WIRELESS LAN

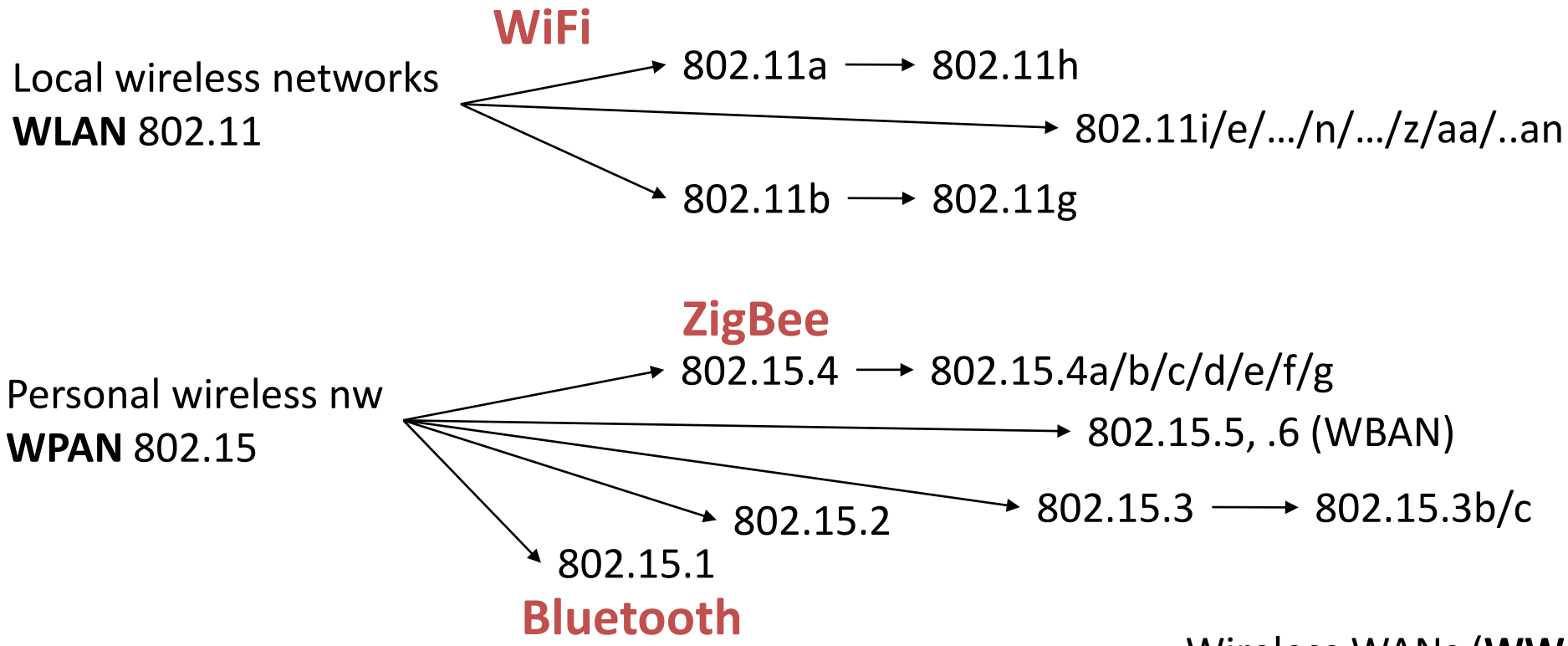
Dr. A. Beulah

AP/CSE

LEARNING OBJECTIVES

- To understand the about wireless LAN protocols.

MOBILE COMMUNICATION TECHNOLOGY ACCORDING TO IEEE (EXAMPLES)



Wireless WANs (**WWAN**)

Cellular Networks: GSM(2G), GPRS(2.5G), UMTS(3G), LTE (4G)

Satellite Networks: Iridium, Globalstar

CHARACTERISTICS OF WIRELESS LANS

- Advantages
  - Very flexible within the reception area (Radio wave can penetrate walls, sender and receiver can be placed anywhere)
  - Ad-hoc networks without previous planning possible
  - (almost) no wiring difficulties (e.g. historic buildings). Current networking technology can be introduced without being visible.
  - Wireless networks can survive disasters like, e.g., earthquakes, fire or users pulling a plug.
  - Cost effective: No network sockets. Adding additional users does not require any infrastructure change.

CHARACTERISTICS OF WIRELESS LANS

- Disadvantages
  - Typically very low bandwidth compared to wired networks (1-10 Mbit/s) due to shared medium
    - IEEE 802.11ac theoretical speed 1.7Gbps ; real-time speed 1Gbps
    - But, Ethernet theoretical speed 100Gbps
  - 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
  - Using radio waves might interference with other high tech equipment ex: hospitals.
  - The open radio interference makes eavesdropping much easier in WLANs than in wired network.

DESIGN GOALS FOR WIRELESS LANS

- Global, seamless operation
- Low power for battery use
- 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
- 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

TYPES OF TRANSMISSION

- Infra Red
- Radio wave

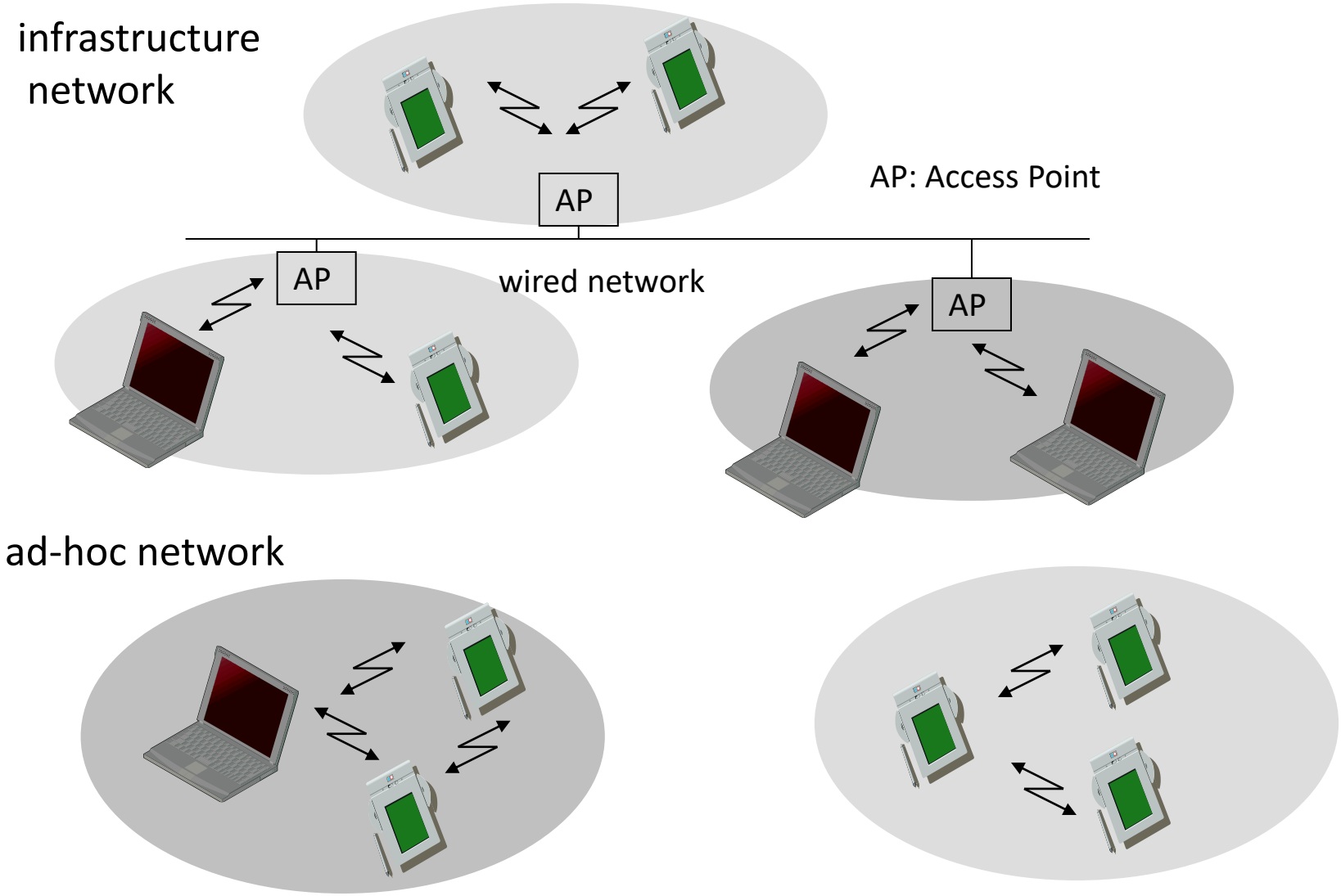
INFRA RED

- Infra Red transmits between 700 nm – 1 mm wavelength
- Diffuse light reflected at walls, furniture etc. or directed light if line of sight(LOS) exists.
- Sender → Laser diodes, Receiver → Photodiodes
- Advantages
  - Simple, cheap
  - No licenses needed
- Disadvantages
  - Interference by sunlight, heat sources etc.
  - Many things shield or absorb IR light
  - Low bandwidth
- Example
  - available in many mobile devices (IR Blaster)

RADIO WAVE

- Typically using the license free ISM band at 2.4 GHz or 5.7GHz
- Advantages
  - Experience from wireless WAN and mobile phones can be used
  - Coverage of larger areas
- Disadvantages
  - Very limited license free frequency bands
  - Interference with other electrical devices
- Example
  - Laptops, Mobile phones

COMPARISON: INFRASTRUCTURE VS. AD-HOC NETWORKS



INFRASTRUCTURE NETWORKS

- The access point does medium access, and also acts as a bridge to other wireless or wired networks.
- Many Network functionalities are done within the access point, but the wireless clients does only data transmission.
- Collisions may occur if medium access of the wireless nodes and the access point is not coordinated.
- Cannot be used for disaster relief in cases where no infrastructure is left

AD-HOC NETWORKS

- Nodes within an ad-hoc network can only communicate if they can reach each other physically, i.e., if they are within each other's radio range or if other nodes can forward the message.
  - Quick replacements of infrastructure or communication scenarios far away from any infrastructure

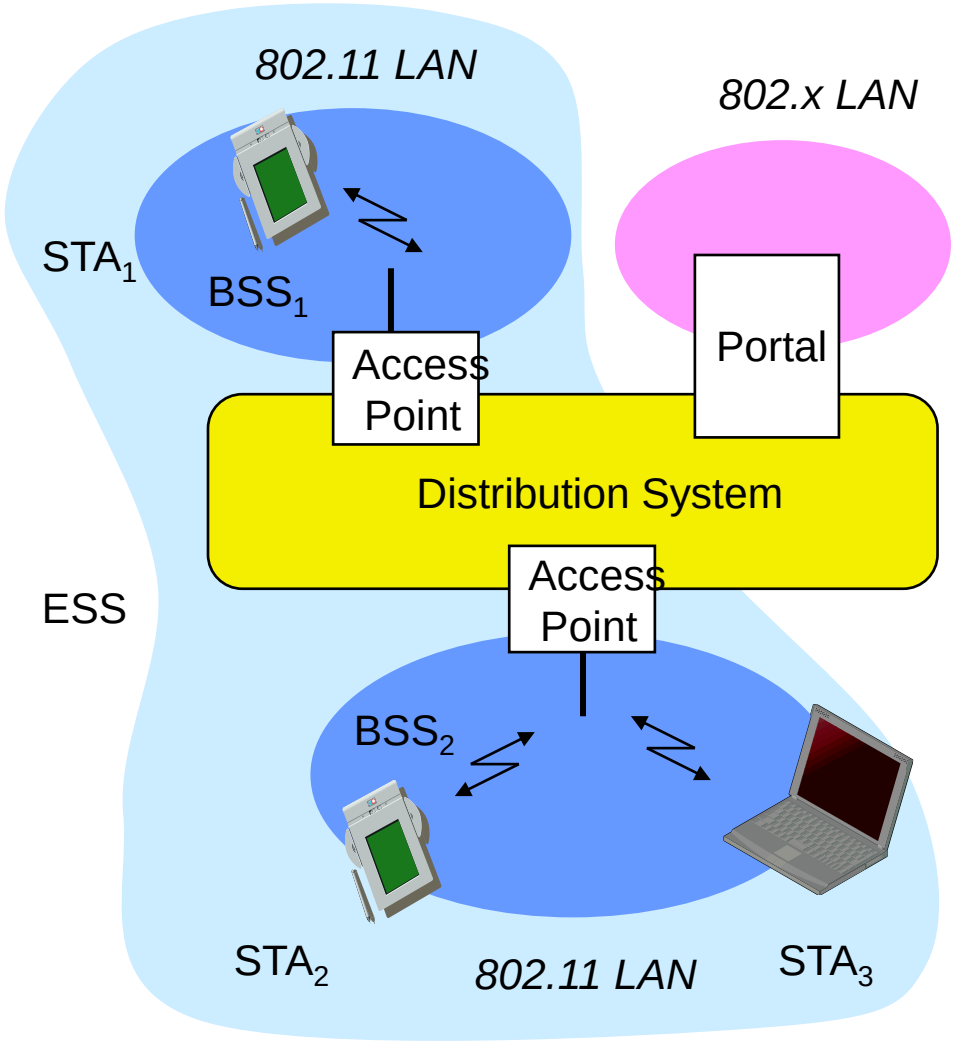
IEEE 802.11

STANDARDS

- LAN standards → 802.x
- 802.11 → Wireless LAN
- The MAC layer should be able to operate with multiple physical layers, each of which exhibits a different medium sense and transmission characteristic.

IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ax
Year Released	1999	1999	2003	2009	2014	2019
Frequency	5Ghz	2.4GHz	2.4GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz	2.4Ghz & 5GHz
Maximum Data Rate	54Mbps	11Mbps	54Mbps	600Mbps	1.3Gbps	10-12Gbps

802.11 - ARCHITECTURE OF AN INFRASTRUCTURE NETWORK

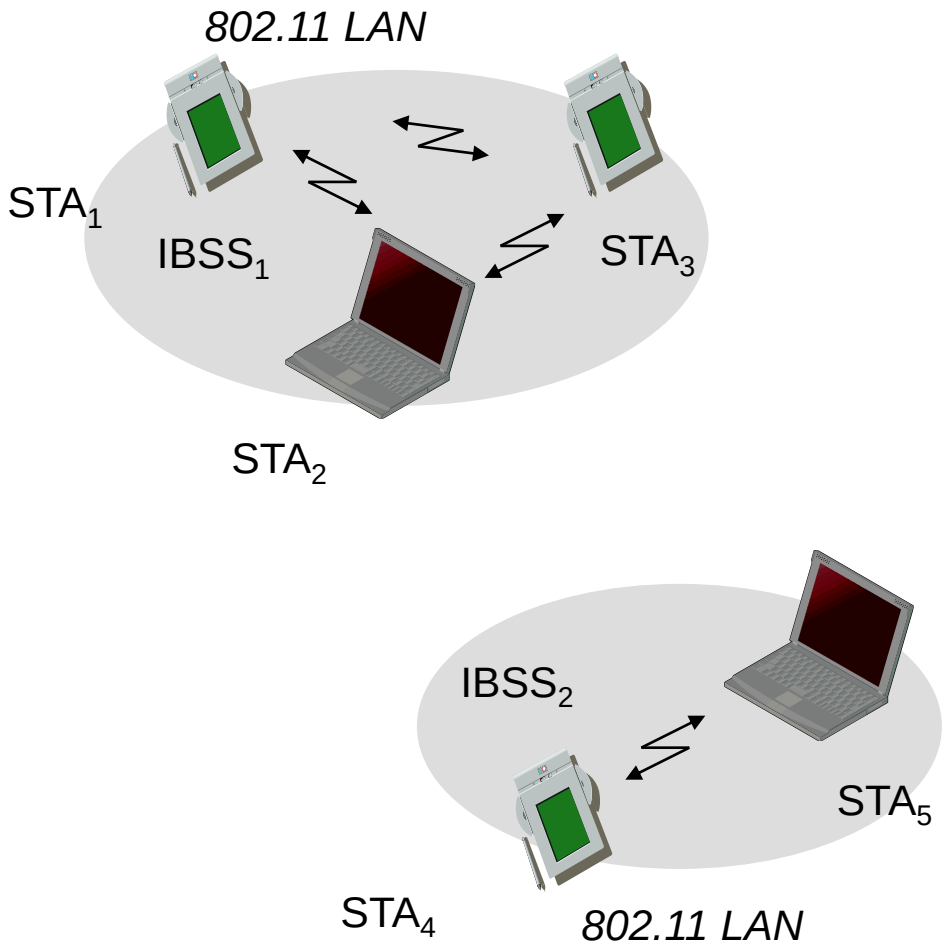


- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

WORKING PRINCIPLE

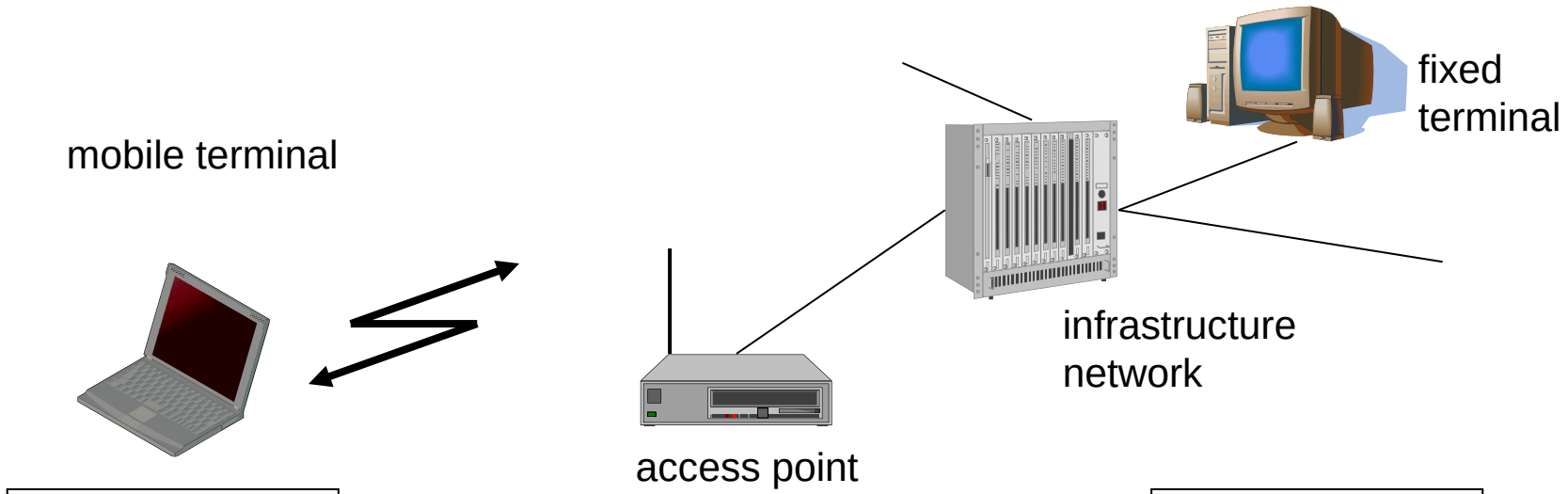
- Stations select an AP and communicate through it.
- The APs support
  - roaming
  - synchronization within a BSS
  - power management
  - media access.
- The distribution system handles data transfer between the different APs.

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

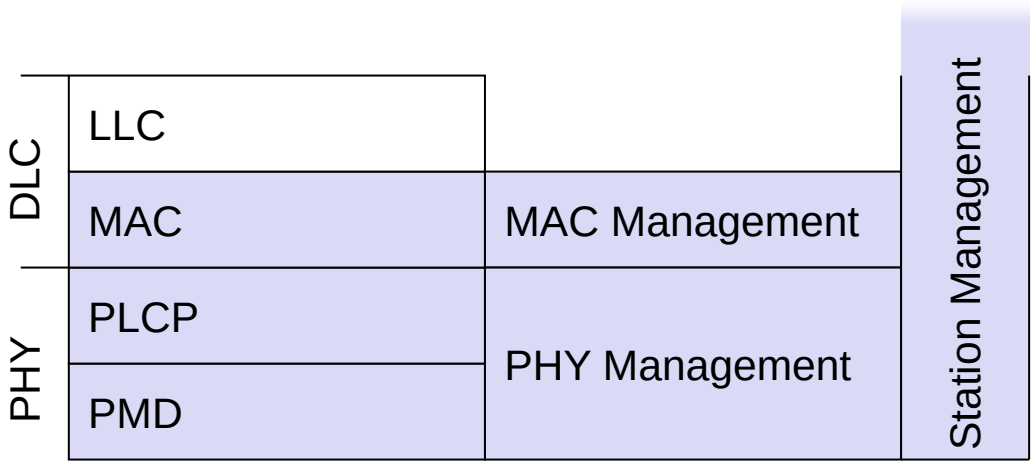
IEEE STANDARD 802.11



application		
TCP		
IP		
LLC	LLC	
802.11 MAC	802.11 MAC	802.3 MAC
802.11 PHY	802.11 PHY	802.3 PHY

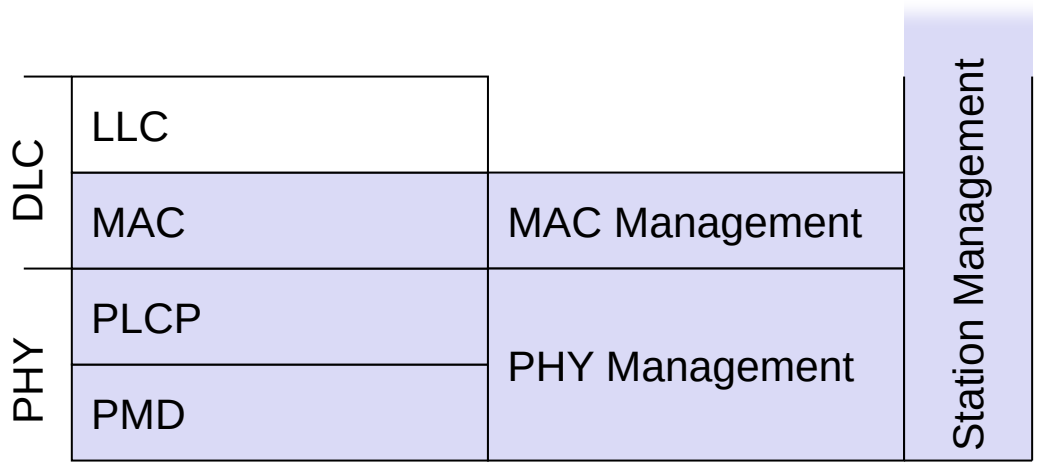
802.11 - LAYERS AND FUNCTIONS

- The IEEE 802.11 standard only covers the physical layer **PHY and medium** access layer **MAC like the other 802.x LANs do.**
- **The physical layer is subdivided** into the **Physical layer convergence protocol (PLCP) and the Physical medium dependent sublayer PMD.**
- The basic tasks of the MAC layer comprise medium access, fragmentation of user data, and encryption.



802.11 - LAYERS AND FUNCTIONS

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, Management Information Base (MIB), power management
- PLCP Physical Layer Convergence Protocol
  - clear channel assessment (CCA) signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding
- PHY Management
  - channel selection, MIB
- Station Management
  - coordination of all management functions



802.11 - PHYSICAL LAYER

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
- All PHY variants include the provision of the **Clear Channel Assessment signal (CCA).**
- This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle.
- The transmission technology determines exactly how this signal is obtained.
- The PHY layer offers a Service Access Point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer (basic version of the standard).

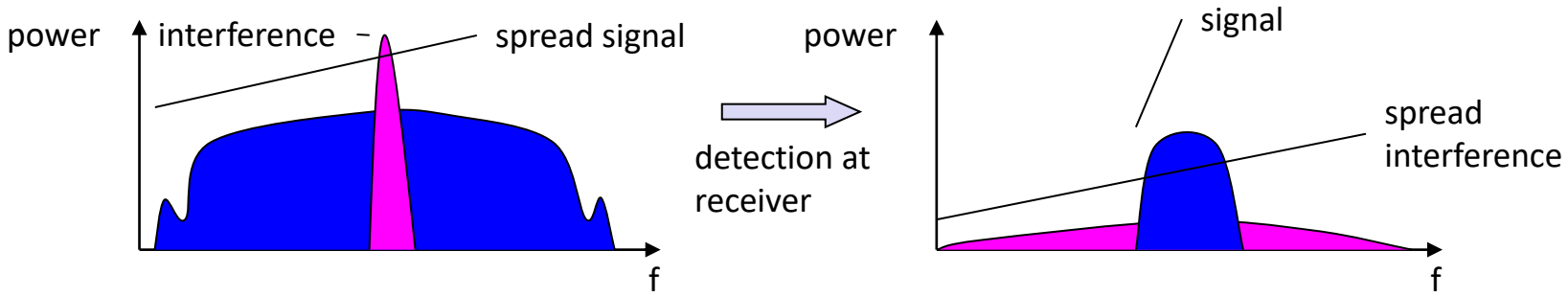
802.11 - PHYSICAL LAYER

- 3 versions: 2 radio (typ. 2.4 GHz), 1 IR
- FHSS (Frequency Hopping Spread Spectrum)
- DSSS (Direct Sequence Spread Spectrum)
- Infrared

802.11 - PHYSICAL LAYER

Spread spectrum technology

- Problem of radio transmission: frequency dependent fading can wipe out narrow band signals for duration of the interference
- Solution: spread the narrow band signal into a broad band signal using a special code
  - protection against narrow band interference

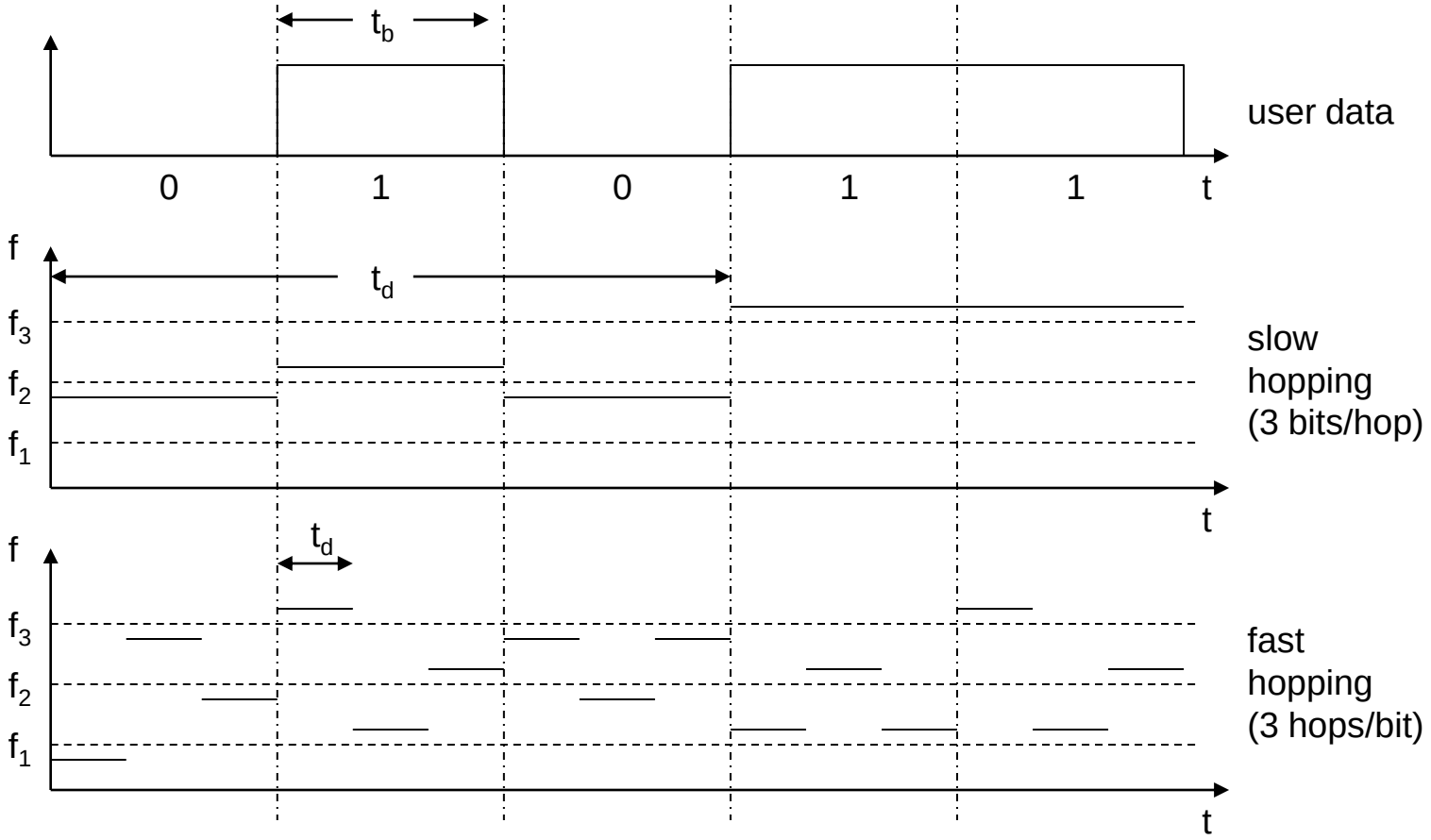


- Side effects:
  - coexistence of several signals without dynamic coordination
  - tap-proof
- Alternatives: Direct Sequence, Frequency Hopping

802.11 - PHYSICAL LAYER

- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typ. 1 Mbit/s
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- Two versions
  - Fast Hopping:
    several frequencies per user bit
  - Slow Hopping:
    several user bits per frequency

802.11 - PHYSICAL LAYER

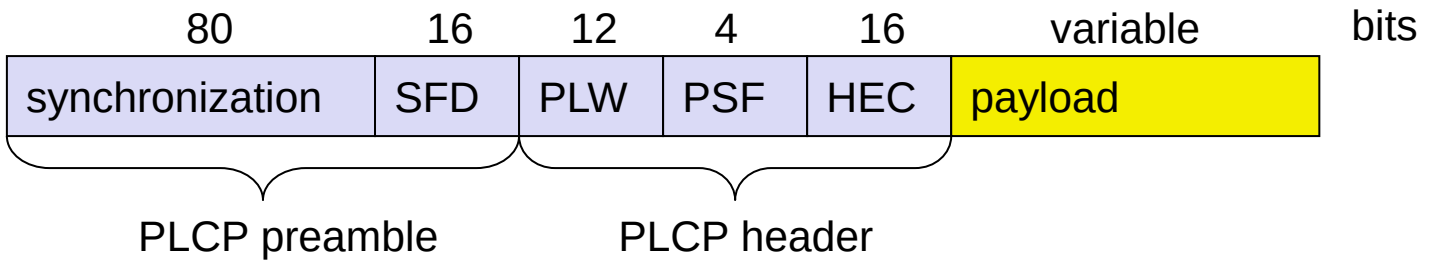


t_b: bit period t_d: dwell time

802.11 - PHYSICAL LAYER

FHSS PHY packet format

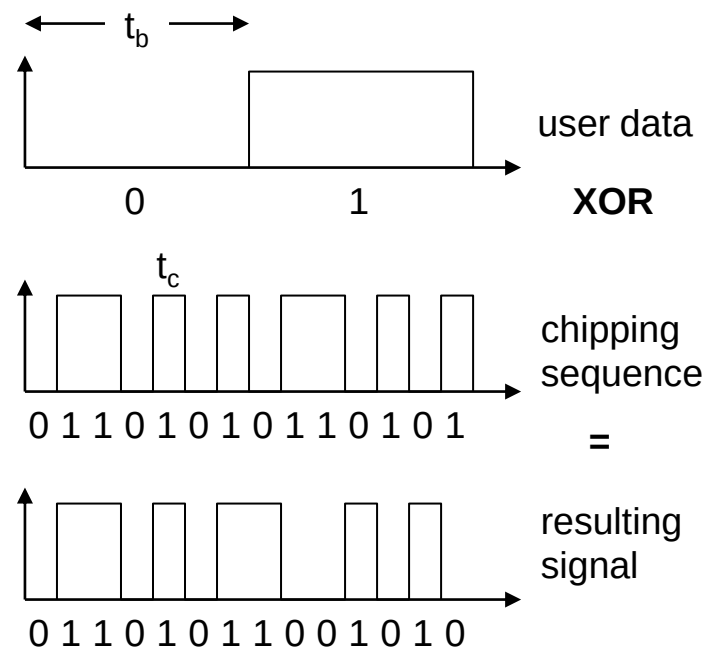
- Synchronization
  - synch with 010101... pattern
- SFD (Start Frame Delimiter)
  - 0000110010111101 start pattern
- PLW (PLCP_PDU Length Word)
  - length of payload incl. 32 bit CRC of payload, PLW < 4096
- PSF (PLCP Signaling Field)
  - data of payload (1 or 2 Mbit/s)
- HEC (Header Error Check)
  - CRC with $x^{16}+x^{12}+x^5+1$



802.11 - PHYSICAL LAYER

- 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

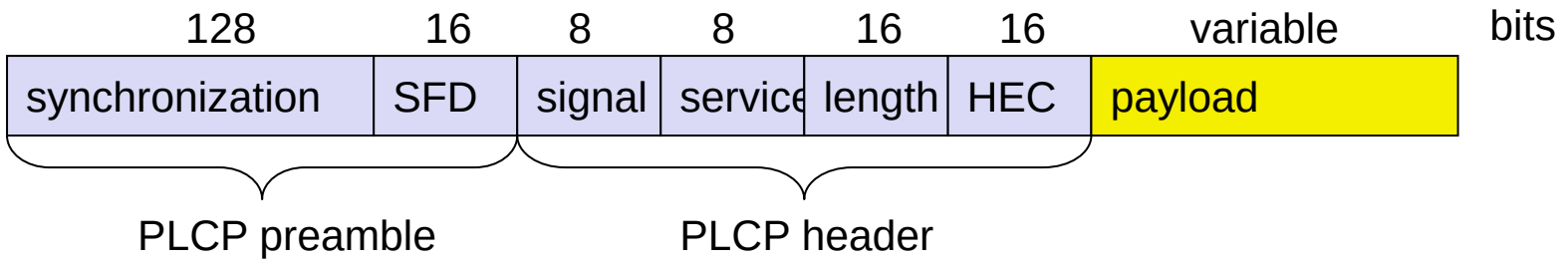


t_b: bit period
t_c: chip period

802.11 - PHYSICAL LAYER

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



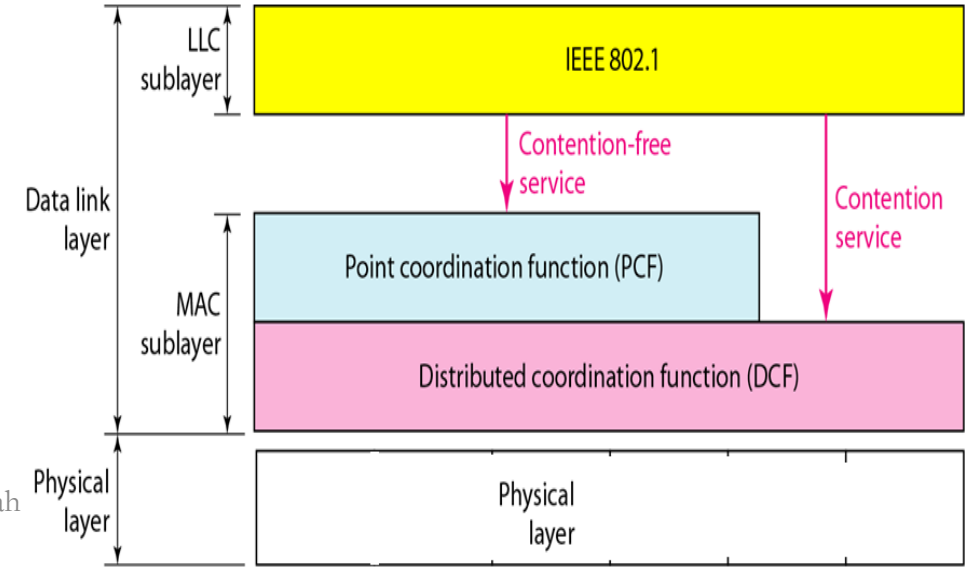
802.11 - PHYSICAL LAYER

Infrared

- The PHY layer, which is based on infra red (IR) transmission, uses near visible light at 850–950 nm.
- The maximum range is about 10 m if no sunlight or heat sources interfere with the transmission.
- Typically, such a network will only work in buildings, e.g., classrooms, meeting rooms etc.
- Frequency reuse is very simple – a wall is more than enough to shield one IR based IEEE 802.11 network from another.

802.11 - MAC LAYER

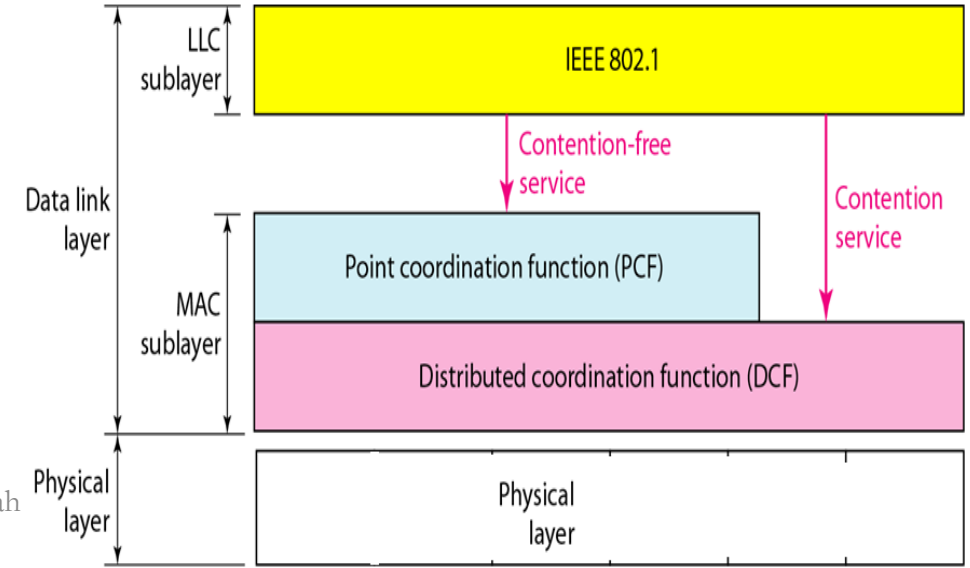
- 3 basic access mechanisms for IEEE 802.11:
  1. The mandatory basic method based on a version of CSMA/CA
  2. An optional method avoiding the hidden terminal problem
  3. A contention- free polling method for time-bounded service.
- The first two methods are also summarized as **distributed coordination function (DCF), the third** method is called **point coordination function (PCF).**



802.11 - MAC LAYER

- **DCF** only offers asynchronous service, while **PCF** offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid contention.
- The MAC mechanisms are also called **distributed foundation wireless medium access control (DFWMAC).**
- For all access methods, there are several parameters for controlling the waiting time before

  medium access are important.



802.11 - MAC LAYER

- 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

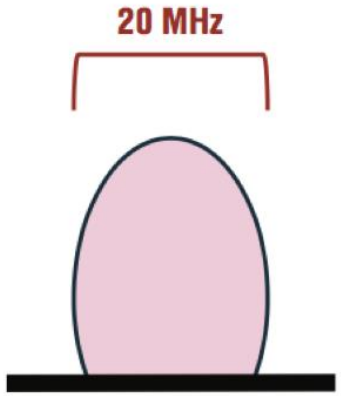
802.11 - MAC LAYER

DCF and CSMA/CA

- Wi-Fi standards (IEEE 802.11) use DCF technique that employs CSMA/CA networking
- Role of DCF and CSMA/CA
  - Used to avoid communication failure due to packet collision
  - Required because the unlicensed ISM band is used
- Carrier Sense
  - To avoid communication failure (due to packets colliding), each node listens to the shared medium (ie 2.4 and 5GHz wireless channel) to detect whether another node is communicating or not.

802.11 - MAC LAYER

- Carrier sense is done base on CCA, Clear Channel Assessment



Signal Detect (SD) threshold is statistically a 4 dB signal-to-noise ratio (SNR) to detect 802.11 preamble

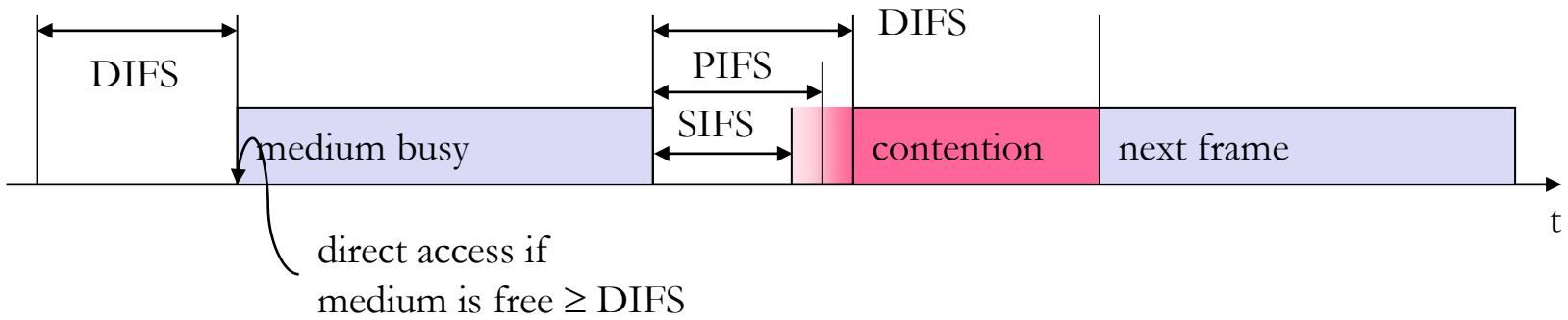
Energy Detect (ED) threshold is 20 dB above the signal detect threshold

CCA:
SD = 4 dB SNR
ED = SD + 20 dB

802.11 - MAC LAYER

- Collision Avoidance
  - If another node's communication is detected, other nodes will not transmit for a specific period of time (NAV period)
- NAV (Network Allocation Vector)
  - Period of time to wait for another node to complete packet communications.
- IFS (Inter Frame Spacing) Priority
  - Control priority using inter-frame space duration

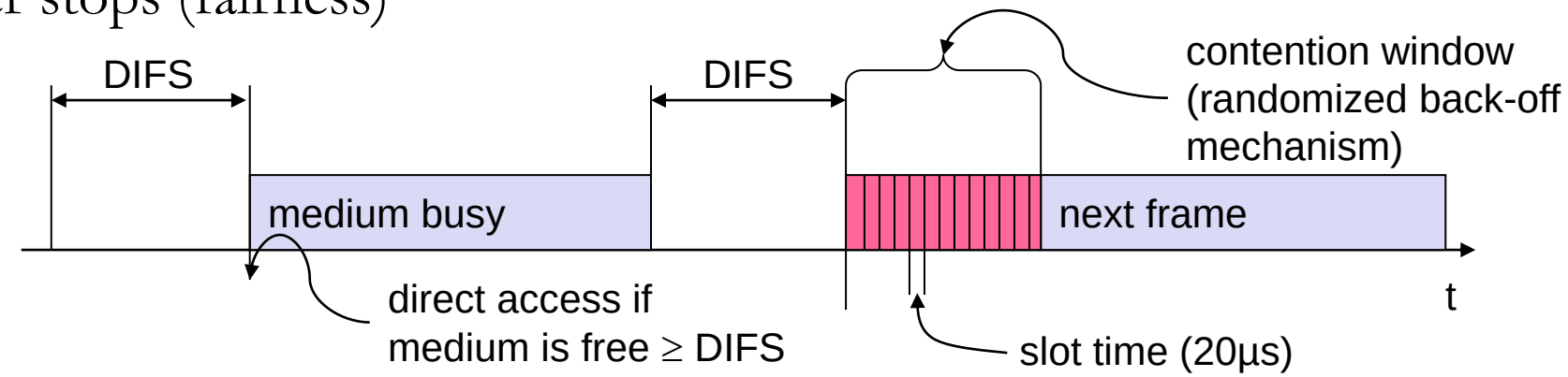
802.11 - MAC LAYER



- SIFS (Short Inter Frame Spacing)
  - Short Waiting Time
  - Highest priority, for ACK, CTS, polling response
  - DSSS →10 µs FHSS →28 µs
- PIFS (Point Coordination Function IFS)
  - Waiting Time between DIFS and SIFS
  - Medium priority, for time-bounded service using PCF
  - PIFS = SIFS +Slot Time
- DIFS (DCF, Distributed Coordination Function IFS)
  - Denotes long waiting Time.
  - lowest priority, for asynchronous data service
  - DIFS = SIFS +2 x Slot Time

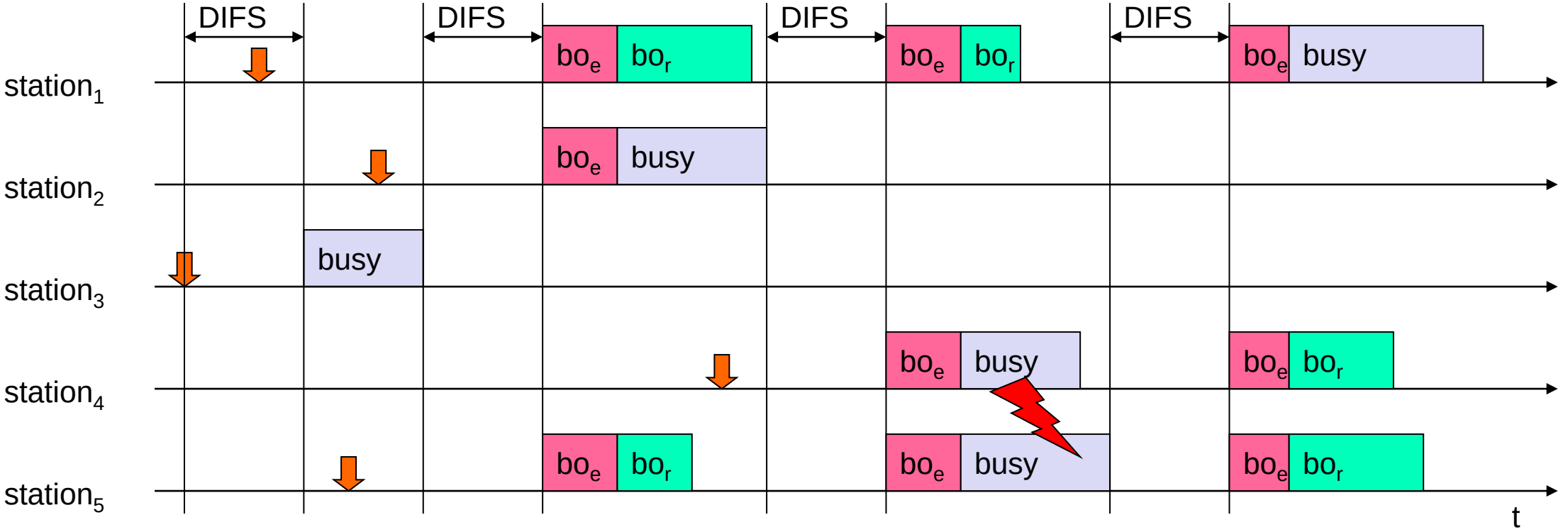
Basic DFWMAC-DCF using CSMA/CA

- 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 - MAC LAYER

- 802.11 - competing stations - simple version



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

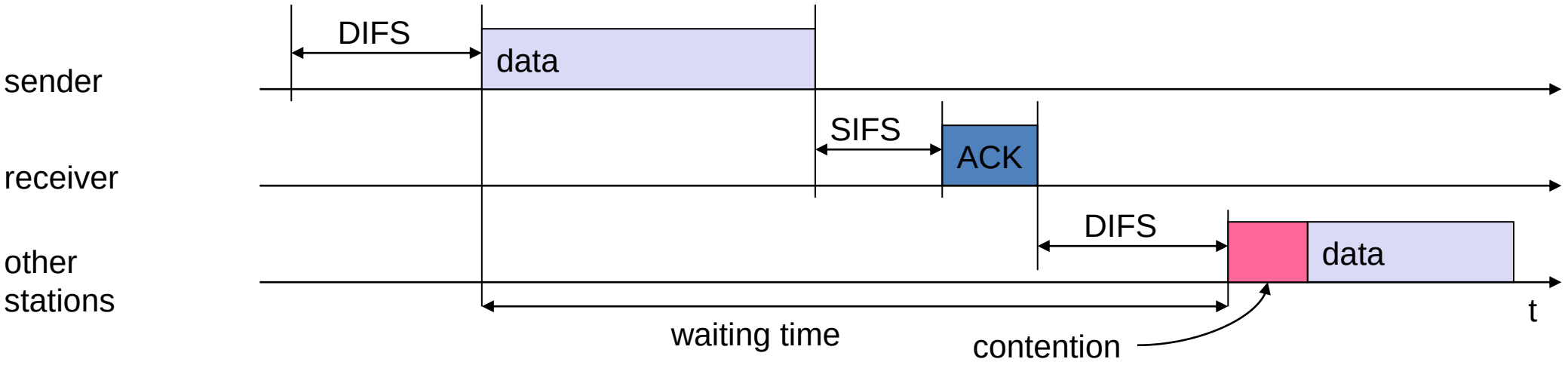
packet arrival at MAC

bo_e — elapsed backoff time

bo_r — residual backoff time

802.11 - MAC LAYER

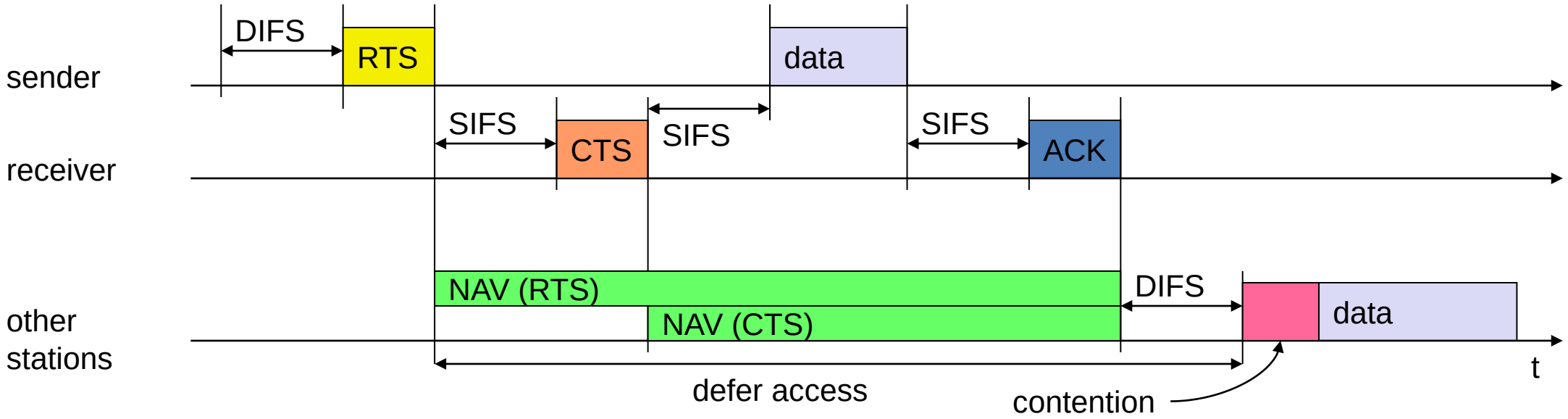
- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors



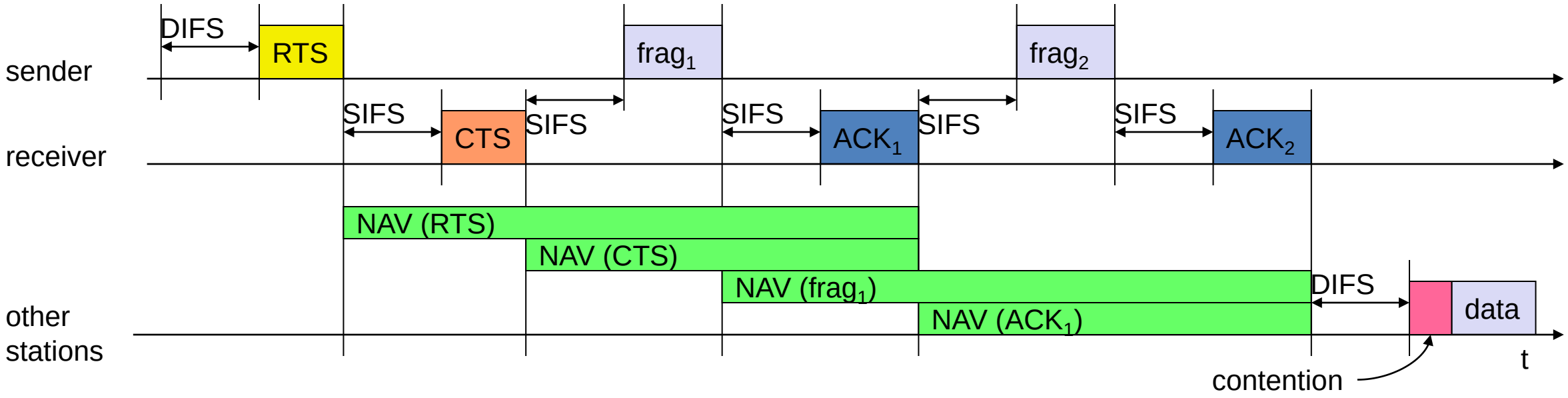
DFWMAC-DCF with RTS/CTS extension

- 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

802.11 - MAC LAYER



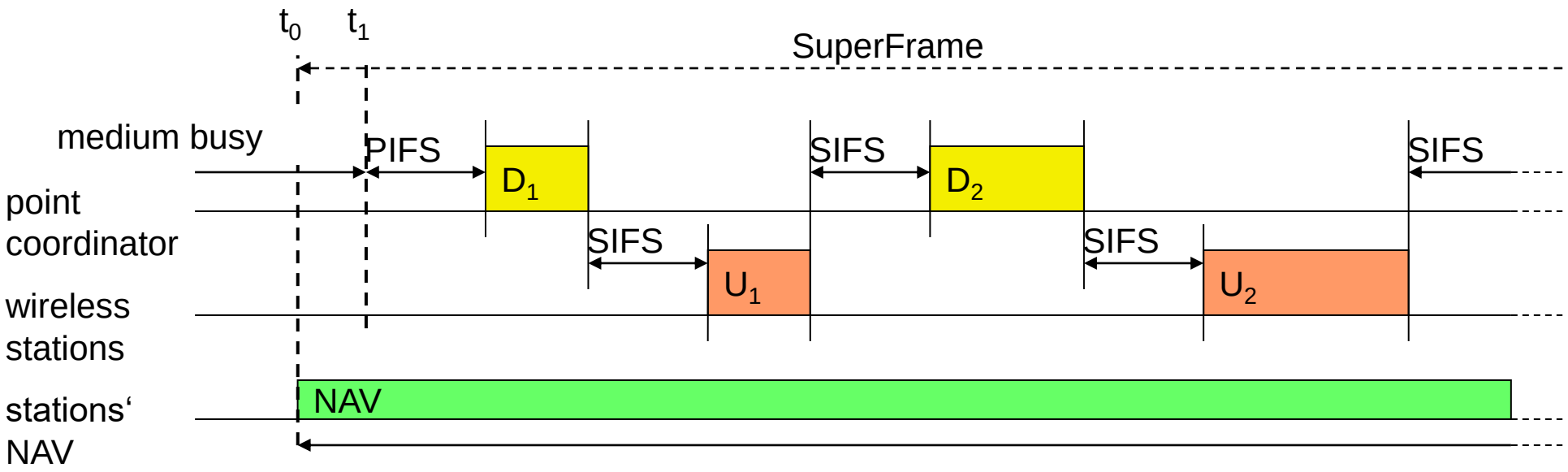
Fragmentation

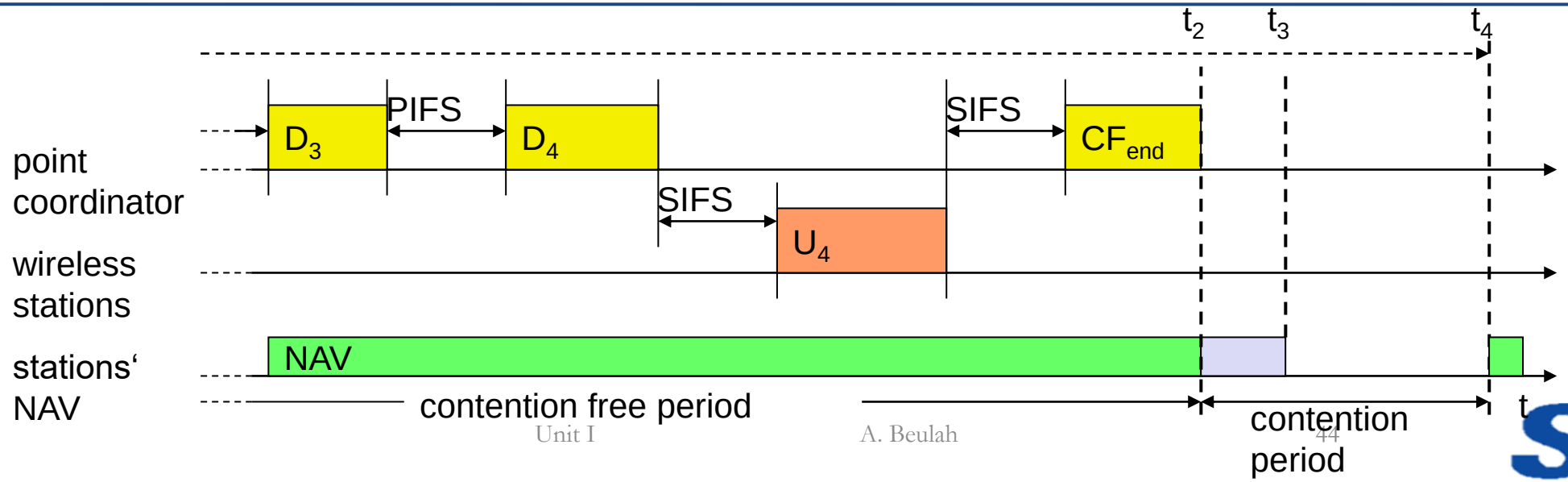


DFWMAC-PCF with polling

- Using PCF requires an access point that controls medium access and polls the single nodes.
- Adhoc networks cannot use this function so, provide no QoS but best effort in IEEE 802.11 WLANs.
- The point coordinator in the access point splits the access time into superframe periods.
- A superframe comprises a contention-free period and a contention period.
- The contention period can be used for the two access mechanisms presented above.

802.11 - MAC LAYER



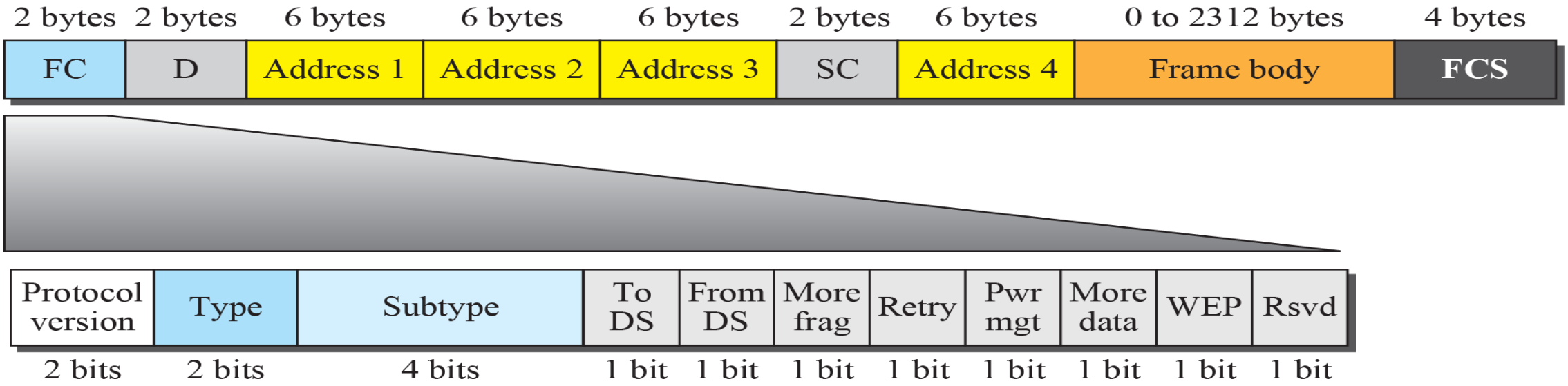


802.11 - Frame format

- 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

802.11 - MAC LAYER

- Frame format



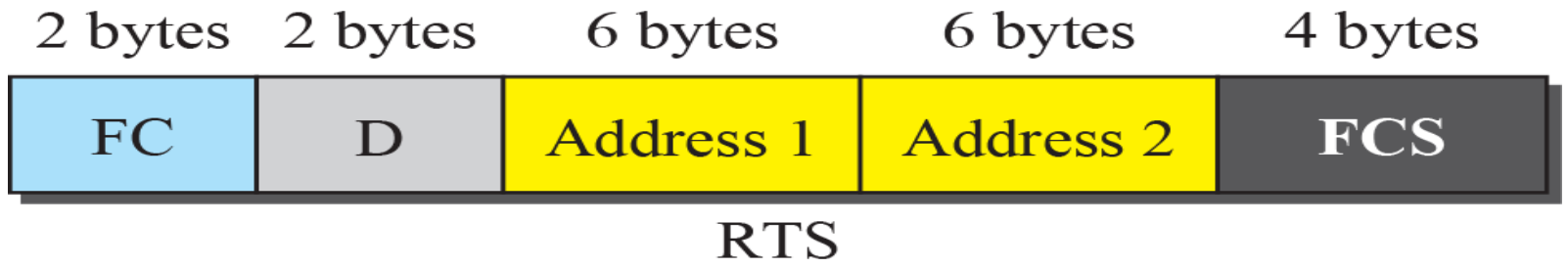
802.11 - MAC LAYER

Field	*Explanation*
Version	Current version is 0
Type	Type of information: management (00), control (01), or data (10)
Subtype	Subtype of each type (see Table 6.2)
To DS	Defined later
From DS	Defined later
More flag	When set to 1, means more fragments
Retry	When set to 1, means retransmitted frame
Pwr mgt	When set to 1, means station is in power management mode
More data	When set to 1, means station has more data to send
WEP	Wired equivalent privacy (encryption implemented)
Rsvd	Reserved

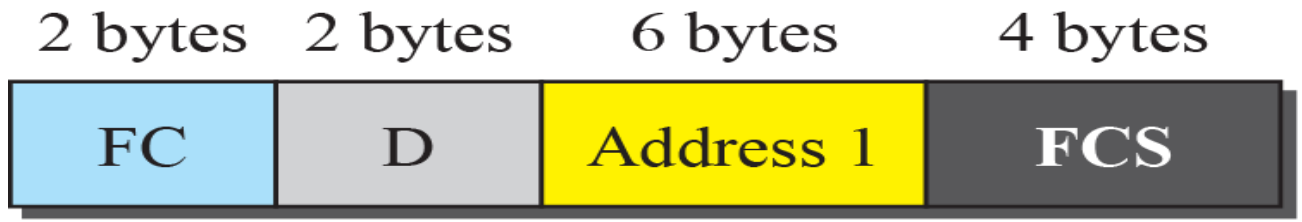
Subtype	*Meaning*
1011	Request to send (RTS)
1100	Clear to send (CTS)
1101	Acknowledgment (ACK)

802.11 - MAC LAYER

- Control Frames



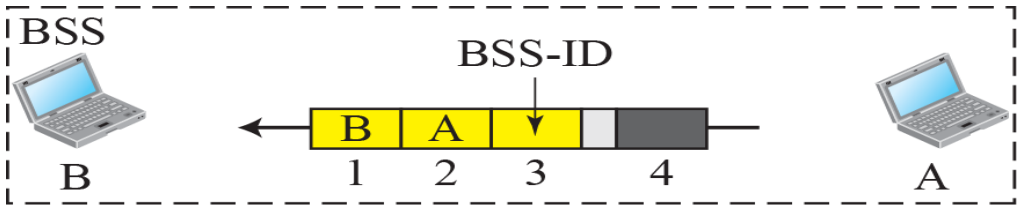
RTS



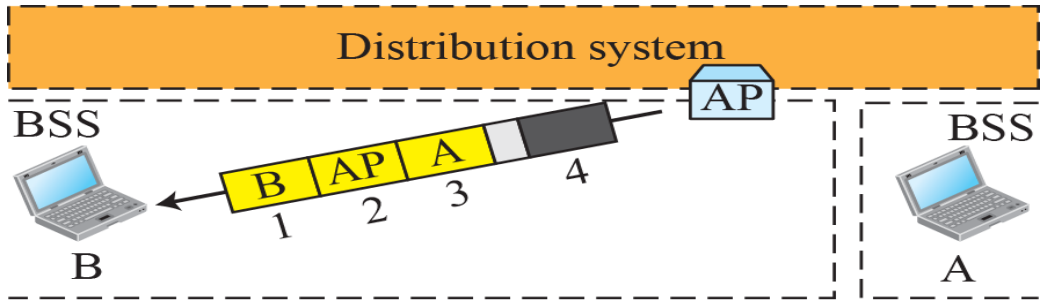
CTS or ACK

802.11 - MAC LAYER

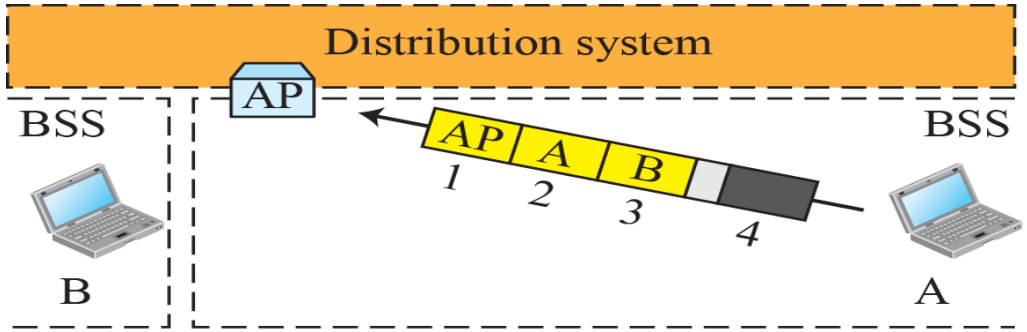
- Addressing mechanism



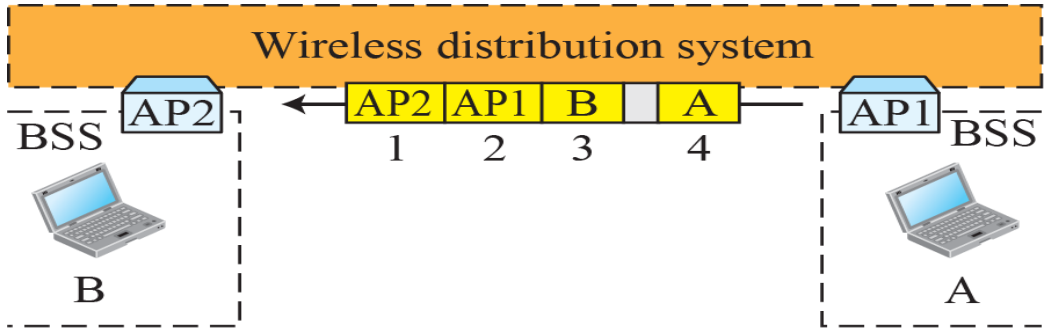
a. Case 1



b. Case 2



c. Case 3



d. Case 4

802.11 - MAC LAYER

- Addressing mechanism

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

802.11 - MAC management

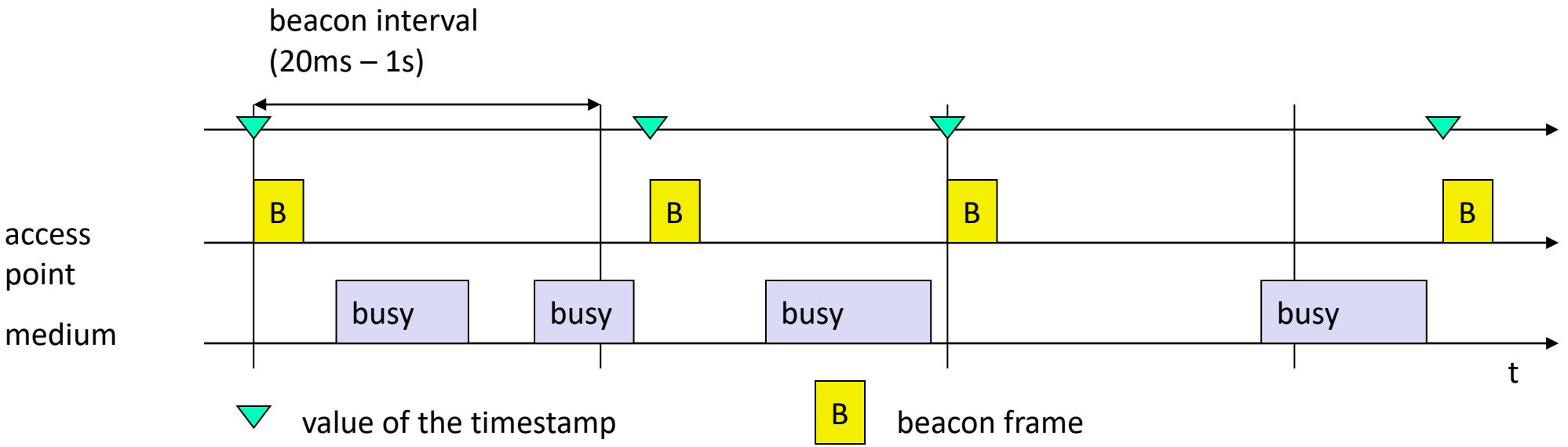
- Synchronization
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

802.11 - MAC LAYER

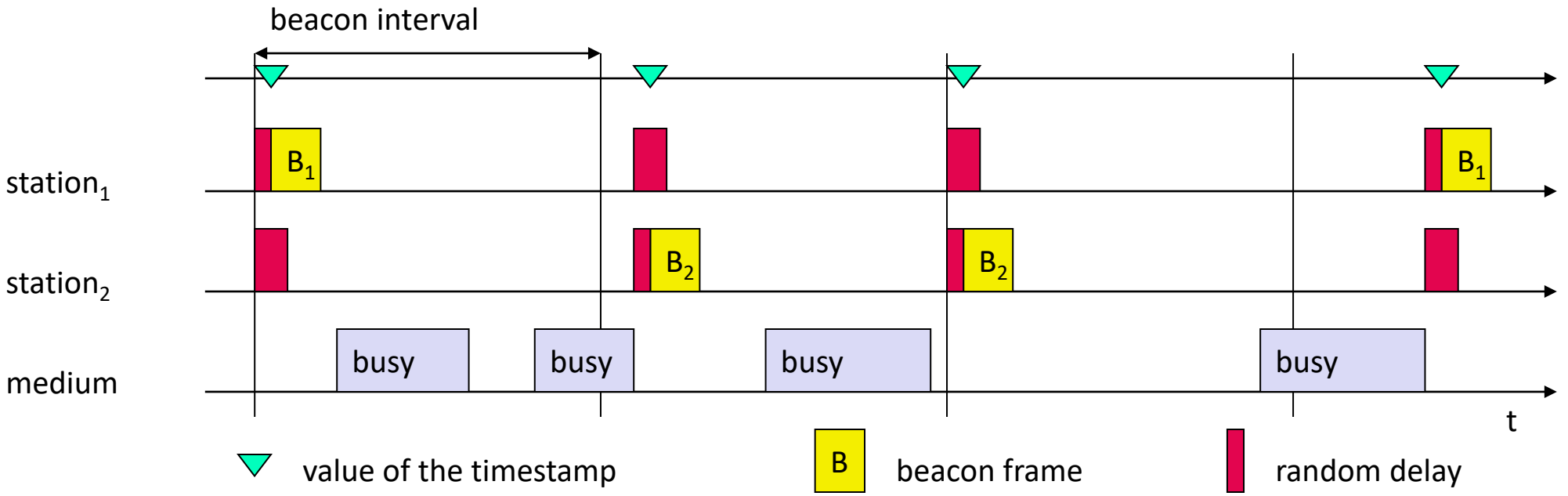
Synchronization

- Timing synchronization function (TSF)
- Used for power management
- Beacons sent at well known intervals
- All station timers in BSS are synchronized

- Synchronization using a Beacon (infrastructure)



- Synchronization using a Beacon (ad-hoc)



802.11 - MAC LAYER

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

802.11 - MAC LAYER

Power management approach

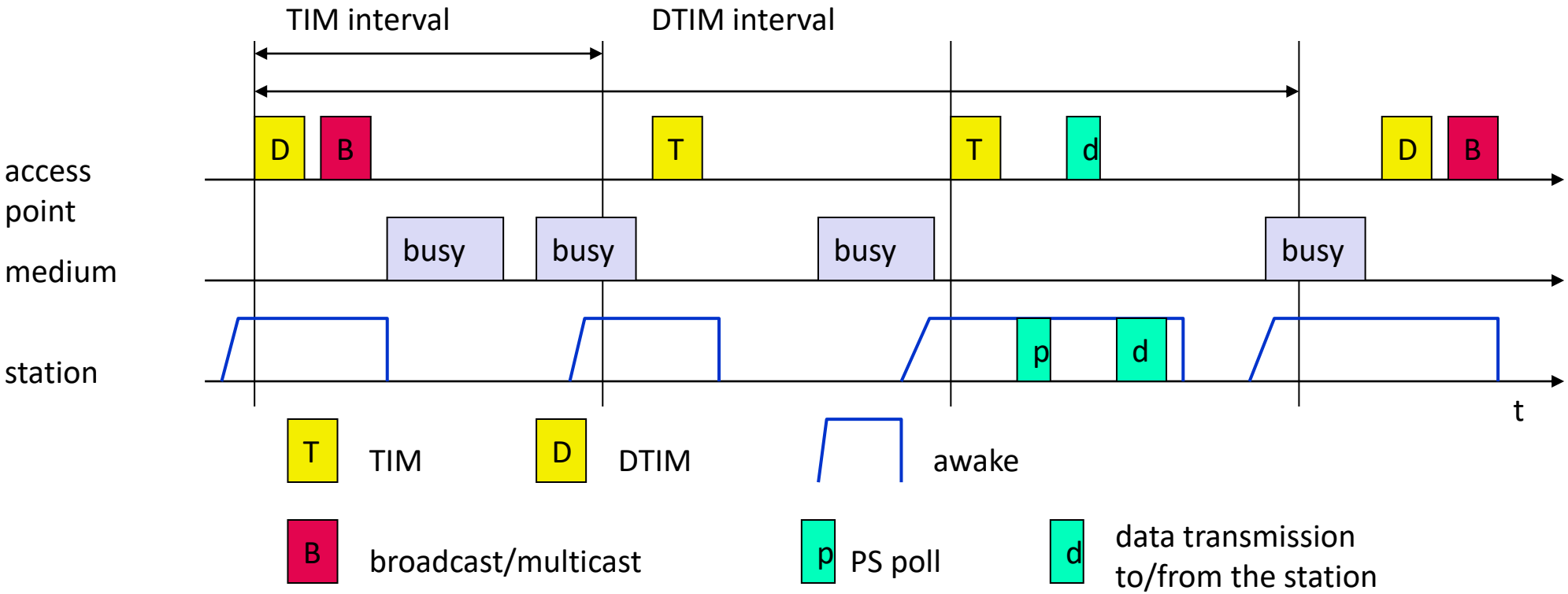
- Allow idle stations to go to sleep

  - station's power save mode stored in AP

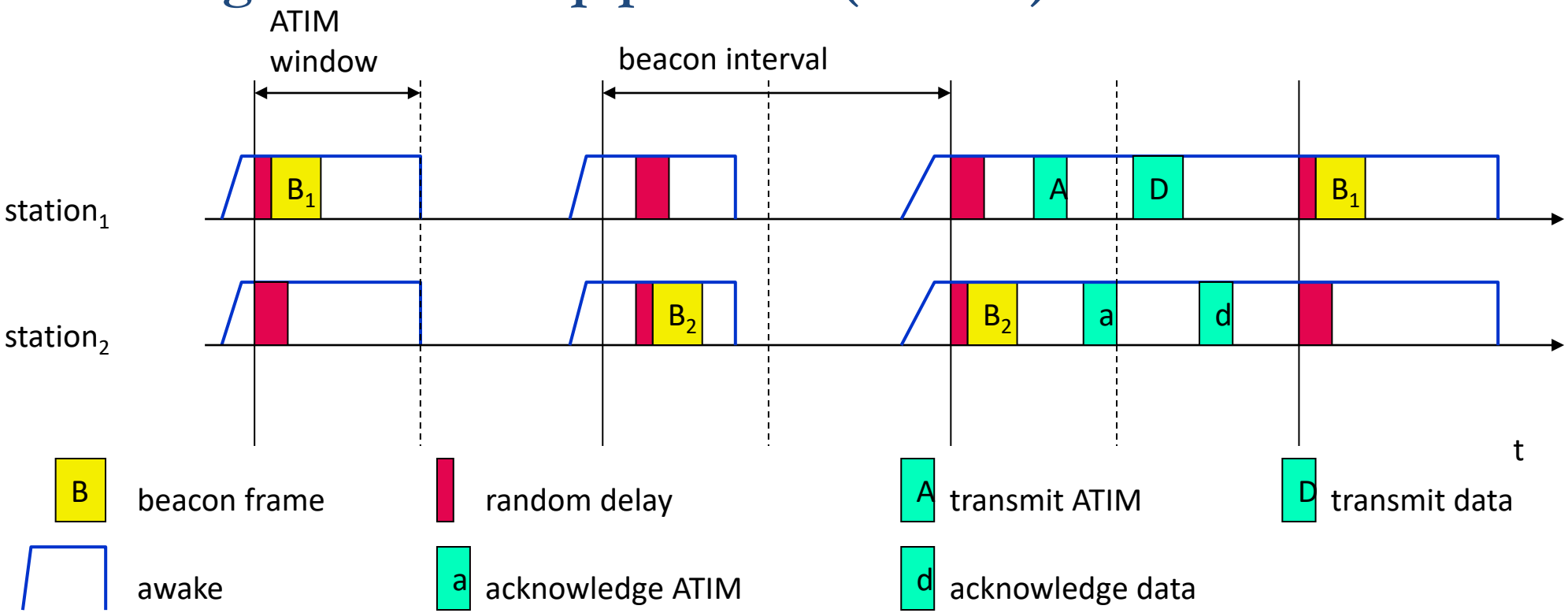
- APs buffer packets for sleeping stations- AP announces which stations have frames buffered - traffic indication map (TIM) sent with every beacon

- Power saving stations wake up periodically

- **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

802.11 - MAC LAYER

- Mobile stations may move - beyond the coverage area of their AP
  - but within range of another AP
- Re association allows station to continue operation.

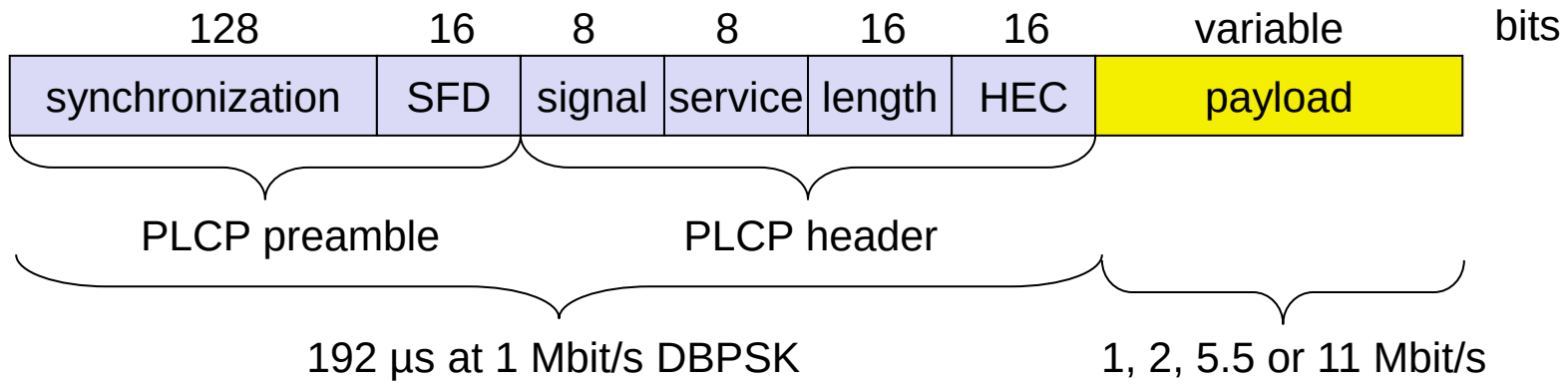
802.11 - MAC LAYER

- **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

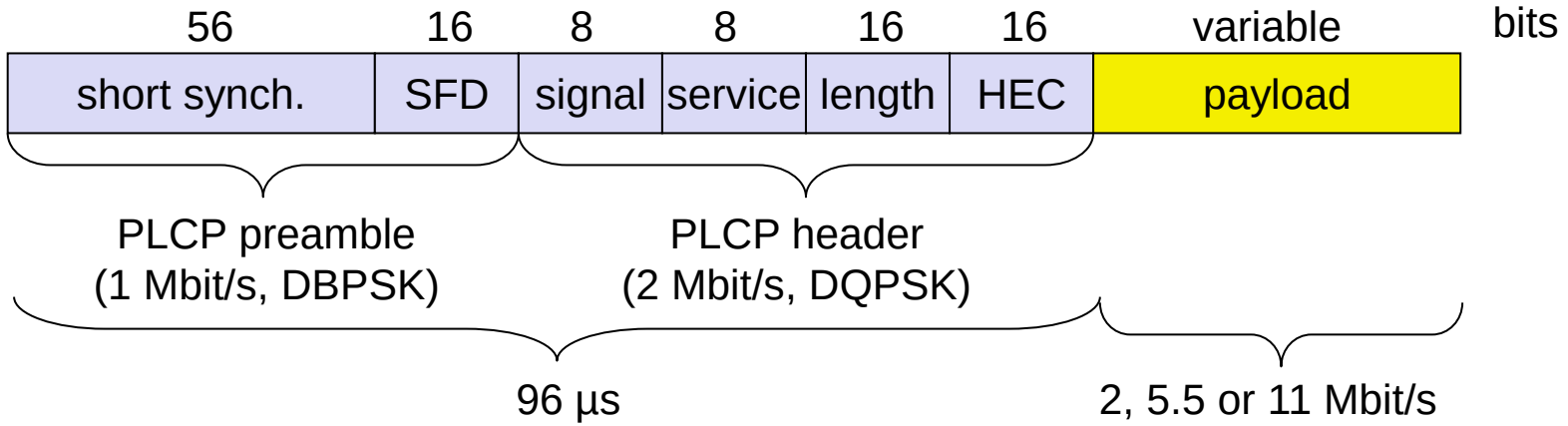
802.11 - MAC LAYER

- **IEEE 802.11b**
- **PHY frame formats**

Long PLCP PPDU format



Short PLCP PPDU format (optional)

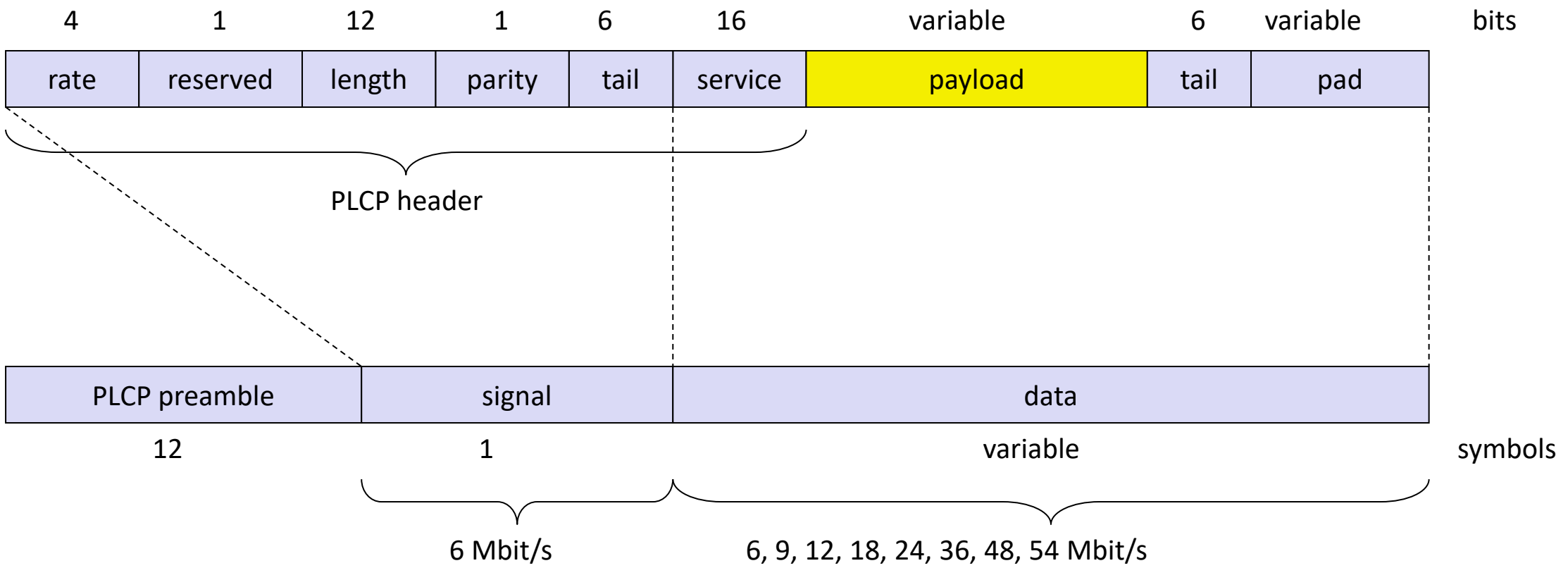


802.11 - MAC LAYER

- **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

802.11 - MAC LAYER

- **IEEE 802.11a**
- **PHY frame formats**



SUMMARY

- MAC Protocols
  - Properties, Issues
  - Different Categories of MAC

TEST YOUR KNOWLEDGE

- Switches are capable of reading the MAC address field from each frame that comes to them. So we can say they work on the _____ layer from the TCP/IP model.
  - Physical
  - Network
  - Data Link

- In IEEE 802.11, a ___ is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP)
  - ESS
  - BSS
  - CSS

TEST YOUR KNOWLEDGE

- A BSS without an AP is called an _____.
  - an ad hoc architecture
  - an infrastructure network

- communication between two stations in two different BSSs usually occurs via two _____.
  - BSSs
  - ESSs
  - APs

TEST YOUR KNOWLEDGE

- When a frame is going from one station to another in the same BSS without passing through the distribution system, the address flag is _____
  - 00
  - 01
  - 10
- When a frame is going from a station to an AP, the address flag is _____.
  - 01
  - 10
  - 11

REFERENCES

- Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.
- Behrouz A. Forouzan, “Data communication and Networking”, Fourth Edition,Tata McGraw – Hill, 2011.