Mobilkommunikation - Mobile Communications

Lecture 7: Wireless Local Area Networks

Prof. Dr.-Ing. Markus Fidler

Institute of Communications Technology
Leibniz Universität Hannover

June 10, 2016

Previous lecture

Random access

- ALOHA: throughput limited to 0.18 resp. 0.37
- CSMA: adds carrier sense to ALOHA
- MACA: RTS/CTS to deal with hidden and exposed stations
- CSMA/CD: collision detection; not applicable in wireless case
- CSMA/CA: collision avoidance using backoff procedure
  - stations wait for a random time before accessing the channel
  - countdown is uniformly distributed in the contention window
  - optimal window size depends on the number of contenders
  - collisions are used to double the contention window
  - as an option 4-way handshake with RTS/CTS
  - implemented in IEEE 802.11 Wifi

Outline

Wireless LAN overview

IEEE 802.11 Wifi
- System overview
- MAC management
- Medium access control
- Physical layer

Overview

Wireless LANs

- wireless access
  - office
  - home
  - production environments
- restricted diameter
  - rooms
  - buildings
  - campus
- usually operated by individuals
- target: replace office cabling

Advantages

Advantages of wireless over wired LANs

- **flexibility:** stations can communicate without restriction within radio coverage; radio waves can penetrate walls
- **no planning:** ad-hoc communication in wireless networks; no wiring plans
- **design:** small, independent devices; stations can be hidden in pockets, walls, etc.
- **robustness:** wired networks often do not survive disasters whereas wireless communications can
- **cost:** once a wireless access point is installed additional users can be added at virtually no cost

Disadvantages

Disadvantages of wireless compared to wired LANs

- **quality of service:** typically quality of service is much lower in wireless LANs due to limited bandwidth, higher error rates due to interference and fading, and higher delays due to error detection and correction
- **proprietary solutions:** wireless LAN development has seen many proprietary, non-interoperable solutions while standardization was slow
- **restrictions:** many government and non-government institutions regulate operation and restrict frequencies; license-free frequency bands differ from country to country
- **safety:** interference can cause safety hazards, e.g. plane
- **security:** eavesdropping is very simple in wireless communications; strong encryption and privacy mechanisms are needed

Design goals

Drivers of commercial success of wireless LANs

- **global operation:** national and international frequency regulations have to be considered
- **licensing:** license-free frequency bands, e.g. ISM
- **robust transmission:** need to handle interference
- **ad-hoc communication:** simple, automatic setup procedure
- **easy to use:** plug and play
- **inter-operability:** protect previous investments; bridging with existing wired LANs; backwards compatibility;
- **low power:** battery power is limited and requires power-saving modes and power management
- **safety and security:** interference and eavesdropping
- **transparency:** hide details from applications; provide the same API as wired LANs

Infrared vs. radio transmission

Infrared

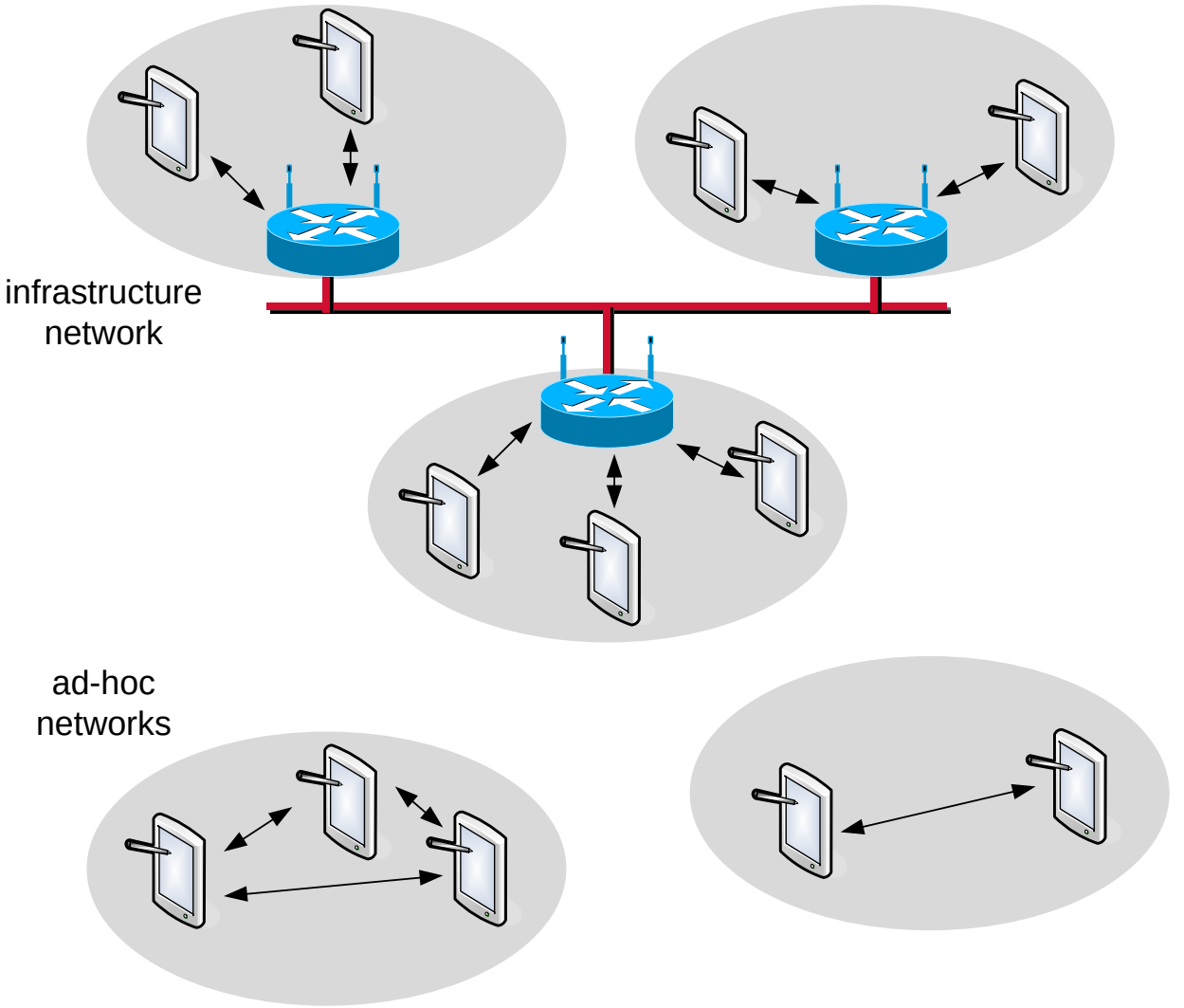
- diffuse light; reflections or direct line-of-sight
- advantages
  - simple and extremely cheap
  - no licensing, local and shielded operation
  - no electrical interference
- disadvantages
  - easily shielded
  - high data rates only in case of line-of-sight communication
- infrared data association (IrDA)
  - version 1.0 up to 115 kb/s
  - version 1.1 up to 4 Mb/s

Infrared vs. radio transmission continued

Radio

- advantages:
  - can cover large areas
  - can penetrate walls and other obstacles
  - typically does not need line-of-sight
  - high transmission rates
- disadvantages:
  - shielding is difficult
  - interference
  - licensing of radio spectrum
  - safety and security issues

Infrastructure vs. ad-hoc networks



Infrastructure vs. ad-hoc networks continued

Infrastructure

- communication only between wireless stations and the access point; no direct communication between wireless stations
- access point provides forwarding functions and access to other networks
  - acts as a bridge to other networks
  - several wireless networks can form one large logical network
- access point can implement centrally coordinated (collision-free) medium access
  - can provide quality of service guarantees
  - but less flexible
- simpler design
  - much functionality in the access point
  - wireless stations remain simple
- typically used in IEEE 802.11 Wifi

Infrastructure vs. ad-hoc networks continued

Ad-hoc

- wireless stations can communicate directly with each other
  - no infrastructure is needed
  - no access point controls medium access
- complexity of wireless stations is higher
  - each station has to implement mechanisms for medium access
- very high flexibility
- used in IEEE 802.15 Bluetooth

Often features of infrastructure and ad-hoc networks are mixed

- infrastructure-based networks may permit direct communication between wireless stations
- ad-hoc networks may have selected stations with the capability to forward data

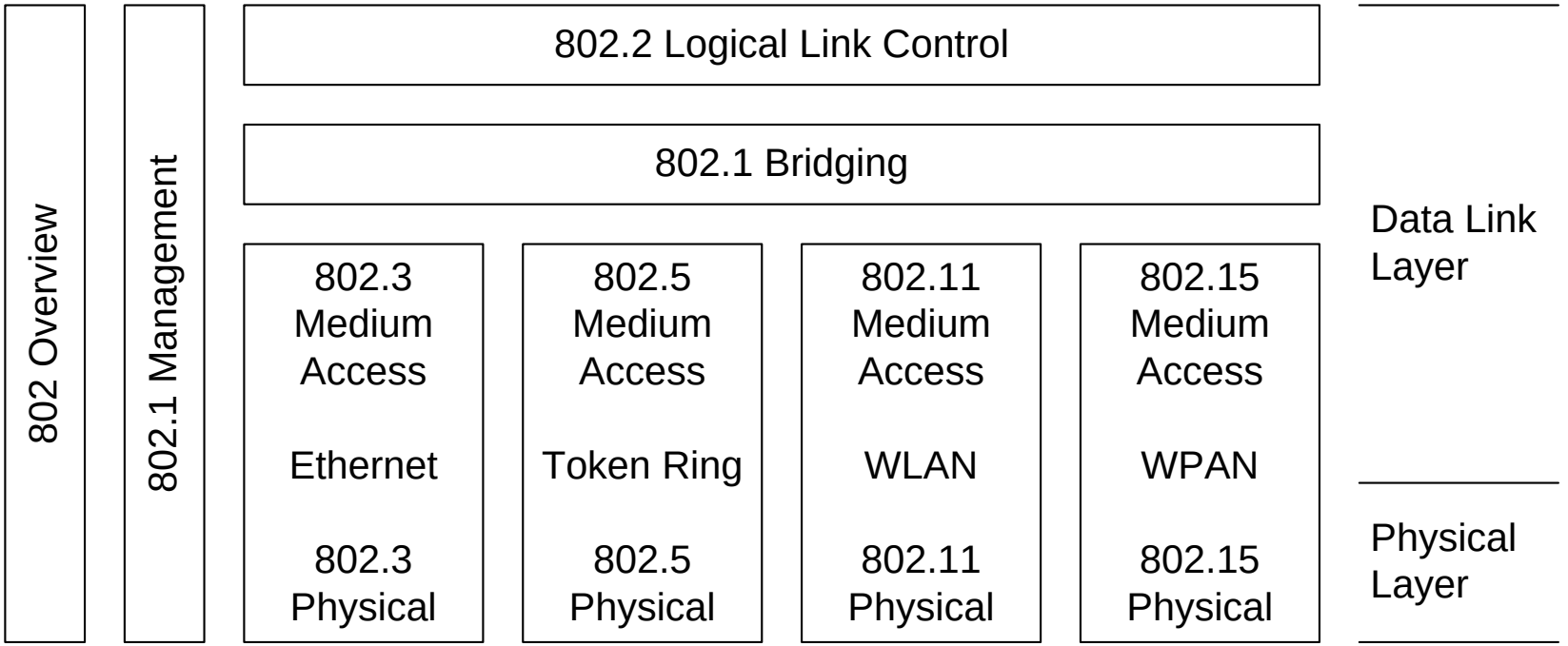
Outline

Wireless LAN overview

IEEE 802.11 Wifi
- System overview
- MAC management
- Medium access control
- Physical layer

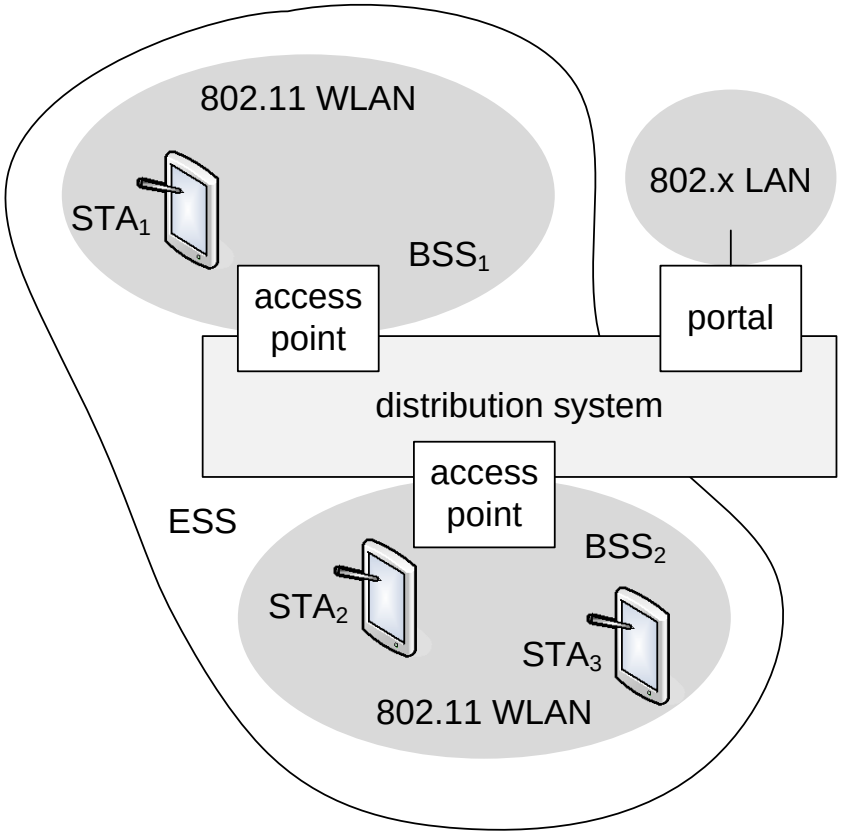
IEEE 802 Standardization

The Institute of Electrical and Electronics Engineers (IEEE) published a number of important standards for local area networks (LANs) and personal area networks (PANs).



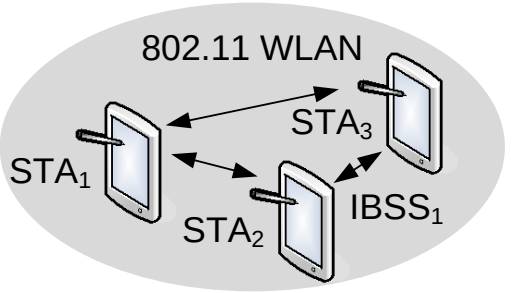
IEEE 802.11 system architecture: infrastructure

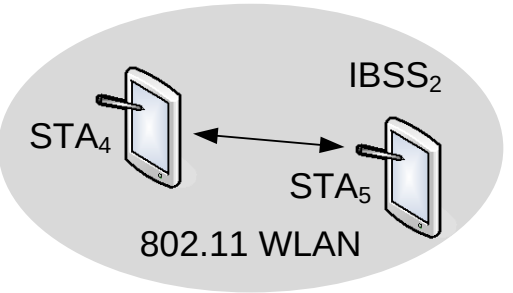
- STA: station
- access point
- BSS: basic service set
- distribution system
- portal
- ESS: extended service set



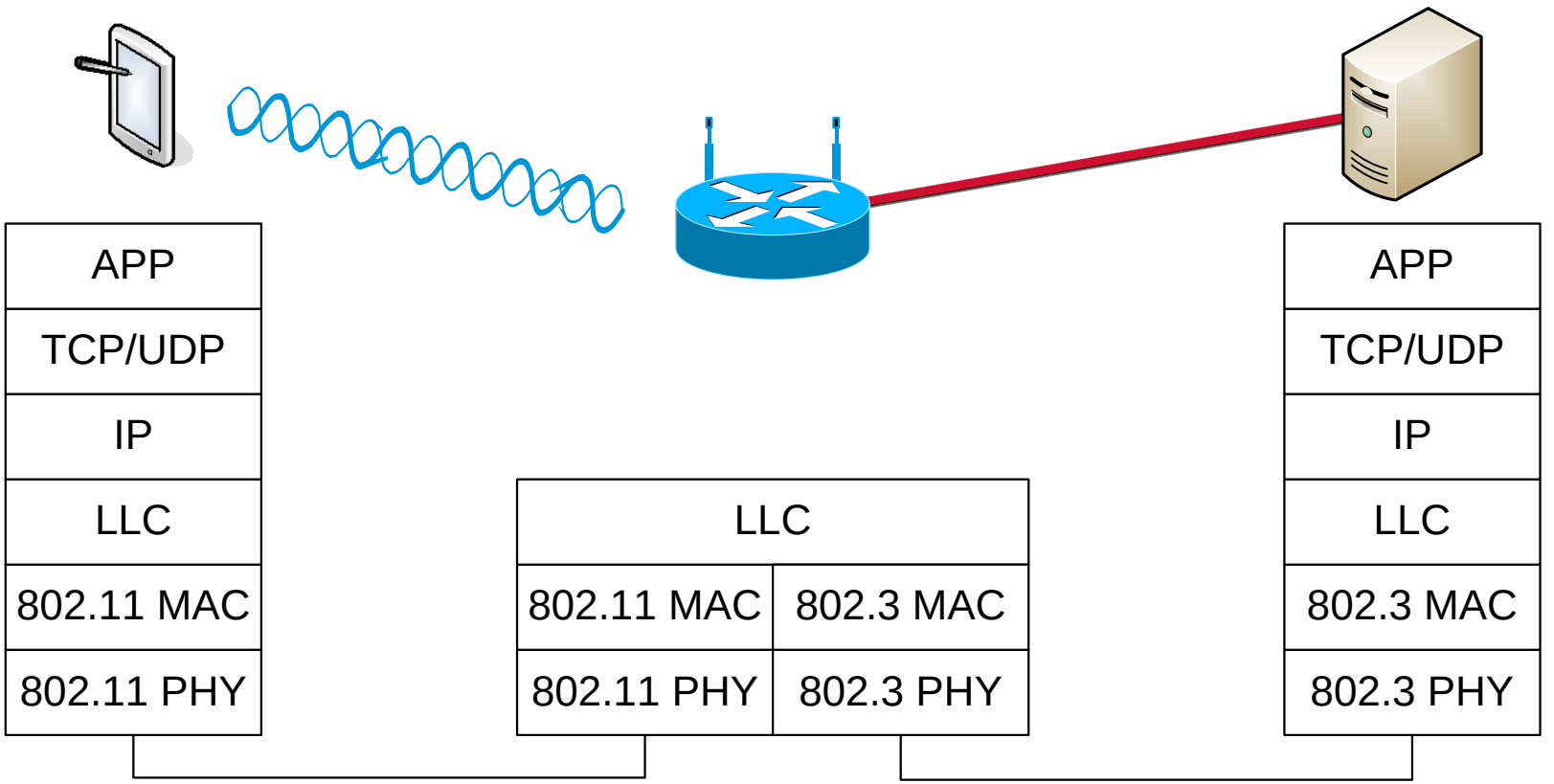
IEEE 802.11 system architecture: ad-hoc

- STA: station
- IBSS: independent basic service set



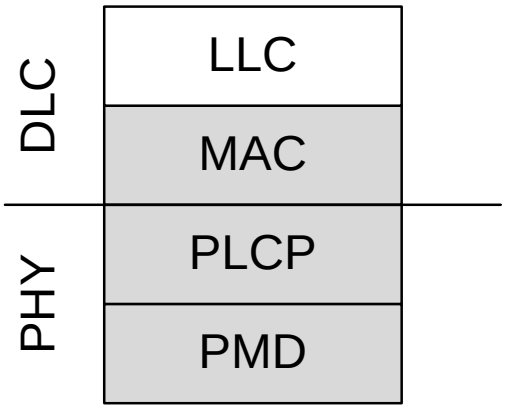


IEEE 802.11 protocol architecture



IEEE 802.11 protocol stack

- DLC: data link control
  - LLC: logical link control
  - MAC: medium access control
    access mechanism, fragmentation
- PHY: physical layer
  - PLCP: physical layer convergence protocol
    clear channel assessment, carrier sense
  - PMD: physical medium dependent
    modulation, encoding



- MAC management: synchronization, roaming, power control
- PHY management: channel selection

MAC management

MAC management includes fundamental functions for e.g.

- integrating a station into a BSS
- forming an ESS, etc.

Functional groups:

- **synchronization:** finding a WLAN; synchronization of internal clocks; generation of beacon signals
- **power management:** control transmitter activity to conserve power; periodic sleep with buffering of data
- **roaming:** scanning for access points; association with an access point; changing access points
- **management information base (MIB):** storing the current state of wireless stations; access via the simple network management protocol (SNMP)

Synchronization

All IEEE 802.11 nodes (stations and access points) maintain internal clocks that have to be synchronized

- timing synchronization function (TSF)

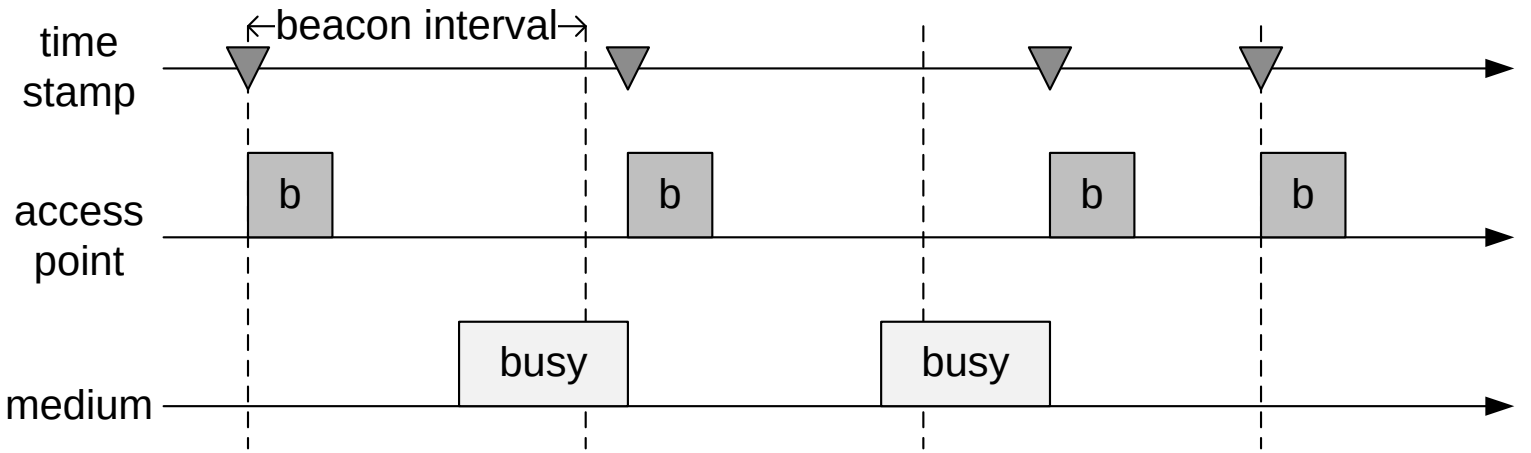
Synchronized clocks are needed e.g. for

- power management
- medium access control
- frequency hopping

Beacon frames

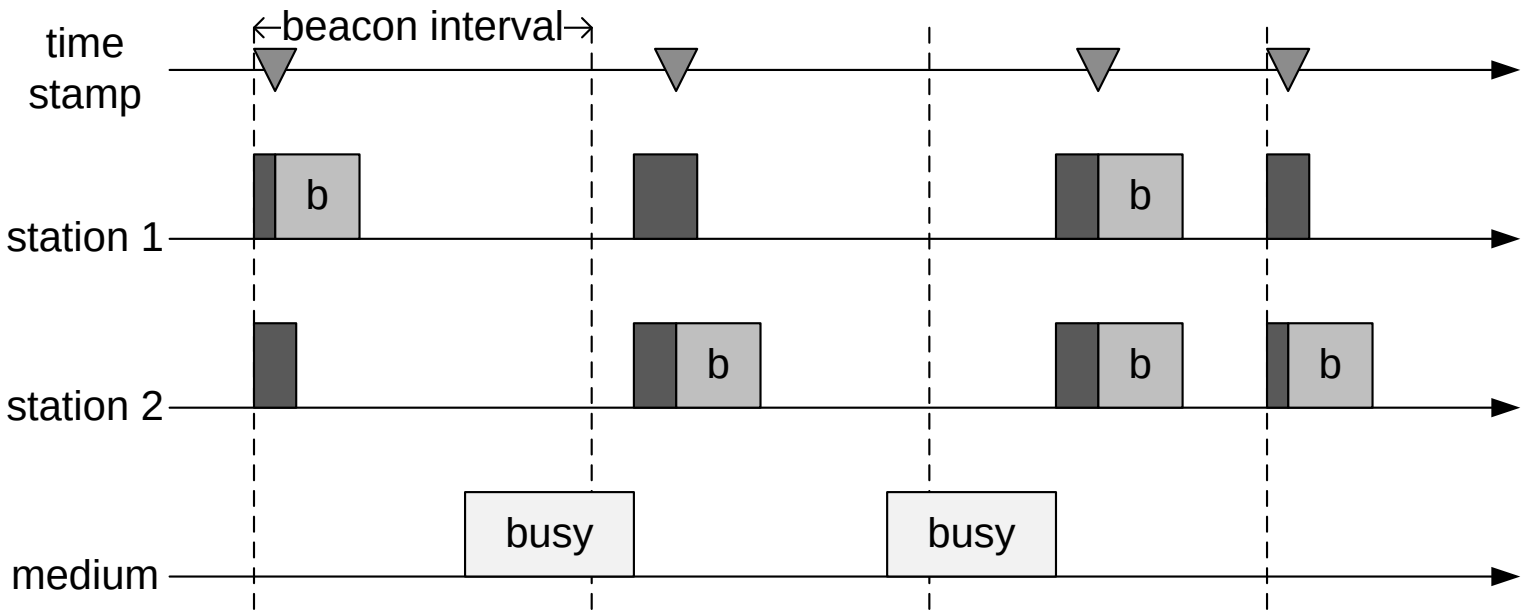
- (quasi)periodic transmission
  (beacon is deferred if the medium is busy)
- contains timestamp to which nodes adjust their local clocks

Synchronization: infrastructure



- beacon frames are transmitted according to a fixed schedule
- a beacon may be delayed if the medium is busy, however, the future schedule is not changed
- the timestamp transmitted in the beacon is the actual time of sending the beacon

Synchronization: ad-hoc



- all stations attempt to transmit beacon frames after a beacon interval expires
- stations perform, however, the random backoff algorithm
- one station wins and all others adjust their time to this station
- collisions of beacon frames are possible

Power management

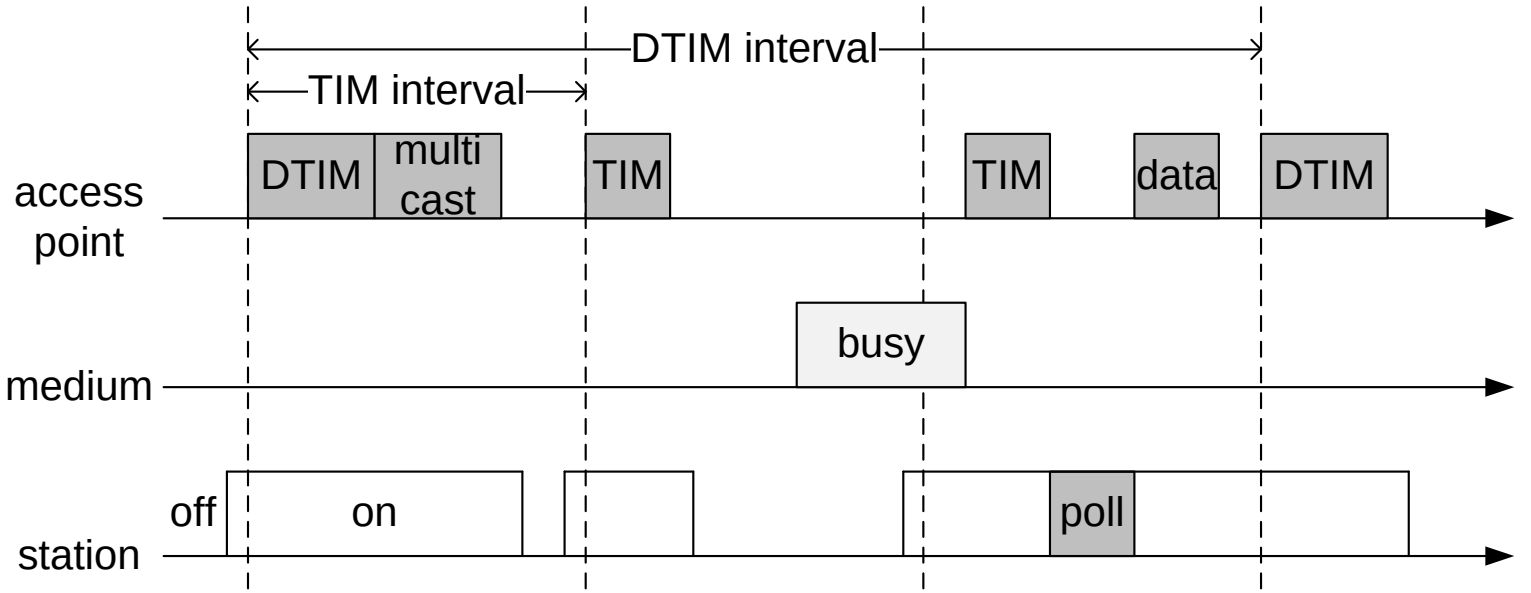
Power saving is crucial

- battery powered devices
- receiver current can be up to 100 mA

Power management

- switch off the transceiver when not needed
- sender wake-up
  - simple since data transfer is caused by the device itself
- receiver wake-up
  - receiver cannot know when it has to be ready to receive
  - data has to be buffered in senders meanwhile
  - receiver has to wake-up periodically and stay awake for a while
  - during this time senders can announce the availability of data
- two states: sleep and awake
- tradeoff battery life vs. delay/bandwidth

Power management: infrastructure



- the access point sends a traffic indication map (TIM) with every beacon
- the TIM contains a list of stations for which data is available
- the TSF assures that stations wake up at the right time
- an additional delivery TIM (DTIM) for multi-/broadcast

Roaming

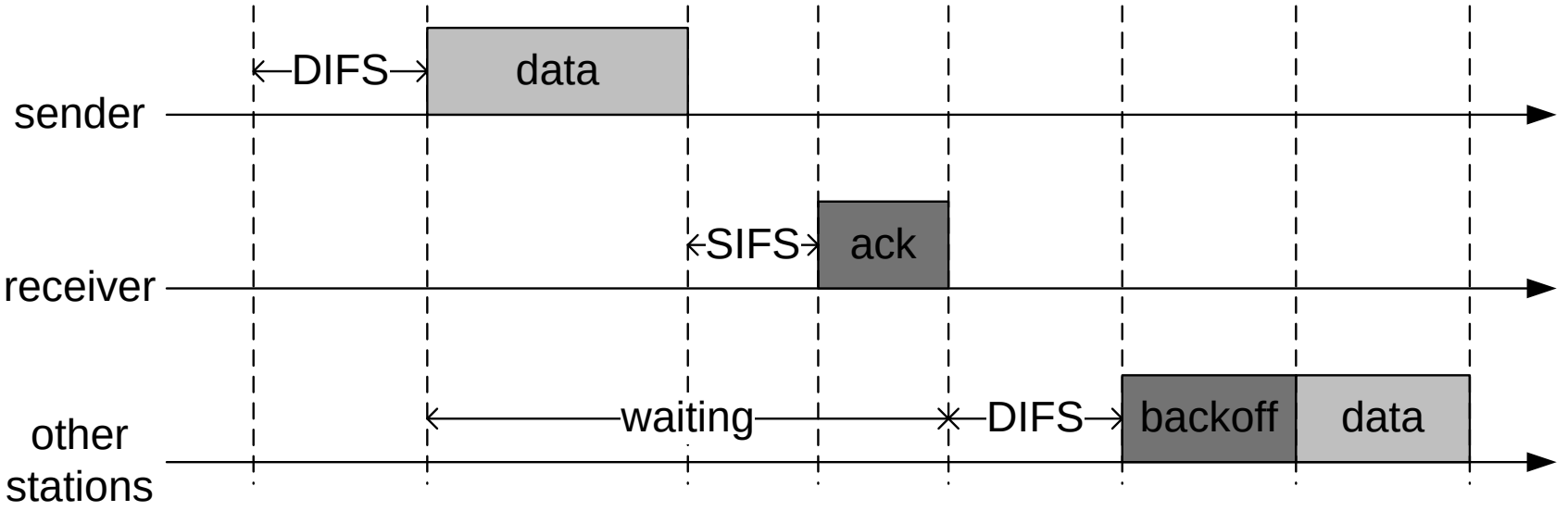
- indoors access points have a transmission range of 10-30 m
- several access points are needed to cover e.g. several rooms
- mobile stations move from one access point to another

$\Rightarrow$ roaming

Roaming involves

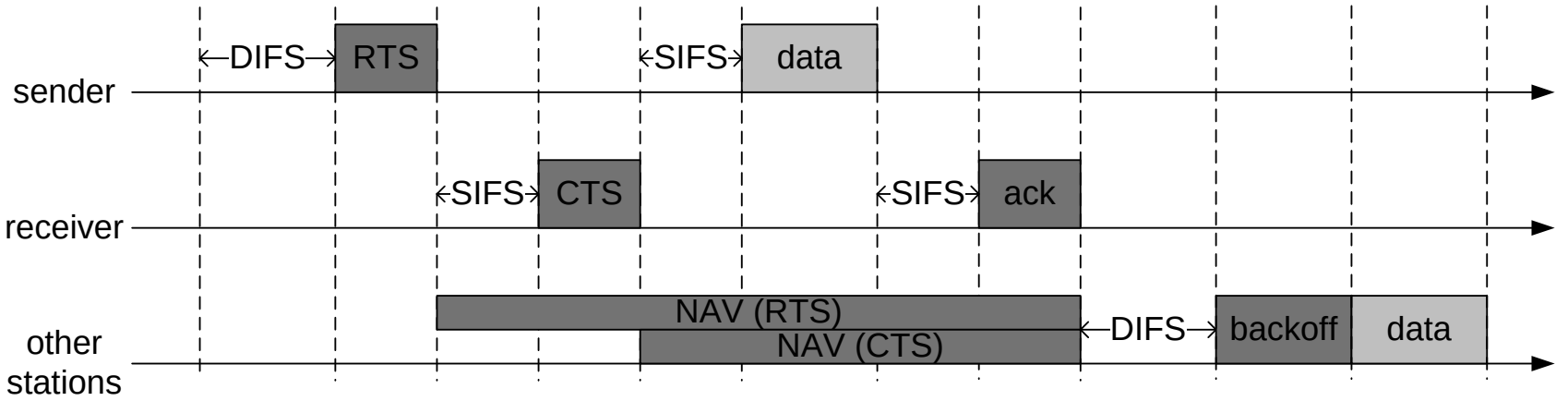
- **scanning** for other access points if the link quality becomes poor; can be performed on multiple channels
  - **passive scanning** listening for beacons of other stations
  - **active scanning** sending of probes and waiting for a response
- **association request** sent by the station to the best BSS
- the access point of the new BSS indicates the presence of the station to the distribution system
- the distribution system stores the location of the station in its database to be able to forward downlink data

Distributed coordination function (DCF)



- stations are permitted to send if the channel is idle for a DIFS period (carrier sense)
- acknowledgements are sent after SIFS (SIFS $<$ DIFS)
- if the channel is busy stations perform random backoff
- stations contend for the channel possibly causing collisions
- in case of a collision the contention window is doubled

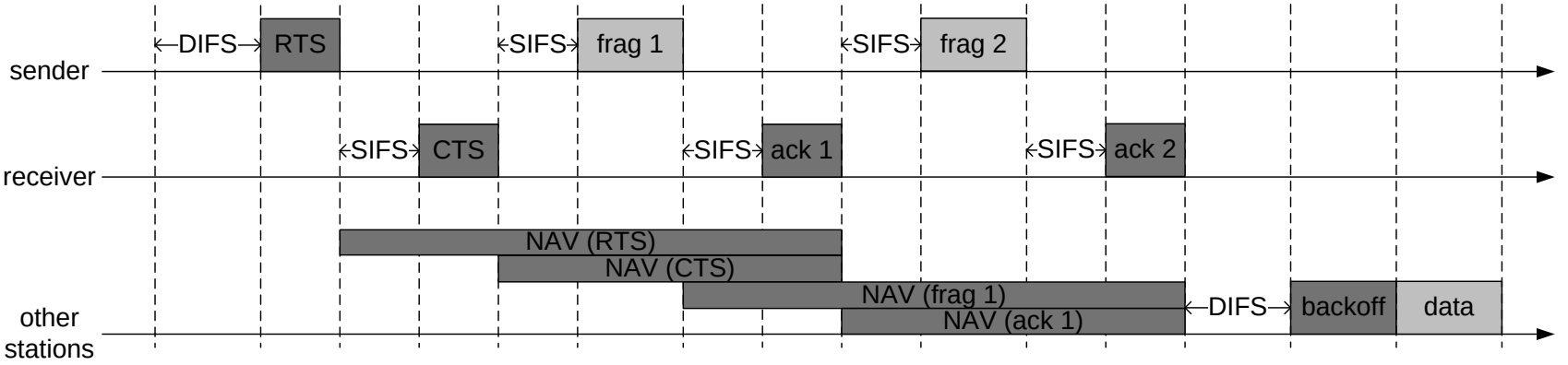
DCF with RTS/CTS



4-way handshake to address the problem of hidden and exposed stations

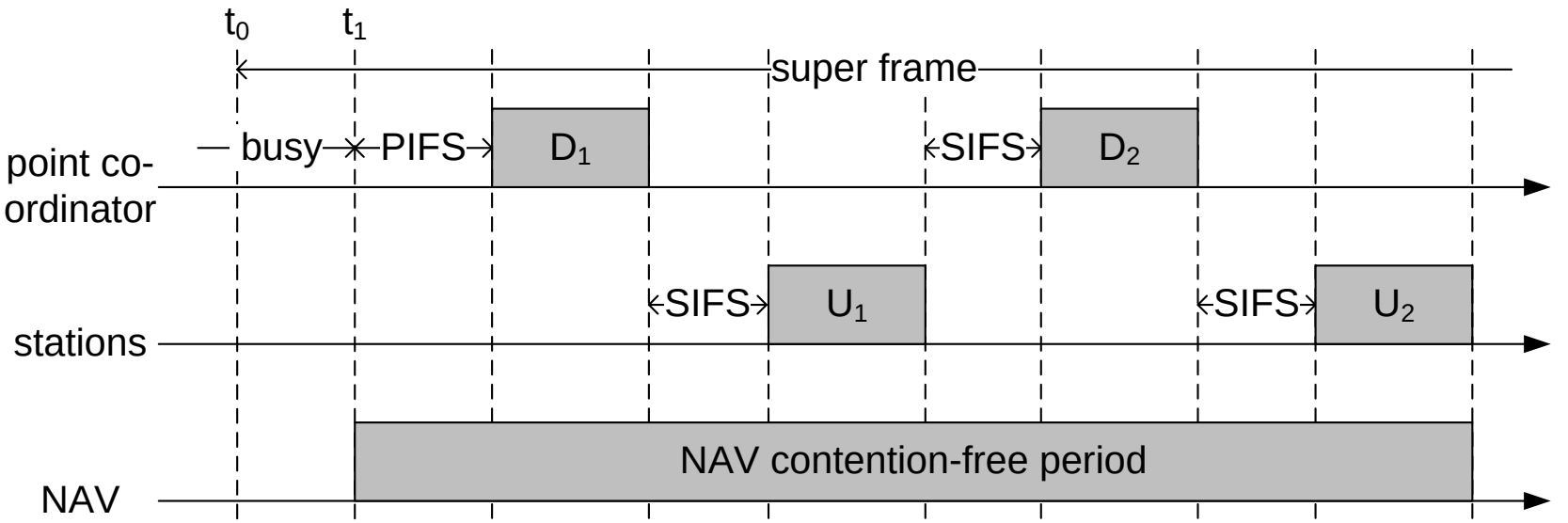
- RTS: request to send
- CTS: clear to send
- NAV: network allocation vector

DCF with RTS/CTS and fragmentation



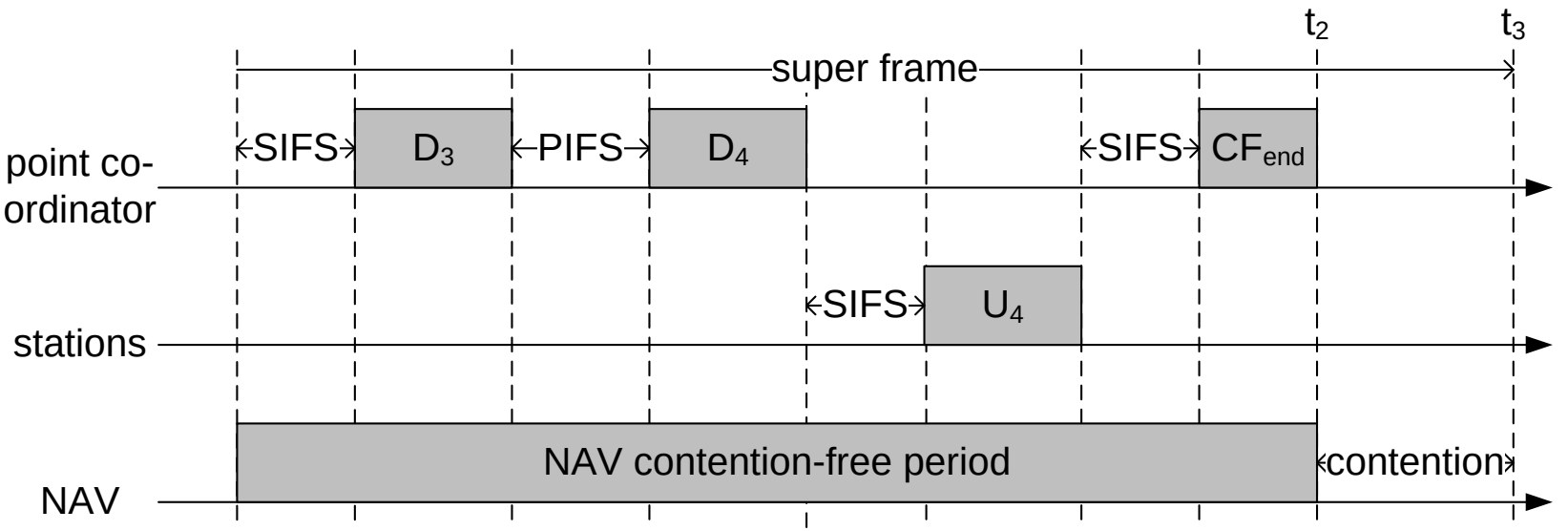
- the 4-way handshake adds significant protocol overhead
- the amount of signalling per unit of data is reduced if larger data packets are transmitted
- larger data packets are, however, more susceptible to bit errors
- solution: fragmentation
- fragments and acknowledgements contain a new NAV except in case of the last fragment

Point coordination function (PCF)



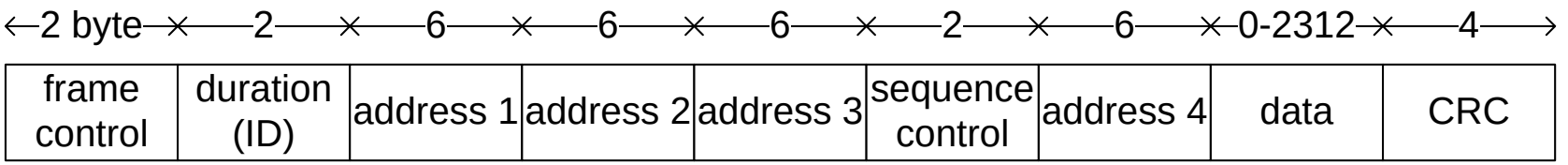
- PCF inter-frame space (PIFS) where SIFS $<$ PIFS $<$ DIFS
- periodic super frames
  - contention-free period with polling
  - point coordinator polls each station (possible resource waste)
- legend: D_i and U_i data to and from station i

PCF continued



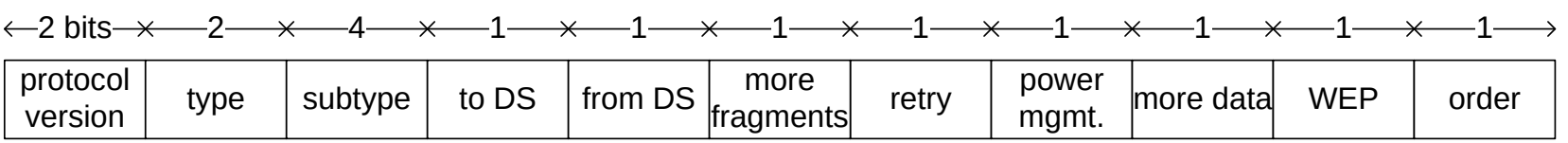
- station 3 has no data to send; the access point polls station 4 after PIFS
- CF_{end} indicates end of the contention-free period
- a contention period using the DCF random access mechanism follows until the next super frame starts

MAC frame format



- **frame control:** 2 control bytes, see next slide
- **duration (ID):** in μs used for NAV
  above 32768 reserved values used as IDs
- **addresses:** 1 to 4 MAC addresses of 48 bits
- **sequence control:** frames are numbered to filter out duplicates at the receiver
- **data:** up to 2312 bytes
- **CRC:** checksum to detect transmission errors

MAC frame control



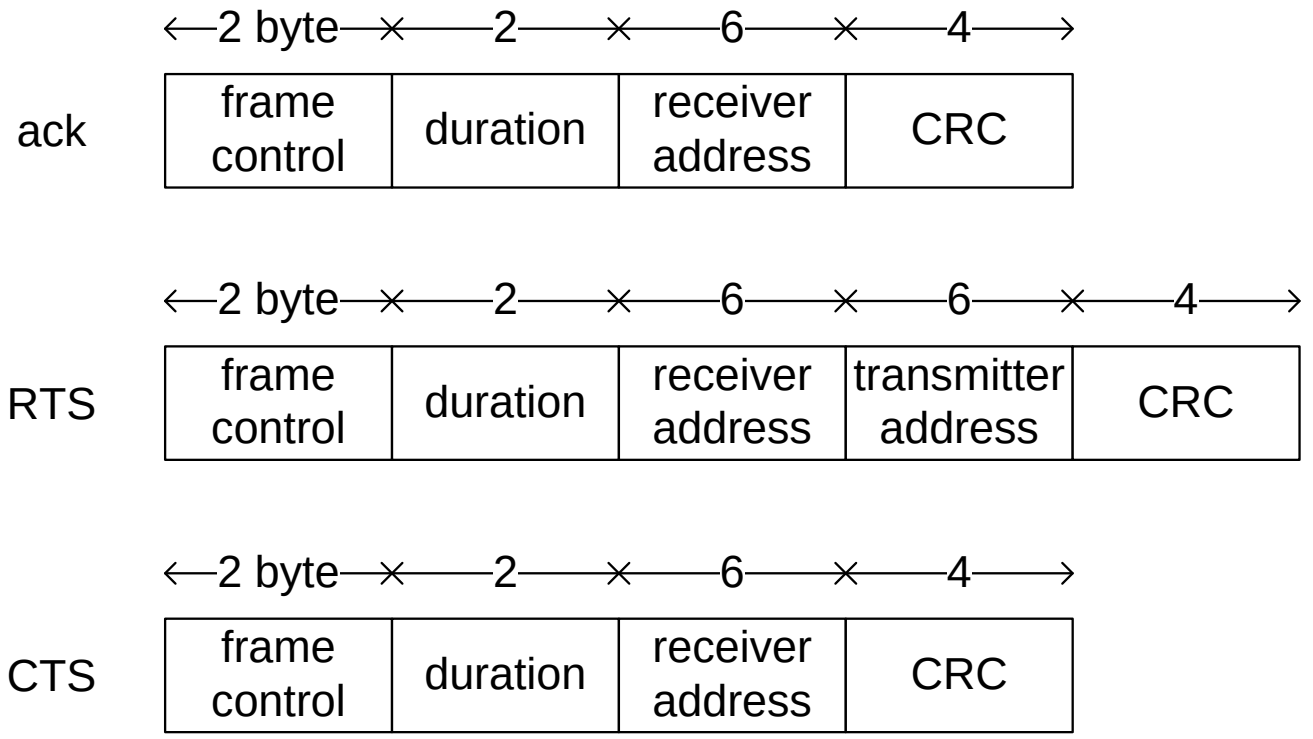
- **protocol version:** 2 bit, current protocol version 00
- **type:** management = 00; control = 01; data = 10
- **subtype:** e.g. management: association request = 0000; beacon = 1000; and control: RTS = 1011; CTS = 1100
- **more fragments:** set to 1 for all but the last fragment
- **retry:** set to 1 to indicate retransmissions
- **power management:** set to 1 if the station goes into power save mode, 0 if it stays awake
- **more data:** set to 1 if there is more data for a destination, e.g. to prevent a receiver from going to power save mode
- **WEP:** wired equivalent privacy (many weaknesses)
- **order:** set to 1 if frames must be processed in order

MAC addresses

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

- DS: distribution system
- AP: access point
- DA: destination address
- SA: source address
- TA: transmitter address
- RA: receiver address
- BSSID: basic service set identifier

Some specific MAC frames

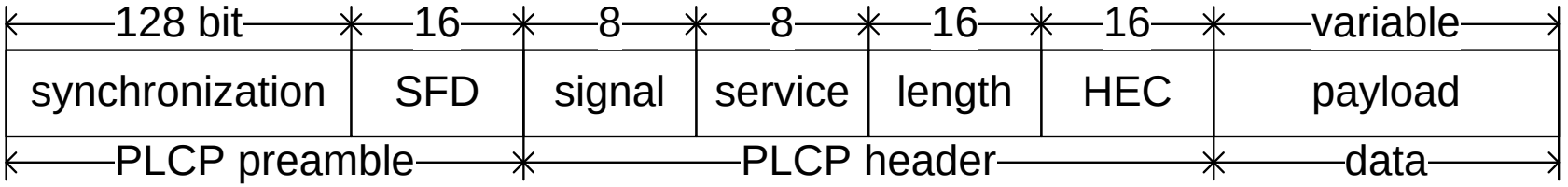


IEEE 802.11 modulation

Three versions with data rates of 1 and 2 Mb/s

- frequency hopping spread spectrum (FHSS)
  - min 2.5 frequency hops per second
  - two-level Gaussian frequency shift keying (GFSK) modulation
- direct sequence spread spectrum (DSSS)
  - Barker code chipping sequence:
    $(+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1)$
  - differential binary phase shift keying (DBPSK) modulation or differential quadrature phase shift keying (DQPSK)
- infrared
  - 850-940 nm
  - diffuse light (non line of sight)
  - range 10 m

IEEE 802.11 DSSS physical frame format

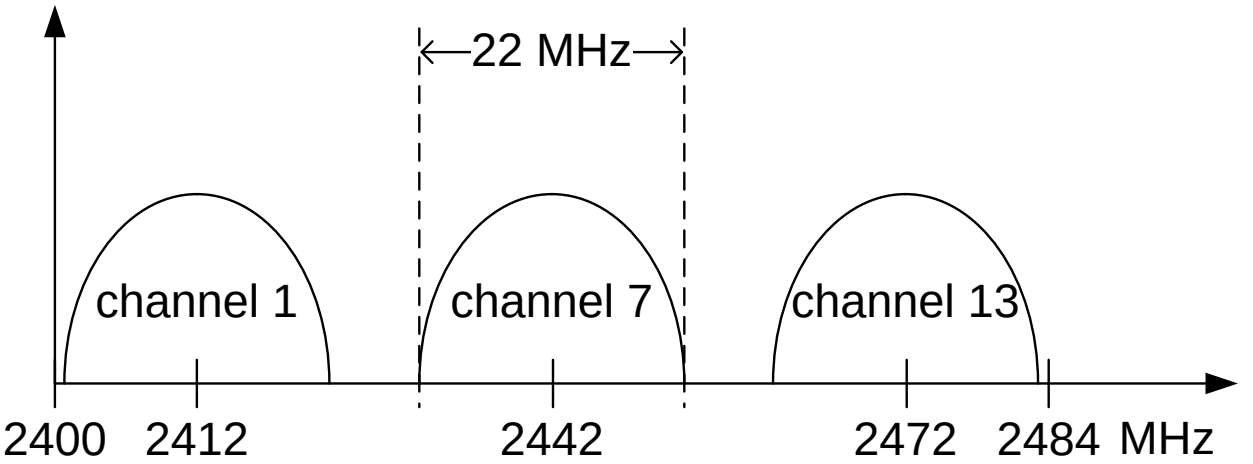


- **synchronization:** synch., gain setting, energy detection (clear channel assessment), frequency offset compensation
- **SFD:** start frame delimiter (pattern 1111001110100000)
- **signal:** 0x0A indicates 1 Mb/s, 0x14 indicates 2 Mb/s following standards define higher data rates
- **service:** 0x00 (reserved for future use)
- **length:** length of the payload (in μs)
- **HEC:** header error checksum

IEEE 802.11a/b/g/n standard evolution

standard	802.11b	802.11a	802.11g	802.11n
released	1999	1999	2003	2009
frequency	2.4 GHz	5.15 GHz	2.4 GHz	both
antenna	SISO	SISO	SISO	MIMO
modulation	DSSS	OFDM	OFDM, DSSS	OFDM
send power	100 mW	30 mW	100 mW	depends
range (indoor)	300(30)m	100(10)m	300(30)m	300(30)m
disjunct channels	3	12	3	depends
bandwidth	22 MHz	20 MHz	20 MHz	10, 20, 40
gross data rate	11 Mb/s	54 Mb/s	54 Mb/s	600 Mb/s
net data rate	≈7 Mb/s	≈26 Mb/s	≈26 Mb/s	>100 Mb/s

IEEE 802.11b channels in Europe



- 13 channels defined
  - centered at 2412, 2417, 2422, ... MHz
  - channel width 22 MHz
- maximum of 3 non-overlapping channels

IEEE 802.11a coding and modulation

data rate Mb/s	modulation	coding rate	coded bits per carrier	coded bits per OFDM symbol	data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

OFDM with 64 subcarriers and 312.5 kHz per subcarrier

- 52 subcarriers, 48 data + 4 pilot, plus $2 \cdot 6$ as guard channel
- 250000 symbols per second, 0.8 μs guard + 3.2 μs data

IEEE 802.11g inter-operation with b

High data rates in the 2.4 GHz band

- new modulation and coding schemes
- OFDM

similar to IEEE 802.11a

However, 802.11g equipment has to coexist with 802.11b equipment in the same frequency band

- 802.11b equipment cannot sense 802.11g transmissions
- preamble is always sent at 1 Mb/s
- CTS sent at 1 Mb/s can be used to protect 802.11g transmissions

Backwards compatibility slows down the transmission

IEEE 802.11n evolution to higher data rates

Key enabling technologies

- OFDM to cope with inter-symbol interference at high data rates (a/g/n); improved OFDM and coding (factor 1.4)
- bond channels, allow use of double the bandwidth (factor 2)
- MIMO with ≤ 4 antennas for spatial multiplexing (factor 4)
- reduce MAC overhead

MAC efficiency enhancements

- frame bursting, block acknowledgements: use one ack for multiple frames
- frame aggregation: pack several IP datagrams into a single MAC frame
- reduced inter frame spacing (RIFS)

IEEE 802.11ac evolution to higher data rates

Increasing the data rate further

- only in the less crowded 5 GHz band
- 256 QAM with coding rates of 3/4 and 5/6, respectively
- guard intervals of 0.8 or 0.4 μs
- channel bonding to use 80 MHz or 160 MHz
- up to 8 spatial MIMO streams

Theoretical gross data rates of up to 867 Mb/s per spatial stream

Literature

- Jochen Schiller, Mobile Communications, Second Edition, Addison-Wesley, 2003.
- Vijay Garg, Wireless Communications & Networking, Morgan Kaufmann, 2007.
- Matthias Hollick, Mobile Networking, TU Darmstadt, 2008.