**A vezeték nélküli átvitel jellemzői**

A **vezeték nélküli közegek rádió- vagy mikrohullámok haszná**latával továbbítják az **elektromágneses jeleket**, amelyek az adatkommunikáció bináris számjegyeinek felelnek meg.

A **vezeték nélküli átvitel biztosítja a legnagyobb mobilitást az összes közegtípus k**özül, emellett a vezeték nélküli eszközök száma is folyamatosan növekszik. Mostanra a felhasználók **leginkább vezeték nélkül csatlakoznak az otthoni és vállalati hálózatokhoz.**

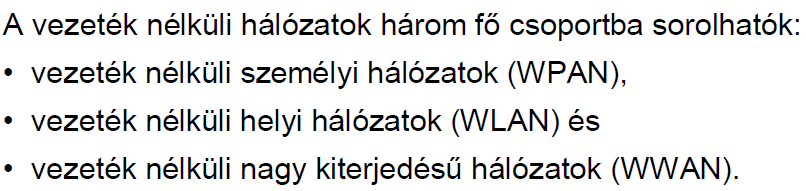
**A vezeték nélküli átvitel korlátai a következők:**

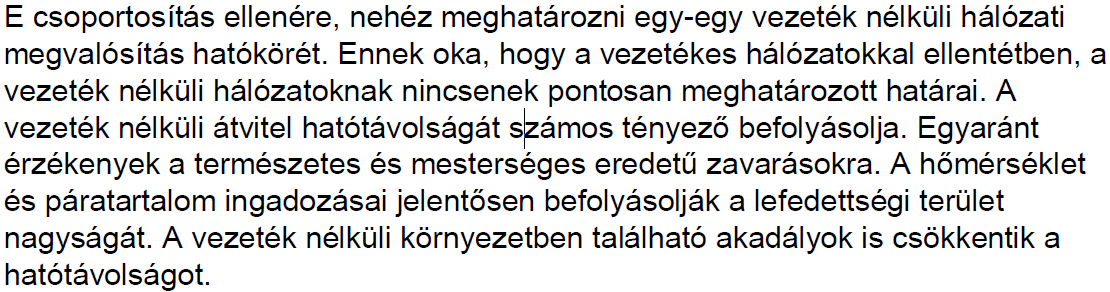
* **Lefedettségi terület** - A vezeték nélküli adatátviteli technológiák kiválóan működnek szabadtéren. Ugyanakkor az épületekben használt egyes építési anyagok és a helyi földrajzi viszonyok korlátozzák a tényleges lefedettséget.
* **Interferencia** - A vezeték nélküli átvitel érzékeny az interferenciára, és olyan hétköznapi eszközök is zavarhatják az átvitelt, mint például a vezeték nélküli telefonok, bizonyos fénycsőtípusok, mikrohullámú sütők és más vezeték nélküli eszközök.
* **Biztonság** - A lefedettségi területen belül nem kell fizikailag a közeghez kapcsolódni annak használatához. Emiatt az erre nem jogosult eszközök és felhasználók is hozzáférhetnek a hálózathoz. A hálózatbiztonság a vezeték nélküli hálózatok felügyeletének egyik fő összetevője.
* **Osztott átviteli közeg** - A WLAN-ok fél-duplex módban működnek, ami azt jelenti, hogy egyidejűleg csak egy eszköz végezhet adatküldést vagy fogadást. A vezeték nélküli közeg az összes vezeték nélküli felhasználó között meg van osztva. Ha a WLAN-hoz egyszerre több felhasználó is hozzáfér, akkor az minden felhasználó számára csökkenti a sávszélességet.







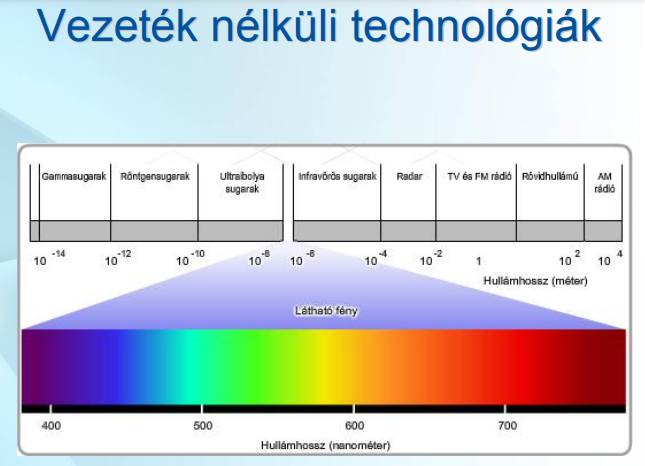




**A vezeték nélküli átvitel típusai**

**A vezeték nélküli átvitelre vonatkozó IEEE és ipari távközlési szabványok mind az adatkapcsolati, mind pedig a fizikai rétegre kiterjednek**. Ezen szabványok mindegyikének a fizikai rétegre vonatkozó specifikációja a következő területeket foglalja magában:

* Az adatok rádiójelekké történő átalakítása
* Átviteli frekvencia és teljesítmény
* A jel vételére és dekódolására vonatkozó követelmények
* Antennák tervezése és kivitelezése



**A vezeték nélküli szabványok a következők:**

* **IEEE 802.11**: A vezeték nélküli LAN (WLAN) technológia, közismertebb nevén Wi-Fi, egy versengés alapú vagy nem determinisztikus rendszer, amely az ütközést elkerülő, vivőérzékeléses, többszörös hozzáférésű (Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) rendszert használja a közeghozzáférés vezérlésére.
* **IEEE 802.15**: A vezeték nélküli személyes hálózatok (Wireless Personal Area Network, WPAN) szabványa, közismert nevén a Bluetooth, amely egy eszközpárosítási folyamatot használ az 1 és 100 méter közötti kommunikáció lebonyolítására. **Átviteli sebesség max.: 3Mb/s.**
* **IEEE 802.16**: Közismert nevén a WiMAX (Worldwide Interoperability for Microwave Access), amely pont-multipont topológiát használ a szélessávú vezeték nélküli hozzáférés biztosításához. **Átviteli sebesség max.: 1Gb/s. (2004-től szabvány)**

Ezen [hálózat](https://www.mimi.hu/informatika/halozat.html#maintitle)ok sebessége és hatótávolsága többszöröse a jelenlegi Wi-Fi hálózatoknak, és lehetővé tesznek min. akár 100 Mbps-os sebességet, 20-40 km-es távolságba.  Fix, mobil és hordozható eszközöknél alkalmazható szélessávú adatátvitel. Wimax 2 eléri az 1 Gbit/s átviteli sebességet.

## Vezetéknélküli LAN:

A vezeték nélküli hálózat közös adatátviteli közege lehetővé teszi az eszközök számára, hogy vezeték nélkül csatlakozzanak egymáshoz egy LAN-on keresztül. Egy WLAN általában a következő hálózati eszközök használatát követeli meg:

* **Vezeték nélküli hozzáférési pont (Access Point, AP)** - Fogadja a felhasználók vezeték nélküli jeleit, és csatlakozik a meglévő rézvezetékes hálózathoz, például az Ethernethez. Az otthoni és kisvállalati környezetben használt vezeték nélküli router egy eszközben tartalmazza a router, a switch és a hozzáférési pont funkcióit. A képen egy ilyen eszköz látható.
* **Vezeték nélküli hálózati adapterek** - Vezeték nélküli kommunikáció képességét biztosítják a hálózati állomásoknak.

A technológia fejlődésével számos Ethernet alapú WLAN szabvány alakult ki. **Vezeték nélküli eszközök vásárlásakor meg kell győződni annak kompatibilitási és az együttműködési képességeiről.**

A vezeték nélküli kommunikáció előnyei nyilvánvalóak, különösen ha a költséges kábelezés megtakarításáról és a hordozhatóságból adódó kényelemről beszélünk. A hálózati rendszergazdának úgy kell megalkotnia és alkalmaznia a szigorú biztonsági szabályokat, hogy a vezeték nélküli LAN védve legyen az illetéktelen hozzáférésektől és támadásoktól.

**Infravörös:** 

* alacsony energiaszintű, és jelei nem képesek áthatolni a falakon vagy egyéb akadályokon
* Az infravörös sugarakat az [emberi szem](https://hu.wikipedia.org/wiki/Emberi_szem) már nem képes fényként érzékelni, a bőr melegérző idegvégződései viszont képesek „meleg érzetként” felfogni.
* csak pont-pont típusú kapcsolatot tesz lehetővé
* kis hatótávolságú, rálátást igénylő kommunikációra használják
* nagyobb távolságok esetén, magasabb frekvenciájú elektromágneses hullámok használatára van szükség

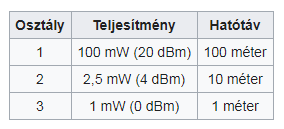
**Felhasználási területek:**

* távirányítóknál
* Pc hardvereknél: bill., egér
* haditechnika: pozíció bemérésére, felmérésre és nyomkövetésre használják
* infravörös hősugárzóval való fűtés
* időjárás –megfigyelő műholdak méréseinél
* óceánok áramlásának megfigyelése
* mezőgazdaság és erdőgazdálkodás is alkalmazza az infravöröst érzékelő műholdak felvételeit
* sok madár és rovar érzékeli szemével

**Bluetooth**: https://upload.wikimedia.org/wikipedia/commons/thumb/f/fc/BluetoothLogo.svg/220px-BluetoothLogo.svg.png

* rövid hatótávolságú, adatcseréhez használt, nyílt, vezeték nélküli szabvány
* Alkalmazásával [számítógépek](https://hu.wikipedia.org/wiki/Sz%C3%A1m%C3%ADt%C3%B3g%C3%A9p), [mobiltelefonok](https://hu.wikipedia.org/wiki/Mobiltelefon) (telefonkihangosítók) és egyéb készülékek között automatikusan létesíthetünk kis hatótávolságú rádiós kapcsolatot
* az 1.2-es verzió 1 Mbps-os, a 2.0-s Bluetooth pedig 3 Mbps-os adatátviteli sebességet tesz lehetővé a világszerte szabadon elérhető 2,4 [gigahertzes](https://hu.wikipedia.org/wiki/Gigahertz) frekvenciasávban
* Európában és az Egyesült Államokban a 2,402 GHz és 2,480 GHz közötti 79 db 1 MHz-es sávban működik
* Az adatcsatorna ebben a sávban másodpercenként 1600-szor változik véletlenszerűen („szórt spektrumú frekvenciaugrás”)
* Egy hálózatban egy időben 1 „mester” eszközhöz legfeljebb 7 másik eszköz csatlakozhat.
* z egymáshoz csatlakozott eszközök ún. *personal-area network*-öt ([PAN](https://hu.wikipedia.org/wiki/PAN)), más szóval **piconet**-et hoznak létre, ami például az egy szobában lévő eszközök által alkotott hálózatot jelenti (vagy az autóban a mobiltelefon és a fejhallgató közötti kicsiny hálózatot).
* A Bluetooth alacsony energiafogyasztása miatt különösen alkalmas hordozható eszközök számára.

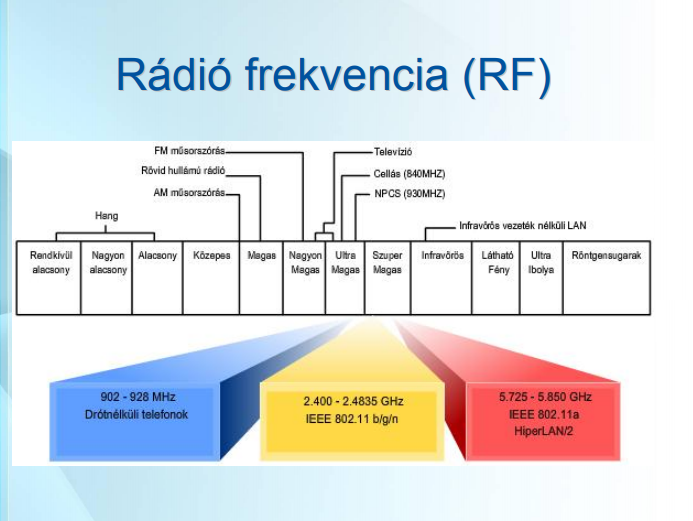
A készülékek osztályuktól függően az alábbi távolságon belül képesek kommunikálni:



**Felhasználási területek:**

* Vezeték nélküli hálózatok kialakítására **asztali és hordozható**[számítógépek](https://hu.wikipedia.org/wiki/Sz%C3%A1m%C3%ADt%C3%B3g%C3%A9p)**között**, illetve **csak asztali gépek között** kis területen, ha nincs szükség nagy sávszélességre
* Számítógép-perifériák csatlakoztatására **nyomtatók,**[billentyűzetek](https://hu.wikipedia.org/wiki/Billenty%C5%B1zet)**,**[egerek](https://hu.wikipedia.org/wiki/Eg%C3%A9r_(sz%C3%A1m%C3%ADt%C3%A1stechnika)) esetében
* Fájlok és adatok átvitelére és szinkronizálására személyi digitális asszisztensek ([PDA](https://hu.wikipedia.org/wiki/PDA)**-k,**[mobiltelefonok](https://hu.wikipedia.org/wiki/Mobiltelefon)**és a számítógép**) **között**
* **Egyes digitális zenelejátszók,**[fényképezőgépek](https://hu.wikipedia.org/wiki/F%C3%A9nyk%C3%A9pez%C5%91g%C3%A9p)**és számítógép között**
* **Autóskészletek és fülhallgatók csatlakoztatására mobiltelefonokhoz**
* **Orvosi és**[GPS](https://hu.wikipedia.org/wiki/Global_Positioning_System)**-készülékek**

**Rádiófrekvencia:** 



## 802.11

* sávszélesség (max): 2Mb/s
* használt frekvencia: 2,4GHz
* Apró sebesség a mai alkalmazásokhoz. Könnyű megérteni, miért nem találja meg a piacon az ilyen szabványnak megfelelő berendezéseket.

## 802.11a

* sávszélesség(max): 54Mb/s
* használt frekvencia: 5GHz
* **magasabb költségei** kevésbé népszerűvé tették, **csökkenti a jel lefedettségét**, nehézségekbe ütköznek a falakon és más tárgyakon. Előnye a kiváló sebesség és az egyéb háztartási készülékekkel való interferencia veszélyének megszüntetése

## 802.11b

* sávszélesség (max): 5,5Mb/s vagy 11Mb/s
* használt frekvencia: 2,4GHz
* **alacsony termelési költség, alacsony működési sebesség** és a kockázata az, hogy **zavarja a háztartási készülékeket** és a 2.4 GHz sávot használó egyéb eszközök.

## 802.11g

A legelterjedtebb változat.

* sávszélesség (max): 54Mb/s
* használt frekvencia: 2,4GHz
* **802.11g** sikeres volt **a 802.11a és az 802.11b kombinációja,** amely akár az **54 Mbps** sebességet is képes működtetni  a **2.4 GHz** frekvenciaspektrumban
* **felülről kompatibilis a 802.11.b-vel**

A továbbfejlesztett változatai: SuperG: 108Mb/s sebesség MIMO (multiple in, multiple out): több antennával a rádióhullámok visszaverődését is képes értelmezni, ezért nagyobb lefedettséget biztosít

## 802.11n

A legelterjedtebb változat.

* sávszélesség (max): 600Mb/s
* használt frekvencia: 2,4GHz, 5GHz
* **megnövekedett hatótávolsággal és átbocsátóképességgel rendelkezik**
* **felülről kompatibilis a 802.11.b és 802.11.g eszközökkel**

## 802.11ac

* sávszélesség (max): 1,3 Gb/s
* használt frekvencia: 5 GHz
* megjelenés dátuma: 2013. december 11.

## 802.11ad

* sávszélesség (max): 7,2 Gb/s
* használt frekvencia: 60 Ghz
* megjelenés dátuma: 2012. december
* hatótávolság: 1-10 m

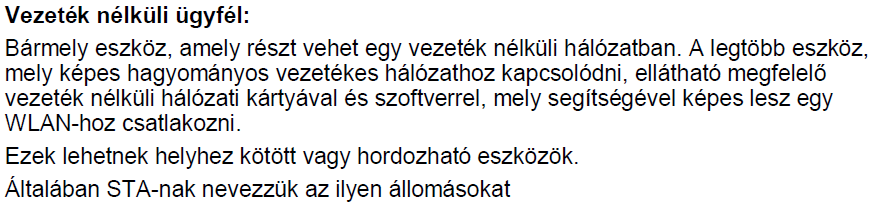
## Felhasználási területek

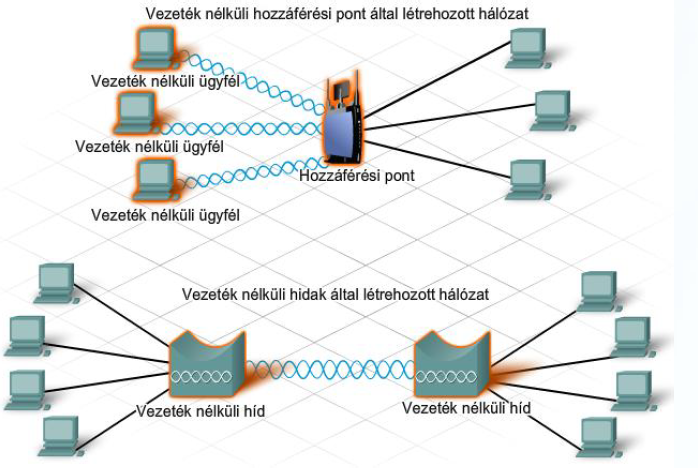
**Irodákban, nyilvános helyeken** (repülőtér, étterem, hotel, magánházak stb.) **megvalósított vezeték nélküli helyi hálózat**, aminek segítségével a látogatók saját számítógépükkel kapcsolódhatnak a világhálóra.

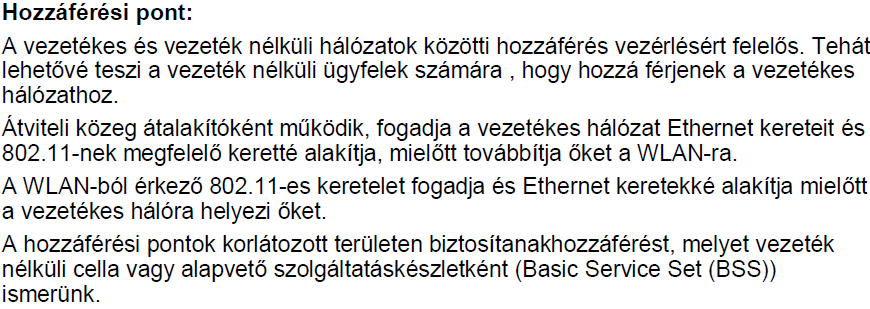
Kialakítása a következő módokon történhet:

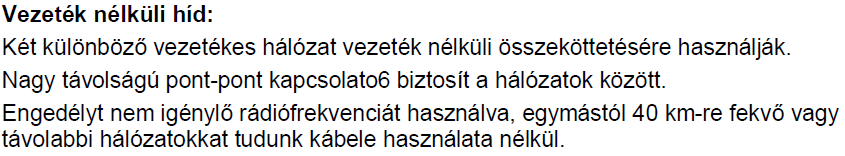
* **Publikus, nyílt hálózat**: **bármely wi-fi routerrel kialakítható, az így létrehozott hálózathoz bárki csatlakozhat mindenféle korlátozás nélkül**
* **Privát hálózat**: **a hálózat saját felhasználásra lett kialakítva, melyet egy titkos jelszó véd**, így ahhoz csak a jelszó ismeretében lehet csatlakozni
* **Publikus, zárt hálózat**: **egy speciális szoftver gondoskodik arról, hogy a hálózatot csak egy kód ismeretében, korlátozott ideig lehessen használni**. Ezt a formát rendszerint *éttermek, kávézók használják*, ahol az internetelérés fogyasztáshoz van kötve
* **Publikus, részlegesen zárt hálózat**: **átmeneti típus** **a nyílt és** egyben **publikus hálózatok**, illetve **a privát hálózatok közt**.
  + Két főbb típusa különböztethető meg,
    - a **hozzáférési pont számára elérhető sávszélesség** bizonyos, akár igen **elenyésző hányadának nyílt**, és publikussá tett formája,
    - illetve **egy szélesebb kör számára elérhető, publikus**, azonban **zárt hálózat** ismeretes.
* **Kereskedelmi HotSpot szolgáltatás**: **a vezeték nélküli hálózat csak díjfizetés ellenében, korlátozott ideig használható**

**WLAN összetevők:**

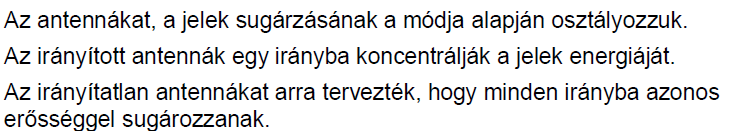


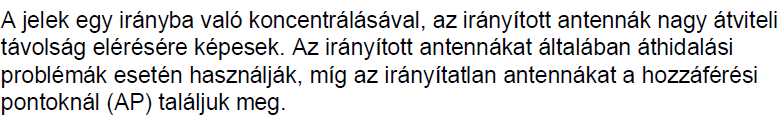




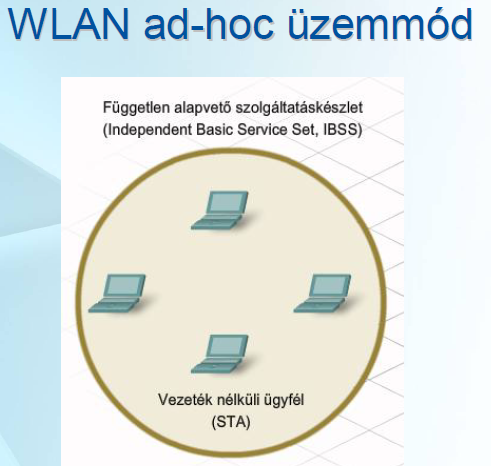


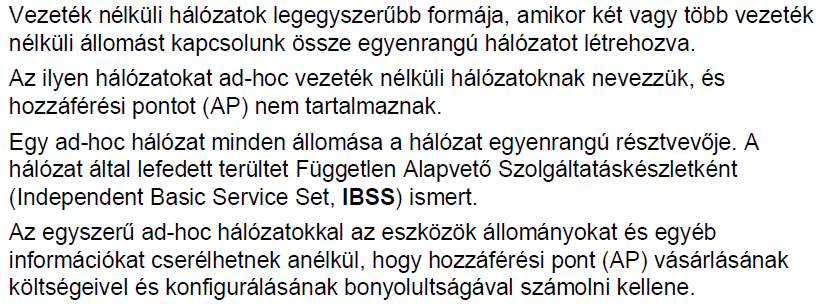


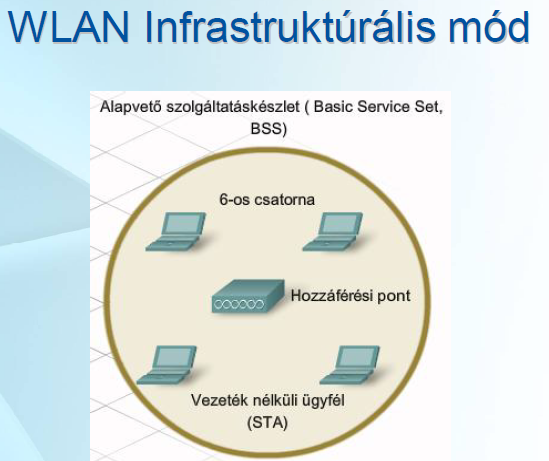


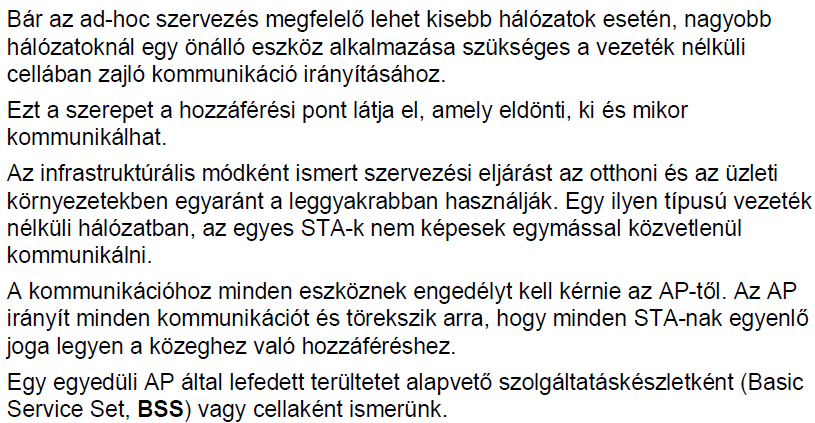


**Üzemmódok:**

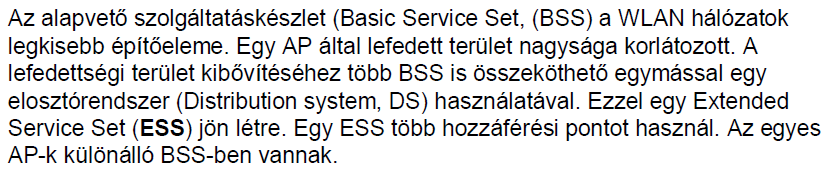


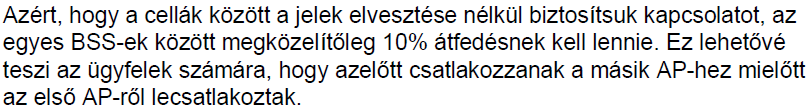


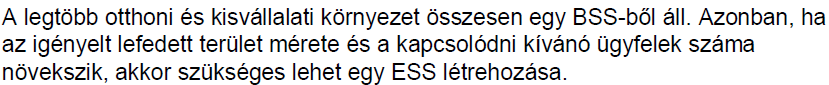




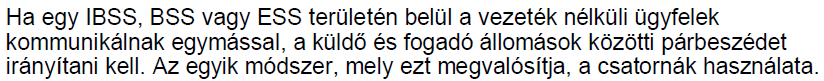


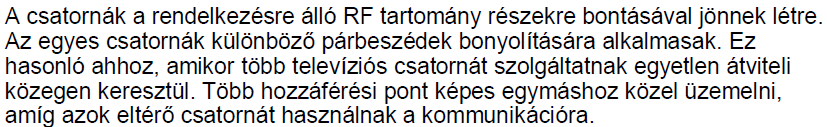


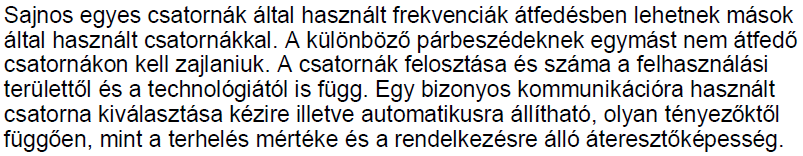


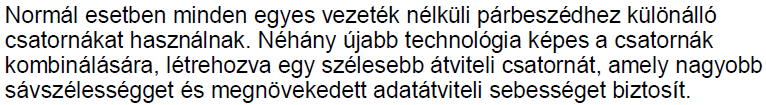




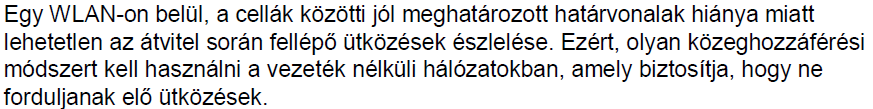


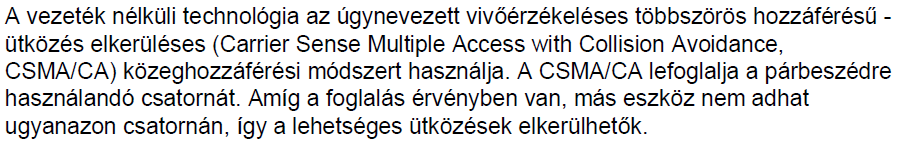


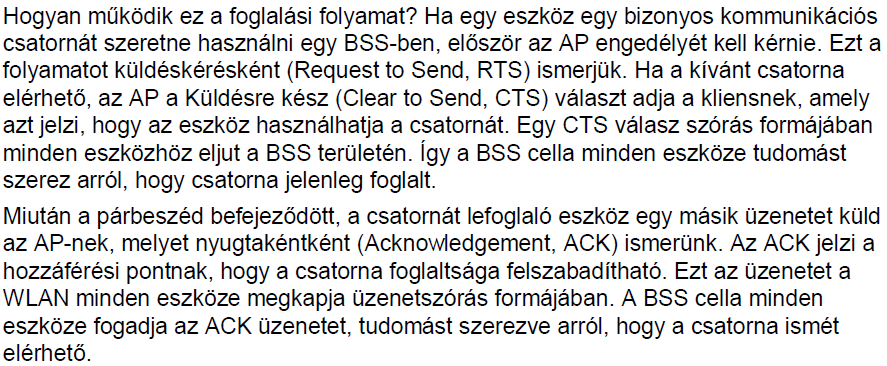




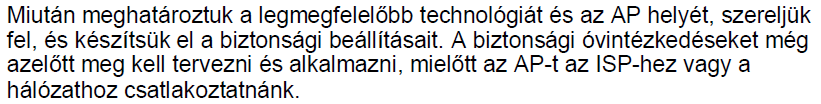


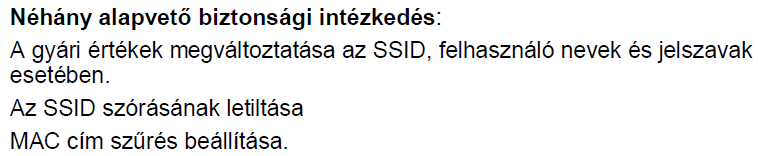


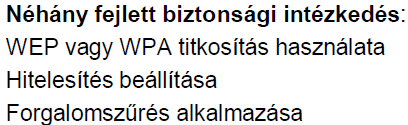


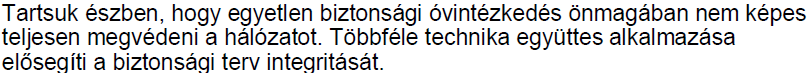


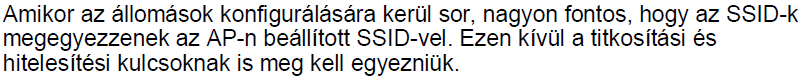












**Miért támadják a WLAN-okat?**

**A vezeték nélküli hálózatok egyik legnagyobb előnye, hogy az eszközök egyszerű és kényelmes csatlakozását teszik lehetővé**. Sajnos a **kapcsolódás egyszerűsége** és annak ténye, hogy az információ a **levegőn keresztül kerül átvitelre, sebezhetővé teszi hálózatunkat a behatolásokkal és támadásokkal szemben.**

A vezeték nélküli kapcsolódás miatt, a támadónak nem szükséges fizikailag csatlakozni számítógépünkhöz vagy hálózatunk bármely eszközéhez. Lehetséges az, hogy egy támadó ráhangolódjon hálózatunk vezeték nélküli jeleire, épp úgy, mint amikor behangolunk egy rádióállomást.

**A támadó a lefedettségi területen belül képes hozzáférni hálózatunkhoz**. Miután bejutott, ingyen használhatja az Internet kapcsolatot, valamint kárt tehet a hálózathoz csatlakozó más számítógépek adataiban vagy ellophat személyes információkat.

**A vezeték nélküli hálózatok sebezhetősége miatt a WLAN támadások elleni védekezés érdekében speciális biztonsági szolgáltatásokra és megvalósítási módszerekre van szükség.** Ezek közé tartoznak a vezeték nélküli eszköz előzetes beállításakor elvégzendő egyszerű teendők ugyanúgy, mint a jóval fejlettebb biztonsági konfigurációk.

Az egyik egyszerű módszer egy vezeték nélküli hálózatba való bejutáshoz, ha tudjuk a hálózat nevét, az SSID-t.

A hálózathoz csatlakozó minden számítógépnek ismernie kell az SSID-t. **Alapértelmezés szerint, a vezeték nélküli forgalomirányítók és hozzáférési pontok a lefedettségi terület minden állomása felé szórják az SSID-t.** Az SSID szórás bekapcsolásával, bármely vezeték nélküli ügyfél észlelheti és csatlakozhat a hálózathoz, ha nincsenek érvényben egyéb biztonsági beállítások.

**Az SSID szórása kikapcsolható**. **Ha ki van kapcsolva, a hálózat létezése többé nem nyilvános**. Bármely csatlakozni kívánó számítógépnek ismernie kell az SSID-t. Továbbá, fontos az alapértelmezett beállítások megváltoztatása. A vezeték nélküli eszközök bizonyos beállításai előre konfiguráltak, például az SSID, jelszavak és az IP címek. Ezen alapértelmezett adatok használata egyszerűvé teszik egy támadó számára a hálózat azonosítását és az abba való behatolást.

Még ha az SSID szórás ki is van kapcsolva, elég valószínű, hogy valaki jól ismert SSID-kkel próbálkozva bejut hálózatunkba. Ezen kívül, **ha az egyéb alapértelmezett beállítások, mint jelszavak és IP címek nem kerülnek megváltoztatásra, akkor a támadók hozzáférhetnek az AP-hez és változtatásokat eszközölhetnek rajta. Az alapértelmezett adatokat érdemes valamilyen biztonságosabb, egyedi értékre változtatni.**

A fenti változtatások önmagukban nem védik meg hálózatunkat. Például **az SSID-k titkosíttatlan szöveg formájában kerülnek átvitelre. Vannak olyan eszközök, amelyek képesek elfogni a vezeték nélküli jeleket és a titkosítattlanul küldött adatokat.** Így, még ha az SSID szórását ki is kapcsoltuk és megváltoztattuk a gyári értékeket, a támadók a vezeték nélküli jeleket elfogva és feldolgozva ki tudják deríteni hálózatunk azonosítóját, és felhasználhatják a hálózathoz való csatlakozáshoz. **Csak többféle módszer együttes alkalmazásával védhetjük meg WLAN-unkat**.

**Egy WLAN elérésének korlátozása**

A vezeték nélküli hálózat használata korlátozásának egyik módszere, hogy pontosan megmondjuk, mely eszközök csatlakozhatnak. Ezt a MAC-címek szűrésével érhetjük el.

**MAC cím szűrés**

A MAC cím szűrés a MAC címeket használja annak eldöntéséhez, hogy mely eszközök engedélyezettek a hálózat elérésére. Ha egy vezeték nélküli állomás megpróbál csatlakozni vagy társítást kezdeményezni egy AP-val, elküldi saját MAC cím információját. Ha a MAC cím szűrés be van kapcsolva, a vezeték nélküli forgalomirányító, illetve a hozzáférési pont megkeresi a kliens MAC címét egy előre létrehozott listában. Csak azon eszközök engedélyezettek a csatlakozásra, melyek MAC címeit előzetesen rögzítették a forgalomirányító adatbázisába.

Ha a MAC cím nem található a listában, akkor az eszköz nem csatlakozhat vagy veheti igénybe a hálózatot.

Ezzel a biztonsági módszerrel is van azonban néhány probléma. Az egyik, hogy a hálózathoz csatlakozni kívánó összes eszköz MAC címének rögzítve kell lennie az adatbázisban, mielőtt a csatlakozási próbálkozások megtörténnének. Ha egy eszköz nincs azonosítva az adatbázisban, akkor nem fog tudni csatlakozni. A másik probléma az, hogy a támadó felhasználhatja egy hozzáféréssel rendelkező, engedélyezett eszköz MAC címét.

**Hitelesítés egy vezetéknélküli hálózatban**

Egy másik módszer a csatlakozások szabályozásához a hitelesítés alkalmazása. A hitelesítés az a folyamat, mely során hitelesítési információk alapján dől el a belépés engedélyezése. Annak eldöntésére használják, hogy a kapcsolódni kívánó eszköz megbízható-e.

**Jelszó és felhasználói név használata a hitelesítés leggyakoribb formája**. Egy vezeték nélküli környezetben, a hitelesítési folyamat biztosítja a csatlakozó állomás megbízhatóságát, de a felülvizsgálati folyamat kissé eltérő módon zajlik. **A hitelesítés folyamat, ha engedélyezve van, még azelőtt megtörténik, mielőtt az ügyfél beléphetne a WLAN-ba. Három különböző típusú vezeték nélküli hitelesítési módszer létezik: *a nyílt hitelesítés, a PSK és az EAP.***

**Nyílt hitelesítés**

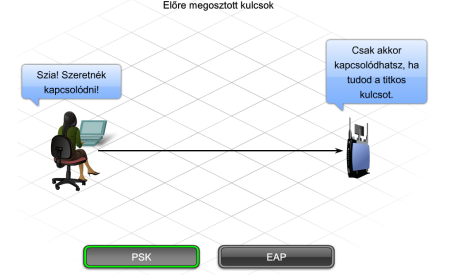
**Alapértelmezés szerint a vezeték nélküli eszközök nem igényelnek hitelesítést**. Minden hálózati eszköz képes a társításra, tekintet nélkül arra, hogy melyek azok valójában. Minden hálózati eszköz képes a csatlakozásra függetlenül attól, ki is valójában. A nyílt hitelesítést közhasznú hálózatok esetén érdemes alkalmazni, például amelyek iskolákban vagy éttermekben találhatóak. Akkor is használható, ha a hálózatba való belépés után más eszközökkel végezzük a hitelesítési eljárást.

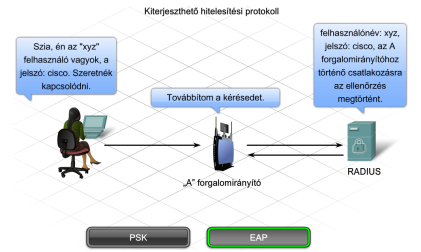
**Előre megosztott kulcs (PSK)**

PSK használata esetén, az AP-n és az ügyfél eszközön ugyanazt a kulcsot vagy titkos szót kell beállítani. **Az AP egy véletlenül generált bájtsorozatot küld az ügyfélnek. Az ügyfél fogadja a bájtsorozatot, a kulcs alapján titkosítja (kódolja), és visszaküldi a hozzáférési pontnak. Az AP fogadja a kódolt üzenetet, és a saját kulcsát használva visszafejti (dekódolja). Ha a visszafejtett bájtsorozat megegyezik az eredetileg küldöttel, az ügyfél kapcsolódhat a hálózatra.** A PSK egyutas hitelesítést végez, azaz csak az állomás hitelesíti magát a hozzáférési ponton. **A PSK nem hitelesíti az AP-t az ügyfél eszközön, és nem azonosítja az állomás tényleges felhasználóját sem.**

**Kiterjeszthető** **Hitelesítési Protokoll** (EAP)

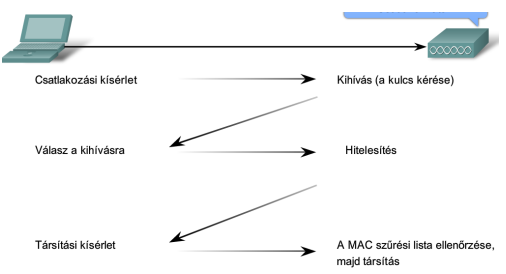
Az EAP kölcsönös vagy kétutas hitelesítést biztosít, és lehetővé teszi a felhasználó azonosítását is. Ha EAP-ot használó programot telepítettek egy állomásra, az ügyfél egy kiszolgáló oldali hitelesítő szerverrel kommunikál, mint például a távoli hitelesítés behívásos felhasználói szolgáltatás (Remote Authentication Dial-in User Service, RADIUS). Ez a kiszolgáló oldali szolgáltatás különválasztva működik a hozzáférési pontoktól és adatbázist tart fenn a hálózatot használni jogosult felhasználókról. **Amikor EAP-ot használnak, a felhasználónak - nem csak az állomásnak - meg kell adnia az azonosítóját és a jelszavát, melyek érvényességét a RADIUS adatbázisban ellenőrzik. Ha az adatok érvényesek, a felhasználó hitelesítése sikeres.**





**Ha valamilyen hitelesítés be van állítva, a hitelesítés módjától függetlenül, az ügyfélnek előbb sikeresen át kell esnie a hitelesítésen, mielőtt az AP-al való társítási folyamat elkezdődne.** Ha a hitelesítés és a MAC-cím szűrés egyaránt be van állítva, a hitelesítési folyamat zajlik le először.

* **Ha a hitelesítés sikeres, az AP ellenőrzi a MAC címet.**
* **Ha a cím érvényes, a hozzáférési pont az állomás táblájába teszi az ügyfél MAC címét.**
* **Az állomást ekkor tekintjük társítottnak a hozzáférési ponthoz (AP), és használhatja a hálózatot.**



**Titkosítás WLAN-on**

**A hitelesítés és a MAC cím szűrés megakadályozhatja a támadók hálózathoz való hozzáférését, de nem előzik meg az átvitt adatok elfogásának lehetőségét**. Mivel ***egy vezeték nélküli hálózatnak nincsenek pontosan definiálható határai és az adatátvitel a levegőn keresztül történik, egy támadó számára egyszerű a vezeték nélküli keretek elfogása vagy más néven lehallgatása*** (sniffing). A titkosítási folyamat az adatok átalakítását jelenti, így az elfogott információk használhatatlanok lesznek.

**Vezetékessel egyenértékű protokoll (Wired Equivalency Protocol, WEP)**

A Vezetékessel Egyenértékű titkosítási Protokoll (WEP) egy fejlett biztonsági lehetőség, mely a levegőben áthaladó hálózati forgalom titkosítását végzi. A WEP előre beállított kulcsok használatával kódolja és fejti vissza az adatokat.

**A WEP-kulcsokat szám- vagy betűsorozat formájában használják, többnyire 64 vagy 128 bit hosszúsággal. Némely esetben a 256 bit hosszú kulcsok is támogatottak**. Ezen kulcsok létrehozásának és beírásának egyszerűsítése végett számos eszköz felkínálja a Jelmondat (Passphrase) lehetőségét. A passphrase segítségével könnyen észben tarthatunk egy szót vagy kifejezést, melyet a kulcsok automatikus létrehozásához használhatunk.

**Annak érdekében, hogy a WEP működjön, a hozzáférési pontnál és az összes engedélyezett állomáson ugyanazon WEP kulcsot kell megadni**. **Ezen kulcs nélkül, az eszközök nem tudnák értelmezni az átvitelt.**

A WEP egy nagyszerű mód arra, hogy megakadályozzuk a támadókat a jelek elfogásában. **Azonban megvannak a WEP hátrányai is, például, hogy az összes WEP állomáson statikus (állandó) érvényű kulcsokat használ.** Léteznek olyan alkalmazások, melyek segítségével a támadók kideríthetik a WEP kulcsot. Ezek a programok hozzáférhetőek az Interneten. Miután a támadó kinyerte a kulcsot, teljes hozzáférést szerez az összes továbbított információhoz.

**A sebezhetőség elkerülésének egyik módja a WEP kulcsok gyakori megváltoztatása. A másik módszer egy jóval fejlettebb és biztonságosabb titkosítási eljárás, a Wi-Fi Védett Hozzáférés (WPA) alkalmazása.**

**WEP2**

Futtatható volt azon a néhány (de nem mindegyik) hardveren, amely nem volt képes a WPA-t vagy a WPA2-t futtatni és kiterjesztették a biztonsági kulcs értékét 128bit-re. Ez némileg segített a "[brute force](https://hu.wikipedia.org/wiki/Brute_force-t%C3%A1mad%C3%A1s" \o "Brute force-támadás) = nyers erőt" alkalmazó támadások kivédésében.

**Wi-Fi Védett Hozzáférés (WPA)**

**A WPA is 64 és 256 bit közötti hosszúságú kulcsokat használ**. A **WPA azonban** a WEP-pel ellentétben új, **dinamikus kulcsokat hoz létre minden alkalommal, amikor egy állomás kapcsolódik a hozzáférési ponthoz.** Éppen ezért a WPA jóval biztonságosabb, mint a WEP, mivel sokkal nehezebb feltörni.

**WPA2**

A [WPA2](https://hu.wikipedia.org/wiki/WPA#WPA2) az ajánlott megoldás a WEP biztonsági problémáira, vagy régebbi berendezésekben a fejletlenebb [WPA](https://hu.wikipedia.org/wiki/WPA), ahol csak az van. Mindkettő biztonságosabb a WEP-nél. **Néhány régebbi [Wi-Fi](https://hu.wikipedia.org/wiki/Wi-Fi" \o "Wi-Fi) eszközhöz is adhatunk WPA vagy WPA2 támogatást, ha frissítjük az eszköz [firmware](https://hu.wikipedia.org/wiki/Firmware" \o "Firmware)-ét.** A WPA egy gyors, időközi megoldás a WEP helyett; ugyanazon a hardveren elfut, mint a WEP. A [TKIP](https://hu.wikipedia.org/wiki/TKIP) (a WPA alapja) már nem fejlődik tovább és a következő teljes 802.11-es szabványban érvénytelenítették.

[**TKIP**](https://hu.wikipedia.org/wiki/TKIP)

A **Temporal Key Integrity Protocol** (röviden: **TKIP** = Időszakos Kulcs Sérthetetlenségi Protokoll). A TKIP-t nem fejlesztették tovább 2005 után és a 802.11 szabvány következő teljes kiadásában hatálytalanítva lett.

**Forgalomszűrés egy WLAN-on**

***Annak szabályozásán kívül, hogy ki fér hozzá a WLAN-hoz, és ki használhatja fel a továbbított adatokat, fontos, hogy a WLAN-on keresztül továbbított hálózati forgalom típusát is szabályozni lehessen. Ezt forgalomszűrés segítségével valósítják meg.***

A forgalomszűrés letiltja mind a hálózatba belépő, mind a hálózatot elhagyni kívánó nemkívánatos forgalmat. **A szűrést az AP végzi el, miközben a forgalom áthalad rajta. A szűrés arra használható, hogy bizonyos forrásállomás felől jövő vagy célállomás felé igyekvő forgalmat MAC vagy IP címek alapján kiszűrjünk**. Ezen kívül számos alkalmazás működését blokkolhatjuk a megfelelő portszámok letiltásával. Azáltal, hogy eltávolítjuk a nemkívánatos, haszontalan és gyanús adatforgalmat a hálózatból, jóval nagyobb sávszélesség áll rendelkezésre a fontos adatok átvitelére, ami a WLAN teljesítményének növekedését eredményezi. Például, a forgalomszűrést használhatjuk arra, hogy letiltsunk minden olyan Telnet forgalmat, amely egy meghatározott számítógépre, például egy hitelesítő kiszolgálóra irányul. Bármely próbálkozás, amely telnet segítségével próbálja elérni a hitelesítő szervert, gyanús hálózati forgalomnak számít és le lesz tiltva.

**WLAN tervezése**

Egy vezeték nélküli hálózat megvalósításakor a telepítést gondos tervezésnek kell megelőznie. Ezek közé tartozik:

* A használandó vezeték nélküli szabvány meghatározása
* Az eszközök leghatékonyabb elhelyezésének meghatározása
* Egy telepítési és biztonsági terv elkészítése
* A vezeték nélküli eszközök firmware-jének mentési és frissítési stratégiája

**Vezeték nélküli szabványok**

Tekintettel kell lennünk számos tényezőre, mielőtt egy WLAN szabvány használata mellett döntenénk. A legfontosabb tényezők közé tartozik: sávszélességi követelmények, lefedettségi területek, meglévő hálózatok szabványa, költségek. Ezen információkat a végfelhasználói igények megismerésével gyűjthetjük össze.

* Ennek legegyszerűbb formája, ha kérdéseket intézünk a felhasználók felé.
* Jelenleg mekkora sávszélességet igényelnek a hálózaton futtatott programok?
* Összesen hány felhasználó használná a WLAN-t?
* Mekkora lefedettségi területre van szükség?
* Milyen a meglévő hálózati kiépítés?
* Mekkora a költségvetés?

A BSS cellában elérhető maximális sávszélességet az adott BSS felhasználói között meg kell osztani. Még ha a használt alkalmazások nem is igényelnek nagy sávszélességet, egy nagyobb sebességű technológia valamelyikére lehet szükség, ha egyidőben több felhasználó is csatlakozik a hálózathoz.

A különböző szabványok eltérő méretű lefedettségi területet biztosítanak. A 802.11 b/g/n technológiák által használt 2,4 GHz-es jelek nagyobb hatótávolságúak, mint a 802.11a szabvány 5 GHz-es jelei. Ezért a 802.11 b/g/n szabványok nagyobb területű BSS-ek kialakítására alkalmasak. Emiatt kevesebb eszközt kell beépíteni, ami alacsonyabb megvalósítási költséggel jár.

A létező hálózatok ugyancsak befolyásolják a telepítésre kerülő WLAN szabványok kiválasztását. Például a 802.11n szabvány felülről kompatibilis a 802.11g és 802.11b szabványokkal, de a 802.11a-val nem. Ha a meglévő hálózati infrastruktúra és a használt berendezések a 802.11a szabványt támogatják, akkor az új megvalósításnak is támogatnia kell ezt a szabványt.

Az ár nem elhanyagolható tényező. Ha a költségeket vesszük figyelembe, számoljunk összköltséggel (TCO), mely magában foglalja a beszerzési és telepítési költségeket is. Egy közepes vagy nagyméretű vállalati környezetben az összköltségnek (TCO) sokkal nagyobb súlya van a választott WLAN szabványra nézve, mint az otthoni vagy kisvállalati környezetekben. Ez azért van, mert a nagyobb vállalatok esetében, több berendezésre és telepítési tervekre van szükség, melyek növelik a költségeket

**Egy AP telepítése és biztonsági beállításai**

Miután meghatároztuk a legmegfelelőbb technológiát és az AP helyét, szereljük fel, és készítsük el a biztonsági beállításait. A biztonsági óvintézkedéseket még azelőtt meg kell tervezni és alkalmazni, mielőtt az AP-t az ISP-hez vagy a hálózathoz csatlakoztatnánk.

Néhány alapvető biztonsági intézkedés:

* A gyári értékek megváltoztatása az SSID, felhasználó nevek és jelszavak esetében.
* Az SSID szórásának letiltása
* MAC cím szűrés beállítása.

Néhány fejlett biztonsági intézkedés:

* WEP vagy WPA titkosítás használata
* Hitelesítés beállítása
* Forgalomszűrés alkalmazása

Tartsuk észben, hogy egyetlen biztonsági óvintézkedés önmagában nem képes teljesen megvédeni a hálózatot. Többféle technika együttes alkalmazása elősegíti a biztonsági terv integritását.

Amikor az állomások konfigurálására kerül sor, nagyon fontos, hogy az SSID-k megegyezzenek az AP-n beállított SSID-vel. Ezen kívül a titkosítási és hitelesítési kulcsoknak is meg kell egyezniük.

