WLAN (Wireless LAN) alias WI-FI (wireless fidelity)

Mi a wlan?

Az IEEE által 802.11 néven szabványosított vezeték nélküli technológiák alapja. Sok verzió létezik belőle, de most csak a fontosabbakat fogjuk részletezni.
Minden WLAN 2 engedélyezett sávban működhet. Az ISM két sávjában (2400MHz – 2483,5MHz és 5725MHz - 5875MHz) és az UNII (5150MHz – 5725MHz, kis kihagyással) tartományaiban. Ezeken a sávokon belül országonkénti eltérések is lehetnek. Például Magyarországon az 5GHz-es tartomány frekvenciái is külön engedélykötelesek, ill. bejelentéskötelesek, néhányuk tiltott.

Az alapok.

A szabványok

802.11
A 802.11 az IEEE-nek a vezeték nélküli hálózatokra vonatkozó eredeti specifikációja, ami még csak az 1Mbps sebességet foglalta magában. Egy csatorna sávszélessége 20MHz.

802.11a
Az 5 GHz-es sávban működő WiFi szabvány, Magyarországon licencdíjköteles a frekvencia, így kevésbé elterjedt.
maximális elméleti átviteli sebesség: 54Mbps
maximális valódi átviteli sebesség: 23Mbps
modulációk (a maximális sebességnél): OFDM
beltéri távolság: 30m

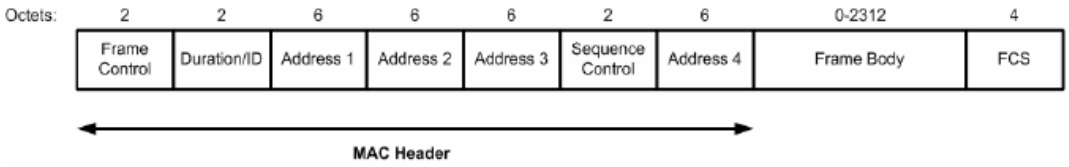
802.11b
A 2.4 GHz-es ISM sávban működő WiFi szabvány, a legelterjedtebb.
maximális elméleti átviteli sebesség: 11Mbps
maximális valódi átviteli sebesség: 6Mbps
modulációk (a maximális sebességnél): DSSS, CCK
beltéri távolság: 35m

802.11g
A 2.4 GHz-es ISM sávban működő WiFi szabvány, a 802.11b-nél nagyobb sebességre képes, szintén elterjedt.
maximális elméleti átviteli sebesség: 54Mbps
maximális valódi átviteli sebesség (titkosítás nélkül): 30Mbps
maximális valódi átviteli sebesség (titkosítással): 15-20Mbps
modulációk (a maximális sebességnél): OFDM, DSSS, CCK
beltéri távolság: 35m

802.11n
A 2,4 GHz-es és az 5 GHz-es tartományban is működik. Két csatornát használ egyszerre, ami 40MHz-et jelent. Hivatalos, végleges szabvány még nincs, de már vannak, a WI-FI Alliance által elfogadott eszközök.
maximális elméleti átviteli sebesség: 300Mbps
maximális valódi átviteli sebesség: 80Mbps
modulációk (a maximális sebességnél): OFDM, DSSS, CCK
beltéri távolság: 70m

A hozzáférésvezérlés a vezetékes hálózatokban használt CSMA/CD-hez (Carrier Sense/Multiple Access with Collision Detection, ütközés érzékelés) hasonló. Az új eljárás neve CSMA/CA (Carrier Sense/Multiple Access with Collision Avoidance, ütközés elkerülés). A node addig nem küld adatot, míg forgalom van a hálózatban. Ha üres a csatorna, akkor ismét megnézi egy adott idő múlva a csatorna foglaltságát, és ha ekkor is üres, akkor egy véletlen idő múlva elküldi az adatkeretet. Mindez az exponenciális backoff algoritmus alapján működik.
Két további csomag bevezetésével próbálták az ütközések valószínűségét csökkenteni. Az RTS és CTS, vagyis Request To Send, ill. Clear To Send. Ezek nevében ott a válasz, de a biztonság kedvéért fejtsük ki. Az első egy kérés, miszerint a kliens adni szeretne, ezért megkérdezi a többi klienst, ill. a célgépet, hogy lefoglalhatja e a sávot. Ha a célgép fizikailag ne elérhető a számára, akkor a köztes kliensek továbbítanak. Ha senkinek „nincs ellene kifogása", a CTS csomaggal válaszol a célgép, és ugyanúgy, mint az RTS csomagnál, itt is segíthetnek a köztes kliensek. A startkliens, addig nem kezd el adni, míg a célklienstől vissza nem érkezett a CTS csomag. A többi kliens pedig addig nem kezd el adni, míg a startkliens nem fejezte be a „mondanivalóját".

A keret felépítése



1 .ábra. 802.11 szabványú átvitel kerete

Frame Control: különböző információk a kerettel kapcsolatban.
Duration/ID: a NAV (network allocation vector) számára tart fenn információkat (pl.: mennyi ideig trt még az adás), de tartalmazhat egy rövid azonosítót is.
Address1-4: A kommunikáló felek MAC címei. Több is található belőle, mert biztonságosabb hálózatoknál szükséges azonosítani a kezdő és vég AP-ok közötti AP-okat is.
Sequence Control: egy 12+4 bitből álló sor, mely a keretmultiplikáció megakadályozására szolgál.
Frame Body: adatok
FCS: frame check sequence, ellenőrző összeg.

Hálózati módok

Ad-Hoc

Egy nagyon egyszerű hálózat. Mint ahogy azt a lentebb, az 2. ábrán is látni lehet (jobb alul), nincs AP. Tehát minden gép össze van kötve minden géppel. Ez mondjuk internetet nem igénylő feladatokhoz (mondjuk hálópartihoz) tökéletes és megszabadulunk a felesleges kábelektől.

Infrastruktúra

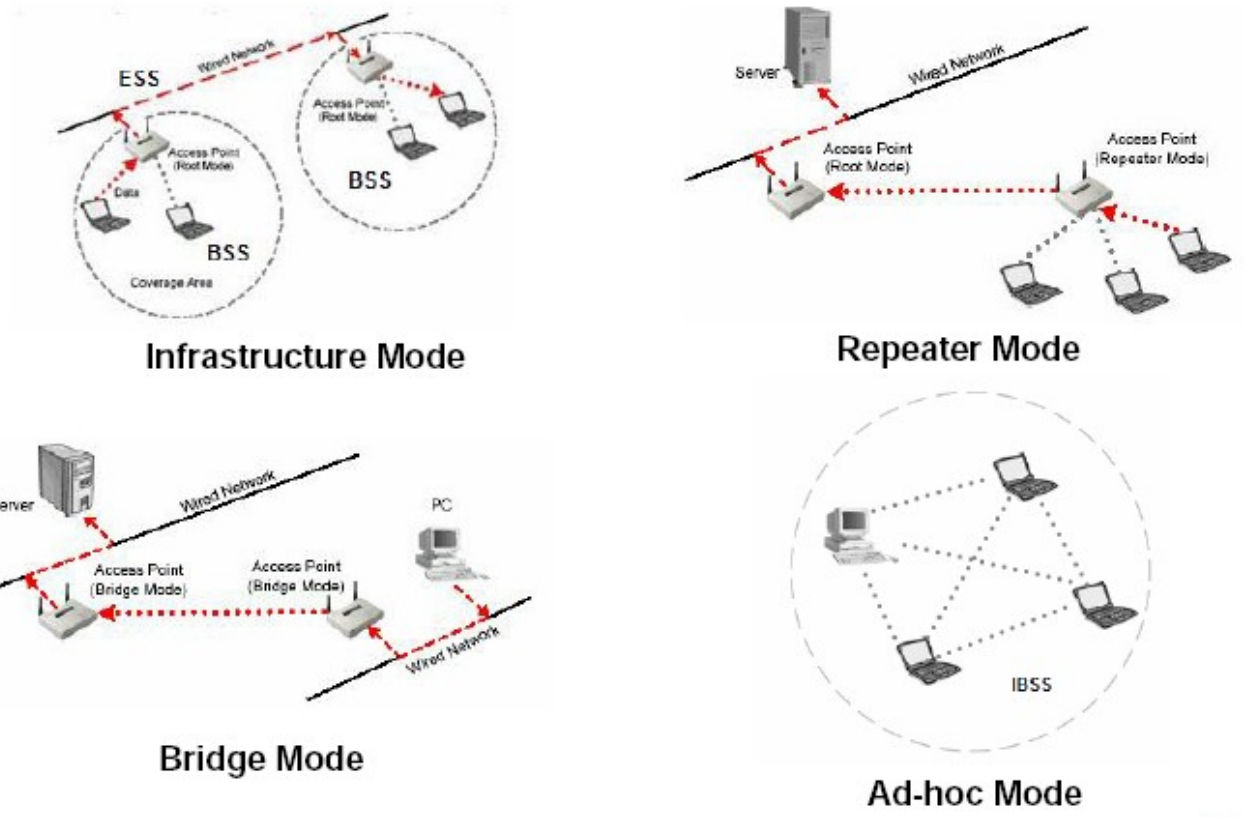
Az Infrastruktúra mód annyit jelent, hogy a vezeték nélküli eszközök egymással nem közvetlen állnak kapcsolatban, hanem minden esetben, egy AP-hoz csatlakoznak. Az AP itt egy vezetékes, vagy egy vezeték nélküli hálózathoz is csatlakozhat.

Root

Az Infrastruktúra mód egyik hálózati formája. A leggyakrabban használt mód a nagyközönség számára. A kliens egy AP-hoz csatlakozik. Tehát a root mód csak a kliens és az AP közti hálózatot jelenti.

Repeater, Bridge, WDS (Wireless Distribution System)
Az Infrastruktúra mód másik hálózati formája, ahol a vezeték nélküli eszközök (kliensek és

kiszolgálók egyaránt) egy nagy, több szintes (leginkább vezeték nélküli) hálózatot képesek kialakítani.
Bridge módban csak AP tud AP-hoz csatlakozni. Repeater módban azonban az AP-okhoz STA-k is csatlakozhatnak.
Ennek továbbfejlesztésére találták ki a WDS-t. Ami lehetővé teszi, hogy akár 6 WAP (wireless AP) is képes legyen egymással működni, akár repeater, akár bridge módban vannak. De egy nagy hátránya azért mégis van. Négyzetesen osztódik a sávszélesség. Vagyis, ha egy STA 1 hop-ra van a fő AP-tól, akkor feleződik a maximális sávszélesség. Ha 2 hop-ra, akkor negyedelődik, és így tovább.



2. ábra. WLAN ismertebb hálózati topológiák

Kapcsolat: STA - AP

Csatlakozás

Kétféle szkennelési mód létezik. Az első a passzív, a második az aktív.
A passzív módszernél az AP-ok folyamatosan küldenek egy úgynevezett *beacon* csomagot, melyben az összes információ megtalálható az AP elérési és csatlakozási lehetőségeiről.
A *beacon* néhány adata Wireshark programmal elfogva tartalmazza:

- az ap márkáját és MAC utolsó 3 számpárát
- a beacon célját (broadcast)
- a protokollt
- az AP nevét (ESSID)
- csatlakozási sebességeket
- a csatorna számát, frekvenciával együtt, pl.: Channel: 2437 (chan 6)
- a szabványokat, melyen működni képes
- a jel erősségét
- a zaj erejét

Az aktív módszer ettől kicsit eltér. Itt a STA keres AP-ot egy *probe request* csomaggal. A felderítő csomagot küldheti a *broadcast*ra, miszerint „én itt vagyok, van e valaki a környéken”. Vagy

küldheti kifejezetten egy már általa ismert AP-nak.

Biztonság és a kapcsolat felvétele
Az alapvető biztonsági formák nagyon egyszerűek, ezért kellett csomagszintű biztonsági protokollokat is kifejleszteni.
megj.: a tűzfalszabályok nem ebbe a témakörbe tartoznak, ezért ezeket nem vesszük ide.
Minden AP-ot elláttak pár alap biztonsági beállítási lehetőséggel (személy szerint a WEP-et is ide sorolnám, ami félig meddig igaz is lenne [a szerk. megjegyzése]). Íme néhány közülük:

- MAC-szűrés
- DHCP off (statikus IP, vagyis a klienseken kézzel állítjuk be az IP-t és a tartományokat)
- az előbbi 2 együtt (vagyis az engedélyezett MAC address-hez mi rendelünk IP címet)
- az SSID broadcast tiltása (ami elég megfelelő biztonság)

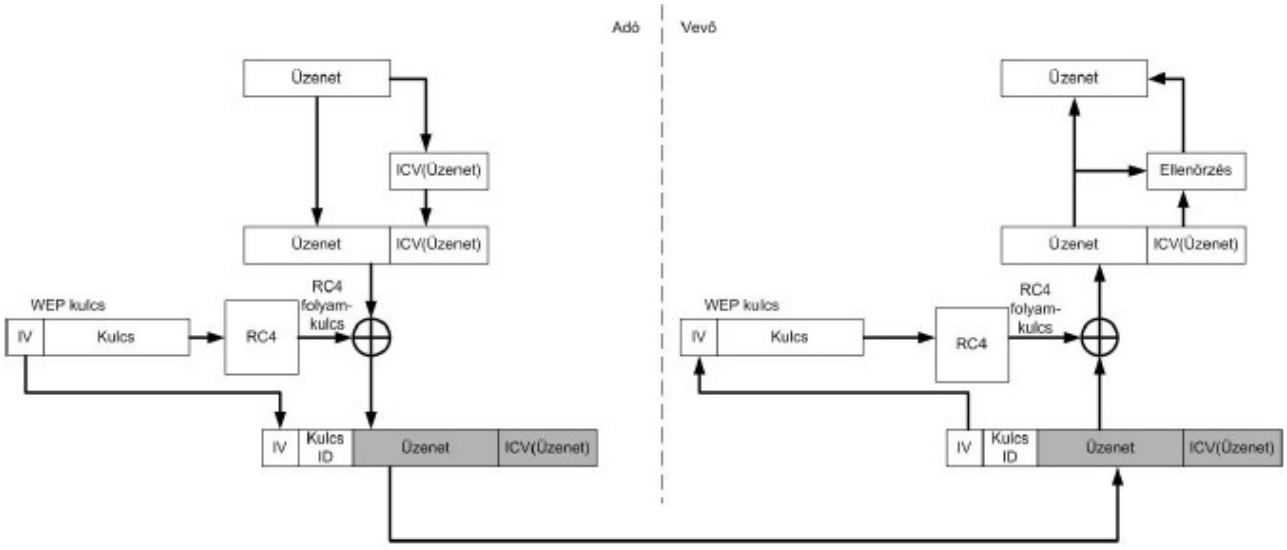
Authentication
Az autentikációnak több formája létezik, de valamiben mindegyik hasonlít. A kapcsolatfelvételt mindig a STA kezdi és az AP fejezi be (egy kérés kapcsolódás céljából és egy engedélyezés).

A nyílt autentikáció
A STA egy autentikációs kérést *(probe request)* küld az AP-nak, majd az AP (ha tényleg nyílt, vagy, ha a STA a szűrési szabályoknak is megfelel) egy engedélyezési választ küld a STA-nak, így létrejön a kapcsolat.

WEP titkosítással (előre megbeszélt kulccsal)
Kapcsolódás

- A STA egy kapcsolódási kérést küld az AP-nak
- Az AP egy „titkos kifejezést” küld vissza kihívásként
- Ezt a STA dekódolja és visszaküldi az AP-nak
- Ha minden egyezik, az autentikációt engedi és létrehozza a kapcsolatot a klienssel.

Biztonság, kódolás
Az üzenetből számolnak egy ellenőrző összeget (ICV – Integritiy Check Value), majd hozzárakják az üzenethez. Az IV (Initialization Vector) + WEP key egy RC4 kódolón megy keresztül, majd ezt a kódot és az üzenetet + ICV-t XOR-olják. A csomag, amit átküldünk, így a következőképpen néz ki: IV + kulcs ID + XOR-olt üzenet. A visszafejtés ugyanez, csak fordított sorrendben (3. ábra).



3. ábra. Vizuális típusoknak képekben a WEP titkosítás

Ennek egy olyan nagy hibája van, hogy az IV-k alapján, ami plain text-ként megy át az éteren, már

nem olyan nehéz kiszámolni a WEP key-t. (a teljes visszafejtési idő fél óra és egy nap közt mozog).

WPA/WPA2-PSK, vagyis a 802.11i szabvány

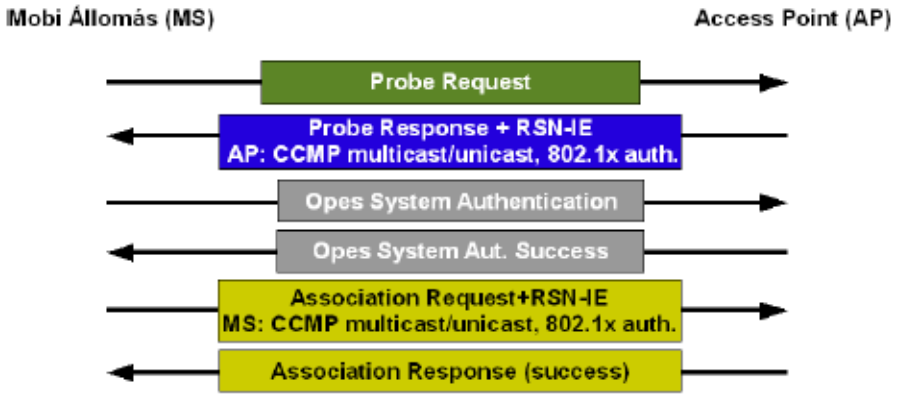
2004-ben elfogadott szabvány egy elég komoly titkosítást foglal magába. Két verziót kellett kifejleszteni, mivel egy ekkora váltást nem tudott volna követni a piac rövid időn belül. A WPA így még a WEP-nél használt RC4-es csipet használja. A WPA2, viszont már egy teljesen új szabvány, új hardverekkel. Plusz, a WEP-nél használatos gyenge 24 bites IV kulcs helyett 48 bitet használ.

„Megfűszerezve" a TKIP eljárással (Temporal Key Integrity Protokoll). A TKIP 3 új mechanizmussal segíti a WPA-t. Csomagonkénti kulcscsere, csomagoknak sorozatszámuk van (amire az IV-t használja fel, az üzenet visszajátszás ellen) és a MIC (alias Michael, Message Integrity Code). A fizikai egyezés, a csip azonossága miatt, így csak egy firmware upgrade szükséges és egy jóval erősebb titkosításhoz jut a felhasználó.

Ezzel szemben a WPA2 már egy szintekkel erősebb blokkrejtjelezőt használ, ami az AES (Advanced Encryption Standard) és ehhez egy új kódolási módot definiáltak, ami a CCMP (CTR (Counter), CBC-MAC (Chipher Block Chaining – Message Authentication Code) Protokoll) nevet kapta. 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.

Kapcsolódás

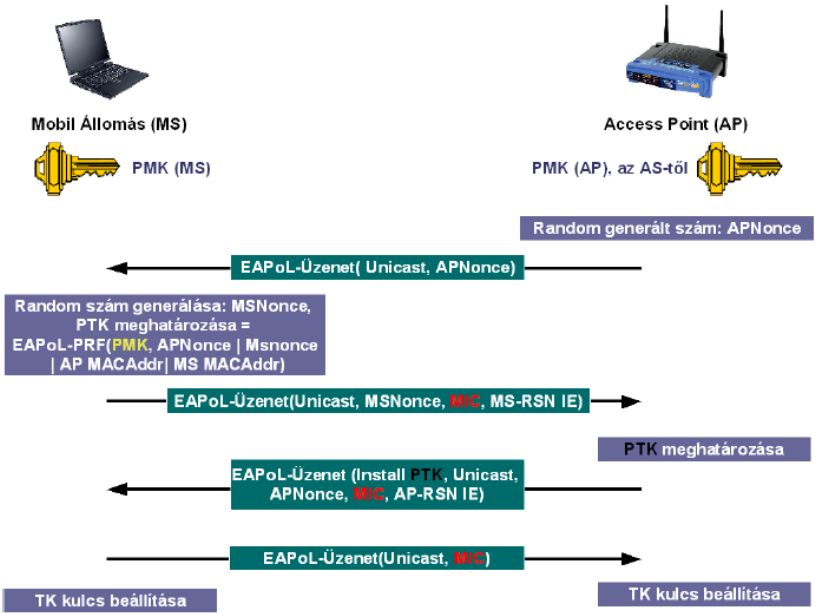
Két részre osztható. Az egyik a felderítés, a másik maga az autentikáció.



4. ábra.

A felderítés egy bemutatkozás a két fél között. A kliens küld egy *probe request*-et az AP-nak, majd az visszaküld egy *probe response* választ olyan információ csomaggal, mely tartalmazza, hogy milyen titkosításokkal lehet hozzá csatlakozni. Ezt követően nyílt autentikáció következik, melyben ellenőrzi az AP, hogy a STA csatlakozhat-e hozzá. Ha igen, akkor a STA küld egy *association request*-et, melyben közli az AP-tal, hogy ő ezekre a titkosításokra képes. Ha ez megfelel az AP titkosítási eljárásai valamelyikének, akkor egy *association response*-zal válaszol, így már félig megtörtént a kapcsolatfelvétel.

Autentikáció



5. ábra. WPA autentikáció

Ezek után következhet az autentikáció, amit 4-utas kézfogásnak hívnak. Természetesen a PMK-t (Pairwise Master Key), vagyis a titkos kulcsot mind a két fél ismeri, amiből számolják a többi ideiglenes kulcsot (pl. TK – Temporary Key).

- Az AP generál egy véletlenszerű számot (AP-nonce)
  - EAPoL-üzenet (Unicast, APNonce)
- A STA az AP-nonce-ból, a saját STA-nonce-ból, a saját és az AP MAC címéből generál egy úgynevezett PTK-t (Pairwise Transient Key)
  - EAPoL-üzenet (Unicast, STA-nonce, MIC (Message Integrity Code), STA-RSN IE(Robust Security Network Information Element)
- Az AP meghatározza a PTK-t (ami meg kell egyezzen a kliens PTK értékével)
  - EAPoL-üzenet (Install PTK, Unicast, AP-nonce, MIC, AP-RSN IE)
- TK alkalmazása
  - EAPoL-üzenet (Unicast, MIC)
- TK használata.

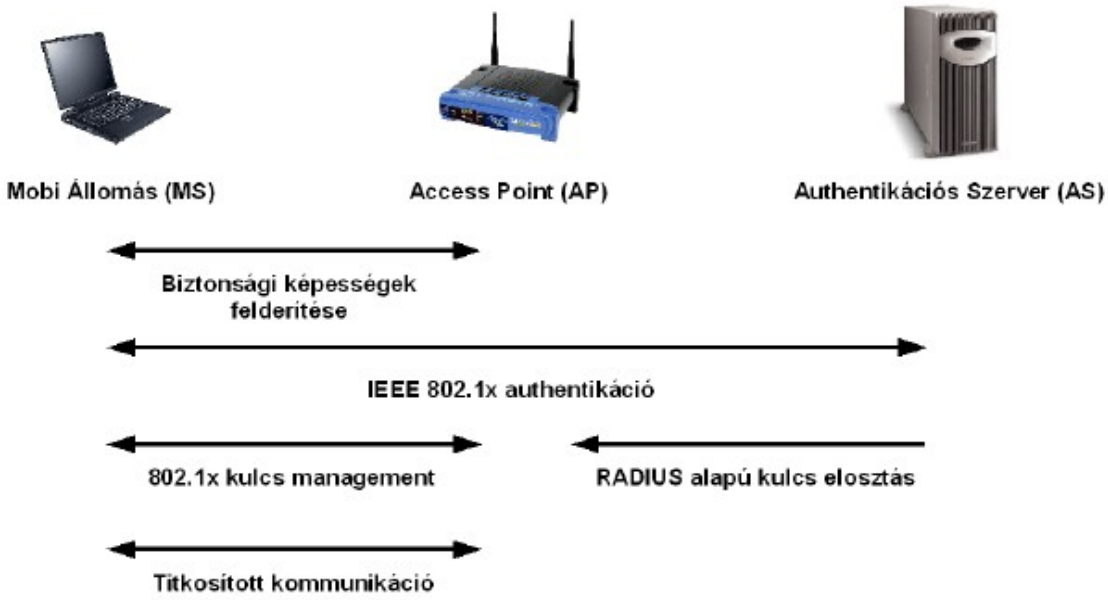
megj.: a WPA-PSK nem EAPoL, hanem normális üzenetekkel történik. de a felépítése, vagyis a 4-utas kézfogás ugyanaz. Az írásbeli magyarázathoz kiegészítés: az EAPoL-üzenet (EAP (Extensible Authentication Protocol) over LAN) megy át a csatornán, a többit az AP, ill. a STA végzi).

Ha megszakadna bármilyen oknál fogva az AP és a STA között a kommunikáció („látótávolságon” kívül esnek egymástól, roaming ...), akkor mindez lezajlik minden egyes újracsatlakozásnál (ezt használják ki, akár elősegítve mindezt direkt módon a hacker-ek, hogy feltörjék a hálózatunk jelszavát, a PMK-t).

IEEE 802.1x

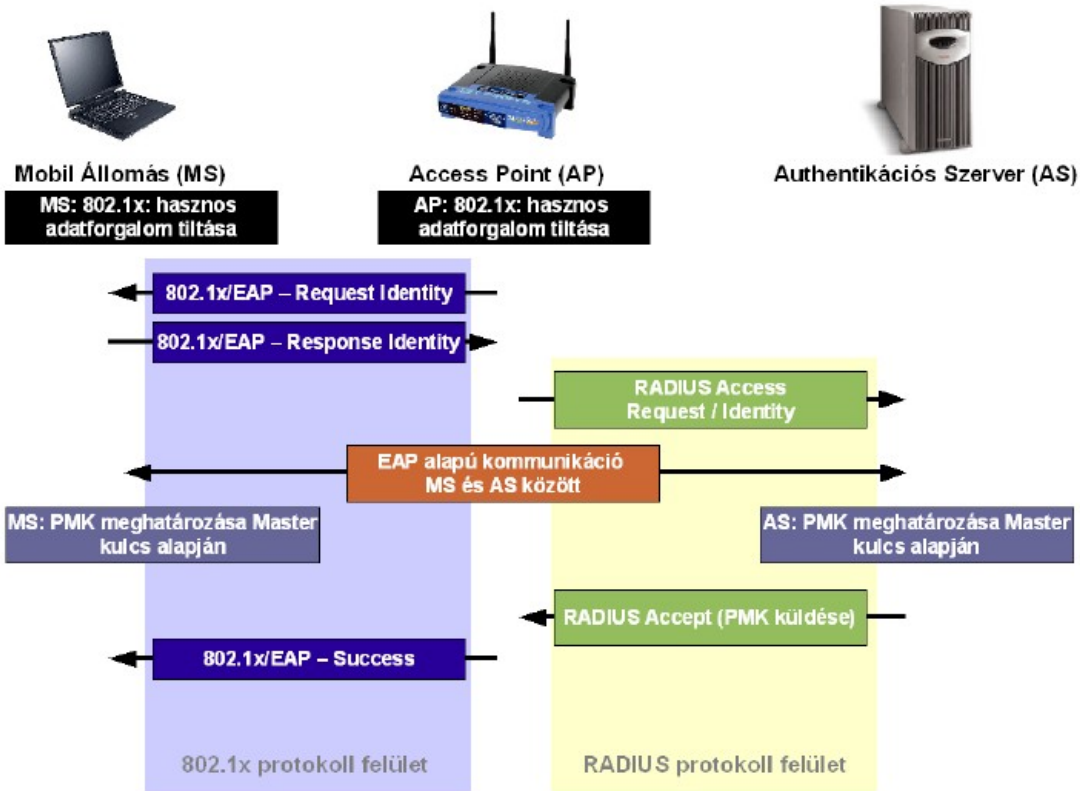
Inkább a vezetékes hálózatoknál elterjedt protokoll, ami az EAP-ot (Extensible Authentication Protocol) és annak alváltozatait használja autentikációra a vezeték nélküli hálózatoknál (EAP/TLS, EAP/TTLS-GTC, PEAP/MSCHAPv2, EAP/FAST, LEAP...).
Ez nagyon hasonlít a 802.11i-re, de ennél a kapcsolatnál nem az AP végzi az autentikációt, hanem egy autentikációs szerver (AS – authentication server), ami vezetéken csatlakozik a AP-hoz. mivel rengeteg verziója létezik, ezért itt elég megnézni az ábrákat.

Kapcsolódás



6. ábra. Autentikációs szerverrel rendelkező hálózathoz való kapcsolódás

Biztonság, autentikáció



7. ábra. Autentikációs szerverrel rendelkező hálózat autentikációs folyamata

készítette:Rabb Gergely a Széchenyi István Egyetem JÁI Távközlési Informatika tanszékék Számítógép hálózatok és Protokollok és szoftverek című tantárgyaihoz
emil: rabb.gergely@gmail.com
felhasznált irodalom: http://www.wikipedia.org http://google.hu

Wyonair – Biztonságos WiFi megoldások, http://www.wyonair.com weboldal
Tóbi Tamás - WLAN authentikációs eljárások vizsgálata, Diplomaterv
további jegyzetek emilben érhetőek el.