



# Sieťová a komunikačná bezpečnosť

## 03 Bezpečnosť bezdrôtových sietí a prenosu



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 štandard
- WDS (Wireless Distribution System)



PLÁN [OBNOVY]





# 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





# 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)





# Bezdrôtový prenos

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



**PLÁN [OBNOVY]**





# 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



PLÁN [OBNOVY]





# 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



**PLÁN [OBNOVY]**





# 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





# 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





# rámce Beacon

wlan.fc.  
type\_subtype  
== 8

## Informácie o sieti:

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	b6:fb:e4:bb:09:75	Broadcast	802.11	298	Beacon frame, SN=722, FN=0, Flags=.....C, BI=100, SSID="IoTnet"
2	0.000105	b6:fb:e4:bb:09:75	Broadcast	802.11	298	Beacon frame, SN=1375, FN=0, Flags=.....C, BI=100, SSID="IoTnet"
3	0.043215	b6:fb:e4:9b:55:a4	Broadcast	802.11	299	Beacon frame, SN=3709, FN=0, Flags=.....C, BI=100, SSID="pf-labs"
4	0.047328	b6:fb:e4:ab:55:a4	Broadcast	802.11	299	Beacon frame, SN=3710, FN=0, Flags=.....C, BI=100, SSID="eduroam"
6	0.067252	b6:fb:e4:9b:09:75	Broadcast	802.11	299	Beacon frame, SN=3193, FN=0, Flags=.....C, BI=100, SSID="pf-labs"

..... 0000 = Fragment number: 0  
0010 1101 0010 .... = Sequence number: 722  
Frame check sequence: 0x08013400 [unverified]  
[FCS Status: Unverified]  
[WLAN Flags: .....C]  
IEEE 802.11 Wireless Management  
 Fixed parameters (12 bytes)  
 Timestamp: 6637829940172  
 Beacon Interval: 0,102400 [Seconds]  
 Capabilities Information: 0x1411  
 Tagged parameters (243 bytes)  
 Tag: SSID parameter set: "IoTnet"  
 Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]  
 Tag: DS Parameter set: Current Channel: 1  
 Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]  
 Tag: Country Information: Country Code SK, Environment All  
 Tag: TPC Report Transmit Power: 14 dBm  
 Tag: RM Enabled Capabilities (5 octets)  
 Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap  
 Tag: RSN Information  
 Tag: ERP Information  
 Tag: HT Capabilities  
 Tag: HT Operation  
 Tag: Extended Capabilities (8 octets)  
 Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element  
 Tag: QoS Load Element 802.11e CCA Version  
 Tag: Power Constraint: 0  
 Tag: Vendor Specific: MediaTek Inc



# rámce

- DS status (From/To)
- adresy

wifi-hodina.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.addr == 00:1d:7e:f0:9a:a3

No.	Time	Source	Destination	Protocol	Length	Info
202524	3275.906333	CiscoLinksys_f0:9a:...	Broadcast	802.11	100	Beacon frame, SN=798, FN=0, Flags=.....C, BI=100, SSID="ops.wep"
202525	3276.008834	CiscoLinksys_f0:9a:...	Broadcast	802.11	100	Beacon frame, SN=799, FN=0, Flags=.....C, BI=100, SSID="ops.wep"
202526	3276.010224	Intel_b6:80:50	Broadcast	802.11	387	Data, SN=234, FN=0, Flags=.p....TC
202527	3276.010466	Intel_b6:80:50	Broadcast	802.11	387	Data, SN=234, FN=0, Flags=.p..R..TC

0000 .... = Subtype: 0

Flags: 0x41

- ....01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0)
- ....0.. = More Fragments: This is the last fragment
- ....0... = Retry: Frame is not being retransmitted
- ...0..... = PWR MGT: STA will stay up
- ..0..... = More Data: No data buffered
- .1..... = Protected flag: Data is protected
- 0..... = +HTC/Order flag: Not strictly ordered

0000 0000 0011 0000 = Duration: 48 microseconds

Receiver address: CiscoLinksys\_f0:9a:a3 (00:1d:7e:f0:9a:a3)

- ....0..... = LG bit: Globally unique address (factory default)
- ....0..... = IG bit: Individual address (unicast)

Transmitter address: Intel\_b6:80:50 (1c:99:57:b6:80:50)

- ....0..... = LG bit: Globally unique address (factory default)
- ....0..... = IG bit: Individual address (unicast)

Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

- ....1..... = LG bit: Locally administered address (this is NOT)
- ....1..... = IG bit: Group address (multicast/broadcast)

Source address: Intel\_b6:80:50 (1c:99:57:b6:80:50)

- ....0..... = LG bit: Globally unique address (factory default)
- ....0..... = IG bit: Individual address (unicast)

BSS Id: CiscoLinksys\_f0:9a:a3 (00:1d:7e:f0:9a:a3)

- ....0..... = LG bit: Globally unique address (factory default)
- ....0..... = IG bit: Individual address (unicast)

STA address: Intel\_b6:80:50 (1c:99:57:b6:80:50)

- ....0..... = LG bit: Globally unique address (factory default)
- ....0..... = IG bit: Individual address (unicast)

0000..... = Fragment number: 0

0000 1110 1010 .... = Sequence number: 234

0000 00 0f 00 2a 00 00 00 50 00 00 00 00 00 08 ..... P..

0010 41 30 00 00 1d 7e f0 9a a3 1c 99 57 b6 80 50 ff A0..... P..

0020 ff ff ff ff ff a0 0e 66 4c 8f 00 61 b2 85 bc 08 ..... f L..

0030 77 0b 14 39 d5 06 2e 20 fe 4d a6 83 2c 60 60 fc w..9... .M-

0040 52 82 13 49 01 24 97 49 f1 44 25 7d 46 f5 da b2 R..I.\$ I D%

0050 2c 4b a1 c9 fc 79 31 9d 06 e8 3b ea 95 c8 71 fe ,K...y1...;

0060 6f df bf 45 b2 de b5 4b 74 5f 77 48 ec a6 a8 a8 o..E...K t..w

0070 13 9b 23 73 ee a0 9c 8b 7b f5 53 0c 35 dd 40 e2 ..#s... {S

0080 0f 6c 6c c9 a9 e6 a3 53 dc 44 d0 a5 3e 1f be 9c ..11...S D-

0090 fe 16 56 8e f5 c9 63 c4 2a 3d da 3f 79 ae e7 8a ..V...c...\*=

00a0 6b e3 19 4a 83 95 d8 60 3d 08 93 af 01 e7 f5 6a >..J...:..=

00b0 8a 3e 1b 98 e3 58 12 f3 98 46 14 5e 90 93 a9 e9 >...X...:..F-

00c0 6d 21 f3 be d7 18 35 de 5c 66 5d 17 d4 47 3f fd m!...5... \f]

00d0 df ea 1c c8 22 ea 4a 2a 96 ac 09 5a 0f da 47 5e 5b ..#...:..\*...Z

00e0 69 3a 4f b0 8f 28 60 76 4d 46 9f de 9c 1f 25 38 i:0...(\v MF-

00f0 85 1a 20 50 48 1c 08 d7 fb 52 95 b2 74 aa 3a 0c ..PH...-R-

0100 e5 6c bc 4e 73 15 49 0a 3c 34 3c a2 43 6a c3 1c .l.Ns-I <4<

0110 a5 96 8a d8 a2 a5 92 ae 0c 06 19 75 63 b9 b0 54 ..i...:..#:

0120 00 43 c2 1c 9b 82 f5 41 3a 9b 40 8d b3 b9 ad 4d .C...:..A :@

0130 bf e3 dd 69 bb a8 19 80 1d 23 d3 75 a3 e0 ad 4e ..i...:..#:

0140 3c c7 be d1 ed 13 f5 f7 37 e3 2d ca 42 a1 0a 79 <...:..7...-

0150 f7 01 06 28 84 79 2c c8 60 d8 aa 2e f7 69 a4 ce ..(y...:..;

0160 5b a6 07 9b 8f 62 3c 0c 60 92 17 fd 73 d4 45 81 [...b<...:..;

0170 93 0f af e0 b1 81 fe 08 cf 42 e9 d4 4d 59 01 8c .....:..B-

0180 01 08 00 .....

Data-frame DS-traversal status (wlan.fc.ds), 2 bit(s)

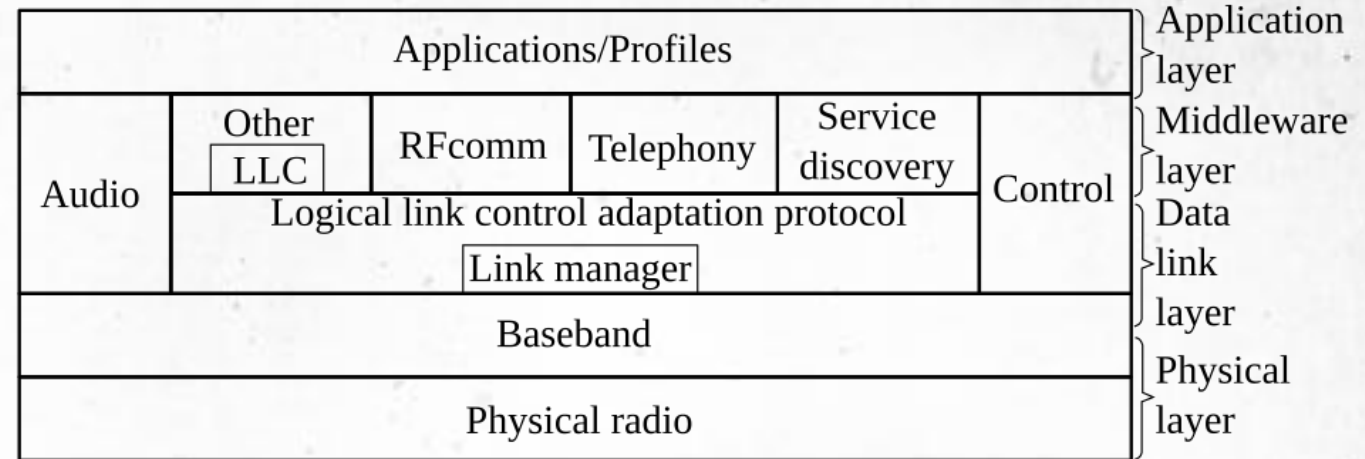
Packets: 202632 · Displayed: 74119 (36.6%) · Marked: 1 (0.0%) · Profile: Default



# 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](https://upload.wikimedia.org/wikipedia/commons/9/9f/Bluetooth_protokoly.svg)

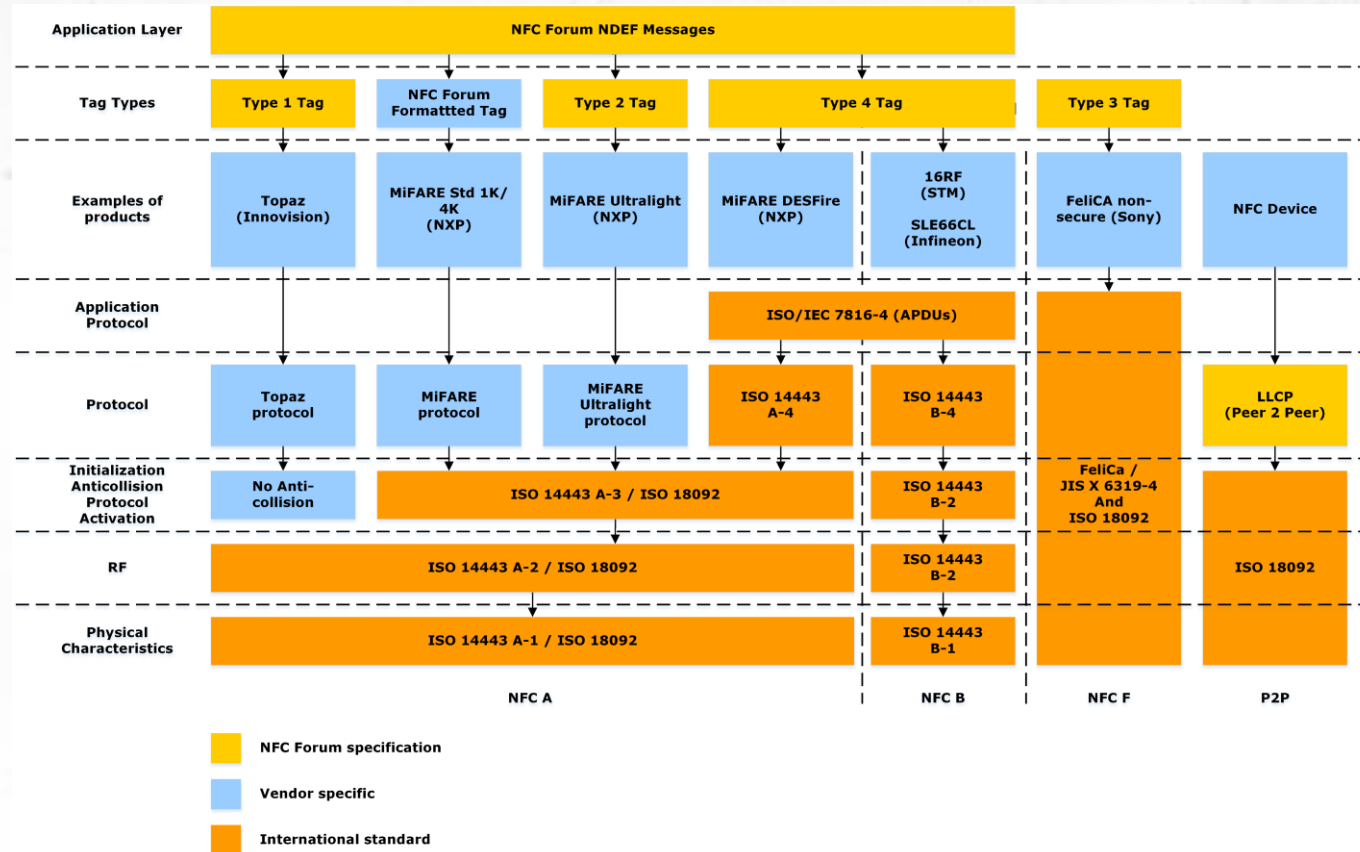
- scatternet

- 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)



# 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](https://upload.wikimedia.org/wikipedia/commons/3/33/NFC_Protocol_Stack.png)



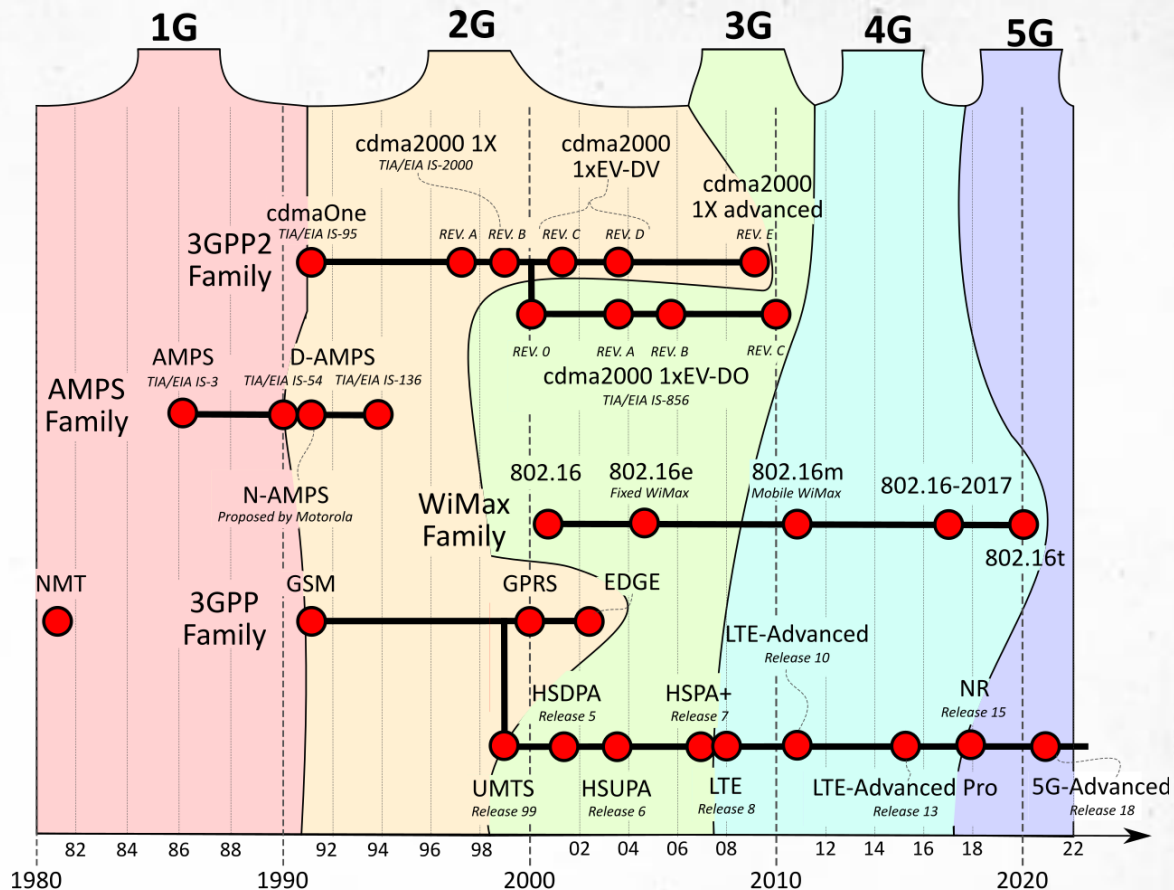
# Mobilné siete

- 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



# Mobilné siete

- Štandardy pre mobilné siete



[https://upload.wikimedia.org/wikipedia/commons/4/4a/Cellular\\_network\\_standards\\_and\\_generation\\_timeline.svg](https://upload.wikimedia.org/wikipedia/commons/4/4a/Cellular_network_standards_and_generation_timeline.svg)



# 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





UNIVERZITA  
PAVLA JOZEFA ŠAFÁRIKA  
V KOŠICIACH



Financované  
Európskou úniou  
NextGenerationEU

---

**PLÁN [OBNOVY]**

---



MINISTERSTVO  
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA  
A INFORMATIZÁCIE  
SLOVENSKEJ REPUBLIKY

**Ďakujeme za pozornosť**

