BLUETOOTH LOW ENERGY

Bluetooth LE, BLE

Objectives

- Describe the main characteristics of Bluetooth LE
- Understand the role of its different layers
- Understand the connection process in Bluetooth LE
- Learn data is exchanged in Bluetooth LE connections

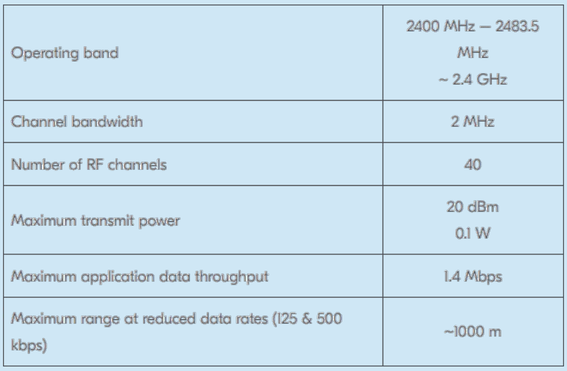
Agenda

- Introduction
  - Protocol stack
  - Main concepts
- Advertising
- Connections
- Data exchange
- Security

Introduction

- Bluetooth (SIG) standards organization
- Bluetooth LE
  - introduced in version 4.0
  - for low-power IoT applications.

https://www.bluetooth.com/



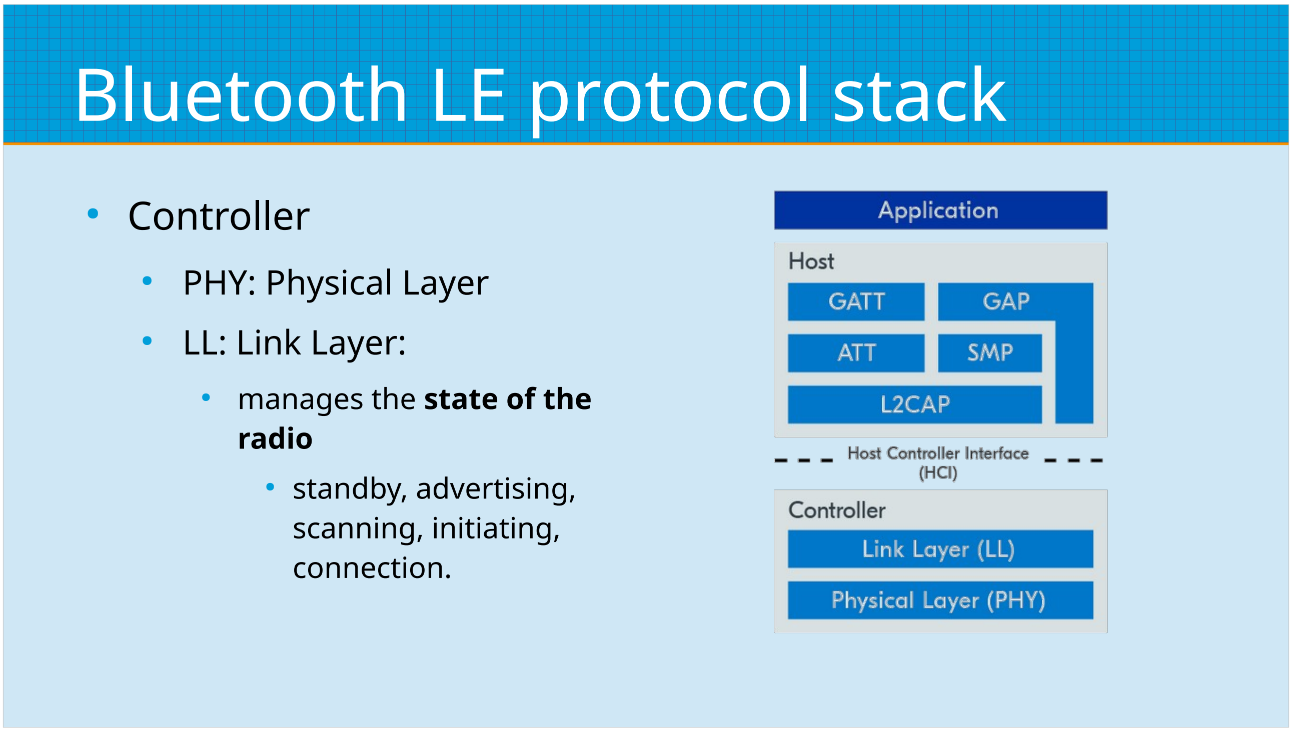
Operating band	2400 MHz – 2483.5 MHz ~ 2.4 GHz
Channel bandwidth	2 MHz
Number of RF channels	40
Maximum transmit power	20 dBm 0.1 W
Maximum application data throughput	1.4 Mbps
Maximum range at reduced data rates (125 & 500 kbps)	~1000 m

: *hagall* (ᚼ) y *berkana* (ᛒ)

Iniciales rey Harald Blåtand

Introduction

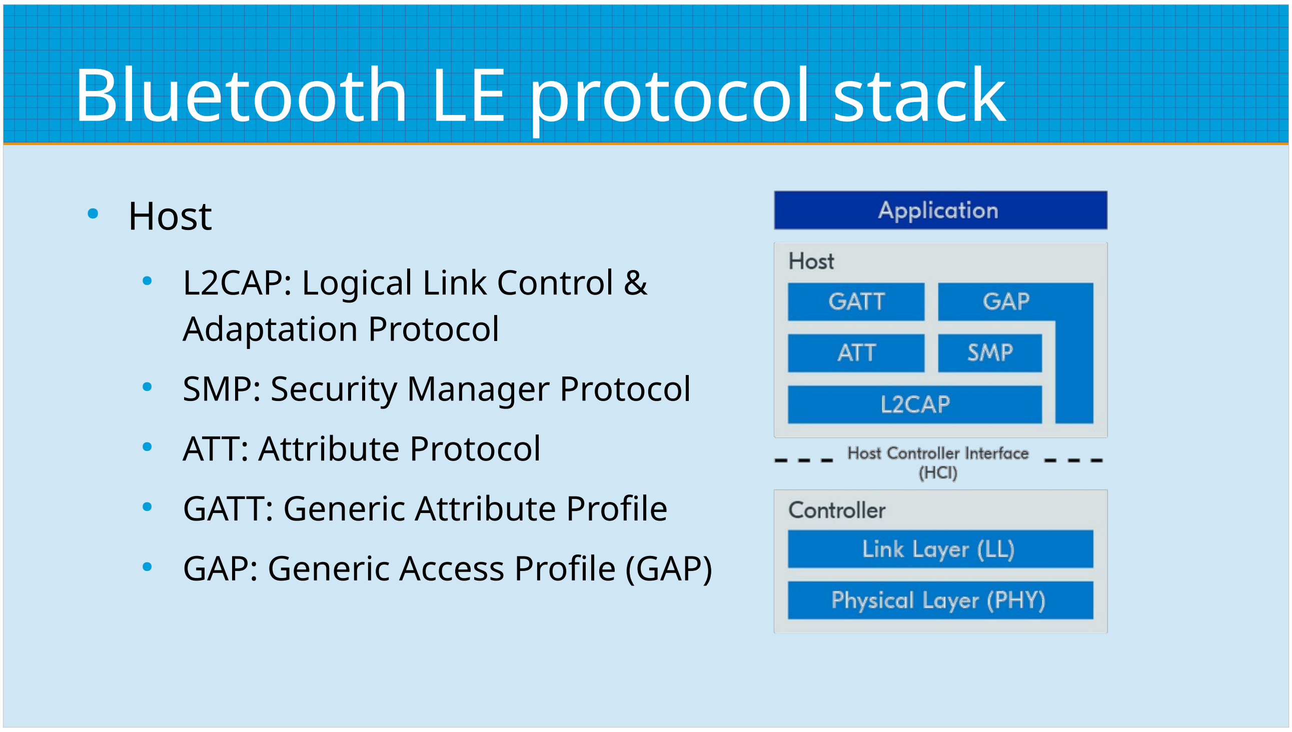
- Bluetooth LE differs from Bluetooth Classic
  - low energy consumption by sacrificing data rate
    - **data packets** are made **smaller (**ranging from 27 to 251 bytes)
    - **data** is being sent as **seldom as possible** (avoid long radio-on times)
  - more suitable for **battery-operated** devices that need to operate on minimal power and only **send small bursts of data**
  - different use cases than Bluetooth classic



Bluetooth LE protocol stack

- Controller
  - PHY: Physical Layer
  - LL: Link Layer:
    - manages the **state of the radio**
      - standby, advertising, scanning, initiating, connection.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.

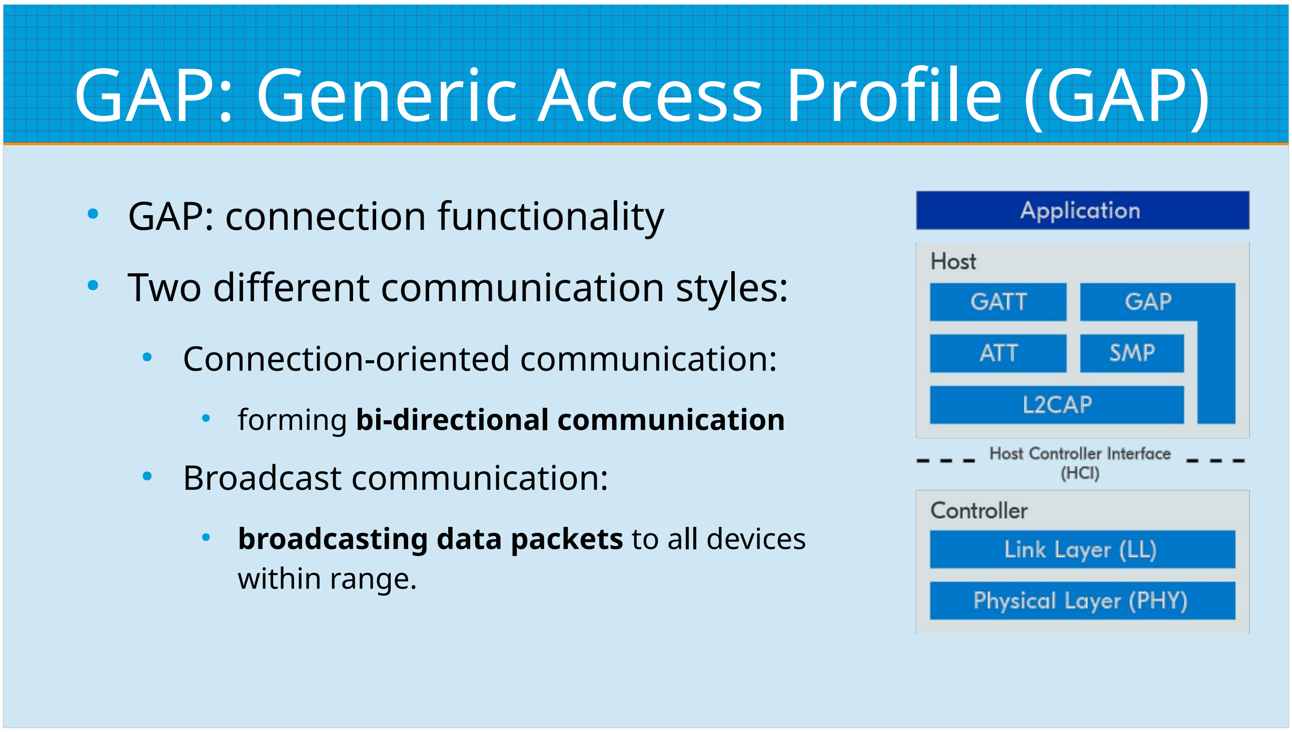


Bluetooth LE protocol stack

- Host
  - L2CAP: Logical Link Control & Adaptation Protocol
  - SMP: Security Manager Protocol
  - ATT: Attribute Protocol
  - GATT: Generic Attribute Profile
  - GAP: Generic Access Profile (GAP)

Application
Host
GATT
GAP
ATT
SMP
L2CAP
Host Controller Interface (HCI)
Controller
Link Layer (LL)
Physical Layer (PHY)

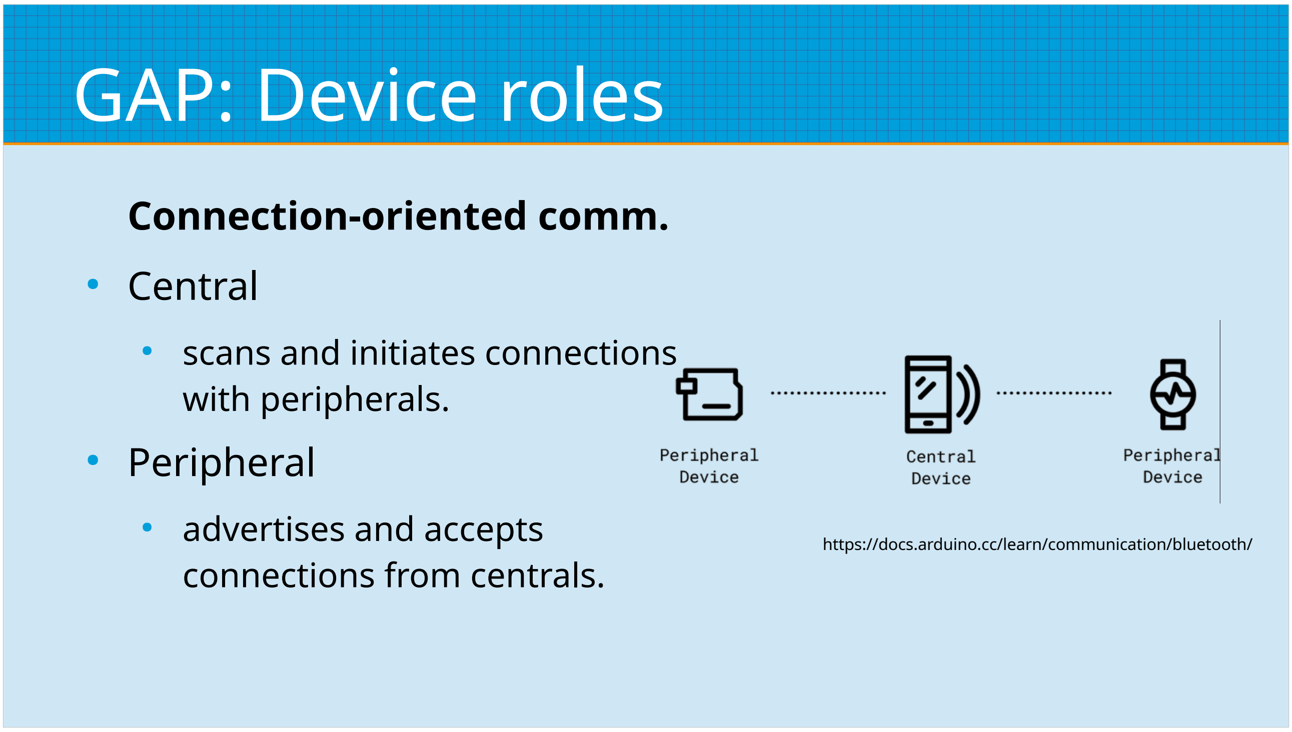
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



GAP: Generic Access Profile (GAP)

- GAP: connection functionality
- Two different communication styles:
  - Connection-oriented communication:
    - forming **bi-directional communication**
  - Broadcast communication:
    - **broadcasting data packets** to all devices within range.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



GAP: Device roles

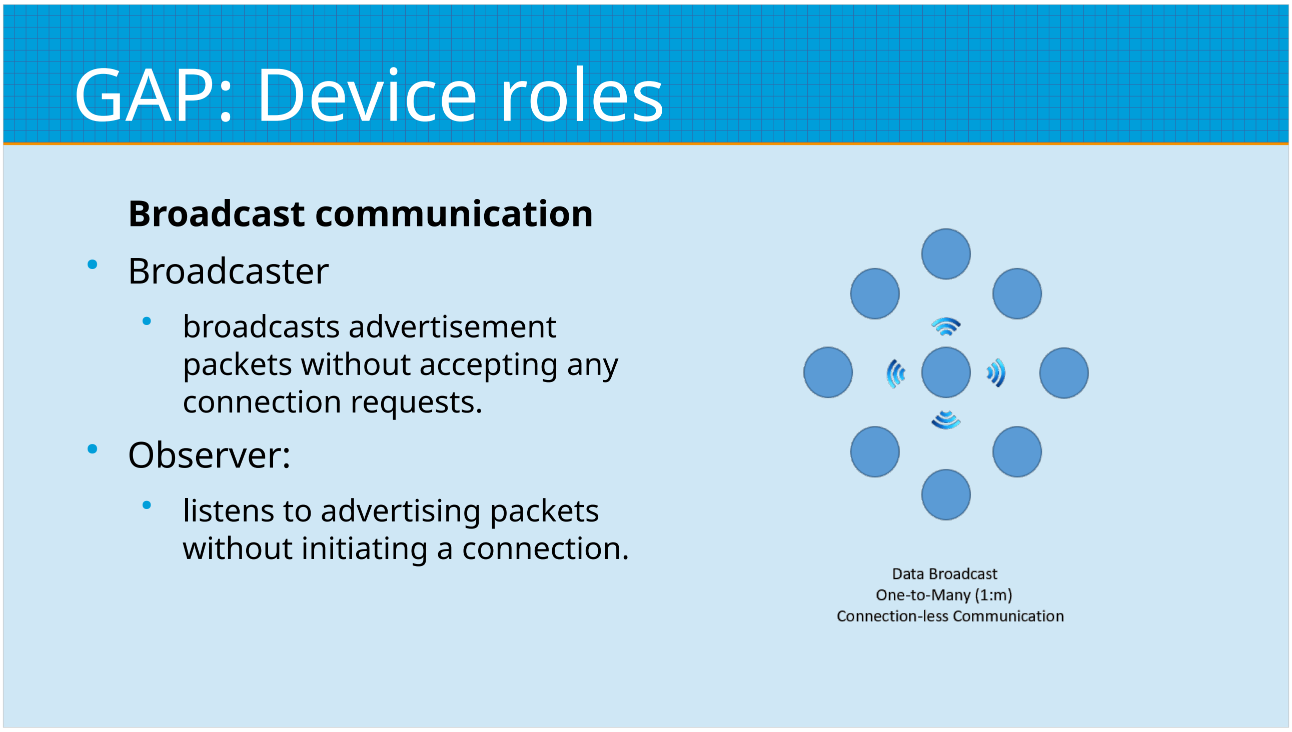
Connection-oriented comm.

- Central
  - scans and initiates connections with peripherals.
- Peripheral
  - advertises and accepts connections from centrals.

Peripheral Device
Central Device
Peripheral Device

https://docs.arduino.cc/learn/communication/bluetooth/

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



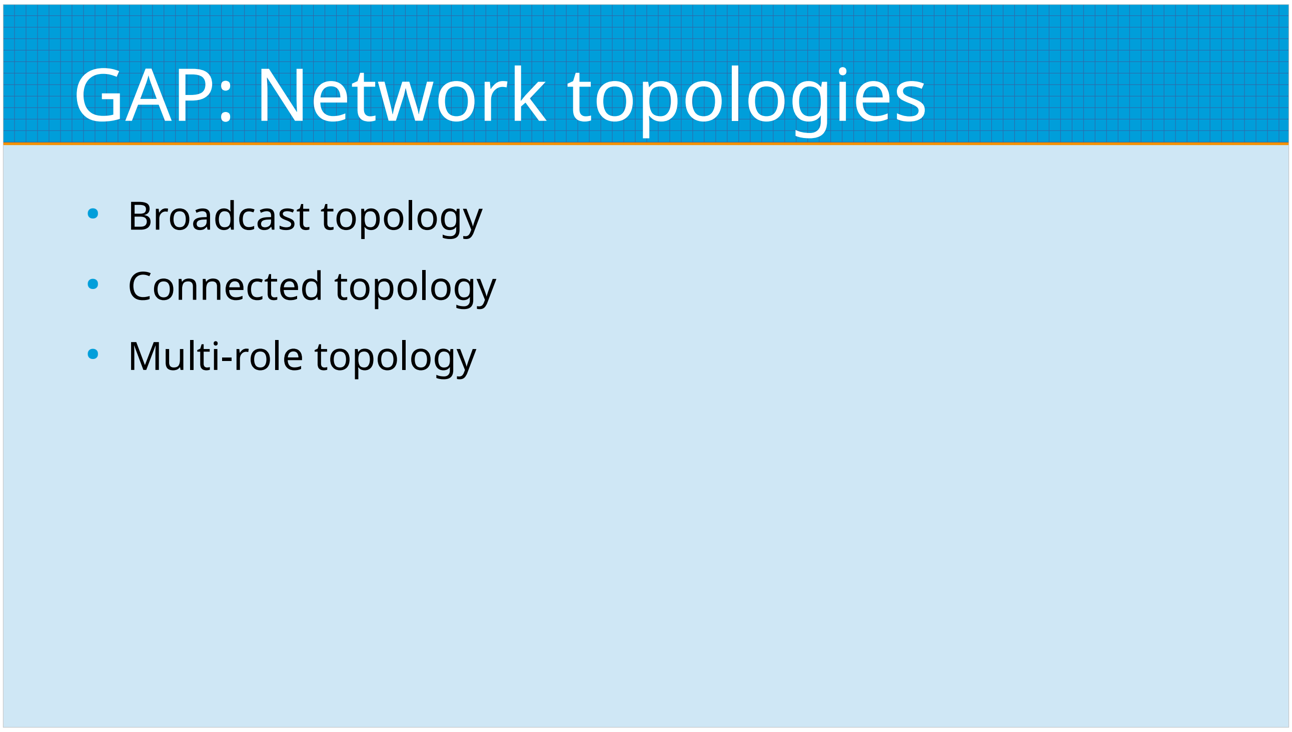
GAP: Device roles

Broadcast communication

- Broadcaster
  - broadcasts advertisement packets without accepting any connection requests.
- Observer:
  - listens to advertising packets without initiating a connection.

Data Broadcast
One-to-Many (1:m)
Connection-less Communication

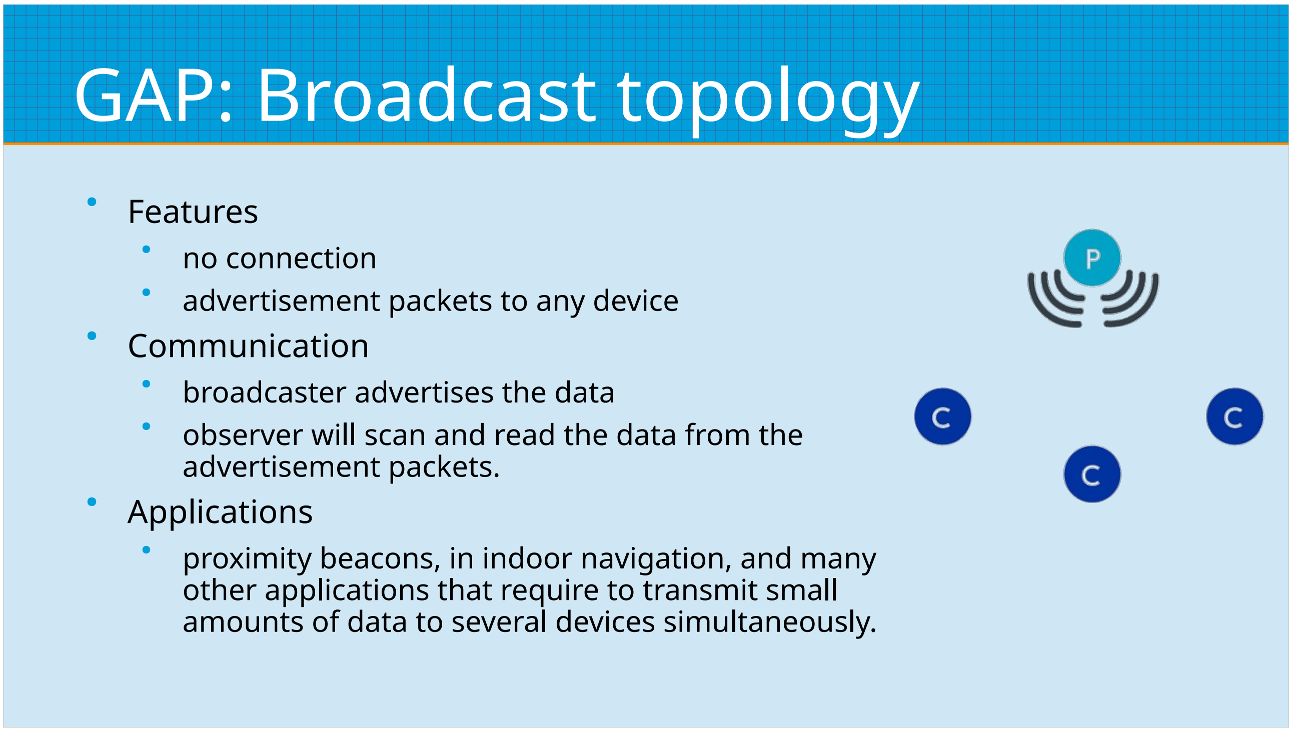
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



GAP: Network topologies

- Broadcast topology
- Connected topology
- Multi-role topology

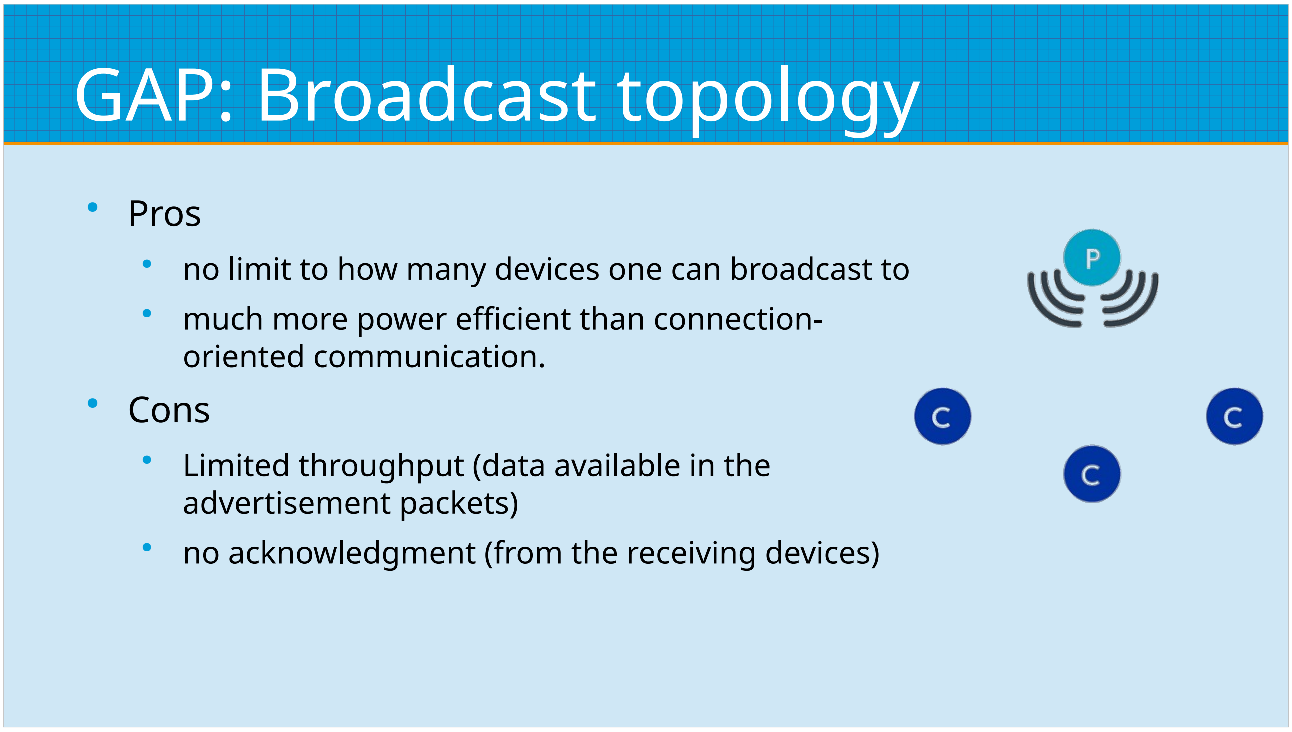
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



GAP: Broadcast topology

- Features
  - no connection
  - advertisement packets to any device
- Communication
  - broadcaster advertises the data
  - observer will scan and read the data from the advertisement packets.
- Applications
  - proximity beacons, in indoor navigation, and many other applications that require to transmit small amounts of data to several devices simultaneously.

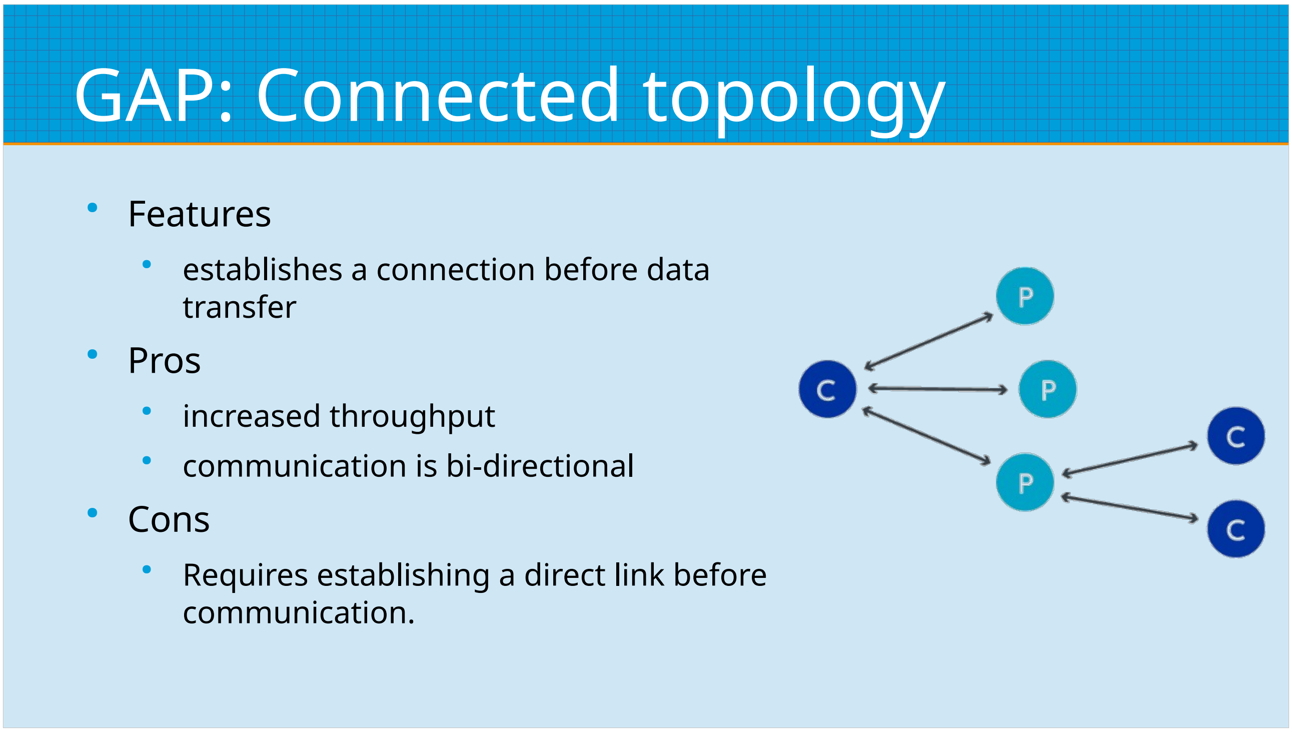
- Broadcast topology
  - data transfer happens without the devices ever establishing a connection.
  - advertisement packets to broadcast the data to any device
  - peripheral (more specifically a broadcaster) advertises the data, and
  - central (more specifically an observer) will scan and read the data from the advertisement packets.
- Applications
  - proximity beacons, in indoor navigation, and many other applications that require a low-power device to transmit small amounts of data to several devices simultaneously.
- Pro and cons
  - Advantage
    - no limit to how many devices one can broadcast to.
    - much more power efficient than connection-oriented communication.
  - Disadvantages
    - Limited throughput (data available in the advertisement packets)
    - no acknowledgment (from the receiving devices)



GAP: Broadcast topology

- Pros
  - no limit to how many devices one can broadcast to
  - much more power efficient than connection-oriented communication.
- Cons
  - Limited throughput (data available in the advertisement packets)
  - no acknowledgment (from the receiving devices)

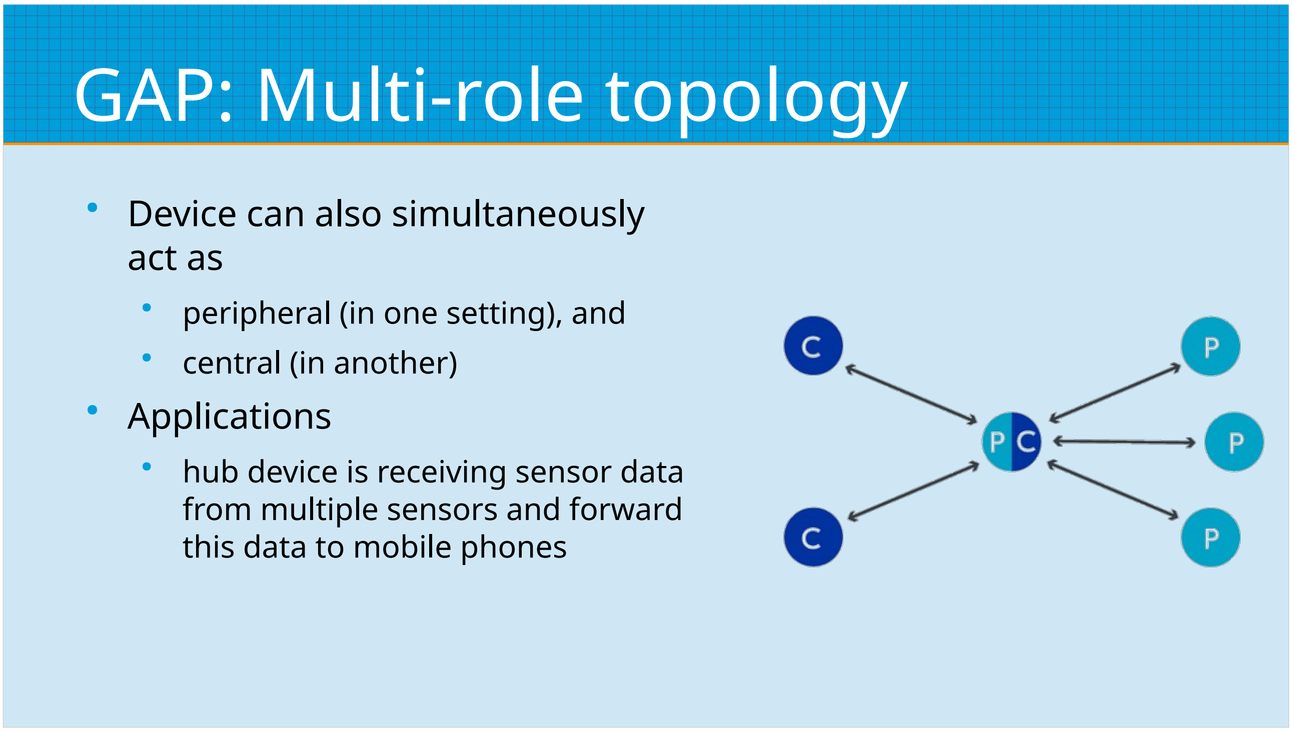
- Broadcast topology
  - data transfer happens without the devices ever establishing a connection.
  - advertisement packets to broadcast the data to any device
  - peripheral (more specifically a broadcaster) advertises the data, and
  - central (more specifically an observer) will scan and read the data from the advertisement packets.
- Applications
  - proximity beacons, in indoor navigation, and many other applications that require a low-



GAP: Connected topology

- Features
  - establishes a connection before data transfer
- Pros
  - increased throughput
  - communication is bi-directional
- Cons
  - Requires establishing a direct link before communication.

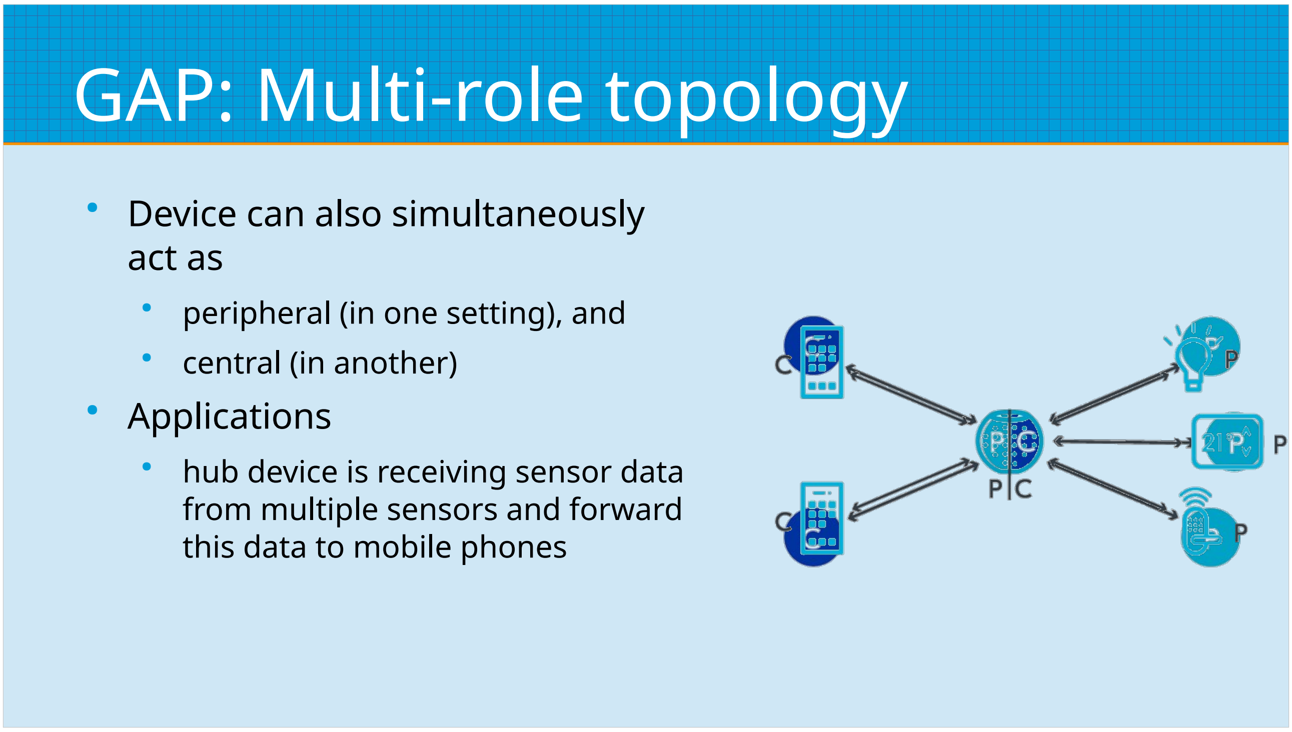
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



GAP: Multi-role topology

- Device can also simultaneously act as
  - peripheral (in one setting), and
  - central (in another)
- Applications
  - hub device is receiving sensor data from multiple sensors and forward this data to mobile phones

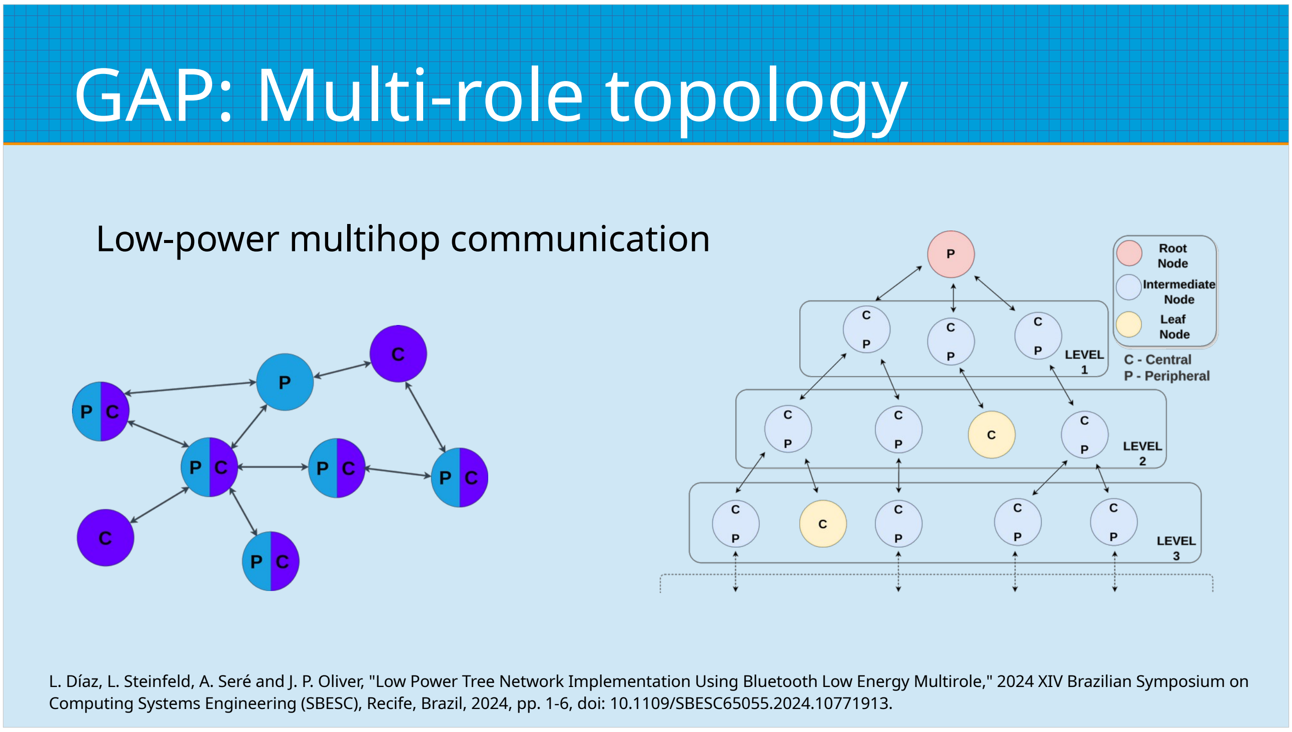
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.



GAP: Multi-role topology

- Device can also simultaneously act as
  - peripheral (in one setting), and
  - central (in another)
- Applications
  - hub device is receiving sensor data from multiple sensors and forward this data to mobile phones

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.

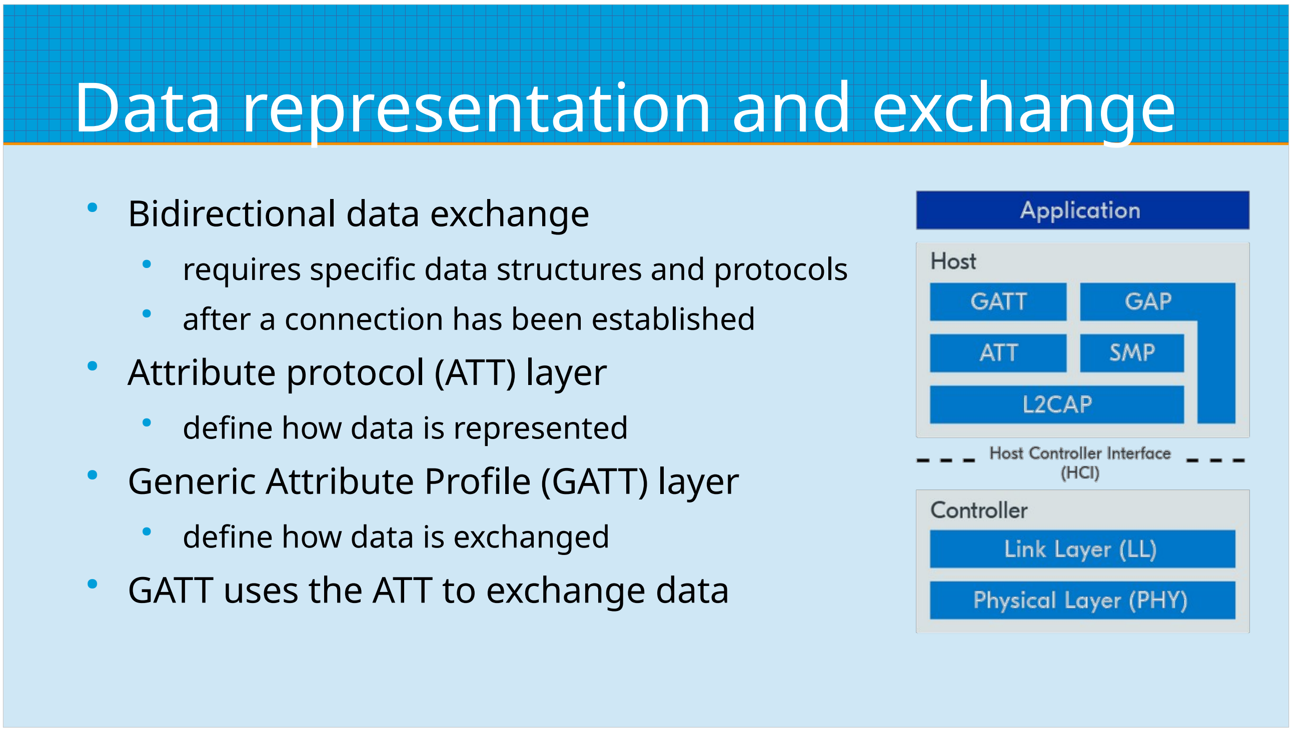


GAP: Multi-role topology

Low-power multihop communication

L. Díaz, L. Steinfeld, A. Seré and J. P. Oliver, "Low Power Tree Network Implementation Using Bluetooth Low Energy Multirole," 2024 XIV Brazilian Symposium on Computing Systems Engineering (SBESC), Recife, Brazil, 2024, pp. 1-6, doi: 10.1109/SBESC65055.2024.10771913.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.

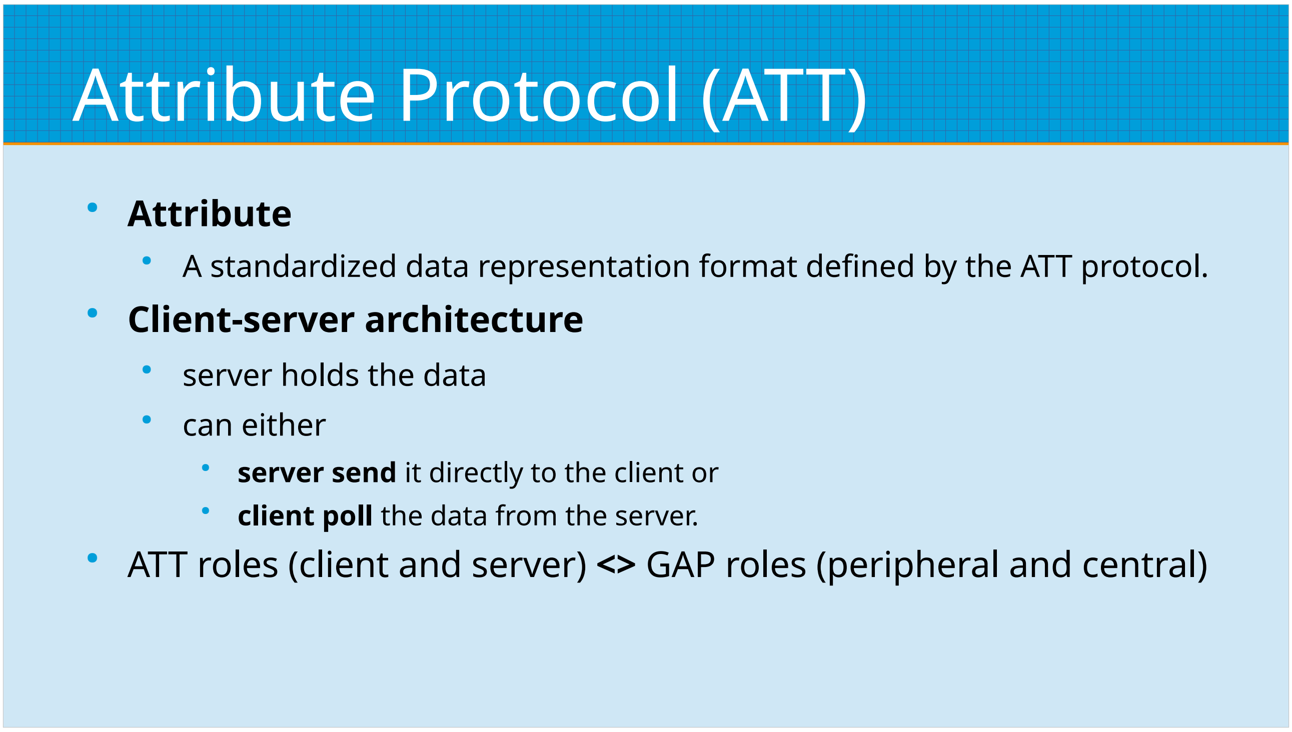


Data representation and exchange

- Bidirectional data exchange
  - requires specific data structures and protocols
  - after a connection has been established
- Attribute protocol (ATT) layer
  - define how data is represented
- Generic Attribute Profile (GATT) layer
  - define how data is exchanged
- GATT uses the ATT to exchange data

Application
Host
GATT
GAP
ATT
SMP
L2CAP
Host Controller Interface (HCI)
Controller
Link Layer (LL)
Physical Layer (PHY)

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



Attribute Protocol (ATT)

- **Attribute**
  - A standardized data representation format defined by the ATT protocol.
- **Client-server architecture**
  - server holds the data
  - can either
    - **server send** it directly to the client or
    - **client poll** the data from the server.
- ATT roles (client and server) **<>** GAP roles (peripheral and central)

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

Generic Attribute Profile (GATT)

- GATT: organize data into a hierarchical stricture

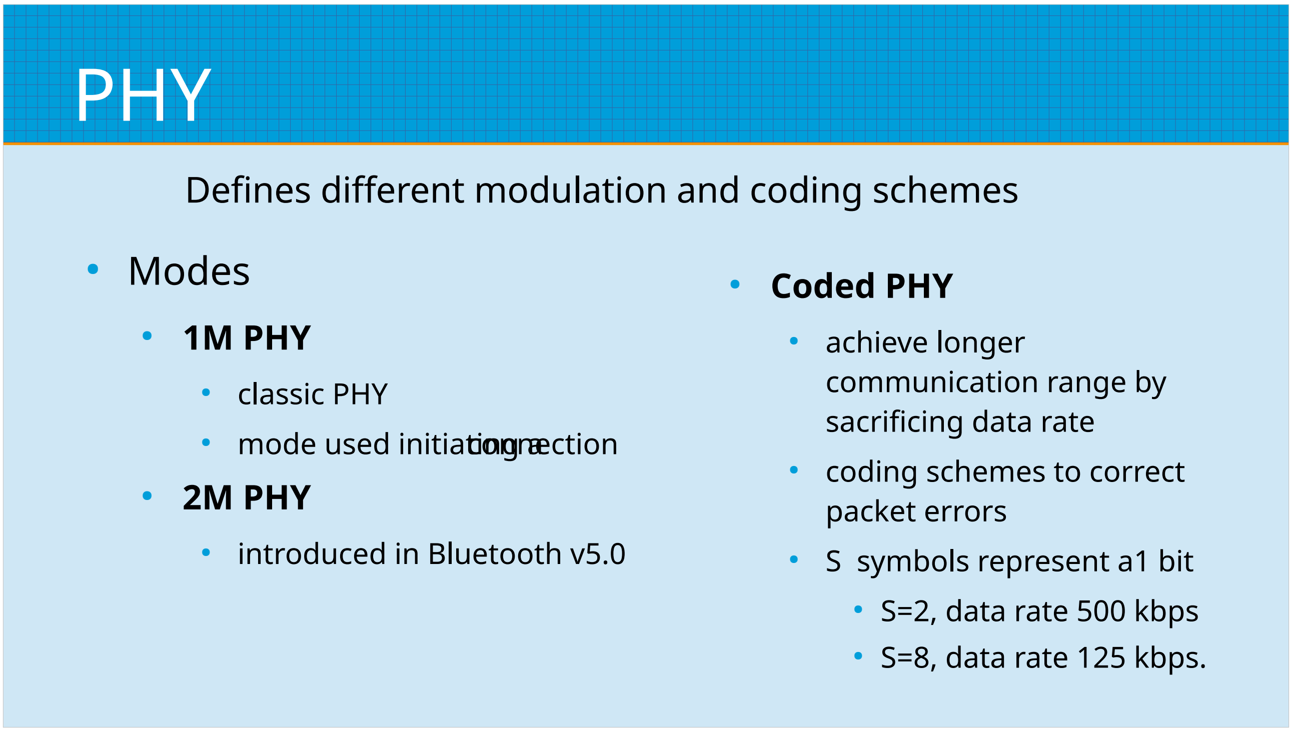
- Profiles
  - Collections of services that address a specific use case (e.g., Heart Rate Profile).
- Services
  - Groups of related characteristics that provide specific functionality (e.g., Battery Service).
- Characteristics
  - Individual pieces of data or functionality within a service (e.g., Battery Level).
- Attributes
  - The smallest unit of data, which can be a characteristic or a descriptor

Generic Attribute Profile (GATT)

Example

- Profile
  - Heart Rate Profile
- Services
  - Heart Rate Service
- Characteristics
  - Heart Rate Measurement Characteristic
  - Body Sensor Location Characteristic
- Attributes
  - Heart Rate Value (UINT8)
  - RR-Interval Value

https://www.bluetooth.com/specifications/specs/heart-rate-profile-1-0/



PHY

Defines different modulation and coding schemes

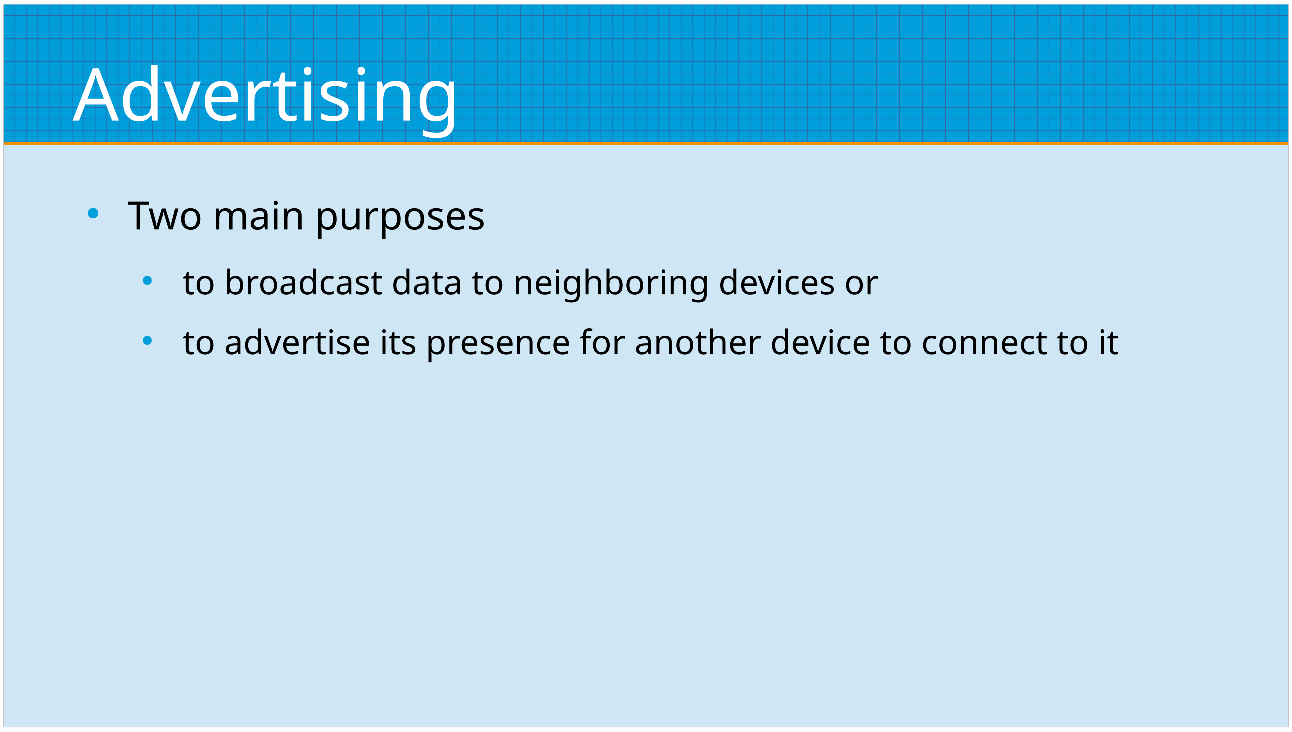
- Modes
  - **1M PHY**
    - classic PHY
    - mode used initiating connection
  - **2M PHY**
    - introduced in Bluetooth v5.0

- **Coded PHY**
  - achieve longer communication range by sacrificing data rate
  - coding schemes to correct packet errors
  - S symbols represent a1 bit
    - S=2, data rate 500 kbps
    - S=8, data rate 125 kbps.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly with the application to handle device discovery and connection-related services.
- **Controller**
- The Bluetooth LE controller is comprised of the following layers:
- Physical Layer (PHY): determines how the actual data is modulated onto the radio waves, and how it is transmitted and received.
- Link Layer (LL): manages the state of the radio, defined as one of the following – standby, advertising, scanning, initiating, connection.

Agenda

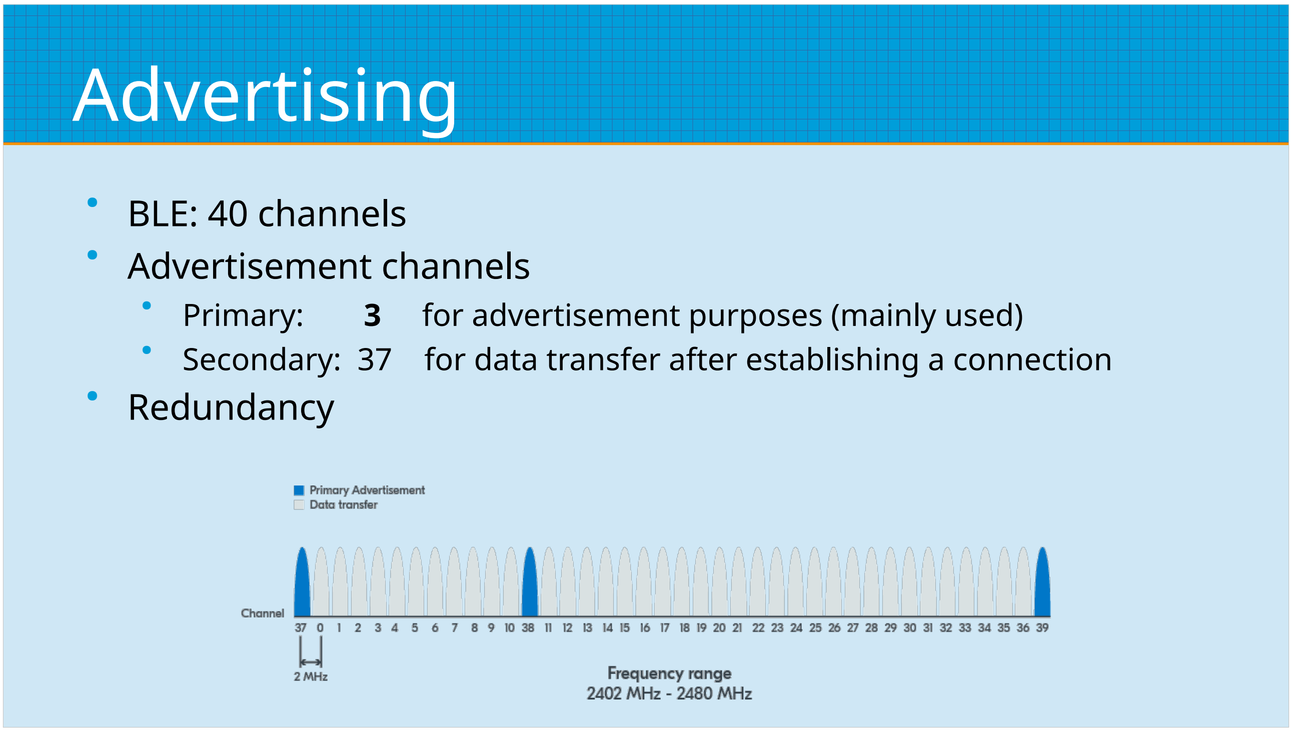
- Introduction
  - Protocol stack
  - Main concepts
- Advertising
- Connections
- Data exchange
- Security



Advertising

- Two main purposes
  - to broadcast data to neighboring devices or
  - to advertise its presence for another device to connect to it

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

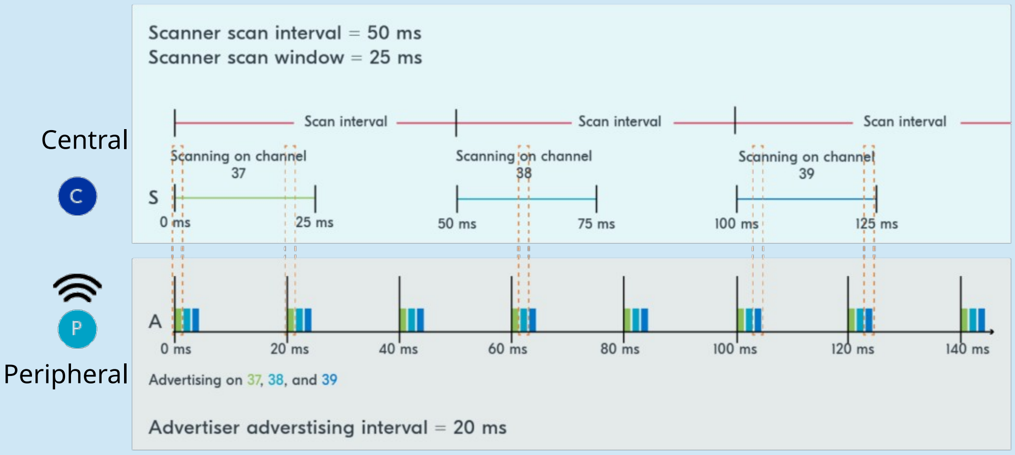


Advertising

- BLE: 40 channels
- Advertisement channels
  - Primary: **3** for advertisement purposes (mainly used)
  - Secondary: 37 for data transfer after establishing a connection
- Redundancy

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

Scan interval and scan window

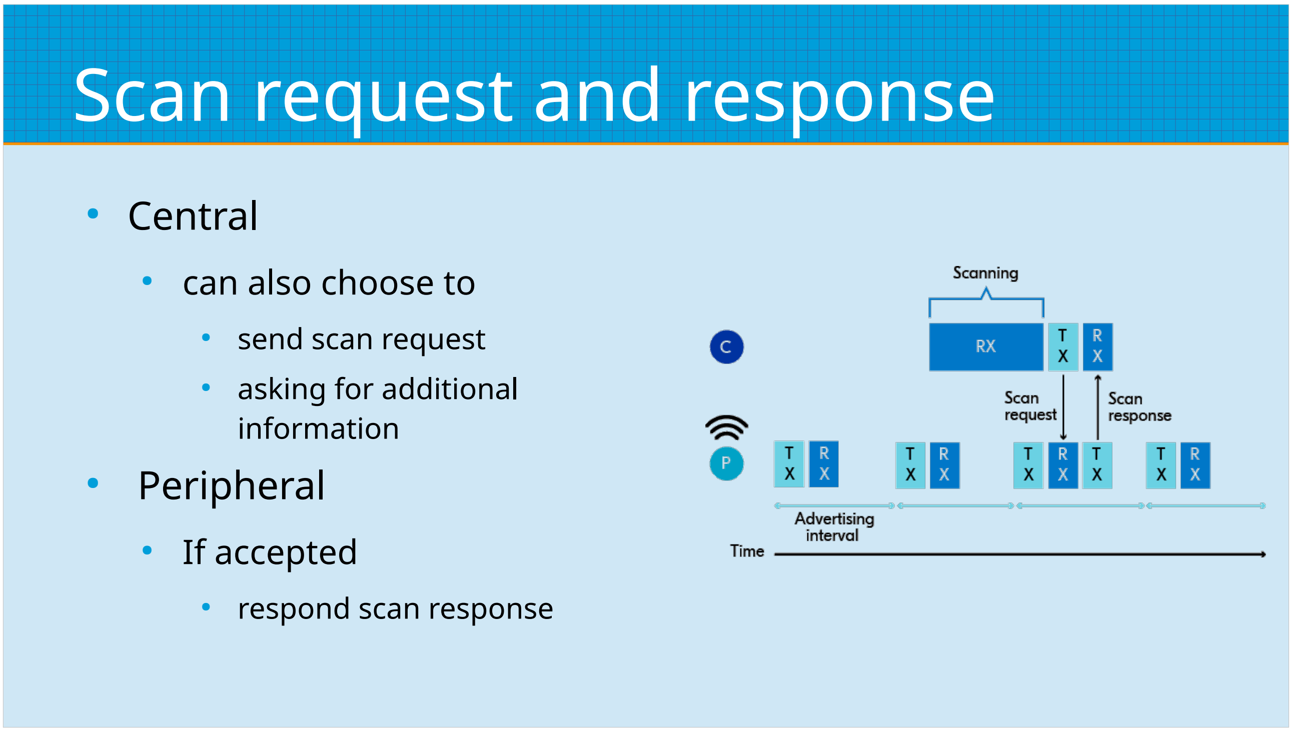


Trade-off

- discovery times
- Power cons.

Both range from 2.5 ms to 10.24 seconds with a step increase of 0.625 ms.

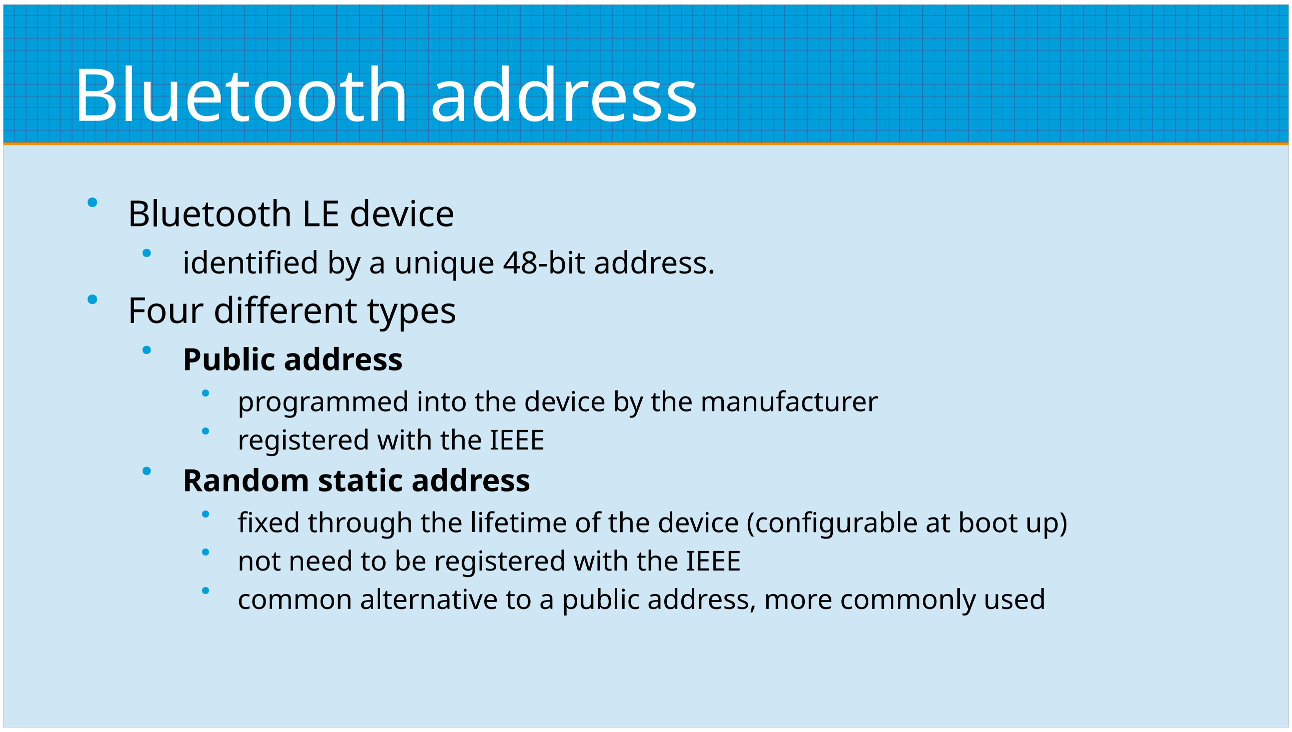
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



Scan request and response

- Central
  - can also choose to
    - send scan request
    - asking for additional information
- Peripheral
  - If accepted
    - respond scan response

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



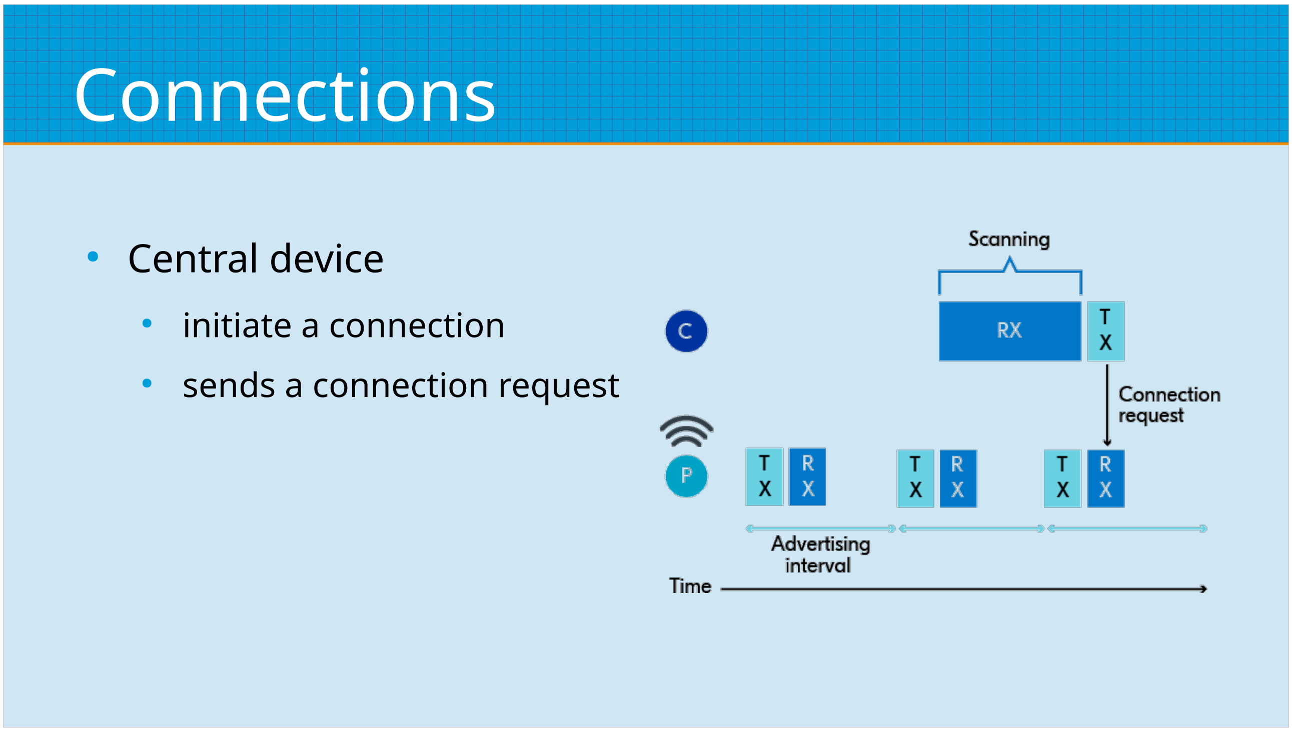
Bluetooth address

- Bluetooth LE device
  - identified by a unique 48-bit address.
- Four different types
  - **Public address**
    - programmed into the device by the manufacturer
    - registered with the IEEE
  - **Random static address**
    - fixed through the lifetime of the device (configurable at boot up)
    - not need to be registered with the IEEE
    - common alternative to a public address, more commonly used

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

Agenda

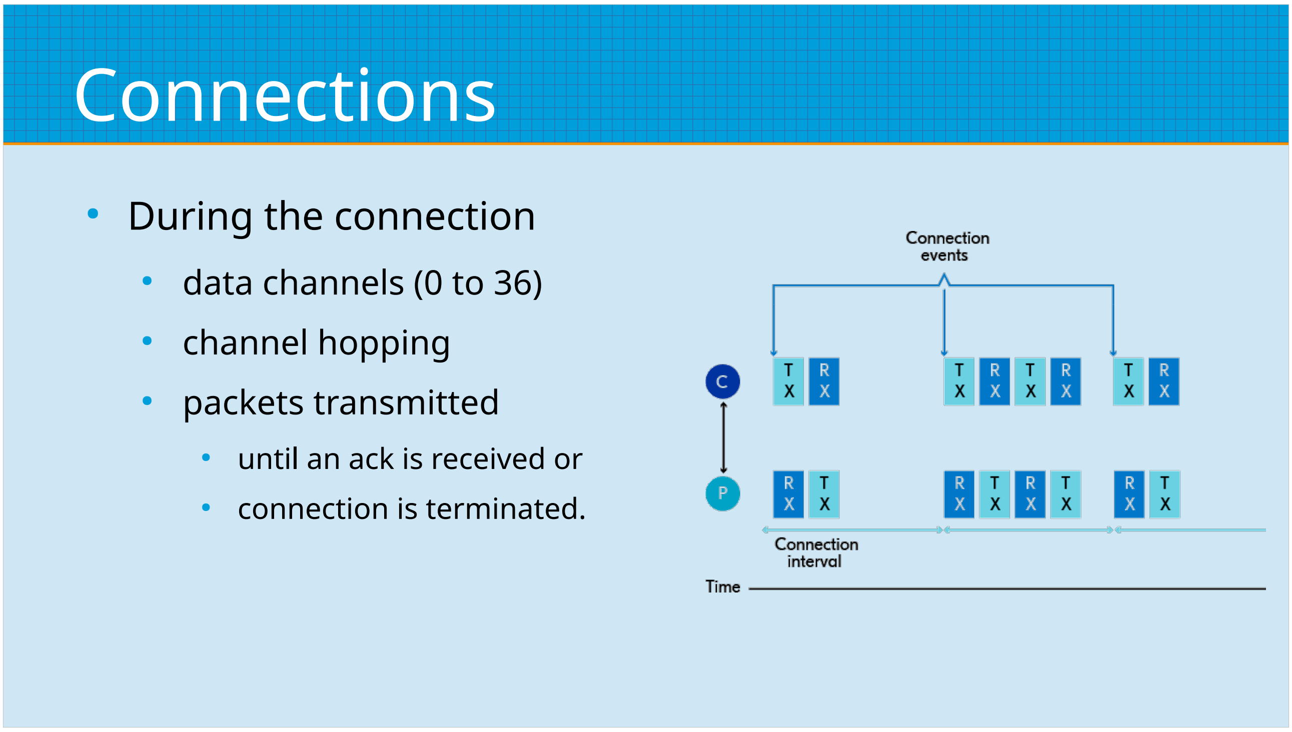
- Introduction
  - Protocol stack
  - Main concepts
- Advertising
- Connections
- Data exchange
- Security



Connections

- Central device
  - initiate a connection
  - sends a connection request

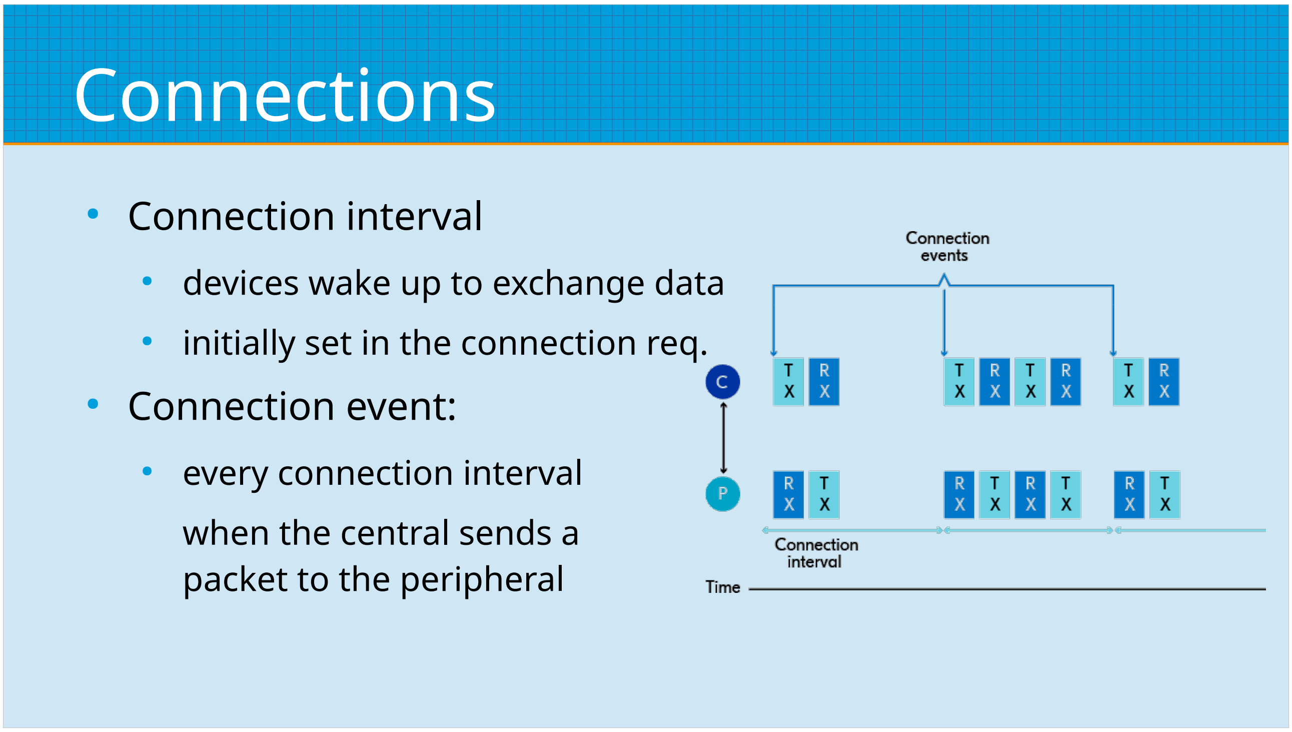
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



Connections

- During the connection
  - data channels (0 to 36)
  - channel hopping
  - packets transmitted
    - until an ack is received or
    - connection is terminated.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

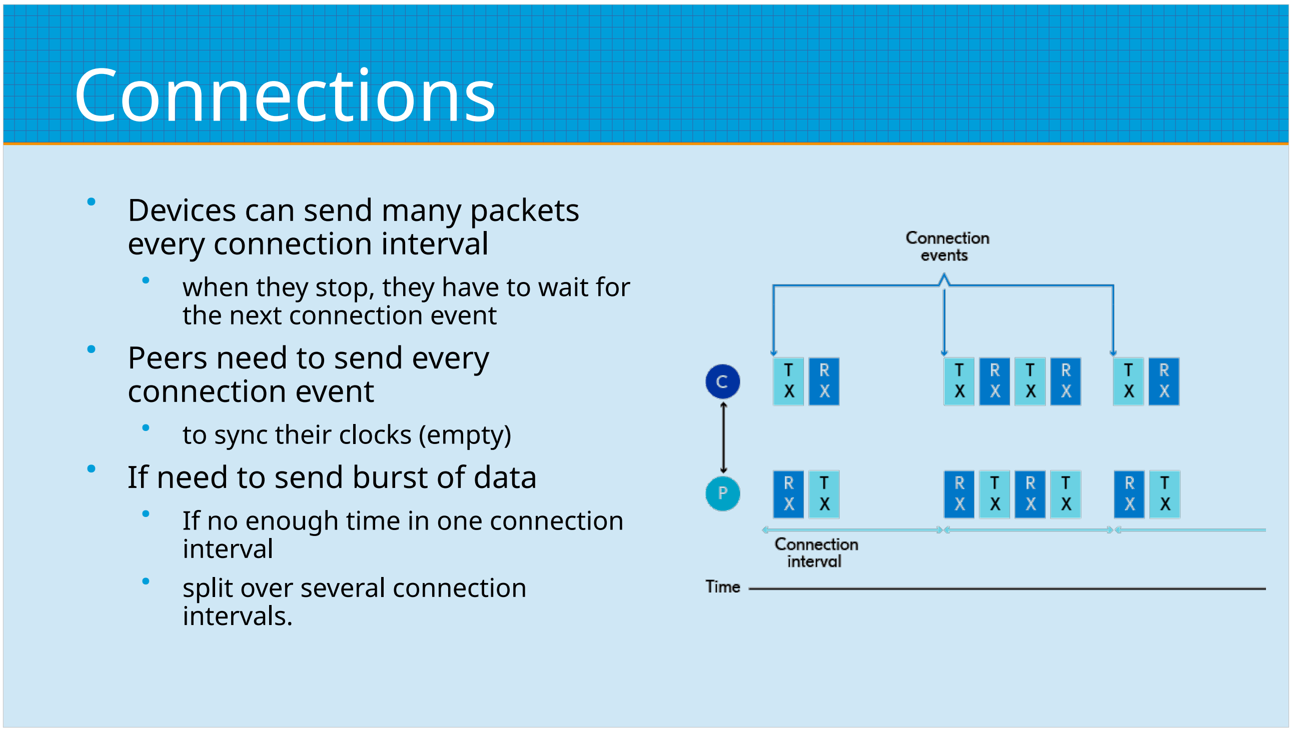


Connections

- Connection interval
  - devices wake up to exchange data
  - initially set in the connection req.
- Connection event:
  - every connection interval

    when the central sends a packet to the peripheral

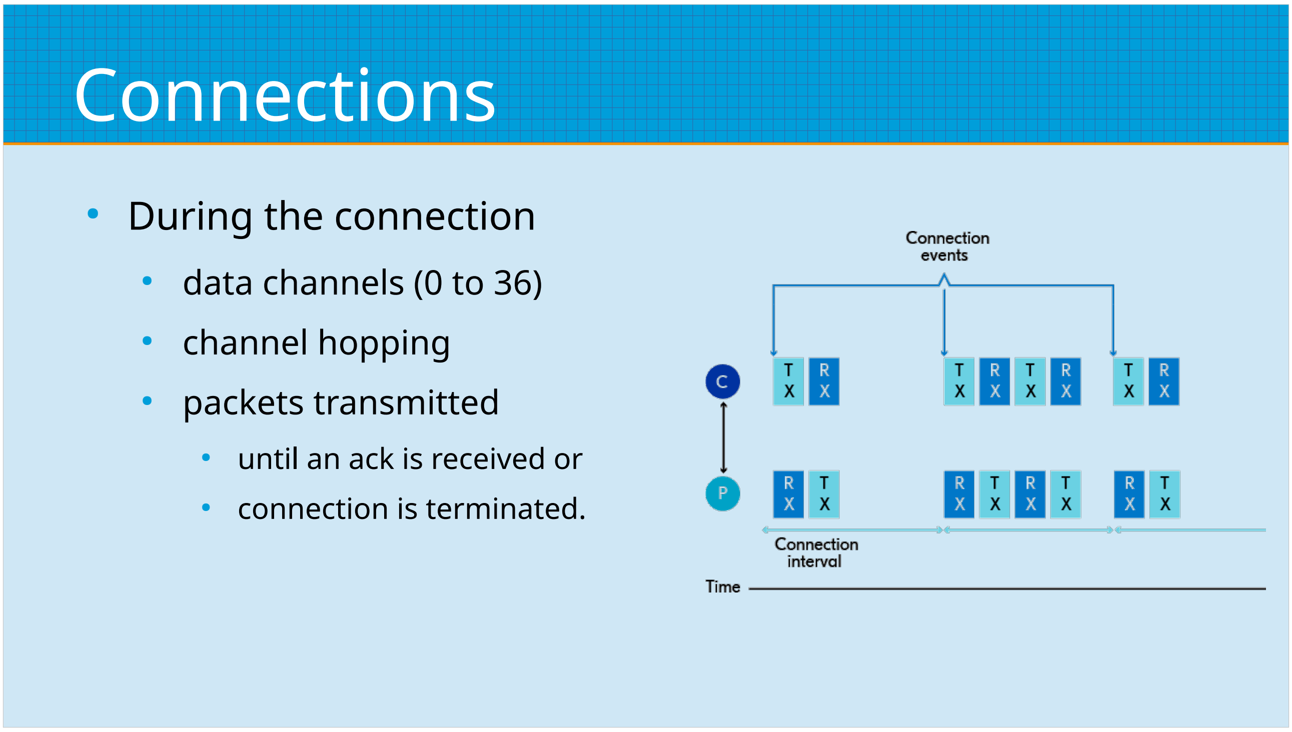
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



Connections

- Devices can send many packets every connection interval
  - when they stop, they have to wait for the next connection event
- Peers need to send every connection event
  - to sync their clocks (empty)
- If need to send burst of data
  - If no enough time in one connection interval
  - split over several connection intervals.

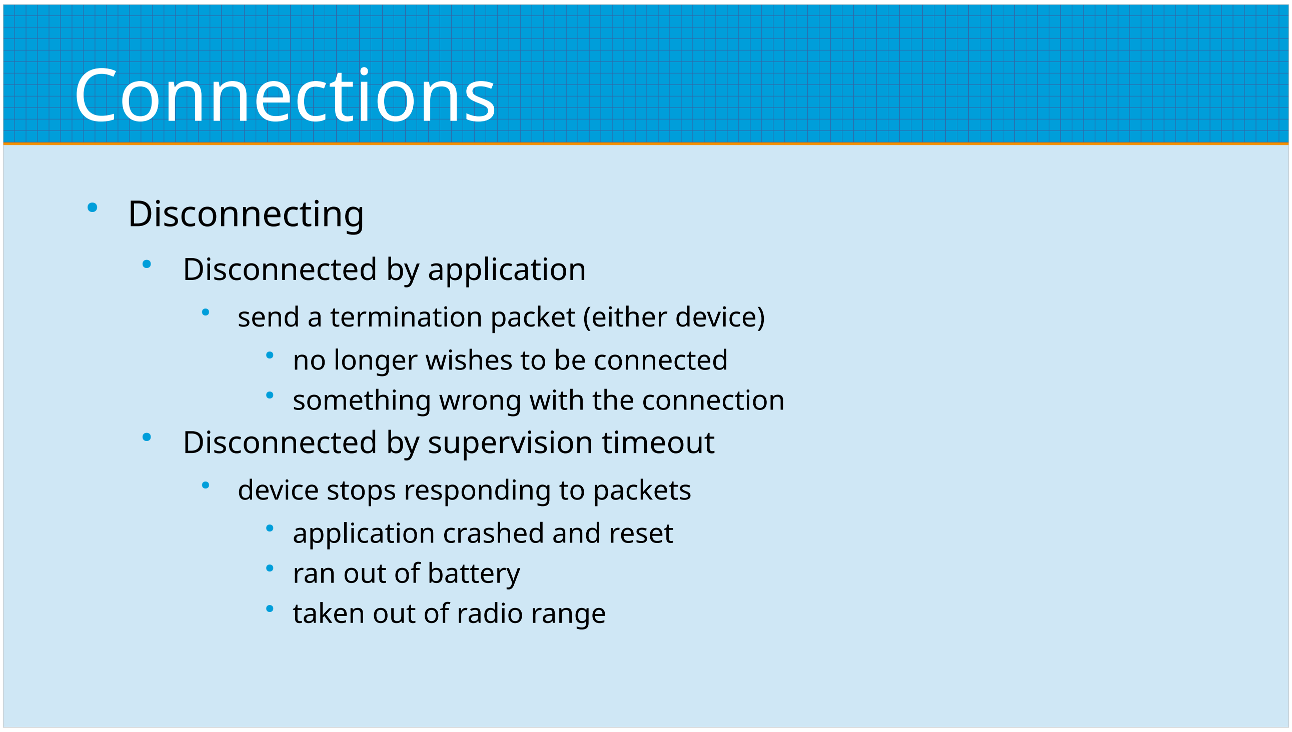
- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



Connections

- During the connection
  - data channels (0 to 36)
  - channel hopping
  - packets transmitted
    - until an ack is received or
    - connection is terminated.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



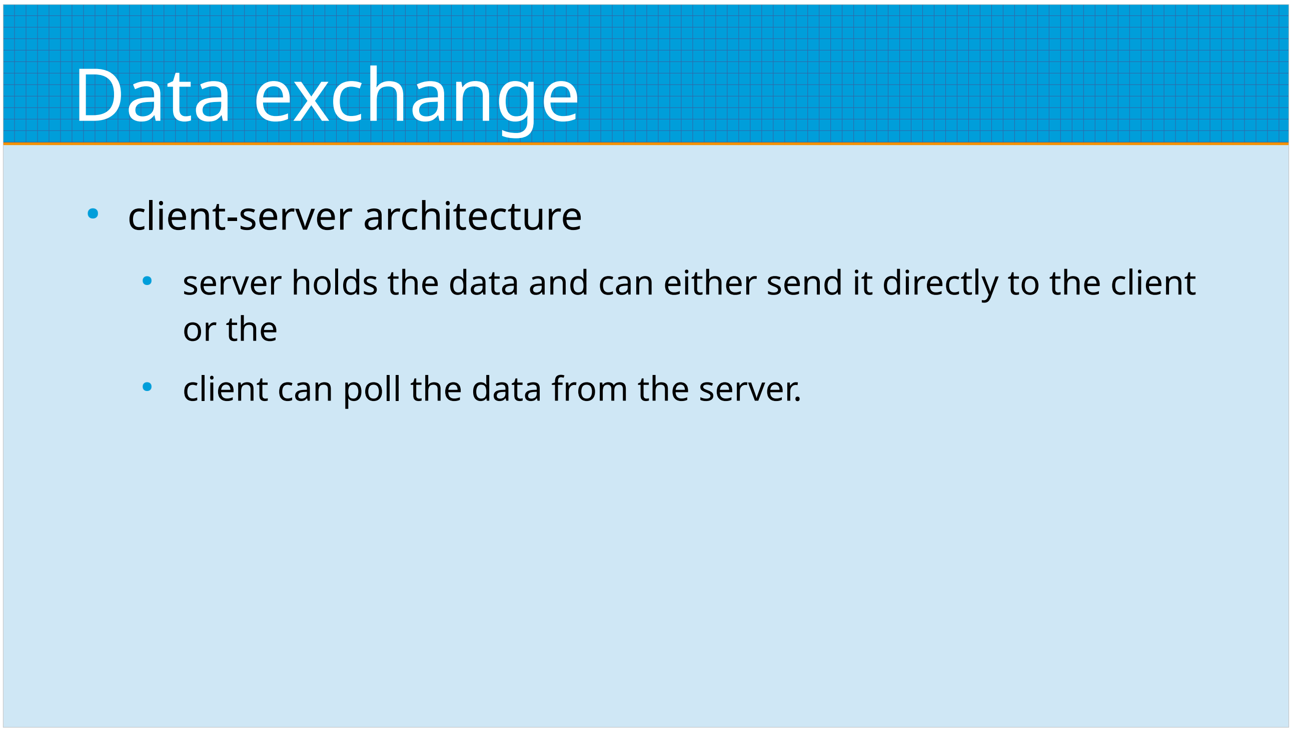
Connections

- Disconnecting
  - Disconnected by application
    - send a termination packet (either device)
      - no longer wishes to be connected
      - something wrong with the connection
  - Disconnected by supervision timeout
    - device stops responding to packets
      - application crashed and reset
      - ran out of battery
      - taken out of radio range

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

Agenda

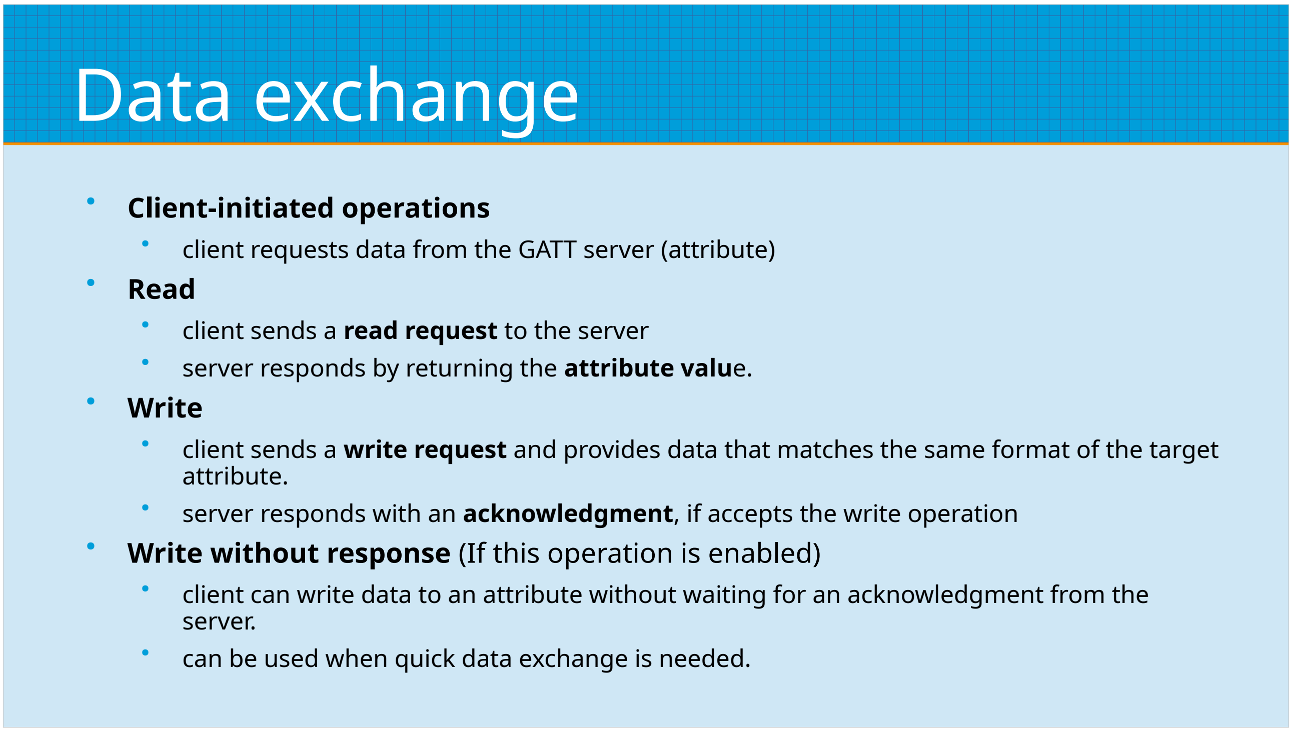
- Introduction
  - Protocol stack
  - Main concepts
- Advertising
- Connections
- Data exchange
- Security



Data exchange

- client-server architecture
  - server holds the data and can either send it directly to the client or the
  - client can poll the data from the server.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly



Data exchange

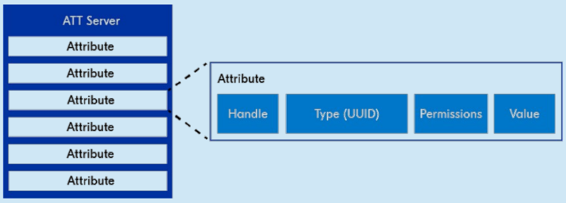
- **Client-initiated operations**
  - client requests data from the GATT server (attribute)
- **Read**
  - client sends a **read request** to the server
  - server responds by returning the **attribute valu**e.
- **Write**
  - client sends a **write request** and provides data that matches the same format of the target attribute.
  - server responds with an **acknowledgment**, if accepts the write operation
- **Write without response** (If this operation is enabled)
  - client can write data to an attribute without waiting for an acknowledgment from the server.
  - can be used when quick data exchange is needed.

- **Host**
- The Bluetooth LE host consists of the following layers:
- Logical Link Control & Adaptation Protocol (L2CAP): provides data encapsulation services to the upper layers.
- Security Manager Protocol (SMP): defines and provides methods for secure communication.
- Attribute Protocol (ATT): allows a device to expose certain pieces of data to another device.
- Generic Attribute Profile (GATT): defines the necessary sub-procedures for using the ATT layer.
- Generic Access Profile (GAP): interfaces directly

Data exchange

- **Server-initiated operations**
  - server sends information directly to the client
  - client is **required to enable** by subscribing to the characteristic and enabling either notifications or indications.
- **Notify**
  - push the value of a certain attribute to the client
  - can be used to update the client about a certain sensor reading
  - Notifications require no acknowledgment back from the client.
- **Indicate**
  - push the attribute value directly to the client.
  - an acknowledgment from the client is required.
  - can only send one Indication per connection interval (slower than notifications)

Services and characteristics

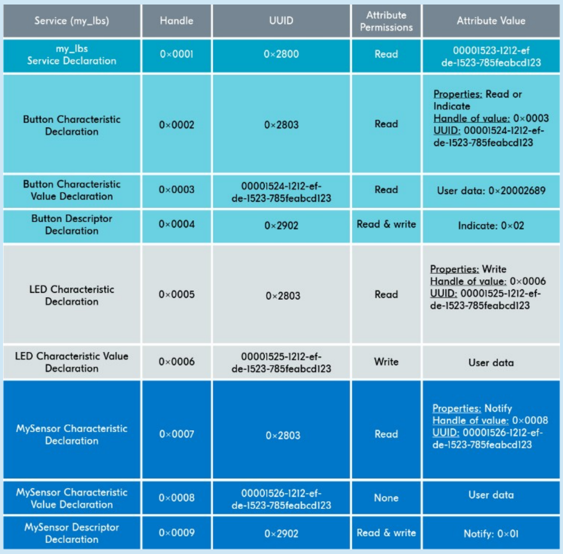


- Handle:
  - A 16-bit unique index in the attribute table
- Type (UUID)
  - Universally unique ID (UUID)
  - attribute type.
- Permissions:
  - security level required (encryption and/or authorization)
  - indicating whether it’s a readable and/or writeable attribute.
- Value:
  - actual user data (ex: sensor reading), any data type: integer even a string.
  - Metadata: information about another attribute

Universally unique ID (UUID)

- UUID: identify attributes
- two types.
  - SIG-defined 16-bit UUID
    - energy and memory efficient
  - 128-bit UUID: vendor-specific UUID.
    - to cover all vendors, users, and use cases
- Examples
  - SIG-defined
    - Heart rate service, UUID 0x180D
    - Heart Rate Measurement characteristic, UUID 0x2A37
  - 128-bit UUID
    - 4A98-xxxx-1CC4-E7C1-C757-F1267DD021E8

Attribute table



Service (my_lbs)	Handle	UUID	Attribute Permissions	Attribute Value
my_lbs Service Declaration	0×0001	0×2800	Read	00001523-1212-ef de-1523-785feabcd123
Button Characteristic Declaration	0×0002	0×2803	Read	Properties: Read or Indicate Handle of value: 0×0003 UUID: 00001524-1212-ef-de-1523-785feabcd123
Button Characteristic Value Declaration	0×0003	00001524-1212-ef-de-1523-785feabcd123	Read	User data: 0×20002689
Button Descriptor Declaration	0×0004	0×2902	Read & write	Indicate: 0×02
LED Characteristic Declaration	0×0005	0×2803	Read	Properties: Write Handle of value: 0×0006 UUID: 00001525-1212-ef-de-1523-785feabcd123
LED Characteristic Value Declaration	0×0006	00001525-1212-ef-de-1523-785feabcd123	Write	User data
MySensor Characteristic Declaration	0×0007	0×2803	Read	Properties: Notify Handle of value: 0×0008 UUID: 00001526-1212-ef-de-1523-785feabcd123
MySensor Characteristic Value Declaration	0×0008	00001526-1212-ef-de-1523-785feabcd123	None	User data
MySensor Descriptor Declaration	0×0009	0×2902	Read & write	Notify: 0×01

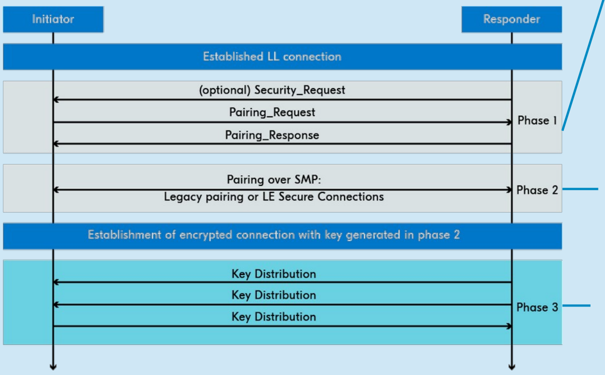
Security

- Four security levels (mode 1)
  - Level 1:
    - No security (open text, meaning no authentication and no encryption)
  - Level 2:
    - Encryption with unauthenticated pairing
  - Level 3:
    - Authenticated pairing with encryption
  - Level 4:
    - Authenticated LE Secure Connections pairing with encryption

Security

- Pairing:
  - The process of generating, distributing, and authenticating keys for encryption purposes.
- Bonding:
  - The process of pairing followed by distribution of keys used to encrypt the link in future reconnections.

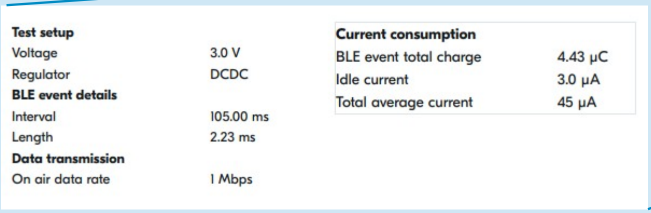
Security


Initiator
Responder
Established LL connection
(optional) Security_Request
Pairing_Request
Pairing_Response
Phase 1
Pairing over SMP:
Legacy pairing or LE Secure Connections
Phase 2
Establishment of encrypted connection with key generated in phase 2
Key Distribution
Key Distribution
Key Distribution
Phase 3

- Phase 1: Initiate pairing
  - peers exchange I/O capabilities
    - DisplayOnly
    - DisplayYesNo
    - KeyboardOnly
    - NoInputNoOutput
    - KeyboardDisplay
- Phase 2: Perform pairing
  - generate a public-private key pair
  - verify the authenticity of the peer device (method depends I/O capabilities) and generate the LTK
- Phase 3: Key distribution
  - LTK is is not directly distributed, but rather derived (in LE Secure Connections)

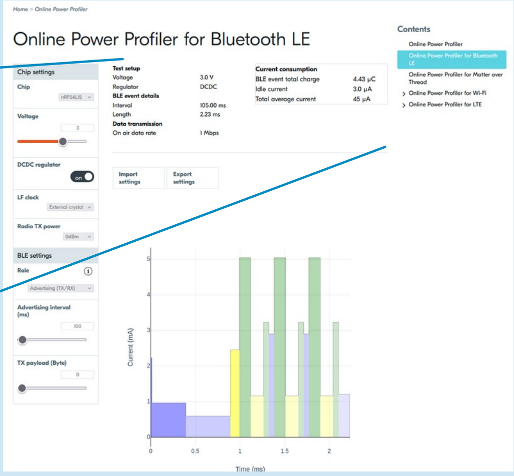
Tools

- Online Power Profiler for Bluetooth LE



Test setup	
Voltage	3.0 V
Regulator	DCDC
BLE event details	
Interval	105.00 ms
Length	2.23 ms
Data transmission	
On air data rate	1 Mbps

Current consumption	
BLE event total charge	4.43 µC
Idle current	3.0 µA
Total average current	45 µA



Home > Online Power Profiler

Online Power Profiler for Bluetooth LE

Chip settings

Chip: nRF54L15

Voltage: 3

DCDC regulator: on

LF clock: External crystal

Radio TX power: 0dBm

BLE settings

Role: Advertising (TX/RX)

Advertising interval (ms): 100

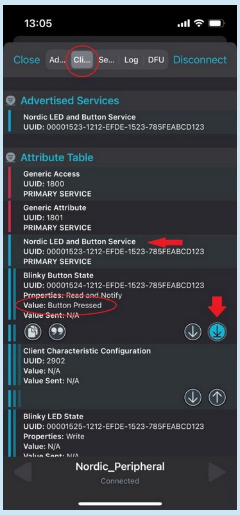
TX payload (Byte): 0

Test setup	
Voltage	3.0 V
Regulator	DCDC
BLE event details	
Interval	105.00 ms
Length	2.23 ms
Data transmission	
On air data rate	1 Mbps

Current consumption	
BLE event total charge	4.43 µC
Idle current	3.0 µA
Total average current	45 µA

Import settings
Export settings
Current (mA)
0
1
2
3
4
5
Time (ms)
0
0.5
1
1.5
2
Contents
Online Power Profiler
Online Power Profiler for Bluetooth LE
Online Power Profiler for Matter over Thread
Online Power Profiler for Wi-Fi
Online Power Profiler for LTE

Examples



Advertised Services

Nordic LED and Button Service
UUID: 00001523-1212-EFDE-1523-785FEABCD123

Attribute Table

Generic Access
UUID: 1800
PRIMARY SERVICE

Generic Attribute
UUID: 1801
PRIMARY SERVICE

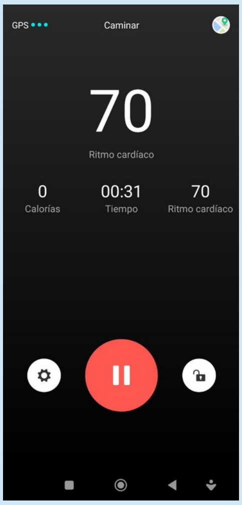
Nordic LED and Button Service
UUID: 00001523-1212-EFDE-1523-785FEABCD123
PRIMARY SERVICE

Blinky Button State
UUID: 00001524-1212-EFDE-1523-785FEABCD123
Properties: Read and Notify
Value: Button Pressed
Value Sent: N/A

Client Characteristic Configuration
UUID: 2902
Value: N/A
Value Sent: N/A

Blinky LED State
UUID: 00001525-1212-EFDE-1523-785FEABCD123
Properties: Write
Value: N/A
Value Sent: N/A

Nordic_Peripheral
Connected



References

- Bluetooth Low Energy Fundamentals
  - Nordic Developer Academy
  - https://academy.nordicsemi.com/courses/bluetooth-low-energy-fundamentals
- Woolley, Martin. "The bluetooth low energy primer." Bluetooth Blog 15 (2022): 2022