Cisco Connect

Bled, 11. april 2018

Brez ustrezne konfiguracije žične in brezžične opreme smo lahka tarča napadalcev

Miha Jozelj *CCNP Wireless*

Robert Bergles *CEHv9, MCSE,MCT,MTA*

Unistar PRO

Agenda

Cisco Connect

- Kako deluje WiFi?
- Pogoste napake
  - Kanali
  - Oddajna moč
  - Namestitev
  - Nadgradnja
  - Legacy devices
- Načrtovanje
  - Načrtovanje za pokritost
  - Poslušajte arhitekta
  - “Outdoor” WIFI
  - “High-Density” WIFI
- Varnost

DEMO

- ARP spoofing
- Man-in-the-Middle
- DHCP Attack

Kako deluje WiFi

802.11 standardi

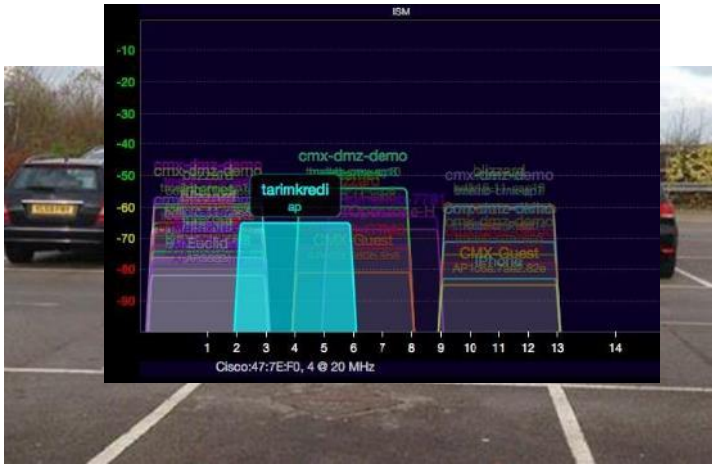
Cisco Connect

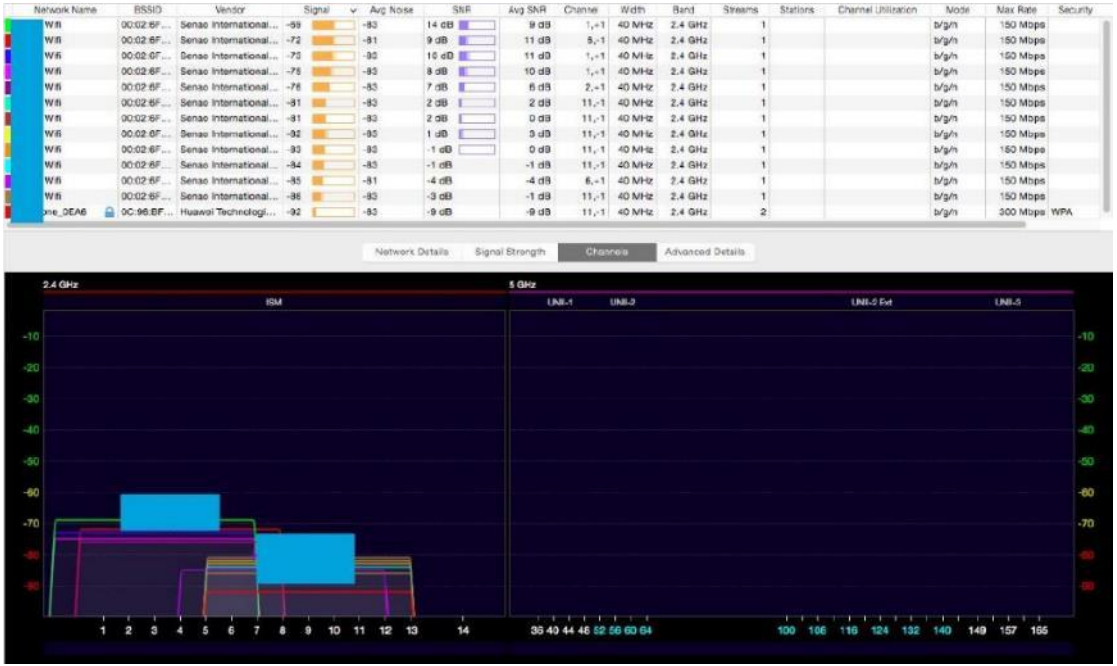
Bandwidth & Data rate

802.11	Frequency	Data rate	Channels	Channels 'usable'
a	5 GHz	54 Mbps	24	24
b	2.4 GHz	11 Mbps	13	3
g	2.4 GHz	54 Mbps	13	3
n	2.4 GHz & 5 GHz	(min) 65, 150, 300, 450, (max) 600 Mbps	2.4 GHz & 5 GHz Rules apply.	2.4 GHz & 5 GHz Rules apply.
ac	5 GHz	867 Mbps 1.3 Gbps, 1.7 Gbps* 3.5 Gbps* 6.9 Gbps*	24* 37**	24* 37**

* = 802.11ac Wave 2
** = 802.11ac Wave 2 (US)

Pogoste napake – Uporaba kanalov

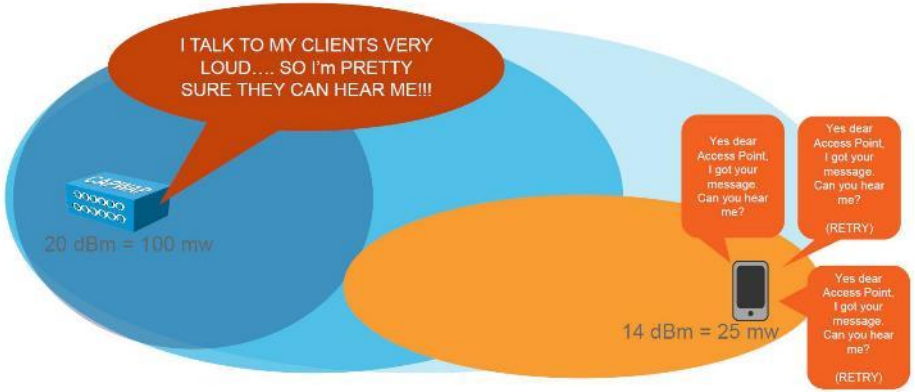




Dobra praksa

- 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)*

Pogoste napake – Oddajna moč



Max oddajna moč (20dBm / 100mW)

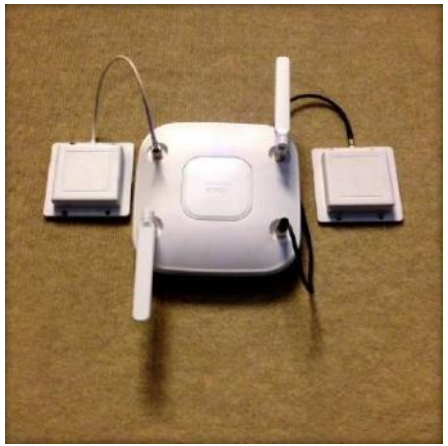
- Interferenca (Co Channel Interference (CCI))
- Uporabniške naprave niso "Max Power"

  (tipično 14 dBm / 25mW)

- **Dobra praksa**
- Oddajna moč (5 dBm – 17 dBm)
- Uporaba RRM
  - DCA – Dynamic Channel Assignement
    - (Dinamično določanje kanalov)
  - TPC – Transmit Power Control
    - (Dinamično uravnavanje oddajne moči)
  - CHDM – Coverige Hole Detection and Mitigation
    - (Detekcija lukenj v pokritosti)
- Pri načrtovanju WiFi sistemov je vedno potrebno/priporočeno narediti meritev (Site Survey)

Pogoste napake – Fizična namestitev

Pogoste napake - Namestitev anten

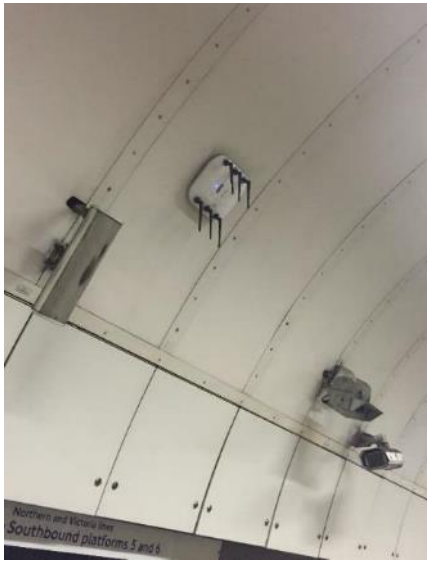


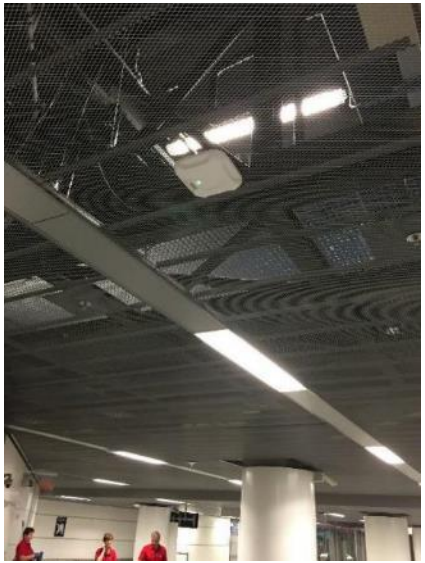
Antene so vedno usmerjene gor in dol

ZAKAJ?

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

Namestitev – dobra praksa

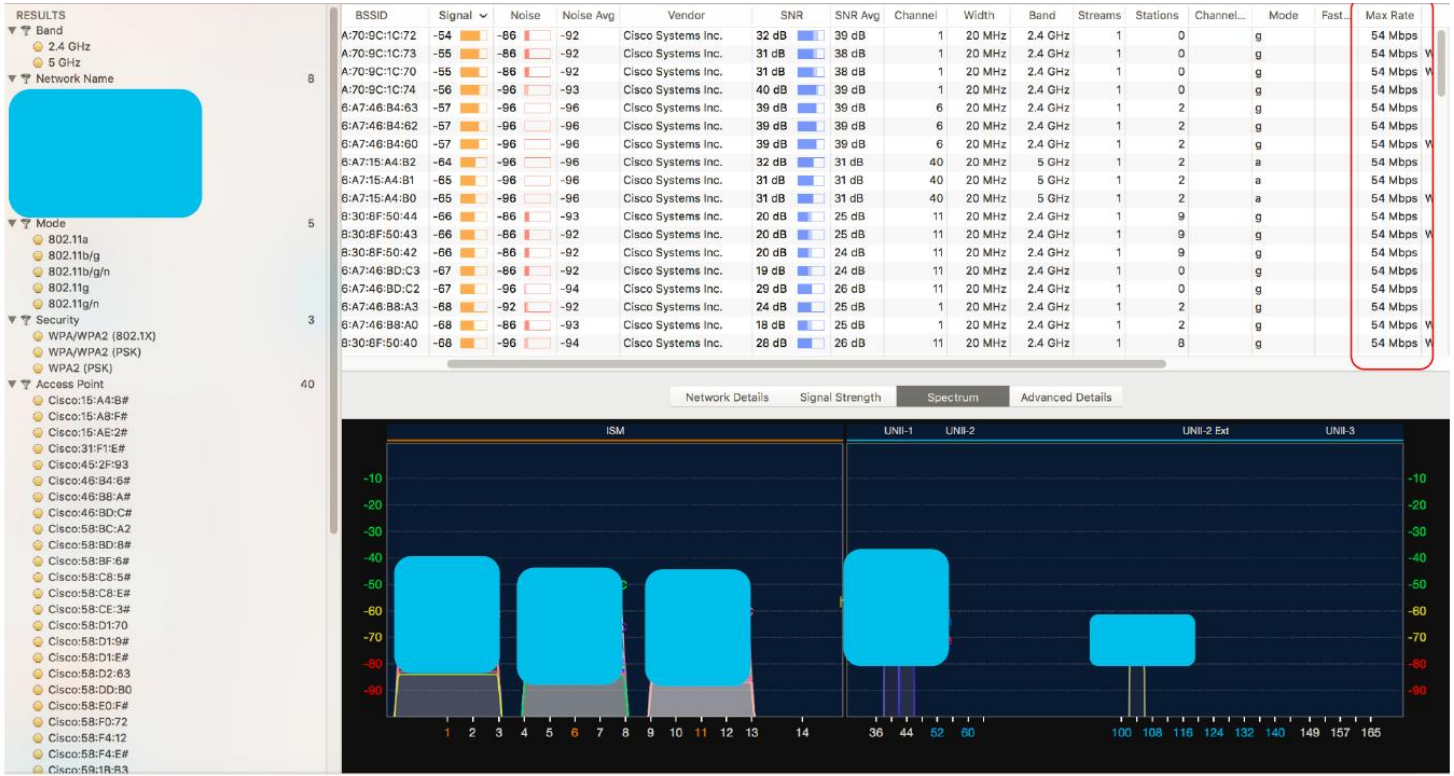




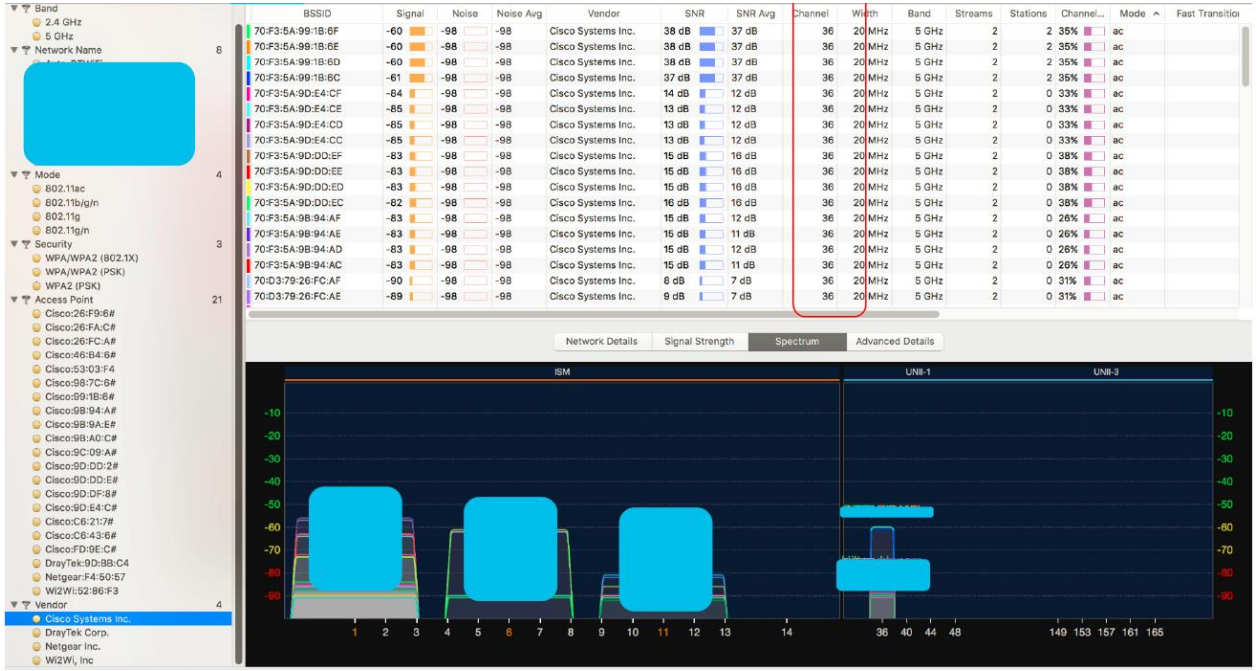
- Vertikalna polarizacija
- Namestitev pod ovirami
- Minimalno 3 m med dvema AP-jema
- Izbira pravih anten – vedno en tip antene
- AP-ji na pravilni višini (optimalno 4 m)
- Ne zaklepajte AP-jev v železne kletke
- Uporabljajte “Outdoor” AP-je za zunanji WiFi

- 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, …)

Pogoste napake - Nadgradnja



Pogoste napake - Nadgradnja



Dobra praksa

- Meritve s tistim AP, ki je predviden za nadgradnjo
- Popravki konfiguracije

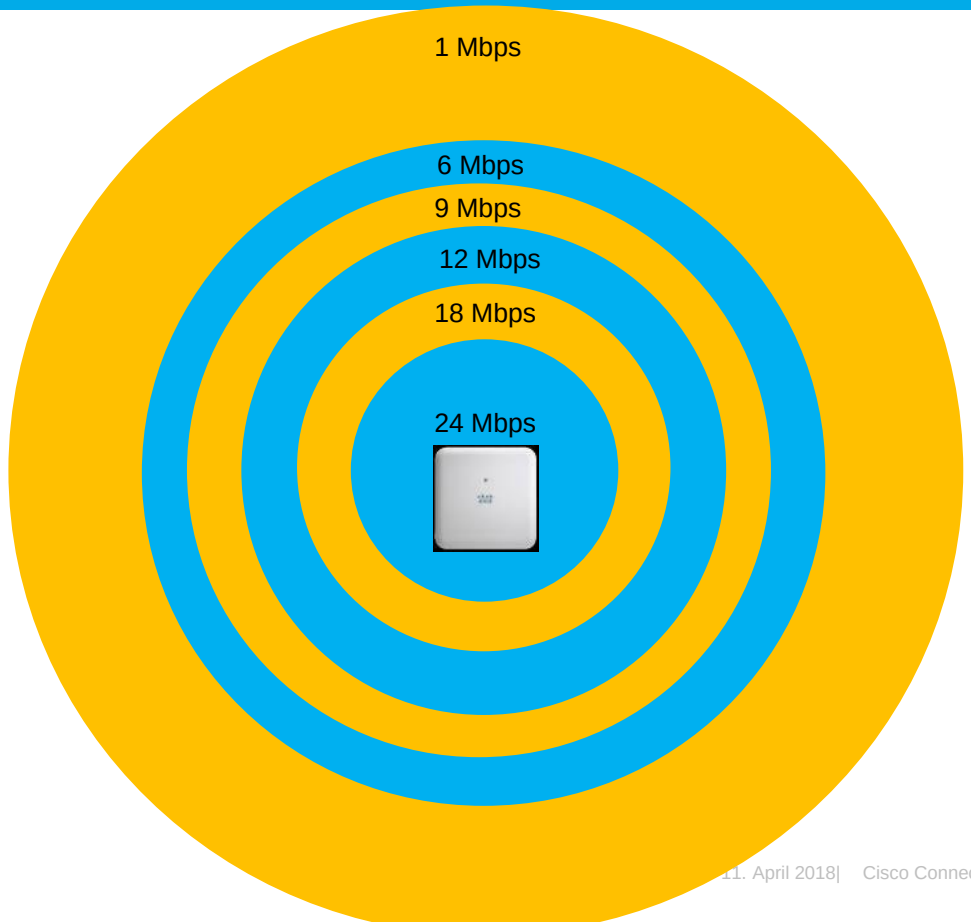
Pogoste napake - Podpora za legacy naprave

Cisco Connect

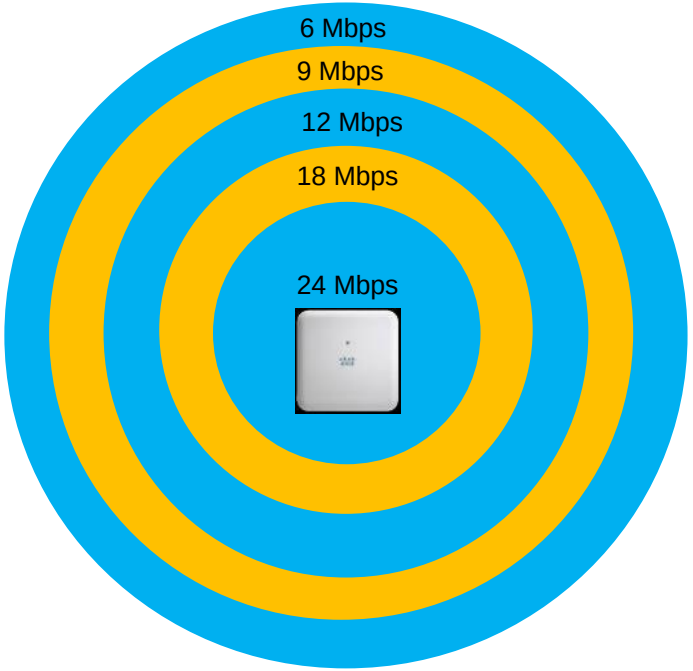
Podpora za legacy naprave:

- Katera vrsta naprav/klientov?
- Kakšna je zmogljivost the naprav/klientov
- Namen uporabe teh naprav/klientov

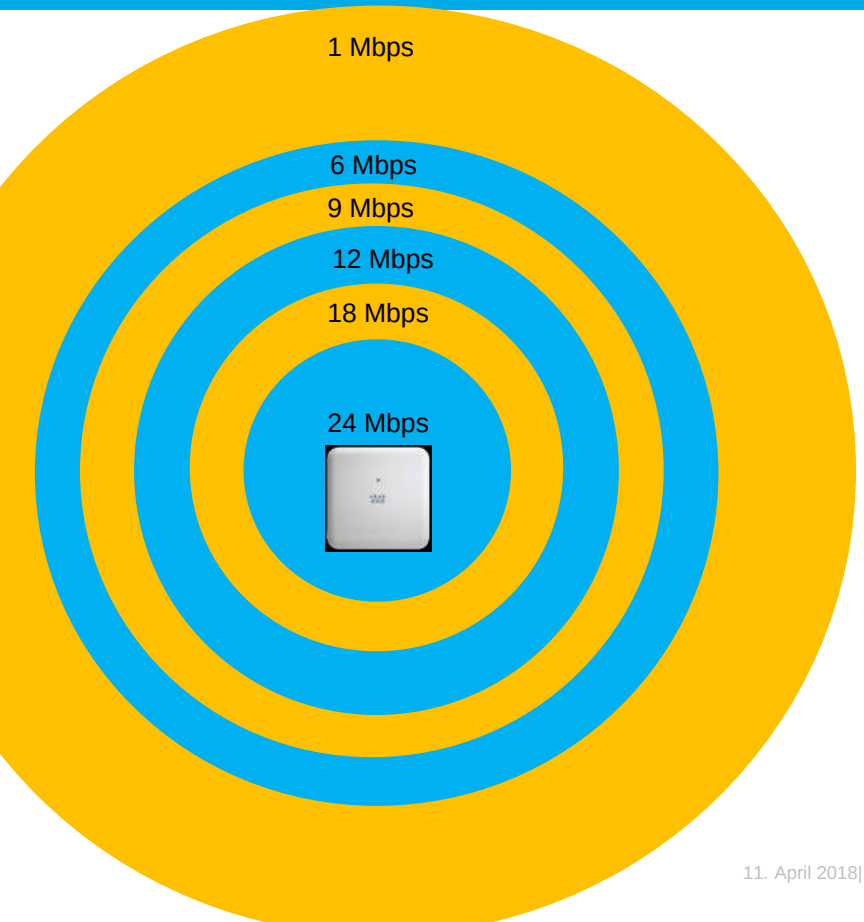
Načrtovanje za pokritost

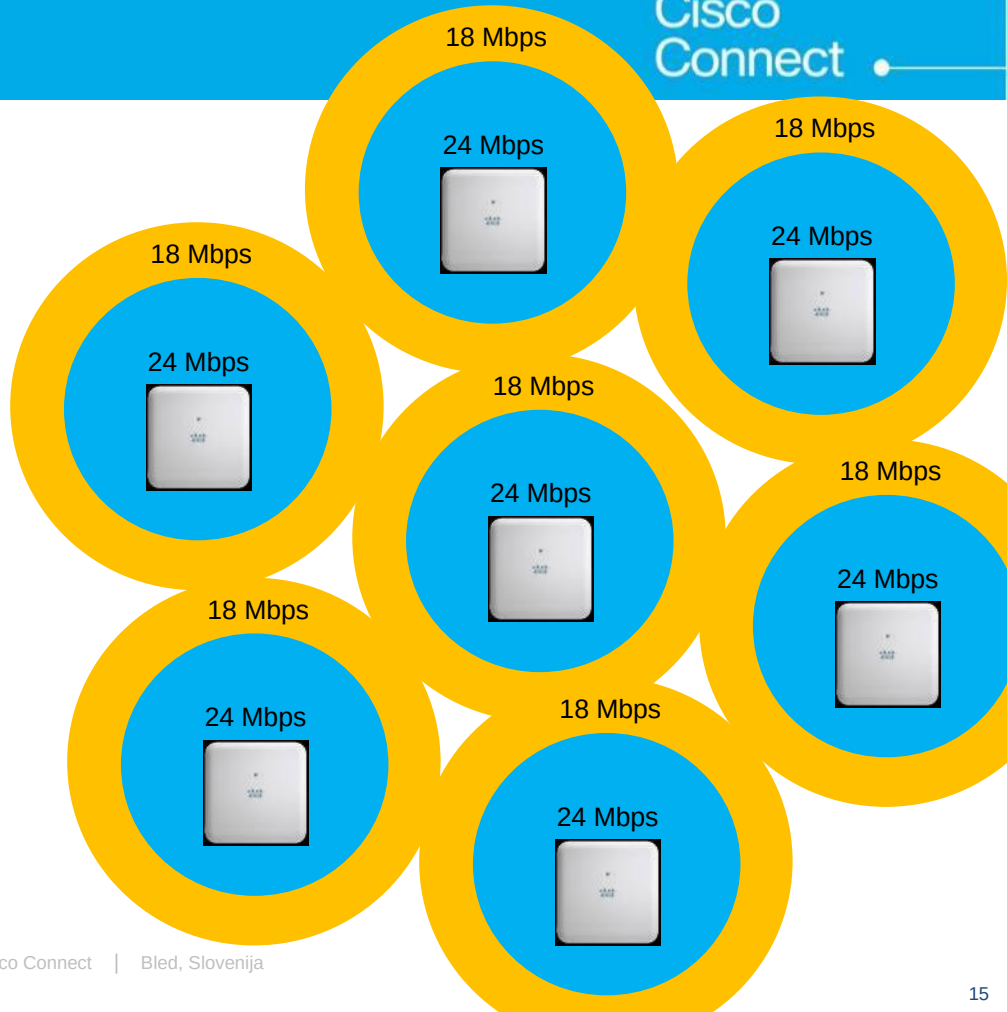


Za optimizacijo WiFi omrežja izklapljamo nižje “datarate”



Načrtovanje za zmogljivost





Načrtovanje – poslušajte arhitekta

Cisco Connect

Ena najbolj pogostih napak ……..

Moramo poslušati arhitekta ……..

…. ki pravi ….

AP-ji so grdi. Moramo jih skriti/namestiti tako, da se jih ne vidi!!

Načrtovanje – poslušajte arhitekta

Cisco Connect

- Kako pa je s tem, zakaj to ni skrito?

KER POTEM NE DELUJE!

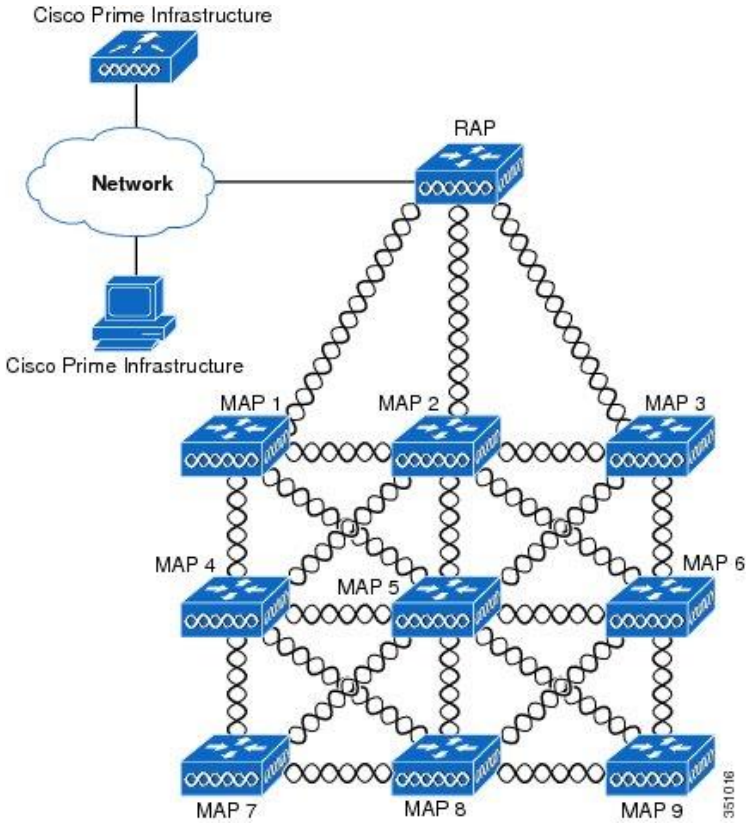
“AHA!!”

Načrtovanje – poslušajte arhitekta

Cisco Connect

AP-ji SO NAMENJENI, DA SERVIRAJO UPORABNIKE, ZATO NAJ BODO TAM TUDI NAMEŠČENI!

Načrtovanje – “Outdoor” in “High-Density” WIFI

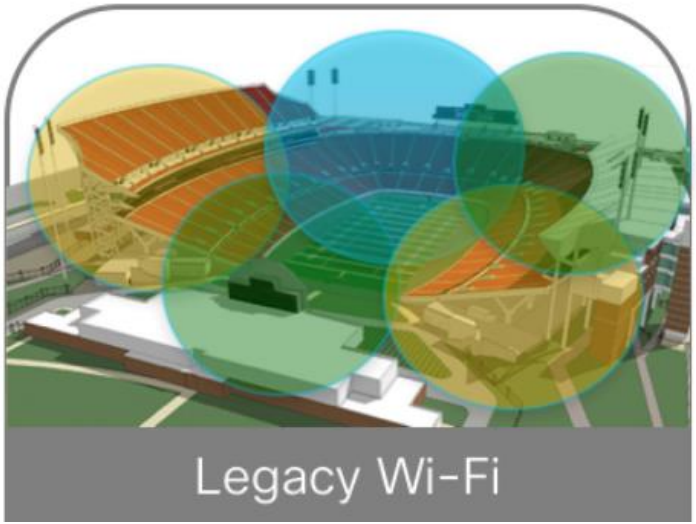


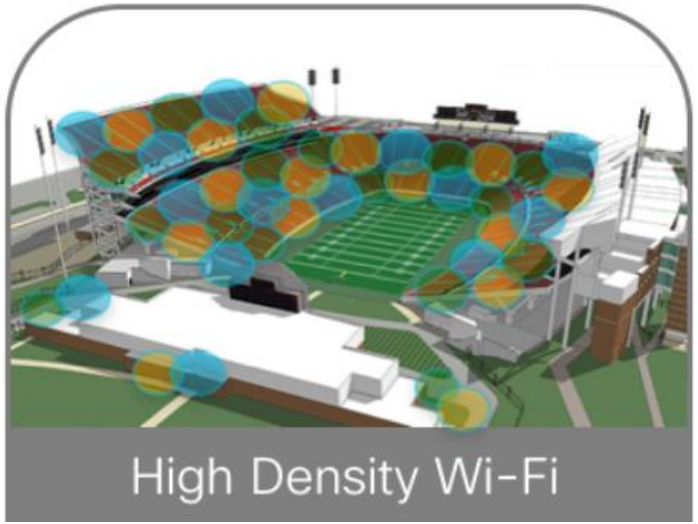
- V zunanjih/outdoor okoljih je veliko motenj, na katere ne moremo vplivati, lahko pa z dobrim načrtovanjem zgradimo WiFi sistem okoli the motenj
- Potrebno je narediti dobre meritve (na višini kjer bodo AP-ji nameščeni in z AP-ji ki bodo na koncu implementirani).
- Potrebno je določiti točke, kjer bodo AP-ji nameščeni (drog javne razsvetljave), potrebno je določiti vire napajanja (stalna faza!)
- Potrebno se je odločiti, ali bo vsaka točka povezana v ožičeno omrežje s svojim kablom, ali bomo gradili MESH sistem (radijske povezave)
- MESH - pomembna vidna linija med AP-ji (po ulicah), sistem je potrebno načrtovati tako, da ima vsak AP najmanj dve poti do ožičenega omrežja, z čim manj skoki (2 – 3 max).
- WIFI sistem ima vgrajen mehanizem, ki računa najbolj optimalno pot do ožičenega omrežja (Gateway/Root) (Adaptive Wireless Path Protocol)

Načrtovanje – “Outdoor” in “High-Density” WIFI

Cisco Connect

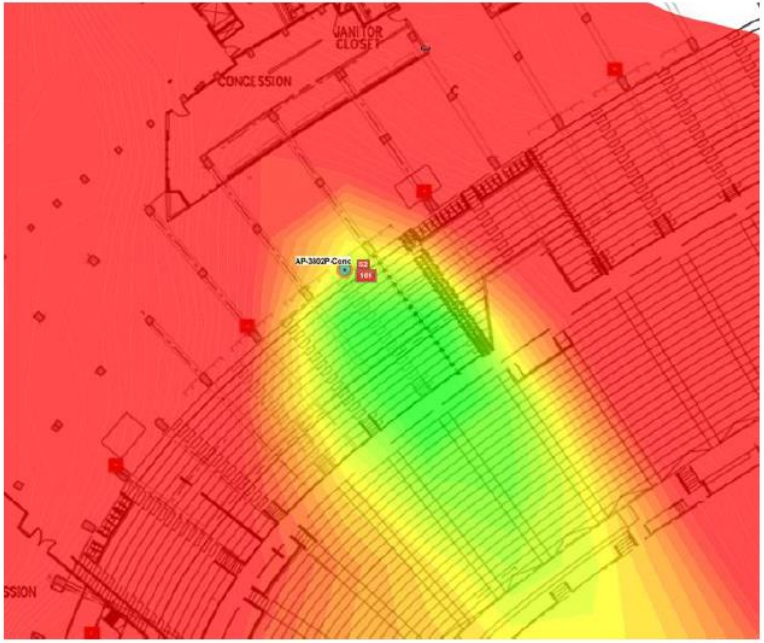
- Kjer je veliko uporabnikov na majhnem prostoru (konferenčne dvorane, stadioni)
- Vsesmerne antene niso najbolj primerne, bolj primerne so usmerjene antene, kjer vsaka antena/AP pokriva točno določeno področje (skupino sedišč)





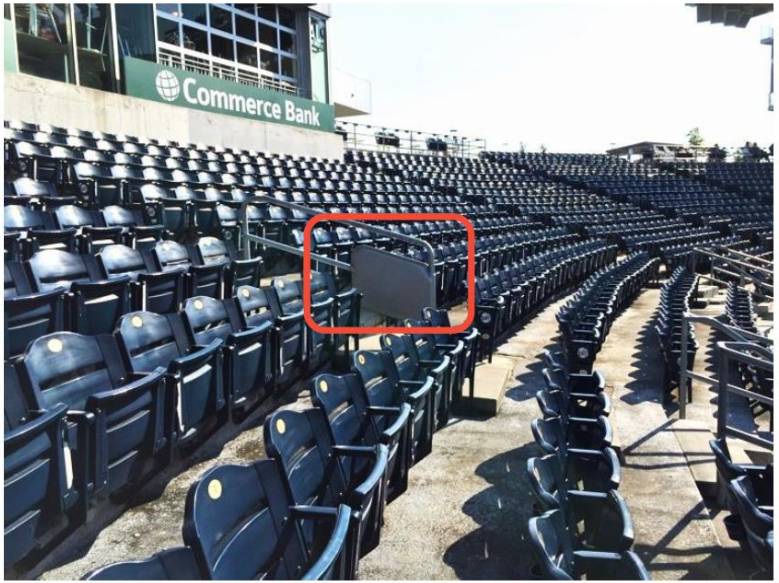
Načrtovanje – “Outdoor” in “High-Density” WIFI

Cisco Connect



Načrtovanje – “Outdoor” in “High-Density” WIFI

Cisco Connect



Varnost - BYOA

Cisco Connect

BYOD

Varnost - BYOA

Cisco Connect

Varnost – BYOA – Bring Your Own AP

BYOA – Kako vpliva na enterprise omrežje?

- Nimamo nobenega nadzora nad napravo
- Naprava ni skladna s politiko podjetja (avtentikacija)
- Naprava ne podpira 802.1x
- Interferenca
- Te naprave so ponavadi nastavljene na Max. Oddajno moč

Napadi na varnostne mehanizme

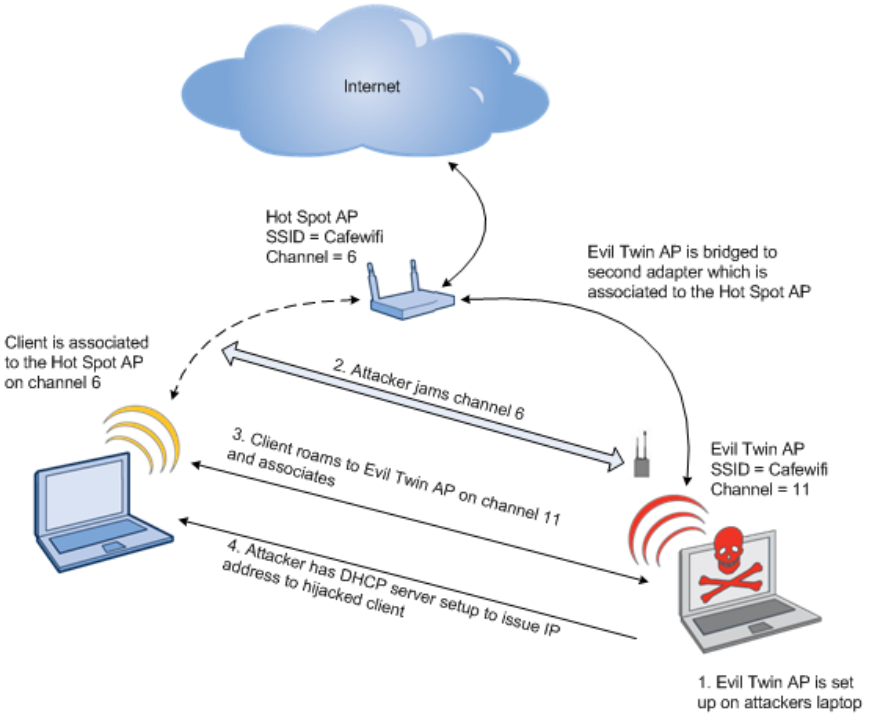
Cisco Connect

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

Primer: Evil Twin – Prevara za pridobitev PSK

Cisco Connect

- 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



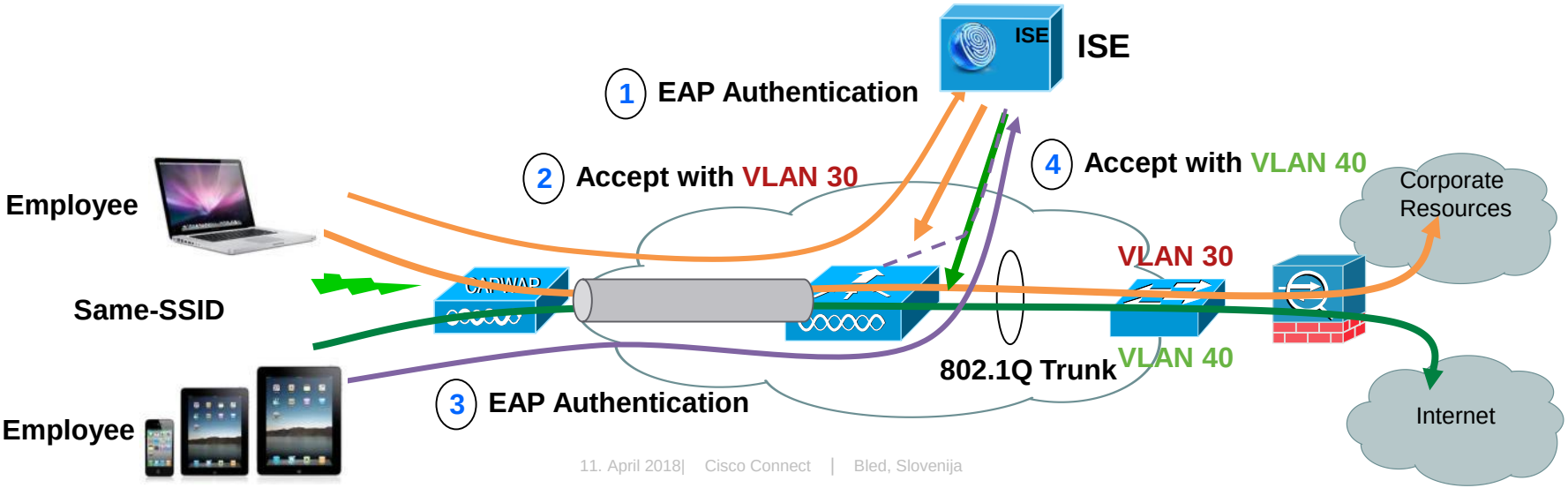
Varnost – Dobra praksa WiFi

Cisco Connect

- 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” (Cisco ISE)
- Na javnih WiFi omrežjih uporabljajte VPN

Primer: Zaščita omrežja (žično in brezžično)

- Uporabniki na istem SSID-ju so lahko razvrščeni v različne VLAN-e po izvedeni avtentikaciji
- Zaposleni, ki uporablja službeni prenosnik z njegovim AD uporabniškim imenom je razvrščen v VLAN 30 in s tem dobi poln dostop do omrežja
- Zaposleni, ki uporablja osebno iNapravo z njegovim AD uporabniškim imenom je razvrščen v VLAN 40 in dobi samo pravice dostopa do interneta



Viri

- www.badfi.com
- www.ciscolive.com
- https://twitter.com/steven_heinsius
- https://twitter.com/emperorwifi
- www.google.com
- www.cisco.com

- Varnostni inženir mora zakrpati 1.000+ ranljivosti
- Hacker mora najti samo eno

Robert Bergles
CEHv9, MCSE⁴, MCITP,MTA,MOS,MCT

Agenda
Windows HACKING

Cisco Connect

- RDP prevzem terminalske seje Windows credential manager
- RDP prevzem terminalske seje s Process explorerjem
- Man-in-the-middle attack
- DHCP starvation
- Kako preprečimo zgornje zlorabe

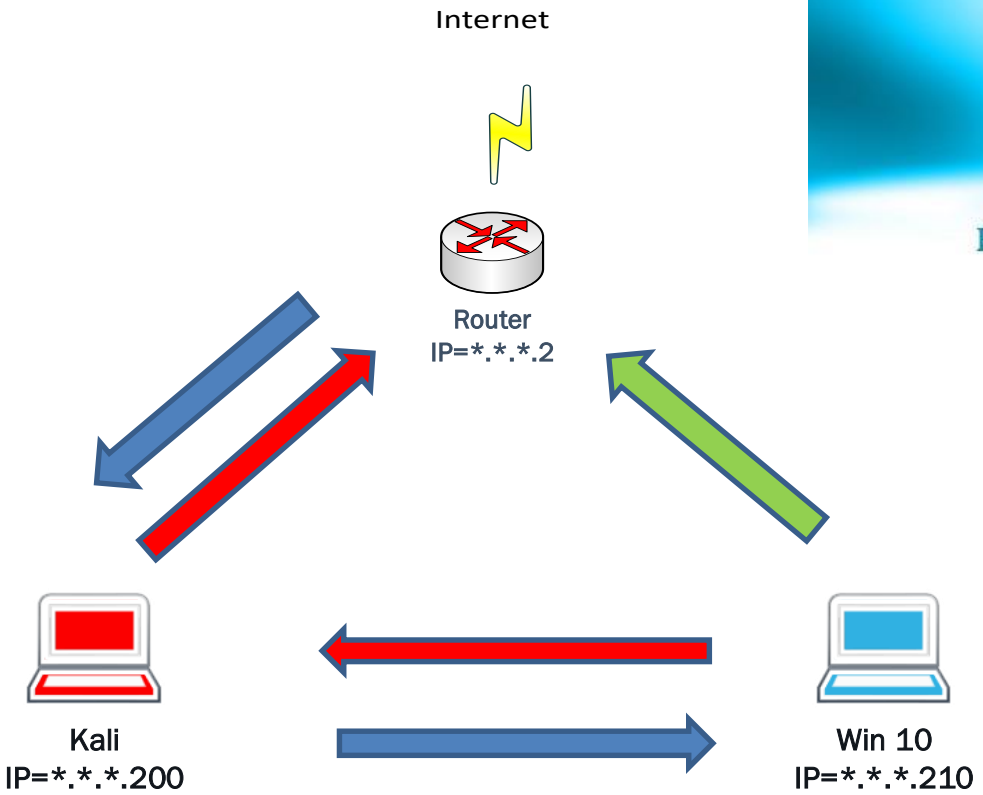
Sedmica "*VZROKI in POSLEDICE*"

Cisco Connect

1. Dopustimo prevzem lokalnih administratorskih pravic na DP
2. Za upravljanje uporabljamo nezaščiten protokol RDP
3. Ne nadgrajujemo ali izločamo starejših operacijskih sistemov
4. Strežnike in delovne postaje upravljamo z Domenskim administratorjem
5. Za večino aktivnih naprav uporabljamo enaka administrativna gesla
6. Ne zaščitimo aktivne opreme in postimo privzete nastavitve
7. Ne uporabljamo BIT lockerja

Man in the Middle

Cisco Connect

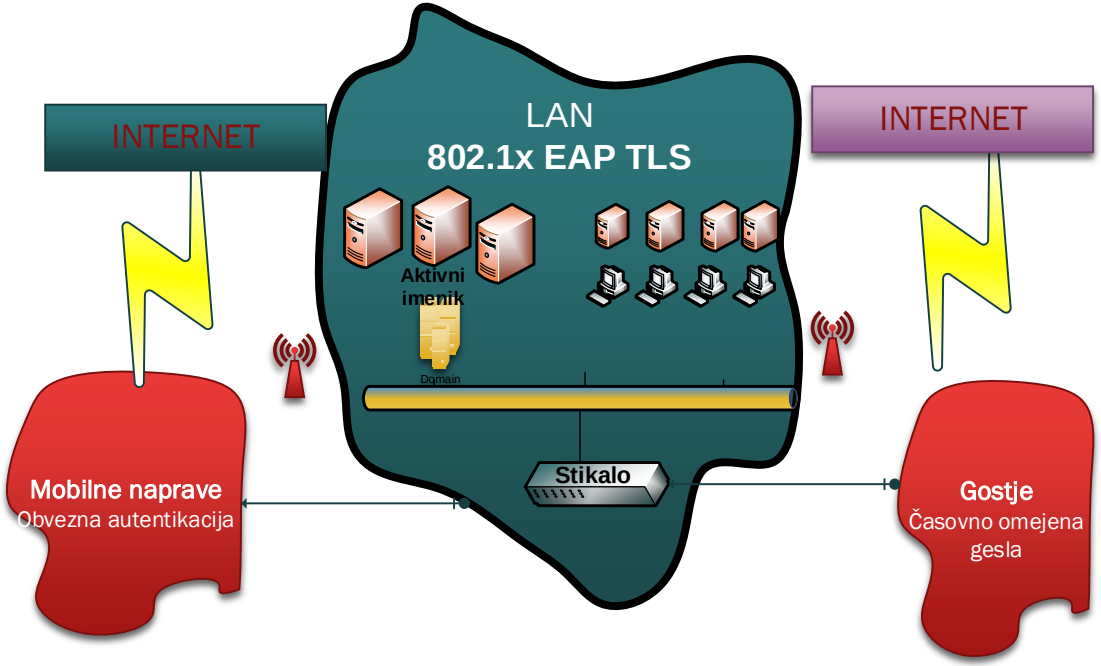


Sedmica REŠITVE

Cisco Connect

1. Na stikalih vklopimo PORT security
2. Na stikalih vklopimo DHCP snooping
3. Na stikalih omogočimo 802.1x
4. Uvedemo BIT locker
5. Izogibamo se RDP protokola za upravljanje
6. Redno nadgrajujemo operacijske sisteme
7. Na delovnih postajah delamo brez privilegijev

Postavitev 802.1x



- **Zaposleni Lan/Wan**
  - 802.1x s certifikati
- **Mobilne naprave zaposlenih**
  - Obvezna autentikacija
- **Gostje**
  - Časovno omejeno geslo

Vedno se najde nekdo, ki je cenejši

www.unistarpro.si