KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Sieťová a komunikačná bezpečnosť

03 Bezpečnosť bezdrôtových sietí a prenosu

KCKB UPJS CSIRT UPJS

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezpečnosť bezdrôtových sietí a prenosu

- WLAN siete
- autentifikačné mechanizmy pre WDS
- prenosy údajov cez mobilné siete (GSM, LTE)

Bezdrôtový prenos

- Bezdrôtové siete sú zraniteľnejšie ako káblové kvôli verejnému prenosovému médiu
- Hlavné bezpečnostné požiadavky: dôvernosť, integrita, dostupnosť, autenticita
- Bezdrôtové signály prenikajú cez steny a obmedzujú fyzickú kontrolu prístupu
- Štandard IEEE 802.11 (Wi-Fi) je najrozšírenejší bezdrôtový standard
- WDS (Wireless Distribution System)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

IEEE štandard 802.11

- 1997 802.11 Legacy, 2.4 GHz, viacero kanálov
- 1999 802.11a, +5 GHz, max. 54 Mbit/s
- 2009 802.11n (WIFI 4), max. 600 Mbit/s, MIMO
- 2013 802.11ac (WIFI 5), max. 6933 Mbit/s
- 2021 802.11ax (WIFI 6), max. 9608 Mbit/s, WIFI 6E pridalo 6 GHz
- 2024 802.11be (WIFI 7), max. 23059 Mbit-s

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

IEEE štandard 802.11

- CSMA/CA [carrier sense multiple access with collision avoidance]
- zmena oproti káblovému /CD [collision detection]:
  - koncové zariadenia nefungujú vo full-duplex režime
  - problém skrytého uzla (hidden station problem) – dve zariadenia pripojené k rovnakému AP nemusia byť navzájom viditeľné a teda nemôžu detegovať kolíziu
  - zoslabenie signálu (signal fading) – vzdialenosť, odrazy od stien, rušenie, pohyby
- fyzická modulácia
  - FHSS (Frequency-hopping spread spectrum)
  - DSSS (Direct-sequence spread spectrum)
  - OFDM (Orthogonal frequency-division multiplexing)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bezdrôtový prenos

- Ad Hoc network
  - priame bezdrôtové spojenie medzi zariadeniami
- Access point
  - tento prístupový bod štandardne prepája káblové a bezdrôtové siete

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Rámce bezdrôtového prenosu

- Manažment
  - naviazanie spojenia medzi stanicou a prístupovým bodom
  - Beacon (pravidelné zasielanie SSID), Probe Request, Probe Response
- Kontrola
  prístup ku kanálu a potvrdzovanie
  - RTS (Request to send)
  - CTS (Clear to send)
  - ACK (Acknowledgment)
- Dáta
  - údaje

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Rámce bezdrôtového prenosu

- Adresovanie
  - 2-4 MAC adresy
  - bity ToDS, FromDS určujúce použitie prístupového bodu na oboch koncoch

- Zachytávanie rámcov
  - karta musí byť v monitorovacom režime

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Autentifikačné mechanizmy pre WDS

- 1997 Wired Equivalent Privacy (WEP)
  - RC4
- 2003 Wi-Fi Protected Access (WPA)
  - RC4+TKIP (Temporal Key Integrity Protocol)
- 2004 Wi-Fi Protected Access II (WPA2)
  - AES-CCMP (128 bit)
  - PSK / 802.1X Enterprise
- 2018 Wi-Fi Protected Access III (WPA3)
  - AES-GCM (192 bit)
  - SAE (Simultaneous Authentication of Equals), Forward secrecy

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Útoky

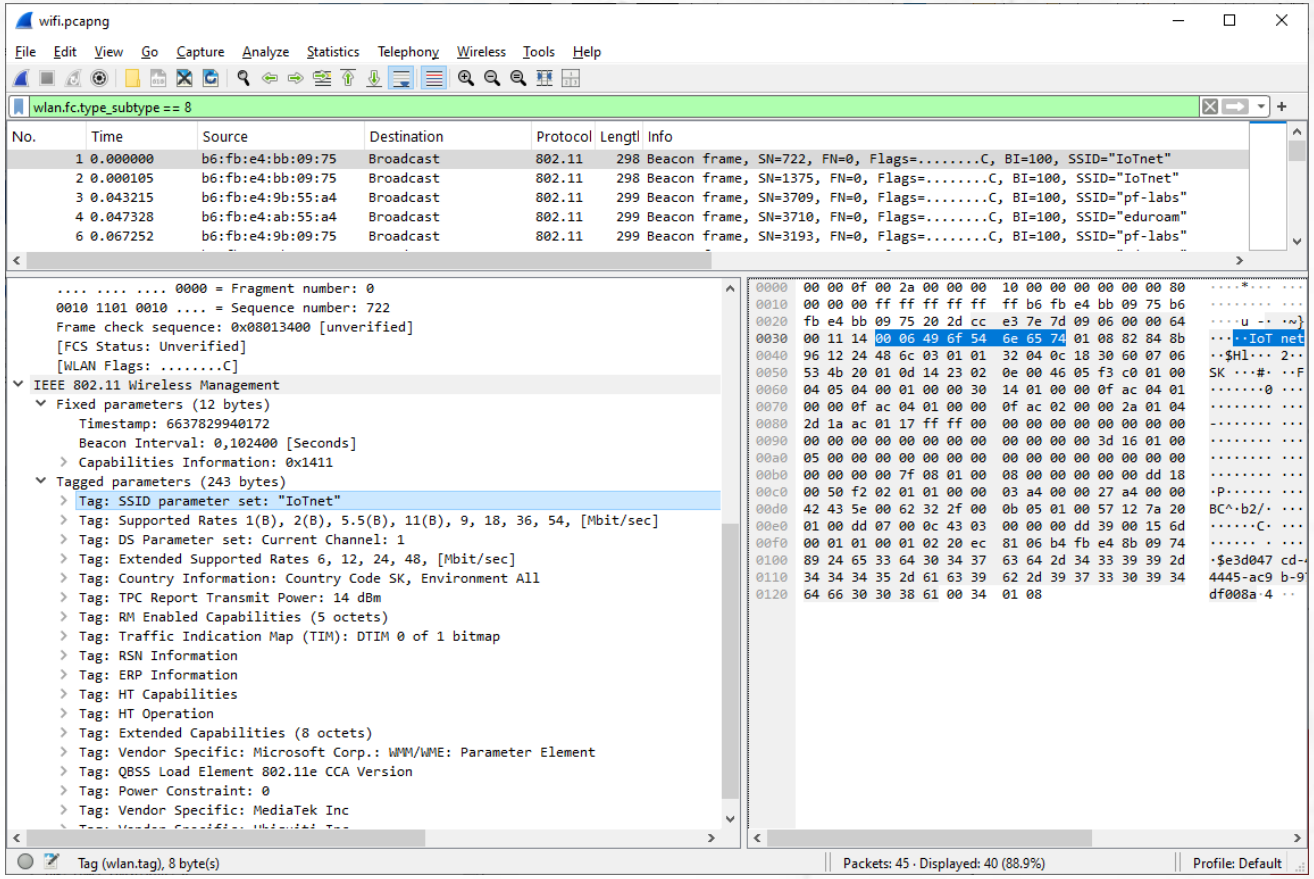
- **Evil Twin**
  - útočník vytvorí falošný prístupový bod s rovnakým SSID ako legitímna site
  - silnejší signál, aby sieť prilákala používateľov
  - útočník odpočúva alebo manipuluje všetku komunikáciu
  - časté vo verejných priestoroch: kaviarne, (železničné/autobusové) stanice, hotely

- **Man-in-the-Middle (MITM)**
  - ARP/DNS spoofing, falošná WIFI
  - odpočúvanie aj modifikácia dát v reálnom čase

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

rámce Beacon

wlan.fc.
type_subtype
== 8



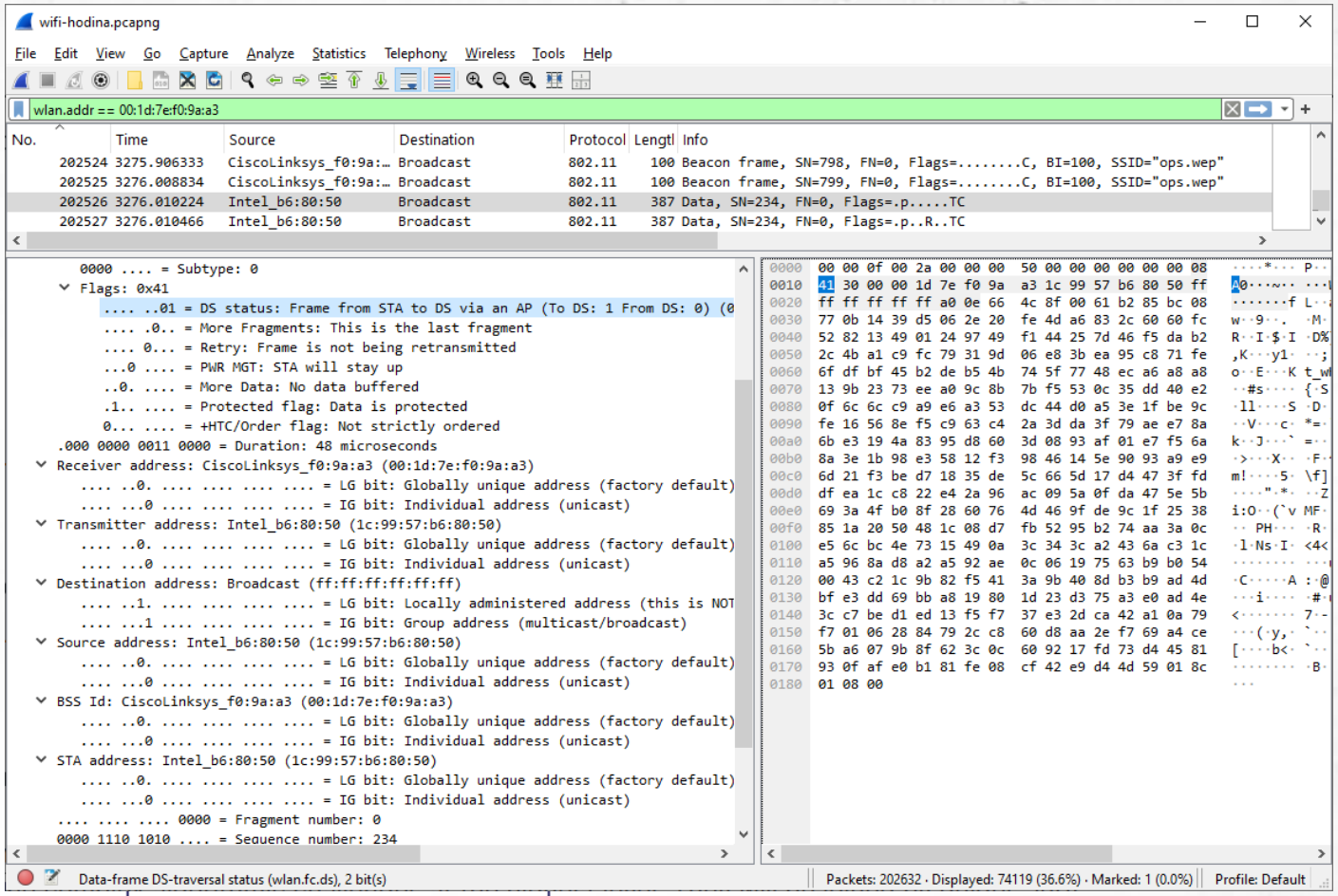
Informácie o sieti:

- SSID
- podporované rýchlosti
- krajina (dostupné kanály, výkon)

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

rámce

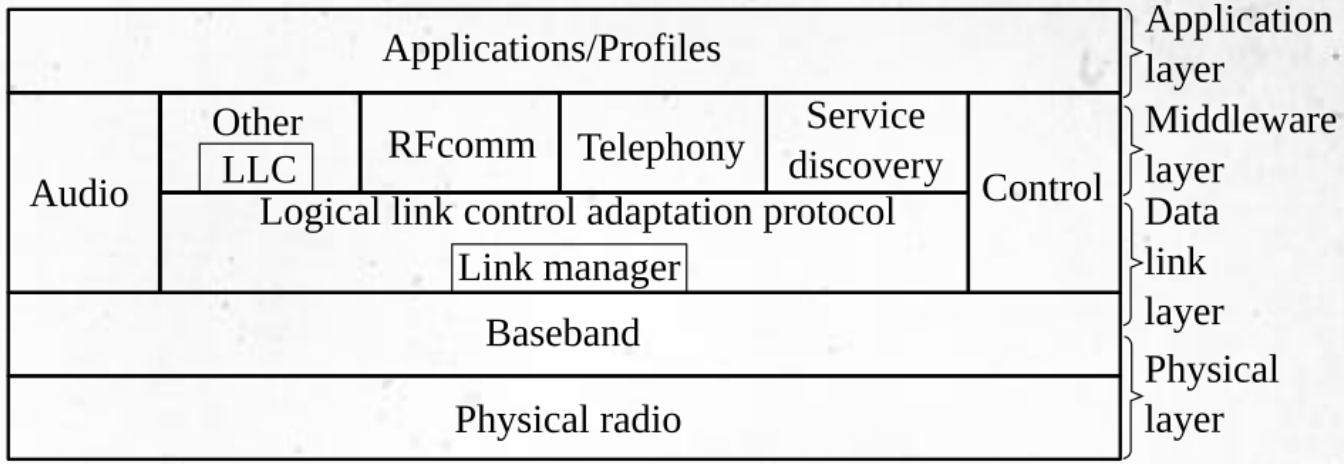
- DS status (From/To)
- adresy



Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Bluetooth

- piconet
  - Ad hoc network
  - 8 stations – primary+secondaries, additional parked stations
  - one-to-one/many



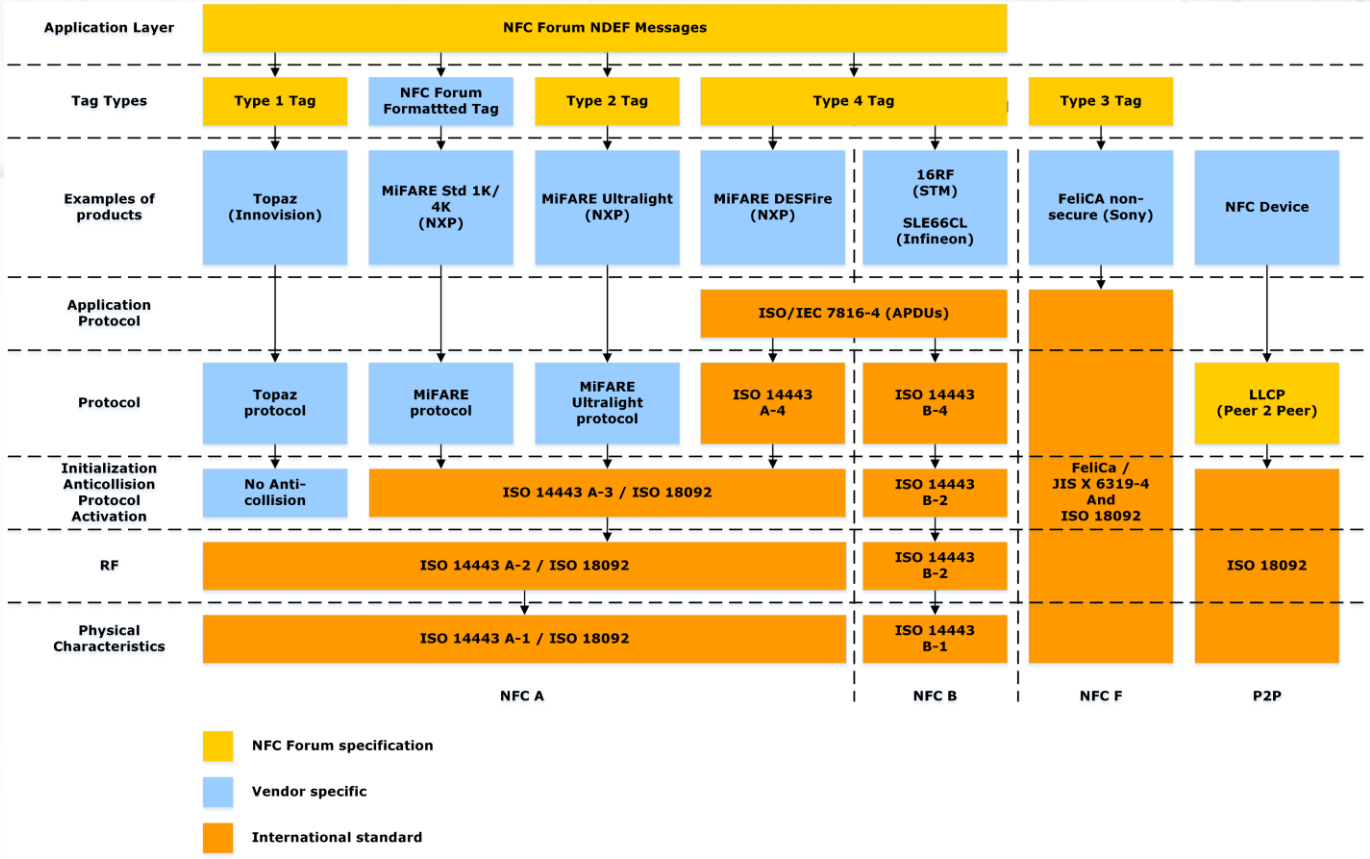
https://upload.wikimedia.org/wikipedia/commons/9/9f/Bluetooth_protokoly.svg

- scatternet
  - secondary funguje ako primary v ďalšom piconet-e
- 2.4 GHz, 1 Mbit/s (v1.2-2003) – 2.1 Mbit/s (v6.0-2024)
- LowEnergy: 1 Mbit/s (v4.0-2009) – 3.0 Mbit/s (v6.0-2024)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

NFC (Near-field communication)

- 1983 RFID (radio-frequency identification technology)
- 13.56 MHz 106-848 Kbit/s
- pasívne/aktívne zariadenie
- kódovanie Manchester, Modified Miller



https://upload.wikimedia.org/wikipedia/commons/3/33/NFC_Protocol_Stack.png

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

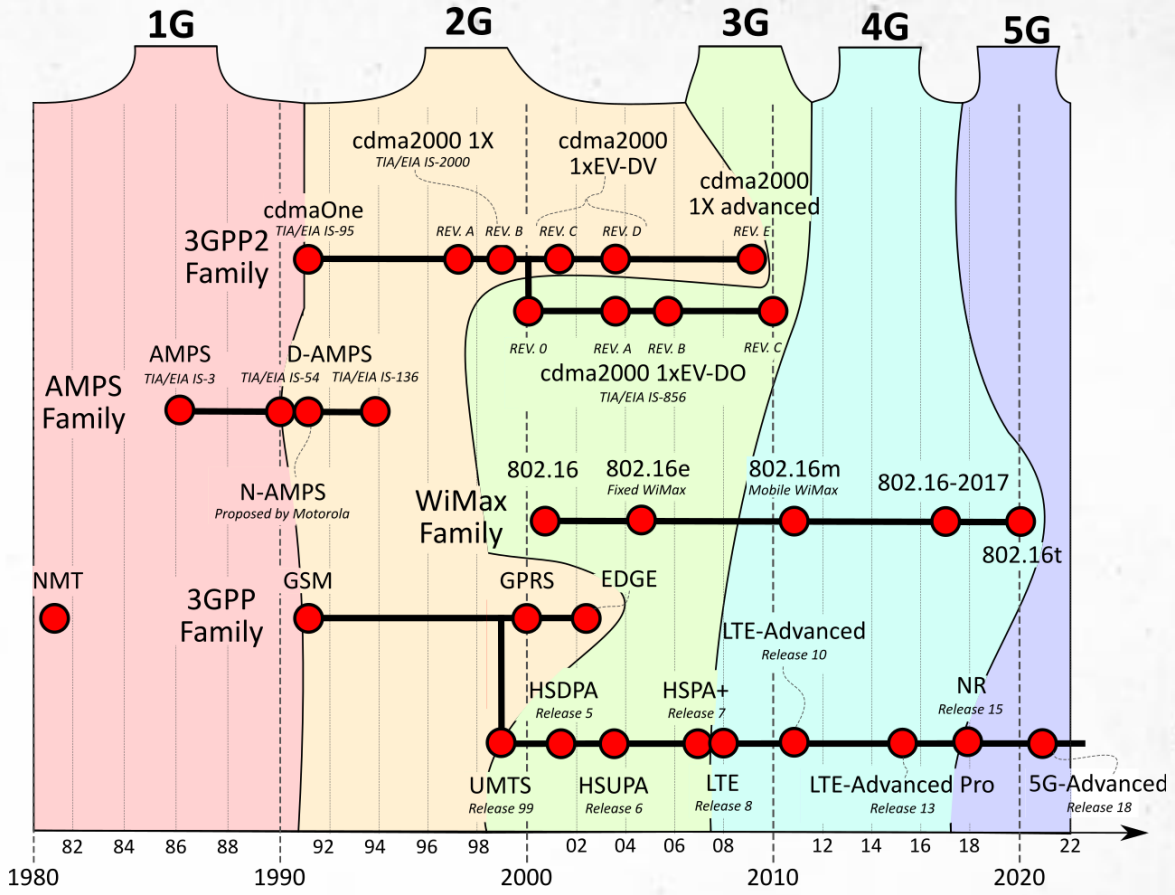
Mobilné siete

- 1G (1980) – analog (NMT v Európe), 824-894 MHz (800-MHz band)
- 2G (1990) – digital, 890-960 MHz
  - Global System for Mobile Communication,
  - GPRS/EDGE 400 Kbit/s
- 3G (1999) – zvuk + dáta, v Európe 900/1800 MHz, UMTS/WCDMA 28 Mbit/s
- 3.5G – HSPA/HSPA+, 42 Mbit/s
- 4G (2008) – LTE (Long Term Evolution), download 1 Gbit/s, upload 500 Mbit/s
- 5G (2019) – NR (New Radio), download 20 Gbit/s, upload 10 Gbit/s

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Mobilné siete

- Štandardy pre mobilné siete



https://upload.wikimedia.org/wikipedia/commons/4/4a/Cellular_network_standards_and_generation_timeline.svg

Financované Európskou úniou
NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Satelitné siete

- **Low Earth Orbit (LEO):**
  - 200 – 2.000 km (nad povrchom Zeme)
  - Starlink
- **Medium Earth Orbit (MEO):**
  - 8.000 – 20.000 km
  - GPS
- **Geostationary Orbit (GEO):**
  - 35.786 km
  - TV

- 1,5 – 30 GHz

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujeme za pozornosť