Outline

- A preliminary overview
- Propagation characteristics
- ISO-OSI Model
- Physical layer: modulation
- MAC layer:
  - Fixed resource assignment
  - Random access
    - Ethernet (CSMA/CD)
    - WiFi (CSMA/CA)
- Personal Area Networks
  - **Bluetooth**
  - Zigbee
- Cellular network dimensioning
- Cellular networks
  - From GSM (2G) to UMTS (3G)
  - LTE (4G)

History Of Bluetooth

- Bluetooth was invented in 1994 by Ericsson.

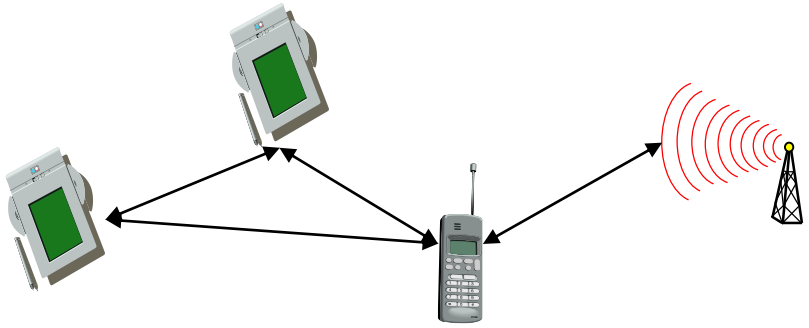
- The company later started working with a larger group of companies called the Bluetooth Special Interests Group, or "SIG," to develop the technology into what it is today.

- Bluetooth is not owned by any one company and is developed and maintained by SIG.

- The name Bluetooth came from a code name originally used by SIG for the project and is a reference to a 10th century Danish king named Harold Bluetooth (940-981 AC), who was responsible for uniting Norway, Sweden, and Denmark.

Bluetooth: Basics

- Consortium: Ericsson, Intel, IBM, Nokia, Toshiba…
- Scenarios:
  - connection of peripheral devices
    - loudspeaker, joystick, headset
  - support of ad-hoc networking
    - small devices, low-cost
  - bridging of networks
    - e.g., GSM via mobile phone - Bluetooth - laptop



- Simple, cheap, replacement of IrDA, low range, lower data rates, low-power
  - Worldwide operation: 2.4 GHz
  - Resistance to jamming and selective frequency fading:
    - FHSS over 79 channels (of 1MHz each), 1600hops/s
  - Coexistence of multiple piconets: like CDMA
  - Links: synchronous connections and asynchronous connectionless
  - Interoperability: protocol stack supporting TCP/IP, OBEX, SDP
  - Range: 10 meters, can be extended to 100 meters

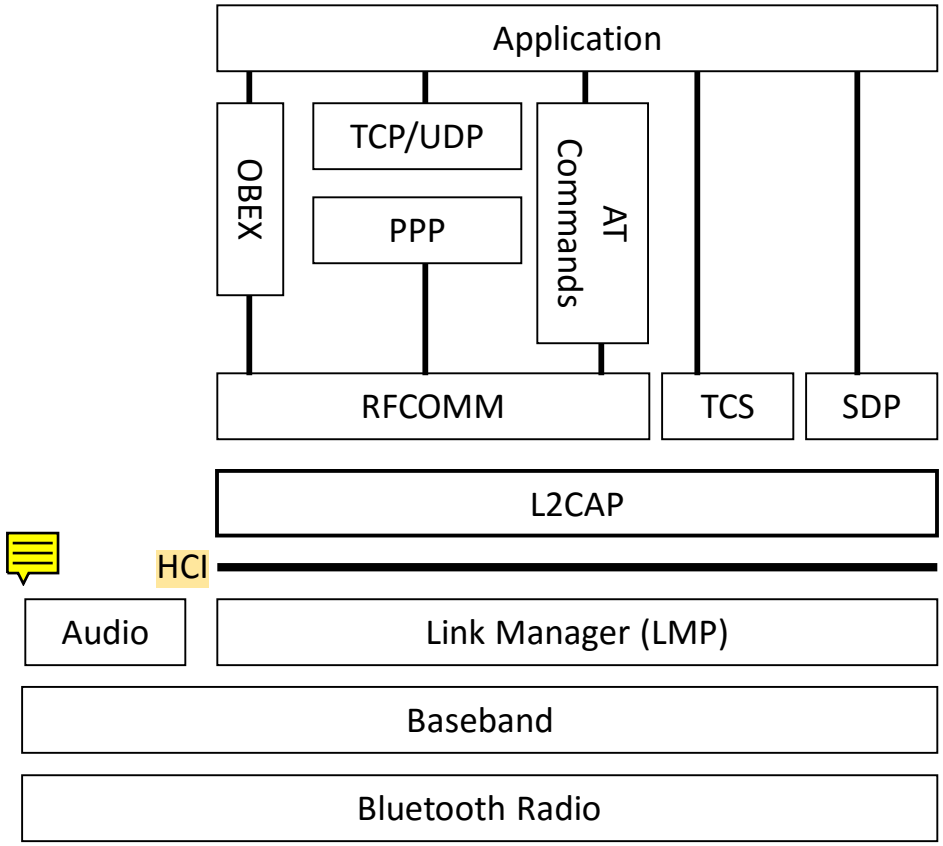
- Documentation: over 1000 pages specification: www.bluetooth.com

Bluetooth Application Areas

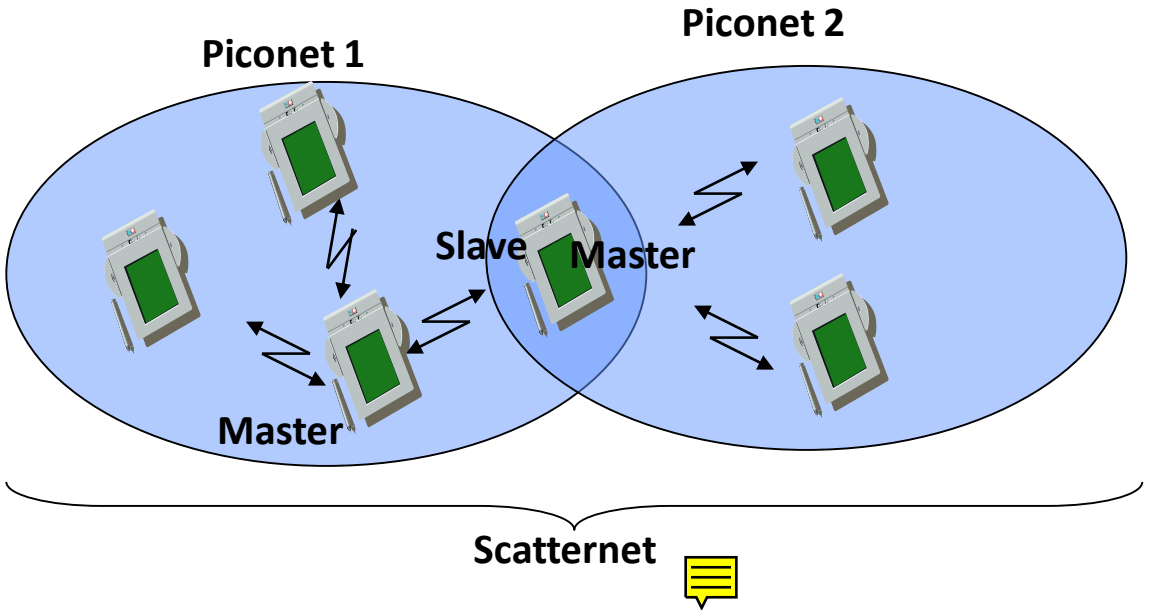
- Data and voice access points
  - Real-time voice and data transmissions
- Cable replacement
  - Eliminates need for numerous cable attachments for connection
- Low cost < $5
- Ad hoc networking
  - Device with Bluetooth radio can establish connection with another when in range
- Use modes:
  - File transfer
  - Internet bridge
  - LAN access
  - Synchronization
  - Three-in-one phone
  - Headset

Protocol Architecture

- BT **Radio** (2.4 GHZ Freq. Band):
- Modulation: Gaussian Frequency Shift Keying
- **Baseband**: FH-SS (79 carriers), CDMA (hopping sequence from the node MAC address)
- **Audio**: interfaces directly with the baseband. Each voice connection is over a 64Kbps SCO link. The voice coding scheme is the Continuous Variable Slope Delta (CVSD)
- Link Manager Protocol (**LMP**): link setup and control, authentication and encryption
- Host Controller Interface: provides a uniform method of access to the baseband, control registers, etc through USB, PCI, or UART
- Logical Link Control and Adaptation Layer (**L2CAP**): higher protocols multiplexing, packet segmentation/reassembly, QoS
- Service Discover Protocol (**SDP**): protocol of locating services provided by a Bluetooth device
- Telephony Control Specification (**TCS**): defines the call control signaling for the establishment of speech and data calls between Bluetooth devices
- **RFCOMM**: provides emulation of serial links (RS232). Upto 60 connections
- **OBEX**: OBject EXchange (e.g., vCard)



Network Topology



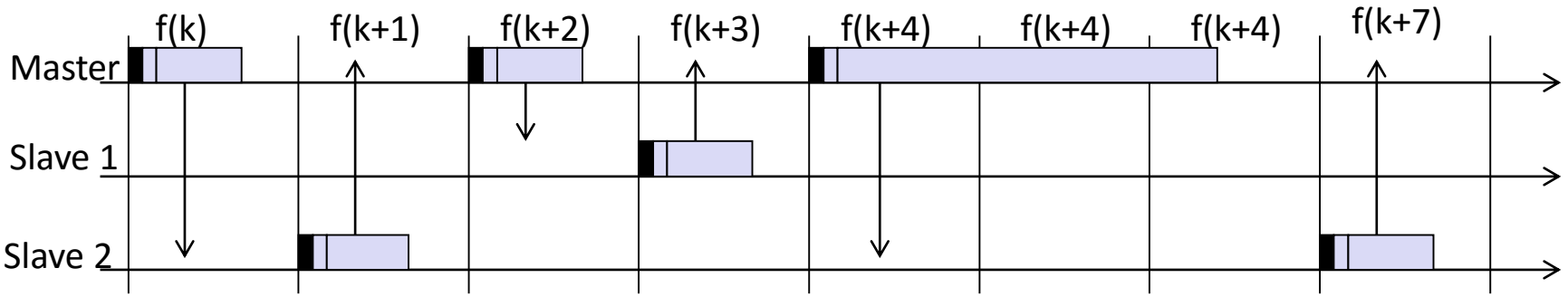
- Piconet = set of Bluetooth nodes synchronized to a unique master node
  - The piconet hopping sequence is derived from the master MAC address (BD_ADDR IEEE802 48 bits compatible address)
- Scatternet = set of piconets
- Master-Slaves can switch roles

Radio Specification

- Classes of transmitters
  - Class 1: Outputs 100 mW for maximum range
    - Power control mandatory
    - Provides greatest distance
  - Class 2: Outputs 2.4 mW at maximum
    - Power control optional
  - Class 3: Nominal output is 1 mW
    - Lowest power
- Frequency Hopping in Bluetooth
  - Provides resistance to interference and multipath effects
  - Provides a form of multiple access among co-located devices in different piconets

Bluetooth Piconet MAC

- Each node has a Bluetooth Device Address (BD_ADDR). The master BD_ADDR determines the sequence of frequency hops

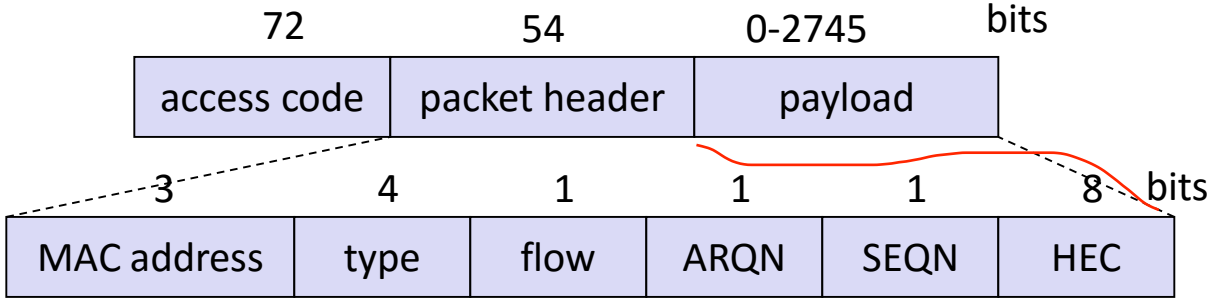


- Types of connections:

  Synchronous Connection-Oriented link (**SCO**) (symmetrical, circuit switched, point-to-point)

  Asynchronous Connectionless Link (**ACL**): (packet switched, point-to-multipoint, master-polls)

- Packet Format:
  - Access code: synchronization, when piconet active derived from master
  - Packet header (for ACL): 1/3-FEC, MAC address (1 master, 7 slaves), link type, alternating bit ARQ/SEQ, checksum



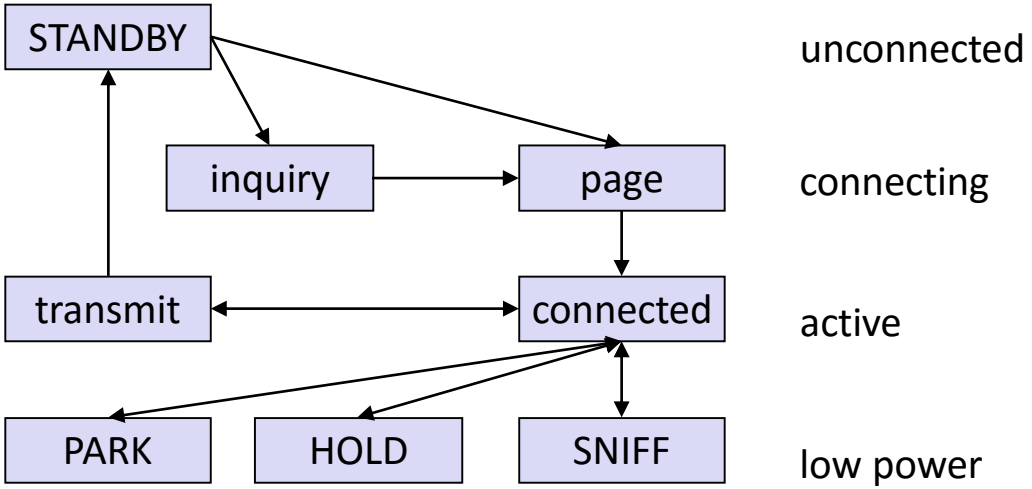
States of a Bluetooth Device

ACTIVE (connected/transmit): the device is uniquely identified by a 3bits AM_ADDR and is fully participating

SNIFF state: participates in the piconet only within the SNIFF interval

HOLD state: keeps only the SCO links

PARK state (low-power): releases AM_ADDR but stays synchronized with master



BT device addressing:

- BD_ADDR (48 bits)
- AM_ADDR (3bits): ACTIVE, HOLD, or SNIFF
- PM_ADDR (8 bits): PARK Mode address (exchanged with the AM_ADDR when entering PARK mode)
- AR_ADDR (8 bits): not unique used to come back from PARK to ACTIVE state

Bluetooth Link Security

- Elements:
  - Authentication – verify claimed identity
  - Encryption – privacy
  - Key management and usage
- Security algorithm parameters:
  - Unit address
  - Secret authentication key (128 bits key)
  - Secret privacy key (4-128 bits secret key)
  - Random number