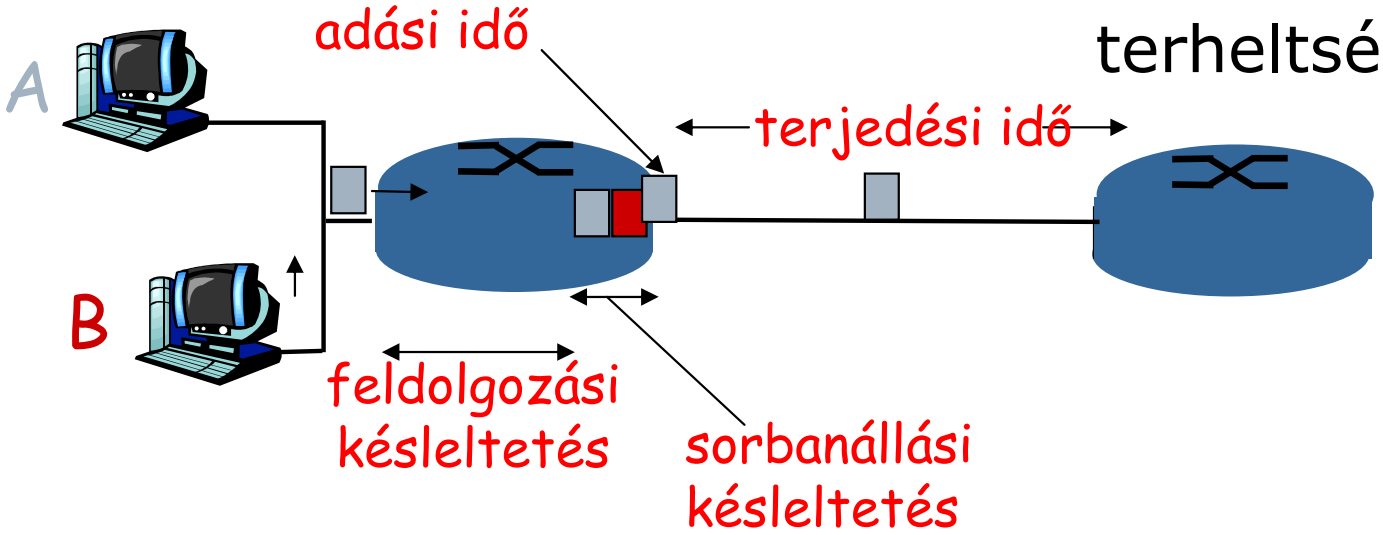
2. gyakorlat

Ismétlés
Számítási példák
Illusztrációk
Demonstrációk

Csomagkésleltetés

A csomagok késésének négy fő oka (1)

- 1. Feldolgozás a csomópontban:
  - hibaellenőrzés
  - a kimenő link meghatározása
- 2. Sorbanállás
  - várakozás továbbításra az adott kimenő linken
  - a router terheltségétől függ



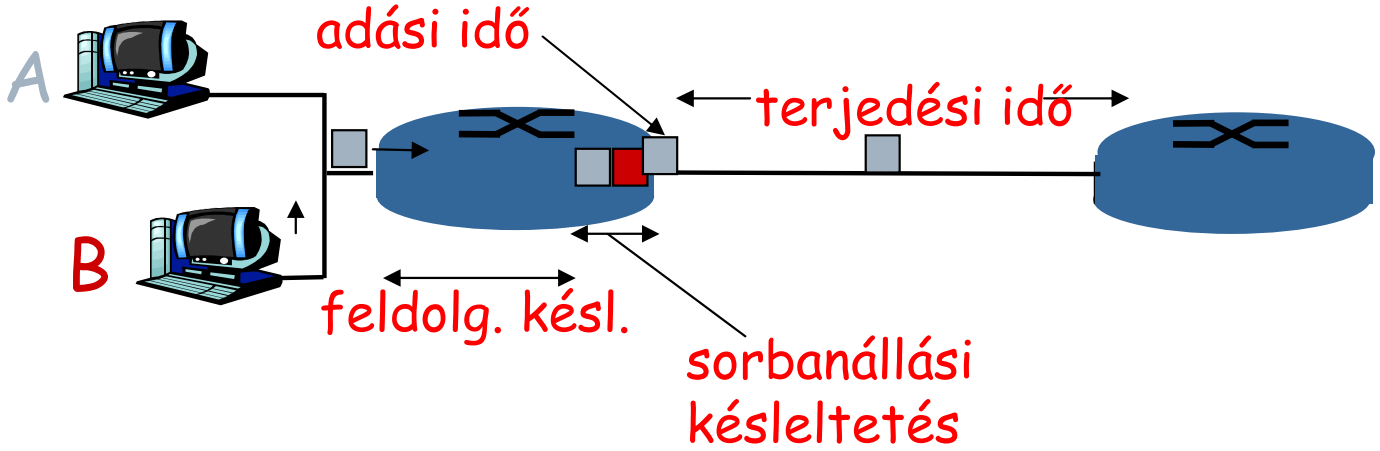
A csomagok késésének négy fő oka (2)

3. Adási idő:

- R= a link adatátviteli sebessége (bit/s)
- L=csomaghossz (bit)
- az adási idő = L/R

4. Terjedési idő:

- d = a link fizikai hossza
- s = terjedési sebesség az átviteli közegben (~$2x10^8$ m/sec)
- terjedési idő = d/s



Csomóponti késleltetés, összefoglalva:

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

- d_{proc} = feldolgozási (processzálási) idő
  - tipikusan pár mikroszekundum
- d_{queue} = sorbanállási idő/késleltetés
  - a forgalomtól függ
- d_{trans} = adási idő
  - = L/R, kissebességű linkeken jelentős lehet
- d_{prop} = terjedési idő
  - pár mikroszekundumtól mp-ig

Számoljunk!

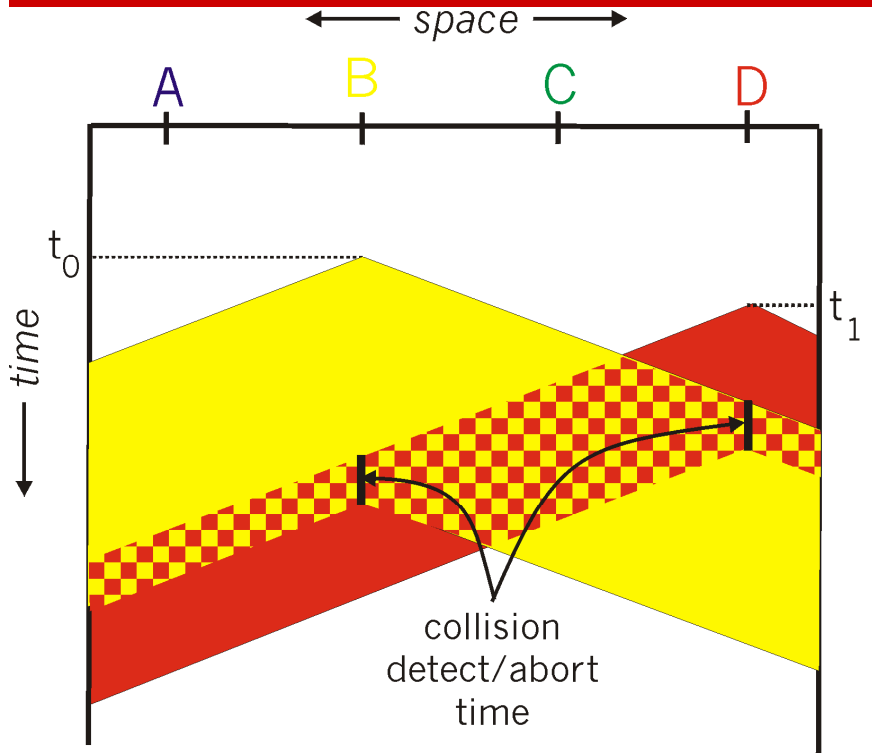
- ADSL link
  - Feltöltés: 8 Mbit/s
  - Letöltés: 512 kbit/s
  - Távolság: 200 m
- Mennyi idő múlva kapunk nyugtát, ha
  - Csomagunk 1000 bájt
  - Nyugta 64 bájt
  - Terjedési sebesség $2 \cdot 10^8$ m/s

Ethernet ütközési tartomány

Résidő

Szegmensméret

Min. csomaghossz, „résidő”: az ütközések biztos érzékeléséhez



- Grafikus ábrázolás: az ütközési területnek folytonosnak kell lennie a busz mentén

- Legkedvezőtlenebb esetben is (két állomás a busz két végén) minden állomás érzékelje az ütközést:

$$T = \frac{2L}{C}$$

- L: szegmens (busz) hossza
- C: jelterjedési sebesség
- T: „résidő”

- L = 500 m; C= $2 \cdot 10^8$ m/s ⇨ kb. T = 51,2 µs

- Ha 10 Mbit/s, akkor 51,2 µs ⇨ 512 bit = 64 bájt

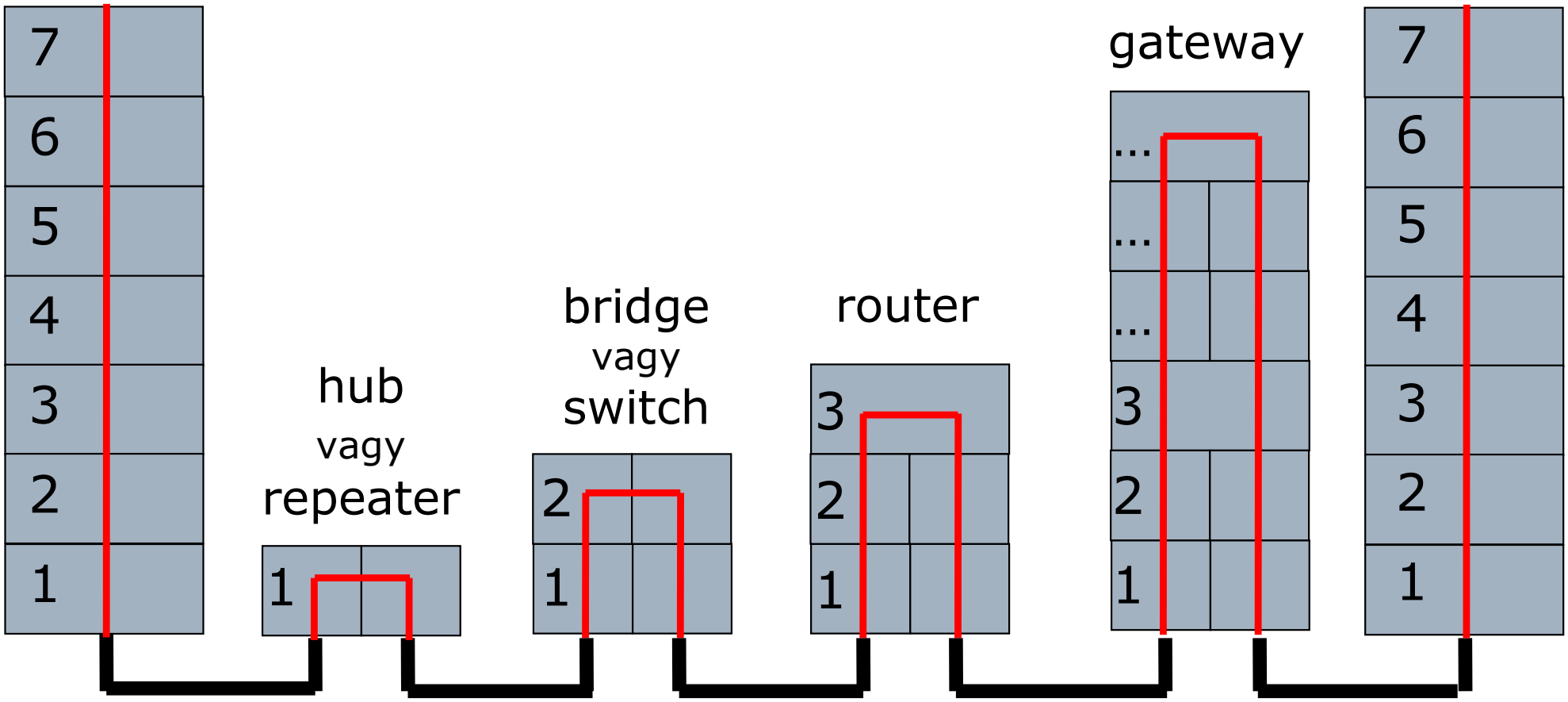
Példa – Ethernet ütközési tartomány

- Hány bájt legyen a minimális kerethossz egy hálózaton, ahol
  - maximális szegmensméret: 100 m;
  - adatsebesség: 100 Mbit/s;
  - fizikai közeg: rézvezető?

Példa – Ethernet összekötés

- Maximum hány szegmenst lehet elvileg összekötni 100BaseT esetén, ha az összekapcsoláshoz használt eszköz:
  - repeater;
  - hub;
  - switch;
  - bridge;
  - router?

Különböző képességű átjátszók



Átjátszó eszközök megnevezése

Angol név	Magyar név	OSI réteg	A portok száma tipikusan	Funkcionalitás
repeater	jelismétlő	L1	2	jelerősítés, -továbbítás
hub	hub (többportos jelismétlő)	L1	4-16	jelerősítés, -továbbítás minden porton; több eszköz összekapcsolása
bridge	híd	L2	2-8	nem ütköző szegmensek összeköttetése; továbbítás csak a szükséges porton; átviteli közegek közötti konverzió újrakeretezéssel
switch	switch (kapcsoló)	L2	4-48	nem ütköző szegmensek összeköttetése; továbbítás csak a szükséges porton, azonos közegen, újrakeretezés nélkül
router	útválasztó	L3	2-10	útválasztás L3 címek alapján
gateway	átjáró	>L3	2-4	protokollkonverzió, -együttműködés

Nagysebességű Ethernet szabványok

- Fast Ethernet (IEEE 802.3u)
- Gigabit Ethernet (IEEE 802.3z)
- 10Gb Ethernet (IEEE 802.3ah)

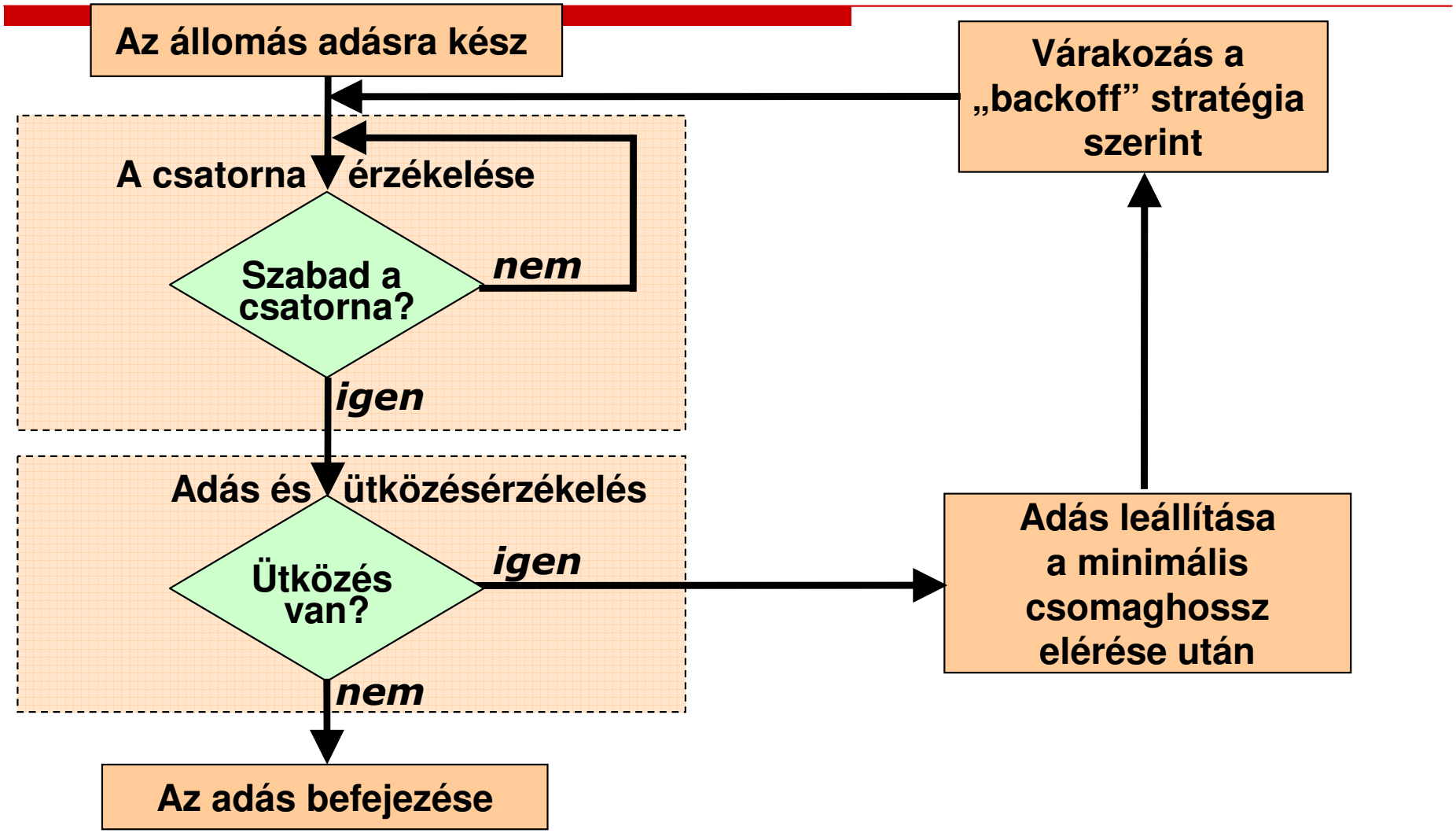
Jellemzők	**10/100 Mbit/s**	**1 Gbit/s**	**10 Gbit/s**
Fizikai közeg	**UTP** **fényv.**	**koax** **UTP** **fényv.**	**fényv.** **(rézv.)**
Résidő (slot time) [byte]	64	512	**NINCS CSMA/CD MAC PROTOKOLL**
Küldési próbálkozás	16		
Visszalépési algoritmus korlátja	10		
Minimális keretméret [byte]	64		
Maximális keretméret [byte]	1518		

Ethernet – CSMA/CD működése

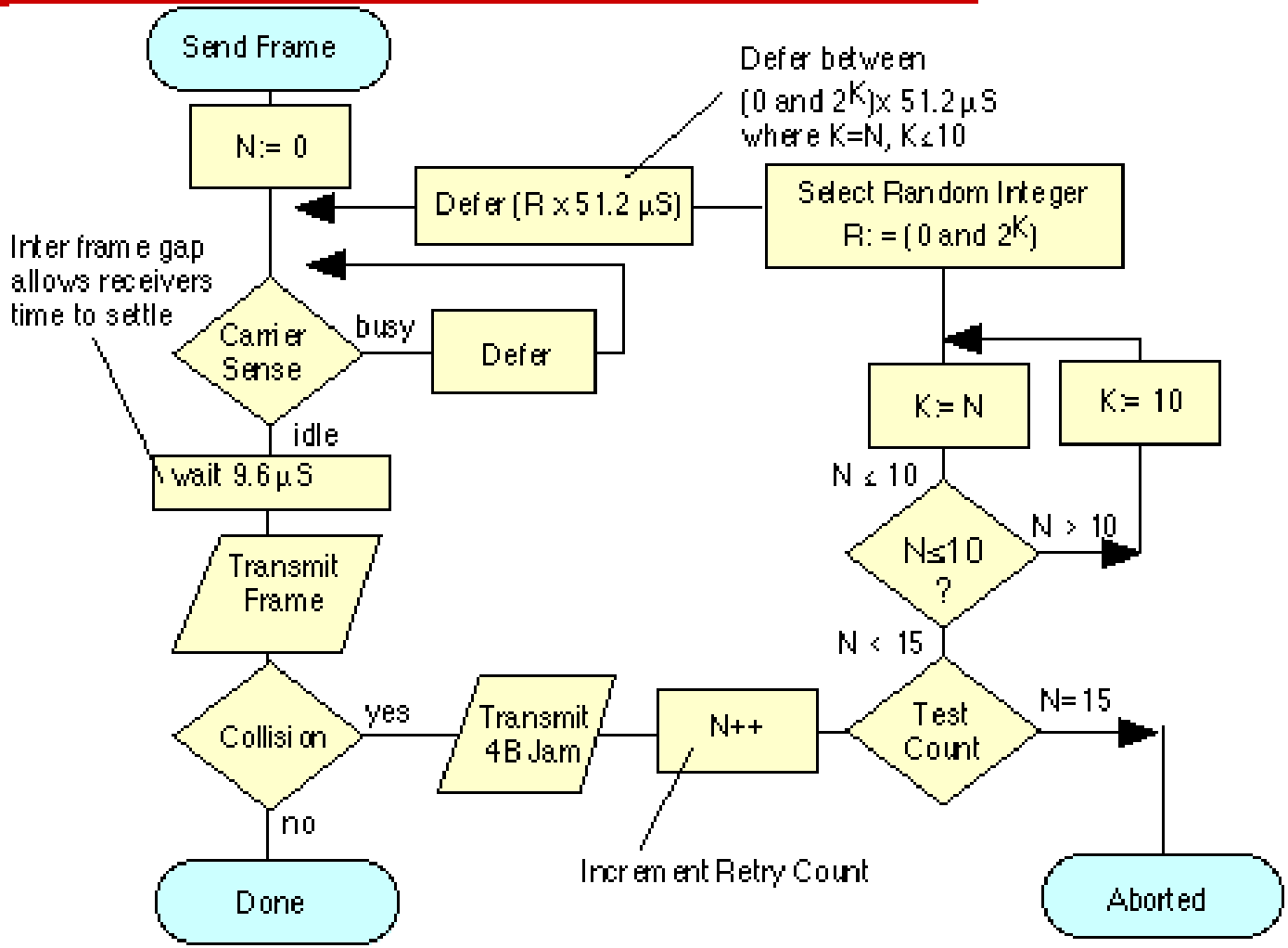
Medium Access Control – CSMA/CD

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - Az állomás figyeli a csatornát, a „vivőt” (carrier sense)
  - Ha nem érzékel adást, elkezdi küldeni a keretet
  - Ha kettő vagy több állomás ad, mindegyik abbahagyja az adást (ütközésérzékelés - collision detection)
  - Valamekkora (véletlen) késleltetést („backoff” time) követően az állomás újból megkísérli az adást
- A CSMA/CD-hoz szükséges, hogy
  - **adás előtt** vivőt érzékeljünk (carrier sensing – CS)
  - **adás alatt** érzékeljük, hogy más is ad (collision detection - CD)

Medium Access Control – a CSMA/CD elvi folyamatábrája



Az Ethernet MAC-protokollja



Backoff stratégia: truncated binary exponential backoff

Magyarázatok a MAC-protokollhoz

- Interframe gap (keretek közötti idő): 96 bit (9,6 µs 10 Mbit/s-nél)
- Retry count (ismétlésszám): N, N=1…15
- Véletlen késleltetésszám: R
  - *R*-et a [*0, 2^{K-1}*] intervallumból sorsoljuk, ahol *K=N*, ha *N<=10,* és *K=10*, ha *N>10*
  - 1. ütközés után: sorsoljuk *R*-et a *{0, 1}*-ből; a késleltetés *R*512* bitidő (1 bitidő 0,1 µs 10 Mbit/s-nál)
  - 2. ütközés után: *R*-et a *{0, 1, 2, 3}*-ből
  - …
  - 10. ütközés után: *R*-et a *{0, 1, 2, 3, 4, …, 1023}*-ből (Ez kb. max. 52,4 ms-ot ad.)
- Résidő: 512 bit = 51,2 µs 10 Mbit/s-en
- Jam (zavarás): 48 bitnyi ideig, hogy minden állomás biztosan érzékelje az ütközést

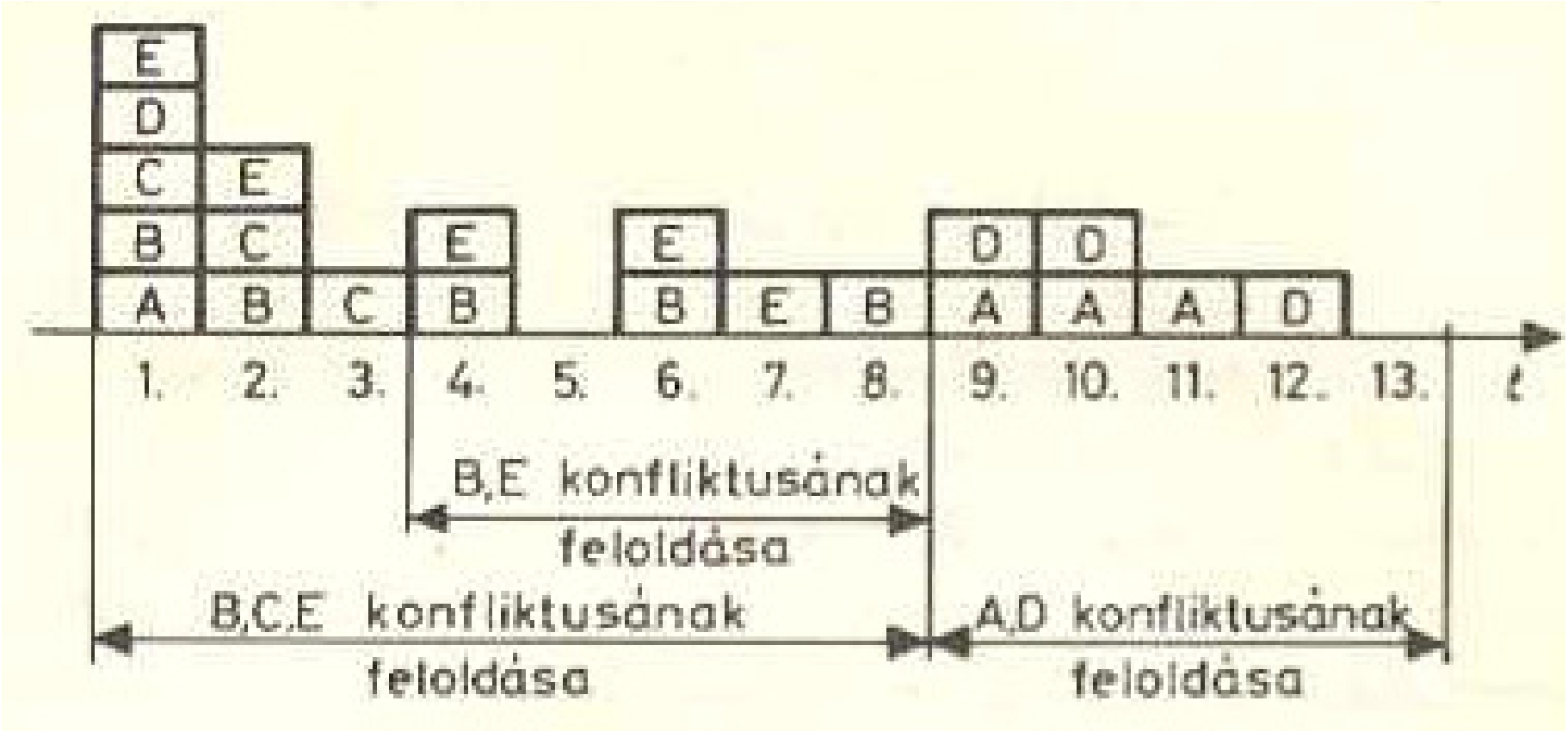
Capetanakis-faalgoritmus

Ütközésfeloldás

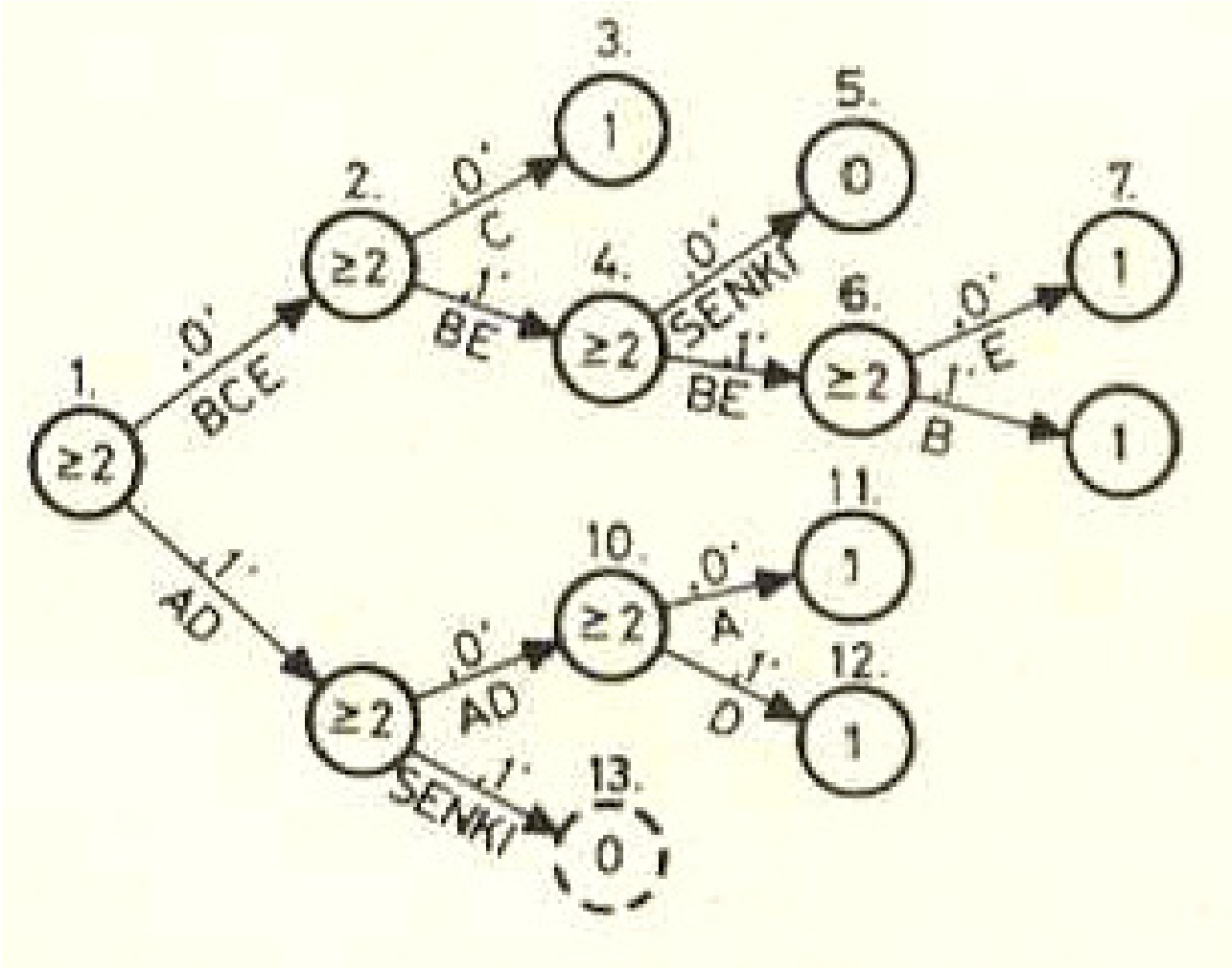
Ütközésfeloldás példa: a Capetanakis-féle faalgoritmus (tree algorithm)

- Első fontos javaslat ütközésfeloldó típusú algoritmusokra:
  - A felhasználók „tudják” a csatornáról
    - üres vagy sikeres vagy ütközött
  - Erre oly módon reagálnak (ez az itt nem részletezett algoritmus), hogy a konfliktus minél hamarább megszűnjék
- Alapvető különbség az Alohákhoz képest: ütközést követően a felhasználók annak feloldásával foglalkoznak
  - módszer, bár nem feltétlenül szükséges: ütközést követően az abban részt nem vettek várnak az ütközés teljes feloldásáig
  - stabil lehet a működés

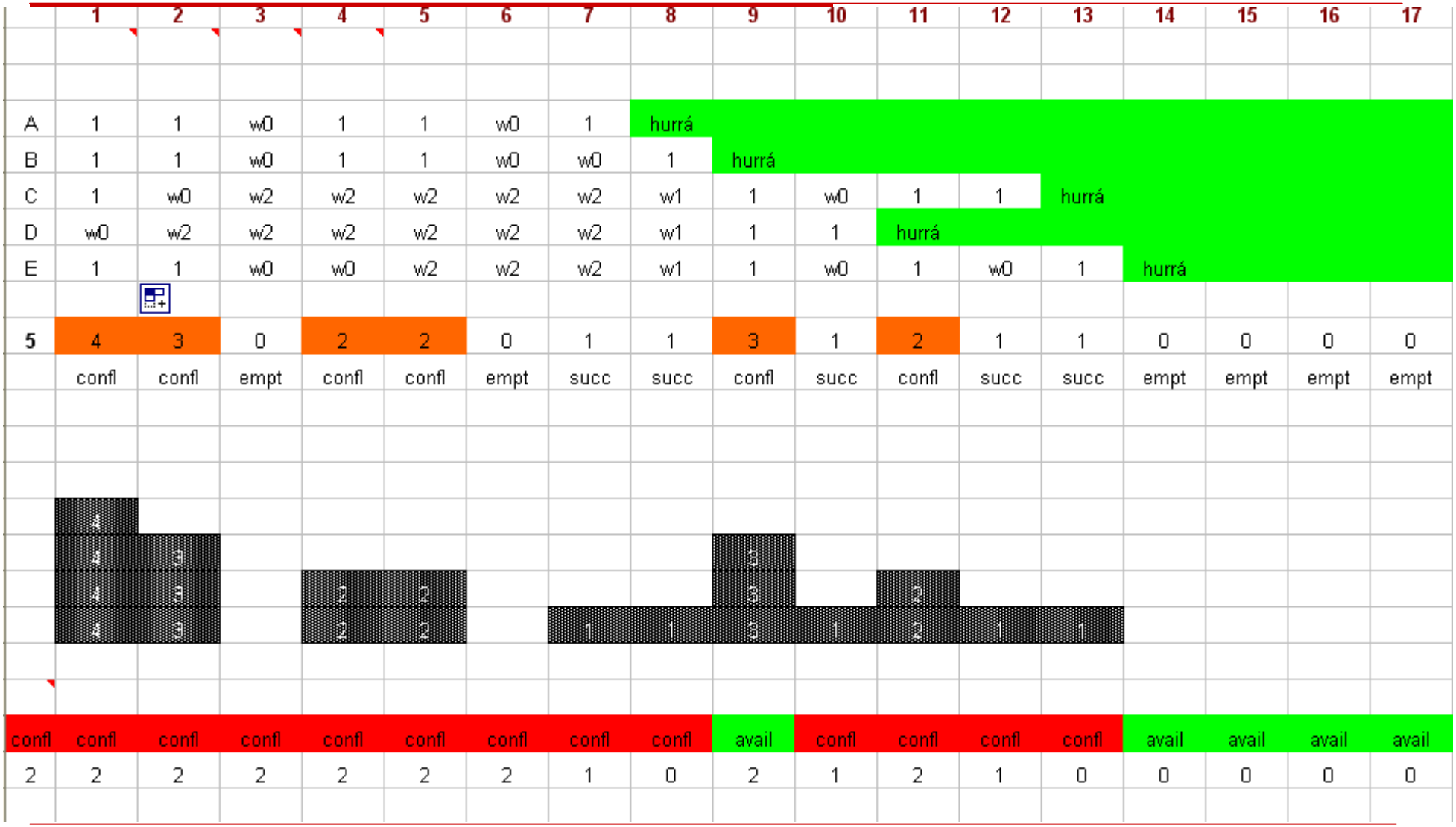
A Capetanakis-algoritmus működése - illusztráció



A Capetanakis-algoritmus működése Miért „faalgoritmus”?



A Capetanakis-algoritmus működése



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
A	1	1	w0	1	1	w0	1	hurrá									
B	1	1	w0	1	1	w0	w0	1	hurrá								
C	1	w0	w2	w2	w2	w2	w2	w1	1	w0	1	1	hurrá				
D	w0	w2	w2	w2	w2	w2	w2	w1	1	1	hurrá						
E	1	1	w0	w0	w2	w2	w2	w1	1	w0	1	w0	1	hurrá			
5	4	3	0	2	2	0	1	1	3	1	2	1	1	0	0	0	0
	confl	confl	empt	confl	confl	empt	succ	succ	confl	succ	confl	succ	succ	empt	empt	empt	empt
confl	confl	confl	confl	confl	confl	confl	confl	confl	avail	confl	confl	confl	confl	avail	avail	avail	avail
2	2	2	2	2	2	2	1	0	2	1	2	1	0	0	0	0	0

WiFi – CSMA/CA

802.11 MAC-réteg
Hozzáférési módszerek

- Carrier Sense Multiple Access/Collision Avoidance – CSMA/CA
  - Nem CSMA/CD (802.3), CS, de nem CD
  - Vezeték nélküli LAN-okban nem lehet ütközést detektálni
- Két hozzáférési módszer:
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)

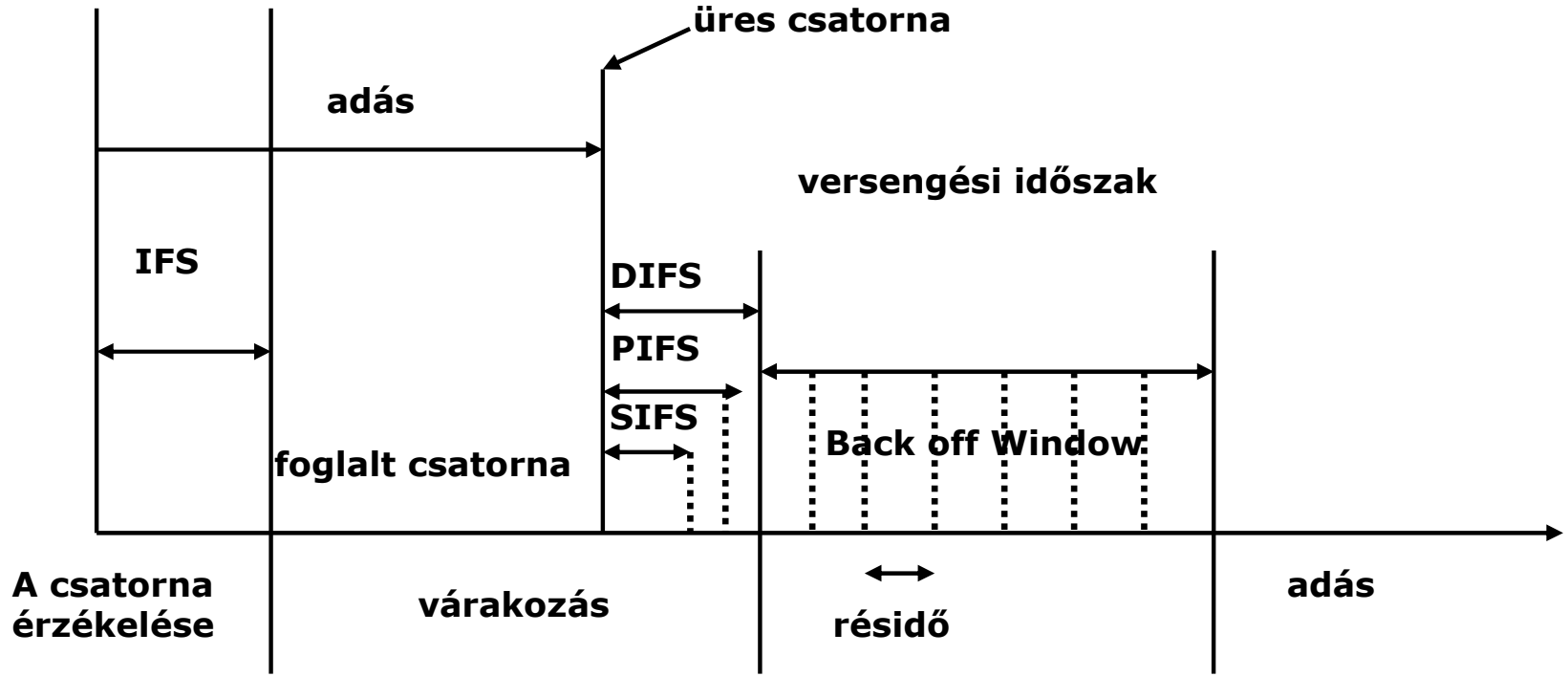
Distributed Coordination Function (DCF)

- A MAC alsó alrétege
- CSMA/CA
  - Collision Avoidance – Ütközés-elkerülés
- Nincs ütközésdetekció (az állomások nem képesek észlelni a máshonnan érkező jelek által létrehozott ütközést).
- Különböző értékű IFS-ek (InterFrame Space)
  - Short IFS – rövid IFS vezérlőüzenetek számára
  - PCF IFS (PIFS)
  - DCF IFS (DIFS) – adatkeretek számára

DCF algoritmus

- Ha a csatorna szabad, az állomás vár, hogy szabad marad-e IFS ideig. Ha igen, ad.
- Ha a csatorna foglalt (vagy már az elején, vagy azzá válik az IFS alatt), az állomás tovább figyeli.
- Amikor a csatorna szabaddá válik, az állomás vár IFS ideig, majd egy véletlen késleltetést választ. Amikor az letelik, megkezdi az adását.

CSMA/CA (DCF)



DIFS: DCF IFS

PIFS: PCF IFS

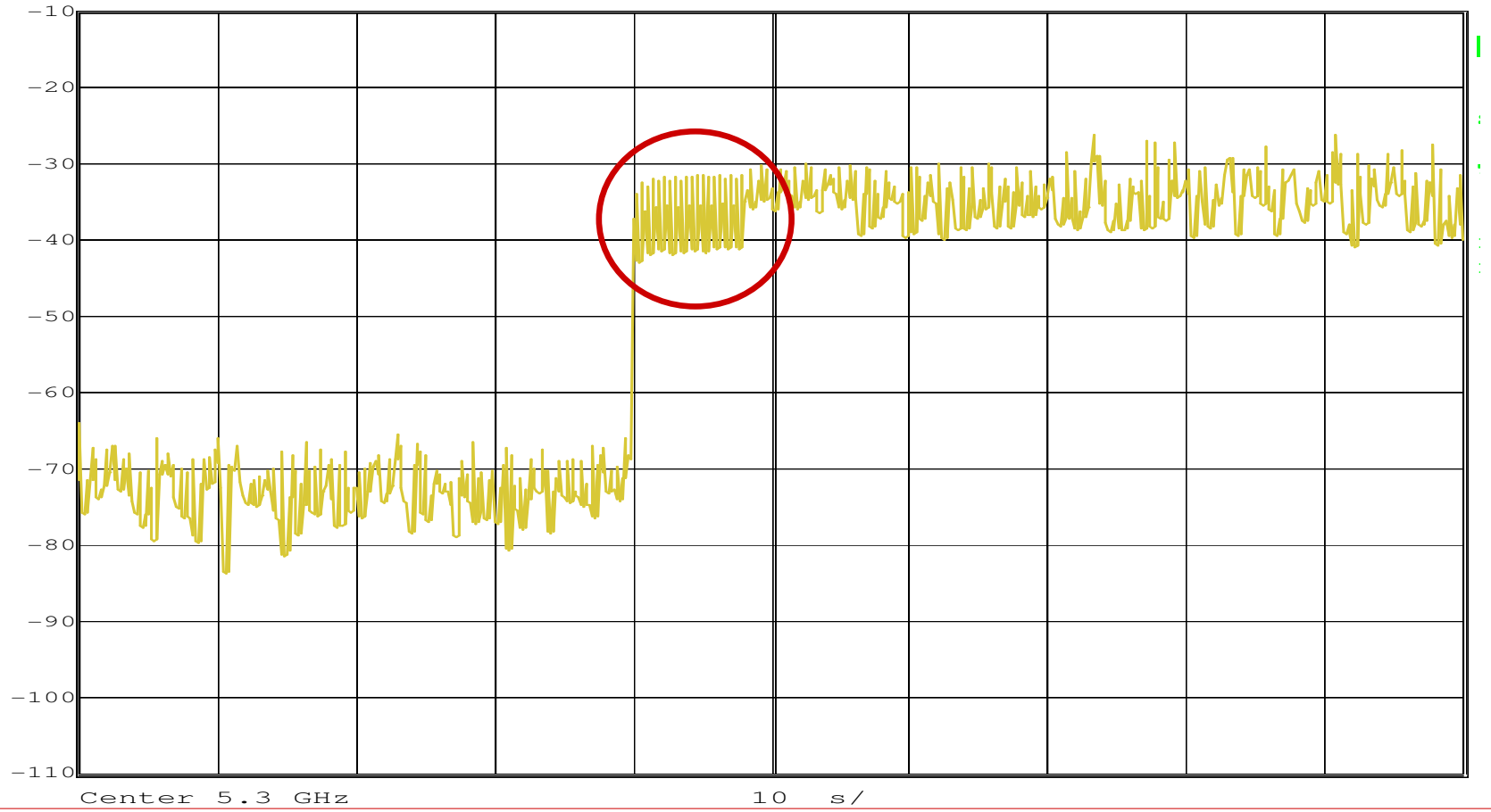
SIFS: Short IFS

Az exponenciális backoff algoritmus

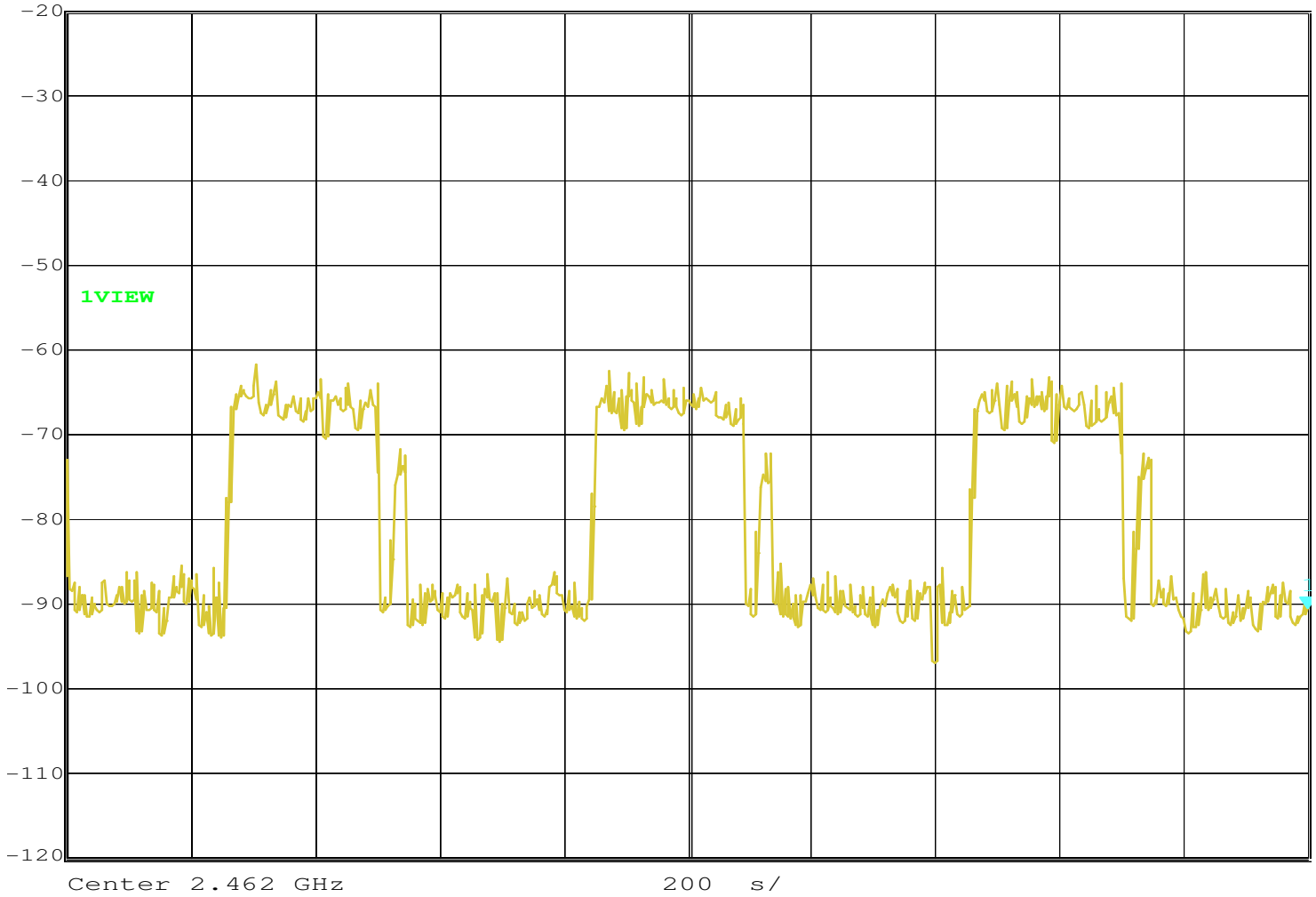
- Backoff_Time=INT(CW*RND())*Slot_Time
  - CW – Contention Window
    - Kezdetben 31, majd 63, 127 stb. A késleltetést itt résidőben (Slot_Time) mérjük
  - Résidő
    - Úgy kerül megválasztásra, hogy azalatt az állomás biztosan érzékelhesse a csatorna foglaltságát; 20 µs (DSSS), 50 µs (FHSS)
  - RND()
    - Véletlen számot generáló függvény 0 és 1 között

Fizikai keretformátum

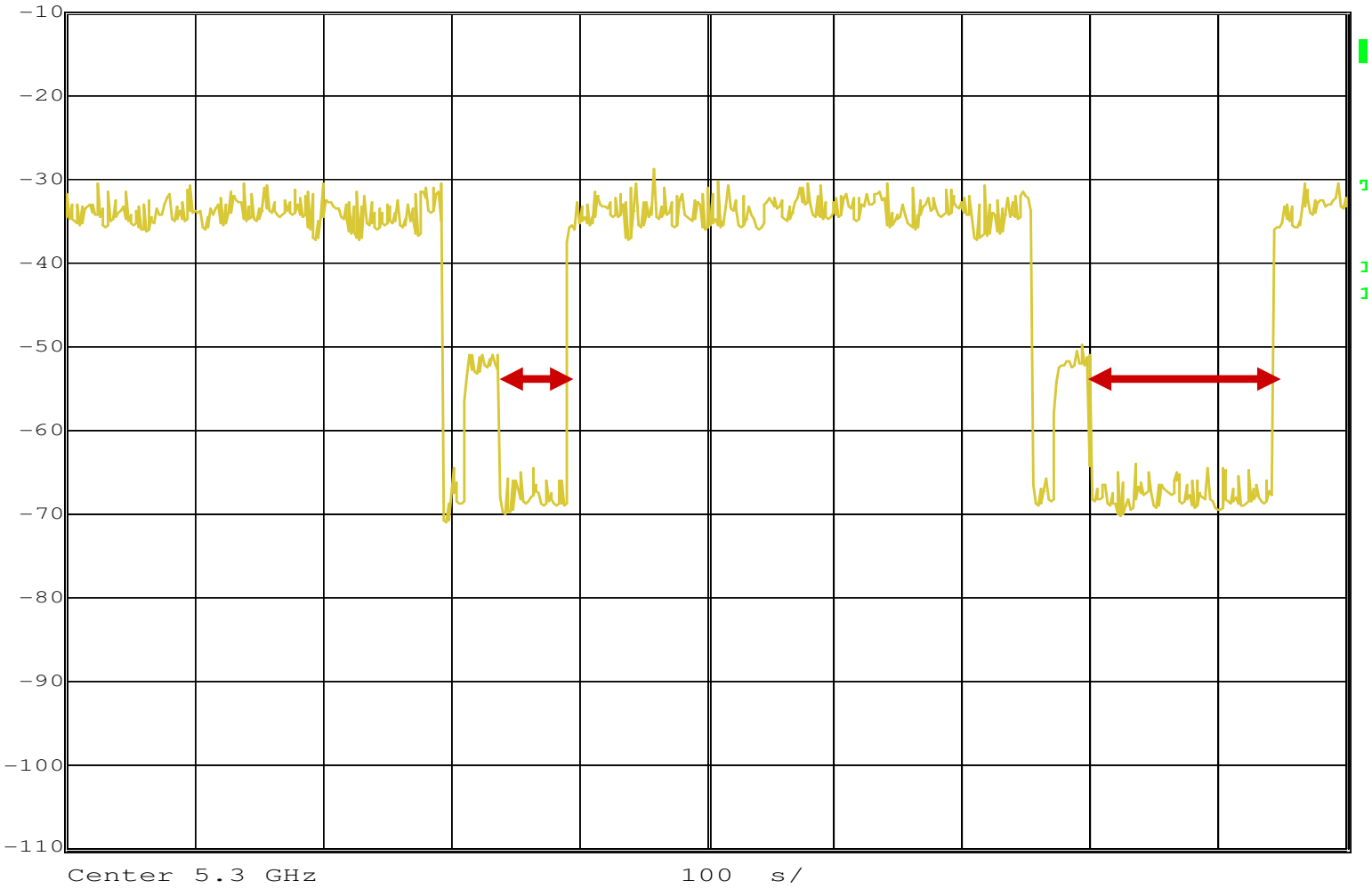
- Preamble („előke”) – szinkronizálás miatt



Időzítés a gyakorlatban: „adás – SIFS – nyugta – DIFS” ciklus



Véletlen backoff idő



WiFi biztonság elméletben *

Összefoglalót tartja: Matúz Tamás

(* A szabványok és működésük nem része a tananyagnak.)

WLAN biztonság

- Szabványok
- Hiányosságok
- A feltörés folyamata
- Jótanácsok

Szabványok - WEP

- WEP - Wired Equivalent Privacy
  (Vezetékessel Egyenértékű Titkosítás)
  - Egy kezdeti szabvány, a 802.11–ben jelent meg, sajnos könnyen törhető
  - 2000-ben hiányosságokat fedeztek fel benne, 2002-ben pedig az FBI ügynökei bemutatót tartottak a feltöréséről.
  - 4 db 64 bites kulcsot használ
  - RC4 folyamkódoló eljárással titkosít (hardverből támogatott)
  - 24 bites IV–ket (Initialization Vector) használ
- WEP2
  - Ugyan az mint a WEP(v1), csak 128 bitesek a kulcsok

Szabványok – WPA

- WPA - Wireless Protected Access (Vezetéknélk. Védett Hozzáférés)
  - 2003 óta létezik 802.11i szabványba került bele
  - Kulcsmenedzsment protokoll és „előtitkosías”:
    TKIP – Temporal Key Integrity Protocol
    (Ideiglenes kulcsintegritás protokoll)
  - 48 bitre nőtt az IV-k hossza
  - 256 bit vagy 8-63 karakter hosszú kulcsot használ
  - A WEP-nél jóval erősebb, de nem kell új hardver hozzá, mivel ugyanúgy az RC4 titkosító chipet használja
- WPA2
  - 802.11i definiálja
  - Erős titkosítás és hitelesítés, de új hardveren.
  - Titkosítás kezelése: CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)
  - Titkosítás:
    AES (Advanced Encryption Standard)
    (Tovább fejlesztett titkosítási szabvány)

Titkosítás és kulcsmenedzsment

	Kulcsmenedzsment protokoll	Titkosítás	Kulcshossz [bit]
OPEN	nincs	nincs	0
WEP	nincs	RC4	64
WEP2	nincs	RC4	128
WPA	TKIP	RC4	256
WPA2	CCMP	AES	256

Gyenge pontok

- PSK – Pre-shared Key (Előre osztott kulcs)
  - A jelszó az AP-n és a kliensen azonos
  - Ezáltal az egész hálózaton ugyanaz

- Hiányosságok
  - WEP
    - Az IV (Initialization Vector) csak 24 bites
    - Hitelesítés és rejtjelezés ugyanazzal a kulccsal történik
  - WPA
    - Kézfogás elcsípése esetén, a jelszó OFFLINE visszafejthető
    - PSK: 2,5*n+12 bitnyi védelem. (20 karakternél hosszabb jelszó)

A törés folyamata

- Környezet felderítése
  - Megnézzük milyen hálózatok vannak a közelben
  - Résztvevők „azonosítása” (AP – kliens)
- Csomagok mentése
  - A rádiós csatornán közlekedő csomagokat lementjük a gépünkre későbbi „felhasználásra”
  - Ehhez úgy kell beállítani a kártyánkat, hogy minden csomagot fogjon ne csak a neki címzetteket
- Jelszó kinyerése
  - WEP-nél közös IV-jű csomagok keresése után a jelszó úgynevezett „Key Recovery Attack”-kel megszerezhető
  - WPA-nál egy teljes „kézfogás” lementése esetén „Dictionary Attack” indítható

Jótanácsok

- Használaton kívüli WLAN-eszközök kikapcsolása
- SSID közzététel tiltása
- MAC-cím alapú szűrés
- WEP, WEP2, WPA, WPA2 engedélyezése
  - lehetőleg egyéni (nem PSK) kulccsal
- DHCP kikapcsolása
- IP tartomány korlátozása
- Tűzfal használata a kliensen a vezetéknélküli interfészre
- A szükséges jelerősség beállítása (a szomszéd ne vehesse :D)
- Tűzfal segítségével vezetékes hálózatunkat izoláljuk el a vezetéknélkülitől

„Minden rendszer olyan erős, mint a leggyengébb láncszeme.”

Felhasznált irodalom

- Szentgyörgyi Attila:
  WEP – AVAGY: Milyen a rossz biztonsági protokoll
  White Paper, Wyonair – WiFi és biztonság, 2007
  http://www.wyonair.com weboldal

- Szentgyörgyi Attila:
  WPA TKIP – A WEP hibáinak javítása
  White Paper, Wyonair – WiFi és biztonság, 2007
  http://www.wyonair.com weboldal

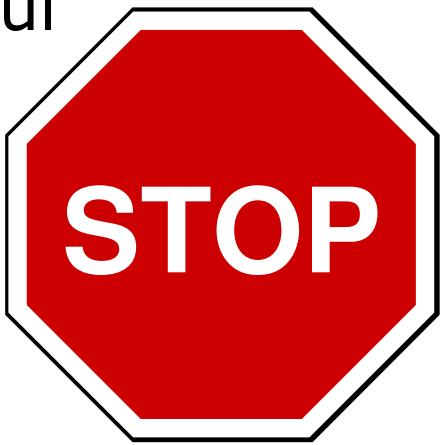
- http://backtrack4.blogspot.com/

Büntető Törvénykönyv 300-as paragrafus

- A törvény szerint ha egy hálózatba jogtalanul
  - Belépsz: egy évig terjedő
  - Adatot is módosítasz: két évig terjedő
  - Kárt is okozol: egy évtől öt évig terjedő

szabadságvesztés a jutalmad.

(Btk. § 300.)



Az előadáson elhangzott információk célja a tanulás elősegítése és az általánosan használt rendszerek biztonsági tényezőinek ismertetése.

Ezek felhasználása szigorúan tilos, mivel bűncselekmények minősül.

Access Point funkciók

Egy otthoni (SOHO) router
AP-funcióinak beállítása

Demó: Soproni Péter

Még egy WiFi-felhasználó

Problémamegoldás

Demó: Bessenyei Csilla

WEP és WPA feltörése

Mennyit ér a gyenge WiFi-biztonság?

Demó: Matúz Tamás