Introduction to Bluetooth Low Energy

Petter Myhre

Today’s host

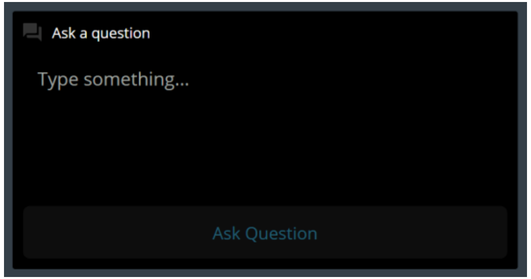
Petter Myhre

Product Marketing Manager

NORDIC® SEMICONDUCTOR

Practicalities

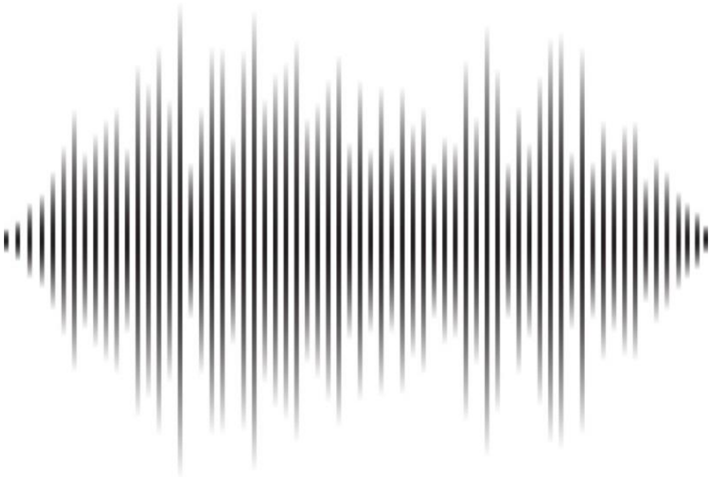
- Duration: 50-60 min
- Questions are encouraged!
- Please type questions in the top of the right sidebar
  - All questions are anonymous
  - Try to keep them relevant to the topic
- I will answer questions towards the end
- The chat is not anonymous, and should **not** be used for questions
- If you have more questions please use DevZone
- A recording of the webinar will be available together with the presentation at webinars.nordicsemi.com



{DevZone

Content

- Basics
- Architecture
- Topology and roles
- Security
- Throughput and range
- Direction Finding
- LE Audio



Basics

Key features

- Wireless personal area network technology
- Open standard -> interoperability
- Ubiquitous
- Efficient and ultra-low power
  - Small packets and short RX and TX windows
  - Use radio as little as possible
- Low RAM footprint (5.6 KB)
- Up to 1.4 Mbps throughput or more than 1000 m range

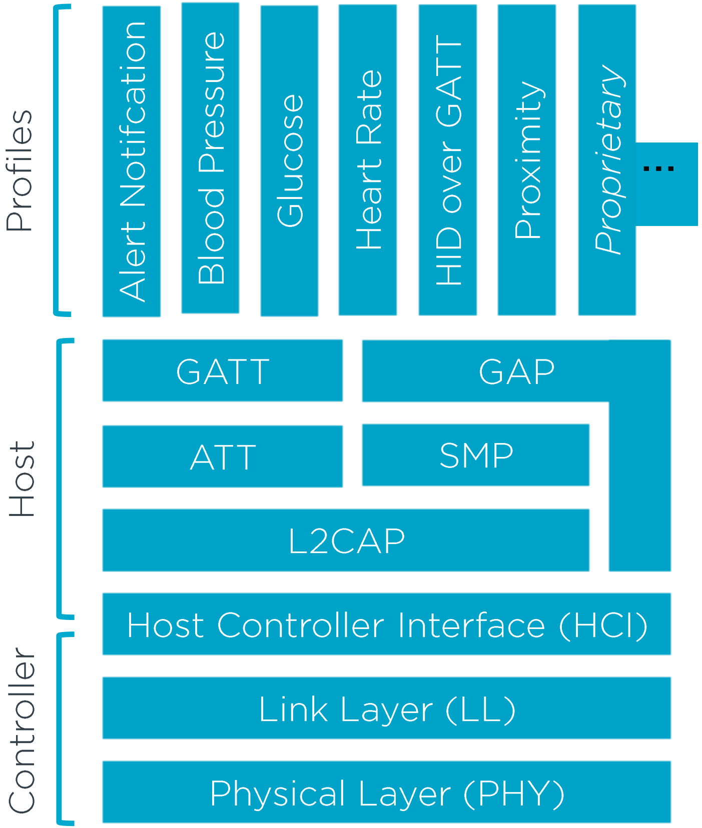
Bluetooth SIG

- Bluetooth Special Interest Group
- Develop and license Bluetooth Low Energy technology
- Network of member organizations
- Founded in September 1998
- Non-profit
- 36000 member companies
- 4.2 billion Bluetooth product shipments in 2019
- Nordic is an associate member
  - Involved in several working groups
  - Help develop specifications

The evolution of Bluetooth Low Energy

- 2010 - Bluetooth 4.0
- 2013 - Bluetooth 4.1
  - Concurrent Peripheral/Central
- 2014 - Bluetooth 4.2
  - LE Secure Connections
  - Data Length Extension
- 2016 - Bluetooth 5
  - 2 Mbps
  - Long Range
  - Advertising Extensions
  - 10 -> 20 dBm max TX power
- 2017 - Bluetooth mesh Profile
- 2019 - Bluetooth 5.1
  - Direction Finding
- 2020 - Bluetooth 5.2
  - Isochronous channels
  - LE Power Control
  - Enhanced Attribute Protocol
- Soon – LE Audio

Architecture



Profiles

Alert Notifcation

Blood Pressure

Glucose

Heart Rate

HID over GATT

Proximity

Proprietary

...

Host

GATT

GAP

ATT

SMP

L2CAP

Host Controller Interface (HCI)

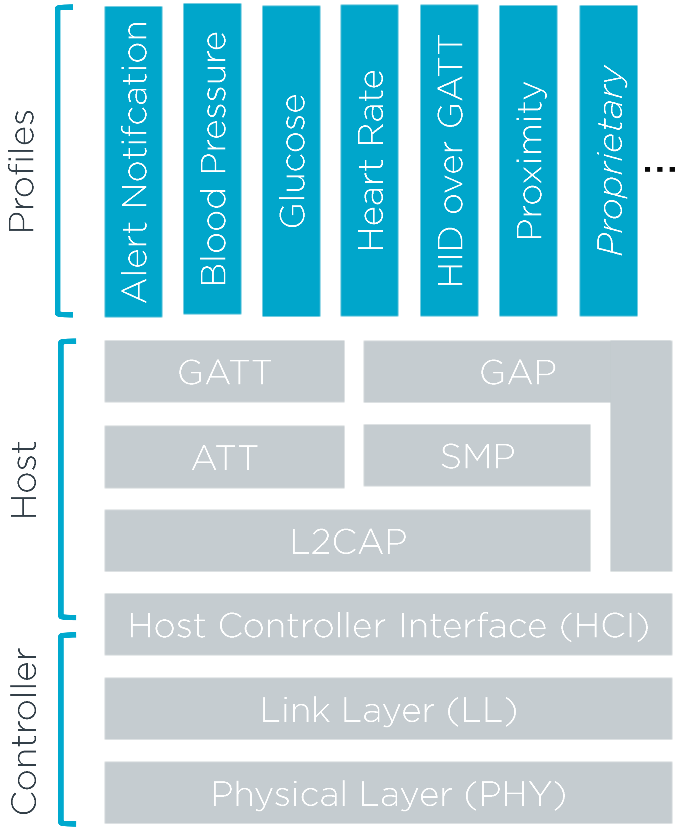
Controller

Link Layer (LL)

Physical Layer (PHY)

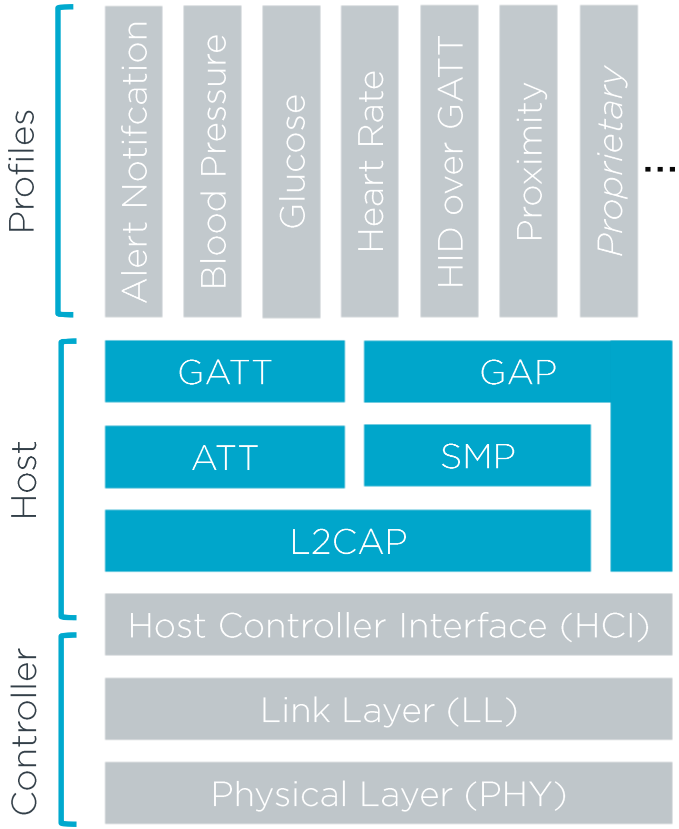
Profiles

- Profiles
  - Describes how two or more devices can discover and communicate with each other
  - Implements a specific application
  - Standard or proprietary
  - Each profile has its own specification



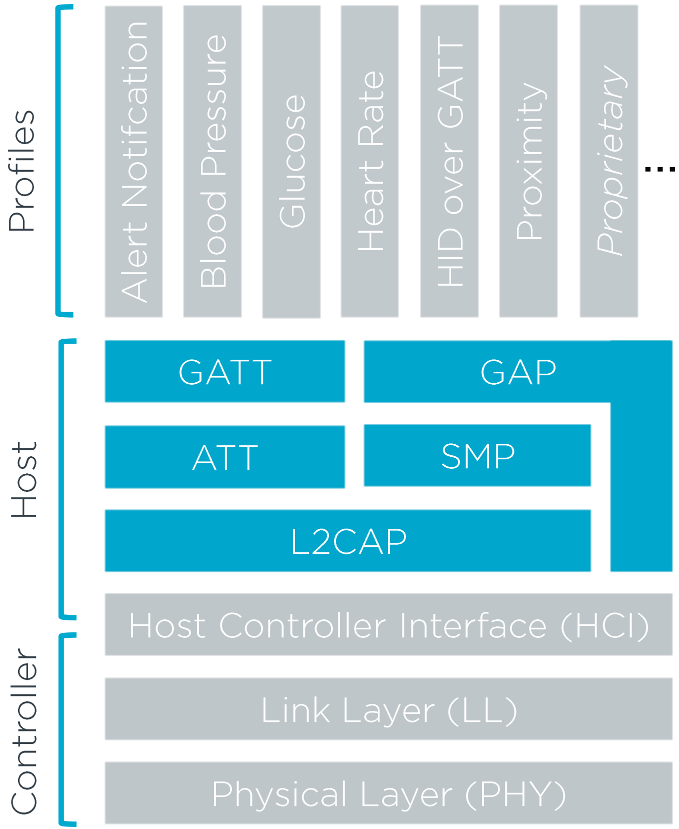
Host

- Upper layers of the Bluetooth LE protocol stack
- Logical Link Control and Adaption Protocol
- Attribute Protocol (ATT)
  - Simple client-server model
  - Client device can access attributes on the server device
- Security manager Protocol (SMP)
  - Defines protocol for pairing and key distribution



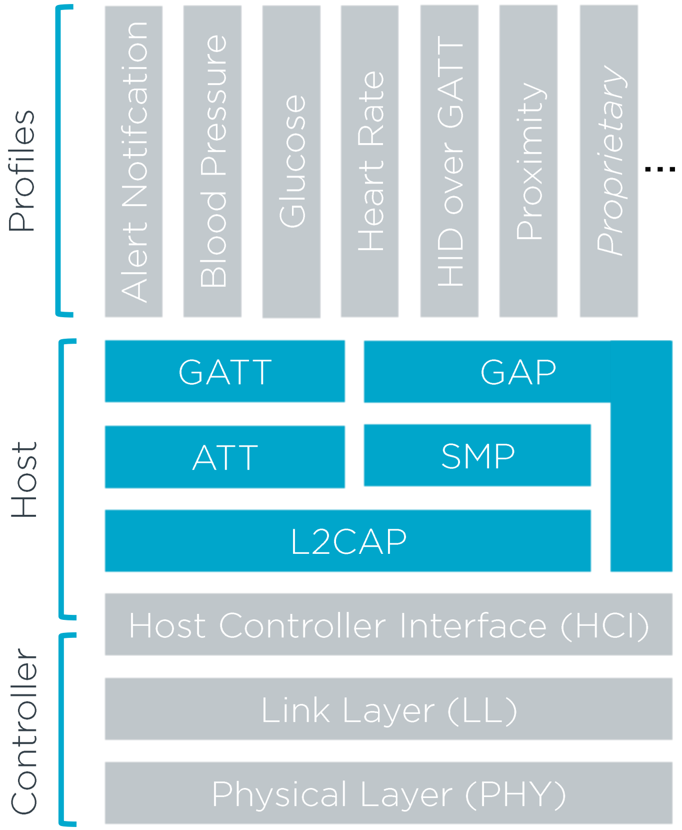
Host - GATT

- Generic Attribute Profile (GATT)
- Highest data layer
- Uses ATT to discover and access attributes
- Specifies a hierarchical structure of attributes
  - Services
  - Characteristics
  - Descriptors



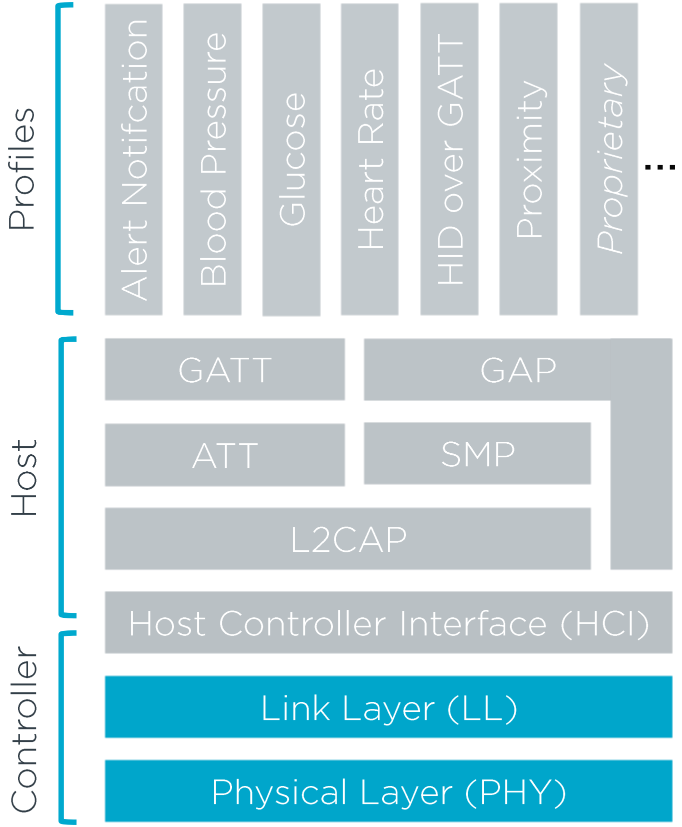
Host - GAP

- Generic Access Profile (GAP)
  - Highest control layer
  - Defines device roles
  - Defines how devices discover and connect to each other
  - Defines security modes and procedures



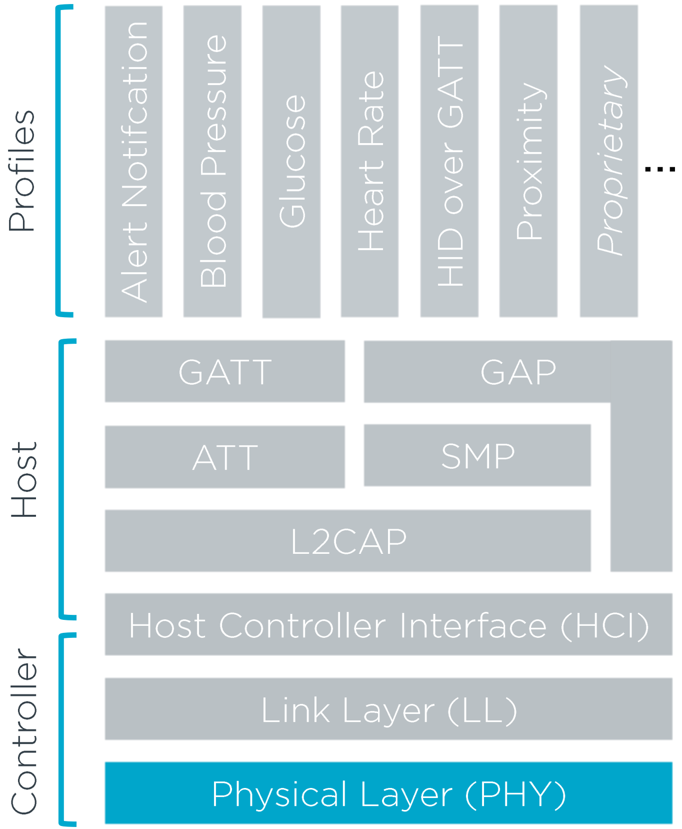
Controller

- Physical layer
  - Defines how two radios can send bits to each other
- Link Layer
  - Defines Link Layer states
  - Defines device address
  - Packet format

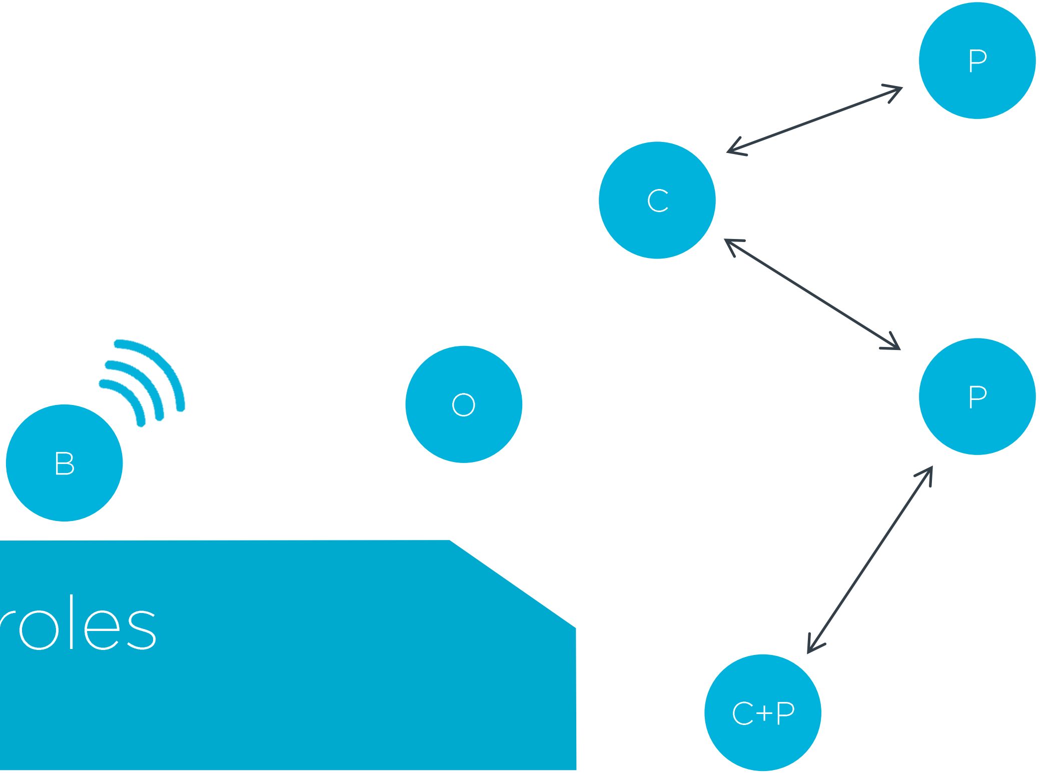


Physical layer

- 2.4 GHz ISM band
- 40 RF channels (2 MHz)
- GFSK modulation
  - 1 or 2 Msps
- Max 20 dBm TX power



Topology and roles

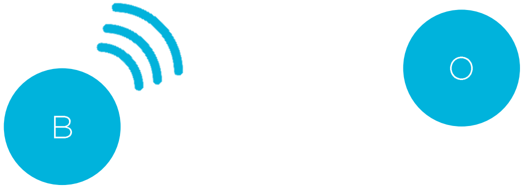


GAP roles and Link Layer states

GAP role	Link Layer state
Broadcaster	Advertising
Observer	Scanning
Peripheral	Advertising Connection (Slave)
Central	Scanning Initiating Connection (Master)

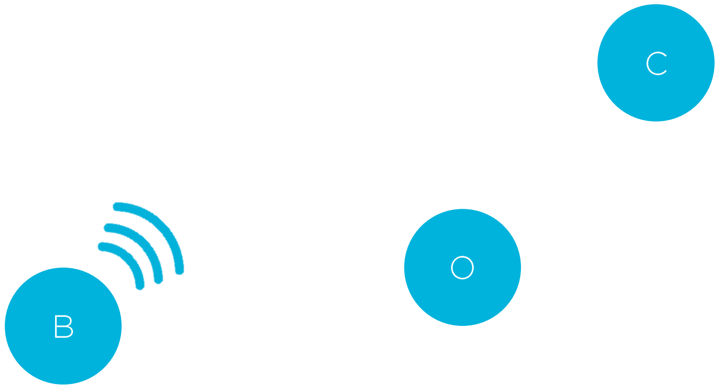
All roles can also be in the standby state

Roles (GAP)



- B Broadcaster
- O Observer
- P Peripheral
- C Central

Roles (GAP)



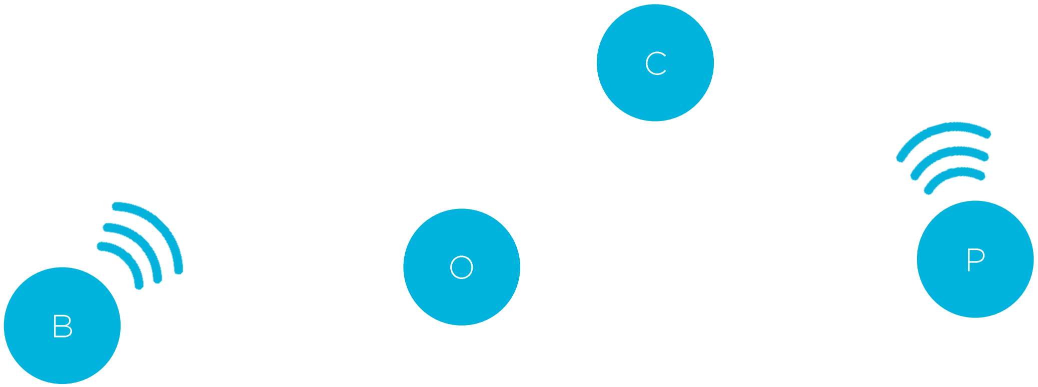
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP)



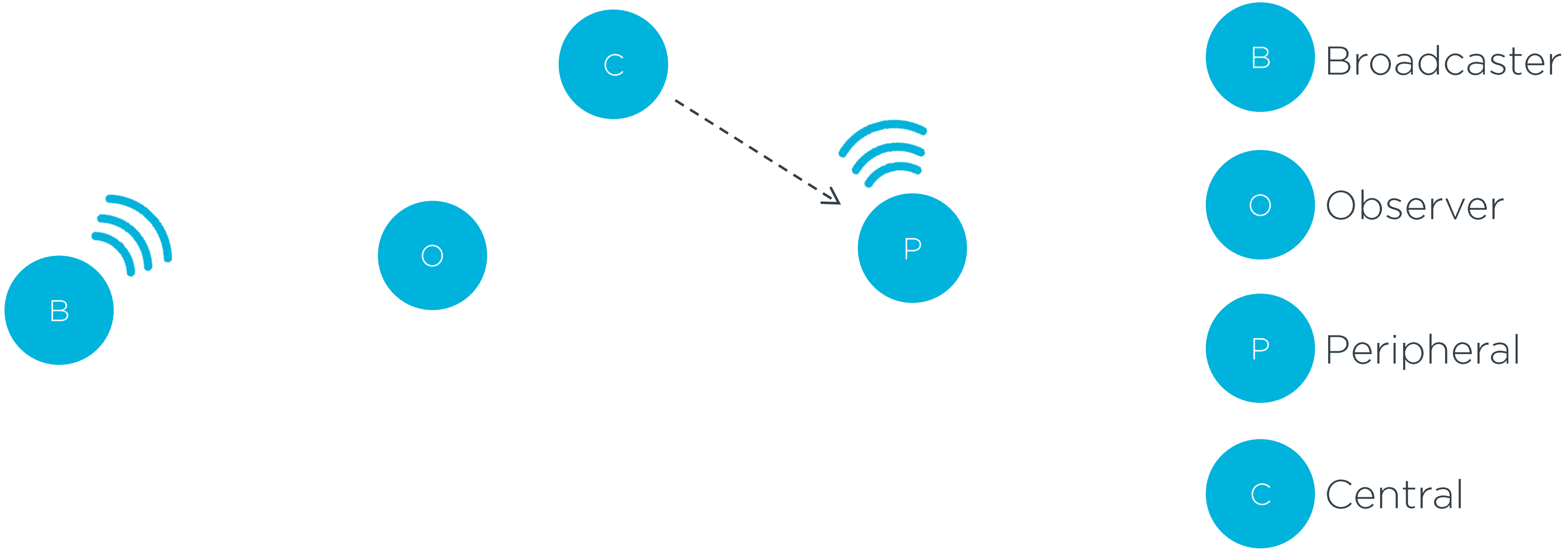
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP)



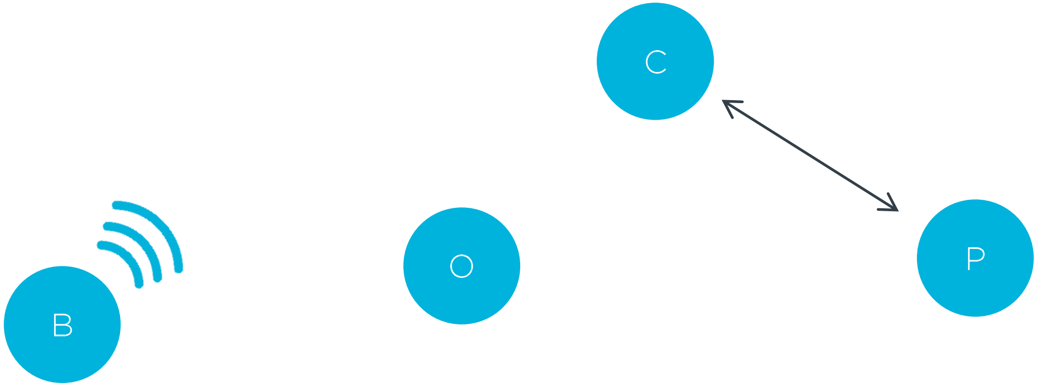
B Broadcaster

O Observer

P Peripheral

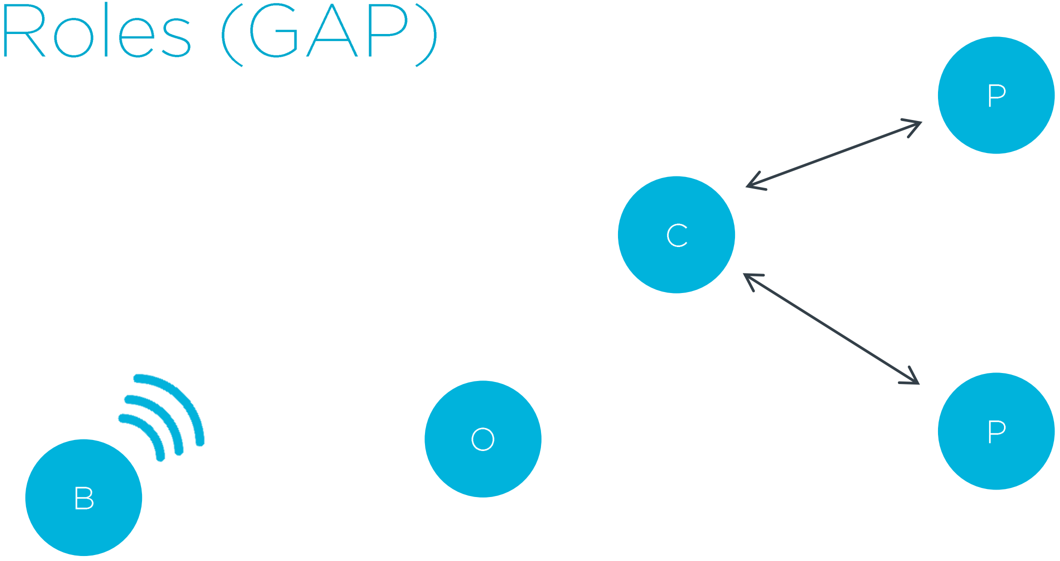
C Central

Roles (GAP)



- B Broadcaster
- O Observer
- P Peripheral
- C Central

Roles (GAP)



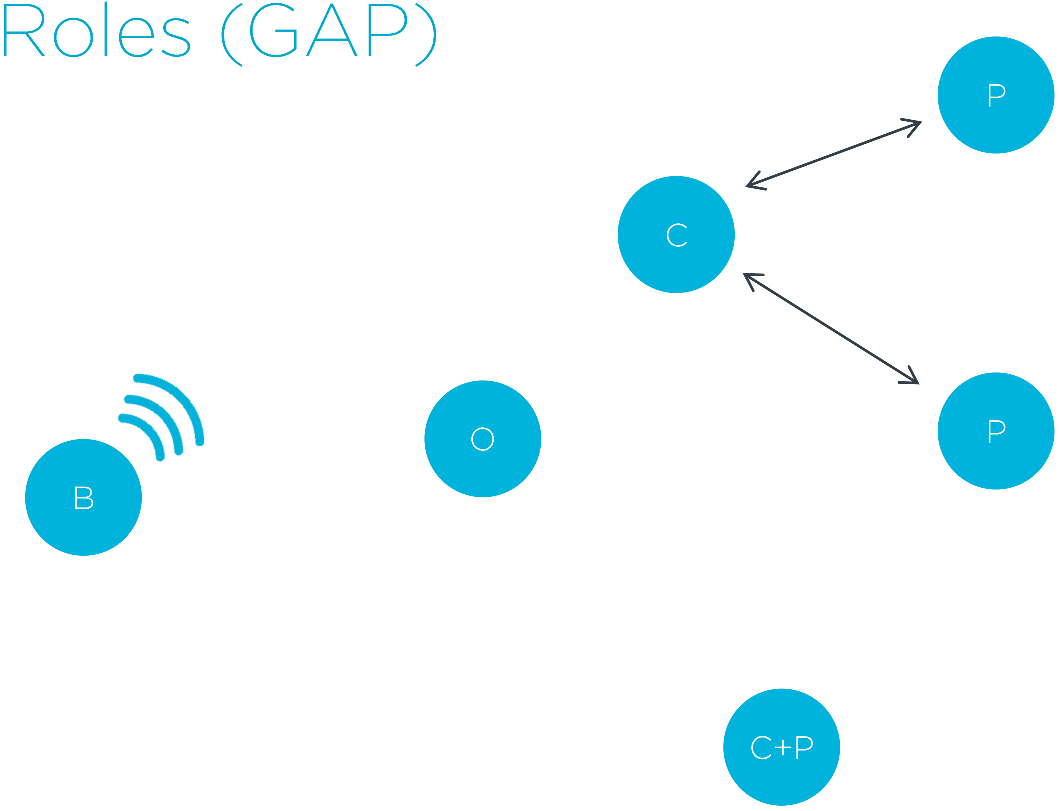
B Broadcaster

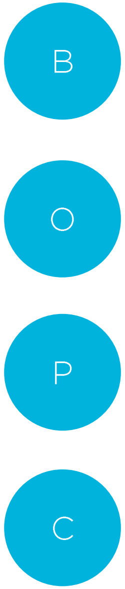
O Observer

P Peripheral

C Central

Roles (GAP)





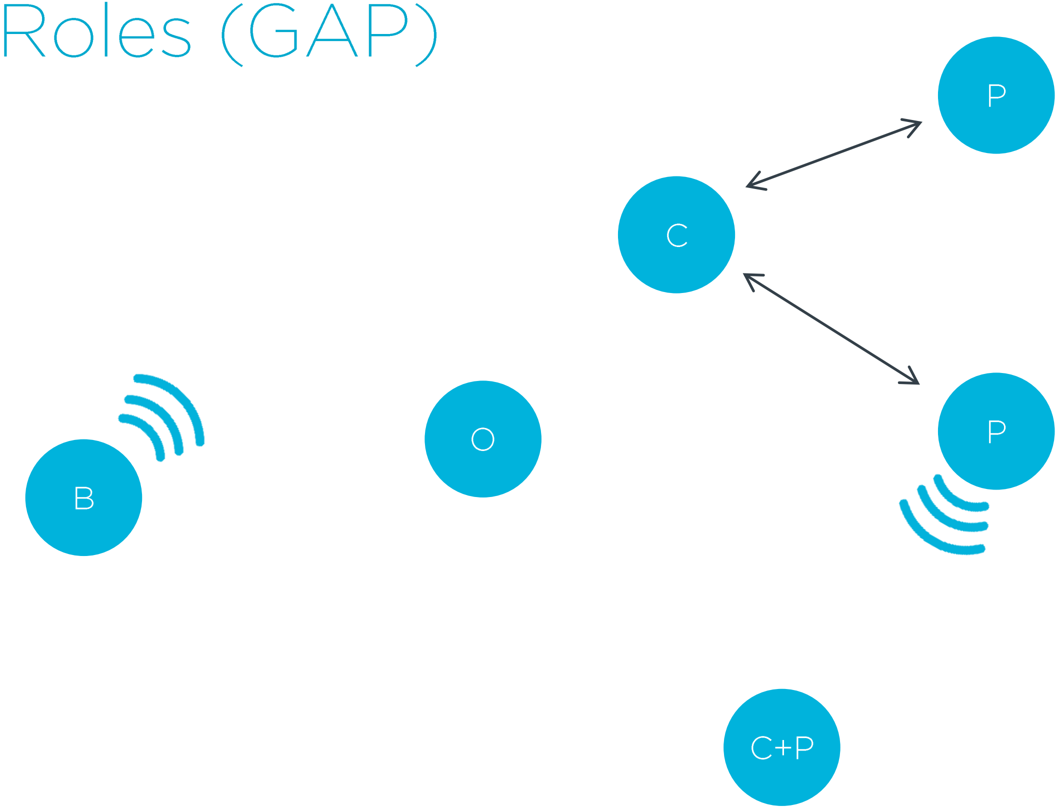
Broadcaster

Observer

Peripheral

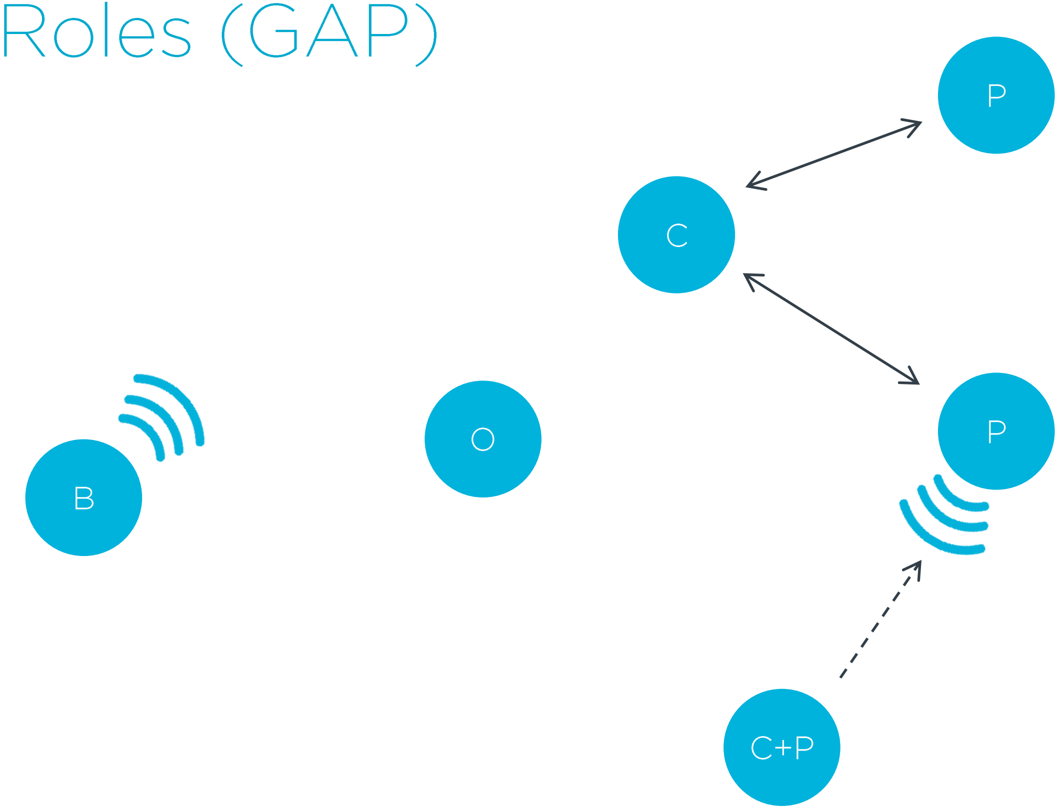
Central

Roles (GAP)



- B Broadcaster
- O Observer
- P Peripheral
- C Central

Roles (GAP)



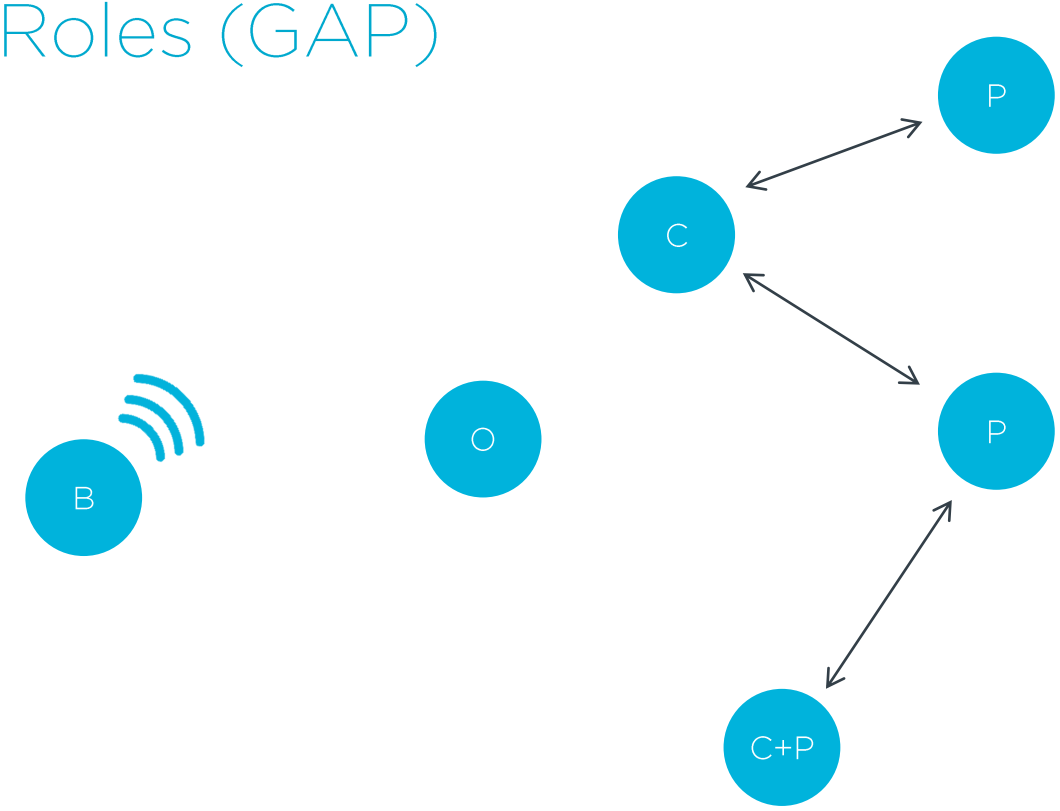
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP)



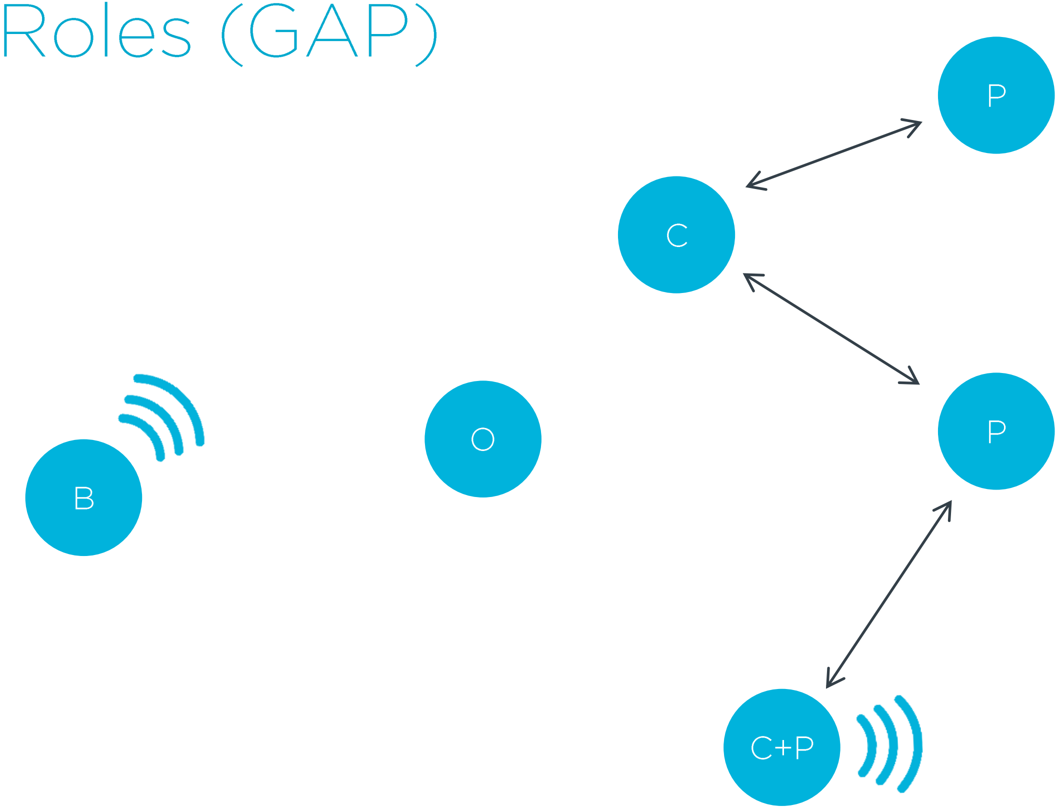
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP)



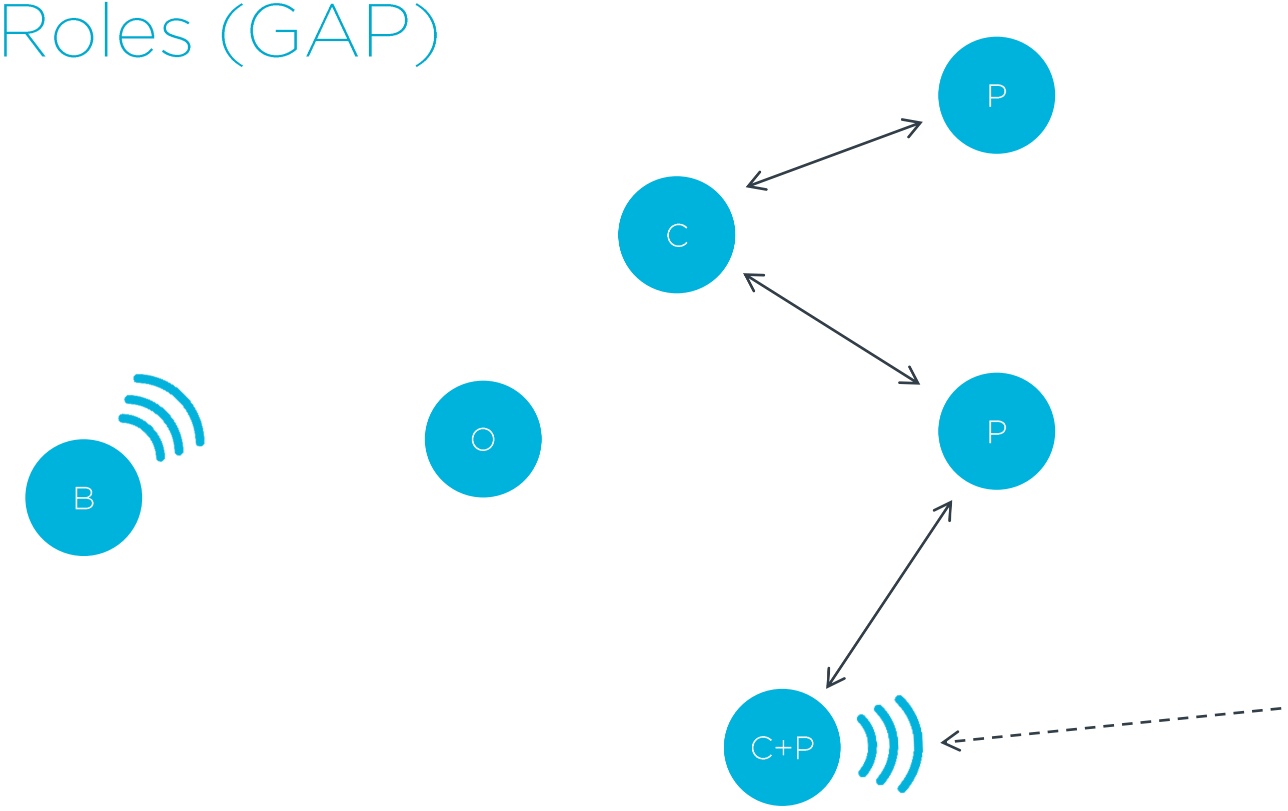
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP)



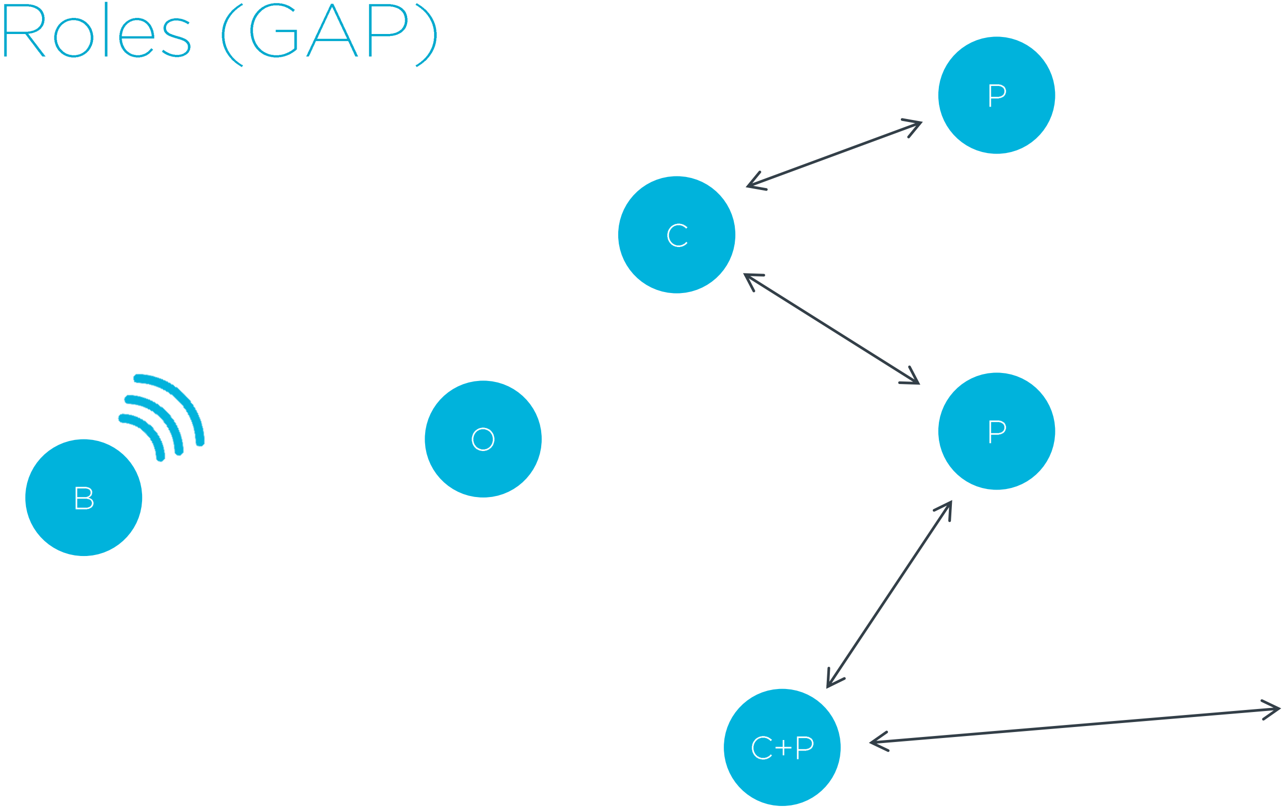
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP)



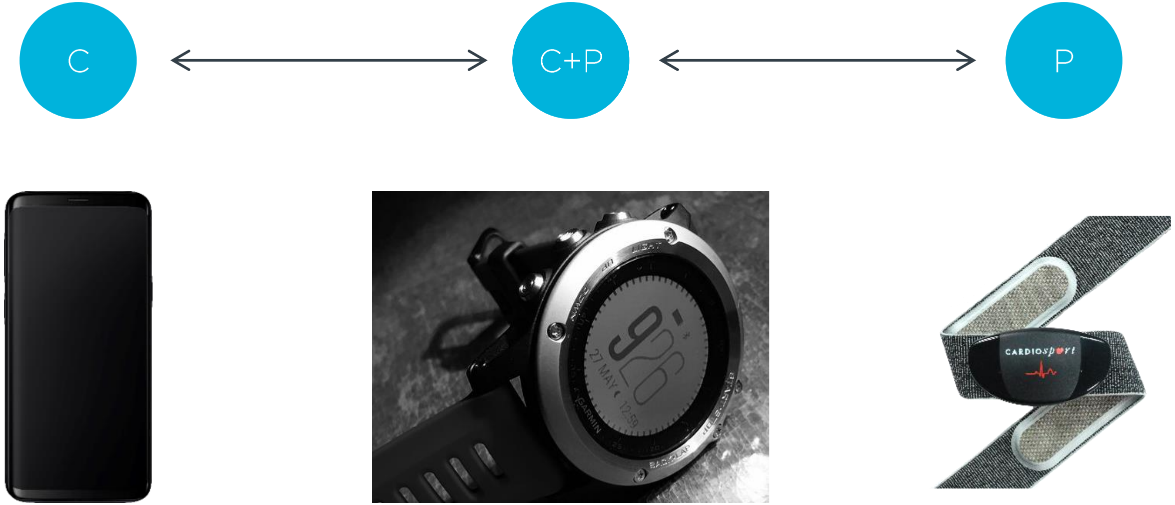
B Broadcaster

O Observer

P Peripheral

C Central

Roles (GAP) - Example



B Broadcaster

O Observer

P Peripheral

C Central

Security

Pairing and bonding

- Pairing is authenticating another device by establishing temporary shared secret keys which can be used to encrypt a link
- Bonding is pairing followed by distribution of keys which can be used to encrypt the link in future reconnections

Authentication and Encryption procedures

Each time two devices connect - connection operate with no security. A higher level of security achieved by performing:

- Authentication procedure
  - Type of pairing determines security level
- Encryption procedure
  - Connection encrypted with encryption keys already available
  - Typically if keys were shared and stored after previously bonding
  - Original pairing determines achieved security level

Legacy Pairing

- Introduced in Bluetooth 4.0
- Three methods
  - Just works
  - Passkey entry
  - Out-of-Band (OOB)
- Not recommended by the Bluetooth SIG
  - If you must use it, use OOB

LE Secure Connections

- Added in the Bluetooth Core Specification version 4.2 (2014)
- Provides protection against eavesdropping
- Provides better protection against MITM attacks
- FIPS-approved algorithms
- Uses Elliptic Curve Diffie-Hellman (ECDH) key agreement
  - Allows two peers, each having public-private key pair, to establish shared secret key over insecure channel
  - Secret key used in derivation of encryption keys
- Recommended by the Bluetooth SIG
  - Not Just Works

LE Secure Connections pairing methods

- Just Works
- Passkey Entry
  - A 6-digit value shared between devices using their IO capabilities
- Numeric Comparison
  - A 6-digit value displayed on both devices and confirmed on both sides by user pressing “OK”
- OOB
  - Encryption keys based on data transferred by other means, for example NFC

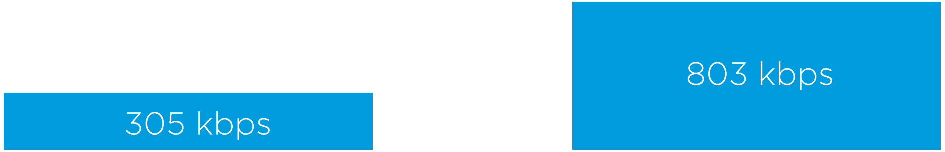
Throughput and range

Throughput

305 kbps

- Bluetooth 4.0/4.1
  - 1 Mbps
  - 27 byte payload

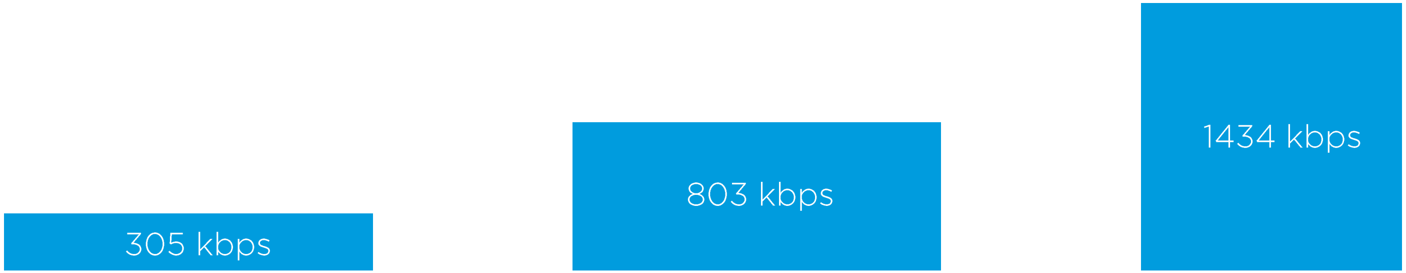
Throughput



- Bluetooth 4.0/4.1
  - 1 Mbps
  - 27 byte payload

- Bluetooth 4.2
  - Data Length Extension
  - 251 byte payload

Throughput



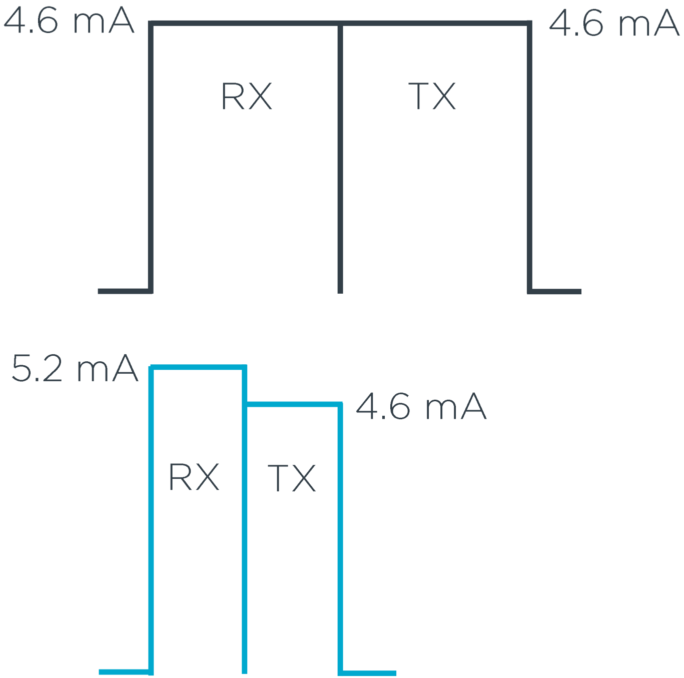
- Bluetooth 4.0/4.1
  - 1 Mbps
  - 27 byte payload

- Bluetooth 4.2
  - Data Length Extension
  - 251 byte payload

- Bluetooth 5
  - High-throughput 2 Mbps

Less Time on Air

~½ Energy Consumption

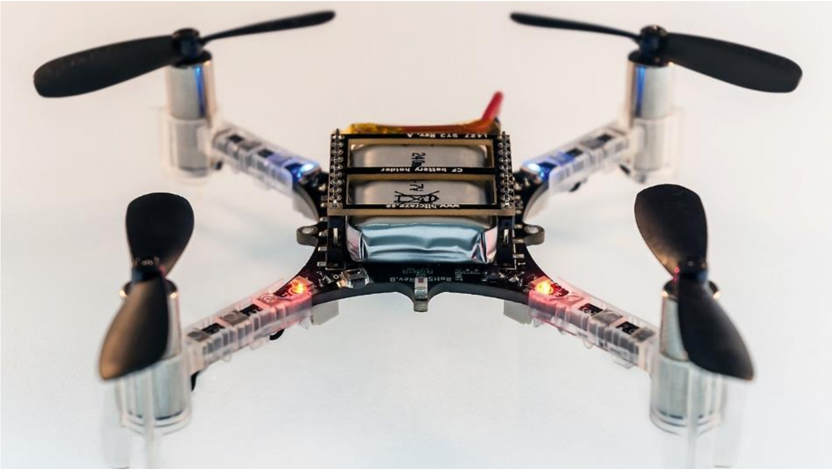


More connections

Improved coexistence

What is the range?

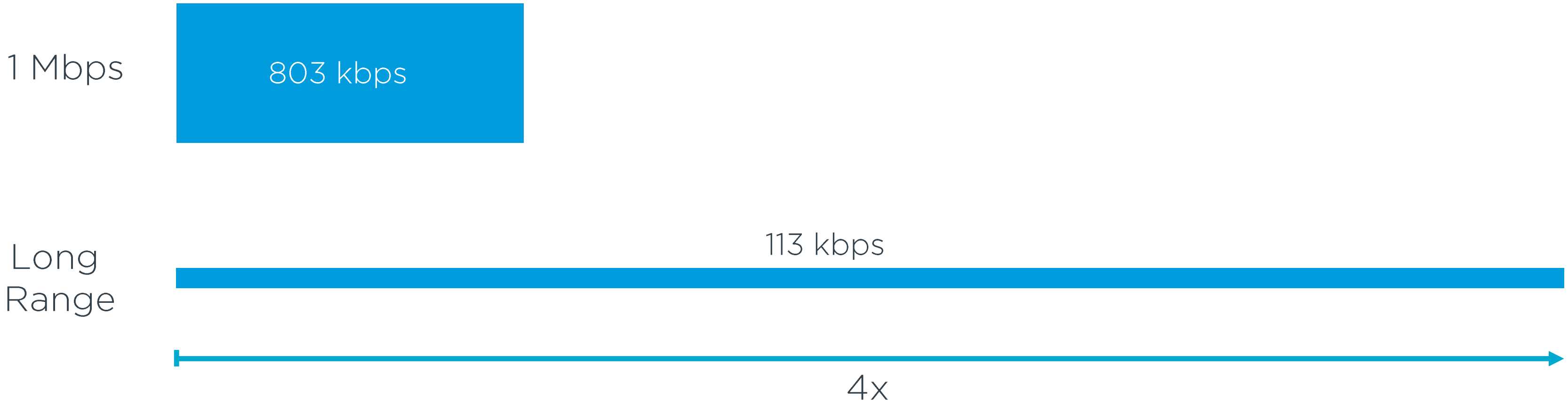
- It is **not** a few meters!
- Depends highly on the environment
- TX power
  - Typically 0-8 dBm
  - Max 20 dBm
- RX sensitivity
- Bluetooth Long Range



Bluetooth Long Range

- Introduced in Bluetooth 5
- Standard 1 Msps modulation
- 8 symbols per bit
  - 125 kbps data rate
- 12 dB increased sensitivity
  - 400% range increase
- Reduces efficiency
- No increase in peak currents
- No increase in BOM

Bluetooth Long Range



1 Mbps

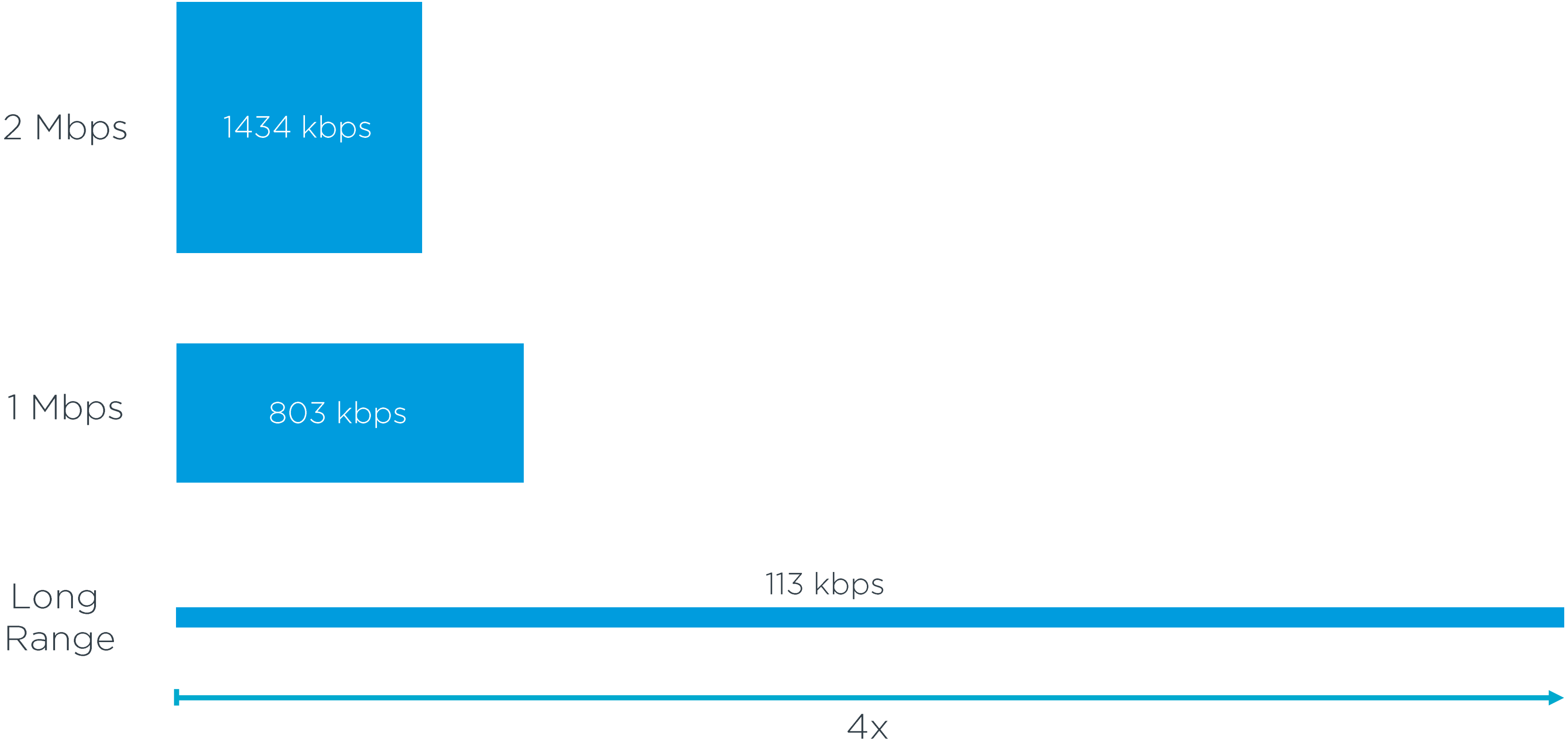
803 kbps

Long Range

113 kbps

4x

Flexibility



2 Mbps

1434 kbps

1 Mbps

803 kbps

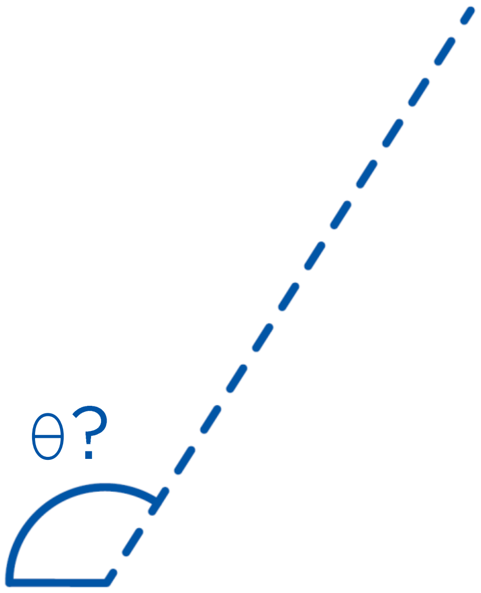
Long Range

113 kbps

4x

Direction Finding

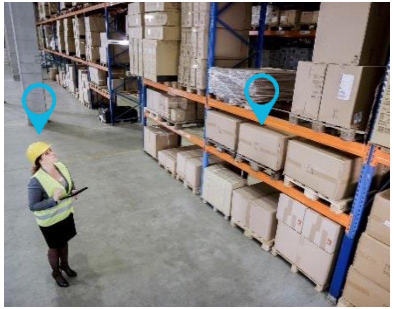
Direction Finding



- Hallmark feature of Bluetooth 5.1 Core Specification
- Adopted January 29th 2019
- Requires radio changes
- Optional feature
- Enables positioning solutions to not only rely on received signal strength indicator (RSSI), but also the actual direction of a signal

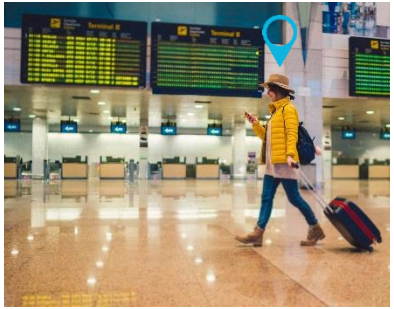
Direction Finding – use cases

Asset tracking



Real-Time Location Systems (RTLS)

Wayfinding



Indoor positioning

Point of interest

Proximity marketing

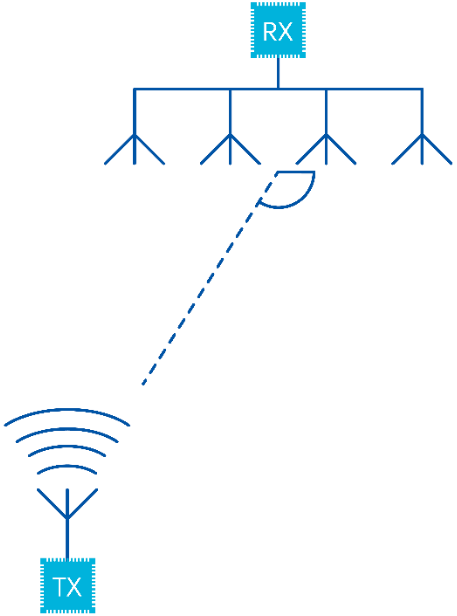
Item finding

More advanced item finding solutions

Positioning systems

Proximity solutions

Angle of Arrival (AoA)



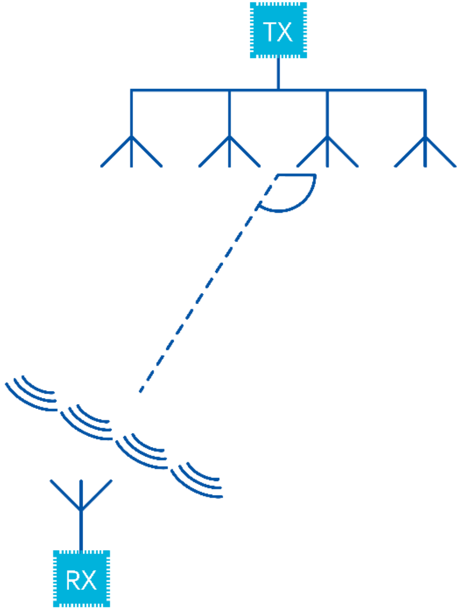
Transmitter

- Simple beacon
- Single antenna
- No I/Q calculations needed

Receiver

- Advanced
- Antenna array and RF switch
- I/Q data needed for angle estimation

Angle of Departure (AoD)



Transmitter

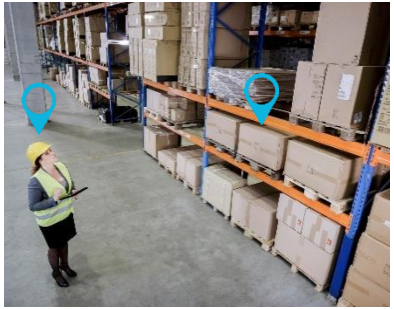
- Simple beacon
- Antenna array and RF switch
- No I/Q calculations needed

Receiver

- Scanner / Observer
- Single antenna
- I/Q data needed for angle estimation

Direction Finding – use cases with AoA/AoD

Asset tracking

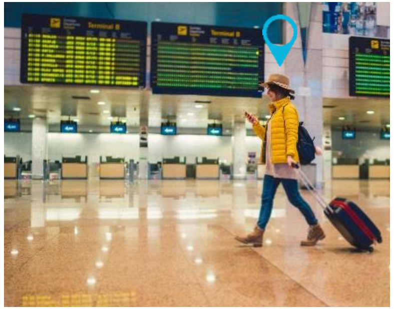


AoA

Multiple receivers at fixed locations

Transmitter can be beacon or smart phone

Wayfinding



AoD

Multiple transmitters at fixed locations

Receiver typically a smart phone

Point of interest

AoD

Only relative direction needed

Receiver typically a smart phone

Item finding

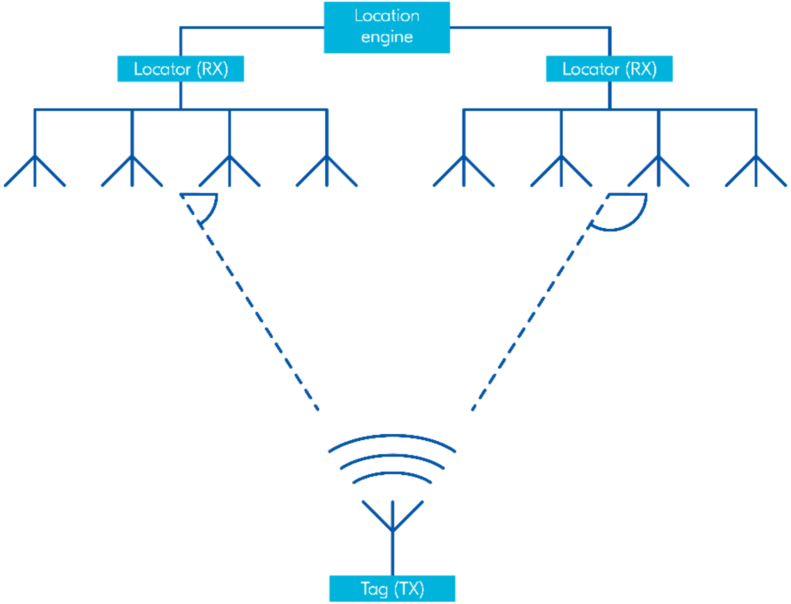
AoD

Only relative direction needed

Receiver typically a smart phone

Asset tracking - RTLS

- Real-time location system
- AoA method
- Tag is a simple transmitter
- Multiple locators at fixed locations
- Each locator determines the direction of the signal
- The location engine determines the position of the tag



LE Audio

Bluetooth audio

Classic Audio

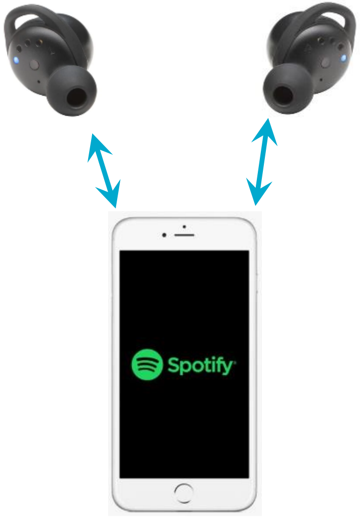
LE Audio

LE Audio

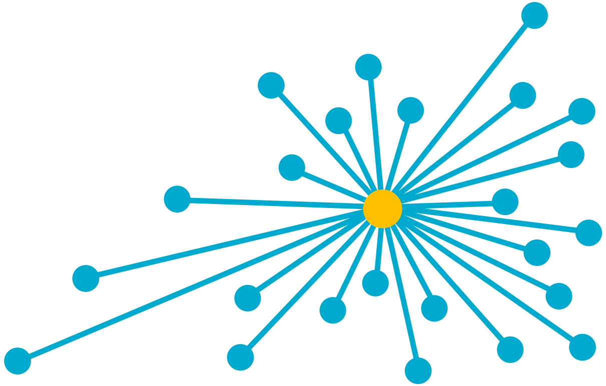
- Announced January 6th 2020
- Isochronous channels
- New audio codec
- Multi-stream audio for earbuds
- Broadcast audio for Audio Sharing

Isochronous channels (ISOC)

- Audio streaming to one or more connected devices
  - Channels are synchronized

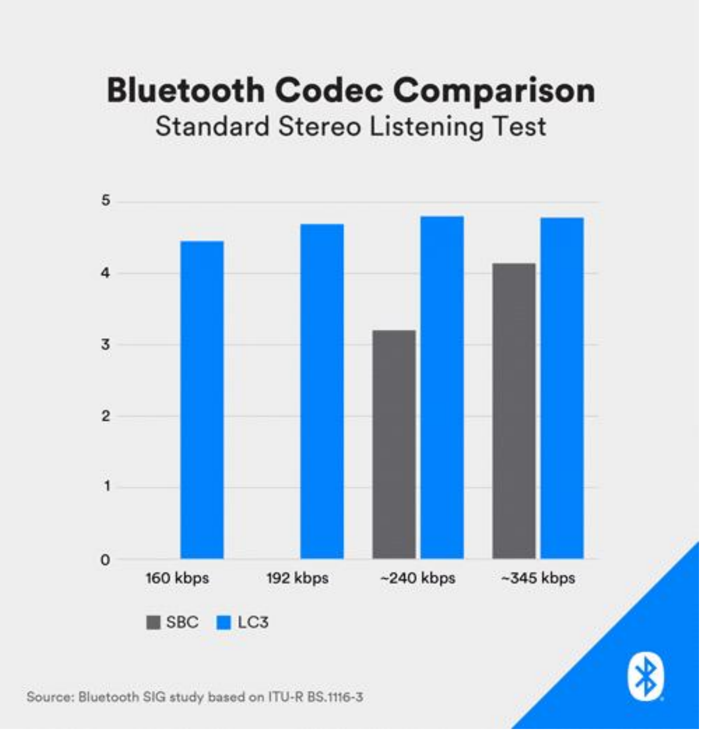


- Audio broadcasting to multiple devices



New audio codec – LC3

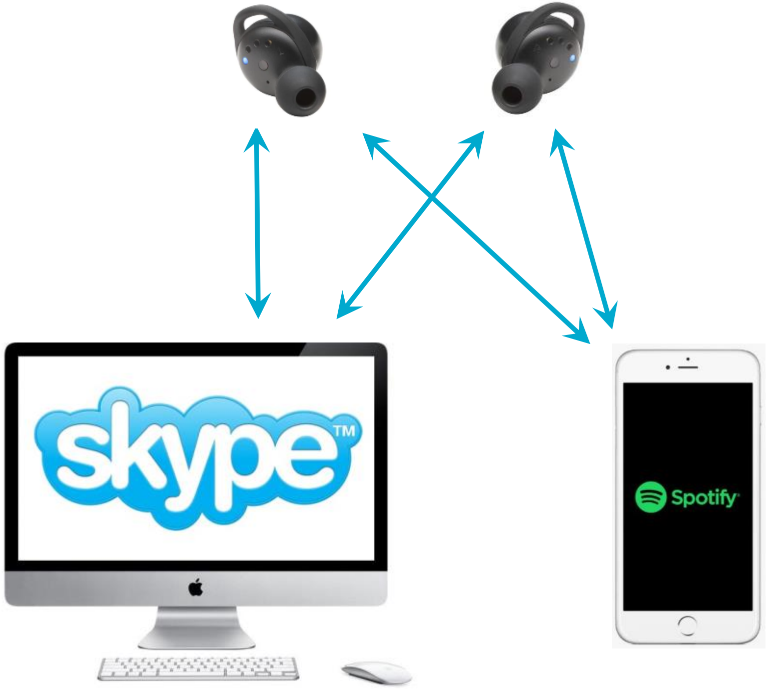
- Low Complexity Communication Codec (LC3)
- High-quality, low-power codec
- Mandatory for LE Audio
- 50% improvement in perceived audio quality
  - 240 kbps
- Offers the flexibility to trade-off audio quality with longer battery life or smaller products (batteries)



Source: Bluetooth SIG study based on ITU-R BS.1116-3

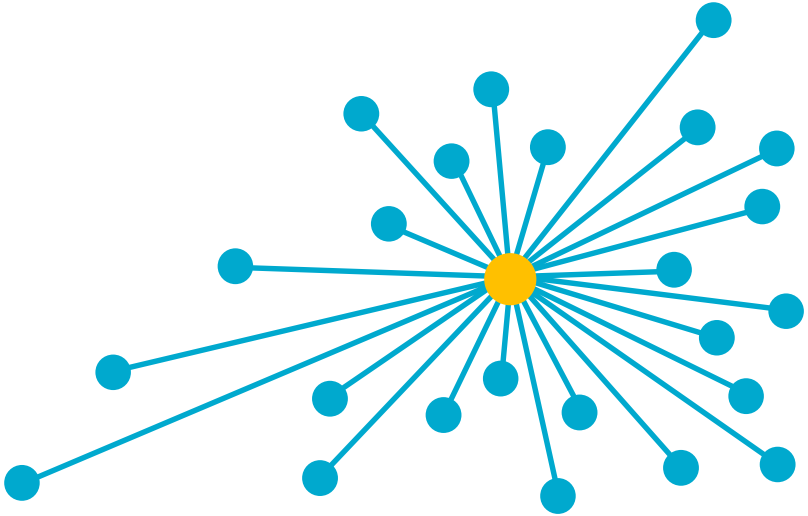
Multi-stream audio for earbuds

- Better performing earbuds
- Multiple, independent, synchronized audio streams
- Smoother transitions between audio source devices



Broadcast audio for Audio Sharing

- Unlimited number of sink devices
- Personal Audio Sharing
  - Shared Listening
  - Shared Watching
- Location Audio Sharing
  - Public TVs
  - Translation Services
  - Hearing assistance



Support and community

Nordic DevZone

Insight*Inspiration*Network

Q&A