Prof. Dr.-Ing Jochen H. Schiller
Inst. of Computer Science
Freie Universität Berlin
Germany

Mobile Communications
Chapter 5: Wireless LANs

- Characteristics
- IEEE 802.11 (PHY, MAC, Roaming, .11a, b, g, h, i, n … z, ac, ad, …, ax, ay, az, ba, bb, …)
- Bluetooth / BLE / IEEE 802.15.x / ZigBee
- IEEE 802.16/.19/.20/.21/.22
- Comparison

Mobile Communication Technology according to IEEE (examples)

WiFi

Local wireless networks
WLAN 802.11

802.11a → 802.11h
802.11i/e/…/n/…/z/az/ba/bb…
802.11b → 802.11g

(see: http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm)

ZigBee

Personal wireless nw
WPAN 802.15

802.15.4 → 802.15.4a/b/c/d/e/f/g…y/z
802.15.5, .6 (WBAN), .7, .8, .10… .15
802.15.3 → 802.15.3b/c/d/e/f
802.15.2
802.15.1
Bluetooth

(see: http://www.ieee802.org/15/)

Wireless distribution networks
WMAN 802.16 (Broadband Wireless Access) WiMAX

+ Mobility
[hist.: 802.20 (Mobile Broadband Wireless Access)]
802.16e (addition to .16 for mobile devices)

Characteristics of wireless LANs

Advantages

- very flexible within the transmission area
- ad-hoc networks without previous planning possible
- (almost) no wiring difficulties (e.g. historic buildings, firewalls)
- more robust against disasters like, e.g., earthquakes, fires - or users pulling a plug...

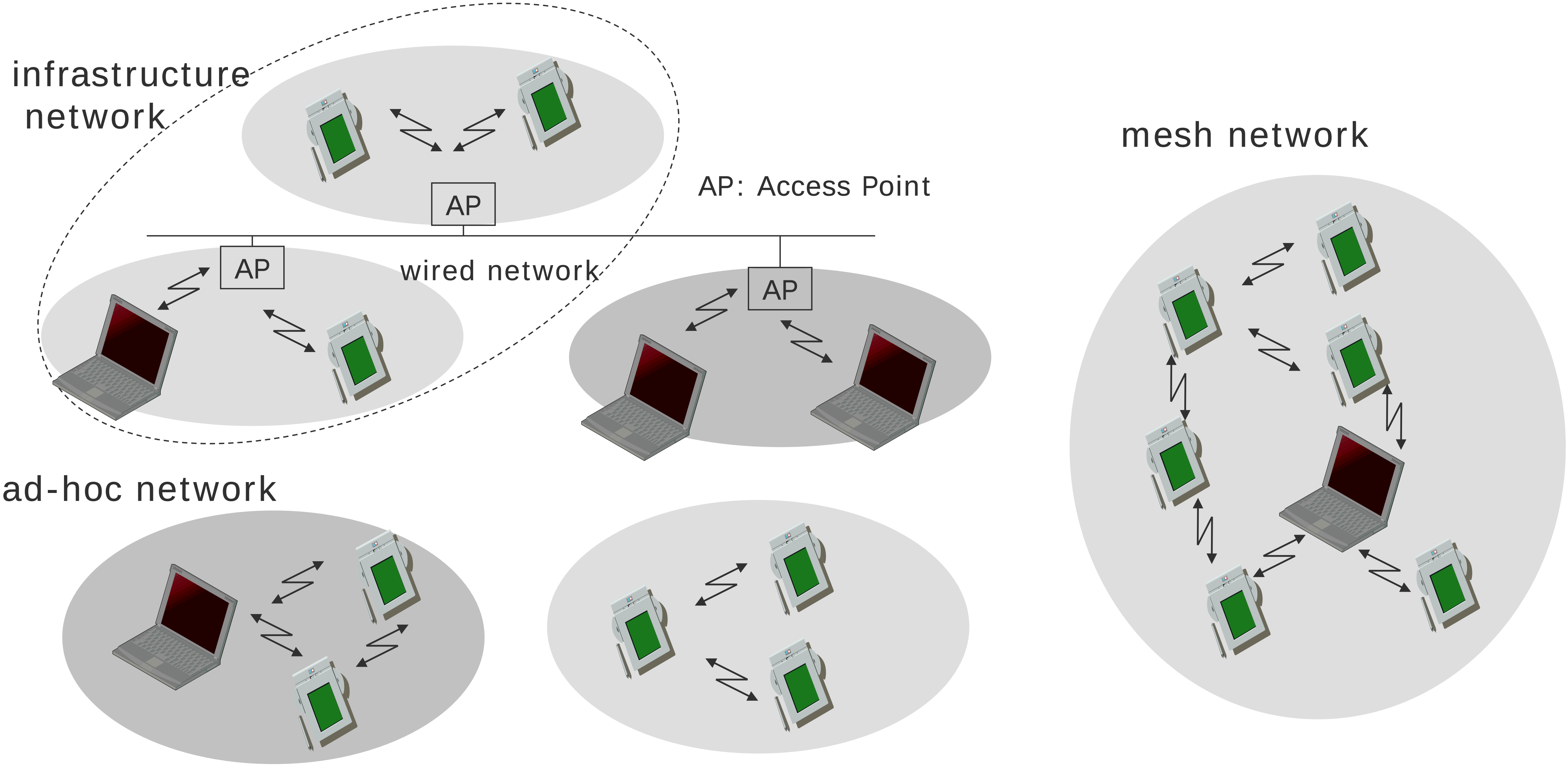
Disadvantages

- typically lower user data rates/higher delays and delay jitter compared to wired networks due to shared medium, lots of interference (it depends on your neighbors!)
- different/proprietary solutions, especially for higher bit-rates or low-power, standards take their time, devices have to fall back to older/standard solutions
- products have to follow many national restrictions if working wireless, it takes longer time to establish global solutions

Design goals for wireless LANs

- global, seamless operation
- low power for battery use
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks
- security (no one should be able to read my data), privacy (no one should be able to collect user profiles), safety (low radiation)
- transparency concerning applications and higher layer protocols, but also location awareness if necessary
- …

Comparison: infrastructure vs. ad-hoc vs. mesh networks



802.11 – Classical architecture of an infrastructure network

Station (STA)

- terminal with access mechanisms to the wireless medium and radio contact to the access point

Basic Service Set (BSS)

- group of stations using the same radio frequency

Access Point

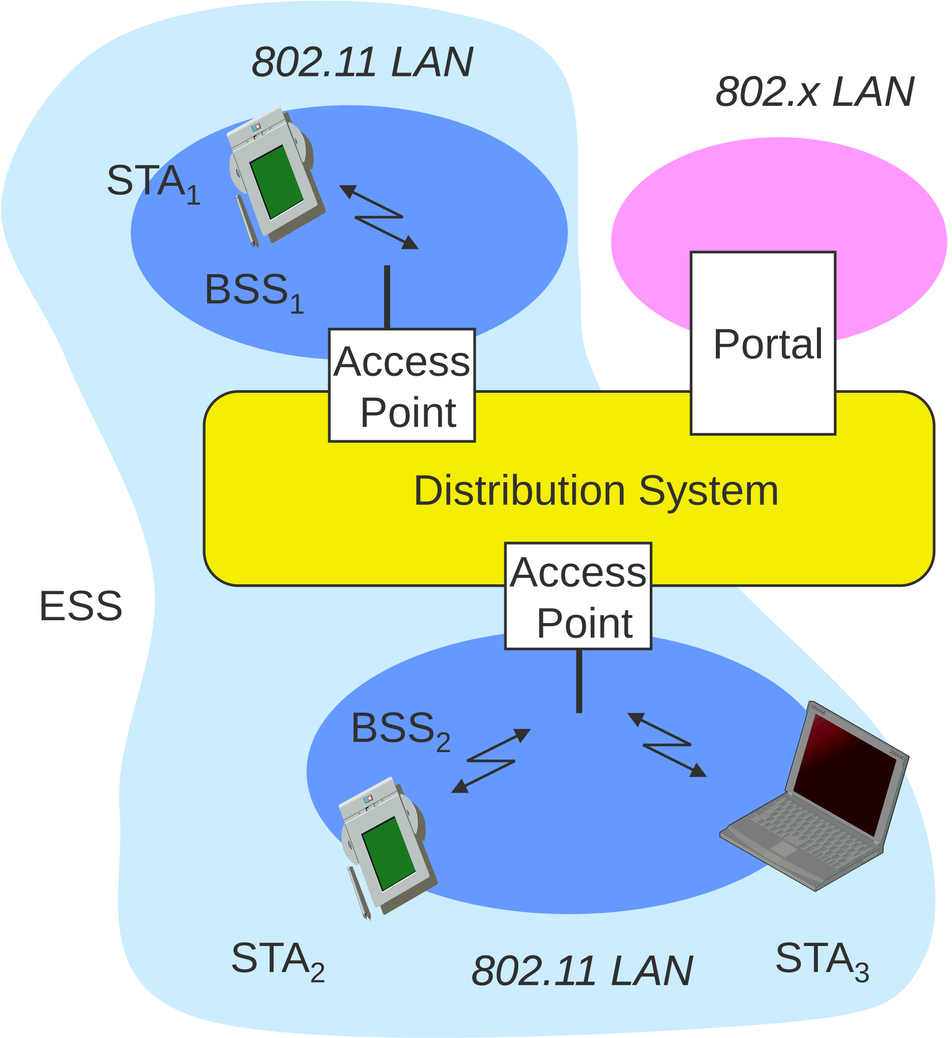
- station integrated into the wireless LAN and the distribution system

Portal

- bridge to other (wired) networks

Distribution System

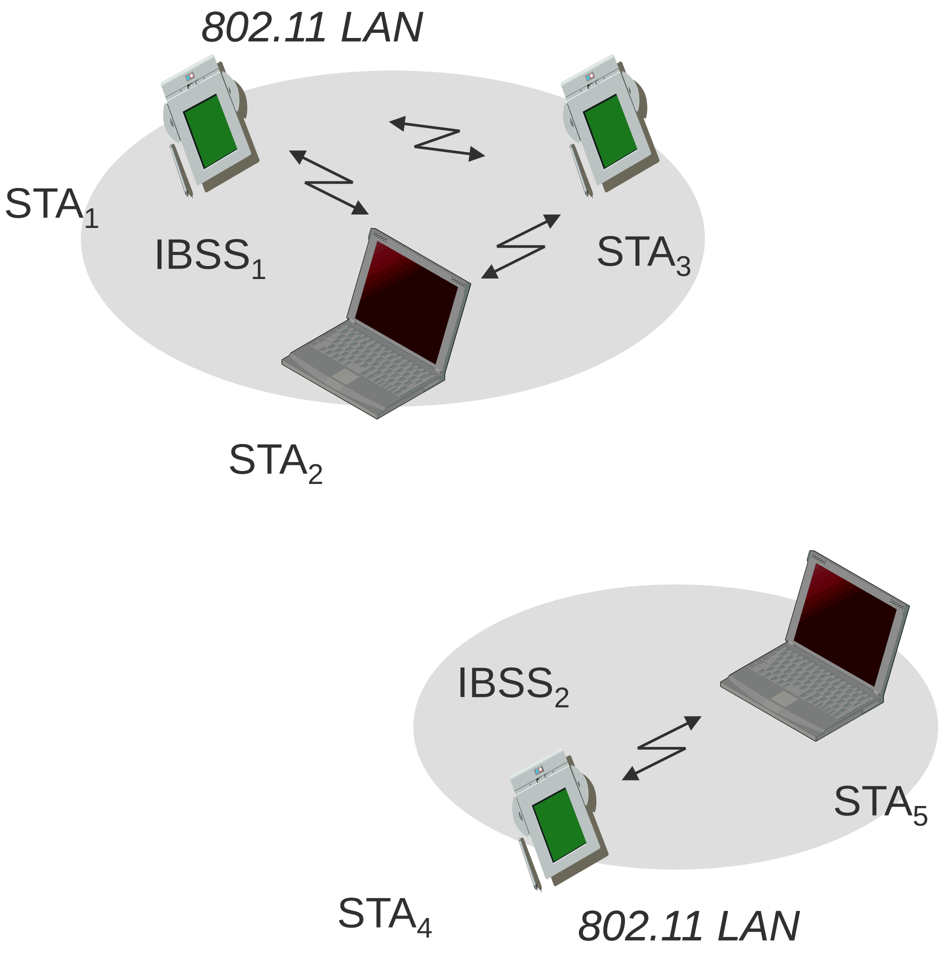
- interconnection network to form one logical network (EES: Extended Service Set) based on several BSS



802.11 - Architecture of an ad-hoc network

Direct communication within a limited range

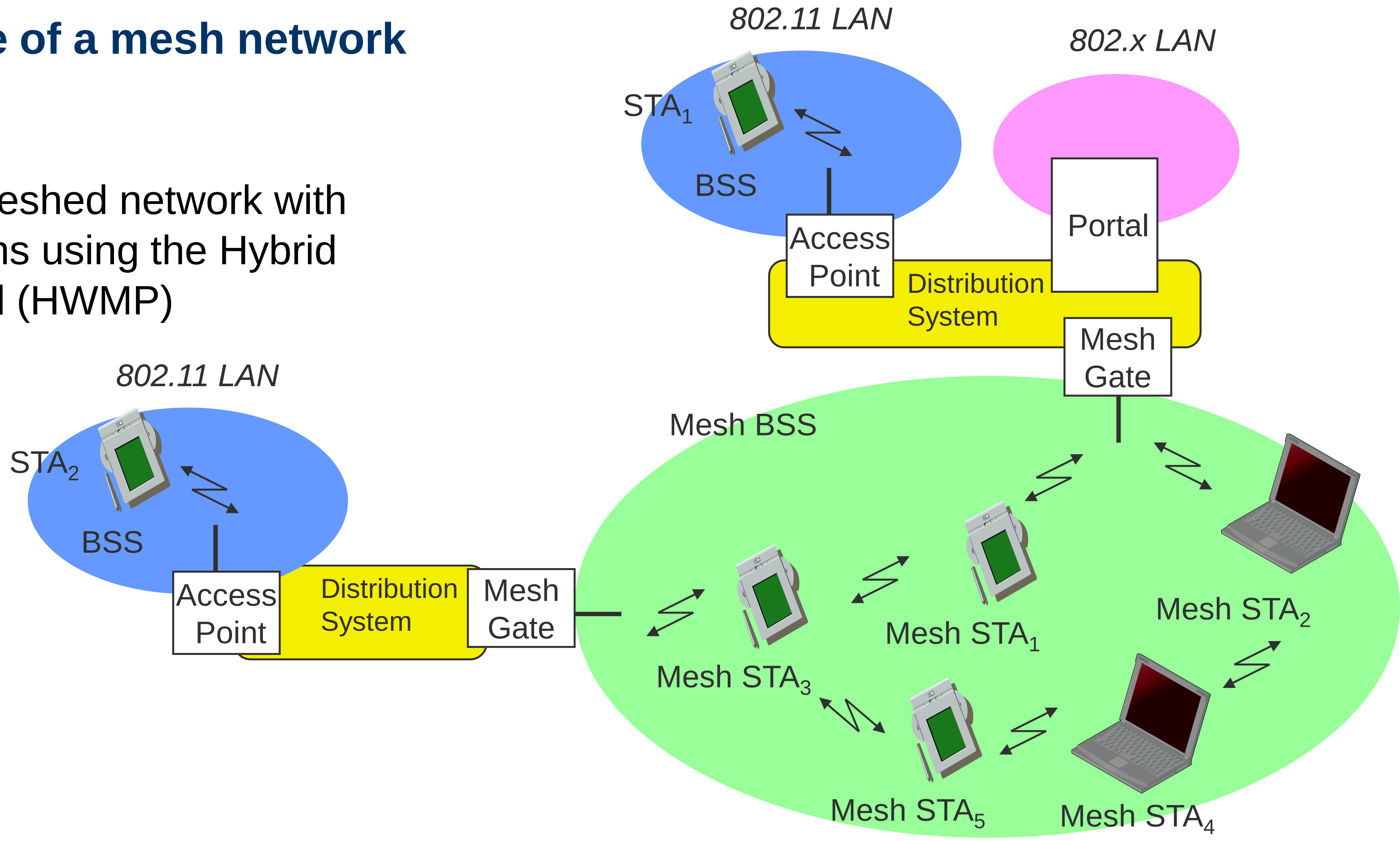
- Station (STA):
  terminal with access mechanisms to the wireless medium
- Independent Basic Service Set (IBSS):
  group of stations using the same radio frequency



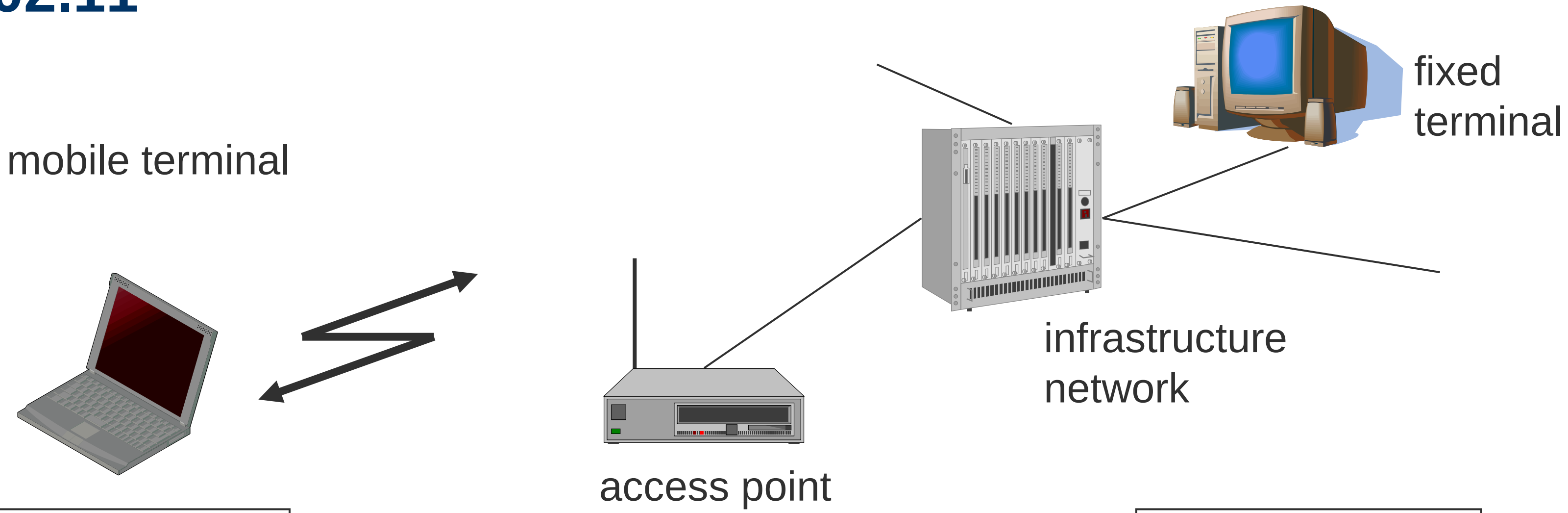
802.11 - Architecture of a mesh network

Mesh BSS forming a meshed network with possibly redundant paths using the Hybrid Wireless Mesh Protocol (HWMP)

Mesh Gate, AP and DS can be co-located in one device



IEEE standard 802.11

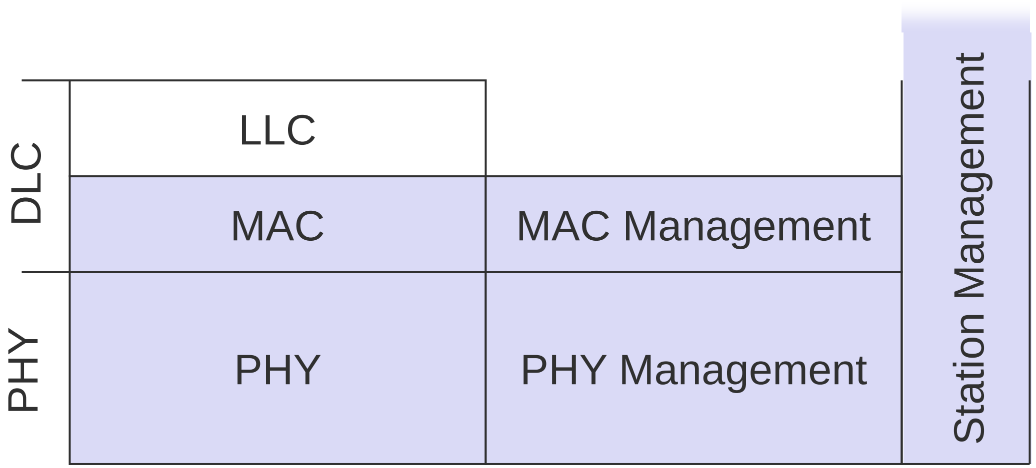


application			application
TCP			TCP
IP			IP
LLC	LLC		LLC
802.11 MAC	802.11 MAC	802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY	802.3 PHY	802.3 PHY

802.11 - Layers and functions

MAC
- access mechanisms, fragmentation, encryption

MAC Management
- synchronization, roaming, MIB, power management



PHY
- clear channel assessment (carrier sense)
- modulation, coding

PHY Management
- channel selection, MIB

Station Management
- coordination of all management functions

Questions & Tasks

- Check the relevant web pages – it is a very dynamic field!
- How is mobility restricted using WLANs? What additional elements are needed for roaming between networks, how and where can WLANs support roaming? In your answer, think of the capabilities of layer 2 where WLANs reside.
- What are the basic differences between wireless WANs and WLANs, and what are the common features? Consider mode of operation, administration, frequencies, capabilities of nodes, services, national/international regulations.

802.11 - Physical layer (historical – not in standard any longer)

3 versions: 2 radio (typ. 2.4 GHz), 1 IR
- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum) - obsolete
- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum) – many products
- DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
- preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- max. radiated power 1 W (USA), 100 mW (EU), min. 1mW

Infrared - obsolete
- 850-950 nm, diffuse light, typ. 10 m range
- carrier detection, energy detection, synchronization

DSSS PHY packet format (legacy)

Synchronization

- synch., gain setting, energy detection, frequency offset compensation

SFD (Start Frame Delimiter)

- 1111001110100000

Signal

- data rate of the payload (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)

Service

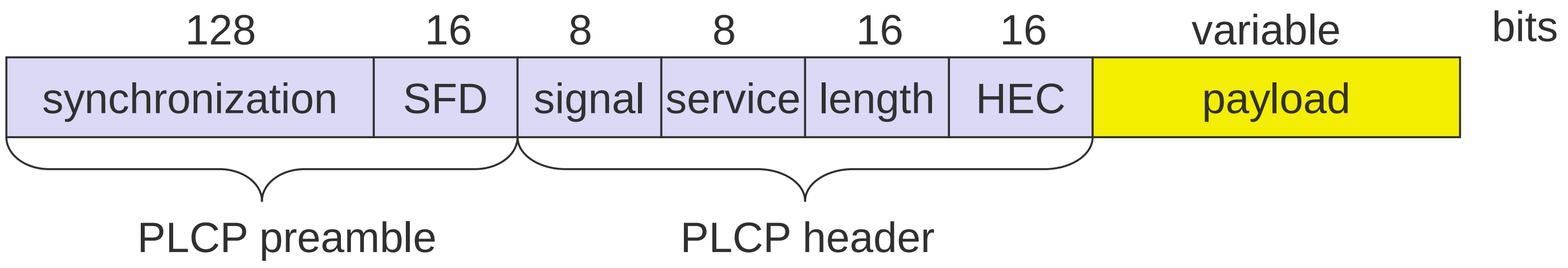
- future use, 00: 802.11 compliant

Length

- length of the payload

HEC (Header Error Check)

- protection of signal, service and length, $x^{16}+x^{12}+x^5+1$

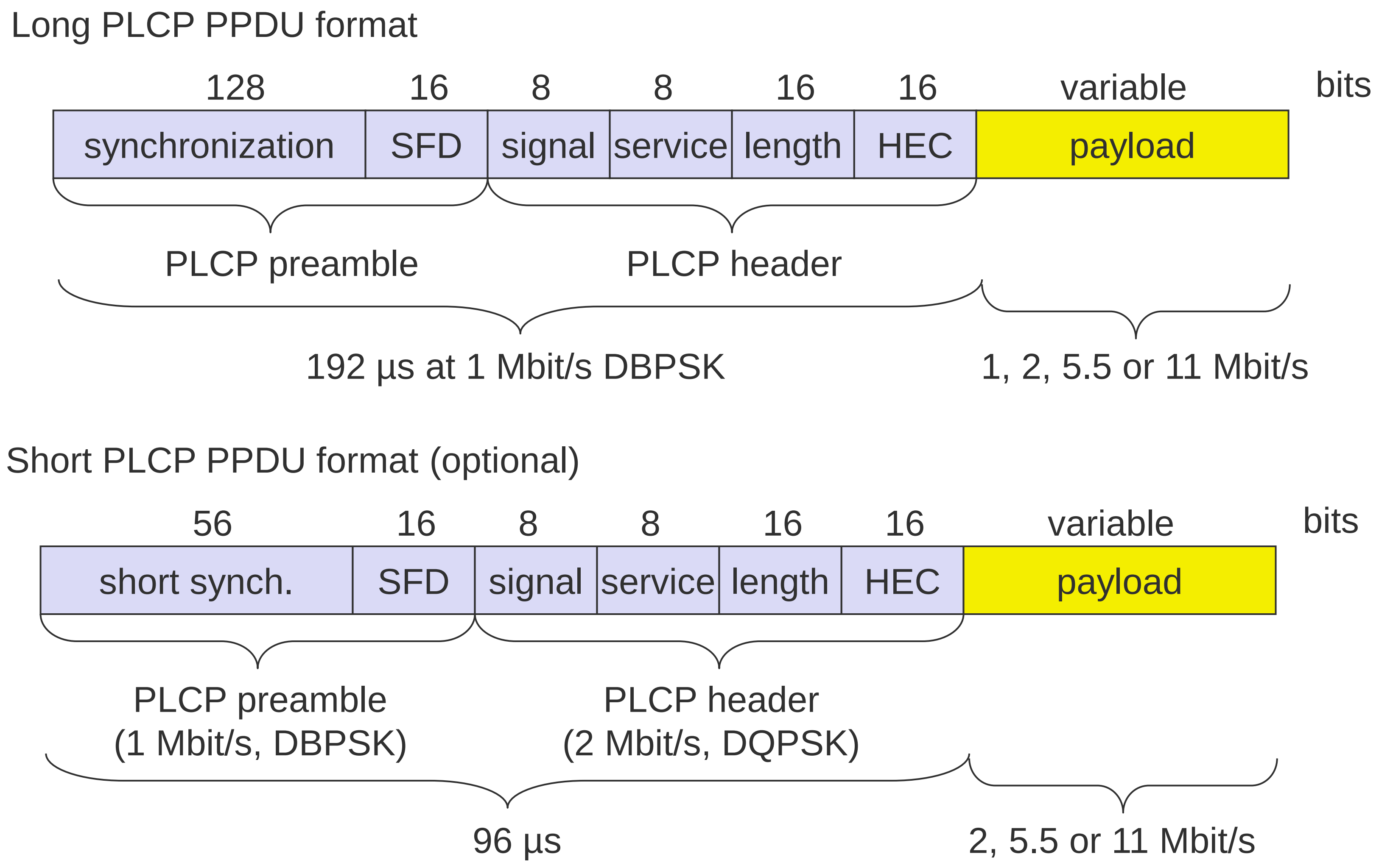


IEEE 802.11 HR/DSSS – PHY frame formats (was 802.11b)

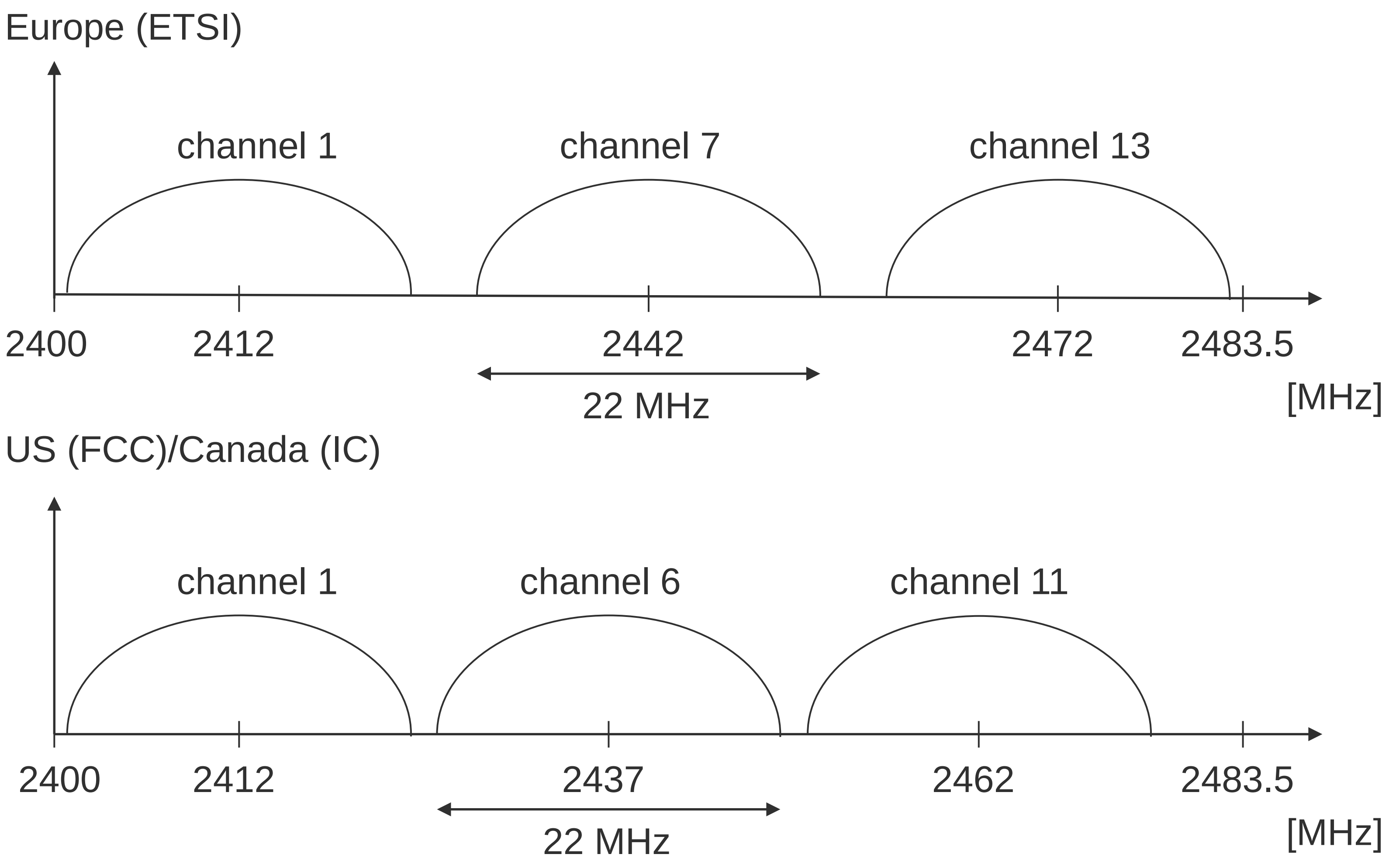
High Rate Direct Sequence Spread Spectrum @ 2.4GHz

Data rate

- 1, 2, 5.5, 11 Mbit/s, depending on SNR
- User data rate max. approx. 6 Mbit/s



Channel selection (non-overlapping)



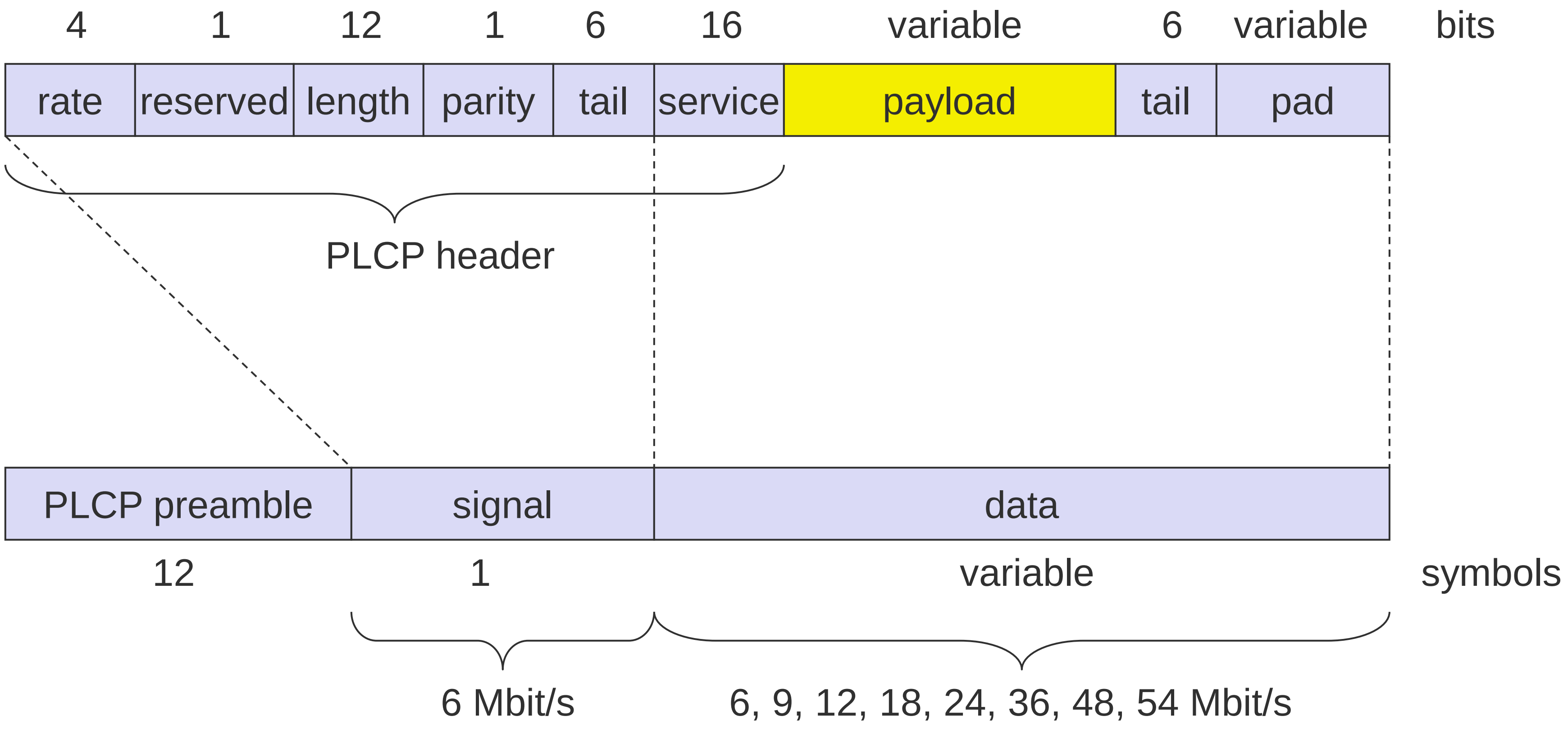
IEEE 802.11 OFDM – PHY frame format (was 802.11a)

Orthogonal Frequency Division Multiplexing @ 5GHz

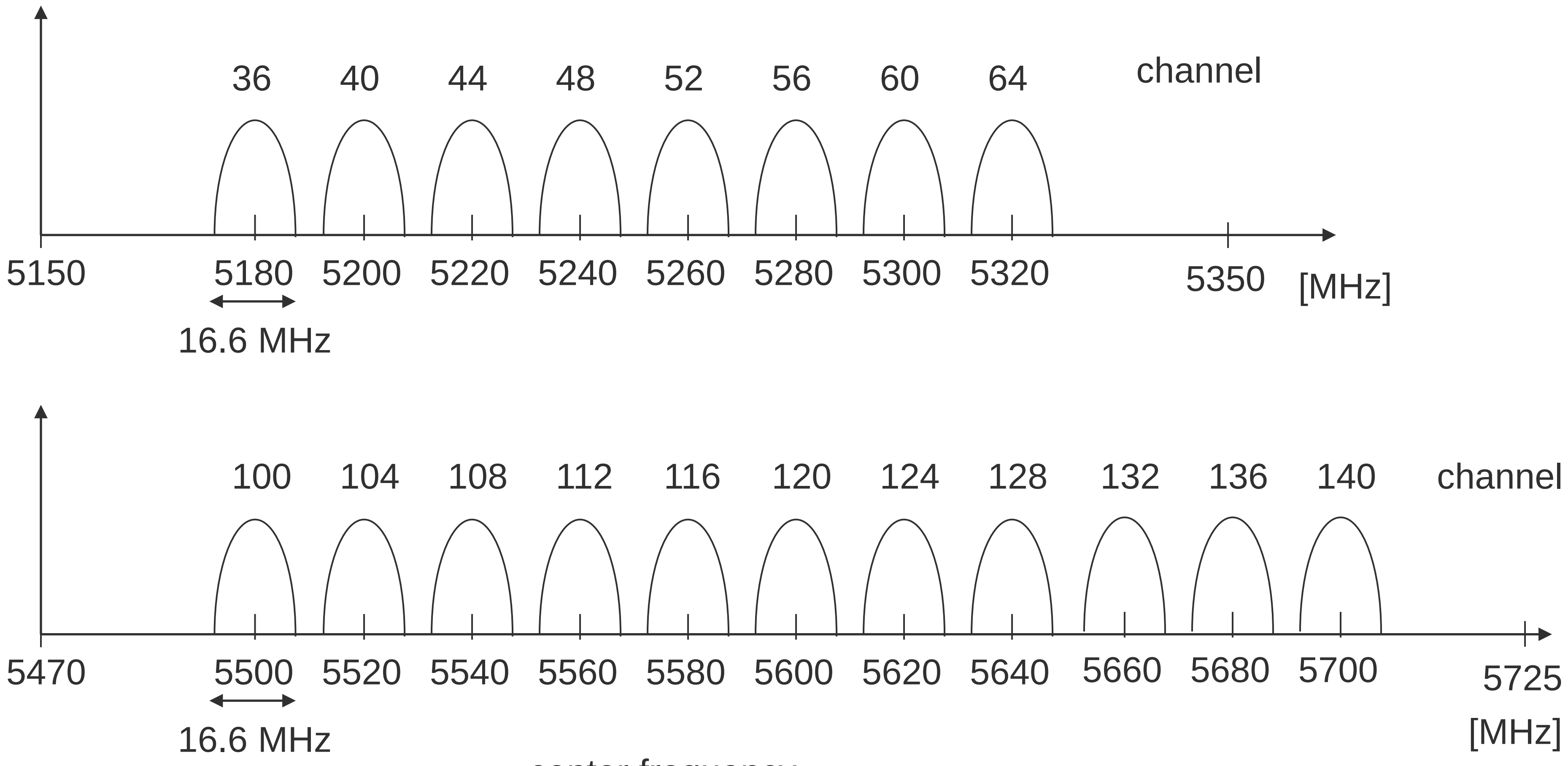
Data rates
- E.g. 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR and channel width
- User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
- 6, 12, 24 Mbit/s mandatory

Transmission range
- 100m outdoor, 10m indoor
  - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 18 up to 40 m, 12 up to 60 m

Frequency
- Free 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz ISM-band

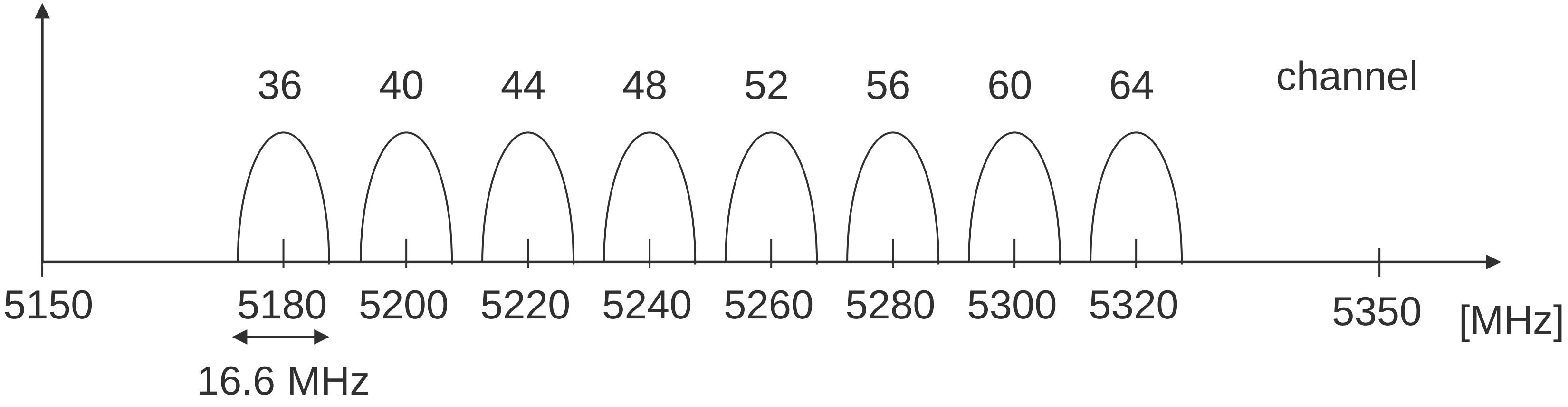


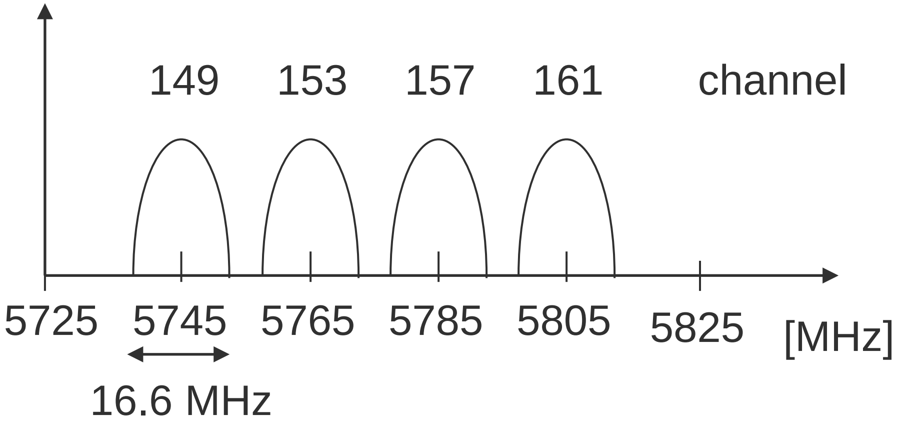
Operating channels of 802.11a in Europe (examples)



center frequency =
5000 + 5*channel number [MHz]

Operating channels for 802.11a / US U-NII (examples)



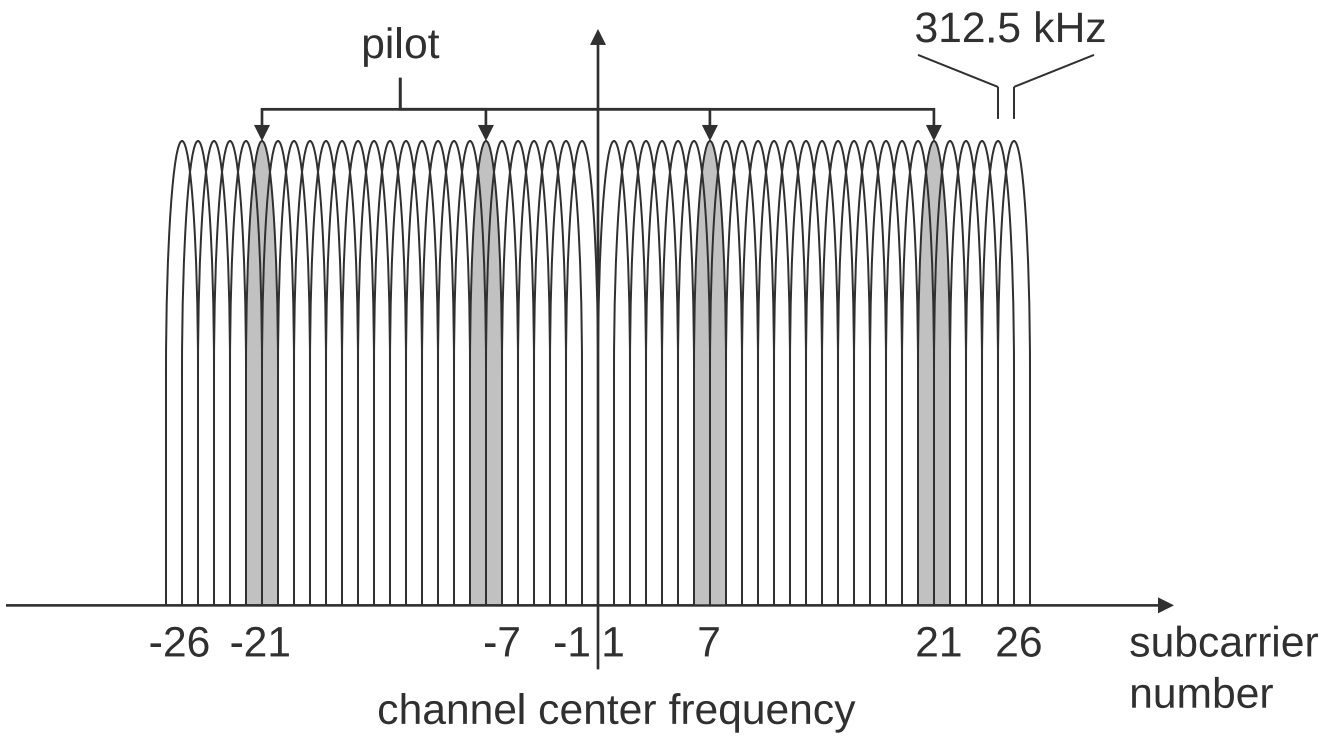


center frequency =
5000 + 5*channel number [MHz]

OFDM in IEEE 802.11

OFDM with 52 used subcarriers (64 in total)

- 48 data + 4 pilot
  - (plus 12 virtual subcarriers)
- 312.5 kHz spacing



IEEE 802.11 ERP – PHY frame formats (was 802.11g)

Extended Rate PHY @ 2.4GHz

Data rates

- Builds on classical 1, 2 Mbit/s (DSSS) and 1, 2, 5.5, 11 Mbit/s (HR DSSS)
- Uses additionally OFDM for 6, 9, 12, 18, 24, 36, 48, and 54 Mbit/s (thus check 802.11 OFDM for frame formats)

Many more options and modulation modes standardized but obsolete or deprecated.

Basically, it applies the old 802.11a @ 2.4 GHz.

IEEE 802.11 HT – PHY frame formats (was 802.11n) – marketed as WiFi 4

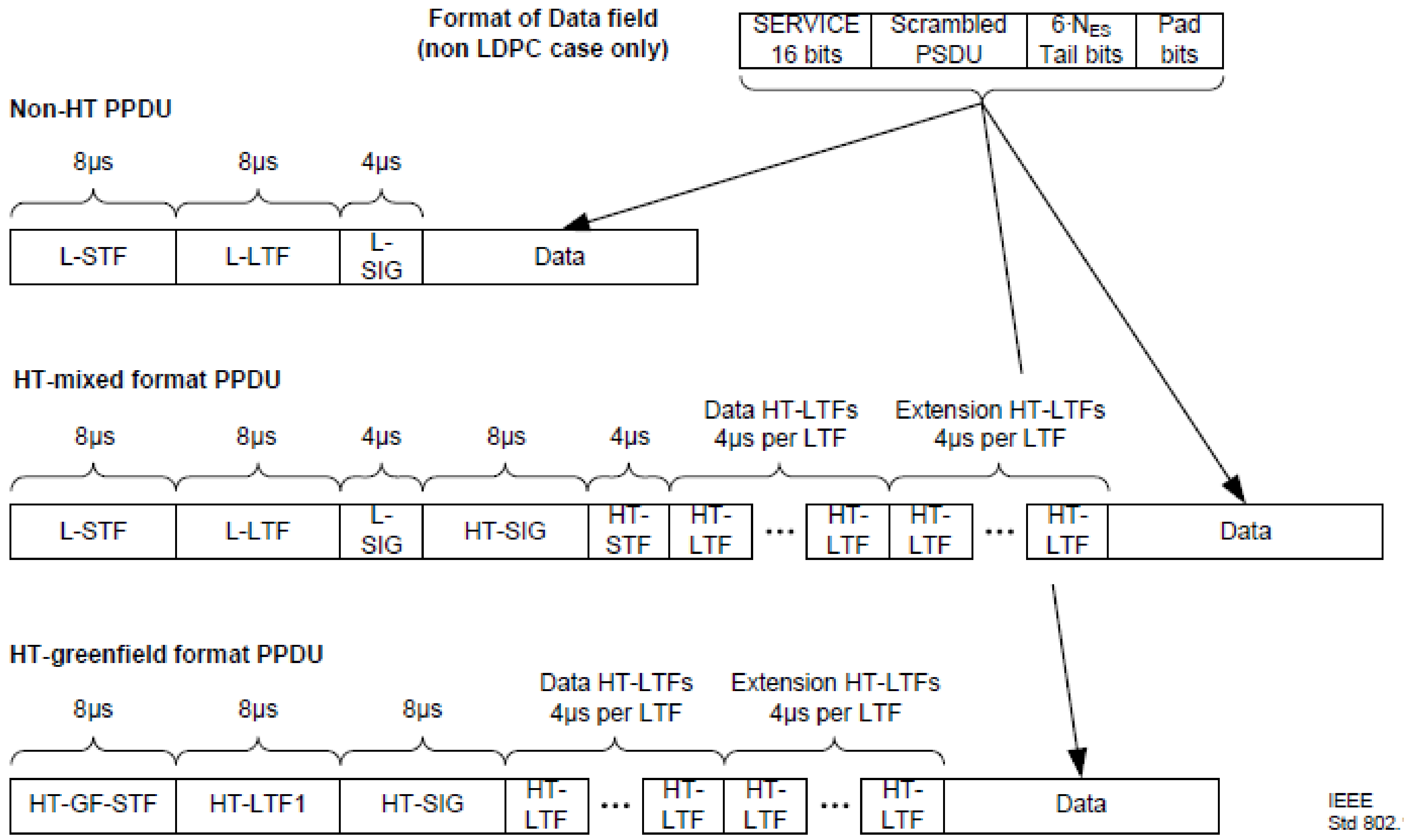
High Throughput (HT) Orthogonal Frequency Division Multiplexing (OFDM) system @ 2.4 and 5 GHz

Based on the OFDM system, but now using up to 4 spatial stream operating in 20 MHz bandwidth (additionally, 40 MHz bandwidth specified offering up to 600 Mbit/s)

Element	Description
L-STF	Non-HT Short Training field
L-LTF	Non-HT Long Training field
L-SIG	Non-HT SIGNAL field
HT-SIG	HT SIGNAL field
HT-STF	HT Short Training field
HT-GF-STF	HT-Greenfield Short Training field
HT-LTF1	First HT Long Training field (Data)
HT-LTFs	Additional HT Long Training fields (Data and Extension)
Data	The Data field includes the PSDU

IEEE
Std 802.11-2012

IEEE 802.11 HT – PHY frame formats (was 802.11n)



IEEE
Std 802.11-2012

Very High Throughput (VHT) PHY – uses OFDM (was 802.11ac)

8 µs	8 µs	4 µs	8 µs	4 µs	4 µs per VHT-LTF symbol	4 µs	
L-STF	L-LTF	L-SIG	VHT-SIG-A	VHT-STF	VHT-LTF	VHT-SIG-B	Data

VHT-MCS Index	Modulation	R	N_{BPSCS}	$N_{SD} \cdot N_{Seg}$	N_{SP}	N_{CBPS}	N_{DBPS}	N_{ES}	Data rate (Mb/s)	
									800 ns GI	400 ns GI
0	BPSK	1/2	1	468	16	3744	1872	1	468.0	520.0
1	QPSK	1/2	2	468	16	7488	3744	2	936.0	1040.0
2	QPSK	3/4	2	468	16	7488	5616	3	1404.0	1560.0
3	16-QAM	1/2	4	468	16	14 976	7488	4	1872.0	2080.0
4	16-QAM	3/4	4	468	16	14 976	11 232	6	2808.0	3120.0
5	64-QAM	2/3	6	468	16	22 464	14 976	8	3744.0	4160.0
6	64-QAM	3/4	6	468	16	22 464	16 848	8	4212.0	4680.0
7	64-QAM	5/6	6	468	16	22 464	18 720	9	4680.0	5200.0
8	256-QAM	3/4	8	468	16	29 952	22 464	12	5616.0	6240.0
9	256-QAM	5/6	8	468	16	29 952	24 960	12	6240.0	6933.3

Source: IEEE Std 802.11-2016

IEEE 802.11 VHT – High-speed for WLANs at 5 GHz – marketed as WiFi 5

Single link throughput > 500Mbit/s, multi-station > 1 Gbit/s

Bandwidth up to 160 MHz (80 MHz mandatory), up to 8x MIMO, up to 256 QAM, beamforming, SDMA via MIMO

Example home configuration:

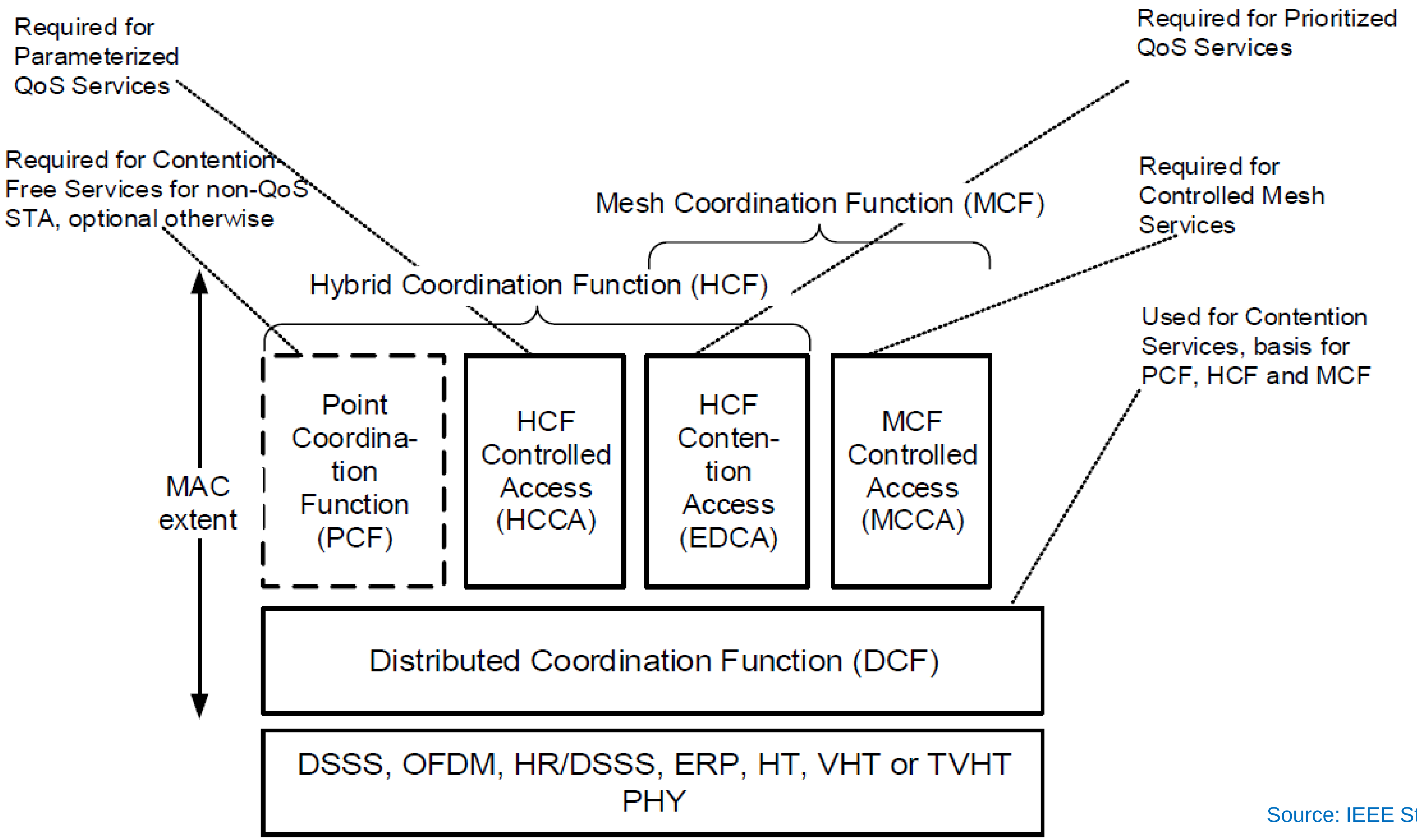
- 8-antenna access point, 160 MHz bandwidth, 6.77 Gbit/s
- 4-antenna digital TV, 3.39 Gbit/s
- 2-antenna tablet, 1.69 Gbit/s
- Two 1-antenna smartphones, 867 Mbit/s each

Redefinition of many protocol fields and procedures!

Questions & Tasks

- Why is the number of non-overlapping channels important?
- Why is the user throughput much lower than the max. available data rate at PHY?
- What are advantages of higher frequency bands? Disadvantages?
- How are higher data rates achieved?

802.11 - MAC layer architecture



Source: IEEE Std 802.11-2016

How to access the medium in 802.11

Distributed Coordination Function (DCF)

- Fundamental access method in 802.11, mandatory
- Also known as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
- Random backoff, certain fairness, refinement with RTS/CTS possible

Point Coordination Function (not really used, will be kicked out of the standard in the future)

- Contention free access, reservation of the medium

Hybrid Coordination Function (HCF)

- QoS support by combining DCF and PCF
- Contention-based channel access (Enhanced Distributed Channel Access, EDCA) and controlled channel access (HCF Controlled Channel Access, HCCA)
- Support of different priorities for, e.g., background, best effort, video, voice traffic (WiFi WMM Designations)

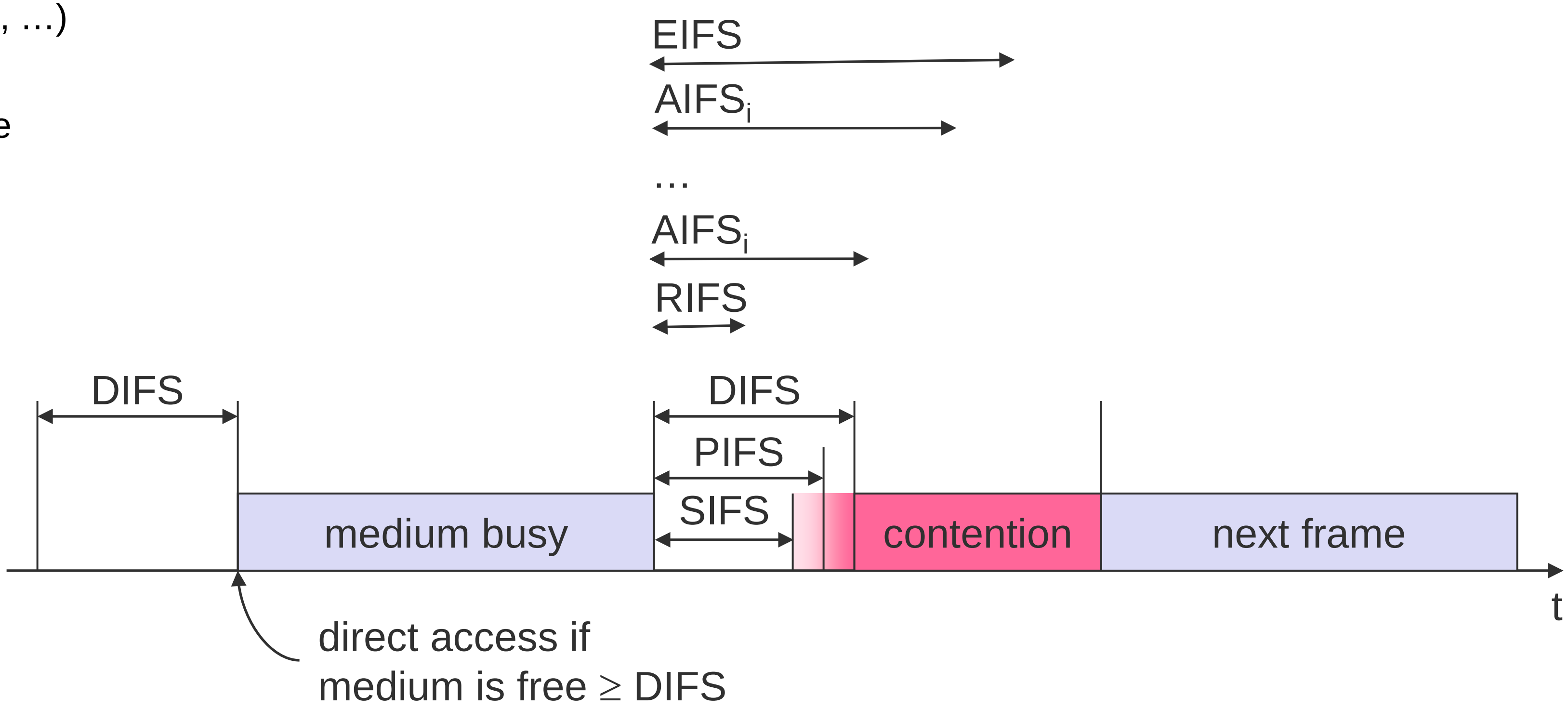
Mesh Coordination Function (MCF)

- Only in a MBSS, EDCA for contention-based access, MCCA (MCS Controlled Channel Access) for contention-free access

802.11 - MAC Inter Frame Space

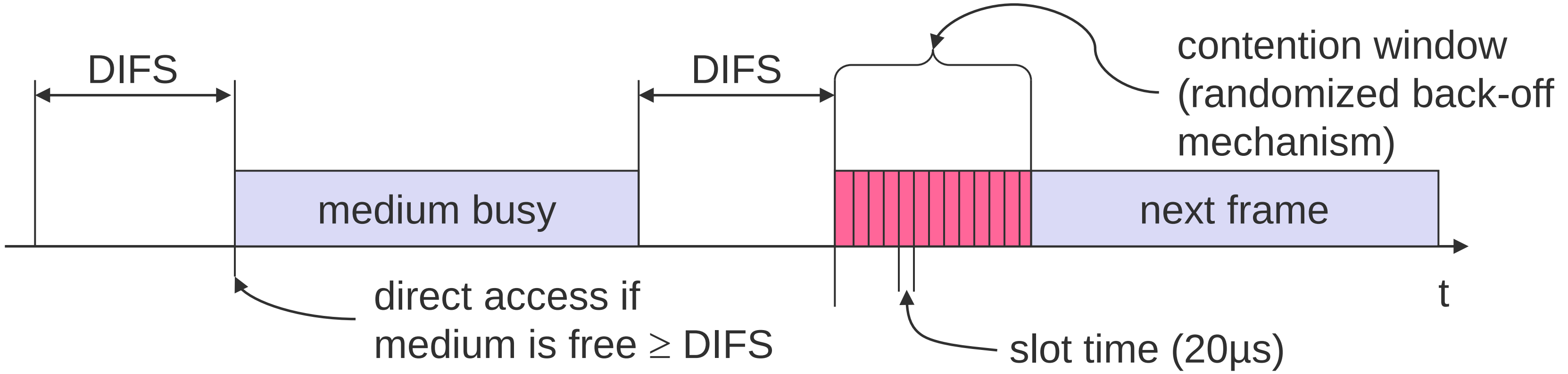
Priorities of packets defined through different inter frame spaces (not always guaranteed)

- RIFS (Reduced IFS)
  - shortest IFS, reduced overhead, only if no SIFS expected, for higher throughput
- **SIFS** (Short IFS)
  - for ACK, CTS, polling response
- PIFS (PCF IFS)
  - used to gain priority access (PCF, TIM, …)
- **DIFS** (DCF IFS)
  - for “normal” asynchronous data service
- AIFS (Arbitration IFS)
  - variable depending on QoS
- EIFS (Extended IFS)
  - IFS e.g. after an incorrect FCS
- Additional “beamforming” IFSs



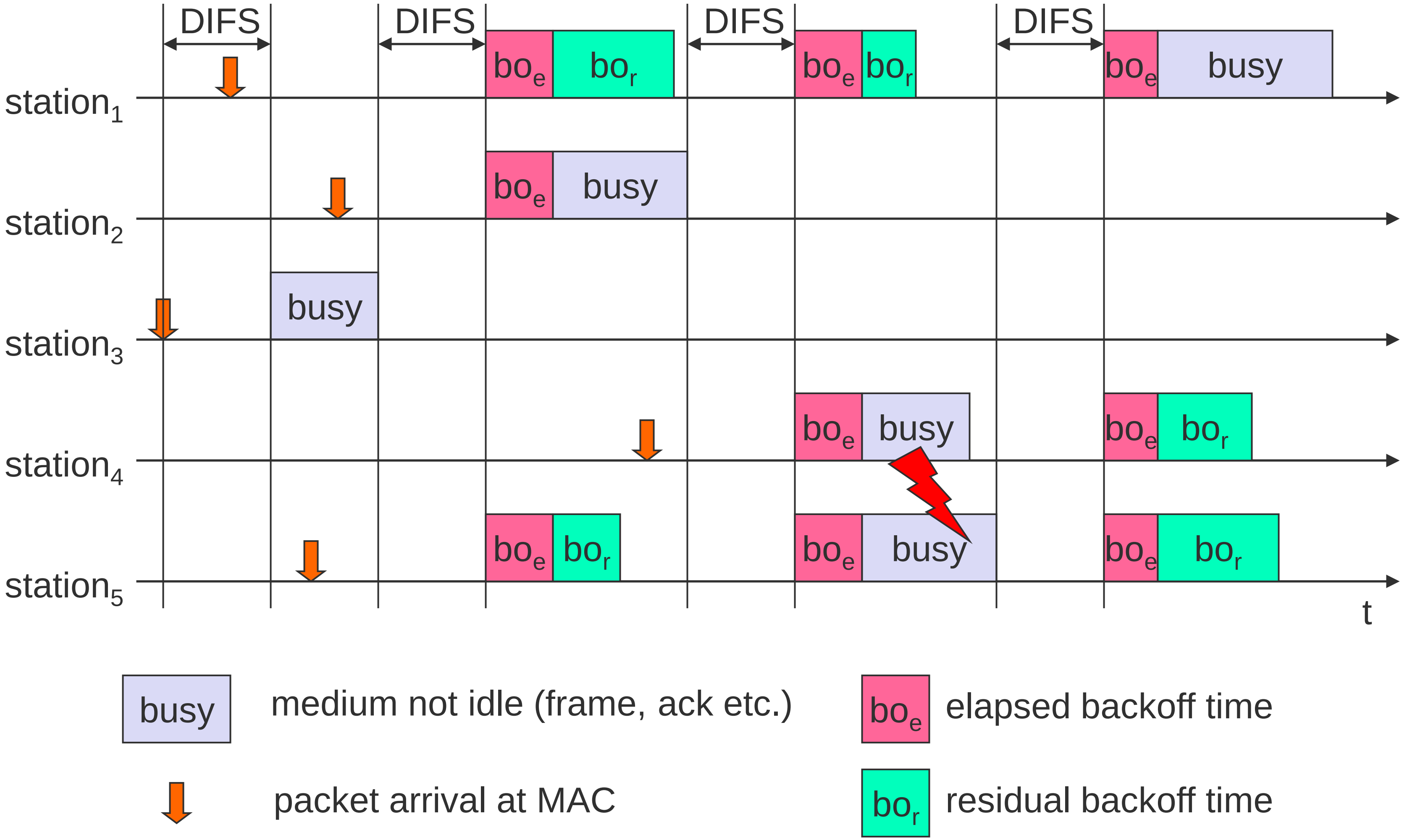
802.11 - CSMA/CA access method I

- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)



Freie Universität Berlin

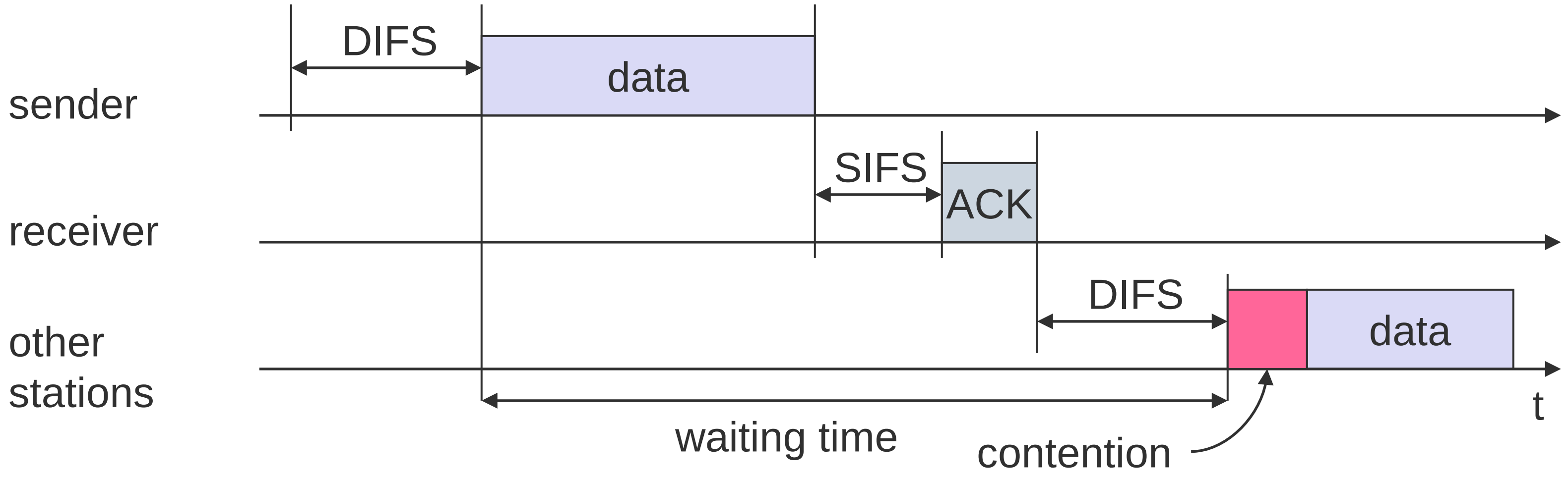
802.11 - Competing stations - simple version

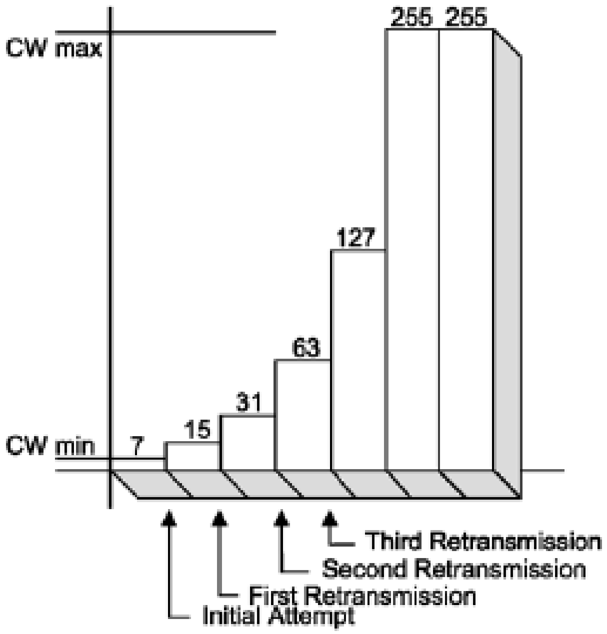


802.11 - CSMA/CA access method II

Sending unicast packets

- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (FCS)
- automatic retransmission of data packets in case of transmission errors, but exponential increase of contention window

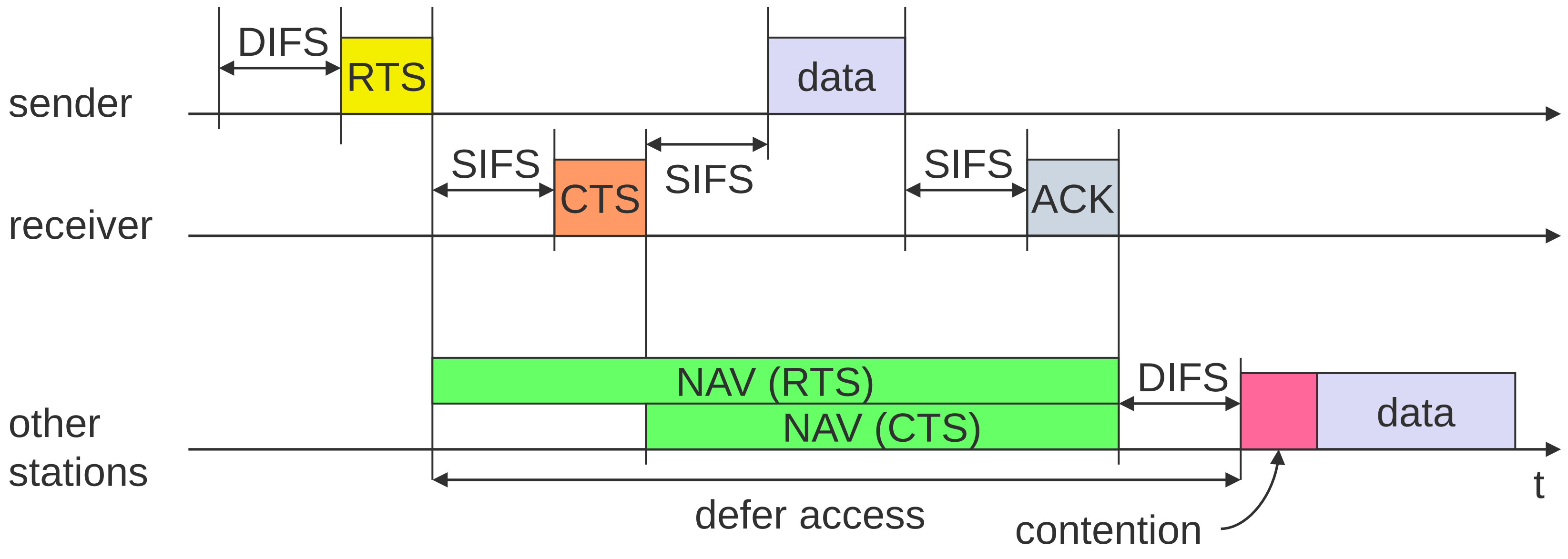




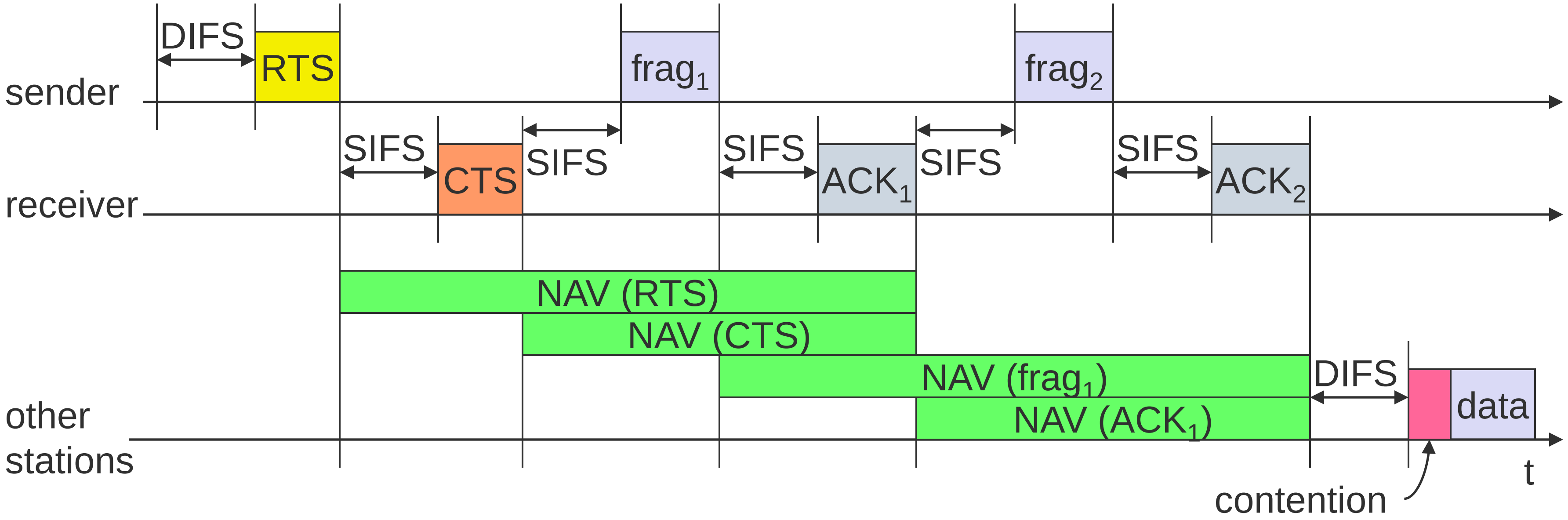
802.11 – DCF with RTS/CTS

Sending unicast packets

- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



Fragmentation



802.11 – MAC Frame format

Types
- control frames, management frames, data frames

Sequence numbers
- important against duplicated frames due to lost ACKs

Addresses
- receiver, transmitter (physical), BSS identifier, sender (logical)

Miscellaneous
- sending time, checksum, frame control, data

- Only the first three and the last field are present in all frames!

bytes	2	2	6	6	6	2	6	2	4	0-7951	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

bits	2	2	4	1	1	1	1	1	1	1	1
	Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	Protec-ted Frame	+HTC/ Order

MAC address format (examples)

Example scenario	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc network	0	0	RA=DA	TA=SA	BSSID	-
infrastructure network, from AP	0	1	RA=DA	TA=BSSID	SA	-
infrastructure network, to AP	1	0	RA=BSSID	TA=SA	DA	-
within mesh BSS	1	1	RA	TA	DA	SA

AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

Acknowledgement

ACK	Frame Control	Duration	Receiver Address	FCS
bytes	2	2	6	4

Request To Send

RTS	Frame Control	Duration	Receiver Address	Transmitter Address	FCS
bytes	2	2	6	6	4

Clear To Send

CTS	Frame Control	Duration	Receiver Address	FCS
bytes	2	2	6	4

Questions & Tasks

- Why is it difficult to guarantee QoS at MAC layer?
- How does 802.11 prioritize different packets?
- What is the behavior of the basic access method under no/light/heavy load?
- How is fairness implemented?
- Why is the contention window mechanism unfair?
- What is the idea of the NAV?
- How is the problem with hidden/exposed stations solved?

802.11 - MAC management

Synchronization

- try to find a LAN, try to stay within a LAN
- timer etc.

Power management

- sleep-mode without missing a message
- periodic sleep, frame buffering, traffic measurements

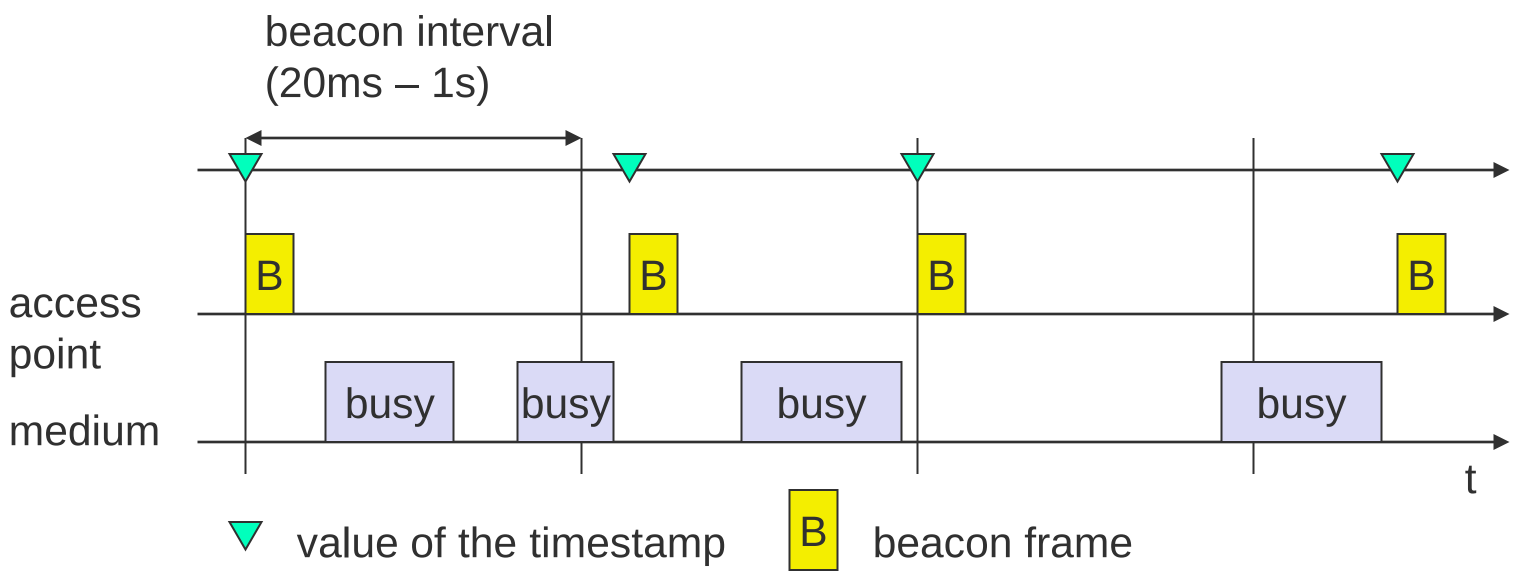
Association/Reassociation

- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

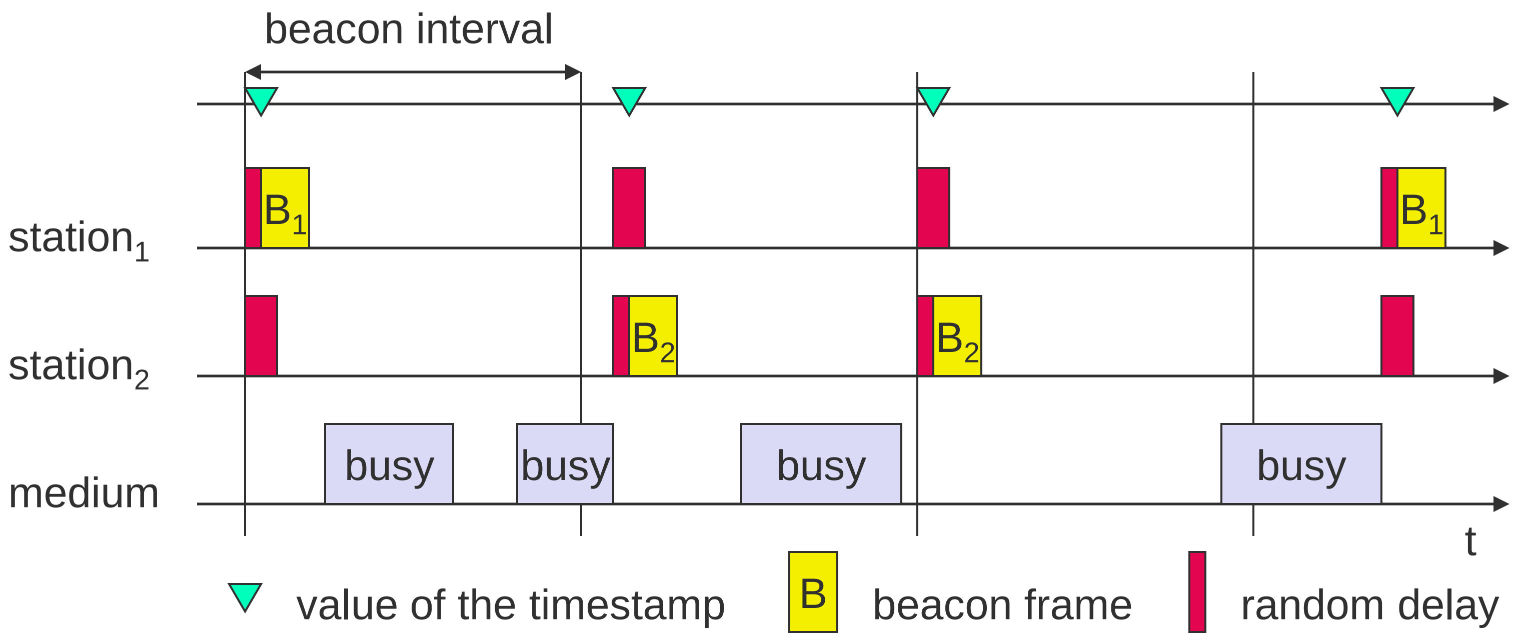
MIB - Management Information Base

- managing, read, write

Synchronization using a Beacon (infrastructure)



Synchronization using a Beacon (ad-hoc)



Power management

Idea: switch the transceiver off if not needed

- States of a station: sleep and awake

Timing Synchronization Function (TSF)

- stations wake up at the same time

Infrastructure

- Traffic Indication Map (TIM)
  - list of unicast receivers transmitted by AP
- Delivery Traffic Indication Map (DTIM)
  - list of broadcast/multicast receivers transmitted by AP

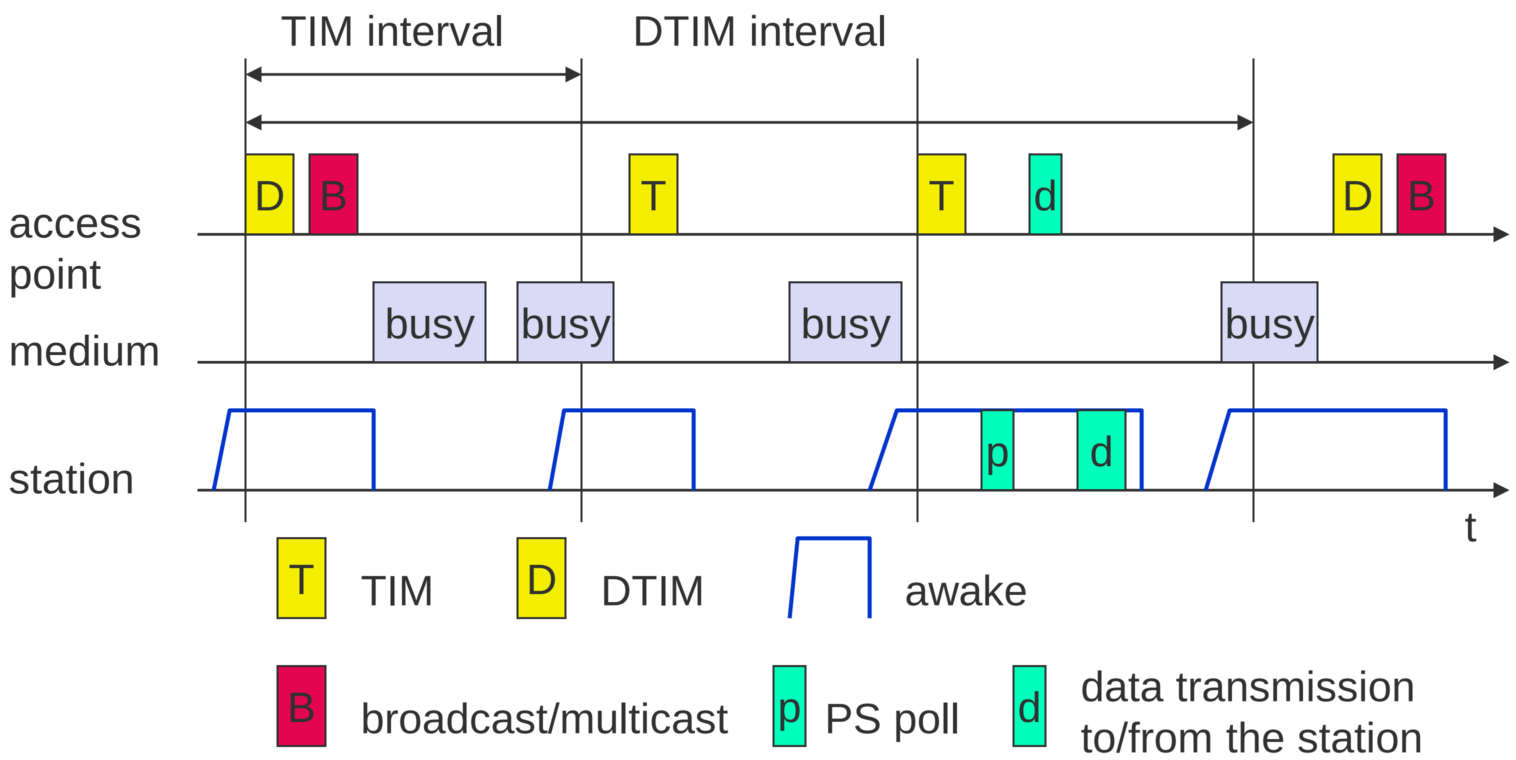
Ad-hoc

- Ad-hoc Traffic Indication Map (ATIM)
  - announcement of receivers by stations buffering frames
  - more complicated - no central AP
  - collision of ATIMs possible (scalability?)

APSD (Automatic Power Save Delivery)

- more efficient method in 802.11e replacing above schemes offering scheduled (S-APSD) and unscheduled service periods (U-APSD)

Power saving with wake-up patterns (infrastructure)



U-APSD – WMM Power Save

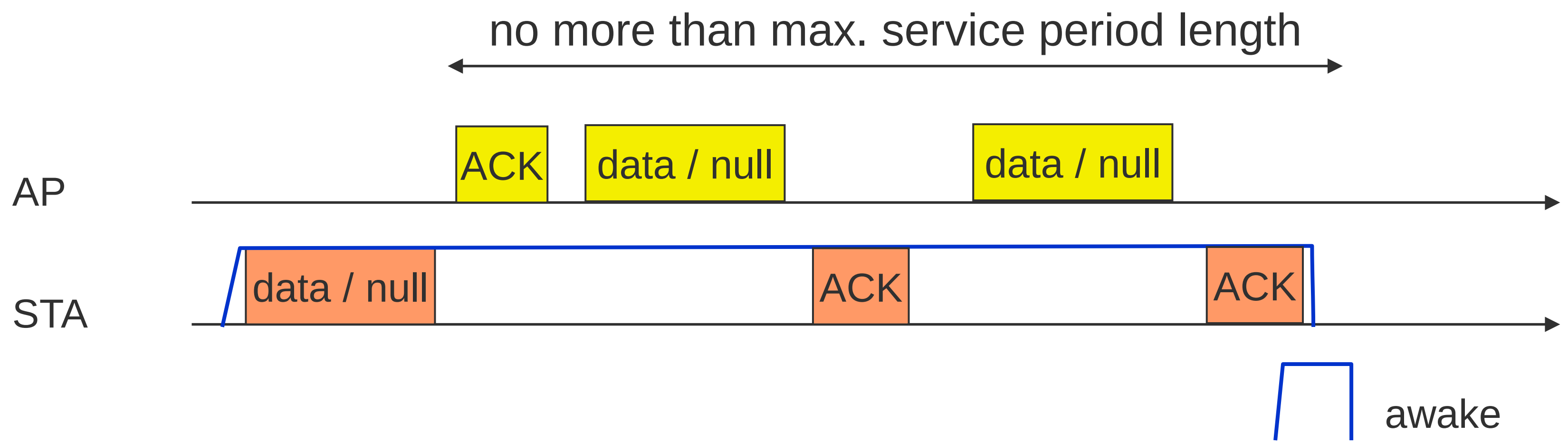
Procedure for unicast data delivered to a STA in PS mode

STA triggers release of buffered data from AP

WMM Power Save based on legacy procedures plus optional U-APSD

Advantages:

- No more polling needed
- Downlink data frames sent together in a fast sequence
- Trigger frame may already contain data – ideal e.g. for VoIP
- Applications specify PS behavior, i.e. sleep period



802.11 - Roaming

No or bad connection? Then perform:

Scanning

- scan the environment, i.e., listen into the medium for beacon signals or send probes into the medium and wait for an answer

Reassociation Request

- station sends a request to one or several AP(s)

Reassociation Response

- success: AP has answered, station can now participate
- failure: continue scanning

AP accepts Reassociation Request

- signal the new station to the distribution system
- the distribution system updates its data base (i.e., location information)
- typically, the distribution system now informs the old AP so it can release resources

May take a long time …

Faster roaming using 802.11k, .11r and .11v

Classical roaming is too slow, e.g., for VoIP over WLAN ➔ service interruption

1. 802.11 authentication message exchange
2. Reassociation messages exchange
3. EAP-request/response identity exchange
4. Access request and challenge packet exchange
5. EAP request/response
6. RADIUS access request/accept exchange
7. Success message to Client
8. Nonce-value exchange
9. Temporal key, acknowledgement exchange

In this example 17 steps (all but 7. are exchanges)!

- See 802.1X for more details about authentication

802.11k: Optimized channel list

- Collect potential roaming networks prior to roaming

802.11r: Fast BSS Transition - only 4 steps left

1. Client and AP exchange 802.11 authentication messages and nonce-values
2. Client and AP exchange reassociation messages and temporal key/acknowledgment

802.11v: BSS Transition Management

- Manage information about alternative access points
- Disassociation Imminent can force client to roam

WLAN: IEEE 802.11 – some developments

802.11c: Bridge Support

- Definition of MAC procedures to support bridges as extension to 802.1D

802.11d: Regulatory Domain Update

- Support of additional regulations related to channel selection, hopping sequences

802.11e: MAC Enhancements – QoS

- Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
- Definition of a data flow (“connection”) with parameters like rate, burst, period… supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
- Additional energy saving mechanisms and more efficient retransmission
- EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access

802.11F: Inter-Access Point Protocol (withdrawn)

- Establish an Inter-Access Point Protocol for data exchange via the distribution system

802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM

- Successful successor of 802.11b, performance loss during mixed operation with .11b

802.11h: Spectrum Managed 802.11a

- Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)

802.11i: Enhanced Security Mechanisms

- Enhance the current 802.11 MAC to provide improvements in security.
- TKIP enhances the insecure WEP, but remains compatible to older WEP systems
- AES provides a secure encryption method and is based on new hardware

WLAN: IEEE 802.11 – some developments

802.11j: Extensions for operations in Japan

- Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range

802.11k: Methods for channel measurements

- Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel

802.11m: Updates of the 802.11-2007 standard

802.11n: Higher data rates above 100Mbit/s

- Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
- MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
- However, still a large overhead due to protocol headers and inefficient mechanisms

802.11p: Inter car communications

- Communication between cars/road side and cars/cars
- Planned for relative speeds of min. 200km/h and ranges over 1000m
- Usage of 5.850-5.925GHz band in North America

802.11r: Faster Handover between BSS (“roaming”)

- Secure, fast handover of a station from one AP to another within an ESS
- Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
- Handover should be feasible within 50ms in order to support multimedia applications efficiently

802.11s: Mesh Networking

- Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
- Support of point-to-point and broadcast communication across several hops

WLAN: IEEE 802.11 – some developments

802.11T: Performance evaluation of 802.11 networks
- Standardization of performance measurement schemes

802.11u: Interworking with additional external networks

802.11v: Network management
- Extensions of current management functions, channel measurements
- Definition of a unified interface

802.11w: Securing of network control
- Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.

802.11y: Extensions for the 3650-3700 MHz band in the USA

802.11z: Extension to direct link setup

802.11aa: Robust audio/video stream transport

802.11ac: Very High Throughput <6Ghz – up to almost 7 Gbit/s @ 5GHz using 8x8 MIMO

802.11ad: Very High Throughput in 60 GHz

802.11af: TV white space, ah: sub 1GHz, ai: fast initial link set-up; … aq: pre-association discovery,

802.11ax: High Efficiency Wireless LAN (HEW)

802.11ay: Next Generation 60 GHz (NG60), az: Next Generation Positioning (NGP), ba: Wake-up radio, bb: light, …

802.11-2016: Current "complete" standard - 3534 pages!
- Comprises many amendments

Note: Not all "standards" will end in products, many ideas get stuck at working group level

Info: www.ieee802.org/11/; dig into Task Group Meetings

Current top standard IEEE 802.11ax – High Efficiency WLAN – marketed as WiFi 6(E)

Increased number of non-overlapping channels at 6 GHz

Improvements of 802.11ax over 802.11ac

- Centrally (AP) controlled MAC with dynamic bandwidth assignment using OFDMA via Resource Units (RU, time-frequency resources, see LTE!)

- Multi-user MIMO in up- and downlink, AP sends trigger with scheduling information (modulation, coding, RUs)

- Mix of assigned and random access RUs for uplinks

- Spatial frequency reuse via “coloring” of signals (distinguishes own/neighboring network) plus adaptive power/sensitivity thresholds

- Two NAVs: own network and overlapping network to avoid misbehavior

- Dynamic fragmentation helps reducing overhead (fill available RUs)

- Longer guard intervals for better protection against signal delay spread (outdoor conditions)

Data rates for 802.11ax

- Values are for a single spatial stream
- Depending on number of streams devices with > 10 Gbit/s available

MCS	Modulation	Coding rate	Data rate in Mbit/s per spatial stream							
			20 MHz channels		40 MHz channels		80 MHz channels		160 MHz channels	
			1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI	1600 ns GI	800 ns GI
0	BPSK	1/2	8	8.6	16	17.2	34	36.0	68	72
1	QPSK	1/2	16	17.2	33	34.4	68	72.1	136	144
2	QPSK	3/4	24	25.8	49	51.6	102	108.1	204	216
3	16-QAM	1/2	33	34.4	65	68.8	136	144.1	272	282
4	16-QAM	3/4	49	51.6	98	103.2	204	216.2	408	432
5	64-QAM	2/3	65	68.8	130	137.6	272	288.2	544	576
6	64-QAM	3/4	73	77.4	146	154.9	306	324.4	613	649
7	64-QAM	5/6	81	86.0	163	172.1	340	360.3	681	721
8	256-QAM	3/4	98	103.2	195	206.5	408	432.4	817	865
9	256-QAM	5/6	108	114.7	217	229.4	453	480.4	907	961
10	1024-QAM	3/4	122	129.0	244	258.1	510	540.4	1021	1081
11	1024-QAM	5/6	135	143.4	271	286.8	567	600.5	1134	1201

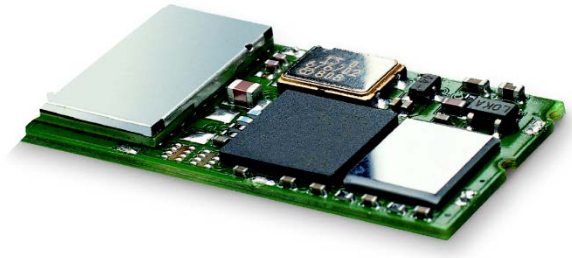
Questions & Tasks

- Check the differences between WiFi, WMM, … and the 802.11 standard!
- Why is synchronization needed?
- What are the negative effects of the power saving mechanisms, what are the trade-offs between power consumption and transmission QoS? What is the advantage of U-APSD?
- Why can roaming consume a lot of time? How to speed-up the process?
- What is left from the distributed WLAN mechanisms when looking at the most current standards?

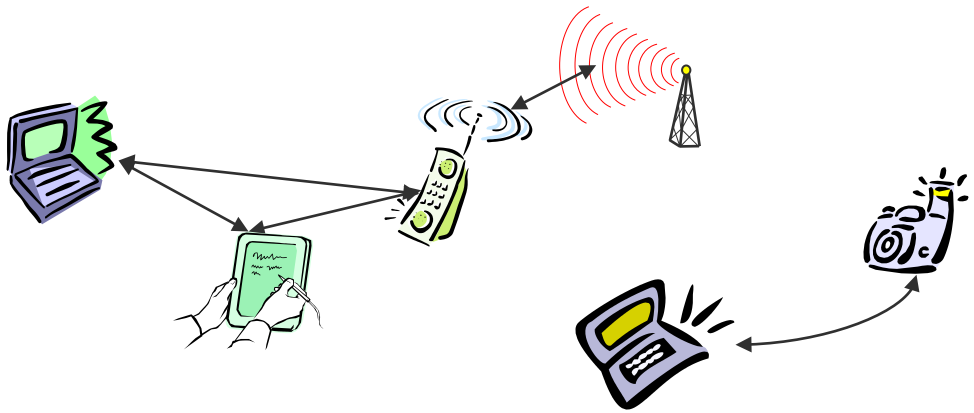
Bluetooth

Basic idea long time ago

- 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 (pretty soon < 1€)
- Short range (10 m), low power consumption, license-free 2.45 GHz ISM band
- Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first modules (Ericsson).



Bluetooth

(was: Bluetooth)

History

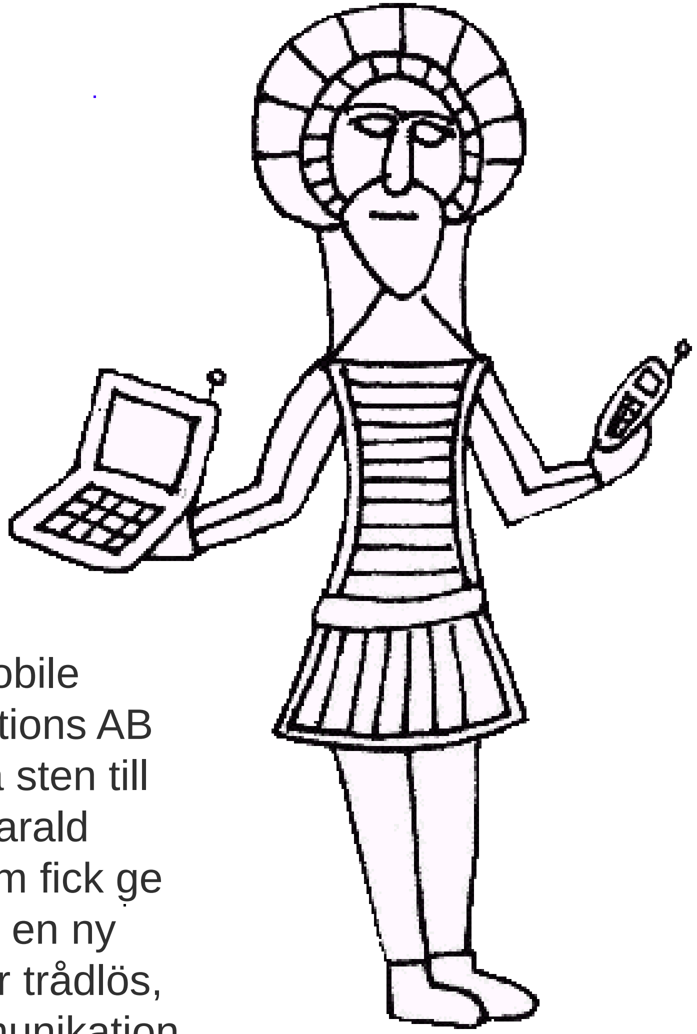
- 1994: Ericsson (Mattison/Haartsen), “MC-link” project
- Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
- 1998: foundation of Bluetooth SIG, www.bluetooth.org
- 1999: erection of a rune stone at Ercisson/Lund ;-)
- 2001: first consumer products for mass market, spec. version 1.1 released
- 2005: 5 million chips/week

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
- 2020: core specification 5.2 comprises 3256 pages!

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)

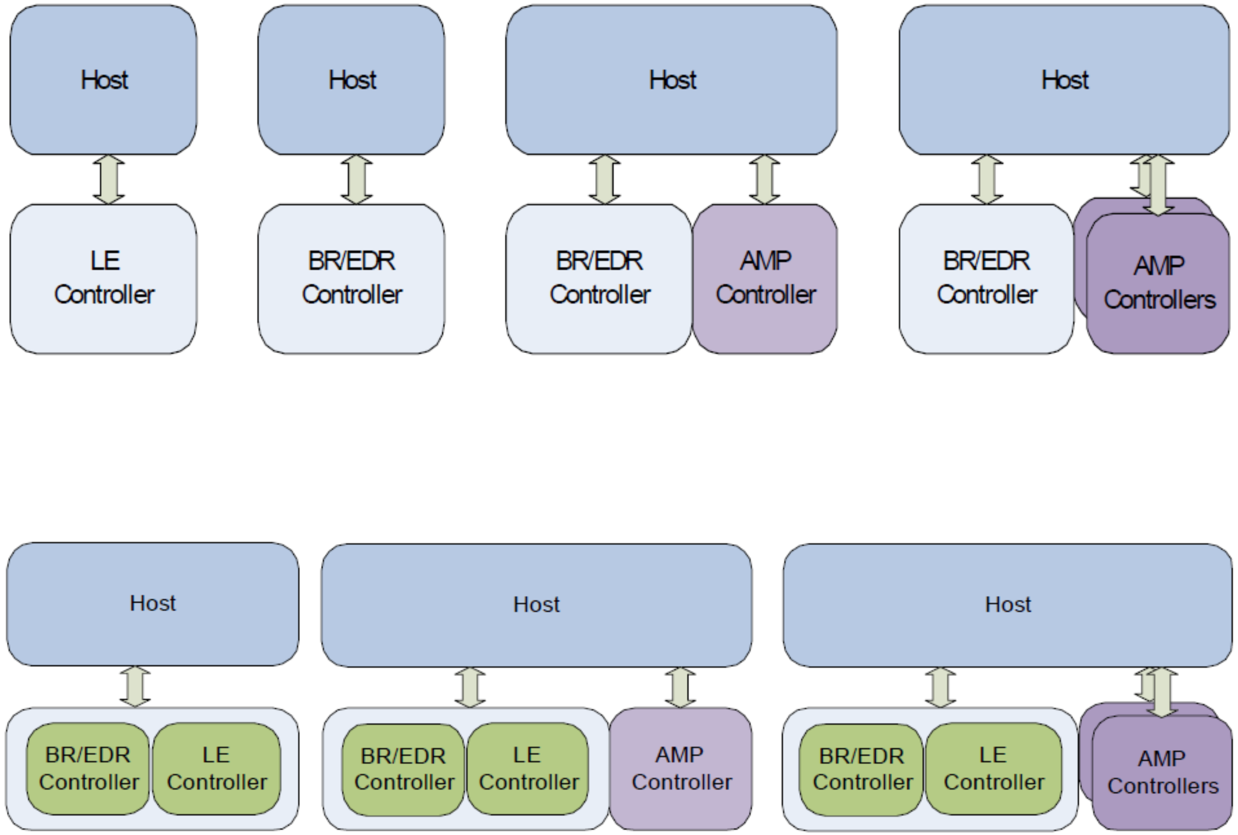
Bluetooth today - Overview

Basic Rate (BR) – up to 723.2 kbit/s

- Optional EDR (Enhanced Data Rate, 2.1 Mbit/s), AMP (Alternate MAC and PHY, 54 Mbit/s)
- Headsets, keyboards, …

Low Energy (LE) – up to 2 Mbit/s

- Lower power, cost, complexity, duty cycles
- Smart beacons, home automation, …



Source: www.Bluetooth.org, BT_Core, v5.2

Characteristics of the classical system – Bluetooth BR

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

- Channel 0: 2402 MHz … channel 78: 2480 MHz
- GFSK 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

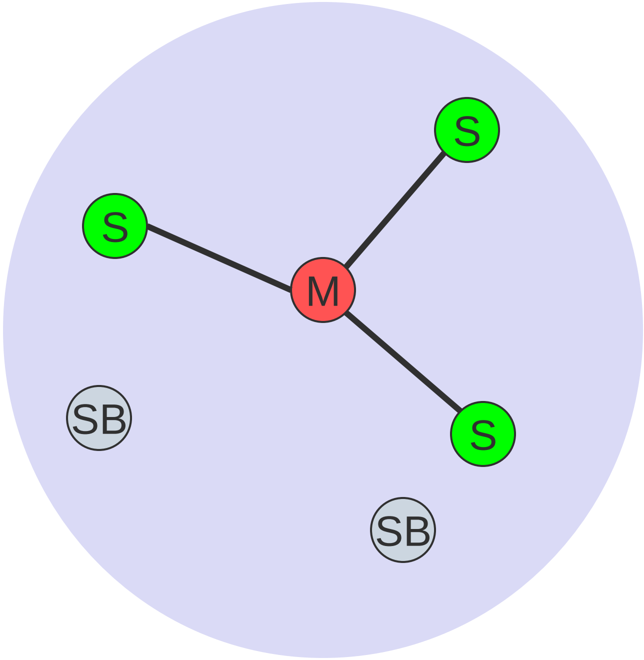
One unit acts as master and the others as slaves for the lifetime of the piconet

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



M=Master
S=Slave

SB=Standby

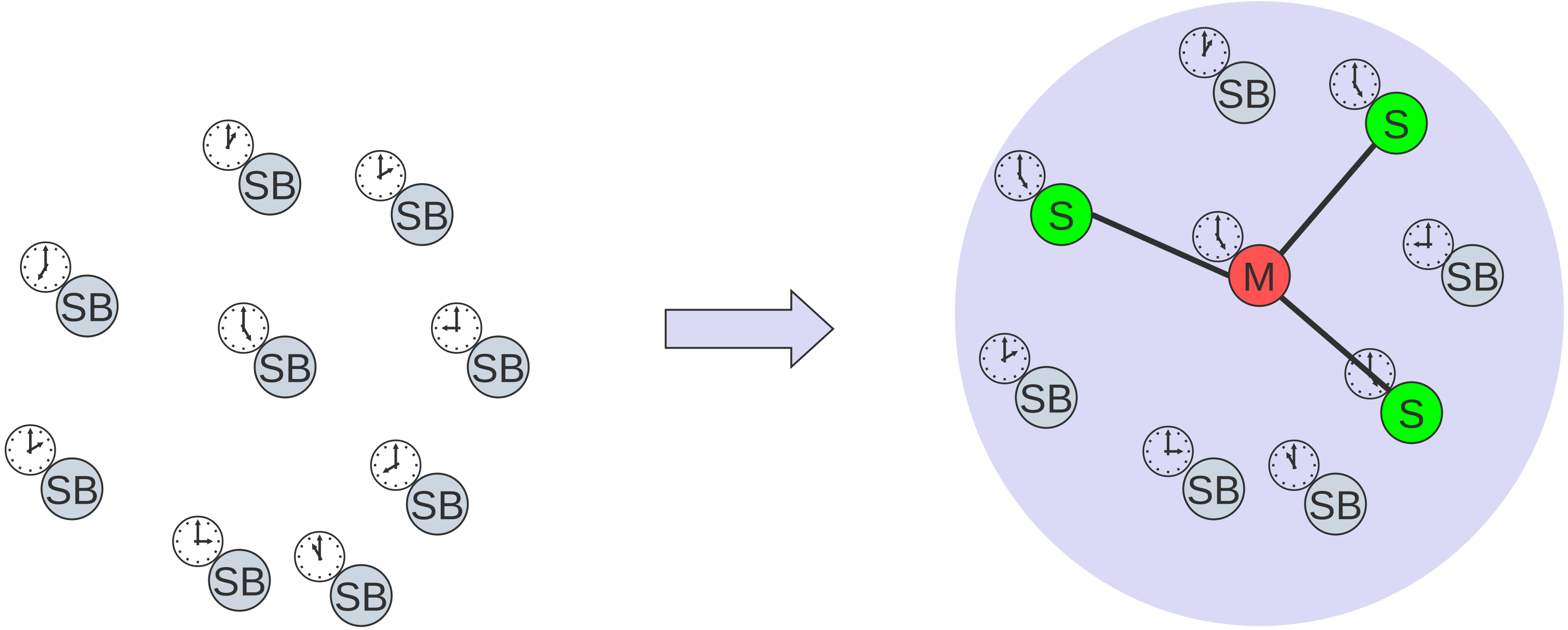
Forming a piconet

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

- Logical Transport Address (LT_ADDR, 3 bit)



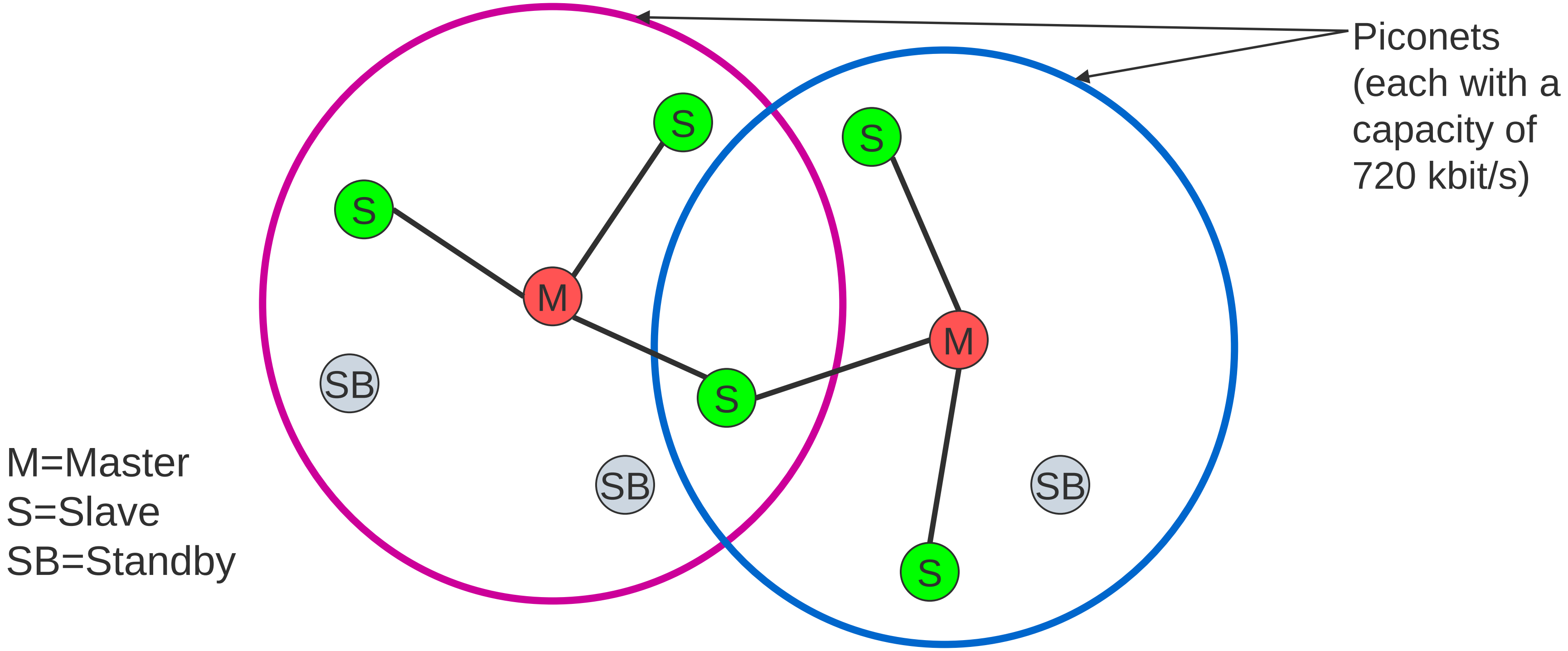
Scatternet

Linking of multiple co-located piconets through the sharing of common master or slave devices

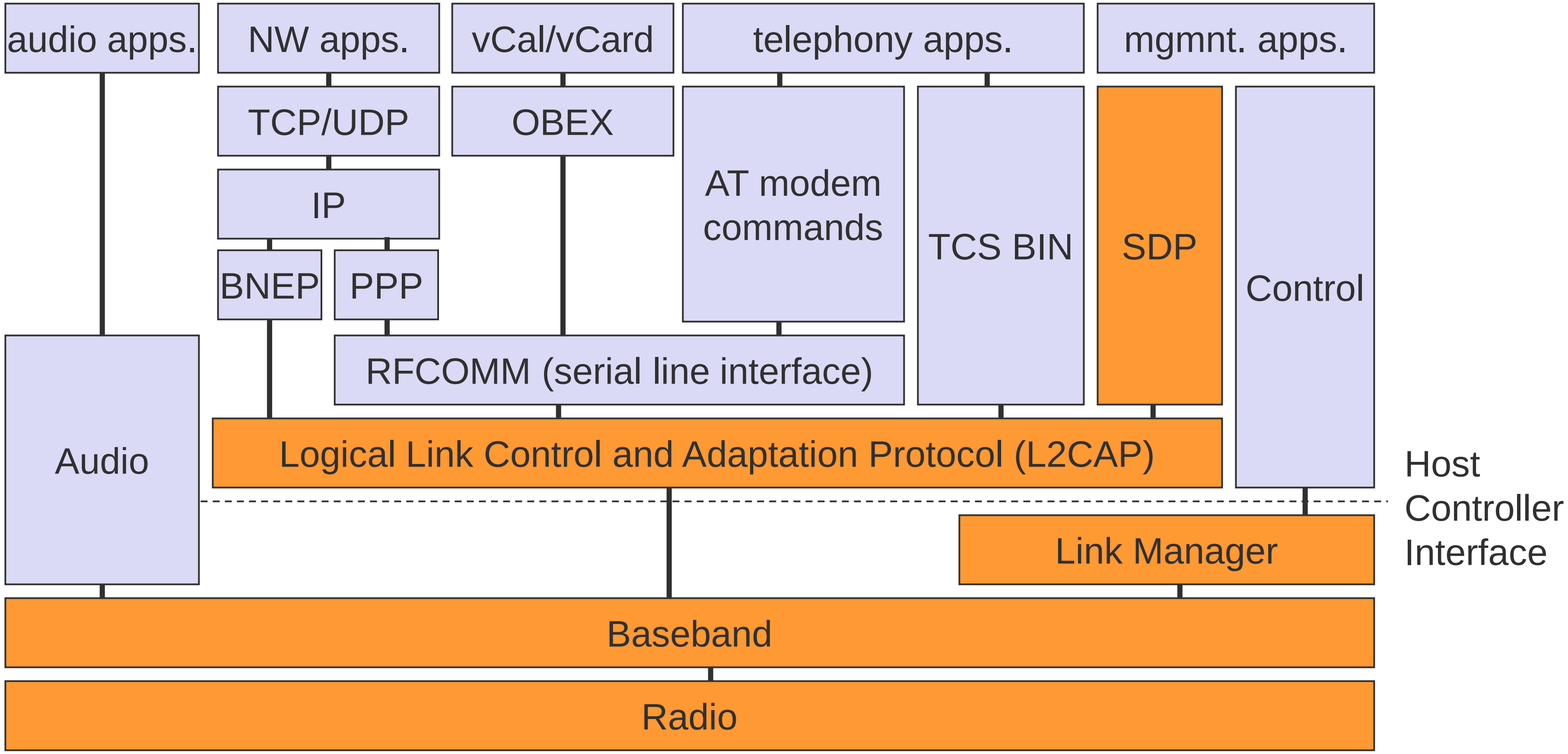
- Devices can be slave in one piconet and master of another

Communication between piconets

- Devices jumping back and forth between the piconets



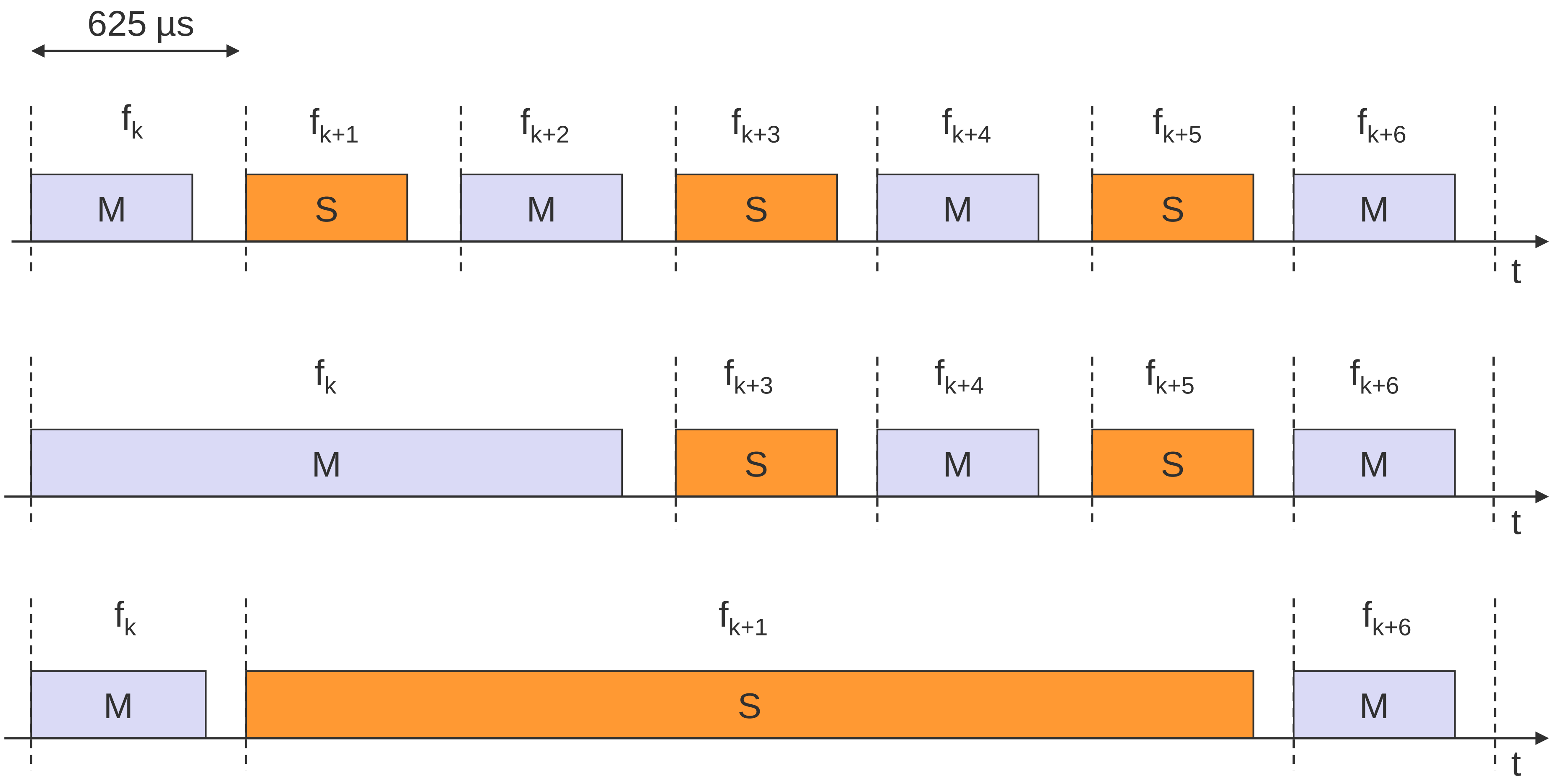
Bluetooth protocol stack – classical view



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

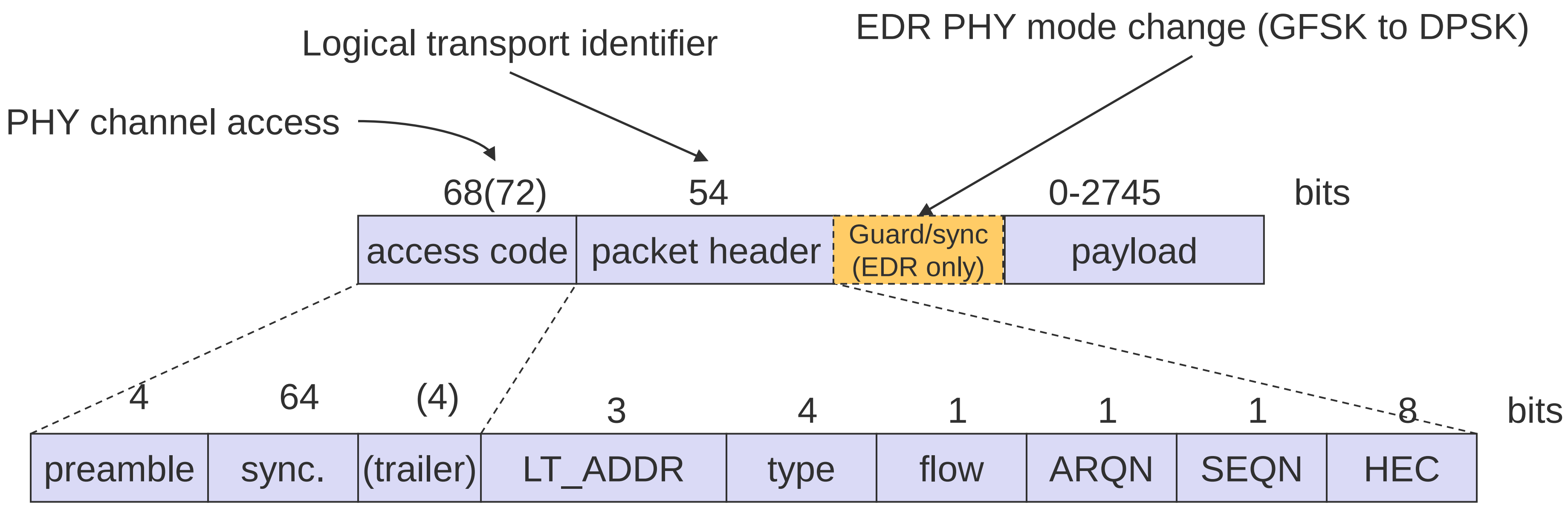


Baseband

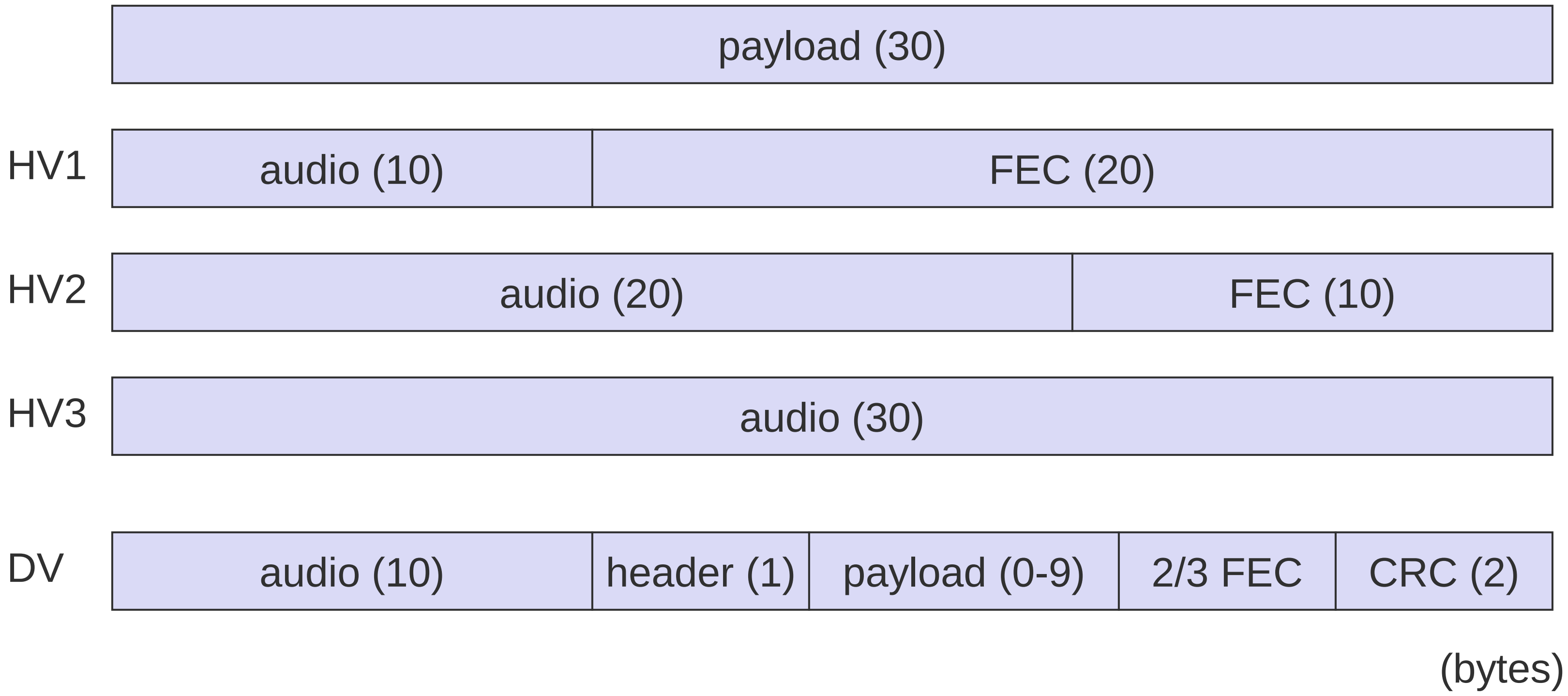
Piconet/channel definition

Low-level packet definition

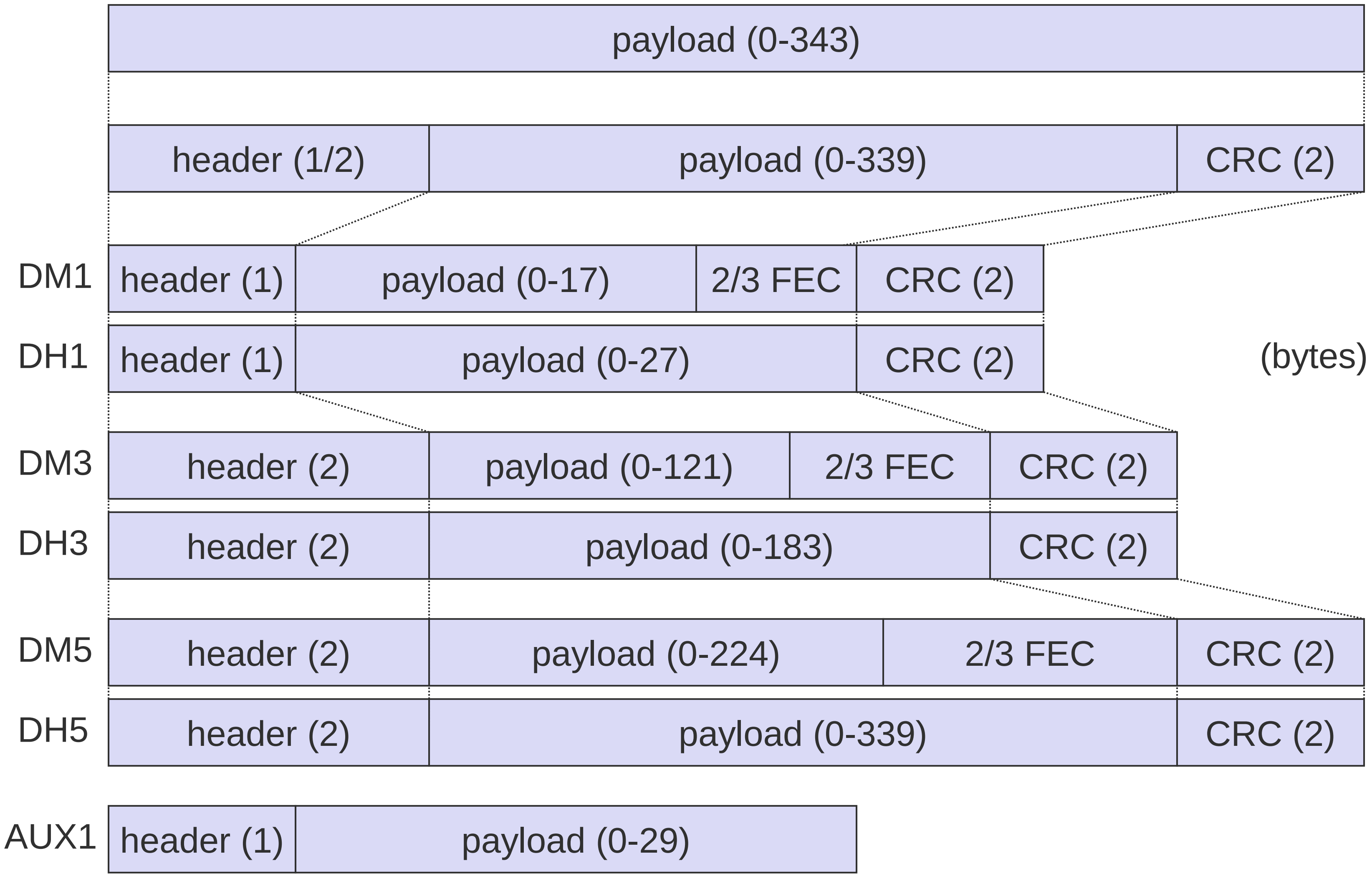
- Access code
  - Channel, device access, e.g., derived from master
- Packet header
  - 1/3-FEC, Logical Transport Address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



Classical SCO payload types



Classical ACL Payload types



Baseband data rates (examples)

ACL packets

Type	Payload Header (bytes)	User Payload (bytes)	FEC	MIC	CRC	Symmetric Max. Rate (kb/s)	Asymmetric Max. Rate (kb/s)	
							Forward	Reverse
DM1	1	0-17	2/3	C.1	Yes	108.8	108.8	108.8
DH1	1	0-27	No	C.1	Yes	172.8	172.8	172.8
DM3	2	0-121	2/3	C.1	Yes	258.1	387.2	54.4
DH3	2	0-183	No	C.1	Yes	390.4	585.6	86.4
DM5	2	0-224	2/3	C.1	Yes	286.7	477.8	36.3
DH5	2	0-339	No	C.1	Yes	433.9	723.2	57.6
2-DH1	2	0-54	No	C.1	Yes	345.6	345.6	345.6
2-DH3	2	0-367	No	C.1	Yes	782.9	1174.4	172.8
2-DH5	2	0-679	No	C.1	Yes	869.1	1448.5	115.2
3-DH1	2	0-83	No	C.1	Yes	531.2	531.2	531.2
3-DH3	2	0-552	No	C.1	Yes	1177.6	1766.4	265.6
3-DH5	2	0-1021	No	C.1	Yes	1306.9	2178.1	177.1

SCO packets

Type	Payload Header (bytes)	User Payload (bytes)	FEC	MIC	CRC	Symmetric Max. Rate (kb/s)
HV1	N/A	10	1/3	No	No	64.0
HV2	N/A	20	2/3	No	No	64.0
HV3	N/A	30	no	No	No	64.0
DV[1]	1 D	10+(0-9) D	2/3 D	No	Yes D	64.0+57.6 D
EV3	N/A	1-30	No	No	Yes	96
EV4	N/A	1-120	2/3	No	Yes	192
EV5	N/A	1-180	No	No	Yes	288
2-EV3	N/A	1-60	No	No	Yes	192
2-EV5	N/A	1-360	No	No	Yes	576
3-EV3	N/A	1-90	No	No	Yes	288
3-EV5	N/A	1-540	No	No	Yes	864

Source: www.Bluetooth.org, BT_Core

Questions & Tasks

- What were in the beginning, what are today the goals of Bluetooth?
- What are basic differences between WLAN and Bluetooth BR/EDR?
- What is a piconet?
- Why is there no collision in a piconet? How can collisions occur?
- How does EDR achieve higher data rates?

Baseband link types

Polling-based TDD packet transmission

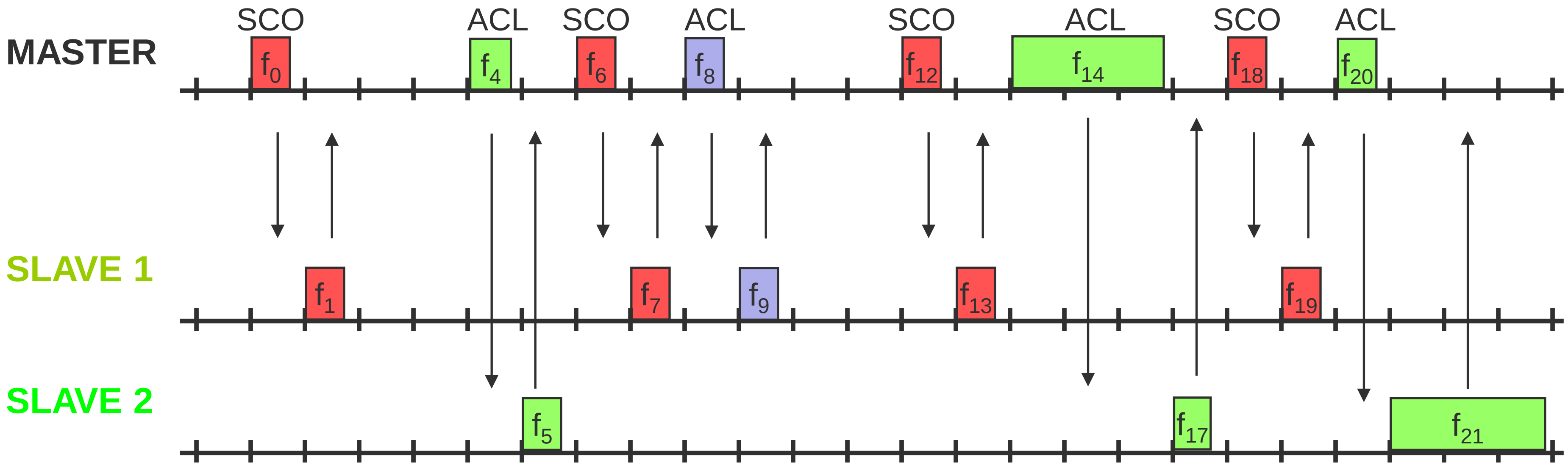
- 625µs slots, master polls slaves

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

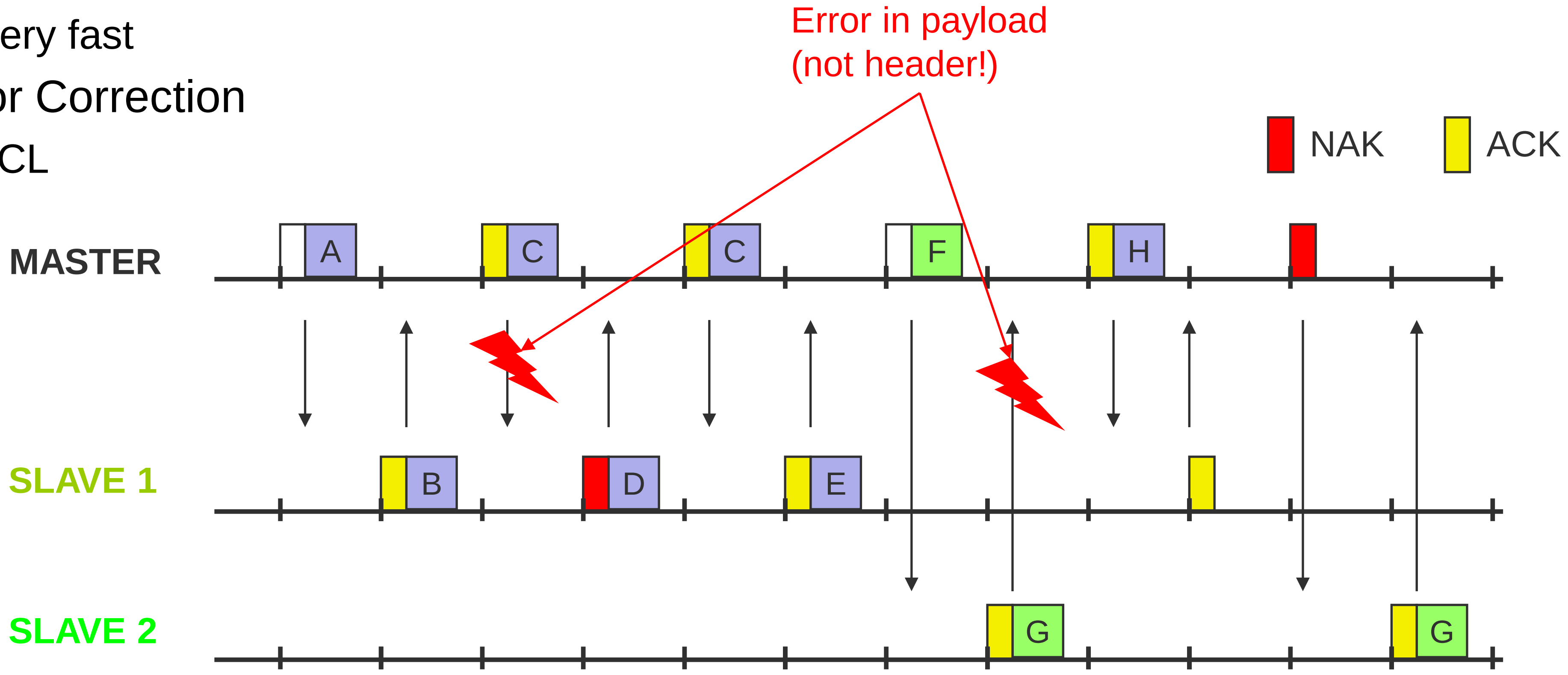
- Protection from interference on certain frequencies
- Separation from other piconets (FH-CDMA)

Retransmission

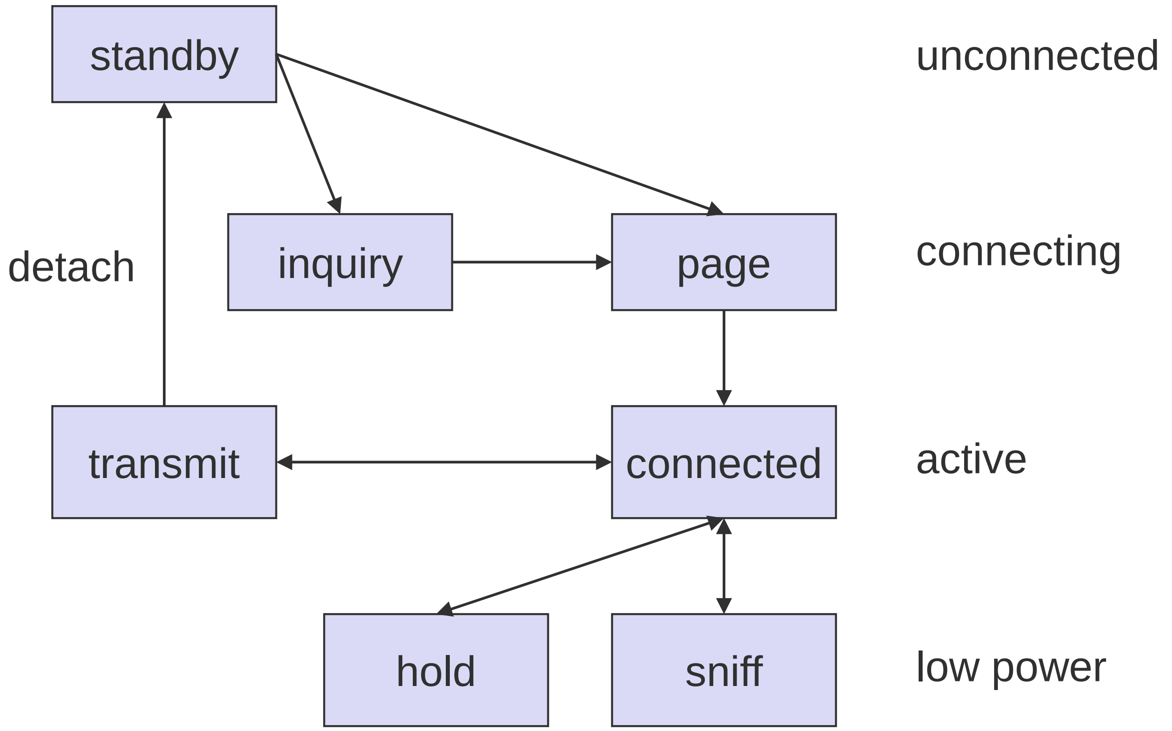
- ACL only, very fast

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

Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet
Some more defined: role swapping, EDR, …

Classical Example: Power consumption/CSR BlueCore2

Typical Average Current Consumption[1]

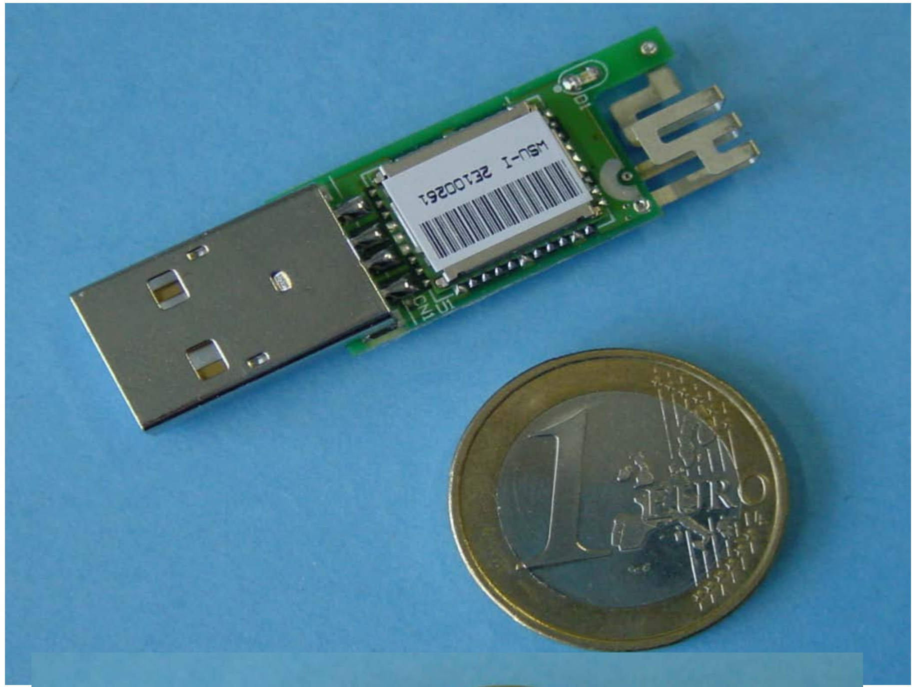
- VDD=1.8V Temperature = 20°C
- **Mode**

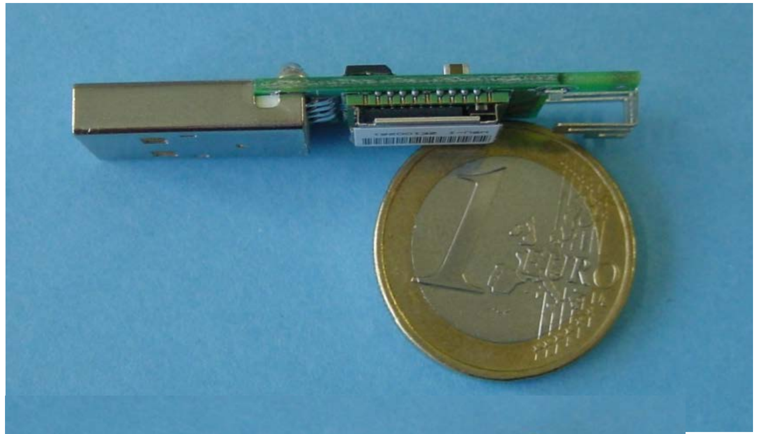
- SCO connection HV3 (1s interval Sniff Mode) (Slave)	26.0 mA
- SCO connection HV3 (1s interval Sniff Mode) (Master)	26.0 mA
- SCO connection HV1 (Slave)	53.0 mA
- SCO connection HV1 (Master)	53.0 mA
- ACL data transfer 115.2kbps UART (Master)	15.5 mA
- ACL data transfer 720kbps USB (Slave)	53.0 mA
- 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

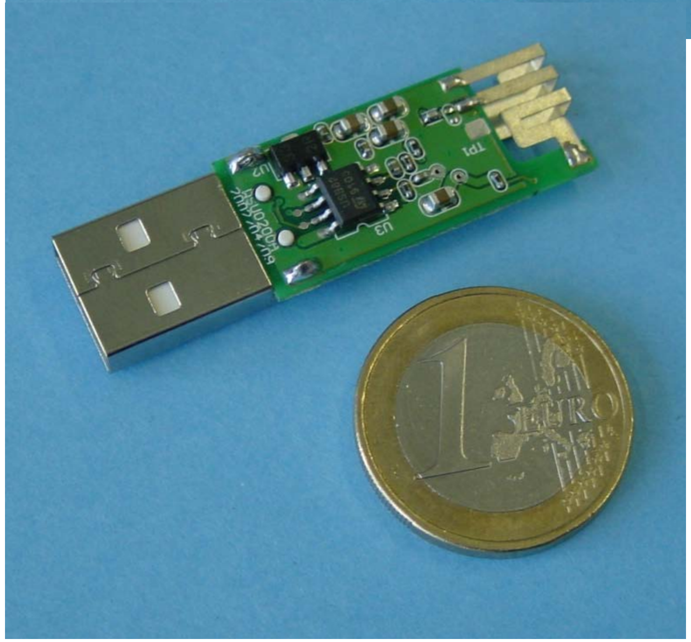
Notes:

- [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

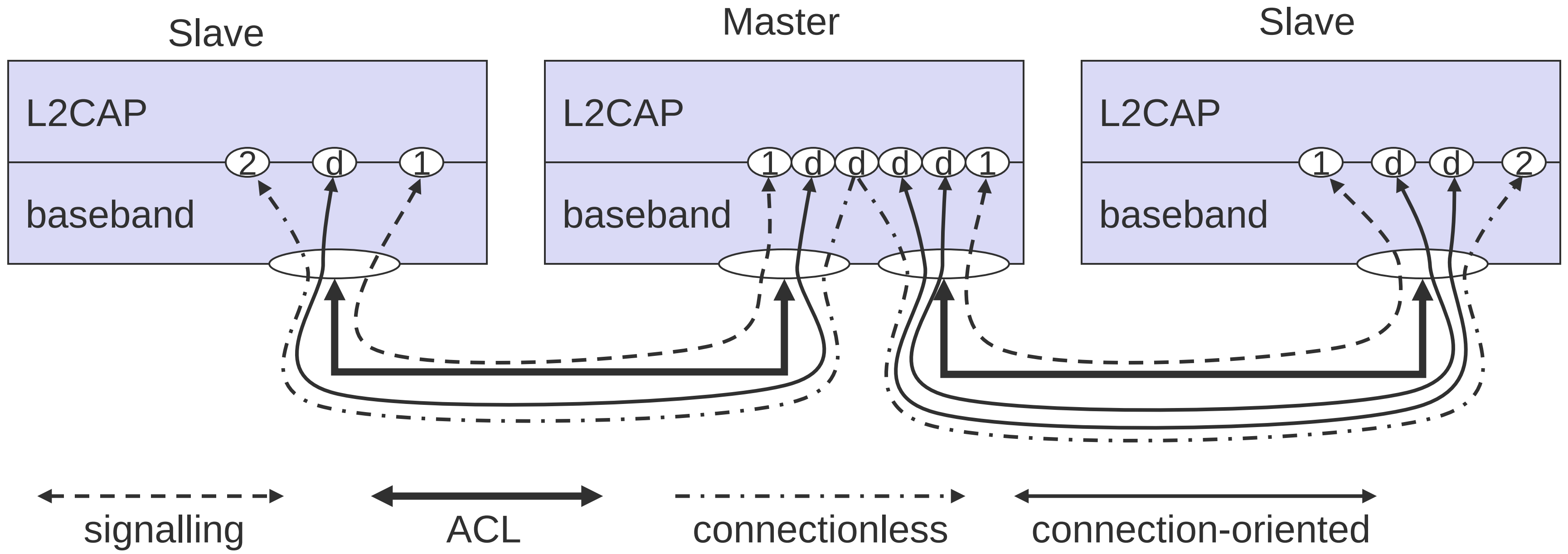
Protocol multiplexing
- RFCOMM, SDP, telephony control

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

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

Connection-oriented PDU

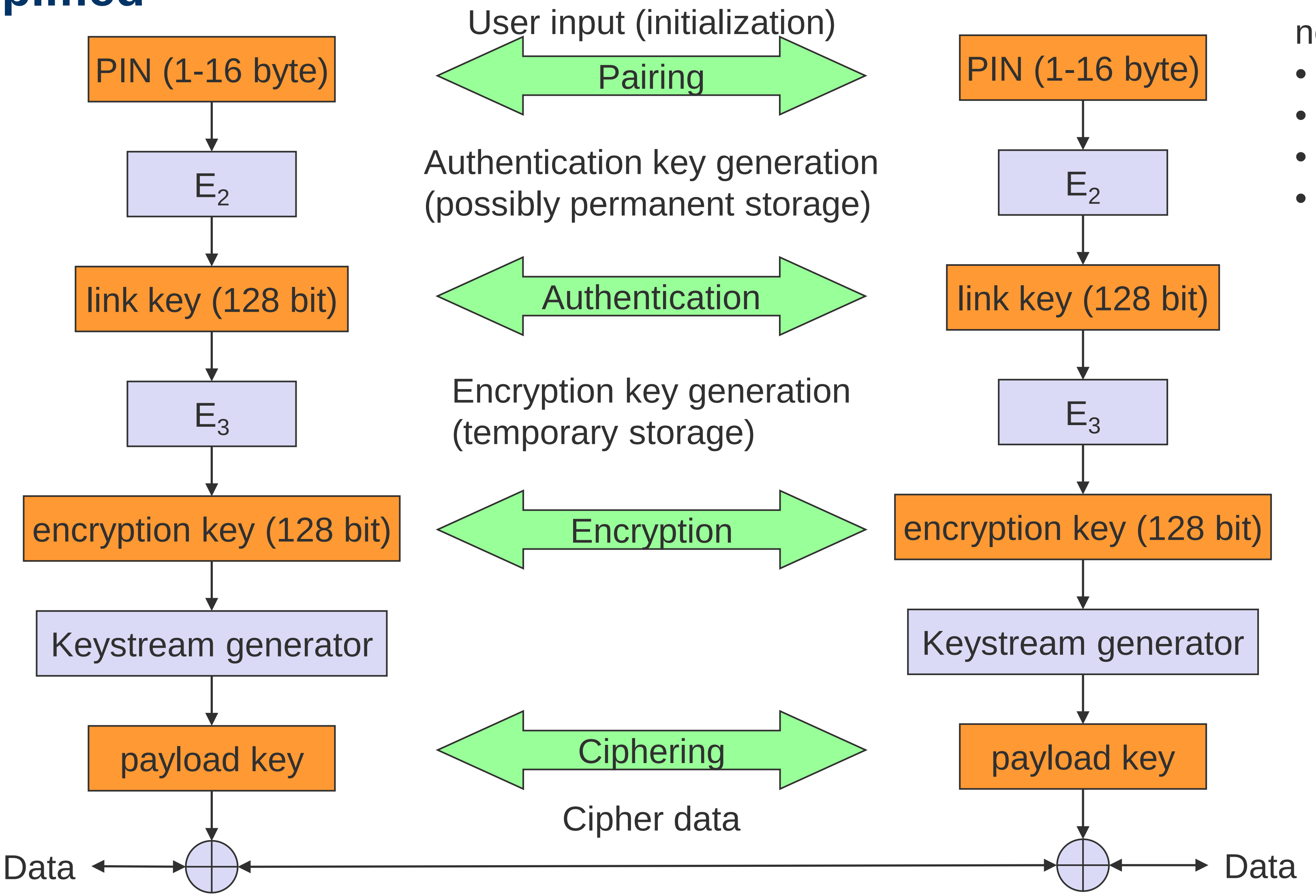
2	2	0-65535	bytes
length	CID	payload	

Signalling command PDU

2	2		bytes
length	CID=1	One or more commands	

1	1	2	≥0
code	ID	length	data

Security - simplified



newer:

- numeric comparison
- just works
- out-of-band
- passkey entry

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

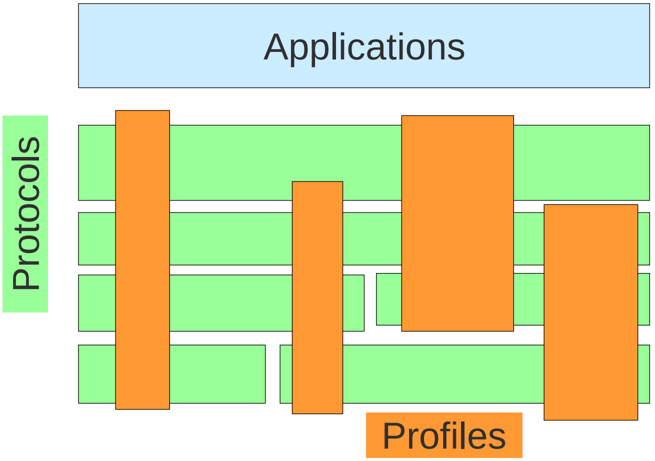
WAP

- Interacting with applications on cellular phones

Profiles

Represent default solutions for a certain usage model

- Vertical slice through the protocol stack
- Basis for interoperability
- Defines options and parameters



Examples

- A2DP: Advanced Audio Distribution Profile
- BIP: Basic Imaging Profile
- CTN: Calendar Tasks and Notes Profile
- FTP: File Transfer Profile
- GNSS: Global Navigation Satellite System Profile
- HDP: Health Device Profile
- HID: Human Interface Device Profile
- PBAP: Phone Book Access Profile
- SPP: Serial Port Profile
- … see https://www.bluetooth.com/specifications/profiles-overview/

Questions & Tasks

- How does Bluetooth guarantee certain data rates and delays?
- Can slaves send on their own?
- How can the sniff mode help reducing power consumption?
- If interested in the current security features – please do have a look at the Core Spec!
- Many protocols, options, parameters – quite complex! What is one offered solution to guarantee compatibility?

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, 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), 4.1 (2013), 4.2 (2014)
- **Low Energy**, much faster connection setup

Bluetooth 5 (2016)
- Longer range (100m) or higher data rate (2 Mbit/s without EDR), localization, no more park state

Bluetooth Low Energy – this is not classical BT anymore!

Also at 2.4 GHz, FHSS, mandatory 1 Mbit/s, 500 kbit/s, 125 kbit/s as well as optional 2 Mbit/s

Special mesh networking for many-to-many communication between thousands of devices

Two MAC schemes
- FDMA
  - 40 channels, 2 MHz spacing, 3 channels for advertising, 37 general purpose (advertising, data)
- TDMA
  - Polling scheme with predetermined intervals

Physical channel sub-divided into “events”
- Advertising, extended advertising, periodic advertising, connection, isochronous

Radio supports direction finding (angle of arrival / departure) useful for RTLS

Source: www.nordicsemi.com, nRF5340

BLE Physical Channels

PHY Channel	RF Center Frequency	Channel Index	RF Channel Group	
			Primary Advertising	General purpose
0	2402 MHz	37	●	
1	2404 MHz	0		●
2	2406 MHz	1		●
...	...	...	...	...
11	2424 MHz	10		●
12	2426 MHz	38	●	
13	2428 MHz	11		●
14	2430 MHz	12		●
...	...	...	...	...
38	2478 MHz	36		●
39	2480 MHz	39	●	

Source: www.Bluetooth.org, BT_Core, v5.2

BLE Packet Format – Example: Uncoded PHY LE 1M and LE 2M)

Preamble

- Synchronization, gain control, symbol timing
- 1 byte for LE 1M, 2 byte for LE 2M

Access Address

- Determined by the link layer

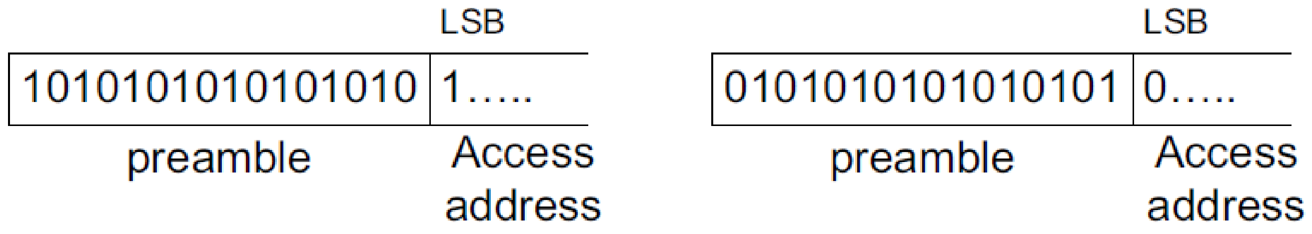
Constant Tone Extension

- Optional for AoA/AoD estimation

LSB — MSB

Preamble (1 or 2 octets)	Access-Address (4 octets)	PDU (2-258 octets)	CRC (3 octets)	Constant Tone Extension (16 to 160 µs)

Preamble for LE 1M packets

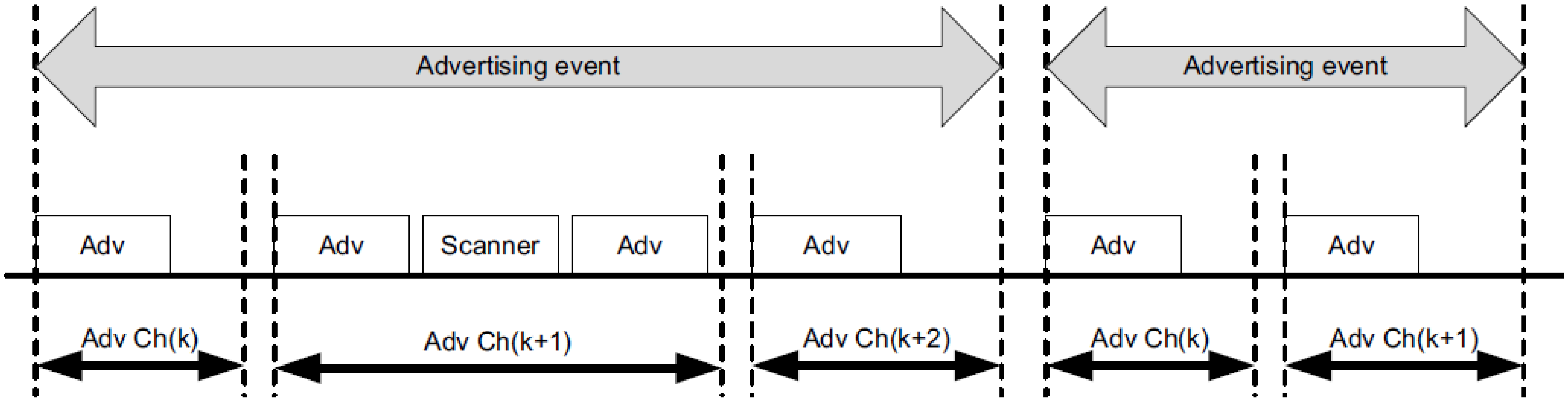


Preamble for LE 2M packets

Source: www.Bluetooth.org, BT_Core, v5.2

BLE Advertisements

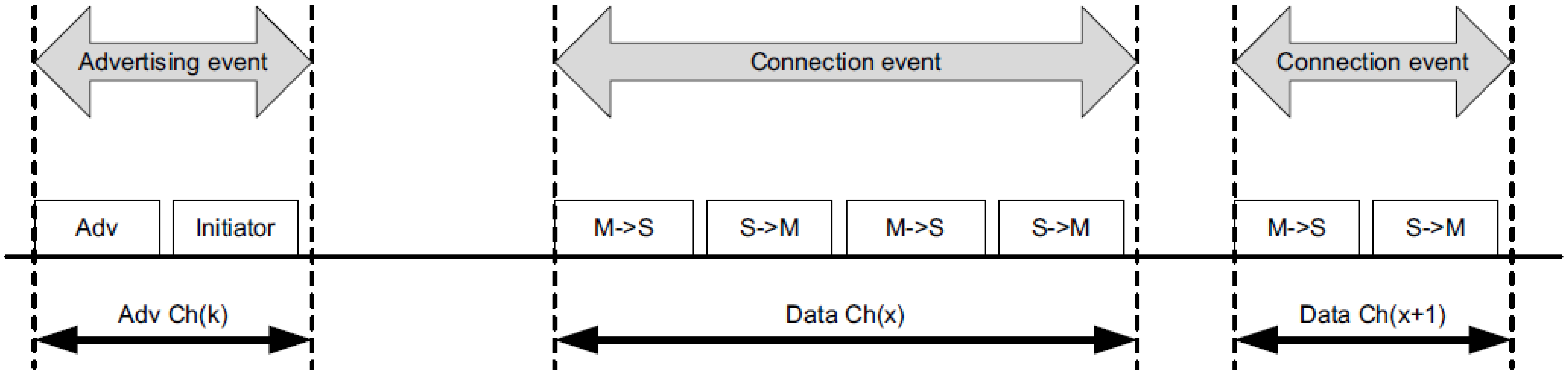
- Communication can happen in advertising events
- Each advertising event starts at the first advertising channel k
- Advertisers send advertisements, scanners receive and may make a request answered by the advertiser
- Advertisements can be used to set-up bidirectional communication, periodic broadcasts, isochronous streams



Source: www.Bluetooth.org, BT_Core, v5.2

BLE setting up ACL connections

- Devices (called initiator) may listen for connectable advertising packets
- After reception the initiator may make a connection request on the same channel
- Start of connecting event if advertiser accepts connection request
- Initiator becomes master in the piconet, advertising device the slave
- Channel hopping at each connection event based on hopping pattern determined by connection request
    - Pseudo-random pattern using 37 frequencies incl. interference prevention via exclusion of channels
- Using an ACL connection the master can establish one or more isochronous connections



Source: www.Bluetooth.org, BT_Core, v5.2

Example Roles and Topologies

Piconet A

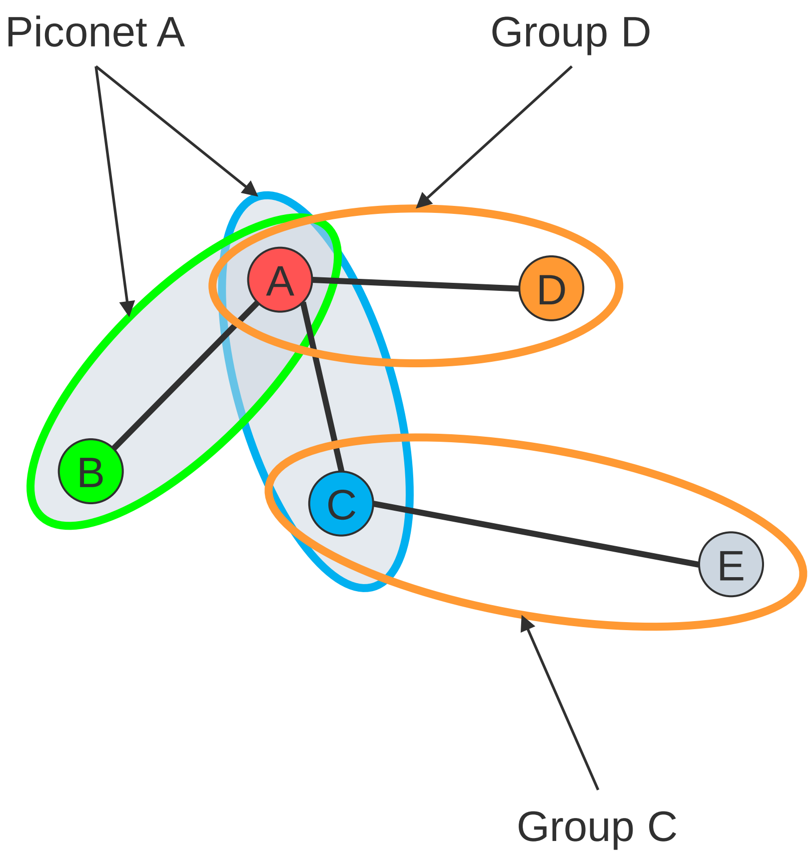
- A is master
- B is slave
- C is slave
- BUT: slaves do NOT share same frequencies!

Group D

- D is advertiser
- A is initiator
- A could add D to piconet A

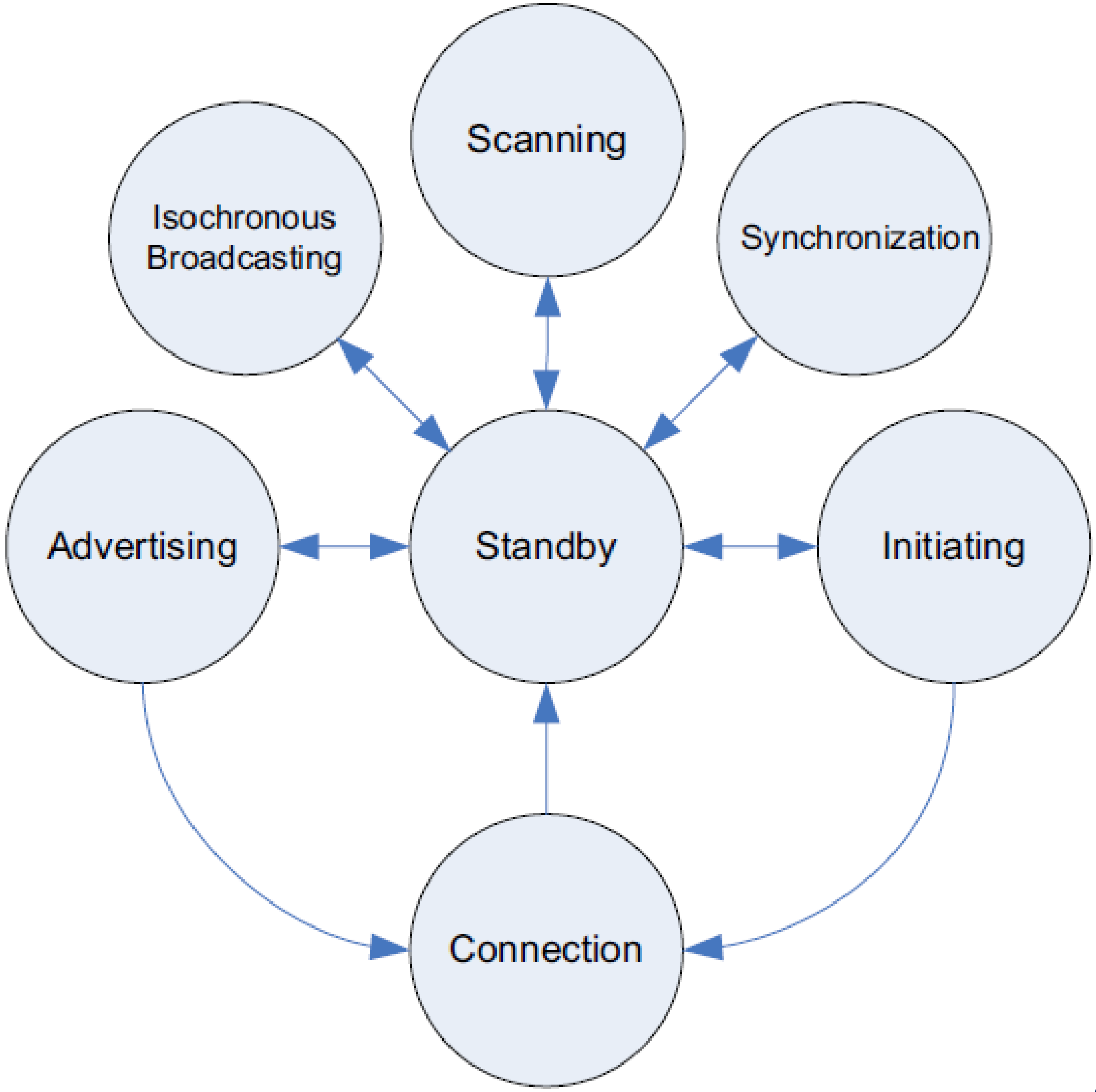
Group C

- C is advertiser
- E is scanner



Advertisements may happen on different advertising channels to avoid collisions

Link Layer State Diagram



Source: www.Bluetooth.org, BT_Core, v5.2

Questions & Tasks

- What are major changes when going from Bluetooth BR/EDR to Bluetooth LE?
- How do devices “find” each other?
- What are differences of BT BR/EDR piconets and BT LE piconets?
- Why can BT LE devices react/transmit faster?
- Where can collisions happen during data transmission?

WPAN: IEEE 802.15 – additional 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 – additional 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

The following IEEE 802.15 projects are either completed or in hibernation.

- 802.15.1
- 802.15.2
- 802.15.3
- 802.15.3a
- 802.15.3b
- 802.15.3c
- 802.15.3d
- 802.15.3e
- 802.15.3f
- 802.15.4
- 802.15.4a
- 802.15.4b
- 802.15.4c
- 802.15.4d
- 802.15.4e
- 802.15.4f
- 802.15.4g
- 802.15.4j
- 802.15.4k
- 802.15.4m
- 802.15.4p
- 802.15.4r
- 802.15.4s
- 802.15.4t
- 802.15.4v
- 802.15.4x
- 802.15.5
- 802.15.6
- 802.15.7
- 802.15.8
- 802.15.10a

Not all these working groups really create a standard, not all standards will be found in products later …

WPAN: IEEE 802.15 – additional 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

Base 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 19 promoters, 133 participants, 162 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 Technical Specifications

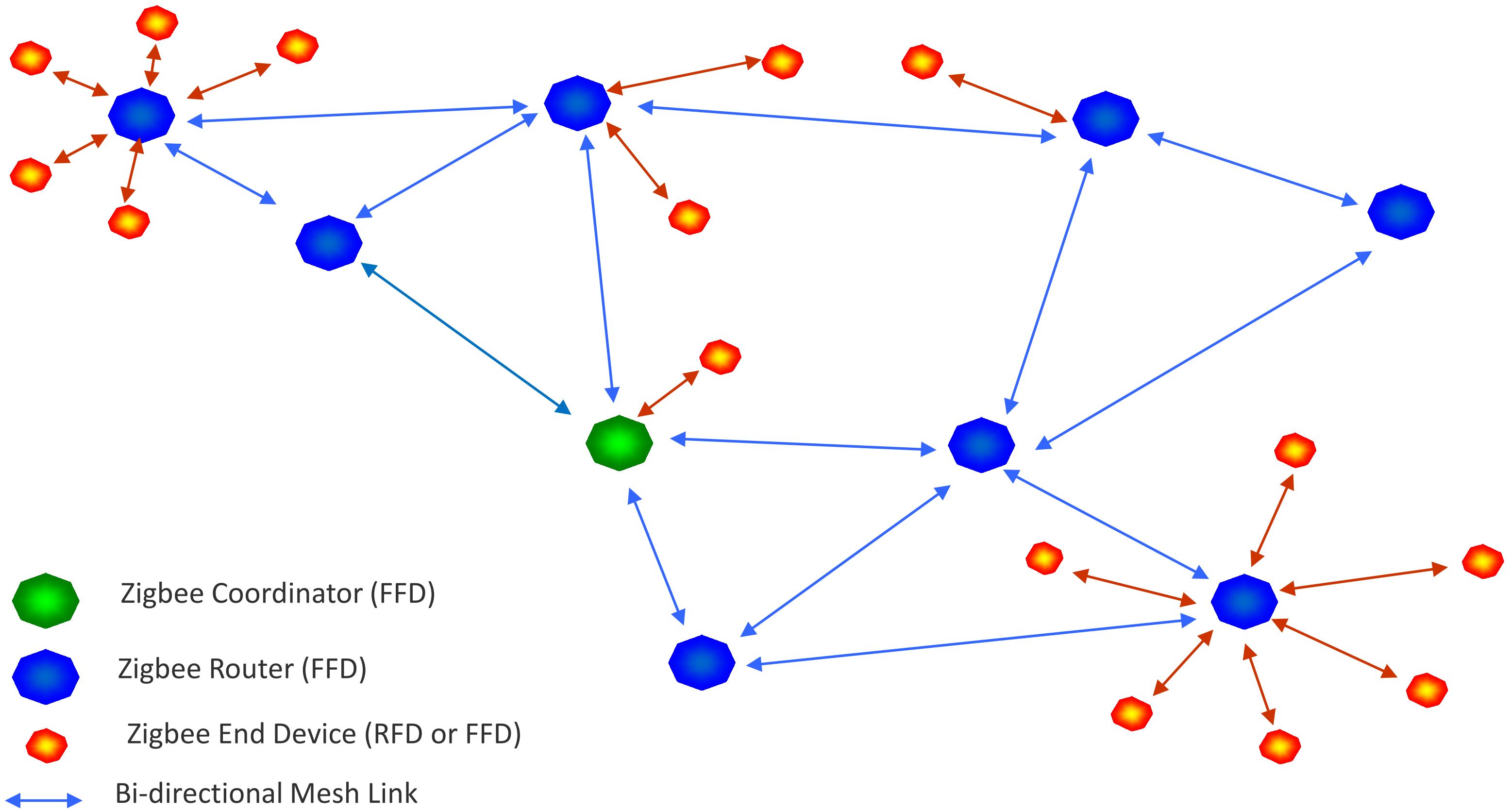
Solution	Description
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Network Size (theoretical # of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band) 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer AES-128 available at Application Layer
Communication Range (Average)	Up to 300+ meters (line of sight) Up to 75-100 meter indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy Profile Support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
Logical device support	Each physical device may support up to 240 end-points (logical devices)

Source: www.zigbeealliance.org

Zigbee Network Topology Example – Centralized Security

- Mesh, self-organizing, self-healing topology scalable to thousands of nodes
- Interference tolerance via clear channel assessments, retries, etc.
- Point to Point communication gives range > 100 m; full mesh deployment can have several kilometer range

- End device
  - Single parent, no routing
  - Often battery powered
- Router
- Coordinator
  - Owns the network
- FFD (Full Function Device)
  - Mains powered, can route, always on
- RFD (Reduced Function Device)
  - Talks only to parent, can sleep



Source: www.zigbeealliance.org

WPAN: IEEE 802.15 – additional 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, … r, s:

- 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 ……………. and many, many more!

Not all these working groups really create a standard, not all standards will be found in products later … see http://www.ieee802.org/15/

Some more IEEE standards for mobile communications

IEEE 802.16: Broadband Wireless Access / WirelessMAN / WiMax – hibernating (dead due to LTE…)
- Wireless distribution system, e.g., for the last mile, alternative to DSL
- 75 Mbit/s up to 50 km LOS, up to 10 km NLOS; 2-66 GHz band
- Initial standards without roaming or mobility support
- 802.16e adds mobility support, allows for roaming at 150 km/h

IEEE 802.19: Wireless Coexistence Working Group
- Standards for the coexistence between wireless standards of unlicensed devices

IEEE 802.20: Mobile Broadband Wireless Access (MBWA) Working Group - disbanded

IEEE 802.21: Media Independent Handover Interoperability - hibernating
- Standardize handover between different 802.x and/or non 802 networks

IEEE 802.22: Wireless Regional Area Networks (WRAN) - hibernating
- Radio-based PHY/MAC for use by license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service

RF Controllers – ISM bands

Data rate
- Typ. up to 115 kbit/s (serial interface)

Transmission range
- 5-100 m, depending on power (typ. 10-500 mW)

Frequency
- Typ. 27 (EU, US), 315 (US), 418 (EU), 426 (Japan), 433 (EU), 868 (EU), 915 (US) MHz (depending on regulations)

Security
- Some products with added processors

Cost
- Cheap: 10€-50€

Availability
- Many products, many vendors

Connection set-up time
- N/A

Quality of Service
- none

Manageability
- Very simple, same as serial interface

Special Advantages/Disadvantages
- Advantage: very low cost, large experience, high volume available
- Disadvantage: no QoS, crowded ISM bands (particularly 27 and 433 MHz), typ. no Medium Access Control, 418 MHz experiences interference with TETRA

ISM band interference

Many sources of interference

- Microwave ovens, microwave lighting
- 802.11, 802.11b, 802.11g, 802.15, …
- Even old analog TV transmission, surveillance
- Unlicensed metropolitan area networks
- …

Levels of interference

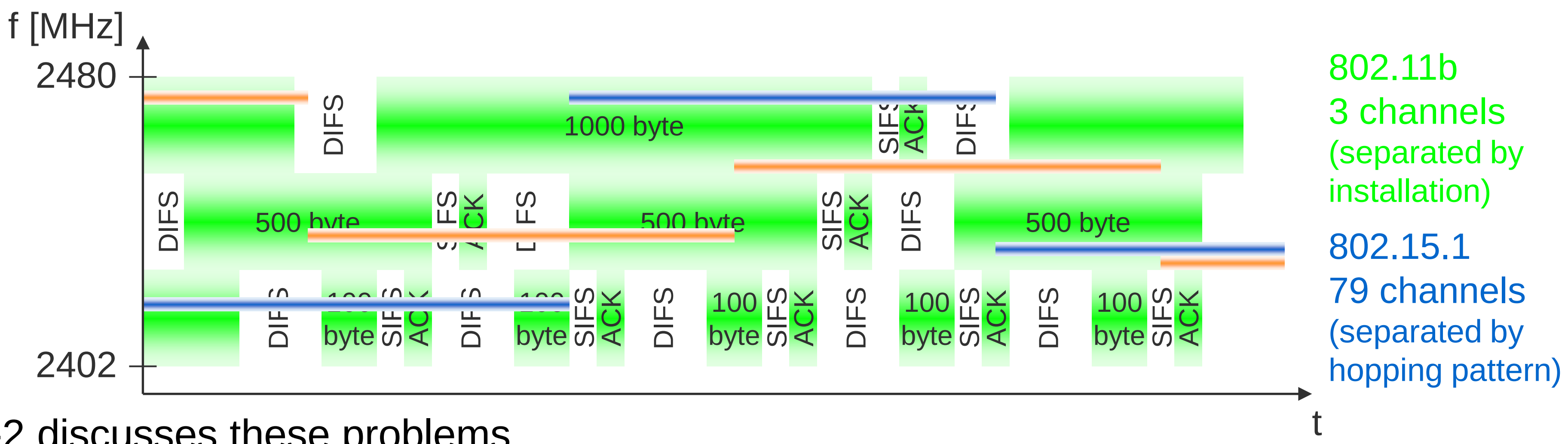
- Physical layer: interference acts like noise
    - Spread spectrum tries to minimize this
    - FEC/interleaving tries to correct
- MAC layer: algorithms not harmonized
    - E.g., Bluetooth might confuse 802.11

© Fusion Lighting, Inc.,
now used by LG as
Plasma Lighting System

802.11 vs.(?) 802.15/Bluetooth – a problem from the beginning?

Bluetooth may act like a rogue member of the 802.11 network

- Does not know anything about gaps, inter frame spacing etc.



IEEE 802.15-2 discusses these problems

- Proposal: Adaptive Frequency Hopping
  - a non-collaborative Coexistence Mechanism

Real effects? Many different opinions, publications, tests, formulae, …

- Results from complete breakdown to almost no effect
- Bluetooth (FHSS) seems more robust than 802.11b (DSSS)

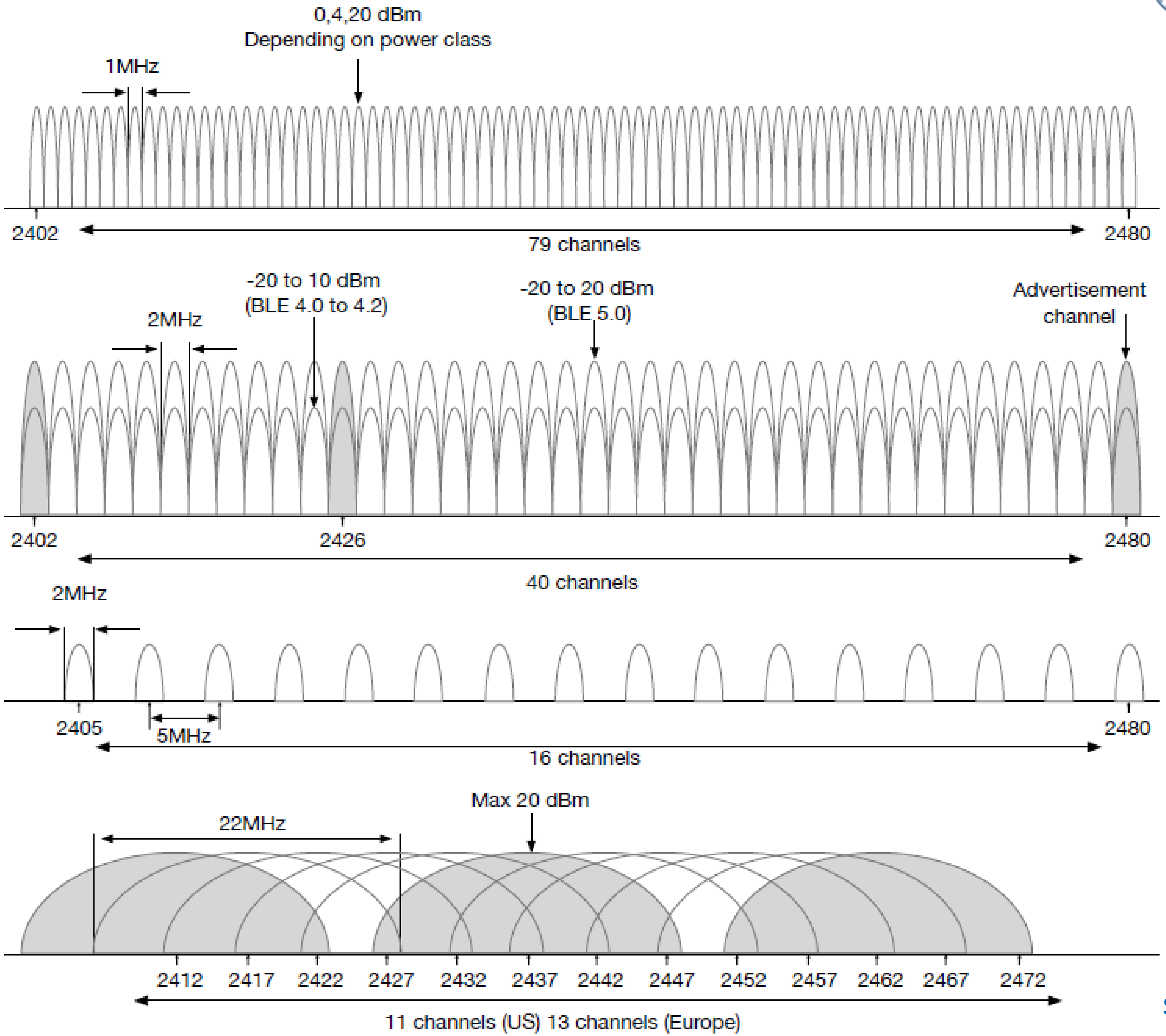
Overview – who is where?

Bluetooth BR/EDR

Bluetooth LE

ZigBee 802.15.4

WLAN 802.11



Source: S. Raza

Mechanisms for Interference avoidance in the ISM band – Example Bluetooth

Adaptive Frequency Hopping

- Reduce the number of channels used in a piconet (min. 20 out of 79)

HCI Set Host Channel Classification

- Host informs BT controller of the occupied channels by e.g. WLAN

Enhanced SCO

- Added retransmissions to SCO

Piconet Clock Adjust

- Align clock with external technology

Slot Availability Mask

- Exchange available time slot

…

Questions & Tasks

- Check the additional developments yourself – several “overlapping” goals and competing standards!
- What is the main purpose of Zigbee?
- What are key characteristics of Zigbee networks? Differences to Bluetooth (LE)?
- How can wireless systems avoid interference? What does Bluetooth offer?