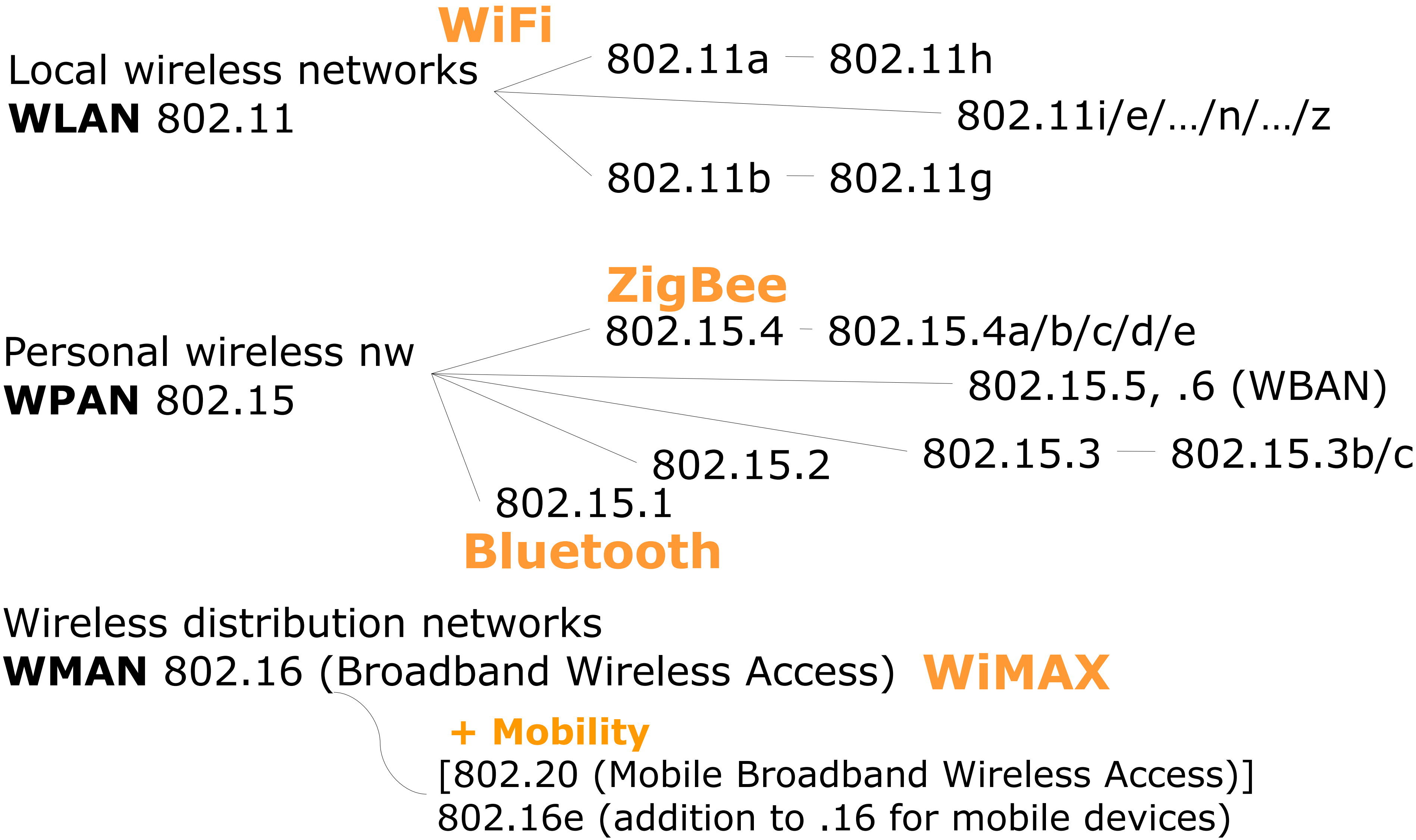
Mobile Communications
Chapter 7: Wireless LANs

- Characteristics
- IEEE 802.11 (PHY, MAC, Roaming, .11a, b, g, h, i, n … z)
- Bluetooth / IEEE 802.15.x
- IEEE 802.16/.20/.21/.22
- RFID
- Comparison

Prof. Jó Ueyama

courtesy from Prof. Dr. Jochen Schiller

Mobile Communication Technology according to IEEE (examples)



WiFi

Local wireless networks
WLAN 802.11

802.11a — 802.11h

802.11i/e/…/n/…/z

802.11b — 802.11g

ZigBee

802.15.4 – 802.15.4a/b/c/d/e

Personal wireless nw
WPAN 802.15

802.15.5, .6 (WBAN)

802.15.3 — 802.15.3b/c

802.15.2

802.15.1

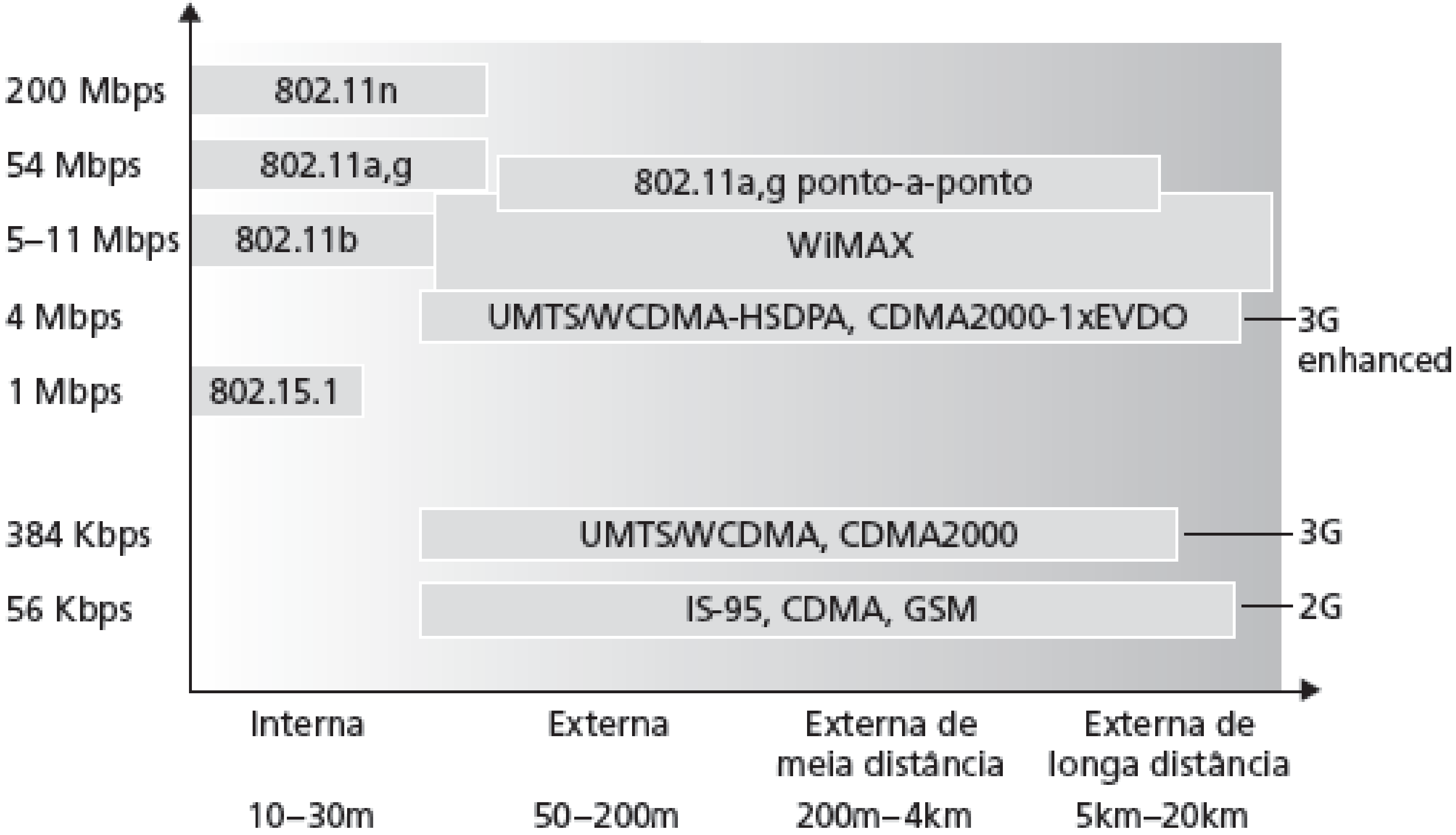
Bluetooth

Wireless distribution networks
WMAN 802.16 (Broadband Wireless Access) **WiMAX**

+ Mobility

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

Main features of the existing wireless technologies



Characteristics of wireless LANs

- Advantages
  - very flexible within the reception 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, fire - or users pulling a plug...
- Disadvantages
  - typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium
  - many proprietary solutions, especially for higher bit-rates, standards take their time (e.g. IEEE 802.11n)
  - products have to follow many national restrictions if working wireless, it takes a vary long time to establish global solutions like, e.g., IMT-2000

Design goals for wireless LANs

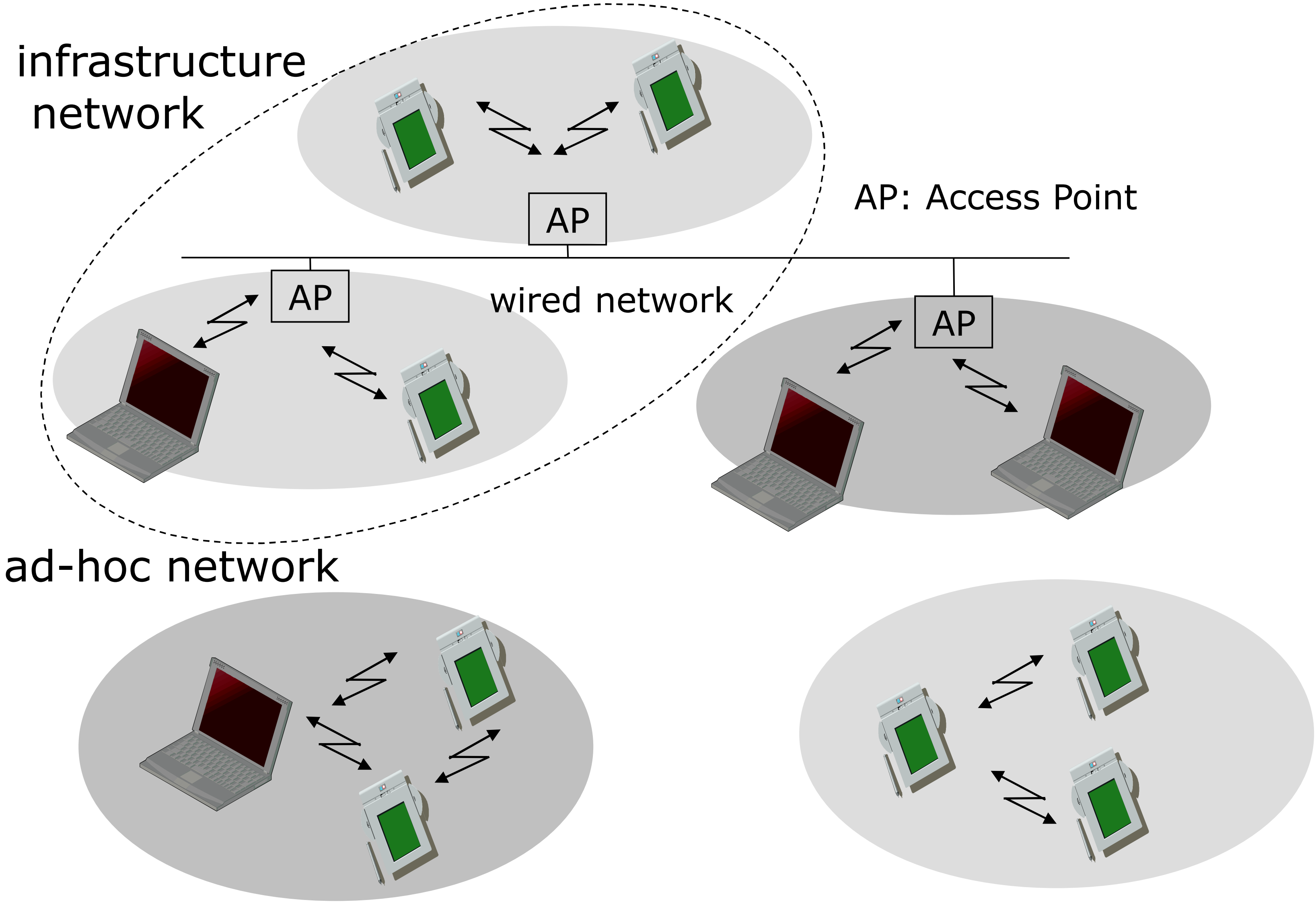
- global, seamless operation
- low power for battery use (e.g. WSNs and cell phones)
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- simplified spontaneous cooperation at meetings
- easy to use for everyone, simple management
- protection of investment in wired networks (i.e. interoperable with wired LANs)
- 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: infrared vs. radio transmission

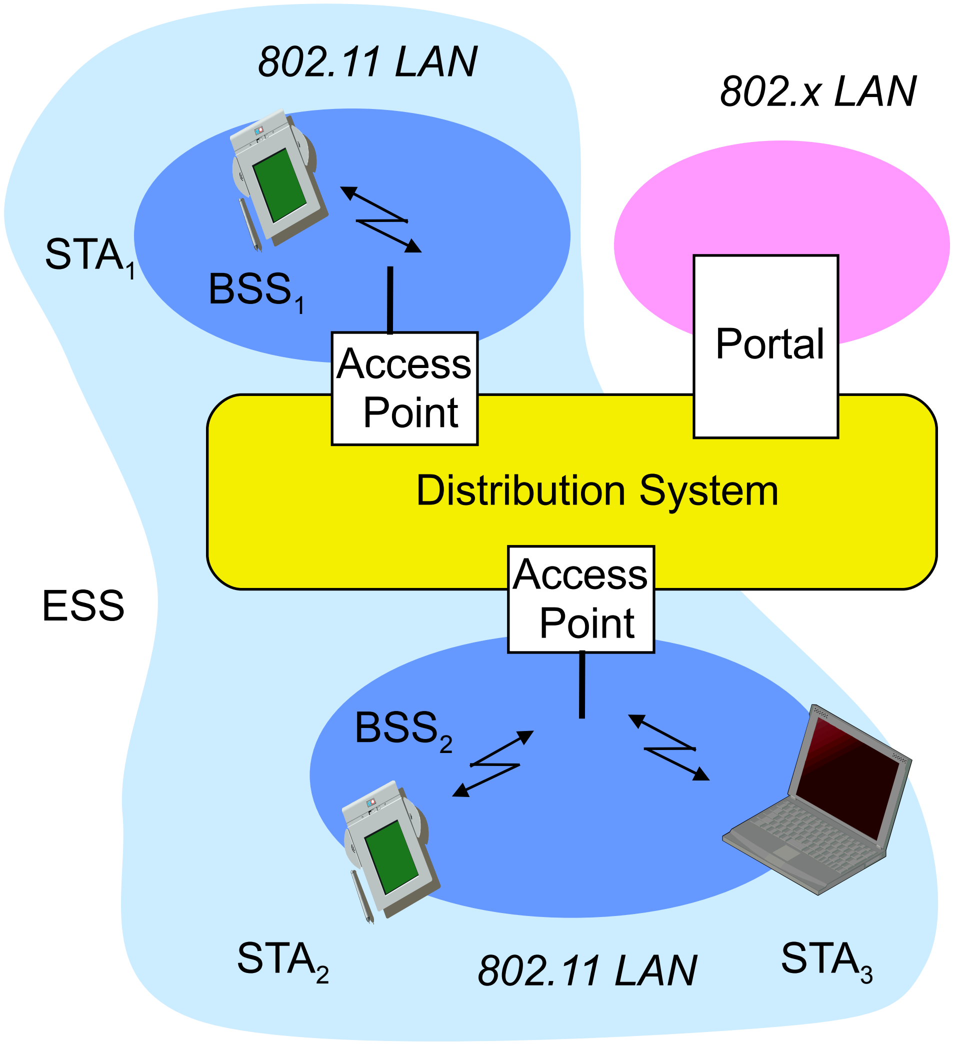
- Infrared
  - uses IR diodes, diffuse light, multiple reflections (walls, furniture etc.)
- Advantages
  - simple, cheap, available in many mobile devices
  - no licenses needed
  - simple shielding possible
- Disadvantages
  - interference by sunlight, heat sources etc.
  - many things shield or absorb IR light
  - low bandwidth
- Example
  - IrDA (Infrared Data Association) interface available everywhere

- Radio
  - typically using the license free ISM band at 2.4 GHz
- Advantages
  - experience from wireless WAN and mobile phones can be used
  - coverage of larger areas possible (radio can penetrate walls, furniture etc.)
- Disadvantages
  - very limited license free frequency bands
  - shielding more difficult, interference with other electrical devices
- Example
  - Many different products

Comparison: infrastructure vs. ad-hoc networks

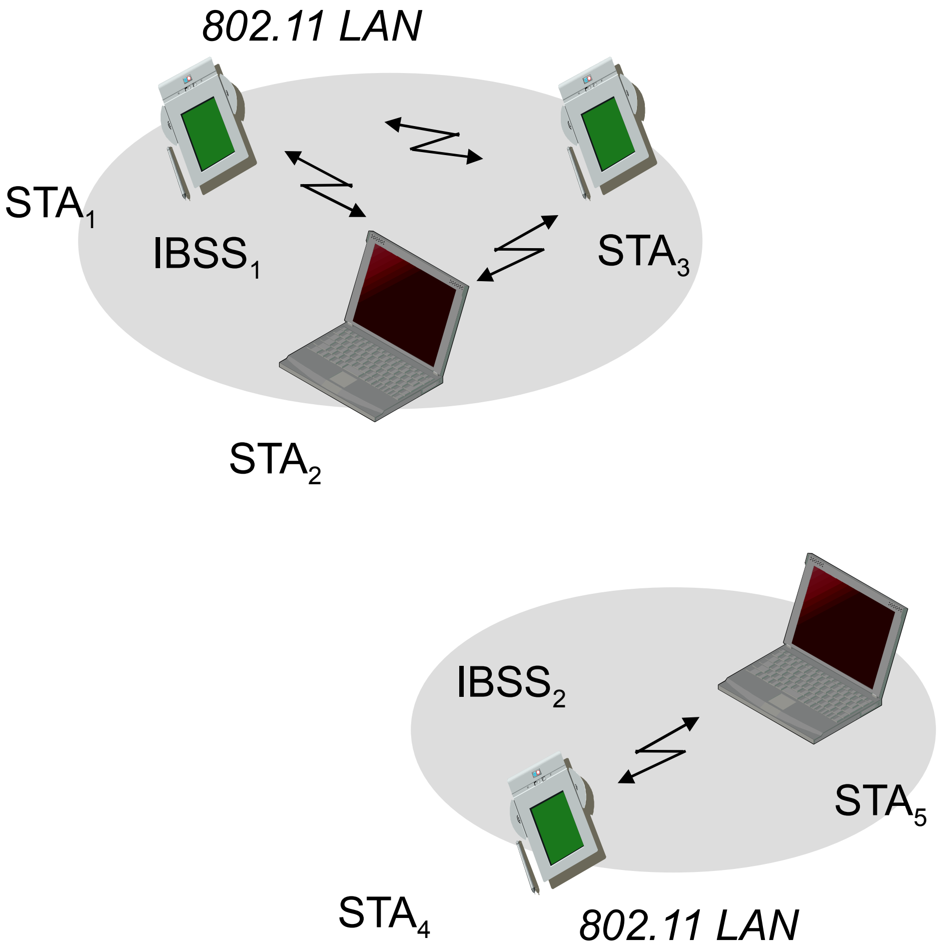


802.11 - Architecture of an infrastructure network



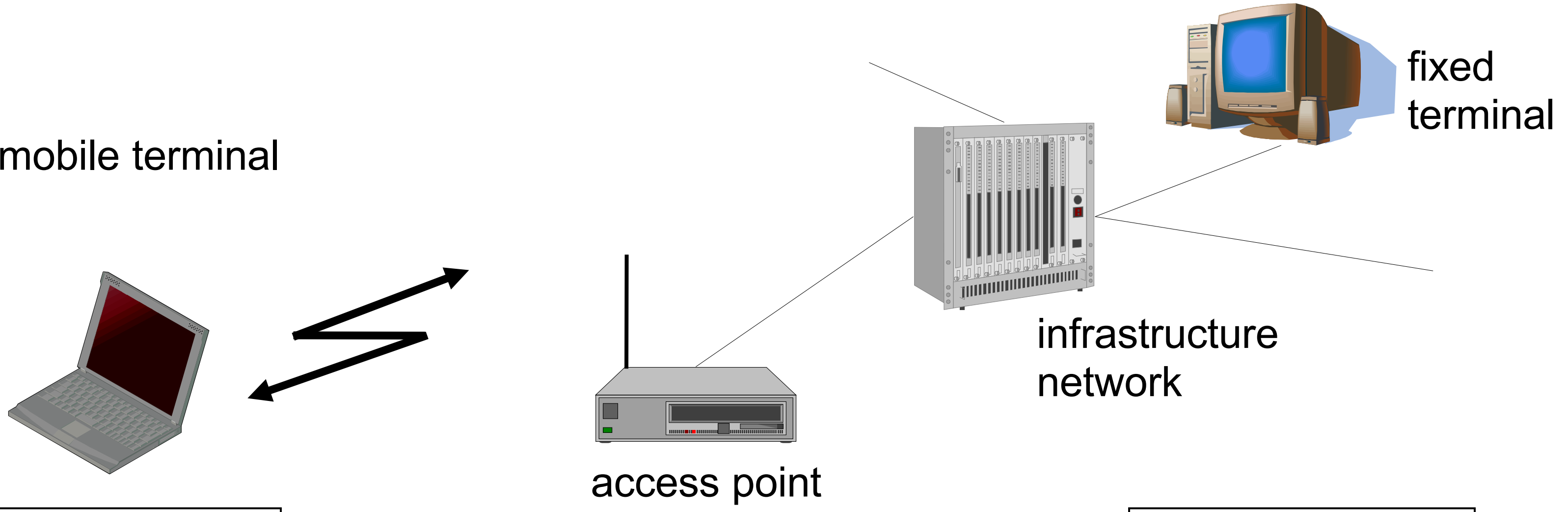
- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to 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

IEEE standard 802.11

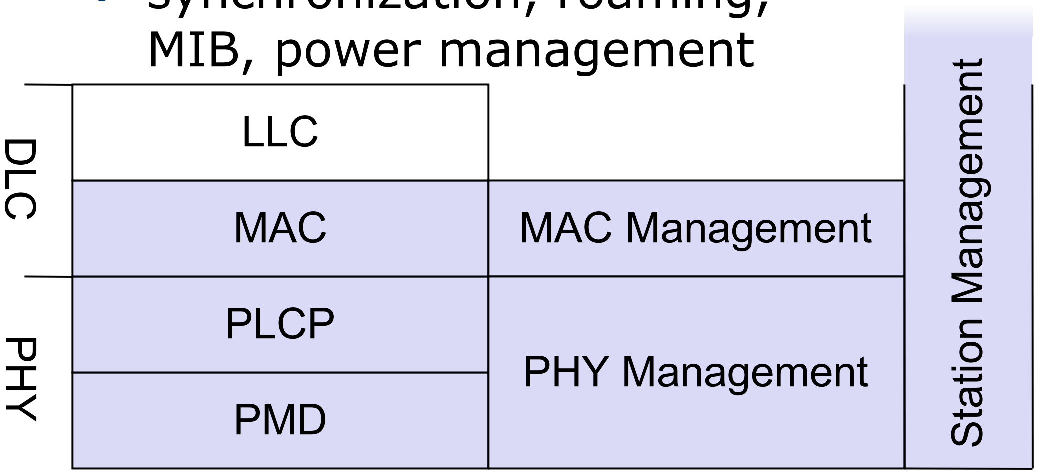


LLC – Logical Link Control – interface between different medias

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



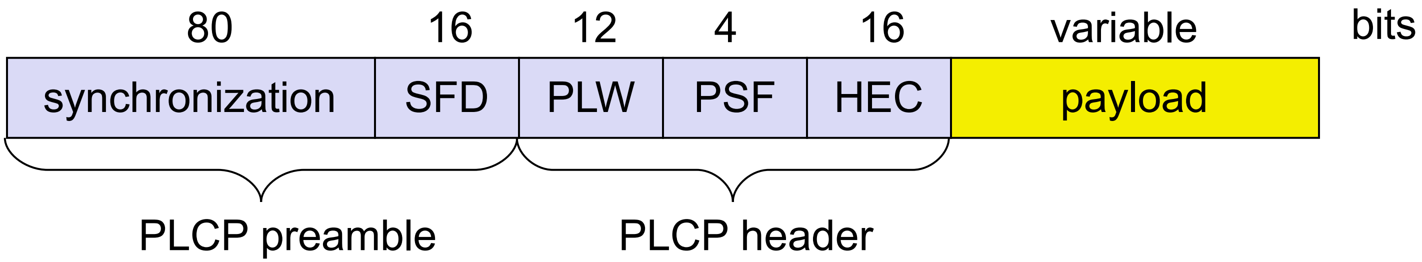
- PHY Management includes
  - PLCP Physical Layer Convergence Protocol
    - clear channel assessment signal (carrier sense)
    - Medium currently idle?
  - PMD Physical Medium Dependent
    - modulation, coding, transforms bits into signals
- Station Management
  - coordination of all management functions

802.11 - Physical layer (legacy)

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading
  - Frequency multiplexing
- DSSS (Direct Sequence Spread Spectrum)
  - Multiplexes by code (i.e. using a chipping code)
  - Implementation is more complex than FHHS
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - DATA XOR chipping code
- Infrared
  - Wavelength around 850-950 nm, diffuse light, typ. 10 m range
  - uses near visible light
  - carrier detection, up to 4Mbits/s data rate

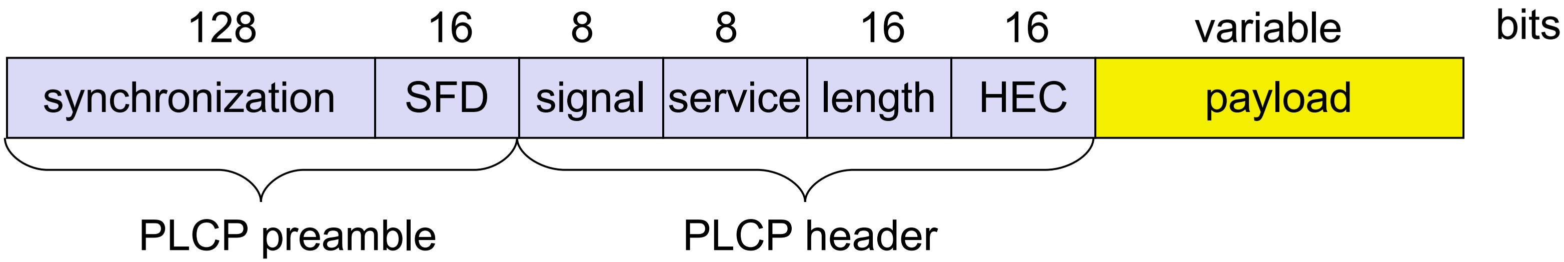
FHSS PHY packet format (legacy)

- Synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - data rate of the payload (0000 -> the lowest data rate)
- HEC (Header Error Check)
  - checksum with the standard ITU-T polynomial generator



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)
  - protected by checksum using ITU-T standard polynomial error check



802.11 - MAC layer I - DFWMAC

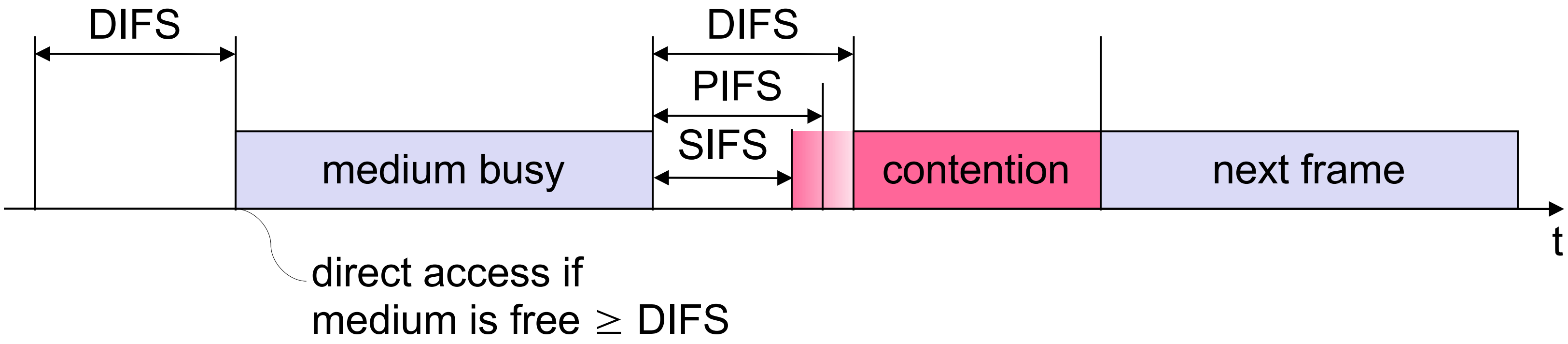
- MAC layer has to fulfill several tasks including:
  - control medium access
  - support for roaming
  - authentication
  - power conservation
- In summary, it has two key tasks:
  - traffic services
  - access control

802.11 - MAC layer I - DFWMAC

- Traffic services (two implementations)
  - Asynchronous Data Service (mandatory)
    - exchange of data packets based on “best-effort”
    - support of broadcast and multicast
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)
- Access methods
  - DFWMAC-DCF CSMA/CA (mandatory)
    - collision avoidance via randomized „back-off“ mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  - DFWMAC-DCF w/ RTS/CTS (optional)
    - Distributed Foundation Wireless MAC
    - avoids hidden terminal problem
  - DFWMAC- PCF (optional)
    - access point polls terminals according to a list

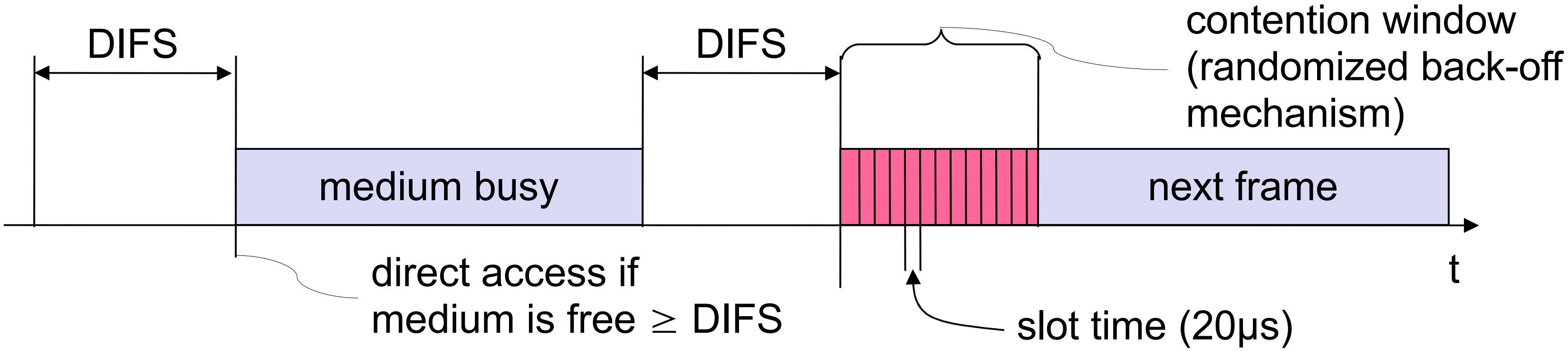
802.11 - MAC layer II

- Priorities
  - defined through different inter frame spaces
  - no guaranteed, hard priorities
  - SIFS (Short Inter Frame Spacing)
    - highest priority, for ACK, CTS, polling response
  - PIFS (PCF IFS)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF Inter frame spacing)
    - lowest priority, for asynchronous data service

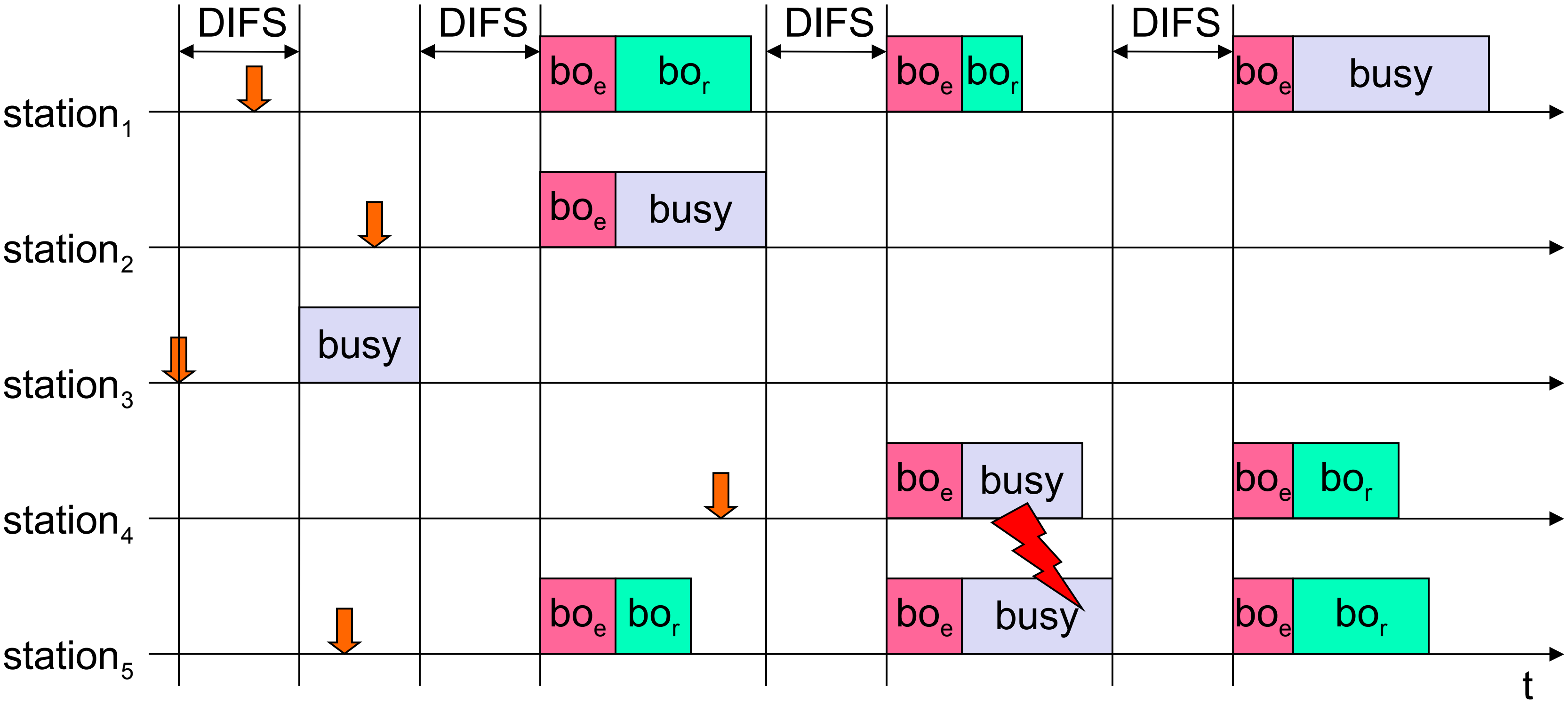


802.11 - CSMA/CA access method I

- 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)



802.11 - competing stations - simple version



busy — medium not idle (frame, ack etc.)

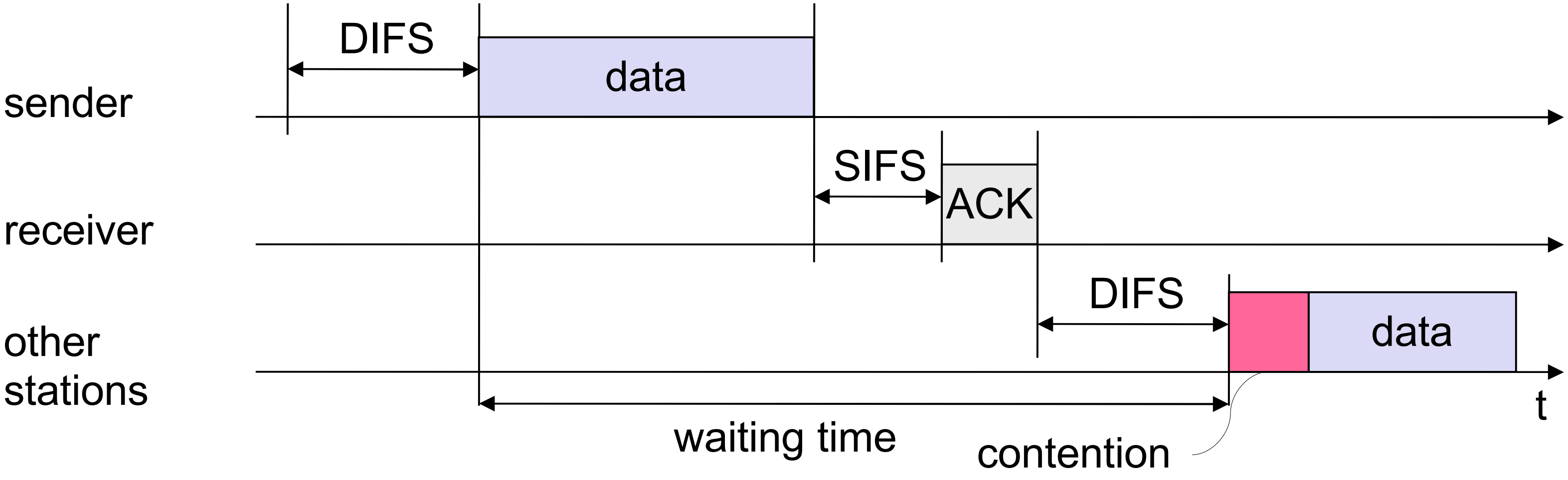
⇩ — packet arrival at MAC

bo$_e$ — elapsed backoff time

bo$_r$ — residual backoff time

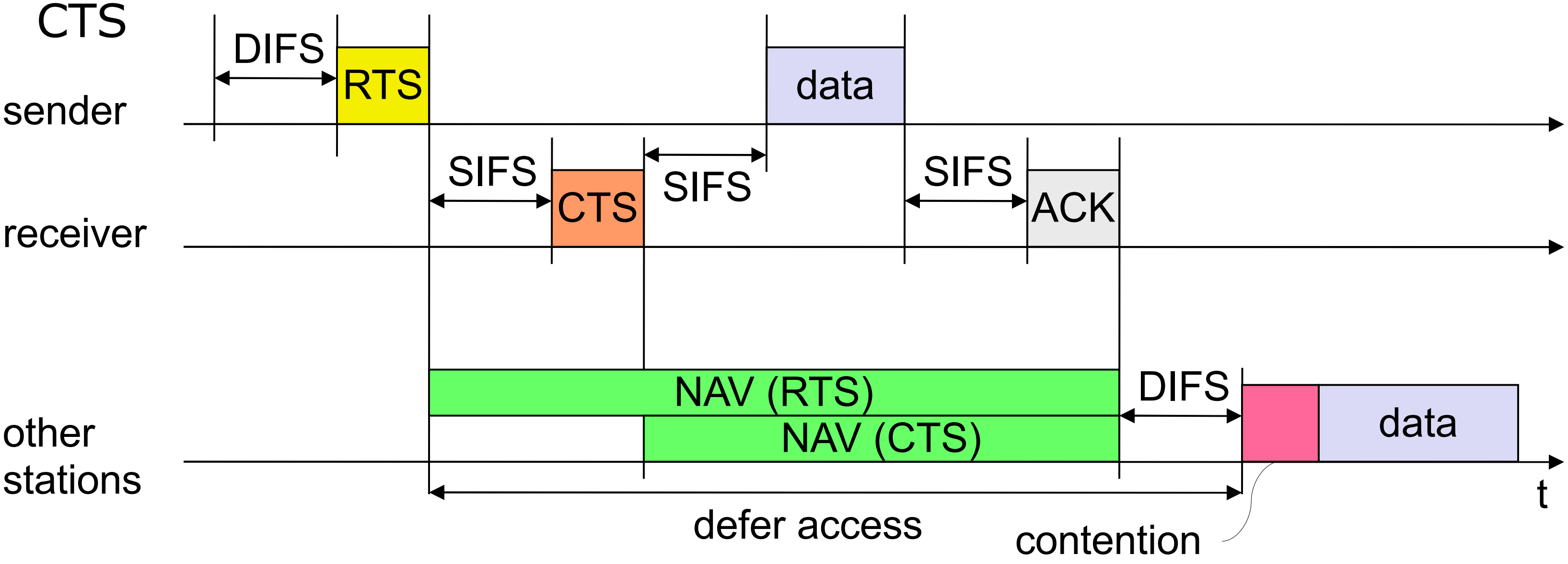
802.11 - CSMA/CA access method II

- 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 (CRC)
  - automatic retransmission of data packets in case of transmission errors

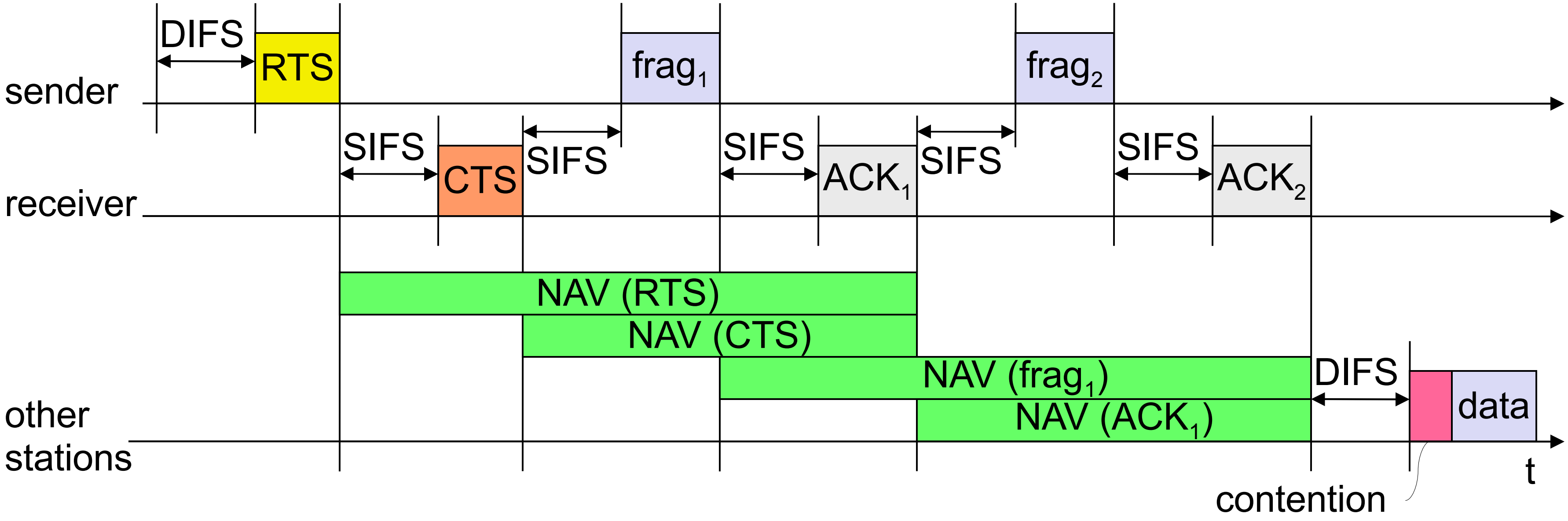


802.11 - DFWMAC

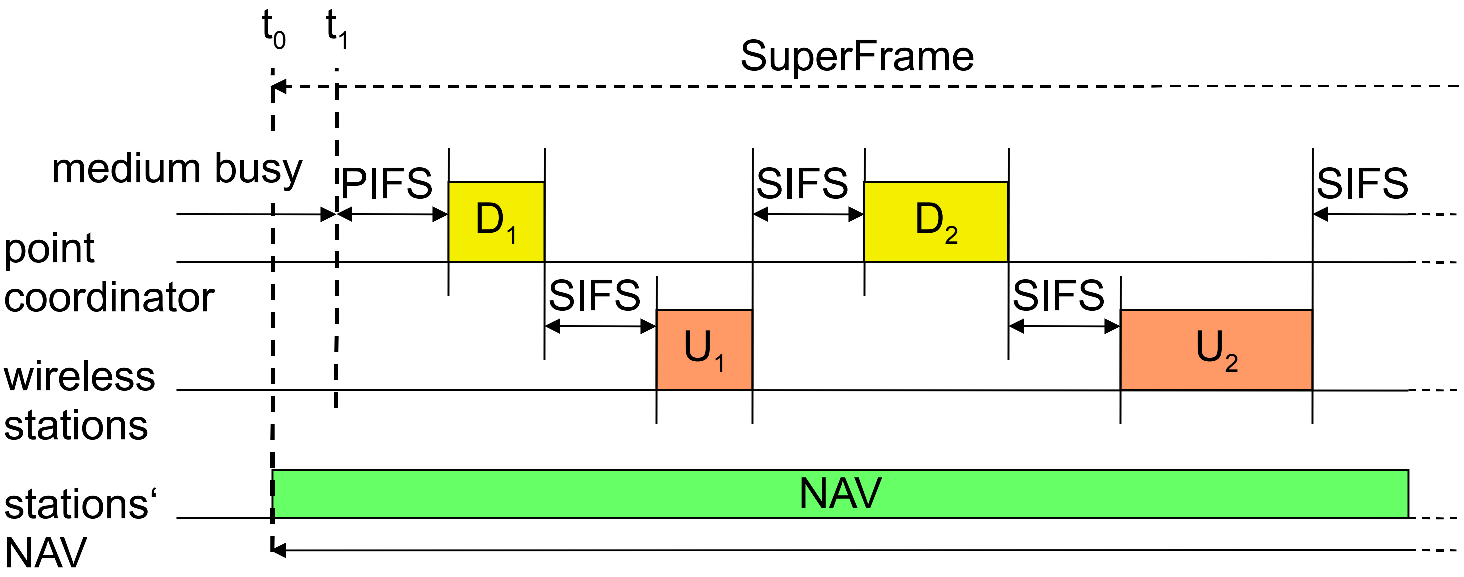
- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement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



Fragmentation



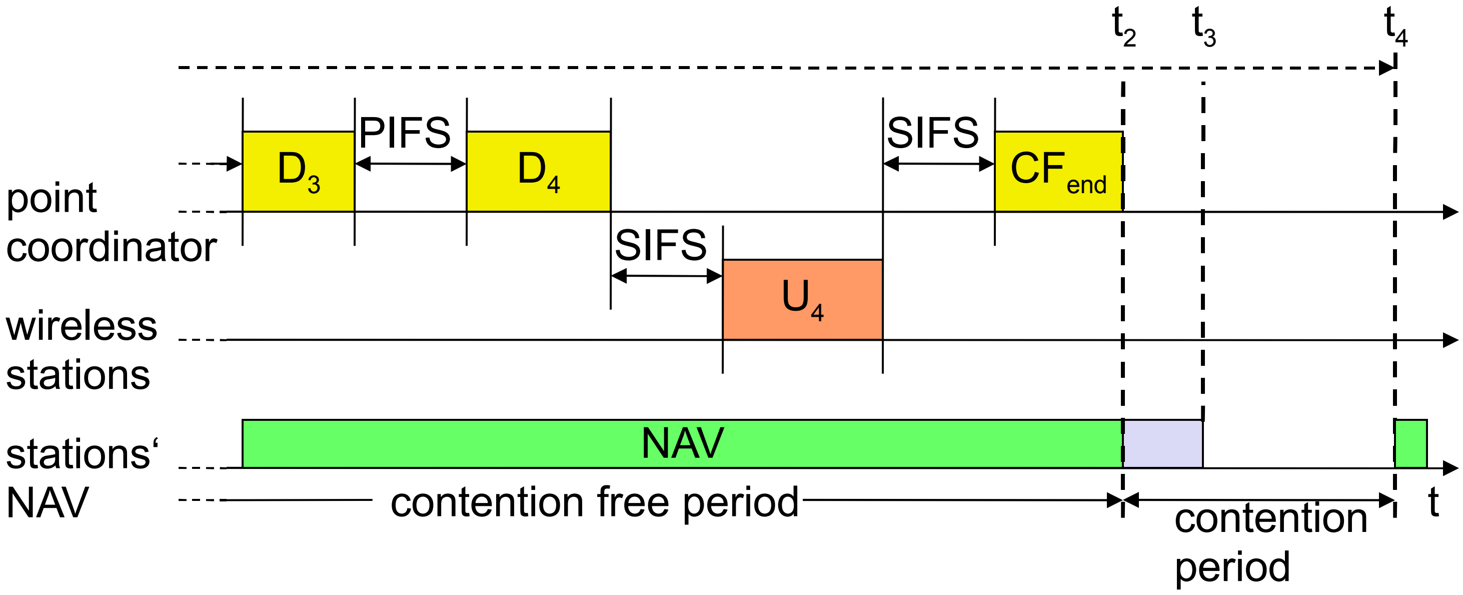
DFWMAC-PCF I (almost never used)



D – downstream data
U – upstram data

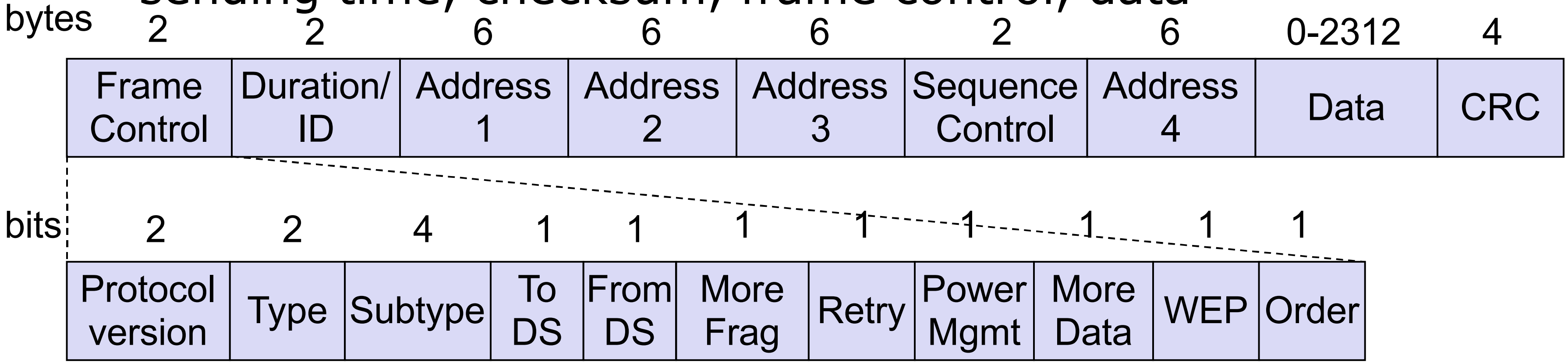
DFWMAC-PCF II

D – downstream data
U – upstram data



802.11 - Frame format

- Types
  - control, management (e.g. beacon) and 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



bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

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	WEP	Order

MAC address format

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

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address
Address1 – destination
Address2 – source (ACK will be sent to)
Address3 – filter (often it will carry BSSID addr)
Address4 – Address of the source Access Point

Special Frames: ACK, RTS, CTS

- Acknowledgement

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

- Request To Send

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

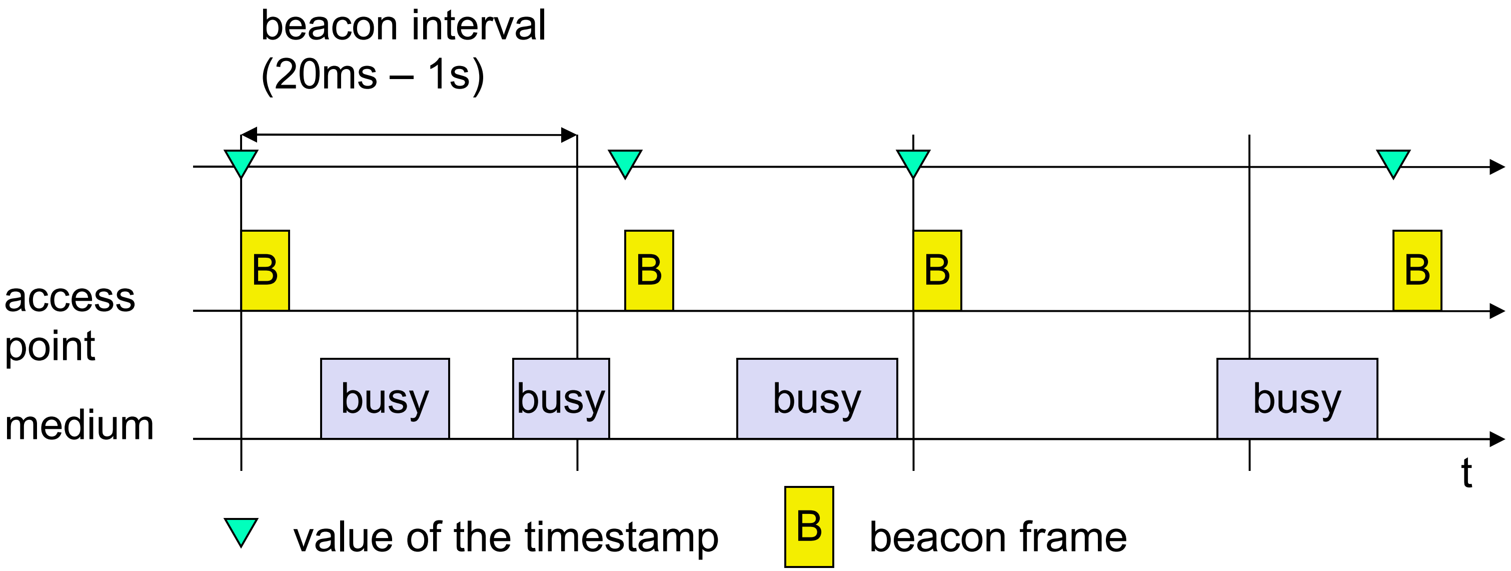
- Clear To Send

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

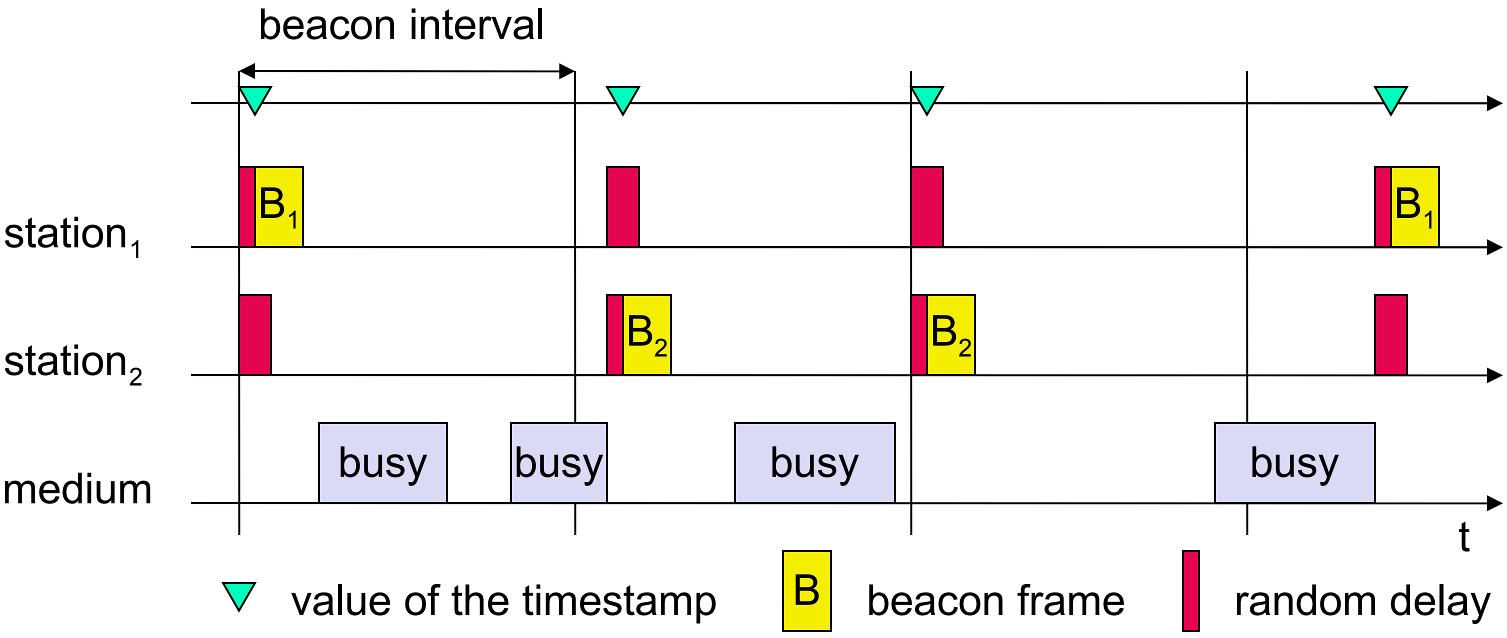
802.11 - MAC management

- 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)



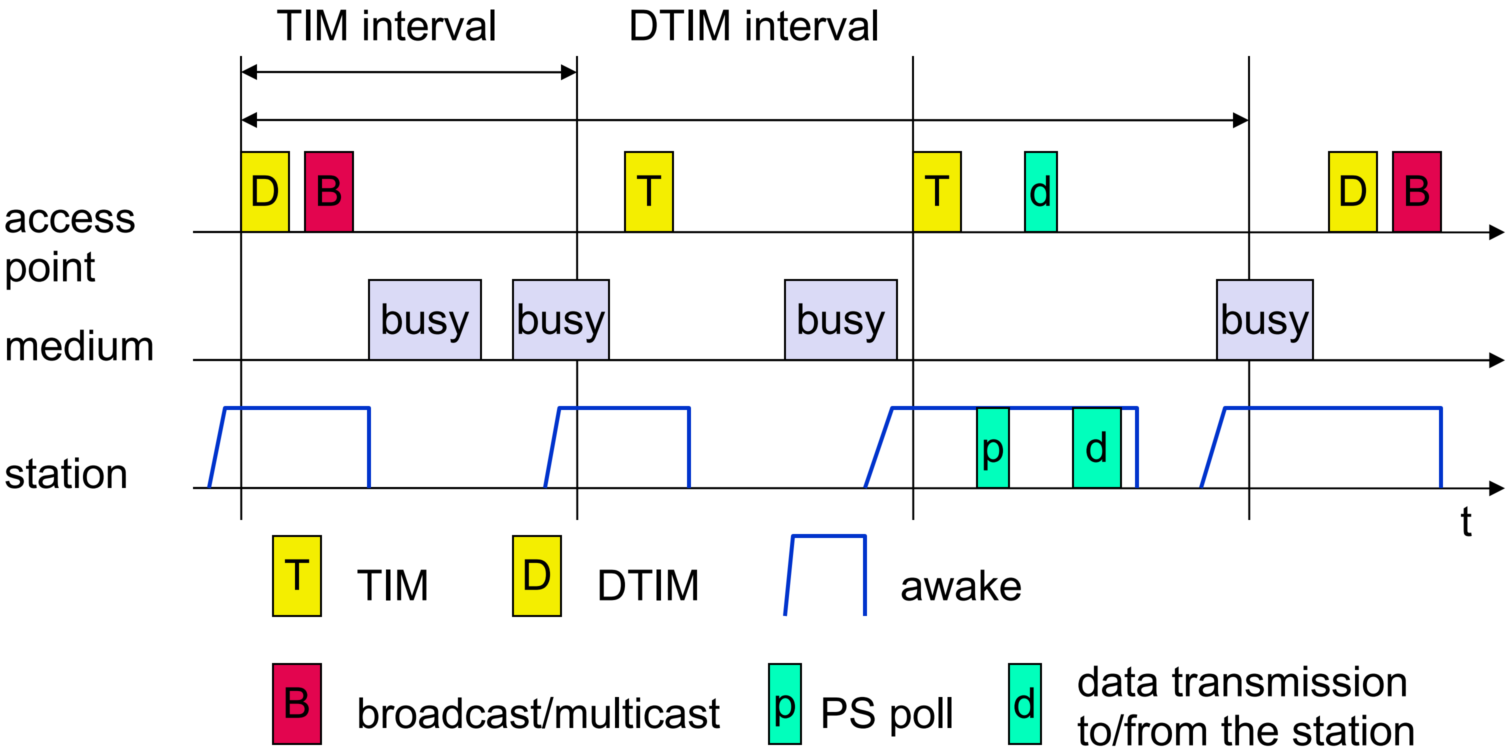
Synchronization using a Beacon (ad-hoc)



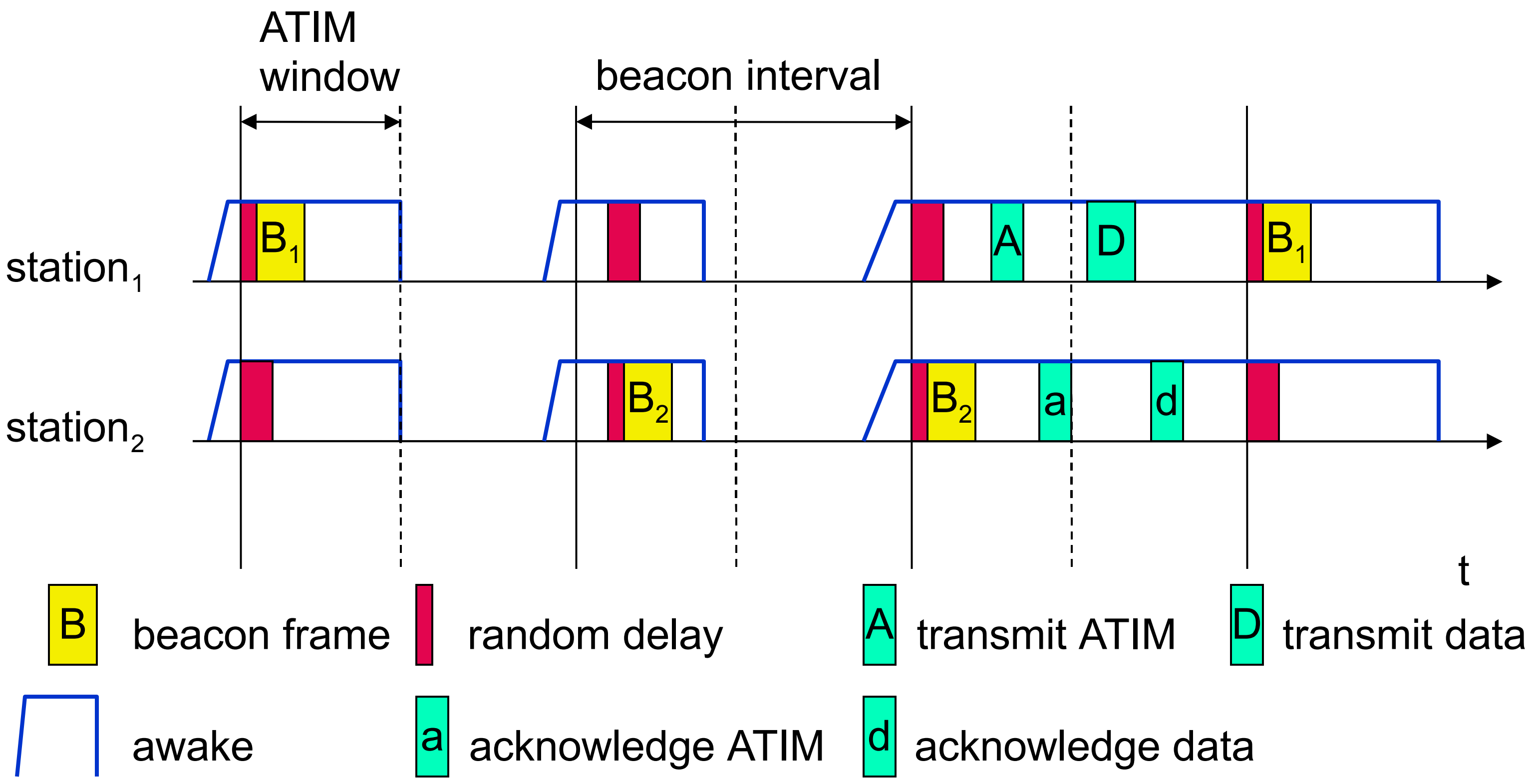
Power management

- 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)
  - new method in 802.11e replacing above schemes

Power saving with wake-up patterns (infrastructure)



Power saving with wake-up patterns (ad-hoc)



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
- Fast roaming – 802.11r
  - e.g. for vehicle-to-roadside networks

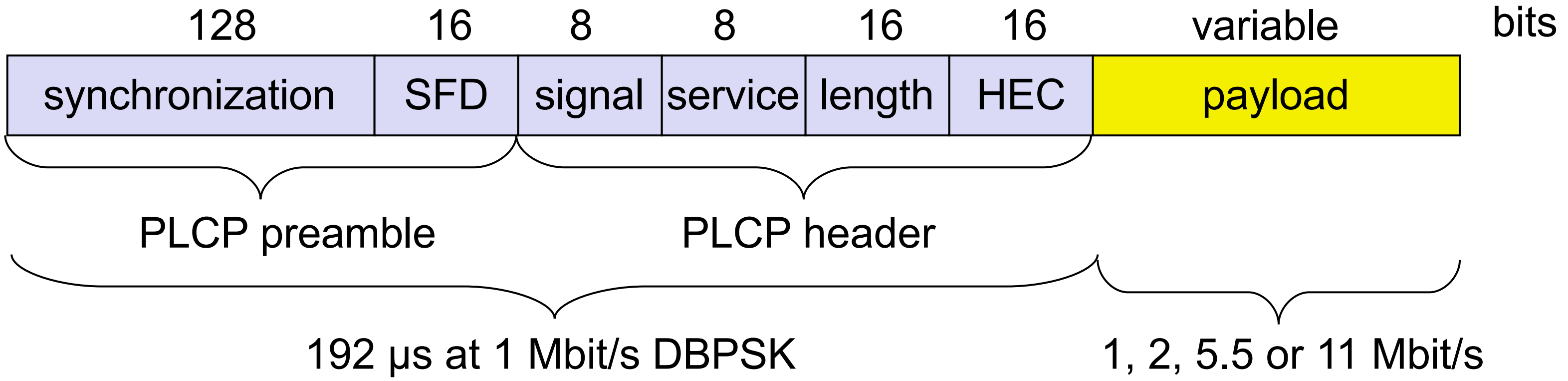
WLAN: IEEE 802.11b

- Data rate
  - 1, 2, 5.5, 11 Mbit/s, depending on SNR
  - User data rate max. approx. 6 Mbit/s
- Transmission range
  - 300m outdoor, 30m indoor
  - Max. data rate ~10m indoor
- Frequency
  - DSSS, 2.4 GHz ISM-band
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Many products, many vendors

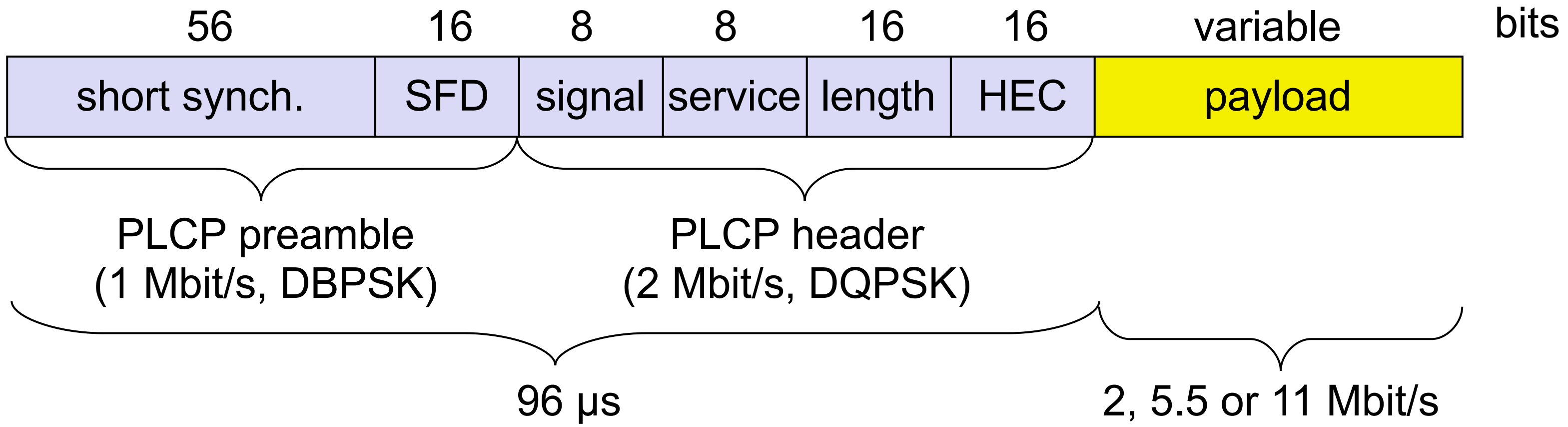
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. Best effort, no guarantees (unless polling is used, limited support in products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
  - Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11b – PHY frame formats

Long PLCP PPDU format

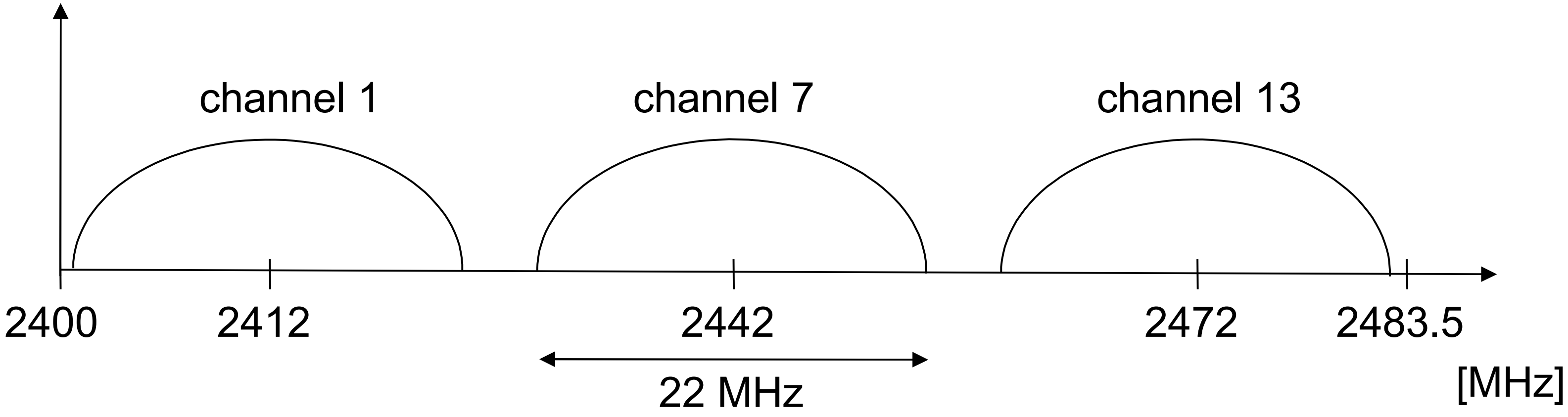


Short PLCP PPDU format (optional)

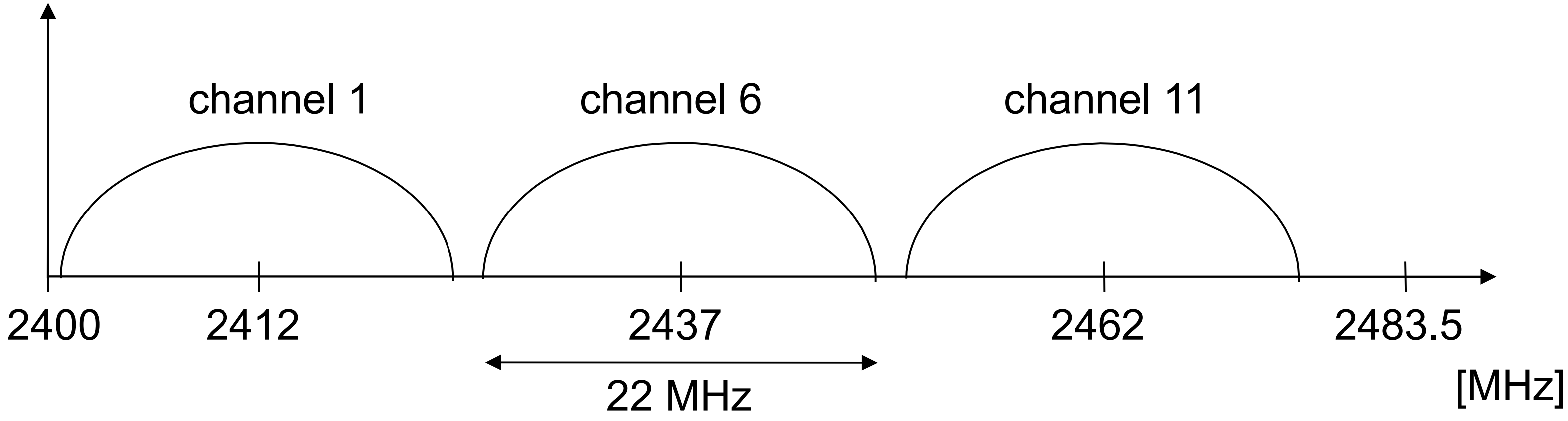


Channel selection (non-overlapping)

Europe (ETSI)



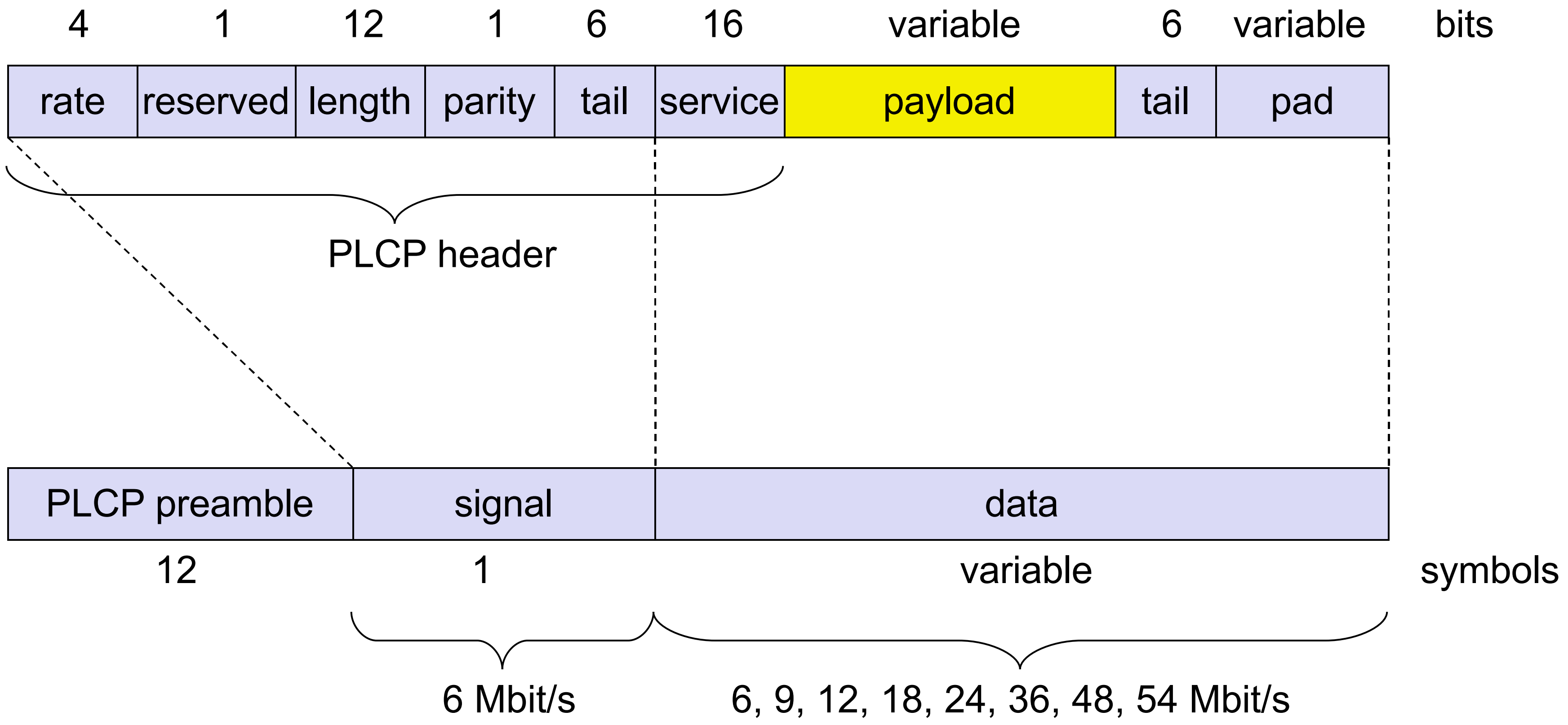
US (FCC)/Canada (IC)



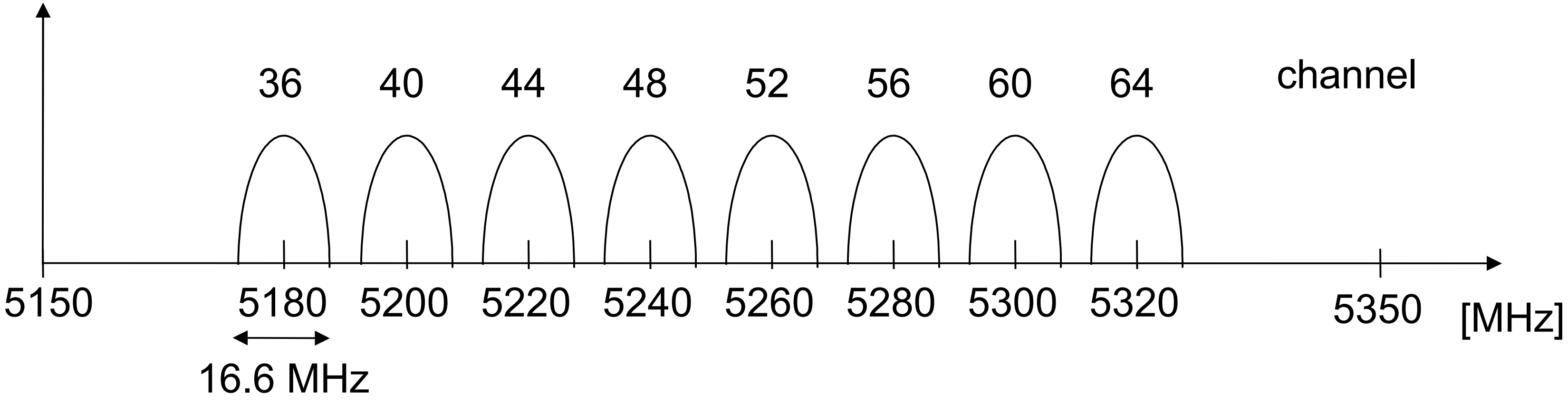
WLAN: IEEE 802.11a

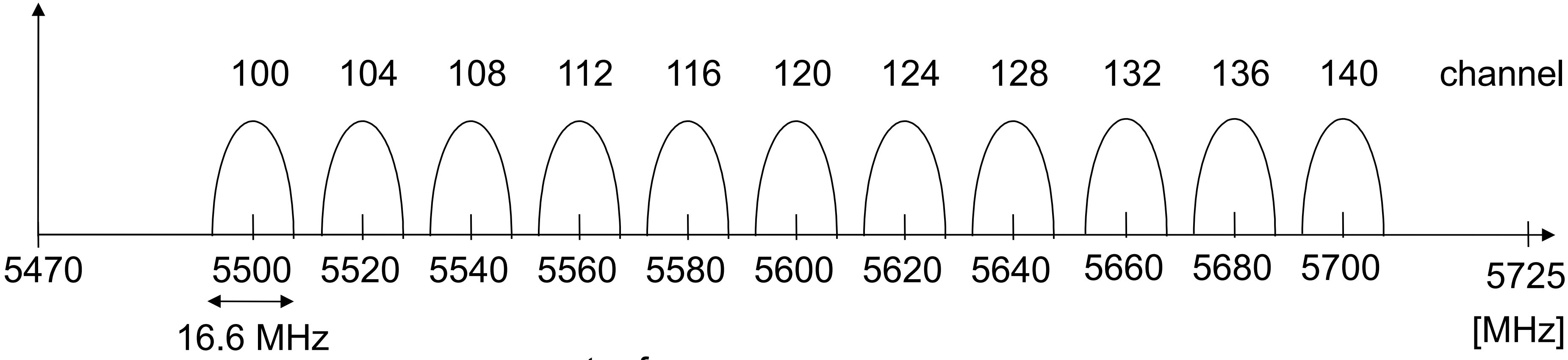
- Data rate
  - 6, 9, 12, 18, 24, 36, 48, 54 Mbit/s, depending on SNR
  - User throughput (1500 byte packets): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - 6, 12, 24 Mbit/s mandatory
- Transmission range
  - 100m outdoor, 10m indoor
    - E.g., 54 Mbit/s up to 5 m, 48 up to 12 m, 36 up to 25 m, 24 up to 30m, 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
- Security
  - Limited, WEP insecure, SSID
- Availability
  - Some products, some vendors
- Connection set-up time
  - Connectionless/always on
- Quality of Service
  - Typ. best effort, no guarantees (same as all 802.11 products)
- Manageability
  - Limited (no automated key distribution, sym. Encryption)
- Special Advantages/Disadvantages
  - Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
  - Disadvantage: stronger shading due to higher frequency, no QoS

IEEE 802.11a – PHY frame format



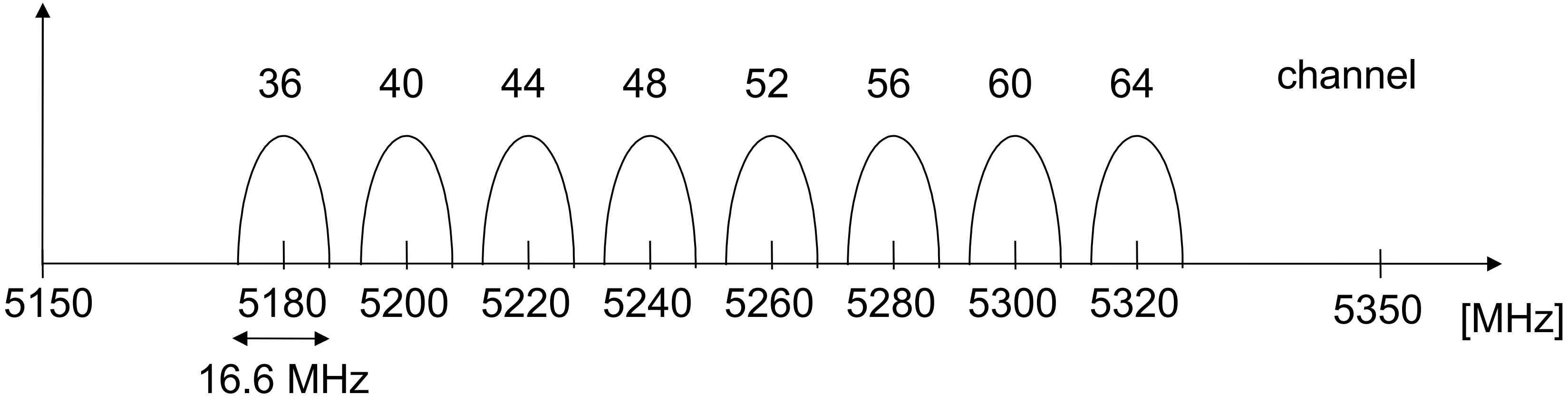
Operating channels of 802.11a in Europe

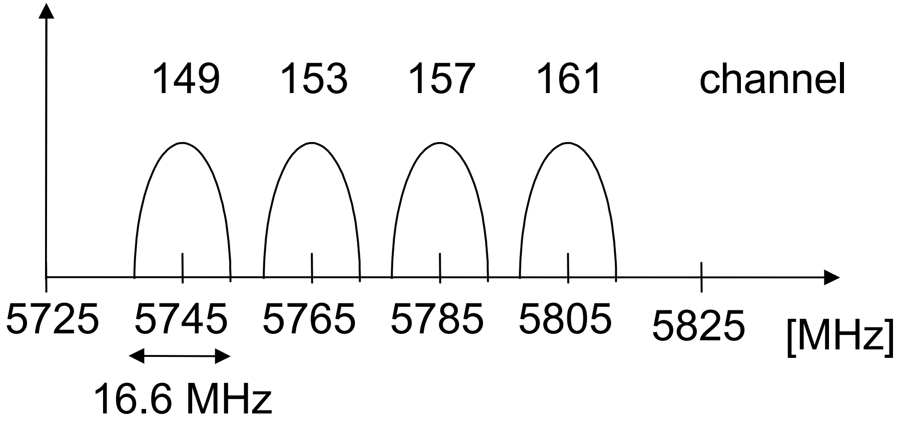




center frequency =
5000 + 5*channel number [MHz]

Operating channels for 802.11a / US U-NII

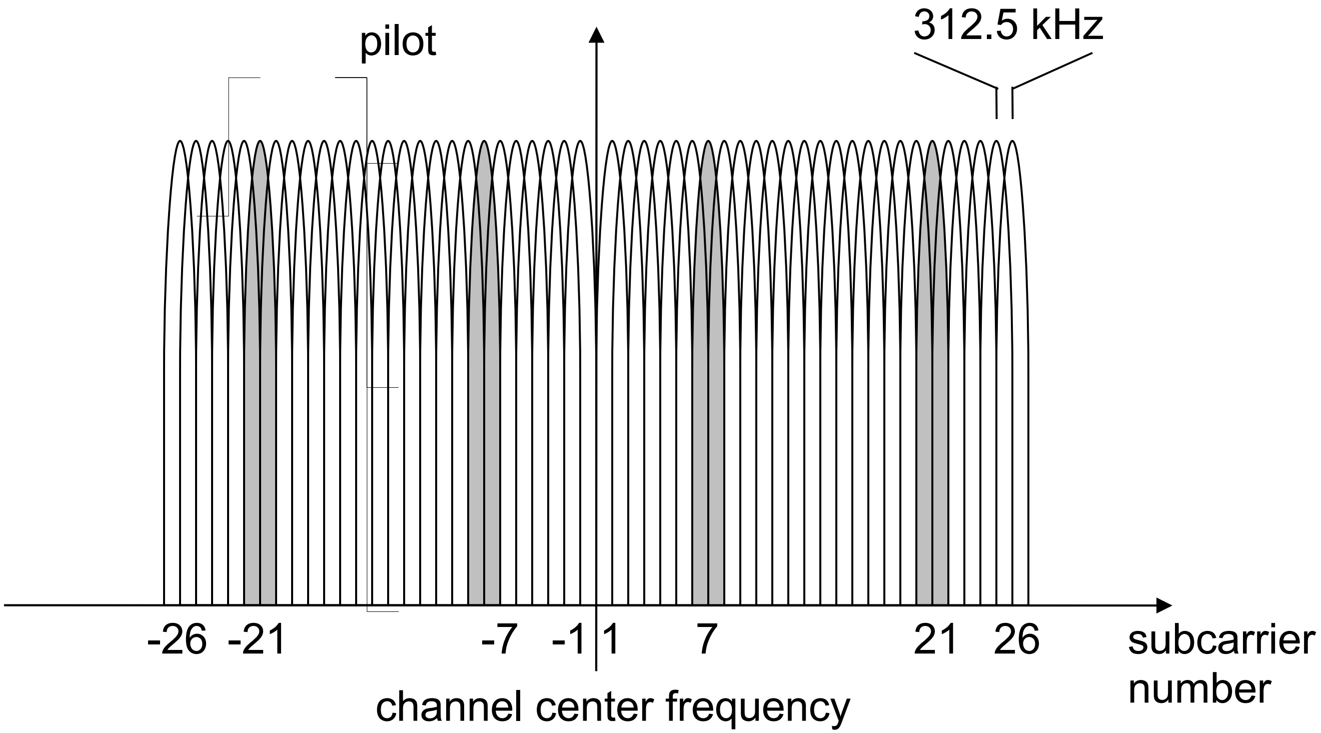




center frequency =
5000 + 5*channel number [MHz]

OFDM in IEEE 802.11a

- OFDM with 52 used subcarriers (64 in total)
  - 48 data + 4 pilot
    - (plus 12 virtual subcarriers)
  - 312.5 kHz spacing


pilot
312.5 kHz
-26
-21
-7
-1
1
7
21
26
subcarrier number
channel center frequency