WLAN hálózatok védelme

Hálózatbiztonság

- Könnyű sebezhetőség
- Nehezen észlelhető a támadás
- Levegő az átviteli közeg
- Stb.

Védelem

- SSID szórás kikapcsolása
  - Így ismerni kell az SSID-t
  - Tikosítatlan szöveg formájában továbbítódik
- Alapértelmezett jelszó, IP cím megváltoztatása
  - Alapszintű védelem a felderítő programok ellen
- MAC cím szűrés
  - Előre létrehozott lista
  - Támadó átállíthatja a saját MAC címét

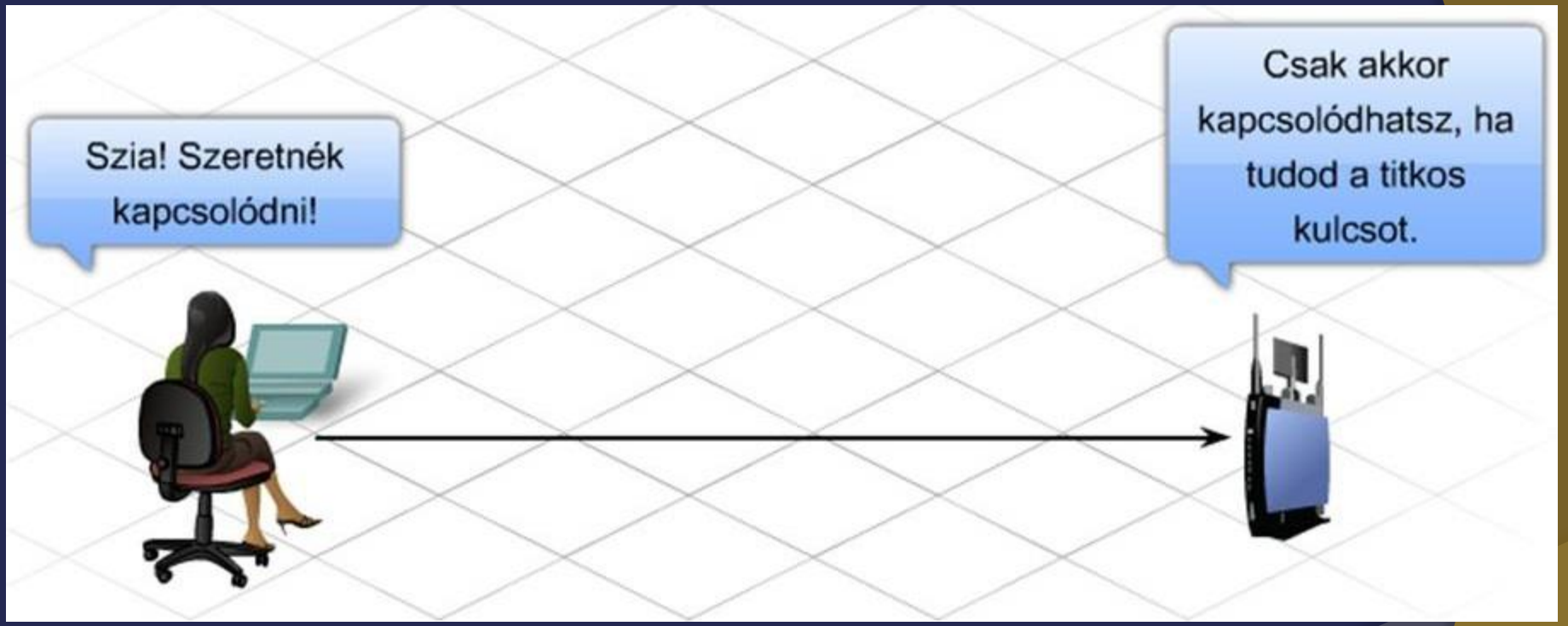
Védelem

- Hitelesítés
  - Jelszó és felhasználónév a leggyakrabb formája
  - WLAN-ba történő belépés előtt megtörténik
- Titkosítás
  - Átvitt adatok védelme
  - Az elfogott információk használhatatlanok lesznek
- Forgalomszűrés

Hitelesítés

- Nyílt hitelesítés
  - Minden vezeték nélküli eszköz tud csatlakozni
  - Közhasznú hálózatok: iskola, étterem
- Előre megosztott kulcs (PSK)
  - AP-n és ügyfélen ugyanazt a kulcsot kell beállítani
  - Egyutas hitelesítés, csak az állomás hiteles
  - A felhasználót és AP-t nem hitelesíti

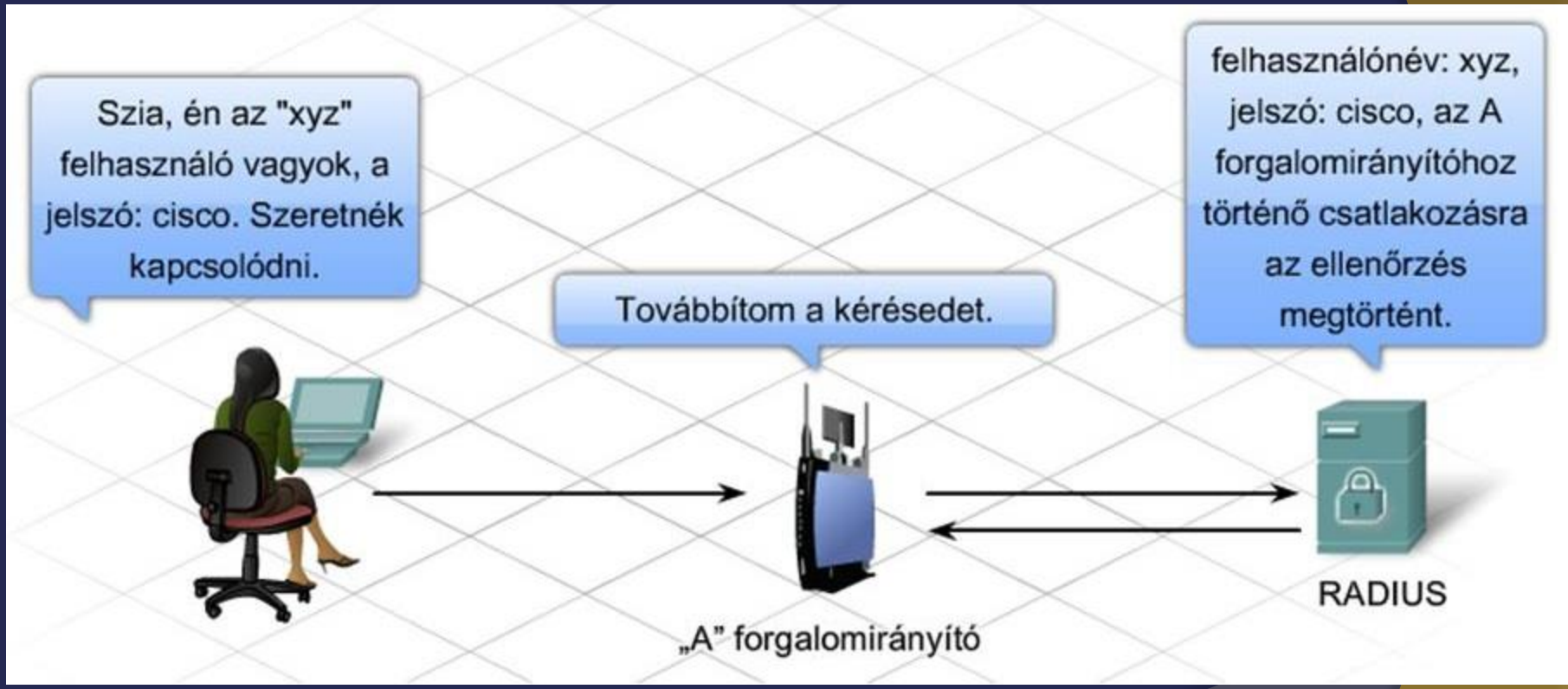
PSK


Szia! Szeretnék kapcsolódni!
Csak akkor kapcsolódhatsz, ha tudod a titkos kulcsot.

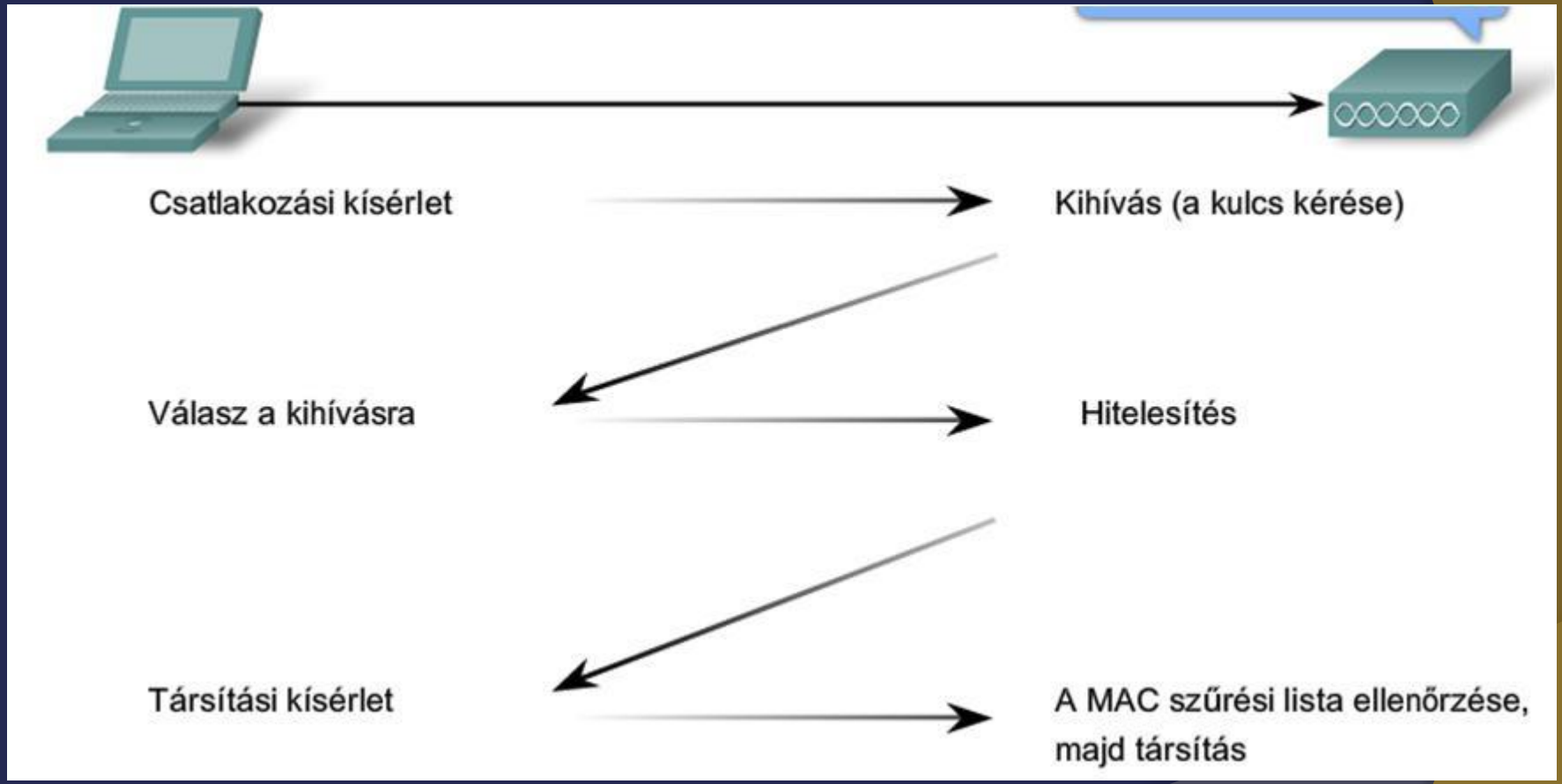
Hitelesítés

- Kiterjeszthető Hitelesítési Protokoll (EAP)
  - Kétutas hitelesítés, felhasználó is azonosítja magát
  - Hitelesítő szerver: RADIUS
    (Remote Authentication Dial-in User Service)
  - Adatbázis a jogosult felhasználókról

EAP Extensible Authentication Protocol



Hitelesítés, társítás



Titkosítás

- Vezetékessel egyenértékű protokoll (Wired Equivalency Protocol, WEP)
  - Statikus állandó kulcsok → megfejthető
  - Gyakori változtatás
  - 64, 128 esetleg 256 bit hosszú kulcsok
  - Passphrase *(összetett jelszó, jelmondat)*
  - Összes állomáson ugyanazt a kulcsot kell beállítani

WEP

A Wired Equivalent Privacy (WEP) = Vezetékessel Egyenértékű (Biztonságú) Hálózat mára már egy korszerűtlen algoritmus az IEEE 802.11-ben megfogalmazott vezeték nélküli hálózatok titkosítására.

A vezeték nélküli hálózatok rádiójelek segítségével sugározzák szét az üzeneteket, ami sokkal könnyebben lehallgatható, mint a vezetékes hálózatok.

WEP

A WEP 1997-es bemutatásakor arra szánták, hogy hasonló bizalmas hálózatként működjön, mint egy általános vezetékes hálózat.

WEP

2001 elején néhány komoly gyengeséget találtak rajta a kriptográfiai szakemberek, amik miatt ma a WEP protokollal titkosított hálózati kapcsolatokat percek alatt fel tudják törni egyszerű szoftverek segítségével.

WEP

Néhány hónapon belül az IEEE egy új szabványt indítványozott, hogy ellensúlyozza a problémát, ez volt a **802.11i**.

2003-ban a Wi-Fi Alliance (= Wi-Fi Szövetség) kihirdette, hogy a WEP-et hatálytalanítja a

Wi-Fi Protected Access (WPA) = Wi-Fi Védett Hozzáférés, ami a 802.11i módosítás része volt.

WEP

2004-ben az egész 802.11i szabvány jóváhagyásakor (aka WPA2), az IEEE kijelentette, hogy mind a WEP-40, mind a WEP-104 érvénytelenné válik, mivel nem felelnek meg a biztonsági előírásoknak.

A gyengeségei ellenére a WEP protokollt még mindig széles körben használják.

Általában ez az első, amit a router-ek lehetőségként felkínálnak a felhasználó számára, mivel azokat elriasztják a különböző biztonsági szintek, amiket legfeljebb csak véletlenül használnak

WPA

A **Wi-Fi Protected Access** (**WPA** és **WPA2**) a vezeték nélküli rendszerek egy, a **WEP**-nél biztonságosabb protokollja.

A létrehozása azért volt indokolt, mert a kutatók több fontos hiányosságot és hibát találtak az előző rendszerben (**WEP**).

WPA

A WPA tartalmazza az IEEE 802.11i szabvány főbb szabályait, és egy átmeneti megoldásnak szánták, amíg a 802.11i szabványt véglegesítik.

A WPA úgy lett kialakítva, hogy együttműködjön az összes vezeték nélküli hálózati illesztővel, de az első generációs vezeték nélküli elérés pontokkal nem minden esetben működik.

WPA

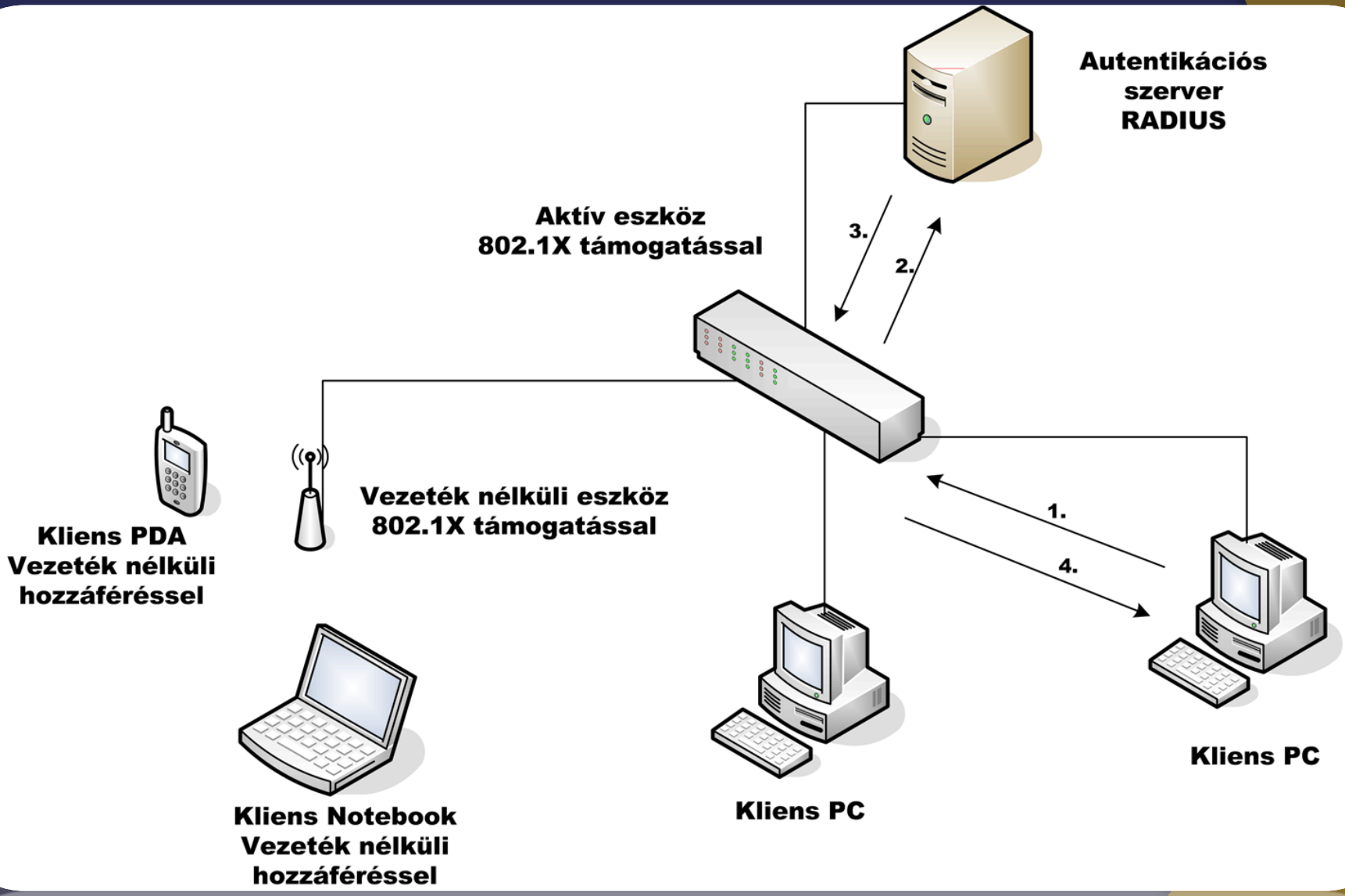
A WPA2 a teljes szabványt tartalmazza, de emiatt nem működik néhány régebbi hálózat kártyával sem.

Mindkét *(WPA, WPA2)* megoldás megfelelő biztonságot nyújt, azonban jelentkezik két jelentős probléma…

WPA problémák

- Vagy a WPA-nak, vagy WPA2-nek engedélyezettnek kell lennie a WEP-en kívül. A telepítések és beállítások során inkább a WEP van bekapcsolva alapértelmezettként, mint az elsődleges biztonsági protokoll.
- A „Personal” (WPA-PSK) módban - amit valószínűleg a legtöbben választanak SOHO környezetben, a megadandó jelszónak hosszabbnak kell lennie, mint a jellegzetes 6-8 karakter, amit az átlagfelhasználók általában még elfogadhatónak tartanak.

WPA/WPA2 működése



WPA-PSK

A WPA vagy WPA2 hálózatok esetében PSK vagyis Pre-shared key (előre megosztott kulcs) módban a hozzáféréshez szükséges biztonsági kulcsot előre megkapjuk, így nincs szükség összetett 802.1x azonosító server konfigurálására a hozzáférési pontnál.

Minden felhasználónak egyszerűen csak a megadott kódot kell beütnie hogy beléphessen a hálózatba.

WPA-PSK

A kód 8-tól 63 nyomtatott ASCII karakterig terjedhet, vagy 64 hexadecimális szám lehet.

A megoldás gyengéje, hogy a felhasználók hajlamosak egyszerű, „sérülékeny” jelszavak megadására, melyek könnyebben feltörhetőek.

A közvetlen próbálgatások útján történő jelszó visszafejtéses támadások kivédésére használjunk teljesen véletlenszerűen generált jelszavakat, melyek legalább 20 vagy még inkább legalább 35 karakter hosszúak.

WPS - WiFi Protected Setup

- a WiFi Szövetség opcionális WiFi Protected Setup (WPS) ajánlásának megfelelő termékek, melyek gyártói biztosítják, hogy a készülékek a legegyszerűbben elérhető módon legyenek beállíthatók - megfelelő biztonsági szint alkalmazása mellett.
- A WiFi Protected Setup legalább a felére csökkenti a beállításhoz szükséges lépéseket.