your Name
I see how simple AES really is, I will not implement it in production code even though it would be really fun.

This agreement shall be in effect until the undersigned creates a meaningful interpretive dance that compares and contrasts cache-based, timing, and other side channel attacks and their countermeasures.

X _____ _____
Signature Date

Средства операционной системы

- `sys/crypto` — алгоритмы шифрования
- `sys/hashes` — хеши, в том числе криптографические
- `sys/random` — генератор **псевдо**случайных чисел

True random number generator

Настоящий генератор случайных чисел может быть только аппаратным:

- Подбрасывание монеты
- Вращение рулетки
- Физические процессы, корнями уходящие в квантовую механику
  - Дробовой шум
  - Туннелирование электронов

Pseudo random number generator

- Сложная числовая функция, выдающая почти непредсказуемую последовательность чисел с очень большим периодом
- Если не сказано иного — всегда предполагайте псевдослучайность
- Последовательность определяется одним числом — *seed*
- При одном и том же *seed* — одна и та же последовательность
- *seed* должен быть *настоящим* случайным числом

Инициализация PRNG

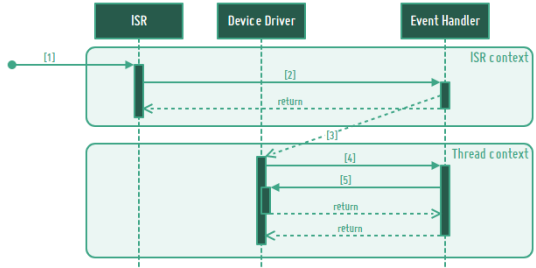
- Источники «настоящих» случайных чисел обычно медленные
- Удобно получить одно случайное число и использовать его, как *seed* для PRNG
- Источники случайности приемлемого качества:
  - Действия пользователя в интерактивной системе
  - Микрошум на «висящем в воздухе» входе АЦП
  - Шум в радиоэфире
  - Отклонения двух тактовых генераторов
- Источники случайности неприемлемого качества:
  - Время, прошедшее с момента старта системы
- Можно собрать много приемлемых случайных чисел и посчитать для них криптографический хеш

Сетевой стек ОС Riot

Основные варианты

- lwIP — популярная реализация TCP/IP для встраиваемых систем (Ethernet, IPv4, TCP, UDP)
- GNRC — собственный сетевой стек Riot (IPv6, UDP, статус реализации TCP — «экспериментальный», альтернативная реализация LoraWAN)
- NimBLE — реализация стека BLE (портирована из ОС Mynewt)
- Semtech LoRaMAC — «эталонная» реализация LoRaWAN и ее адаптация для Riot

Интерфейс netdev




```
const netdev_driver_t sx127x_driver = {
    .send = _send,
    .recv = _recv,
    .init = _init,
    .isr = _isr,
    .get = _get,
    .set = _set,
};
```

Сетевой стек GNRC

- Каждый сетевой протокол обслуживается отдельным потоком
- В ходе обработки пакета он передается между уровнями с помощью средств IPC
- Пакет состоит из нескольких фрагментов (snips), это могут быть заголовки, фрагменты заголовков, данные...
- Для хранения данных используется «буфер пакетов» с собственным управлением памятью