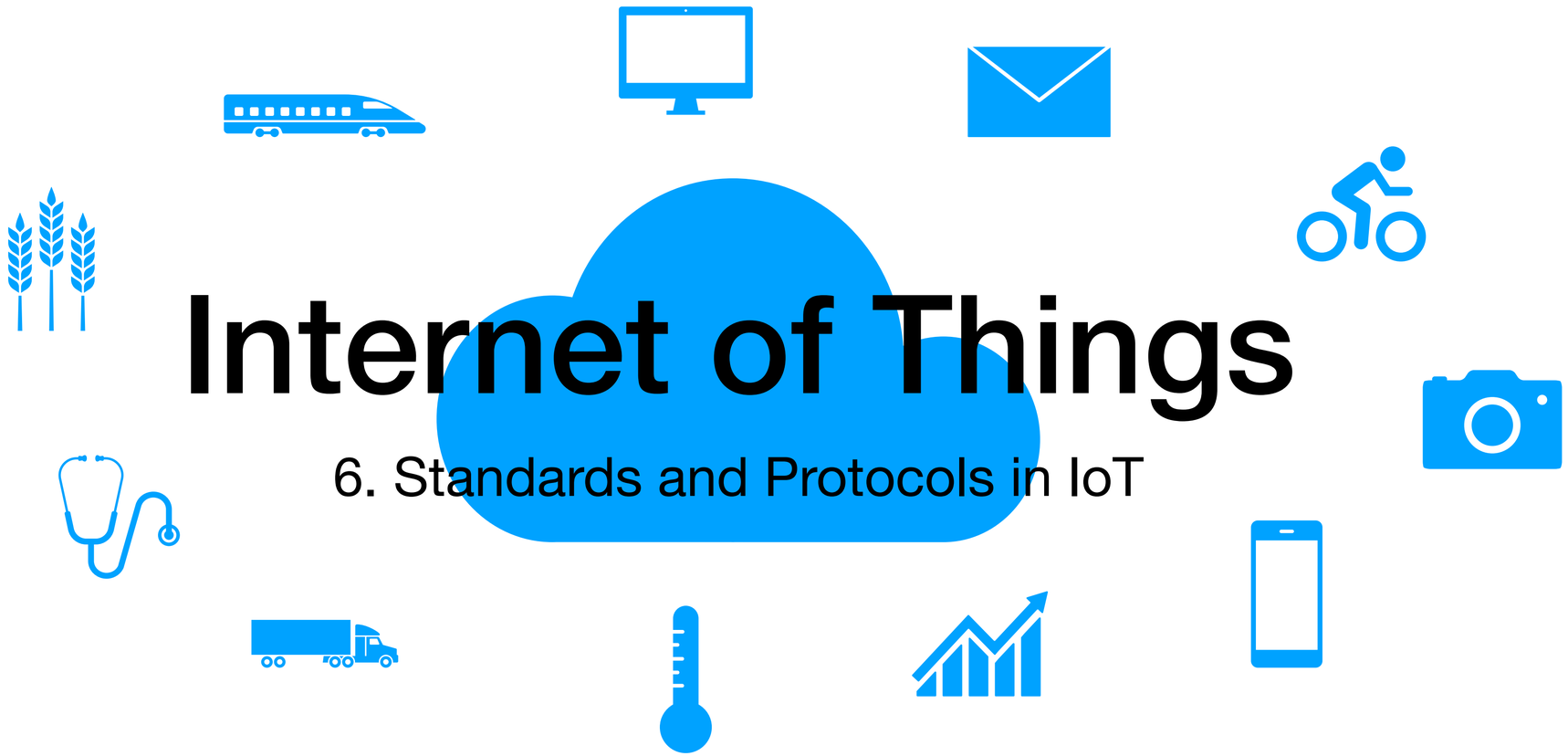


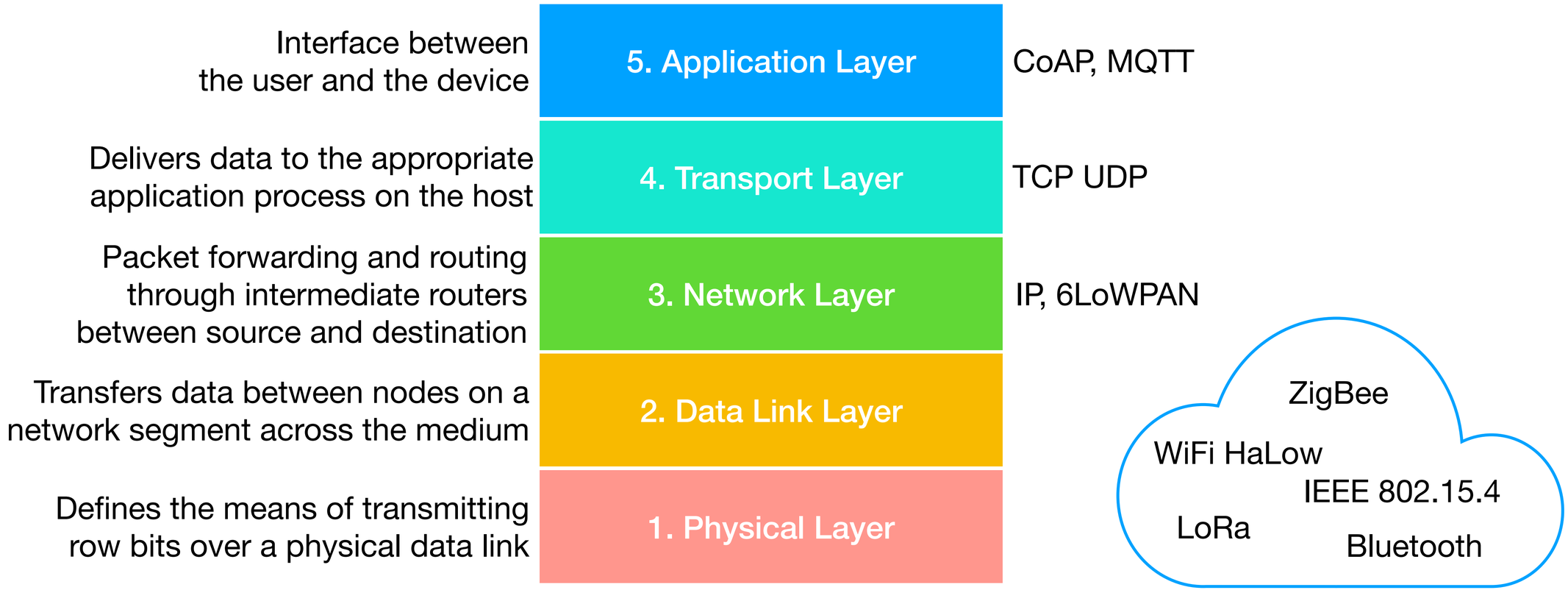
Internet of Things

6. Standards and Protocols in IoT

M.Sc. Computer Science 2024-2025

Viviana Arrigoni

- A protocol is a set of rules and procedures that define how devices communicate in a network.
- A standard is an agreed-upon framework or a set of guidelines established by a governing body to ensure interoperability between different systems and vendors.
- Protocols and standards can operate on different layers



Radio spectrum regulation

- Radio spectrum is regulated by countries and/or organisations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).
    - They regulate how portions of the spectrum are allocated to different types of telecommunications such as radio, television, military, etc.
- In IoT access technologies, the frequency bands leveraged by wireless communication are either **licensed** or **unlicensed bands.**

Licensed Bands

- Licensed bands communication infrastructures are deployed by service providers and public services.
- Users must subscribe to services when connecting their IoT devices (subscription fee).

This adds more complexity to a deployment involving large numbers of sensors and other IoT devices

The network operator can guarantee the exclusivity of the frequency usage over the target area (lack of congestion, minimal interference).

- Licensed bands are used in cellular networks, satellite communication, emergency services, FM/AM radio and TV.

Unlicensed Bands

- The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands (**ISM bands**).
- Mostly used in communication technologies for **short-range devices** (SRDs).
- Unlicensed does not mean unregulated.
  - Regulations exist, mandating devices on parameters such as transmit power, duty cycle, channel bandwidth…

Simpler deployment than licensed (does not require a service provider).

Can suffer from more interference because other devices may be competing for the same frequency in a specific area.

- Most well known ISM bands:

2.4 GHz band (WiFi)

IEEE 802.15.1 Bluetooth

IEEE 802.15.4 WPAN

Unlicensed Bands - sub-GHz bands

- Some protocols within the ISM bands operate in the sub-GHz range

✓ Sub-GHz frequency bands allow greater distances between devices.

✓ These bands have a better ability than the 2.4 GHz ISM band to penetrate building infrastructures or go around obstacles.

✗ Lower rate of data delivery compared to higher frequencies.

Didn’t we say that unlicensed bands are for short range communication?

- Sub-ghz bands allow for longer distances, but sending low power signals that degradate early, allows to create multiple small networks with very little interference.

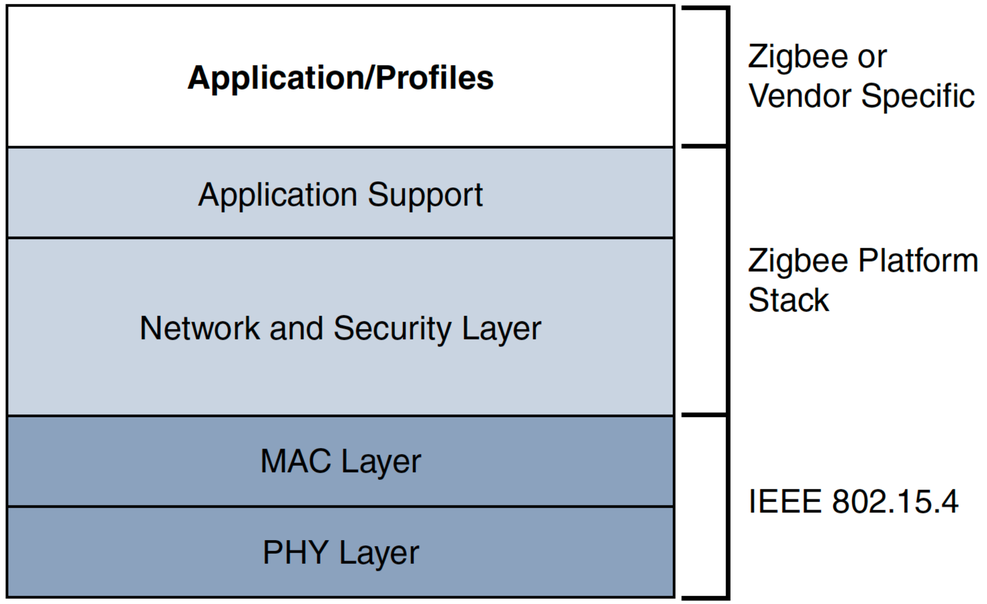
6.1 Layer 1 and 2 Protocols
6.1.1 IEEE 802.15.4

- IEEE 802.15.4 is a wireless technology for low-cost, low-data-rate devices that are battery-powered, whose batteries may need to last months
- Deployed in WSNs and MANETs, and in the network range of WPAN.
- Defines low-data-rate **PHY** and **MAC** layer specifications
- The IEEE 802.15.4 PHY and MAC layers are the foundation for several networking protocol stacks.

ZigBee

- ZigBee solutions are aimed at smart objects with low bandwidth and low power needs.
- ZigBee-compliant products can interoperate even though different vendors might manufacture them.
  - 400 companies are members of the **ZigBee Alliance**, an industry group to certify interoperability between vendors.
- Mostly used in industrial automation (measuring temperature and humidity, tracking assets) and home applications (lighting thermostats and security control).

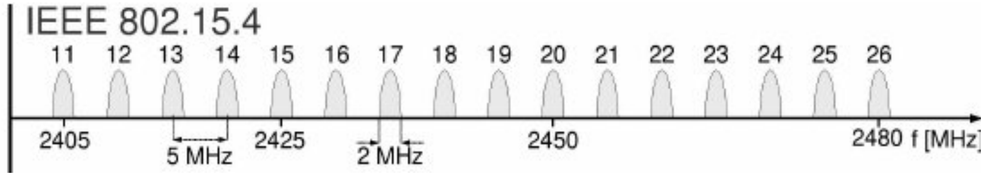
ZigBee stack



- PHY and MAC layers use IEEE 802.15.4 standard.
- Network and security layer provides mechanisms for network startup, configuration, routing and securing communication.
  - Hierarchical addressing
  - Ad hoc On Demand Distance Vector Routing.
- Uses 802.15.4 for security at the MAC layer.

802.15.4 PHY (1)

- The original IEEE 802.15.4 standard specified three PHY options:
  - 2.4 GHz, up to 16 channels with data rate of 250 Kbps (global)



Sub-GHz bands

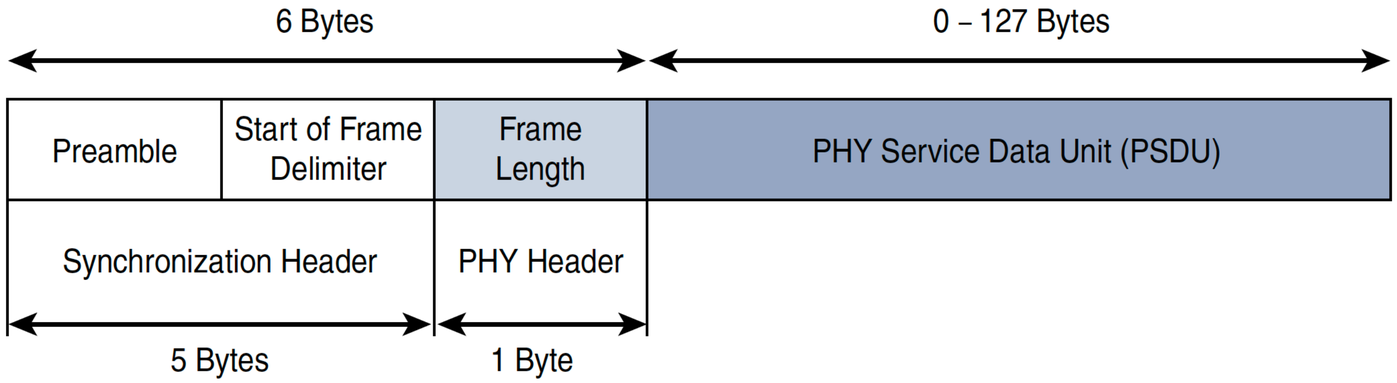
  - 902–928 MHz, 10 channels with data rate of 40 Kbps (North and South America)
  - 868.0–868.6 MHz, 1 channel with data rate of 20 Kbps (Europe, Middle East and Africa)
- Latest version (IEEE 802.15.4-2020) uses dozens of different frequency bands, optimised for regions and applications, allowing more flexibility. The 2400–2483.5 MHz frequency band remains unchanged.

802.15.4 PHY (2)

- The first release was based on Direct-Sequence Spread Spectrum (DSSS).
- The latest release, supports many different modulation schemes, including QPSK, BPSK, ASK, OOK,
- and supports a mix of **contention-based** and **contention-free** methods, depending on the MAC mode.

802.15.4 PHY Frame

- Synchronisation Header (5 bytes):
  - Preamble: identifies the start of the frame and is used to synchronise data transmission (4 bytes).
  - Start of Frame Delimiter: informs the receiver that frame contents start immediately after this byte (1 byte).
- PHY Header contains the frame length in number of bytes (1 byte).
- PSDU (PHY Service Data Unit) is the payload (0-127 Bytes).



Very smaller than the lowest MTU setting of e.g., IPv6, that is 1280 bytes. Fragmentation of IPv6 packets is required

802.15.4 MAC

- The 802.15.4 MAC layer manages access to the PHY channel by defining how devices share the frequencies allocated.
- The 802.15.4 MAC layer performs the following tasks:
  - **Network beaconing** for devices acting as coordinators (also, new devices use beacons to join a 802.15.4 network).
  - PAN **association** and **disassociation** by a device.
  - Reliable **link** communications between two peers MAC entities.

802.15.4 MAC Frame types

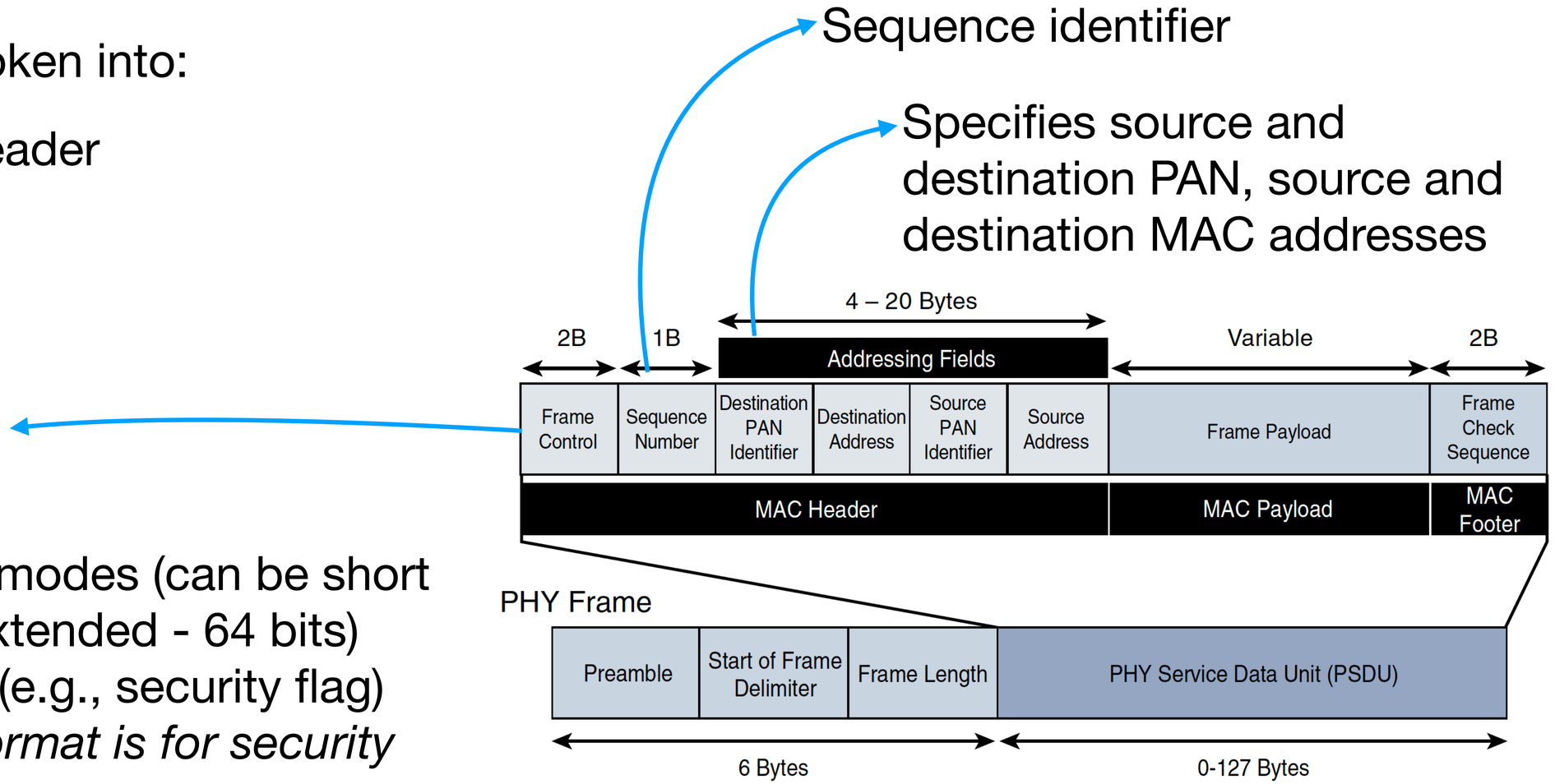
- To accomplish these tasks, uses four types of frames:
  - **Data frame:** handles all transfer of data
  - **Beacon frame:** used for beaconing by a PAN coordinator
  - **Acknowledgement frame:** confirms the successful reception of a frame
  - **MAC command frame:** controls communication between devices
- MAC frame is carried as the PHY payload (maximum of 127 bytes).

802.15.4 MAC Frame (1)

Can be broken into:

- MAC Header

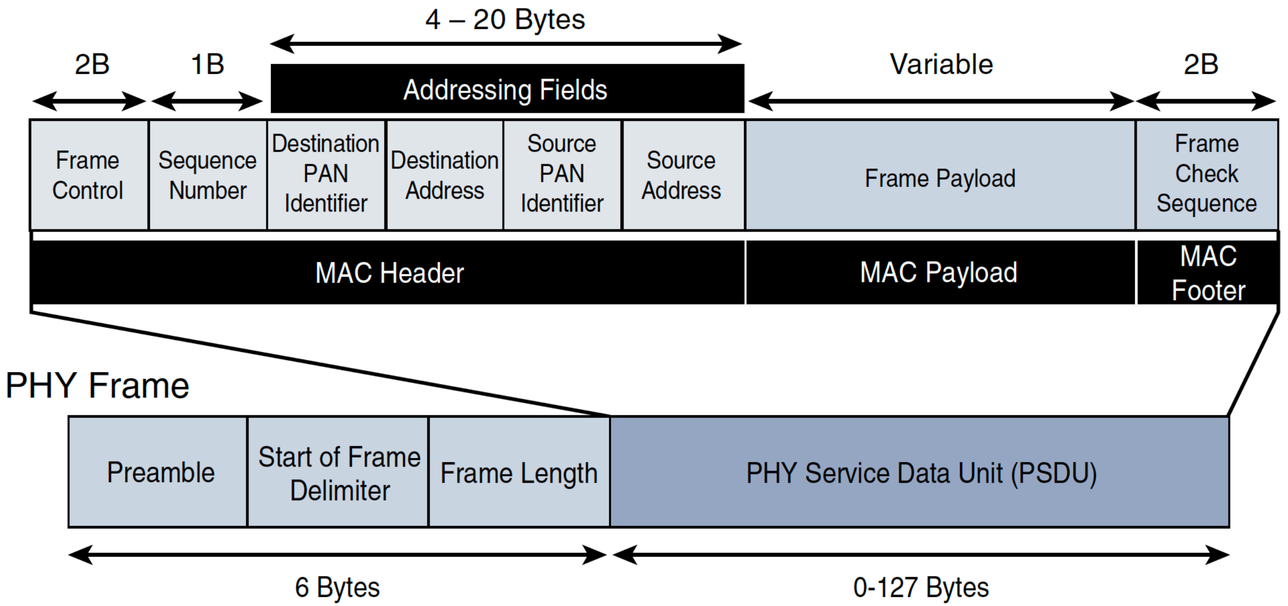
Defines:
-frame type
-addressing modes (can be short
-16 bits or extended - 64 bits)
-control flag (e.g., security flag)
this frame format is for security flag = 0



802.15.4 MAC Frame (2)

Can be broken into:

- MAC Payload, variable length depending on frame type.
- The MAC footer is a frame check sequence used by the receiver to check integrity.



802.15.4 MAC Frame (3)

- IEEE 802.15.4 requires all devices to support a unique 64-bit extended MAC address (assigned by the vendor).
  - Because the maximum MAC frame length is 127 bytes, the standard also defines how a 16-bit “short address” is assigned to devices by the coordinator.
  - The short address is local to the PAN and substantially reduces the frame overhead.

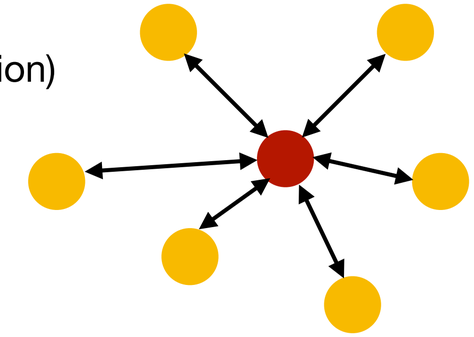
802.15.4 Topologies

- IEEE 802.15.4 supports networks with star, tree or mesh topologies.
- Every 802.15.4 PAN should be set up with a unique ID, shared among nodes in the same network.
- Two types of devices:
  - Full Function Devices - at least one acting as the coordinator, delivering services.
  - Reduced Function Devices

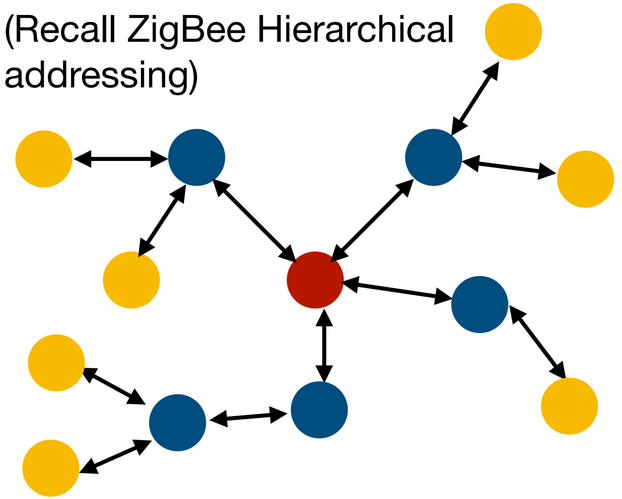
End device (reduced function)

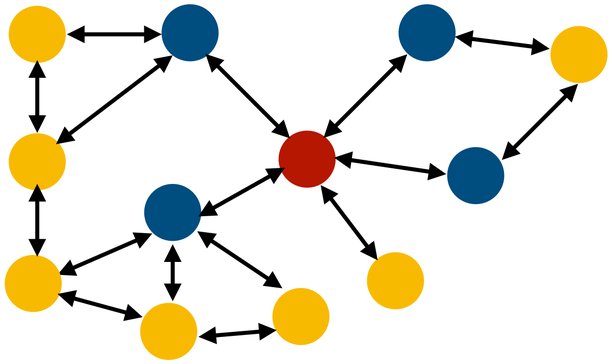
Router (full function)

Coordinator (full function)



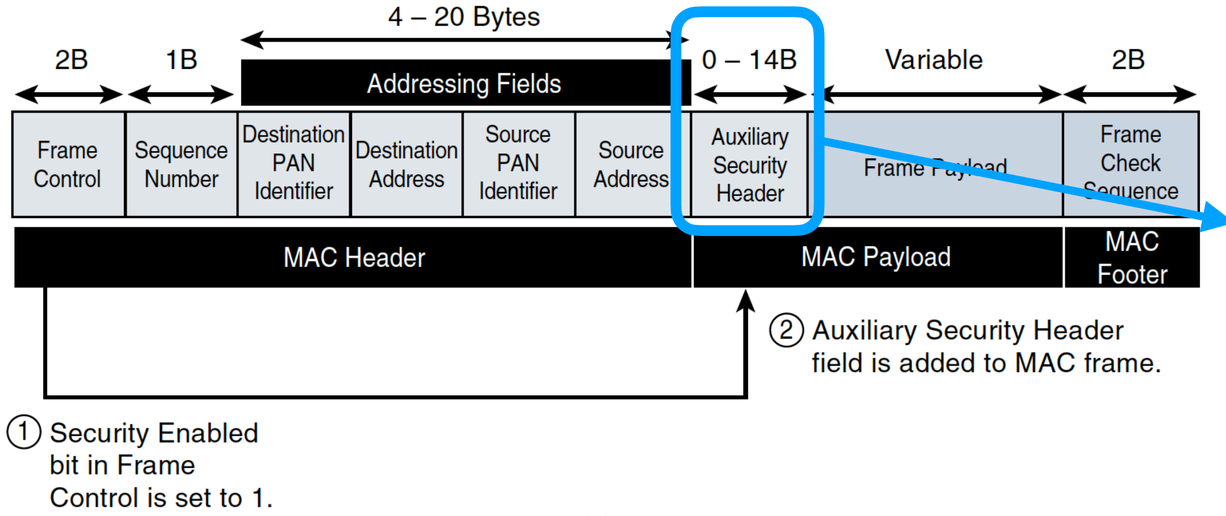
(Recall ZigBee Hierarchical addressing)





Security

- The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128 bit key length as the base encryption algorithm to secure its data.
- 802.15.4 validates sent data by a message integrity code (MIC), calculated from the entire frame using the same AES key.
- Enabling these features changes the frame format, consuming more payload.

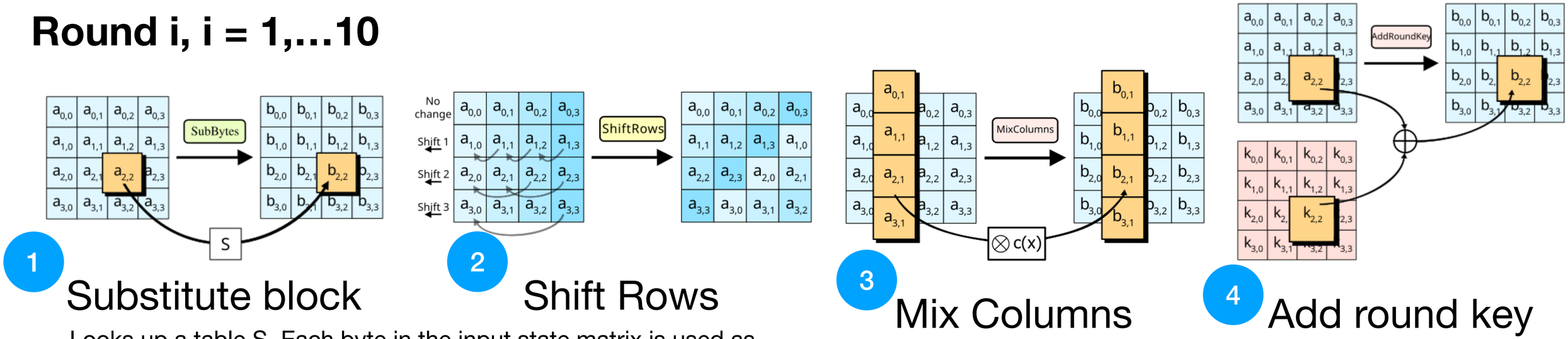


Contains key info for the receiver to validate the security features of the frame

Advanced Encryption Standard

- 128-bit symmetric block cipher
- AES arranges the 128 bite message in a 4x4 state matrix (each entry is one byte).
- **Key Schedule**: uses a 128-bit key to generate 11 round keys are derived (1 for each of 10 rounds + initial one) using a key expansion algorithm.
- **AddRoundKey**: XOR the state matrix with the first round key. Then run for 10 rounds these operations:

Round i, i = 1,…10



Substitute block

Looks up a table S. Each byte in the input state matrix is used as an index to find its corresponding replacement in the S table, which is built using operation in the 2-Galois field.

Shift Rows

Mix Columns

Add round key

6.1 Layer 1 and 2 Protocols
6.1.2 IEEE 802.11ah

IEEE 802.11

- IEEE 802.11 is the **WiFi** standard, the most successful wireless technology for unconstrained networks.
- It is a key wireless access technology:
  - Can connect endpoints such as computing nodes, high data rate sensors, audio/video analytics devices
  - WiFi backhaul infrastructures include also WiFi mesh in smart cities.

IEEE 802.11 versions

- 802.11 (1997), 2.4GHz, 2Mbps
- 802.11a (1999), 5GHz, 54Mbps
- 802.11b (1999), 2.4GHz, 11Mbps
- 802.11g (2003), 2.4GHz 54Mbps
- 802.11n (2009) 2.4GHz and 5GHz, 600 Mbps
- 802.11ac (2013), 5GHz, 6.93Gbps
- 802.11ax (2019), 2.4 GHz and 5GHz, 4x 802.11ac (if all wireless clients support 802.11ax)
- 802.11be (2024) - WiFi7, 2.4GHz, 5GHz, 6GHz (not many devices support it yet)

Came out the same year, 802.11a had better throughput but never took off because it needed a special silicon chip in the access point that was in shortage

802.11ah (WiFi HaLow)

Traditional WiFi

- designed for providing **high throughput for small-scale networks** with a **few dozen nodes** and a **coverage of tens of meters**.

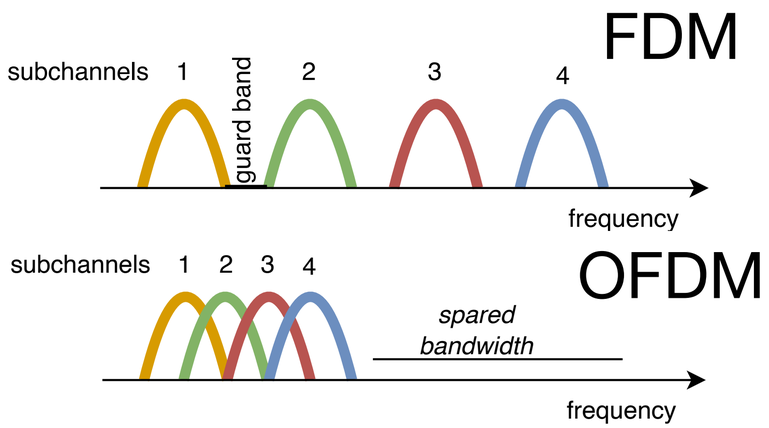
IEEE 802.11ah (2017)

- is the **first Wi-Fi solution optimised for IoT applications**.
  - It supports sub-GHz frequency bands for better signal penetration (up to **1km transmission range**), **low power** for battery-powered nodes, and the ability to support a **large number** of devices.

802.11ah PHY (1)

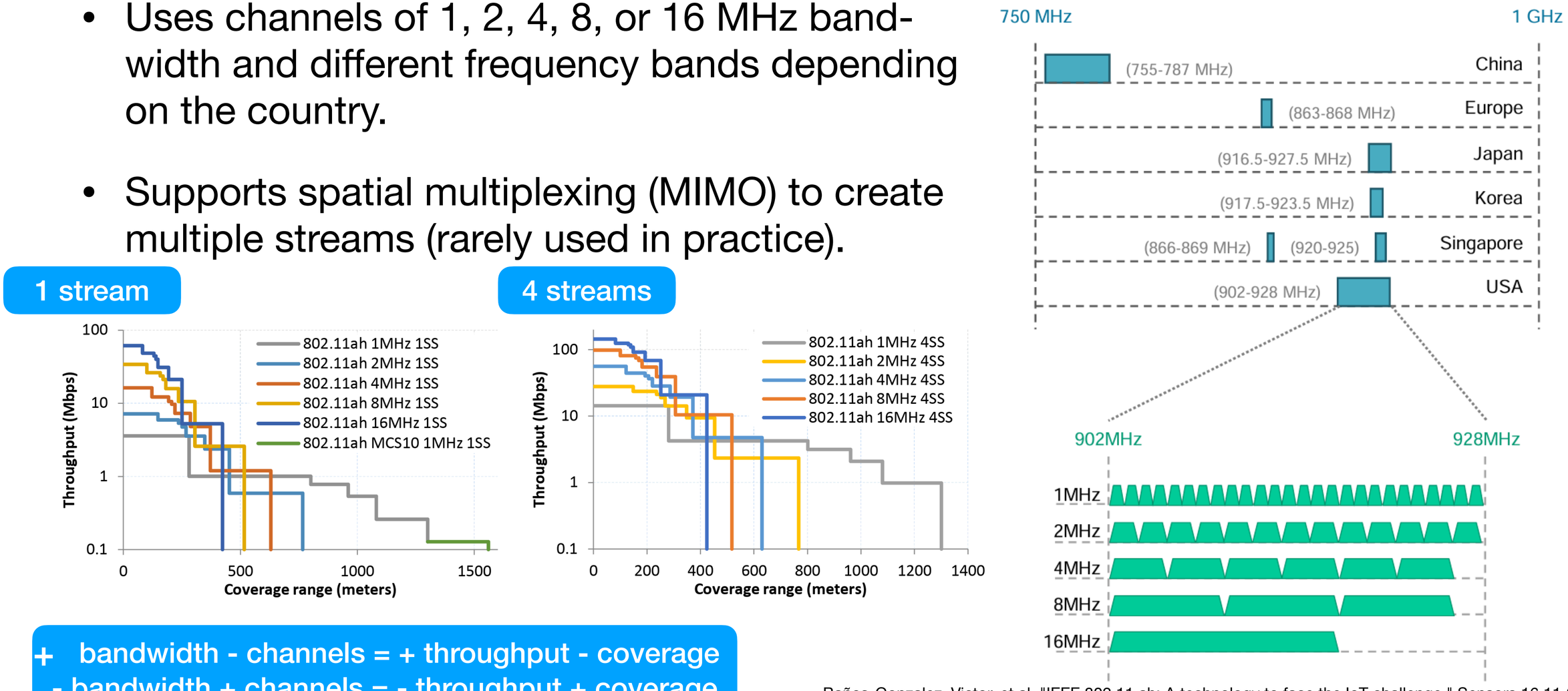
- Operates in unlicensed sub-GHz bands, varying from Country to Country.

- Uses Orthogonal Frequency Division Multiplexing (OFDM) modulation.
  - OFDM is a frequency-division multiplexing (FDM) scheme.
  - In FDM, signals are non overlapping.
  - In OFDM, signals overlap, but with peak of one signal being at the zero of other signals (orthogonality).
    - Improved bandwidth usage.



802.11ah PHY (2)

- Uses channels of 1, 2, 4, 8, or 16 MHz band-width and different frequency bands depending on the country.
- Supports spatial multiplexing (MIMO) to create multiple streams (rarely used in practice).



1 stream

4 streams

+ bandwidth - channels = + throughput - coverage
- bandwidth + channels = - throughput + coverage

Baños-Gonzalez, Victor, et al. "IEEE 802.11 ah: A technology to face the IoT challenge." Sensors 16.11 (2016): 1960.

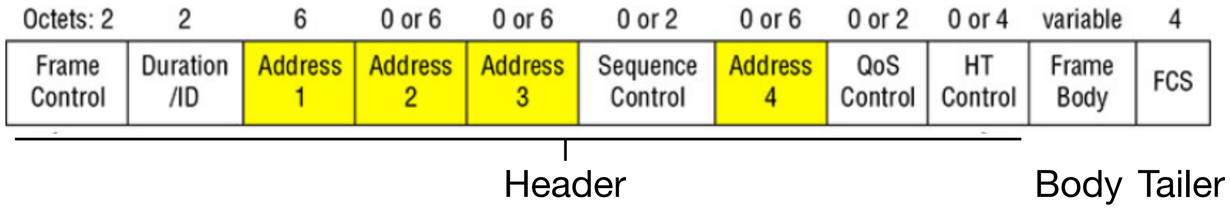
802.11ah MAC (1)

- The IEEE 802.11ah MAC layer is optimized to support the new **sub-GHz** Wi-Fi PHY while providing **low power consumption** and the ability to support **a larger number of endpoints.**

Differences wrt Wi-Fi

- Reduced Header in MAC frame
- Frame control: contains information about protocol version, type of frame (ACK, Beacon, etc), encryption status, etc.
- Sequence control: used to filter duplicate frames.
- Duration: represents the amount of time (in microseconds) that the medium will be occupied.
- Addresses of station/access points. Can use 3 or 4 addresses.
- QoS control: indicates the access category (AC), policy type, and payload type.
- High Throughput: manages advanced features such as MIMO, channel aggregation, and others.

802.11 Frame



802.11ah MAC (1)

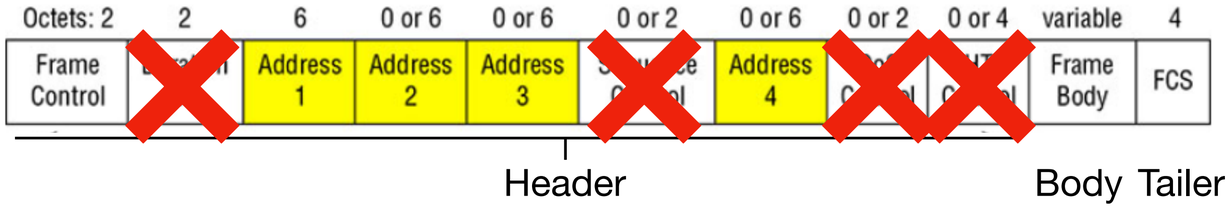
- The IEEE 802.11ah MAC layer is optimized to support the new **sub-GHz** Wi-Fi PHY while providing **low power consumption** and the ability to support **a larger number of endpoints.**

Differences wrt Wi-Fi

- Reduced Header in MAC frame
- Frame control: contains information about protocol version, type of frame (ACK, Beacon, etc), encryption status, etc.
- Sequence control: used to filter duplicate frames.
- Duration: represents the amount of time (in microseconds) that the medium will be occupied.
- Addresses of station/access points. Can use 3 or 4 addresses.
- QoS control: indicates the access category (AC), policy type, and payload type.
- High Throughput: manages advanced features such as MIMO, channel aggregation, and others.

Removed in 802.11ah MAC

802.11ah Frame



802.11ah MAC (2)

Differences wrt Wi-Fi

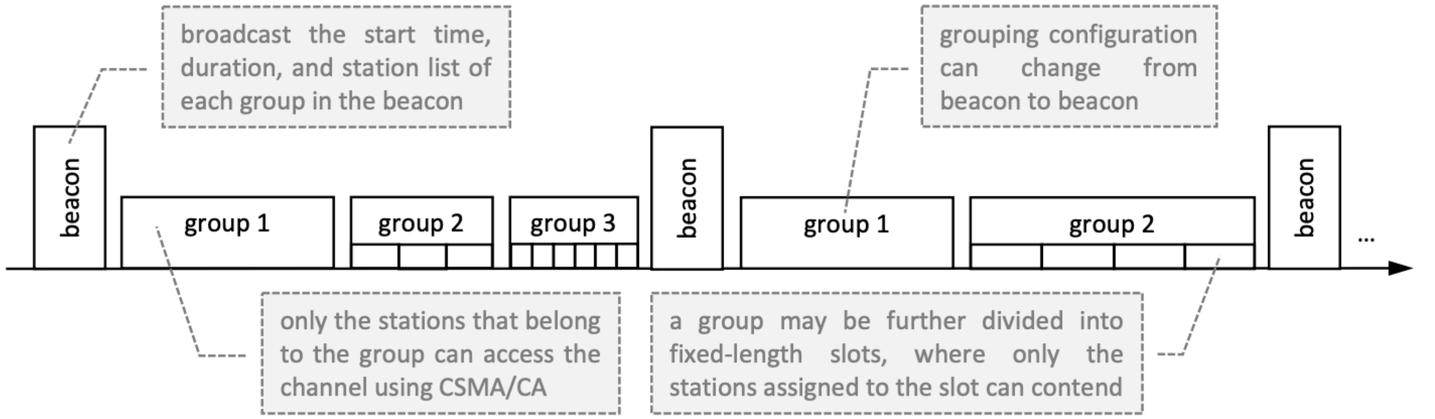
- Null Data Packet (NDP) Support:
  - Can send frames with no payload.
  - **Relevant information is concentrated in the PHY header** and the additional overhead associated with decoding the MAC header and data payload is avoided.
  - This change makes the control frame exchanges **efficient** and less power consuming for the receiving stations.
- Short Beacons:
  - In addition to full beacons.
  - Short beacons are sent more frequently when there are not changes in the network and at the lowest rate. Used for stay synchronisation and keep alive.
  - Full beacons are sent less frequently.

802.11ah MAC (3)

- Restricted Access Window (RAW) Mechanism:

Differences wrt Wi-Fi

- AP sends beacons to announce the presence of a wireless LAN and to provide a timing signal to synchronise communications with the devices using the network.
- 8192 devices per access point (possibly many collisions occur when stations want to talk to AP).
- The AP **allocates different time slots for medium access** during the beacon interval, called **Restricted Access Windows**, that are further divided into smaller time slots.
- RAW uses a combination of **TDMA** and **CSMA/CA**, and splits stations into groups and only allows stations assigned to a certain group to access the channel
- IEEE 802.11ah can provide two-level grouping to alleviate contention in a dense network.
- RAW groups are dynamically managed by the AP based on devices' behaviour, spatial location, QoS, and energy considerations.



802.11ah MAC (4)

Differences wrt Wi-Fi

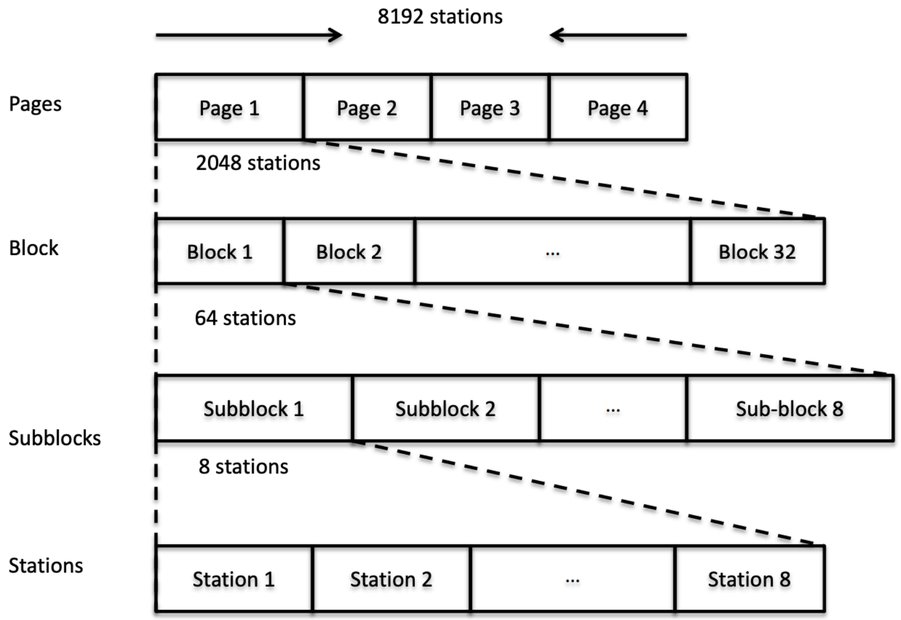
- Target Wake Time (TWT):
  - Reduces energy consumption by permitting an access point to define times when a device can access the network.
  - This allows devices to enter a low-power state until their TWT arrives.
  - It reduces the probability of collisions in areas with many clients.
  - Used for stations transmitting data sporadically.
- Group sectorization:
  - Consists in dividing different areas into into sectors (spatial division), each containing a subset of stations, aiming to mitigate hidden node problem, contention or interference.
  - It is particularly effective when the AP has multiple directional antennas.

802.11ah MAC (5)

- Hierarchical Organization:

Differences wrt Wi-Fi

- The AP assigns an AID (Association ID) to a station during association handshake. AID is 2^{13} bits long (8192).
- The AP supports Hierarchical Organization of AIDs.
  - Stations are organised in P pages of B blocks each. Each block contains 8 sub-blocks of 8 stations each.
  - Stations with similar characteristics are grouped together to reduce overheads while referring to them.



6.1 Layer 1 and 2 Protocols
6.1.3 LoRaWAN

LPWA

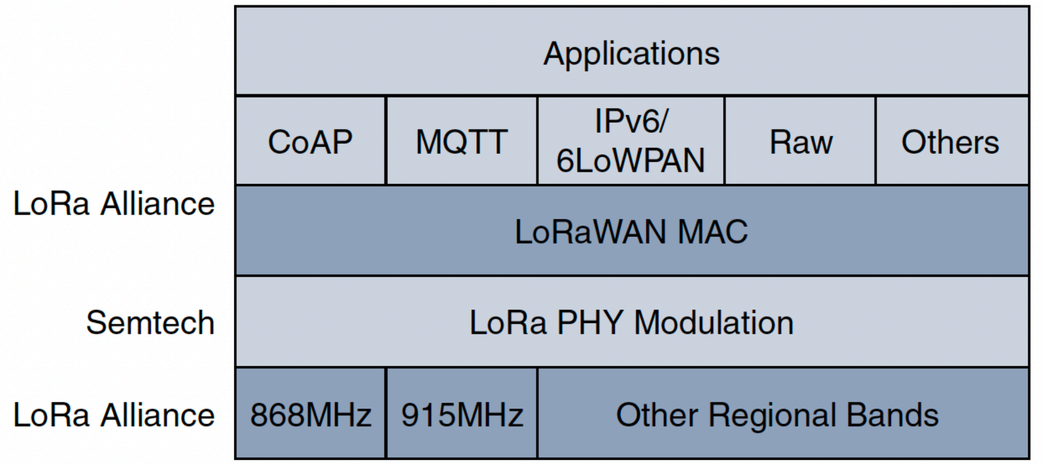
- In recent years, a new set of wireless technologies known as Low-Power Wide-Area (LPWA) has received a lot of attention from the industry.
- Particularly well adapted for long-range and battery-powered endpoints.
- **LoRaWAN** (Long-Range Wide-Area Network) is an **unlicensed band** LPWA technology.
  - NB-IoT (Narrow-Band IoT) and LTE are LPWA-based licensed band protocols using cellular networks.

LoRaWAN standardisation

- Initially, LoRa was a physical layer modulation developed by a French company named Cycleo.
  - Cycleo was acquired by Semtech.

LoRa Alliance®

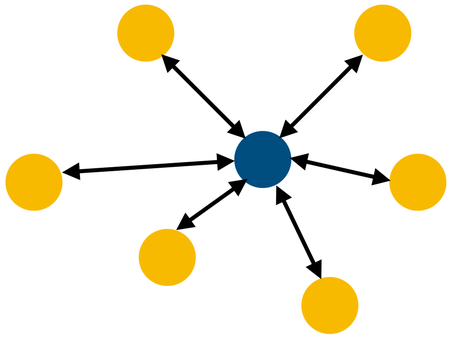
- Optimised for long-range, two-way communications and low power consumption, the technology evolved from Layer 1 to a broader scope through the creation of the **LoRa Alliance.**
- Semtech LoRa as a Layer 1 PHY modulation technology is available through multiple chipset vendors.
- “LoRaWAN” refers to the entire architecture and its specifications that describe end-to-end LoRaWAN communications and protocols



LoRaWAN layers

LoRa PHY (1)

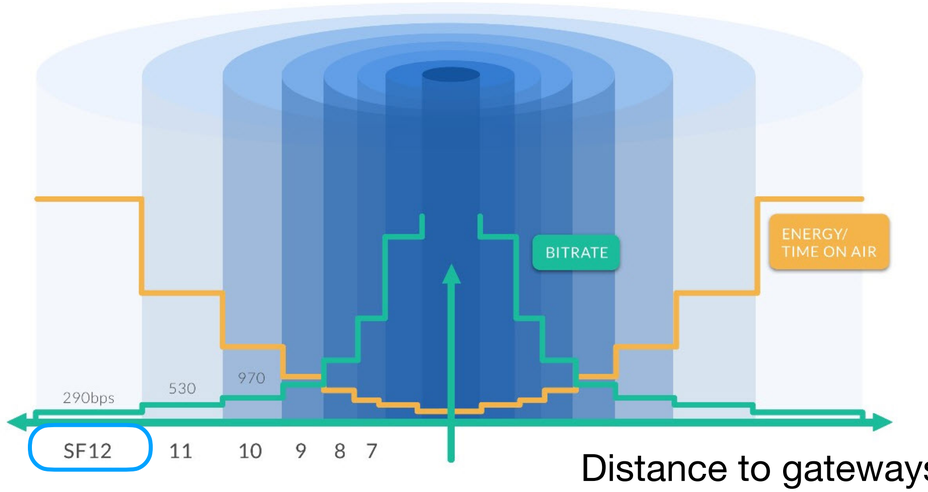
- LoRa PHY uses many unlicensed frequencies depending on geographical areas (Australia: 915–928 MHz, South Korea: 920–923 MHz, Japan: 920–928 MHz).
- A **LoRa gateway** is deployed as the center hub of a star network architecture.
  - It uses multiple transceivers and can demodulate multiple channels at once or even demodulate multiple signals on the same channel simultaneously.
  - It serves as a **bridge** relaying data between endpoints, which are a single-hop away from the gateway.



- Star of stars topology may be used (multiple LoRa gateways).

LoRa PHY (2)

- The data rate in LoRaWAN varies depending on the frequency bands and **adaptive data rate (ADR)**. The ADR is decided through the ADR algorithm, that manages the data rate and radio signal for each endpoint.
  - The ADR algorithm ensures that packets are delivered at the best data rate possible and that network performance is both optimal and scalable.
  - Endpoints close to the gateways with good signal values transmit with the highest data rate
    - shorter transmission time
    - lowest transmit power.
  - Endpoints at the edge of the link budget communicate at the lowest data rate and highest transmit power.

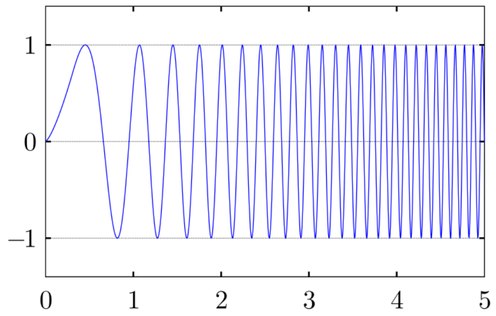


SF = “spreading factor” = **number of bits per symbol**

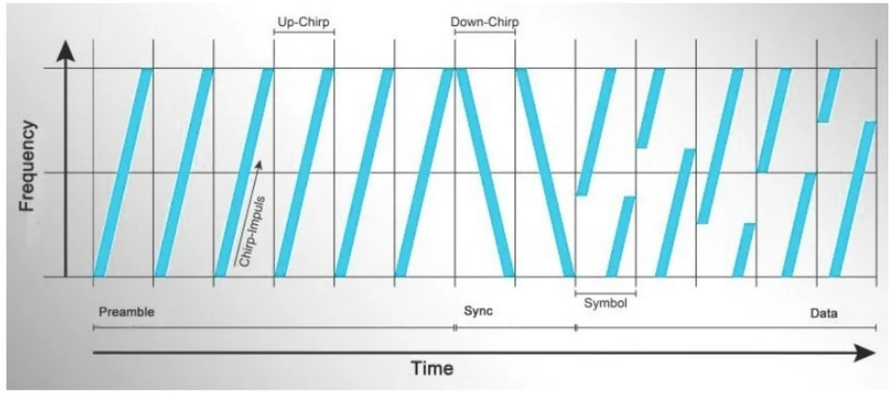
So the bit rate decreases with the number of bits per symbol!!

LoRa PHY - CSS (1)

- LoRa uses **Chirp Spread Spectrum (CSS)** as a modulation scheme.
- The signal is encoded using chirps — signals whose frequency increases (up-chirp) or decreases (down-chirp) linearly over time.
- Each chirp is **one symbol.**
- **We can encode data in chirps by changing the chirp's timing** (offset or delay of the chirp within a fixed time frame)**, phase or sweep direction.**
- It is a spread spectrum technique (the entire bandwidth is used for representing each symbol).

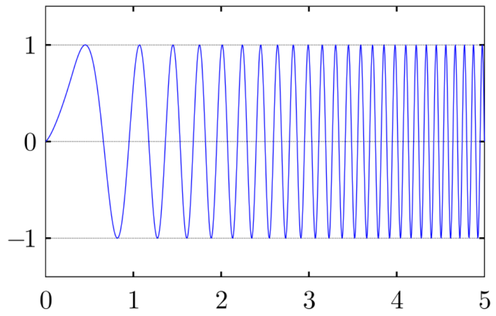


up-chirps

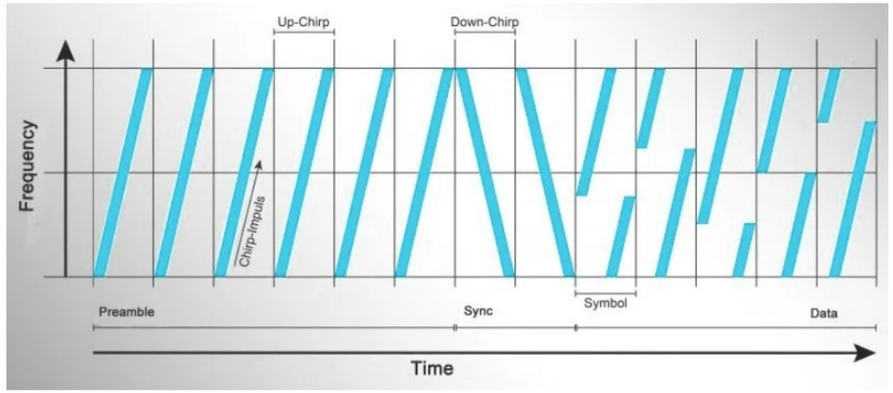


LoRa PHY - CSS (1)

- LoRa uses **Chirp Spread Spectrum (CSS)** as a modulation scheme.
- The signal is encoded using chirps — signals whose frequency increases (up-chirp) or decreases (down-chirp) linearly over time.
- Each chirp is **one symbol.**
- **We can encode data in chirps by changing the chirp's timing** (offset or delay of the chirp within a fixed time frame)**, phase or sweep direction.**
- It is a spread spectrum technique (the entire bandwidth is used for representing each symbol).



up-chirps



LoRa PHY - CSS (2)

- In LoRa, the spreading factor has 6 possible values: SF7, SF8,…, SF12.
- A SFn, means 2^n different symbols: higher SF (higher bits per symbol) -> more symbols.
- **But we have seen that higher SF means lower data rate! While modulation schemes with more bits per symbol allow more data rate (with powerful enough signals)!**
- In other modulation schemes that we have seen (ASK, PSK, FSK etc), the symbol duration (i.e., how long it takes to transmit a symbol) was the same for all symbols.
- In CSS it is not! Instead, the duration of chirp increases exponentially with SF!
  - To distinguish more symbols (higher SF), the chirp must sweep more finely across frequency to detect smaller differences in phases and frequencies.
    - That requires more time (the longer you observe a signal, the better you can resolve small frequency differences). In fact:

How long it takes to transmit a symbol

$$T_s = \frac{2^{SF}}{B}$$

How many symbols

Bandwidth

That's why higher SF means lower DR

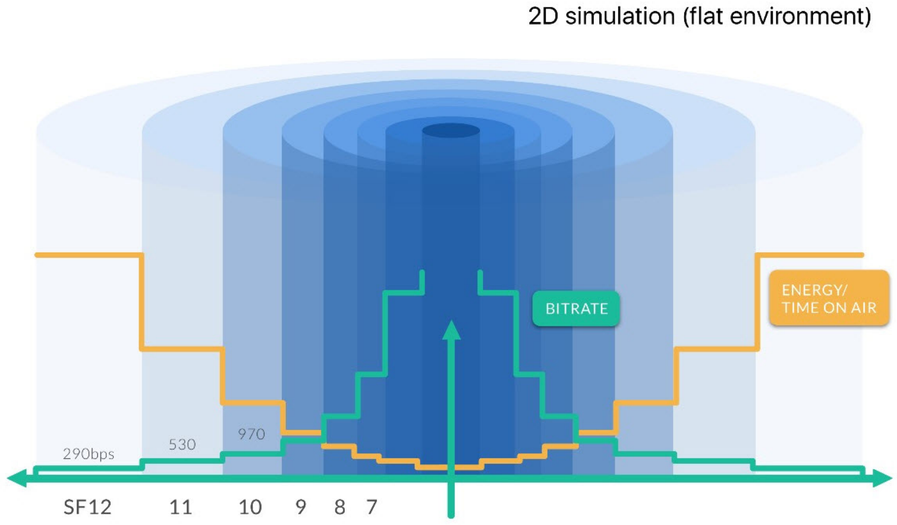
$$DR = \frac{SF}{T_s} = \frac{SF}{2^{SF}} \cdot B$$

T_s = symbol duration

DR = Data Rate

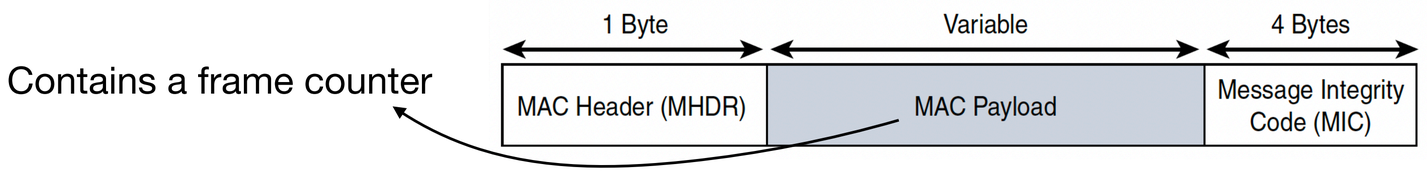
LoRa PHY (3)

- ADR adaptively arranges the spreading factors depending on the distance to the LoRa gateway.
- Devices with a low spreading factor achieve:
  - less distance in their communications
  - transmit at faster speeds.
- Devices with a high spreading factor achieve:
  - slower transmission rates
  - higher reliability at longer distances.
- Best practices:
  - use ADR for fixed endpoints
  - use fixed SF for mobile endpoints.



LoRaWAN MAC

- LoRaWAN messages have a PHY payload composed of a 1-byte MAC header, a variable-length MAC payload, and a 4 byte Message Integrity Code (MIC).
- The MAC payload size depends on the frequency band and the data rate.

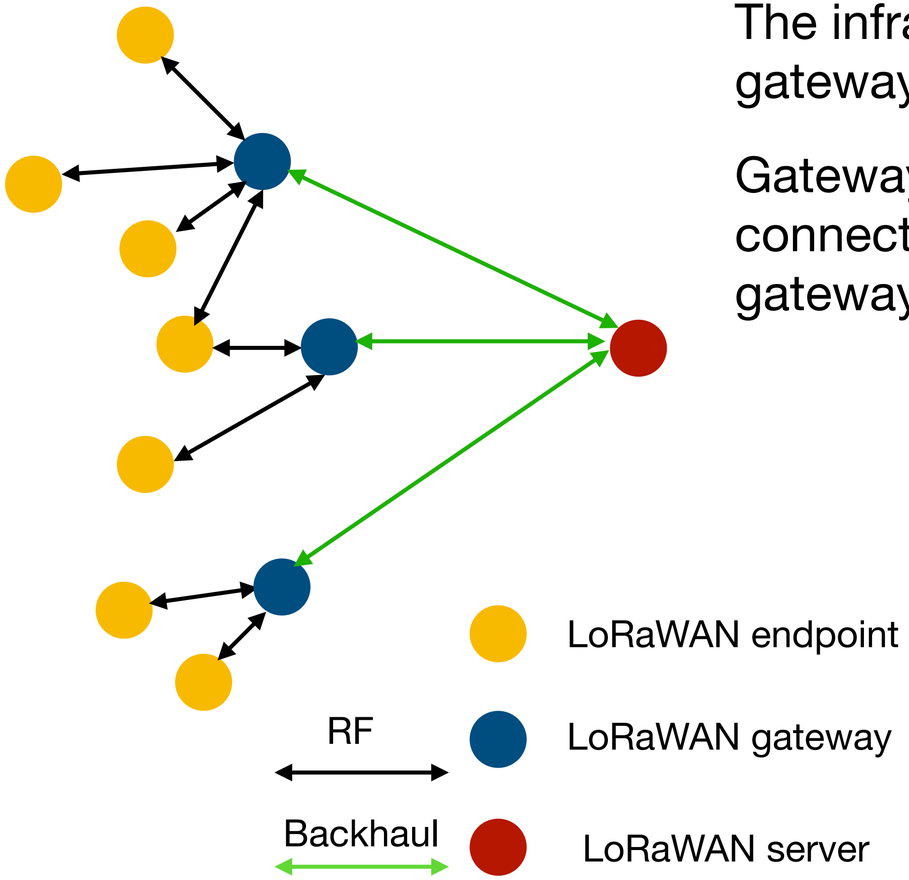


High-Level LoRaWAN MAC Frame Format

- LoRaWAN endpoints are uniquely addressable through a variety of methods, including:
  - An endpoint can have a global end device ID (DevEUI)
  - An endpoint can have a global application ID (AppEUI) that uniquely identifies the application provider, such as the owner of the end device
  - 32 bit device address, DevAddr, The 7 most significant bits are the network identifier (NwkID), which identifies the LoRaWAN network. The 25 least significant bits are used as the network address (NwkAddr) to identify the endpoint in the network.

LoRaWAN topology

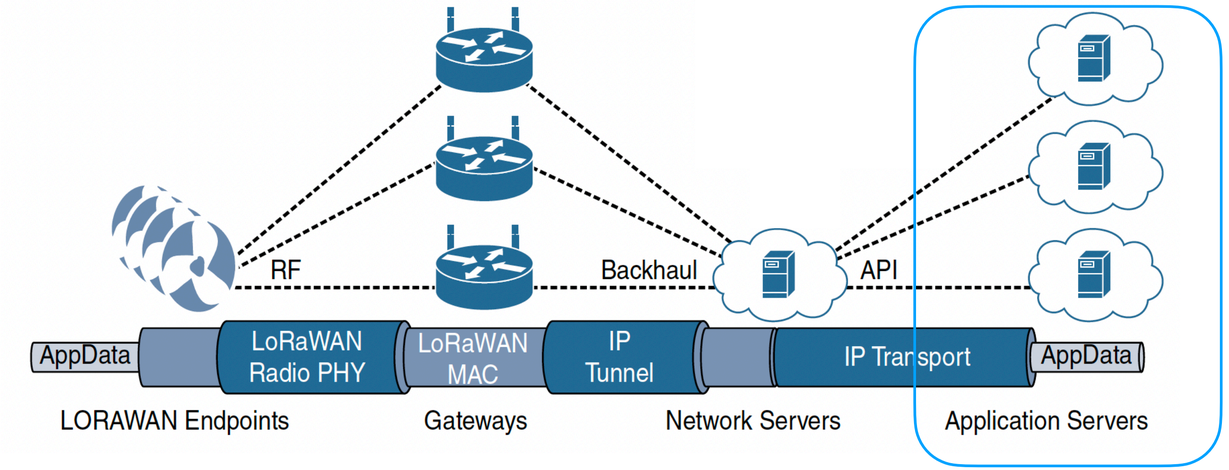
Star of Stars topology



The infrastructure consists of endpoints exchanging packets through gateways acting as bridges, with a central LoRaWAN network server.

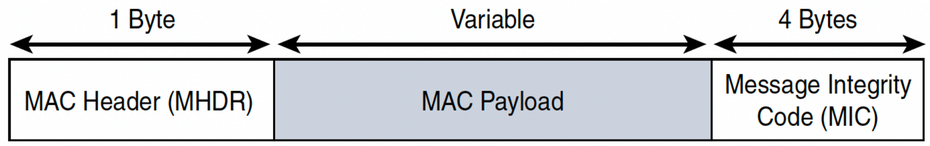
Gateways connect to the backend network using standard IP connections, and endpoints communicate directly with one or more gateways.

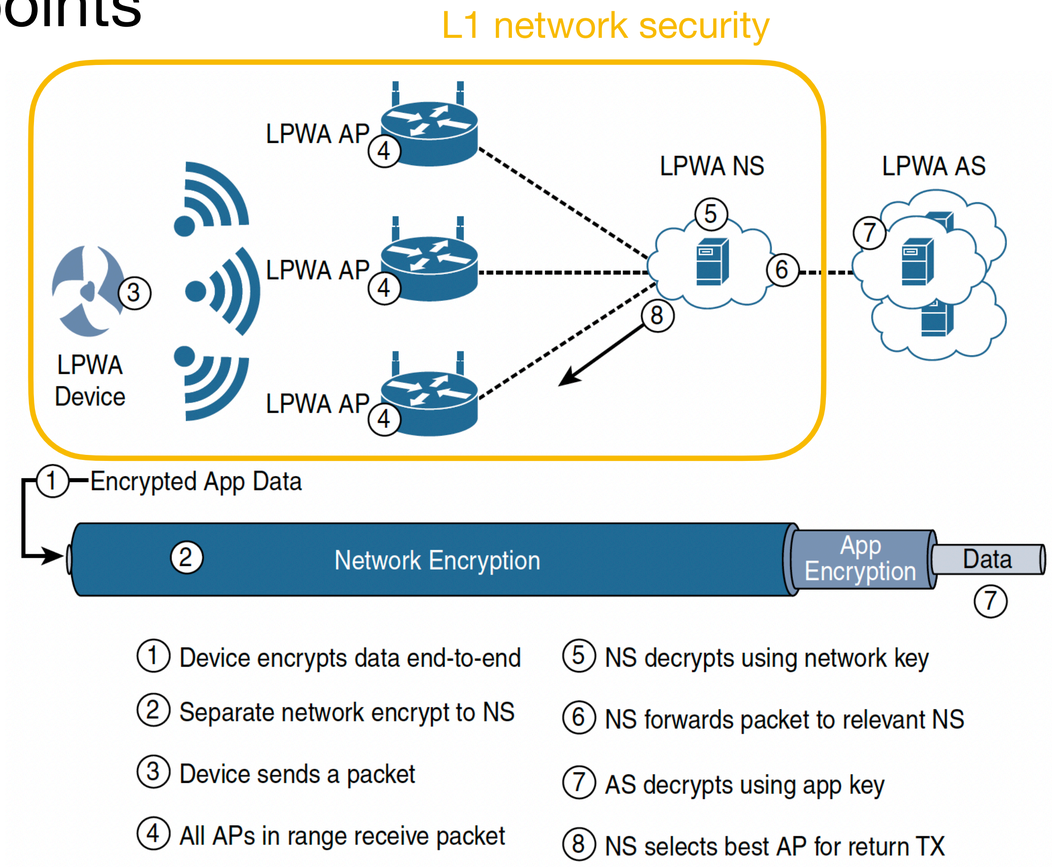
Not specified by LoRaWAN



LoRaWAN security (1)

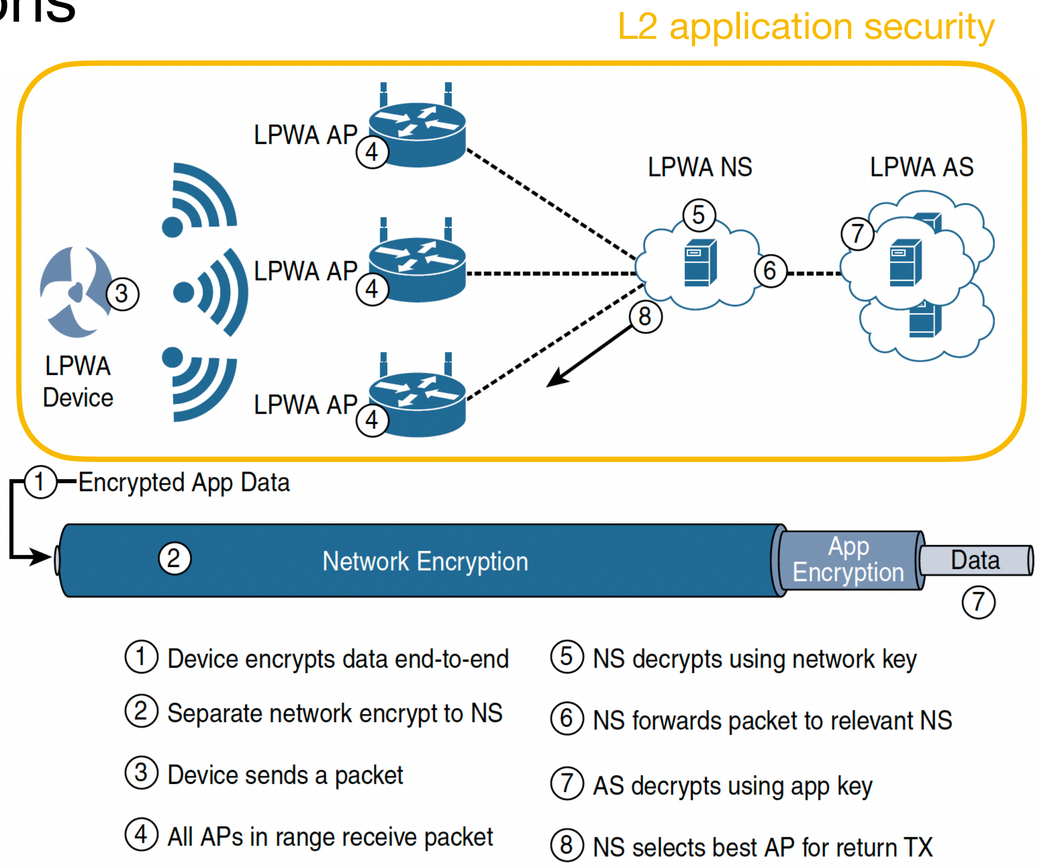
- LoRaWAN endpoints must implement **two layers of security**:
  - L1: “network security” (but applied at the MAC layer):
    - Guarantees the authentication of the endpoints by the **LoRaWAN network server**
    - Ensures message integrity by performing AES-CMAC (Cipher-based Message Authentication Code) using a network session key (**NwkSKey**) -used by the endpoint itself and the LoRaWAN network server. AES-CMAC generates the Message Integrity Code (MIC) that is appended to the MAC frame.





LoRaWAN security (2)

- LoRaWAN endpoints must implement two layers of security:
  - L2: application security.
    - performs encryption and decryption functions between the endpoint and the application server.
    - Uses AES-CTR with the application Session key (**AppSKey**).
    —> Allows only LoRaWAN service providers with correct AppSKey to have access to the application payload.
- Both **AppSKey** and **NwkSKey** are generated at each session from a unique key called **AppKey**

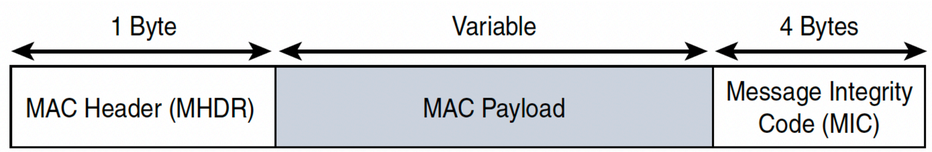


AES Counter mode (AES-CTR)

LoRa uses AES-CMAC (Cipher-based Message Authentication Code) to create a MIC and ensure data integrity and authenticity.

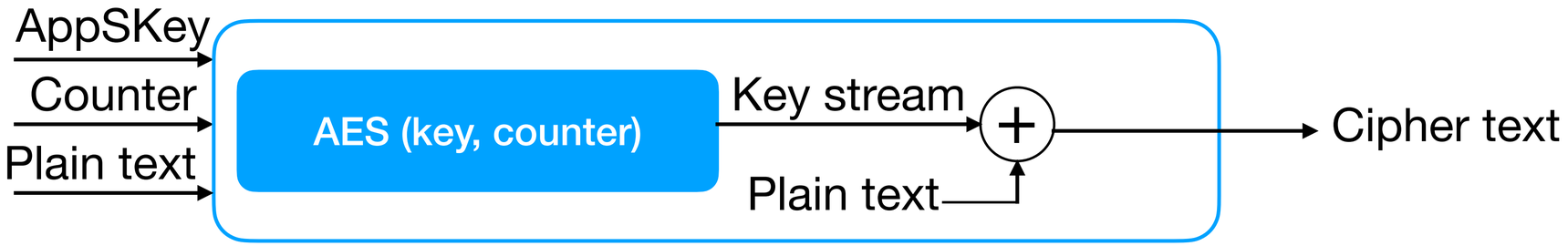
Procedure:

- Generate two keys, K1 and K2, from the NwkSKey K.
- Divide the message (MAC header + payload) into 128 bit long blocks M_i (possibly padding).
- Initialise a variable $X_i = 0$ (128 bit long).
  - For each block M_i, i>0, compute X_i=AES(K, X_{i-1} XOR M_i).
- Depending on whether padding was applied, XOR the last block either with K1 or K2.
- The output is the output is the **CMAC tag**, that is 128 bit long. The MIC is obtained by using its first 4 Bytes.



AES Counter mode (AES-CTR)

- LoRa uses AES in counter mode for encrypting data with the application server.
- Instead of applying AES on the plaintext, it applies it to a 128 bit long counter, called nounce. The result is a 128 bit keystream.
- The resulting key stream is XORed with the plain text.

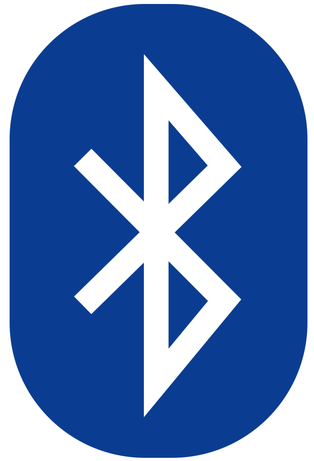


- If the plain text is longer than 128 bits, AES is applied multiple times on (key, counter+1), (key, counter+2), etc.
- The frame counter (entry available in the MAC payload) is used as the counter.

6.1 Layer 1 and 2 Protocols
6.1.3 Bluetooth Low Energy

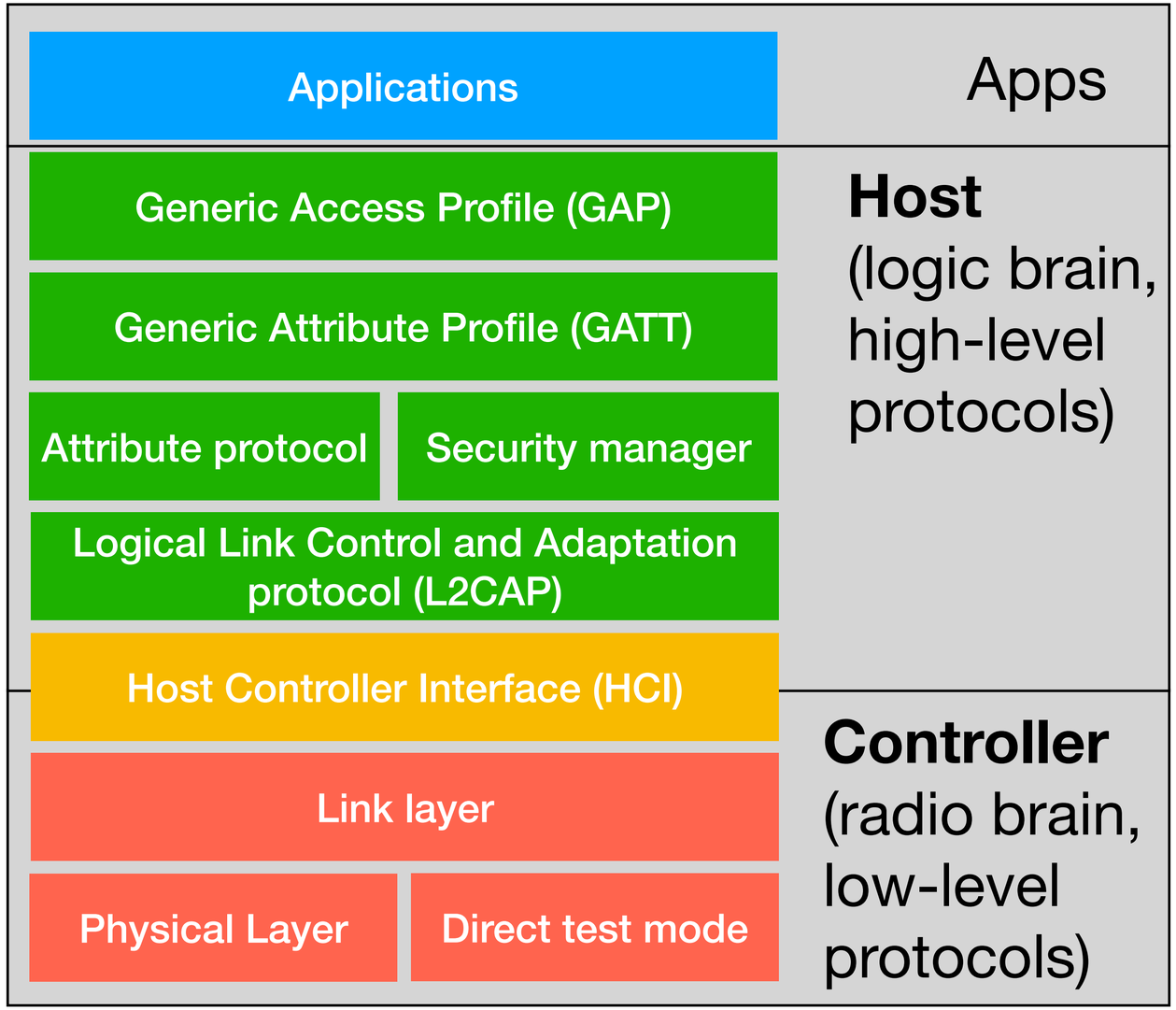
Bluetooth - history

- First version of Bluetooth was released in the late ‘90s to allow short range wireless communication and replace wires.
- Named after the nickname of Harald Blåtand, king od Denmark of the 10th century that unified Scandinavian Countries.
- The logo is the union of the two germanic letters ᚼ (Hagall) H, and ᛒ(Berkanan), B.



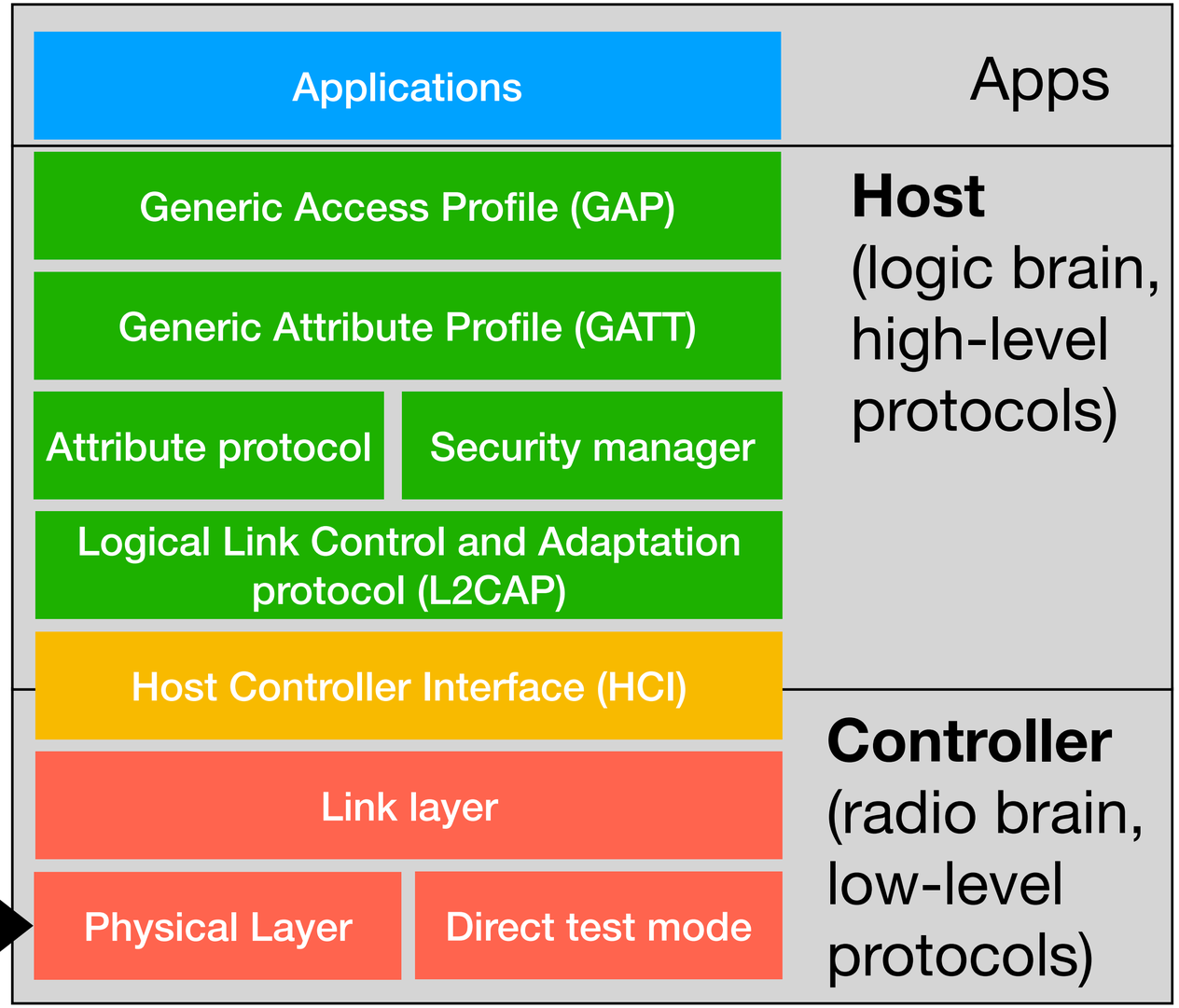
- The protocol really emerged as a turning point technology after its version 4 - Bluetooth Low Energy (BLE) or Bluetooth smart

BLE architecture and stack

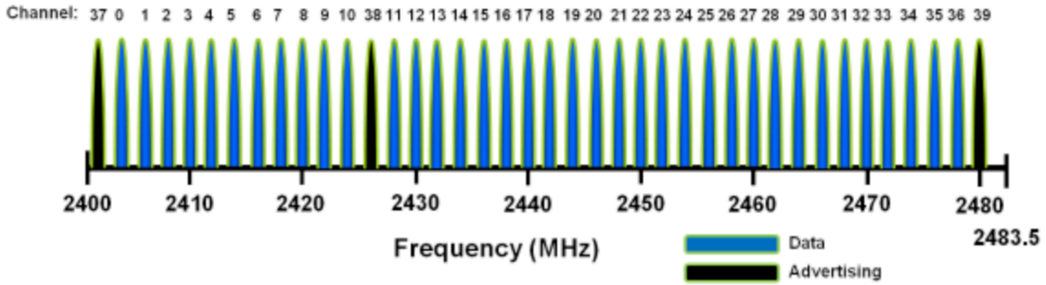


The functionality of the Bluetooth LE protocol stack is divided between three main layers:
- Controller
- Host
- Application

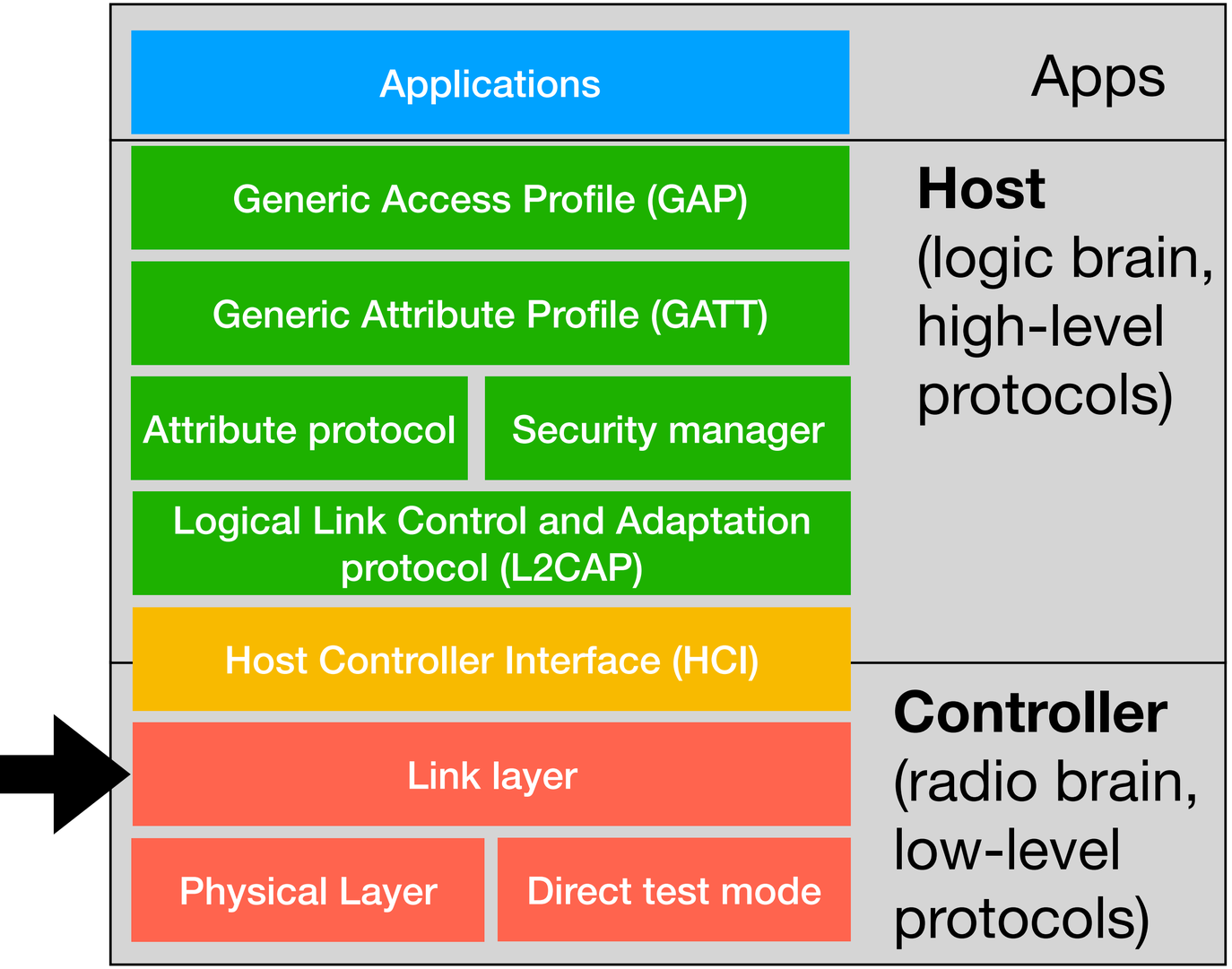
BLE architecture and stack



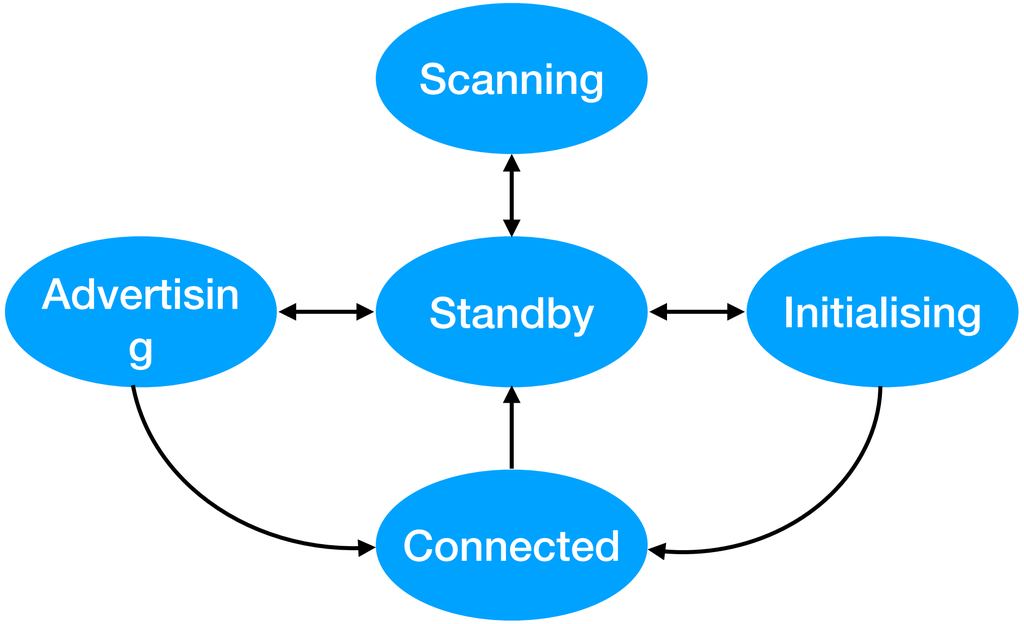
BLE transmits in the 2.4 GHz radio spectrum.
The frequency band is divided into 40 channels, three of which are used for advertising, while the others are for data transmission.



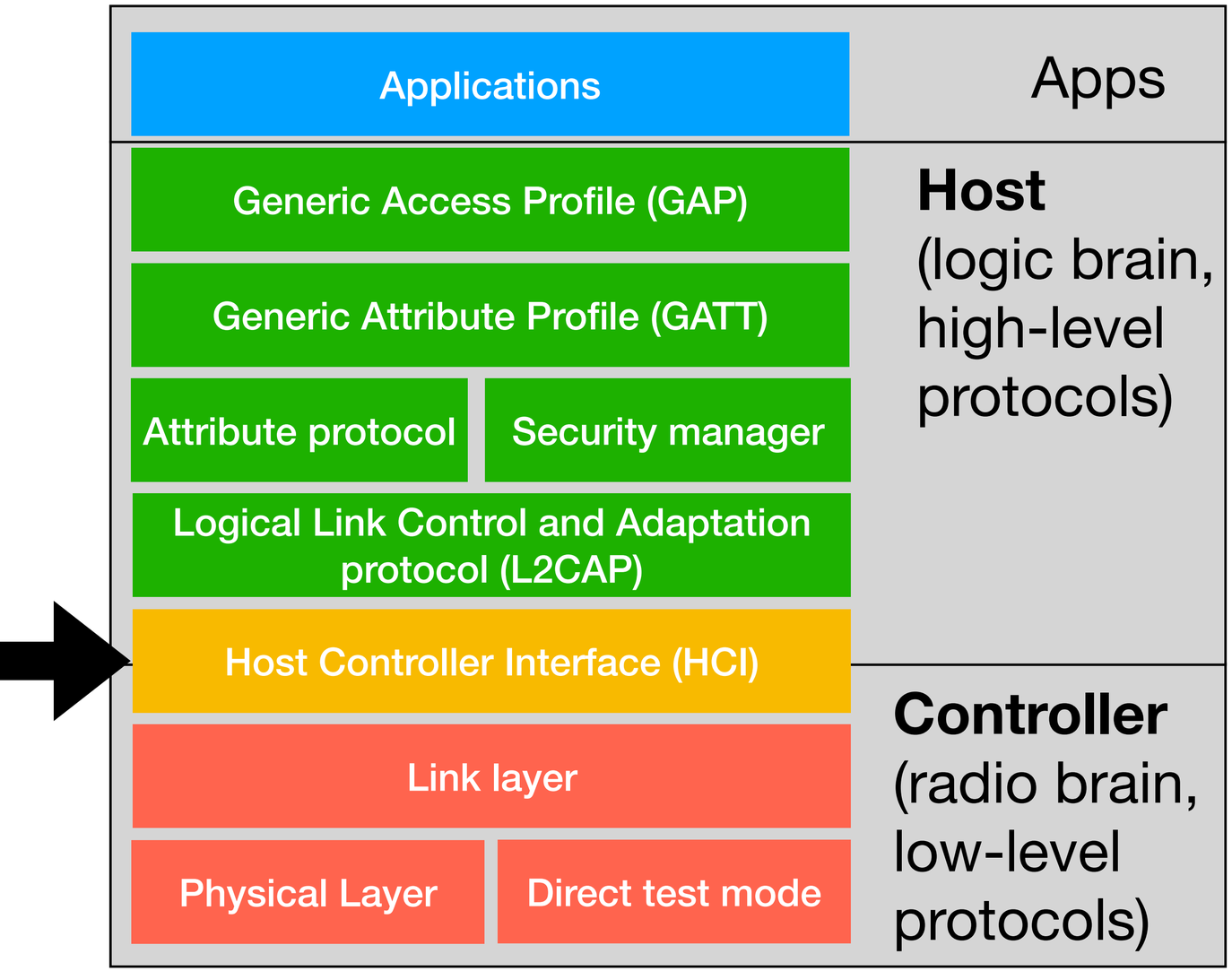
BLE architecture and stack



The link layer describes how different devices share the channel to communicate. Its operation can be described as a state machine with 5 possible states.

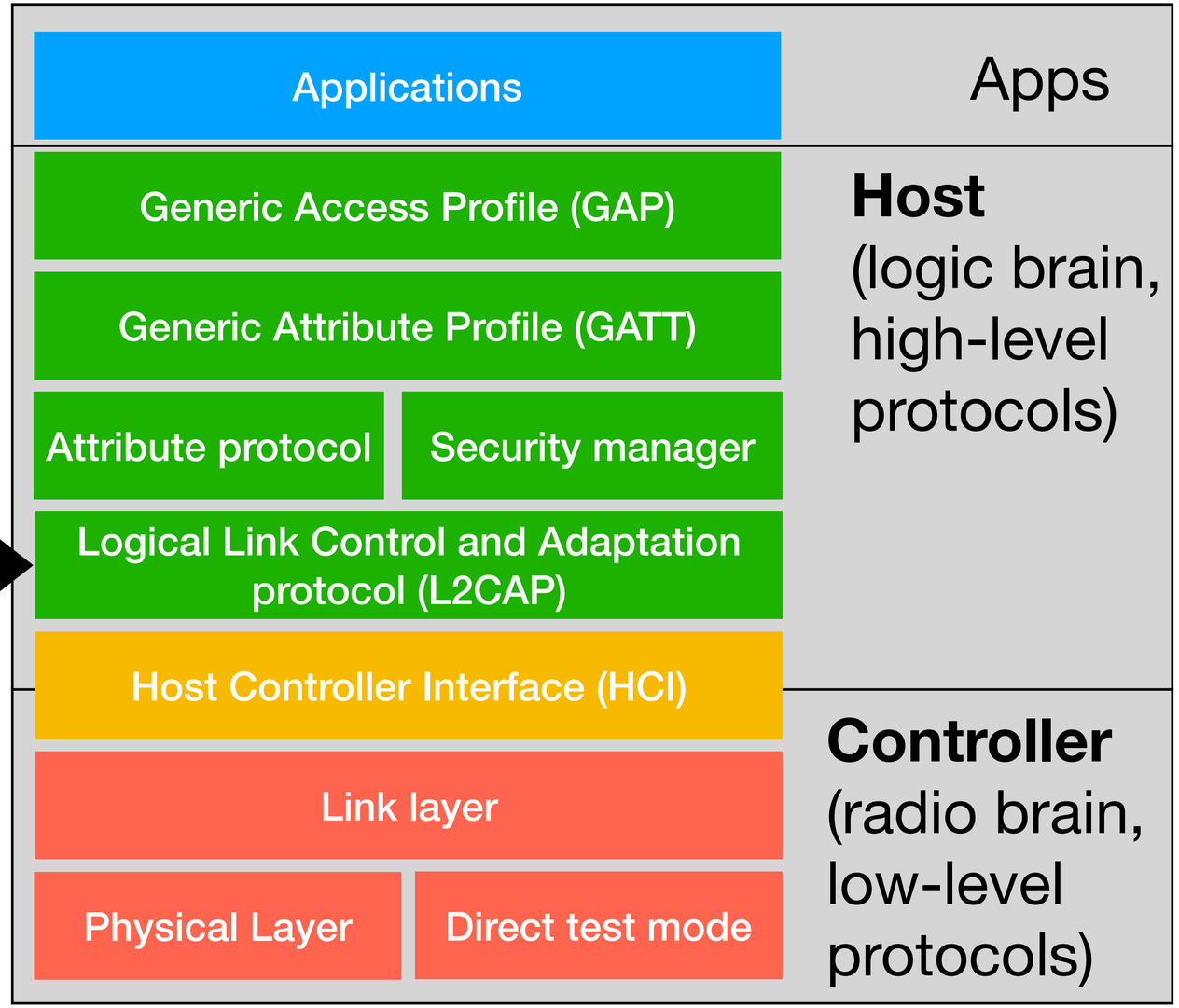


BLE architecture and stack



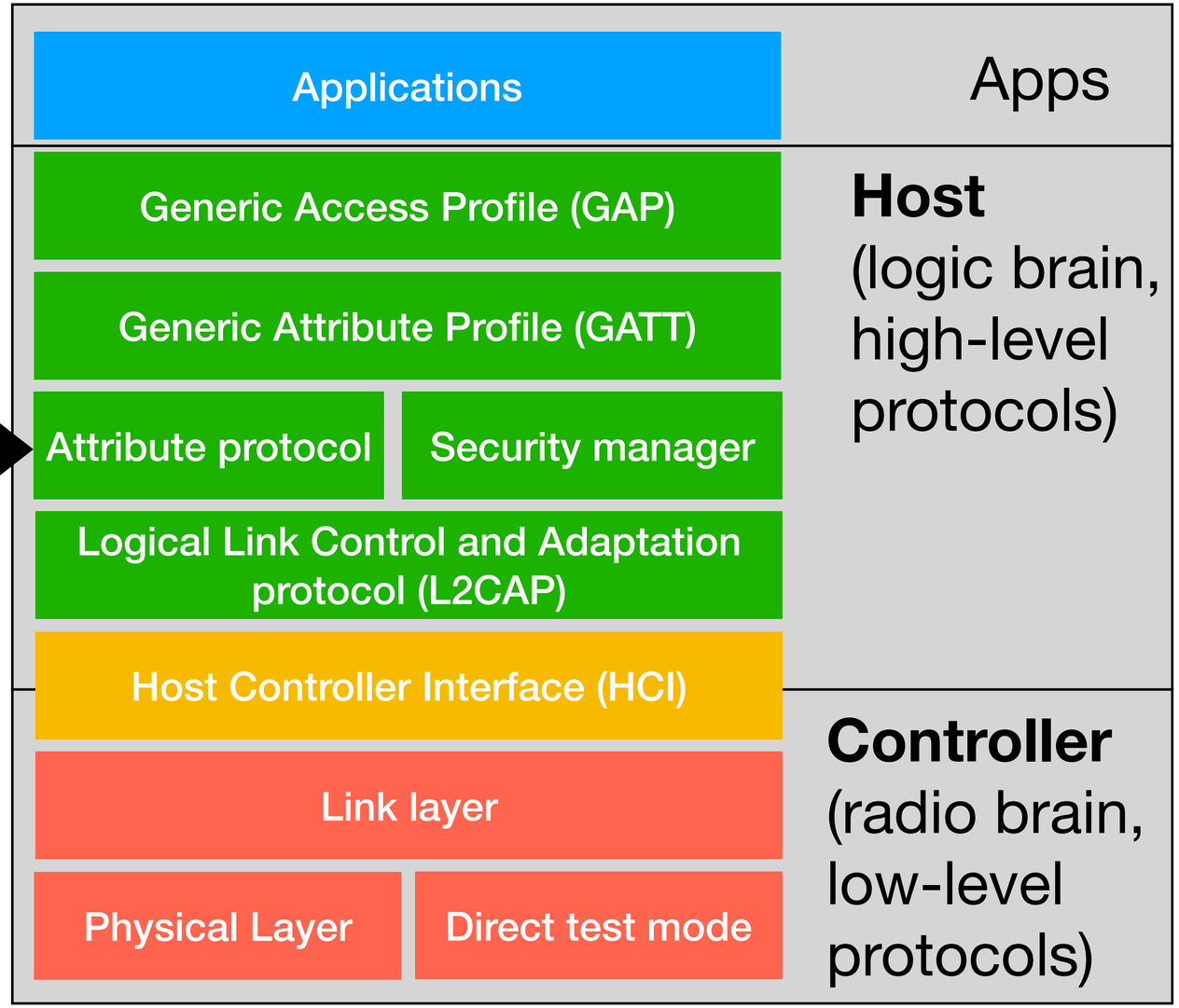
The host controller interface (HCI) layer is is a standard protocol that transports commands and events between the host and controller elements

BLE architecture and stack



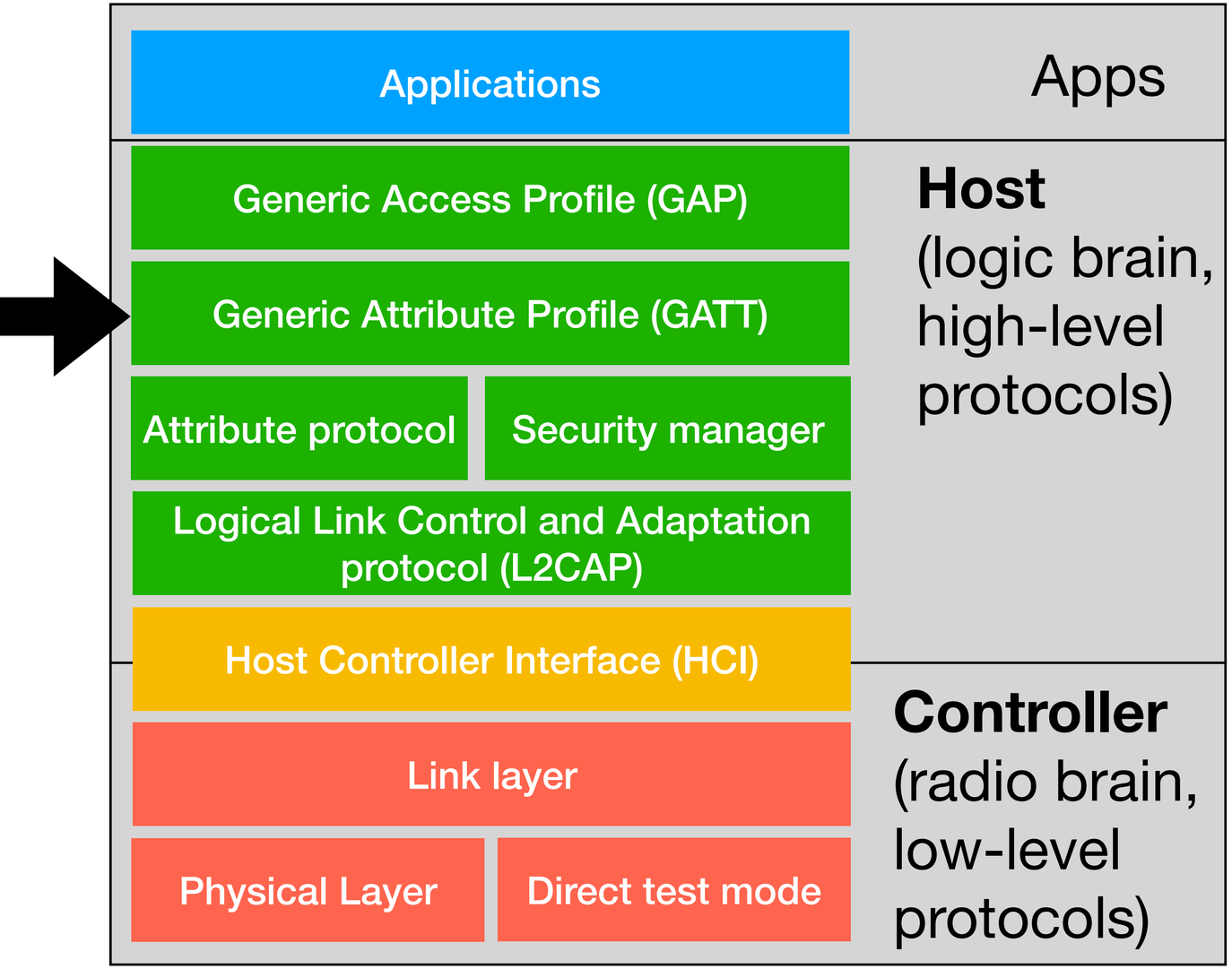
L2CAP offers segmentation and reassembly services for large packets.

BLE architecture and stack



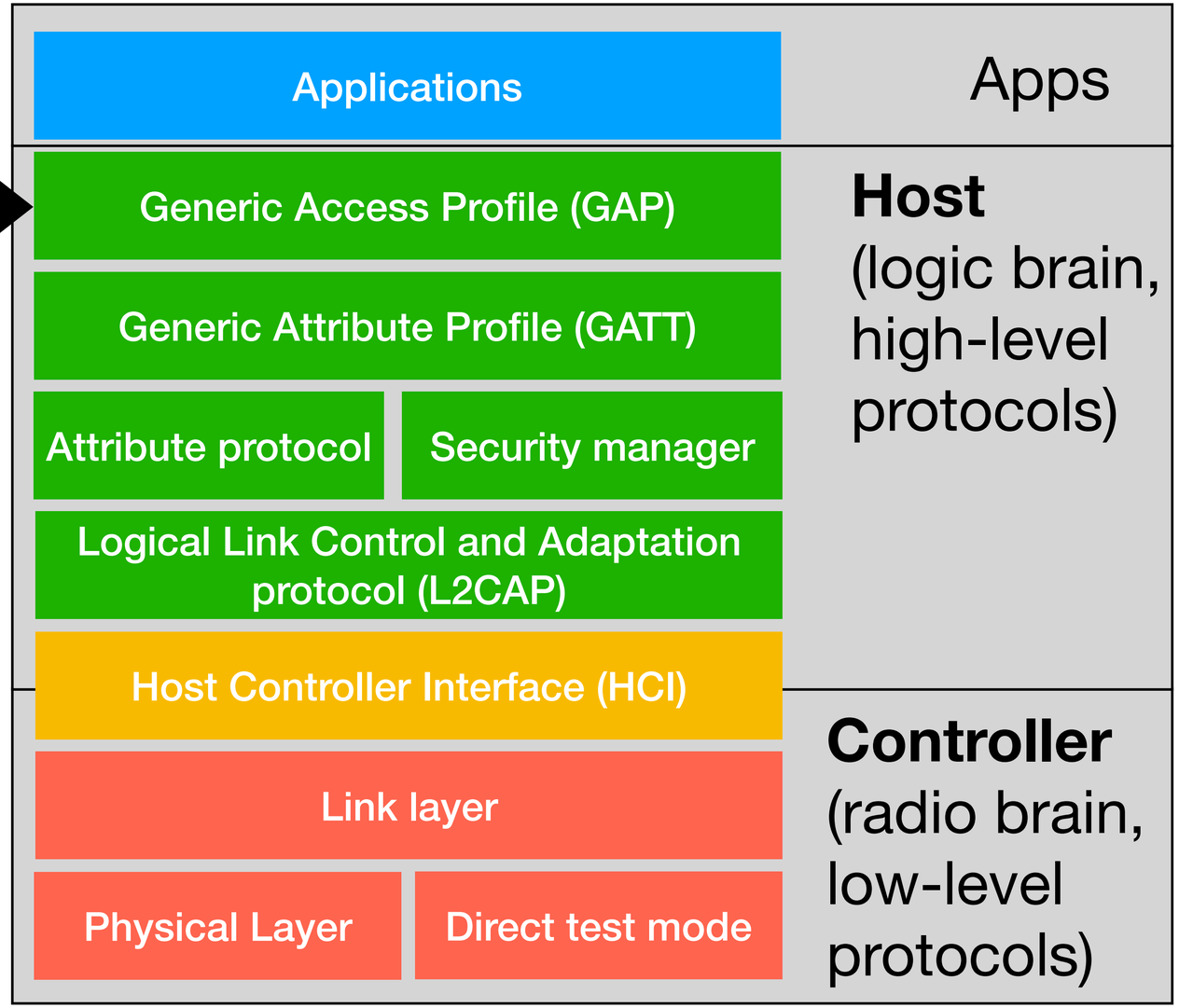
The attribute protocol defines how data is represented in a BLE server database and the methods by which that data can be read or written.

BLE architecture and stack



The GATT layer is used by the application for data communication between two connected devices

BLE architecture and stack



The GAP determines how two Bluetooth units discover and establish a connection with each other.

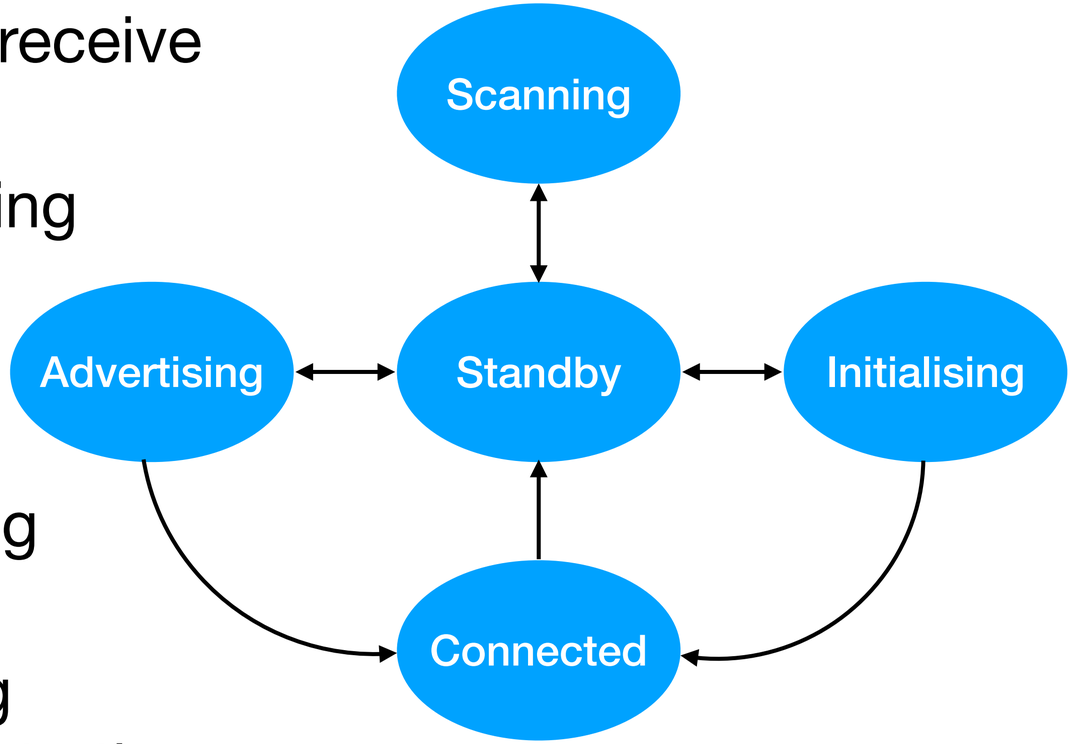
Roles in BLE

- There are many different roles that BLE devices can have, depending on how they interact during communication.

- Different types of roles exist at different layers (can be a little confusing).

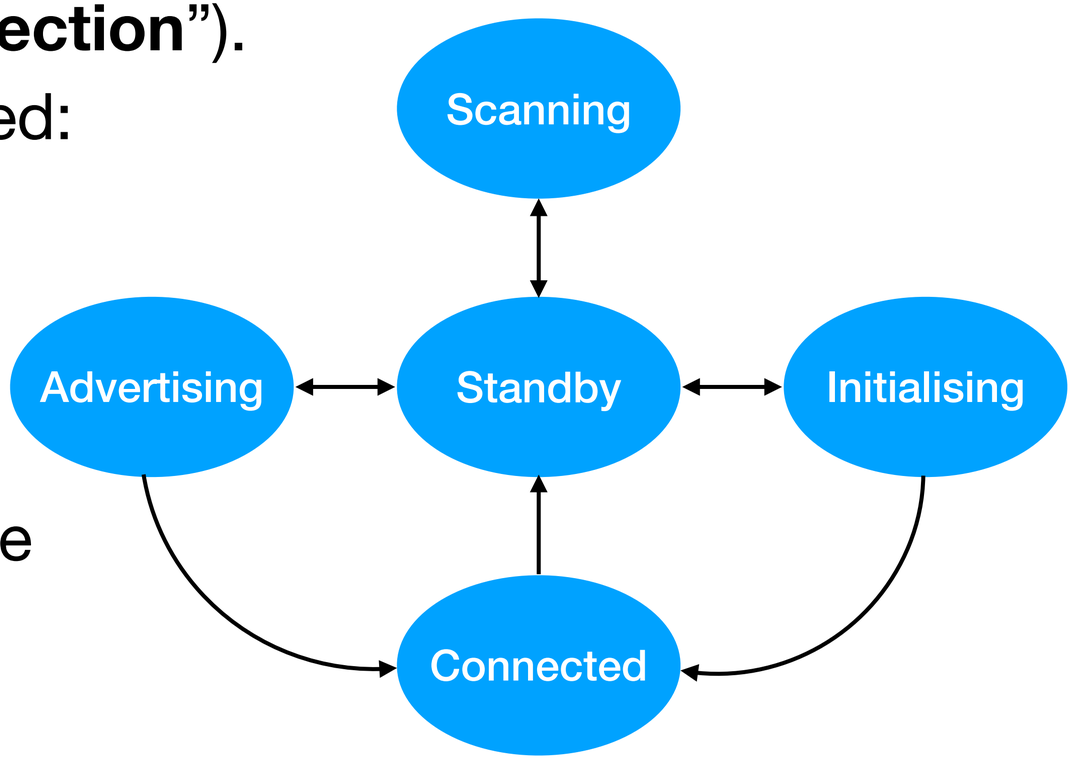
BLE Link Layer

- Link Layer state machine defines different states BLE nodes can be in.
- A device in Standby state does not transmit or receive any packets.
- A device in Advertising state transmits advertising packets (on channels 37,38,39) and listens to and responds to responses triggered by its advertising packets (“**advertiser**”).
- A device in Scanning state listens for advertising packets (“**scanner**”).
- A device in Initiating state listens for advertising packets from a specific device(s) and responds to these packets to initiate a connection with another device (“**initiator**”).

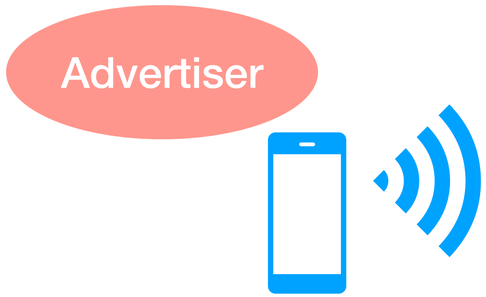


BLE Link Layer

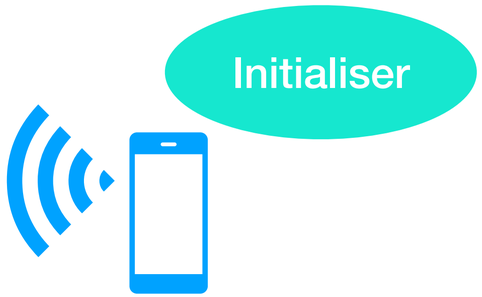
- When connection between devices is established, they enter the Connected state (they “**are in a connection**”).
- Within the connected state, two roles are defined:
  - **Central Role** - if the device enters the connected state from the initalizing state.
  - **Peripheral Role** - is the device enters the connected state from the advertising state.
- A device holding a central role will communicate with a device in peripheral role, defining the timings of transmission, based on TDMA.



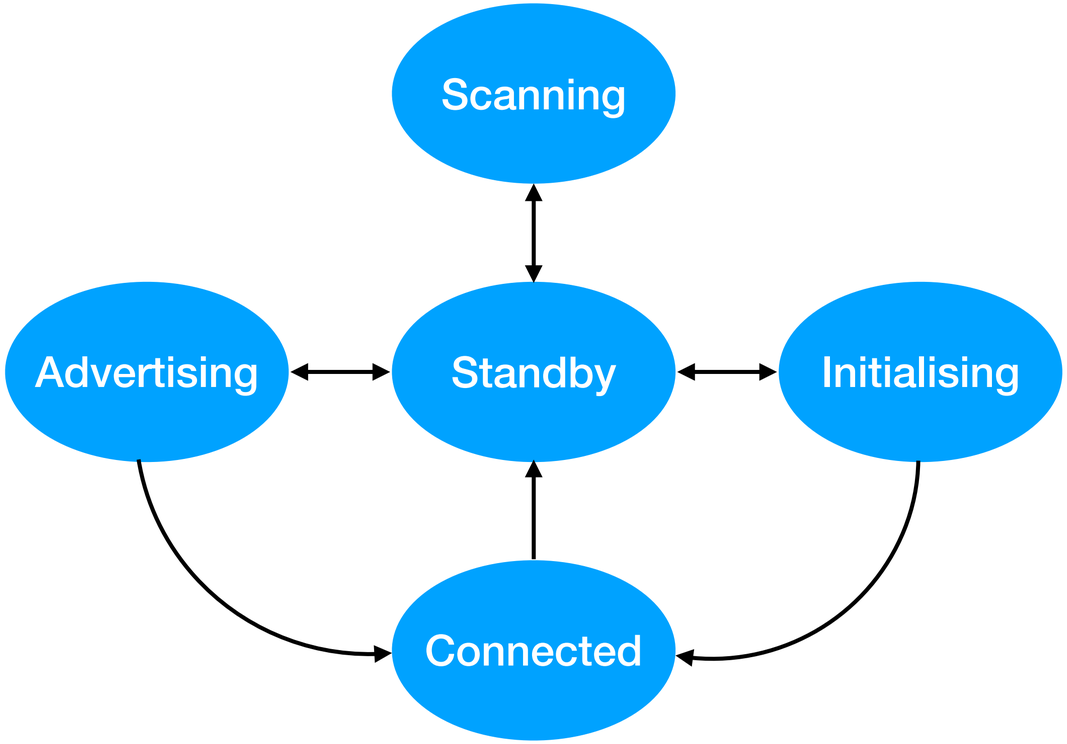
BLE Link Layer



Device 1 advertise its presence and willingness to connect.



Device 2 listens for advertising packets from Device 1 and responds to them.



The two devices connect, Device 1 is the **peripheral**, while Device 2 is the **central.**

- The applications running on top of the BLE device are responsible for deciding its role, based on their functional needs, power constraints, or communication intent.
- The protocol responsible for defining and controlling these roles is

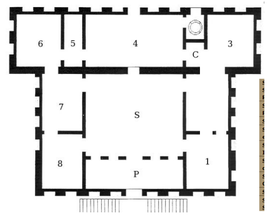
GAP

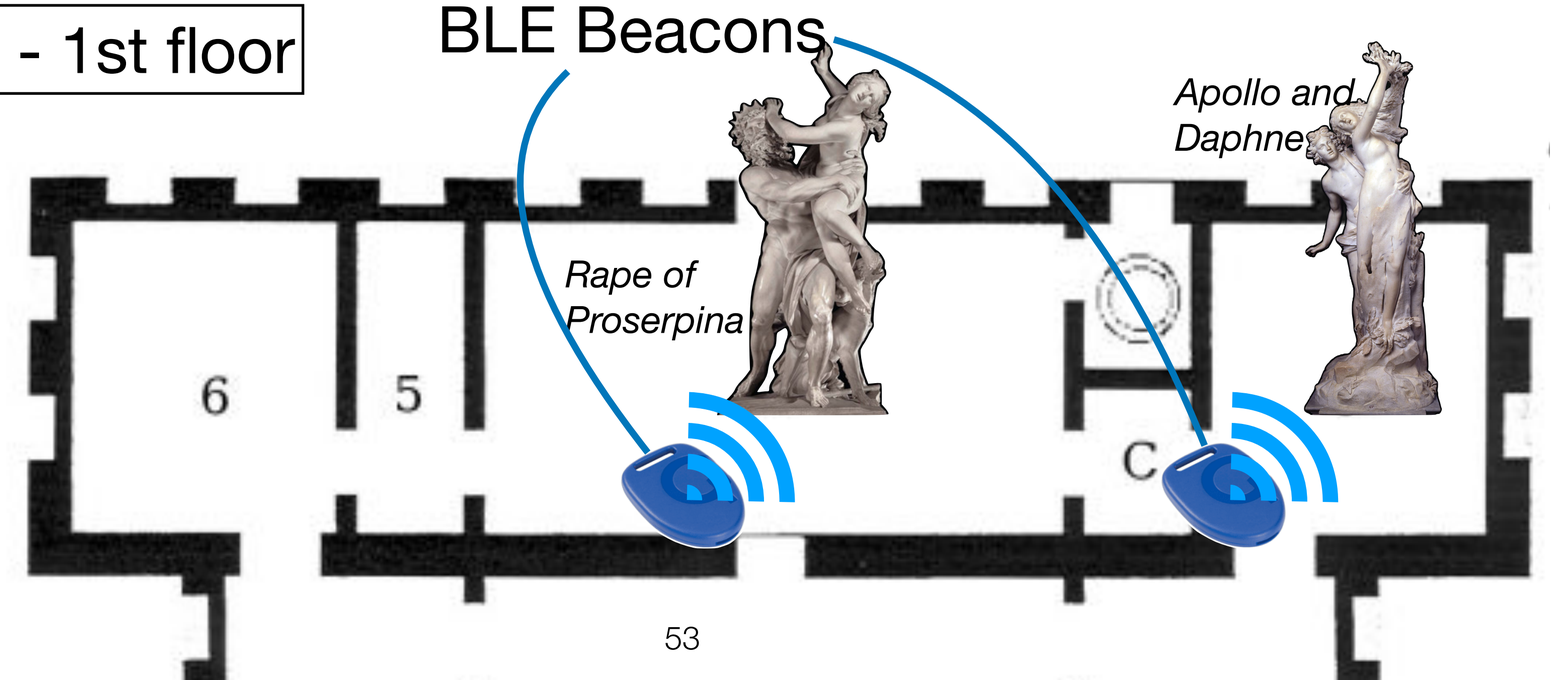
- Generic Access Profile, controls connections and advertising in BLE. Defines **communication modes** and **roles**.
- BLE supports two different communication modes:
  - **Connection-oriented communication**
  - **Broadcast communication**

GAP - communication modes

- **Connection oriented communication**: when there is a dedicated connection (link) between devices, forming a **bi-directional** communication (central and peripheral roles).
- **Broadcast communication**: when devices communicate **without establishing a connection** and by **broadcasting** data packets to all devices within its range. **Unidirectional** communication. Example:

Galleria borghese - 1st floor

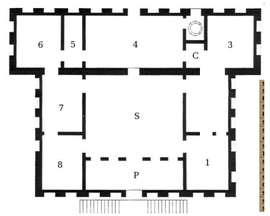


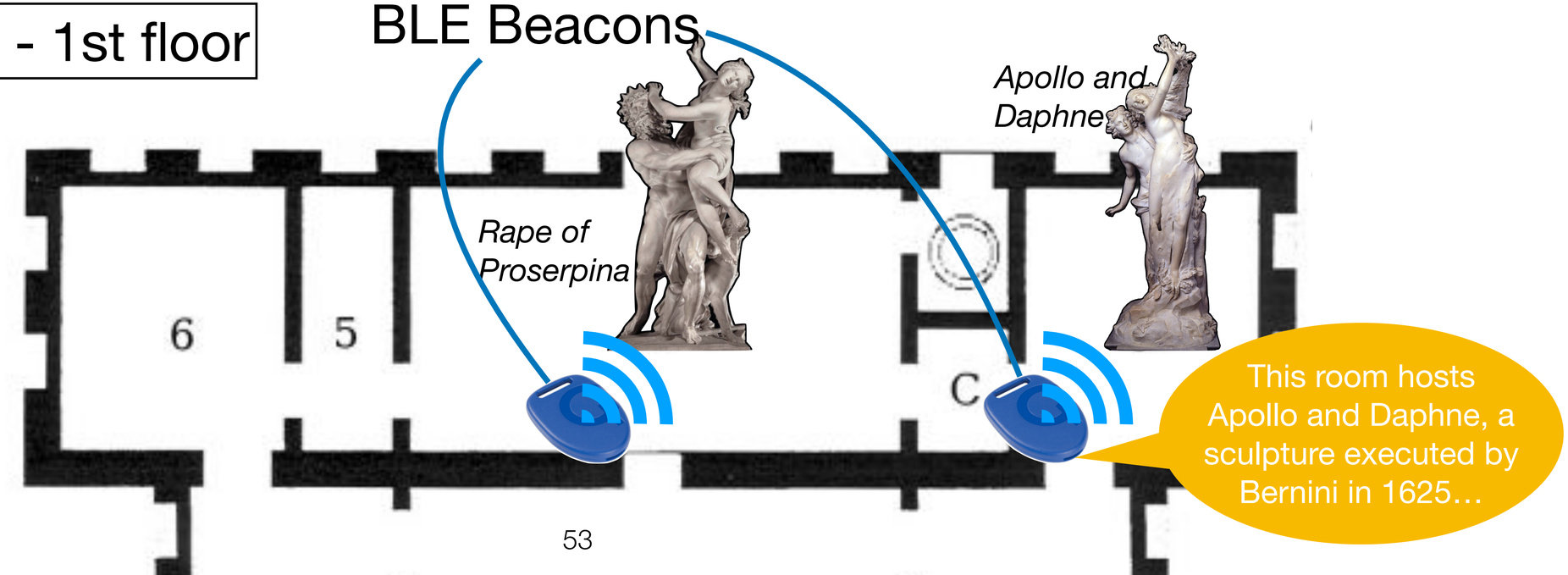


GAP - communication modes

- **Connection oriented communication**: when there is a dedicated connection (link) between devices, forming a **bi-directional** communication (central and peripheral roles).
- **Broadcast communication**: when devices communicate **without establishing a connection** and by **broadcasting** data packets to all devices within its range. **Unidirectional** communication. Example:

Galleria borghese - 1st floor

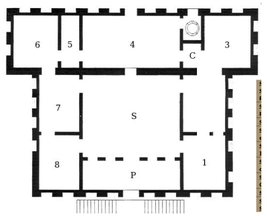


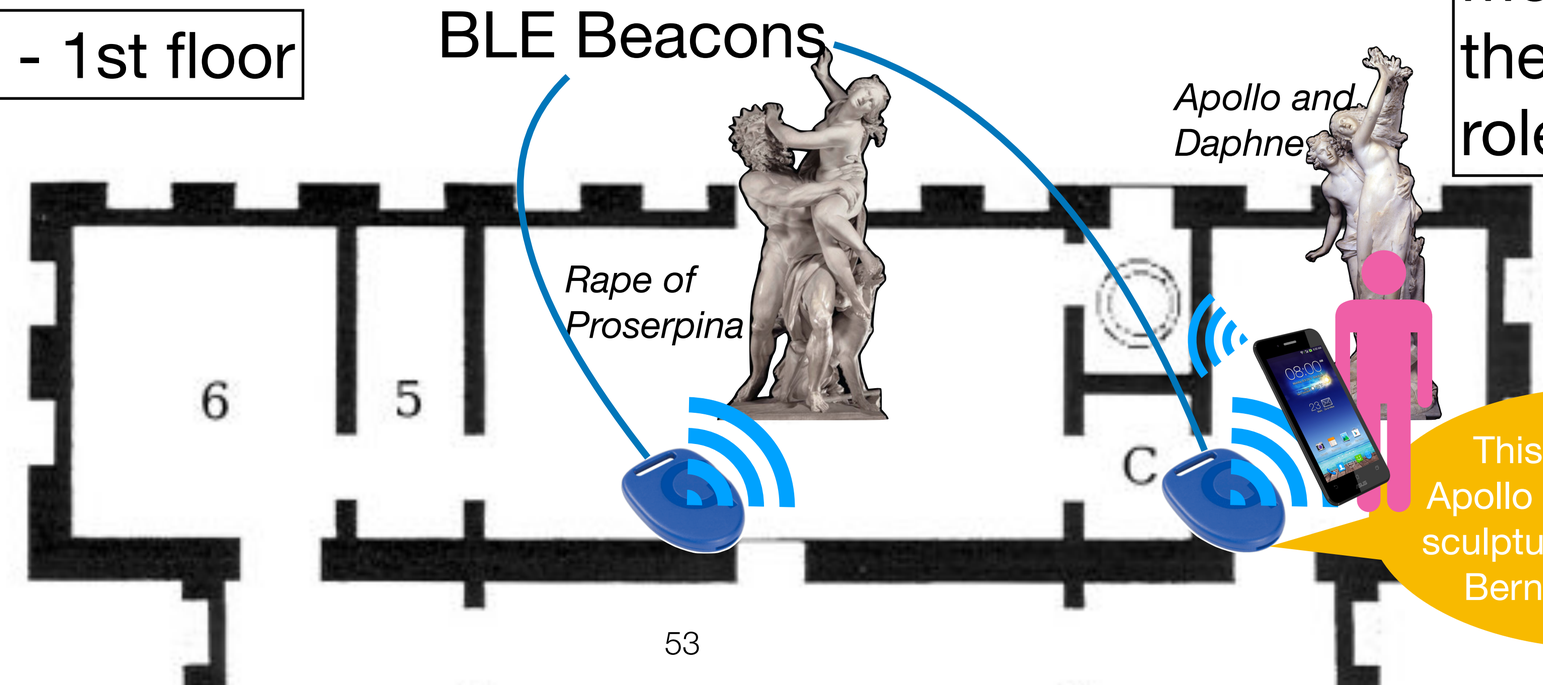


GAP - communication modes

- **Connection oriented communication**: when there is a dedicated connection (link) between devices, forming a **bi-directional** communication (central and peripheral roles).
- **Broadcast communication**: when devices communicate **without establishing a connection** and by **broadcasting** data packets to all devices within its range. **Unidirectional** communication. Example:

Galleria borghese - 1st floor

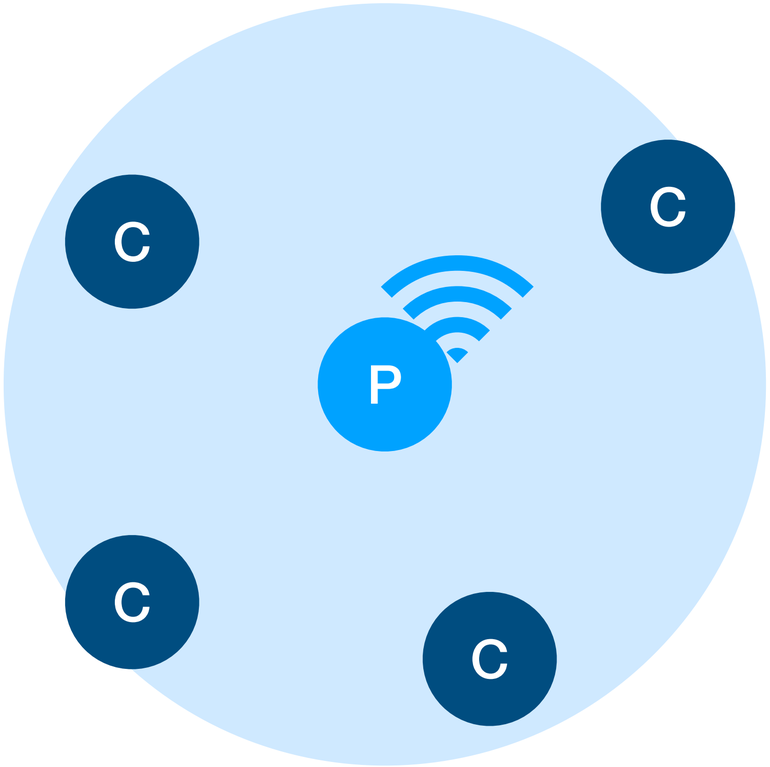




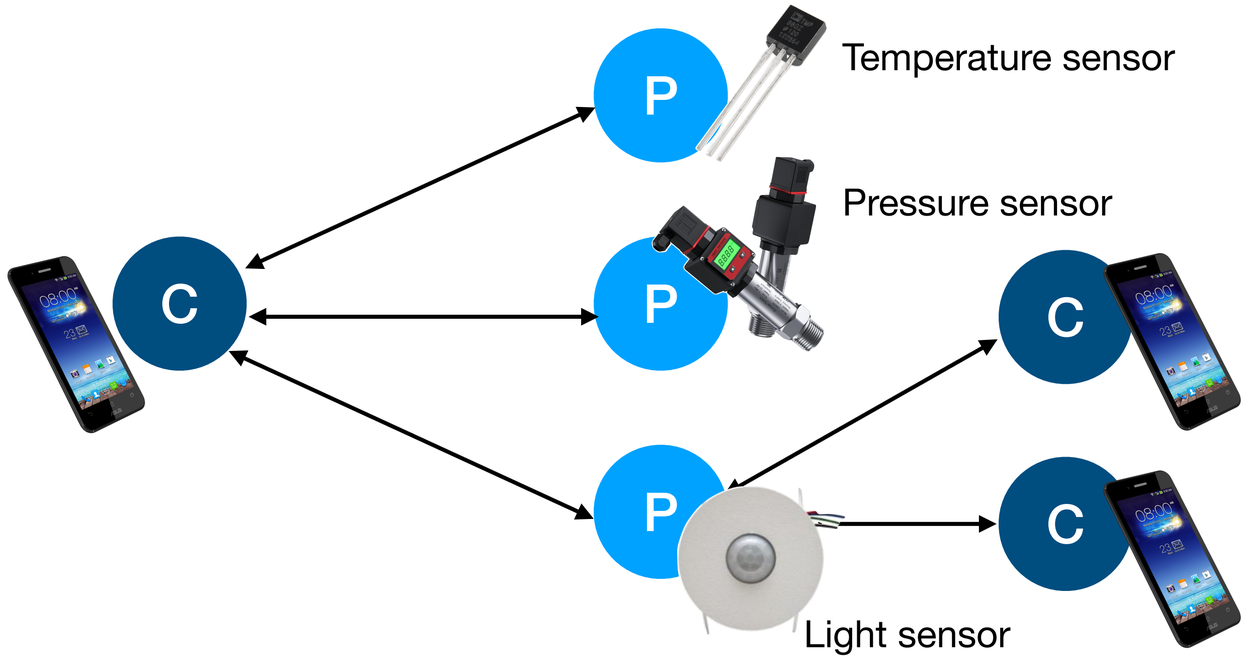
Mobile has the "**observer**" role

Broadcast topology

- A broadcaster that advertises data. Observers scan and read data from the advertisement packets sent by the broadcaster.
- No limit in how many devices one can broadcast to (anyone in the range).
- **More power efficient** than communication oriented communication.
- **Less throughput**, because of limited data available in the advertisement packets.
- No ACKS.



Connection-oriented topology

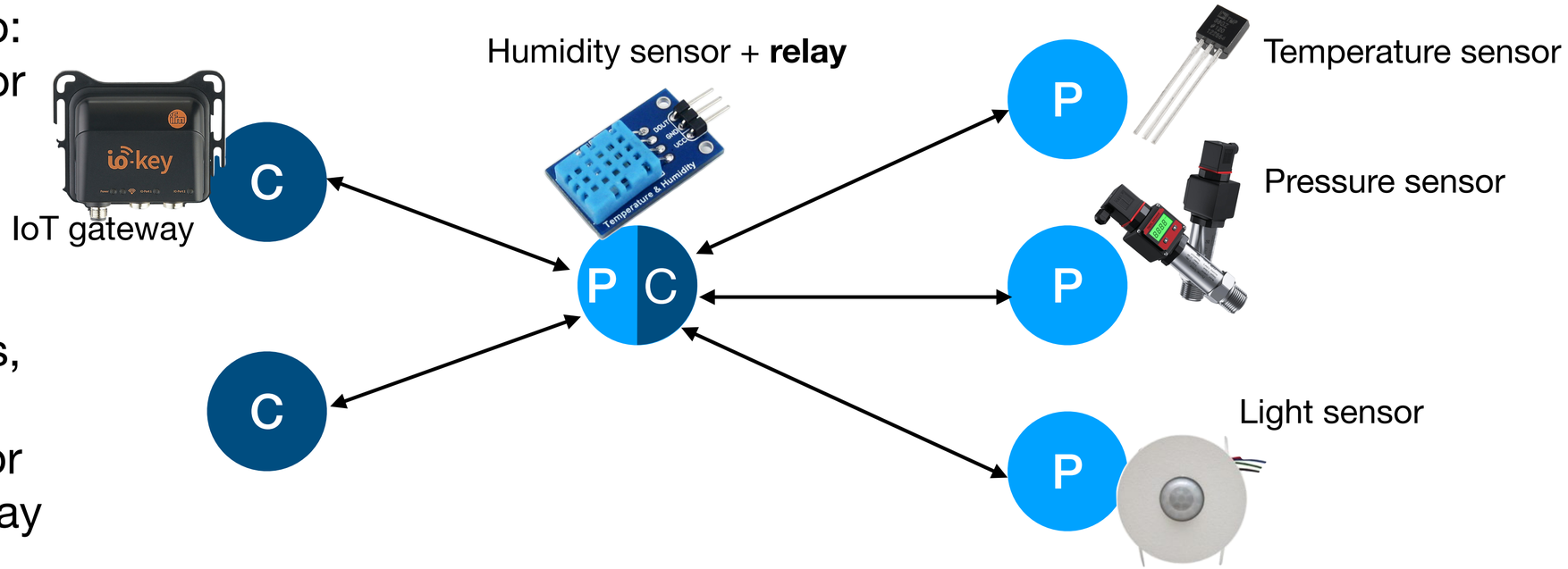


IoT example scenario: peripherals are sensor nodes, advertising their measurements. Centrals are mobile phones reading that information.

- Establishes a bidirectional connection before data transfer occurs.
- Increased throughput by establishing a direct link before communication.

Mesh (multi-role) Topology

IoT example scenario: peripherals are sensor nodes, advertising their measurements. A node acts as a central by collecting data from peripherals, and as a peripheral (may have a sensor or not) for an IoT gateway



- A device can operate in multiple different roles simultaneously, i.e., it can act as a peripheral in one setting and a central in another.

- Often used in systems where a device acts as a hub and receives sensor data from multiple sensors and at the same time wants to forward this data to other devices.

ATT & GATT: Data representation and exchange

- The just seen GAP layer defines communication modes (connection-oriented/broadcast oriented) and roles (peripheral and central/broadcaster and observer) and is responsible for the advertising phase.

- In **connection-oriented communication** mode, after the bi-directional communication is established, the Attribute protocol (ATT) and the Generic Attribute Profile (GATT) layers define how data is r**epresented and exchanged between BLE devices**.

  - The ATT and GATT layers are concerned with the phase **after** a connection has been established, as opposed to the GAP layer which takes care of the advertisement process which occurs **before** a connection is established.

ATT Protocol (1)

- The ATT protocol is used to discover, read and write **attributes** on a peer device.

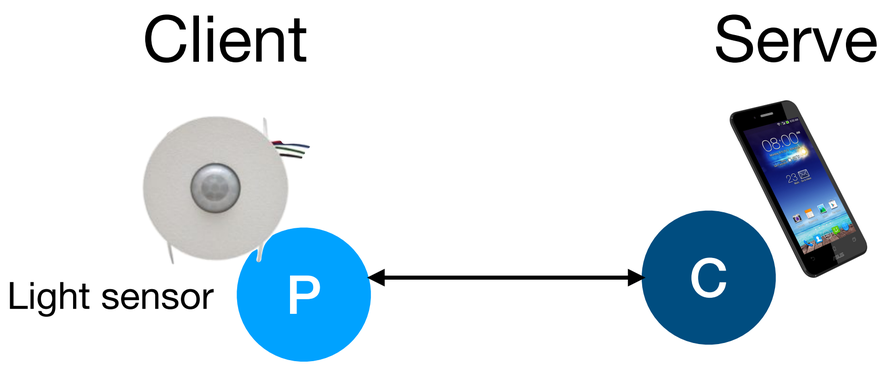
- Based on a **client-server** architecture where the server holds the data and can either send it directly to the client or the client can poll the data from the server.

- The client and server roles defined in this layer are assigned **independently** from the peripheral and central roles defined in the GAP layer
  - Nevertheless, usually a peripheral is the server since it is the one acquiring data and holding it, and the central is usually the client.

- These roles are decided by the GATT layer

ATT Protocol (2)

- Most of the times, the mobile phone (central) acts as client, reading data advertised by the sensor (peripheral - server).
- Sometimes, the mobile phone acts as a server and the sensor as a client, as in the picture, which requests a firmware update to the mobile.



- In this case, the mobile is still a central, listening to the advertisement transmitted by the sensor.

ATT Protocol - Attributes

Some UUIDs

UUID	Attribute
0x2A19	Battery level
0x2A37	Heart beat rate
0x2A6E	Temperature
0x2A6F	Humidity

- Attributes is a standardised data representation format.
- Attributes are composed of four fields:
  - **Type**, defined by a Universally Unique Identifier (UUID), 128-bit value.
  - **Handle**, unique unsigned 16-bit identifier that is used by the client to reference an attribute on the server. It makes the attribute “addressable,” and it does not change during a single connection.
  - **Permissions**, defines the level of access control for a resource (read/ write/notify).
  - **Value**, the attribute data.

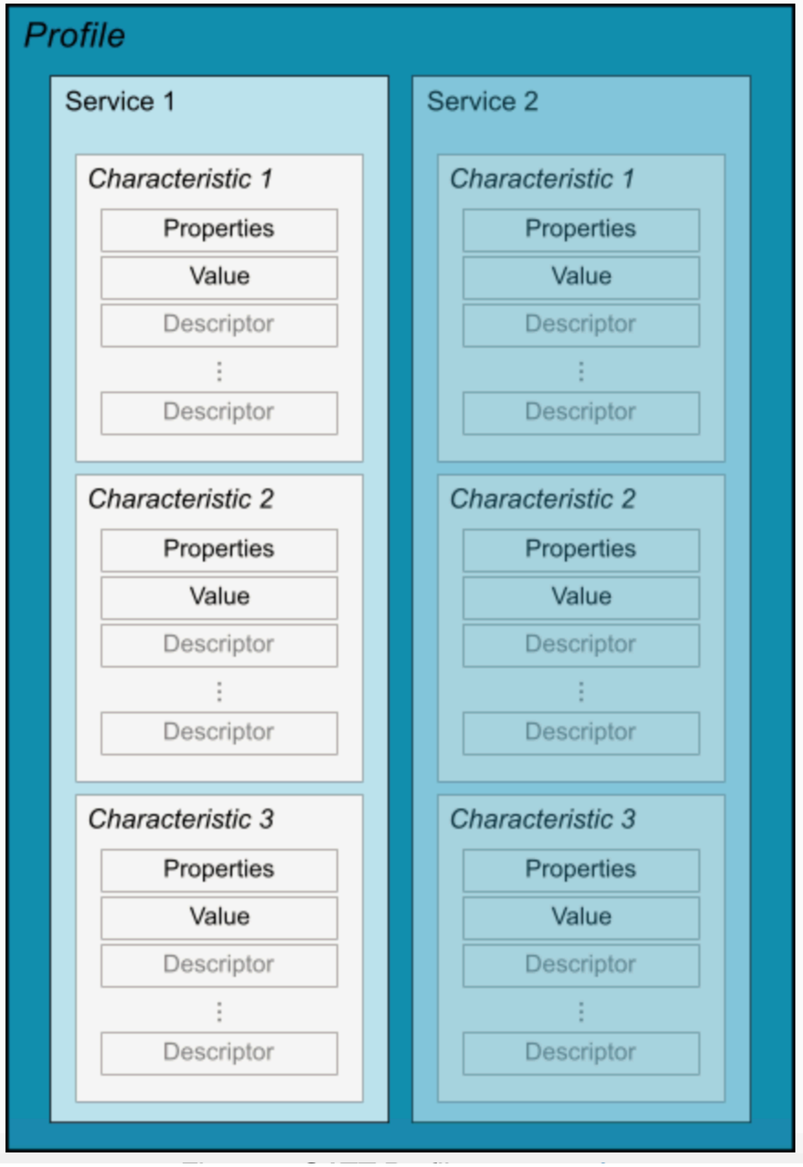
ATT Protocol - operations

ATT protocol defines six methods by which attributes can be read or written. They define different Protocol Data Units (PDU), i.e., different packets to be encapsulated and sent over the physical link.

- **Request**: sent to a server by a client to perform an operation (i.e., clients need to read a value).
- **Response**: sent to a client in response to a request.
- **Command**: sent to a server by a client (does not require acknowledgement).
- **Indication**: unsolicited PDUs sent to a client by a server, used when the server needs to sent critical data reliably.
- **Confirmation**: PDUs sent to confirm receipt of an indication by a client.
- **Notification**: unsolicited PDUs sent to a client by a server for frequent, low-latency updates (do not require acknowledgement).

GATT Layer

- The generic Attribute Profile layer sits on top of the ATT layer and provides a logical hierarchical classification of attributes using:
  - **profiles**,
  - **services** and
  - **characteristics**.
- It uses these concepts to govern the data transfer between BLE devices.



GATT Layer - Profiles, Services and Characteristics

- A **profile** is a pre-defined collection of Services.

  - Profiles foster interoperability across products from different vendors. To adhere to a profile, software must offer a predefined set of capabilities.
    - List of officially adopted GATT-based profiles

Dictates the use case that the device supports

- **Services** are used to break data up into logical entities and contain specific chunks of data, the characteristics.
  - can have one or more characteristics,
  has a unique UUID
  - List of BLE Services

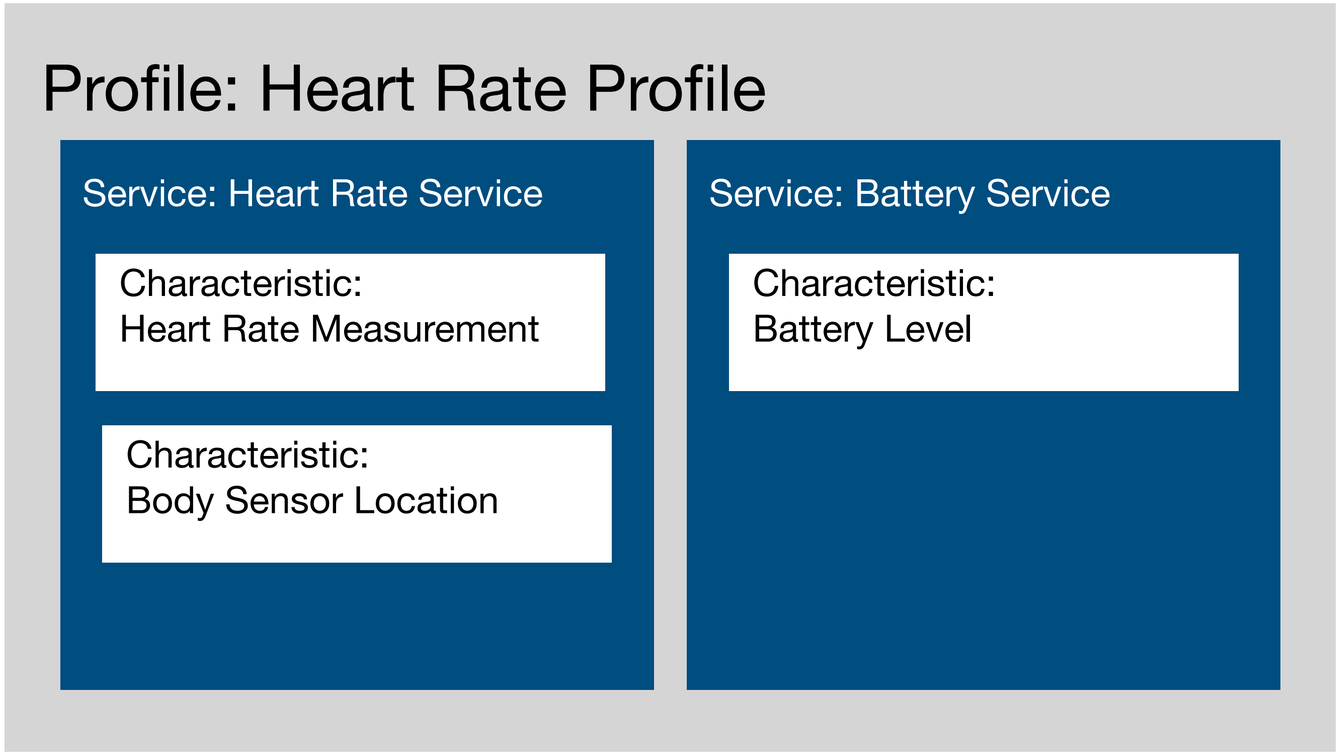
Describes a particular function that the server supports

- **Characteristics** are the lowest concept in GATT. They encapsulate single data point and include properties like **read**, **write**, **notify**, etc.

user or application data that is sent from one device to another

GATT Layer - Profiles, Services and Characteristics

- Example



Before a client starts interacting with a server, the client is not aware of the nature of the attributes stored on that server. Therefore, the client first performs **Service Discovery** where it inquires the server about its attributes.

Sensor

Mobile

Advertising (broadcasts advertising data)	Initialising. Hears advertisements from sensor and sends connection request to it
Receives connection requests	
(As peripheral) CONNECTED! (As central)	
	Performs GATT Primary Service Discovery
Sends its Services' UUID	
	Sends read request for a service
Send list of characteristics	

Disconnection
mobile sends disconnect command
or sensor disconnects after timeout

ROLES:
GAP peripheral,
GATT server

ROLES:
GAP central,
GATT client

Curiosity

- Our mobile phones have Bluetooth or BLE?
- They have both, and are used for different purposes.
  - For instance, Bluetooth is used for wireless earphones/headphones
  - BLE is used for Health & fitness sensors. IPhones uses BLE for iBeacons (location beacons).

6.2 Layer 3 Protocols