
Hálózati Ismeretek

OSI modell, Fizikai réteg



Az OSI modell

- ▶ **Open Systems Interconnection Reference Model**
- ▶ ISO/IEC 7498-1
- ▶ Számítógépek kommunikációját leíró absztrakt modell
- ▶ Ténylegesen csak és kizárólag papíron létezik.
- ▶ Gyakorlatban a TCP/IP modell terjedt el, ami szintén az OSI modellen alapul
- ▶ Kidolgozni az 1970-es években kezdték
- ▶ ISO kezdeményezés volt



Az OSI modell

- ▶ A kezdeményezés oka az volt, hogy abban az időben is léteztek hálózatok
- ▶ Azonban egyik sem volt kompatibilis más gyártó technológiájával, csak saját magával
- ▶ Kezdetben csak modell ajánlás volt, később lett szabvány szintre emelve
- ▶ Szabványokból két fajta létezik (kiegészítés):
 - ▶ De-jure: nemzetközi szakmai bizottságok által megalkotottak, hivatalos dokumentumok rögzítik
 - ▶ De-facto: egy-egy megoldás széleskörű elterjedése biztosítja „szabványosságukat”, mivel nincsenek „kőbe vésve” el lehet térni tőlük kisebb-nagyobb mértékben



Az OSI modell

- ▶ A tervezésekor figyelembe vett célok:
 - ▶ Rétegekre bontott legyen
 - ▶ Minden réteg feladata jól definiált legyen, a feladatokat a már nemzetközileg elfogadott szabványok figyelembe vételével alakították ki
 - ▶ A rétegek közötti információcsere minimalizálásával kell a rétegek határait megállapítani
 - ▶ Elegendő rétegszámot definiáljon, hogy különböző feladatok feleslegesen ne kerüljenek egy rétegbe
 - ▶ Egyik gép n-edik rétege csak a másik gép azonos szintű rétegével tudjon kommunikálni a réteg protokollja szerint

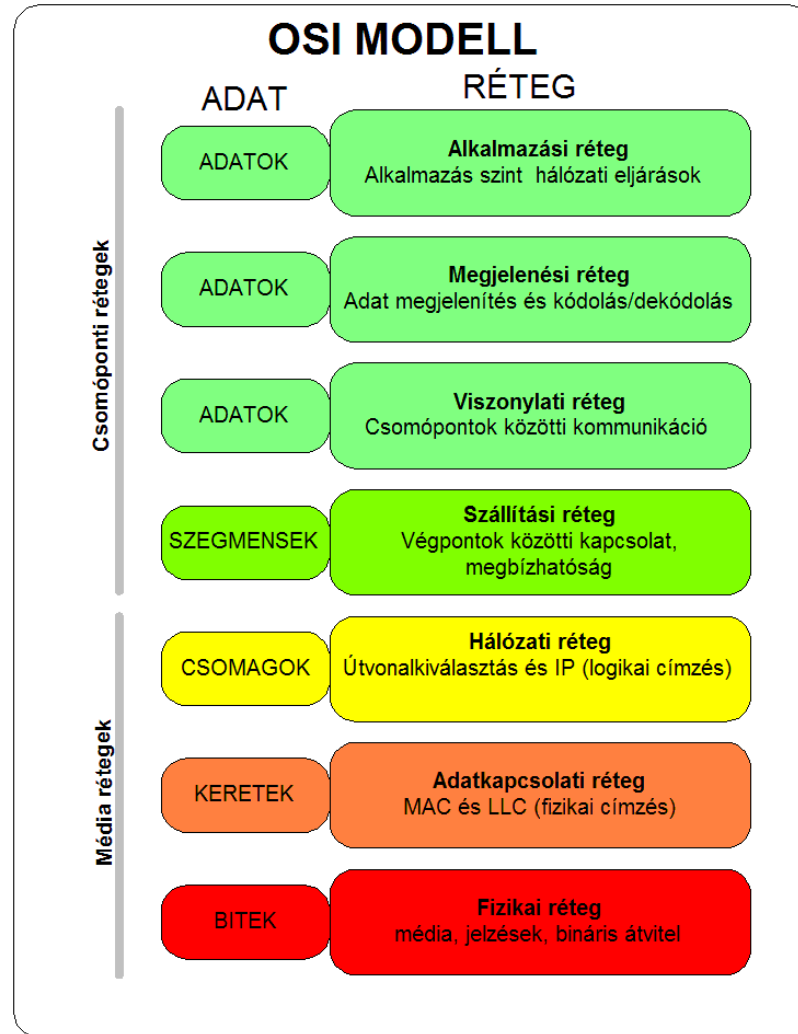


Az OSI modell

- ▶ A kapcsolat során használt szabályok és megállapodások összességét nevezzük protokollnak.
- ▶ A hálózati architektúrát a rétegek és a protokollok alkotják együttesen.
- ▶ Az OSI modell 7 réteget alkalmaz, míg a gyakorlati TCP/IP „csak” 5-öt.



Az OSI modell



Fizikai réteg

- ▶ Fő feladata a bitek kommunikációs csatornára való juttatása.
- ▶ Beleértve:
 - ▶ Az adatok olyan átalakítását, konverzióját, jelátalakítását, ami biztosítja, hogy a felhasználó adatait a kiválasztott csatorna továbbítani tudja
- ▶ Ez a réteg határoz meg minden, az eszközökkel kapcsolatos fizikai és elektromos specifikációt.
 - ▶ Pl: Érintkezők kiosztása, kábelek típusa, használatos jeltípusok, stb...



Fizikai réteg

- ▶ Információt hordozó közegek:
 - ▶ Fém kábelek (UTP, Koax)
 - ▶ Fény kábelek
 - ▶ Rádióhullám.
- ▶ Ebben a rétegben dolgozik a HUB és a Repeater.



Adatkapcsolati réteg

- ▶ Feladata az adatok megbízható továbbítása az adó és fogadó között.
- ▶ Ezt üzenetszórásos vagy pont-pont kapcsolat kialakításával teszi meg.
- ▶ A fentebbi rétegekből származó adatokat keretekké tördeli, majd a kereteket továbbítja.
- ▶ Minden kerethez nyugtakeret is tartozik, amit a címzett küld vissza, hogy megkapta a keretet.
- ▶ Problémaként a rétegben kell kezelni az alábbi eseményeket:
 - ▶ Keret elvesztése
 - ▶ Nyugtakeret elvesztése
 - ▶ Adó sebessége nagyobb, mint a fogadó sebessége probléma kezelése



Adatkapcsolati réteg keret felépítése

- ▶ Előtag: váltakozó 0-ák és 1-esek, régen aszinkron közegeknél (Koax kábel) szinkronizálásra szolgált
- ▶ Cél és forrás MAC cím alapján van azonosítva
- ▶ A hossz mező az adat hosszát adja meg, ami maximum 1536 byte lehet.

8BYTE	6BYTE	6BYTE	2BYTE	46-1500BYTE	4BYTE
Előtag / Preamble	CÉL MAC CÍME	FORRÁS MAC CÍME	Típus/ Hossz	Adatok	CRC

Adatkapcsolati réteg keret felépítése

- ▶ Amennyiben a típus értéke 1536-nál nagyobb, akkor az arra utal, hogy melyik felsőbb rétegbeli protokollnak kell átadni a keretet.
- ▶ CRC mező ellenőrzőértéket ad meg CRC-32 algoritmus alapján.

8BYTE	6BYTE	6BYTE	2BYTE	46-1500BYTE	4BYTE
Előtag / Preamble	CÉL MAC CÍME	FORRÁS MAC CÍME	Típus/ Hossz	Adatok	CRC

Ciklikus Redundancia számítás

- ▶ Egy fajta hash algoritmus.
- ▶ A hash algoritmus egy olyan algoritmus, amely végtelen hosszú adatmennyiséget képez le egy fix hosszúságú adatmennyiségre.
- ▶ A kimeneti adatmennyiség egyedien jellemző lesz a bemeneti adatra.
- ▶ A folyamat egyirányú, hash adatból a definícióból adódóan a tényleges adat nem nyerhető ki.
- ▶ Adatellenőrzési és titkosítási célokra egyaránt alkalmazhatóak.
- ▶ Gond lehet algoritmus esetén a hash ütközés



MAC-cím

- ▶ MAC = Media Access Control
- ▶ Fizikai végpont azonosításra szolgál
- ▶ 12db hexadecimális számjegy formájában határozzák meg (48 bit)
- ▶ Szabványügyi hivatal adja ki gyártóknak a címtartományokat
- ▶ Eszközönként egyedi
- ▶ Két részből áll:
 - ▶ 24 bit gyártó és típus meghatározása
 - ▶ 24 bit egyedi sorszám



MAC-cím

- ▶ Elméletileg nem módosítható a felhasználó által
- ▶ Gyakorlatilag azonban lehetséges vagy könnyebben, vagy nehezebben. (MAC spoofing)
- ▶ Ennek oka az, hogy előfordulhat egyes gyártók hibájából az, hogy azonos MAC-címmel látnak el két eszközt vagy két kártyát.
- ▶ Ezt a címezési sémát használja az Ethernet hálózaton kívül a Bluetooth is.



Adatkapcsolati réteg

- ▶ Ebben a rétegben dolgozik a Switch.
- ▶ A Switch a MAC-címek alapján továbbítja a csomagokat a cél felé.
- ▶ A hatás azonban nem azonnali, a Switch-nek először fel kell térképeznie a hálózatot, tanulási folyamattal rendelkezik.



Hálózati réteg

- ▶ A kommunikációs alhálózatok működését vezérli.
- ▶ Itt már csomagokról beszélünk.
- ▶ Egy nagyobb hálózat esetén elvileg a feladótól a célig az adatok eljuttatása több útvonalon is lehetséges.
- ▶ Ezért feladat az optimális útvonal kiválasztása.
- ▶ Ez kiterjedt hálózatok esetén alapvető jelentőségű.
- ▶ Ez a réteg már logikai címezési sémát alkalmaz, ami felhasználó barátabb kicsivel*



Hálózati réteg

- ▶ A kommunikáció kezdetén döntünk arról, hogy a teljes üzenet csomagjai milyen útvonalon jussanak el a célba.
- ▶ Figyelembe kell venni az útvonal választás során az egyes vonalak terhelését, igény szerint módosítani kell őket.
- ▶ Továbbá ebben a rétegben kell megoldani a túl sok csomag hálózatban maradása miatt kialakult torlódást
- ▶ Valamint itt kell megoldani a különböző hálózatok összekapcsolását.



Hálózati réteg

- ▶ Itt van megoldva az adatátvitel helyességének ellenőrzése a gyakorlatban manapság.
- ▶ Hálózati eszköz, amely ebben a rétegben dolgozik:
Router
- ▶ Protokollja az IP, két változata van jelenleg elterjedve:
 - ▶ V4 – 32 bites címzési séma ~4 milliárd egyenrangú csomópont megkülönböztetése
 - ▶ V6 – 128 bites címzési séma $\sim 3,4 \times 10^{34}$ egyenrangú csomópont megkülönböztetése.



Szállítási réteg

- ▶ Biztosítja, hogy a felhasználók közötti adatátvitel transzparens legyen.
- ▶ Biztosítja, és ellenőrzi egy adott kapcsolat megbízhatóságát.
- ▶ Két fő protokoll dolgozik a rétegben: TCP és UDP
- ▶ Protokoll függő a kapcsolat kezelése.
- ▶ TCP esetén kapcsolat orientált, UDP esetén üzenetszórásos



Viszony réteg

- ▶ A végfelhasználói alkalmazások közötti dialógus menedzselésére alkalmas mechanizmust valósít meg
- ▶ A megvalósított mechanizmus lehet duplex vagy félduplex
- ▶ Gyakorlatban nem létezik, mivel ezen feladatokat a szállítási réteg protokolljai látják el.



Megjelenítési réteg

- ▶ Az alkalmazási réteg igényeit teljesíti szolgáltatásaival
- ▶ Ez a réteg felelős az információ formázásáért és eljuttatásáért az alkalmazási rétegnek, ahol a további feldolgozás, illetve megjelenítés történik.
- ▶ Gondoskodik róla, hogy az alkalmazási rétegnek már ne kelljen foglalkoznia a végfelhasználói rendszerek esetleg különböző adatértelmezési módszereiből származó szintaktikai eltérésekkel.
- ▶ Pl: ASCII bájtok kódolása UTF adattá.
- ▶ Gyakorlatban nem létezik, mivel a feladatait a hetedik réteg látja el.



Alkalmazási réteg

- ▶ Szolgáltatásai támogatják a szoftver alkalmazások közötti kommunikációt, és az alsóbb szintű hálózati szolgáltatások képesek értelmezni alkalmazásoktól jövő igényeket, illetve, az alkalmazások képesek a hálózaton küldött adatok igényenkénti értelmezésére.
- ▶ Magas szintű protokollok használata a jellemző



OSI modell a gyakorlatban

- ▶ A gyakorlatban nem terjedt el, mivel a specifikáció alapján megvalósított struktúra a célhoz feleslegesen bonyolult.
- ▶ Helyette a TCP/IP avagy Internet modell van alkalmazva.
- ▶ Ez a modell szakirodalomtól függően 3-5 rétegből áll.
- ▶ Általánosan azonban az 5 réteges bontás terjedt el.



OSI modell és a TCP/IP kapcsolata

OSI	TCP/IP
Alkalmazási	Alkalmazási
Megjelenítési	
Viszony	
Szállítási	Szállítási
Hálózati	Internet
Adat kapcsolati	Adatkapcsolati
Fizikai	Fizikai



TCP/IP beágyazódás

Szoftver

Data

Application

UDP
header

UDP
data

Transport

IP
header

IP data

Internet

Frame
header

Frame data

Frame
footer

Link

Hardver



Fizikai réteg jellemzői

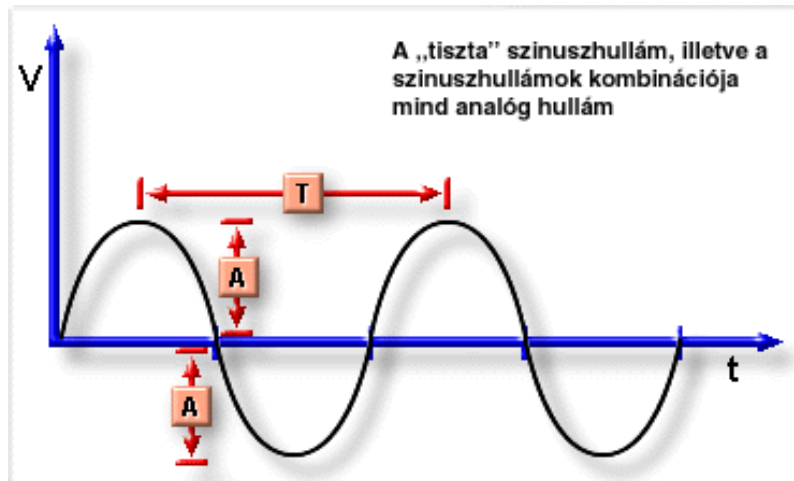
Szükséges fogalmak



Analóg és Digitális jelek

▶ Analóg jel

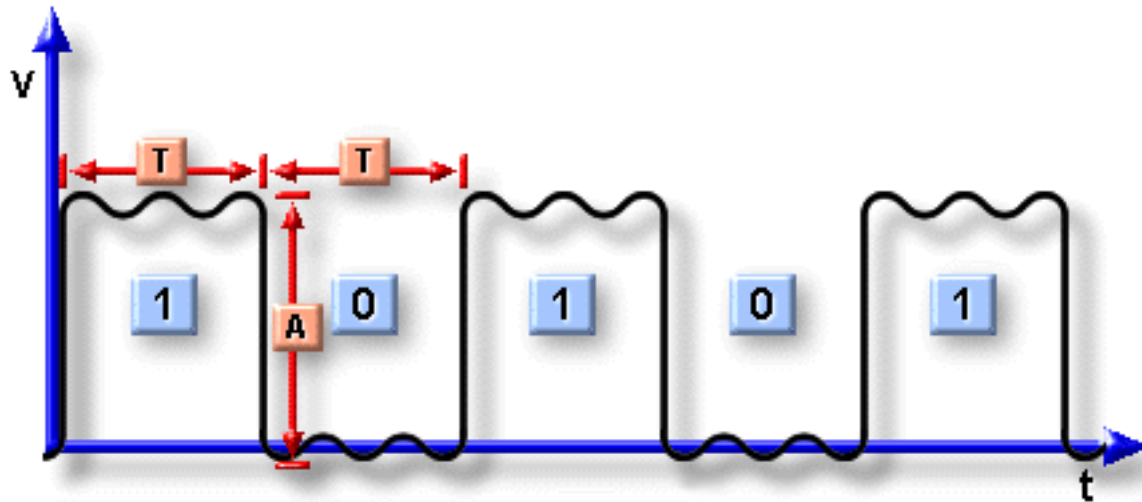
- ▶ Hullámzó, a jel feszültsége, folyamatosan változik az időben.
- ▶ Jó példa analóg jelre a szinusz hullám



Analóg és Digitális jelek

► Digitális jel:

- A feszültség ugrásszerűen változik az idő függvényében
- Pl: Négyszögjel



Jelterjedés

- ▶ A bitet jelképező energiacsomag végighalad az átviteli közegen
- ▶ A *terjedés* sebessége az átviteli közeg anyagától, geometriájától és szerkezetétől, valamint az impulzusok frekvenciájától függ
- ▶ Ha a terjedési idő túl rövid, lehetséges, hogy a biteket le kell lassítanunk, illetve azokat ideiglenesen tárolnunk kell (ezt *pufferelésnek* nevezzük), hogy a hálózati eszközök lépést tudjanak tartani a bitek érkezésével.



Bitek terjedésének problémái

- ▶ csillapítás
- ▶ visszaverődés
- ▶ zaj
- ▶ ütközés



Csillapítás

- ▶ a jel energiát ad le a környezetnek, így energiát veszít
- ▶ az üzenetet szállító jel energiáját a kábel elnyeli
- ▶ optikai jelek esetében is fennáll - az optikai szál elnyeli és szétszórja a fényenergia egy részét, miközben a fényimpulzusok (a bitek) az üvegszálon áthaladnak
- ▶ a rádió- és mikrohullámok esetén is fellép, mivel azt a légkör egyes molekulái elnyelhetik és szétszórhatják



Csillapítás

- ▶ Az átviteli közeg hosszát úgy kell megállapítani, hogy még biztonsággal értelmezhető legyen a csatorna végén.
- ▶ Csillapítás= $10 \log_{10} P_1/P_2$ (dB)



Visszaverődés, reflexió

- ▶ A feszültségimpulzusok, illetve a bitek egy határfelülethez érnek, a hullámenergia egy része visszaverődik.
- ▶ Az ellenkező fázisú hullámok kioltják, míg az azonosak erősítik egymást.
- ▶ Fontos, hogy a hálózati átviteli közeg hullámimpedanciája illeszkedjen a hálózati kártya elektromos komponenseihez
- ▶ Hasonlít a visszhang jelenséghez.



Zaj

- ▶ Egy nemkívánatos jel, mely hozzáadódik a feszültségimpulzusokhoz
- ▶ Zajmentes elektromos jel nem létezik, viszont fontos, hogy a jel/zaj viszonyt a lehető legmagasabb értéken tartsuk
- ▶ Módszerek:
 - ▶ *árnyékolás: koaxiális kábel*
 - ▶ *kioltás: sodort érpár*



Ütközés

- ▶ Ugyanabban az időben két, kommunikáló számítógép egy megosztott átviteli közeget használ
- ▶ A két bináris számjegyhez tartozó feszültségérték összeadódik, ami egy harmadik feszültség szintet eredményez
- ▶ A bináris rendszerben nem engedélyezett, mivel az csak két feszültség szintet ismer. Ebben az esetben a bitek "megsemmisülnek".



Maximális sávszélesség

- ▶ Maximális adatátviteli sebesség zajtalan környezetben, Nyquist – frekvenciatétele
- ▶ Max. adatátviteli sebesség= $2 B \log_2 V$ (bit/sec)
- ▶ Ahol:
 - ▶ B – sávszélesség (jelzés sebesség, átviteli technológia korlátozza.)
 - ▶ V – a továbbítandó jel különböző diszkrét szintje (digitális esetben 2)



Max adatátviteli sebesség

- ▶ Shannon (1948) meghatározta a maximális adatsebességet zajos csatornára.
- ▶ Maximális adatátviteli sebesség = $B \log_2 [1+S/N]$ (bit/sec)
- ▶ Ahol:
 - ▶ B – sávszélesség,
 - ▶ S – átlagos jelteljesítmény,
 - ▶ N – átlagos zajteljesítmény
 - ▶ S/N – az átvitelre jellemző jel-zaj viszony



Kódolás

- ▶ A kódolás az 1-es és 0-s bitek fizikailag megfogható dologgá való átalakítását jelenti:
 - ▶ vezetékekben haladó elektromos impulzusok
 - ▶ optikai szálban haladó fényimpulzus
 - ▶ elektromágneses hullámimpulzus a térben



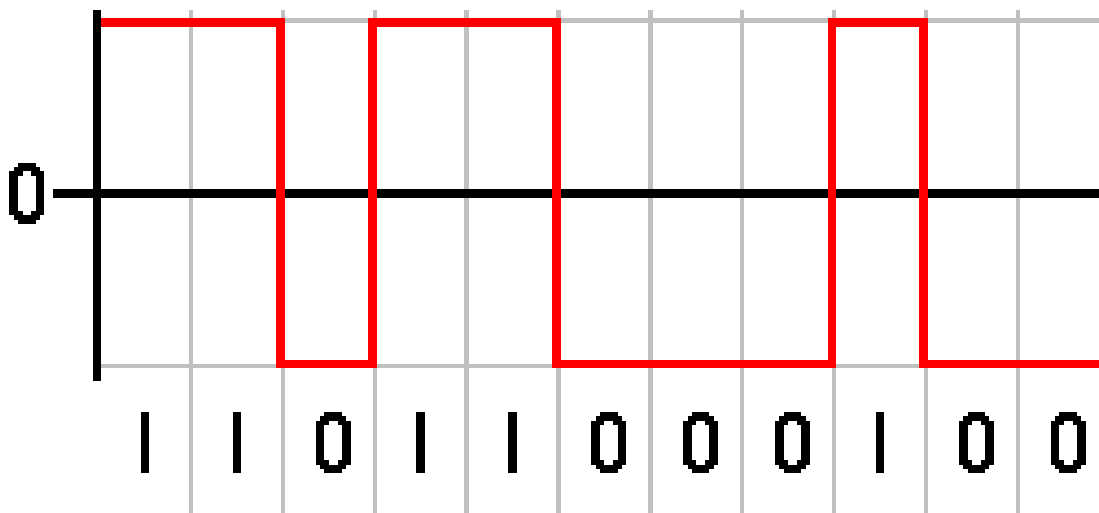
Feszültség alapú átvitel

- ▶ 1 értékű bit átviteléhez vagy 3.3 V vagy 5 V impulzus tartozik
- ▶ 0 értékű bit átviteléhez 0 V tartozik
- ▶ A kódolás problémája, hogy nincs felkészülve a vezeték szakadás esetére.
- ▶ Ezért nagy hálózat építése esetén nem alkalmazott.
- ▶ Leggyakoribb alkalmazási helye: számítógépen belül.
- ▶ Az egyes bitek idejét egy órajel határozza meg.



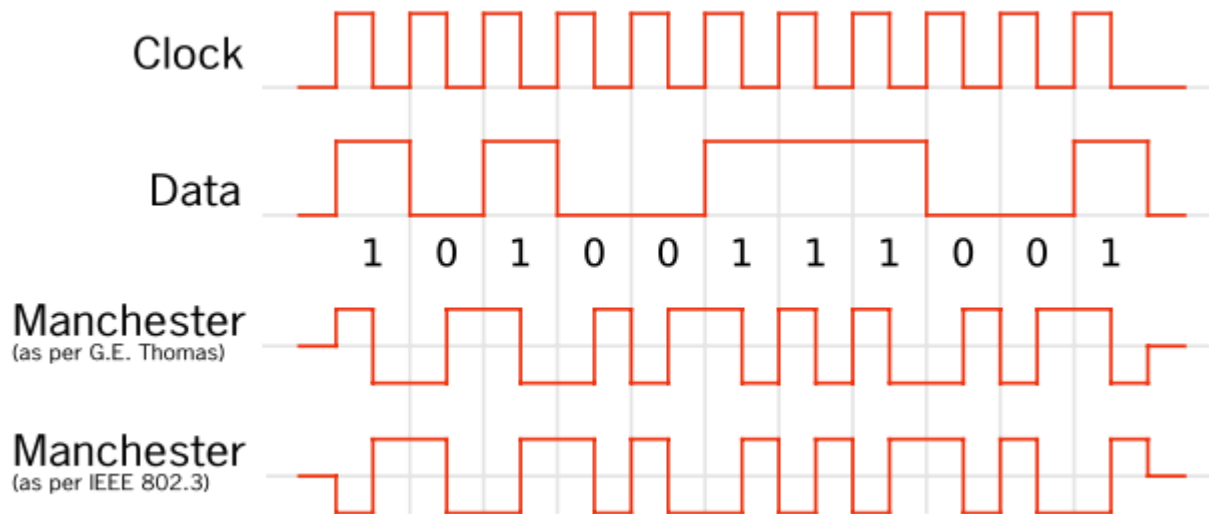
Nullára vissza nem térő kódolás (NRZ)

- ▶ A 0 értékű bit kódolása nem 0 V feszültség szinttel történik, hanem -5V feszültséggel.
- ▶ Előny, hogy a 0V állapot vezeték szakadást jelenthet.
- ▶ Szintén kell órajel



Manchester kódolás

- ▶ Nem kell hozzá órajel.
- ▶ A biteket az impulzusok átmenete jelzi
- ▶ Magas -> alacsony átmenet jelenti az 1-es állapotot
- ▶ Alacsony -> magas átmenet jelenti a 0 állapotot.
- ▶ Adat XOR órajel -> Manchester kód



Multiplexelés

- ▶ Egy vagy több csatornát összefognak egy csatornába úgy, hogy az inverz multiplexelés művelettel, vagy demultiplexeléssel, vagy demuxálással elő tudják állítani az eredeti csatornákat.
- ▶ Fő fajtái:
 - ▶ Frekvencia osztásos
 - ▶ Időosztásos

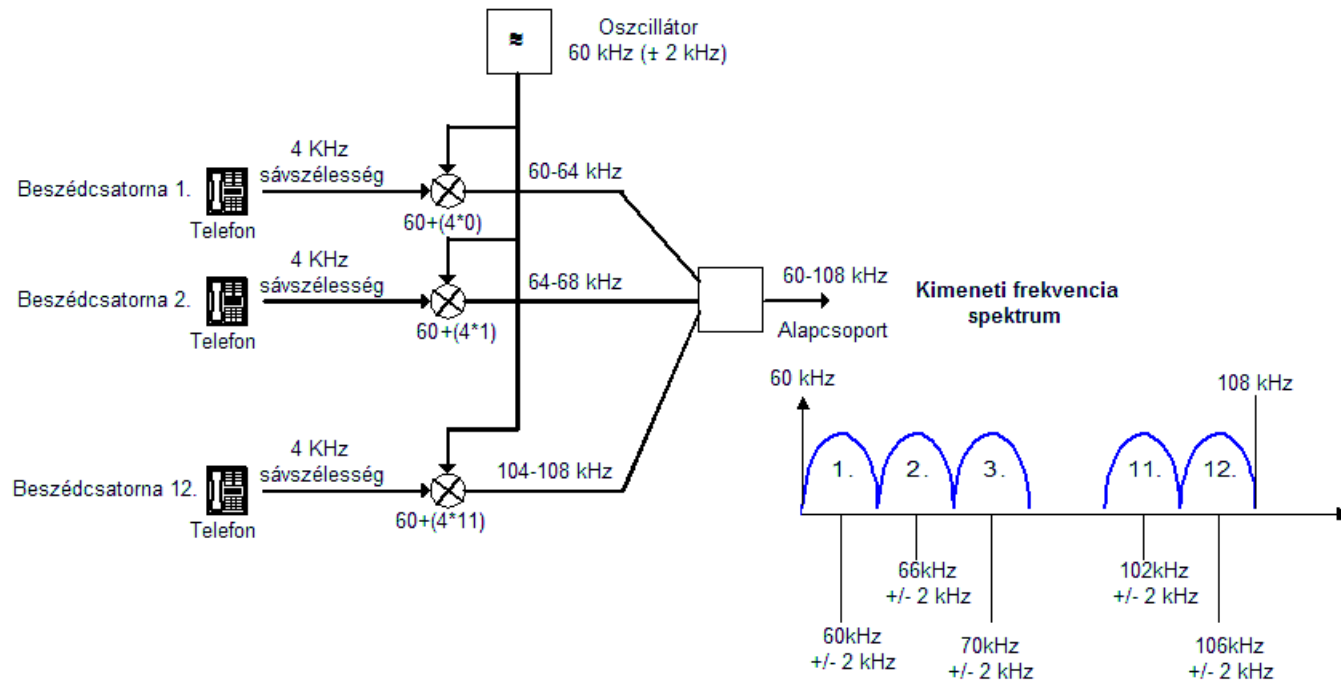


FDM – Frequency Division Multiplexing

- ▶ Frekvenciaosztásos multiplexelés
- ▶ Frekvencia tartomány: 500-1500 kHz
- ▶ Frekv. tartom. felosztása 4000 Hz sávokra
- ▶ Hangátviteli csatornák 3100 Hz-re korlátozva
- ▶ Hangsávok modulálása a vivő frekvenciákkal
- ▶ Majd ezek összegzése, továbbítása

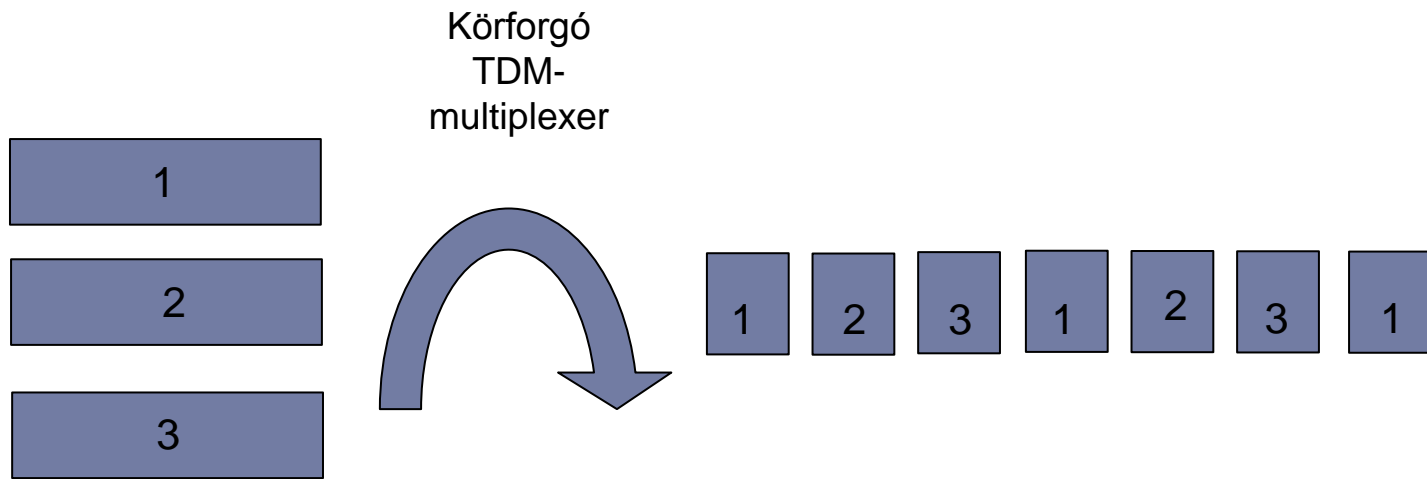


FDM – Frequency Division Multiplexing



TDM – Time Division Multiplexing

- ▶ Az egyes felhasználók időosztással férnek hozzá a teljes csatornához, így ki tudják használni a csatorna teljes sáv szélességét.



További multiplexelések

▶ STDM – Statistical Time Division Multiplexing

- ▶ A küldendő jelek statisztikai elemzésen mennek keresztül, ez alapján kerül meghatározásra az idő és/vagy frekvencia igényük. Így az átvitel optimalizáltabb, de bonyolultabb is, mivel elemezni kell őket.

▶ CDMA - Code Division Multiple Acces

- ▶ Kódosztásos többszörös hozzáférés, mobiltelefonok használják. Egyszerre többen használják ugyanazt a frekvencia sávot, azonban minden egyes felhasználó egyedi kóddal modulálja az üzenetét, amiből később kihámozható az eredeti üzenet.





Fizikai réteg



Átviteli közegek

- ▶ Koaxiális kábelek
- ▶ UTP
- ▶ STP
- ▶ Optikai kábelek
- ▶ Vezeték nélküli hálózatok

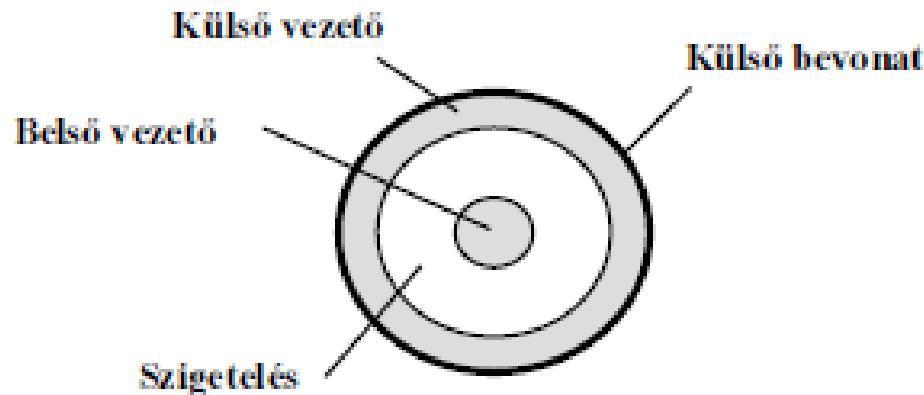


Koaxiális kábel

- ▶ Az egyik vezető egy rézszál, amely a kábel geometriai középvonalában helyezkedik el
- ▶ Ezt egy rugalmas szigetelőréteg veszi körül
- ▶ A szigetelőanyagot egy rézfonat vagy fémfólia borítja, ami egyrészt a második jelvezetéként funkcionál az áramkörben, másrészt árnyékolja a belső vezetőt
- ▶ Az árnyékoló réteget védőköpeny borítja.



Koaxiális kábel



Koaxiális kábel keresztmetszete

- A kábel átmérője: 5 - 25 mm.
- A koncentrikus felépítés miatt kevésbé érzékeny a zavarokra és az áthallásra, mint a csavart érpár.
- Nagyobb távolságra használható és többpontos alkalmazásban több állomást támogat a csavart érpárnál.

Koaxiális kábel

▶ Két fő változata:

- ▶ Alapsávú – 50 ohm ellenállás méterenként, számítógépes hálózatokban használt, szegmenshossz maximálisan 500 méter
- ▶ Szélessávú – 75 ohm ellenállás méterenként, analóg és digitális hálózatban egyaránt használt, szegmenshossz maximálisan 1 km



UTP kábel

- ▶ Árnyékolatlan csavart érpáras kábel
- ▶ A vezetékek páronkénti összesodrásával csökkentik az elektromágneses (EMI) és rádiófrekvenciás (RFI) interferencia jeltorzító hatását
- ▶ Az árnyékolatlan érpárok közötti áthallást úgy csökkentik, hogy az egyes érpárokat eltérő mértékben sodorják
- ▶ Szegmenshossz maximálisan 100 méter
- ▶ 4 érpár, a sáv szélességet a kötés módja határozza meg



STP kábel

- ▶ Árnyékolt csavart érpáras kábel
- ▶ Mint az UTP, azonban a vezetékek érpáranként árnyékoltak
- ▶ Nagyobb védelmet nyújt a külső interferenciaforrásokkal szemben, viszont drágább, mint az árnyékolatlan csavart érpáras kábel.
- ▶ Szintén 100 méteres szegmenshossz



UTP kábelek fajtái

▶ Egyenes kötés

- ▶ A vevő és adó oldalon a kábelek sorrendje megegyezik. Aktív hálózati eszközök esetén használt, mint: Router, Switch, aktív hub.

▶ Kereszt kötés

- ▶ A vevő és az adó oldalon a kábelek sorrendje eltér, hogy ne legyen adatütközés. Olyan helyeken használt, ahol nincs aktív eszköz, csak 2 számítógép pl.

▶ Rollover

- ▶ Speciális kábel, router konfiguráció során alkalmazott, leginkább egy gyártóhoz kötődik: Cisco



UTP kábelek kategóriái és sávszélességek

- ▶ 4 érpár van az UTP kábelben
 - ▶ 4 adó/vevő pár. Attól függően, hogy mennyit használunk ki és milyen a kábel határozhatjuk meg az adatátvitel sebességét.
- ▶ CAT4
 - ▶ Csavart érpár árnyékolás nélkül. 10Mbit/s érhető el ezzel a kábel fajtával. 1db érpár használt csak az átvitel során.
- ▶ CAT5
 - ▶ Csavart érpár egy külső árnyékolással. 100Mbit/s, 2db érpár van használva.



UTP kábelek kategóriái és sávszélességek

▶ CAT6

- ▶ Csavart érpár külső árnyékolással és érpárankénti árnyékolással. 4db érpár van használva 1Gbit/s.

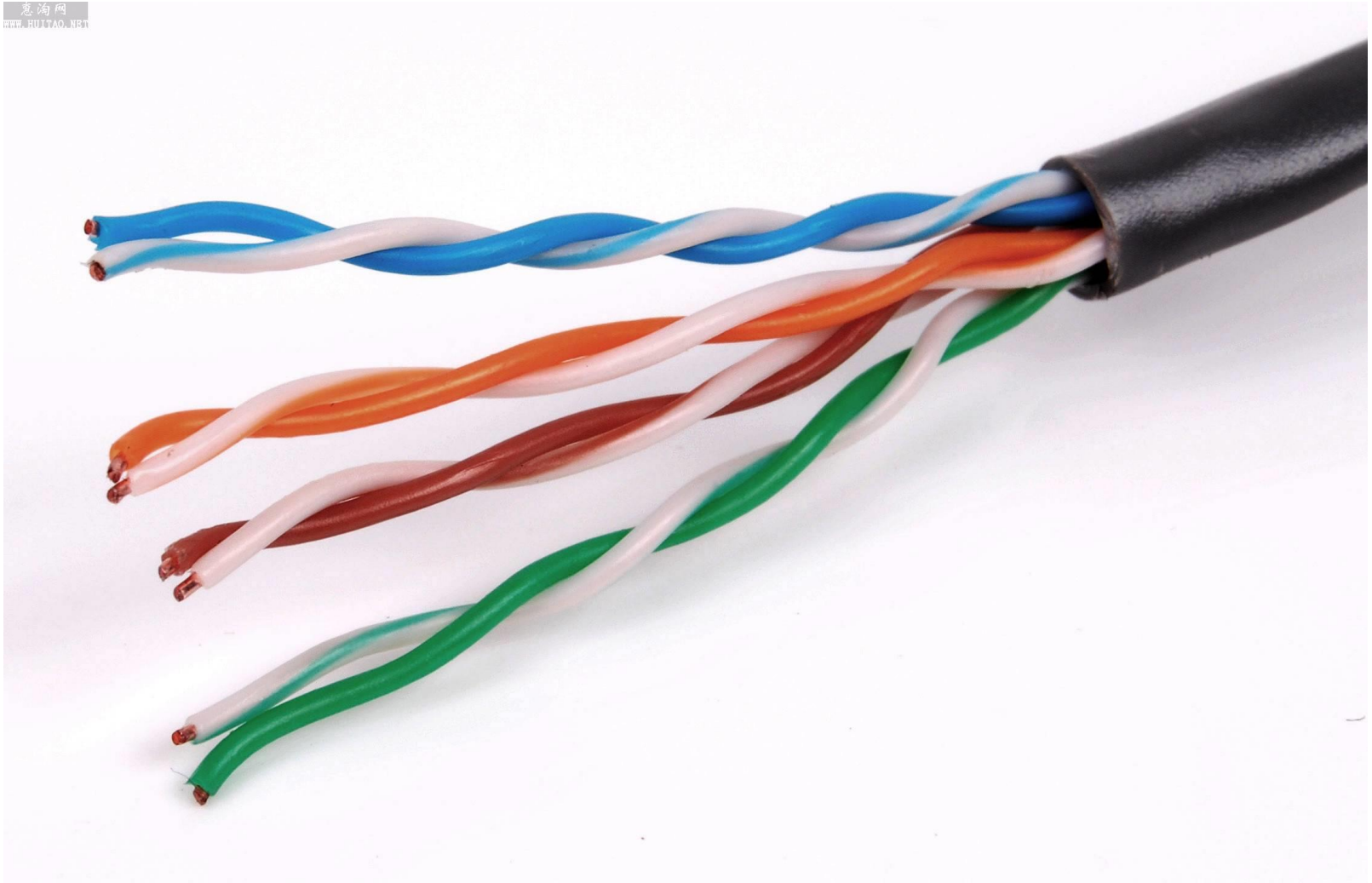
▶ CAT7

- ▶ Mint a CAT6, azonban 10Gbit/s illetve 50 méteres szegmenshosszal 40Gbit/s sebesség.



UTP Kábel

意淘网
WWW.HUITAO.NET

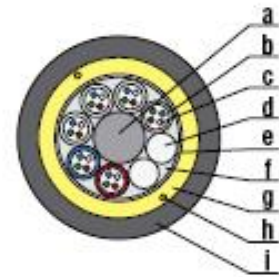


Optikai kábel

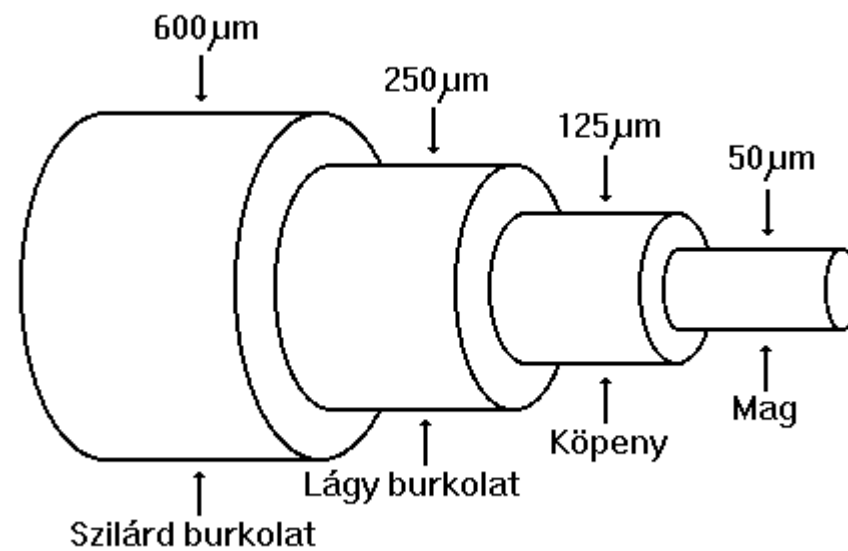
- ▶ A jel fényként továbbított az üvegszáliban.
- ▶ Galvanikusan izolált, kültéren remekül alkalmazható, mivel a kábelre nem jelent veszélyt a villám.
- ▶ Két részből áll a szál:
 - ▶ Mag:
 - ▶ Nagy tisztaságú nagy törésmutatójú üvegből készül.
 - ▶ Köpeny:
 - ▶ Kisebb törésmutatójú műanyagból készült védő héj, ami megakadályozza a fény kijutását a magból.



Optikai kábel



Optikai kábel



Optikai kábelek fajtái

▶ Monomódusú

- ▶ A mag átmérője közelít a használt fény hullámhosszához, így a kábelben a fény visszaverődések, pattanások nélkül szinte egyenesen halad a kábelben.
- ▶ Egy szálon így egyszerre egy jel továbbítható.

▶ Multimódusú

- ▶ A mag átmérője nagyobb a fény hullámhosszánál, így a fény a kábel falán pattogva halad végig.
- ▶ A beesési szög módosításával elérhető, hogy egy kábelben több jel is haladjon.
- ▶ „Nagy” a jelvesztesége, így manapság nem igen alkalmazott.



Vezeték nélküli átvitel

- ▶ Átviteli közegre nincs hozzá szükség
- ▶ A jelek elektromágneses hullámok
- ▶ Rengeteg helyen alkalmazott
- ▶ Hálózat esetén számunkra érdekes technológia:
 - ▶ WLAN, 802.11



WLAN

- ▶ 1997 óta
- ▶ A fizikai réteget és az adatkapcsolati réteget definiálja a szabvány.
- ▶ Az adatkapcsolati réteg definiálására azért van szükség, mivel titkosítási feladatokat is el kell látnia a hálózatnak.
- ▶ Több szabvány van manapság használatban



WLAN szabványok

Szabvány	Megjelenés ideje	Működési frekvencia (Ghz)	Jellemző sebesség (Mbit/s)	Maximális sebesség (Mbit/s)	Hatótávolság beltéren (méter)	Hatótávolság kültéren (méter)
802.11	1997	2,4	0,9	2	~20	~100
802.11 a	1999	5	23	54	~35	~120
802.11 b	1999	2,4	4,3	11	~38	~140
802.11 g	2003	2,4	19	54	~38	~140
802.11 n	2008	2,4 / 5	74	150/300	~70	~250



WLAN fizikai réteg

- ▶ IR – infravörös, nincs szükség közvetlen rálátásra, csak beltéren használható, max. 2Mb/s
- ▶ FHSS - Frekvenciaugrásos szórt spektrum, 2,4GHz
- ▶ DSSS - Direct-sequence spread spectrum 5GHz

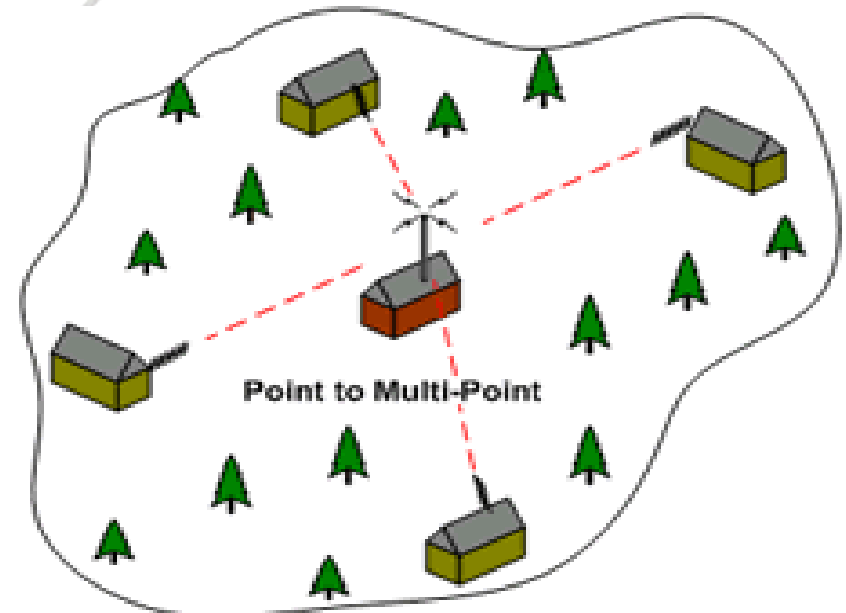


Antenna típusok

- ▶ Irány antenna

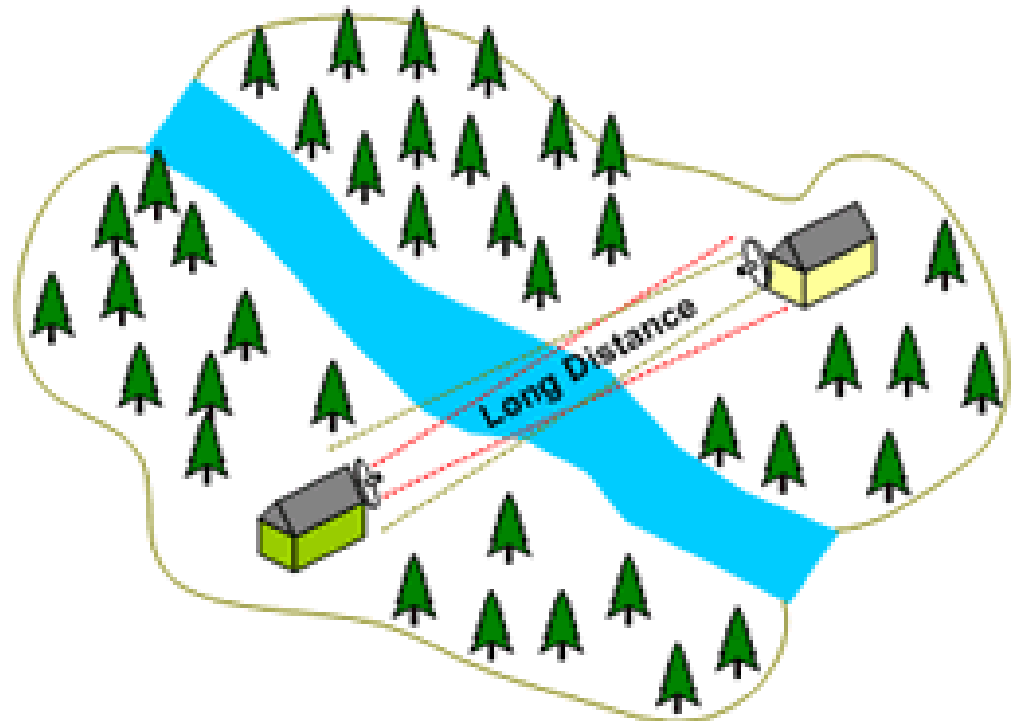


- Pont-Multipont



Antenna típusok

- ▶ Sáv antenna / Grid



www.Radiolabs.com

Sebességet befolyásoló tényezők

- ▶ Árnyékolás (Pl. beton, fák)
- ▶ Vezeték nélküli telefonok
- ▶ Mikrohullámú sütő
- ▶ Bluetooth eszközök
- ▶ Időjárás
- ▶ Használt kábel típusa



Wi-Fi minősítés

- ▶ Vezeték nélküli hálózat != Wi-Fi
- ▶ Wi-Fi Alliance teszt alapján kaphatja meg a termék
- ▶ Teszt feltételek, aminek a terméknek meg kell felelnie (2008-as):
 - ▶ Kimeneti teljesítmény (max. 56mW)
 - ▶ WPA2 titkosítás támogatása
 - ▶ WMM / WME támogatás



Vezeték nélküli biztonság

- ▶ Mac Filtering
- ▶ WEP
 - ▶ Elavult
- ▶ WPA
- ▶ WPA2



A WEP problémái

- ▶ 24 bites titkosító kulcs (16 777 216 lehetséges kulcs)
- ▶ Minden csomaghoz 1 titkosító kulcs
- ▶ Kellő mennyiségű adat passzív lehallgatása (Kb 1GB) után a kezdeti kulcs könnyen visszafejthető (Kb 1-3 perc alatt a kulcs bonyolultságától függően)
- ▶ 2003 óta hivatalosan is elavultnak számít, ennek ellenére még ma is széles körben használt



WPA

- ▶ 1999-ben jelent meg először, azonban 2003-ig nem nagyon terjedt el.
- ▶ TKIP („tee-kip”) titkosítást használ
- ▶ Újdonságai:
 - ▶ Kulcskeverés (Kiinduló kulcs módosítása titkosítás előtt)
 - ▶ Csomag sorrend figyelés
 - ▶ 64 bites csomag hashelés
 - ▶ Minden csomaghoz egyedi kulcs



Mitől biztonságos ?

- ▶ Csomag sorrend figyelés: Ha egy csomag hamarabb érkezik meg, mint ami előtte van, az AP dobja a csomagot
- ▶ A csomag hash alapján eldönthető, hogy az módosult, vagy nem
- ▶ Ha 60 mp-en belül 2db rossz hash értékű csomag érkezik, akkor az AP új kulcsot vezet be
- ▶ Minimum 8, maximum 63 karakteres kiinduló titkosító kulcs kell



WPA2

- ▶ 2004-ben vezették be, a WPA-t váltotta
- ▶ AES alapú titkosítás
- ▶ Belátható időn belül lehetetlen visszafejteni a kulcsot
- ▶ Bevezetésének oka az volt, hogy a WPA titkosítást használó hálózatokból óránként 12 bit információ nyerhető ki
- ▶ WPA esetén egy egyszerűbb kulcs visszafejthető 3-4 nap alatt.



WMM / WME

- ▶ Wireless Multi Media, Wireless Multi Media Extensions
- ▶ QoS csomag ütemezési támogatás alkalmazása:
 - ▶ WiFi telefonok (Skype funkcionalitás)
 - ▶ Otthoni multimédia megosztók. Pl. Linksys DMA2100, DMA2200

