UNIVERSITÀ
DEGLI STUDI
DI PADOVA

MIME
Master's degree ICT Internet Multimedia Engineering

Department of Information Engineering (DEI)
Master degree on ICT for Internet and Multimedia Engineering (MIME)

Internet of Things and Smart Cities
05 – Bluetooth Low Energy (BLE)

Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

Bluetooth

Overview

- **Bluetooth** is a wireless technology designed to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers, when they are at a **short distance** from each other.
  - Initially proposed by Ericsson.
  - Standardized as **IEEE 802.15.1**.
  - Originally thought as a solution to replace wired connections within computers.
- 3 classes of Bluetooth:
  - **Bluetooth Classic** (Basic Rate / Enhanced Data Rate – BR/EDR).
  - Bluetooth High Speed.
  - **Bluetooth Low Energy.**

Bluetooth

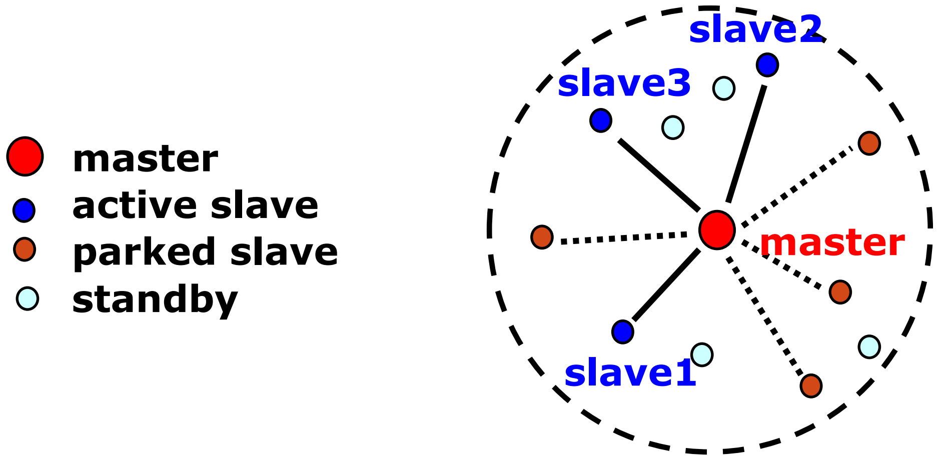
Applications

- **Bluetooth Classic (Basic Rate / Enhanced Data Rate – BR/EDR)**
  - Audio streaming (headphones, speakers, car audio systems, …).
  - Peripheral devices (keyboards, mice, printers, …).
  - File transfers (sending files between phones, computers, and other devices).
- **Bluetooth High Speed**
  - (High-resolution) video streaming.
  - Tethering (for sharing internet connections between devices).
- **Bluetooth Low Energy**
  - Wearables
  - Beacons (utilized in proximity marketing and location-based service)
  - Smart Home devices

BR/EDR

Topology

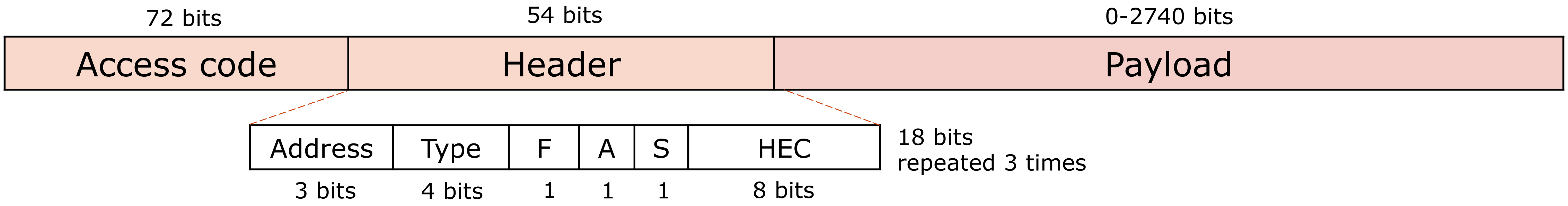
- Units connect in small networks called **piconets** (that can be combined to form what is called a **scatternet**).
  - Each piconet can host from 2 to 8 **active** devices.
  - Up to 255 in sleep (**parked**) state: synchronized but cannot take part in communication until it is moved to the active state.
  - One unit acts as **Master**, the others as **Slaves.**
  - Master manages the channel access by using a **polling** algorithm.



BR/EDR

Frame

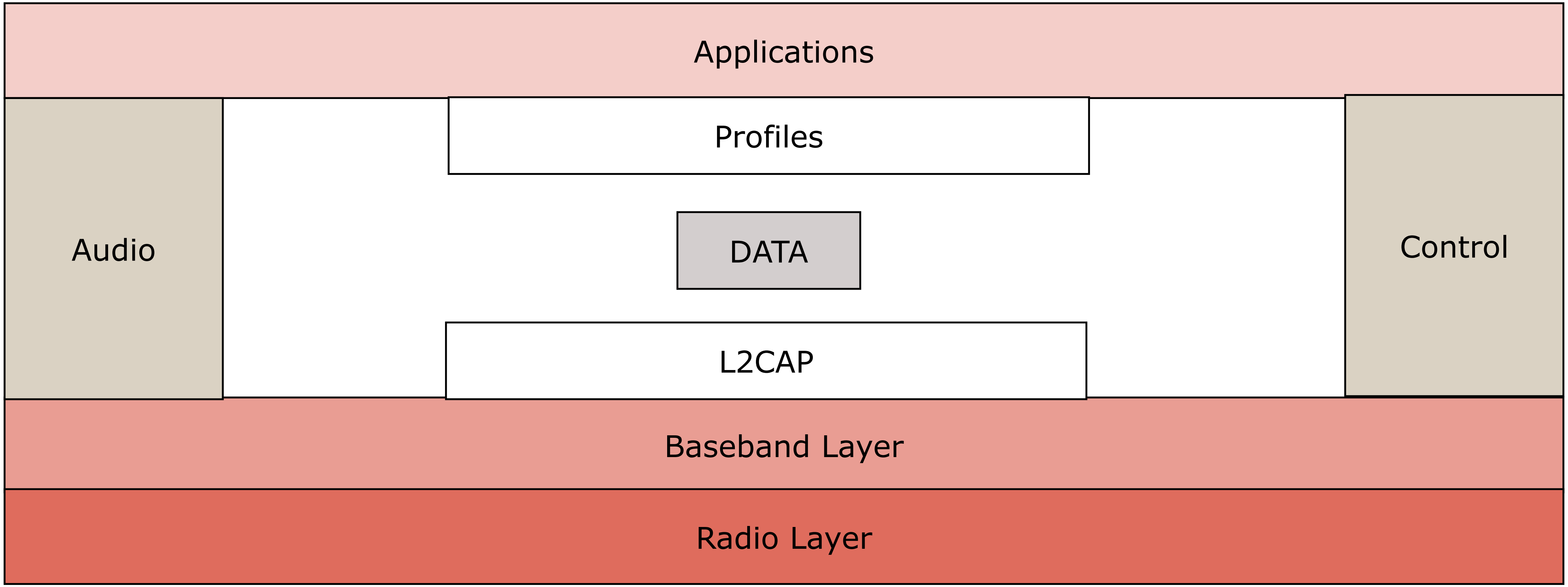
- **Access code**: Synchronization bits and piconet ID.
- **Header**: 18-bit pattern repeated 3 times.
  - Address (3 bits for 2^3-1=7 possible destinations in the piconet).
  - Type of message.
  - F: Flow (=1 is receiver cannot accept packets).
  - A: Acknowledgment (Stop and Wait, 1 bit is enough).
  - S: Sequence number (Stop and Wait, 1 bit is enough).
  - HEC: header error correction.



Internet of Things and Smart Cities

BR/EDR

Layers



BR/EDR

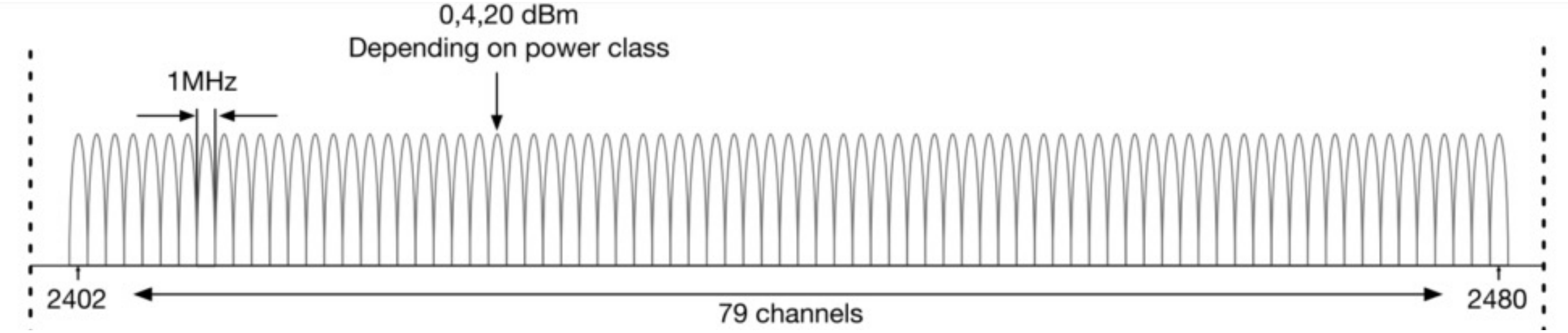
Radio Layer

- Roughly equivalent to the **PHY** layer in LANs.
- Three different **modulation** schemes:
  - Gaussian Frequency Shift Keying (**GFSK**) with Gaussian Filtering: 1 Mbit/s.
  - **π/4-DQPSK**: 2 Mbit/s.
  - **8-DQPSK**: 3 Mbit/s.

BR/EDR

Radio Layer

- Operate in the **2.4 GHz ISM band**, divided into 79 channels of 1 MHz each.
- The range depends on the transmission power (up to ~100 m).
- **Frequency-Hopping Spread Spectrum (FHSS)**: Bluetooth hops 1600 times/s→ frequency used for only 625 μs (**dwell time**) before it hops to another frequency.
  - This is also to reduce interference, since ISM bands are very crowded.

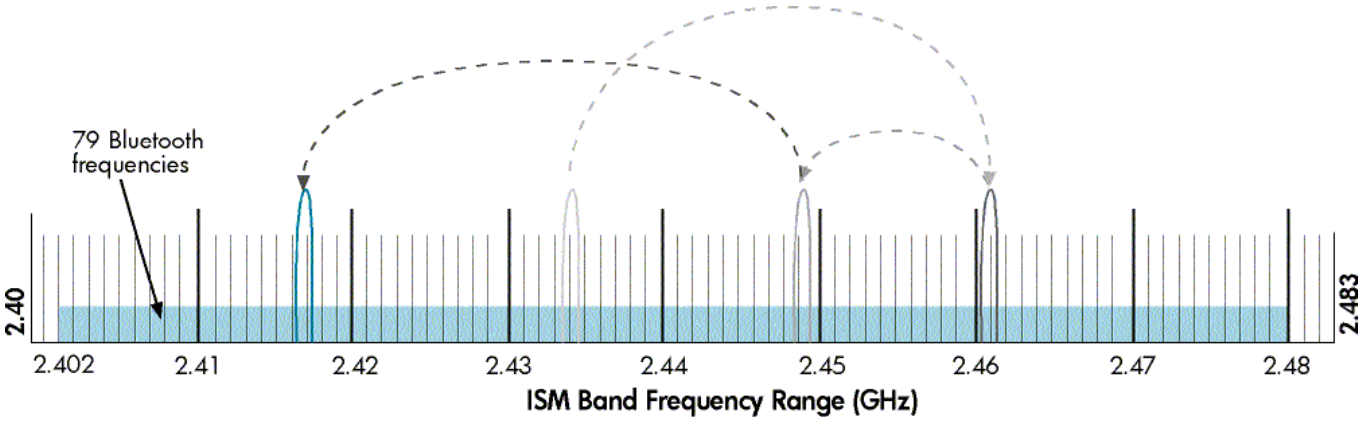


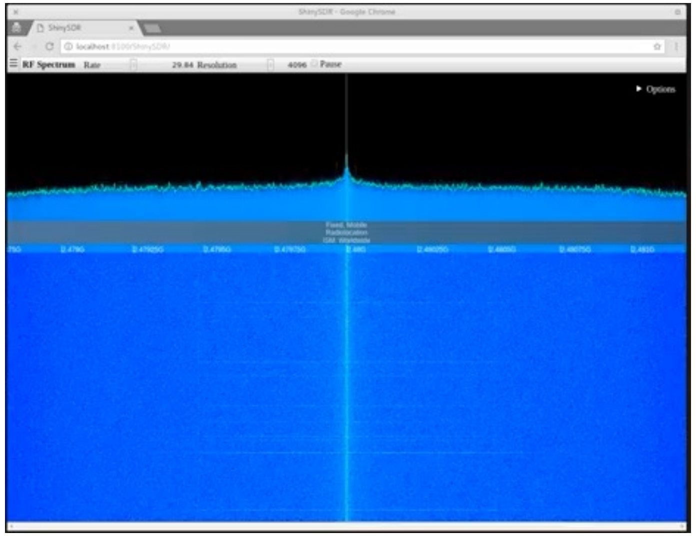
BR/EDR

Radio Layer – FHSS

Problem: where/how to hop? How can two devices know what is the next frequency to hop to? → Bluetooth needs **coordination** and **link establishment** (we'll see.....).

https://www.youtube.com/watch?v=6qNWQxRKoss



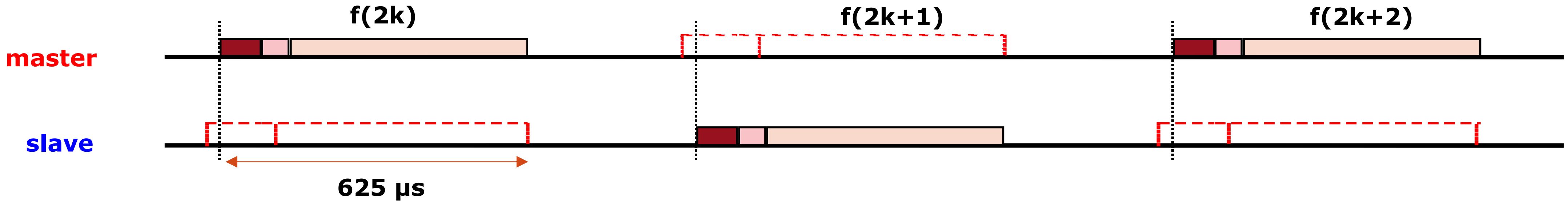


RF Spectrum Rate 29.84 Resolution 4096 □ Pause

BR/EDR

Baseband Layer

- Roughly equivalent to the **MAC** layer in LANs.
- **Time Division Duplex (TDD)**, with slots of 625 µs.
  - Bi-directional data transmission is realized by alternating slots in the two directions.
  - Master to a slave (**EVEN** slots) or slave to the master (**ODD** slots).
- Each transmission occurs on a different 1-MHz RF channel, according to a frequency-hopping pattern that is different for each piconet (this is similar to walkie-talkies using different carrier frequencies) → WHERE and HOW?

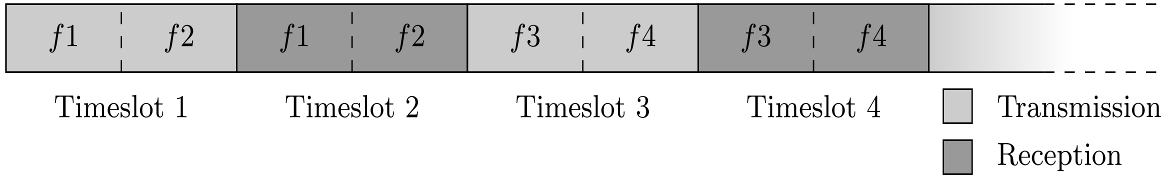


Internet of Things and Smart Cities

BR/EDR

Baseband Layer: Connection procedure

- **PHASE 1: Inquiry**
  - Master initializes the communication link.
  - Master establishes the pseudo-random hopping sequence for the piconet.
  - Terminals go in sleep mode.
- **PHASE 2: Paging (it may take a lot of time)**
  - The Master pages another Slave.
  - The Slave sends a reply to the source (Device Access Code (DAC)).
  - The Master sends the list of future planned hops of frequency.
  - The Slave sends a second DAC to the source.



BR/EDR

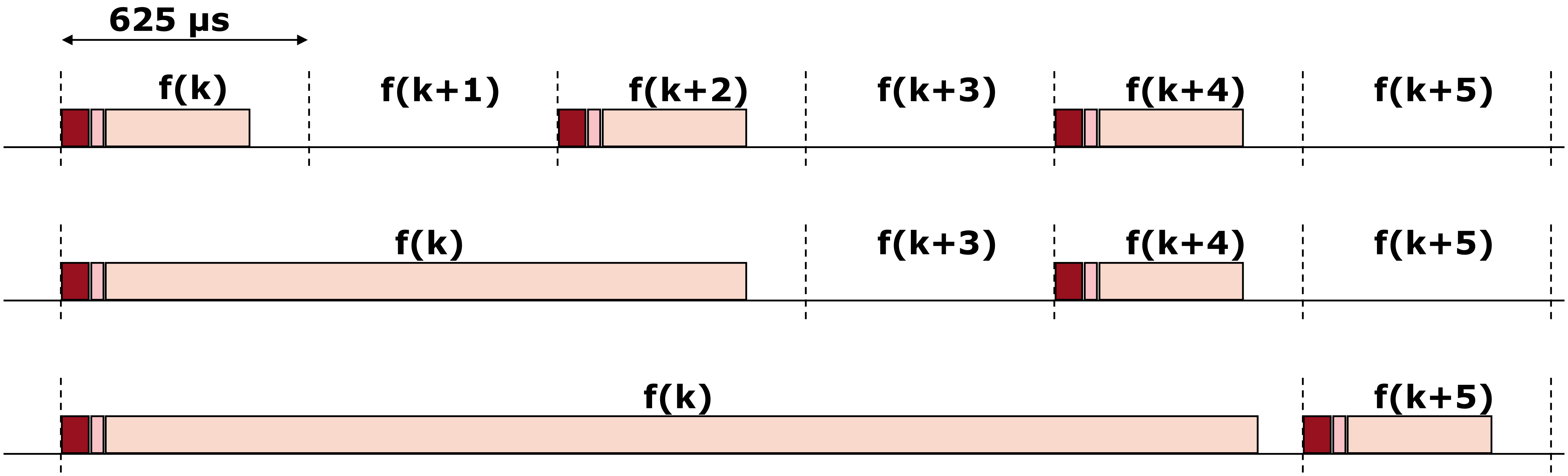
L2CAP

- **Logical Link Control and Adaptation Protocol (L2CAP)** is used for multiplexing, segmentation, reassembly, QoS and group management.
- Supports two types of communication:
  - **Synchronous Connection Oriented (SCO)** (latency more important than integrity).
    - Synchronous, symmetric, connection-oriented service.
    - MAC is deterministic: slots reserved to voice traffic at regular time intervals.
  - **Asynchronous Connection-Less (ACL)** (integrity is more important than latency).
    - Packet oriented, asymmetric, asynchronous.
    - If a payload encapsulated in the frame is corrupted, it is retransmitted.
    - Packets can be 1, 3 or 5 slot long.
    - Carrier frequency does not change during the transmission in a multislot.
    - Multislot packets reduce overhead due to header and guard time (~259 μs).

BR/EDR

L2CAP ACL

- Packets can be 1, 3 or 5 slot long.



Internet of Things and Smart Cities

BR/EDR

Profiles

- **Profiles**: different application-specific protocol stacks.
- Nearly 40 profiles.
- Some profiles have a quite narrow application score (e.g., headset profile).
- Some profiles support more flexible and general applications (e.g., PAN).
- The networking capability of BR/EDR depends on the profile.

List of Bluetooth profiles
https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles

BLE

Overview

- **Bluetooth Low Energy (BLE)** is a more recent extension meant specifically for sensors or low-power IoT devices.
- Some differences wrt BR/EDR:
  - Fewer channels: 40 (2 MHz) instead of 79 (1 MHz).
    - 3 (out of 40) **advertisement channels** for special use.
  - **GPSK** modulation only.
  - Data rate up to 2 Mbit/s (vs. 1 Mbit/s in GPSK-BR/EDR).
    - Higher data rate results in shorter transmission times → **less energy consumption**.
  - Lower power consumption.
  - Different codes for error protection.
  - Dwell time for frequency hopping is only determined during connection establishment.

BLE

Communication modes

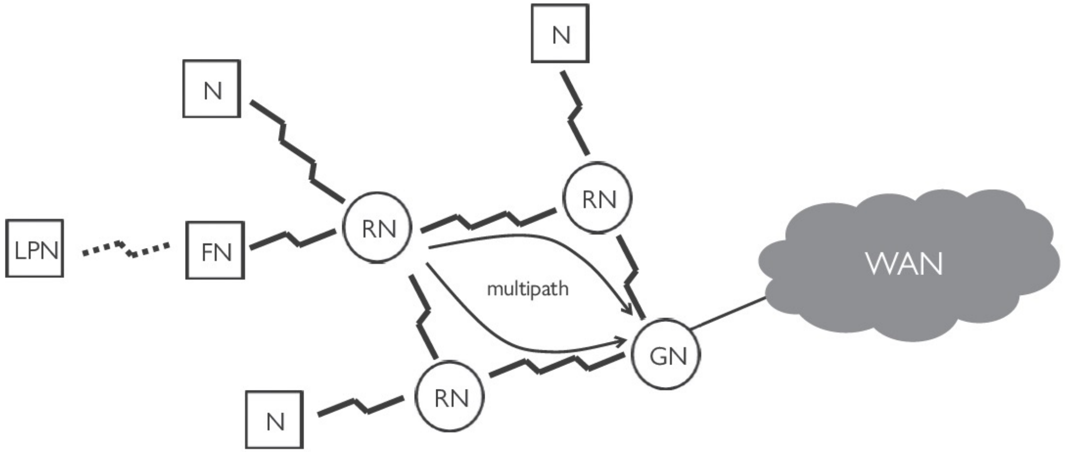
- In BLE the nodes can assume 4 roles (vs. 2 in BR/EDR):
  - **Broadcaster**: a node which periodically transmits advertisements, but does not allow connections to be established (e.g., iBeacon).
  - **Observer**: a node that just listens for advertisements and does not attempt to open connections (e.g., smartphone with an active localization App).
  - **Peripheral**: a node which transmits advertisements and may accept connection requests, acting as a **Slave**.
  - **Central**: a node which may open connection towards a peripheral, acting as the **Master** once the information relative to a peripheral has been received through advertisements.

BLE

New profiles

- New profiles: Heart Rate, Internet Protocol Support Profile, **Mesh Profile**…
- **Mesh Profile**: it allows the creation and management of mesh networks.
  - Some nodes may act as relays.
  - **Low Power Nodes**: sleep for some time, and wake up periodically to talk with **Friend Nodes** nearby, which store the message that they could not receive while sleeping.
  - **Managed flooding mechanisms** to avoid loops.

RN: relay node
GN: gateway node
LPN: low power node
FN: friend node



BR/EDR vs. BLE

Comparison

Feature	BR/EDR	BLE
Power consumption	Higher	Lower
Data rate	Up to 3 Mbps (8-DPSK)	Up to 2 Mbps (GFSK)
Latency	Lower	Higher
Connection Type	Point-to-point	Point-to-point, broadcast, mesh
Use case	Audio, peripherals, …	IoT, wearables, sensors. …
Compatibility	Classic Bluetooth devices	Bluetooth 4.0 and newer