

Tartalomjegyzék

1	Bevezetés	3
2	A hálózattal szemben támasztott követelmények	5
2.1	IT követelmények a WLAN rendszerrel kapcsolatban.....	5
2.1.1	A WLAN hálózat rendeltetése	5
2.1.2	A WLAN hálózattal szembeni elvárások.....	5
2.1.3	Megoldási javaslat	6
2.1.4	Specifikációk	11
2.1.5	WLAN rádiófrekvenciás lefedettség helyének meghatározása.....	12
2.1.6	Hozzáférési hálózati topológia	12
2.2	WLAN végponti alkalmazások és szolgáltatások	13
2.3	WLAN hozzáférés szabályozása.....	13
2.3.1	A cég belső mobil számítógépei.....	13
2.3.2	Vendég felhasználók mobil számítógépei.....	14
2.3.3	A cég belső mobil IP telefonjai	14
2.4	Biztonsági követelmények – WLAN Security	15
2.4.1	Általános WLAN Security követelmények.....	15
2.4.2	WLAN kliens végponti előírások.....	15
2.5	Vezetékes LAN hálózati infrastruktúra	16
2.6	WLAN hálózat felügyelete, menedzselése	16
3	A megvalósított WLAN hálózat bemutatása	19
3.1	Rendszertechnika.....	19
3.1.1	Átviteltechnika	19
3.2	UTP kábelhálózati rendszer	19
3.2.1	UTP – Switch Port bekötés	23
3.3	WLAN AP-k fizikai elhelyezése.....	24
3.4	Rádiófrekvenciás peremfeltételek	24
3.5	WLAN kontroller elhelyezése.....	25
4	Eszközök IP cím kiosztása	27
4.1	WLAN AP-k IP címei	27
4.2	WLAN kontroller IP címe	27
4.3	WLAN kliens végpontok IP cím kiosztása.....	27
5	WLAN Security kialakítása.....	29
5.1	Eszköz konfiguráció hozzáférés.....	29
5.2	Átviteli forgalom biztonsága.....	30
5.3	WLAN felhasználói csoportok biztonsági beállítása	30

6	WLAN Menedzsment.....	32
6.1	SysLog Server	32
6.2	SNMP	32
7	Eszközlista	34
7.1	Wireless LAN Controller (WLC).....	34
7.2	Light Weight Access Pointok (LWAP)	34
8	Mellékletek	36
8.1	WLAN AP elhelyezési terv.....	36
8.2	Konfigurációs file.....	44
8.2.1	WLC futó konfiguráció	44
8.2.2	WLC rádiós beállítások és jellemzők:	49
8.3	WLAN árlista	60
9	Irodalomjegyzék.....	62

1 Bevezetés

A vezetékes hálózatokat már jó harminc éve használjuk, a „vezeték nélküiség” viszont csak néhány éve került be a köztudatba, kecsegtető lehetőségei azonban rendkívüli ütemben növelik ismertségét és alkalmazását. Ez a technológia már nem csak a nagy cégek, kormányzati és oktatási intézmények sajátja, hanem bárki által elérhető mivel ma már rengeteg olyan termék van, amellyel olcsón kiépíthetjük akár otthoni vezeték nélküli hálózatunkat is!

A vezetékes hálózat hátránya a vezeték nélküivel szemben, hogy ha kapcsolódni akarunk hozzá, mindenképpen valamilyen kábeles összeköttetés kell létrehozunk, ami igen csak korlátozza a mozgásunkat, vagy mai divatos kifejezéssel élve a mobilitásunkat. Vezeték nélküli hálózat esetében azonban nincs szükségünk kábelekre, készülékeink hatósugarán belül bárhol kapcsolatot létesíthetünk más eszközökkel. A WLAN (*wireless LAN*) rádióhullámot használó vezeték nélküli helyi hálózat, ami szórt spektrum vagy ortogonális frekvencia-osztásos multiplexálás technológia segítségével lehetővé teszi a közeli számítógépek összekapcsolódását. Számítógépek vezetékes hálózathoz kapcsolására és önálló ad hoc hálózatok létrehozására egyaránt alkalmas. A legnépszerűbb WLAN szabványcsalád a WiFi (IEEE 802.11); a WiFi és a WLAN nevet gyakran egymás szinonimájaként használják. Leggyakoribb változatai a 802.11b (11 Mbit/s sávszélesség, 2.4 Ghz-es frekvencia), 802.11a (54 Mbit/s sávszélesség, 5 GHz-es frekvencia) és a 802.11g (54 Mbit/s, 2.4 Ghz). (A készülőfélben levő 802.11n tervezett sebessége 248 Mbit/s.)

A szakdolgozatomban egy cég vezeték nélküli hálózatának megtervezését és megvalósítását szeretném bemutatni. Azért választottam ezt a témát, mert a cégnél ahol dolgozom, épp most valósítottunk meg egy ilyen hálózati rendszert, így saját szemszögből tudom azt bemutatni.

A cég központi telephelyén beltéri, WLAN hozzáférési hálózati rendszer kiépítését tervezte. A kivitelezés kialakíthatósága érdekében előzetes helyszíni bejárással egybekötött rádiófrekvenciás mérési vizsgálatot végeztünk, majd a vezeték nélküli hozzáférési pontok elhelyezéséhez ESSv2.2 Prof programmal támogatott szimulációs tervezéssel határoztuk meg a szükséges Access Point számokat és rádiófrekvenciás adatokat. A cég telephelyén jelenleg üzemelő WLAN hozzáférési hálózat 1 db Cisco Aironet sorozatú, AIR-AP1220B-E-K9 típusú berendezése biztosítja. A földszinten elhelyezkedő tárgyalók rádiófrekvenciás lefedettségét az IEEE 802.11b vezeték nélküli Ethernet protokoll szerint valósítja meg.

Szakedolgozatom első részében a rendszer tervezési folyamatokat írom le majd a második részében magát a megvalósítást mutatom be.

2 A hálózattal szemben támasztott követelmények

2.1 IT követelmények a WLAN rendszerrel kapcsolatban

2.1.1 A WLAN hálózat rendeltetése

A vezeték nélküli LAN hozzáférési hálózat feladata, hogy megfelelő rádiófrekvenciás lefedettség alkalmazásával a vállalat megfelelő helyszínein (telephely1 és telephely2 épületek) a mobil kiépítésű WLAN kliensei részére a vezetékes LAN hálózathoz történő hozzáférést, a hozzáférési jogosultságának megfelelően biztosítsa.

A kialakítandó vezeték nélküli hozzáférési hálózatnak Ethernet protokollon keresztül, mind a mobil számítógépek adatátviteli forgalmát, mind a WLAN telefonok hangátviteli forgalmát képesnek kell lennie továbbítani a mobil kliensek és a vezetékes hálózat Ethernet portjai között.

2.1.2 A WLAN hálózattal szembeni elvárások

A vezeték nélküli LAN hozzáférési hálózattal szemben a cég IT részéről a következő követelmények fogalmazódtak meg:

- A kialakítandó WLAN hozzáférési hálózat lefedettségének területei
 - telephely1 Fsz
 - telephely1 Első emelet
 - telephely1 Második emelet
 - telephely1 Harmadik emelet
 - telephely2 Fsz
 - telephely2 Első emelet

- Az alkalmazandó hozzáférés WLAN Ethernet protokoll szabványa
 - IEEE 802.11bg, 54Mbps kapacitással
 - IEEE 802.11a, 54Mbps kapacitással
 - Legyen alkalmas a jövőben bevezetésre kerülő szabványok követésére!
- A WiFi végfelhasználók által tervezett alkalmazások elkülöníthetők legyenek
 - Általános adat felhasználói alkalmazások. A WiFi számítógépek WLAN adapter csatoló kártyái legyenek képesek kapcsolódni a hálózathoz, megfelelően elszeparált hierarchiában.
 - Lehetőség szerint legyen alkalmas a bevezetésre kerülő WLAN hozzáférési hálózat valós idejű felhasználói alkalmazás, mint pl. hang megfelelő átvitelére.
- A WLAN hozzáférési hálózat rendelkezzen korszerű biztonsági megoldásokkal.
 - Támogassa a központosított azonosítási szerver alapú (802.1x) EAP protokoll megoldásokat.
 - Biztosítson a vezeték nélküli hozzáféréshez biztonsági megoldást a vendég felhasználók azonosítására és megfelelő elkülönítésére a belső hálózattól!
 - Maximális biztonsági szint mellett biztosítson alkalmazási felhasználóknak megfelelően elkülönített megoldást!
- Menedzselése és üzemeltetése legyen egyszerű és könnyen megvalósítható!

2.1.3 Megoldási javaslat

A feladat megoldásához Cisco Unified Wireless hozzáférési hálózat kialakítást javasoltuk, melynek kialakításához két alkalmazási lehetőség (csak adat, adat + hang) bevezetését ajánlottuk. Az egységesített vezeték nélküli LAN hozzáférési hálózat és autonóm AP-ből felépített hálózat összehasonlítását és főbb bevezetési szempontjait jellemzik az 1-3 számú táblázatok. Az egységes vezeték nélküli LAN hozzáférési hálózat több funkcióban biztosít hatékonyabb és jobb megoldást az autonóm Access Pointokból felépített rendszerénél:

- Kialakítása és bevezetése időtálló megoldást nyújt. A kontroller szoftver verziója támogatja az IEEE 802.11n szabvány (> mint 100Mbps WLAN) protokollt, mely jelenleg draft verziójú és várhatóan 2008-as évben véglegesítik. A ratifikáció után megjelenő rádiófrekvenciás hozzáférési eszközök kapacitás igénye ugrásszerűen megnövekszik.
- A WLAN rendszer üzemeltetése és menedzselése egyszerűsödik, elegendő csak a WLAN Controller berendezésen a konfiguráció kialakítása és fw verzió frissítése.
- Vendég felhasználók részére kontrollált (Username/Password alapú) internet hozzáférés biztosítása.
- A dinamikus rádiófrekvencia kezelésnek és a kontrollált AP vezérlésnek megfelelően a különböző WLAN kliens felhasználók kapacitás megosztása és csatlakozása megbízhatóbb.
- Vezeték nélküli Ethernet protokollon keresztüli hang átvitele biztosítható több más WLAN kliens felhasználó egy időben történő üzemeltetése során.

Hatékony, idegen WLAN hozzáférési csomópont, vagy kliens forgalom detektálásának képesség

<i>Szempont</i>	<i>Leírás</i>	<i>Unified WLAN Megoldás</i>	<i>Autonóm WLAN Megoldás</i>
<i>Egyszerű Bevezetés</i>	A vezeték nélküli LAN hozzáférési technológia bevezetésének lehetősége	Centralizált rendszerben az AP-k és a kontroller egy hálózatba kerülnek. Nincs szükség újramaszkolásra és VLAN trónkölésre a hozzáférési rétegben.	Kis AP szám esetén megoldott. Nagyobb AP esetén, nagyobb kiterjedésű területen körültekintő tervezést, Site Survey szükséges az AP elhelyezésének meghatározásához.
<i>Egyszerű Üzemeltetés</i>	A WLAN hozzáférési rendszer berendezéseinek üzemeltetése. A csomópontok, WLAN AP és kliensek eszközeire vonatkoztatva.	A kontrolleren egy imageben vannak tárolva az AP-k beállítási konfigurációja. Amikor a kontroller imaget frissítjük, úgy az összes csatlakoztatott AP beállítása upgradelt állapotba kerül.	Az autonóm AP-k önálló konfigurációjait külön-külön szükséges változtatgatni, egyenként vagy egy template script segítségével. Az AP-k FW-t is egyenként kell frissíteni.
<i>Rádiófrekvenciás kezelési mód, megbízható WLAN csatlakoztatás</i>	Az átviteli média, rádiófrekvenciás spektrum kezelésének módja	Dinamikus rádiófrekvenciás menedzselés. Az AP-k összehangolt működtetésével a kontroller alakítja ki az AP-k vivőcsatornáját és jelszintjét a kialakítható optimális WLAN lefedettség és hozzáférési kapacitás érdekében.	Statikus rádiófrekvenciás környezet. Az AP-k konfigurációjában a vivő frekvencia és kimenő teljesítmény statikusan van kialakítva. Ez nem veszi figyelembe a már meglévő, külső szomszédos WLAN-ból származó interferenciából jelentkező hatásokat. Használj rendszer szintű alkalmazási eszközt vagy egy SNMP! Az RF információ rendelkezésre áll manuális áttekintéshez és cselekvéshez.
<i>Kliens csatlakoztatásának módja</i>	A WLAN kliens rádiófrekvenciás kapcsolat kialakítása során milyen mechanizmusok biztosítják a sikeres csatlakoztatást.	Optimalizált felhasználókénti működtetés a kiegyenlített felhasználói feltöltésen keresztül. A kontroller fogja eldönteni, hogy egy kliens a kapcsolatának kialakításakor, melyik AP-hoz csatlakozzon, hogy optimális legyen a rádiós kapacitása.	A 802.11 protokoll alapján a kliens dönti el, hogy számára melyik a legjobb vételi képességű AP. Ezen kapcsolódás során a hozzáférési kapacitás nincs kontrollálva. Előfordulhat, hogy ugyanazon AP-hoz több kliens kapcsolódik lecsökkentve egymás kapacitását.
<i>Vendég hozzáférési hálózat</i>	Külső vendég felhasználók részére könnyen és kontrolláltan elérhetővé tenni a WLAN hozzáférést, pl. internet hozzáférést, úgy hogy megtartjuk a hálózat biztonságos csatlakoztatási módját.	Ugyanazon hálózat megosztható belső és vendég felhasználók részére, megtartva a kontrollált biztonságot mindenki részére.	Különböző policyval és jogosultságokkal rendelkező VLAN kialakítással a vendég felhasználók csökkentett biztonsággal rendelkeznek. Alakíts ki speciális trónk VLAN-okat minden egyes AP-ban és hirdesd azokat a hálózaton keresztül!
<i>Layer2 Fast Secure Roaming</i>	Folyamatos IP kapcsolat a kliens roamingja alatt a subnetekben az AP és a VLAN-n keresztül.	A kontroller látja el ezen feladatot. Nincs szükség VLAN-ok közötti roamingra. A kontroller menedzsel minden roamingot és tunnelinget egyik subnetből a másikba.	Egy WDS berendezés (AP vagy Switch module) hozzáadása a roaming biztosítása érdekében.

1. táblázat Unified és Autonóm WLAN hozzáférési hálózati megoldások összehasonlítása

<i>Szempont</i>	<i>Leírás</i>	<i>Unified WLAN Megoldás</i>	<i>Autonóm WLAN Megoldás</i>
<i>Beágyazott vezeték nélküli behatolás detektálási rendszer - Intrusion Detection System (IDS)</i>	Detektálási képesség AP kialakítás, támadás és nem azonosított hozzáférés előrejelzéséhez	Idegen, nem a rendszerhez tartozó AP, vagy kliens detektálása ezen jellemző segítségével valósítható meg. A kontroller és AP-jai közötti MAC protokoll megosztás segítségével az AP-k szkennelik a frekvenciát az adatforgalom szolgáltatása mellett. Az AP-k x.509-s tanúsítvánnyal csatlakoznak a kontrollerhez.	Használj egy WDS alapú IDS-t vagy adj egy burkolt WLAN megoldást! Bonyolultabb, külön RF menedzselő megoldás és eszköz gondoskodik ezen funkció kialakításáról. Pl. WLSE rádiófrekvenciás menedzsmment WDS funkció az AP-kon.
<i>Helymeghatározási szolgáltatás</i>	WLAN lefedettséget képviselő RSSI információ és a WiFi eszközök helyzetének láthatóvá tétele.	Akár 1000 WiFi berendezés szimultán követhető közvetlenül a WLAN infrastruktúrában. A kontroller összegyűjti az AP-k által küldött kliensekre jellemző rádiófrekvenciás információt és továbbküldi ezen információk grafikus megjelenítésére alkalmas eszköz csoportnak (WCS-Wireless Control System és Wireless Location Appliance). A kliensek helyzetei valós időben kerülnek megjelenítésre.	Használj egy Site Survey-t vagy egy burkolt WLAN! Bonyolultabb, külön RF menedzselő megoldás és eszköz gondoskodik ezen funkció kialakításáról. Pl. WLSE rádiófrekvenciás menedzsmment WDS funkció az AP-kon.
<i>WLAN-n keresztüli hang átvitele (VoIP)</i>	Költség hatékony, valós idejű hang szolgáltatás használata meglévő vezeték nélküli infrastuktúrán.	A kontroller előre meghatározza és koordinálja a hang hívások CAC kapacitását minden AP között ugyanazon csatornán. Ugyanakkor a kontrollernek van egy holisztikus képe a hálózatban lévő összes kliensről. Ez a képesség gondoskodik a felépült hívás kapacitásának biztosításáról minden AP-n keresztül.	Az autonóm AP rendszerben a híváshoz tartozó kapacitás vezérlését a 802.11e szabvány protokoll biztosítja az AP és kliens között. Azonos csatornán nincs mód koordinálni a híváshoz tartozó CAC képességet. Minden berendezés, mely ugyanazon csatornán működik interferenciának van alárendelve. Telepíts AP alapú Call Admission Control (CAC)! Vezérlés van egy AP-ként és nincs koordinálva az összetett AP-kon keresztül.
<i>Alacsonyabb TCO megtérülési költség</i>	Kisebb beruházási költség	Nagy kiterjedésű WLAN hálózati rendszernél az üzemeltetési és menedzselési költségek kedvezőbbek. Szoftver frissítés, konfiguráció kialakítás kliens hibakeresés	Kis számú AP kialakítású rendszernél.
<i>Vezetékes és vezeték nélküli egységesítés</i>	Egységes hálózati környezet	A vezetékes és vezeték nélküli hálózat integrálása kritikus az egységes hálózat ellenőrzése, skálázhatósága biztonsága és rendelkezésre állása terén. A kontroller képességei beintegrálható switchbe és routerbe is. A Cisco Unified Wireless Network támogatja a NAC-Network Admission Control és a CCX-Cisco Compatible Extensions kliens eszközökre	A vezetékes és vezeték nélküli hálózat integrálása kritikus az egységes hálózat ellenőrzése, skálázhatósága biztonsága és rendelkezésre állása terén. Az autonóm AP egységesítését a működtető szoftver biztosíthatja

2. táblázat Unified és Autonóm WLAN hozzáférési hálózati megoldások összehasonlítása

<i>Szempont</i>	<i>Leírás</i>	<i>Unified Megoldás</i>	<i>Autonóm Megoldás</i>
<i>Layer3 Fast Secure Roaming</i>	Folyamatos IP kapcsolat a kliens roamingja alatt a subnetekben az AP és a VLAN-n keresztül.	A kontroller látja el ezen feladatot. Nincs szükség VLAN-ok közötti roamingra. A kontroller menedzsel minden roamingot és tunnelinget egyik subnetből a másikba.	Nem elérhető autonóm AP rendszerben, önmagában az AP nem képes rá. Egy centralizált megoldás szükséges a roaming elősegítése érdekében. A kapcsolódó vezetékes hálózatnak szükséges biztosítania.
<i>Frissítési költségek</i>	Idő a fejlődéshez, megnövekedett menedzsment kapacitás és beilleszteni az új imaget az AP-ba	A kontrolleren egy imageben vannak tárolva az AP-k beállítási konfigurációja. Amikor a kontroller imaget frissítjük, úgy az összes csatlakoztatott AP beállítása upgradelt állapotba kerül.	Fejlessz ki egy központosított menedzsment állomást vagy használj menedzsment scriptet!
<i>Load Balancing</i>	Automatikus kliens feltöltési kiegyenlítés a közeli AP-k között.	A kontroller látja el ezen feladatot. Az AP-k kontrollált vezérlése során ismert az AP-k kihasználtsága.	Önálló AP-k hirdetik a feltöltést, de a feltöltés nem automatikusan van szétkenve az AP-k között.
<i>Management</i>	Költség hatékony, egyszerűsített WLAN menedzselés és bevezetés.	A kontroller menedzsment felületéből egyszerűen konfigurálhatók az egyes profilok. További rádiófrekvenciás menedzsment felhasználói funkciók külön eszközzel biztosítható.	Implementálj scriptet vagy SNMP megoldással konfigurálj WLAN menedzsmentet és konfigurálj minden egyes AP-t önállóan!

3. táblázat Unified és Autonóm WLAN hozzáférési hálózati megoldások összehasonlítása

2.1.4 Specifikációk

A kialakítandó WLAN hozzáférési hálózati rendszer szabványos protokollokat és szabadon felhasználható frekvenciasávot, üzemi vivőfrekvenciát alkalmazzon az IP csomagok átviteléhez! Legyen alkalmas a jövőben bevezetésre kerülő szabványok támogatására és kezelésére!

A kialakítandó WLAN hozzáférési rendszer a következő műszaki tulajdonságokkal rendelkezzen:

A kiválasztott gyártó és eszköz:	Cisco Aironet 1130 sorozat berendezés családja.
WLAN rendszer kialakítás:	Egységesített, kontroller alapú, központi menedzselésű WLAN hozzáférési rendszer Access Point típusú hozzáférési csomópontokkal.
Antenna kiválasztás:	Az Access Pointokon integrált kivitelű megoldással.
Átviteli frekvencia tartomány:	2,4GHz az IEEE 802.11bg protokoll használatával, 5GHz az IEEE 802.11a protokoll használatával.
Frekvencia működtetés normája:	Európai, az NHH szabályozásnak megfelelően.
Megfelelőségi szabvány:	CE tanúsítvány, WiFi, WPA/WPA2, WMM minősítés.
Tervezett hozzáférési kapacitás:	54Mbps átviteli frekvencián.
LAN interfész kapcsolódás:	10/100 BaseT Tx, szükség esetén 1000BaseT Tx
WLAN AP tápfeszültség ellátása:	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 és CLI egyidejű alkalmazás lehetőségét támogassa az üzemeltetés során.

2.1.5 WLAN rádiófrekvenciás lefedettség helyének meghatározása

A kialakítandó WLAN hozzáférési hálózat lefedettségének területei terjedjenek ki a telephely1 és telephely2 épületek következő emeleti szintjeire:

- telephely 1 Földszint
- telephely 1 Első emelet
- telephely 1 Második emelet
- telephely 1 Harmadik emelet
- telephely 2 Földszint
- telephely 2 Első emelet

2.1.6 Hozzáférési hálózati topológia

Meglévő, vagy újonnan kialakítandó, vezetékes LAN Ethernet hozzáférési pont kiterjesztése szabványos WLAN rendszer segítségével a telephely 1 és telephely 2 épületben működő vezeték nélküli LAN felhasználók részére.

A rádiófrekvenciás lefedettséget biztosító AP-k Ethernet interfészen keresztül kapcsolódjanak a meglévő LAN hálózathoz 10/100BaseT csatlakozási pontjaihoz. Az AP-k beállításai egy erre alkalmas központi szerveren (WLAN kontroller) kerüljön tárolásra és működtetésre. Az AP-k és a kontroller között a kapcsolat Layer3 OSI modell szerinti kialakítású legyen. A WLAN kontroller Gigabit Ethernet Tx csatlakozással kapcsolódjon a meglévő vezetékes LAN hálózathoz.

A kialakítandó WLAN hozzáférési hálózati rendszer architektúrája egy WLAN AP által kiterjesztett pont több pont (PMP) felépítésű legyen.

2.2 WLAN végponti alkalmazások és szolgáltatások

A vezeték nélküli LAN hozzáférési rendszer végponti kliensei részére - jogosultságnak megfelelően - az AP-kon keresztül teljes IT hálózati joggal bíró kliensek. Ezért ugyanazon alkalmazások futtatására van lehetőség, mint a vezetékes LAN hálózatokon keresztül. A WLAN klienseken elkülöníthetően a következő szolgáltatási típusok, kialakítása legyen biztosítható:

- Vendég felhasználók részére nyilvános WiFi internet szolgáltatás, megfelelő biztonsági kontroll alkalmazásával.
- A cég belső WLAN telefon készülékei számára, IP alapú hang szolgáltatás megfelelő Layer2 szintű biztonsági protokoll használatával.
- A cég WLAN végponti kliensei részére a belső vezetékes hálózathoz történő hozzáférése megbízható Layer2 biztonsági protokoll alkalmazásával. Valamint ugyanezen mobil számítógépek képesek legyenek külső VPN kapcsolat kialakítására is.

2.3 WLAN hozzáférés szabályozása

A vezeték nélküli LAN hozzáférési hálózati rendszer szabványos WiFi felhasználói csoportok számára biztosít csatlakozási lehetőséget.

2.3.1 A cég belső mobil számítógépei

A cég belső mobil számítógépei, vagy külső adapter csatoló-; vagy integrált WLAN kártyával rendelkeznek, melyeknek a belső vezetékes LAN hálózathoz történő hozzáférése szükséges. A mobil számítógépek hardver kialakítása pl. HP nx8220 típusú, lehet, melyek Intel Centrino Mobile Technology, szabványos 802.11abg WiFi technológiát használnak.

A cég belső vezeték nélküli felhasználóinak azonosításánál meglévő, központi Cisco ACS RADIUS szerver végezi az azonosítást. A hálózat használati jogosultságának eldöntése egy meglévő AD-ban tárolt központi adatbázisból történik felhasználó név-jelszó páros alkalmazásával.

2.3.2 Vendég felhasználók mobil számítógépei

A vállalat területén a vendég felhasználók WLAN kliens végpontjai részére szabad hozzáférésű, vezeték nélküli internet szolgáltatás kialakítása valósuljon meg, megfelelően elkülönítve a belső hálózattól. A WiFi kliensek hálózathoz történő csatlakoztatásánál legyen lehetőség megbízható azonosítás és idő felhasználási korlátozás kialakítására!

2.3.3 A cég belső mobil IP telefonjai

A vállalat területén a belső, mobil IP telefon felhasználók, WLAN kliens végpontjai részére a telefonos hálózathoz történő hozzáférése a meglévő CallManager központ segítségével, más WiFi felhasználói csoporttól elkülönítetten valósuljon meg. A kialakítandó telefon kapcsolat működtetését, mint pl. hívószám kiosztását, hívás felépítését-, tartását és kapcsolat lebontási folyamatát a CallManager kontrollált vezérlésén keresztül biztosítsa. A WiFi VoIP kliensek hálózathoz történő csatlakoztatásánál legyen lehetőség megbízható Layer2 szintű azonosítás, jogosultság és titkosítás kialakítására!

2.4 Biztonsági követelmények – WLAN Security

2.4.1 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, L2 szinten az IEEE802.11i szabványajánlásnak megfelelően.

A vezeték nélküli végponti kliens felhasználók azonosítása szabványos szerver alapú azonosítás alapján valósuljon meg, mely a cég 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, 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.

2.4.2 WLAN kliens végponti előírások

A vezeték nélküli LAN hozzáférési hálózathoz minden olyan egyéb más gyártójú, végponti berendezés is csatlakozhat, amely a következő elsődleges feltételeknek megfelel:

- Rendelkezzen Wi-Fi minősítéssel. A WECA (Wireless Ethernet Compatibility Alliance - Wi-Fi Alliance, www.wi-fi.org) előírásnak megfelelően alapvető feltétel az AP-tal és a WLAN hozzáférési hálózattal történő, megbízható együttműködésre.
- Legyen alkalmas WPA, WPA2 kulcsmenedzsment kialakítására. Szintén WECA minősítés, mely a WLAN biztonsági együttműködést szavatolja és biztosítja.
- A WLAN kapcsolat biztonsági együttműködés kialakításánál feleljen meg a Cisco Compatible Extensions (CCX) program által megkívánt és megfelelő verziójával.

2.5 Vezetékes LAN hálózati infrastruktúra

A cég belső hálózatán meglévő switchelt portok használatával a WLAN hozzáférési hálózat AP-ja és WLAN kontroller központi berendezése egy erre a feladatra dedikált és elkülönített virtuális hálózatban működjenek.

Az AP-k 10/100BaseT FastEthernet interfész csatlakozással, RJ45 fizikai csatlakozóval, full duplex módon kapcsolódjanak a LAN switch hálózati porthoz.

A központi vezérlő berendezés 1000BaseT GigabitEthernet protokoll, full duplex és RJ45 fizikai csatlakozóval rendelkezzen.

A meglévő vezetékes LAN hálózat virtuális kapcsolatai előre definiált, routolt konfigurációban működnek egymással. A kontroller Layer3 szintű IP kapcsolatainak kialakítását és hálózatba történő integrálását ezen meglévő, szabály figyelembe vételével és betartásával szükséges végrehajtani!

2.6 WLAN hálózat felügyelete, menedzselése

A távközlésben a hálózat menedzsment a felügyelet azon megkívánt összes, szükséges funkcióinak és beállításainak üzemeltetési feladatait jelenti, melyek az adatátviteli forgalom

tartós fenntartása érdekében történik. Ezen feladatok az ellenőrzés, tervezés, allokáció, fejlesztés, koordinálás, monitorozás és riportkészítés.

A szabványos vezeték nélküli LAN menedzselési megoldások végleges kidolgozásáig (IEEE 802.11v) a gyártók különféle gyártó specifikus megoldásokkal - természetesen figyelembe véve a standardajánlás tervezett, draft útmutatásait is - biztosítják a WLAN eszközrendszerük minél szélesebb körű hálózat fenntartási feladatainak kiszolgálását.

A WLAN hozzáférési hálózati rendszer menedzselésének feladatai, terjedjen ki:

- Kezdeti és utólagos hálózat kialakítási és fejlesztési feladatok támogatására (Site Survey támogatása, rádióallokáció, Re-Site Survey),
- WLAN berendezés, eszköz menedzselésére (konfiguráció-; és Firmware módosítás; hibadetektálás és hibakezelés; forgalmi adatok ellenőrzés, mérése; lokáció-menedzselés)
- Rádiófrekvenciás menedzselésre (AP radio scan; kliens vándorlás nyomon követése; AP, kliens rádiómonitorozás, AP lefedettség megjelenítés),
- Interferencia zavartatás detektálása (Idegen WLAN AP kezelése; más azonos sávban működő rádiófrekvenciás zavartatás feltérképezése és elkülönítése;
- Más, nem 802.11 hálózattal történő együttműködtetési feladatok kezelése, támogatása (Más menedzsment rendszer integráció, egyéb vezeték nélküli rendszer és/vagy vezetékes hálózati elemek menedzselési képessége),
- WLAN kliens végpont menedzselése (forgalmi adatainak megjelenítése, ellenőrzése; kliens vándorlás követése),
- WLAN hozzáférési hálózat biztonsági folyamatainak ellenőrzési támogatása,
- WLAN menedzselési feladatok riport készítésének támogatása.

A vezeték nélküli hozzáférési hálózat AP berendezései legyenek alkalmasak, mind lokálisan, mind távolról történő elérésre és konfigurálhatóságra.

A WLAN rendszer központi eleméből ellenőrizhető legyen, a hozzá csatlakoztatott vezeték nélküli kliens végpontok főbb kapcsolati jellemzői.

A WLAN hálózati rendszer együttes működése és kontrolja központosítva, távolról is ellenőrizhető legyen! A hálózat felügyelet legyen alkalmas, a csatlakoztatott WLAN kliens végpontok alapvető rádiófrekvenciás és biztonsági beállítási jellemzőinek ellenőrzésére és megjelenítésére.

A WLAN hozzáférési rendszer Access Pointjainak konfigurációs beállításait és összegyűjtött rádiófrekvenciás paramétereit a vezeték nélküli hálózat kontroller berendezésében, egy helyről legyen elérhető, felügyelhető és monitorozható.

A rendszer biztosítson lehetőséget a jövőbeni WLAN lefedettség bővítésére további AP szám növelésével és üzembe helyezési lehetőséggel.

3 A megvalósított WLAN hálózat bemutatása

A WiFi hozzáférési hálózatot Cisco Unified WLAN centralizált hálózat rendszer telepítésével valósítottuk meg. A központi kontroller funkcióját egy AIR-WLC4402-25-K9 típusú berendezés biztosítja, mely 25 db LWAPP WLAN Access Point menedzselését és dinamikus rádiófrekvenciás működtetését engedi meg. Access Pointként összesen 20 db AIR-LAP1131AG-E-K9 típus került telepítésre.

A kiépített WLAN rendszer, mind adat, mind hang együttes átvitelét biztosítja 802.11abg Ethernet protokollon keresztül.

3.1 Rendszertechnika

Az elfogadott végleges WLAN rendszertechnika általános logikai felépítését, kapcsolatait és a meglévő hálózati eszközök integrációját az 1 ábra szemlélteti.

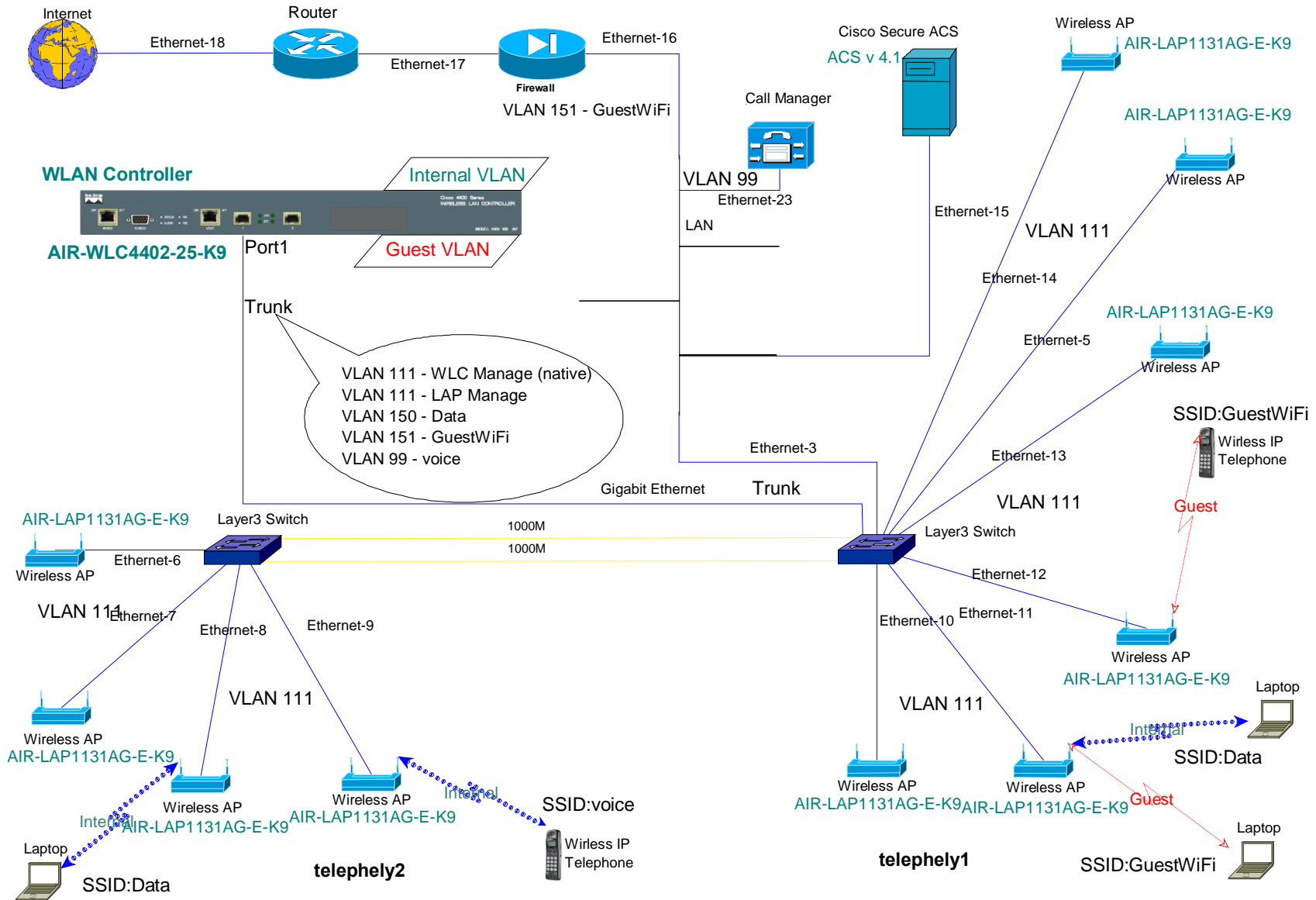
3.1.1 Átviteltechnika

A WLAN hozzáférési hálózati rendszer kialakított VLAN átviteli útjait a 2. számú ábra logikai vázlat alapján követhetjük nyomon.

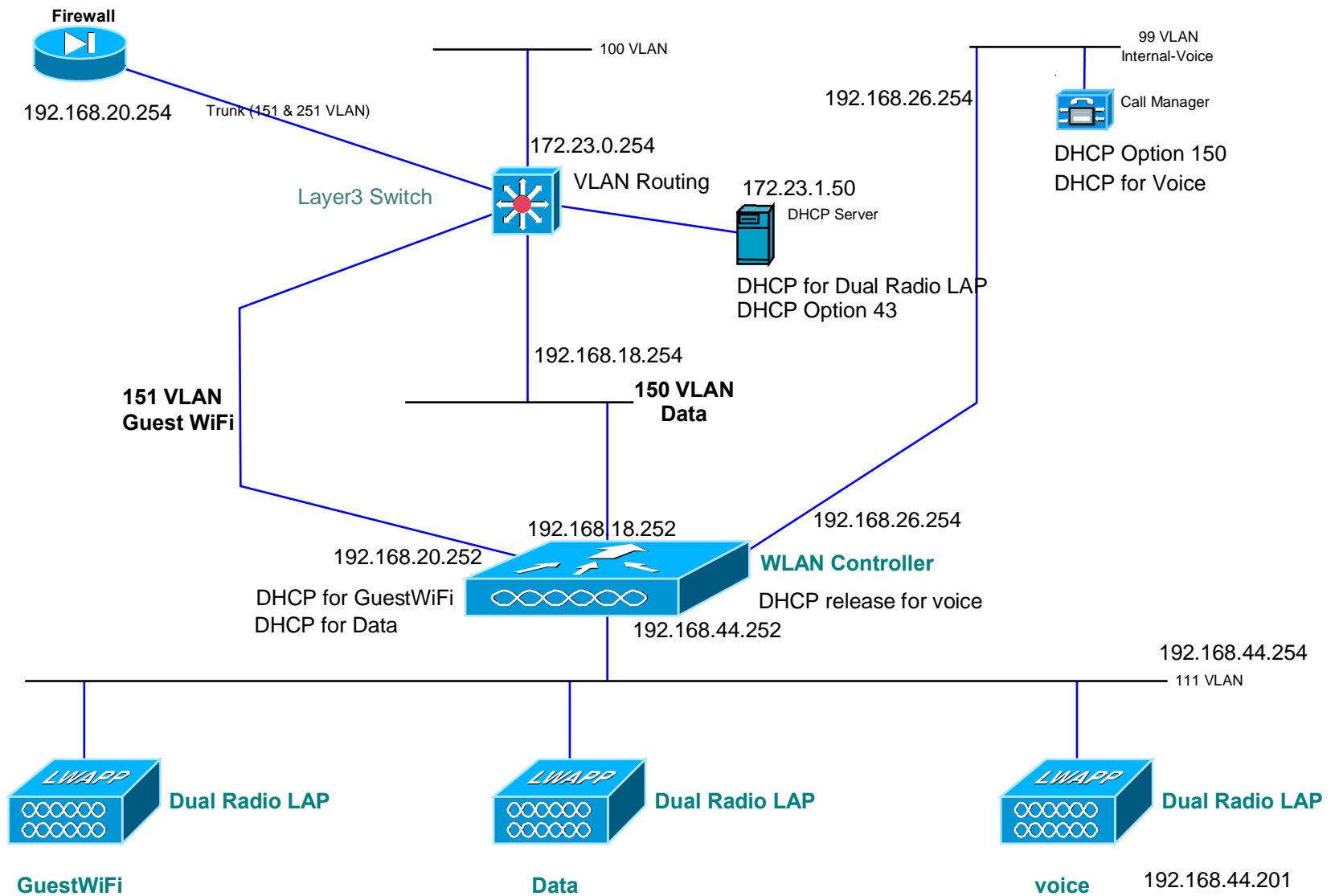
3.2 UTP kábelhálózati rendszer

A WLAN kontroller és a távoli LWAP Access Pointok kapcsolatának biztosításához fizikai Cat5-s kábel hálózat bővítése vált szükségessé a disztribúciós hálózati oldalon.

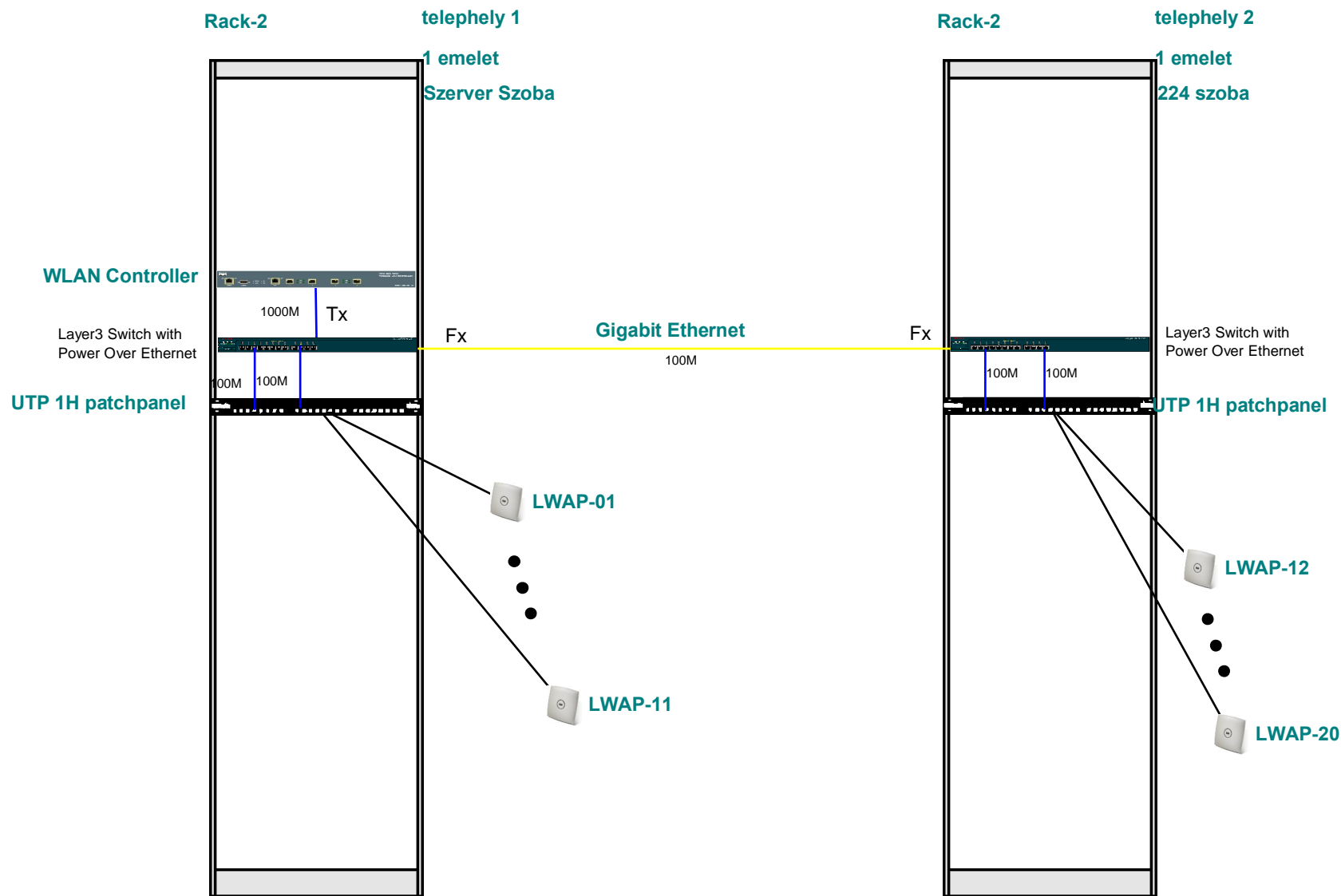
Az UTP hálózat kiépítése a 3. ábra logikai vázlata és az AP tervezett fizikai elhelyezése alapján valósult meg egy külső alvállalkozó telepítési munkája segítségével.



1. ábra, A cég egységesített WLAN hozzáférési hálózatának logikai vázlata



2. ábra, A cég egységesített WLAN hozzáférési hálózatának VLAN átviteli vázlatja



3. ábra WLC elhelyezése és LWAP AP bekábelezésének logikai vázlatja

3.2.1 UTP – Switch Port bekötés

A kihelyezett és telepített WLAN AP-k rendezői és switch port bekötését az 1 számú táblázat részletezi.

AP Név	Rendező Helyiség	Rack Szekrény	Patch Panel UTP Csatlakozó	Switch Port
AP_TI_fszt_Elso_lepcso	telephely1	1	1	2/0/24
AP_TI_fszt_Kozep	telephely1	1	2	2/0/27
AP_TI_fszt_Hatso_lepcso	telephely1	1	3	2/0/28
AP_TI_Atjaro_TII_fele	telephely1	1	4	2/0/45
AP_TI_1em_1	telephely1	1	5	2/0/32
AP_TI_1em_2	telephely1	1	6	2/0/31
AP_TI_2em_1	telephely1	1	7	2/0/29
AP_TI_2em_2	telephely1	1	8	2/0/30
AP_TI_3em_Elso_lepcso	telephely1	1	9	2/0/25
AP_TI_3em_Kozep	telephely1	1	10	2/0/26
AP_TI_3em_Hatso_lepcso	telephely1	1	11	2/0/23
AP_TII_Fsz_Sarok	telephely2	2	1	1/0/45
AP_TII_Fsz_Service	telephely2	2	2	3/0/45
AP_TII_Fsz_Bejarat	telephely2	2	3	3/0/47
AP_TII_Fsz_Iroda1	telephely2	2	4	3/0/48
AP_TII_Fsz_Iroda2	telephely2	2	5	1/0/46
AP_TII_1em_Iroda1	telephely2	2	6	2/0/45
AP_TII_1em_Iroda2	telephely2	2	7	1/0/47
AP_TII_1em_Iroda3	telephely2	2	8	3/0/46
AP_TII_1em_Iroda4	telephely2	2	9	3/0/33

1. számú táblázat WLAN Access Pointok UTP és Switch bekötése

3.3 WLAN AP-k fizikai elhelyezése

A WLAN AP-k fizikai elhelyezése és telepítése a Rendszertechnikai tervnek megfelelően valósult meg.

Az AP-k szimulációs, alaprajzon feltüntetett elhelyezési rajzait a Rendszertechnika terv alapján, jelen dokumentum Melléklete is tartalmazza.

Az AP-k fizikai elhelyezése általában takartan került kivitelezésre, az álmennyezetet tartó acél szerkezet fölé.

Néhány helyszínen, ahol nem található bontható álmennyezet (telephely II Fsz Iroda2 és telephely II 1em Iroda2) az AP-k rögzítését az álmennyezet szintje alatti falfelületre valósítottuk meg.

3.4 Rádiófrekvenciás peremfeltételek

A WLAN hozzáférési hálózati rendszer rádiófrekvenciás jellemzőjét a WLC kontroller alap beállítása biztosítja (dinamikus RRM), mindkét frekvencia sávban, melyeknek értékei a következők:

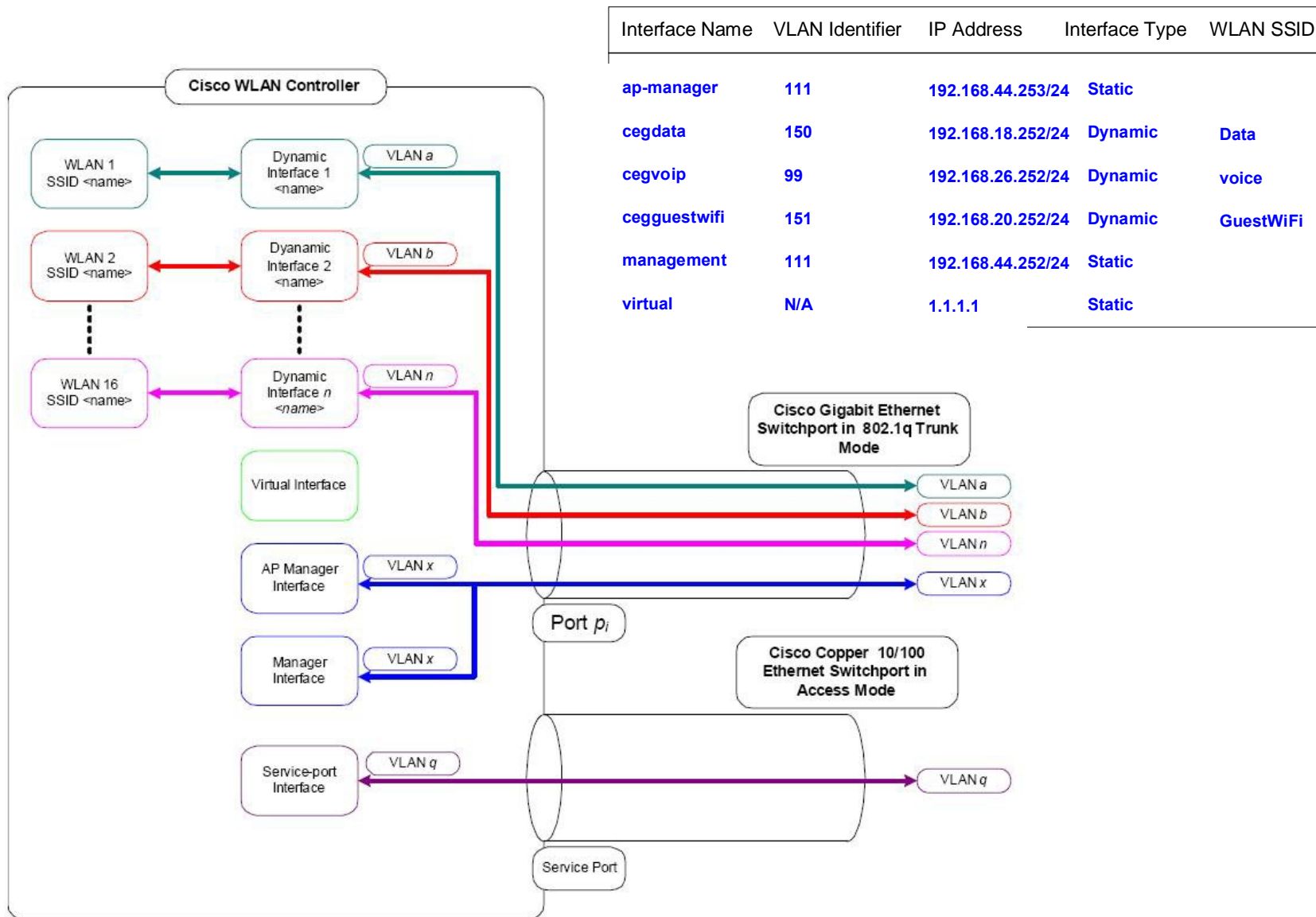
- Protokoll: IEEE802.11abg
- AP Tx Power: Automatikusan minden 600sec (1-től 8-ig (Minimális) változhat, általában: 1=Maximális, 2=50%-kal csökkentett értéket vesz fel)
- Coverage Treshold: RSSI mind adatnál, mind hang átvitelénél jobb, mint -80dBm vételi jelszint,
- Kapacitása: 802.11a: 6-tól 54Mbps-ig, 802.11bg: 1-től 54Mbps-ig.
- Interferencia: Minimalizálva (-85dBm-nél gyengébb zavartatási jelszint)
- Csatorna kiosztás: Európai, 2,4GHz (CH1; CH7; CH13); 5GHz (CH36-CH64)

3.5 WLAN kontroller elhelyezése

A Cisco Unified Wireless hozzáférési hálózat központi berendezését (AIR-WLC4402-25-K9) a telephely I első emeleti rendező helyiségének 2-s 19"-s rack szekrényében telepítettük és helyeztük üzembe. A kontroller redundáns 230Vac betáplálást kap a hálózati feszültségből.

A WLC4402 kontroller rezes GigabitEthernet interfészen keresztül csatlakozik a meglévő Ethernet hálózati switch port-hoz.

A WLC logikai kapcsolatának és működésének megértését segíti a 3. számú ábra. A kontroller konfigurációjában az ábrán szereplő táblázati interfészek és jellemzők kerültek beállításra



3. ábra, Wireless LAN Controller (WLC) átviteli kapcsolatai és interfészei

4 Eszközök IP cím kiosztása

Az alkalmazásra került IP címeket, interfészeket és azok fő jellemzőjét a 3. számú ábra táblázata részletezi.

4.1 WLAN AP-k IP címei

A WLAN hozzáférési hálózati rendszerben működő csomópontok, AP-k IP címének kiosztását a központi DHCP szerver és azon megfelelő szabály kialakítása biztosítja.

4.2 WLAN kontroller IP címe

A WLC4402 kontrollert a 192.168.44.252 IP címen keresztül a 111-s logikai VLAN-ban akár grafikusán, akár CLI felületen menedzseljük. A WLC konfigurációjában ezen, jellemzőket a „management” interfész névhez kapcsoltuk.

4.3 WLAN kliens végpontok IP cím kiosztása

A WLAN rendszerhez hozzáférő és csatlakozni kívánó kliens végpontok IP cím kiosztása az alkalmazott hálózatnak megfelelően a következőképpen valósul meg:

- Vendég felhasználók (SSID=GuestWiFi, VLAN=151) IP cím kiosztását a WLC4402 kontroller „cegguestwifi” interfész felületén keresztül a 192.168.20.x IP cím tartományból biztosítja a mobil kliensek részére.

A kontroller belső DHCP Serverén „guest_lan” nevű DHCP pool a 192.168.20.224 – 192.168.20.251 IP cím tartomány került kialakításra.

- A belső vállalati felhasználók részére (SSID=Data, VLAN=150) az IP cím kiosztását szintén a WLC4402 kontroller biztosítja a „cegdata” interfészén keresztül a 192.168.18.x IP cím tartományból.

A kontroller belső DHCP Serverén „Internal_lan” nevű DHCP pool a 192.168.18.224 – 192.168.18.251 IP cím tartomány került kialakításra.

- A belső WLAN hangfelhasználók részére (SSID=voice, VLAN=99) az IP cím kérés a WLC4402 kontroller „cegvoip” interfészén keresztül továbbításra kerül az IP címet biztosító központi CallManager felé. A CallManager a 192.168.26.x hálózatból oszt ki IP címet a jogosult WLAN mobil kliens felhasználók részére.

5 WLAN Security kialakítása

A kontroller és a kihelyezett AP-k a WLAN biztonság kialakítási folyamatában fontos (authenticator) helyet foglalnak el. A belső WLAN kliensek azonosítását Cisco Secure Access Control Server (ACS) 4.1-s verziójú szerver (172.23.1.23; 1812 Port) biztosítja. A WLC szabványos RADIUS protokollon keresztül kommunikál az azonosítási szerverrel.

A kontroller konfigurációjában definiálva lett a RADIUS szerver IP címe, az alkalmazott Port azonosítója és a kétirányú kommunikációhoz használt Shared Secret azonosító karakter sorozata.

A WLC grafikus felületén a Security menüpontban ellenőrizhetjük és módosíthatjuk az azonosításban résztvevő RADIUS szervereket. Jelenleg kialakított WLC-Radius szerver kapcsolati lehetőségek a Server Index sorszámoknak megfelelően:

- 172.23.1.23 Port:1812
- 172.23.1.72 Port:1812
- 172.23.1.36 Port:1812

A WLAN hálózat 802.1x alapú kapcsolat kialakításához megadhatjuk az azonosításban résztvevő RADIUS szervert a WLANs/CegData/Edit/AAA Servers menü pontban. Maximum 3 Radius szerver fő jellemzőit adhatjuk meg egy kapcsolathoz. Jelenleg a belső WLAN hozzáférési hálózathoz kapcsolódó WiFi supplicant kliensei a 172.23.1.23 IP című Radius szerverhez kerül továbbításra az EAP azonosítási csomagok a WLC4402-25-k9 kontroller által a 1812-s porton keresztül.

5.1 Eszköz konfiguráció hozzáférés

A WLAN hozzáférési hálózat konfigurációs állományát a központi kontroller tartalmazza. A berendezés beállításának hozzáféréséhez három felhasználónév és jelszó páros került kialakításra, melyből egy végső felhasználás céljából zárolt jellegű.

A használatban lévő account felhasználó neveket és jogosultságukat a Management/Local Management Users menüpont alatt tekinthetjük meg és módosíthatjuk a grafikus felületen:

- „admin” ReadWrite
- „dobosd” ReadWrite
- „auditor” ReadOnly

5.2 Átviteli 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 vezeték nélküli LAN felhasználók Internet hozzáférése teljesen nyílt (Open), szabad hozzáférésű. A rádiófrekvenciás média nem kerül titkosításra.
- A belső WiFi felhasználók WPA/WPA2 kulcs menedzsment és TKIP/AES titkosítás kódolási algoritmussal csatlakozhatnak a hálózathoz. A belső vezeték nélküli LAN kliensek hitelesítéséhez pedig a 802.1x szerver alapú, EAP módozatú megoldások közül a Microsoft által is támogatott PEAP-MSChapv2 módozatot ajánljuk bevezetni. Ez a hitelesítési eljárás tanúsítvány használatát is megengedi, meglévő PKI infrastruktúrával.
- A belső, mobil hang forgalom biztonsága érdekében WPA kulcsmenedzsment és TKIP titkosítás került beállításra. A hálózathoz, történő kapcsolódáskor előre definiált kulcs (Pre-Shared Key) megfelelő alkalmazása szükséges.

5.3 WLAN felhasználói csoportok biztonsági beállítása

A vállalat WLAN hozzáférési hálózati rendszerében a csatlakozni kívánó 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 WiFi felhasználók a cég belső hálózatát nem érhetik el. Csak nyilvános internet hozzáféréssel és szolgáltatással rendelkezhetnek. A 151-s VLAN-hoz tartozó WiFi Internet forgalom a cég Firewall-hoz kerül továbbításra.
- A cég belső WLAN IP kliensei részére a mobil telefon forgalmi szolgáltatásait, mind a belső mellékállomás, mind a külső hívás kialakítása érdekében a CallManagerben beállított szabály szerint valósíthatják meg.

6 WLAN Menedzsment

A cég WLAN hozzáférési hálózat eszközeinek felügyeleti menedzselése a következőképpen valósul meg:

- A LWAP és a WLC4402 kontroller ugyanazon hálózatba (VLAN=111), a valós forgalomtól történő elkülönítéssel alakítottuk ki.
- A WLC4402 kontrollert a 192.168.44.252 IP címen keresztül akár grafikusan, akár CLI felületen menedzseljük.
- A LWAP menedzselése a WLC4402 kontroller 192.168.44.253 IP című, „ap-manager” nevű interfész felületén keresztül alakítottuk ki.
- Syslog a WLC-n engedélyezve van.
- Biztonságos, tanúsítvány alapú https (SSH) protokoll alkalmazásával
- 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.

6.1 SysLog Server

A WLC által küldött Syslog hibaüzenetek a 172.23.1.50 Syslog Szerverre kerülnek továbbításra.

6.2 SNMP

A WLC4402-25-K9 típusú WLAN kontroller SNMP jellemzőinek beállítását a következők szerint állítottuk be, a Management/SNMP menüpont alatt:

- General
 - SNMP Port Number: 161
 - Trap Port Number: 162

- SNMP v1/v2c Community Name
 - Read Only: kis-sarkany 172.23.1.100/16
 - Read-Write: nagy-sarkany 172.23.1.100/16

7 Eszközlista

7.1 *Wireless LAN Controller (WLC)*

A letelepített és üzembe helyezett WLC kontrollerek főbb jellemzői:

- Manufacturer: Cisco Systems Inc.
- Model: WLC4402
- Type: AIR-WLC4402-25-E-K9
- Version ID: V02
- Name: ceg_wlc
- Serial Number: FOC1143F095
- Burned-in MAC: 00:1E:13:2A:C9:60
- Power Supply1: Operational
- Power Supply2: Operational
- Port1: GLC-T
- Port2: -
- Location: telephely I 1em. Rendező
- Software Version: 5.0.148

7.2 *Light Weight Access Pointok (LWAP)*

A letelepített és üzembe helyezett Access Pointok fő jellemzőit az 2 számú táblázat tartalmazza.

AP Name	Product ID	AP Serial Number	AP Ethernet MAC	AP Base Radio MAC	Location	802.11 CH
AP_TI_Fsz_Elso_lepcso	AIR-LAP1131AG-E-K9	FCZ1140Q1RH	00:1d:a1:ed:1e:90	00:1d:e6:24:fd:00	Elso lepcso 1-s patch panel port	g1
AP_TI_Fsz_Kozep	AIR-LAP1131AG-E-K9	FCZ1140Q1RP	00:1d:a1:ed:1e:f0	00:1d:e6:24:ff:d0	Kozep 2-es p. p. port	g7
AP_TI_Fsz_Hatso_lepcso	AIR-LAP1131AG-E-K9	FCZ1140Q1RT	00:1d:a1:ed:1f:10	00:1d:e6:25:00:b0	Hatso lepcso 3-as p. p. port	g13
AP_TI_1em_1	AIR-LAP1131AG-E-K9	FCZ1140Q1RB	00:1d:a1:ed:1e:7c	00:1d:e6:24:fc:30	Lift felöli 5-ös patch panel port	g13
AP_TI_1em_2	AIR-LAP1131AG-E-K9	FCZ1140Q1RC	00:1d:a2:7f:6b:84	00:1d:a2:84:e8:f0	Hátsó lépcső felöli 6-os p.p. port	g1
AP_TI_2em_1	AIR-LAP1131AG-E-K9	FCZ1140Q1RE	00:1d:a1:ed:1e:b8	00:1d:e6:24:fe:30	Lift felöli 7. patch panel port	g1
AP_TI_2em_2	AIR-LAP1131AG-E-K9	FCZ1140Q1RF	00:1d:a1:ed:1e:78	00:1d:e6:24:fc:b0	Hátsó lépcső felöli 8-as p. p. port	g7
AP_TI_3em_Elso_lepcso	AIR-LAP1131AG-E-K9	FCZ1140Q1RL	00:1d:a1:ed:1e:ac	00:1d:e6:24:fd:e0	Elso lepcso 9-es patch panel port	g7
AP_TI_3em_Kozep	AIR-LAP1131AG-E-K9	FCZ1140Q1RU	00:1d:a1:ed:1f:54	00:1d:e6:25:03:20	Kozep 10-es patch panel port	g13
AP_TI_3em_Hatso_lepcso	AIR-LAP1131AG-E-K9	FCZ1140Q1RA	00:1d:a1:ed:1e:64	00:1d:e6:24:fb:a0	Hatso lepcsol 11-es p. p. port	g1
AP_TI_Atjaro_TII_fele	AIR-LAP1131AG-E-K9	FCZ1140Q1RY	00:1d:a1:ed:1f:52	00:1d:e6:25:03:10	TI-TII atjaro folyoso 4-es p. p. port	g13
AP_TII_Fsz_Sarok	AIR-LAP1131AG-E-K9	FCZ1140Q1RM	00:1d:a1:ed:1e:e2	00:1d:e6:24:ff:80	Sarok 1-es p. p. port	g1
AP_TII_Fsz_Iroda1	AIR-LAP1131AG-E-K9	FCZ1140Q1RZ	00:1d:a2:7f:6b:cc	00:1d:a2:84:eb:40	Iroda1 4-es p.p. port	g13
AP_TII_Fsz_Iroda2	AIR-LAP1131AG-E-K9	FCZ1140Q1S1	00:1d:a1:ed:1a:e2	00:1d:e6:24:df:a0	Iroda2 2-es patch panel port	g7
AP_TII_Fsz_Iroda3	AIR-LAP1131AG-E-K9	FCZ1140Q1RD	00:1d:a1:ed:1e:8e	00:1d:e6:24:fc:f0	Iroda3 5-ös p. p. port	g13
AP_TII_Fsz_Bejarat	AIR-LAP1131AG-E-K9	FCZ1140Q1RG	00:1d:a1:ed:1e:2e	00:1d:e6:24:f9:f0	Fsz Bejárat 3-as p. p. port	g13
AP_TII_1em_Iroda1	AIR-LAP1131AG-E-K9	FCZ1140Q1RJ	00:1d:a2:7f:6b:a4	00:1d:a2:84:e9:f0	Iroda1 6-os p. p. port	g13
AP_TII_1em_Iroda2	AIR-LAP1131AG-E-K9	FCZ1140Q1RW	00:1d:a1:ed:11:a6	00:1d:e6:24:95:d0	Iroda2 9-es p. p. port	g1
AP_TII_1em_Iroda3	AIR-LAP1131AG-E-K9	FCZ1140Q1RX	00:1d:a2:7f:6b:ea	00:1d:a2:84:ec:20	Iroda3 7-es p. p. port	g1
AP_TII_1em_Iroda4	AIR-LAP1131AG-E-K9	FCZ1140Q1RK	00:1d:a1:ed:1e:72	00:1d:e6:24:fc:10	Iroda4 8-as p. p. port	g1

2. számú táblázat Eszközlista WLAN Access Pointok

8 Mellékletek

8.1 WLAN AP elhelyezési terv

Cég WLAN rendszer Access Pointok fizikai elhelyezés

Az AP-k tervezett telepítési helye általában az álmennyezet acéltartó fém szerkezetére történjen! Amennyiben ez nem kivitelezhető, ott a falra, az álmennyezet alá, maximum fél méterrel lejjebb szükséges az AP-t rögzíteni!

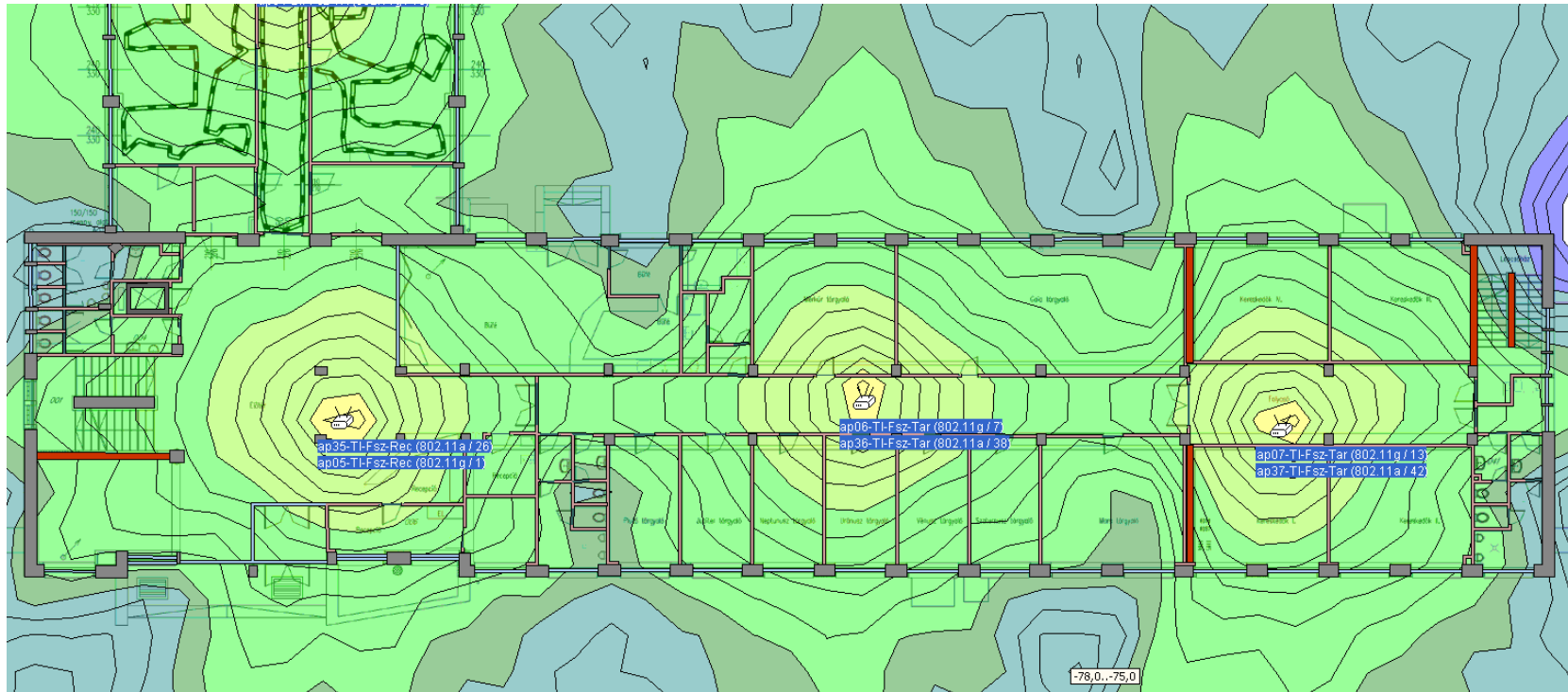
Az AP-k UTP kábelezésének kialakítása során az IEEE 802.3 protokoll alapján a kábel hosszúsága ne haladja meg a 90 métert a switch portja és a távoli AP portja között. Az UTP kábel végződtetésénél az AP-kat maximum 5 méteres patch kábellel végződtetve is 99 méter alatt maradjon a kábel hosszúsága!

A távoli végen 5 méter UTP kábel ráhagyás szükséges azért is, hogy az AP-k pontos elhelyezése korrigálható legyen a beállításakor!

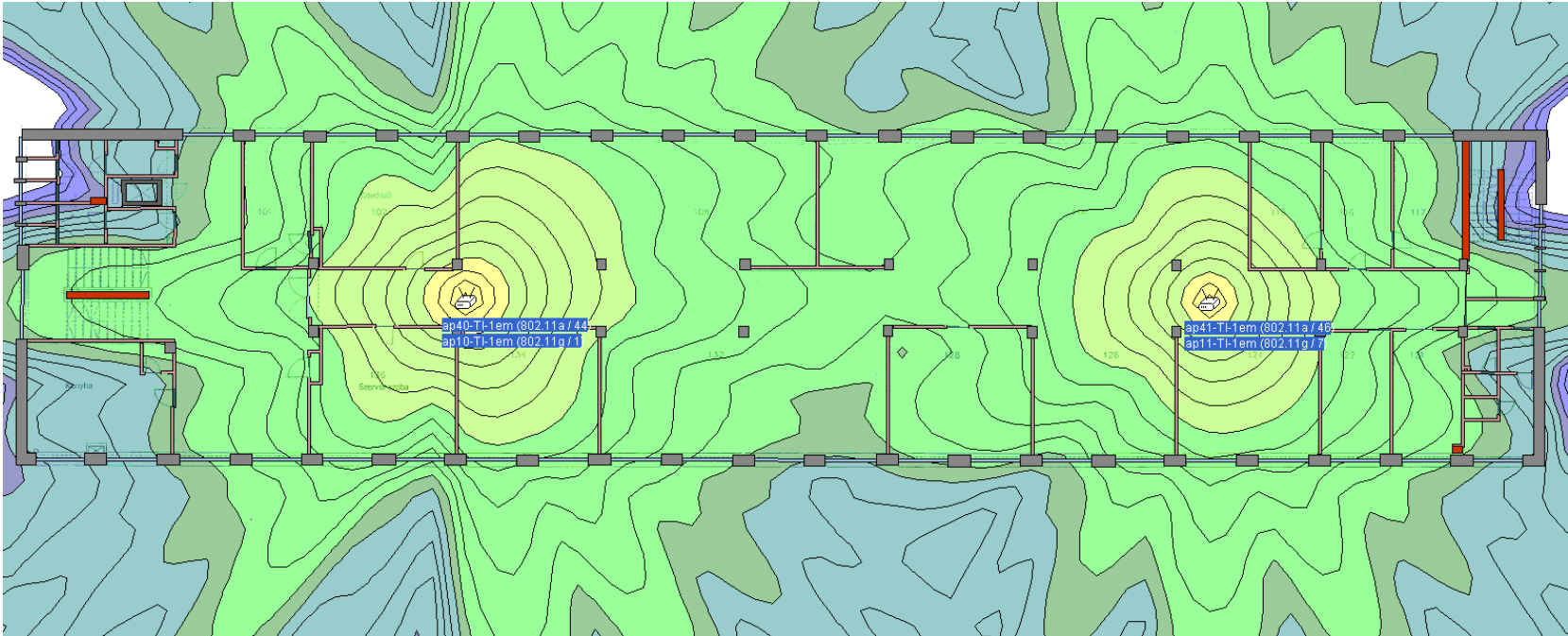
Az AP elhelyezésének meghatározását az ESS Prof v2.2 Site Survey program alapján készítettem.

Összefoglalva a következő helyszíneken kell AP-kat telepíteni:

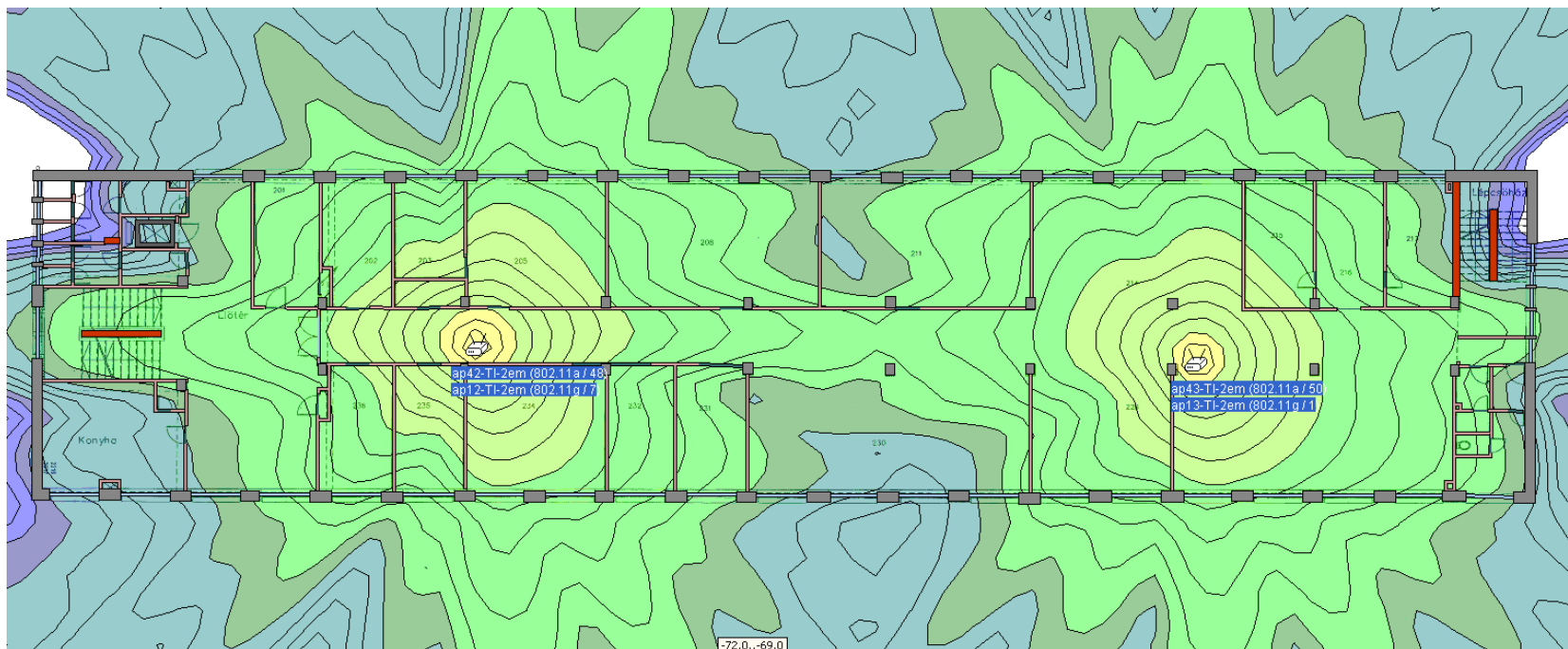
1. Telephely1 Földszint



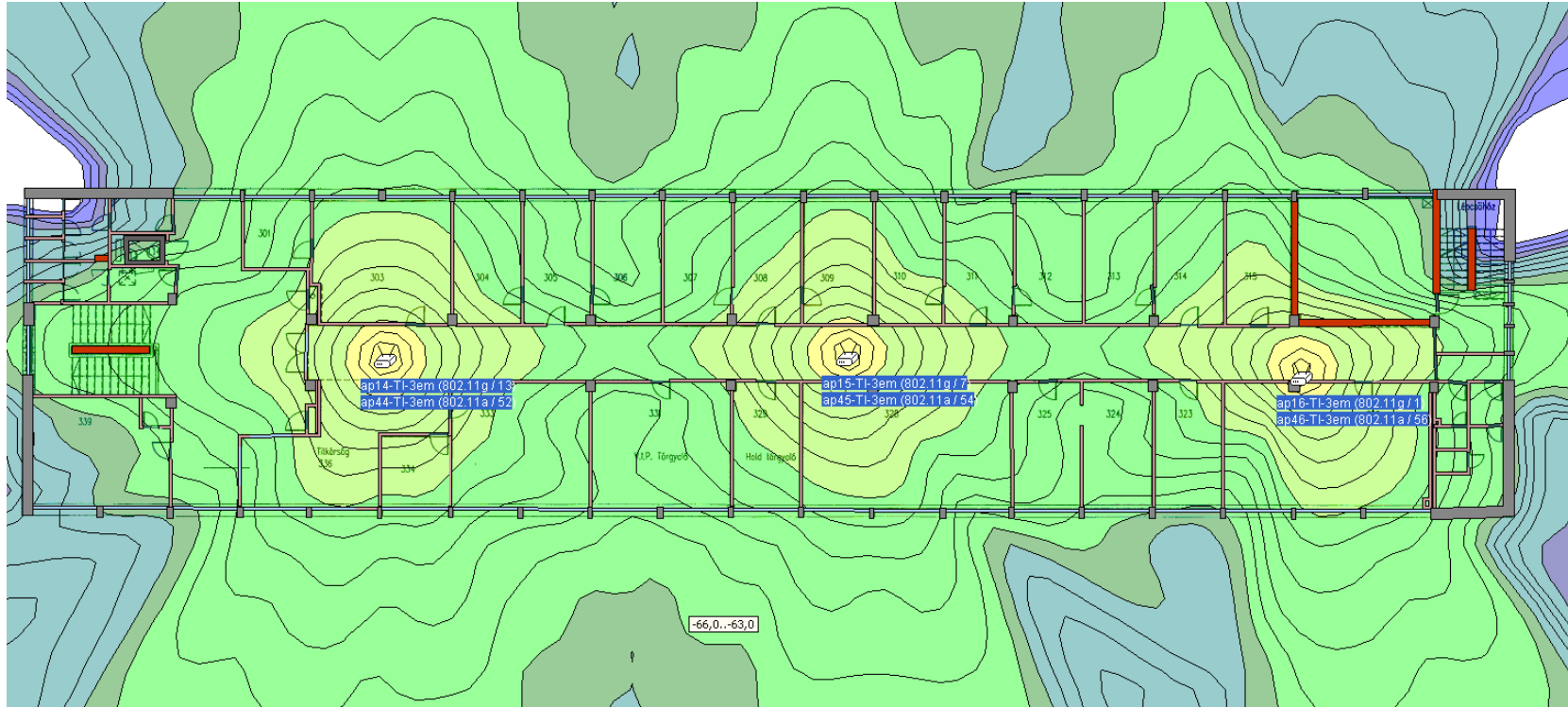
2. Telephely1 1 emelet



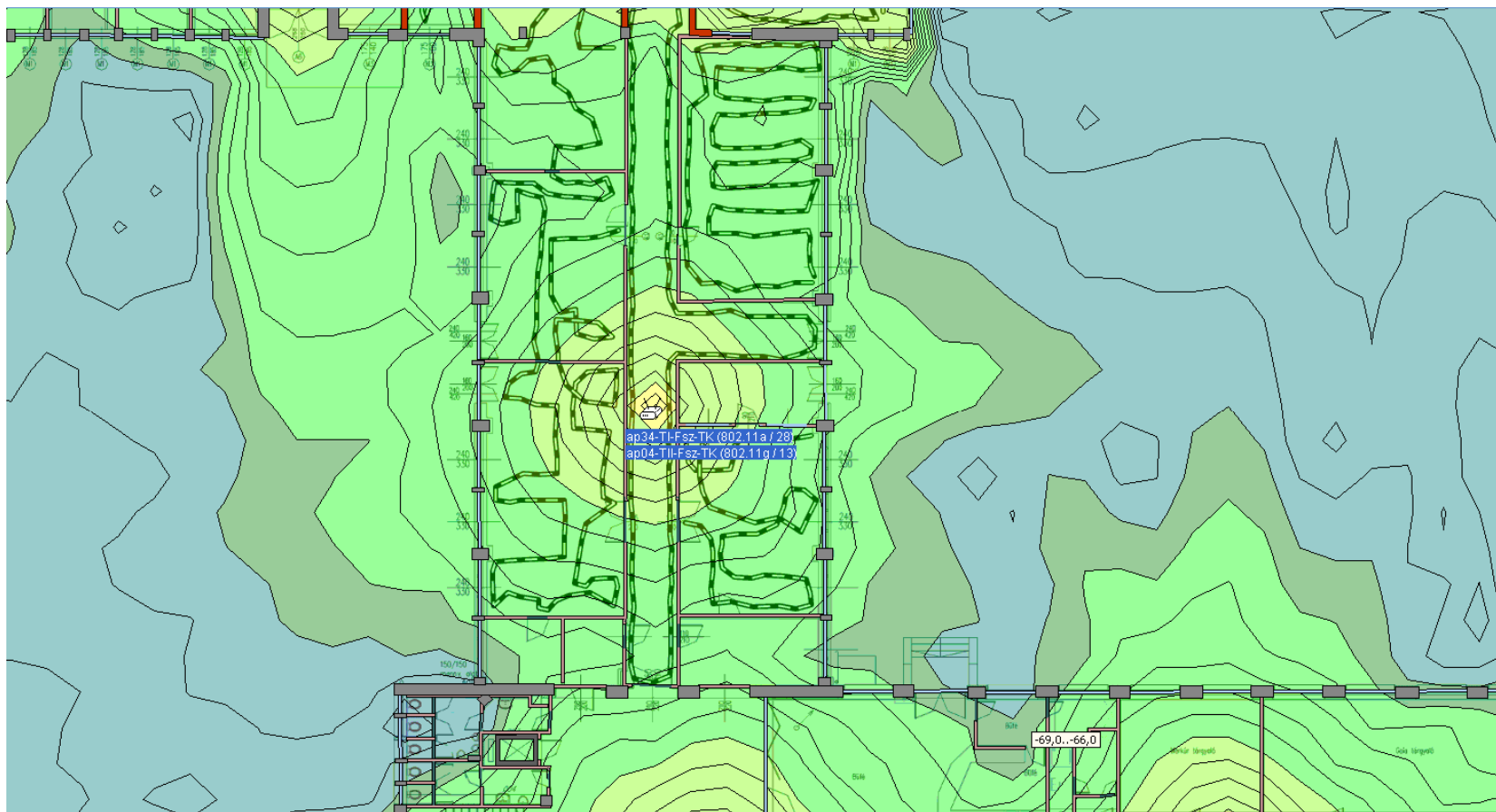
3. Telephely1 2 emelet



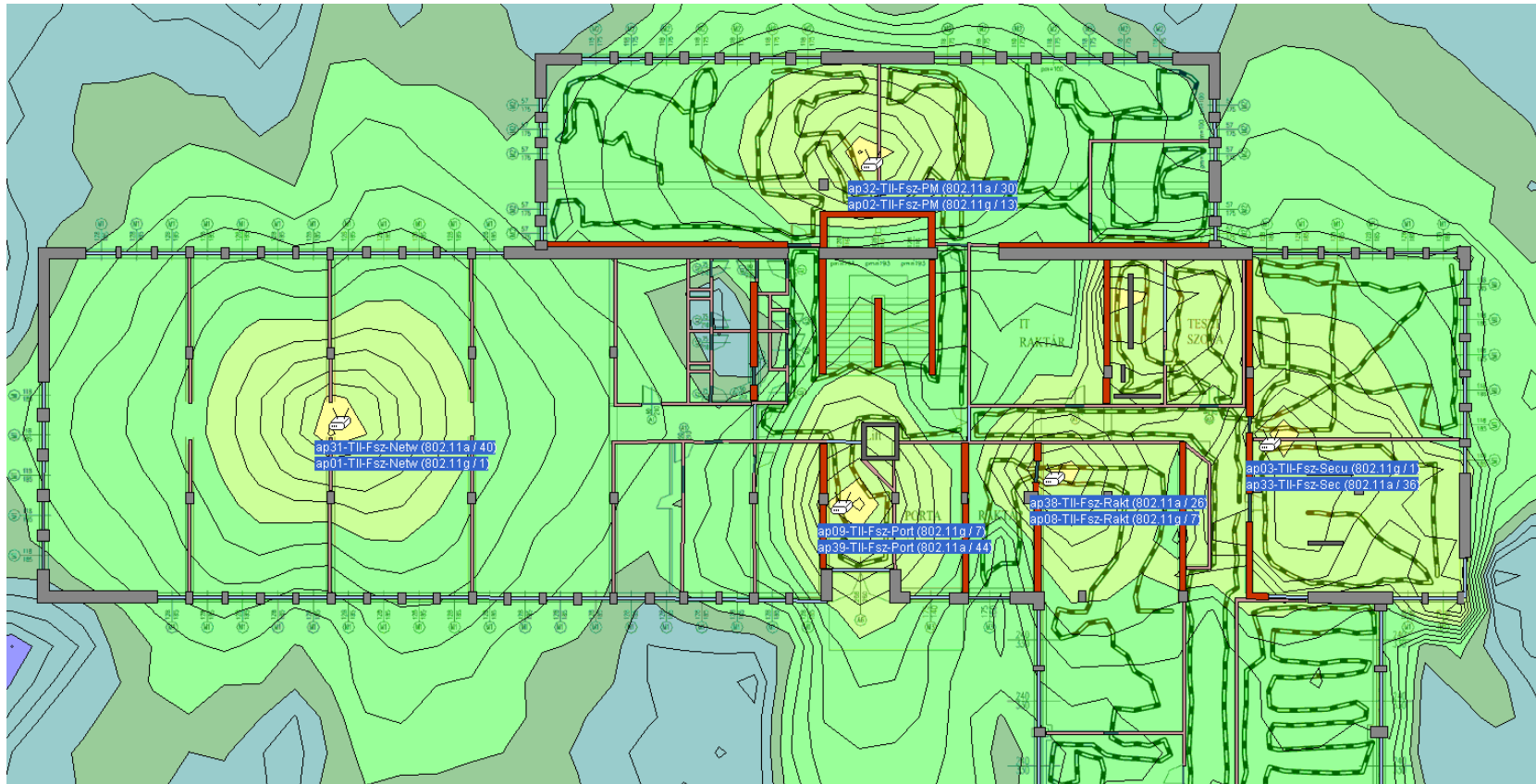
4. Telephely1 3 emelet



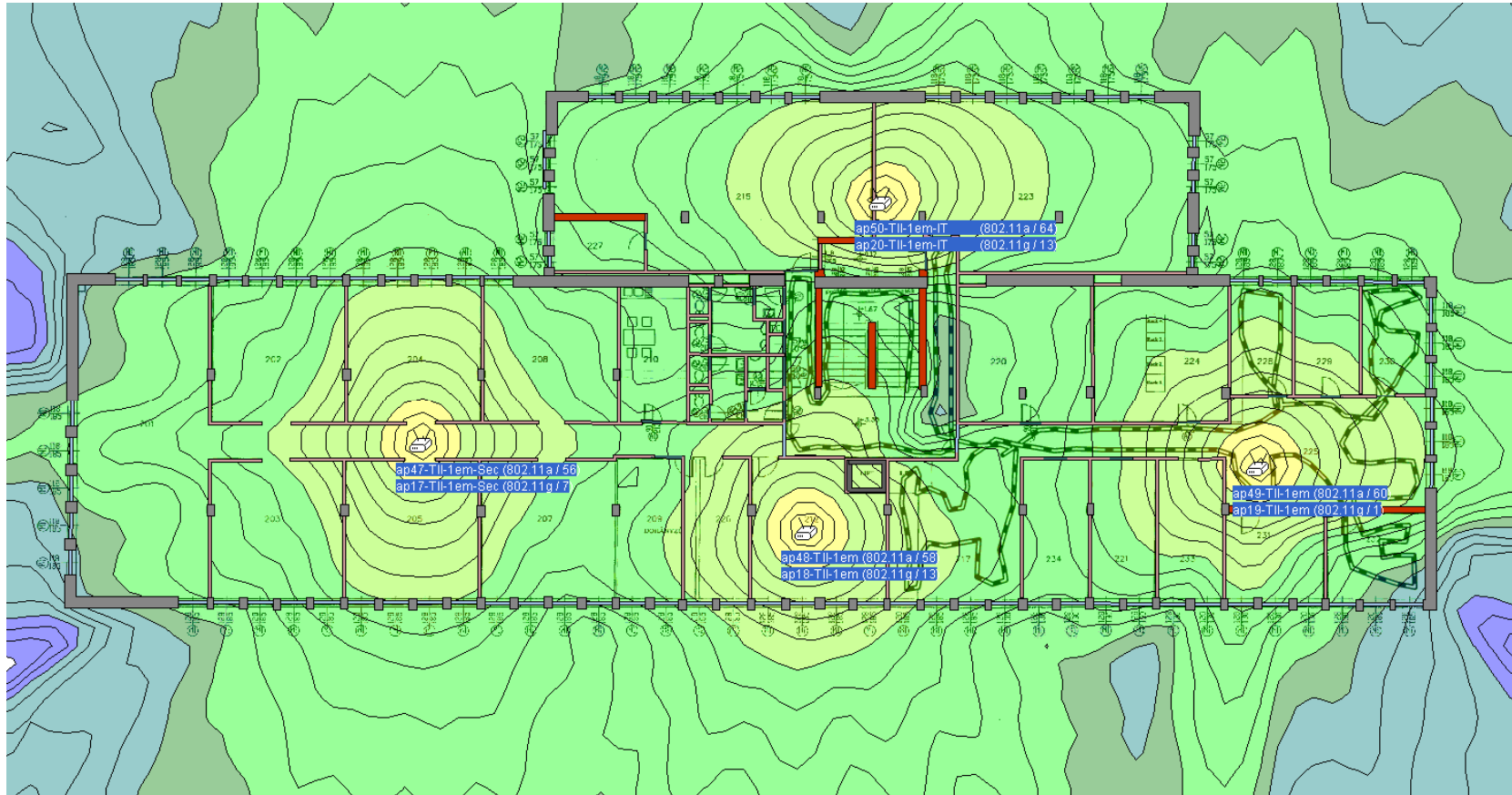
5. Telephely1 és Telephely2 átjáró folyosó



6. Telephely2 Földszint



7. Telephely2 1 emelet



8.2 Konfigurációs file

A „ceg_wlc” nevű, WLC4402-25-K9 típusú kontroller konfigurációs beállítását a következő állomány listák részletezik.

8.2.1 WLC futó konfiguráció

A WLC-n futó konfiguráció beállítását az alábbi állománylista tartalmazza.

```
(Cisco Controller) >show running-config
country HU

dhcp create-scope guest_lan

dhcp create-scope Internal_lan

dhcp address-pool guest_lan 192.168.20.224 192.168.20.251
dhcp address-pool Internal_lan 192.168.18.224 192.168.18.251
dhcp default-router guest_lan 192.168.20.254
dhcp default-router Internal_lan 192.168.18.254

dhcp enable guest_lan
dhcp enable Internal_lan
dhcp dns-servers guest_lan 194.38.96.80 193.225.86.1
dhcp dns-servers Internal_lan 172.23.1.17 172.23.1.23
dhcp domain guest_lan vallalat.hu
dhcp domain Internal_lan vallalat.hu
dhcp lease guest_lan 7200
dhcp lease Internal_lan 7200
dhcp netbios-name-server Internal_lan 172.23.1.17 172.23.1.23
dhcp network guest_lan 192.168.20.0 255.255.255.0
dhcp network Internal_lan 192.168.18.0 255.255.255.0

local-auth method fast server-key 736563726574

interface create cegdata 150

interface create cegguestwifi 151

interface create cegvoip 99

interface address ap-manager 192.168.44.253 255.255.255.0 192.168.44.254
```

```
interface address management 192.168.44.252 255.255.255.0 192.168.44.254
interface address dynamic-interface cegdata 192.168.18.252 255.255.255.0 192.168.18.254
interface address dynamic-interface cegguestwifi 192.168.20.252 255.255.255.0 192.168.20.254
interface address dynamic-interface cegvoip 192.168.26.252 255.255.255.0 192.168.26.254
interface address virtual 1.1.1.1
interface dhcp ap-manager primary 172.23.1.50
interface dhcp management primary 172.23.1.50
interface dhcp dynamic-interface cegdata primary 192.168.44.252
interface dhcp dynamic-interface cegguestwifi primary 192.168.44.252
interface dhcp dynamic-interface cegvoip primary 192.168.26.250
interface vlan ap-manager 111
interface vlan management 111
interface vlan cegdata 150
interface vlan cegguestwifi 151
interface vlan cegvoip 99
interface port ap-manager 1
interface port management 1
interface port cegdata 1
interface port cegguestwifi 1
interface port cegvoip 1

load-balancing status enable
logging buffered 2

logging syslog host 172.23.1.50

mesh security eap

mgmtuser add admin **** read-write
mgmtuser add auditor **** read-only
mgmtuser add dobosd **** read-write
```

```
mobility group domain vallalat
mobility dscp value for inter-controller mobility packets 0
network fast-ssid-change enable
network rf-network-name vallalat
radius acct add 1 172.23.1.72 1813 ascii ****
radius acct add 2 172.23.1.36 1813 ascii ****
radius acct add 3 172.23.1.23 1813 ascii ****
radius auth add 1 172.23.1.23 1812 ascii ****
radius auth add 2 172.23.1.72 1812 ascii ****
radius auth add 3 172.23.1.36 1812 ascii ****
radius auth rfc3576 enable 1
radius auth rfc3576 enable 2
radius auth rfc3576 enable 3
radius auth retransmit-timeout 2 10
radius fallback-test mode off
radius fallback-test username cisco-probe
radius fallback-test interval 300
wps rogue-ap rldp enable alarm-only
snmp version v2c enable
snmp version v3 enable
snmp syscontact Dobos Daniel
snmp syslocation TI_1em_Rendezo
snmp community create nagy-sarkany
snmp community create kis-sarkany
snmp community accessmode rw nagy-sarkany
snmp community accessmode ro kis-sarkany
snmp community ipaddr 172.23.1.100 255.255.0.0 nagy-sarkany
```

```
snmp community ipaddr 172.23.1.100 255.255.0.0 kis-sarkany
sysname ceg_wlc
time ntp server 1 172.23.0.254
wlan create 1 CegVoIP voice
wlan create 2 CegData Data
wlan create 3 CegGuestWiFi GuestWiFi
wlan 7920-support client-cac-limit enable 1
wlan 7920-support ap-cac-limit enable 1
wlan interface 1 cegvoip
wlan interface 2 cegdata
wlan interface 3 cegguestwifi
wlan broadcast-ssid disable 1
wlan broadcast-ssid disable 2
wlan broadcast-ssid disable 3
wlan qos 1 platinum
wlan session-timeout 1 disable
wlan session-timeout 2 1800
wlan session-timeout 3 disable
wlan wmm allow 2
wlan wmm allow 3
wlan security wpa disable 3
wlan radius_server auth add 2 1
wlan radius_server acct add 2 1
wlan radius_server acct disable 3
wlan security static-wep-key encryption 1 104 <mode unknown> <passwd hidden> 1
wlan security static-wep-key encryption 2 104 <mode unknown> <passwd hidden> 1
wlan security web-auth server-precedence 2 local
```

wlan security wpa akm 802.1x disable 1
wlan security wpa akm psk enable 1
wlan security wpa akm ft reassociation-time 20 1
wlan security wpa akm ft over-the-air enable 1
wlan security wpa akm ft over-the-ds enable 1
wlan security wpa akm ft reassociation-time 20 2
wlan security wpa akm ft over-the-air enable 2
wlan security wpa akm ft over-the-ds enable 2
wlan security wpa akm ft reassociation-time 20 3
wlan security wpa akm ft over-the-air enable 3
wlan security wpa akm ft over-the-ds enable 3
wlan security wpa wpa1 enable 1
wlan security wpa wpa1 enable 2
wlan security wpa wpa1 ciphers tkip enable 1
wlan security wpa wpa1 ciphers aes enable 2
wlan security wpa wpa1 ciphers tkip enable 2
wlan security wpa wpa2 disable 1
wlan security wpa wpa2 ciphers tkip enable 2
wlan dhcp_server 1 192.168.26.250 required required
wlan dhcp_server 2 192.168.44.252 required required
wlan dhcp_server 3 192.168.44.252 required required
wps client-exclusion 802.11-assoc disable
wps client-exclusion 802.11-auth disable
wps client-exclusion 802.1x-auth disable
wlan enable 1
wlan enable 2
wlan enable 3

8.2.2 WLC rádiós beállítások és jellemzők:

A WLC-n kialakított rádiófrekvenciás automatizmusoknak és jellemzőknek csak egy kivontát mutatom be területi okok miatt. Ezt a kivonatot úgy választottam ki, hogy önmagában érthető legyen. Az AP Config és az AP Airewave Direction Configuration részben a 20 AP részletes konfigurációs beállításából csak 1 AP részletes konfigurációs beállítása szerepel.

System Inventory

NAME: "Chassis" , DESCR: "4400 Series WLAN Controller:25 APs"
PID: AIR-WLC4402-25-K9, VID: V02, SN: FOC1143F095

Burned-in MAC Address..... 00:1E:13:2A:C9:60
Crypto Accelerator 1..... Absent
Crypto Accelerator 2..... Absent
Power Supply 1..... Present, OK
Power Supply 2..... Present, OK

System Information

Manufacturer's Name..... Cisco Systems Inc.
Product Name..... Cisco Controller
Product Version..... 5.0.148.0
RTOS Version..... Linux-2.6.10_mvl401
Bootloader Version..... 3.2.195.10
Build Type..... DATA + WPS

System Name..... ceg_wlc
System Location..... TI_1em_Rendezo
System Contact..... Dobos Daniel
System ObjectID..... 1.3.6.1.4.1.14179.1.1.4.3
IP Address..... 192.168.44.252
System Up Time..... 22 days 1 hrs 22 mins 24 secs
System Timezone Location..... (GMT +1:00) Amsterdam, Berlin, Rome, Vienna

Configured Country..... HU - Hungary
Operating Environment..... Commercial (0 to 40 C)
Internal Temp Alarm Limits..... 0 to 65 C
Internal Temperature..... +38 C

State of 802.11b Network..... Enabled
State of 802.11a Network..... Enabled
Number of WLANs..... 3
3rd Party Access Point Support..... Disabled

Number of Active Clients..... 4

Burned-in MAC Address..... 00:1E:13:2A:C9:60

Crypto Accelerator 1..... Absent

Crypto Accelerator 2..... Absent

Power Supply 1..... Present, OK

Power Supply 2..... Present, OK

Switch Configuration

802.3x Flow Control Mode..... Disable

FIPS prerequisite features..... Disabled

secret obfuscation..... Enabled

Network Information

RF-Network Name..... vallalat

Web Mode..... Disable

Secure Web Mode..... Enable

Secure Web Mode Cipher-Option High..... Disable

Secure Shell (ssh)..... Enable

Telnet..... Disable

Ethernet Multicast Mode..... Disable Mode: Ucast

Ethernet Broadcast Mode..... Disable

IGMP snooping..... Disabled

IGMP timeout..... 60 seconds

User Idle Timeout..... 300 seconds

ARP Idle Timeout..... 300 seconds

ARP Unicast Mode..... Disabled

Cisco AP Default Master..... Disable

Mgmt Via Wireless Interface..... Disable

Mgmt Via Dynamic Interface..... Disable

Bridge MAC filter Config..... Enable

Bridge Security Mode..... EAP

Over The Air Provisioning of AP's..... Enable

Apple Talk Disable

AP Fallback Enable

Web Auth Redirect Ports 80

Fast SSID Change Enabled

802.3 Bridging Disable

Port Summary

	STP	Admin	Physical	Physical	Link	Link	Mcast		
Pr	Type	Stat	Mode	Mode	Status	Status	Trap	Appliance	POE
1	Normal	Forw	Enable	Auto	1000 Full	Up	Enable	Enable	N/A
2	Normal	Disa	Enable	Auto	Auto	Down	Enable	Enable	N/A

AP Summary

Number of APs..... 20
 Global AP User Name..... Not Configured

AP Name	Slots	Ethernet MAC	Location	Port	Country
AP_TI_Fsz_Elso_lepcs	2	00:1d:a1:ed:1e:90	TI 1-es patch port	1	HU
AP_TI_1em_2	2	00:1d:a2:7f:6b:84	TI 6-os patch port	1	HU
AP_TI_2em_1	2	00:1d:a1:ed:1e:b8	TI 7-es patch port	1	HU
AP_TII_1em_Iroda2	2	00:1d:a1:ed:11:a6	TII 9-es patch port	1	HU
AP_TI_3em_Elso_lepcs	2	00:1d:a1:ed:1e:ac	TI 9-es patch port	1	HU
AP_TII_1em_Iroda1	2	00:1d:a2:7f:6b:a4	TII 6-os patch port	1	HU
AP_TII_Fsz_Sarok	2	00:1d:a1:ed:1e:e2	TII 1-es patch port	1	HU
AP_TII_Fsz_Iroda2	2	00:1d:a1:ed:1a:e2	TII 2-es patch port	1	HU
AP_TI_2em_2	2	00:1d:a1:ed:1e:78	TI 8-as patch port	1	HU
AP_TI_3em_Kozep	2	00:1d:a1:ed:1f:54	TI 10-es patch port	1	HU
AP_TII_Fsz_Bejarat	2	00:1d:a1:ed:1e:2e	TII 3-as patch port	1	HU
AP_TII_Fsz_Iroda1	2	00:1d:a2:7f:6b:cc	TII 4-es patch port	1	HU
AP_TI_Fsz_Hatso_lepc	2	00:1d:a1:ed:1f:10	TI 3-as patch port	1	HU
AP_TI_Atjaro_TII_fele	2	00:1d:a1:ed:1f:52	TI 4-es patch port	1	HU
AP_TII_1em_Iroda3	2	00:1d:a2:7f:6b:ea	TII 7-es patch port	1	HU
AP_TI_1em_1	2	00:1d:a1:ed:1e:7c	TI 5-os patch port	1	HU
AP_TII_1em_Iroda4	2	00:1d:a1:ed:1e:72	TII 8-as patch port	1	HU
AP_TI_Fsz_Kozep	2	00:1d:a1:ed:1e:f0	TI 2-es patch port	1	HU
AP_TI_3em_Hatso_lepc	2	00:1d:a1:ed:1e:64	TI 11-es patch port	1	HU
AP_TII_Fsz_Iroda3	2	00:1d:a1:ed:1e:8e	TII 5-os patch port	1	HU

AP Config

Cisco AP Identifier..... 0
 Cisco AP Name..... AP_TI_Fsz_Elso_lepcso
 Country code..... HU - Hungary
 Regulatory Domain allowed by Country..... 802.11bg:-E 802.11a:-E
 AP Country code..... HU - Hungary
 AP Regulatory Domain..... -E
 Switch Port Number 1
 MAC Address..... 00:1d:a1:ed:1e:90
 IP Address Configuration..... DHCP
 IP Address..... 192.168.44.215
 IP NetMask..... 255.255.255.0
 Gateway IP Addr..... 192.168.44.254
 Telnet State..... Disabled
 Ssh State..... Disabled
 Cisco AP Location..... TI 1-es patch port
 Cisco AP Group Name..... default-group
 Primary Cisco Switch Name.....
 Primary Cisco Switch IP Address..... Not Configured

Secondary Cisco Switch Name.....
 Secondary Cisco Switch IP Address..... Not Configured
 Tertiary Cisco Switch Name.....
 Tertiary Cisco Switch IP Address..... Not Configured
 Administrative State ADMIN_ENABLED
 Operation State REGISTERED
 Mirroring Mode Disabled
 AP Mode Local
 Public Safety Global: Disabled, Local: Disabled
 Remote AP Debug Disabled
 S/W Version 5.0.148.0
 Boot Version 12.3.8.0
 Mini IOS Version 3.0.51.0
 Stats Reporting Period 180
 LED State..... Enabled
 PoE Pre-Standard Switch..... Enabled
 PoE Power Injector MAC Addr..... Disabled
 Number Of Slots..... 2
 AP Model..... AIR-LAP1131AG-E-K9
 IOS Version..... 12.4(13d)JA
 Reset Button..... Enabled
 AP Serial Number..... FCZ1140Q1RH
 AP Certificate Type..... Manufacture Installed
 Management Frame Protection Validation..... Enabled (Global MFP Disabled)
 AP User Mode..... Not Configured
 AP User Name..... Not Configured
 Cisco AP system logging host..... 255.255.255.255
 AP Up Time..... 22 days, 01 h 25 m 51 s
 AP LWAPP Up Time..... 22 days, 01 h 21 m 50 s
 Join Date and Time..... Wed Mar 12 07:19:24 2008

 Join Taken Time..... 0 days, 00 h 01 m 22 s

AP Airewave Director Configuration

Number Of Slots..... 2
 AP Name..... AP_TI_Fszt_Elso_lepcso
 MAC Address..... 00:1d:a1:ed:1e:90
 Radio Type..... RADIO_TYPE_80211b/g

Nearby APs

AP 00:1d:a2:84:e8:f0 slot 0..... -85 dBm on 7 (192.168.44.252)
 AP 00:1d:a2:84:e9:f0 slot 0..... -94 dBm on 13 (192.168.44.252)
 AP 00:1d:a2:84:ec:20 slot 0..... -91 dBm on 1 (192.168.44.252)
 AP 00:1d:e6:24:df:a0 slot 0..... -87 dBm on 7 (192.168.44.252)

 AP 00:1d:e6:24:fc:30 slot 0..... -55 dBm on 13 (192.168.44.252)
 AP 00:1d:e6:24:fc:b0 slot 0..... -94 dBm on 13 (192.168.44.252)

AP 00:1d:e6:24:fd:e0 slot 0..... -81 dBm on 7 (192.168.44.252)
AP 00:1d:e6:24:fe:30 slot 0..... -72 dBm on 1 (192.168.44.252)
AP 00:1d:e6:24:ff:80 slot 0..... -93 dBm on 1 (192.168.44.252)
AP 00:1d:e6:24:ff:d0 slot 0..... -57 dBm on 13 (192.168.44.252)
AP 00:1d:e6:25:00:b0 slot 0..... -67 dBm on 1 (192.168.44.252)
AP 00:1d:e6:25:03:10 slot 0..... -71 dBm on 13 (192.168.44.252)

Radar Information

Channel Assignment Information

Current Channel Average Energy..... unknown
Previous Channel Average Energy..... unknown
Channel Change Count..... 0
Last Channel Change Time..... Wed Mar 12 07:19:22 2008
Recommended Best Channel..... 7

RF Parameter Recommendations

Power Level..... 2
RTS/CTS Threshold..... 2347
Fragmentation Threshold..... 2346
Antenna Pattern..... 0

Interface Configuration

Interface Name..... ap-manager
MAC Address..... 00:1e:13:2a:c9:63
IP Address..... 192.168.44.253
IP Netmask..... 255.255.255.0
IP Gateway..... 192.168.44.254
VLAN..... 111
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 172.23.1.50
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... Yes
Guest Interface..... No

Interface Name..... management
MAC Address..... 00:1e:13:2a:c9:60
IP Address..... 192.168.44.252
IP Netmask..... 255.255.255.0
IP Gateway..... 192.168.44.254
VLAN..... 111
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 172.23.1.50
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured

AP Manager..... No
Guest Interface..... No

Interface Name..... service-port
MAC Address..... 00:1e:13:2a:c9:61
IP Address..... 0.0.0.0
DHCP Option 82..... Disabled
DHCP Protocol..... Enabled
AP Manager..... No
Guest Interface..... No

Interface Name..... cegdata
MAC Address..... 00:1e:13:2a:c9:63
IP Address..... 192.168.18.252
IP Netmask..... 255.255.255.0
IP Gateway..... 192.168.18.254
VLAN..... 150
Quarantine-vlan..... no
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.44.252
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No
Guest Interface..... No

Interface Name..... cegguestwifi
MAC Address..... 00:1e:13:2a:c9:63
IP Address..... 192.168.20.252
IP Netmask..... 255.255.255.0
IP Gateway..... 192.168.20.254
VLAN..... 151
Quarantine-vlan..... no
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.44.252
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No
Guest Interface..... No

Interface Name..... cegvoip
MAC Address..... 00:1e:13:2a:c9:63
IP Address..... 192.168.26.252
IP Netmask..... 255.255.255.0

IP Gateway..... 192.168.26.254
VLAN..... 99
Quarantine-vlan..... no
Active Physical Port..... 1
Primary Physical Port..... 1
Backup Physical Port..... Unconfigured
Primary DHCP Server..... 192.168.26.250
Secondary DHCP Server..... Unconfigured
DHCP Option 82..... Disabled
ACL..... Unconfigured
AP Manager..... No
Guest Interface..... No

Interface Name..... virtual
MAC Address..... 00:1e:13:2a:c9:60
IP Address..... 1.1.1.1
DHCP Option 82..... Disabled
Virtual DNS Host Name..... Disabled
AP Manager..... No
Guest Interface..... No

WLAN Configuration

WLAN Identifier..... 1
Profile Name..... CEGVoIP
Network Name (SSID)..... voice
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 0
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Webauth DHCP exclusion..... Disabled
Interface..... cegvoip
WLAN ACL..... unconfigured
DHCP Server..... 192.168.26.250
DHCP Address Assignment Required..... Enabled
Quality of Service..... Platinum (voice)
WMM..... Disabled
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920).....
. client-cac-limitap-cac-limit
Wired Protocol..... None

IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Enabled
WPA (SSN IE)..... Enabled
TKIP Cipher..... Enabled
AES Cipher..... Disabled
WPA2 (RSN IE)..... Disabled
Auth Key Management
802.1x..... Disabled
PSK..... Enabled
CCKM..... Disabled
CKIP Disabled

IP Security..... Disabled
IP Security Passthru..... Disabled
Web Based Authentication..... Disabled
Web-Passthrough..... Disabled
Conditional Web Redirect..... Disabled
Splash-Page Web Redirect..... Disabled
Auto Anchor..... Disabled
Cranite Passthru..... Disabled
Fortress Passthru..... Disabled
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled)
Client MFP..... Optional but inactive (WPA2 not configured)
Tkip MIC Countermeasure Hold-down Timer..... 60

WLAN Identifier..... 2
Profile Name..... CegData
Network Name (SSID)..... Data
Status..... Enabled

MAC Filtering..... Disabled
Broadcast SSID..... Disabled
AAA Policy Override..... Disabled
Number of Active Clients..... 3
Exclusionlist Timeout..... 60 seconds

Fortress Passthru..... Disabled
H-REAP Local Switching..... Disabled
Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled)
Client MFP..... Optional
Tkip MIC Countermeasure Hold-down Timer..... 60

WLAN Identifier..... 3
Profile Name..... CegGuestWiFi
Network Name (SSID)..... GuestWiFi
Status..... Enabled
MAC Filtering..... Disabled
Broadcast SSID..... Disabled

AAA Policy Override..... Disabled
Number of Active Clients..... 1
Exclusionlist Timeout..... 60 seconds
Session Timeout..... Infinity
Webauth DHCP exclusion..... Disabled
Interface..... cegguestwifi
WLAN ACL..... unconfigured
DHCP Server..... 192.168.44.252
DHCP Address Assignment Required..... Enabled
Quality of Service..... Silver (best effort)
WMM..... Allowed
CCX - AironetIe Support..... Enabled
CCX - Gratuitous ProbeResponse (GPR)..... Disabled
CCX - Diagnostics Channel Capability..... Disabled
Dot11-Phone Mode (7920)..... Disabled
Wired Protocol..... None
IPv6 Support..... Disabled
Peer-to-Peer Blocking Action..... Disabled
Radio Policy..... All
DTIM period for 802.11a radio..... 1
DTIM period for 802.11b radio..... 1
Radius Servers
 Accounting..... Disabled

Local EAP Authentication..... Disabled
Security

802.11 Authentication:..... Open System
Static WEP Keys..... Disabled
802.1X..... Disabled
Wi-Fi Protected Access (WPA/WPA2)..... Disabled
CKIP Disabled
IP Security..... Disabled
IP Security Passthru..... Disabled

Web Based Authentication..... Disabled
 Web-Passthrough..... Disabled
 Conditional Web Redirect..... Disabled
 Splash-Page Web Redirect..... Disabled
 Auto Anchor..... Disabled
 Cranite Passthru..... Disabled
 Fortress Passthru..... Disabled
 H-REAP Local Switching..... Disabled
 Infrastructure MFP protection..... Enabled (Global Infrastructure MFP Disabled)
 Client MFP..... Optional but inactive (WPA2 not configured)
 Tkip MIC Countermeasure Hold-down Timer..... 60

RADIUS Configuration

Vendor Id Backward Compatibility..... Disabled
 Call Station Id Type..... IP Address
 Aggressive Failover..... Enabled
 Keywrap..... Disabled
 Fallback Test:
 Test Mode..... Off
 Probe User Name..... cisco-probe
 Interval (in seconds)..... 300

Authentication Servers

Idx	Type	Server Address	Port	State	Tout	RFC3576	IPSec - AuthMode/Phase1/Group/Lifetime/Auth/Encr
1	NM	172.23.1.23	1812	Enabled	2	Enabled	Disabled - none/unknown/group-0/0 none/none
2	NM	172.23.1.72	1812	Enabled	10	Enabled	Disabled - none/unknown/group-0/0 none/none
3	NM	172.23.1.36	1812	Enabled	2	Enabled	Disabled - none/unknown/group-0/0 none/none

Accounting Servers

Idx	Type	Server Address	Port	State	Tout	RFC3576	IPSec - AuthMode/Phase1/Group/Lifetime/Auth/Encr
1	N	172.23.1.72	1813	Enabled	2	N/A	Disabled - none/unknown/group-0/0 none/none
2	N	172.23.1.36	1813	Enabled	2	N/A	Disabled - none/unknown/group-0/0 none/none
3	N	172.23.1.23	1813	Enabled	2	N/A	Disabled - none/unknown/group-0/0 none/none

Dhcp Scope Info

Scope: guest_lan

Enabled..... Yes
Lease Time..... 7200 (2 hours)
Pool Start..... 192.168.20.224
Pool End..... 192.168.20.251
Network..... 192.168.20.0
Netmask..... 255.255.255.0
Default Routers..... 192.168.20.254 0.0.0.0 0.0.0.0
DNS Domain..... vallalat.hu
DNS..... 194.38.96.80 193.225.86.1 0.0.0.0
Netbios Name Servers..... 0.0.0.0 0.0.0.0 0.0.0.0

Scope: Internal_lan

Enabled..... Yes
Lease Time..... 7200 (2 hours)
Pool Start..... 192.168.18.224
Pool End..... 192.168.18.251
Network..... 192.168.18.0
Netmask..... 255.255.255.0
Default Routers..... 192.168.18.254 0.0.0.0 0.0.0.0
DNS Domain..... vallalat.hu

DNS..... 172.23.1.17 172.23.1.23 0.0.0.0
Netbios Name Servers..... 172.23.1.17 172.23.1.23 0.0.0.0

8.3 WLAN árlista

Ez az árlista az első ajánlat kéreşkor érvényben lévő állapotot tartalmazza. Az eltelt idő során ezek az árak már többször módosulhattak, mivel havonta frissül a Cisco Systems árlista.

Deviza:	USD	Cisco Systems árlista								
Global Price List - EMEA - Effective: 02-05-2007										
					Rolling Window vagy más néven szerviz	a Cisco USD listaára,				
		Termékkód	Megnevezés	RW	listaár	Ossz Listaár				
Version 2 - Based on Standalone Wireless LAN Controller (Cisco 4400 Series WLC) 12 to 100 LWAP support										
Telephely 1 Fsz-Tárgyalók										
3	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$2 097				
3	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$177				
Telephely 1 1.emelet										
2	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$1 398				
2	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$118				
Telephely 2.emelet										
2	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$1 398				
2	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$118				
Telephely 1 3.emelet										
3	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$2 097				
3	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$177				
Telephely 1-2 Fsz-Átjáró										
1	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$699				
1	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$59				
Telephely 2 Fsz										
5	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$3 495				
5	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$295				
Telephely 2 1.emelet										
4	db	AIR-LAP1131AG-E-K9	802.11ag LWAPP AP Integrated Antennas ETSI Cnfg	D	\$699	\$2 796				
4	db	AIR-PWRINJ3	Power Injector for 1100, 1130AG, 1200 1230AG, 1240AG Series	S	\$59	\$236				
Standalone WLAN Controller - LWAP management										
1	db	AIR-WLC4402-25-K9	4400 Series WLAN Controller for up to 25 Lightweight APs	C	\$14 395	\$14 395				
Option - Redundant Power Supply										
1	db	AIR-PWR-4400-AC=	4400 Series WLAN Controller AC Power Supply (redundant)	C	\$1 495	\$1 495				
CiscoSecure Access Control Server - WLAN client user authentication										
1	db	CSACS-4.1-WINUP-K9	ACS 4.1 Windows upgrade for ACS 3.x	N/A	\$4 495	\$4 495				
Unified LWAP and Standalone WLC						\$35 545				

9 Irodalomjegyzék

- **Joseph Davies:** Biztonságos vezeték nélküli hálózatok
Microsoft® Windows® alatt az IEEE 802.11 szabvány szerint
Szak kiadó
- **Eric Ouellet-Robert Padjen-Arthur Pfund:** Building a Cisco® Wireless LAN
Syngress®
- **Matthew S.Gast:** 802.11 Wireless Networks
The Definitive Guide O'REILLY®
- Deployment Guide for Cisco Guest Access Using the Cisco Wireless LAN Controller,
Release 4.1
- Certified Wireless Network Administrator™ *Official Study Guide*
Vendor-neutral wireless network training and certification
- Cisco Wireless LAN Controller Configuration Guide
- PEAP under Cisco Unified Wireless Networks with ACS 4.0 and Windows 2003
- www.wikipedia.hu
- www.pdamania.hu