Wireless LANs

Characteristics of Wireless LANs

Advantages (flexibility, mobility, robustness, cost efficiency)

- very flexible including mobility within the reception area
- Ad-hoc (mobile) 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
- compared to classical (wired) LANs very low Quality of Service (QoS)
- standards, especially for higher bit-rates (bandwidth) and QoS, take their time (e.g. IEEE 802.11a,g and 802.1x)

Ultimate goal: Be as good as LAN's

Major Drawbacks

Less to no Quality of Service (QoS) regarding the most important parameters

- Bandwidth
  - much lower in general (1-10 Mbit/sec vs 100 - 1000Mbit/sec) (**performance aspect)**
  - difficult to predict (**real-time aspect)**
- Transmission errors
  - tremendously higher loss rates (on average 10^{-4} versus 10^{-12}) **(reliability aspect)**
- Latencies
  - much higher (**performance aspect)**
  - less predictable **(real-time aspect)**

Additional safety and security problems may arise

- Radio communication may affect other electronic devices and radio communication
- Communication medium (air) difficult to shield against unauthorized individuals

Conclusion:

Depending on

- **standard, architecture, and size**

of the network, wireless communication in computing networks is quite a challenge!

IEEE 802.11 (WLAN)

Characteristics:

- Worldwide mostly used, available in most products used for wireless communicatin
- Member of the IEEE 802.x family for LANs like Ethernet (802.3) and Token Ring (802.5)
- Like the others specifies the Physical Layer and the MAC layer of the TCP/IP reference model
- Supports two different kinds of architectures

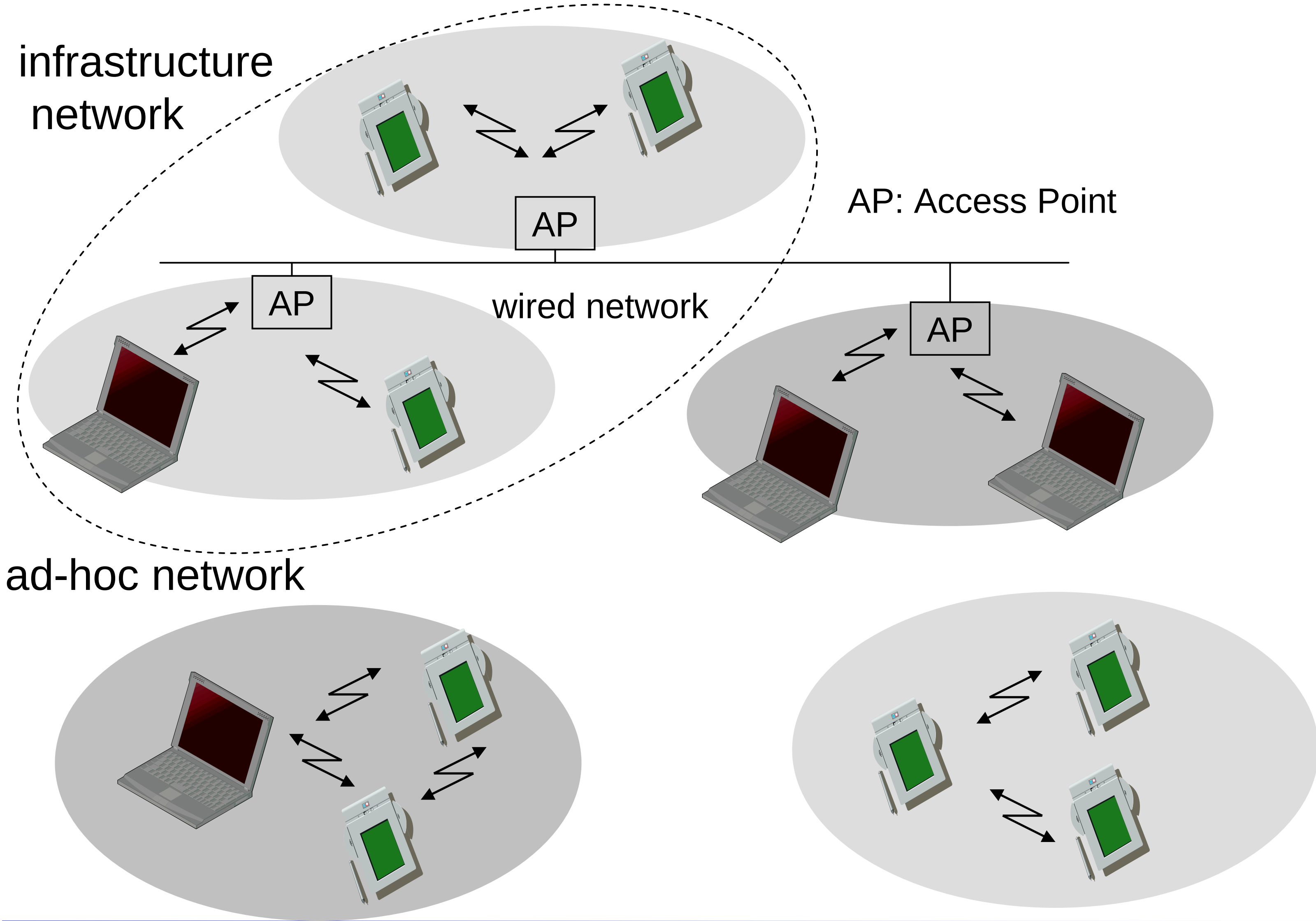
Primary goal:

- Specifying a simple and robust LAN providing time-bounded and asynchronous data service
- Still, services above the MAC layer are considered to be of best-effort character.

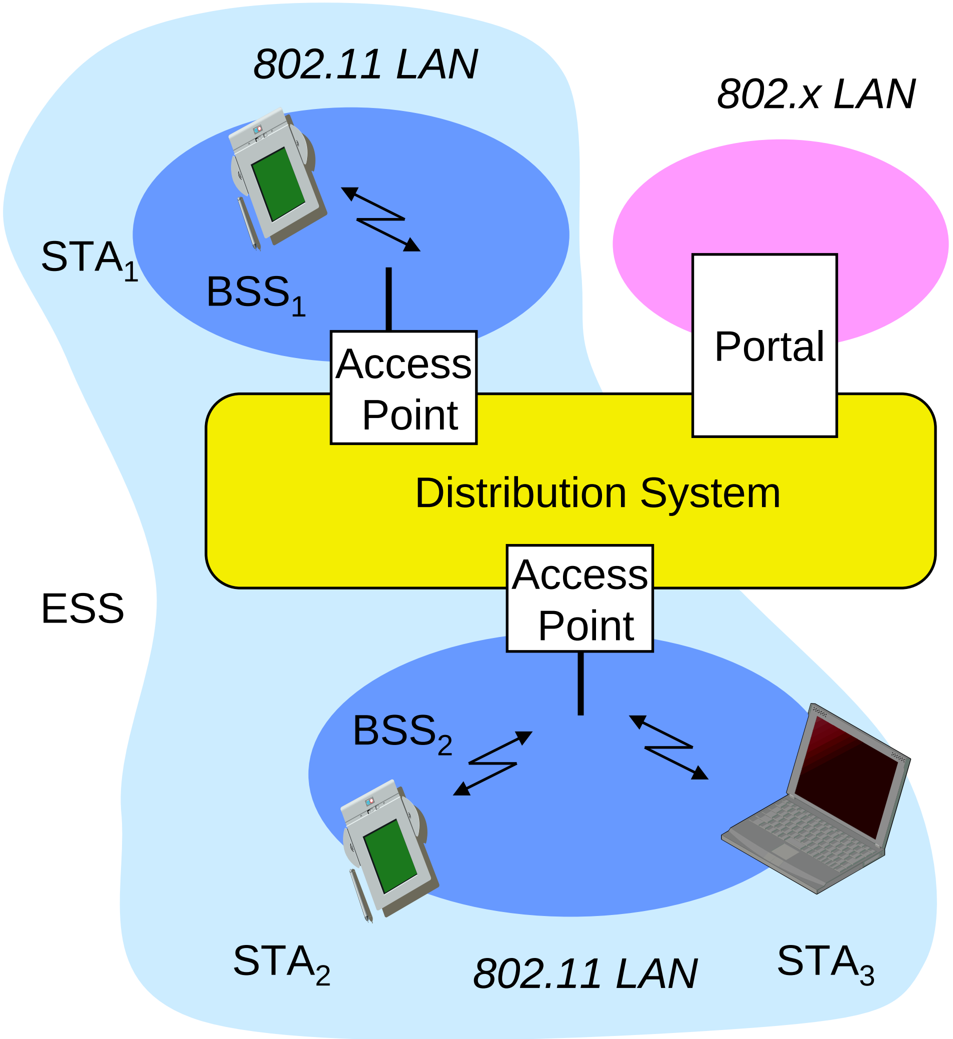
Other standards:

- HIPERLAN
  - European Standard (ETSI), improved QoS specifications, never reached product status (but several mechanisms have been adopted by other standards (e.g. 802.11a and g))
- Bluetooth
  - Industry standard for WPAN (adopted in 802.15)

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 associated access point (AP)

Basic Service Set (BSS)

- group of stations being in the same transmission range as the associated AP + the AP itself

Access Point

- station integrated into the wireless LAN and the distribution system

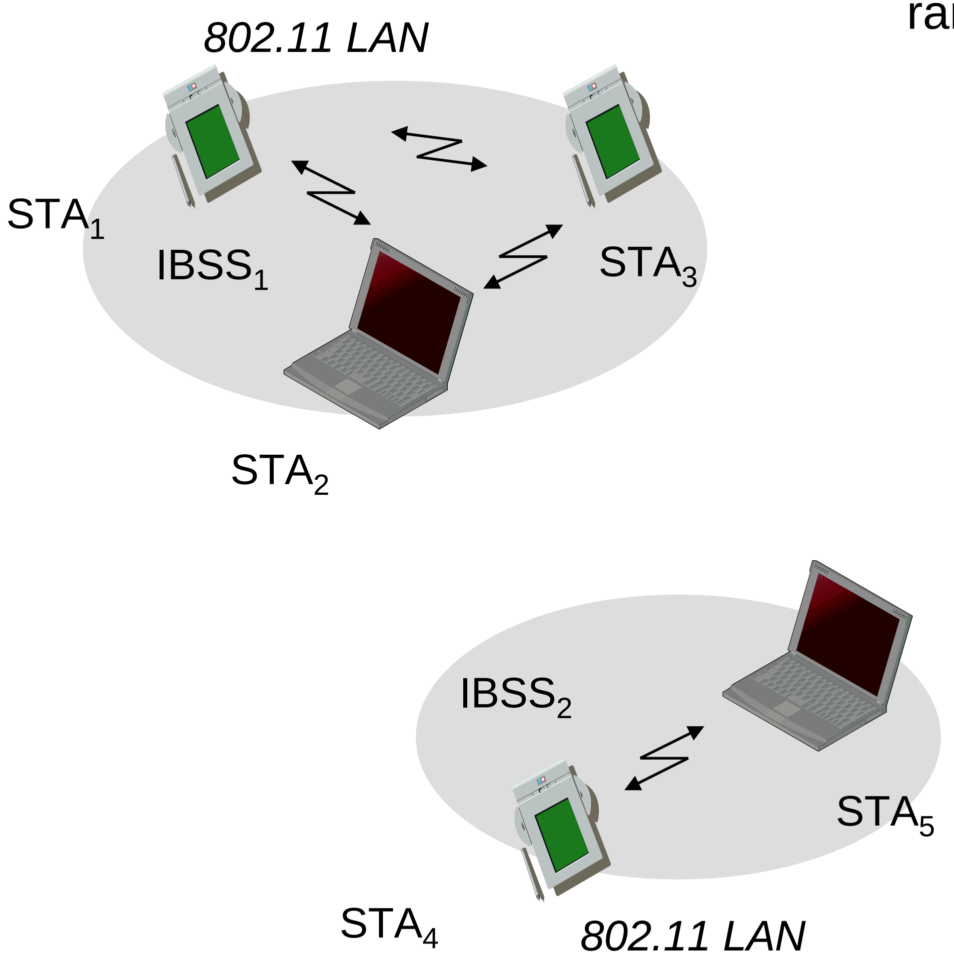
Distribution System

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

Portal

- Bridge from one ESS to other (wired) networks

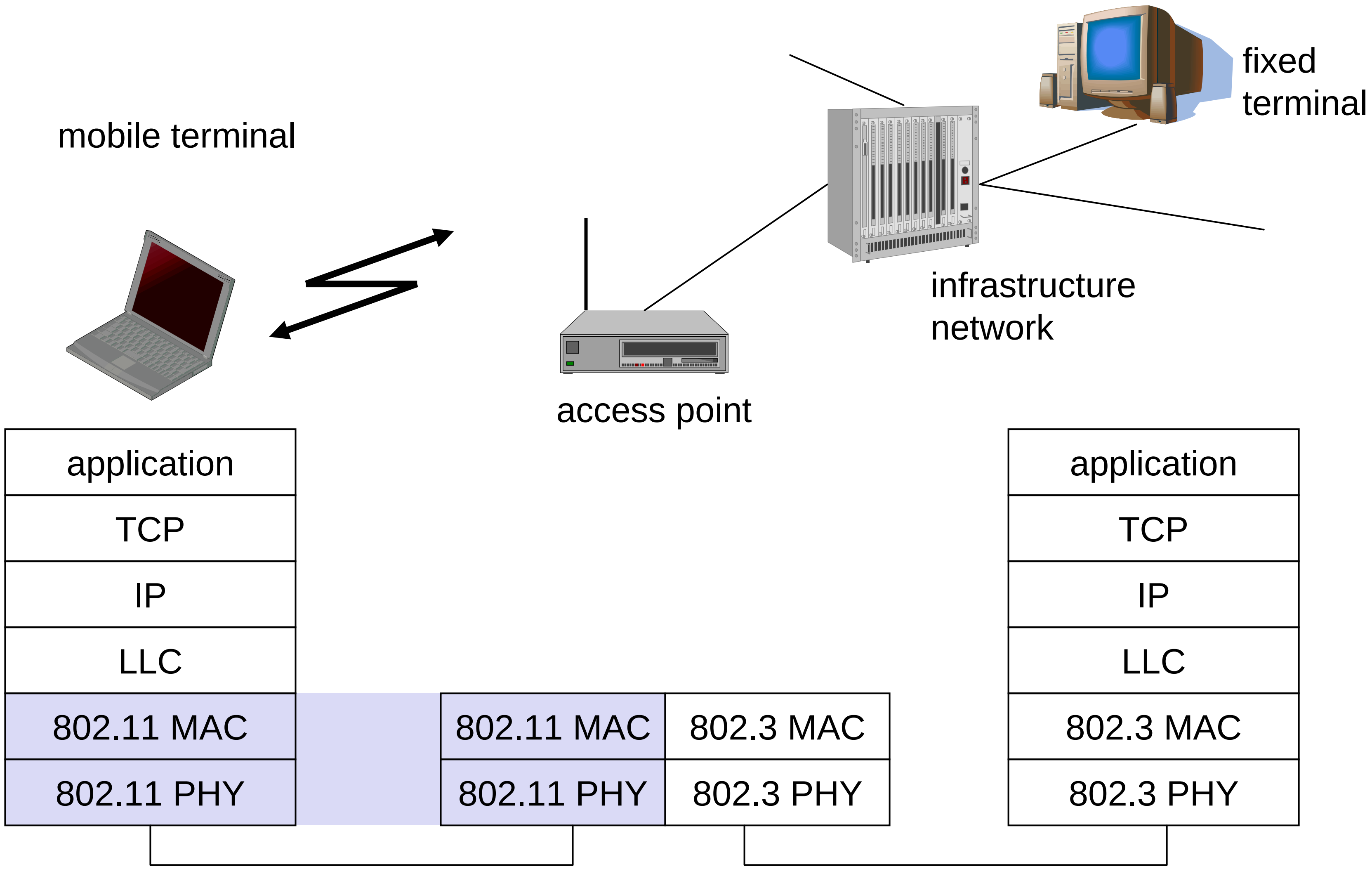
802.11 - Architecture of an ad-hoc network



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 being within the same transmission range

802.11 - Protocol architecture (infrastructure embedded)



802.11 - Physical layer (classical)

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

- Offer CCA-signal allowing carrier sense on the MAC layer

Infrared

- wave length ca.850-950 μm (ca. 300 GHz)
- range about 10m if conditions are very good

FHSS (Frequency Hopping Spread Spectrum)

- Separation of nets due to different hoping sequences
- Individual channels have a bandwidth of about 1MHz each

DSSS (Direct Sequence Spread Spectrum)

- chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
- Individual channels have a bandwidth of about 22 MHz each

802.11 - MAC layer

Traffic services

- Asynchronous Data Service implementing CSMA/CA (mandatory)
  - exchange of data packets based on “best-effort”
  - support of broadcast and multicast
- Time-Bounded Service (optional)
  - needs a central coordinator (master)

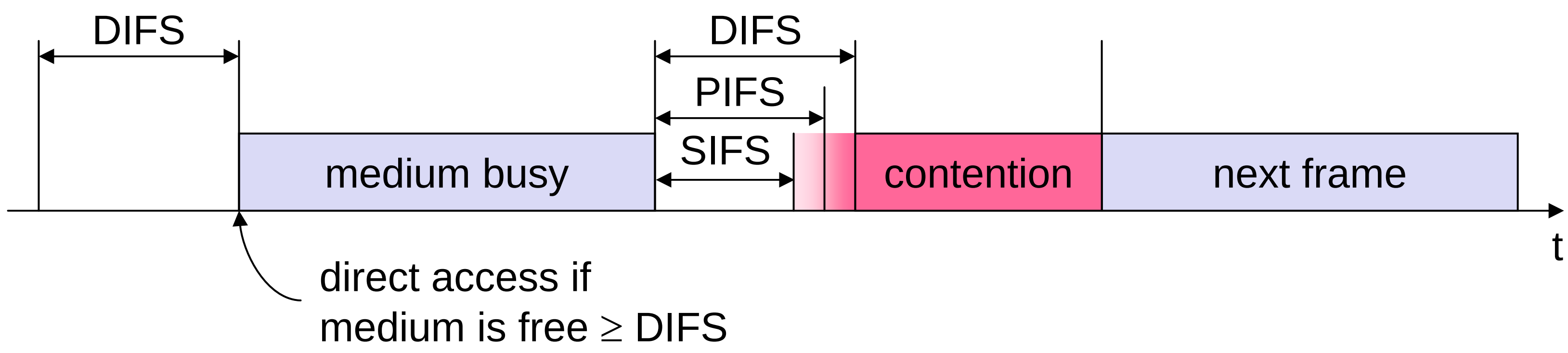
Access methods

- Distributed Coordination Function (DCF) -simple version- (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - ACK packet for acknowledgements (not for broadcasts)
- Distributed Coordination Function (DCF) -enhanced version- (optional)
  - avoids hidden station problem by adopting the MACA approach (providing additional RTS/CTS control frames)
- Point Coordination Function (PCF) (optional)
  - instead of doing CS, access point polls stations and ensures CA by assigning exclusive time slots to the potential senders (TDMA approach)
  - requires an infrastructure network

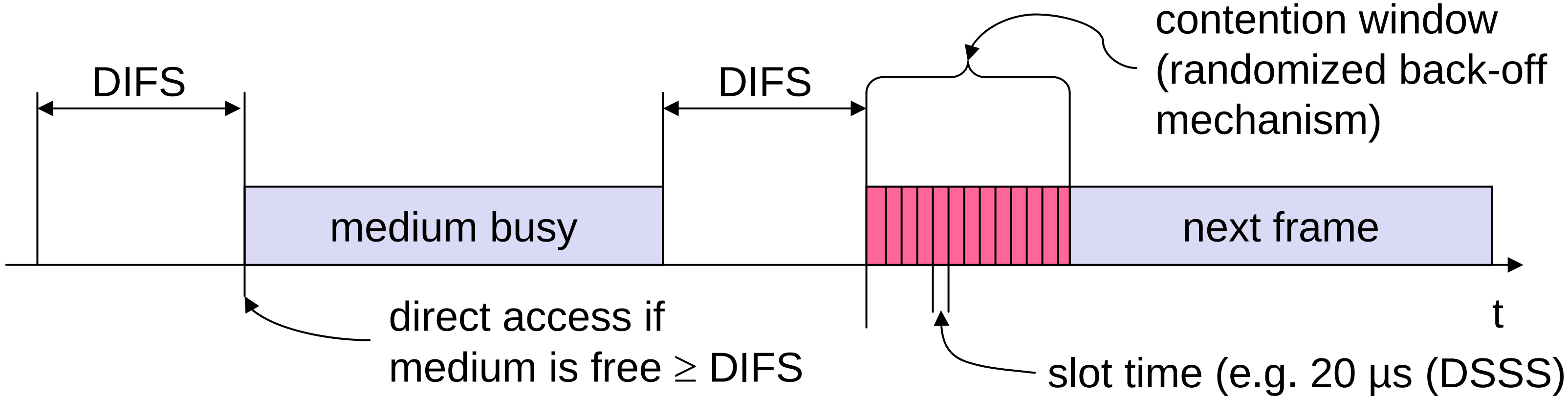
General approach to CSMA/CA

Priorities

- defined through Inter Frame Spaces (IFS)
- no guaranteed, hard priorities
- SIFS (Short Inter Frame Spacing)
  - highest priority used for control messages like ACK, CTS, polling response
- PIFS (P(CF) IFS)
  - medium priority, for time-bounded service using PCF
- DIFS (D(CF) IFS)
  - lowest priority, for asynchronous data service

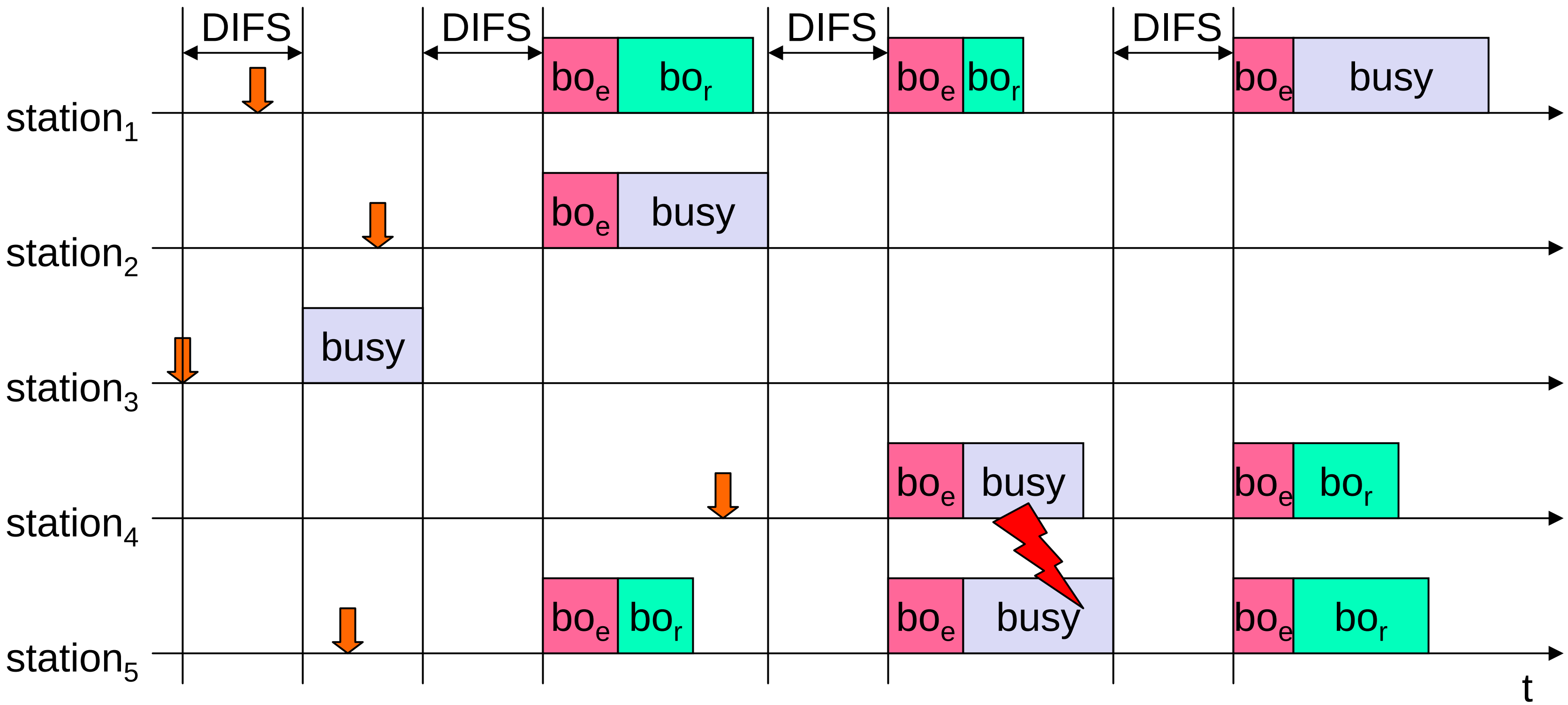


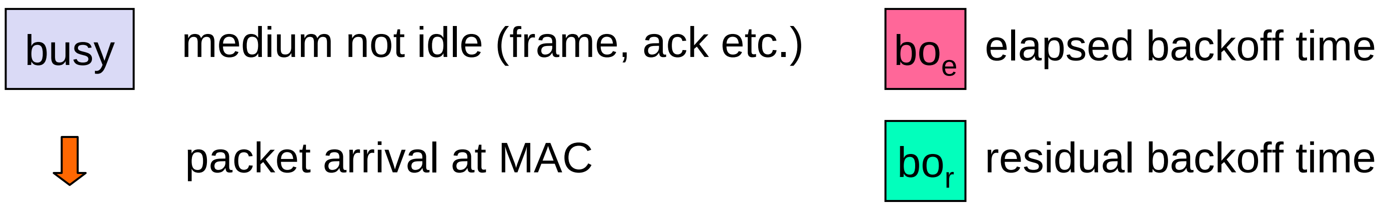
Simple version of DCF (mandatory)



- station ready to send starts sensing the medium (Carrier Sense based on Clear Channel Assessment (CCA) - signal provided by PHY layer
- if the medium is free for the duration of an DIFS, the station can start sending next frame (which IFS depends on service type)
- if the medium is busy, the station has to wait for a free DIFS, then the station must additionally wait a random back-off time (the multiple of slot-time) while constantly sensing the medium, thus implementing Collision Avoidance (CA)
- if another station occupies the medium during the back-off time of the station, the procedure starts from the beginning but the back-off timer stops (fairness), i.e. only the remainder of the timer must be waited in the next round

Example with 5 competing stations

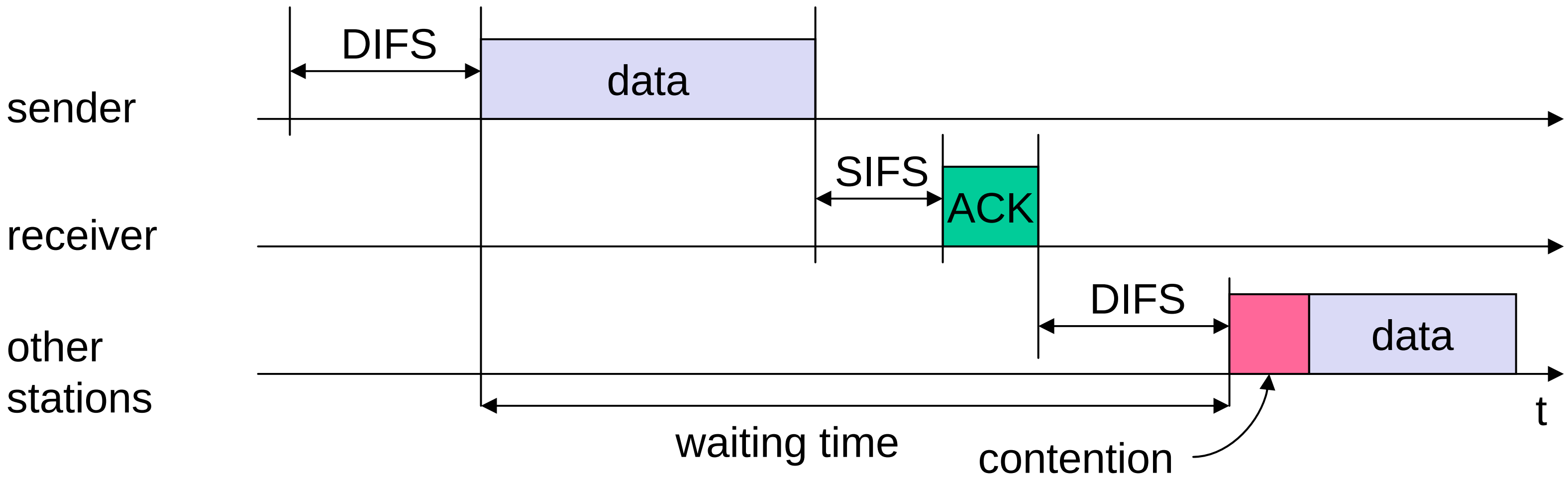




Unicast with additional Ack message

Sending unicast packets

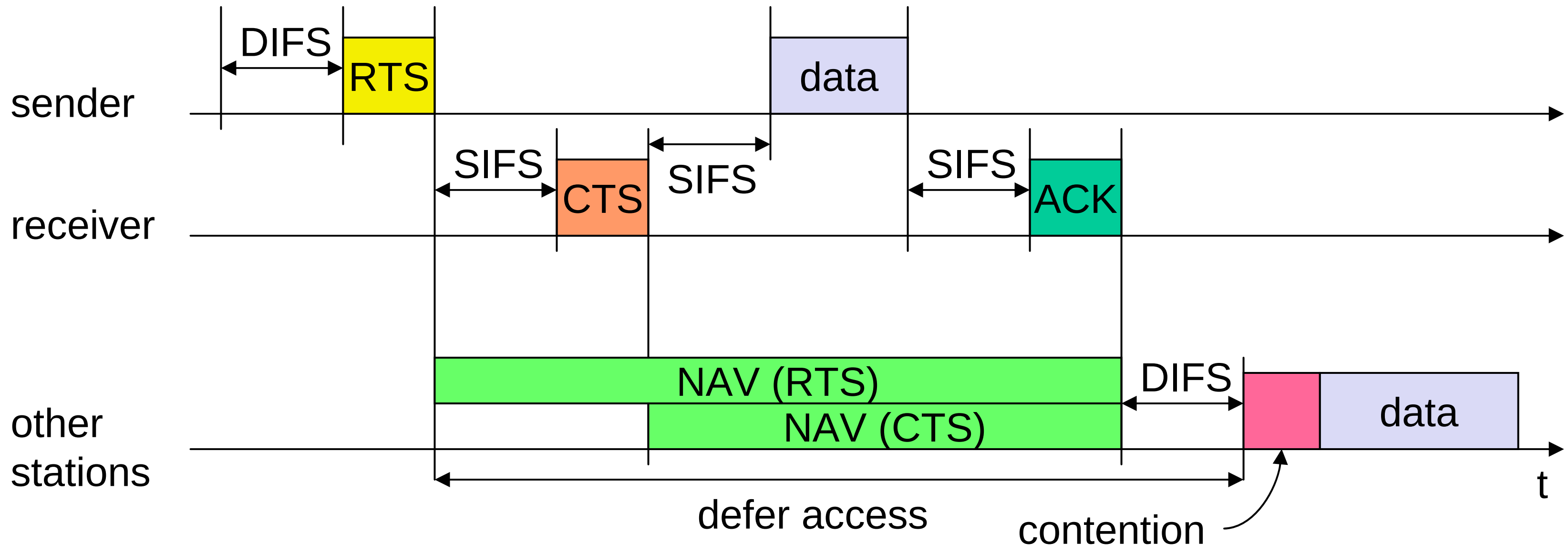
- station has to wait for DIFS before sending data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors
- not provided in case of broadcasts



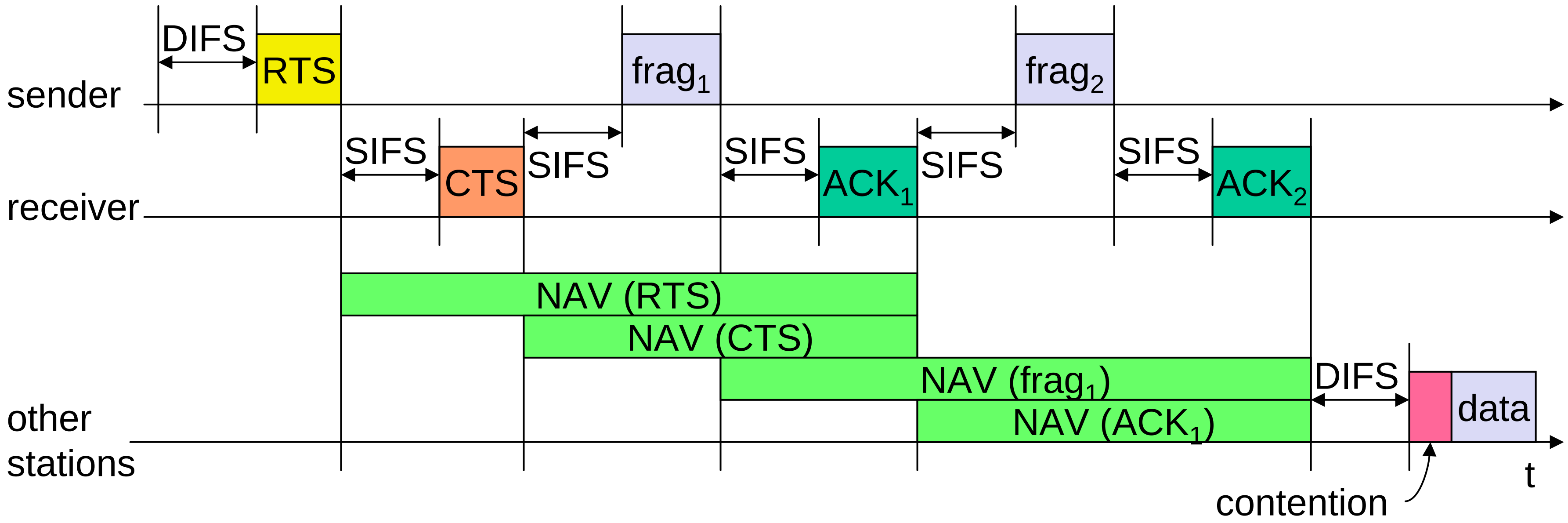
Enhanced version of DCF (optional)

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 after one more SIFS, acknowledgement via ACK
- other stations store medium reservations distributed via RTS **and** CTS in their *Net Allocation Vector (NAV)*

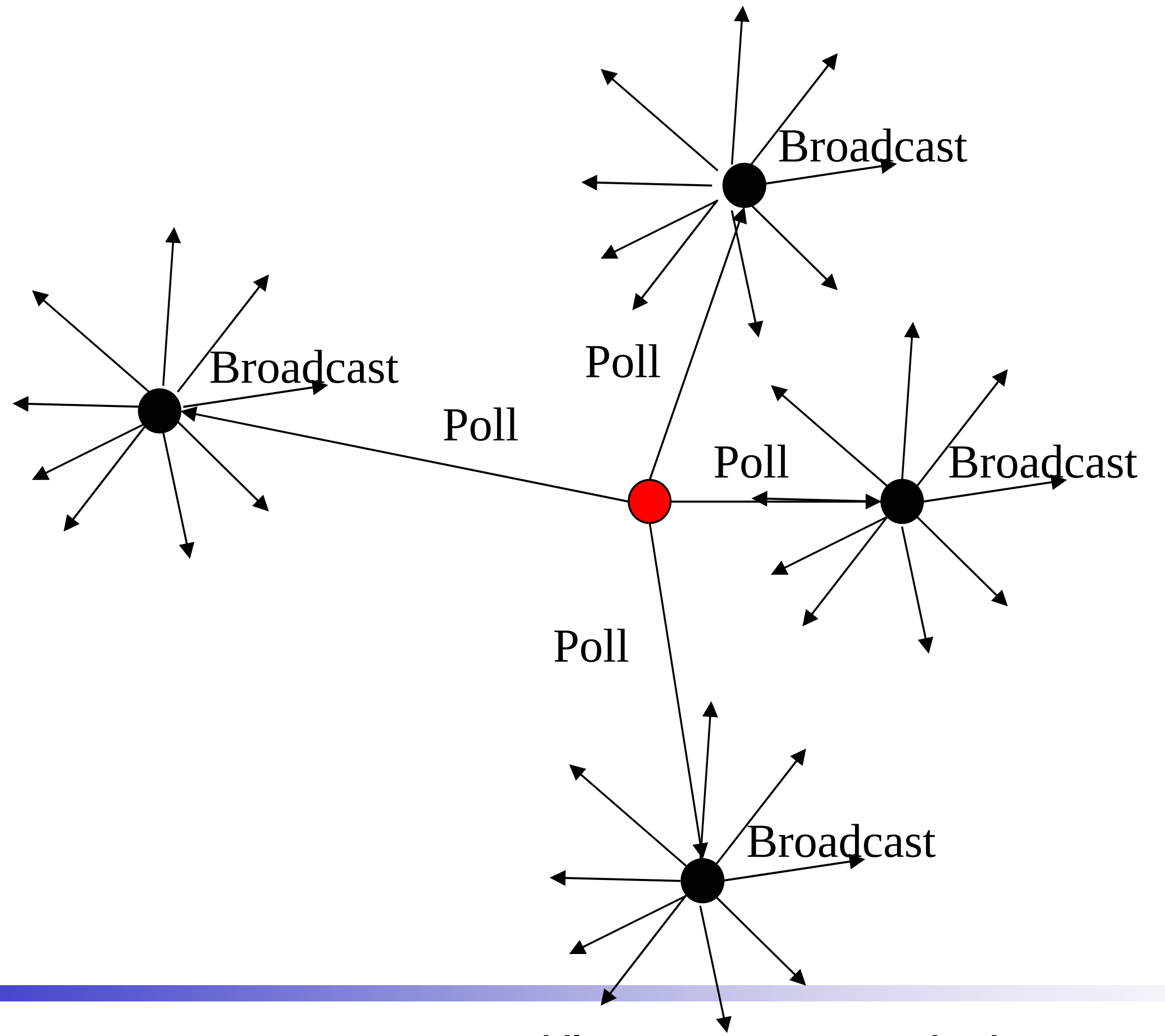


Fragmentation

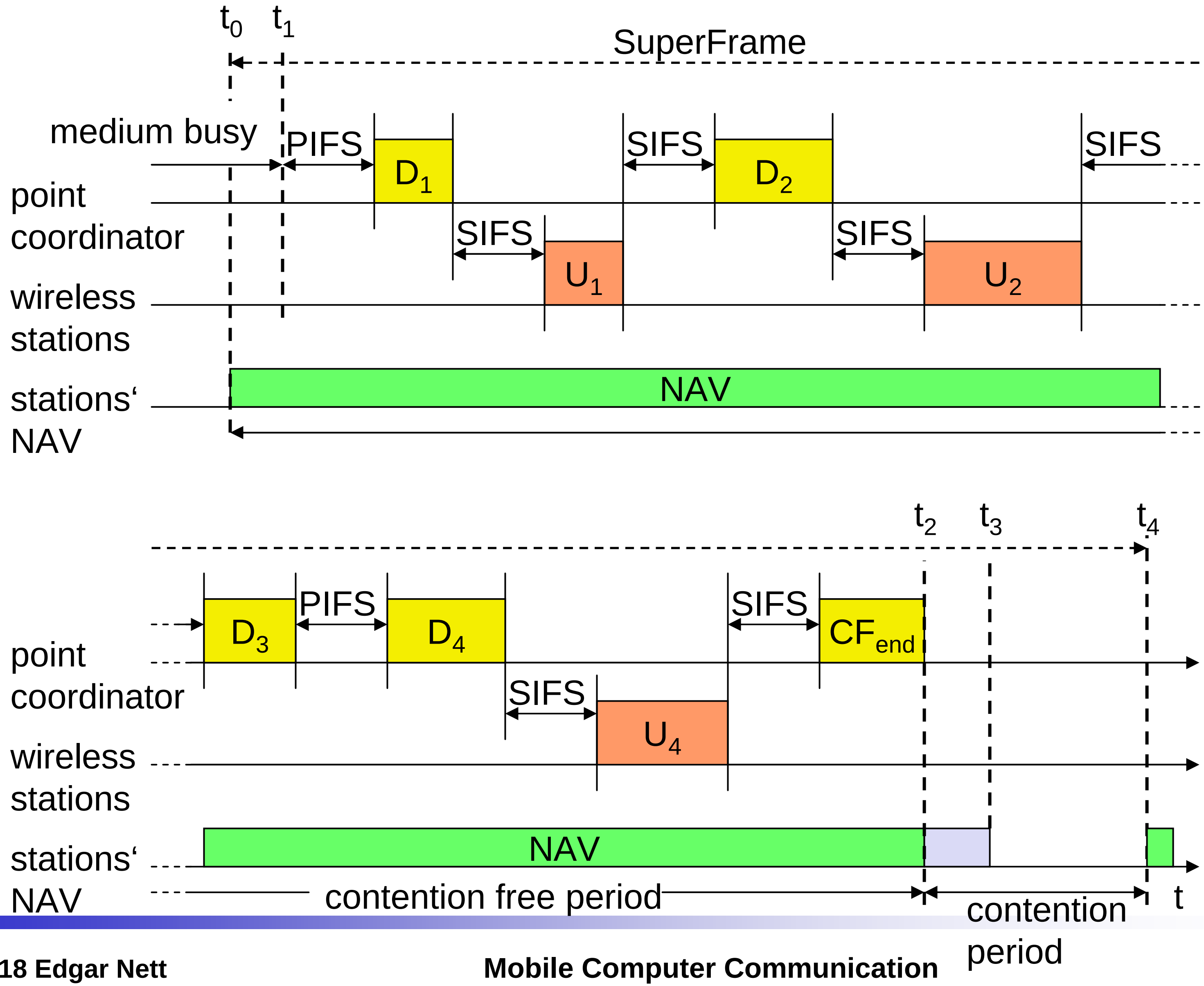


PCF (optional) (1)

PCF: A central point coordinator grants access to the medium by polling the stations



PCF (optional) (2)



802.11 - Frame and Address format

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

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, e.g. Control Frames ACK, RTS, CTS

Acknowledgement — ACK

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

Request To Send — RTS

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

Clear To Send — CTS

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

802.11 - MAC management

Synchronization of station-internal clocks is important, e.g.for

- running the PCF mode
- synchronization of frequency hopping between sender and receiver
- implementing energy saving mechanisms

Power management which essentially means energy saving by e.g.

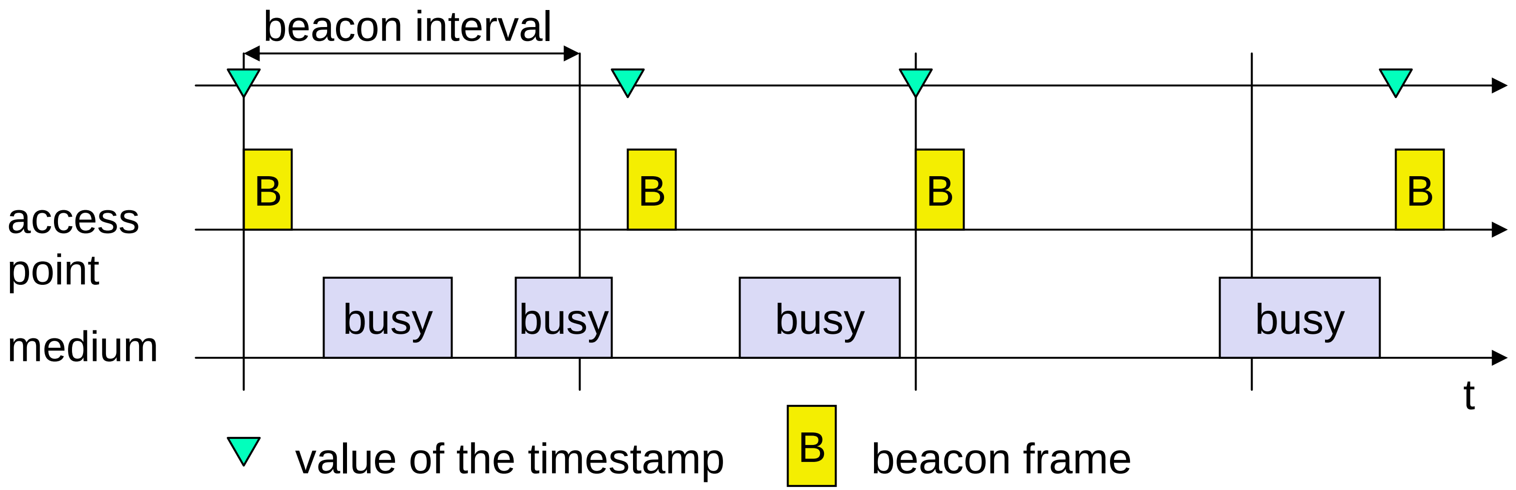
- periodic sleep, frame buffering
- sleep-mode without missing a message (early wake-up)

Association/Reassociation of stations to an infrastructure network by

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

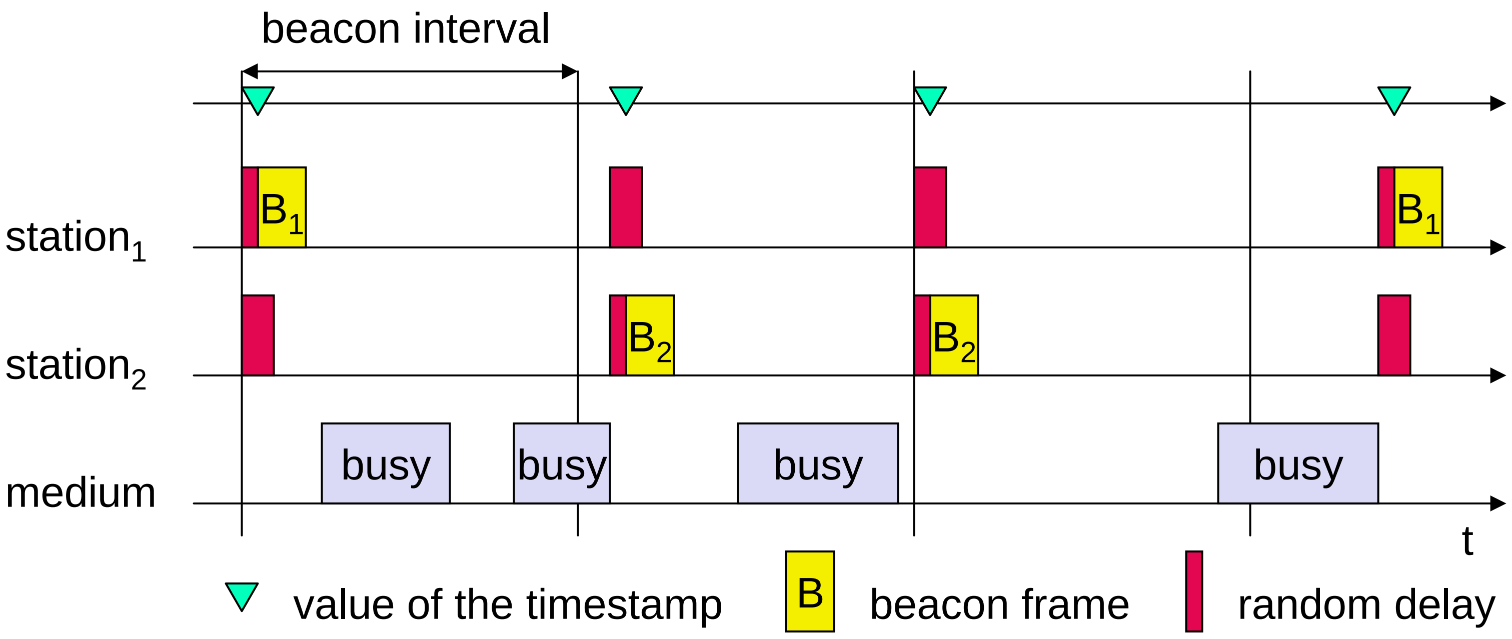
Synchronization using a Beacon frame (1)

in Infrastructure networks:



Synchronization using a Beacon frame (2)

in Ad - hoc networks:



Power management

Idea: switch the station off if not needed

States of a station: sleep and awake

Timing Synchronization Function (TSF)

- stations wake up early enough at the same time

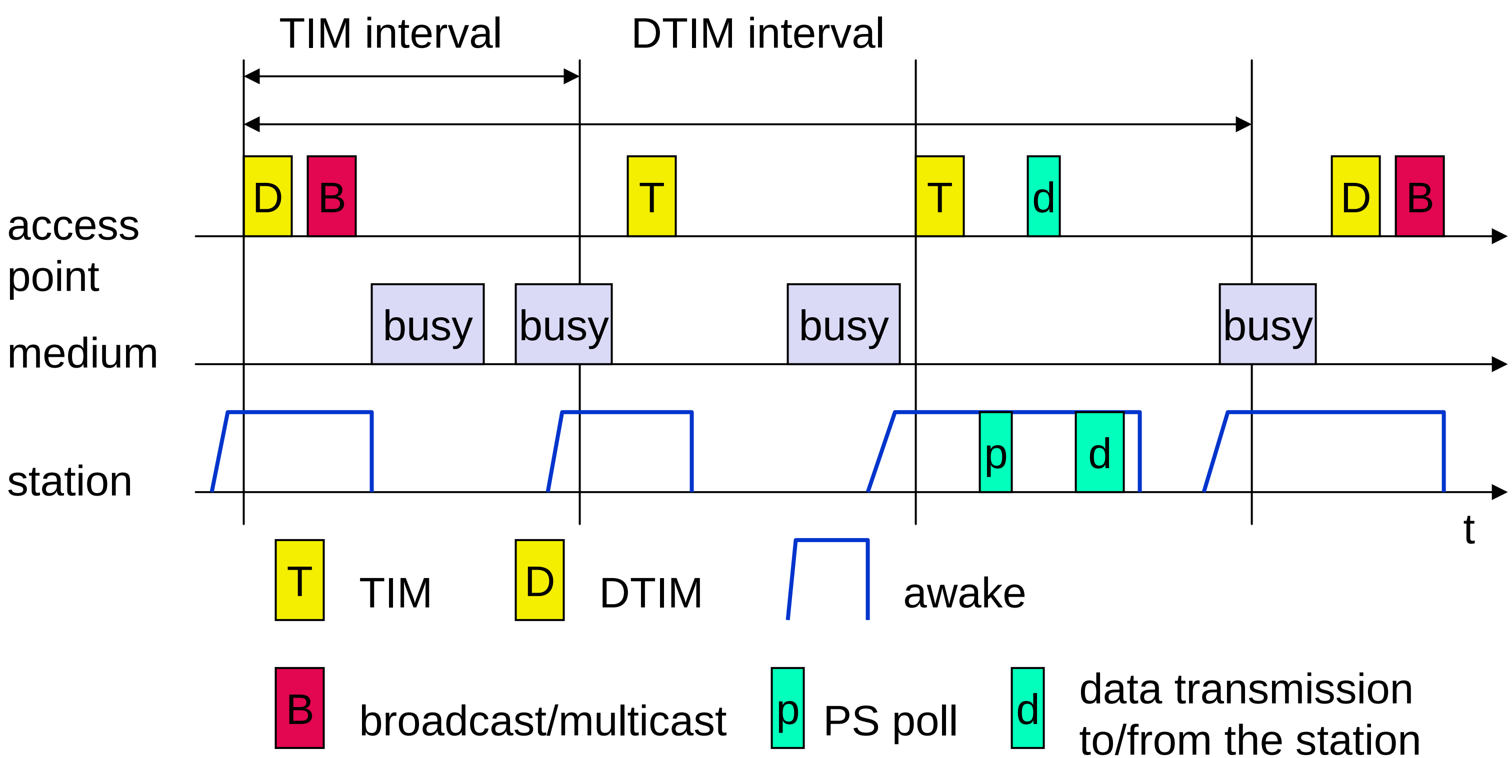
Infrastructure

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

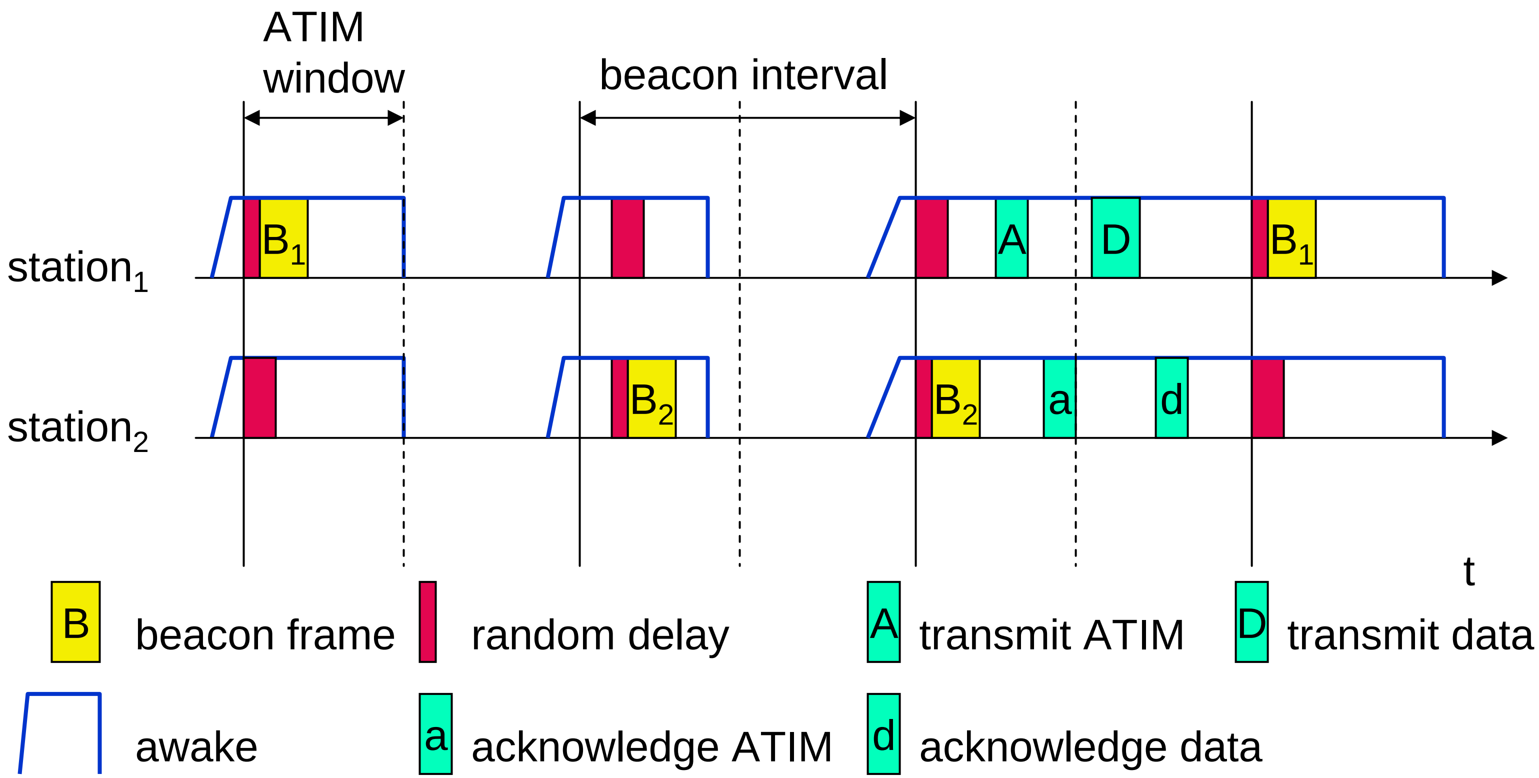
Ad-hoc

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

Power management in infrastructure networks



Power management in Ad-hoc networks



Roaming in infrastructure networks

No or bad connection? Then perform roaming by:

Scanning

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

Association Request

- station selects the best AP and sends an association request to it

Association Response

- success: AP has answered positively, station can now participate
- failure: no positive answer, continue scanning

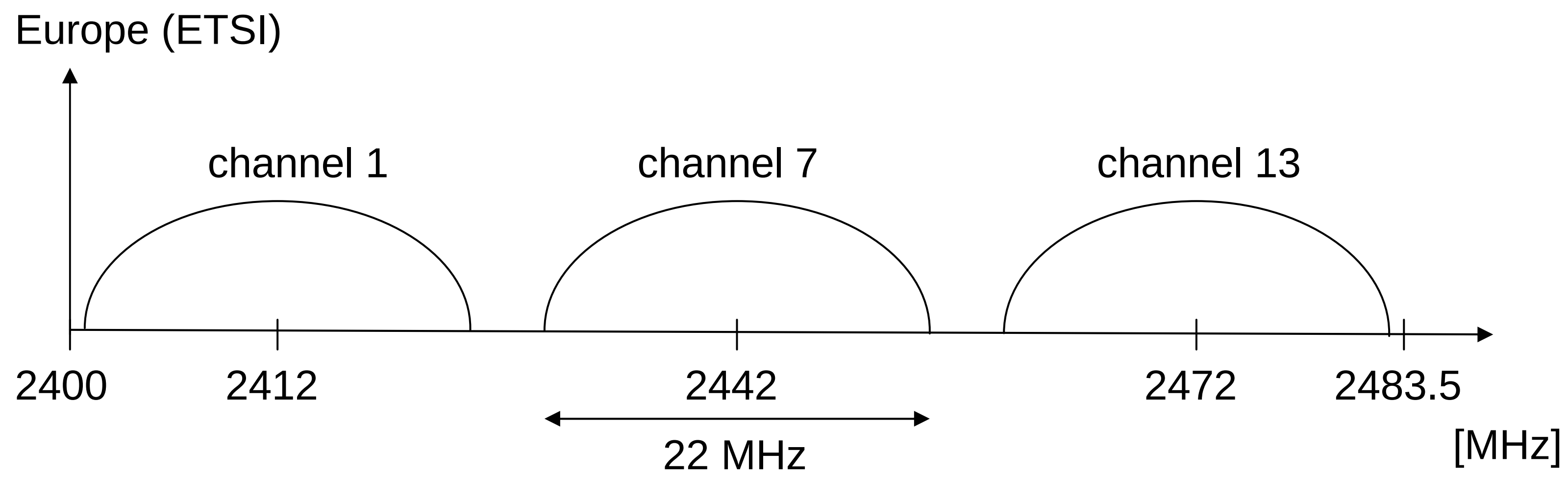
IF AP accepts Association Request, it

- signals the new station to the Distribution System (DS)
- 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

Variations of the IEEE 802.11 (WLAN) Standard (1)

802.11 b

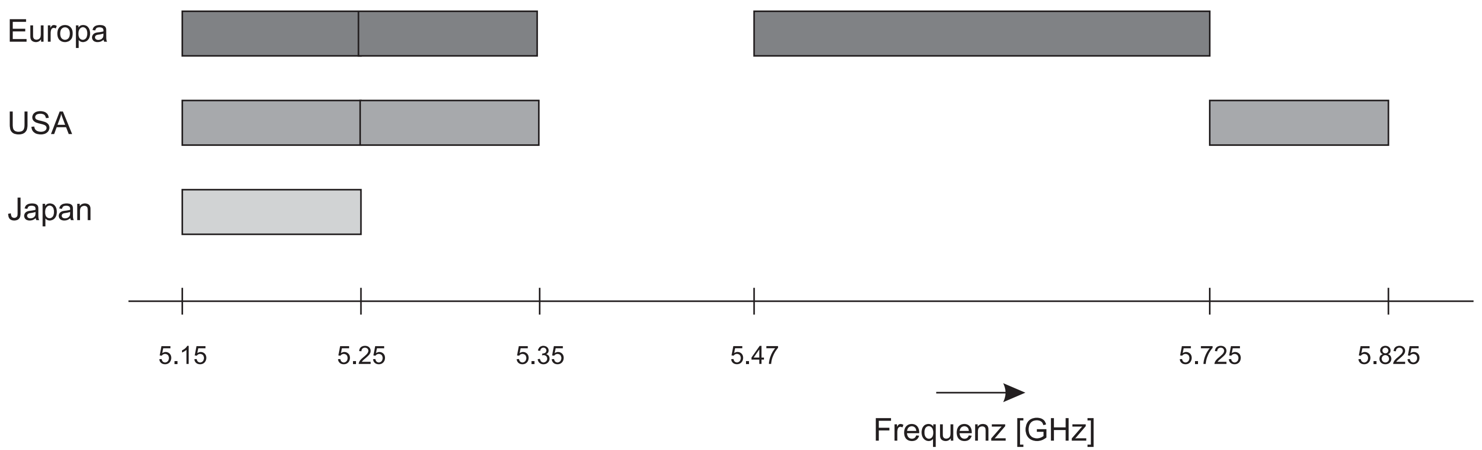
- Modifications in the transmission (physical layer) allowing data rates up to ca. 11 Mbit/s
- within license-free 2.4 GHz ISM-band
- 13 channels (N. America 11, Japan 14), each channel has a bandwidth of 22MHz



- Mac-layer remains the same

802.11 a

- Modifications in the transmission (physical layer) allowing data rates up to ca. 54 Mbit/s
- within 5 GHz ISM-band
- OFDM (Orthogonal Frequency Division Multiplexing) used
- altogether 455 MHz available (USA 300, Japan 100)



- less transmission range (e.g. 54 Mbit/s up to 5 m, 24 up to 30m, 12 up to 60 m)
- some products
- Mac-layer remains the same

WLAN: IEEE 802.11 – actual developments

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 priority classes
- 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; if 54 Mbit/s ---> OFDM

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

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

Summary (1)

- For WLANs (corresponding to the IEEE 802.11 standard) exist different physical layers all having a uniform interface to the MAC layer.
- The 802.11 standard (1997) defines two physical layers in the license-free 2,4 GHz ISM -band (FHSS and DSSS) and one physical layer in the infrared frequency range supporting data rates of 1 and 2 Mbit/s each.
- Almost all commercial products use FHSS or DSSS technology, in the beginning mostly FHSS.
- Nowadays DSSS is mostly used because can also support data rates of 5,5 and 11 Mbit/s. Those extensions have been defined 1999 in the 802.11b standard.
- Also since 1999, the 802.11a standard defines an additional physical layer in the licensed 5 GHz band. It uses the OFDM technology providing data rates up to 54 Mbit/s. It has strong similarities to the European standard HIPERLAN/2 using the same technology.
- Higher data rates in general imply less transmission range. E.g., FHSS und DSSS systems with 2 Mbit/s offer a range of about 100m, with OFDM technology providing 24 Mbit/s it is only about 30m, providing 54 Mbit/s only 5 m.

Summary (2)

- Ad-hoc networks consist of cells with limited range in which stations can communicate wireless.
- Infrastructure networks connect many individual cells via a wired (backbone) network called Distribution System. The connection point for each cell to the DS is the Access Point. This allows the stations of the cells to access also external networks like the Internet. However, the necessary protocols so far are not part of the 802.11 standard specification, but is vendor-dependent (802.11f is an ongoing attempt to change this).
- In infrastructure networks APs support the *roaming* of mobile stations, meaning that stations can freely move from one cell to the other without leaving connection to the external network at any time. Scanning allows stations to find adequate new APs to submit registration requests.
- The standard procedure to control shared access on the MAC-layer (CSMA/CA) is adopted from its wired pendant, the Ethernet (CSMA/CD). Because the radio medium does not allow to detect collisions reliably, collisions should be avoided by introducing random back-off (waiting) times.
- Additionally exchanging short control messages (Request-to-Send/Clear-to-Send) enhances considerably the probability of collision-free medium access because it introduces an implicit medium reservation scheme and it solves the *hidden station* problem.
- The optional PCF approach may support time- critical (real-time) applications, because collision-free access can be guaranteed due to a centralized (master/slave) control of the medium access.
- Synchronization of station-internal clocks and power management allowing stations to enter a „sleep“ mode contributes to save energy without risking message losses.

802.11 versus 802.3

802.3 MAC Sublayer:

- implements CSMA/CD
- CD works because the medium takes care that every collision at the receiver of a message also happens at the sender

  --> CD in 802.3 relies on the fact that the sender detects the collision at his site and concludes from that the collision at the receiver

Problem:

This does no longer hold if radio communication is applied --> CD does not work in 802.11

- signal strength decreases proportional to the square of the distance

  ---> radio range is restricted
- collisions at the sender do no longer compare to collisions at the receiver

  ---> hidden station problem

  ---> exposed station problem