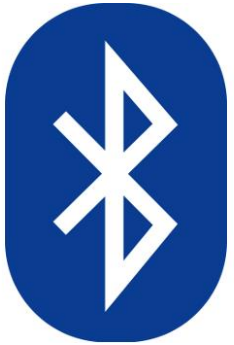


BLUETOOTH LOW ENERGY (BLE)

WPAN TECHNOLOGY (IEEE 802.15.1)

Bhupendra Pratap Singh
Connected Products (AIOT)

BLE OVERVIEW

BLE started as part of Bluetooth 4.0 core specification.

It is originally designed by Nokia as wibree (Baby Bluetooth) before being adopted by Bluetooth Special Interest Group (SIG).

802.15.1 – Original foundation of the Bluetooth PAN.

BLUETOOTH HISTORY

- Bluetooth technology was first conceived at Ericsson in 1994 with the intent to replace the litany of cables and cords connecting computer peripherals with an RF medium.
- Intel and Nokia also joined in with the intent to wirelessly link cell phones to computers in a similar manner.
- The three formed an Special Interest Group (SIG) in 1996 at a conference held at Ericsson, Sweden.

BLUETOOTH HISTORY

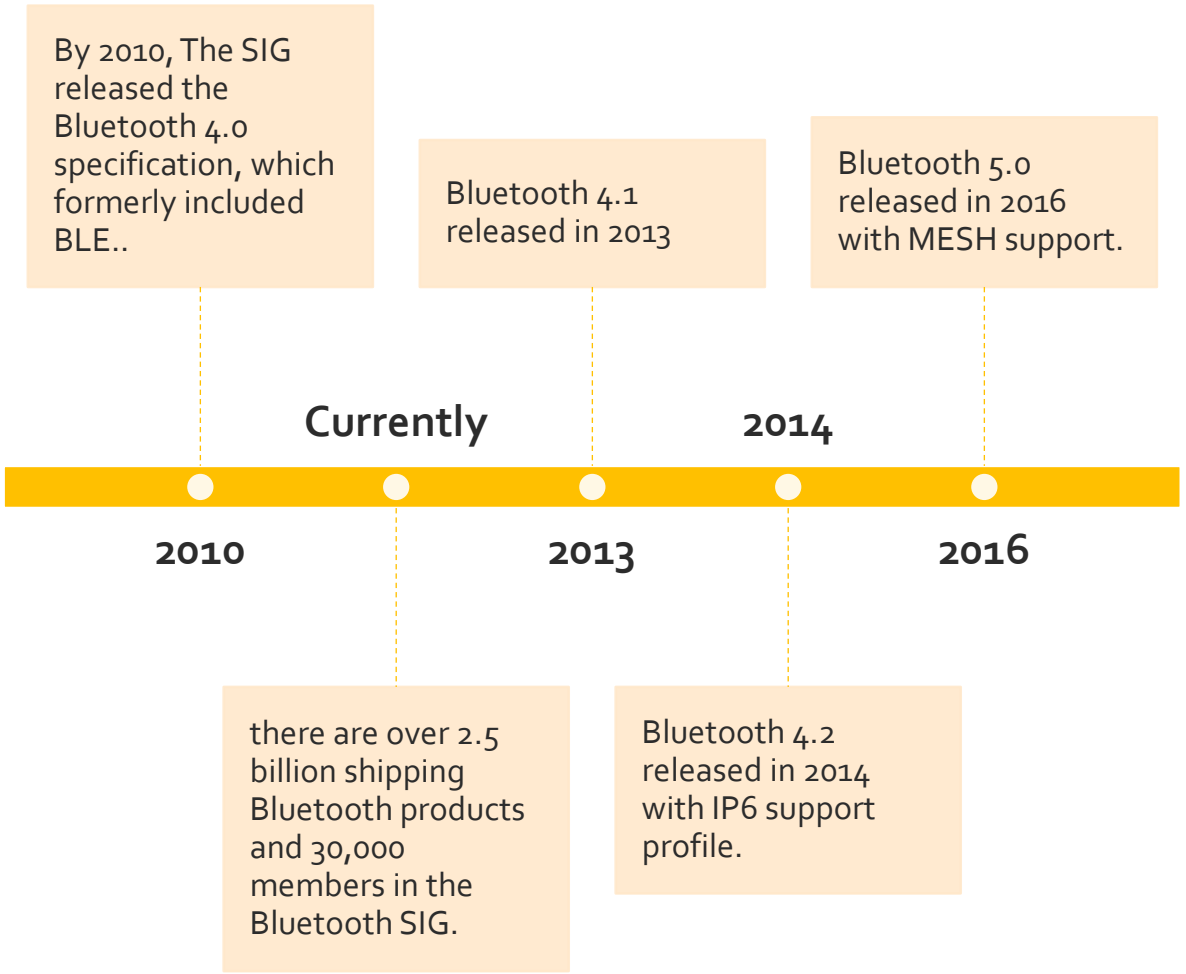
By 1998 – Toshiba and IBM also joined the group. Version 1.0 released.

Version 2.0 (EDR – 3Mbps) was later ratified in 2005 when SIG had over 4000 members.

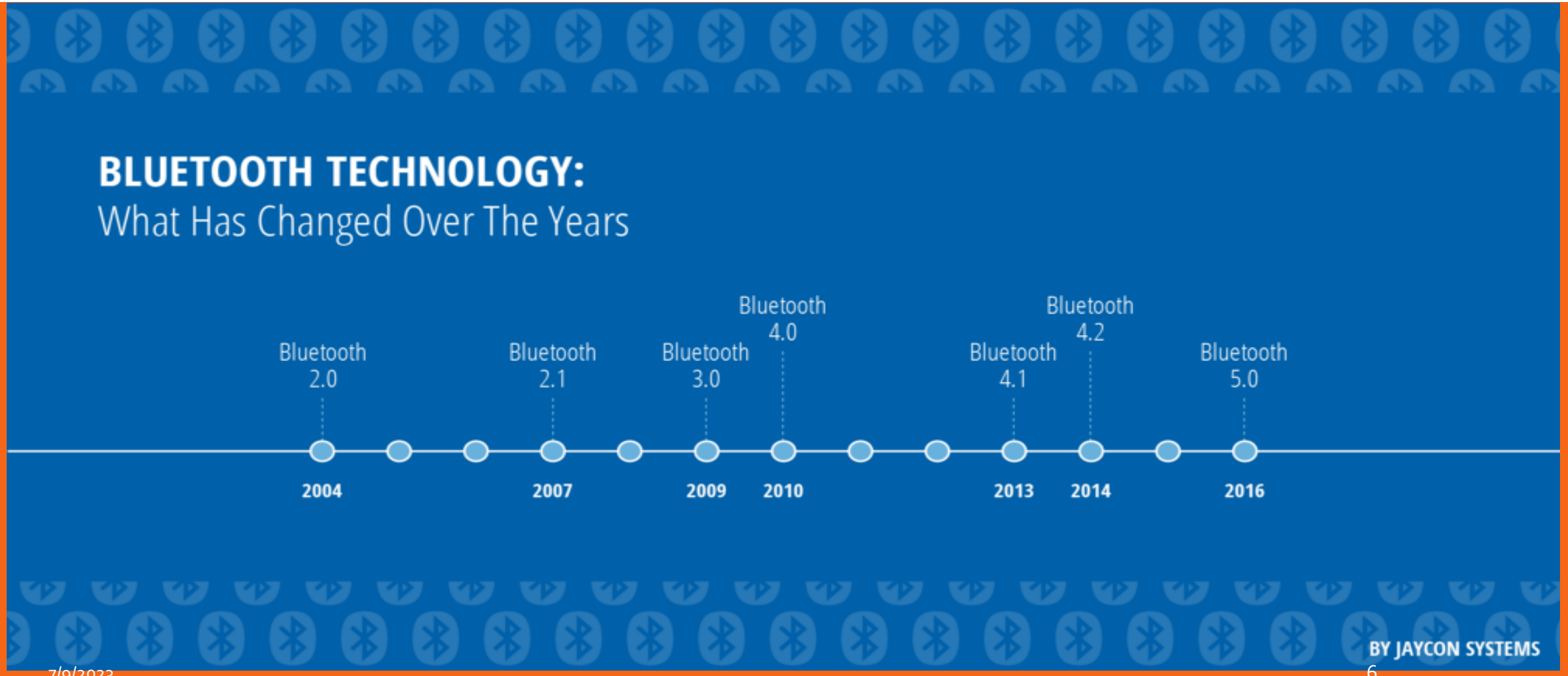
In 2007, The Bluetooth SIG worked with Norrdic Semiconductor and Nokia to develop Ultra Low Power Bluetooth, which now goes by the name Bluetooth Low Energy.

BLE brought an entirely new segment to the market in devices that could communicate using a coin cell battery.

BLUETOOTH HISTORY



BLUETOOTH TECHNOLOGY – OVER THE YEARS



References: https://medium.com/jaycon-systems/bluetooth-technology-what-has-changed-over-the-years-385da7ec7154

BLUETOOTH 5 COMMUNICATION PROCESS AND TOPOLOGIES

Bluetooth wireless is comprised of two wireless technology systems: Basic Rate (BR) and Bluetooth Low Energy (BLE). Nodes can either be advertisers or scanners by this definition.

Advertiser – Device Transmitting advertiser packets.

Scanner – Device receiving advertiser packets without the intention to connect.

Initiator – Device attempting to form a connection.

BLUETOOTH 5 COMMUNICATION PROCESS AND TOPOLOGIES – BLUETOOTH EVENTS

- **Advertising –** Initiated by a device to broadcast to scanning devices to alert them of the presence of a device wishing to either pair or simply relay a message in the advertising packet.
- **Connecting –** This event is the process of pairing a device and host.

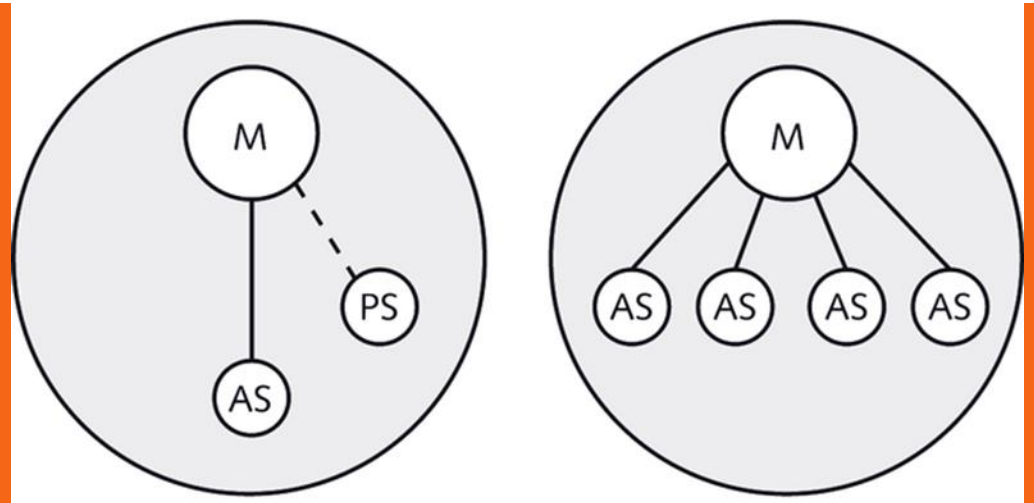
BLUETOOTH 5 COMMUNICATION PROCESS AND TOPOLOGIES – BLUETOOTH EVENTS

- **Periodic Advertising – (Bluetooth – 5)** Allows an advertising device to periodically advertise over the 37 non-primary channels by channel hopping at an interval of 7.5 ms to 81.91875s.
- **Extended Advertising – (Bluetooth 5) –** allows for extended PDUs to support advertisement chaining and large PDU payloads.

	BLUETOOTH V2.1	BLUETOOTH 4.0 (LE)	BLUETOOTH 5 (LE)
Range	Up to 100 m	Up to 100 m	Up to 400 m
Max range (free field)	Around 100 m (class 2 outdoors)	Around 100 m (outdoors)	Around 1,000m (outdoors)
Frequency	2.402 – 2.481 GHz	2.402 – 2.481 GHz	2.402 - 2.481 GHz
Max data rate	1- 3 Mbit/s	1 Mbit/s	2 Mbit/s
Application Troughput	0.7-2.1 Mbit/s	Up to 305 kbit/s	Up to 1,360 kbit/s
Topologies	Point-to-point, scatternet	Point-to-point, mesh network	Point-to-point, mesh network
Network Standard	IEEE 802.15.1	IEEE 802.15.1	IEEE 802.15.1

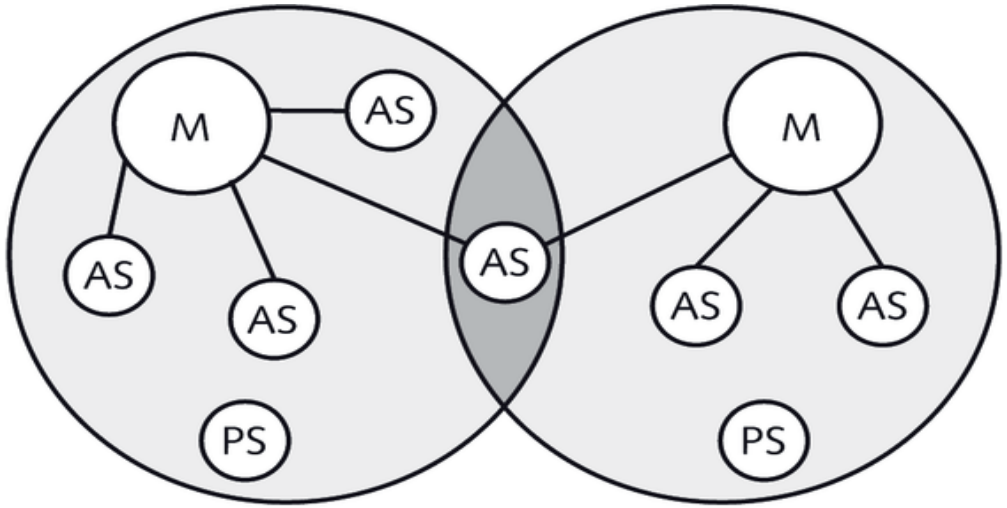
SOURCE : NORDIC SEMICONDCTOR

REVISTING PICONET AND SCATTERNET



M = Master
AS = Active slave
PS = Parked slave

Figure 5-9 Piconets



M = Master
AS = Active slave
PS = Parked slave

Figure 5-16 Scatternet

PICONET – One Master, 7 Slave Devices (Max 255 Devices, but other than 8 should be in parked mode/standby mode

Scatternet – Group of Piconet form a Scatternet

MODES OF DEVICES (REVISION)

Devices in a Piconet can be in one of five different modes

- Standby—waiting to join a Piconet
- Inquire—looking for other devices
- Page—master device is asking to connect to specified slave
- Connected—either active slave or master is connected
- Park/Hold—device is part of piconet, but in a low-power state.

NOTE – POINT TO REMEMBER

- IN BR/EDR Mode, the network uses same frequency hopping schedule and all the nodes will be guaranteed to be on same channel at a given time.
- In BLE mode, that system uses 24 bit addressing so the number of slaves associated with the master is in millions.

- Bluetooth 5.0 has deprecated and removed parked states in Piconet; only Bluetooth devices up to version 4.2 will support a parked state.
- Standby mode is still supported by Bluetooth 5.0

BLE MODES AND PROFILES

Peripheral and central devices v servers and clients

When we connect devices over BLE, we think of them as being either a peripheral (slave) device or a central (master) device.

The Bluetooth standard established this division to match the resources available on the devices:

DEVICE NAMES

- **Master/central**

will typically have more computing resources and available energy - for example - A computer or a tablet, mobile phone.

- **Slave/peripheral**

Mbed Devices, NRF Devices (NRF51822), sensor tag - will be constrained in both computing resources and energy.

DEVICE NAMES

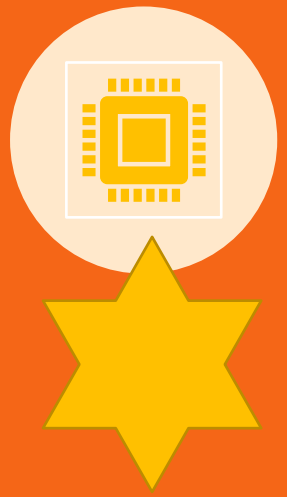
- BLE uses two additional terms to describe the connecting entities - server and client.

SERVER

The device that has information it wishes to share, and in BLE that is typically the peripheral. (Less computing Resources)

- (the mbed board, sensor tag, nrfdk).

CLIENT

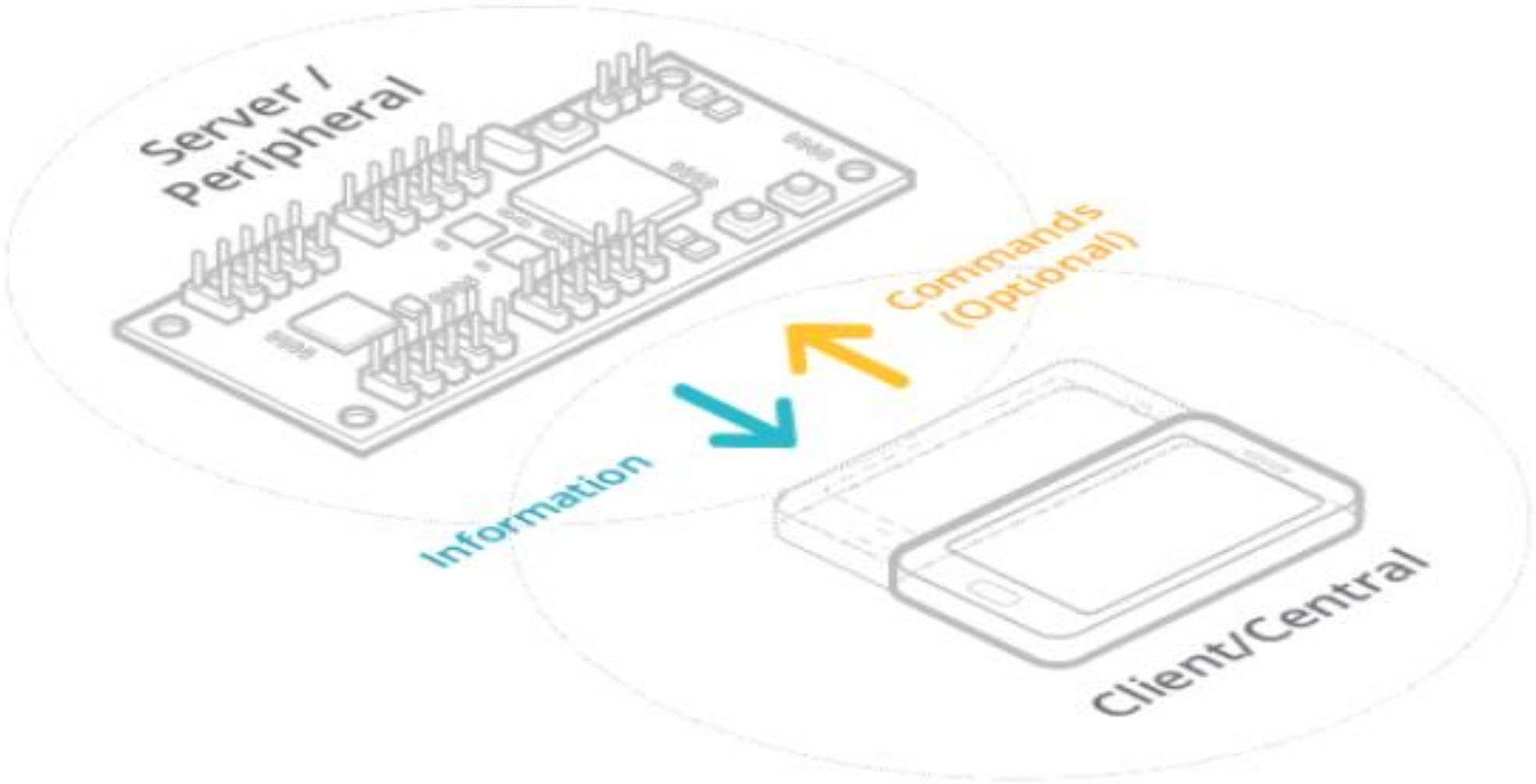


The device that wants information and services, and in BLE that is typically the central.

Device - The phone, Tablet.

We use the terms server and client when discussing the exchange of information. We use central and peripheral to denote the origin and target of a BLE connection

PICTORIAL REPRESENTATION



INITIATING CONNECTIONS

- The central initiates, controls and ends the connection - the peripheral cannot force the central to act scan for BLE devices, view their information, connect and so on).

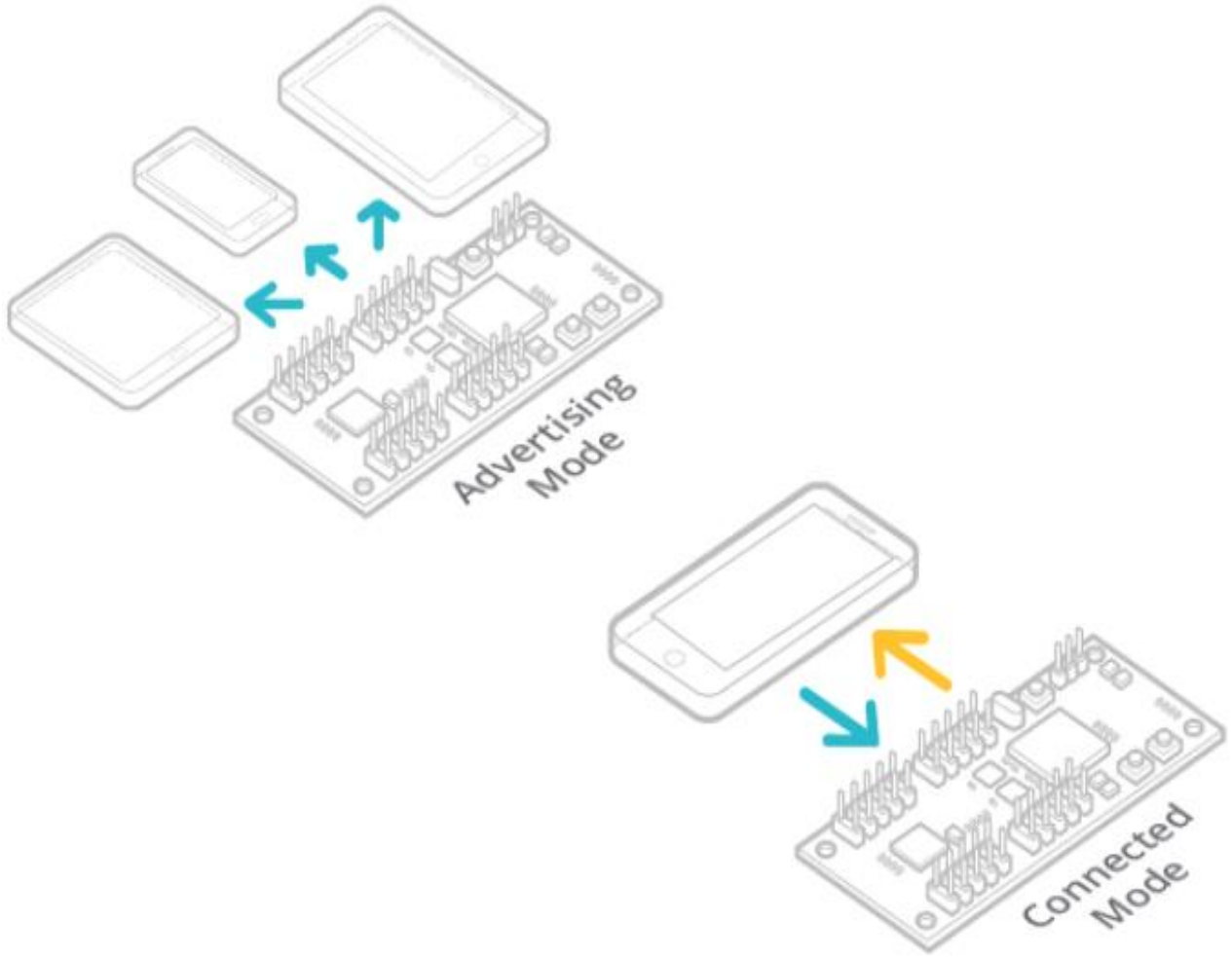
BLE MODES

- The two modes BLE uses are:
- Advertising Mode
- Connected Mode
- **Advertising Mode :**
- The peripheral sends out a bit of information that any device in the area can pick up. This is how central devices know that there are peripherals around.

BLE MODES

- **Connected Mode**
- The peripheral and a central device establish a one-to-one conversation. This is how they can exchange complex information.
- **NOTE:**
- A central device must know that a peripheral device exists to be able to connect with it. A peripheral will therefore advertise its presence using the BLE advertising mode. In this mode, the device uses the Generic Access Profile (GAP) to send out a bit of information - an advertisement - at a steady rate. This advertisement is what other devices, like your phone, pick up. It tells them about the presence of a BLE device in the neighbourhood, and whether that device is willing to talk to them.

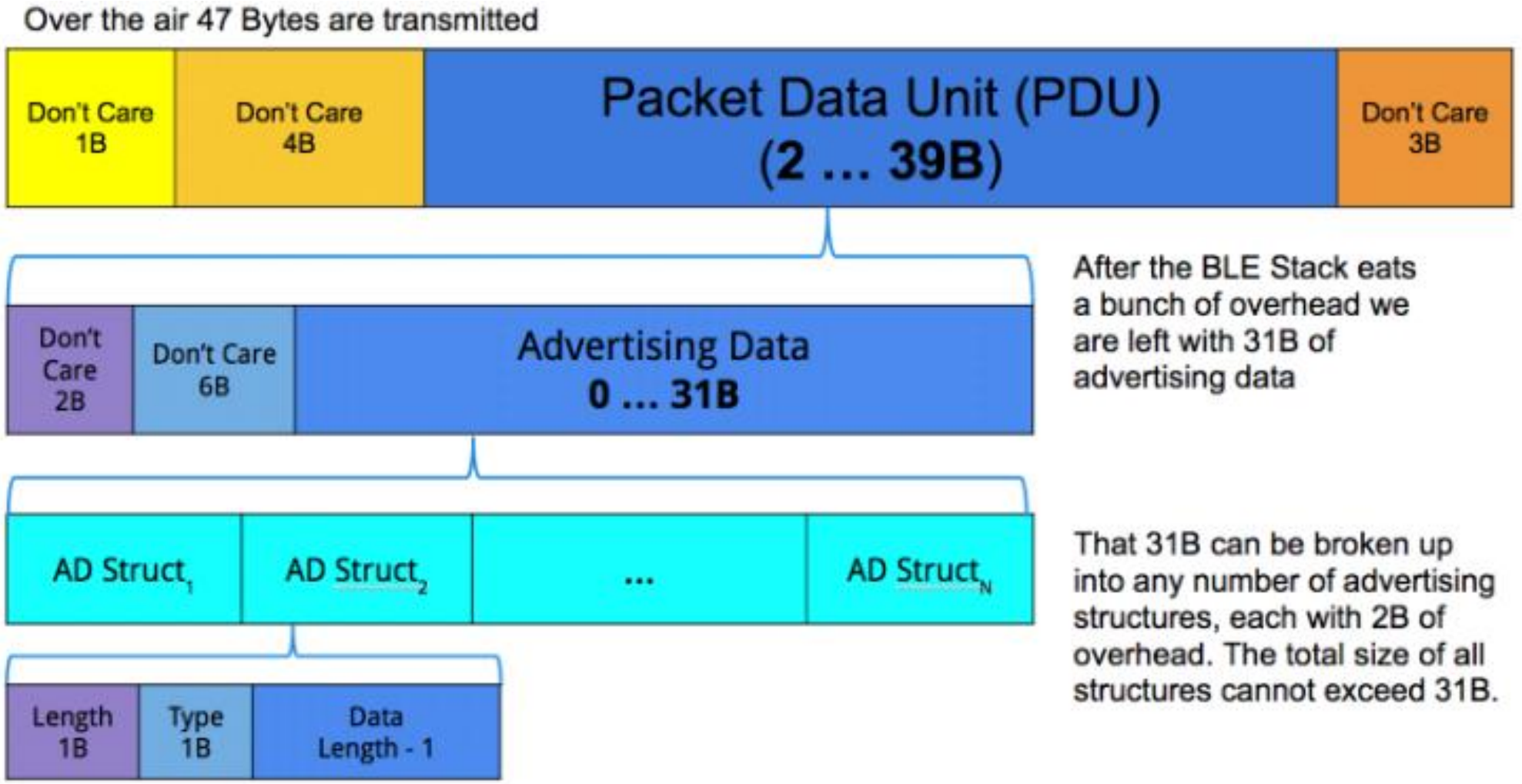
PICTORIAL REPRESENTATION



Advertising mode is one-to-many, whereas connected mode is one-to-one.

Advertisements are very limited in size. The general GAP broadcast's data breakdown is illustrated in the next slide with a pictorial representation.

THE GENERAL GAP BROADCAST'S DATA BREAKDOWN



BLUETOOTH PROFILES

Understanding the roles of GAP and GATT

GAP:

- Is used for connection and advertising.

GATT :

- GATT is an acronym for the Generic Attribute Profile, and it defines the way that two Bluetooth Low Energy devices transfer data back and forth using concepts called Services and Characteristics. It makes use of a generic data protocol called the Attribute Protocol (ATT), which is used to store Services, Characteristics and related data in a simple lookup table using 16-bit IDs for each entry in the table

GENRIC ACCESS PROFILE(GAP)

The Generic Access Profile defines the following roles when operating over the LE physical channel:

- **Broadcaster role:** A device operating in the Broadcaster role can send advertising events. It is referred to as a Broadcaster. It has a transmitter and may have a receiver.
- **Observer role:** A device operating in the Observer role is a device that receives advertising events. It is referred to as an Observer. It has a receiver and may have a transmitter.
- **Peripheral role:** A device that accepts the establishment of an LE physical link using any of the connection establishment procedures is termed to be in a "Peripheral role." A device operating in the Peripheral role will be in the "Slave role" in the Link Layer Connection State. A device operating in the Peripheral role is referred to as a Peripheral. A Peripheral has both a transmitter and a receiver.
- **Central role:** A device that supports the Central role initiates the establishment of a physical connection. A device operating in the "Central role" will be in the "Master role" in the Link Layer Connection. A device operating in the Central role is referred to as a Central. A Central has a transmitter and a receiver.

PROFILE LAYER

- **In BLE, data is organized into concepts called Profiles, Services, and Characteristics.**
- **PROFILE**
- A Profile describes how devices connect to each other to find and use Services. It is a definition used by Bluetooth devices to describe the type of application and the general expected behavior of that device.

PROFILE LAYER

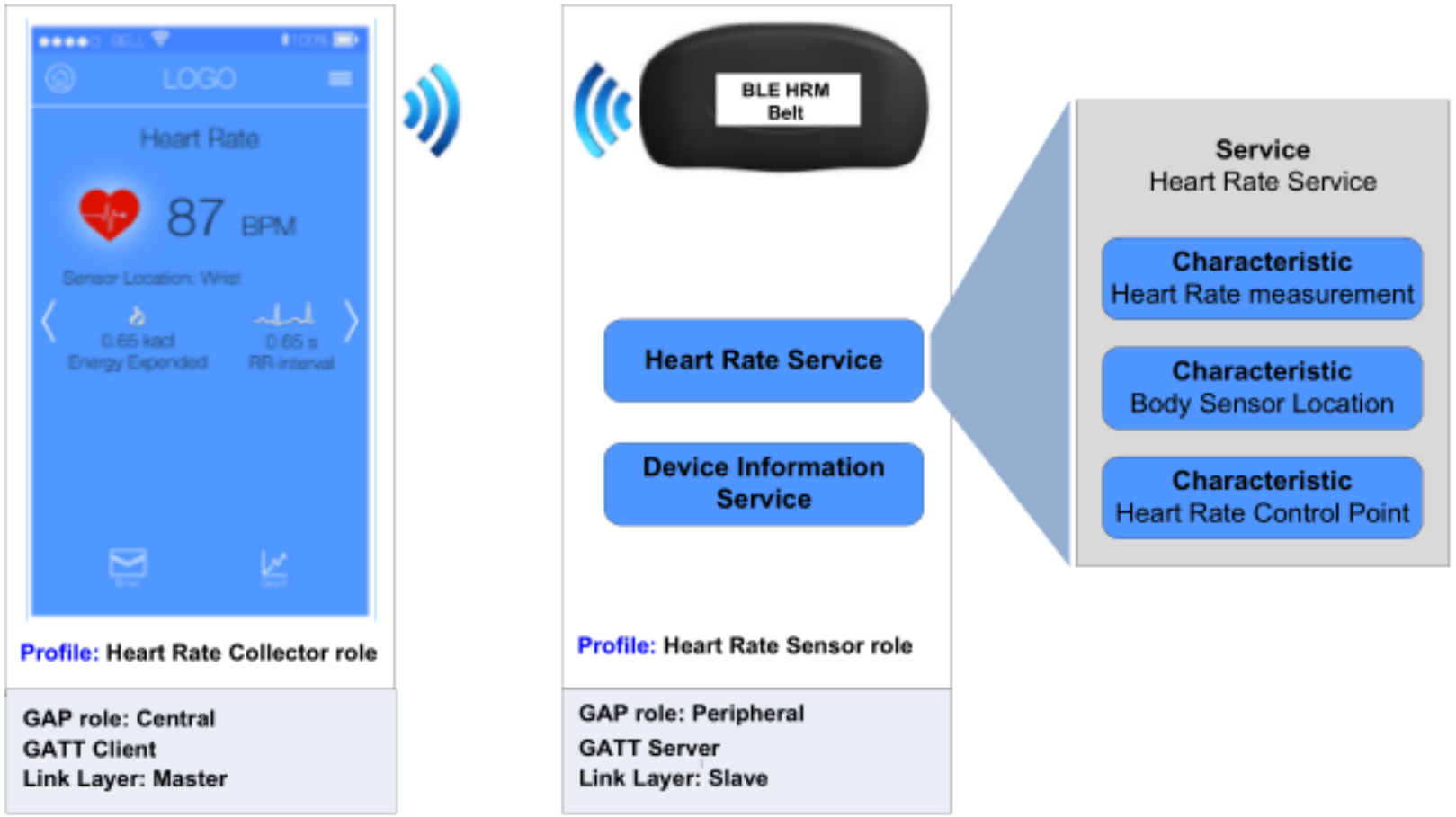
- **SERVICE**
- Service is a collection of data entities called Characteristics. A Service is used to define a certain function in a Profile. A Service may also define its relationship to other Services. A Service is assigned a Universally Unique Identifier (UUID). This is 16 bits for SIG adopted Services and 128 bits for custom Services.

PROFILE LAYER

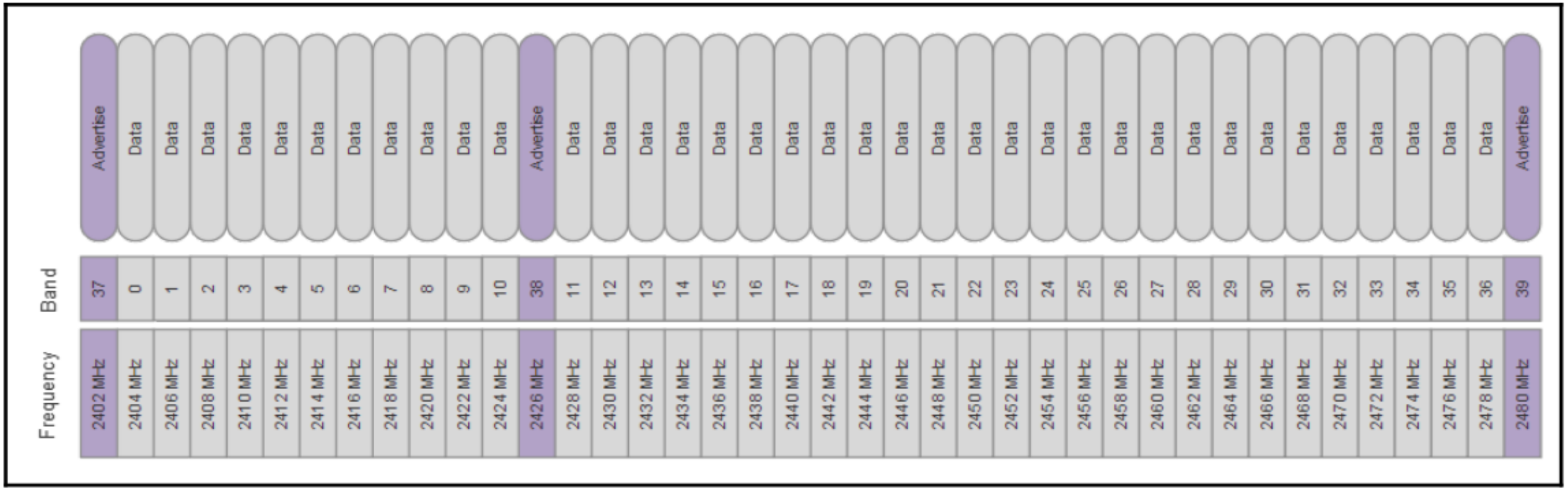
- **CHARACTERISTICS**
- A Characteristic contains a Value and the Descriptor that describes a Characteristic Value. It is an attribute type for a specific piece of information within a Service. Like a Service, each Characteristic is designated with a UUID; 16 bits for SIG adopted Characteristics and 128 bits for custom Characteristics.

EXAMPLE

The following diagram shows the relationship between Profiles, Services, and Characteristics in a sample BLE heart rate monitor application using a Heart Rate Profile.



BLE CHANNELS
(DATA – 37, ADVERTISING – 03)

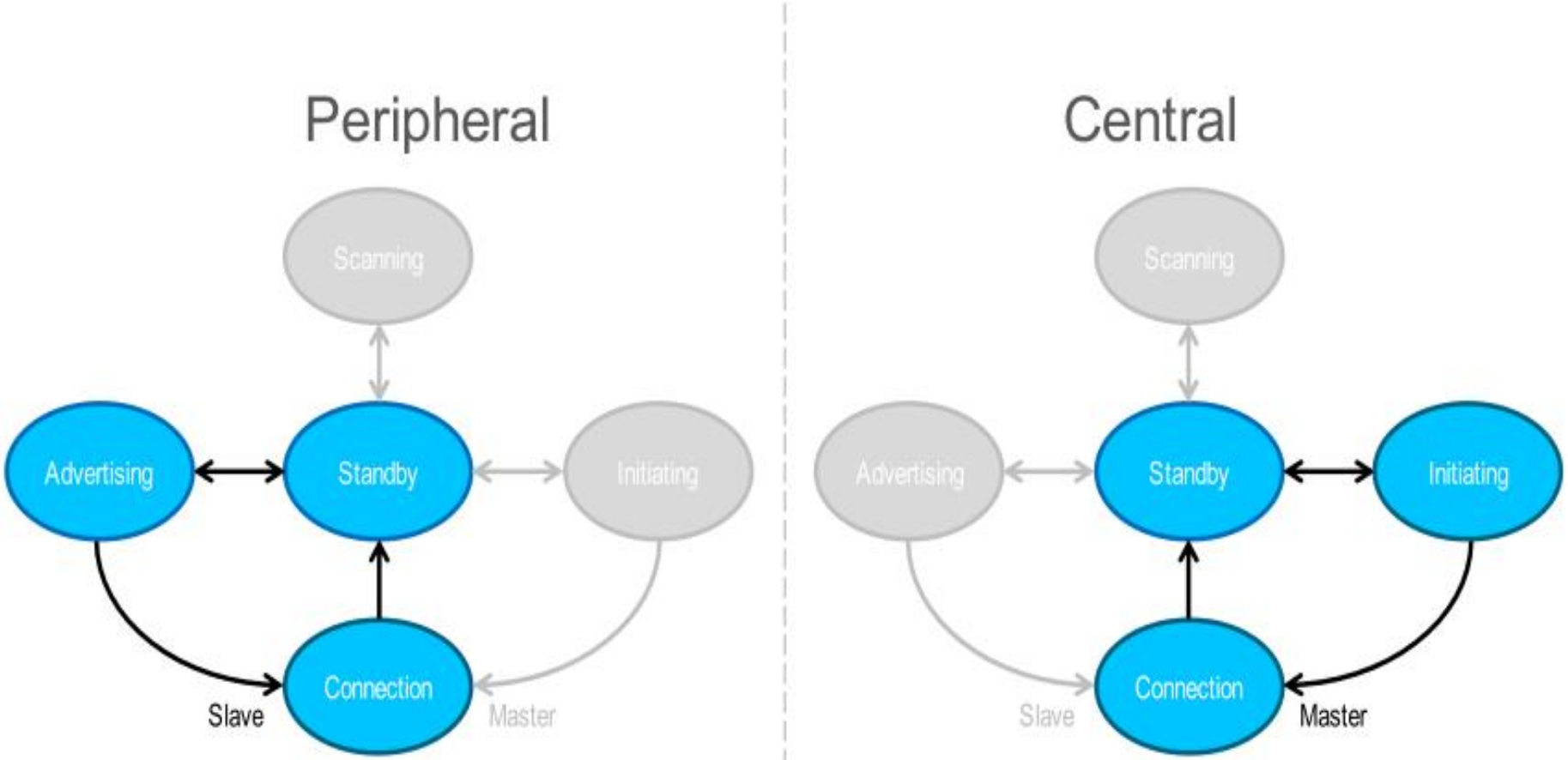


ZERO TO 36 – DATA CHANNELS

37 TO 39 – ADVERTISING CHANNELS

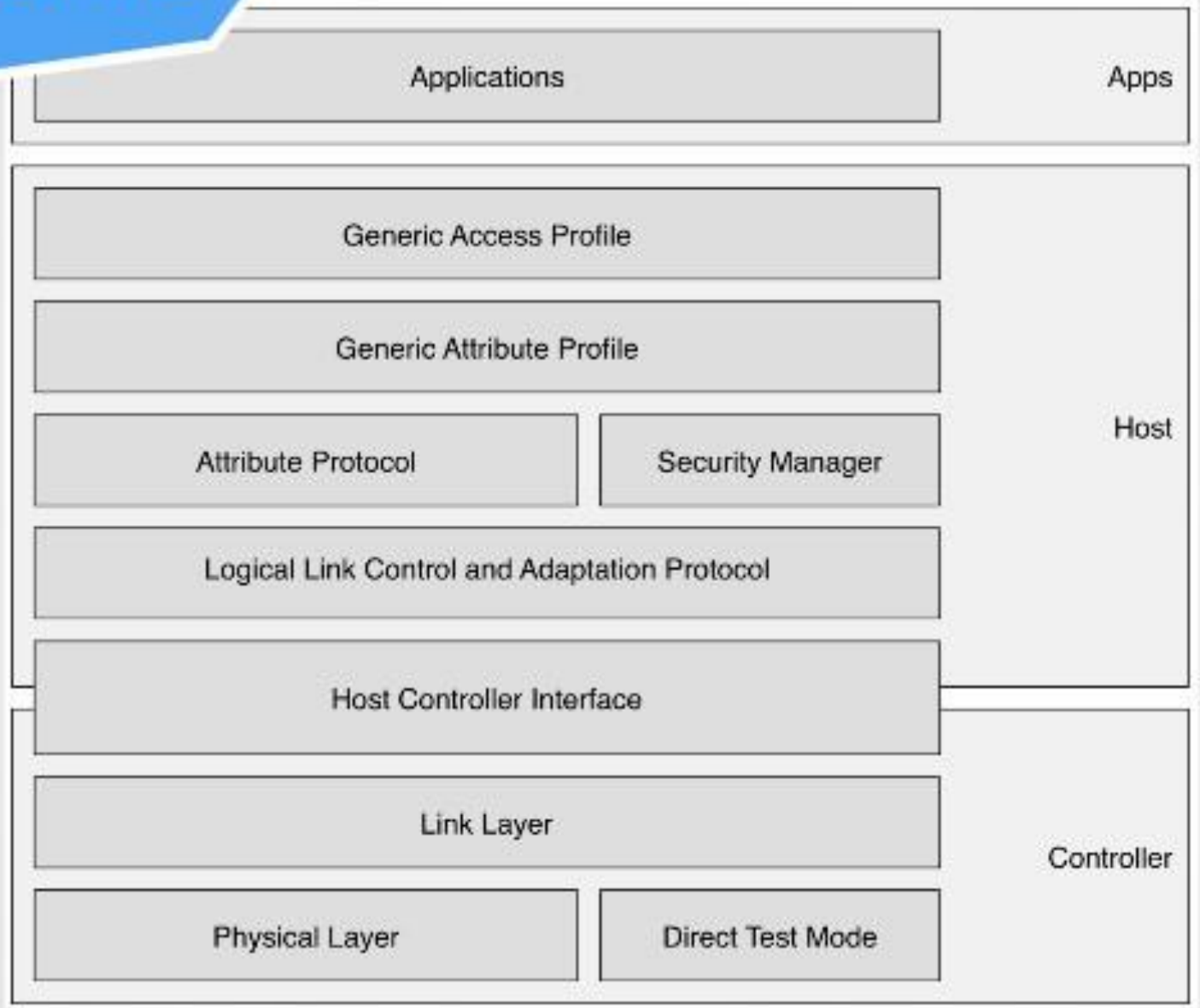
BLE LINK STATE

(PERIPHERAL AND CENTRAL)



BLE STACK

ARCHITECTURE



Source: Bluetooth Low Energy - The Developer's Handbook (Robin Heydan)

PHYSICAL LAYER

- The physical layer is the part that actually **contains the analog communications circuitry, capable of modulating and demodulating analog signals** and transforming them into digital symbols.
- The radio uses the 2.4 GHz ISM (Industrial, Scientific, and Medical) band to communicate and divides this band into **40 channels** from 2.4000 GHz to 2.4835 GHz.

THE LINK LAYER

- The Link Layer is the part that directly interfaces with the physical layer and it is usually implemented as a combination of custom hardware and software and it defines the main role of ble devices.

HOST CONTROLLER INTERFACE (HCI)

- Bluetooth specification defines HCI as a set of commands and events for the host and the controller to interact with each other, along with a data packet format and a set of rules for flow control and other procedures.

LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL (L2CAP)

- This layer provides two pieces of functionality First, it serves as a protocol multiplexer that takes multiple protocols from the upper layers and encapsulates them into the standard BLE packet format.

L2CAP

- It also performs fragmentation and recombination, a process by which it takes large packets from the upper layers and breaks them up into chunks to draw a simple comparison, L2CAP is similar to TCP, in that it allows a wide range of protocols to seamlessly coexist through a single physical link, each with a different packet size and requirements.

L2CAP

- Bluetooth Low Energy, the L2CAP layer is in charge or routing two main protocols
- The **Att**ribute Protocol (ATT)
- **S**ecurity **M**anager **P**rotocol (SMP)

ATT

- The Attribute Protocol (ATT) is a simple client/server stateless protocol based on attributes presented by a device. In BLE, each device is a client, a server, or both, irrespective of whether it's a master or slave. A client requests data from a server, and a server sends data to clients.
- Each server contains data organized in the form of attributes, each of which is assigned a **universally unique identifier** (**UUID**), a set of permissions, and finally, of course, a value.

ATT

- When a client wants to read or write attribute values from or to a server, it issues a **read** or **write request** to the server . The server will respond with the attribute value or an acknowledgement. In the case of a read operation, it is up to the client to parse the value and understand the data type based on the UUID of the attribute. On the other hand, during a write operation, the client is expected to provide data that is consistent with the attribute type and the server is free to reject the operation if that is not the case.

SMP

- The Security Manager (SM) is both a protocol and a series of security algorithms designed to provide the Bluetooth protocol stack with the ability to generate and exchange security keys, which then allow the peers to communicate securely over an encrypted link, to trust the identity of the remote device, and finally, to hide the public Bluetooth Address if required to avoid malicious peers tracking a particular device.

BLUETOOTH ADDRESS

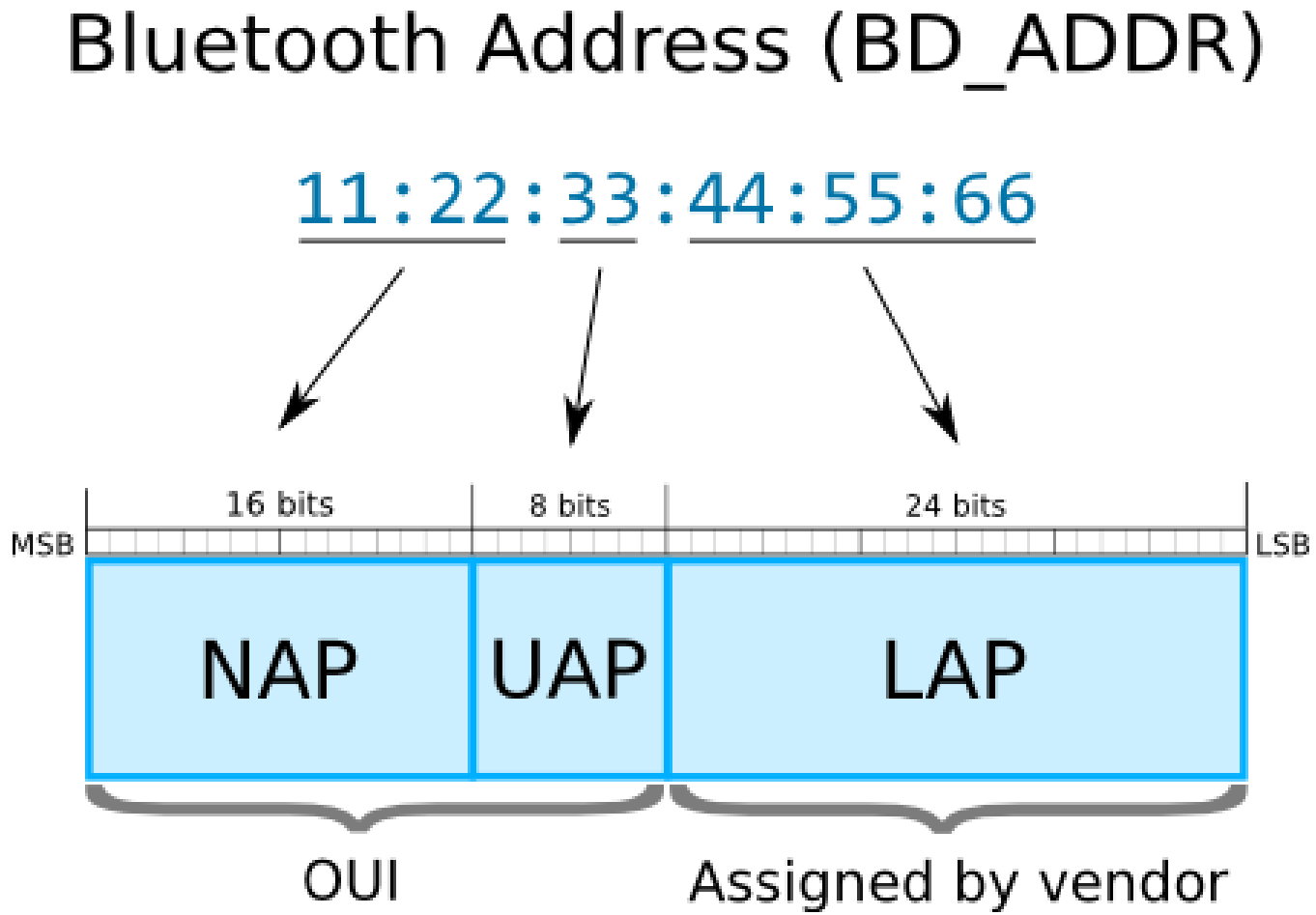
Bluetooth Device Address (or BD_ADDR) is a unique 48-bit identifier assigned to each Bluetooth device by the manufacturer.

Bluetooth Address is usually displayed as 6 bytes written in hexadecimal and separated by colons (example - 00:11:22:33:FF:EE).

The upper half of a Bluetooth Address (most-significant 24 bits) is so called Organizationally Unique Identifier (OUI). It can be used to determine the manufacturer of a device (Bluetooth MAC Address Lookup form). OUI prefixes are assigned by the Institute of Electrical and Electronics Engineers (IEEE).

Additionaly to identification, Bluetooth Device Address is used to determine the frequency hopping pattern in radio communication between Bluetooth devices.

BLUETOOTH ADDRESS



NAP

Non-significant Address Part (2 bytes). Contains first 16 bits of the OUI. The NAP value is used in Frequency Hopping Synchronization frames.

UAP

Upper Address Part (1 byte). Contains remaining 8 bits of the OUI. The UAP value is used for seeding in various Bluetooth specification algorithms.

LAP

Lower Address Part (3 bytes). This portion of Bluetooth Address is allocated by the vendor of device. The LAP value uniquely identifies a Bluetooth device as part of the Access Code in every transmitted frame.

The LAP and the UAP make the significant address part (SAP) of the Bluetooth Address.

Q&A

THANK YOU !!

TODO:

- Bluetoothctl
- Hcitool
- Obexftp
- Rfcomm
- hciconfig