Mobile communications

Bluetooth

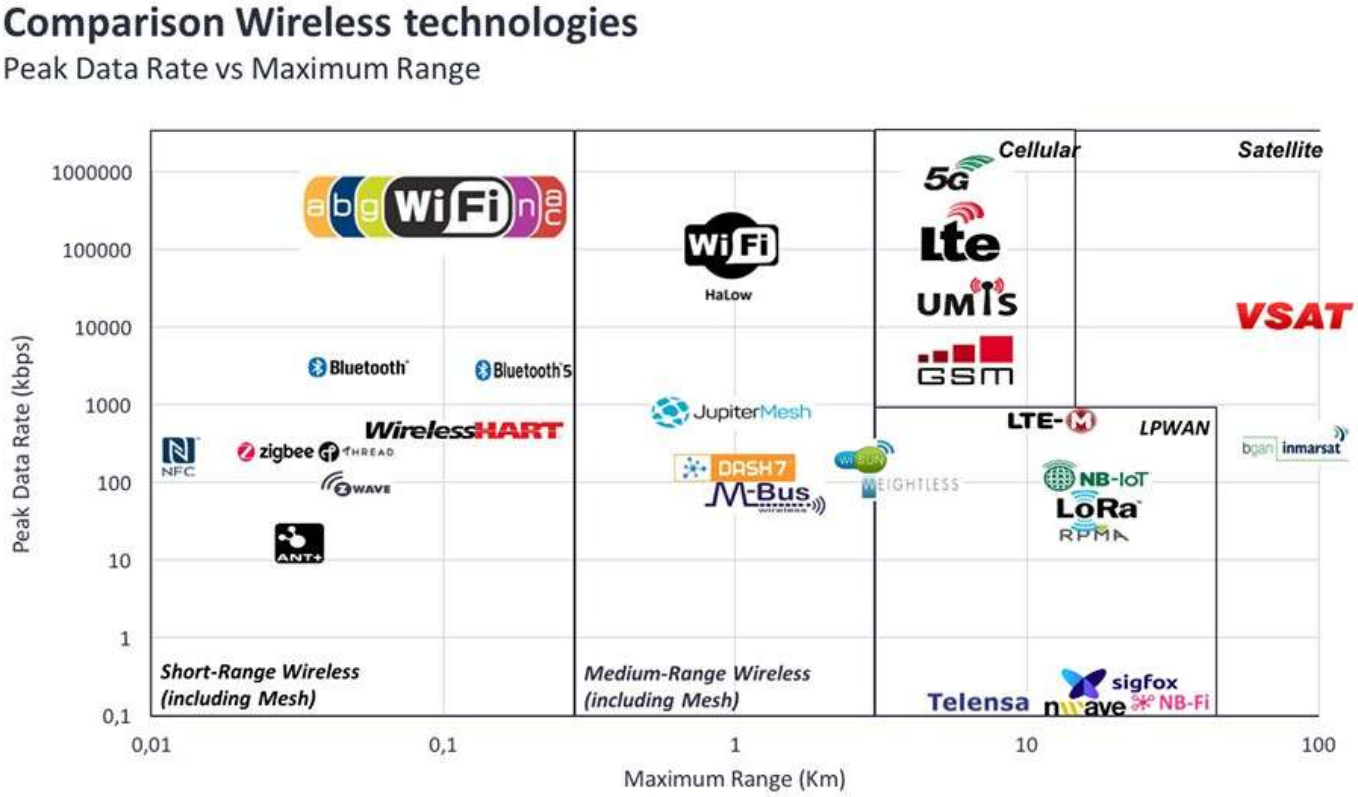
(WPAN)

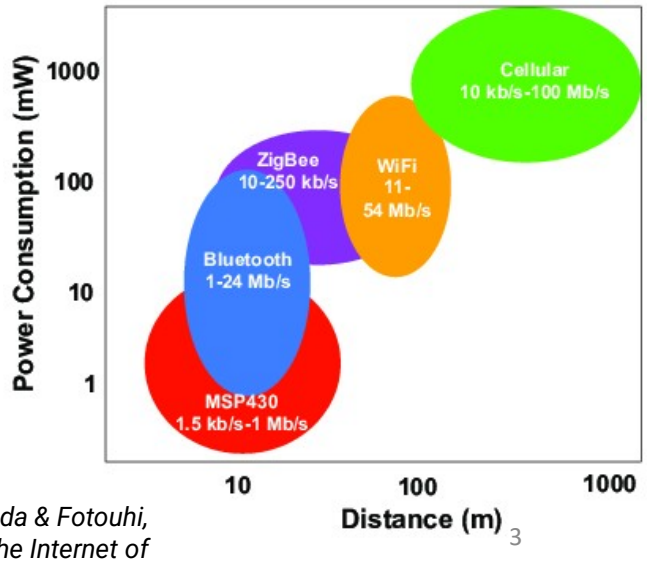
Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE

Comparison Between Wireless Technologies

Tradeoff between data rate, range and energy





Ahmed, Mobyen & Björkman, Mats & Causevic, Aida & Fotouhi, Hossein & Linden, Maria. (2015). An Overview on the Internet of Things for Health Monitoring Systems.

Personal Area Networks

- Target deployment environment: communication of personal devices working together
  - Short-range
  - Low Power
  - Low Cost
  - Small numbers of devices
  - Sometimes have more “bus-like” characteristics

- PAN Standards
  - Bluetooth – Industry consortia (Bluetooth SIG)
  - IEEE 802.15.1 – ”Bluetooth” based
  - IEEE 802.15.2 – Interoperability and coexistence
  - IEEE 802.15.3 – High data rate WPAN (UWB)
  - IEEE 802.15.4 – Low data rate WPAN (Zigbee,…)
  - IEEE 802.15.5 – Mesh Networks
  - IEEE 802.15.6 – Body Area Network

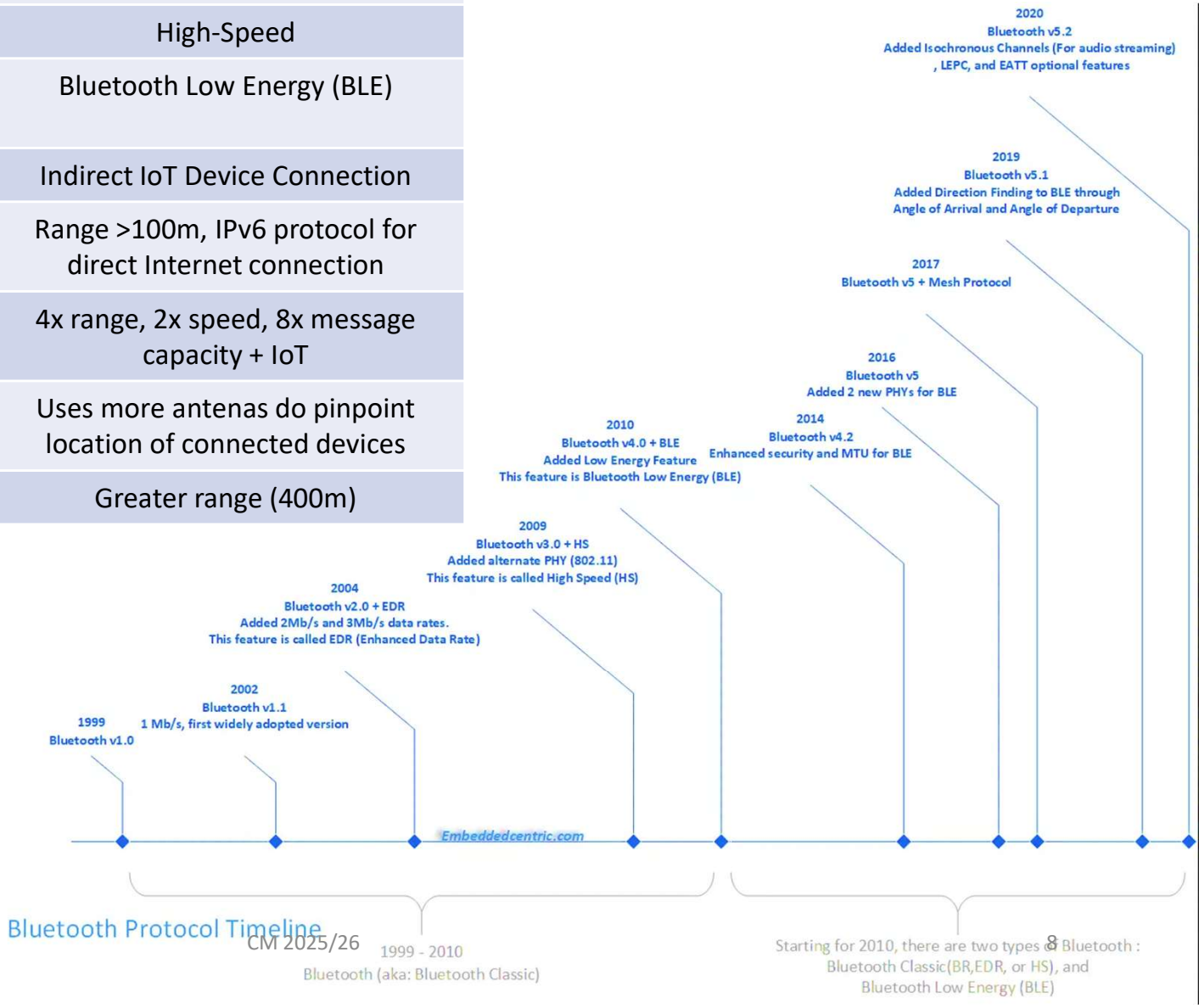
Bluetooth

- Originally for replacing “USB”, not “Ethernet”
  - Cable replacement technology
  - Later also used as Internet connection, phone, or headset
- PAN - *Personal Area Network*
  - Up to 1 Mbps connections
  - Includes synchronous, asynchronous, voice connections
  - Piconet routing
- Small, low-power, short-range, cheap, versatile radios
- Master/slave configuration and scheduling

Created by Ericsson; Maintained by the Bluetooth SIG

Bluetooth Versions

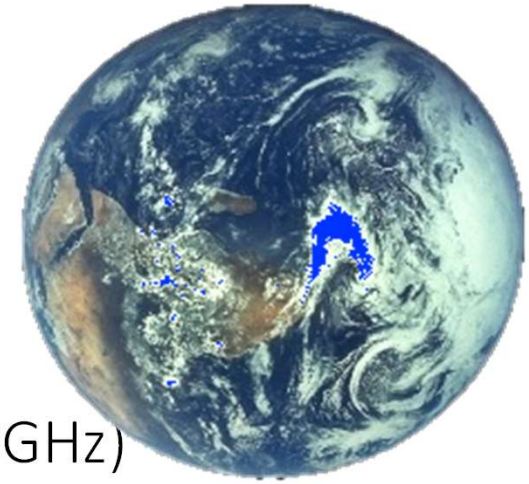
Version	Data rate	Feature
1.2	732 kbps	
2.0 + EDR	3 Mbps	Enhanced Data Rate (EDR)
3.0 + HS	24 Mbps	High-Speed
4.0	24 Mbps/ 1 Mbps (BLE)	Bluetooth Low Energy (BLE)
4.1	25 Mbps	Indirect IoT Device Connection
4.2	25 Mbps	Range >100m, IPv6 protocol for direct Internet connection
5.0	50 Mbps	4x range, 2x speed, 8x message capacity + IoT
5.1	50 Mbps	Uses more antenas do pinpoint location of connected devices
5.2	50 Mbps	Greater range (400m)



WLAN vs. Bluetooth

	Bluetooth	WLAN / WiFi
Specifications authority	Bluetooth SIG	IEEE, WiFi Alliance
Year of development	1994	1991
Bandwidth	Low (800 Kbps)	Very High (2 Gbps 802.11ax)
Hardware requirement	Bluetooth adaptor on all the devices connecting with each other	Wireless adaptors on all the devices of the network, a wireless router and/or wireless access points
Cost	Low	High
Power Consumption	Low	High
Frequency	2.4 GHz	2.4/5 GHz
Security	It is less secure	It is more secure
Range	10 meters	100 meters
Primary Devices	Mobile phones, mouse, keyboards,office and industrial automation devices	Notebook computers, desktop computers, servers
Ease of Use	Fairly simple to use. Can be used to connect upto seven devices at a time. It is easy to switch between devices or find and connect to any device.	It is more complex and requires configuration of hardware and software

Bluetooth features



- Radio network, on the 2.4 GHz, world-wide!
  - ISM; Unlicensed but regulated
- FH (Frequency Hopping) spread spectrum:
  79 (23 - .jp .es .fr) channels (de 2.402GHz - 2.480GHz)
- Defines a master that synchronizes everyone to his hop-pattern
- Defines two types of networks:
  - piconets
  - scaternets
- Maximum 8 devices per piconet (1 master + 7 slaves)
- Transmission rate: 720 Kb/s (max), assymetrical variable

Frequency Hopping Spread Spectrum (FHSS)

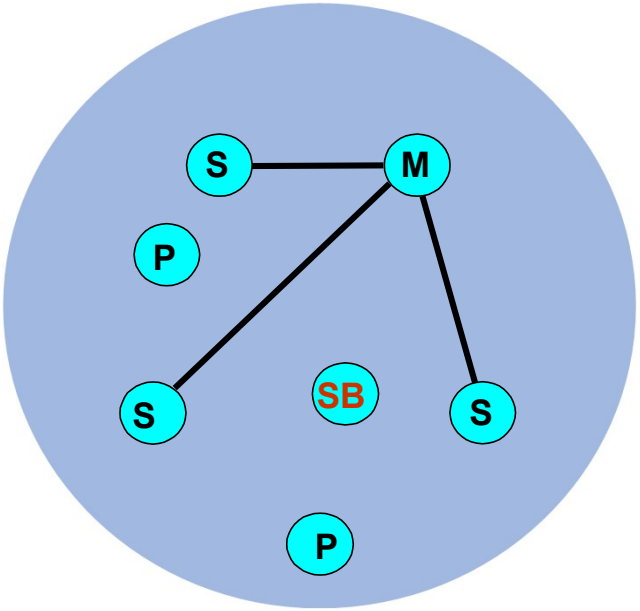
- Signal broadcast over seemingly random series of frequencies
- Receiver hops between frequencies in sync with transmitter
  - Each frequency has the bandwidth of the original signal
  - Dwell time is the time spent using one frequency
- Spreading code determines the hopping sequence
  - Must be shared by sender and receiver (e.g. standardized)
- Eavesdroppers hear unintelligible blips
- Jamming on one frequency affects only a few bits
  - Typically large number of frequencies used
    - Improved resistance to jamming

Hang on a minute!

- Wi-Fi 2.4GHz and Bluetooth share the same spectrum!
  - Wi-Fi: from 2400 MHz to 2483.5 MHz
  - BT: from 2402 MHz to 2480 MHz
- How do they work this way?
  - Wi-Fi uses CSMA/CA
  - BT uses Adaptive Frequency Hopping (AFH), avoiding channels currently busy with Wi-Fi transmissions
  - Modern devices use coexistence hardware, which coordinates both radios if they share an antenna or module
- So, there is interference… (somewhat reduced, but there is)

Piconets

- Bluetooth devices connected in an “ad-hoc” cell
- There is a Master with up to 7 active slaves and several hundreds parked
  - Slaves only communicate with master
  - Slaves must wait for permission from master
- Master defines radio parameters (”clock” and “deviceID”)
  - Channel, hopping sequence, timing, …
- Each piconet has an unique FH pattern (and a single ID)
- Each piconet has a maximum bandwidth (1 MSPS)
- A slave in one piconet can also be part of another piconet
  - Either as a master or as a slave
  - If master, it can create scatternets

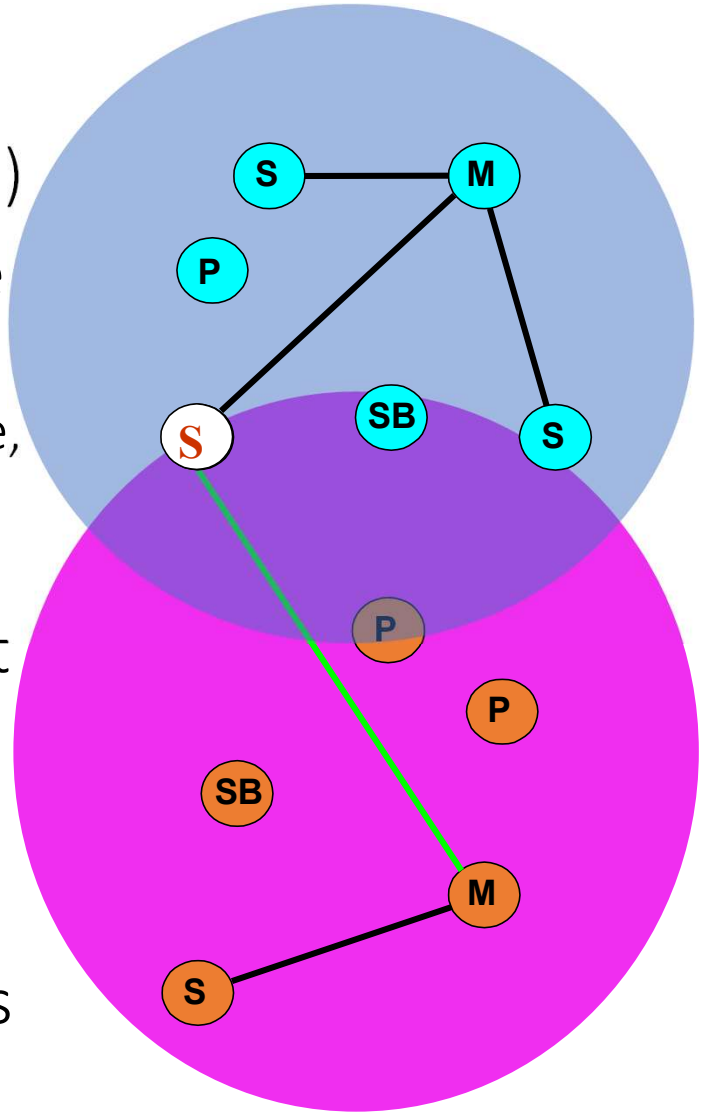


M=Master
S=Slave

P=Parked
SB=Standby

Scatternet

- Connection of several piconets
- Through a common device (bridge) (M/S)
- One device can be M/S at the same time
  - Or at least Slave in two piconets
  - Bridge node “stay” in a piconet for some time, then switch to another piconet by changing hop sequence.
- Global system BW unlimited, but piconet BW always <1Mbps
- Impact on piconets is minimal for < 10 piconets.
- Potentially any device can share piconets
  - Reality: limitations on commercial stacks



M=Master
S=Slave

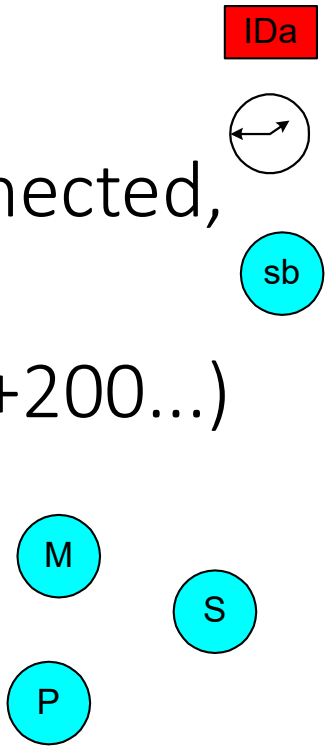
P=Parked
SB=Standby

Outline

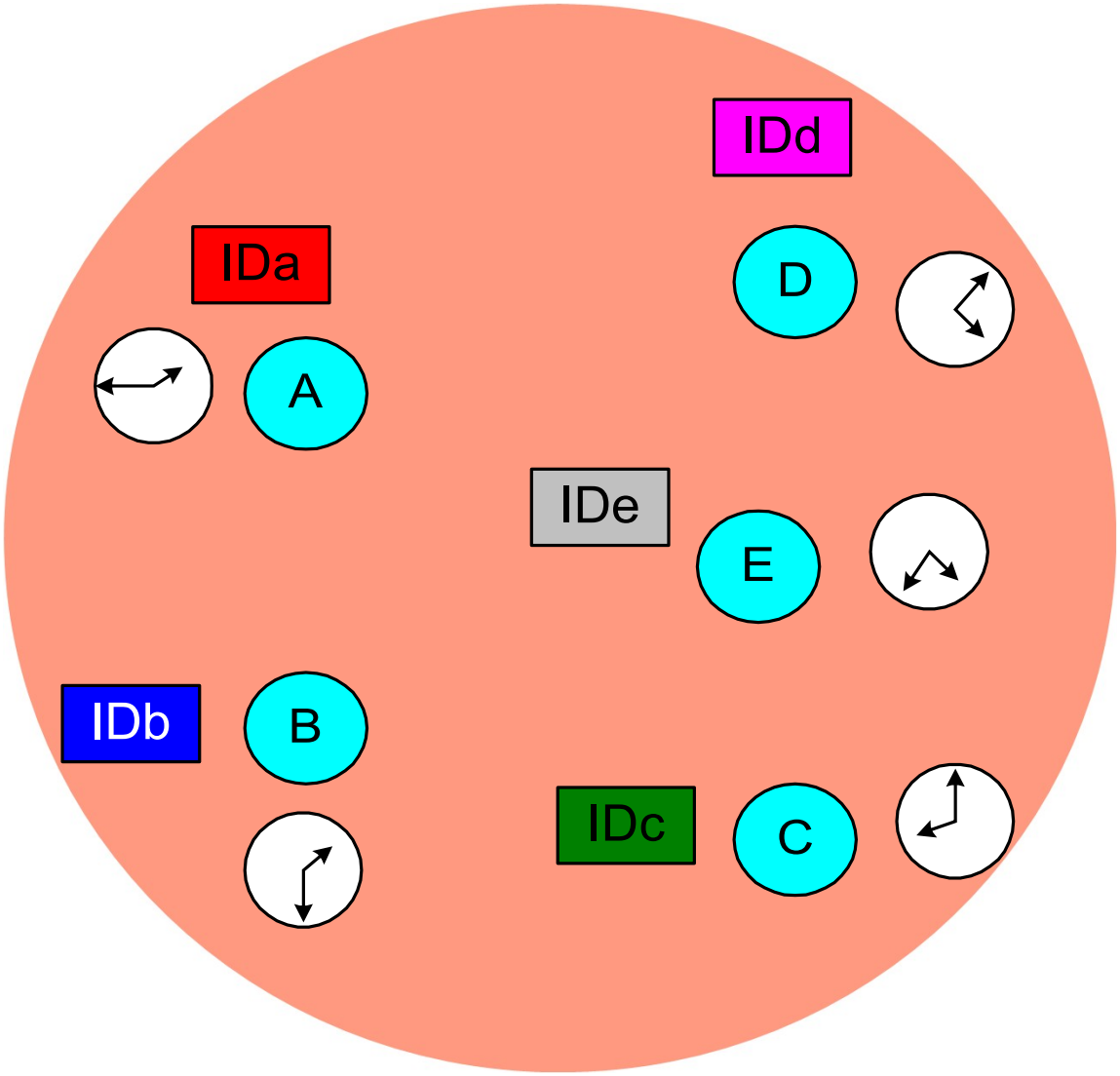
- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- 802.15.x

Piconet operation

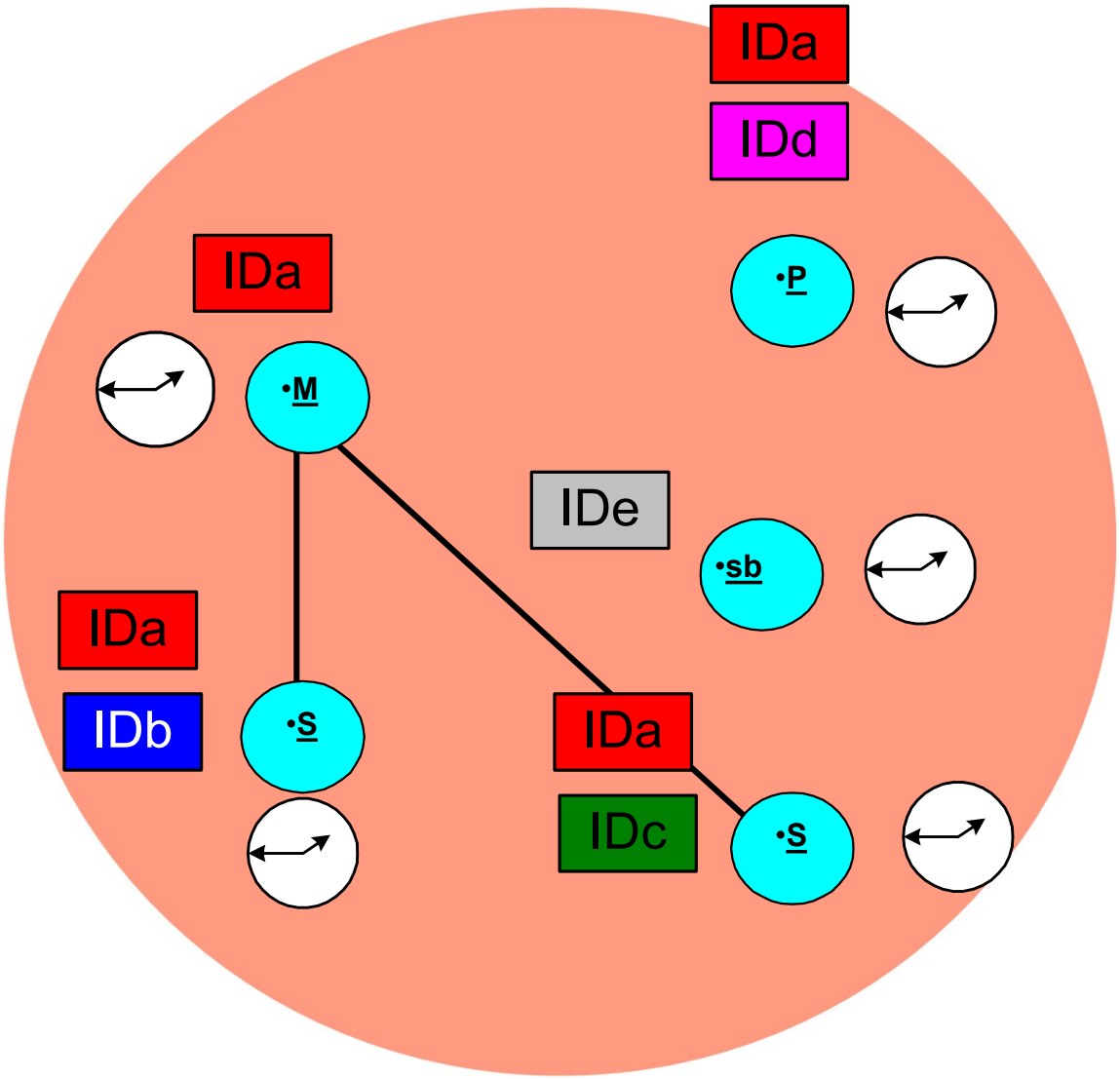
- FHSS: all devices must share the same hopping pattern:
  - M*aster* provides clock and deviceID such that:
    - deviceID (48-bits) defines hopping pattern
    - Clock defines phase inside the pattern
- If a device is inside a piconet, and is not connected, it must be in *standby*
- There are two types of piconet addresses (7+200...)
  - *Active Member Address* (AMA, 3-bits)
  - *Parked Member Address* (PMA, 8-bits)
    - Logically connected to piconet but not actively participating in communication



Piconet before setup



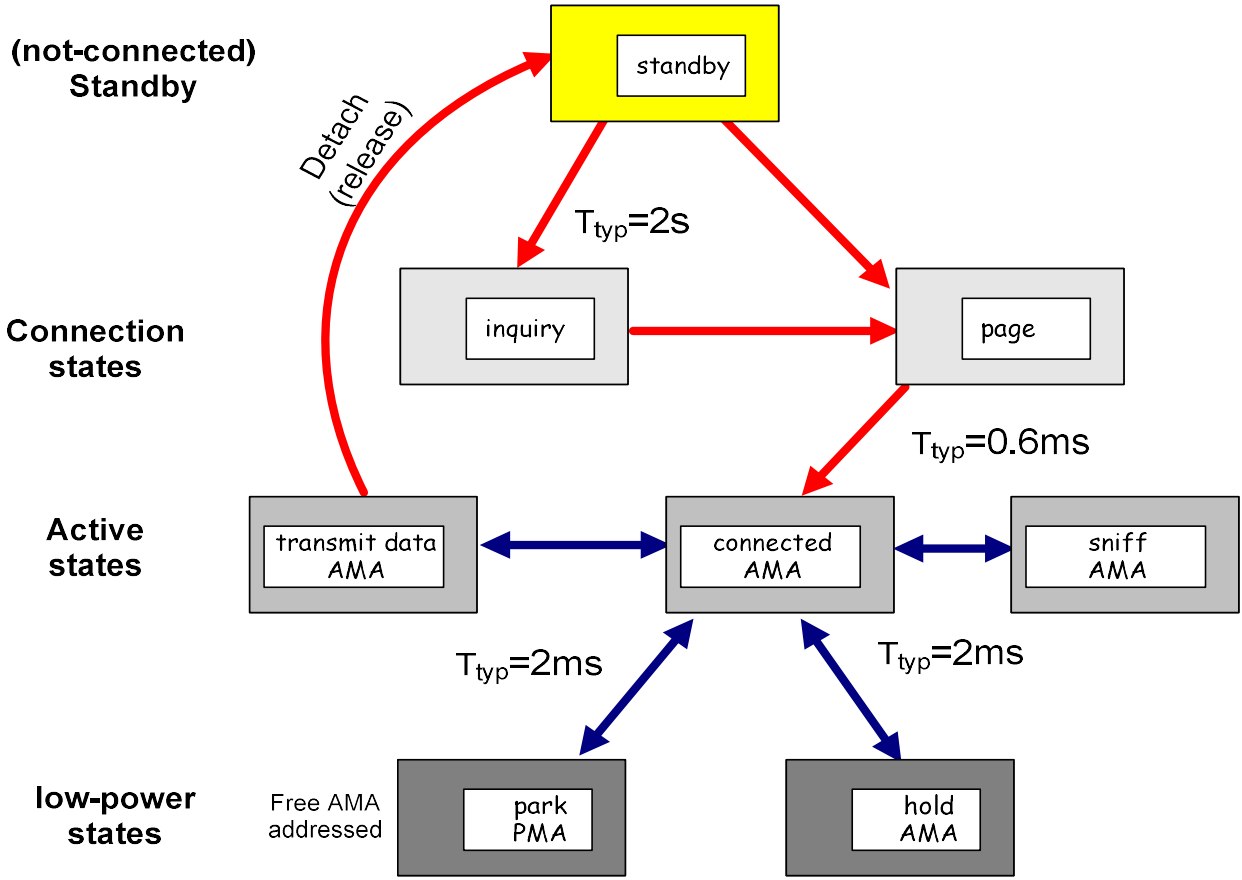
Piconet in operation



Piconet built!

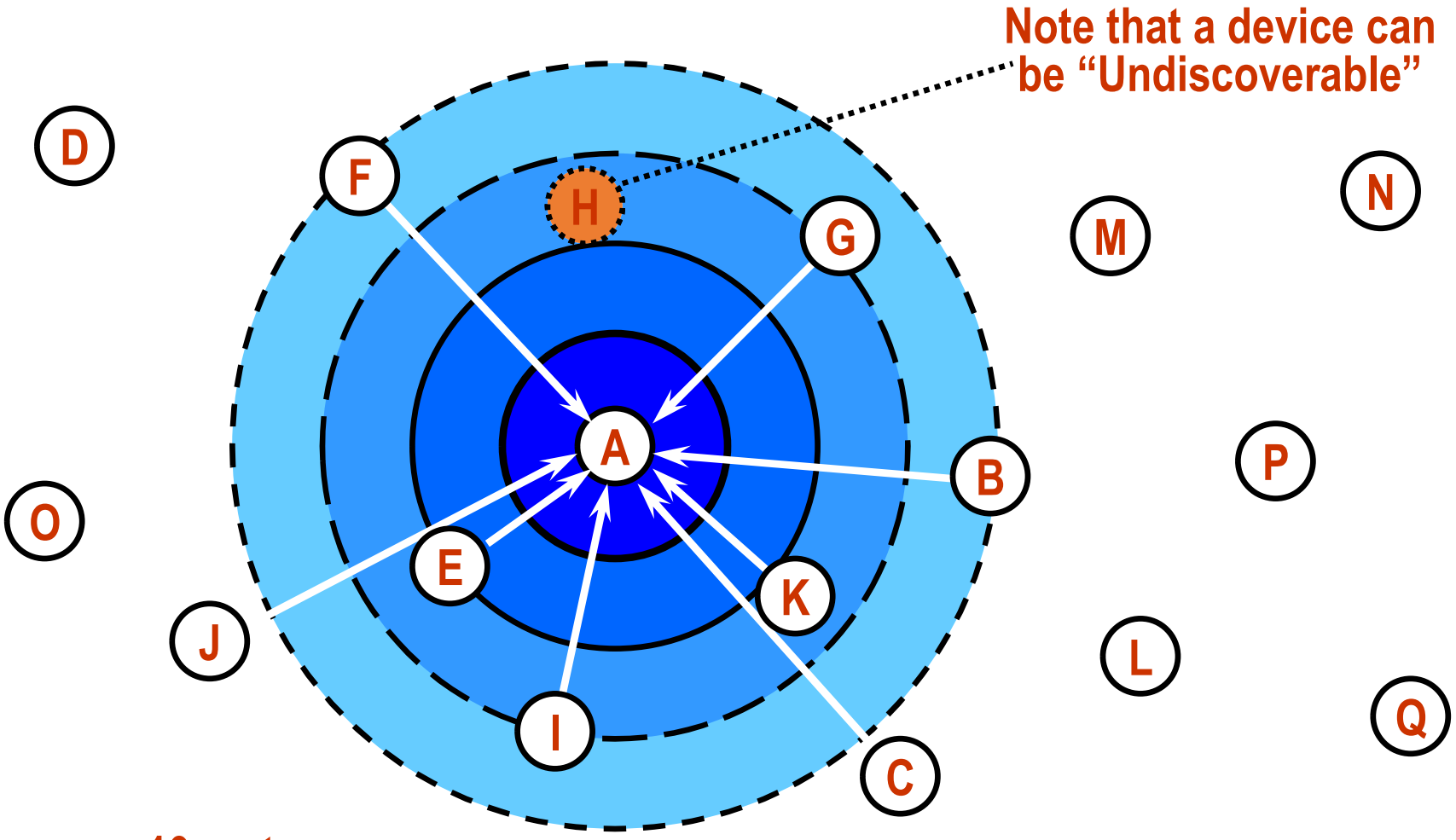
Device states

- Standby
  - Waiting to join a piconet
- Inquire
  - Ask about radios to connect to (discover nodes)
- Page
  - Connect to a specific radio
- Connected
  - Active on a piconet (master or slave)
- Park/Sniff/Hold
  - Low Power connected states
    - Park: fully inactive, but synchronized
    - Sniff: Listens periodically
    - Hold: Temporarily stops data exchange (still active, but inactive for a period)



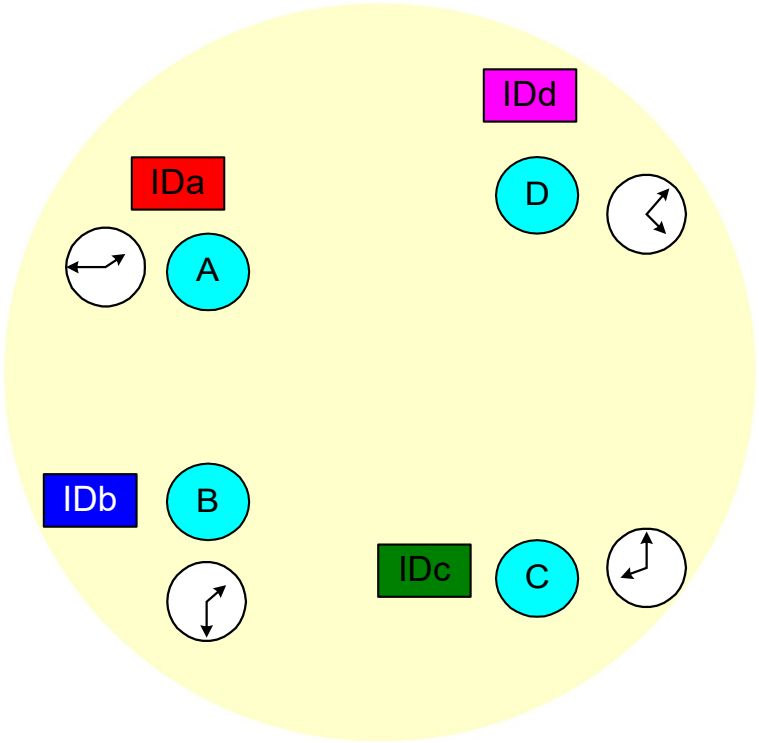
AMA: Active Member Address
PMA: Park Member Address

Device Discovery Illustrated



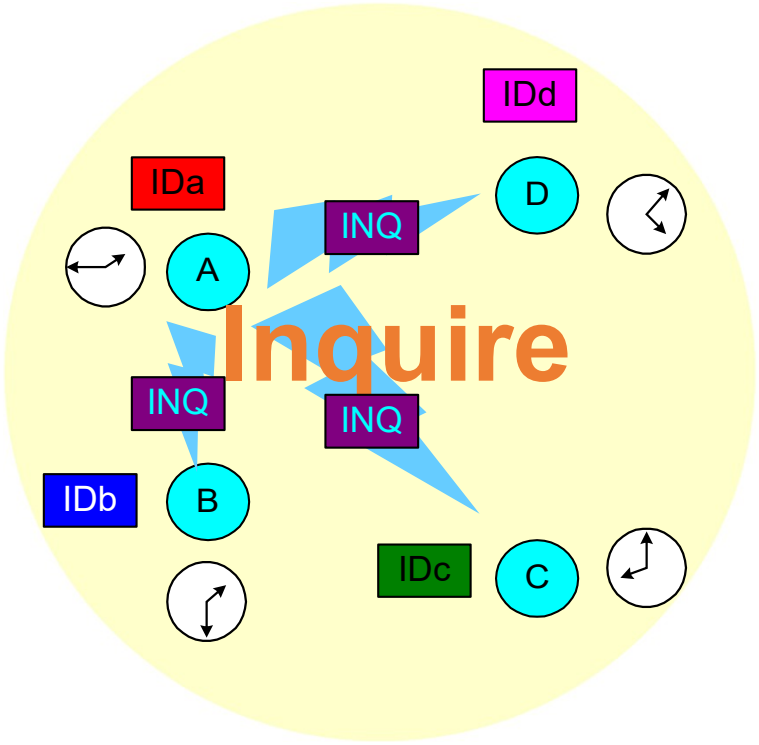
After inquiry procedure, A knows about others within range

Scanning units



- Device A wants to search for stations

Scanning units

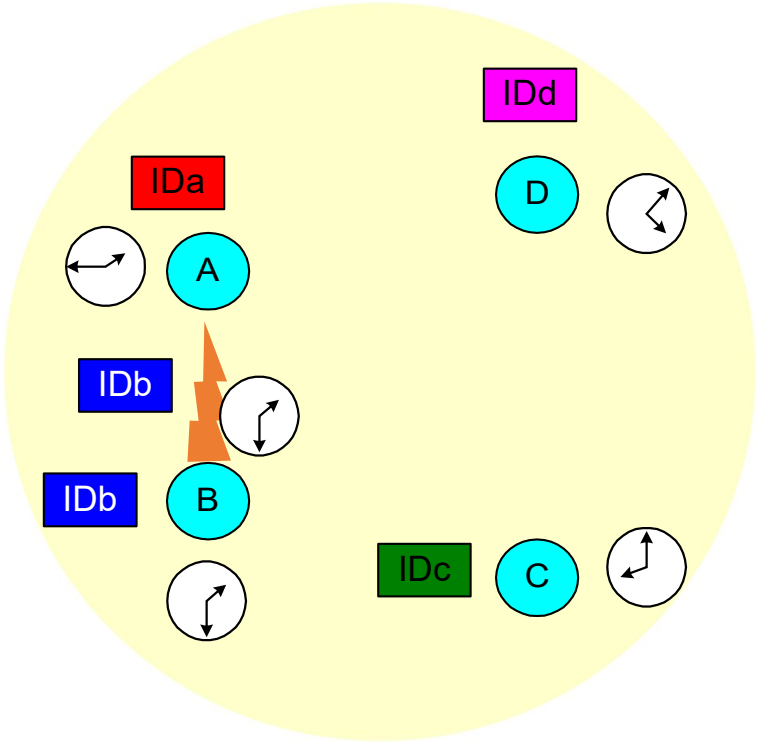


Device A wants to search for stations

A does an inquire (page with ID 000)

Devices B,C,D are doing an inquire scan

Scanning units



Device A wants to search for stations

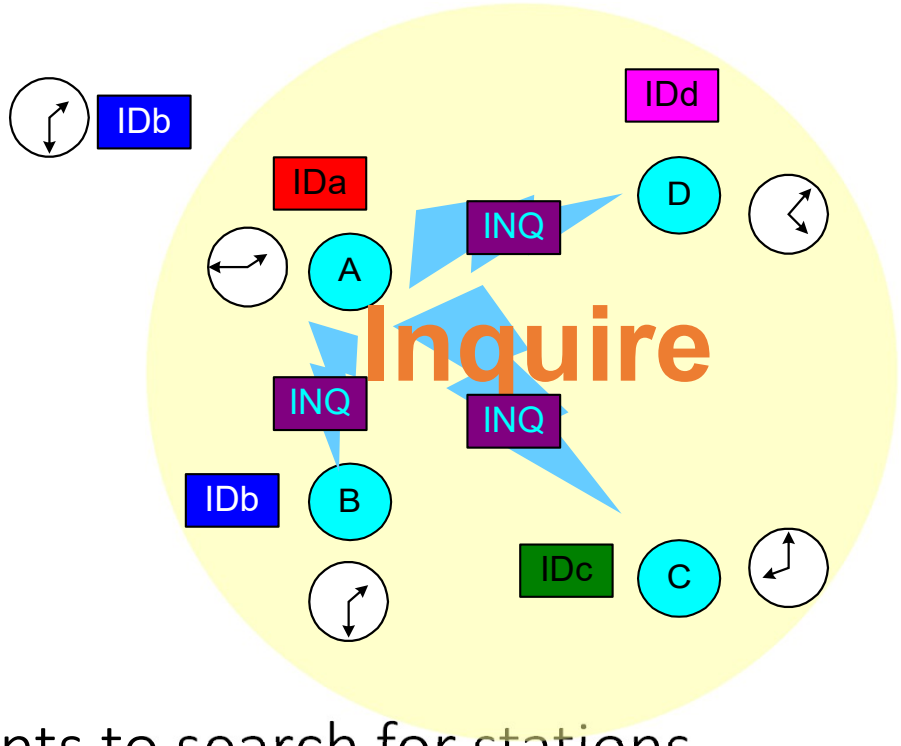
A does an inquire (page with ID 000)

Devices B,C,D are doing na inquire scan

B answers with FHS packet

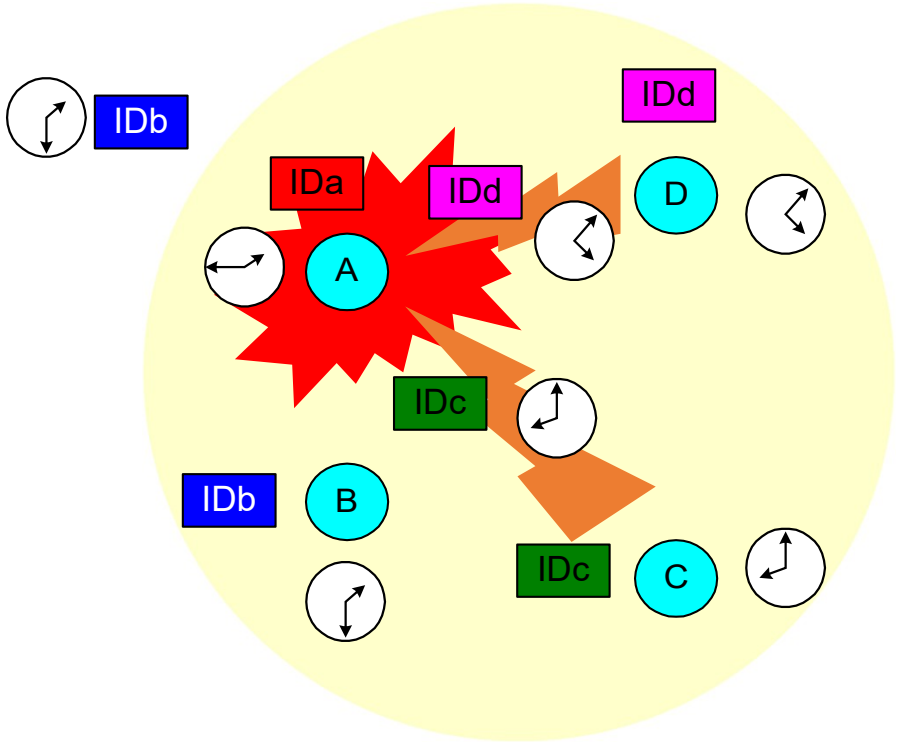
Contains *DeviceID* and *Clock*

Scanning units



- Device A wants to search for stations
- A does an inquire (page with ID 000)
  - Devices B,C,D are doing an inquire scan
- B answers with FHS packet
  - Contains DeviceID and Clock
- A does an inquire again

Scanning units



A wants to search for stations

A does an inquire again

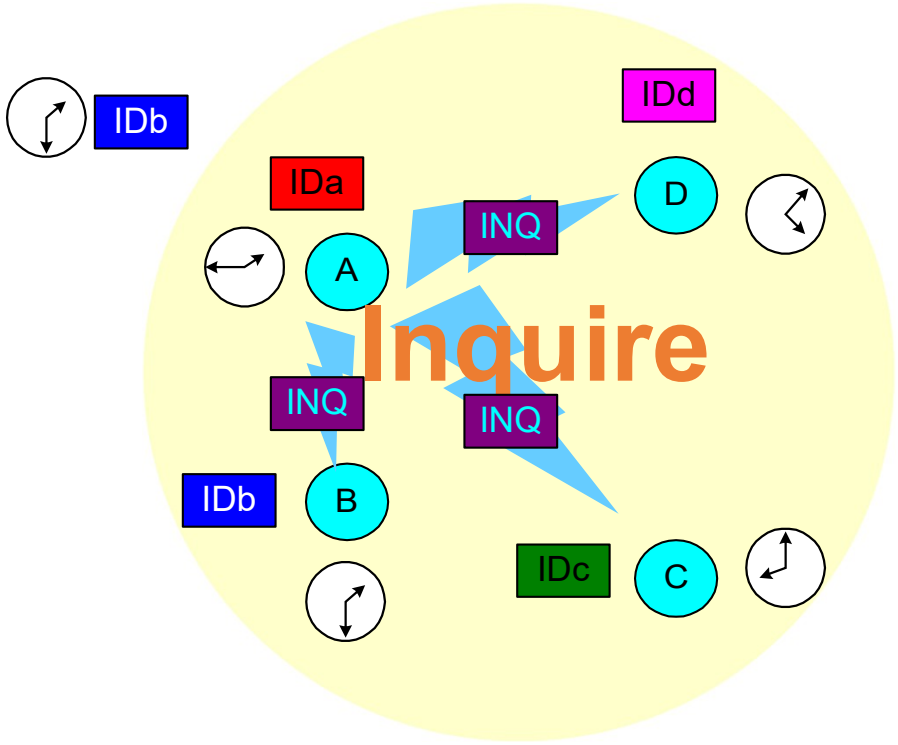
C e D answer at the same time with FHS packet

Packets are corrupted

A does not answer

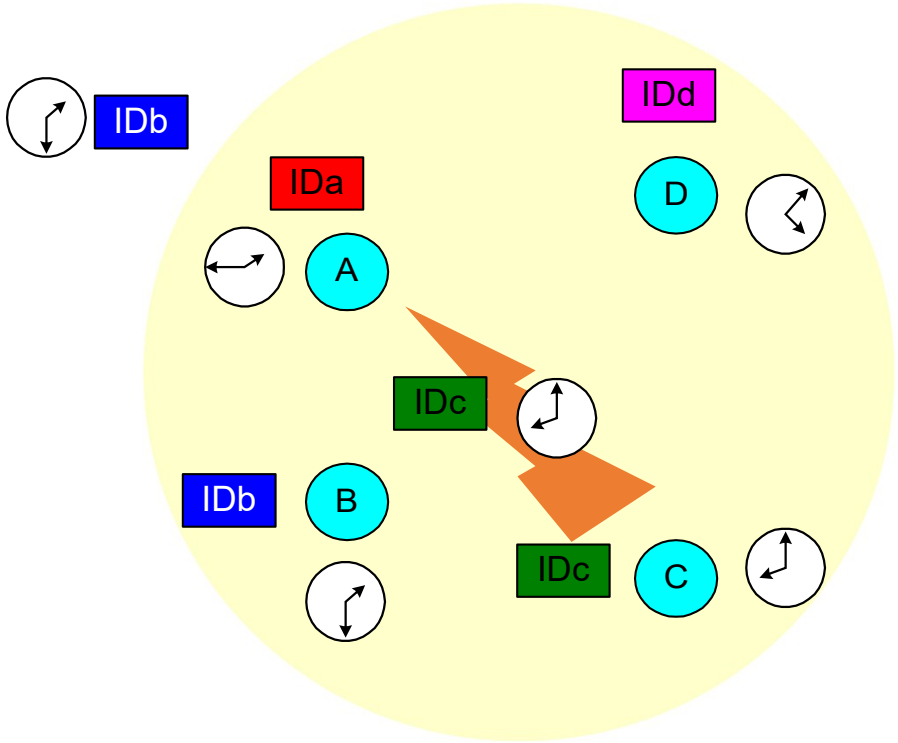
C and D will wait an random number of slots

Scanning units



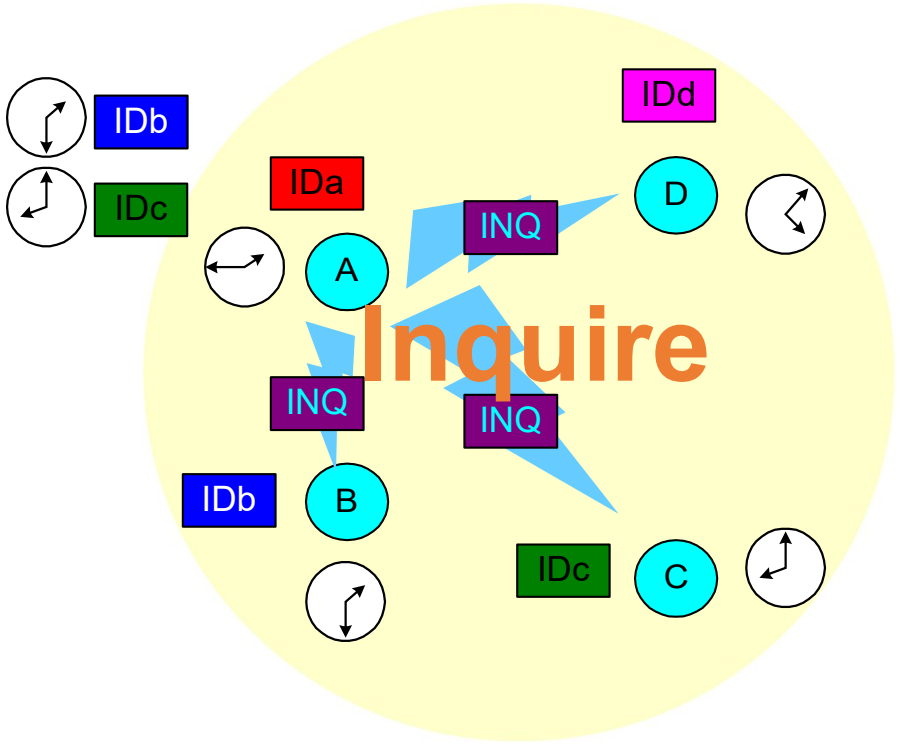
- A wants to search for stations
- A does an inquire again

Scanning units



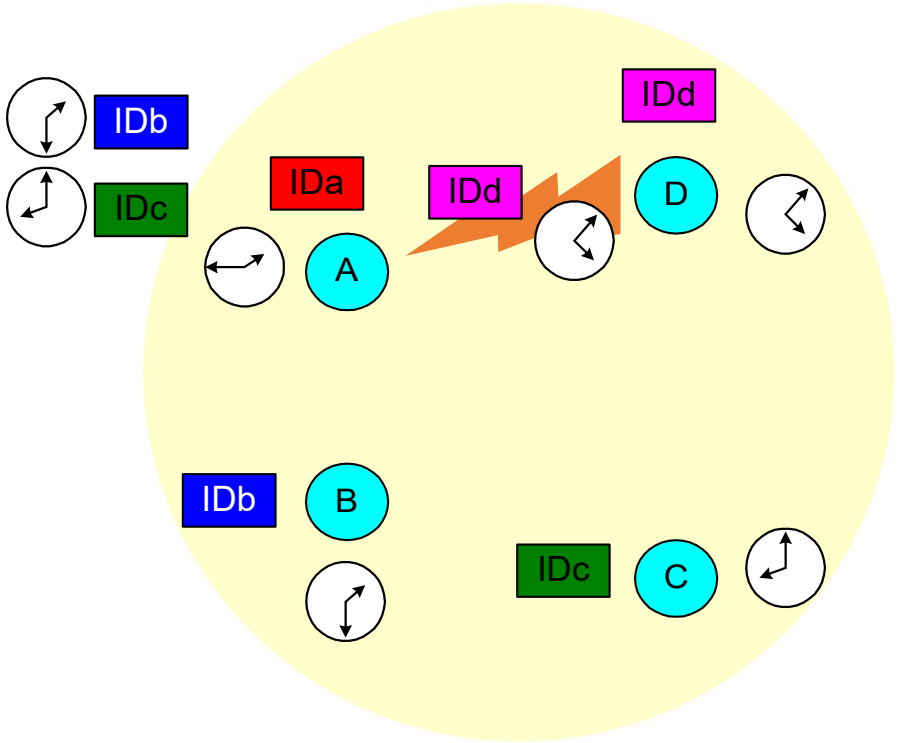
- A wants to search for stations
- A does an inquire again
- C answers with FHS packet

Scanning units



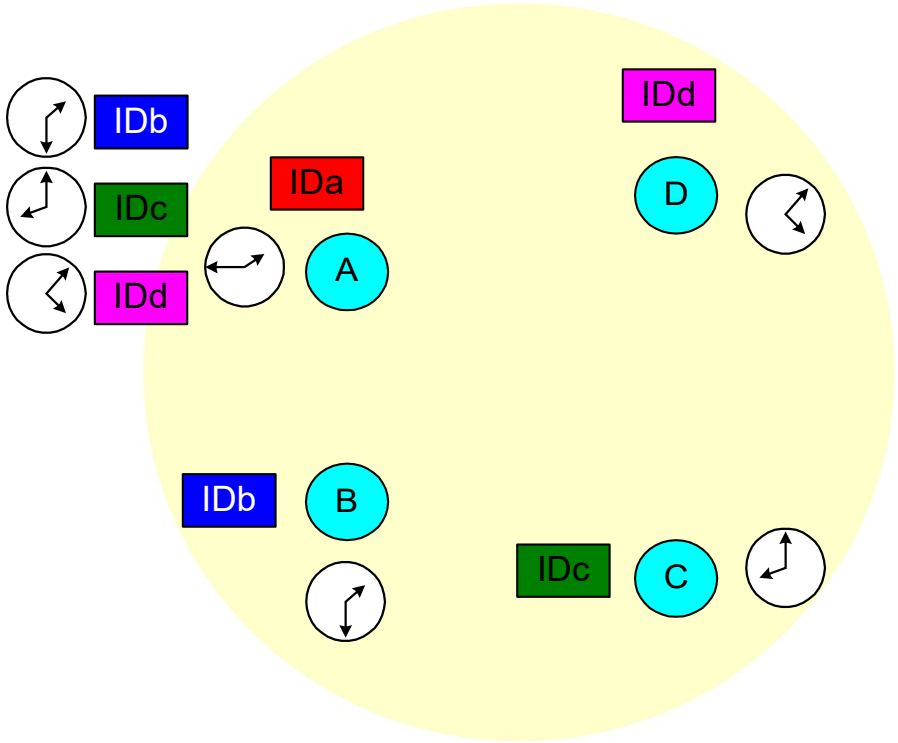
A wants to search for stations
A does an inquire again

Scanning units



- A wants to search for stations
- A does an inquire again
- D answers with FHS packet

Scanning units



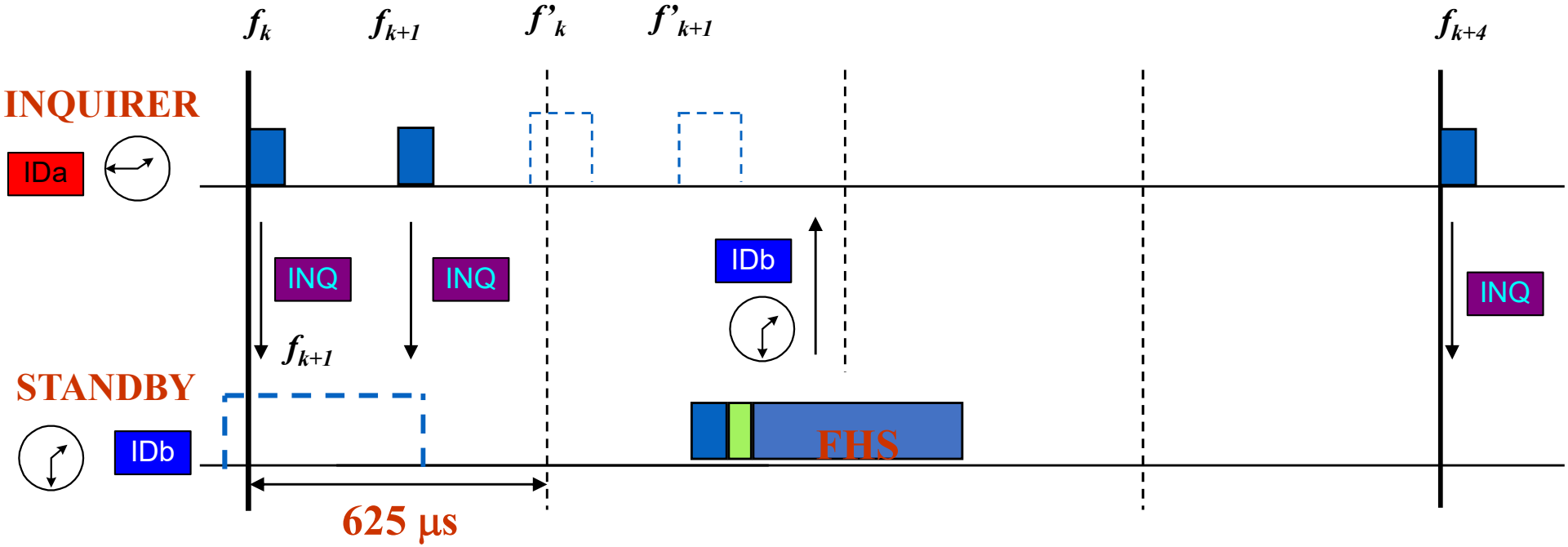
- A has all the information it needs about the units in the cell.

Inquiry scanning: summary

- Inquiry scanning has a common address
  - And a common frequency pattern (from 32 frequencies)
- All devices can page this address (and become masters)
- All machines hearing an inquiry will answer the inquiry request
- There is a detector (correlator hit) in the slaves, that detects inquiries, before answering with a FHS providing:
  - Device ID and Clock
- A machine in low power waits a random time before answering again to a scan
- If there is a collision on answering to a scan, they also wait a random period before answering again

Timing: Inquiry

- Inquiry requires two packets before the slave answers
  - To cover all channels (16 at a time) due to being unsynchronised (BT hops 1600 times per second)
  - 625 block

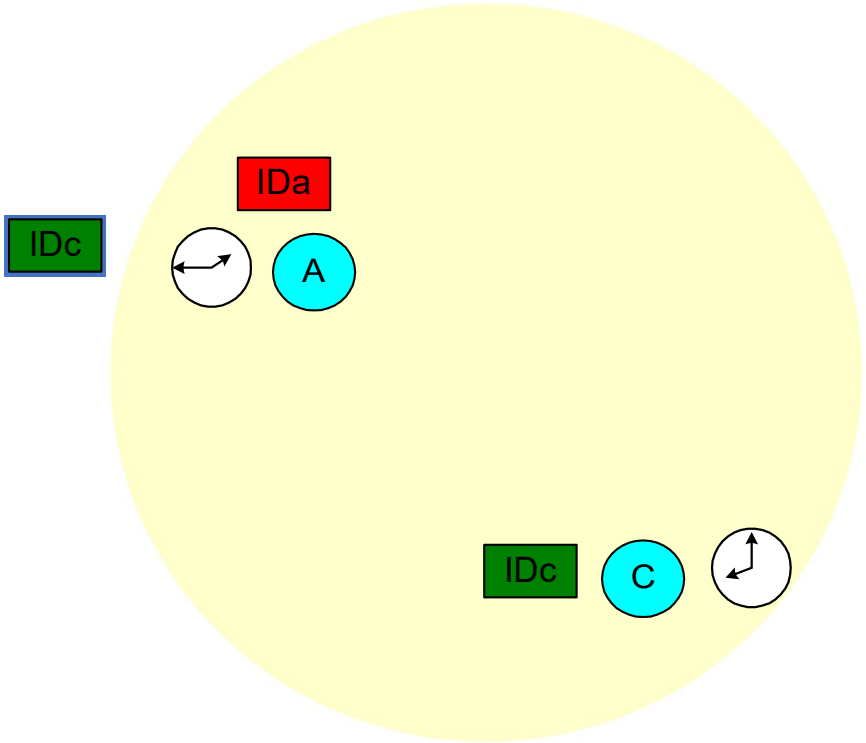


Paging: Will you connect to me?

- Very similar to inquire
- Still have not synchronized clocks or frequencies
- Establishes actual Piconet connection with a device that it knows about
- Connection process involves a 6 steps of communication between the master and the slave

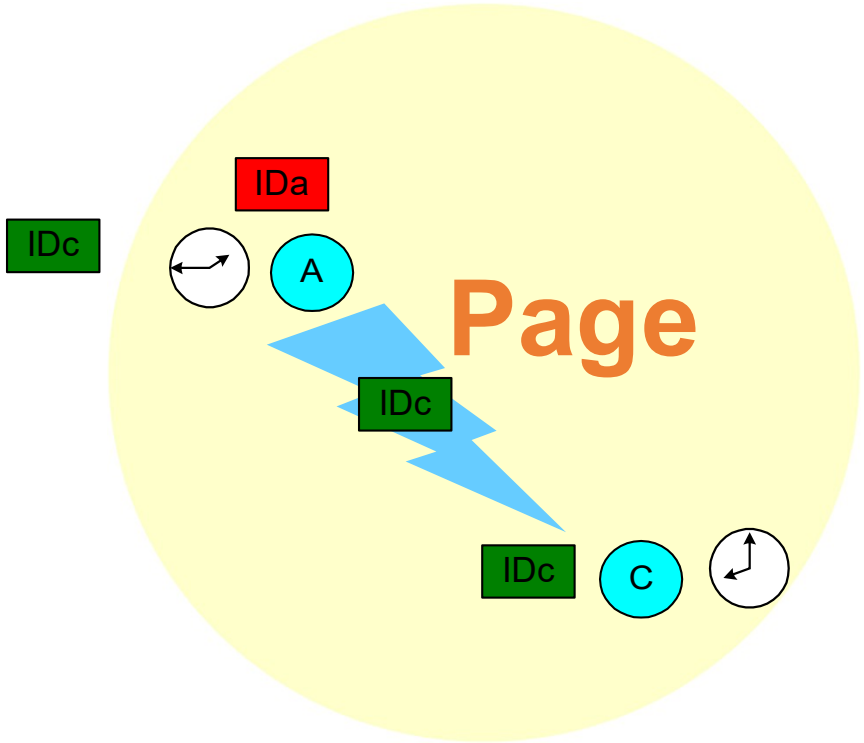
Step	Message	Direction	Hopping Pattern	Pattern Source and Clock
1	Slave ID	Master to Slave	Page	Slave
2	Slave ID	Slave to Master	Page Response	Slave
3	FHS	Master to Slave	Page	Slave
4	Slave ID	Slave to Master	Page Response	Slave
5	1st Master Packet	Master to Slave	Channel	Master
6	1st Slave Packet	Slave to Master	Channel	Master

Master Paging Slave



- Paging:
  - Assumes that the master has the Device ID and Clock

Master Paging Slave

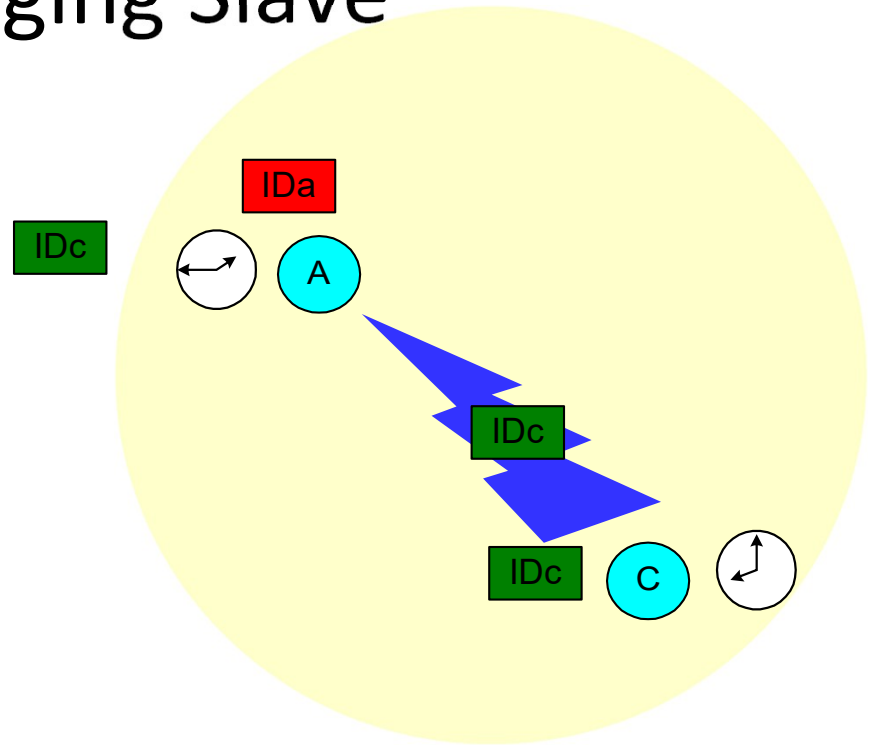


- Paging:

  Assumes that the master has the *Device ID* and *Clock*

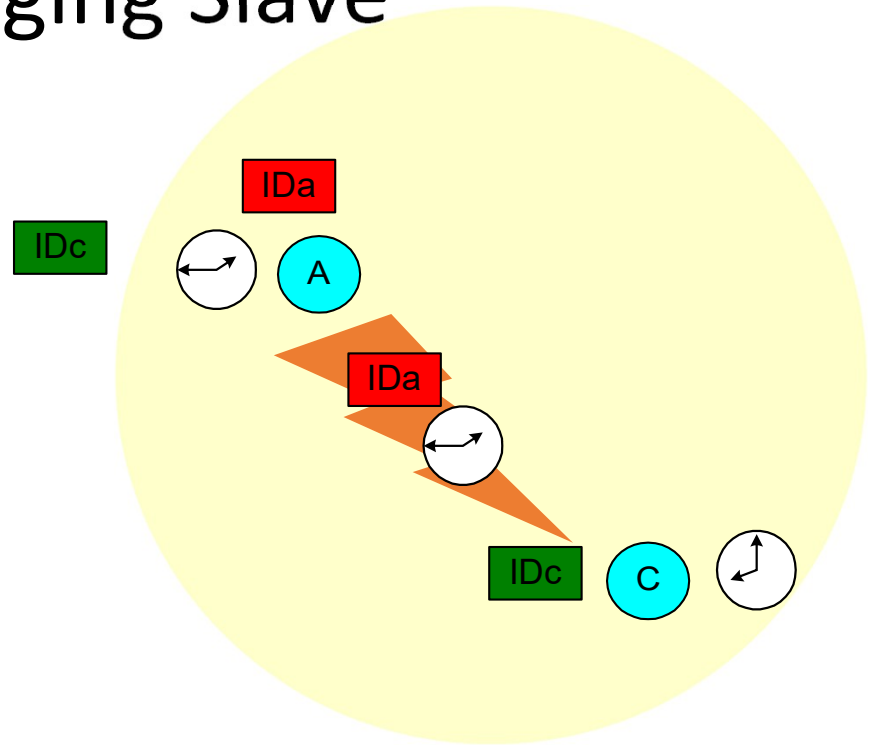
  – *A* pages C with the *deviceID* of C

Master Paging Slave



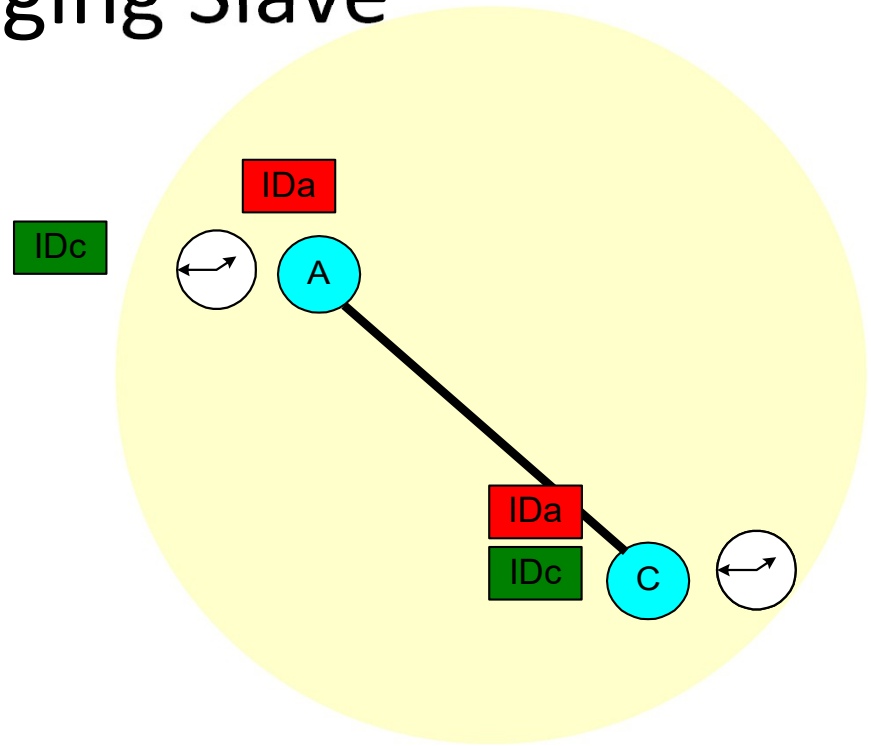
- Paging: master has the Device ID and Clock
  - A pages C with the deviceID of C
  - C answers A with his deviceID

Master Paging Slave



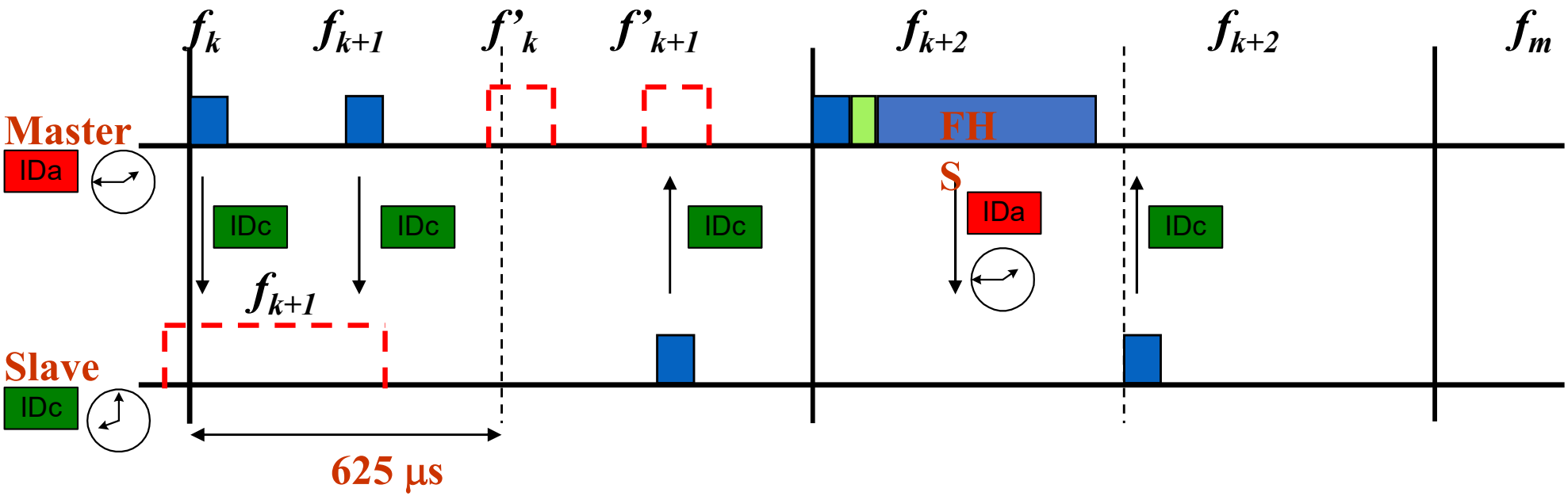
- Paging: master has the *Device ID* and *Clock*
  - *A* pages C with the *deviceID* of C
  - C answers A with his *deviceID*
  - A send C his *deviceID* and *Clock* (FHS packet)

Master Paging Slave



- Paging: master has the *Device ID* and *Clock*
  - *A* pages C with the *deviceID* of C
  - C answers A with his *deviceID*
  - A send C his *deviceID* and *Clock* (FHS packet)
  - A becomes master of C

Time: Master Paging Slave

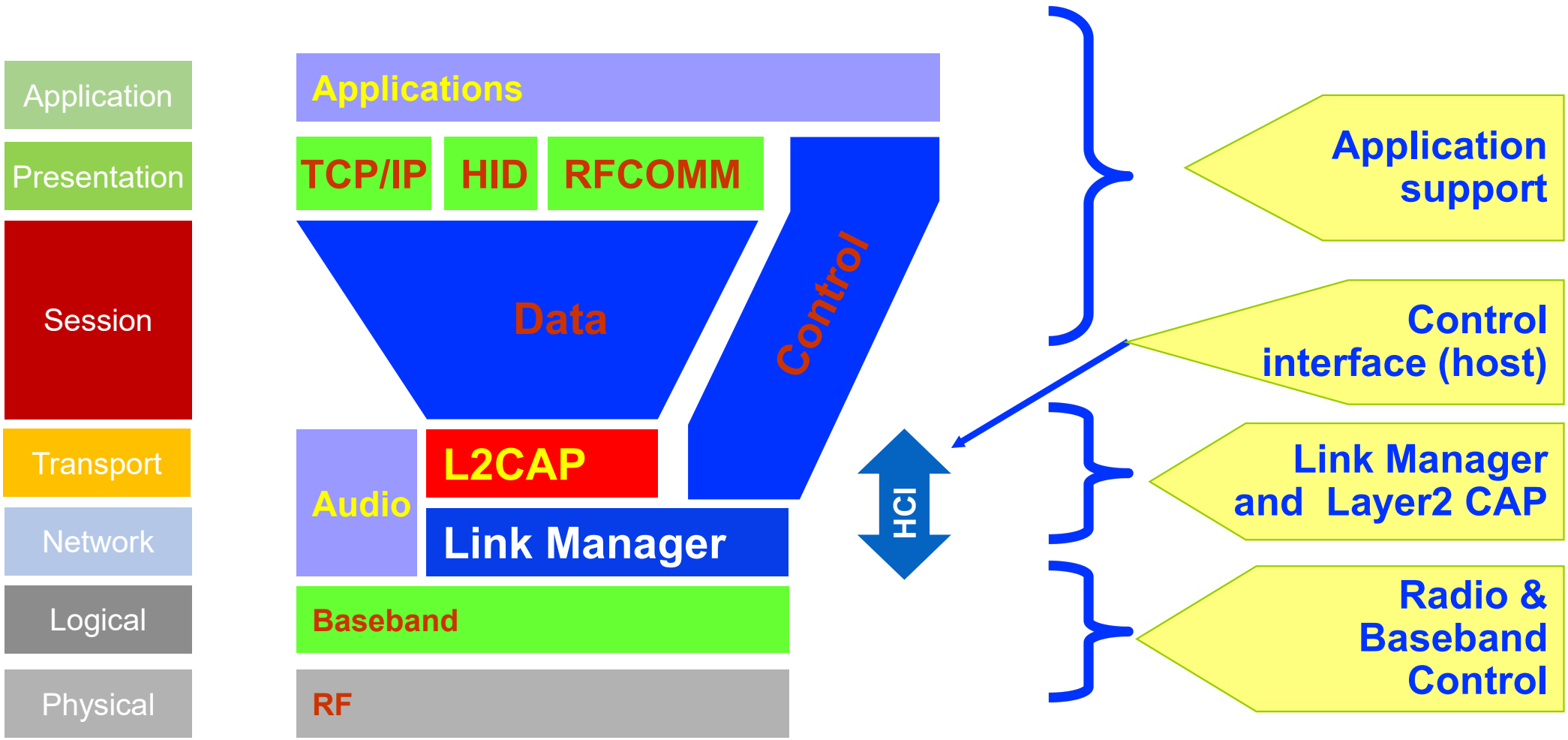


- Master pages slave (packet has slave's ID) at the paging frequency of the slave (1 of 32)
  - Master send a train of 16 fqs in the slave hop set.
    - Slave ID sent twice in the slave frequency
    - Master waits for two answers in the slave frequency
  - If it does not work, master will send
- Slave listens for 11 ms (page scan)
  - If it identifies packets, slave wakes up and sends packets in that frequency.
  - Master answers with FHS (Device ID e Clock)
  - Slave joins piconet.

Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- 802.15.x

stack Bluetooth



Bluetooth includes:

- A HW description
- An environment for applications

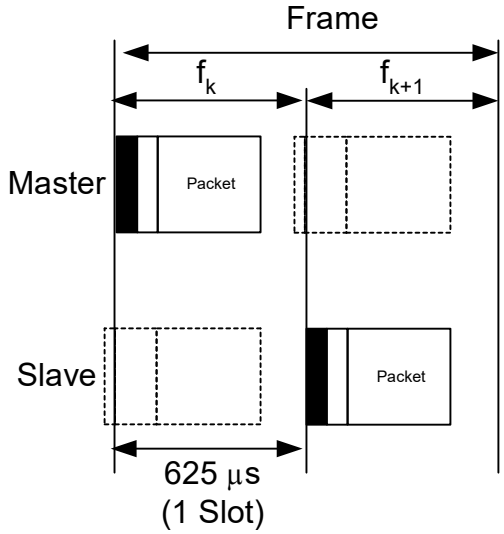
L2CAP:	Logical Link Control and Adaptation Protocol
LMP:	Link Manager Protocol
HID:	Human Interface Device
RFCOMM:	serial cable emulation (ETSI)

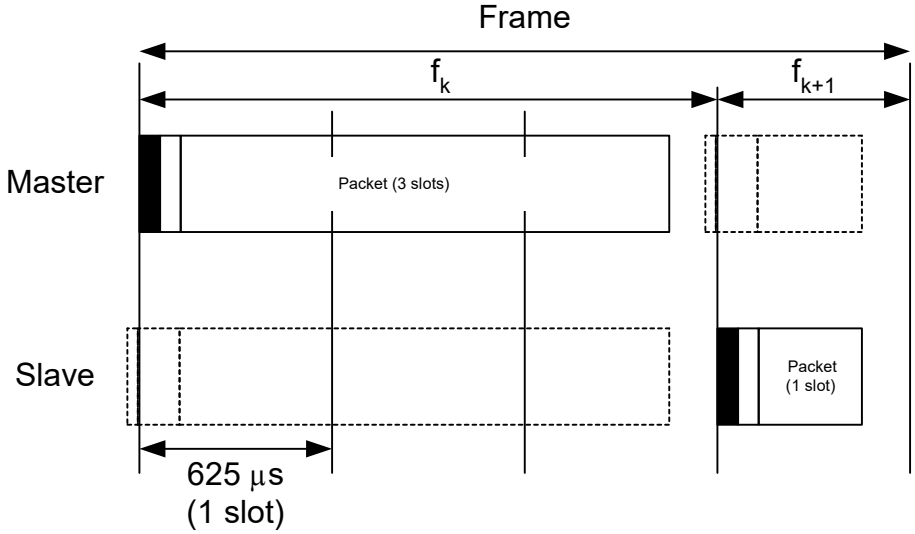
Bluetooth Protocol

- Radio layer
  - Defines requirements for a Bluetooth radio transceiver
  - Handles conformity to 2.4GHz (ISM) band
  - Establishes specifications for using Spread-Spectrum Frequency Hopping (FHSS)
  - Classifies device into one of three power classes:
    - Long range; Class 1 - 100mW, 100m
    - Normal/standard range; Class 2 - 2.5mW, 10m
    - Short range; Class 3 - 1 mW, 1m

Radio Layer

- Radio: FH SS
  - 79/23 channels of 1 Mb/s
    - 23 → France (although now is harmonized)
    - 23 → Low cost implementations
  - Hoping: per slot
    - Packets have 1, 3, or 5 slots of 625 microseconds
      - Control, Medium Data or Large Data
    - Hoping (nominal) 1600 times per second
  - Frame includes two packets
    - BT shares one frequency channel between two devices
    - It alternates transmit and receive in time
      - Transmission followed by reception
    - Alternation is done in 625microseconds
  - Radio designed to low cost and universal usage
    - noise, synchronous action technology 2.4GHz, etc…,

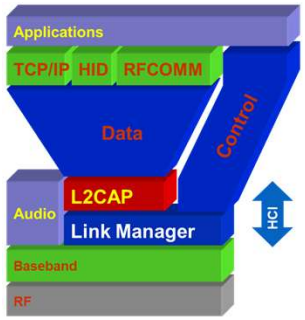




Baseband in Bluetooth

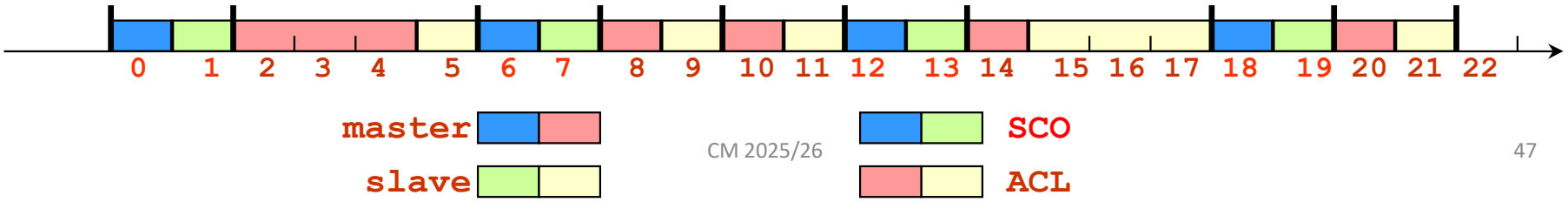
- Manages physical channels and logical lines
  - Controls device addressing, channel control, power-saving operations, and flow control and synchronization among devices
  - Implements TDD aspects: master and slave switch in communications

- Works closely with Link controller:
  - Manages link (a)synchronism
  - Controls paging and inquiries
  - Controls power save modes

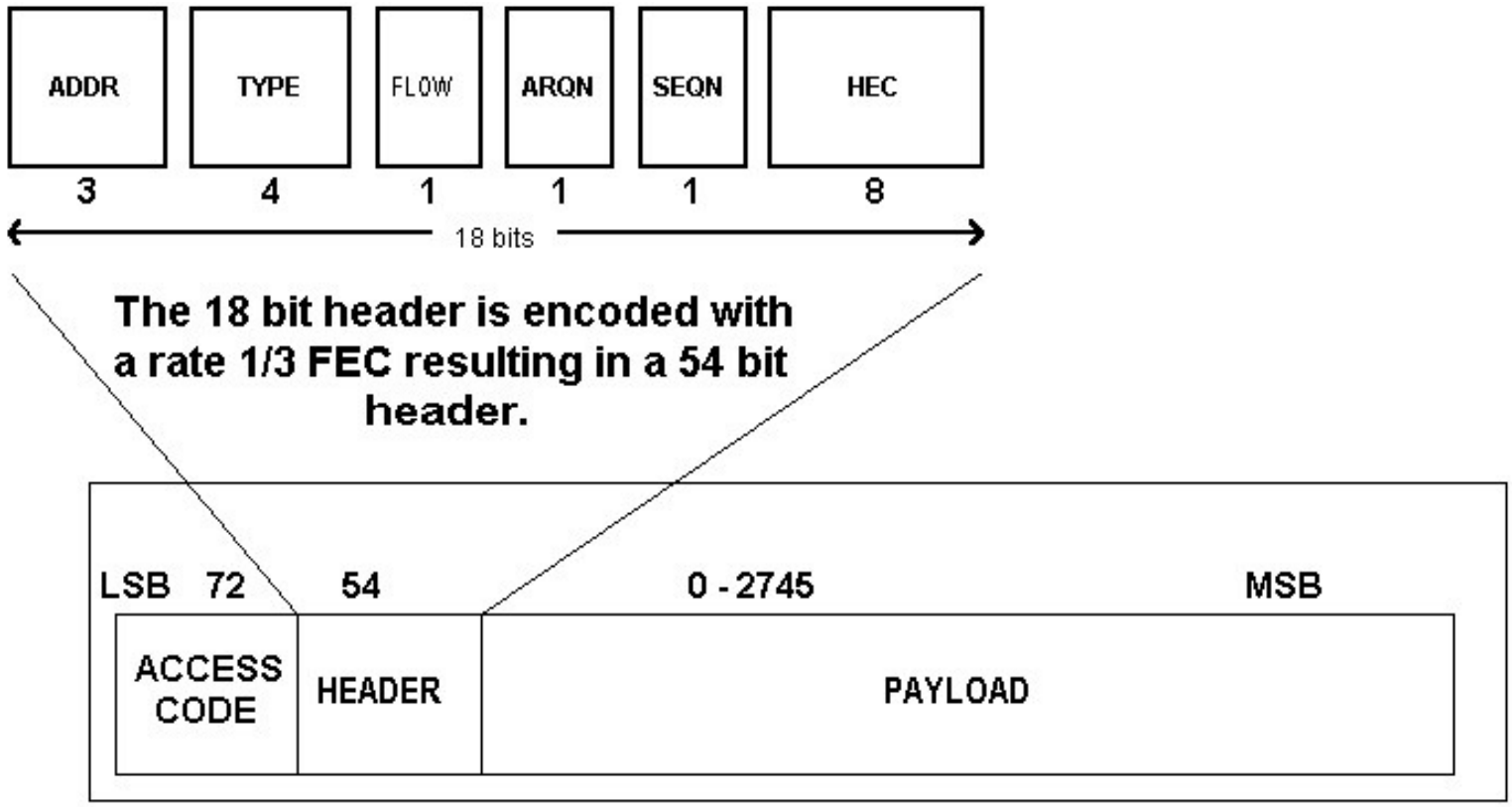


Baseband link types

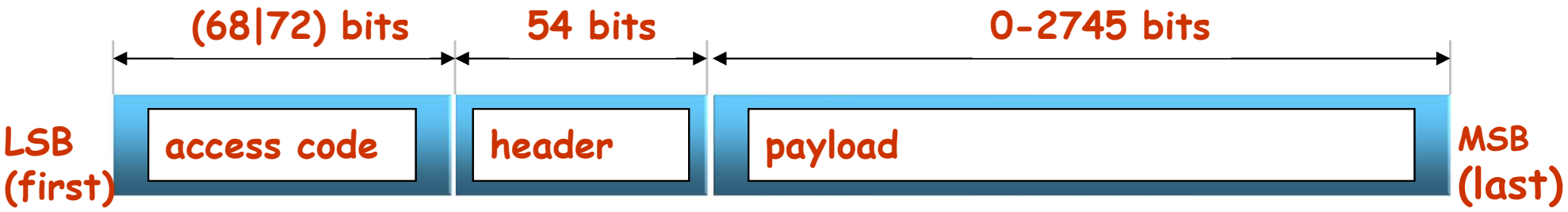
- Polling-based (TDD) frame transmissions
  - 1 slot: 0.625msec (max 1600 slots/sec)
  - Master/slave slots (even-/odd-numbered slots)
  - Polling: master always “polls” slaves
- Synchronous Connection-Oriented (SCO) link
  - “Circuit-switched”
    - periodic single-slot frame assignment
  - Symmetric 64Kbps full-duplex
- Asynchronous Connection-Less (ACL) link
  - Frame switching
  - Asymmetric bandwidth
    - Variable frame size (1-5 slots)
      - max. 721 kbps (57.6 kbps return channel)
      - 108.8 - 432.6 kbps (symmetric)



Baseband Packet



Baseband Frame



- Access Code: time synchronization, offset, paging, inquiry.
  - Channel Access Code (CAC), piconet identification, synchronization, DC offset.
  - Device Access Code (DAC), paging and replies.
  - Inquiry Access Code (IAC), inquiries (GIAC, general; DIAC, dedicated)
- Header: packet acknowledgement and numbering, flow control, slave address, error checking
- Payload: voice, data or both (DV packets)
  - When data, the payload has additional internal header

Packets (common)

TYPE	NAME	#	DESCRIPTION
Common	ID	1	Carries device access code (DAC) or inquiry access code (IAC).
	NULL	1	NULL packet has no payload. Used to get link information and flow control. Not acknowledged.
	POLL	1	No payload. Acknowledged. Used by master to poll the slaves to know whether they are up or not.
	FHS	1	A special control packet for revealing Bluetooth device address and the clock of the sender. Used in page master response, inquiry response and frequency hop synchronization. 2/3 FEC encoded.
	DM1	1	To support control messages in any link type. can also carry regular user data. Occupies one slot.

DM1 – Data Medium rate, 1-slot Packet

Packets: Synchronous Connection-oriented

SCO	HV1	1	Carries 10 information bytes. Typically used for voice transmission. 1/3 FEC encoded.
	HV2	1	Carries 20 information bytes. Typically used for voice transmission. 2/3 FEC encoded.
	HV3	1	Carries 30 information bytes. Typically used for voice transmission. Not FEC encoded.
	DV	1	Combined data-voice packet. Voice field not protected by FEC. Data field 2/3 FEC encoded. Voice field is never retransmitted but data field can be.

HM1 – Header + Medium rate, 1-slot packet with Synchronous Connection-Oriented
DV –Data + Voice

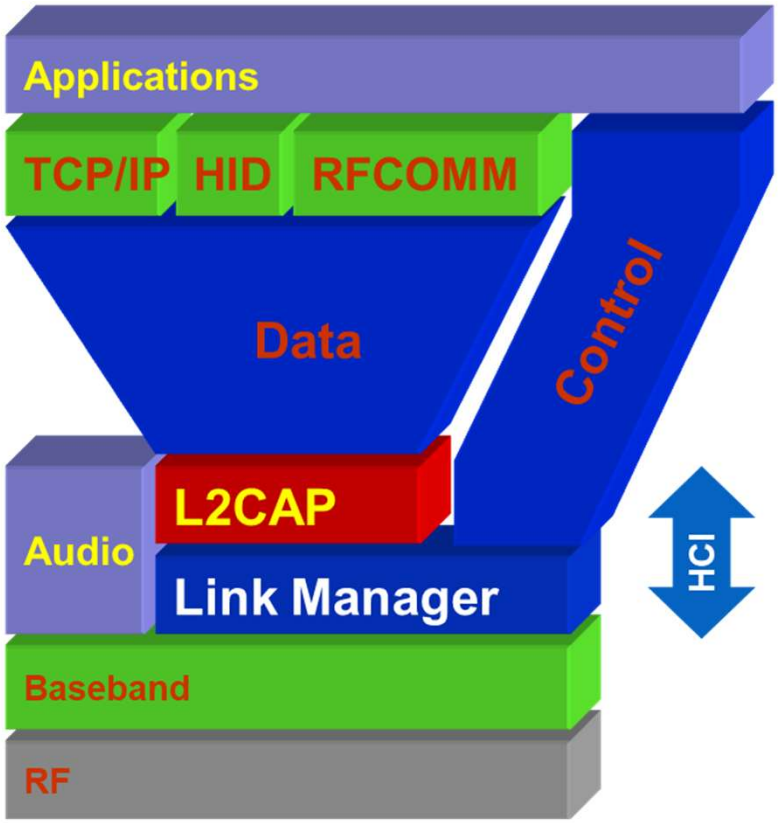
Packets : Assynchronous Connection-Less

ACL	DM1	1	Carries 18 information bytes. 2/3 FEC encoded.
	DH1	1	Carries 28 information bytes. Not FEC encoded.
	DM3	3	Carries 123 information bytes. 2/3 FEC encoded.
	DH3	3	Carries 185 information bytes. Not FEC encoded.
	DM5	5	Carries 226 information bytes. 2/3 FEC encoded.
	DH5	5	Carries 341 information bytes. Not FEC encoded.
	AUX1	1	Carries 30 information bytes. Resembles DH1 but no CRC code.

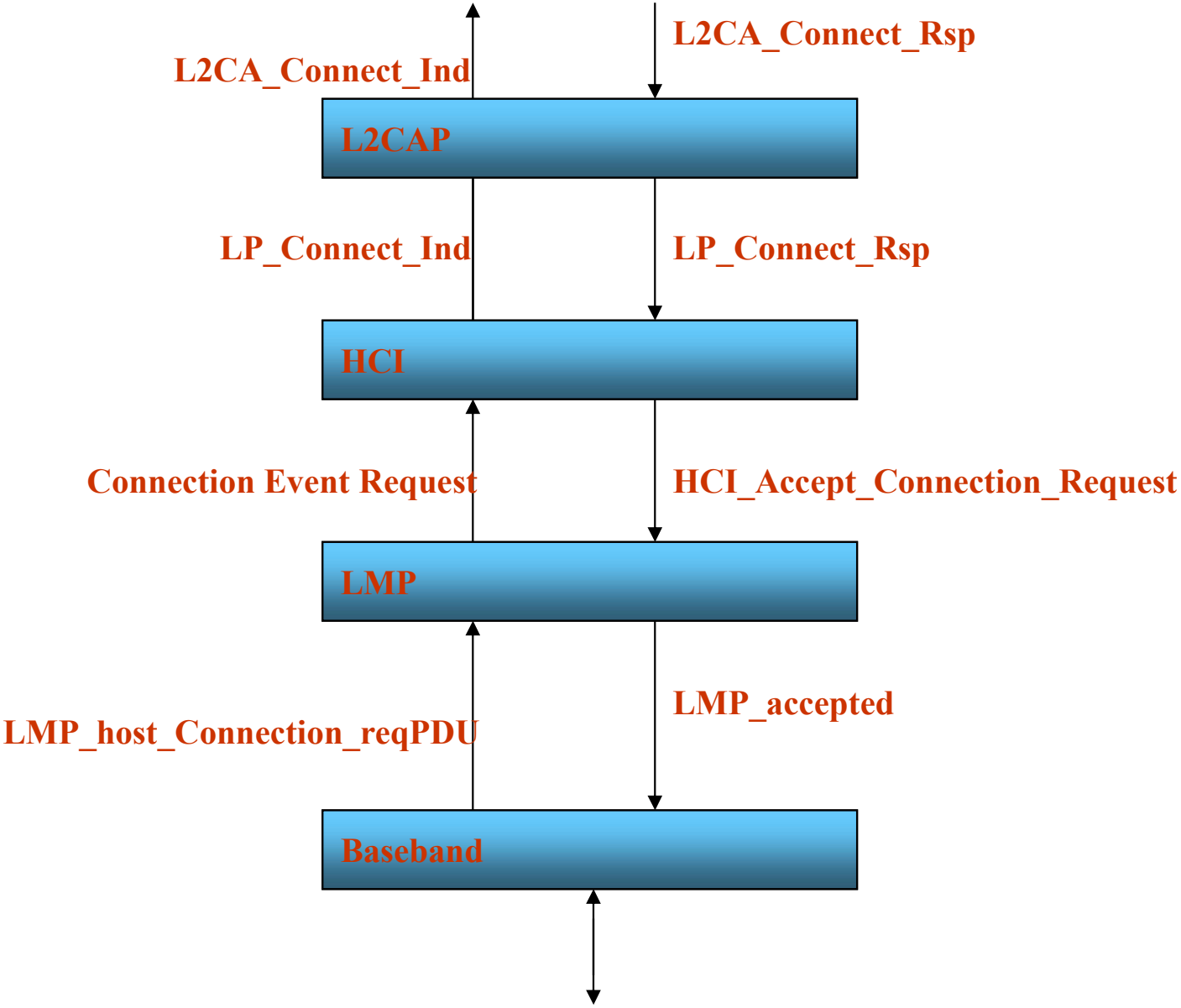
AUX1 – Auxiliary, not a main payload packet but carries extra control/voice information
Can be used for error correction, retransmission or extending capacity.

Adaptation protocols

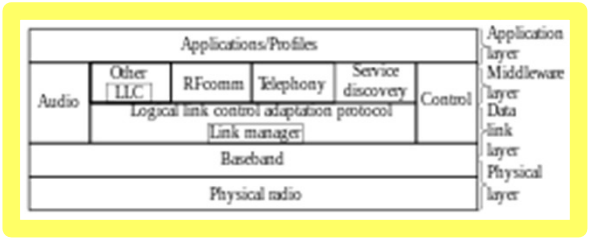
- Link Manager
  - Carries out link setup, above baseband, with authentication, link configuration and other protocols
    - Support protocol multiplexing
      - BT may support other protocols besides IP
    - Segmenting and reassembly
- Link Layer Control & Adaptation (L2CAP)
  - Link control protocol, provides connection-oriented and connectionless data services to upper layer protocols
    - Handles ACL and SCO connections
    - Handle QoS specifications per connection (logical channel)
    - Manages concepts as “group of connections”
- Host Controller Interface (HCI)
  - Allows command line access to the baseband layer and LM for control and status information
    - Current interfaces: USB; UART; RS-232
  - Made up of three parts:
    - HCI firmware, HCI driver, Host Controller Transport Layer
- RFCOMM – Radio Frequency Communication
  - Emulates the functionality of a serial port over the Bluetooth Link

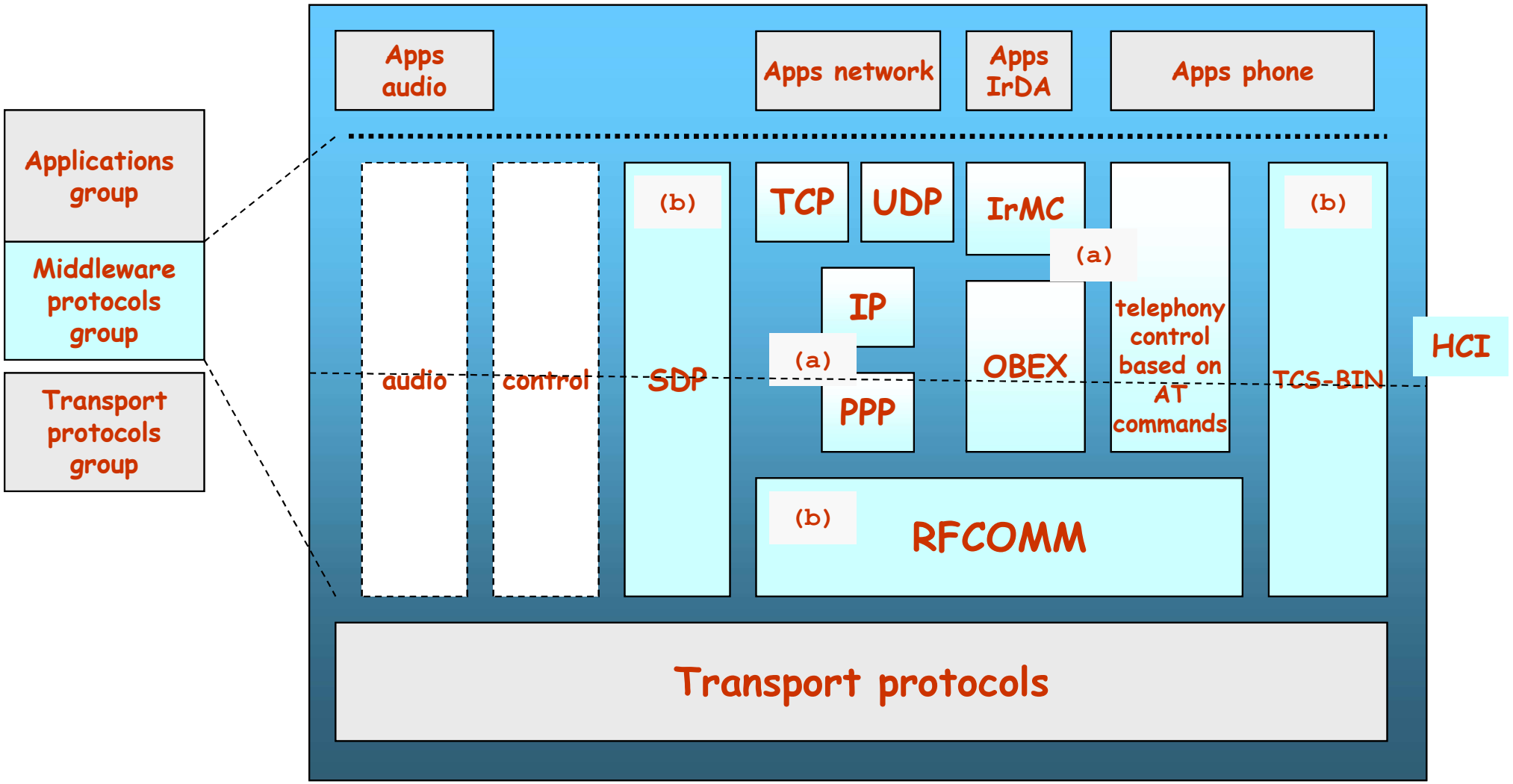


Interlayer communication



Protocols (middleware)





a: common protocol
b: Bluetooth dedicated protocol

SDP: Service Discovery Protocol
OBEX: Facilitates binary transfers between BT devices
TCP-BIN: Telephony-control protocol binary (call control)

Middleware

- Service Discovery Protocol (SDP)
  - Provides a way for applications to detect which services are available and their characteristics
  - Protocol question ⮜⮞ answer
    - (search and browsing of services)
  - Defines a format for service registry
    - Information provided by the service *attributes,* a name (ID) + value
    - IDs can be universal (UUID)
- Protocol reusage
  - BT aims to reuse older protocols (e.g. WAP, OBEX–IrDA)
    - Interaction with applications and phones, as commonly done before

Middleware

- RFCOMM
  - Based on GSM TS07.10
  - Emulates a serial port, supporting all traditional applications that were able to use a serial port
  - Supports multiple ports over a single physical channel between two devices

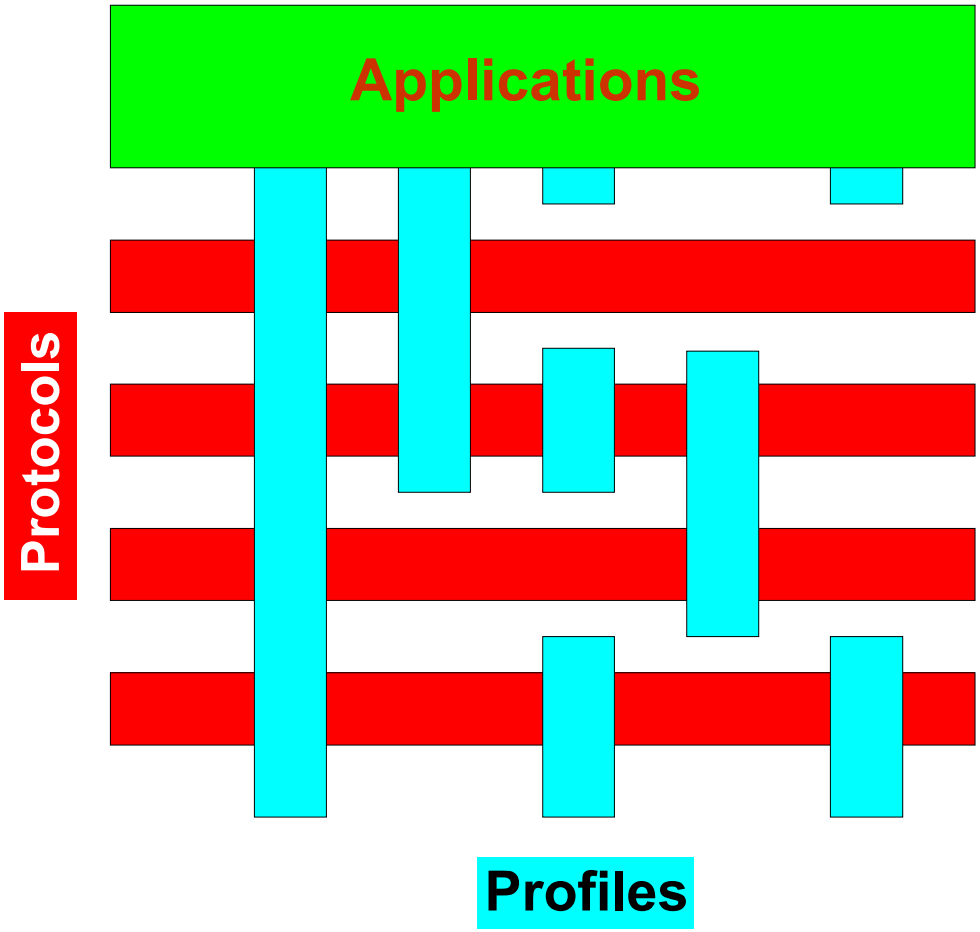
- Telephony Control Protocol Spec (TCS)
  - Handles call control (setup, release)
  - Group management for gateways, serving multiple devices
    - Audioconference, e.g.

Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- 802.15.x

Interoperability: Profiles

- Profile: base for BT interoperability (BT too much flexible!)
- “vertical cut” in Bluetooth stack
- A given usage model (typical solution)
- Each BT device supports one or more profiles



Profiles (v.1)

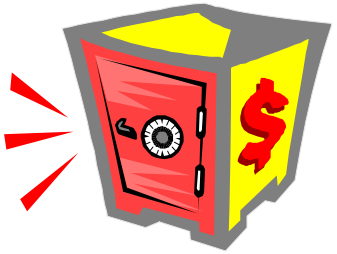
- Generic Access
  - Profile SDA
    (service discovery application)
  - Profiles for serial port, including:
    - Profile Dial-up
    - Profile Fax
    - Profile headset
    - LAN Access (uses PPP)
    - Profile for generic object exchange (OBEX)
      - File transfer
      - Data synchronization
      - Push-pull
- Profile of coordless phone (TCS_BIN)
  - Profile interphone
  - Profile Cordless Telephony

Profiles (v.2)

- Radio 2 (next generation radio)
  Compatible with existing systems
- Car Profile
- PAN Profile
- GPS Profile
- Printing Profile
- Still image Profile

(globally better facilities in audio/voice/video)
(better service discovery)
(improved human interfaces)
(improved interoperation with other devices at the 2.4GHz ISM)

Bluetooth: security



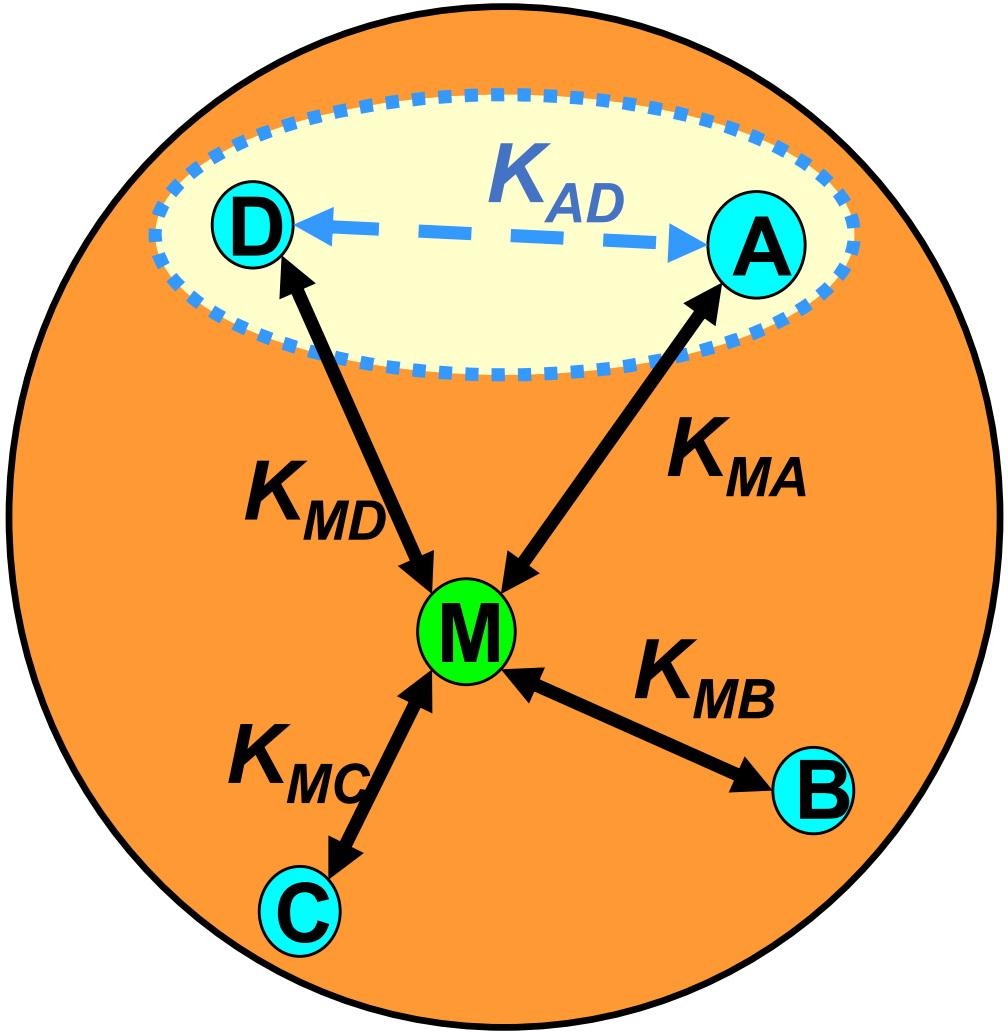
- Devices can be:
  - “Trusted”
  - “Untrusted”
    - Also “unknown” devices
- Services security types:
  - Open services – cypher only
  - Authentication only – machine ID
  - Authentication and authorization (ID+explicit service grant)
- Levels of security:
  - Mode 1
    - No security
  - Mode 2
    - Security guaranteed at service level
  - Mode 3
    - Security guaranteed at link level

Bluetooth: security features

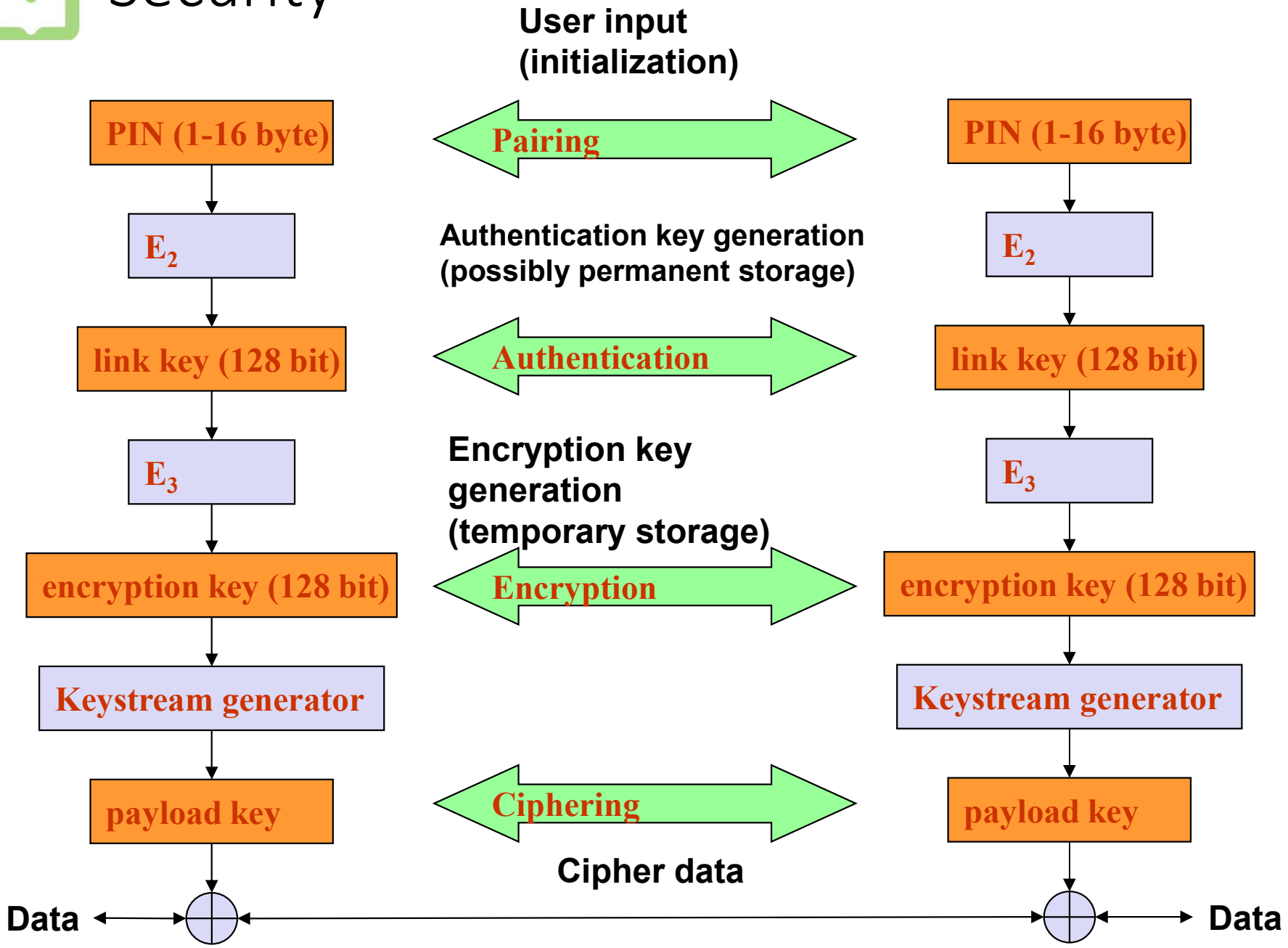
- Mechanisms used in BT for security
  - Fast frequency hopping
  - Low range
  - Authentication
    - Two way challenge/response mechanism
  - Cypher (to ensure privacy)
    - Data between two devices can be encrypted
    - Keys used
      - Cypher size configurable (0-16bytes) by the devices, but there are security constrains (goverment)
      - Keys using standard well-known algorithms
  - Security initialization – device pairing
    - PIN (user input)
    - Shared key

Link keys in a piconet

- Link keys are generated via a PIN entry
- A different link key for each pair of devices is allowed
- Authentication:
  - Challenge-Response Scheme
- Permanent storage of link keys



Security


User input
(initialization)
PIN (1-16 byte)
Pairing
PIN (1-16 byte)
E2
Authentication key generation
(possibly permanent storage)
E2
link key (128 bit)
Authentication
link key (128 bit)
E3
Encryption key
generation
(temporary storage)
E3
encryption key (128 bit)
Encryption
encryption key (128 bit)
Keystream generator
Keystream generator
payload key
Ciphering
payload key
Cipher data
Data
Data

Bluetooth 4.0: Low Energy

Short range wireless application areas

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS	x	Y	Y	x	x
Bluetooth SCO/eSCO	Y	x	x	x	x
Bluetooth low energy (BLE)	x	x	x	x	Y
Wi-Fi	(VoIP)	Y	Y	Y	x
Wi-Fi Direct	Y	Y	Y	x	x
ZigBee	x	x	x	x	Y

What is Bluetooth Low Energy?

- Bluetooth low energy is a open, short range radio technology
  - Blank sheet of paper design
  - Different to Bluetooth classic (BR/EDR)
  - Optimized for ultra low power
  - Enable coin cell battery use cases
    - < 20mA peak current
    - < 5 uA average current

Basic Concepts of Bluetooth 4.0

- Everything is optimized for lowest power consumption
  - Short packets reduce TX peak current
  - Short packets reduce RX time
  - Less RF channels to improve discovery and connection time
  - Simple state machine
  - Single protocol
  - Etc.

Bluetooth low energy factsheet

Range:	**~ 150 meters open field**
Output Power:	**~ 10 mW (10dBm)**
Max Current:	**~ 15 mA**
Latency:	**3 ms**
Topology:	**Star**
Connections:	**> 2 billion**
Modulation:	**GFSK @ 2.4 GHz**
Robustness:	**Adaptive Frequency Hopping, 24 bit CRC**
Security:	**128bit AES CCM**
Sleep current:	**~ 1µA**
Modes:	**Broadcast, Connection, Event Data Models, Reads, Writes**

Bluetooth 5.0

- Released in 2016, targeting IoT and BLE (too!)
- Focused on range, speed, broadcast capacity and reliability
- Extended Range
  - BLE range increased up to 4× (up to ~240 m in ideal conditions) using Coded PHY (LE Coded).
- Higher Speed
  - BLE data rate doubled from 1 Mbps to 2 Mbps with LE 2M PHY.
- Increased Broadcast Capacity
  - Advertising packets up to **255 bytes** (vs. 31 bytes in BLE 4.x)
- Improved Coexistence
  - Better coexistence mechanisms for crowded 2.4 GHz environments.
- Improved Location Services
  - Improved accuracy in positioning and proximity applications.
- Enhanced Privacy & Security
  - LE Secure Connections, improved pairing.

Bluetooth 6.0

- Focused on privacy, power efficiency and smarter device interaction
- Ideal for dense IoT environments, privacy-sensitive applications and long-term deployments
- Enhanced Privacy
  - Randomized Resolvable Private Addresses (RPA) that change more unpredictably for better anti-tracking.
- Energy Efficiency Improvements
  - Offloading address rotation to the controller reduces CPU load and saves battery
- Smarter Advertising
  - Decision-Based Advertising Filtering (DBAF) to reduce noise and increase efficiency in crowded environments.
- Channel Sounding
  - Enables precise distance measurement and location services.
- Improved IoT Support
  - New mechanisms for large-scale device deployments with better reliability and security.