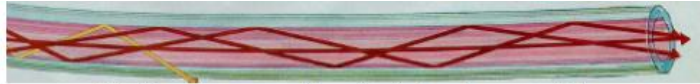


1.) Mi a különbség a multi módusú és az egymódusú üvegszál között?

■ Többmódusú szál

- A fényimpulzusok hosszanti irányban szétszóródnak a szálban
- Egyszerre több, különböző szögben visszaverődő fénysugár halad
- Minden sugárnak más a „módusa”
- Olcsó megoldás, de csak kis távolságokra hatékony (500 m)



■ Egymódusú szál

- Ha az üvegszál átmérője nagyon kicsi, a fény visszaverődés nélkül, egyenesen terjed
- Jóval drágább a szál, és nagyobb kapacitású, jobb lézereket igényel
- Nagyobb távolságok áthidalására sokkal jobb
 - 50 Gbps 100 km távolságba erősítés nélkül
 - A transzatlanti optikai kábeleknél nagyon fontos, hogy kevés erősítő legyen
- A gerinchálózatban csak egymódusú szálakat használnak



2.) FTTC rendszer működése

■ Fiber To The Curb / Building

- Üvegszál az elosztódobozig / épületig

■ Üvegszál a helyi központból minden lakóközrzig

- A szál egy ONU-ban végződik
 - Optical Network Unit – optikai hálózategység
- Több helyi rézhurok, koax, Ethernet kábel csatlakozhat hozzá
 - Nagyon rövid hurkok, lehetséges szimmetrikus nagysebességű kiterjesztés
 - Pl. VDSL – Dél-kelet Ázsiában nagyon elterjedt
 - Alkalmas MPEG-2 átvitelre, videokonferenciázásra
 - Az FTTC/FTTB maga szimmetrikus átviteli sebességeket biztosít

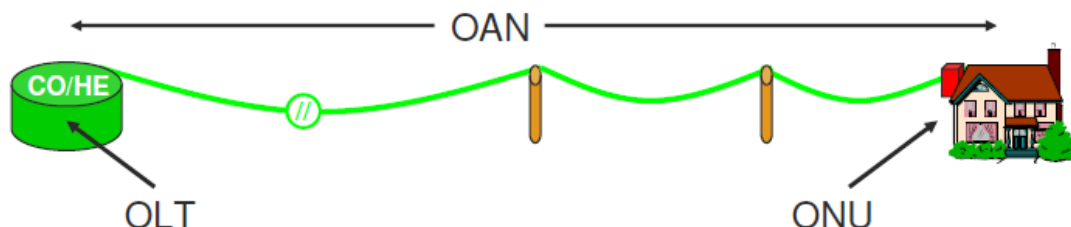
3.) FTTH architektúra

■ Fiber To The Home

- Üvegszál otthonra

■ Rendszerelemek

- OAN: Optical Access Network
 - Optikai hozzáférési hálózat
- ONU/ONT: Optical Network Unit/Terminal
 - Az előfizető otthonában
- OLT: Optical Line Termination
 - végződtetés a szolgáltató hálózatában



a.) Mi a különbség az aktív és passzív architektúra között?

- PON – Passive Optical Networks
 - Több felhasználó (max. 32) megoszt egy fényvezető szálát
 - Optikai splitter-ek a jel szétválasztására és aggregálására
 - Áramellátás csak a végeknél szükséges
 - Osztott hálózat – Point to Multipoint (P2MP)
- Active Node
 - Az előfizetőknek saját fényvezető száluk
 - Point to Point (P2P)
 - Aktív, árammal táplált csomópontok a forgalom elosztására
 - Ethernet switch
 - Layer2/Layer3 switching/routing
- Hybrid PON
 - Az előbbi két architektúra kombinált változata

b.) APON vs. EPON

APON:

- **Segmentation and Reassembly (SAR)**
 - Fix hosszúságú csomagok
 - 53 byte-os ATM cellák
 - Az adatok átmennek egy ATM Adaptation Layer-en (AAL) ahol 48 byte-os darabokra osztják őket
 - Plusz 5 byte a fejléc
 - A címzettnél az eredeti forgalmat újból összerakják
- A SAR miatt az ATM kifejezetten alkalmas video, hang és adatátvitelre
 - A kis, fix hosszúságú cellákban jól lehet késleltetésre érzékeny forgalmat szállítani
 - A procedura időigényes, az 5 byte-os fejléc pedig nem hatékony (10%-os overhead)
- A fix hosszúságú cellák jól illeszkednek a PON TDMA alapú feltöltéséhez
 - Könnyű az időszeletek kezelése, nincsenek ütközések

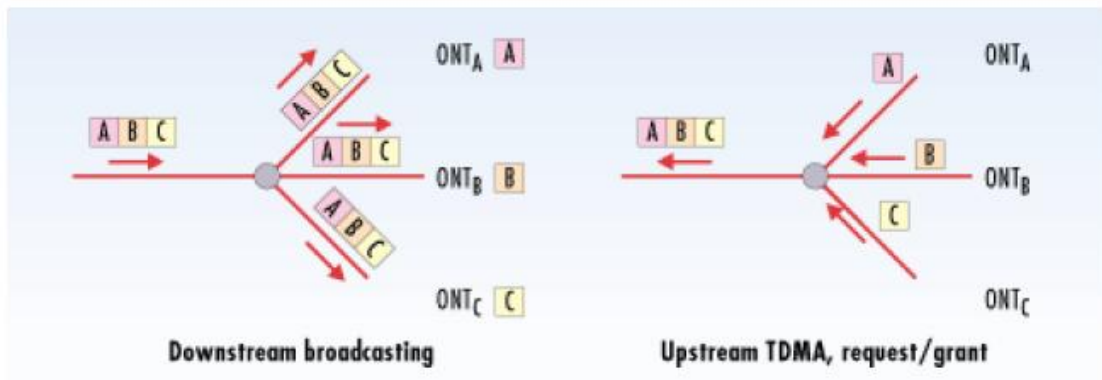
EPON:

- Az adatok az IEEE 802.3 (Ethernet) formátumot használják
 - Változó hosszúságú csomagok 64 és 1518 byte között
- Hogyan oldjuk meg a TDMA alapú feltöltést?
 - Feloszthatjuk az Ethernet kereteket (frame) fix hosszúságú részekre
 - Egyszerűbb lesz a feltöltés
 - Az ár egy SAR funkció hozzáadása az EPON protokoll stack-hez
 - Lehetne max. hosszúságú időszeleteket kiosztani
 - Bármilyen csomag befér
 - Nem hatékony, sávszél pazarlás
 - **Alkalmazott megoldás:** fix hosszúságú időszeletek, melyekbe több csomagot be tud rakni az ONU
 - Javít a hatékonyságon
 - Nehéz változó hosszúságú csomagokkal jól feltölteni egy fix hosszú időszeletet

c.) Hogyan van megoldva a le- és feltöltés?

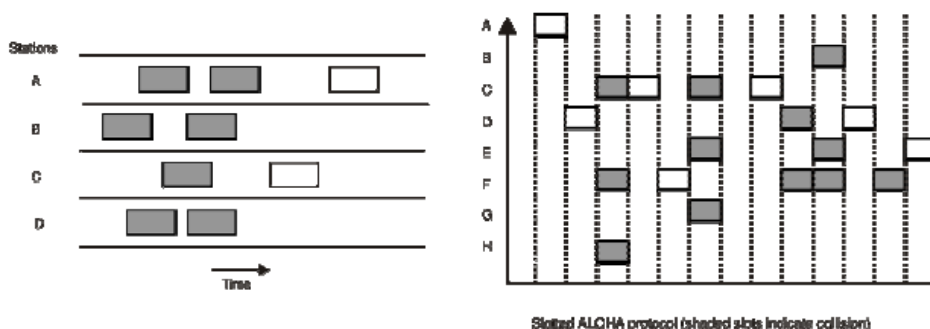
A le- és feltöltés nem egyformán működik

- A letöltés broadcast
 - A splitter minden szálra kitesz minden csomagot
 - Az ONU csak azt a csomagot kezeli melyet neki címeztek (fejléc alapján)
- A feltöltés TDMA-t használva történik
 - Az OLT időszeleteket oszt ki az ONU-knak
 - Szinkronizált csomagküldés
 - Az ONU kérhet plusz szeleteket, ha van küldeni valóját



4.) Aloha Network működése. Mi a különbség az Aloha és Slotted Aloha között?

- Hawaii – 70-es évek elején nem volt telefonhálózat
 - A távoli szigeteken lévő felhasználókat a Honoluluban lévő központi számítógépekhez kellett csatlakozni
- Megoldás: ALOHANET – kis hatósugarú rádiózás
 - Norman Abramson, Hawaii Egyetem
 - Minden felhasználó terminálon kis rádió
 - Két frekvencián üzemelt
 - Egy a lefele, egy a felfele menő adatoknak
 - Lefele csak a központ küldött, nem volt gond
 - Felfele versenyhelyzet, többen használták ugyanazt a csatornát
 - Ha sikerült elküldeni valamit, a központ visszaküldte a csomagot a másik csatornán
 - Ha nem jött vissza, a csomag valószínűleg elveszett
 - Újra próbálkozott
 - Alacsony terhelés mellett egész jó, nagy upstream terhelés mellett szinte használhatatlan

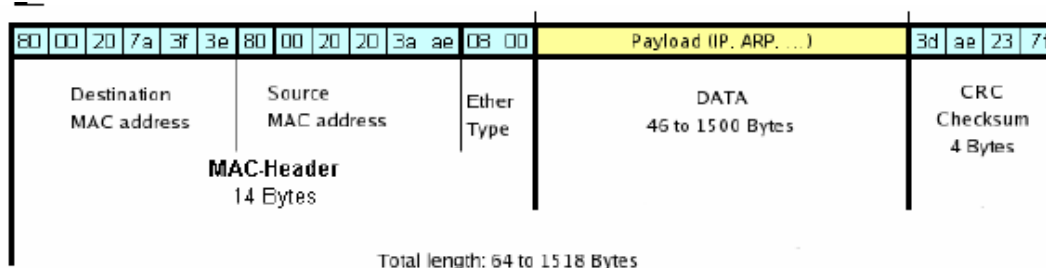


Újítás: csak adott időpontokban küldhet (slots)

5.) Hogyan működik a CSMA/CD az Ethernet hálózaton? Hogyan néz ki az Ethernet Frame Burst? Paddig, Carrier Extension és Frame Bursting szükségességei?

CSMA=Carrier Sense Multiple Access; CD=Collision Detection

- Kommunikáció az osztott közegen
 - Mint egy beszélgetés vacsora közben
- Az Ethernet kábelén adás előtt a gépek belehallgatnak a csatornába
 - Ha foglalt, megvárja az adás végét
 - Ha mégis ütközés, akkor ezt detektálják
 - zajlőketet küld, hogy más is értesüljön az ütközésről
 - Véletlen hosszúságú idő után újra próbálkoznak
 - Több ütközés után exponenciálisan nő a max. várakozási idő
 - Az Alohanet-en ez nem volt megoldható
 - Két felhasználó két külön szigeten nem biztos, hogy hallotta egymást



- A data mező legfeljebb 1500 byte
 - Minimális data hossz 46 byte
 - Ha túl rövid a keret, nem lehet CD-t használni
 - Hamar befejeződik a keret elküldése, lehet hogy az első bit még el sem érkezett a kábel végére
 - Ha esetleg ott lenne ütközés, arról nem értesül
 - A rövid csomagokat fel kell tölteni „haszontalan adatokkal” (Pad)
- Ha nő a hálózat sebessége...
 - növelni kell a minimális keretméretet, vagy...
 - csökkenteni kell a megengedett maximális kábelhosszt
 - Ha 2500 méter a kábel és 1 Gb/s a sebesség, akkor a minimális keretméret 6400 byte kell legyen
 - Ha a minimális keret 640 byte, akkor a kábel csak 250 méter lehet
 - Egyre kényelmetlenebb megkötések egy gigabites hálózatonál
 - A minimális keretméretet megemelték 512 byte-ra
- Carrier Extension
 - A küldő hardver a CRC mező után illeszt egy kitöltő bitsorozatot
 - A vevő hardver levágja azt, a CRC-be nem számít bele
 - Nagyon pocsékolja a kapacitást
- Frame Bursting
 - Egyetlen adás során több, egymás után fűzött keretet visz át
 - Jelentősen növeli a hatékonyságot

6.) Mi a különbség a full duplex és a half duplex átvitel között a Gigabit Ethernetben?

- Duplex – mindkét irányba megy forgalom egyidőben
 - Egy központi kapcsolót (**switch**) kötnek össze a periférián lévő gépekkel
 - Minden vonalat pufferelemek
 - Bárki bármikor küldhet adatokat
 - Nem kell a csatornát figyelni, a versengés kizárt
 - Nincs szükség CSMA/CD-re, viszont akkor már nem Ethernet
- Fél-duplex
 - A gépeket egy egyszerű elosztóhoz csatlakoztatják
 - Nincs pufferelem, lehetnek ütközések

7.) Mi a különbség a hub és switch között?

HUB:

Fizikai szintű ismétlő eszköz

- Bit szinten ismétli a csomagot
- A bejövő csomagokat azonnal minden interfészén kiküldi
 - Mindenki megkap minden csomagot

Több egyidejű küldő: ütközés

- A „collision domain” (ütközési tartomány) megmarad

A hub-okat általában hierarchikusan, fa topológiába kapcsolják

Minden állomás ütközhet a hub-ra kapcsolt bármely más állomással

- Ez rontja a hálózat teljesítményét
- Csökkenti a skálázhatóságot
- Mindenki látja a többiek forgalmát

Különböző médiumok nem kapcsolhatók össze

- Pl. ha van 10Mbps állomás a rendszerben, a teljes sebesség visszaesik 10-re

SWITCH:

Link Layer eszköz

- megvizsgálja a MAC fejlécet és szelektíven továbbít
 - switch table: (MAC, interfész, timer)
 - A kapott csomagokból építi fel
 - Ha nem ismer egy címet, minden interfészre továbbárasztja a csomagot
- elválasztja az ütközési zónákat
 - pufferelem a csomagokat
 - csak a megfelelő szegmensre továbbít

Előnyök:

- jobban skálázható
- hatékonyabb, biztonságosabb
- a pufferelem lehetővé teszi különböző médiumok/sebességek összekapcsolását

8.) Hogyan működik a spanning-tree protocol?

Spanning Tree Protocol (STP)

- IEEE 802.1D szabvány része
- Hurokmentes fák egy bridge-lt LAN-on
 - Az Ethernetben nincs TTL (Time To Live)
 - Hurok esetén végtelenül keringenek a csomagok a hálózatban
 - Redundanciára viszont szükség van
 - Hiba esetén van egy védelmi útvonal

Root bridge kiválasztása

- Minden bridge-nek MAC címe és konfigurálható prioritási száma
 - BID – Bridge Identification
- A legkisebb prioritású bridge lesz a root
 - Egyenlőség esetén a kisebb MAC cím nyer
 - A második helyezett lesz a secondary (backup) root
- Teljesen automatikus, de ha rendszergazda egy bizonyos bridge-et szeretne root-nak, beállíthatja egy alacsony prioritási számra

„Legolcsóbb” utak keresése a root bridge-hez

- BPDU – Bridge Protocol Data Units
 - Periódikusan (2s) küldöztetik egymásnak a bridge-ek
- Egy bridge kiszámolja az összes lehetséges útvonal árát a **root bridge** felé
 - minden port rendelkezik egy árral (*Port Cost*)
 - Adminisztratív érték, pl. fordítottan arányos a sávszélességgel
- Kiválasztja a legolcsóbb (least-cost) útvonalat
 - Az útvonalhoz vezető port lesz a **root port**
- A bridge-ek közösen kiszámolják minden LAN szegmensre hogy melyik bridge-en keresztül a legolcsóbb eljutni a root bridge-hez
 - *Designated bridge, designated port*
- A designated és a root port-ok **forwarding state**-be kerülnek
- Az összes többi porton blokkolni fog
 - Csak BPDU-k mennek át

A fa kiépülése után megtanulja a címeket

- 15 másodperc tanulási idő

9.) Mi az a piconet és a scatternet? Milyen a piconetes kommunikáció?

- **Piconet**
 - egy mester (master) és max. 7 szolga csomópont (slave)
 - Szolgák 10 méteres távon belül a master-től
 - Több piconet alkothat egy **scatternet**-et (szórt hálózat)
 - Az aktív szolgák mellett legfeljebb 255 várakozó (parked) csomópont
 - A mester alacsony teljesítményű állapotba vitte őket
 - Kímélik az akkumulátort
 - Semmit nem csinálnak, csak a mester aktiválására várnak
 - Más állapotok
 - Hold – tartás
 - Sniff – szimatolás
- Piconet – frekvenciaosztásos multiplexelés – FHSS
 - A mester vezérli az órát, kiosztja az időszeleteket
 - Két szolga csak a mesteren keresztül kommunikálhat egymással
 - Egy mester az egyik piconet-ben lehet slave a másikban

10.) Hogyan működik az FHSS?

- **Frequency Hopping Spread Spectrum** (frekvenciaugrásos szórt spektrum)
 - 2.4 GHz-s ISM sávban
 - 79 db 1 MHz-es csatorna 2.402 GHz és 2.480 GHz között (Európa, USA)
 - 23 db csatorna 2.473 GHz és 2.495 GHz között (Japán)
 - Álvéletlenszám generátorral előállított frekvencia ugrássorozatok
 - Ha két állomás ugyanazt a kezdőértéket (seed) használja, akkor ugyanazokat a frekvenciákat fogják egyszerre végigjárni
 - Időben szinkronban kell maradniuk
 - 78 db ugrássorozat, mindegyik 79 csatornával (USA, Európa)
 - Az 1. sorozat az USA-ban 3,26,65,11,46,19,74,50,22,64,79,32,62...
 - 12 db ugrássorozat, mindegyik 23 csatornával (Japán)
 - A tartózkodási idő (dwell time) az egyes frekvenciákon állítható
 - Nem lehet nagyobb 400 ms-nál
 - Leggyakrabban használt értékek: 32 ms vagy 128 ms

■ Előnyök

- Hatékony spektrumkihasználás a szabályozatlan ISM sávban
- Valamennyire biztonságos
 - Aki nem ismeri az ugrássorozatot vagy a tartózkodási időket, nem tud lehallgatni
- Jó védelem a többutas csillapítás (multipath fading) ellen
 - A jel az adótól elindulva, különböző tárgyakról visszaverődve terjed
 - Többször is eléri a vevőt
 - A vevő csak egy rövid ideig hallgat azon a csatormán
 - Nem fogják zavarni a késéssel érkező jelek a régi csatormán
- Kevéssé érzékeny a rádiós interferenciára
 - A zavaró jelek egy adott frekvenciatartományra korlátozódnak
 - A vevő hamar kiugrik onnan

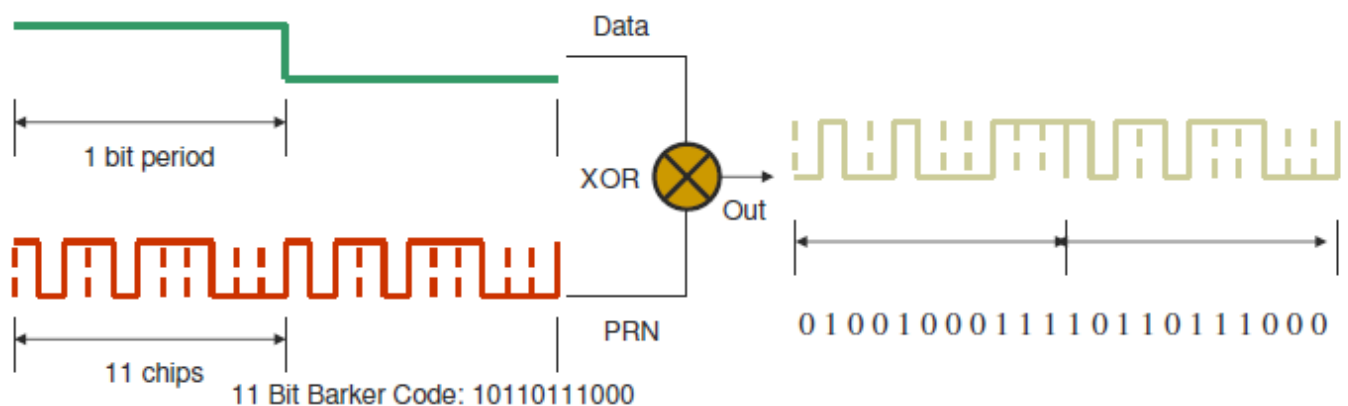
■ Hátrányok

- Kis sávszélesség (1 Mb/s)

11.) Hogyan működik a DSSS?

■ Direct Sequence Spread Spectrum (közvetlen sorozatú szórt spektrum)

- Átviteli kapacitás szintén 1 vagy 2 Mb/s
- A „hasznos” adatokat szétszórjuk a teljes frekvencia tartományban
 - XOR művelet 11 bitből álló chip-kóddal (zaj)
 - Pseudo-random sorozat, 1-ből és 0-ból, sokkal nagyobb frekvencián mint az eredeti jel
 - A zajt a fogadó ki tudja szűrni
 - Vissza tudja állítani a hasznos adatokat



■ A hasznos adatot szétszórjuk a teljes frekvenciatartományban

- A szélessávú jel nehezebben detektálható
 - Aki le szeretne hallgatni csak „zajt” érzékel
 - Nem tudja kiszűrni belőle az információt
 - Eredetileg katonai alkalmazásokra vezették be
- 11 bites chip-kód esetén 22 MHz széles sávra szór
 - 30 MHz két DSSS rendszer között, az interferenciák elkerülésére
 - Az ISM sáv 83.5 MHz széles
 - csak 3 DSSS rendszer működtethető egyszerre egy helyen interferencia nélkül

802.11a (Wi-Fi5)

A nagyobb sávszélesség érdekében újabb eljárásokat dolgoztak ki ('99)
OFDM - Orthogonal Frequency Division Multiplexing

- 5 GHz-es ISM sávban
- Akár 54 Mb/s-os átviteli sebesség
 - A frekvenciatartomány több apró szeletre osztva
 - Az átvivendő jelet is részekre osztjuk
 - Egyidejűleg több frekvencián (alvivőn) is átvitel, nagyobb átviteli sebesség
- A hagyományos FDM-ben védősávok az interferenciák elkerülésére
 - Kevesebb lehetséges frekvenciaszelet
- Az OFDM-ben ortogonális frekvenciák
 - Az egyes alvivők középfrekvenciáján a többi jel nulla értéket vesz fel

802.11b (Wi-Fi)

- **Wireless Fidelity**
 - Vezetéknélküli torzításmentesség
- Ez az első 802.11x szabvány
 - Nem a 802.11a utóda, egyszerre fejlesztették őket
- **HR-DSSS**
 - High Rate Direct Sequence Spread Spectrum
 - Hatékonyabb moduláció mint a hagyományos DSSS-ben
 - 4 átviteli sebesség a 2,4 GHz-es sávban
 - 1, 2, 5.5 és 11 Mb/s
 - Gyakorlatban szinte mindig 11 Mb/s, 100 méteres hatótávolságon
- Kisebb sebesség mint a 802.11a-nál
 - Nagyobb működési tartomány

802.11g

- 2001-ben fogadták el
 - OFDM-et használ (mint a 802.11a)
 - A 2,4 GHz-es ISM tartományban (mint a 802.11b)
 - Ugyanúgy érzékeny az interferenciákra
- 54 Mb/s-os adatátviteli sebesség
- **A jövő technológiájának ígérkezik**
 - vagy már az is...
 - Nagyon sok telepített 802.11b hálózat, eszköz létezik
 - Ameddig ezek beszerzési költsége amortizálódik, nem biztos, hogy könnyen terjed majd

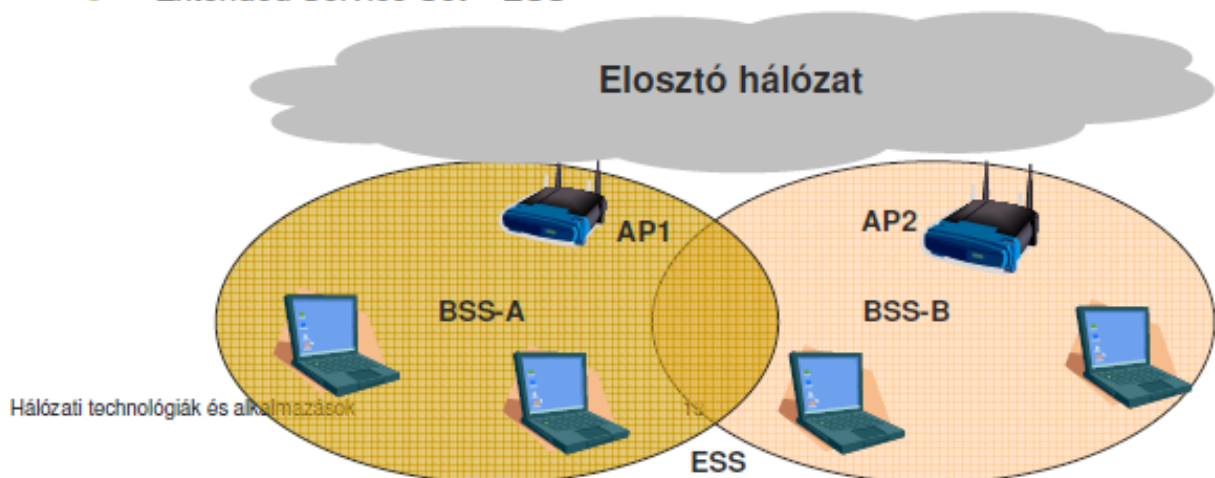
13.) Mi a különbség az ad-hoc és infrastrukturális mód között a WIFI-nél?

AD-HOC:

- Minden csomópont közvetlenül kommunikál a hatósugarán belüli többi csomóponttal
- Távolabbi csomópontok közötti kommunikáció **ad-hoc útválasztással**
 - AODV, DSR, DSDV, stb.
- Minden állomás egyben router is
 - Többugrásos ad-hoc hálózatok
 - Nincs szükség AP-ra
- Nagyon gyorsan fel lehet építeni egy ideiglenes hálózatot
 - Egy rendezvény vagy konferencia résztvevői között

INFRASTRUKURÁLIS:

- **Cellás rendszer**
 - Basic Service Set (BSS) – cella
 - Access Point (AP) – hozzáférési pont
 - Minden cellát egy AP vezérel
 - A csomópontokat periódikusan lekérdezve (polling) a csomagküldést vezérli
 - Elosztó hálózat – Distribution System (DS)
 - Az AP-kat egymáshoz kapcsoló vezetékes (Ethernet) vagy vezeték nélküli hálózat
- Több cella alkot egy kiterjesztett szolgáltatási hálózatot
 - Extended Service Set – ESS



14.) Hogyan foglalja le a 802.11b a csatornákat?

- Milyen frekvencián kommunikáljunk a cellán belül?

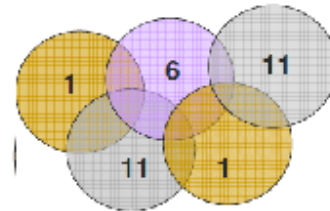
- 802.11b a 2.4 GHz-es ISM sávban
 - Max. 14 csatorna
 - Részben egymásra lapolódnak

- Országonként változó szabályozás
 - Magyarországon és Európában általában az 1-13 csatornák
 - Az USA-ban 1-11 csatornák
 - Japánban mind a 14 csatorna

- A csatornák az adóvevők által használt központi frekvenciát jelentik
 - Pl. 2,412 GHz az 1. csatorna, 2,417 GHz a 2. csatorna
 - Csak 5 MHz eltérés a központi frekvenciák között
 - A 802.11b jel kb. 30 MHz-es spektrumot fed le
 - A jel kb. 15 MHz-et foglal el a központi frekvencia mindkét oldalán
 - Átfedés jön létre több szomszédos csatorna frekvenciasávja között
 - Cellás megoldásban a szomszédos cellák frekvenciátávolságának legalább 5 csatornának kell lennie
 - Használhatjuk pl. az (1, 6, 11) kombinációt

Kis cellákat alakítunk ki

- Minden szomszédos cella más-más frekvencián kommunikál
- A cellákban használt frekvenciák nem fedik egymást



15.) Mi az a Rejtett állomás és Látható állomás problémája?

Eltér az Ethernet megfelelő protokolljától (CSMA/CD)

- Egy Ethernet állomás vár ameddig csend nem lesz, aztán elkezd adni
 - Ha nem hall zajlöketet, akkor nem volt ütközés
- Vezeték nélküli környezetben nem működik

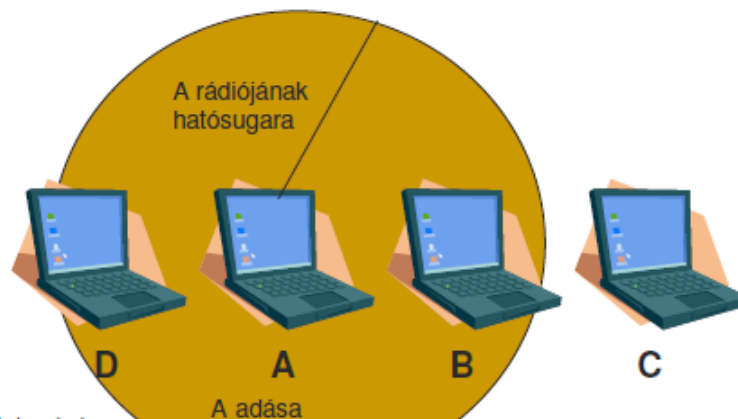
Rejtett állomás problémája

- Nem minden állomás tartózkodik az összes többi vételkörzetében
 - C ad a B-nek
 - A nem hall semmit a csatornán
 - Ő is elkezd adni B-nek



Látható állomás problémája

- B akar küldeni C-nek
 - Belehallgat a csatornába, és látja hogy foglalt A által
 - Arra következtet, hogy nem küldhet C-nek
 - Lehet, hogy A D-nek küld, nem zavarná C-t



16.) Hogyan működik a DCF és a PCF? Tudnak együttműködni?

Fél-duplex rádiók

- Nem képesek egyidejűleg adni és zajlőketet venni ugyanazon a csatornán

A 802.11 ezért nem használ CSMA/CD-t

Két másik megoldás:

- DCF – Distributed Coordination Function
 - Nem használ központi vezérlést
 - Minden megvalósításnak támogatnia kell
- PCF – Point Coordination Function
 - A bázisállomás segítségével vezényel minden tevékenységet a cellában
 - Támogatása opcionális

802.11 DCF

CSMA/CA-t használ

- Carrier Sense Multiple Access with Collision Avoidance
 - CSMA ütközésselkerüléssel
- Kétféle működési elv:
 - Fizikai és virtuális csatornaérzékelés

Fizikai csatornaérzékelés:

- Ha egy állomás adni akar, belehallgat a csatornába
 - Ha szabad, elkezd adni
- Nem figyel a csatornát adás közben
 - Lehet, hogy interferencia miatt a vevőnél megsemmisül
- Ha foglalt a csatorna, megvárja míg szabad lesz és akkor kezd el adni

802.11 PCF

- A bázisállomás vezérli a kommunikációt
 - Nincsenek ütközések
- Körbekérdezi a többi állomást, hogy van-e elküldésre váró keretük
 - A szabvány csak a körbekérdezés menetét szabályozza
 - Nem szabja meg annak gyakoriságát, sorrendjét
 - Nem írja elő, hogy minden állomásnak egyenlő kiszolgálásban kell részesülnie
- A bázisállomás periódikusan elküld egy beacon frame-et
 - 10-100 beacon/s
 - Rendszerparamétereket tartalmaz
 - Ugrási sorozatok és tartózkodási idő (FHSS-nél), óraszinkronizáció, stb.
 - Ezzel hívja az új állomásokat is, hogy csatlakozzanak a körbekérdezéshez
- A bázisállomás utasíthatja az állomásokat, menjenek készenléti állapotba
 - Addig amíg a bázisállomás vagy a felhasználó fel nem ébreszti őket
 - Kiméli az állomások akkumulátorát
 - A bázisállomás puffereket a készenléti állapotban lévőknek szánt kereteket

- A PCF és a DCF egy cellán belül egyszerre is működhet
 - Egyszerre elosztott és központosított vezérlés?
 - Gondosan definiálni kell a keretek közti időintervallumot
 - Egy keret elküldése után kell egy holtidő, mielőtt bárki elkezdene küldeni valamit
- Négy ilyen intervallumot rögzítettek
 - **SIFS – Short Inter-Frame Spacing**
 - A legrövidebb intervallum, a rövid párbeszédet folytatókat részesíti előnyben
 - A SIFS után a vevő küldhet egy CTS-t egy RTS-re
 - Egy vevő küldhet egy ACK-ot egy részre vagy a teljes keretre
 - A részlöket adója elküldheti az újabb részt, új RTS nélkül
 - **PIFS – PCF Inter-Frame Spacing**
 - PCF keretek közti időköz
 - A SIFS után mindig egyvalaki adhat csak
 - Ha ezt nem teszi meg a PIFS végéig, a bázisállomás elküldhet egy új beacon-t vagy egy lekérdező keretet
 - Az adatkeretet vagy részlöketet küldő nyugodtan befejezheti a keretet
 - A bázisállomásnak is van alkalma magához ragadnia a csatornát
 - Nem kell a mohó felhasználókkal versengenie érte
 - **DIFS – DCF Inter-Frame Spacing**
 - DCF keretek közti időköz
 - Ha a bázisállomásnak nincs mondanivalója, a DIFS elteltével bárki megpróbálhatja megszerezni a csatornát
 - Szokásos versengési szabályok
 - Kettes exponenciális visszalépés ütközés esetén
 - **EIFS – Extended Inter-Frame Spacing**
 - Olyan állomások használják, akik egy hibás vagy ismeretlen keretet vettek, és ezt próbálják jelenteni
 - Legalacsonyabb priorítás



17.) Mik az előnyei és hátrányai...

a.) ...az önkormányzati WiFi hálózatoknak?

Önkormányzati hálózatok

- Sok amerikai városban terveznek önkormányzati forrásokból a város teljes területét lefedő WiFi hálózatot létrehozni
 - Los Angeles, Boston, Philadelphia, stb.
 - Budapesten is?
- Sokan ellenzik az ötletet
 - Sokba kerül, az adófizetők pénzéből
 - Az önkormányzati források szűkösek, sok mást lehetne csinálni a pénzzel
 - A technológia hamar elavulhat, anélkül hogy a befektetés megtérülne
 - Rossz hatással lenne a helyi, kis szolgáltatókra
 - Sokak szerint gazdasági fellendülést hozhat egy városnak a WiFi lefedettség
 - A közvetlen kapcsolat nem bizonyított

b.) ... a p2p-szerű kaotikus WiFi hálózatoknak?

Az Internet szolgáltatók nem fognak örülni

- Általában nem engedélyezik a megosztást
 - Ha megosztom a szomszédommal, elesnek egy potenciális előfizetőtől
 - Még kevésbé szeretik ha valaki „viszonteladó” lesz (Bill)
- Lehet hogy mégis megérné nekik
 - Kaphatnának egy részt a bevételből
 - Minden peer amúgy is fizetne a vezetékes hozzáférésért amit megoszt
 - Annál hatékonyabb, minél több előfizető – **ma több mint 1 millió**
- Biztonsági kérdések
 - Ki a felelős az esetleges illegális letöltésekért melyek a WiFi router-emen keresztül mennek?

Több „kaotikus” módon létrehozott hotspot összekötése

- **Nem egy tervezett hálózat**
 - Néhol nagyon sűrű, máshol gyér
 - Interferenciák a sűrűn lehelyezett AP-k között
 - 4.5 millió eladott AP a világban csak 2004 harmadik negyedében
 - Az AP-kat nem konfigurálják ezek minimalizálására
- **Nem egy menedzselte hálózat**
 - A hotspotok menedzselése, karbantartása nincs összehangolva
 - SSID, biztonsági intézkedések, AP-k elhelyezése, teljesítményszabályozása
 - Legtöbbször az alapbeállításokat használják pl. a csatornaválasztásnál
 - Legtöbbször eszköz a 6-os csatornán
- Egy önmenedzselő megoldás nagyban javítaná a hozzáférés minőségét

18.) Különbségek a 802.11 (WiFi) és 802.16 (WiMax) között

- Más problémák megoldására tervezték
 - Mindkettő nagy sávszélességű vezeték nélküli kommunikáció
 - A 802.16 „épületeknek” nyújt szolgáltatásokat, nincs mobilitás
 - A 802.11 kifejezetten mobil környezetre lett kifejlesztve
- Az épületekben több felhasználó, a 802.11-ben a célállomás egy adott gép
- A 802.16 egész városrészeket, több kilométeres távolságokat fed le
 - A bázisállomáson vett jel teljesítménye a különböző adók esetén nagy szórást mutathat
 - Többféle modulációs eljárásra van szükség, a távolságtól függően
- A város feletti nyílt kommunikáció miatt a biztonság és a bizalmasság (security & privacy) elengedhetetlen követelmény
- Egy 802.16 cellában sokkal több felhasználó
 - Sokkal nagyobb sávszélesség szükséges mint amit az ISM sáv tud
- A milliméteres hullámhosszú hullámoknak más fizikai sajátosságaik vannak
 - Nagyon jól elnyeli őket a víz, a hó, sőt a köd is
 - A hibakezelésnek nagyobb szerep kell jusson, mint egy épületen belüli környezetben

19.) 802.16 MAC réteg QoS?

- A GSM cellákban azonos frekvenciasáv az upstream és downstream forgalomnak
 - A beszédátviteli forgalom általában szimmetrikus
- Internetelérésnél cél volt a nagyobb downstream kapacitás
 - A 802.16-ban rugalmas lehetőségek a sávszélesség kiosztására
- FDD – Frequency Division Duplexing
 - Frekvenciaosztásos kettőzés
 - Külön frekvenciasáv az upstream és a downstream forgalomnak
 - Két egyforma sáv
 - Egy védősáv (guard band) a kettő között
 - Inkább a szimmetrikus forgalomnak jó
- TDD – Time Division Duplexing
 - Időosztásos kettőzés
 - Nagyon jó megoldás aszimmetrikus forgalomnál, változó igényeknél

■ Közös hozzáférés megvalósítása

- Lefelé irány – TDM (Time Division Multiplex)
 - A bázisállomás egymás után szolgálja ki a kapcsolatokat
- Felfelé irány – TDMA (Time Division Multiple Access)
 - Verseny az állomások között

- Egy MAC keret egész számú időrést foglal le a fizikai rétegben
 - A keretek alkeretekből állnak
 - Az első kettő a lefele és felfele irányuló forgalom térképét adja
 - Melyik időrésben mi található, és melyek a szabad időrések
 - A lefele forgalomhoz tartozó térkép rendszerparamétereket is tartalmaz
 - Felvilágosítással szolgál a rendszerbe bekapcsolódó új állomásoknak
- A lefele irányuló csatornát a bázisállomás irányítja
- A felfele irányuló csatornáért versenyhelyzet alakul ki
 - A csatornakiosztás szorosan összefügg a szolgáltatásminőséggel (QoS)
 - Négy szolgáltatásosztály (Class of Service) definiálva a szabványban
 - **Constant Bit Rate (CBR)** – állandó adatsebességű szolgálat
 - **Real Time Variable Bit Rate (rt-VBR)** – valós idejű, változó sebességű szolgálat
 - **Non-Real Time Variable Bit rate (nrt-VBR)** – nem valós idejű, változó sebességű szolgálat
 - **Best Effort (BE)** – garanciák nélküli szolgálat
- **CBR**
 - Tömörítetlen, csendelnyomás nélküli beszédátvitelre
 - **Unsolicited Grant Services (UGS)**
 - Előre meghatározott adatmennyiség előre meghatározott időközönként
 - Minden ilyen összeköttetés számára fenntartanak időréseket
 - Nem kell egyenként kérni őket
- **rt-VBR**
 - pl. valós idejű tömörített multimédia (MPEG video)
 - **Real-time Polling Services (rtPS)**
 - Az igényelt sávszélesség folyamatosan változhat
 - A bázisállomás rögzített időközönként körbekérdezi az előfizetőket, hogy most mennyi sávszélességet akarnak
- **nrt-VBR**
 - Nem valós idejű átvitel, tárolt (pufferelt) videó vagy audio tartalom
 - Nem érzékeny a csomagvesztésre vagy a késleltetésre
 - Van idő az újraküldésekre, hibajavításra
 - **Non-real-time Polling Services**
 - A bázisállomás gyakran, de nem szigorúan előírt időközönként körbekérdezi
 - Ha egy állomás k egymást követő alkalommal nem válaszol a körbekérdezésre, a bázisállomás megvonja tőle a személyes lekérdezést
 - Egy többesküldéses (multicast) csoportba helyezi
 - A többesküldés csoport is sorra kerül a lekérdezésben
 - A csoportból bárki válaszolhat, verseny a csatornáért
 - Az alacsony forgalommal rendelkező állomások nem pazarolják az értékes lekérdezéseket

Best Effort

- Az összes fennmaradó célra
- Nincs körbekérdezés, az előfizetők versengenek a sávszélességért
 - A felfele irányuló térkép szerint vannak a verseny céljára szánt időrések
 - Ezekben kell elküldeni a sávszélességre vonatkozó igényeket
 - Az elfogadott kérésekről értesítés a következő térképben
 - A visszautasított előfizetők később újra próbálkozhatnak
- Az ütközések elkerülésére az Ethernet kettős visszalépési algoritmus

20.) Distance Vector

■ Distance vector protokollok

- csak a szomszédos routerek között kommunikálnak
 - minden router elmondja összes szomszédjának:
 - mekkora költségű utat ismer egy adott célponthoz
 - arról nem szól, hogy az út merre vezet
 - a routerek begyűjtik szomszédaiktól ezeket a hirdetéseket és kiválasztják, hogy ki hirdette a legolcsóbb utat az adott célpontokhoz
 - a megfelelő csomagokat a legkedvezőbb irányba továbbítják
 - saját költségüket a legkedvezőbbekhez hozzáadva ők is hirdetik az adott célponthoz vezető utat
- RIPv1 (RFC 1058, '88)
 - Routing Information Protocol
 - Rest In Pieces ☹
 - RIPv2 (RFC 2453, '98)
 - RIPv6 (RFC 2080, '97)
 - IPv6-os verzió
 - IGRP
 - Interior Gateway Routing Protocol
 - Cisco proprietary szabvány

Bellman-Ford algoritmus.

Távolságvektorokat tárol az útvonalakról

- Adathármasok:
 - Cél (mi a célállomás)
 - Költség
 - Következő csomópont (merre küldje)
- Rendszeresen frissítik adataikat a közvetlen szomszédok
 - Frissítő üzenet (2 részből áll):
 - Cél, költség
 - Ha a router ilyenkor jobb utat talál egy célhoz, frissíti tábláját 2 ok miatt:
 - Kisebb költségű utat talál
 - Szomszéd költsége megváltozik

Egyszerű, de nem tökéletes:

- A kapcsolatok ára változhat
- Kapcsolatok meg is szakadhatnak
 - Egy megszakadt kapcsolat ára végtelen
 - Egy olyan egész érték, mely nagyobb bármilyen lehetséges valós értéknél (RIP-nél jellemzően 16)
- A routerek topológiaváltozás esetén nem egyidőben frissítik táblázataikat
 - Periodikus időközönként (pl. 30 s) frissítő üzenet
 - Ha 6 frissítés elmarad, az ár végtelen
 - A szomszédok is frissítik a bejegyzéseiket
- **Konvergál, de lassan**
 - Csak kis hálózatokban használható

Split horizon módszer

Megakadályozás

- ha A B-től megismer egy utat, akkor az azt kiterjesztő utat B-vel már nem közli

Poisoned Reverse módszer:

- Végtelen elérhetőség hirdetése az adott linken elérhető csomópontokhoz
 - ha A B-től megismer egy utat, akkor az azt kiterjesztő utat B-nek végtelen költségű útként jelzi

21.) Link-state

A link-state protokollok működése 2 részből áll:

1. minden állomás felderíti a hálózat topológiáját
 - Hálózati topológia leírása a link állapot leíró rekordokban található
 - Link állapot leíró rekordokat kell terjeszteni
2. a kapott gráfban megkeresi a legrövidebb útvonalat és az ahhoz tartozó első állomást
 - **Fontos!**
 - A routerekben lévő topológia megegyezzen
 - Az optimális út kiválasztása ugyanúgy történjen
 - ha A router B felé számolja az optimális utat, B meg A router felé – hurok!

Dijkstra algoritmus: élek költsége a pontból, ahova el lehet jutni

OSPF – Open Shortest Path First

- Első szabvány – RFC 1131 ('89)
- OSPFv2 – RFC 2178 ('97)
- OSPFv3 – RFC 2740 ('99)
 - IPv6-os verzió

22.) OSPF

- **LSA (Link State Advertisement)** terjesztés a területeken belül
- Területek között aggregáció
 - A változások egy területen belül nem látszanak kívülre
 - Speciális terület - **Gerinchálózat (backbone)** területe (AreaID=0)
- **Internal Router (IR)**
 - Minden interfésze ugyanahhoz a területhez tartozik
- **Area Border Routers (ABR)**
 - Legalább két területhez kapcsolódik
 - Minden területet összekötünk a gerinchálózattal egy ABR-en keresztül
 - lehet virtuális is, egy tranzit területen keresztül
 - **Route summarization** – aggregált útvonalak
- **Backbone Router (BR)**
 - Legalább az egyik interfésze a backbone-hoz csatlakozik
- **Autonomous System Border Routers (ASBR)**
 - Kapcsolat az Internet felé

23.) IP v4-ről IP v6-ra való áttérés

Dual Stack (dupla protokoll verem)

- IPv4/IPv6 egyszerre ugyanazon az eszközön

Alagutak

- Kezdetben, IPv6 csomagok alagutazása IPv4 felhőkben
- Később IPv4 csomagok alagutazása IPv6 felhőkben

Protokoll fordítás

- Protokoll információkat hordozó fejlécből másik protokoll fejléc létrehozása fordítási szabályok alkalmazásával
- IPv6 <-> IPv4

24.) IP v6 kiegészítő fejlécek

Hop-by-hop Options Header

- A csomag útvonalán található gépek számára tartalmaz IP opciókat
- Az útvonal minden útvonalválasztójának meg kell vizsgálnia és fel kell dolgoznia a Hop-by-hop Header-t
- Router Alert opció riasztja a tranzit útvonalválasztókat
 - Ha a csomag olyan információkat tartalmaz, melyeket egy közbeeső routernek fel kell dolgoznia
 - Különben nem próbálja meg értelmezni a csomagot, csak továbbküldi

Routing Header

- Normál esetben az IP csomag forrása a hálózatra bízta a csomag eljuttatását a célhoz
- Lehetőség van forrás oldali útvonal megadására az útválasztók címeivel
 - A teljes lista a Routing Header-ben (pl. A, B, C, D)
 - A célcím mindig a következő útválasztó címe (A), kivéve az utolsó útválasztót
 - A célcímet minden útválasztó átírja továbbítás előtt

Fragment Header

- IPv4 – tördelés és visszaállítás automatikusan, ha explicit módon nem tiltják
- IPv6 - alapértelmezésben a csomagokat nem tördelik
 - ha a csomag túl nagy a közeg számára, eldobják és ICMP üzenet
 - a host felderíti az átviteli közegre jellemző MTU-t
 - Maximum Transmission Unit
 - alapesetben megpróbál kisebb csomagokat küldeni, mint az MTU
 - ha tördelésre van szükség, az a Fragmentation Extension Header-el oldható meg

Authentication Header

- Garantálja, hogy a ...
 - vett csomag hiteles
 - nem változtatták meg az út során
 - megadott küldőtől érkezett

Destination Option Header

- A cél opció a cél számára tartalmaz IP opciókat

25.)