SZAKDOLGOZAT

Szőke Lajos

Debrecen

2007

Debreceni Egyetem
Informatika Kar

VEZETÉKNÉLKÜLI HÁLÓZAT TERVEZÉSE

Témavezető:
Dr. Almási Béla
egyetemi docens

Készítette:
Szőke Lajos
Programtervező
informatika (Bsc)

Konzulens:
Kiss Attila
System Administrator
National Instruments

Debrecen
2007

Tartalomjegyzék

1. Bevezetés

A vezeték nélküli technológia lehetővé teszi információk elérését a világ szinte bármely pontjáról. A vezeték nélküli helyi hálózatok, vagy más néven WLAN –ok (Wireless Local Area Network) csökkentik az informatikai infrastruktúra kiépítésének költségeit, és biztosítják a hagyományos hálózatok funkcióit és előnyeit. Megjelenésük óta az összeköttetések már nem igényelnek helyhez kötöttséget, így könnyen igazodhatnak a felhasználók gyakran változó igényeihez. A WLAN –ok által nyújtott szabadság és egyszerű összekapcsolhatóság lehetővé tette a korábbi technológiák (Ethernet, Token Ring) előnyeinek kihasználását a mobil felhasználók számára és így a kábelek kötöttségeinek elhagyása új távlatokat nyitott az üzleti alkalmazások számára is. A hagyományos hálózatokhoz hasonlóan a vezeték nélküli LAN –okban is szükség van a jelek továbbítását lehetővé tevő fizikai médiumra, de a megszokott réz-, üveg- vagy műanyag szálakból álló kábelek helyett itt infravörös fényt (infrared light - IR) vagy rádiófrekvenciás hullámokat (radio frequencies - RF) alkalmaznak. A rádiófrekvenciás hullámok használata jobban elterjedt, mivel nagyobb sávszélességet és lefedettséget biztosítanak. A rajtuk alapuló technológiák a 2,4 gigahertz -es (GHz) vagy az 5 GHz –es frekvenciatartományban működnek, mert ezek használatához nem szükséges kormányzati engedély. A WLAN –ok lehetővé teszik épületek közti kapcsolatok kialakítását és irodán belüli hálózatok építését kábelek használata nélkül, de a vezeték nélküli hálózatot vezetékek segítségével kapcsolhatjuk hozzá a már meglévő hagyományos LAN infrastruktúrához, így a kábelek használata ezután sem válik feleslegessé. Az ilyen eszközök feladata legtöbb esetben a vezetékes helyi hálózatok kiegészítése és azok funkcióinak kiterjesztése a kábelekből származó kötöttségek feloldásával, azonban a vezeték nélküli technológia mára már megfelelő adatátviteli sebességet és megbízhatóságot nyújt viszonylag alacsony költségek mellett, így sok esetben lehet a hagyományos helyi hálózatok alternatívája is. A WLAN –ok számos előnnyel rendelkeznek, ezért ideálisak lehetnek otthoni vagy irodai hálózatok (Small Office / Home Office, SOHO) kialakításakor, főleg ha azoknak gyakran változó igényeknek vagy gyorsan növekvő felhasználó számnak kell megfelelniük. Néha a vezetékek lefektetése is akadályba ütközhet. Ha bérelt irodában szeretnénk LAN -t kialakítani vagy az épület adottságai nem teszik lehetővé a kábelezést, vezeték nélküli technológiák segítségével akkor is könnyen kialakítható a megfelelő infrastruktúra. Az ilyen technológiákra épülő hálózatok nagyon hamar kiépíthetőek, könnyen bővíthetőek, ezáltal rugalmasak és jól

skálázhatóak. Telepítésük a hagyományos vezetékes hálózatokénál kevesebb költséggel jár és fenntartásuk sem drága, ezért a kezdeti befektetés hamar megtérül. A dolgozat írásakor a legtöbb WLAN 11 Mbps és 54 Mbps közötti sebességen üzemelt. A vezeték nélküli hálózatok által nyújtott szolgáltatások és a megfelelő adatátviteli teljesítmény lehetővé tette a WLAN -ok gyors elterjedését és a vezetékes LAN –okkal történő eredményes együttműködést. A dolgozat célja a vezeték nélküli hálózatoknál használt eljárások és technológiák ismertetése és egy minta követelményrendszerre épülő hálózat tervének elkészítése. A terv dokumentációján kívül a dolgozat törekszik a javasolt megoldások bemutatására, előnyeiknek és hátrányaiknak leírására is, hogy az olvasó átfogó képet kapjon a hálózatterv elkészítésének összetettségéről és a vezeték nélküli hálózatok működéséről is.

2. A vezeték nélküli hálózatok kialakulása

A WLAN –ok első generációja nem volt problémamentes. Számos biztonsági és teljesítményt érintő kérdés merült fel. A korai megoldások nem biztosítottak megfelelő sebességet és mivel nem voltak szabványosak, a különböző gyártótól származó eszközök nem működtek megfelelően együtt. A problémák megoldására 1991-ben több gyártó együttműködésével megalakult a WECA (Wireless Ethernet Compatibility Alliance), mely később Wi-Fi –re változtatta a nevét. A WECA célja a vezeték nélküli technológiák szabványosítása volt. 1997 júniusában az IEEE (Institute of Electrical and Electronics Engineers) kiadta a 802.11 -es szabványcsaládot, mely a vezeték nélküli helyi hálózatokat definiálta. A WLAN –ok rohamos elterjedése ekkor kezdődött el, azonban a technológia alapjai az 1940-es évekbe nyúlnak vissza. 1942-ben a zeneszerző és zongoraművész, George Antheil és a színésznő Hedy Lamarr szabadalmaztatta a frekvenciaugrásos rádiótitkosító technikát, melyet később szórt sprektumú modulációnak (spread spectrum modulation) neveztek el. 1958-ban az amerikai tengerészet kifejlesztett egy rádió kommunikációs chippet, mely a szórt sprektrumú moduláción alapult. 1985-ben a civil közösség számára is elérhetővé vált a korábbi katonai technológia. 1989-ben az FCC (Federal Communications Commission - Amerikai Hírközlési Hatóság) engedélyezte a technológia alkalmazását három szabad rádió sávra. A vezeték nélküli technológia az IEEE szabványcsalád megjelenése után rohamosan terjedni kezdett. A szabványosításnak köszönhetően a WLAN –ok megbízhatósága nőtt,

telepítési költségeik csökkentek és az eszközök fejlesztési ideje lerövidült. 2000-ben és az utána következő néhány évben egyre többen indították el WLAN szolgáltatásaikat és egyre több WLAN –t támogató készülék jelent meg. 2005-re fél milliárd 802.11 -es szabványon alapuló eszköz eladását jósolták.

3. Az IEEE 802.11 -es szabványcsalád

Az IEEE által elkészített szabványok az OSI (Open Systems Interconnection) referencia modell fizikai és adatkapcsolati rétegét érintik (lásd [CISCO]):

<table>
<tr><td>802.2 Logikai kapcsolatvezérlés
(Logical Link Control - LLC)</td><td rowspan="2">Adatkapcsolati réteg
(Data Link Layer - DLL)</td></tr>
<tr><td>802.11 Közeghozzáférés vezérlés
(Media Access Control – MAC)</td></tr>
<tr><td>IR, FHSS, DSSS, OFDM, stb.</td><td>Fizikai réteg
(Physical Layer - PHY)</td></tr>
</table>

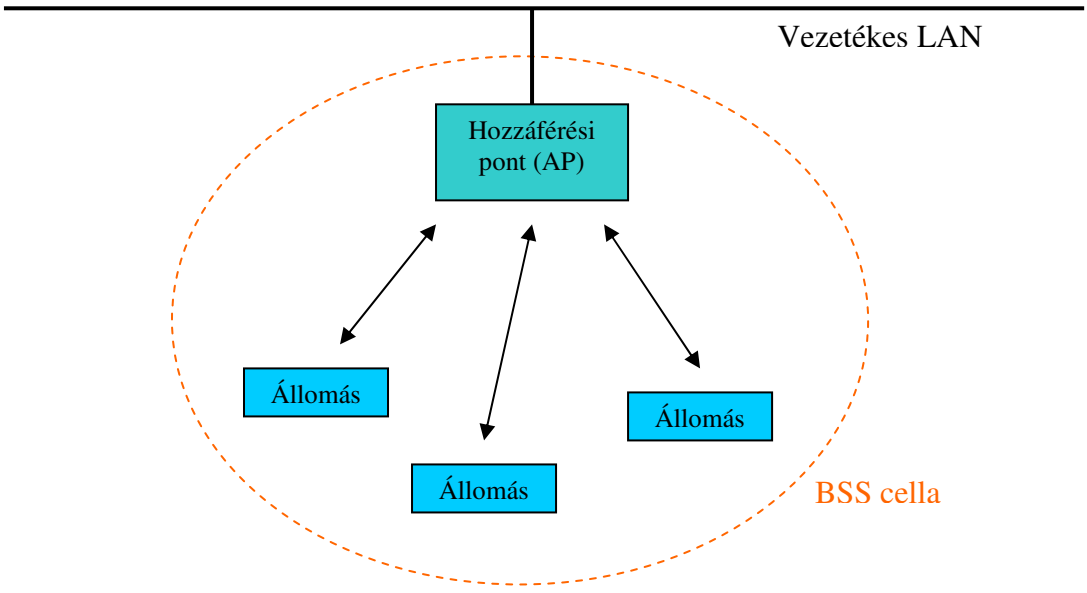
1. ábra

A 802.11 -es szabványcsalád magában foglalja többek közt az eredeti specifikációt a 802.11-et, a 802.11b -t és a 802.11a, 802.11g és 802.11n szabványokat. Ezeken kívül egyéb szabványok a biztonsággal (802.11i) és szolgáltatásminőséggel (Quality of Service – QoS, 802.11e) is foglalkoznak. A 802.11 -es szabványok fő funkciója a különböző eszközök közti vezeték nélküli kapcsolatok kialakítása és a kommunikáció megvalósítása a létrehozott összeköttetéseken keresztül a társ LLC rétegek közti MAC szolgáltatás adategységek továbbításával (MAC Service Data Unit - MSDU). A vezeték nélküli LAN –ok fizikai rétege sokban különbözik a hagyományos hálózatoknál használtaktól. A WLAN –ok időben változó, dinamikus topológiával rendelkeznek, és olyan médiumot használnak, ami a szokásos vezetékes közegnél sokkal kevésbé megbízható. Nem védettek a külső jelektől és nem jellemző rájuk a teljes összekapcsoltság, azaz a különböző állomások nem mindig érzékelik egymást.

A 802.11 -es hálózatok feladatai közzé tartozik nemcsak a helyhez kötött vagy hordozható (portable), de a mobil eszközök támogatása is. A hordozható és mobil készülékek abban különböznek, hogy az utóbbit helyváltoztatás közben is használják. Az IEEE által kiadott szabvány szerint a vezeték nélküli hálózatoknak a MAC alrétegben kell megvalósítaniuk az állomások mobilitását, ezért ezek a hálózatok számos egymással együttműködő komponensből állnak. Az alkotóelemek a felsőbb rétegek számára transzparens módon biztosítják a hordozhatóságot és a vezeték nélküli összeköttetéseket.

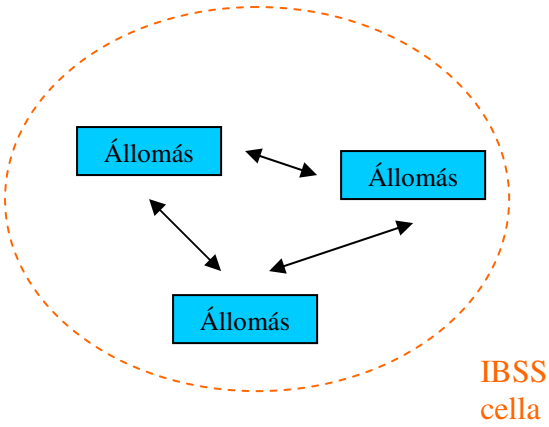
4. Az IEEE 802.11 -es hálózatok logikai architektúrája

A WLAN -ok építőkockáit alap-szolgáltatáskészletnek (Basic Service Set - BSS) nevezzük. A BSS egy egybefüggő rádiófrekveciás területet (más néven cellát) fed le (2. ábra). Központjában a hozzáférési pont (Access Point - AP) áll. A cellán belül elhelyezkedő állomások tudnak egymással kommunikálni. Az összes eszköz a hozzáférési ponttal áll kapcsolatban, egymással közvetlenül nem kommunikálnak. Az AP feladata az is, hogy a vezeték nélküli LAN –t összekapcsolja a vezetékes hálózattal.



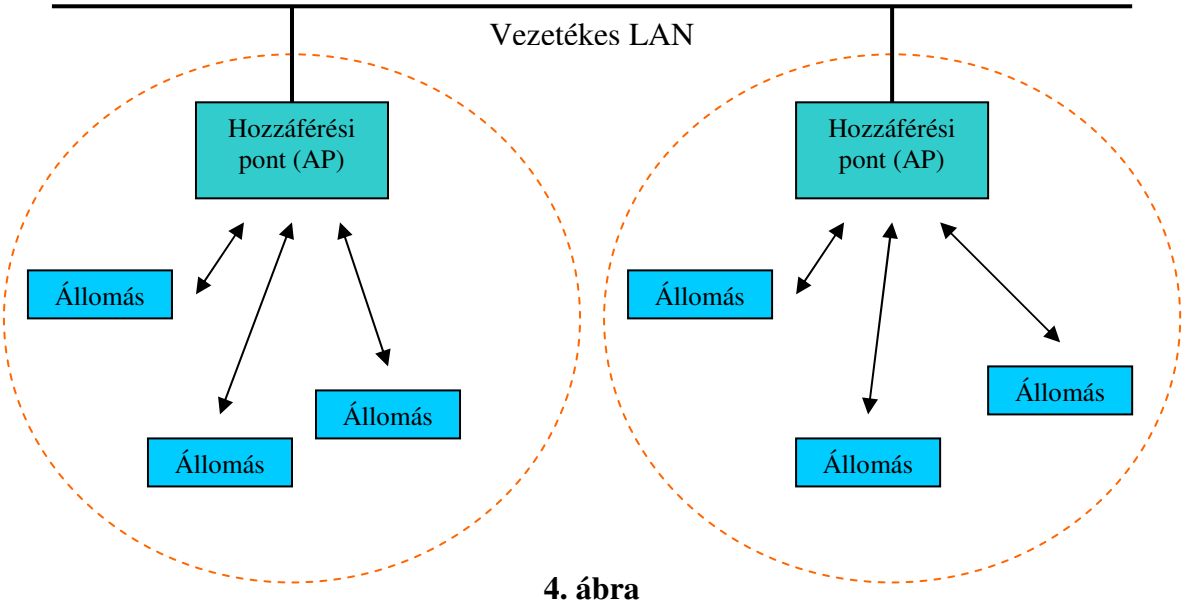
2. ábra

A BSS –t alapvető építőkockának nevezzük, mégis a legegyszerűbb felépítésű 802.11 -es hálózatok e helyett úgynevezett független alap-szolgáltatáskészletet (Independent Basic Service Set - IBSS) használnak. A legkisebb WLAN –ok nem tartalmaznak AP -t, az ugyanahhoz az IBSS –hez tartozó állomások közvetlen összeköttetésben állnak egymással (3. ábra). Mivel az ilyen hálózatok előzetes tervezés nélkül könnyen kiépíthetők és használhatók ameddig csak szükségesek, úgynevezett „ad hoc" hálózatnak is nevezik őket. Vezetékes LAN –hoz kapcsolásukhoz ki kell jelölni egy állomást az IBSS –ből, amely átjáróként (gateway) funkcionál majd.



3. ábra

A BSS –ből vagy IBSS –ből álló vezeték nélküli hálózatok előnye a könnyű telepíthetőség, hátrányuk viszont, hogy az általuk biztosított lefedettség gyakran nem elegendő. A távolsági korlátokat elosztórendszerek (Distribution System - DS) segítségével küszöbölhetjük ki. A DS –ek lehetnek vezetékesek vagy vezeték nélküliek is. Feladatuk a független BSS és IBSS cellák egy egységbe foglalása. Ezt nevezzük kiterjesztett szolgáltatáskészletnek (Extended Service Set - ESS).



4. ábra

Az ESS definíció szerint két vagy több közös elosztórendszerhez kapcsolt BSS –ből áll és lehetővé teszi tetszőleges méretű és bonyolultságú vezeték nélküli hálózatok kialakítását (4. ábra). A kiterjesztett szolgáltatáskészleten belül az állomások szabadon kommunikálhatnak egymással, de a csomagok mindig áthaladnak egy AP –n. A BSS vagy ESS felépítésű WLAN –ok úgynevezett infrastrukturális módban üzemelnek. A mobil eszközök az adott ESS –en belül egyik BSS –ből (cellából) a másikba szabadon átvándorolhatnak anélkül, hogy elvesztenék a kapcsolatot a hálózattal. Ezt a folyamatot nevezzük roaming –nak (a szó jelentése barangolás). A roaming a kliens számára a transzparens módon történik, azaz a mobil állomások felhasználói nem érzékelnek belőle semmit. Az IEEE 802.11 szabványok nem definiálják pontosan, hogyan kellene a roaming -nak történnie, de megadják a művelethez szükséges építőkockákat. Ezek közzé tartozik az aktív és passzív felderítés (active and passive scanning) és az állomás új AP –hoz történő társítása (re-association process) is, amire akkor kerül sor, ha az állomás egyik hozzáférési ponttól a másikhoz vándorol. Ahhoz hogy roaming közben fennmaradjon a kapcsolat a hálózattal a cellákat úgy kell kialakítani, hogy 15% -ban átfedjék egymást.

5. MAC szolgáltatások

A vezeték nélküli hálózatok szabványosításakor fő szempont volt, hogy előírásokat fogalmazzanak meg a MAC (Media Access Control – közeghozzáférés vezérlés) alrétegben és a fizikai (Physical - PHY) rétegben nyújtott szolgáltatásokra. Az IEEE 802.11 három szolgáltatást definiál a MAC alrétegben. Ezek az Aszinkron Adatszolgáltatás (Asynchronous data service), a biztonsági szolgáltatások (Security services) és az MSDU rendelés (MSDU ordering). (lásd [TANENBAUM])

5.a Aszinkron adatszolgáltatás

Ez a szolgáltatás teszi lehetővé a társ LLC rétegek számára az MSDU –k egymás közti cseréjét. A helyi MAC alréteg az alsóbb szintű fizikai réteg szolgáltatásait használja, hogy a társ MAC alréteghez továbbítsa a szolgáltatás adategységeket, majd az adja át a felsőbb szintű LLC alrétegnek. Ez a fajta aszinkron MSDU átvitel összeköttetés-mentes, legjobb szándékú

továbbításon alapul, azaz nincs biztosíték a sikeres kézbesítésre. A MAC alréteg az MSDU –k broadcast (szórásos) és multicast (többes címzési mód) típusú továbbítását is támogatja az unicast (egyedi címzés) mellett.

5.b Biztonsági szolgáltatások

Az IEEE 802.11 szabvány szerint a vezeték nélküli hálózatok biztonsági szolgáltatásait többek közt a hitelesítés (authentication) és a WEP (Wired Equivalent Privacy, jelentése: vezetékessel egyenértékű biztonság) mechanizmus biztosítja. A WEP az MSDU –k titkosítását a MAC alréteg feletti rétegek számára transzparens módon valósítja meg. Célja hogy hozzáférés-szabályozást valósítson meg, mialatt megőrzi az adatok integritását és bizalmasságát. A WEP a mai környezetekben már nem számít elégséges, megfelelő biztonságot nyújtó eljárásnak. A biztonsági kérdésekről a dolgozat későbbi fejezetében bővebben lesz szó.

5.c MSDU rendelés

A MAC alréteg által nyújtott szolgáltatások az MSDU –k újraküldését igényelhetik. A MAC csak akkor kéri szándékosan újra az adategységeket, ha az növeli a sikeres továbbítás valószínűségét. A unicast címzési módú MSDU –k elsőbbséget élveznek a broadcast és multicast módon továbbítottaktól.

6. MAC architektúra

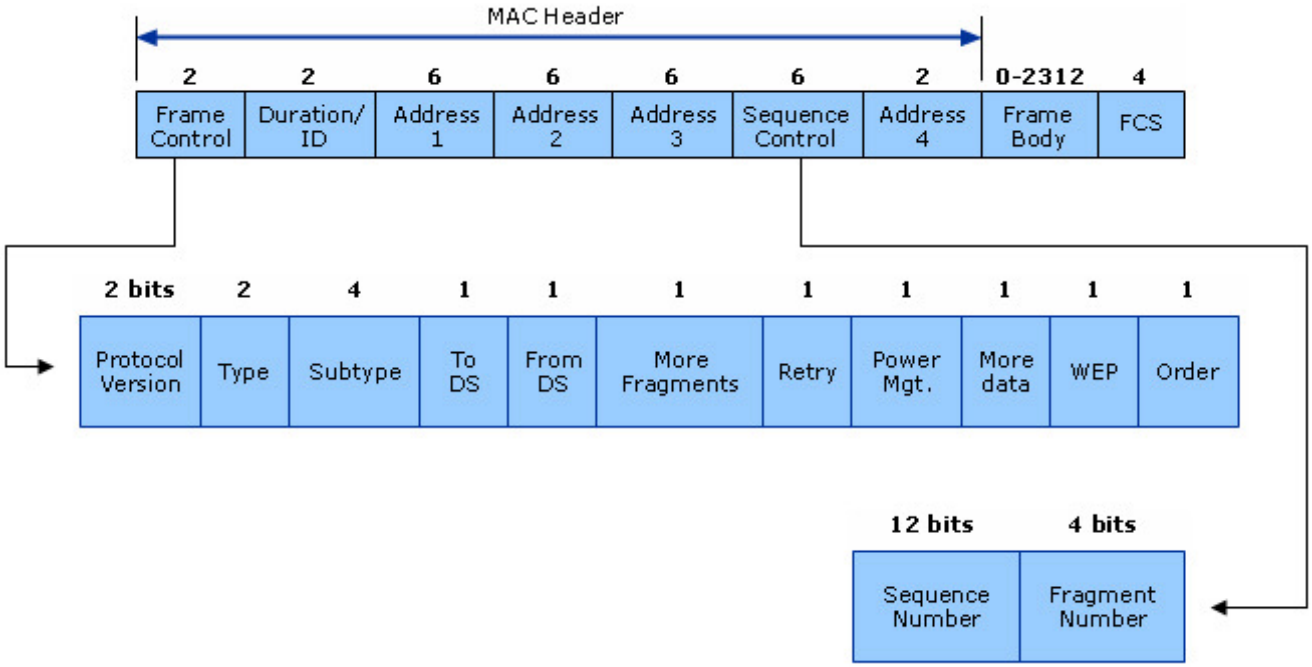
Mikor egy állomás keretet szeretne továbbítani a vezeték nélküli médiumon, először meg kell szereznie a közeg használati jogát. Erre két módszert is kidolgoztak. Az IEEE 802.11 szabvány szerinti hálózatok alapvető eljárása a DCF (Distributed Coordination Function – elosztott koordinációs funkció), amely a CSMA/CA (carrier sense multiple access with collision avoidance – vivőjel érzékeléses többszörös hozzáférés ütközés elkerüléssel) protokollt használja a közeghozzáférés vezérlésére. A médium foglaltságának ellenőrzését két technika közös használatával valósítják meg, ezek a fizikai és virtuális vivőjel érzékelés. Ha

mindkét eljárás egyszerre szabadnak mutatja a közeget, akkor szabadnak tekintjük, egyébként foglaltként kezeljük. A fizikai módszert a fizikai réteg biztosítja. A virtuális vivőjel érzékelés a MAC alrétegben definiált és a NAV –on (network allocation vector – hálózat kiosztási vektor) alapszik. A NAV az egyedi címzésű (unicast) keretek mezőit vizsgálva próbálja megjósolni a jövőbeli hálózati forgalmat. A DCF –et minden állomás ismeri, akár ad hoc, akár infrastrukturális módban üzemel. Az IEEE 802.11 MAC ezen kívül definiál egy opcionális hozzáférési technikát is, melyet PCF –nek (Point Coordination Function – központosított koordinációs funkció) neveznek. A PCF lényege, hogy segítségével olyan WLAN –ok alakíthatók ki, melyekben nincs versengés a közegért (contention-free access - CF). A PCF csak infrastrukturális üzemmód esetén alkalmazható, tehát szükség van hozzá legalább egy hozzáférési pontra (AP). A DCF és PCF technika egy BSS –en belül egyszerre is alkalmazható. Ilyen esetben a két módszert felváltva használjuk, azaz a DCF által vezérelt időben versengéses, a PCF által irányított időszakban pedig versengés-mentes periódusról beszélünk. A PCF szerint működő állomások két keret továbbítása közt kevesebb ideig várakoznak, kisebb az IFS (Interframe Space – keretek közti rés), tehát a PCF forgalom nagyobb prioritású a DCF módban üzemelő állomások forgalmánál.

7. Kerettípusok

A MAC alréteg három alapvető kerettípust használ: adatkeretek, vezérlő keretek és menedzsment keretek. Az adatkereteket adatok továbbításakor alkalmazzuk. A vezérlő keretek a médiumhoz való hozzáférést szabályozzák. Ezek közzé tartoznak az RTS (Request To Send – adatküldés kérelem), a CTS (Clear to Send – adatküldésre felkészülve), és az ACK (Acknowledgment – megerősítés) típusú keretek. A menedzsment keretek kezelési információkat tartalmaznak. Ezek közzé tartozik például az úgynevezett beacon keret is, amely a hozzáférési pontokról tartalmaz információkat, és amelyet az AP –k periodikusan sugároznak. A menedzsment keretek az adatkeretekhez hasonlóan továbbítódnak, de nem adódnak tovább a felsőbb rétegekhez. (lásd [CISCO]).

8. A MAC keretek felépítése



5. ábra

Az 5. ábrán a 802.11 MAC keret felépítése látható.

A ***Frame Control*** mező keretvezérlő információkat tartalmaz:

- ***Protocol Version***: megadja az IEEE 802.11 –es szabvány aktuális verzióját.
- ***Type***: típus, ez a mező határozza meg, hogy a keret adat, vezérlő vagy menedzsment típusú.
- ***Subtype***: altípus, értéke a keret típusától függ, például: RTS, CTS, ACK, stb.
- ***To DS***: 1 az értéke, ha az AP –nak továbbítania kell a keretet az elosztórendszernek (Distribution System - DS), különben 0.
- ***From DS***: 1 az értéke, ha a keret egy elosztórendszertől érkezett, egyébként 0.
- ***More Fragments***: megadja a fogadó állomásnak, hogy ezt a keret fregmenst követik-e további fregmensek.
- ***Retry***: Ha be van állítva, azt adja meg, hogy ez a keret egy korábbi keret újraküldött változata.

- ***Power Mgt***.: két lehetséges értéke van. Az egyik azt adja meg, hogy a fogadó állomás aktívan fogad kereteket, azaz CAM (Constant Awake Mode – folytonos ébrenléti mód) módban üzemel. A másik érték ennek az ellentéte. Az állomás ekkor energiatakarékos üzemmódban (Power Safe Mode) működik a PSP protokoll (Power Saving Protocol, jeletése: energiatakarékos protokoll) szerint és addig nem fogad keretet, amíg azt ő nem kéri vagy az állapota meg nem változik CAM módúra.
- ***More Data***: jelzi az állomásnak, hogy további keretek is érkeznek ez után.
- ***WEP***: Wired Equivalent Privacy (jelentése: vezetékessel egyenértékű biztonság). Ha be van állítva arra utal, hogy a keret titkosítva van a WEP algoritmus szerint.
- ***Order***: Jelzi, hogy az összes megérkezett adatkeretet sorrendben kell feldolgozni.

A ***Duration/ID*** (időtartam / azonosító) mező 16 bit hosszú. Vezérlő keret esetén, ha az altípus Power-Safe Poll akkor az értéke egy állomás AID -ja (association identity), minden más esetben a keret fogadásához szükséges hátralévő időtartamot jelöli. A CF (contention-free, versengés-mentes) periódus alatt továbbított kereteknél az értéke 32768.

Az ***Address1, Address2, Address3, Address4*** mezők a Basic Service Set azonosítót (BSSID), a forrás címet, a cél címet, az adóállomás címét, és a fogadó állomás címét tartalmazhatják. Bizonyos keretek nem tartalmazzák az összes mezőt.

A ***Sequence Control*** mező 16 bit hosszú és az alábbi mezőket tartalmazza:

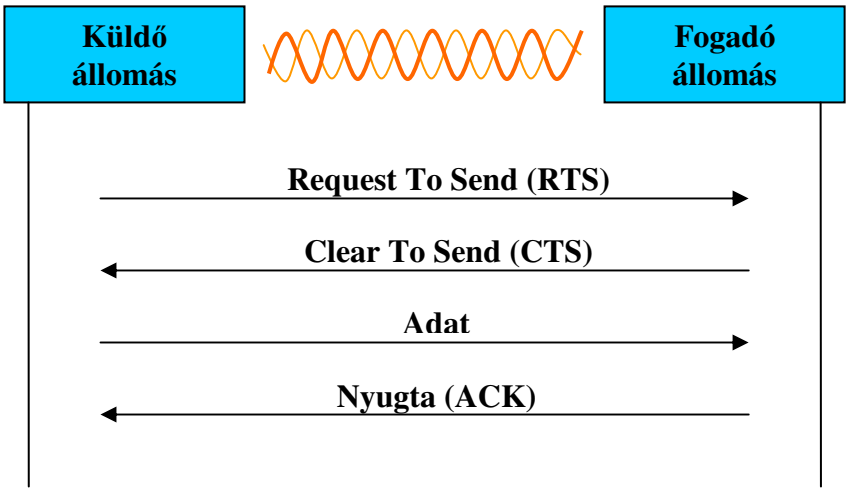
- ***Sequence Number***: megadja az elküldött kerethez tartozó sorozatszámot. Ha a keret darabolt (fragmented), akkor az összes darabhoz ugyanaz a sorozatszám tartozik. Értéke maximum 4095 lehet, ha ezt eléri ismét nulláról kezdődik a számozás.
- ***Fragment Number***: az adott kerethez tartozó darabok sorszámát adja meg. Nulláról indul, és egyesével növekszik, ha van több fregmens is.

A ***Frame Body*** (keret törzs, adatmező) egy változó hosszúságú mező. A keret típusától függően különböző információkat tartalmazhat.

Az ***FCS*** (Frame Check Sequence - keret ellenőrző sorozat) mező 32 bites CRC ellenőrző összeget tartalmaz, melyet az összes mezőt felhasználva számítanak ki.
További részleteket lásd [MICROSOFT TECHNET].

9. Keretek nyugtázása

Az IEEE 802.11 szabványra épülő vezeték nélküli hálózatokban pozitív nyugtázást alkalmaznak. Ez annyit jelent, hogy ha a fogadó állomás probléma nélkül megkapta a keretet és az abban szereplő FCS ellenőrző mező alapján is helyesnek találta azt, akkor visszaigazolást küld a forrás állomásnak. Ez a visszaigazolás egy ACK típusú keret, melyet nyugtának is neveznek. A várt nyugta elmaradása jelzi a küldő állomásnak, hogy a fogadó állomásnál probléma lépett fel és a keretet újra kell küldeni. Az is lehetséges, hogy a keret helyesen megérkezett, de a rávonatkozó nyugta sérült. Ezt az esetet nem tudja elkülöníteni a hálózat, ezért egyenértékű azzal, hogy az adatkeret sérült és újraküldést eredményez. A 6. ábrán két állomás közti kapcsolatfelvétel és adatcsere látható.

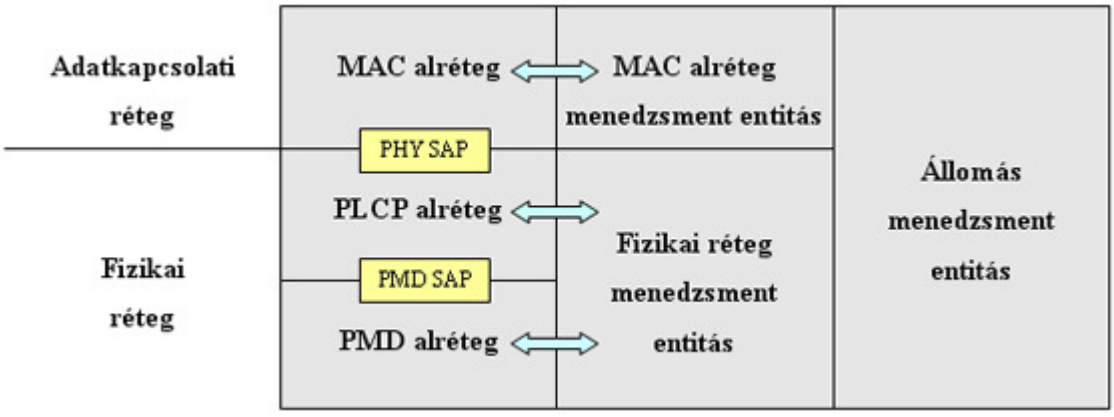


6. ábra

10. Fizikai réteg

A MAC alrétegre vonatkozó előírások csak a 802.11 –es szabványok egyik részét alkotják. A szabványok másik része a fizikai rétegre vonatkozó meghatározásokat tartalmazza. Az IEEE 802.11 -es szabványcsalád különböző médiumokat definiál vezeték nélküli átviteli célokra: a lehetséges alternatívák között szerepel az infravörös fény és a rádiófrekvencia használatának több különböző megvalósítása is (a dolgozat a rádiófrekvencián alapuló megoldásokkal fog foglalkozni, mivel a dolgozat írásának időpontjában egyre több ezt támogató technológia jelenik meg). Mivel a fizikai rétegbeli megoldások nagyon sokszínűek, ezért ezt a réteget is további alrétegekre bontották. A felosztás következtében csökkent a komplexitást és lerövidült a fejlesztési idő, mivel az egyes egységek fejlesztése párhuzamosan is folyhat. A legtöbb fizikai réteget érintő definíció három funkcionális entitást tartalmaz, ezek a következők:

- Réteg menedzsment funkciók (Layer Management Function)
- PLCP (Physical Layer Convergence Procedure)
- PMD rendszer (Physical Medium-dependent System – fizikai médiumtól függő rendszer)



7. ábra

A PMD rendszer az egyező fizikai réteget használó állomások közti vezeték nélküli közegen történő adatküldés és fogadás módszereit és jellemzőit definiálja, és megadja a PMD és PLCP alréteg közi interfész leírását is. Ezt az interfészt PMD SAP –nak (Service Access Point – szolgálat-elérési pont) nevezzük.

A PMD ezen keresztül nyújt szolgáltatásokat a PLCP számára (például foglalkozik a jelek paramétereivel, az időzítéssel, stb.). A PLCP feladata, hogy minimalizálja a MAC alréteg PMD alrétegtől való függését, és elérhetővé tegye a PMD funkcióit és szolgáltatásait a MAC számára is. A fizikai réteg szolgáltatásait a MAC alréteg ezen az alrétegen keresztül éri el egy interfész segítségével, amit PHY SAP –nak neveznek (lásd 7. ábra). A PLCP továbbá meghatároz egy eljárást, amivel lehetővé válik a MAC alréteg protokoll adategységeinek (MPDU) az adott PMD alrendszert használó állomások közti adatküldésnek és fogadásnak megfelelő keret formátumba történő leképezése.

11. Modulációs technikák

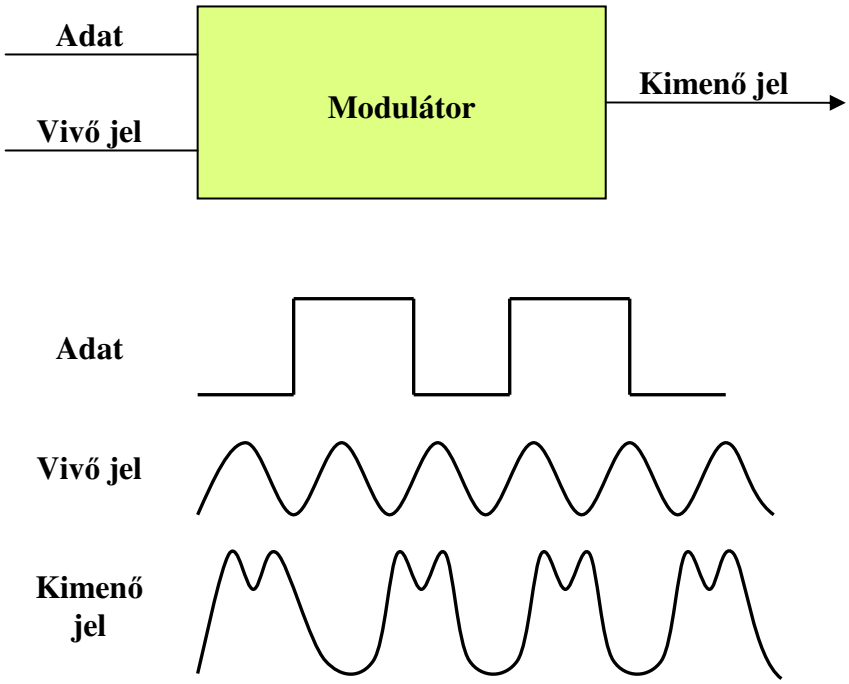
Vezeték nélküli hálózatok kialakításakor többféle médiumokat használhatunk. Tervezéskor lehetőségünk van infravörös fény és rádiófrekvenciás hullámok közül választani, illetve megválaszthatjuk a frekvenciatartományt és a modulációs technikát is, melyek meghatározóak a kiépülő hálózat szempontjából.
A moduláció olyan eljárások csoportja, amelyek biztosítják, hogy egy tipikusan szinuszos jel, a vivőjel képes legyen információ hordozására. A modulációs eljárás a jel három fő paraméterét módosíthatja, ezek: az amplitúdó, a fázis vagy a frekvencia. A moduláció több ok miatt is szükséges:

- A médiumot több felhasználó között kell megosztani (többszörös hozzáférés).
- Az átviendő jel és a közvetítő közeg fizikai jellemzői tehetik fontossá.

11.a Vivő frekvencia

A vivő frekvencia egy hullám, amelyet az információt hordozó jellel kombinálnak és a kombinált jelet továbbítják a kommunikációs csatornán. Erre több okból is szükség lehet. Az egyik ok, hogy a fizika törvényei szerint az adóállomás antennájának akkorának kell lennie, hogy a mérete megegyezzen a továbbítandó jel hullámhosszával. Ez bizonyos esetekben azt jelentené, hogy az antennáknak kilométeres nagyságúaknak kell lenniük. Mivel a frekvencia és a hullámhossz fordítottan arányosak, ha egy magas frekvenciás vivőjelet használunk az információ átküldésére, akkor a továbbított jelnek kis hullámhossza lesz és kisebb méretű

antenna is elegendő. Ezenkívül vivő frekvencia segítségével előállítható az átvitel szempontjából jó tulajdonságú jel és ezzel növelhető a megbízhatóság és az áthidalt távolság is. (lásd [ANDREA GOLDSMITH])



8. ábra

A 8. ábrán egy példa látható a modulációs eljárásra.

11.b Alapvető modulációs technikák

Három alapvető eljárás létezik attól függően, hogy a jel melyik jellemzőjét módosítjuk. Ha a jel amplitúdója változik, akkor Amplitúdó Modulációról (AM - Amplitude modulation) beszélünk. A jel frekvenciáját módosító eljárás a Frekvencia Moduláció (FM - Frequency modulation), a fázist változtató módszer neve pedig Fázis Moduláció (PM - Phase modulation). A legtöbb kommunikációs rendszer e technikák valamilyen kombinációján alapszik. A rádiófrekvenciát alkalmazó hálózatok legtöbbször a szabadon használható 2.4 GHz -es és 5 GHz –es tartományban üzemelnek és a következő eljárások valamelyikét veszik alapul: FHSS, DSSS, vagy OFDM.

11.c FHSS

Az FHSS jelentése frekvenciaugrásos szórt spektrum (Frequency Hopping Spread Spectrum). Az eljárás lényege, hogy a kommunikáló állomások nem használják egyszerre a teljes spektrumot (a 2.4 GHz –es frekvenciatartomány esetén 83 MHz), hanem csak egy részét, de a használt frekvenciatartomány folyamatosan változik. Ezt az időről-időre végrehajtott változtatást nevezik „ugrásnak" (hop). Az ugrást egy pszeudo-véletlenszerű sorozat alapján hajtják végre az állomások (gyakran ezt az ugrás kódjának is nevezik), ami egy lista azokról a frekvenciákról, amiket az átvitel során használni fognak. A frekvenciák sorrendje definiálja a kommunikációs csatornát. Az adóállomás az ugrási sorozatot felhasználva meghatározza az adás frekvenciáját, majd magadott ideig azon sugároz. Ha az idő letelt, akkor az adó kikeresi a következő sávot és átvált rá. Azt az időt, amíg az adó átkapcsol egyik frekvenciáról a másikra ugrási időnek (hop time) nevezzük. Ha az állomás a listán lévő összes sávon adott már, azaz végig ért a sorozaton, akkor az elejére ugrik és újra kezdi. Ahhoz, hogy a kommunikáció megvalósuljon a vevőnek és az adónak is ugyanazt a frekvenciát kell adott időpillanatban használnia, ezért az átvitelben részt vevő állomások szinkronban vannak. Az FHSS –nek két megvalósítása létezik:

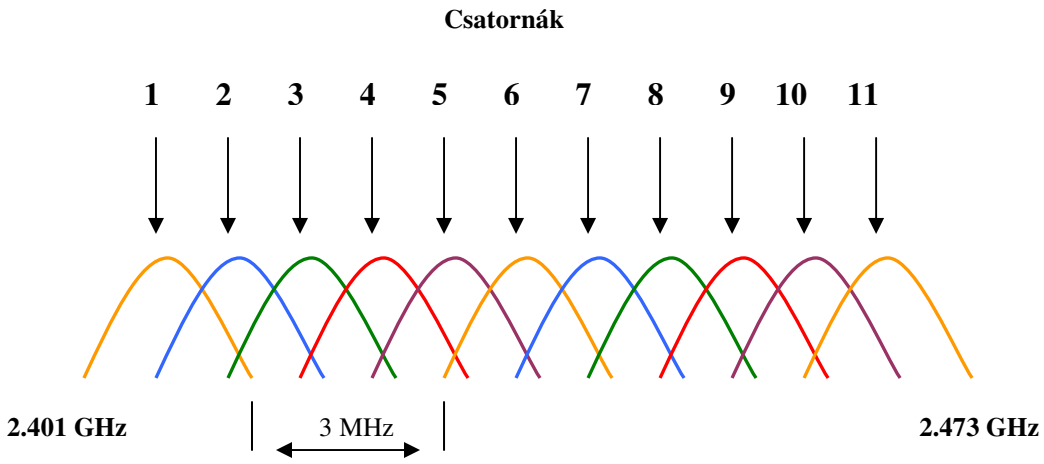
- keskenysávú frekvenciaugrás
- szélessávú frekvenciaugrás

A keskenysávú FHSS 1MHz –es jel-sávszélességet használ és 79 különböző frekvenciára lehet ugrani, így összesen 78 egyedi ugrási minta létezik.
A szélessávú frekvenciaugrásnál használt jelek akár 5MHz szélesek is lehetnek. A tipikus megvalósításuk 1,7 MHz –es sávokat használ, így 43 különböző frekvencia létezik.

11.d DSSS

A DSSS (Direct Sequence Spread Spectrum – közvetlen sorozatú szórt spektrum) kialakításakor az alapötlet az volt, hogy az összes csatornát használva egy gyors sávot hozzanak létre. A 802.11 –es szabványok megjelenésével ez az eljárás tovább már nem volt használható, helyett a magasabb sebességek eléréséhez egy fejlett modulációs eljárást vezettek be. A DSSS a csatornákat 22MHz széles egybefüggő frekvenciasávnak tekinti. Különböző országokban különböző számú csatorna használható.

Az Amerikai Egyesül Államokban 11, Európában 13, Japánban pedig 14 különböző csatorna használható. Mivel a csatornák középfrekvenciái 5MHz távolságra vannak egymástól és minden csatorna 22 MHz széles ezért a csatornák közt jelentős átfedés van. Két csatorna akkor nem fedi át egymást, ha a sorszámuk között legalább 5 az eltérés, azaz az Egyesül Államokba összesen három nem átfedő csatorna van, az első, a hatodik és a tizenegyedik.



9. ábra

Az egymást nem átfedő csatornák között 3 MHz –es „védősáv" található.
A DSSS eljárás a jelet a csatornán szétterítve továbbítja, az adott csatornán így folyamatosan a teljes a 22 MHz széles sáv használatban van. Az adóállomás minden adatbit továbbításakor egy chip sorozatot (chipping sequence) sugároz párhuzamosan a csatornán. A 10. ábrán egy példa látható:

A továbbítandó adat legyen: **1001** (= 9)

Az **1** –et jelölje például a következő sorozat: **11001100100.**
A **0** jele pedig legyen: **00110011011**.

A továbbított adat a következőképpen fog kinézni:

1	0	0	1
11001100100	00110011011	00110011011	11001100100

10. ábra

11.e OFDM

Az OFDM (Orthogonal Frequency Division Multiplexing) merőleges frekvenciaosztásos multiplexelést jelent. Lényege, hogy egy nagysebességű hordozót számos alacsony sebességű alcsatornára oszt és ezeket egyidejűleg használja információ továbbítására. Minden nagysebességű hordozó 20 MHz széles és 52 alcsatornára van felosztva, így egy alcsatorna körülbelül 300 KHz széles. Az OFDM 48 alcsatornát használ az adatok átvitelére, a fennmaradó 4 alcsatorna pedig hibajavítási célokra van fenntartva. Az alcsatornák úgy vannak kialakítva, hogy a sugárzott jelek egymással merőlegesek legyenek. Mivel a csatornák közelebb vannak elhelyezve egymáshoz ez az eljárás jobban kihasználja a spektrumot, mint a DSSS és működési elvéből adódóan bizonyos interferenciákra is kevésbé érzékeny. (lásd [KAVEN PAHLAVAN] és [WILLIAM WEBB])

12. Az IEEE 802.11 szabvány

A 802.11 –es szabvány 1997-ben jelent meg. Ez a szabvány tartalmazza az IEEE által kiadott meghatározások első változatát. Az átviteli sebesség maximum 1 vagy 2 Mbps lehetett, a támogatott médiumok között pedig az infravörös fény és a 2.4 GHz -es fekvenciatartomány is szerepelt. Rádiófrekvencia esetén az FHSS vagy a DSSS eljárás használható. Az eredeti szabvány definiálta a közeghozzáférést szabályozó CSMA/CA eljárást is. Megjelenése után több gyártó is bejelentette ezen a szabványon alapuló termékeit, de a felmerülő együttműködési, biztontonsági és teljesítménybeli problémák kezdetben igen nagy kihívást jelentettek.(lásd [WIKIPEDIA])

13. Az IEEE 802.11b szabvány

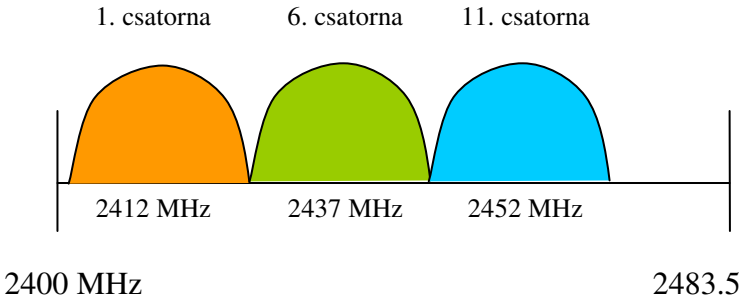
A 802.11b szabványt WiFi –nek is nevezik, de ismert még 802.11 High-Rate néven is, mivel a fizikai réteg nagysebességű átvitelre képes kiegészítését tartalmazza DSSS rendszerhez. Ez az első fejlesztett változata az eredeti 802.11 –es szabványnak.

Ez is a 2.4 GHz -es frekvenciát veszi alapul, de a maximális átviteli sebességet a többszörösére, 11Mbps –ra növeli. A 802.11b többféle átviteli sebességet is támogat. Az legalacsonyabb sebesség 1 Mbps DBPSK (Differential Binary Phase Shift Keying) modulációs eljárás és Barker kód alkalmazásával. A DBPSK modulációt 2-PSK –nak is nevezik, mert két egymástól 180 fokban eltérő fázist használ. A DBPSK a vivőjel fázisát változtatja meg a továbbítandó információ függvényében, a Barker kód pedig egy N hosszú, +1 és -1 értékekből álló sorozat, melyet egy matematikai képlet alapján számítanak ki. A szabvány ezen kívül támogatja a 2 Mbps, 5.5 Mbps és 11 Mbps átviteli sebességeket is.

2 Mbps esetén szintén Barker kódot használhatunk, de a modulációs eljárás DBPSK helyett DQPSK (Differential Quadrature Phase Shift Keying). A DQPSK (más néven 4-PSK) 4 eltérő fázist alkalmaz, így a maximális átviteli sebesség a duplájára nő. 5.5 Mbps és 11 Mbps esetén a modulációs eljárás szintén DQPSK, de ilyenkor Barker kód helyett CCK (Complementary Code Keying) modulációs sémát használunk. Bár a szabvány szerinti maximális átvitelisebesség 11 Mbps, PBCC (Packet Binary Convolutional Coding) módban az elméleti legnagyobb sebesség 22 Mbps –re nő.

A 802.11b szabványra épülő hálózatokat tipikusan pont-multipont felépítésben használják. Ekkor a hozzáférési pont (AP) egy gömbsugárzó (omni-directional, nem irányított) antennát használva kommunikál az állomásokkal. Az ilyen konfigurációk tipikus épületen belüli hatótávolsága 30 méter 11 Mbps sebesség mellett és 90 méter 1 Mbps sebesség mellett, de pont-pont kiépítés esetén irányított antennák segítségével nagyobb távolságok is áthidalhatók. Sajnos a 11 Mbps sebesség csak az elméleti maximum, a valós mérések eredménye maximum 5.9 Mbps TCP protokoll esetén és 7.1 Mbps UDP használatakor. Ennek az oka, az hogy átvitelkor a protokollok fejrészének továbbítása is időbe telik. Minél nagyobb a protokoll fejrésze, annál kisebb a valós átviteli sebesség (ezt nevezik overhead -nek).

A 11. ábrán az Amerikában használt kiosztás szerinti nem átlapoló csatornák és középfrekvenciáik láthatók.



11. ábra

14. Az IEEE 802.11a szabvány

A 802.11a szabvány az eredeti 802.11 második kiegészítése. Ugyanazt az alapprotokollt használja, mint a korábbi szabvány, viszont ez az 5 GHz –es frekvenciatartományban üzemelő, 54 Mbps maximális átviteli sebességű hálózatokat definiálja. Az 5 GHz –es frekvencia használata nagyobb sebességet tesz lehetővé és kisebb az interferencia is, mivel ez jóval kevésbé foglalt, mint a 2.4 GHz –es tartomány. A 802.11a OFDM –et használ, tehát a rendelkezésre álló tartományt 52 alcsatornára osztja. Az alcsatornák között 12 darab egymást nem átfedő alcsatorna található, amiből 8 épületen belüli és 4 pont-pont átvitelnek van fenntartva. Az ilyen hálózatok tipikus hatótávolsága 54 Mbps sebesség mellett 12 méter, 6 Mbps sebesség mellett pedig 90 méter. Sajnos az 54 Mbps itt is főleg elméleti sebesség, a valós érték ez alatt van. A 802.11b –hez hasonlóan ez a szabvány is többféle átviteli sebességet támogat, az értékeket a kódolási technika és a moduláció határozza meg. A használt modulációk között szerepel a BPSK, a QPSK, a 16QAM és a 64QAM. Az utóbbi két eljárás a QAM (Quadrature Amplitude Modulation) technika két típusa. A QAM lényege, hogy a vivőjel amplitúdóját módosítva továbbítjuk az információt.

A használható átviteli sebességek: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps és 6 Mbps. A következő táblázat a moduláció-sémákat és sebességeket foglalja össze:

Kódolás	Modulációs eljárás	Sebesség (Mbps)
OFDM	BPSK	6
OFDM	BPSK	9
OFDM	QPSK	12
OFDM	QPSK	18
OFDM	16QAM	24
OFDM	16QAM	36
OFDM	64QAM	48
OFDM	64QAM	54

12. ábra

A 802.11a szabvány előnyei mellett hátrányaival is találkozhatunk. Legnagyobb problémát a kompatibilitás okozza. A 802.11b és az eredeti 802.11 szabvány is a 2.4 GHz –es frekvenciát használja, ezért azok lefelé kompatibilisek egymással. Ez a szabvány más frekvencián alapul, azaz az ilyen készülékek nem, vagy csak külön bővítő modul behelyezése után képesek együttműködni a már meglévő, nem 802.11a szabványt követő vezeték nélküli hálózatokkal.

15. Az IEEE 802.11g szabvány

A 802.11g szabványt 2003 júliusában publikálták. A 802.11a –hoz hasonlóan ez a szabvány is 54 Mbps –os elméleti maximális sebességet biztosít, de nem az 5 GHz –es frekvencián, hanem az eredeti 802.11 és a 802.11b által használt 2.4 GHz –es sávban működik. A használt frekvencia miatt a 802.11g szabványon alapuló eszközök visszafelé kompatibilisek a korábbi 802.11 és 802.11b hálózatokkal. Az IEEE 802.11g állomások több különböző modulációt és átviteli sebességet is támogatnak. Az OFDM modulációs eljárást alkalmazzák, amíg a sebesség 6, 9, 12, 18, 24, 36, 48 vagy 54 Mbps. Ha kompatibilitási okokból 11 Mbps, 5.5 Mbps, 2 Mbps vagy 1 Mbps a kapcsolat sebessége, akkor a 802.11b szabványhoz hasonlóan az első kettőhöz CCK –t az utolsó kettőhöz pedig sorrendben DQPSK -t és DBPSK -t használnak. A 802.11g hálózatok tipikus hatótávolsága 54 Mbps sebesség mellett 15 méter, 11 Mbps sebesség esetén pedig 45 méter.

Az új szabvány lehetővé tette a korábbi eszközökkel és hálózatokkal való együttműködést, miközben a sebességet a 802.11a szabvány által definiált 54 Mbps -ra növelte. Az előnyök mellett azonban továbbra is komoly kihívást jelent az alkalmazott frekvenciatartomány foglaltsága (a 2.4 GHz –en működő készülékek közzé tartoznak a mikrohullámú sütők, a Bluetooth eszközök és a vezeték nélküli házi telefonok is, sőt ez a frekvencia a víz saját frekvenciája is, amely bizonyos esetekben problémákat okozhat).

16. Az IEEE 802.11n szabvány

A dolgozat írásakor a 802.11n szabványnak még nem jelent meg végleges változata, csak nyers (draft) specifikációk. A fejlesztők ígéretei szerint a végleges szabvány bizonyos kedvező körülmények között akár 600 Mbps –os sebességet és a 802.11g szabványnál nagyobb lefedettséget biztosít, miközben továbbra is kompatibilis marad a korábbi 802.11, 802.11b és 802.11g eszközökkel. Az átviteli sebességekkel szemben támasztott növekvő követelmények arra késztetik a gyártókat, hogy a korai fázisban lévő szabványt alapul véve úgynevezett pre-802.11n eszközöket dobjanak piacra, még akkor is, ha a nyers specifikációt követő eszközök különböző együttműködési, kompatibilitási és teljesítménybeli problémákat is felvetnek. A 802.11n végleges változatában sok újszerű és fejlett megoldással találkozhatunk majd. Ezek közül néhány:

- *javított OFDM*: szélesebb frekvenciasáv használata a nagyobb átviteli sebességért.
- *SDM* (Space Division Multiplexing - térosztásos multiplexelés): növekvő teljesítmény több antenna használatával.
- *MIMO* (Multiple Input Multiple Output): a többutas (multipath) interferenciát használva növeli a teljesítményt.
- *40 MHz –es csatornák* használata 20 MHz –es helyett: megduplázódik a sebesség.
- *RIFS* (Redued Inter-Frame Spacing): a korábbinál kisebb várakozási idő két keret adása között.

A 802.11n szabvány megjelenése 2008 –ra várható.

17. Biztonság

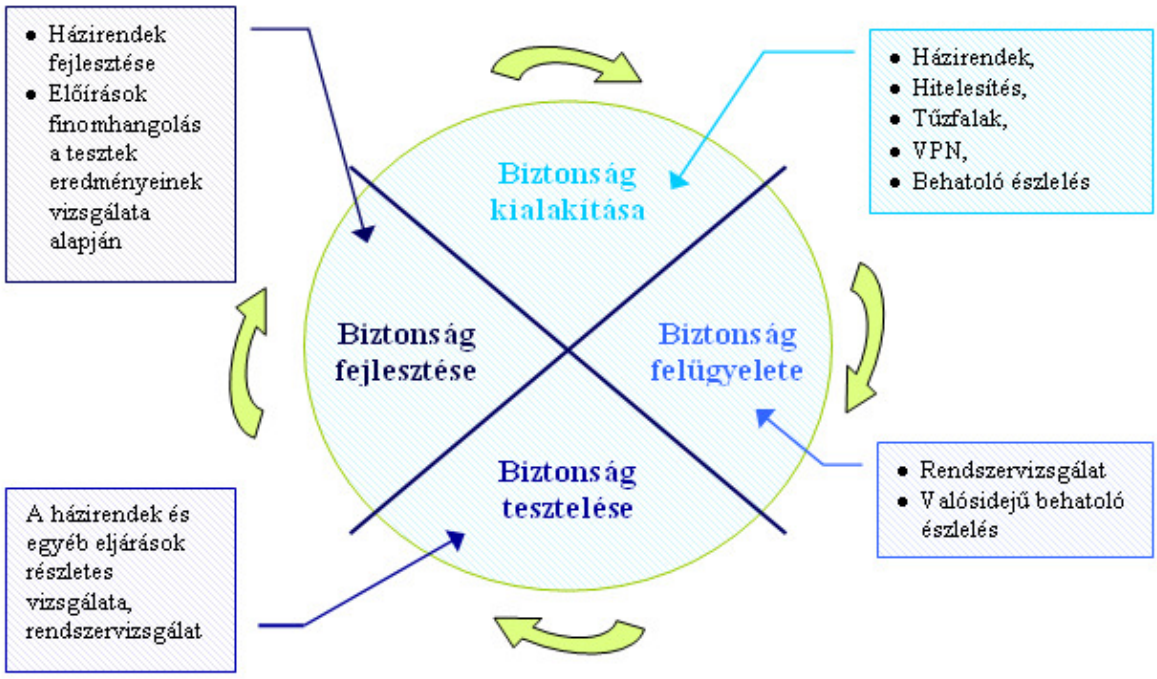
A biztonsági előírások célja egy olyan környezet megteremtése, melyben a felhasználók csak azokhoz az erőforrásokhoz férhetnek hozzá, és csak azokat a feladatokat végezhetik el, amikre jogosultságuk van. Garantálni kell azt is, hogy a felhasználók nem tudnak kárt tenni az adatokban vagy a rendszer többi komponensében. A biztonsági szabályrendszerek ezeken kívül a bekövetkezett hibák és kritikus események hatásait is igyekeznek irányítani. Sajnos sok esetben a biztonság fokozása a teljesítmény, az egyszerű használat, a kezelhetőség vagy az összekapcsolhatóság rovására megy. Meg kell találni az egyensúlyt az ellenőrzés és a használhatóság közt. A vezeték nélküli hálózatok biztonsági szempontból a hagyományos hálózatoknál sokkal sérülékenyebbek. Ennek oka, hogy a technológia viszonylag új és hogy a vállalatok nem mindig szentelnek elegendő figyelmet az előírások betartására. Például a legtöbb eszköz vásárláskor alapértelmezett adminisztrátori jelszóval rendelkezik, melyet később sem változtatnak meg. A technológia gyengeségei közül a következők a legkritikusabbak:

- *gyenge hitelesítés*: csak az eszközt hitelesítik, a felhasználót nem
- *gyenge adattitkosítás*: a kezdetben használt WEP (Wired Equivalent Privacy – vezetékessel egyenértékű biztonság) eljárás nem biztosít megfelelő adattitkosítást. Könnyen elérhető programok segítségével bármelyik WEP kulcs feltörhető kevesebb, mint 1 perc alatt.
- *üzenet integritási problémák*: az üzenetek sértetlenségének biztosítására használt ICV (Integrity Check Value – integritás ellenőrző összeg) nem biztosít megfelelő védelmet.

A WLAN –ok kellően biztonságossá tételére több gyártó is megalkotta saját rendszerét, mellyel a szabvány hiányosságait igyekeznek pótolni, illetve további funkciókat valósítanak meg a könnyű kezelhetőség és a megbízhatóság érdekében. Ilyen rendszer a Cisco Systems úgynevezett Cisco Wireless Security Suite nevű architektúrája is, amely központosított felhasználó alapú hitelesítést és további fejlett szolgáltatásokat nyújt.
A komplex, teljes hálózatot érintő megoldásokon kívül megfogalmazódtak olyan könnyen elsajátítható irányelvek is, melyek segítségével az adminisztrátorok a követelmények figyelembe vételével a vállalatuk számára megfelelően biztonságos hálózatokat alakíthatnak ki.

18. A vezeték nélküli hálózatok „biztonsági kereke”

A biztonsági kerék egy hatásos, grafikus eszköz az adminisztrátorok teendőinek meghatározására. Az ábra egy ismétlődő folyamatot ír le, melynek lépéseit követve a hálózatok kellően biztonságossá tehetők.



13. ábra

A folyamatot 4 lépésre osztja, ezek sorrendben a következők:

1. *A biztonság kialakítása*: Ez a lépés magában foglalja a biztonsági követelmények felmérését, az eredmények dokumentálását, és a biztonsági házirendek kifejlesztését és alkalmazását egyéb biztonsági megoldásokkal együtt.
2. *A biztonság felügyelete*: az első lépésben kialakított előírások, eljárások helyességének bizonyítása.
3. *A biztonság tesztelése*: Ebben a lépésben a rendszervizsgálatra alapozva azt teszteljük, hogy megfelelő szintű-e a biztonság.
4. *A biztonság fejlesztése*: az előző lépésekben megfigyelt eredmények alapján továbbfejlesztjük a biztonsági megoldásokat.

A 13. ábrán láthatóak az egyes lépések feladatai.

19. WLAN biztonsági technológiák

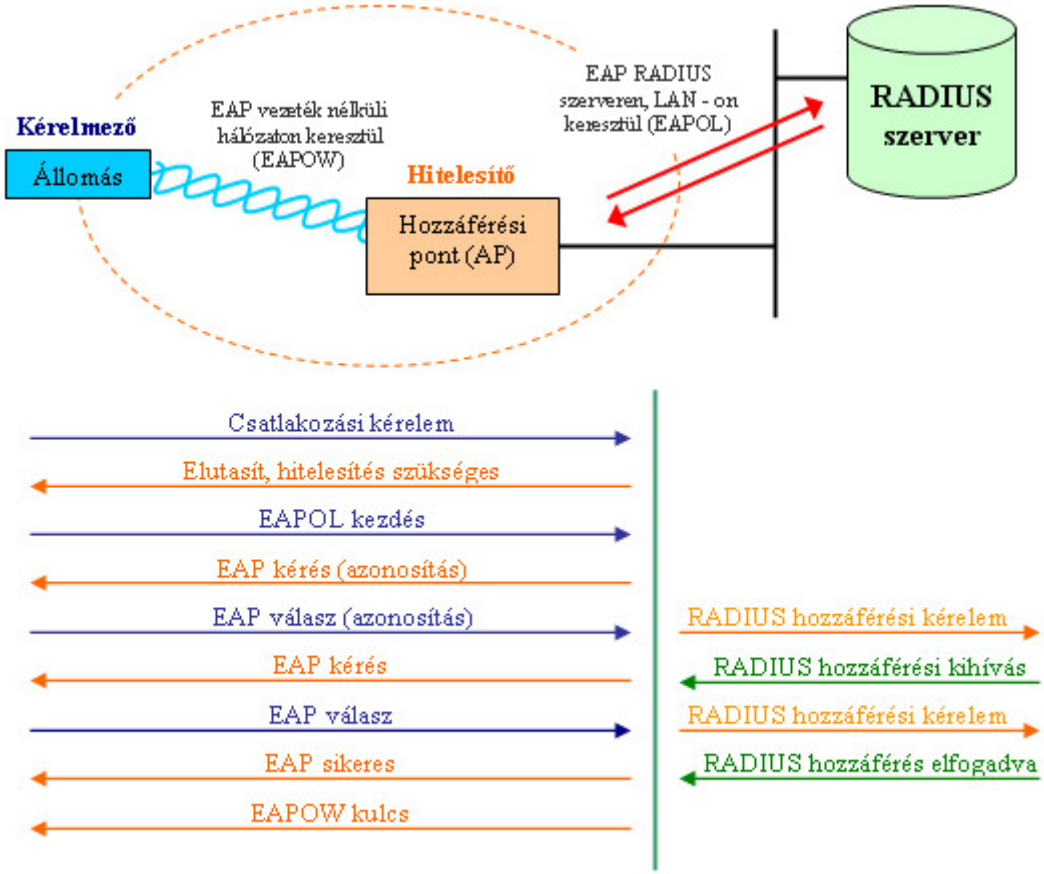
Kezdetben a vezeték nélküli hálózatok biztonságára nem fektettek túl nagy hangsúlyt. A legtöbb WLAN csak szolgáltatáskészlet azonosítót (SSID – Service Set Identifier) és MAC cím szűrést használt a hálózat védelmére. Egyik sem jelent biztonságot, mivel mindkettő titkosítatlan és az elküldött csomagok elkapásával és vizsgálatával (ezt angolul „sniffing" – nek, azaz szimatolásnak nevezik, magyarul inkább hallgatózásként említik) könnyen érvényes MAC címhez vagy SSID –hez juthat a behatoló. Tovább rontja a helyzetet, hogy a legtöbb hozzáférési pont (AP) alapértelmezetten a hálózat kiépítésének megkönnyítése miatt még olyan kliens eszközök csatlakozását is fogadja, ahol a SSID nincs megadva (azaz NULL).

19.a WEP (Wired equivalent privacy)

A WEP jelentése vezetékessel egyenértékű biztonság. Az IEEE 802.11 definiálta az eljárást 1999 –ben. A WEP célja a hálózat védelme a hallgatózás ellen. A szabvány 40 bites kulcsokat és RC4 (Rivest Cipher 4) titkosító eljárást használ, de több gyártó kiterjesztette a kulcs méretét 128 vagy több bitre is. A hálózat használatához a hozzáférési pontoknak és a klienseknek is ugyanazt a WEP kulcsot kell használniuk. A szabvány két eljárást definiál a kulcsok meghatározására. Az első változatban maximum 4 alapértelmezett kulcsot definiálnak a hozzáférési pontokon és az összes kliens ezeket használhatja. Ez könnyen megvalósítható, de alacsony biztonságot nyújtó módszer a széleskörben terjesztett kulcsok miatt. A második megoldás lényege, hogy minden állomás egy kulcsfeltérképező kapcsolatot épít ki egy szomszédos állomással. A kulcsokat itt nem terjesztjük széleskörűen, ezért ez az eljárás biztonságosabb, de nehezebb a megvalósítása is. Mivel a WEP egyik fajtája sem nyújt elegendő biztonságot, ezért a gyártók általában az első változatot valósítják meg eszközeikben (például Cisco Systems). A WEP szabványnak több továbbfejlesztett változata is született. Egyik ilyen a WEP+, amely a titkosítás hibáit igyekezett javítani és a WEP2, amely 128 bites kulcsokat ír elő és erősebb titkosítást használ. A WEP2 –t olyan eszközökön valósítják meg, amelyek nem képesek a fejlettebb biztonsági szabványok (WPA, WPA2) támogatására, mivel ez a szabvány sem nyújt igazán megbízható védelmet a behatolók ellen. A WEP –et 2003 – ban felváltotta a WPA. (lásd [WIKIPEDIA] és [RON FULLER]).

19.b Hitelesítés

A szakemberek idővel rájöttek, hogy a WEP hibáinak kijavítása nem elegendő a megfelelő biztonság eléréséhez. Az igazán biztonságos vezeték nélküli hálózatokban a felhasználókat is hitelesíteni kell és nem csak az eszközöket. A későbbi biztonsági megoldások (WPA, WPA2) a felhasználó alapú hitelesítést az IEEE 802.1X protokollon keresztül valósítják meg. A 802.1X kölcsönös hitelesítést biztosít, azaz a kliensnek és a hálózatnak is igazolnia kell önmagát. A szabvány egyik előnye, hogy többféle hitelesítési eljárást is támogat. Azok a hozzáférési pontok, amelyek támogatják a 802.1X szabványt és az általa definiált EAP (Extensible Authentication Protocol – kiterjeszthető hitelesítési protokoll) protokollt egyfajta interfészként működnek a vezeték nélküli kliensek és a hitelesítő szerver (például egy RADIUS - Remote Access Dial-In User Service - szerver) között. A hozzáférési pont a vezetékes hálózaton kommunikál a szerverrel, és segítségével hitelesíti a klienst. A következő ábrán a 802.1X hitelesítési folyamat látható:



14. ábra

19.c 802.1X hitelesítési típusok

A 802.1X szabvány több különböző hitelesítési eljárást is támogat. Ezek a következők:

- LEAP (Lightweight Extensible Authentication Protocol – „könnyűsúlyú" kiretjeszthető hitelesítési protokoll): Ezt a megoldást a Cisco Systems fejlesztette, ezért EAP-Cisco –nak is nevezik. Olyan hálózatokban javasolt a használata, ahol Cisco eszközök találhatóak és nincs lehetőség az EAP alkalmazására, mégis megfelelő hitelesítést szeretnénk.
- EAP-TLS (EAP Transport Layer Security): ez a típus az EAP szállítási rétegbeli biztonságot megvalósító fajtája. Munkaigényes a használata, mivel az adott WLAN - beli összes kliensen és szerveren be kell állítani egy X.509 szabványon alapuló digitális tanusítványt.
- PEAP (Protected EAP – védett EAP): Ez az EAP hitelesítés szabványtervezetben szereplő formája. Hibrid hitelesítést tesz lehetővé azáltal, hogy a szerver oldalon PKI (Public Key Infrastructure – nyilvános kulcsú infrastruktúra) eljárást használ, de a kliens oldali hitelesítés típusát nem írja elő. A PEAP használatával a vállalatok mentesülhetnek az EAP-TLS konfigurálásával járó többletmunkától és a számukra legmegfelelőbb kliens oldali hitelesítést választhatják.
- EAP-MD5: Ez az eljárás nem biztosít kölcsönös hitelesítést, ezért használata nem javasolt. Lényege, hogy megduplázza a CHAP (Challenge Handshake Authentication Protocol) jelszavak biztonságát az egyirányú hitelesítés segítségével.
- EAP-OTP (EAP One Time Passwords – egyszeri jelszavakat használó EAP): Kerülendő, mivel ez sem valósít meg kölcsönös hitelesítést. EAP-GTC (EAP- Generic Token Card, azaz EAP - általános vezérjel kártya) –nek is nevezik.
- EAP-SIM: Ez a módszer a mobil telefonokban használt SIM kártyához hasonló eszközzel biztosítja a hitelesítést.
- EAP-TTLS (EAP - Tunneled Transport Layer Security): Ezt a típust a Funk software and Certicom fejlesztette. A PEAP –hoz hasonló funkciókat biztosít. Használatához RADIUS szerver szükséges.
- Kerberos: Nem része a 802.1X szabványnak, de több gyártó is javasolja a használatát. A Kerberos hitelesítési rendszer egy egyedi kulcs (ticket - jegy) segítségével teszi lehetővé a nyitott hálózatokon keresztüli védett kommunikációt.

19.d AES (Advanced Encryption Standard)

A 802.11i szabvány magában foglalja a korábban kidolgozott AES eljárást, melynek neve fejlett titkosító szabványt jelent. Az AES jellemzői:

- erősebb titkosító eljárást használ az RC4 –nél,
- 128, 192 vagy 256 bites kulcsok alkalmazását írja elő,
- MIC (Message Integrity Check – üzenet integritás ellenőrző) mezőt tartalmaz,
- statikus (PSK- Pre Shared Keys, előre kiosztott kulcsok) és dinamikus (802.1X) kulcsokkal is üzemelhet,
- az Amerikai Egyesült Államok kormánya is az AES használatát írja elő hivatalaiban,
- hardveres támogatást igényel.

19.e WPA és WPA2 (Wi-Fi Protected Access)

A WPA (Wi-Fi Protected Access – védett vezeték nélküli hozzáférés) biztonsági megoldások rendszere, amelyet a korábban alkalmazott WEP eljárás leváltására hoztak létre. Az IEEE 802.11i szabványtervezet 3. változatán alapszik, arra szánták, hogy a végleges szabvány megjelenéséig biztosítsa a hálózatok megfelelő védelmét. A WPA az összes vezeték nélküli hálózati csatolókártyával használható, de nem feltétlenül működik együtt az első generációs hozzáférési pontokkal. A WPA a 802.1X szabványon alapuló hitelesítést tesz lehetővé és használható hitelesítő szerverrel vagy a kevésbé biztonságos PSK (Pre Shared Key – előre kiosztott kulcsok) módban is. Az adatokat 128 bites kulcsú, 48 bites kezdővektort (Initialization Vector - IV) használó RC4 eljárás segítségével titkosítja. A nagyobb kezdővektor és a TKIP (Temporal Key Integrity Protocol – ideiglenes kulcs integritási protokoll: dinamikusan változtatja a rendszer által használt kulcsot) eljárás segítségével kiküszöbölték a WEP biztonsági hiányosságait. A WPA CRC (cyclic redundancy check) ellenőrző mező helyett MIC (Message Integrity Check – üzenet integritás ellenőrző) mezőt használ, mivel a CRC eljárás kevésbé biztonságos.
A WPA rendszer második kiadása a WPA2, amely teljes mértékben megvalósítja a 802.11i szabvány végleges változatát. A WPA2 TKIP –et, MIC mezőt és AES alapú titkosító eljárást (CCMP) használ a biztonság növeléséhez. Ezt a rendszert 2006 elejétől az összes Wi-Fi tanúsítvánnyal rendelkező eszköznek kötelező támogatnia. (lásd [WIKIPEDIA])

20. Vezeték nélküli hálózatok tervezése

Vezeték nélküli hálózatok tervezésekor 4 alapvető követelményt kell figyelembe venni:

- Magas rendelkezésre állás
- Skálázhatóság
- Menedzsment, kezelhetőség
- Együttműködés

A WLAN –ok kellően magas rendelkezésre állását redundáns eszközök használatával és megfelelően megtervezett lefedettségi területekkel érhetjük el. Ide tartozik a szünetmentes áramellátás biztosítása, a tartalék hozzáférési pontok (AP) telepítése (azonos frekvencián standby módban vagy külön frekvencián), megfelelő antennák és ismétlők (repeater) használata és az automatikus sebesség megválasztás (gyengébb jel esetén alacsonyabb sebesség használata) is.
A skálázhatóság úgy érhető el, hogy több hozzáférési pontot telepítünk adott lefedettségi területre, és terhelésmegosztásra konfiguráljuk őket. A WLAN –ok menedzsmentjéhez sok diagnosztikai eszköz nyújt segítségét. Ezek a szoftver és hardver kellékek lehetővé teszik a központosított felügyeletet, a védelem bizonyos funkcióinak megvalósítását és a hálózat finomhangolását, továbbfejlesztését is. A negyedik követelmény az egyik legfontosabb az összes közül. A hálózatot úgy kell megalkotni, hogy biztosítsa az ügyfelek számára a munkavégzéshez, a vállalat működéséhez szükséges szolgáltatásokat. A szakembereknek nagyon gyakran kell heterogén hálózatot tervezniük, azaz fel kell készülniük több gyártótól származó, különböző szabványokat támogató eszközök kiszolgálására is (például 802.11 a, b, és g szabványú készülékek). A hálózatban később üzemeltetni kívánt eszközök alapvetően befolyásolják a hálózati tervet, de a használt készülékeken kívül az alkalmazások teljesítmény igénye is kulcsfontosságú a terv szempontjából. Figyelembe kell venni, hogy a WLAN –oknál megadott sebességek csak az elméleti maximumot jelentik és a valós átbocsátóképesség gyakran jóval alatta van a szabványban megadott maximumnak. Például 802.11b szabvány esetén 11 Mbps helyett általában 5-7 Mbps sebességgel kell számolnunk, ezért ezt a szabványt a 10 Mbps –os Ethernet szabvánnyal egyenértékűnek szokták tekinteni, mikor a sebességről és a csatlakoztatható eszközök számáról esik szó.

A hálózati terv létrehozása több részfeladatból álló folyamat. A lépések sorrendjét a 15. ábra mutatja:

15. ábra

A szakdolgozat írása során én is ezt az ábrát követem, de a dolgozatban csak a követelmények elemzése, a logikai és fizikai terv készítése, ezek mérésekkel való alátámasztása és a kész tervek dokumentációja szerepel majd, mivel nincs lehetőség az általam tervezett hálózat kivitelezésére.

A dolgozat elkészítésekor Kiss Attila System Administrator volt segítségemre, aki a debreceni National Instruments Europe Kft. –nél dolgozik (a 16. ábrán a National Instruments logója látható). Az NI Debrecen 2001-ben kezdte meg működését, a National Instruments első gyártóbázisaként, Amerikán kívül. Debrecenben történik az NI hardver termelésének közel 90%-a. Az alapítás óta Debrecenbe települt új szolgáltatások következményeként a National Instruments új irodaépületet nyitott 2007 februárjában. A dolgozat az új épület vezetékes hálózatának vezeték nélküli eszközökkel történő kibővítését tartalmazza.

16. ábra

20.a Követelmények elemzése

A tervezés első szakasza a követelmények összegyűjtése és elemzése. Erre több eszköz is rendelkezésre áll. Lehetőség van többek közt kérdőívek használatára, megfigyelésen alapuló követelménygyűjtésre, és a kulcsfelhasználókkal történő személyes elbeszélgetésre is. Az összegyűjtött követelményeket dokumentálni kell, majd ajánlatos az eredményt ismét egyeztetni a felhasználókkal. Ez a lépés alapvető fontosságú, mert a rosszul felmért követelményrendszer rossz hálózati tervet és nem megfelelő hálózatot eredményez. Mivel a dolgozatban megtervezett hálózat csak példaként szolgál a WLAN –ok tervezéséhez, ezért az itt összegyűjtött követelményeket nem a leendő felhasználók reprezentatív csoportjaival történő egyeztetés, hanem Kiss Attila segítségével határoztam meg.

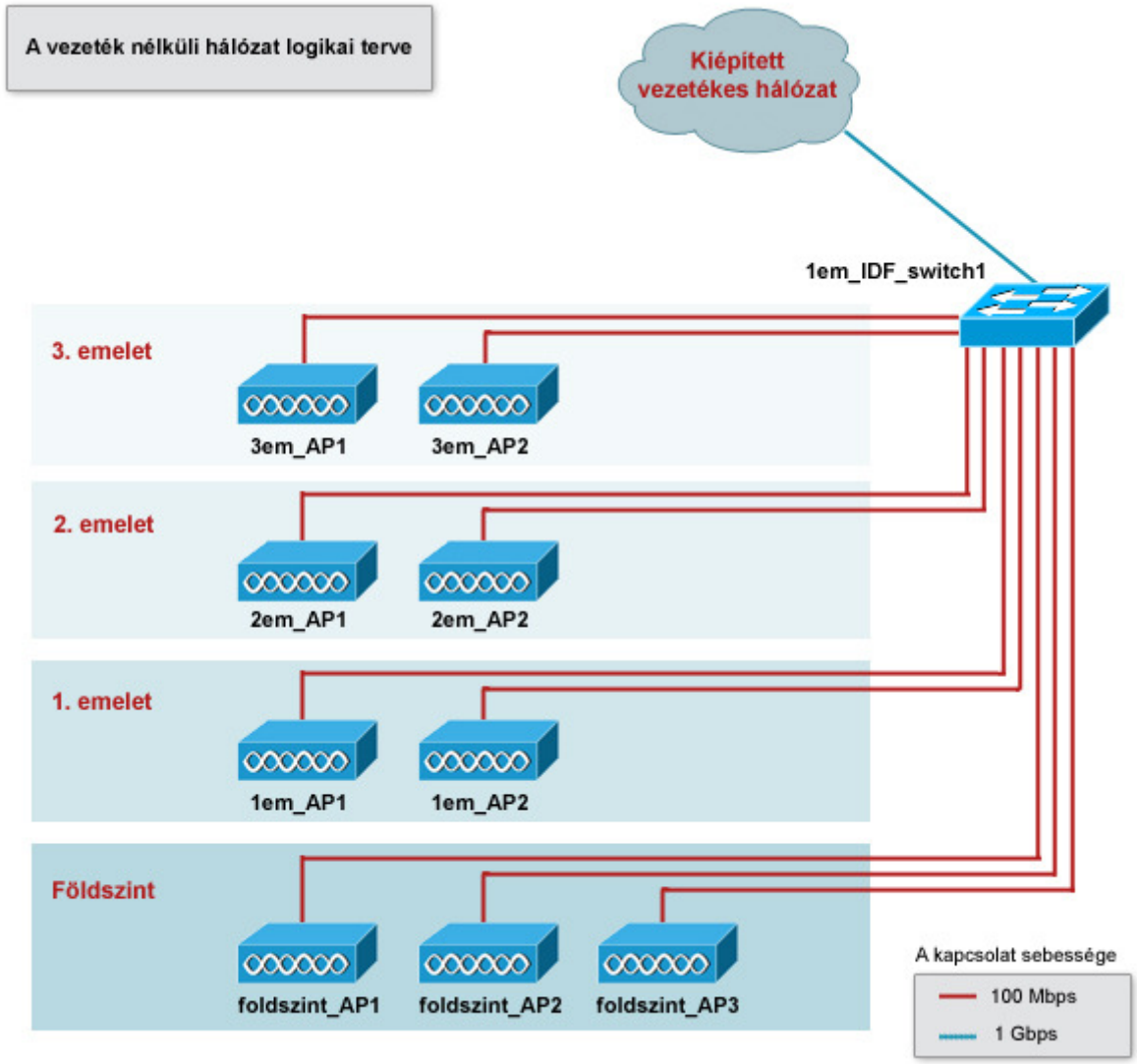
Az összegyűjtött követelmények listája:

1. Az újonnan átadott épület 3 emeletes. Emeletenként 5-10 mobil vagy hordozható eszköz (laptop, PDA, vonalkód leolvasó) használatára lehet számítani. Ez a földszinti készülékekkel együtt összesen 20-40 állomást jelent. A megfelelő sávszélesség és rendelkezésre állás biztosítása érdekében illetve az épület adottságai miatt minden szintre legalább 2 hozzáférési pont kerül, így a hálózat jól skálázhatóvá válik, és felkészülünk az eszközök számának későbbi növekedésére is. A terv elkészítésekor a redundancia fontos szempont a kellő rendelkezésre állás biztosítása miatt.
2. Az állomások az IEEE 802.11b és IEEE 802.11g szabvány szerinti csatolókkal rendelkeznek. A 802.11a szabvány támogatása nem feltétlenül szükséges, de ajánlott, az esetlegesen idelátogató külföldi partnerek miatt.
3. Az épületben kiépített vezetékes hálózat található. A nagyobb átbocsátóképességet igénylő alkalmazások a vezetékes hálózatra kapcsolt munkaállomásokon futnak. A vezeték nélküli hálózat célja főleg az Internet elérés biztosítása, tehát az állomások nem igényelnek nagy sávszélességet.
4. A kiépített vezetékes hálózatban csak a Cisco Systems által gyártott hálózati elemek találhatók. Az egységes Cisco eszközökből álló hálózat (Cisco Unified Network) könnyű kezelhetőséget, skálázhatóságot, megbízhatóságot és további fejlett szolgáltatásokat nyújt, ezért az NI számára fontos, hogy a vezeték nélküli hálózati elemek is a Cisco kínálatából származzanak.

5. Biztonság: a vezeték nélküli hálózat használata minden dolgozó és partner számára engedélyezett. A WLAN a vezetékes hálózatra csatlakozik, a felhasználók korlátozását magasabb szinten, a vezetékes hálózatba tartozó eszközökön kell megvalósítani. A WLAN biztonságáért a megfelelő titkosítás felel.

20.b A logikai terv elkészítése

A logikai terv elkészítése a tervezés második fázisa. A tervet mindig az összegyűjtött és egyeztetett követelményekre támaszkodva kell megalkotni. Az előző lépésben megadott elvárások alapján a vezeték nélküli hálózat logikai felépítése a következő:



17. ábra

A vezetékes és vezeték nélküli hálózat között egy kapcsoló (switch) található, ehhez csatlakoznak a hozzáférési pontok. A földszinten három, a többi emeleten pedig 2 AP található, erre az épület felépítése miatt van szükség (lásd a későbbi fizikai tervet). Az AP –k 100 Mbps –os kapcsolaton keresztül csatlakoznak a kapcsolóhoz, aminek pedig 1 Gbps –os kapcsolata van a vezetékes hálózattal. Az eszközök úgy lettek elnevezve, hogy nevük utaljon az elhelyezkedésükre is. Ez megkönnyíti a konfigurációt, a felügyeletet és a későbbi hibaelhárítást is. A tervezés során mindig fontos az eszközök konzisztens és beszédes elnevezése és az elnevezések pontos dokumentációja is.

Az eszközök címeinek meghatározása is a logikai terv része. A hozzáférési pontok IP címeit a következő táblázat mutatja:

IP címkiosztás	
A hálózati cím és maszk:	
A hálózati azonosító:	192.168.10.0
A hálózatazonosító bitek száma:	25
Alhálózati maszk:	255.255.255.128
A rendelkezésre álló címtartomány:	192.168.10.1 - 192.168.10.126
Broadcast cím:	192.168.10.127
A hozzáférési pontok (AP-k) címei:	
foldszint_AP1	192.168.10.1
foldszint_AP2	192.168.10.2
foldszint_AP3	192.168.10.3
1em_AP1	192.168.10.4
1em_AP2	192.168.10.5
2em_AP1	192.168.10.6
2em_AP2	192.168.10.7
3em_AP1	192.168.10.8
3em_AP2	192.168.10.9
Állomásoknak kiosztható címtartomány:	
192.168.10.16 - 192.168.10.126	összesen 110 cím

18. ábra

A vezeték nélküli hálózat címe egy privát címtartományba tartozó hálózati cím. Az alhálózati maszkot úgy kell kialakítani, hogy figyelembe vesszük az állomások számának későbbi

növekedését is. A hálózat tervezésekor 20-40 eszköznek kell címet biztosítani, de később ez a szám akár duplájára is nőhet. A maszk hálózat azonosító bitjeinek száma ezért 25, ami 126 állomás címzését teszi lehetővé a 192.168.10.0 azonosítóval rendelkező hálózaton belül. A hozzáférési pontok a tartomány elejéről kapnak címeket Ez címzési konvenció, amelynek betartása segíti a konzisztens címzés kialakítását. Gyakran az eszközök címeit úgy adják meg, hogy azok kettő hatványaira essenek, így később a maszk átállításával könnyen kialakíthatóak alhálózatok. Itt erre nincs szükség, mert nem tervezzük a hálózat alhálózatokra bontását. A DHCP segítségével kiosztható címek a 192.168.10.16 és 192.168.10.126 közzé eső címek. A 192.168.10.10 és 192.168.10.15 közzé eső tartomány pedig további hozzáférési pontok címzésére van fenntartva. Ha privát címekkel rendelkező állomások számára akarjuk biztosítani az Internet hozzáférést, akkor hálózati címfordításra (NAT – Network Address Translation) van szükség. A NAT konfigurálása a vezetékes hálózatba tartozó forgalomirányítókon (router) történik. A címfordítás beállítása nem része a dolgozat témájának. A vezeték nélküli hálózat minden partner és dolgozó számára elérhető nyilvános hálózat, ezért nem szükséges külön VLAN –okra osztani. Az egyben kezelt WLAN előnye, hogy megkönnyíti a roaming (barangolás) megvalósítását is. Ha VLAN –ok használata mellett szeretnénk biztosítani a zavartalan kapcsolatot a teljes épületben, akkor további teendőink is lennének, például Proxy Mobil IP szolgáltatást kellene konfigurálnunk az összes hozzáférési ponton.

20.c Fizikai hálózatterv

A logikai terv elkészítése után a hálózat fizikai felépítését kell megtervezni. A követelmények alapján meg kell határozni a szükséges eszközök típusát, darabszámát és elhelyezkedését és a tervnek tartalmaznia kell a kábelrendező és az eszközök közötti kábelezés pontos leírását is. Az elvárásoknak legmegfelelőbb hozzáférési pont a Cisco Aironet 1230AG.

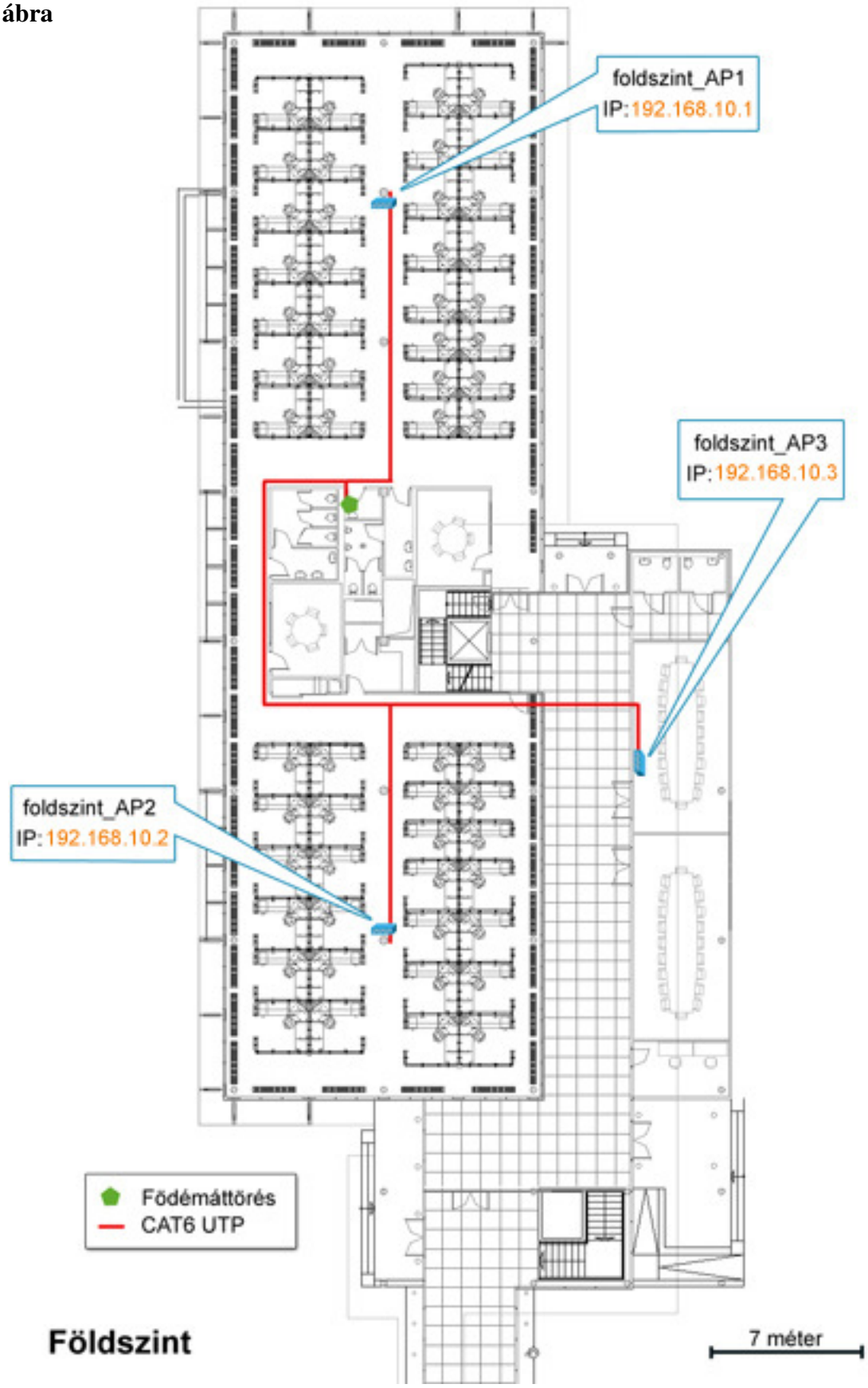
Az eszköz fontosabb jellemzői:

- Kétsávos működés: egyaránt támogatja a 802.11a és 802.11g szabványokat és együttes használatuk esetén 108 Mbps sebességre képes.
- Ellenálló fém váz

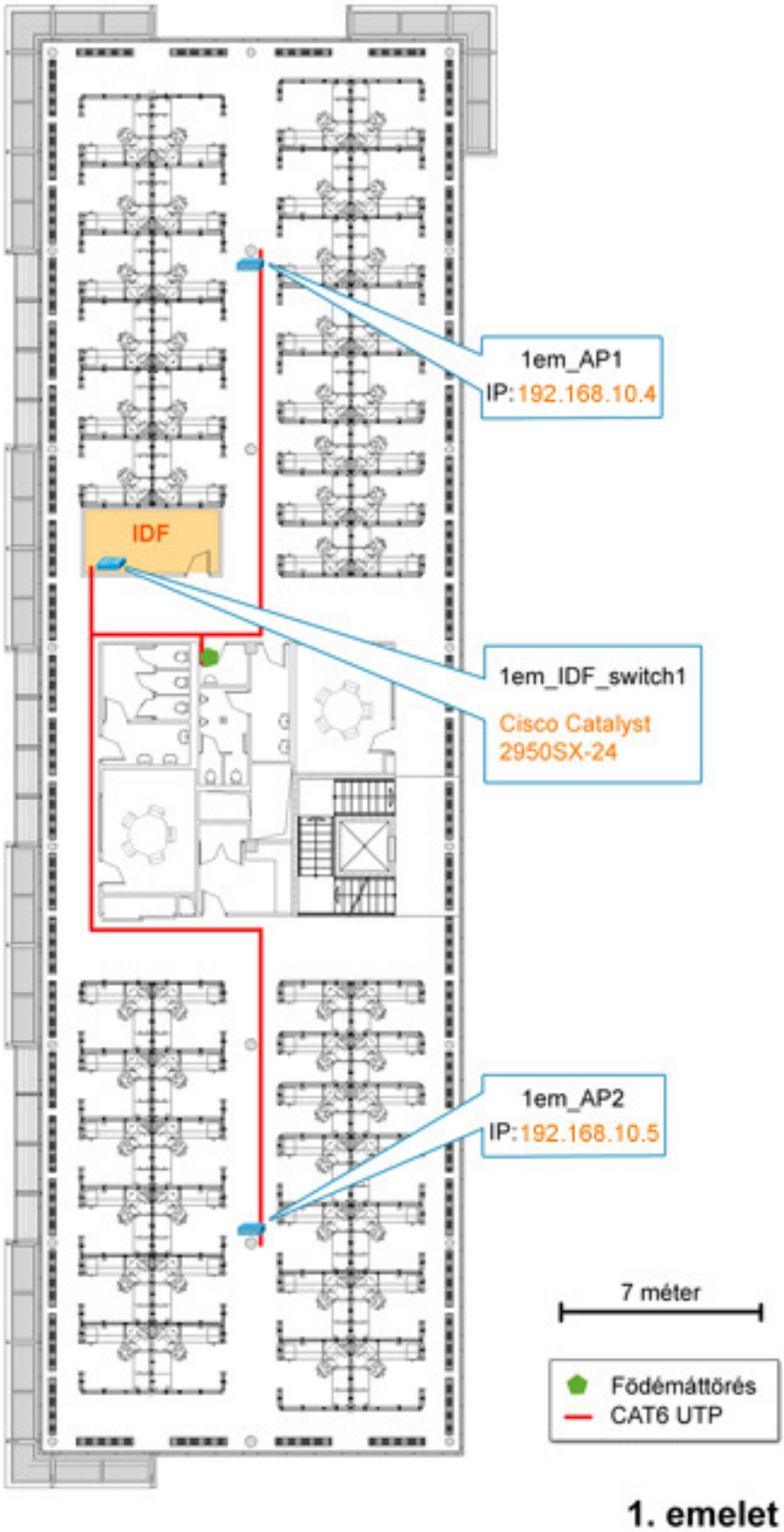
- -20 és +55 fok között üzemképes
- Támogatja az RP-TNC csatlakozókkal rendelkező külső antennákat
- Inline power támogatás (a működéshez szükséges áramellátás biztosítása hálózati kábelen keresztül)
- Az eszköz a 2.4 GHz –es frekvenciához 2.2 dBi –s, az 5 GHz –es frekvenciához pedig 3.5 dBi –s kétpólusú (dipole) antennákat használ.

Az AP –kat 3 méter magasan az épület belső terében lévő középső tartóoszlopokon helyeztem el lefelé fordított antennákkal, mivel így biztosíthatnak optimális lefedettséget és megfelelő jelminőséget. Az áramellátást nem a hálózati kábelek biztosítják, az eszközök az elektromos hálózatra csatlakoznak. A szünetmentes áramellátásáért az épületben lévő elektromos hálózat felel, ez biztosítja a többi eszköz és a gyártósor zavartalan működését is. A földszinten három, a többi szinten két AP található, erre az épület jellemzői miatt volt szükség. A hozzáférési pontokat egy Cisco Catalyst 2950SX-24 típusú 24 port –os kapcsoló csatlakoztatja a vezetékes hálózathoz. Ez a kapcsoló az első emeleten elhelyezkedő közbülső kábelrendezőben (IDF - intermediate distribution frame) található és 24 darab 100 Mbps –os porttal és 2 darab 1 Gbps -os uplink porttal rendelkezik a kellő sebesség biztosításához. A kapcsoló és az AP –k közötti kábelek 6 –os kategóriájú UTP (CAT6 UTP) kábelek. Azért ezt a típust választottam, mert áruk megközelíti a CAT5 UTP kábelek árát, viszont a későbbi hálózatbővítés során az alacsonyabb kategóriájú kábelek használata már lehet nem lesz elegendő a megfelelő sebességű átvitel biztosításához. A kábelek az álmennyezet felett elhelyezett kábeltálcában futnak. A szükséges hossz meghatározásakor mindig ajánlott a kiszámított hosszérték 1,25 -szorosát használni, így később nem érhet kellemetlen meglepetésként a kábel rövidsége. Fontos, hogy a szükséges hossz számításakor mindig számoljunk az épület belmagasságával is. A fizikai terv létrehozásakor figyelembe kell venni az épület építésekor felhasznált anyagokat is. A National Instruments új épületének padlóját legtöbb helyen szőnyegpadló borítja, de bizonyos helyiségek padlóját greslap (más néven kőporcelán lap) fedi. Az épület oldala speciális, nagy vastagságú üveglapból van, és ez néhány helyen elválasztóelemként is megjelenik a belső térben. Tervezéskor azért nagyon fontos az építőanyagok ismerete, mert azok nagy hatással lehetnek a rádiójelekre és ez által a vezeték nélküli hálózat teljesítményére is. Az itt használt speciális üveg például nagyon csökkenti a rajta áthaladó jelek teljesítményét és ezáltal korlátozza a hozzáférési pontok hatótávolságát. A következő ábrákon a hálózat kábelezési terve látható.

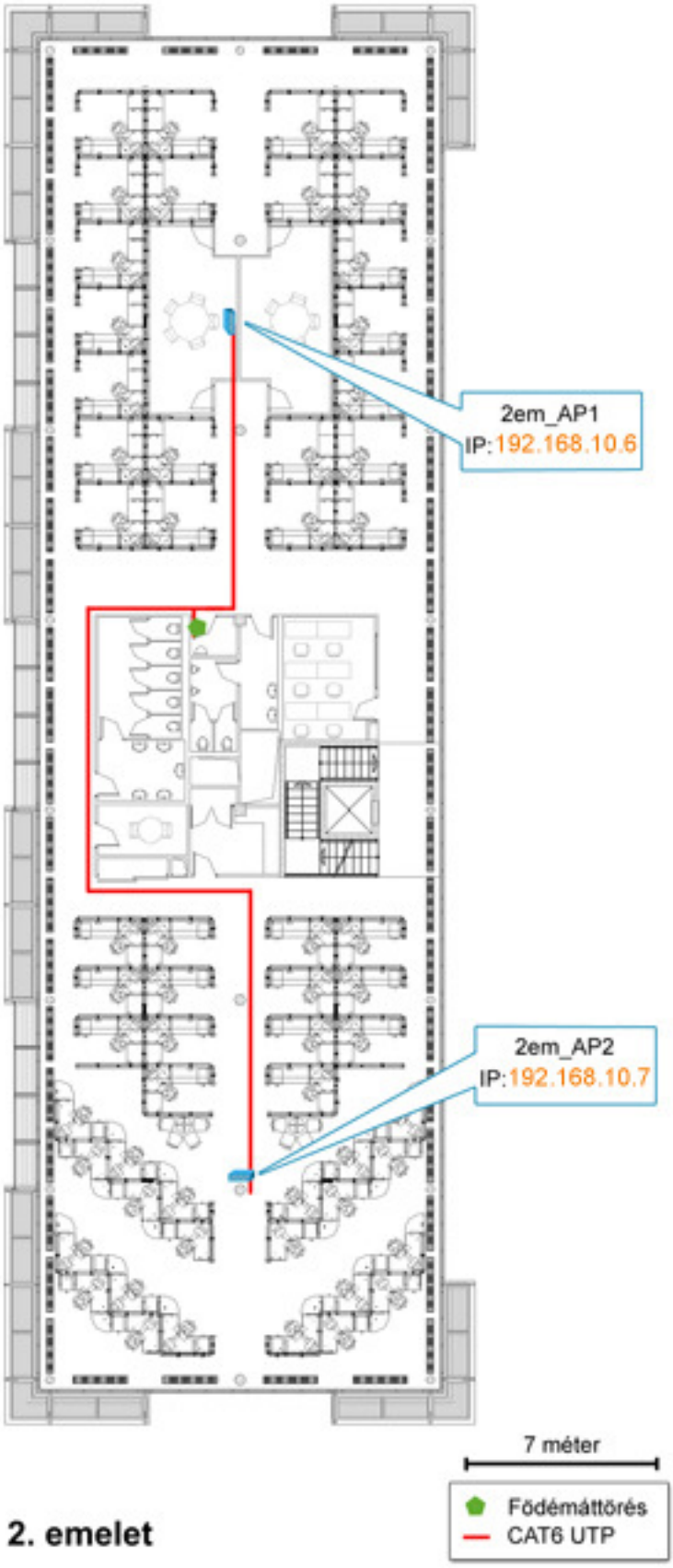
19. ábra


foldszint_AP1
IP:192.168.10.1
foldszint_AP3
IP:192.168.10.3
foldszint_AP2
IP:192.168.10.2
Födémáttörés
CAT6 UTP
Földszint
7 méter

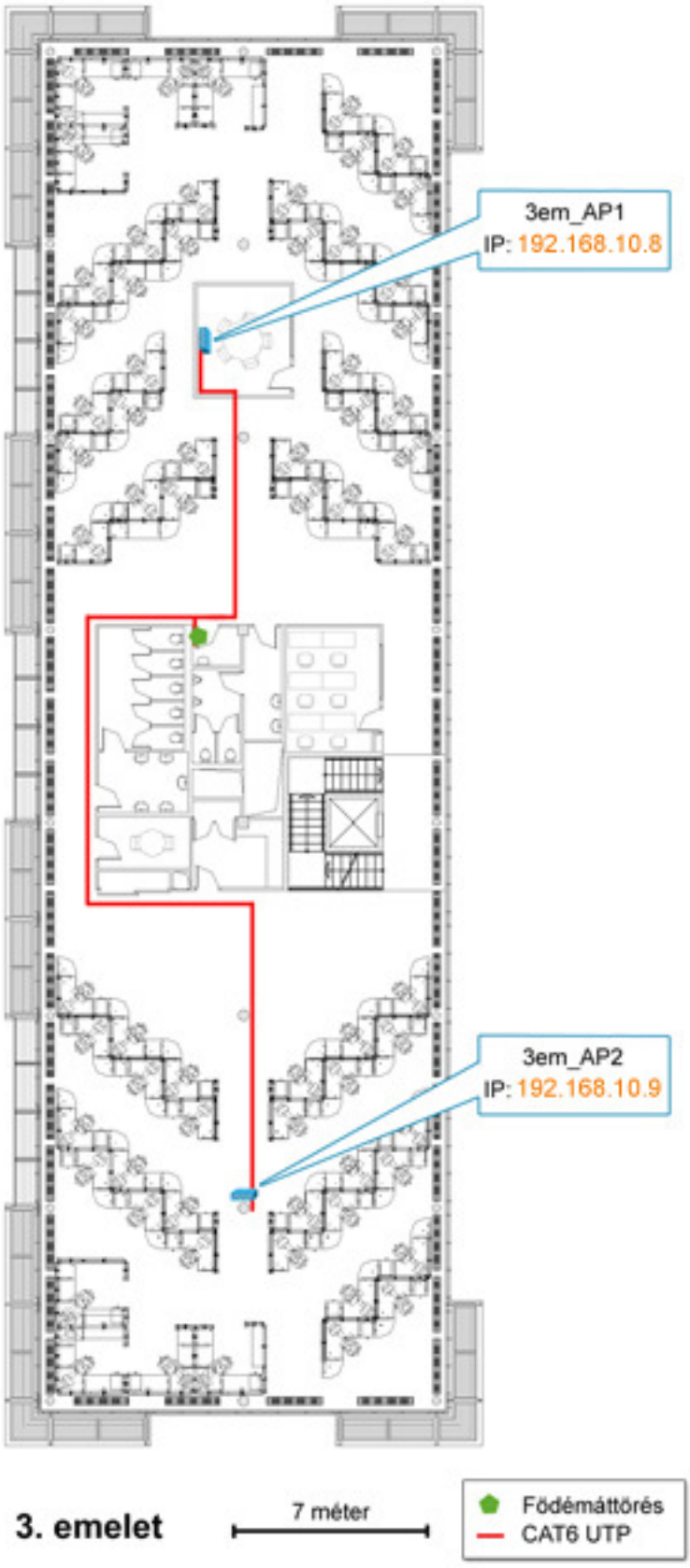
20. ábra


1em_AP1
IP:192.168.10.4
IDF
1em_IDF_switch1
Cisco Catalyst
2950SX-24
1em_AP2
IP:192.168.10.5
7 méter
Födémáttörés
CAT6 UTP
1. emelet

21. ábra


2em_AP1
IP:192.168.10.6
2em_AP2
IP:192.168.10.7
7 méter
Födémáttörés
CAT6 UTP
2. emelet

22. ábra


3em_AP1
IP: 192.168.10.8
3em_AP2
IP: 192.168.10.9
3. emelet
7 méter
Födémáttörés
CAT6 UTP

Kábelek elnevezése

Név	Honnan	Hova
1_IDF_switch1-F_AP1	1em_IDF_switch1	foldszint_AP1
1_IDF_switch1-F_AP2	1em_IDF_switch1	foldszint_AP2
1_IDF_switch1-F_AP3	1em_IDF_switch1	foldszint_AP3
1_IDF_switch1-1_AP1	1em_IDF_switch1	1em_AP1
1_IDF_switch1-1_AP2	1em_IDF_switch1	1em_AP2
1_IDF_switch1-2_AP1	1em_IDF_switch1	2em_AP1
1_IDF_switch1-2_AP2	1em_IDF_switch1	2em_AP2
1_IDF_switch1-3_AP1	1em_IDF_switch1	3em_AP1
1_IDF_switch1-3_AP2	1em_IDF_switch1	3em_AP2

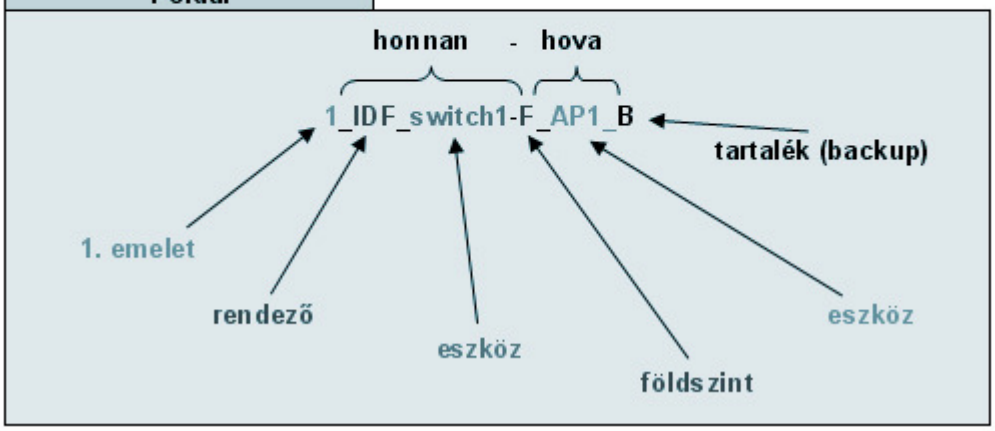
Tartalék kábelek

1_IDF_switch1-F_AP1_B	1em_IDF_switch1	foldszint_AP1
1_IDF_switch1-F_AP2_B	1em_IDF_switch1	foldszint_AP2
1_IDF_switch1-F_AP3_B	1em_IDF_switch1	foldszint_AP3
1_IDF_switch1-1_AP1_B	1em_IDF_switch1	1em_AP1
1_IDF_switch1-1_AP2_B	1em_IDF_switch1	1em_AP2
1_IDF_switch1-2_AP1_B	1em_IDF_switch1	2em_AP1
1_IDF_switch1-2_AP2_B	1em_IDF_switch1	2em_AP2
1_IDF_switch1-3_AP1_B	1em_IDF_switch1	3em_AP1
1_IDF_switch1-3_AP2_B	1em_IDF_switch1	3em_AP2

Formátum:

emelet_rendező_eszköz-emelet_eszköz

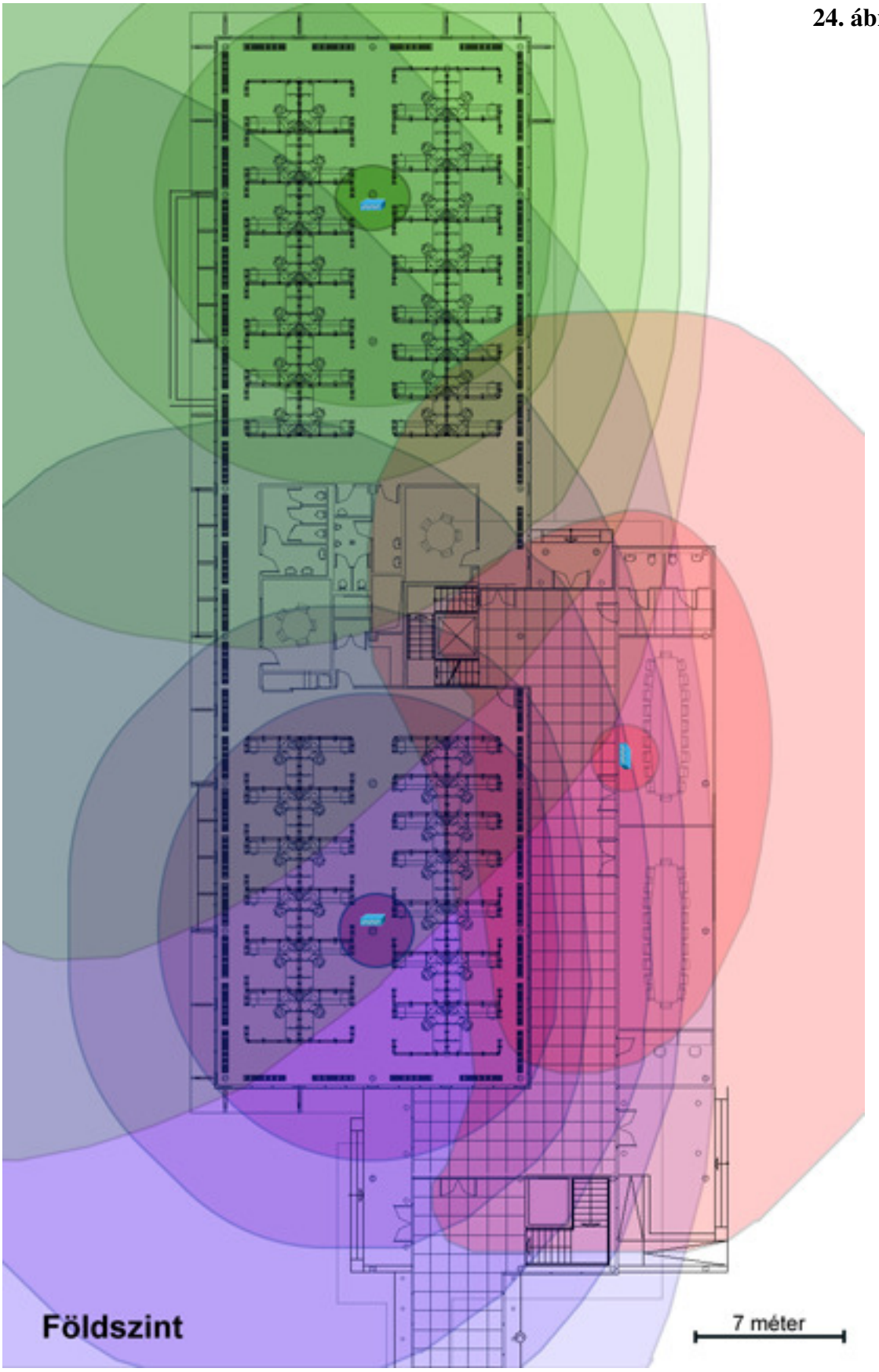
Példa:



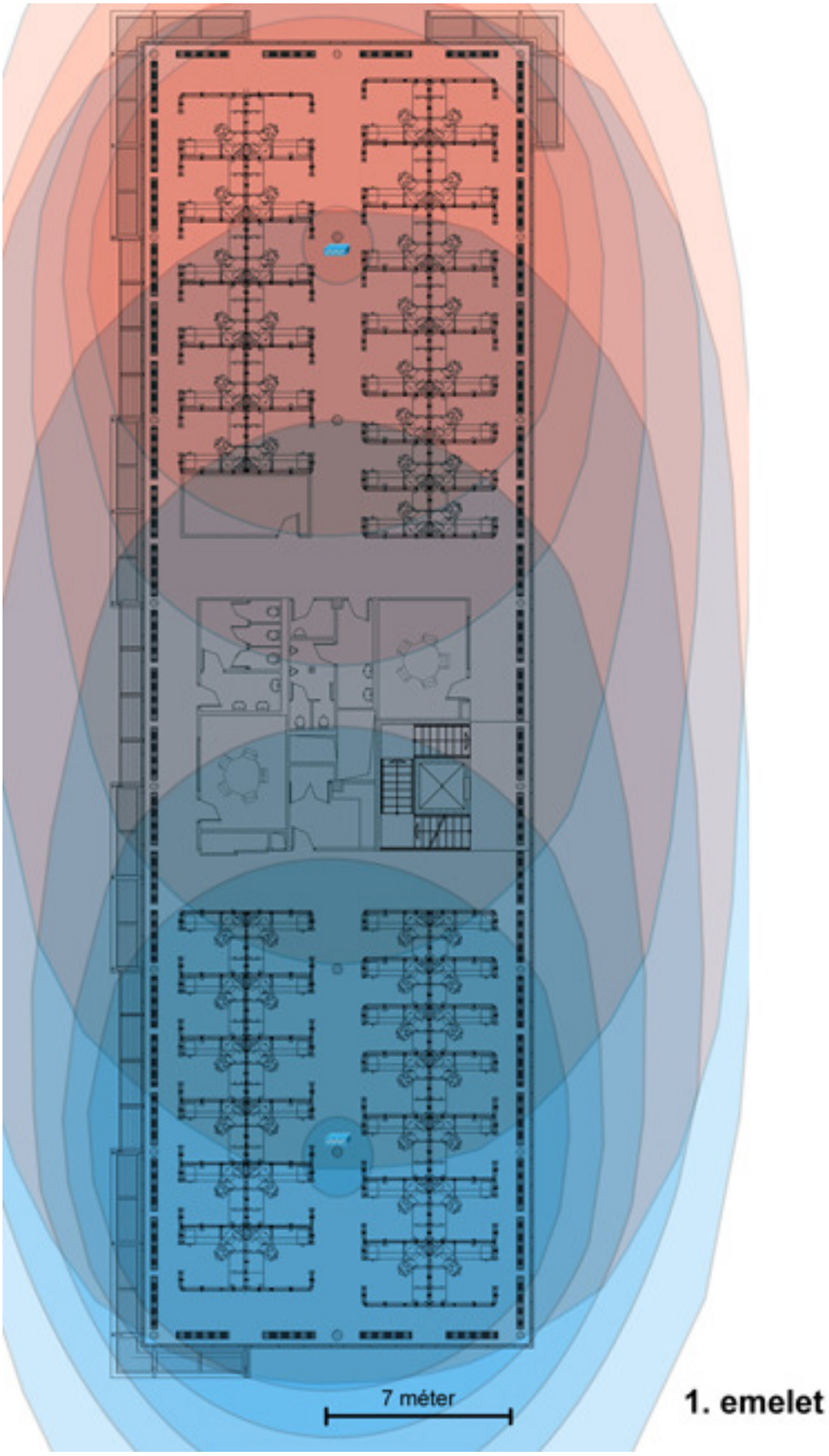
23. ábra

A kábelek elnevezése látható a 23. ábrán. Minden útvonalon (a kapcsoló adott portja és a hozzáférési pont közti útvonal) a szükséges kábel mellett egy tartalék kábel is ki van vezetve. Erre azért van szükség, mert a hibás kábelek későbbi cseréje sokkal több költséggel jár, mint a tartalékkábelek kezdetben történő lefektetése. A következő ábrákon a hálózati lefedettség és a jelek erőssége látható.

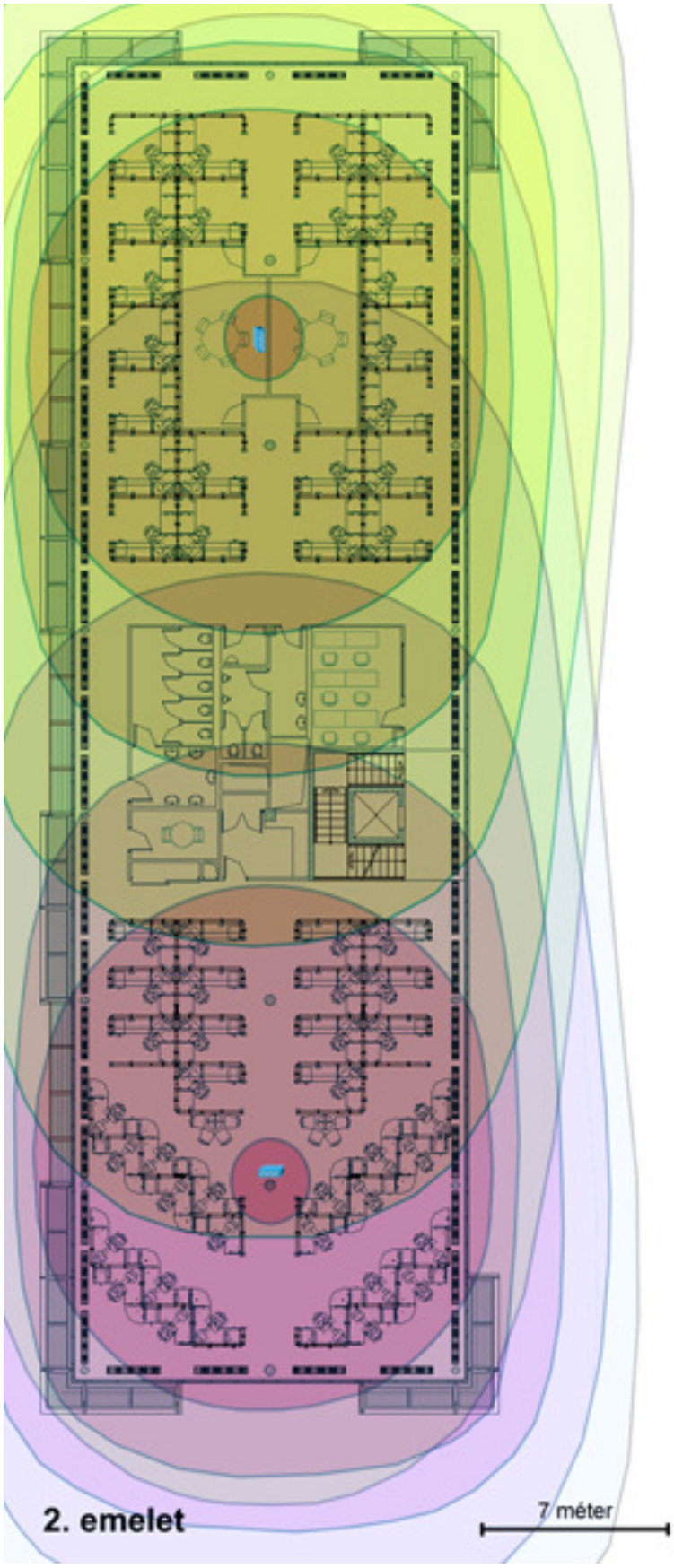
24. ábra



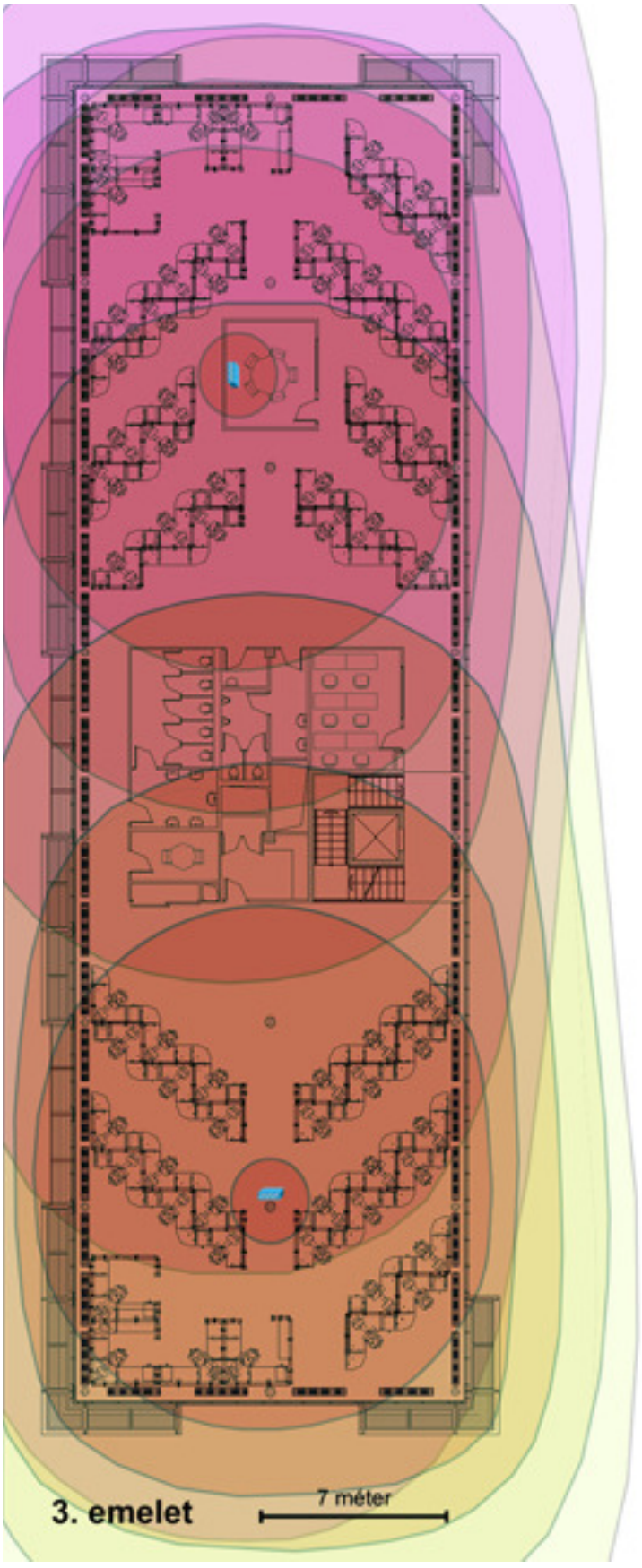
25. ábra



26. ábra



27. ábra



Az előző négy ábrán látható sávok a legsötétebbtől a legvilágosabbig sorrendben a -40, -50, -60, -70, -80, -90 dB –es erősségű jelet jelölik. A dB értékeket a következő képlet alapján kell kiszámítani: dB = 10 log10 (Pfinal/Pref).

A Pfinal a mért jel, a Pref pedig a kibocsátott jel teljesítményét jelöli. A Cisco Aironet 1230AG hozzáférési pont maximális teljesítménye 802.11a szabványú átvitel használata esetén 40 mW, 802.11b esetén pedig 100 mW. A -40 dB –es érték azt jelöli, hogy ha 1 mW a kibocsátott teljesítmény, akkor ennek csak a 10000 –ed része ér el a mérés helyére (100 mW kibocsátott teljesítménynél ez 0,01 mW). Ha a hozzáférési pont a legnagyobb teljesítményen üzemel, akkor a -70 dB –es érték még elfogadható erősségű jelet jelent.

A jel minőségét nem csak a jel erőssége befolyásolja, hanem a környezetben megtalálható interferencia mértéke is. Elképzelhető, hogy a jel nagyon erős a minősége mégis gyenge. Ez akkor fordulhat elő, ha nagy az interferencia. Az interferencia származhat más adóktól, de a saját jelünk visszaverődése, elhajlása, szóródása is ronthatja az adás minőségét. Azért, hogy pontosabb képet kapjunk a jel milyenségéről egy jel-zaj viszonyszámot (SNR – Signal to Noise Rate) szoktak megadni. Hálózat tervezésekor és a későbbi finomhangolás során érdemes ezt az SNR –t is figyelembe venni.

Fontos szabály az is, hogy a hozzáférési pontokat mindig úgy kell elhelyezni, hogy a lefedettségi területek 15-20% -ban fedjék egymást, így biztosítható, hogy a kapcsolat roaming esetén se szakadjon meg.

A 24. ábrán a földszint lefedettségi térképe látható. Megfigyelhető, hogy az alaprajz jobb oldalán található vastag üvegből készült ajtó milyen nagymértékben befolyásolja a jel terjedését. Az ilyen jelenségek miatt elengedhetetlenül fontos, hogy a tervezést megelőzően helyszíni szemlét tartson a tervező, és mérésekkel meghatározza a zavaró tényezőket. Sajnos a helyesen elkészített és mérésekkel alátámasztott hálózatterv sem garancia a WLAN megfelelő működésére. Gyakran az évszakok is befolyásolhatják a hálózatot (például a nyár során a fák megnövekedett lombkoronája akadályozhatja a kültéri antennák adását), vagy egy már meglévő jól működő hálózat mellé egy újat telepítenek és ez okoz problémát.

20.d Költségterv

A hálózatterv alapvető fontosságú része a költségek meghatározása. A következő ábrán a költségeket tartalmazó táblázat látható:

Költségterv					
Eszköz	**Mennyiség**	**Egység**	**Egységár**	**Összesen**	**Kép**
Cisco Aironet 1230AG	9	darab	113 952 Ft	1 025 568 Ft	
Cisco Catalyst 2950SX-24	1	darab	143 964 Ft	143 964 Ft	
CAT6 UTP fali kábel	910	méter	130 Ft	118 300 Ft	
CAT6 UTP csatlakozó	36	darab	45 Ft	1 620 Ft	
Törésgátló	36	darab	10 Ft	360 Ft	
Összesen:				**1 289 812 Ft**	

28. ábra

Hálózat telepítésekor a hálózati kábeleket gyakran előre gyártott, megadott hosszúságú darabokban vásárolják meg. Egy méter kábel ára tartalmazni szokta a vezeték, a csatlakozó, a törésgátló és a szerelés árát is, sőt a költségek tervezésekor beleveszik a telepítés díját is. A táblázatban azért szerepelnek a kábel részei külön, hogy azokról is kapjunk információt.

20.e A hozzáférési pontok beállításai

A hálózat megtervezése után a következő részfeladat az eszközök beállítása. A többi lépéshez hasonlóan a konfigurációt is tervezni kell. Ide tartoznak az alapvető eszközjellemzőkön (IP, eszköznév, SSID) kívül a működéshez szükséges beállítások (eszköz szerepe a hálózatban, menedzsment, gyártóspecifikus kiegészítő szolgáltatások, stb.), a biztonságot érintő kérdések és a hálózat finomhangolása is. A beállításokat elvégezhetjük grafikus felhasználói felületen (GUI) vagy parancssorban is. Tekintsük a paraméterek közül a legfontosabbakat (a következő beállítások a Cisco Systems által gyártott hozzáférési pontokon érvényesek, gyártótól függően változhatnak):

- Eszköznév (system name): ez a beállítás nem alapvető fontosságú, de segít azonosítani a hozzáférési pontot a hálózati szakemberek számára.
- Konfigurációs protokoll: megadhatjuk hogyan kapjon IP címet és egyéb alapvető beállításokat az AP. Lehetőség van DHCP használatára vagy kézi beállításra is.
- IP cím, alhálózati maszk, alapértelmezett átjáró: az eszköz alapvető jellemzői. DHCP használata esetén üresen kell hagyni.
- SSID: A SSID egy kis- és nagybetűérzékeny, egyedi azonosító, amit a kliens eszközök a hálózathoz való csatlakozáshoz használnak.
- A SSID hirdetése a keretekben: Ha igazra állítjuk üres, vagy nem egyező SSID –val rendelkező kliensek is csatlakozhatnak a hozzáférési ponthoz. Ez a beállítás az alapértelmezett, mert segíti a WLAN gyors telepítését. Javasolt letiltani a kiépített hálózatban, hogy növeljük a biztonságot.
- A hálózatban betöltött szerep: megadja az eszköz rendeltetését, ami lehet gyökér (root), vagy nem gyökér (non-root), attól függően, hogy az AP kapcsolódik-e vezetékes hálózathoz vagy sem.
- Rádió finomhangolása: optimalizálhatjuk a vezeték nélküli hálózatot úgy, hogy az átbocsátóképesség vagy a lefedettségi terület maximális legyen, vagy megadhatunk saját konfigurációt is.
- SNMP jellemzők: itt adhatjuk meg az SNMP protokollhoz kapcsolódó speciális paramétereket.

- Sebesség és az átvitel iránya: a vezetékes hálózathoz hasonlóan itt megadhatjuk, hogy az eszköz milyen maximális sebességen használja az adott interfészt, és milyen legyen a kommunikáció iránya. (váltakozó irányú, azaz half duplex, vagy kétirányú, full duplex). Az alapértelmezett beállítás mindkét esetben az automatikus választás.
- Rádió teljesítmény: itt kiválaszthatjuk a hozzáférési pont adójának teljesítményét. Ezt a paramétert használhatjuk a lefedettségi terület korlátozására. Megadhatjuk, azt is, hogy a kliensek maximálisan milyen teljesítménnyel üzemelhetnek. Ha a kliens nem tartja be a korlátozást az AP nem engedélyezi a csatlakozást.
- Csatorna: az itt beállított csatornát fogja használni az eszköz. Az alapértelmezett konfiguráció szerint a hozzáférési pont a legkevésbé foglalt csatornát választja ki az indulási folyamat során.
- Beágyazás (encapsulation): Lehetőség van a 802.1H vagy az RFC1042 típusú beágyazások közül választani.
- Szolgáltatások: A hozzáférési pont különféle szolgáltatásokat (Telnet, VLAN, DNS, QoS, CDP, Hot Standby, Proxy Mobile IP, stb.) nyújthat a kliensek számára.

A hozzáférési pontok beállításai	
Eszköznév	lásd logikai topológia
Konfigurációs protokoll	DHCP
IP cím	lásd címtáblázat
Alhálózati maszk	lásd címtáblázat
Alapértelmezett átjáró	lásd címtáblázat
SSID	Public
SSID hírdetése a keretekben	Igen
A hálózatban betöltött szerep	Root
Optimalizálás	Átbocsátóképesség (throughput)
SNMP	nem használt
Sebesség	Auto
Átvitel iránya	Auto
Rádió teljesítmény	Maximális
Csatorna	Legkevésbé használt csatorna
Beágyazás	RFC1042 (alapértelmezett)
Szolgáltatások	Engedélyezve: Telnet, CDP, HTTP

29. ábra

A 29. ábrán a dolgozatban szereplő hálózat hozzáférési pontjainak konfigurációja látható. Az eszközök DHCP segítségével kapják meg az IP címüket, a hálózati maszkot, és az alapértelmezett átjáró címét. A DHCP szerveren statikusan van összerendelve az AP –k fizikai és IP címe. A hálózat a „Public" SSID –t használja. Az SSID hirdetése engedélyezett, azaz nem csak azok a kliensek csatlakozhatnak, amik ezzel megegyező azonosítóval rendelkeznek. Ez a beállítás csökkenti a biztonságot, ezért csak indokolt esetben ajánlott. Itt azért van szükség rá, mert a vállalathoz érkező partnerek számára úgy szeretnénk biztosítani a hálózati kapcsolatot, hogy az ne igényeljen konfigurációt. Ha ilyen beállítást választunk nagyon fontos, hogy a vezeték nélküli hálózatot használó klienseket a vezetékes hálózaton található eszközökkel megfelelően korlátozzuk, különben nagy biztonsági kockázatot vállalunk. A tervezett hálózat egy olyan vezetékes LAN –hoz csatlakozik, ahol ezek a korlátozások be vannak állítva. A „Public" (vagy üres) SSID –t használó kliensek nem férhetnek hozzá a vezetékes hálózaton található erőforrásokhoz, csak az Internet elérése engedélyezett. Ha szeretnénk kialakítani egy biztonságos WLAN –t, akkor a korábban leírt előírásokat kell követnünk, tehát felhasználó szintű hitelesítésre és megfelelő titkosításra is szükség van. Az ilyen esetekben lehetőség van több SSID beállítására a hozzáférési pontokon. Az egyes azonosítók más-más lehetőségeket nyújthatnak a felhasználók számára, így elérhetővé válnak a belső hálózati erőforrások is. Ekkor használhatnánk például a „Secure" SSID –t és szükség lenne a vezetékes hálózatra csatlakozó hitelesítő (RADIUS) szerverre is, amely például EAP-TTLS típusú hitelesítést valósítana meg. A hitelesítő szerver használatával lehetőség nyílik a hitelesítés címtárszolgáltatásba (például Microsoft Active Directory) való integrálására is, aminek előnye, hogy központosított, egységes kezelhetőséget biztosít. A hitelesítésen túl szükség van a megfelelő titkosításra is. A biztonság érdekében mindig ajánlott a 802.11i szabvány használata, ha az eszközök támogatják. A tervben lévő összes hozzáférési pont csatlakozik a vezetékes hálózathoz, ezért a vezeték nélküli hálózatban gyökér (root) szerepet töltenek be. Minden eszköz úgy van beállítva, hogy a lehető legnagyobb átbocsátóképességet biztosítsa (még akkor is, ha ez a lefedettségi terület csökkenésével jár). Az interfészeik sebességét automatikusan választják az AP –k (mindig a lehető legnagyobb). A rádió teljesítmény maximálisra van állítva, ez 802.11a esetén 40 mW, 802.11b esetén pedig 100 mW. Minden hozzáférési pont a legkevésbé foglalt csatornán üzemel. Az eszköz ezt indulásakor határozza meg és nem is változtatja meg újraindításig. Ezzel a beállítással nincs szükség külön csatornakiosztás

elkészítésére, az állomások alkalmazkodni fognak a környezetükhöz. A beágyazás típusa RFC1042, mivel ez biztosítja a legjobb együttműködést a különböző gyártótól származó készülékek között. Ha csak Cisco Aironet eszközök támogatása szükséges, akkor a 802.1H beágyazás a jó választás, mert az optimálisabb teljesítményt biztosít.

20.f A hálózat továbbfejlesztése

A hálózatokat mindig úgy kell megtervezni, hogy a terv később könnyen módosítható, bővíthető legyen. Fel kell készülni az állomások számának növekedésére és az új technológiák támogatására is. Gyakran új szolgáltatások beindítására is szükség van a már működő hálózatban. Ilyen nagyobb sávszélességet igénylő alkalmazások és technológiák például a hang vagy videó átvitelen alapuló megoldások (VoIP, videokonferencia rendszerek mint a Cisco Telepresence, stb). Ha a hálózatterv készítésekor nem készültünk fel a jövőbeli bővítésre később sokkal több utólagos költséggel és szolgáltatás-kiesésből származó kellemetlenséggel kell majd szembenéznünk. A jó hálózatterv mindig tartalmaz tartalék erőforrásokat (például még nem igényelt sávszélesség, tartalék eszközök és bővítőhelyek). A dolgozatban szereplő hálózat is úgy lett megtervezve, hogy később könnyen bővíthető és alakítható legyen a változó igényeknek megfelelően. Be lehetne vezetni például szolgáltatásminőségre (QoS - Quality of Service) vonatkozó előírásokat és különféle hang és videó alapú szolgáltatásokat is, ennek bemutatása viszont már nem témája a dolgozatnak.

21. Összegzés

A vezeték nélküli hálózatok korai változatai nem voltak problémamentesek. Kezdetben gondot okozott a megfelelő megbízhatóság, a teljesítmény, a biztonság és a különféle gyártók készülékei közti együttműködés is. Azóta a WLAN –ok nagy fejlődésen mentek keresztül. Egyre több korai problémára születik jó megoldás, ezért a vezeték nélküli hálózatok is egyre népszerűbbek. Mára sem a sebesség, sem a megbízhatóság nem jelent gondot, ezért a WLAN –ok száma rohamosan növekszik. A 802.11 szabványra épülő hálózatok hamar kiépíthetőek, könnyen bővíthetőek, ezáltal rugalmasak és jól skálázhatóak. Telepítésük a hagyományos vezetékes hálózatokénál kevesebb költséggel jár és fenntartásuk sem drága, ezért a kezdeti befektetés hamar megtérül. Jelenleg több különféle technológia közül is választhatunk aszerint, hogy céljainknak és elvárásainknak melyik felel meg a legjobban, ezért a WLAN –ok egyre több területen válnak a vezetékes hálózatok ésszerű alternatívájává. Vezeték nélküli hálózatok tervezésekor a hagyományos hálózatok tervezésénél használt irányelveken kívül egyéb szabályokat is be kell tartani és bizonyos esetekben körültekintőbben kell eljárni, de megfelelő szaktudással és odafigyeléssel a hagyományos hálózatoknál megszokott teljesítménnyel és megbízhatósággal rendelkező WLAN alakítható ki. A dolgozat célja egy olyan hálózatterv elkészítésének bemutatása, amely az elvárásoknak megfelelő jellemzőkkel rendelkező hálózatot eredményez. A dolgozat magába foglalja a terv elkészítéséhez szükséges ismereteket és a használt technológiák és eljárások működésének leírását is, mivel ezek megértése elengedhetetlenül fontos a tervezéskor. Megismerjük a hálózatok kialakulását, a kezdeti elvárásokat és problémákat és a felmerült kérdésekre adott válaszokat. A későbbi fejezetekben olvashatunk az IEEE által kiadott 802.11 –es szabványcsalád megoldásairól és a hálózatok különböző technológiájú megvalósításairól is. A dolgozat foglalkozik a vezeték nélküli LAN –ok egyik legnagyobb problémát jelentő kérdésével, a biztonsággal is. Ezután megismerhetjük a hálózatterv készítésének alapvető lépéseit: a követelmények elemzésétől az eszközök beállításáig. Az elkészített minta hálózat terve tartalmazza az összegyűjtött követelmények, a logikai felépítés és a fizikai megvalósítás leírását és a szükséges eszközöket tartalmazó költségtervet is. A kábelek elhelyezkedésén kívül a fizikai terv tartalmazza a hozzáférési pontok által biztosított lefedettségi területeket szemléltető ábrákat is, melyek helyszíni mérések alapján készültek és alátámasztják a tervben

szereplő megoldások szükségességét. A terv bemutatása után olvashatunk a hálózat továbbfejlesztéséről, lehetséges új funkciók bevezetéséről is.

A dolgozat a minta hálózat dokumentációján kívül törekszik a javasolt megoldások ismertetésére, előnyeiknek és hátrányaiknak bemutatására is, így az olvasó átfogó képet kaphat a hálózatterv elkészítésének összetettségéről és a vezeték nélküli hálózatok működéséről is.

Irodalomjegyzék

1. **[ANDREA GOLDSMITH]**
   Andrea Goldsmith**:** Wireless communications. Cambridge; New York: Cambridge University Press, 2005.

2. **[BROADCOM]**
   Broadcom Corporation: 802.11n - Next-Generation Wireless LAN Technology, 2006. In http://www.broadcom.com/docs/WLAN/802_11n-WP100-R.pdf
   Megnyitva: 2007-05-01

3. **[CISCO]**
   Cisco Systems: Fundamentals of Wireless LANs Version 1.2, 2005.
   In http://www.cisco.com/web/learning/netacad/index.html
   Megnyitva: 2007-05-01

4. **[JIM GEIER]**
   Jim Geier**:** Vezeték nélküli hálózatok. Budapest: Panem, 2005.

5. **[KAVEN PAHLAVAN]**
   Kaven Pahlavan, Allen Levesque: Wireless information networks. Hoboken, NJ: John Wiley, 2005.

6. **[MATTHEW S. GAST]**
   Matthew S. Gast**:** 802. 11 wireless networks: the definitive guide. Beijing [u.a.]: O'Reilly, 2005.

7. **[MICROSOFT TECHNET]**
   Microsoft Corporation: How 802.11 Wireless Works, 2003. In http://technet2.microsoft.com/WindowsServer/en/library/370b019f-711f-4d5a-8b1e-4289db0bcafd1033.mspx?mfr=true
   Megnyitva: 2007-05-01

8. **[RON FULLER]**
Ron Fuller, Tim Blankenship: Building a Cisco Wireless LAN. U.S: Syngress Media, 2002.

9. **[WIKIPEDIA]**
Wikipedia: IEEE 802.11, 2007.
In http://en.wikipedia.org/wiki/IEEE_802.11
Megnyitva: 2007-05-01

10. **[WILLIAM WEBB]**
William Webb: Wireless Communications: The Future.
John Wiley and Sons Ltd, 2007.

11. **[TANENBAUM]**
Andrew S. Tanenbaum: Számítógép-hálózatok. Budapest: Panem, 2004.

Köszönetnyilvánítás

Szeretném megköszönni Dr. Almási Bélának és Kiss Attilának a dolgozat elkészítése során nyújtott segítséget és a National Istruments –nek, hogy rendelkezésemre bocsátotta a munkámhoz szükséges eszközöket.