IEEE 802.11

Dragoş Niculescu
dragos.niculescu at cs pub ro

de A.I. **HotNews.ro**
11:16 Sport | Fotbal

Liga 1
Foto: Agerpres

Liga 1 se afla pe locul 15 in Europa in ierarhia intocmita de Federatia Internationala de Istorie si Statistica a Fotbalului (IFFHS). Astfel, in ultimii zece ani (in intervalul 2001-2011), campionatul din Romania a adunat 5382 de puncte. Lider este Premier League (Anglia), britanicii fiind urmati de Primera Division (Spania) si Serie A (Italia).

citeste **tot articolul** [4 comentarii

Traficul global de date mobile pe internet va creste de 18 ori in perioada 2011 – 2016 - studiu Cisco

documente
Estimari Cisco (20 Feb 2012) DOC, 101KB

de Adrian Vasilache **HotNews.ro**
11:40 Economie | Telecom

Traficul de date mobile la nivel mondial va creste de 18 ori in perioada 2011-2016, ajungand la o rata de rulare anuala de 130 exabytes, echivalenta cu 33 miliarde DVD-uri, cu 4,3 cvadrilioane de fisiere MP3 (muzica/audio) sau cu 813 cvadrilioane de mesaje text (SMS) prin serviciul de mesaje scurte, conform estimarilor producatorului de echipamente si solutii IT Cisco. In Europa Centrala si de Est, traficul video de date mobile va creste de 32 de ori in perioada mentionata, iar in 2016 traficul video va reprezenta 67% din traficul de date mobile, comparat cu 45% la finalul lui 2011, arata raportul.

citeste **tot articolul** [0 comentarii

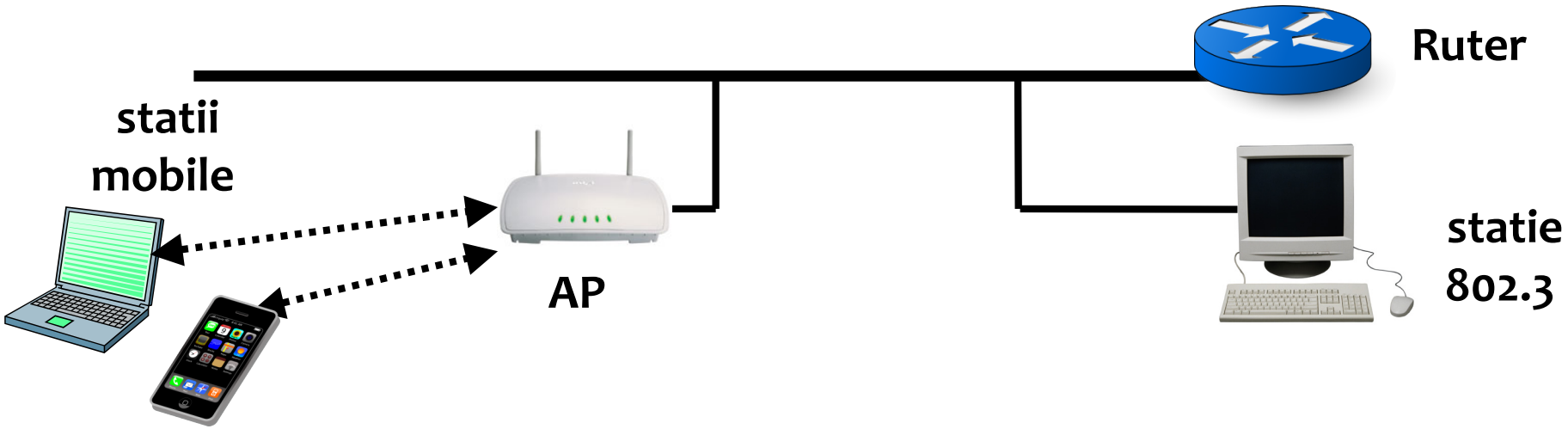
Corespondenta din SUA

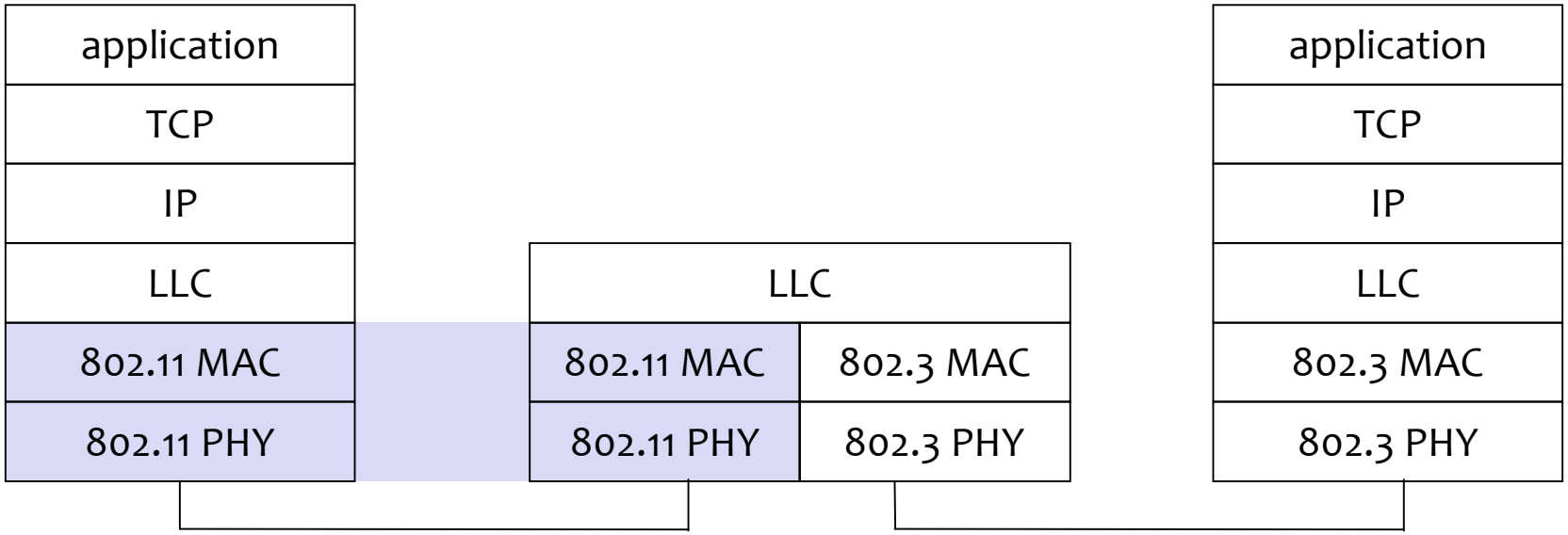
Victor Ponta, la Chicago: Eu nu cred intr-o opozitie care vine sa distruga tot ceea ce au facut cei dinainte. Ei au putut face atat, noi vom face si mai mult!

Cuprins

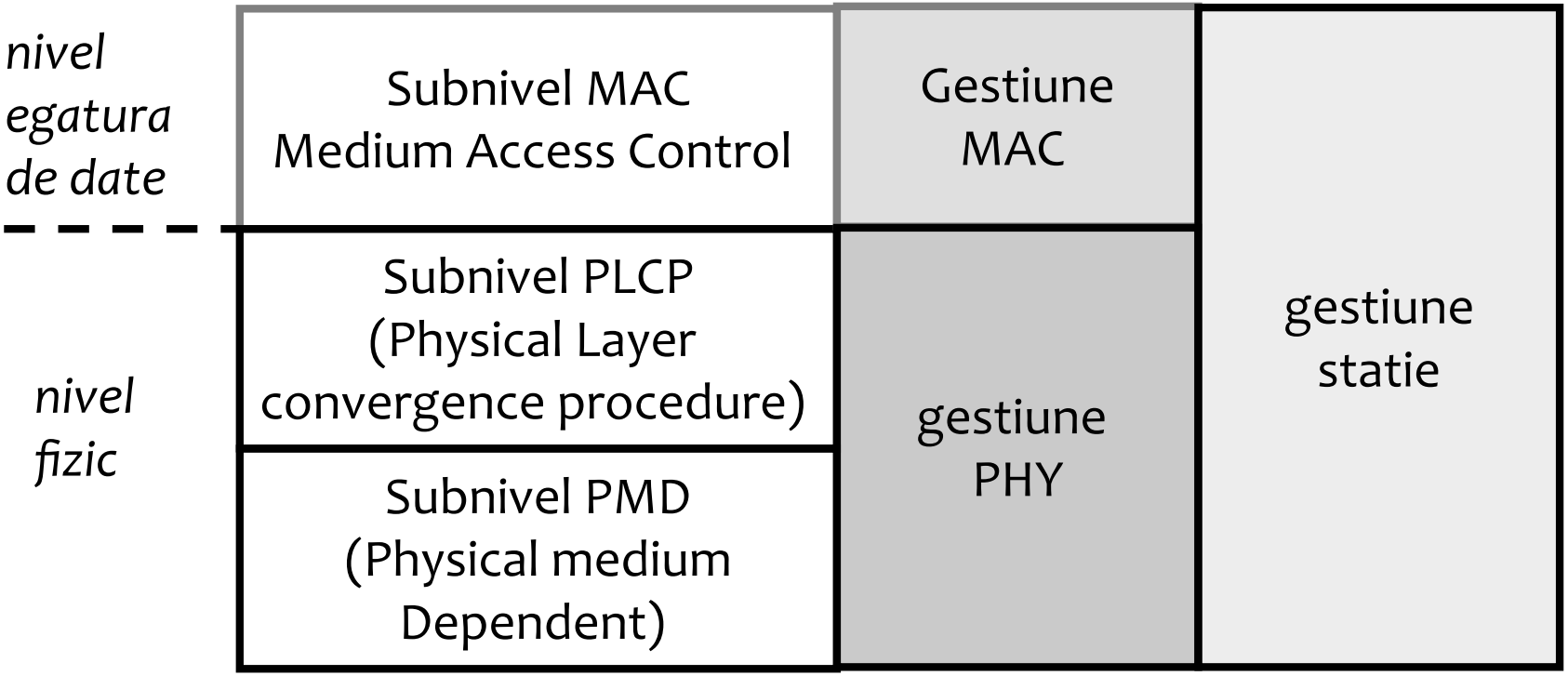
- organizare, standarde
- nivelul fizic
  - FHSS, DSSS, OFDM
  - 802.11b, 802.11a, 802.11g, 802.11n
- nivelul legatura de date
  - CSMA/CA, Schimbul de cadre
  - Terminale ascunse, expuse, handover
- multihop
  - modul ad-hoc

exemplu 802.11 + 802.3





nivelele 802.11



802.11 nivele, funcții

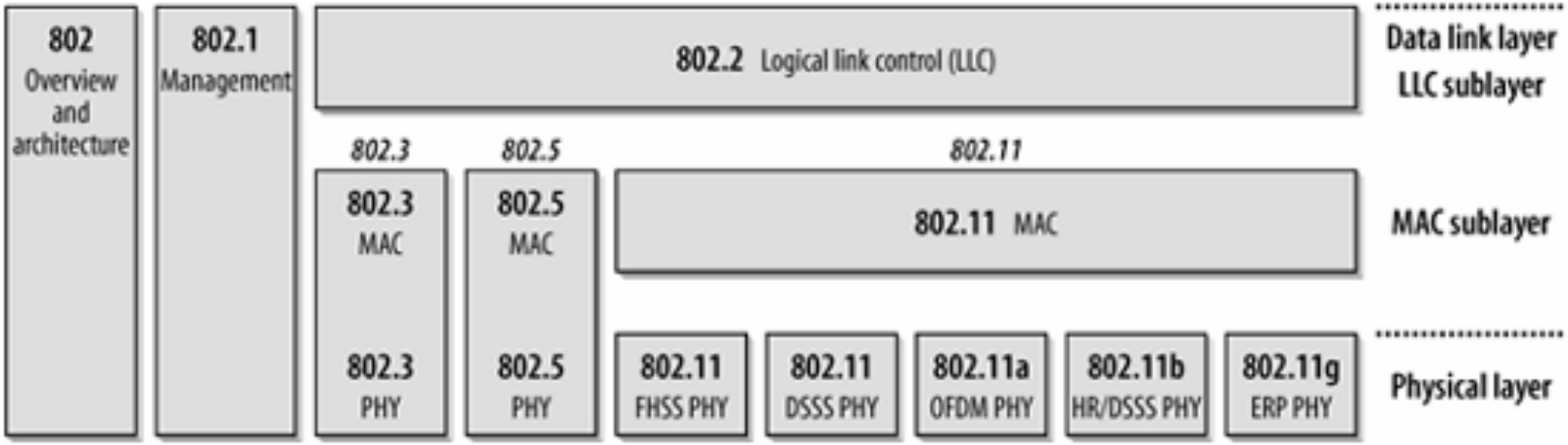
- MAC
  - access la mediu
  - fragmentare, criptare
  - gestiune putere (power save mode)
- MAC management
  - sincronizare, handover, asociere, autentificare
- PLCP (PHY layer convergence protocol)
  - incapsulare pachete MAC
  - carrier sense
- PMD (PHY medium dependent)
  - codare, modulare BPSK, QPSK, QAM
  - Dependent de DSSS, FHSS, sau OFDM
- management PHY
  - alegerea canalului

organizare 802.11

Familia de standarde IEEE 802.11

- Specifică PHY(L1) si MAC(L2) pt rețele locale wireless (WLAN)
- MAC: bazat pe CSMA/CA
- PHY: infrarosu, radio 2.4GHz, 5GHz

- IEEE 802.11b (Wi-Fi) - 1999
  - 11 Mbps in banda 2.4GHz, foloseste DSSS, CCK
- IEEE 802.11a - 1999
  - 54 Mbps in banda 5 GHz ,
  - OFDM (orthogonal frequency division multiplexing)
- IEEE 802.11g - 2003
  - 54 Mbps in banda 2.4 GHz, OFDM
- IEEE 802.11n - 2009
  - 150Mbps/canal in banda 2.4 GHz OFDM, MIMO (max 600Mbps)



802.11n MIMO OFDM

nivelul fizic (L1)

802.11 PHY

Tipuri de radio:

- Spread Spectrum
- Diffused Infrared

Secvențe de împrăștiere (spread spectrum)

- Frequency hopping (FH)
- Direct sequence (DS)

Interfața radio folosește banda de 2.4GHz/5GHz fără licență în SUA, Europa, Japonia.

- *1 Mbps & 2Mbps folosește FH – standard vechi*
- 1, 2, 5.5, &11Mbps folosește DSSS
- 6,9,12,18,24,36,48,54 folosește OFDM

Împrăștiere

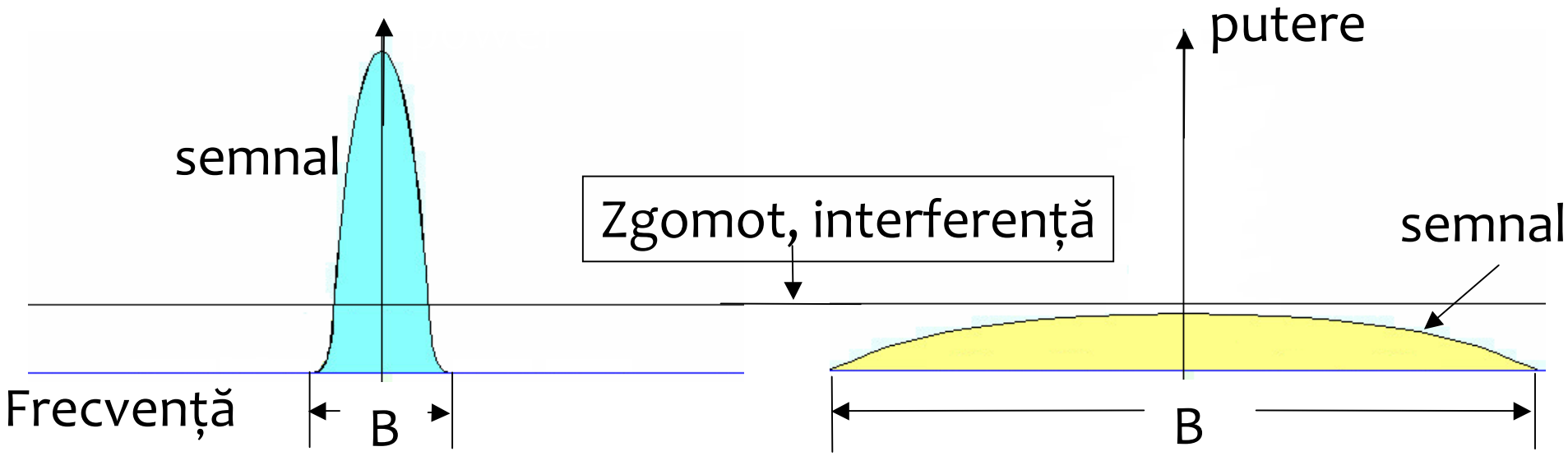
$C = B*\log_2(1+S/N)$ . . . [Shannon]

Pentru a obtine aceeasi capacitate C

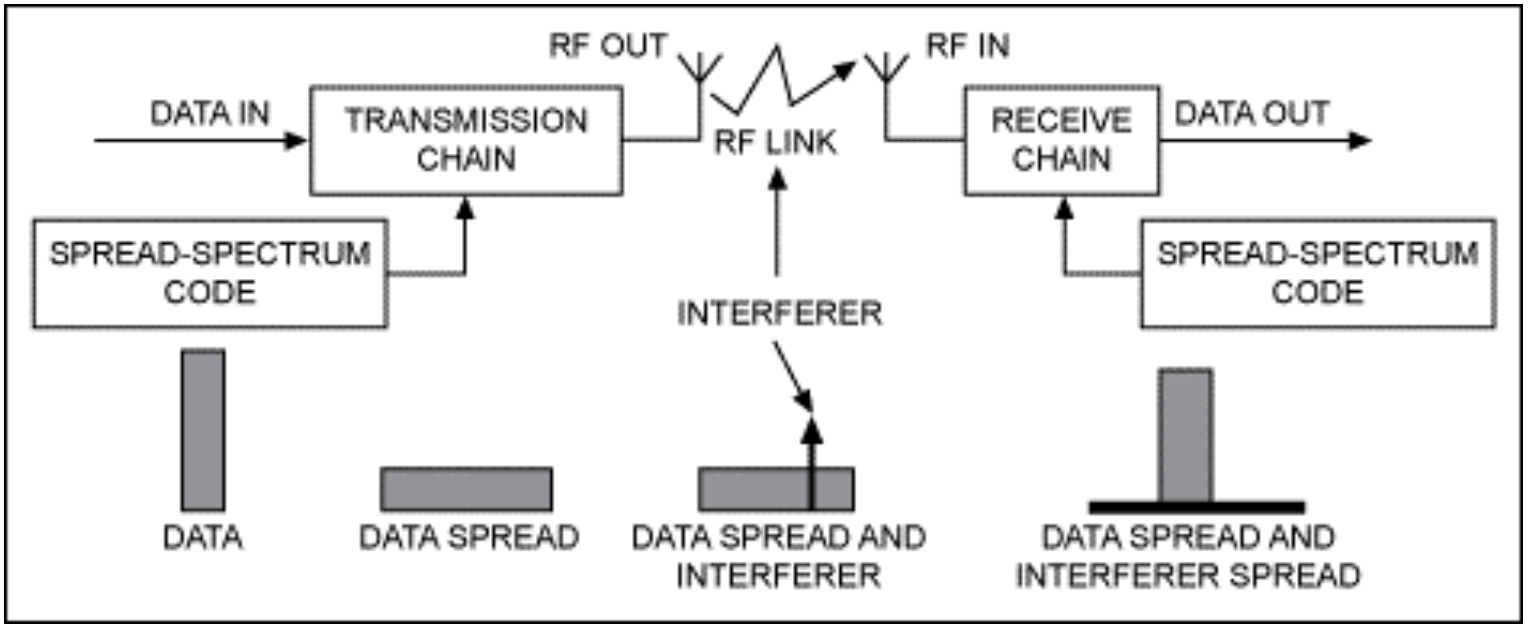
S/N mare, B mic

S/N mic, B mare

Creșterea S/N este ineficientă datorită logaritmului



Schematică împrăștiere

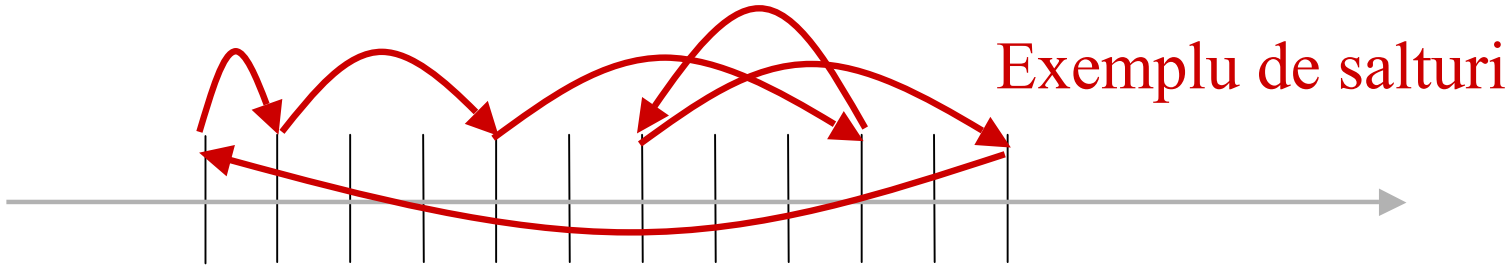


- Motivația?
  - » Rezistenta la bruiaj
  - » Rezistența la interferență
  - » Rezistența la interceptie
  - » Energia factorului de interferență => despread
  - » Energia datelor transmise => spread

Frequency Hopping SS (FHSS)

Banda de 2.4GHz divizată în 75 1MHz subcanale

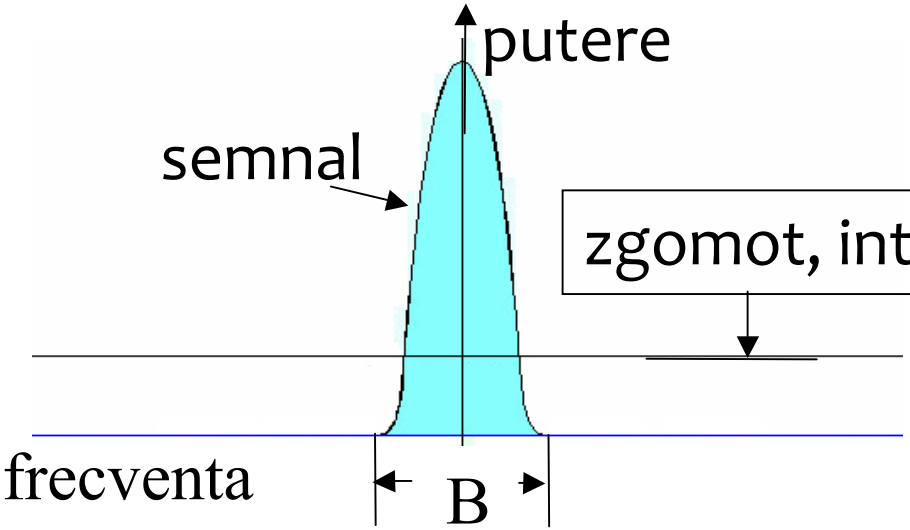
Emițătorul și receptorul folosesc aceeasi secvență de frecvențe (pseudoaleatoare).

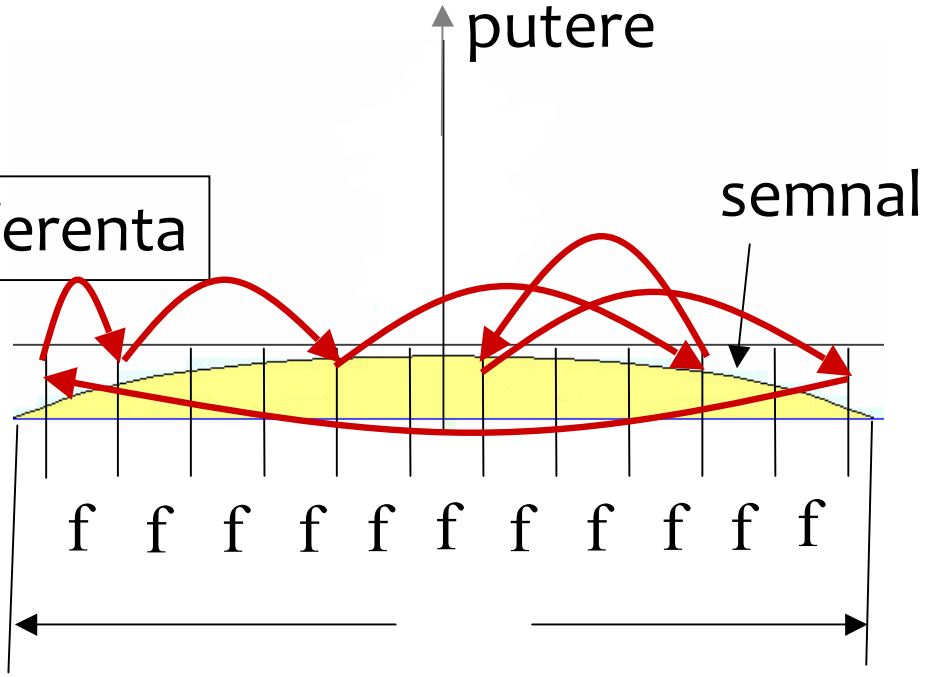


Secvențe de salturi diferite permit coexistența mai multor domenii BSS

Robust interferențelor în benzi inguste

FHSS inventat de [Lamarr1940]





Design simplu, viteza ~ 2Mbps

Saltul in frecvente inventat de Hedy Lamarr (actriță de Hollywood) in 1940

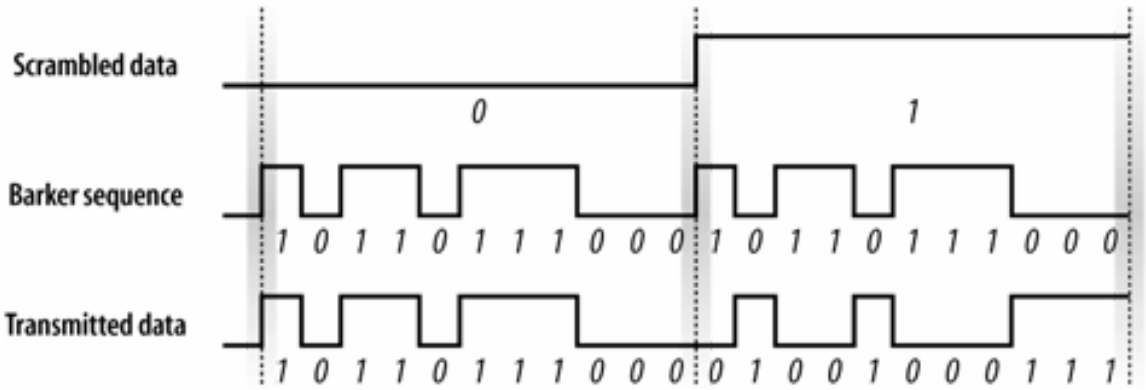
Direct Sequence SS

Direct sequence (DS)

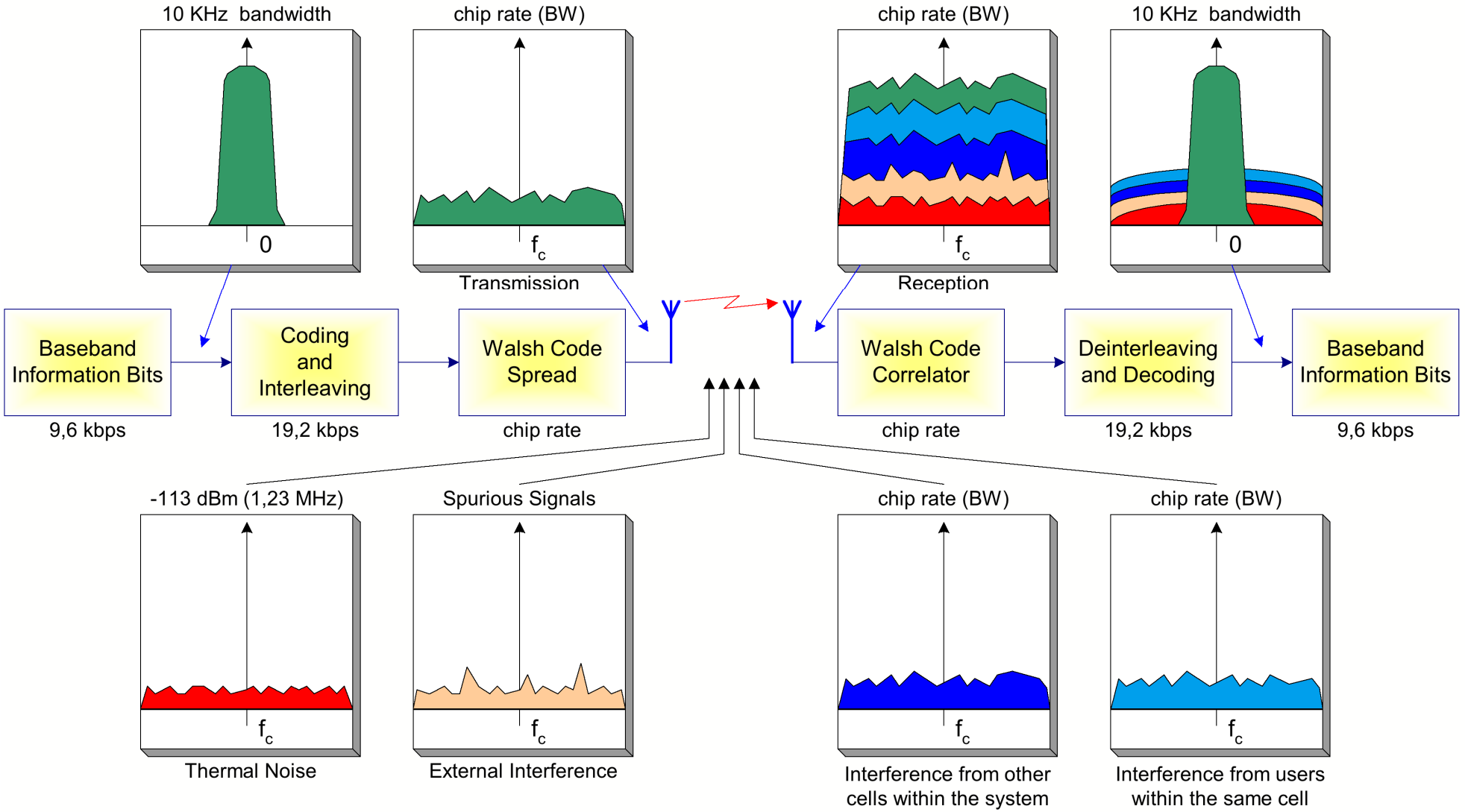
- mai popular, rate mai mari, 11b,g
- secvența Barker 10110111000
- Se transmite o întreagă secvență pentru fiecare bit
- Semnalul este împrăștiat cu o secvență Barker, și apare ca zgomot de bandă largă pentru alți receptori
- Nodurile in același domeniu folosesc același cod
- Similitudine cu CDMA

DSSS: Direct Sequence SS

- Foloseste o lățime de bandă mai mare decat este necesar
- Se generează biți extra prin combinare XOR cu o secventa de împrăștiere



Spreading și De-spreading DSSS



802.11b DSSS

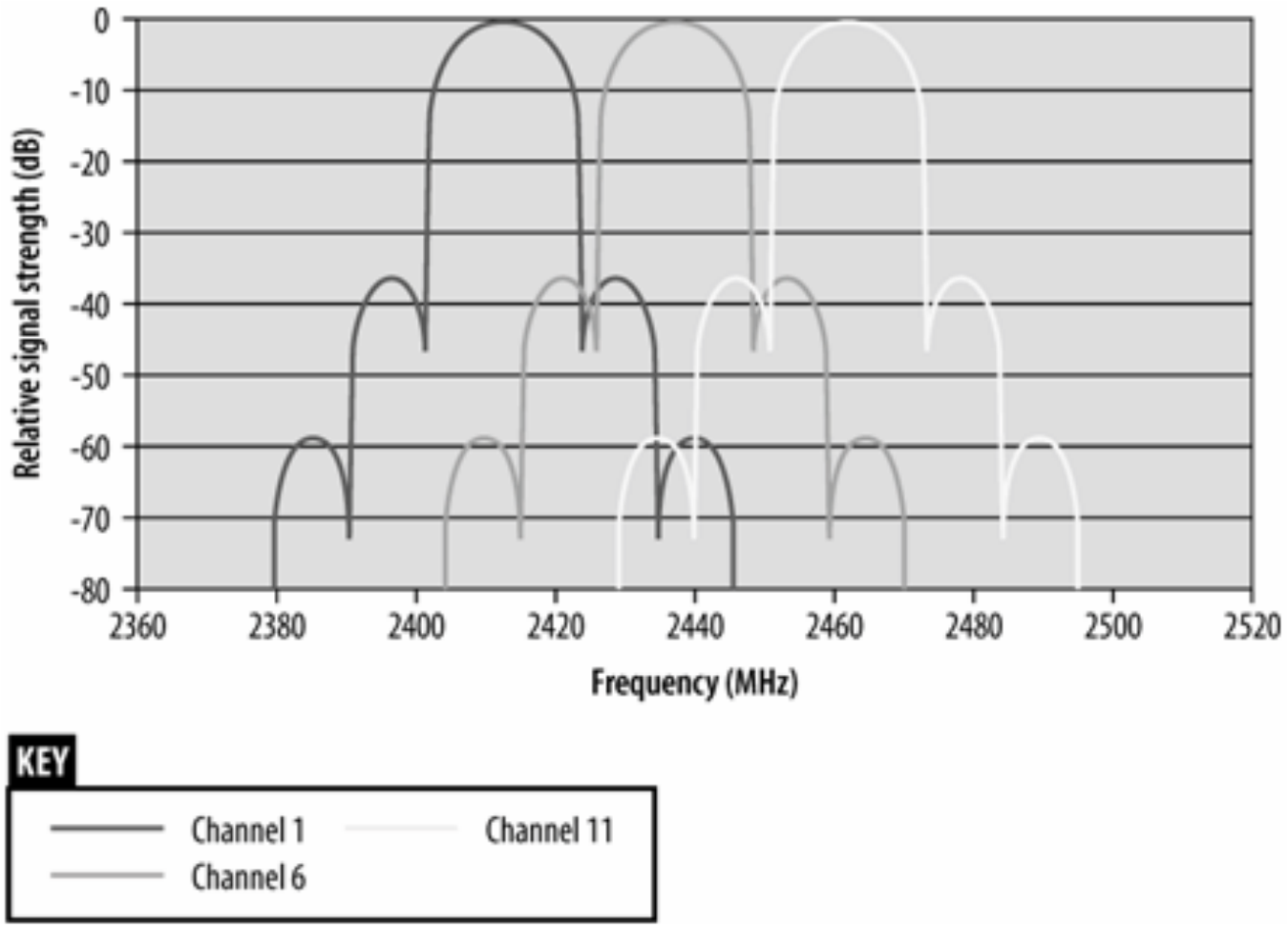
- Frecvențe fara licenta ISM (industrial științific medical) 2.4GHz
- Un canal $f_{sus} - f_{jos} = 22$ MHz
- DSSS în fiecare canal
- 3 canale independente

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		

IEEE 802.11b - caracteristici

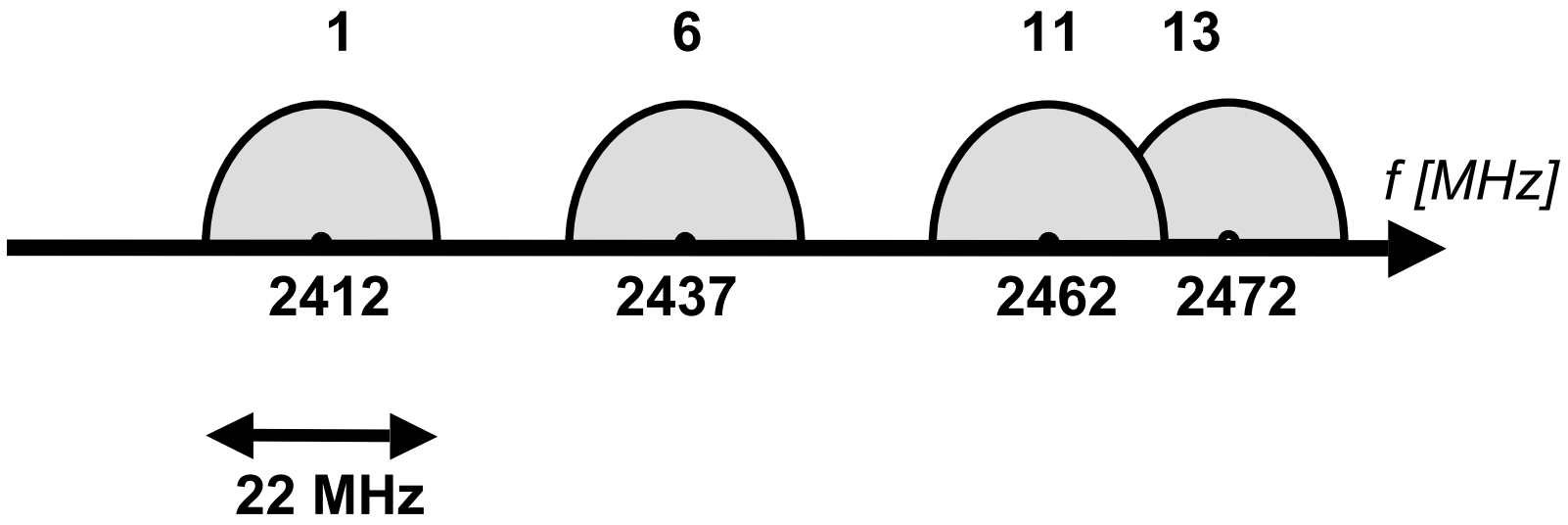
- rate
  - » 1, 2, 5.5, 11 Mbps, depinde de SNR
  - » rata maxima la utilizator 6.3Mbps
- Aria de transmisie
  - » 150m exterior, 50m interior
- Frecventa
  - » 2.4 GHz, DSSS, CCK
- Securitate
  - » limitata, WEP, SSID
- Avantaje:
- Disponibilitate:
  - multe produse,
  - experienta tehnica,
- frecventa fara licenta,
- Multi producatori,
  - integrat in portabile, telefoane,
  - Preț scazut
- Dezavantaje:
  - » Interferență
  - » QoS Inexistent,
    - » “best effort”,
    - » fără garanții (PCF neimplementat)
  - » viteză redusă
  - » Gestiune limitată
    - » nu există distribuție de chei,
    - » criptare simetrică

Dispersia energiei pentru un canal DS 802.11b



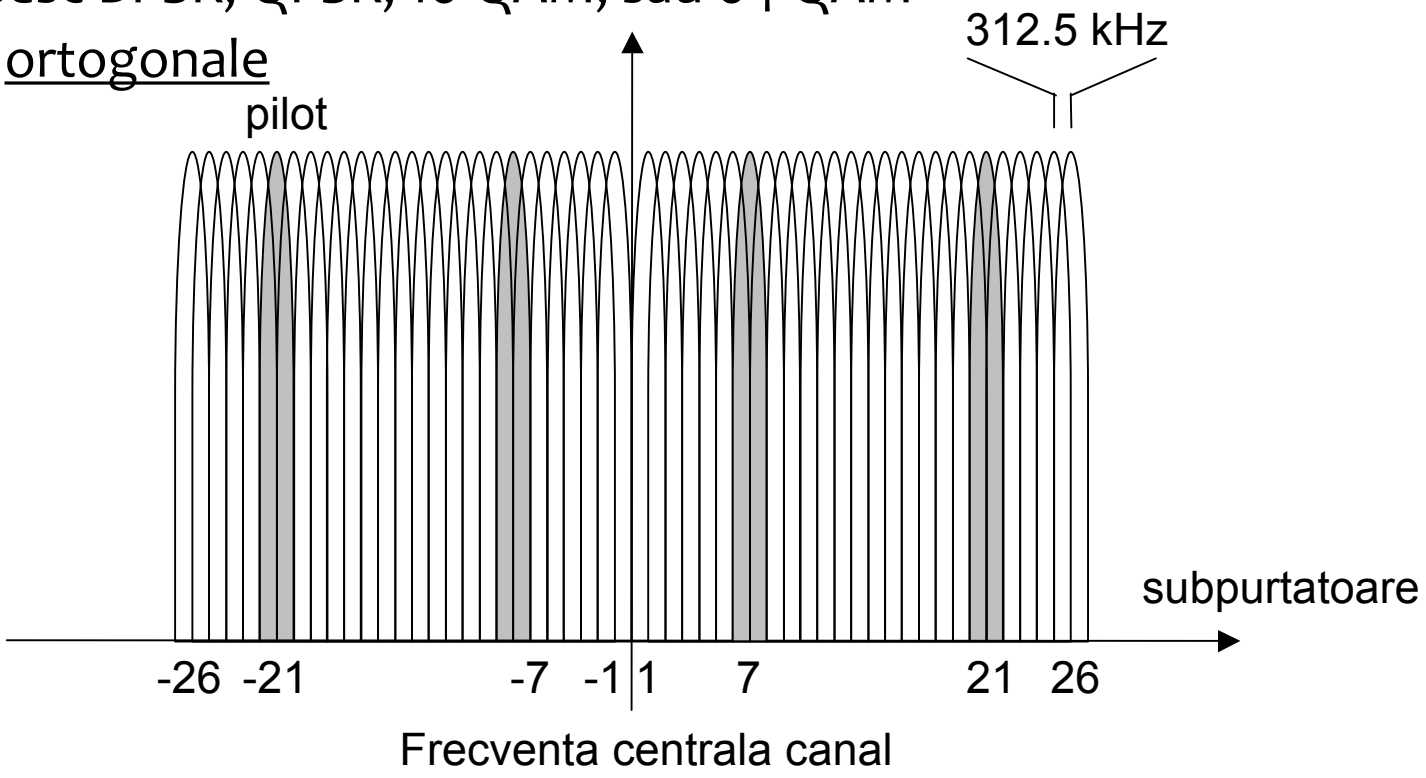
dispunerea canalelor 2.4GHz

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



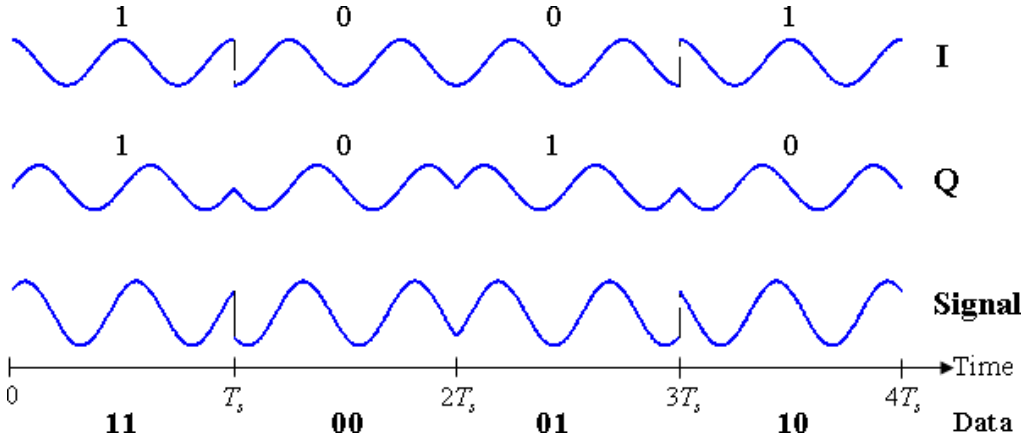
OFDM in 802.11a,g

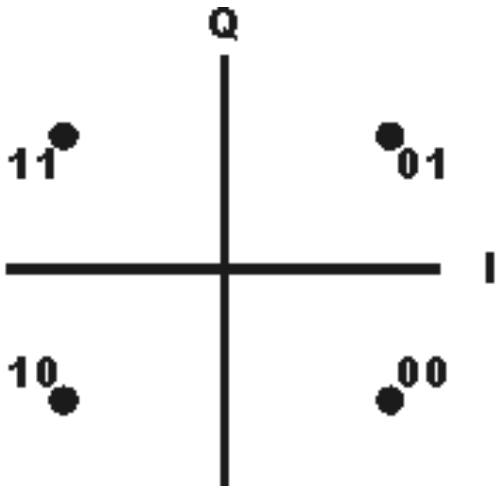
- OFDM cu 52 subpurtatoare (64 in total)
  - » 48 data + 4 pilot
  - » Spatiere 312.5 kHz
  - » Subpurtatoarele
    - – folosesc BPSK, QPSK, 16-QAM, sau 64-QAM
    - – sunt ortogonale



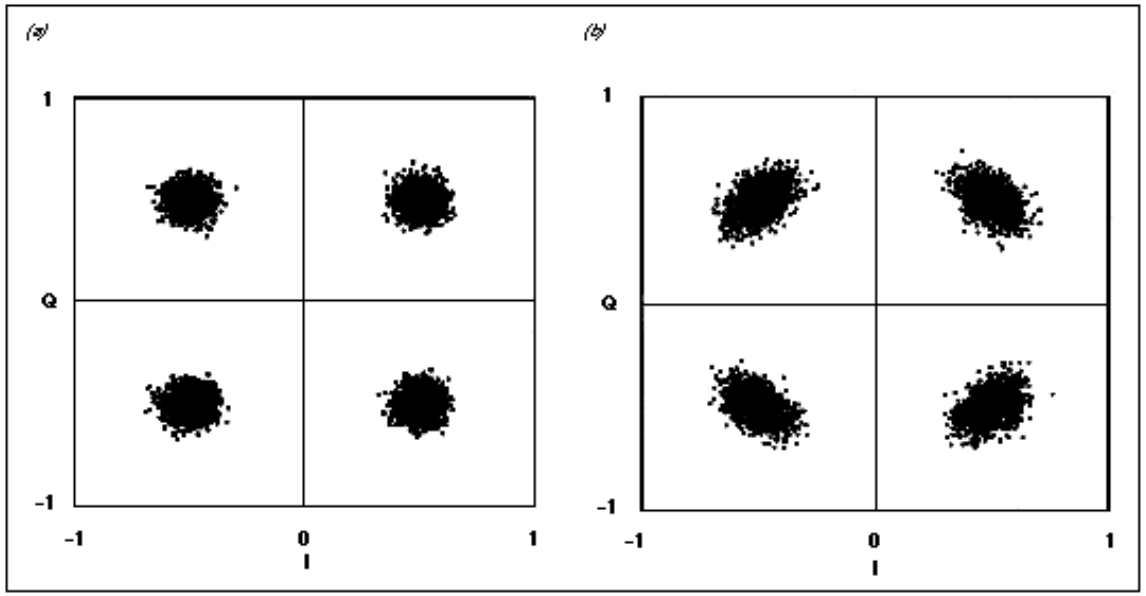
Modulații BPSK, QPSK

- PSK = phase shift keying
- Purtătoare
  - 2 componente: I(nphase) și Q(uadrature)
  - eșantionare - simboluri





teoretic



real

Comparație BPSK/QPSK/QAM

Exemplu performanțe card EDUP b/g USB adapter
802.11b

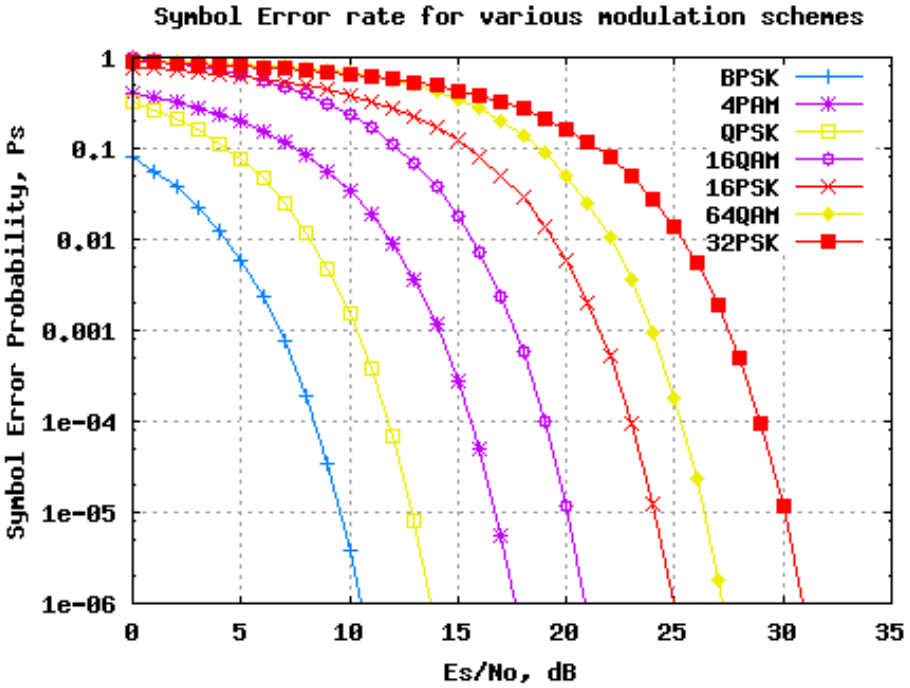
1, 2 Mbps (BPSK, **QPSK**): - 96dBm
11 Mbps (CCK): -91dBm
(Typically @PER < 8% packet size 1024 and @25oC + 5oC)

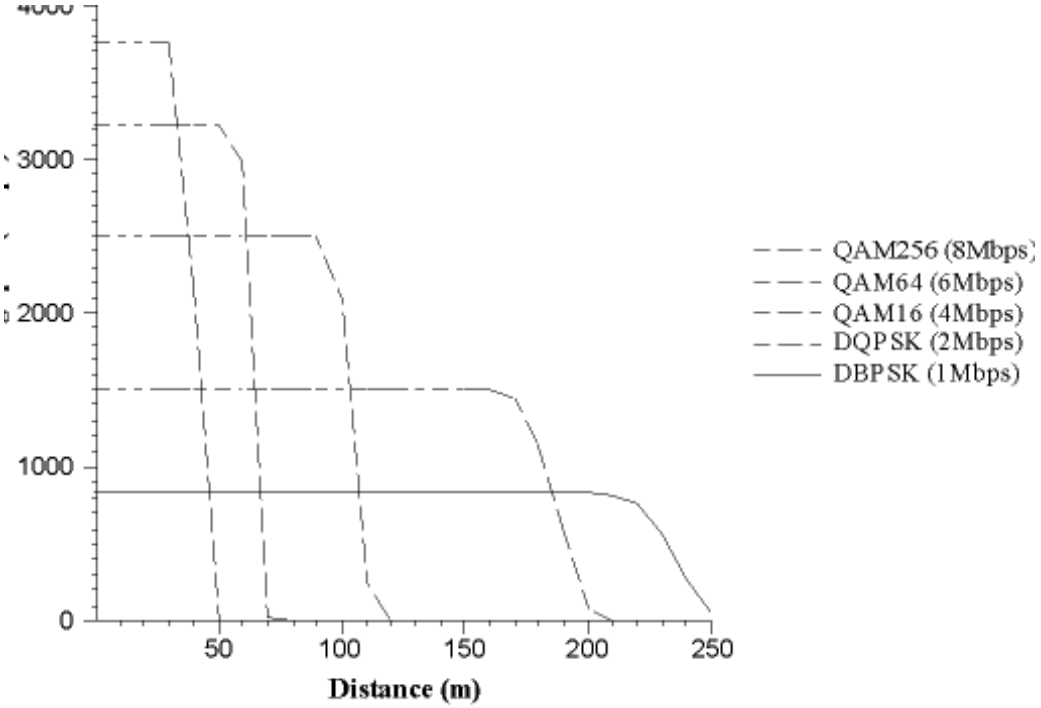
Constelațiile mai bogate necesită putere mai mare!

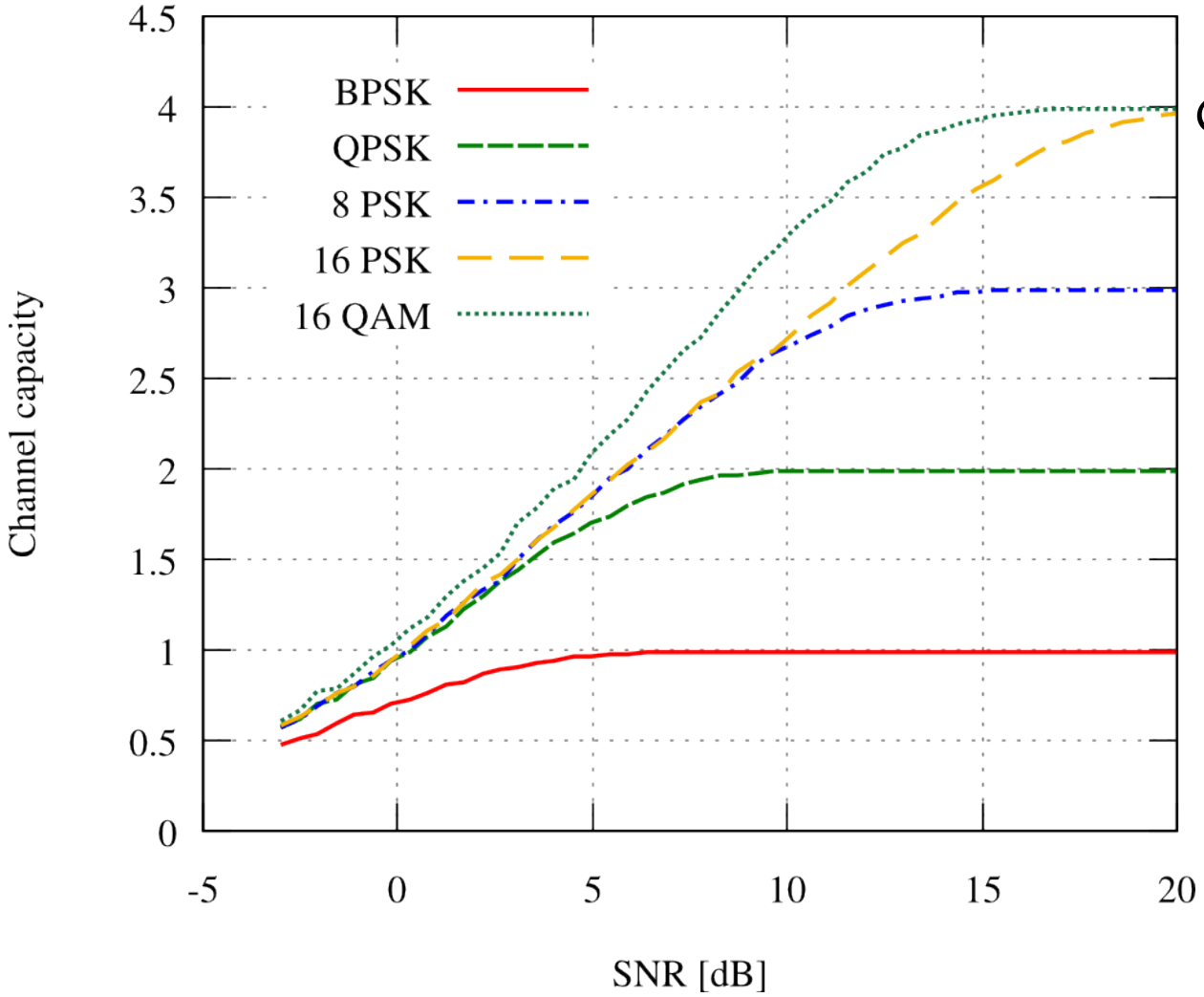
802.11g
54Mpbs (64QAM): -76dbm
48Mbps (64QAM): -71dbm
36Mpbs (16QAM): -78dbm
24Mbps (16QAM): -80dbm
18Mbps (QPSK): -81dbm
12Mpbs (QPSK): -82dbm
9Mbps (BPSK): -85dbm
6Mbps (BPSK): -91dbm
(typically @PER < 10% packet size 1024 and @25oC + 5oC)

Constelațiile mai bogate

- necesită putere mai mare
- Funcționează la distanță mai mică



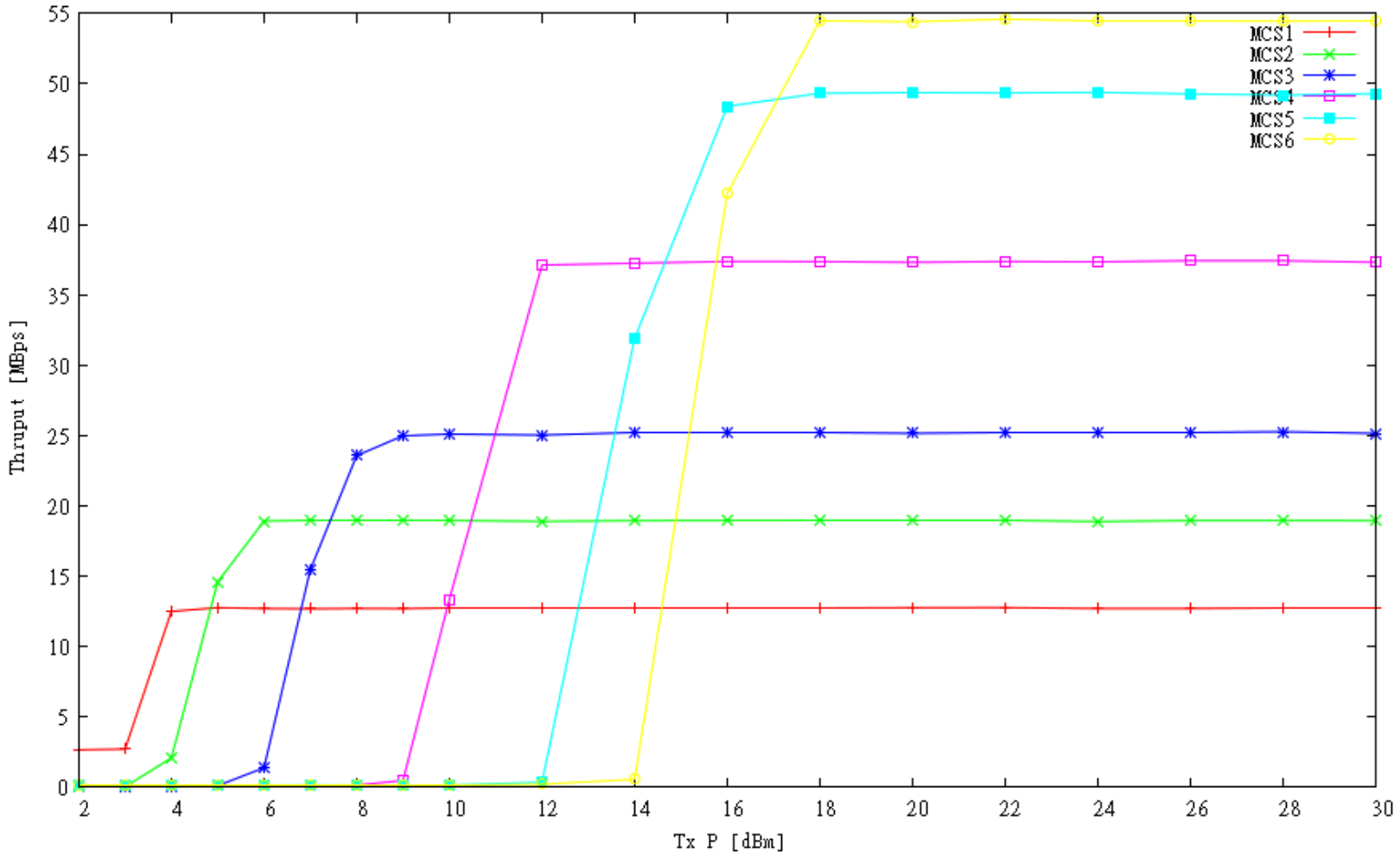




Constelațiile mai bogate

- necesită putere mai mare
- Oferă eficiență b/s/Hz mai bună

Măsurători în Leu corp A, 5.7GHz distanța 10m MCS=1-6:
La creșterea puterii la emisie, constelațiile bogate devin eficiente



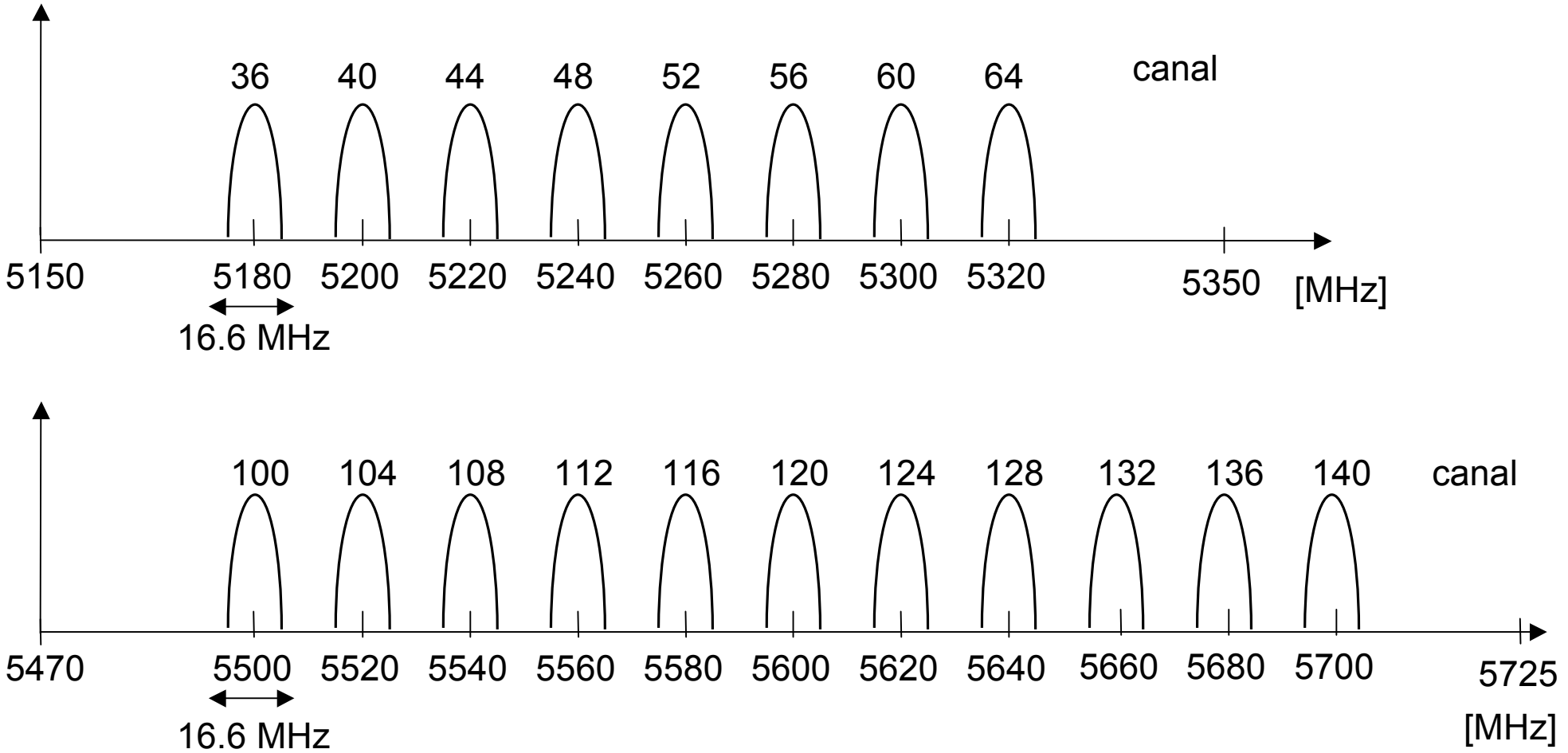
IEEE 802.11a - caracteristici

- rate
  - » 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

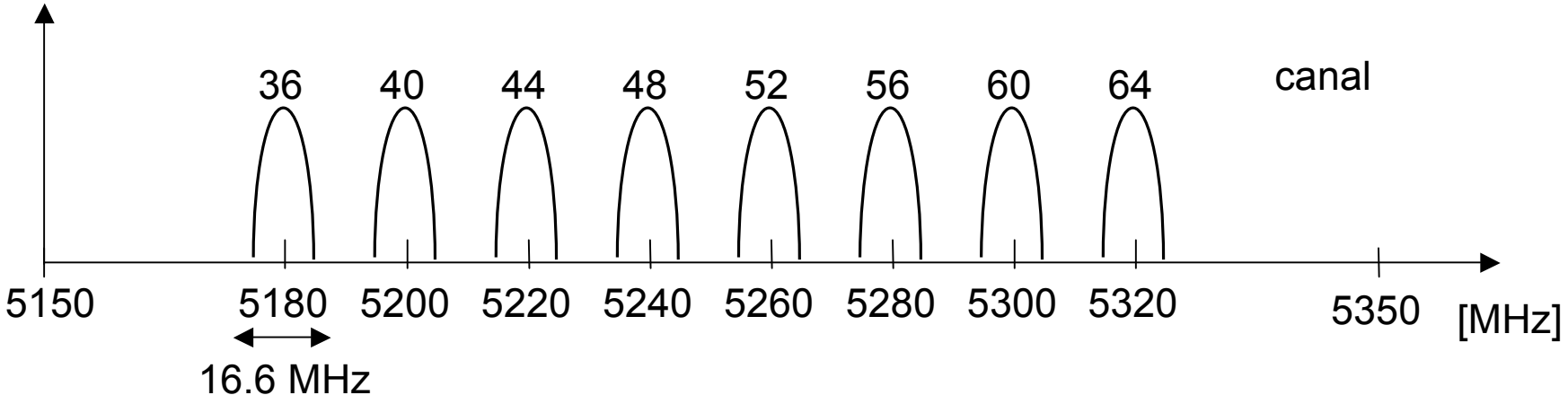
- Dezavantaje:
  - Disponibilitate
    - Mai redusa decat 802.11 b & g
  - » propagare redusa (5GHz)
  - » QoS Inexistent,
    - » best effort
    - » fara garantii
    - » (PCF neimplementat)
  - » Gestiune limitata

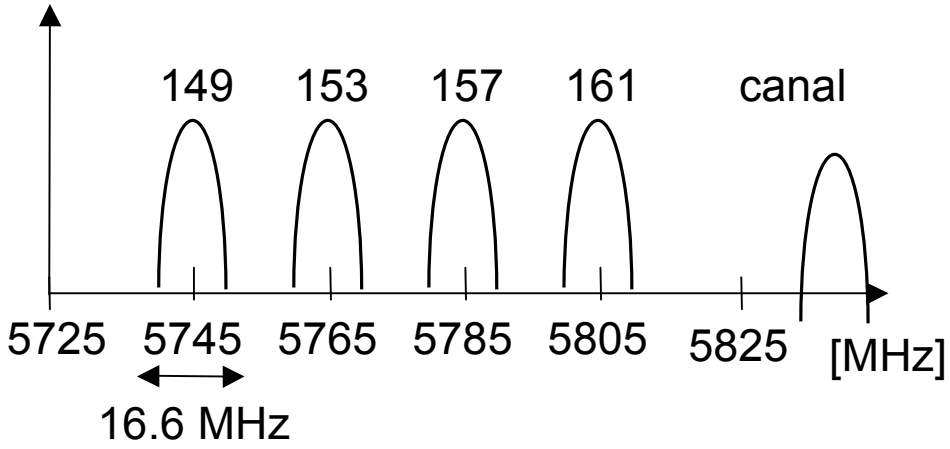
Canale 802.11a (Europa)



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

Canale 802.11a (SUA/Canada)





Frecventa centrala [MHz] =
5000 + 5*canal

Propagare 802.11a

- De ce propagarea este mai slabă la 5GHz?

Free Space Loss = $(4\pi df/c)^n$

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

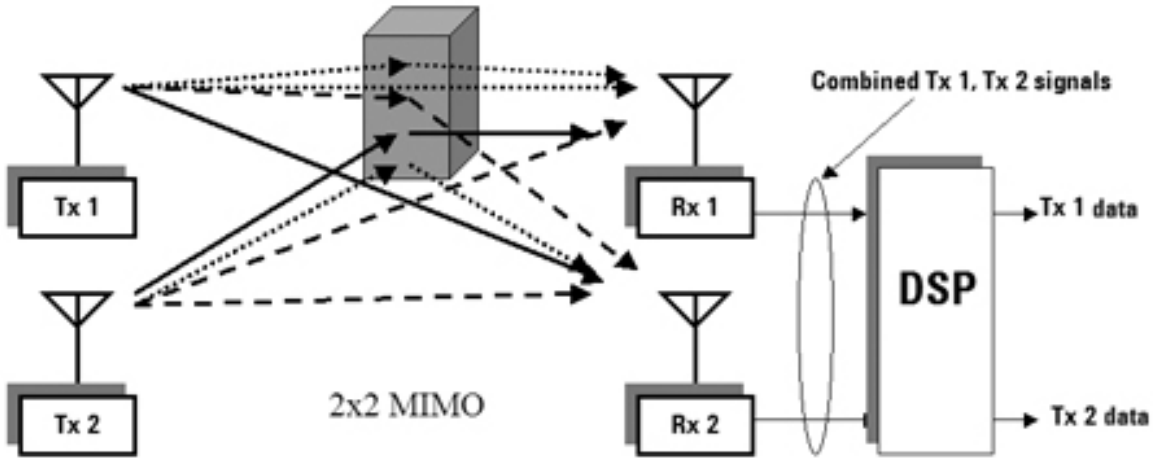
802.11g

- 802.11g : Similar cu 802.11a, dar compatibil cu 802.11b
  - 2.4GHz
  - DSSS/CCK – 1, 2, 5.5, 11 Mbps
  - OFDM – 6, 9, 12, 18, 24, 36, 54 Mbps

- Coexistența cu 802.11b: CTS to self
  - activat doar dacă AP 802.11g vede stații 802.11g
  - CTS folosește DSSS pentru a putea fi decodat de 802.11b
  - conține rezervarea în timp
  - schimbul date/ACK folosește OFDM

802.11n (2009)

- 2.4GHz și 5GHz, backward compatible cu a/b/g
  - Metode de coexistență cu dispozitivele vechi
- MIMO
  - max 4 antene
  - 600Mbps



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

Discuție: consum de putere

Routerboard RB230

- alimentare CC 16V
- 2 carduri Atheros 802.11a
- Computer fără încărcare 2.24W
- Cu 2 carduri pornite +1.44W
- Transmisie
  - CPU + 2.08W
  - Carduri +2.08W
- Total 7.8W
- Un card = 0.72W idle + 1.04W transmisie = 1.76W
- Baterie telefon celular (2009) 3Wh

Subnivelele PHY

Physical layer convergence protocol (PLCP)

Furnizeaza o interfața comuna pentru MAC

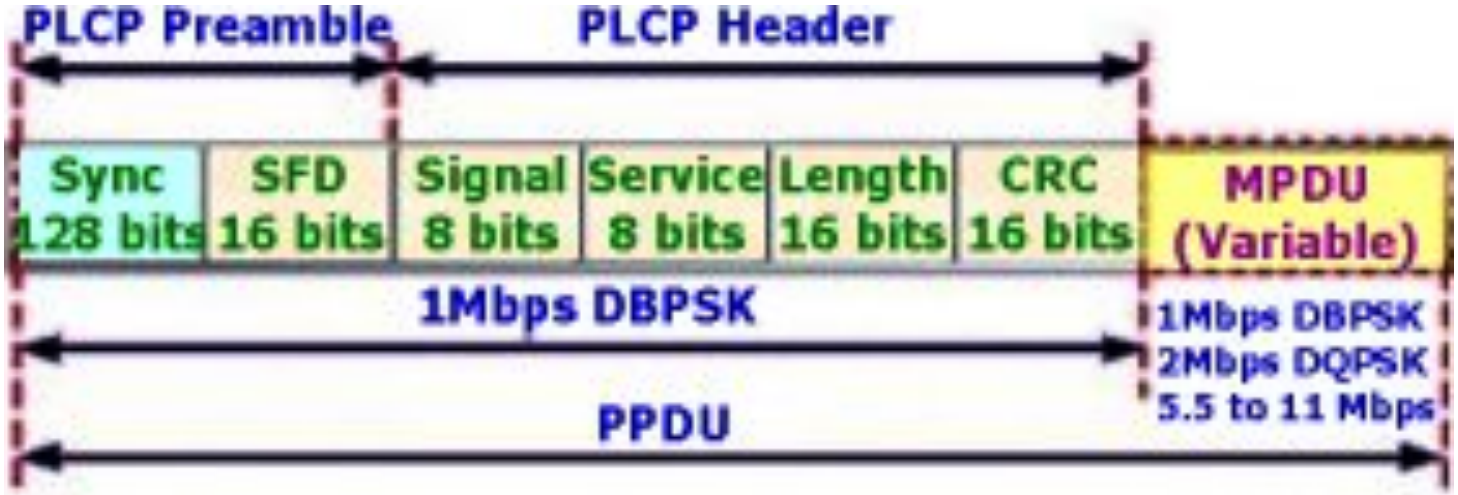
- Ofera detectia purtatoarei (carrier sense) si CCA (clear channel assesment)
- Se ocupa de sincronizarea canalului, antrenare pentru decodare

Physical medium dependent sublayer (PMD)

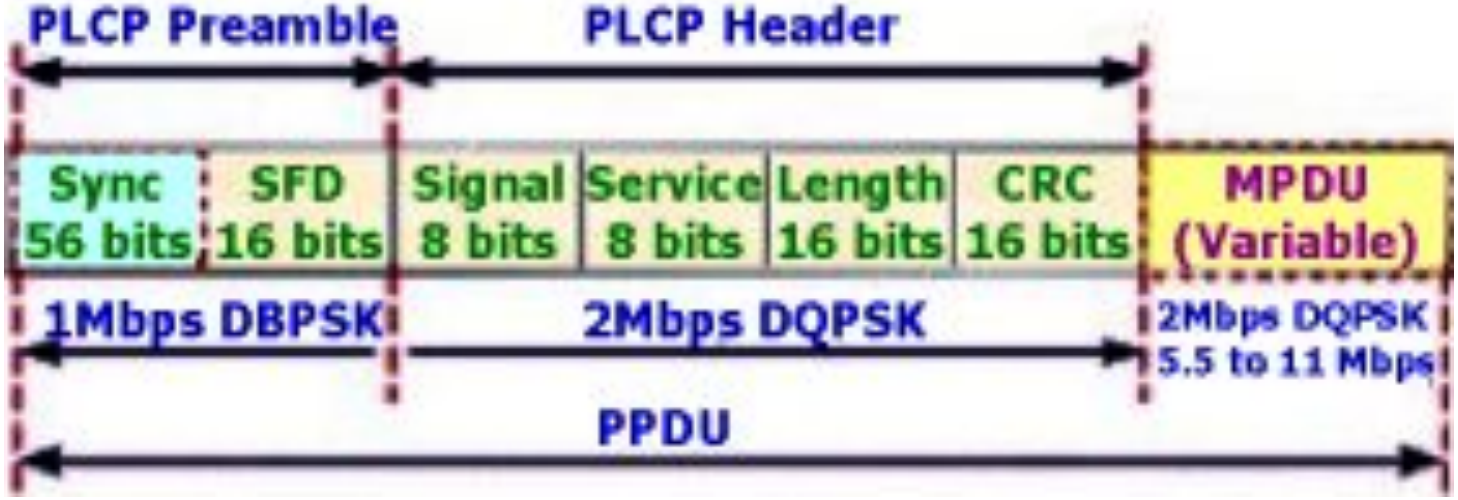
Implementeaza functii care tin de calitatea canalului – decodare/demodulare

Exemplu antet nivel fizic (802.11b)

long preamble 192us



short preamble 96us (VoIP, video)



Nivelul access la mediu

wired == wireless?

- Asemănări cu Ethernet:
  - » wireless e un mediu partajat
  - » interferenta intre transmitatori
  - » CSMA (carrier sense multiple access)
    - – stația emițătoare detectează purtatoarea altei stații
    - – “ascultă înainte de a transmite”
  - » de dorit:
    - – o singură stație transmite la un moment dat
    - – eficiență, echitate
- Diferențe:
  - » CD (detectia coliziunilor) dificilă:
    - – O singura antenă, comunicare simplex
  - » Canale de calitate slabă: BER, variabilitate in spatiu/timp
  - » Terminal ascuns, terminal expus

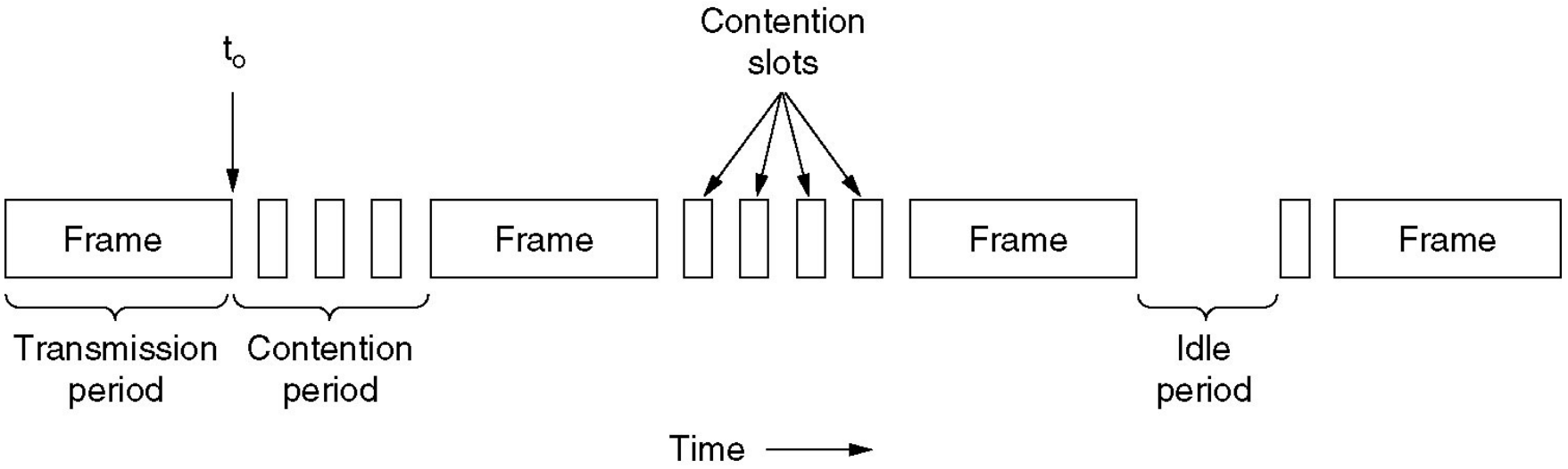
Carrier Sense

- 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)

Recapitulare Ethernet

CSMA/CD = carrier sense multiple access with collision detection

Ethernet - CSMA/CD

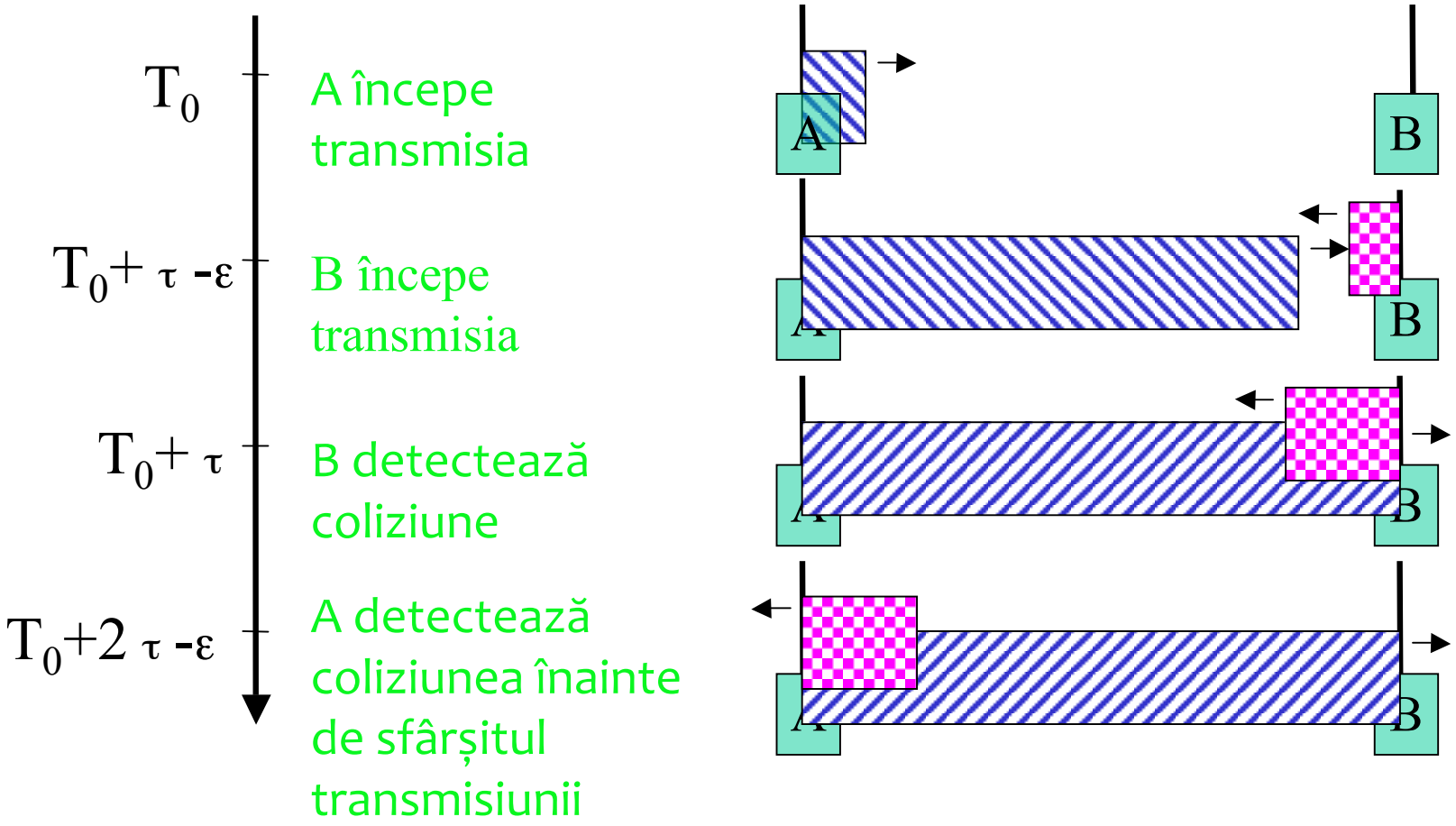


Cât durează detecția coliziunii?

- Depinde de timpul de propagare între stații τ
- Rezultă că după τ, canalul este ocupat de o stație transmițătoare?

NU, de fapt e nevoie de RTT => 2τ

Ethernet:CSMA/CD: exemplu detecție



Ethernet: CSMA/CD

De ce este nevoie de lungime minimă de 64 octeți la cadrul Ethernet?

- Pt LAN 10Mbps, 2500m, 4 repetoare 2t = 50ms
  - 1bit = 100ns => sunt necesari 500biți pentru cadrul cel mai scurt
- Ce se întâmplă când crește banda?
  - Este nevoie de cadre minime mai lungi, sau
  - Lungime cablu redusă

Lungime minimă 512 octeți pentru Giga Ethernet 802.3z (1998)

- Cadrul este extins după câmpul Checksum
- Doar pentru half-duplex. De ce?

Ethernet: regresie binară exponențială

- Un slot este de 512biți (51.2us pt 10Mbps)

ALGORITM

- După coliziunea *k*, se așteaptă aleator între 0 și 2^k -1sloturi
- După 10 coliziuni, intervalul maxim de așteptare rămâne 1023 sloturi
- După 16 coliziuni, se raportează pierderea nivelului superior

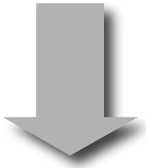
- Scop: adaptarea dinamică la numărul de stații
- Neajuns: CSMA/CD nu oferă confirmări (ACK), deși ar fi posibil

Două observatii despre CSMA/CD

1. Transmițătorul poate trimite/asculta simultan

   if (trimis - primit == 0) then succes

2. Semnalul este aproape identic la Tx si Rx

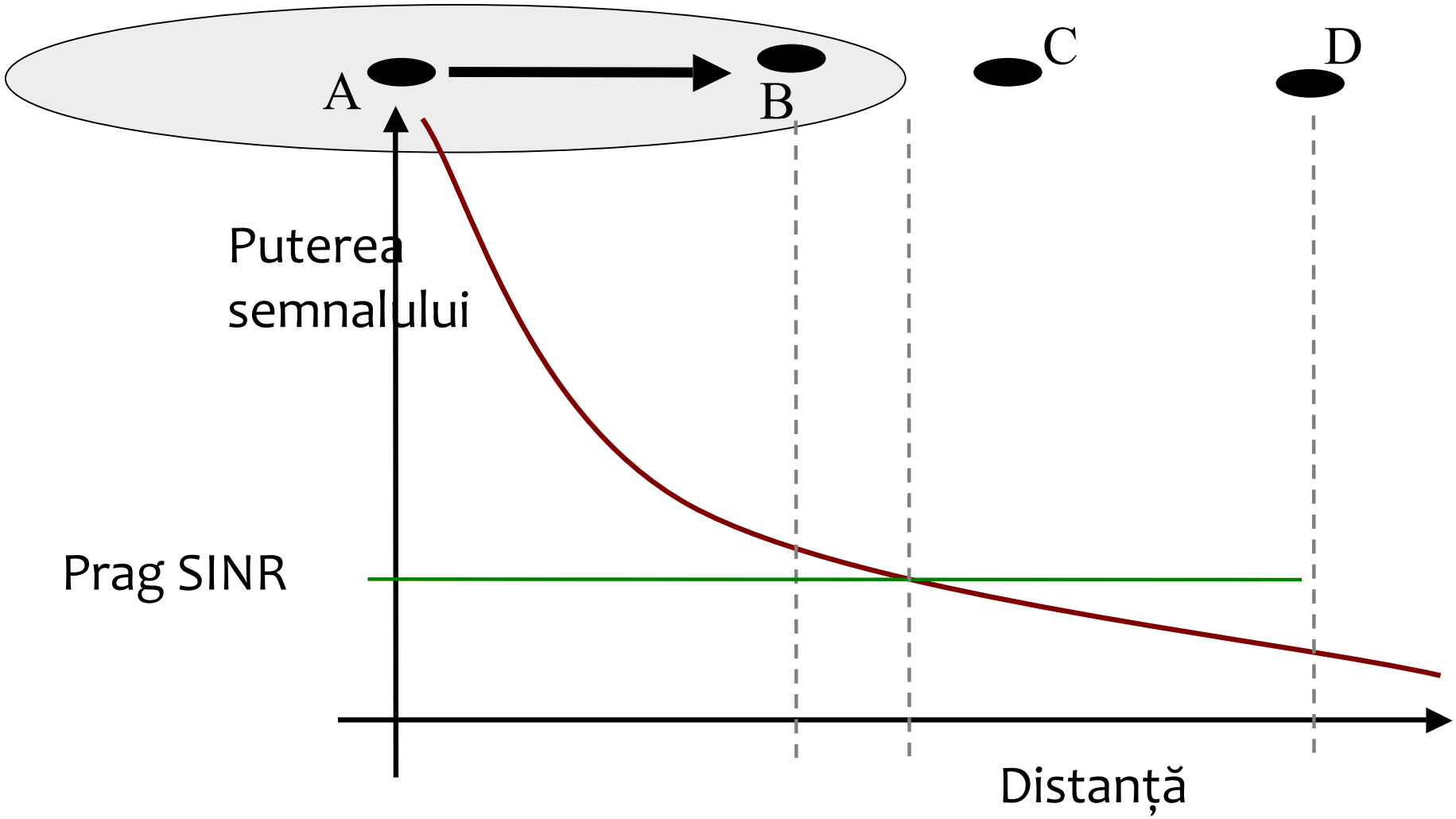


TRANSMIȚĂTORUL poate detecta dacă și când se produce coliziunea

Din nefericire…

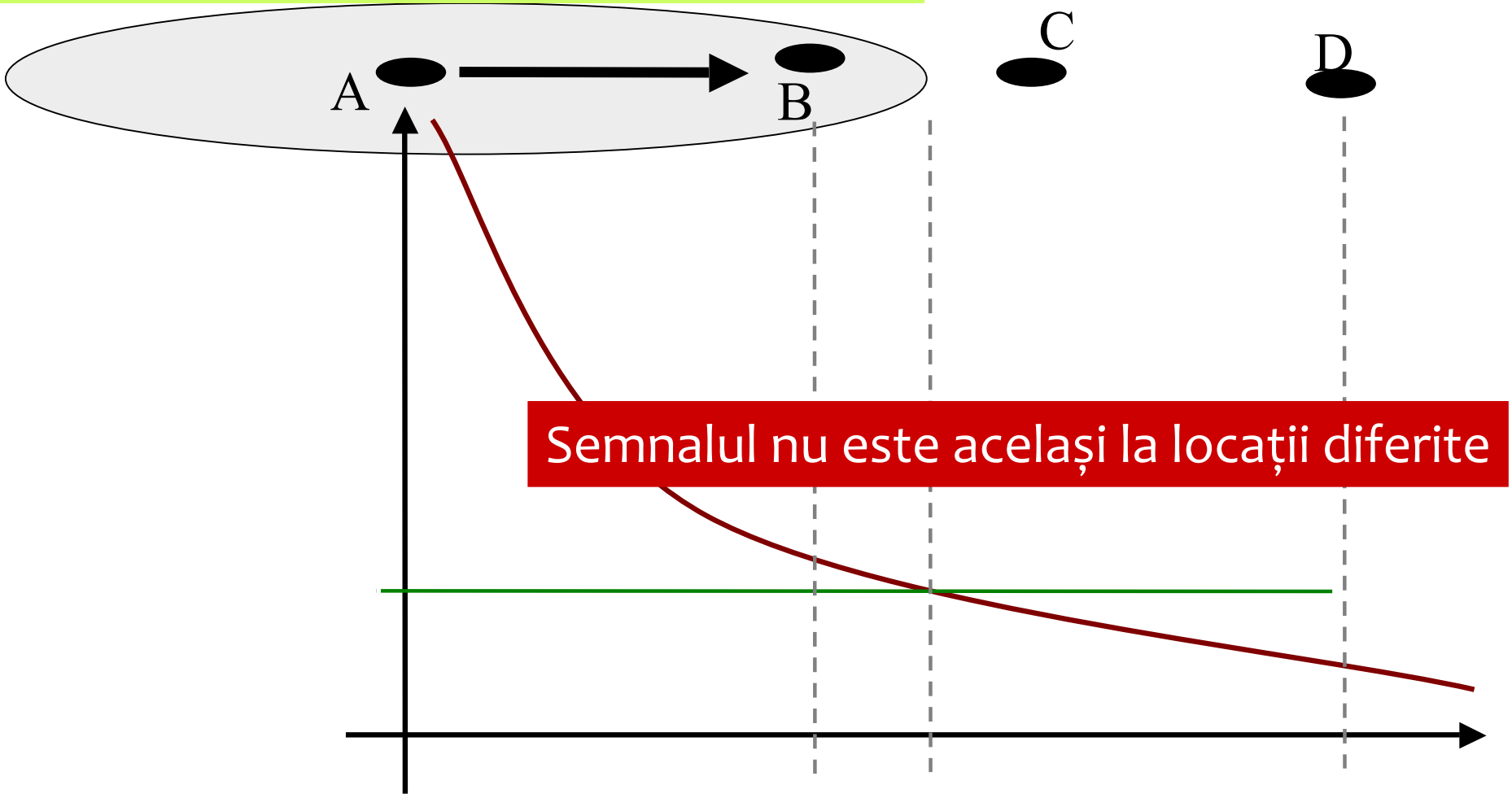
Nici una din cele două observații nu este valabilă în wireless, deoarece…

Wireless MAC

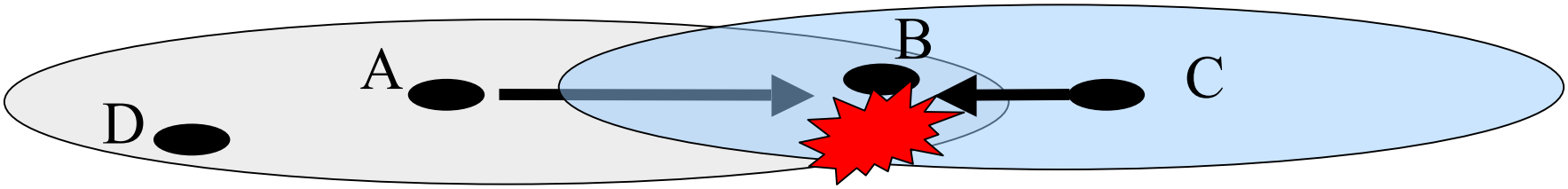


Mediul wireless disperseaza energia

A nu poate trimite și recepționa simultan



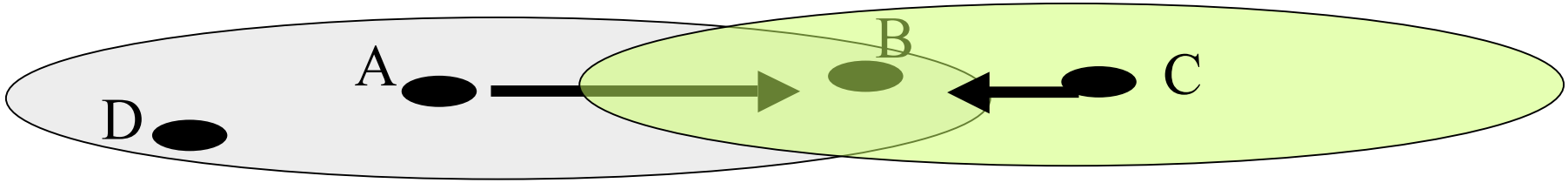
Detecția coliziunilor dificilă



Recepția semnalelor bazată pe SINR

- Transmițătorul se aude doar pe sine
- Nu poate estima calitatea semnalului la receptor

Calculul SINR

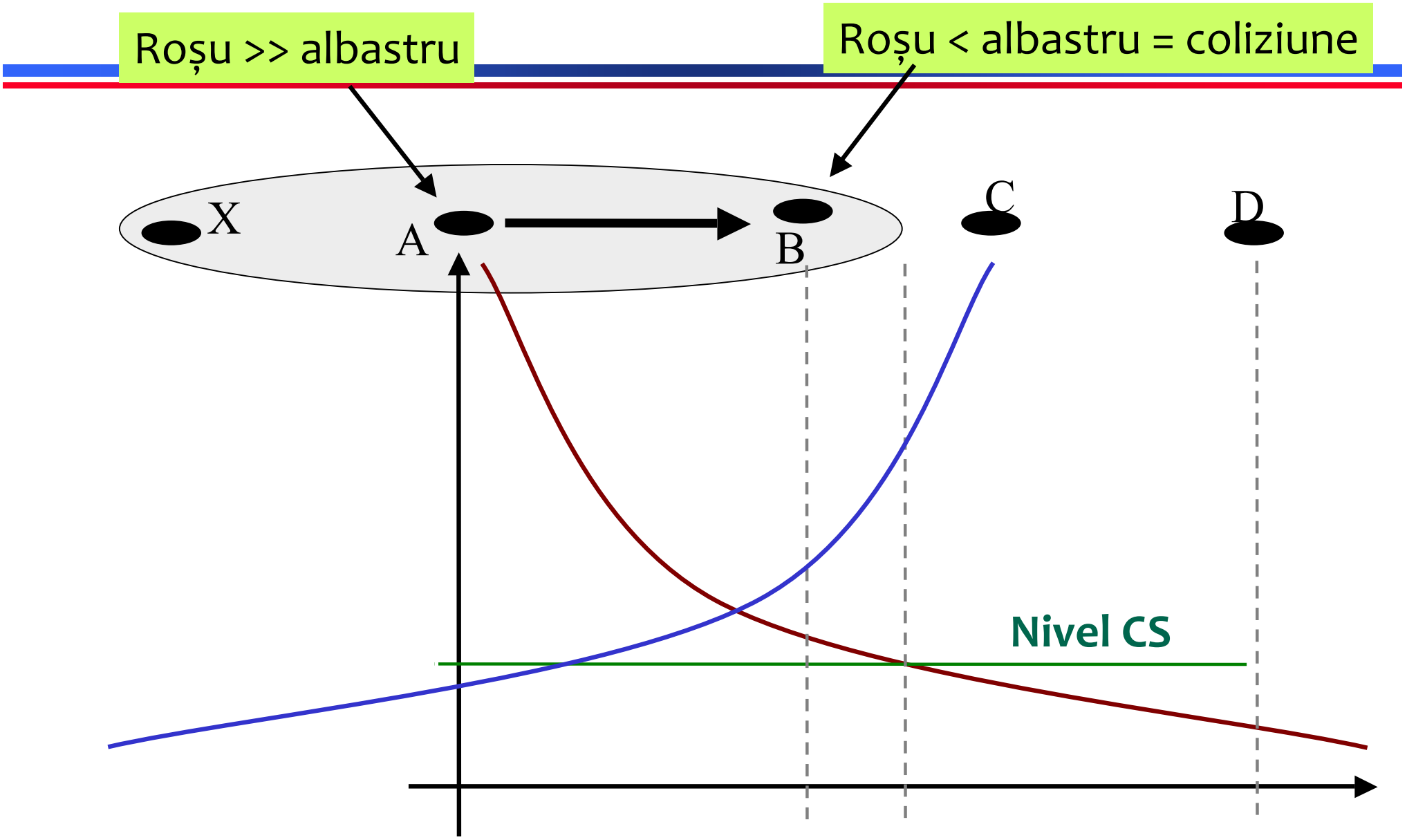


$$SINR = \frac{Semnal(S)}{Interferenta(I) + Zgomot(N)}$$

$$S_B^A = \frac{P^A_{transmit}}{d_{AB}^{\alpha}}$$

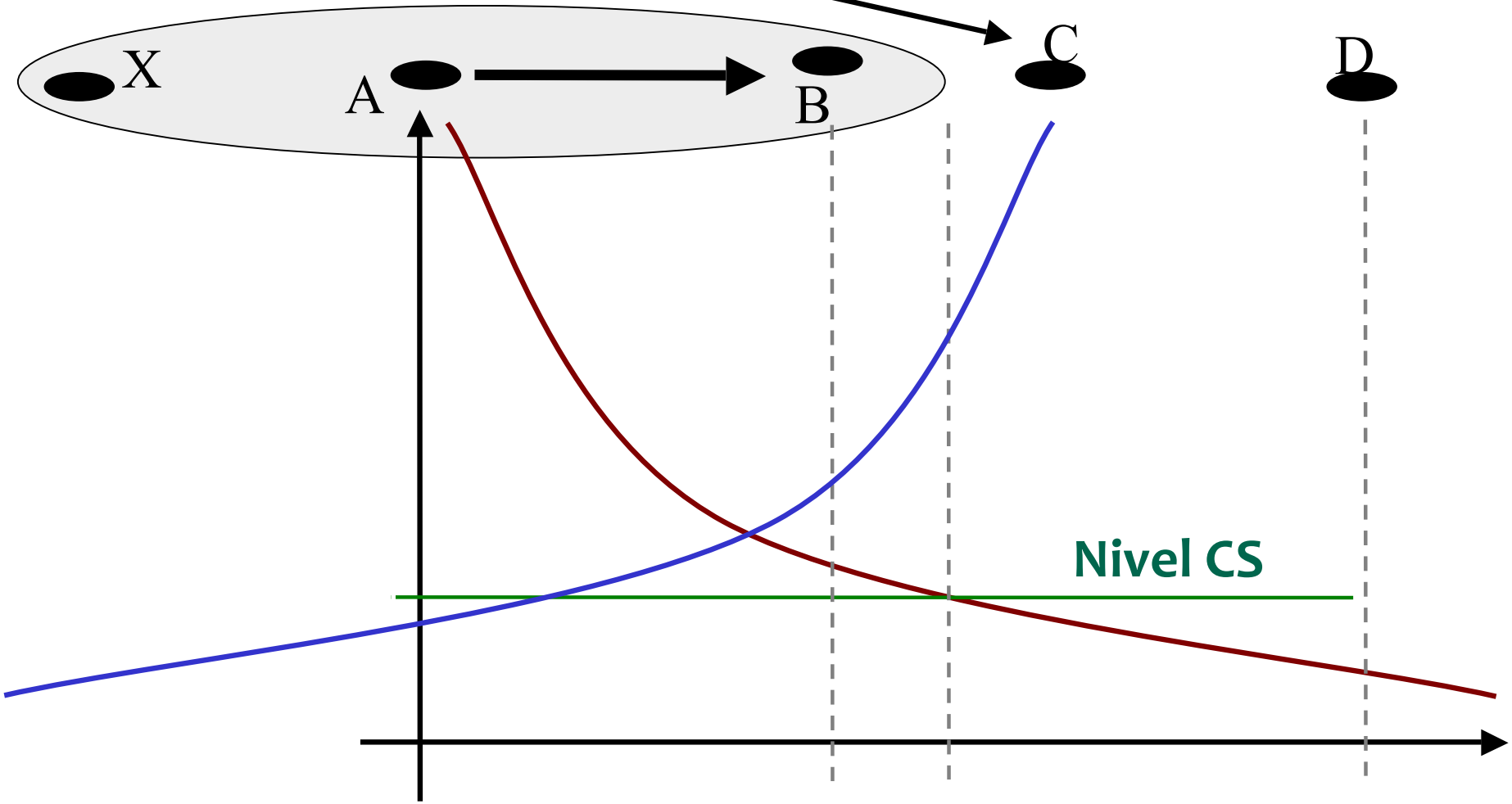
$$I_B^C = \frac{P^C_{transmit}}{d_{CB}^{\alpha}}$$

$$\rightarrow \quad SINR_B^A = \frac{\frac{P^A_{transmit}}{d_{AB}^{\alpha}}}{N + \frac{P^C_{transmit}}{d_{CB}^{\alpha}}}$$


Roșu >> albastru
Roșu < albastru = coliziune
X
A
B
C
D
Nivel CS

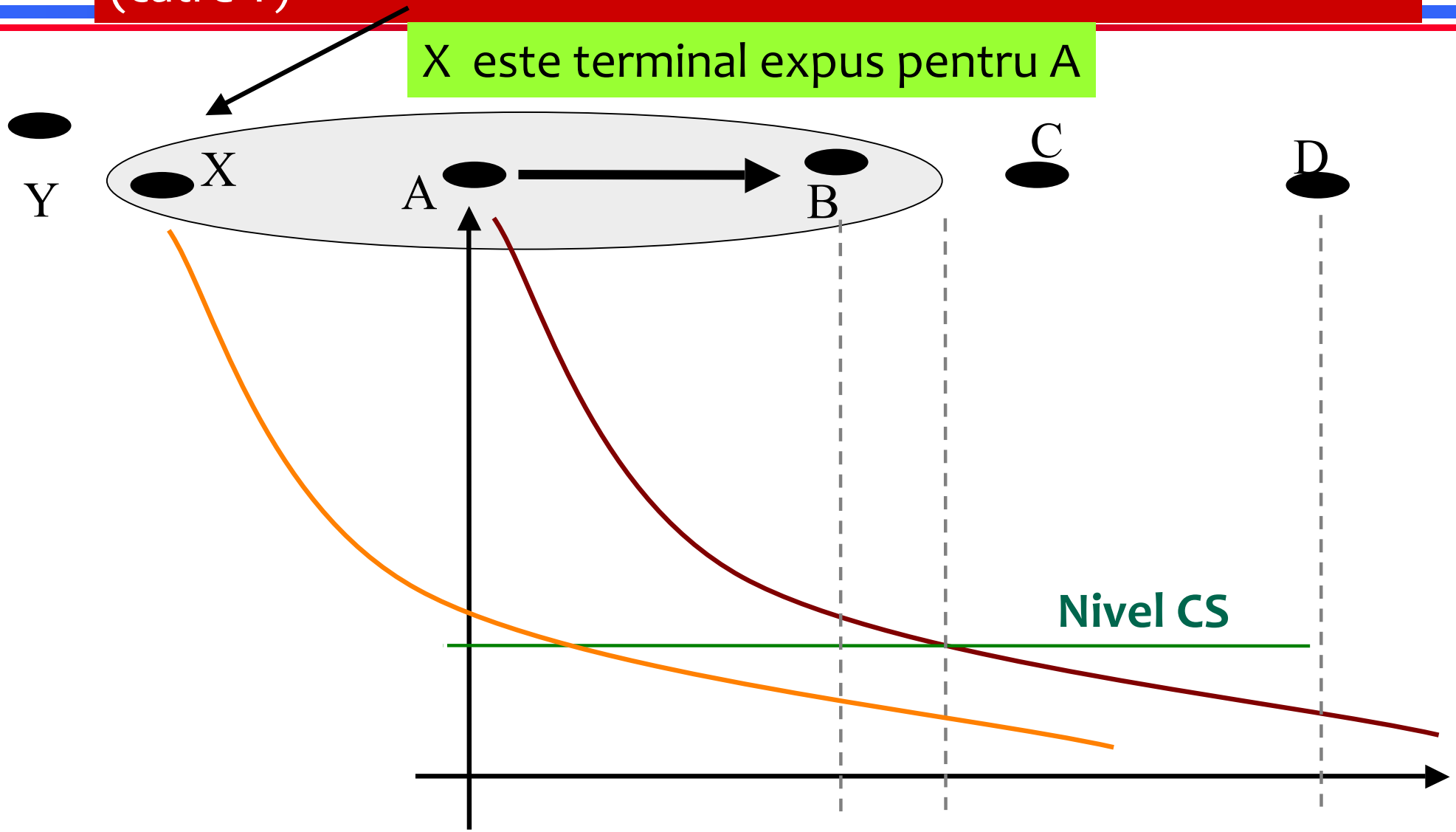
Important: C nu-l aude pe A, produce interferenta la B

C este terminal ascuns pt A



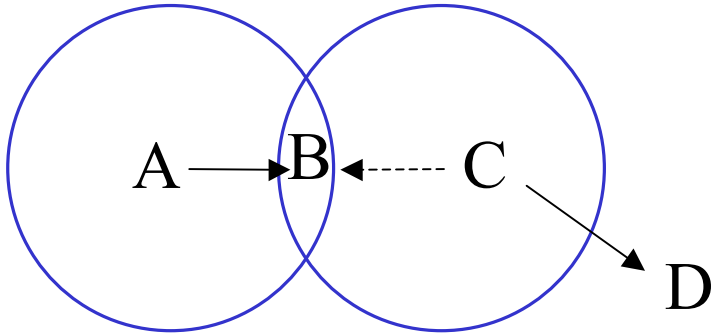
Important: X îl aude pe A, dar nu nu trebuie să cedeze accesul (catre Y)

X este terminal expus pentru A

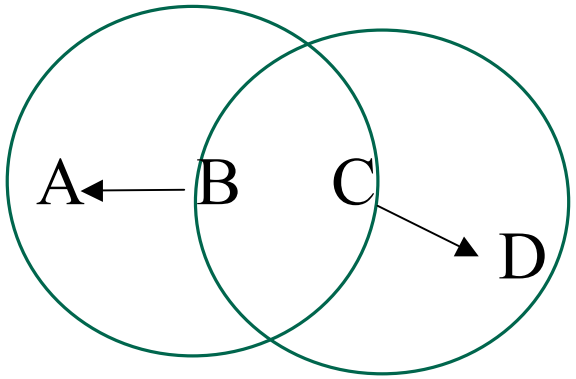


Sumar terminale ascunse, expuse

- Terminal ascuns
  - » A si C pot transmite in acelasi timp

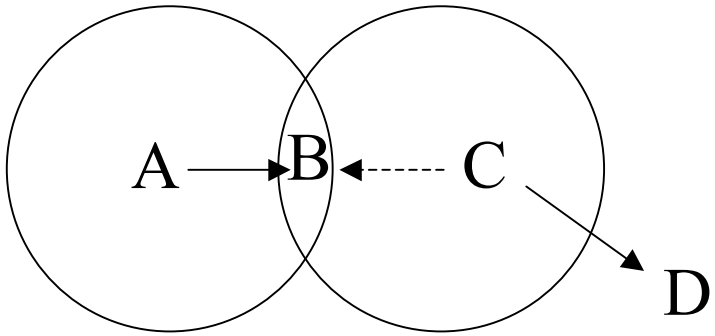


- Terminal expus
  - » B si C nu pot transmite in acelasi timp



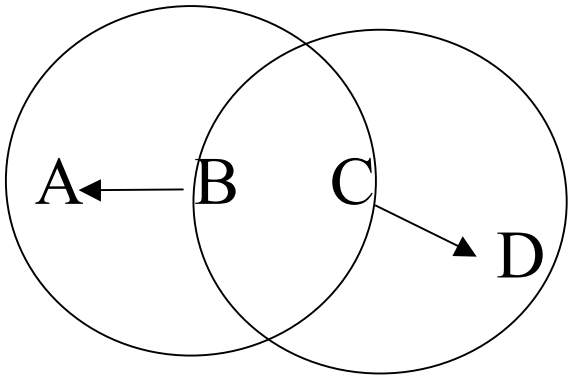
terminale ascunse, expuse

- Situațiile reale sunt rareori doar TA sau doar TE
  - canale asimetrice
  - hardware diferit
  - Combinații de TA, TE



- Captura: TA, dar la B $P_A > P_C + 10dB$

- TE asimetric: doar B aude pe C => lipsa de echitate între debitele BA și CD

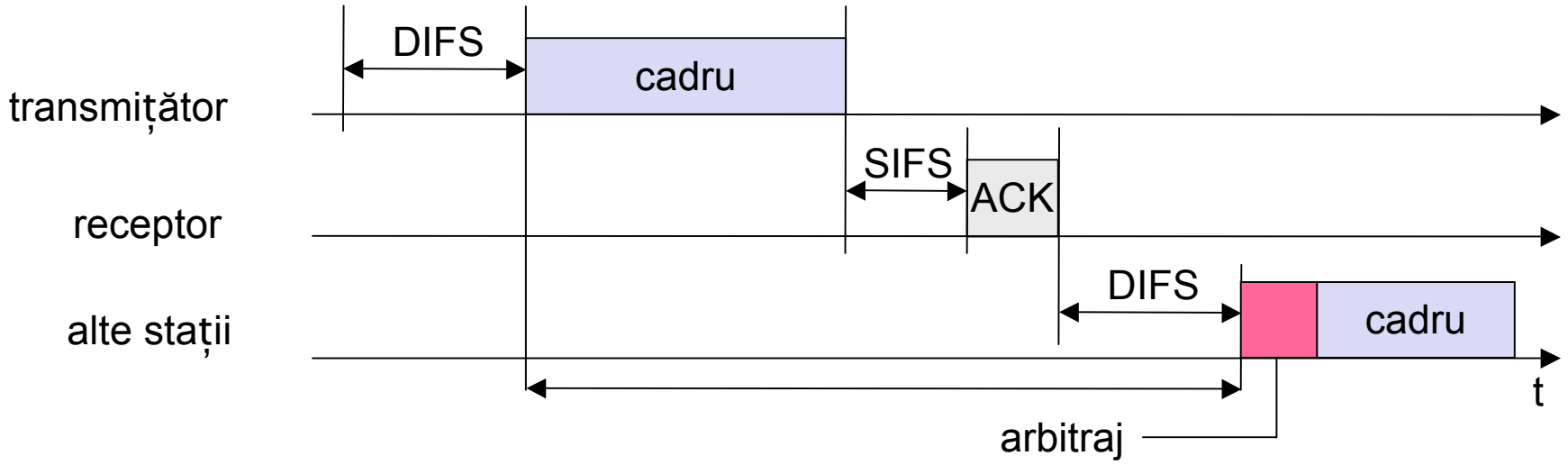


802.11 - MAC

- 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
  - *PCF (optional)*
    - *AP ofera accesul pe baza unei liste*

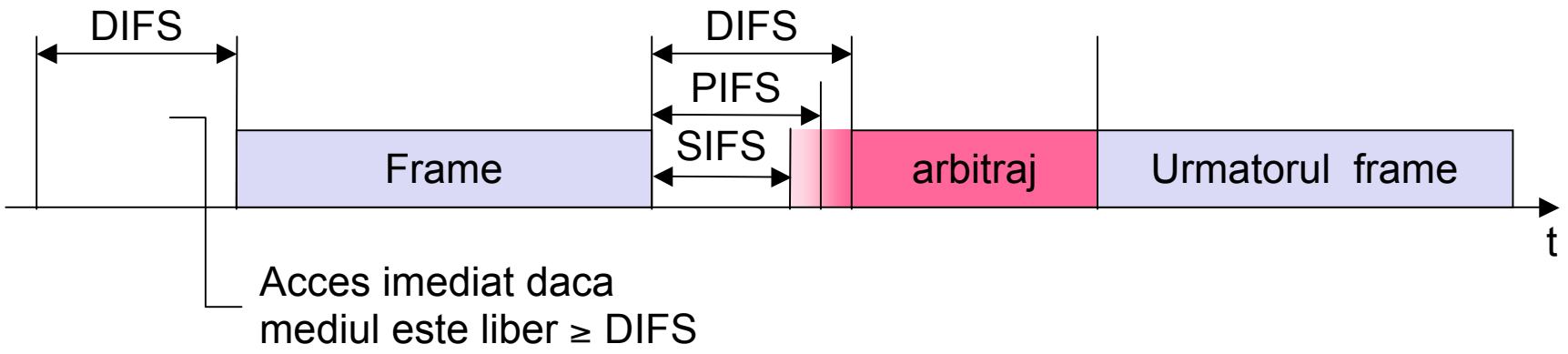
802.11 Date unicast

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

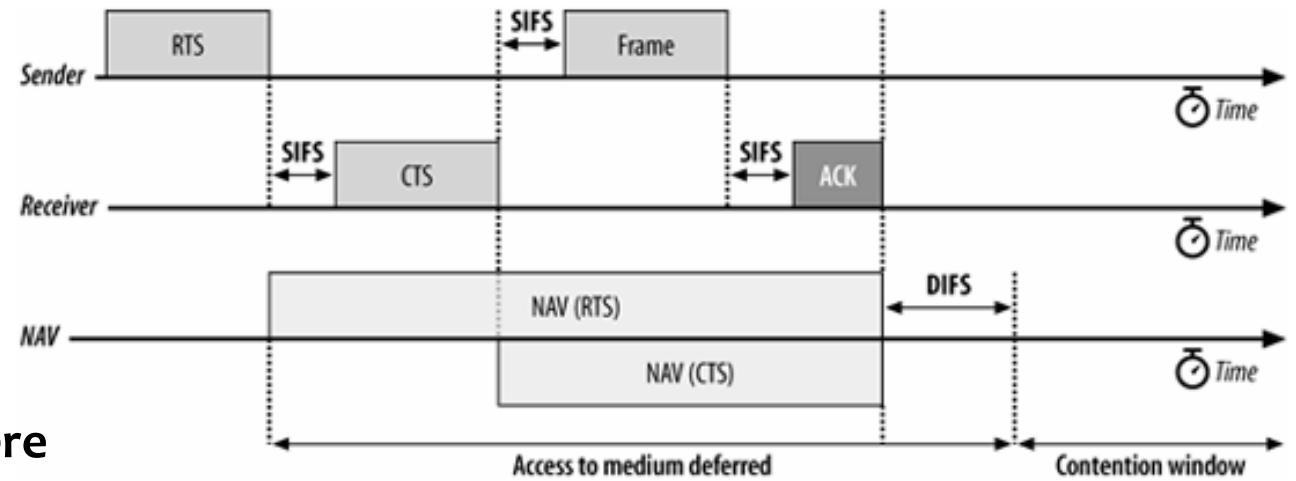


802.11 - MAC

- IFS - inter frame space
- Prioritati
  - » 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
  - » PIFS (PCF IFS)
    - – prioritate medie, pentru serviciul sincron PCF



Carrier sense (detecția purtătoarei)



Detecția purtătoarei

- **Fizic – nivel de putere**
- **Virtual – NAV**

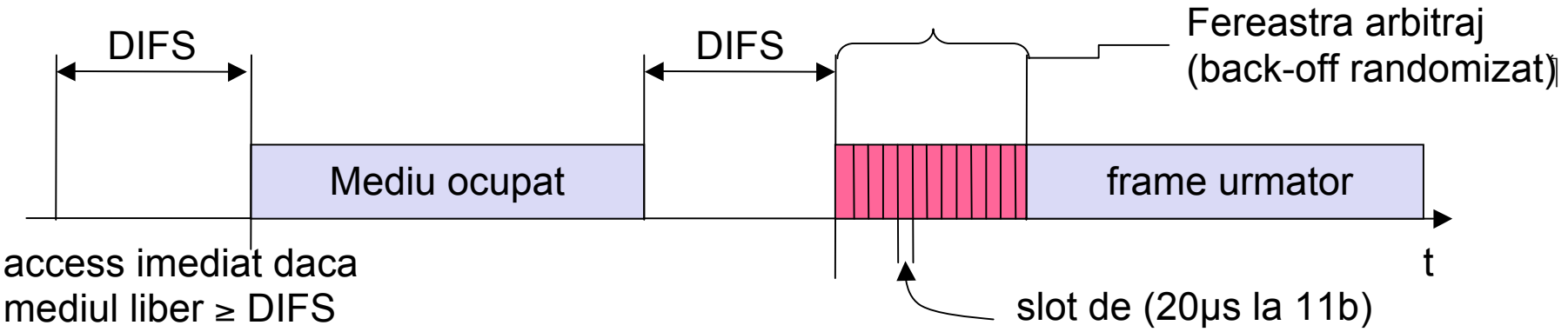
NAV (network allocation vector)

- **Un timer care indică durata pentru care mediul este rezervat (ms)**
- **NAV!=0 => mediul este ocupat**
- **Majoritatea cadrelor 802.11 conțin un câmp 'durată'**
- **Se folosește pentru operațiuni atomice (unitare)**
  - **RTS/CTS/Date/ACK**
  - **Date/ACK**

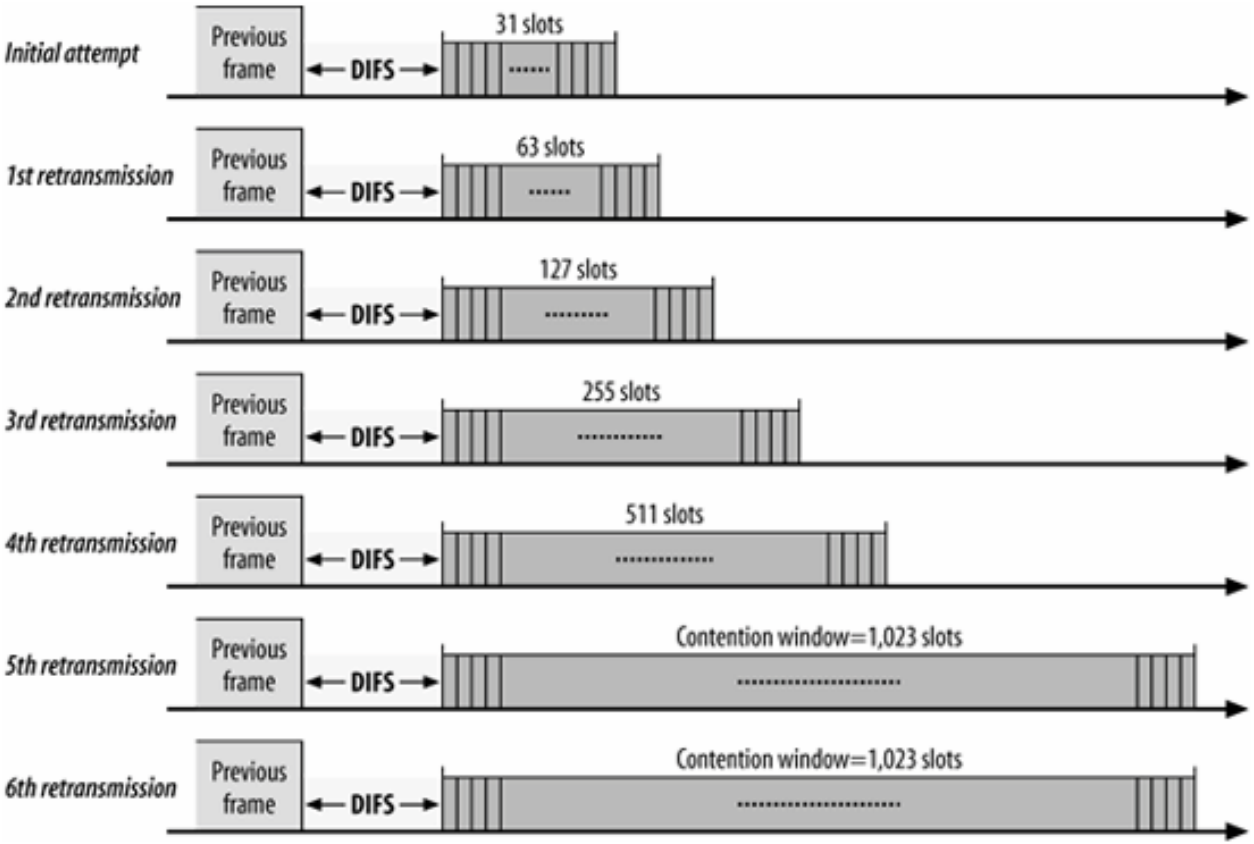
802.11 - CSMA/CA

Important!

- statia evaluează daca mediul e liber (Carrier Sense)
- mediu liber pentru DIFS => se poate transmite imediat
- mediu ocupat => statia așteaptă DIFS liber, apoi se asteaptă 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)



Standard	Slot [μs]	SIFS [μs]	DIFS [μs]	CW	
11b	20	10	50	31-1023	
11a	9	16	34	15-1023	
11g	9	10	28	15-1023	
11n/2.4GHz	9	10	28	15-1023	
11n/5GHz	9	16	34	15-1023	

DIFS: Care este regula?

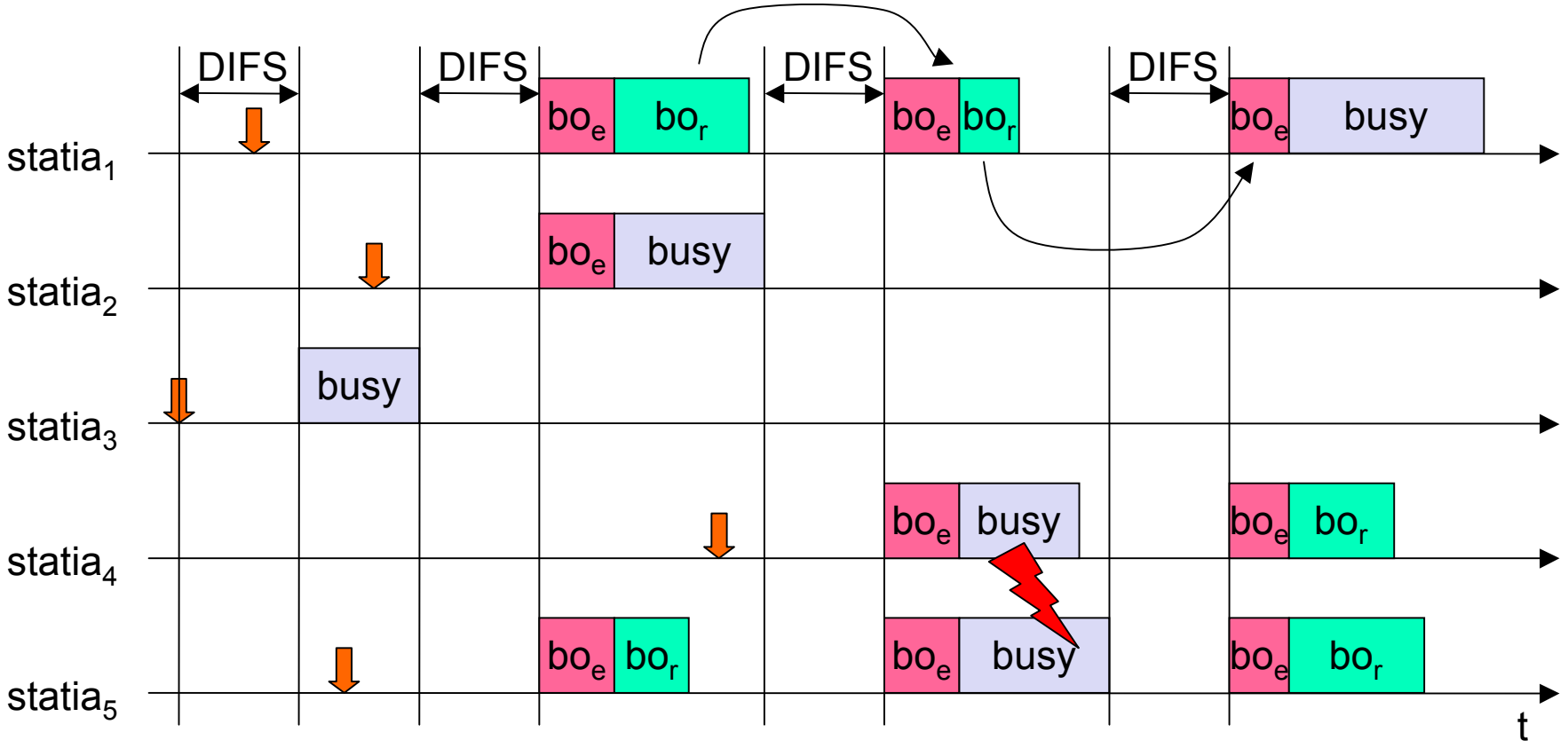
802.11 unicast la distanță mare

- La distanță mare, lungimea slotului și ACK timeout trebuie modificate
- 300m~1μs

- ACK timeout depinde de fabricant
- ACK Timeout = SIFS + Air Propagation Time (max) + Time to transmit 14 byte ACK frame [14 * 8 / bitrate in Mbps] + Air Propagation Time (max)
- Slottime = MAC and PHY delays + Air Propagation Time (max)

- exemplu Atheros ACK timeout pentru 802.11a
  - default 22μs
  - maximum 409μs (61km)
  - Atenție la DIFS!

802.11 - exemplu 5 stații



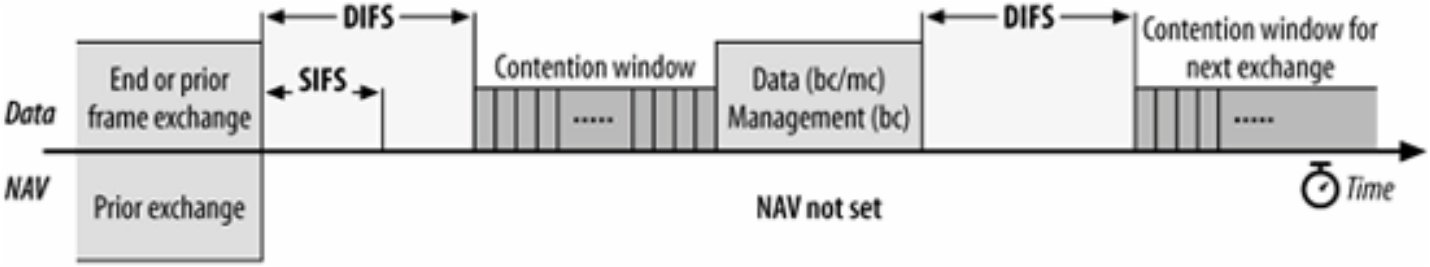
busy — Mediu ocupat (frame, ack etc.)

bo_e — backoff expirat

Un pachet devine disponibil

bo_r — backoff rămas

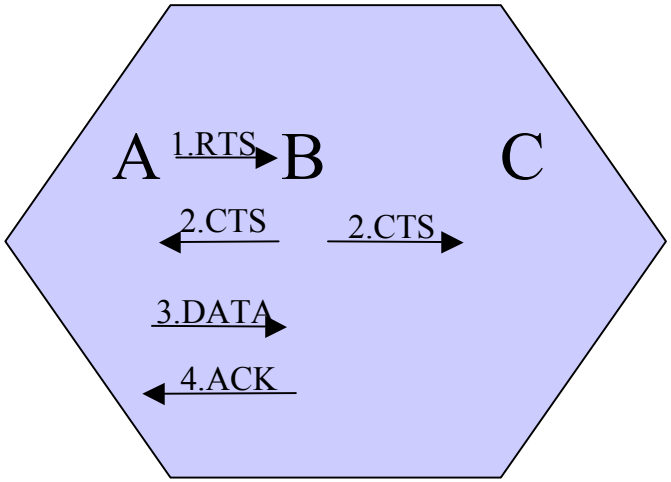
802.11 date broadcast

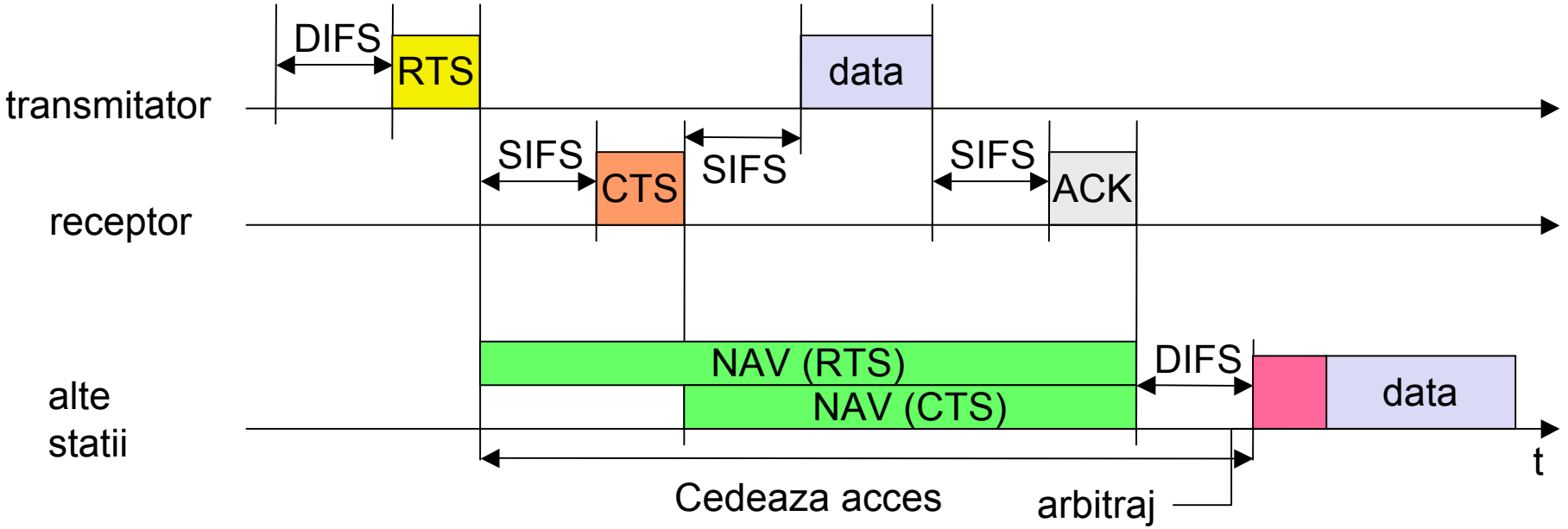


- nu se fragmentează,
- nu se confirmă
- nu se folosește NAV

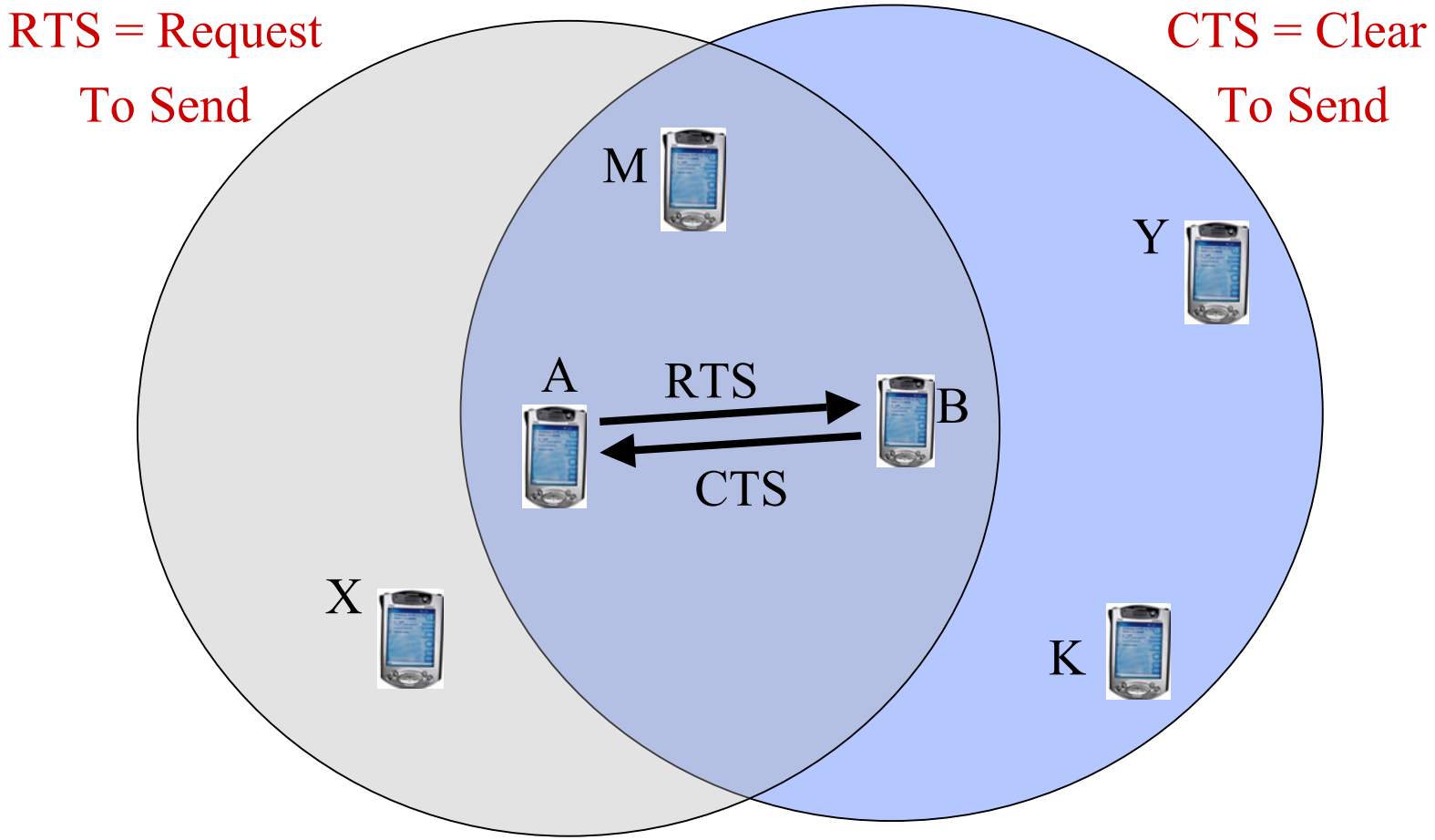
802.11 - RTS/CTS

- pentru pachete unicast
  - » Transmitator: RTS cu rezervare (rezerva timpul necesar)
  - » Receptor: CTS
  - » Transmitator: frame
  - » Receptor: ACK
  - » Celelalte statii mentin NAV
  - » RTS threshold

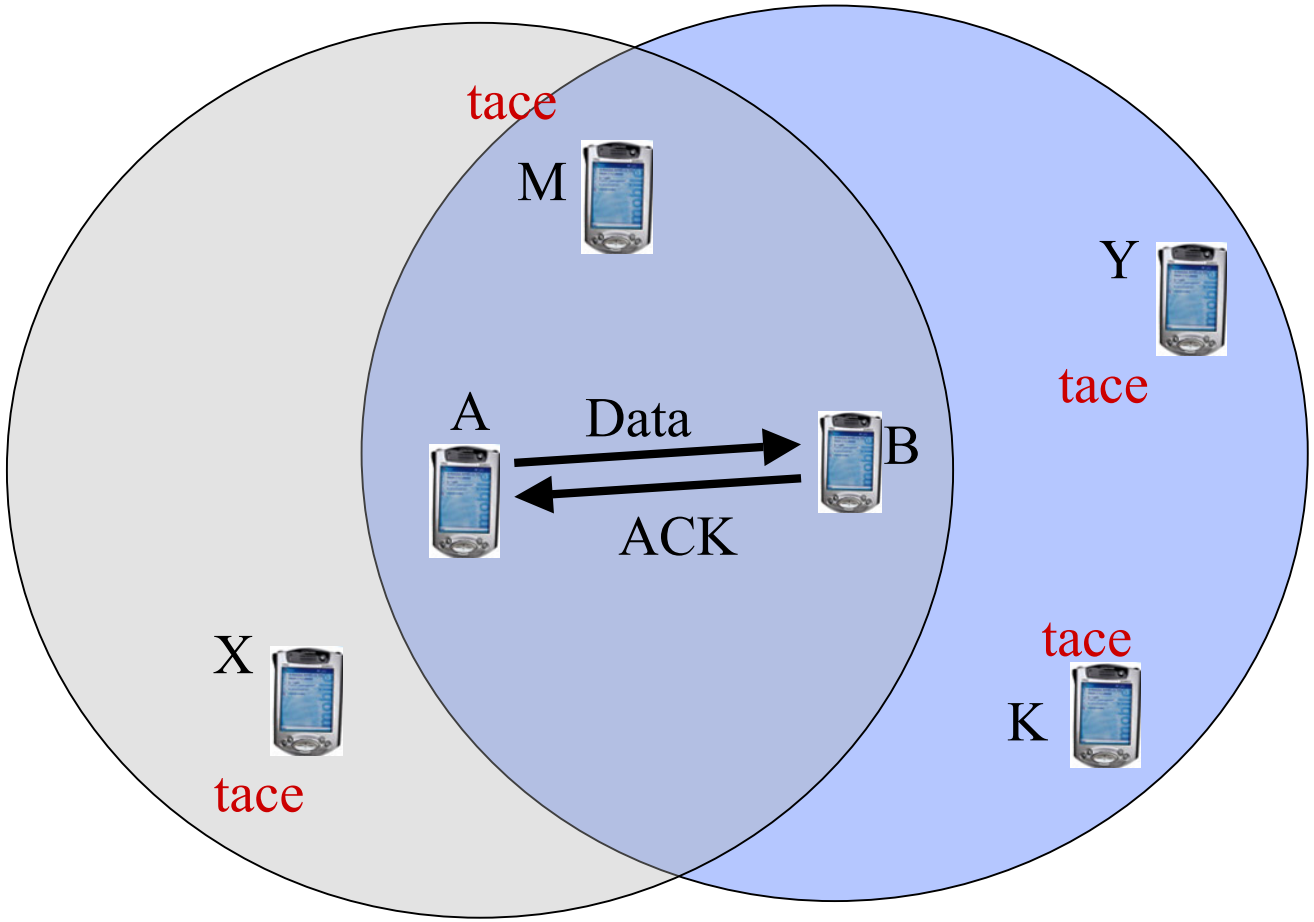




802.11 RTS/CTS



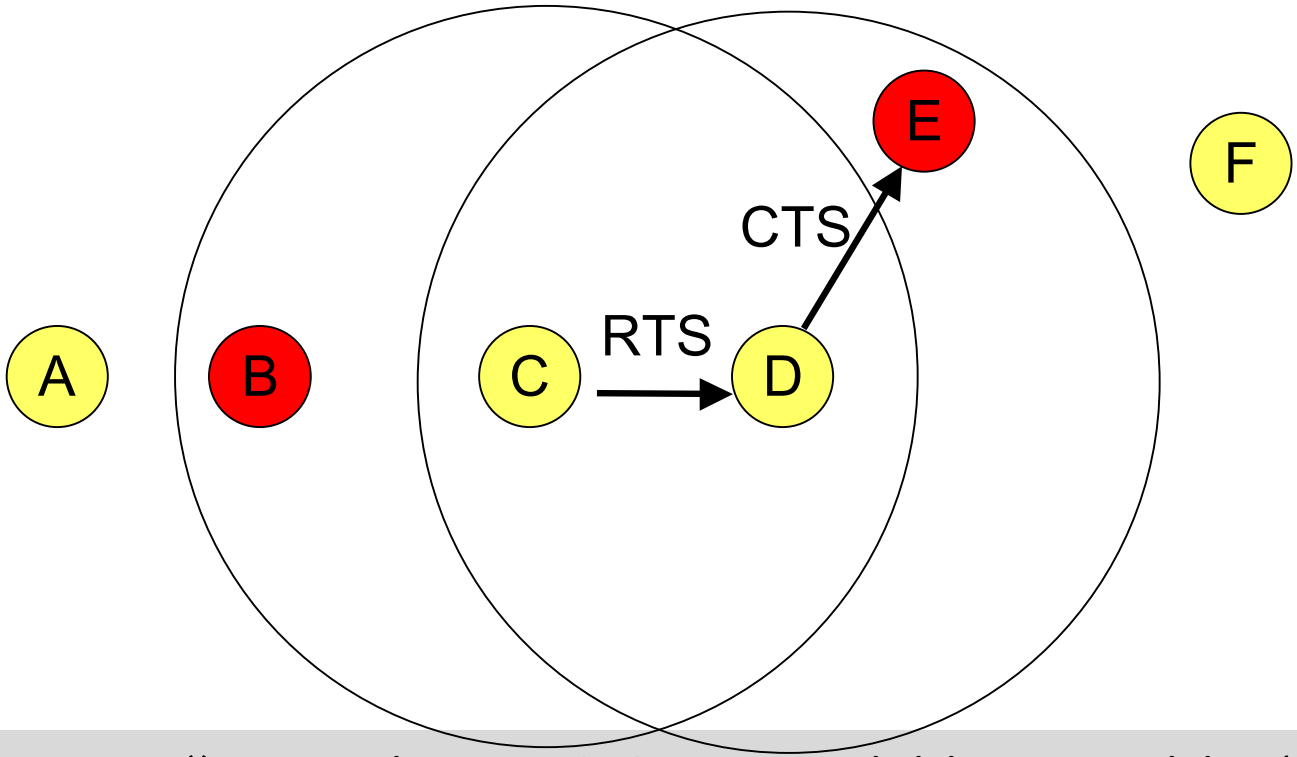
802.11 RTS/CTS



Terminal ascuns cu RTS/CTS

Rezolva problema terminalelor ascunse?

Exemplu zona CS = zona de comunicare

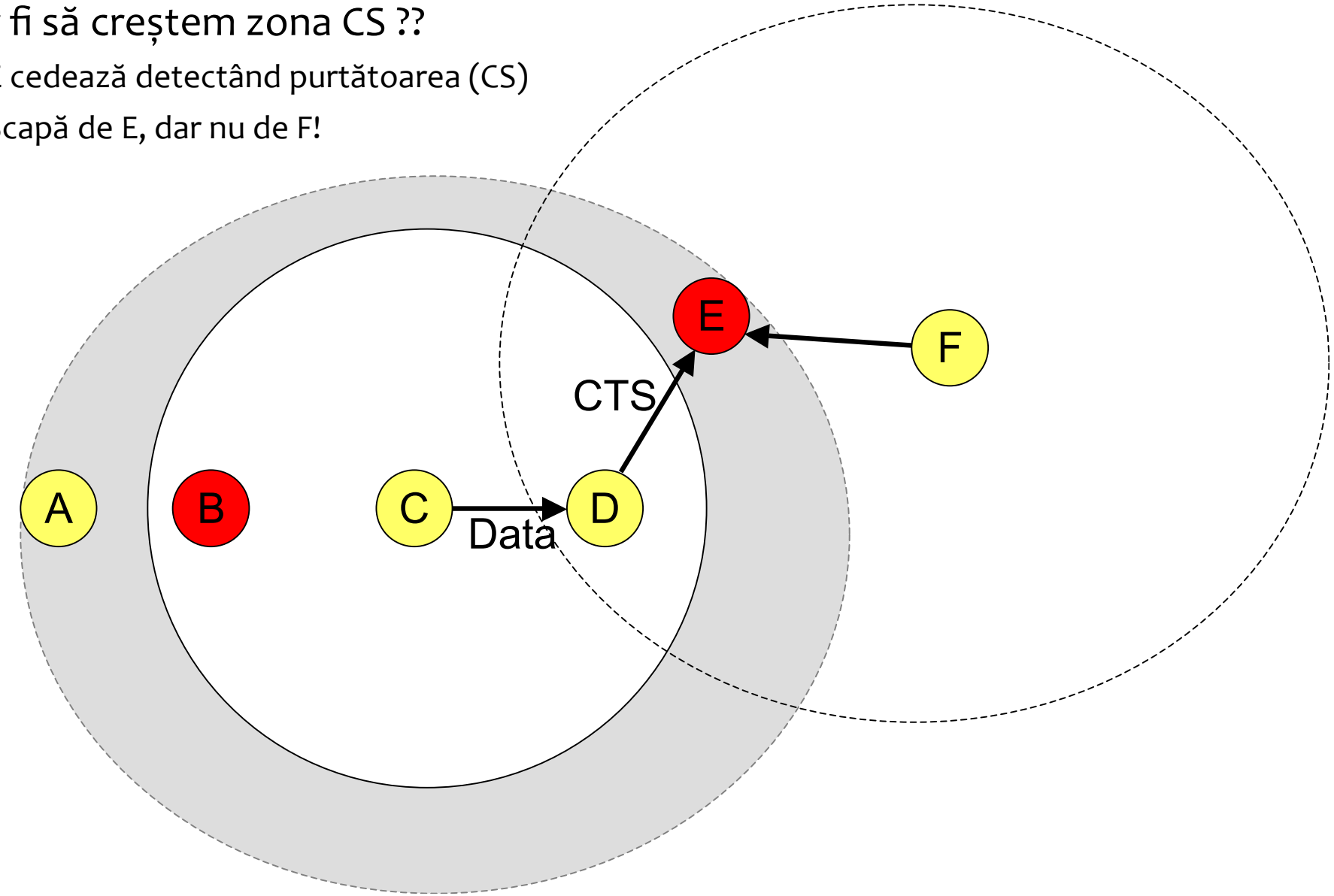


Dacă E nu primeste CTS -> poate iniția transmisia către D.
Problema terminalului ascuns rămâne!

Terminal ascuns cu RTS/CTS CS extins

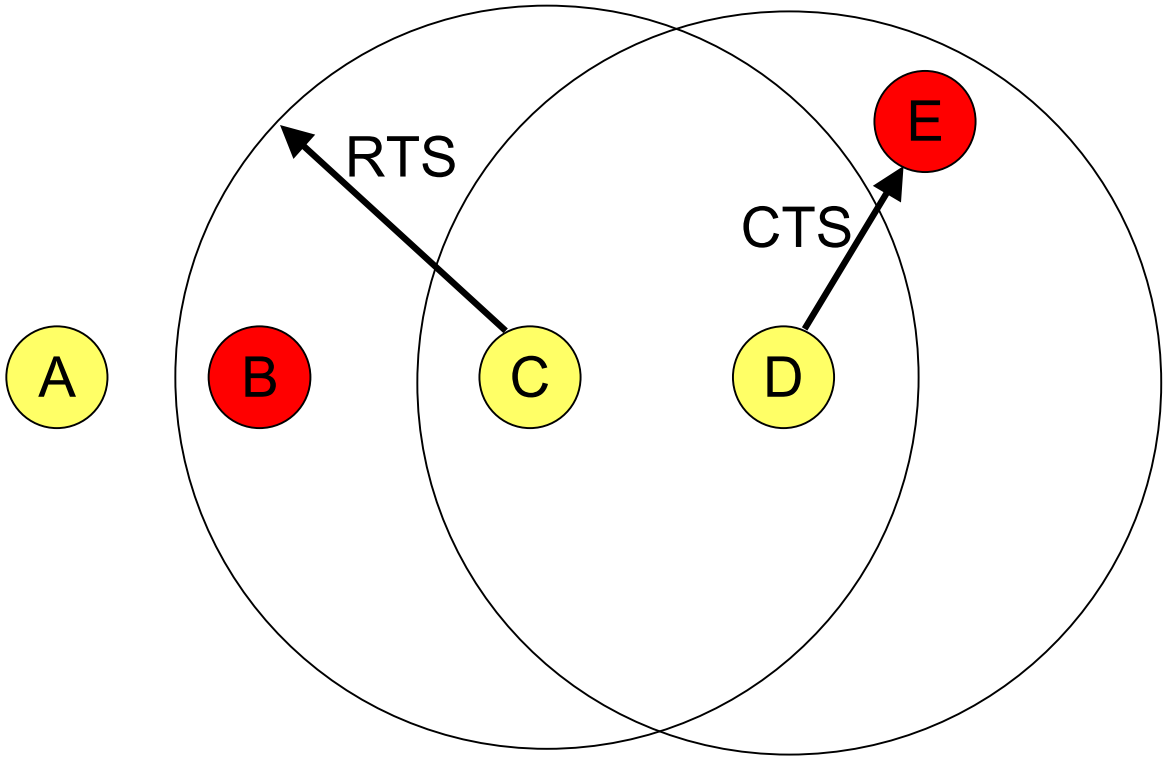
Ce-ar fi să creștem zona CS ??

- E cedează detectând purtătoarea (CS)
- Scapă de E, dar nu de F!



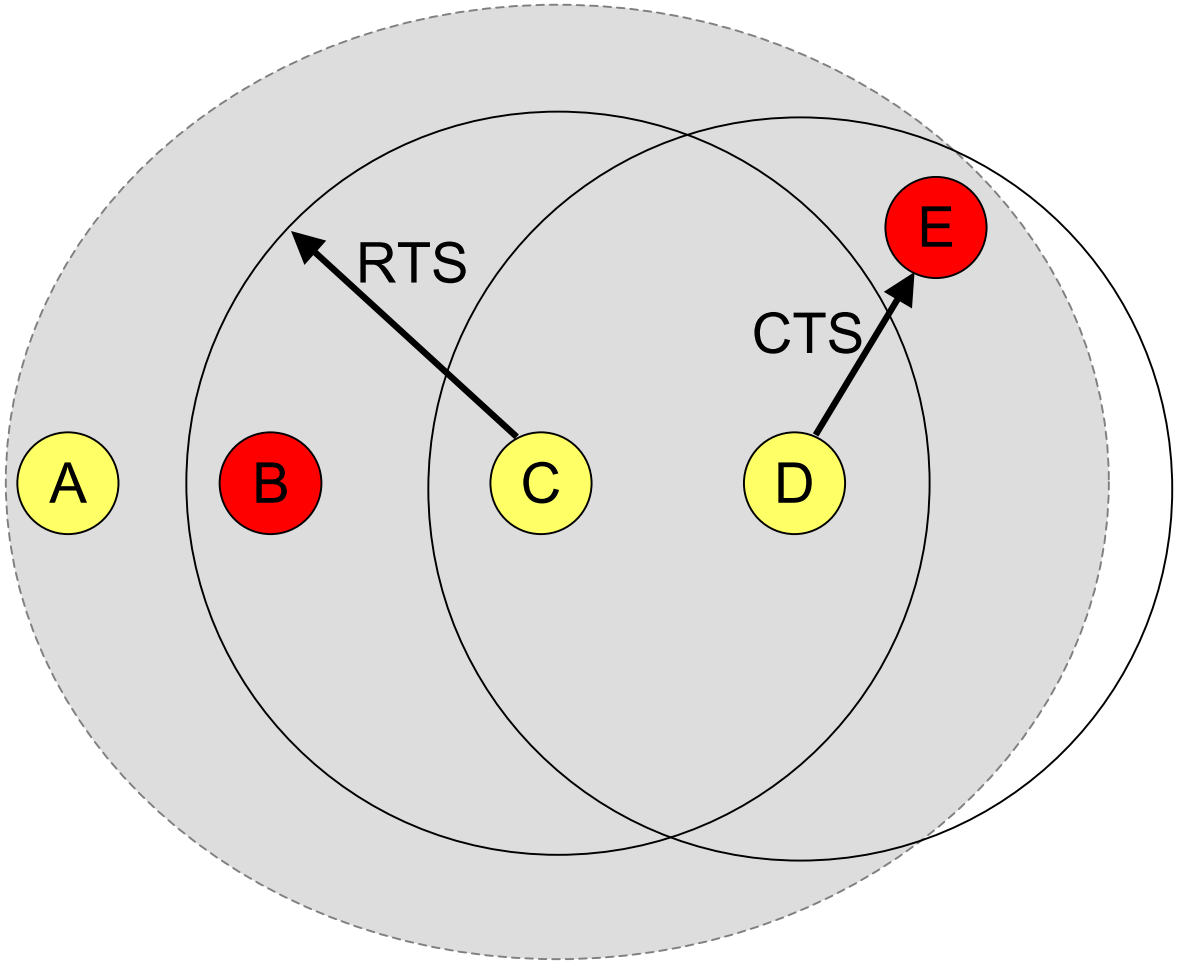
Terminal expus cu RTS/CTS

B ar putea să transmită către A, dar RTS nu-l permite



Terminal ascuns, CS extins

B ar putea transmite către A, dar CS extins înrăutățește situația



Concluzii RTS/CTS, CS extins

802.11 nu rezolvă complet TA, TE

Tratează doar parțial problema cu RTS/CTS și recomandă CS extins

CS extins agravează terminalele expuse

Reduce refolosirea mediului = un compromis

RTS/CTS consumă bandă

Mecanismul de backoff este ineficient

- Cercetarea pentru un protocol MAC cât mai bun continuă…
- 802.11 este încă optimizat

Zone de propagare

- **Zona de recepție 0-250m**
- **Zona de CS (fără recepție) 250-550m**
- **Zona de interferență/captură 0 - ?**

Distanțe idealizate (ns2)

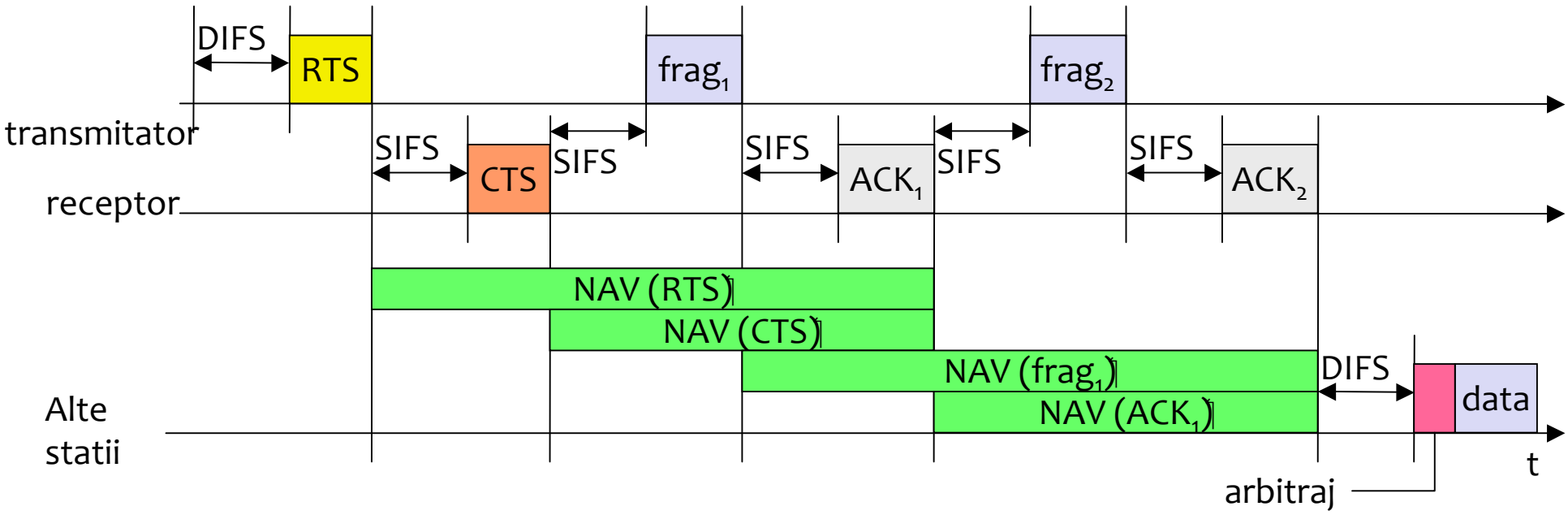
Pentru a putea evita coliziunea cu ACK, după detecția mediului ocupat de CS (fără decodare), se folosește EIFS

EIFS = SIFS + DIFS + (ACK + Preamble + PLCP)/BitRate

1Mbps, EIFS=364μs

2Mbps => EIFS = 212μs

Fragmentare



Parametri specifici 802.11b

Table 12-9. HR/DSSS PHY parameters

Parameter	Value	Notes
Maximum MAC frame length	4,095 bytes	
Slot time	20 µs	
SIFS time	10 µs	The SIFS is used to derive the value of the other interframe spaces (DIFS, PIFS, and EIFS).
Contention window size	31 to 1,023 slots	
Preamble duration	144 µs	Preamble symbols are transmitted at 1 MHz, so a symbol takes 1 ms to transmit; 96 bits require 96 symbol times.
PLCP header duration	48 bits	The PLCP header transmission time depends on whether the short preamble is used.
Minimum sensitivity	-76 dBm	
Adjacent channel rejection	35 dB	See text for measurement notes.

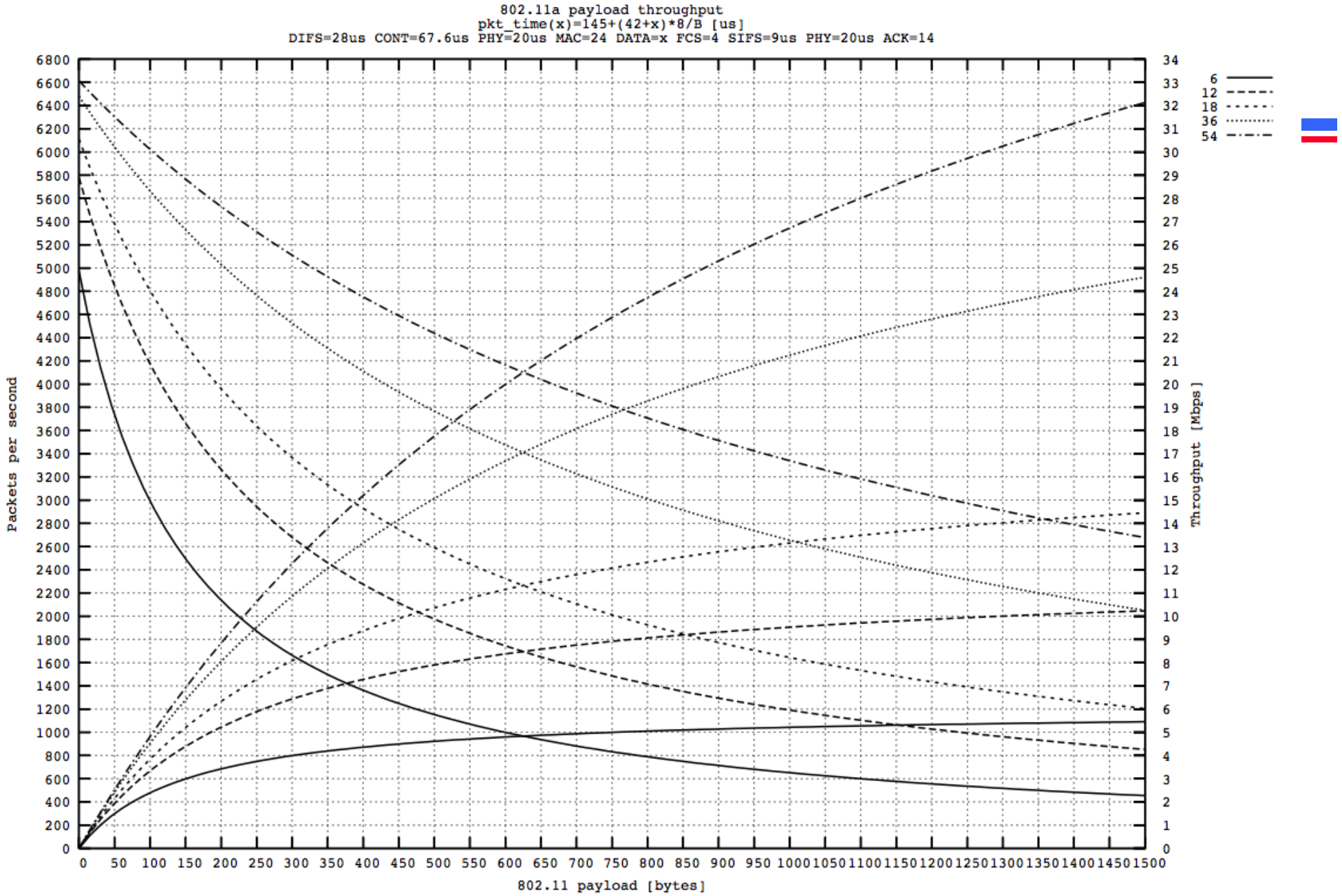
Parametri specifici 802.11a

Table 13-5. OFDM PHY parameters

Parameter	Value	Notes
Maximum MAC frame length	4,095 bytes	
Slot time	9 µs	
SIFS time	16 µs	The SIFS is used to derive the value of the other interframe spaces (DIFS, PIFS, and EIFS).
Contention window size	15 to 1,023 slots	
Preamble duration	20 µs	
PLCP header duration	4 µs	
Receiver sensitivity	-65 to -82 dBm	Depends on speed of data transmission.

Analiză capacitate 802.11a

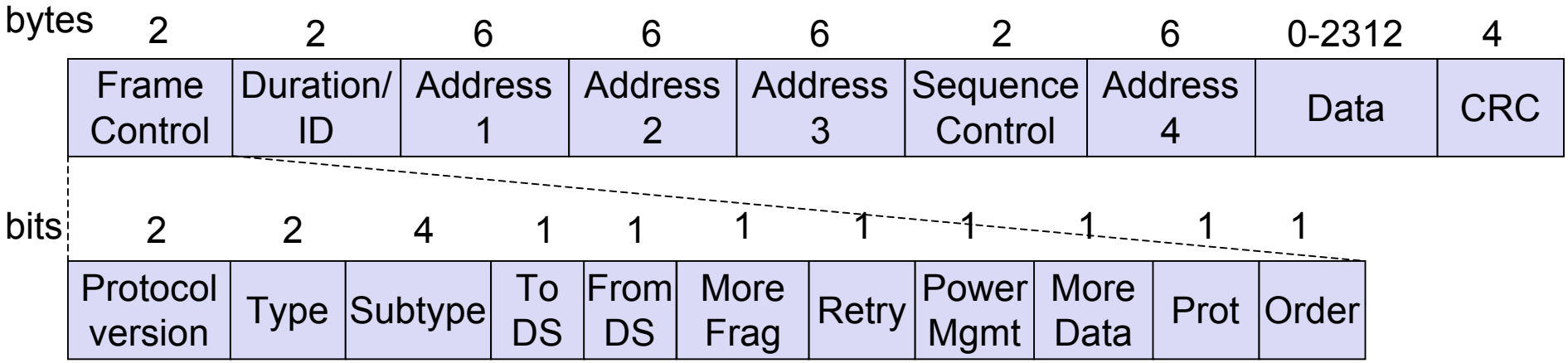
- http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html?page=2
- DIFS 28μs
- Conflict 72μs
- Preambul 24μs
- Date x octeți
- SIFS 9μs



Pachetele mici au overhead mare!

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



Tipuri de pachete (Gast, tabela 3.1)

Management frames (type=00)[a]	
0000	Association request
0001	Association response
0010	Reassociation request
0011	Reassociation response
0100	Probe request
0101	Probe response
1000	Beacon
1001	Announcement traffic indication message (ATIM)
1010	Disassociation
1011	Authentication
1100	Deauthentication

Control frames (type=01)

1000	Block Acknowledgment Request (QoS)
1001	Block Acknowledgment (QoS)
1010	Power Save (PS)-Poll
1011	RTS
1100	CTS
1101	Acknowledgment (ACK)
1110	Contention-Free (CF)-End
1111	CF-End+CF-Ack

Data frames (type=10)

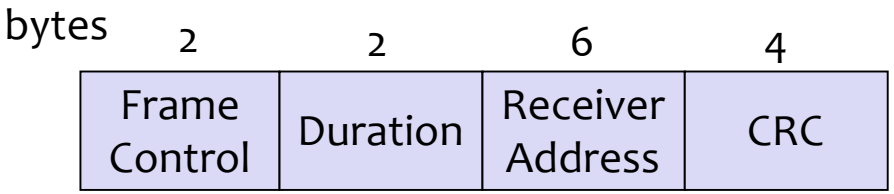
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll

Interpretarea biților ToDS și FromDS

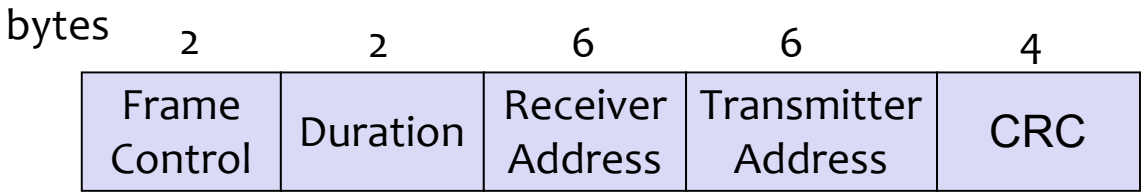
	ToDS=0	**ToDS=1**
FromDS=0	mgmt, control, modul ad hoc	uplink
FromDS=1	downlink	wireless bridge

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

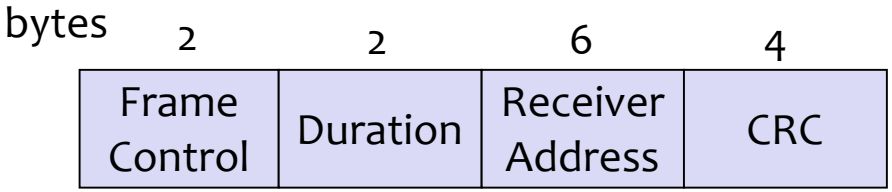
ACK



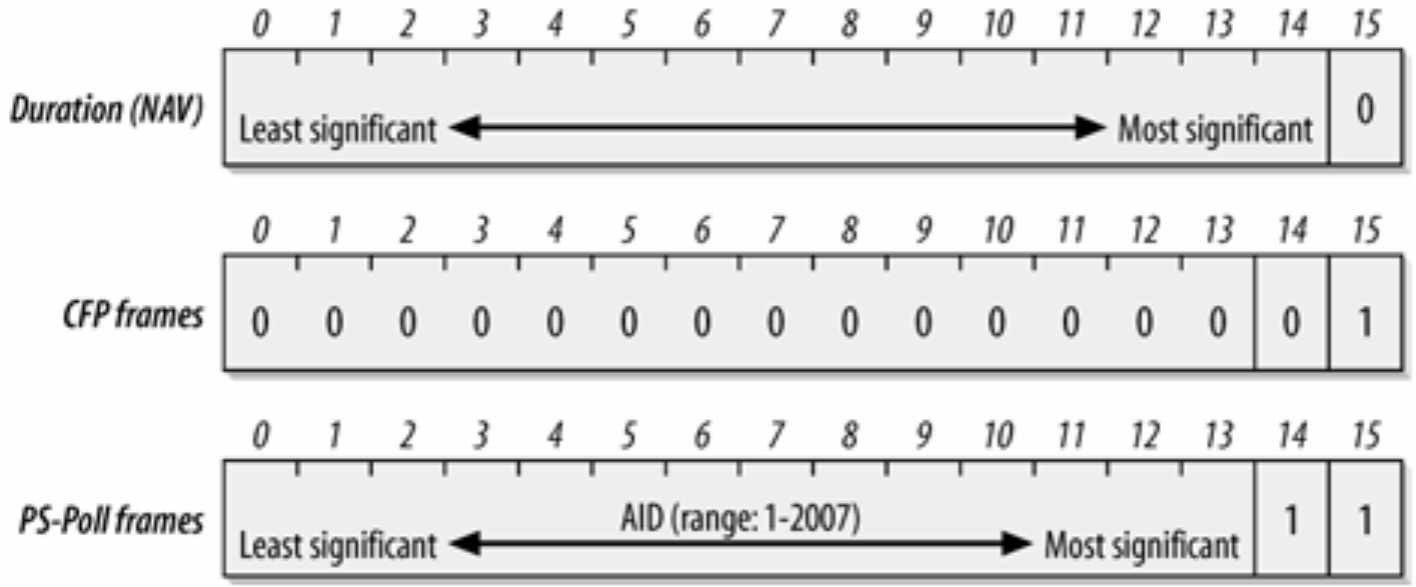
RTS



CTS

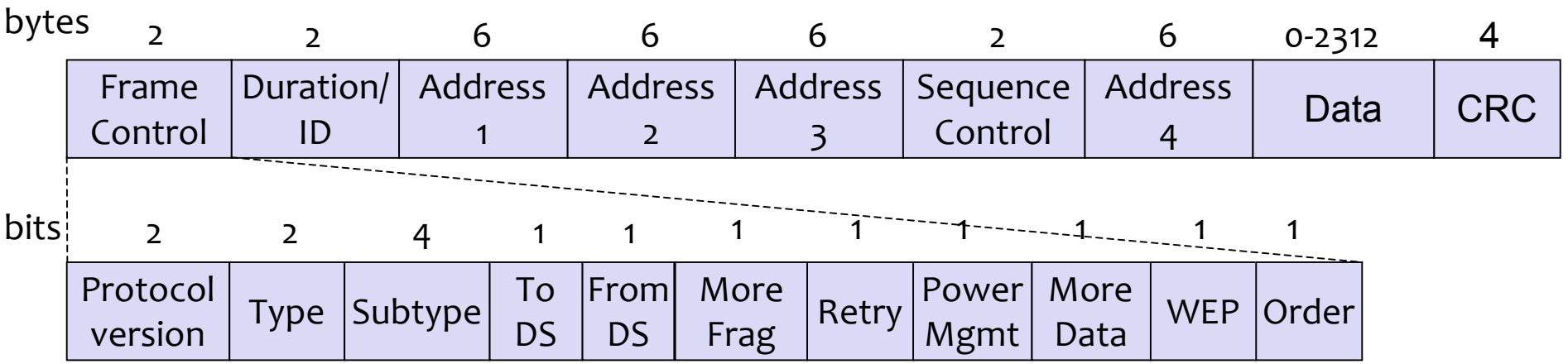


Durata - NAV



- Fiecare stație indică în acest câmp estimarea de ocupare a mediului
- Toate stațiile monitorizează toate transmisiile => inspectează NAV

802.11 – cadre de date



De ce sunt necesare mai mult de două adrese?

adrese

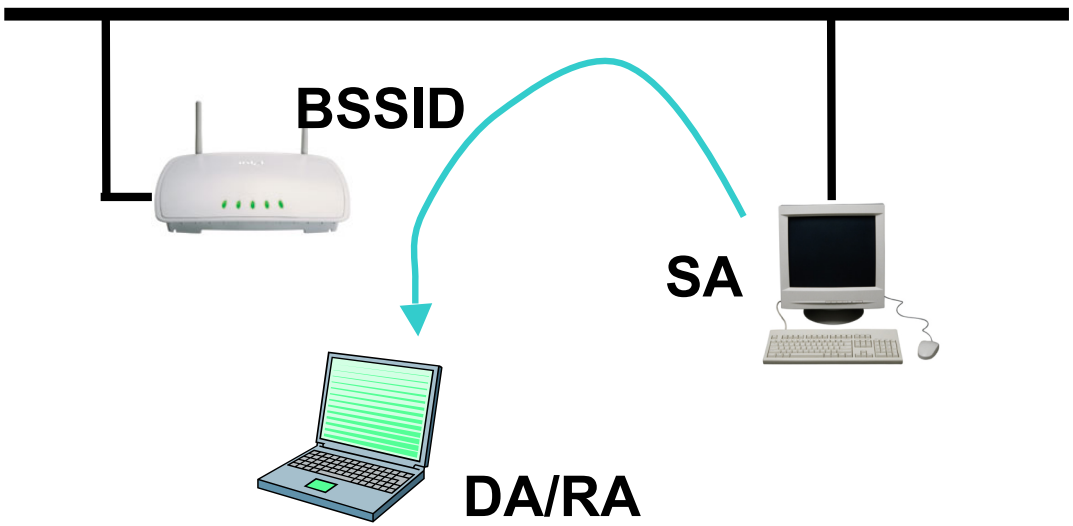
Reguli orientative

- **Adresa 1: stație destinație**
- **Adresa 2: stație sursă**
- **Adresa 3: filtrare**

Formatul adreselor

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



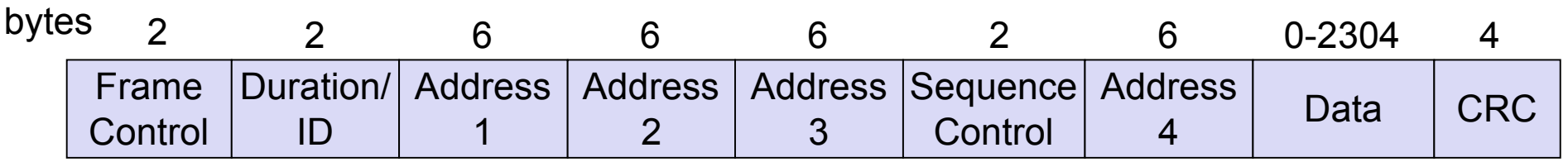
recepția cadrelor wireless ->wired

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

emisia cadrelor 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

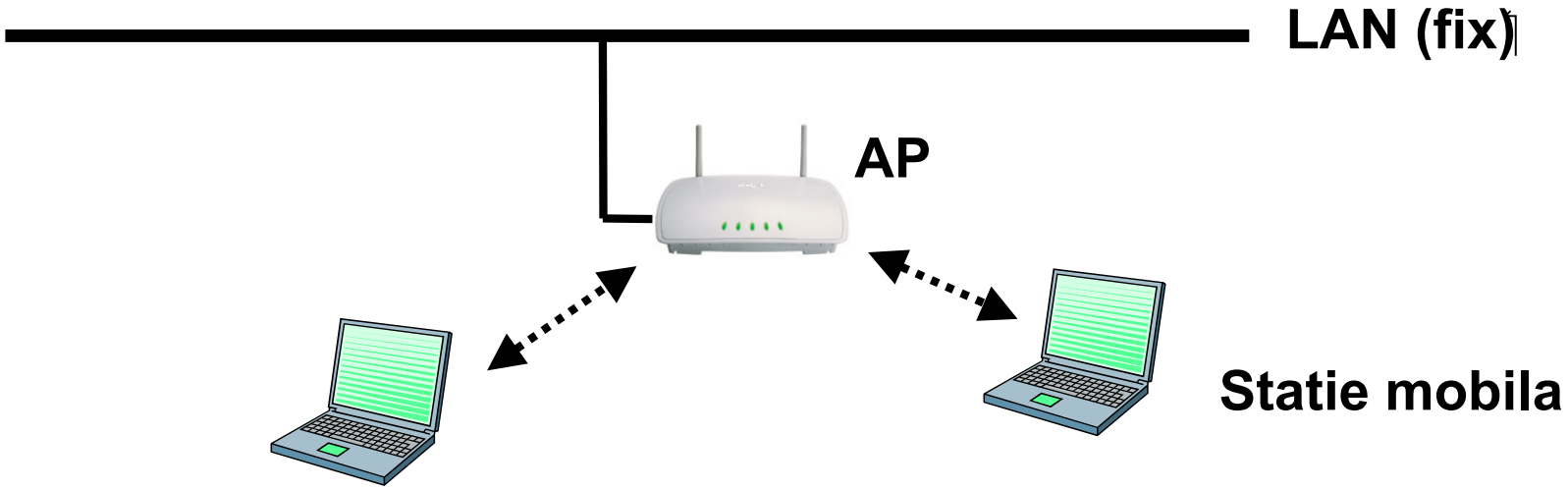
Alte câmpuri din antet



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

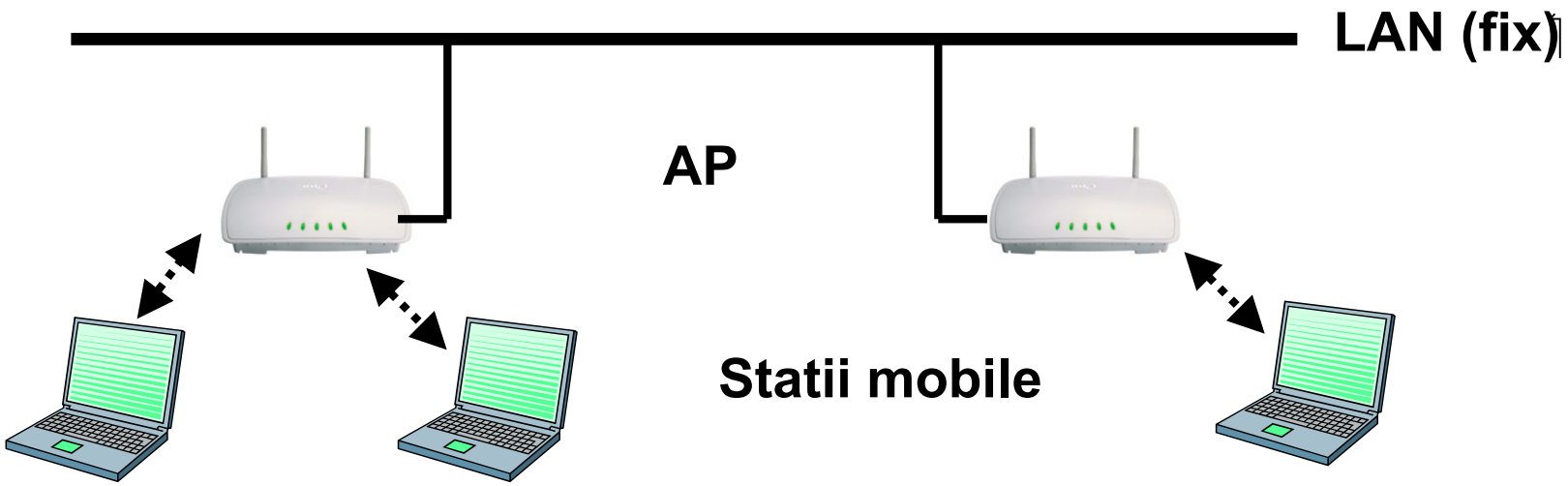
- Diferențe față de alte antete
  - Nu există “tip” pentru datele la nivel superior
  - Nu este necesară o lungime minimă

Modul infrastructură



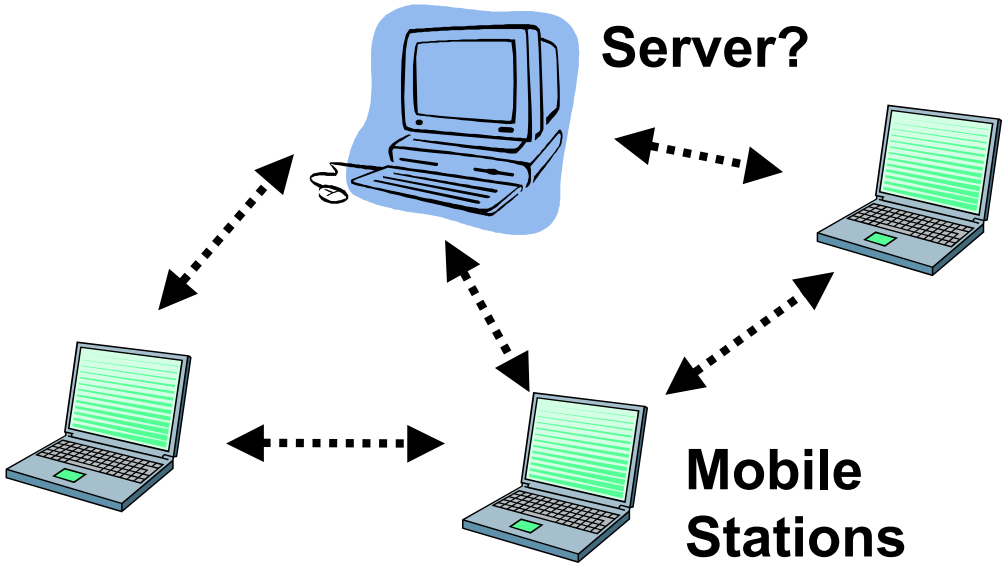
- Basic Service Set (BSS)
- AP functioneaza ca bridge
- Comunicarea intre statii se face numai prin intermediul AP
- distribution system (DS)

Modul infrastructură - extins



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

Modul Ad Hoc



- Independent Basic Service Set (IBSS)
- Stațiile comunica direct
- Când contactul direct nu este posibil, stațiile intermediare pot ruta
- rutarea nu este definită de 802.11!

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

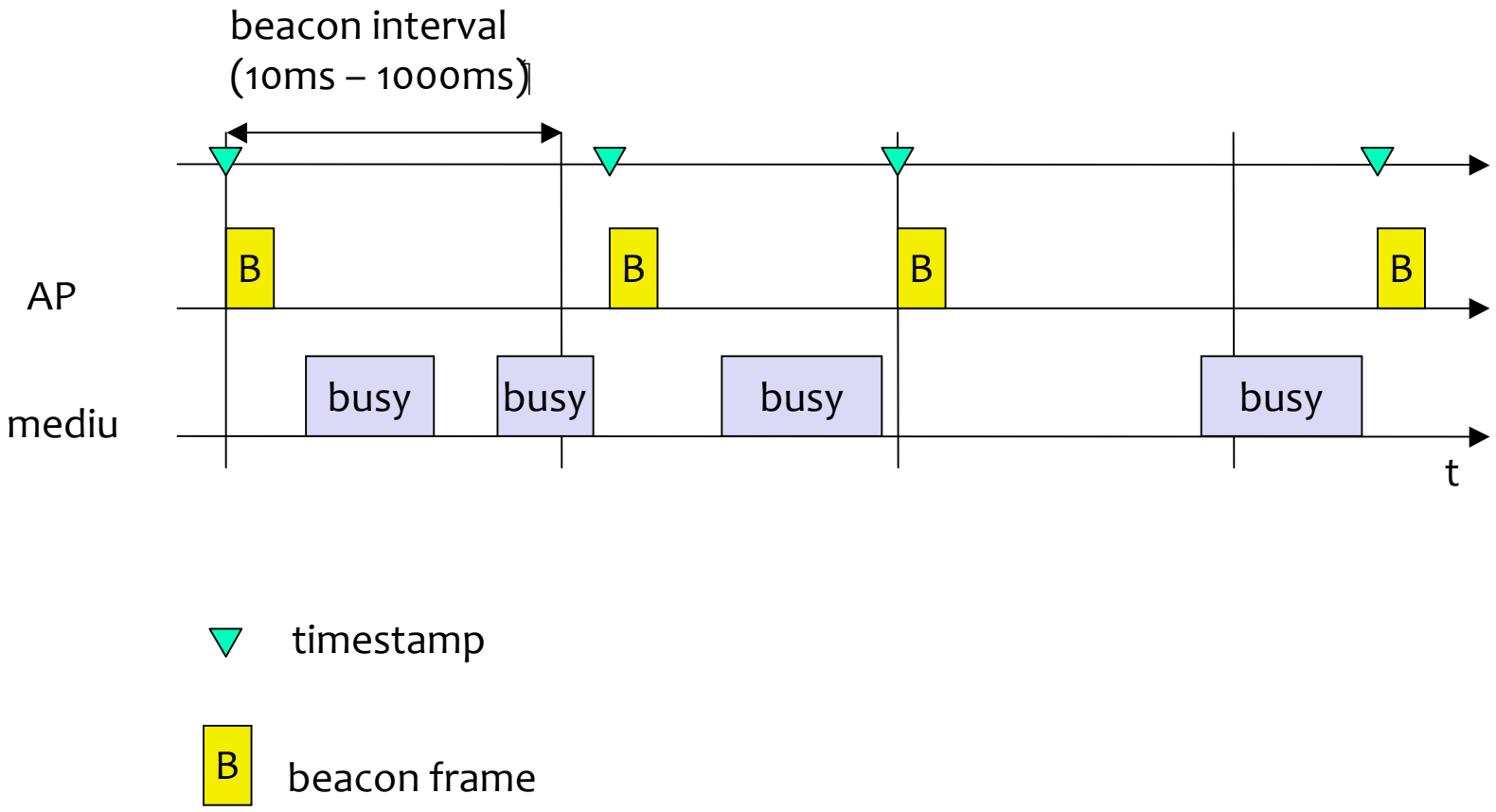
Timing Synchronization Function (TSF)

- 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 (infrastructura)



Beacon: suport pentru rate multiple

Fiecare beacon declară

- o listă de rate acceptabile
- o listă de rate de bază (obligatorii)
  - Pentru RTS, CTS, ACK, beacon

Gestiune PS (powersave mode)

- 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
- Modul ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - statiile care acumuleaza frame-uri anunta receptorii
    - mai complicat – nu exista AP
    - coliziune ATIMs posibilă (scalabilitate?)
- APSD (Automatic Power Save Delivery)
  - metoda mai nouă (802.11e) care înlocuiește TIM, DTIM, ATIM

- 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

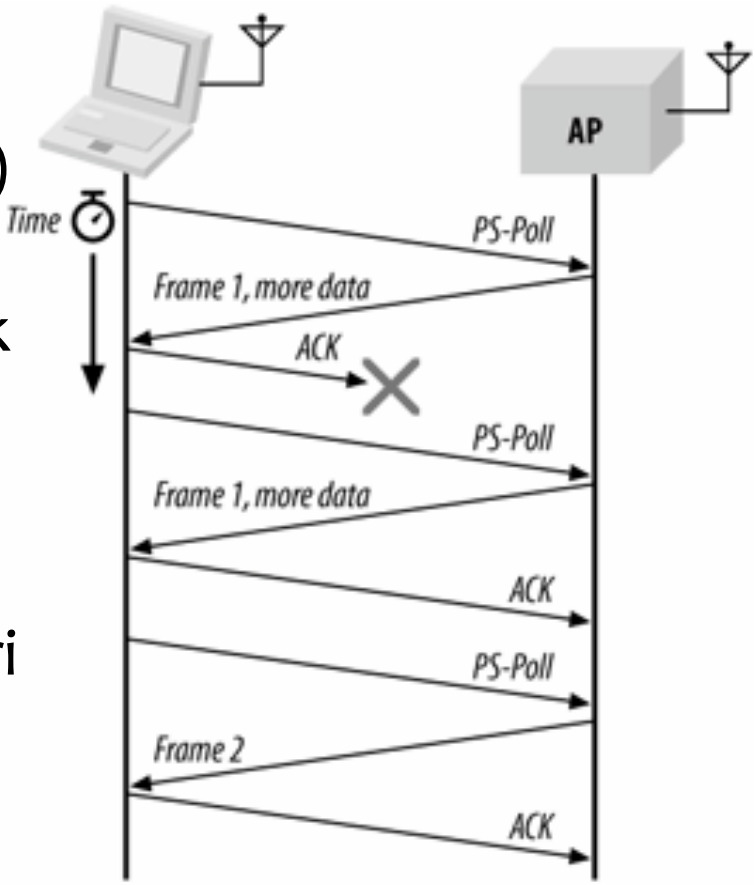
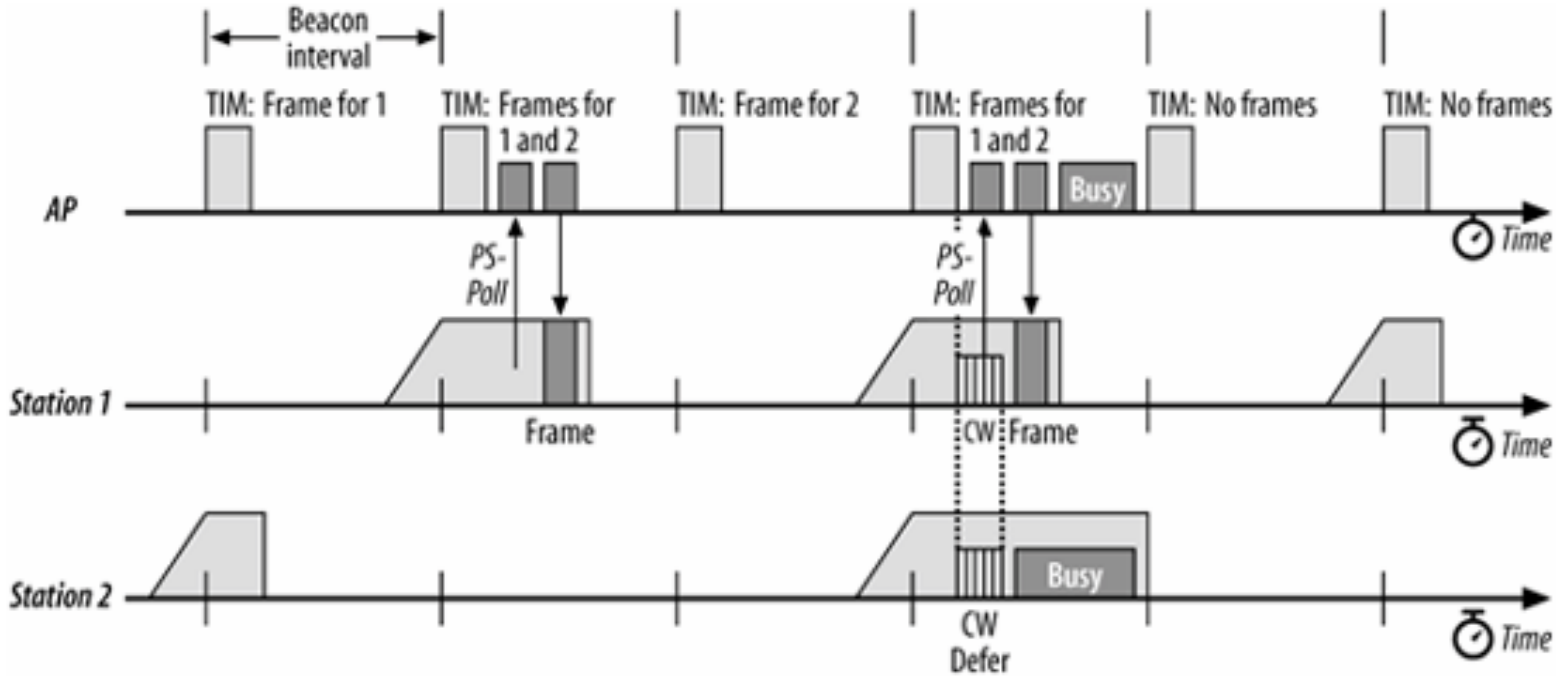
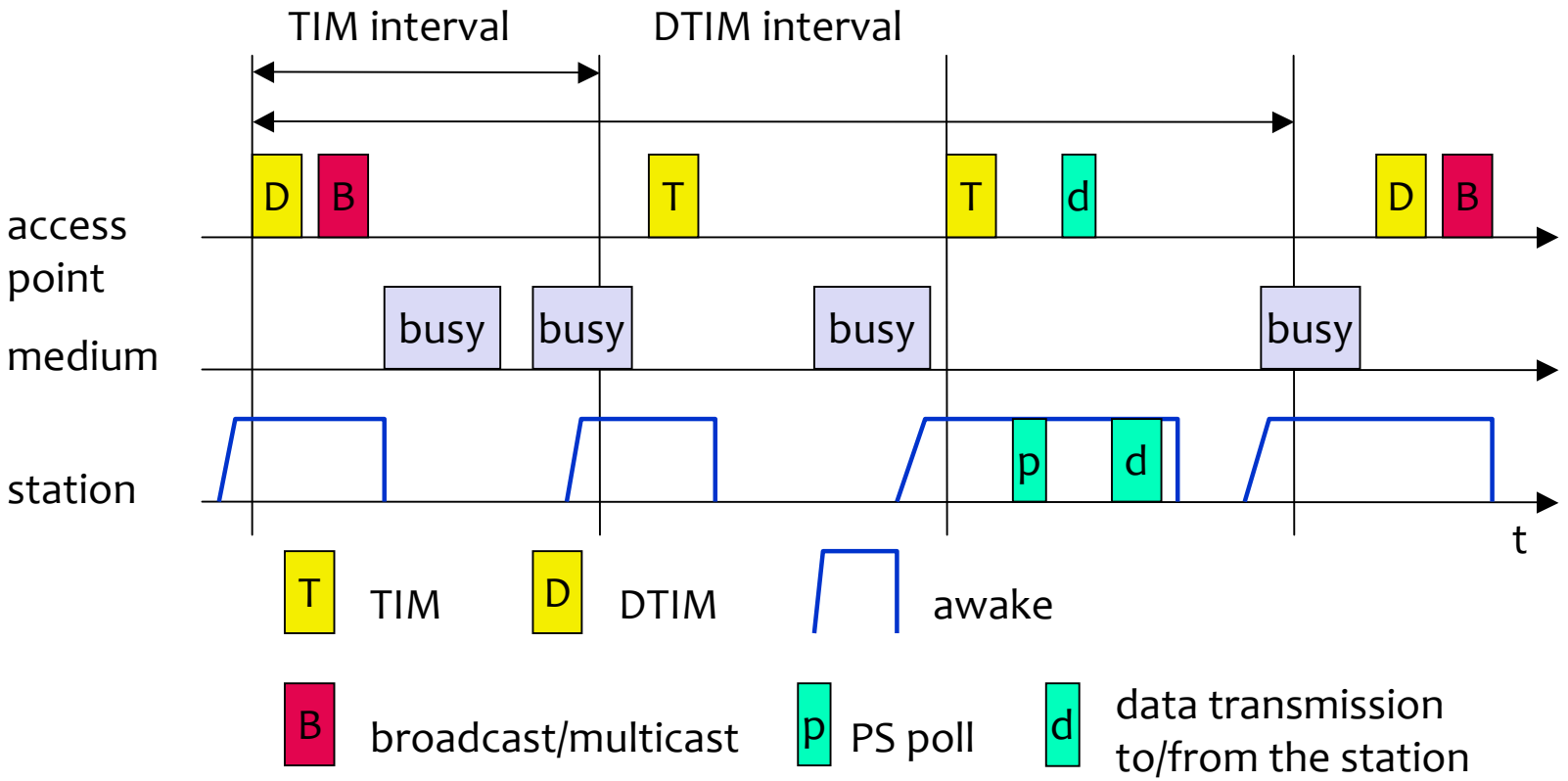


Figure 8-13. Buffered frame retrieval process

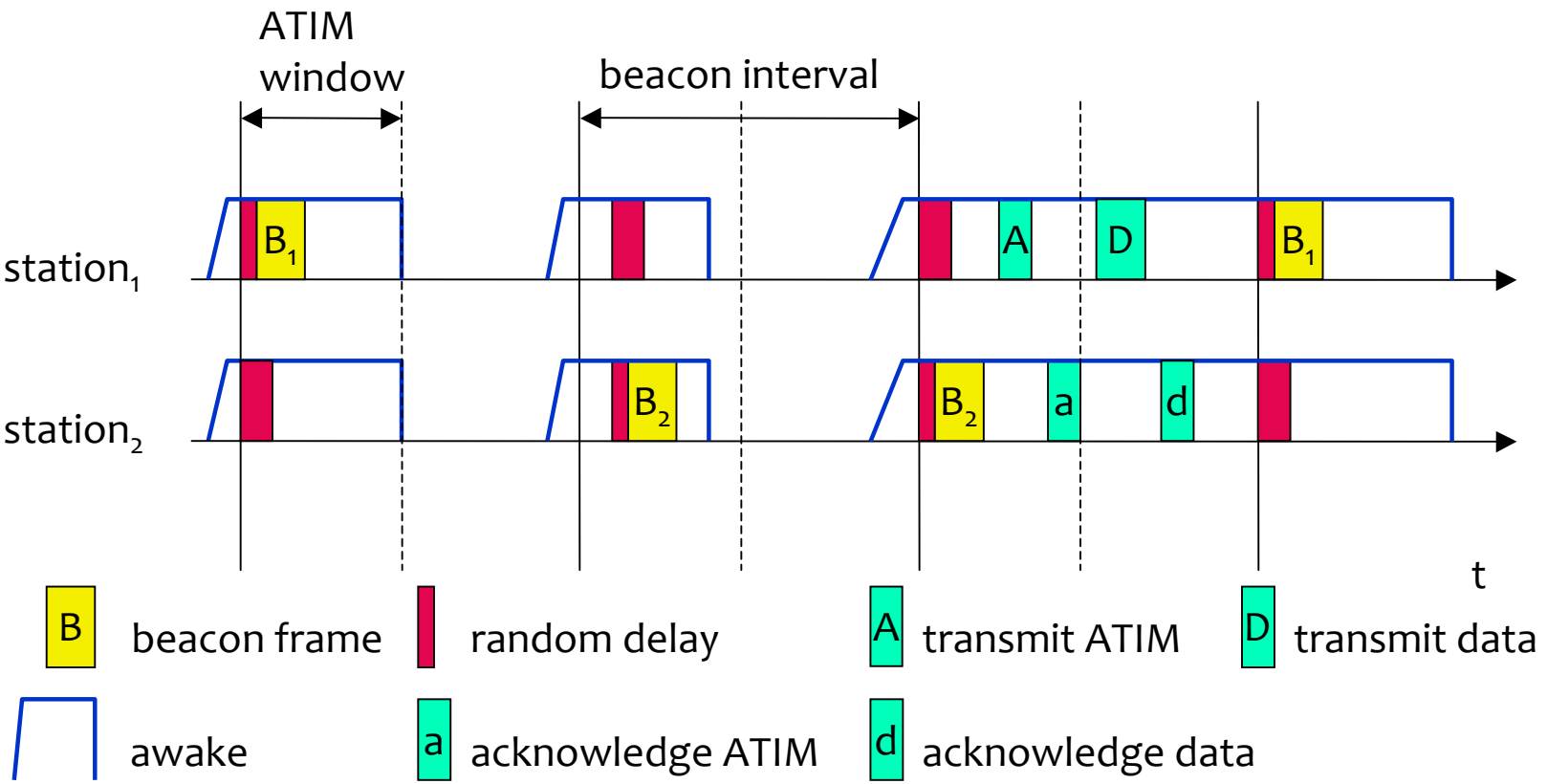


- Beacon 1: există cadre pentru stația 1
  - Stația 2 se întoarce în PS-mode
- Beacon 2: stația 1 cere cadrele, trece în PS-mode
- Beacon 3: ambele stații doresc PS-Poll
- Beacon 5: mediul este ocupat de o stație invizibilă
- Beacon 6: cadrul pentru stația 2 a fost aruncat

Gestiune PS, modul infrastructură



Gestiune PS (modul ad-hoc)



Gestiune PS

- 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 - Roaming

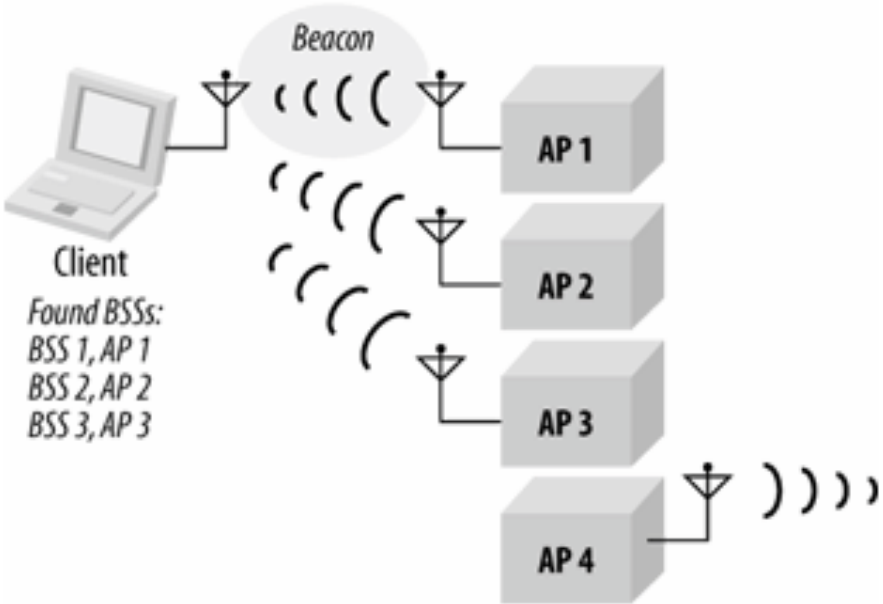
Ce se intâmplă când cade conexiunea?

- 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

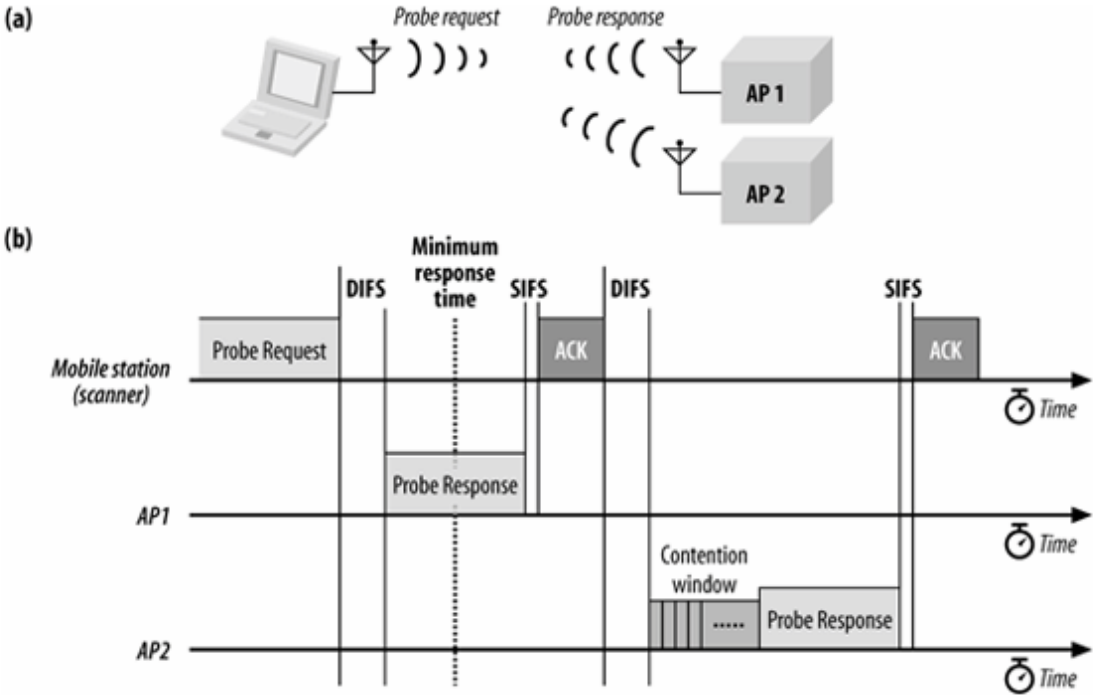


Scanare activă

Pe fiecare canal disponibil:

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

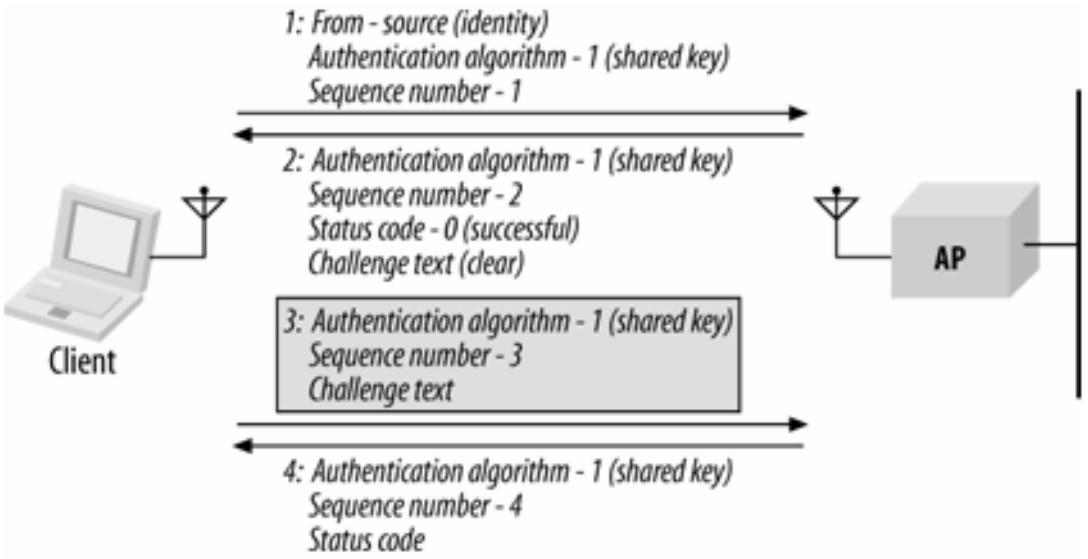
Figure 8-3. Active scanning procedure and medium access



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



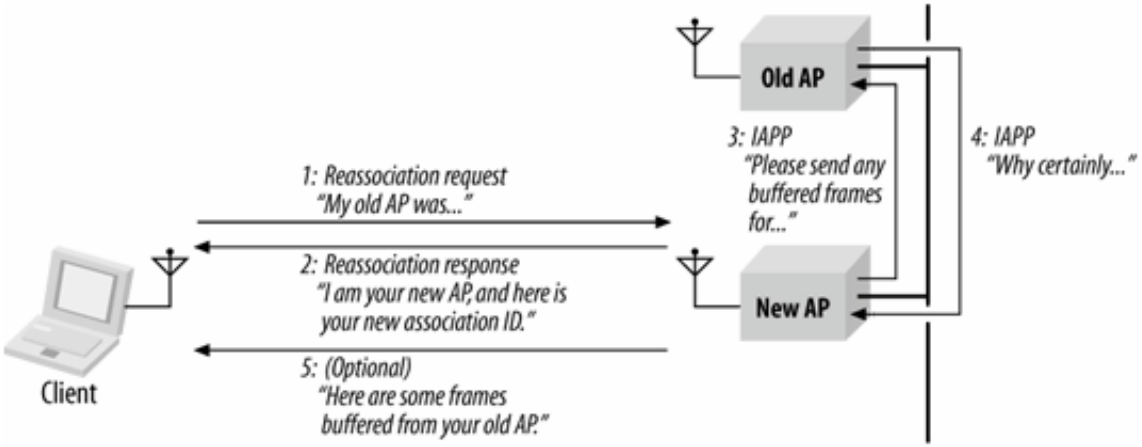
Asocierea

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



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

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

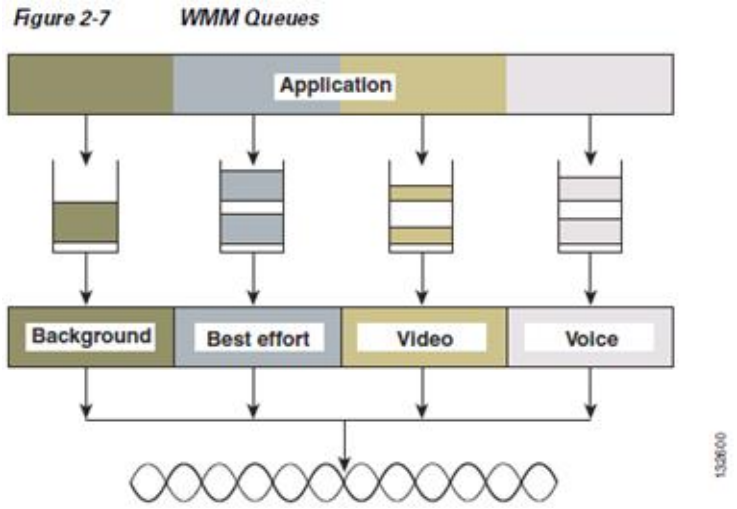
Confidențialitate (privacy)

- Implicit mesajele sunt necriptate (in clar)
  - » WEP optional, dar implementat pe scara larga
    - – criptare slabă!
  - » WPA, WPA2
    - » foloseste proceduri implementate în hardware
    - » schimba periodic cheile

802.11e (suport parțial QoS)

Trei elemente

1. cozi cu priorități
   - Voice, video, best effort, background
   - IFS și timerele sunt calculate independent pt fiecare coadă
   - Coliziuni între cozi – retry, BEB, …
2. AIFS cu lungimi diferite
3. CW specifice



802.11e (suport parțial QoS)

2. AIFS cu lungimi diferite
   - VO SIFS + 2*slot
   - VI SIFS + 2*slot
   - BE SIFS + 3*slot
   - BK SIFS + 7*slot

AC	AIFSN	802.11b AIFS[AC]	802.11g AIFS[AC]	802.11a AIFS[AC]	802.11n 2.4GHz AIFS[AC]	802.11n 5GHz AIFS[AC]
SIFS Time	---	10µs	10µs	16µs	10µs	16µs
Slot Time	---	20µs	Long = 20µs Short = 9µs	9µs	Long = 20µs Short = 9µs	9µs
AC_VO	2	50µs	Long = 50µs Short = 28µs	34µs	Long = 50µs Short = 28µs	34µs
AC_VI	2	50µs	Long = 50µs Short = 28µs	34µs	Long = 50µs Short = 28µs	34µs
AC_BE	3	70µs	Long = 70µs Short = 37µs	43µs	Long = 70µs Short = 37µs	43µs
AC_BK	7	150µs	Long = 150µs Short = 73µs	79µs	Long = 150µs Short = 73µs	79µs

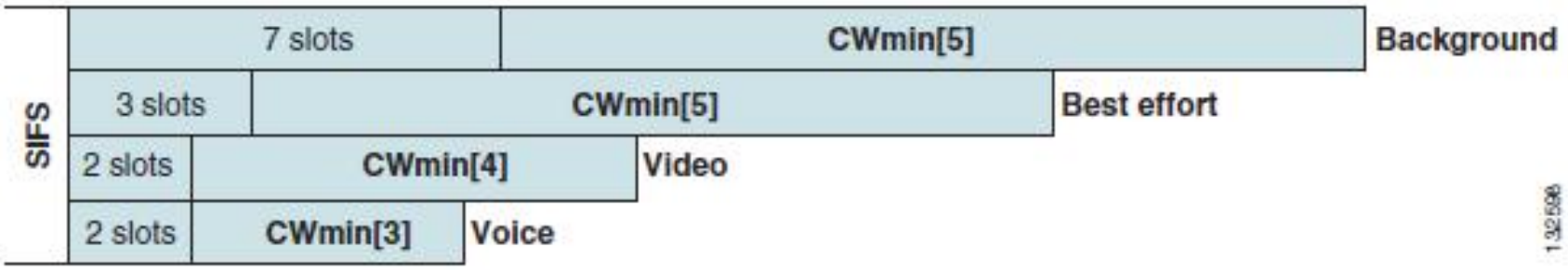
802.11e (suport partial QoS)

3. CW specifice - pt 11a/g/n
   - VO CW = 3..7
   - VI CW = 7..15
   - BE CW = 15..1023
   - BK CW = 15..1023

CW specifice pt 11b
- VO CW = 7..15
- VI CW = 15..31
- BE CW = 15..1023
- BK CW = 15..1023

AIFS + CW pentru 11b:

Figure 2-8 Access Category (AC) Timing



802.11: standardizarea continuă

- 802.11e – suport pentru QoS
- 802.11h – management frecvente 5GHz
- 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
- 802.11n -- capacitate sporită
- 802.11p – pt vehicule – viteza 200km/h
- 802.11s – mesh, capabilitati multihop
- 802.11t – predictia performantei
- … toate literele pana la z, si mai departe!
- 802.11-2012 - cumulativ 802.11-2007, 802.11n-2009, k, r, y, n, w, p, z, v, u, s

Actualizari standarde

802.11c: Bridge Support

Definition of MAC procedures to support bridges as extension to 802.1D

802.11d: Regulatory Domain Update

Support of additional regulations related to channel selection, hopping sequences

802.11e: MAC Enhancements – QoS

Enhance the current 802.11 MAC to expand support for applications with
Quality of Service requirements, and in the capabilities and efficiency of the protocol
Definition of a data flow ("connection") with parameters like rate, burst, period…
supported by HCCA (HCF (Hybrid Coordinator Function) Controlled Channel Access, optional)
Additional energy saving mechanisms and more efficient retransmission
EDCA (Enhanced Distributed Channel Access): high priority traffic waits less for channel access

802.11F: Inter-Access Point Protocol (withdrawn)

Establish an Inter-Access Point Protocol for data exchange via the distribution system

802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; 54 Mbit/s, OFDM

Successful successor of 802.11b, performance loss during mixed operation with .11b

802.11h: Spectrum Managed 802.11a

Extension for operation of 802.11a in Europe by mechanisms like channel measurement for
dynamic channel selection (DFS, Dynamic Frequency Selection) and
power control (TPC, Transmit Power Control)

802.11i: Enhanced Security Mechanisms

Enhance the current 802.11 MAC to provide improvements in security.
TKIP enhances the insecure WEP, but remains compatible to older WEP systems
AES provides a secure encryption method and is based on new hardware

Actualizari standarde

802.11j: Extensions for operations in Japan
- Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range

802.11k: Methods for channel measurements
- Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel

802.11m: Updates of the 802.11-2007 standard

802.11n: Higher data rates above 100Mbit/s
- Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP
- MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible
- However, still a large overhead due to protocol headers and inefficient mechanisms

802.11p: Inter car communications
- Communication between cars/road side and cars/cars
- Planned for relative speeds of min. 200km/h and ranges over 1000m
- Usage of 5.850-5.925GHz band in North America

802.11r: Faster Handover between BSS
- Secure, fast handover of a station from one AP to another within an ESS
- Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
- Handover should be feasible within 50ms in order to support multimedia applications efficiently

Actualizari standarde

802.11s: Mesh Networking

- Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
- Support of point-to-point and broadcast communication across several hops

802.11T: Performance evaluation of 802.11 networks

- Standardization of performance measurement schemes

802.11u: Interworking with additional external networks

802.11v: Network management

- Extensions of current management functions, channel measurements
- Definition of a unified interface

802.11w: Securing of network control

- Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.

802.11y: Extensions for the 3650-3700 MHz band in the USA

802.11z: Extension to direct link setup

802.11-2012 = 802.11-2007, 802.11k-2008, 802.11r-2008, 802.11y-2008, 802.11w-2009, 802.11n-2009, 802.11p-2010, 802.11z-2010, 802.11v-2011, 802.11u-2011,802.11s-2011

Nu toate "standardele" vor apărea în produse, multe idei vor rămâne doar promulgate în grupurile de lucru!

Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

Actualizări standarde

802.11ac

- Draft 3.0, AP-uri disponibile acum(2013)
- 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)

802.11ad (WiGig)

- 2.4GHz, 5GHz, compatibil cu 11a/b/g/n/ac
- 60GHz, beamforming, < 10m LOS?
- Max 7Gbps
- WiGig Display Extension

Rețele 802.11 multihop

Rețele multihop – de ce?

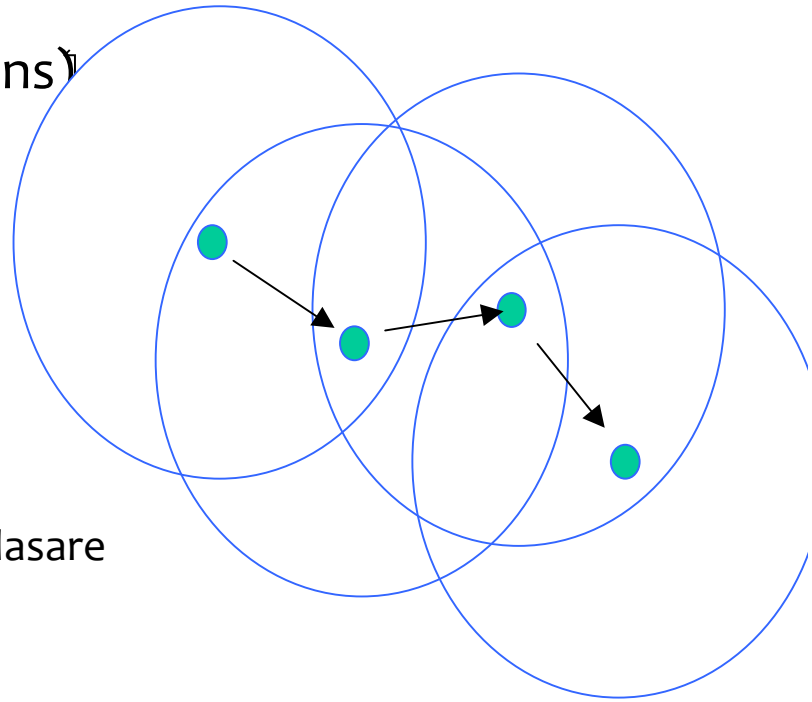
In multe cazuri, rețelele celulare nu sunt de dorit.

Multihop – aplicații posibile:

- medii neplanificate (adhoc)
  - » instalare rapida, cost redus
  - » retea de vehicole
  - » sedinte, conferinte, LAN parties
- domeniu militar, dezastre
  - » lipsa infrastructurii
- Rețele personale
  - » conectarea dispozitivelor: MP3 player, ceas, laptop
- acces internet
  - » infrastructura este tot 802.11, ca si mobilele

Retele multihop - probleme

- Probleme
  - exacerbeaza interferenta (terminal ascuns)
    - UDP poate obtine 1/7 din rata nominala
    - TCP 1/n (n este lungimea rutei)
  - mobilitate
    - Disconectari, partitionare
    - overhead
  - asimetrii
    - Propagare, baterie, viteza CPU, viteza de deplasare
  - variatii de traffic
  - inca subiect de cercetare



- Metodele de rutare standard nu sunt direct aplicabile

802.11 multihop

- Proactiv: rute disponibile permanent
- Reactiv: rute cautate cand e necesar

- Rutare proactiva OLSR
  - Similar cu LS in retelele fixe (OSPF)
  - Optimizat pt a reduce nr de mesaje
  - Overhead la mobilitate

- Rutare proactiva DSDV (destination sequenced DV)
  - similar cu DV in retelele fixe (BGP)
  - necesita link-uri bidirectionale
  - overhead – majoritatea rutelor nu sunt folosite niciodata
  - scalabilitate redusa

802.11 multihop

- Rutare reactiva DSR (dynamic source routing)
  - cai complete sunt mentinute de fiecare sursa
  - caile sunt descoperite prin broadcast
  - overhead redus – sunt mentinute doar rutele folosite
  - latenta mare la descoperirea rutelor
- Rutare ajutata de locatie (LAR)
  - flooding modificat
  - exploateaza locatia pentru a limita broadcast
  - aplicabilitate limitata (GPS)

Subiecte actuale în cercetare

- Controlul puterii crește reutilizarea
- Controlul ratei bazat pe calitatea canalului
- Exploatarea diversității canalului
  - Uplink către AP-uri diferite
- Conectarea simultană la rețele diferite (multihoming)
- Efectul canalului radio asupra protocoalelor de transport
- Utilizarea canalelor multiple pentru a discuta în paralel
- Utilizarea antenelor directive pentru a reduce interferența
- Auto-interferența în topologii multihop

… și multe altele.

Acknowledgments

- This presentation uses materials borrowed from
  - M. Gast, 802.11 Wireless Networks 2nd ed.
  - R.R.Choudhury@duke, online lectures
  - B.Awerbuch@johns hopkins, online lectures
  - wikipedia