**20. tétel**

**Hálózati ismeretek – Otthoni és kisvállalati hálózatok gyakorlat (3.2.1)**

Jellemezze a vezeték nélküli hálózatokat a sebezhetőség szempontjából! Mutassa be a vezeték nélküli otthoni hálózatok alapszintű biztonsági beállításait! Ismertesse a vezeték nélküli hálózatok hitelesítési és titkosítási lehetőségeit! A rendelkezésre álló vezeték nélküli eszközön állítsa be a vezeték nélküli elérést a következő paraméterekkel és csatlakoztasson hozzá egy klienst:

***IP:*** *192.168.10.100/24*

***Jelszó:*** *Password123*

***SSID:*** *Liska*

***Titkosítás:*** *WPA2 TKIP*

***Kulcs:*** *Erett1234*

***Szempontok a tartalom rész értékeléséhez***

− A vezeték nélküli hálózatok sebezhetősége (pl.: elkapható forgalom, hitelesítés problémája, hálózathoz való hozzáférés könnyűsége)

− A vezeték nélküli hálózatok alapszintű biztonsági beállításai (alap IP-cím megváltoztatása, alapértelmezett jelszó megváltoztatása, SSID rejtése, MAC cím-szűrés stb.)

− A vezeték nélküli hálózatok hitelesítési és titkosítási lehetőségei (nyílt, hitelesített és titkosított elérés, helyi adatbázis vagy hitelesítő szerver használatával védett hozzáférés; WEP, WPA, RADIUS, TKIP, AES)

A vezeték nélküli eszközök elektromágneses hullámokat használva cserélik az információkat egymás közt.

Ezeket a hálózatokat védő titkosítási szabványokat, és ezeknek hiányát lejjebb láthatjuk.

***Titkosítási szabványok***

***A WEP***

(*vezetékessel egyenértékű titkosság*) volt az első ilyen jellegű szabvány. A problémája a könnyen feltörhető kódolása (alátámasztva több adatvédelemmel foglalkozó oldal által), körülbelül 4-5 perc alatt feltörhető. WEP titkosítás ugyan védelmet nyújthat az alkalmi próbálkozók ellen, de hamis biztonságérzetet ad, hiszen ingyenes, bárki számára hozzáférhető eszközökkel – mint például az aircrack-ng programcsomag – megfelelő jelerősség esetén nagyon egyszerűen visszafejthető a WEP kulcs. A titkosított csomagok lehallgatása után az aircrack-ng másodpercek alatt megtalálja a használt kulcsot. A szükséges csomagok akkor is kikényszeríthetőek, ha senki se kapcsolódik a hálózatra vezeték nélkül!

Többek között a „social engineering” is szóba jöhet, ami azt jelenti, hogyha egynél több ember tud egy titkot (pre shared key/\*jelszó\*), akkor a nem titok, és ki lehet deríteni (kisebb-nagyobb energia befektetéssel).

A WEP szabványt kevésbé használják nagyobb cégek, adminisztratív problémái, és a fent említett hátrányai miatt.

Ha eszközünk támogatja a WPA-t, akkor inkább használjuk azt, mert a WEP nyilvánvalóan gyengébb biztonságot nyújt a WPA-hoz képest. Ha a WPA-t nem támogatja eszközünk, akkor lehetőleg minden nap cseréljünk WEP kulcsot, de legalábbis olyan gyakran, ahogy csak tehetjük.

Ezek mellett gyakori a hálózati kártyák fizikai címének (MAC) szűrése, bár ez a szűréstípus egyszerűen kijátszható.

802.11-es típusú WEP hálózatokhoz használt feltörő programok:

* AirSnort
* BSD-Airtools
* WEP Crack
* WEP Attack
* WEPWedgie

Rövid összefoglaló:

* Könnyen feltörhető
* A leggyengébb titkosítási szabvány
* Ingyenes
* Egy átmeneti állapot a védelmi szabványok történelmében

**A *WPA***

(*Wi-Fi védett hozzáférés*) egy 2003 óta élő titkosítási szabvány, ma már szinte minden eszköz támogatja – erősen ajánlott használni a WEP helyett. A WPA a TKIP nevű titkosító algoritmust használja az adatok titkosítására.

(A TKIP fő előnye, hogy a beállított idő vagy forgalmazott adatmennyiség után új kulcsot generál.)

Igazi biztonságot a WPA is csak akkor nyújt, ha kellően hosszú és összetett jelszót használunk, amivel elkerülhetjük a brute force, illetve a szótár alapú támadásokat.

(A **brute force** lényegében a „próbáljuk ki a világ összes lehetőségét”, mert gyakorlatban ez történik)

Az osztott (Pre-shared) kulcs módot (PSK, más néven „Personal” mód) azon otthoni és kisirodai felhasználóknak fejlesztették ki, akik nem tudnak megengedni (ára és bonyolultsága miatt) egy dedikált 802.1x kiszolgálót. Az összes felhasználó a „phassphrase”-el éri el (lényegében ez egy hosszabb jelszó).

[A 802.1x kiszolgáló minden felhasználóhoz különálló kulcsot rendel (fent említett „passphrase”-t) a nagyobb biztonság fenntartása érdekében]

A jelszónak 8-63 darab nyomtatható ASCII karakterből vagy 64 darab hexadecimális számjegyből (256 bit) kell állnia.

Megnövelhető a biztonság egy PBKDF2(Cryptography - “ titkosírás”) kulcsgenerálási függvény használatával.

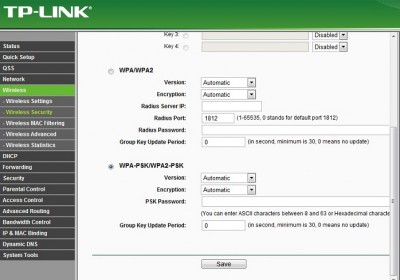
(A maximális WPA-PSK védelemhez (256 bit) olyan kulcs kell, ami 54 véletlenszerű karaktert, vagy 39 véletlenszerű ASCII karaktert tartalmaz.)

Rövid összefoglaló:

* A 802.1x kiszolgáló nem ingyenes, felhasználása a laikusoknak bonyolult
* A jelszavak újragenerálódnak = a „brute force” végzete

**A *Radius***

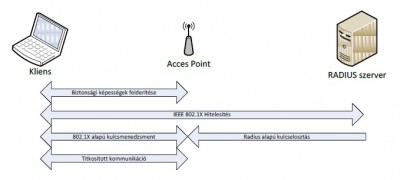
A legkézenfekvőbb megoldás a Radius, amely WPA alapú titkosításra épül.

[](https://logout.hu/dl/upc/2012-07/126917_wparadius.jpg)  
TP-LINK router radius beállításai

Ez az úgynevezett EAP alapú hitelesítés. Az EAP (Extensible Authentication Protocol, Kiterjeszthető Hitelesítési Protokoll) hitelesítési eljárás, és átviteli technológia, ami eredetileg az EAPOL (EAP Over Lan) protokollból lett fejlesztve, hogy megfeleljen az egyéb hálózati technológiák, többek között a vezeték nélküli hálózatokon való hitelesítéshez is.

Bár az adatátvitel a fizikai réteg felett történik speciális EAP keretüzenetek formájában, az access point és a kapcsolódni kívánó eszköz EAP keretüzeneteket használva kommunikálnak egymással.

A hitelesítés és azonosítás nem a fizikai rétegben történik, hanem felsőbb rétegekben, így jóval kifinomultabb lehet az azonosítás és hitelesítés.

[](https://logout.hu/dl/upc/2012-07/126917_hitelesites.jpg)  
Hitelesítés folyamata

A RADIUS (Remote Authentication Dial-In User Service) nem képezi szerves részét a vezeték nélküli titkosítási és azonosítási szabványoknak. A RADIUS szolgáltatásra vonatkozó ajánlás fő célja, hogy a más környezetben (eredetileg modemes internethez) már bevált protokollt vezeték nélküli hálózatban alkalmazza. A RADIUS egy adatbázis-alapú szolgáltatás, amely az access pointtal kommunikálva ellenőrzi és hitelesíti a kapcsolódni kívánó fél jelszavait és tanúsítványait saját adatbázisa alapján.

A fentiekből látszik, hogy ehhez az azonosításhoz szükség van egy, általában a hálózaton belül futó szolgáltatásra. Szerencsére ez nem egy túl erőforrásigényes dolog, ha van otthon egy kisebb szerver adattárolásra, letöltésre, azon bőven elvan egy RADIUS szolgáltatás is. És persze léteznek ingyenes megoldások Windows és Linux környezetre. Valamint a szerver, így router is hitelesíthető tanúsítvánnyal, nem kell attól tartani, hogy harmadik fél állna be a kapcsolatba.

Hatalmas előnye, hogy itt már a RADIUS szerveren beállítható, hogy történjen naplózás, és egyéni felhasználónév/jelszó párosokat is kreálhatunk, akár időkorláttal is, maximális próbálkozások számának beállításával is. Egy darabig el lehet szórakozni, mire bárki feltöri, de nem lehetetlen.

Persze nem csak felhasználónév/jelszó páros lehet a hitelesítés módja. Lehet tanúsítvány, valamilyen hardverkulcs, SIM kártya.

Néhány típusa:

• **EAP-TLS:** Digitális tanúsítványokon alapul.

• **EAP-TTLS:** Szerver oldalon tanúsítvány, kliens oldalon felhasználónév és jelszó.

**• PEAP:** Hasonló az EAP-TTLS-hez, a Cisco és Microsoft támogatja ezt a szabványt.

**• EAP-SIM:** SIM kártya alapú hitelesítés.

**• EAP-LEAP:** Felhasználónév és jelszó alapú, nem igényel hitelesítést a szerver részéről.

Az EAP sem tökéletes, néhány kapcsolódási módszer beállítása egy átlagember számára elég nehéz, nagy terjedelmű mankót igényel, és a siker még így sem garantált (kipróbáltuk, kudarc lett).

***Hitelesítés***

Minden eszköznek a forgalmazás megkezdése előtt hitelesítenie kell magát az AP felé (Access Point),

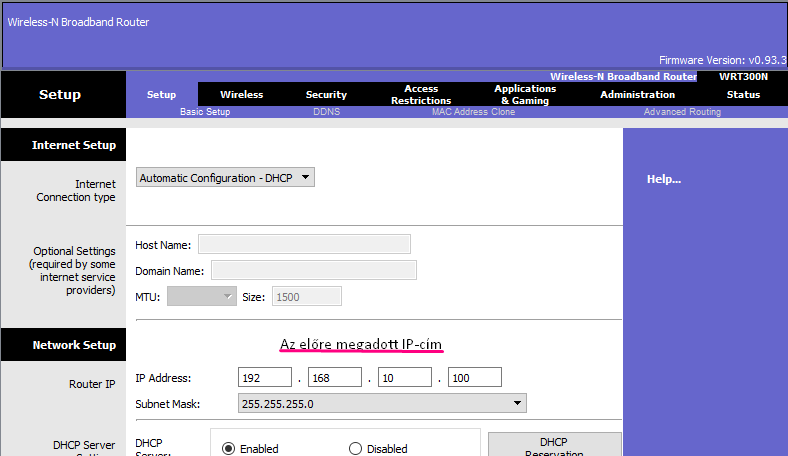
Mely egy négy lépcsőből álló üzenetváltásból áll.

1. A mobil állomás jelzi egy „authenticate request” küldéssel a hitelesítési szándékát az AP felé.
2. Az AP generál egy véletlenszerű számot és azt elküldi a mobil állomásnak. Ez az authenticate challenge”
3. A mobil állomás rejtjelzi ezt a számot a beállított WEP kulcsával és visszaküldi az eredményt az AP-nak „authenticate respond” formában.
4. Ha az AP ezt dekódolni tudja, akkor a két eszközön beállított kulcs egyezik, tehát az állomás csatlakozhat a hálózathoz.

***Gyakorlati példa***

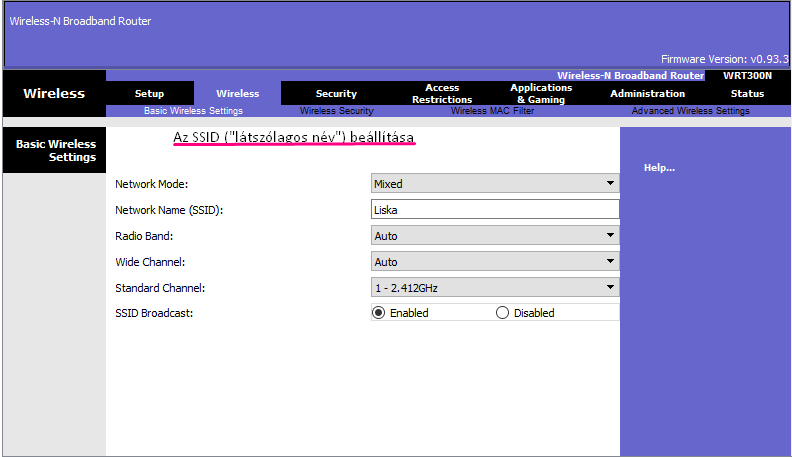
**A következő példa az IP cím megadását mutataj be.**

Ehhez a vezeték nélküli routerünk GUI ( Graphic User Interface ) –ébe kell belépnünk,és ott a „Setup”,majd „Basic Setup” almenüpontra van szükségünk.



**A következő példa az SSID beállítását mutaja be.**

Az SSID beállításához a „Wireless” menüpont első alpontjára lesz szükségünk,azaz a „Basic Wireless Settings”-re. Itt elég nyilvánvalóan a „Network Name” utáni textboxba beírt szöveg fog megjelenni ezentúl, mint a hálózatunk neve.



**A következő példa a titkosítással foglalkozik.**

A „Wireless” menüpont „Wireless Security” almenüpontjában beállíthatjuk a kívánt paramétereket,itt a mintán láthatóakat.

