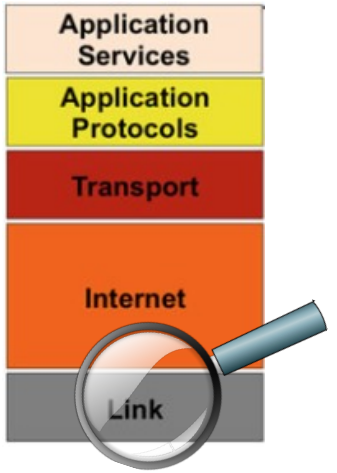
Ch. 11 - IoT Link Layer

Sec 2 – Short Range

COMPSCI 147

Internet-of-Things; Software and Systems



Overview

- IEEE 802.15.4: low-rate wireless personal area network (LR-WPAN)
- IEEE 802.15.4e (Time Slotted Channel Hopping)

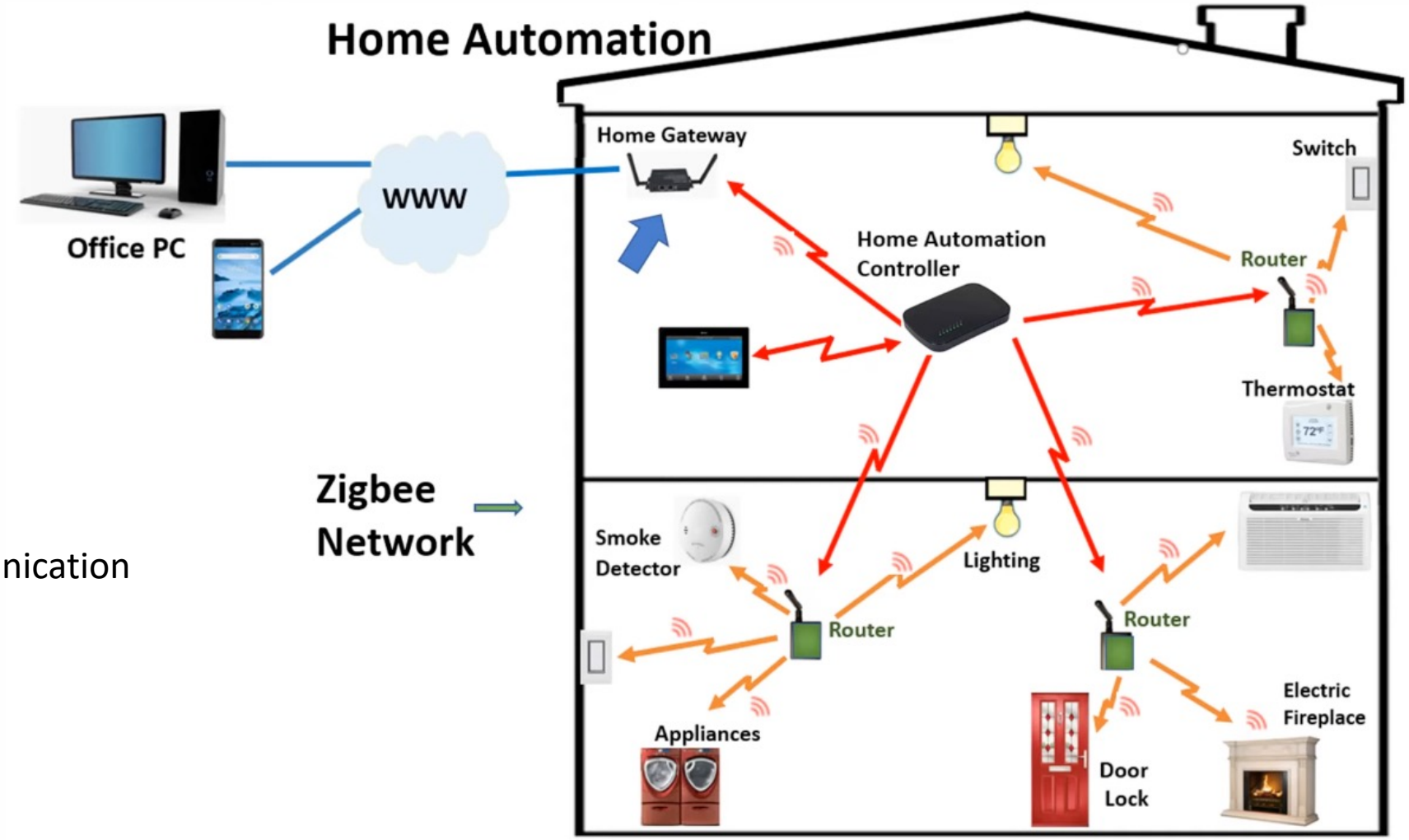
- IEEE 802.15.1 (Bluetooth, BLE)

- IEEE 802.11ah (Wi-Fi HaLow)

Zigbee

ZigBee® Alliance

- Low-cost,
- Low-power,
- Low-data rate
- For short wireless communication

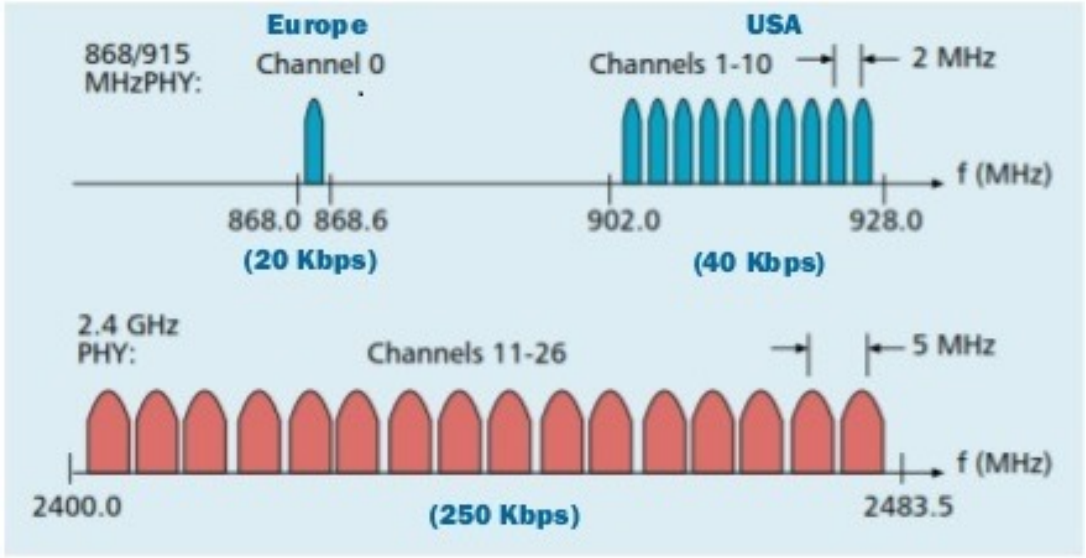


IEEE 802.15.4 (ZIGBEE)

- **Low data rate** wireless mesh connectivity
  - Data rates of 1 Mbps, 850, 250, 100, 40, and 20 kbps
- Very **low complexity** and extended **battery** life-span
  - Multiple months to multiple years
- **Unlicensed** international frequency band
- Transmission range: from tens of meters up to 1 km
- One of the most commonly used standards for IoT
- Fully **acknowledged** for transfer **reliability**
- Foundation for several protocol stacks (both IP and non-IP)
  - Zigbee, Zigbee RF4CE, Zigbee Pro, 6LoWPAN, Wireless HART and RPL

IEEE 802.15.4 (ZIGBEE)

- 868.0–868.6 MHz:
  - **Europe**, allows **one** communication channel
- 902–928 MHz:
  - **North America**, up to **thirty** channels
- 2400–2483.5 MHz:
  - **Worldwide** use, up to **sixteen** channels



IEEE 802.15.4 (ZIGBEE)

- Typical application areas include:
  - Home/Building automation
  - Wireless sensor networks
  - Industrial control systems
  - Embedded sensing/ Medical data collection
  - Smoke and intruder warning

IEEE 802.15.4 (ZIGBEE): TYPES OF DEVICES

- Three types of devices:

Coordinator

- Most Capable device
- Root of the network
- One coordinator in each network

Tasks
- Channel Selection
- Assign network ID
- Allocate unique addresses to each device

Routers

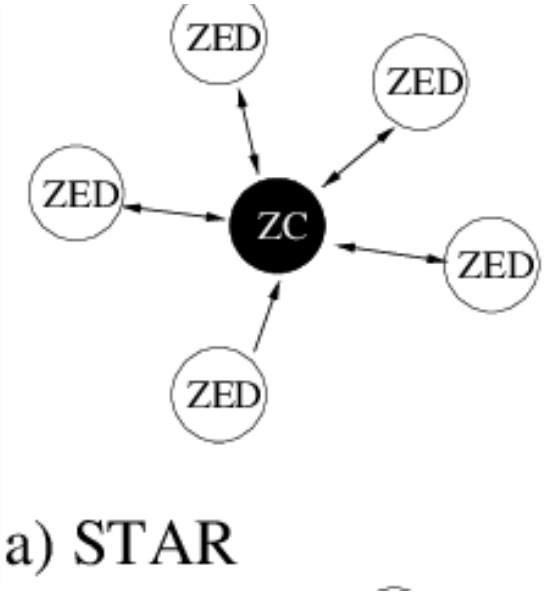
- Intermediate nodes (between coordinator and end-device)
- Route traffic between nodes
- Buffer messages

End Device

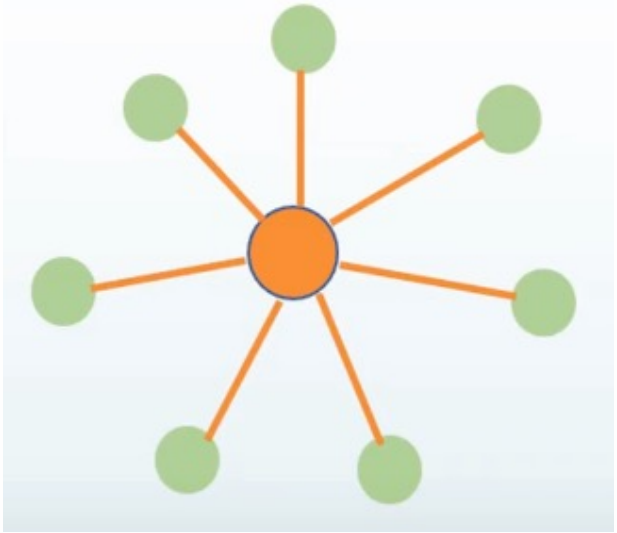
- Minimal information to talk to parent
- May sleep

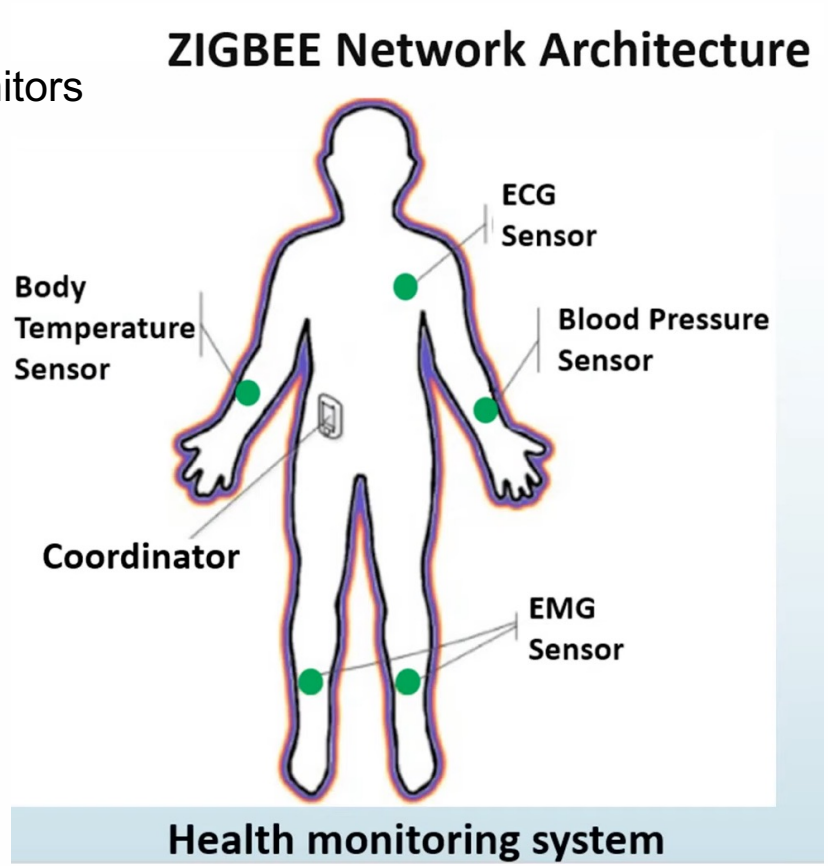
IEEE 802.15.4 (ZIGBEE): STAR TOPOLOGY

- Star
  - One single central controller
    - Simplest and least expensive to implement
    - No routers, end devices cannot talk to each other
  - Other nodes are most likely battery-operated
  - Applications: Smart homes, computer peripherals, personal health monitors



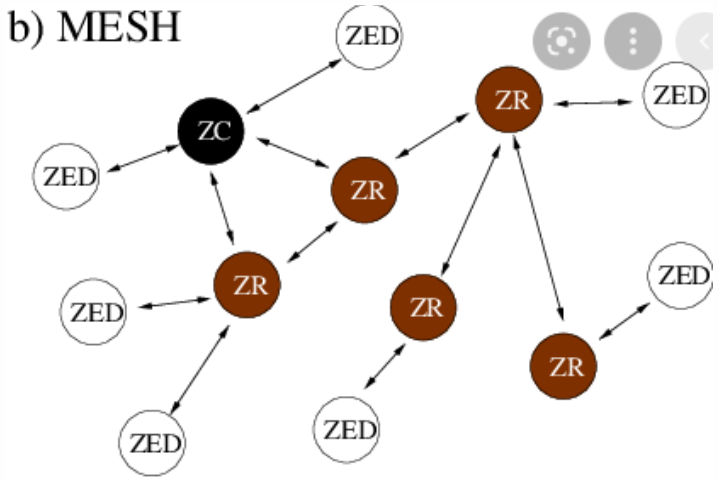
a) STAR

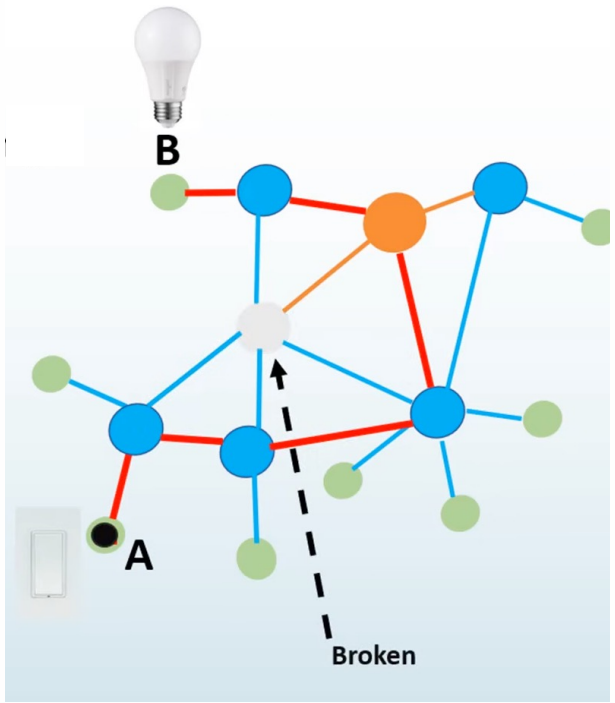


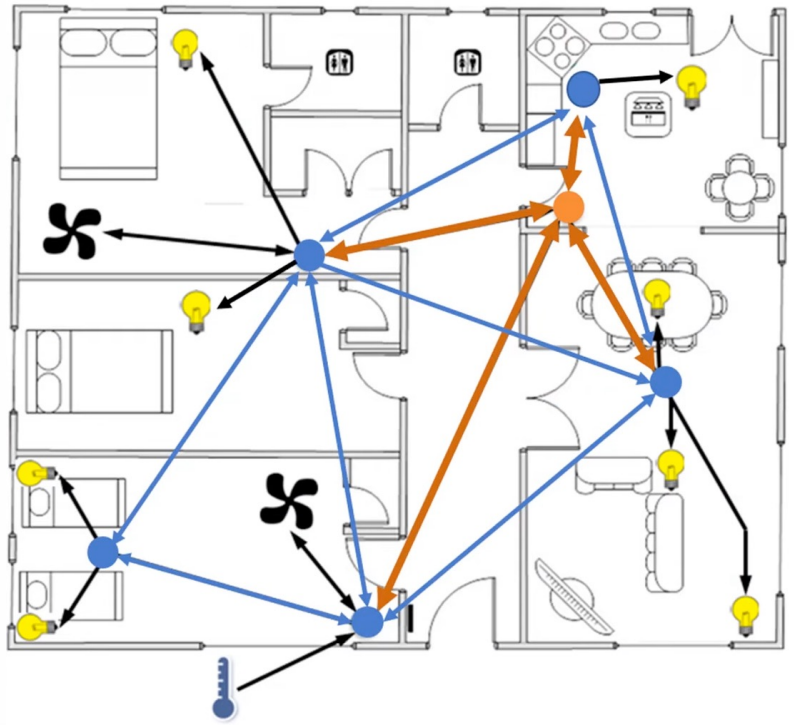


IEEE 802.15.4 (ZIGBEE): MESH TOPOLOGY

- Mesh
  - Any device can communicate with any other device if the two are within radio range
  - Can be ad-hoc in formation, self-organizing, and self-healing on node or link failures
  - Reliability through multipath routing
  - Applications: Precision agriculture, environmental monitoring, security, inventory management

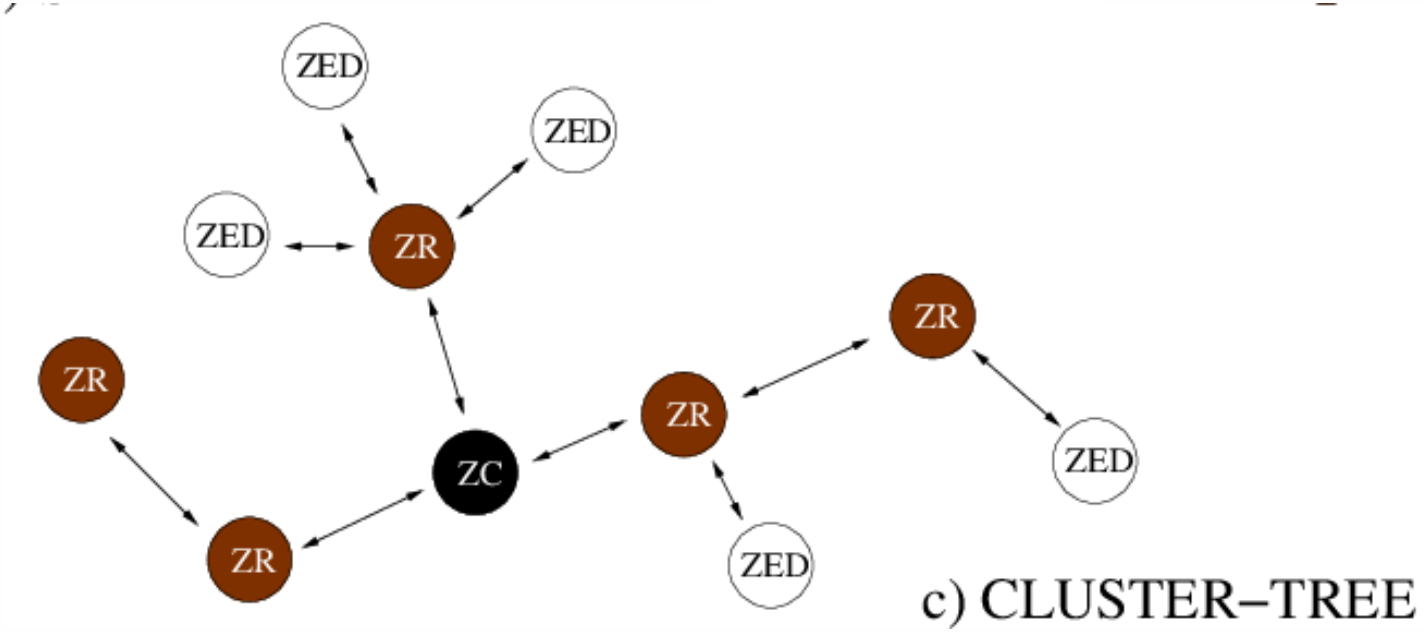


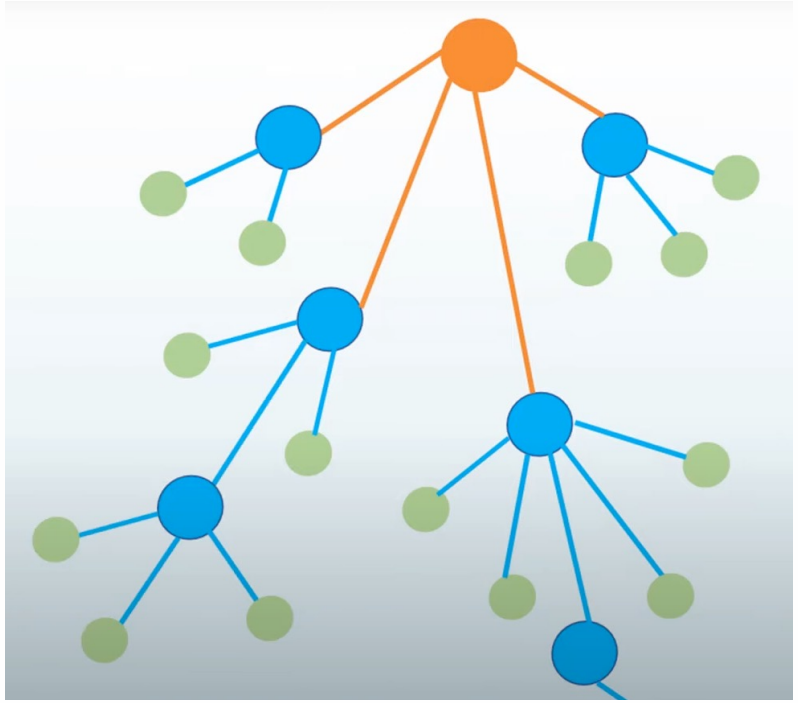




IEEE 802.15.4 (ZIGBEE): CLUSTER –TREE TOPOLOGY

- Cluster-tree
  - A special case of a mesh and hierarchical
  - Routers are not interconnected
  - The ability to achieve larger coverage area at the expense of increased message latency



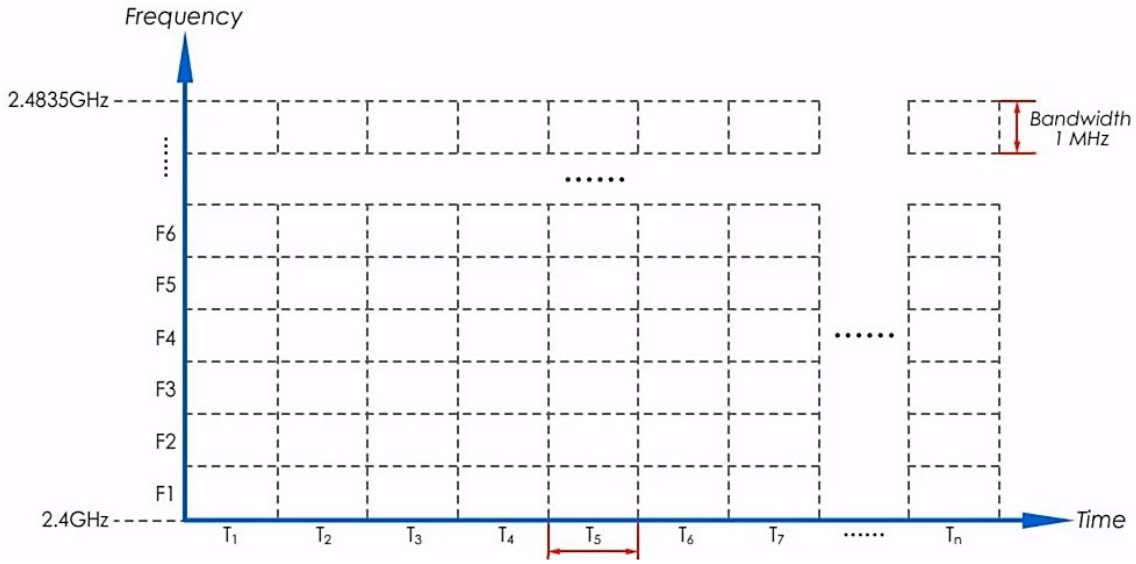


IEEE 802.15.4E TSCH

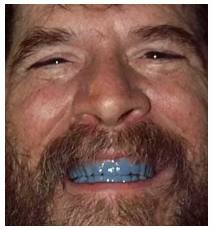
- Next-generation 802.15.4 wireless mesh standard
  - Lower energy consumption
  - Increased reliability
- A new MAC layer while maintaining the same PHY layer
  - Supported on existing 802.15.4 hardware
- Key added capabilities:
  - Time Synchronization (or Timeslotted) (TS) = > lowering energy consumption
  - Channel Hopping (CH) => increasing the reliability
- Time is sliced into fixed length timeslots and all nodes are synchronized
  - **Timeslots are grouped** into **slot frames** of **flexible** width
  - The flexibility allows different deployments to optimize for bandwidth or for energy saving

IEEE 802.15.4E TSCH

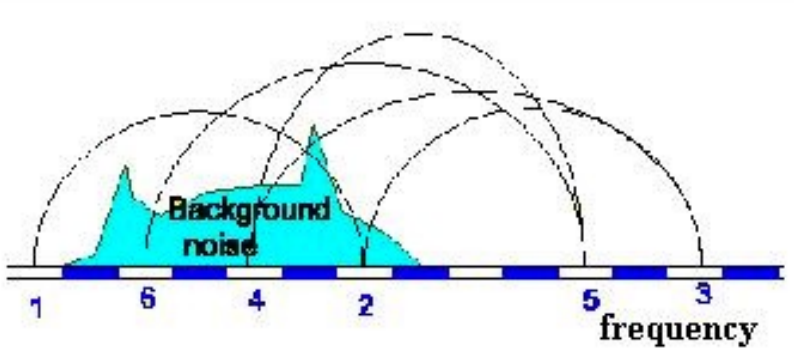
- Channel hopping
  - Each message transmission between nodes occurs on a **specified channel offset**.
    - Offset refers to the separation between the input frequency and output frequency of a repeater/node .
  - The channel offset is then mapped to a radio frequency.
  - If a specific frequency is subject to **fading** or **interference** only a subset of the messages will be lost.



IEEE 802.15.1 (BLUETOOTH)

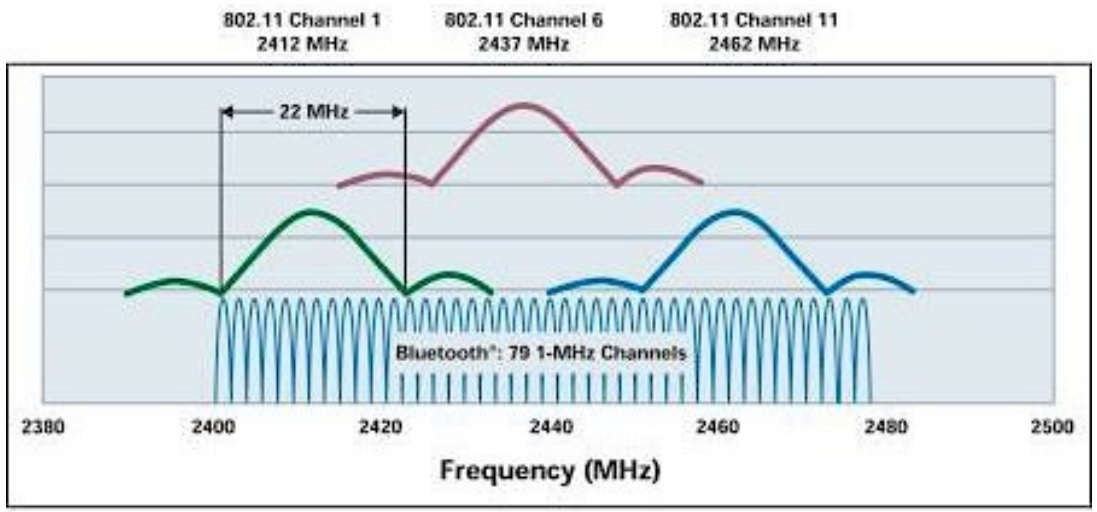


- Main **competitor** against IEEE 802.15.4 (ZigBee) until few years ago.
- The building block of a **Bluetooth Personal Area Network** is represented by the **Piconet**.
  - A set of up to 8 devices sharing the same physical channel
  - One of these devices assumes the role of **master** (establishing and managing the communication)
  - All the others play the role of **slave**
  - Devices **synchronized on the same clock** and adopt the same frequency hopping scheme
    - Time Division Multiplexing technique that divides the channel in 625/sec slots.
  - Transmissions occur in packets transmitted on **different hop frequencies**
    - Max freq rate of 1600 hops/s.



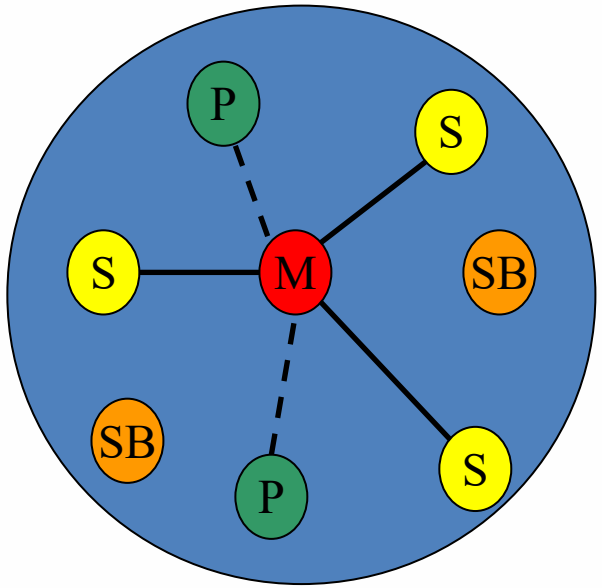
BLUETOOTH RADIO

- Uses 2.4 GHz ISM band spread spectrum radio (2402 – 2480 MHz)
- Advantages
  - Free
  - Open to everyone worldwide
- Disadvantages
  - Can be noisy (microwaves, cordless phones, garage door openers)



BLUETOOTH - PICONET

- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
- Non-piconet devices are in standby
- Video explanation
  - https://youtu.be/cxP0Mdoz_Bo



M=Master P=Parked
S=Slave SB=Standby

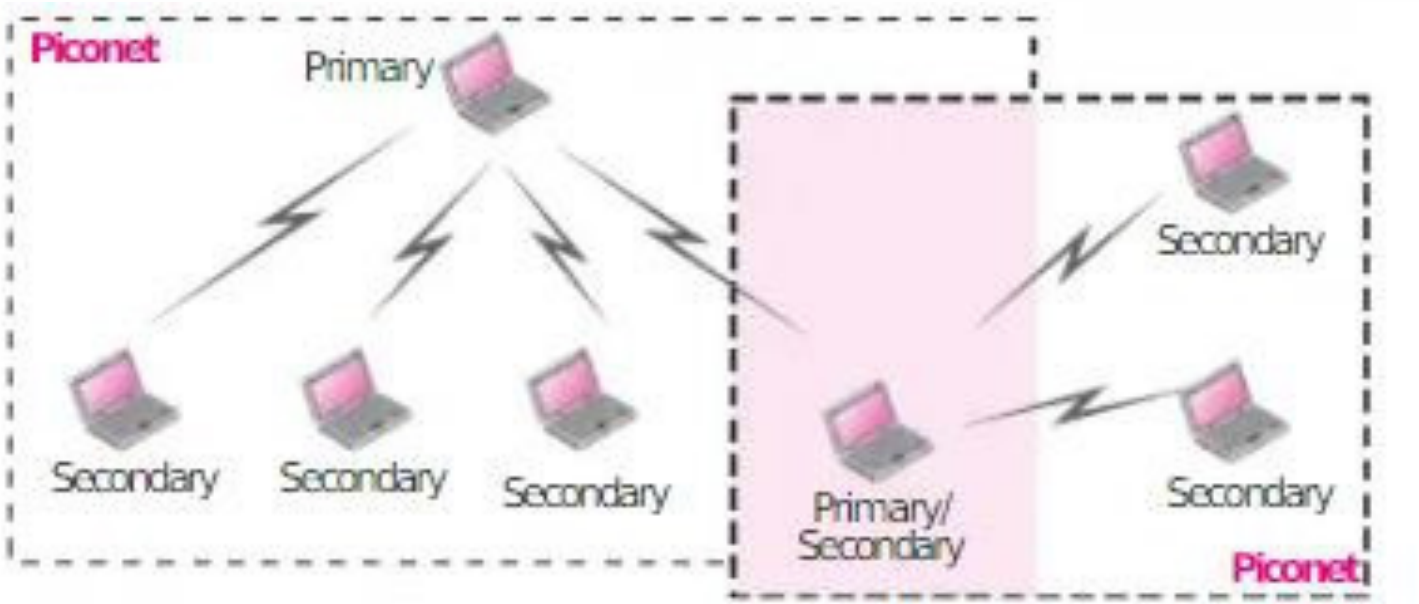
BLUETOOTH COMM. PROTOCOL

- The communication protocol is divided into two phases:
  - discovery phase
  - data exchange
- Bluetooth mainly presents **scalability issues** related to the **limited number of sensors per collecting device** (max 7 slaves for each piconet) and packet loss problems in case of **multiple piconets** for the same receiver (master) due to **interferences**.
- Even though **power** consumption during **transmission** is quite **low**, the need of Bluetooth devices to be **active** most of the time for device **discovery** or **joining** new piconets implies higher power requirements.

	Frequency range	Channels	Data rate
802.15.4	868 MHz	1	20 Kbps
	902–928 MHz	10	40 Kbps
	2.4–2.4835 GHz	16	250 Kbps
Bluetooth	2.402–2.480 GHz	79	1 Mbps

https://www.businessinsider.sg/why-bluetooth-sucks-bad-problems-issues-disconnects-2018-2/

Variant of Piconet: Scatternet



- Available in version 4 or newer
- Connects multiple piconets using Bluetooth
- A slave/secondary device can act as a master/primary for another piconet.
- Supports more than 8 nodes, by connecting piconets.

BLUETOOTH - CONNECTING TO INTERNET

- Being able to gain access to the Internet by using “Bluetooth access points”
  - Access point is used as a gateway to the internet
  - Both the access point and the device are Bluetooth-enabled
  - An example of Service Discovery Protocol
    - Access point provides a service to the device

BSP1000: Bluetooth SPP server designed to connect Bluetooth devices to the 10/100 Base-T Ethernet network.

BLUETOOTH LOW ENERGY (BLE) TECHNOLOGY

- Bluetooth for **low-power and low-cost applications** (2.4 GHz).
- It implements a completely **new lightweight Link Layer** that provides
  - Ultra-low power idle mode operation
  - Simple and fast device discovery
  - Reliable and secure point-to-multipoint data transfers
  - Allows mesh networking.
- Bluetooth-LE inherits **1 Mbps** data rate from classical Bluetooth and, in order to provide an **ultra-low power** transmission, it utilizes **short data packets with a dynamic length**.

HANDS ON LAB 4: ESP32

The Bluetooth stack of the chip is compliant with the Bluetooth v4.2 BR/EDR and Bluetooth LE specifications.

Classic Bluetooth

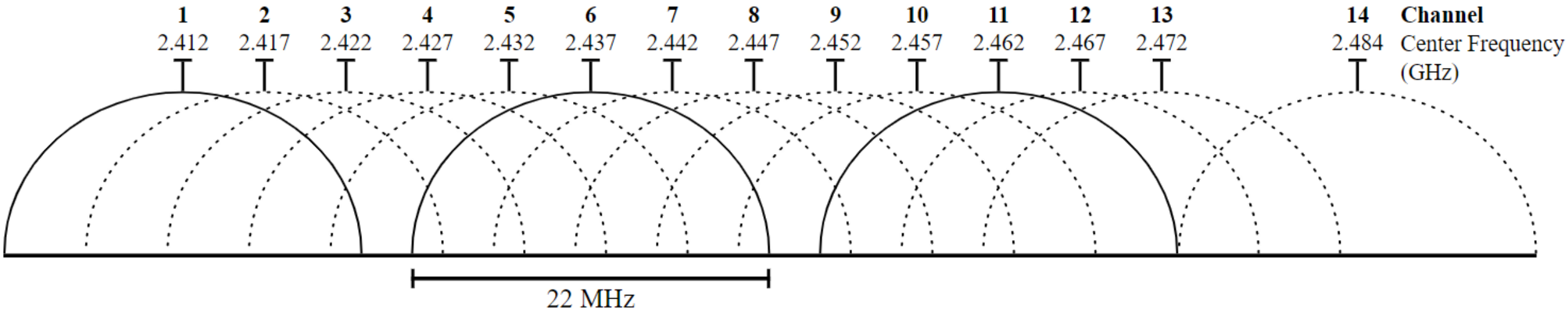
- Device Discovery (inquiry, and inquiry scan)
- Connection establishment (page, and page scan)
- Multi-connections
- Asynchronous data reception and transmission
- Synchronous links (SCO/eSCO)
- Master/Slave Switch
- Adaptive Frequency Hopping and Channel assessment
- Broadcast encryption
- Authentication and encryption
- Secure Simple-Pairing
- Multi-point and scatternet management

BLE

- Advertising
- Scanning
- Simultaneous advertising and scanning
- Multiple connections
- Asynchronous data reception and transmission
- Adaptive Frequency Hopping and Channel assessment
- Connection parameter update
- Data Length Extension
- Link Layer Encryption
- LE Ping

IEEE 802.11 (WI-FI)

- Original version released in 1997 and evolved over the years..



IEEE 802.11 (Wi-Fi): ESP-NOW

- ESP-NOW:
- Protocol developed by Espressif
- Connectionless Wi-Fi communication protocol
- Enables a direct and low-power control of ESP devices, without the need of a router.
- This method is convenient for device-to-device communication with short packets.

IEEE 802.11 (Wi-Fi): ESP-NOW

Advantages

- Encrypted and unencrypted unicast communication;
- Mixed encrypted and unencrypted peer devices;
- **Up to 250-byte** payload can be carried;
- Sending callback function that can be set to inform the application layer of transmission success or failure.

Disadvantages

- Limited encrypted peers. 10 encrypted peers at the most are supported in Station mode; 6 at the most in SoftAP or SoftAP + Station mode;
- Multiple unencrypted peers are supported, however, their total number should be less than 20, including encrypted peers;
- **Payload is limited to 250 bytes**.

IEEE 802.11 (Wi-Fi): ESP-NOW

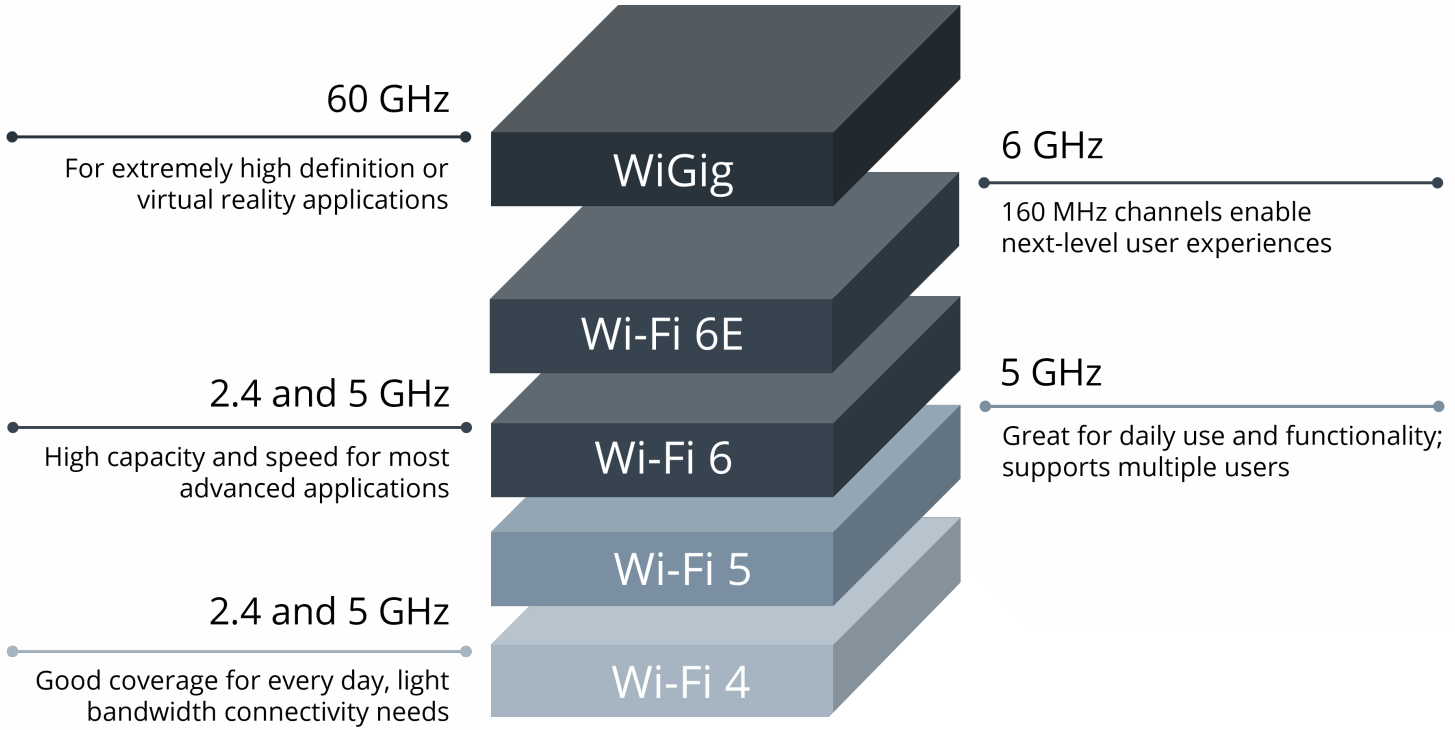
ESP-NOW Useful Functions

Here's a summary of the most essential ESP-NOW functions:

Function Name and Description
`esp_now_init()` Initializes ESP-NOW. You must initialize Wi-Fi before initializing ESP-NOW.
`esp_now_add_peer()` Call this function to pair a device and pass as an argument the peer MAC address.
`esp_now_send()` Send data with ESP-NOW.
`esp_now_register_send_cb()` Register a callback function that is triggered upon sending data. When a message is sent, a function is called – this function returns whether the delivery was successful or not.
`esp_now_register_rcv_cb()` Register a callback function that is triggered upon receiving data. When data is received via ESP-NOW, a function is called.

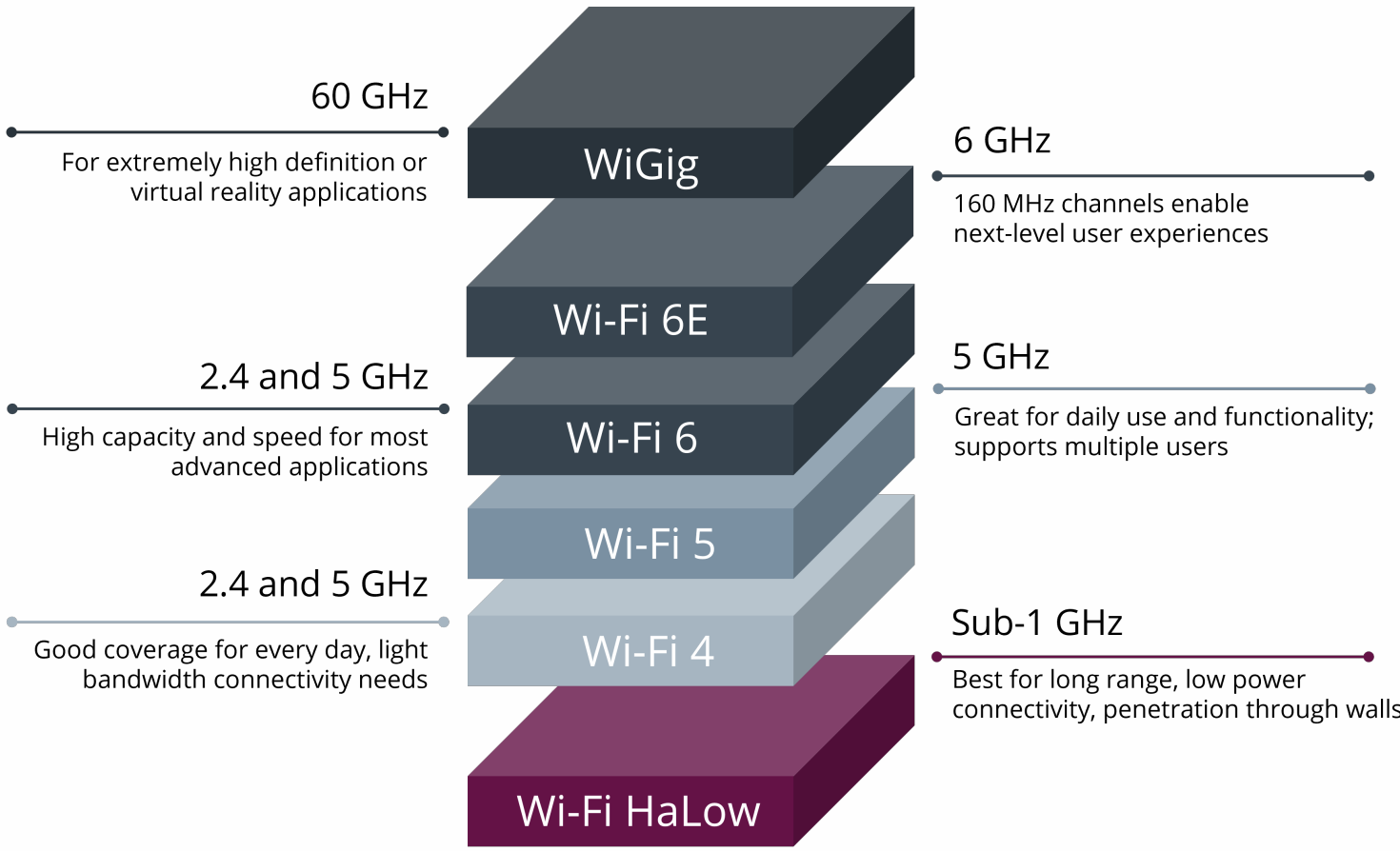
IEEE 802.11AH (WI-FI HALOW)

- Traditional IEEE 802.11 (Wi-Fi) cannot sufficiently address the requirements of IoT
  - High power consumption for Client Stations
    - The need for client devices **to wake up at regular intervals** to listen to **AP** announcements
  - Unsuitable frequency bands
    - 2.4 – 5 GHz frequency bands => **short transmission range** and **high degree of loss**



IEEE 802.11AH (WI-FI HALOW)

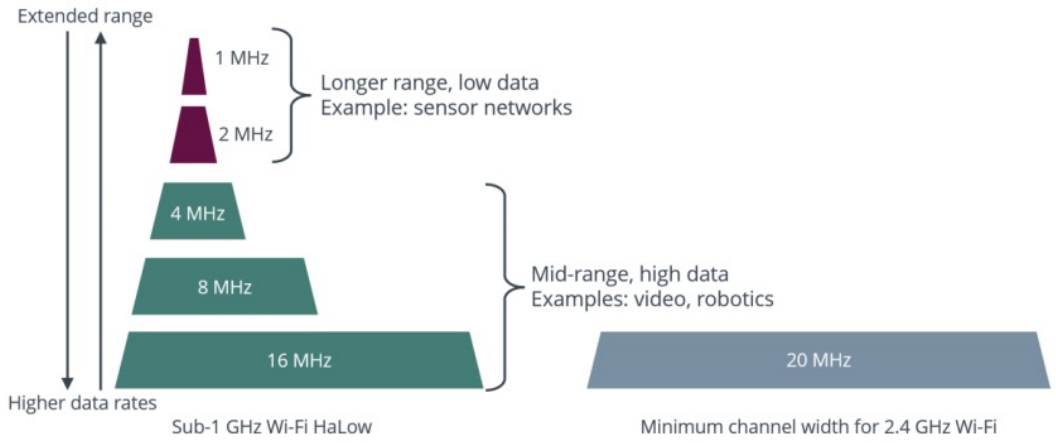
- IEEE 802.11**ah** (Wi-Fi HaLow)
- Released in 2017
- A wireless connectivity solution competing against BLE
  - **Allows large # devices**
  - **long** transmission **range**
  - **small** and **infrequent** data messages (100 bytes, >30s) (low data rates)



IEEE 802.11AH (WI-FI HALOW)

- Uses the 900 MHz industrial, scientific and medical (ISM) unlicensed bands to extend the Wi-Fi range.
- Enhancements over Wi-Fi
  - Client stations save **power** through **longer sleep times** and reducing the need to wake up
  - Reducing the overhead (more efficient handling)
    - Reducing frame headers
    - Simplifying and speeding management frames exchanges

Country	Various IEEE 802.11ah/ Wi-Fi HaLow Frequency Band allocation
China	755 - 787 MHz
Europe	863 - 868 MHz
Japan	916.5 - 927.5 MHz
Korea	917.5 - 923.5 MHz
Singapore	866 - 869 & 920 - 925 MHz
USA	902 - 928 MHz



IEEE 802.11AH (WI-FI HALOW)

- Transmission range of up to **1 km** (outdoor)
  - Data rates above **100 kbps**
- Scalability => a large # devices (up to **8191**) per AP
- New PHY and MAC layers
  - better penetration of the radio waves through obstructions
- Different channel availability in different countries
  - Europe: 868 – 868.6 MHz
  - USA: 902 – 928 MHz
  - China: 314 – 316, 390 – 434, 470 – 510 and 779 – 787 MHz
- Data rates ranging from **150 kbps** up to **340 Mbps**

IEEE 802.11AH (WI-FI HALOW)

Wi-Fi CERTIFIED HaLow™ for IoT

Features

- Sub-1 GHz spectrum operation
- Narrow band OFDM channels
- Several device power saving modes
- Native IP support
- Latest Wi-Fi® security

Benefits

- Long range: approximately 1 km
- Penetration through walls and other obstacles
- Supports coin cell battery devices for months or years
- No need for proprietary hubs or gateways