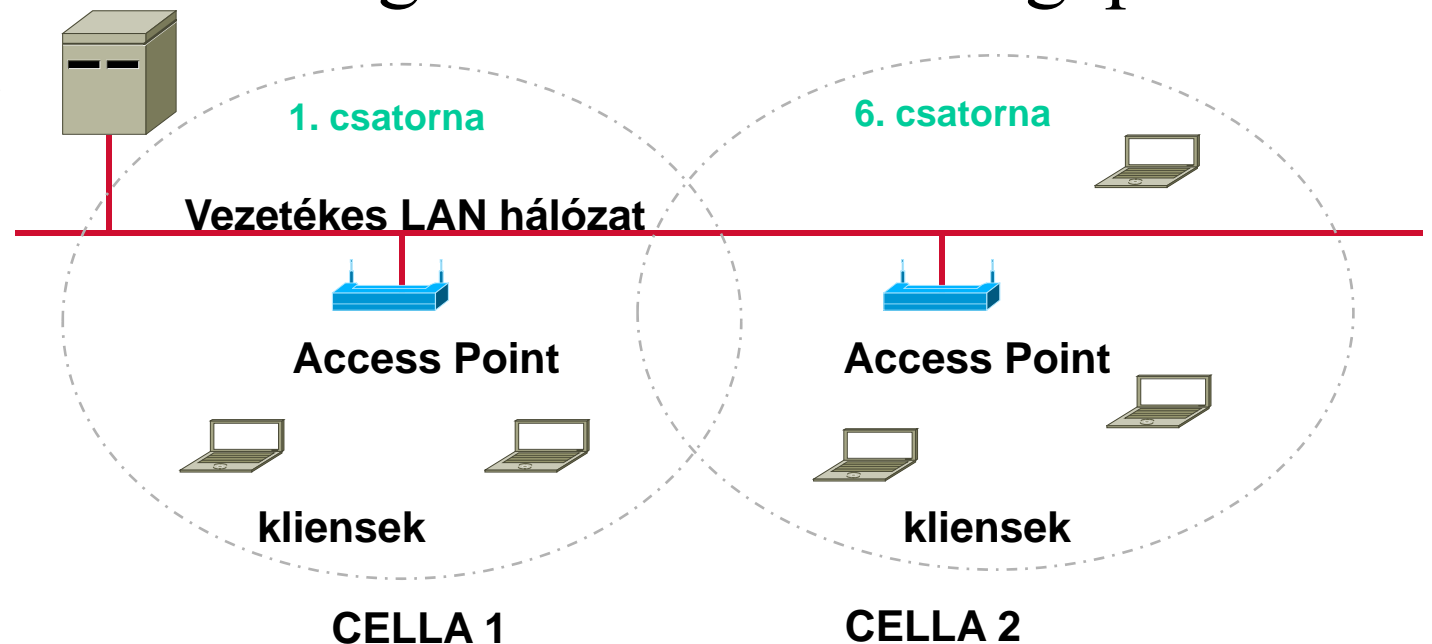


# IEEE 802.11

Fazekas Péter

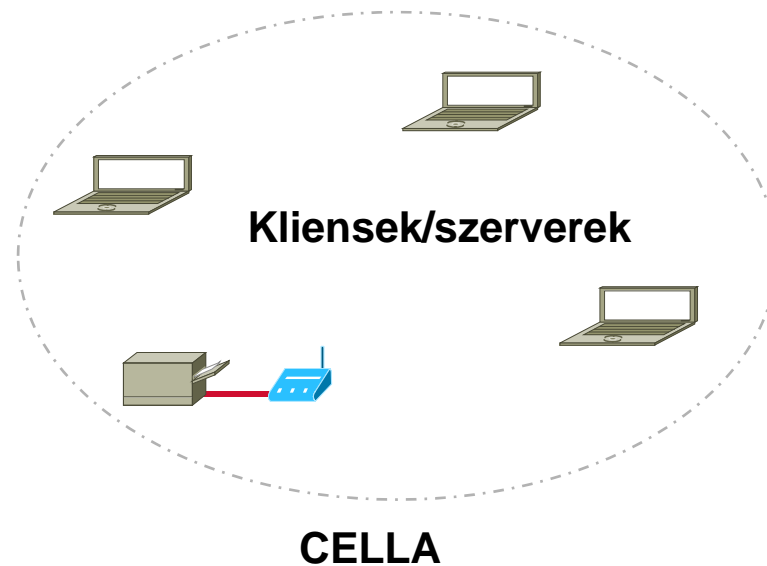
# Mi az a Wireless LAN?

- A vezetékes LAN hálózat vezeték nélküli meghosszabbítása.
- Vezeték nélkül megvalósított számítógép hálózat.



# Mi az a Wireless LAN?

- A vezetékes LAN hálózat vezeték nélküli meghosszabbítása.
- Vezeték nélkül megvalósított számítógép hálózat.



# IEEE 802.11

- IEEE 802.11: WLAN
- IEEE 802.3: Ethernet
- IEEE 802.5: Token Ring
  
- Együttműködés: IEEE 802.2 közös LLC réteg specifikáció, a fenti szabványok ez alatt működnek

# Felépítés

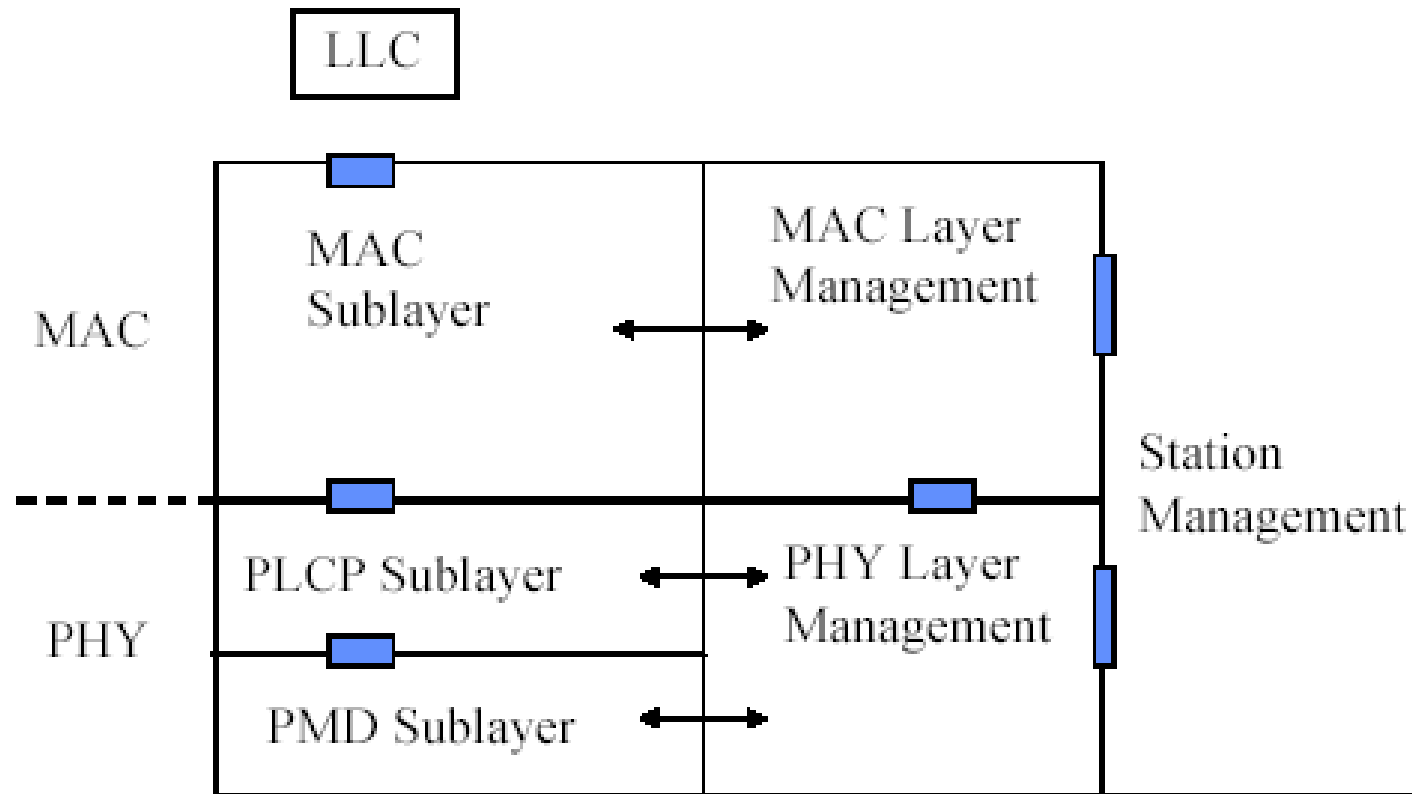
- alapegység: cella (**Basic Service Set, BSS**, a 802.11 terminológiában) egy
- bázisállomás vezérel (**Access Point, AP**), egy WLAN állhat egyetlen cellából egyetlen APvel a legtöbb esetben több cella alkot egy hálózatot
- az AP-eket egy elosztó hálózat köti össze (**Distribution System, DS**)
- Az összekapcsolt WLAN cellákból és a hozzájuk tartozó AP-kből valamint az elosztó hálózatból áll, együtt egy 802.11 hálóza a felsőbb OSI rétegek számára
- a szabványbeli elnevezése: **Extended Service Set (ESS)**
- a **Portal** : Portál a 802.11 és egy másik 802 LAN összekapcsolására szolgáló eszköz, gyakorlatban: az AP tartalmazza, így ez „híd” (bridge) az Ethernet háló felé
- ez így: infrastruktúra mód. de létezik ezen kívül: ad-hoc mód, nincs infrastruktúra, nincs bázisállomás, minden csp. egyenrangú és továbbítja egymás csomagjait

# Elosztó hálózat

- Az elosztó rendszer konkrét megvalósítását a szabvány nem definiálja, csak az általa nyújtott szolgáltatásokat
- topológia lehet gyűrű (token ring)
- sín (Ethernet: ez a tipikus), lehet token bus
- logikai gyűrű: sínen kialakítva
- csillag: központi egységen keresztül megy minden kommunikáció, a közp. egység lekérdezi, vagy kiosztja hogy melyik AP mikor
- Az elosztó rendszer kiterjesztett hálózati szolgáltatásokat nyújt a hozzákapcsolódó BSS-ek és LAN integrációkon keresztül és tetszőleges bonyolultságú vezeték nélküli hálózat kialakítását teszi lehetővé
- az elosztó rendszer függetlenül definiálható bármelyik fizikai megvalósítás jellegzetességeitől, ezért a közeghozzáférést szabályzó réteg fölött elhelyezkedő réteg számára úgy tűnik, mintha a különálló BSS-ek egyetlen független BSS-et alkotnának

# Protokoll rétegek

- Mint minden 802.x protokoll, a 802.11 protokoll a MAC és a Fizikai réteget definiálja



# Protokoll rétegek

- MAC Entitás
  - alap közeghozzáférés
  - fragmentáció
  - titkosítás
  - szinkronizálás
- MAC Layer Management Entity
  - szinkronizálás
  - teljesítmény menedzsment
  - roaming (cellaváltás)
  - MAC MIB (Management Information Base) fenntartás
- Physical Layer Convergence Protocol (PLCP)
  - PHY-specifikus, közös PHY SAP-ot biztosít, azaz a MAC kereteket (MPDU) fizikai csomagokká alakítja oda és vissza.
  - Clear Channel Assessment jelet biztosít (vivőérzékelés)



# Protokoll rétegek

- Physical Medium Dependent Sublayer (PMD)
  - moduláció és kódolás
- PHY Layer Management
  - csatorna hangolás – link adaptáció
  - PHY MIB fenntartás
- Station Management
  - a MAC és a PHY menedzsmenttel működik együtt, illetve az együttműködésüket hangolja össze

# Protokoll rétegek

- A MAC rétegek által ellátott tipikus szabványos funkcionalitásokon túl a 802.11 MAC további funkciókat is ellát, melyeket tipikusan felsőbb rétegek szoktak pl. fragmentáció, csomag újraadás, nyugtázás.
- az IEEE802.11 szabvány egyetlen MAC-et definiál, ami 3 PHY-vel tud együttműködni, melyek 1 vagy 2 Mbps-os átvitelt biztosítanak
  - Frekvenciaugratásos szórt spektrumú (Frequency Hopping Spread Spectrum, FHSS) a 2.4 GHz sávban
  - Direkt szekvenciális szórt spektrumú (Direct Sequence Spread Spectrum, DSSS) a 2.4 GHz sávban és
  - infravörös

# MAC

- *Elosztott*: Distributed Coordination Function (DCF): ahol a mobil terminálok ugyanazt az egyszerű szabályt alkalmazzák a rádiócsatorna megszerzésére, mindenféle központi „döntőbíró” nélkül. Az az időszak, amíg ez tart: CP, contention period
- *Központosított*: Point Coordination Function (PCF), ahol a terminálok kérései alapján az AP dönt a rádiócsatorna kiosztásáról, és a döntésének megfelelően adja meg a jogot az egyes mobil állomásoknak az adásra. Az időszak, amíg ez tart: CFP, Contention Free Period
- Elvileg: a CFP és CP időszakok periodikusan váltják egymást, hosszuk, arányuk beállítható de állandó, nem alkalmazkodik a pillanatnyi forgalmi igényekhez.

# MAC

- Az alap közeghozzáférési módszer a **Distributed Coordination Function** alapvetően CarrierSense Multiple Access megoldásra épül Collision Avoidance mechanizmussal kiegészítve (**CSMA/CA**)
- A CSMA protokollok jól ismertek az iparban, ilyen pl. az Ethernet, ami CSMA/CD módszer használ
- Az adni kívánó állomás figyeli a közeget. Ha a közeg foglalt (másik állomás ad) akkor elhalasztja az adását egy későbbi időpontra. Ha a közeget szabadnak érzékelté, akkor megkezdheti
- akkor hatékony, ha a közeg nem túl terhelt, ilyenkor minimális késleltetéssel adhatnak
- előfordulhat, hogy több állomás egyidejûleg szabadnak érzékeli a közeget és egyszerre kezd adni, ütközés
- ütközési helyzeteket fel kell tudni ismerni és így a MAC réteg újraadhatja a csomagot és nem a felsőbb rétegeknek kell ezzel foglalkozni, ami jelentős késleltetést okozna
- Ethernet esetén az ütközést az adó állomás ismeri fel és ezután egy ún. újraadási fázisba megy át

# MAC

- CD-t WLAN-oknál nem célszerű alkalmazni a következők miatt:
- Collision Detection eljárás megvalósítása Full Duplex rádiós képességeket igényelnek, ami jelentősen növelné az árakat
- ütközés érzékelése nehézkes, mert a saját jel elnyomja az esetleg távoli másik terminál kis teljesítményű jelét
- vezeték nélküli környezetben nem tételezhetjük fel, hogy minden állomás hallja a többit (ami a Collision Detection alapja), így a tény, hogy egy állomás szabadnak érzékelt a közeget, nem jelenti azt, hogy az a vevőnél csakugyan szabad is

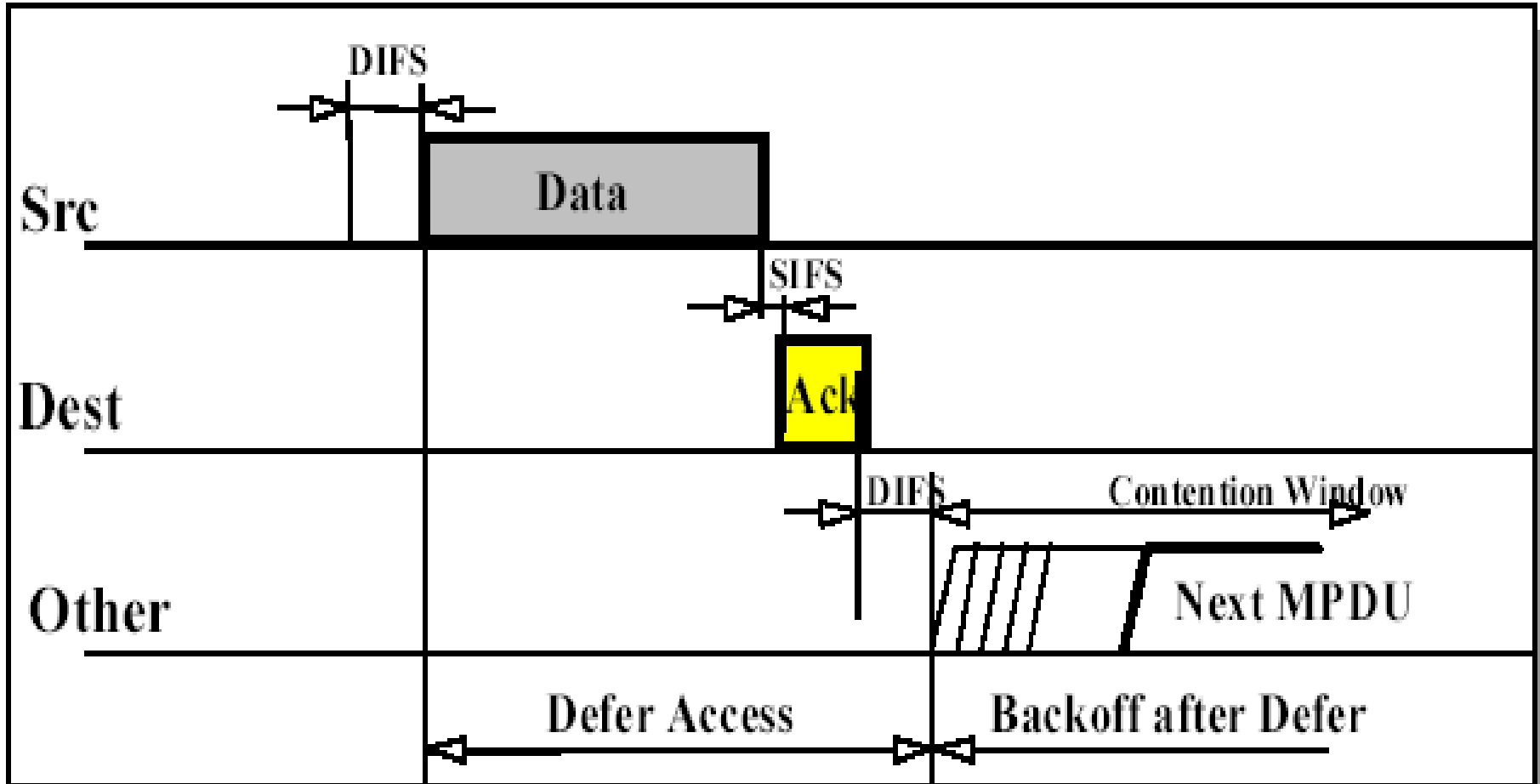
# MAC – CSMA CA

- Az adni kívánó állomás érzékeli a közeget. Ha foglalt, akkor elhalasztja az adását.
- Ha szabad egy előre definiált ideig (Distributed Inter Frame Space, DIFS), akkor adhat.
- A vevő állomás ellenőrzi a vett csomag CRC-jét és nyugtát küld SIFS (Short Interframe Space) idő után (acknowledgment packet, ACK, MAC nyugta)
- A nyugta vétele jelzi az adónak, hogy nem történt ütközés. Ha az adó nem kapott nyugtát újra küldi a csomagot amíg nyugtát nem kap vagy el nem dobja adott számú próbálkozás után.
- A SIFS azért kisebb, mint a DIFS, hogy a harmadik állomás ne kezdhesen el adni a nyugta elküldése előtt. (Az egynél több célcímű csomagokra, pl. multicast, nincs nyugta).

**Table 4.5**  
Interframe Space Specifications

<b>Interframe Space</b>	<b>DSSS</b>	<b>FHSS</b>	<b>DFIR</b>
<b>SIFS</b>	10 $\mu\text{s}$	28 $\mu\text{s}$	7 $\mu\text{s}$
<b>PIFS</b>	30 $\mu\text{s}$	78 $\mu\text{s}$	15 $\mu\text{s}$
<b>DIFS</b>	50 $\mu\text{s}$	128 $\mu\text{s}$	23 $\mu\text{s}$
<b>Slot time</b>	20 $\mu\text{s}$	50 $\mu\text{s}$	8 $\mu\text{s}$

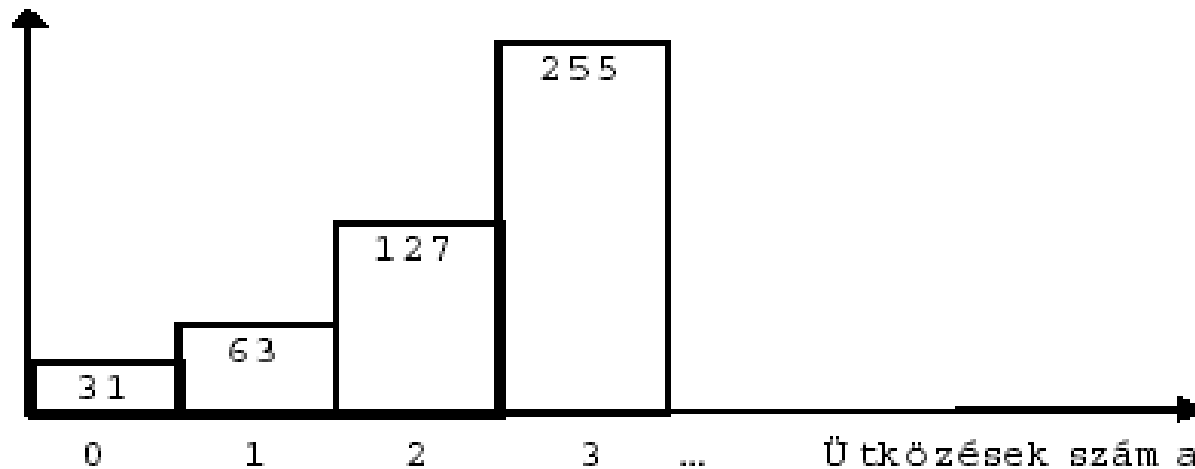
# MAC – CSMA CA





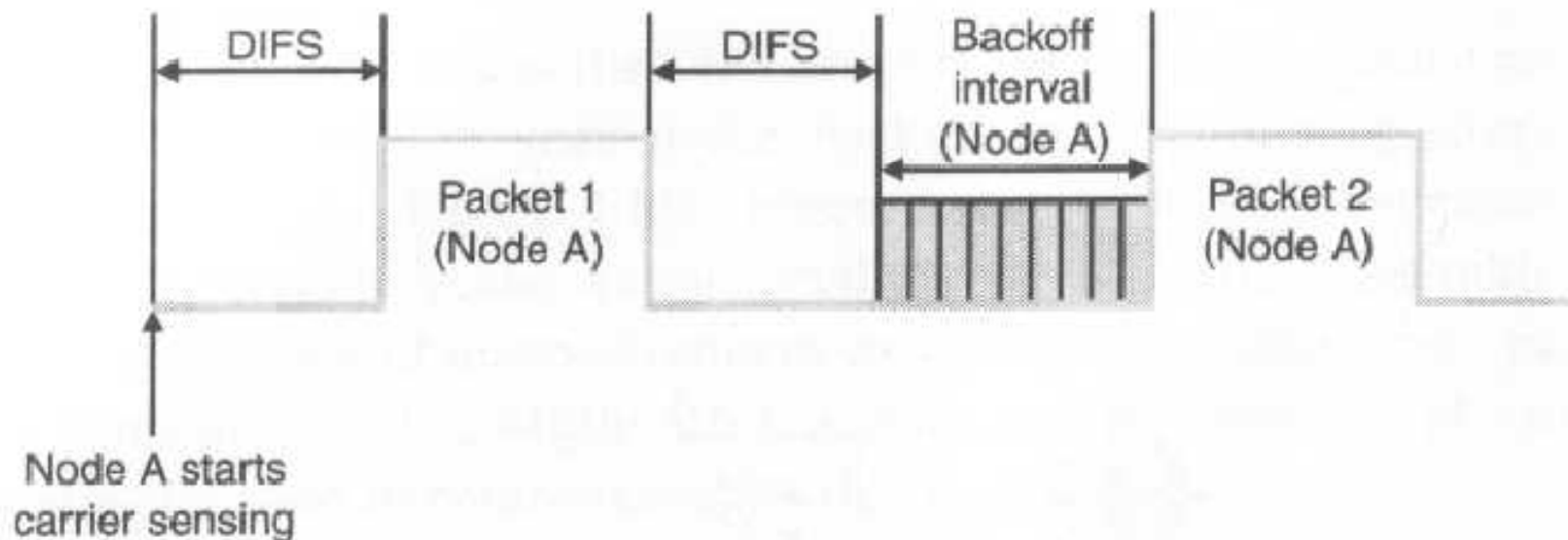
# MAC – CSMA CA

- backoff: minden állomás egy véletlen számot generál  $n$  és 0 között és a generált számnyi üres időrést (slot) vár mielőtt a közeghez fordulna.
- egy állomás egy időrést választ és az ütközik, akkor a véletlen szám generálás felső határát duplázza



# MAC – CSMA CA

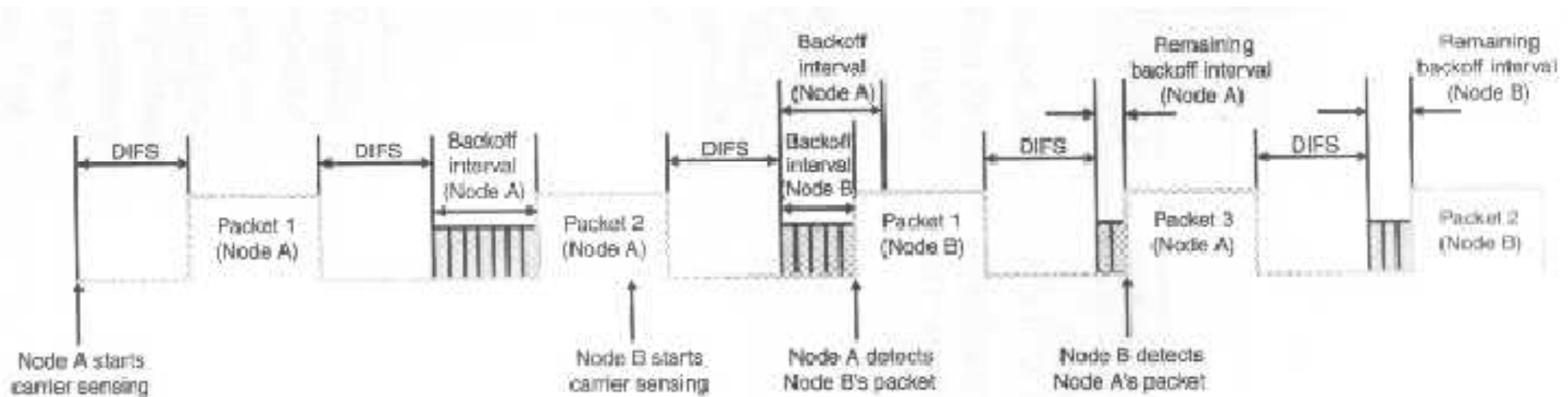
- amikor az első átvitel előtt az állomás figyel a közeget és azt foglaltnak találja
- Ha nem jön ACK
- minden sikeres átvitel után (multipacket transmission során, így fair, esélyt adunk, hogy a többi is adáshoz jusson



2.6. ábra Multipacket transmission szemléltetése

# MAC – CSMA CA

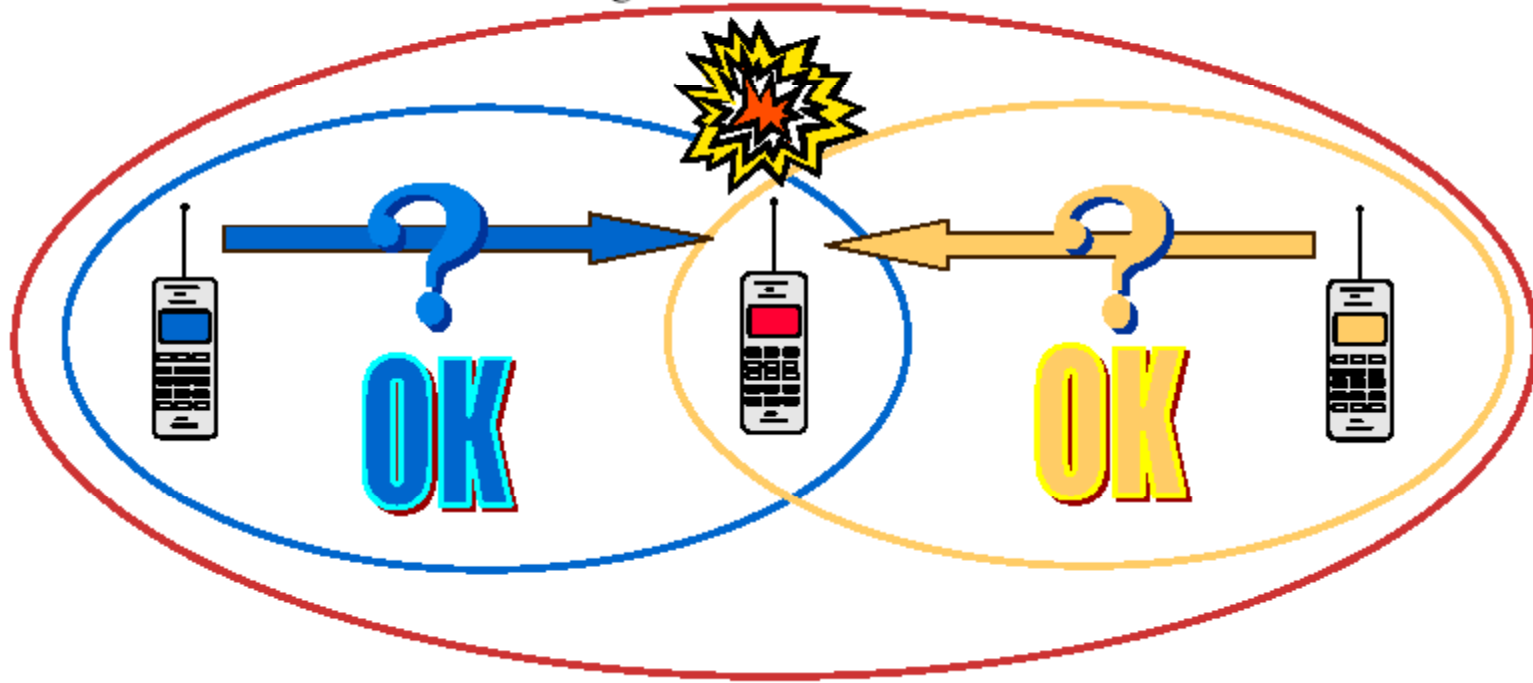
- nem használandó ez az eljárás, ha az állomás adni kíván és előtte DIFS ideig szabadnak érzékelt a közeget
- késleltetési idő csökkentése akkor kezdődhet meg, ha a médium DIFS ideig szabad időrelenként eggyel csökkentik
- ez a folyamat egészen addig tart, míg a médiumon átvitelt nincs, ha van, a késleltetési idő csökkentése befejeződik a következő DIFS idejű üresnek érzékelésig.
- egy terminál akkor adhat, ha a késleltetési ideje nullára csökken.



2.7. ábra Közeghozzáférés működésének szemléltetése

# Rejtett terminál probléma

terminál összekötés a csomágon.

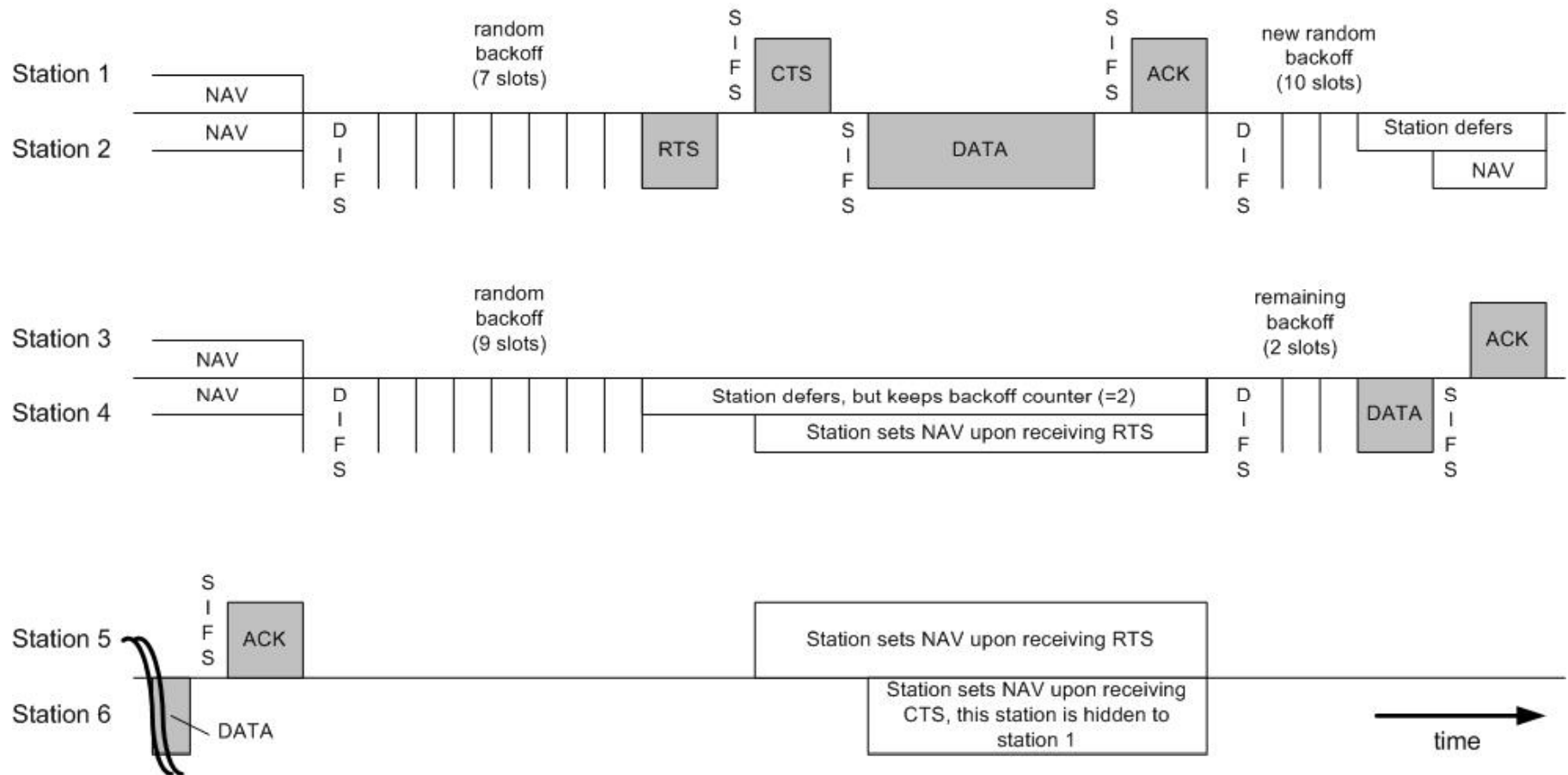


2.9 ábra Rejtett terminál probléma szemléltetése

# virtual carrier sense

- adás előtt RTS
- SIFS után az AP CTS-t
- mindkettőben benne van az adás hossza (ack-kal együtt)
- minden terminál, aki az RTS-t, CTS-t hallja, megjegyzi (NAV: network allocation vector), addig nem próbálkozik
- **RTS Threshold** változó: csak az ennél hosszabb csomagokra alkalmazható az RTS/CTS eljárás (rövidnél nem érdemes)

# DCF Operation



# Központosított: PCF

- PIFS - Point Coordination Inter Frame Space, az AP használja a többi állomás előtti közeghez való hozzáférésre értéke a SIFS plusz egy Slot Time (azaz  $SIFS < PIFS < DIFS$ )
- időkorlátos szolgáltatások, pl. video vagy beszédátvitel magasabb prioritást igényelnek, mint a sima adatátvitel, erre lett kitalálva
- PCF alapja: AP lekérdezi a terminálokat sorban egymás után (akik részt vesznek a PCF működésben)
- ilyenkor nem kell RTS,CTS, AP kezdi a lekérdezést PIFS időt várva az első lekérdezés előtt
- lekérdezésre válasz SIFS idő múlva, ACK is. ACK is, lekérdezés is hasznos csomaghoz csatolva, nem kell neki külön megszerezni a csatornát
- ACK mehet a versenyzéses időszakban
- PCF időtartam alatt a DCF-ben részt vevők nem figyelik a csatornát (NAV-ot PCF idejére állítják)
- a biztonság kedvéért PCF idején a kereteket SIFS időnként adják, így az alap terminálok soha nem csökkentenék várakozási idejüket
- keretekben információ: mennyi ideig tart a keret és a nyugta, időtartam alapján felülírja a NAVt, ha az nagyobb az eredetinél
- a PCF opcionális, az alap CSMA/CA ra épül

# MAC Layer mngmt

- egy állomás egy létező BSS-hez akar kapcsolódni
- Passive Scanning: egy Beacon Frame-t vár az AP-tól (a beacon keretet az AP periodikusan küldi szinkronizációs információval ellátva)
- Active Scanning: az állomás megpróbál egy AP-t találni Probe Request Frame-ek küldésével és ezután Probe Response-ra vár az AP-től
- Probe responsok alapján választ egy AP-t, aminek association req. t küld
- megkezdődik a csatlakozás az APhez



# MAC Layer mgmnt

- hitelesítési eljárás: csatlakozási kérelem és válasz után, mindkét fél hitelesíti magát
- csatlakozási eljárás: sikeres hitelesítés után, információcsere a terminál és AP képességeiről, valamint néhány AP-s környezetben meglesz a mobil helye
- szinkronizáció megtartása: az AP által küldött beacon keretek segítségével, periodikusan (CSMA miatt némi késés lehet)

# MAC Layer mgmnt

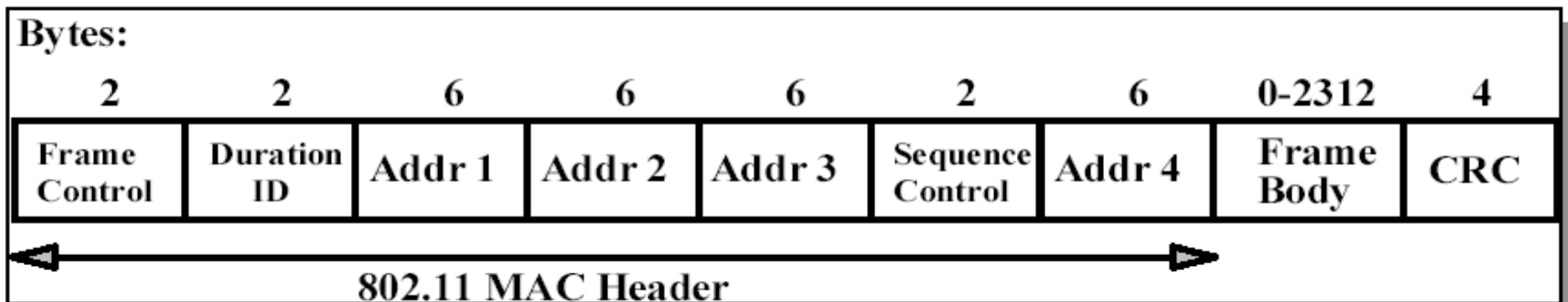
- energiatakarékos üzemmód: mobilok alvó állapota, nem hallgatják a csatornát
- az AP nyilvántartja hogy melyik MS-ek alszanak, tárolja a nekik szóló csomagokat
- a mobilok csak a beacon kereteket figyelik (periodikusan küldve), ebben jelzi az AP, ha van adat
- a mobilnak normál üzemmódba kell lépnie és lekérdeznie az AP-től a neki szóló adatot
- a beaconban jelezve, ha broadcast v. multicast üzenet jön, jelezve az idő is DTIM, amikor megkísérli küldeni

# MAC Layer mgmnt

- energiatakarékos üzemmód: mobilok alvó állapota, nem hallgatják a csatornát
- az AP nyilvántartja hogy melyik MS-ek alszanak, tárolja a nekik szóló csomagokat
- a mobilok csak a beacon kereteket figyelik (periodikusan küldve), ebben jelzi az AP, ha van adat
- handover: mobil dönt, új AP passzív vagy aktív kiválasztása, a legjobbhoz csatlakozási kérelem, ez a hálózaton keresztül értesíti a régi AP-t

# Keret típusok

- Data Frame-k: adatátvitel céljaira
- control Frame-k: a közeghozzáférés vezérlés céljaira (pl. RTS, CTS, és ACK),
- menedzsment Frame-k: az adat keretekkel megegyező módon küldik őket a menedzsment információk cseréje végett, de nem továbbítják őket a felsőbb rétegekhez (pl. authentication, probe request, stb.)
- MAC keret:



2.23. ábra Általános MAC keretformátum

# Keret típusok

- **CONTROL**

- RTS
- CTS
- ACK
- PS-Poll
- CF-End & CF-End ACK

- **DATA**

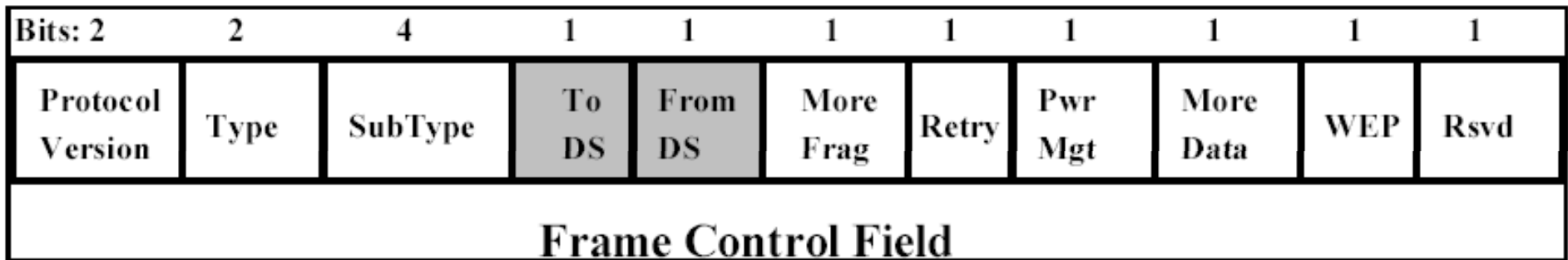
- Data
- Data+CF-ACK
- Data+CF-Poll
- Data+CF-ACK+CF-Poll
- Null Function
- CF-ACK (nodata)
- CF-Poll (nodata)
- CF-ACK+CF+Poll

- **MANAGEMENT**

- Beacon
- Probe Request & Response
- Authentication
- Deauthentication
- Association Request & Response
- Reassociation Request & Response
- Disassociation
- Announcement Traffic Indication Message (ATIM)

# Keret típusok

- MAC keret frame control:



2.24. ábra Frame Control mező

- Protocol Version, Type and Subtype: pl. RTS, CTS, ACK, poll, authentication, stb.
- ToDS, FromDS: hálózatba/ból a keret (tehát 0 pl. RTS, CTS), More Fragments: a MAC keret egy nagyobb felső keret darabja, Retry: újraadott keret-darab
- *Power Management*: jelzi, hogy ezen keret átvitele után az állomása Power Management üzemmódba megy át, azok az állomások használják, melyek Power Save állapotból Active állapotba lépnek vagy fordítva

# Keret típusok

- *More Data*: jelzi, a Power Management-nek az AP révén, hogy további tárolt keretek vannak az állomás részére
- WEP: jelzi, hogy a keret törzsét a WEP-nek megfelelően titkosították
- MAC keret további mezők:
- Duration/ID: Power-Save Poll üzenetekben az Station ID., egyébként a NAV számításhoz időtartam
- **Address Fields** max. 4 címet tartalmazhat a ToDS-től és a FromDS bitektől függően:
- **Address-1** mindig a Recipient Address, **Address-2** mindig a Transmitter Address
- **Address-3** a legtöbb esetben a maradék hiányzó cím. Egy keretben ahol FromDS=1, Address-3 az eredeti Source Address, ha a keretben ToDS=1, akkor Address 3 a célcím.
- **Address-4** speciális esetekben használják, amikor Wireless Distribution System-t alkalmaznak és az éppen adás alatt levő keretet egyik Ap-től a másiknak küldik. Ilyen esetben mind ToDS=1 és FromDS=1, így az eredeti cél és forrás cím is hiányzik.

# Keret típusok

- **Sequence Control**
- A Sequence Control Field mutatja a egyazon kerethez tartozó különböző fragmentek sorrendjét és segít a csomagduplikációk felismerésében. Két almezőt tartalmaz, Fragment Number és Sequence Number, melyek megadják a keret és a fragment sorszámát a keretben.
- **CRC** A CRC 32 bites mező 32-bites Cyclic Redundancy Check-t (CRC) tartalmaz.