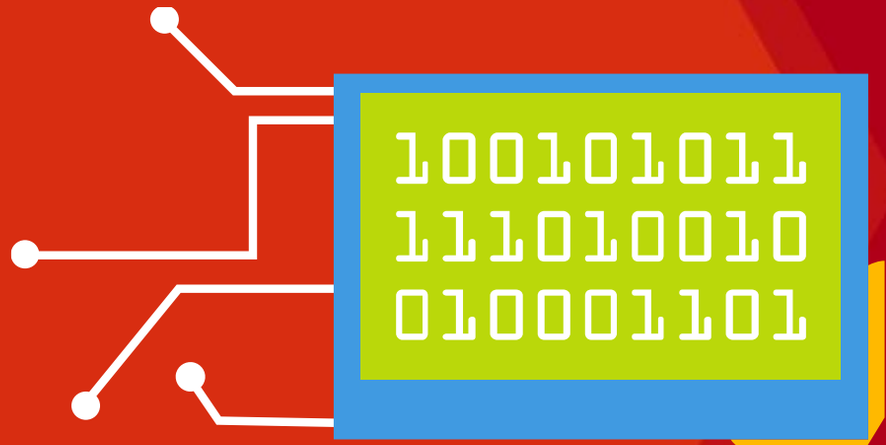
KONFERENCA

Microsoft

Kdo vam je “heknil” wireless

Kaj je prav in kaj narobe?



- Miha Jozelj
- Robert Bergles

Unistar LC d.o.o.

TEHNOLOGIJA

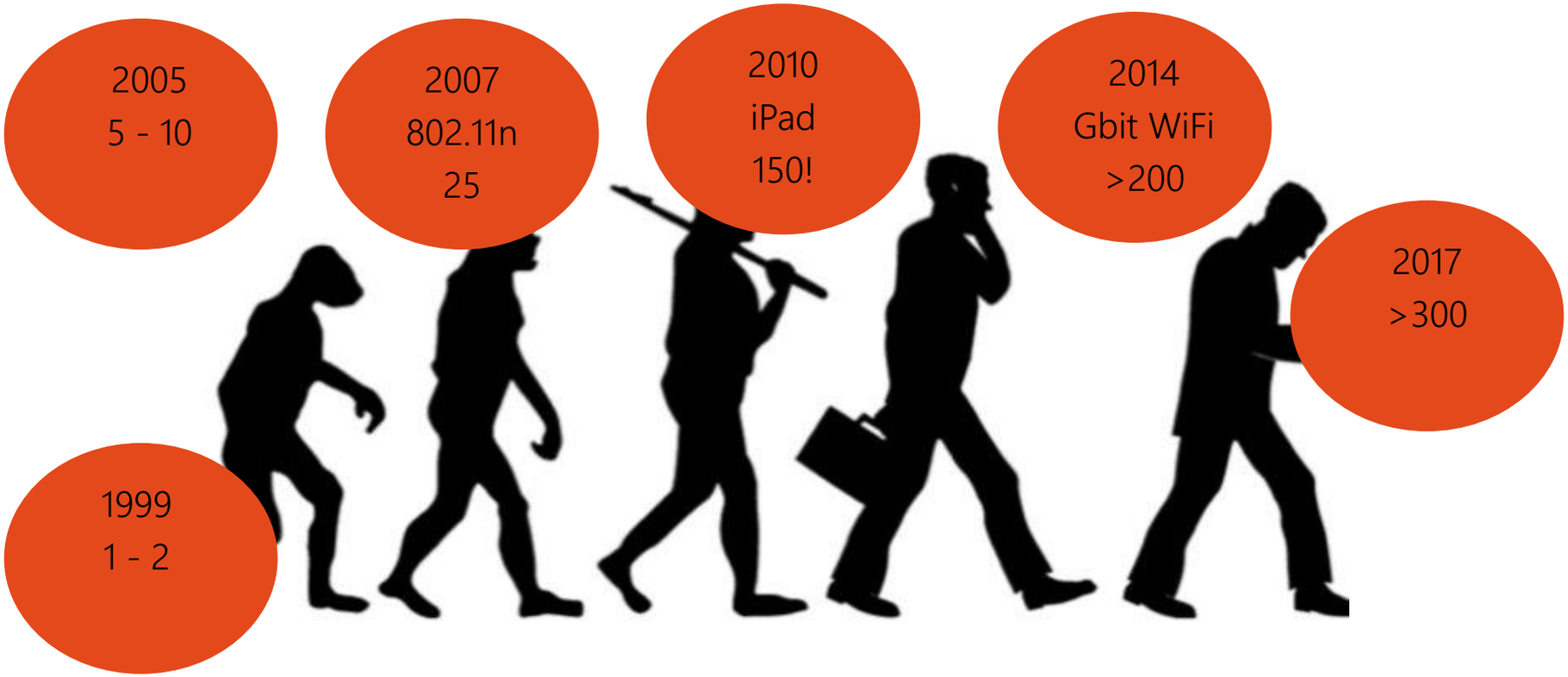
O čem bomo govorili?

- Wireless – Kako se je začelo?
- Optimizacija nastavitev
  - Uporaba kanalov
  - Oddajna moč
  - Fizična namestitev
  - Varnost
- 802.1x
  - AD
  - NPS
  - EAP-TLS

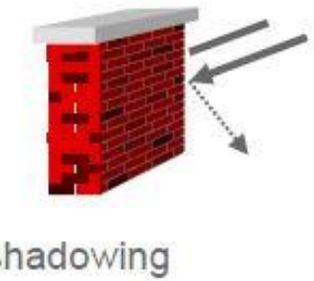
IZZIVI

- Počasen WiFi
- Naprava se ne poveže
- Ni prehoda med AP-ji
- Ali je WiFi varen?
- Omrežje za goste
- Primarni način priklopa
- Dosegljivost 99,999%

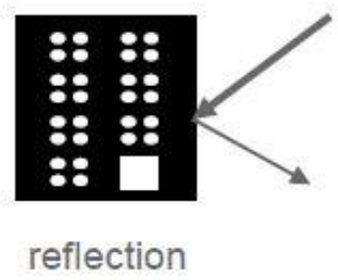
Wireless – Kako se je začelo?



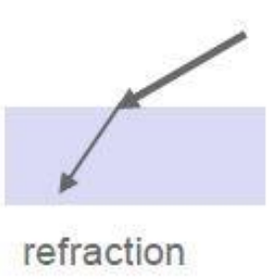
Kaj se dogaja v zraku?



senčenje

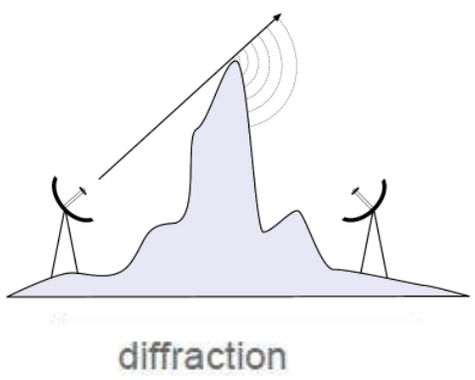


odsev



lom

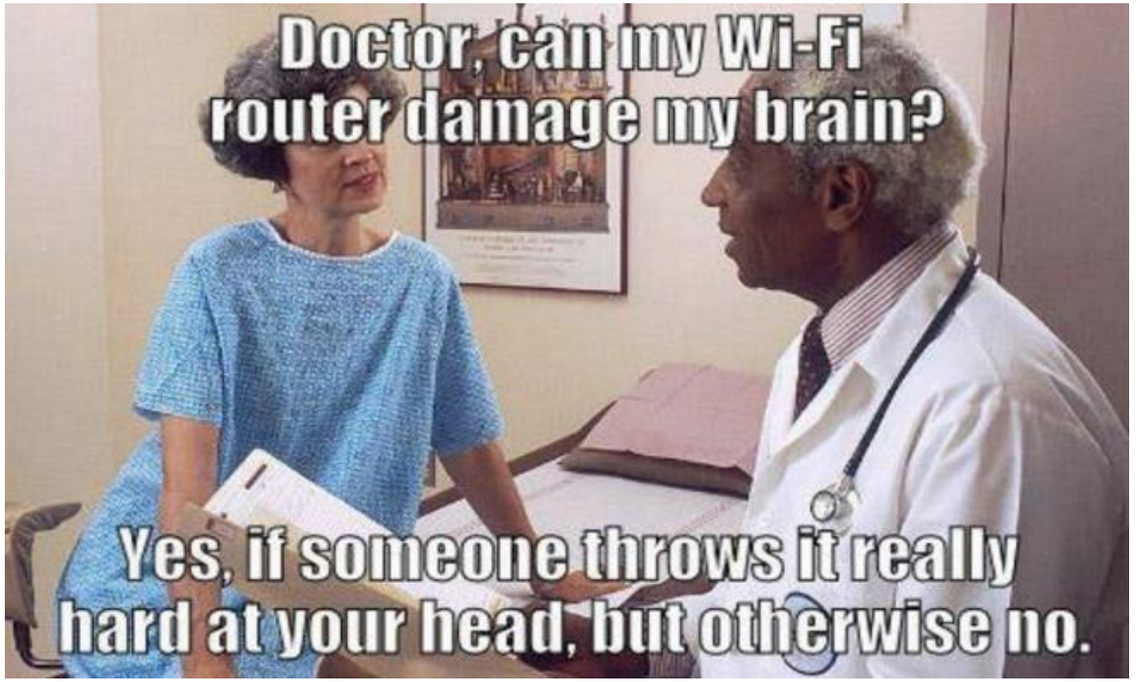
sipanje



difrakcija

Nevarno za zdravje?

- GSM ima oddajno moč 1W
  - 1W = 1000mW = 30dBm
- Oddajna moč WiFi AP
  - 100mW (max)
- RSSI (npr. -66 dBm)
  - To je 0,00000000025W



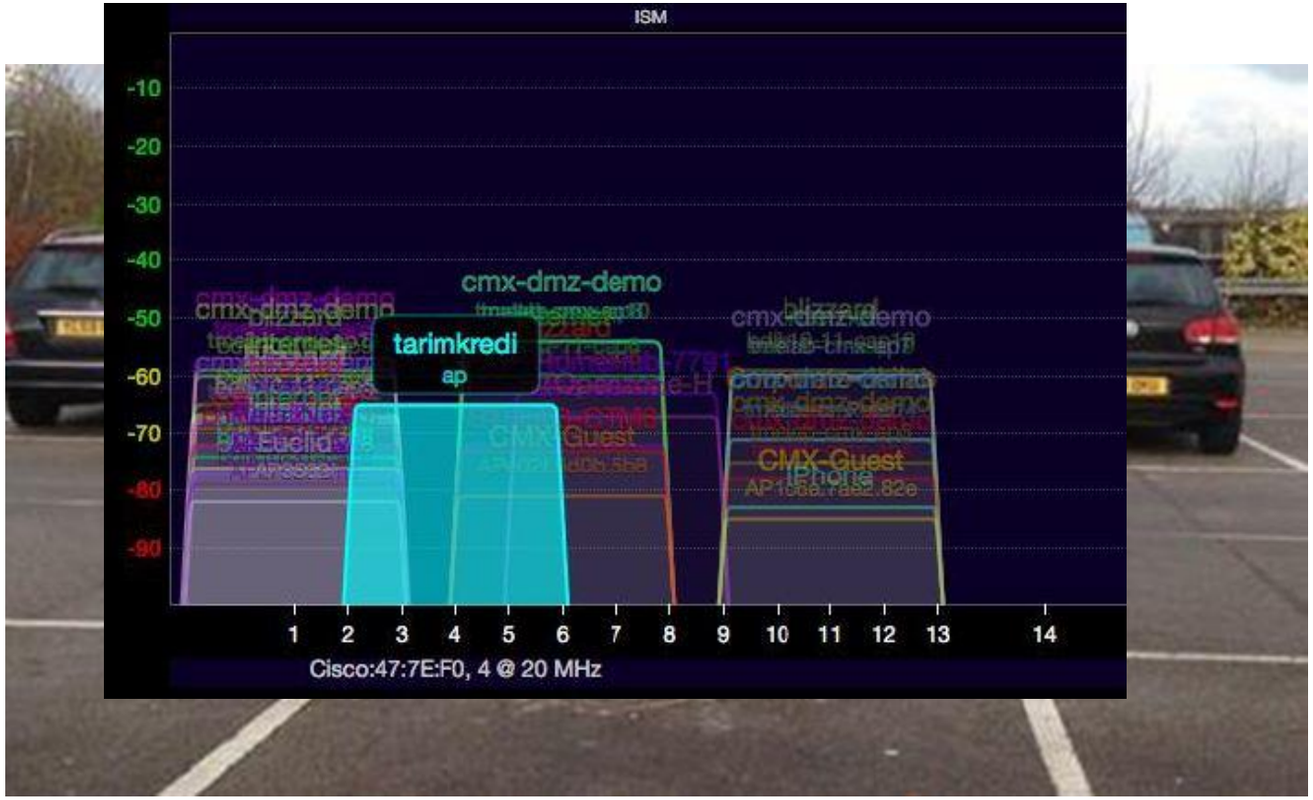
Uporaba kanalov

Kaj je prav in kaj narobe?

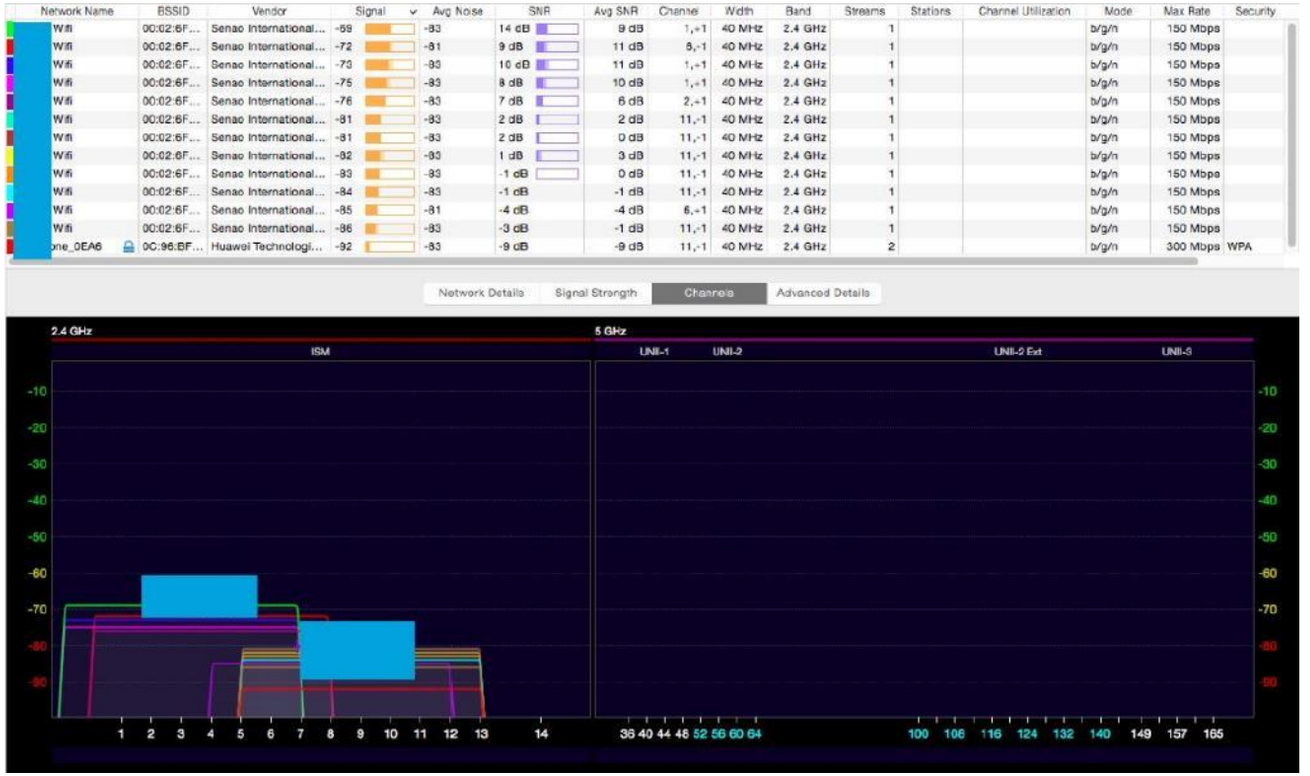
Microsoft

KONFERENCA

Uporaba kanalov na frekvenci 2,4GHz

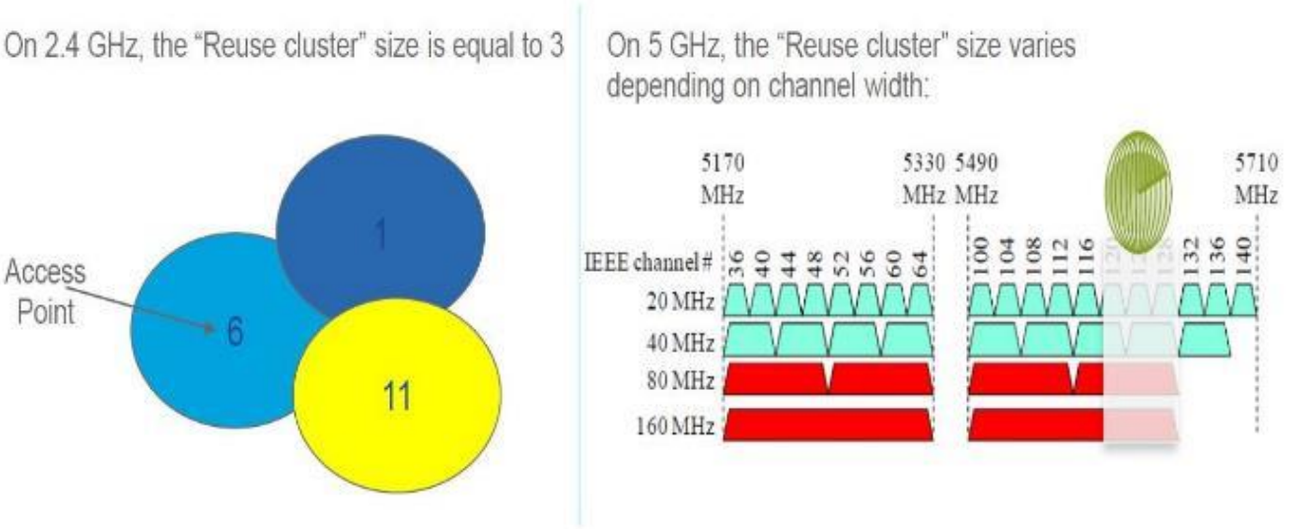


Širina kanala na frekvenci 2,4GHz



Uporaba kanalov – Dobra praksa

- Na frekvenci 2,4GHz kanali 1, 6 in 11
- Uporaba 5GHz frekvence, če je le mogoče
  - (več neprekrivajočih kanalov)
- Mehanizem DCA (*Dynamic Channel Assignement*)
  - *Dinamično določanje kanalov*
- Mehanizem *Dynamic Bandwidth Selection*
  - *Najboljša širina kanala (Channel Width Best)*



Oddajna moč AP

Kaj je prav in kaj narobe?

Microsoft

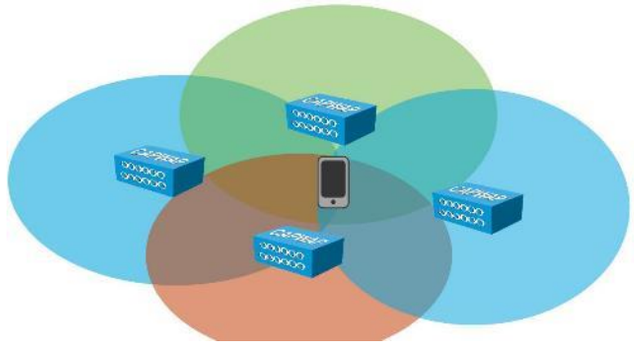
KONFERENCA

Uporabljam MAX oddajno moč, ker …

- zato rabim manj AP-jev
- mora AP pokrivati čim večje področje
- je to privzeta nastavitev

MAX oddajna moč (20dBm / 100mW

- Interferenca (CCI - Co Channel Interference)
- Uporabniške naprave niso “Max Power”
  - Tipično 14dBm / 25mW
- MIMO design uporabniških naprav
  - 1 send, 1 receive, 1 spatial stream



Oddajna moč – Dobra praksa

- Ne uporabljajte 100% oddajne moči
  - Priporočeno 5dBm – 17dBm
- Uporaba RRM
  - DCA (Dynamic Channel Assignement)
  - TPC (Transmit Power Control)
  - CHDM (Coverige Hole Detection and Mitigation)
- Naredite meritve

Setting Tx power is like drinking scotch:
The right amount is great, but "more" does not mean "better", and too much will make you sick …

Fizična namestitev

Kaj je prav in kaj narobe?

Microsoft

KONFERENCA

Namestitev: Ali je res pomembno?

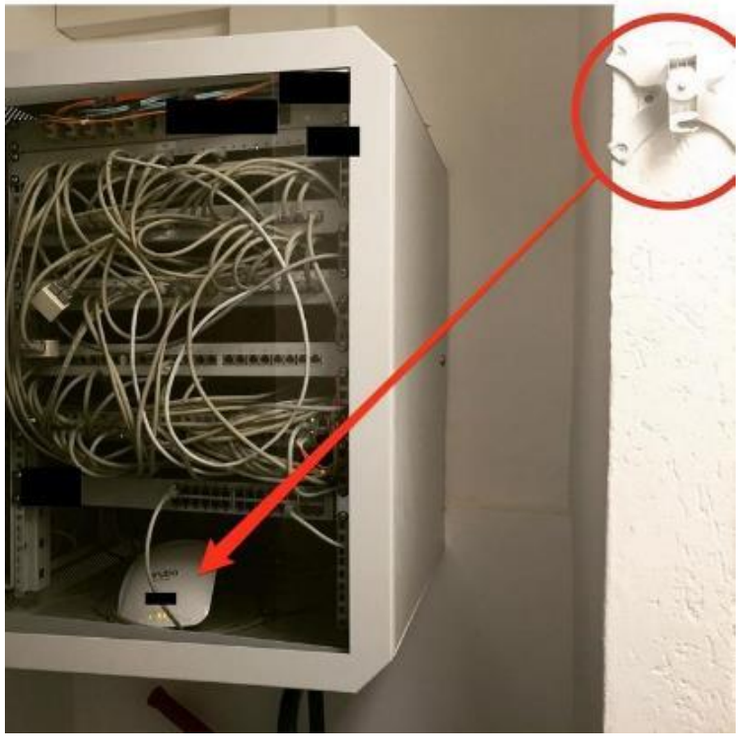
Napačna namestitev

Eden od načinov kako skriti SSID

SAD-FI
BAD-FI

Duct Tape
on a Duct

Napačna namestitev



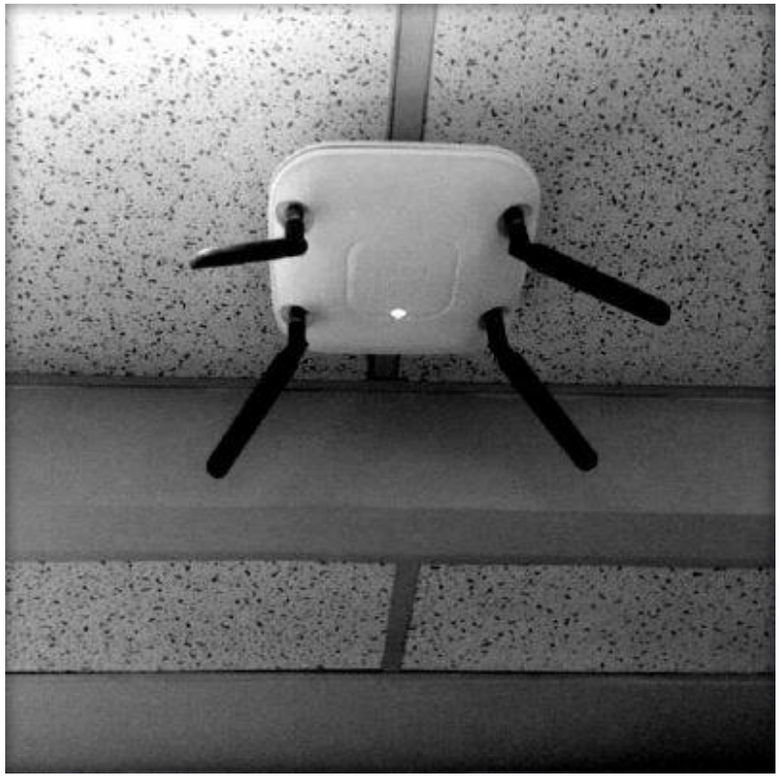
Namestitev anten

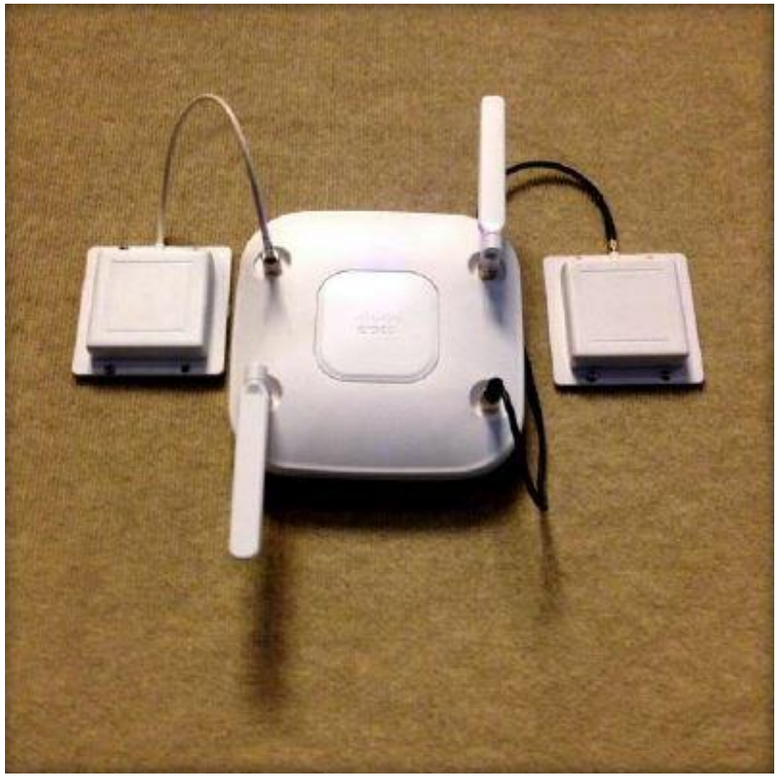
Antene so vedno usmerjene gor in dol

ZAKAJ?

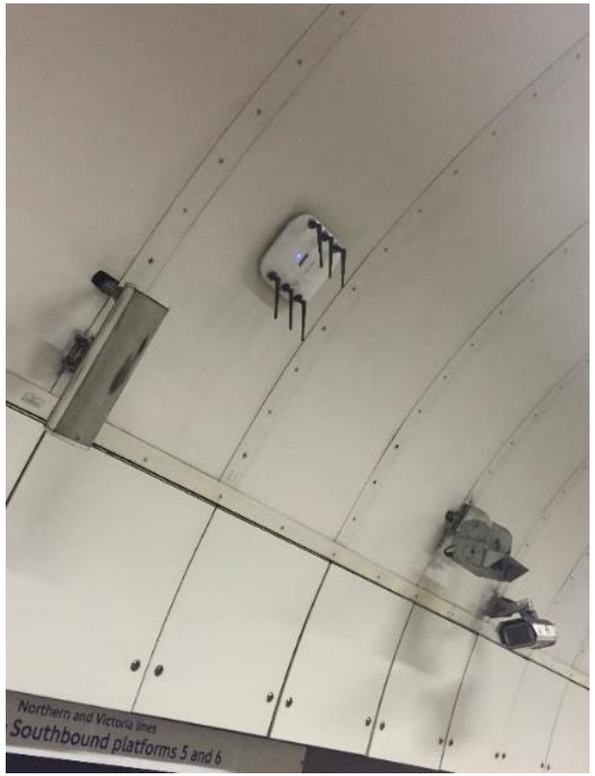
- Večina uporabniških naprav je narejena za vertikalno polarizacijo!
- Če je polarizacija horizontalna, izgubimo približno 20 – 30 % kapacitete/zmogljivosti!

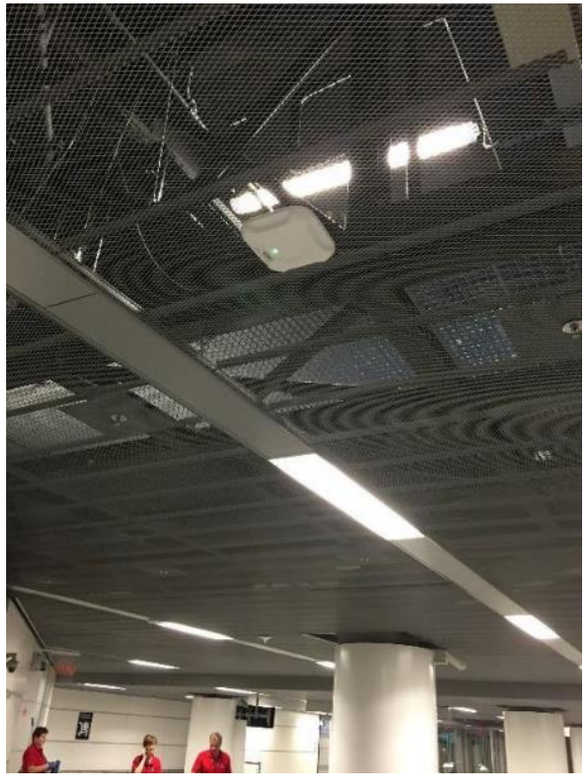
Namestitev anten – NE TAKO!





Pravilna namestitev in dobra praksa





- Vertikalna polarizacija
- Namestitev pod ovirami
- Minimalno 3 m med dvema AP-jema
- Izbira pravih anten – vedno en tip antene
- AP-ji na pravilni višini (optimalno 4 m)
- Ne zaklepajte AP-jev v železne kletke
- Uporabljajte “Outdoor” AP-je za zunanji WiFi

- AP-ji ki so namenjeni za namestitev na steno, se namestijo na steno
- AP-ji, ki so namenjeni za namestitev na strop, se namestijo na strop
- AP-ji z vgrajenimi antenami so za pisarniško okolje
- AP-ji z zunanjimi antenami za bolj zahtevno okolje (skladišča, zunanje postavitve, …)

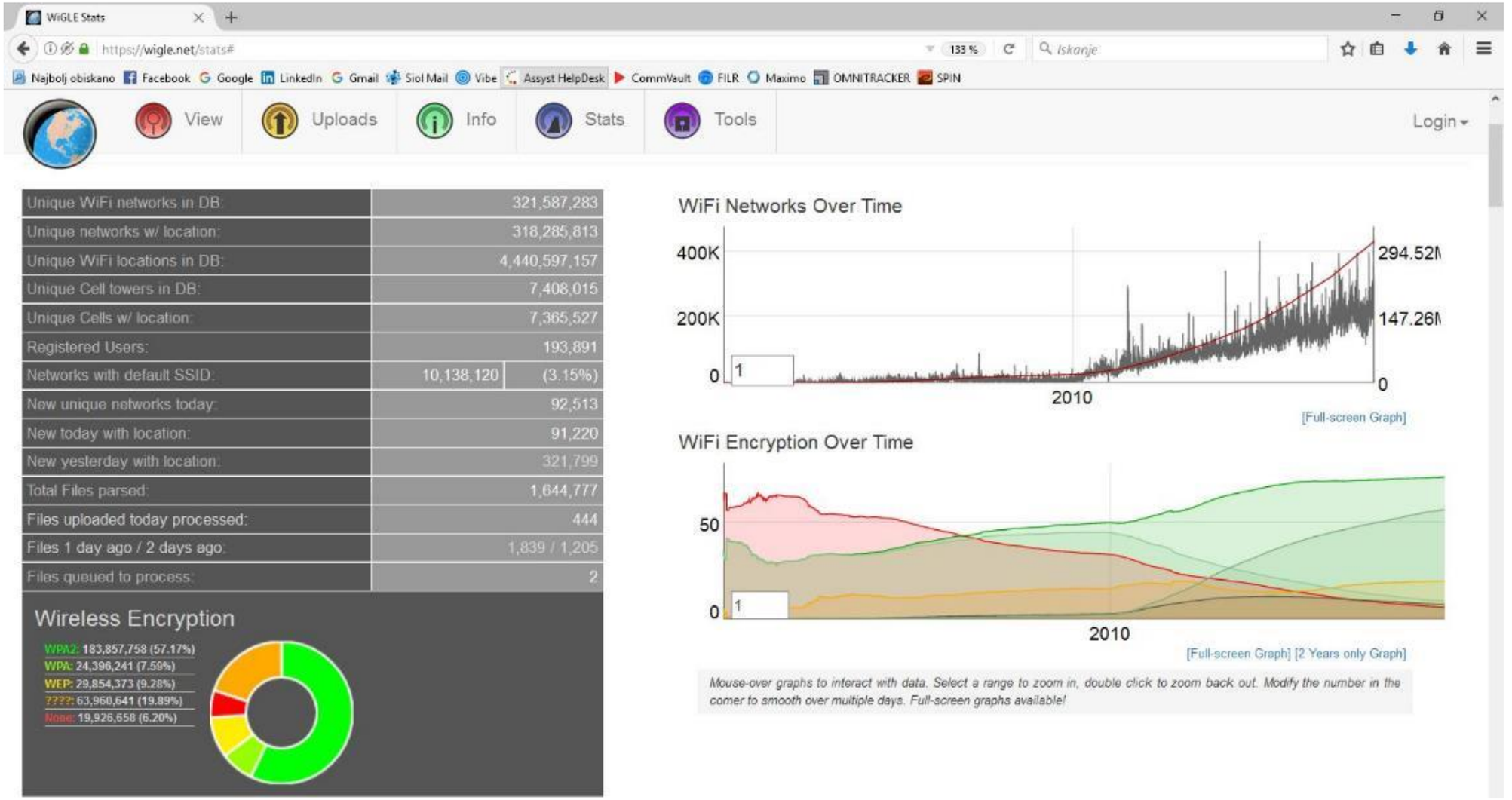
Varnost

Kaj je prav in kaj narobe?

Microsoft

KONFERENCA

https://wiggle.net



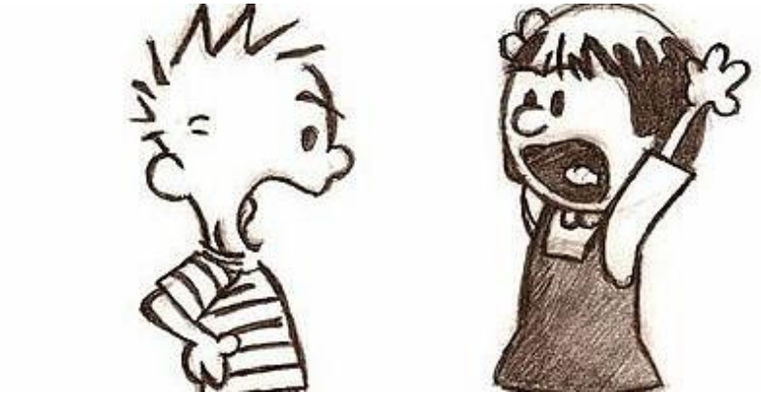
WiFi – Varnostne grožnje

- Na začetku – Iskanje dostopa do internet
- Danes drugi motivi
  - Pridobivanje uporabniških imen in gesel
  - Prestrezanje sej
  - Prestrezanje elektronske pošte
  - Elektronsko bančništvo
  - Industrijsko vohunjenje

Napadi na varnostne mehanizme

- MAC Filter - ☺☺☺
- WEP – geslo napadalec dobi v 6 minutah
- WPS – Reaver bruteforce
- WPA/WPA2 – napad na geslo s pomočjo slovarja
- WPA/WPA2 – Socialni inženiring

FIREWALLS, Routers, Switches, Proxies, Web security, gateways, VPN concentrators, NID NIPS, IPS, IDS, ACCESS control lists, Flood guards, Loop protection, IMPLICIT deny, Network separation IPSEC, SSH, TLS, SSL, HTTPS, Man-in-the-middle, DDoS, Replay, SMURF ATTACK, Spoofing, Spam, Phishing, Spim VISHING, Brute force, Dictionary attacks, Birthday attacks, RAINBOW tables, Malware inspection, Behavior based, Signature based, Anomaly based, 802.1x



Trditev:

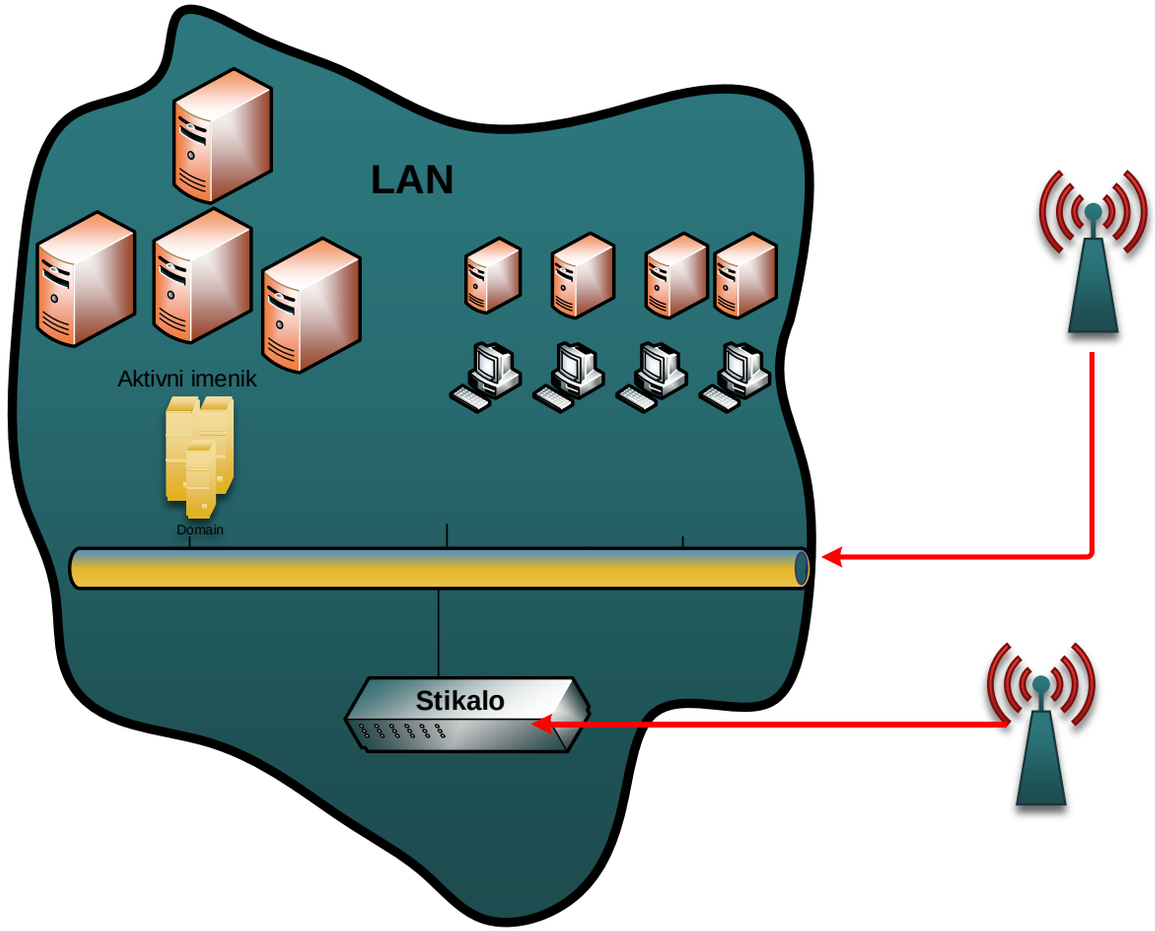
Če nimate brezžične povezave zaščitene z 802.1x **EAP standardom** „+**CERTIFIKATi**“ obstaja velika možnost penetracije v sistem !!

Zavarovanje brezžičnega omrežja

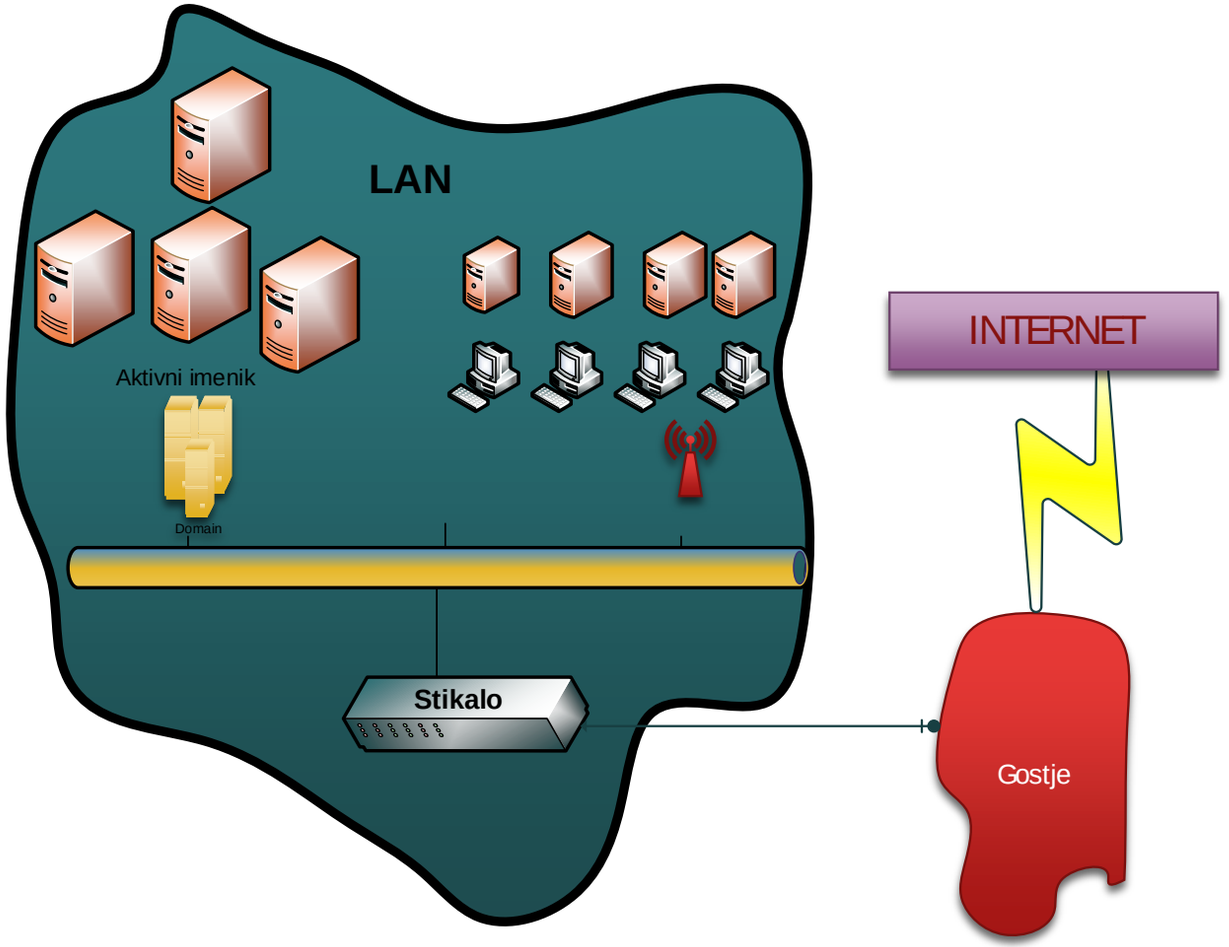
Premalo

- SSID WEP
- SSID WPA
- Skriti SSID
- MAC

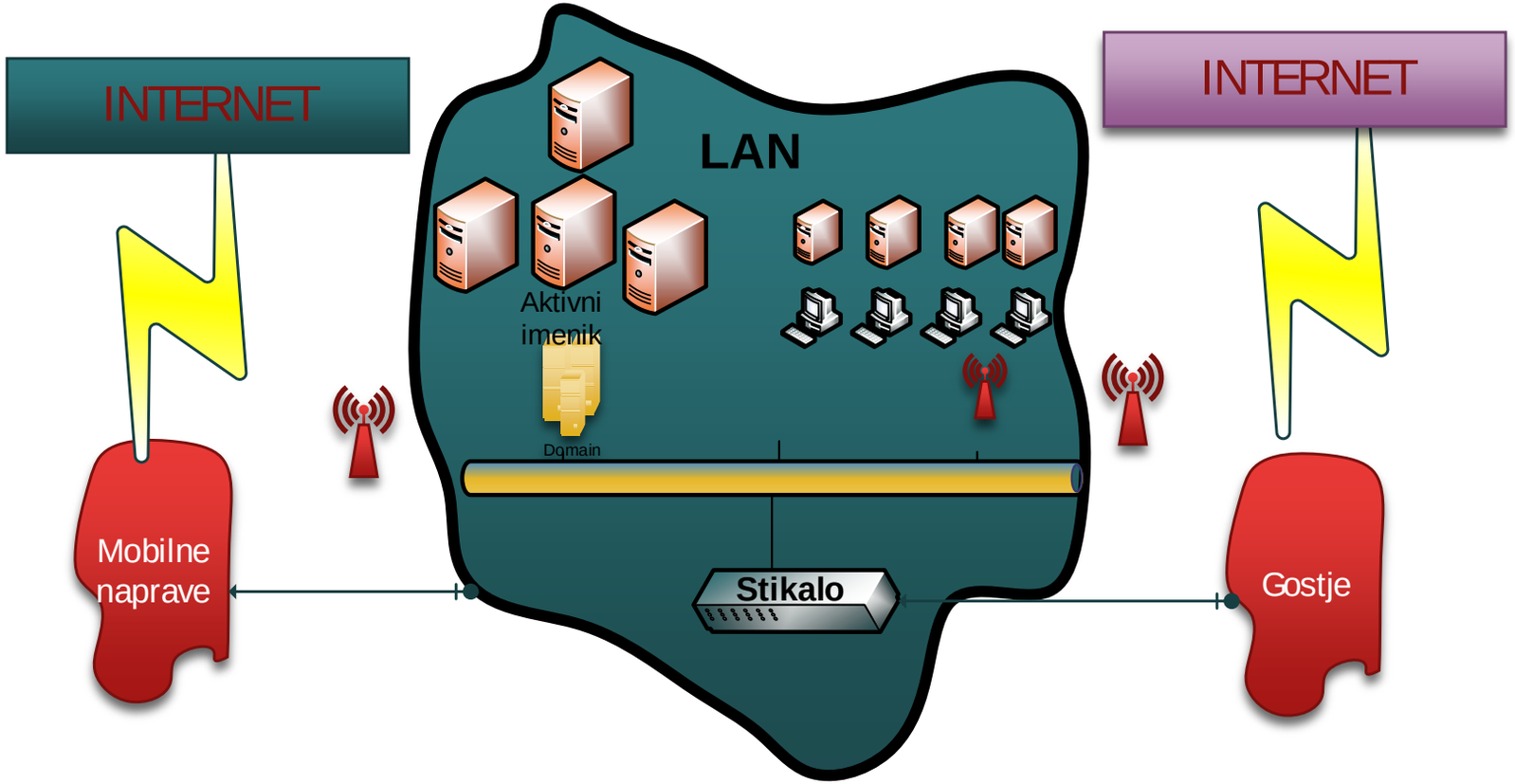
Slabo



Malo boljše



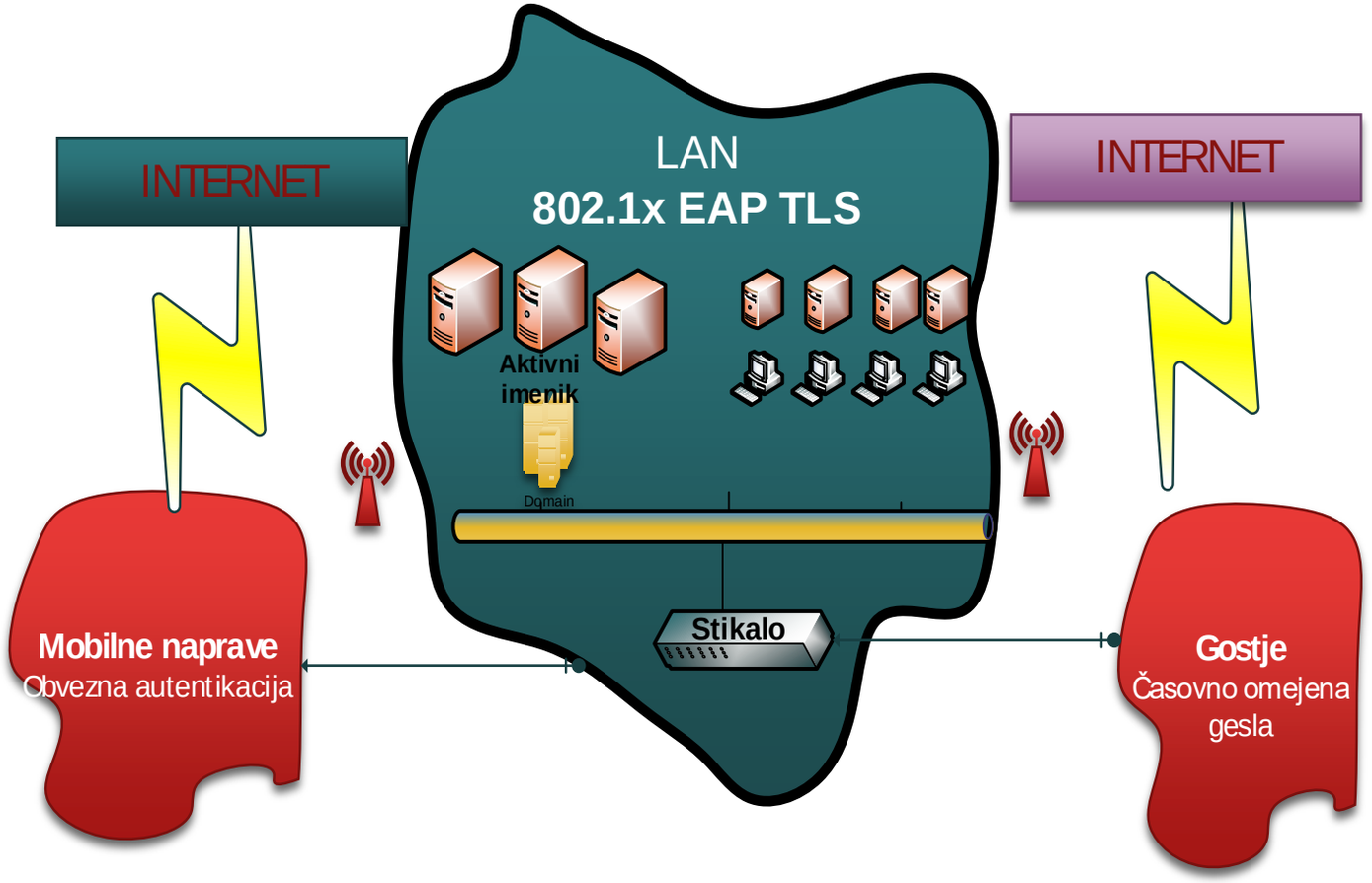
Skoraj primerno



Načini razbijanja zaščite

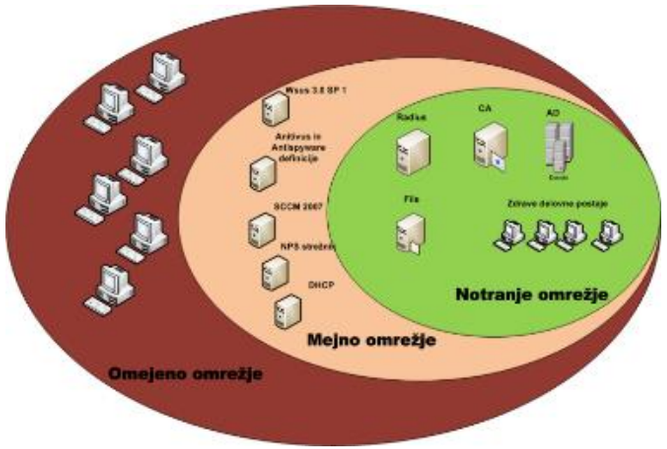
- Brute force ??
- Privzete nastavitve „DEFAULT“ Wifi usmerjevalnikov
- Socialni inženiring
  - Dostop do telefona
  - Dostop do prenosnika
- Vdor v mobilni telefon
  - Pregled INI datotek za Wifi dostope
- Vdor v prenosni računalnik
  - Pregled Wifi nastavitev
- Penetracija preko slabše zavarovanega domačega omrežja

Pravilno



- **Gostje**
  - Časovno omejeno geslo One time password
- **Interne mobilne naprave**
  - Obvezna autentikacija Ločen autentikacija od AD
- **LAN uporabniki**
  - 802.1x s certifikati

Potrebna infrastruktura

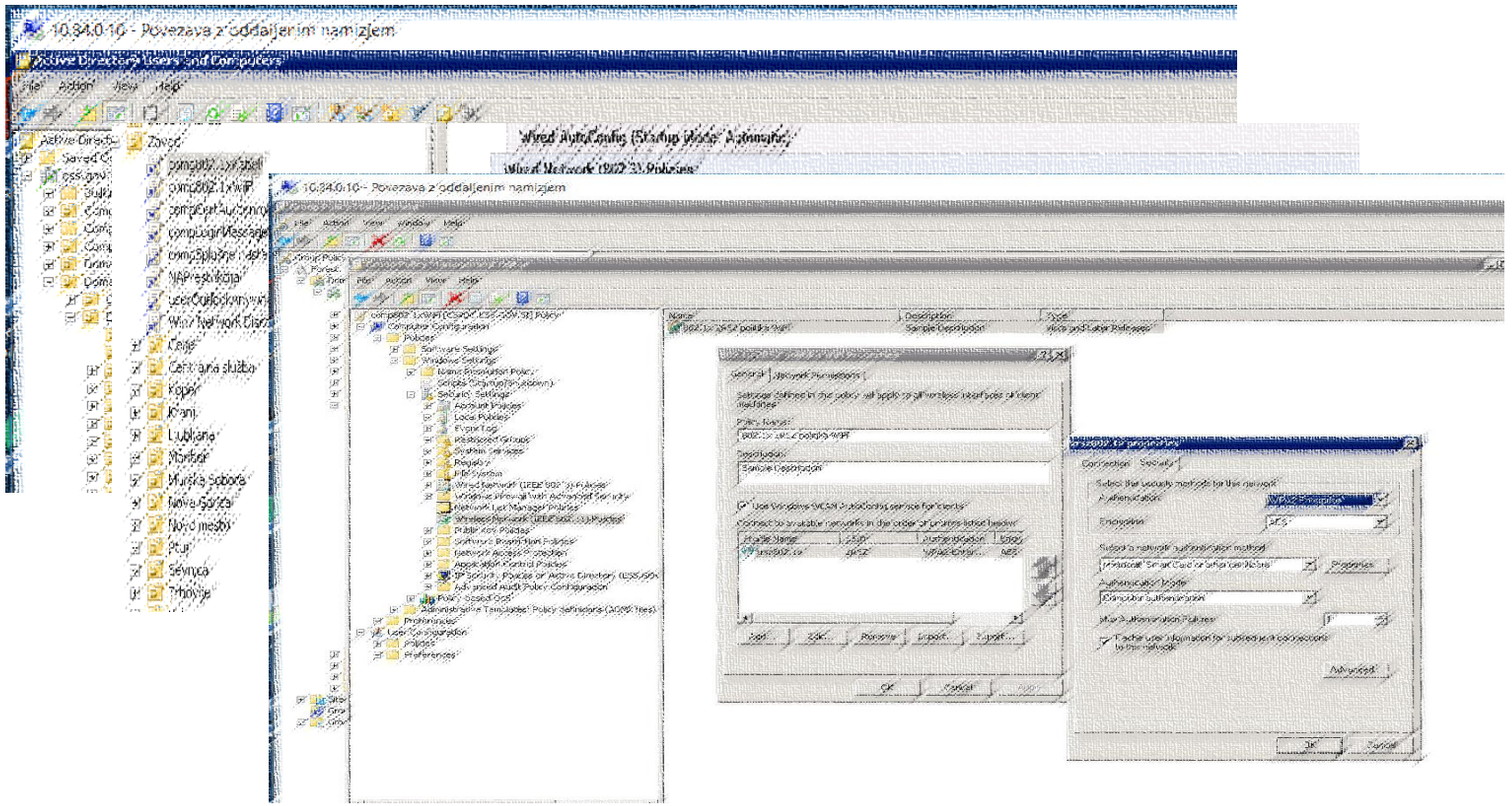


- Stikala podprta standardom 802.1x
- Aktivni imenik
- Radius
- NPS (Cisco ISE, Microsoft NPS)
- Interna infrastruktura za certifikate
- DNS

Zaupanja vreden EAP- autentikacijski protokol

- EAP-Transport Layer Security (EAP-TLS)
- Tunneled Transport Layer Security (TTLS)
- Cisco Light Weighted EAP (LEAP)
- Protected EAP (PEAP)
- .....

Nastavitve naprav v Aktivnem imeniku



- Nastavitve preko GPO
  - prevzem certifikata
  - omrežne nastavitve
  - 802.1x profilne nastavitve

Reference

- Zavod za zaposlovanje RS
- ComLand d.o.o.
- Ministrstvo za zunanje zadeve
- Ministrstvo za kmetijstvo okolje in prostor
- Ustavno sodišče RS
- DZ (državni zbor)
- MP (Ministrstvo za pravosodje)
- Acroni Jesenice
- GSV (Generalni sekretariat vlade)
- ….

Sedaj veste malo več

- **Če sami skrbite za WiFi omrežje**
- **Če najemate zunanjega izvajalca**

Vendar …

Kraja PSK

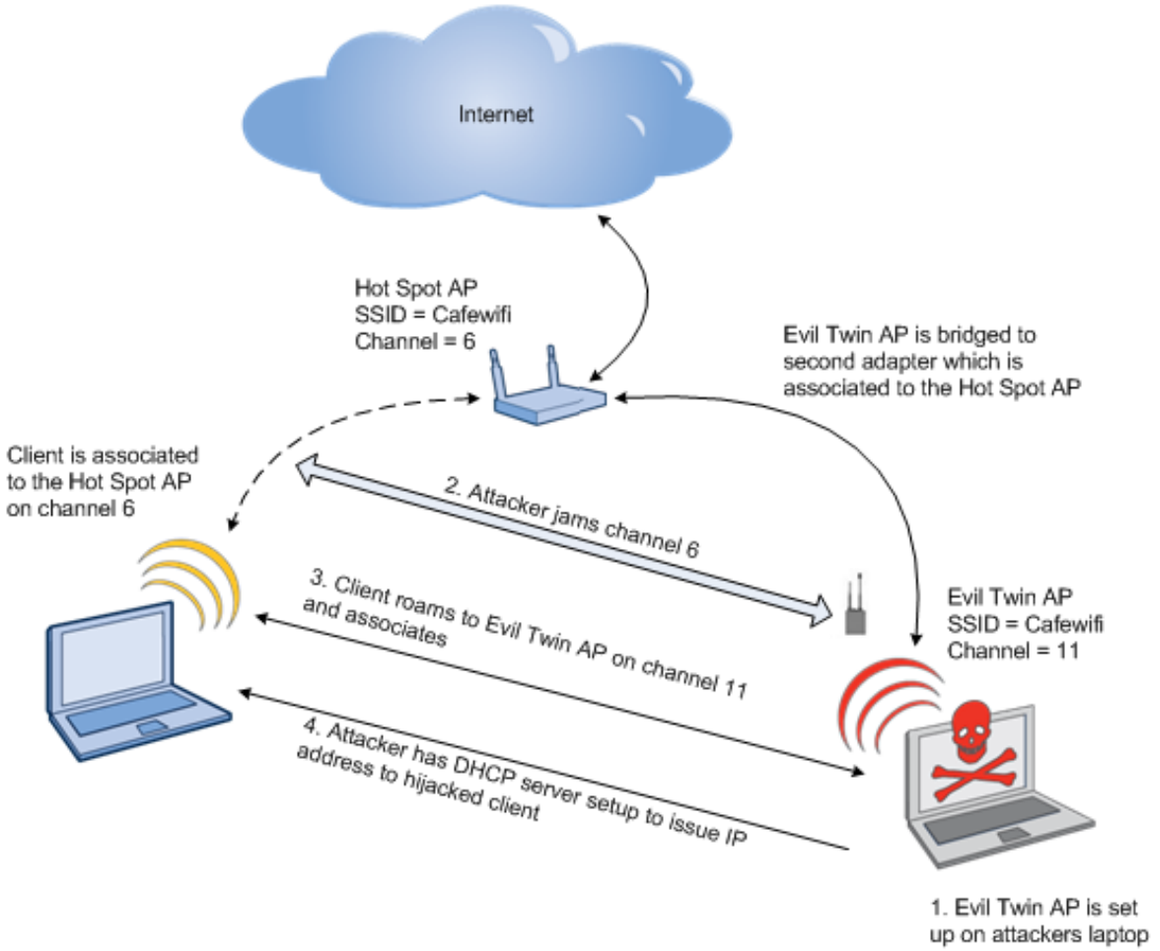
Evil Twin AP in socialni inženiring

Microsoft

KONFERENCA

Evil Twin – Prevara za pridobitev PSK

- Naredimo Evil Twin AP
- Naredimo DoS na pravi AP
- Počakamo, da se uporabnik asociira z napadalčevim AP
- Uporabniku ponudimo spetno stran, kjer zahtevamo vpis PSK



Varnost – Dobra praksa

- WPA2 je minimum
- WPA2 Personal (PSK) je za domačo uporabo
- Za poslovno okolje WPA2 Enterprise
  - 802.1x z uporabo certifikatov (EAP-TLS)
- Uporaba "Role Based Access" (MS NPS)
- Na javnih WiFi omrežjih uporabljajte VPN

Microsoft

KONFERENCA

PORTOROŽ, 15. DO 17. MAJ 2017