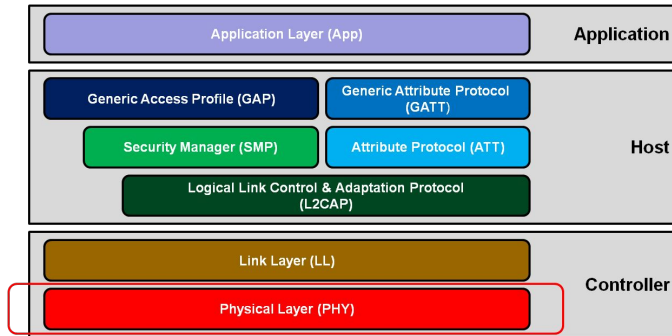# BLE
Bluetooth Low Energy

BACLE Lucas, ESTIVAL Emilie,
POTIERS Léo, SERONIE-VIVIEN Paul
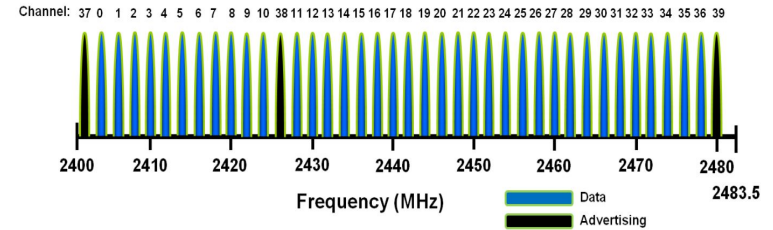
Physical layer

First layer of the protocol

The services provided by this layer go directly to the **link layer**
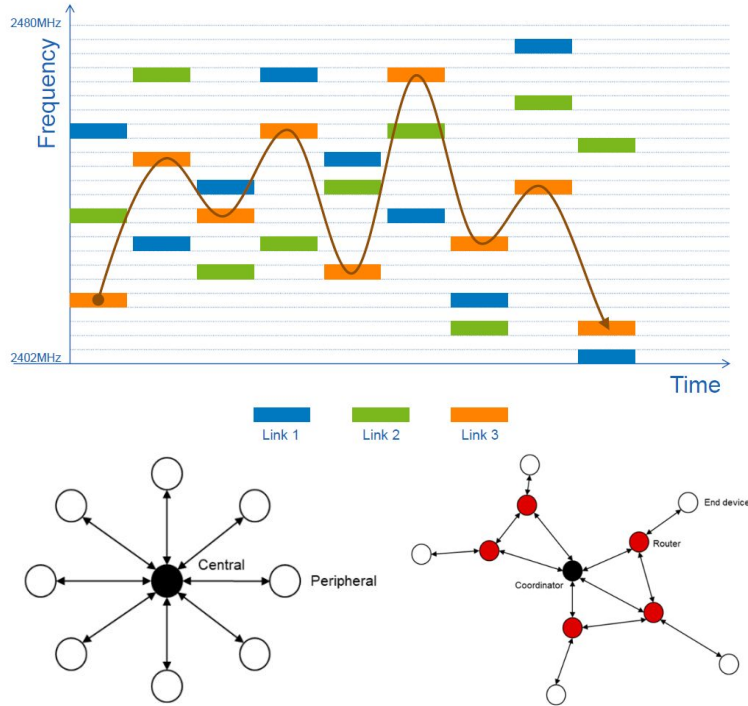
→ Link Layer (LL)

2.4GHz range and 40 channels

BLE has **40 different channels** that are spaced by 2MHz, either dedicated to data or advertising.

→ Connection is made with channels that are out of the Wi-Fi range

Link layer

- Device address

- Packets format

- Reliability

- Encryption

- MAC level operations

Power consumption

Low power consumption

- Peak current 2 times lower than Bluetooth Classic
- Power consumption 2 to 100 times lower

→ But highly dependent on the use case

Optimizing current consumption

- Extends battery life and makes better products
- Peripherals can function for 1 to 4 years on coin cell battery

→ BLE is designed to enable devices to have very low power consumption

What can affect power consumption in BLE ?

- Amount of power transmitted
- Total amount of time that the radio is active

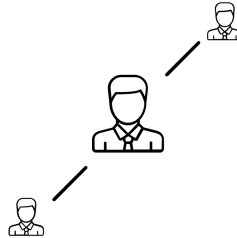→ Highly dependent on the environment and parameters

4

Security

Passive eavesdropping

When a **third device listens to the data** being exchanged between the two paired devices.

→ AES Encryption, but vulnerabilities in the key exchange protocol

Men In The Middle (MITM) attacks

When both the central and peripheral **devices will connect to the malicious device which redirects the communication route to himself**.

→ Data interception and false data injection risk

Identity tracking

When a malicious entity is able to **associate the address of a BLE device with a specific user** and tracks him.

→ Need to change frequently the device connection address (but it is not done efficiently or frequently enough)

Do you have any questions ?