**1. Giới thiệu về BLE**

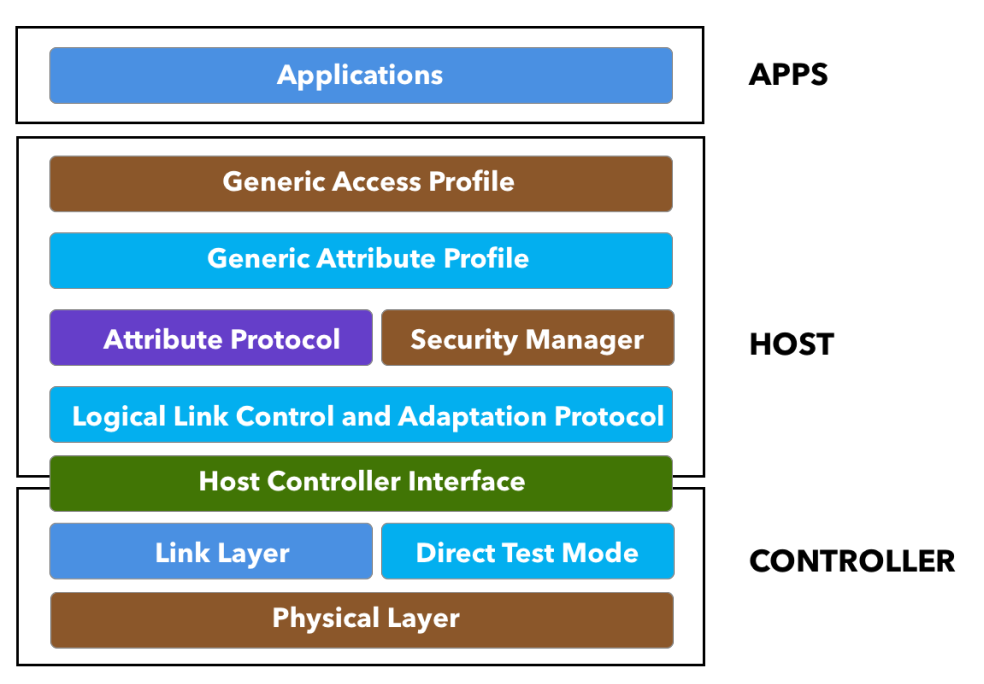
**1.1 Sơ lược về BLE**

Bluetooth Classic được sử dụng rộng rãi cho các ứng dụng thông qua việc truyền dữ liệu với tốc độ cao và dễ sử dụng. Tuy nhiên, đối với các thiết bị đeo tiết kiệm năng lượng và ứng dụng IoT, việc sạc pin thường xuyên không khả thi. Để giải quyết vấn đề này, Bluetooth Low Energy (BLE) đã được giới thiệu như một phiên bản tiết kiệm năng lượng trong Bluetooth Specification 4.0. Mục tiêu của BLE là cho phép các ứng dụng IoT tiết kiệm năng lượng mà vẫn đảm bảo kết nối và tốc độ truyền dữ liệu.

Bluetooth LE tập trung vào việc tiết kiệm năng lượng bằng cách giảm tốc độ truyền dữ liệu từ bằng cách chia nhỏ các gói dữ liệu từ 27 bytes đến 251 bytes và tối ưu hoá thời gian phát sóng radio. Điều này làm cho nó phù hợp cho các thiết bị hoạt động bằng pin như đồng hồ thông minh, cảm biến thông minh, và các thiết bị IoT. Ngoài ra, Bluetooth LE có các khía cạnh khác biệt với Bluetooth Classic, bao gồm các hình thức kết nối và loại thiết bị được hỗ trợ, nhằm phục vụ cho các ứng dụng IoT đặc biệt.

**1.2 Bluetooth LE protocol stack**

Hình ảnh dưới đây mô tả kiến trúc ngăn xếp giao thức của BLE, cho thấy các tầng tạo thành phần Host của Bluetooth LE và tầng tạo phần Controller của Bluetooth LE.



Tâng ứng dụng (Applications): là nơi mà người dùng tương tác thông qua các API được hỗ trợ để sử dụng giao thức bên trong BLE.

Tầng chủ (Host): quyết định cách các thiết bị Bluetooth LE lưu trữ và trao đổi dữ liệu với nhau

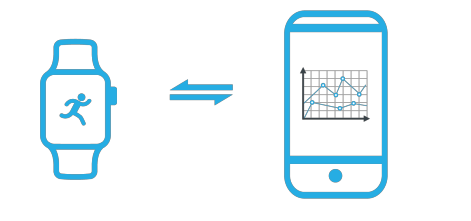
* Giao thức Logical Link Control & Adaptation Protocol (L2CAP): cung cấp dịch vụ đóng gói dữ liệu cho các tầng trên cùng. Nó giúp gói gọn dữ liệu và cung cấp khả năng truyền và nhận dữ liệu giữa các thiết bị Bluetooth LE
* Giao thức Security Manager Protocol (SMP): xác định và cung cấp phương pháp để thiết lập kết nối an toàn. Nó đảm bảo rằng dữ liệu được truyền qua kết nối Bluetooth LE được bảo vệ và mã hóa đúng cách.
* Giao thức Attribute Protocol (ATT): cho phép một thiết bị biểu diễn một số dữ liệu cụ thể cho thiết bị khác. Nó cho phép trao đổi thông tin và thu thập dữ liệu giữa các thiết bị Bluetooth LE.
* Giao thức Generic Attribute Profile (GATT): xác định các quy trình cần thiết để sử dụng tầng ATT. Nó mô tả cách truy cập và quản lý các services và characteristics trên thiết bị Bluetooth LE.
* Giao thức Generic Access Profile (GAP): tương tác trực tiếp với ứng dụng để xử lý các dịch vụ liên quan đến phát hiện thiết bị và kết nối. Nó cung cấp các chức năng như tìm kiếm thiết bị và thiết lập kết nối giữa các thiết bị Bluetooth LE.

Tầng điều khiển (Controller): gồm các thành phần như sau:

* Tầng Vật lý (Physical Layer - PHY): xác định cách dữ liệu thực tế được biến đổi thành sóng radio, và cách nó được truyền và nhận. Tầng này quyết định các thông số về tần số, công suất và phương thức truyền dữ liệu trên sóng radio.
* Tầng Liên kết (Link Layer - LL): quản lý trạng thái của radio, được định nghĩa là một trong các chế độ sau - chế độ chờ (standby), chế độ quảng bá (advertising), chế độ quét (scanning), chế độ khởi tạo (initiating), và chế độ kết nối (connection). Tầng này điều khiển việc gửi và nhận các gói tin trong quá trình kết nối Bluetooth LE.

**1.3 GAP và vai trò các thiết bị trong kết nối BLE**

Tầng GAP trong Bluetooth LE xác định các vai trò và chức năng của các thiết bị trong kết nối Bluetooth LE. Vai trò quảng bá và quét là các vai trò quan trọng trong quá trình thiết lập kết nối giữa các thiết bị Bluetooth LE. Một thiết bị quảng bá sẽ thông báo về sự tồn tại và khả năng kết nối của nó, trong khi một thiết bị khác sẽ quét và tìm kiếm các thiết bị quảng bá để thiết lập kết nối.

Trong Bluetooth LE, có hai vai trò chính là **peripheral** và **central**. Peripheral là thiết bị quảng bá sự hiện diện và mong muốn kết nối, trong khi central là thiết bị quét và tìm kiếm các thiết bị peripheral. Khi central quét và phát hiện gói quảng bá của peripheral, nó có thể khởi tạo một yêu cầu kết nối tới peripheral để thiết lập kết nối. Khi kết nối được thiết lập, peripheral và central có thể trao đổi dữ liệu và tương tác với nhau.

**1.4 ATT và GATT: Biểu diễn và trao đổi dữ liệu**

ATT xác định cách dữ liệu được truyền và xử lý trong quá trình kết nối của các thiết bị Bluetooth LE. Nó dựa trên mô hình client-server, trong đó server là thiết bị chứa dữ liệu và có thể gửi dữ liệu cho client (thiết bị khác) hoặc client có thể yêu cầu dữ liệu từ server.



GATT là một lớp giao thức nằm trên lớp ATT và sử dụng các khái niệm như profile, dịch vụ (service) và đặc điểm (characteristics) để quản lý việc truyền dữ liệu giữa các thiết bị Bluetooth LE.

* Profile: Một profile là một tập hợp các dịch vụ và đặc điểm liên quan đến một ứng dụng cụ thể. Ví dụ, profile Heart Rate Monitor (Bộ đo nhịp tim) xác định các dịch vụ và đặc điểm liên quan đến việc đo nhịp tim.
* Service (Dịch vụ): Một dịch vụ đại diện cho một chức năng cụ thể của một thiết bị Bluetooth LE. Ví dụ, dịch vụ Heart Rate (Nhịp tim) trong profile Heart Rate Monitor sẽ chứa thông tin về việc đo nhịp tim.
* Characteristic (Đặc điểm): Một đặc điểm là một phần của dịch vụ và chứa dữ liệu hoặc thông tin cụ thể. Ví dụ, trong dịch vụ Heart Rate, đặc điểm Heart Rate Measurement chứa dữ liệu về nhịp tim đo được.

