

A vezeték nélküli adatátviteli és a WLAN

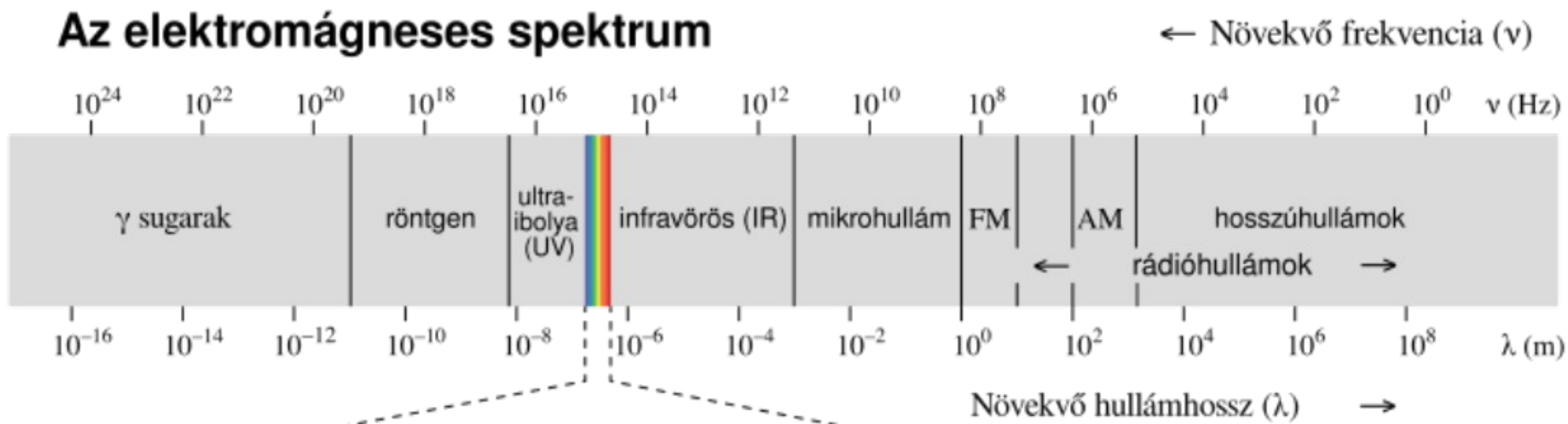
Számítógép-hálózatok

Kajdocsi László
A-602,
kajdocsi.laszlo@sze.hu

Adatátvitel jellemzői

- **Elektromágneses hullámok**
- **Gazdaságos**
- **Frekvenciafüggő terjedés**

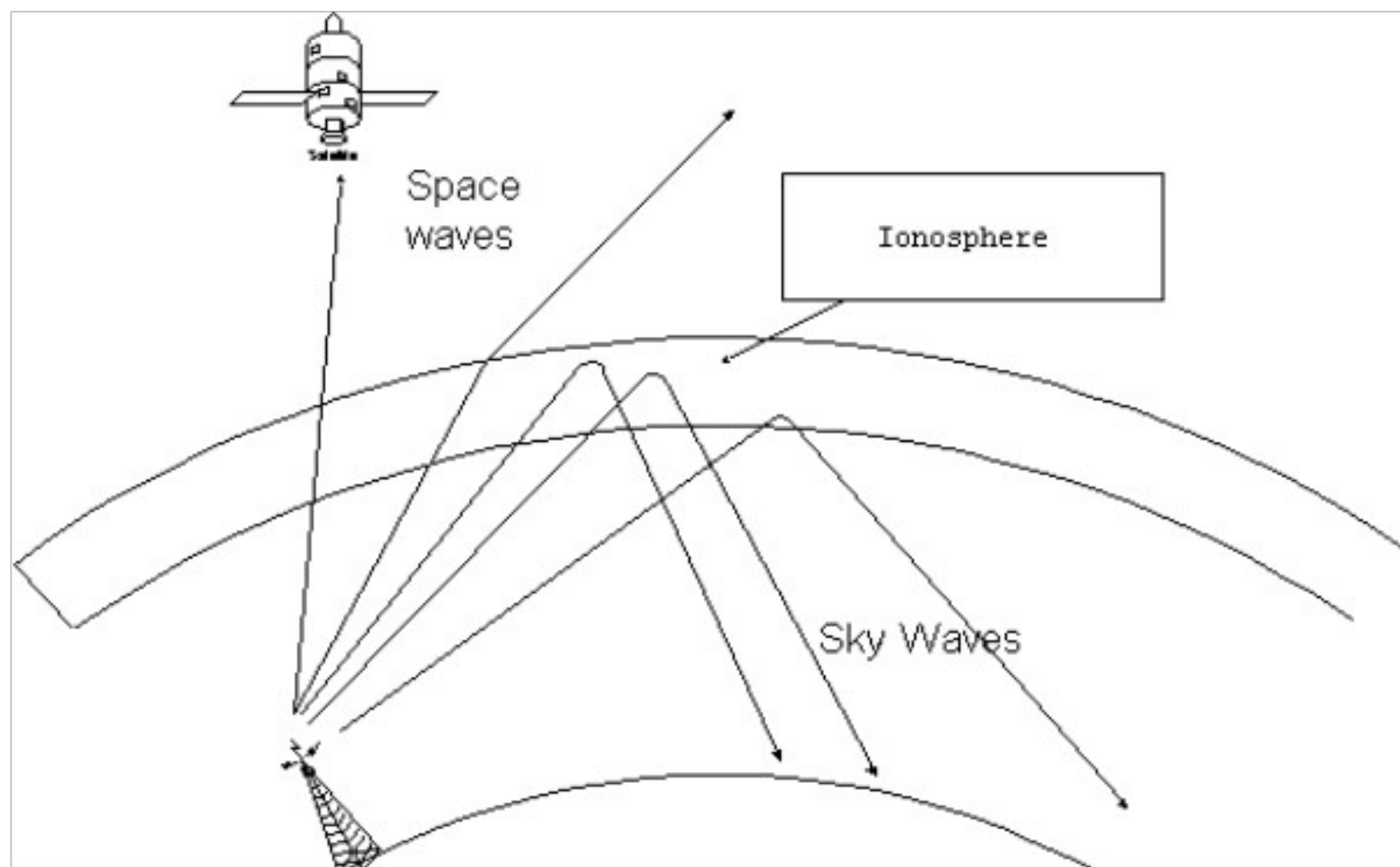
Az elektromágneses spektrum



Aspektrum tulajdonságai

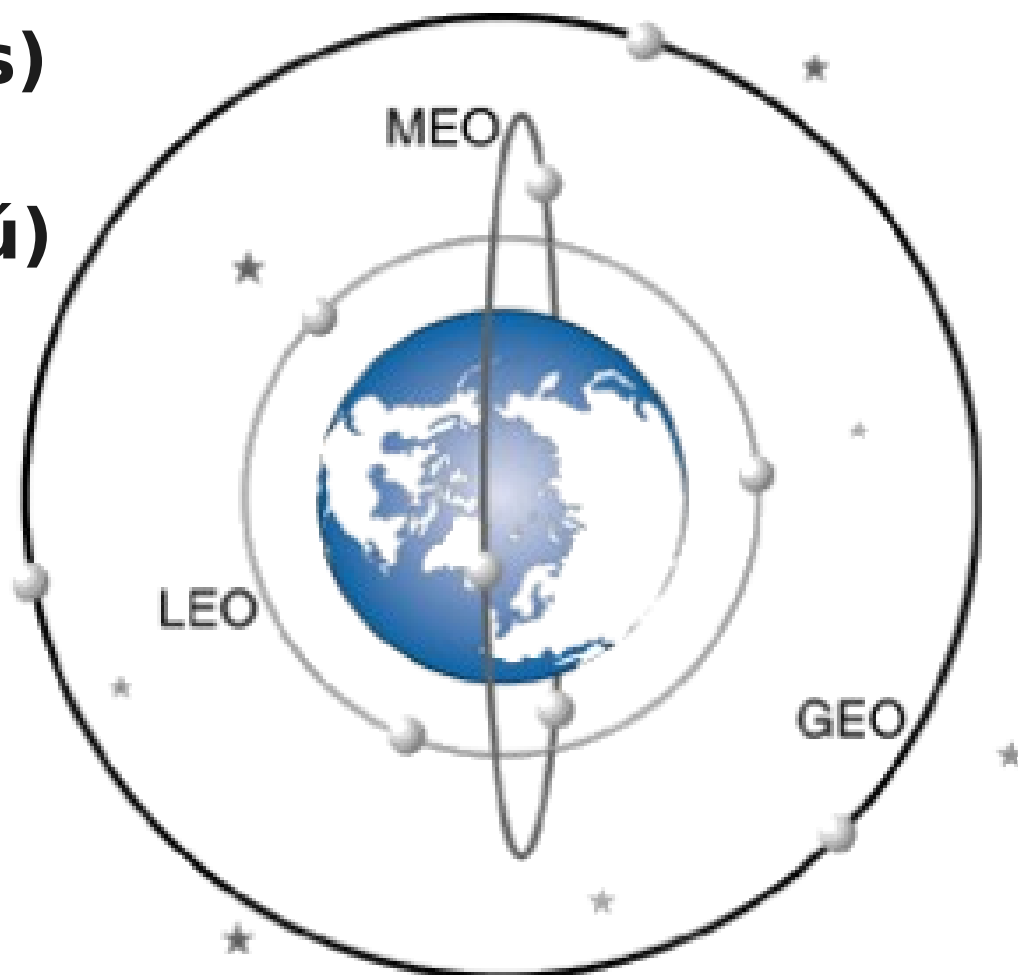
- **Az alacsonyabb frekvenciájú hullámok követik a Föld görbületét; könnyebben haladnak át szilárd testeken; visszaverődnek az ionoszféráról**
- **A magas frekvenciájú hullámok célirányosak; nehezebben hatolnak át szilárd testeken, de könnyedén áthatolnak az ionoszférán**
- **Fényhullámok nagyon korlátosak**

Egyes frekvenciák tulajdonsága



Kommunikációs műholdak

- **LEO (Alacsony röppályás)**
- **MEO (Közepes-távolságú)**
- **GEO (Geostacionárius)**



Navigációs műholdak

- A MEO pálya magasabb régiókban keringenek!
- A pálya minél közelebb van annál kisebb a jel futási ideje
- A légkör fékező hatása a közeli pályákon a legnagyobb, de még a legtávolabbi pályákon sem elhanyagolható!
- Ezek pl.:
 - GPS
 - GLONASS
 - GALILEO
 - COMPASS

Kommunikációs műholdak

- **A geostacionárius pályákon keringenek**
- **Együtt kering a Földdel, fix pontban**
- **Fix parabola antennával fogható**
- **Kb. 35.800km-re a tengerszint felett kering**
- **A vétel működik, az adás bonyolultabb!**

Műholdas távközlés

- **A gyakorlatban a távközlési műholdak nagy többsége gyakorlatilag adatszórást végez, főleg a Földről felsugárzott TV és Rádió műsorokat sugározzák vissza**
- **Jelentős a műholdak szerepe a telefonhálózatok összekapcsolásában is, de A közvetlen műholdas telefon polgári használatban nem jelenik meg a mindennapokban.**
- **Klasszikus számítógépes hálózat komponensként, például az internetes forgalom továbbításában részt vesznek műholdak, de polgári alkalmazásokban jellemzően főleg vételi irányban.**

Vezetéknélküli LAN-ok

- A vezeték nélküli hálózatokkal az IEEE 802.11 szabvány foglalkozik. (láttuk korábban)
- A szabványos vezeték nélküli hálózatok létrehozásának első lépése annak a frekvencia sávnak a megtalálása volt, ahol a szintén szabványos adóteljesítménnyel dolgozó kliensek sem egymást sem más elektronikus berendezéseket sem zavartak (túlságosan).
- Ezeket a frekvenciasávokat az ITU-R (International Telecommunication Union) az ISM sávban (Industrial, Scientific and Medical) sávban jelölte ki.

WLAN-ok tulajdonságai

- **Felépítését tekintve lehet „Ad-hoc” ahol a kliensek közvetlenül kommunikálnak egymással, vagy állhat bázisállomásokból (Access Point) melyek a kliensek közötti kapcsolatot biztosítják.**
- **Az IEEE 802.11 szabvány a „duplex” alapon adja meg a sáv szélességet.**
- **Egy WLAN eszköz csak Half-Duplex átvitelre képes.**

Wi-Fi

- **SSID (Service Set Identifier) – max. 32 karakter**
- **Rejtett SSID – biztonsági megfontolás**
- **Titkosítás módja – fontos ismeret**
- **IP kiosztás lehet dinamikus vagy statikus**
- **MAC cím alapú azonosítás (pl. korlátozás)**

Wi-Fi szabványok

IEEE szabvány	Megjelenés ideje	Működési frekvencia (GHz)	Sebesség (jellemző) (Mbit/s)	Sebesség (maximális) (Mbit/s)	Hatótávolság beltéren (méter)	Hatótávolság kültéren (méter)	Moduláció
Eredeti 802.11	1997	2,4	0,9	2	~20	~100	Frekvencia-ugrás
802.11a	1999	5	23	54	~35	~120	OFDM
802.11b	1999	2,4	4,3	11	~38	~140	DSSS
802.11g	2003	2,4	19	54 (108 SuperG)	~38	~140	OFMD
802.11n	2009	2,4 / 5	74	300, 450, 600	~70	~250	MIMO, OFMD
802.11ac	2012	5	200	6930	~50	~5000	multi user MIMO, 256-QAM

Titkosítás - WEP

- **Első wireless titkosítási szabvány**
- **Létezik 64, 128, 256, vagy 512 bites változat**
- **Legelterjedtebb a 64 és a 128 bites WEP**
- **Viszonylag könnyen feltörhető (Publikus adatok szerint egy 64 bites kulcsot 25.000, míg egy 128 bites kulcsot 100.000 csomaggal már nagy valószínűséggel fel lehet törni.)**

Titkosítás - WPA

- 2003 óta létező titkosítási szabvány
- A WPA a TKIP-et (Temporal Key Integrity Protocol/Időszakos Kulcs Sérthetetlenségi Protokoll) használja az adatok titkosítására, ami egy RC4 alapú titkosító algoritmus
- Időnként, vagy adatmennyiségként új kulcsot generál
- Elég biztonságos

Titkosítás - WPA2

- 2006-ban jelent meg, és szinte azonnal ki is szorította az első generációs WPA-t.
- A TKIP mellett az AES (Advanced Encryption Standard/Fejlett titkosítási Szabvány) titkosítást is támogatja.
- Biztonságosabb mint elődje
- Kellően erős jelszó használata alap követelmény minden titkosítás mellett

A WPA és WPA2 további tulajdonságai

- Képesek hitelesítési szolgáltatást nyújtó szerverrel (pl. **RADIUS** – Remote Authentication Dial-In User Service) is együttműködni **EAP** (Extensible Authentication Protocol) hitelesítési eljárással, vagy akár **PSK** (Pre Shared Key) üzemmódban is.
- Az osztott kulcs módot azon otthoni és kirodai felhasználóknak fejlesztették ki, akik nem tudnak megengedni (pl. az ára és a bonyolultsága miatt) egy dedikált 802.1X kiszolgálót.

Titkosítás - WPS

- **QSS (Quick Security Settings) vagy WPS (Wi-Fi Protected Setup) feliratú gomb**
- **Mindkettő lehetőség egy kényelmi funkció az eszközeink gyors csatlakoztatására**
- **A gomb megnyomása után a kapcsolódást kérő eszközön megjelenő párbeszédablakba be kell írni azt általában 8 számjegyből álló a PIN-kód kódot, ami az Access Point adattábláján szerepel, vagy amit az Access Point esetileg generált.**

Titkosítás - további érdekesség

- Egyes Access Point (illetve WLAN Router) gyártók eszközeinek beállításakor 802.11n üzemmód beállítása esetén is választható a WEP titkosítás, miközben a 802.11n szabvány leírásában a WEP már nem szerepel.
- Ez a gyakorlatban annyit jelent, hogy 802.11n mellett WEP titkosítást beállítva az adott eszköz vagy 802.11b/g módban fog működni, vagy egyáltalán nem fog működni.

THE END

Köszönöm a figyelmet!