Bluetooth (802.15)

CDAC Mumbai

What is Bluetooth?

- **Bluetooth** is a wireless technology standard for exchanging data over short distances (using short-wavelength radio transmissions in the ISM band from 2400–2480 MHz), from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecom vendor Ericsson in 1994

- Ratified as IEEE Standard 802.15 in 2002

Bluetooth Overview

- Motivation
  - In 1994 the Ericsson company wanted to connect mobile phones to other devices without using cables.

- Bluetooth Special Interest Group(SIG) Founded in 1998 by :

  Ericsson

  IBM

  Intel

  Nokia

  Toshiba

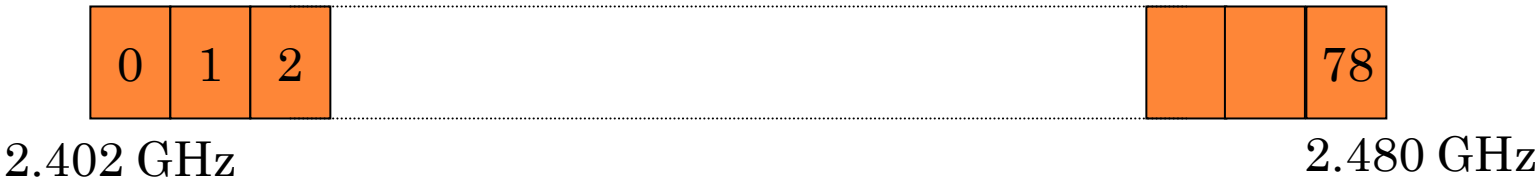
- which has more than 17,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics Created in order to promote, shape an define the specification and position Bluetooth in the market place
- Current specification : Bluetooth 3.0

Bluetooth Overview(History)

- Harald Blaatand II (translated Bluetooth)
- A Danish king that unified (conquered) Denmark and Norway in 940 – 981(Tenth Century).

Salient Features

- It is a Low cost, Low Power technology.
- The Bluetooth system is operating in the 2.4 GHz ISM (Industrial Scientific Medicine) band. The regulatory range of this frequency band is 2.400 – 2.4835 GHz.
- The Bluetooth radio accomplishes spectrum spreading by in 79 hops displaced by 1 MHz.



- 2Mhz of Lower Guard Band and 3.5 Mhz of Upper Guard Band.

Salient Features

- Achieve Secure Communication using frequency hopping with frequency hop rate of 1600 hops/sec (FHSS)
- **Frequency-hopping spread spectrum** (**FHSS**) is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels, using a pseudorandom sequence known to both transmitter and receiver.
- Radio modulation uses GFSK for Basic Rate(BR) of 1Mbps or DPSK for Enhanced data rate(EDR) of 2 to 3 Mbps.
  - Binary 1 is represented by positive frequency deviation and Binary 0 by negative frequency deviation in GFSK.
  - differentially encoded BPSK a binary '1' may be transmitted by adding 180° to the current phase and a binary '0' by adding 0° to the current phase.
- Operating range
  - Class 1 devices transmit Maximum of 100mW. The range of such devices is 100 Meters.
  - Class 2 devices transmit 10mW. The range is 50 Meters.
  - Class 3 devices transmit 1mW. The range is 10 Meters.

Salient Features

Data Rates:

- Asynchronous (data) and synchronous (voice) service available
- Bluetooth devices supports three Synchronous voice links and one asynchronous data link.
- For voice communication, 64Kbps data rate is used in both directions.
- For asynchronous data link , two types of channel defined with different data rates
  - Asymmetric channel: data rates are 723.2Kbps in one direction and 57.6 Kbps in other direction.
  - Symmetric Channel: data rate is 433.9 Kbps in both directions.

Bluetooth nodes states

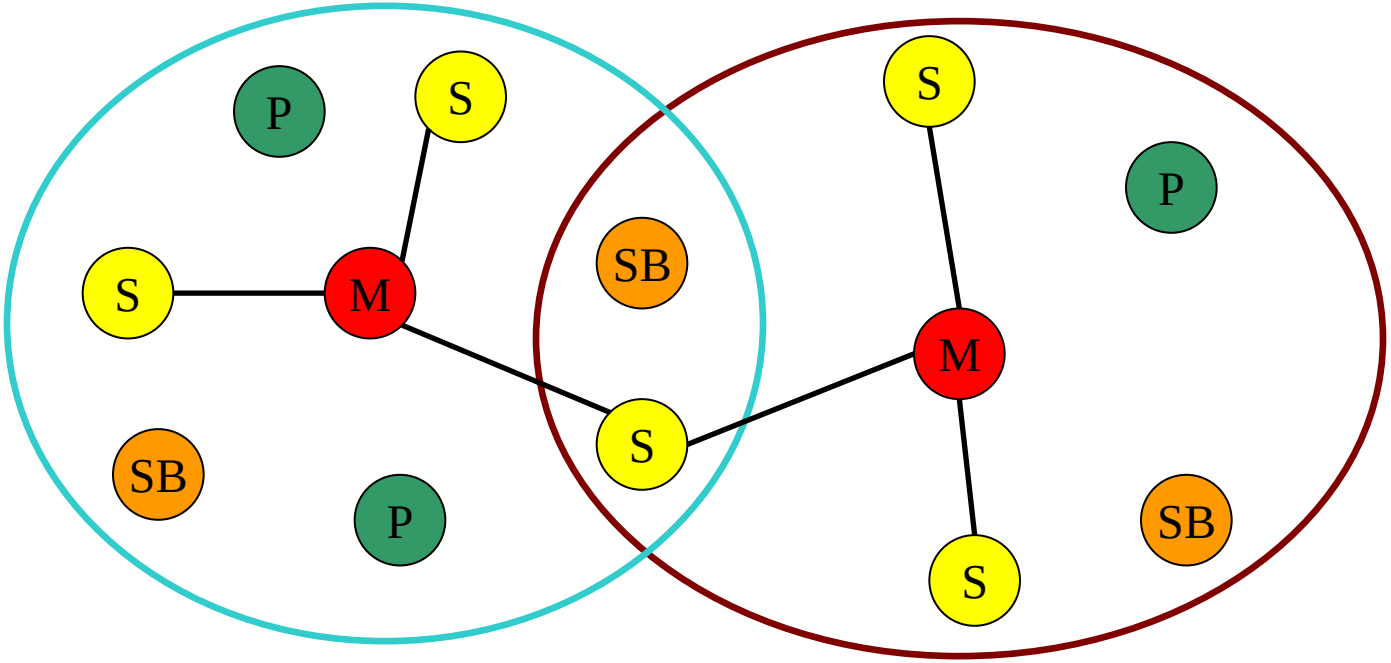
- Nodes can assume the role of **master** or **slave**
  - One or more slaves can connect to a master, forming the piconet
  - The master sets the hopping pattern for the piconet, and all slaves must synchronize to that pattern
  - Maximum of 7 slaves controlled by a master (3-bit addresses used)
- **Other operational states**
  - **Parked:** device does not participate in the piconet, but is known to the master and can be quickly reactivated
  - **Standby:** device does not participate in the piconet

Bluetooth Network Topology

- Piconet
  - Each piconet has one master and up to 7 simultaneous slaves
    - Master : device that initiates a data exchange.
    - Slave : device that responds to the master
- Scatternet
  - Linking of multiple piconets through the master or slave devices
  - Bluetooth devices have point-to-multipoint capability to engage in Scatternet communication.

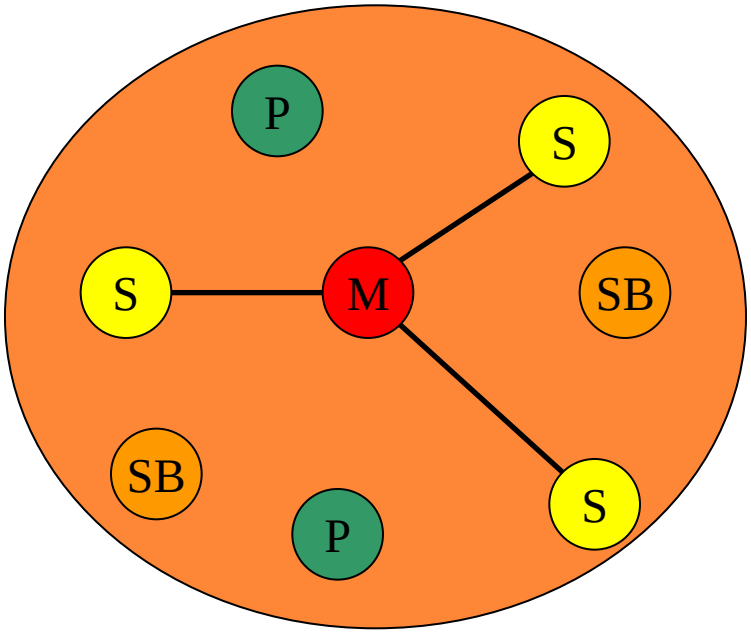
Scatter-net

- Devices can be slave in one piconet and master of another



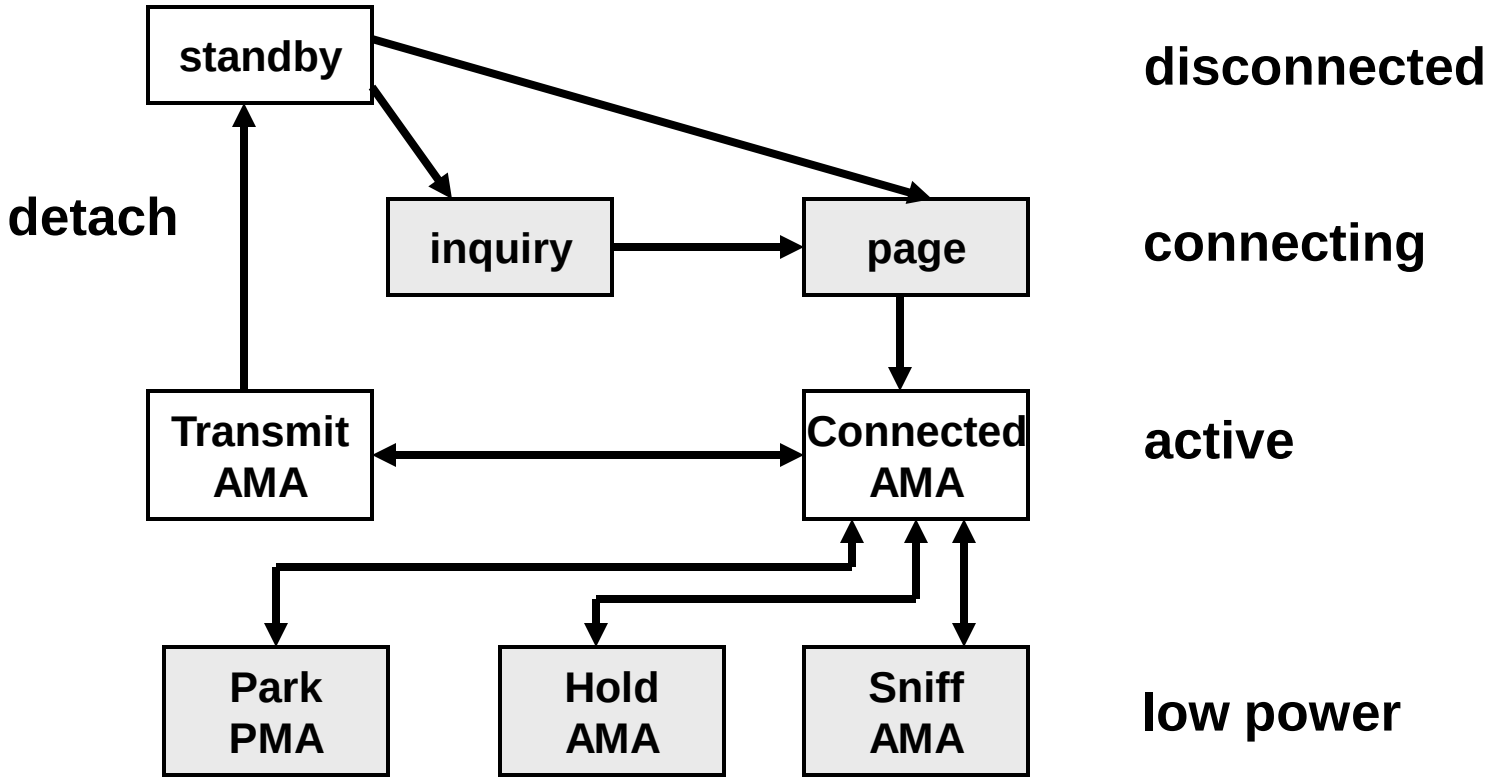
PICONET

- The master sets the hopping pattern for the piconet, and all slaves must synchronize to that pattern



M=Master P=Parked
S=Slave SB=Standby

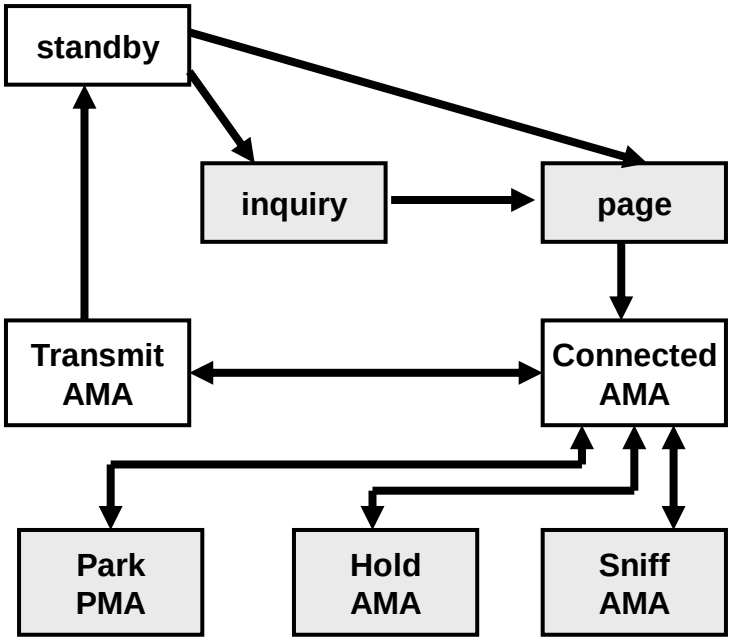
Establishing Network Connections



AMA = Active Member Address
PMA = Parked Member Address

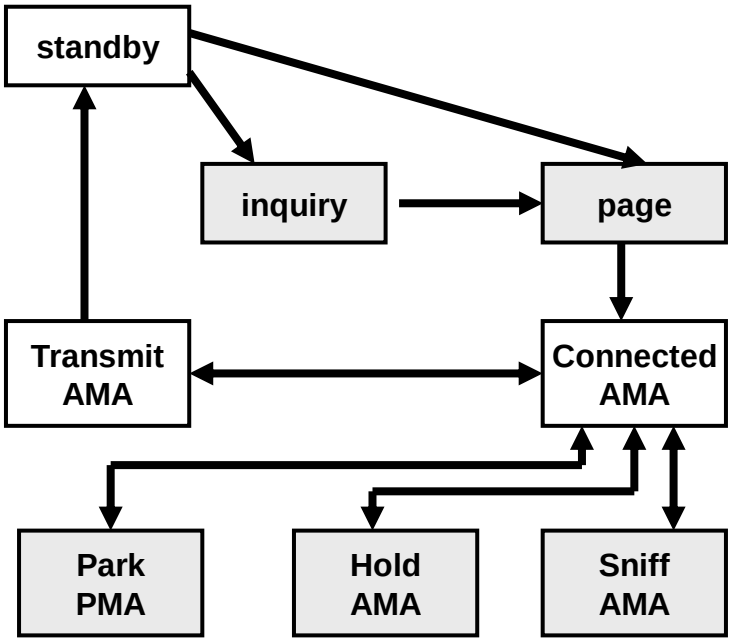
Connecting to a Piconet

- Device in standby listens periodically
- If a device wants to establish a piconet, it sends an inquiry, broadcast over all wake-up carriers
  - It will become the master of the piconet
  - If inquiry was successful, device enters page mode
- Devices in standby may respond to the inquiry with its device address
  - It will become a slave to that master



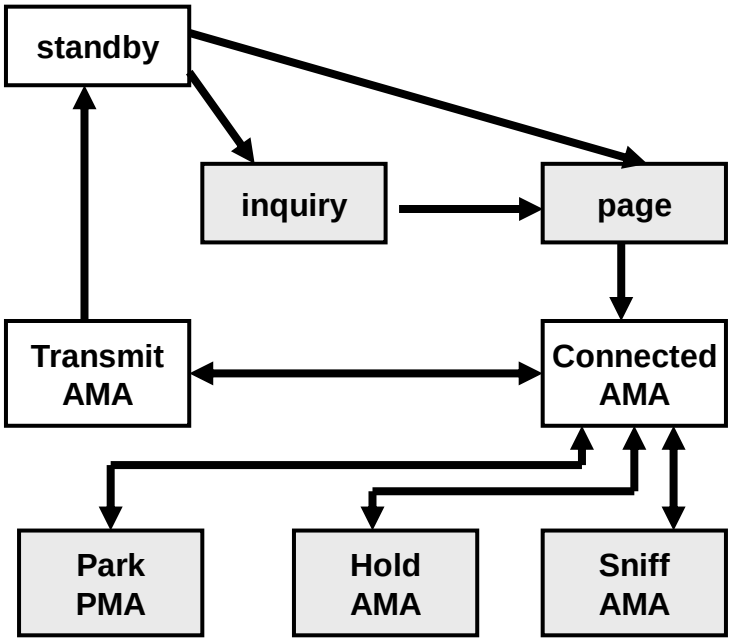
Page and Connect States

- After receiving a response from devices, the master can connect to each device individually
  - An AMA is assigned
  - Slaves synchronize to the hopping sequence established by the master
- In active state, master and slaves listen, transmit and receive
  - A disconnect procedure allows devices to return to standby mode



Low Power States

- Sniff state
  - Slaves listen to the piconet at a reduced rate
  - Master designates certain slots to transmit to slaves in sniff state
- Hold state
  - Slave stops receiving data traffic for a specific amount of time, so other devices in the piconet, can use the channel.
- Park state
  - Slave releases its AMA
  - Still FH synchronized and wakes up periodically to listen to beacon

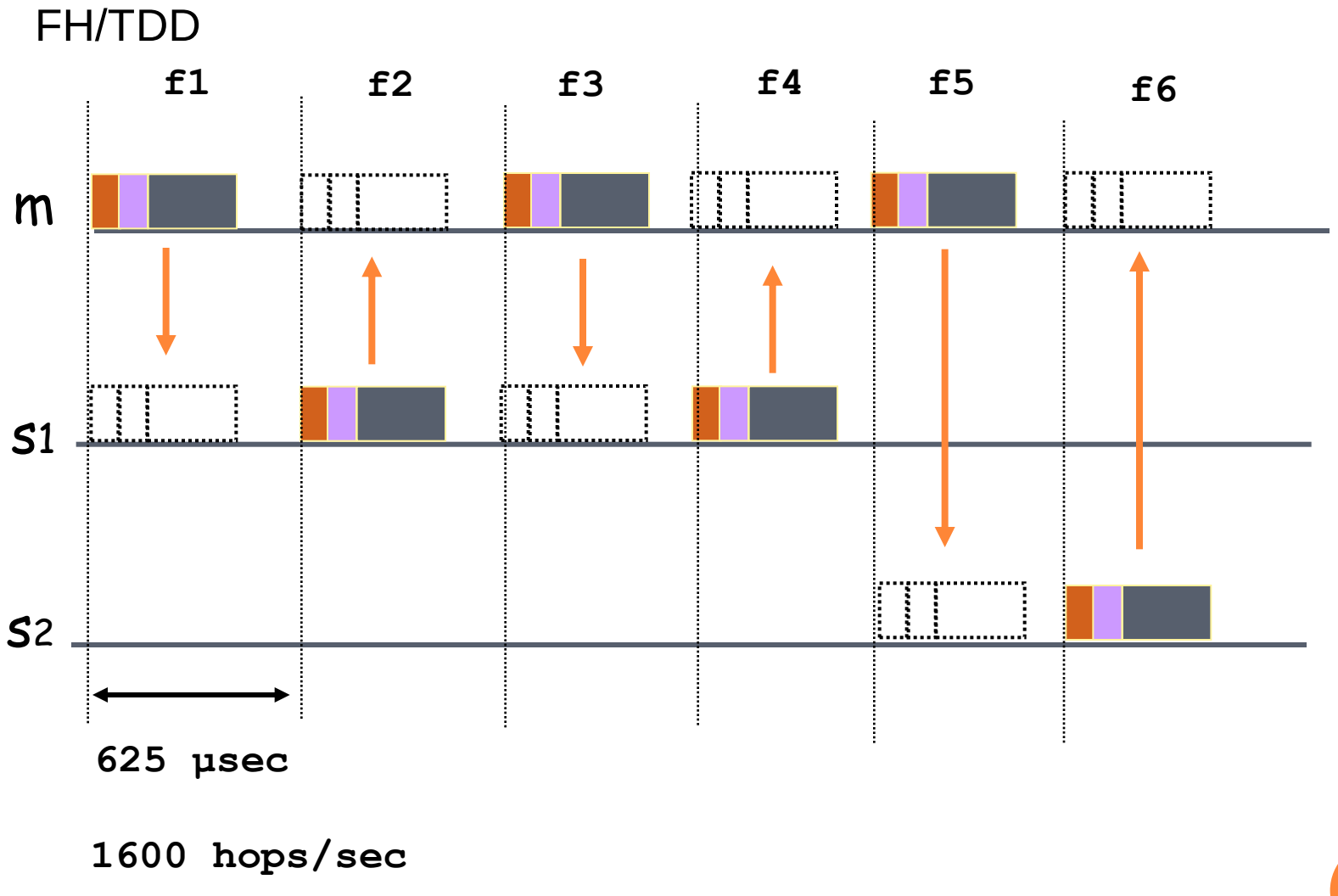


Bluetooth Addressing

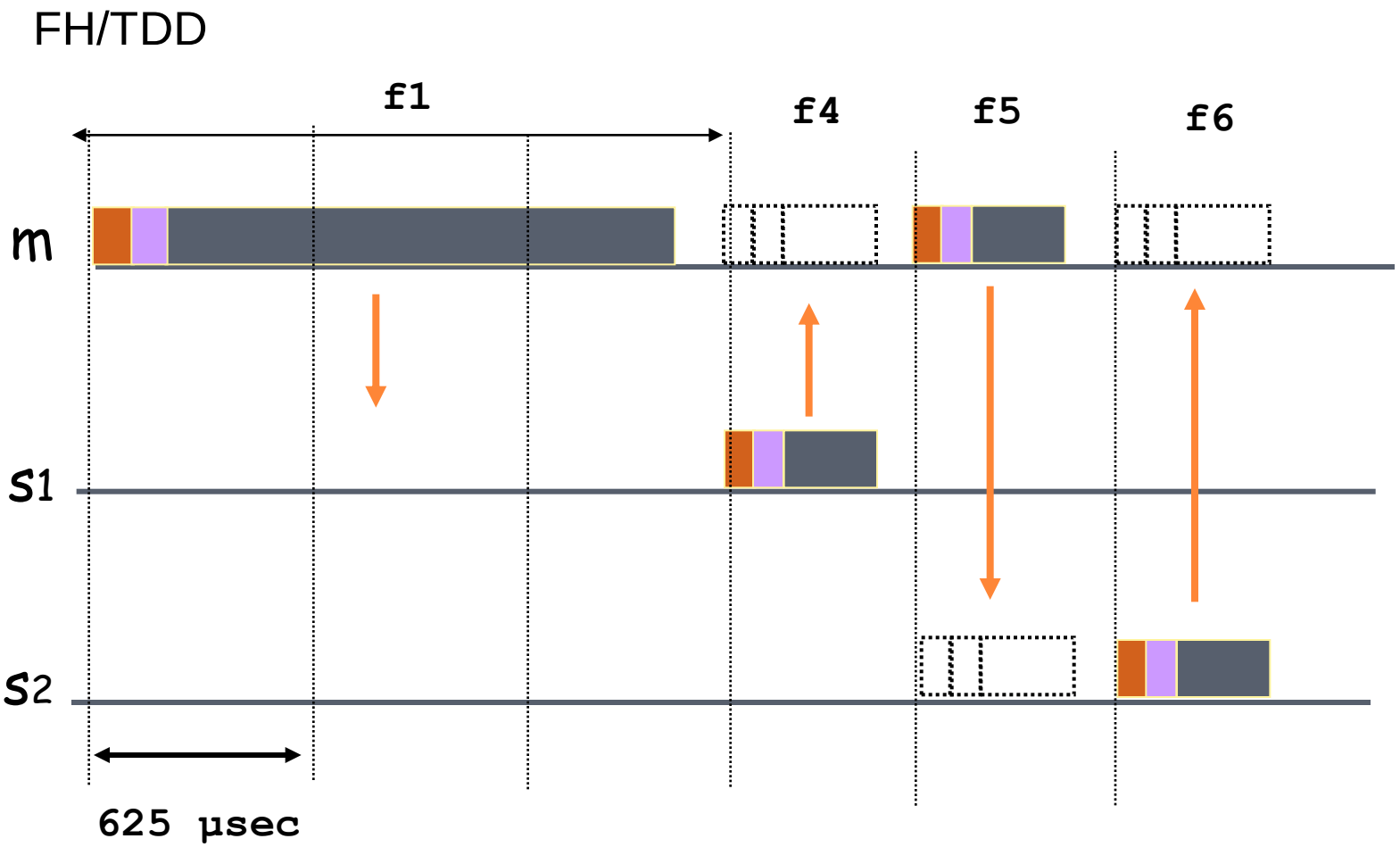
- Bluetooth module is given a 48-bit MAC address containing three fields:
- **Bluetooth device address (BD_ADDR)**
  - LAP(Lower Address Part) – 24 bits
  - UAP(Upper Address Part) – 08 bits
  - NSP(Non Significant Part) –16 bits

  This Address is Assigned by Manufacturer and consist of Company ID and Company assigned number.
- **Active Member address (AM_ADDR)**
  - 3 bits active slave address
  - all zero broadcast address
- **Parked Member address (PM_ADDR)**
  - 8 bit parked slave address

PICONET CHANNEL

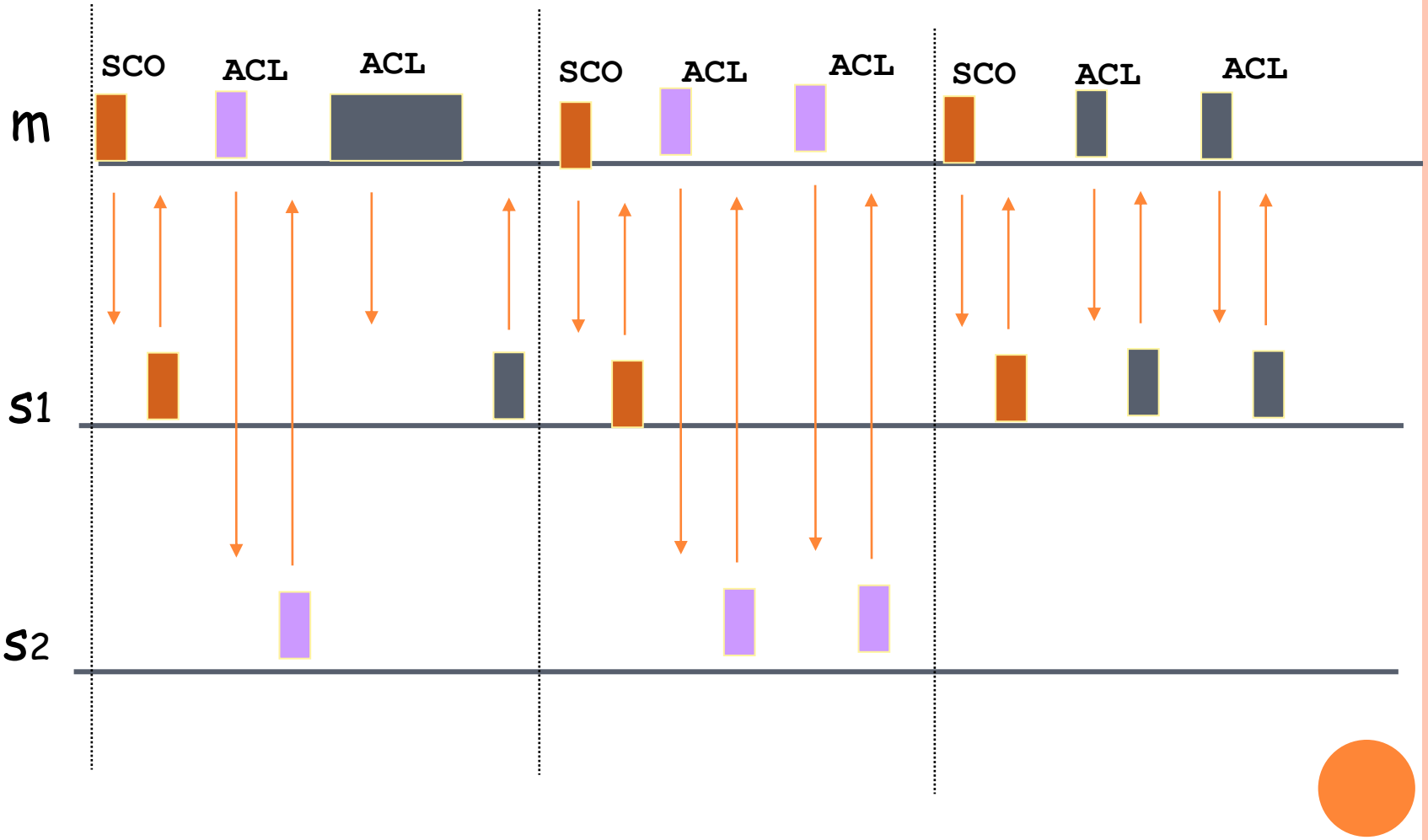


Multi slot packets



Data rate depends on type of packet

Mixed Link Example

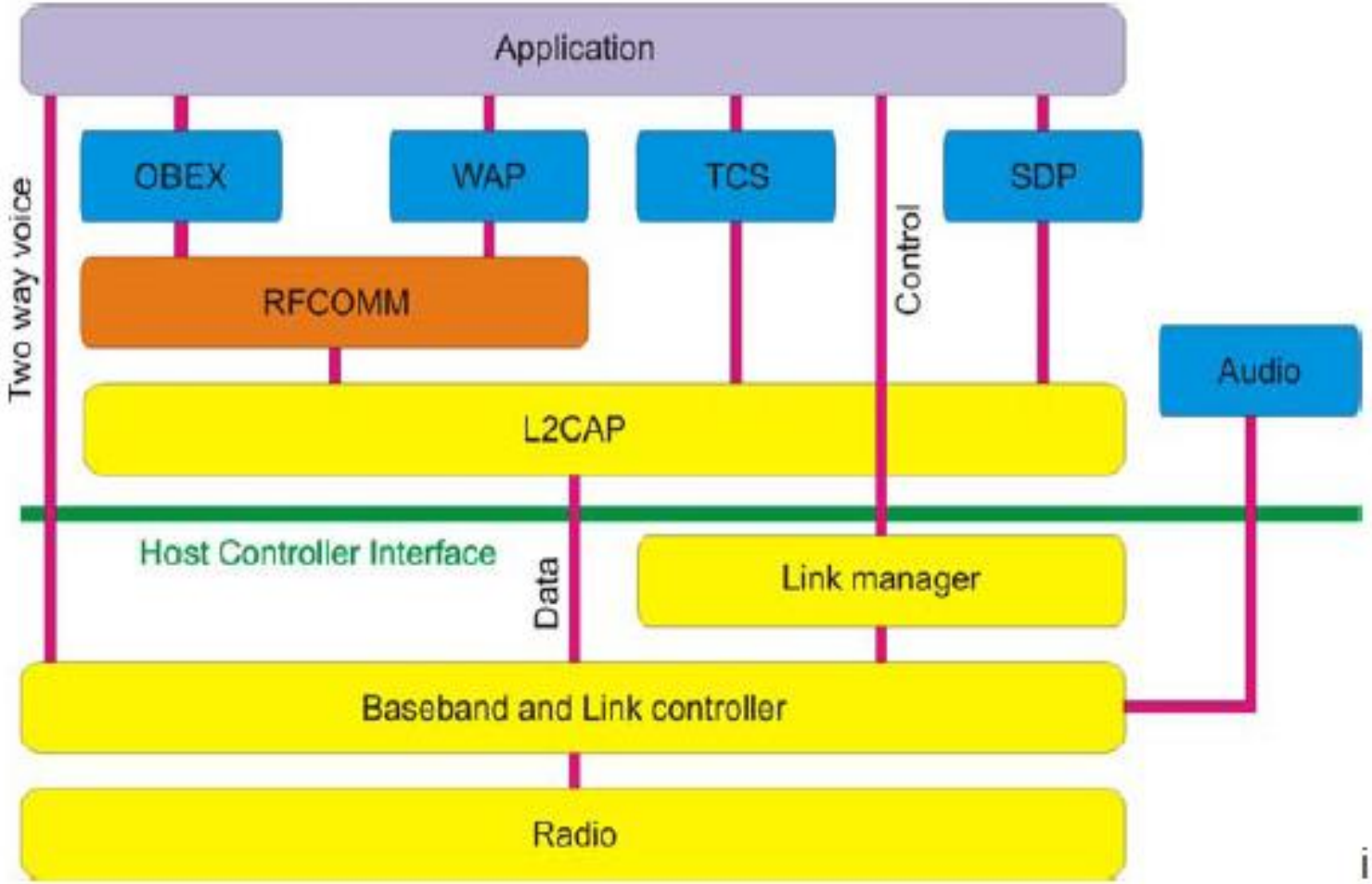


Asynchronous Connection less & Synchronous Connection Oriented

- Used for Data
- ACL uses Packet Switching for data
- Data comes from L2CAP layer on the sending side and delivered to the L2CAP on the receiver side
- Frame can be lost and may need to retransmitted

- Used for Voice
- SCO uses Circuit Switching for voice
- Their channel is allocated a fixed slot in each direction
- Frame send are never retransmitted
- Forward error correction can be used to provide high reliability
- Can have up to 3 slave SCO links with its master
- Each SCO links can transmitted one 64000 bps PCM audio channel

Bluetooth Protocol Stack



Radio Layer and Baseband Layer

- The Bluetooth module contains the hardware and firmware that implements the Radio, baseband, and Link management protocols.

- The Radio layer
  - corresponds to the physical layer
  - deals with radio transmission and modulation
- The Baseband layer
  - is used for establishing the links between devices based on the type of services required.
  - ACL for data services and SCO for voice services.
  - also takes care of addressing and managing the different states of the Bluetooth device.

Link Manager Protocol(LMP)

- The three layers – **Radio , Link controller and Link manager**- will be on Bluetooth module attached to the device.
- Link Manager Protocol (LMP) is used to setup and control links using LMP messages.
- LMP messages having higher priority compared to data.

Link Manager Protocol(LMP)

- The functions of the LMP are
  - Authentication
  - Encryption
  - Clock Synchronization
  - Switching Master/Slave role
  - Name request
  - Detach
  - Hold mode
  - Park mode
  - Request SCO link after ACL link is established
  - Multi-slot packet control
  - Link Supervision

Host Controller Interface, Logical Link Control and Adaptation Protocol

- The Host Controller Interface (HCI) provides a common interface between the Bluetooth host device (Laptop) and the Bluetooth module.
- Three interfaces are defined to get HCI packets from host to the Bluetooth module: a) USB b) UART

- L2CAP layer is only for ACL links. It does not support SCO links.
- L2CAP data packets can be up to 64 Kb long and does not support multicasting.
- The Function of L2CAP layer are
  - Protocol Multiplexing
  - Segmentation and reassembly

Service Discovery Protocol(SDP)

- This protocol is used for discovering the services offered by a device and to determine the characteristics of these services in the piconet.
- The SDP offers the following services
  - A device can search for the service needed by it in a piconet.
  - Browsing of services.
  - Discovery of new services when devices enter in the radio range of other devices.
  - Mechanism to find out when a service becomes unavailable when the device goes out of radio range.
  - Retrieve attributes that detail how to connect to the service

RFCOMM

- RFCOMM is a simple transport protocol which emulates the serial communication(RS-232 port) and used for example in a laptop to printer connection.
- RFCOMM provides compatibility with legacy applications that uses the serial port.
- It supports two types of devices
  - Type I : devices are communication endpoints such as computers and printers
  - Type II: devices are part of communication segments such as modems.

Telephony Control Protocol Specs. (TCS)

- L2CAP handles the signaling required for establishing voice connection through Telephony Control Protocol Specification.
- TCS defines call control signaling for establishing speech and data calls between Bluetooth devices and mobility management procedures

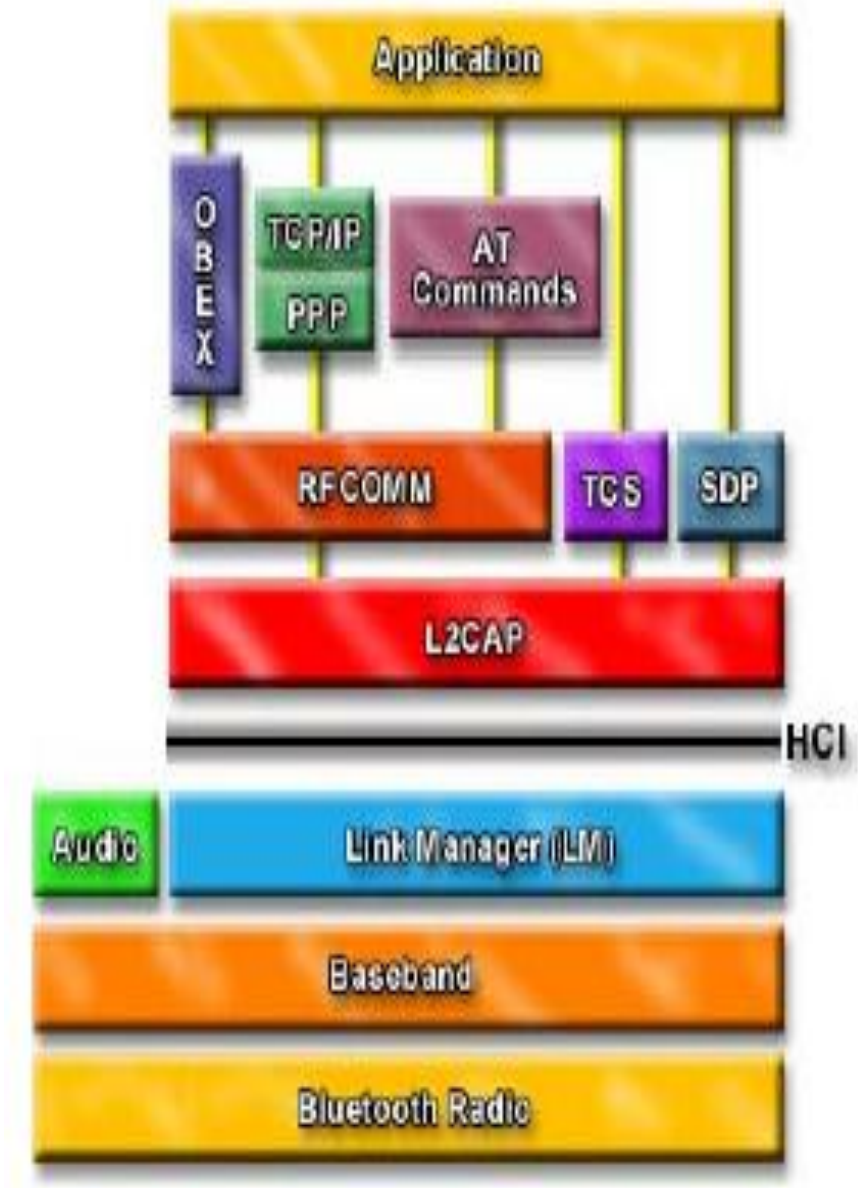
COMPLETE PROTOCOL STACK

A number of other protocols are available for different applications,
for example:

OBEX(Object exchange protocol) used for file transfer.

TCP/IP
Used for internet applications.

AT commands to support user terminal control.
For example, entering a PIN for Authentication



Bluetooth On Linux using BLUEZ

- Command Summary:
  1) hciconfig or hciconfig -a
  2) hciconfig hci0 up
  3) hcitool scan
  4) hcitool info 00:04:0E:81:06:FD