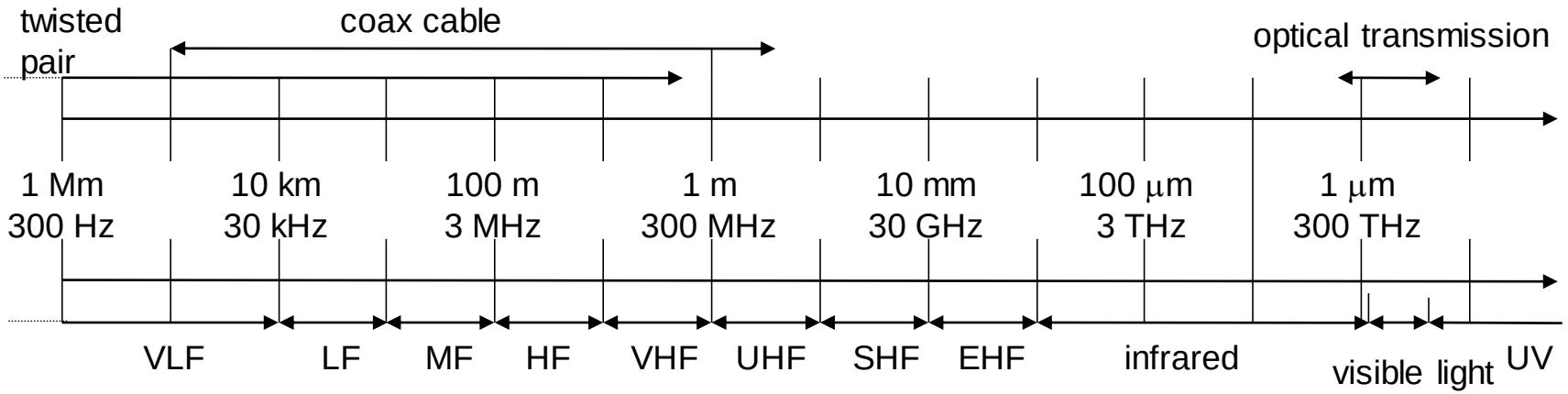
Wireless Communication
Session 4
Wi-Fi IEEE802.11 standard

M. Daneshvar Farzanegan

Soourosh.blogfa.com
smdanesh@yahoo.com

Reminder on frequencies and wavelenghts



VLF = Very Low Frequency
LF = Low Frequency
MF = Medium Frequency
HF = High Frequency
VHF = Very High Frequency

UHF = Ultra High Frequency
SHF = Super High Frequency
EHF = Extra High Frequency
UV = Ultraviolet Light

Frequency and wave length:

$\lambda = c/f$

wave length λ, speed of light $c \cong 3 \times 10^8$ m/s, frequency f

Frequencies for mobile communication

- VHF-/UHF-ranges for mobile radio
  - simple, small antenna for handset
  - deterministic propagation characteristics, reliable connections
- SHF and higher for directed radio links, satellite communication
  - small antenna
  - large bandwidth available
- Wireless LANs use frequencies in UHF to SHF spectrum
  - some systems planned up to EHF
  - limitations due to absorption by water and oxygen molecules (resonance frequencies)
    - Weather-dependent fading, signal loss caused by heavy rainfall etc.

Frequency allocation

	Europe	USA	Japan
Mobile phones	**Dig. Dividend** 800MHz **GSM** 890-915 MHz, 935-960 MHz; 1710-1785 MHz, 1805-1880 MHz **UMTS** 1920-1980 MHz 2110-2170 MHz **LTE** 800 and 2600MHz	**AMPS**, **TDMA**, **CDMA** 824-849 MHz, 869-894 MHz; **TDMA**, **CDMA**, **GSM** 1850-1910 MHz, 1930-1990 MHz; **UMTS** 1850-1910 MHz 1930-1990 MHz	**PDC** 810-826 MHz, 940-956 MHz; 1429-1465 MHz, 1477-1513 MHz **UMTS** 1749.9-1784.9 1844.9-1879.9
Cordless telephones	**CT1+** 885-887 MHz, 930-932 MHz; **CT2** 864-868 MHz **DECT** 1880-1900 MHz	**PACS** 1850-1910 MHz, 1930-1990 MHz **PACS-UB** 1910-1930 MHz	**PHS** 1895-1918 MHz **JCT** 254-380 MHz
Wireless LANs	**IEEE 802.11** 2400-2483 MHz 5725–5875 MHz	**IEEE 802.11** 2400-2483 MHz 5725–5875 MHz	**IEEE 802.11** 2471-2497 MHz 5725–5875 MHz

Note: in the coming years, frequencies will become technology-neutral

Characteristics of Wireless LANs

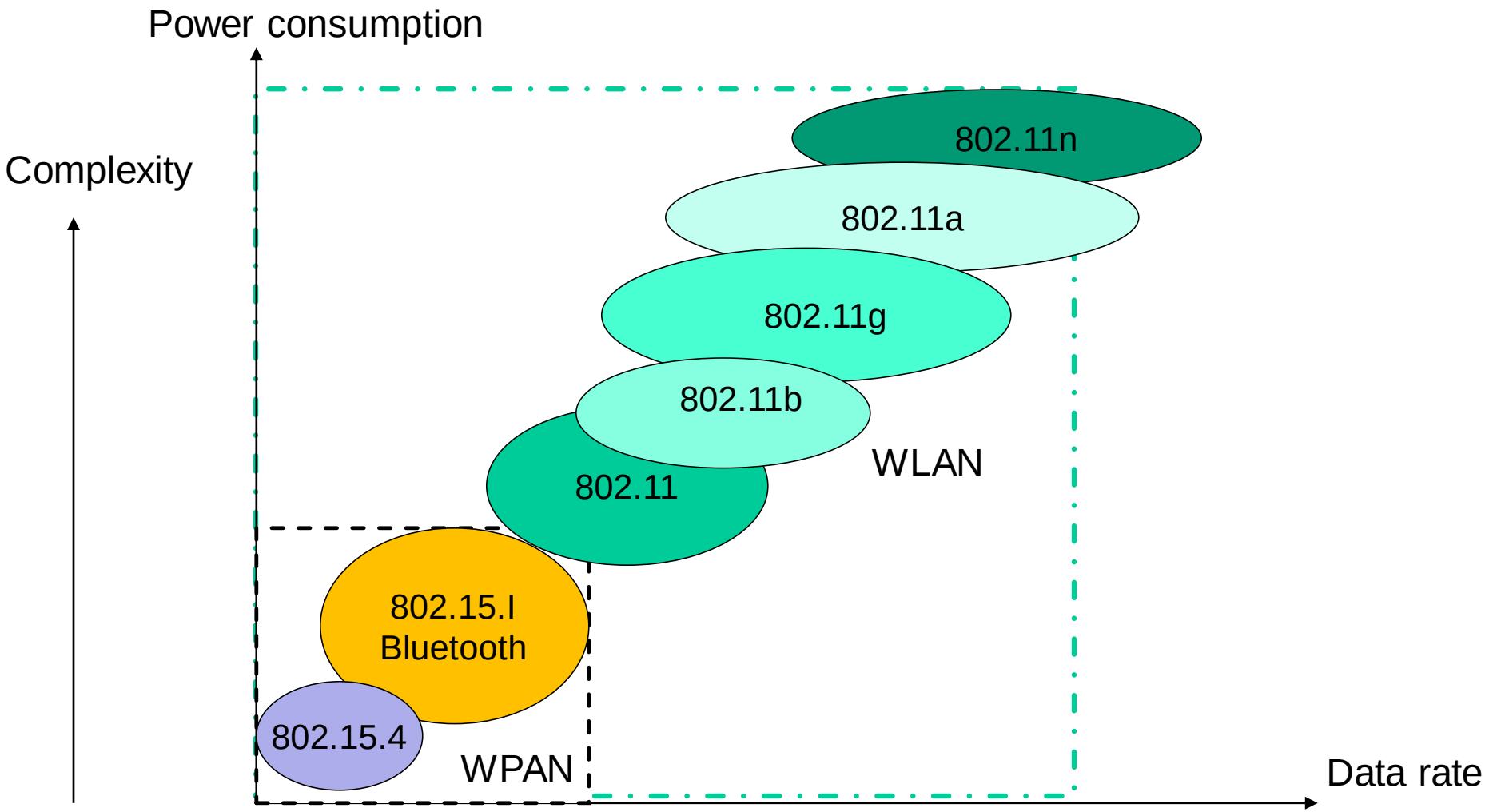
Advantages

- flexibility
- (almost) no wiring difficulties (e.g., historic buildings)
- more robust against disasters like, e.g., earthquakes, fire - or users pulling a plug...

Disadvantages

- lower bitrate compared to wired networks
- More difficult to secure

Scope of Various WLAN and WPAN Standards



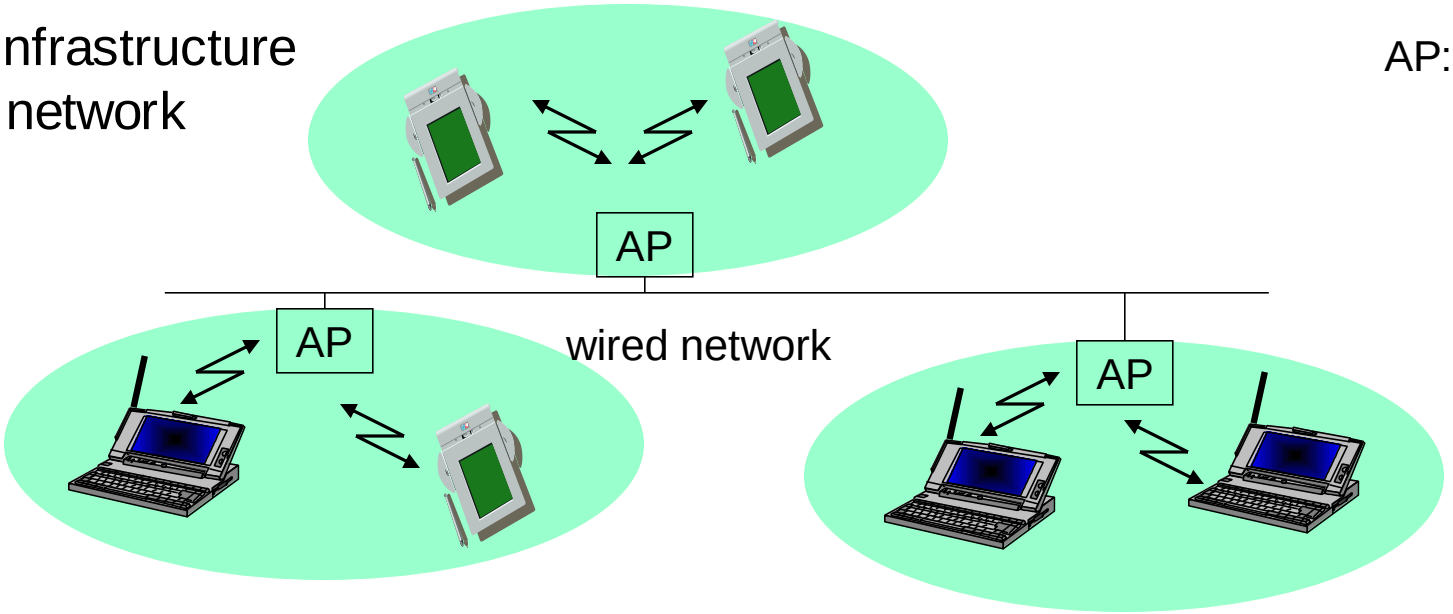
WPAN: Wireless Personal Area Network

Design goals for wireless LANs

- low power
- no special permissions or licenses needed to use the LAN
- robust transmission technology
- easy to use for everyone, simple management
- protection of investment in wired networks (internetworking)
- security, privacy, safety (low radiation)
- transparency concerning applications and higher layer protocols
- location awareness if necessary

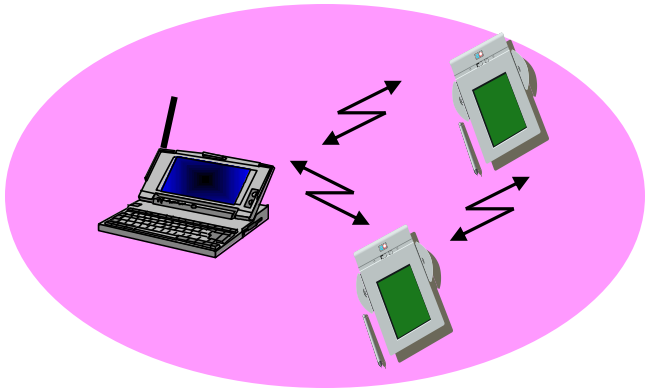
Infrastructure vs. ad hoc networks

infrastructure network

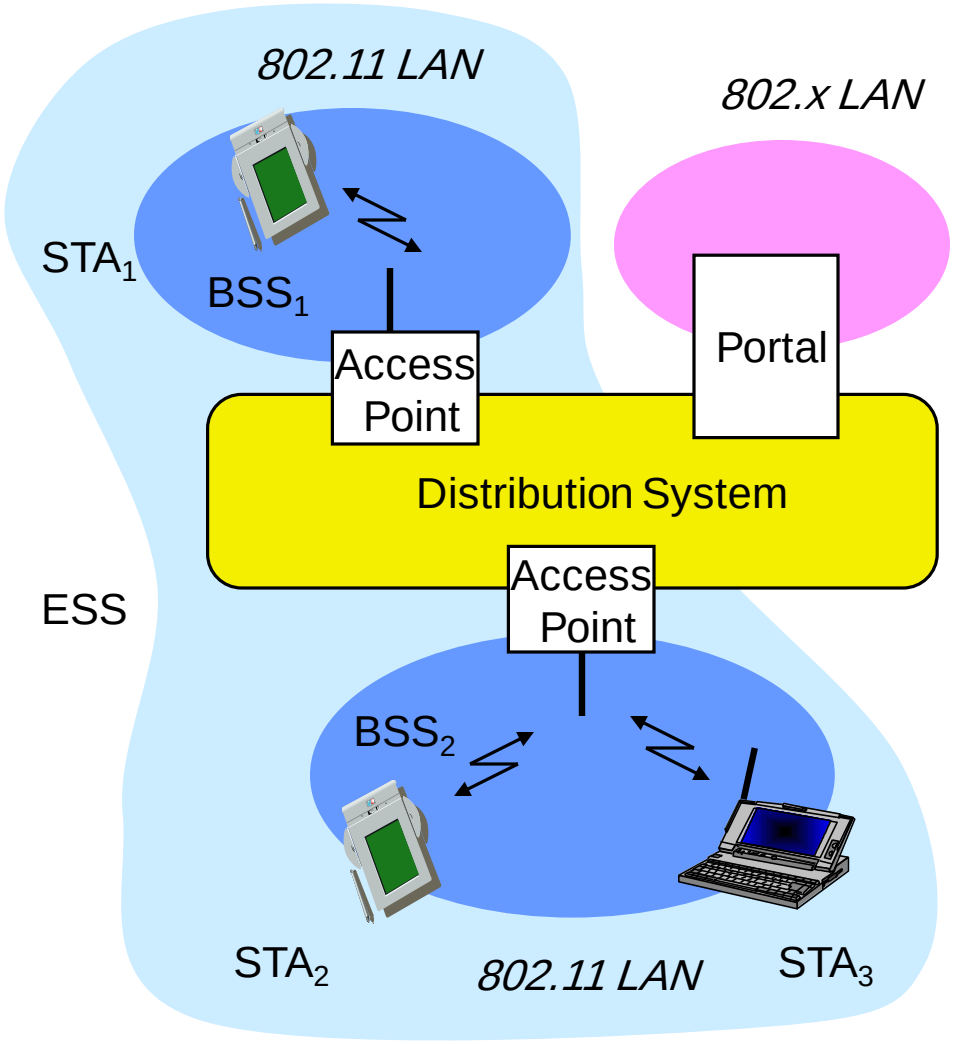


AP: Access Point

Ad hoc network



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

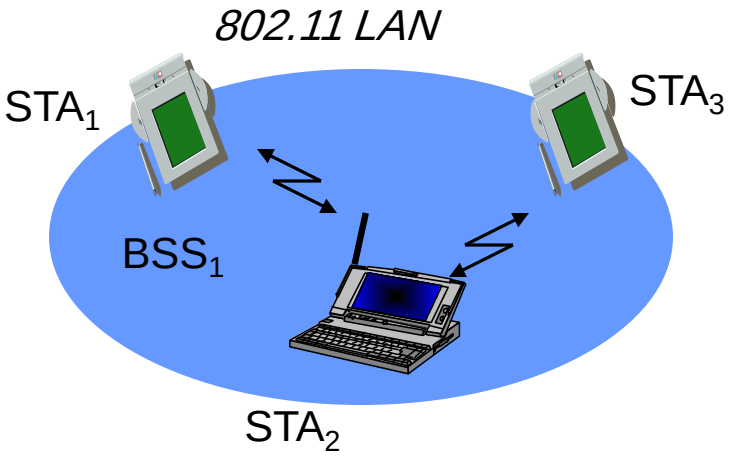
Portal

- bridge to other (wired) networks

Distribution System

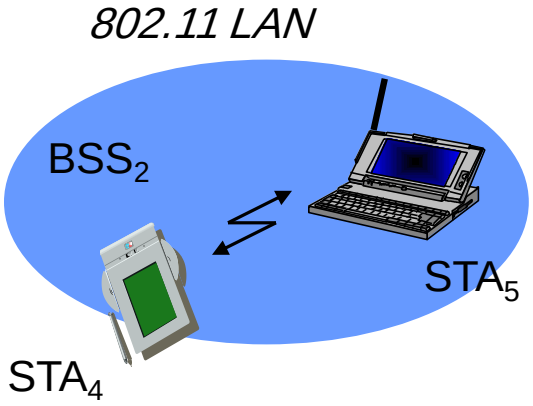
- interconnection network to form one logical network (ESS: Extended Service Set) based on several BSS

802.11 - Architecture of an ad-hoc network

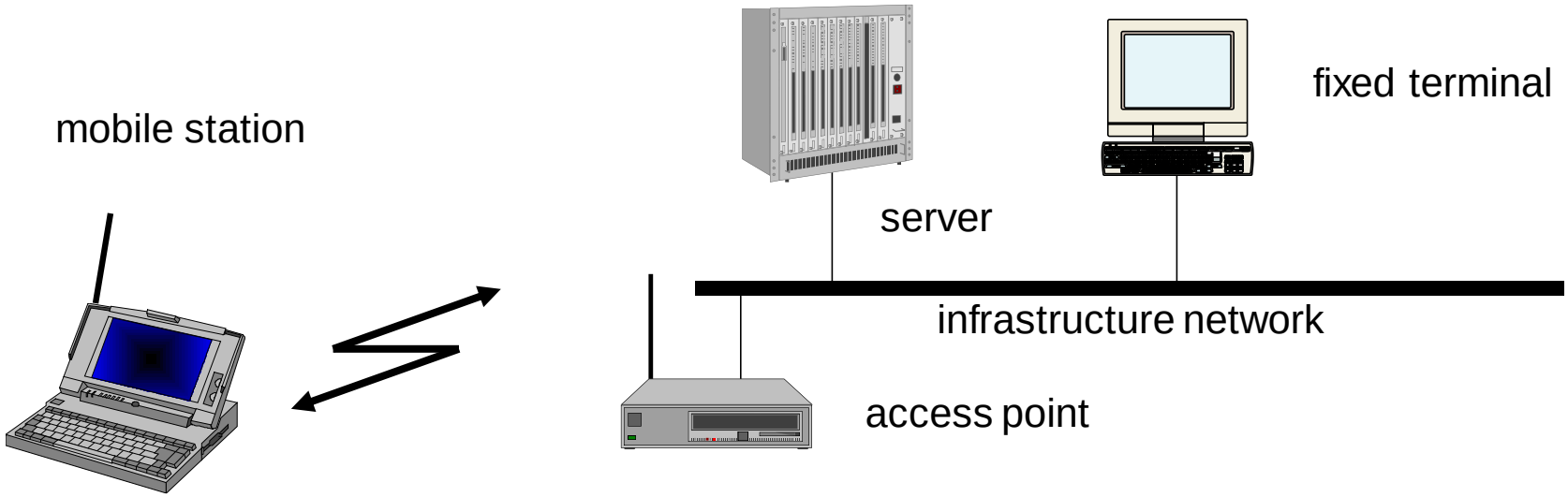


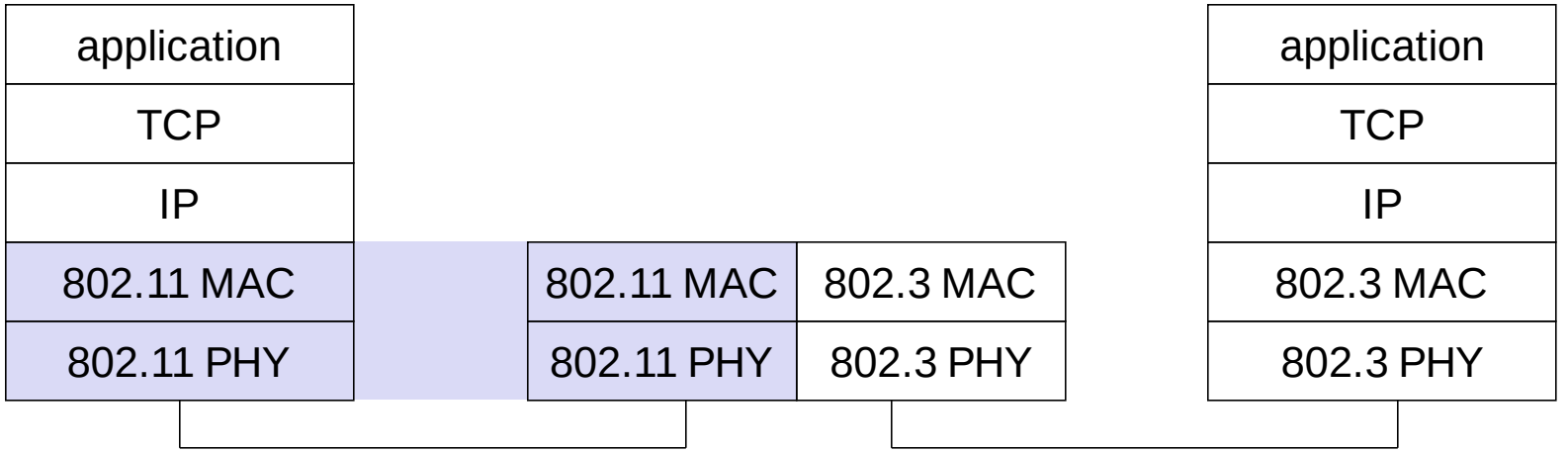
Direct communication within a limited range

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



Interconnection of IEEE 802.11 with Ethernet





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)

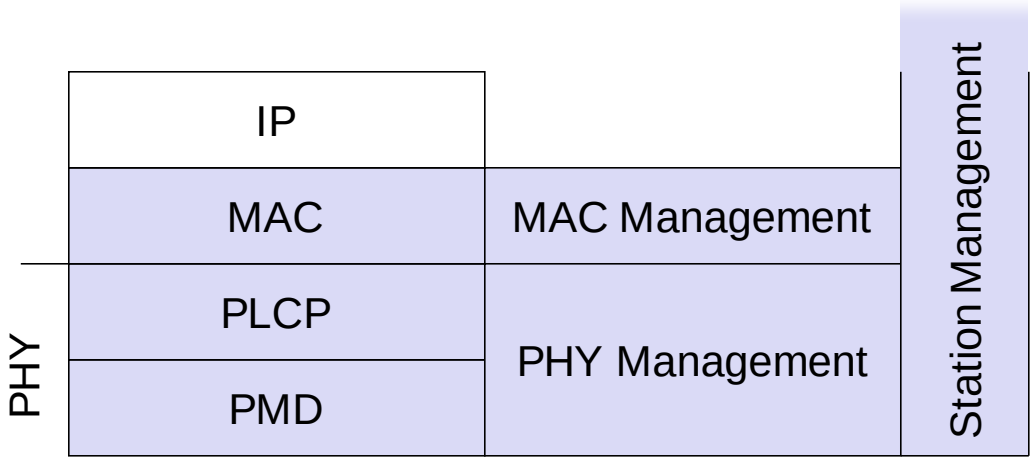
- modulation, coding

PHY Management

- channel selection, MIB

Station Management

- coordination of all management functions



802.11b - Physical layer

2 versions: DSSS and FHSS (both typically at 2.4 GHz)

- data rates 1, 2, 5 or 11 Mbit/s

DSSS (Direct Sequence Spread Spectrum)

- DBPSK modulation (Differential Binary Phase Shift Keying) or DQPSK (Differential Quadrature PSK)
- 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

FHSS (Frequency Hopping Spread Spectrum)

- spreading, despreading, signal strength
- min. 2.5 frequency hops/s, two-level GFSK modulation (Gaussian Frequency Shift Keying)

802.11 - MAC layer principles (1/2)

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 (called DFWMAC: Distributed Foundation Wireless MAC)

- DCF CSMA/CA (mandatory)
  - collision avoidance via randomized „back-off“ mechanism
  - minimum distance between consecutive packets
  - ACK packet for acknowledgements (not for broadcasts)
- DCF with RTS/CTS (optional)
  - avoids hidden terminal problem
- PCF (optional and rarely used in practice)
  - access point polls terminals according to a list

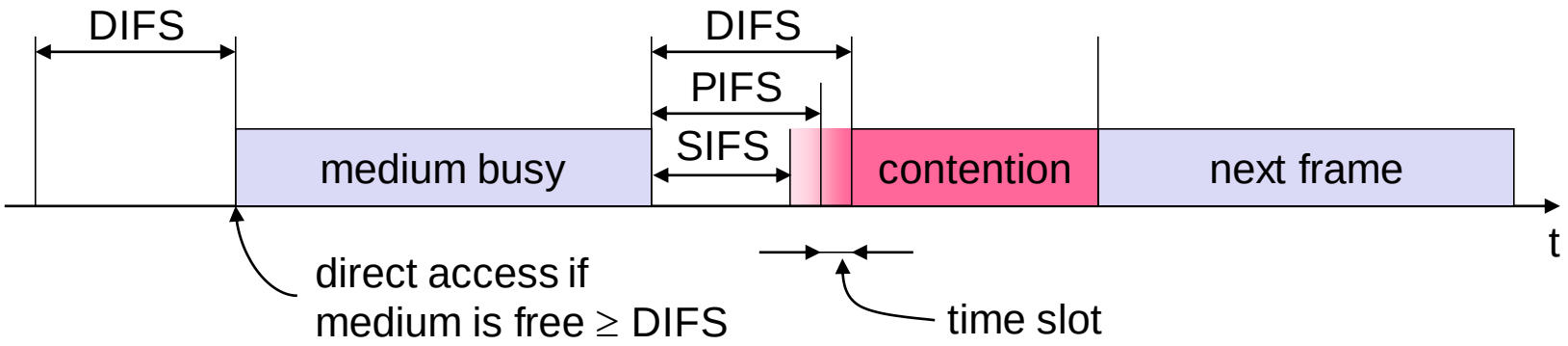
DCF: Distributed Coordination Function

PCF: Point Coordination Function

802.11 - MAC layer principles (2/2)

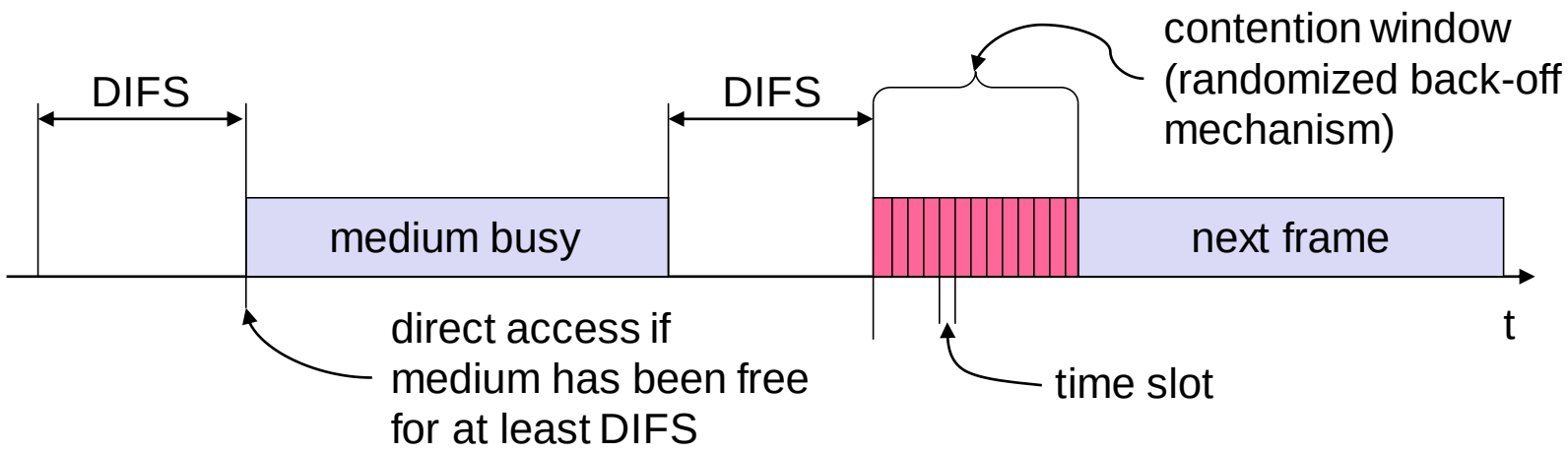
Priorities

- 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



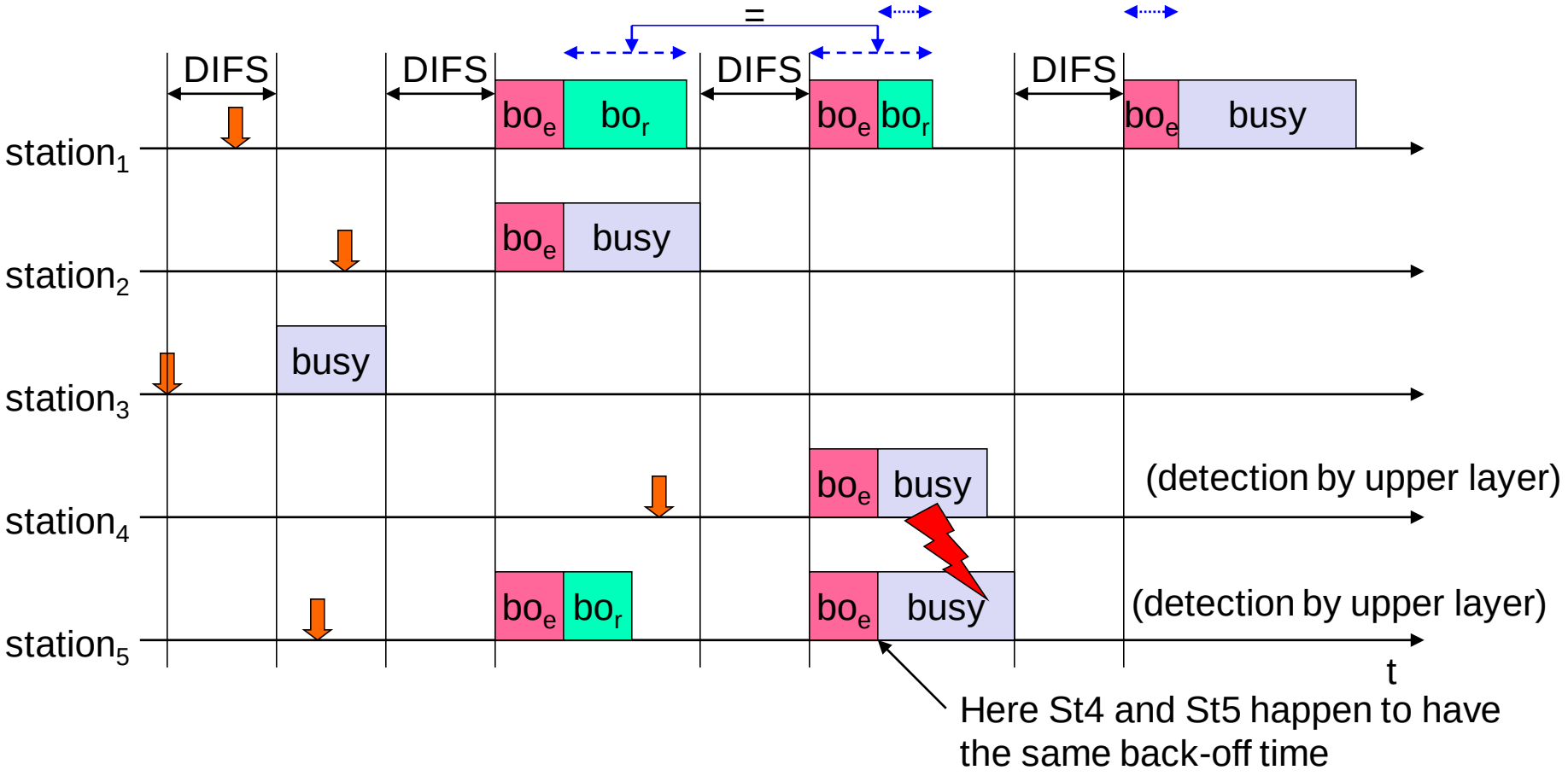
Note : IFS durations are specific to each PHY

802.11 - CSMA/CA principles



- 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 (to increase fairness)

802.11 – CSMA/CA broadcast



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

bo_e — elapsed backoff time

packet arrival at MAC

bo_r — residual backoff time

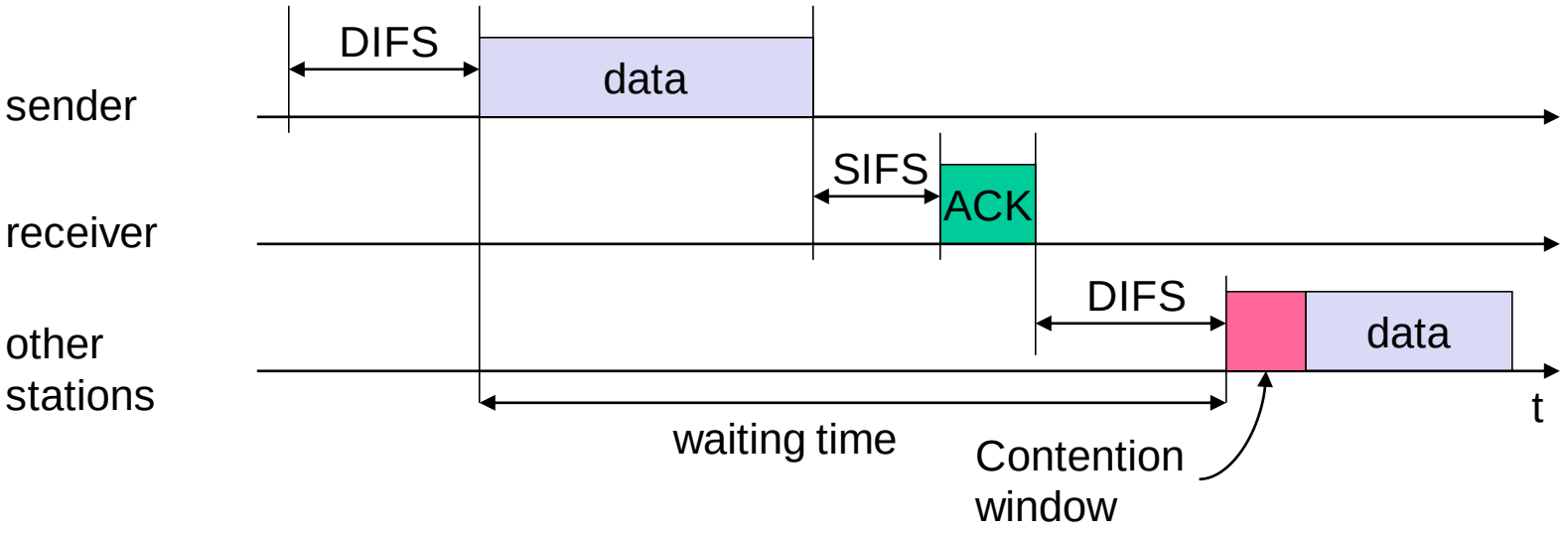
The size of the contention window can be adapted (if more collisions, then increase the size)

Note: broadcast is not acknowledged

802.11 - CSMA/CA unicast

Sending unicast packets

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



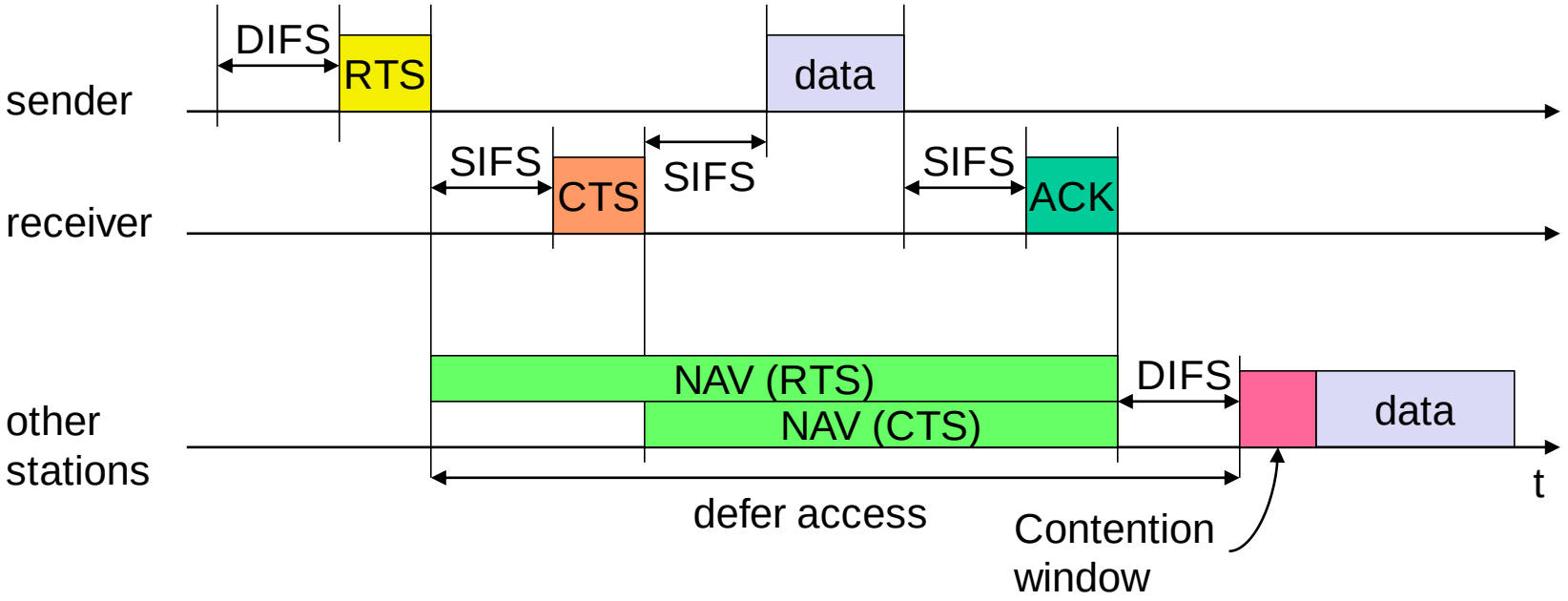
The ACK is sent right at the end of SIFS (no contention)

See file B1-802-11-Traces.pdf

802.11 – DCF with RTS/CTS

Sending unicast packets

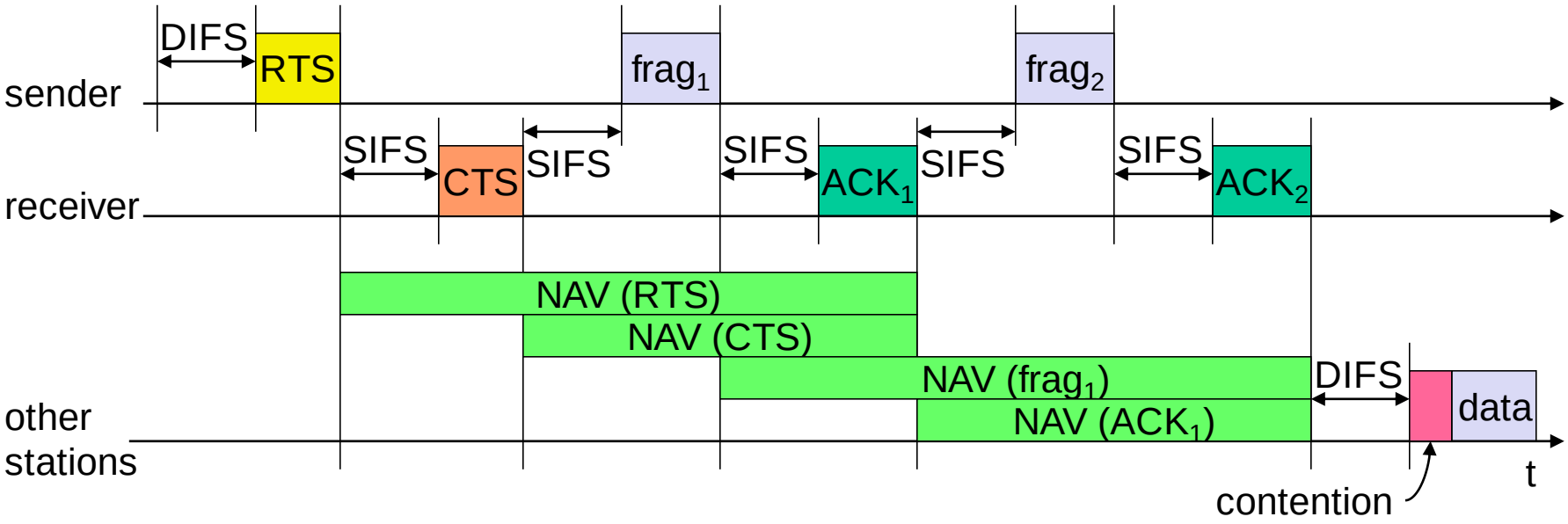
- station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium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



NAV: Net Allocation Vector

RTS/CTS can be present for some packets and not for other

Fragmentation mode



- Fragmentation is used in case the size of the packets sent has to be reduced (e.g., to diminish the probability of erroneous frames)
- Each $frag_i$ (except the last one) also contains a duration (as RTS does), which determines the duration of the NAV
- By this mechanism, fragments are sent in a row
- In this example, there are only 2 fragments

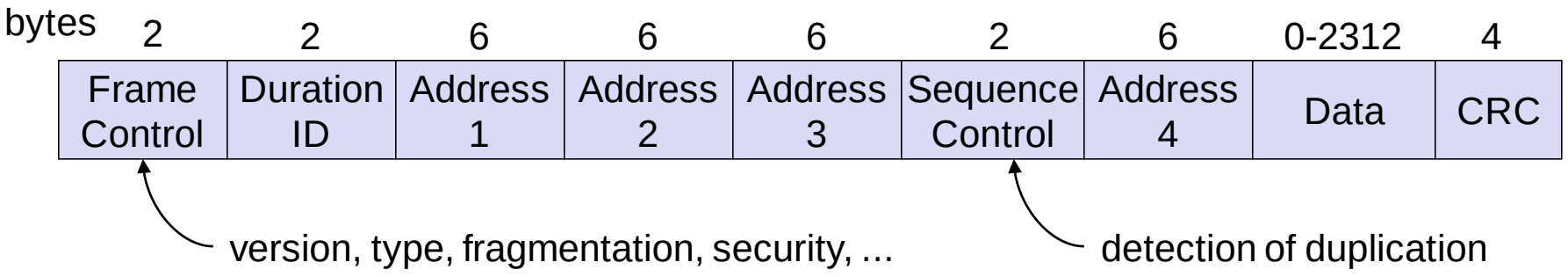
802.11 - MAC frame format

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



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
- infrastructure BSS : MAC address of the Access Point
- ad hoc BSS (IBSS): random number

RA: Receiver Address
TA: Transmitter Address

802.11 - MAC management

Synchronization

- Purpose
  - for the physical layer (e.g., maintaining in sync the frequency hop sequence in the case of FHSS)
  - for power management
- Principle: beacons with time stamps

Power management

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

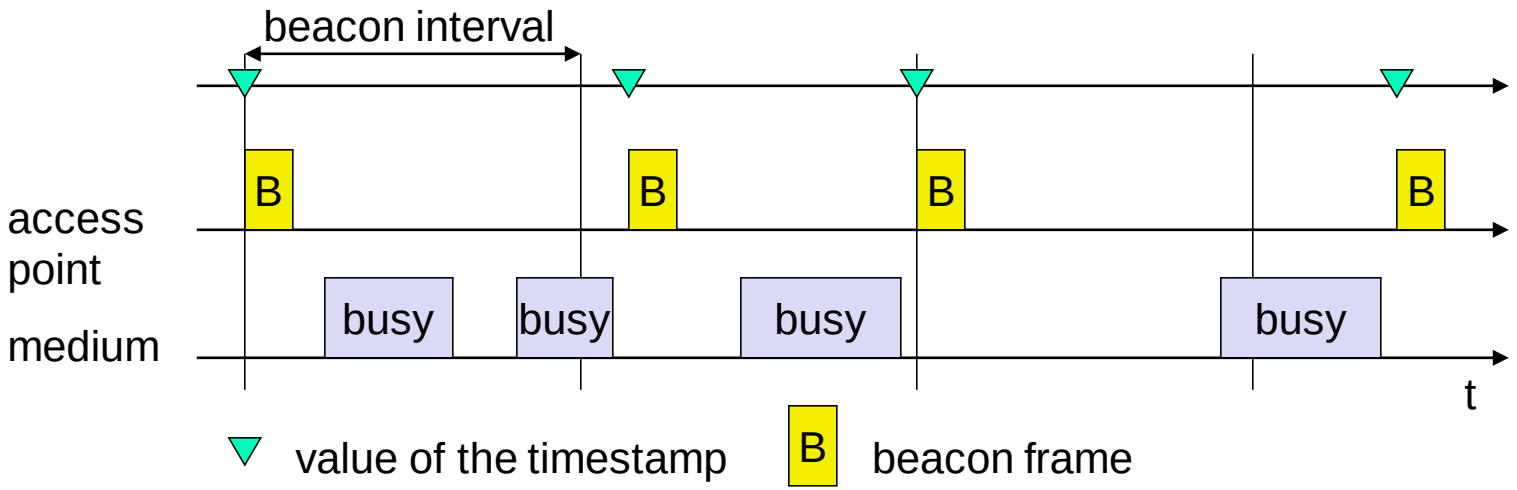
Association/Reassociation

- 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

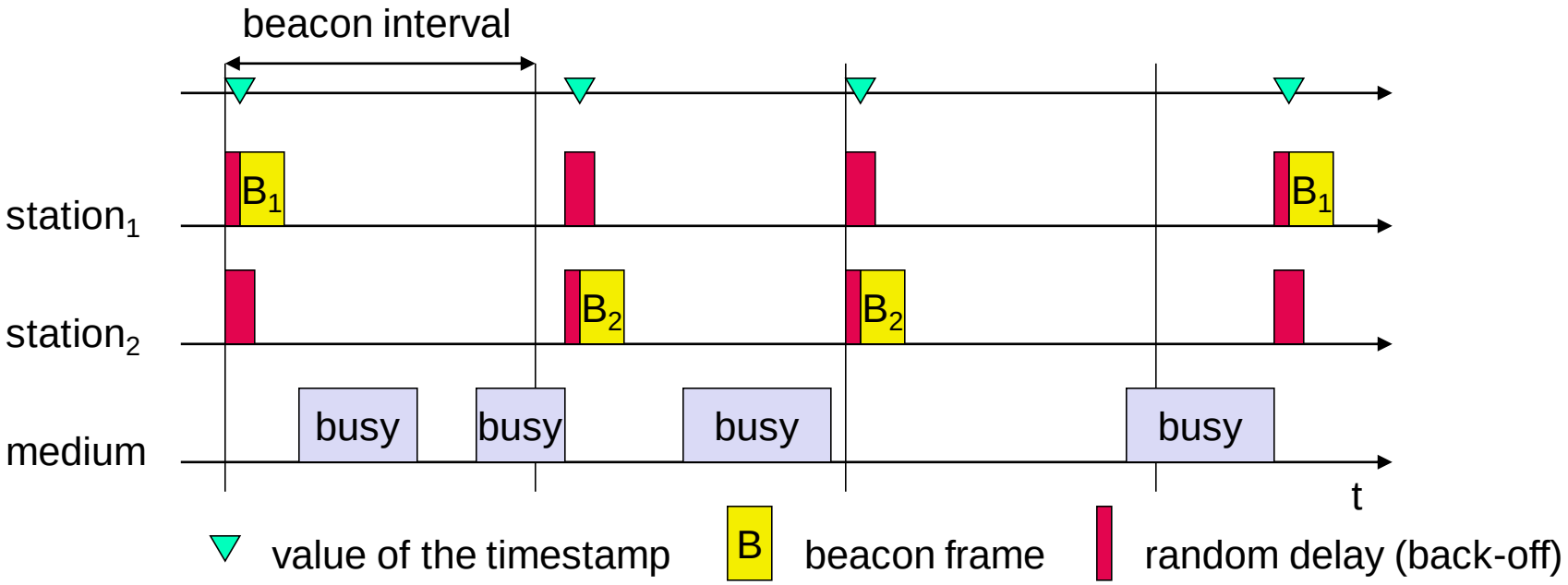
- managing, read, write

Synchronization (infrastructure case)



- The access point transmits the (quasi) periodic beacon signal
- The beacon contains a timestamp and other management information used for power management and roaming
- All other wireless nodes adjust their local timers to the timestamp

Synchronization (ad-hoc case)



- Each node maintains its own synchronization timer and starts the transmission of a beacon frame after the beacon interval
- Contention ➔ back-off mechanism ➔ only 1 beacon wins
- All other stations adjust their internal clock according to the received beacon and suppress their beacon for the current cycle

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

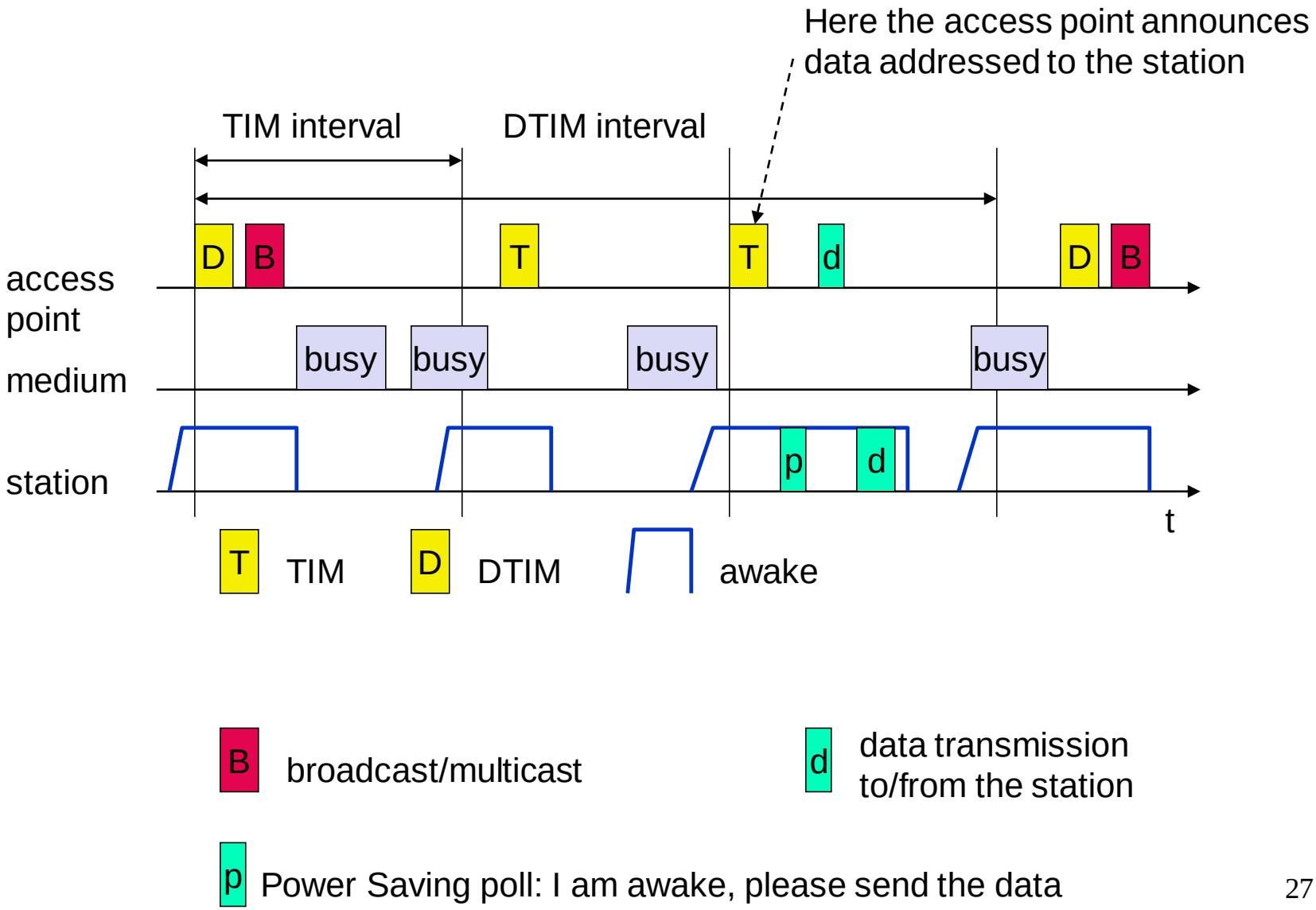
Infrastructure case

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

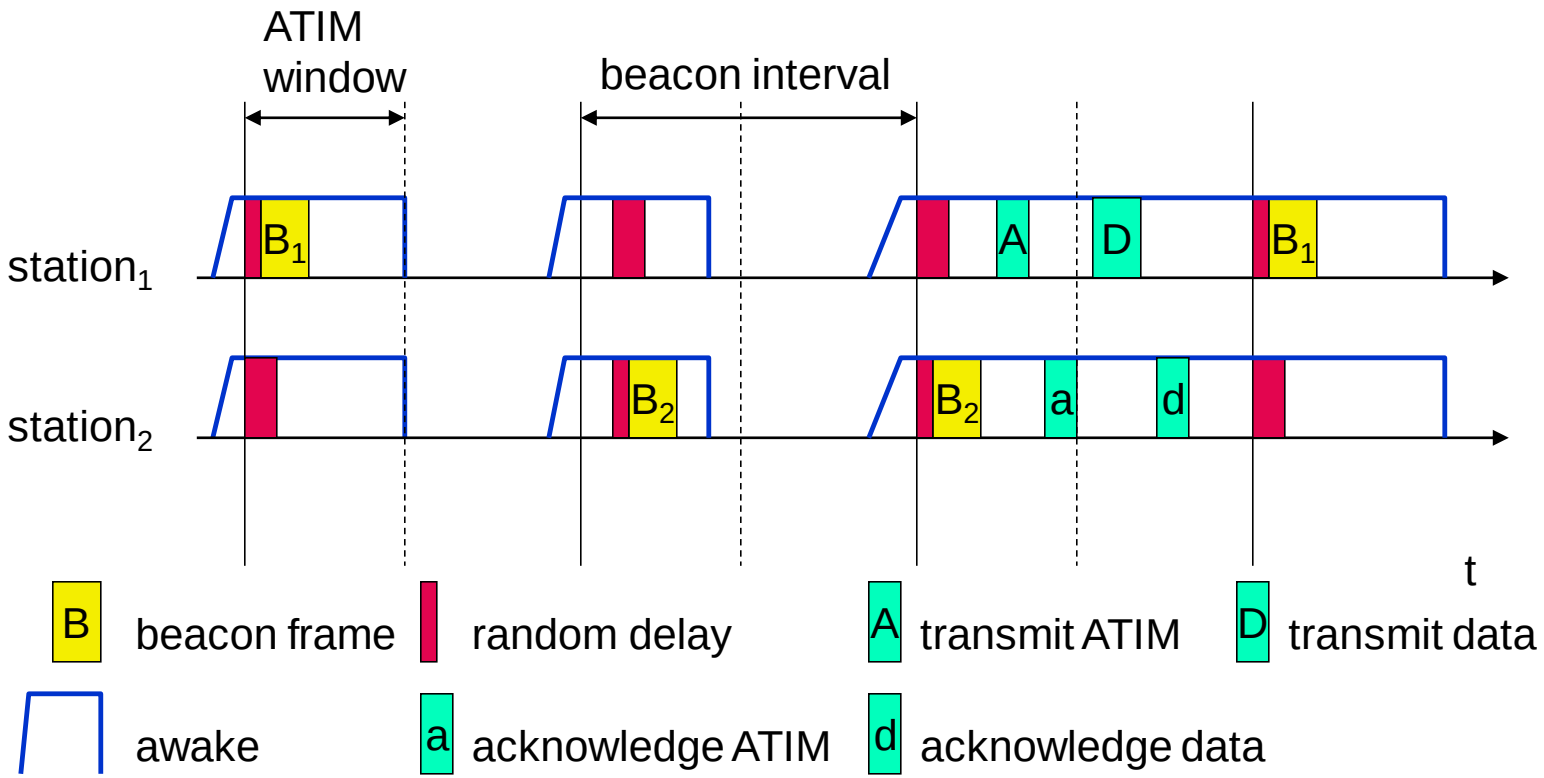
Ad-hoc case

- 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 (infrastructure case)



Power saving (ad-hoc case)



- ATIM: Ad hoc Traffic Indication Map (a station announces the list of buffered frames)
- Potential problem: scalability (high number of collisions)

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