192620010
Mobile & Wireless Networking

Lecture 8:
Bluetooth & Zigbee

[Schiller, Section 7.5]
[Reader, Part 7]
[*Optional: Wikipedia, “Bluetooth”*]

Geert Heijenk

Outline of Lecture 10

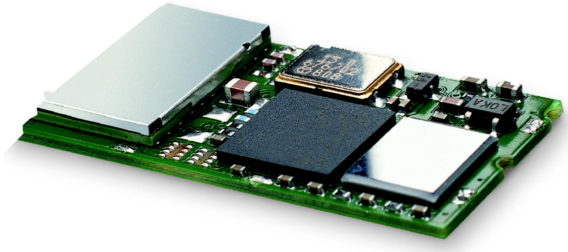
- Bluetooth
  - General characteristics
  - Piconets & scatternets
  - Basic Access scheme
  - Baseband (MAC layer)
  - Higher layer protocols
  - Profiles and Versions

- Zigbee
  - Zigbee vs. IEEE 802.15.4
  - Architecture & Topologies
  - IEEE 802.15.4 MAC layer

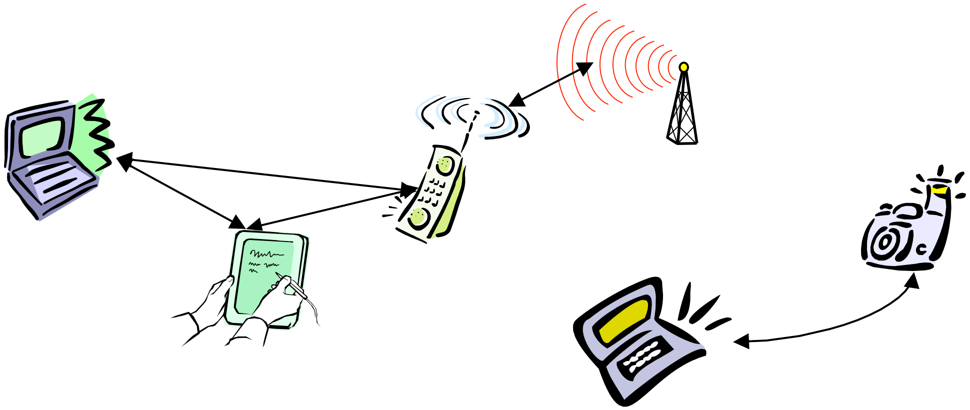
Bluetooth

Idea

- ❑ Universal radio interface for ad-hoc wireless connectivity
- ❑ Interconnecting computer and peripherals, handheld devices, PDAs, cell phones
- ❑ 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 (original version)



One of the first modules (Ericsson).



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
- 2001: first consumer products for mass market, spec. version 1.1 released
- 2005: 5 million chips / week
- 2014: Cumulative product shipments appr. 3 billion

Special Interest Group

- Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
- Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
- > 10000 members
- Common specification and certification of products

Characteristics

2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing

- ❑ Channel 0: 2402 MHz … channel 78: 2480 MHz
- ❑ GFSK modulation (1Mbit/s), 1-100 mW transmit power
- ❑ π/4-DQPSK (2Mbit/s) and 8DPSK (3Mbit/s) for Bluetooth 2.0+EDR

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)

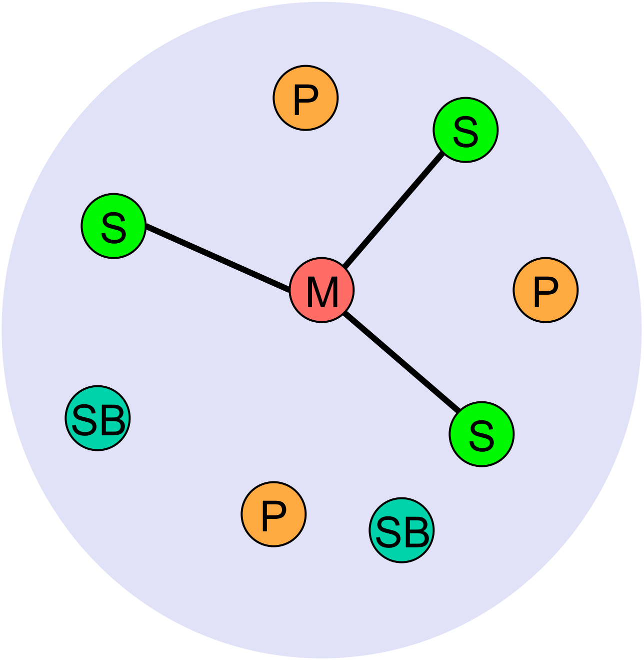
- ❑ Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

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)

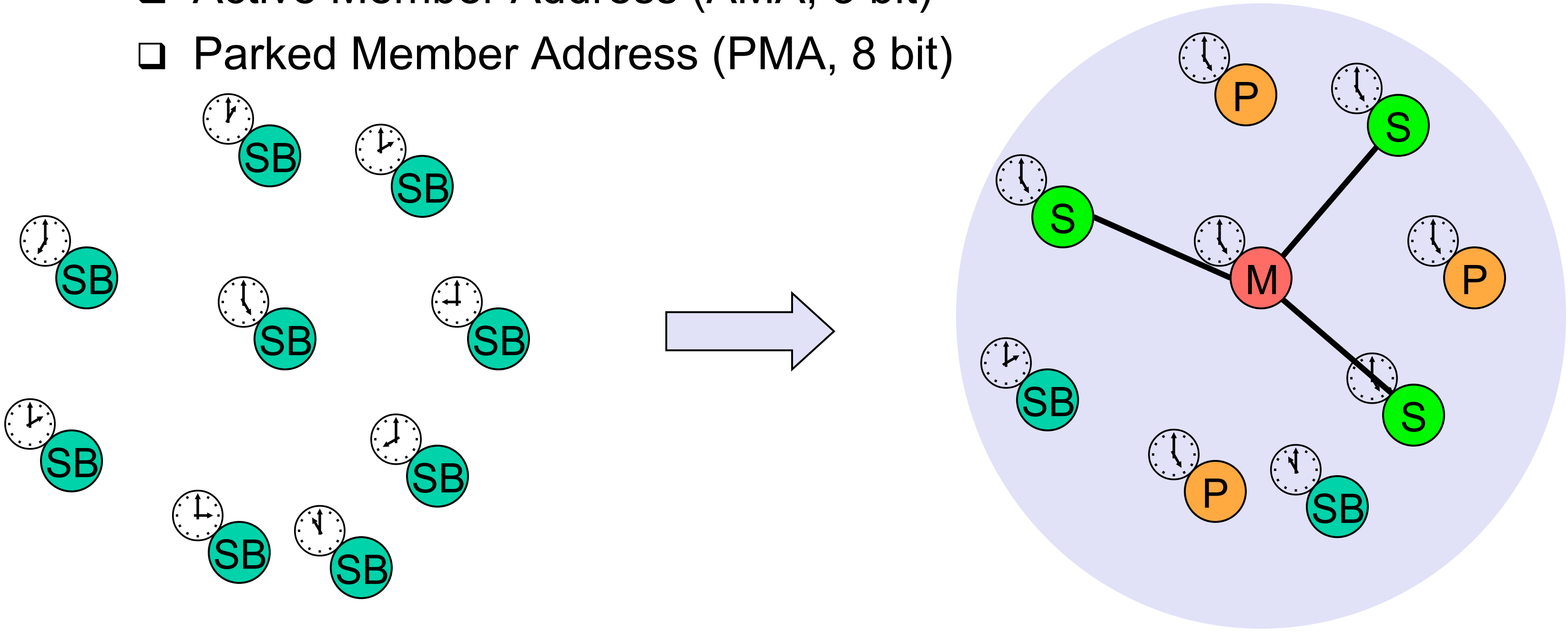


M=Master
S=Slave

P=Parked
SB=Standby

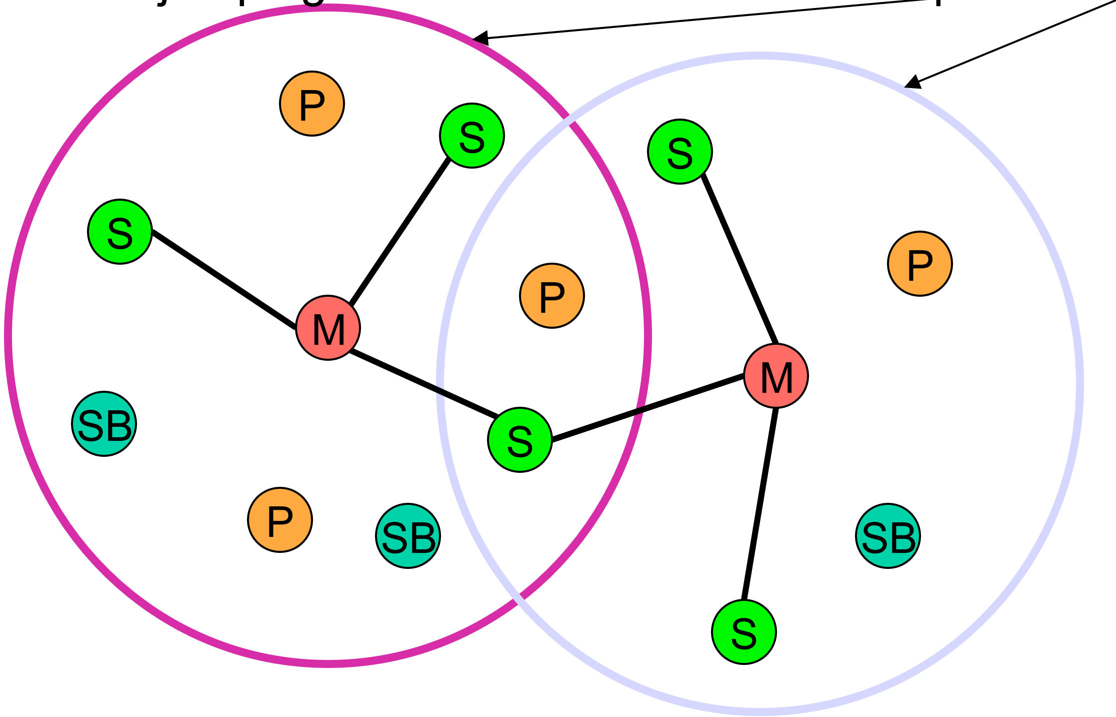
Forming a piconet

- 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

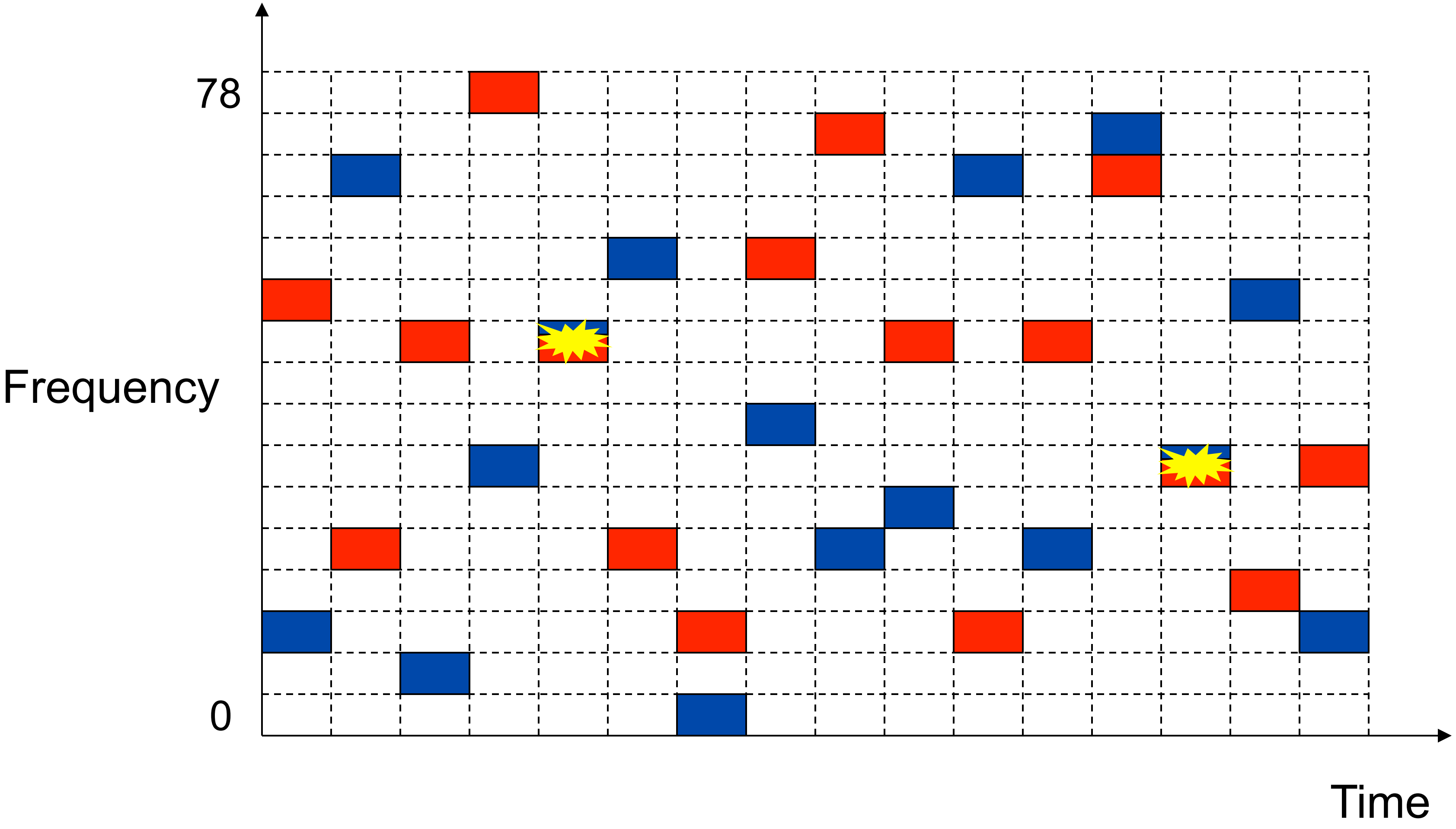
- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets



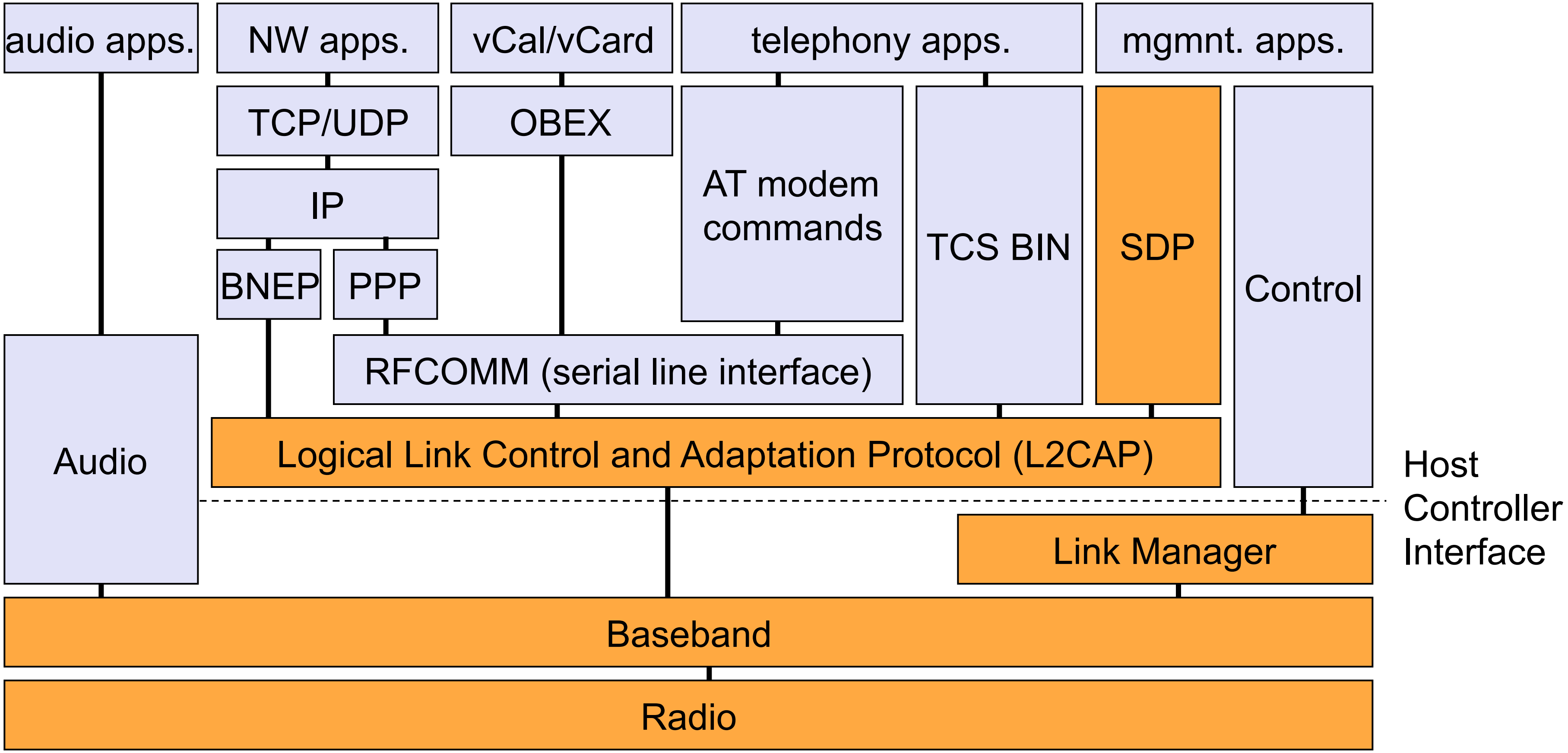
Piconets
(each with a
capacity of
< 1 Mbit/s)

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

Frequency hopping



Bluetooth protocol stack

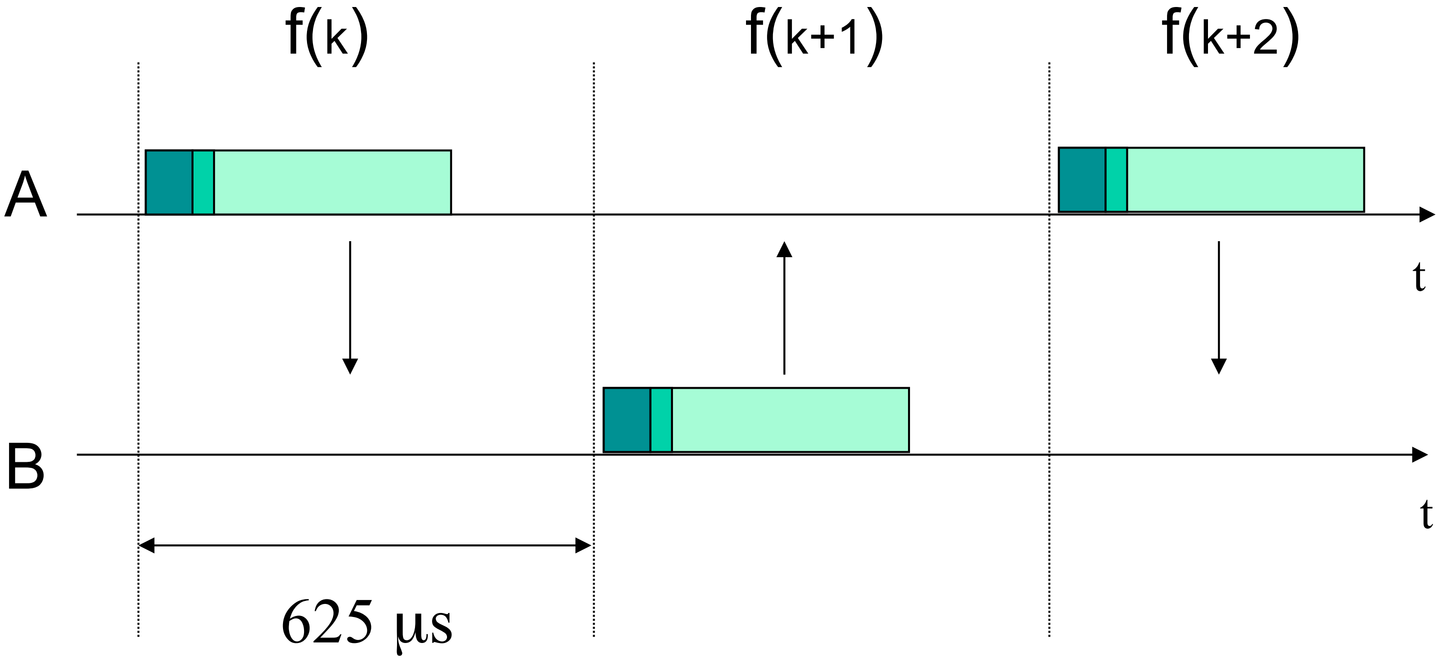


AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

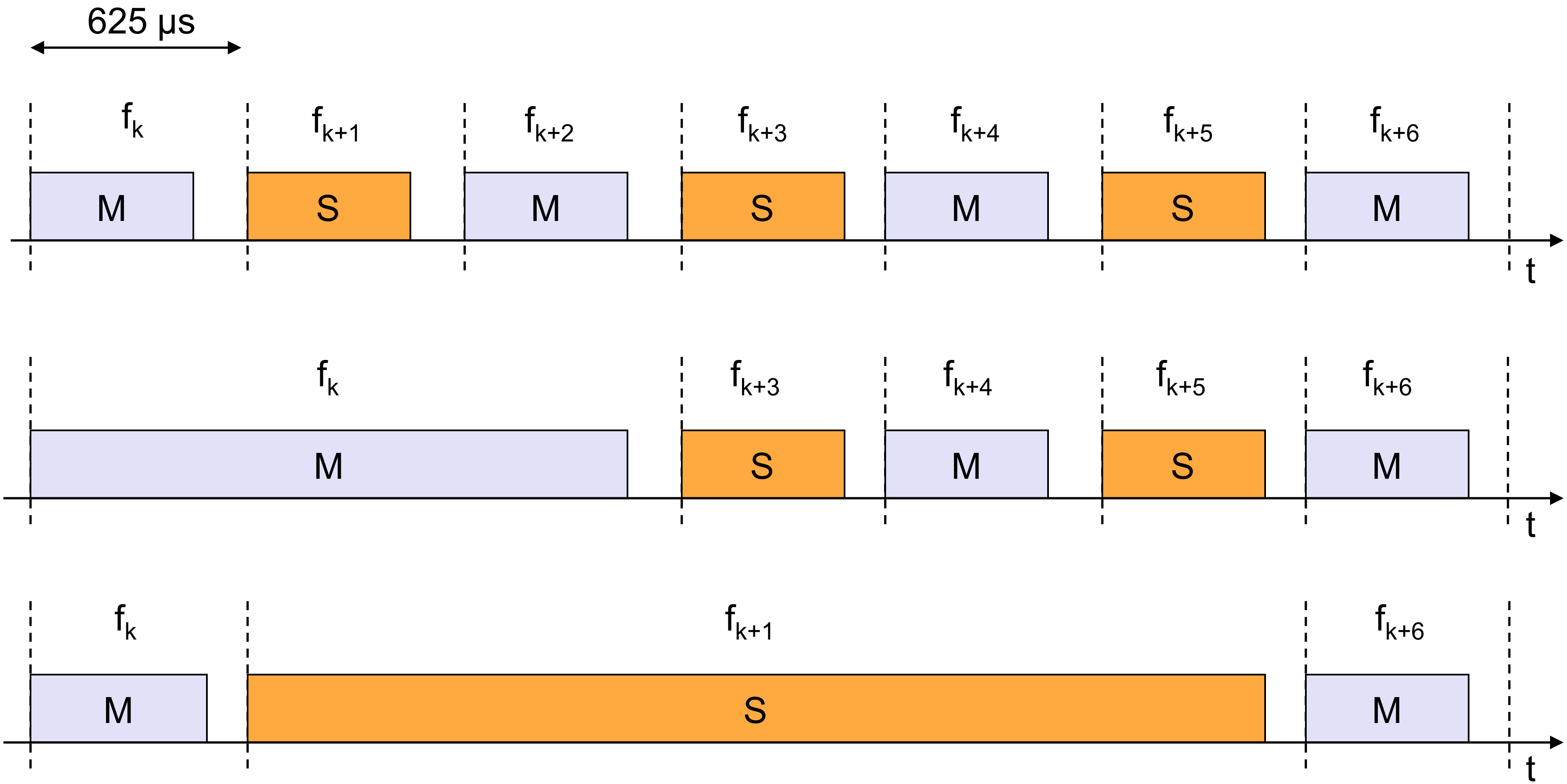
SDP: service discovery protocol
RFCOMM: radio frequency comm.

Basic access scheme

- 79 hops (in Japan, Spain, and France 23) at a 1 Mhz spacing
- dwel time of 625 μs
- master determines the hopping sequence
- TDD

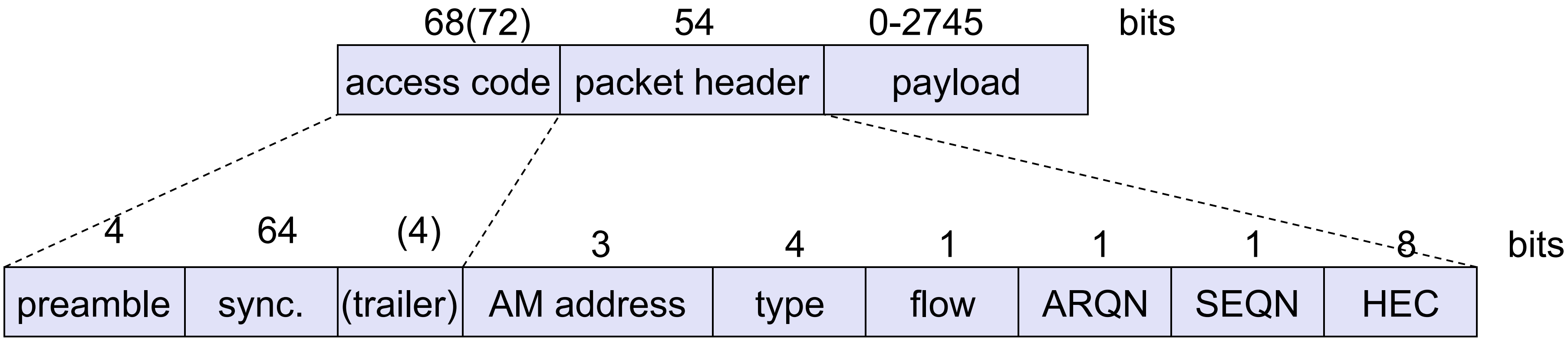


Frequency selection during data transmission



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



68(72)	54	0-2745	bits
access code	packet header	payload	

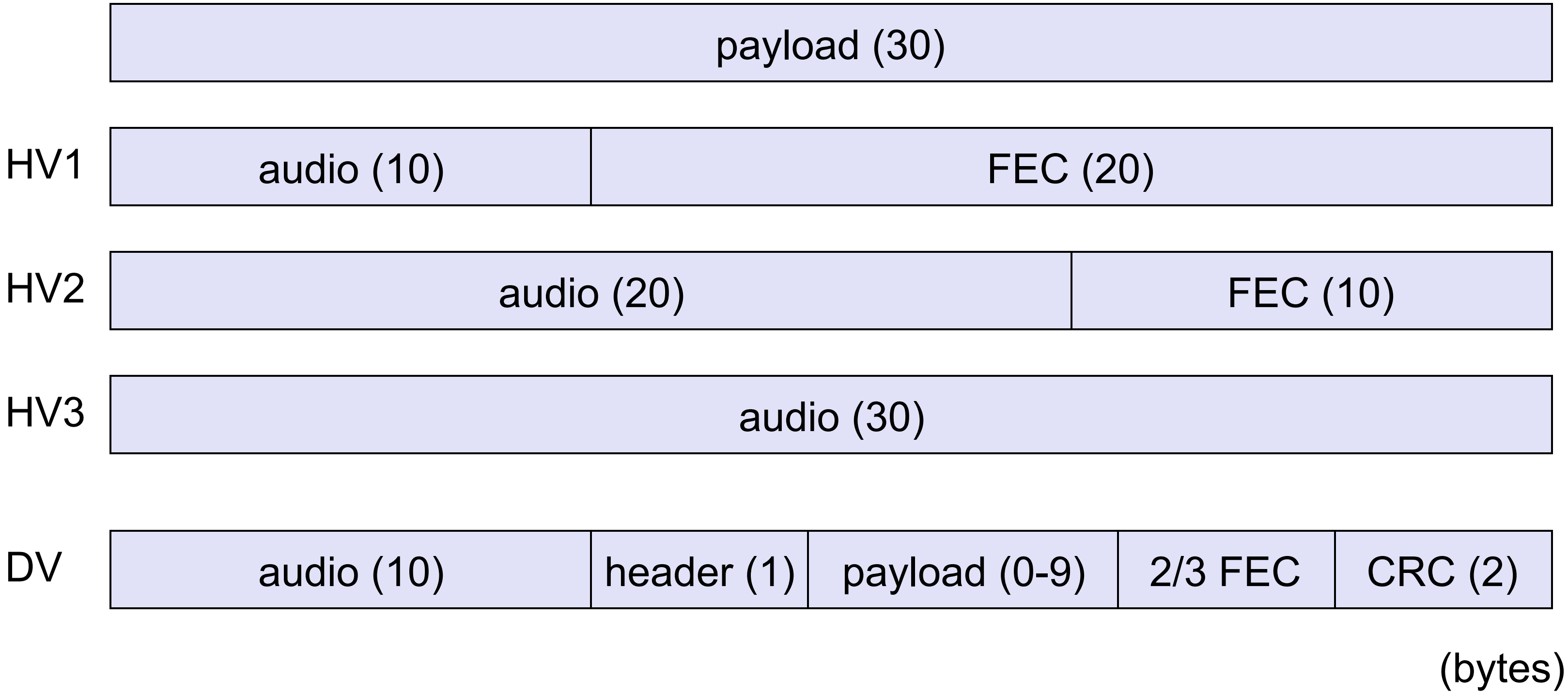
4	64	(4)	3	4	1	1	1	8	bits
preamble	sync.	(trailer)	AM address	type	flow	ARQN	SEQN	HEC	

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		

Data Medium/*High* rate, *High*-quality *Voice*, *Data* and *Voice*

SCO payload types



payload (30)

HV1 audio (10) FEC (20)

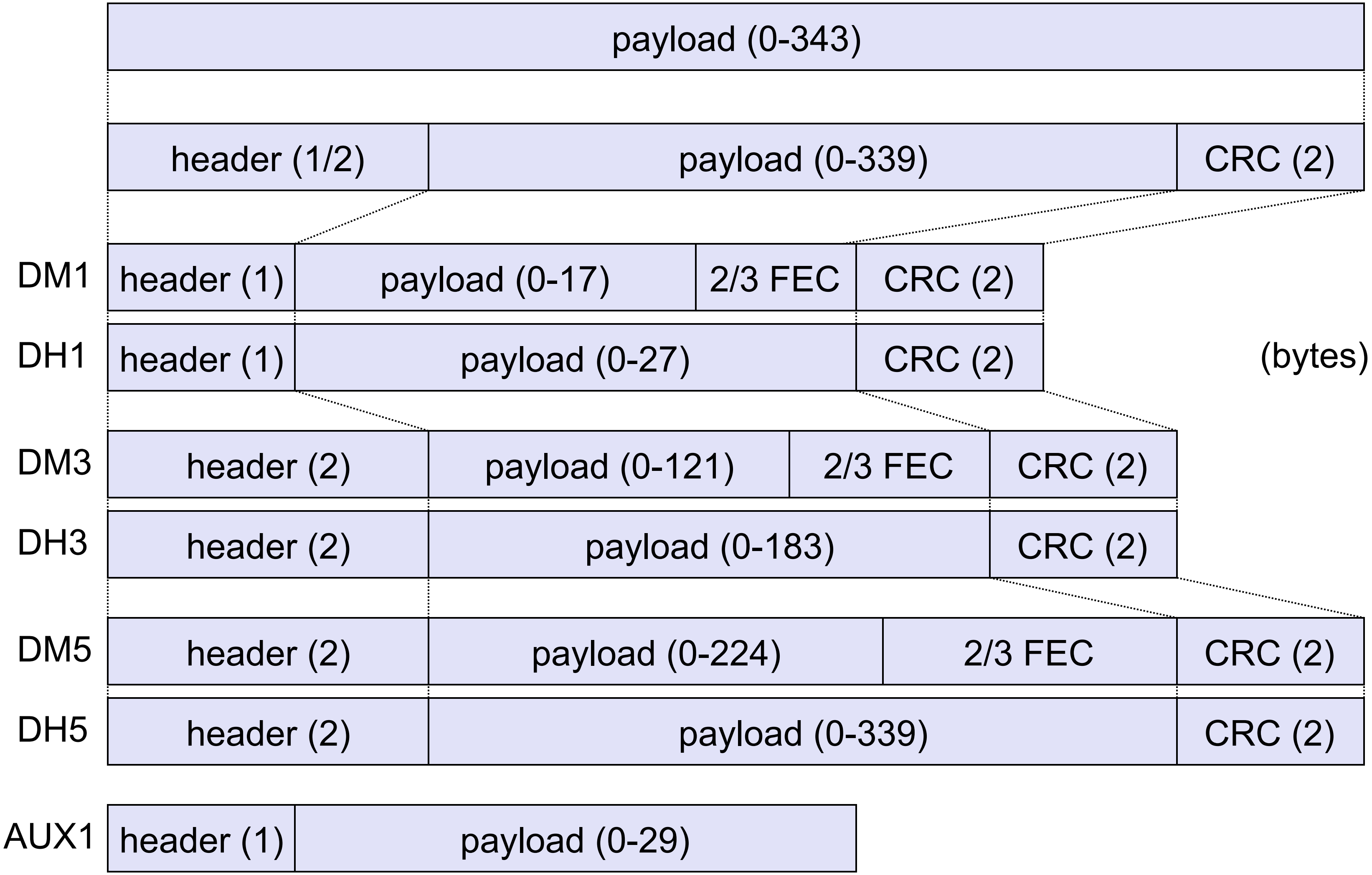
HV2 audio (20) FEC (10)

HV3 audio (30)

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

(bytes)

ACL Payload types



payload (0-343)

header (1/2) | payload (0-339) | CRC (2)

DM1 | header (1) | payload (0-17) | 2/3 FEC | CRC (2)

DH1 | header (1) | payload (0-27) | CRC (2)

(bytes)

DM3 | header (2) | payload (0-121) | 2/3 FEC | CRC (2)

DH3 | header (2) | payload (0-183) | CRC (2)

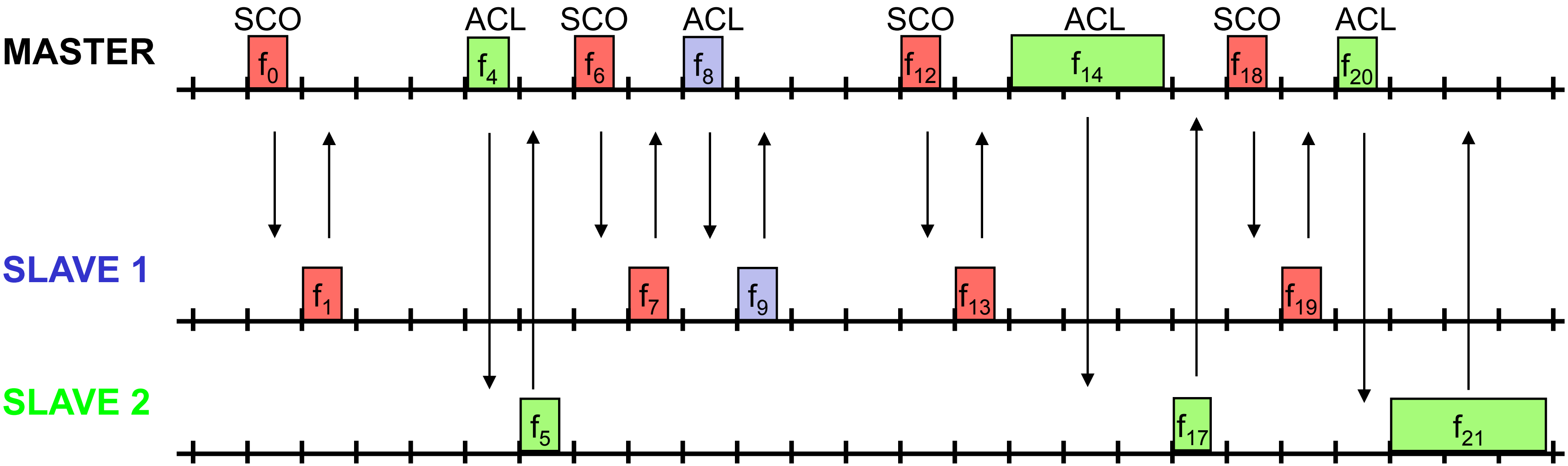
DM5 | header (2) | payload (0-224) | 2/3 FEC | CRC (2)

DH5 | header (2) | payload (0-339) | CRC (2)

AUX1 | header (1) | payload (0-29)

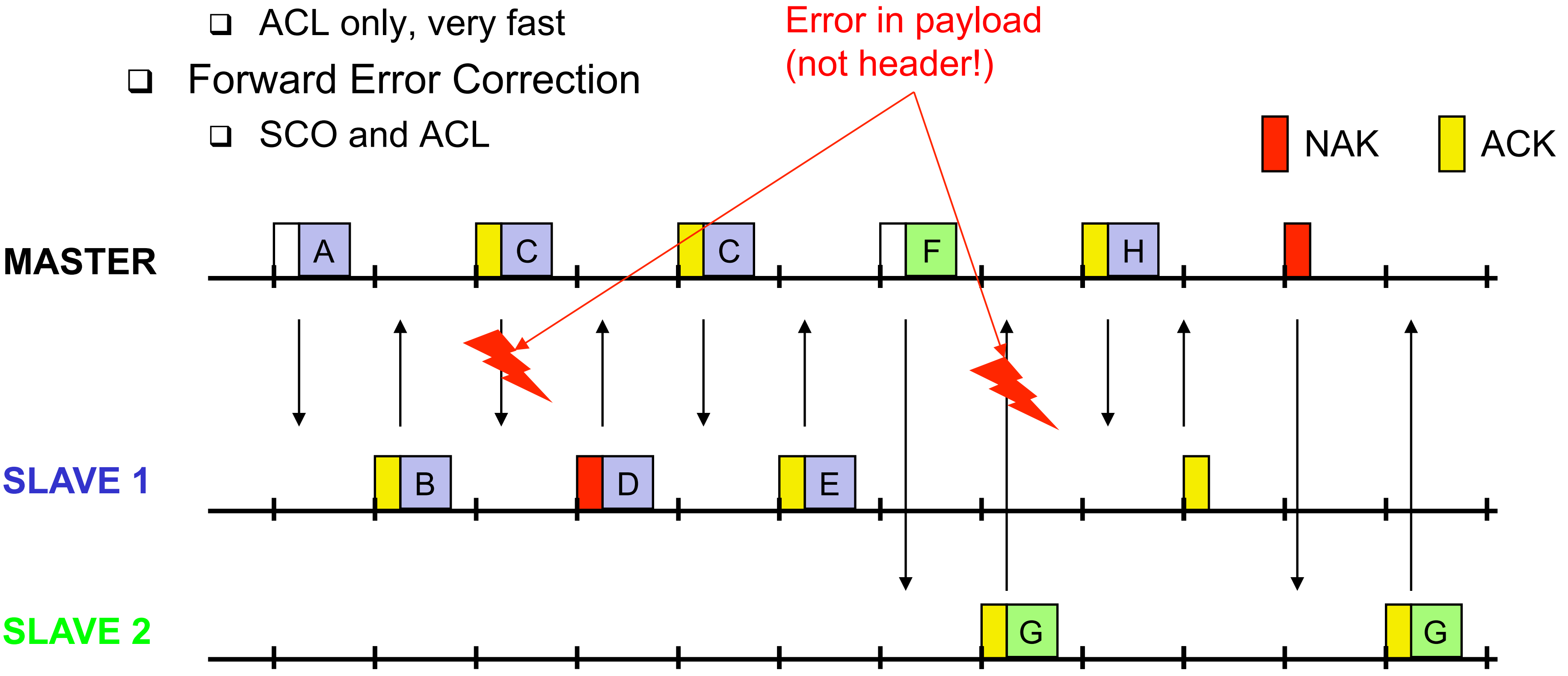
Baseband link types

- 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

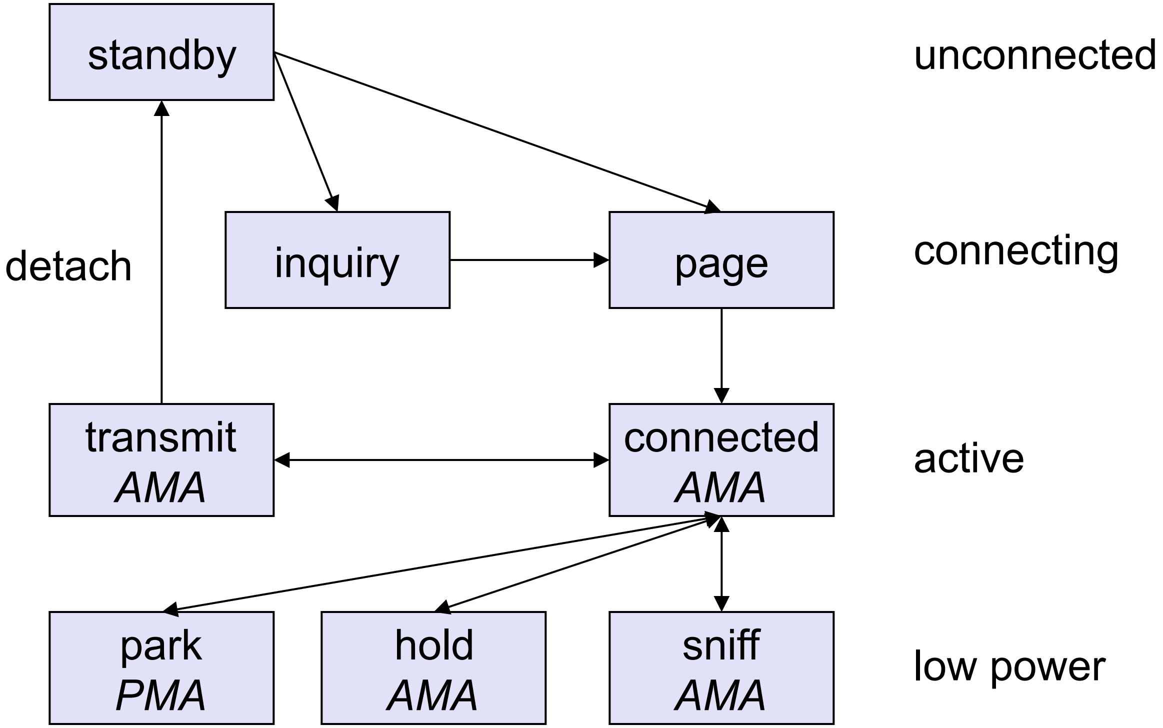
- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets (FH Spread Spectrum)
- Retransmission
  - ACL only, very fast
- Forward Error Correction
  - SCO and ACL



Link manager protocol

- Authentication, pairing and encryption
- Synchronization
- Capability negotiation
- Quality of service negotiation
- Power control
- State and transmission mode change

Baseband states of a Bluetooth device



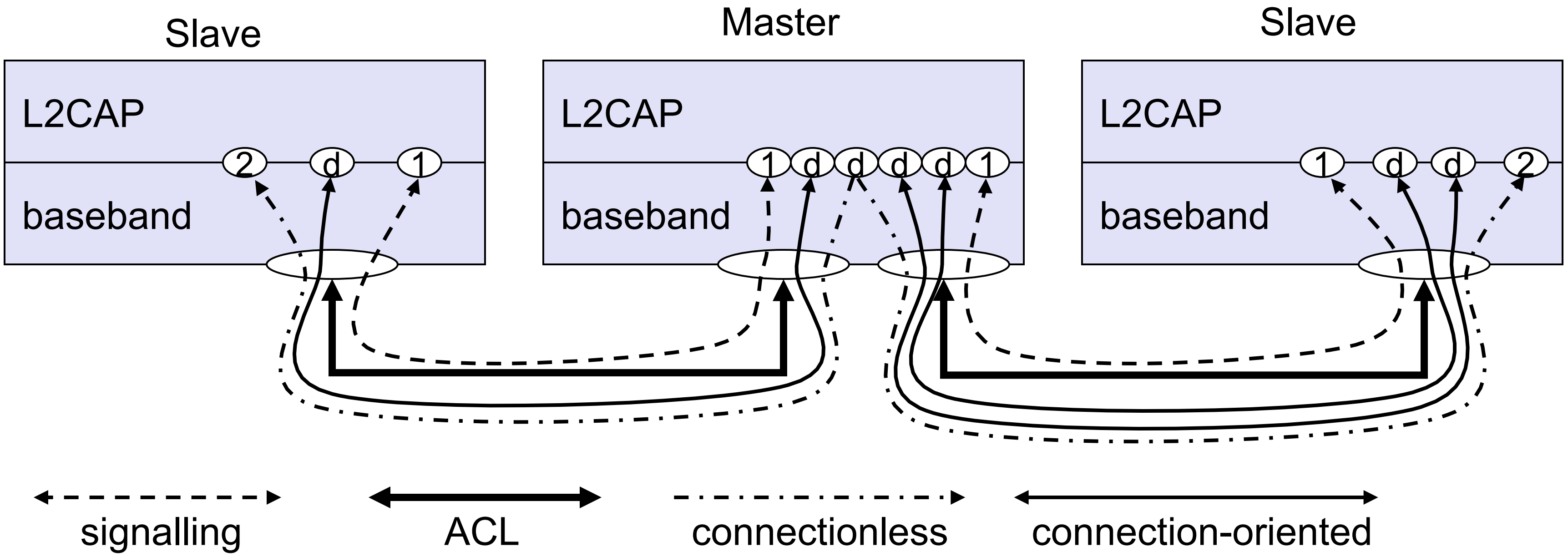
Standby: do nothing
Inquire: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

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

L2CAP - Logical Link Control and Adaptation Protocol

- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signalling 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

2	2	≥2	0-65533	bytes
length	CID=2	PSM	payload	

Connection-oriented PDU

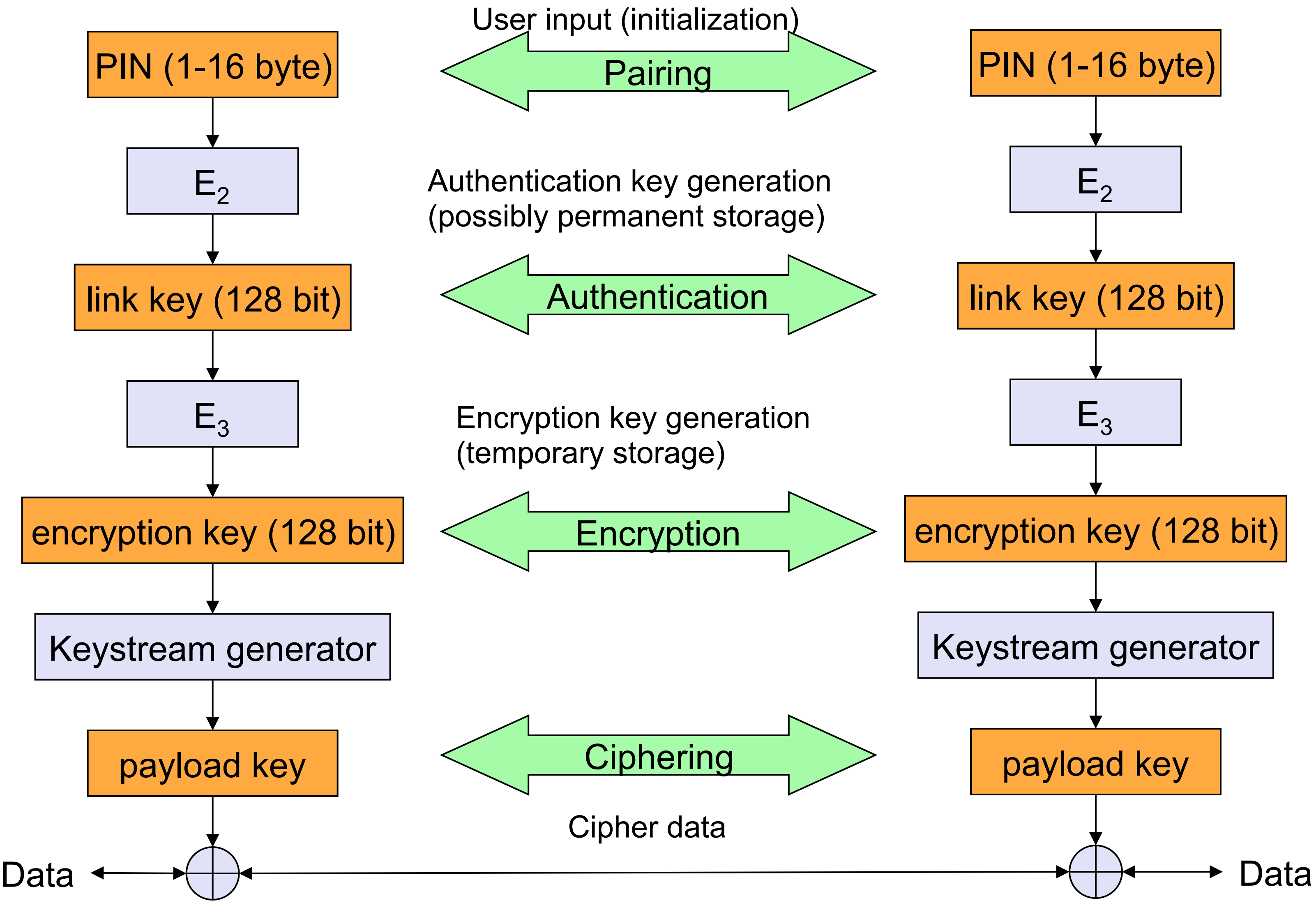
2	2	0-65535	bytes
length	CID	payload	

Signalling command PDU

2	2		bytes
length	CID=1	One or more commands	

1	1	2	≥0
code	ID	length	data

Security


User input (initialization)
PIN (1-16 byte)
Pairing
PIN (1-16 byte)
E_2
Authentication key generation
(possibly permanent storage)
E_2
link key (128 bit)
Authentication
link key (128 bit)
E_3
Encryption key generation
(temporary storage)
E_3
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

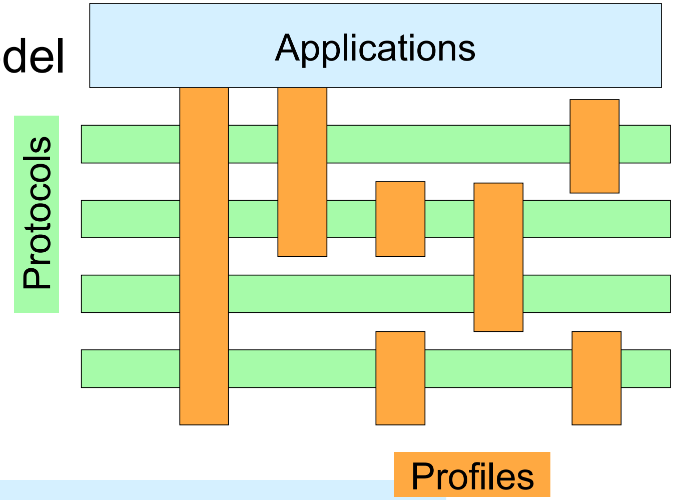
- Inquiry/response protocol for discovering services
  - Searching for and browsing services in radio proximity
  - Adapted to the highly dynamic environment
  - Can be complemented by others like SLP, Jini, Salutation, …
  - Defines discovery only, not the usage of services
  - Caching of discovered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

Profiles

Represent default solutions for a certain usage model

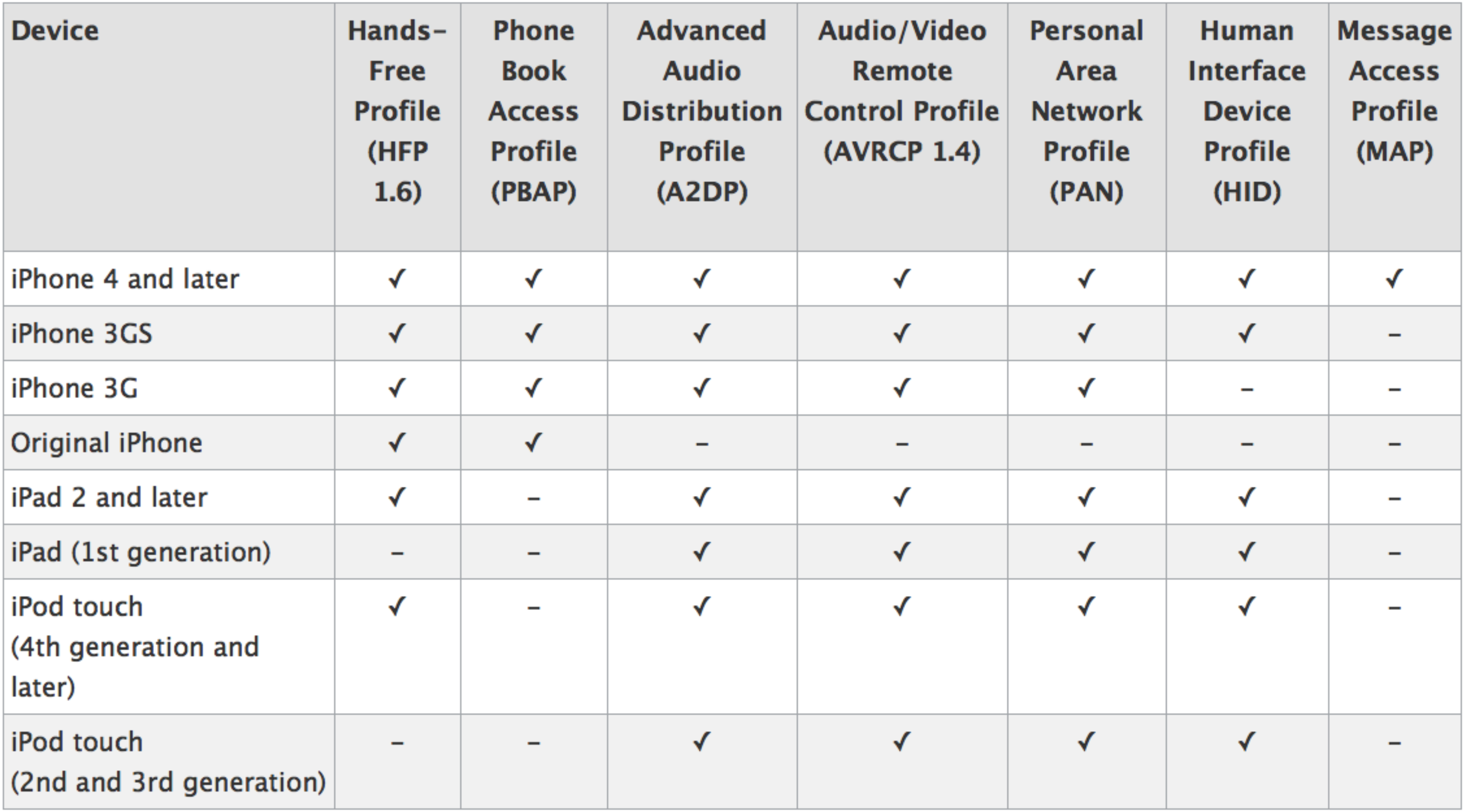
- ❑ Vertical slice through the protocol stack
- ❑ Basis for interoperability

- ❑ 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



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

Example use of Bluetooth Profiles



Device	Hands-Free Profile (HFP 1.6)	Phone Book Access Profile (PBAP)	Advanced Audio Distribution Profile (A2DP)	Audio/Video Remote Control Profile (AVRCP 1.4)	Personal Area Network Profile (PAN)	Human Interface Device Profile (HID)	Message Access Profile (MAP)
iPhone 4 and later	✓	✓	✓	✓	✓	✓	✓
iPhone 3GS	✓	✓	✓	✓	✓	✓	–
iPhone 3G	✓	✓	✓	✓	✓	–	–
Original iPhone	✓	✓	–	–	–	–	–
iPad 2 and later	✓	–	✓	✓	✓	✓	–
iPad (1st generation)	–	–	✓	✓	✓	✓	–
iPod touch (4th generation and later)	✓	–	✓	✓	✓	✓	–
iPod touch (2nd and 3rd generation)	–	–	✓	✓	✓	✓	–

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): variable bitrates, retransmission for SCO
- ❑ Faster connection & discovery
- ❑ AFH (adaptive frequency hopping) to avoid interference

Bluetooth 2.0 + EDR (2004, no more IEEE)

- ❑ EDR (enhanced date rate) of 3.0 Mbit/s (2.1 Mbit/s net) for ACL and eSCO using higher order modulation (GPSK → DQPSK / 8DPSK)
- ❑ lower power consumption due to shorter duty cycle

Bluetooth 2.1 + EDR (2007)

- ❑ better pairing support, e.g. using NFC
- ❑ improved security

Bluetooth 3.0 + HS (2009)

- ❑ Bluetooth 2.1 + EDR + IEEE 802.11a/g = 54 Mbit/s

Bluetooth 4.0 (2010)

- ❑ Classic Bluetooth + Bluetooth HS + Bluetooth Low Energy

Bluetooth 4.1 (2013)

Outline of Lecture 10

- ❑ Bluetooth
  - ❑ General characteristics
  - ❑ Piconets & scatternets
  - ❑ Basic Access scheme
  - ❑ Baseband (MAC layer)
  - ❑ Higher layer protocols
  - ❑ Profiles and Versions

- ❑ Zigbee
  - ❑ Zigbee vs. IEEE 802.15.4
  - ❑ Architecture & Topologies
  - ❑ IEEE 802.15.4 MAC layer

Zigbee / IEEE 802.15-4 Background

- Low-Rate, Very Low-Power
- IEEE 802.15.4 for PHY and MAC
- Zigbee specifies higher layers

  - ❑ Low data rate solution with multi-month to multi-year battery life
  - ❑ very low complexity
  - ❑ range 10 - 75 meter
  - ❑ Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation

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

- about 15 promoters, 133 participants, 111 adopters
- must be member to commercially use ZigBee spec

ZigBee platforms comprise

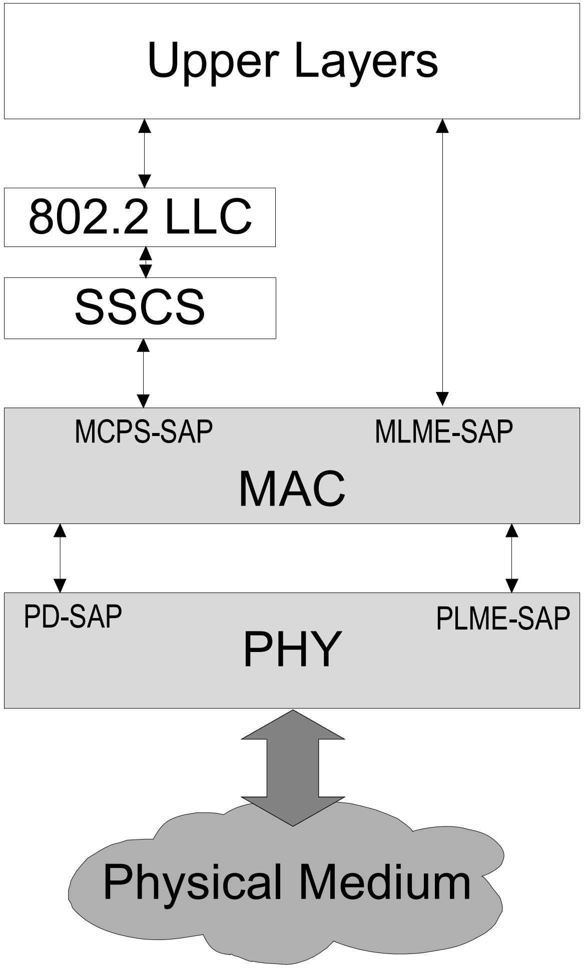
- IEEE 802.15.4 for layers 1 and 2
- ZigBee protocol stack up to the applications

ZigBee™ Alliance
Wireless Control That Simply Works

802.15.4 Characteristics

- 16 channels in the 2.4 GHz ISM band (worldwide), 30 (was 10) channels in the 915 MHz US ISM band and 1 channel in the European 868 MHz band
- Various Physical Layers
- Data rates of 20-250 kbit/s, latency down to 15 ms
- Data packets up to 127 bytes
- Master-Slave or Peer-to-Peer operation
- Up to 254 devices or 64516 simpler nodes
- CSMA/CA channel access, slotted (beacon) or unslotted
- Automatic network establishment
  by a PAN (Personal Area Network) coordinator

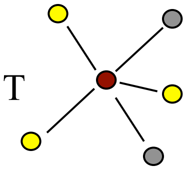
IEEE 802.15.4 Architecture



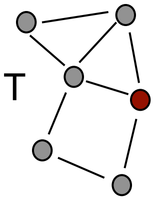
IEEE 802.15.4 Topologies

Topologies:

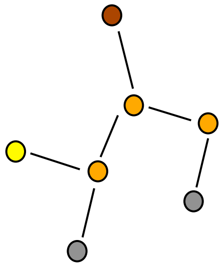
Star N.T

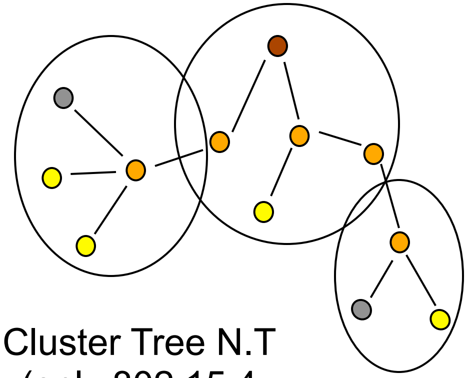


Mesh N.T



Tree N.T





Cluster Tree N.T
(only 802.15.4,
not Zigbee)

● **R**educed **F**unction **D**evice

● **F**ull **F**unction **D**evice (FFD)

● **Router** (role of FFD)

● **PAN** Coordinator
(role of FFD)

Modes of operation:

- Beacon-enabled
- Non-beacon-enabled

MAC frames

- ❑ Beacon-enabled : 4 frame types
  - Beacon frame
  - Data frame
  - Acknowledgment frame
  - MAC command frame
- ❑ Non-beacon-enabled : 2 frame types
  - Data frame
  - Acknowledgment frame

IEEE 802.15.4 Basic MAC characteristics

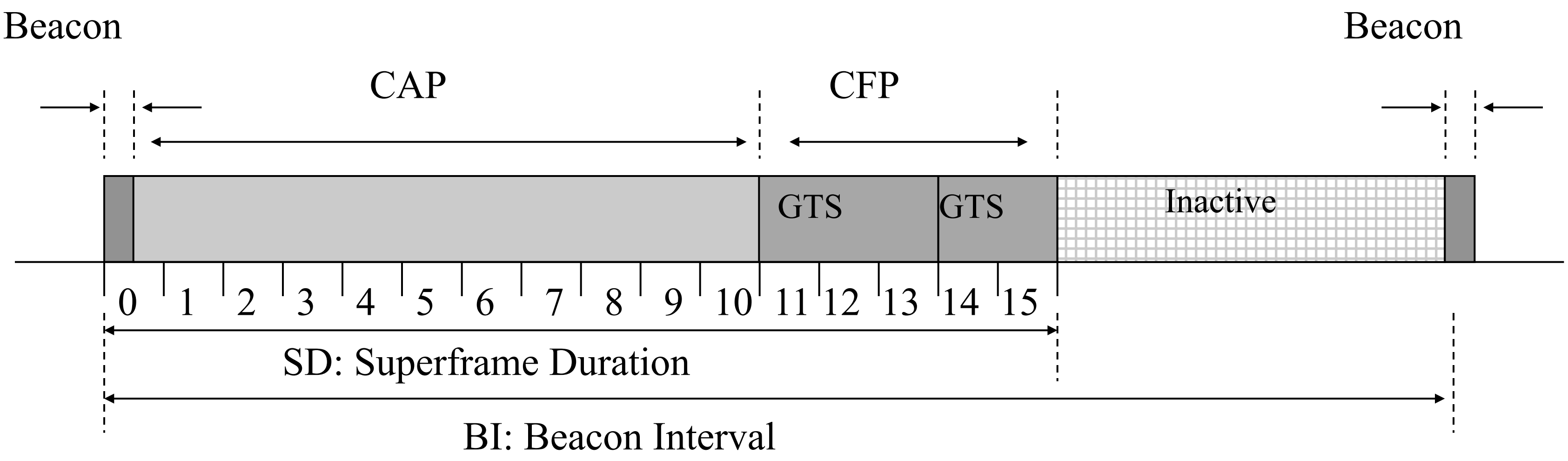
Beacon-enabled networks (star / tree):

- ❑ use of a superframe structure based on beacons
- ❑ slotted CSMA-CA
- ❑ Guaranteed time slots (GTS) in a (contention-free period) for time critical applications
- ❑ allows for low duty cycle operation
- ❑ beacon interval can range from 15 ms to 786 s

Non-beacon enabled networks (only peer-to-peer):

- ❑ no coordinator
- ❑ (Un-slotted) CSMA-CA

IEEE 802.15.4 Beacon-enabled MAC



CAP: **C**ontention **A**ccess **P**eriod

CFP: **C**ontention **F**ree **P**eriod