Biztonságos Wi-Fi hálózat tervezése

RÉTI ZOLTÁN, CZUCZ DÁVID

Synergon Informatikai Nyrt.
{reti.zoltan, czucz.david}@synergon.hu

Kulcsszavak: Wi-Fi Site Survey, WLAN, RF tervezés, Wireless Controller, EAP-TLS, biztonságos Wi-Fi hálózat

A megnövekedett mobilszámítógép-felhasználás maga után vonta a vezetéknélküli hálózatok ugrásszerű növekedését is. A szabadon használható WLAN frekvenciák üzleti célú alkalmazásakor elengedhetetlen a megfelelő biztonsági megoldások használata, illetőleg az előzetes rádiófrekvenciás tervezés és mérés. Írásunkban egy konkrét, nagyvállalati környezetben megvalósított rendszeren keresztül mutatjuk be egy WLAN hálózat tervezését, mérését, megvalósítását és felügyeletét.

1. Bevezetés

Napjaink mobil számítógépes világában igen csak megnövekedett a Wi-Fi alkalmazások száma. Az ingyenes frekvenciahasználat és az egyre olcsóbb berendezések megjelenése lehetővé tette a szabadon használható WLAN infrastruktúra széles körű elterjedését mind nagyvállalati, mind otthoni környezetben. Az egyre sűrűbb, egymástól függetlenül kiépülő rádiós infrastruktúrák megjelenése és üzemeltetése a felhasználóik számára azonban rengeteg hibaforrás kiinduló pontját jelentheti.

Amíg lokálisan csak a saját Wi-Fi hozzáférési hálózati rendszerünk működik a környezetünkben, addig könnyen kezelni lehet az esetlegesen felmerülő üzemeltetési problémákat. Azonban ha a közvetlen környezetében kettőnél több, egymástól független rendszer jelenik meg, nem lehet ugyanúgy kézben tartani a rádiós hálózatunk üzemeltetését megfelelő rádiófrekvenciás menedzsment nélkül. A vezetéknélküli rendszerünk berendezései interferenciás zavartatást fognak szenvedni és így a hálózat hozzáférési kapacitása sérülni fog. A kommunikáció bizonytalanná válik, ami legrosszabb esetben akár az összeköttetés megszakadását is eredményezheti.

Ebben a cikkben WLAN-ok rádiófrekvenciás tervezéséről és a biztonságos Wi-Fi-hálózat tervezésének módszereivel foglalkozunk.

2. WLAN-ok RF-tervezése

Egy-egy Wi-Fi hálózat kiépítésekor a felhasználók részben, vagy teljes egészében megfeledkeznek a rádiófrekvenciás (RF-) tervezés szükségszerűségéről. A tervezés első fázisában a kialakítandó rendszer optimális kihasználhatósága érdekében szükséges a környezet rádiófrekvenciás vizsgálata is.

A rádiós rendszerek által kisugárzott jel lefedettségének láthatóvá tétele, megjelenítése nagymértékben megkönnyíti a Wi-Fi rendszerek RF-tervezését, a telepítést követően pedig az üzemeltetését.

Mielőtt WLAN hozzáférési hálózati rendszert kívánunk üzembe helyezni, a tervezés első lépéseként lényeges előzetesen meggyőződni helyszíni felmérés (Site Survey) keretén belül

- az adott helyszín és annak környezetének rádiófrekvenciás telítettségéről, kihasználtságáról,
- a lefedendő terület rádiófrekvenciás interferencia zavartatást kiváltó tulajdonságairól,
- RF-szempontból a térrész jellegéről (zártságáról, nyitottságáról) és azt határoló elemek fizikai tulajdonságáról,
- mindazon egyéb felhasználói követelményekről és jellemzők meglétéről, melyek befolyásolhatják a telepítendő WLAN rendszerünk üzembiztos működését.

A helyszíni felmérést nagymértékben megkönnyíti egy erre alkalmas dokumentáló eszköz, a Site Survey program alkalmazása, mely képes a mérési eredményeket rögzíteni, majd különböző nézetekben hitelesen megjeleníteni és az egész műveletről megfelelő részletezéssel riportot készíteni.

Az aktív helyszíni felmérés során rádiófrekvenciás mérési pontokat kell felvenni egy mérő WLAN klienssel a lefedendő területen belül elhelyezett és ideiglenesen telepített vizsgáló AP (Access Point – elérési pont) közvetlen és távoli környezetében. A helyszíni felmérést megelőzően ismertnek kell lennie, hogy milyen céllal szükséges elvégezni a méréseket. Más és más a mérés lefolytatásának kimenetele és a WLAN hozzáférési hálózat tervezési procedúrája. Minden esetben szükséges megismerni ügyfél igényeit, amelyet a Wi-Fi hálózati rendszerrel szemben támaszt. Ezen igényeket célszerű rendszertechnikai tervben összefoglalni.

Új hálózat kiépítése esetén ismertnek kell lennie, hogy hova kell Wi-Fi lefedettséget biztosítani és az milyen vezetéknélküli LAN alkalmazást fog kiszolgálni. A vizsgálat célja, hogy meghatározásra kerüljön a WLAN hálózat csomópontjainak száma és helye, valamint ismertté váljon a zavaró objektumok és források helyzete.

A lefedettség igényét célszerű méretezett, méretarányos alaprajzon definiálni. A mérési elrendezés kiala-

kításához segítséget ad, ha az alaprajzon feltüntetésre kerülnek a helyiségek berendezései. A mérési pontok számát mindig az határozza meg, hogy a vizsgálandó helyszín mikrohullámú átviteli szempontból milyen telítettséggel rendelkezik. Más és más az elegendő mérési pontok száma nyílt, vagy erősen zárt (berendezett) helyiségek esetében. Nyílt tér esetében, amikor nagy valószínűséggel biztosítható az AP sugárzó elemének optikai láthatósága, csökkenthető a mérési pontok száma. Zárt, zsúfolt tér esetében célszerű minél részletesebb mérést készíteni.

A mérési pontokat a mérő az általa definiált útvonal mentén veszi fel. Ezért az alaprajznak a mérést megelőzően, hosszúságra kalibráltan rendelkezésre kell állnia a mérésadatgyűjtő programban (ESS Professional). Az összes begyűjtött rádiófrekvenciás mérési eredményeket a program a méretarányos alaprajzon grafikusan jeleníti meg. A mérésadatgyűjtő program utólagosan lehetőséget biztosít a mérési eredmények analizálásához, valamint a mért eredmények adminisztrációjához.

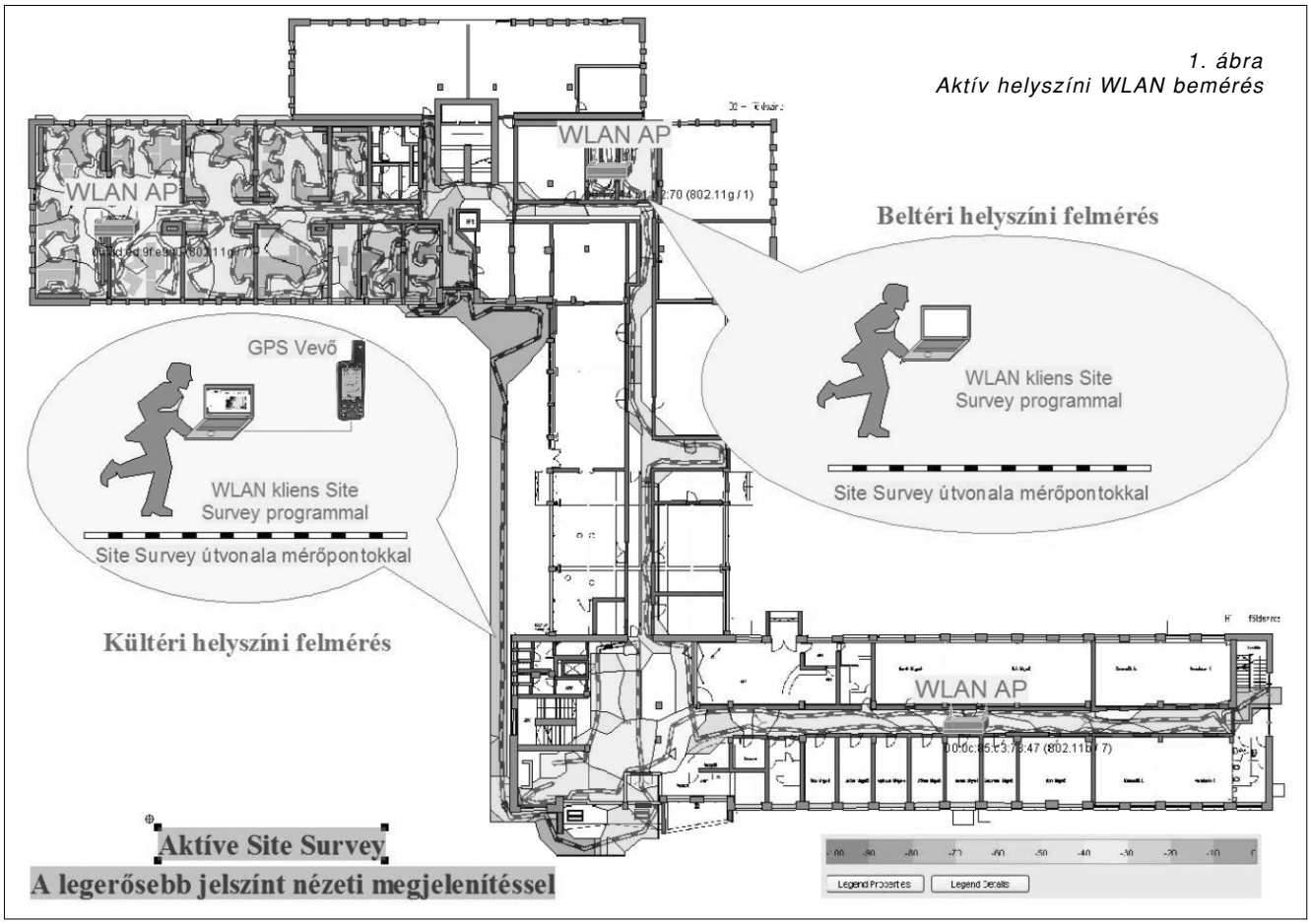
Az *1. ábrán* egy ESS v2.2 Prof programmal támogatott aktív site survey mérés folyamata látszik. Az AP-ok a „WLAN AP” pontba kerültek elhelyezésre. A mérő kliens végponttal a „fehér-fekete” vonallal jelölt útvonalon – valósan berendezett környezetben – megmértük a „WLAN AP” által indukált rádiófrekvenciás jelszint nagyságát.

A mért értékeket az ESSv2.2 Prof. program grafikusan jelenítette meg. A grafikus eredményt felhasználva az ESS program lehetőséget biztosít arra, hogy meghatározzuk a „WLAN AP” rádiófrekvenciás határfelületét. Ezt a vizsgált helyszín térrészére húzott egér kurzor segítségével tehetjük meg, amikor is a program megmutatja a mérővevővel detektált jelszint nagyságát. A kialakítandó hálózat tervezési paraméterének megfelelően (például a demodulációs értéknek megfelelő rádiófrekvenciás jelszint nagyságát figyelembe véve) szükséges elhelyezni és telepíteni a „WLAN AP”-t a következő mérőpontba. Az ideiglenesen telepített „WLAN AP” következő helyzetében ismételten mérési pontokat gyűjtünk, az ESS programmal és azt megjelenítünk. Ezt az iterációs folyamatot mindaddig végezzük, míg a megkívánt lefedett alapterületet bejártuk.

A mérés során a következő két fontos jellemzőt kell vizsgálni:

1) A vevő által mért rádiófrekvenciás jelteljesítmény nagyságát a vizsgált frekvenciasávban. Elsődlegesen az AP által kisugárzott és a vevőben indukált hasznos bejövő jelszint nagyságát mérjük, mely a hely függvényében megfelelően jellemzi az adott térrész rádiófrekvenciás lefedettségének jellemzőjét és a vevő vételi képességét.
2) A vevő által érzékelt rádiófrekvenciás jel-zaj viszony értékét, Signal to Noise Ratio (SNR).

A vizsgáló WLAN kliensen futó Site Survey programnak megfelelően rendszerezve kell begyűjteni a mérési adatokat a későbbi igényes kiértékelhetőség és megjeleníthetőség érdekében.



1. ábra
Aktív helyszíni WLAN bemérés

A szoftvernek képesnek kell lennie:
– a mérési eredmények RF-tervezés szempontjából fontos jellemzői szerinti megjelenítésére;
– tervezési funkciójával egy előre elkészített, modellezett helyszíni környezetben elhelyezett WLAN hálózat lefedettségének szemléltetésére;
– interferenciás zavartatás kialakulása helyének megmutatására;
– idegen WLAN hozzáférési hálózat AP rádiófrekvenciás jelének detektálására, helyzetének becslésére;
– a mért eredményekről részletes riport készítésére.

Az *1. ábra* szól a felmérésről és a korábban meghatározásra került peremfeltételeknek megfelelő (a rendszertechnikai tervben összefoglalt) WLAN AP elhelyezési tervezésről. Más és más WLAN AP szám és elhelyezési sűrűség szükséges egy kis kapacitású WLAN Ethernet átviteléhez, mint egy hangátvitelre szolgáló vagy helyfüggő alkalmazásokat kiszolgáló Wi-Fi tervezéséhez.

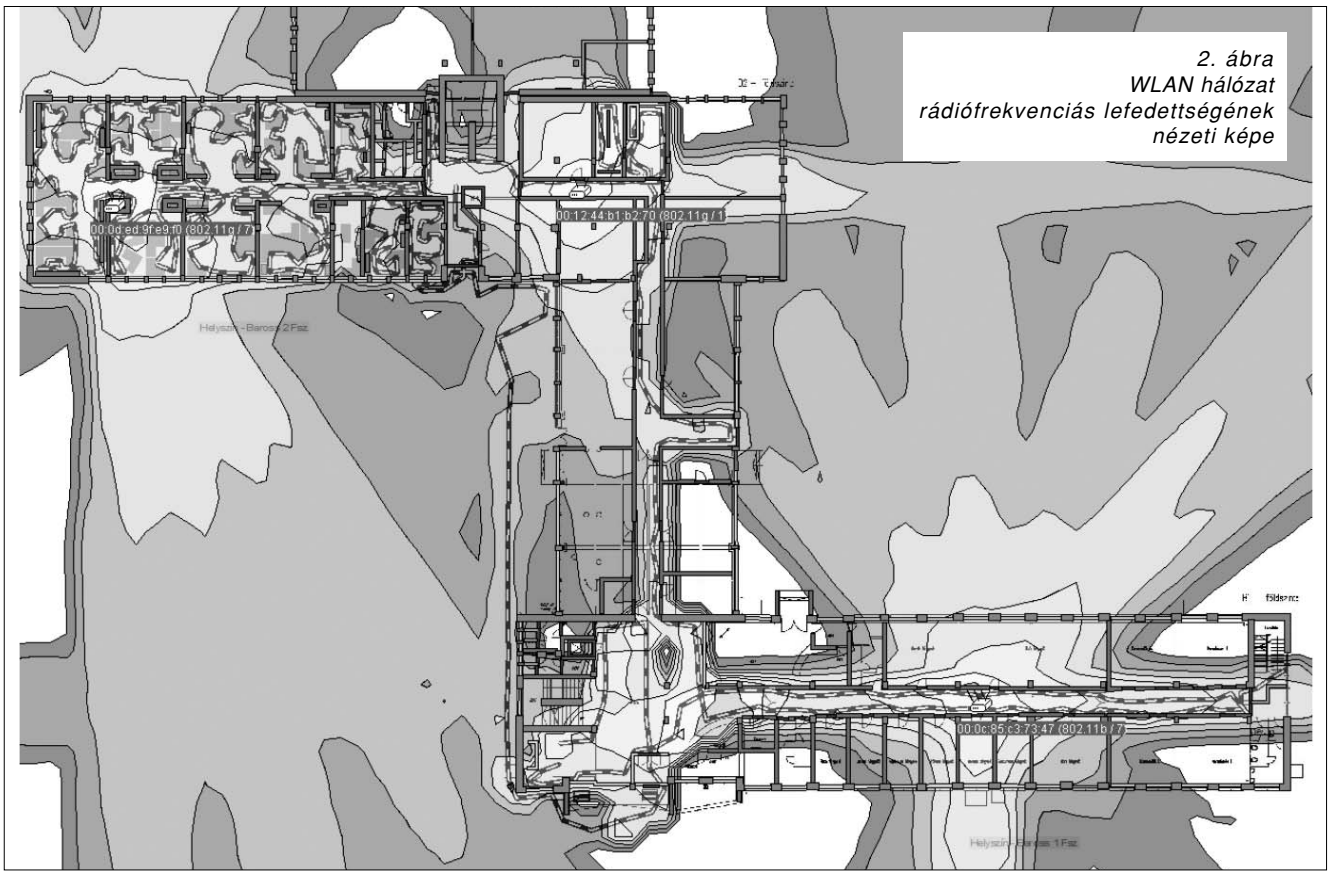
Sok esetben a ráfordítható idő rövidsége miatt, vagy az épület struktúráját figyelembe vevő egyszerűsíthetőség és következtethetőség feltétele miatt nem lehetséges, vagy nem szükséges elvégezni a teljes lefedettség alapterületére az aktív helyszíni felmérést. Ebben az esetben az ESS tervező modulja lehetőséget biztosít passzív Site Survey elvégzésére. Ekkor az ESS program szimulálja az építészeti falak csillapító és szóródó hatását és ennek megfelelően grafikusan jeleníti meg a felvételre került WLAN AP-k rádiófrekvenciás besugárzási jelszintjeit.

A különböző használandó WLAN alkalmazásoknak megfelelő rádiófrekvenciás jelszínt demodulációs értékei és az egy időben jelen lévő WLAN AP-k száma adják meg a tervező részére az alkalmazandó peremfeltételeket a Wi-Fi hozzáférési csomópontok elhelyezéséhez. Az AP-kat manuálisan a tervező helyezi el az alaprajzon, a program csak szimulálva jeleníti meg a várt lefedettség nagyságát grafikus értékét.

A *2. ábra* egy meglévő WLAN hálózat ismételt helyszíni felméréséről (re-site survey) szól. Az AP-k telepítése és üzembe helyezése a korábbi terveknek megfelelően megtörtént. Ezek után egy mérő WLAN kliens segítségével ellenőrizzük a valós környezetbe letelepített Wi-Fi hozzáférési hálózat rádiófrekvenciás lefedettség jelszínt és zajszint értékének nagyságát. Az ESS program grafikusan képes megjeleníteni ezen értékeken túl a tervezésnél felhasznált további származtatott értékeket, mint például a detektált interferenciás zavartatási jelszint, vagy az idegen WLAN hálózatok jelszintjeit, SNR, adatkapacitás értéke.

Az ESS v4.5 Prof. program segítségével lehetőség van többek között egy előre definiált peremfeltétel és követelményrendszer alapján történő grafikus megjelenítésre, ellenőrzésre, megfeleltetésre, mely a tervezést, vagy a mért eredmények kiértékelését megkönnyíti.

A „Live Network Status” elnevezésű táblán az ESS v4.x program megjeleníti a vizsgált helyszínen detektálható valamennyi Wi-Fi hálózat főbb rádiófrekvenciás paramétereit. Ezen a táblán a beállított és kiválasztott rádiófrekvenciás követelmények paraméterei és értékei is visszajelzésre kerülnek.



2. ábra
WLAN hálózat rádiófrekvenciás lefedettségének nézeti képe

A jelenlegi Wi-Fi alkalmazások gombamód-szerű terjedése elkerülhetetlenné teszi a WLAN hálózat RF-s tervezését, majd menedzselését. A professzionális, nagy kapacitású és valós idejű alkalmazások előtérbe kerülése egyenesen megköveteli a szakszerű vezeték nélküli rendszertervezés és dokumentálás tényszerűségét.

3. Biztonságos WiFi hálózat tervezése, megvalósítása és mérése

Egy korszerű, kiemelt biztonságú vezetéknélküli hálózat megvalósítását egy konkrét példán keresztül mutatjuk be. Egy üzleti titkokat is kezelő közintézmény WLAN hálózatának kialakításakor a legmagasabb biztonsági előírásoknak kellett megfelelni, amelyeket csak a legkorszerűbb, mindenre kiterjedő megoldásokkal lehet kielégíteni, ugyanakkor biztosítani kellett az intézményhez érkező kül- és belföldi partnerek, munkacsoportok munkatársai számára a nyilvános hálózat könnyű elérhetőségét.

3.1. A hálózattal szemben támasztott követelmények

A kiépítendő vezetéknélküli hálózat alapvető feladata, hogy megfelelő rádiófrekvenciás lefedettséget biztosítson az intézmény telephelyeinek meghatározott területein (elsősorban tárgyalók) a mobil kliensek számára. A mobil kliensek két csoportba sorolhatók, egyrészről külsős vendégek, másrészről intézményi dolgozók férhetnek a vezetéknélküli hálózathoz. A vezetéknélküli kliensek nem érhetik el az intézmény belső vezetékes hálózatát, a vendég felhasználók számára internet hozzáférést kell biztosítani, az intézményi felhasználók pedig a tűzfal külső lábát érhetik el, ezen keresztül IPSec VPN csatorna felépítésével juthatnak a belső hálózatra.

A kialakítandó vezetéknélküli hálózatnak csak mobil számítógépek adatátviteli forgalmát szükséges továbbítani a vezetékes hálózat felé, nem szükséges valós idejű végpontok forgalmának, mint például hang, vagy videó átvitelét az adat mellett biztosítania.

3.2. Specifikációk

A tervezés során elvárás volt, hogy a kialakítandó WLAN hozzáférési hálózati rendszer szabványos protokollokat és szabadon felhasználható frekvenciasávot, üzemi vivőfrekvenciát alkalmazzon az IP csomagok átviteléhez. A hozzáférési kapacitás és a végponti alkalmazások épületen belüli történő használata megengedett.

További követelmény, hogy a WLAN rendszer legyen alkalmas a jövőben bevezetésre kerülő szabványok támogatására és kezelésére, az elérési pontok (AP) száma szükség esetén, bővíthető legyen.

A kialakítandó WLAN hozzáférési rendszer a következő műszaki tulajdonságokkal rendelkezzen:

– *WLAN rendszer kialakítása:*

Egységesített, kontroller alapú, központi menedzselésű WLAN hozzáférési rendszer Access Point típusú hozzáférési csomópontokkal.

– *Antenna kiválasztása:*

Az AP-k rádiófrekvenciás kimenő pontjára külső antenna csatlakoztatható a megfelelő lefedettség kialakíthatósága érdekében.

– *Átviteli frekvenciatartomány:*

Jelenleg csak a 2,4 GHz az IEEE 802.11bg protokoll használatával.

Az 5 GHz az IEEE 802.11a protokoll használatával a jövőben kialakítható legyen.

– *Frekvenciaműködtetés normája:*

Európai, az NHH szabályozásnak megfelelően.

– *Megfelelőségi szabvány:*

CE tanúsítvány, Wi-Fi, WPA/WPA2, WMM minősítés.

– *Tervezett hozzáférési kapacitás:*

Maximum 54 Mbps kapacitás.

– *LAN interfész kapcsolódás:*

AP-k csatlakoztatáshoz 10/100 BaseT Tx, a központi vezérlő berendezés illesztéséhez pedig 1000BaseT Tx.

– *WLAN AP tápfeszültség ellátása:*

Inline Power Ethernet, vagy szabványos Power over Ethernet (802.3af).

– *WLAN Security:*

802.11i protokollnak megfelelő, Layer2 szintű biztonság, Korszerű idegen WLAN hálózat detektálási rendszer.

– *WLAN menedzselés módja:*

Biztonságos protokollon, egyszerű grafikus megjelenítési felülettel. A CLI egyidejű alkalmazás lehetőségét támogassa az üzemeltetés során.

3.3. WLAN rádiófrekvenciás lefedettség helyének meghatározása

A kialakítandó WLAN hozzáférési hálózat lefedettségének területei, terjedjen ki az intézmény budapesti és több vidéki irodájának tárgyaló és közvetlen környezetére.

3.4. Wi-Fi hálózati topológia

A mobil kliensek számára biztonságos, az intézmény hálózatától szeparált módon biztosít hozzáférést az IT erőforrásokhoz (Internet, intézményi VPN).

A *3. ábra* mutatja be az eszközök intézményi rendszerbe illesztését. A folyamatos vonal a vendég felhasználók hálózatát jelöli, a szaggatott a belső hálózatot. A „belső” forgalom a WPA2/AES biztonság mellett IPSec titkosítást is tartalmaz, a kliensek és a tűzfal között, a „vendég” forgalom WPA/TKIP titkosítással védett a kliensek és a kontroller között, a kontroller utáni forgalom nem titkosított.

3.5. WLAN végponti alkalmazások és szolgáltatások

A vezetéknélküli LAN hozzáférési rendszer végponti kliensei részére két csoportra oszthatók:

- Vendég felhasználók részére nyilvános Wi-Fi internet szolgáltatás, megfelelő biztonsági kontroll alkalmazásával.
- Az intézmény WLAN végponti kliensei részére az intézmény tűzfalán keresztül IPSec VPN csatorna kiépítésével a VPN szabályozásban meghatározott belső erőforrásokhoz való hozzáférés.

3.6. Az intézmény belső mobil számítógépei

Az intézmény belső vezetéknélküli felhasználóinak azonosítását meglévő, központi Steel Belted RADIUS szerver végzi. A Wi-Fi hálózathoz történő IP csatlakozást a kliens használati jogosultságának eldöntése – érvényes, az intézmény által kibocsátott X.509 tanúsítvány ellenőrzése – előzi meg. Amennyiben jogosult a belső WLAN hálózathoz történő csatlakozásra, úgy valós IP címet kap a vezeték nélküli kliens végpont hálózati csatoló kártyája.

A WLAN kliens végpont IP csatlakoztatásakor a következő feltételek biztosítása szükséges:

– Csak akkor induljon el a kapcsolódási folyamat, ha a mobil számítógép vezetékes LAN Ethernet csatlakoztatása megszűnik.
– A WLAN és az IP kapcsolat felépítése csak a mobil végponton előre beállított konfigurációnak megfelelő, valós WLAN hálózaton keresztül valósuljon meg.
– Amennyiben a mobil számítógép ismét a vezetékes LAN hálózathoz kapcsolódik, úgy a WLAN hálózati IP kapcsolata érvényét veszítse és a mobil PC végpont ismét csak a vezetékes IP címével működjön.
– Tegye lehetővé, hogy külső helyszíneken a Wi-Fi felhasználó által előre beállított, más Wi-Fi rendszerekhez is csatlakozhasson (ITU, CEPT stb. ülések).
– A mobil számítógépek forgalmazása csak a központ felé történjen.
– A File and print sharing protocol nem kerül továbbításra.

3.7. Vendég felhasználók mobil számítógépei

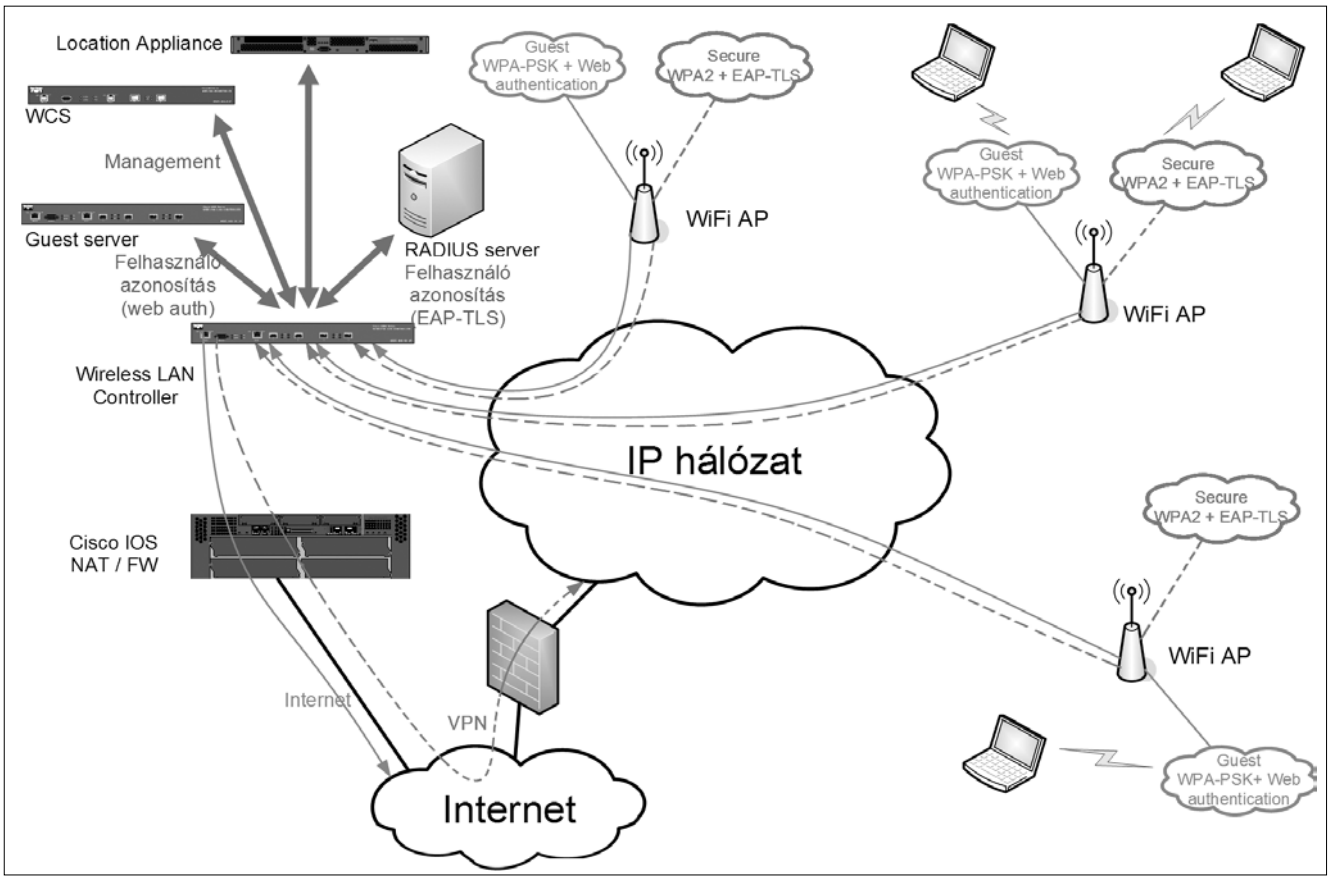
Az intézmény területén csatlakozni kívánó vendég felhasználók WLAN kliens végpontjai részére a következő szempontok valósuljanak meg:

– Megfelelő biztonságú (WPA, vagy WPA2 kulcsmenedzsment és TKIP, illetve AES titkosítás) Layer2 titkosítású adatkapcsolat.
– Kontrollált vezetéknélküli internetszolgáltatás kialakítása valósuljon meg. A vezetéknélküli kapcsolat időtartama és hozzáférési jogosultsága az intézmény részéről könnyen beállítható legyen.
– A vendég felhasználók Wi-Fi forgalma az intézmény belső hálózatától elkülönítve kerüljön átvitelre és a Wi-Fi kliensek hálózathoz történő csatlakoztatásánál szükséges a megbízható azonosítás és az időfelhasználási korlátozás kialakítása!

3.8. Általános biztonsági követelmények

A vezetéknélküli kliensek forgalmát az intézmény hálózatától teljesen elkülönítve kell kezelni, a vezetéknélküli kliensek az intézmény belső IT erőforrásait nem érhetik el (kizárólag a tűzfalon keresztül felépített IPSec VPN csatornán, amelynek használatához csak a belső felhasználók rendelkeznek megfelelő jogosultsággal)

2. ábra WLAN hálózat rádiófrekvenciás lefedettségének nézeti képe



3.9. Általános WLAN Security követelmények

A belső, vezetékes LAN hálózaton szereplő adatok biztonsága érdekében a kialakítandó WLAN hozzáférési hálózat támogassa az IEEE 802.1x port szintű azonosítási protokollt, Layer2 szinten az IEEE802.11i szabványajánlásnak megfelelően.

A vezetéknélküli végponti kliens felhasználók azonosítása szabványos szerver alapú azonosítás alapján valósuljon meg, mely az intézmény belső biztonsági szabályozásával összhangban kerüljön kialakításra.

Az AP-k és a WLAN kontroller közötti kapcsolat kialakítása biztonságos protokoll alkalmazásával valósuljon meg. A WLAN hozzáférési rendszer csomópontjai számára csak azonosított AP csatlakoztatását tegye lehetővé.

Biztosítson idegen WLAN hálózat detektálás megjelenítésének lehetőségét, mind infrastruktúra-alapú, mind ad-hoc hálózati architektúra esetében.

A rádiófrekvenciás média-titkosításához WPA-TKIP vagy WPA2-AES kulcsmenedzsment-titkosítás párosítás használatával biztosítson a végponti kliens tudásának megfelelően lehetőséget a csatlakoztatásra.

4. A WLAN hálózat részletes ismertetése

A vezetéknélküli LAN-ok rendszertechnikája az elmúlt években nagyon sokat változott. A technika népszerűségének növekedése a skálázhatóság növelésének folyamatos igényét tartja életben. A jelenleg legkorszerűbb a Cisco controller-alapú rendszertechnikája, amely a rádiós AP-k vezérlését a vezetékes hálózaton intelligens célberendezésekre, úgynevezett WLAN Controllerekre (WLC) bízza, a WLC-ket pedig a Wireless Control System menedzsment szoftveren keresztül tudjuk kézben tartani. Az intézmény számára ezen az architektúrán alapuló rendszert terveztünk, amelyet kiegészítünk egyéb szolgáltatásokkal is (Location Based Services, Guest Services); ennek részletes eszközeit és rendszertervét ismertetjük a továbbiakban.

4.1. LAP-ok (Ligtweight Access Point)

Olyan mikrohullámú berendezések, amelyek biztosítják a rádiós közeget és annak csatlakozását a vezetékes közeghez. Tápellátásuk az intézménynél power injectorokkal történik, a szabványos PoE (IEEE 802.3af) technikával. A LAP-ok az architektúra triviálisan szükséges elemei. Az LAP-k nem, vagy legalábbis korlátozott funkcionalitással működhetnek (REAP vagy H-REAP üzemmódban) a WLC vezérlése nélkül.

4.2. WLAN controllerek (WLC)

A WLC Controller-ek olyan vezetékes eszközök, melyek az AP-k vezérlését látják el. Az AP-k a Ligtweight Access Point Protocol-lal (LWAPP) kommunikálnak azzal a WLC-vel, amelyhez ugyanezen a protokollon regisztráltak. Az LWAPP egy szabványos, IP alapú tunnel protokoll, amely az AP-k és a WLC között épül ki, az UDP szolgáltatásait használja és a teljes rádiós 802.11 keretet tartalmazza. (Az LWAPP-nek van L2 üzemmódja, amely választható a WLC-kben is, de skálázhatósági korlátai miatt nem javallott.) Az LWAPP két alapvető szolgáltatása az AP vezérlés, és a felhasználói forgalom szállítása.

A vezérlés X.509 certificate alapú, AES algoritmussal titkosított csatornán zajlik, míg a felhasználói forgalom számára az LWAPP a tunnelezésen kívül nem biztosít semmilyen titkosítási szolgáltatást. Ennek oka, hogy a teljes 802.11 keretet becsomagolja, így az alkalmazott rádiós hálózati biztonság (WPA+TKIP, WPA2+AES) a LAP-tól WLC-ig változatlanul érvényesül a vezetékes hálózaton.

4.3. Wireless Control System (WCS)

A Cisco menedzsment szoftvere, amelyen keresztül a WLC-k és AP-k összefogását és kezelését egy vezérlőpultról végezhetjük. Az architektúrának nem alapvető eleme, de kiterjedtebb hálózat (több WLC) és egyéb szolgáltatások igénye (például location-based services) esetén szükséges.

4.4. Location Appliance

Opcionális elem, amely a WCS-sel és az architektúra többi elemével együttműködve elhelyezkedésre vonatkozó szolgáltatásokat nyújt (például meg tudja jeleníteni egy felhasználói gép, Wi-Fi telefon vagy RFID (rádiófrekvenciás azonosító) címkével ellátott tárgy elhelyezkedését az épület térképén). Rack-be szerelhető appliance (szoftver+hardver együtt) kiépítésű, amely a WCS nélkül nem működőképes.

4.5. NAC Guest Server

Opcionális elem, amely a vendég felhasználók adminisztrációját könnyíti meg: a vendég felhasználó felvételét, ideiglenes accountjának nyomtatását, mailben vagy SMS-ben történő elküldését, a használat időkorlátját és a felhasználó azonnali letiltását, valamint vendéglisták készítését teszi lehetővé. Természetesen regisztrálja a felhasználói aktivitást, a be- és kijelentkezés idejét valamint a kliens IP címét. A NAC Guest Server valójában egy speciális AAA szerver, amely RADIUS protokollon szolgálja ki klienseit: a WLC-ket.

4.6. Cisco Secure Services Client (CSSC)

A kliens gépeken futó program, amely csak a kijelölt biztonsági elvek szerint enged csatlakozni a konfigurált vezetékes és vezetéknélküli hálózatokhoz. Az intézménynél érvényben levő szigorú biztonsági szabályozás érvényesítése érdekében a vezetéknélküli szolgáltatást is használni jogosult felhasználók gépére telepíteni kell.

4.7. Az elemek együttműködése

A rendszer központi eleme a kontroller, minden kommunikáció, ellenőrzés és irányítás ezen keresztül történik. A kontroller és a kihelyezett AP-k a WLAN biztonság kialakítási folyamatában fontos (authenticator) helyet foglalnak el. A belső WLAN kliensek azonosítását IEEE 802.1x protokollnak megfelelően meglévő, Steel Belted RADIUS Server-pár biztosítja. A WLC szabványos RA-

DIUS protokollon keresztül kommunikál az azonosítási szerverrel. A vendég Wi-Fi felhasználók azonosítását a NAC Guest server RADIUS szervere biztosítja. A kontrolleren minden WLAN hálózathoz (SSID-hez) külön RADIUS szervereket állítottunk be.

4.8. Eszközkonfiguráció-hozzáférés

A WLAN hozzáférési hálózat konfigurációs állományát a központi kontroller tartalmazza. A berendezés beállításának hozzáféréséhez jelenleg három felhasználónév és jelszó páros került kialakításra.

4.9. Az átvitt forgalom biztonsága

A rádiós forgalom titkosítását a WLC kontroller konfigurációja és a távoli AP-k biztosítják. A hálózatot azonosító SSID-k nincsenek nyilvánosan megosztva a 802.11 Ethernet keretben (No broadcast). Vagyis nem jelennek meg automatikusan a Microsoft Windows operációs rendszerével elérhető hálózatok között egy olyan felhasználó gépén, amelyen az adott SSID-t tartalmazó profile nem ismert. A kapcsolat kialakítása előtt ezen azonosítót mindig szükséges megadni!

A kialakított WLAN hálózatok eltérő biztonságot alkalmaznak a felhasználóik részére:

• A vendég vezetéknélküli LAN felhasználók Internet hozzáférése védett, mind a rádiófrekvenciás média Layer2 titkosítása, mind a forgalom jogosultsága szempontjából. Jelenleg a rádiófrekvenciás forgalmat előre definiált WPA kulccsal és TKIP titkosítással láttuk el. A WLAN kapcsolat kialakítása után az Internet forgalom hozzáféréséhez szükséges egy időkorlátos felhasználó név és jelszó, melyet korábban a NAC Guest szerverrel szükséges generálni a vendég felhasználók részére.

• A belső Wi-Fi felhasználók WPA2 kulcs menedzsment és AES titkosítás kódolási algoritmussal és meglévő digitális tanúsítvány hitelesítése után csatlakozhatnak a hálózathoz. A belső vezetéknélküli LAN kliensek hitelesítéséhez 802.1x szerver alapú, EAP-TLS módozatú megoldás használatos, meglévő PKI infrastruktúrával. A kliens oldalon CSSC felhasználói program v5.1 verziójának előre kialakított konfigurációja alapján gondoskodik az intézmény belső Wi-Fi végpontok kapcsolatának további biztonságáról, mind a vezetékes LAN, mind a WLAN kapcsolódásakor. Amennyiben az intézmény belső mobil kliens végponti PC-je a vezetékes LAN hálózathoz kapcsolódik, úgy a CSSC program gondoskodik a WLAN kapcsolat (IP és rádiófrekvenciás) megszüntetéséről. Ha a mobil végpont megszakítja a vezetékes Ethernet kapcsolatát, úgy a CSSC program átvált a Wi-Fi rádiófrekvenciás IP kapcsolatra. A biztonsági funkció kiszolgálásához minden egyes belső WLAN mobil számítógépre szükséges telepíteni a CSSC felhasználói programot.

4.10. WLAN felhasználói csoportok biztonsági beállítása

Az intézmény WLAN hozzáférési hálózati rendszerében a csatlakozni kívánó Wi-Fi felhasználók elkülönítetten, megfelelő azonosítás után kapcsolódhatnak. A megfelelő IP csatlakoztatással rendelkező kliens végpontok hálózati környezetüktől függően a következő jogosultsággal és szolgáltatási igénnyel rendelkezhetnek:

– A belső WLAN felhasználók teljes jogosultsággal rendelkeznek és érhetik el a vezetékes LAN hálózat erőforrásait.
– A vendég Wi-Fi felhasználók az intézmény belső hálózatát nem érhetik el. Csak nyilvános internet hozzáféréssel és szolgáltatással rendelkezhetnek.

4.11. WLAN Menedzsment

Az intézmény WLAN hozzáférési hálózat eszközeinek felügyelet-menedzselése a következőképpen valósul meg:

• A LWAP és a WLC4404 kontroller ugyanazon hálózatba (VLAN=2), a valós forgalomtól történő elkülönítéssel menedzselhető.

• A WLC4404 kontrollert egy erre a célra adott IP címen akár grafikusan, akár CLI felületen menedzseljük.

• A LWAP menedzselését a WLC4404 kontroller megadott IP címtől kezdődően, az „ap-manager” nevű interfész felületén keresztül biztosítja.

• A menedzsment funkciók grafikus megjelenítése és ellátása érdekében WCS (v5.0.148) hálózat felügyeleti szerver szoftver került telepítésre az erre a célra adott IP címen. A WLC-től érkező információkat a WCS SNMP-n keresztül kérdezi le.

• Biztonságos, tanúsítvány alapú https (SSH) protokoll került kialakításra.

• A kontroller CLI konfigurációja közvetlenül a soros portjáról is ellenőrizhető és módosítható (9600Bps Baud Rate, 8bits, Flow Control tiltva, Stop Bits:1, Paritás nélkül).

• WLAN-n keresztül a menedzselés tiltva van.

5. Összefoglalás

A fentiek alapján elmondhatjuk, hogy egy közintézmény megfelelően védett, ugyanakkor széles kör számára szolgáltatásokat nyújtó Wi-Fi hálózatában szinte minden ma elérhető technikai és biztonsági megoldásra szükség volt. A vezetékes hálózattól elválasztott, központi kapcsolású adatforgalom, WPA és WPA2 titkosítás, tanúsítvány alapú felhasználó azonosítás, ideiglenes felhasználók kezelése és ellenőrzése, terület alapú szolgáltatások, idegen kliensek és hálózatok felderítése, központi grafikus adminisztráció... A végeredmény egy minden igényt kielégítő, biztonságos, jól adminisztrálható és ellenőrizhető Wi-Fi rendszer.

A szerzőkről

RÉTI ZOLTÁN 1968-ban született Mohácson. 1992-ben diplomázott a BME Villamosmérnöki Karán. 1992-től számítógépes hálózatok tervezésével és megvalósításával (LAN, WAN) valamint hálózatmenedzsmenttel, IP telefóniával és VPN hálózatokkal foglalkozik. Több országos rendszer tervezésében és megvalósításában vett részt. Jelenleg technikai tanácsadóként dolgozik a Synergon Informatika Nyrt. Infrastruktúra divízió Hálózati kommunikációs üzletágában.

CZUCZ DÁVID 1962-ben született Budapesten. 1985-ben diplomázott a Kandó Kálmán Villamos Ipari Műszaki Főiskolán, majd 1993-ban szerzett szaküzemmérnöki másoddiplomát Mikrohullámú PCM hírközlés szakon. Jelenleg technikai tanácsadóként dolgozik a Synergon Infrastruktúra divízió Hálózati kommunikációs üzletágában. Fő területe a vezetéknélküli hozzáférési hálózati rendszerek. 2006 óta CAWLANFS minősítésű vizsgával rendelkezik.