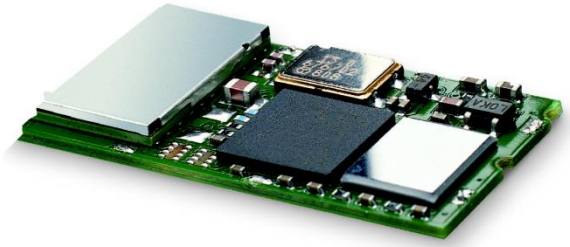
Bluetooth

José Augusto Afonso
Jose.afonso@dei.uminho.pt

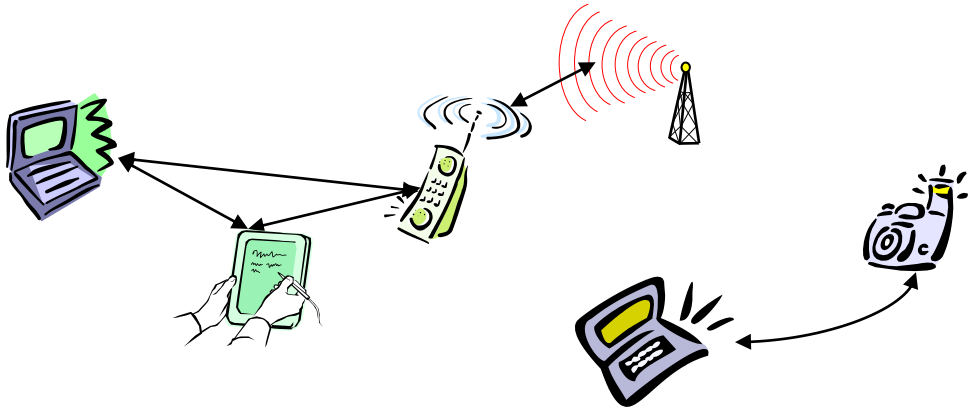
Bluetooth

Original Idea

- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- Embedded in other devices, goal: 5€/device
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first modules (Ericsson).



Bluetooth

- **Early History**
  - 1994: Ericsson (Mattison/Haartsen), “MC-link” project
  - Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org (was: Bluetooth)
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week

- **Special Interest Group (SIG)**
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 2500 members
  - Common specification and certification of products

Usual Applications

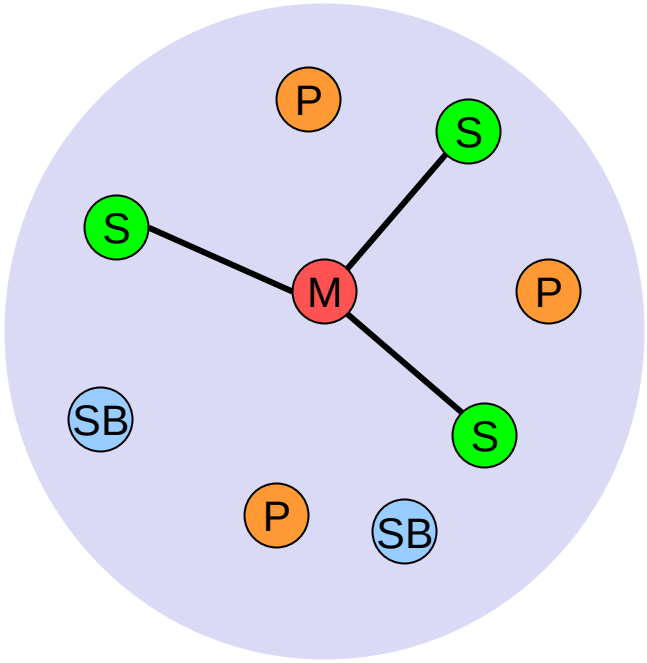
- Wireless control of and communication between a cell phone and a **hands-free headset or car kit**.
- **Wireless networking between PCs** where little bandwidth is required.
- Wireless communications with PC input and output devices, the most common being the **mouse, keyboard and printer**.
- Transfer of files between devices with OBEX.
- Transfer of contact details, calendar appointments, and reminders between devices with OBEX.
- **Replacement of traditional wired serial communications** in test equipment, GPS receivers, medical equipment and traffic control devices.
- For controls where infrared was traditionally used.
- Sending small advertisements from Bluetooth enabled advertising hoardings to other, discoverable, Bluetooth devices.
- Some **game consoles** — Nintendo Wii, Sony PlayStation 3 — use Bluetooth for their respective wireless controllers.

Characteristics (Bluetooth version 1.1)

- PHY
  - 2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing
  - Bit rate: 1 Mbit/s
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - GFSK modulation, 1-100 mW transmit power
  - Frequency hopping (FHSS) with 1600 hops/s, slots of 625 µs
  - Pseudo random hopping sequence, determined by the master
- MAC protocol: polling based (contention free)
- Voice link – SCO (Synchronous Connection Oriented)
  - Optional FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, ARQ (fast acknowledge), point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology: overlapping piconets (stars) forming a scatternet

Piconet

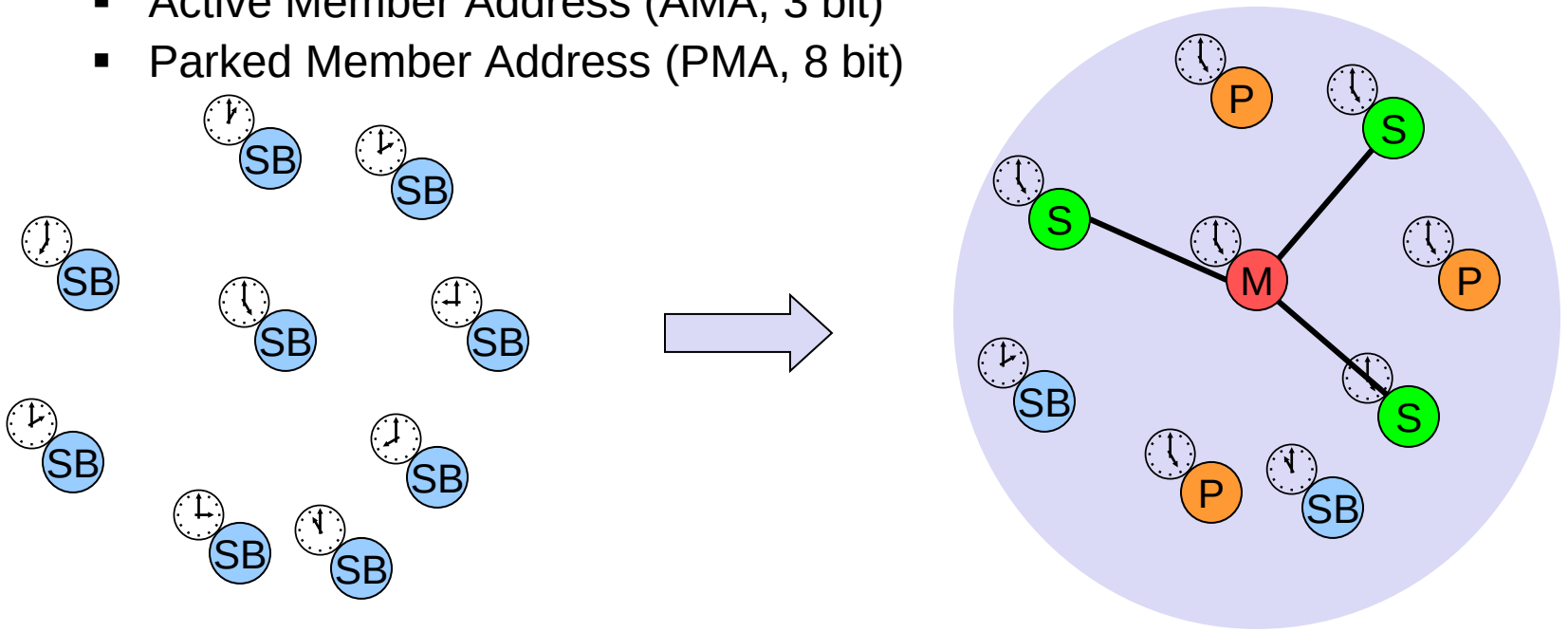
- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)



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

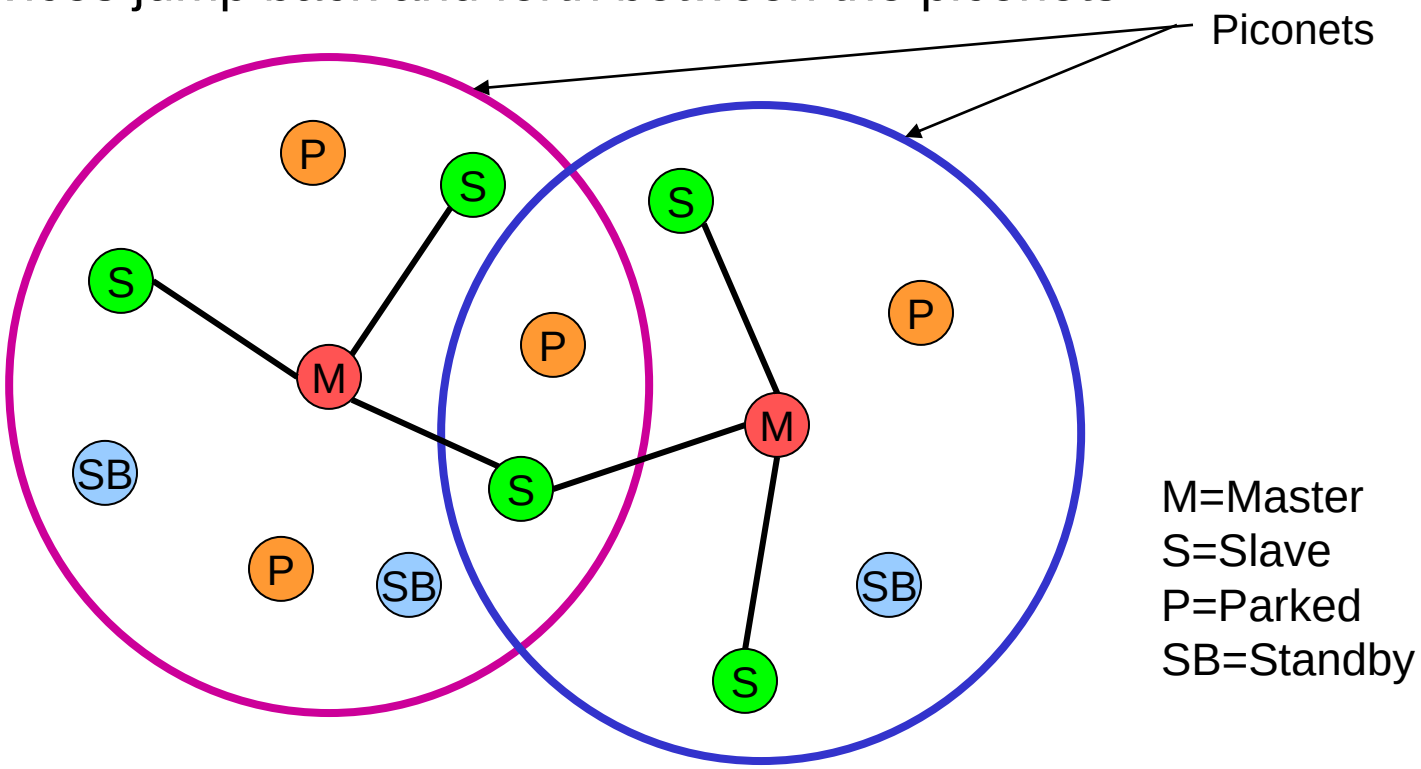
Forming a Piconet

- The unit that establishes the piconet becomes the master
- All devices in a piconet hop together
  - Master gives slaves its clock and device address (BD_ADDR)
    - Hopping pattern determined by address (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock of the master
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

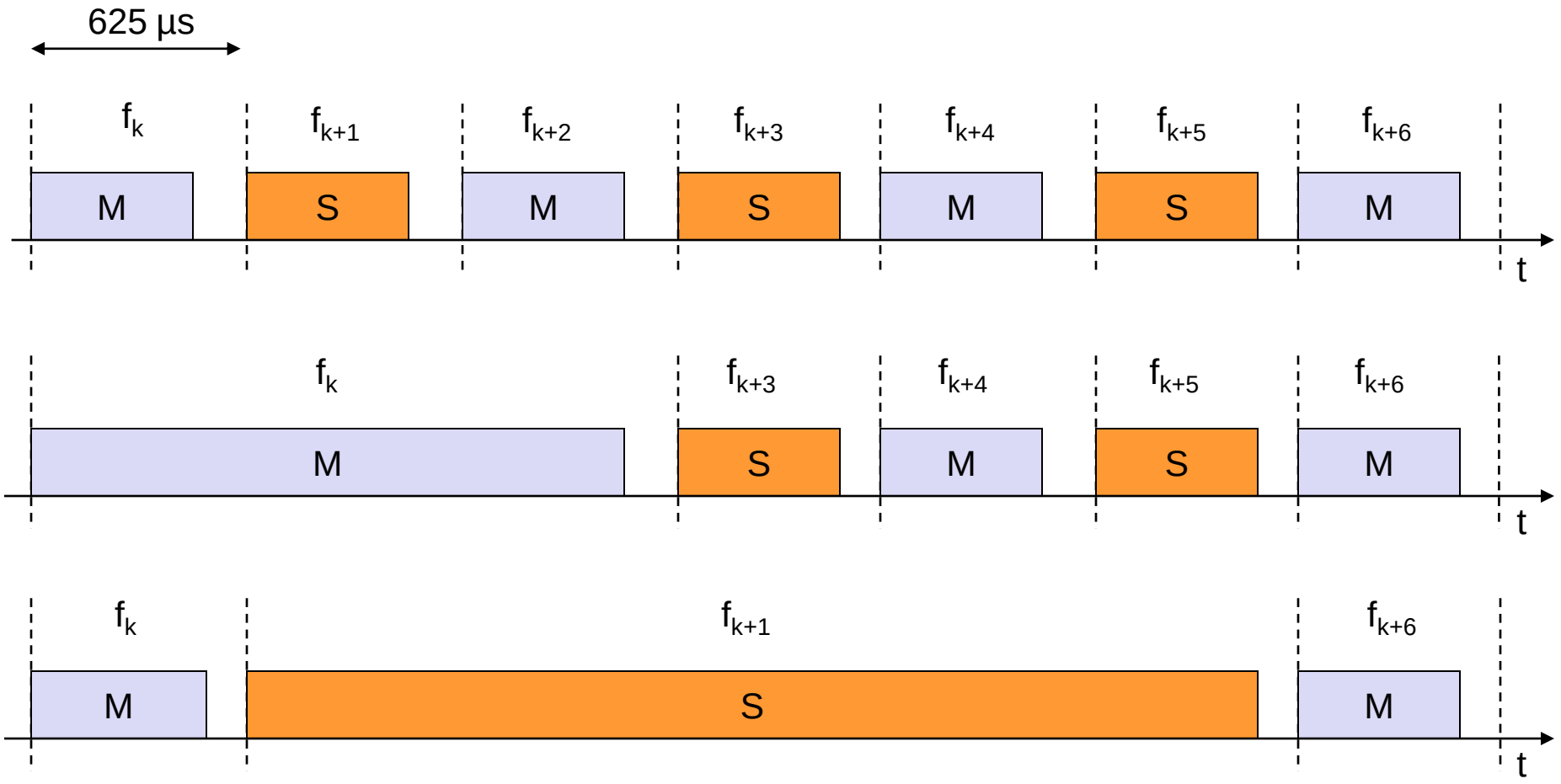


Scatternet

- Linking of multiple co-located piconets through the sharing of common devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jump back and forth between the piconets

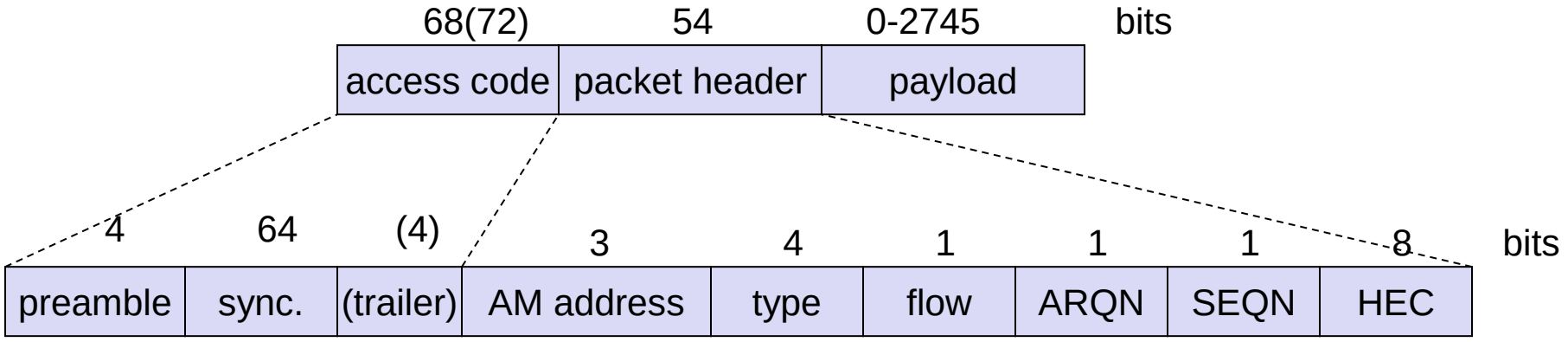


Frequency Selection and Packet Sizes



Baseband Packet Format

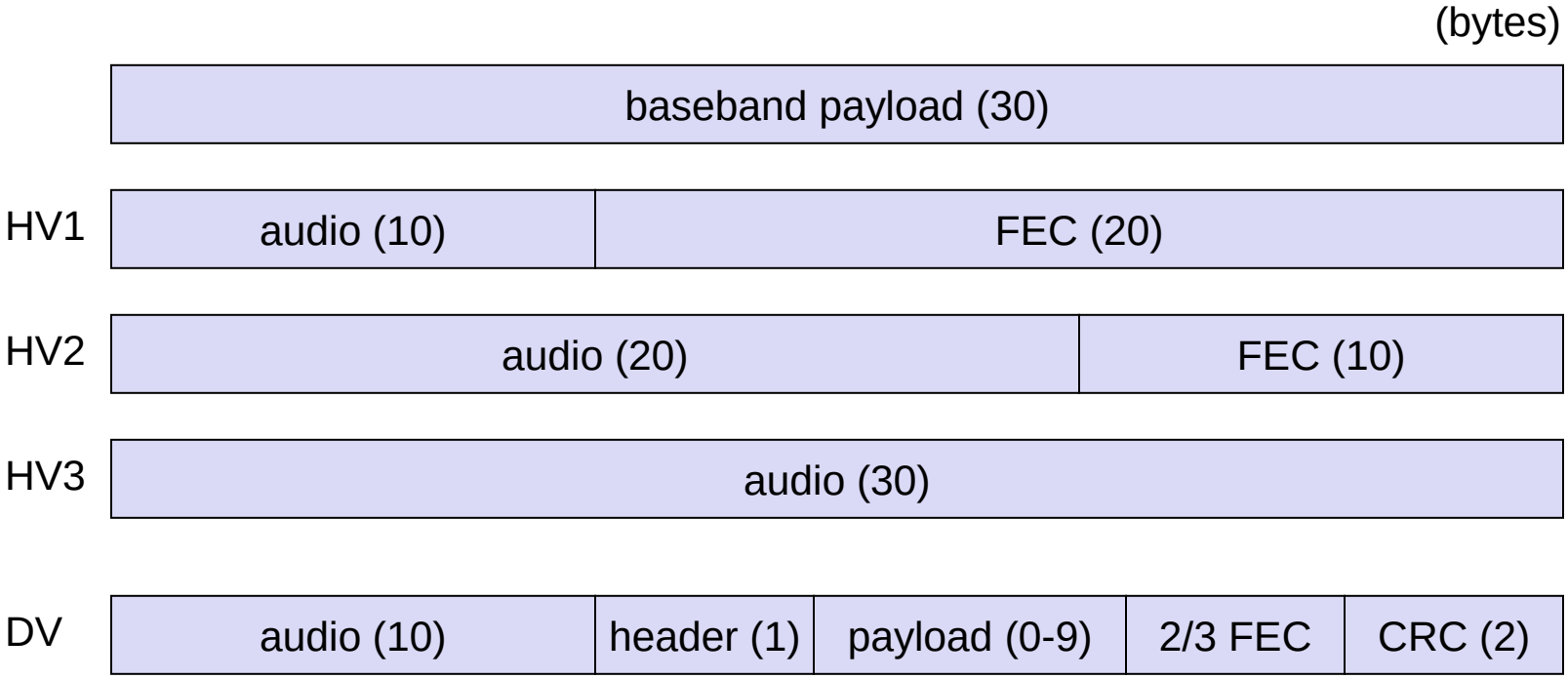
- Access code
  - Used for synchronization and identification of all packets exchanged in a piconet.
  - Derived from the master device address (BD_ADDR)
- Packet header (protected with 1/3-FEC)
  - active member (AM) address (broadcast + 7 slaves), packet type, flow control, ACK/NAK (ARQN), sequence number (SEQN), checksum (HEC - Header Error Check)



Control Packet Types

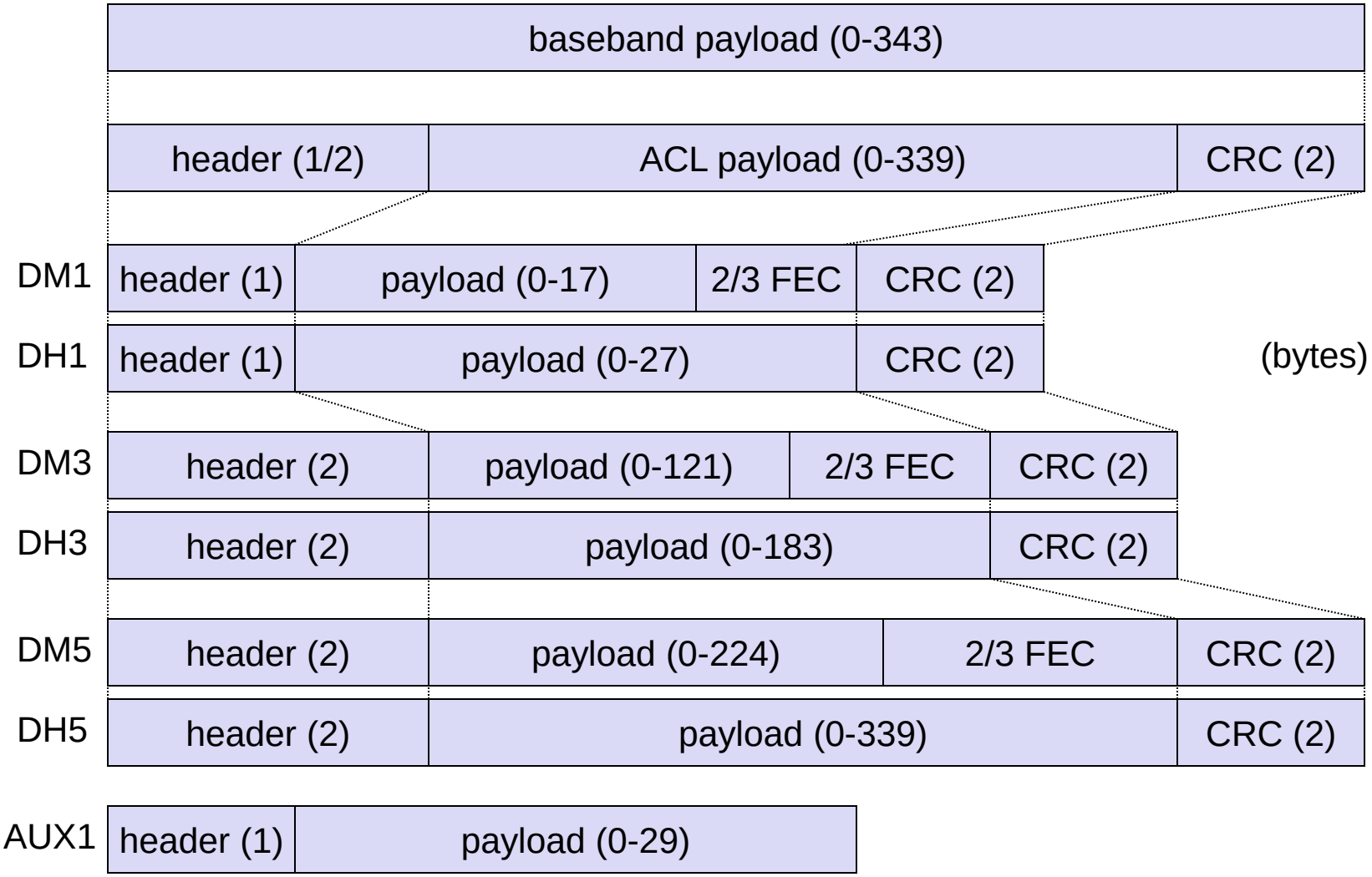
- **Identification Packet (ID):** Only contains the access code. Used for signaling (e.g., connection establishment).
- **FHS (FH-Synchronization) Packet:** Used to exchange clock and identity information. Contains all information to get two devices hop synchronized.
- **NULL Packet:** Only has an access code and a packet header, but no payload. Used if information carried by the packet header has to be conveyed.
- **POLL Packet:** Similar to the NULL packet. Used by the master to force slaves to return a response.

SCO Packet Types



10 bytes / 2 slots de 625 µs = 64 kbps

ACL Packet Types



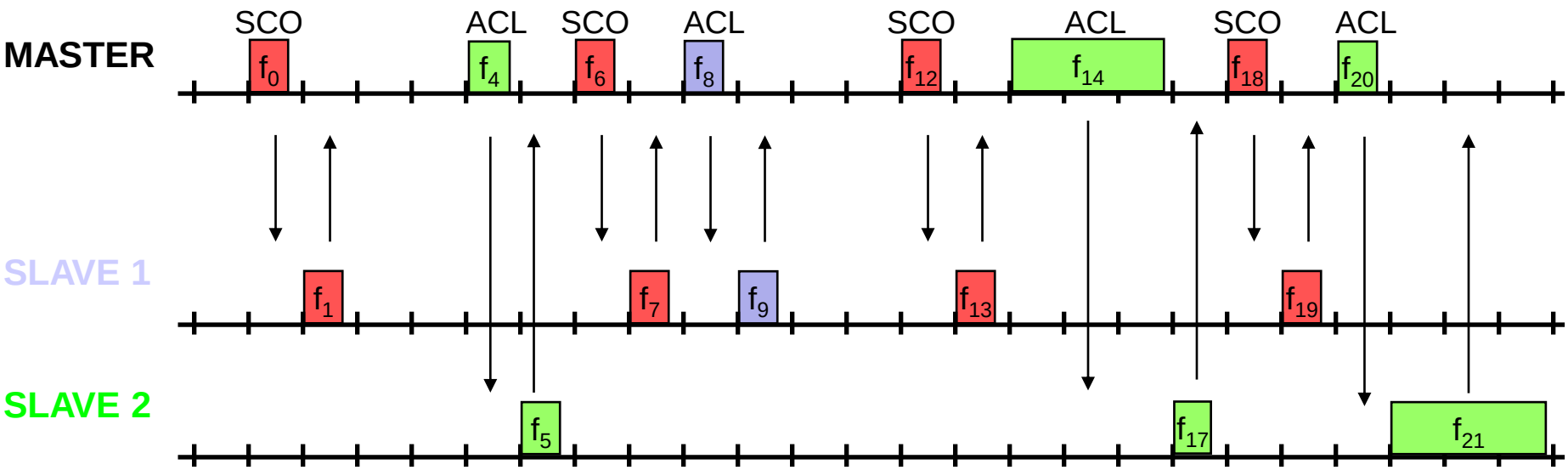
ACL and SCO Data Rates

	Type	Payload Header [byte]	User Payload [byte]	FEC	ARQ	Symmetric max. Rate [kbit/s]	Asymmetric max. Rate [kbit/s] Forward	Reverse
ACL 1 slot	DM1	1	0-17	2/3	yes	108.8	108.8	108.8
	DH1	1	0-27	no	yes	172.8	172.8	172.8
3 slot	DM3	2	0-121	2/3	yes	258.1	387.2	54.4
	DH3	2	0-183	no	yes	390.4	585.6	86.4
5 slot	DM5	2	0-224	2/3	yes	286.7	477.8	36.3
	DH5	2	0-339	no	yes	**433.9**	**723.2**	57.6
	AUX1	1	0-29	no	no	185.6	185.6	185.6
SCO	HV1	na	10	1/3	no	64.0 (max. 1)		
	HV2	na	20	2/3	no	64.0 (max. 2)		
	HV3	na	30	no	no	64.0 (max. 3)		
	DV	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D		

DM - Data Medium rate, DH - Data High rate, HV - High-quality Voice, DV - Data and Voice

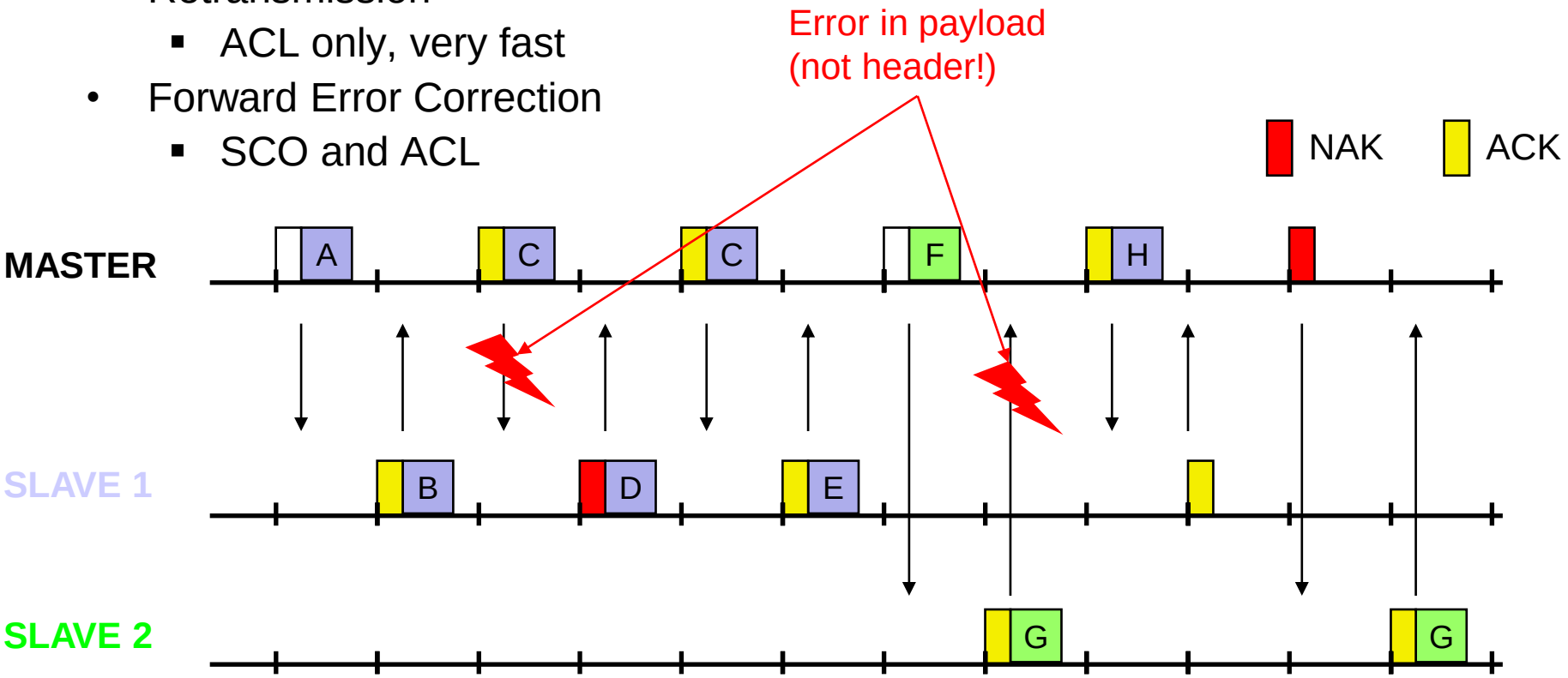
Master/Slave Communications

- Polling-based TDD packet transmission
  - 625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint

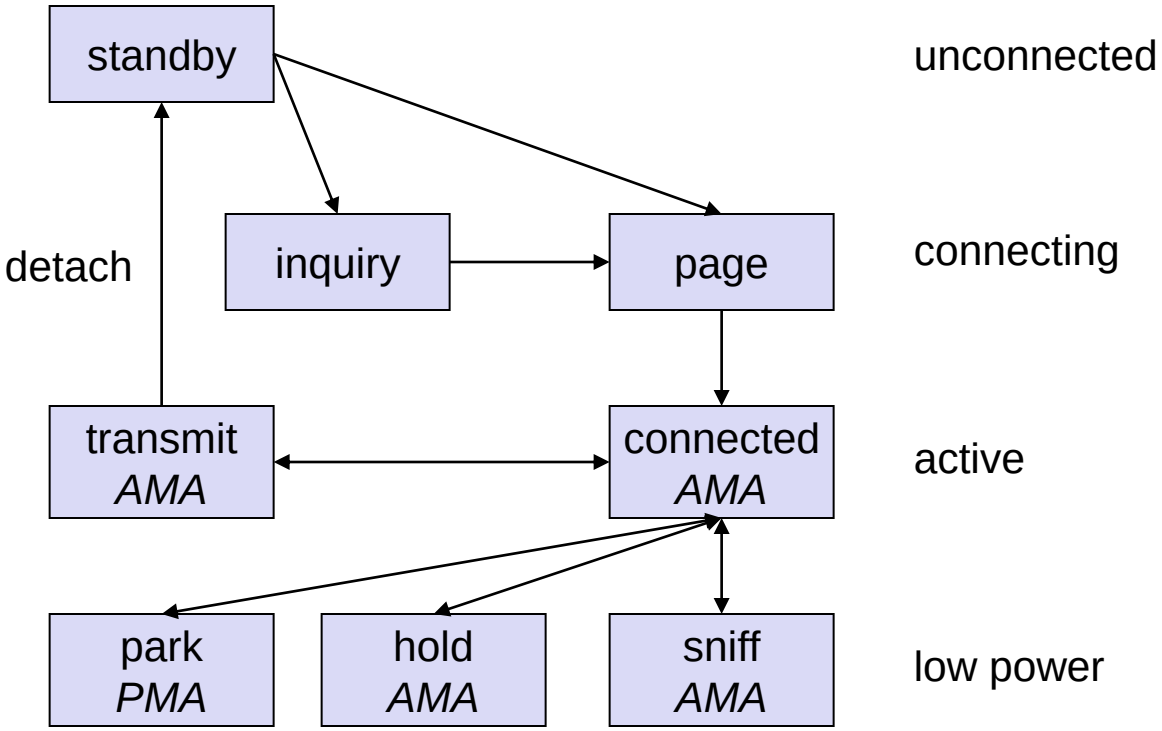


Robustness

- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets
- Retransmission
  - ACL only, very fast
- Forward Error Correction
  - SCO and ACL



Baseband States of a Bluetooth Device



Standby: idle (unconnected)
Inquiry: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

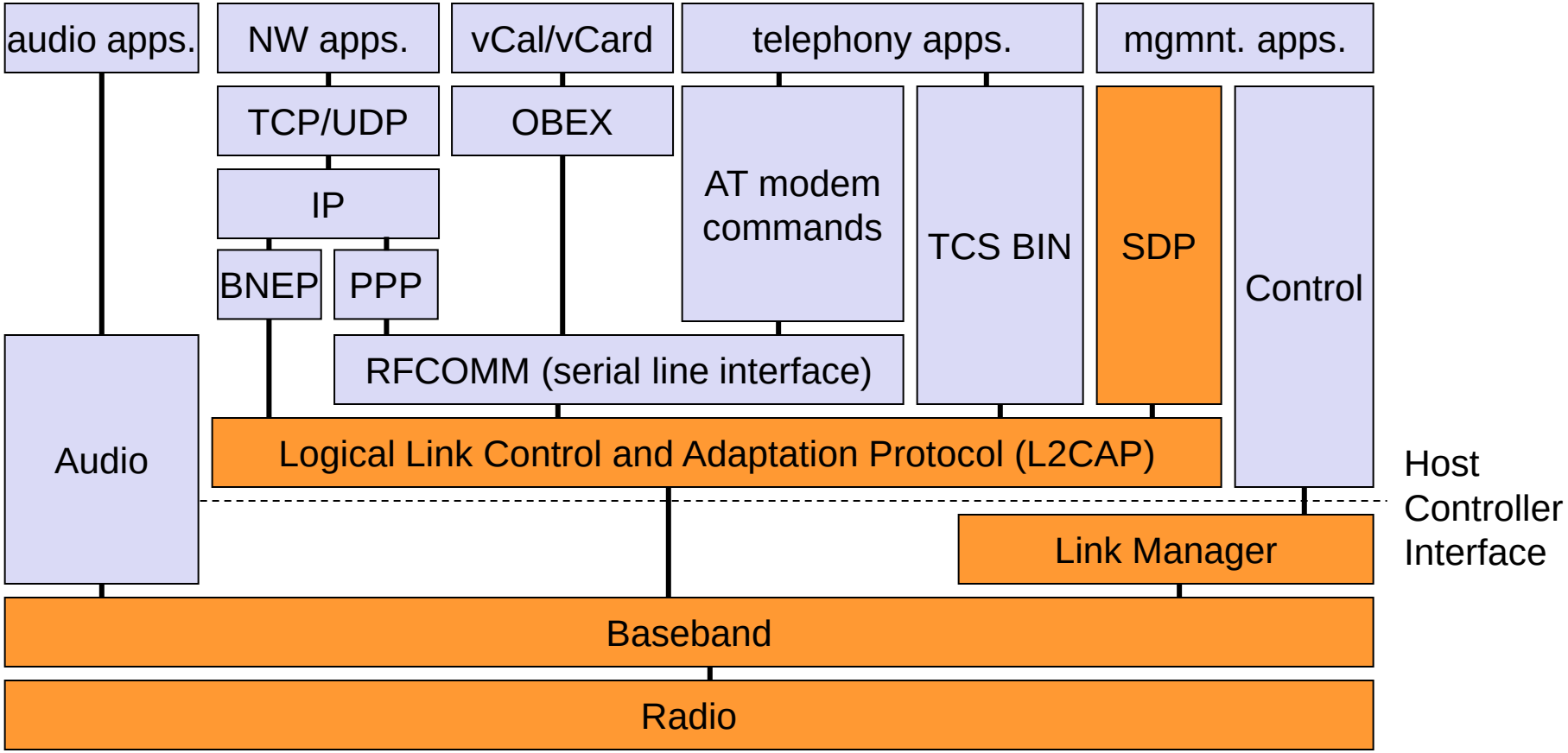
Park: release AMA, get PMA
Sniff: listen periodically, not each M-S slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

Power Classes

Class	Maximum Permitted Power (mW/dBm)	Range (approximate)
Class 1	100 mW (20 dBm)	~100 meters
Class 2	2.5 mW (4 dBm)	~10 meters
Class 3	1 mW (0 dBm)	~1 meter

- Power control is mandatory for power class 1 equipment.
- Power control capability under 0 dBm is optional and could be used for optimizing the power consumption and overall interference level.
- Power control is based on closed-loop Received Signal Strength Indicator (RSSI).

Bluetooth Protocol Stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

Bluetooth Core Protocols

- **Controller Layers**
  - **Radio**: Specification of radio parameters, e.g., frequencies, modulation and transmit power.
  - **Baseband**: Specification of lower-level operations at bit and packet levels (packet formats, timing, FEC, ARQ, CRC, encryption).
  - **Link Manager:** Connection establishment, authentication, link set-up and management, traffic scheduling and power management.
- **Host Layers**
  - **Logical Link Control and Adaptation Protocol (L2CAP):** Interface between standard data transport protocols and Bluetooth. Handles multiplexing of high-layer protocols and segmentation/reassembly.
  - **Service Discovery Protocol (SDP):** Used to query and discover the service capabilities of other devices in range (e.g. printing, faxing, network bridging).
- **Host Controller Interface (HCI):** Provides a command interface to the baseband controller and link manager, and access to the hardware status and control registers.

Additional Protocols to Support Legacy Protocols/Apps

- **RFCOMM:** Emulates a RS-232 serial line interface.
  - Allows replacement of serial line cables enabling many legacy applications and protocols to run over Bluetooth.
  - Supports multiple serial ports over a single physical channel.
- **Telephony Control protocol Specification – Binary (TCS BIN):** Defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. It also defines mobility management procedures for handling Bluetooth TCS devices.
- **OBEX (OBject EXchange):** Used to quickly “Push” files into devices. In Bluetooth, OBEX offers the same features for applications as within the IrDA protocol hierarchy.
- **WAP (Wireless Application Protocol):** Use of Bluetooth as communications bearer for WAP protocols and applications.

Bluetooth Profiles

- The profiles specify which protocols are mandatory to certain applications
  - Prevent devices with little resources from implementing all BT stack
  - Basis for interoperability between devices

Basic Profiles
Generic Access Profile
Service Discovery Application Profile
Cordless Telephony Profile
Intercom Profile
Serial Port Profile
Headset Profile
Dial-up Networking Profile
Fax Profile
LAN Access Profile
Generic Object Exchange Profile
Object Push Profile
File Transfer Profile
Synchronization Profile

Additional Profiles
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

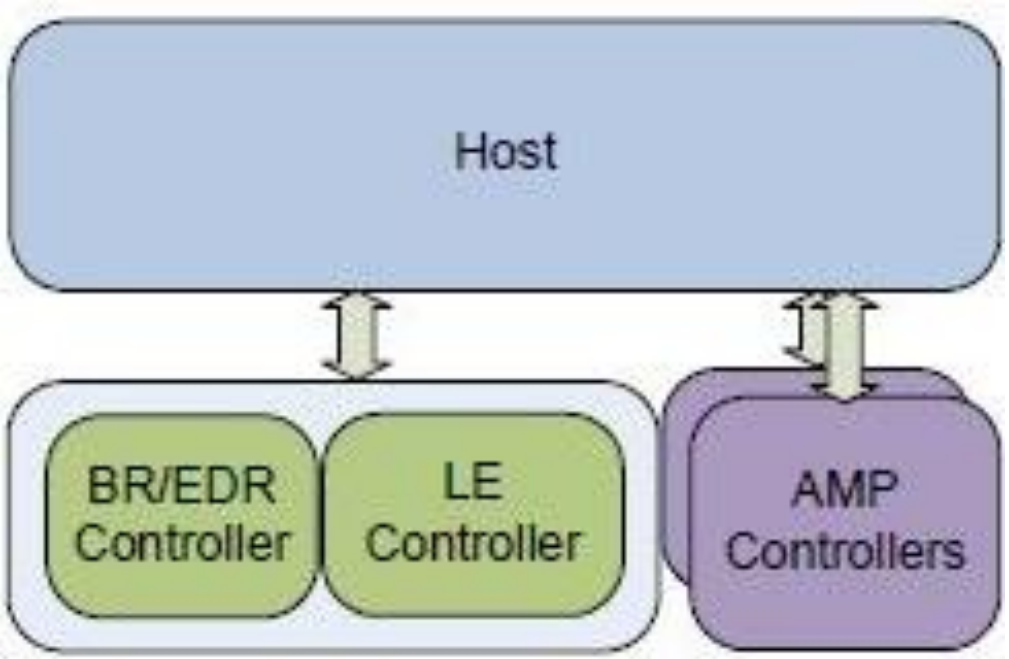
Bluetooth Versions

- Bluetooth 1.0 and 1.0B
- Bluetooth 1.1
  - Fixed many errors found in the 1.0B specifications.
- Bluetooth 1.2
  - Adaptive Frequency-hopping spread spectrum (AFH) - improves robustness to radio frequency interference by avoiding the use of crowded frequencies in the hopping sequence.
  - extended Synchronous Connections (eSCO) - improves voice quality of audio links with retransmissions of corrupted packets.
- Bluetooth 2.0
  - Enhanced Data Rate (EDR) of 2 Mbps and 3 Mbps, achieved by using higher speed modulation schemes for the payload data.
- Bluetooth 3.0
  - High Speed (HS), Alternative MAC/PHY (AMP). Bluetooth link is used for negotiation and connection establishment, data transfer is carried using an IEEE 802.11 link.
- Bluetooth 4.0
  - Includes Bluetooth Low Energy (BLE).

Bluetooth 4.0

Controllers

- BR (Basic Rate)/EDR (Enhanced Data Rate)
- LE (Low Energy) - Not compatible with classic Bluetooth
- AMP (Alternative MAC/PHY)

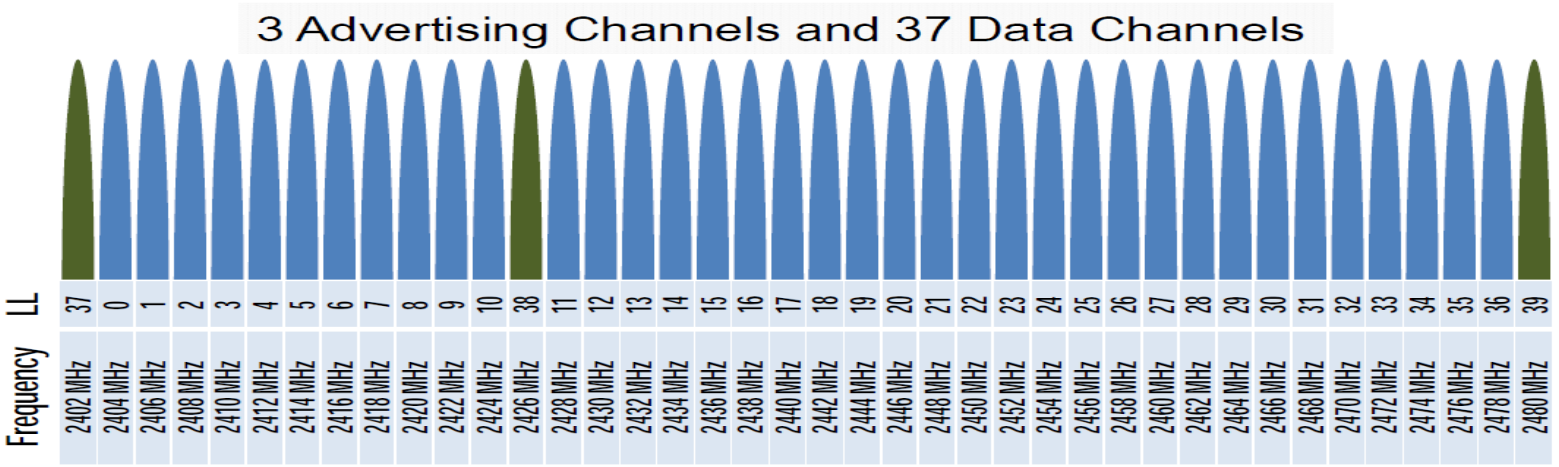


Bluetooth Device Types

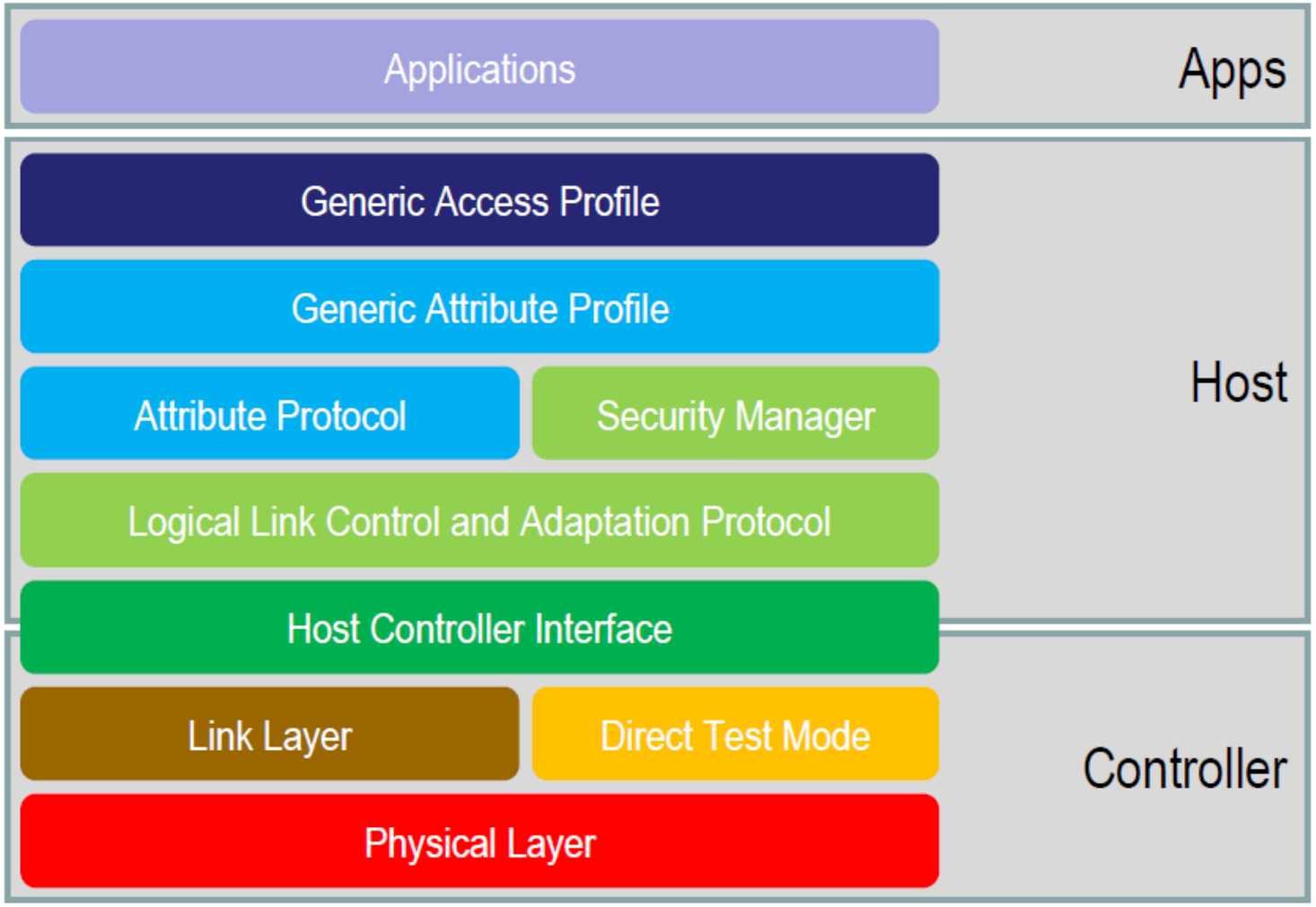
- **Bluetooth** – Only classic Bluetooth (single mode)
- **Bluetooth Smart** – Only BLE (single mode)
  - Low cost, low energy, battery-operated devices such as sensors
- **Bluetooth Smart Ready** – Bluetooth and BLE (dual mode)
  - Laptops, smartphones, etc.

BLE Overview

- Like Bluetooth, Bluetooth Low Energy operates in the 2.4 GHz frequency band using adaptive frequency hopping spread spectrum (FHSS)
- Physical layer provides bit rate of 1 Mbps using GFSK modulation
- Two types of RF channels
  - Advertising channels - 3 channels, can be used to discover devices, establish connections and broadcast data
  - Data channels - 37 channels, used for bidirectional communication
- Like Bluetooth, BLE networks (piconets) are based on star topology and define 2 device roles at the link layer: master and slave
- Unlike Bluetooth, BLE supports more than 7 slaves per piconet



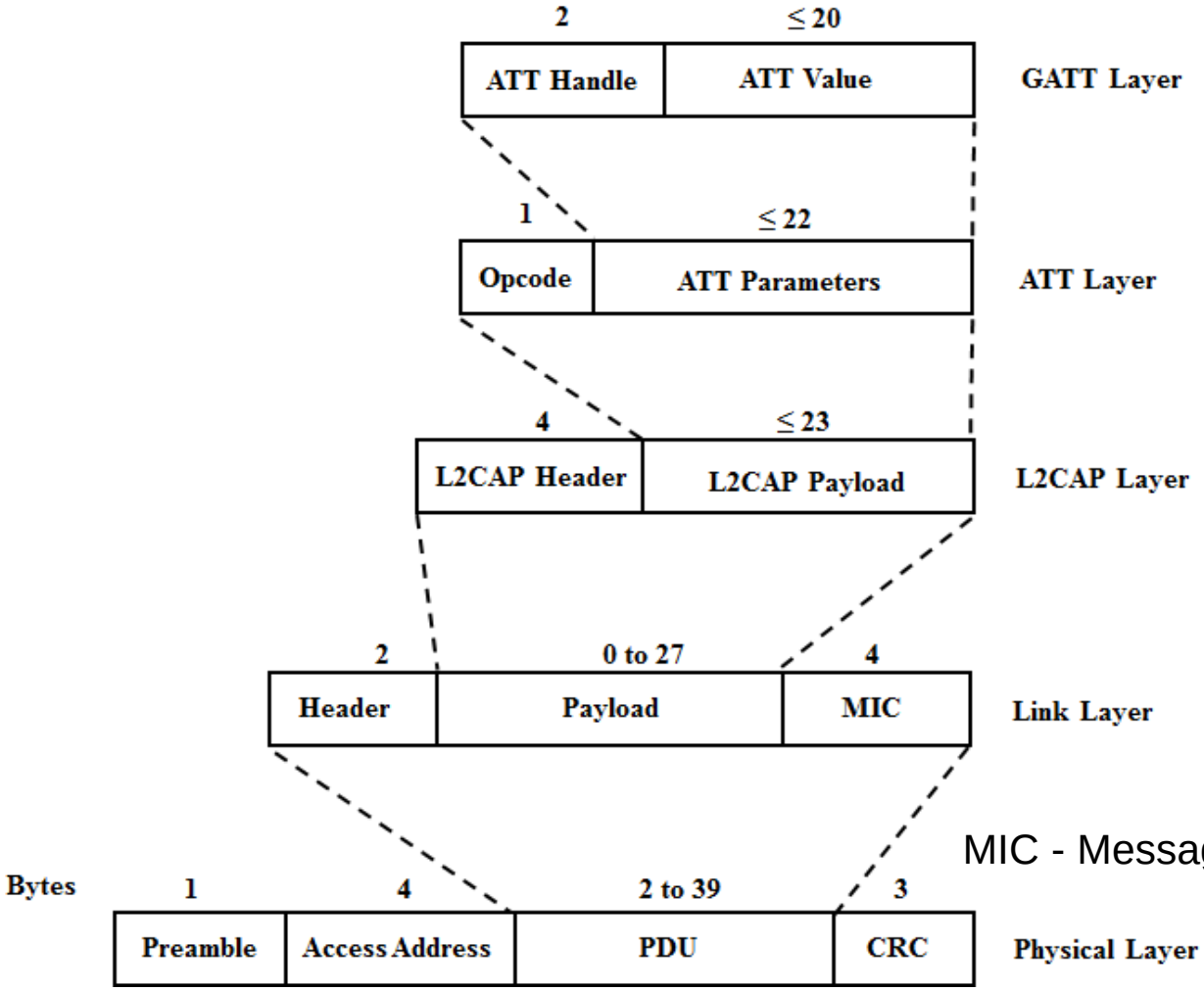
BLE Protocol Architecture



BLE Layers and Protocols

- L2CAP (Logical Link Control and Adaptation) layer multiplexes the data of three higher layer protocols: ATT (Attribute Protocol), SMP (Security Manager Protocol) and link layer control signaling.
- ATT defines the communication between two devices with the roles of server and client.
  - The server maintains a set of attributes, storing information managed by the GATT protocol. A server can also send unsolicited messages to a client, containing attributes, by using either notifications (without ACK) or indications (with ACK).
  - The client can access the server's attributes by sending requests, which originate responses from the server, or send commands to the server in order to write attribute values.
- GAP (Generic Access Profile) roles
  - Central station (master) - Responsible for initiating and managing multiple connections
  - Peripheral station (slave) - Simple devices which may only establish a single connection with the central station.

BLE Data Packet Format at Different Layers



MIC - Message Integrity Check

MAC Protocol for Connected-Oriented Data Transfer

- Communication occurs during connection events and is based on polling.
- Time between connection events is a parameter called connection interval.
- Slaves can sleep between connection intervals to save energy.
- Slaves may be configured with different connection intervals.
- Master and slave alternate transmission until the devices don't have more data to transmit or the connection event period ends.
- During a connection event, packets are transmitted using the same channel.