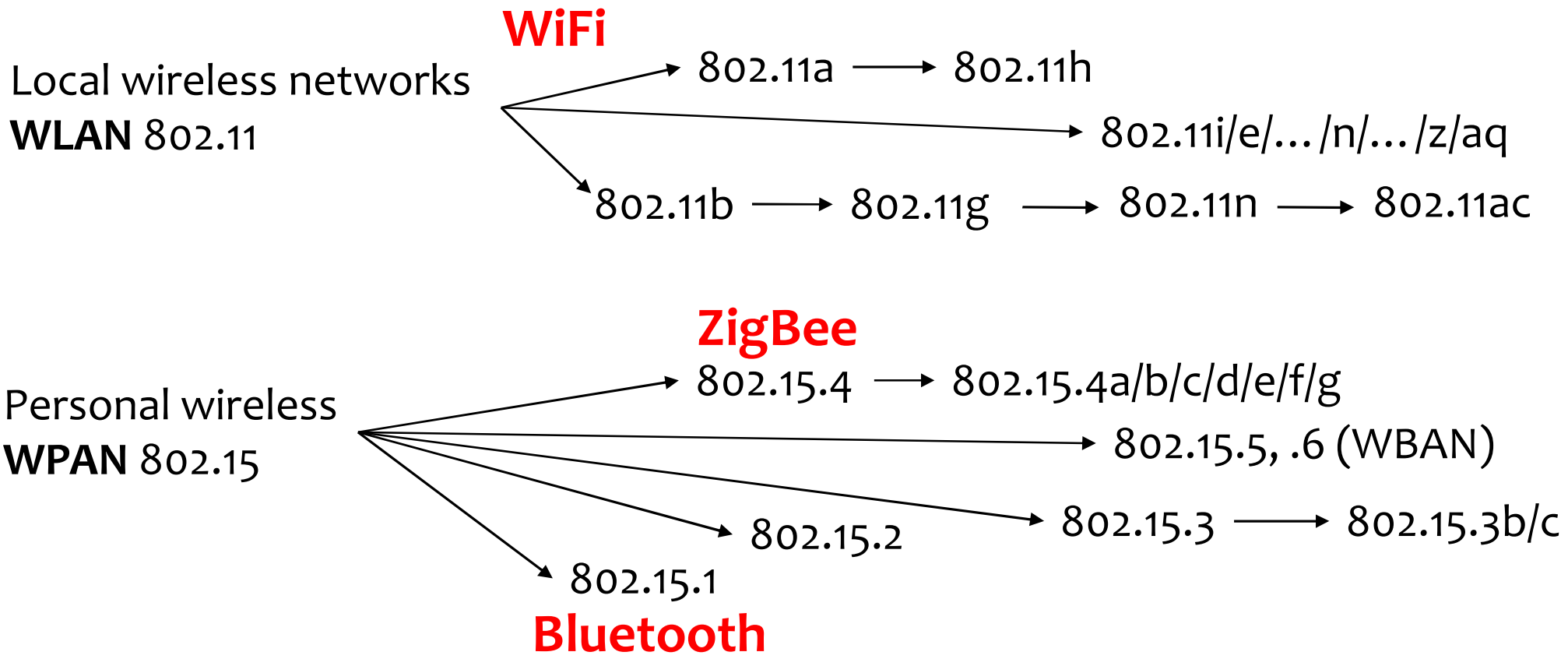
Rețele locale fără fir (Wireless LANs)

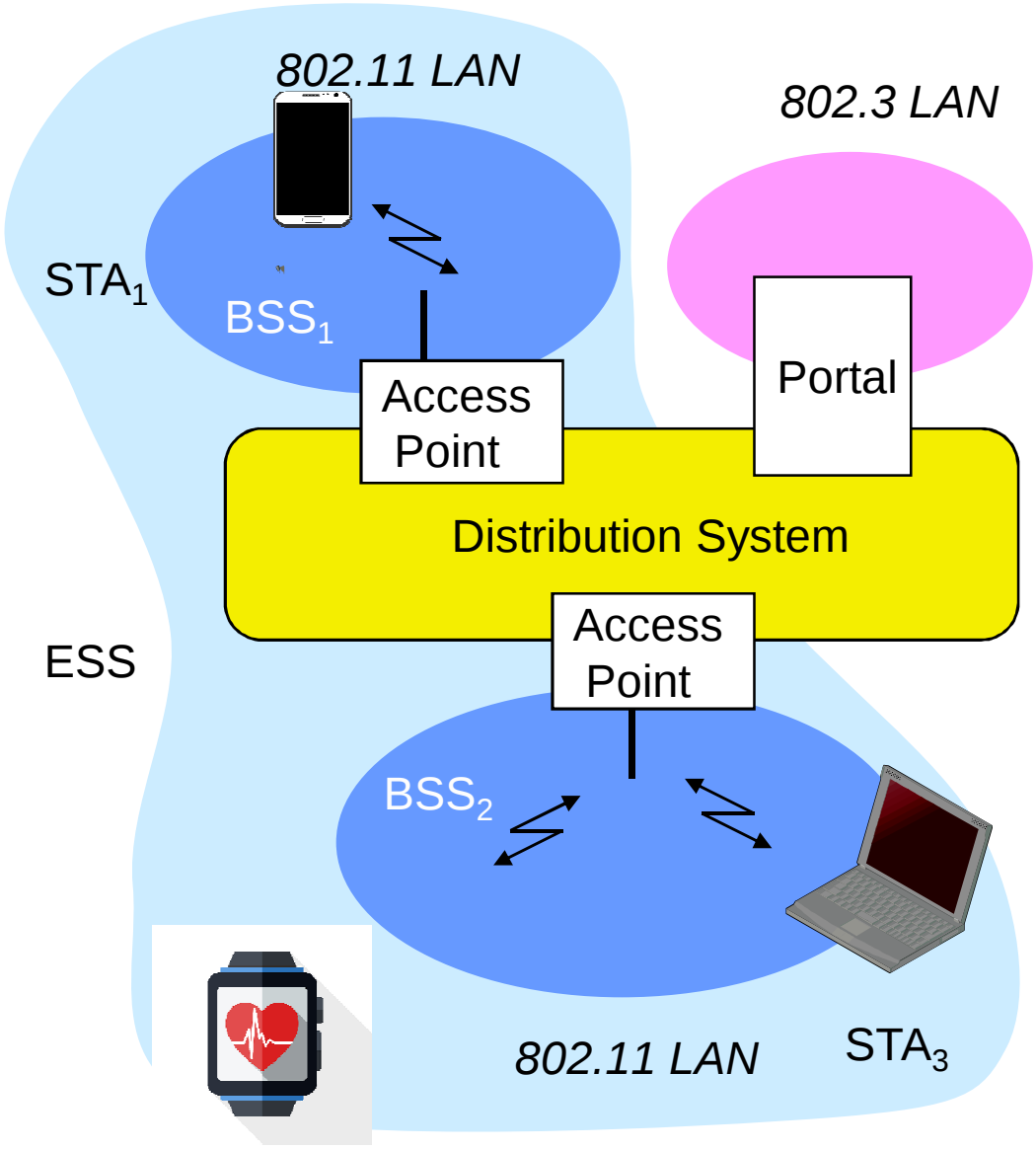
Cuprins

- organizare, standarde
- nivelul fizic
  - » 802.11b, 802.11a, 802.11g, 802.11n, ac
- nivelul legatura de date
  - » CSMA/CA, Schimbul de cadre
  - » powersave, handover
- Ce urmează
  - 802.11ad

Standarde comunicații mobile IEEE

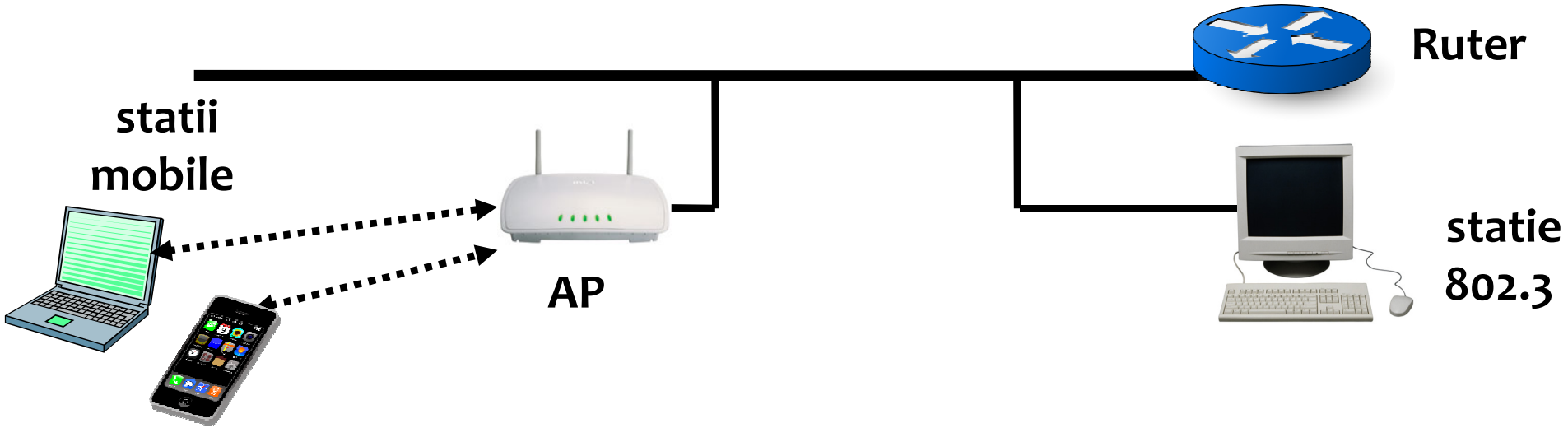


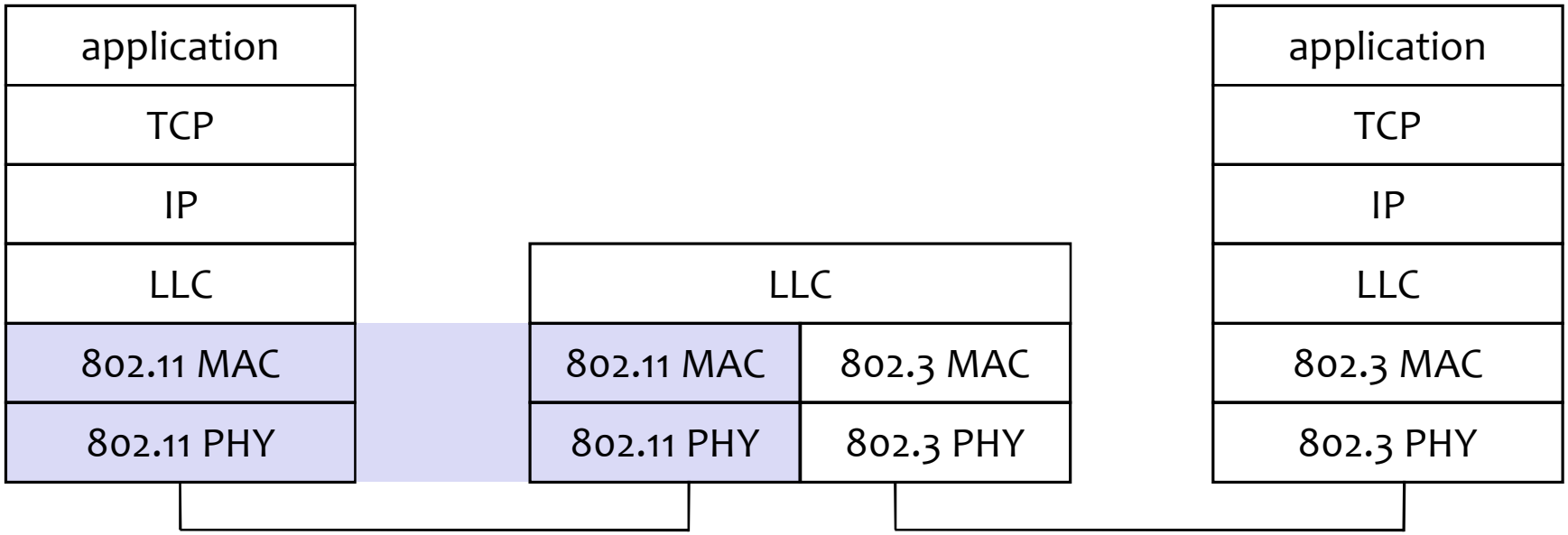
802.11 - infrastructure network



- **Station (STA)**
  - **telefon, laptop, dispozitiv IoT**
- **Basic Service Set (BSS)**
  - **Stații și AP-ul lor curent**
- **Access Point**
  - **Stație wireless LAN + distribution system**
- **Portal**
  - **bridge către alte rețele wired**
- **Distribution System**
  - **Interconectare între AP-uri: Ethernet**
- **ESS**
  - **Mai multe BSS-uri**

exemplu 802.11 + 802.3





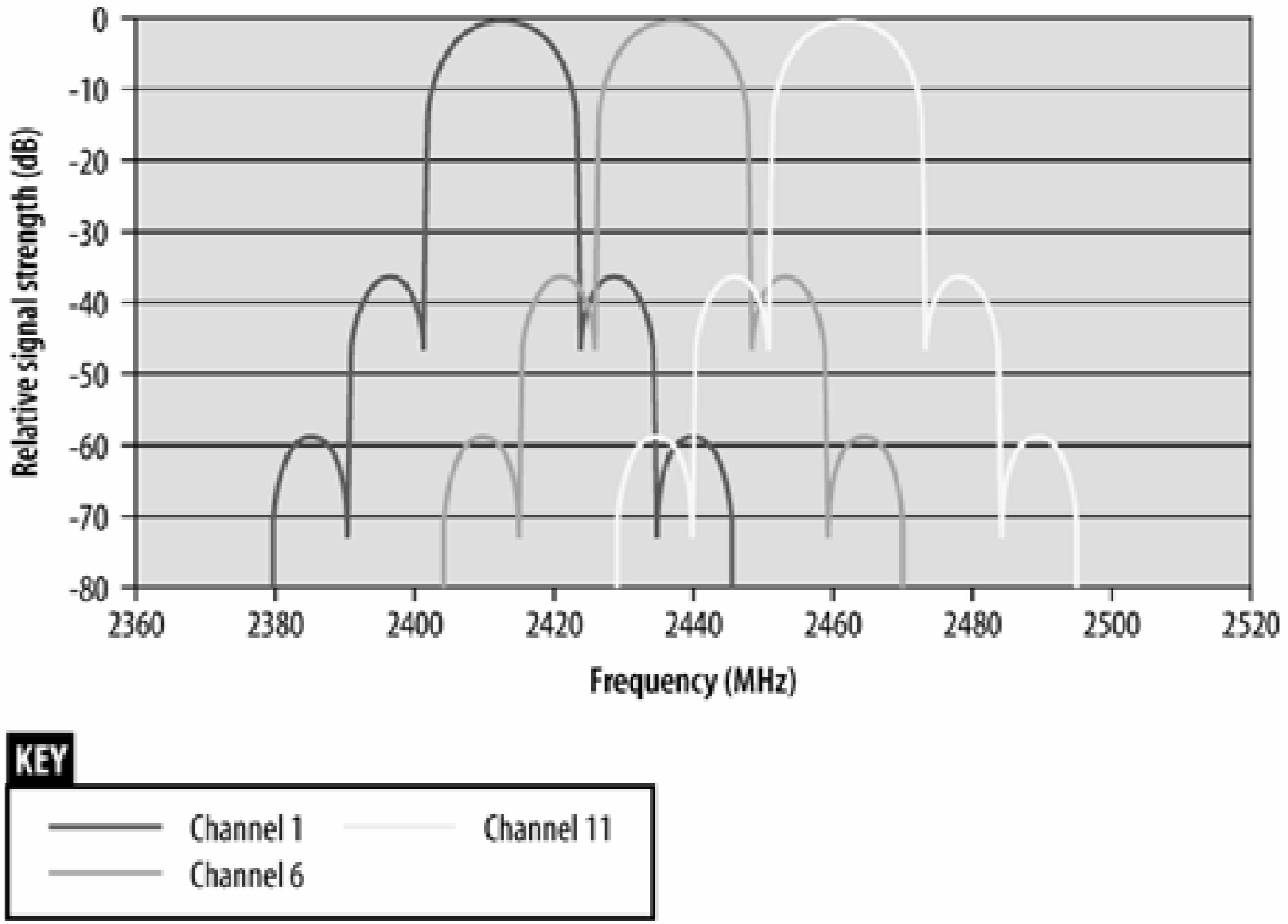
nivelul fizic (L1)

802.11 în 2.4GHz

- **Frecvențe fara licență ISM (industrial științific medical) 2.4GHz**
- **Un canal** $f_{sus} - f_{jos} =$ **22 MHz**
- **3 canale independente**

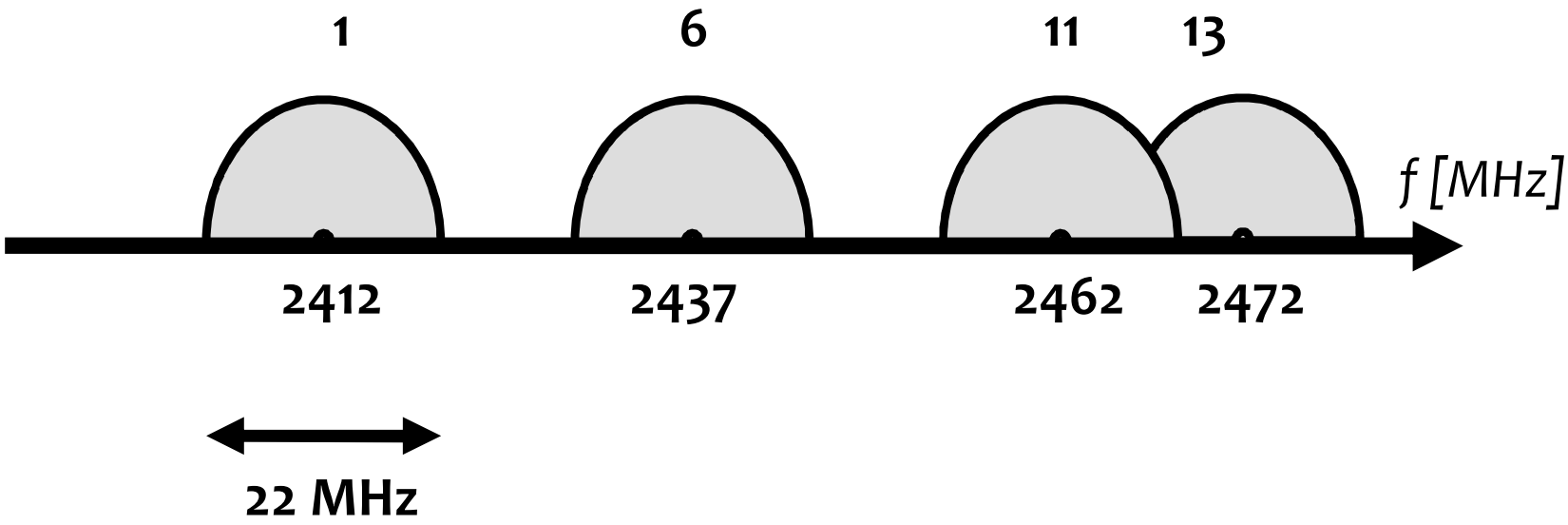
canal	f_{jos}	f_{sus}
1	2.401	2.423
2	2.404	2.428
3	2.411	2.433
4	2.416	2.438
5	2.421	2.443
6	2.426	2.448
7	2.431	2.453
8	2.436	2.458
9	2.441	2.463
10	2.446	2.468
11	2.451	2.473
12		
13		

Benzile 2.4GHz (11b, 11g, 11n)



Dispunerea canalelor în 2.4GHz

Europa: 1-13 **SUA/Canada 1-11**

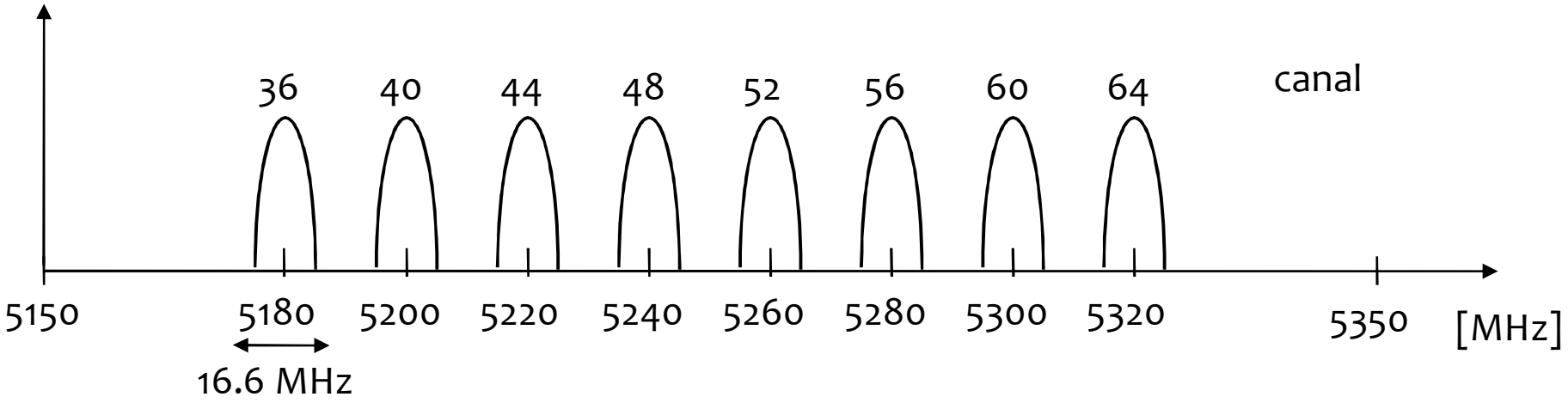


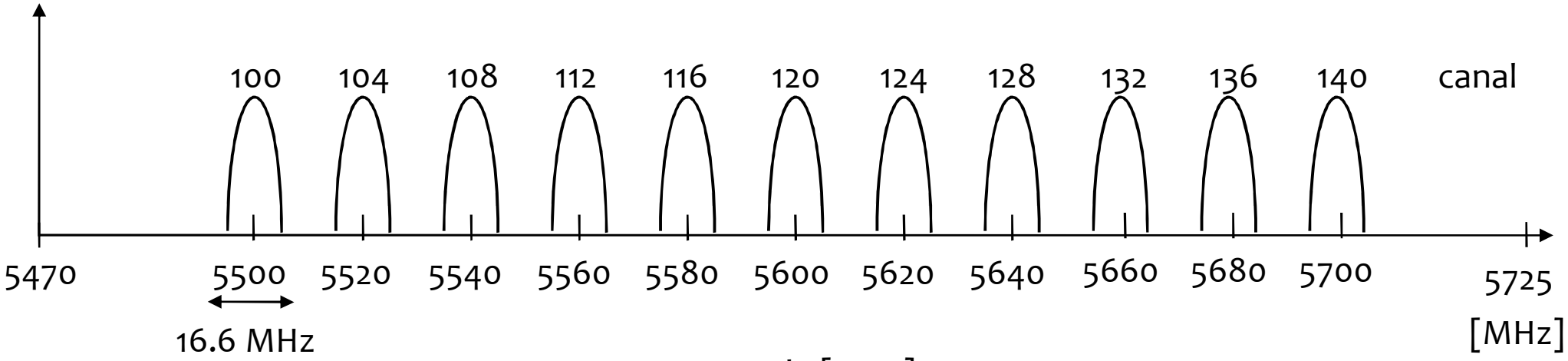
Caracteristici 802.11b

- MCS
  - » 1, 2, 5.5, 11 Mbps, depinde de SNR
  - » rata maxima la utilizator 6.3Mbps
- Aria de transmisie
  - » 150m exterior, 50m interior
- Frecventa
  - » 2.4 GHz
- Securitate
  - » limitata, WEP, SSID
- Avantaje:
- Disponibilitate:
  - multe produse,
  - experienta tehnica,
- frecventa fara licenta,
- Multi producatori,
  - integrat in portabile, telefoane,
  - Preț scazut

- Dezavantaje:
  - » Interferență
  - » QoS Inexistent,
    - » “best effort”, fără garanții
    - » viteză redusă
  - » Gestiune limitată
    - » nu există distribuție de chei,
    - » criptare simetrică

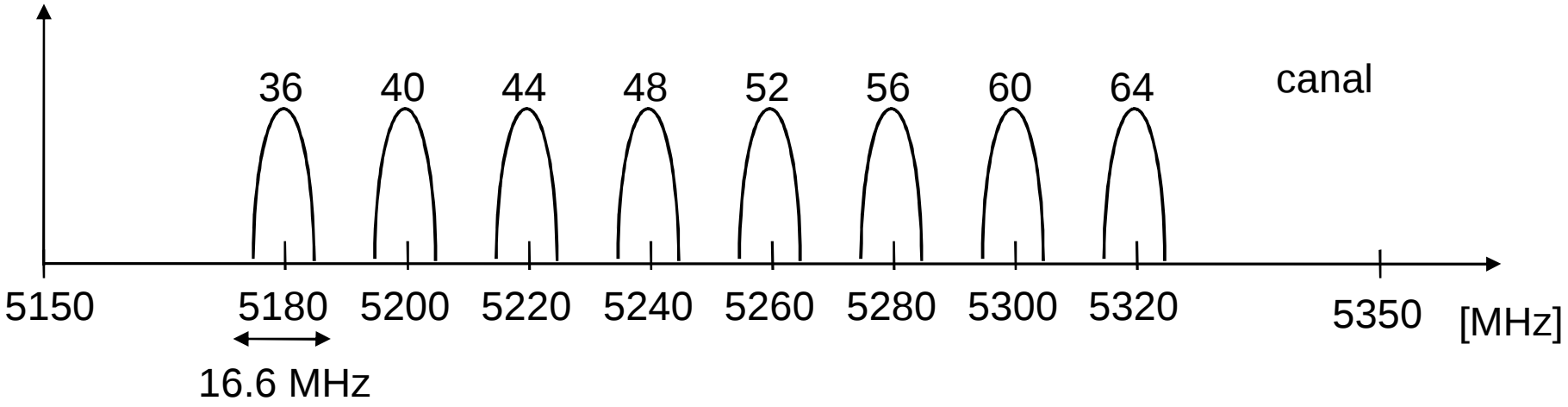
Canale 802.11a (Europa)

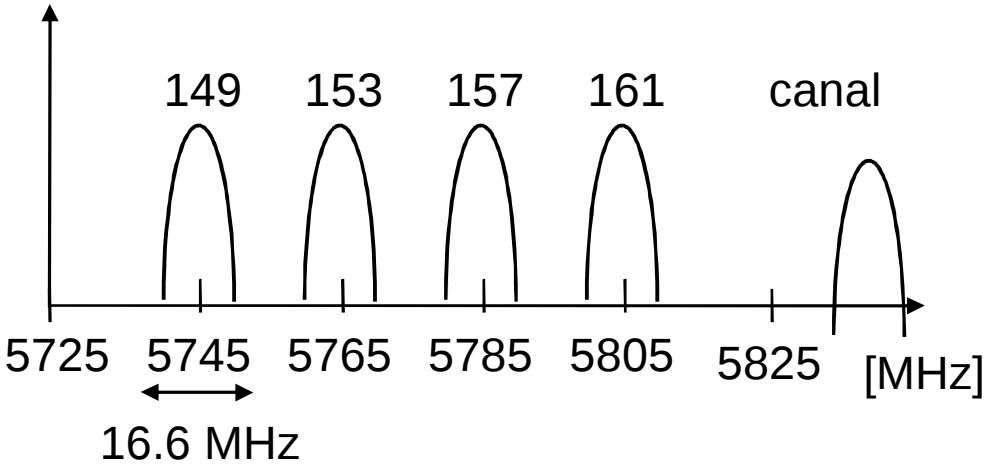




Frecventa centrala [MHz] =
5000 + 5*numar canal

Canale 802.11a (SUA/Canada)





Frecventa centrala [MHz] =
5000 + 5*canal

Caracteristici 802.11a

- MCS
  - » 6, 9, 12, 18, 24, 36, 48, 54 Mbps, in functie de SNR
  - » Rata la utilizator (pachete mari): 5.3 (6), 18 (24), 24 (36), 32 (54)
  - » 6, 12, 24 Mbps obligatorii
- Aria de transmisie
  - » 100m exterior, 30m interior
- Frecvente
  - » 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz, canale: 12 (SUA), 19 (Euro)
  - » OFDM + DBPSK/DQPSK/QAM
- Security
  - » WEP, WPA, SSID

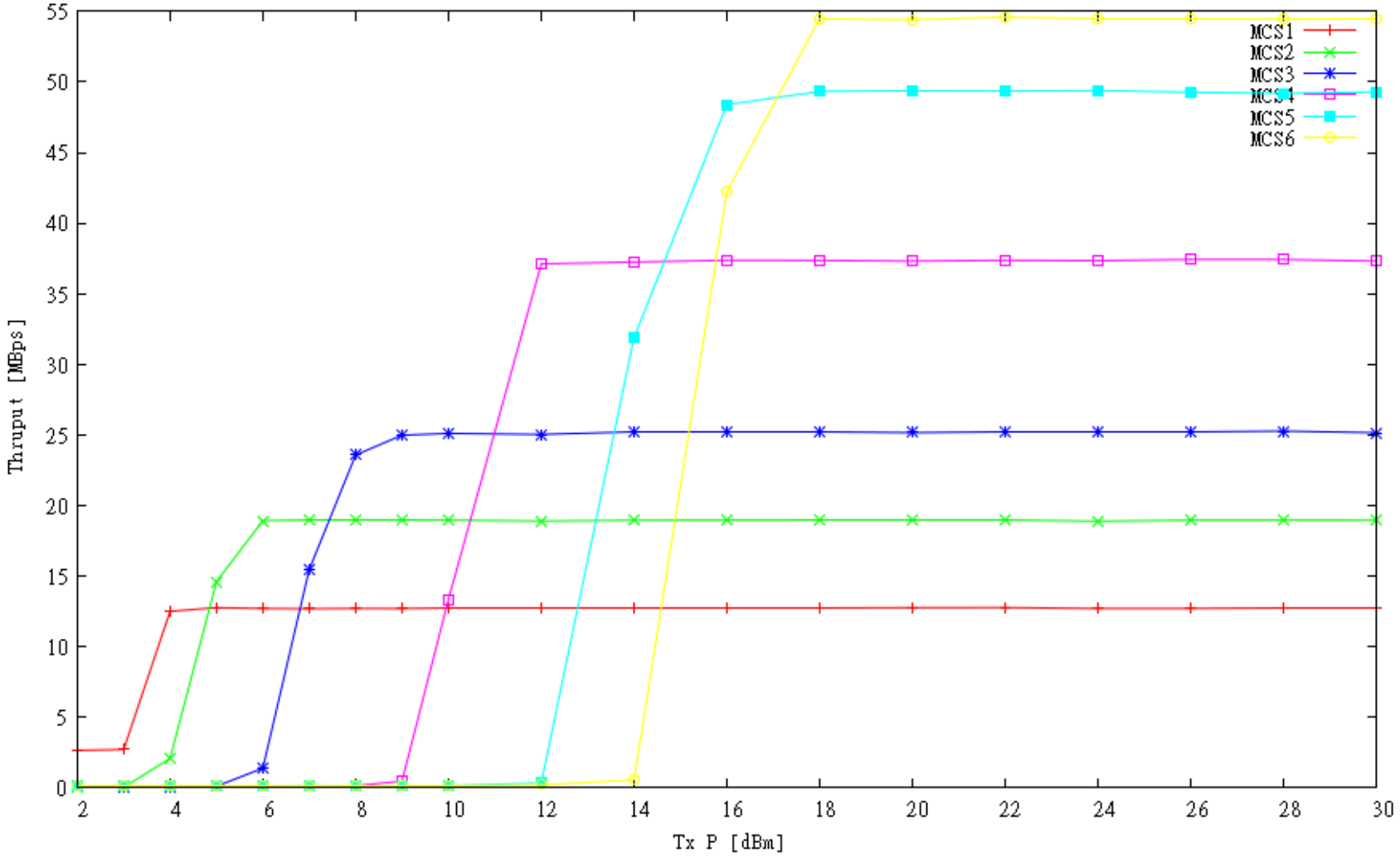
- Avantaje:
  - » frecventa fara licenta
  - » interferenta redusa
  - » pret scazut

- Dezavantaje:
  - disponibilitate < 802.11 b & g
  - » propagare redusa (5GHz)
  - » QoS Inexistent,
    - » best effort
    - » fara garantii
  - » Gestiune limitata

MCS – puterea necesară

Măsurători în UPB Leu corp A, 5.7GHz distanța 10m MCS=1-6:

MCS cu rată mare necesită putere mare



Propagare 802.11a

- De ce propagarea este mai slabă la 5GHz?

Free Space Loss = $(4pdf/c)^n$

d = distanța

f = frecvența purtătoarei

n = exponent

mediu	n	propagare
coridoare	1.4 – 1.9	ghid undă
Camere mari, libere	2	free space loss
Camere cu mobilă	3	FSL + multicăi
Camere încărcate	4	non LOS, difracție, împrăștiere
Între etaje	5	traversare podele, pereți

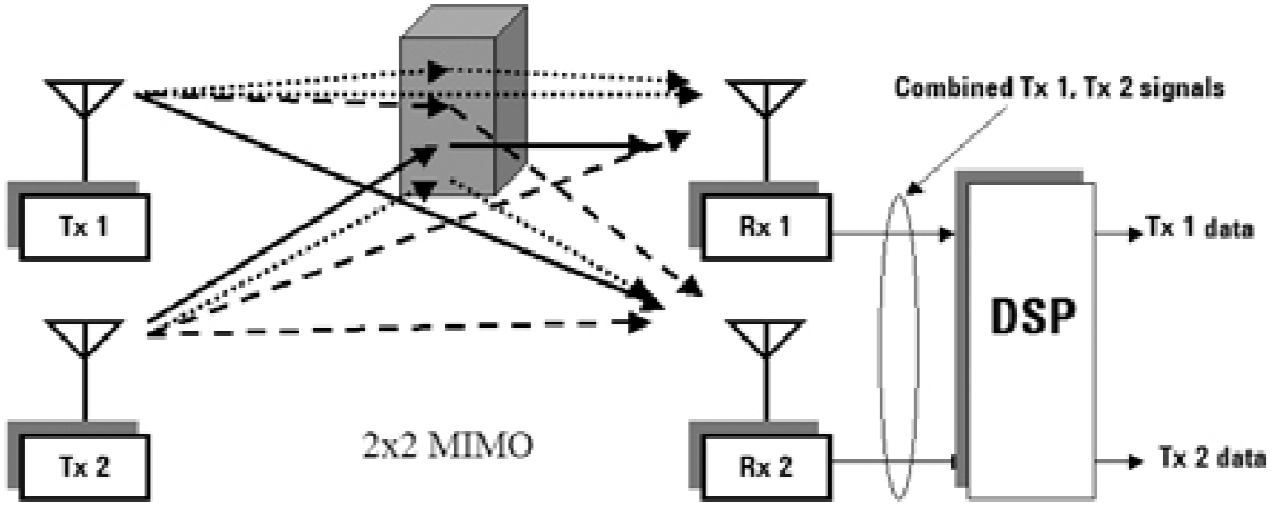
802.11g

- 802.11g : Similar cu 802.11a, dar compatibil cu 802.11b
  - 2.4GHz
  - Rate(MCS) 11b 1, 2, 5.5, 11 Mbps
  - Rate(MCS) 11g cu OFDM – 6, 9, 12, 18, 24, 36, 54 Mbps

802.11n(2009)

- 2.4GHz și 5GHz, backward compatible cu a/b/g
  - Metode de coexistență cu dispozitivele vechi

- MIMO = Multiple Input Multiple Output
  - max 4 antene
  - Max 600Mbps



- Canale de 40Mhz
  - Ocupă 80% din spectrul 2.4GHz
- Agregare de cadre
  - Block acknowledgement
- Distanțe crescute: 70m interior

802.11n throughput

- Canal de 40MHz
  - Greenfield mode: doar în absența 11g
  - alipirea a 2 canale vecine (1+6 sau 6+11)

- Cum se obțin 600Mbps?
  - 1 stream, 20MHz = 72.2Mbps
  - 1 stream, 40MHz = 150Mbps
  - 2 stream, 20MHz = 144.4Mbps
  - …
  - 4 stream, 40MHz = 600Mbps

802.11ac(2014)

- Doar 5GHz
- Compatibil cu 11a și 11n
- Obligatoriu 80MHz, opțional 160MHz
- Maximum 8 fluxuri spațiale
- 1 flux, 80MHz, 64QAM => 293Mbps (obligatoriu)
- 8 fluxuri, 160MHz, 256QAM => 3.5Gbps (maximum)

802.11ac

- Banda pâna la 160 MHz (80 MHz obligatoriu), 8x MIMO, beamforming
- Exemplu configurație home:
  - 8-antenna access point, 160 MHz bandwidth, 6.77 Gbit/s
  - 4-antenna digital TV, 3.39 Gbit/s
  - 2-antenna tablet, 1.69 Gbit/s
  - Two 1-antenna smartphones, 867 Mbit/s each

Canale alipite în 802.11ac

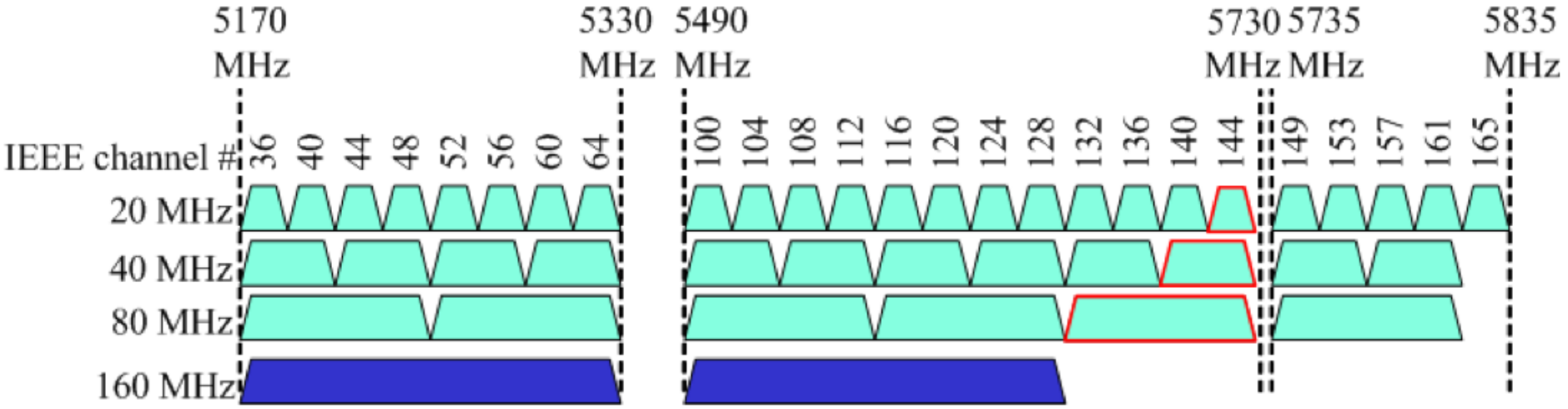


Figure 1: US and Global Operating Class Channel Allocation

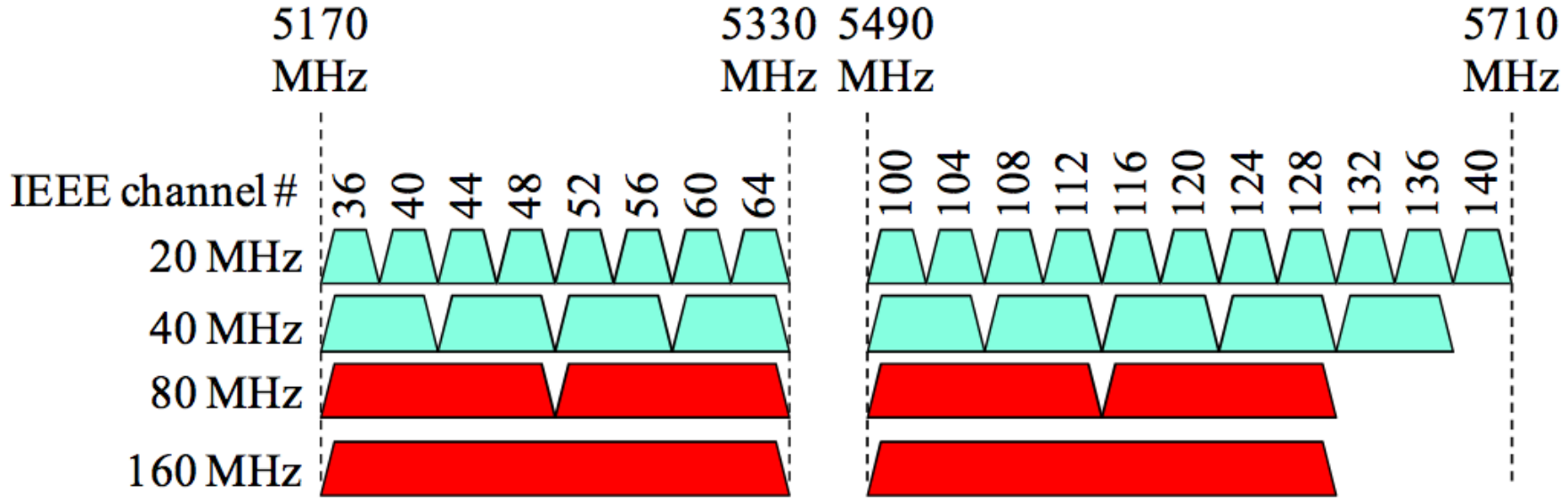


Figure 2: Europe and Japan Class Channel Allocation

Nivelul access la mediu

Carrier Sense

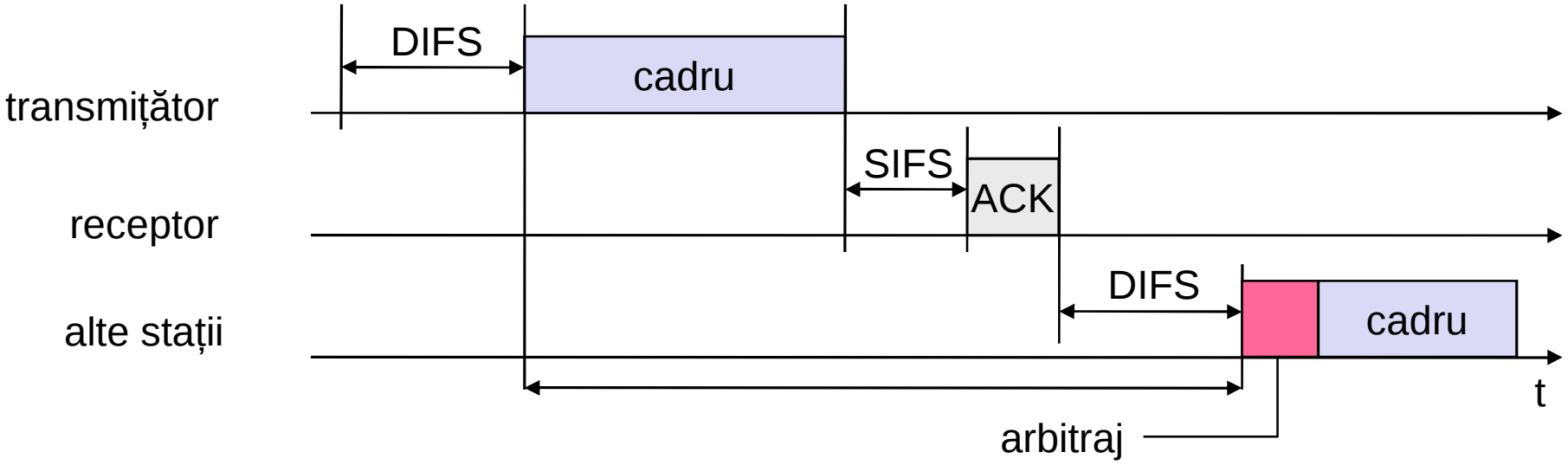
- Daca mediul este ocupat, se amână transmisia
- Analogie: discuții la petrecere
- Virtual
  - » NAV = network allocation vector
  - » Fiecare stație asculta indicațiile de temporizare din toate cadrele
- Fizic
  - » Se detecteaza prezenta purtatoarei unei alte stații
  - » Depinde de implementare => prag (decibeli)

802.11 MAC

- Acronime
  - » DCF (Distributed Coordination Function) - acces asincron
  - » PCF (Point Coordination Function) - acces sincron
  - » CSMA/CA - carrier sense multiple access, collision avoidance
- Metode de acces
  - » DCF + CSMA/CA (obligatoriu)
    - – politica de tip “best-effort”
    - – broadcast and multicast
    - – Evitarea coliziunilor (CA) prin „back-off“randomizat
    - – Distanta minima intre pachete consecutive
    - – ACK
  - » DCF + RTS/CTS (optional, dar implementat)
    - – minimizeaza terminalele ascunse

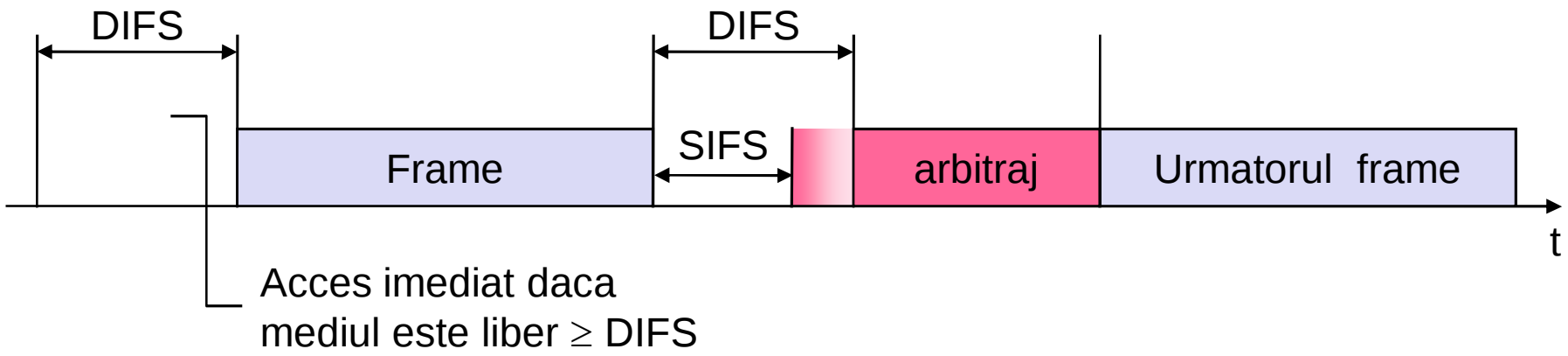
802.11 date unicast

- transmitatorul asteapta DIFS inainte de transmisie
- receptorul asteapta SIFS, trimite ACK pentru cadre corecte (CRC)
- retransmisie automată a frame-urilor care nu primesc ACK



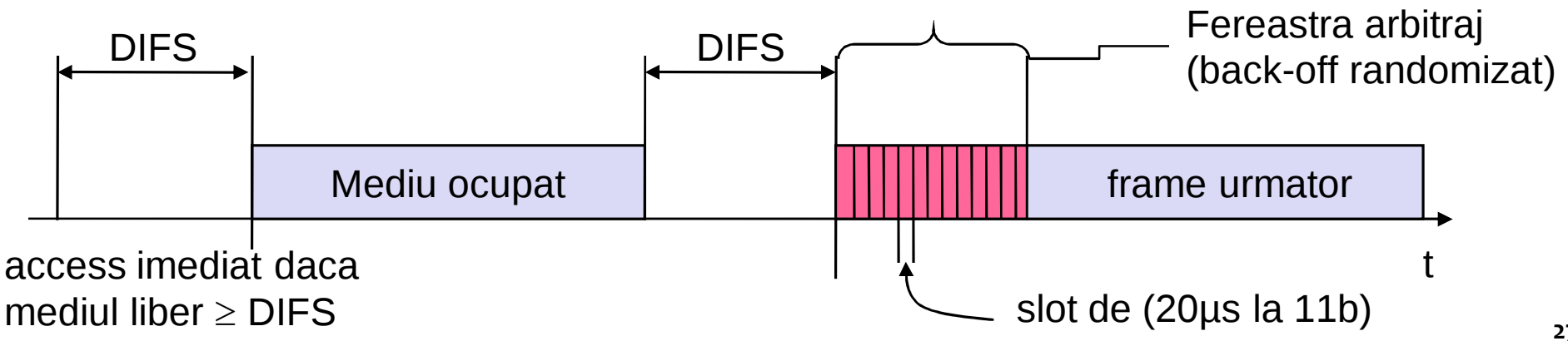
802.11 date unicast

- IFS - inter frame space
- Priorități
  - » definite prin folosirea IFS diferite
  - » nu sunt garantate
  - » SIFS (Short IFS) = 10us pt 11b
    - – prioritate mare: ACK, CTS, raspuns polling response
  - » DIFS (DCF IFS) = 50us pt 11b
    - – prioritate redusa, pentru date

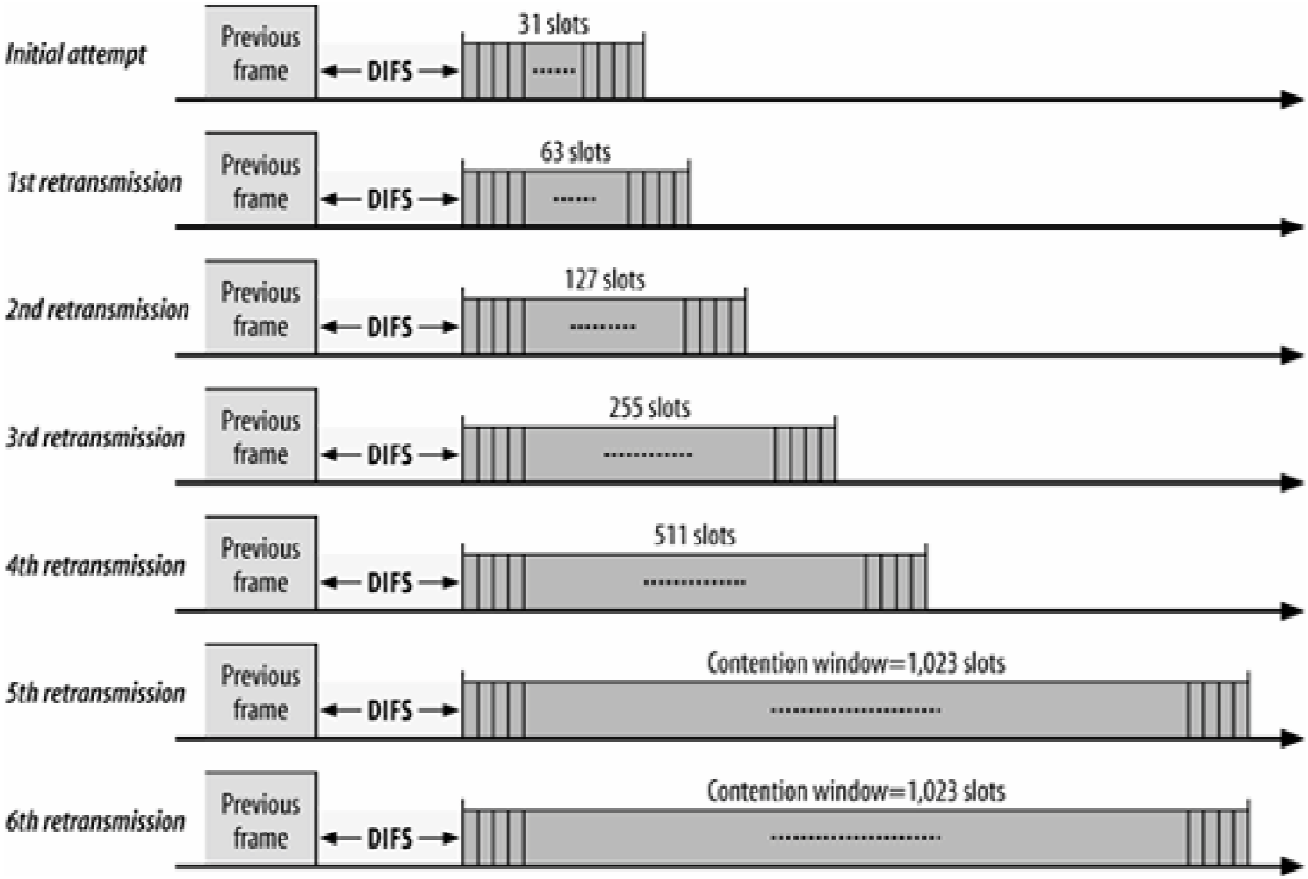


802.11 CSMA/CA

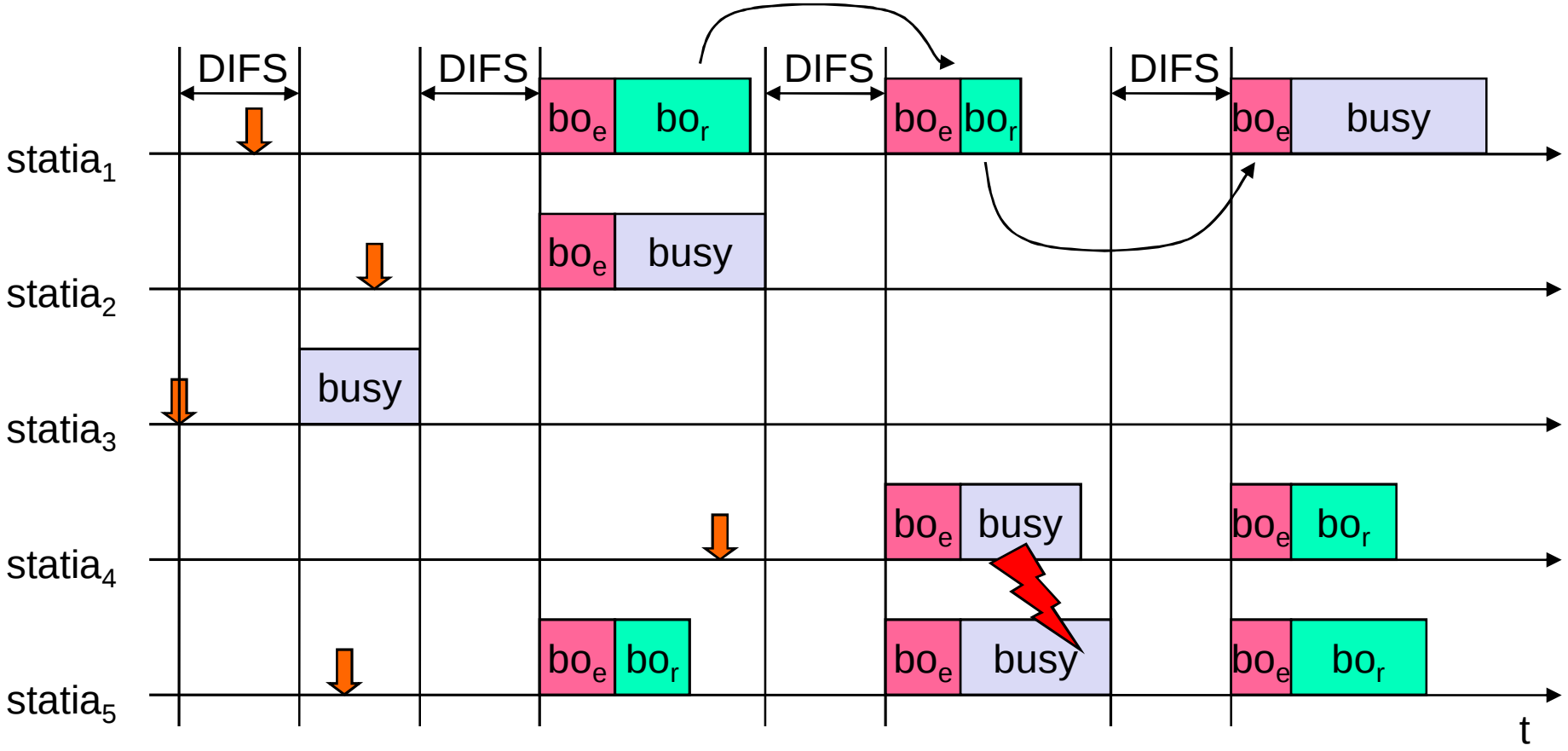
- Stația evaluează dacă mediul e liber (Carrier Sense)
- mediu liber pentru DIFS => se poate transmite imediat
- mediu ocupat => statia așteaptă DIFS liber, apoi se așteaptă pentru arbitraj o perioadă randomizată in intervalul [0..CW) sloturi:
  - » daca stația pierde arbitrajul (mediul devine ocupat) timpul ramas este memorat
  - » Transmisie + Succes (ACK) - se reseteaza nr sloturi = 31
  - » Transmisie + Insucces (no ACK) => nr de sloturi se dubleaza, max=1023



BEB (binary exponential backoff)



802.11 backoff - exemplu 5 stații



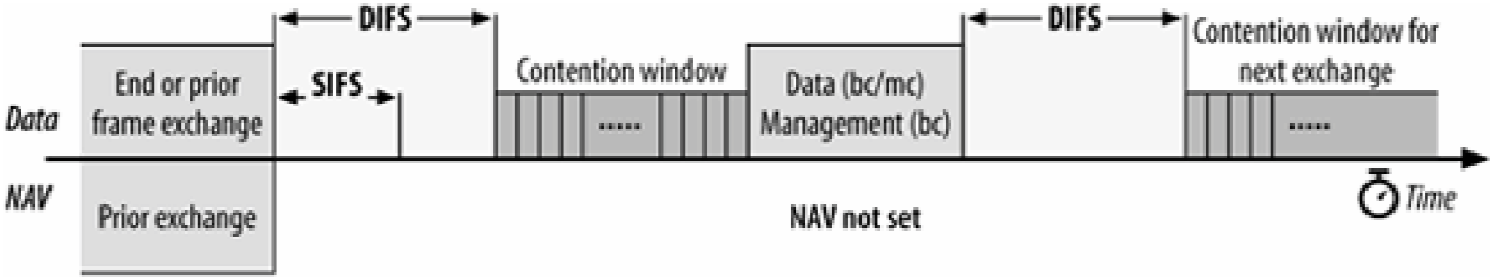
busy — Mediu ocupat (frame, ack etc.)

Un pachet devine disponibil

bo_e backoff expirat

bo_r backoff rămas

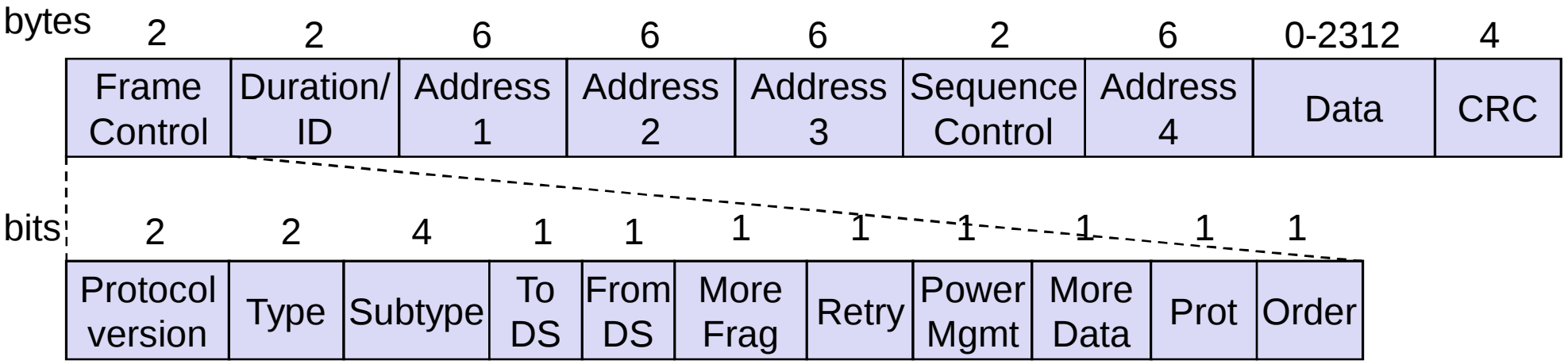
802.11 date broadcast



- nu se fragmentează,
- nu se confirmă
- nu se folosește NAV

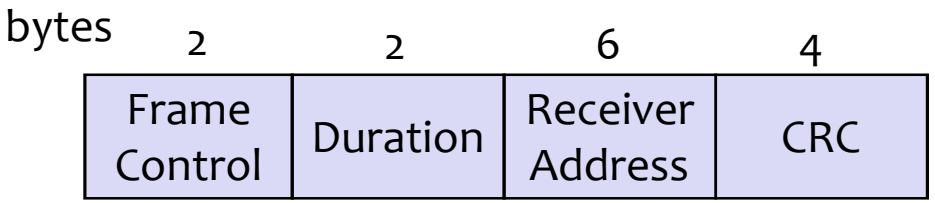
802.11 formatul cadrelor

- Tipuri de cadre
  - » control, management, data
- Fiecare cadru are număr de secvență
  - » ce se intampla daca ACK se pierde?
- Adrese (ethernet, 6 octeți)
  - » receptor, transmitator, sursa, destinatie
- Altele
  - » durata (NAV), checksum, control frame, data

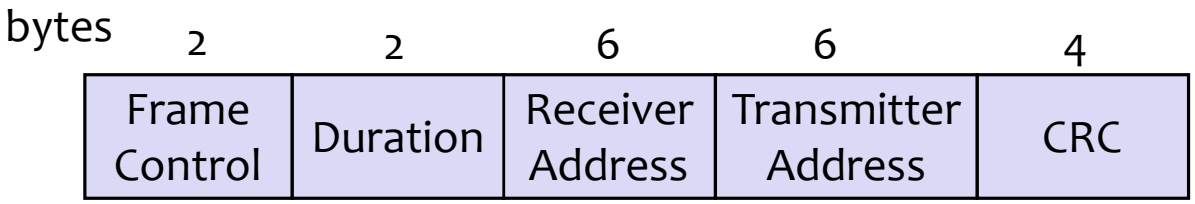


Cadre de control: ACK, RTS, CTS, PS-Poll

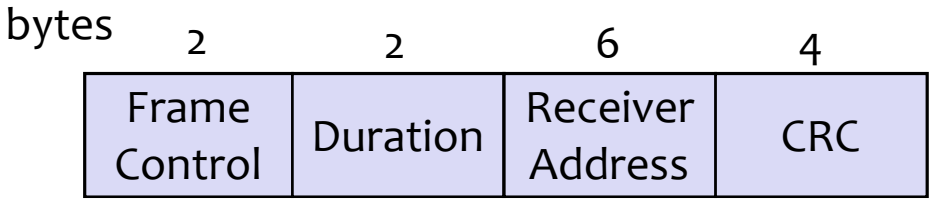
ACK



RTS

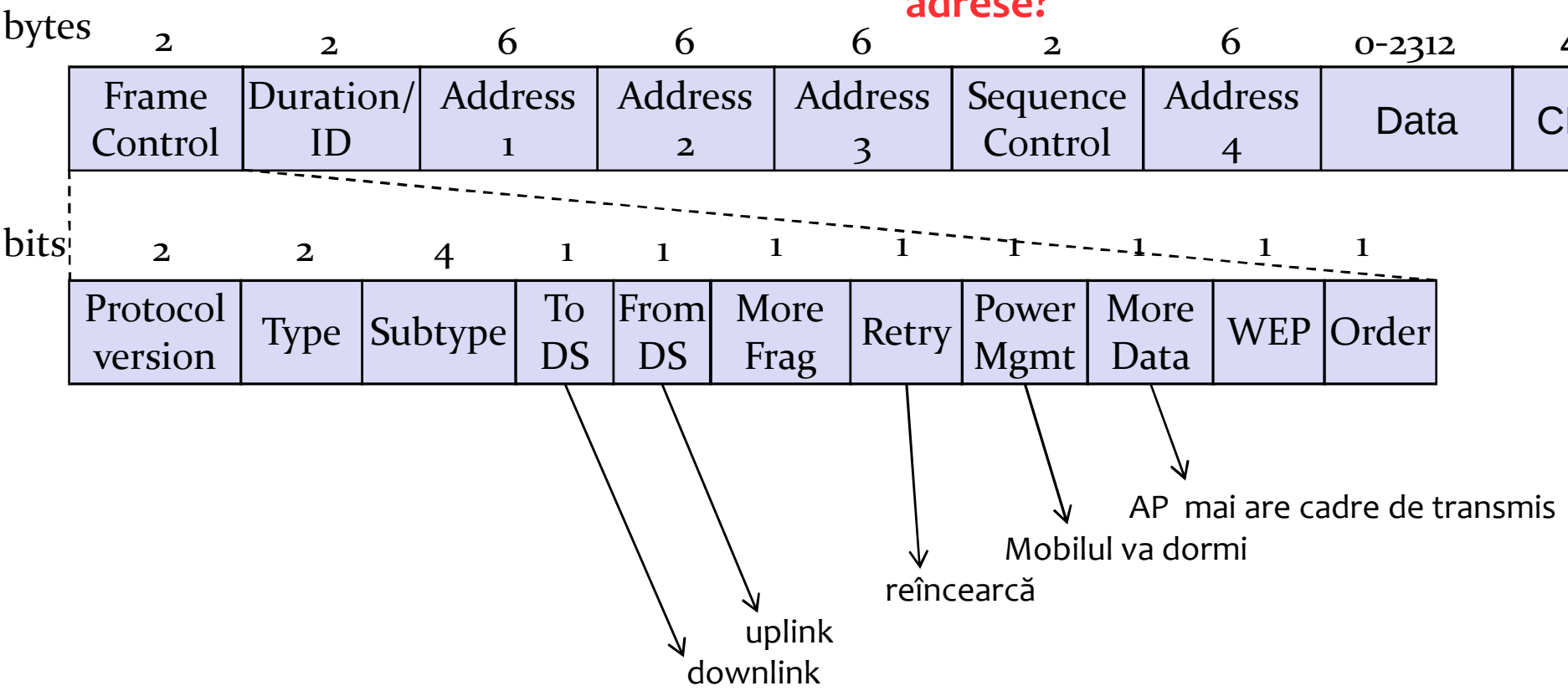


CTS



802.11 cadrele de date

De ce sunt necesare mai mult de două adrese?



adrese 802.11

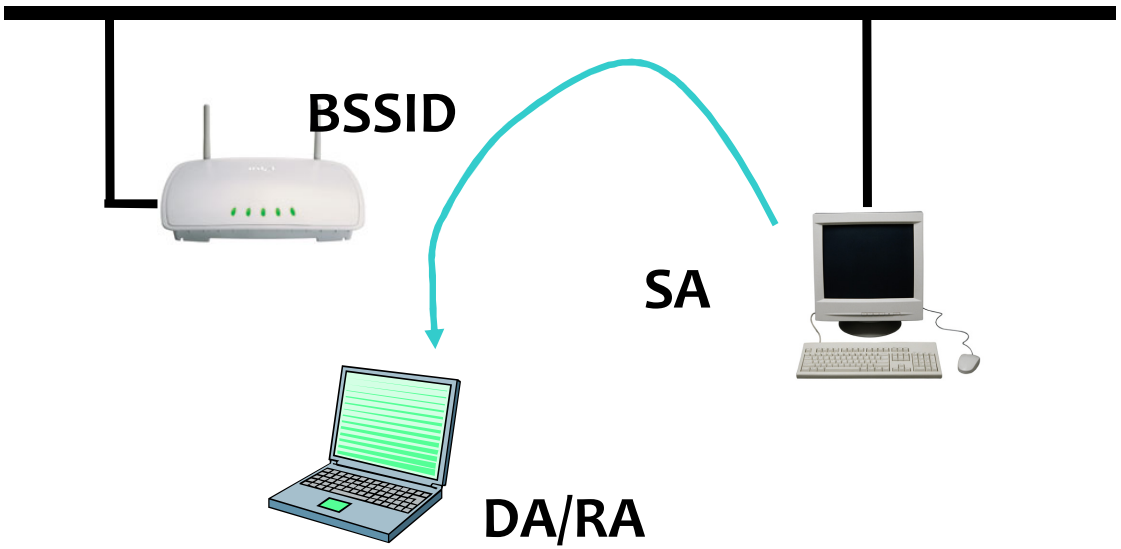
Reguli orientative

- **Adresa 1: stație destinație (wired sau wireless)**
- **Adresa 2: stație sursă (wired sau wireless)**
- **Adresa 3: filtrare – prin ce AP se livrează?**

802.11 adrese

situatia	to DS	from DS	address 1	address 2	address 3	address 4
ad-hoc	0	0	DA	SA	BSSID	-
infrastructura, de la AP	0	1	DA	BSSID	SA	-
infrastructura, catre AP	1	0	BSSID	SA	DA	-
Infrastructura in DS	1	1	RA	TA	DA	SA

DS: Distribution System
AP: Access Point
DA: Destination Address
SA: Source Address
BSSID: de fapt o adresa de AP
RA: Receiver Address
TA: Transmitter Address



cadre wireless > wired

1. Se verifică CRC
2. Uplink – se verifica adresa AP pe poziția 1
3. Se aruncă duplicatele
4. Decriptare (WEP, WPA2)
5. Reasamblare fragmente
6. Translatarea la schemă de adresare Ethernet
    1. DA (addresa 3) devine destination address
    2. SA (addresa 2) devine source address
    3. Daca exista SNAP header => tip pachet
7. CRC recalculat

cadre wired > wireless

1. Validarea CRC ethernet, verificarea stației destinație, dacă este asociată
2. SNAP header dacă este cazul
3. Planificarea pt transmisie (coadă, PS mode)
4. Asignare număr de secvență, fragmentare
5. Criptare
6. Construcție header
    1. Dest address copiat în Address 1
    2. BSSID copiat în Address 2
    3. Src address copiat în Address 3
    4. Se completează câmpul ‘Duration’
7. CRC recalculat

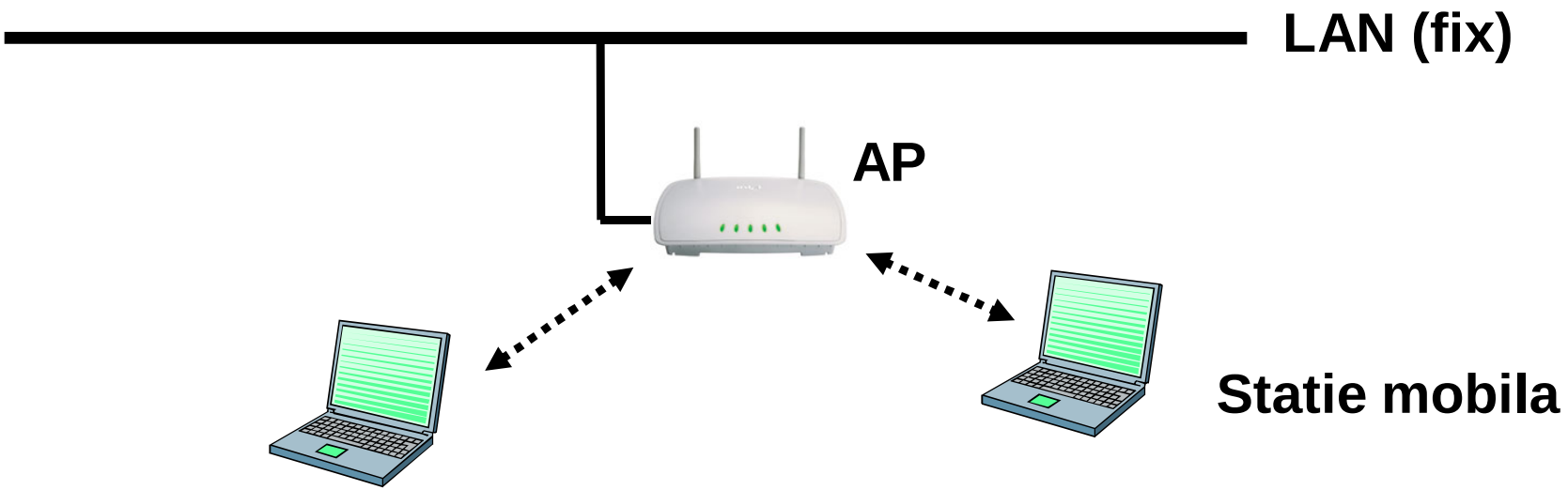
Alte câmpuri

bytes	2	2	6	6	6	2	6	0-2304	4
	Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

- Număr de secvență
- Date – maximum 2304 octeți
- CRC – antet + date

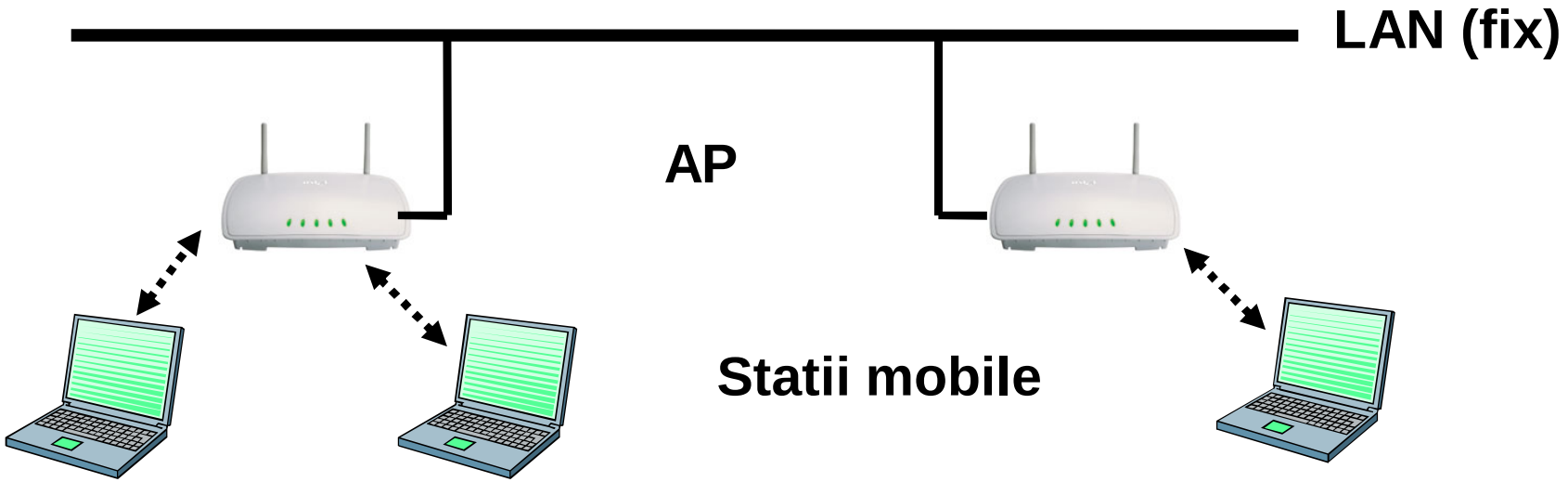
- Diferențe față de alte antete
  - Nu există “tip” pentru datele la nivel superior
  - Nu este necesară o lungime minimă

Modul infrastructură



- Basic Service Set (BSS)
- AP functioneaza ca bridge
- Comunicarea intre statii se face numai prin intermediul AP
- distribution system (DS)

Modul infrastructură - extins



- Extended Service Set (ESS)
- Un set de mai multe BSS
- AP comunică între ele
  - » Frame forwarding
  - » Roaming

802.11 - gestiune MAC

- Sincronizare
  - » TSF = time synchronization function
  - » Timere și beacon-uri TSF
- Gestiunea puterii
  - » sleep-mode fara a se pierde mesaje
  - » periodic sleep, acumulare de frame-uri, masuratori
  - » Traffic Indication Map (TIM): lista receptorilor unicast declarata de AP
- Asociere/Reasociere
  - » integrare in LAN
  - » roaming - schimbare domeniu
  - » Probe - cautare domeniu

Sincronizarea

Timing Synchronization Function (TSF)

Permite sincronizarea perioadelor de somn/veghe – power save

Permite trecerea de la DCF la PCF

Permite saltul in frecvente in FHSS PHY (emitatorul si receptorul stationeaza acelasi interval la fiecare frecventa)

Cum se realizează TSF

Toate statiile mențin un ceas local

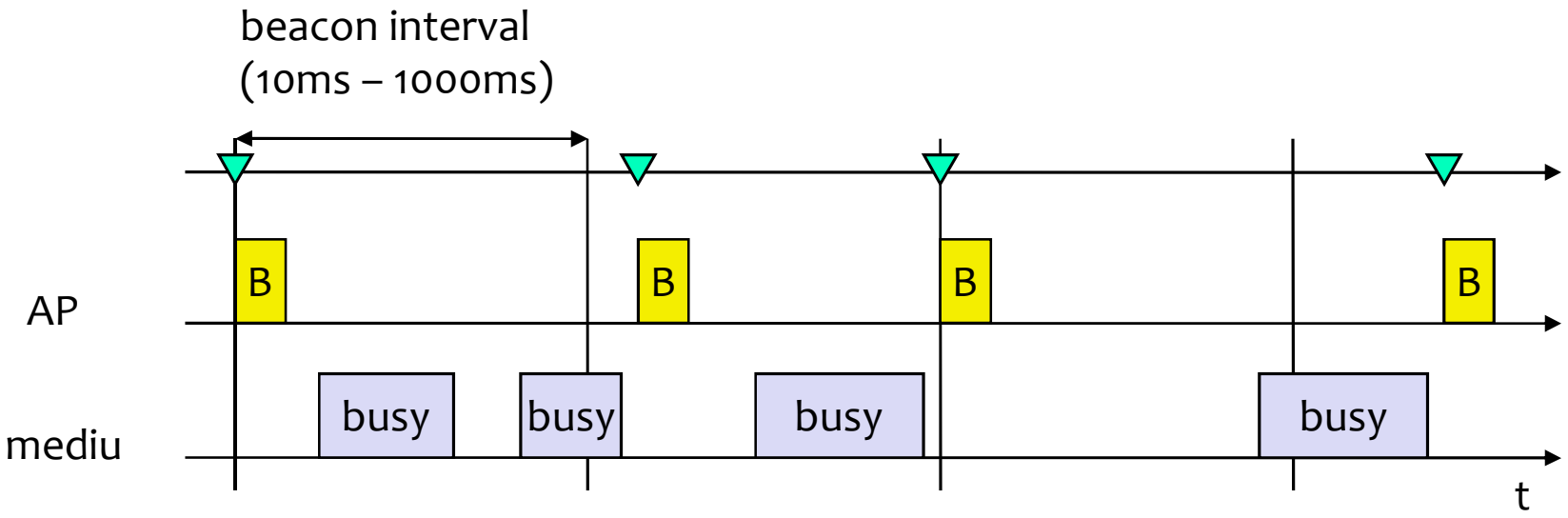
AP difuzează periodic un beacon cu timestamp, informatii de management, roaming

Nu este absolut necesar ca o statie sa primească fiecare beacon

Beacon sincronizeaza intregul BSS

(doar pt infrastructura, ad hoc este mai dificil)

Sincronizare cu beacon



timestamp

B beacon frame

beacon

Fiecare beacon declară

- o listă de rate(MCS) acceptabile
- o listă de rate de bază (obligatorii)
  - Pentru RTS, CTS, ACK, beacon
- Non standard
  - Lista SSID-urilor dorite
  - Modelul telefonului

Gestiune powersave

- Oprește transceiver când nu e necesar
- Starea stației: sleep / awake
- Timing Synchronization Function (TSF)
  - Stațiile devin active la acelasi moment
- Modul infrastructura
  - Traffic Indication Map (TIM)
    - lista receptorilor unicast declarata de AP
  - Delivery Traffic Indication Map (DTIM)
    - lista receptorilor broadcast/multicast declarata AP
- APSD (Automatic Power Save Delivery)
  - metoda mai nouă (802.11e) care înlocuiește TIM, DTIM, ATIM

Gestiune powersave

- AP
  - Menține AID pt fiecare stație
  - stochează cadre pentru stațiile în PS
  - beacon: Traffic Indication Map (TIM)
  - TIM=hartă de 2007 biți (bit per AID)
  - Folosește bitul *MoreData* în downlink

- Stațiile
  - Folosesc bitul PS în uplink
  - se trezesc la *ListenInterval* beacon-uri
  - Contract între AP și stație
  - Cere *un cadru* stocat folosind PS-Poll
  - PS-Poll succesive sunt ignorate

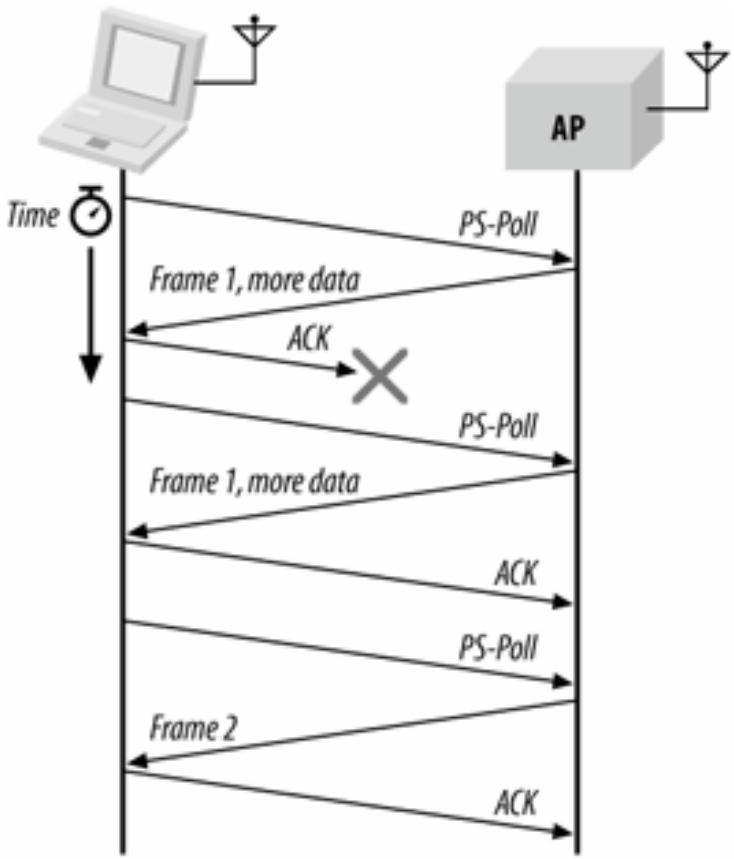
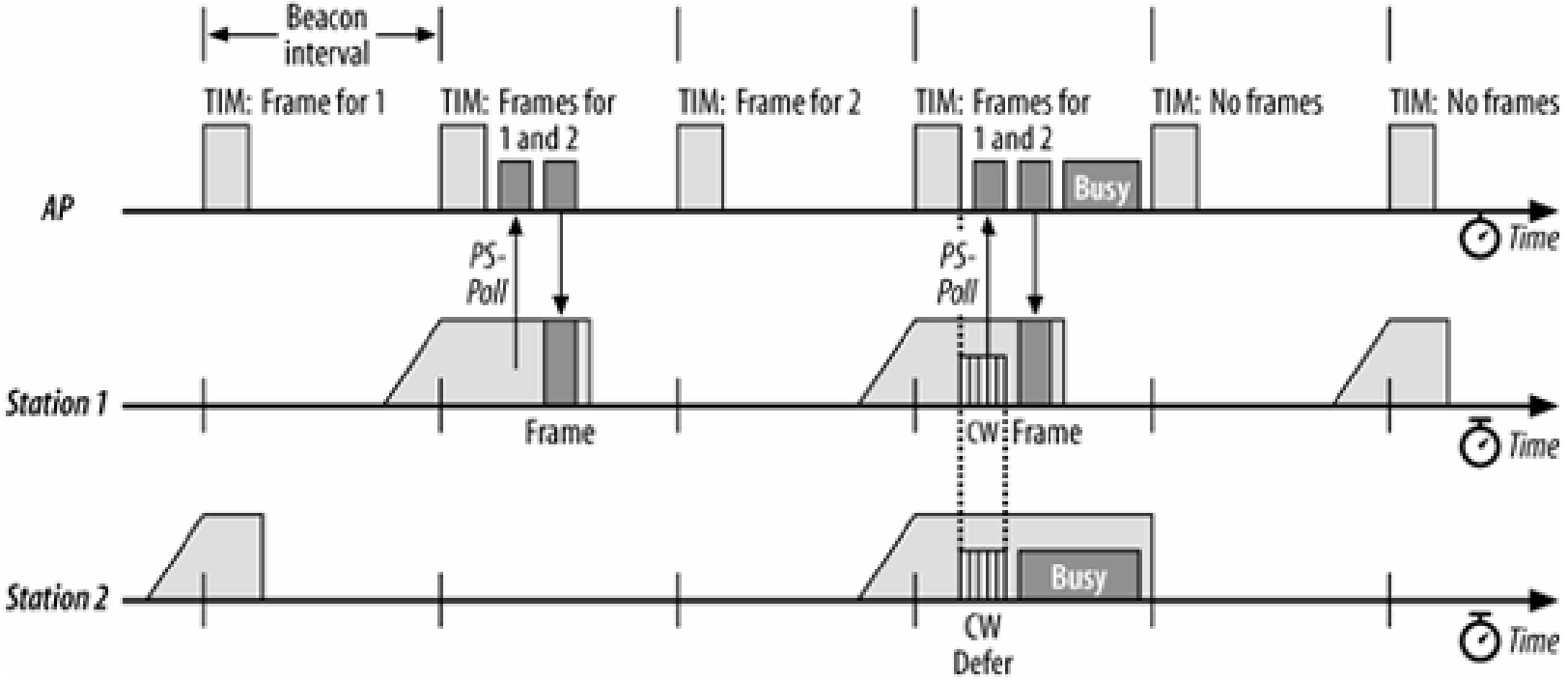
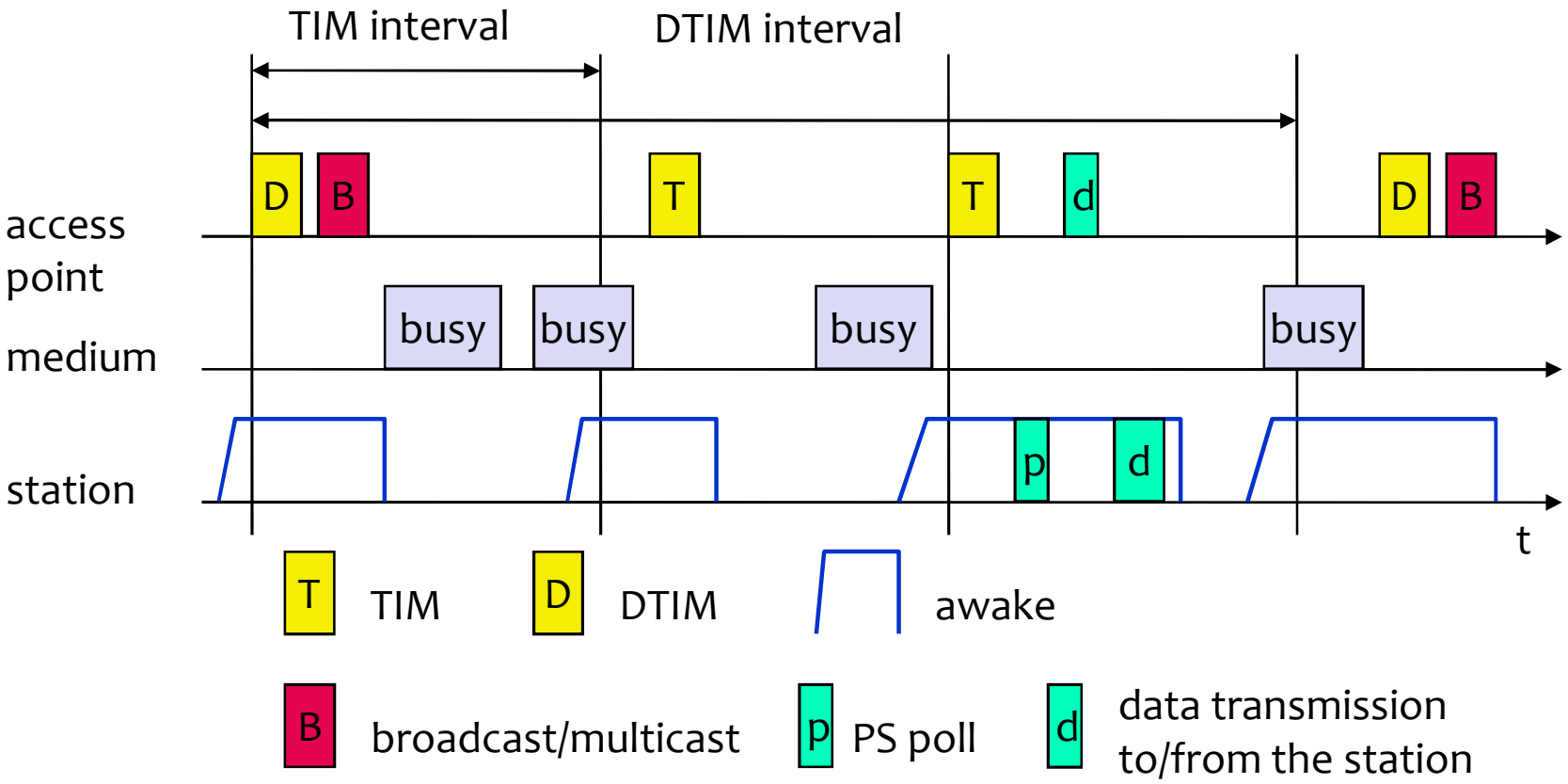


Figure 8-13. Buffered frame retrieval process



- Beacon 1: există cadre pentru stația 1
  - Stația 2 se întoarce în PS-mode
- Beacon 2: stația 1 cere cadrele, trece în PS-mode
- Beacon 3: ambele stații doresc PS-Poll
- Beacon 5: mediul este ocupat de o stație invizibilă
- Beacon 6: cadrul pentru stația 2 a fost aruncat

Gestiune powersave



TIM = cadrele unicast sunt indicate în fiecare beacon
DTIM = cadrele broadcast sunt indicate periodic

Gestiune powersave

- Default TIM=100ms, DTIM = 300ms
  - problematic pentru VoIP
- APSD
  - Stația intră în sleep mode
  - După ce trimite cadru uplink, este gata să primească cadrele stocate la AP
  - Consumă doar 1/6 din putere

802.11 handover

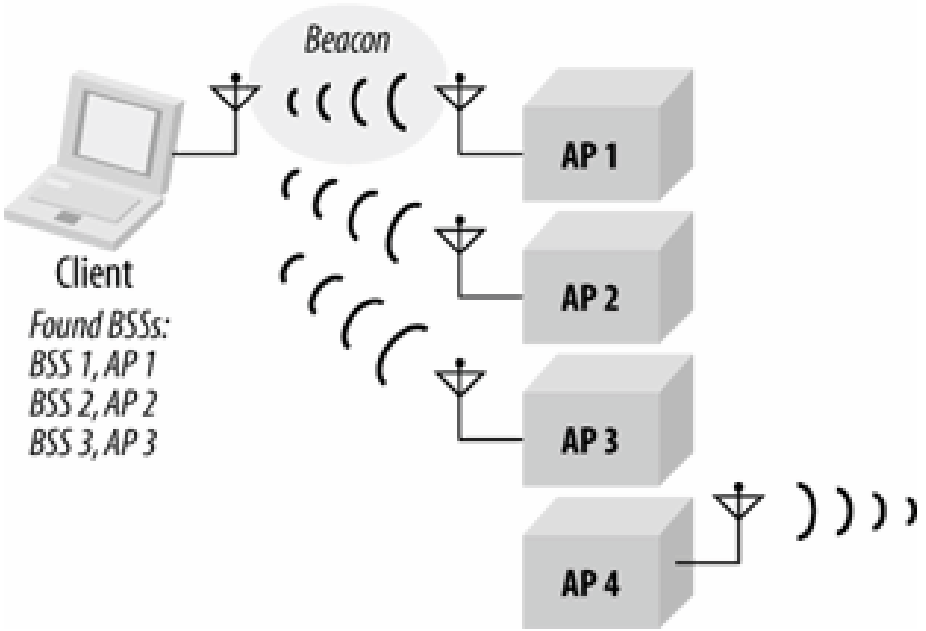
Ce se intâmplă când cade conexiunea?

- Scanare
  - Passive Scanning
  - Rective Scanning
  - se trimit pachete de proba pentru a gasi cel mai bun AP
- Reasociere – cerere
  - statia trimite cererea la unul sau mai multe AP
- Reasociere - Raspuns
  - succes: AP raspunde, statia e primita
  - insucces: continua scanarea
- AP accepta Reasocierea
  - Anunta noua statie in DS (distribution system)
  - DS actualizeaza baza de date (locatii statii)
  - DS anunta vechiul AP
- roaming rapid – 802.11r (e.g. pentru retele vehiculare)

Scanare pasivă

Cea mai economică energetic
- doar se ascultă beacon-uri
- se baleiază toate canalele

Figure 8-2. Passive scanning

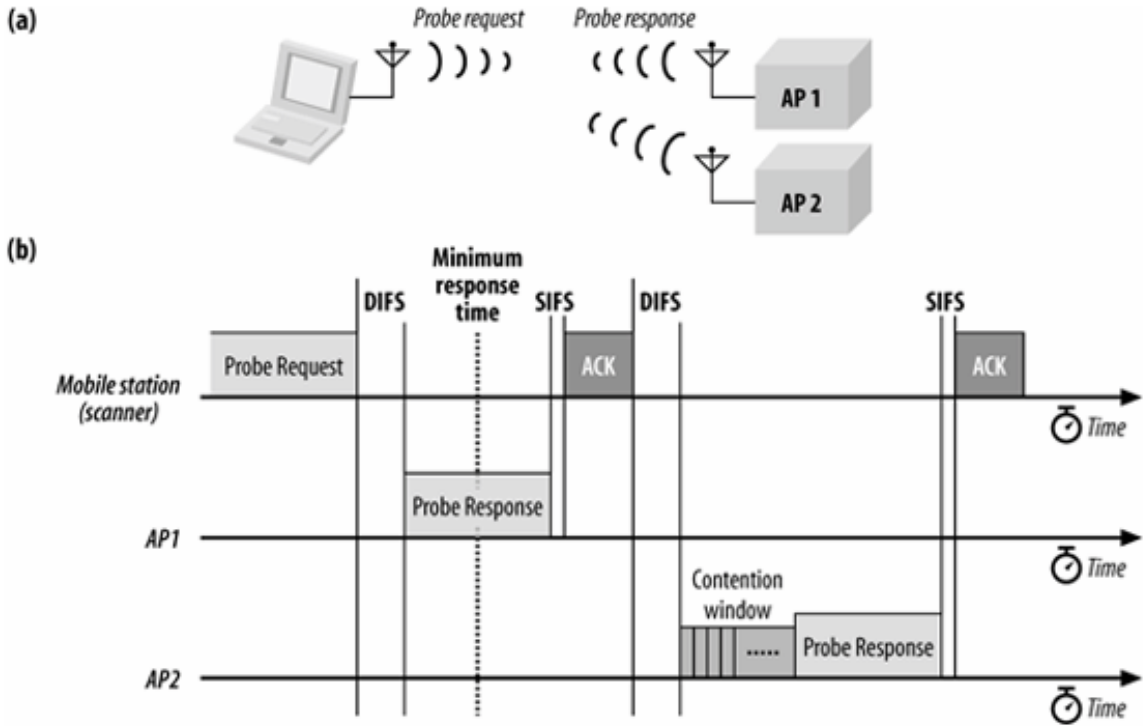


Scanare activă

Pe fiecare canal disponibil:

- Se transmite *ProbeRequest*, folosind DCF
- Se așteaptă *ProbeResponse* un timp maxim
- Se procesează răspunsurile: Beacon interval, DTIM period, basic rates

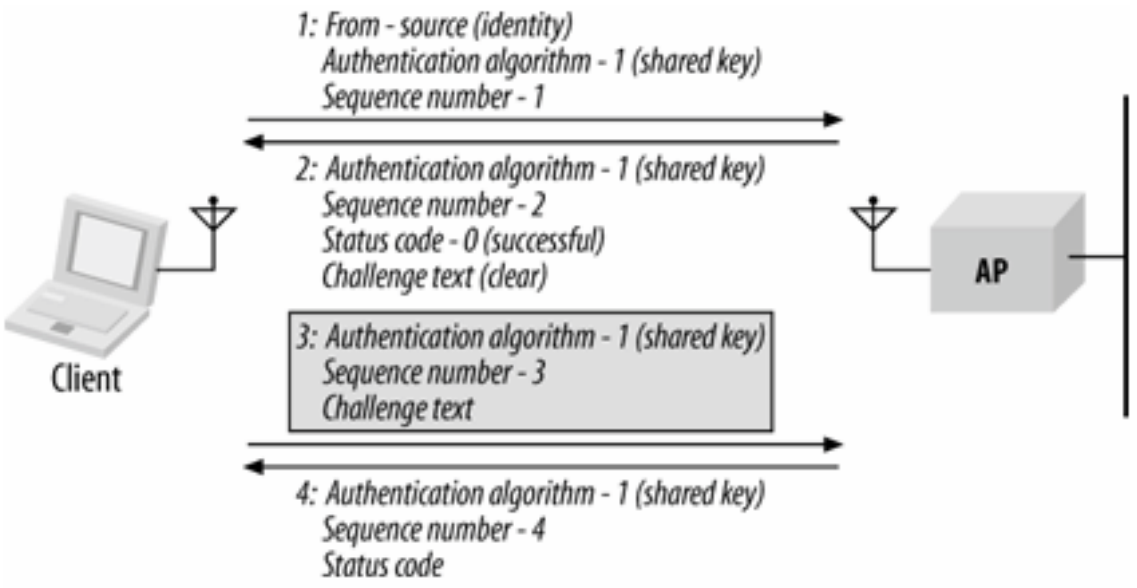
Figure 8-3. Active scanning procedure and medium access



Autentificare

- Open Authentication – de fapt doar o cerere răspuns, obligatorie
- MAC based authentication – nestandard, securitate minimă
- Shared-key
- Preautentificare – pentru a accelera procesul de roaming

Figure 8-5. Shared-key authentication exchange



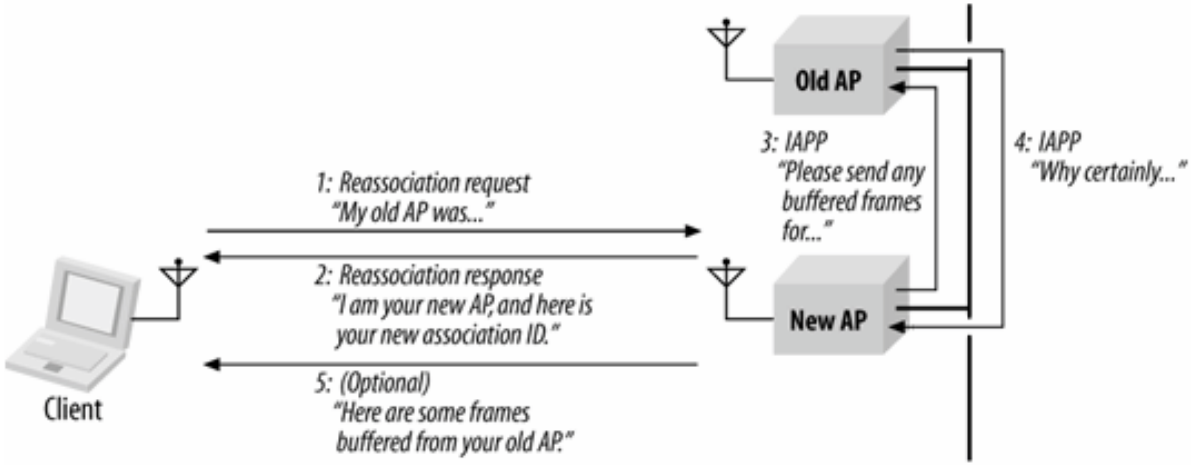
Asociere

Scopuri:

- permite sistemului de distribuție (DS) să știe locația unei stații
- locația trebuie să fie vizibilă și în Ethernet – cum?
    - ARP gratuit pentru a popula porturile din switch-uri

- Întrebare, răspuns cu AID (assoc ID)
- Asociere, reasociere

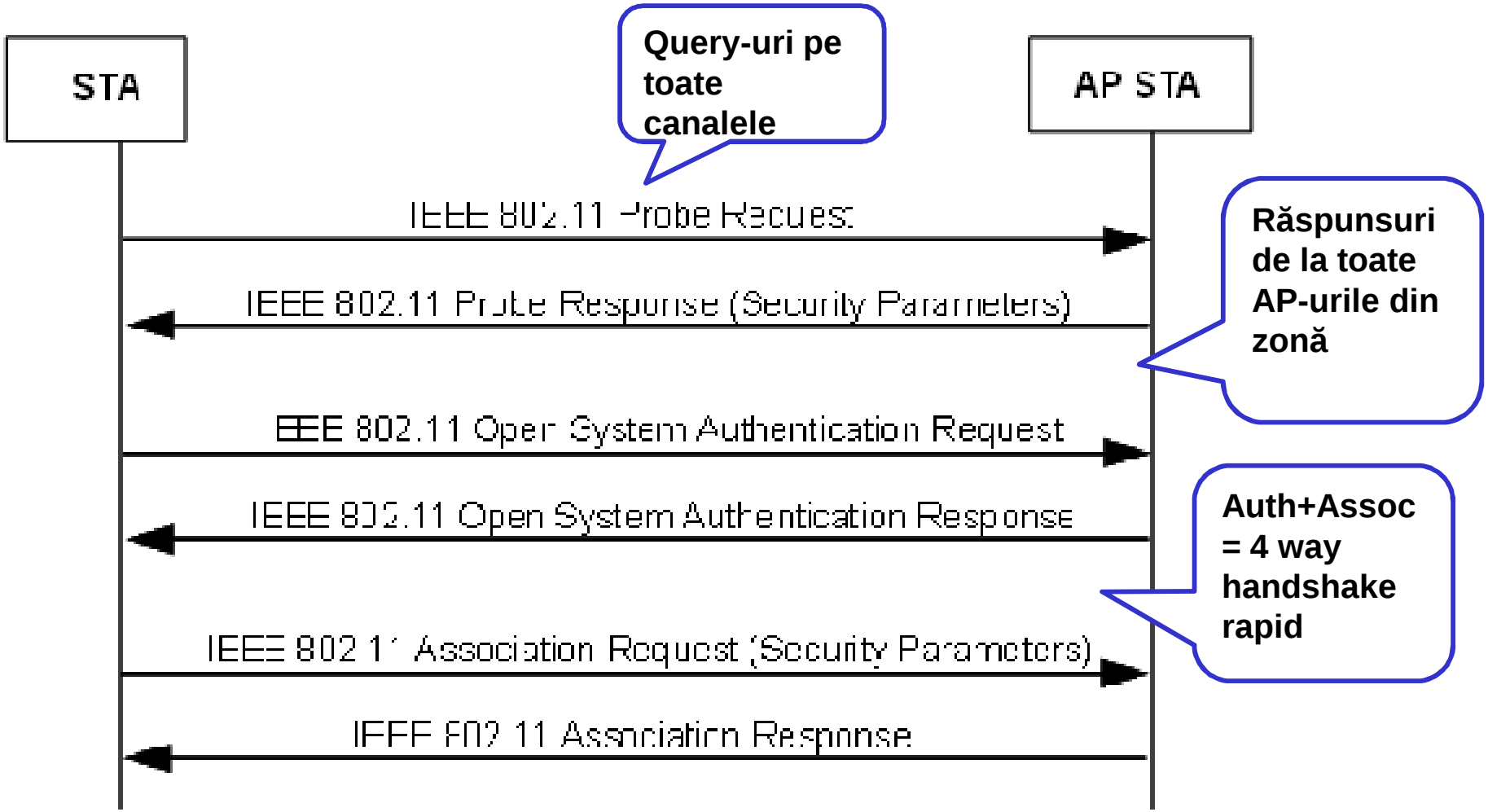
Figure 8-10. Reassociation procedure



Confidențialitate (privacy)

- Hidden SSID?
- MAC based ACL?
- Implicit mesajele sunt necriptate (in clar)
  - » WEP optional, dar implementat pe scara larga
    - – Publicat în 1997, spart în 2001!
  - » WPA, WPA2
    - » foloseste proceduri implementate în hardware
    - » schimbă periodic cheile
  - » WPA2
    - » PSK = personal shared key (parolă)
    - » Enterprise = EAP + 802.1x + RADIUS (user + parolă)

Autentificare + Asociere la AP



Sumar cadre de management

Beacon

- Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
- Traffic Indication Map

Probe

- ESSID, Capabilities, Supported Rates

Probe Response

- Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
- same for Beacon except for TIM

Association Request

- Capability, Listen Interval, ESSID, Supported Rates

Association Response

- Capability, Status Code, Station ID, Supported Rates

Sumar cadre de management

Reassociation Request

Capability, Listen Interval, ESSID, Supported Rates, Current AP Address

Reassociation Response

Capability, Status Code, Station ID, Supported Rates

Disassociation

Reason code

Authentication

Algorithm, Sequence, Status, Challenge Text

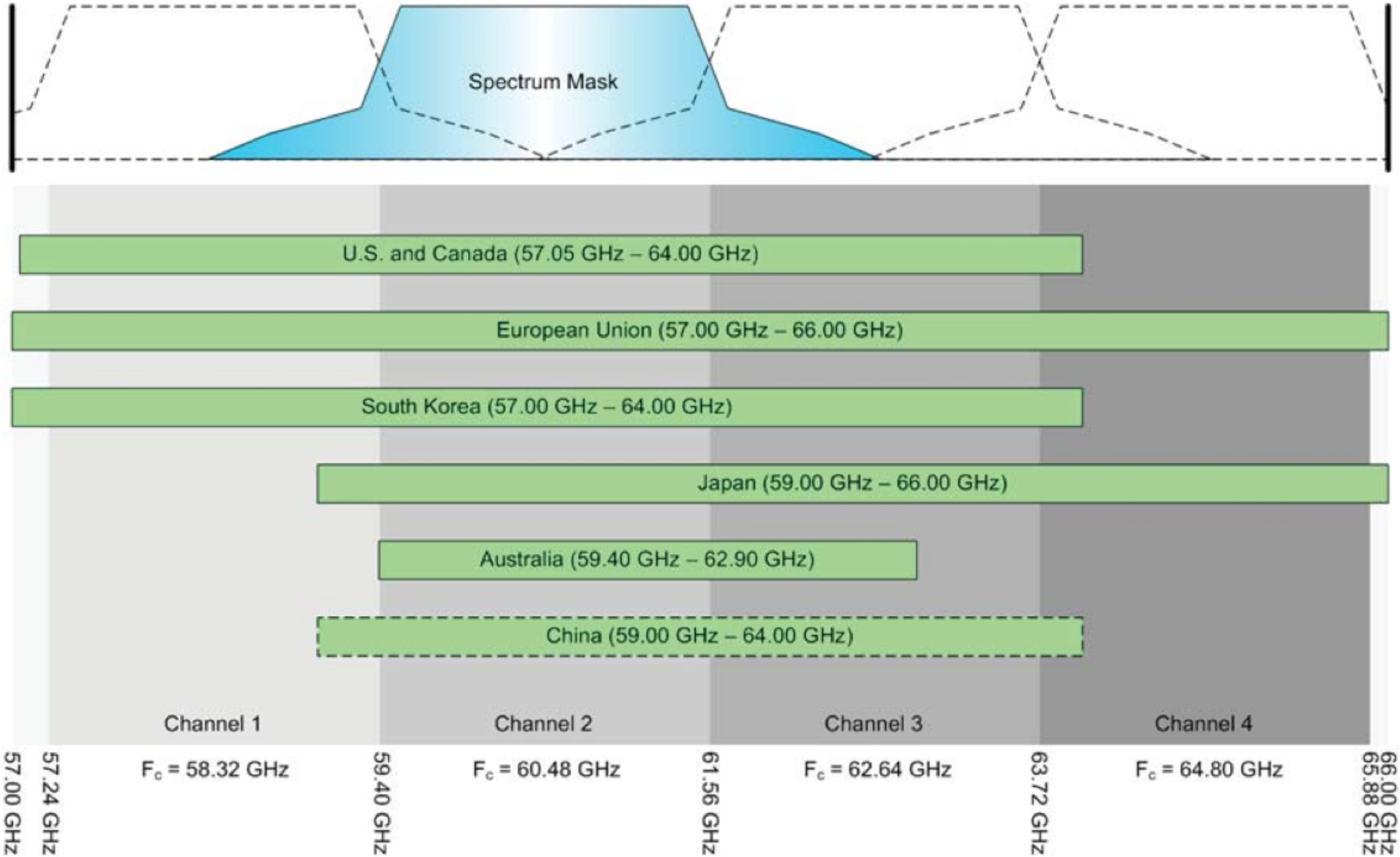
Deauthentication Reason

802.11 – ce urmează?

802.11ad (WiGig)

- 60GHz, beamforming, < 10m LOS?
  - loss over 1 m at 60 GHz is 68 dB
  - avantaj și dezavantaj
- Max 7Gbps :-D
- Power consumption: 6W :-(
- WiGig Display Extension

Canale la 60GHz



802.11 standardizarea continuă

- 802.11e – suport pentru QoS
- 802.11h – management frecvente 5GHz
- 802.11i – securitate WPA2, 802.1x
- **802.11-2007** = cumulativ 802.11, a, b, d, e, g, h, i, j
- 802.11f – comunicare intre puncte de access
- 802.11k – management resursa radio
- 802.11r – fast handoff
- 802.11n -- capacitate sporită
- 802.11p – pt vehicule – viteza 200km/h
- 802.11s – mesh, capabilitati multihop
- 802.11t – predictia performantei
- … toate literele pana la z, și mai departe!

802.11-2012 = cumulativ 802.11-2007, 802.11n-2009, k, r, y, n, w, p, z, v, u, s

802.11-2016 = 802.11-2012 + aa, ac, ad, ae, af