Háló dolgozat

1. **<u>Vezeték nélküli adatátvitel</u>**
   a. **Def**.: A vezeték nélküli közegek rádió- vagy mikrohullámok használatával továbbítják az elektromágneses jeleket
   b. **Korlátai**:
      - Lefedettségi terület
      - Interferencia
      - Biztonság
      - Osztott átviteli közeg
   c. **Előnyei**:
      - Hordozhatóság
      - Skálázhatóság
      - Rugalmasság
      - Költségtakarítás
      - Rövid telepítési idő
      - Megbízhatóság mostoha körülmények között

2. **<u>Vezeték nélküli hálózatok típusai</u>**
   a. 3 fő csoportja
      - WPAN
      - WLAN
      - WWAN
   b. IEEE és ipari távközlési szabványok

IEE 802.11	Wi-fi	Akár 9,6Gbs
IEEE 802.15	Bluetooth	Max.: 3Mb/s
IEEE 802.16	Wi-Max	Max.: 1Gb/s

3. **<u>Vezeték nélküli LAN</u>**
   a. **A vezeték nélküli hálózat közös adatátviteli közege** lehetővé teszi az eszközök számára, hogy vezeték nélkül csatlakozzanak egymáshoz egy LAN-on keresztül.
   b. **Eszközei**:
      - Vezeték nélküli hozzáférési pont (Access Point, AP)
        - Fogadja a felhasználók vezeték nélküli jeleit, és csatlakozik a meglévő rézvezetékes hálózat-hoz, például az Ethernethez.
      - Vezeték nélküli hálózati adapterek
        - Vezeték nélküli kommunikáció képességét biztosítják a hálózati állomásoknak.

4. **<u>INFRA</u>**
   a. Jellemzők
      - alacsony energiaszintű, és jelei nem képesek áthatolni a falakon vagy egyéb akadályokon
      - Az infravörös sugarakat az 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

b. 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

5. Bluetooth

a. Jellemzői

- rövid hatótávolságú, adatcseréhez használt, nyílt, vezeték nélküli szabvány
- Alkalmazásával számítógépek, mobiltelefonok (telefonkihangosítók) és egyéb készülékek között automatikusan létesíthetünk kis hatótávolságú rádiós kapcsolatot
- PAN
- A Bluetooth alacsony energiafogyasztása miatt különösen alkalmas hordozható eszközök számára.

b. Verziói

1.2	1Mbps
2.0	3Mbps

c. Felhasználási területek

- Vezeték nélküli hálózatok kialakítására asztali és hordozható számítógépek között, illetve csak asztali gépek között kis területen, ha nincs szükség nagy sávszélességre
- Számítógép-perifériák csatlakoztatására nyomtatók, billentyűzetek, egerek esetében
- Fájlok és adatok átvitelére és szinkronizálására személyi digitális asszisztensek (PDA-k, mobiltelefonok és a számítógép) között
- Egyes digitális zenelejátszók, fényképezőgépek és számítógép között
- Autóskészletek és fülhallgatók csatlakoztatására mobiltelefonokhoz
- Orvosi és GPS-készülékek

6. Rádiófrekvencia

a. Szabványok

Szabvány	Sávszélesség (max)	Használt frekvencia	Jellemző	Kompatibilitás
802.11	2Mb/s	2.3GHz	Apró sebesség a mai alkalmazásokhoz	-
802.11a	54Mb/s	5GHz	Magas költség, alacsony jellefedettség	-
802.11b	5,5Mb/s 11Mb/s	2.4GHz	alacsony termelési költség, alacsony működési sebesség, zavarja a háztartási készülékeket	-
802.11g	54Mb/s	2,4GhZ	Legelterjedtebb	802.11b

802.11n	600Mb/s	2,4GHz, 5GHz	megnövekedett hatótávolsággal és átbocsátóképességgel rendelkezik	802.11b és 802.11g
802.11ac	1.3Gb/s	5GHz	-	-
802.11ad	7,2Gb/s	60GHz	1-10 méteres hatótávval rendelkezik	-

b. Felhasználási területek

- 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
- Publikus, zárt hálózat: egy speciális szoftver gondoskodik arról, hogy a hálózatot csak egy kód ismeretében, korlátozott ideig lehessen használni.
- 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

7. WLAN összetevők (buta képesen van benne)

Vezeték nélküli ügyfél:

Bármely eszköz, amely részt vehet egy vezeték nélküli hálózatban. A legtöbb eszköz, mely képes hagyományos vezetékes hálózathoz kapcsolódni, ellátható megfelelő vezeték nélküli hálózati kártyával és szoftverrel, mely segítségével képes lesz egy WLAN-hoz csatlakozni.

Ezek lehetnek helyhez kötött vagy hordozható eszközök.

Általában STA-nak nevezzük az ilyen állomásokat

Hozzáférési pont:

A vezetékes és vezeték nélküli hálózatok közötti hozzáférés vezérlésért felelős. Tehát lehetővé teszi a vezeték nélküli ügyfelek számára , hogy hozzá férjenek a vezetékes hálózathoz.

Átviteli közeg átalakítóként működik, fogadja a vezetékes hálózat Ethernet kereteit és 802.11-nek megfelelő keretté alakítja, mielőtt továbbítja őket a WLAN-ra.

A WLAN-ból érkező 802.11-es keretelet fogadja és Ethernet keretekké alakítja mielőtt a vezetékes hálóra helyezi őket.

A hozzáférési pontok korlátozott területen biztosítanakhozzáférést, melyet vezeték nélküli cella vagy alapvető szolgáltatáskészletként (Basic Service Set (BSS)) ismerünk.

Vezeték nélküli híd:

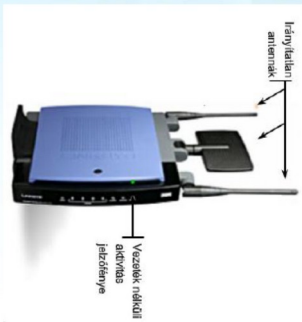
Két különböző vezetékes hálózat vezeték nélküli összeköttetésére használják.

Nagy távolságú pont-pont kapcsolato6 biztosít a hálózatok között.

Engedélyt nem igénylő rádiófrekvenciát használva, egymástól 40 km-re fekvő vagy távolabbi hálózatokkat tudunk kábele használata nélkül.

Antennák:

- Az AP-k és vezeték nélküli hidak esetében használják.
- Megnövelik a vezeték nélküli eszköz által kibocsátott jelek erősségét.
- Fogadják más eszközök, például STA-k jeleit.
- Az antennák által okozott jelerősség növekedést más néven erősítésnek nevezzük.
- A nagyobb erősítés rendszerint megnövekedett hatótávolságot jelent.



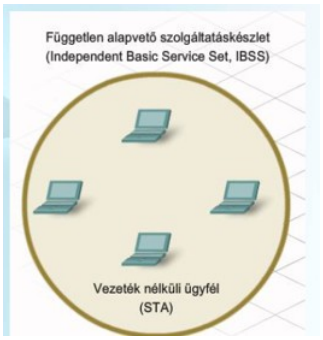
Az antennákat, a jelek sugárzásának a módja alapján osztályozzuk.

Az irányított antennák egy irányba koncentrálják a jelek energiáját.

Az irányítatlan antennákat arra tervezték, hogy minden irányba azonos erősséggel sugározzanak.

8. Üzemmódok (ez is)

a. WLAN ad-hoc üzemmód



Vezeték nélküli hálózatok legegyszerűbb formája, amikor két vagy több vezeték nélküli állomást kapcsolunk össze egyenrangú hálózatot létrehozva.

Az ilyen hálózatokat ad-hoc vezeték nélküli hálózatoknak nevezzük, és hozzáférési pontot (AP) nem tartalmaznak.

Egy ad-hoc hálózat minden állomása a hálózat egyenrangú résztvevője. A hálózat által lefedett területet Független Alapvető Szolgáltatáskészletként (Independent Basic Service Set, **IBSS**) ismert.

Az egyszerű ad-hoc hálózatokkal az eszközök állományokat és egyéb információkat cserélhetnek anélkül, hogy hozzáférési pont (AP) vásárlásának költségeivel és konfigurálásának bonyolultságával számolni kellene.

b. WLAN infrastrukturális mód



Bár az ad-hoc szervezés megfelelő lehet kisebb hálózatok esetén, nagyobb hálózatoknál egy önálló eszköz alkalmazása szükséges a vezeték nélküli cellában zajló kommunikáció irányításához.

Ezt a szerepet a hozzáférési pont látja el, amely eldönti, ki és mikor kommunikálhat.

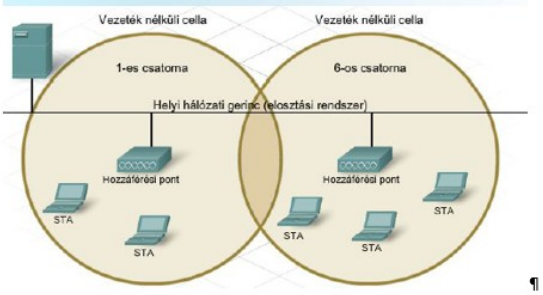
Az infrastruktúrális módként ismert szervezési eljárást az otthoni és az üzleti környezetekben egyaránt a leggyakrabban használják. Egy ilyen típusú vezeték nélküli hálózatban, az egyes STA-k nem képesek egymással közvetlenül kommunikálni.

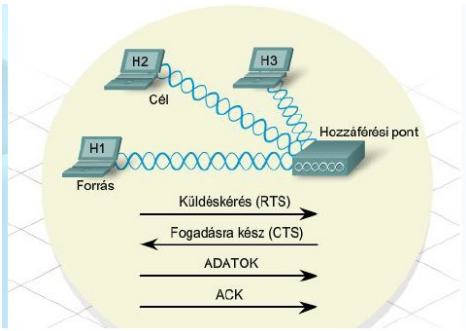
A kommunikációhoz minden eszköznek engedélyt kell kérnie az AP-től. Az AP irányít minden kommunikációt és törekszik arra, hogy minden STA-nak egyenlő joga legyen a közeghez való hozzáféréshez.

Egy egyedüli AP által lefedett területet alapvető szolgáltatáskészletként (Basic Service Set, **BSS**) vagy cellaként ismerünk.

c. Vezeték nélküli csatornák

Ha egy IBSS, BSS vagy ESS területén belül a vezeték nélküli ügyfelek kommunikálnak egymással, a küldő és fogadó állomások közötti párbeszédet irányítani kell. Az egyik módszer, mely ezt megvalósítja, a csatornák használata.





d. AP telepítése és beállítása

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:

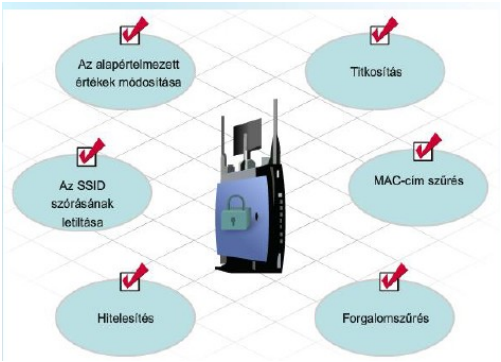
WEP vagy WPA titkosítás használata

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.



9. WLAN-ok támadása

a. Mért támadhatók egyszerűbben?

- Sajnos a kapcsolódás egyszerűsége és annak ténye, hogy az információ a levegőn keresztül kerül átvitelre, sebezhetővé teszi hálózatunkat a behatolásokkal és támadásokkal szemben.

b. Hogyan támadhatják?

- A támadó a lefedettségi területen belül képes hozzáférni hálózatunkhoz.

c. Hogyan védekezhetünk?

- SSID titkosítása (alapértelmezetten minden állomásnak szórja)
- Alapértelmezett jelszavak megváltoztatása
- IP címek megváltoztatása
- Alapértelmezett adatok egyedire változtatása

d. MAC-cím szűrés

- A MAC cím szűrés a MAC címeket használja annak eldöntéséhez, hogy mely eszközök enge-délyezettek a hálózat elérésére.

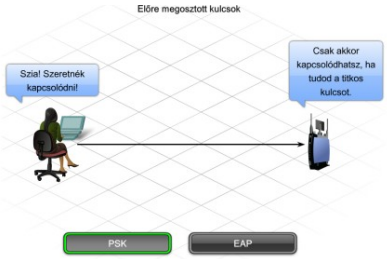
10. Hitelesítés vezetéknélküli hálózatba

a. Leggyakoribb formája

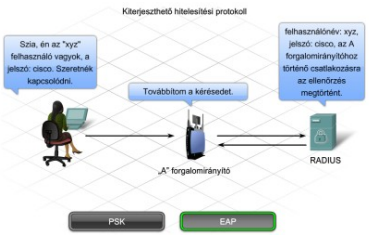
- Jelszó és felhasználónév használata

b. 3 típusa

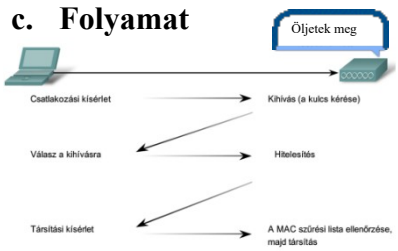
- Nyílt hitelesítés
  - Alapértelmezés szerint a vezeték nélküli eszközök nem igényelnek hitelesítést.
- Előre megosztott kulcs (PSK)
  - Az AP egy véletlenül generált bájtsorozatot küld az ügyfélnek. Az ügyfél fogadja a bájt-sorozatot, a kulcs alapján titkosítja (kódolja), és visszaküldi a hozzáférési pontnak. Az AP fogadja a kódolt üzenetet, és a saját kulcsát használva visszafejti (dekódolja). Ha a vissza-fejtett bájtsorozat megegyezik az eredetileg küldöttel, az ügyfél kapcsolódhat a hálózatra.



  - A PSK nem hitelesíti az AP-t az ügyfél eszközön, és nem azonosítja az állomás tényleges felhasználóját sem.
- Kiterjeszthető Hitelesítési Protokoll (EAP)
  - 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.



c. Folyamat



- 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.

11. <u>Titkosítás WLAN-on</u>

a. Vezetékessel egyenértékű protokoll (Wired Equivalency Protocol, WEP)
- A WEP-kulcsokat szám- vagy betűsorozat formájában használják, többnyire 64 vagy 128 bit hosszúsággal. Némely esetben a 256 bit hosszú kulcsok is támogatottak.
- Gyakran változtassuk

b. WEP2

c. 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

d. WPA 2
- Kijavítja a WEP biztonsági problémáit

12. <u>Forgalomszűrés</u>

a. Mi végzi?
- A szűrést az AP végzi el, miközben a forgalom áthalad rajta

b. Mire jó?
- A szűrés arra használható, hogy bizonyos forrásállomás felől jövő vagy célállomás felé igyekvő forgalmat MAC vagy IP címek alapján kiszűrjünk.

13. <u>WLAN tervezés</u>

a. Miket határozzunk meg?
- 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

b. Gondoljuk át még egyszer!
- 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?