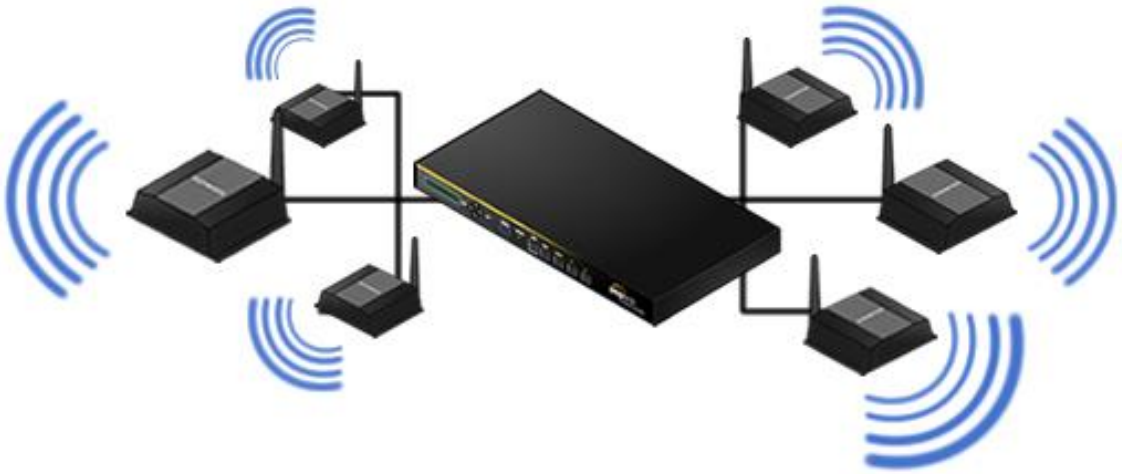
SZÉCHENYI ISTVÁN EGYETEM
GYŐR
TÁVKÖZLÉSI TANSZÉK

Kontrolleres WLAN alapok
-
„Controller-less” architektúra vizsgálata



2013.04.05.
Készítette: Drotár István

1. Mérés célja

A mérés során a hallgató megismerkedik a WLAN architektúra új technológiáival, ezáltal a „hagyományos” WLAN hiányosságaival is. Mindezek után ellenőrző kérdésekre adott választ követően felkonfigurál Controller-less alapú architektúrában több WLAN hálózatot és vizsgálja azok működését, paraméterezési lehetőségeit.

(A mérés során Aruba Networks IAP-93 típusú hozzáférési pontok kerülnek üzembe állításra és vizsgálatra a már meglévő háttér infrastruktúrát felhasználva.)

2. Elméleti összefoglaló

Az Enterprise („vállalati”) Wi-Fi

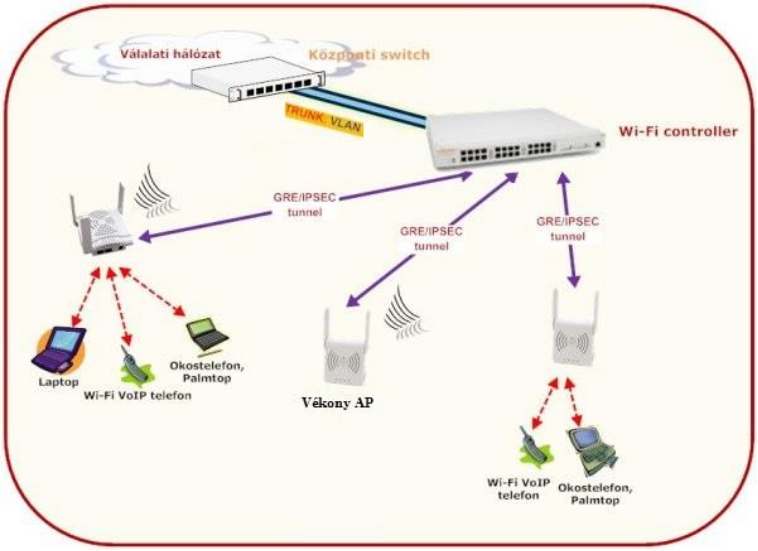
Az elmúlt években a WLAN technológiák olyan mértékben fejlődtek, hogy alkalmassá váltak a kábeles hálózatok kiváltására. A megbízhatóság, biztonsági funkciók, menedzselhetőség és megnövekedett adatátviteli sebesség kritériumainak az Enterprise WLAN megoldások megfelelnek, és nem utolsó sorban felülmúlják a vezetékes LAN hálózatokat költség-hatékonyság szempontjából.

Hagyományos vs. Enterprise

A széles körben elterjedt és mindenki számára ismert hagyományos Wi-Fi berendezések kiválóan használhatóak SOHO környezetben néhány kliensig, viszont alkalmatlanok egy nagyobb igényű hálózat kiszolgálására (megfelelő biztonság, jó minőségű, magas rendelkezésre állás mellett).

(Néhány kérdés a cinikusokhoz:
Képesek-e összehangolni a rádiófrekvenciás működést, követni a rádiófrekvenciás környezet állandó változásait, dinamikusan kezelni a különböző kliensek különböző adó/vevő teljesítményét, megoldani a roamingot, hálózatbővítés esetén a manuális konfigurálás nélkülözését? - Erre csak az Enterprise/”vállalati” WLAN megoldások képesek)

Enterprise WLAN technológiák (Controller és Controller-less WLAN)



Fat AP, vagy autonóm AP-k voltak az első típusú hozzáférési pontok Ezek tökéletes kisméretű vezeték nélküli helyi hálózati megoldások (max. 10-15 kliens/AP) vagy "hot-spot" típusú szolgáltatásokhoz (autonóm AP). Minden fat AP-t manuálisan kell konfigurálni mind hálózati részről, mind a biztonsági beállításokat tekintve. Ezek alapján jó megoldás, ha csak néhány AP-val rendelkező hálózatot tervezünk, azonban nem biztosított a skálázhatóság illetve az illeszthetőség. A probléma a hagyományos Wi-Fi architektúrából fakad. A hagyományos Wi-Fi ugyanis szigetmegoldás. A felhasználó magához az AP eszközhöz csatlakozik, és kapcsolatát az AP eszköz terminálja, így szükség van a változásra.

Az Enterprise megoldás a hagyományos WLAN architektúrával szemben egészen más módon működik. Ezen WLAN architektúra az AP eszközökön felül tartalmaz egy kontrollert is, amely a hozzáférési pontok menedzsment feladatait látja el. Ez volt az elsődleges evolúciós pont a vállalati Wi-Fi tekintetében.

A kontroller konszolidált menedzsmentet tesz lehetővé a teljes vezeték nélküli hálózatra egy helyen. Biztosítja, hogy a hozzáférési pontok automatikusan igazodni tudjanak a rádiós környezethez, csatornát vagy adáserősséget váltsanak, vagy szabályozzák a kliensek működését. Azonban ez az infrastruktúra még nem teszi egyszerűbbé a hálózathoz illeszthetőséget, ezért az AP-okra érkező adatforgalmat egy tunel-en keresztül a kontrollerre irányítja (VLAN tekintetében a kontrollert egy trunk portra csatlakoztatva, megfelelő VLAN-ba irányítódik a tunel-ben érkező adatforgalom). Ezzel a funkcióval biztonságosan szétválaszthatóak az egyes SSID-k, a felhasználók adatforgalma, ezáltal az illeszthetőség biztosított. A csomagoknak mindenképpen a hálózatba kell jutniuk, és a kontroller az egyetlen pont, ahol központilag szabályozható, hogy milyen csomagokat engedünk be a hálózatba. Az egyetlen hátrány a késleltetés lehet, azonban ez csak technológia kérdése.

A tunel-alapú megközelítés egyszerűbbé teszi a menedzsmentet és az illeszthetőséget. Architekturális szempontból azonban további változás igényeltetik, mivel a felhasználó még mindig közvetlenül az AP eszközhöz csatlakozik (fat AP). Erre ad megoldást a vékony AP (thin AP, lightweight AP) architektúra, ahol a legtöbb hálózati funkciót nem az Access Point végzi.

A teljesen *Vékony AP alapú infrastruktúrában* a felhasználók a központi vezérlést megvalósító wireless kontrollerhez csatlakoznak. A vékony AP egyszerűen egy hozzáférési pont, amelyet a WLAN vezérlő irányít, fogadják a csomagokat, és terminálás nélkül, titkosított kapcsolaton keresztül továbbítják a csomagokat a kontrollerhez. Minden intelligencia és adat a kontrollerben található.

Az üzemmódból számos előny következik:

- A kontrollernek nincs szüksége az AP eszközök lekérdezésére,
- minden pillanatban ismeri az AP és a kliens eszközök környezetét és képes beavatkozni,
- a kliens eszközöket is képesek vezérelni – csatorna / AP-váltás / adóteljesítmény változtatás.

Maguk a WLAN kontrollerek rack-be szerelhető fizikai eszközök, amely egyszerre kommunikál minden egyes AP-val. Ez lehetővé teszi egyidejűleg több AP könnyű és gyors konfigurálását anélkül, hogy manuálisan kellene beállítani minden egyes eszközt. Ugyancsak nincs szükség a vezetékes hálózat újraszervezéséhez, hogy fogadja a WLAN hálózatot. Ahogy azt feltételezzük a skálázhatóság jelentősen javult a WLAN kontroller hozzáadásával, mert a hálózat könnyen lehetővé teszi a telepítést több AP-ra, csökkenti a telepítési és kezelési bonyolultságot.

A következő technológiai újítást, áttörést a *kontroller nélküli hozzáférési pontok* jelentették a mai WLAN technológiában. Eleinte kérdéses volt a technológia létköre, köszönhetően az elnevezésnek „kontroller nélküli", hiszen a központosított menedzselhetőség, skálázhatóság rengeteg előnnyel jár és megkönnyíti a rendszergazda életét. De nem kell aggódni, a WLAN vezérlő nem „megy” sehova. Az elmúlt néhány év nagy technológiai fejlesztései a WLAN szegmenst is elérték. Az egyik ilyen a virtualizáció, melyet a gyártók már elkezdtek implementálni eszközeikbe, mivel előrelépés történt a hozzáférési pontok hardveres felépítésében is (chipset, memória, stb). Ezek együttesen lehetővé tették, hogy a kontroller virtualizált szoftver formájában fusson az eddigi „öreg” vékony AP-kban. Ez egy hatalmas áttörés, mert azt jelenti, hogy ismét együttesen menedzselhető több AP egyetlen interfészen, azonban nincs szükség egy rack-be szerelt fizikai kontrollerre. Ennek elsődleges jelentősége a költségvetésben van, mivel a fizikai kontroller így kikerült abból, illetve előnyös lehet mindazok számára, akiknek egyszerűen túlzás volt a fizikai kontroller által megvalósított funkcióik, azaz egyszerű, de vezérlő-alapú menedzselést szeretnének elérni.

A kontrolleres/ kontroller „nélküli" WLAN néhány hasznos tulajdonsága:

Néhány kontroller további funkciók ellátását is lehetővé teszi, mint például az „állapottartó tűzfal" a vezetékes - vezeték nélküli hálózatok között, VPN kapcsolat, behatolás detektálás - megelőzés szolgáltatások, spektrum monitoring…stb.

- User centrikus infrastruktúra

A felhasználó bármerre mozoghat, a hálózat és a jogosultságok követik, hiszen a csoport- vagy szervezeti tagsága nem változik.

- Wireless Roaming

A roaming szolgáltatás segítségével biztosított a kliens mobilitása. A kontroller érzékeli, ha egy kliens átviteli sebessége lecsökken és utasítani tudja a klienst, hogy jelentkezzen át egy jobb átviteli lehetőséget biztosító eszközre. Ez akkor is szükséges, ha az AP túlterhelté válik. Ebben az esetben a kontroller felhasználókat mozgat át egy másik hozzáférési pontra, így mindenki, megfelelő adatkapcsolatokkal rendelkezhet.

A vékony AP technológiának köszönhetően a központi kontroller minden adatforgalmat észlel és képes a legkritikusabb adatforgalmakat felismerni és a többitől eltérő prioritással kezelni.

Manapság, elsősorban a komolyabb vállalati és oktatási intézményekben kontroller alapú WLAN hálózatok üzemelnek. A kontrolleres megoldások (fizikai / virtualizált) bevezetése korszerűsíti a WLAN hálózatot, illetve csökkenti annak összetettségét, nehézkességét.

3. Aruba Instant

A nevéhez méltóan a Controller-less WiFi-hálózatok vállalati funkcióira helyezi a hangsúlyt. Jó teljesítményt, biztonságot és skálázhatóságot nyújt dedikált fizikai kontroller nélkül. Az ilyen megoldás tipikusan kis-vállalati WLAN megoldás. IEEE 802.11 n-es hozzáférési pontokban valósítja meg a kontrolleres funkciók nagy részét, így segítségével kisebb (maximum 16 db AP) WLAN rendszerek hozhatók létre.

Ezek a hozzáférési pontok "felfelé kompatibilisek", vagyis amennyiben a felhasználó szervezet igényei később megkövetelik, külső kontrollerre is felfűzhetőek. Ezzel nem kell majd a teljes infrastruktúrát lecserélni.

A vékony AP-k tudását képesek kiszolgálni Controller nélkül, valamint további integrált funkciókat tartalmaz:

Nem kell minden egyes AP-t egyenként bekonfigurálni, csupán a telepítés helyén bekapcsolni, majd az eszköz automatikusan letölti a megfelelő beállításokat. A rendszer folyamatosan figyeli a futó alkalmazásokat, priorizálja a titkosított hang- és videó forgalmat, csökkenti az interferenciát. Az integrált spektrumanalízis segítségével, automatikusan észleli és megpróbálja elkerülni a zavaró rádiófrekvenciás forrásokat, így tisztább lesz a jel és gyorsabb az adatátvitel.

Néhány tulajdonsága az Instant eszközöknek / rendszernek:

- 6 SSID-ból álló architektúra
- Automatikus MESH hálózatok
  Ha egy már konfigurált AP eszköz Etherneten keresztül nem tud a Virtual Controllerre csatlakozni, automatikusan MESH kapcsolatot épít ki a kontrollerrel és a többi AP eszközzel.
- Gyorstelepítés
  Az elsőként beállított eszköz lesz az elsődleges Virtual Controller, amely automatikusan egységbe szervezi és beállítja a többi hozzáférési pontot.
- Magas rendelkezésre állás
  Mivel minden AP eszközben egy-egy Virtual Controller fut, így ha az elsődleges Virtual Controller egy AP leállás során kiesik, automatikusan egy másik AP eszköz veszi át a kontroller szerepét.
- Adaptive Radio Management
  Dinamikusan változtatja az AP-k csatornahasználatát, csökkentheti / növelheti az adóteljesítményeket, klienseket és/vagy AP-ket léptethet át másik csatornákra.
- Integrált Tűzfal és QoS
- Behatolás-érzékelés (wIPS)

4. Ellenőrző kérdések:

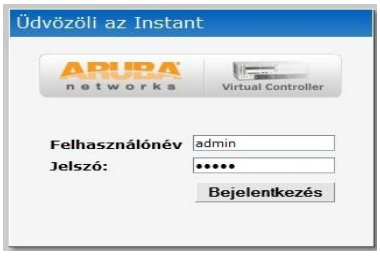
1. Milyen architekturális WLAN technológiák terjedtek el?
2. Mi indokolta az Enterprise WLAN rendszerek megjelenését?
3. Mi az a kontroller és mi a szerepe?
4. Milyen kontrolleres technológiák jelentek meg? Ezek miben különböznek egymástól?
5. Aruba Instant eszközök esetén mit jelent a „felfelé kompatibilitás”?

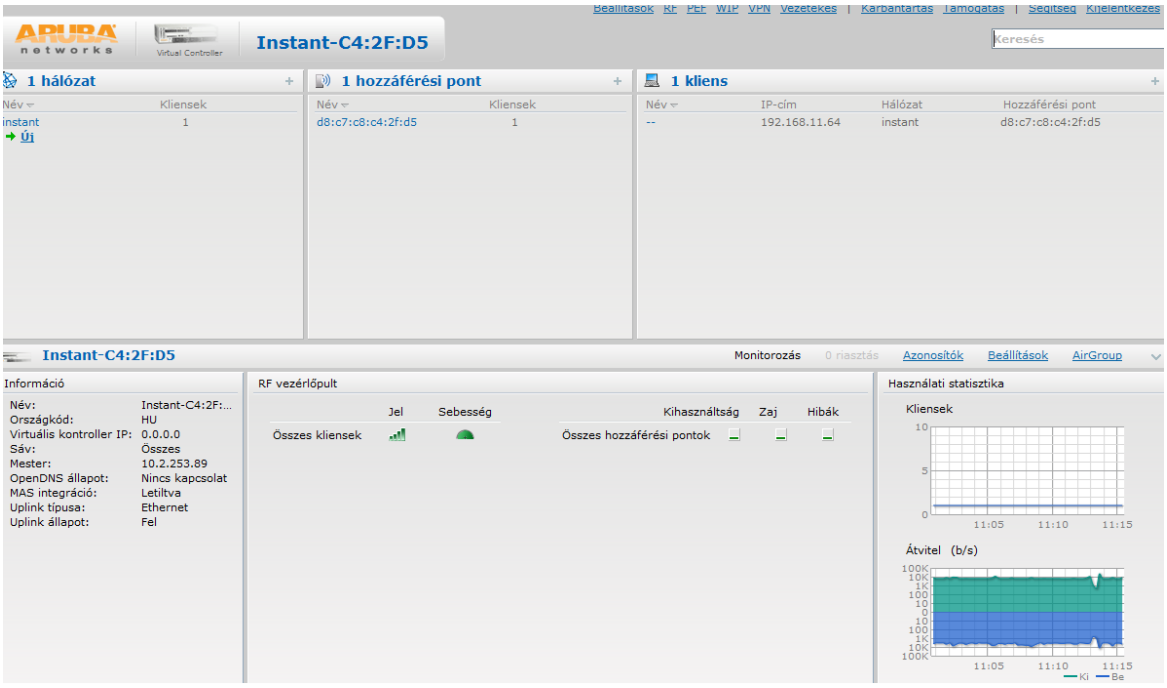
5. Mérési feladatok

(A feladatok megoldása során dokumentálja jegyzőkönyvben az egyes lépéseket, ahol szükséges illesszen be képet az eredményről – „PrntScrn”.)

- Állítson össze 2db IAP-93-as AP segítségével egy Controller-less WLAN.
- a hozzáférési pontok a labor hálózatból kapnak IP-t DHCP-n keresztül

  A megfelelő authentikációs adatok megadásával lépjen be az eszköz menedzsment felületére. (a szükséges adatokat kérje a laborvezetőtől)





Vizsgálja meg a különböző füleket / beállítási lehetőségeket.

1. A megfelelő területi beállítások elvégzése után hozzon létre multiple SSID-val rendelkező hálózatot:

   Kommre_<csoport_azonosító> SSID / a tárgy hallgatói és oktatói számára.

   - IP kiosztást a labor DHCP szervere végzi
   - adási szint
   - WPA2-PSK
   - Ne legyen korlátozva a hozzáférése

Captive portal

Magyarul begyűjtő portálok. Fő célja a hálózati hozzáférés szabályozása, ez azonban nem nyújt védelmet a csatlakozott állomás számára.

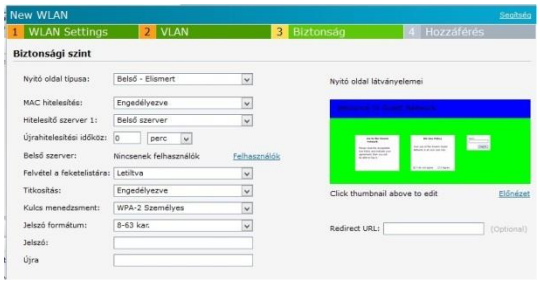
A csatlakozott állomás számára először egy azonosító felület jelenik meg. Amíg a kliens nem végzi el a szükséges feltételeket, addig minden HTTP és HTTPS kérése átirányításra kerül az authentikációs szerverre, minden más forgalom pedig szűrve van (kivéve, amelyek a whitelist-ben szerepelnek). Miután a kliens azonosította magát, és / vagy elfogadta a feltételeket (AUP - Acceptable Use Policy), létrejön a valós kapcsolat. A kliens felőli DNS lekérés sikeresen lezajlik, majd egy HTTP kérést küld az lekérdezett címre. A Captive portal-t üzemeltető állomás tűzfala ezt a kérést átirányítja a Redirect Servernek, amely 302-es Status Code-ú üzenetet küld válaszként és a csatlakozást kezdeményező állomást átirányítja a Captive Portal-ra.

Minden egyes átirányítást a hálózati réteg valósít meg, ezáltal a felhasználók számára teljesen transzparens a működése, valamint a Layer 3 miatt előfordulhat IP-cím probléma.

DNS lekérdezés során a CP-t üzemeltető szerver a kliens állomást egy fix DNS szerverhez csatlakoztatja (ezáltal egy DNS poisoning támadás esetén konfrontálódhat a forgalom).

Integrált guest access és Captive Portal

A vállalati Wi-Fi hálózathoz csatlakozó vendég felhasználók kezelésére az Aruba integrált guest access szerver szolgáltatást biztosít. A vendég felhasználókat szeparáltan a kontrollerben tárolhatjuk. A vendégek hitelesítéséért és beléptetéséért egy teljesen testre szabható Captive Portal felület felel és a rendszerben tetszőleges számú és a cég arculatára szabott Captive Portak is létrehozható.



2. Hozzon létre egy új WLAN hálózatot, majd konfigurálja be, hogy a captive portálon keresztül lehessen authentikálni, a belső címtár alapján.