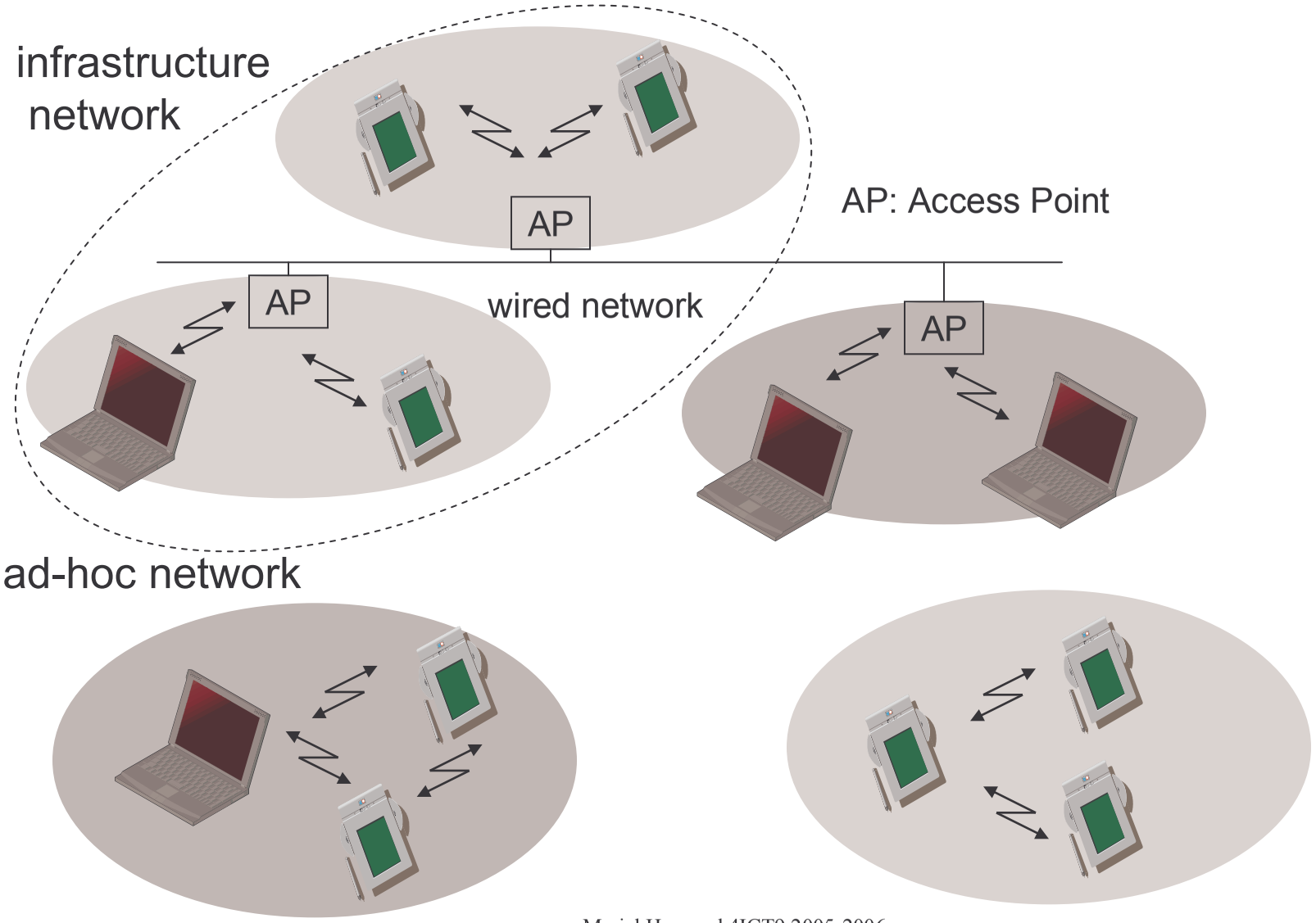
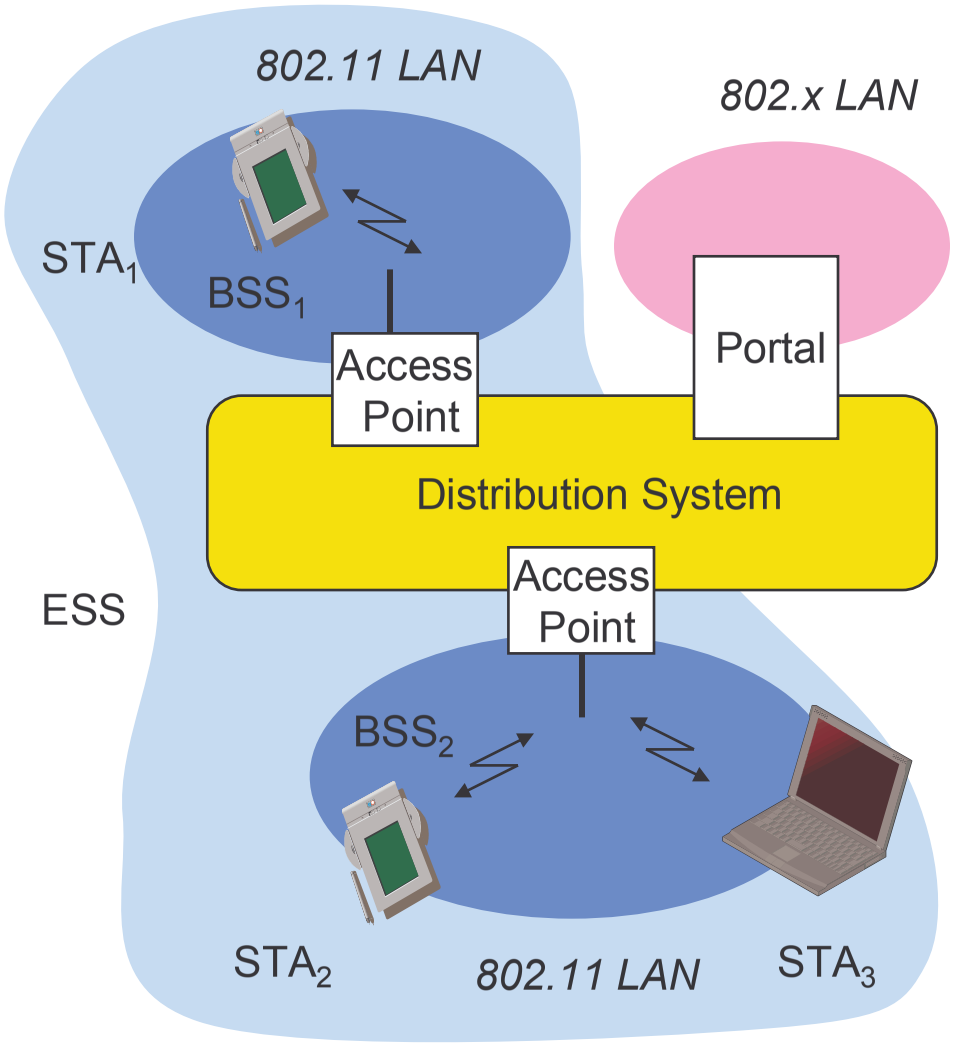
IEEE 802.11 Comparison: infrastructure vs. ad-hoc networks



IEEE 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

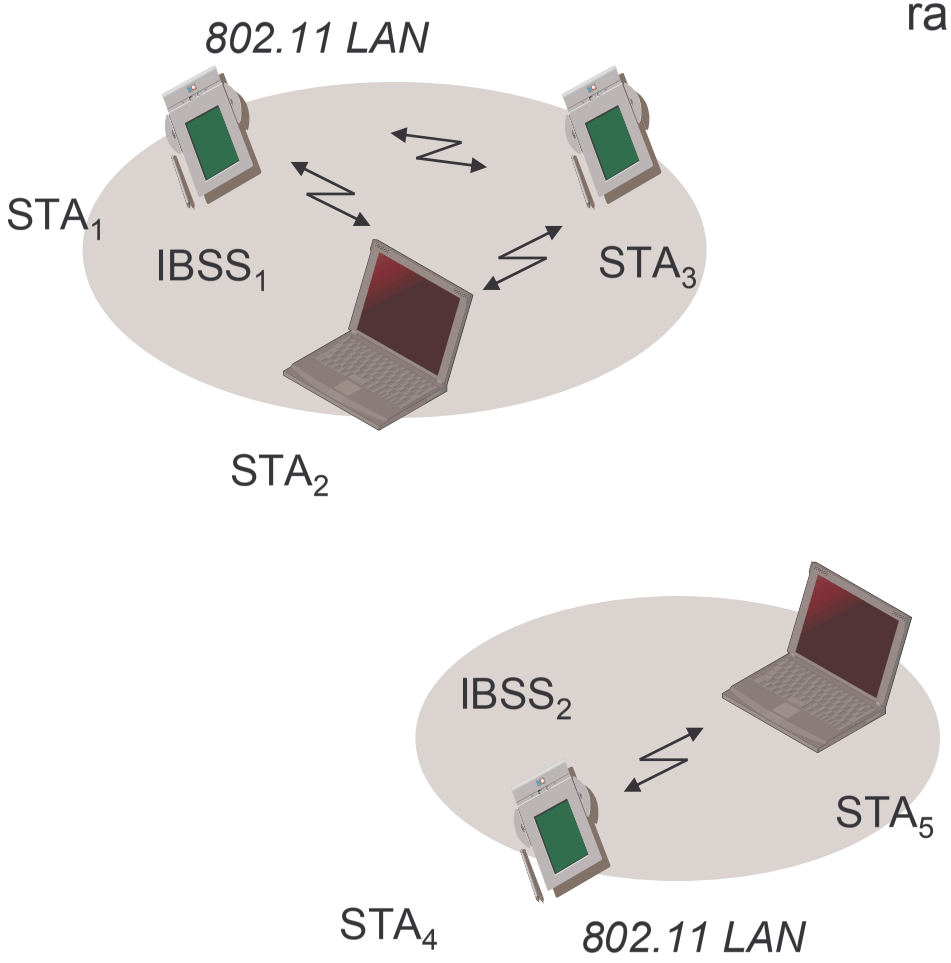
Portal

- bridge to other (wired) networks

Distribution System

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

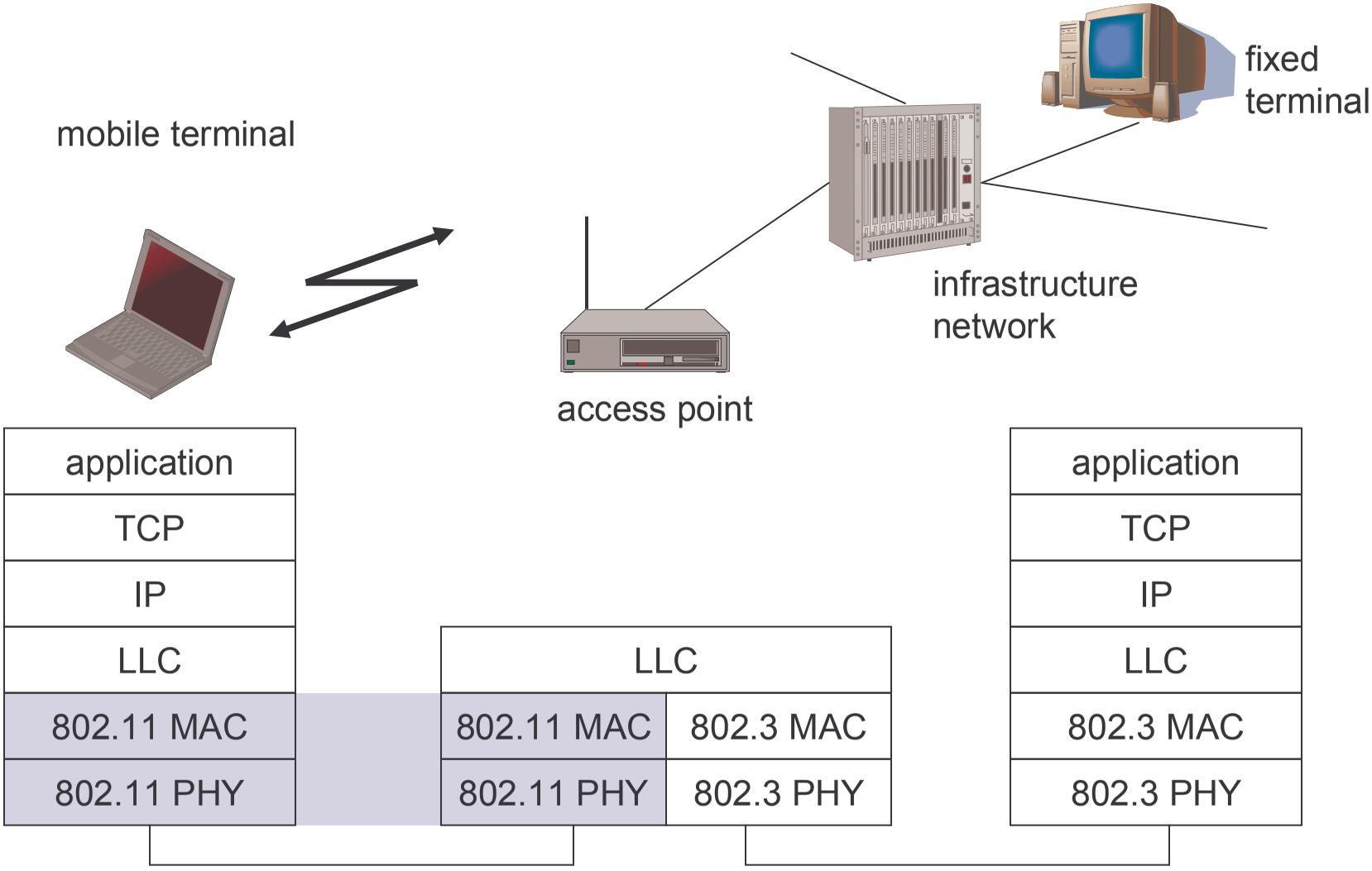
IEEE 802.11 Architecture of an ad-hoc network



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



IEEE 802.11 Layers and functions

MAC
- access mechanisms, fragmentation, encryption

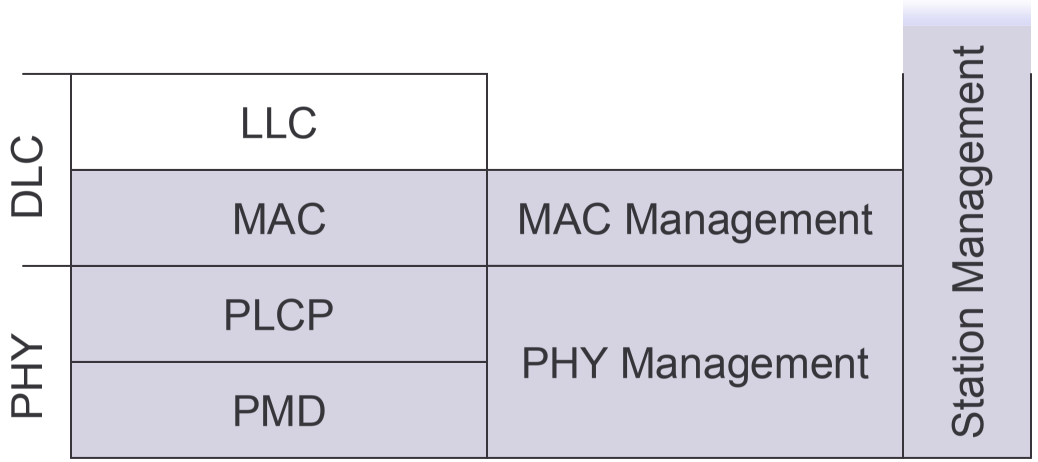
MAC Management
- synchronization, roaming, MIB, power management

PLCP Physical Layer Convergence Protocol
- clear channel assessment signal (carrier sense)

PMD Physical Medium Dependent
- modulation, coding

PHY Management
- channel selection, MIB

Station Management
- coordination of all management functions



IEEE 802.11

Physical layer (classical)

3 versions: 2 radio (typically 2.4 GHz), 1 IR

- data rates 1 or 2 Mbit/s

FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength, typ. 1 Mbit/s
- min. 2.5 frequency hops/s (USA), two-level GFSK modulation

DSSS (Direct Sequence Spread Spectrum)

- 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

- 850-950 nm, diffuse light, typical 10 m range
- carrier detection, energy detection, synchronization

FHSS PHY packet format

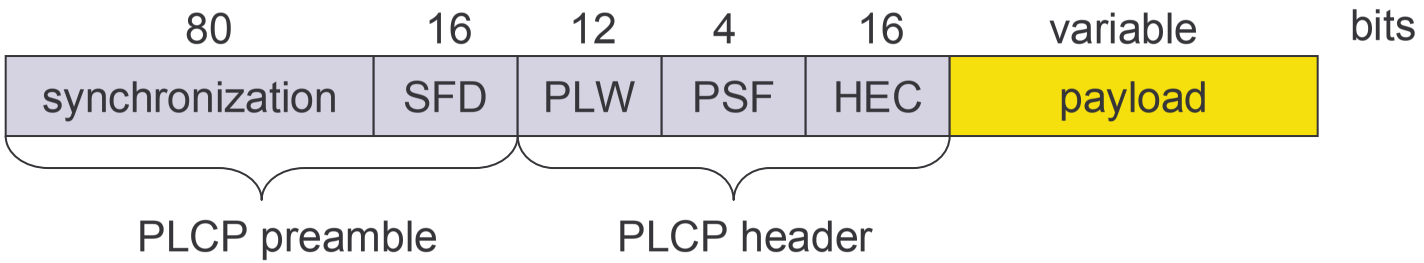
Synchronization
- synch with 010101... pattern

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 of payload (1 or 2 Mbit/s)

HEC (Header Error Check)
- CRC with $x^{16}+x^{12}+x^{5}+1$



DSSS PHY packet format

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

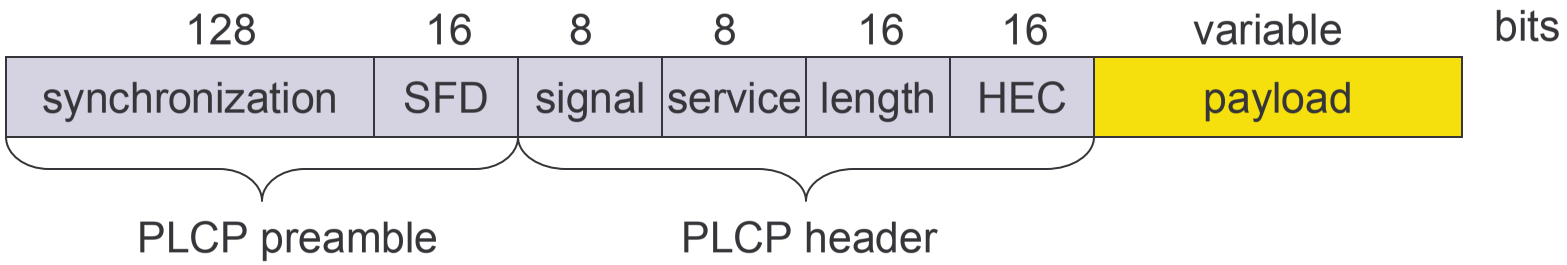
SFD (Start Frame Delimiter)
- 1111001110100000

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, $x^{16}+x^{12}+x^{5}+1$



MAC layer I - DFWMAC

Traffic services

- 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)

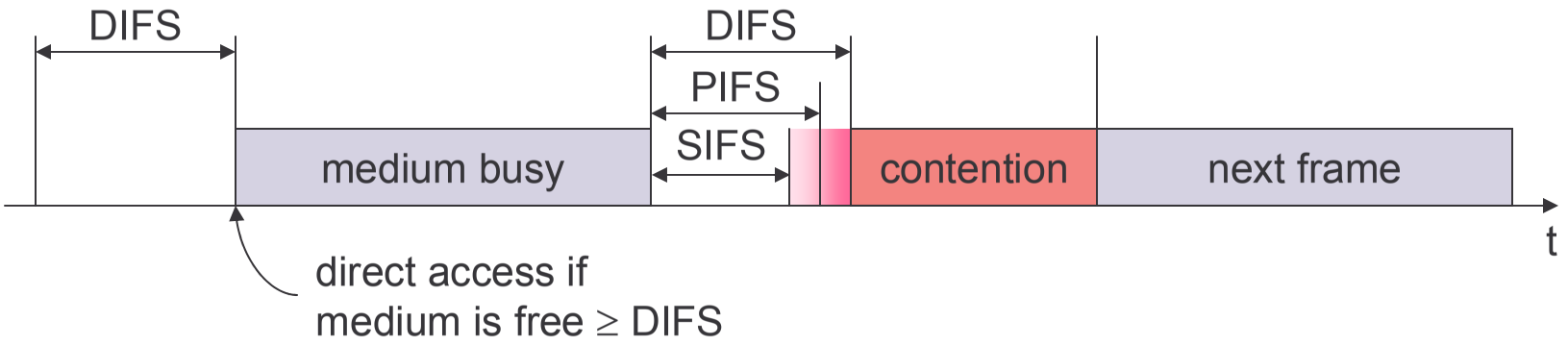
Access methods

- 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

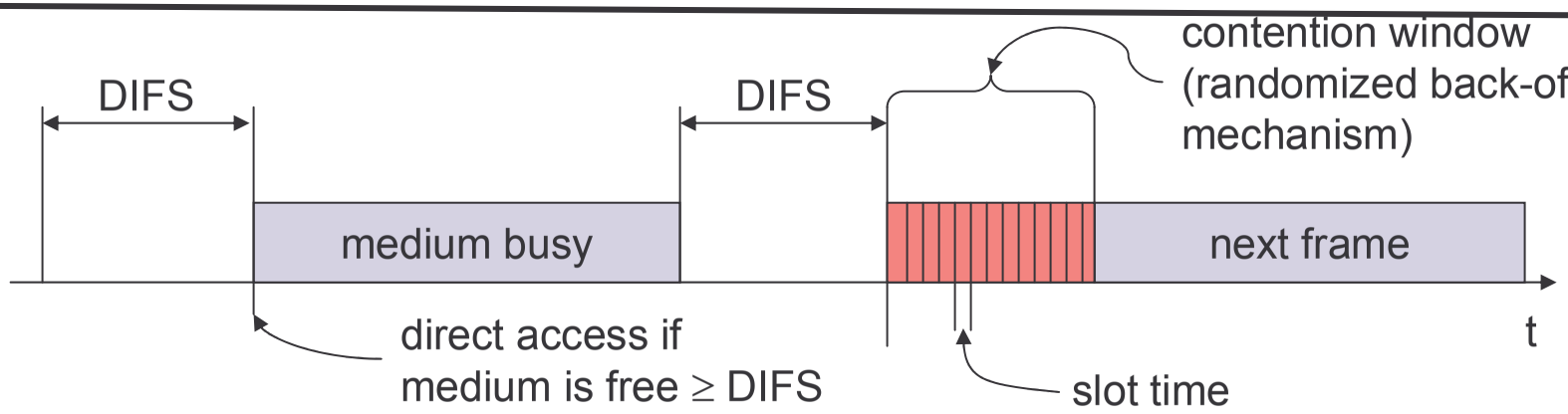
MAC layer II

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, Distributed Coordination Function IFS)
  - lowest priority, for asynchronous data service

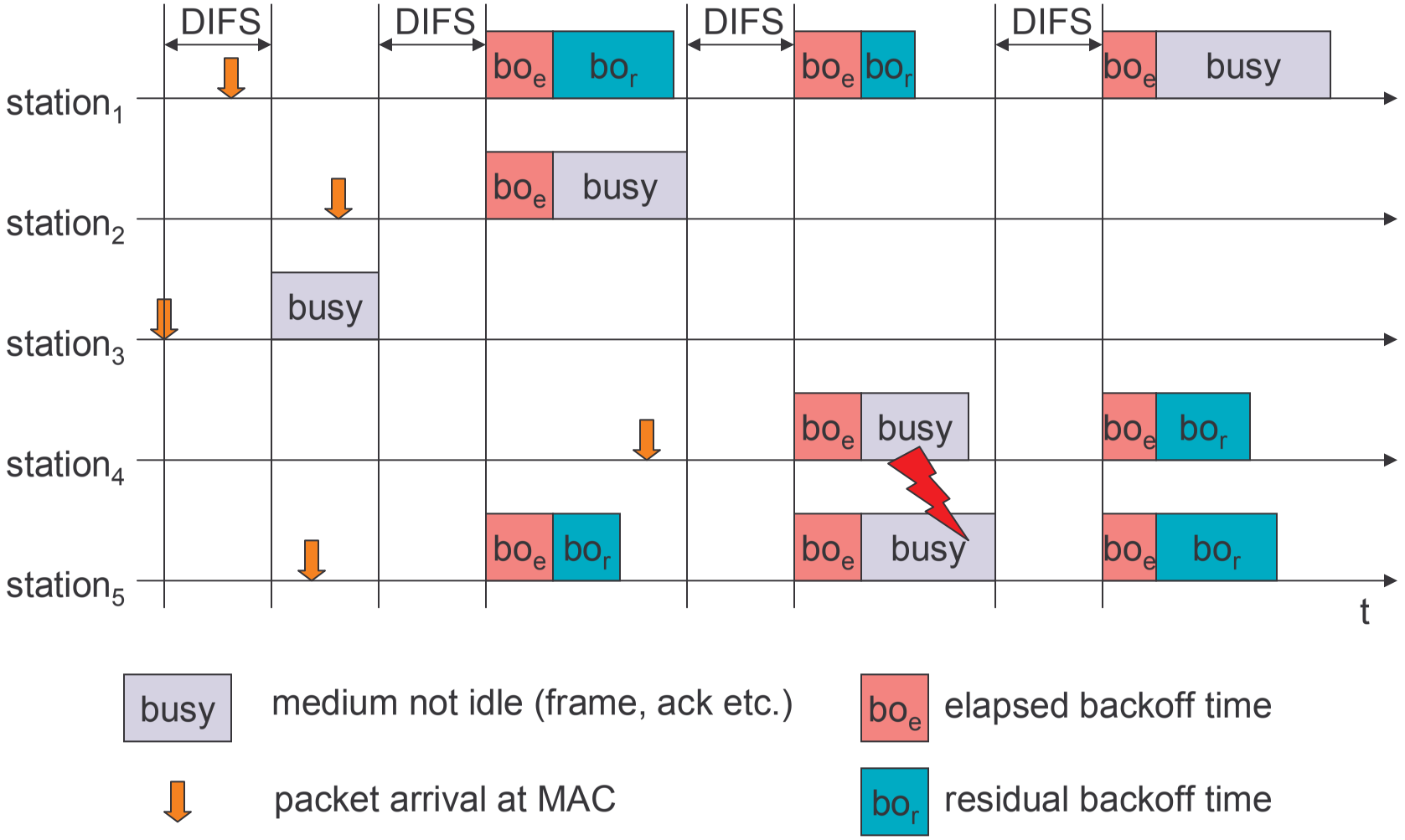


CSMA/CA access method I



- 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)

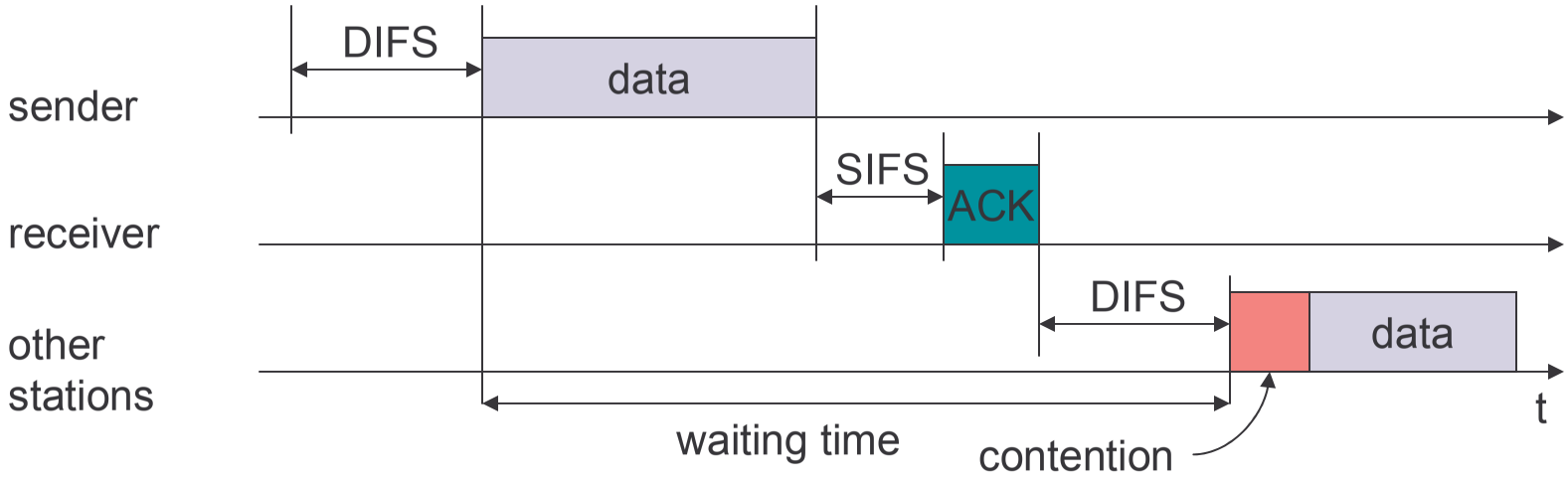
Competing stations - simple version



CSMA/CA access method II

Sending unicast packets

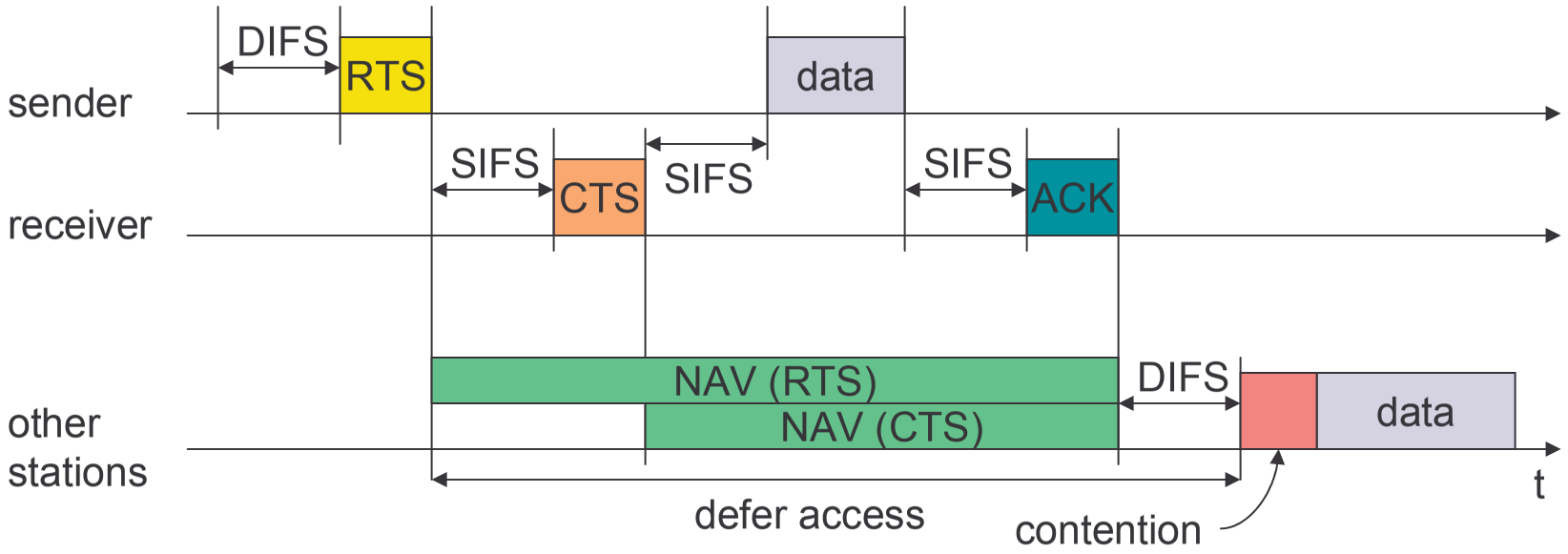
- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



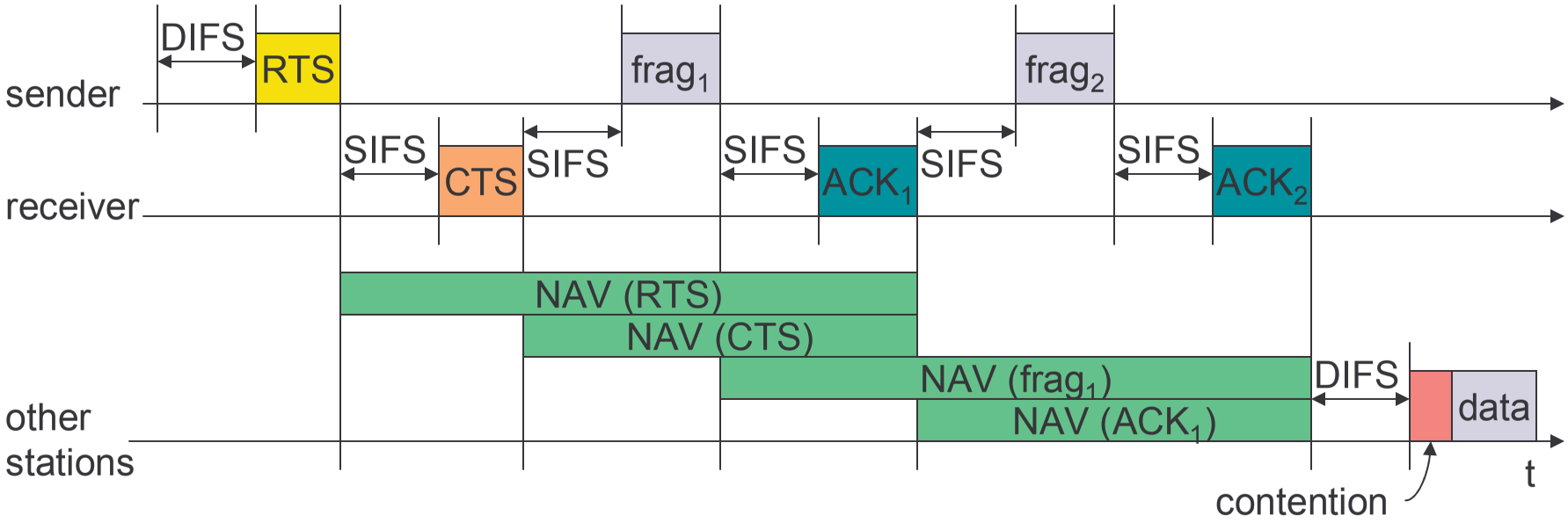
DFWMAC

Sending unicast packets

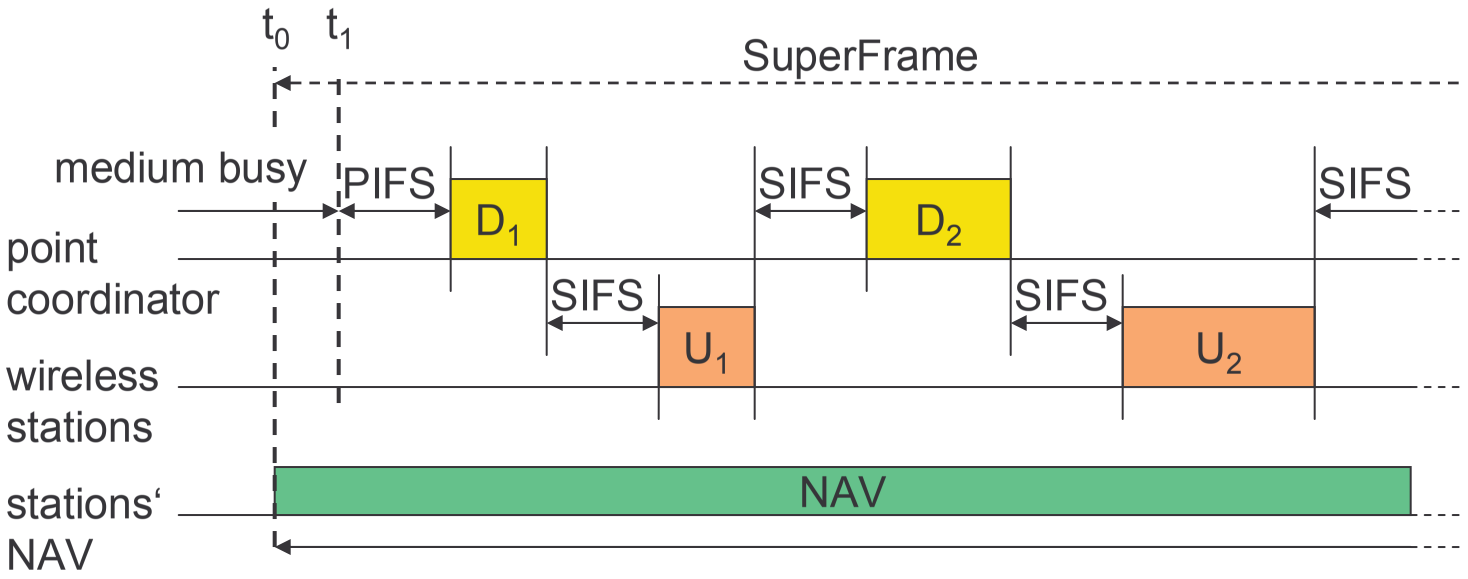
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium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



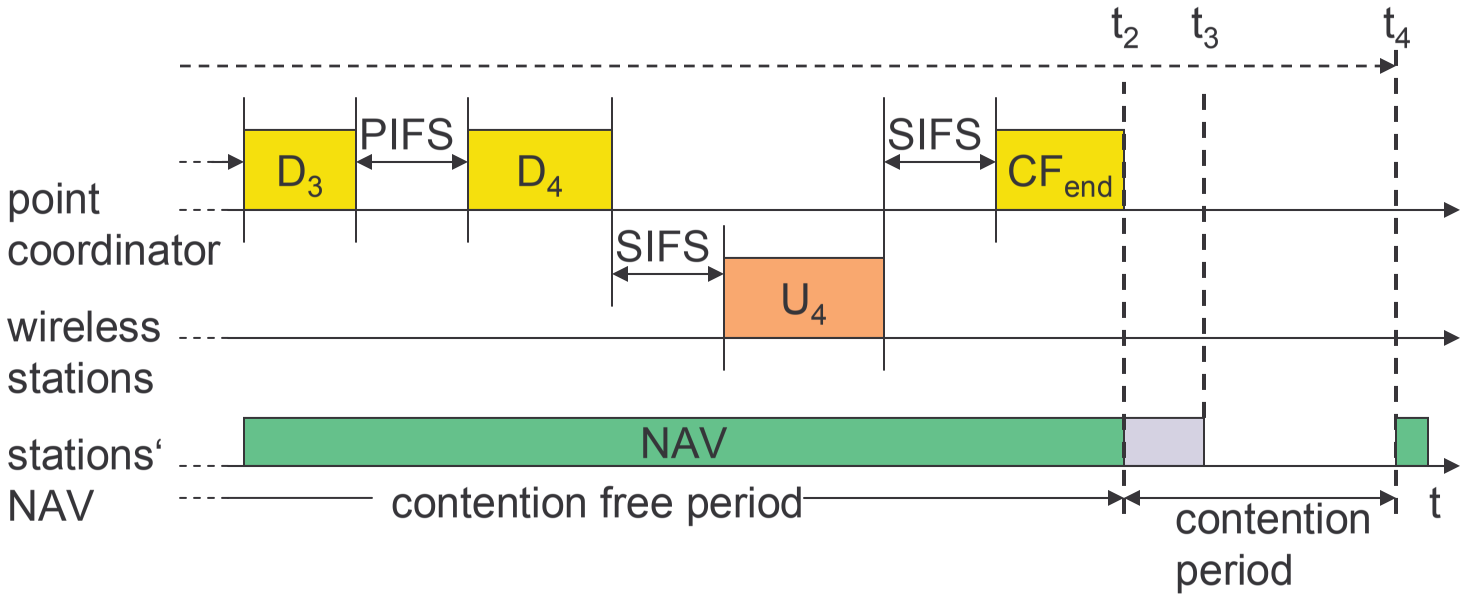
Fragmentation



DFWMAC-PCF I


t0
t1
SuperFrame
medium busy
PIFS
D1
SIFS
D2
SIFS
point coordinator
SIFS
U1
SIFS
U2
wireless stations
stations' NAV
NAV

DFWMAC-PCF II



IEEE 802.11

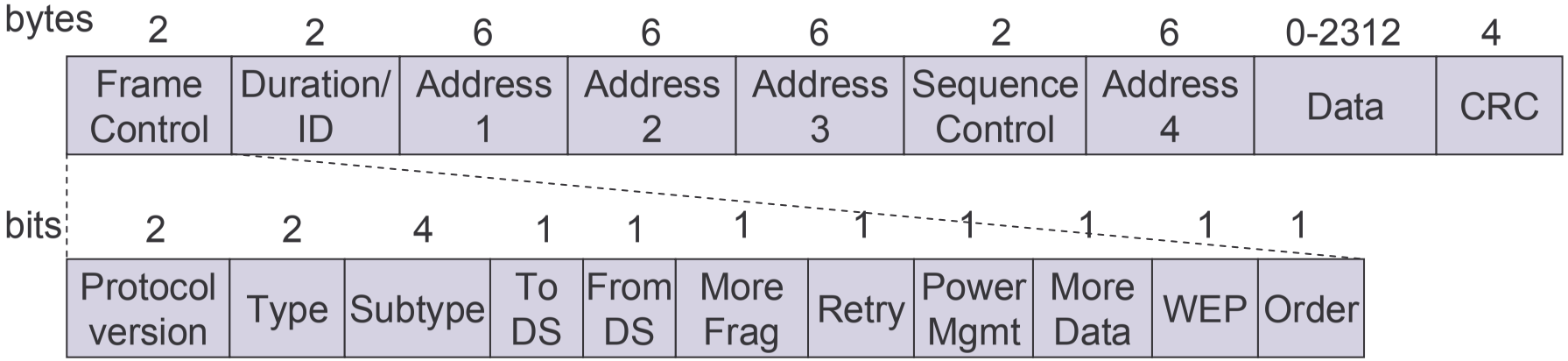
Frame format

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



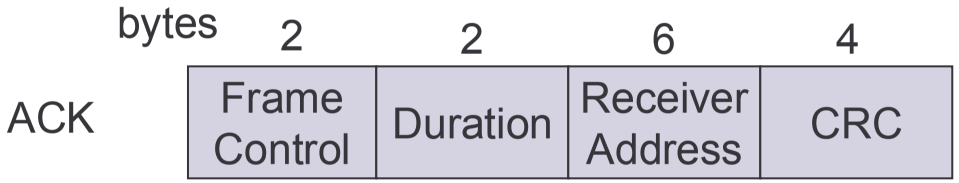
MAC address format

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

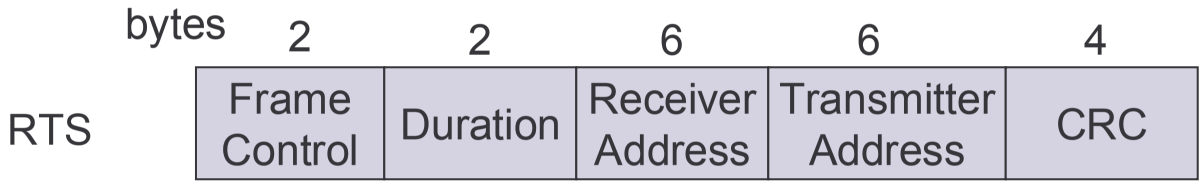
DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: Basic Service Set Identifier
RA: Receiver Address
TA: Transmitter Address

Special Frames: ACK, RTS, CTS

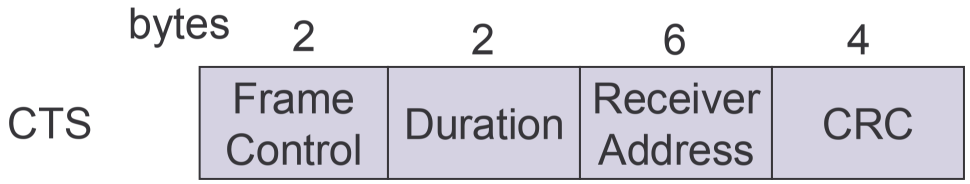
Acknowledgement



Request To Send



Clear To Send



MAC management

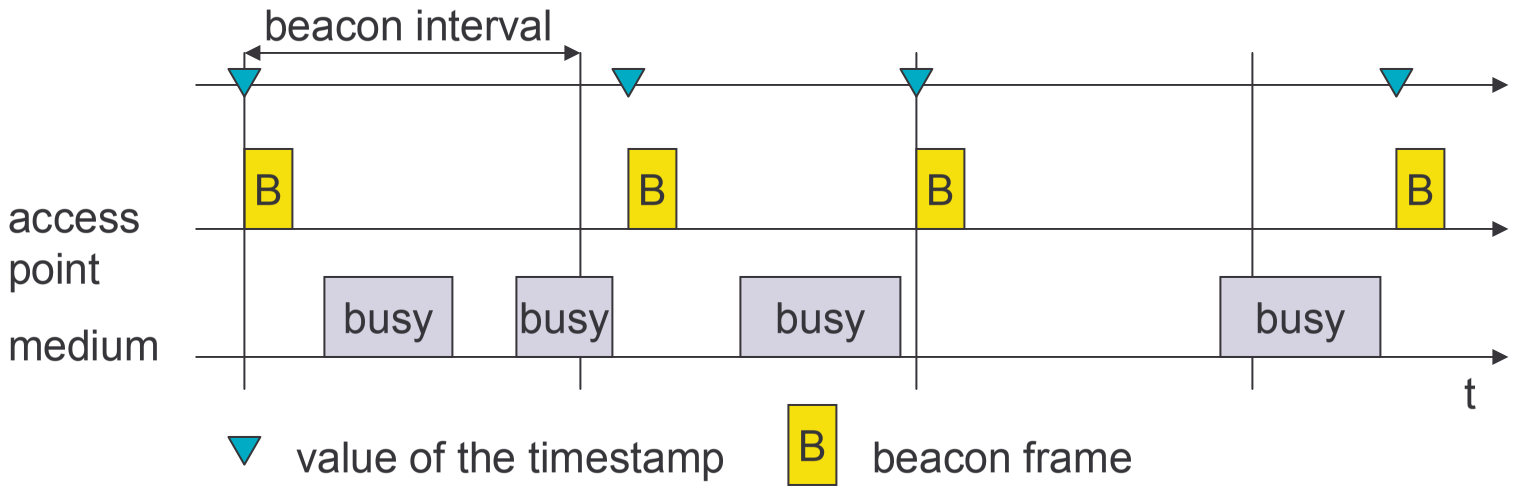
Synchronization
- try to find a LAN, try to stay within a LAN
- timer etc.

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

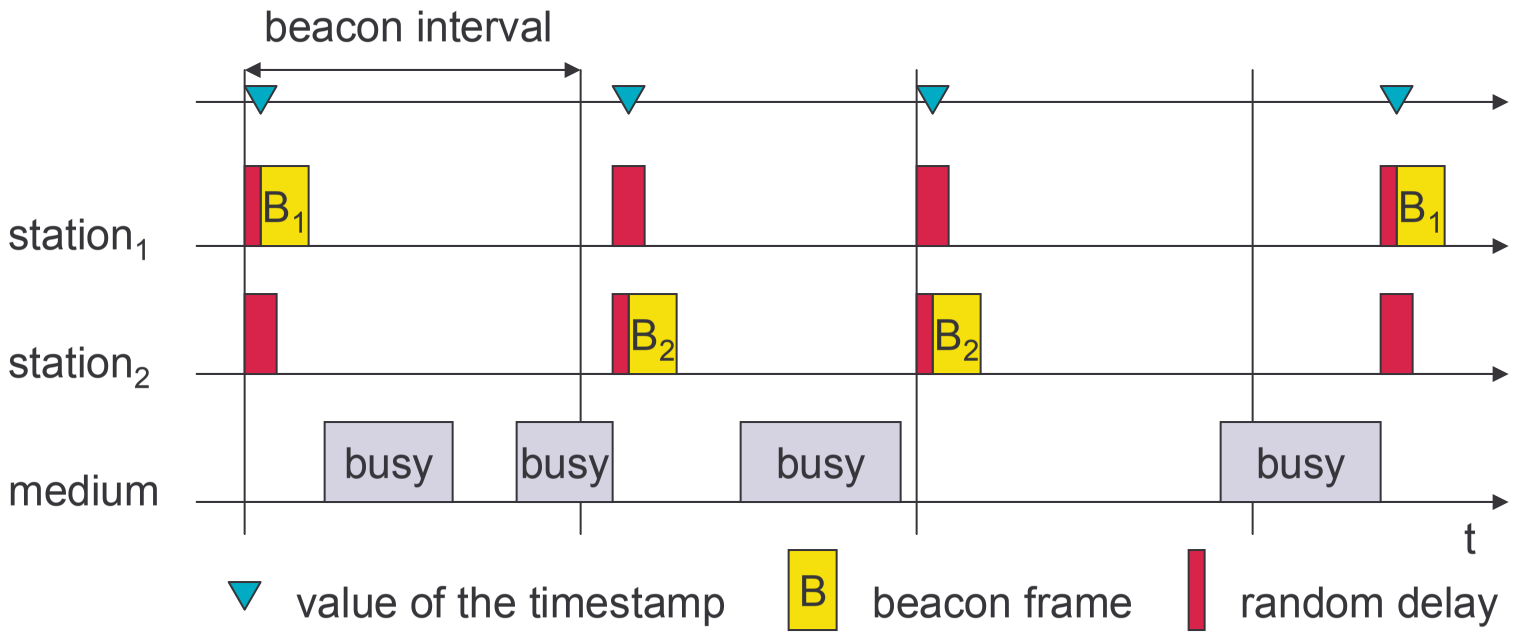
Association/Reassociation
- integration into a LAN
- roaming, i.e. change networks by changing access points
- scanning, i.e. active search for a network

MIB - Management Information Base
- managing, read, write

Synchronization using a Beacon (infrastructure)



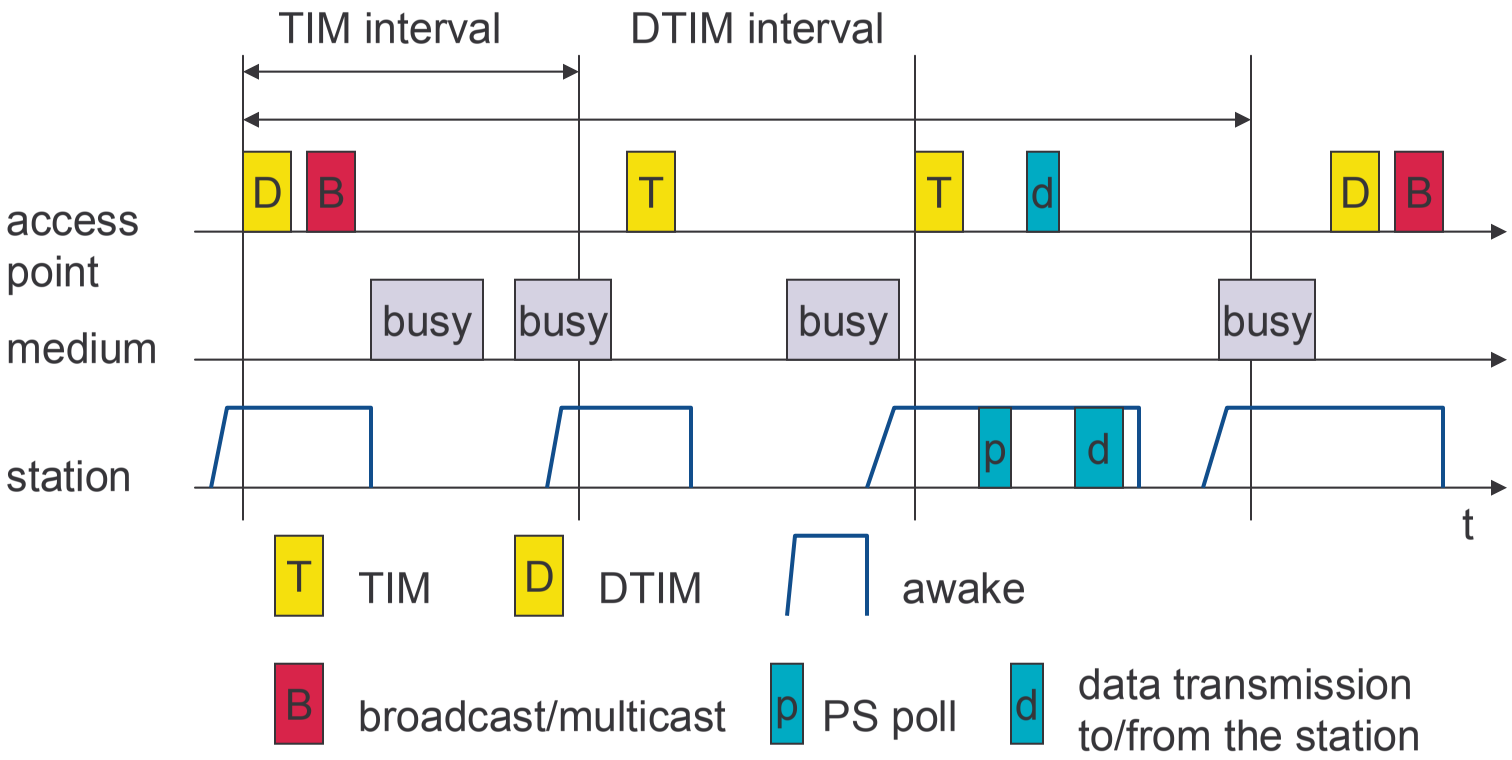
Synchronization using a Beacon (ad-hoc)



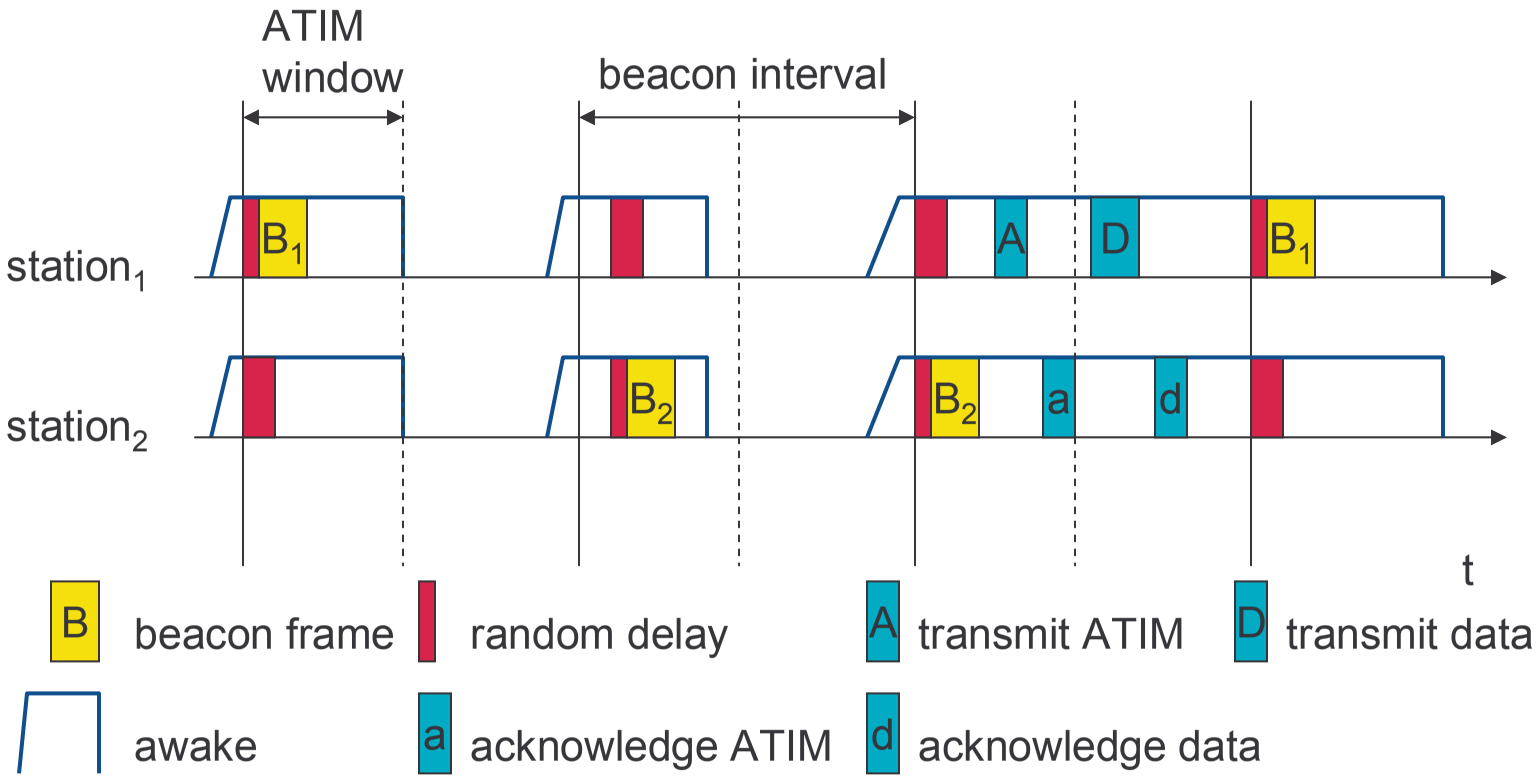
Power management

- 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?)

Power saving with wake-up patterns (infrastructure)



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



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

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
- Free 2.4 GHz ISM-band

Security
- Limited, WEP insecure, SSID

Availability
- Many products, many vendors

Connection set-up time
- Connectionless/always on

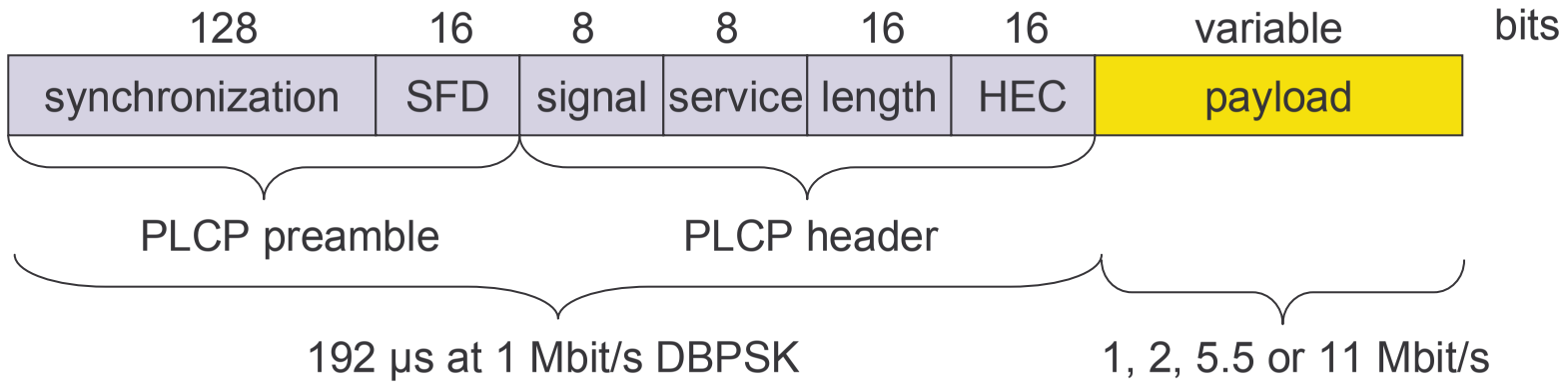
Quality of Service
- Typ. Best effort, no guarantees (unless polling is used, limited support in products)

Manageability
- Limited (no automated key distribution, sym. Encryption)

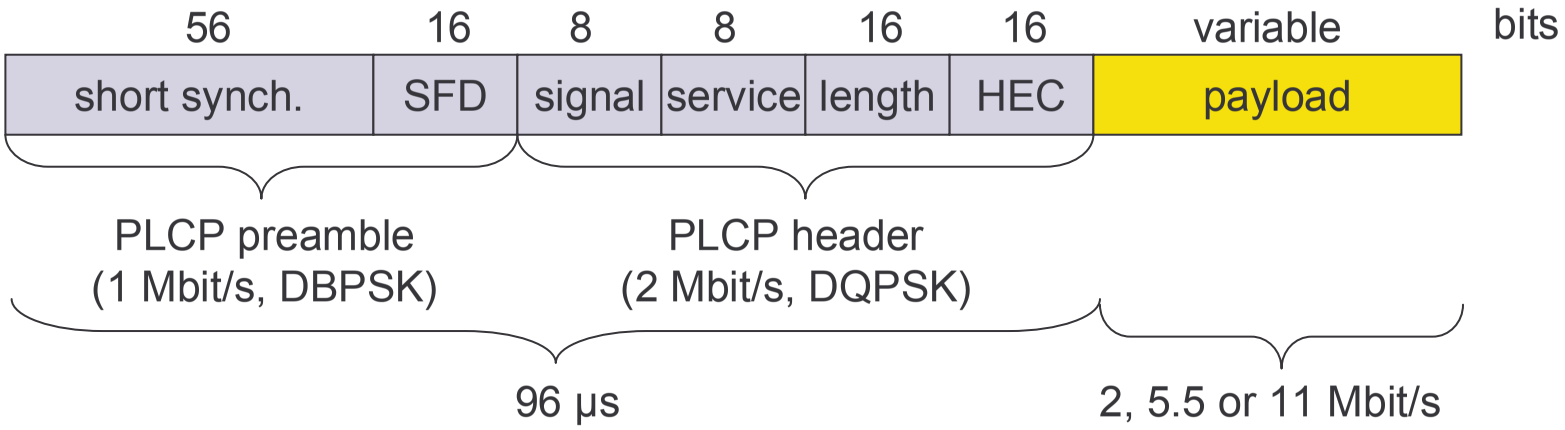
Special Advantages/Disadvantages
- Advantage: many installed systems, lot of experience, available worldwide, free ISM-band, many vendors, integrated in laptops, simple system
- Disadvantage: heavy interference on ISM-band, no service guarantees, slow relative speed only

IEEE 802.11b – PHY frame formats

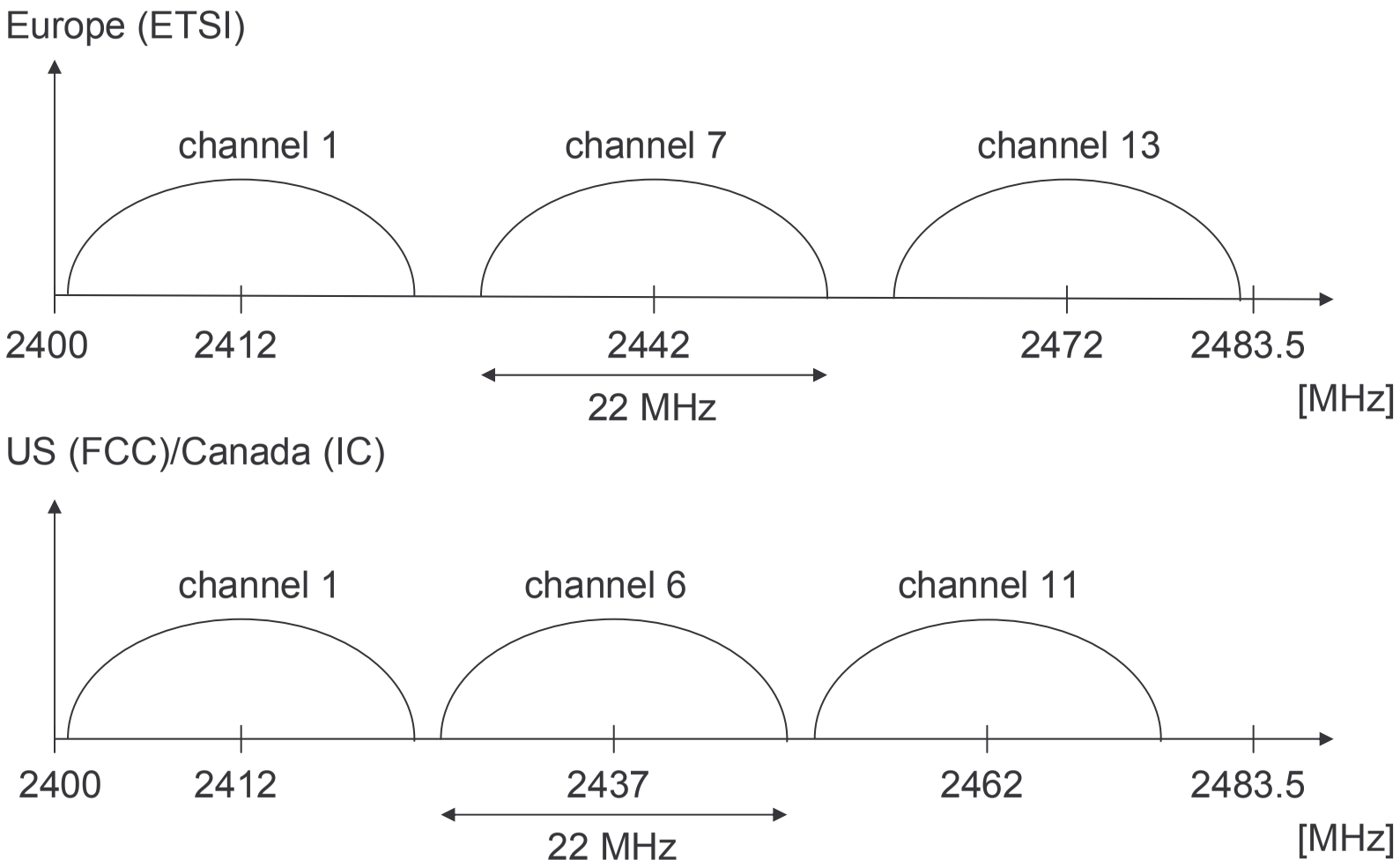
Long PLCP PPDU format



Short PLCP PPDU format (optional)



Channel selection (non-overlapping)



IEEE 802.11

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

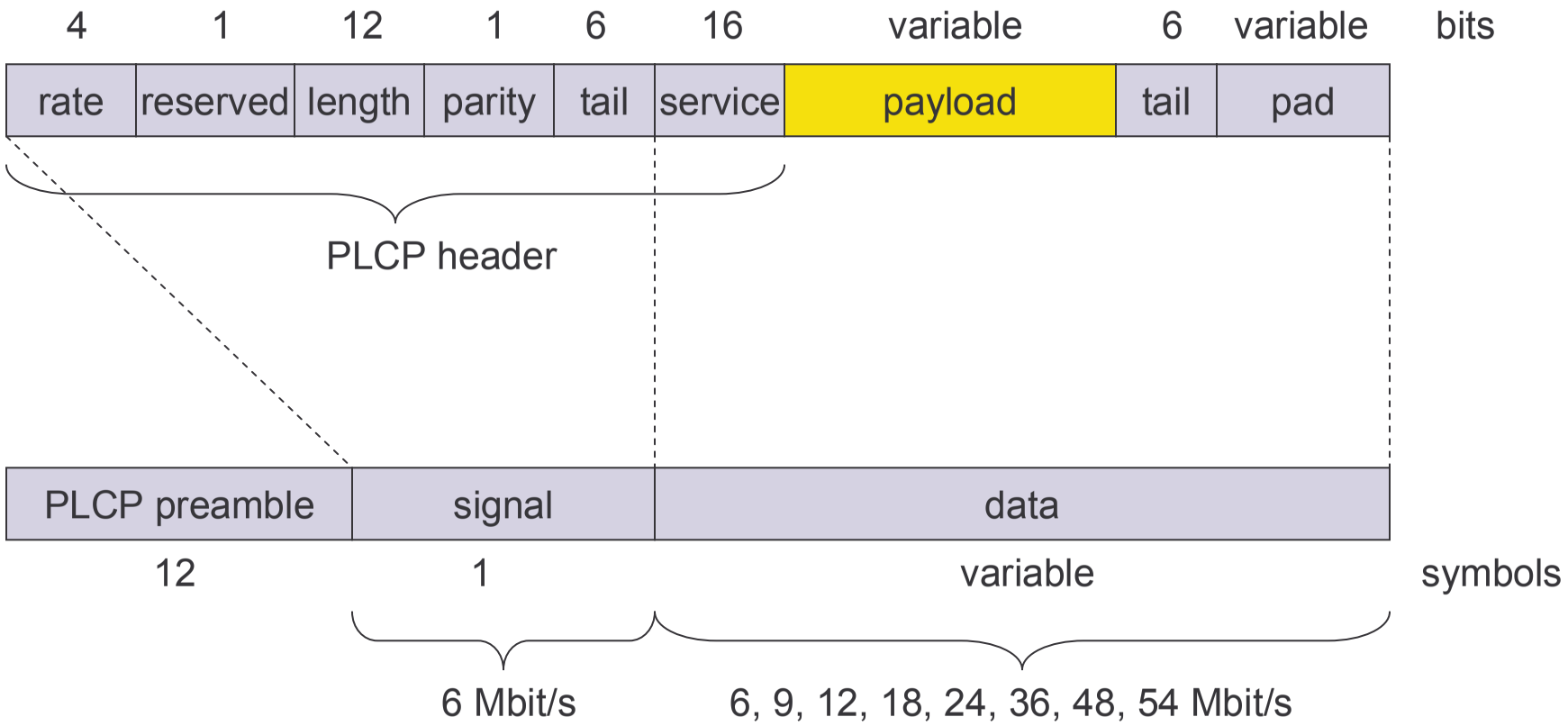
Connection set-up time
- Connectionless/always on

Quality of Service
- Typ. best effort, no guarantees (same as all 802.11 products)

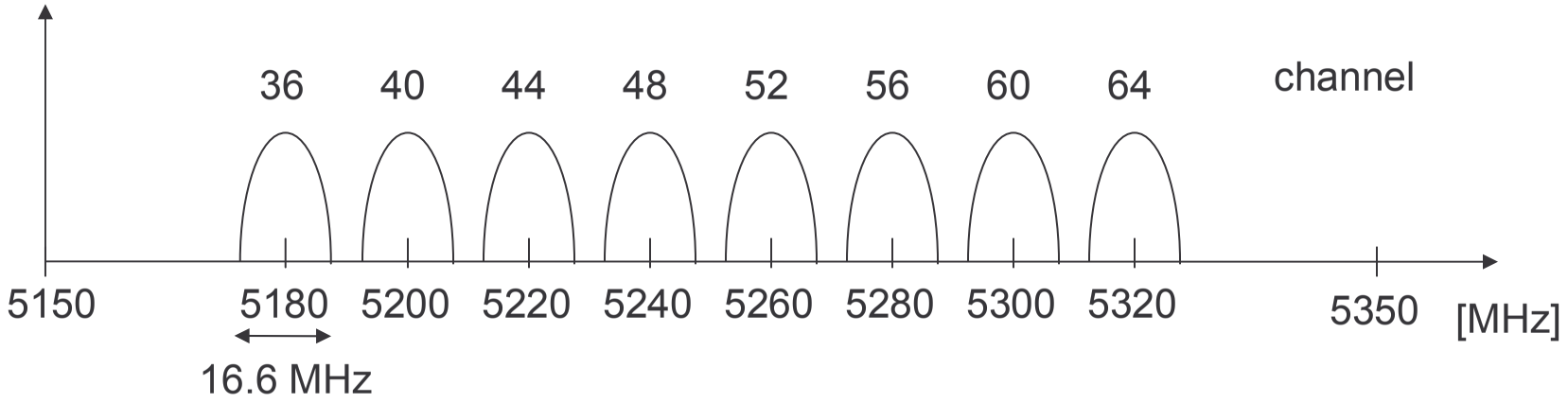
Manageability
- Limited (no automated key distribution, sym. Encryption)

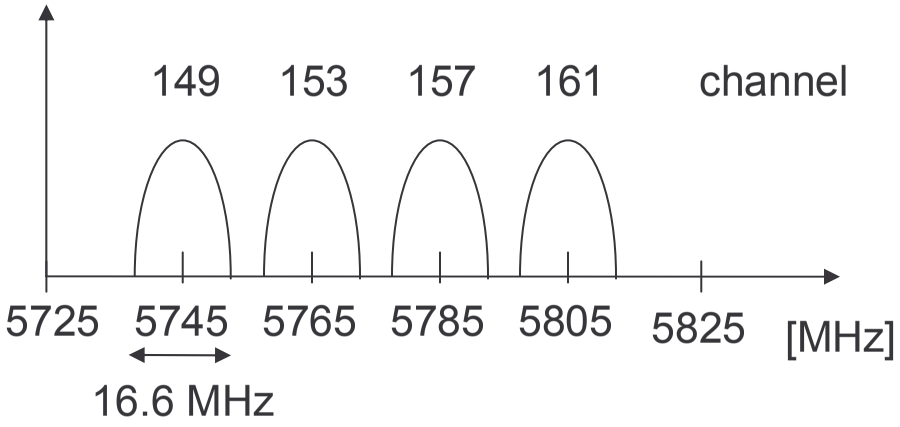
Special Advantages/Disadvantages
- Advantage: fits into 802.x standards, free ISM-band, available, simple system, uses less crowded 5 GHz band
- Disadvantage: stronger shading due to higher frequency, no QoS

IEEE 802.11a – PHY frame format



Operating channels for 802.11a / US U-NII



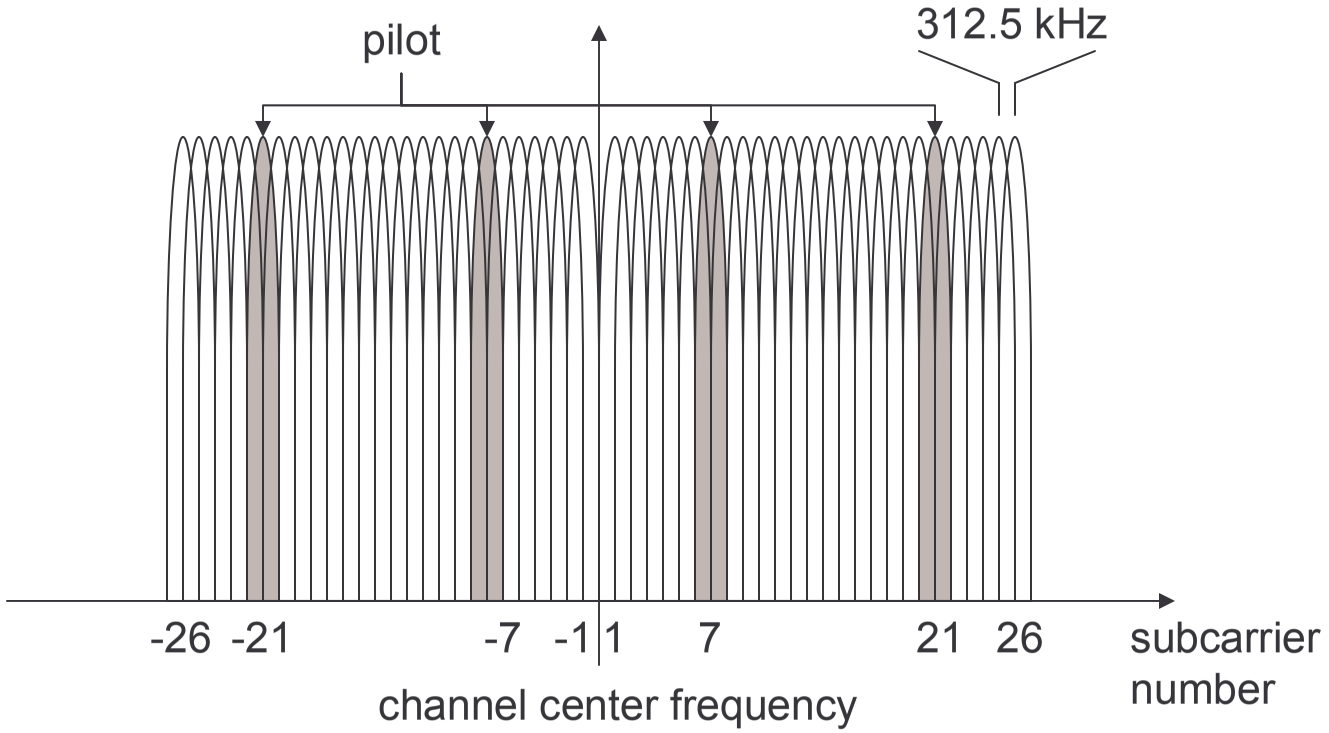


center frequency =
5000 + 5*channel number [MHz]

OFDM in IEEE 802.11a (and HiperLAN2)

OFDM with 52 used subcarriers (64 in total)

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



WLAN: IEEE 802.11 – future 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…
- Additional energy saving mechanisms and more efficient retransmission

802.11f: Inter-Access Point Protocol
- Establish an Inter-Access Point Protocol for data exchange via the distribution system
- Currently unclear to which extend manufacturers will follow this suggestion

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)

WLAN: IEEE 802.11– future developments

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

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 standards

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

WLAN: IEEE 802.11– future developments

802.11r: Faster Handover between BSS
- 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

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.

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

Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/