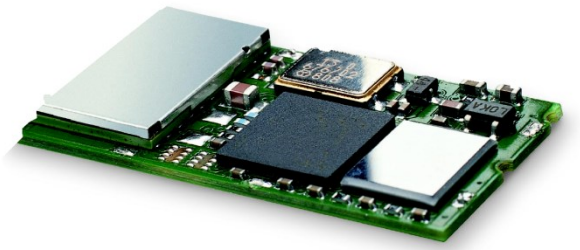
Δίκτυα Μικρής Απόστασης

Σαράντης Πασκαλής <paskalis@di.uoa.gr>
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

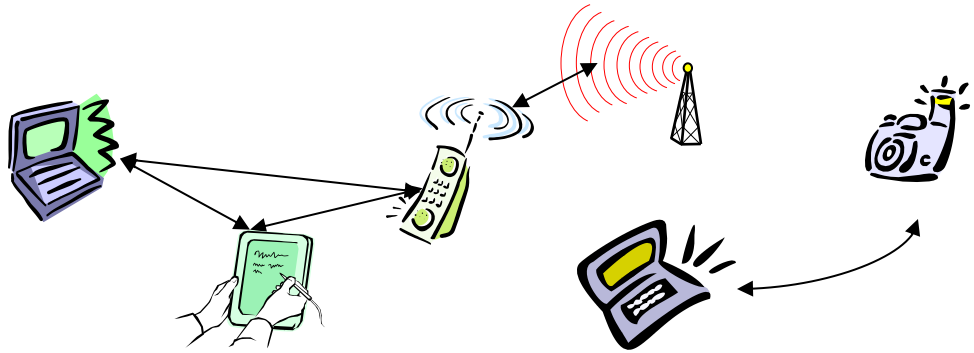
ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών
ΙΔΡΥΘΕΝ ΤΟ 1837

Bluetooth

- Basic 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 (already << 1€)
  - 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

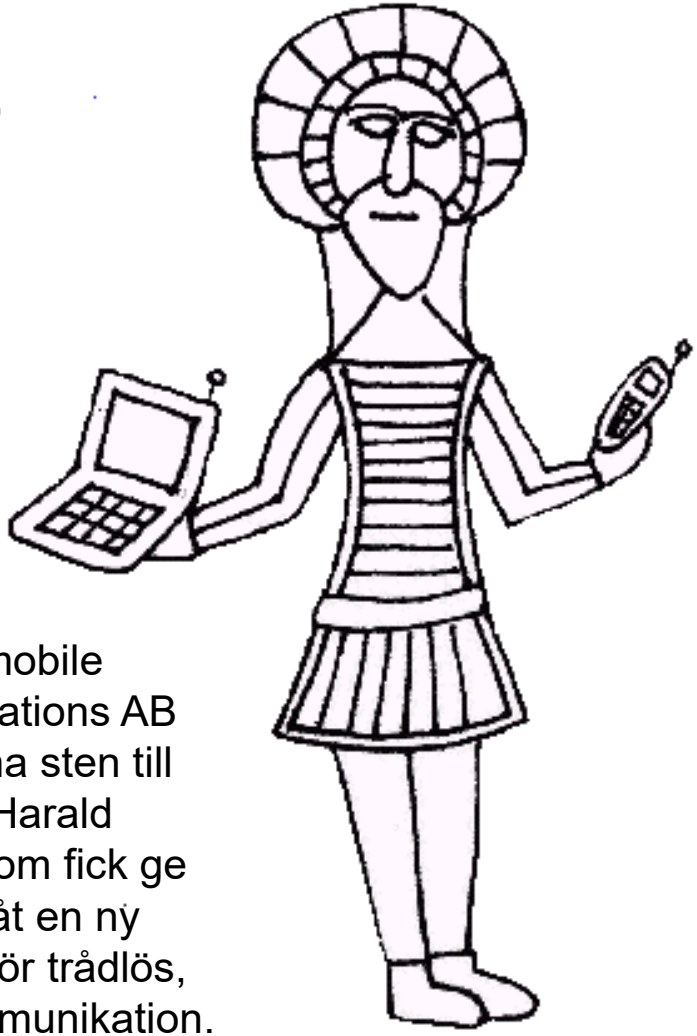
(was: Bluetooth)

- 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
  - 1999: erection of a rune stone at Ercisson/Lund ;-)
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week
  - 2009: 920 million chips/year

Bluetooth™

- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 35000 members
  - Common specification and certification of products

History and hi-tech…



1999:
Ericsson mobile communications AB reste denna sten till minne av Harald Blåtand, som fick ge sitt namn åt en ny teknologi för trådlös, mobil kommunikation.

…and the real rune stone

Located in Jelling, Denmark, erected by King Harald “Blåtand” in memory of his parents.
The stone has three sides – one side showing a picture of Christ.

Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

Btw: Blåtand has nothing to do with a blue tooth…

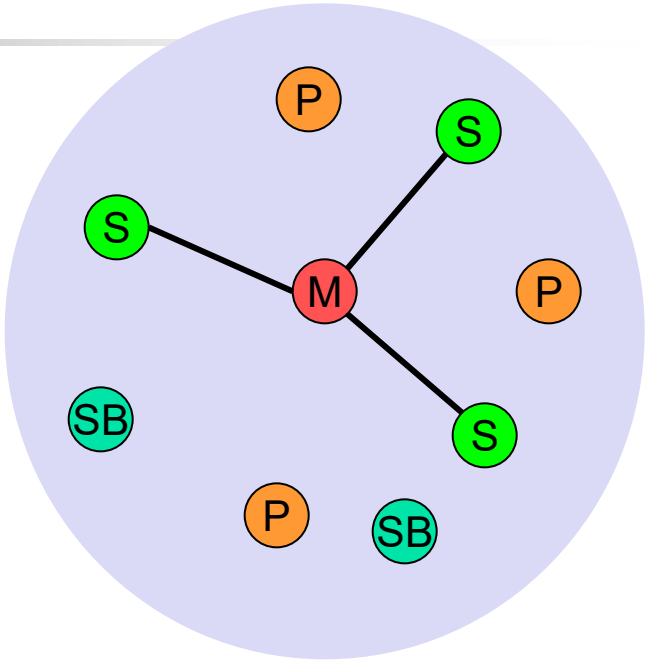
This could be the “original” colors of the stone.
Inscription:
“auk tani karthi kristna” (and made the Danes Christians)

Characteristics

- 2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - G-FSK modulation, 1-100 mW transmit power
- FHSS and TDD
  - Frequency hopping with 1600 hops/s
  - Hopping sequence in a pseudo random fashion, determined by a master
  - Time division duplex for send/receive separation
- Voice link – SCO (Synchronous Connection Oriented)
  - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, 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

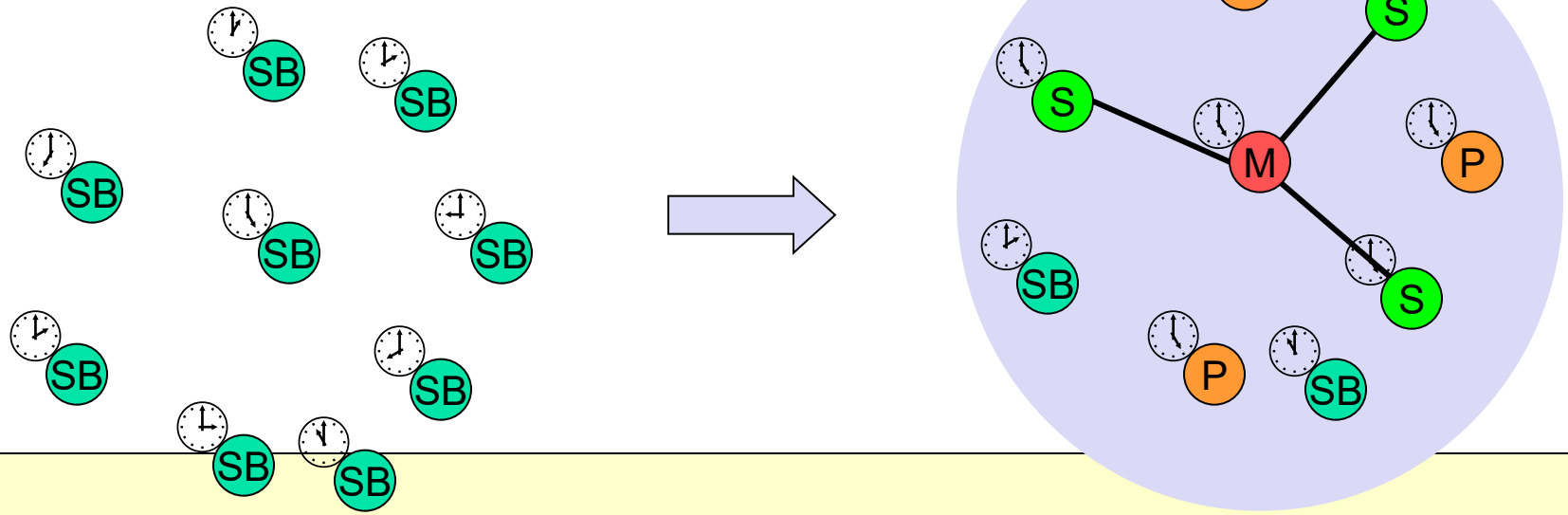
- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping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



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

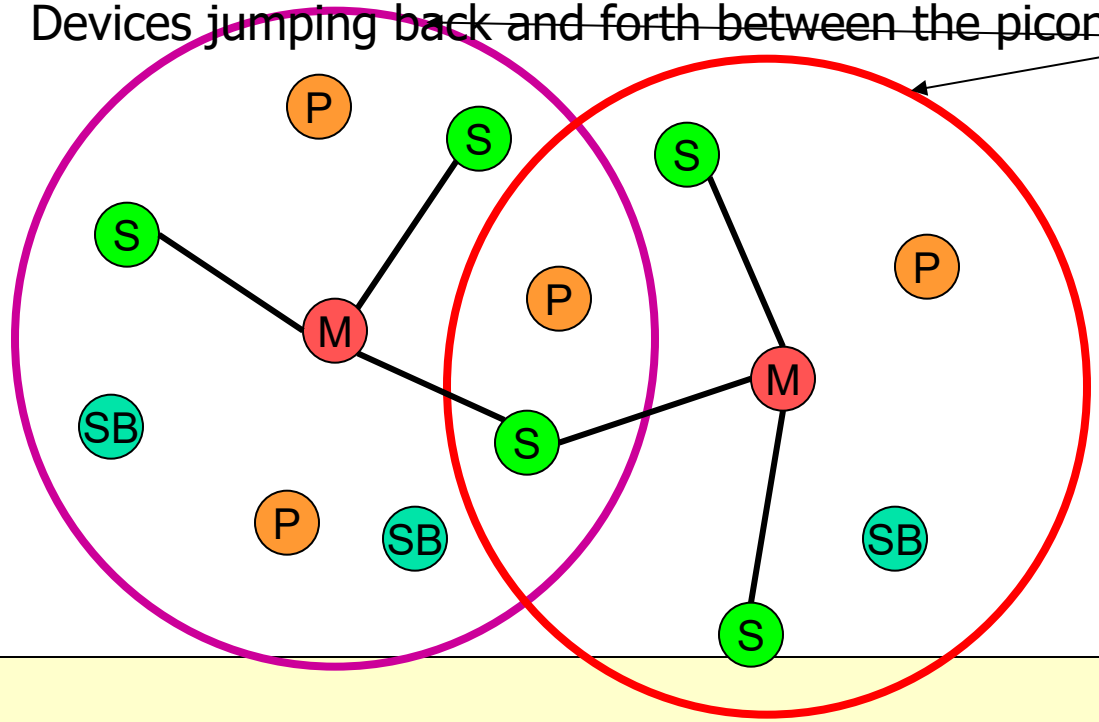
Forming a piconet

- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



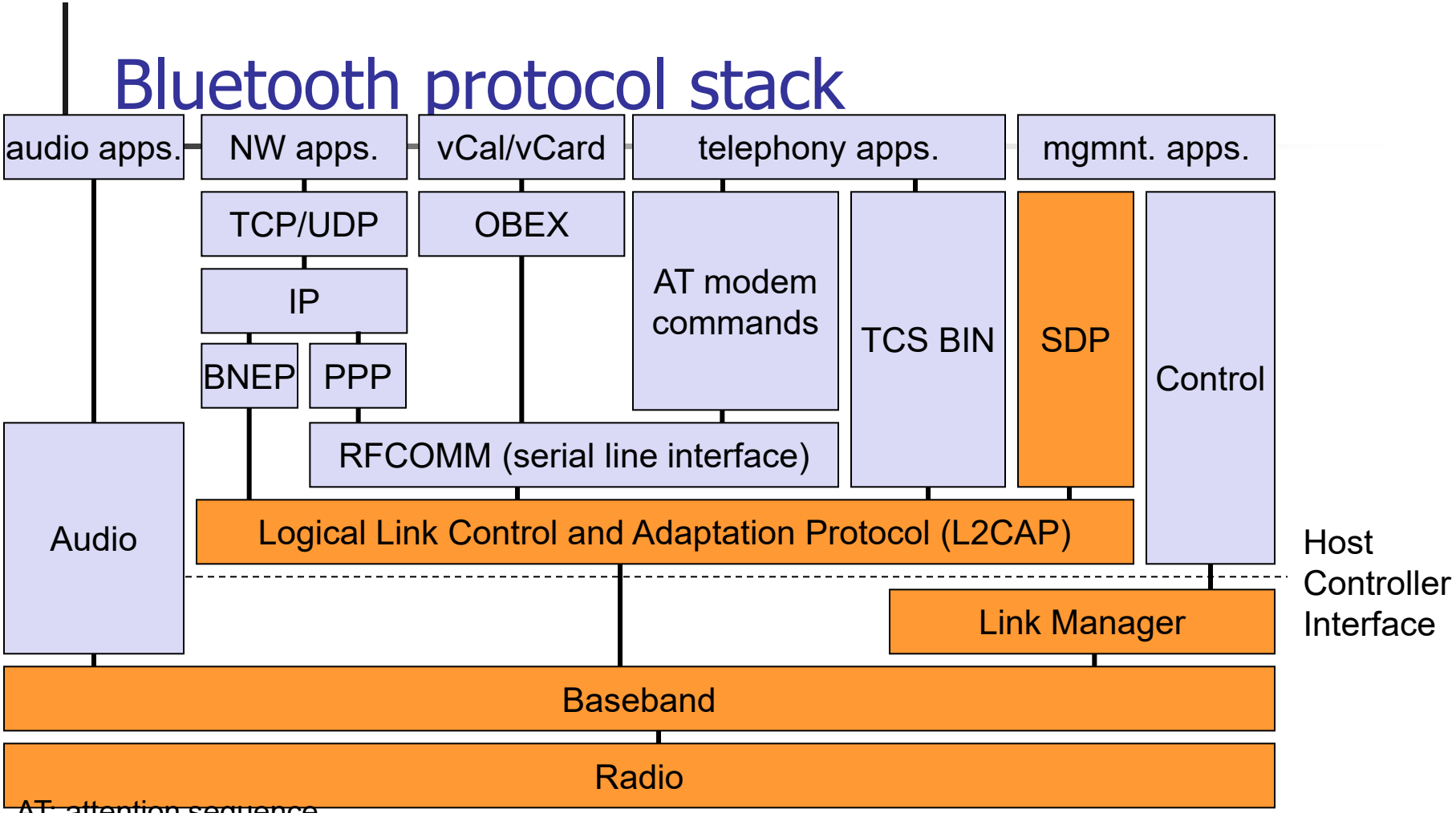
Scatternet

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



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

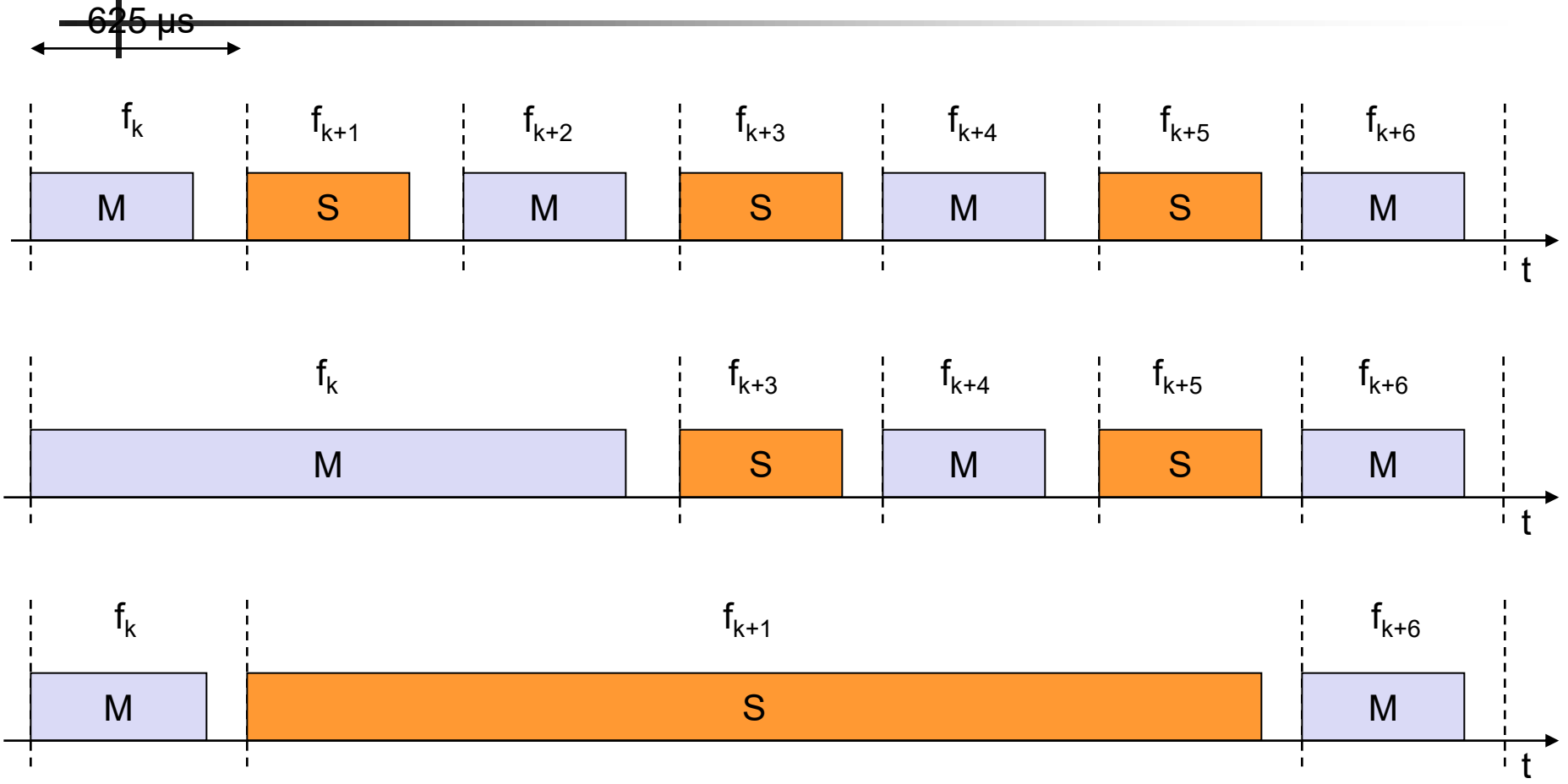
Bluetooth protocol stack



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

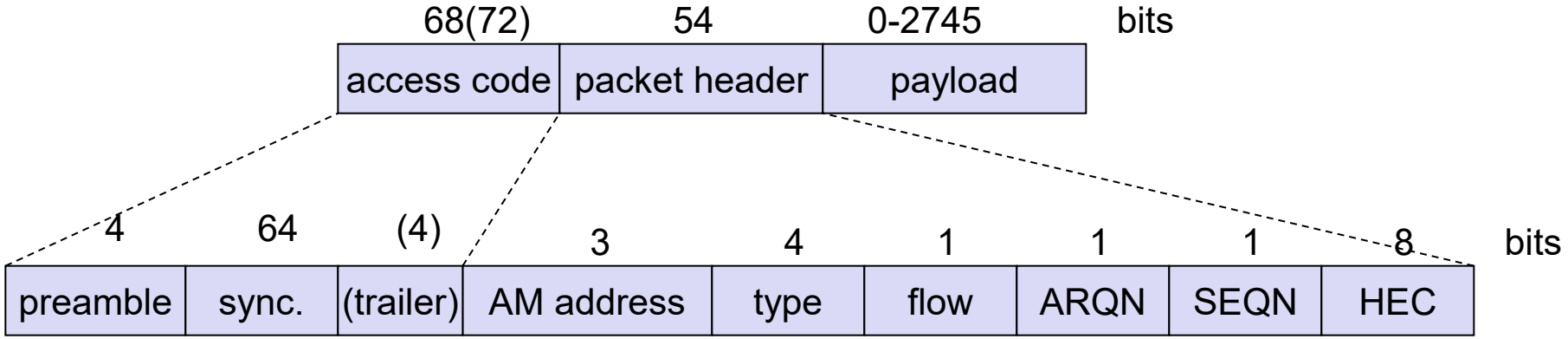
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Frequency selection during data transmission

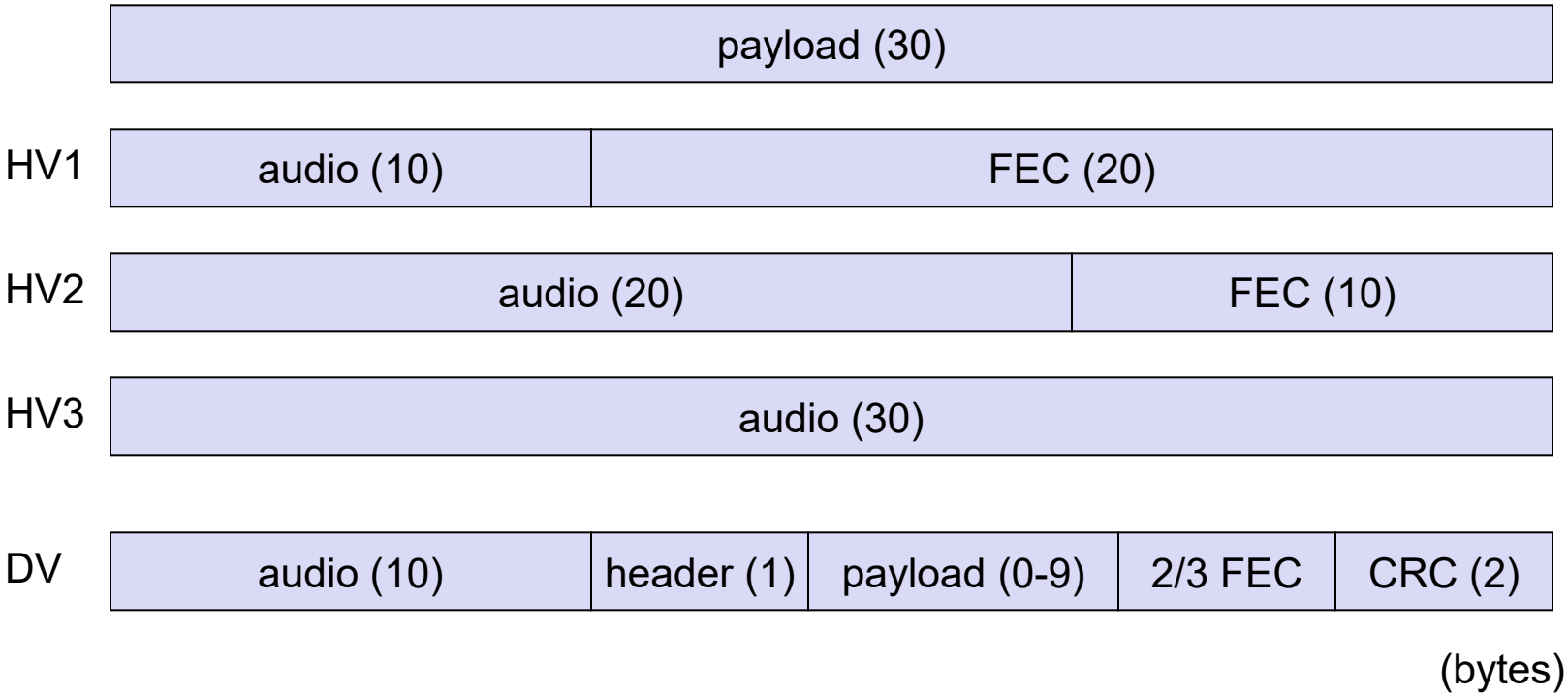


Baseband

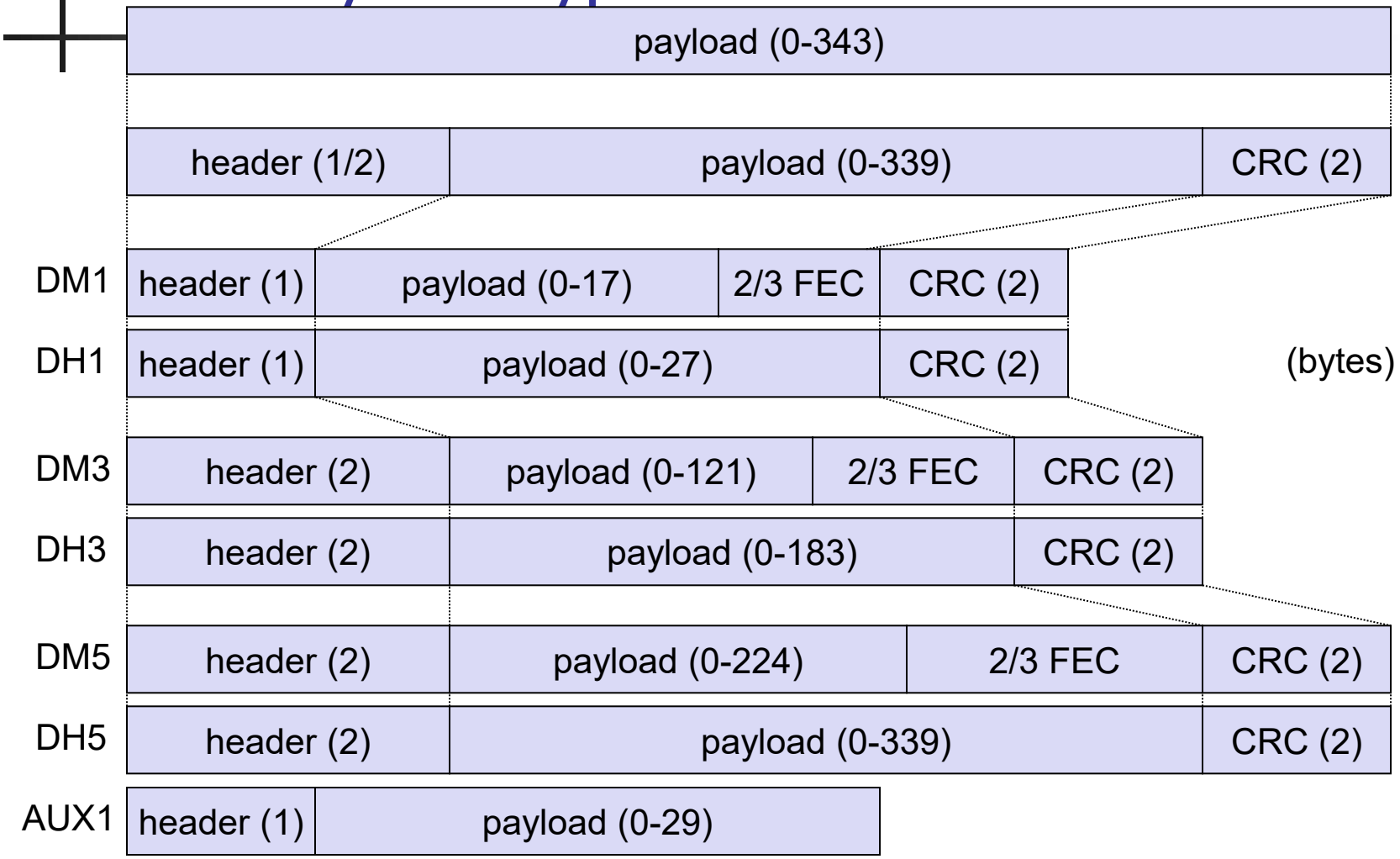
- Piconet/channel definition
- Low-level packet definition
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



SCO payload types



ACL Payload types



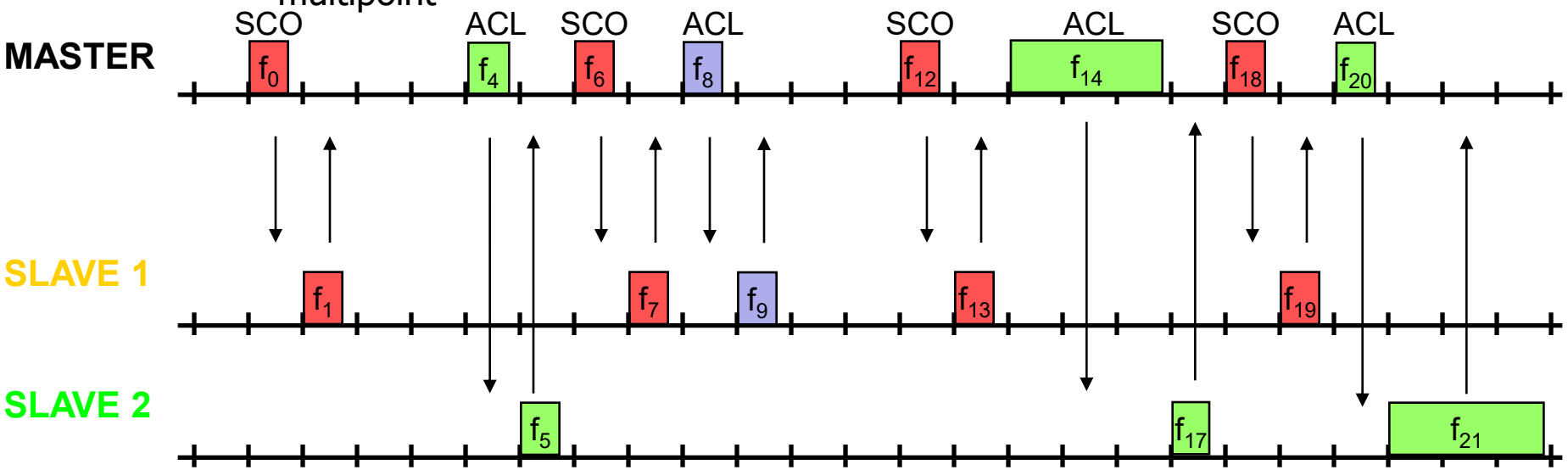
Baseband data rates

	Type	Payload Header [byte]	User Payload [byte]	FEC	CRC	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		
	HV2	na	20	2/3	no	64.0		
	HV3	na	30	no	no	64.0		
	DV	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D		

*D*ata *M*edium/*H*igh rate, *H*igh-quality *V*oice, *D*ata and *V*oice

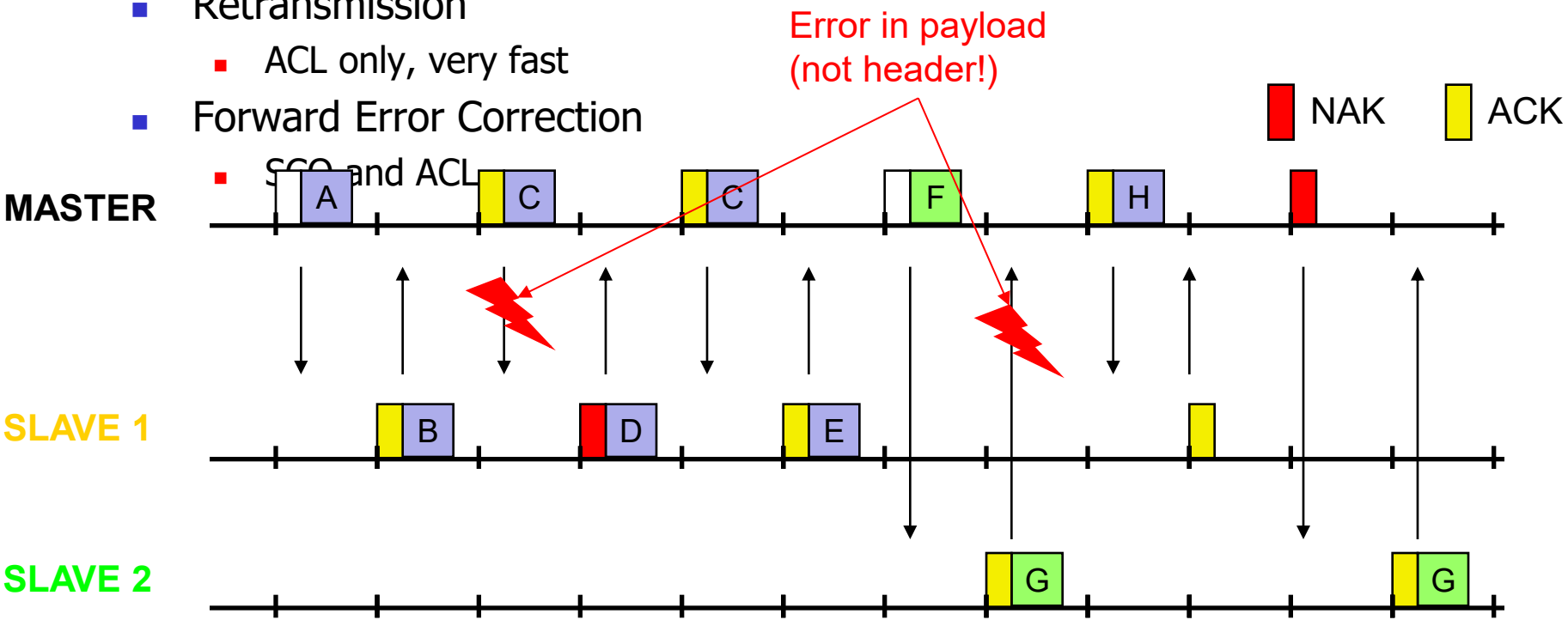
Baseband link types

- 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

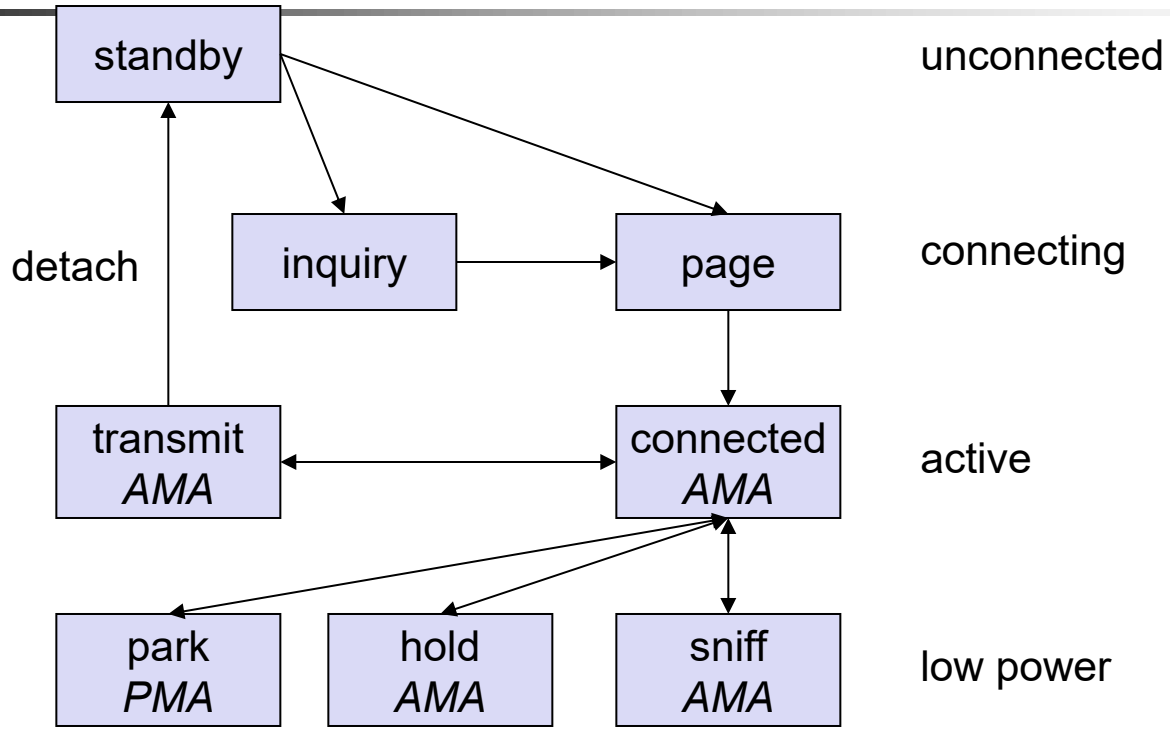


Robustness

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



Baseband states of a Bluetooth device



Standby: do nothing
Inquire: 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 slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

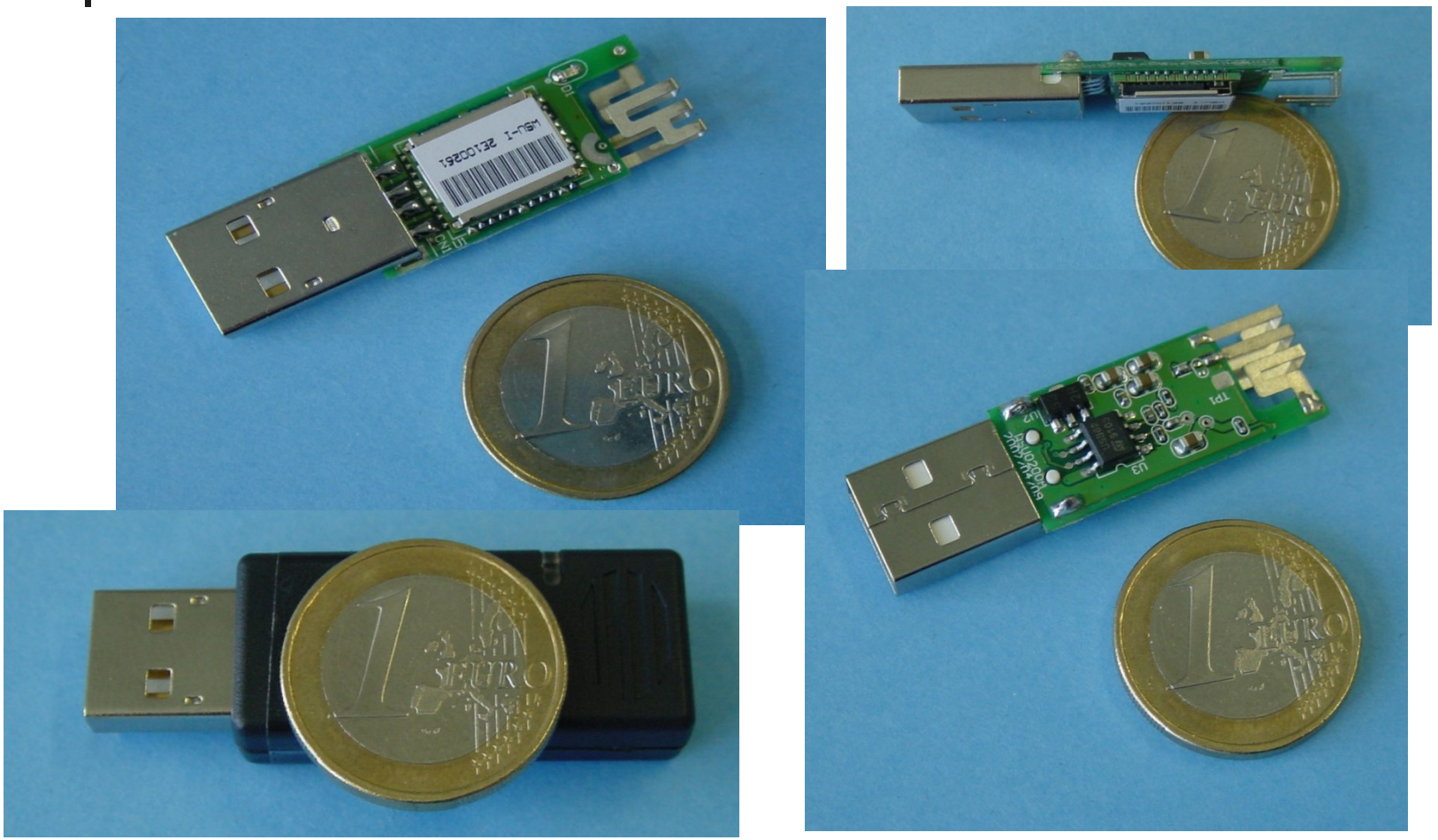
Example: Power consumption/CSR BlueCore2

- **Typical Average Current Consumption[1]**
  - VDD=1.8V Temperature = 20°C
  - **Mode**

SCO connection HV3 (1s interval Sniff Mode) (Slave)	26.0 mA
SCO connection HV3 (1s interval Sniff Mode) (Master)	26.0 mA
SCO connection HV1 (Slave)	53.0 mA
SCO connection HV1 (Master)	53.0 mA
ACL data transfer 115.2kbps UART (Master)	15.5 mA
ACL data transfer 720kbps USB (Slave)	53.0 mA
ACL data transfer 720kbps USB (Master)	53.0 mA
ACL connection, Sniff Mode 40ms interval, 38.4kbps UART	4.0 mA
ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART	0.5 mA
Parked Slave, 1.28s beacon interval, 38.4kbps UART	0.6 mA
Standby Mode (Connected to host, no RF activity)	47.0 μA
Deep Sleep Mode[2]	20.0 μA

- **Notes:**
  - [1] Current consumption is the sum of both BC212015A and the flash.
  - [2] Current consumption is for the BC212015A device only.

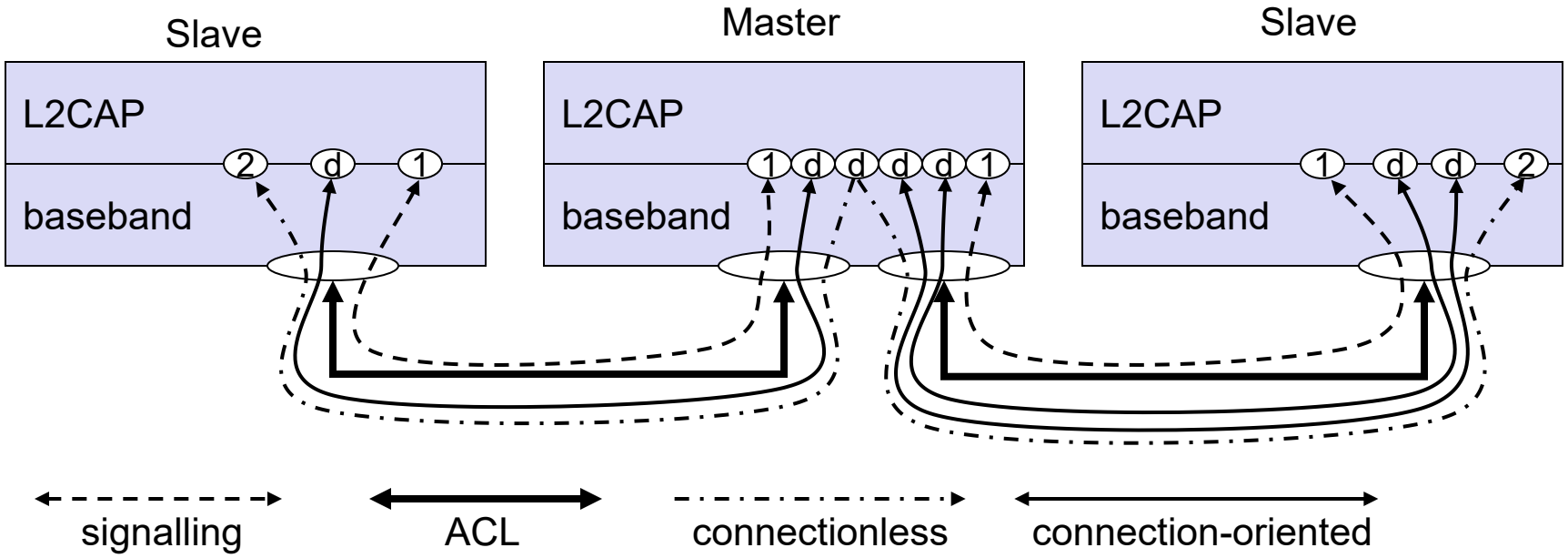
Example: Bluetooth/USB adapter (2002: 50€, today: some cents if integrated)



L2CAP - Logical Link Control and Adaptation Protocol

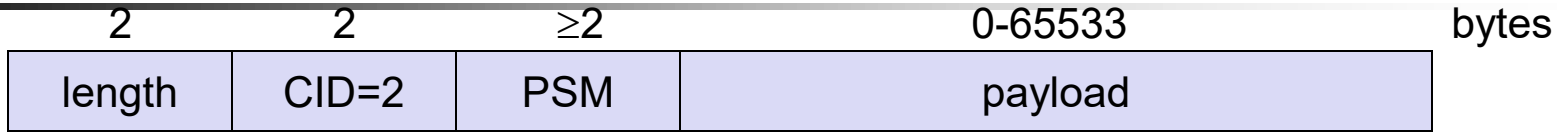
- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signaling channels
- Protocol multiplexing
  - RFCOMM, SDP, telephony control
- Segmentation & reassembly
  - Up to 64kbyte user data, 16 bit CRC used from baseband
- QoS flow specification per channel
  - Follows RFC 1363, specifies delay, jitter, bursts, bandwidth
- Group abstraction
  - Create/close group, add/remove member

L2CAP logical channels

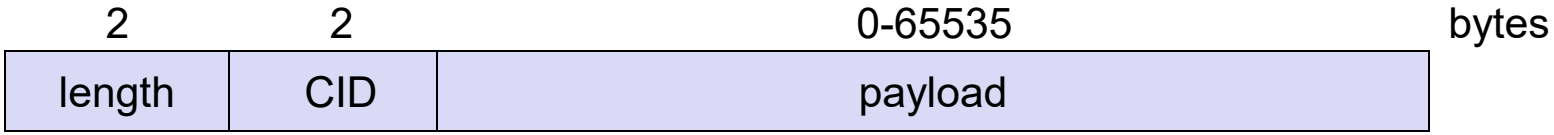


L2CAP packet formats

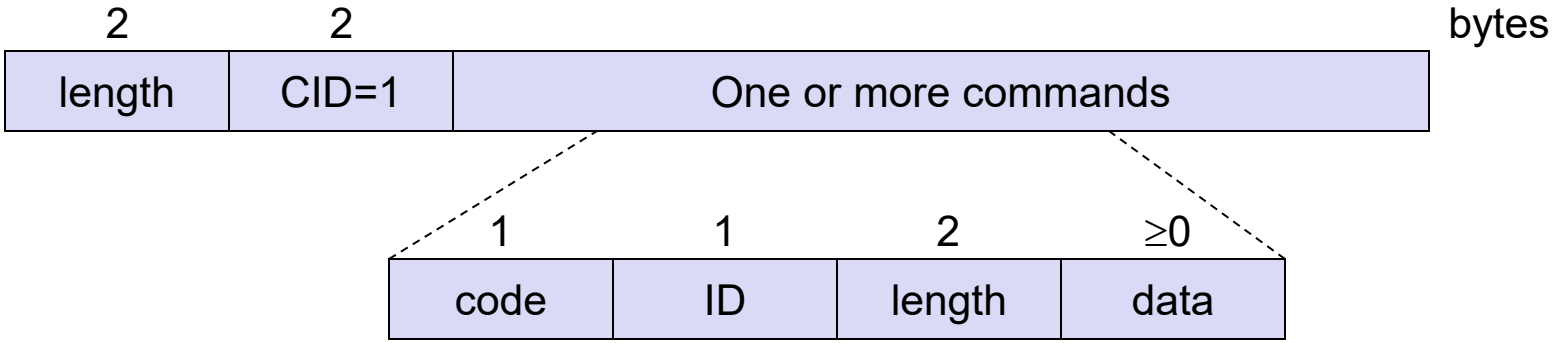
Connectionless PDU



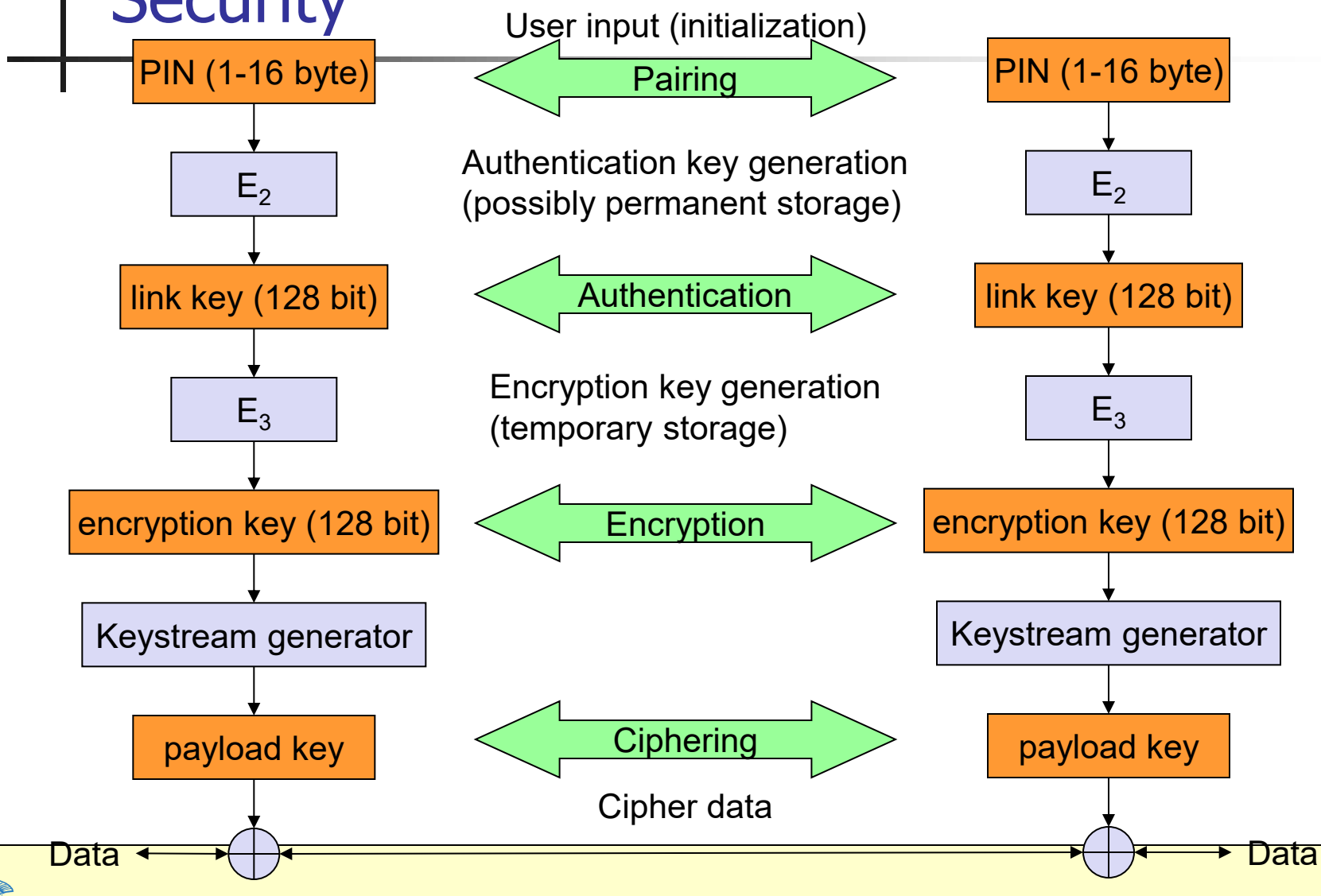
Connection-oriented PDU



Signalling command PDU



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

SDP – Service Discovery Protocol

- Inquiry/response protocol for discovering services
  - Searching for and browsing services in radio proximity
  - Adapted to the highly dynamic environment
  - Can be complemented by others like SLP, Jini, Salutation, …
  - Defines discovery only, not the usage of services
  - Caching of discovered services
  - Gradual discovery

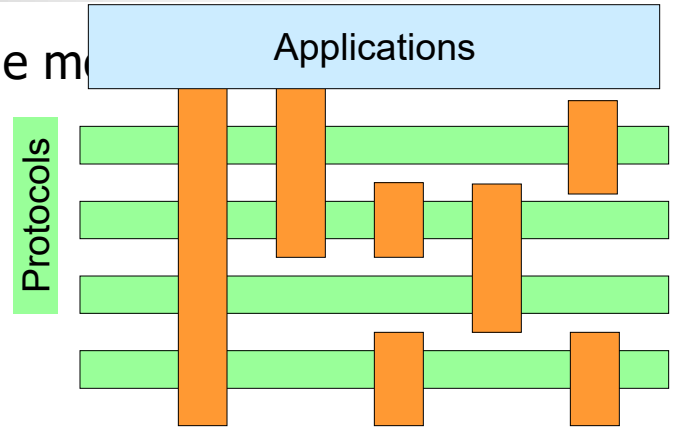
- Service record format
  - Information about services provided by attributes
  - Attributes are composed of an 16 bit ID (name) and a value
  - values may be derived from 128 bit Universally Unique Identifiers (UUID)

Additional protocols to support legacy protocols/apps.

- RFCOMM
  - Emulation of a serial port (supports a large base of legacy applications)
  - Allows multiple ports over a single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
- OBEX
  - Exchange of objects, IrDA replacement
- WAP
  - Interacting with applications on cellular phones

Profiles

- Represent default solutions for a certain usage m
  - Vertical slice through the protocol stack
  - Basis for interoperability
- 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



Profiles

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 1.1
  - also IEEE Standard 802.15.1-2002
  - initial stable commercial standard
- Bluetooth 1.2
  - also IEEE Standard 802.15.1-2005
  - eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
  - AFH (adaptive frequency hopping) to avoid interference
- Bluetooth 2.0 + EDR (2004, no more IEEE)
  - EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
  - lower power consumption due to shorter duty cycle
- Bluetooth 2.1 + EDR (2007)
  - better pairing support (Secure Simple Pairing – SSP)
- Bluetooth 3.0 + HS (2009)
  - Bluetooth 2.1 + EDR + IEEE 802.11a/g = 54 Mbit/s
  - L2CAP enhanced mode
- Bluetooth 4.0 (2010)
  - Classic Bluetooth, Bluetooth High Speed, Bluetooth Low Energy (BLE)
  - BLE – entirely new protocol stack (former WiBree)

Bluetooth versions

- Bluetooth 4.1 (2013)
  - Incremental software update, no hardware update
- Bluetooth 4.2 (2014)
  - Features for IoT
    - Low Energy Secure Connection
    - Link Layer privacy
    - IPv6 support
- Bluetooth 5 (2016)
  - BLE options to trade off between range and data rate
- Bluetooth 5.1 (2019)
  - Location/tracking (AoA, AoD)
  - Advertising Channel Index
  - GATT Caching
- Bluetooth 5.2 (2020)
  - LE Audio, LE Power Control, LE Isochronous Channel
  - Enhanced Attribute Protocol (EATT)

Bluetooth versions

- Bluetooth 5.3 (2021)
  - Connection Subrating
  - Periodic Advertisement Interval
  - Channel Classification Enhancement
  - Encryption Key Size Control Enhancements
- Bluetooth 5.4 (2023)
  - Periodic Advertising with Responses (PAwR)
  - Encrypted Advertising Data
  - LE GATT Security Levels Characteristic
  - Advertising Coding Selection

Bluetooth versions

- Bluetooth 6.0 (2024)
  - Bluetooth Channel Sounding
  - Decision-based advertising filtering
  - Monitoring advertisers
  - ISOAL enhancement
  - LL extended feature set
  - Frame space update
- Bluetooth 6.1 (2025)
  - Increased device privacy
  - Improved power efficiency

WPAN: IEEE 802.15.1 – Bluetooth

- Data rate
  - Synchronous, connection-oriented: 64 kbit/s
  - Asynchronous, connectionless
    - 433.9 kbit/s symmetric
    - 723.2 / 57.6 kbit/s asymmetric
- Transmission range
  - POS (Personal Operating Space) up to 10 m
  - with special transceivers up to 100 m
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Challenge/response (SAFER+), hopping sequence
- Availability
  - Integrated into many products, several vendors
- Connection set-up time
  - Depends on power-mode
  - Max. 2.56s, avg. 0.64s
- Quality of Service
  - Guarantees, ARQ/FEC
- Manageability
  - Public/private keys needed, key management not specified, simple system integration
- Special Advantages/Disadvantages
  - Advantage: already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
  - Disadvantage: interference on ISM-band, limited range, max. 8 active devices/network, high set-up latency

WPAN: IEEE 802.15 – future developments 1

- 802.15.2: Coexistance
  - Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference
- 802.15.3: High-Rate
  - Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
  - Data Rates: 11, 22, 33, 44, 55 Mbit/s
  - Quality of Service isochronous protocol
  - Ad hoc peer-to-peer networking
  - Security
  - Low power consumption
  - Low cost
  - Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

WPAN: IEEE 802.15 – future developments 2

- Several working groups extend the 802.15.3 standard
- 802.15.3a: - withdrawn -
  - Alternative PHY with higher data rate as extension to 802.15.3
  - Applications: multimedia, picture transmission
- 802.15.3b:
  - Enhanced interoperability of MAC
  - Correction of errors and ambiguities in the standard
- 802.15.3c:
  - Alternative PHY at 57-64 GHz
  - Goal: data rates above 2 Gbit/s
- Not all these working groups really create a standard, not all standards will be found in products later …

WPAN: IEEE 802.15 – future developments 3

- 802.15.4: Low-Rate, Very Low-Power
  - Low data rate solution with multi-month to multi-year battery life and very low complexity
  - Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
  - Data rates of 20-250 kbit/s, latency down to 15 ms
  - Master-Slave or Peer-to-Peer operation
  - Up to 254 devices or 64516 simpler nodes
  - Support for critical latency devices, such as joysticks
  - CSMA/CA channel access (data centric), slotted (beacon) or unslotted
  - Automatic network establishment by the PAN coordinator
  - Dynamic device addressing, flexible addressing format
  - Fully handshaked protocol for transfer reliability
  - Power management to ensure low power consumption
  - 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band
- Basis of the ZigBee technology – www.zigbee.org

ZigBee

- Relation to 802.15.4 similar to Bluetooth / 802.15.1
- Pushed by Chipcon (now TI), ember, freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung…
- More than 260 members – see www.zigbee.org
  - about 11 promoters, 160 participants, 240 adopters
  - must be member to commercially use ZigBee spec
- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications

WPAN: IEEE 802.15 – future developments 4

- 802.15.4a:
  - Alternative PHY with lower data rate as extension to 802.15.4
  - Properties: precise localization (< 1m precision), extremely low power consumption, longer range
  - Two PHY alternatives
    - UWB (Ultra Wideband): ultra short pulses, communication and localization
    - CSS (Chirp Spread Spectrum): communication only
- 802.15.4b, c, d, e, f, g:
  - Extensions, corrections, and clarifications regarding 802.15.4
  - Usage of new bands, more flexible security mechanisms
  - RFID, smart utility neighborhood (high scalability)
- 802.15.5: Mesh Networking
  - Partial meshes, full meshes
  - Range extension, more robustness, longer battery live
- 802.15.6: Body Area Networks
  - Low power networks e.g. for medical or entertainment use
- 802.15.7: Visible Light Communication
- Not all these working groups really create a standard, not all standards will be found in products later … see http://www.ieee802.org/15/