Debreceni Egyetem

Informatikai Kar

Wireless rendszerek hatékonysági vizsgálatai

Témavezető:
Dr. Sztrik János
tanszékvezető egyetemi tanár
a MTA doktora

Készítette:
Zelerik Attila
mérnök informatikus

Debrecen
2009

Tartalomjegyzék

1 Köszönetnyilvánítás

1995 óta foglalkozom az informatikával. Vezetékes távközlési technikus végzettséggel kezdtem a pályámat egy informatikai vállalkozásnál. Abban az időben főként arcnet hálózatokat üzemeltettünk és kicsit később kezdtük el az ethernet hálózatok építését. Eleinte koaxiális ethernet kábelekkel, majd csavart érpáras technológiával létesítettük a hálózatokat. 2000 –től optikai hálózatokat is építünk ragasztott és hegesztett technológiával egyaránt.

A Debreceni Egyetemen megszerzett tudás nagymértékben hozzájárult ahhoz, hogy az eddigiekben – főként tapasztalati úton – összeszedett szakmai hátteret mélységeiben megértsem, a jövőben még jobban alkalmazni tudjam. A korábbi ismereteim alapján nagyjából tisztában voltam azzal, hogy egy hálózatot hogyan kell kiépíteni, most már azt is tudom, hogy miért úgy.

Köszönetet mondok Dr. Sztrik János professzor Úrnak a dolgozatom témavezetéséért és a valószínűségszámítás rejtelmeinek megismertetéséért. Az egyetemi oktatóimnak, akik közreműködésükkel elősegítették a szakmai fejlődésemet.

Külön köszönet a Mondi Bags Hungária Kft –nek, Lelesz Miklós gyárigazgató Úrnak, aki lehetővé tette, hogy az üzemük területén lévő informatikai rendszerekhez hozzáférjek.

2 Bevezetés

Napjaink infokommunikációs hálózatait egyre inkább a sokszínűség, a heterogenitás jellemzi. A felhasználók adatátviteli szükségleteinek kiszolgálására ma már számos különböző technológia és átviteli közeg (például réz érpár, koaxiális kábel, fényvezető szál, szabad tér) áll rendelkezésre. Az infokommunikációs hálózatok elektronikus tartalmak elérésére és elérhetővé tételére szolgálnak. Habár - úgy a hálózati technológiák (átviteli közegek, kommunikációs technikák), mint a felettük megvalósított szolgáltatások (specifikus erőforrásigények és minőségi követelmények szempontjából) - alapvetően inhomogének, egyre erőteljesebbé válik az a törekvés, hogy bármilyen szolgáltatást képesek legyünk bármilyen hálózati környezetben biztosítani, a felhasználó számára transzparens módon.

Dolgozatomban a fent felsorolt közegek közül a szabad térben – mint fizikai közegben – megvalósított infokommunikációs hálózatokkal foglalkozom behatóbban.

A „vezeték – nélküliség” számos pozitív tulajdonsággal bír, melyek közül talán a legfontosabb a mobilitás. Mármint hogy a felhasználó bizonyos körülhatárolt (lefedett) területen belül szabadon mozoghat, nincs vezetékkel odaláncolva a hálózati csatlakozóhoz. De ennek bizony ára van. Mégpedig az, hogy a sávszélesség erősen korlátozott a vezetékes technológiákhoz képest.

A továbbiakban egy létező ipari telephelyen lévő alapanyag raktárban és üzemcsarnokban kiépítendő vezeték nélküli hálózat megtervezéséről, megvalósításáról, a kész hálózat hatékonysági vizsgálatairól lesz szó. A megrendelő cég egy komplett termelés-irányítási rendszert helyez üzembe, aminek szerves része az alapanyag, és a készáru folyamatos nyomon-követése. A cég papírzsákokat-, zacskókat gyárt. Az alapanyagok 4 – 5 tonnás papírtekercsek, amelyek egy két részre osztott alapanyagraktárban vannak tárolva. A termelésirányító rendszer része néhány mobil adatgyűjtő, amelyeket a - papírtekercseket és a készárut mozgató - targoncás személyzet kezel. Emiatt szükséges a vezeték-nélküli hálózat kiépítése, mivel semmilyen módon nem lehetséges a felmerülő igényt vezetékes környezetben kielégíteni.

3 A fizikai környezeti adottságok, hálózati követelmények

3.1 Környezet leírása

Dolgozatomban a Mondi Bags Hungária Kft. Nyíregyházi telephelyén kialakításra kerülő vezeték nélküli hálózat megtervezéséről, kiépítéséről, hatékonysági vizsgálatairól lesz szó.

A megrendelő telephelyén SAP ISCA rendszer kerül bevezetésre, ami a komplett termelési folyamatot nyomon követi. Az alapanyag bevételétől a termelési folyamatokon át egészen a készáru kiszállításáig. Emiatt szükséges az áruk mozgásának nyomon követése, amelyet Symbol mobil adatgyűjtőkkel kívánják megvalósítani. A mobil adatgyűjtők részére folyamatos kapcsolatot kell biztosítani az adatbázis-szerverrel az adatok konzisztenciája miatt. Ezt az adatkapcsolatot kizárólag vezeték nélküli hálózattal lehet megvalósítani. A megrendelő részéről a következő területek lettek kijelölve a vezeték nélküli lefedettség kiépítésére: alapanyagraktár bejárata (ahol a papírtekercseket beszállítják a raktárba), a teljes alapanyagraktár, az üzemcsarnok alapanyag behordási szakasza, az üzemcsarnok készáru kihordási szakasza, a teljes készáru raktár.

A tervezés folyamán nagy figyelmet kell fordítani arra, hogy az alapanyagraktárban tárolt áru mennyire befolyásolja a rádiófrekvenciás jelek terjedését. Mivel az alapanyagraktárban nagyméretű (átlagban 1,5m átmérőjű, 1,5m magas) papírtekercsek vannak egymáson (5-6 magas rakatokban) tárolva, azok komoly árnyékolást okoznak a jelek terjedésében.

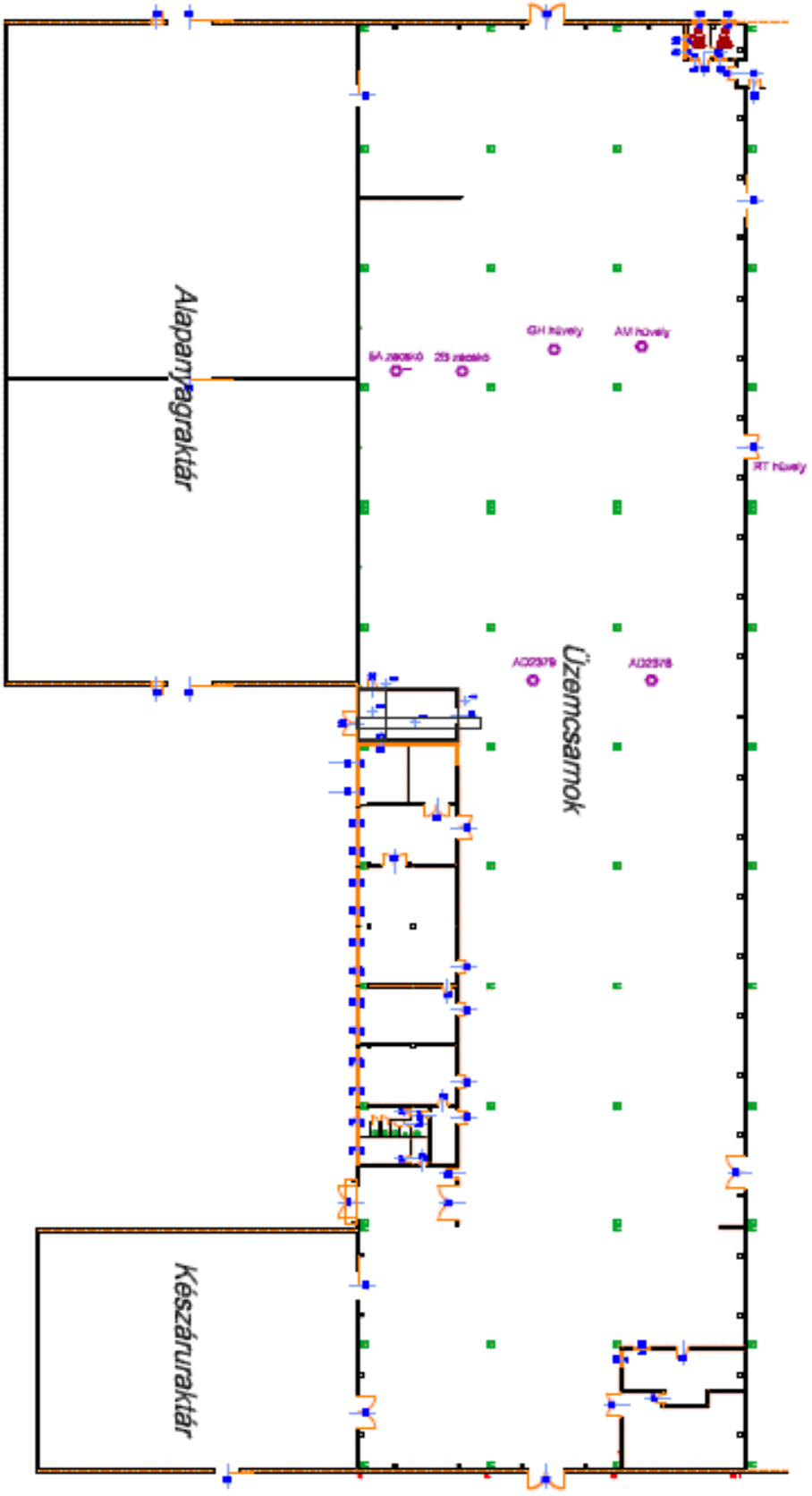
1. ábra Alapanyagraktár

2. ábra Alapanyagraktár a papírtekercsekkel

A hálózat tervezésének folyamatát helyszíni bejárással kezdtem. Méréseket végeztem a rádiófrekvenciás jelek terjedésével kapcsolatban. A mérések folyamán 1 db Cisco AIR-AP1242AG-E-K9 AP –t használtam, továbbá NetStumbler – 0.4.0 szoftvert futtató mobil számítógépet.

A mérések folyamán arra a következtetésre jutottam, hogy a hálózattal lefedni kívánt területre 10 db Access Point felszerelése szükséges.

3. ábra Az üzem alaprajza



3.2 Hálózat működésével szemben támasztott követelmények

A raktárakban és az üzemcsarnokban a hálózatnak úgy kell működni, hogy az épületek (megrendelő által kijelölt épületrészek) bármelyik pontján legyen kellő wifi lefedettség az adatgyűjtők üzembiztos működéséhez. Emiatt az IEEE 802.11g szabványt vettem figyelembe a tervezés folyamán. Az IEEE 802.11g szabvány szerint az adatátvitel 2.4 GHz frekvencián történik. A vezeték nélküli adatátviteli szabványok közül ez felel meg leginkább a fizikai adottságok miatt.

A megrendelő által megadott információk alapján az IEEE 802.11g szabványban megadott maximális adatátviteli sebesség – figyelembe véve az ISCA rendszer által megkövetelt sávszélességet – bőségesen elegendő a biztonságos működéshez.

4 Az IEEE 802.11g szabvány szerinti adatátvitel ismertetése

4.1 Vezeték nélküli adatátviteli szabványok általános ismertetése

Az **IEEE 802.11** egy vezeték nélküli adatátviteli protokoll. Az OSI modell két legalsó rétegét, a fizikai és az adatkapcsolati réteget definiálja.

Fizikai réteg szempontjából három lehetőséget határoz meg:

IR – infravörös - közvetlen rálátásra van szükség, csak beltérben használható, sebesség max. 2 Mb/s

FHSS (Frequency Hopping Spread Spectrum) – frekvenciaugrásos szórt spektrum, 2,4 GHz

DSSS (Direct Sequence Spread Spectrum) – 5 GHz, redundancia a kódban (Barker sequence)

1999-ben megjelent a 802.11b szabvány, amely az előző továbbfejlesztett változata volt. Az adatátviteli sebesség egy új modulációs technikának (CCK) köszönhetően 11Mbps-ra növekedett, és a csatorna hozzáférés direkt-sorrendűre változott (DS). A 802.11b kisebb sebességre kapcsolt az adó és vevőegységek távolságának növekedésével, és jóval nagyobb sebességének köszönhetően pár év alatt kiszorította az FHSS rendszereket. Érdekes volt, hogy ezzel egyidejűleg, szintén 1999-ben ratifikálták az 5GHz-es tartományban működő 802.11a protokollt, amely már ekkor 54Mbps-os sebességet produkált, az újonnan kifejlesztett OFDM moduláció alkalmazásával.

A vezetékes világgal egy nagyságrendben lévő adatátviteli sebesség ellenére a 802.11a rendszerek mind a mai napig nem terjedtek el. Ennek egyik oka az 5GHz-es tartomány korlátozott hozzáférhetősége a katonai radarok hasonló frekvenciái miatt, másrészt 2003 folyamán megjelent a 802.11g szabvány, amely az OFDM moduláció alkalmazásával megsokszorozta a 802.11b rendszerek sebességértékét, elérve ebben a frekvenciasávban is az 54Mbps-os értéket. Az új szabvány különlegessége volt a „b” rendszerrel történő kompatibilitás. A gyakorlatban ez azt jelenti, hogy a 802.11g eszközök automatikusan felismerik és hozzákapcsolódnak a 802.11b elérési pontokhoz, és fordítva, a régi 802.11b eszközöket felismerik az új 802.11g cellák.

A 802.11 LAN egy celluláris architektúrára épül, ahol a rendszer cellákra van osztva. Az egyes cellákat (**B**asic **S**ervice **S**et, röviden BSS-nek nevezik a 802.11 terminológiában) bázisállomások irányítják, melyeket hozzáférési pontnak (**A**ccess **P**oint, AP) hívunk.

Bár egyetlen cellából is állhat a vezeték nélküli LAN, leggyakrabban néhány cellából álló rendszereket valósítanak meg, ahol a hozzáférési pontok valamilyen gerinchálózaton, elosztórendszeren (Distribution System) keresztül kapcsolódnak egymáshoz. Logikailag elkülönül a BSS-en belül használt átviteli közeg az elosztórendszer átviteli közegétől, ez a kulcsa az architektúra rugalmasságának. A gerinchálózat általában Ethernet, de maga is lehet vezeték nélküli. A teljes összekapcsolt WLAN – beleértve a különböző cellákat, a hozzájuk tartozó hozzáférési pontokat és az elosztórendszert – a felsőbb rétegek számára egy egyszerű 802-es (Ethernet) hálózatnak látszik és a szabványban **E**xtended **S**ervice **S**et-ként van meghatározva.

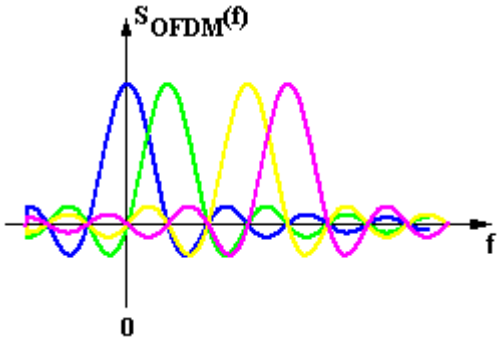
A vezeték nélküli LAN-ok két alapvető konfigurációja az ad-hoc és az infrastruktúra hálózat. Ad-hoc, amikor köztes access-point nélkül, csupán a mobil eszközök kapcsolódnak egymáshoz, míg az infrastruktúra hálózatoknál a mobil eszközök access-pointokhoz csatlakoznak, és azon keresztül érik el a hálózat egyéb csomópontjait.

4.2 IEEE 802.11g

Ezt a protokollt 2003-ban fejlesztették ki. Célja az volt, hogy a már adott 2.4 GHz-es frekvenciatartományban az elődeinél (802.11, 802.11b) nagyobb adatátviteli sebességgel bírjon. A 802.11g-nek ugyanaz az ISM hatásköre/hatótávolsága, mint a 802.11b-é, de más moduláció sémát használ, amit ***Orthogonal Frequency Division Multiplexing*** (***OFDM-nek)*** hívnak. Maximális adatátviteli sebessége 54 Mbps, de használható 22 Mbps teljesítménnyel és vissza tud esni 11 Mbps DSSS-re vagy lassabbra a visszább lévő kompatibilitásúakra az eddigi legnépszerűbb 802.11b-ére.

OFDM moduláció:

Orthogonal Frequency Division Multiplex, sok független, keskenysávú vivőfrekvenciát alkalmazó moduláció. Minden egyes vivőfrekvencia tetszőleges PSK vagy QAM jellel modulálható. Az OFDM-et gyakran DMT-nek (*discrete multitone modulation* = diszkrét sokhangú moduláció) is nevezik.



4. ábra OFDM spektrumképe

Előnyös tulajdonságai:

- Egyenletesen használja ki a rendelkezésre álló sávszélességet.
- Átlapoltság megengedett, ezáltal ugyanakkora sávszélességben egyetlen modulált vivőhöz képest dupla mennyiségű adat vihető át OFDM-el.
- Időnként ismert szimbólumot átvíve felmérhetjük a csatorna pillanatnyi torzítását, adaptív algoritmusokkal korrigálhatunk. Ez többutas terjedés és ionoszférán keresztüli átvitelnél nagyon fontos.
- DSP-technika egyre olcsóbb. Fourier transzformáció mára már alapvető algoritmus.

5 A hálózat kiépítéséhez felhasznált aktív eszközök

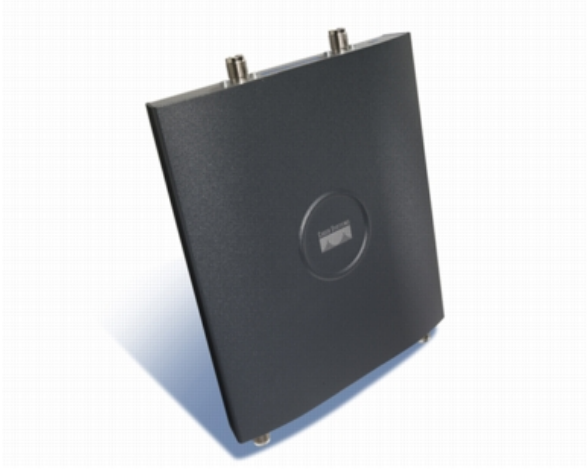
5.1 Megrendelő által támasztott követelmények

A Mondi Bags Hungária Kft. nyíregyházi telephelyén a jelenleg működő vezetékes hálózathoz kell csatlakoztatni a kiépítendő vezeték nélküli hálózatot. A szerverszoba az üzemcsarnok északi oldalának a nyugati harmadában helyezkedik el. A vezetékes hálózatot ellátó központi Rack szekrény a szerverszobában található. Jelenleg 3 db Cisco switch látja el a számítógépeket. Ezek a switch-ek 1 Gb/s-os linkekkel vannak egymással láncba kötve. Az üzemcsarnok és a készáru raktár lefedettségét biztosító access-pointok számára még van elegendő szabad port a meglévő switcheken és az access-pointokat el lehet úgy helyezni, hogy azok a 100 méteres 100 Mb/s csavart érpáras ethernet határon belül helyezkedjenek el.

Az alapanyagraktárba és a feldolgozó csarnok keleti részébe telepítendő access-pointok hálózatba kötéséhez egy új Rack szekrényt kell beépíteni az üzemcsarnok északi falának keleti harmadába, mivel nagyjából itt lesz a vezeték nélküli hálózat közepe. Ebbe a Rack szekrénybe kerül beépítésre 1 db Cisco WS-C2960G-24T CL switch, ami optikai 1 Gb/s linken csatlakozik a szerverszobában lévő központi switch –ekhez. Ebben a Rack-ben helyezik el az ide csatlakozó access-pointok POE tápforrásait is.

5.2 Vezeték nélküli hálózat kialakításához szükséges eszközök

A vezeték nélküli hálózatot 10 db Cisco AIR-AP1242AG-E-K9 típusú hozzáférési pont (AP) felhasználásával alakítjuk ki.



5. ábra Cisco AIR-AP1242AG-E-K9

A hozzáférési pontok mindegyikére 2 db Cisco AIR-ANT 4941 antennát szerelek fel a biztonságos lefedettség elérésének érdekében.

6. ábra Cisco AIR-ANT 4941

Az üzemcsarnokban kialakított Rack szekrénybe kerül 1 db Cisco Catalyst 2960G -24TC-L switch.

7. ábra Cisco Catalyst 2960G-24TC-L

Az access-pointok tápfeszültség ellátása Cisco AIR-PWRINJ3 power injectorok segítségével történik távolról a Rack szekrényekből POE technológiát felhasználva.

8. ábra Cisco AIR-PWRINJ3

A Wi-fi hálózathoz a felhasználók 11 db Symbol MC9090-GJ0HBEGA2WR típusú kézi, vonalkód olvasóval ellátott adatgyűjtő számítógéppel fognak csatlakozni.

9. ábra Symbol MC9090-G Scanner

Symbol MC9090- GJ0HBEGA2WR paraméterei röviden:

Wireless Gun Terminal: 802.11a/b/g, Extended Range Laser (Lorax), Color, 64MB, 53 key, Windows CE 5.0, Bluetooth. RoHS.

6 Wireless roaming

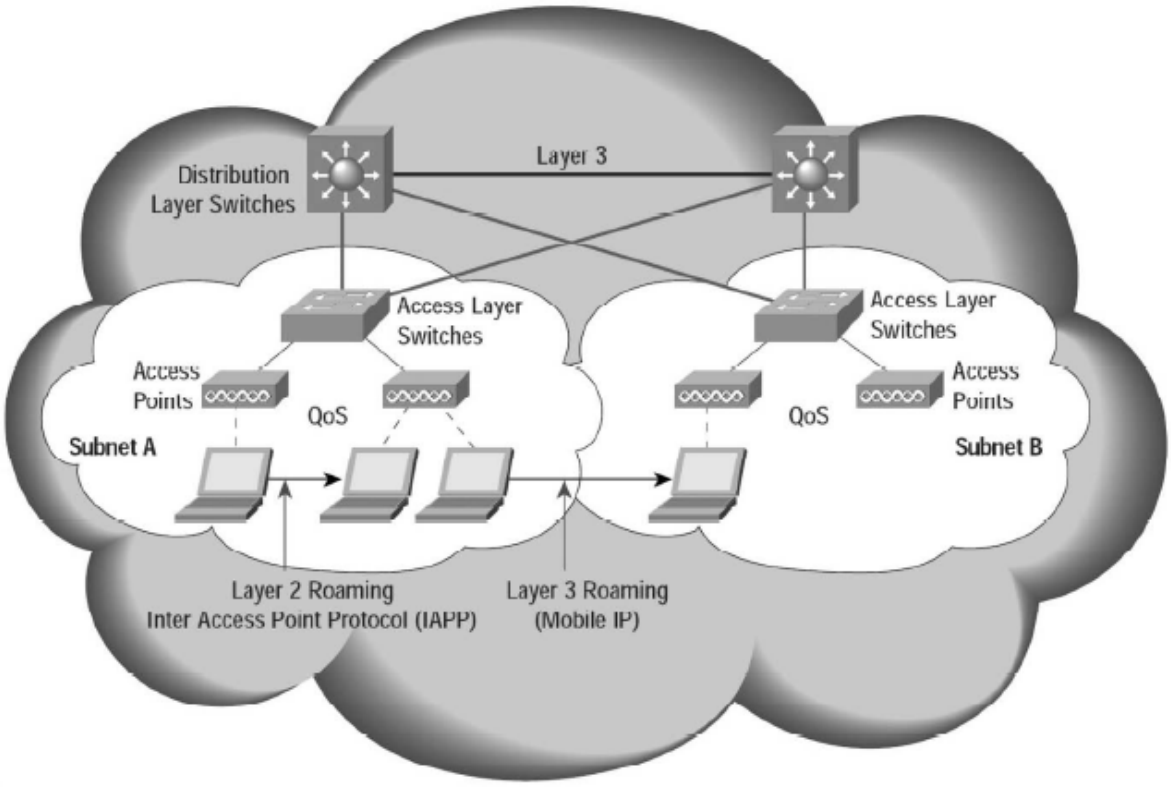
6.1 Wireless kliens folyamatos hálózati kapcsolata

A Megrendelő által behatárolt területek vezeték nélküli hálózattal történő lefedéséhez 10 db Access Pointot kell telepíteni. Ennyivel biztosítható a hálózat üzemszerű működése. Azonban elengedhetetlen a kliensek mozgása – sőt a kliensek mozgásán van a fő hangsúly – a megadott területen. Emiatt az AP –k között roamingolniuk kell a klienseknek.

6.2 Roaming mechanizmusok

A vezeték nélküli LAN-ok lehetővé teszik, hogy a csomópontok a vállalati hálózathoz virtuálisan kapcsolódjanak. A cellaváltás (roaming) olyan időben lejátszódó folyamat, amely során a mobil terminál egyik kiszolgáló AP-bázisállomástól egy másik AP-ra csatlakozik rá.

Adatkapcsolati (L2) roamingról beszélünk, ha a folyamat azonos alhálózatba tartozó AP-k között történik.



10. ábra L2 és L3 roaming

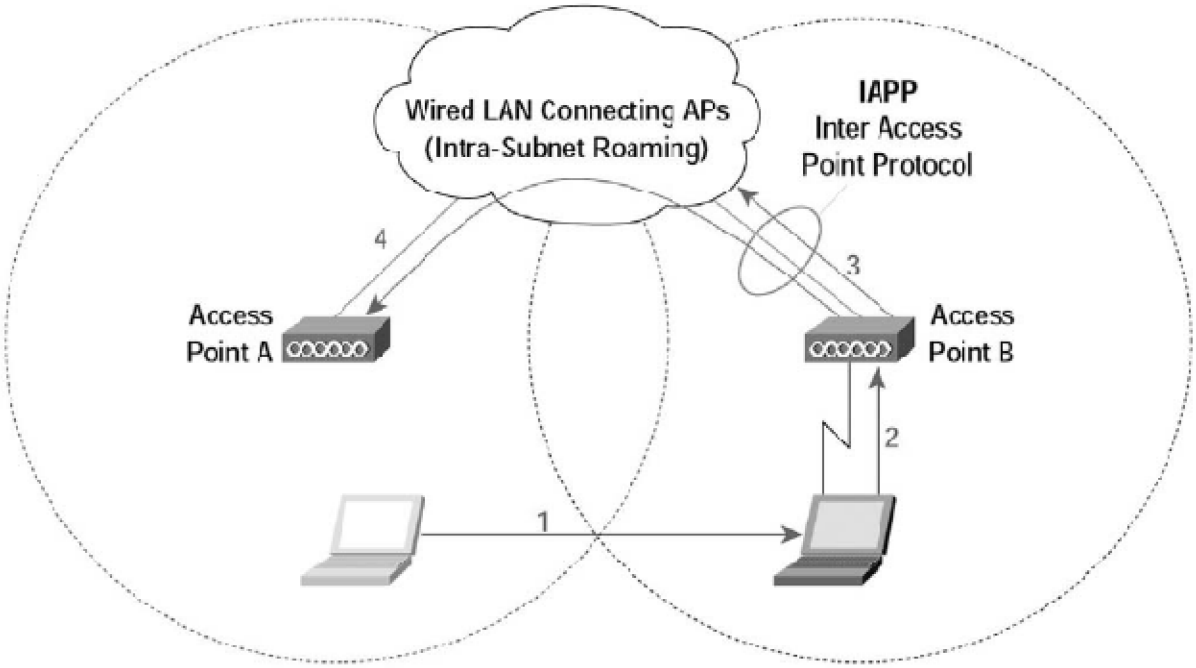
Ha a terminál másik alhálózatba tartozó új AP-hoz csatlakozik, akkor hálózati (L3) roamingról beszélünk. Hálózati cellaváltás az adatkapcsolati roaming sikeres lezajlása után következhet be. A cellaváltás mindig a terminál döntésén alapul, amelynek feladata a lehetséges bázisállomások felderítése, az ezekhez tartozó paraméterek értékelése, majd a lehetséges cellák közül az új kiválasztásának eldöntése. Az adatkapcsolati cellaváltás az alábbi fázisokat foglalja magába:

1) A terminál az „A” cellából elmozdul a „B” cellába. A bázisállomások ugyanabban az alhálózatban vannak, így L2 roamingról beszélünk. Ahogy a terminál kilép az „A” cellából, az AP „A” bázisállomással fennálló kapcsolat paraméterei közül valamelyik átlépi a megadott küszöbértéket, s ez kiváltja a roaming folyamat indítását.

2) A kliens végigelemzi az összes IEEE 802.11-es csatornát, lehetséges bázisállomást keresve. Megtalálja az AP „B”-t, lezajlik a fizikai rádiós csatornán a hitelesítés és az asszociáció folyamata.

3) Az AP „B” a kliens alhálózatába egy nulla tartalmú multicast üzenetet küld, amelynek forrás fizikai címe éppen a mobil terminál címével egyezik meg. Ez alapján a huzalos LAN hálózatban található switch-ek frissítik kapcsolási táblájukat. Így a terminálnak címzett Ethernet keretek ezután nem az AP „A”, hanem az AP „B” bázisállomáshoz kerülnek.

4) Az AP „B” a saját forrás MAC címével küld egy multicast üzenetet, amelyben értesíti az alhálózat összes bázisállomását arról, hogy az adott MAC című terminál hozzá asszociált. Ahogy az AP „A” ezt megkapja, törli a mobil terminál MAC címét az asszociációs táblájából.



11. ábra L2 roaming lépései

A roaming folyamatot mindig a kliens kezdeményezi, de a folyamatra vonatkozóan még nem létezik IEEE szabvány. A Cisco gyártmányú terminálok esetében az alábbi események váltják ki a roaming folyamat indítását:

a) Maximális csomagküldés próbálkozási szám átlépése.

Ha a kliens a maximum data retry-ként megadott számú próbálkozás után sem tudja a csomagot elküldeni, elindítja a roaming folyamatot. A Cisco Aironet kliensben ez az érték alapértelmezés szerint 16, és az Aironet Client Utilityben állítható.

b) Túl sok „bacon” kihagyása.

Minden, bázisállomáshoz társított kliensgép periodikusan kap „bacon” keretet. Alapértelmezésben 100 milliszekundumonként küld „bacon”-t a bázisállomás. Ez a periódus egyben konfigurációs paraméter is. A terminál a „bacon”-ben található érték alapján megtanulja annak periódusát. Amennyiben a terminál nyolc periódus ideig nem kap „bacon”-t, kezdetét veszi a roaming folyamat. A beérkező „bacon”-ök folyamatos figyelésével – még egy „idle” állapotban levő kliens is – képes érzékelni a vezeték nélküli kapcsolat minőségének romlását, majd pedig roamingot kezdeményezni.

c) Átviteli ráta váltása.

Normál esetben a rádiós keretek átvitele a bázisállomás alapértelmezett adatátviteli sebességével történik. Ez a ráta a legmagasabb átviteli sebesség, amelyet „required” vagy „enable” paraméterként lehet az AP-n beállítani. Minden olyan alkalommal, amikor egy csomagot alacsonyabb sebességgel kell újraküldeni, a „retransmit” számláló hárommal növekszik. Minden olyan csomag esetében, amikor az alapértelmezett átviteli sebességgel sikerült a továbbítás, ez a számláló eggyel csökken egészen addig, míg a nulla értéket el nem éri. Amennyiben a számláló eléri a 12-es felső határt, az alábbi események valamelyike következik be:

– Ha a kliens nem hajtott végre cellaváltást az elmúlt 30 másodpercben, akkor bekövetkezik a gyors cellaváltás (fast roaming).

– Ha az említett időn belül roaming-ot hajtott vége, akkor eggyel alacsonyabb fokozatra csökkenti az átviteli rátát. Az alapértelmezett átvitelnél alacsonyabb rátájú sikeres átvitel esetén, egy rövid idő elteltével ismét visszaugrik az eggyel magasabb sebességű üzemmódba.

d) Periódikus kliens intervallum (opcionális).

A Cisco Aironet v6.1-től kezdve konfigurálni lehet, hogy a mobil terminál milyen gyakorisággal, illetve milyen jelerősség mellett keressen jobb vételi minőségű bázisállomást. Ezekkel a beállításokkal a terminál egy jobb térerejű bázisállomást fog keresni feltéve, hogy az alábbi feltételek mindegyike teljesül:

– A terminál már legalább 20 másodperce asszociált az aktuális AP-hoz. Ez a feltétel megakadályozza, hogy a kliens túl gyorsan kapcsoljon a bázisállomások között. Érvényes értékek 5-255 másodperc.

– A térerősség 50%-nál gyengébb. Érvényes intervallum: 0-75%-ig.

e) Kliens inicializáció.

A terminál bekapcsolásakor és újraindításakor lezajló folyamat. A roaming folyamathoz új bázisállomás keresése szükséges. Ennek érdekében a terminál a rádiós csatornákon scan technika segítségével meghatározza az elérhető bázisállomások listáját, amelyből a legjobbat választja ki. A scan technika csatornánként egy-egy „probe” teszt üzenet küldését jelenti, amire „probe” válasz vagy „bacon” érkezik a csatornán üzemelő bázisállomástól.

Az AP-tól érkező „bacon”-öket csak akkor veszi figyelembe a kliens, ha az SSID és a titkosítási beállítások megegyeznek. A keresés befejezése után a listából kiválaszt egy bázisállomást, hogy az elérési paramétereit összehasonlítsa a lista többi tagjával. Ha a terminál kezdeti „start-up” fázisban van, akkor az új AP a listában elsőként szereplő tag lesz; ha a terminál roaming fázisban van, akkor az új AP a korábbi marad amennyiben válaszolt a teszt „probe” keretekre. Válasz hiánya esetén a lista első tagja lesz az új AP. Az aktuális AP a lista többi elemével összehasonlításra kerül. Ahhoz, hogy egy tag új AP lehessen, minden listabeli AP-nak az alábbi szempontokat kell teljesítenie:

- A potenciális cél AP jelerőssége legalább 20%. Ha a térerő több mint 20%-kal gyengébb, mint az aktuális AP térereje, akkor legalább 50% jelerősséggel kell rendelkezzen.
- Ha a potenciális cél AP repeater módban van, és több rádió hop-ra van a gerinchálózattól, mint az aktuális AP, akkor 20%-kal nagyobb jelerőssége kell, hogy legyen, mint a jelenlegi AP-nak.
- A potenciális cél AP-nál a küldő egység terheltsége maximum 10%-kal lehet nagyobb, mint a jelenlegi AP esetén.

A terminál a felsorolt alapkritériumoknak megfelelő bázisállomásokat összehasonlítja a jelenlegi bázisállomással. Ha egy elfogadott AP teljesít egyet az alábbi feltételek közül, akkor azt a terminál új, aktuális AP-nak választja, majd a lista többi AP-ját már ehhez az újonnan választott AP-hoz hasonlítja a továbbiakban:

- a jelerősség 20%-kal nagyobb, mint az aktuális bázisállomásé;
- kevesebb hop távolság a gerinchez;
- legalább néggyel kevesebb a kapcsolódott kliensek száma, mint a jelenlegi AP esetén;
- legalább 20%-kal kisebb a küldő egység terheltsége.

A 12.2.(11)JA IOS verziótól kezdődően a Cisco „fast secure roaming” implementáció két újabb lehetőséggel bővült: egyrészt növelt hatékonyságú a 802.11-es csatornakeresés a fizikai roaming alatt, másrészt hatékonyabb újra hitelesítési mechanizmus jelenik meg, amely fejlett titkosító kulcs menedzsmentet alkalmaz. Függetlenül az alkalmazott biztonsági módszertől, a hatékonyabb csatornakeresés gyorsabb L2 roaming-ot tesz lehetővé.

Az újrahitelesítés hatékonyságát növelő kulcs menedzsment felgyorsítja a Cisco LEAP hitelesítési folyamatot, így a roaming rövid idő alatt és biztonságosan zajlik le. A Cisco terminálokon és bázisállomásokon az IEEE 802.11 csatornakeresés alapértelmezés szerint egyaránt engedélyezett.

A „fast secure roaming”-ot egy csatornakeresés előzi meg. A 12.2(11)JA előtti IOS verziók esetén a kliensnek 37 ms-ot vett igénybe egy rádiócsatorna ellenőrzése, ami a magyar szabványok szerinti 13 csatorna esetén összességében 481 ms-ot jelent. A kliens minden egyes csatorna esetén az alábbi lépéseket hajtja végre:

Miután a terminál rádiós hardvere ráhangolódik az adott WLAN csatornára, figyel, hogy elkerülje az ütközést, majd „probe” keretet küld és várja a „probe response” vagy a „bacon” jelzést. A fast secure roaming esetén hatékonyabb a csatornakeresés: az újrahitelesített kliens informálja az új AP-t a korábbi AP-val való kapcsolat elvesztése óta eltelt időről, a csatornaszámról, és az SSID-ről.

Ezeket az információkat felhasználva, az új AP felépít egy listát a szomszédos bázisállomásokról, és az általuk használt rádiócsatornákról. Ha a szomszédos AP-król információt szolgáltató mobil terminál több mint 10 másodperce kapcsolódott le az előző AP-ról, akkor az általa küldött információkat nem veszi figyelembe az új AP.

A bázisállomások maximum 30 szomszédos AP-ról tárolnak információt. Ez a lista egy egynapos periódus alatt elévül. Amikor a terminál asszociál egy AP-hoz, az új bázisállomás unicast csomagban visszaküldi számára a szomszédos AP-k listáját. Ha a kliensnek roamingot kell végrehajtania, megvizsgálja az aktuális AP-tól kapott listát, és csak azokat a rádiócsatornákat ellenőrzi, melyeket a szomszédos bázisállomások valamelyike használ.
A kliensállomás az elfoglaltságától függően az alábbi három roaming típus egyikét alkalmazza:

– Normal roam:

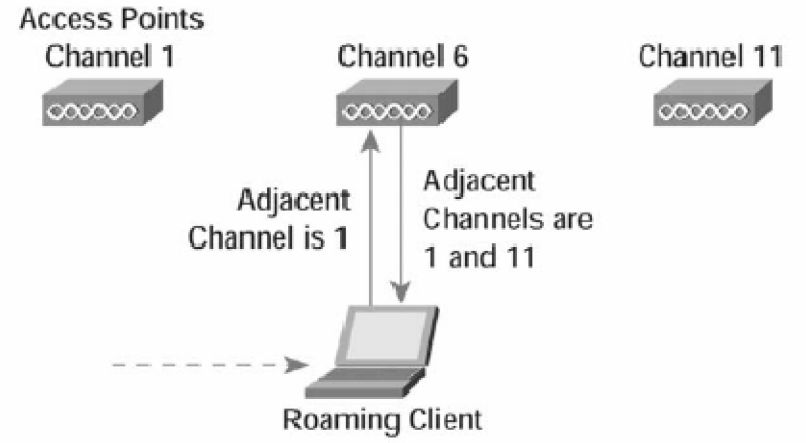
A kliens nem kapott és nem küldött unicast csomagot az elmúlt 500 ms-ban. Nem használja az AP-tól kapott listát, ellenőrzi az adott térségben érvényes összes 802.11-es csatornát.

– Fast roam:

A kliens kapott vagy küldött unicast csomagot az elmúlt 500 ms-ban. A szomszédos AP-k által használt csatornákat ellenőrzi. Ha nem talál új AP-t a lista alapján, átvizsgálja az összes csatornát. A kliens 75 ms-ra korlátozza a keresési idejét, ha legalább egy jobb AP-t tudott találni.

– Very fast roam:

A kliens kapott vagy küldött unicast csomagot az elmúlt 500 ms-ban, és nullánál nagyobb százalékkal növeli az adott cella terheltségét. A többi esemény a „fast roaming”-gal megegyező kivéve, hogy jobb bázisállomás találata esetén a keresés azonnal befejeződik.



12. ábra A Fast roaming csatornakeresése

6.3 Roaming helyi implementációja

A megrendelő meglévő számítógépes hálózata egy alhálózatot tartalmaz, vagyis minden csomópont ugyanabban a hálózatban található.

Az alhálózat adatai:

Network Address: 10.74.0.0

Netmask: 255.255.0.0

Default Gateway: 10.74.100.1

Ebből az következik, hogy az AP-k szintén ebbe az alhálózatba kerülnek. Mivel ebben a hálózatban minden aktív eszköz Cisco, így a mobil kliensek roaming-ját meg lehet oldani Layer 2 –es szinten.

Az AP-k IP címei: 10.74.6.1 –től 10.74.6.11 –ig.

A roaming működésének alapvető feltétele az AP –k megfelelő csatornakiosztása.

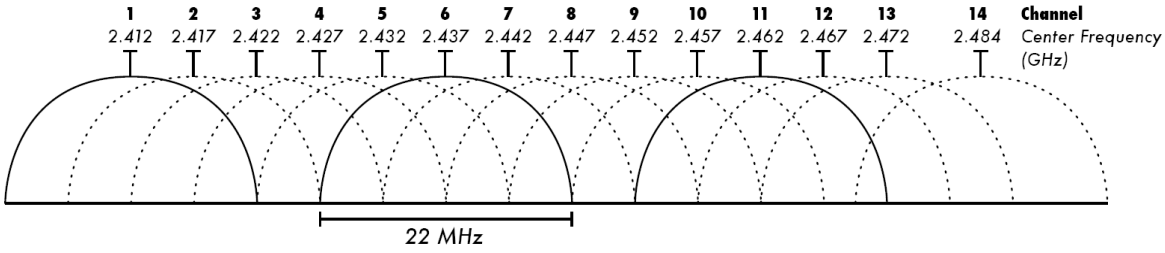
7 Wifi RF csatornák

7.1 RF csatorna kiosztás 2.4 GHz-en

A 2,4 GHz-en történő adatátvitel az alábbi frekvenciájú csatornákon történhet:

Csatorna száma	Frekvencia MHz	Csatorna száma	Frekvencia MHz
1.	2412	8.	2447
2.	2417	9.	2452
3.	2422	10.	2457
4.	2427	11.	2462
5.	2432	12.	2467
6.	2437	13.	2472

A 13-as ábrán jól látható, hogy az egyes csatornák 22 MHz szélességűek, és emiatt a csatornák között átfedés van.



13. ábra Wifi RF csatornák kiosztása

A 2.4 GHz-es sávot kijelölték ipari, tudományos és orvosi eszközök működtetésére. Az ipari használat jellegzetes példája az a nagyszámú háztartási mikrohullámú sütő, ami a 2,4 GHz-es sávban működik. Az ipari berendezések mikrohullámú zavarkisugárzása a sávhasználat alapvető meghatározója.

A 2,4 GHz-es sávot kijelölték továbbá kis hatótávolságú eszközök (távirányítók, riasztók, stb.) működtetésére is. Ezek az eszközök tovább növelik a nem ellenőrizhető zavarszintet.

Ebben a kisugárzásokkal erősen terhelt frekvenciasávban megengedett a kis hatótávolságú rádiótávközlés is. Tudatában kell azonban lenni annak, hogy a távközlő eszközök működtetése során mindig lehet zavaró interferenciára számítani.

A távközlési sávhasználat prioritási foka harmadlagos. Ez azt jelenti, hogy a berendezések nem tarthatnak igényt interferencia- védelemre más eszközök zavarásával szemben.

A 2,4 GHz-es távközlés az egyszerűség és könnyű megvalósíthatóság miatt népszerű. Az elterjedt használat és az állomások nagy száma következtében mostanra már a 2,4 GHz-es távközlési összeköttetések kölcsönös egymásra hatása vált a zavarok elsődleges okozójává.

7.2 A 2,4 GHz-es sáv távközlési használata

A sávhasználatot meghatározó műszaki szabályozás csak a kötelezően betartandó teljesítményszinteket limitálja, az alkalmazott technológiára nem tesz megkötést, tehát technológia-semleges. Az előírások betartása mellett bármilyen rádió-távközlési átviteli alkalmazás megvalósítható. A teljesítmény-korlátozási előírásból adódóan a 2,4 GHz-es távközlési alkalmazások általában 150 m-nél kisebb távolságú átvitelre használhatók előnyösen. Jellegzetes alkalmazások:

– Bluetooth, általában 10 m-nél kisebb távolságra;

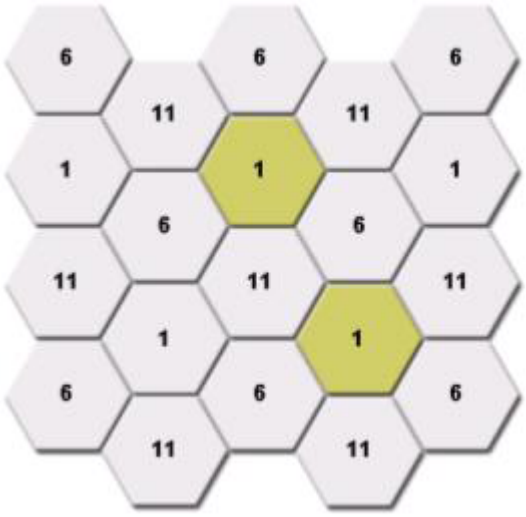
– HomeRF, általában 50 m-nél kisebb távolságra;

– WiFi, az RLAN egy jellegzetes megoldása, amelyik az IEEE 802.11 szabvány előírásainak tesz eleget, általában 150 m-nél kisebb távolságra.

A 2,4 GHz-es RLAN-ok előnyösen épületeken belüli hozzáférési rendszerekhez használható. Külső téri RLAN (azaz ORLAN) nincs ugyan tiltva, de műszakilag rendkívül előnytelen ebben a frekvenciasávban (a CEPT deklarációja szerint nem rendeltetésszerű rádióhasználatnak minősíthető).

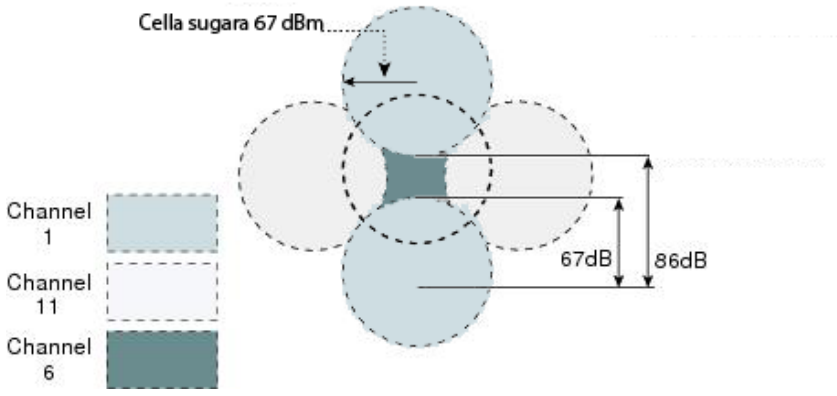
7.3 Területek lefedése WiFi cellákkal

Mint ahogyan azt már fentebb részleteztem az RF csatornák között átfedés van. Emiatt célszerű olyan RF csatornákat választani a cellák kialakításához, amelyek frekvenciasávjai biztonságos távolságra vannak egymástól. Egy lehetséges megoldás a 14 –es ábra szerint 1, 6, 11 –es csatornák felhasználásával.



14. ábra WiFi cellák kialakítása

A cellák kialakításánál az alábbi kritériumokat kell figyelembe venni:



15. ábra Cellák kialakításának kritériumai

Egy cella lefedettségének maximális sugara 67 dBm.

Két azonos csatornájú cella közötti minimális távolság 19 dBm, vagyis egy AP-tól minimum 86 dBm-re lehet egy vele azonos RF csatornán lévő AP által lefedett cella széle.

Az imént részletezett csatornakiosztás szerinti lefedés egy „abszolút” túlbiztosított kialakítás, mivel a rádiós csatornák átfedés-mentesen helyezkednek el. Minden kiosztott csatorna (1, 6, 11) között 5.5 MHz üres sáv marad.

Az elérhető átviteli teljesítmény szintek:
802.11g CCK:

• 20 dBm (100 mW)

• 17 dBm (50 mW)

• 14 dBm (25 mW)

• 11 dBm (12 mW)

• 8 dBm (6 mW)

• 5 dBm (3 mW)

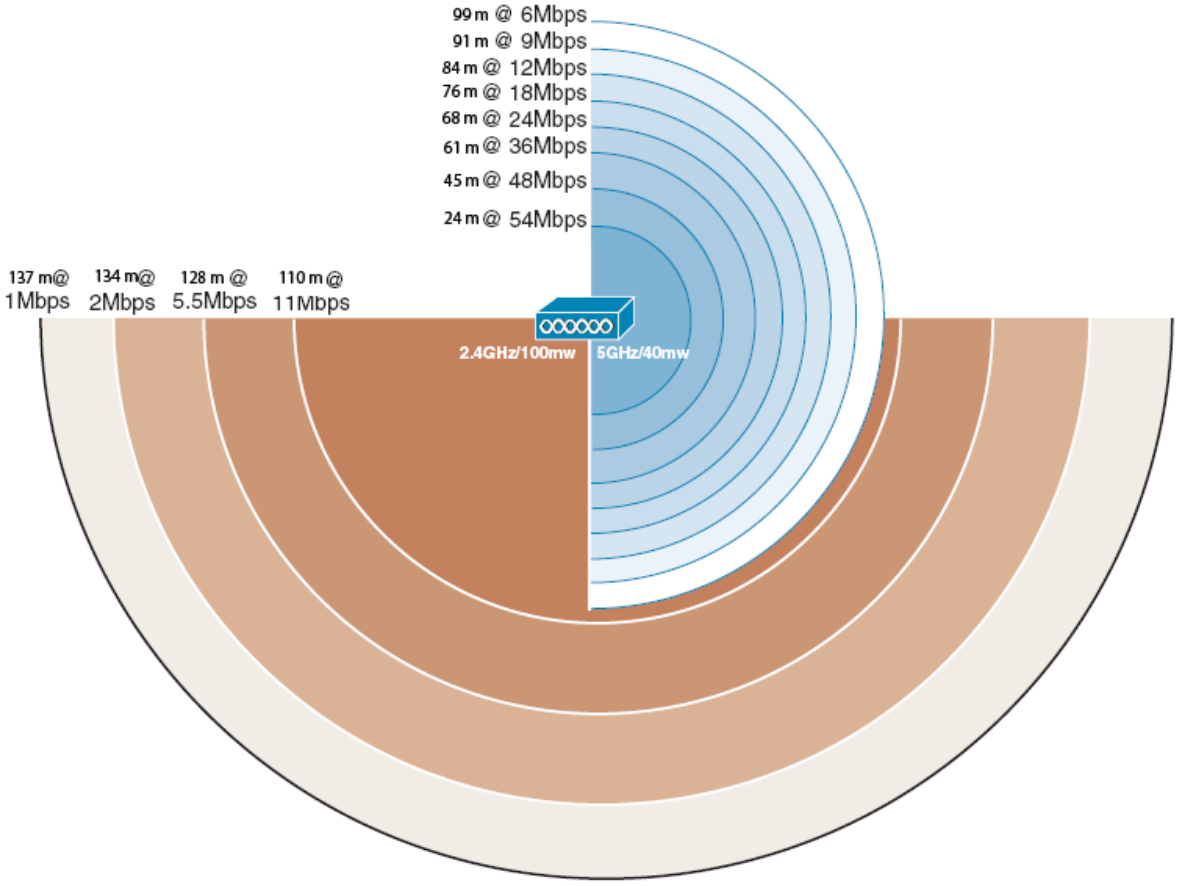
• 2 dBm (2 mW)

• 1 dBm (1 mW)

A Cisco AIR-AP1242AG-E-K9 készülékek IOS-a a fent felsorolt teljesítmény szintek beállítását teszi lehetővé. Továbbá beállítható az is, hogy a két antenna csatlakozó közül melyikre, vagy mindkettőre szerelünk-e antennát. A felszerelt antenna külső, nagyobb nyereséget biztosító irányított antenna-e, ami kábellel csatlakozik, esetleg közvetlenül csatlakozó körsugárzó botantenna.

A mi esetünkben a közvetlenül csatlakozó körsugárzó botantennát használjuk. Ennek megfelelően programozom az AP-ket.

7.4 Sávszélesség változása a távolság függvényében



16. ábra Adatátviteli sebesség a távolság függvényében

Az ábrán látható adatátviteli sebesség értékek számításánál feltételeztük, hogy az eszközök beltérben vannak beüzemelve, továbbá standard antennával van ellátva a hálózati csatoló kártya és az Access-Point. A sávszélesség értékeket nagyban befolyásolja a fizikai környezet. Ezek a számított értékek azt feltételezik, hogy semmilyen árnyékoló tényező nincs jelen. Ha tehát a lefedett területen falak, vagy egyéb (főleg fémes) nagy kiterjedésű tárgyak helyezkednek el, azok nagymértékben lecsökkentik a besugározható terület mértékét.

Mivel a megrendelő olyan környezetbe igényelte a vezeték nélküli hálózat kialakítását, ahol nagyméretű papírtekercsek vannak jelen, indokolt az AP-k viszonylag sűrű telepítése.

7.5 Területi lefedettség helyi implementációja

A Megrendelő telephelyén olyan csatornakiosztást alkalmazunk, ahol a kiosztott csatornák között nincs üres rádiófrekvenciás sáv. Így 4 RF csatornát lehet felhasználni a hálózat kialakításához: 1, 5, 9, 13. Négy csatornára azért van szükség, mert viszonylag kis földrajzi területen kell elhelyezni az Access-Point –okat:

1 – es csatorna: 2412 MHz (2402-2422)

5 – ös csatorna: 2432 MHz (2422-2442)

9 – es csatorna: 2452 MHz (2442-2462)

13 – as csatorna: 2472 MHz (2462-2482)

Jól látható, hogy ebben az esetben sincs rádiófrekvenciás átfedés a csatornák között, csak szabad frekvenciasáv sem marad közöttük.

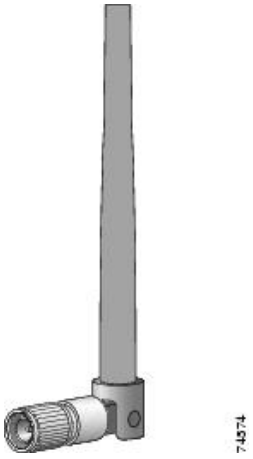
Az Access-Point–okat úgy kell elhelyezni a megadott területen, hogy minél kisebb olyan hely legyen a raktárban, ahol a lefedettségben átfedés lehet (azonos csatornákra állított AP –k esetében).

A stabil rádiós működés elérésének érdekében minden Access-Point–ra 2 db antennát szerelek fel.

Az Access-Point–ok felszerelése, programozása után 1 db hordozható számítógéppel, NetStumbler – 0.4.0 szoftver segítségével feltérképezem a fizikai terület lefedettségét. Pontos méréseket végzek minden hozzáférési pont rádiós lefedettségi adatairól és e mérések után pontosan beállítom az AP-k teljesítményeit. Gondosan ügyelve arra, hogy azonos rádiós csatornán üzemelő hozzáférési pontok által lefedett területek között ne legyen átfedés.

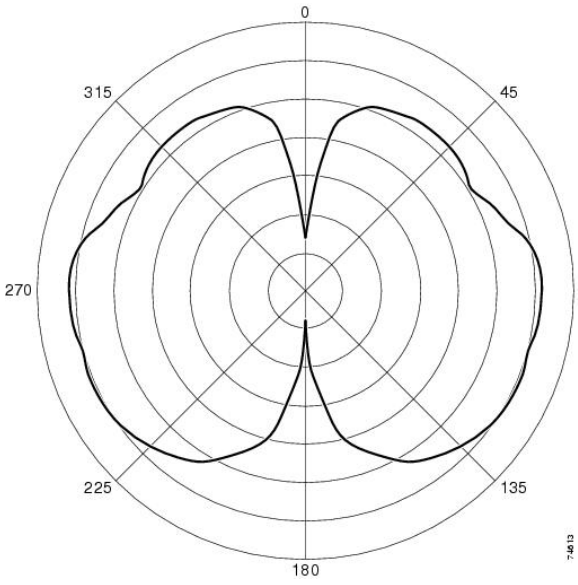
Az antennák paraméterei:

Antenna type	Dipole
Operating frequency range	2402-2495 MHz
Nominal input impedance	50 Ω
2:1 VSWR bandwidth	2385 - 2515 Mhz
Peak gain	2 dBi
Polarization	Linear, vertical
E-Plane 3-dB beamwidth	70 degrees
H-Plane 3-dB beamwidth	Omnidirectional
Dimensions	5.5 in. (13 cm)
Weight	1 oz.
Connector type	RP-TNC plug
Environment	Indoor
Operating temperature range	(0°C to 60°C)

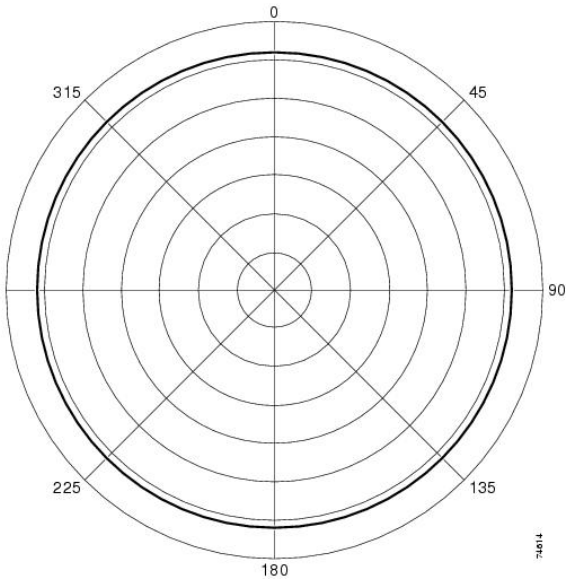


Karakterisztikájuk:

Vertikális karakterisztika



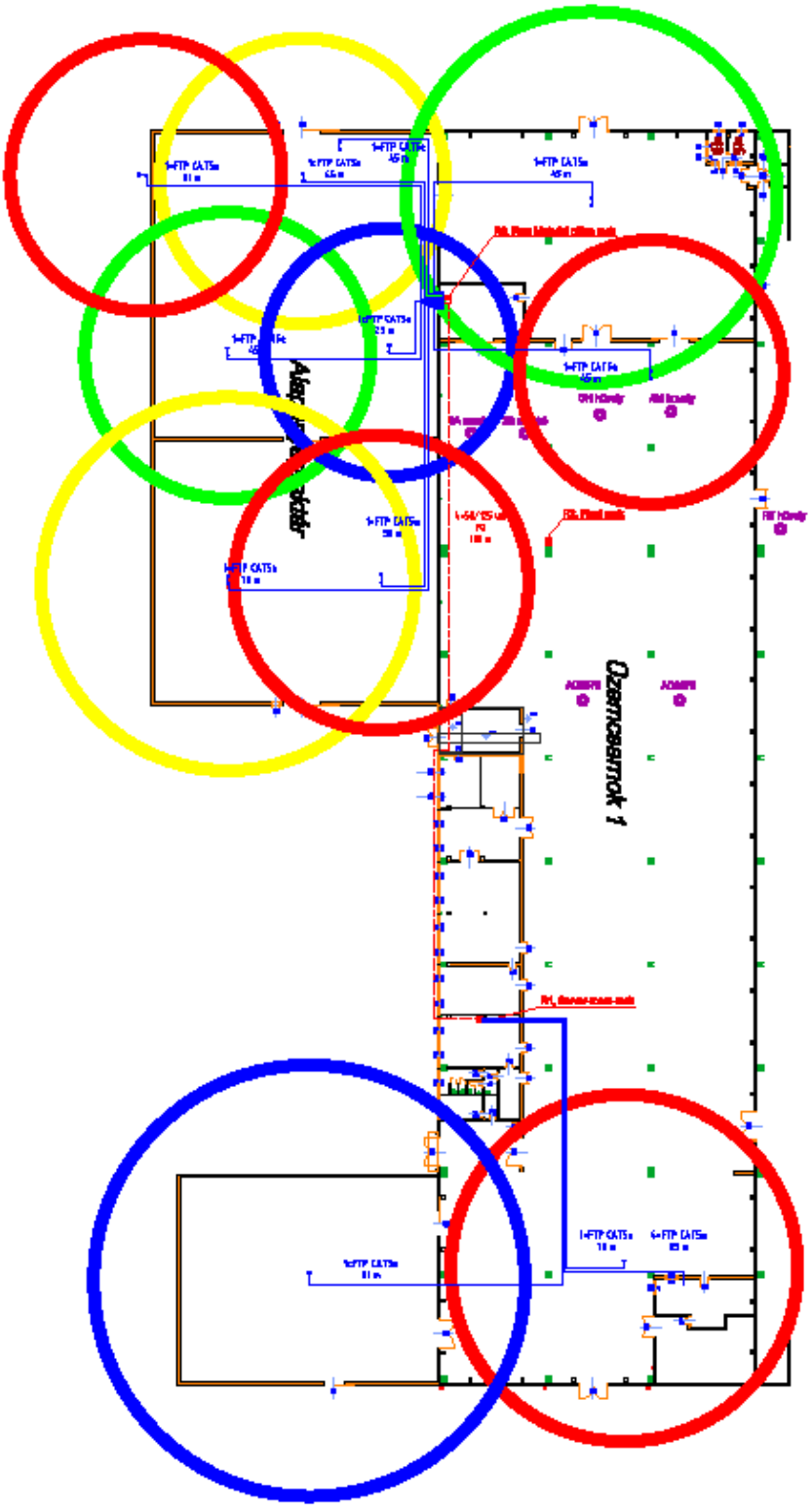
Horizontális karakterisztika



A két antennát az AP-n úgy állítjuk be, hogy egymással 90^{o} –os szöget zárjanak be. Ezzel azt segítjük elő, hogy minél kevésbé zavarják egymás működését.

17. ábra A raktárban tárolt papírtekercsek

7.6 AP-k elhelyezése



18. ábra WLAN lefedettség

7.7 A rádiófrekvenciás csatornák kiosztása

A 18 –as ábrán az AP-k fizikai elhelyezése és a hozzájuk tartozó RF csatornák láthatóak:

- 1 – es csatorna
- 5 – ös csatorna
- 9 – es csatorna
- 13 – as csatorna

Az Access-Point –ok beállításánál különös gondot kell fordítani azok teljesítményének beállítására. A 16 –os ábrán jól látható, hogy egy rádiós hozzáférési pont ideális esetben mekkora sugarú kört tud lefedni. Mivel a mi esetünkben nem beszélhetünk ideális esetről, ezért a rendszer beállítását lehetőleg olyan időpontban kell végezni, amikor a raktárban jelentős mennyiségű papírtekercs található. Vigyázni kell azonban arra is, hogy az így beállított rádiós teljesítmény nehogy túl nagy legyen olyankor, amikor a raktár üres. Emiatt az Access-Point –ok teljesítményét a rendszer beállítása után többször ellenőrizni kell.

19. ábra Alapanyagraktár

8 A hálózattal szemben támasztott biztonsági kritériumok

8.1 A vezeték nélküli hálózatok biztonságáról általában (történelmi áttekintés)

Először a WEP működéséről és hibáiról néhány mondat.

A WEP az első biztonsági architektúra, melyet 802.11 hálózatok számára javasoltak, ám hamar kiderült, hogy nem nyújt megfelelő védelmet. Utána a 802.11i szabvány következett, amely a WEP utódjának tekinthető. Áttekintjük a 802.11i-ben javasolt biztonsági architektúra elemeit: a hitelesítési és hozzáférés-védelmi mechanizmust, a kulcsmenedzsmentet, valamint a TKIP és az AES-CCMP protokollokat.

8.1.1 WEP

Az IEEE 802.11 vezeték nélküli LAN szabvány tervezői kezdettől fogva fontosnak tartották a biztonságot. Ezért már a 802.11 korai verziója [802.11] is tartalmazott biztonsági mechanizmusokat, melyek összességét WEP-nek (Wired Equivalent Privacy) nevezték el. Ahogy arra a név is utal, a WEP célja az, hogy a vezeték nélküli hálózatot legalább olyan biztonságossá tegye, mint egy – különösebb biztonsági kiegészítésekkel nem rendelkező – vezetékes hálózat. Ha például egy támadó egy vezetékes Ethernet hálózathoz szeretne csatlakozni, akkor hozzá kell férnie az Ethernet hub-hoz. Mivel azonban a hálózati eszközök általában fizikailag védve, zárt szobában találhatók, ezért a támadó nehézségekbe ütközik. Ezzel szemben egy védelmi mechanizmusokat nélkülöző vezeték nélküli LAN-hoz való hozzáférés – a rádiós csatorna nyitottsága miatt – triviális feladat a támadó számára. A WEP ezt a triviális feladatot hivatott megnehezíteni. Fontos azonban megjegyezni, hogy a WEP tervezői nem törekedtek „tökéletes” biztonságra, mint ahogy a zárt szoba sem jelent tökéletes védelmet egy Ethernet hub számára. A tervezők tehát nem tették túl magasra a lécet, ám a WEP még ezt a korlátozott célt sem érte el. Pár évvel a megjelenése után, a kriptográfusok és az IT biztonsági szakemberek súlyos biztonsági hibákat találtak a WEP-ben [Walker00, Borisov+01, Arbaugh+02], s nyilvánvalóvá vált, hogy a WEP nem nyújt megfelelő védelmet. A felfedezést tett követte, és hamarosan megjelentek az Interneten a WEP feltörését automatizáló programok. Válaszul, az IEEE új biztonsági architektúrát dolgozott ki, melyet a 802.11 szabvány i jelzésű kiegészítése tartalmaz [802.11i].

8.1.2 A WEP működése

Vezeték nélküli hálózatok esetében két alapvető biztonsági probléma merül fel. Egyrészt a rádiós csatorna jellege miatt a kommunikáció könnyen lehallgatható. Másrészt – s ez talán fontosabb – a hálózathoz való csatlakozás nem igényel fizikai hozzáférést a hálózati csatlakozóponthoz (Access Point), ezért bárki megpróbálhatja a hálózat szolgáltatásait illegálisan igénybe venni. A WEP az első problémát az üzenetek rejtjelezésével igyekszik megoldani, a második probléma megoldása érdekében pedig megköveteli a csatlakozni kívánó mobil eszköz (Station, vagy röviden STA) hitelesítését az AP felé. A hitelesítést egy egyszerű kihívás-válasz alapú protokoll végzi, mely négy üzenet cseréjéből áll. Elsőként a STA jelzi, hogy szeretné hitelesíteni magát (authenticate request). Válaszul az AP generál egy véletlen számot, s azt kihívásként elküldi a STA -nak (authenticate challenge). A STA rejtjelezi a kihívást, s az eredményt visszaküldi az AP-nak (authenticate response). A STA a rejtjelezést egy olyan titkos kulccsal végzi, melyet csak a STA és az AP ismer. Ezért ha az AP sikeresen dekódolja a választ (azaz a dekódolás eredményeként visszakapja saját kihívását), akkor elhiszi, hogy a választ az adott STA állította elő, hiszen csak az ismeri a helyes válasz generálásához szükséges titkos kulcsot. Más szavakkal, a válasz sikeres dekódolása esetén az AP hitelesítette a STA-t, és ennek megfelelően dönthet arról, hogy a csatlakozást engedélyezi vagy sem. A döntésről az AP a protokoll negyedik üzenetében tájékoztatja a STA-t (authenticate success vagy failure). Miután a hitelesítés megtörtént, a STA és az AP üzeneteiket rejtjelezve kommunikálnak. A rejtjelezéshez ugyanazt a titkos kulcsot használják, mint a hitelesítéshez. A WEP rejtjelező algoritmusa az RC4 kulcsfolyam kódoló.
A kulcsfolyam kódolók úgy működnek, hogy egy kisméretű, néhány bájtos titkos kulcsból egy hosszú ál véletlen bájtsorozatot állítanak elő, és ezen sorozat bájtjait XOR-olják az üzenet bájtjaihoz. Ez történik a WEP esetében is. Az M üzenet küldője (a STA vagy az AP) a titkos kulccsal inicializálja az RC4 kódolót, majd az RC4 által előállított K ál véletlen bájtsorozatot XOR-olja az üzenethez. Az $M \square K$ rejtjelezett üzenet vevője ugyanazt teszi, mint a küldő: a titkos kulccsal inicializálja az RC4 algoritmust, amely így ugyanazt a K ál véletlen bájtsorozatot állítja elő, amit a rejtjelezéshez használt a küldő. Ezt a rejtjelezett üzenethez XOR-olva – az XOR művelet tulajdonságai miatt – a vevő az eredeti üzenetet kapja vissza: $(M \square K) \square K = M$.

A fent leírtak majdnem megfelelnek a valóságnak, van azonban még valami, amit a WEP rejtjelezés kapcsán meg kell említeni. Könnyen látható, hogy ha a rejtjelezés a fentiek szerint működne, akkor minden üzenethez ugyanazt a *K* ál véletlen bájtsorozatot XOR-olnánk, hiszen a kódolót minden üzenet elküldése előtt ugyanazzal a titkos kulccsal inicializáljuk. Ez több szempontból is hiba lenne. Tegyük fel például, hogy egy támadó lehallgat két rejtjelezett üzenetet, $M_1 \square K$-t és $M_2 \square K$-t. A két rejtjelezett üzenetet XOR-olva, a támadó a két nyílt üzenet XOR összegét kapja: $(M_1 \square K) \square (M_2 \square K) = M_1 \square M_2$.

Ez olyan, mintha az egyik üzenetet a másik üzenettel, mint kulcsfolyammal rejtjeleztük volna. Ám ebben az esetben M_1 és M_2 nem ál véletlen bájtsorozatok. Valójában tehát $M_1 \square M_2$ egy nagyon gyenge rejtjelezés, és a támadó az üzenetek statisztikai tulajdonságait felhasználva könnyen meg tudja fejteni mindkét üzenetet. Az is elképzelhető, hogy a támadó esetleg (részlegesen) ismeri az egyik üzenet tartalmát, s annak segítségével a másik üzenet (részleges) tartalmához azonnal hozzájut.

Ezen problémák elkerülése érdekében, a WEP nem egyszerűen a titkos kulcsot használja a rejtjelezéshez, hanem azt kiegészíti egy IV-nek (Initialization Vector) nevezett értékkel, mely üzenetenként változik. A rejtjelezés folyamata tehát a következő: az IV-t és a titkos kulcsot összefűzzük, a kapott értékkel inicializáljuk az RC4 kódolót, mely előállítja az ál véletlen bájtsorozatot, amit az üzenethez XOR-olunk. A dekódolás folyamata ezzel analóg. Ebből következik, hogy a vevőnek szüksége van a kódolásnál használt IV-re. Ez a rejtjelezett üzenethez fűzve, nyíltan kerül átvitelre. Ez elvileg nem jelent problémát, mert az üzenet dekódolásához csupán az IV ismerete nem elegendő, ahhoz a titkos kulcsot is ismerni kell.
A méreteket illetően megemlítjük – s ennek később még lesz jelentősége – hogy az IV 24 bites, a titkos kulcs pedig (általában) 104 bites.

8.1.3 WEP hibái

Hitelesítés: A WEP hitelesítési eljárásának több problémája is van. Elsőként mindjárt az, hogy a hitelesítés egyirányú, azaz a STA hitelesíti magát az AP felé, ám az AP nem hitelesíti magát a STA felé. Másodszor, a hitelesítés és a rejtjelezés ugyanazzal a titkos kulccsal történik. Ez azért nem kívánatos, mert így a támadó mind a hitelesítési, mind pedig a rejtjelezési eljárás potenciális gyengeségeit kihasználhatja egy, a titkos kulcs megfejtésére irányuló támadásban. Biztonságosabb lenne, ha minden funkcióhoz külön kulcs tartozna.

A harmadik probléma az, hogy a protokoll csak a hálózathoz történő csatlakozás pillanatában hitelesíti a STA-t. Miután a hitelesítés megtörtént és a STA csatlakozott a hálózathoz, bárki küldhet a STA nevében üzeneteket annak MAC címét használva. Úgy tűnhet, hogy ez annyira nem nagy gond, hiszen a támadó, a titkos kulcs ismeretének hiányában, úgysem tud helyes rejtjelezett üzenetet fabrikálni, amit az AP elfogad. Ám ahogy azt korábban említettem, a gyakorlatban az összes STA egy közös titkos kulcsot használ, s így a támadó megteheti azt, hogy egy STA_1 által küldött – és a támadó által lehallgatott – rejtjelezett üzenetet STA_2 nevében megismétel az AP felé; ezt az AP el fogja fogadni.

A negyedik probléma egy gyöngyszem a protokolltervezési hibák között. A WEP rejtjelezési algoritmusa az RC4 folyamkódoló. Nemcsak az üzeneteket kódolják az RC4 segítségével, hanem a STA ezt használja a hitelesítés során is az AP által küldött kihívás rejtjelezésére. Így a támadó a hitelesítés során küldött üzenetek lehallgatásával könnyen hozzájut a C kihíváshoz és az arra adott $R = C \oplus K$ válaszhoz, melyből $C \oplus R = K$ alapján azonnal megkapja az RC4 algoritmus által generált K ál véletlen bájtsorozatot. A játéknak ezzel vége, hiszen K segítségével a támadó bármikor, bármilyen kihívásra helyes választ tud generálni a STA nevében (s ezen az IV használata sem segít, mert az IV-t a rejtjelezett üzenet küldője, jelen esetben a támadó választja). Sőt, mivel a gyakorlatban minden, az adott hálózathoz tartozó eszköz ugyanazt a titkos kulcsot használja, a támadó ezek után bármelyik eszköz nevében csatlakozni tud a hálózathoz. Persze a csatlakozás önmagában még nem elegendő, a támadó használni is szeretné a hálózatot. Ehhez olyan üzeneteket kell fabrikálnia, amit az AP elfogad. A rejtjelezés követelménye miatt ez nem triviális feladat (hiszen magához a titkos kulcshoz még nem jutott hozzá a támadó), de a WEP hibáinak tárháza bőven tartogat még lehetőségeket.

8.1.4 802.11i

A WEP hibáit felismerve, az IEEE új biztonsági megoldást dolgozott ki, melyet a 802.11i specifikáció tartalmaz [802.11i]. A WEP-től való megkülönböztetés érdekében, az új koncepciót RSN-nek (Robust Security Network) nevezték el. Az RSN-t körültekintőbben tervezték meg, mint a WEP-et. Új módszer került bevezetésre a hitelesítés és a hozzáférés-védelem biztosítására, mely a 802.1X szabvány által definiált modellre épül, az integritás-védelmet és a titkosítást pedig az AES (Advanced Encryption Standard) algoritmusra támaszkodva oldották meg.

Sajnos azonban az új RSN koncepcióra nem lehet egyik napról a másikra áttérni. Ennek az az oka, hogy a használatban levő WiFi eszközök az RC4 algoritmust támogató hardver elemekkel vannak felszerelve, és nem támogatják az RSN által előírt AES algoritmust. Ezen pusztán szoftver upgrade-del nem lehet segíteni, új hardverre van szükség, s ez lassítja az RSN elterjedésének folyamatát.

Ezt a problémát az IEEE is felismerte, és egy olyan opcionális protokollt is hozzáadott a 802.11i specifikációhoz, mely továbbra is az RC4 algoritmust használja, és így – szoftver upgrade után – futtatható a régi hardveren, de erősebb, mint a WEP. Ezt a protokollt TKIP-nek (Temporal Key Integrity Protocol) nevezik.

A WiFi eszközöket gyártó cégek azonnal adaptálták a TKIP protokollt, hiszen annak segítségével a régi eszközökből álló WEP-es hálózatokat egy csapásra biztonságossá lehetett varázsolni. Meg sem várták, amíg a 802.11i specifikáció a lassú szabványosítási folyamat során végleges állapotba kerül, azonnal kiadták a WPA (WiFi Protected Access) specifikációt [WPA], ami a TKIP-re épül. A WPA tehát egy gyártók által támogatott specifikáció, mely az RSN egy azonnal használható részhalmazát tartalmazza. A WPA- ban a hitelesítés, a hozzáférés-védelem, és a kulcsok menedzsmentje megegyezik az RSN-ben használt módszerekkel, a különbség csak az integritás-védelemre és a rejtjelezésre használt algoritmusokban mutatkozik.

Hitelesítés és hozzáférés-védelem

A 802.11i-ben a hitelesítés és hozzáférés-védelem modelljét a 802.1X szabványból kölcsönözték [802.1X]. Ezt a szabványt eredetileg vezetékes LAN-ok számára tervezték, de az elvek végülis vezeték nélküli WiFi hálózatokban is ugyanúgy alkalmazhatóak.

A 802.1X modell három résztvevőt különböztet meg a hitelesítés folyamatában: a hitelesítendő felet (supplicant), a hitelesítőt (authenticator), és a hitelesítő szervert (authentication server). A hitelesítendő fél szeretne a hálózat szolgáltatásaihoz hozzáférni, és ennek érdekében szeretné magát hitelesíteni, azaz kilétét bizonyítani. A hitelesítő kontrollálja a hálózathoz történő hozzáférést. A modellben ez úgy történik, hogy a hitelesítő egy ún. port állapotát vezérli. Alapállapotban a porton adatforgalom nincs engedélyezve, ám sikeres hitelesítés esetén a hitelesítő „bekapcsolja" a portot, ezzel engedélyezve a hitelesítendő fél adatforgalmát a porton keresztül. A hitelesítő szerver az engedélyező szerepet játssza. Tulajdonképpen a hitelesítendő fél hitelesítését nem a hitelesítő, hanem a hitelesítő szerver végzi, és ha a hitelesítés sikeres volt, engedélyezi, hogy a hitelesítő bekapcsolja a portot.

WiFi hálózatok esetében a hitelesítendő fél a mobil eszköz, mely szeretne a hálózathoz csatlakozni, a hitelesítő pedig az AP, mely a hálózathoz történő hozzáférést kontrollálja. A hitelesítő szerver egy program, mely kisebb hálózatok esetében akár az AP-ben is futhat, nagyobb hálózatoknál azonban tipikusan egy külön erre a célra dedikált hoszton futó szerveralkalmazás. WiFi esetében a port nem egy fizikai csatlakozó, hanem egy logikai csatlakozási pont, amit az AP-ben futó szoftver valósít meg.

Maga a hitelesítés az EAP (Extensible Authentication Protocol) segítségével történik [EAP]. Az EAP egy igen egyszerű protokoll, aminek az az oka, hogy nem maga az EAP végzi a hitelesítést. Az EAP csak egy illesztő-protokoll, amit arra terveztek, hogy tetszőleges hitelesítő protokoll üzeneteit szállítani tudja (ezért „extensible"). Egy adott hitelesítő protokoll EAP-ba történő beágyazásának szabályait külön kell specifikálni. Több elterjedt hitelesítő protokollra létezik már ilyen specifikáció (pl. EAP-TLS, LEAP, PEAP, EAP-SIM).

Négy fajta EAP üzenet létezik: request, response, success, és failure. Az EAP request és response üzenetek szállítják a beágyazott hitelesítő protokoll üzeneteit.

Az EAP success és failure speciális üzenetek, melyek segítségével a hitelesítés eredményét lehet jelezni a hitelesítendő fél felé. WiFi esetében az EAP protokollt (és az abba beágyazott tényleges hitelesítő protokollt, például a TLS-t) lényegében a mobil eszköz és a hitelesítő szerver futtatják. Az AP csak továbbítja az EAP üzeneteket a mobil eszköz és a hitelesítő szerver között, de nem érti azok tartalmát. Az AP csak az EAP success és failure üzeneteket érti meg, ezeket figyeli, és ha success üzenetet lát, akkor engedélyezi a mobil eszköz csatlakozását a hálózathoz.

Az EAP üzeneteket a mobil eszköz és az AP között a 802.1X-ben definiált EAPOL (EAP over LAN) protokoll szállítja. Az AP és a hitelesítő szerver között a WPA a RADIUS protokoll [RADIUS] használatát írja elő. A RADIUS-t az RSN opcióként ajánlja, de más alkalmas protokoll használatát is lehetővé teszi a specifikáció. Végülis tetszőleges protokoll használható, amely az EAP üzenetek szállítására alkalmas. Elterjedtsége miatt azonban várhatóan a legtöbb hálózat RADIUS-t használ majd.

A hitelesítés eredményeként nemcsak a hálózathoz való hozzáférést engedélyezi a hitelesítő szerver, hanem egy titkos kulcs is létrejön, mely a mobil eszköz és az AP további kommunikációját hivatott védeni. Mivel a hitelesítés a mobil eszköz és a szerver között folyik, ezért a protokoll futása után ezt a kulcsot csak a mobil eszköz és a hitelesítő szerver birtokolja, és azt még el kell juttatni az AP-hez. A RADIUS protokoll biztosít erre használható mechanizmust az MS-MPPE-Recv-Key RADIUS üzenet-attribútum formájában, mely kifejezetten kulcs-szállítás céljára lett specifikálva. A kulcs rejtjelezett formában kerül átvitelre, ahol a rejtjelezés egy a hitelesítő szerver és az AP között korábban létrehozott (tipikusan manuálisan telepített) kulcs segítségével történik.

Kulcsmenedzsment

A hitelesítés során, a mobil eszköz és az AP között létrehozott titkos kulcsot páronkénti mesterkulcsnak (pairwise master key, vagy röviden PMK) nevezik. Azért „páronkénti”, mert csak az adott mobil eszköz és az AP ismeri (na meg a hitelesítő szerver, de az megbízható entitásnak tekinthető), s azért „mester”, mert ezt a kulcsot nem használják közvetlenül rejtjelezésre, hanem további kulcsokat generálnak belőle. Egészen pontosan a PMK-ból mind a mobil eszköz, mind pedig az AP négy további kulcsot generál: egy adat-rejtjelező kulcsot, egy adat-integritás-védő kulcsot, egy kulcs-rejtjelező kulcsot, és egy kulcs-integritás-védő kulcsot.

Ezeket együttesen páronkénti ideiglenes kulcsnak (Pairwise Transient Key, vagy röviden PTK) nevezik. Megjegyezzük, hogy az AES- CCMP protokoll az adatok rejtjelezéséhez és az adatok integritás-védelméhez ugyanazt a kulcsot használja, ezért AES-CCMP használata esetén csak három kulcs generálódik a PMK-ból. A PTK előállításához a PMK-n kívül felhasználják még a két fél (mobil eszköz és AP) MAC címét, és két véletlen számot, melyet a felek generálnak.

A véletlen számokat az ún. *négy utas kézfogás* (four way handshake) protokollt használva juttatják el egymáshoz a felek. Ennek a protokollnak további fontos feladata az, hogy segítségével a felek közvetlenül meggyőződjenek arról, hogy a másik fél ismeri a PMK-t. A négy utas kézfogás protokoll üzeneteit az EAPOL protokoll Key típusú üzeneteiben juttatják el egymáshoz a felek.

Az üzenetek tartalma és a protokoll működése vázlatosan a következő:

1. Első lépésként az AP elküldi az általa generált véletlen számot a mobil eszköznek. Mikor a mobil eszköz ezt megkapja, rendelkezésére áll minden információ a PTK előállításához. A mobil eszköz tehát kiszámolja az ideiglenes kulcsokat.

2. A mobil eszköz is elküldi az általa generált véletlen számot az AP-nek. Ez az üzenet kriptográfiai integritás-ellenőrző összeggel (Message Integrity Code, vagy röviden MIC) van ellátva, amit a mobil eszköz a frissen kiszámolt kulcs- integritás-védő kulcs segítségével állít elő. Az üzenet vétele után az AP-nek is rendelkezésére áll minden információ a PTK kiszámításához. Kiszámolja az ideiglenes kulcsokat, majd a kulcs-integritás- védő kulcs segítségével ellenőrzi a MIC-et. Ha az ellenőrzés sikeres, akkor elhiszi, hogy a mobil eszköz ismeri a PMK-t.

3. Az AP is küld egy MIC-et tartalmazó üzenetet a mobil eszköznek, melyben tájékoztatja a mobil eszközt arról, hogy a kulcsokat sikeresen telepítette, és készen áll a további adatforgalom rejtjelezésre. Ez az üzenet tartalmaz továbbá egy kezdeti sorozatszámot. A későbbiekben ettől az értéktől kezdik majd sorszámozni a felek az egymásnak küldött adatcsomagokat, és a sorszámozás segítségével detektálják a visszajátszásos támadásokat. Az üzenet vétele után a mobil eszköz a kulcs-integritás- védő kulccsal ellenőrzi a MIC-et, és ha az ellenőrzés sikeres, akkor elhiszi, hogy az AP ismeri a PMK-t.

4. Végül a mobil eszköz nyugtázza az AP előző üzenetét, mely egyben azt is jelenti, hogy a mobil eszköz is készen áll a további adatforgalom rejtjelezésére.

A továbbiakban a mobil eszköz és az AP az adat-integritás- védő és az adat-rejtjelező kulccsal védik egymásnak küldött üzeneteiket. Szükség van azonban még olyan kulcsokra is, melyek segítségével az AP többes szórással küldhet üzeneteket biztonságosan minden mobil eszköz számára. Értelemszerűen, ezeket a kulcsokat az összes mobil eszköznek és az AP-nek is ismernie kell, ezért ezeket együttesen ideiglenes csoportkulcsnak (Group Transient Key, vagy röviden GTK) nevezik. A GTK egy rejtjelező és egy integritás-védő kulcsot tartalmaz. AES-CCMP esetén a két kulcs ugyanaz, ezért csak egy kulcsból áll a GTK. A GTK-t az AP generálja, és a négy utas kézfogás során létrehozott kulcs-rejtjelező kulcsok segítségével titkosítva juttatja el minden mobil eszközhöz külön-külön.

TKIP és AES-CCMP

A TKIP (Temporal Key Integrity Protocol) és az AES-CCMP (AES CTR Mode and CBC MAC) a fent leírt kulcsmenedzsment megoldásra támaszkodó protokollok, melyek az üzenetek integritás-védelmével és rejtjelezésével foglalkoznak. Mint azt korábban említettük, a TKIP egy olyan köztes megoldás, amely a régi, WEP-es hardveren is működik, de a WEP-nél jóval magasabb szintű biztonságot nyújt. Az AES-CCMP új hardvert igényel, de cserébe egyszerűbb, tisztább megoldást nyújt, mint a TKIP.

A TKIP a WEP hibáit a következő módon igyekszik javítani:

Integritás-védelem: A TKIP egy új integritás-védelmi mechanizmussal egészíti ki a WEP-es megoldást (utóbbi általában hardverben van implementálva, úgyhogy benne hagyták a TKIP-ben is). Az új mechanizmust Michael-nek hívják. A Michael SDU szinten működik (azaz a felsőbb protokollszintről a MAC szintre érkező adatokon, fragmentálás előtt végzi az integritás-védő ellenőrző összeg számítását), ami lehetővé teszi a hálózati kártya meghajtó programjában (device driver) történő megvalósítást. Ez azért fontos, mert így a Michael bevezetése egyszerű szoftver upgrade-del megoldható.

Az üzenet-visszajátszás detektálása érdekében a TKIP az IV-t használja sorozatszámként.

Ennek megfelelően, a TKIP előírja, hogy az IV értékét minden üzenetben eggyel növelni kell (a WEP-ben ez nem volt kötelező). A vevő nyilvántartja az utolsó néhány vett IV értéket. Ha egy frissen érkezett üzenet IV-je kisebb, mint a legkisebb nyilvántartott IV, akkor a vevő eldobja az üzenetet, míg ha az üzenet IV-je nagyobb, mint a legnagyobb nyilvántartott IV, akkor a vevő megtartja az üzenetet és módosítja a nyilvántartását. Ha egy vett üzenet IV-je a legkisebb és a legnagyobb nyilvántartott IV közé esik, akkor a vevő ellenőrzi, hogy az adott IV szerepel-e a nyilvántartásában. Ha igen, akkor eldobja az üzenetet, ha nem, akkor megtartja azt és módosítja a nyilvántartását.

Titkosítás: A WEP titkosítás legfőbb hibáját az IV kis mérete és a gyenge RC4 kulcsok használata jelentette. A TKIP-ben ezért az IV méretét 24 bitről megnövelték 48 bitre. Ez egyszerű megoldásnak látszik, ám a nehézséget az okozza, hogy a WEP-et támogató hardverek adott hosszúságú (128 bites) értékkel inicializálják az RC4 algoritmust, s így a megnövelt IV-t, a rejtjelező kulccsal együtt, valamilyen módon „bele kell gyömöszölni" ebbe az adott hosszúságba. A gyenge kulcsok problémáját a TKIP úgy oldja meg, hogy minden üzenet rejtjelezését más kulccsal végzi. Így a támadó nem tud a sikeres támadáshoz szükséges számú, azonos (potenciálisan gyenge) kulccsal kódolt üzenetet megfigyelni. Az üzenetkulcsokat a TKIP a négy utas kézfogás során generált adat-rejtjelező kulcsból állítja elő. Az AES-CCMP tervezőinek bizonyos értelemben könnyebb dolguk volt, mint a TKIP tervezőinek, hiszen nem volt megkötés arra vonatkozóan, hogy a protokollnak milyen hardveren kell futnia. A tervezők ezért egyszerűen megszabadultak az RC4 algoritmustól, s helyette az AES blokkrejtjelezőre építették fel a protokollt. Definiáltak egy új AES használati módot, mely a régóta ismert CTR (Counter) mód és a CBC-MAC (Cipher Block Chaining – Message Authentication Code) kombinációja. Ebből származik a CCMP rövidítés. CCMP módban, az üzenet küldője először kiszámolja az üzenet CBC- MAC értékét, ezt az üzenethez csatolja, majd az üzenetet CTR módban rejtjelezi. A CBC-MAC számítás kiterjed az üzenet fejlécére is, a rejtjelezés azonban csak az üzenet hasznos tartalmára és a CBC-MAC értékre vonatkozik. A CCMP mód tehát egyszerre biztosítja a teljes üzenet (beleértve a fejlécet is) integritásának védelmét és az üzenet tartalmának titkosságát. A visszajátszás ellen az üzenetek sorszámozásával védekezik a protokoll. A sorszám a CBC-MAC számításhoz szükséges inicializáló blokkban van elhelyezve.

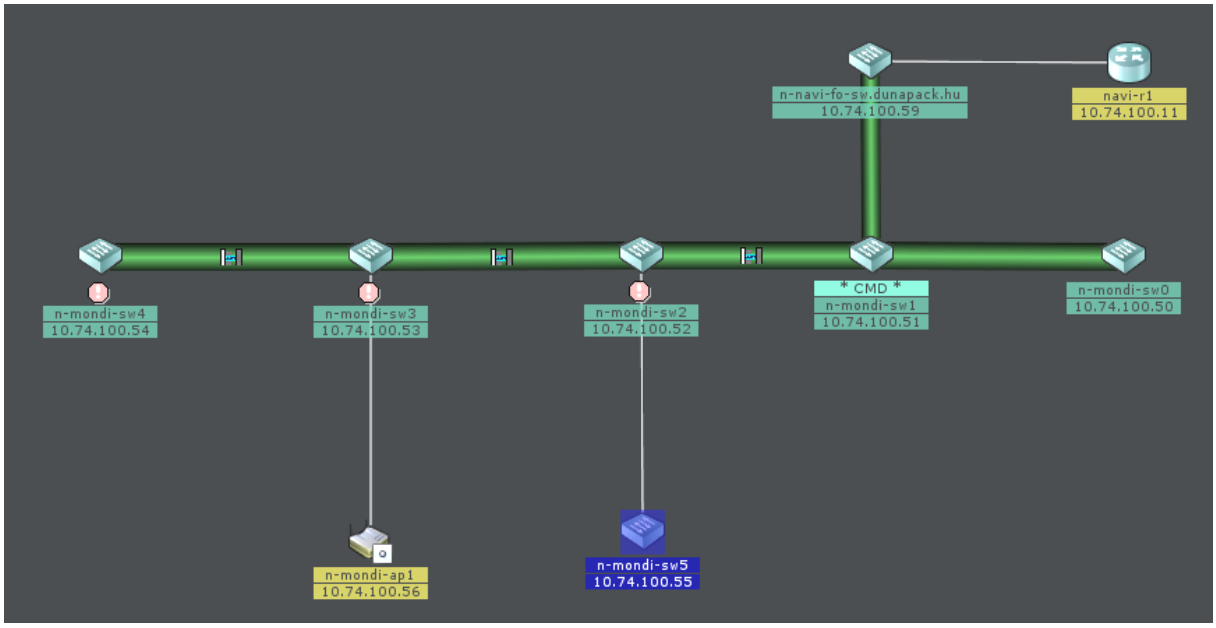
8.2 A vezeték nélküli adatátvitel biztonsága

A rádiós forgalom titkosítását az 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. Mivel ez a vezeték nélküli hálózat kizárólag a Symbol mobil eszközöket fogja ellátni adatkapcsolattal, ezért azokat a beüzemelésük folyamán kellően fel kell programozni. Be kell rajtuk állítani az összes elérhető AP SSID –jét, mert csak így fognak tudni csatlakozni a hálózathoz.

Az adatforgalom biztonsága érdekében WPA kulcsmenedzsment és TKIP titkosítás kerül beállításra. A hálózathoz, történő kapcsolódáskor előre definiált kulcs (Pre-Shared Key) megfelelő alkalmazása szükséges. A kulcs minden AP esetében azonos.
Ezeket a biztonsági beállításokat a Cisco Aironet AIR-AP1242AG-E-K9 AP-k IOS-a alapértelmezésben ismeri, így nincs szükség külön RADIUS szerverre.
A vezeték nélküli adatátvitel biztonságát tovább növelem az Access Point –okba beépített MAC Address Filter beállításával. Ez annyit takar, hogy a kliensek fizikai címeit előre beprogramozom minden AP-be, és beállítom, a MAC filtert. Ennek következtében az AP-k csak ezeket a klienseket engedik csatlakozni a hálózathoz.
Mindezen védelmi beállítások elvégzése után (SSID No Broadcast + WPA/TKIP + MAC filter) nyugodtan állíthatjuk, hogy a hálózatunk nagyfokú védettségben részesül a külső, illetéktelen behatolásokkal szemben.

9 Hálózati beállítások

9.1 Meglévő hálózati topológia



20. ábra Jelenlegi hálózati topológia

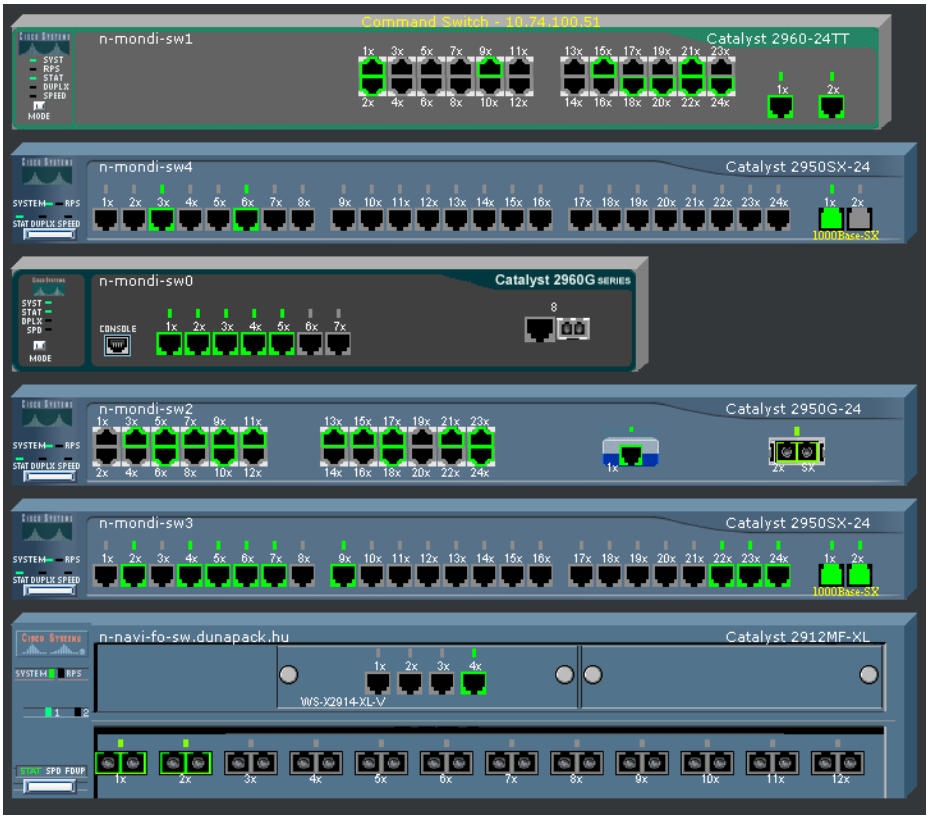
Hálózati eszközök címzése:

1. n-mondi-sw1 10.74.100.51 (*CMD* switch)
2. n-mondi-sw0 10.74.100.50
3. n-mondi-sw2 10.74.100.52
4. n-mondi-sw3 10.74.100.53
5. n-mondi-sw4 10.74.100.54
6. n-mondi-sw5 10.74.100.55
7. n-mondi-ap1 10.74.100.56
8. n-navi-fo-sw 10.74.100.59
9. navi-r1 10.74.100.11

A hálózati aktív eszközök Cluster-be vannak szervezve.

Cluster információk:

Switch-ek:



21. ábra A jelenlegi hálózat aktív eszközei

Amint a 21. ábrán is látható, a Mondi Bags Hungária Kft számítógépes hálózatát kizárólag Cisco switch-ek vezérlik. Így a meglévő hálózat aktív eszközeinek bővítése után az L2 roaming tökéletesen működik.

9.2 Új eszközök címkiosztása

Új eszközök címzése:

Eszköz	Host Name	IP cíp
Cisco Catalyst 2960G-24TC-L	n-mondi-sw6	10.74.100.57
Cisco AIR-AP1242AG-E-K9	n-mondi-ap2	10.74.100.60
Cisco AIR-AP1242AG-E-K9	n-mondi-ap3	10.74.100.61
Cisco AIR-AP1242AG-E-K9	n-mondi-ap4	10.74.100.62
Cisco AIR-AP1242AG-E-K9	n-mondi-ap5	10.74.100.63
Cisco AIR-AP1242AG-E-K9	n-mondi-ap6	10.74.100.64
Cisco AIR-AP1242AG-E-K9	n-mondi-ap7	10.74.100.65
Cisco AIR-AP1242AG-E-K9	n-mondi-ap8	10.74.100.66
Cisco AIR-AP1242AG-E-K9	n-mondi-ap9	10.74.100.67
Cisco AIR-AP1242AG-E-K9	n-mondi-ap10	10.74.100.68
Cisco AIR-AP1242AG-E-K9	n-mondi-ap11	10.74.100.69

A mobil adatgyűjtők stabil, folyamatos hálózati kapcsolati működésének érdekében, továbbá a L2 roaming miatt az eszközöket statikus IP címmel kell ellátni.

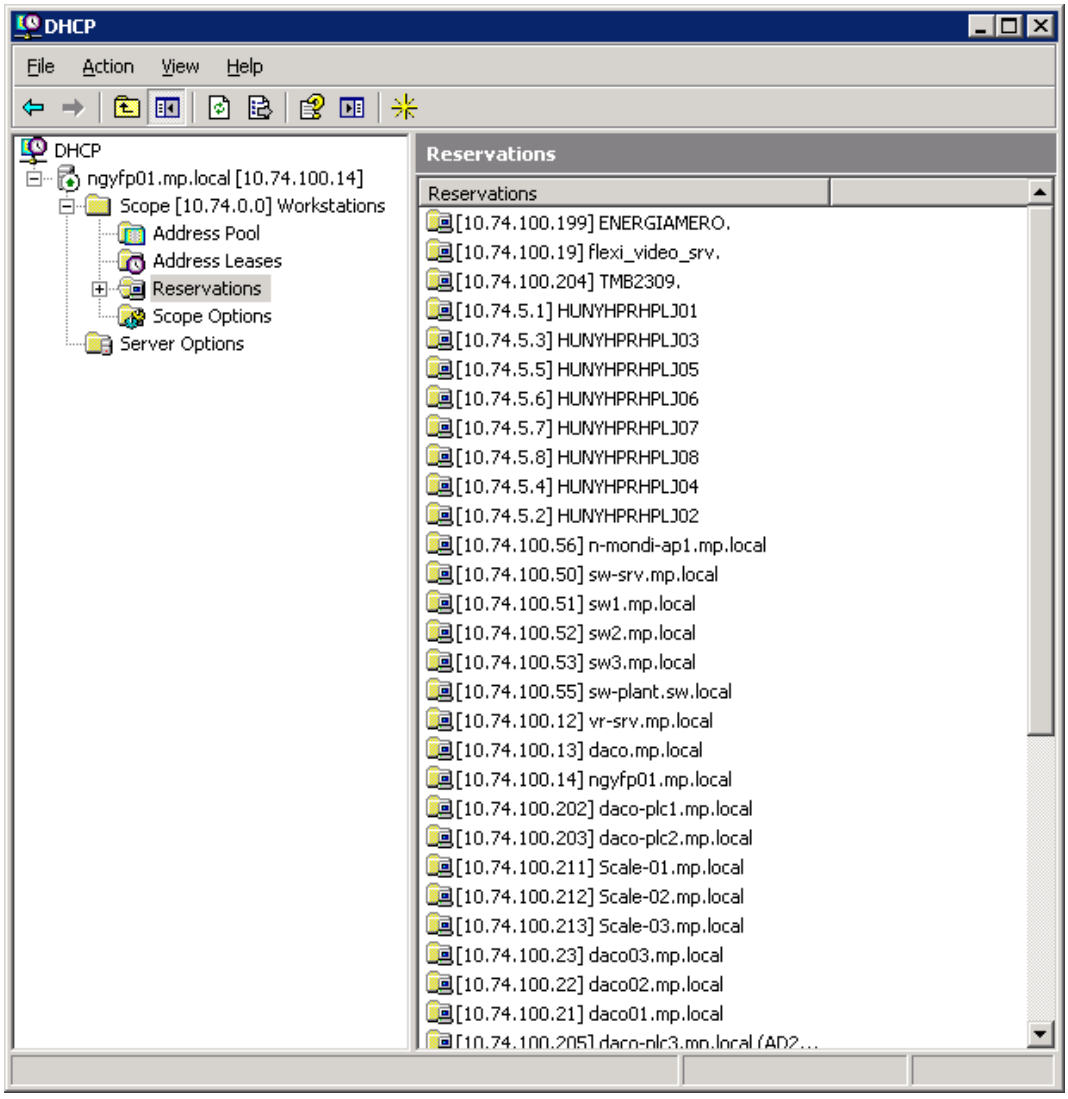
A Symbol scannerek címei:

11 db Symbol MC9090-G Scanner: 10.74.101.201 – 10.74.101.211

10 Egyéb – a biztonságos üzemeltetést szolgáló intézkedések

A Mondi Bags Hungária Kft központi szervere (NGYFP01) MS Windows 2003 szerver, amelyen konfigurálva van a DHCP szolgáltatás.

A hálózati aktív eszközök, az Access-Point-ok és a mobil adatgyűjtők statikus IP címmel rendelkeznek. A beállítások dokumentálása végett a DHCP-ben konfigurálom a fent felsorolt eszközök címeit. Ez azért előnyös, ha a későbbiekben bármilyen oknál fogva meg kell találni egy adott eszközt a hálózaton, akkor nagyban lerövidíthető a keresés ideje.
Ha valamelyik eszközből bármilyen okból törlődnek a hálózati beállítás paraméterei, akkor a dhcp-től megkapja a címét, beállításait.



A Cisco AIR –AP1242-AG Access-Point -ok konfigurálása, programozása után a startup config beállításokat egyenként elmentem, egy erre a célra kialakított ftp könyvtárba a központi szerveren. Erre szintén biztonsági okokból van szükség, mivel így bármikor betölthető bármelyik AP –re a működő startup config –ja. Ez az eljárás arra az esetre is alkalmazható, ha meghibásodás miatt valamelyik AP helyére cserekészüléket kell felszerelni.

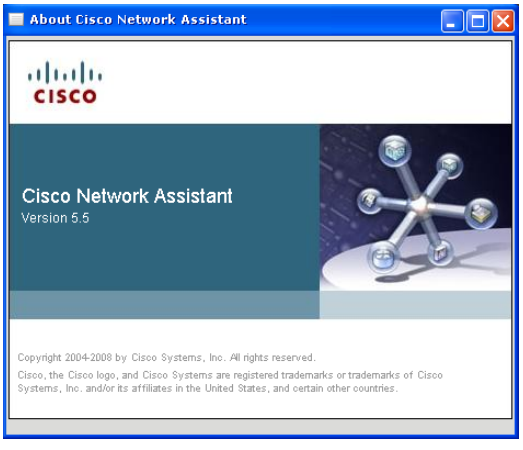
11 Összegzés

A dolgozatom témája a Mondi Bags Hungária Kft Nyíregyházi Zsákgyár telephelyén létesítendő vezeték nélküli hálózat tervezése, megvalósíthatóságának vizsgálata volt. Ez egy valós projekt, ami a dolgozatom készítése közben ténylegesen kiépítésre kerül. Így a szakdolgozatban leírtakat a valóságban nyomon lehet követni. Sajnos a dolgozat leadásáig a hálózat nem készült el teljes mértékben, ezért a kész hálózatról mérési eredményekről nem tudtam beszámolni a dolgozatomban.

Az azonban megállapítható, hogy a hálózat az elvárt követelményeknek teljes mértékben megfelel:

- Lefedi a megrendelő által megjelölt területeket
- Az alapanyag raktárban a papírtekercsek között is stabil hálózatot biztosít
- Mobilitást nyújt a Symbol scannerek részére L2 –es roaming segítségével.
- Biztonságos hálózati kapcsolatot létesít a kliensekkel, továbbá védett az illetéktelen behatolási próbálkozásokkal szemben (SSID No Broadcast + WPA/TKIP + MAC filter)
- Hálózati eszközök meghibásodása esetén gyors hibajavítási lehetőség (DHCP, ftp-n startup config). Itt jegyzem meg, hogy az aktív eszközökből 1 db tartalék beszerzését javaslom.

Mindezek figyelembevételével elmondható, hogy a Megrendelő egy stabilan, nagy biztonsággal működő vezeték nélküli hálózatot kap, amely szerves részeként beleilleszkedik a meglévő vezetékes hálózatába.



Az aktív eszközök felügyeletét a Cisco Network Assistant v5.5 szoftver segítségével végzem.

Ezzel a programmal a Cisco switch-ek és AP –k teljes körű felügyelete biztosított.

12 Irodalomjegyzék

- **A WLAN hálózatok története napjainkig** – www.bcs.hu/letoltes.php?d_id=872
- **IPv6 kapcsolatok elemzése mobil WiFi környezetben** – Gál Z. Karsai A. Orosz P. – Híradástechnika 2005/11 LX Évfolyam
- http://www.cisco.com/en/US/docs/wireless/technology/mesh/design/guide
- **NHH: Tájékoztató** – Szélessávú adatátvitel rádiós hozzáférési eszközökkel (RLAN, WiFi, WMAN, WIMAX,..) 2. kiadás 2006. október 1.
- **MSZ EN 300 328-2**
- **WiFi biztonság – A jó, a rossz, és a csúf** - Buttyán L. és Dóra L. (Budapesti Műszaki és Gazdaságtudományi Egyetem Híradástechnikai tanszék)
- **Wireless Networking in the Developing World** – Second Edition December 2007 *http://wndw.net/*

13 Függelék

Az **n-mondi-ap1** Access Point konfigurációja:

```
------------------ show version ------------------

Cisco IOS Software, C1240 Software (C1240-K9W7-M), Version 12.3(8)JEA,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Wed 23-Aug-06 16:45 by kellythw

ROM: Bootstrap program is C1240 boot loader
BOOTLDR: C1240 Boot Loader (C1240-BOOT-M) Version 12.3(7)JA1, RELEASE
SOFTWARE (fc1)
n-mondi-ap1 uptime is 2 days, 22 hours, 25 minutes
System returned to ROM by power-on
System restarted at 18:08:15 GMT Thu Nov 5 2009
System image file is "flash:/c1240-k9w7-mx.123-8.JEA/c1240-k9w7-mx.123-
8.JEA"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco AIR-AP1242AG-E-K9    (PowerPCElvis) processor (revision A0) with
24566K/8192K bytes of memory.
Processor board ID FOC110443EU
PowerPCElvis CPU at 266Mhz, revision number 0x0950
Last reset from power-on
1 FastEthernet interface
2 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:19:30:77:0D:30
Part Number                          : 73-10256-05
PCA Assembly Number                  : 800-26918-04
PCA Revision Number                  : B0
PCB Serial Number                    : FOC110443EU
Top Assembly Part Number             : 800-26965-03
Top Assembly Serial Number           : FCZ111181QH
Top Revision Number                  : A0
Product/Model Number                 : AIR-AP1242AG-E-K9

Configuration register is 0xF
```

```
------------------ show running-config ------------------


Building configuration...

Current configuration : 1999 bytes
!
! Last configuration change at 16:32:58 GMT Sun Nov 8 2009
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname n-mondi-ap1
!
enable secret 5 <removed>
!
clock timezone GMT 1
ip subnet-zero
!
!
no aaa new-model
!
dot11 ssid Mondi_nyh
   authentication open
   authentication key-management wpa
   guest-mode
   infrastructure-ssid optional
   wpa-psk ascii 7 03290D05550677551A
!
power inline negotiation prestandard source
!
!
username Cisco password 7 <removed>
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption mode ciphers aes-ccm tkip
 !
 ssid Mondi_nyh
 !
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0
48.0 54.0
 station-role root
 antenna receive right
 antenna transmit right
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
```

```
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 encryption mode ciphers aes-ccm tkip wep128
 no dfs band block
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
 hold-queue 160 in
!
interface BVI1
 ip address dhcp client-id FastEthernet0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
!
!
control-plane
!
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
 login local
!
sntp server 10.74.100.12
sntp broadcast client
end
```

```
------------------ show stacks ------------------


Minimum process stacks:
 Free/Size   Name
 4576/5500   soap_flash init
 5236/5500   dot11 platform init
 8696/12000  Init
 5084/5500   RADIUS INITCONFIG
 3544/5500   RAC I/F Conf.
 8184/11000  Soap Upgrade fetch Config File
 2580/3000   Rom Random Update Process
 5144/11000  HTTP CP

Interrupt level stacks:
Level    Called Unused/Size  Name
  4     4370064   7260/9000  dot11 radio interrupt
  6         851   8956/9000  NS16550 VECTOR

------------------ show interfaces ------------------


BVI1 is up, line protocol is up
  Hardware is BVI, address is 0019.3077.0d30 (bia 001a.e300.bd00)
  Internet address is 10.74.100.56/16
  MTU 1500 bytes, BW 54000 Kbit, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  5 minute input rate 9000 bits/sec, 9 packets/sec
  5 minute output rate 23000 bits/sec, 8 packets/sec
     338948 packets input, 32170151 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     10698 packets output, 1853185 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
Dot11Radio0 is up, line protocol is up
  Hardware is 802.11G Radio, address is 001a.e300.bd00 (bia 001a.e300.bd00)
  MTU 1500 bytes, BW 54000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 1d22h, output 1d22h, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/30 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     919497 packets input, 170395657 bytes, 0 no buffer
     Received 10143 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     941668 packets output, 493521270 bytes, 0 underruns
```

```
     2136 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
Dot11Radio1 is administratively down, line protocol is down
  Hardware is 802.11A Radio, address is 001a.e304.bcf0 (bia 001a.e304.bcf0)
  MTU 1500 bytes, BW 54000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/30 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
FastEthernet0 is up, line protocol is up
  Hardware is PowerPCElvis Ethernet, address is 0019.3077.0d30 (bia
0019.3077.0d30)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, MII
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/160/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 9000 bits/sec, 11 packets/sec
  5 minute output rate 23000 bits/sec, 8 packets/sec
     1517850 packets input, 523705113 bytes
     Received 671793 broadcasts, 0 runts, 0 giants, 1 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog
     0 input packets with dribble condition detected
     851866 packets output, 169374836 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

```
------------------ show controllers ------------------


!
interface Dot11Radio0
Radio AIR-AP1242GR, Base Address 001a.e300.bd00, BBlock version 0.00,
Software version 6.00.1
Serial number: GAM110443EU
Number of supported simultaneous BSSID on Dot11Radio0: 8
Carrier Set: EMEA (EU )
Uniform Spreading Required: No
Current Frequency: 2427 MHz  Channel 4
Allowed Frequencies: 2412(1) 2417(2) 2422(3) 2427(4) 2432(5) 2437(6)
2442(7) 2447(8) 2452(9) 2457(10) 2462(11) 2467(12) 2472(13)

Listen Frequencies: 2412(1) 2417(2) 2422(3) 2427(4) 2432(5) 2437(6) 2442(7)
2447(8) 2452(9) 2457(10) 2462(11) 2467(12) 2472(13) 2484(14)
Beacon Flags: 0; Beacons are enabled; Probes are enabled
Current CCK Power: 17 dBm
Allowed CCK Power Levels: -1 2 5 8 11 14 17
Current OFDM Power: 17 dBm
Allowed OFDM Power Levels: -1 2 5 8 11 14 17
Allowed Client Power Levels: 2 5 8 11 14 17
ERP settings: short slot time.
Neighbors in non-erp mode:

Current Rates:  basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0
24.0 36.0 48.0 54.0
Active Rates:  basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0
24.0 36.0 48.0 54.0
Allowed Rates:  1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates:  basic-1.0 2.0 5.5 6.0 9.0 11.0 12.0 18.0 24.0 36.0 48.0
54.0
Best Throughput Rates:  basic-1.0 basic-2.0 basic-5.5 basic-6.0 basic-9.0
basic-11.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0 basic-48.0 basic-
54.0
Default Rates:  basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0
24.0 36.0 48.0 54.0
Current Voice Rates:  5.5 6.0 11.0 12.0 24.0 [disabled until voice packet-
discard enabled]
Default Voice Rates:  5.5 6.0 11.0 12.0 24.0
Channel / Max Power Table
  1 O=17 D=17,    2 O=17 D=17,    3 O=17 D=17,    4 O=17 D=17,    5 O=17
D=17
  6 O=17 D=17,    7 O=17 D=17,    8 O=17 D=17,    9 O=17 D=17,   10 O=17
D=17
 11 O=17 D=17,   12 O=17 D=17,   13 O=17 D=17

Data Rate Sensitivity (rate, SNR dB, Contention dBm)
( 1.0, 10, -93)   ( 2.0, 10, -92)   ( 5.5, 11, -90)   (11.0, 14, -90)
( 6.0, 15, -89)   ( 9.0, 16, -88)   (12.0, 18, -88)   (18.0, 19, -86)
(24.0, 20, -85)   (36.0, 24, -81)   (48.0, 27, -78)   (54.0, 31, -77)
Radio Management (RM) Configuration:
 Regular AP RM Mode 1   Temp Setting Disabled
 Temp  Settings: AP Tx Power 0    AP Tx Channel 0    Client Tx Power 0
      Rates:
 Saved Settings: AP Tx Power 0    AP Tx Channel 4    Client Tx Power 0
      Rates:
```

```
MCST RSCs: [0]0x0 [1]0x0 [2]0x0 [3]0x0 [4]0x0
TKIP Cum Stats: STA            MIC-L-Errs MIC-R-Errs Replay   C-Measure
                0000.0000.0000 00000000   00000000   00000000 00000000
AES-CCMP Cum Stats: 00000000 replays discarded

QBSS Load: 0x0
Policing Stats:Rx downgardes 0, Tx downgrades 0

Configured Local Access Class Parameters
  Back      : cw-min 4 cw-max 10 fixed-slot 7 admission-control Off txop 0
  Best      : cw-min 4 cw-max 6 fixed-slot 3 admission-control Off txop 0
  Video     : cw-min 3 cw-max 4 fixed-slot 1 admission-control Off txop
3008
  Voice     : cw-min 2 cw-max 3 fixed-slot 1 admission-control Off txop
1504
Configured Cell Access Class Parameters
  Back      : cw-min 4 cw-max 10 fixed-slot 7 admission-control Off txop 0
  Best      : cw-min 4 cw-max 10 fixed-slot 3 admission-control Off txop 0
  Video     : cw-min 3 cw-max 4 fixed-slot 2 admission-control Off txop
3008
  Voice     : cw-min 2 cw-max 3 fixed-slot 2 admission-control Off txop
1504
Transmit queues: Active 0 In Progress 0
       ---- Active --- In-Progress --------------- Counts -------------
       Cnt Quo Bas Max Cnt Quo Bas       Sent   Discard  Fail   Retry Multi
Uplink   0   0   0   0   0   0   0          0         0     0       0     0
Voice    0   0   0   0   0   0   0       3078         0    47    2023  1930
Video    0   0   0   0   0   0   0          0         0     0       0     0
Best     0   2  70   2   0   2  24     858322         0     2   23562  8815
Mcast    0   0   0   0   0   0   0      80245         0     0       0     0
Back     0   0   0   0   0   0   0      80245         0     0       0     0
BSSIDS Index Flags State Next Held Defer NonDefer Clients Tsf Dtim Txq
  BD00     0    20     0    0    0     0        0       0   0    2   0
UP ClientQAged    AcQAged PacketAged Drop  Retry/Thresh Timeout CQMax
 7           0          0          0       3/100  0/500      35     4
 6           0          0          0       3/100  0/500      35     4
 5           0          0          0       3/100  0/500      35     4
 4           0          0          0       3/100  0/500      35     4
 3           0          0          0       3/100  0/500      35     4
 2           0          0          0       3/100  0/500      35     4
 1           0          0          0       3/100  0/500      35     4
Driver TX blocks: in use 0, high 54, at reset 0, fail 0, reclaim 0
Clients: 8021x auth in prog 0 allowed 0
Vlan BSSID   Clients PSP Pri Encr  Key0 Key1 Key2 Key3 SSIDs
   0n BD00 0       0   0   0  234       x128
0 0 flags 3
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
```

```
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
17 0 flags 0
18 0 flags 0

Registers: io E8000000 mem 80000000 aux A0000000
 0000 FF50 0000 0000 0021 0000 0000 0000
 0001 0000 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000
 0500 0007 0000 0000 0020 0B88 F39D 0504
 0000 0000 0000 0000 8893 002F A700 C723
 00000000 0000B080 00008021 FFFFFFFF FFFFFFFF 00000000 01018440 0800020A
 FFFFDFEE 00002FFF E3377E0D 0000026C 00000000 00000000 0000800C 00008041
 00000000 00000000 00000000 00000000 00007974 0000779A 00000000 0000F8B6
Radio running:  temp 0 C tx_power 17 bb_code 0x0
    rssi_threshold 0x0 gain offset 0

Antenna: external , gain 4 (platform 2, domain class E)
PCI sys_id: 0xA506 subsys_id 0x7100 (0x7101)

Unicast ciphers 0x1 mcast ciphers 0x1
Rid Ring:
 A0000970: 009C8000 2197FC28 * n
Rx Ring:
 A0000950: 893E0002 219D1D04   v, 893E0002 219CCA64 * v
 A0000960: 893E0002 219CE960   v, 893E0002 219CFE08   v
Tx Ring:
 A0000800: 00728000 21806534   n, 00728000 21800FB4   n
 A0000810: 00728000 21805A84   n, 00648000 21B5F890   n
 A0000820: 00728000 21808544   n, 00648000 21B32EB8   n
 A0000830: 00768000 21AF7924   n, 00768000 21AE2F28   n
 A0000840: 033D8000 21830ED0 * n, 00648000 21B38D00   n
 A0000850: 00768000 21B32EB0   n, 00768000 21B3AEA4   n
 A0000860: 00648000 21B5F890   n, 00728000 218030F4   n
 A0000870: 00648000 21B135A4   n, 00768000 21AF7924   n
 A0000880: 00768000 21AE2F28   n, 00728000 21802FC4   n
 A0000890: 00648000 21B2DDE8   n, 00768000 21B35DD4   n
 A00008A0: 00768000 21AE793C   n, 00728000 21807CF4   n
 A00008B0: 00728000 21800C24   n, 00728000 21806074   n
 A00008C0: 00728000 218029D4   n, 00728000 218088D4   n
TxDn Ring:
 A0000930: 802C0000 21980428   v, 802C0000 21980500   v
 A0000940: 802C0000 219805D8 * v, 802C0000 219806B0   v
Multicast counters:
Internal MC counts:
79937 (14401) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0
(0) 0 (0) 0 (0) 0 (0) 0 (0)
Log Buffer:


!
interface Dot11Radio1
Radio AIR-AP1242A, Base Address 001a.e304.bcf0, BBlock version 0.00,
Software version 6.00.1
Serial number: ALP110443EU
```

```
Number of supported simultaneous BSSID on Dot11Radio1: 8
Carrier Set: ETSI (OFDM) (EU )
Uniform Spreading Required: Yes
Current Frequency: 0 MHz  Channel 0
Allowed Frequencies: *5180(36) *5200(40) *5220(44) *5240(48) *5260(52)
*5280(56) *5300(60) *5320(64) *5500(100) *5520(104) *5540(108) *5560(112)
*5580(116) *5600(120) *5620(124) *5640(128) *5660(132) *5680(136)
*5700(140)
* = May only be selected by Dynamic Frequency Selection (DFS)

Listen Frequencies: 5170(34) 5190(38) 5210(42) 5230(46) 5180(36) 5200(40)
5220(44) 5240(48) 5260(52) 5280(56) 5300(60) 5320(64) 5500(100) 5520(104)
5540(108) 5560(112) 5580(116) 5600(120) 5620(124) 5640(128) 5660(132)
5680(136) 5700(140) 5745(149) 5765(153) 5785(157) 5805(161) 5825(165)

DFS Blocked Frequencies: none
Beacon Flags: 0; Beacons are disabled; Probes are disabled
Current Power: 17 dBm
Allowed Power Levels: -1 2 5 8 11 14 15 17
Allowed Client Power Levels: 2 5 8 11 14 15 17
Current Rates:  basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Active Rates:
Allowed Rates:  6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Range Rates:  basic-6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0
Best Throughput Rates:  basic-6.0 basic-9.0 basic-12.0 basic-18.0 basic-
24.0 basic-36.0 basic-48.0 basic-54.0
Default Rates:  basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
Current Voice Rates:  6.0 12.0 24.0 [disabled until voice packet-discard
enabled]
Default Voice Rates:  6.0 12.0 24.0
Channel / Max Power Table
 36 O=17,   40 O=17,   44 O=17,   48 O=17,   52 O=17
 56 O=17,   60 O=17,   64 O=17,  100 O=17,  104 O=17
108 O=17,  112 O=17,  116 O=17,  120 O=17,  124 O=17
128 O=17,  132 O=17,  136 O=17,  140 O=17

Data Rate Sensitivity (rate, SNR dB, Contention dBm)
( 6.0, 15, -89)   ( 9.0, 16, -88)   (12.0, 18, -88)   (18.0, 19, -86)
(24.0, 20, -85)   (36.0, 24, -81)   (48.0, 27, -78)   (54.0, 31, -77)
Radio Management (RM) Configuration:
 Regular AP RM Mode 1   Temp Setting Disabled
 Temp  Settings: AP Tx Power 0    AP Tx Channel 0    Client Tx Power 0
      Rates:
 Saved Settings: AP Tx Power 0    AP Tx Channel 0    Client Tx Power 0
      Rates:

MCST RSCs: [0]0x0 [1]0x0 [2]0x0 [3]0x0 [4]0x0
TKIP Cum Stats: STA            MIC-L-Errs MIC-R-Errs Replay   C-Measure
                0000.0000.0000 00000000   00000000   00000000 00000000
AES-CCMP Cum Stats: 00000000 replays discarded

QBSS Load: 0x0
Policing Stats:Rx downgardes 0, Tx downgrades 0

Configured Local Access Class Parameters
  Back      : cw-min 5 cw-max 10 fixed-slot 7 admission-control Off txop 0
  Best      : cw-min 5 cw-max 6 fixed-slot 3 admission-control Off txop 0
```

```
  Video     : cw-min 4 cw-max 5 fixed-slot 1 admission-control Off txop
3008
  Voice     : cw-min 3 cw-max 4 fixed-slot 1 admission-control Off txop
1504
Configured Cell Access Class Parameters
  Back      : cw-min 5 cw-max 10 fixed-slot 7 admission-control Off txop 0
  Best      : cw-min 5 cw-max 10 fixed-slot 3 admission-control Off txop 0
  Video     : cw-min 4 cw-max 5 fixed-slot 2 admission-control Off txop
3008
  Voice     : cw-min 3 cw-max 4 fixed-slot 2 admission-control Off txop
1504
Transmit queues: Active 0 In Progress 0
       ---- Active --- In-Progress --------------- Counts -------------
       Cnt Quo Bas Max Cnt Quo Bas       Sent   Discard  Fail   Retry Multi
Uplink   0   0   0   0   0   0   0          0         0     0       0     0
Voice    0   0   0   0   0   0   0          0         0     0       0     0
Video    0   0   0   0   0   0   0          0         0     0       0     0
Best     0   0   0   0   0   0   0          0         0     0       0     0
Back     0   0   0   0   0   0   0          0         0     0       0     0
BSSIDS Index Flags State Next Held Defer NonDefer Clients Tsf Dtim Txq
UP ClientQAged    AcQAged PacketAged Drop  Retry/Thresh Timeout CQMax
 7           0          0          0       3/100  0/500      35     4
 6           0          0          0       3/100  0/500      35     4
 5           0          0          0       3/100  0/500      35     4
 4           0          0          0       3/100  0/500      35     4
 3           0          0          0       3/100  0/500      35     4
 2           0          0          0       3/100  0/500      35     4
 1           0          0          0       3/100  0/500      35     4
Driver TX blocks: in use 0, high 0, at reset 0, fail 0, reclaim 0
Clients: 8021x auth in prog 0 allowed 0
Vlan BSSID   Clients PSP Pri Encr  Key0 Key1 Key2 Key3 SSIDs
   0n 0000 0       0   0   0    0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0
0 0 flags 0

Registers: io E8000100 mem 80010000 aux A0040000
 0000 FF6A 0000 0000 0021 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0020 1DF4 FFFF 0504
 0000 0000 0000 0000 0FD2 004E A700 F635
```

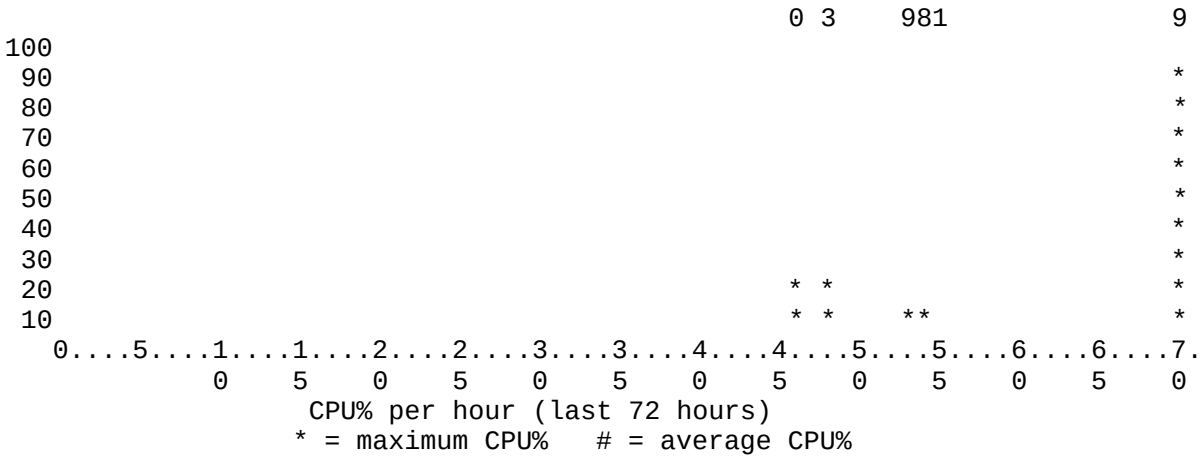
```
 00000000 00020080 01084114 FFFDFFFF FFFFFFFF 00000000 00040240 46200000
 FFFDBFF2 00002FFF E317FF23 2000023B 00000000 00000000 0000800C 00008041
 00000000 00000000 00000000 00000000 0000317A 00000000 00000000 00003DF0
Radio running:  temp 0 C tx_power 0 bb_code 0x0
    rssi_threshold 0x0 gain offset 0

Antenna: external , gain 4 (platform 2, domain class E)
PCI sys_id: 0xA506 subsys_id 0x6700 (0x6701)

Unicast ciphers 0x0 mcast ciphers 0x0
Rid Ring:
 A0040970: 01C08000 21A25B88 * n
Rx Ring:
 A0040950: 893E0002 21A2670C * v, 893E0002 21A27160   v
 A0040960: 893E0002 21A27BB4   v, 893E0002 21A28608   v
Tx Ring:
 A0040800: 00000000 00000000 * n, 00000000 00000000   n
 A0040810: 00000000 00000000   n, 00000000 00000000   n
 A0040820: 00000000 00000000   n, 00000000 00000000   n
 A0040830: 00000000 00000000   n, 00000000 00000000   n
 A0040840: 00000000 00000000   n, 00000000 00000000   n
 A0040850: 00000000 00000000   n, 00000000 00000000   n
 A0040860: 00000000 00000000   n, 00000000 00000000   n
 A0040870: 00000000 00000000   n, 00000000 00000000   n
 A0040880: 00000000 00000000   n, 00000000 00000000   n
 A0040890: 00000000 00000000   n, 00000000 00000000   n
 A00408A0: 00000000 00000000   n, 00000000 00000000   n
 A00408B0: 00000000 00000000   n, 00000000 00000000   n
 A00408C0: 00000000 00000000   n, 00000000 00000000   n
TxDn Ring:
 A0040930: 802C0000 21A26388 * v, 802C0000 21A26460   v
 A0040940: 802C0000 21A26538   v, 802C0000 21A26610   v
Multicast counters:
Internal MC counts:
0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0 (0) 0
(0) 0 (0) 0 (0) 0 (0)
Log Buffer:

PowerPCElvis Ethernet unit 0
PHY Hardware is Broadcom BCM5914 rev. 2 (id_register: 0x40, 0x6322)

rx_intr: 0 tx_intr: 0 mac_err_isr: 0 phy_link_isr:0
Current station address 0019.3077.0d30, default address 0019.3077.0d30
MAL register dump:
malcr        0x0007C082  0x180
malesr       0xC0100010  0x181
malier       0x0000000F  0x182
maltxcasr    0x80000000  0x184
maltxcarr    0x80000000  0x185
maltxeobisr  0x00000000  0x186
maltxdeir    0x00000000  0x187
malrxcasr    0x80000000  0x190
malrxcarr    0x80000000  0x191
malrxeobisr  0x00000000  0x192
malrxdeir    0x00000000  0x193
maltxctp0r   0x01ACBC40  0x1A0
malrxctp0r   0x01ACBB40  0x1C0
malrcbs0   0x00000060  0x1E0
```

```
EMAC register dump:
emacmr0      0x18000000  0x00
emacmr1      0xA1788000  0x04
emactmr0     0x00000000  0x08
emactmr1     0x380F0000  0x0C
emacrmr      0x7D180000  0x10
emacisr      0x00000002  0x14
emacier      0x00000001  0x18
emaciah      0x00000019  0x1C
emacial      0x30770D30  0x20
emacptr      0x0000FFFF  0x2C
emaclsah     0x00000022  0x50
emaclsal     0x909E0AA2  0x54
emacipgr     0x00000004  0x58
emacstacr    0x002F8018  0x5C
emactrtr     0x18000000  0x60
emacrwmr     0x0F002000  0x64
emacoctx     0x0A4E8E86  0x68
emacocrx     0x1F9E8A52  0x6C

UIC register dump:
uicsr      0x00009FA0  0xC0
uicer      0x803F0058  0xC2
uicmsr     0x00000000  0xC6

PHY register dump:
3000 782D 0040 6322 05E1 45E1 0005 2001 0000 0000 0000 0000 0000 0000 0000
0000
1000 0300 0000 0000 0200 003A 0400 0000 002F 8D1F 4400 008A 002F 0000 80A0
RX ring with 16 entries at 0x1ACBB40, Buffer size 1524
Rxhead = 0x1ACBB60 (4), Rxp = 0xDAAF44 (4)
00 pak=0x0DC49C8 buf=0x1B01438 status=9C00 pak_size=0
01 pak=0x0DE4D7C buf=0x1B45074 status=9C00 pak_size=0
02 pak=0x0DB4988 buf=0x1ADF978 status=9C00 pak_size=0
03 pak=0x0DDF098 buf=0x1B38D28 status=9C00 pak_size=0
04 pak=0x0DE009C buf=0x1B3AED4 status=9C00 pak_size=0
05 pak=0x0DDDA2C buf=0x1B35E04 status=9C00 pak_size=0
06 pak=0x0DF1748 buf=0x1B5F8B8 status=9C00 pak_size=0
07 pak=0x0DB598C buf=0x1AE1B24 status=9C00 pak_size=0
08 pak=0x0DC001C buf=0x1AF7954 status=9C00 pak_size=0
09 pak=0x0DB6328 buf=0x1AE2F58 status=9C00 pak_size=0
10 pak=0x0DEAA60 buf=0x1B513C0 status=9C00 pak_size=0
11 pak=0x0DD9D50 buf=0x1B2DE10 status=9C00 pak_size=0
12 pak=0x0DCD384 buf=0x1B135CC status=9C00 pak_size=0
13 pak=0x0DB8664 buf=0x1AE796C status=9C00 pak_size=0
14 pak=0x0DB4320 buf=0x1ADEC00 status=9C00 pak_size=0
15 pak=0x0DCED24 buf=0x1B16BAC status=DC00 pak_size=0

TX ring with 8 entries at 0x1ACBC40, tx_count = 0
tx_head = 0x1ACBC70 (6), head_txp = 0xDAAFA8 (6)
tx_tail = 0x1ACBC70 (6), tail_txp = 0xDAAFA8 (6)
00 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
01 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
02 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
03 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
04 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
05 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
```

```
06 pak=0x0000000 buf=0x0000000 status=1400 pak_size=0
07 pak=0x0000000 buf=0x0000000 status=5400 pak_size=0
0 missed datagrams, 0 overruns
0 transmitter underruns, 0 excessive collisions
0 single collisions, 0 multiple collisions
0 dma memory errors, 0 CRC errors

0 alignment errors, 0 runts, 0 giants
emac/mal specific errors:
0 rx in range, 0 rx out range
0 mal_rx_serr, 0 mal_tx_serr
1 mal_rx_de, 0 mal_tx_de
0 emac_int
0 mal_err_isr
0 SQE errors, 0 tx CRC errors
0 output queue fail



------------------ show file systems ------------------


File Systems:

     Size(b)     Free(b)      Type  Flags  Prefixes
*   15998976    10943488     flash     rw   flash:
           -           -    opaque     rw   bs:
    15998976    10943488   unknown     rw   zflash:
           -           -    opaque     rw   archive:
           -           -    opaque     rw   system:
       32768       29605     nvram     rw   nvram:
           -           -   network     rw   tftp:
           -           -    opaque     rw   null:
           -           -    opaque     ro   xmodem:
           -           -    opaque     ro   ymodem:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   http:
           -           -   network     rw   scp:
           -           -   network     rw   https:


------------------ show flash: ------------------


Directory of flash:/

    2  -rwx           5  Nov 03 2009 23:06:47 +01:00  private-config
    3  -rwx        2082  Nov 03 2009 23:06:47 +01:00  config.txt
    4  drwx         320  Jan 01 1970 01:05:24 +01:00  c1240-k9w7-mx.123-
8.JEA
  153  -rwx        1048  Nov 03 2009 23:06:47 +01:00  private-multiple-fs
  155  -rwx         108  Nov 05 2009 17:06:52 +01:00  env_vars

15998976 bytes total (10943488 bytes free)
```

```
------------------ dir nvram: ------------------


Directory of nvram:/

   28  -rw-        2082                    <no date>  startup-config
   29  ----           5                    <no date>  private-config
    1  -rw-           0                    <no date>  ifIndex-table

32768 bytes total (29605 bytes free)

------------------ show memory statistics ------------------


               Head    Total(b)     Used(b)     Free(b)   Lowest(b)
Largest(b)
Processor     B92E84    13019516     3776976     9242540     8978492
8975696
      I/O    1800000     8388608     3538640     4849968     4849968
4849876


------------------ show process cpu history ------------------



100
 90
 80
 70
 60
 50
 40
 30 ****               *****
 20 ****     ***************                   **********
 10 ****************************              ***************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per second (last 60 seconds)

    22
    02
100
 90
 80
 70
 60
 50
 40
 30
 20 **
 10 *#
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
              * = maximum CPU%   # = average CPU%
```

2 2 8



---------- show dot11 associations all-client ----------

---------- show wlccp ap mobility traffic ----------

---------- show wlccp ap mobility forwarding ----------

---------- show inventory ----------

NAME: "AP1240", DESCR: "Cisco Aironet 1240 Series (IEEE 802.11a/g) Access Point"
PID: AIR-AP1242AG-E-K9 , VID: V02, SN: FCZ111181QH

---------- Mempool statistics ----------

	Head	Total(b)	Used(b)	Free(b)	Lowest(b)	Largest(b)
Processor	B92E84	13019516	3776976	9242540	8978492	8975696
I/O	1800000	8388608	3538640	4849968	4849968	4849876