
IEEE 802.11

Dragoş Niculescu

dragos.niculescu at cs pub ro

de A.I. **HotNews.ro**

11:16 Sport | Fotbal

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).



Liga 1
Foto: Agerpres

citeste **tot articolul** [4 comentarii

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

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.

documente

Estimari Cisco
(20 Feb 2012) DOC,
101KB

citeste **tot articolul** [0 comentarii

Correspondenta 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!



Traficul pe internet in Europa Centrala si de Est se va majora de trei ori in intervalul 2013 – 2018 - studiu Cisco



de Vlad Barza  HotNews.ro

Vineri, 27 iunie 2014, 13:42 Economie | IT

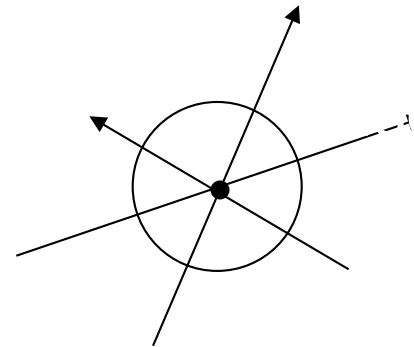
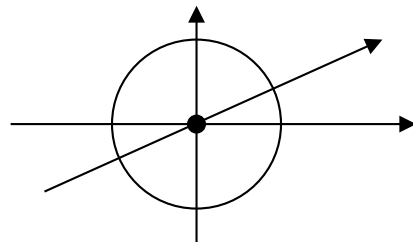
Traficul pe internet in Europa Centrala si de Est se va majora de trei ori in intervalul 2013 - 2018, iar traficul de date mobile va creste de 12 ori in acelasi interval, arata cel mai nou studiu Cisco Visual Networking Index. In regiune sunt in prezent aproape 530 de milioane de dispozitive conectate la internet, insa in 2018 numarul va creste cu 300 de milioane, mai arata studiul companiei de retelistica.

Cuprins

- generalități despre wireless
- standarde
- nivelul fizic
 - » Modulare, 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

Antennas: isotropic radiator

- Radiation +reception of electromagnetic waves
- Isotropic radiator: equal radiation in all directions
 - only a theoretical reference antenna
 - Real antennas always have directive effects
- Radiation pattern: measurement of radiation around an antenna

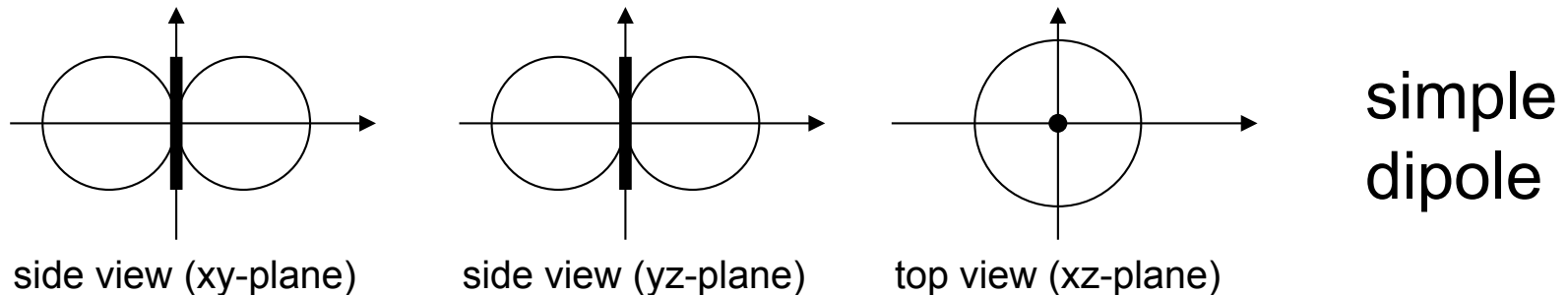


Antennas: simple dipoles

- dipoles with lengths $\lambda/4$, $\lambda/2$ as Hertzian dipole
→ shape of antenna proportional to wavelength



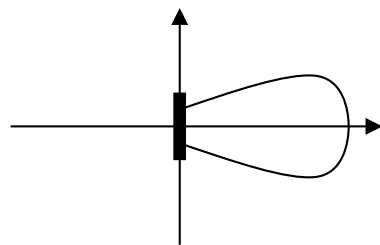
- Example: Radiation pattern of a simple Hertzian dipole



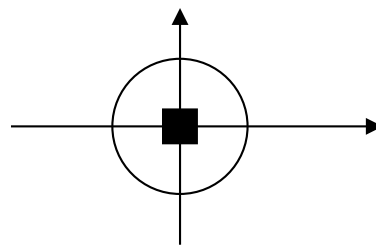
- **Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)**

Antennas: directed and sectorized

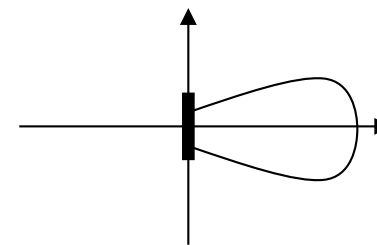
- Long distance WiFi, cellular BTS



side view (xy-plane)

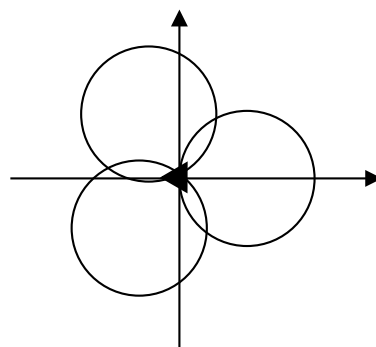


side view (yz-plane)

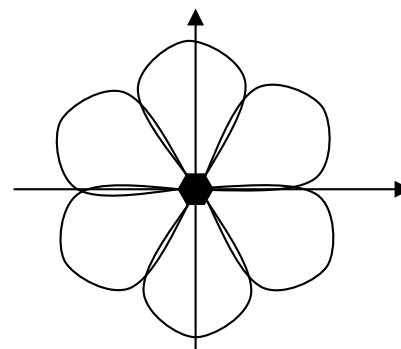


top view (xz-plane)

directed
antenna



top view, 3 sector

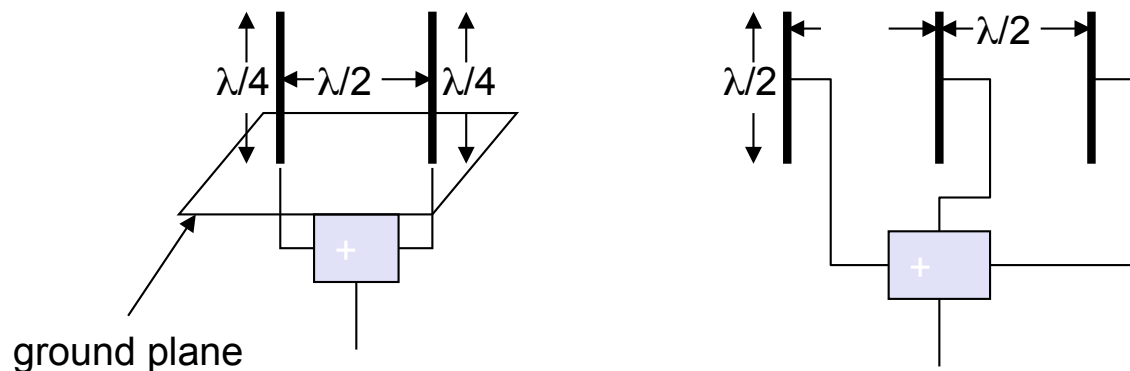


top view, 6 sector

sectorized
antenna

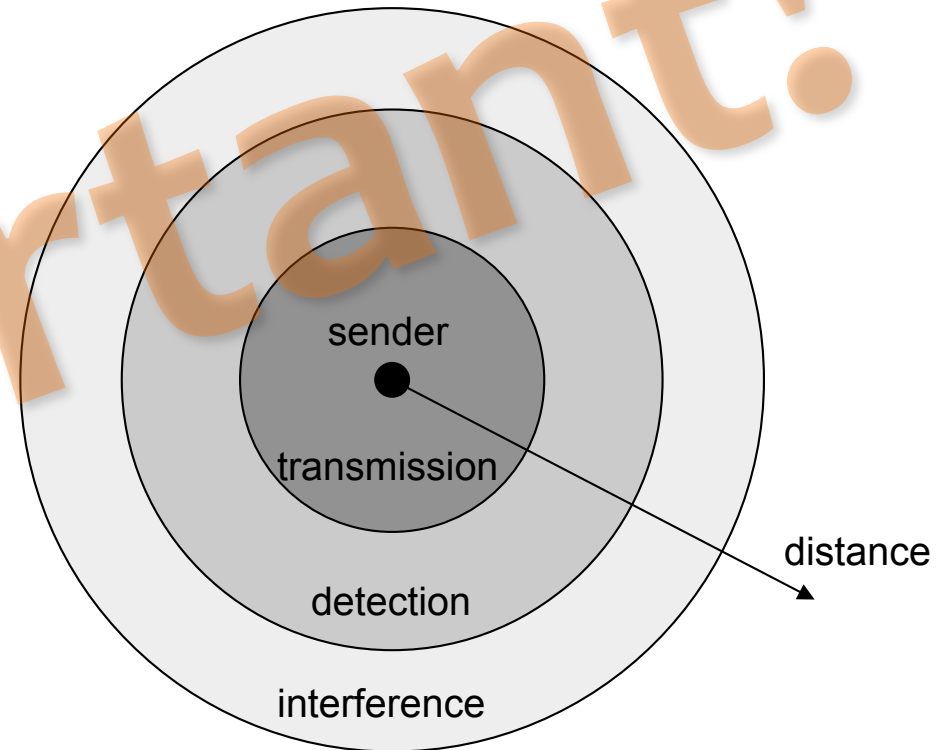
Antennas: diversity

- Grouping of 2 or more antennas
 - multi-element antenna arrays
- Antenna diversity
 - switched diversity, selection diversity
 - receiver chooses antenna with largest output
 - diversity combining
 - combine output power to produce gain
 - cophasing needed to avoid cancellation



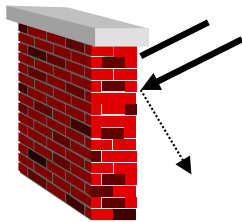
Signal propagation ranges

- **Transmission range**
 - communication possible
 - low error rate
- **Detection range**
 - detection of the signal possible
 - no communication possible
- **Interference range**
 - signal may not be detected
 - signal adds to the background noise
- **Warning: irregular shaped, time-varying**

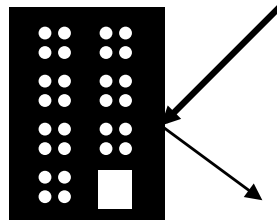


Signal propagation

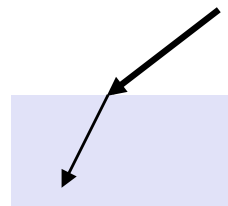
- Propagation in free space always like light (straight line)
- Receiving power proportional to $1/d^2$ in vacuum – much more in real environments, e.g., $d^{3.5} \dots d^4$
- Receiving power additionally influenced by
 - fading (frequency dependent)
 - shadowing
 - reflection at large obstacles
 - refraction depending on the density of a medium
 - scattering at small obstacles
 - diffraction at edges



shadowing



reflection



refraction

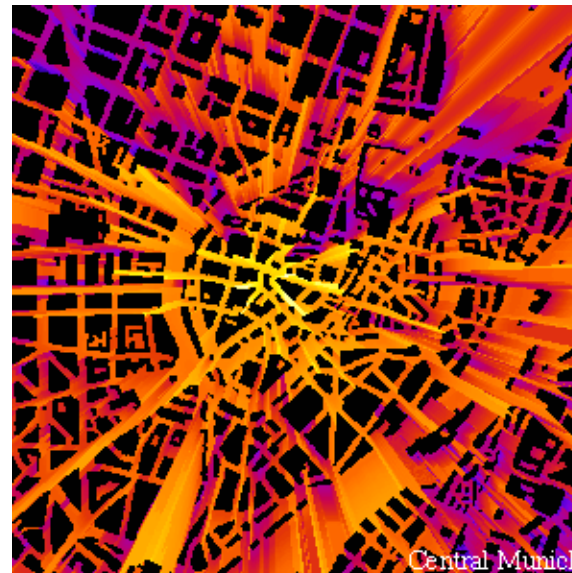
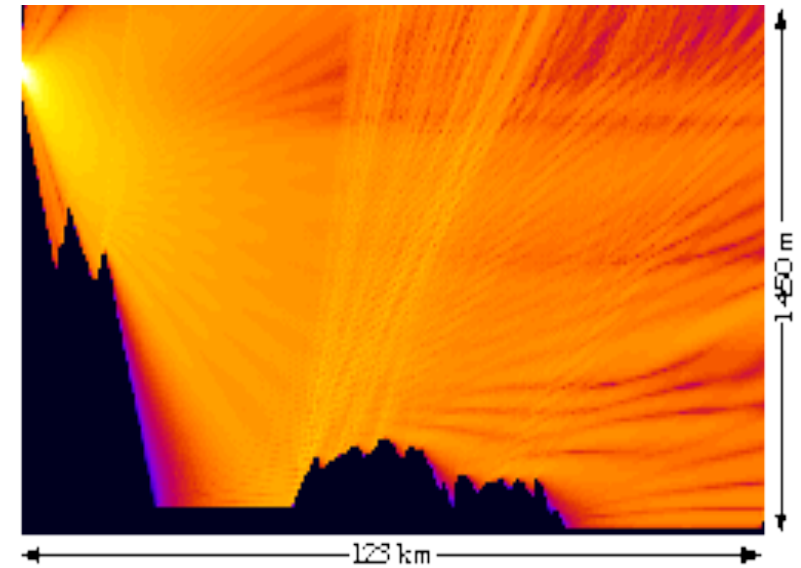
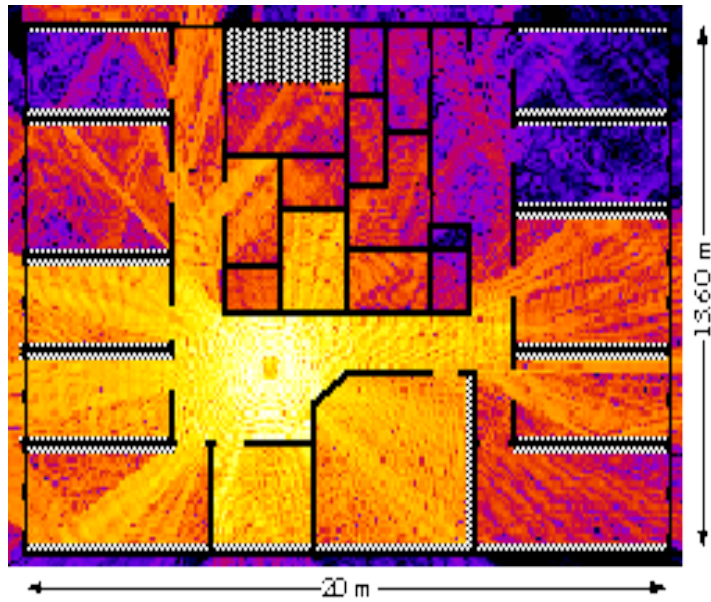


scattering



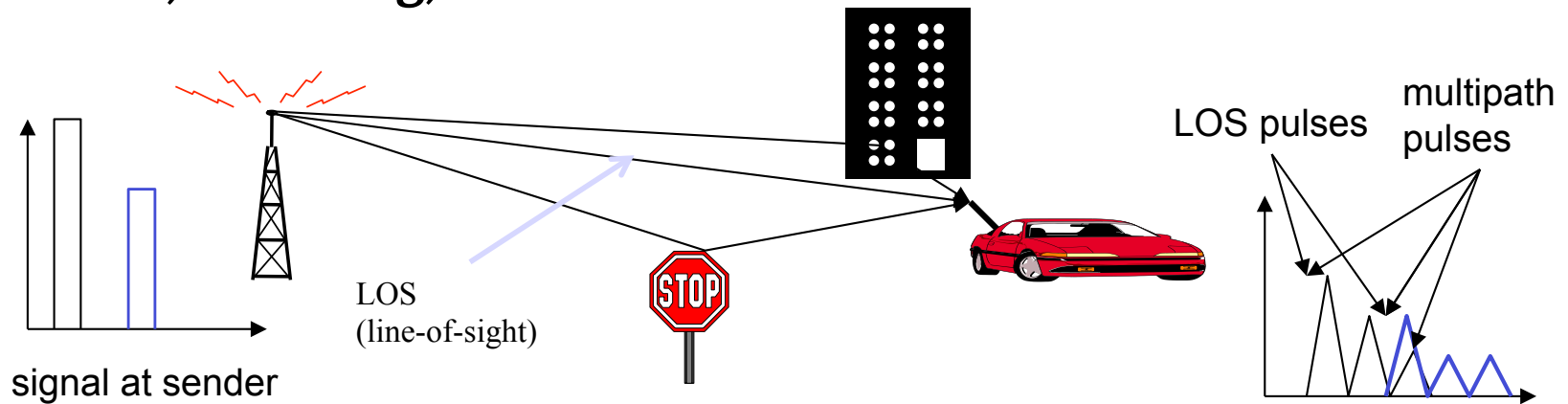
diffraction

Real world examples



Multipath propagation

- Signal can take many different paths between sender and receiver due to reflection, scattering, diffraction

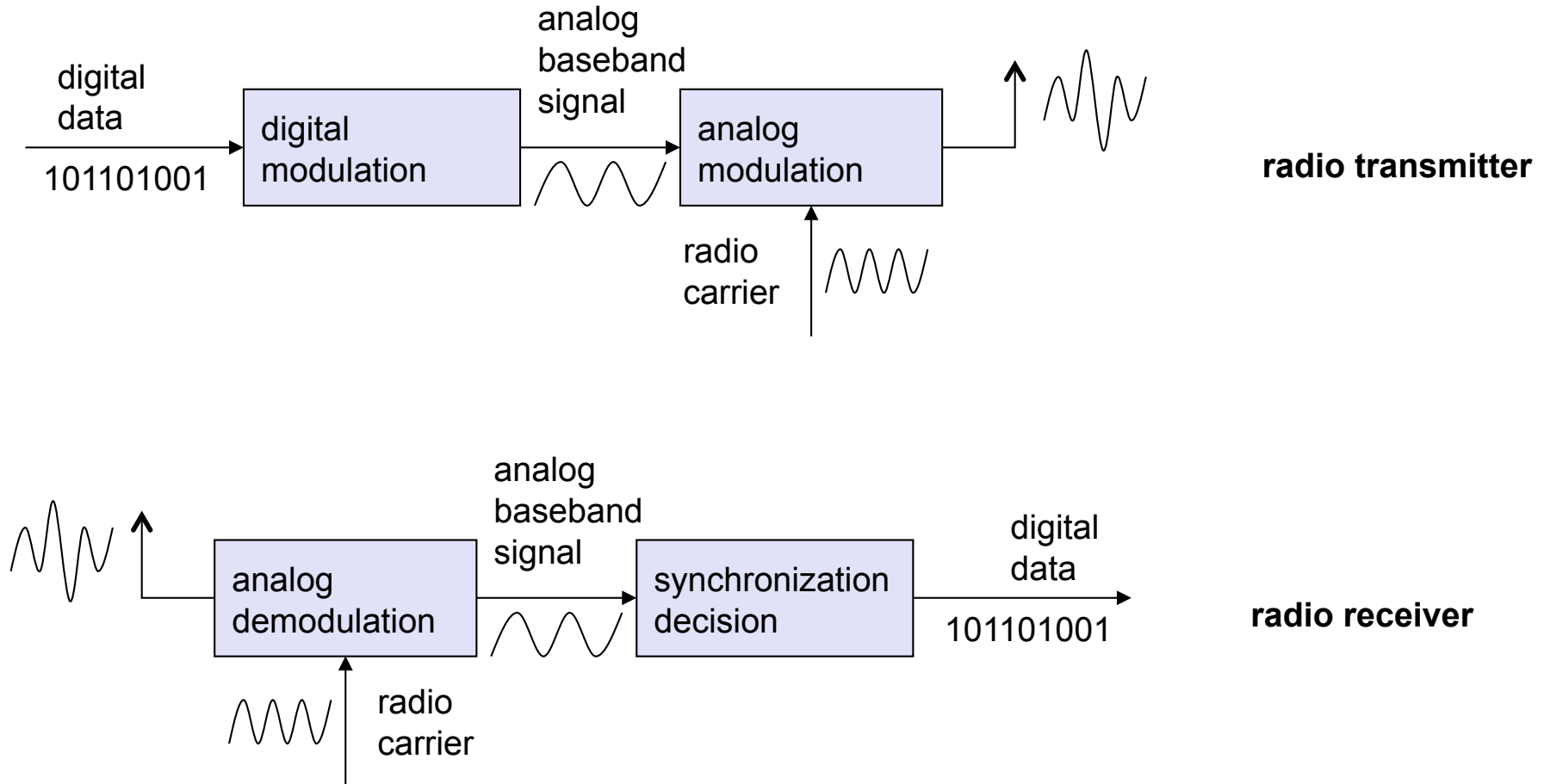


- Time dispersion: signal is dispersed over time
 - Inter Symbol Interference (ISI)
- The signal reaches a receiver directly and phase shifted
 - distorted signal depending on the phases of the different parts

Modulation & Coding

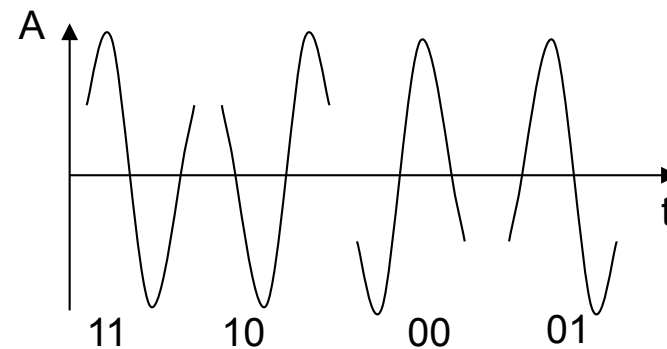
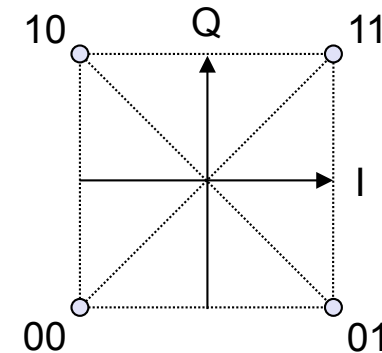
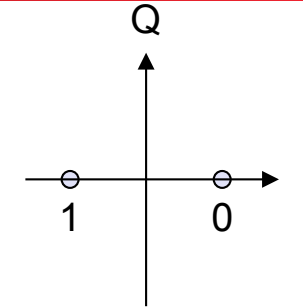
- **Digital modulation**
 - digital data is translated into an analog signal (baseband)
 - PSK (Phase Shift Keying)
- **Coding**
 - Digital data recast for “optimal” transmission
- **WiFi**
 - MCS = modulation and coding scheme

Modulation and demodulation



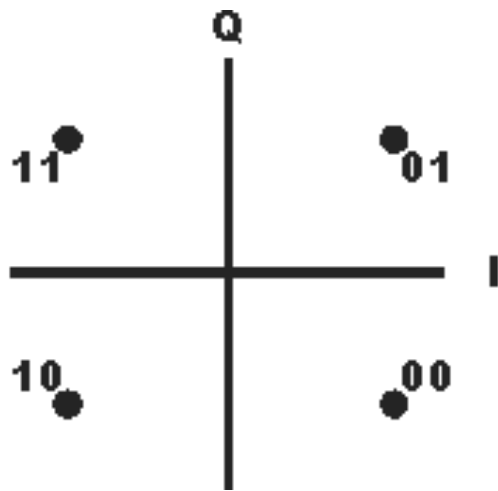
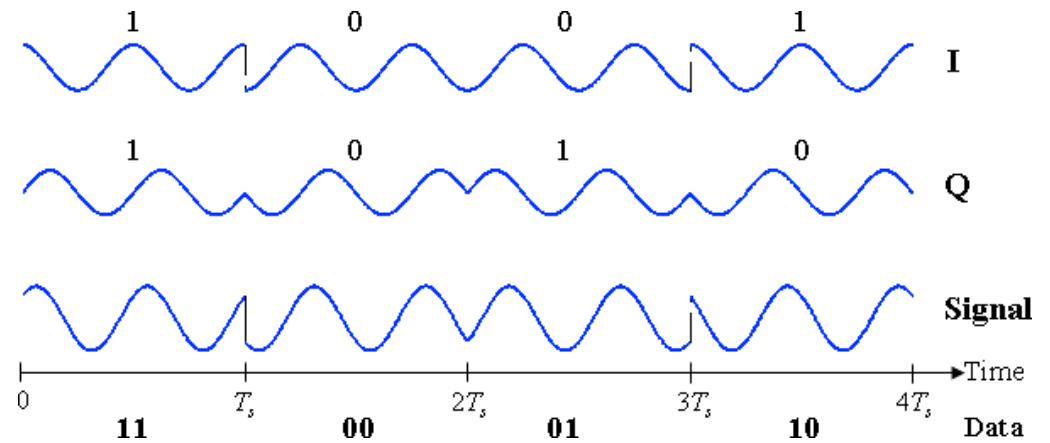
Phase Shift Keying

- **BPSK (Binary PSK):**
 - bit value 0: sine wave
 - bit value 1: inverted sine wave
 - very simple PSK
 - low spectral efficiency
 - robust
- **QPSK (Quadrature PSK):**
 - 2 bits coded as one symbol
 - symbol determines shift of sine wave
 - needs less bandwidth than BPSK
 - more complex

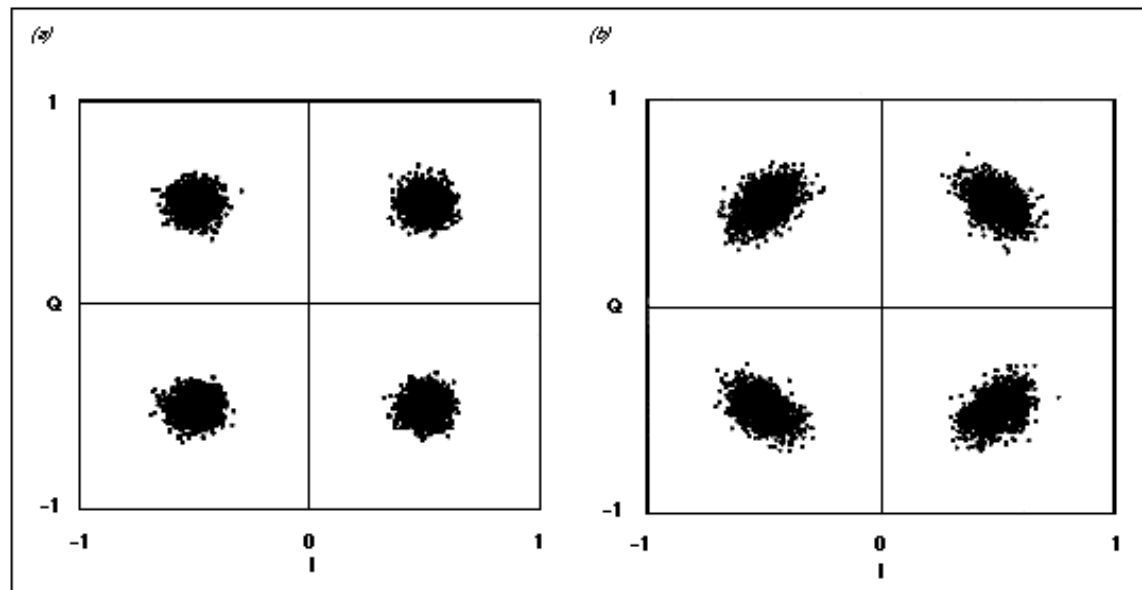


Modulații BPSK, QPSK

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



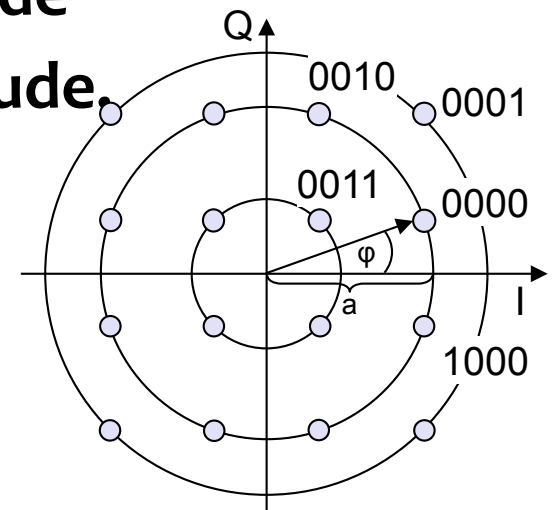
teoretic



real

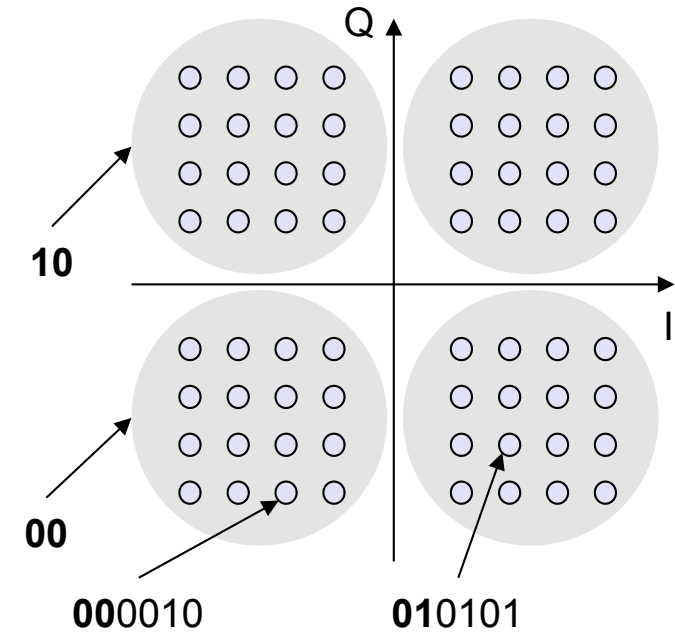
Quadrature Amplitude Modulation

- Quadrature Amplitude Modulation (QAM)
 - combines amplitude and phase modulation
 - it is possible to code n bits using one symbol
 - 2^n discrete levels, $n=2$ identical to QPSK
- Bit error rate increases with n , but less errors compared to comparable PSK schemes
- 16-QAM (4 bits = 1 symbol)
 - 0011, 0001 same phase, different amplitude
 - 0000, 1000 different phase, same amplitude.



Hierarchical Modulation

- Example: 64QAM

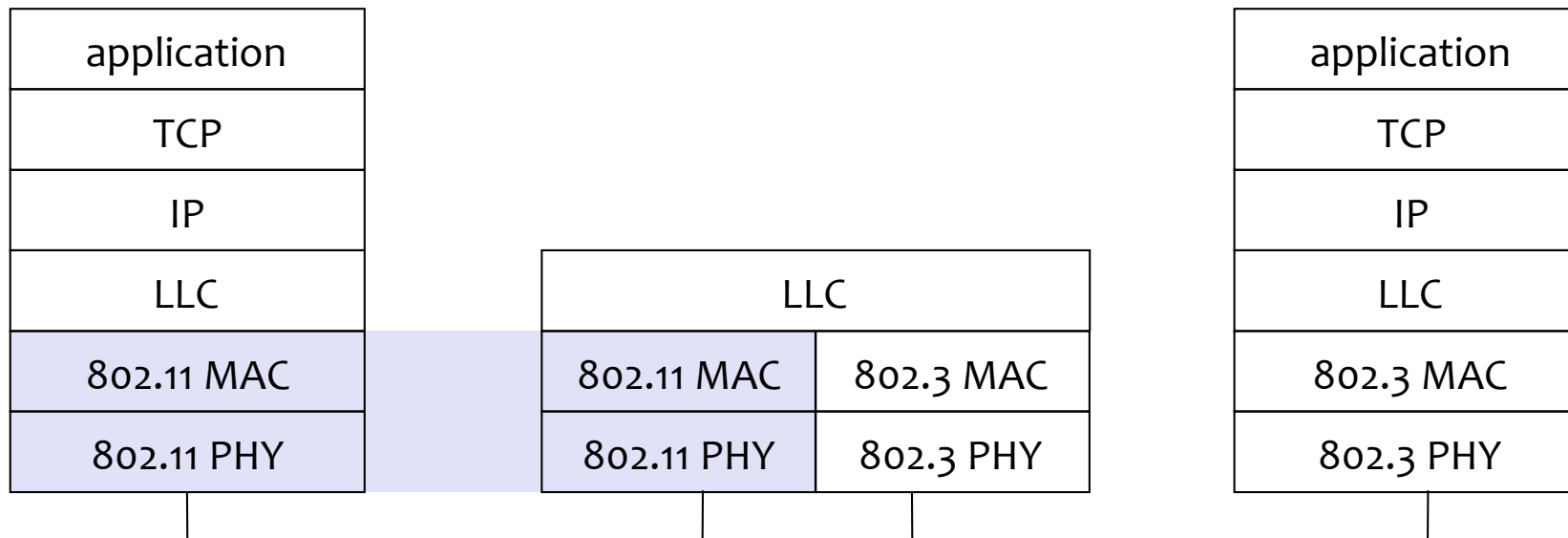
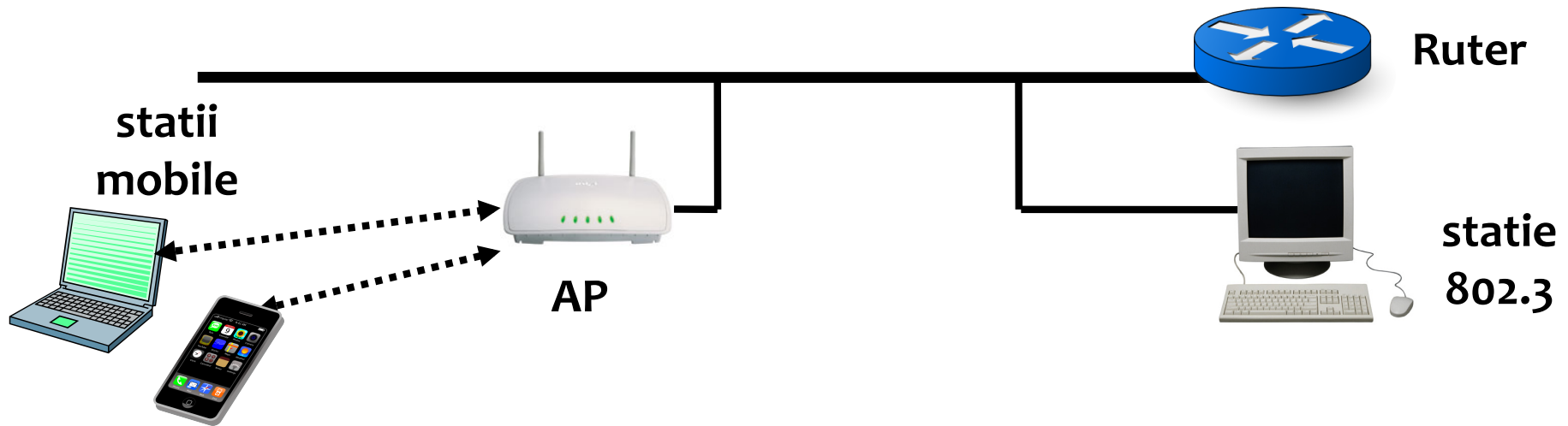


- 802.11ac uses 256QAM



Standard 802.11

exemplu 802.11 + 802.3



nivelele 802.11

<i>nivel egatura de date</i>	Subnivel MAC Medium Access Control	Gestiune MAC	gestiune statie
<i>nivel fizic</i>	Subnivel PLCP (Physical Layer convergence procedure)	gestiune PHY	
	Subnivel PMD (Physical medium Dependent)		

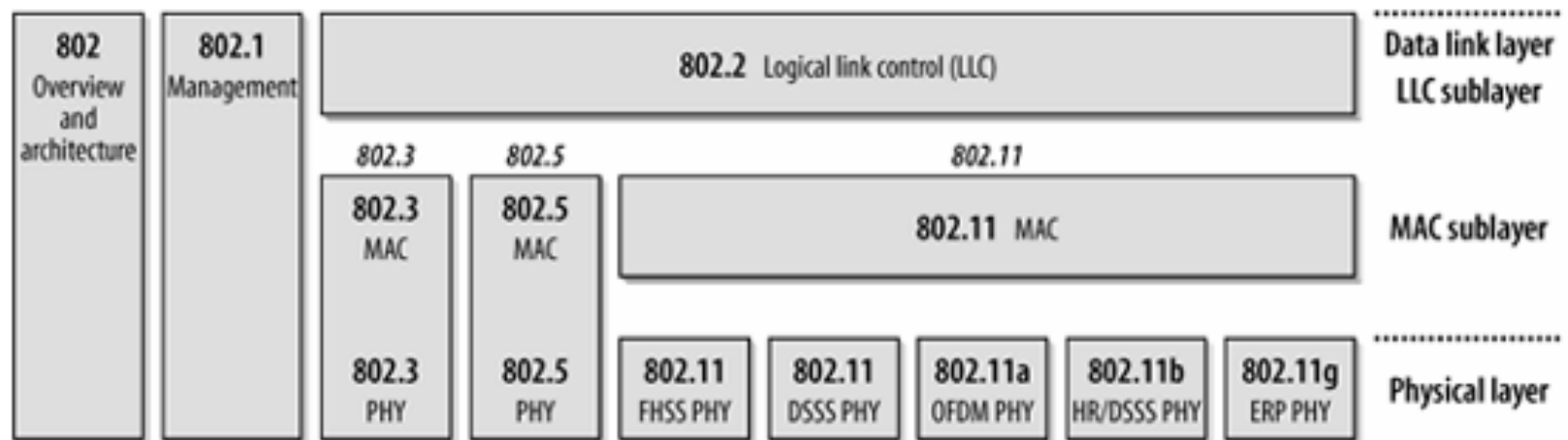
802.11 nivele, funcții

- 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 folosesc DSSS

6, 9, 12, 18, 24, 36, 48, 54, folosesc OFDM

802.11b

- Frecvențe fara licenta ISM (industrial științific medical) **2.4GHz**

- Un canal $f_{\text{sus}} - f_{\text{jos}} = \mathbf{22\text{ MHz}}$

- DSSS în fiecare canal

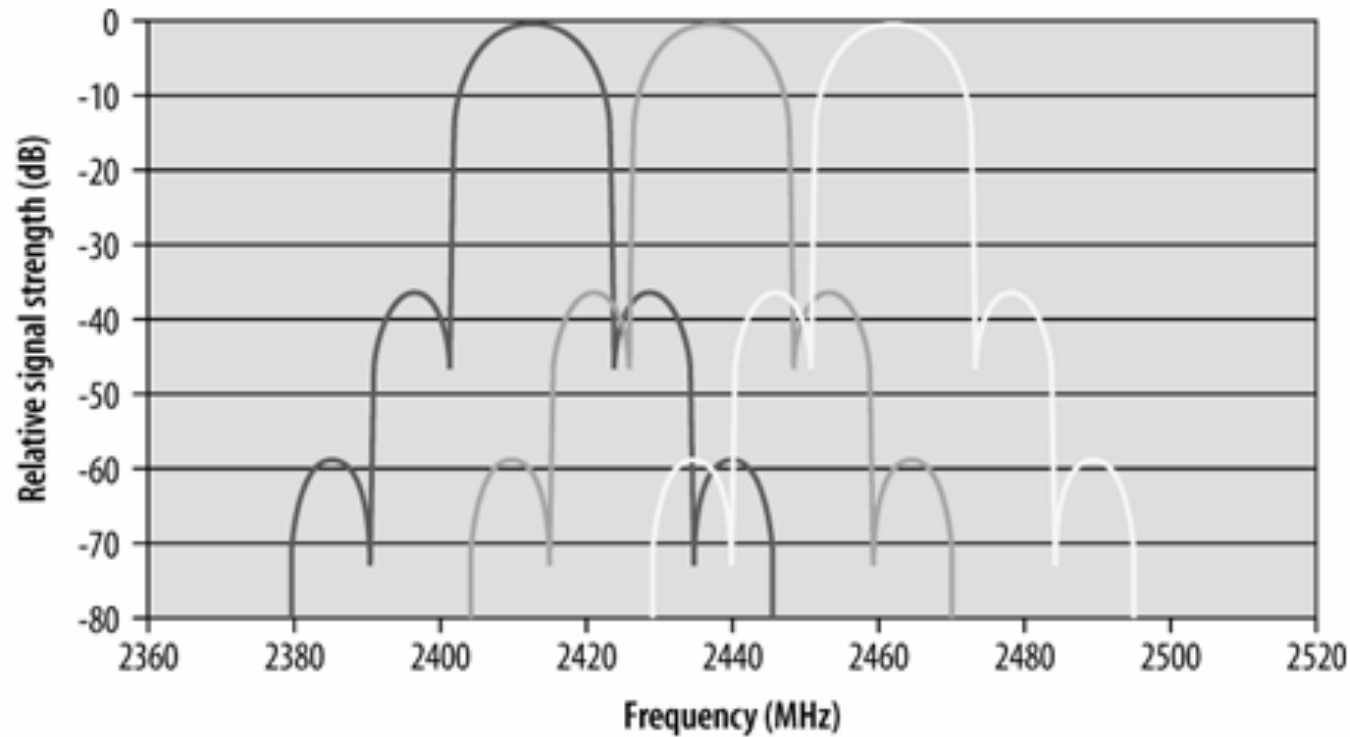
- **3 canale independente**

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



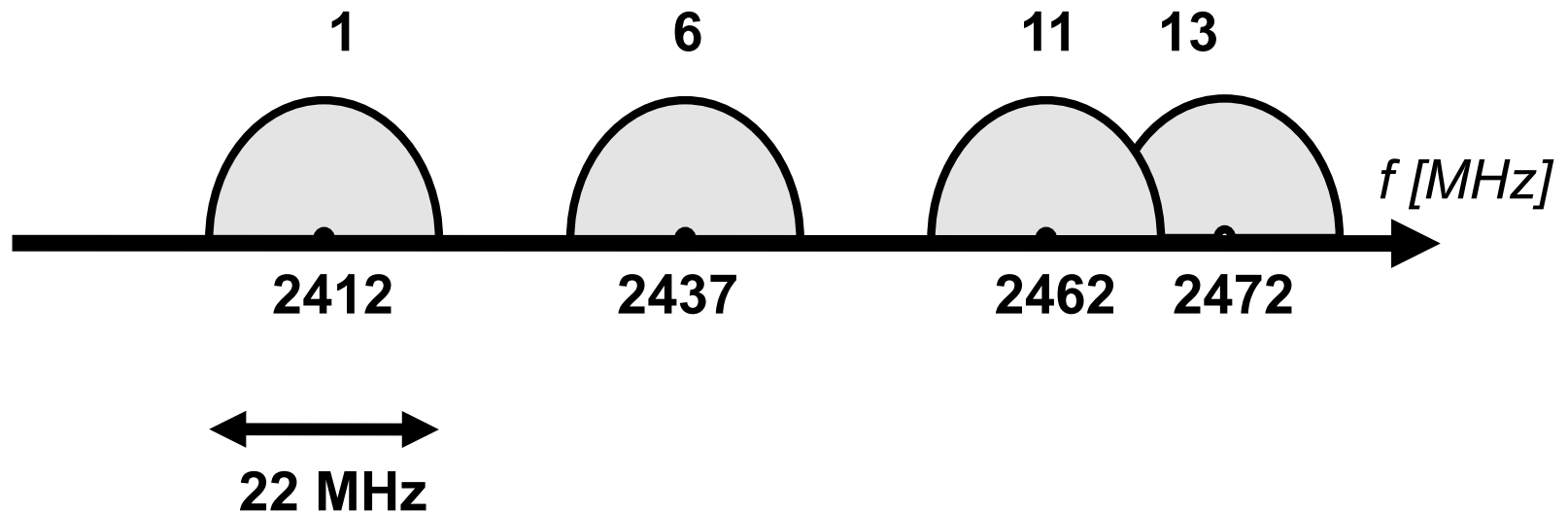
KEY

— Channel 1 — Channel 11
— Channel 6

dispunerea canalelor 2.4GHz

Europa: 1-13

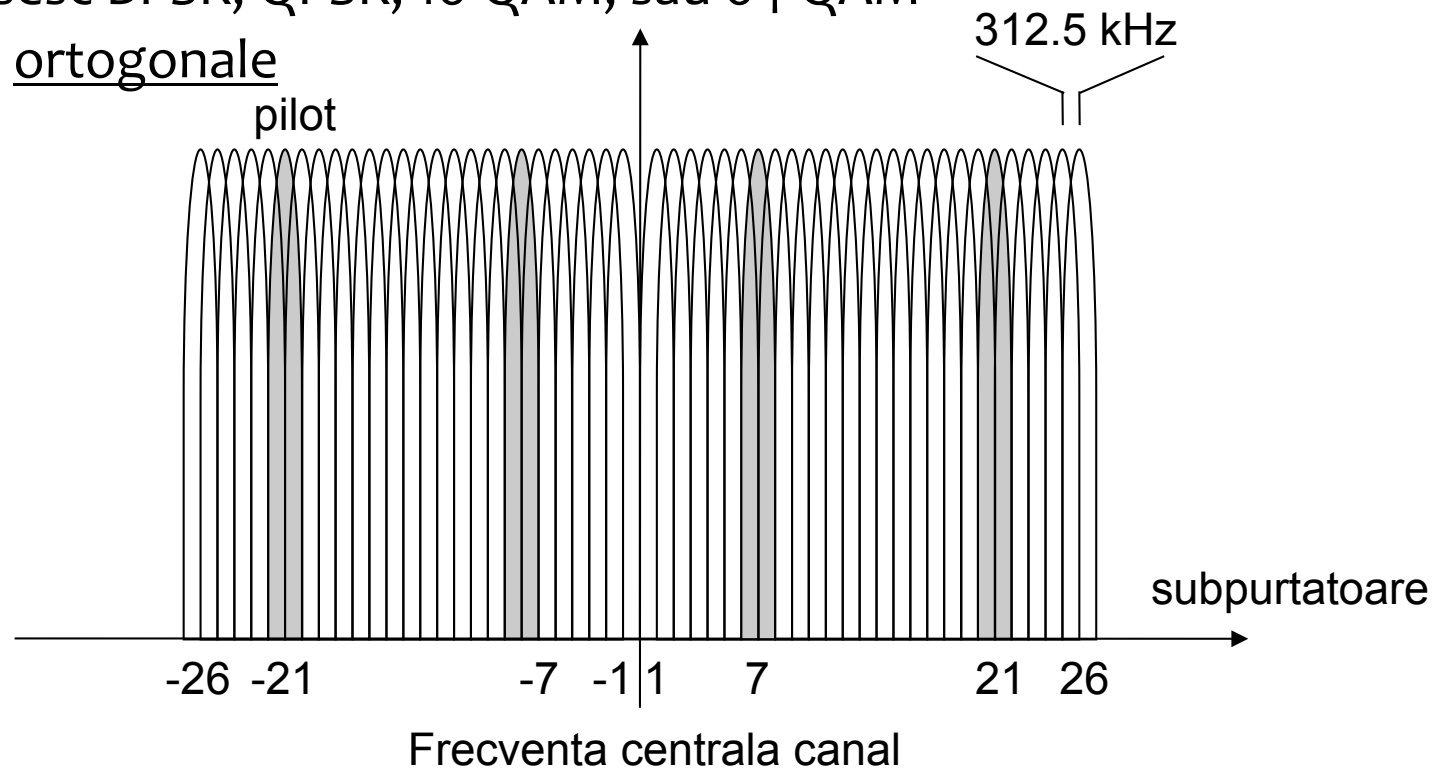
SUA/Canada 1-11



OFDM in 802.11a,g,n,ac

- 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



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 @25°C)

Constelațiile mai bogate necesită putere mai mare!

802.11g

54Mbps (64QAM): -76dbm

48Mbps (64QAM): -71dbm

36Mbps (16QAM): -78dbm

24Mbps (16QAM): -80dbm

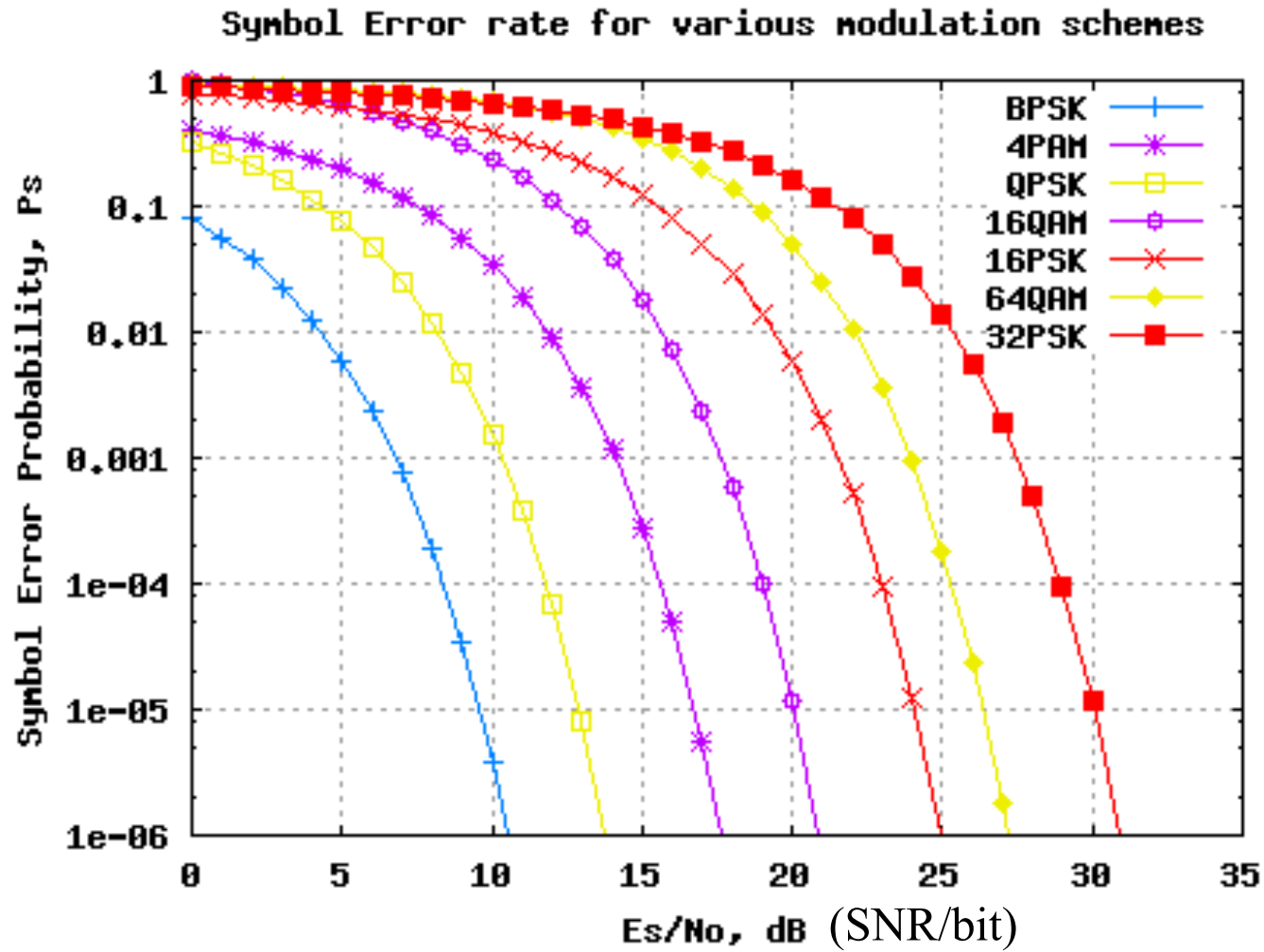
18Mbps (QPSK): -81dbm

12Mbps (QPSK): -82dbm

9Mbps (BPSK): -85dbm

6Mbps (BPSK): -91dbm

(typically @PER < 10% packet size
1024 and @25°C)

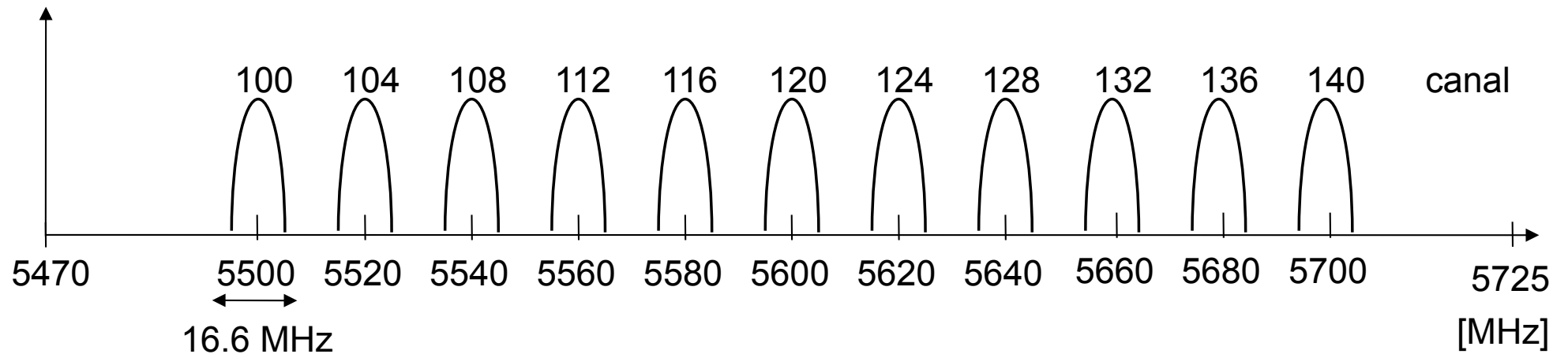
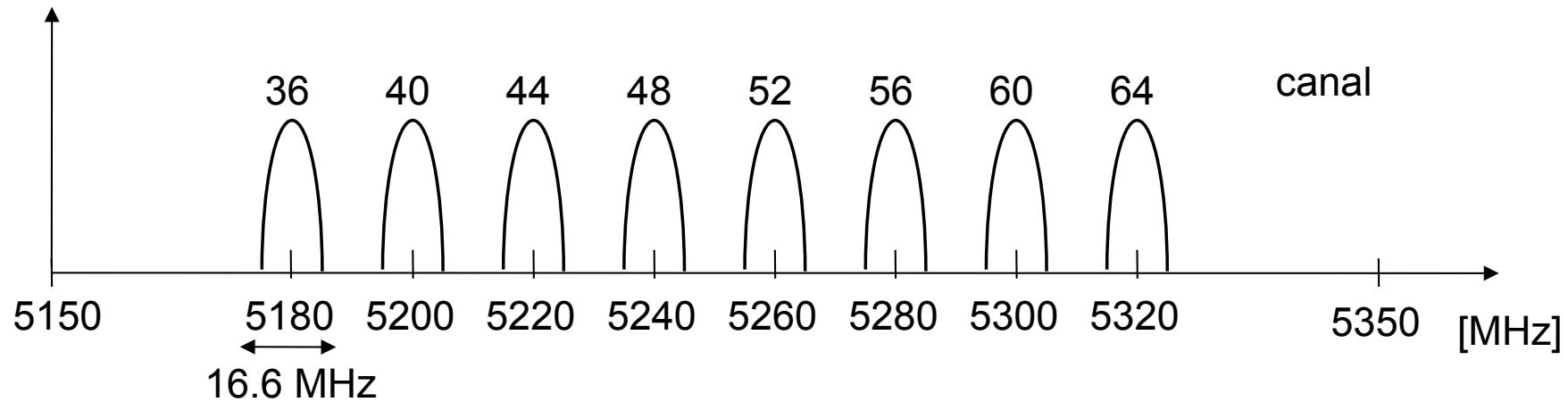


Constelațiile mai bogate necesită putere mai mare

IEEE 802.11a - caracteristici

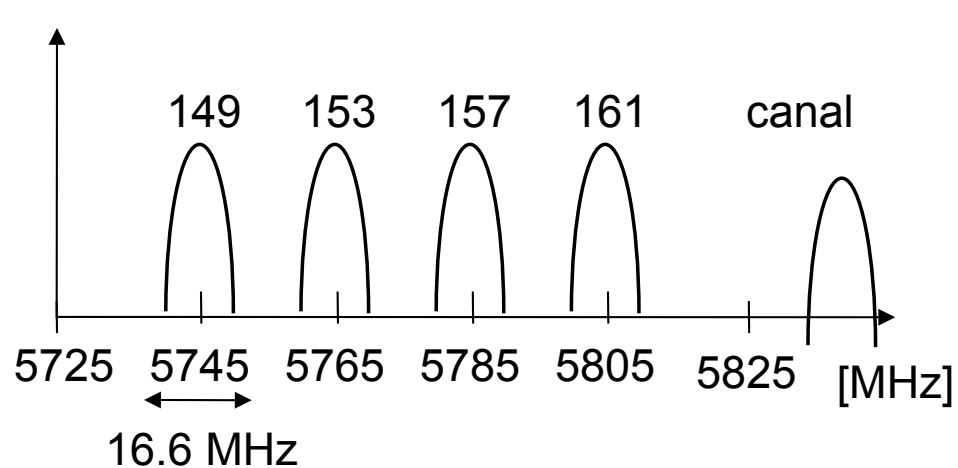
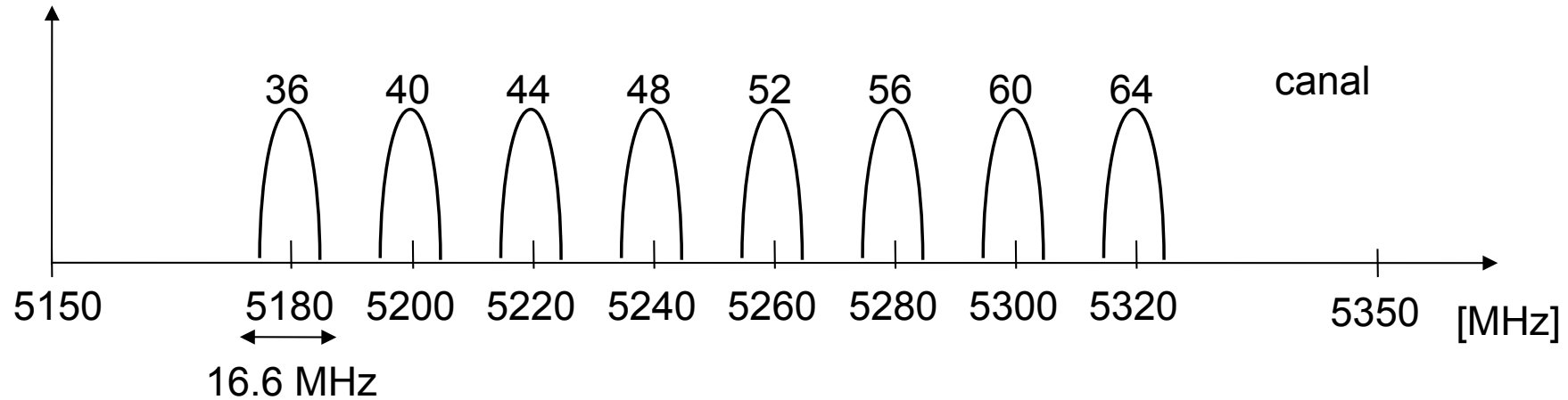
- rate
 - » 6, 9, 12, 18, 24, 36, 48, 54 Mbps, in functie de SNR
 - » Rata la utilizator (pachete mari): 5.3 (6), 18 (24), 24 (36), 32 (54)
 - » 6, 12, 24 Mbps obligatorii
- Aria de transmisie
 - » 100m exterior, 30m interior
- Frecvente
 - » 5.15-5.25, 5.25-5.35, 5.725-5.825 GHz, canale: 12 (SUA), 19 (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)



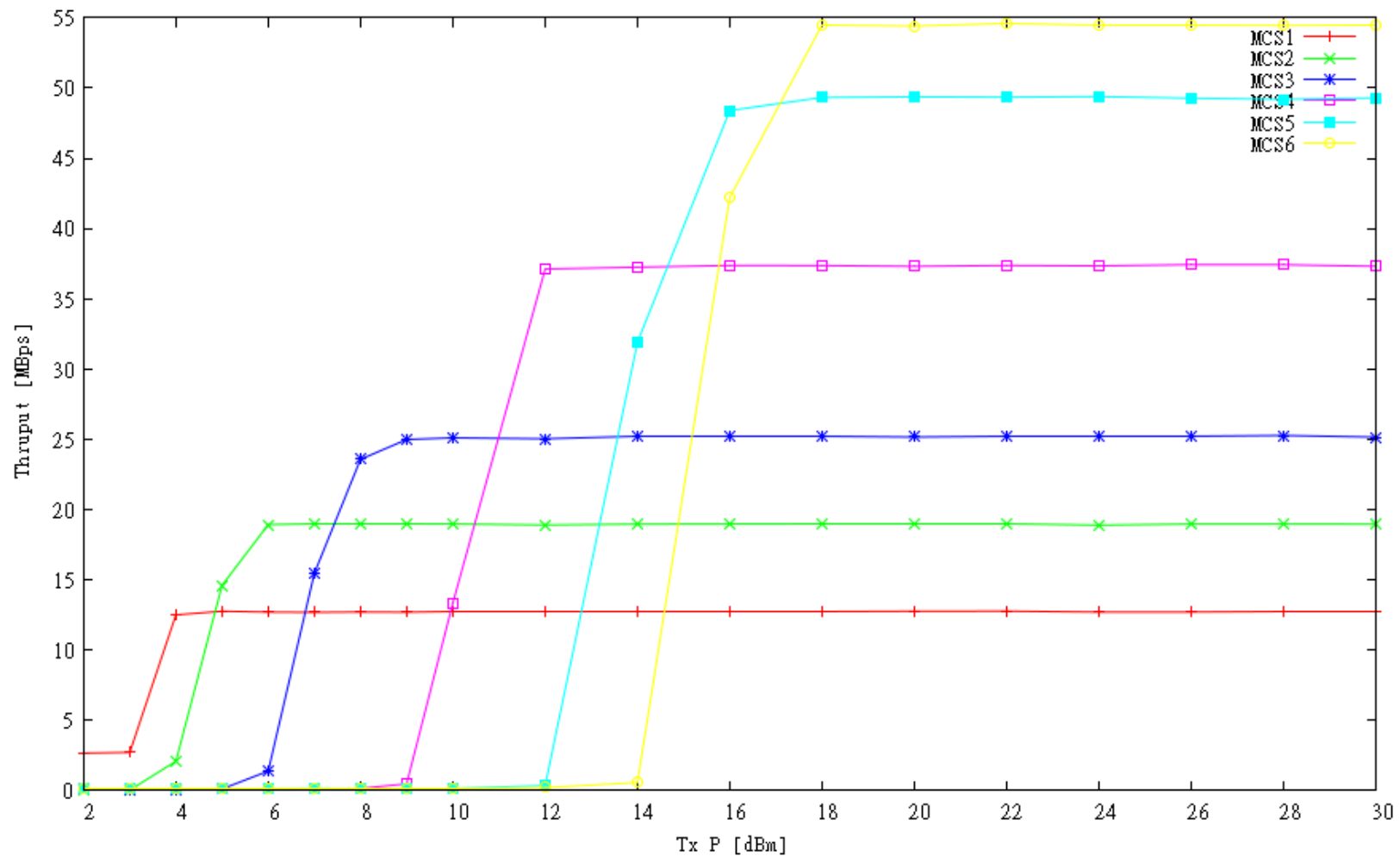
Frecventa centrala [MHz] =
 $5000 + 5 \cdot \text{numar canal}$

Canale 802.11a (SUA/Canada)



Frecventa centrala [MHz] =
 $5000 + 5 * \text{canal}$

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



Propagare 802.11a

- De ce propagarea este mai slabă la 5GHz?

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

d = distanța

f = frecvența purtătoarei

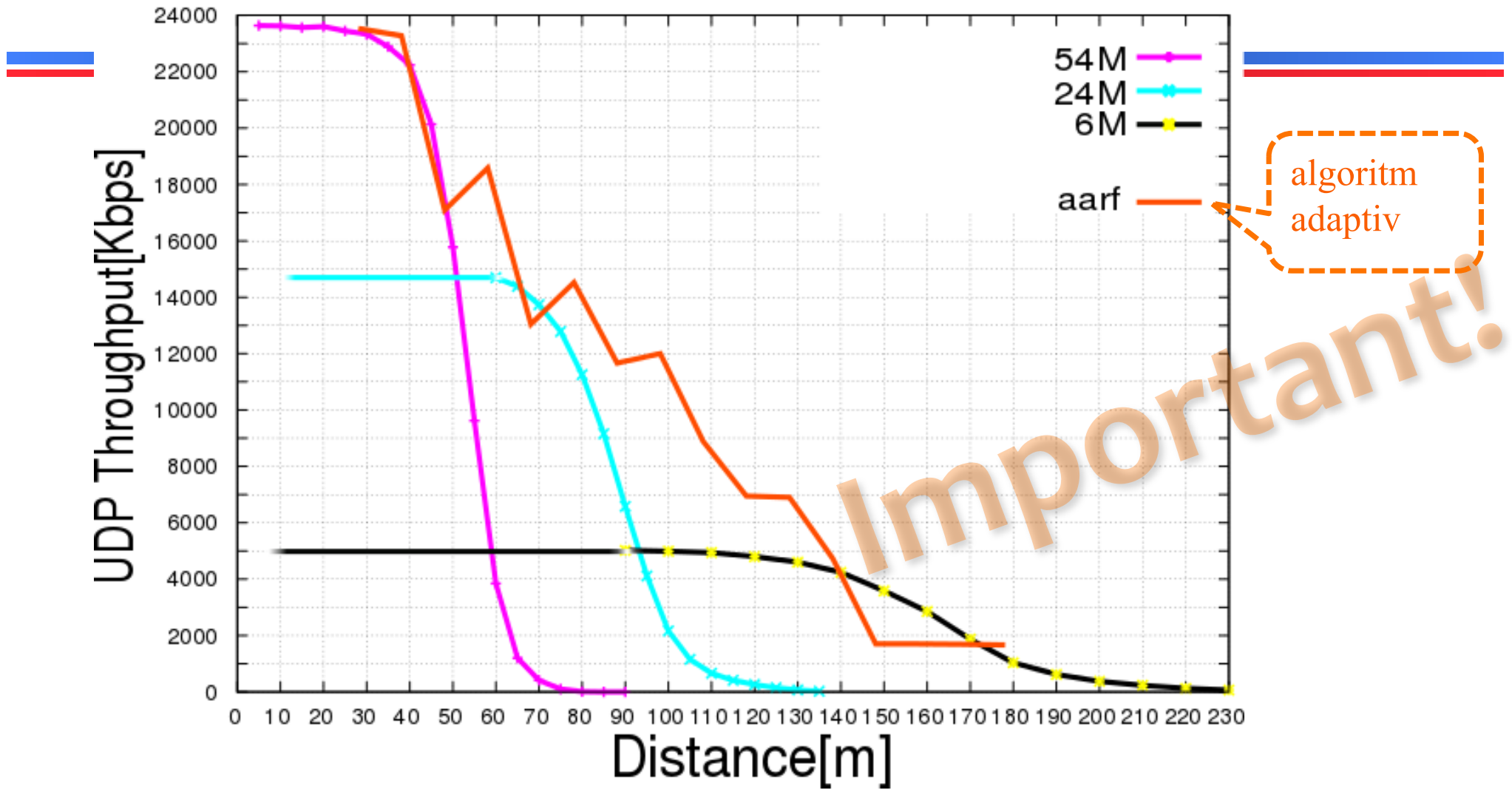
n = exponent

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

ns-3 simulation: 802.11g, Nakagami, 3log distance



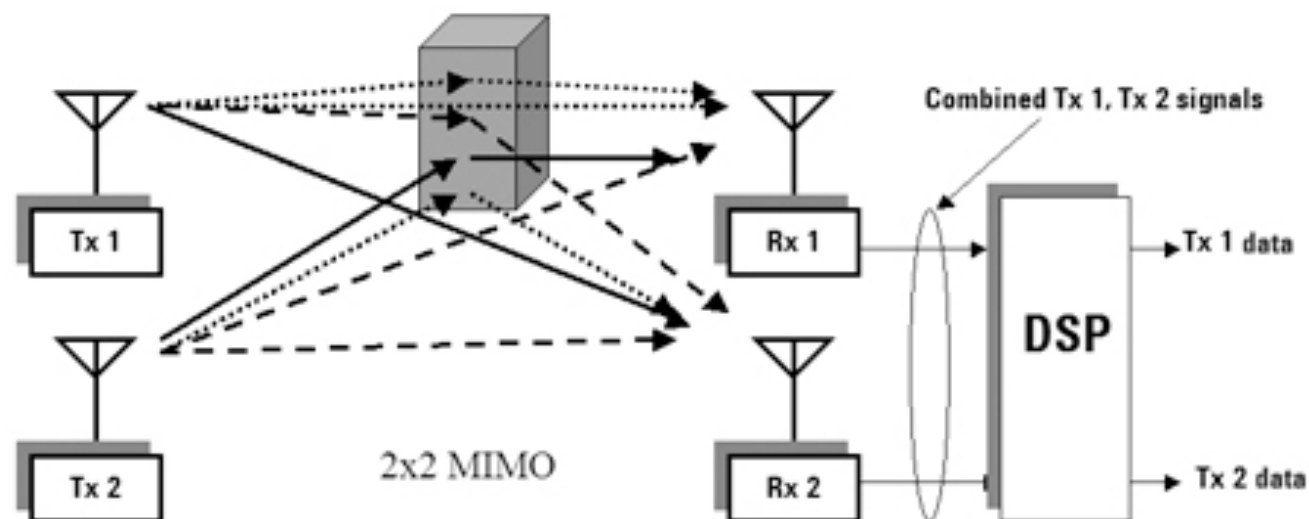
Constelațiile mai bogate necesită putere mai mare...
... funcționează la distanță mai mică

802.11n (2009)

- 2.4GHz și 5GHz, backward compatible cu a/b/g
 - Metode de coexistență cu dispozitivele vechi
- Canale de 40Mhz
 - Ocupă 80% din spectrul 2.4GHz
- Agregare de cadre
 - Block acknowledgement
- Max 600Mbps
- Distanțe crescute: 70m interior
- MIMO cu maximum 4 antene

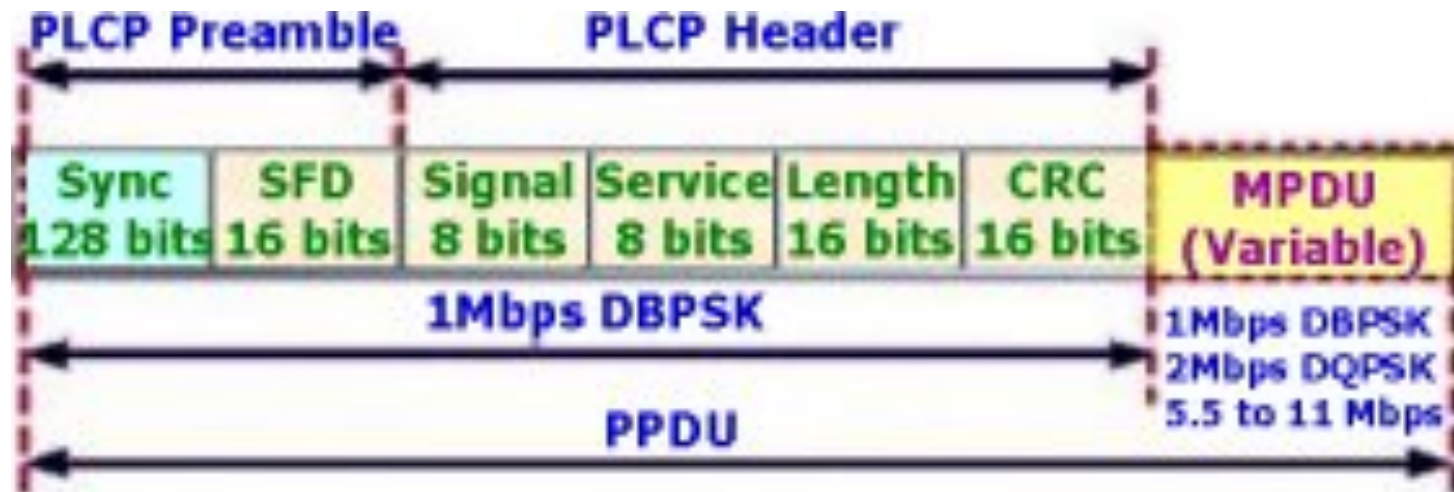
MIMO

- Multiple-Input Multiple-Output
 - Antene multiple la emițător și la receptor
 - MCS **și** distanțe ridicate, fără putere adițională
- Funcții
 - **Beamforming**: emite același semnal pe toate antenele => maximizare recepție
 - **Spatial multiplexing**: fluxuri diferite pe antene diferite, **aceeași purtătoare**
 - **Diversity coding**: emite același semnal codat diferit pt a exploata diversitatea

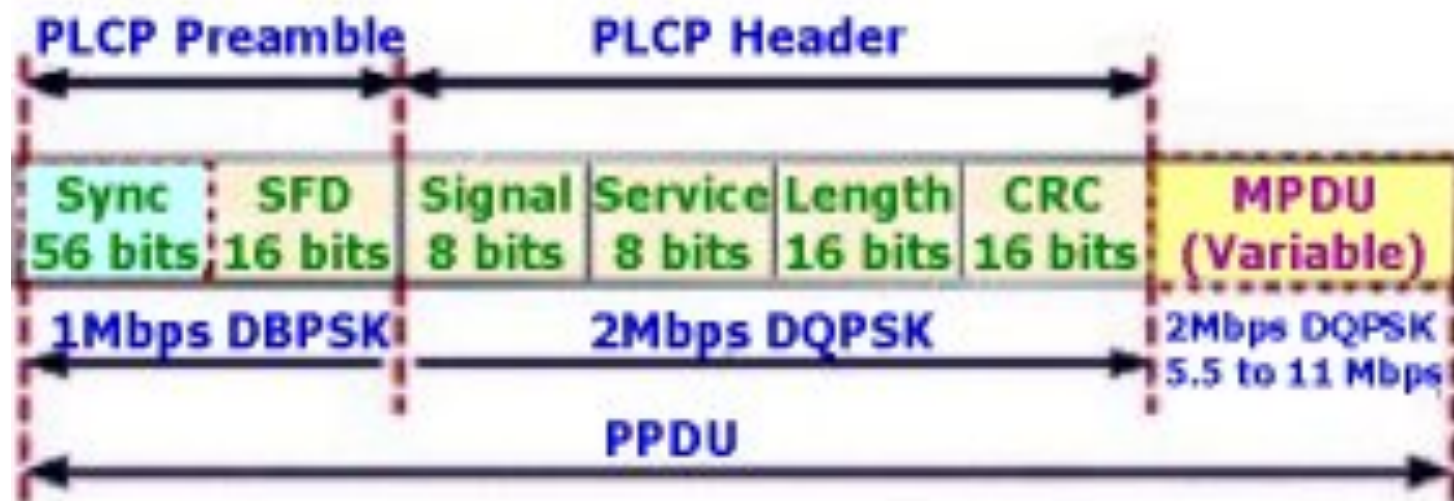


Exemplu antet nivel fizic (802.11b)

long
preamble
192us



short
preamble
96us
(VoIP, video)



Nivelul access la mediu

wired == wireless?

- Asemănări cu Ethernet:

- » wireless e un mediu partajat
- » interferența între transmițători
- » CSMA (carrier sense multiple access)
 - stația emițătoare detectează prezența altor stații
 - “ascultă înainte de a transmite”
- » de dorit:
 - o singură stație transmite la un moment dat
 - eficiență, echitate

- Diferențe:

- » CD (detectia coliziunilor) dificilă:
 - O singură antenă, comunicare simplex
- » Canale de calitate slabă: BER, variabilitate în spațiu/timp
- » Terminal ascuns, terminal expus

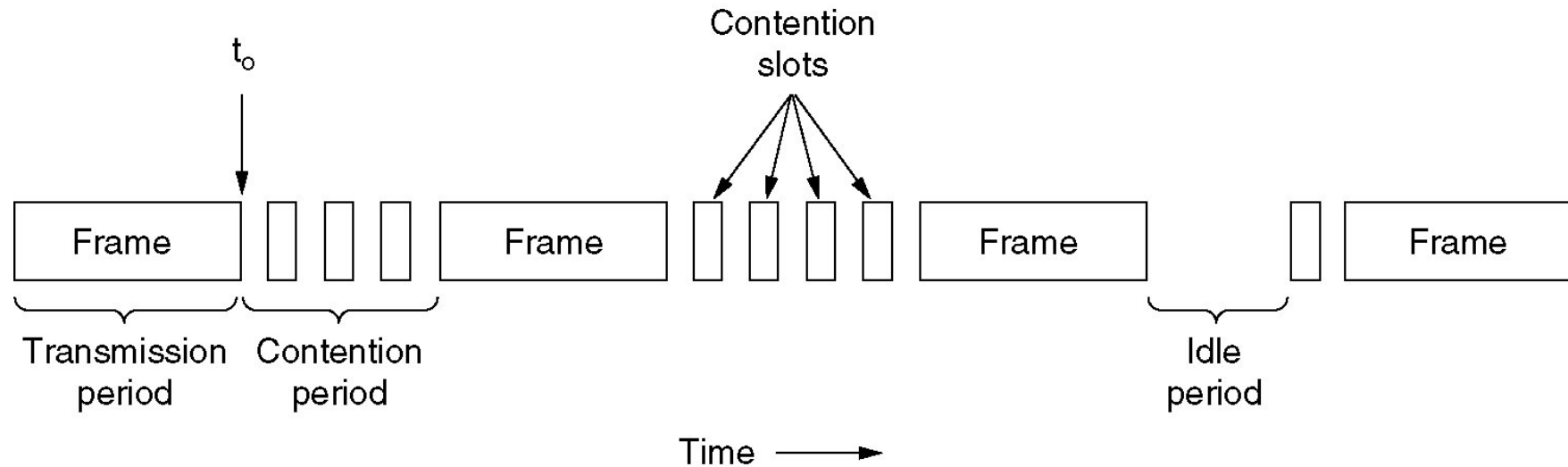
Carrier Sense

- 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 detectează prezența purtătoarei unei alte stații
 - » Depinde de implementare => prag (decibeli)

Recapitulare Ethernet

CSMA/CD = carrier sense multiple access with collision detection

Ethernet - CSMA/CD

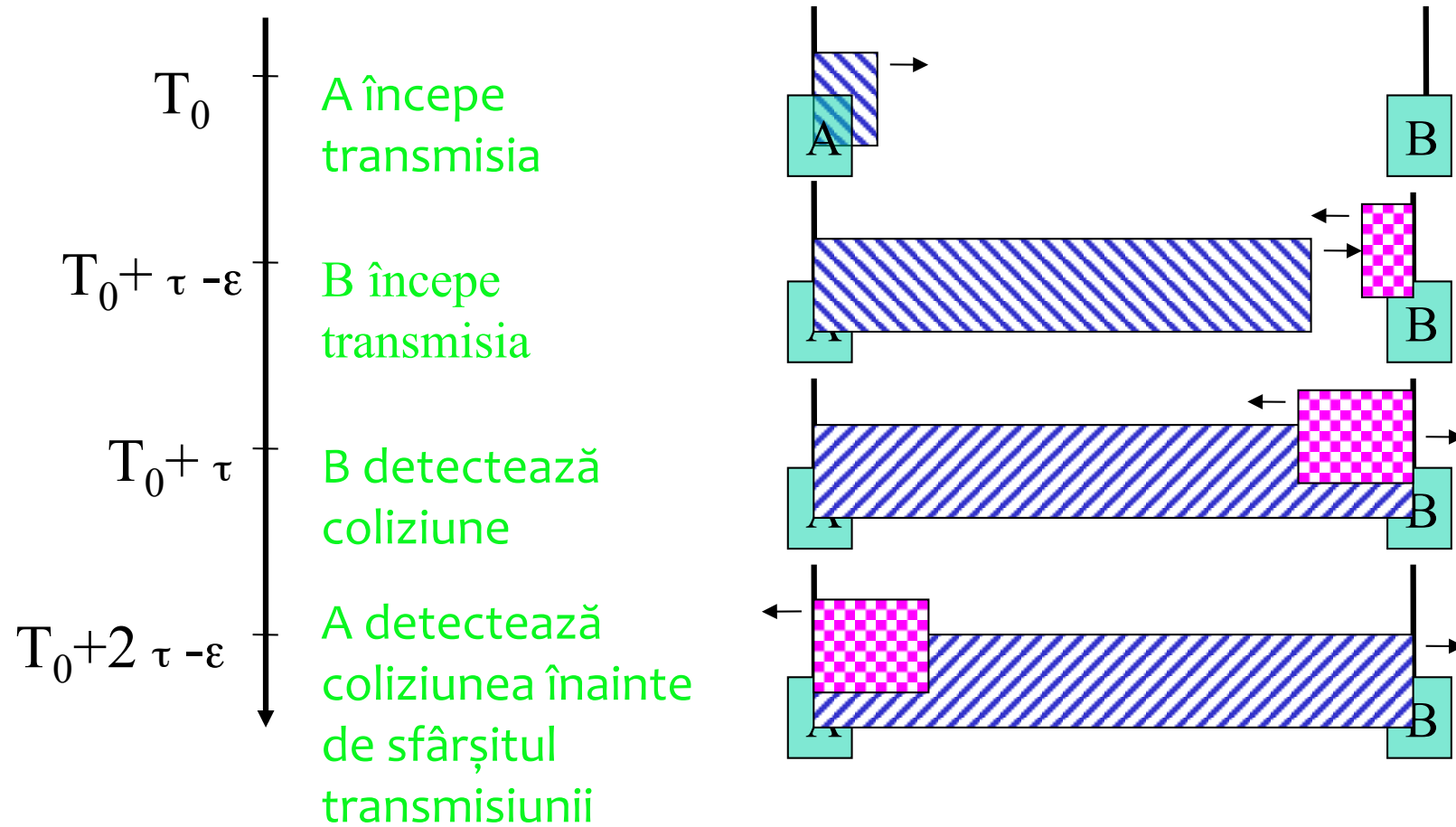


Cât durează detecția coliziunii?

- 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 $\Rightarrow 2\tau$

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 $2\tau = 50\mu\text{s}$
 - 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)

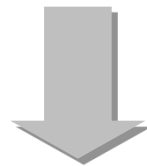
ALGORITM

- După coliziunea k , se așteaptă aleator între 0 și $2^k - 1$ sloturi
- 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

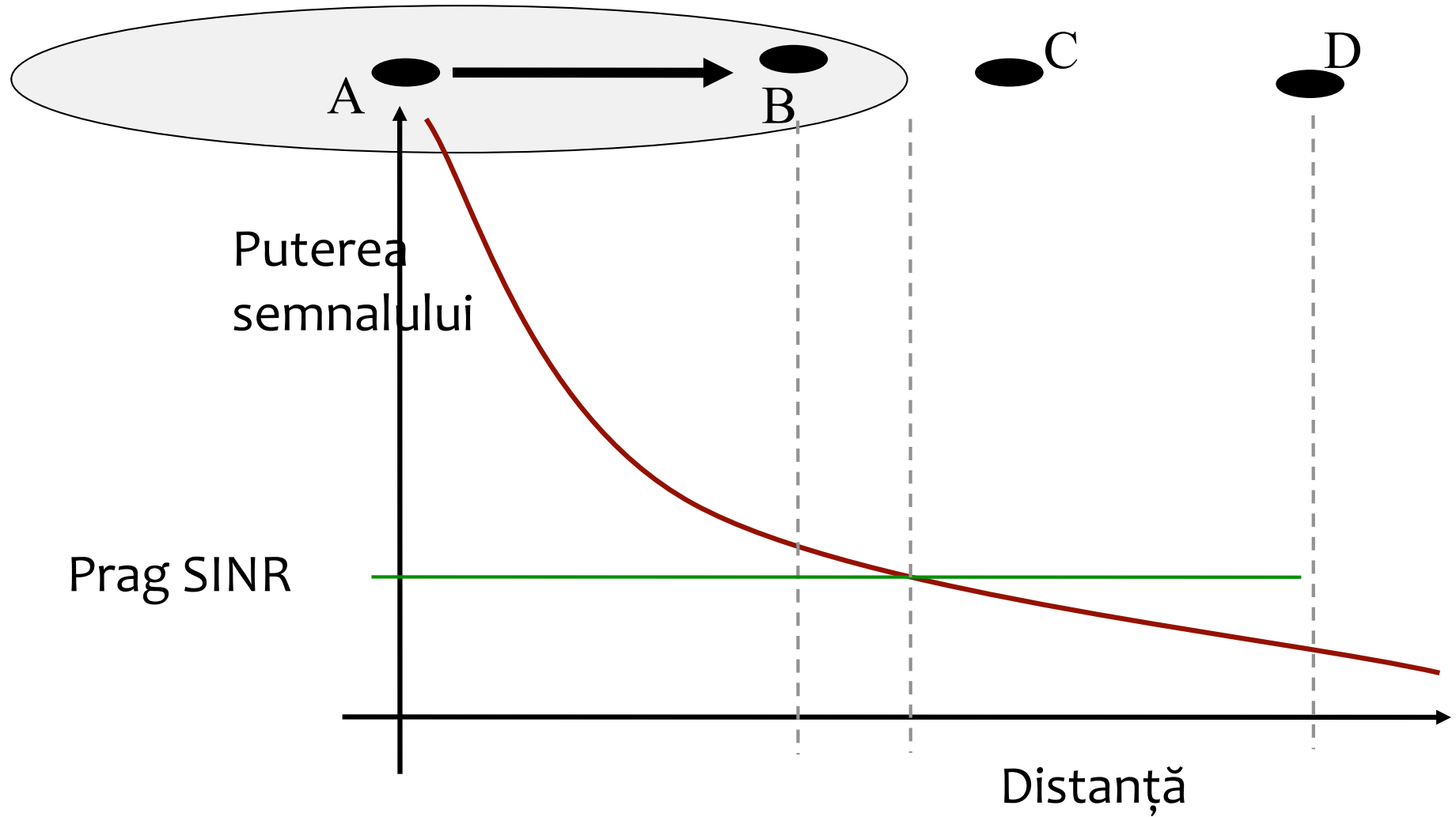


TRANSMIȚĂTORUL poate detecta dacă și când se produce coliziunea

Din nefericire...

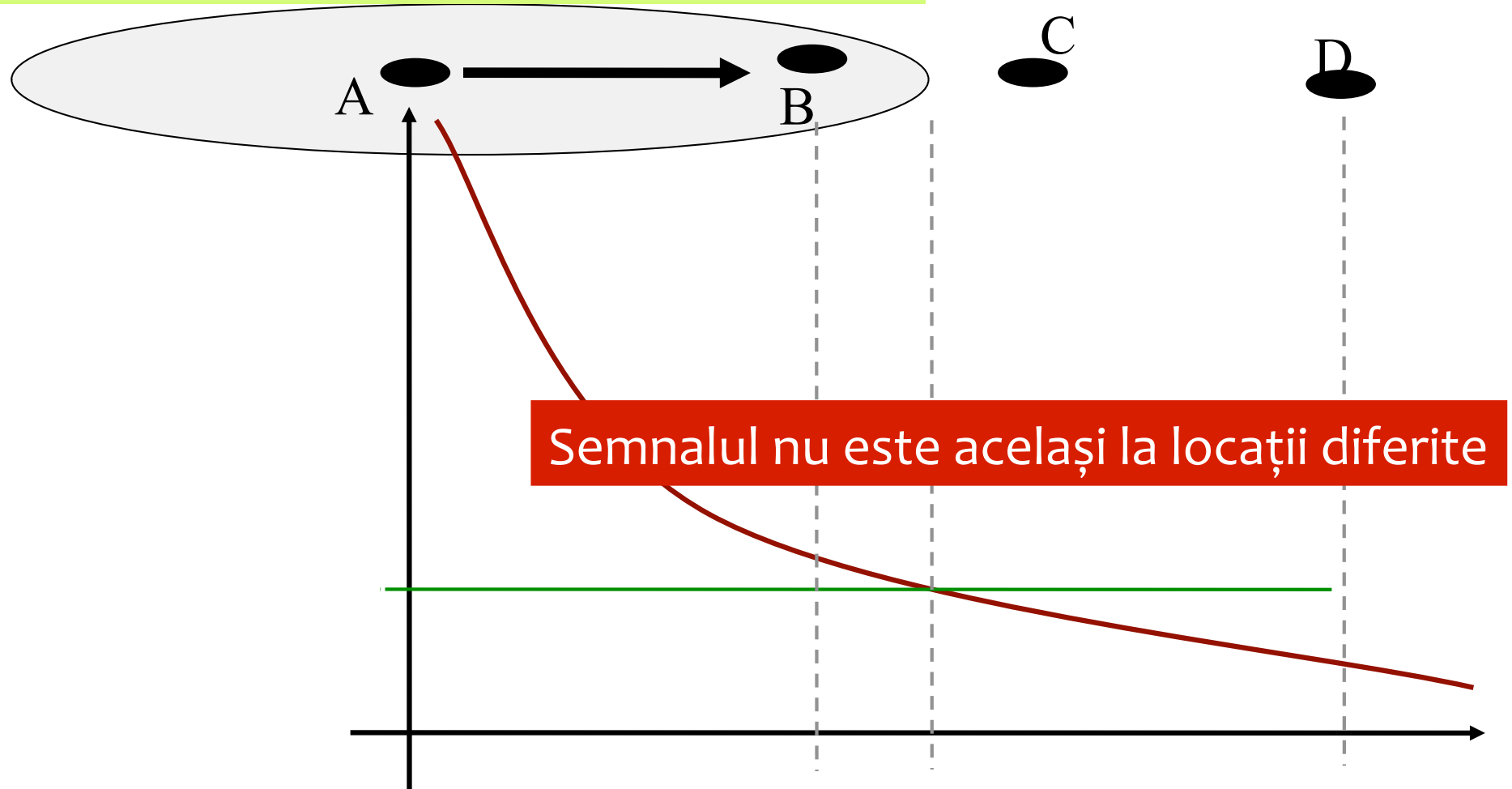
Nici una din cele două observații nu este valabilă în wireless, deoarece...

Wireless MAC

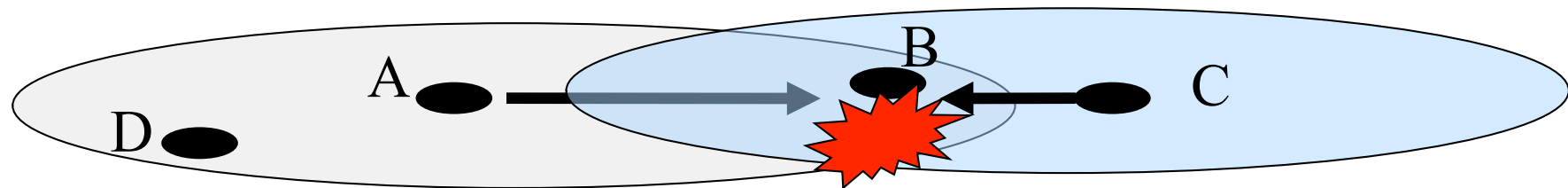


Mediul wireless dispersează energia

A nu poate trimite și recepționa simultan



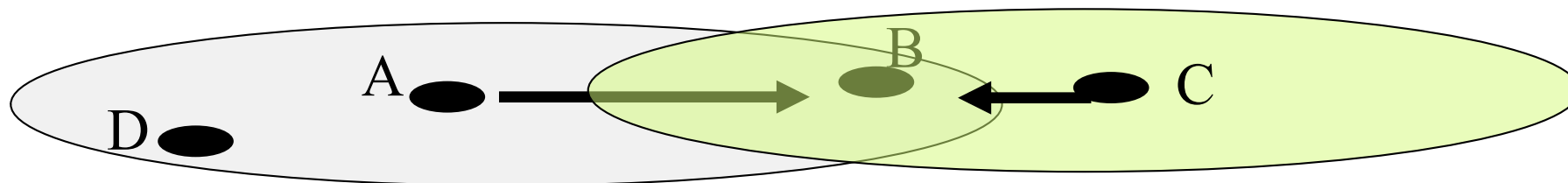
Detecția coliziunilor dificilă



Recepția semnalelor bazată pe SINR

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

Calculul SINR



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

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

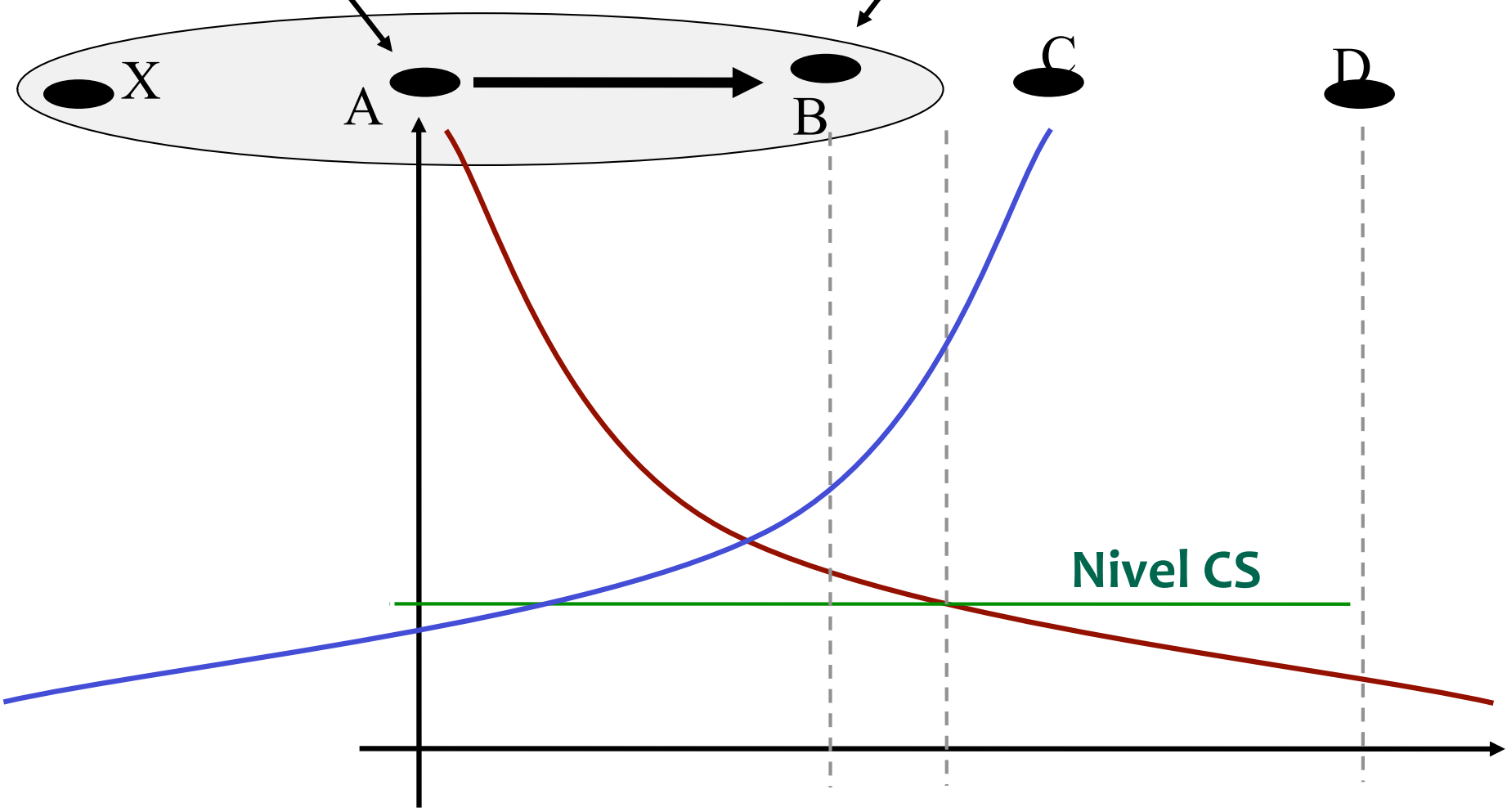
$$I_B^C = \frac{P_{transmit}^C}{d_{CB}^\alpha}$$



$$SINR_B^A = \frac{\frac{P_{transmit}^A}{d_{AB}^\alpha}}{N + \frac{P_{transmit}^C}{d_{CB}^\alpha}}$$

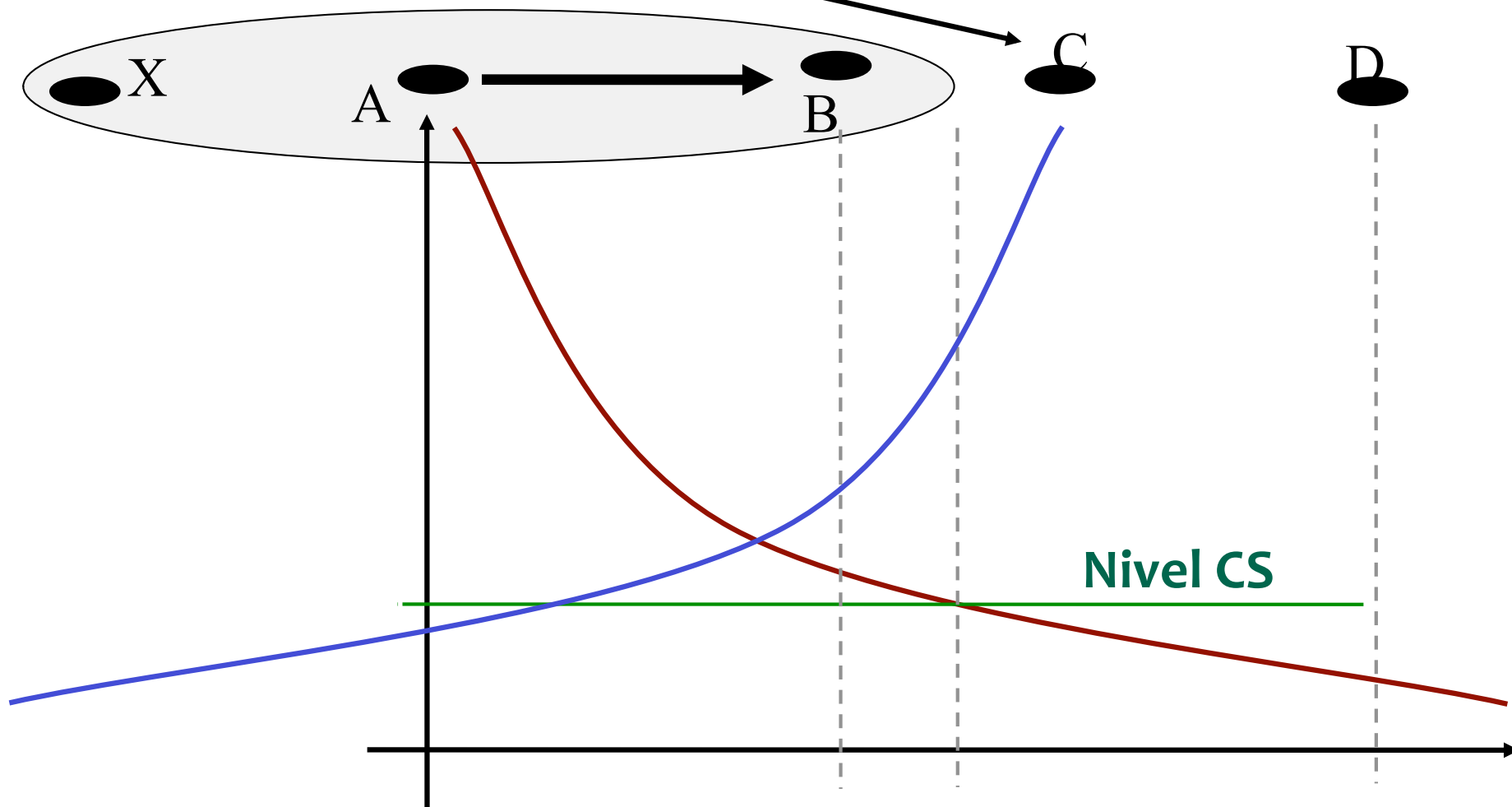
Roşu \gg albastru

Roşu $<$ albastru = coliziune



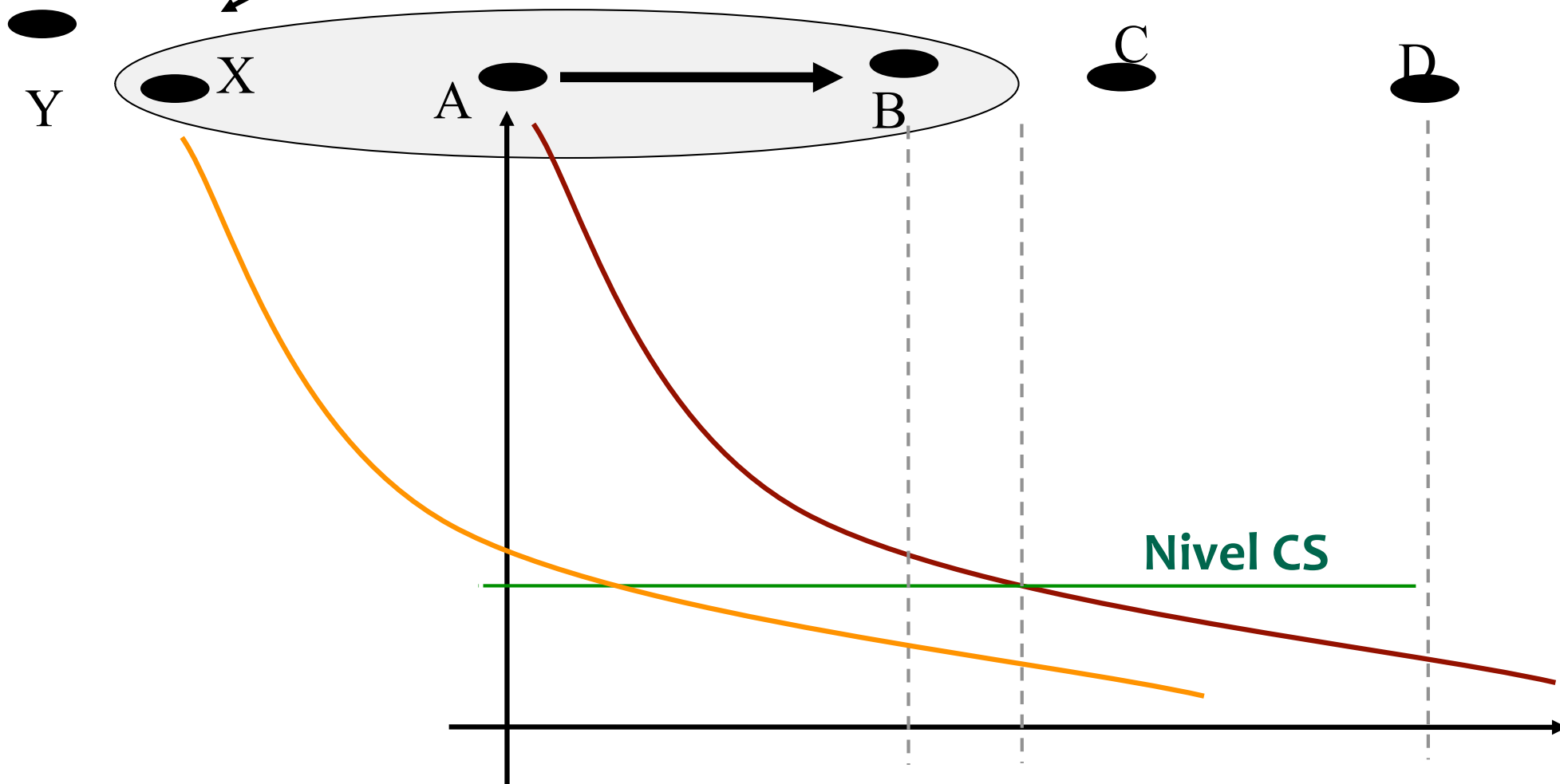
Important: C nu-l aude pe A, produce interferenta la B

C este terminal ascuns pt A



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

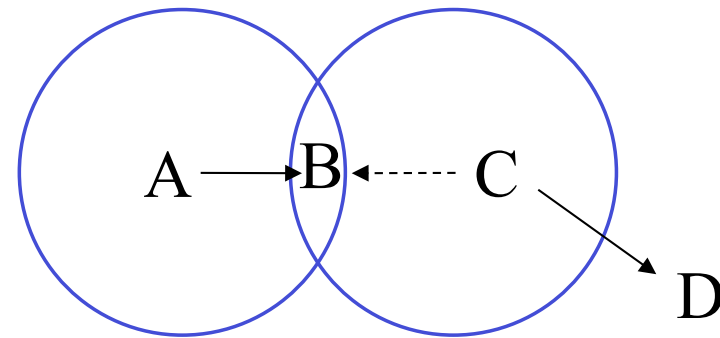
X este terminal expus pentru A



Sumar terminale ascunse, expuse

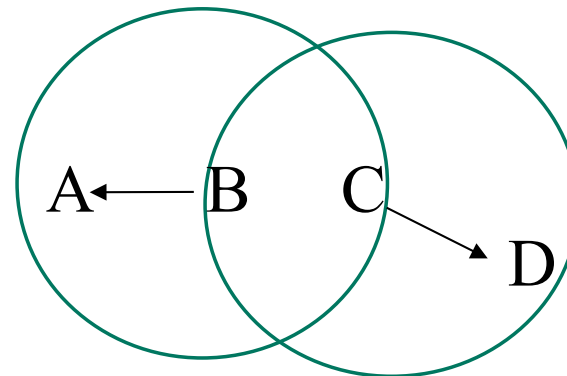
● Terminal ascuns

- » A si C pot transmite in același timp



● Terminal expus

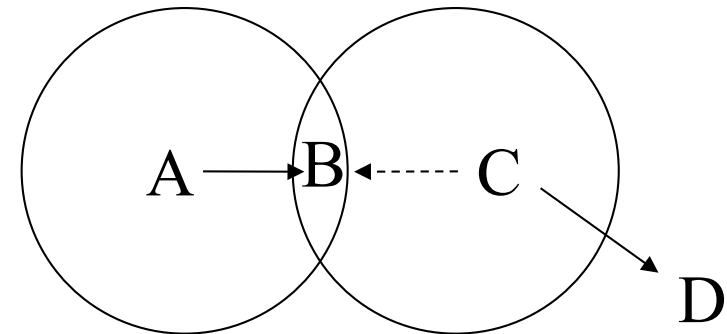
- » B si C nu pot transmite in același timp



terminale ascunse, expuse

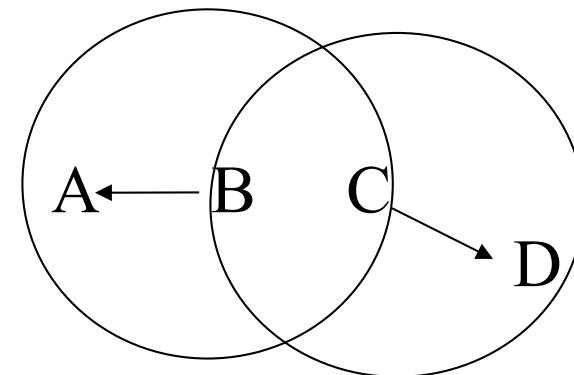
- Situațiile reale sunt rareori doar TA sau doar TE

- canale asimetrice
- hardware diferit
- Combinații de TA, TE



- Captura: TA, dar la B $P_A > P_C + 10\text{dB}$

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



802.11 - MAC

● Acronime

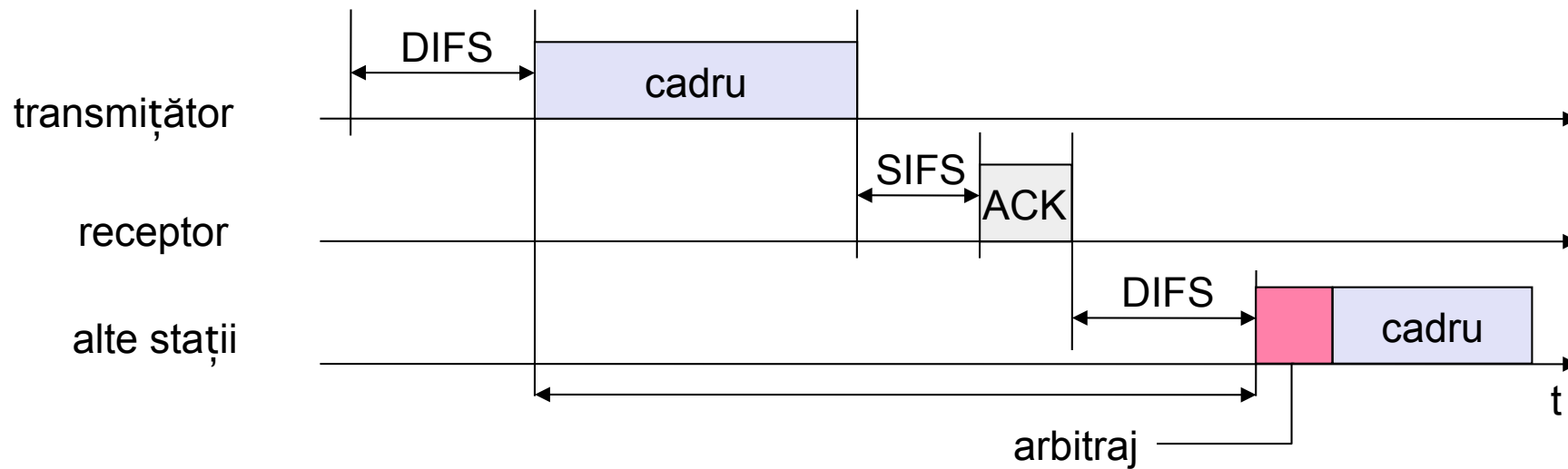
- » DCF (Distributed Coordination Function) - acces asincron
- » PCF (Point Coordination Function) - acces sincron
- » CSMA/CA - carrier sense multiple access, collision avoidance

● Metode de acces

- » DCF + CSMA/CA (obligatoriu)
 - politica de tip “best-effort”
 - broadcast and multicast
 - Evitarea coliziunilor (CA) prin „back-off” randomizat
 - Distanța minimă între pachete consecutive
 - ACK
- » DCF + RTS/CTS (optional, dar implementat)
 - minimizează terminalele ascunse
- » PCF (*optional*)
 - AP oferă accesul pe baza unei liste

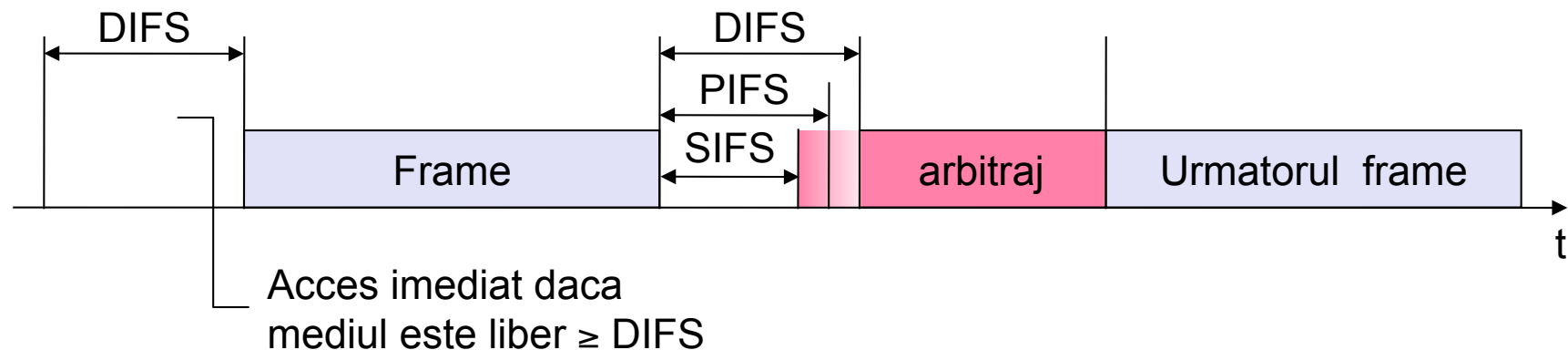
802.11 Date unicast

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

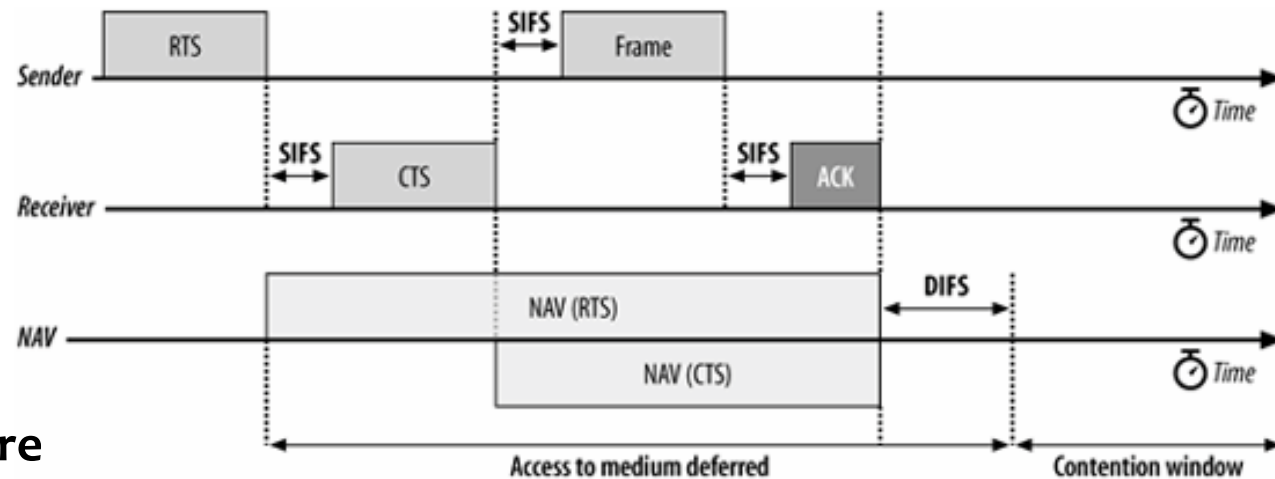


802.11 - MAC

- 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

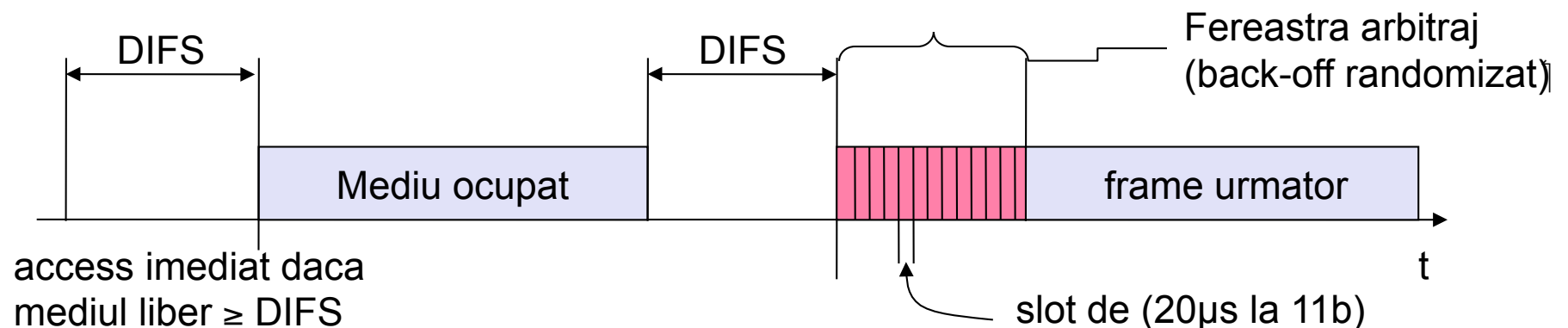
- Fizic – nivel de putere
- Virtual – NAV

NAV (network allocation vector)

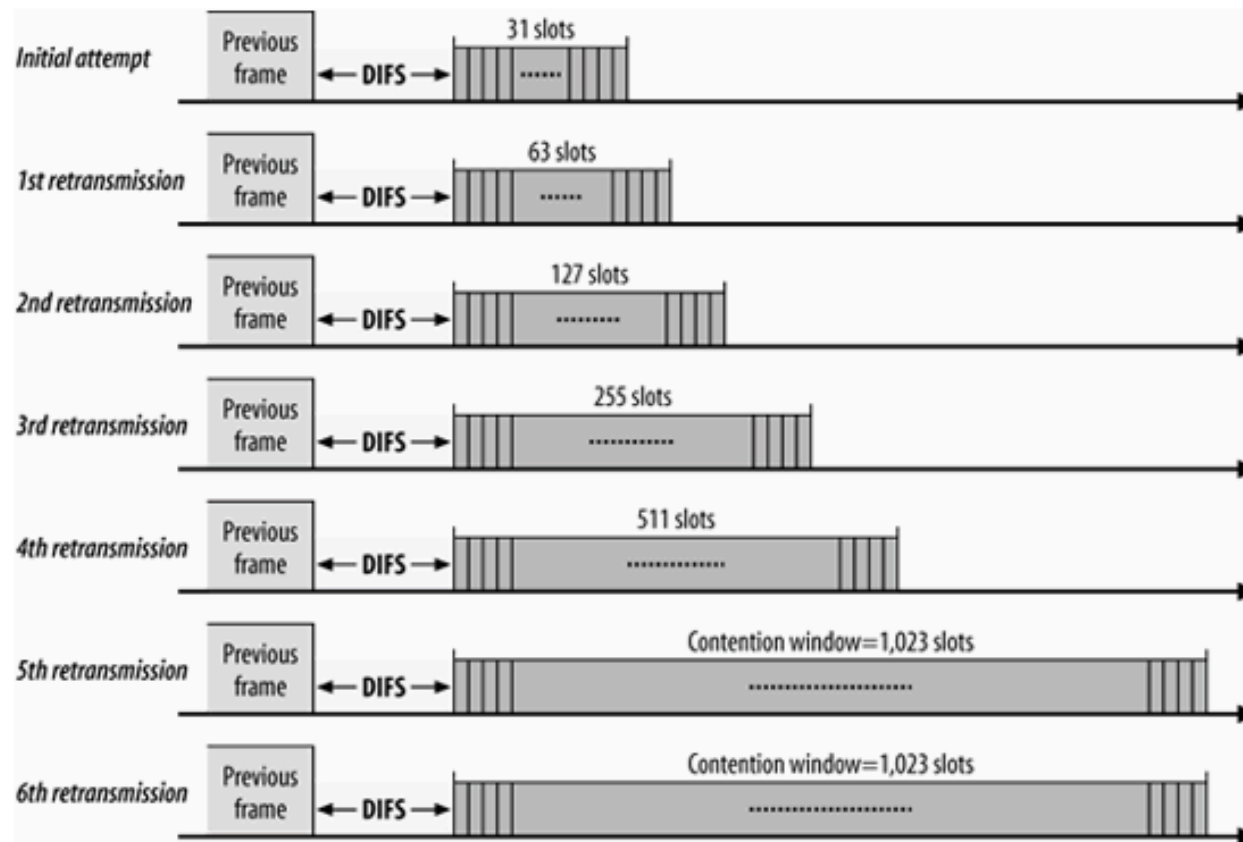
- Un timer care indică durata pentru care mediul este rezervat (ms)
- NAV!=0 => mediul este ocupat
- Majoritatea cadrelor 802.11 conțin un câmp 'durată'
- Se folosește pentru operațiuni atomice (unitare)
 - RTS/CTS/Data/ACK
 - Data/ACK

802.11 - CSMA/CA

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



BEB (binary exponential backoff)



Standard	Slot [μ s]	SIFS [μ s]	DIFS [μ s]	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?

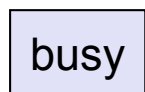
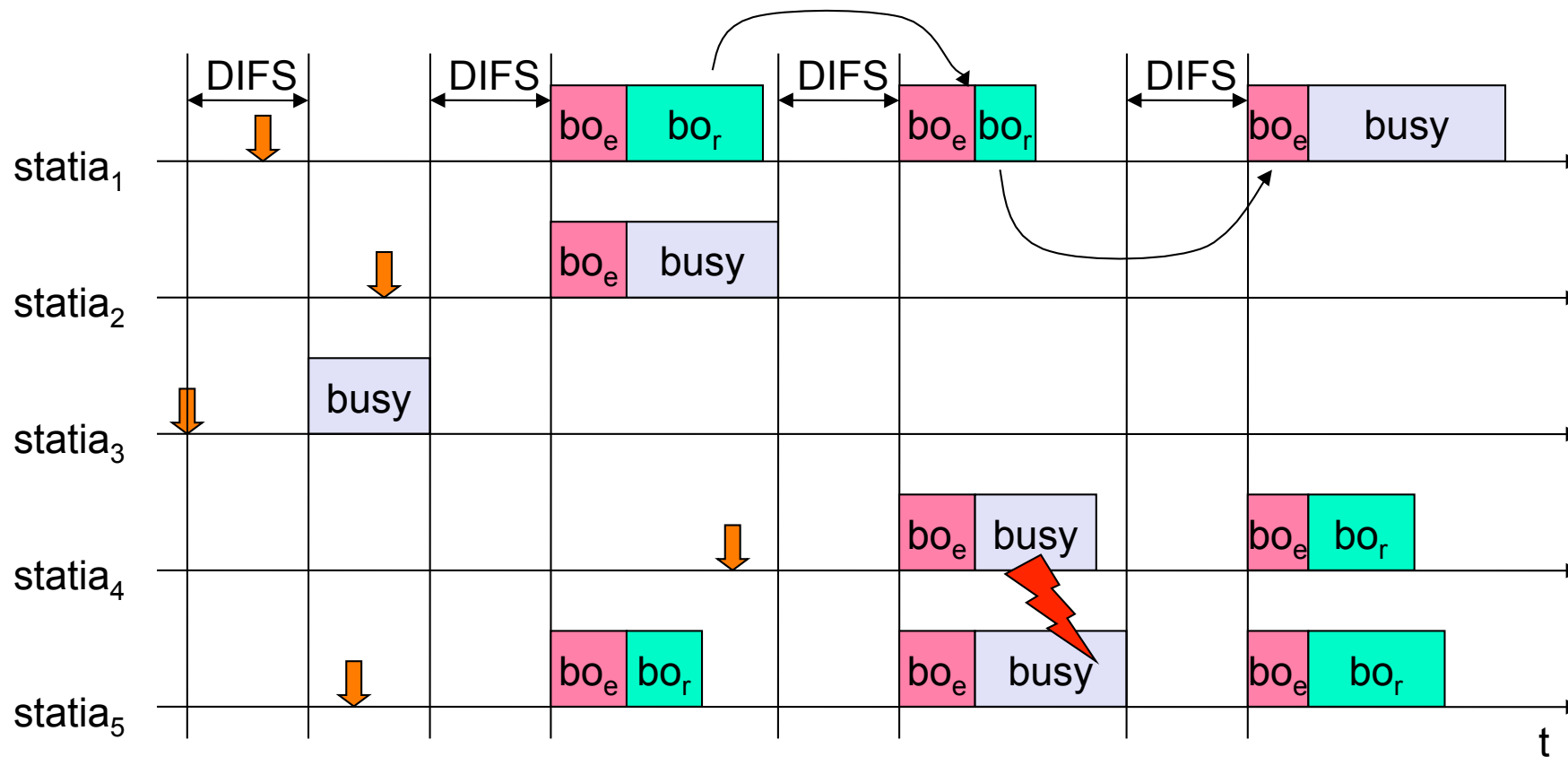
802.11 unicast la distanță mare

- » 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 $[14 * 8 / \text{bitrate in Mbps}] + \text{Air Propagation Time (max)}$
- » 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



Mediu ocupat (frame, ack etc.)



backoff expirat

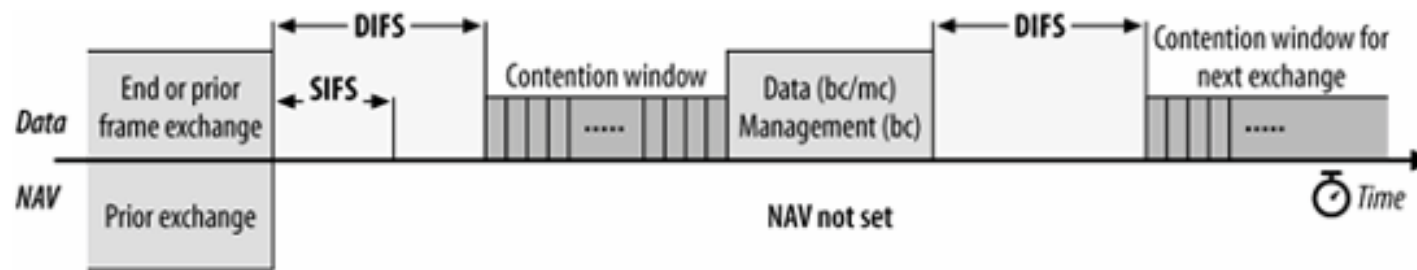


Un pachet devine disponibil



backoff rămas

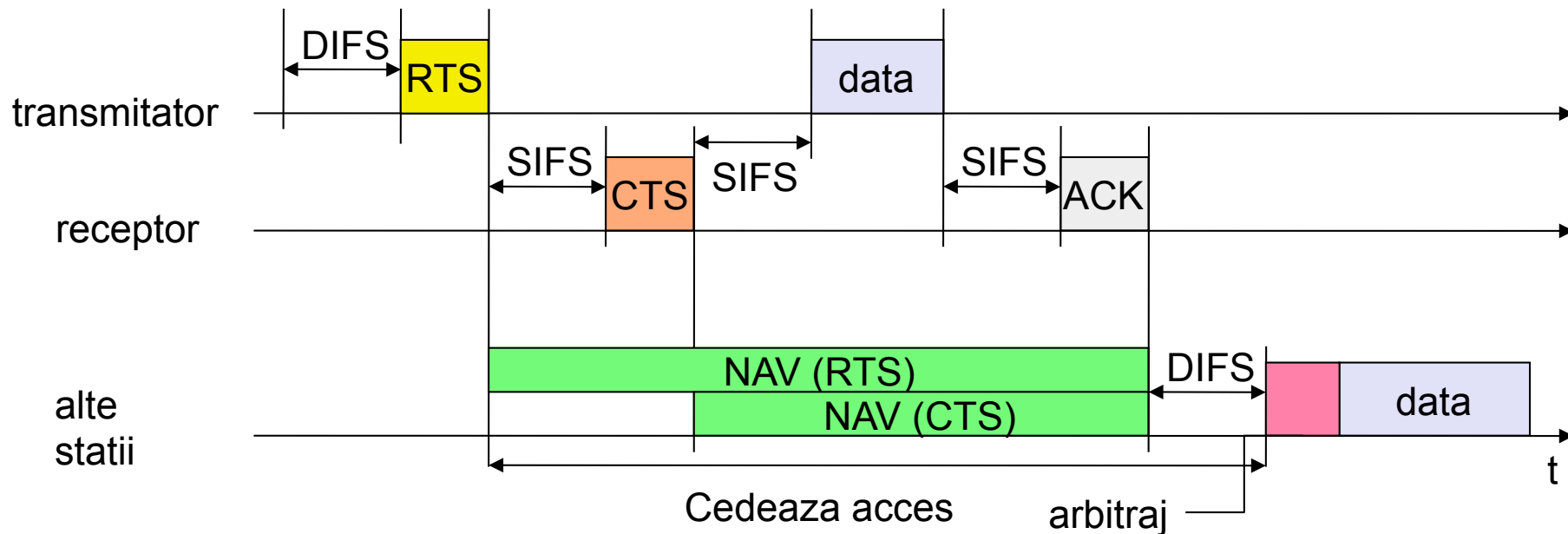
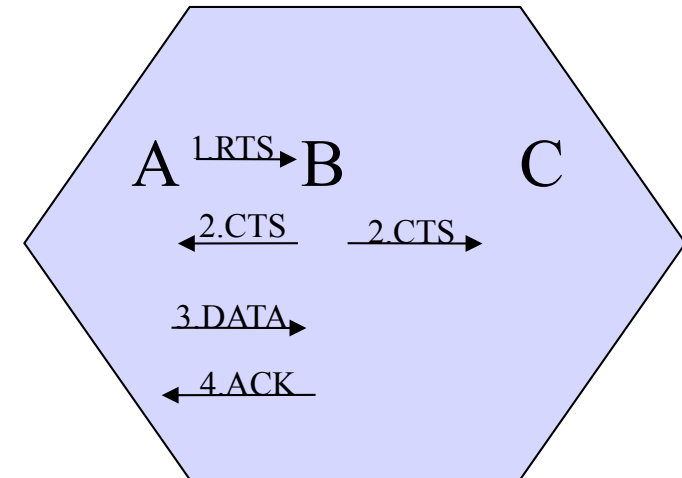
802.11 date broadcast



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

802.11 - RTS/CTS

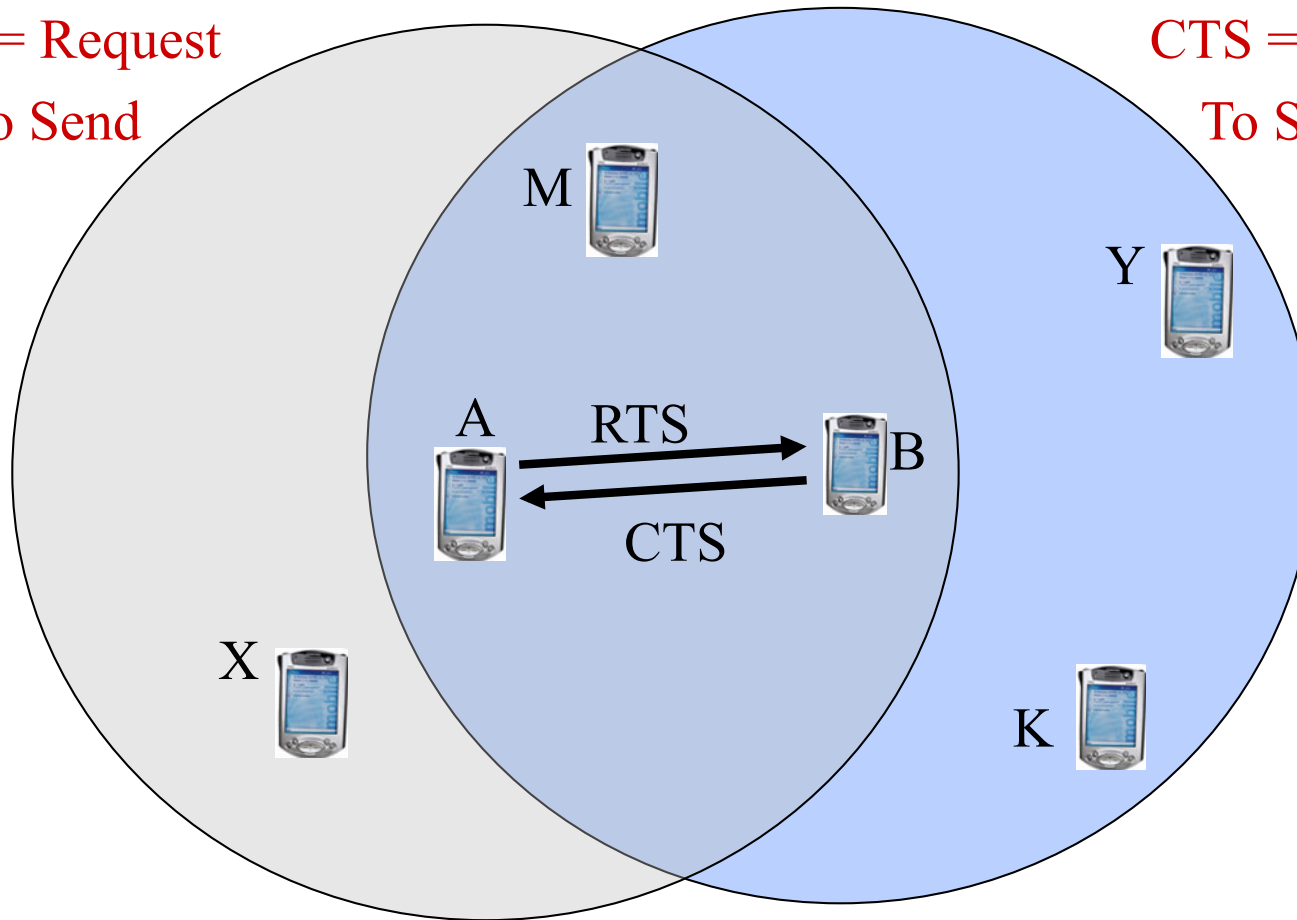
- pentru pachete unicast
 - » Transmitator: RTS cu rezervare (rezerva timpul necesar)
 - » Receptor: CTS
 - » Transmitator: frame
 - » Receptor: ACK
 - » Celelalte statii mentin NAV
 - » RTS threshold



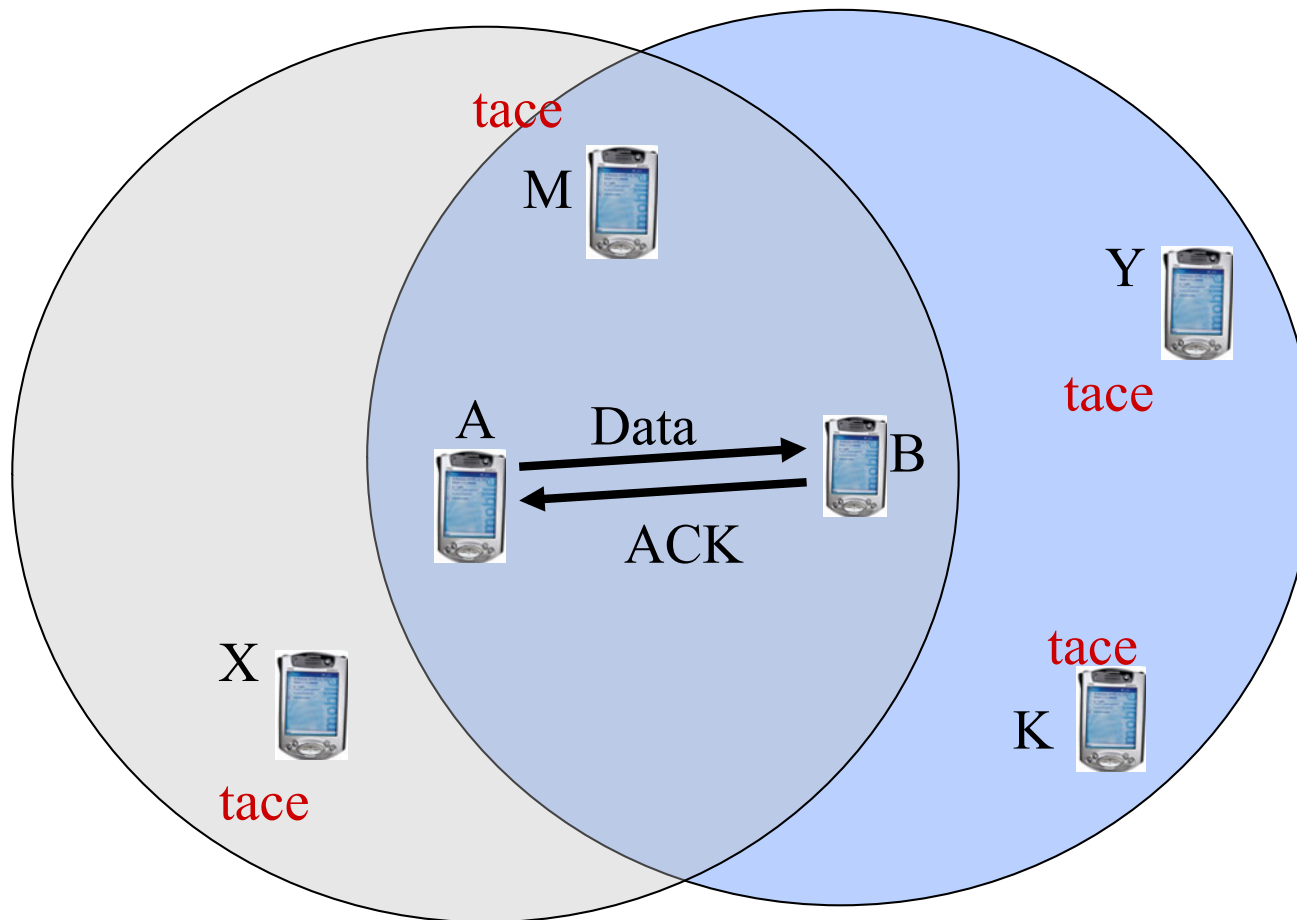
802.11 RTS/CTS

RTS = Request
To Send

CTS = Clear
To Send



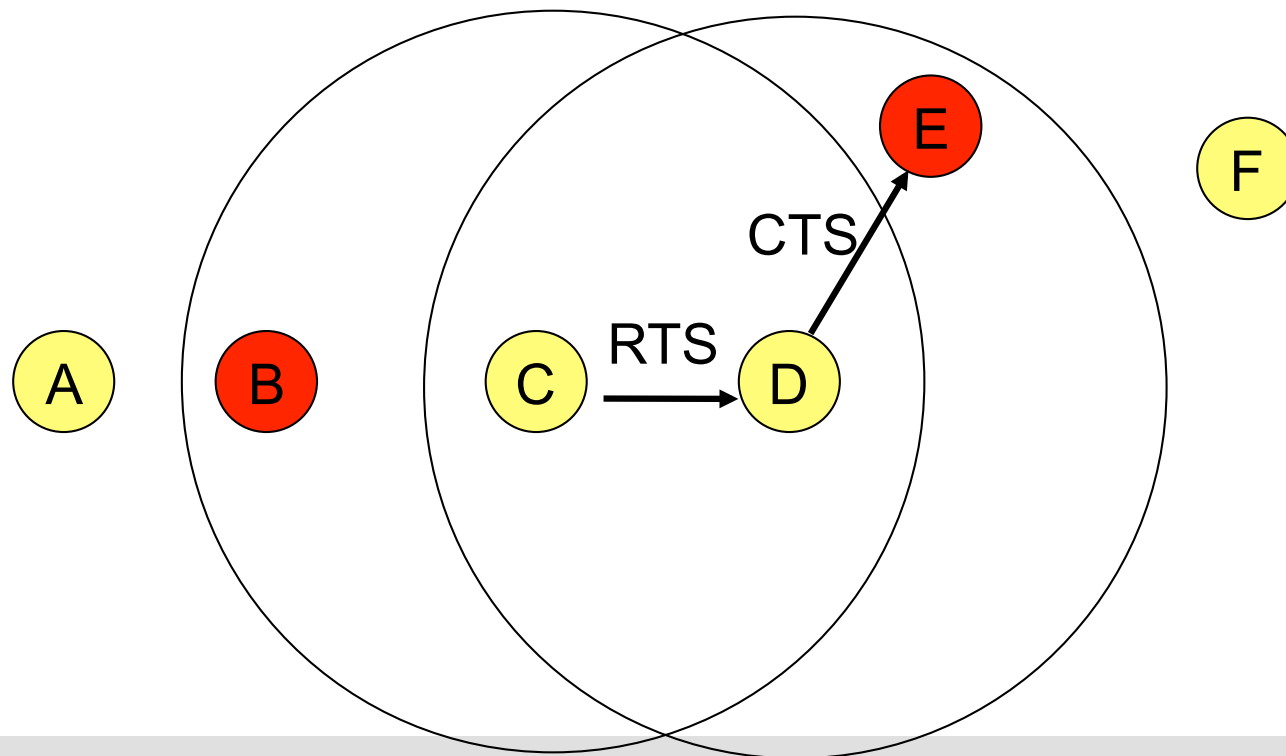
802.11 RTS/CTS



Terminal ascuns cu RTS/CTS

Rezolva problema terminalelor ascunse?

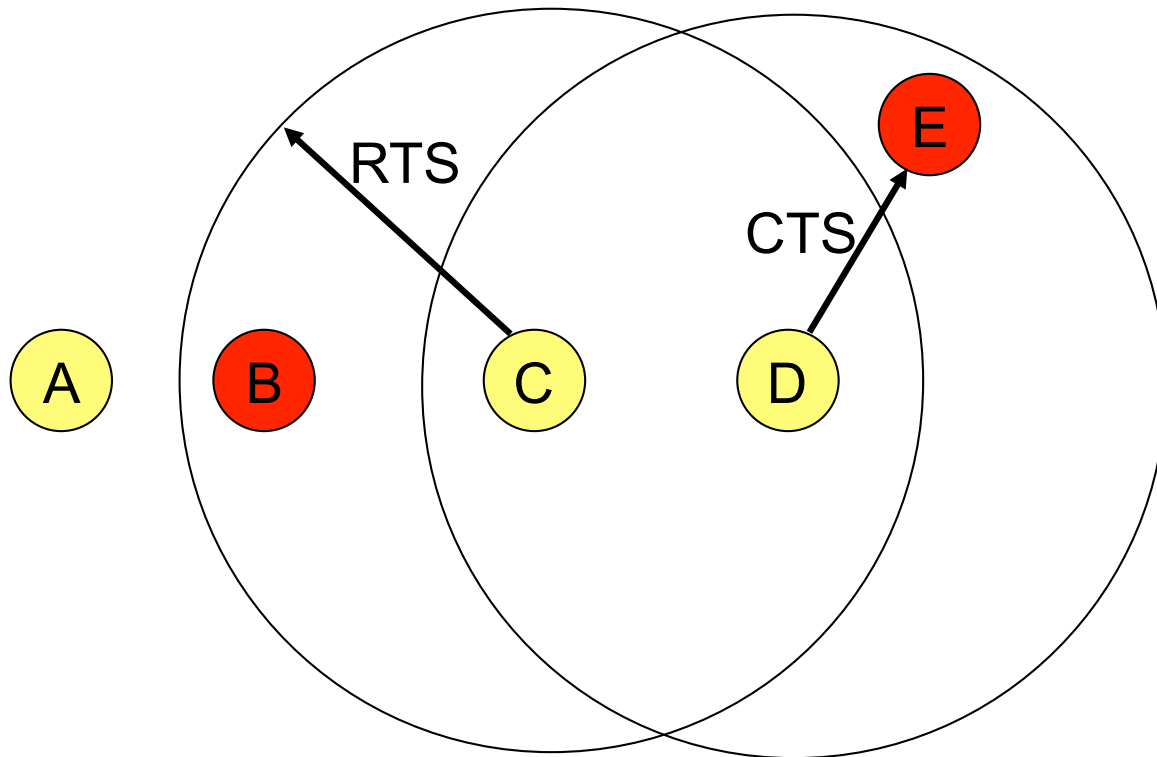
Exemplu zona CS = zona de comunicare



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

Terminal expus cu RTS/CTS

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



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 re folosirea 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

$$\text{EIFS} = \text{SIFS} + \text{DIFS} + (\text{ACK} + \text{Preamble} + \text{PLCP})/\text{BitRate}$$

$$1\text{Mbps}, \text{EIFS}=364\mu\text{s}$$

$$2\text{Mbps} \Rightarrow \text{EIFS} = 212\mu\text{s}$$

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.

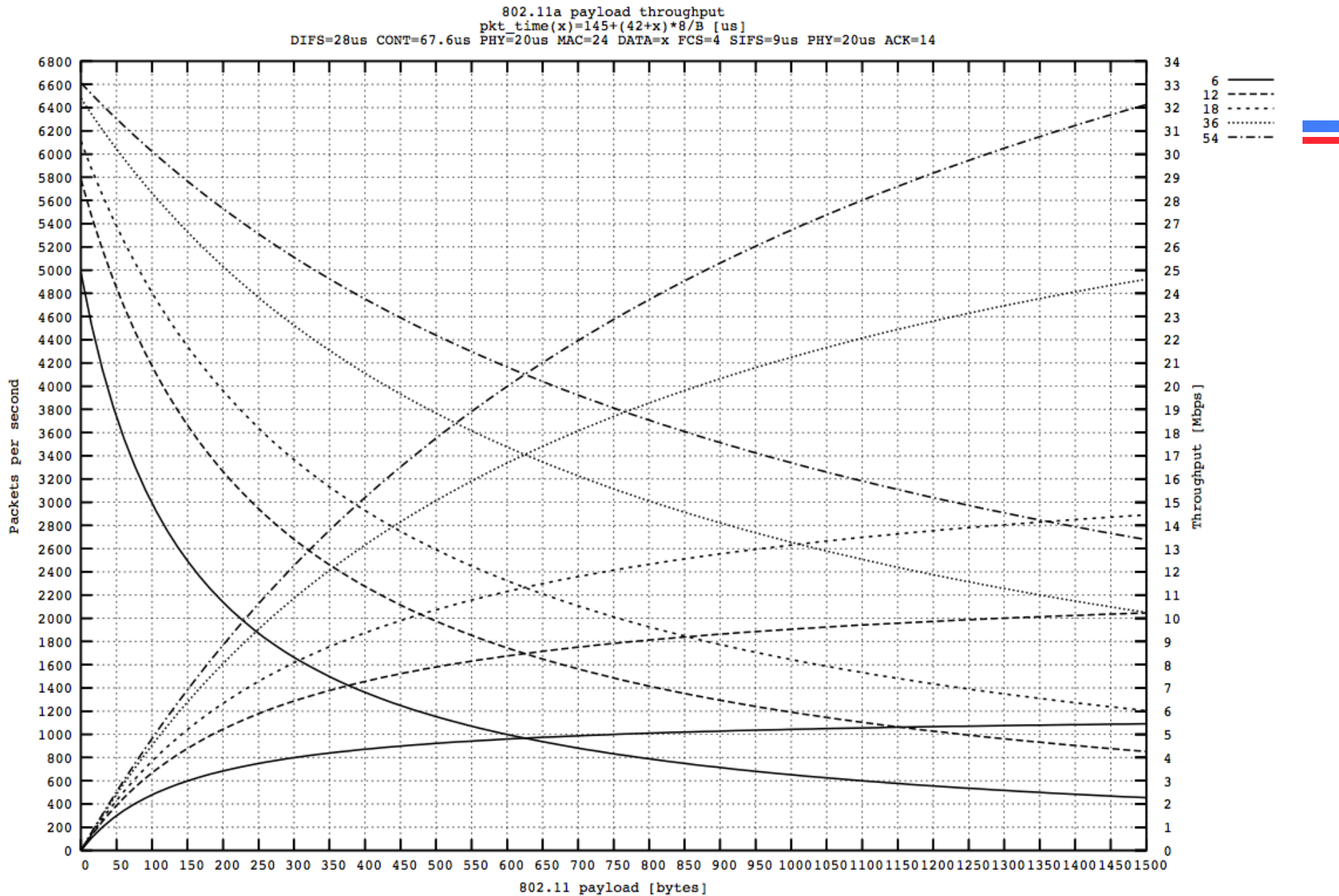
Parametri specifici 802.11a

Table 13-5. OFDM PHY parameters

Parameter	Value	Notes
Maximum MAC frame length	4,095 bytes	
Slot time	9 μ s	
SIFS time	16 μ s	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 μ s	
PLCP header duration	4 μ s	
Receiver sensitivity	-65 to -82 dBm	Depends on speed of data transmission.

Analiză capacitate 802.11a

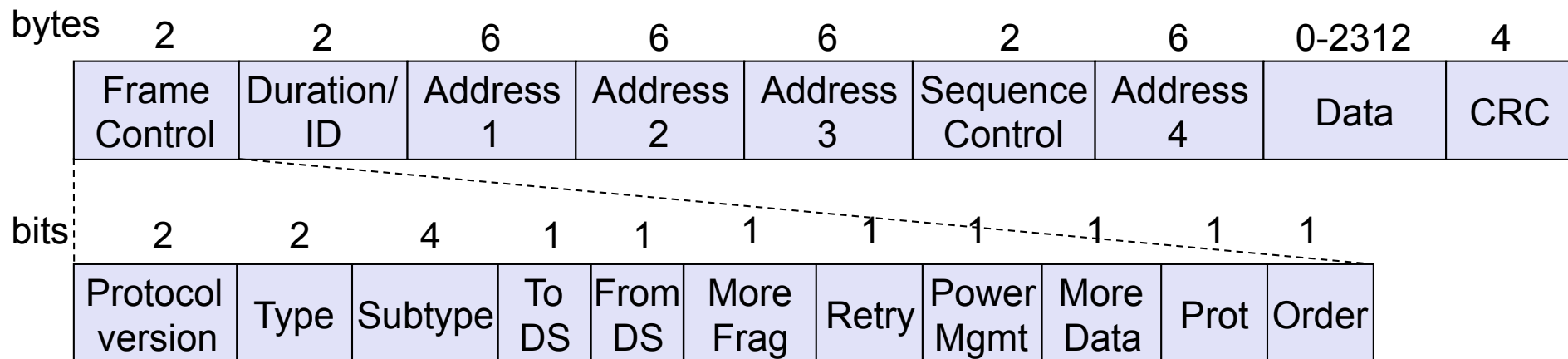
- http://www.oreillynet.com/pub/a/wireless/2003/08/08/wireless_throughput.html?page=2
- DIFS $28\mu\text{s}$
- Conflict $72\mu\text{s}$
- Preambul $24\mu\text{s}$
- Date x octeți
- SIFS $9\mu\text{s}$



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)

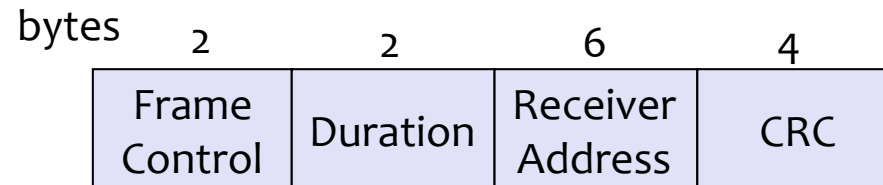
0000	Data
0001	Data+CF-Ack
0010	Data+CF-Poll

Interpretarea biților ToDS și FromDS

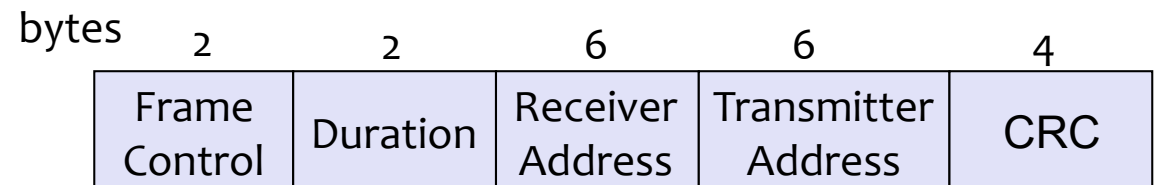
	ToDS=0	ToDS=1
FromDS=0	mgmt, control, modul ad hoc	uplink
FromDS=1	downlink	wireless bridge

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

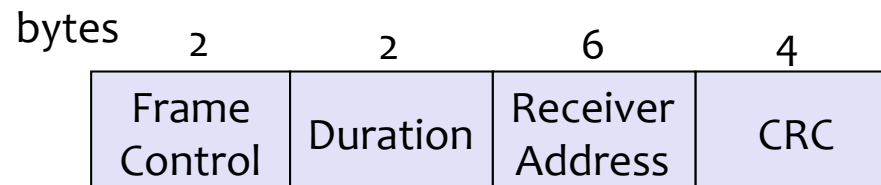
ACK



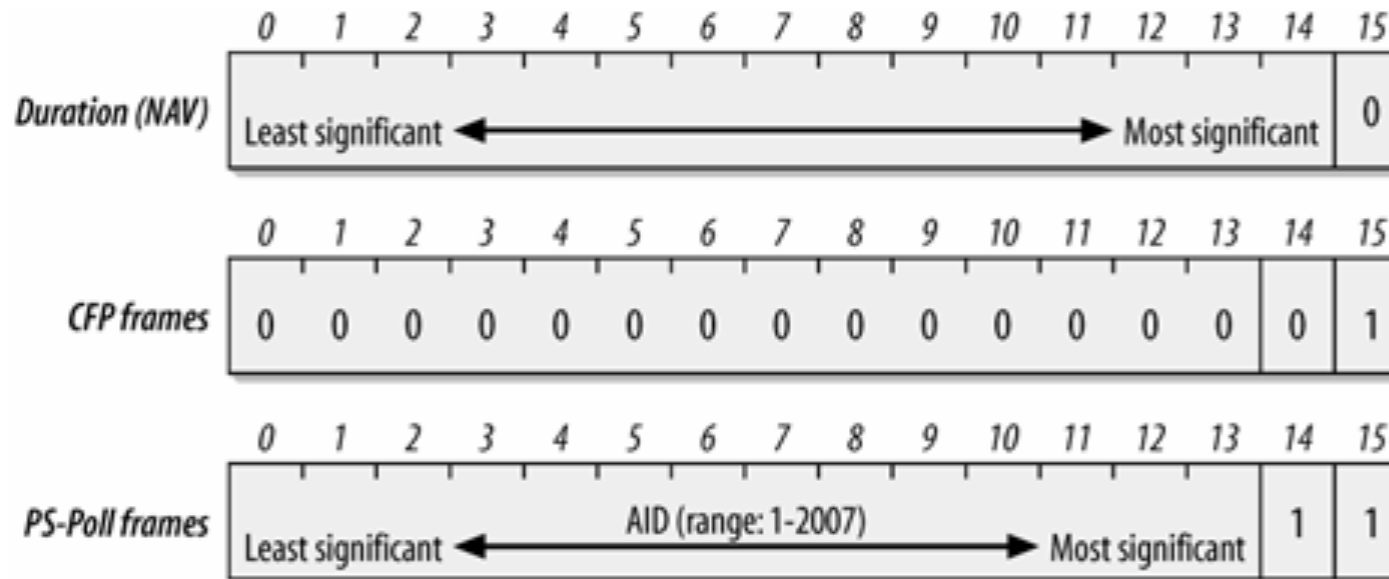
RTS



CTS

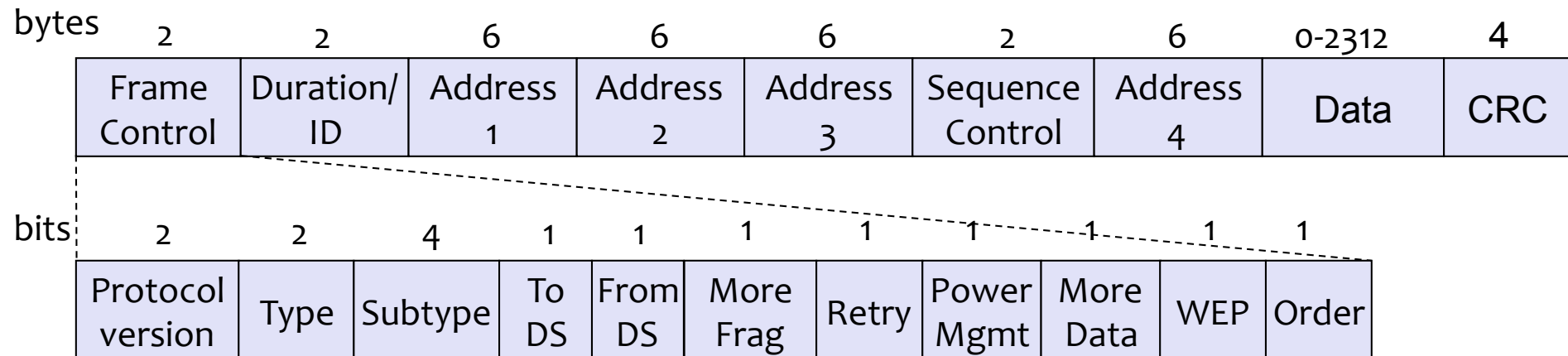


Durata - NAV



- 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

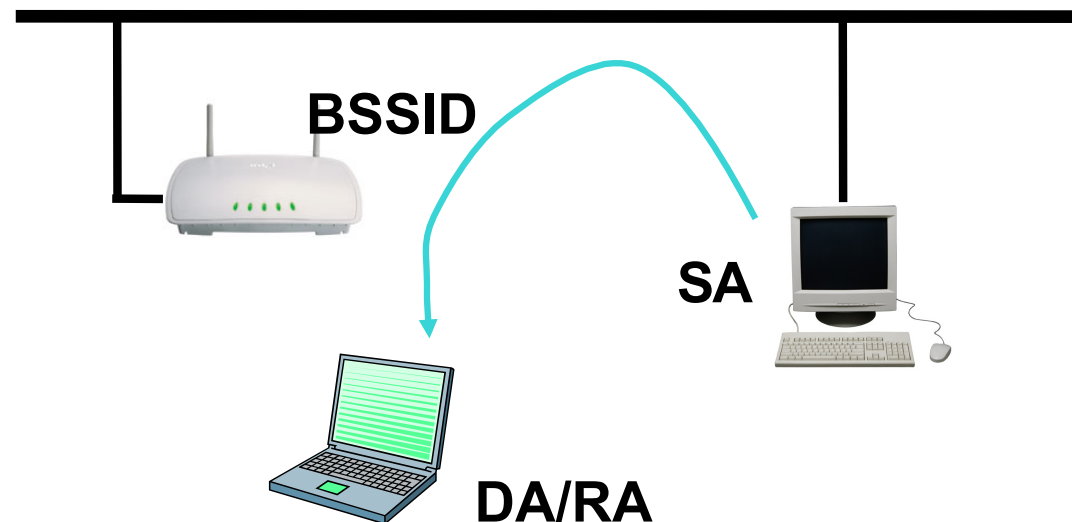
DA: Destination Address

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 (adresa 3) devine destination address
 2. SA (adresa 2) devine source address
 3. Daca exista SNAP header => tip pachet
7. CRC recalculat

emisia cadrelor wired -> wireless

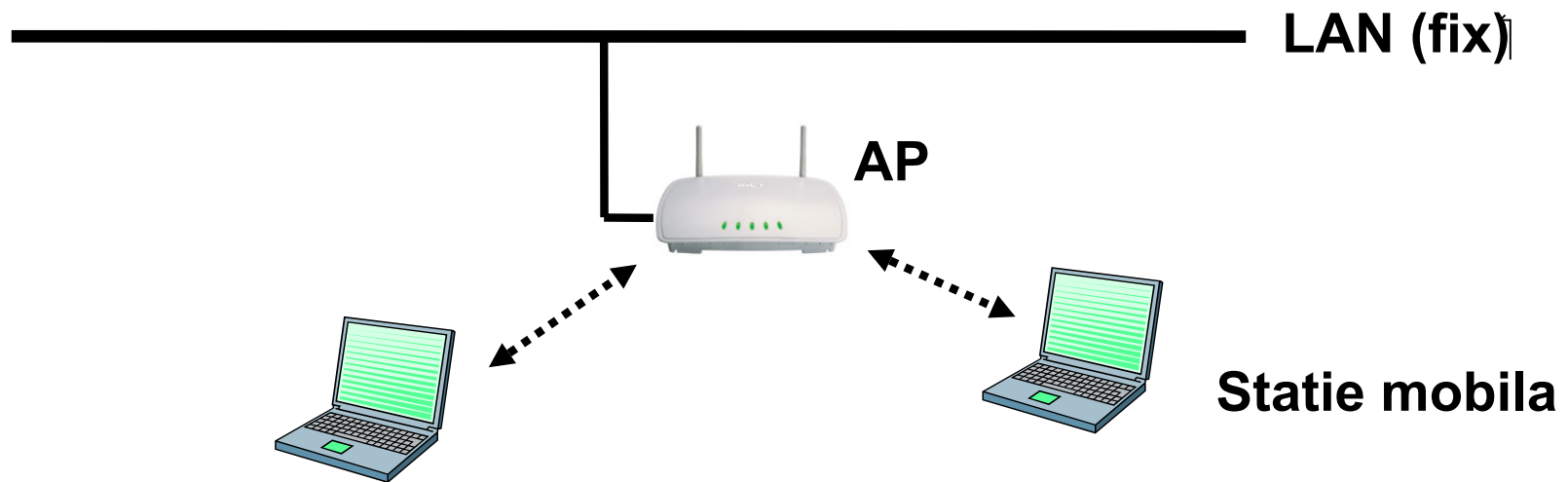
1. Validarea CRC ethernet, verificarea stației destinație, dacă este asociată
2. SNAP header dacă este cazul
3. Planificarea pt transmisie (coadă, PS mode)
4. Asignare număr de secvență, fragmentare
5. Criptare
6. Construcție header
 1. Dest address copiat în Address 1
 2. BSSID copiat în Address 2
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

Alte câmpuri din antet

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

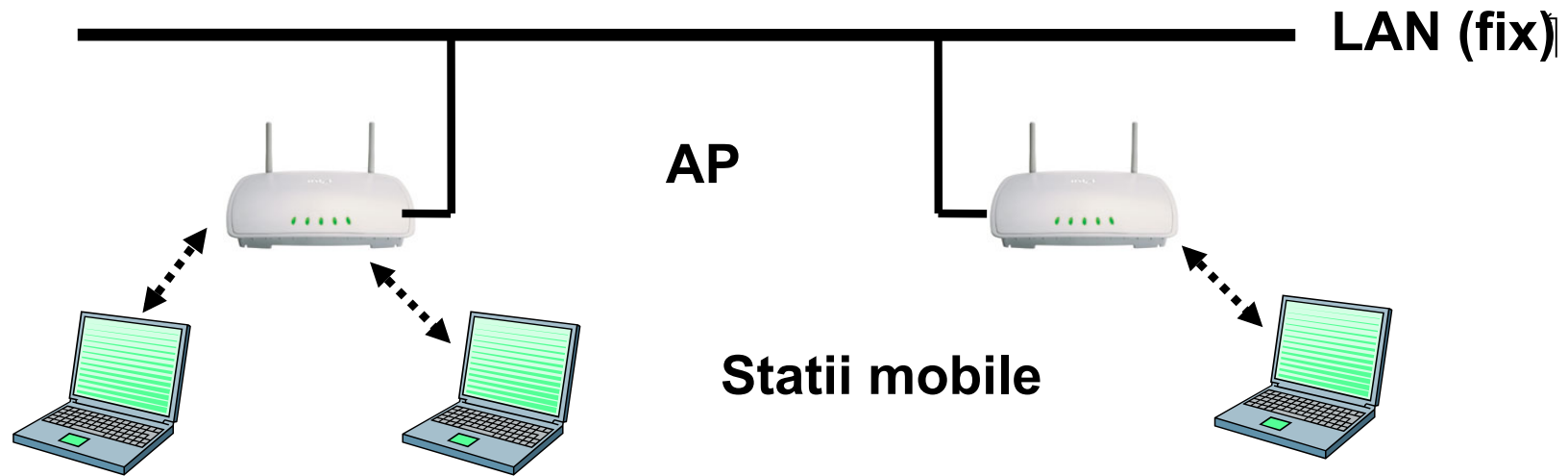
- Număr de secvență
- Date – maximum 2304 octeți
- CRC – antet + date
- Diferențe față de alte antete
 - Nu există “tip” pentru datele la nivel superior
 - Nu este necesară o lungime minimă

Modul infrastructură



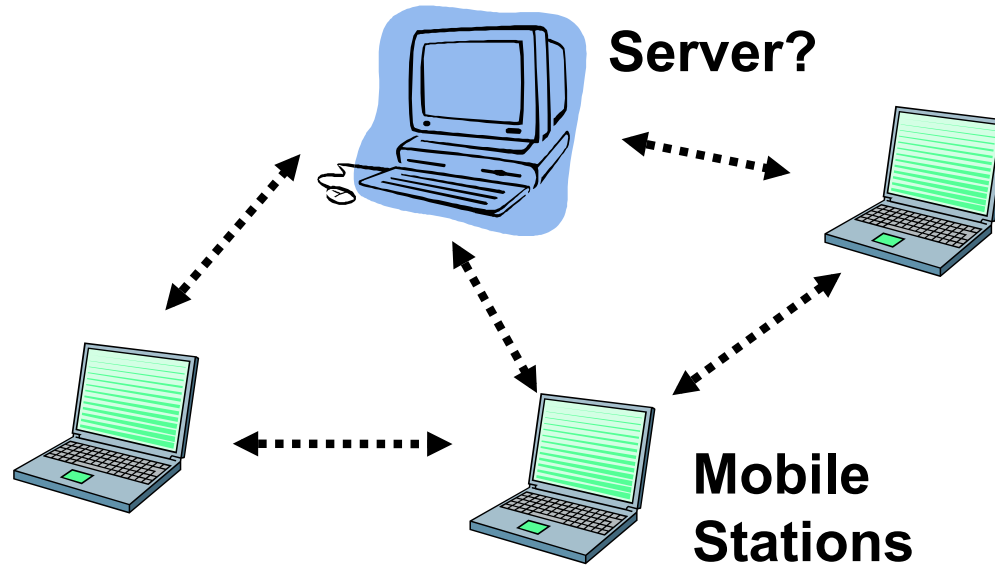
- Basic Service Set (BSS)
- AP functioneaza ca bridge
- Comunicarea intre statii se face numai prin intermediul AP
- distribution system (DS)

Modul infrastructură - extins



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

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 (emitorul si receptorul stationeaza acelasi interval la fiecare frecventa)

Cum se realizează TSF

Toate statiile mențin un ceas local

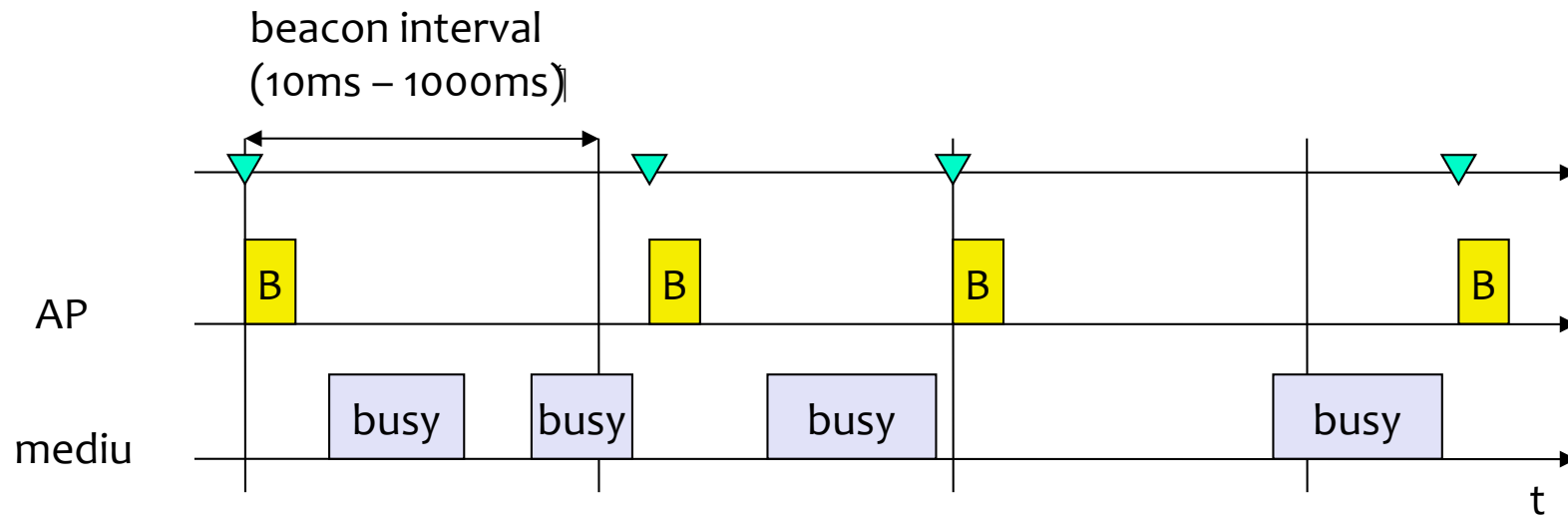
AP difuzează periodic un beacon cu timestamp, informatii de management, roaming

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)



▼ timestamp

B beacon frame

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 același 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

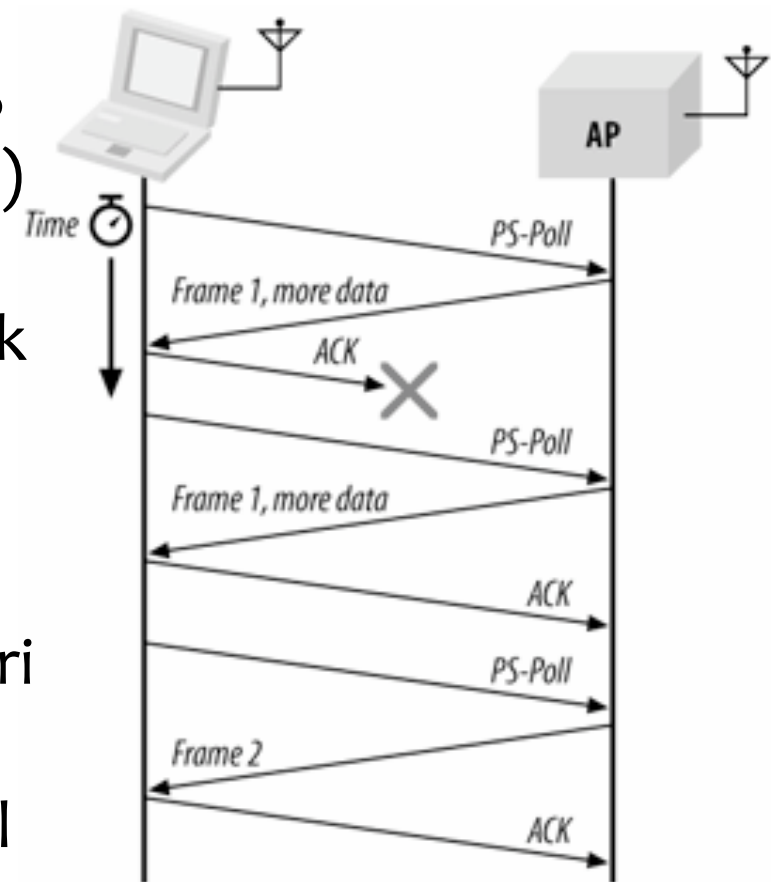
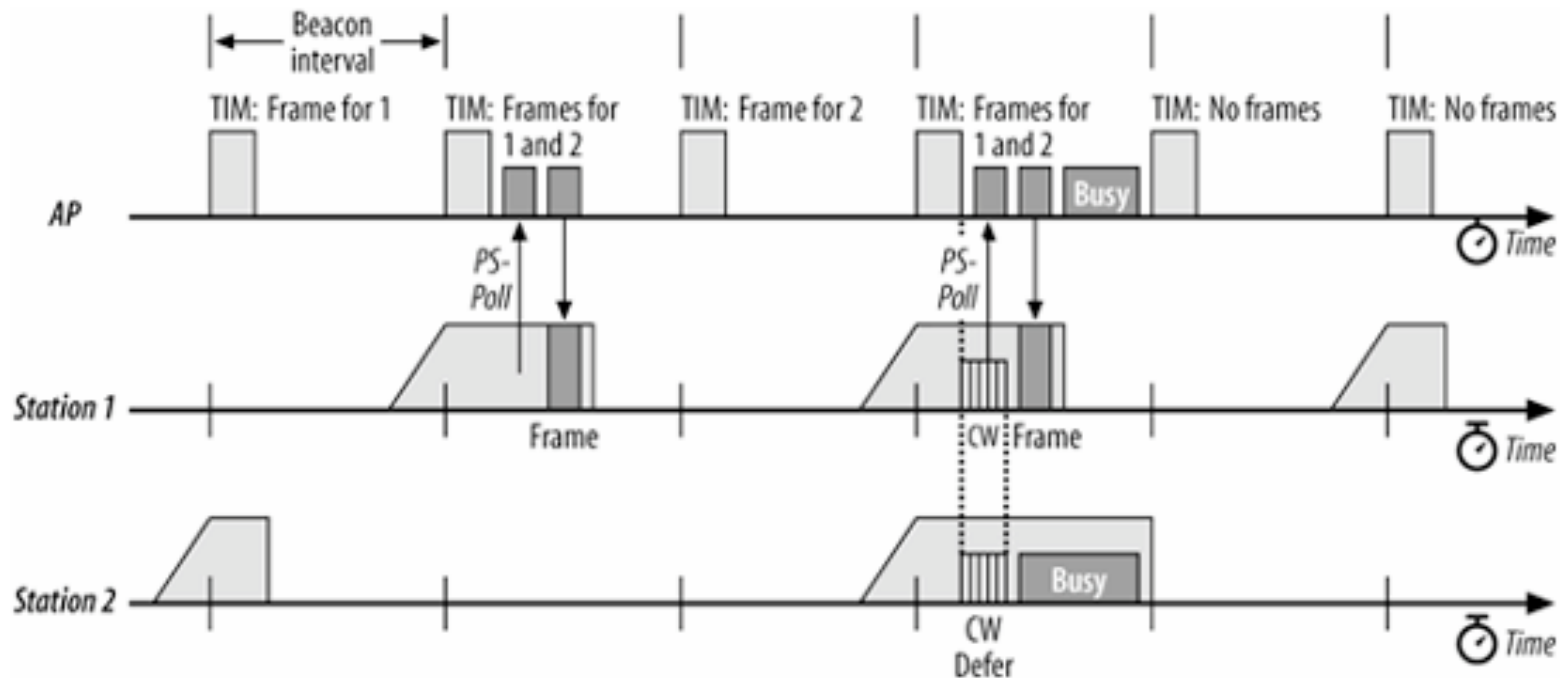
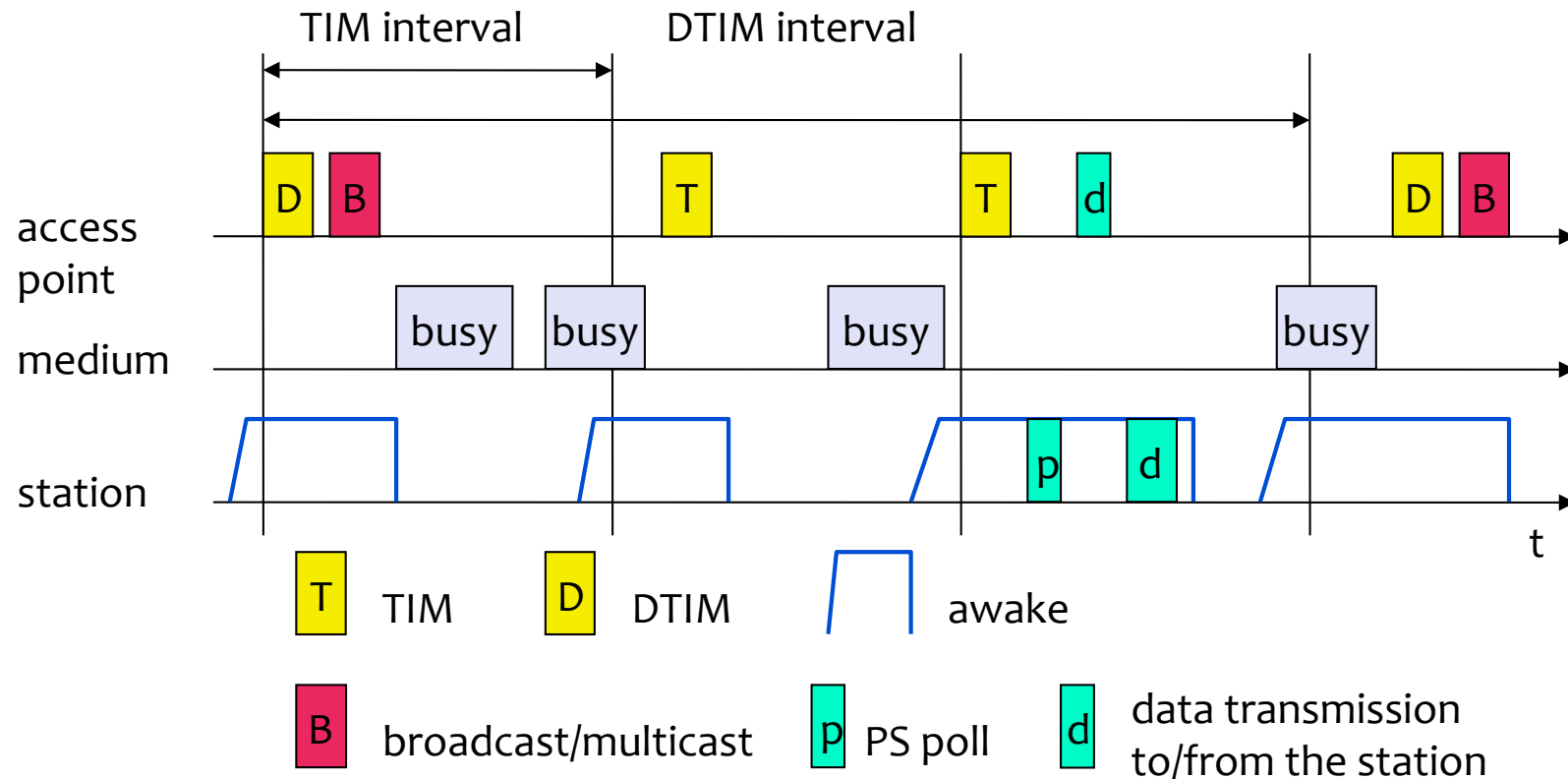


Figure 8-13. Buffered frame retrieval process



- 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

- 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 întâmplă când cade conexiunea?

- Scanare

 - Passive Scanning

 - Reactive Scanning

 - se trimit pachete de proba pentru a găsi cel mai bun AP

- Reasociere – cerere

 - statio 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

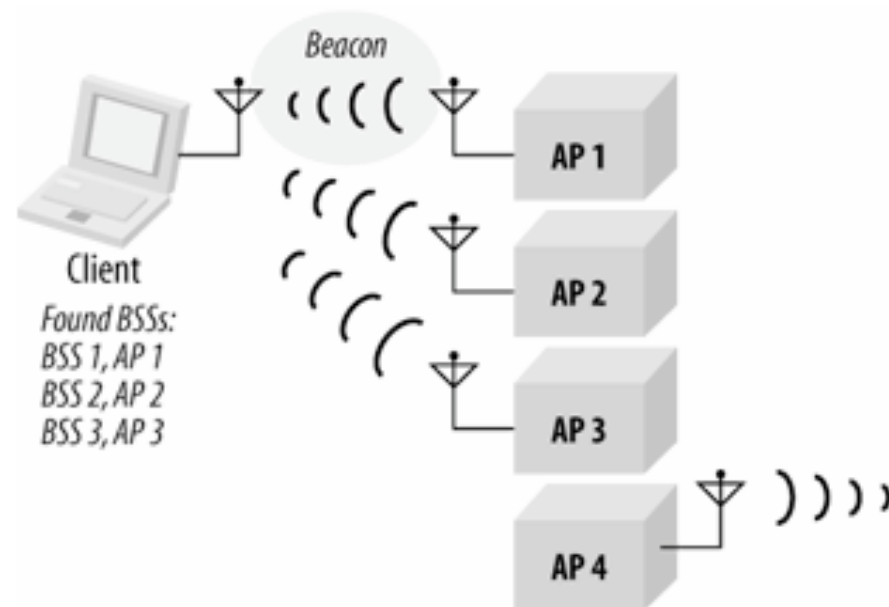
 - e.g. pentru retele vehiculare

Scanare pasivă

Cea mai economică energetic

- doar se ascultă beacon-uri
- se baleiază toate canalele

Figure 8-2. Passive scanning

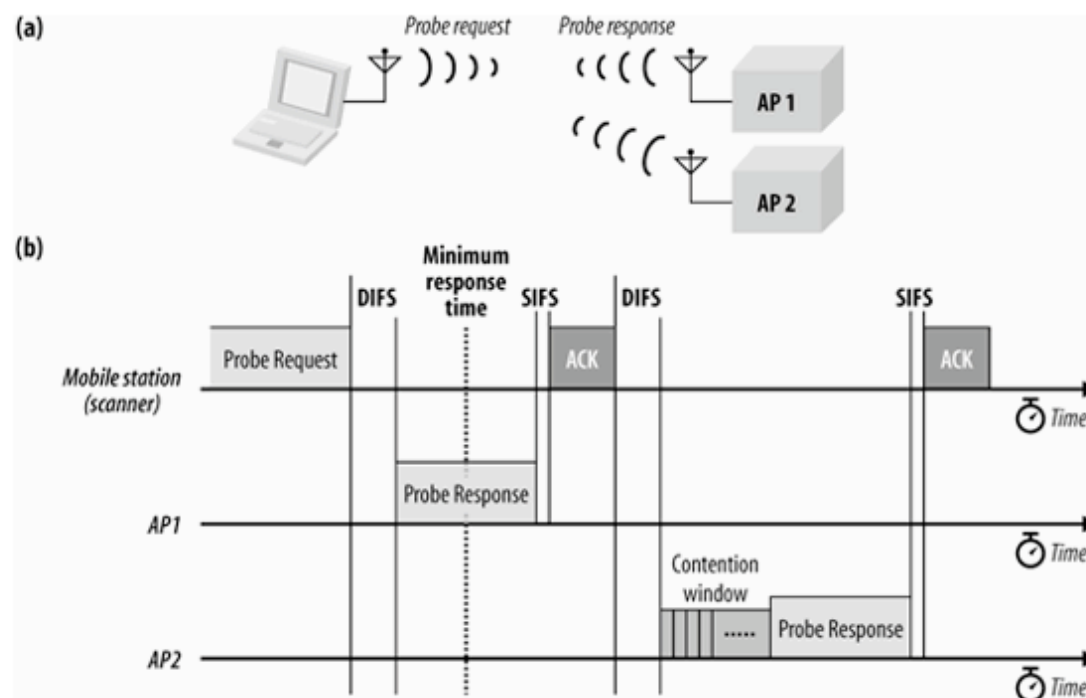


Scanare activă

Pe fiecare canal disponibil:

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

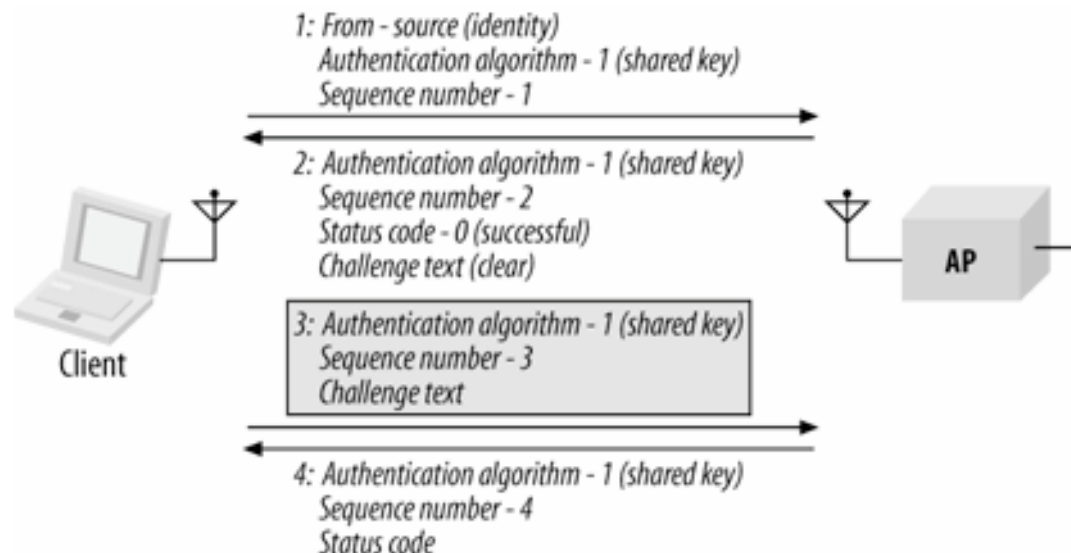
Figure 8-3. Active scanning procedure and medium access



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

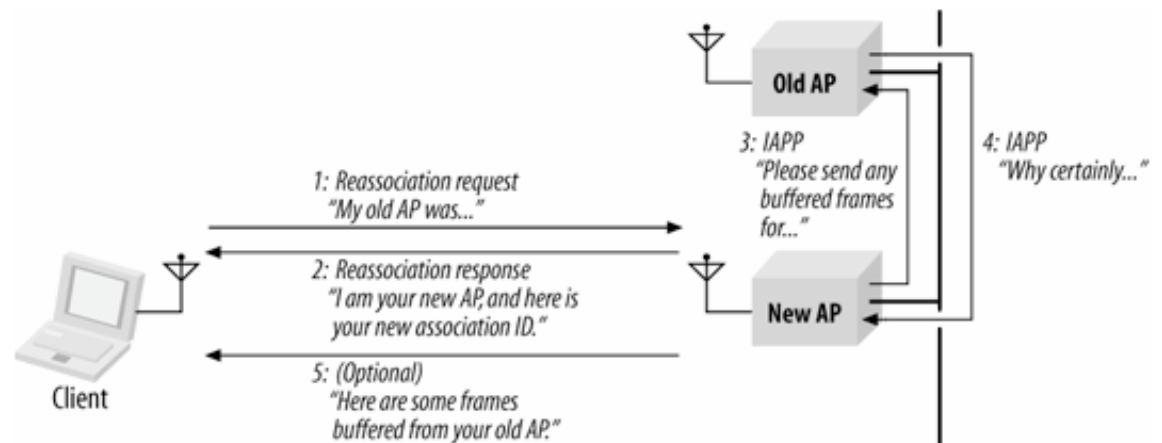
Scopuri:

- 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

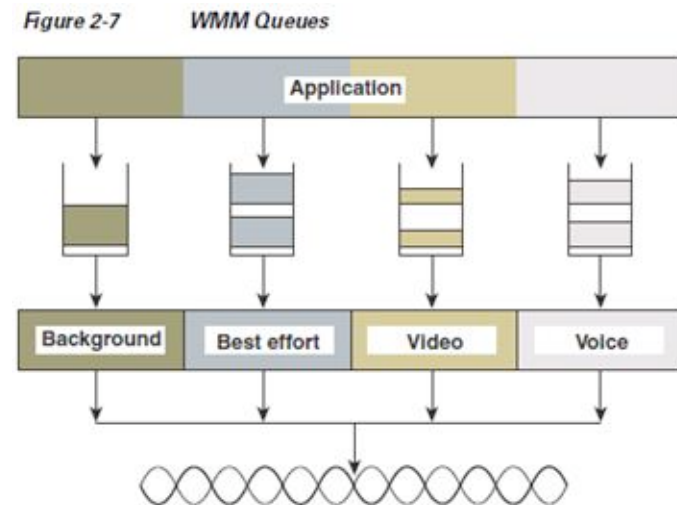
Confidențialitate (privacy)

- 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 parțial QoS)

3. CW specifice - pt 11a/g/n

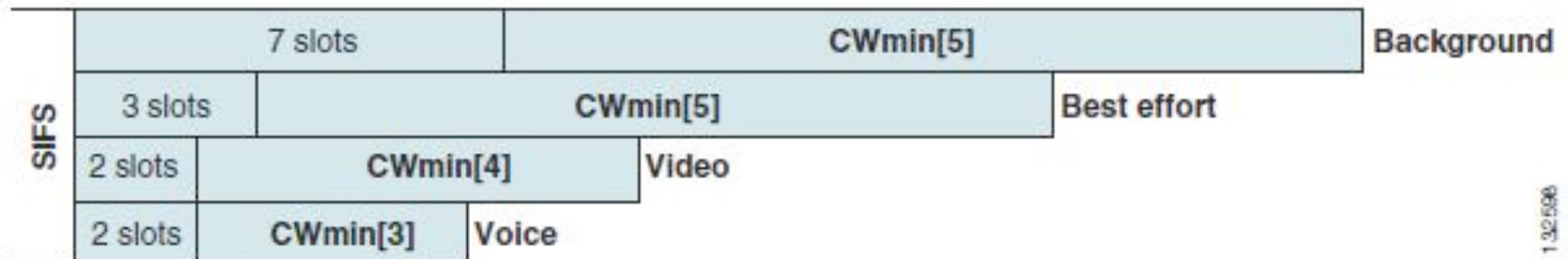
- VO CW = 3..7
- VI CW = 7..15
- BE CW = 15..1023
- BK CW = 15..1023

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



1.32.696

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(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)

802.11ad (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.

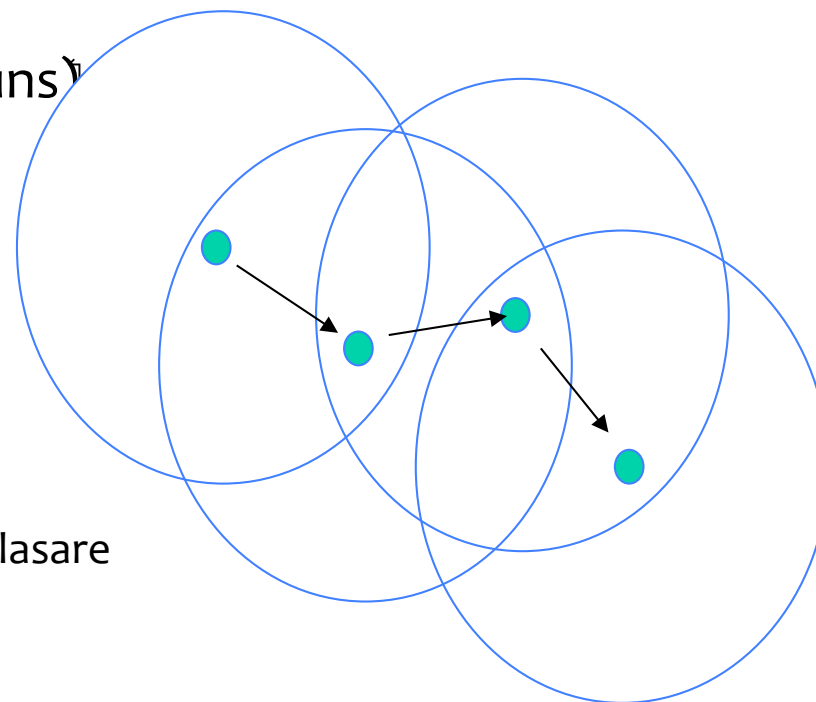
Multihop – aplicații posibile:

- medii neplanificate (adhoc)
 - » instalare rapida, cost redus
 - » retea de vehicule
 - » 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 trafic
- 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
 - Jochen H. Schiller, online lectures
 - wikipedia