Bluetooth

What is Bluetooth?

- A **cable-replacement** technology that can be used to connect almost any device to any other device
- Radio interface enabling electronic devices to communicate wirelessly via short range (10 meters) ad-hoc radio connections
- a standard for a **small , cheap radio chip to be plugged into computers, printers, mobile phones, etc**

What is Bluetooth?

- Uses the radio range of 2.45 GHz
- Theoretical maximum bandwidth is 1 Mb/s
- Several Bluetooth devices can form an ad hoc network called a “piconet”
  - In a piconet one device acts as a master (sets frequency hopping behavior) and the others as slaves
  - Example: A conference room with many laptops wishing to communicate with each other

History

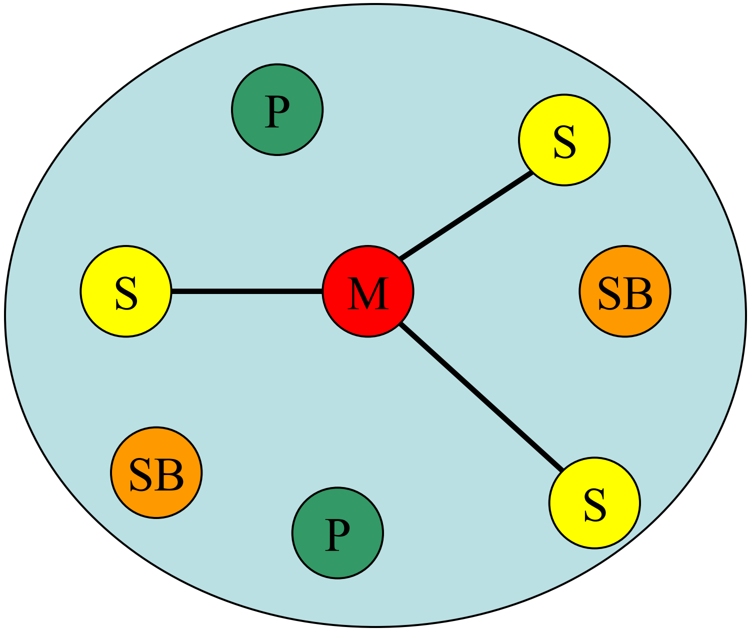
- Harald Bluetooth : 10th century Danish King, managed to unite Denmark and Norway
- Bluetooth SIG (Special Interest Group) :
  - Founded in 1998 by : Ericsson, Intel, IBM, Toshiba and Nokia
  - Currently more than 2500 adopter companies
  - Created in order to promote, shape an define the specification and position Bluetooth in the market place Current specification : Bluetooth 2.1

Bluetooth Architecture

- 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.

Piconet

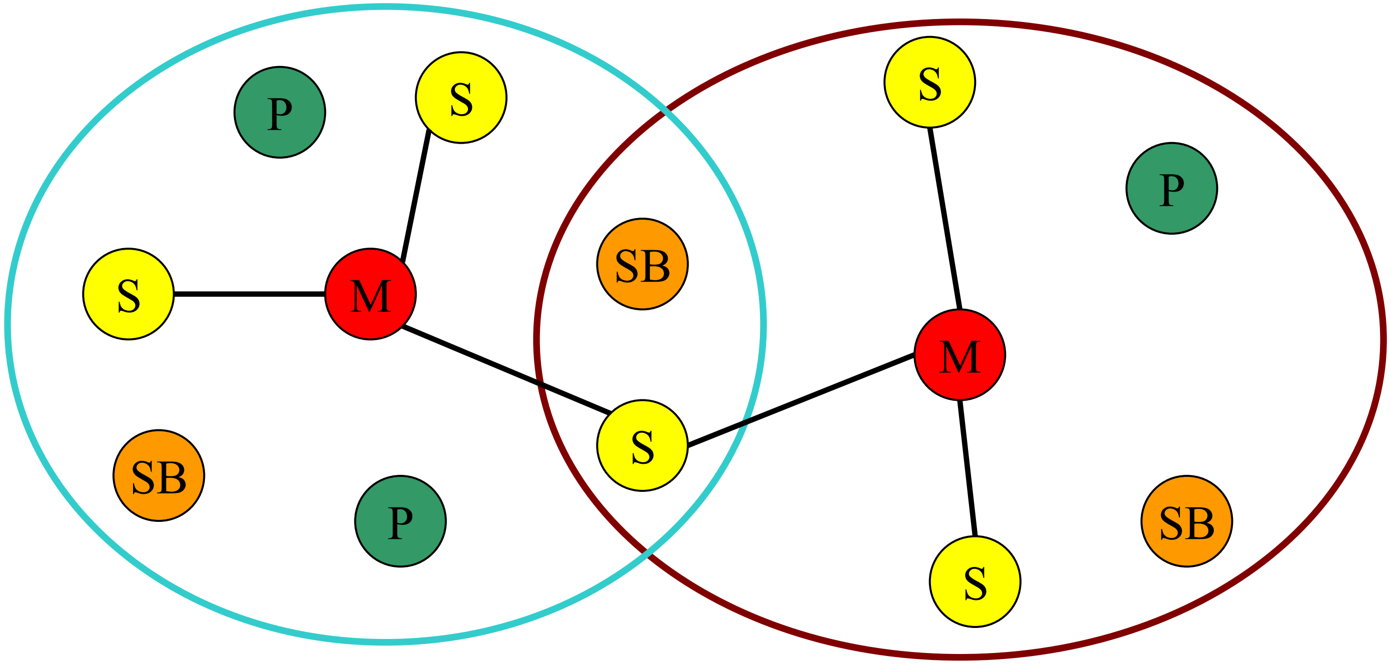
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
- Non-piconet devices are in standby



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

Scatternet

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



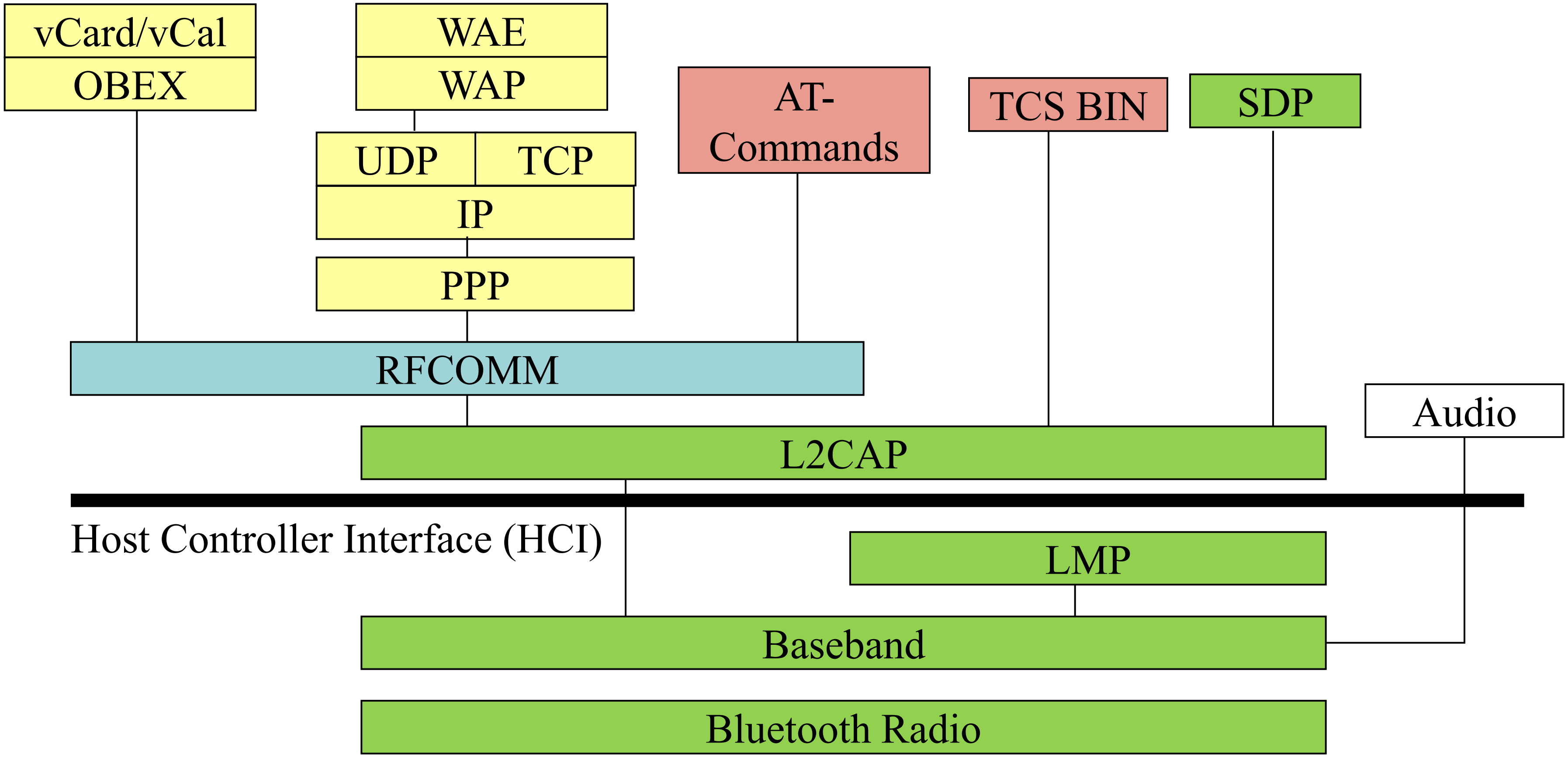
Physical links

- Between master and slave(s), different types of links can be established. Two link types have been defined:
  - Synchronous Connection-Oriented (SCO) link
  - Asynchronous Connection-Less (ACL) link

Physical links

- Synchronous Connection Oriented (SCO)
  - Support symmetrical, circuit-switched, point-to-point connections
  - Typically used for voice traffic.
  - Data rate is 64 kbit/s.
- Asynchronous Connection-Less (ACL)
  - Support symmetrical and asymmetrical, packet-switched, point-to-multipoint connections.
  - Typically used for data transmission .
  - Up to 433.9 kbit/s in symmetric or 723.2/57.6 kbit/s in asymmetric

Bluetooth Protocol Stack



vCard/vCal

OBEX

WAE

WAP

UDP

TCP

IP

PPP

AT-Commands

TCS BIN

SDP

RFCOMM

Audio

L2CAP

Host Controller Interface (HCI)

LMP

Baseband

Bluetooth Radio

🟩 Bluetooth Core Protocol	🟦 Cable Replacement Protocol
🟨 Adopted Protocol	🟥 Telephony Protocol

Bluetooth Protocol Stack

- **Bluetooth Radio** : specifics details of the air interface, including frequency, frequency hopping, modulation scheme, and transmission power.

- **Baseband**: concerned with connection establishment within a piconet, addressing, packet format, timing and power control.

- **Link manager protocol (LMP)**: establishes the link setup between Bluetooth devices and manages ongoing links, including security aspects (e.g. authentication and encryption), and control and negotiation of baseband packet size

Bluetooth Protocol Stack

- **Logical link control and adaptation protocol (L2CAP)**: adapts upper layer protocols to the baseband layer. Provides both connectionless and connection-oriented services.

- **Service discovery protocol (SDP)**: handles device information, services, and queries for service characteristics between two or more Bluetooth devices.

- **Host Controller Interface (HCI):** provides an interface method for accessing the Bluetooth hardware capabilities. It contains a command interface, which acts between the Baseband controller and link manager

Bluetooth Protocol Stack

- **TCS BIN (Telephony Control Service)**: bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices.

- **OBEX(OBject EXchange)** : Session-layer protocol for the exchange of objects, providing a model for object and operation representation

- **RFCOMM**: a reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol

- **WAE/WAP**: Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

Connection Establishment States

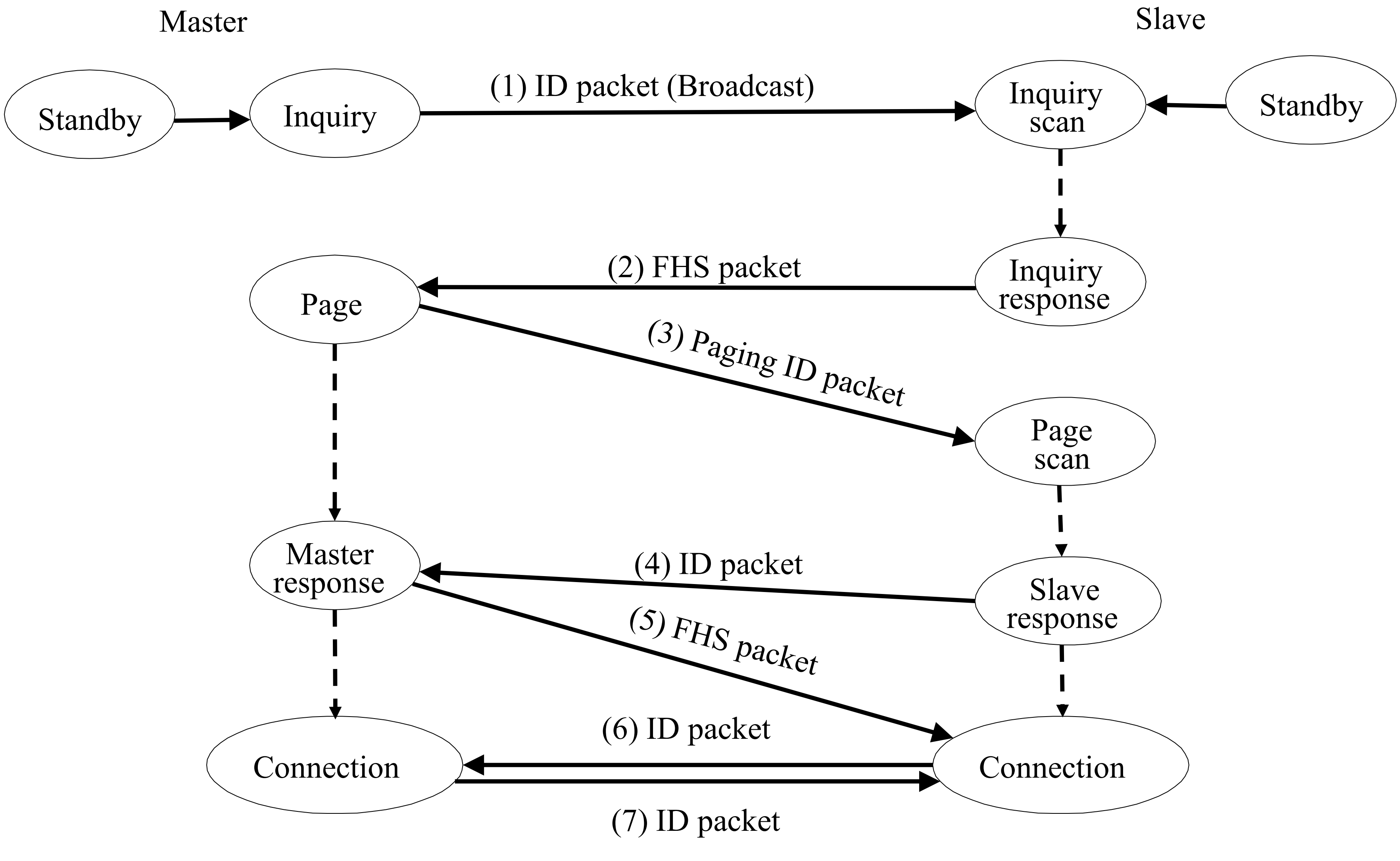
- **Standby**
  - State in which Bluetooth device is inactive, radio not switched on, enable low power operation.
- **Page**
  - Master enters page state and starts transmitting paging messages to Slave using earlier gained access code and timing information.
- **Page Scan**
  - Device periodically enters page state to allow paging devices to establish connections.

Connection Establishment States

- **Inquiry**
  - State in which device tries to discover all Bluetooth enabled devices in the close vicinity.

- **Inquiry scan**
  - Most devices periodically enter the inquiry scan state to make themselves available to inquiring devices.

Inquiry and Page



Bluetooth Security

- There are three modes of security for Bluetooth access between two devices.
  - non-secure
  - service level enforced security
  - link level enforced security
- Device security level
  - Trusted
  - untrusted
- Service security level
  - Authorization and Authentication
  - Authentication only
  - Open to all devices

Bluetooth Security

- The following are the three basic security services specified in the Bluetooth standard:
  - **Authentication**
    - verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.
  - **Confidentiality**
    - preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.
  - **Authorization**
    - allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.