# *IEEE 802.11*

## *Basic Connectivity*

*Manuel Ricardo*

*Faculdade de Engenharia da Universidade do Porto*

# *Acknowledgements*


- Based on *Jochen Schiller* slides

- Supporting text
  - » Jochen Schiller, “Mobile Comunications”, Addison-Wesley
  - » Section 7.3 – Wireless LAN

# *Characteristics of Wireless LAN*

- Advantages over wired LANs
  - » Terminal is free to move
  - » Network uses less cabling
  - » Possibility of forming unplanned, ad-hoc, networks

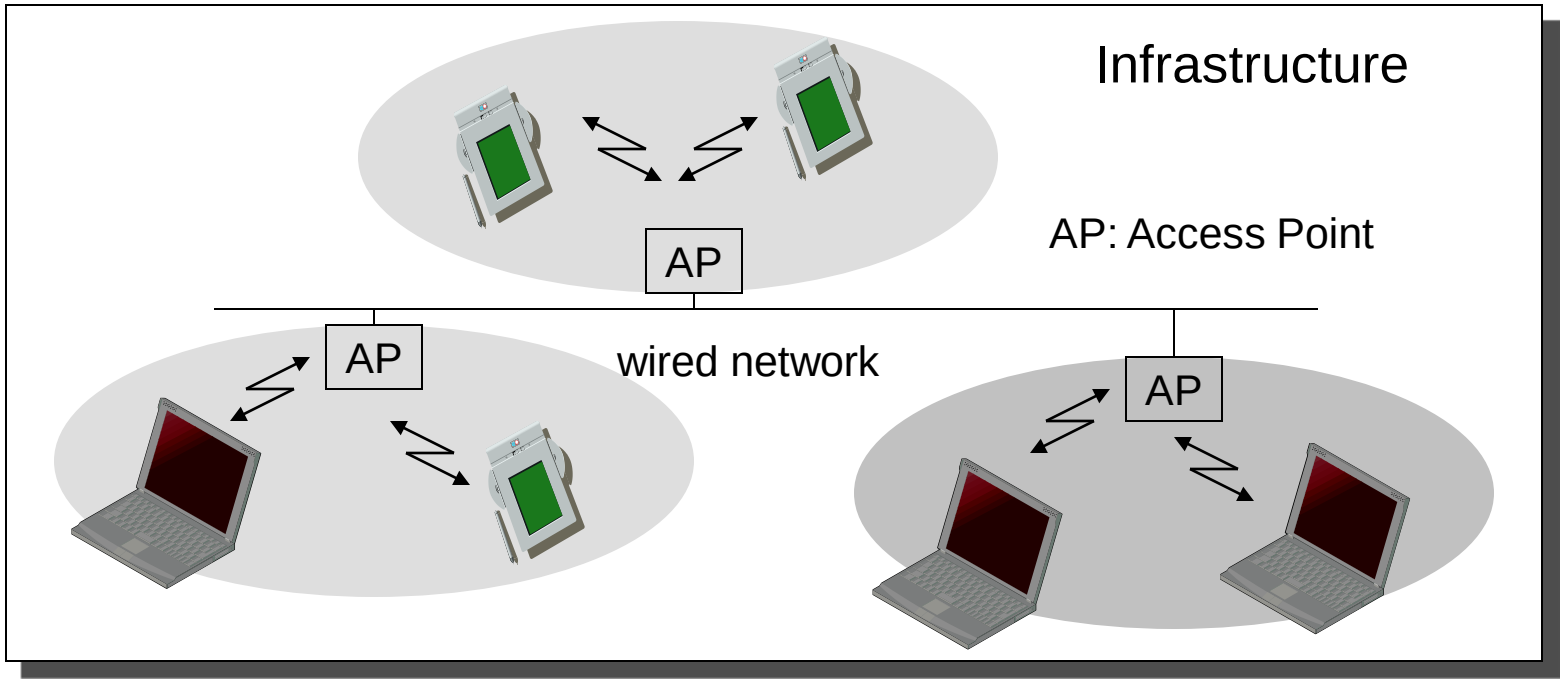
- Disadvantage
  - » Smaller and variable bitrates

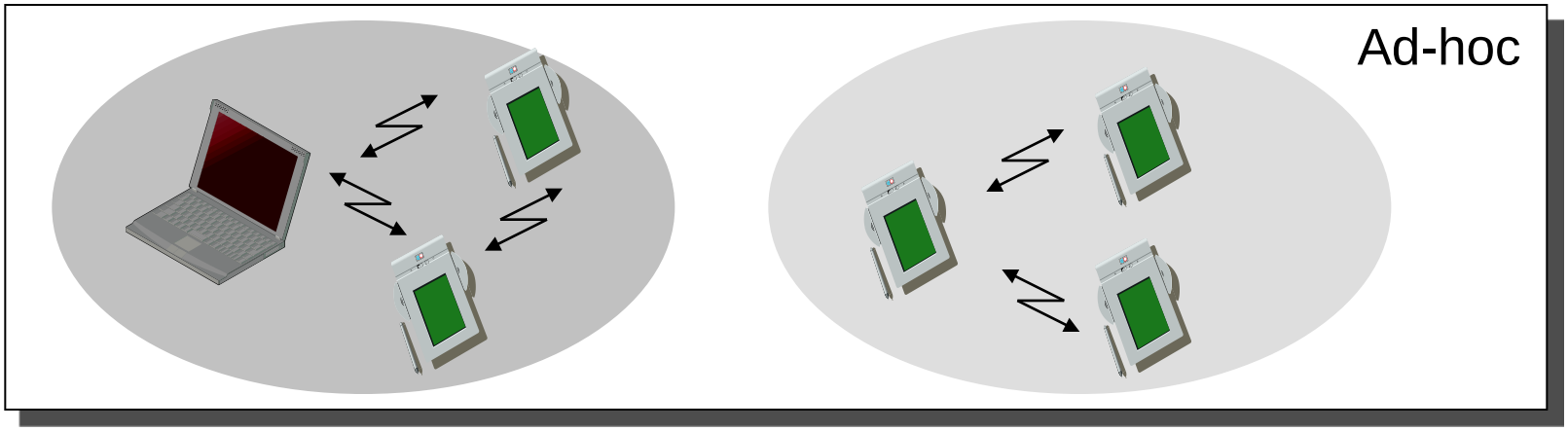
# *Transmission - Radio and Infrared*

- Radio
  - » Band ISM, 2.4 GHz and 5 GHz
- Advantages
  - » Planning similar to cellular networks
  - » Large coverage
- Disadvantages
  - » Limited resources
  - » ISM, noisy channels

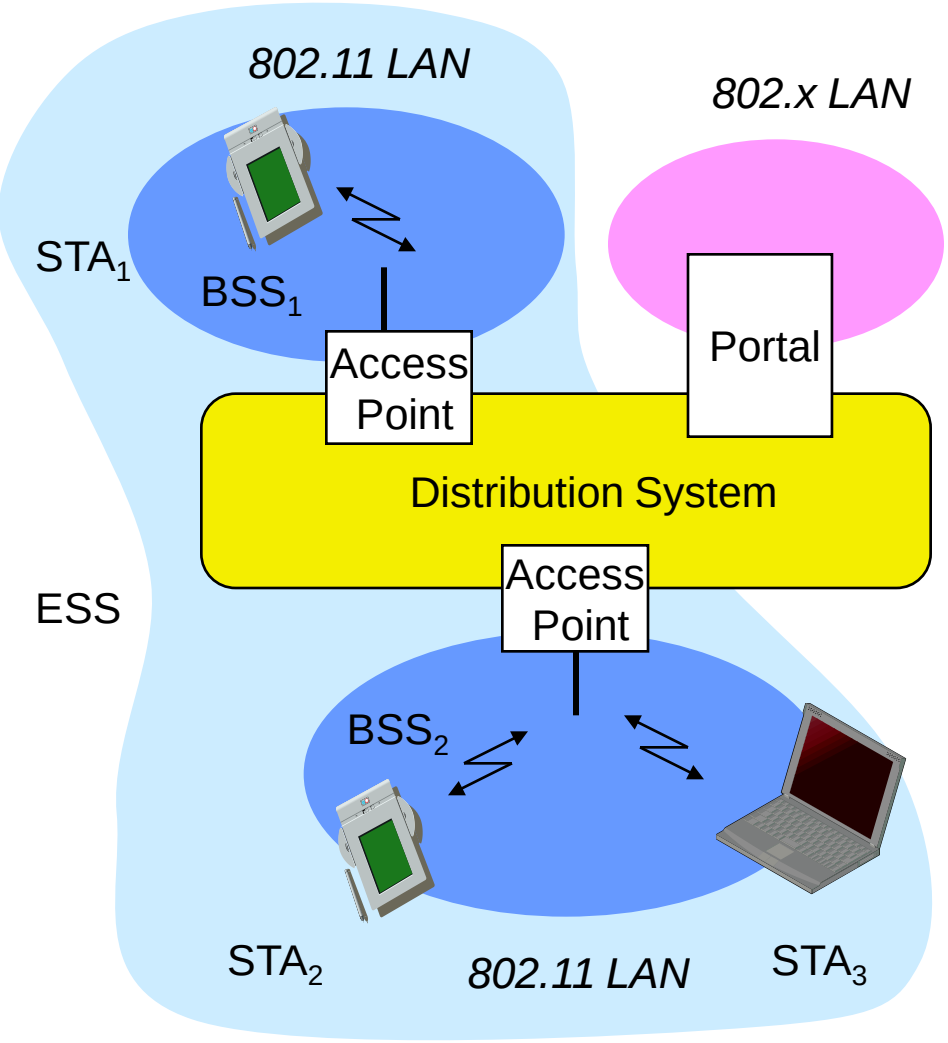
- Infrared
  - » Diods, multiple reflection
- Advantages
  - » Simple
- Disadvantages
  - » Interferences
    - – Solar light, heat sources
  - » Smaller bitrates

# *Infrastructure Networks vs Ad-Hoc Networks*



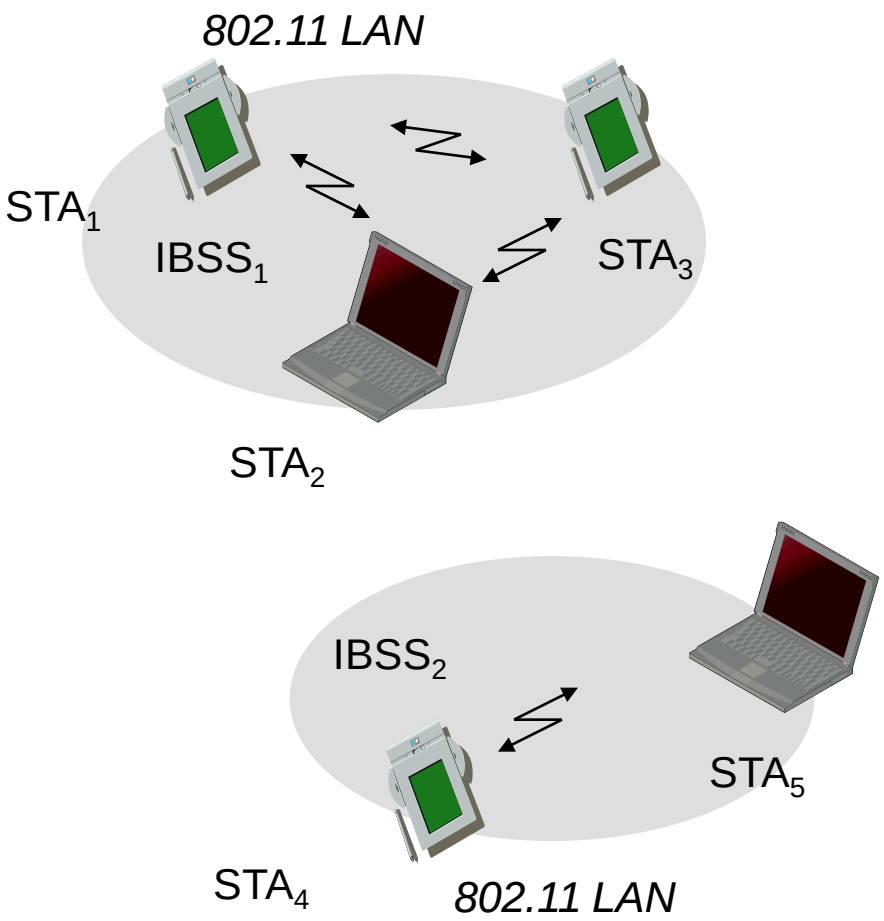



# *IEEE 802.11 – Infrastructure Network*



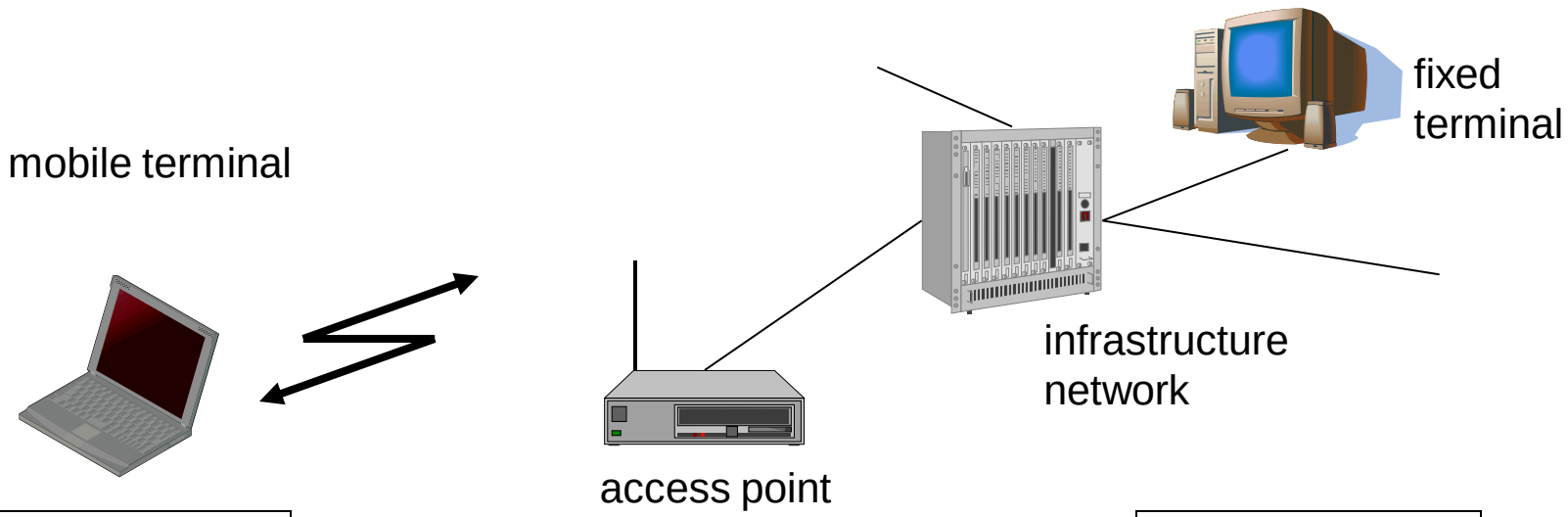

- Station
  - » Terminal with radio access
- Basic Service Set (BSS)
  - » Set of stations in the same band
- Access Point (AP)
  - » Interconnects LAN to wired network
  - » Provides access to stations
- Stations communicate with AP
- Portal → bridge to other networks
- Distribution System
  - » Interconnection network
  - » Logical network
    - – EES, Extended Service Set
    - – Based on BSSs

# *IEEE 802.11 –Ad-Hoc Network*



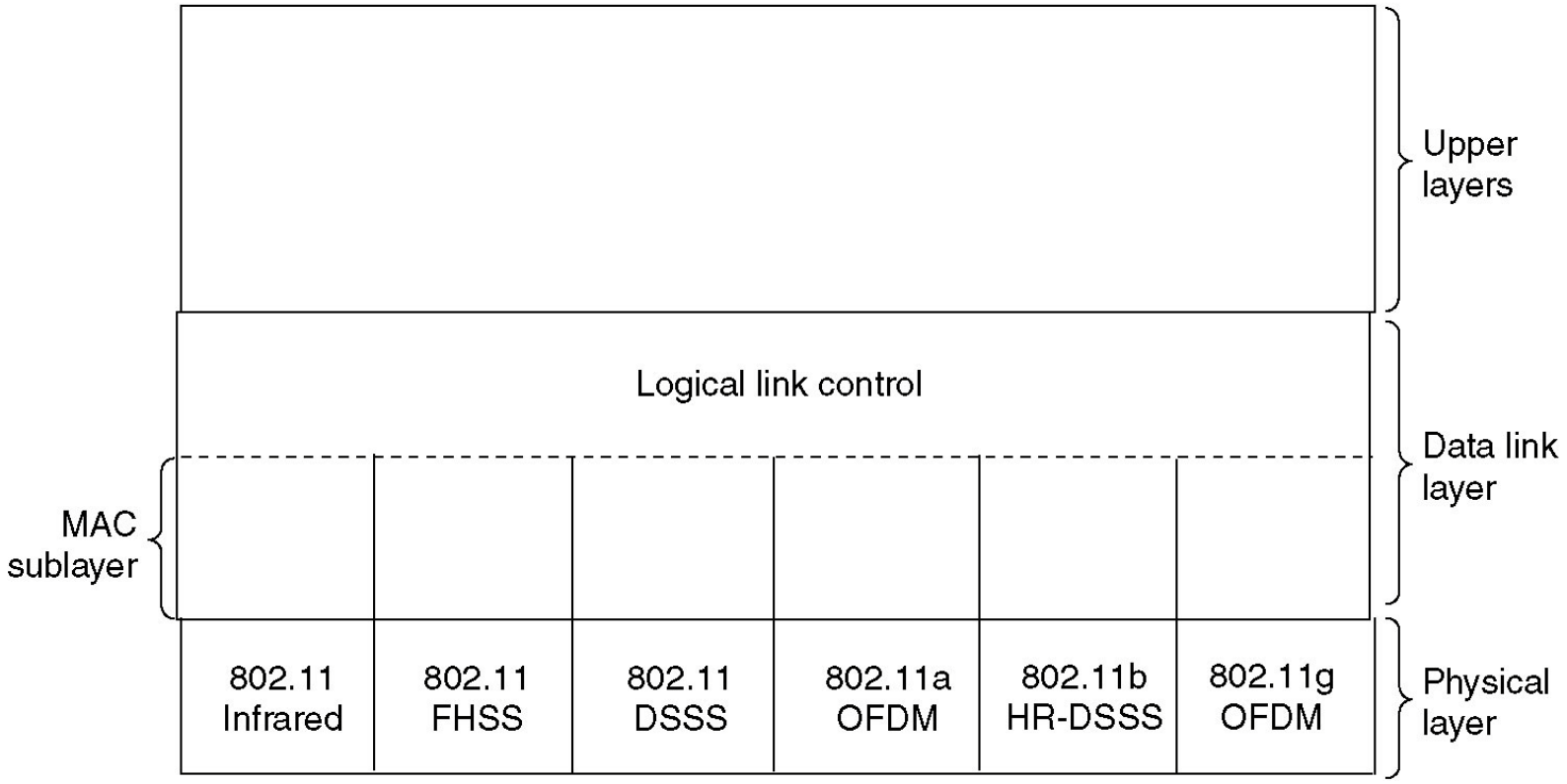

- Direct communication between stations
- Independent Basic Service Set, IBSS
  - » Set of stations working the the same carrier (radio channel)

# IEEE 802.11 – Protocol Stack



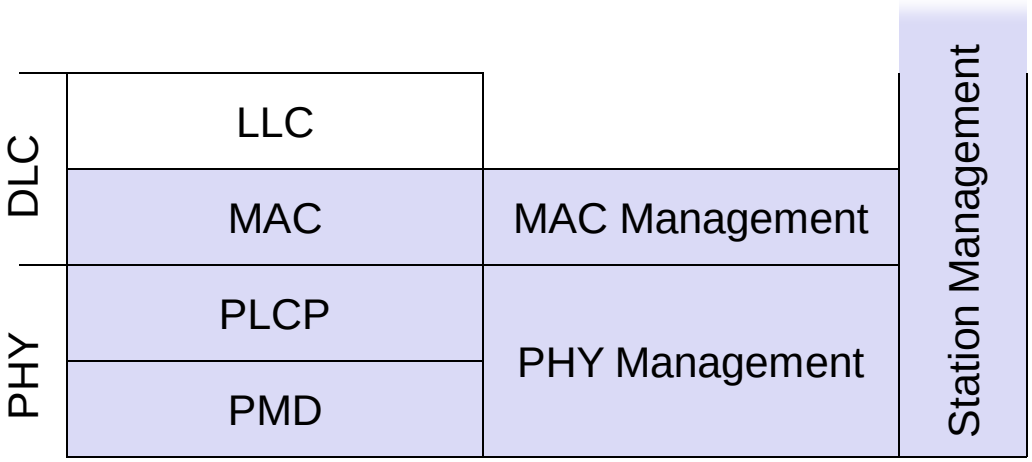

| application | | | application |
|---|---|---|---|
| TCP | | | TCP |
| IP | | | IP |
| LLC | LLC | | LLC |
| 802.11 MAC | 802.11 MAC | 802.3 MAC | 802.3 MAC |
| 802.11 PHY | 802.11 PHY | 802.3 PHY | 802.3 PHY |

# *802.11 – Protocol Stack*



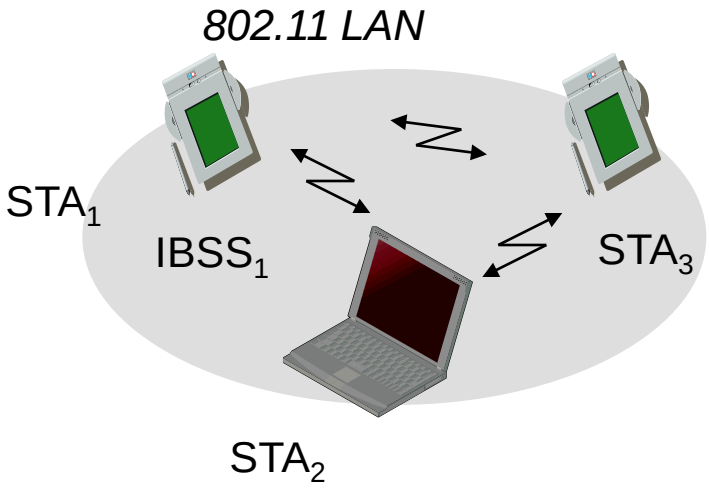
# *802.11 – Layers and Functionalities*

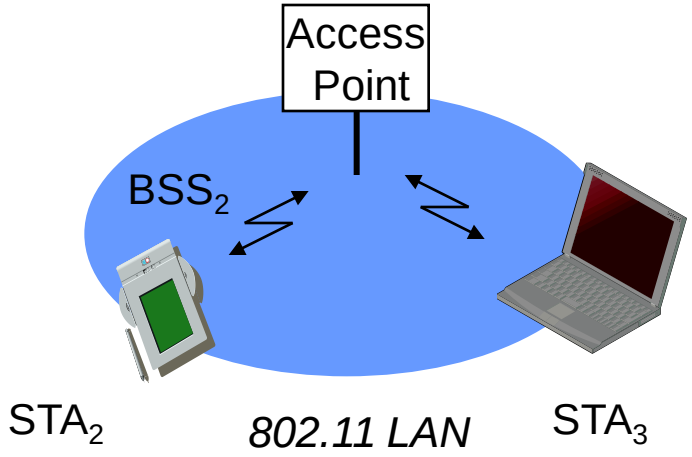
- Data plane
  - » MAC → medium access, fragmentation, encryption
  - » PLCP - Physical Layer Convergence Protocol → carrier detection
  - » PMD - Physical Medium Dependent → modulation, codification
- Management plane
  - » PHY Management → channel selection, MIB
  - » MAC Management → synchronisation, mobility, power, MIB
  - » Station Management → coordenation management functions



# *To Think About?*

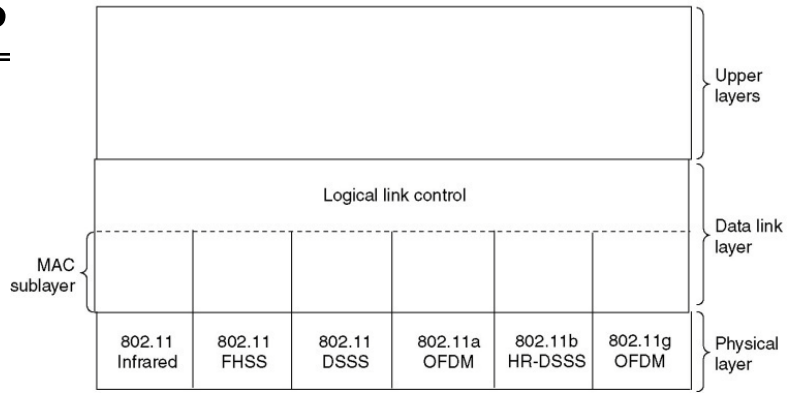
- *How to minimize collision in a wireless, shared, medium?*



# *MAC Layer – Access Methods*

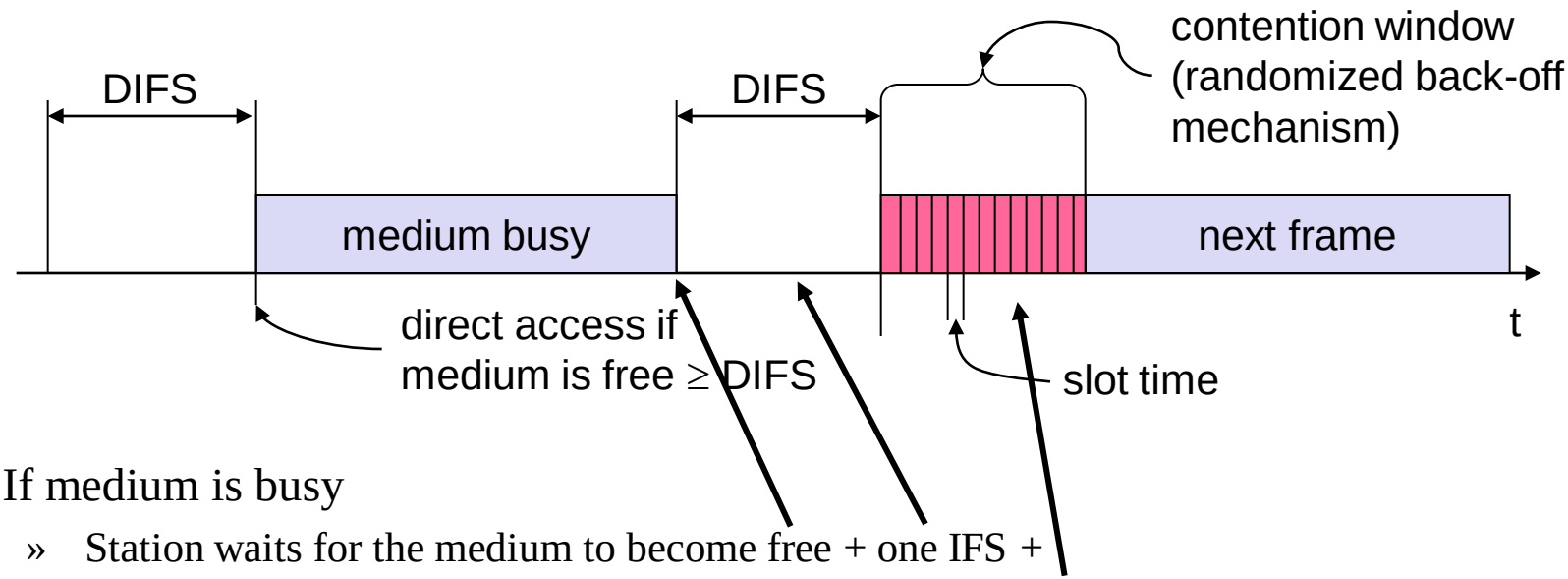
DCF – Distributed Coordination Function
PCF - Point Coordination Function




- MAC-DCF CSMA/CA
  - Carrier sense, collision avoidance using back-off mechanism
  - ACK packet required for confirmations (except for broadcast packets)
  - mandadory
- MAC-DCF with RTS+CTS
  - Used to avoid hidden terminal problem
  - Optional
- MAC- PCF
  - Access Point asks stations to transmit
  - Optional

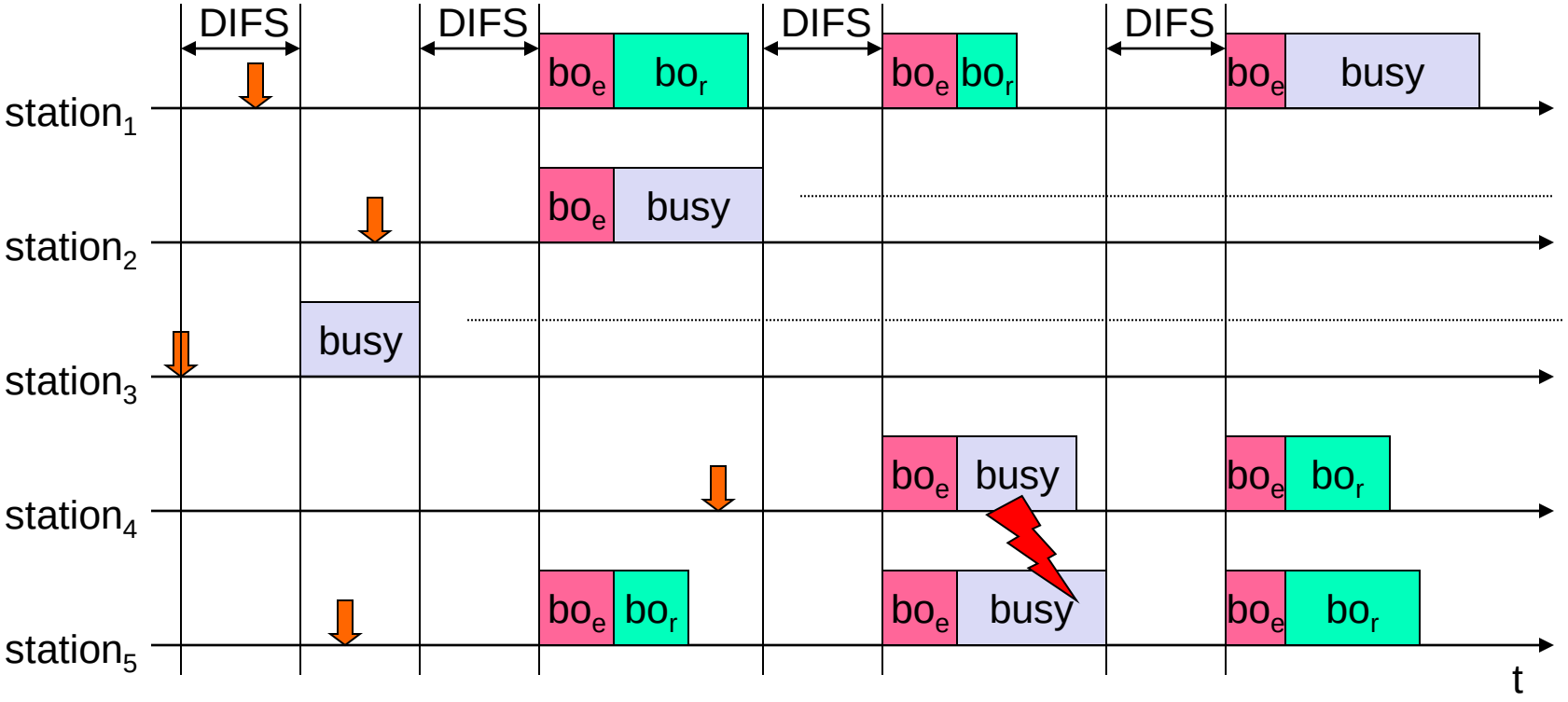
# *MAC-DCF CSMA/CA*

- Station having a packet to transmit senses the medium
- If the medium is free during one Inter-Frame Space (IFS)
  - » Station starts sending the frame




- If medium is busy
  - » Station waits for the medium to become free + one IFS + random contention period (collision avoidance, múltiplo de slot→ n* 20 us)
- If other station accesses to the medium during the contention time
  - » Waiting timer is suspended

# *MAC-DCF CSMA/CA – Concurrent Stations*



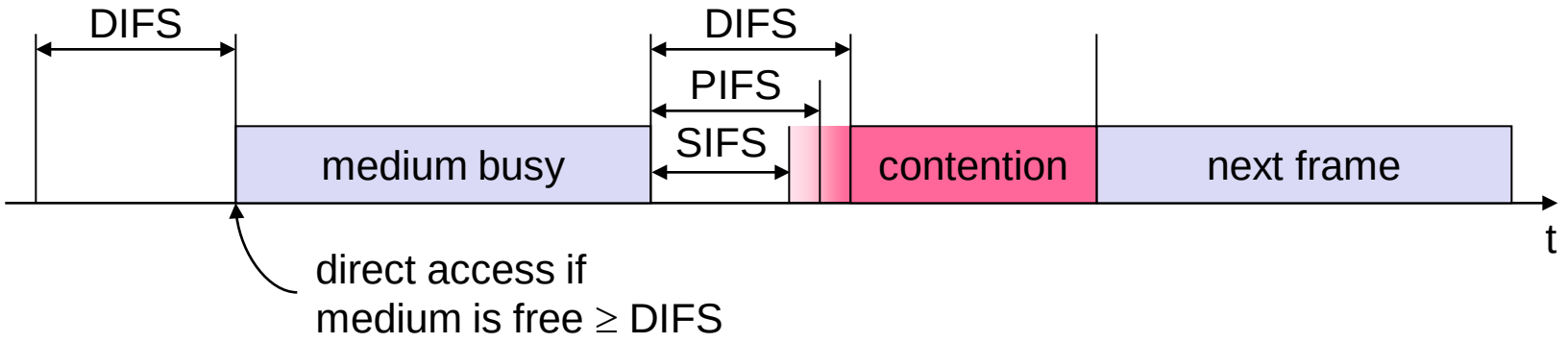

busy — medium not idle (frame, ack etc.)

packet arrival at MAC

$bo_e$ — elapsed backoff time

$bo_r$ — residual backoff time

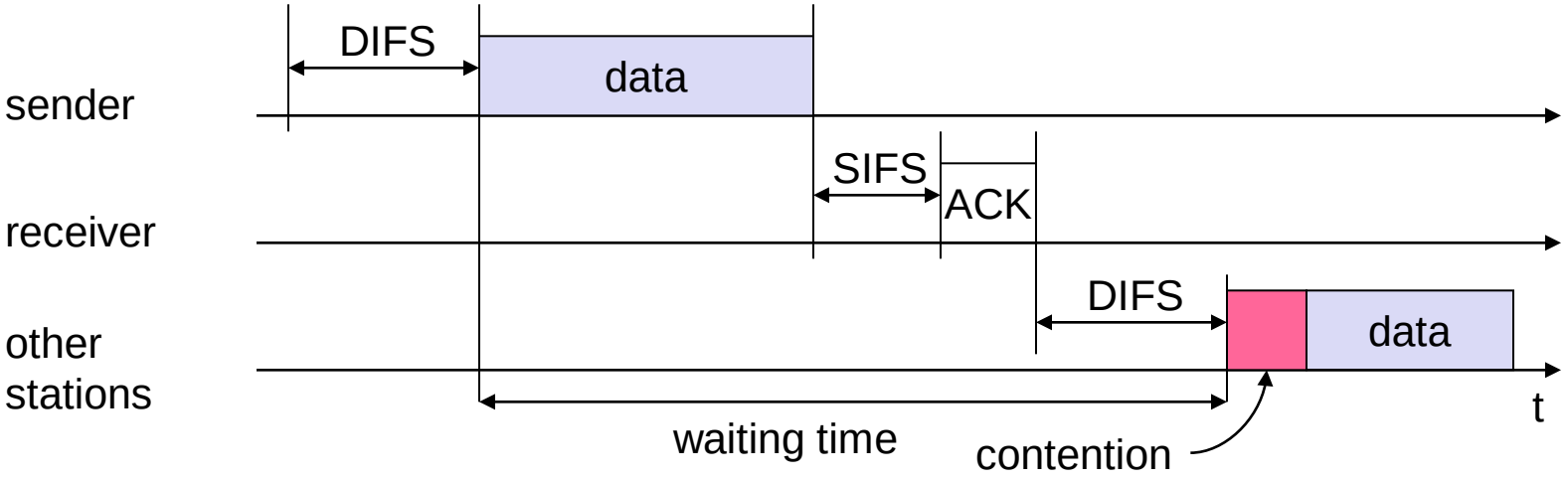
# *MAC Layer – Guard Time Intervals*




- DIFS (DCF IFS)
  - Lowest priority, used for asynchronous data
- PIFS (PCF IFS)
  - Medium priority, used for real time traffic /QoS
- SIFS (Short Inter Frame Spacing)
  - Maximum priority→ used for signalling: ACK, CTS, answers to polling

# *MAC-DCF CSMA/CA*

- Sending a frame in unicast
  - » Station waits DIFS before sending the packet
  - » If packet is correctly received (no errors in CRC)
    - Receiver confirms reception immediatly, using ACK, after waiting SIFS
  - » In case of errors, frame is re-transmitted
  - » In case of retransmission
    - Maximum value for the contention window duplicates
    - Contetion window has minimum and maximum values (eg.: 7 and 255)



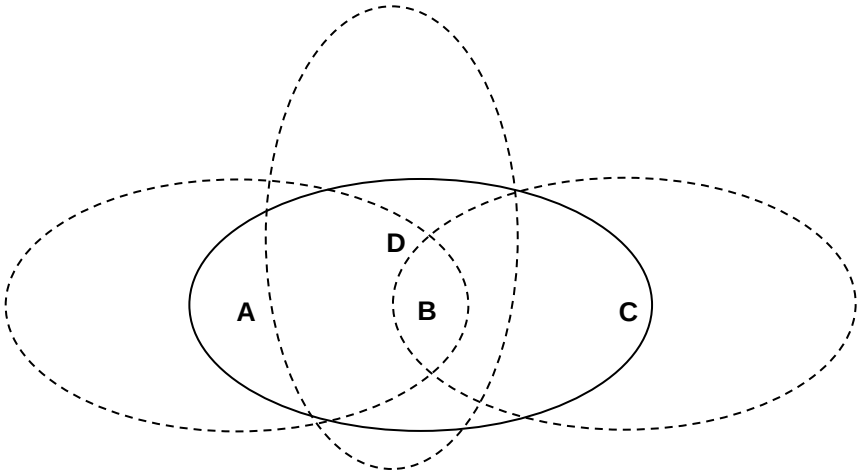
# *Virtual Carrier Sensing – Network Allocation Vector*

- How does a station know if the medium is free?
  - » Usually, by listening the carrier

- IEEE 802.11 also uses Network Allocation Vector (NAV)
  - » 802.11 frames contain a duration field; used to reserve the medium
  - » Stations have a timer ***NAV***
    - – Updated with the values seen in the frames
    - – Decremented in real-time
    - – If != zero ➔ medium not free

# *To Think About*

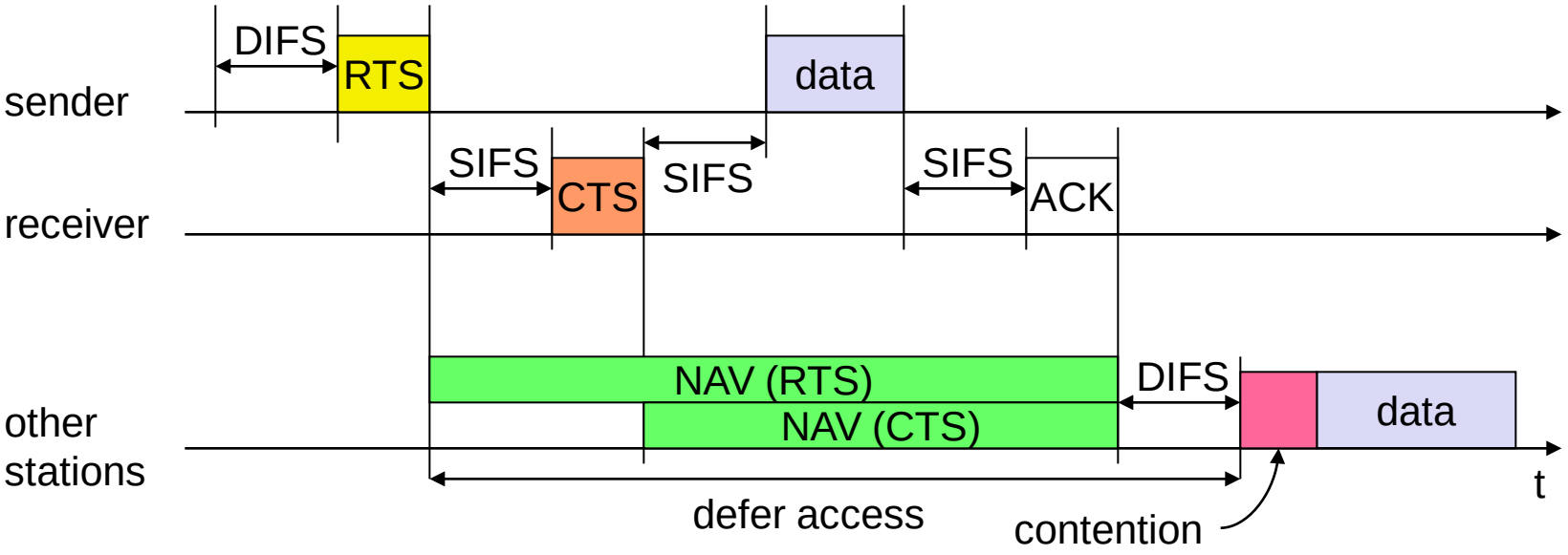
- *How to enable hidden terminals to sense the carrier?*



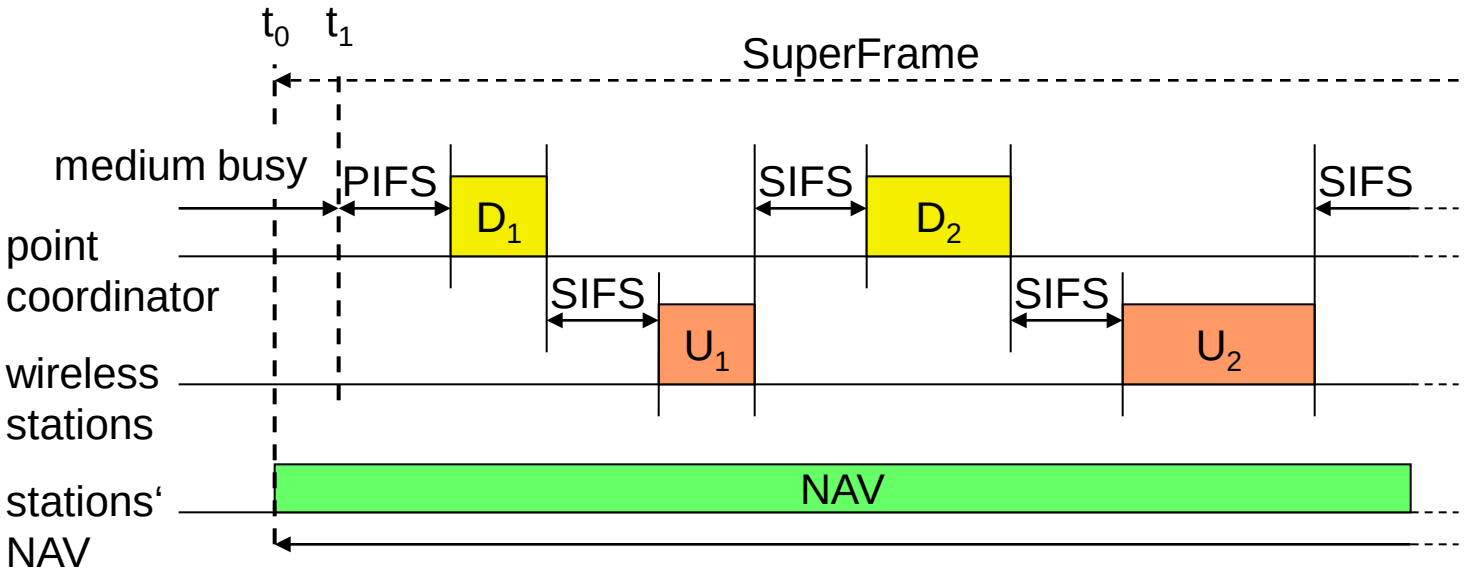

***Hidden node: C is hidden to A***

# *MAC DCF with RTS+CTS*

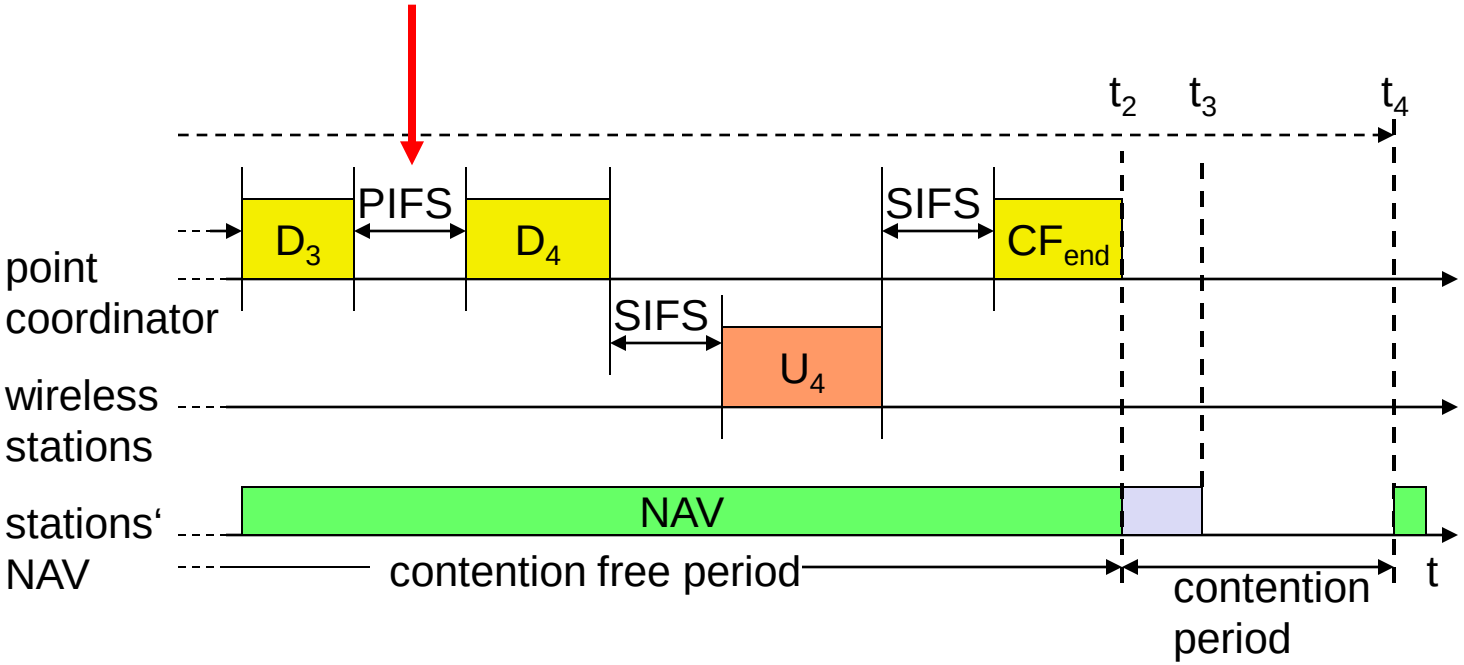
- Sending a frame in unicast
  - » Station sends RTS with a reserve parameter, after waiting DIFS
    - – Reserve time includes RTS+SIFS+CTS+SIFS+DATA+SIFS+ACK
  - » Receiver confirms with CTS, after waiting SIFS
  - » Transmitter sends frame, after waiting SIFS. Confirmation with ACK
  - » Other stations become aware of reserved time by listening RTS and CTS



# *MAC- PCF*

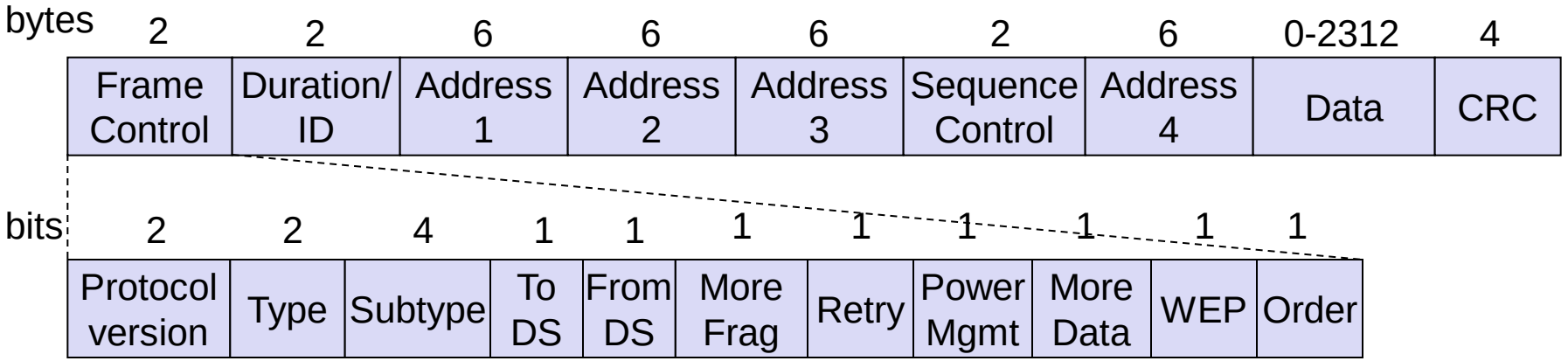

t0
t1
SuperFrame
medium busy
PIFS
D1
SIFS
D2
SIFS
point coordinator
SIFS
U1
SIFS
U2
wireless stations
stations‘ NAV
NAV

# MAC-PCF II


t2
t3
t4
PIFS
SIFS
SIFS
D3
D4
CFend
point coordinator
U4
wireless stations
NAV
stations' NAV
contention free period
contention period
t

# *MAC – Frame Format*

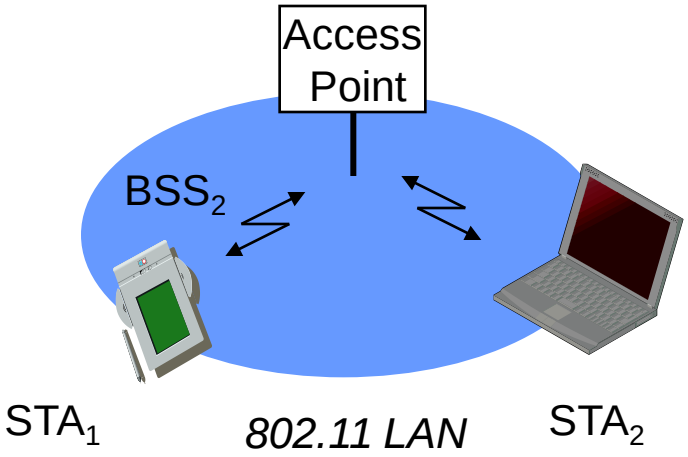
- Frame types
  - » Data, control, management
- Sequence number
- Addresses
  - » destination, source, BSS identifier, ...
- Others
  - » Error control, frame control, data



# *To Think About*

- *$STA_1$ needs to send a frame to $STA_2$. In the Infrastructure mode, the frame is sent via the AP.*

  *What MAC addresses are required in the frame sent by $STA_1$ to the AP?*



# *Addresses in MAC*

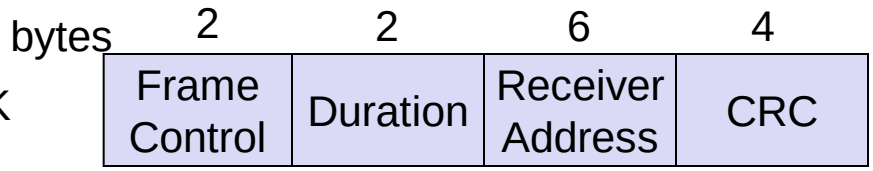
| scenario | to DS | from DS | address 1 | address 2 | address 3 | address 4 |
|---|---|---|---|---|---|---|
| ad-hoc network | 0 | 0 | DA | SA | BSSID | - |
| infrastructure network, from AP | 0 | 1 | DA | BSSID | SA | - |
| infrastructure network, to AP | 1 | 0 | BSSID | SA | DA | - |
| infrastructure 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*

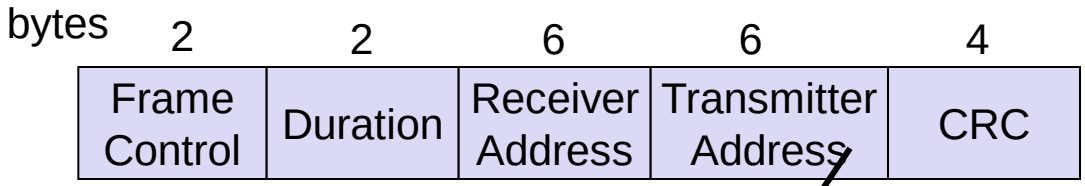
- Acknowledgement

ACK



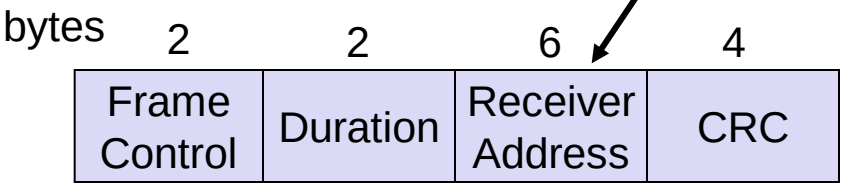

- Request To Send

RTS



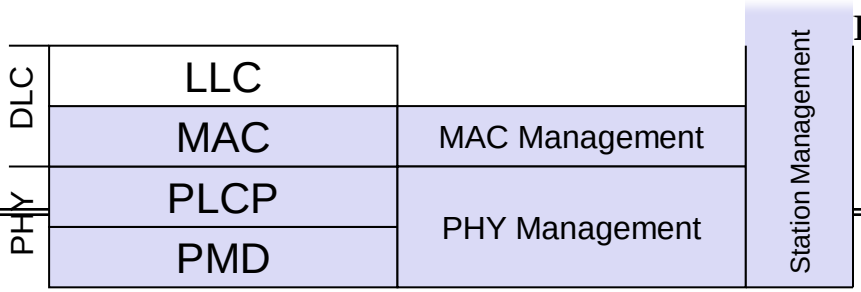

- Clear To Send

CTS




(Fig. 7.17 do livro está errada)

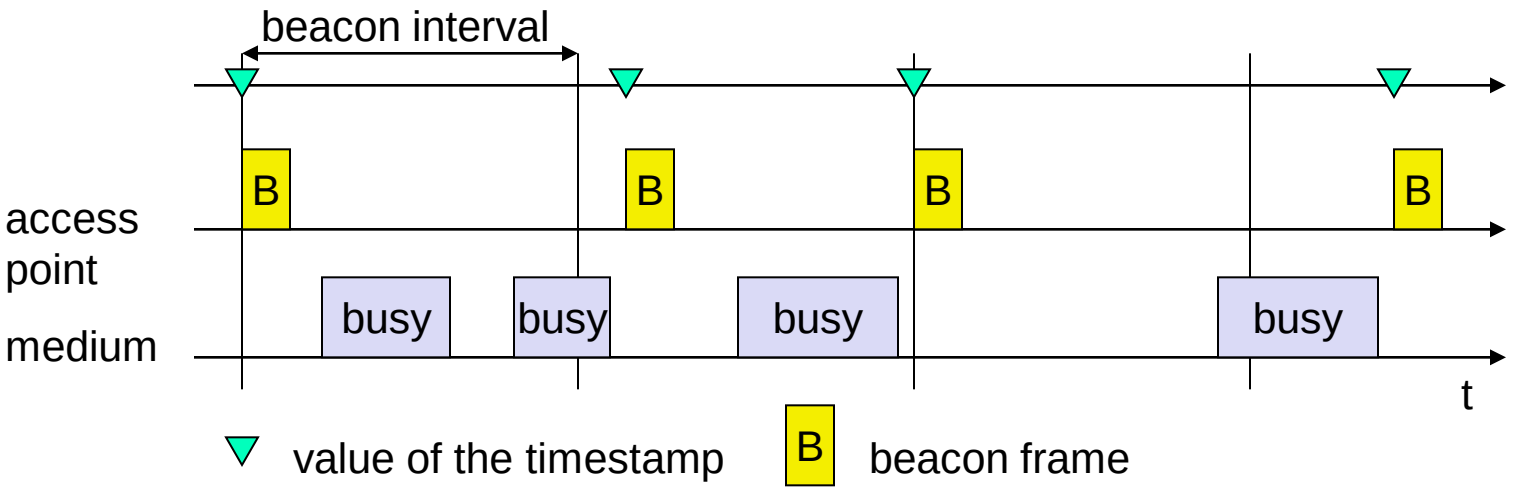
# *MAC Management*




- Synchronization
  - Station discovers a LAN; station associates to an AP
  - stations synchronize clocks; *Beacon is generated by AP*
- Power management
  - Save terminal's power → terminal enters *sleep* mode
    - Periodically
    - No frame loss; frames are stored
- Roaming
  - Station looks for new access points
  - Station decides about best access point
  - Station (re-)associates to new AP
- MIB - Management Information Base

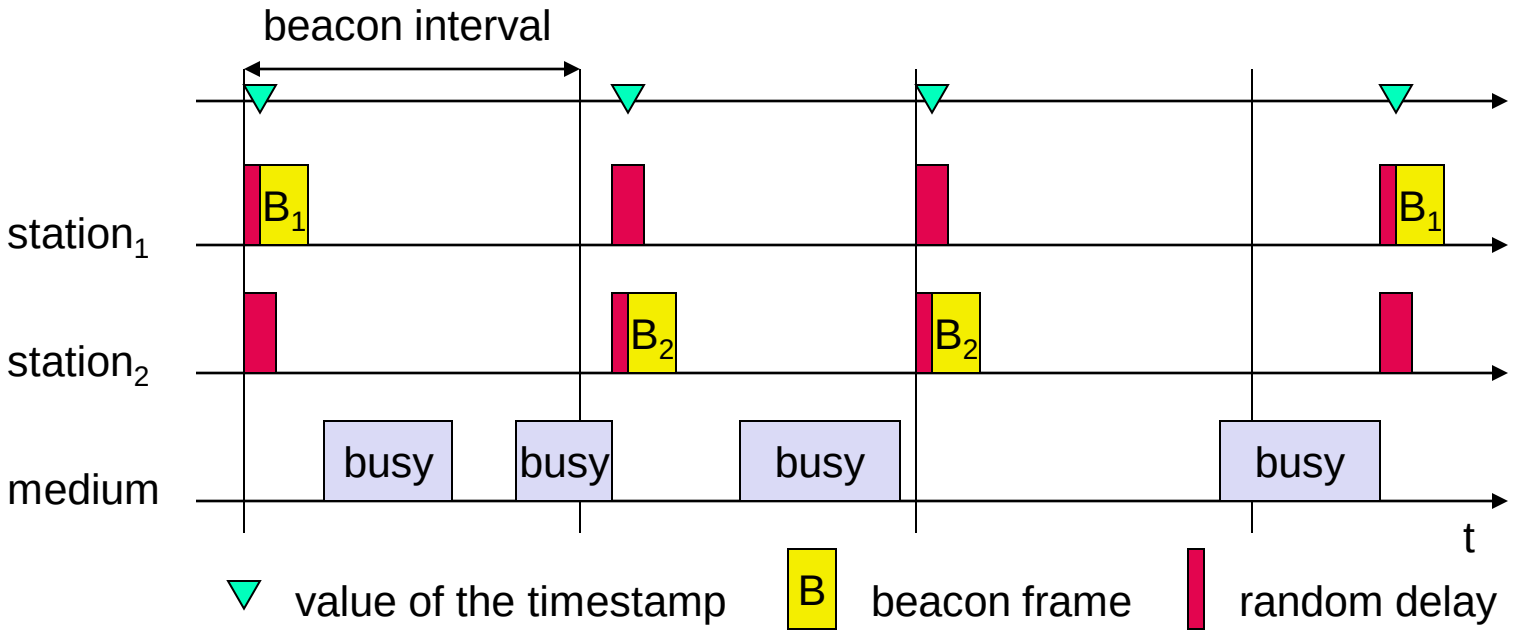
# *Synchronization by Beacon – Infrastructure Network*

- Stations must be synchronised. E.g.
  - To preview PCF cycles
  - To change state: sleep ←→ wake
- Infrastructure networks
  - Access Point sends (almost) periodically a *Beacon* with *timestamp* e *BSSid*
    sometimes medium is busy
  - Timestamp sent is the correct
  - Other stations adjust their clocks



# *Syncronization by Beacon – Ad-hoc Network*

- Every station tries to send a ***beacon***
- Stations use normal method to access the networks → CSMA/CA
- Only one station gains the medium → the others differ attempt to next period

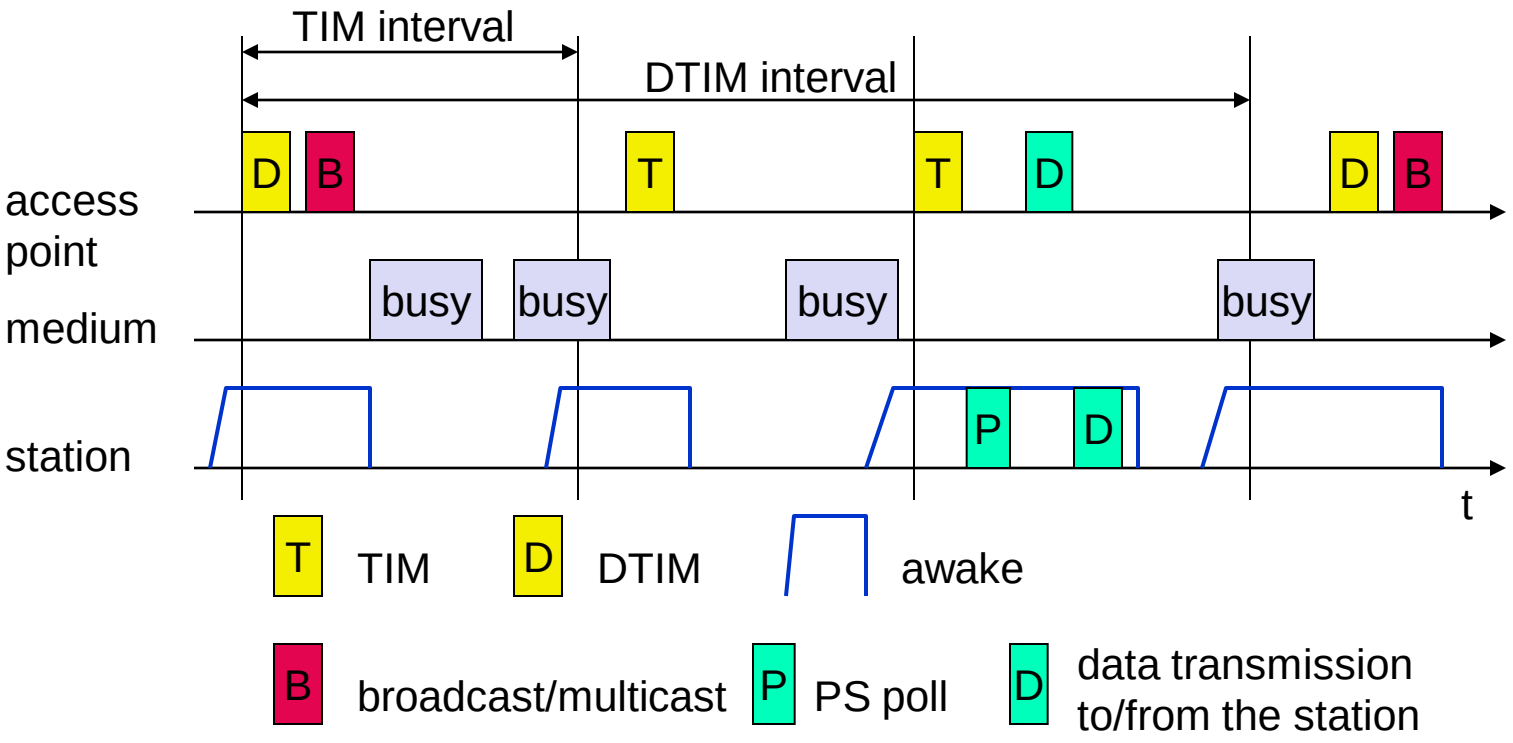


# *Power Management*

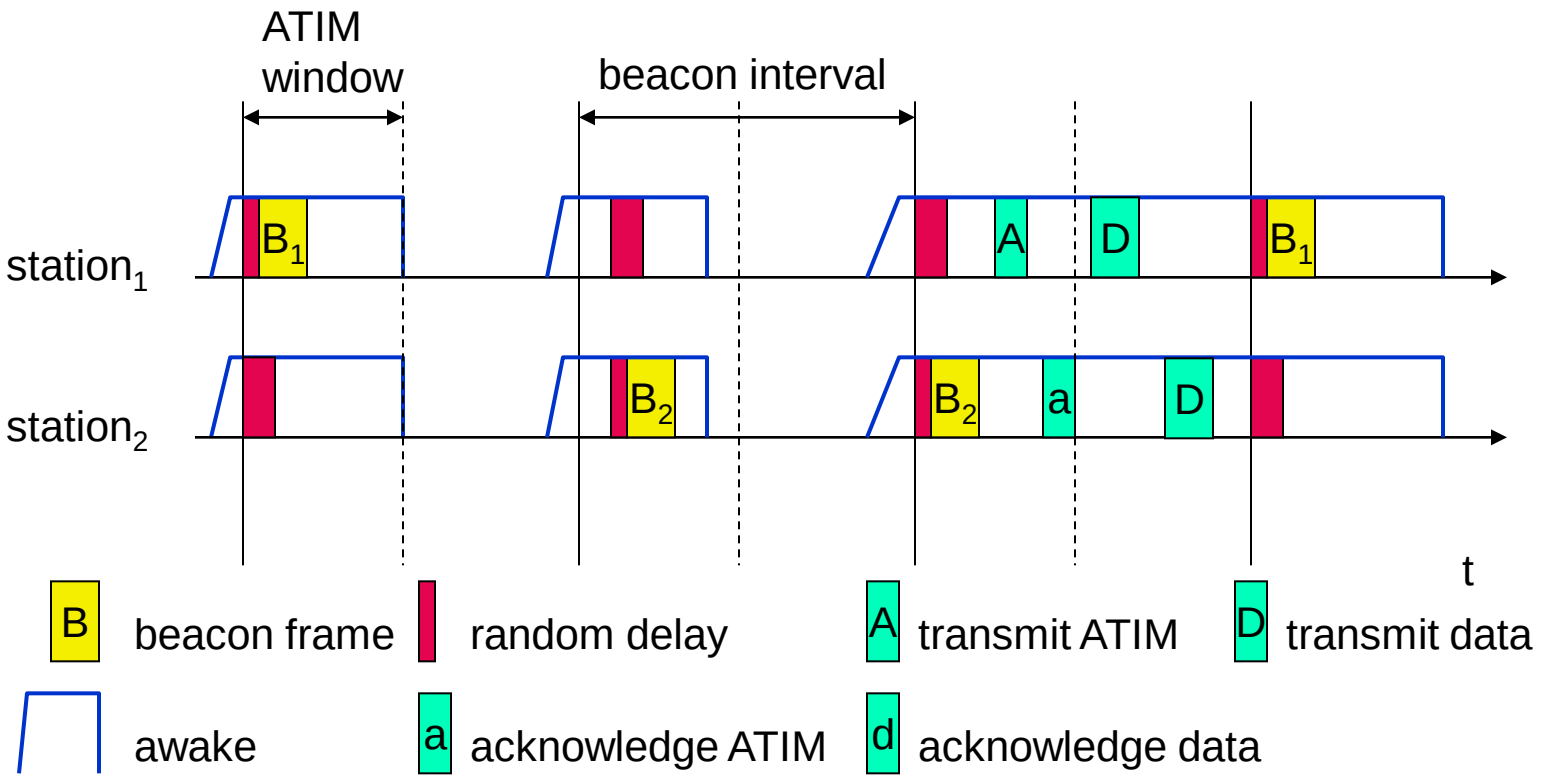
- Objective
  - » If transceiver not in use→ sleep mode
- Station in 2 states: ***sleep***, ***wake***
- Infrastructure network
  - » Stations wake periodically and simultaneously
  - » They listen beacon to know if there are packets to receive
  - » If a station has packets to receive → remains awake until it receives them
    - – If not, go sleep; after sending its packets!
- Ad-hoc network, a station
  - » Listens/sends the beacon
  - » Informs other stations it has packets for them
  - » Receives and sends packets
  - » Sleeps again

# *Power Management – Infrastructure Network*

- Infrastructure network → traffic information sent in the *beacon*
  - » *Traffic Indication Map – TIM:* list of unicast receivers
  - » *Delivery Traffic Indication Map - DTIM:* list broadcast/multicast receivers



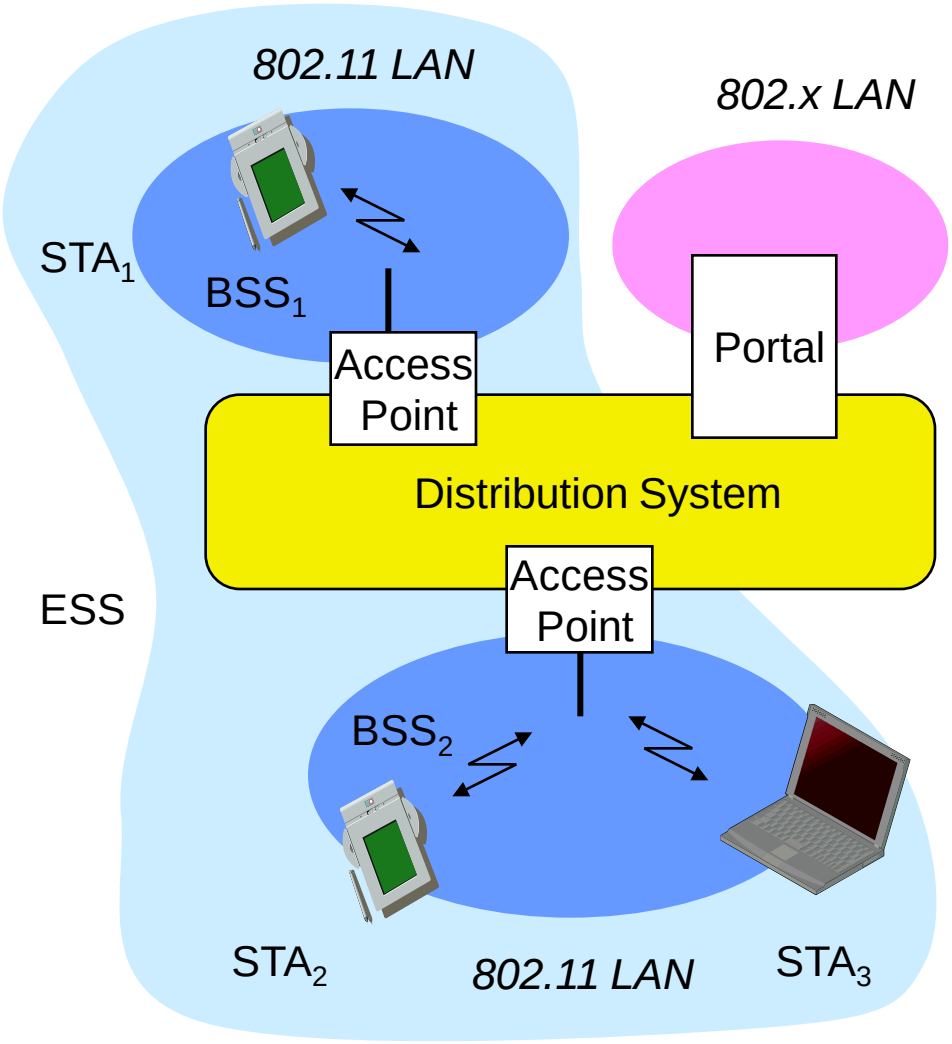
# *Power Management – Ad-hoc Network*



# *(Micro) Mobility*

- Station without link or with bad link? Then:
  - » Monitor the medium
    - Passively → listen to *Beacons*
    - Actively → sending *Probe* message in every channel; waits an answer
  - » Re-association request. Station
    - – Selects best access point (eg., AP with best power received)
    - – Sends Re-association Request to AP
  - » Answer to request
    - – Sucess → AP answered; station can use new AP.
    - – Fail → station continues monitoring
  - » New AP accepts Re-association Request
    - – AP informs distribution system about the new station arrival
    - – Distribution system may inform old AP about the new location of station
    - – 4 addresses used to route traffic

# (Micro) Mobility

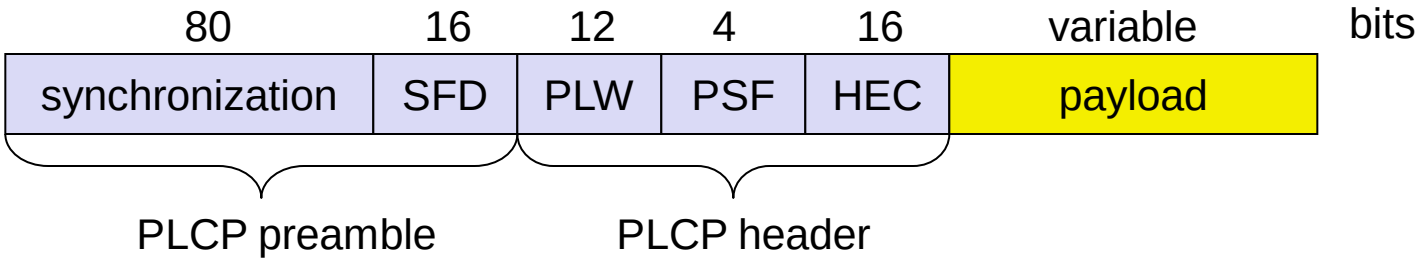


# *802.11 – Nível Físico*

- 3 versões: 2 rádio, 1 IR
  - Bitrates: 1, 2 Mbit/s
- FHSS (Frequency Hopping Spread Spectrum)
  - Spreading, despreading
  - 79 sequências de salto pseudo aleatórias. Para 1 Mbit/s, modulação de 2 níveis GFSK
- DSSS (Direct Sequence Spread Spectrum)
  - 1 Mbit/s → Modulation DBPSK (Differential Binary Phase Shift Keying)
  - 2 Mbit/s → Modulation DQPSK (Differential Quadrature PSK)
  - Preamble and header of frame transmitted at 1 Mbit/s (DBPSK)
    - Remainning transmitted at 1 (DBPSK) ou 2 Mbit/s (DQPSK)
  - Maximum radiated power → 1 W (EUA), 100 mW (UE), min. 1mW
- Infravermelho
  - 850-950 nm, distância de 10 m
  - Detecção de portadora, detecção de energia, sincronização
- All versions provide ***Clear Channel Assessment (CCA)***
  - Used by MAC to detect if medium is free

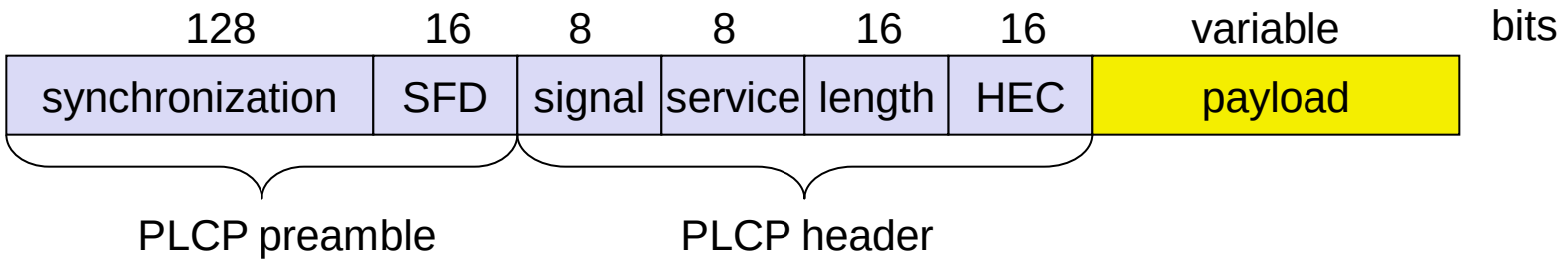
# *Frame FHSS PHY*

- Sincronization → 010101...
- SFD (Start Frame Delimiter → 0000110010111101
- PLW (PLCP_PDU Length Word)
  - Payload length in bytes, including 2 CRC bytes. PLW < 4096
- PSF (PLCP Signaling Field)
  - Transmission bitrate of payload (1, 2 Mbit/s)
    - PLCP (preâmbulo and header) sent at 1 Mbit/s
    - Payload sent at 1 ou 2 Mbit/s
- HEC (Header Error Check)
  - CRC with $x^{16}+x^{12}+x^5+1$
- Data MAC → scrambled with $z^7+z^4+1$



# *Frame DSSS PHY*

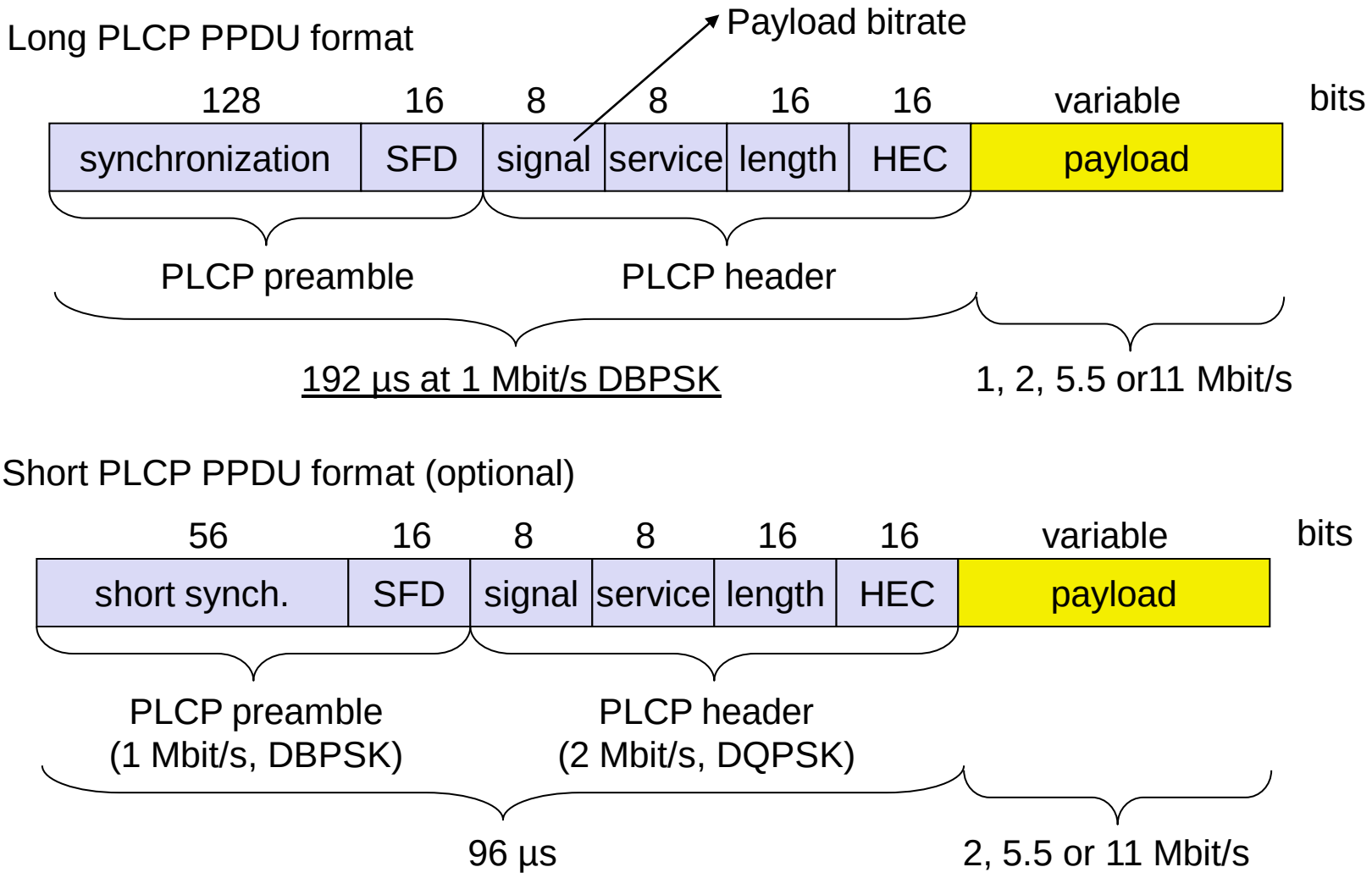
- Barker sequence of 11 chips → +1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1
- Sincronization
  - Sincronization
  - Gain control, Clear Channel Assessement, compensate frequency deviation
- SFD (Start Frame Delimiter → 1111001110100000
- Signal
  - Payload bitrate (0A: 1 Mbit/s DBPSK; 14: 2 Mbit/s DQPSK)
- Service → utilização futura, 00 = conforme 802.11
- Length → Payload length **in us**
- HEC (Header Error Check)
  - Protection of sinal, service and length, using $x^{16}+x^{12}+x^5+1$
- Data (payload) MAC → scrambled with $z^7+z^4+1$



# *IEEE 802.11b*

- Bitrate (Mbit/s)
  - 1, 2, 5.5, 11 (depends on SNR)
  - Useful bitrate → 6
- Transmission range
  - 300m outdoor, 30m indoor
- Frequencies → open, ISM 2.4 GHz band
- Only physical layer is redefined
  - » MAC and MAC management are the same

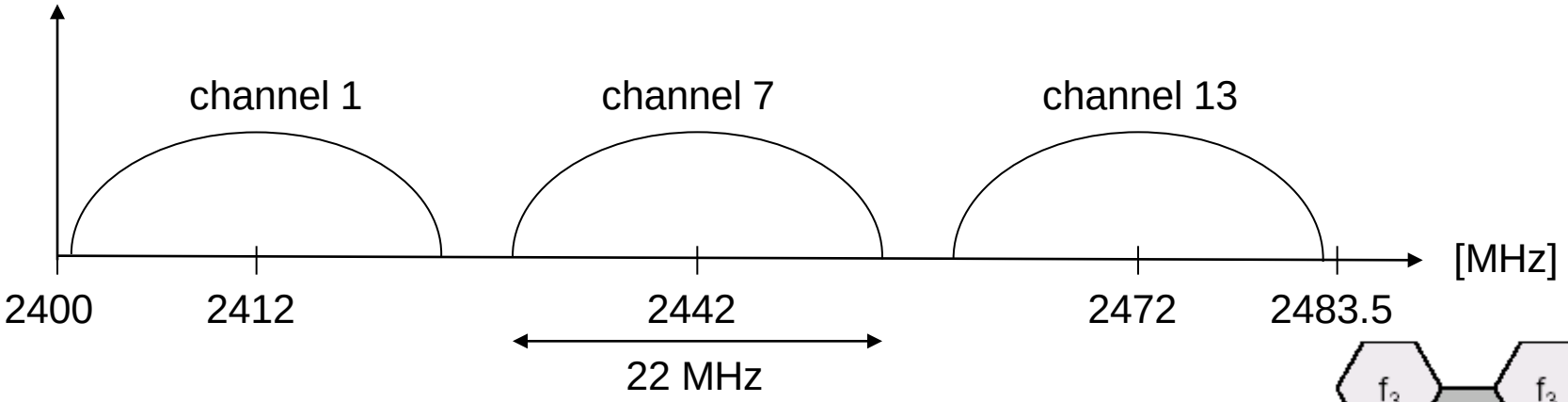
# *IEEE 802.11b – Trama PHY*



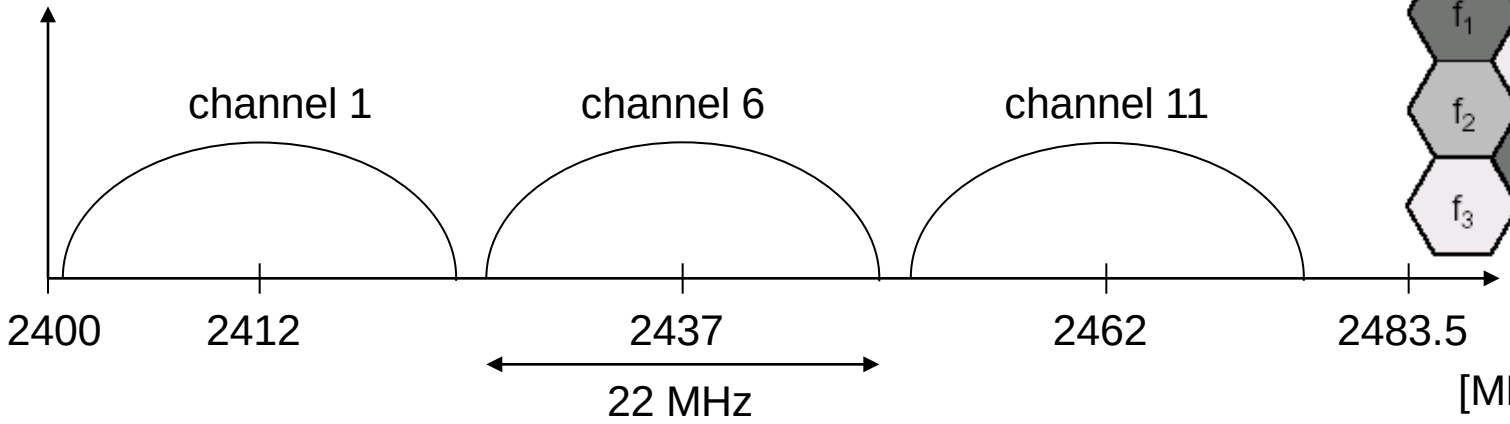
# *Channel Selection*

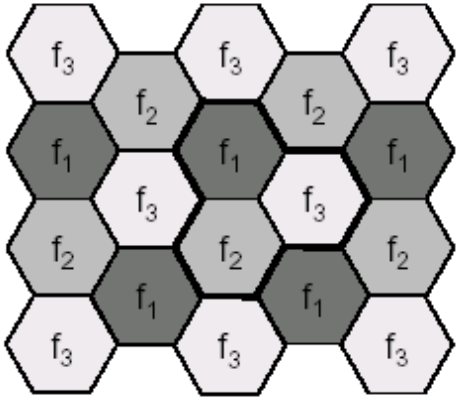
channel i = 2412MHz + (i-1)*5MHz
There are 14 channels of 5MHz
In 801.11b only 3 non-overlap channels can be used

Europe (ETSI)




US (FCC)/Canada (IC)

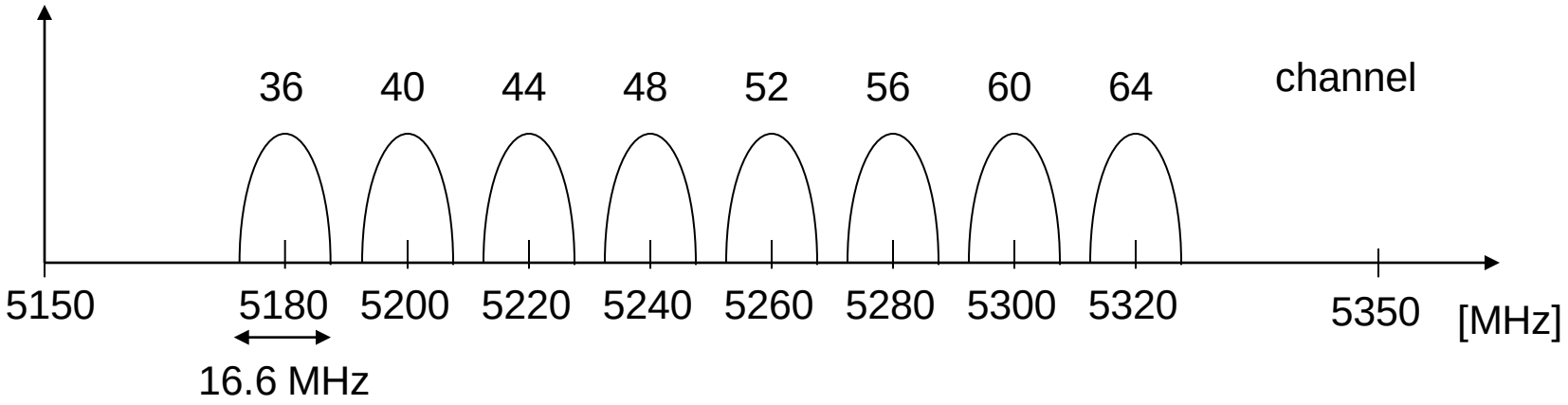


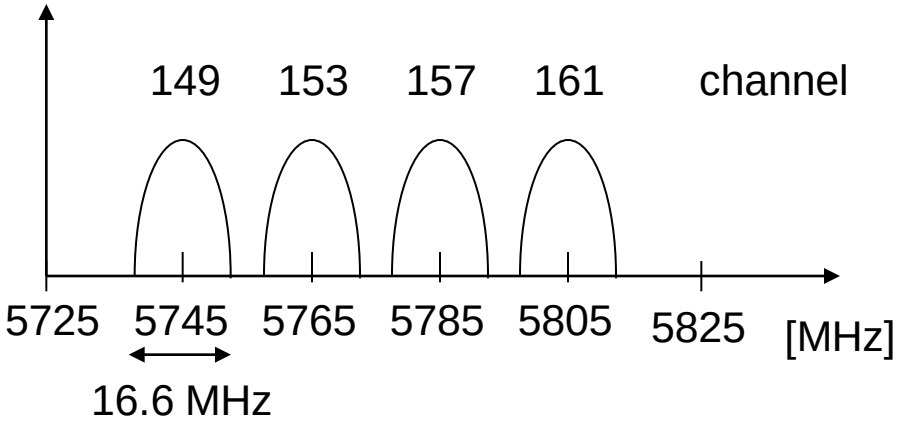



# *IEEE 802.11a*

- Bitrate (Mbit/s)
  - » 6, 9, 12, 18, 24, 36, 48, 54 (depends on SNR)
  - » Mandatory → 6, 12, 24
- Useful bit rate (frames 1500 bytes, Mbit/s)
  - » 5.3 (6), 18 (24), 24 (36), 32 (54)
- Transmission range
  - » 100m outdoor, 10 m indoor
    - – 54 Mbit/s até 5 m, 48 até 12 m, 36 até 25 m, 24 até 30m, 18 até 40 m, 12 até 60 m
- Frequencies
  - » Free, band ISM
  - » 5.15-5.35, 5.47-5.725 GHz (Europa)
- Only the physical layer changes

# *Operating channels for 802.11a / US U-NII*

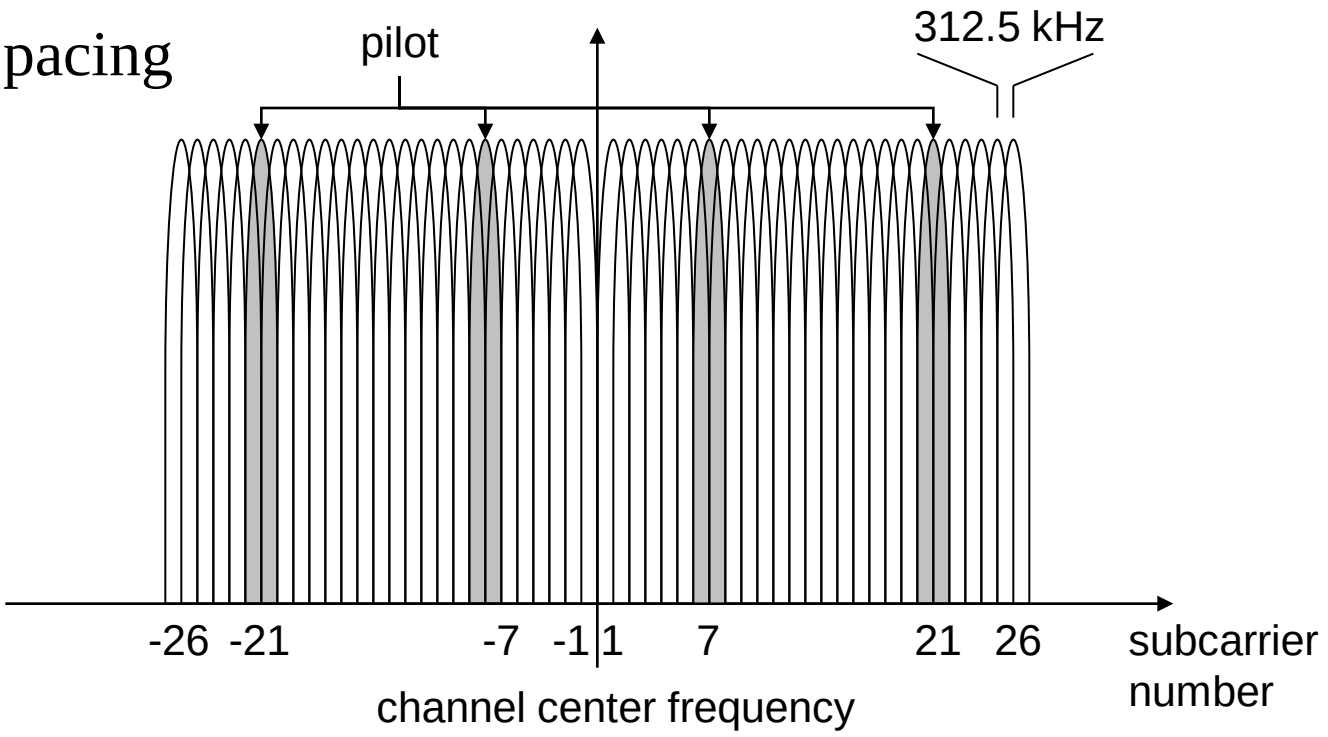



center frequency =
5000 + 5*channel number [MHz]

# *OFDM in IEEE 802.11a*

- OFDM with 52 used subcarriers (64 in total)
- 48 data + 4 pilot
- (plus 12 virtual subcarriers)
- 312.5 kHz spacing



Percebem a tabela!

# 802.11a – Rate Dependent Parameters

| Data rate (Mbits/s) | Modulation | Coding rate (R) | Coded bits per subcarrier ($N_{BPSC}$) | Coded bits per OFDM symbol ($N_{CBPS}$) | Data bits per OFDM symbol ($N_{DBPS}$) |
|---|---|---|---|---|---|
| 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 |

*% of useful information*

*250 kSymbol/s*

# *Homework*

- How is the bitrate of 24 Mbit/s obtained in 802.11a?
  - » Explain it by using the values given in the Table of previous slide.
  - » Keep in mind the symbol rate of 250 kSymbol/s

| Data rate (Mbits/s) | Modulation | Coding rate (R) | Coded bits per subcarrier ($N_{BPSC}$) | Coded bits per OFDM symbol ($N_{CBPS}$) | Data bits per OFDM symbol ($N_{DBPS}$) |
|---|---|---|---|---|---|
| 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 |

- How does 802.11n work?

**Short answers emailed to (mricardo@fe.up.pt) before the next lecture.**