

Hálózati Technológiák és Alkalmazások

Vida Rolland
BME TMIT

2016. március 10.



TMIT



INTERNET_{OF} THINGS

VERSENY



Fődíj: **250 000 Ft**

Közönségdíj: **100 000 Ft**

A prototípus elkészítéséhez: **6 x 50 000 Ft**

Jelentkezés:

március 10.
MA ÉJFÉLIG!

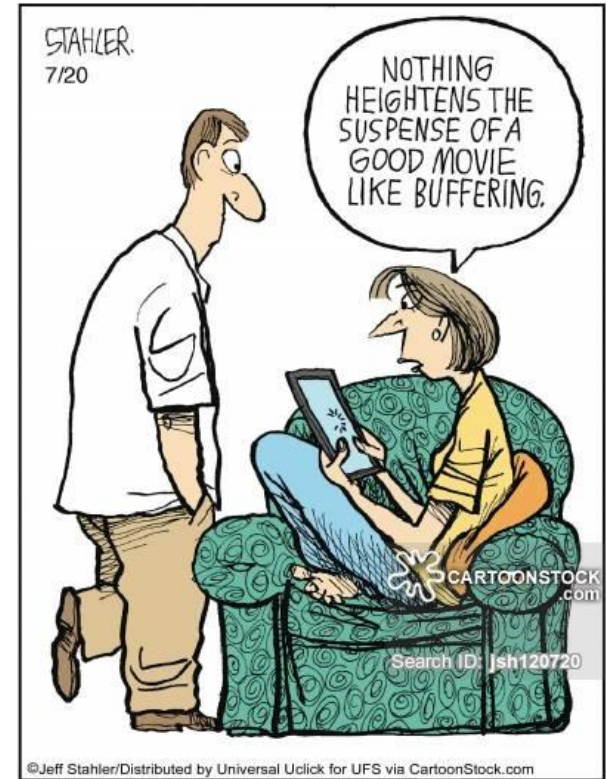
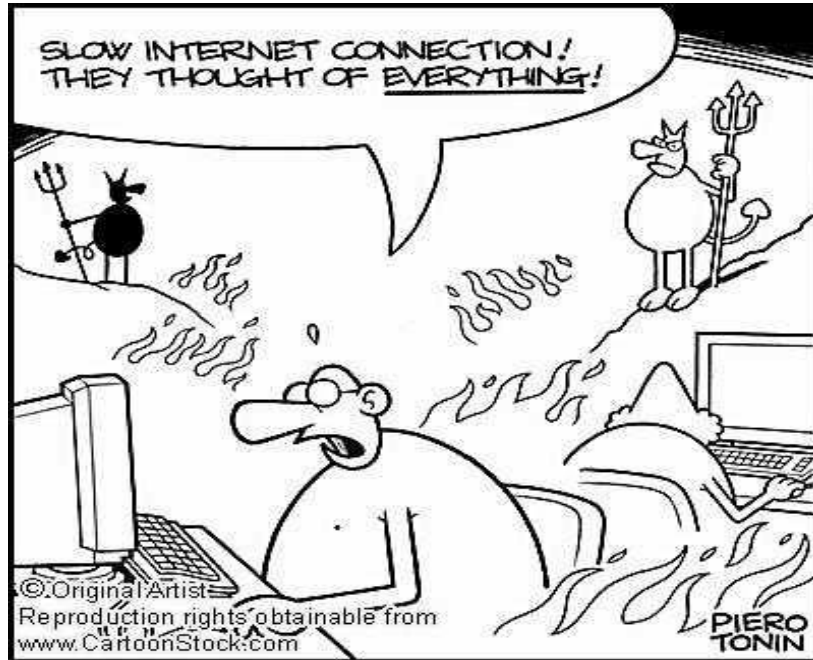
Miért kellene mégis optikai hálózatok?

- Ma már nem a webezés, hanem a multimédia a fontos
 - MPEG-1 – ISO/IEC szabvány
 - Moving Pictures Experts Group
 - 50:1 – 100:1 video tömörítés
 - 1.5 Mbps, VHS minőségű kép
 - MPEG-2
 - DVD minőségű kép
 - Nagy felbontás, nagy színmélység, sok mozgás (pl. sportközvetítés) – 4-8 Mbps
 - HDTV – 14 Mbps, **8K UHD TV – 50 Mbps** (7680 x 4320, 60 fps)
- Az xDSL sávszélessége messze nem elegendő ehhez
 - Csak nagyon rövid helyi hurkok esetén

Miért kellene mégis optikai hálózatok?

- HFC (Hybrid Fiber Coax)
 - Az eredeti 300-550 MHz-es kábeleket 850 MHz-s koax kábelek váltják föl
 - Plusz 300 MHz → 50 db új 6 MHz-es csatorna
 - QAM-256-al 40 Mbps egy csatornán → 2 Gbps új sávszél
 - 500 ház egy kábelén → mindenkinek jut 4 Mbps downstream, ami elég egy MPEG-2 filmhez
 - Szépen hangzik, de...
 - Minden kábelt le kell cserélni 850 MHz-es koaxra
 - Új fejállomások, új fényvezető csomópontok (fiber node), kétirányú erősítők
 - Szinte a teljes kábelhálózati rendszert le kell cserélni
- **Akkor miért ne legyen minél több fényvezető szál benne?**

A kis sebesség ma már kínzás!!



Adatátvitel fényvezető szálon

- Három fő komponens:
 - **Fényforrás**
 - LED (light emitting diode), félvezető lézer
 - **Átviteli közeg**
 - Rendkívül vékony üvegszál
 - **Fényérzékelő (detektor)**
 - fény hatására elektromos impulzusokat állít elő
- Az adatátviteli sebességet az átalakítás sebessége határozza meg
 - A gyakorlati sebesség egy szálon ma 10-50 Gbps

Fényvezető szálak



- 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)

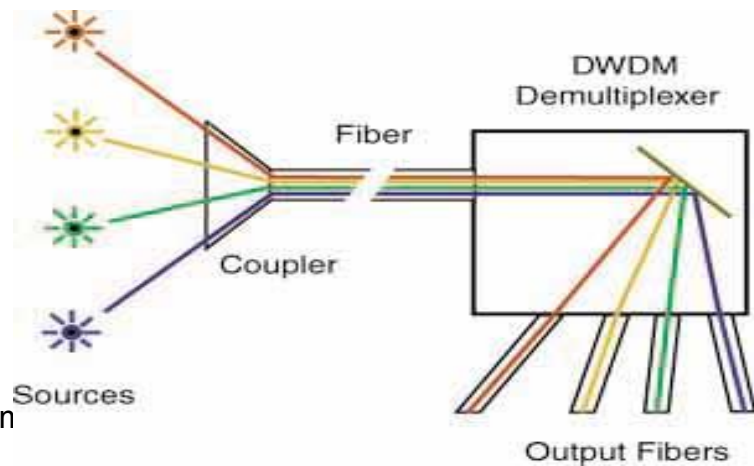


- Egymódusú szál

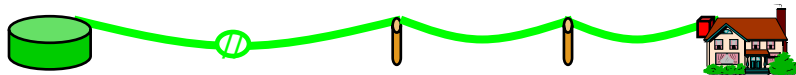
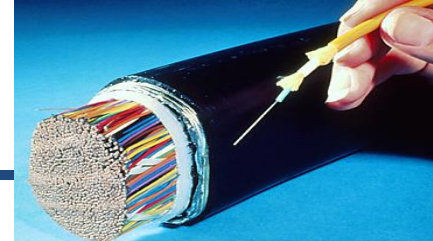
- Ha az üvegszál átmérője nagyon kicsi, a fény visszaverődés nélkül, egyenesen terjed
- Jóval drágább a szál, és nagyobb kapacitású, jobb lézereket igényel
- Nagyobb távolságok áthidalására sokkal jobb
 - 50 Gbps 100 km távolságba erősítés nélkül
 - A transzatlanti optikai kábeleknél nagyon fontos, hogy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

Hullámhossz osztás

- WDM – Wavelength Division Multiplexing
 - Több hullámhossz (szín) ugyanazon az üvegszálon
 - Kezdetben csak 2 szín
 - Ma már akár 160
 - 10 Gbit/s szálon elméletileg 1.6 Tbit/s



Fiber vs. Réz érpár



- Optikai kábel

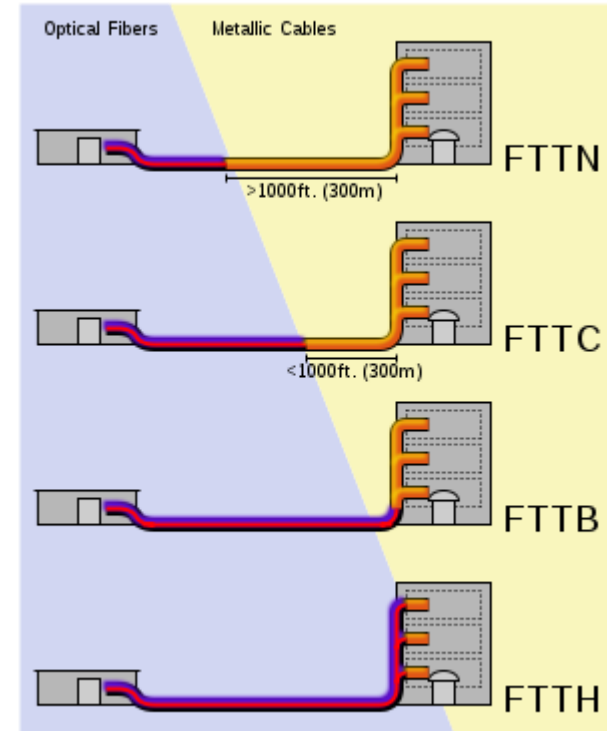
- Fényjelekkel működik
- Nem érzékeny az elektromágneses interferenciákra
- Ismétlők kb. 30 km után
- Kismértékű hőágulás
- Törékeny, viszonylag merev anyag
- Kémiaailag stabil

- Réz érpár

- Elektromos hullámok
- Érzékeny az elektromágneses interferenciákra
- Ismétlők 5 km után
- Nagymértékű hőágulás
- Hajlítható anyag
- Érzékeny a korrózióra és galvanikus reakciókra
- Újrahasznosítható
 - Jó pénzért el lehet adni a rezet

FTTx

- FTTx – Fiber To The x
 - FTTN – Fiber To The Neighborhood
 - FTTC – Fiber To The Curb
 - FTTB – Fiber To The Building
 - **FTTH – Fiber To The Home**
 - ...
 - FTTO – Fiber To The Office
 - FTTD – Fiber To The Desk
 - FTTE – Fiber To The Enclosure
 - FTTP – Fiber To The Premises
 - FTTU – Fiber To The User

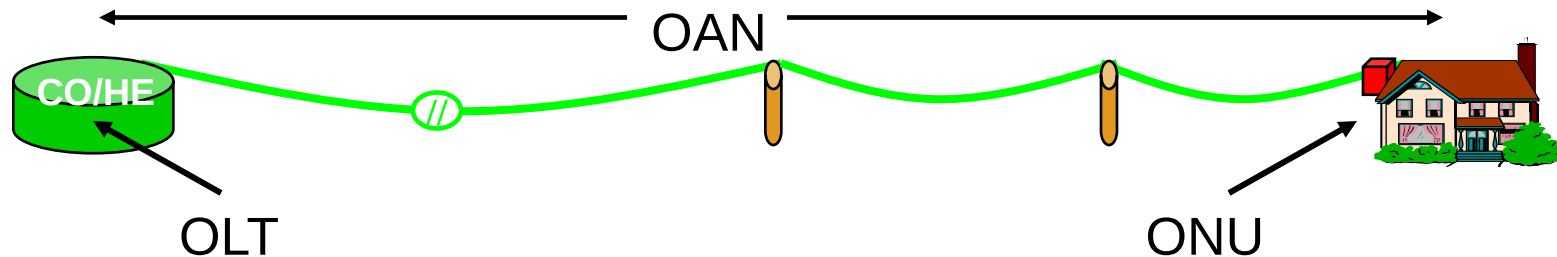


FTTC/FTTB

- **Fiber To The Curb / Building**
 - Üvegszál az elosztódobozig / épületig
- Üvegszál a helyi központból minden lakókörzetig
 - A szál egy ONU-ban végződik
 - Optical Network Unit – optikai hálózategység
 - Több helyi rézhurok, coax, 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

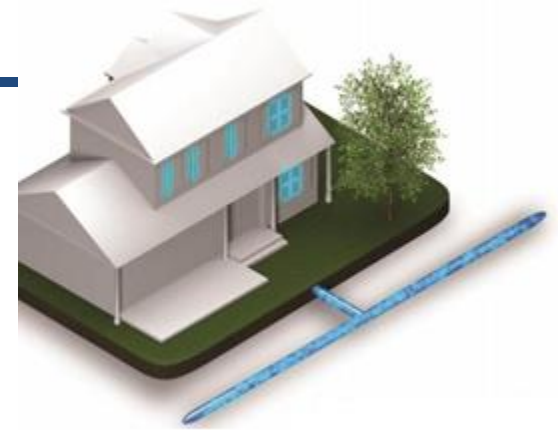
FTTH – Fiber To The Home

- 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



Miért FTTH?

- Az FTTH előnyei
 - Hatalmas adatátviteli kapacitás
 - Könnyen feljavítható (upgrade)
 - Könnyen telepíthető
 - Földben és levegőben vezethető kábelek
 - Teljesen szimmetrikus szolgáltatásokat biztosít
 - Külön hullámhosszon a downstream és upstream forgalom
 - Korábban kétszál as verziók is
 - Alacsony üzemeltetési és karbantartási költségek
 - Nagyon nagy távolságok esetén is működik
 - Kis átmérőjű, könnyű kábelek
 - Nem zavarják elektromágneses interferenciák

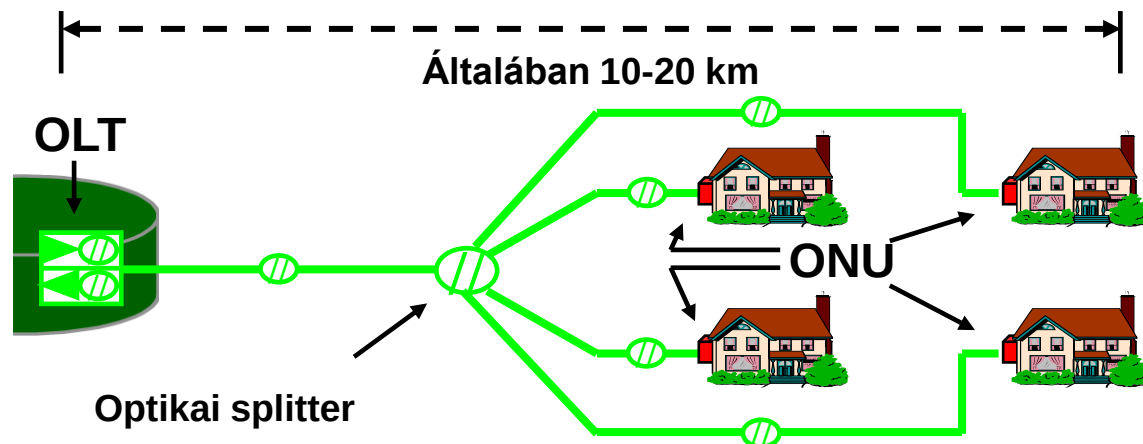


FTTH architektúrák



- **PON – Passive Optical Networks**

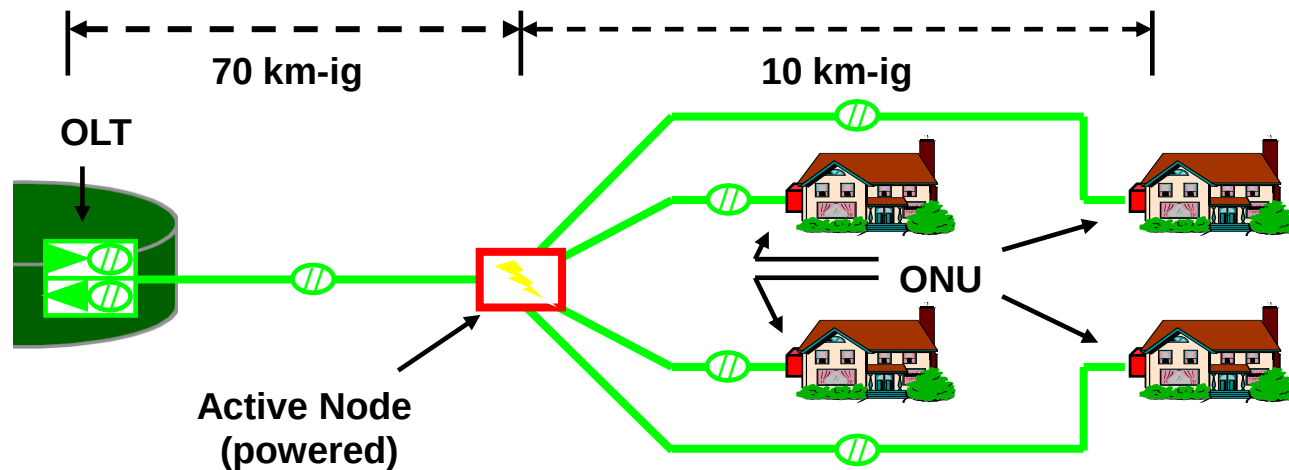
- Több felhasználó megoszt egy fényvezető szálát
- Optikai splitter-ek a jel szétválasztására és aggregálására
- Áramellátás csak a végeknél szükséges
- Osztott hálózat – Point to Multipoint (P2MP)



FTTH architektúrák

- **Active Node**

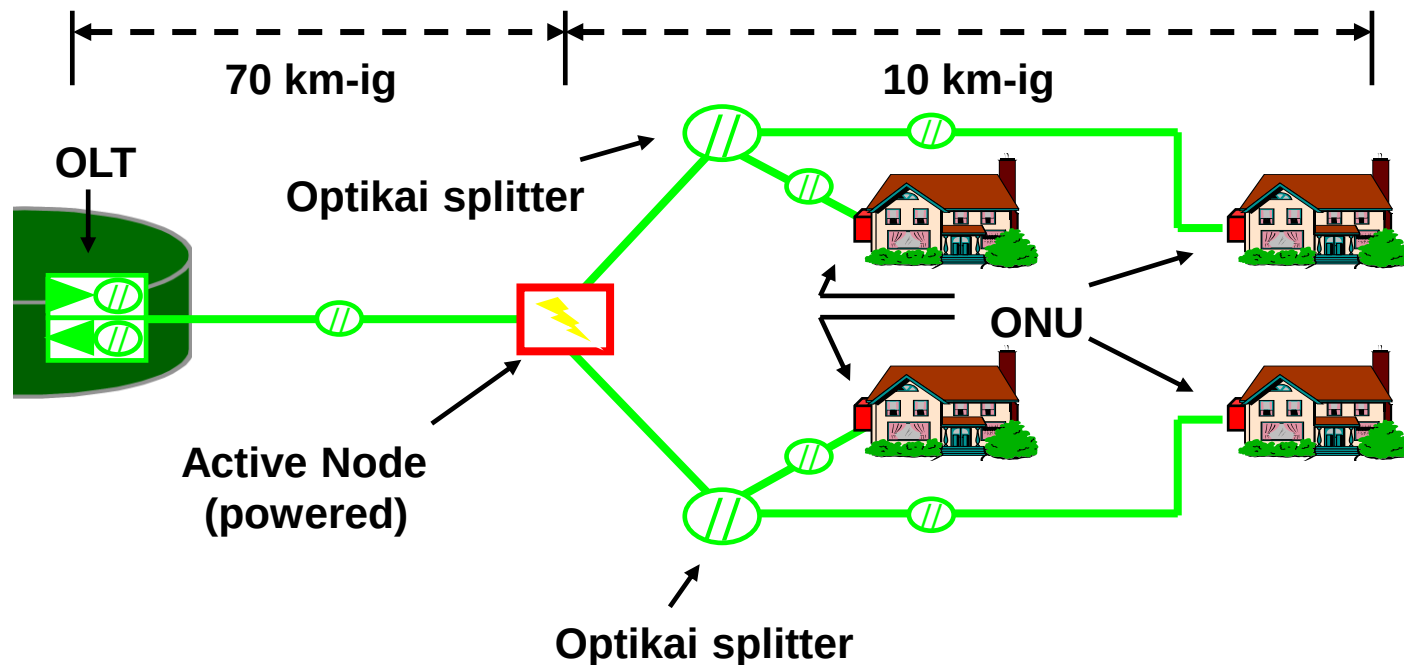
- Az előfizetőknek saját fényvezető száluk - Point to Point (P2P)
- Aktív, árammal táplált csomópontok a forgalom elosztására - Ethernet switch
- Layer2/Layer3 switching/routing



FTTH architektúrák

- Hybrid PON

- Az előbbi két architektúra kombinált változata

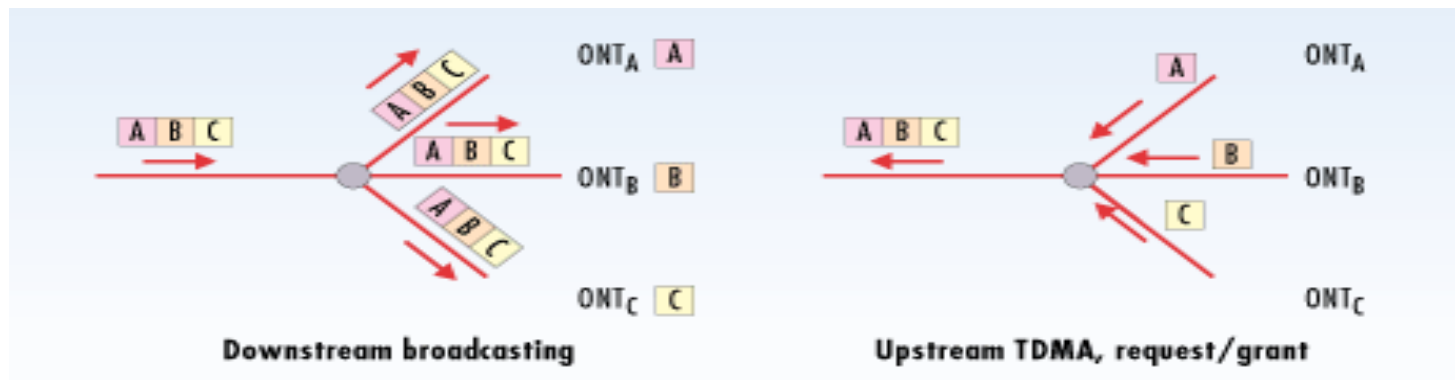


Ethernet vagy ATM alapú PON?

- Egy OLT-hez több PON köthető
 - Mindegyik olcsó passzív optikai filtereken keresztül jut el sok ONU-hoz
- Két külön technológia vetélkedik egymással
 - APON – ATM-based PON
 - ITU-T G.983.x
 - Az első PON implementáció
 - EPON – Ethernet-based PON

PON 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
 - Időszeletek kiosztása igénylések függvényében



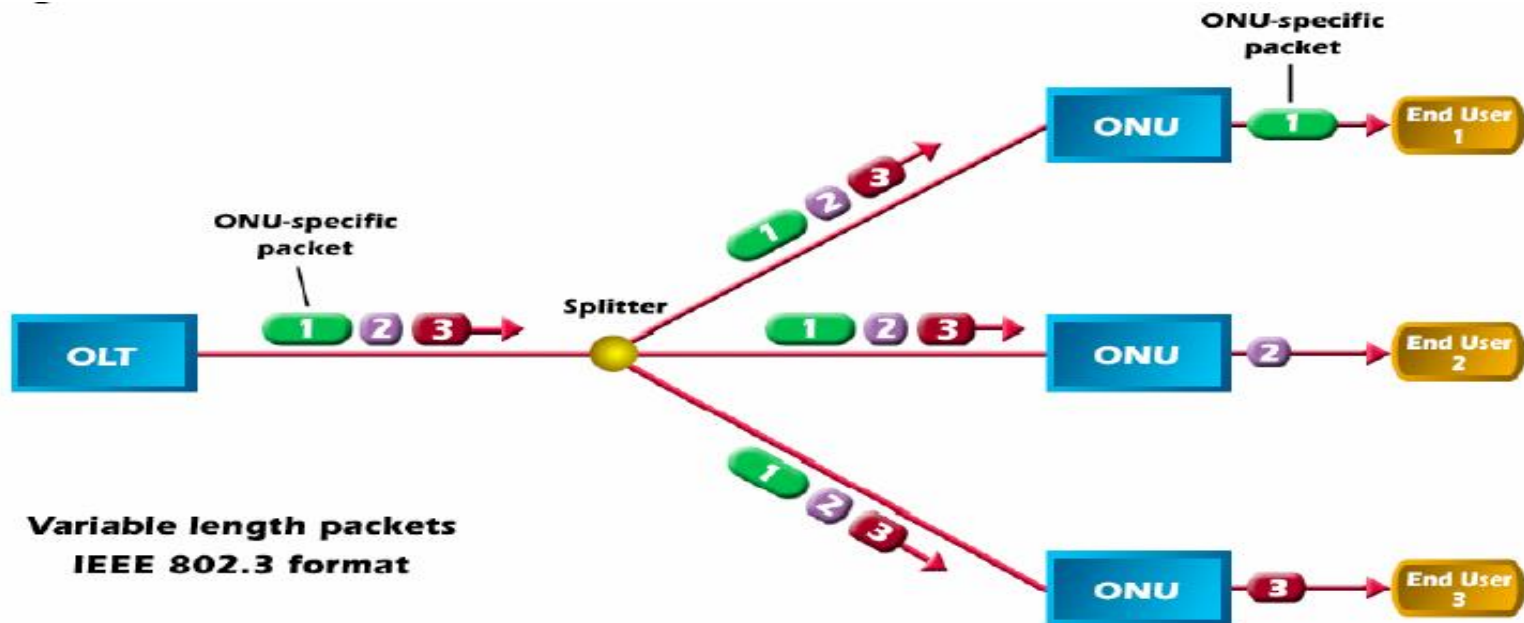
APON

- **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

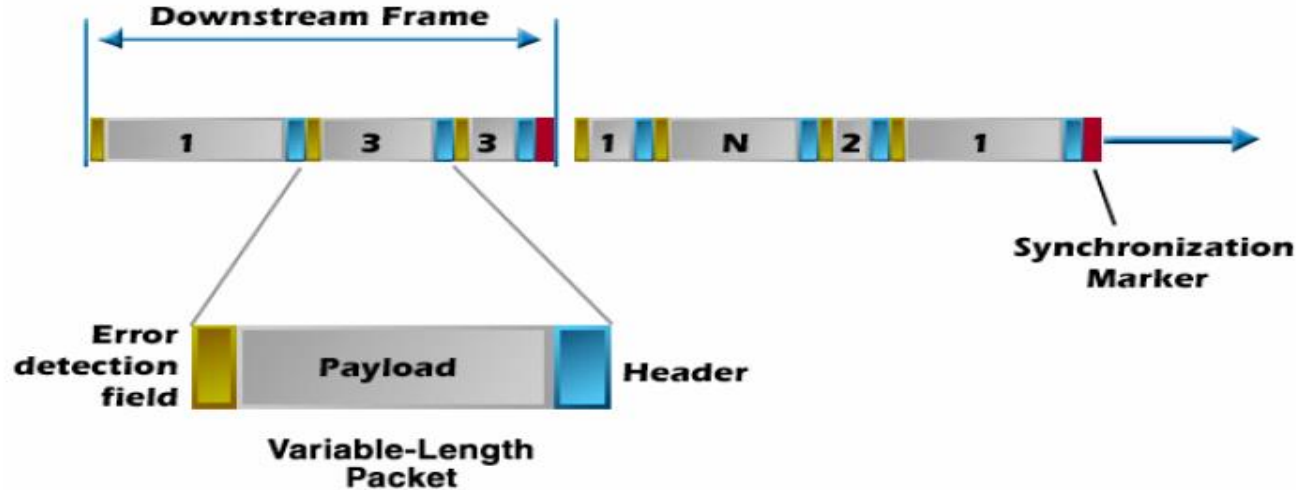
EPON

- Az adatok az IEEE 802.3 (Ethernet) formátumot használják
 - Változó hosszúságú csomagok 64 és 1518 byte között
- Hogyan oldjuk meg a TDMA alapú feltöltést?
 - Feloszthatnánk az Ethernet kereteket (frame) fix hosszúságú részekre
 - Egyszerűbb lesz a feltöltés
 - Az ár egy SAR funkció hozzáadása az EPON protokoll stack-hez
 - **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

EPON downstream forgalom

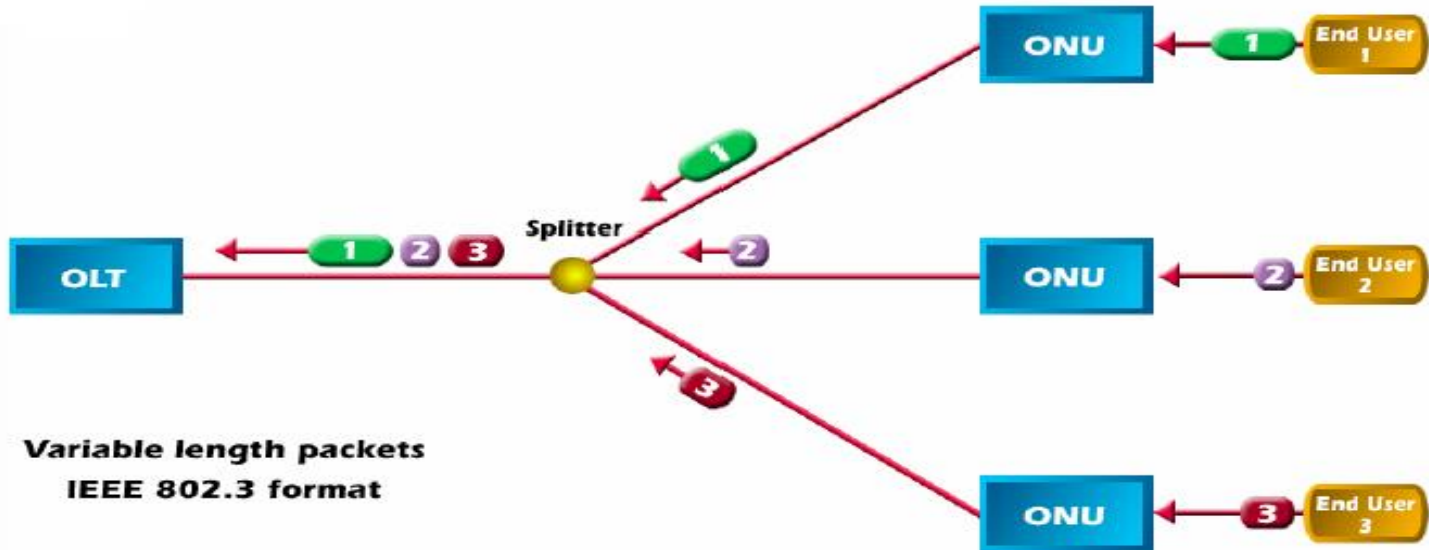


EPON downstream csomagok

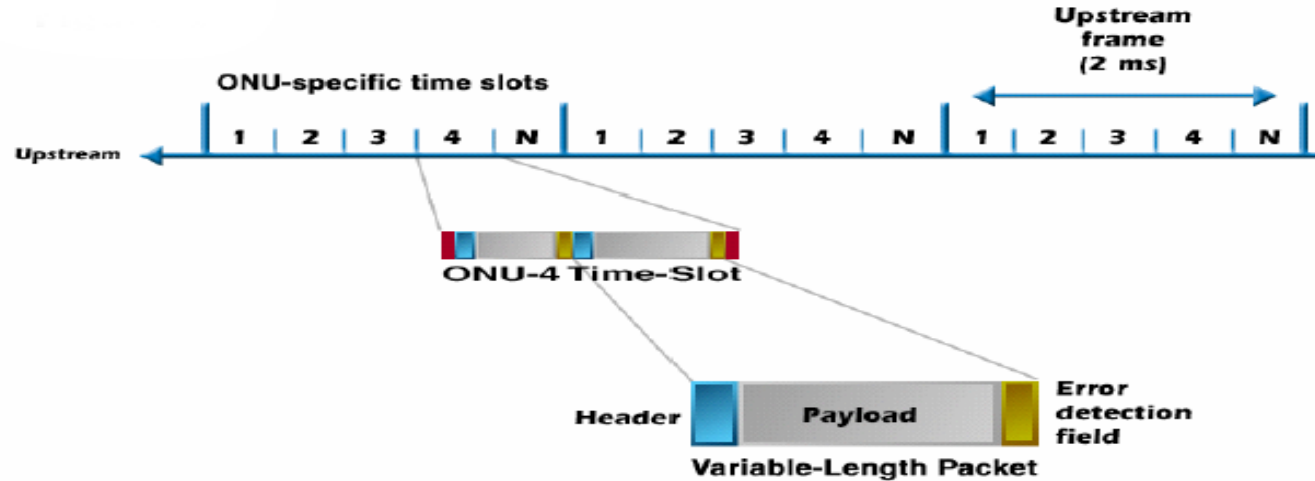


- Fix időközönként (2ms) küldött frame-ek, változó hosszúságú csomagokkal
- Szinkronizációhoz szükséges információ minden frame előtt
- Minden csomag fejléce megmondja ki a címzett
- Hibaellenőrző információ a csomag végén

EPON upstream forgalom



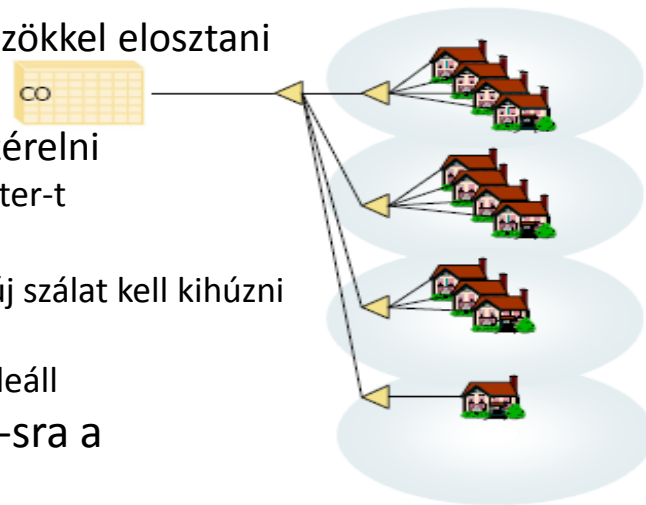
EPON upstream csomagok



- Az upstream forgalom frame-ekre (2ms) osztva
- Minden ONU-nak van egy saját időszelete, melyet változó hosszúságú csomagokkal tölthet fel

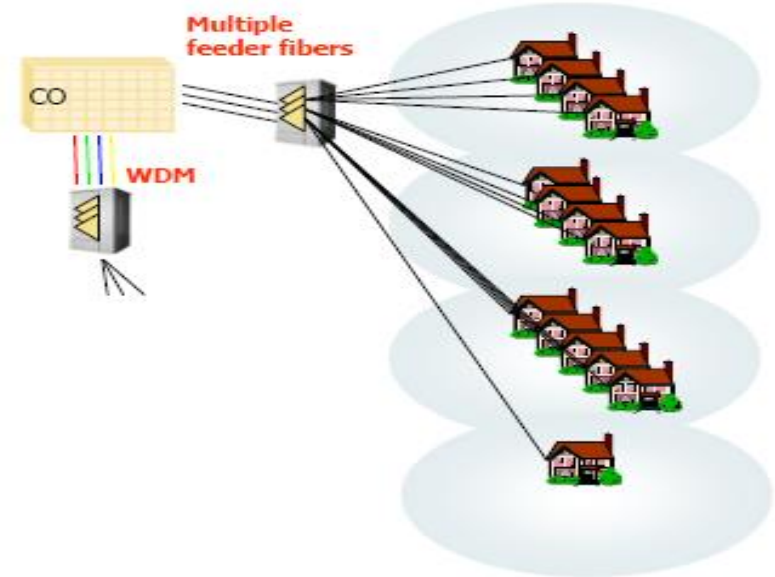
Hagyományos PON

- Az alapötlet:
 - Mindenki nem éri meg külön szálát kihúzni az OLT-től
 - Elég egy szálát közel vinni a felhasználókhoz, majd passzív eszközökkel elosztani
- Hátrányok
 - A splitter-ekben nincs intelligencia, nem tudod őket távolról vezérelni
 - Ha valami hiba van, nem könnyű egyenként megnézni minden splitter-t
 - Nem flexibilis
 - Ha egy 4-es splitter-en keresztül csatlakozol, egy 5-ik előfizetőnek új szálát kell kihúzni
 - Újratervezni a hálózatot, betenni egy nagyobb splitter-t
 - Egy splitter cseréjénél minden downstream előfizető szolgáltatása leáll
- Megoldás: ha 1x32-es splittert használsz, ne tervezd 32 ONU-sra a hálózatot, csak 16-osra vagy 24-esre
 - Van hely bővítésre
 - A maradék 16-nak többre fog kerülni a szolgáltatás



Passive Star PON

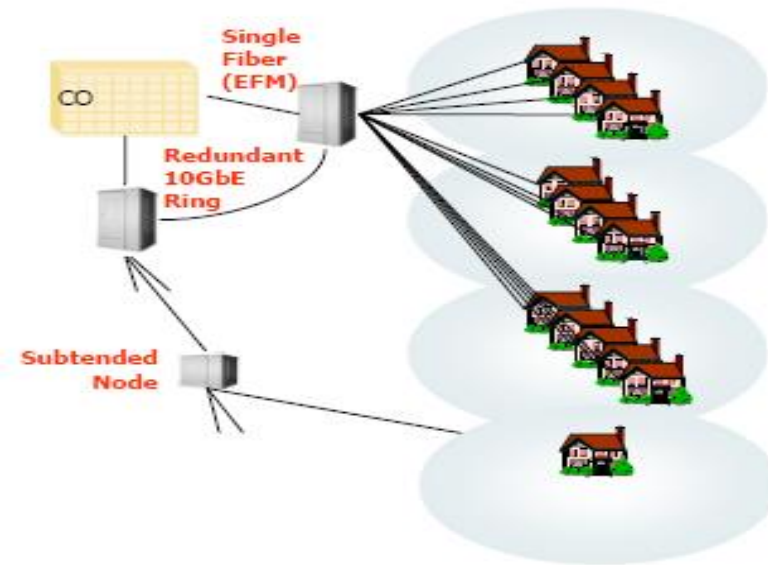
- A splitter-ek egy dobozban csoportosítva
 - Egyszerűbb a hibaelhárítás
- Továbbra is fa struktúra
 - Ha a splitter és a CO közötti szál meghibásodik, nincs backup
 - A splitterek passzívak, nem tudnak átváltani egy új útvonalra hiba esetén



Active Star

- Hátrány az aktív (árammal ellátott) node szükségessége
- Sok szempontból előnyös intelligens eszközöket használni a hálózat szélén
 - Az aktív node **IGMP*** proxy-ként működhet
 - Multicast forgalom támogatása
 - Hatékony erőforráskihasználás
 - Hibatűrő megoldás
 - Az aktív node-ok gyűrűbe kötve
 - **Ethernet Protection Switching Rings (EPSR)**
 - 50 ms alatti váltás hiba esetén
 - Video esetén pillanatnyi kockás kép
 - Egy telefon kapcsolat nem szakad meg
 - Könnyen menedzselhető, könnyű hibaelhárítás

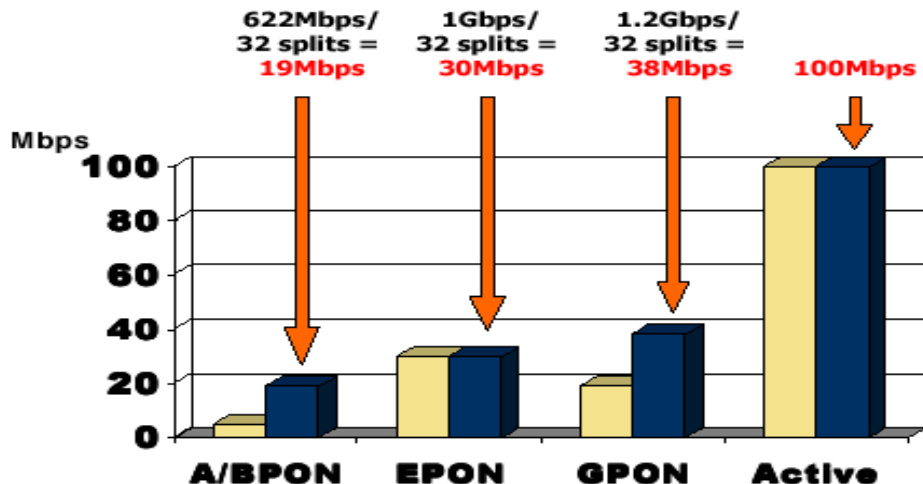
***IGMP- Internet Group Management Protocol**



Újabb verziók

- **Broadband PON**
 - 622 Mbps downstream, 622 Mbps upstream
- **Gigabit PON**
 - Több downstream/upstream változat
 - Legelterjedtebb az 2.48 Gbps downstream és 1.244 Gbps upstream
- **XGPON (10G-PON) – 2010**

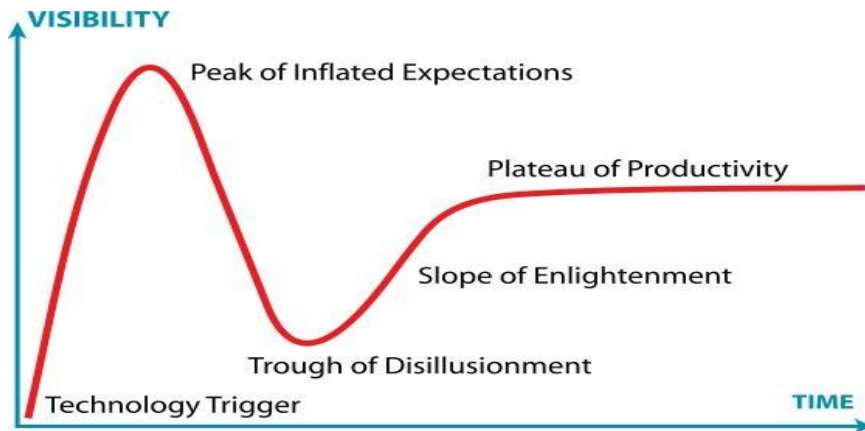
Adatátviteli sebességek összehasonlítása



- PON megoldásoknál kisebb sebességek
 - Osztott rész az OLT és az első splitter között
 - Valamivel jobb a helyzet ha nem telített a splitter
 - Nem 32-be, hanem csak 16-ba vagy 24-be kell osztani
- Active Node-nál mindenkinek saját fényvezető szála
 - Magánfelhasználóknak általában 100 Mbps mindkét irányban
 - Üzleti előfizetőknek akár több Gbps

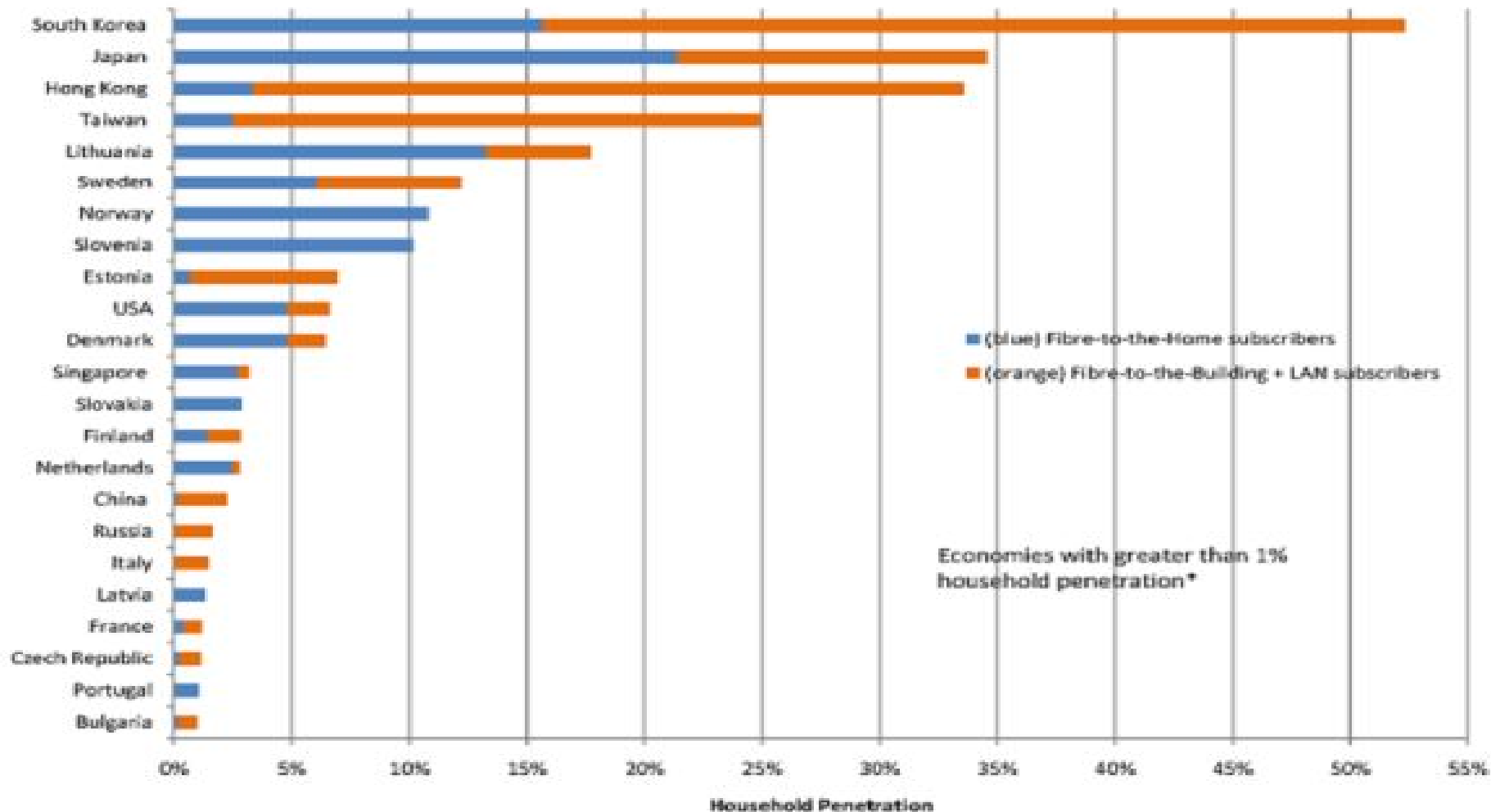
FTTH/FTTB elterjedése

- Az FTTH/FTTB még gyerekcipőben
 - Kezdeti, növekedési fázis
 - A közeljövőben továbbra is Ázsia vezeti majd a versenyt
- A nagy Telco cégek közül kevesen vezették be

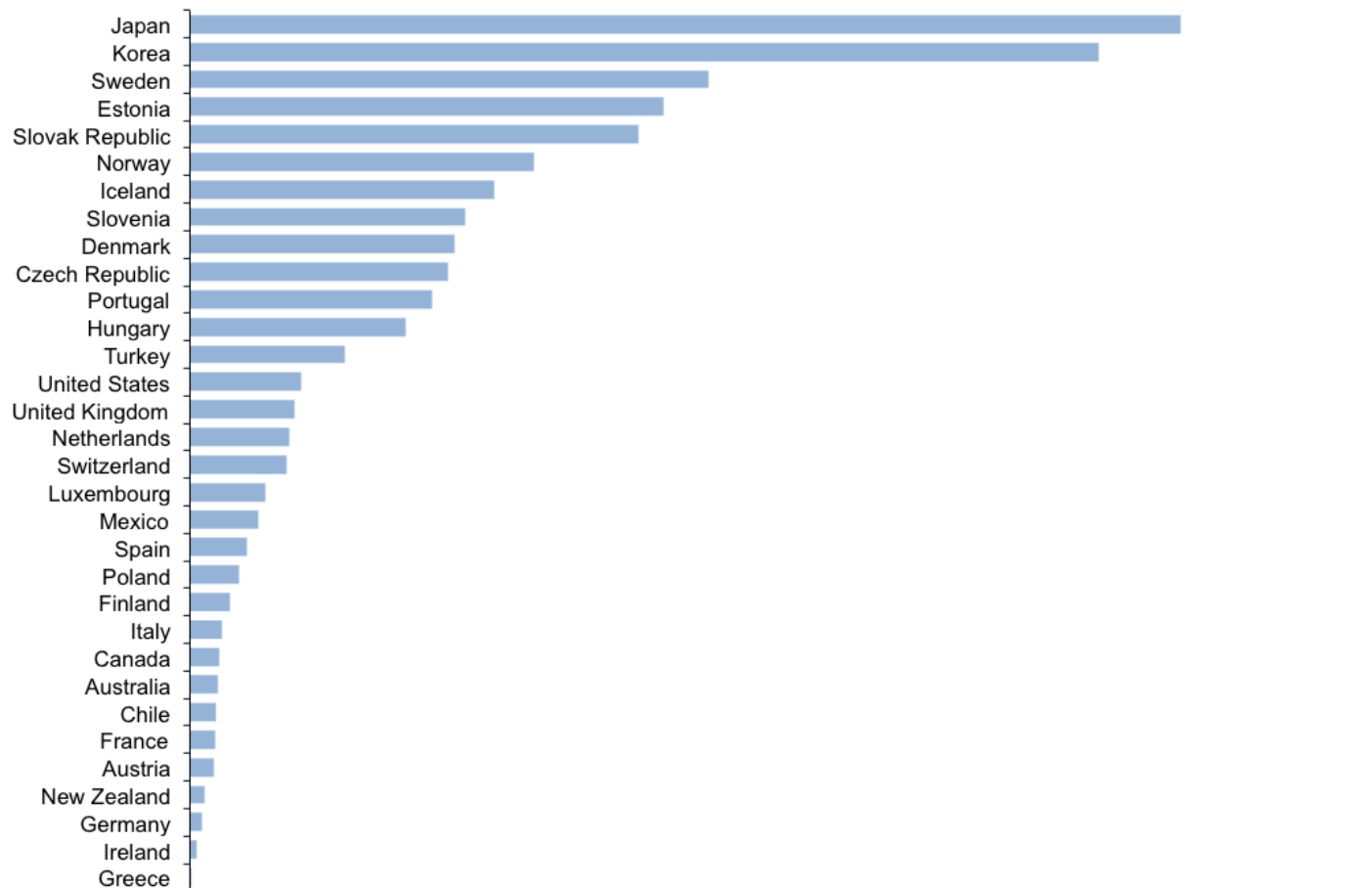


Feb. 2010

Economies with the Highest Penetration of Fibre-to-the-Home / Building + LAN



Percentage of fibre connections in total broadband subscriptions, June 2013

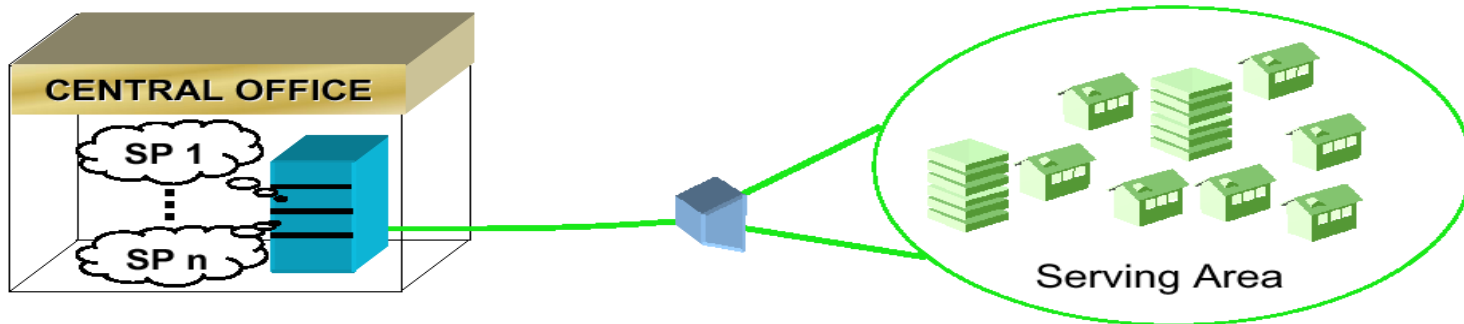


FTTx szolgáltatás

- Két szolgáltatási modell
 - Saját hálózat
 - Az FTTx szolgáltatások nagy része
 - A hálózat tulajdonosa egyenesen a felhasználóknak adja el a szolgáltatást
 - Hagyományos telefon és kábeltévé szolgáltatási modell
 - Nyílt hozzáférés
 - Több országban törvényi szabályozás miatt
 - A hálózat tulajdonosa átadja az infrastruktúrát több viszonteladó szolgáltatónak, ők szerződnek a felhasználókkal

Nyílt hozzáférés (Open Access)

- A tulajdonos egyenlő feltételek mellett adja át a hálózatát különböző szolgáltatóknak (Telco, ISP, video szolgáltató, stb)
 - Saját maga nem lép be a versenybe
- Általában önkormányzati, városi hálózatok
 - A hálózati infrastruktúra közszolgáltatásnak számít
 - Úgy mint a víz, az áram vagy az úthálózat



Open Access példák

- Sok önkormányzati Open Access hálózat Nyugat Európában és főként Skandináviában
 - Stokab (Stockholm) – az első önkormányzati FTTx hálózat (1996)
 - Vasterbotten – vidéki régió, fele akkora mint Hollandia, 260.000 lakos
 - 15 önkormányzat összekötve egy FTTx hálózaton
 - Svédországban 289 önkormányzat, több mint 200-nak saját hálózata
 - CityNet, Amsterdam – 450.000 házat bekötő hálózat
 - Több önkormányzati hálózat Dániában
- Franciaországban és Angliában új törvényjavaslatok a nyílt hozzáférésű hálózatok támogatására vagy kötelezővé tételére
- Néhány önkormányzati hálózat az USA-ban

FTTH Európában

- Sok országban jogilag szabályozva
 - Nemzeti szélessávú stratégiák
- Miért nem építenek saját optikai hálózatot az „incumbens” szolgáltatók?
 - Így is uralják a piacot, nincsenek rákényszerítve
 - A rövid előfizetői hurkok miatt viszonylag magas xDSL sebességek
 - Skandináviában olcsóbb az önkormányzatok hálózatait bérelni, mint sajátot építeni
 - A videoátvitel még nem annyira követelmény mint Ázsiában
- A helyi önkormányzatoknak az FTTH egy fontos eleme a regionális fejlesztésnek
 - Vonzóvá teszi a régiót, megéri befektetni

FTTx saját hálózaton

- Versenyhelyzetes piacok
 - Minden szolgáltatónak saját hálózata, mellyel lefedik ugyanazt a területet
 - Leginkább jellemző az USA-ban és Japanban
 - 9 japán szolgáltatónak van saját hálózata
 - Európában is van rá példa (Hollandia)
 - Nagyobb sebességek, kisebb üzemeltetési költségek (OpEx)
 - Nagyobb tőkeberuházás (CapEx)



FTTH verseny Tokió belvárosában



Biztonságos kommunikáció

- Egy osztott közegen bárki elolvashatja a mellette elhaladó forgalmat
- Hogy a szomszédot ne hallgathasd le, a forgalom titkosítva halad mindkét irányban
 - Meg kell egyezni egy közös titkosítási kulcsban
 - Két „idegen” között, egy osztott, lehallgatható közegen
 - **Diffie-Hellman** algoritmus
 - Aliz és Bob megegyezik két nagy prímszámban: **n** és **g**
 - Bizonyos feltételeket teljesíteniük kell
 - Nyilvánosak, mondjuk Bob választ és elküldi nyíltan Aliznak
 - Aliz kisorsol egy nagy (512 bites) számot: **x**
 - Bob kisorsol egy hasonlót: **y**
 - Aliz elkezdi a kulcscserét: elküldi Bobnak az **(n, g, $g^x \bmod n$)** hármast
 - Bob visszaküldi a **$g^y \bmod n$** értéket
 - Mindketten kiszámolják a közös kulcsot:
 - **$(g^x \bmod n)^y = (g^{xy} \bmod n) = (g^{yx} \bmod n) = (g^y \bmod n)^x$**
 - Cecil ismeri **g**-t és **n**-t, de nem tudja visszafejteni **x**-et és **y**-t
 - Túl sok időt venne igénybe, még egy szuperszámítógéppel is

MITM támadás

- A Diffie-Hellman algoritmus nem véd a MITM támadás ellen
 - Man-In-the-Middle
 - Honnan tudom hogy Alíz tényleg Alíz-e?
 - Cecil kisorsol egy saját számot: z
 - Elfogja Aliz $(n, g, g^x \bmod n)$ hármasát és saját $(n, g, g^z \bmod n)$ hármasát küldi tovább Bobnak
 - Elfogja Bob $g^y \bmod n$ válaszát és a saját $g^z \bmod n$ választát küldi tovább Aliznak
 - Megegyezik Alizzal a $(g^{xz} \bmod n)$ és Bobbal a $(g^{yz} \bmod n)$ közös kulcsban
 - Aliz és Bob azt hiszik egymással beszélnek, pedig Cecil közöttük van
- Szükséges valamilyen autentikációs megoldás
 - Digitális aláírás
 - Publikus/privát kulcspár
 - Aliz ismeri Bob publikus kulcsát
 - » Biztos hogy ez tényleg Bob publikus kulcsa?
 - » Certificate authority – trusted third party (megbízható harmadik fél)
 - Bob egy digitális aláírást csatol a csomagjához, a privát kulcsot használva
 - Aliz ellenőrizni tudja Bob publikus kulcsával hogy a csomag tényleg Bobtól származik