tilb
Távközlés-
Informatika
Laboratórium

IP alapú kommunikáció

8. Előadás – WLAN alapok

Kovács Ákos

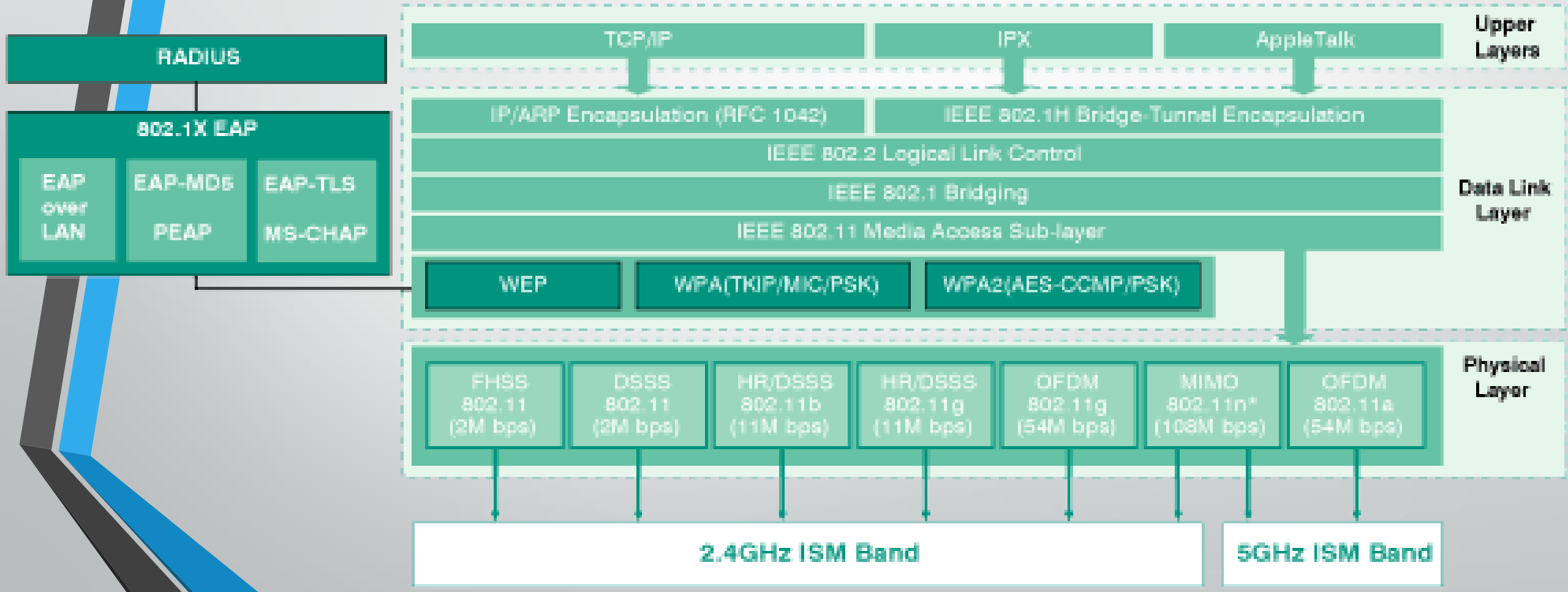
tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok

- 1997-ben kiadott, 99-ben elfogadott IEEE802.11 szabványcsalád
- Wi-Fi -> Wireless Fidelity minősítés nem protokoll
- Egy általános MAC réteget (tipikusan levegő) de használható infravörös- és lézerfény is
- 802.11 szabványcsalád mely a 900MHz, 2.4, 3.6, 5, 60GHz tartományban használható (ISM, U-NII 1-2, 2e, 3)
- MAC és PHY layer szabványok
  - Funny Fact: A Wi-Fi-vel elért eddigi (2007-es évben történt kísérlet) legnagyobb hatótávolság 382 km. Venezuelában az El Aguila és Platillon hegyek között. Ezt bolti hosszútávú (60 dolláros eszköz) és saját eszközök összekapcsolásával érték el. Mindkét irányba 3 MB/s sebességet tudtak elérni, hang és videokapcsolat is sikerült. (Wikipedia)

tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok

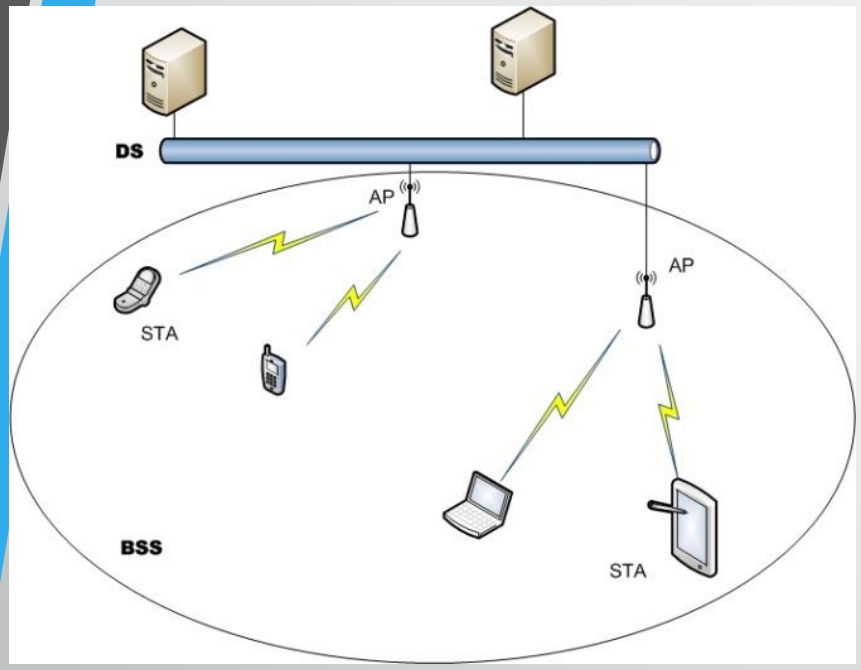


tilb
Távközlés-
Informatika
Laboratórium

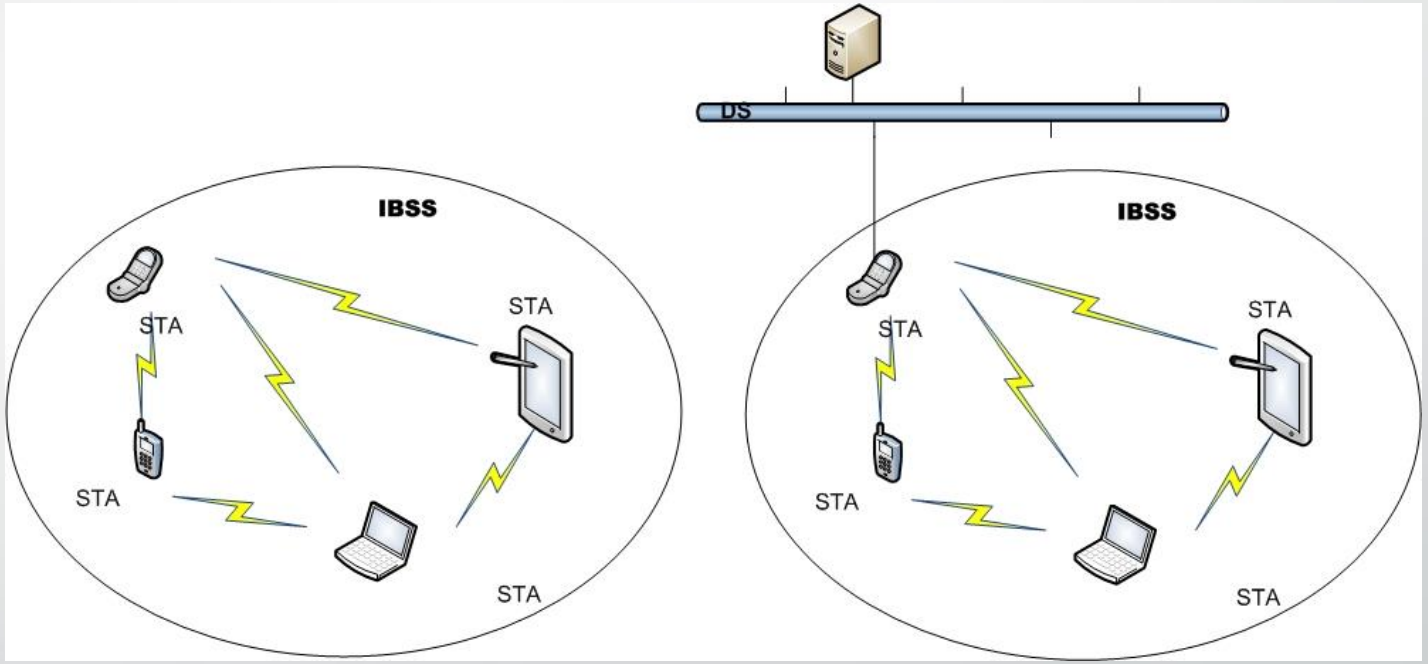
WLAN alapok - Építőelemek

- DS - Distributed system, az AP-k gerinchálózata
- STA – minden eszköz mely képes 802.11 hálózathoz csatlakozni
- AP – Egy eszköz mely egyaránt rendelkezik STA funkcionalitással valamint hidat képez a DS és az STA-k között
- BSS – Basic Service Set, Egy AP-ból és a hozzá tartozó STA-kból álló rendszer
- IBSS – Independent BSS, nem tartalmaz AP-t a STA-k önállóan alkotnak egy hálózatot
- ESS – Extended Service Set, Több BSS-ből álló rendszer
- SSID – (BSSID,ESSID) a hálózatok megkülönböztetésére szolgáló ID

WLAN alapok - topológiák



BSS



IBSS

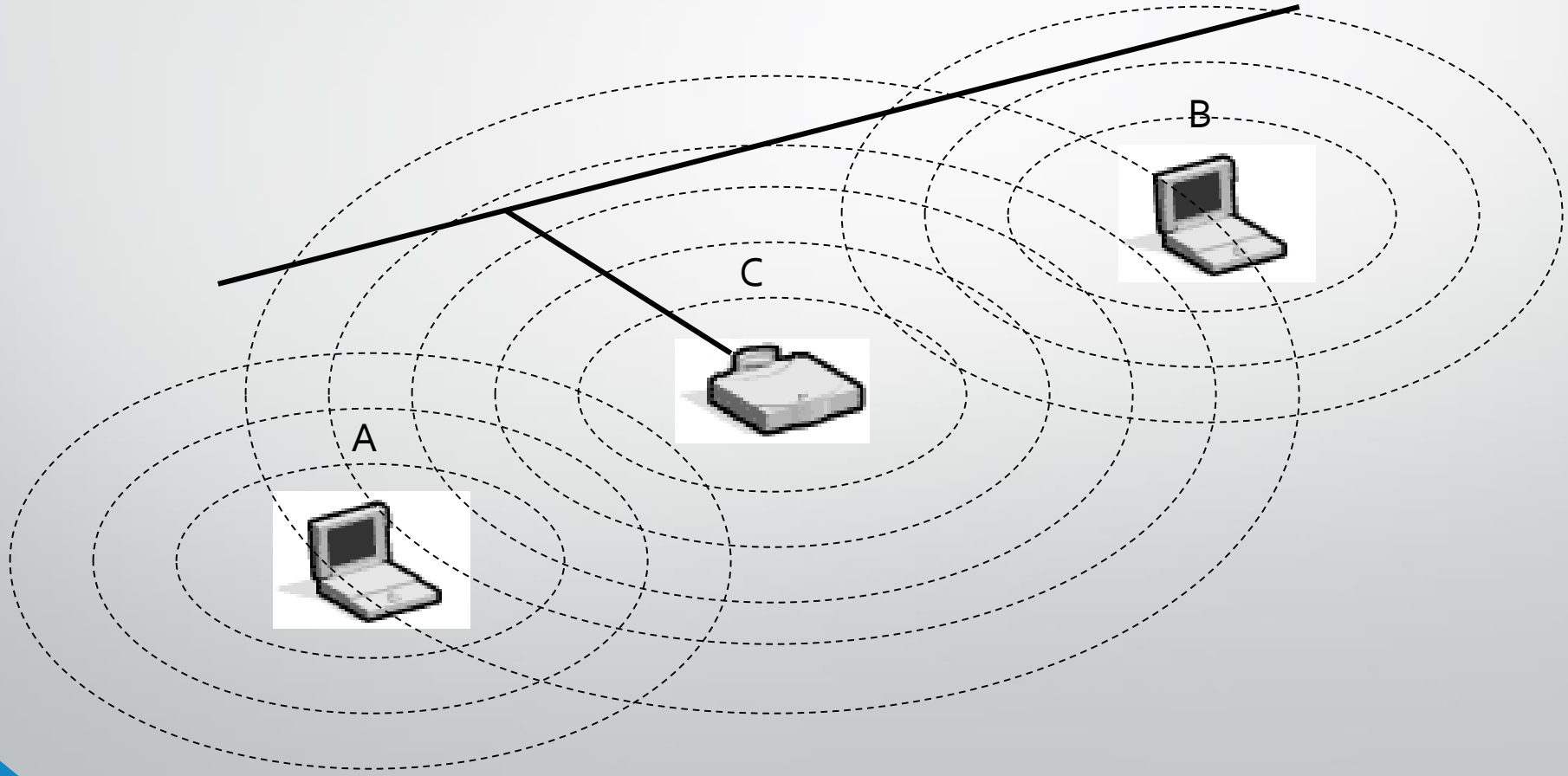
tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok - Közeghozzáférés

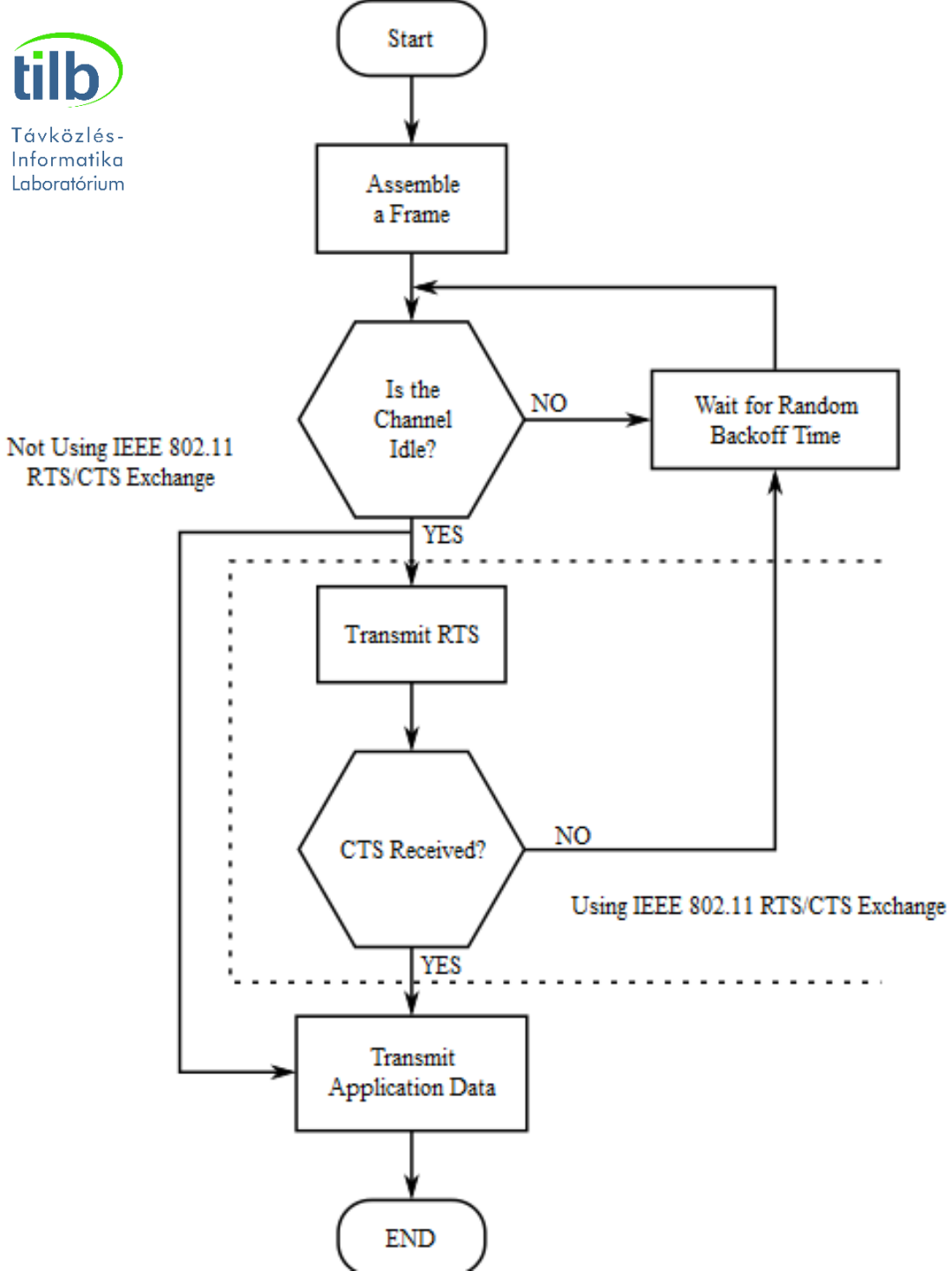
- Mivel a WLAN rendszer half duplex rendszer, így az állomások nem képesek párhuzamosan sem ütközésvizsgálatra sem annak eldöntésére, hogy az adat átjutott-e épségben, valamint a topológiák miatt nem biztos, hogy minden állomás látja egymást
- Az Ethernetben használt CSMA/CD nem használható, mivel az állomásnak engedélyt kell kapnia a közeghez ezért a CSMA/CA ütközés elkerülő közeghozzáférési protokollt használja

WLAN alapok –Rejtett Állomás probléma

- A,B nem látja egymást, mindkettő el kezd adni C-nek, ekkor C-nél ütközés lép fel

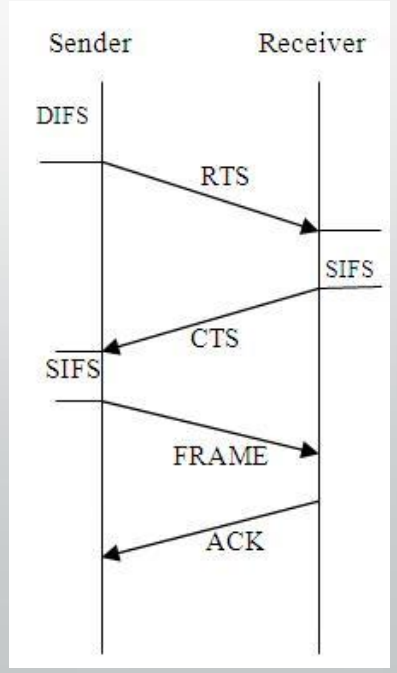


tilb
Távközlés-
Informatika
Laboratórium



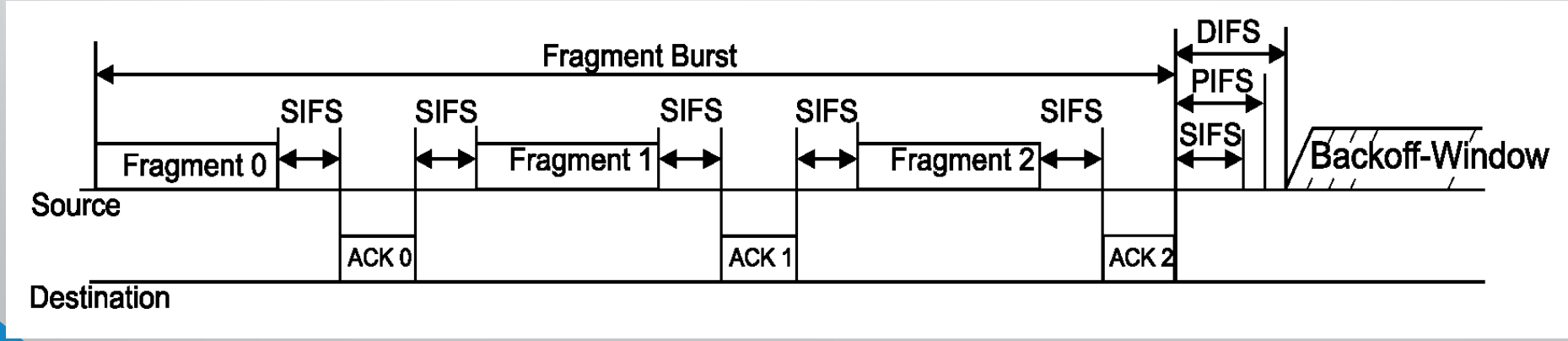
WLAN alapok – CSMA/CA

- Összerakjuk az elküldeni kívánt csomagot
- Megnézzük, hogy foglalt-e a csatorna
- Elküldjük a RTS (ReadyToSend) csomagot
- Várunk egy CTS (ClearToSend) csomagot
- Ha üres a csatorna küldöm.



WLAN alapok - Keret

- A LAN 1518 bájt hosszú keretéhez képest a WLAN-nál célszerűbb kisebb kereteket használni
  - Rádiós kapcsolat miatt minél hosszabb a keret annál nagyobb a hiba valószínűsége a BER miatt
  - FHSS miatt sokszor meg kellene szakítani az átvitelt
  - Kerethiba esetén kisebb keretet kell újraküldeni
  - Send-And Wait algoritmus, minden egyes töredék nyugtázva van



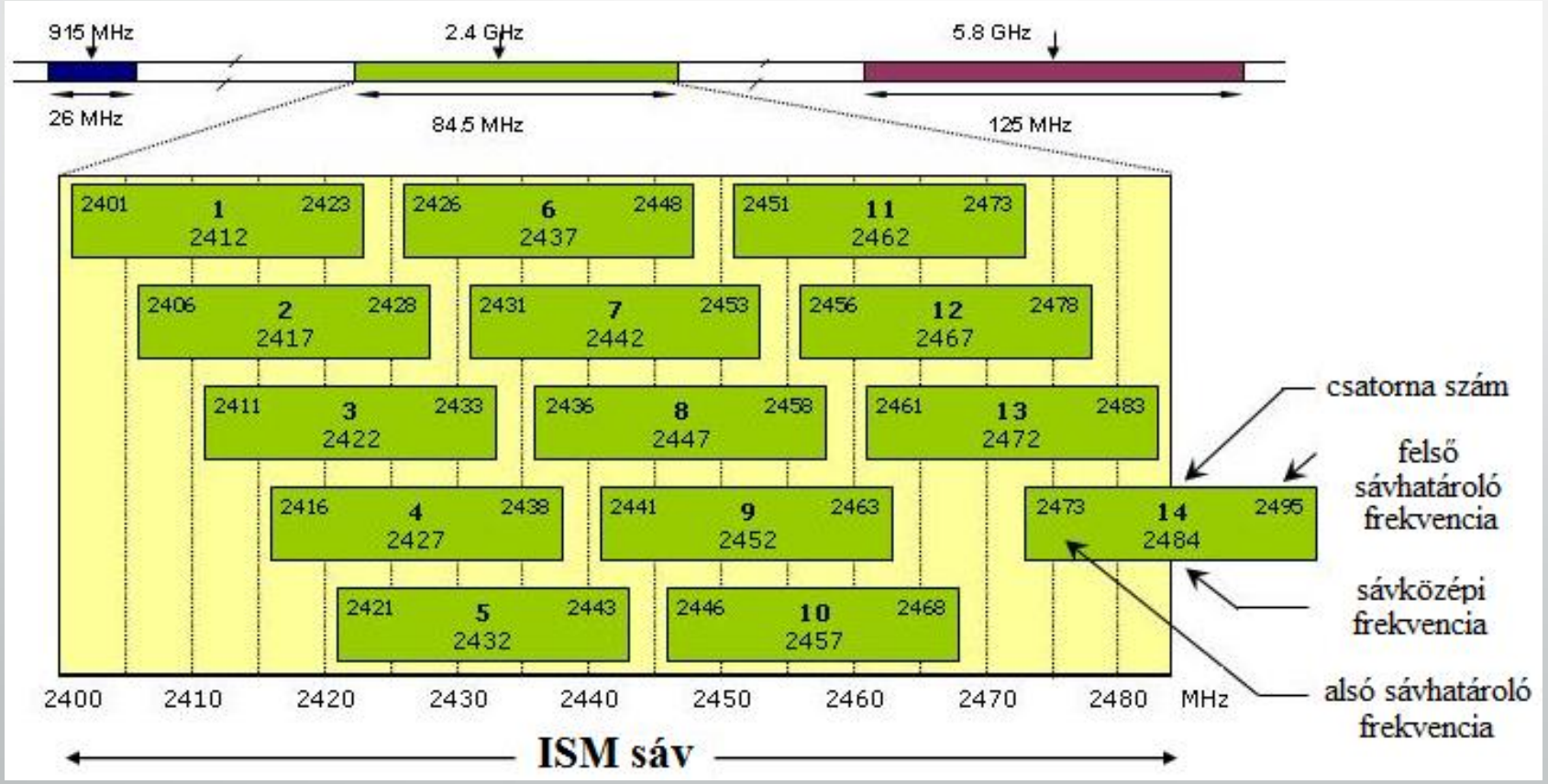
tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok – Cellaváltás/Roaming

- Egy 802.11 eszköz mozgás közben folyamatosan szkenneli az étert
- Ha tudja egy jobb kapcsolatra váltja le a meglévőt
- Cellaváltás – Handover a teljesítménycsökkenés szempontjából:
  - Soft Handover – csomagvesztés és teljesítmény csökkenés nélküli cellaváltás
  - Hard Handover – pont az ellentéte
- Beacon keret – az AP küldi, mely a szinkronizációt hivatott fenttartani, valamint a rendszerhez tartozó információkat tartalmazza (pl.: SSID)
  - Passzív handover – a kliens vár egy megfelelő BEACON-re majd átvált
  - Aktív handover – a kliens megpróbál egy Probe Request üzenettel új AP-t találni magának
- Roaming – ha a STA mozgás közben talál egy erősebb AP-t akkor oda újraasszociál

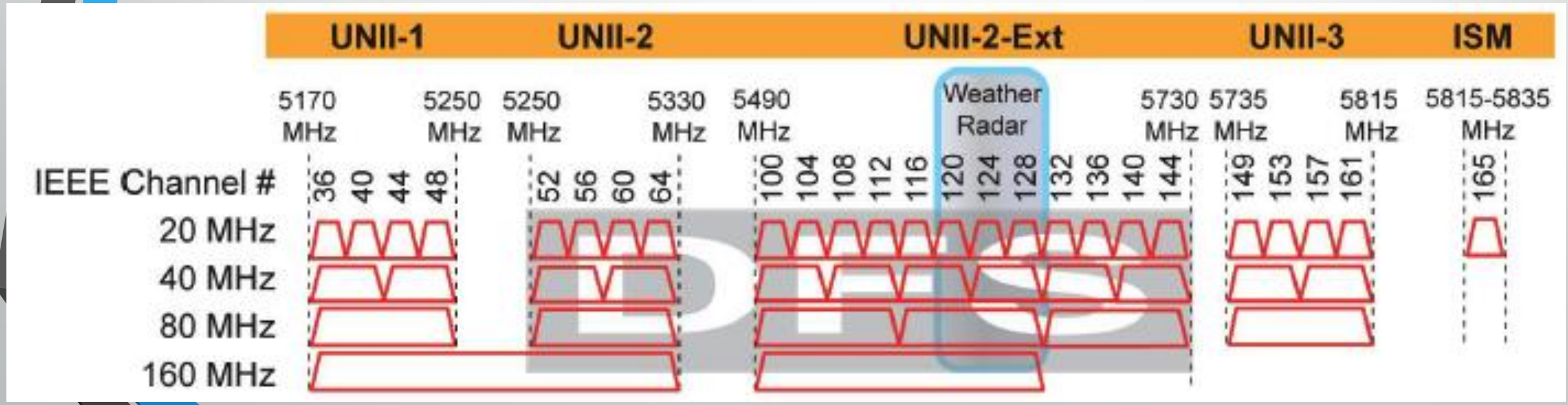
WLAN alapok – PHY

- A 802.11-re több frekvenciasáv is használható:
  - 2,4Ghz (2400MHz-2483,5MHz) ISM
  - 5,2GHz (5150MHz-5250MHz-5350MHz) UNII 1,2
  - 5,8GHz (5725MHz-5825MHz) UNII 2, Extended



WLAN alapok – PHY

- A 802.11-re több frekvenciasáv is használható:
  - 2,4Ghz (2400MHz-2483,5MHz) ISM
  - 5,2GHz (5150MHz-5250MHz-5350MHz) UNII 1,2 Extended
  - 5,8GHz (5725MHz-5825MHz) UNII 3

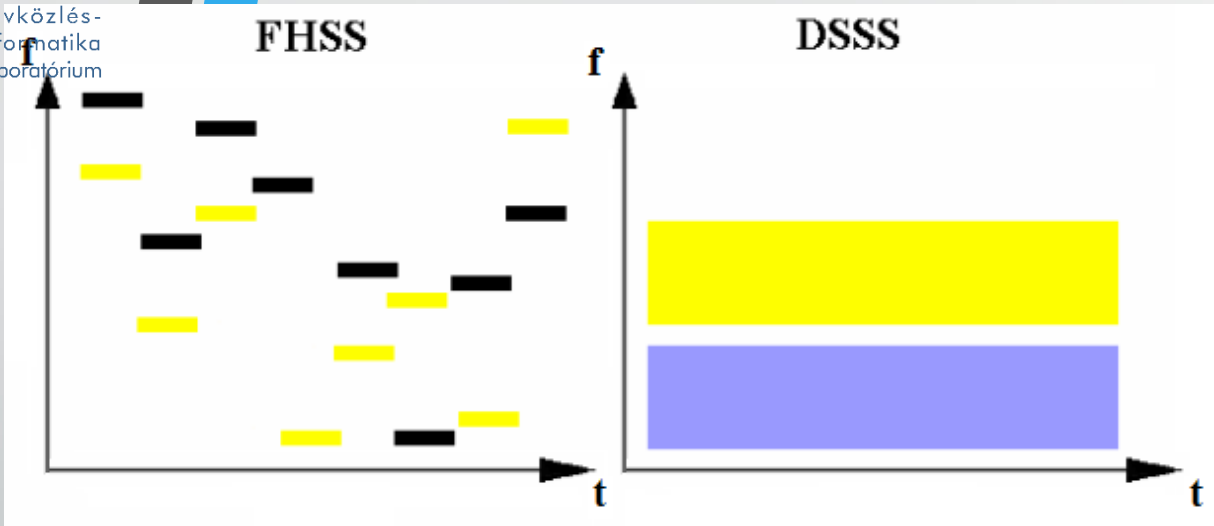


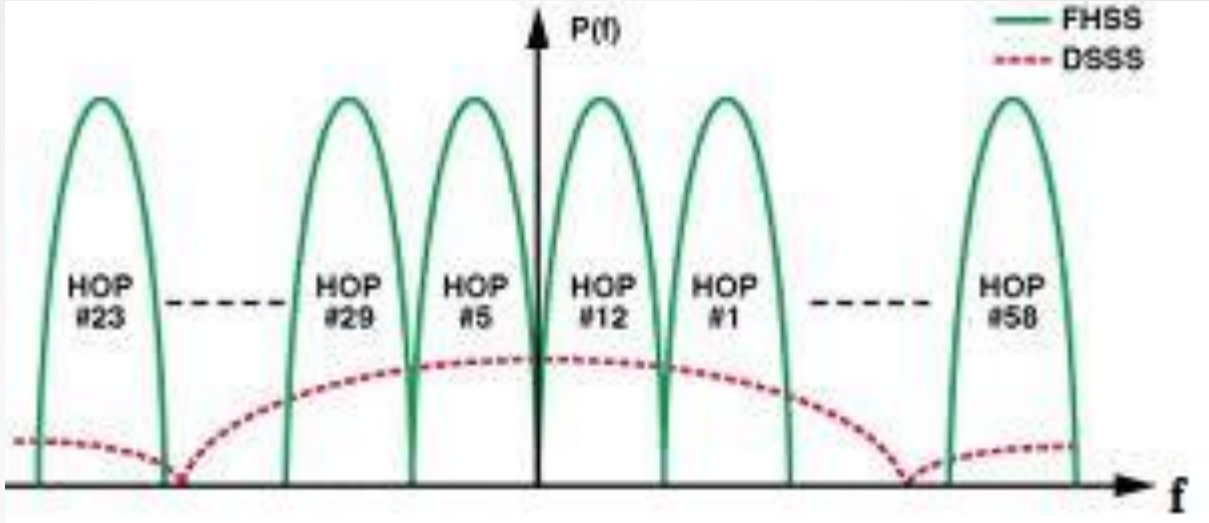
WLAN alapok – HUN

- Magyarországon a hatályban lévő üzemeltetési feltételek a rádióállomások (jelen esetben WLAN eszközök) számára a következők:

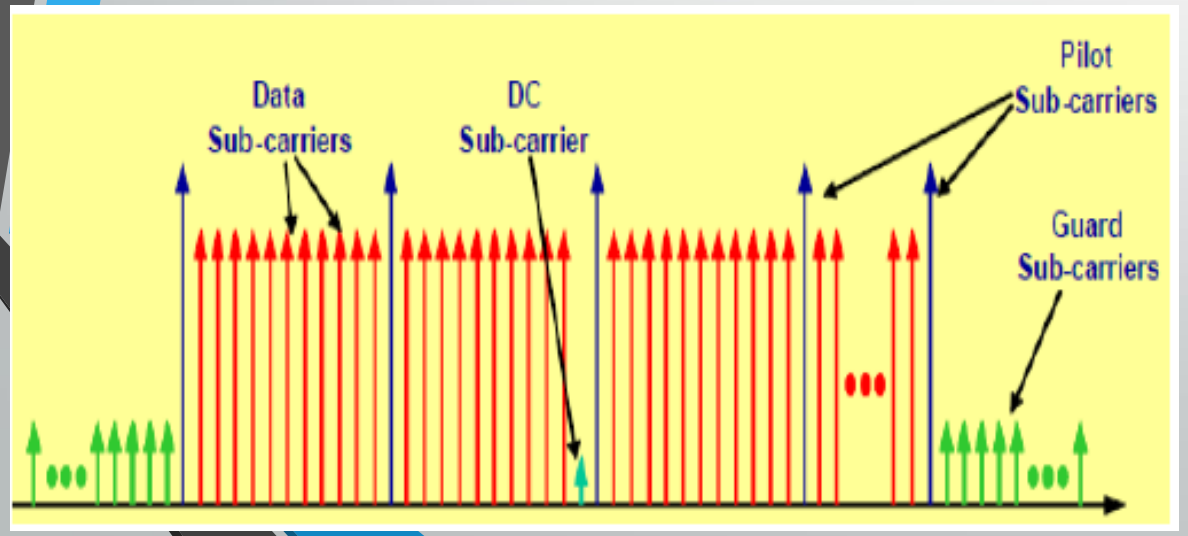
Sáv megnevezés	Frekvenciatartomány	Egyedi engedélyezés
2,4 GHz	2400 – 2483,5 MHz	mentes
3,5 GHz	3410 – 3494 / 3510 – 3594 MHz	köteles
5,2 GHz	5150 – 5350 MHz	mentes
5,6 GHz	5470 – 5725 MHz	mentes

WLAN alapok – RF Átvitel





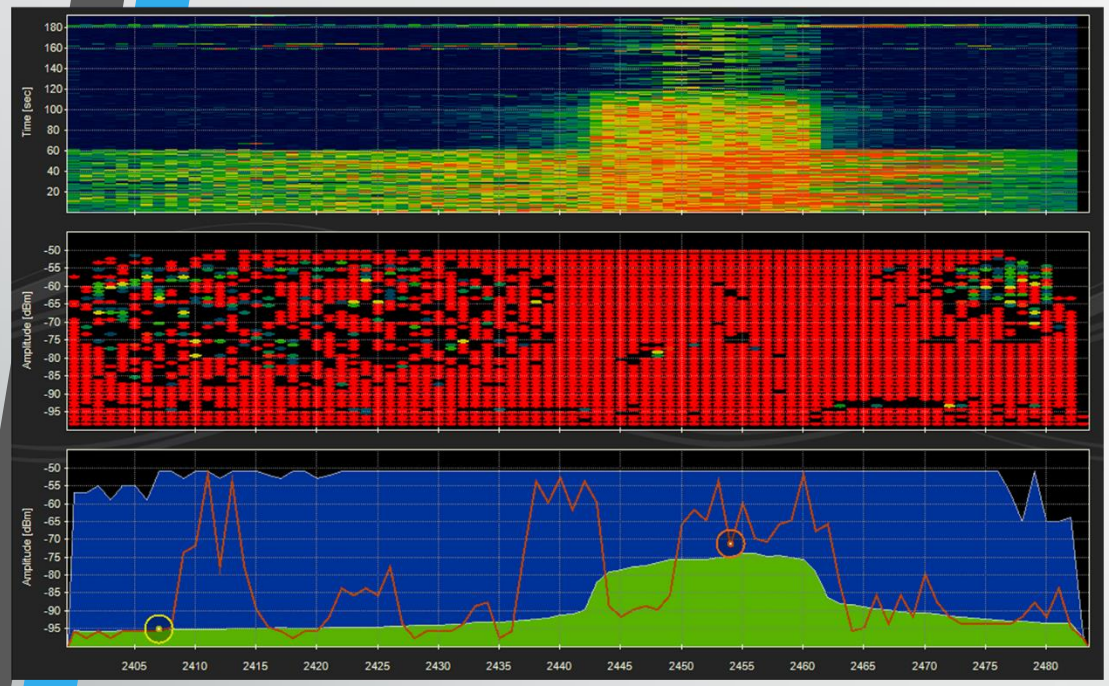
- FHSS – Freqvency Hopping Spread Spectrum
- DSSS – Direct Sequence Spread Spectrum



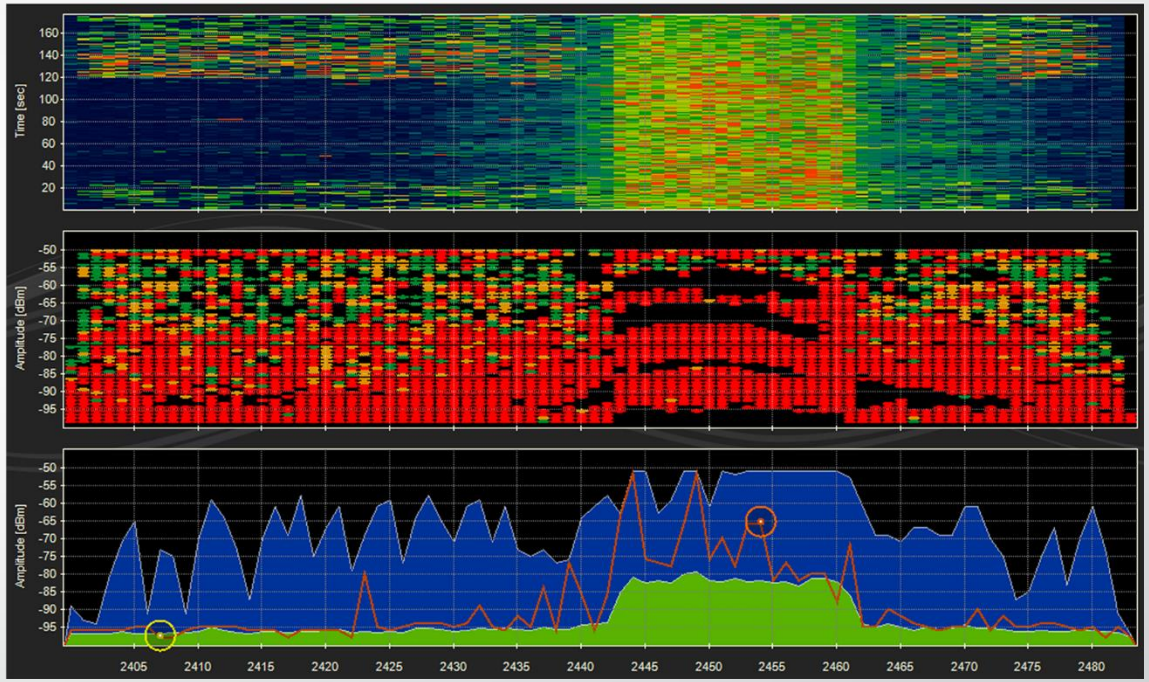
- Összehasonlítás
- OFDM - Orthogonal Frequency Division Multiplexing
- Az adatfolyamot több párhuzamos adatfolyamra osztják fel majd több vivőfrekvenciára felkeverve sugározzák ki

WLAN alapok – RF Átvitel

2,4 GHz



- Mikrosűtő



- Bluetooth

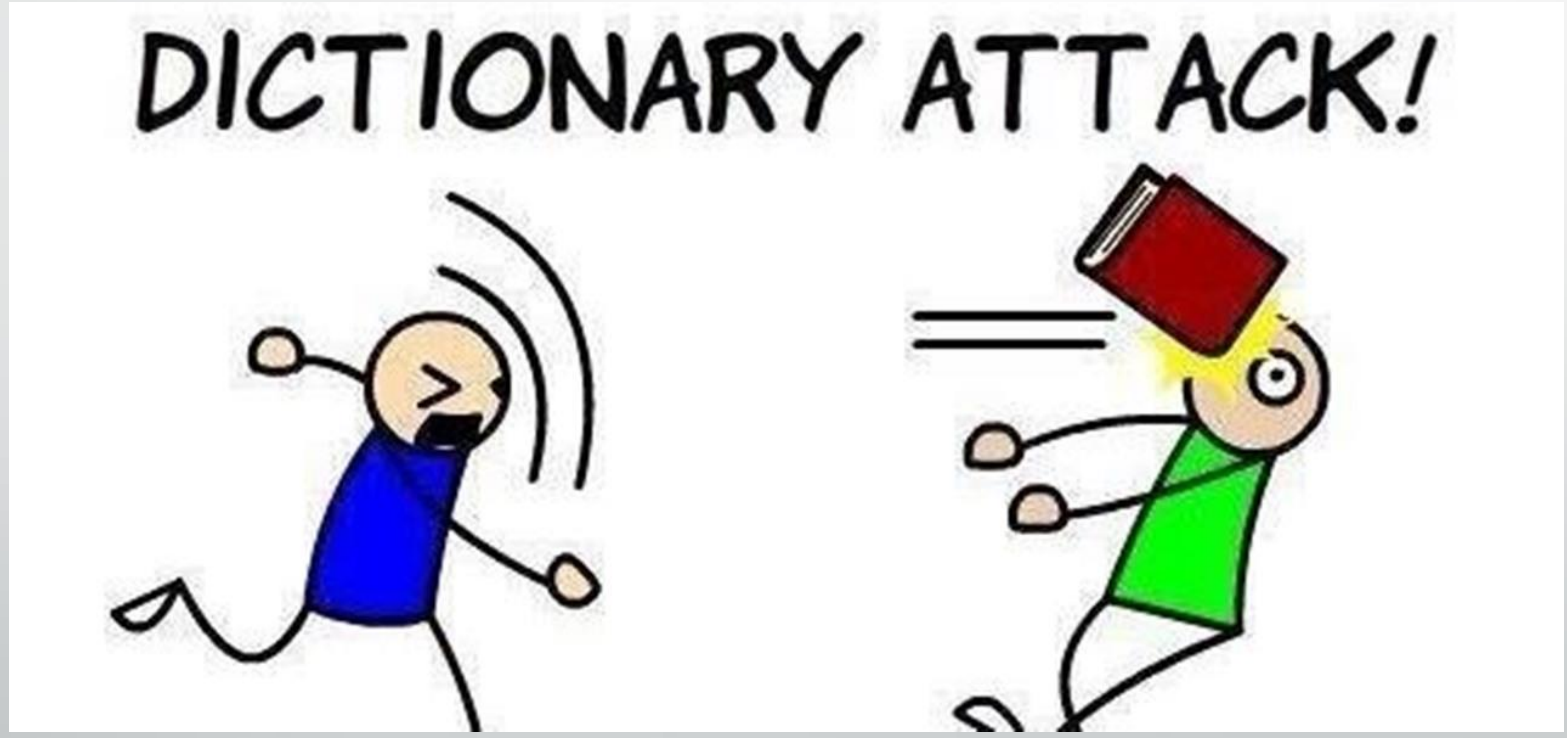
tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok – Kriptográfia/Autentikáció

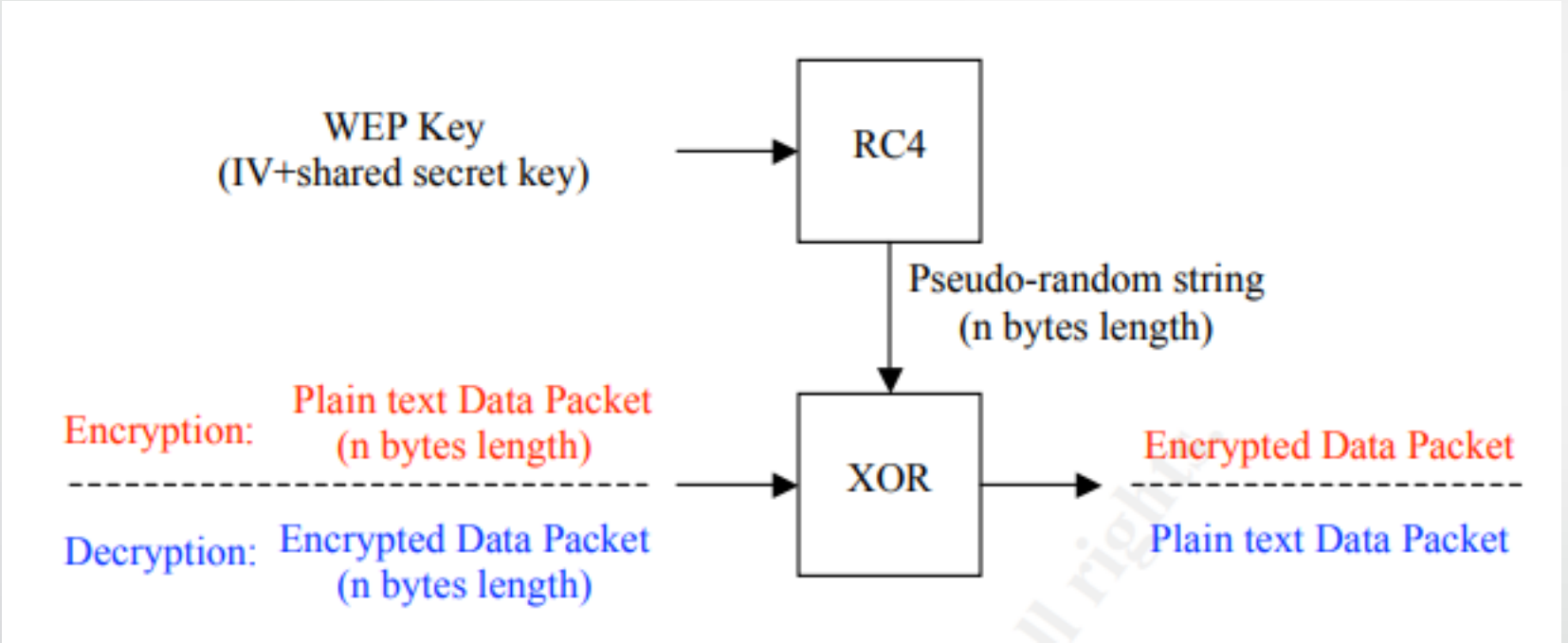
- A WLAN szegmensben 3 fő titkosítást használnak
  - Wired Equivalent Privacy (WEP)
  - Wi-Fi Protected Access (WPA)
  - Wi-Fi Protected Access 2 (WPA2)
  - Wi-Fi Protected Access 3 (WPA3)
- WEP - RC4 kódolót használ ami a mai napra már elavult (Deprecated) biztonsági rései miatt, könnyen visszafejthető a jelszó
- WPA – Bemutatkozik a TKIP (Temporary Key Integrity Protocol) Ezzel minden csomag egyedi titkosító kódot kap, így nehezebb volt feltörni, de a kompatibilitás megőrzése miatt ugyanúgy RC4 kódolót használ így ez is törhető, bár a egyedi kulcsok miatt sokkal nehezebb
- WPA2 – Az RC4-et lecserélték a sokkal biztonságosabb AES kódolóra.
- WPA3 – Az eddigi 128bites kulcsot 192-esre cserélik, a nyílt hálózatokon is lesz titkosítás, Brute-force elleni védelem

WLAN alapok – Kriptográfia/Autentikáció

- Bármilyen titkostást, kódolást használhatunk, ha gyenge a jelszó akkor a PSK törhető szótáras támadással.

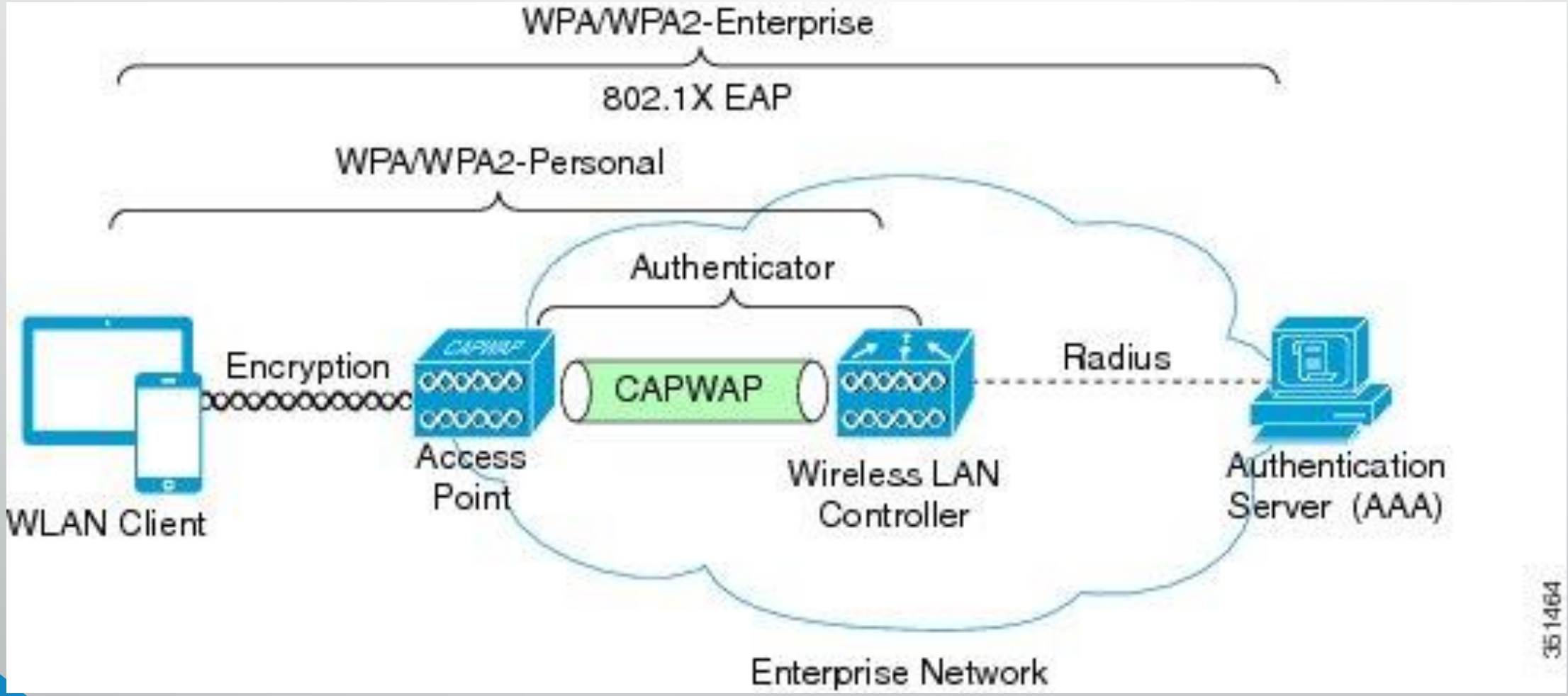


WLAN alapok – Kriptográfia/Autentikáció



- A WEP fő hibája az, hogy az RC4 kódóló pseudo-random algoritmusa nem megfelelő így a pseudo-random szám sokszor információkat tartalmazhat a tényleges WEP kulcsról

WLAN alapok – Kriptográfia/Autentikáció



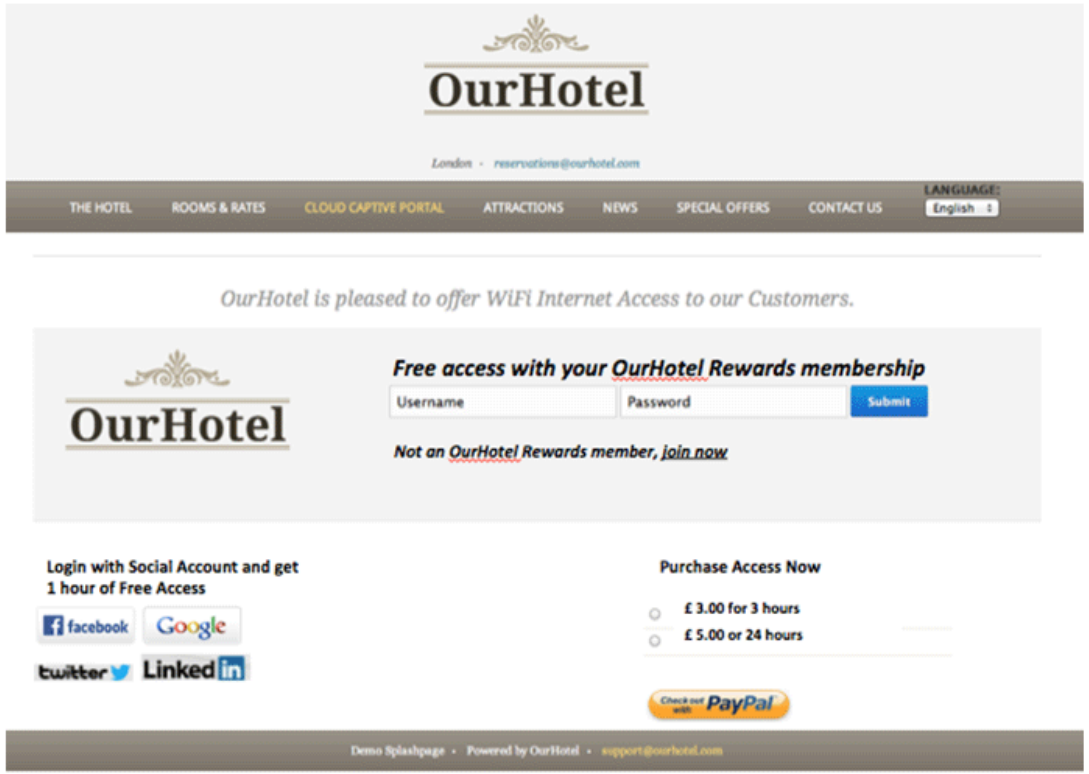
tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok – Captive Portal

- A Wireless hálózatok egyik elterjedt autentikációs metódusa
- Nem PSK, hanem minden user kap jelszót
- Alapvetően nyílt hálózat, bárki felcsatlakozhat DE:
- Csak akkor fér hozzá a hálózati erőforrásokhoz: DHCP, DNS internet elérés
- Ha autentikál egy megadott oldalon, általában erre az oldalra irányít át minden forgalmat amíg nem autentikál a user
- Itt van lehetőség a hálózati policy leírására és elfogadtatására
- Lehet adni mindenki számára elérhető guest hozzáférést

tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok – Captive Portal



WLAN alapok – Támadások típusai

- Mérgezett hot spot
  - Ezek nyílt hálózatnak tűnő, védelem nélküli Wi-Fi hozzáférési pontok. Tipikusan adatszerzés céljából üzemeltetett ál hot spotok.
- Plain Text
  - Alapja, hogy a vezeték nélküli médiumban közlekedő csomagok mindegyike hordoz egy kis részletet a kulcsból. Amennyiben elegendő ilyen mozaikdarabbal rendelkezik a támadó, képes azt teljes egészében rekonstruálni, egy összehasonlító mechanizmust használva (egy kiválasztott szövegrészt, a titkosított szöveghez hasonlítva próbálja kitalálni a kulcsot). Ez csak olyan esetben lehetséges, ha előzetesen, már ismert a titkosításhoz használt algoritmus, valamint egy titkosított adatrész.
- Rogue Access Point
  - Úgynevezett „kópé AP”. Tipikusan egy meglévő infrastrukturális hálózatban felállított, engedély- és védelem nélküli Access Point-ok, melyekhez bárki szabadon hozzáférhet, így a hálózat forgalmához is.

tilb
Távközlés-
Informatika
Laboratórium

WLAN alapok – Támadások típusai

- Közbeékelt támadás (Man-in-the-Middle)
  - A hozzáférési pont és a kliens állomás közé ékelődött AP, amely elhiteti a klienssel, hogy hozzá kívánt csatlakozni, valamint elhiteti az AP-vel, hogy ő a hitelesített kliens állomás. A támadó először passzívan figyel, begyűjti a hitelesítési információkat (AP által küldött hívó (challenge) és összerendelési üzeneteket (associate), kliens azonosítóját, IP-címeket), majd ezek birtokában kész megszemélyesíteni mind a klienst, mind az AP-t.
- Rejtett eszközök felderítése
  - A rejtett kapcsolódások megkerülésére szolgál. Ezáltal felfedhetővé válik az eszköz gyártója és típusa.
- War Driving
  - A nyílt, gyengén védett vezeték nélküli hálózatokat lokalizálja, mely során a hálózatokról begyűjtött információkat az Interneten mindenki számára elérhetővé teszik. Ehhez egy vezeték nélküli adapterrel szerelt mobil állomás, egy nagy nyereségű antenna és egy monitorozó szoftver szükséges. Gyakran GPS koordináták segítségével határozzák meg a sebezhető hálózatok pontos helyét.
- DoS (Denial of Service)
  - A széles körben elterjedt szolgáltatás megtagadás támadási technika.
- Nyerserő támadás (Brute Force)

WLAN alapok – 802.11 protokollcsalád

802.11 protokoll	Dátum	Frekvencia (GHz)	Sávszélesség (MHz)	Átviteli sebesség (Mbit/s)	MIMO	Moduláció	Távolság	
							Beltér	Kültér
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35 m	120 m
		3.7						5,000 m
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35 m	140 m
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38 m	140 m
n	Okt 2009	2.4/5	20	288.8-ig	4	MIMO-OFDM	70 m	250 m
			40	600-ig				
ac	Dec 2013	5	20	346.8-ig	8		35 m	
			40	800-ig				
			80	1733.2-ig				
			160	3466.8-ig				
		0.054-0.79	6-8	568.9-ig	4			
ad	Dec 2012	60	2,160	6,757 (6.7 Gbit/s)	N/A	OFDM	3.3 m	
ah	Dec 2016	0.9		347-ig				
ax	SEP 2019	2.4/5	20	1147	8	MIMO-OFDM	30 m	120 m [G]
			40	2294				
			80	4803				

tilb
Távközlés-
Informatika
Laboratórium

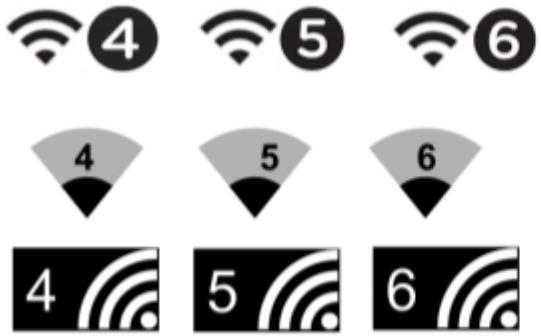
2018, a változás éve

- A Wi-Fi alliance belátja hogy átláthatatlan káosz a 802.11 szabványcsalád. A legtöbb ember max 2-3 technológiáról tud. (g,n,ac)
- Korábban is voltak már kísérletek:

802.11 Rollups								
802.11-2007	Mar 2007	2.4, 5		Up to 54		DSSS, OFDM		
802.11-2012	Mar 2012	2.4, 5		Up to 150[B]		DSSS, OFDM		
802.11-2016	Dec 2016	2.4, 5, 60		Up to 866.7 or 6,757[B]		DSSS, OFDM		

Átnevezések

- Sztenderdizált megnevezések 2018. október.
- Wi-Fi 4 – 802.11n
- Wi-Fi 5 – 802.11ac
- Wi-Fi 6 – 802.11ax



802.11ax, vagy WIFI6

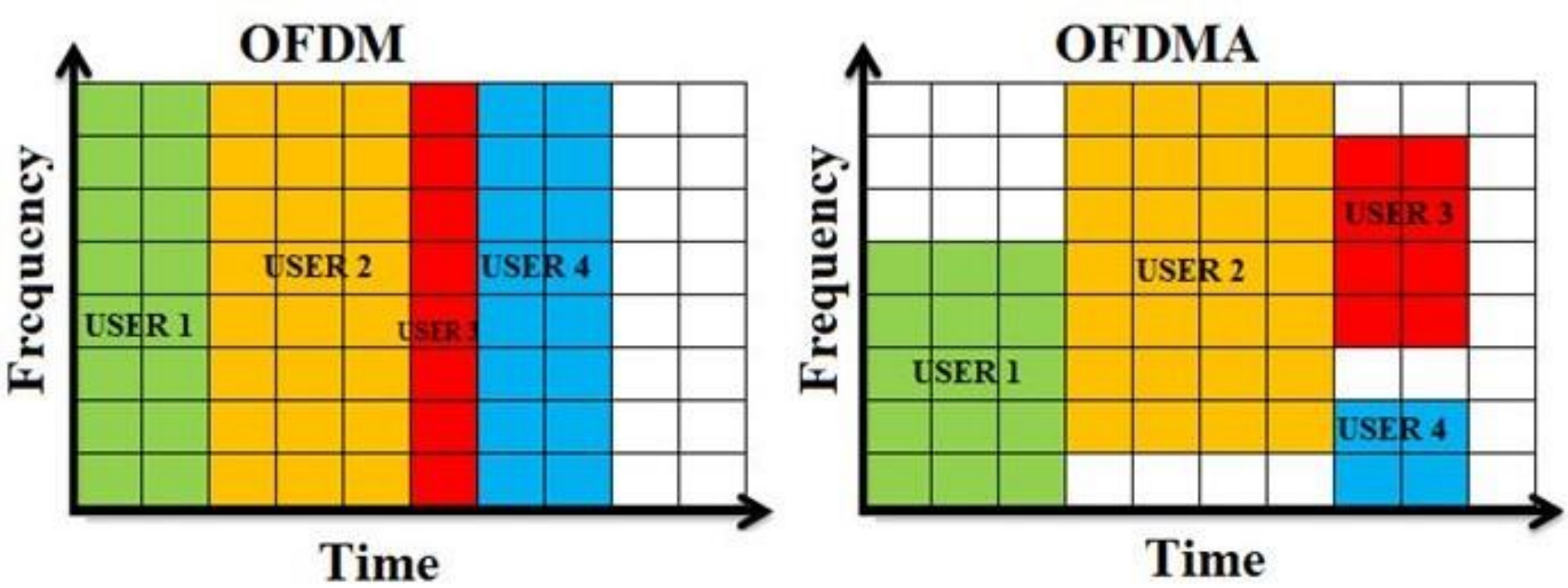
- 802.11ac, WIFI5 utódja

Szabvány	802.11ac	802.11ax
Frekvencia	5 GHz	2,4 és 5 GHz
Csatornák sávszélessége	20; 40; 80; 80+80 & 160 MHz	20; 40; 80; 80+80 & 160 MHz
FFT	64, 128, 256, 512 pontos	256, 512, 1024, 2048 pontos
Modulációs átviteli technika	OFDM	OFDMA
Alvivők modulációja	256-QAM	1024-QAM

Forrás: Filtermax Kft.

802.11ax, vagy WIFI6

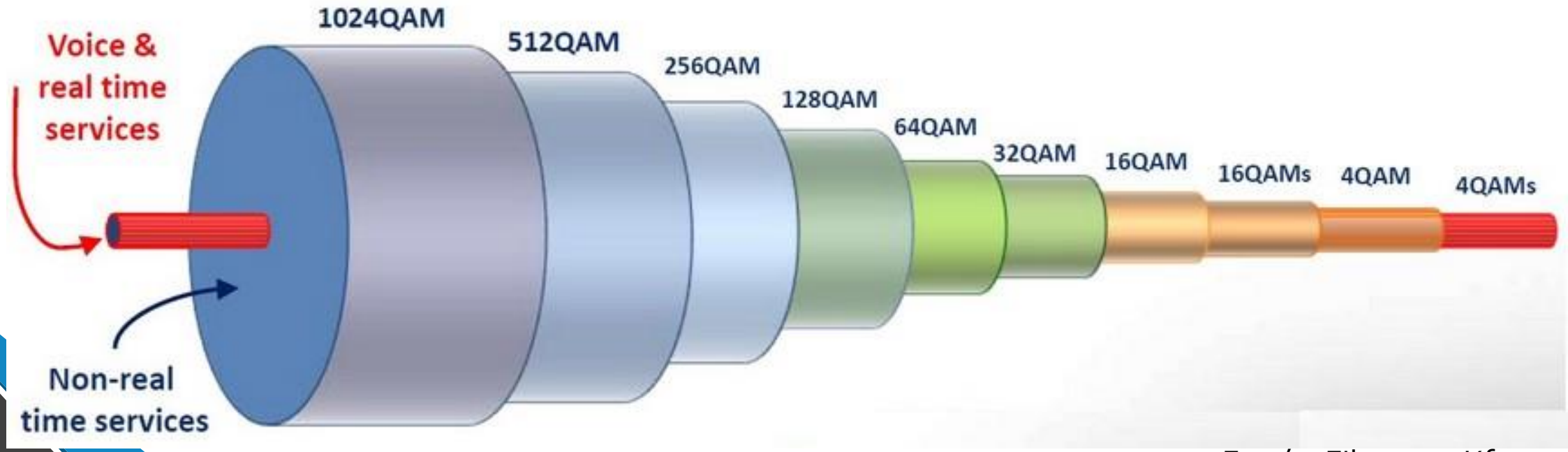
- **OFDMA vagy OFDM?**
  - Az OFDMA az OFDM többfelhasználós verziója. Az OFDM lényege abban áll, hogy az adatfolyamunkat több ezer alvivőre multiplexáljuk, így jóval ellenállóbb a különböző zavarok ellen. Az OFDMA pedig ebből a több ezer alvivőből képes hozzárendelni adott frekvenciatartományokat adott kliensekhez.



Forrás: Filtermax Kft.

802.11ax, vagy WIFI6

- A QAM moduláció lényege, hogy a jel fázis és amplitúdó helyzete hordozza az információt. Azzal, hogy 1024-QAM modulációval modulálják az egyes alvivőket 256-QAM helyett, egy adott amplitúdó és fázis állapot 32 bit információt jelent 8 bit helyett. Ezzel négyszeres elméleti átviteli sebesség érhető el az ac-vel szemben!



Forrás: Filtermax Kft.