



„Információvédelem menedzselése”
LXXIX. Szakmai Fórum Budapest, 2018.
január 17.

A wifi technológia biztonsági kihívásai vállalati környezetben

Csuhai Gergely

Szenior hálózati mérnök

CCNA, CCSA, CCNP-R&S, CCNA-W, CCNP-W, CWNA, CWDP

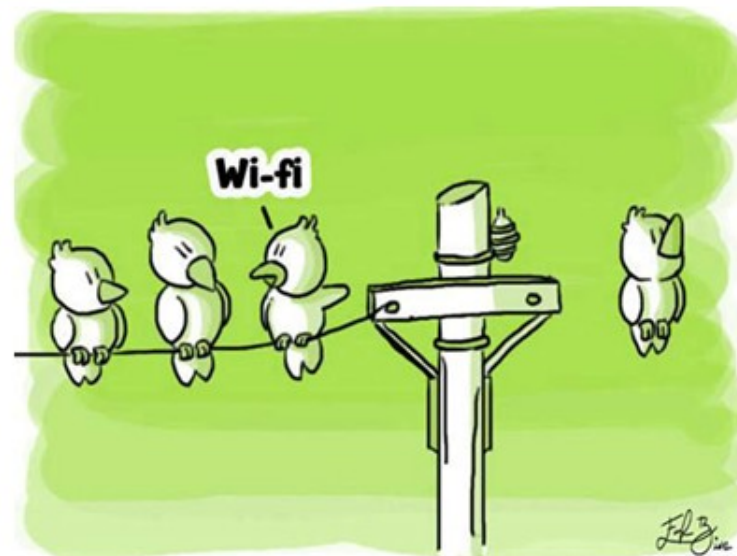




Hogyan is működik?



Biztonságos?



Veszélyforrások



Tervezés...

Mi történik valójában?





Hogyan is működik? Miért is...?

- Mobilitás
- Kényelem
- Rugalmasság

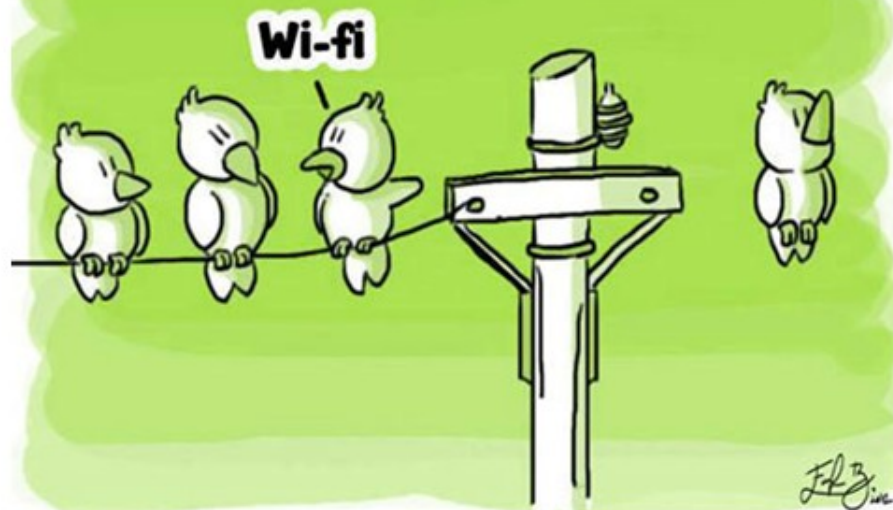
...és ez mennyire biztonságos?!





Hogyan is működik? Hogy képzeljük el?

Létezik, hiába nem „látjuk”



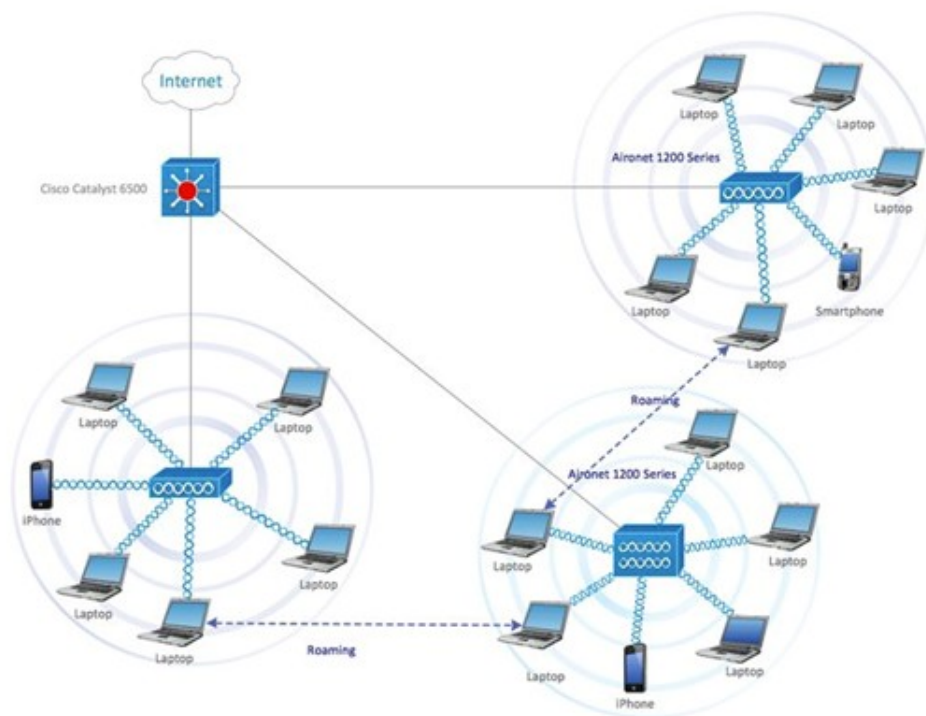
- Kettő vagy több eszköz közötti kommunikáció
- Átviteli közeg a levegő
- Frekvenciasávok (2,4GHz / 5GHz)
- Kódolási sémák



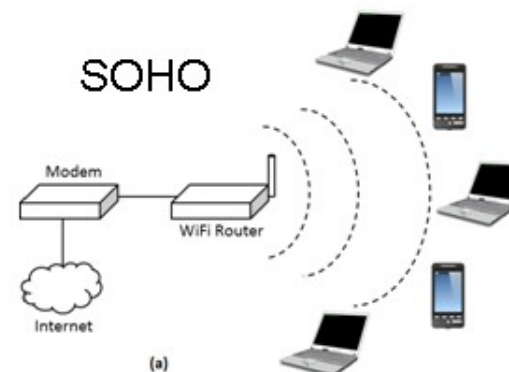


Hogyan is működik? Miből áll össze?

Enterprise



SOHO



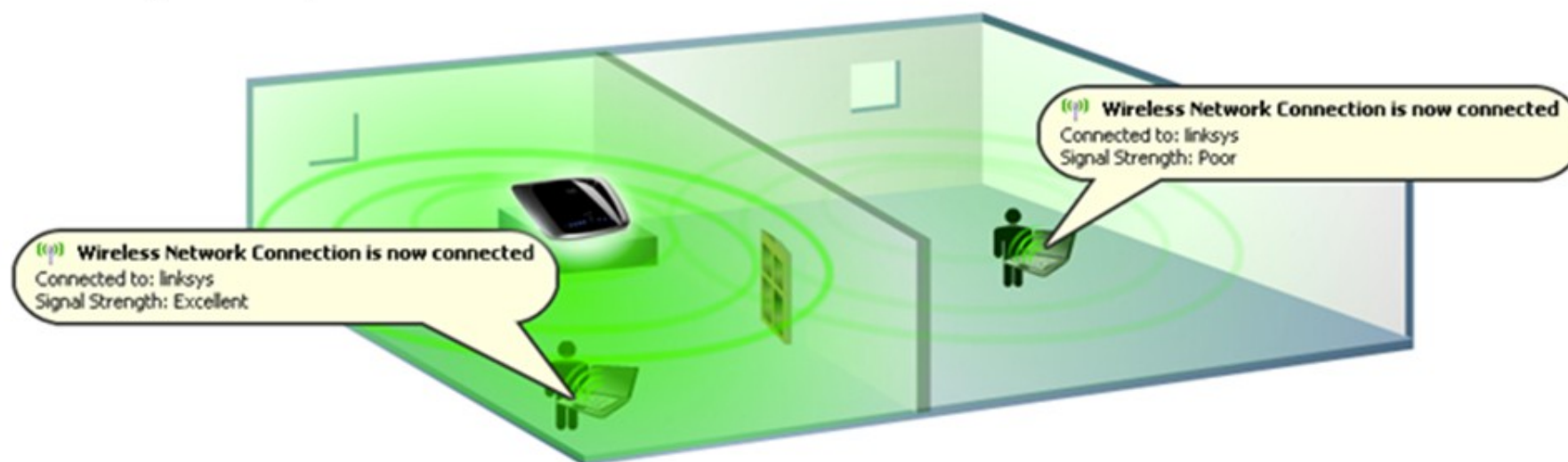
AD-HOC





Hogyan is működik? Fizikai korlátok

- Területi adottságok
- Kapacitás
- Teljesítmény





Tervezés Alapvető szempontok

- Felhasználás célja
- Felhasználás területe
- Területi adottságok
- Cella kapacitás
- Biztonságos zónák
- Süket / Zajos zónák
- Működésfolytonosság
- Felhasználói élmény





Mennyire biztonságos? Hogyan lesz biztonságos?



Milyen adatokat kell védeni?

Ki férhet hozzá az információhoz?

Ki nem férhet hozzá?





Mennyire biztonságos? Authentikáció, titkosítás



- 1997 – WEP (**Wired Equivalent Privacy**)
Statikus kulcs, gyenge titkosítás
- 2001 – EAP (802.1x)
Dinamikus kulcs, fejlesztett titkosítás,
felhasználó azonosítás
- 2003 – WPA
Dinamikus kulcs, fejlesztett titkosítás (128 bit),
felhasználó azonosítás
- 2004 – WPA2 (802.11i)
Dinamikus kulcs, fejlesztett titkosítás (256 bit),
felhasználó azonosítás
- 2018 - WPA3
Management frame protection





Mennyire biztonságos? Tévhitiek



1. SSID elrejtés

2. MAC cím szűrés

The screenshot shows the AirMagnet software interface. The top window displays a list of captured frames with columns for No., Length, Signal strength, Quality, Source, Destination, and Summary. The selected frame (No. 58) is an 802.11 association request. The bottom window shows the detailed structure of this frame, including the 802.11 MAC header, frame control, and frame body. The frame body contains capability information, SSID (0), supported rates (1), and extended supported rates (50).

No.	Ch	Length	Signal	Quality	Source	Destination	Summary
54	2	86	-65	1	00:0F:3D:08:16:6D	FF:FF:FF:FF:FF:FF	802.11 beacon
55	2	30	-39	1	00:0F:3D:09:E8:38	00:0F:3D:08:16:6D	802.11 authentication
56	2	30	-66	1	00:0F:3D:08:16:6D	00:0F:3D:09:E8:38	802.11 authentication
57	2	10	-47	1		00:0F:3D:08:16:6D	802.11 acknowledgement
58	2	58	-45	1	00:0F:3D:09:E8:38	00:0F:3D:08:16:6D	802.11 association request
59	2	46	-65	1	00:0F:3D:08:16:6D	00:0F:3D:09:E8:38	802.11 association response
60	2	10	-41	1		00:0F:3D:08:16:6D	802.11 acknowledgement
61	1	86	-57	1	00:0F:3D:08:16:6D	FF:FF:FF:FF:FF:FF	802.11 beacon

802.11 MAC header

- frame control
 - duration : 250 usec
 - dest addr : 00:0F:3D:08:16:6D
 - src addr : 00:0F:3D:09:E8:38
 - ssid : 00:0F:3D:08:16:6D
 - frag number : 0
 - seq number : 2118
- 802.11 frame body
 - capability info
 - listen interval : 10
 - info : SSID (0)
 - length : 12
 - SSID : WirelessGuru
 - info : supported rates (1)
 - info : extended supported rates (50)





Veszélyforrások Sebezhetőség



- Hozzáférési adatok nem biztonságos tárolása
- Hozzáférési szintek nem megfelelő szeparálása
- Nem megfelelő komponensek használata
Kulcs, eszköz, protokoll
- Monitorozás hiánya
- Emberi tényező...





Veszélyforrások Támadási típusok



- DOS
- Spoofing and Hijacking
- Evil twin
- Lehallgatás





Mi történik valójában? Működésfolytonosság

Monitorozás:

- Elég erős a jel?
- Nem túl zajos a környezet?
- Elegendő a sávszélesség?
- Stabil a kapcsolat?
- Milyen befolyásoló körülmények fordulhatnak elő?





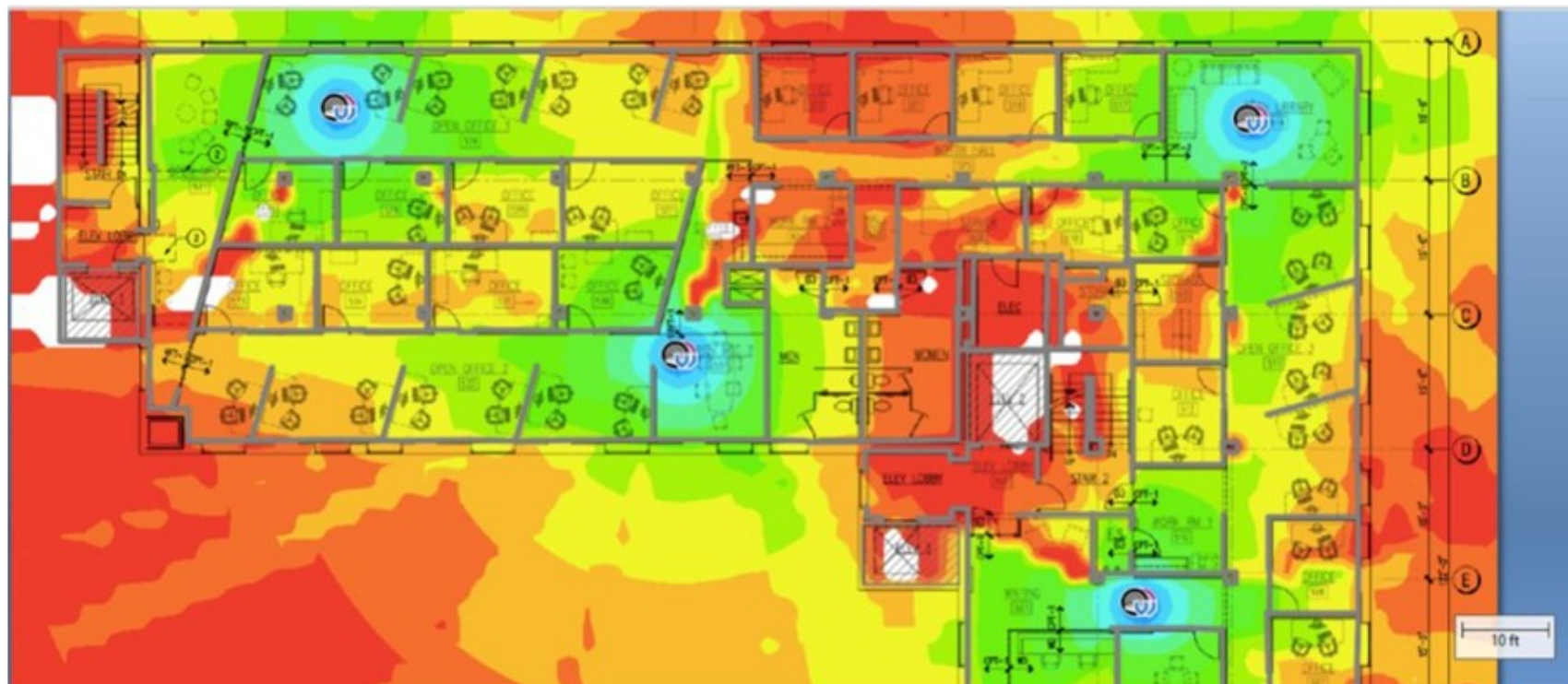
Mi történik valójában? Hogyan tegyük láthatóvá?

- Mérőeszközök
- Monitorozás



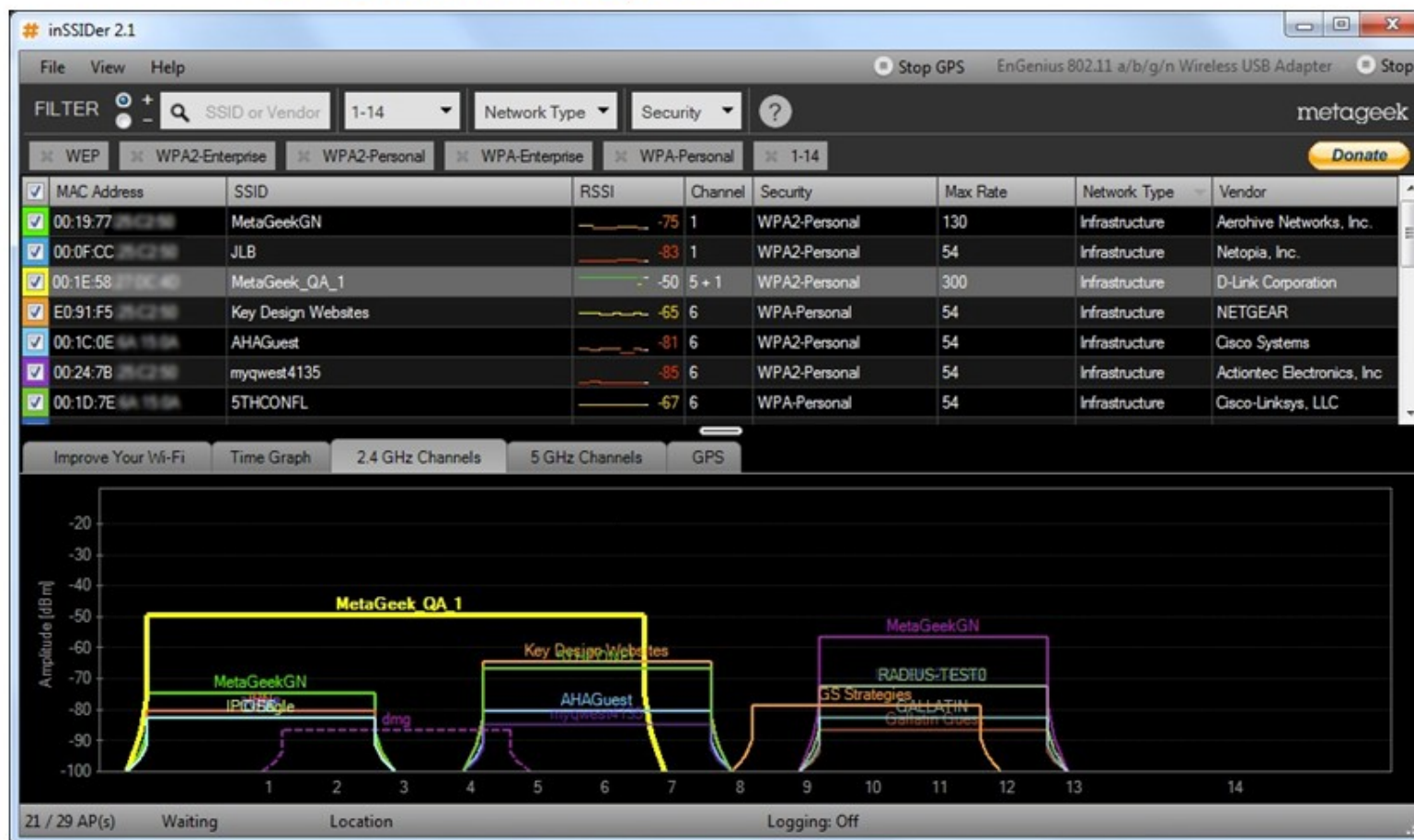


Mi történik valójában?
Hogyan tegyük láthatóvá?





Mi történik valójában?





Konkluzió

Biztonság vagy kényelem?

Tökéletesen biztonságos megoldás nincs,
de lehet és érdemes rá törekedni!

Eszköztárunk és ismereteink napról napra bővülnek.

