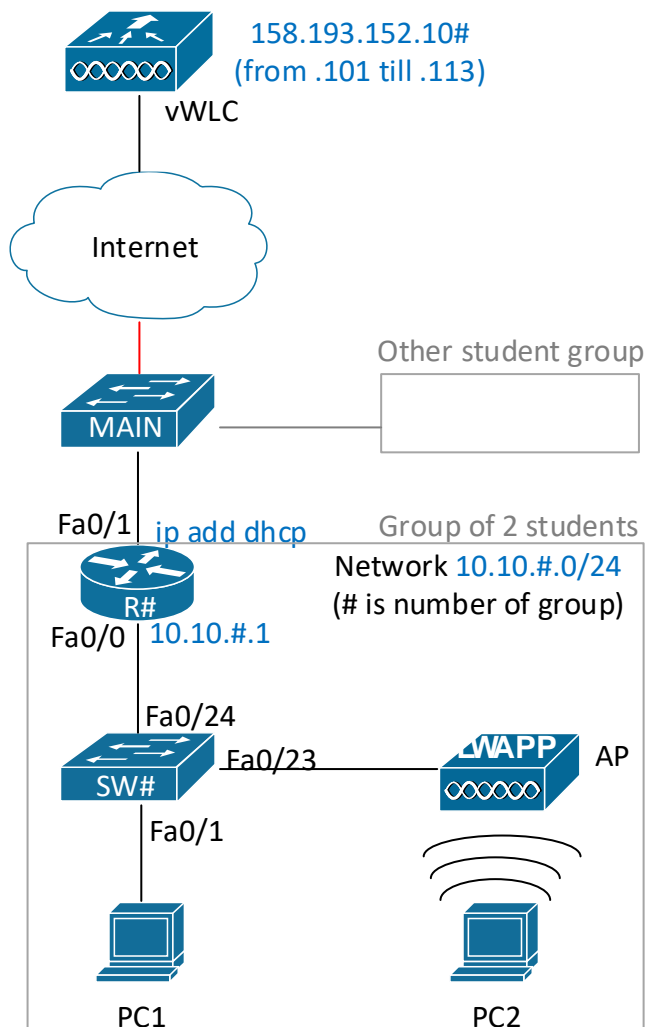


## PS1 / Cvičenie 12 / WLAN

### Topológia



### Scenár

Topológiu môže riešiť **dvojica**, alebo **jednotlivec**:

- K dispozícii v šk. roku 2022/23 je počet **13 virtuálnych WLC** (vWLC) s IP adresami od 158.193.152.101-158.193.152.113
  - Skupina # bude využívať vWLC dostupné na adrese: 158.193.152.10#, t.j. napríklad 158.193.152.101 pre skupinu 1, alebo 158.193.152.113 pre skupinu 13
- Učiteľ priradí každej skupine číslo skupiny, v zadaní ďalej ako #
- Skupina teda môže byť dvojica, alebo jednotlivec
- Pokiaľ je na cvičení 20 študentov, možno vytvoriť 7 skupín ktoré budú dvojice, a zvyšní 6 študenti budú za odmenu pracovať samostatne, ako jednotlivci
- **Modré časti** v texte nižšie je potrebné ukázať inštruktovi pre kontrolu.

### Informácie pre cvičiaceho/inštruktora:

- Virtuálne vWLC majú spravený snapshot z úvodnej konfigurácie, aby na ďalšie cvičenia počas týždňa nebolo potrebné znova manuálne setup-ovať vWLC a ušetril sa čas.
  - IP adresa servera, kde sú nainštalované vWLC a prihlasovacie meno a heslo, sú dostupné v inštruktorskej verzii tohto zadania v kanáli Učiteľa v PS1
- Kroky na **začiatku** cvičenia:
  1. Zariadenia vWLC bootovať po jednom.
  2. Snapshot je pomenovaný "úvodnáKonfigurácia".
  3. Snapshot sa aktivuje jednoducho a to na každom virtuálnom zariadení stačí kliknúť pravým tlačidlom, a dať **restore** snapshot.
  4. Aby vWLC korektne nabootovali je potreba **stlačiť** ľubovoľnú klávesu v konzole na ESXi napríklad **enter** hneď na začiatku bootovania, po zobrazení prvých cca 3 riadkov výpisov. Následne začne vWLC bootovať.
  5. Niekedy sa stane že vWLC zamrzne. Tento stav nastane väčšinou vtedy, keď nestlačíme enter na začiatku bootovania. V tomto prípade treba virtuálne zariadenie otočiť (reload/reset).
  6. Snapshot-y môžu byť využité aj v prípade, ak sa konfigurácia študentov výrazne zamotá, namiesto zdĺhavého hľadania chybné nastavenej položky vo veľmi obsiahlej konfigurácii, je rýchlejšie natiehnúť snapshot a ísť od znova (krok 2).
- Kroky po **skončení** cvičenia:
  - Vypnúť všetky vWLC aby zbytočne nezaťažovali server (Power Off)
  - Snapshot ani vymazanie konfigurácie nie je potrebné robiť, nakoľko na ďalšom cvičení sa bude na začiatku pre istotu na každom vWLC dávať restore.

## Obsah

1. Základné nastavenie smerovača
2. Základné nastavenie prepínača
3. NAT (PAT)
4. Pripojenie na vWLC a systémové akcie
5. Vytvorenie WLAN na vWLC
6. Aktivácia vysielania SSID pre klientov (broadcast SSID)
7. Zabezpečenie WLAN
8. Pripojenie na WLAN
9. Overenie konfigurácie na AP
10. Overenie pomocou wifi aplikácií
11. Pridajte iné nastavenia pre vaše AP cez web GUI vášho vWLC (dobrovoľná úloha)

## Postup

### 1. Základné nastavenie smerovača

- a. Nastavte hostname smerovača na **R#**.
- b. Nastavte na smerovači IP adresy podľa topológie, kde na rozhranie vedúce k svojmu prepínaču nastavíte **prvú** možnú IP adresu z prideleného adresného rozsahu, a rozhranie smerujúce do internetu, nech dostane IP adresu z **DHCP** servera.
- c. Nakonfigurujte na smerovači **DHCPv4** server s poolom adries, ktoré máte uvedené v obrázku s topológiou.
  - i. Vyjmite z pridelovania prvých 5 adries.
  - ii. Ako DNS server posielajte IP adresu smerovača – nakonfigurujete ho neskôr.
  - iii. Nastavte doménové meno: **domain-name wlc.local**.
  - iv. Posielajte aj adresu default routera.
- d. Na smerovači vytvorte **DNS server**
  - i. DNS server je potrebný na preklad mena kontrolera na IP adresu. . Vytvoríme DNS server na smerovači, inak by mohol byť aj na dedikovanom DNS serveri.
  - ii. Nakoľko na predchádzajúcich cvičeniach ani prednáškach sme nepreberali ako vytvoriť na Cisco smerovačoch DNS záznamy, a DNS server, zadajte na smerovač tieto potrebné príkazy:

```
ip dns server
ip dns primary wlc.local soa <ip_address_of_router_R#>
admin.wlc.local 3000 3000 3000 3000
ip host wlc.local ns ns.wlc.local
ip host ns.wlc.local <ip_address_of_router_R#>
ip host CISCO-CAPWAP-CONTROLLER.wlc.local
<ip_address_of_your_vWLC>
ip host CISCO-LWAPP-CONTROLLER.wlc.local
<ip_address_of_your_vWLC>
ip name-server 1.1.1.1
ip name-server 1.1.1.3
```
  - iii. Význam konfiguračných príkazov je nasledovný:
    - `ip dns server` aktivuje DNS server na zariadení
    - `ip dns primary wlc.local soa <ip_address_of_router> admin.wlc.local 3000 3000 3000 3000` nastavuje, že zariadenie je primárnym DNS serverom pre zónu `wlc.local`, autoritatívnym zdrojom sa stáva v našom prípade router, čísla v príkaze sú časovače na refresh, retry, expire ttl a minimum ttl
    - `ip host` definuje statické mapovanie na IP adresy
    - `ip name-server <ip_address>` nastavuje DNS server na poskytovanie ďalších DNS záznamov
- e. Na smerovači nakonfigurujte **SSHv2**

### 2. Základné nastavenie prepínača

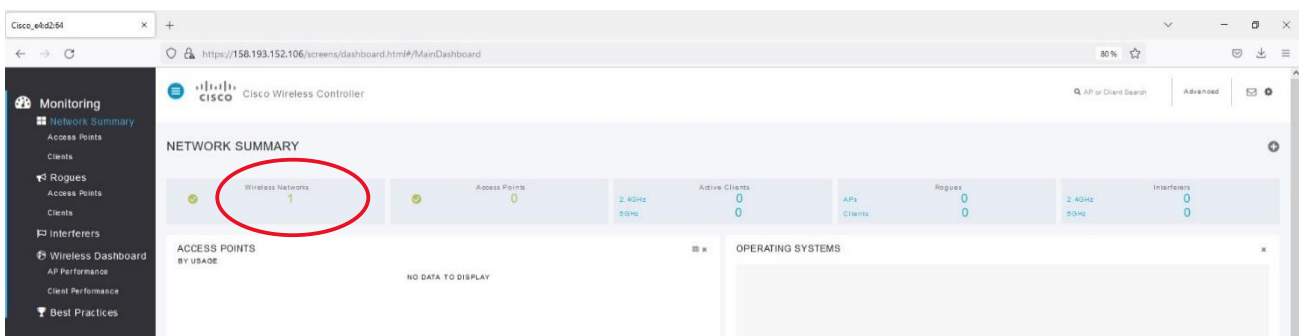
- a. Zabezpečte, aby bol prepínač v defaultnom nastavení a prázdny
- b. Zapnite RapidSTP
- c. Voliteľne: rozbehnite remote login

### 3. NAT (PAT)

- Na PC1 nastavte IP adresu manuálne/staticky z prideleného IP rozsahu, najvyššiu možnú (.254), doplňte masku, default GW a overte konektivitu k vášmu smerovaču.
- Nakonfigurujte na rozhraní smerovača smerujúcom do internetu NAT typu PAT.
  - Zabezpečte, aby sa celý váš privátny rozsah prekladal na IP adresu, ktorú ste cez DHCP získali na vonkajšom (hornom) rozhraní vášho smerovača
  - Správne zadefinujte rozhrania ako vstupné a výstupné
  - Overte konektivitu do internetu z PC1, skontrolujte NAT prekladovú tabuľku na smerovači, aj smerovaciu tabuľku
- Nastavte na PC1 teraz IP adresu dynamicky z DHCP, skontrolujte priradenú adresu, a zopakujte predošlý krok b. iii.

### 4. Pripojenie na WLC (vWLC) a systémové akcie

- Na WLC sa pripojíte pomocou webového prehliadača cez `https://158.193.152.10#` (píšte `https://` keďže WLC používa `https`; do URL zadáte pridelenú IP adresu `158.193.152.10#`, pre skupinu 1 dajte `.101`, pre skupinu 13 dajte `.113`).
- Do WLC sa prihlásite pomocou účtu:
  - Meno:** admin
  - Heslo:** Class123
- Kliknite na Wireless Networks**



- Aktivujte licenciu:
  - karta **MANAGEMENT**, zvislé menu vľavo **Software activation – Licenses – ap\_count**, License status: Active, tlačidlo **Set Status**.

Management

Summary

SNMP

HTTP-HTTPS

IPSEC

Telnet-SSH

Serial Port

Local Management Users

User Sessions

Logs

Mgmt Via Wireless

Cloud Services

Software Activation **1**

Licenses

License Usage

License Type

Tech Support

Licenses

Add License

License Count

License	Type	Time(expires)	RTU Count	Status
<b>2</b> ap_count	Evaluation	12 weeks, 5 days	200	Active, Not-In-Use

MONITOR WLANs CONTROLLER WIRELESS SECURITY **MANAGEMENT** COMMANDS HELP

Save Configuration

Management

License Detail

Name ap\_count

Type Evaluation

Version 1.0

Expires 12 weeks, 5 days

Built-In License Yes

Current Status Active, In-use

License Status

Summary

SNMP

HTTP-HTTPS

IPSEC

Telnet-SSH

Serial Port

Local Management Users

User Sessions

Logs

Mgmt Via Wireless

Cloud Services

Software Activation

Licenses

License Usage

License Type

Tech Support

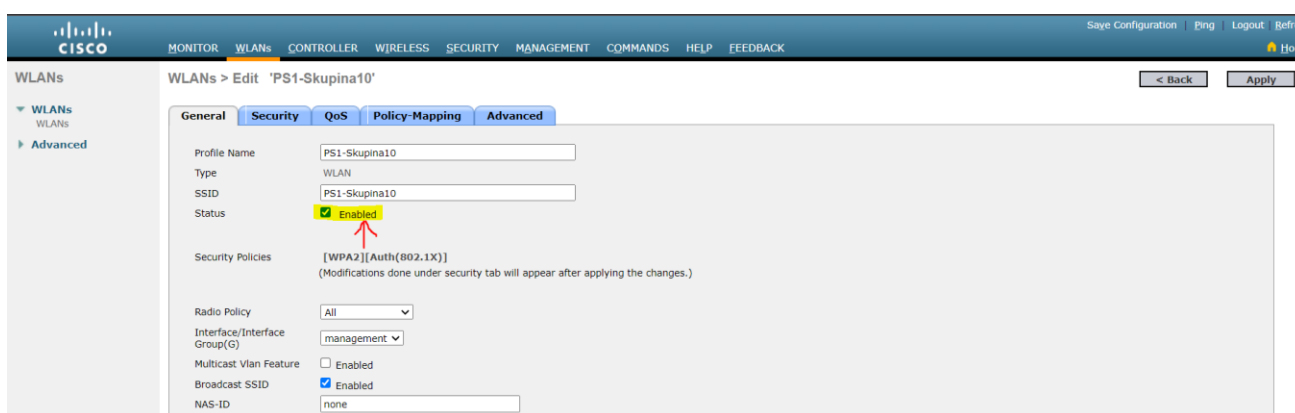
- e. Na AP nastavte starší dátum (medzi rokom 2016 a 2021), aby nebol problém s neplatným certifikátom
- Pripojte počítač na konzolový port AP
  - Prihláste sa menom a heslom: Cisco/Cisco
  - Vstúpte do privilegovaného módu: enable, Cisco
  - Pozrite si podporované príkazy, verziu operačného systému a nastavený čas:
    - ?
    - sh ver
    - sh clock
  - Nastavte dátum
    - clock set 9:00:00 15 Non 2020
    - sh clock

## 5. Vytvorenie WLAN na WLC

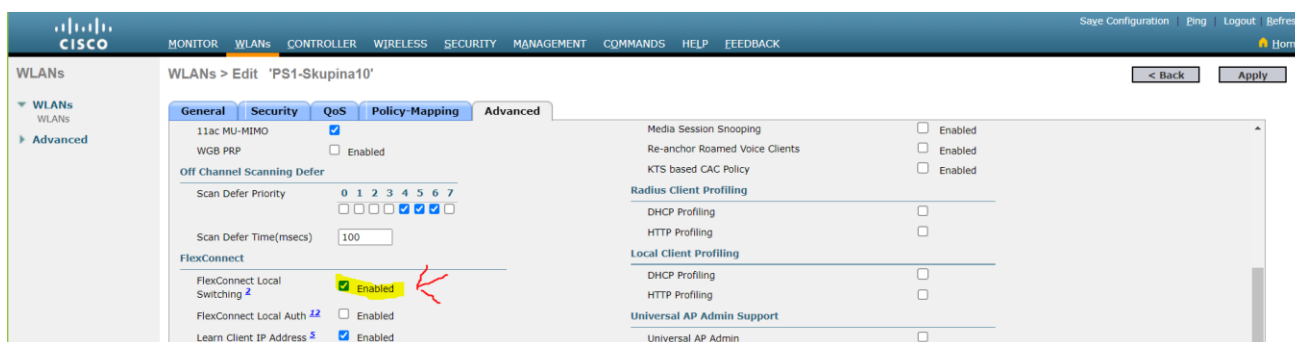
- a. WLANy na WLC vytvárame v menu WLANs. Vytvorte WLAN kde:
  - i. V **Profile Name** zadajte názov PS1-Skupina# (napríklad PS1-Skupina10)
  - ii. Ako **SSID** zvolíte názov PS1-Skupina#
  - iii. **ID** vyberte podľa čísla vašej skupiny (napríklad 10)
  - iv. Stlačte tlačidlo **Apply** (v pravom hornom rohu).



- b. Zapnite WLAN (pri nápis **Status** zaškrtnite políčko **Enable**), aby s ňou dokázal kontrolér pracovať. Stlačte tlačidlo **Apply**.



- c. V záložke **Advanced** zapne funkcionality **FlexConnect Local Switching** (aby AP vedel zabezpečovať komunikáciu medzi lokálne pripojenými klientami, aj keď stratí konektivitu na WLC). Stlačte tlačidlo **Apply**.



## 6. Aktivácia vysielania SSID pre klientov (broadcast SSID)

- a. Aby pre klientov boli viditeľné dostupné wifi siete (s danými SSID), je potrebné:
  - i. V záložke **WIRELESS** otvoriť náš registrovaný Access Point.  
Upozornenie: Ak sa vám nezobrazuje Access point, tak v AP dajte príkaz v privilegovanom móde:  
**capwap ap restart .**

```

COM1 - PuTTY
AP843d.c6a9.751c#capwap ?
  ap  lwapp ap commands

AP843d.c6a9.751c#capwap ap ?
  ant-band-mode      antenna band mode
  ap-group           AP group configurations
  auth-token         SSC auth token config
  controller         lwapp primary controller
  daisy-chaining     daisy-chaining enable/disable
  dot1x              Configure the dot1x username and password
  easy-config        Set AP easy-config status
  ethernet           Configure ethernet parameters like vlan tag id
  hostname           Configure ap hostname
  ip                 lwapp ap ip command
  log-server         Configure the syslog server where all LWAPP errors will be
                    logged
  mode               Configure an AP mode
  pppoe              Change AP sub-mode to PPPoE
  preferred-domain   Configure the preferred domain used for DNS based
                    controller discovery
  preferred-mode     capwap mode of operation ipv4 or ipv6
  primary-base       Primary Controller
  primed-timer       primed-timer enable/disable
  restart            Restart CAPWAP Protocol
  secondary-base     Secondary Controller
  tertiary-base      Tertiary Controller

AP843d.c6a9.751c#capwap ap re
AP843d.c6a9.751c#capwap ap restart
AP843d.c6a9.751c#capwap ap restart
restart capwap
AP843d.c6a9.751c#
AP843d.c6a9.751c#
AP843d.c6a9.751c#
AP843d.c6a9.751c#
AP843d.c6a9.751c#
Dec  8 14:21:42.079: %EVT-4-WRN: Write of flash:/event.capwap done
Dec  8 14:21:42.131: %LWAPP-3-CLIENTERRORLOG: Switching to Standalone mode
Dec  8 14:21:42.155: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to 158.193.152.102:5246
Dec  8 14:21:42.159: %WIDS-6-DISABLED: IDS Signature is removed and disabled.
Dec  8 14:21:52.159: AP has SHA2 MIC certificate - Using SHA2 MIC certificate for DTLS.

Dec  8 14:21:52.000: %CAPWAP-5-DTLSREQSEND: DTLS connection request sent peer_ip: 158.193.152.106 peer_port: 5246
Dec  8 14:21:52.003: %CAPWAP-1-SSC_CERT_AUTH_FAILED: Failed to authorize controller, SSC certificate validation failed.
Dec  8 14:21:52.247: %CAPWAP-5-DTLSREQSUCC: DTLS connection created successfully peer_ip: 158.193.152.106 peer_port: 5246
Dec  8 14:21:52.247: %CAPWAP-5-SENDJOIN: sending Join Request to 158.193.152.106
Dec  8 14:21:52.423: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface Dot11Radio1 due to the reason code 21
Dec  8 14:21:52.443: %LWAPP-4-CLIENTEVENTLOG: OfficeExtend Localssid saved in AP flash
Dec  8 14:21:52.627: %LINK-6-UPDOWN: Interface Dot11Radio1, changed state to down
Dec  8 14:21:53.027: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset
Dec  8 14:21:53.183: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller Cisco_e4:d2:64
Dec  8 14:21:53.251: %LWAPP-3-CLIENTERRORLOG: Switching to Connected modecapwap_delete_all_l2Acls_in_nacl_list:336. Deleting all L2Acls in AP config
Dec  8 14:21:53.287: %DOT11-5-EXPECTED_RADIO_RESET: Restarting Radio interface Dot11Radio0 due to the reason code 10
Dec  8 14:21:53.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface Dot11Radio1, changed state to down
Dec  8 14:21:53.867: %LINK-6-UPDOWN: Interface Dot11Radio1, changed state to up
Dec  8 14:21:53.875: %LINK-6-UPDOWN: Interface Dot11Radio0, changed state to down
Dec  8 14:21:53.883: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to reset

```

ii. A potom na WLC dajte (vpravo hore) **Refresh**.

Poznámka z cvičenia: AP sa najprv skúša pripojiť na .102, potom správne na .106, pre skupinu #=6.

AP sa zaregistuje – vidno ho na WIRELESS karte.

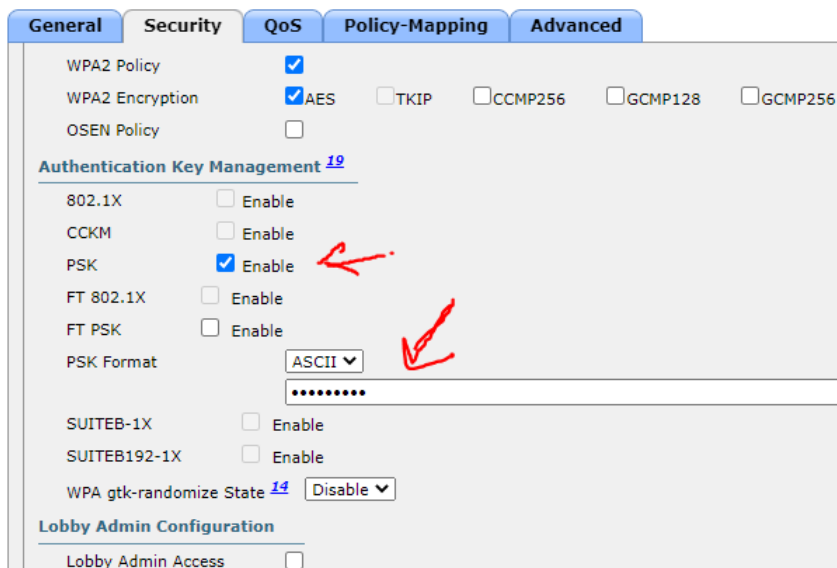
b. Následne treba na karte General v položke **AP mode** vybrať **FlexConnect** (to zapne posielanie SSID). Potom stlačte tlačidlo **Apply**.

## 7. Zabezpečenie WLAN

- Kliknite na WLAN a potom na WLAN ID. V záložke **Security** nastavujeme zabezpečenie WLAN.
- Nastavte zabezpečenie WLAN na WPA2 kde:
  - V **Layer 2 Security** vyberte **WPA+WPA2**
  - Zaškrtnite **WPA2 Policy**
  - Ako autentifikačnú metódu **Authentication Key Management** - vyberte **PSK**, kde ako heslo zadajte v ASCII tvare heslo: **#Cisco123** kde # je číslo vašej skupiny. Potom dajte **Apply**.

Pokračovanie predošlého screen shotu:





## 8. Pripojenie na WLAN

- a. Pomocou mobilného zariadenia sa pripojte na vašu WLAN. V prípade že sú v laboratóriu externé wireless sieťové karty, môžete využiť aj pripojenie pomocou nich.
  - i. K dispozícii v šk. roku 2022/23 máme **14 tp-link USB wifi kariet**, ktoré máme zapožičané od vyučujúcich predmetu ZBS. Budú k dispozícii v RB303 počas týždňa, keď sa realizuje toto cvičenie na PS1, v papierovej krabici.
  - ii. Jedno pre každú skupinu, vyžiadať si od vyučujúceho, a **nezabudnite vrátiť**.

## 9. Overenie konfigurácie na AP

- a. V záložke **WIRELESS** vyberte znovu váš registrovaný Access Point. Následne zvolte záložku **Credentials** kde si nastavíte prístupové údaje.
- b. Pripojte si konzolový port z počítača do Access Pointu.
- c. Prihláste sa pomocou prihlasovacích údajov z kroku a.
  - i. Cisco IOS je na Access Pointoch a vWLC trocha odlišný od toho, na ktorý ste zvyknutý zo smerovačov a prepínačov.
  - ii. Nakoľko úlohou tohto cvičenia je zoznámenie sa so základným nastavením AP a kontroléra, odporúčame sa skôr zamerať na show výpisy. Vo výpise **sh capwap ip config** – pozrite IP primárneho kontrolera, ktorú si načítal po naboťovaní (LWAPP Static IP Configuration, Primary Controller 158.193.152.102 ?). (Pozrite kde sa dá znížiť výkon AP)
  - iii. Priestor na pokročilejšie konfigurácie bezdrôtových sietí budete mať na predmete základy bezdrôtových technológií (ZBS).

## 10. Overenie pomocou wifi aplikácií

- a. V prípade, že počítače v laboratóriu obsahujú Wireless sieťové karty, môžete konfiguráciu overiť pomocou programu **WirelessNetView** a skontrolujte či vaša „wifi“ je nastavená na daný kanál vysielania. Na overenie môžete využiť aj aplikácie pre mobilné zariadenia, napríklad **Wifi analyzer** a jemu podobné aplikácie.

- i. Link pre stiahnutie WirelessNetView (nie je potrebná inštalácia) na PC s wifi kartou: [https://www.nirsoft.net/utils/wireless\\_network\\_view.html](https://www.nirsoft.net/utils/wireless_network_view.html)
- b. Overte konektivitu medzi PC1 a PC2 a z oboch do internetu.

**11. Pridajte iné nastavenia pre vaše AP cez web GUI vášho vWLC (dobrovoľná úloha)**

- a. V prípade že Vám zvýšil čas, môžete experimentovať s nastaveniami na vašom vWLC, a následne sledovať efekt na vašom AP a pripojených wifi klientoch.
- b. Učiteľ môže za zaujímavé a funkčné riešenie prideliť bonusový bod, a rozšíriť toto zadanie o novú úlohu, ktorej zadanie pridá pred tento bod 11, a súčasný bod 11 sa posunie ako bod 12.