Sunbeam Institute of Information Technology
Pune and Karad

Module – Internet of Things (IoT)

Trainer - Devendra Dhande

Email – devendra.dhande@sunbeaminfo.com

Bluetooth

- Bluetooth technology is a high-speed low powered wireless technology
- It is a specification (IEEE 802.15.1) for the use of low-power radio communications
- Wireless signals transmitted with Bluetooth cover short distances, typically up to 30 feet (10 meters).

- Bluetooth wireless technology was named after a Danish Viking and King, Harald Blatand; his last name means “Bluetooth” in English. (He is credited with uniting Denmark and Norway)
- Emerged from the task undertaken by Ericsson Mobile Communications in 1994 to find an alternative to the use of cables for communication between mobile phones and other devices.
- In 1998, the companies Ericsson, IBM, Nokia, and Toshiba formed the Bluetooth Special Interest Group (SIG) which published the 1st version in 1999.

How Bluetooth works?

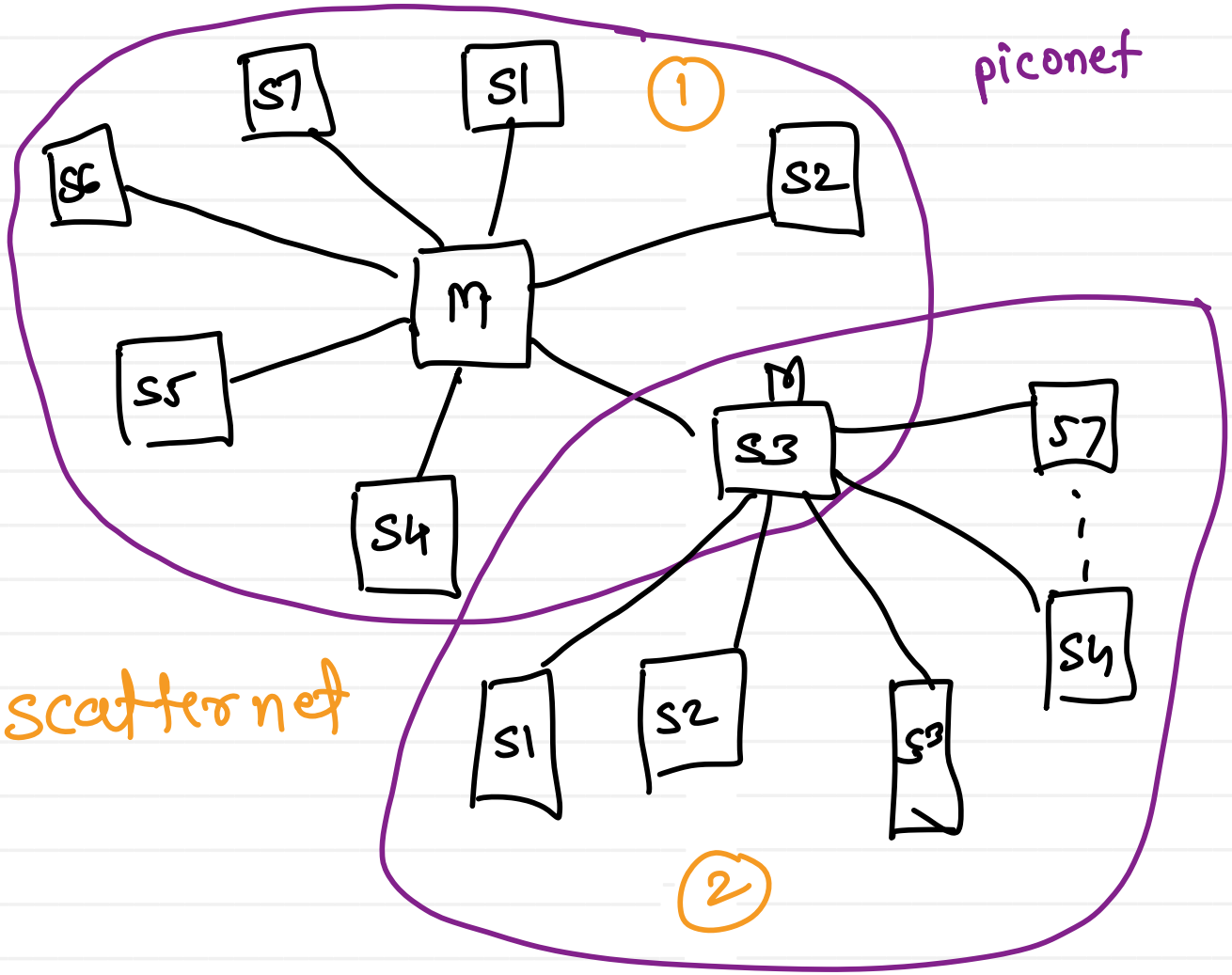
- Bluetooth Network consists of a minimum of 2 to a maximum of 8 BlueTooth peer devices Usually a single master and up to 7 slaves.
- A master is a device that initiates communication with other devices.
- The master device governs the communications link and traffic between itself and the slave devices associated with it.
- A slave device is a device that responds to the master device.
- Transmissions by slave devices are governed by the master device (i.e., the master device dictates when a slave device may transmit).
- A slave may only begin its transmissions in a time slot immediately following the time slot in which it was addressed by the master, or in a time slot explicitly reserved for use by the slave device.
- The frequency hopping sequence is defined by the Bluetooth device address (BD_ADDR) of the master device.
- The master device first sends a radio signal asking for a response from the particular slave devices within the range of addresses.
- The slaves respond and synchronize their hop frequency as well as a clock with that of the master device.

Bluetooth Architecture

- The Bluetooth architecture uses two networks like Piconet and Scatternet
- **Piconet Network**
  - Piconet includes one main node (master node) and seven secondary nodes (slave nodes).
  - There are eight active nodes totally which are arranged at a10 meters distance.
  - The message between these two nodes can be done one-to-one otherwise one-to-many.
  - Communication can be possible only among the master and slave but the communication like Slave-slave cannot be possible.
  - It also includes 255 parked nodes which are known as secondary nodes. These cannot communicate until it gets altered to the active condition.

- **Scatternet Network**
  - The formation of the Scatternet Network can be done through various piconets.
  - Slave in one piconet acts as a master in another piconet.
  - This type of node gets a message from the master within one piconet & transmits the message toward its slave in another piconet.
  - This kind of node is called a bridge-node. In two piconets, a station cannot be master.

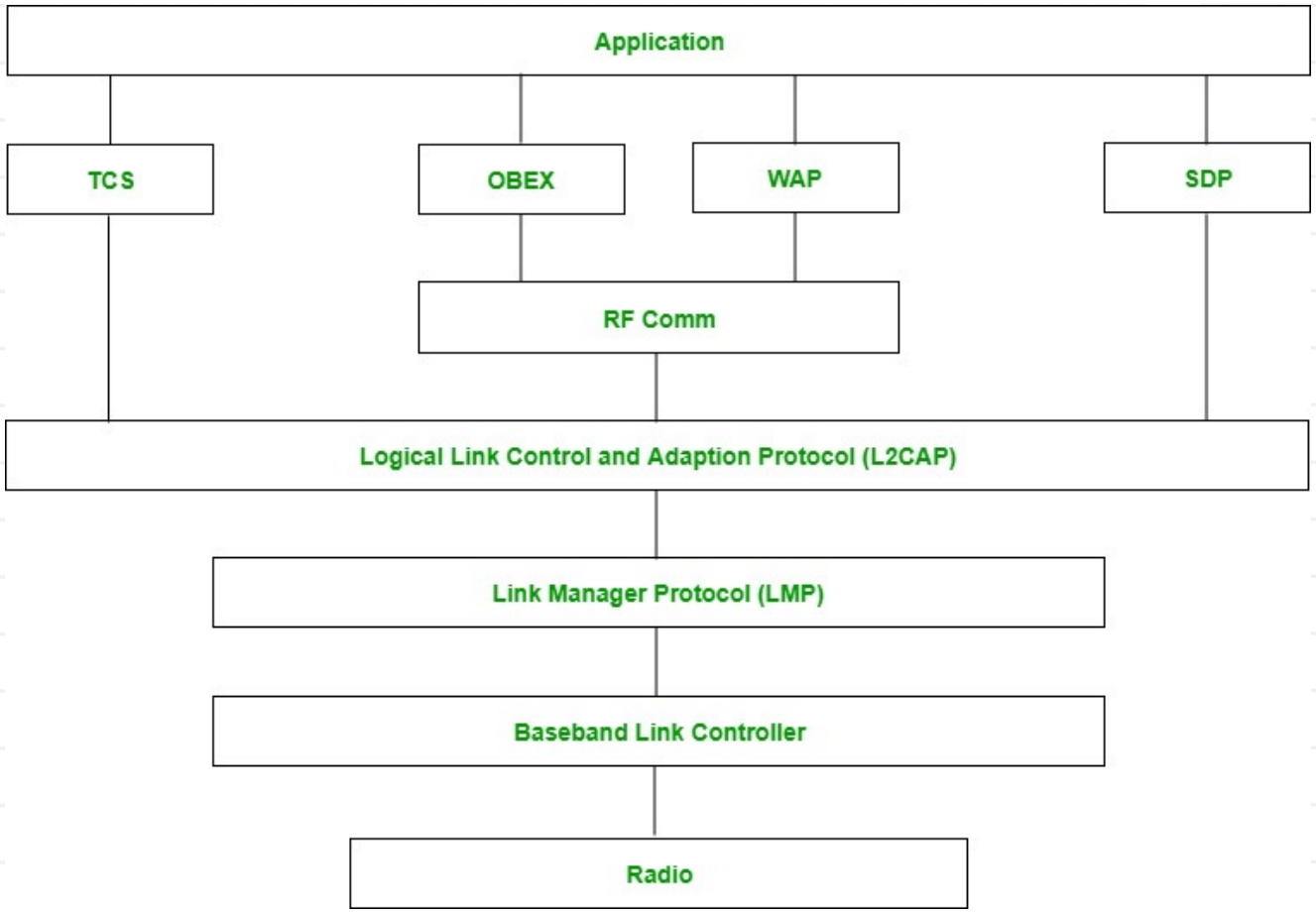
Bluetooth

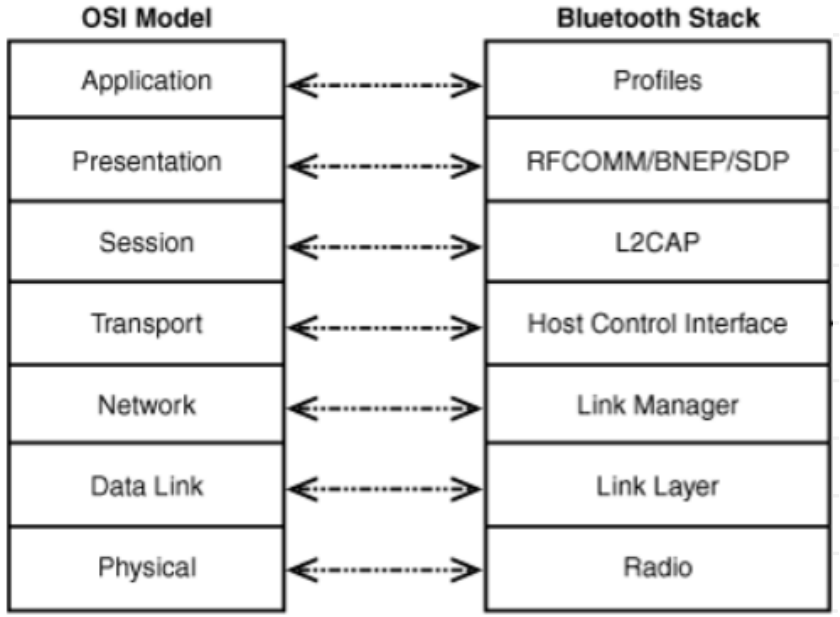


Bluetooth Specifications

- The **Bluetooth specifications** include the following.

- **Core Specifications**:
  - It defines the Bluetooth protocol stack and the requirements for testing and qualification of Bluetooth-based products.
- **The Profiles Specification**:
  - It defines usage models that provide detailed information about how to use the Bluetooth protocol for various types of applications.


Application
TCS
OBEX
WAP
SDP
RF Comm
Logical Link Control and Adaption Protocol (L2CAP)
Link Manager Protocol (LMP)
Baseband Link Controller
Radio


OSI Model
Bluetooth Stack
Application
Presentation
Session
Transport
Network
Data Link
Physical
Profiles
RFCOMM/BNEP/SDP
L2CAP
Host Control Interface
Link Manager
Link Layer
Radio

Bluetooth Core Specifications

- The core specifications of Bluetooth consists of 5 layers
- **Radio**: Radio specifies the requirements for radio transmission – including frequency, modulation, and power characteristics – for a Bluetooth transceiver.

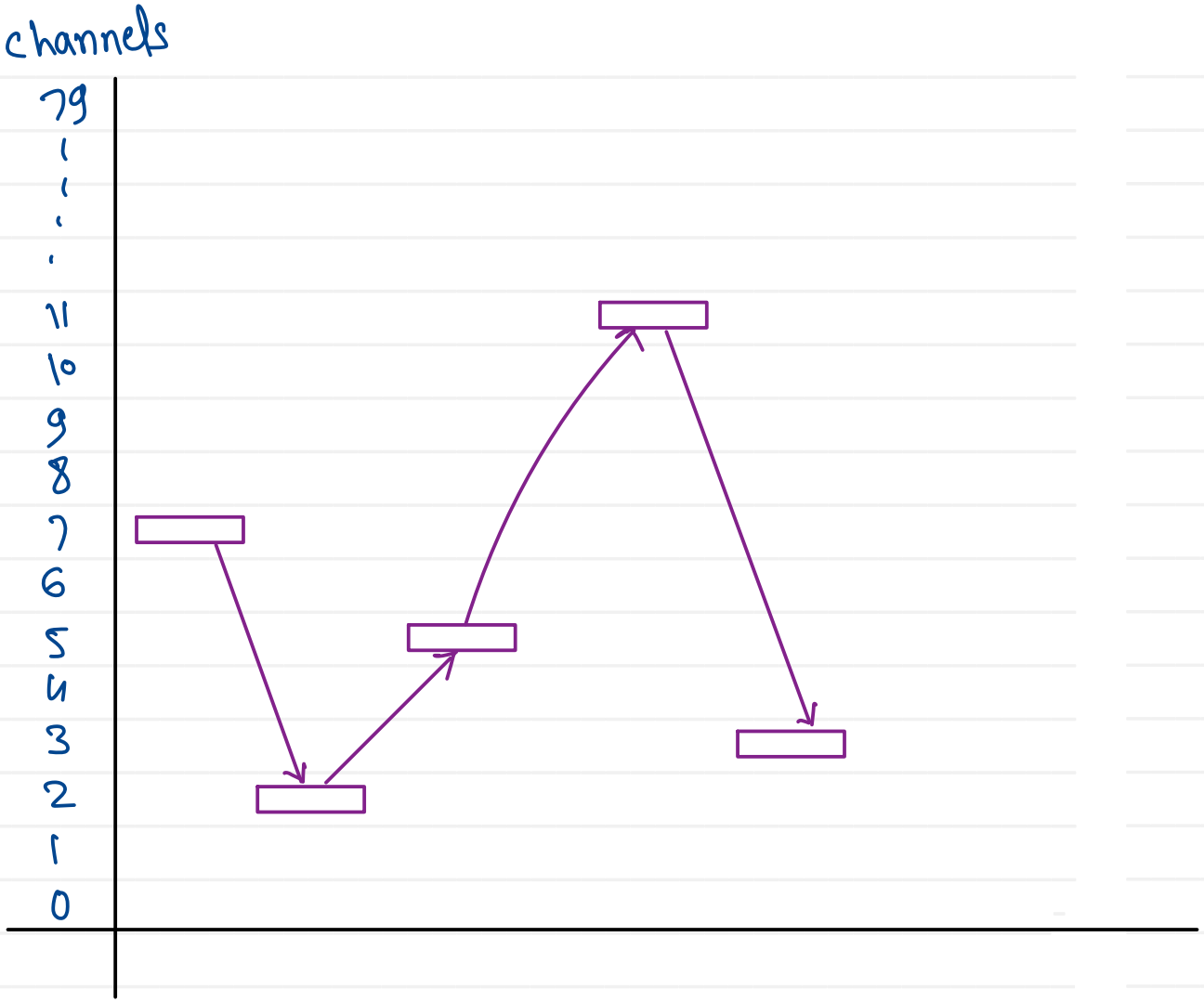
- **Baseband Layer**: It defines physical and logical channels and link types (voice or data); specifies various packet formats, transmit and receive timing, channel control, and the mechanism for frequency hopping (hop selection) and device addressing.It specifies point to point or point to multipoint links. The length of a packet can range from 68 bits (shortened access code) to a maximum of 3071 bits.

- **LMP- Link Manager Protocol (LMP):** It defines the procedures for link setup and ongoing link management.

- **Logical Link Control and Adaptation Protocol (L2CAP):** It is responsible for adapting upper-layer protocols to the baseband layer.

- **Service Discovery Protocol (SDP):** – Allows a Bluetooth device to query other Bluetooth devices for device information, services provided, and the characteristics of those services.

Bluetooth



- **Physical Layer (Radio Layer)**
  - **What it does**
    - Responsible for **actual wireless transmission**
    - Uses **radio waves** in the **2.4 GHz ISM band**
    - Handles modulation and transmission power
  - **Key points**
    - Range: ~10–100 meters (depends on class)
    - Uses **frequency hopping** to avoid interference
    - Data is transmitted as radio signals
  - This is the **lowest layer** where bits are transmitted over air.

- **Baseband Layer**
  - **What it does**
    - Controls **device discovery and connection**
    - Manages **time slots and hopping sequence**
    - Handles **packet formation**

  Functions
    - Device addressing
    - Error detection
    - Data packet framing
  - Converts raw radio signals into structured packets.

- **Link Manager Protocol (LMP)**
  - **What it does**
    - Manages the **link between Bluetooth devices**
    - Controls connection setup and termination
  - **Functions**
    - Authentication
    - Pairing
    - Encryption
    - Power management
  - Ensures a **secure and reliable link** between devices.

- **Host Controller Interface (HCI)**
  - **What it does**
    - Acts as a **bridge** between hardware and software
    - Provides a standard interface
  - **Functions**
    - Sends commands from host to controller
    - Receives events and data from controller
- Separates Bluetooth hardware from software implementation.

- **Logical Link Control and Adaptation Protocol (L2CAP)**
  - **What it does**
    - Provides **logical communication channels**
    - Adapts data for higher layers
  - **Functions**
    - Packet segmentation and reassembly
    - Multiplexing multiple connections
    - Quality of Service (QoS)
  - Makes Bluetooth suitable for different applications.

- *(Mainly used in Bluetooth Low Energy – BLE)*
- **Attribute Protocol (ATT)**
  - **What it does**
    - Defines how data is stored and accessed
    - Uses **attributes (key-value pairs)**
  - **Functions**
    - Read/write operations
    - Client–server model
  - Enables structured data exchange.

- **Generic Attribute Profile (GATT)**
  - **What it does**
    - Builds on ATT
    - Defines **how applications use BLE data**
  - **Key components**
    - Services
    - Characteristics
    - Descriptors
  - Used in **IoT, fitness bands, health devices**, etc.

- **Profiles Layer**
  - **What it does**
    - Defines **specific use cases**
    - Ensures interoperability
  - **Examples**
    - A2DP – Audio streaming
    - HID – Keyboard & mouse
    - Heart Rate Profile
    - File Transfer Profile
  - Profiles define **how devices should behave** for a given application.

- **Application Layer**
  - **What it does**
    - User-level applications
    - Uses Bluetooth profiles and APIs
  - **Examples**
    - Music streaming app
    - Smartwatch app
    - IoT sensor application
  - This is what the **end user interacts with**.

Step-by-Step Working of Bluetooth Communication

- **Step 1: Device Discovery**
  - Bluetooth device scans for nearby devices
  - Devices advertise their presence
- **Step 2: Pairing**
  - Devices exchange security information
  - Authentication and key generation occur
- **Step 3: Connection Establishment**
  - Logical link is created
  - Roles assigned (master/slave or central/peripheral)
- **Step 4: Data Transfer**
  - Application sends data
  - Data passes through:
    - Profile → GATT/ATT → L2CAP → HCI → Baseband → Radio
- **Step 5: Connection Termination**
  - Link is released
  - Resources are freed

Advantages of Bluetooth

- It removes the problem of radio interference by using a technique called ~~Speed~~ spread Frequency Hopping. This technique utilizes 79 channels of the particular frequency band, with each device accessing the channel for only 625 microseconds, i.e. the device must toggle between transmitting and receiving data from one-time slot to another.

- This implies the transmitters change frequencies 1,600 times every second, meaning that more devices can make full use of a limited slice of the radio spectrum. This ensures that the interference won't take place as each transmitter will be on different frequencies.

- The power consumption of the chip (consisting of a transceiver) is low, at about 0.3mW, which makes it possible for the least utilization of battery life.

- It is possible to use Bluetooth for both transferring data and verbal communication as Bluetooth can support data channels of up to 3 similar voice channels.

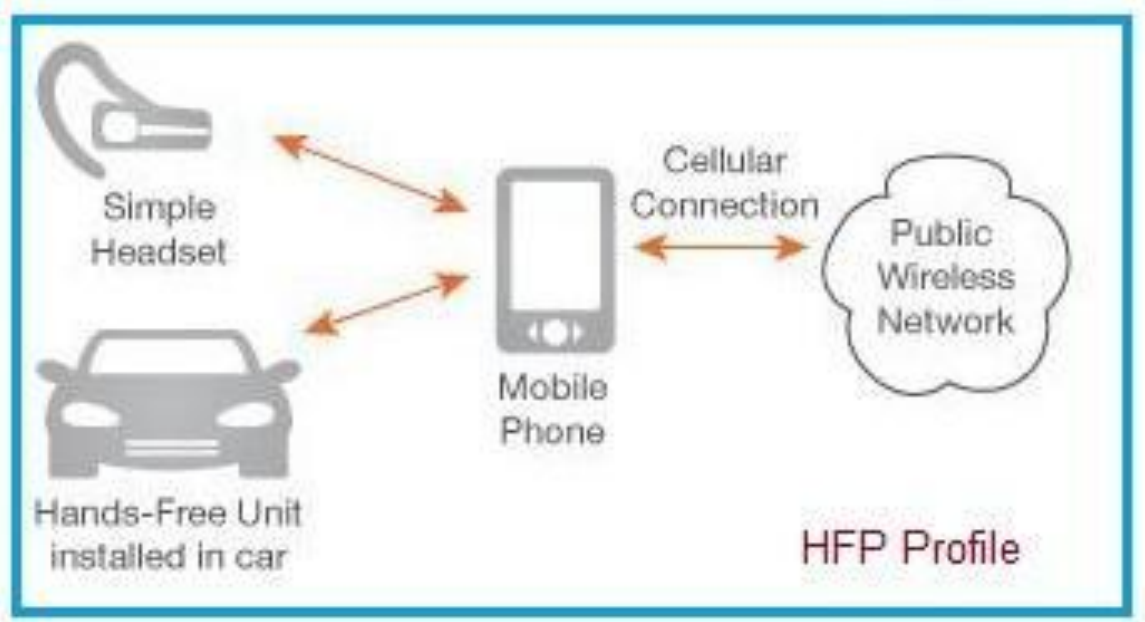
- It overcomes the constraints of the line of sight and one-to-one communication as in another mode of wireless communications like infrared.

Bluetooth profiles

- Bluetooth profiles serve various communication and entertainment needs.
- They ensure compatibility and smooth interactions between different Bluetooth-enabled devices.
- The choice of profile depends on the intended use case, such as
  - making calls
  - listening to music
  - controlling media playback
  - accessing contact and message data.

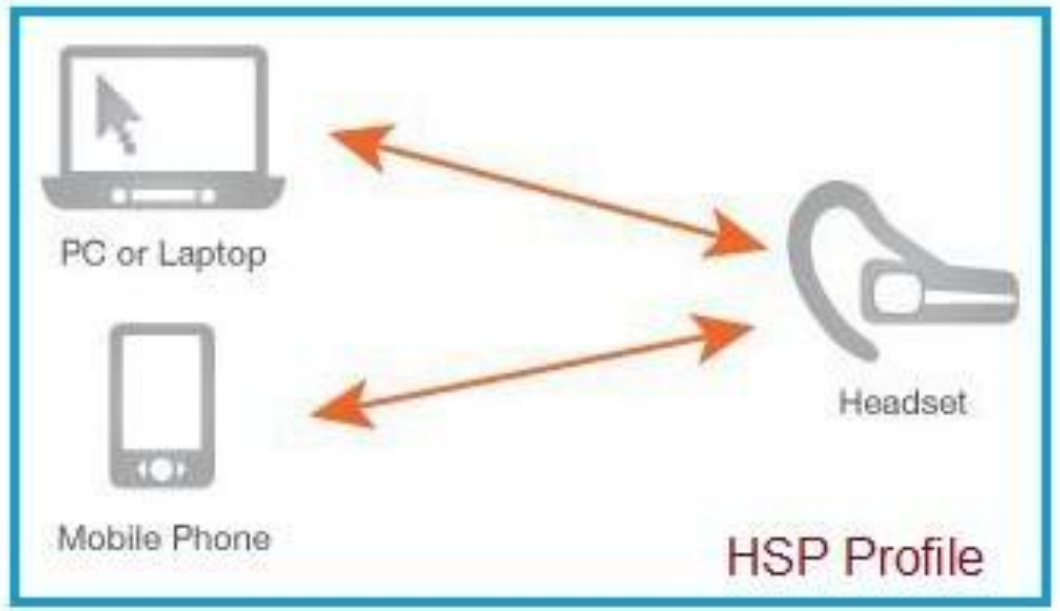
HFP Bluetooth Profile

- HFP is designed for hands-free calling in vehicles and headsets.
- It allows for voice calls and audio streaming. It provides call control functions such as answer, end, and reject calls
- HFP stands for Hands-Free Profile
- Audio is transmitted over a synchronous SCO channel. A separate data channel is used to control the audio stream.
- Other features include support for mono audio, sampling rates from 8 KHz to 16 KHz, and an audio delay of about 20 to 30 ms.
- The HFP Bluetooth profile supports audio codecs such as CVSD and mSBC.
- AT commands are used to control the mobile phone.



HSP Bluetooth Profile

- It enables voice transmission between a mobile phone and a wireless Bluetooth headset.
- The primary use case is mono voice calls using Bluetooth headsets.
- It supports limited audio streaming capabilities and is often used in mono Bluetooth headsets.
- HSP stands for Headset Profile.
- Audio is transmitted over a synchronous SCO channel.
- It has become obsolete due to the availability of the HFP profile.
- Other features of the HSP Bluetooth profile are mono audio, 8 KHz sampling, audio delay of 20 to 30 ms, and CVSD codec, etc.



A2DP Bluetooth Profile

- A2DP stands for Advanced Audio Distribution Profile.
- It enables stereo audio streaming between a music player (as source) and speakers/headphones (as sink).
- It provides high-quality audio streaming (stereo). It is ideal for music playback from devices to Bluetooth audio output devices.

AVRCP Bluetooth Profile

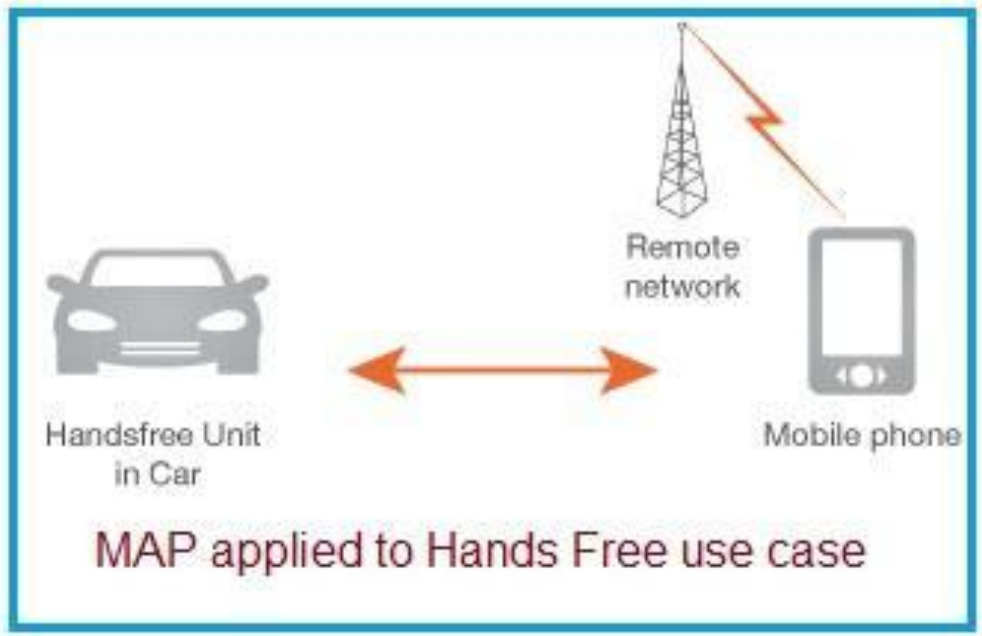
- AVRCP stands for Audio/Video Remote Control Profile.
- It enables an audio sink to control the audio sources' music player and streaming status.
- It uses a data channel to transmit control information between the audio controller and target.
- AVRCP v 1.5 enables advanced features like media browsing, audio player, and playlist management.
- Other features of the AVRCP Bluetooth profile are as follows:
  - Content browsing (artists, songs, etc.)
  - Content searching
  - Audio player management
  - Enables audio stream status control
  - Enables transmission of track, title, and other media information
  - Playlist management, etc.

PBAP Bluetooth Profile

- PBAP provides access to contact and address book information stored on a mobile device, typically used in car infotainment systems for accessing phone contacts and caller ID information.
- PBAP stands for Phone Book Access Profile.
- This profile enables the exchange of phone book objects between, for example, a smartphone and a car kit.
- It uses a data channel to transmit vCARDS over a Bluetooth connection.
- The other features of the PBAP Bluetooth profile are:
  - Download phone book items
  - Access call history
  - Access subscriber number information, etc

MAP Bluetooth Profile

- MAP stands for Message Access Profile.
- MAP allows access to text messages and email data on a paired device, often used in car infotainment systems for hands-free access to messages and emails.
- The primary use case is accessing text messages and email data while driving through the car's infotainment system.
- This profile enables the exchange of messages between a smartphone and a car kit.
- It uses a data channel to transmit SMS and email notifications and messages over Bluetooth.
- The other features of the MAP Bluetooth profile are as follows:
  - SMS and email notifications
  - Download of messages
  - Upload of messages
  - Browsing message folders
- Bluetooth MAP Version specifications are developed to allow the exchange of messages between devices. It is mostly used for automotive hands-free use.



Bluetooth profiles

Profile	Full Form	Description
HFP	Hands-Free Profile	Allows for hands-free calling in cars and headsets.
HSP	Headset Profile	Basic audio communication between headsets and phones.
A2DP	Advanced Audio Distribution Profile	High-quality audio streaming between devices.
AVRCP	Audio/Video Remote Control Profile	Allows remote control of media playback.
PBAP	Phone Book Access Profile	Access to contact and address book information.
MAP	Message Access Profile	Access to text messages and email.

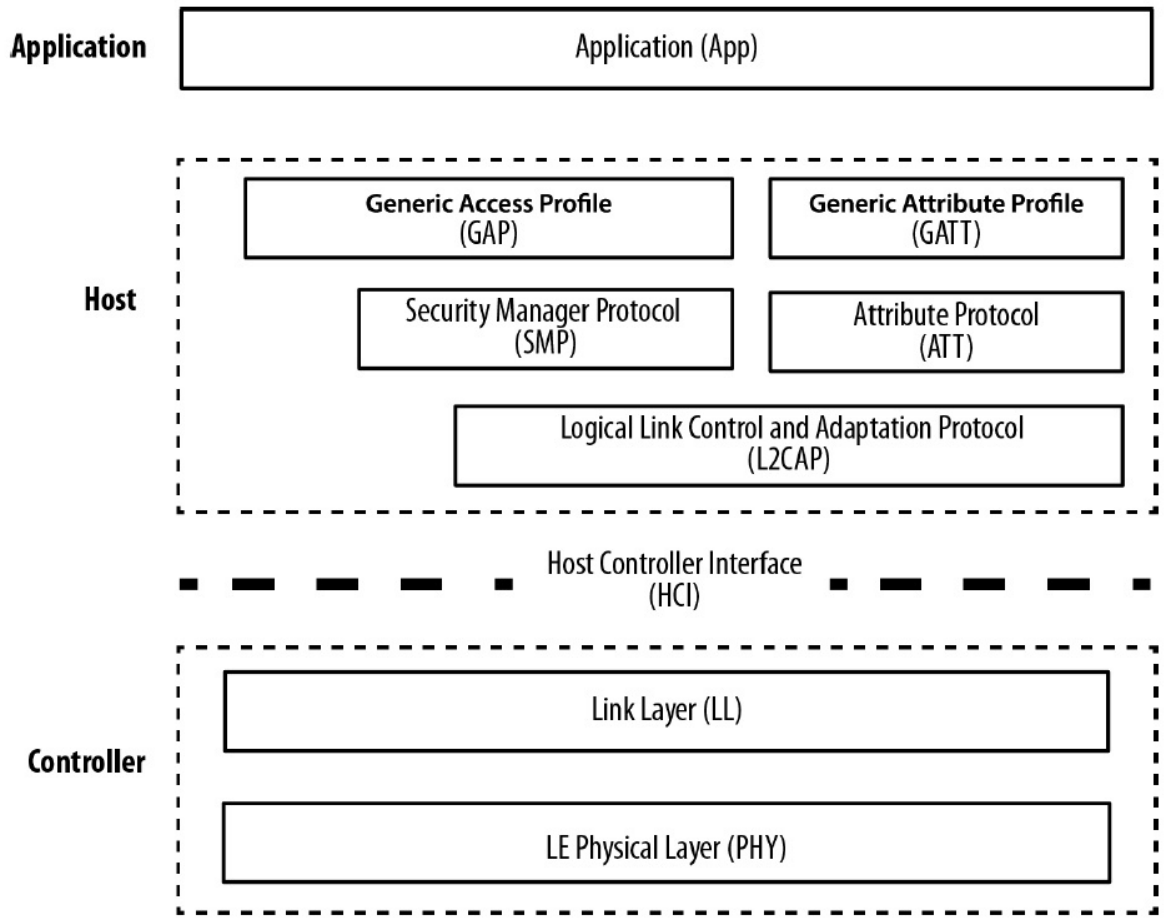
BTLE (Bluetooth Low Energy)

- a wireless personal area network technology designed and marketed by the Bluetooth Special Interest Group (Bluetooth SIG)
- Aimed at applications in the healthcare, fitness, beacons, security, and home entertainment industries.
- Compared to Classic Bluetooth, Bluetooth Low Energy is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.
- The original specification was developed by Nokia in 2006 under the name Wibree, which was integrated into Bluetooth 4.0 in December 2009 as Bluetooth Low Energy.
- Mobile operating systems including iOS, Android, Windows Phone and BlackBerry, as well as macOS, Linux, Windows 8, Windows 10 and Windows 11, natively support Bluetooth Low Energy.

BLE Architecture

- BLE architecture is divided into **three layers**:
- **1. Controller**
  - Physical Layer (PHY)
  - Link Layer (LL)
- **2. Host**
  - L2CAP
  - ATT
  - GATT
  - Security Manager (SM)
- **3. Application Layer**
  - User applications and profiles

- **BLE Device Roles**
  - **Central**: Initiates connection (e.g., smartphone)
  - **Peripheral**: Advertises and accepts connection (e.g., sensor)
  - **Broadcaster**: Sends advertising packets only
  - **Observer**: Scans for advertisements



BLE Communication Process (Step-by-Step)

- **Step 1: Advertising**
  - Peripheral sends advertising packets
  - Contains device information and services
- **Step 2: Scanning**
  - Central scans for advertising devices
- **Step 3: Connection Establishment**
  - Central sends connection request
  - Connection parameters are negotiated
- **Step 4: Data Exchange**
  - Data transferred using **GATT services and characteristics**
  - Read, Write, Notify, Indicate operations
- **Step 5: Disconnection**
  - Devices disconnect to save power

- **Security in BLE**
- BLE uses:
  - Pairing and bonding
  - AES-128 encryption
  - Secure key exchange
  - Privacy features
- Security Manager (SM) handles:
  - Authentication
  - Authorization
  - Encryption

- **Power Management in BLE**
  - BLE achieves low power by:
  - Sleeping most of the time
  - Short transmission bursts
  - Adjustable connection intervals
  - Low duty cycle operation

- **BLE Topologies**
  - **Point-to-Point** (Central ↔ Peripheral)
  - **Star topology** (One central, many peripherals)
  - **Mesh topology** (using Bluetooth Mesh)

BLE vs Classic Bluetooth

Feature	BLE	Classic Bluetooth
Power consumption	Very low	High
Data rate	Low–Medium	High
Latency	Low	Higher
Use case	IoT, sensors	Audio, media

- **Applications of BLE**
  - Fitness trackers
  - Smartwatches
  - Healthcare monitoring
  - Smart locks
  - Home automation
  - Asset tracking
- **Advantages of BLE**
  - Long battery life
  - Low cost
  - Widely supported
  - Secure and scalable
- **Limitations of BLE**
  - Limited data rate
  - Short range
  - Not ideal for large file transfer

Thank you!!!

Devendra Dhande

devendra.dhande@sunbeaminfo.com