CSE/PC/B/T/316
Computer Networks
Topic 9- IEEE 802.15.1 Bluetooth

Sarbani Roy

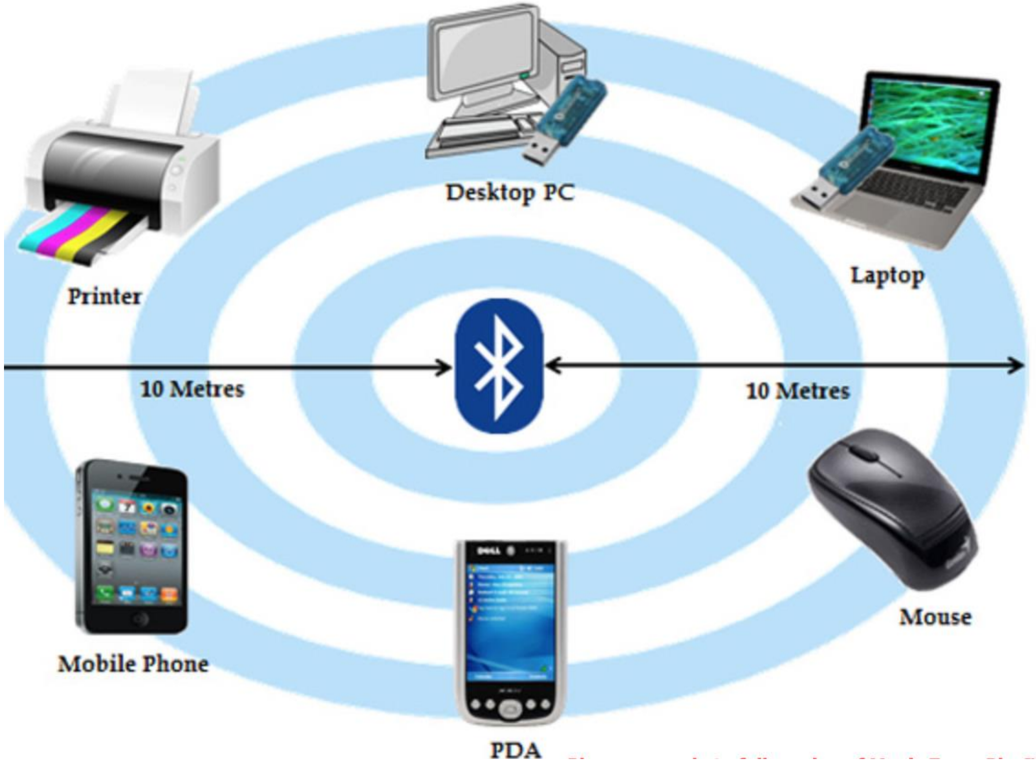
sarbani.roy@jadavpuruniversity.in

Office: CC-5-7

Cell: 9051639328

Bluetooth

- Bluetooth is a wireless LAN technology 802.15 (Wireless Personal Area Network) designed to connect devices of different functions such as telephones, notebooks, computers, cameras, printers, coffee makers, and so on. A Bluetooth LAN is an ad hoc network, which means that the network is formed spontaneously.



Bluetooth Overview

- Wireless technology for short-range voice and data communication
  - Devices can communicate with each other with wireless connectivity
- Low-cost and low-power
- Connects a wide range of computing and telecommunication devices
- Expand communication capabilities
- Provides a communication platform between a wide range of “smart” devices
- Not limited to “line of sight” communication

Summary

- Bluetooth is a global, RF-based (ISM band: 2.4 GHz), short-range, connectivity solution for portable, personal devices
  - it is not just a radio, it is an end-to-end solution
- The Bluetooth spec comprises
  - a HW & SW protocol specification
  - usage case scenario profiles and interoperability requirements
- IEEE 802.15.1 is working on standardizing the PHY and MAC layers in Bluetooth
- More Info:
  - http://www.bluetooth.org
  - http://ieee802.org/15/pub/TG1.html

Products

- Notebook PCs & desktop computers
- Printers
- PDAs
- Other handheld devices
- Cell phones
- Wireless periperals:
  - Headsets
  - Cameras
- Access Points
- CD Player
- TV/VCR/DVD
- Telephone Answering Devices
- Cordless Phones
- Cars
- Hands free calls

Connecting to Internet

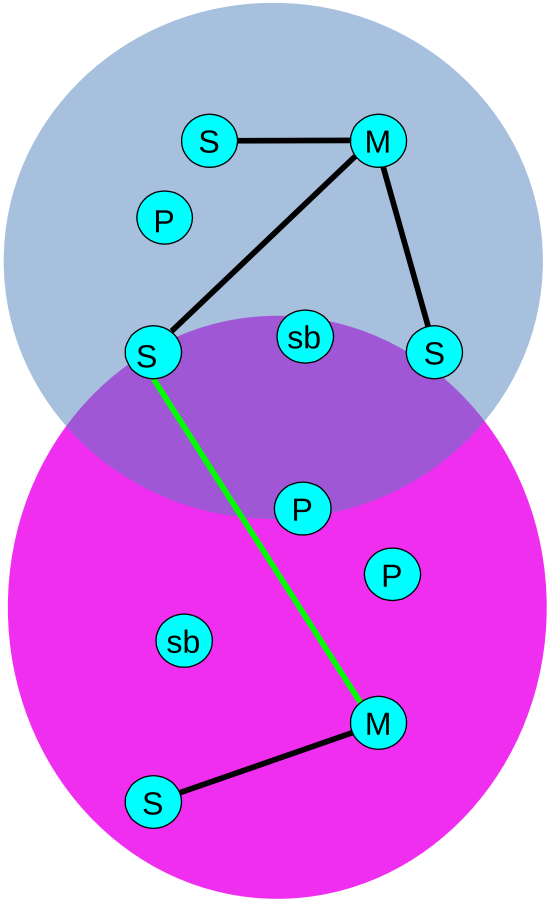
- Being able to gain access to the Internet by using “Bluetooth access points”
  - Access point is used as a gateway to the internet
  - Both the access point and the device are Bluetooth-enabled
  - An example of Service Discovery Protocol
    - Access point provides a service to the device

Bluetooth Specifications

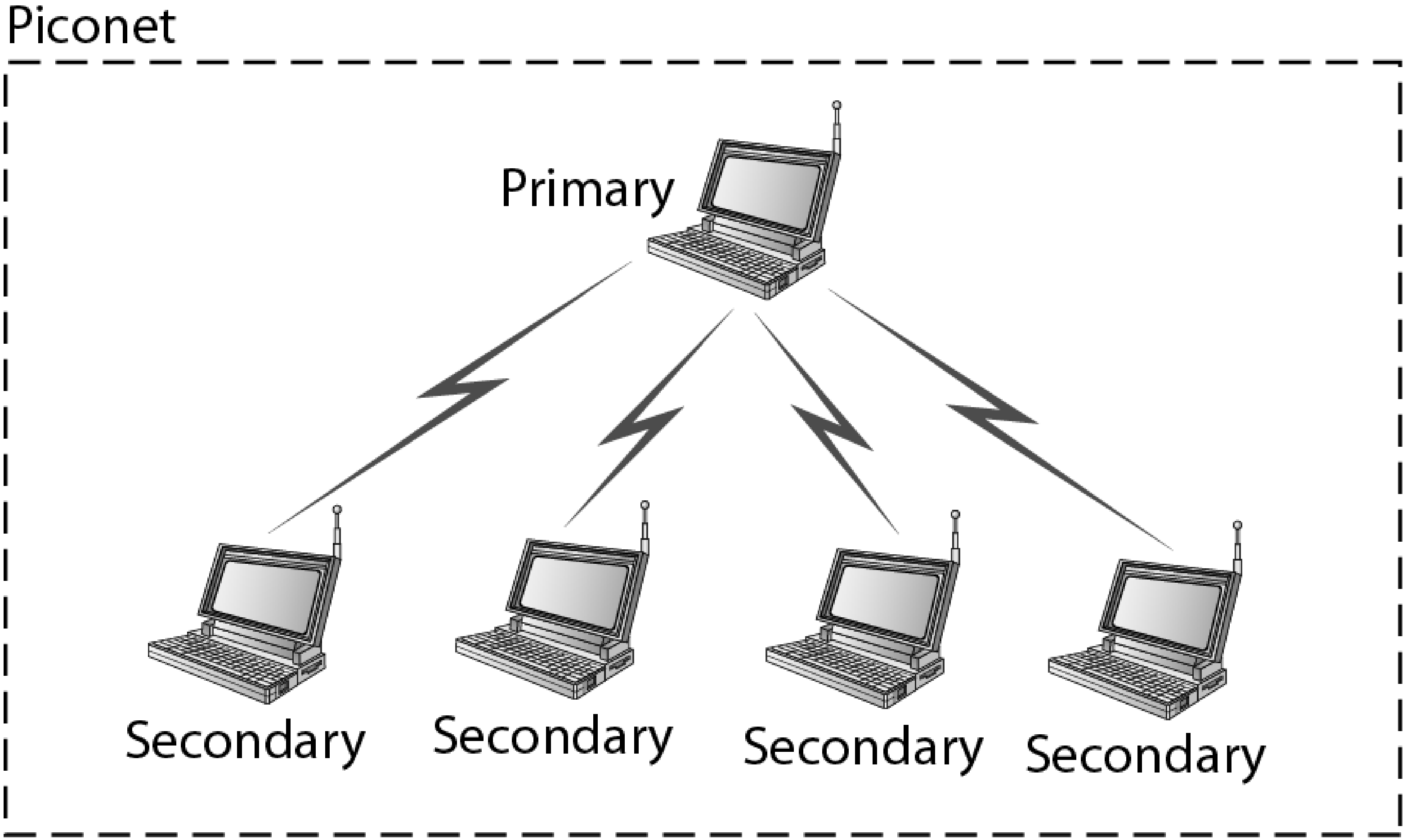
- Things that you must have:
  - Transceivers and Receivers that can send and receive data because they use **Radio Waves.**
  - MAC Address (Physical Address)
    - Burnt on the NIC card by the manufacturer.
  - PIN Number
    - To identify the user using the device.
  - A Piconet
  - A FHSS protocol

The Bluetooth network topology

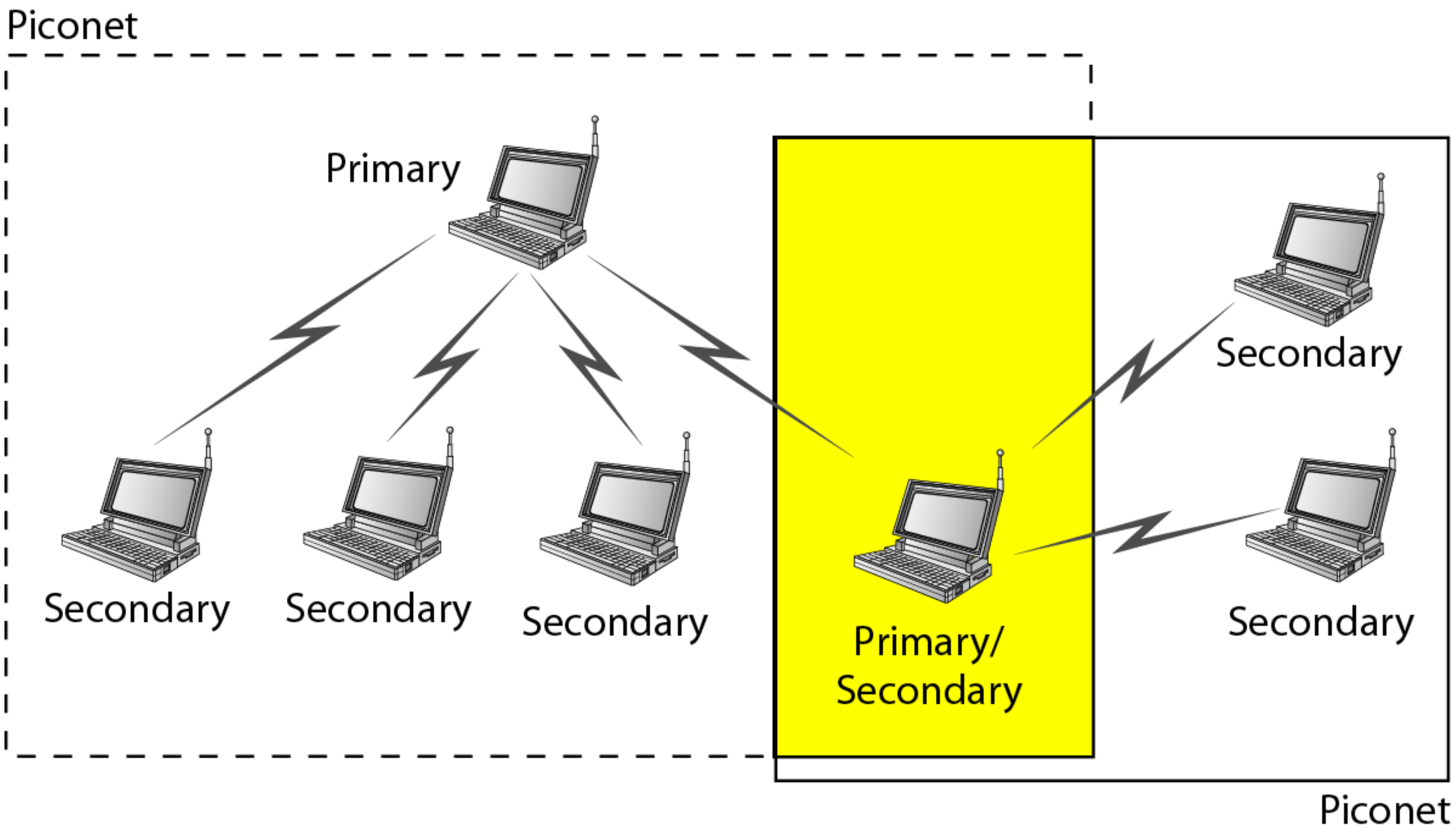
- Radio designation
  - Connected radios can be master or slave
  - Radios are symmetric (same radio can be master or slave)
- Piconet
  - Master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet
  - Each piconet has maximum capacity (1 MSPS (Mega Samples Per Second)
  - Unique hopping pattern/ID
- Scatternet
  - Piconets can coexist in time and space



Piconet

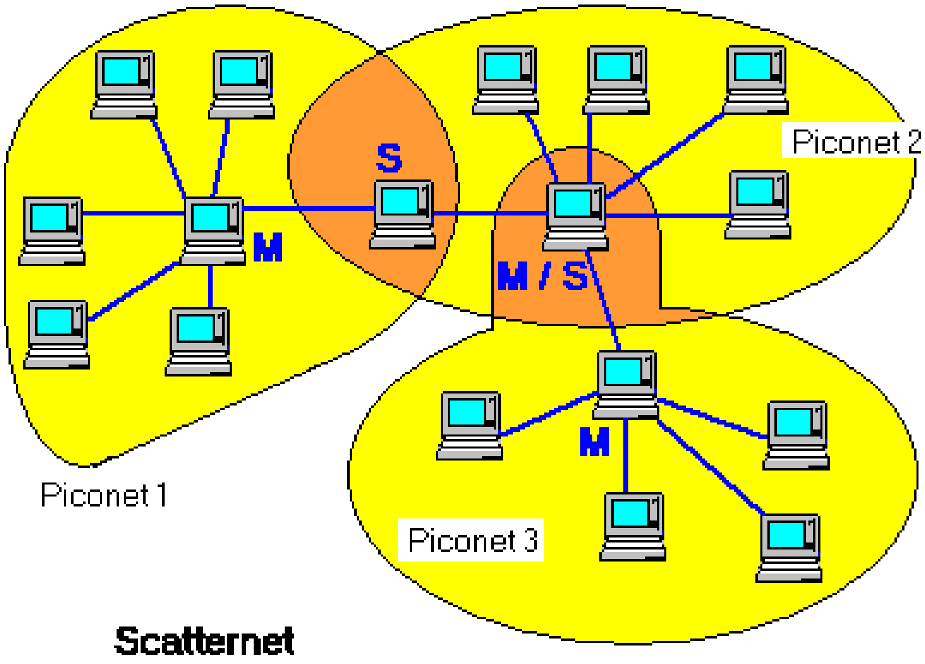

Piconet
Primary
Secondary
Secondary
Secondary
Secondary

Scatternet


Piconet
Primary
Secondary
Secondary
Secondary
Primary/
Secondary
Secondary
Secondary
Piconet

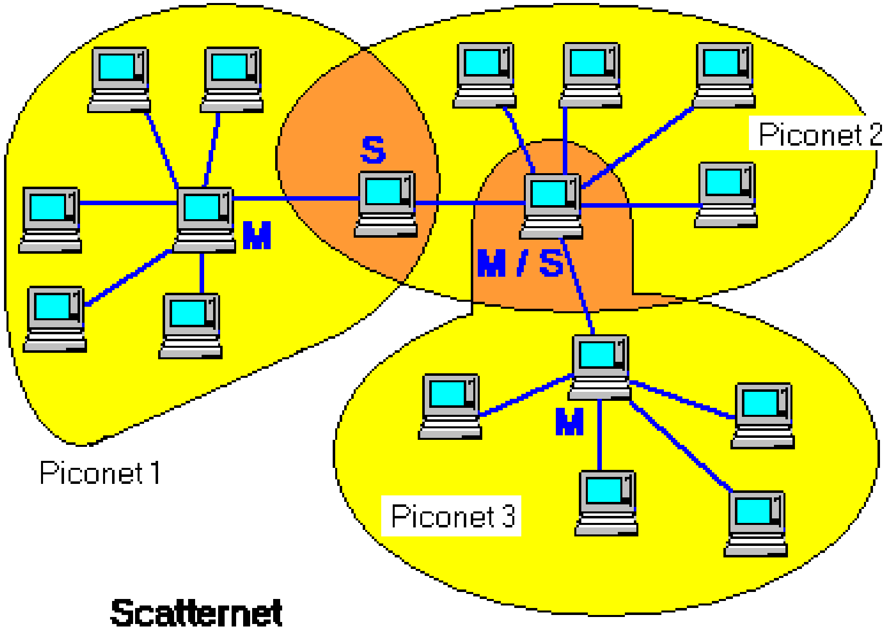
Establishing Piconets

- Whenever there is a connection between two Bluetooth devices, a piconet is formed
- Always 1 master and up to 7 active slaves
- Any Bluetooth device can be either a master or a slave
- Can be a master of one piconet and a slave of another piconet at the same time (scatternet)
- All devices have the same timing and frequency hopping sequence

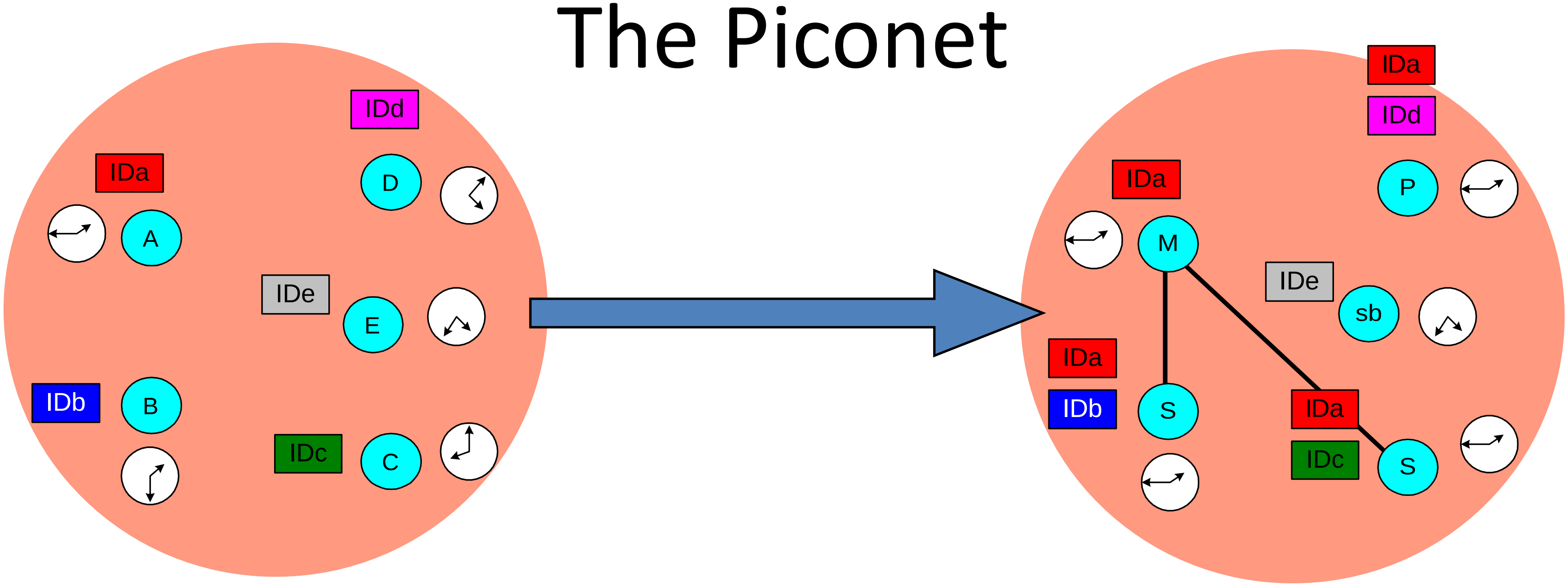


Scatternets

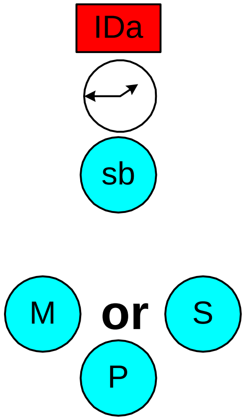
- Formed by two or more Piconets
- Master of one piconet can participate as a slave in another connected piconet
- No time or frequency synchronization between piconets



The Piconet

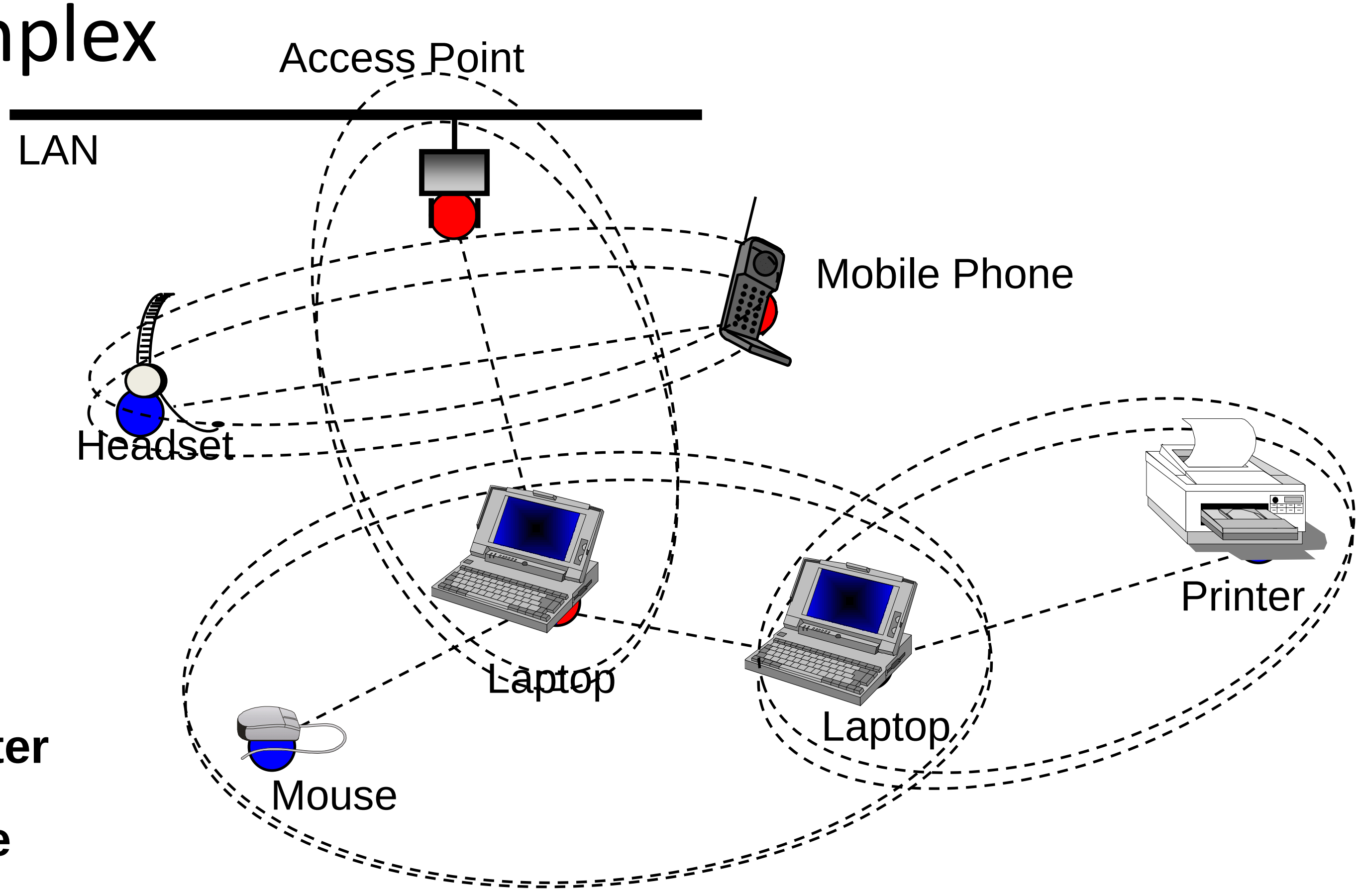


- All devices in a piconet hop together
  - To form a piconet: master gives slaves its *clock* and *device ID*
    - Hopping pattern determined by *device ID* (48-bit)
    - Phase in hopping pattern determined by *Clock*
- Non-piconet devices are in standby
- Piconet Addressing
  - Active Member Address (AMA, 3-bits)
  - Parked Member Address (PMA, 8-bits)



Inter-connected Piconets - The Scatternet

- Complex



🔴 **master**

🔵 **slave**

◐ **master/slave**

FHSS

- Bluetooth devices use a protocol called (FHSS) Frequency-Hopping Spread Spectrum .

- Uses packet-switching to send data.

- Bluetooth sends packets of data on a range of frequencies.

- In each session one device is a master and the others are slaves.

- The master device decides at which frequency data will travel.

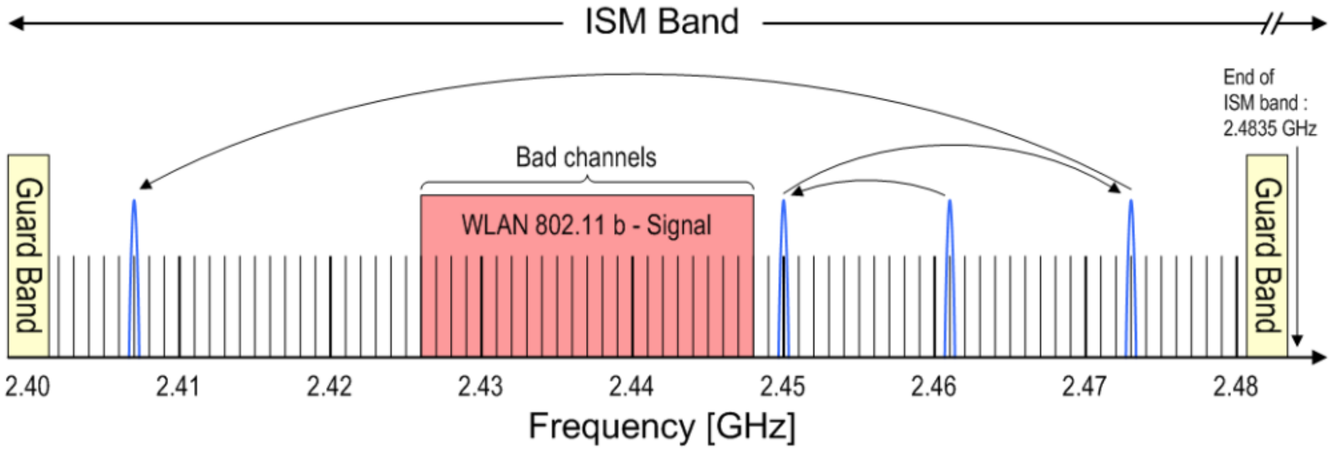
FHSS

- Transceivers “hop” among 79 different frequencies in the 2.4 GHz baud at a rate of 1600 frequency hops per second.

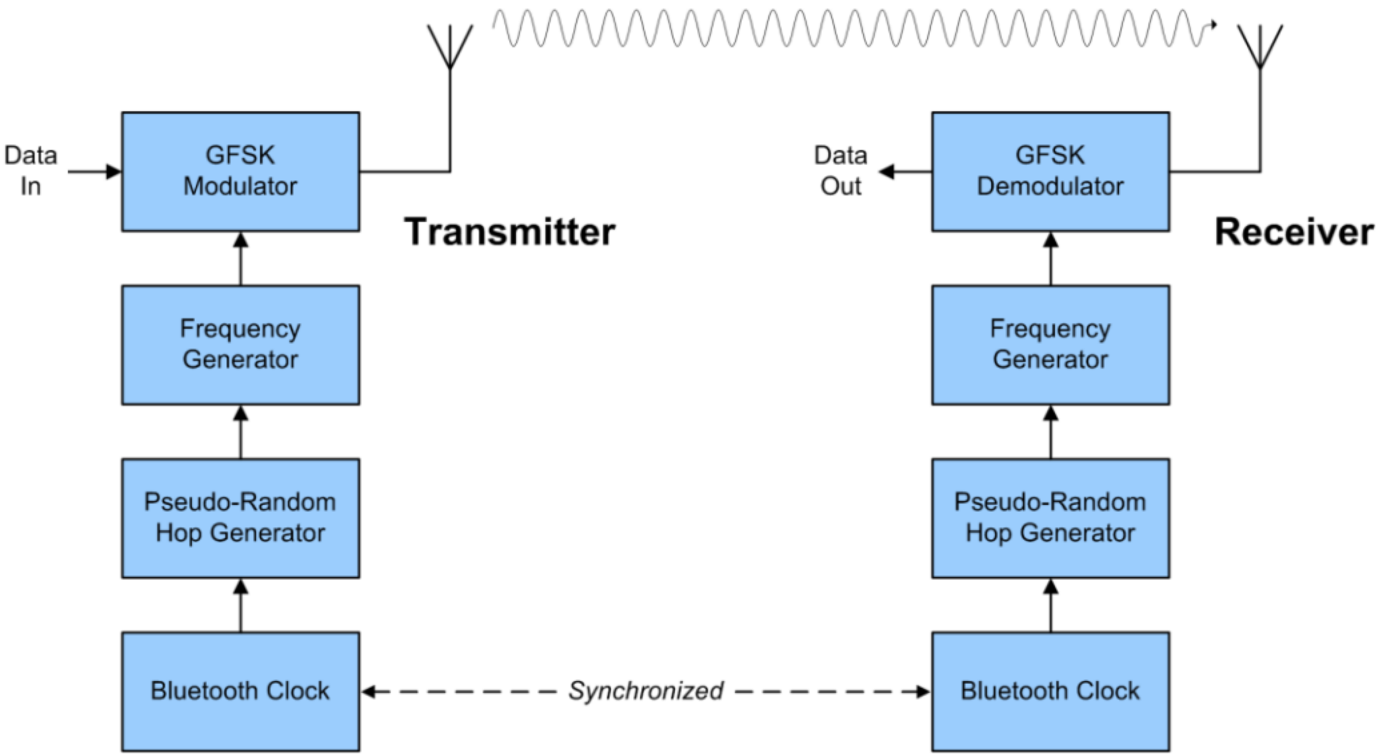
- The master device tells the slaves at what frequency data will be sent.

- This technique allows devices to communicate with each other more securely.

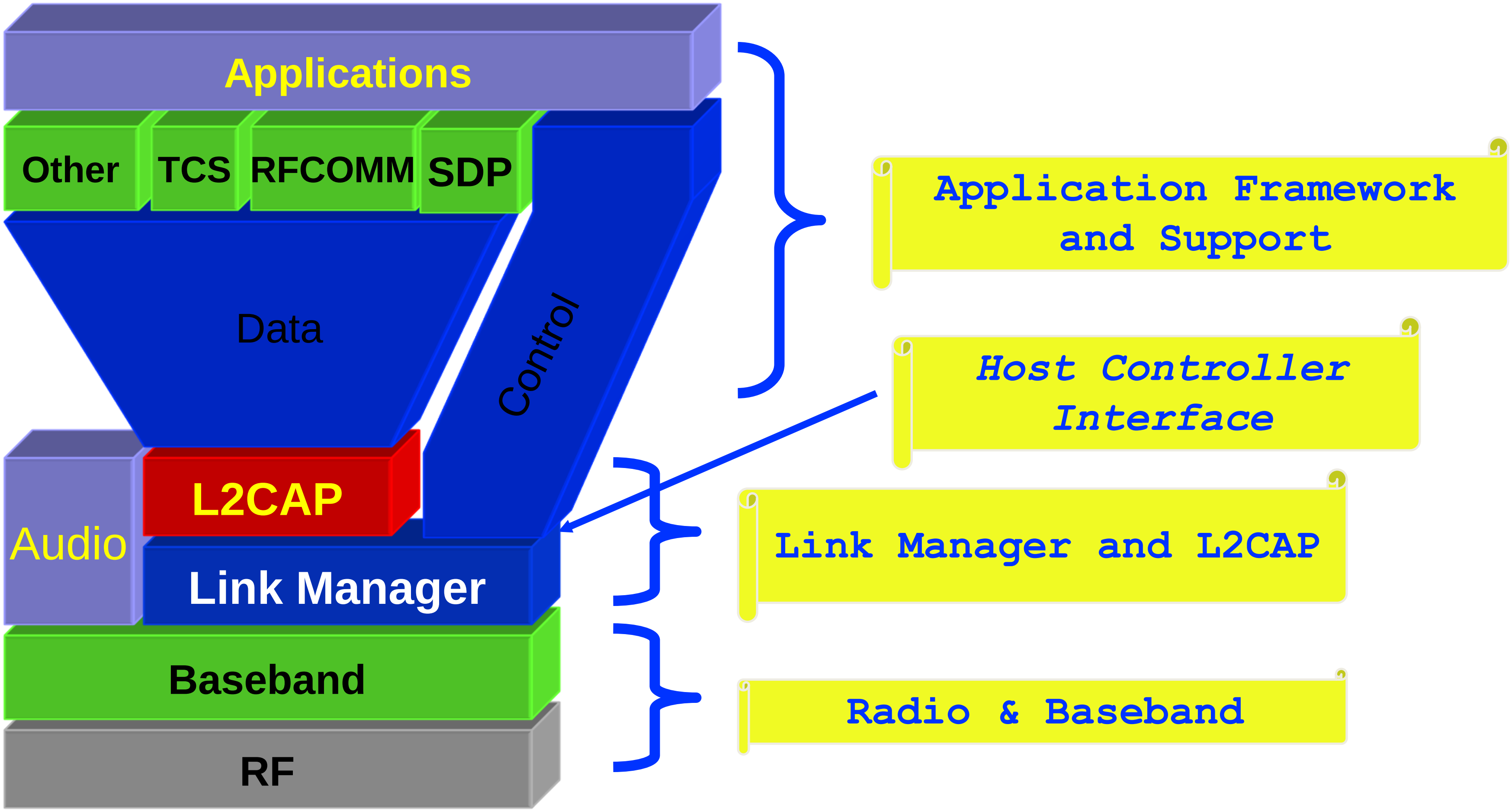
FHSS example in the ISM band & bad channels due to a coexisting WLAN signal



BT Frequency Hopping Spread Spectrum (FHSS) block diagram



The Bluetooth protocols



Applications

Other

TCS

RFCOMM

SDP

Data

Control

Audio

L2CAP

Link Manager

Baseband

RF

Application Framework and Support

Host Controller Interface

Link Manager and L2CAP

Radio & Baseband

- A hardware/software description
- An application framework

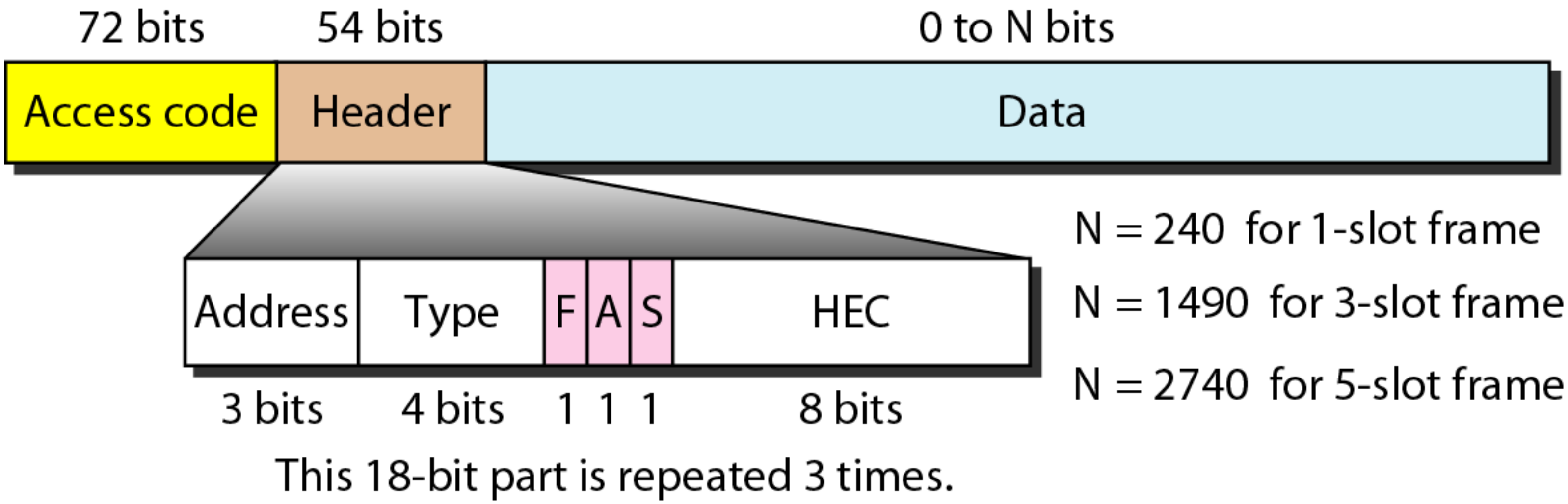
Core Protocols

- Radio: Specification of the air interface, i.e., frequencies, modulation, and transmit power
- Baseband: Description of basic connection establishment, packet formats, timing, and basic QoS parameters
- Link manager protocol: Link set-up and management between devices including security functions and parameter negotiation
- Logical link control and adaptation protocol (L2CAP): Adaptation of higher layers to the baseband (connectionless and connection-oriented services
- Service discovery protocol: Device discovery in close proximity plus querying of service characteristics

Adaptive hopping

- The term 'Adaptive' comes from the ability of the master and all slaves within a piconet to be able to monitor channel conditions and avoid bad channels, if necessary.
- The channel quality measurements are made by all devices within the piconet, since interference depends on the device location and transmitted power. Common metrics for making the judgement on RX channel quality are as follows:
  - Received Signal Strength Indication (RSSI)
  - Packet or Bit Error Rate (PER / BER)
  - Signal to Noise Ratio (SNR)

Frame format types



- Access code: This 72-bit field, normally contains synchronization bits and the identifier of the primary to distinguish the frame of one piconet from that of another.
- Header: This 54-bit field is a repeated 18-bit pattern. Each pattern has the following subfields:
  - Address: The 3-bit address subfield can define up to seven secondaries (1 to 7). If the address is zero, it is used for broadcast communication from the primary to all secondaries. Type.
  - The 4-bit type subfield defines the type of data coming from the upper layers.
  - F: This 1-bit subfield is for flow control. When set (1), it indicates that the device is unable to receive more frames (buffer is full).
  - A: This 1-bit subfield is for acknowledgment. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for acknowledgment.
  - S: This 1-bit subfield holds a sequence number. Bluetooth uses Stop-and-Wait ARQ; 1 bit is sufficient for sequence numbering.
- HEC. The 8-bit header error correction subfield is a checksum to detect errors in each 18-bit header section.

Access code

- The access code consists of a 4 bit preamble, a synchronization field, and a trailer (if a packet header follows).
- The 64-bit synchronization field is derived from the lower 24 bit of an address (lower address part, LAP).
  - If the access code is used for channel access (i.e., data transmission between a master and a slave or vice versa), the LAP is derived from the master's globally unique 48-bit address.
  - In case of paging the LAP of the paged device is used.
  - If a Bluetooth device wants to discover other (arbitrary) devices in transmission range (general inquiry procedure) it uses a special reserved LAP.
- Special LAPs can be defined for inquiries of dedicated groups of devices.

Packet header: address, type

- This field contains typical layer 2 features: address, packet type, flow and error control, and checksum.
- The 3-bit active member address represents the active address of a slave Active addresses are temporarily assigned to a slave in a piconet.
  - If a master sends data to a slave the address is interpreted as receiver address.
  - If a slave sends data to the master the address represents the sender address.
  - The zero value is reserved for a broadcast from the master to all slaves.
- The 4-bit type field determines the type of the packet.

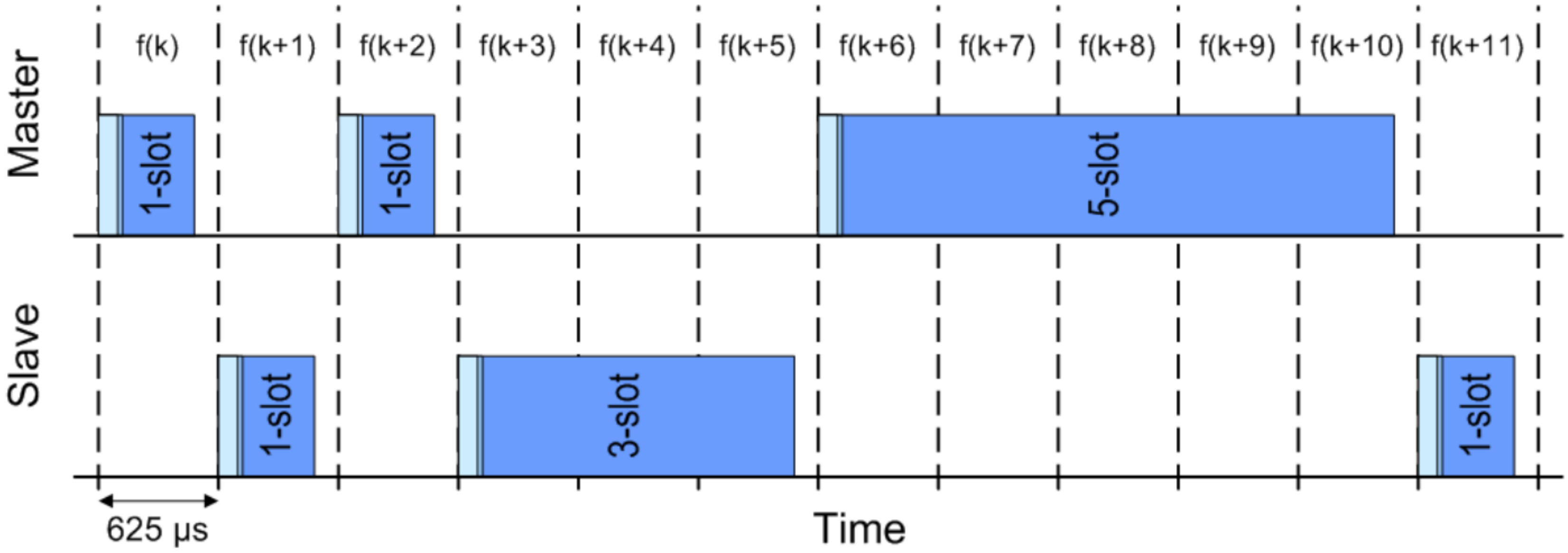
Packet header: flow, ARQN

- A simple flow control mechanism for asynchronous traffic uses the 1-bit flow field.
  - If a packet is received with flow=0 asynchronous data, transmission must stop.
  - As soon as a packet with flow=1 is received, transmission may resume.
- If an acknowledgement of packets is required, Bluetooth sends this in the slot following the data (using its time division duplex scheme).

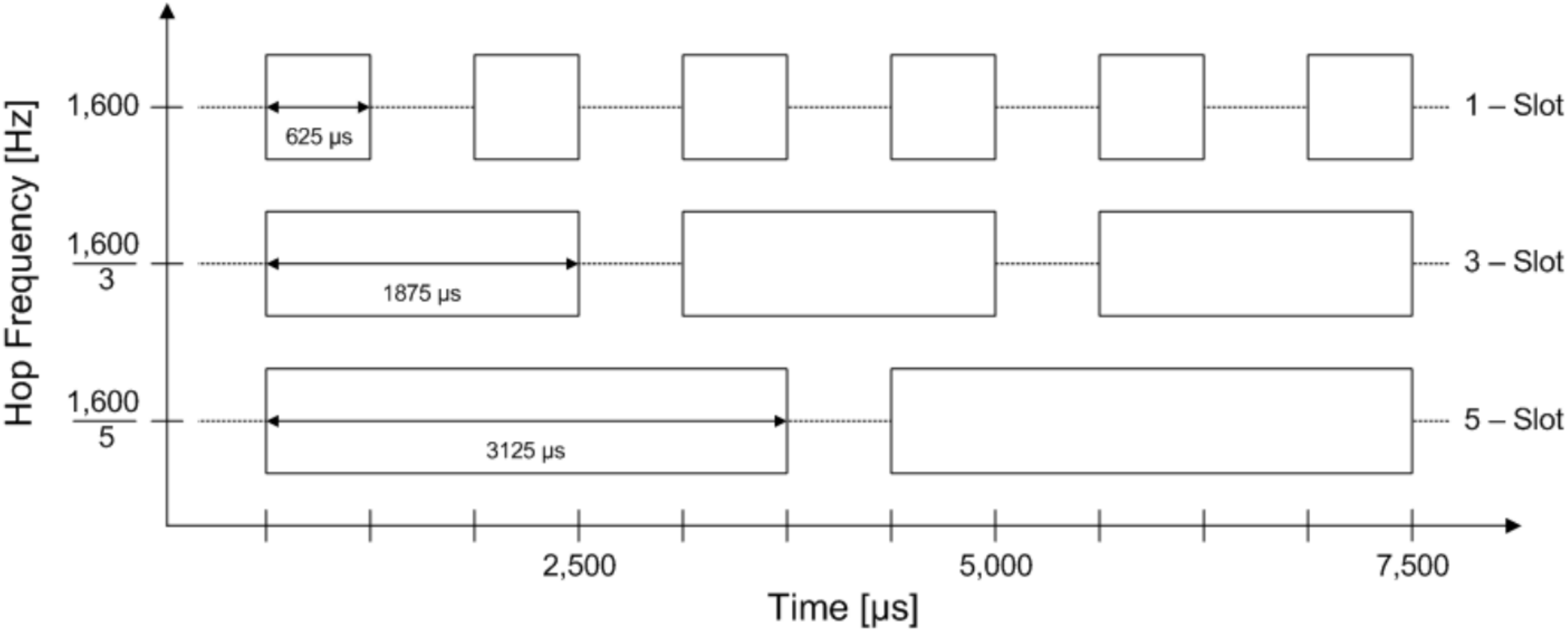
Packet header: SEQN, HEC

- A simple alternating bit protocol with a single bit sequence number SEQN and acknowledgement number ARQN can be used.
- An 8-bit header error check (HEC) is used to protect the packet header.
- The packet header is also protected by a one-third rate forward error correction (FEC) code because it contains valuable link information and should survive bit errors. Therefore, the 18-bit header requires 54 bits in the packet.

Time slots and Frequency hops



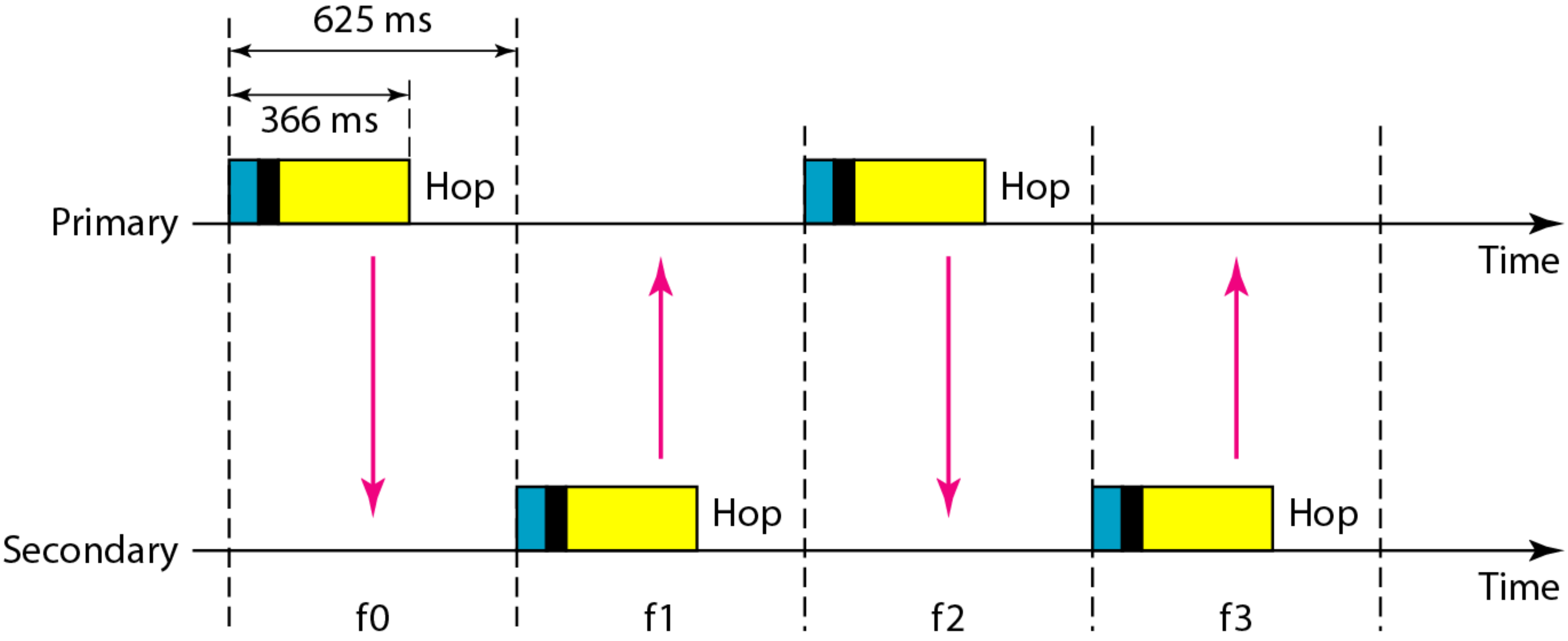
Hopping Frequency and Time Slot duration



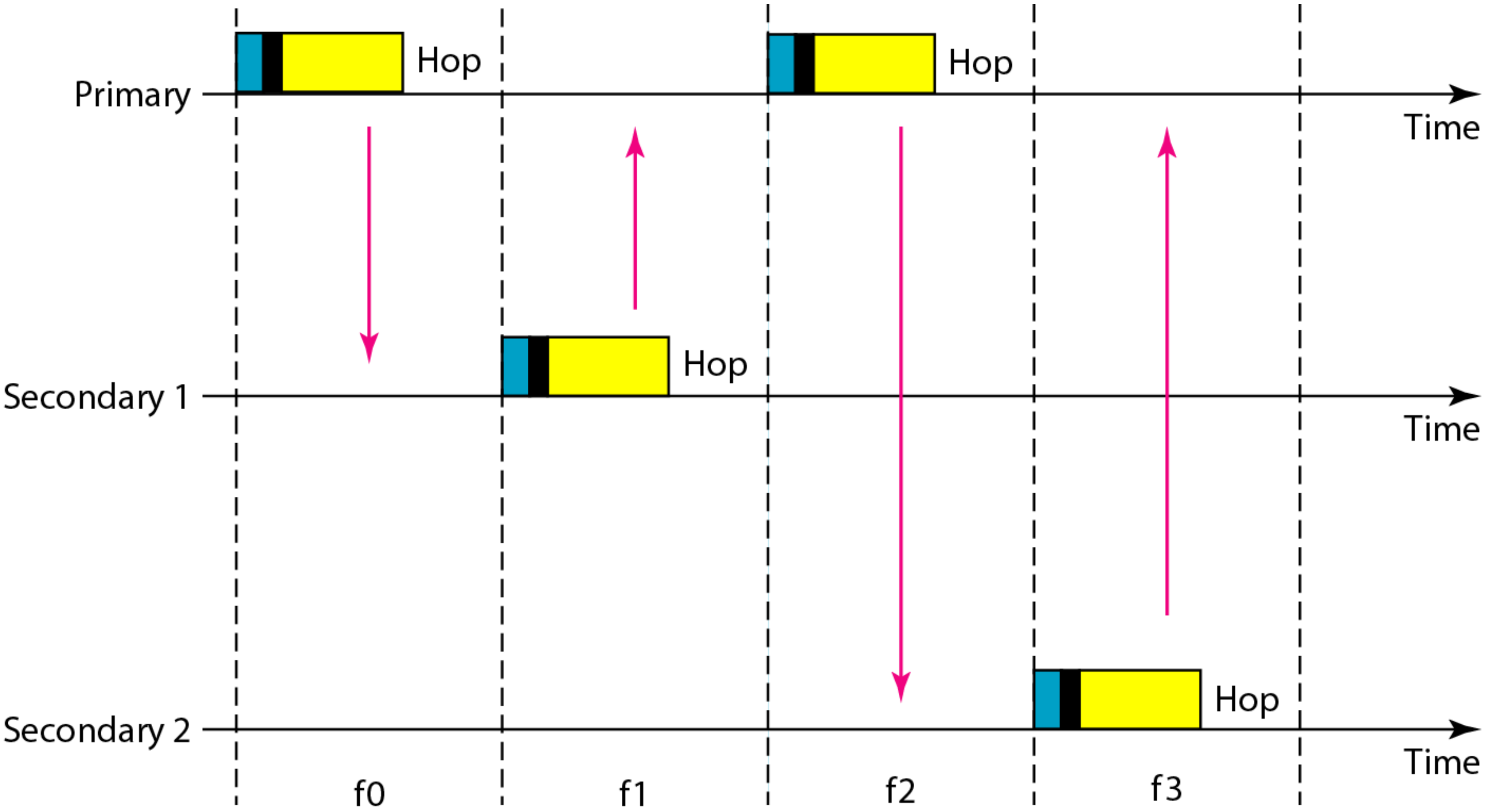
Frame

- A frame in the baseband layer can be one of three types: one-slot, three-slot, or five slot.
- In a one-slot frame exchange, 259 μs s needed for hopping and control mechanisms. This means that a one-slot frame can last only 625 − 259, or 366 μs.
  - With a 1-MHz bandwidth and 1 bit/Hz, the size of a one slot frame is 366 bits.
- A three-slot frame occupies three slots. Since 259 μs is used for hopping, the length of the frame is 3 × 625 − 259 = 1616 μs or 1616 bits.
  - A device that uses a three-slot frame remains at the same hop (at the same carrier frequency) for three slots.

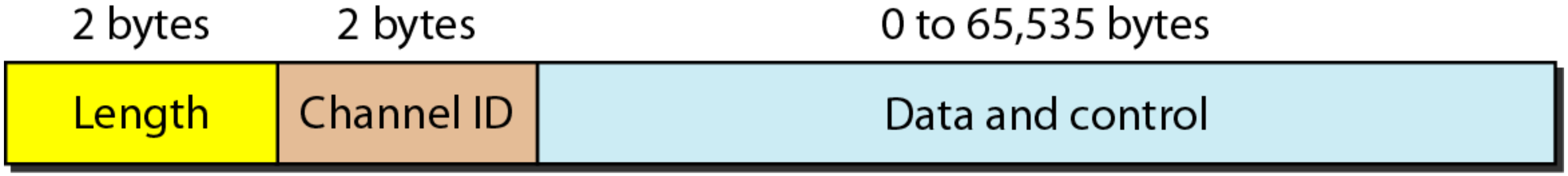
Single-secondary communication



Multiple-secondary communication



L2CAP data packet format

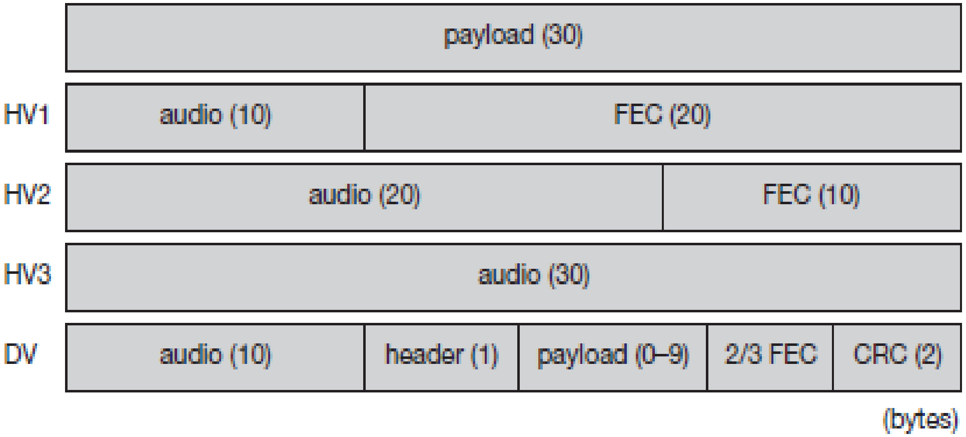


Baseband Layer

- Provides in-order delivery of byte streams
- Handles Frequency Hop Sequences for Synchronization and Transmission
- Establishes Links
  - Synchronous Connection Oriented (SCO)
  - Asynchronous Connection-Less (ACL)
- Provides functionality to determine nearby Bluetooth devices

SCO

- Classical telephone (voice) connections require symmetrical, circuit-switched, point-to-point connections.
- For this type of link, the master reserves two consecutive slots (forward and return slots) at fixed intervals.
  - A master can support up to three simultaneous SCO links to the same slave or to different slaves.
  - A slave supports up to two links from different masters or up to three links from the same master.



payload (30)

HV1 audio (10) FEC (20)

HV2 audio (20) FEC (10)

HV3 audio (30)

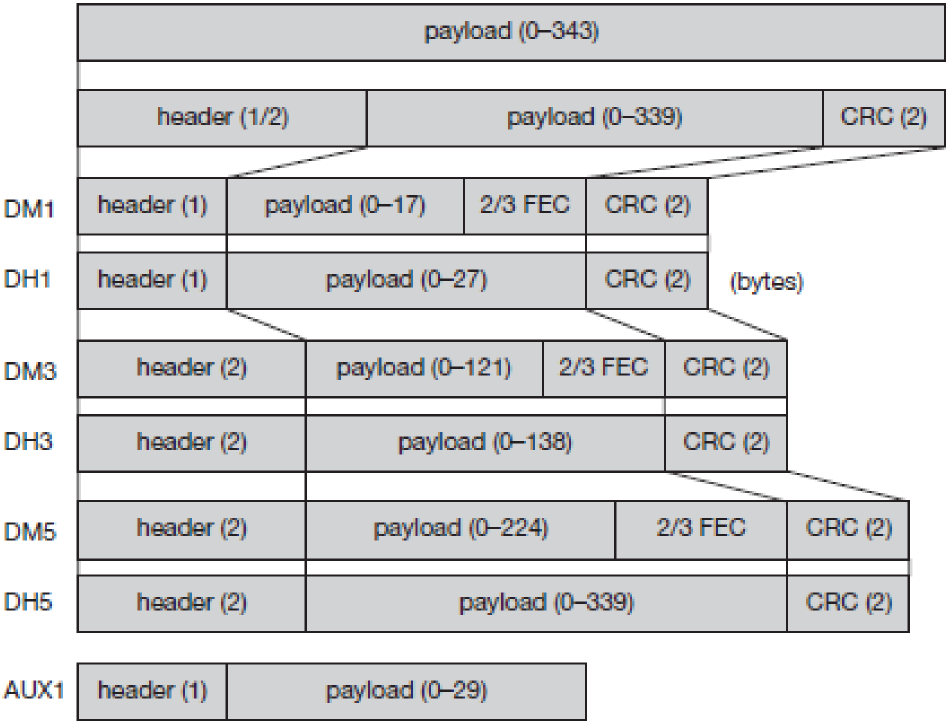
DV audio (10) header (1) payload (0–9) 2/3 FEC CRC (2)

(bytes)

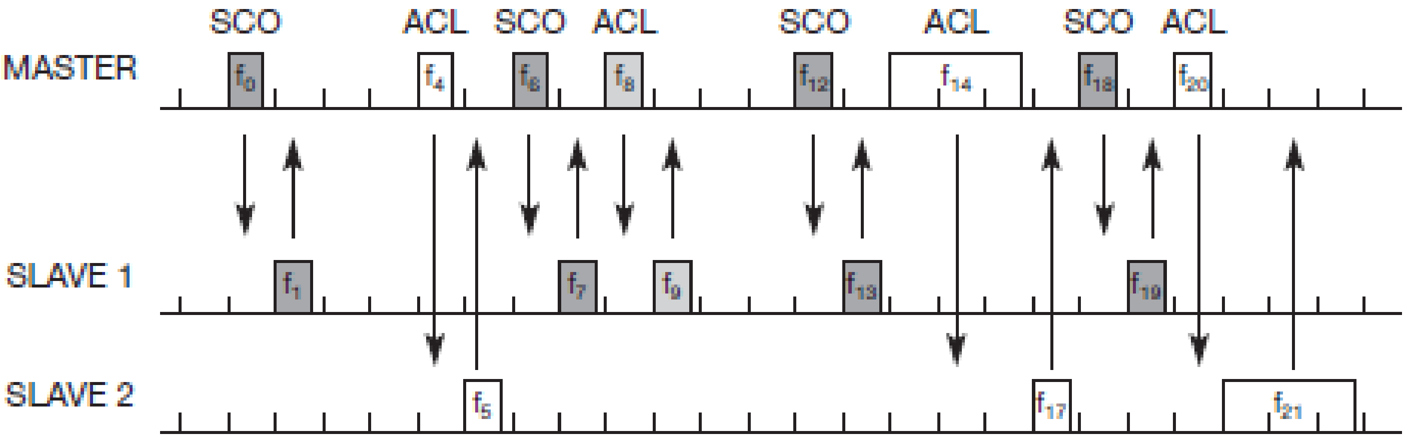
- Using an SCO link, three different types of single-slot packets can be used
- HV: High quality voice
- DV: Data and Voice together

ACL

- Typical data applications require symmetrical or asymmetrical (e.g., web traffic), packet-switched, point-to-multipoint transfer scenarios (including broadcast).
- Here the master uses a polling scheme. A slave may only answer if it has been addressed in the preceding slot.
- Only one ACL link can exist between a master and a slave.
- DM: Data medium rate (FEC added)
- DH: Data High rate (No FEC)



Example data transmission

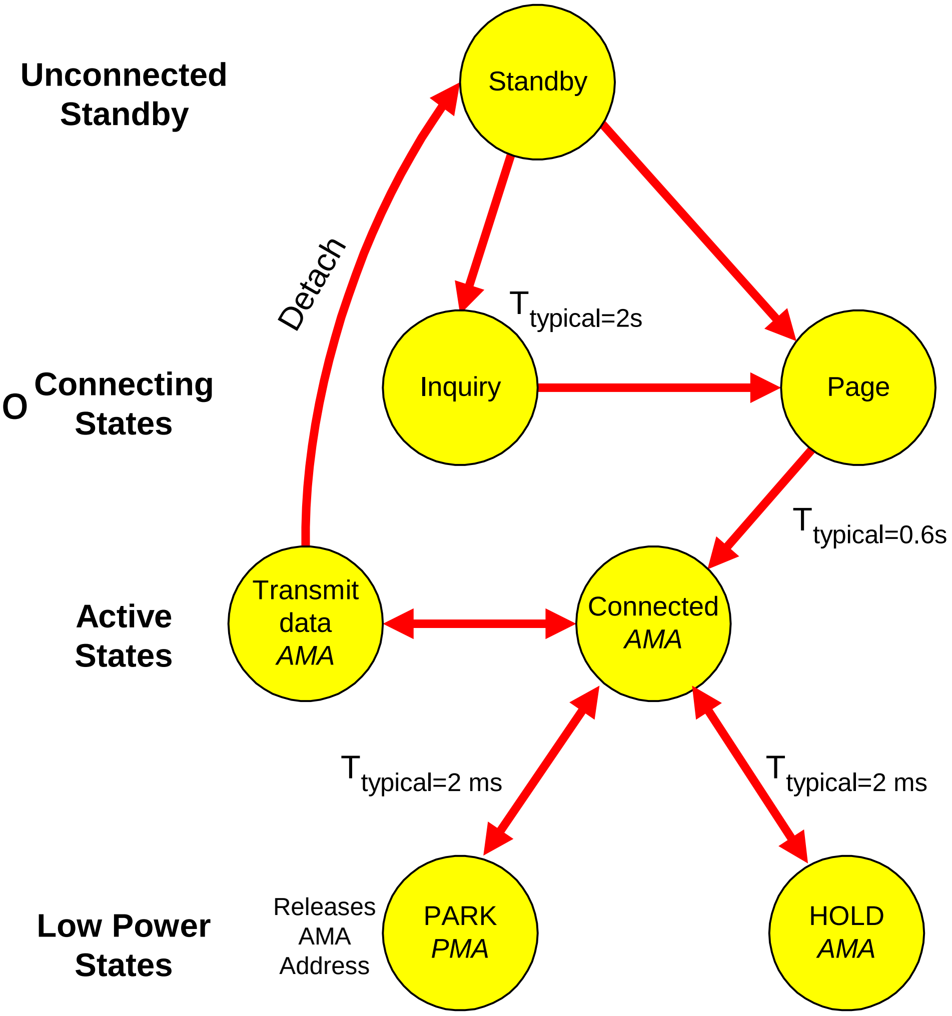


- for the

- In this example every sixth slot is used for an SCO link between the master and slave 1. The ACL links use single or multiple slots providing asymmetric bandwidth for connectionless packet transmission. This example again shows the hopping sequence which is independent of the transmission of packets.

Functional Overview

- Standby
  - Waiting to join a piconet
- Inquire
  - Ask about radios to connect to
- Page
  - Connect to a specific radio
- Connected
  - Actively on a piconet (master or slave)
- Park/Hold
  - Low Power connected states



Link Manager Operation

- Devices operate in standby mode by default until they become connected to a piconet
- 4 Connection Modes
  - Active
  - Hold
  - Park
  - Sniff
- Modes allow devices to adjust power consumption, performance, and the number/role of participants in a piconet

Active Mode

- Limited to 7 Active slaves for each master
- Three bit address (AM_ADDR) given to each active slave
- Unit actively participates on channel
- Can receive communications in any given frame
- Active slaves are polled by master for transmissions
- Unit operates on high-power

Hold Mode

- Frees slave to
  - Attend another Piconet
  - Perform scanning, paging, or inquiry operations
  - Move into low-power sleep
- Unit keeps active member address
- Unit does not support ACL packets on the channel but may support SCO packets
- Master and slave agree on a one time hold duration after which the slave revives and synchronizes with channel traffic
- Unit operates on low-power

Sniff Mode

- Very similar to hold mode
- Slave is freed for reoccurring fixed time intervals
- Master can only communicate during arranged “sniff” time slots

Park Mode

- Parked unit gives up active member address and is assigned
  - 8 bit Parked member address (PM_ADDR) – allows master to unpark slave
  - 8 bit Access request address (AR_ADDR) – allows slave to ask master to unpark it
- Unit stays synchronized to channel
- Operates in very low-power sleep

Park Mode (cont.)

- Provides the ability to connect more than 7 devices to a master (8 bit PM_ADDR allows 255 parked devices)
- Active and Parked slaves can be switched in and out to allow many connections to a single piconet

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.