Introduction to Bluetooth Low Energy

Module syllabus

- Bluetooth overview
- Bluetooth key versions
- Bluetooth Low Energy (BLE) Protocol
- BLE architecture

Bluetooth overview

- Bluetooth is a wireless technology standard
  - Used for short distance data exchanging, such as Personal Area Networks
  - RF from 2.4 to 2.485 GHz
  - Invented by Ericsson, a telecom vendor, in 1994
  - Now managed by the Bluetooth Special Interest Group
  - 16,000+ SIG member companies
  - Frequency hopping spread spectrum (FHSS)
  - Billions of products shipped

Bluetooth key versions

Version	Year published	Over the air data rate	Application data transfer rate	Notes
Bluetooth 1.1	2002	1 Mbit/s	Up to 0.7 Mbit/s	
Bluetooth 2.0 + Enhanced Data Rate (EDR)	2004	3 Mbit/s	Up to 2.1 Mbit/s	
Bluetooth 3.0 + High Speed (HS)	2009	24 Mbit/s	~24 Mbit/s	
Bluetooth 4.0, also called Bluetooth Smart	2010	24 Mbit/s	0.27 Mbit/s	Includes Classic Bluetooth, Bluetooth high speed and Bluetooth low energy protocols
Bluetooth 4.2	2014	24 Mbit/s	0.27 Mbit/s	Introduced some key features for IoT

Terminology

Term	Introduced	Features
BR (Basic Rate)	1.1 (2002)	1 Mbit/s
EDR (Enhanced Data Rate)	2.0 (2004)	2 and 3 Mbit/s
HS (High Speed)	3.0 (2009)	Alternative MAC/PHY
LE (Low Energy)	4.0 (2010)	1 Mbit/s, ultra low power
Bluetooth Smart	4.0	Single-mode, LE-only radio
Bluetooth Smart Ready	4.0	Dual-mode, BR/EDR and LE dual radio

Range vs power consumption

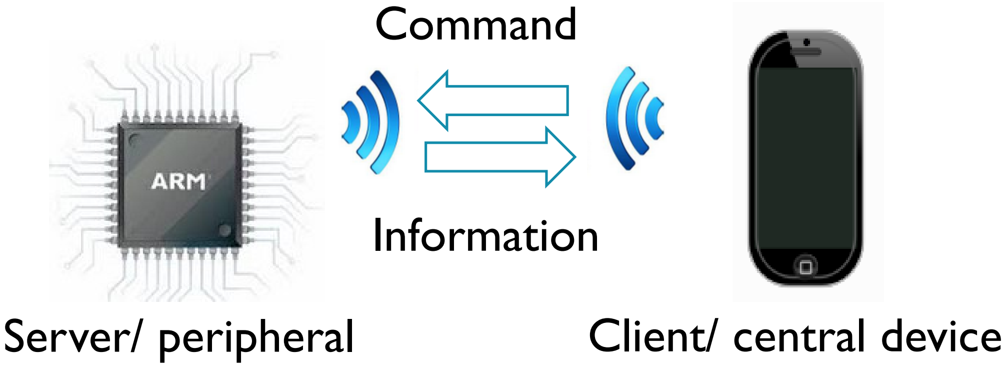
Version	Transmit range	Average power consumption
Bluetooth 1.x	Up to 10 meters	1 mW
Bluetooth 2.x	Up to 30 meters	2.5 mW
Bluetooth 3.x	Up to 100 meters	
Bluetooth Smart	50 meters	~1 uA (depending on use case)

Bluetooth Low Energy (BLE) protocol

- Profiled in Bluetooth Smart (Bluetooth 4.0)
- Key features
  - low power requirements
  - Coin-cell battery lasts 1+ year
  - Short transmitting and receiving window
  - Race to idle
    - Stay in a deep idle state for longer
    - Turn radio on as infrequently as possible
    - Turn radio off as soon as possible
  - Requires less memory
  - Fast connection and disconnection (~6ms)

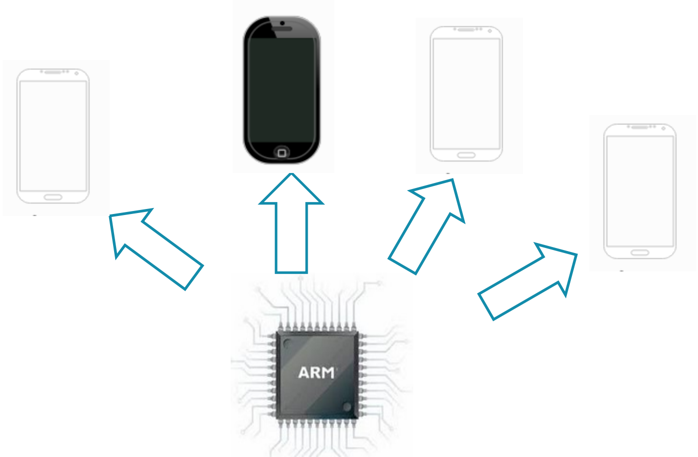
BLE device roles

- GAP roles: peripheral and central devices
  - Master/central: will typically have more computing resources and available energy; e.g., a computer or a tablet
  - Slave/peripheral: an embedded device; will have less computing resources and energy
- GATT roles: servers and clients
  - Server: the device containing information it wishes to share; in BLE, typically the peripheral (i.e. the embedded device)
  - Client: the device that wants to receive information and services; in BLE, typically the central device (i.e. the phone)

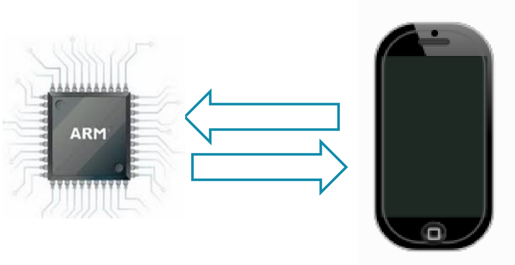


BLE protocol

- Initiating connections
  - The central device is free to establish or terminate a connection
  - The peripheral device cannot force the central device to scan for BLE devices
- BLE uses two modes
  - Advertising mode: the peripheral sends out Generic Access Profile (GAP) that any device in the area can pick up, which is how central devices know that there are peripherals around.
  - Connected mode: the peripheral and a central device establish a one-to-one conversation, which is how they can exchange complex information.

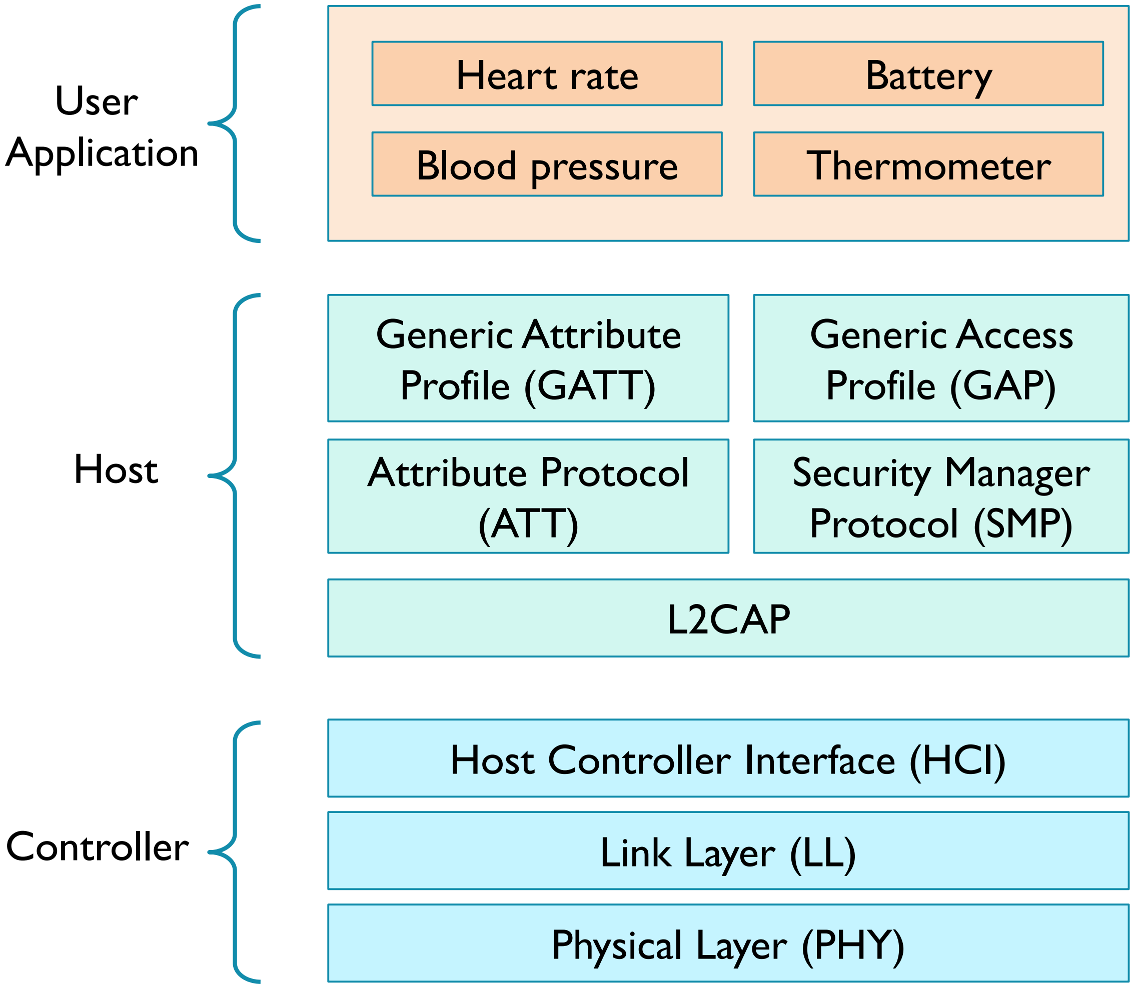


Advertising mode

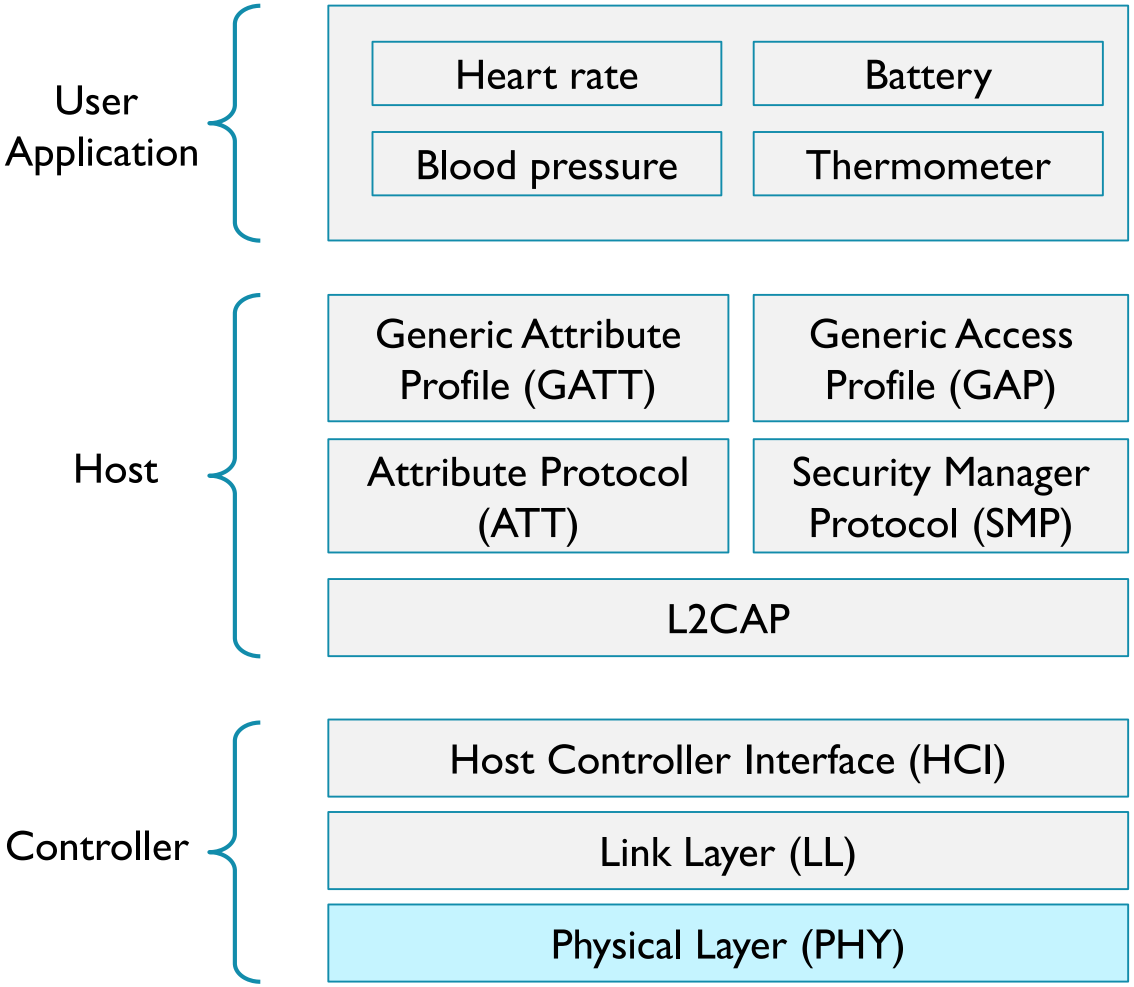


Connected mode

BLE architecture

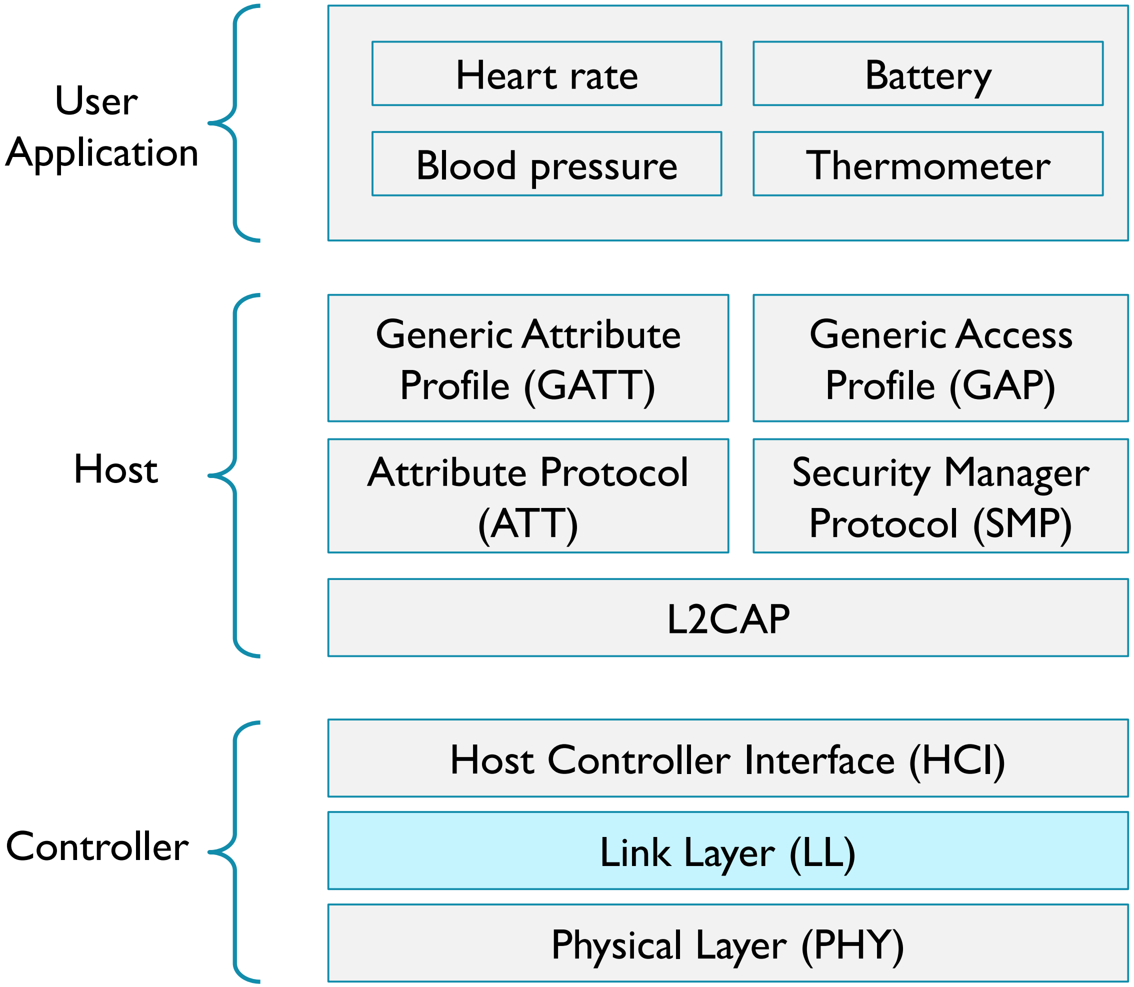


Physical layer (PHY)



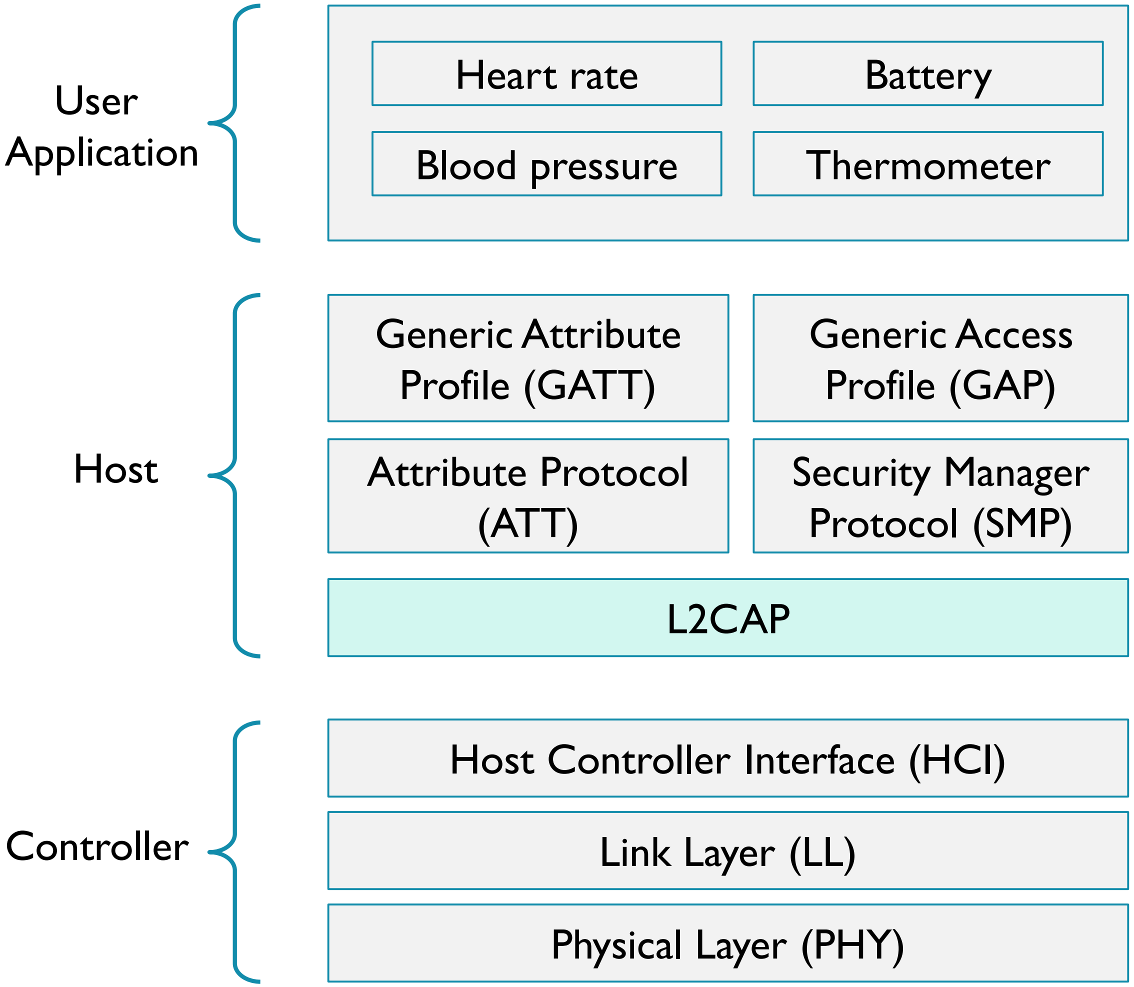
- RF: 2.4 GHz free ISM band
- Signalling rate: 1Mbit/s
- 40 RF channels
  - 3 channels for advertising
    - Discover
    - Connect
    - Broadcast
  - 37 channels for data
- GFSK modulation
- Maximum transmit power: 4 dBm

Link Layer (LL)



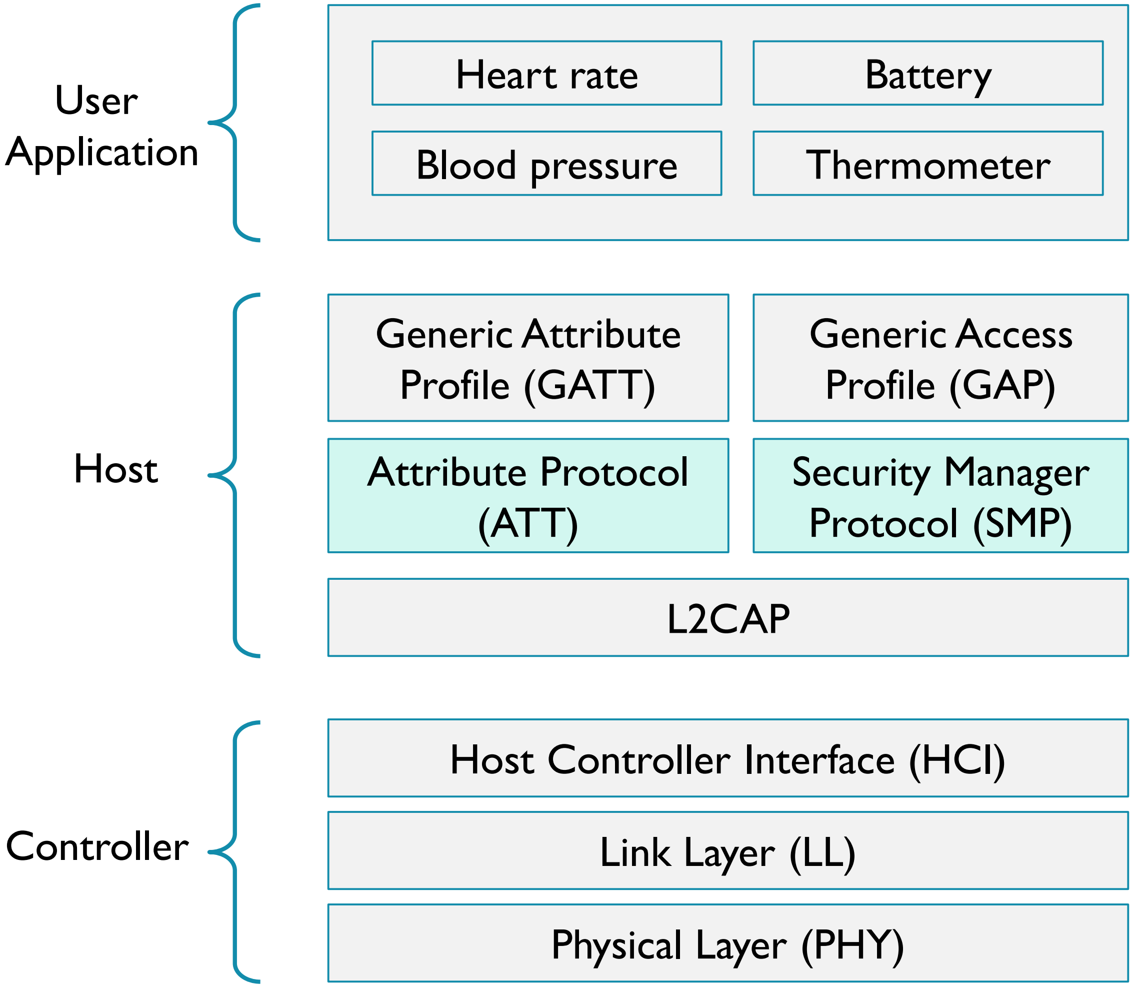
- Provides low power idle mode operation
- Simple device discovery
  - Advertising: connectable and non-connectable
  - Scanning: active or passive
- Point-to-multipoint data transfer
- Power-save and encryption functionalities
  - CRC generation and verification
  - Preample, addressing, and protocol framing
  - Random number generation
  - AES crypto

Logical Link Control and Adaptation Protocol



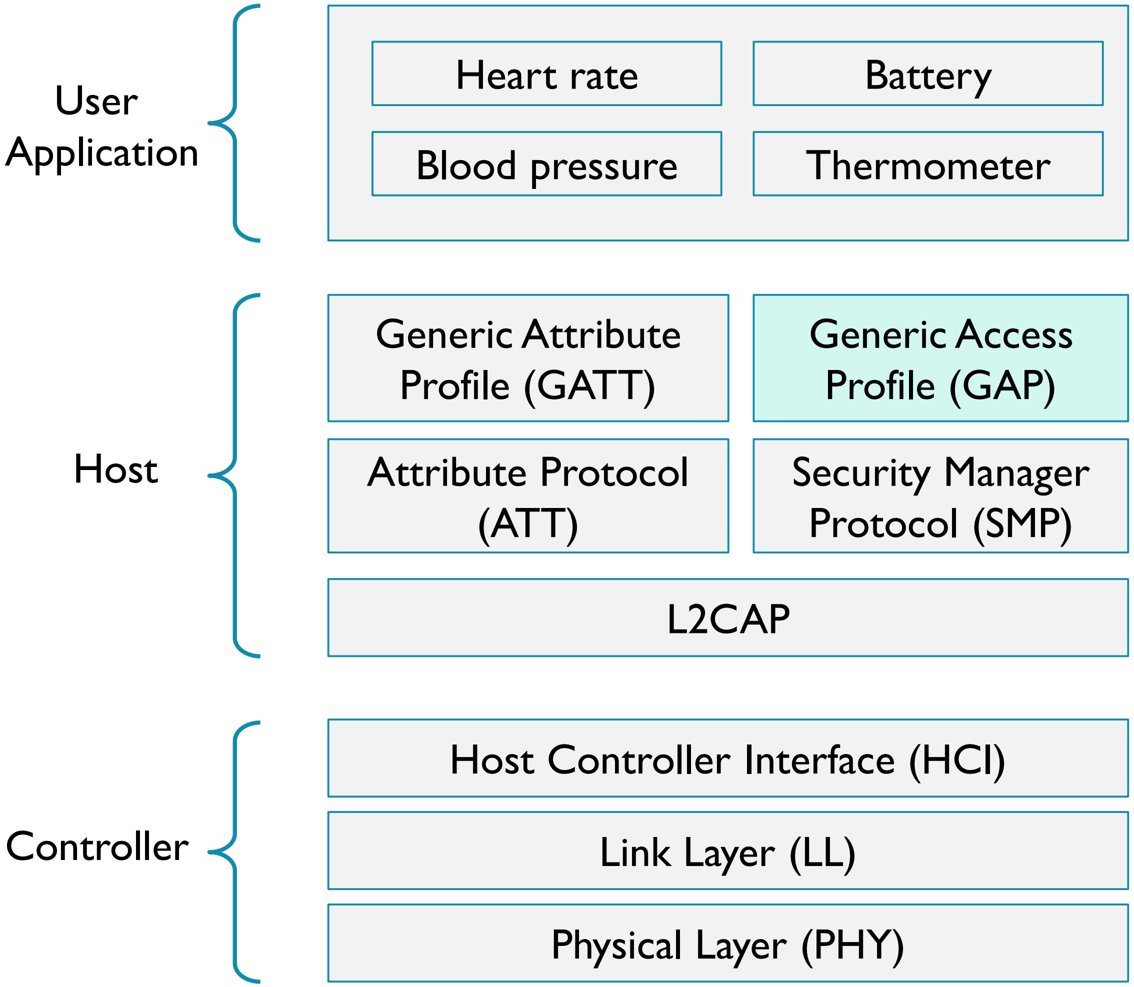
- Logical Link Control and Adaptation Protocol (L2CAP)
  - Protocol multiplexer
  - Encapsulates data into BLE packet format
  - Packet splits and recombines

Attribute Protocol (ATT) and Security Manager Protocol (SMP)



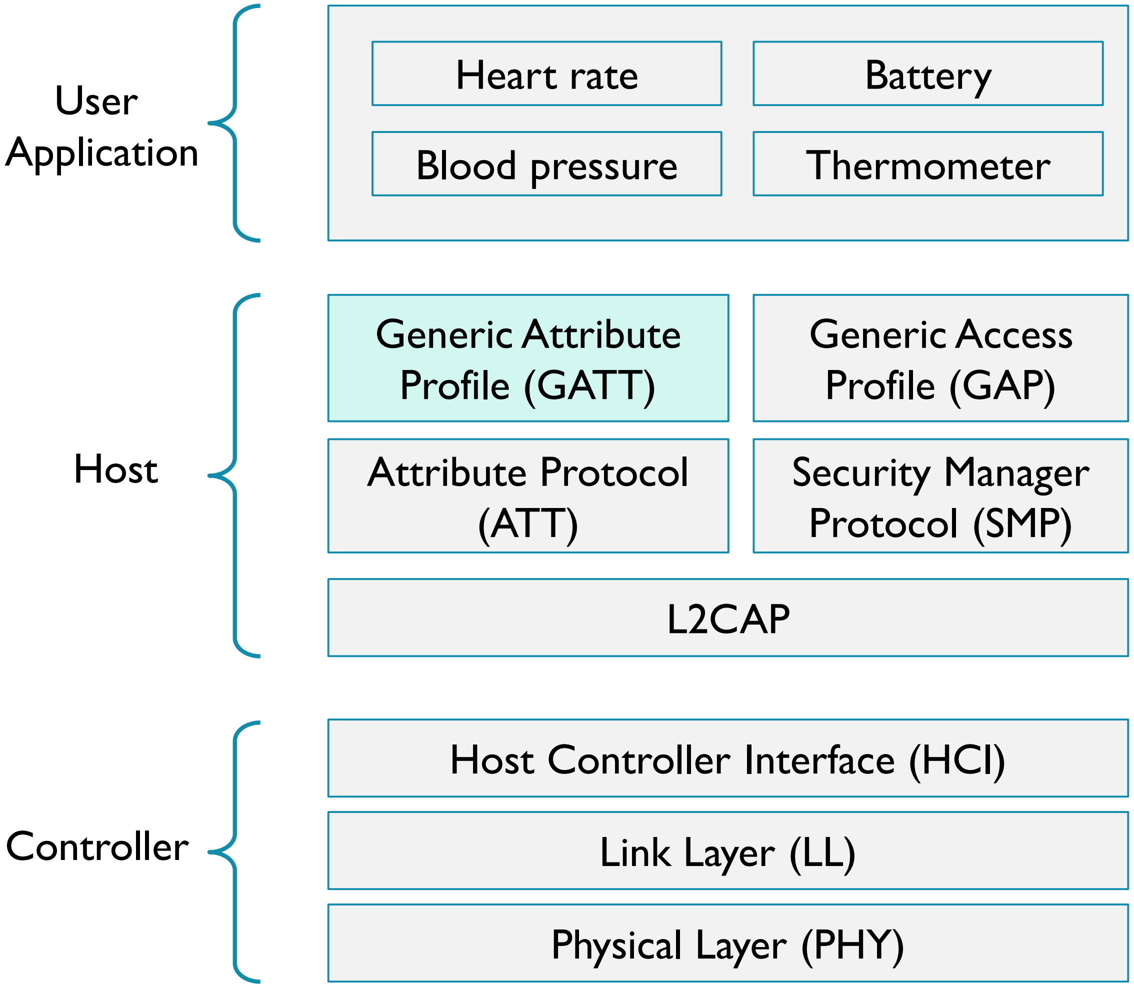
- Attribute Protocol (ATT):
  - Handle - Index in the ATT Table
  - UUID - Universal Unique Identifier
  - Permissions – data access such as Read, Write, Authenticated, Encrypted, etc.
  - Value – data to be read/written
- Security Manager Protocol (SMP)
  - Security Management
  - Pairing, bonding, and Encryption re-establishment
  - Privacy control
  - Generate/ distribute encryption key

Generic Access Profile (GAP)



- Generic Access Profile (GAP)
  - Used to discover and connect devices
  - Can be used as different roles
    - Peripheral (Slave)
    - Central (Master)
    - Server
    - Client
  - Security and privacy control
  - Usually the lowest level user could program from a BLE API

Generic Attribute Profile (GATT)

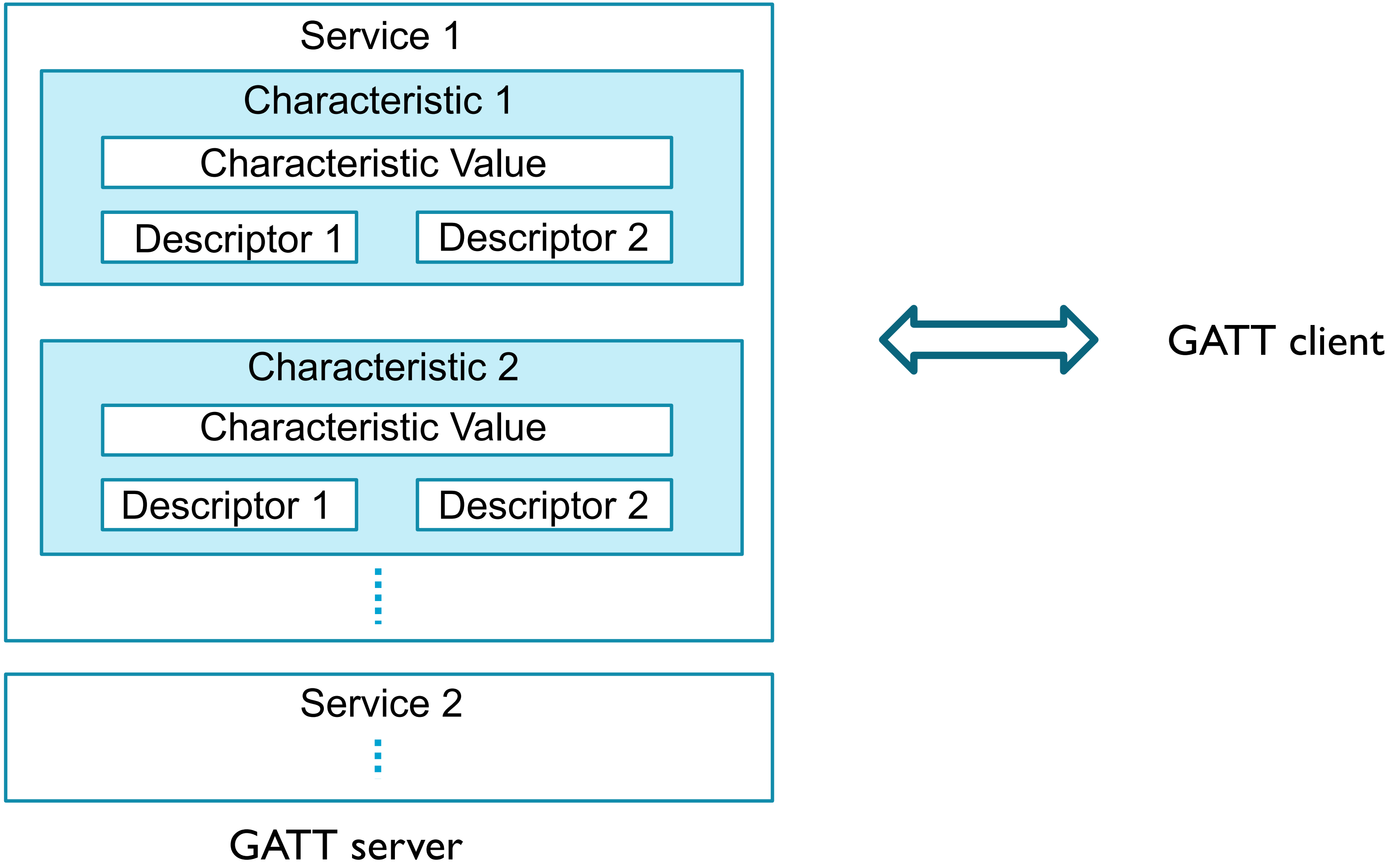


- Generic Attribute Profile (GATT)
  - General specification for transmitting data over BLE connection
  - Is used once connection is established
  - Hierarchical classification of Attributes
    - Services
    - Characteristics
    - Descriptors

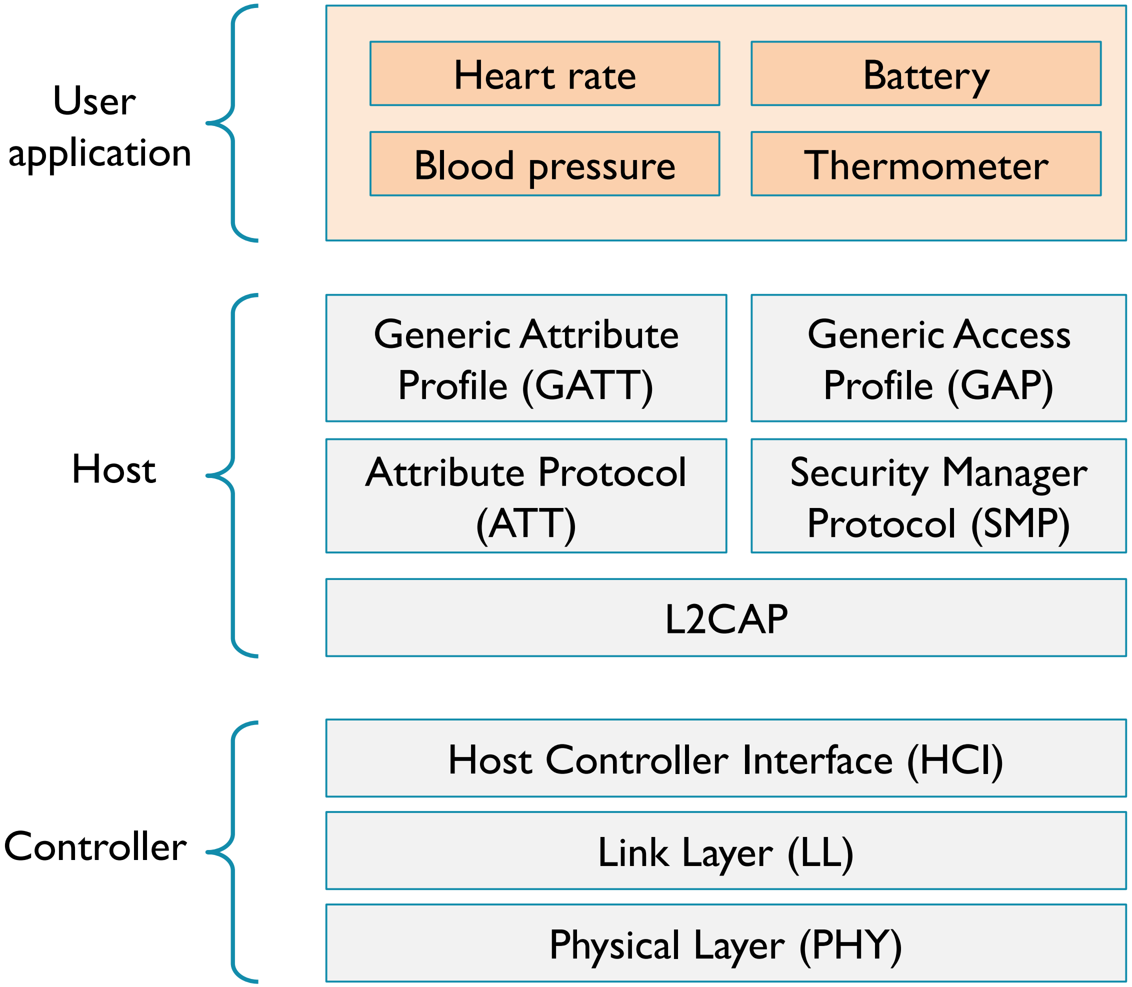
Generic Attribute Profile (GATT)

- Characteristic: Data transferred over a BLE link, e.g. , current battery voltage, temperature
- Service: A collection of related characteristics that work together for a specific function, e.g. a heart rate monitor service contains heart rate measurement, body sensor location, etc.
- Descriptor: Provides additional information about a characteristic, e.g. , a temperature characteristic can have its temperature range or units (e.g. Celsius) as descriptors

Generic Attribute Profile (GATT)



User application



- User application
  - Describes a particular use case
  - Uses one particular set of GATT services
  - Chooses required features from the stack
  - Defines roles, procedures and security