

Számítógép Hálózatok BSC képzés

**(nem hivatalos)
Összefoglaló Jegyzet
2007/08 tavasz**

*2006/07 Zsoldos Viktor - zv602@hszk.bme.hu
2007/08 Juhász Péter – holzerbane@gmail.com*

Forrás: EA slide-ok, Tanenbaum könyv (régi kiadás), wiki, egyéb net(pl. berkeley.edu ☺)

Tartalomjegyzék

Bevezetés.....	3
1. Fizikai Szintű Kommunikáció.....	4
2. Többszörös Hozzáférés.....	13
3. Kapcsolás.....	19
4. Hívásvezérlés, Címzés.....	26
5. Routing.....	30
6. Feladatütemezés, csomagkezelés.....	34
7. Forgalom Szabályozás (Flow Control).....	39
8. Hibakezelés (Error Control).....	41
9. Forgalommenedzselés (Traffic control).....	45
10. Aszinkron Átviteli Mód (Asynchronous Transfer Mode, ATM).....	46
11. Protokoll Architektúrák.....	52
12. Adatkapcsolati rétegbeli kommunikáció.....	55
13. Lokális Hálózatok (Local Area Network - LAN).....	59
14. BWA – Broadband Wireless Access -szélessávú vezeték nélküli hozzáférés.....	67
15. Internet Protocol – IP.....	73
16. Mobil IP.....	81
17. Szállítási protokollok: UDP és TCP.....	82
18. Multimédia továbbítása IP felett (RTP, RTCP, RTSP).....	85
19. Hívásvezérlő Protokollok.....	88
20. QoS: a Best Effort-on túl - IntServ, DiffServ.....	89
21. MPLS – Multi-Protocol Label Switching.....	93
22. Hálózati alkalmazások.....	96

Bevezetés

Példák számítógép-hálózatokra

- Az ARPANET
- Az Internet
- Az európai kutatói gerinchálózat (GEANT)
- A magyarországi kutatói gerinchálózat (H-Bone)
- A PlanetLab
- Helyi hálózat
- Vezetéknélküli hot-spot

Internet „nagybetűvel”:

A fizikai hálózat, amely az ARPANET -ből nőtt ki.

Kezdetben egyszintű, elosztott, ma alapvetően hierarchikus

A középpontban: “tier-1”ISP-k (pl. az USA-ban: MCI, Sprint, AT&T, Cable and Wireless), nemzeti/nemzetközi lefedés, egyenrangúak.

Tier-1 szolgáltatók a nyilvános hálózatokhoz is kapcsolódnak (NAP –network access point)

Tier-2 ISP-k: kisebb (gyakran regionális) ISP-k. Egy, vagy több Tier-1 ISP-hez csatlakoznak, és esetleg más tier-2 ISP-khez.

Tier-3 ISP-k és helyi ISPs-k. Az utolsó szakasz (“hozzáférési” hálózat), legközelebb a végponti rendszerekhez

(Magyarország a legizmosabb kapcsolattal rendelkezők közé tartozik a GEANT-nál: 10Gbit/sec)

A számítógép hálózat

Számítógépek és felhasználói végkészülékek összekapcsolása különböző célokkal:

- WAN –wide area network–nagy területű hálózat
távolsági megkötés nélküli, tetszőleges kiterjedésű hálózat, akár globális méretű is lehet
- MAN –metropolitan area network – városi hálózat
eredetileg: egy tipikus USA-beli metropolitan area, de nem feltétlenül város, néhány tíz km
- LAN –local area network–helyi v. lokális hálózat
tipikusan vállalaton, intézményen belüli hálózat, néhány km-es távolságok
- HAN vagy PAN –home/personal area network–otthoni hálózat/személyi hálózat
otthoni, kis irodai hálózat (SOHO –small office/home office), esetleg többszintes épület, ~100m-es kiterjedés
- BAN –body area network
az emberi testen kiépített hálózat

Fő szabványosítási szervezetek

- IEEE –Institute of Electrical and Electronic Engineers
- IETF –Internet Engineering Task Force
- ISO –International Standardization Organization
- ANSI –American National Standards Institute
- ITU –International Telecommunication Union
- ITU –T (Telecommunications) –távközlés
- ITU –R (Radio Communications) –rádióhírközlés
- ETSI –European Telecommunication Standard Institute

1. Fizikai Szintű Kommunikáció

A hálózati rendszernek az a része, amely két végpont között bitek továbbításával foglalkozik. A bitekből az adó szimbólumokat csinál, továbbítja az átviteli közegen keresztül, ahol a jelek torzulhatnak (zaj, zavarok). A vevőben a feladat az, hogy a szimbólumsorozatot kiértékelve, a kapott bitsorozat a lehető legjobban feleljen meg a leadottnak.

Bitfolyamok továbbítása hírközlő csatornákon

Alapfogalmak:

- bit, bitsebesség (információátviteli sebesség) - **bit/s**
- szimbólum, szimbólum-sebesség, jelzési sebesség: másodpercenkénti jelváltások (pl. feszültség szint változások) száma - **baud, Bd**

Bináris jelátvitel esetén a két sebesség megegyezik, többszintű jelátvitel esetén a bitsebesség többszöröse lehet a jelzési sebességnek (azaz 1 jellel több bitnyi információt is továbbítani lehet).

Átvitel sávhatárolt csatornán:

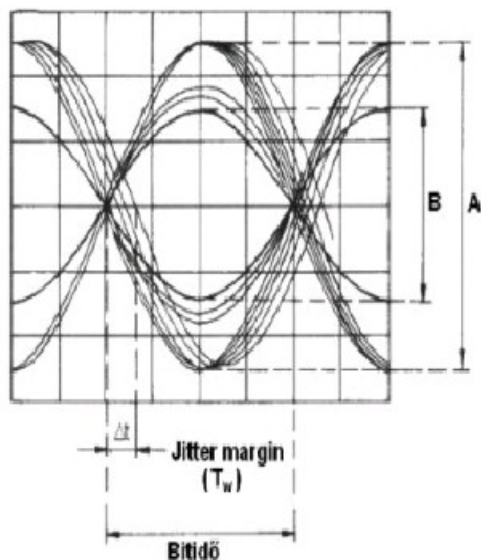
A jelszintek számát elvileg tetszőlegesen növelhetjük, de gyakorlatban a csatornák sávkorlátozottak, és zajosak. Minél több szintre van felosztva, annál nagyobb a tévesztés kockázata két szint között (Szimbólumközi Áthallás - **Inter-Symbol Interference (ISI)**)

Nyquist-tétel a zajmentes csatornára a következőt mondja ki:

maximális adatsebesség = $2H \log_2 V$ [b/s]

A szükséges legkisebb sávszélesség tehát a szimbólum-frekvencia felének felel meg, ha a jelszintek száma 2 (bináris).

Ahol H az adott csatorna sávszélessége, V pedig az elküldött jel jelszintjeinek száma.



Szemábra: Oszilloszkópos megfigyelés, amelynél az egymás utáni jelalakok egymásra rajzolódnak. A szem nyitottsága jelzi, hogy mennyi esélyünk van a helyes döntésre. Az additív zaj miatt természetesen előfordulnak tévesztések, minél nagyobb a zaj, annál többször

Átvitel zajos csatornán:

A csatorna zajának mértékét a jel és a zaj teljesítményének arányával, vagy más szóval a jel-zaj viszonytal (**signal-to-noise ratio**) jellemezhetjük. Ha a jel teljesítményét S -sel, a zaj teljesítményét pedig N -el jelöljük, akkor a jel-zaj viszony S/N .

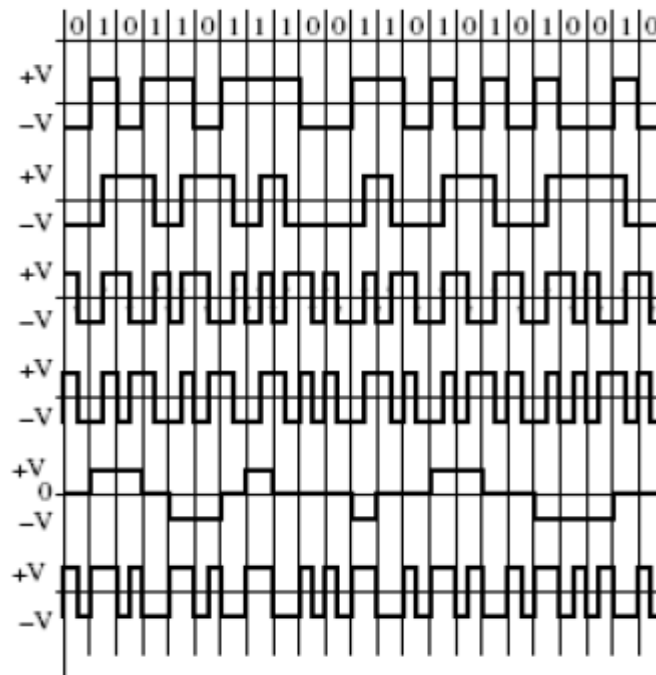
Maximális adatátviteli sebességet egy olyan zajos csatornán, amelynek sávszélessége H , jel-zaj viszonya pedig S/N : maximális adatsebesség =

$H \log_2 (1 - S/N)$ [b/s]

Vonali kódolások:

A nullafrekvenciás komponens és a bitszinkron biztosításához, az órajel kinyeréséhez a hosszú egyforma bitsorozatok kerülendők. A probléma egyik megoldása a vonali kódolás.

Néhány vonali kódolás:



Eredeti bitsorozat

NRZ: Hosszú 1-es, v. 0-ás sorozat esetén egyenkomponens, és a váltások hiánya miatt szinkronvesztés

NRZI: Az 1-eseknél mindig van váltás a bitidő közepén, hosszú 0-ás sorozat itt is problémát okoz

Manchester: 1-esnél felfelé, 0-ásnál lefelé váltás a bitidő közepén, egymás utáni azonos biteknél a bithatáron mindig váltás. Jól szinkronizálható, de kétszeresre növeli a bitsebességet

Differenciális Manchester: 0-nál a bitidő elején is és közepén is van váltás

MLT-3: -1,0,+1 feszültségszintek. Ha 1-es jön, egyet változik a szint(körbe megy: 0..1..0..-1..0..stb). Ha 0-s jön, nem változik.

FM-0

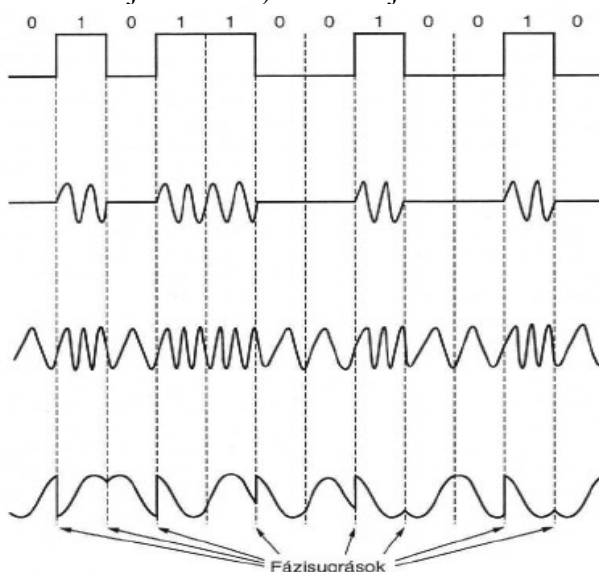
4B/5B kódolás:

A bemeneti bitfolyam minden bit-négyesét 5 bites kóddal helyettesítjük

A $2^4 = 16$ helyett $2^5 = 32$ kombinációnk van, ezért megtehetjük, hogy csak azokat használjuk, amelyek jó tulajdonságú sorozatot eredményeznek (elől legf. 1, végén legf. 2 „0” értékű bit, így legfeljebb 3 db „0” lehet egymás után). A többiből 8-at használunk speciális jelzésekre (pl keretezés hibavédelmi és szinkronizálási célokra), a fennmaradó 8-at nem használjuk fel.

Digitális modulációs eljárások

Moduláció: A szimbólumsorozat továbbítására egy - a jelzési sebességnél általában nagyobb frekvenciájú - szinuszos vivőt használunk. A vivő valamely jellemzőjét(amplitúdóját/frekvenciáját/ fázisát) változtatjuk a szimbólumoknak megfelelően.



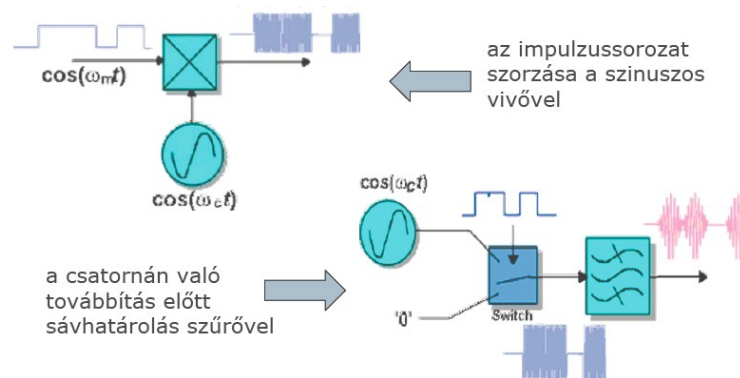
Digitális jel

ASK(Amplitude Shift Keying): „0”: nincs vivő, „1”: van (on-off-keying, ki-bekapcsolásos moduláció)

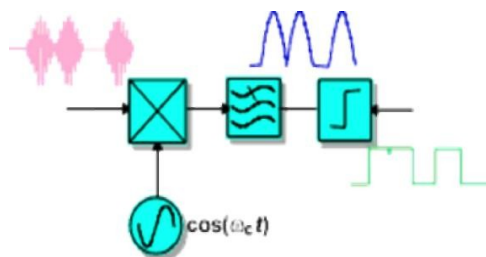
FSK(Frequency Shift Keying): A „0” szimbólumnak f_1 frekvenciájú vivő, az „1”-es szimbólumnak f_2 frekvenciájú felel meg (digitális frekvenciamoduláció: a vivő frekvenciáját változtatjuk a moduláló jel szerint)

PSK(Phase Shift Keying): A jel fázisát változtatjuk (Többszintű PSK: pl 4 szint esetén 00: 0° ; 01: 90° ; 10: 180° ; 11: 270° - azaz 11-re váltáskor 270° -ot változik a fázis)

ASK (Amplitude-Shift-Keying) jel előállítás:

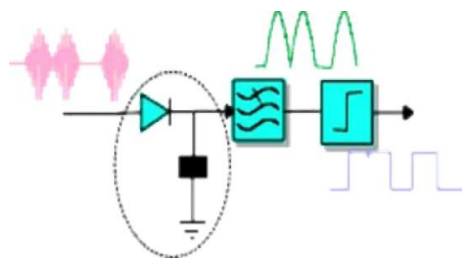


ASK jel visszaállítása:



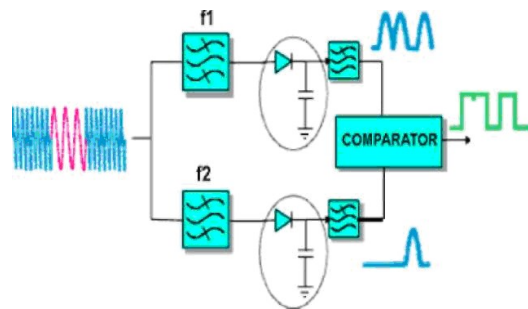
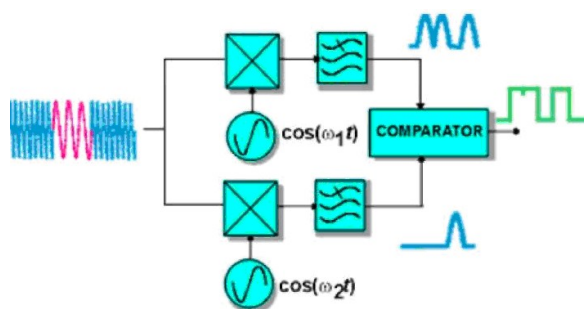
Koherens demodulálás: A vett jelet visszaszorozzuk a szinusos vivőjellel.

Ehhez ismernünk kell a vivő jel tulajdonságait.



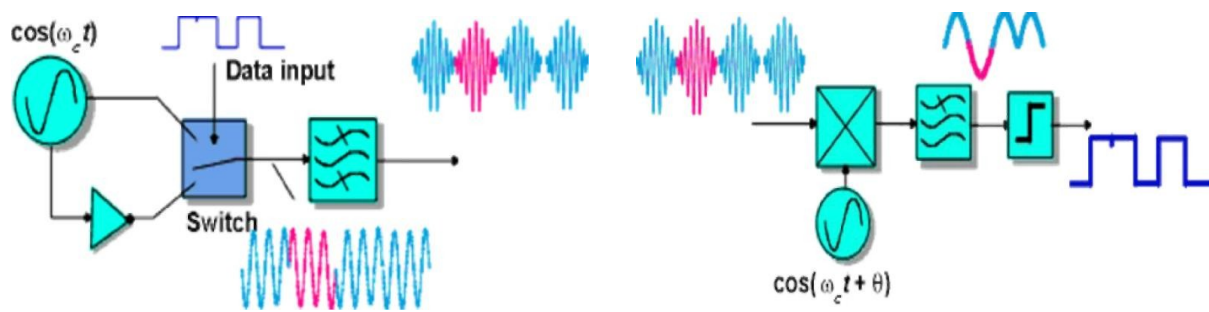
Nem koherens demoduláció: dióda+ellenállás – igénytelenebb, de egyszerűbb. Ennek az ára, hogy megnő a Bit Error Probability

FSK (Frequency-Shift-Keying) jel koherens és nem koherens demodulálása:



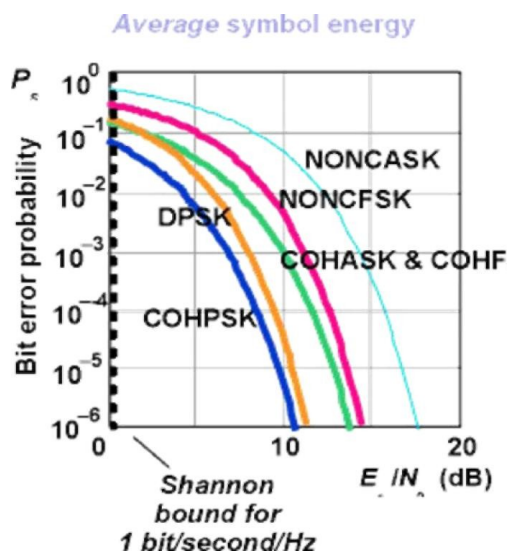
f1, f2: sáváteresztő szűrők

PSK (Phase-Shift-Keying) jel előállítása és demodulálása:



A (bináris) PSK jel egy speciális ASK jel, ahol a 0: „-1”, és az 1: „+1” (hasonlítsd össze az ASK ábrájával..)

ASK, FSK és PSK hibavalószínűségei:



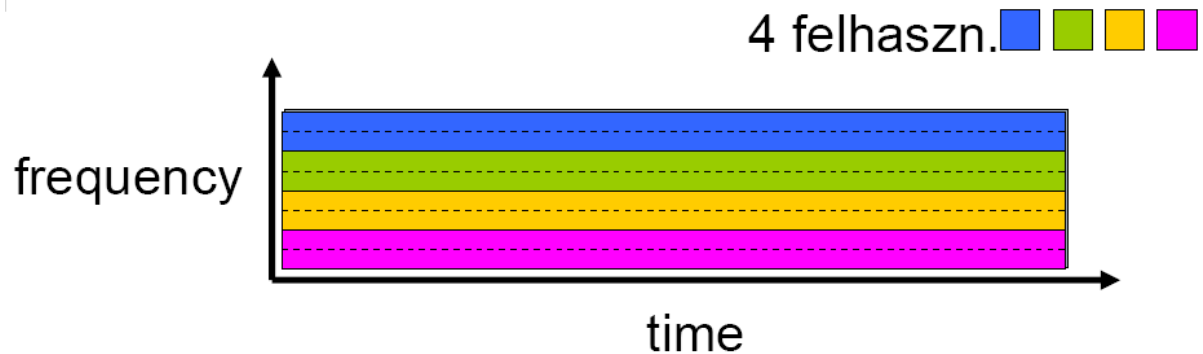
Jel/Zaj viszony: $\frac{1}{2}$ a legnagyobb hibavalószínűség, hisz vagy eltalálja a kódot, vagy nem.

Bitenergia + zaj [dB]

Többcsatornás átvitel multiplexeléssel

Frequency Division Multiplexing (FDM):

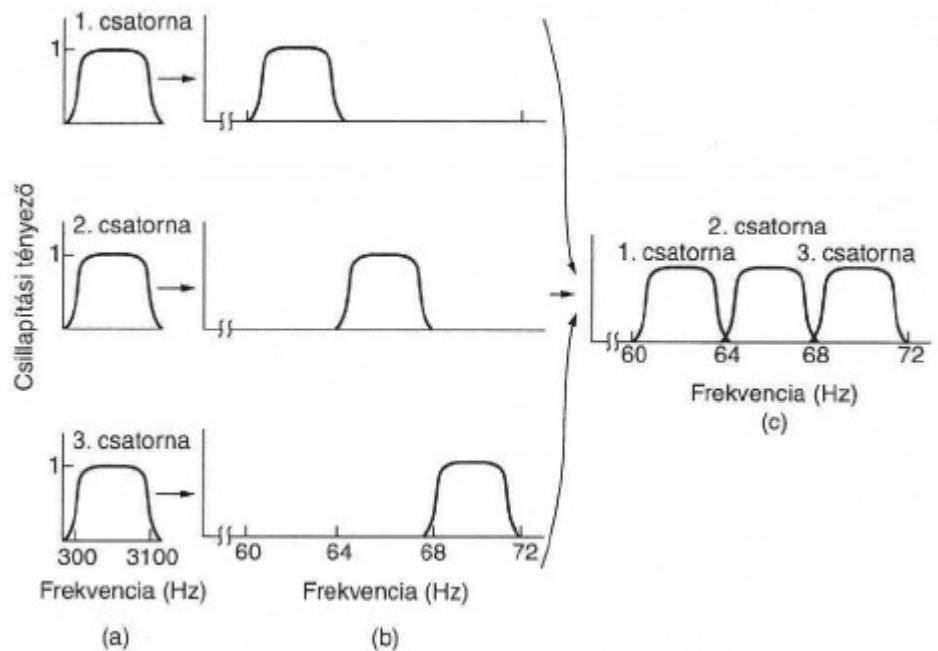
Frekvenciaosztásos multiplexelésnél a **frekvenciatartományt logikai csatornákra osztják fel**, és minden felhasználónak kizárólagos joga van valamelyik csatorna használatára. Ilyet használnak pl a kábeltévénél.



Frekvenciaosztású nyalábolás elve:

Frekvenciaosztással hogyan lehet három beszédátvitelre szánt telefonvonalat egy csatornára multiplexelni.
(a) eredeti sávszélességek.

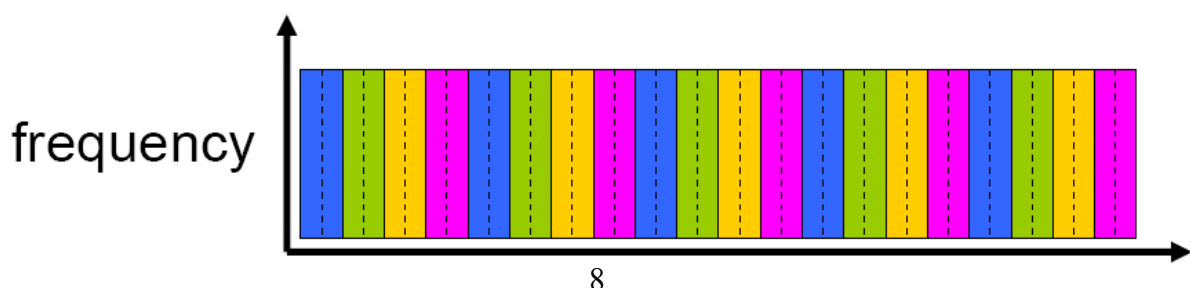
(b) frekvenciatartományban eltoltsávszélességek.
(c) Multiplexelt csatorna



Time Division Multiplexing (TDM):

Időosztásos multiplexelés esetén kétféle vagy több adatfolyam látszólag egyidejűleg fut, de fizikailag a csatornát felváltva használják.

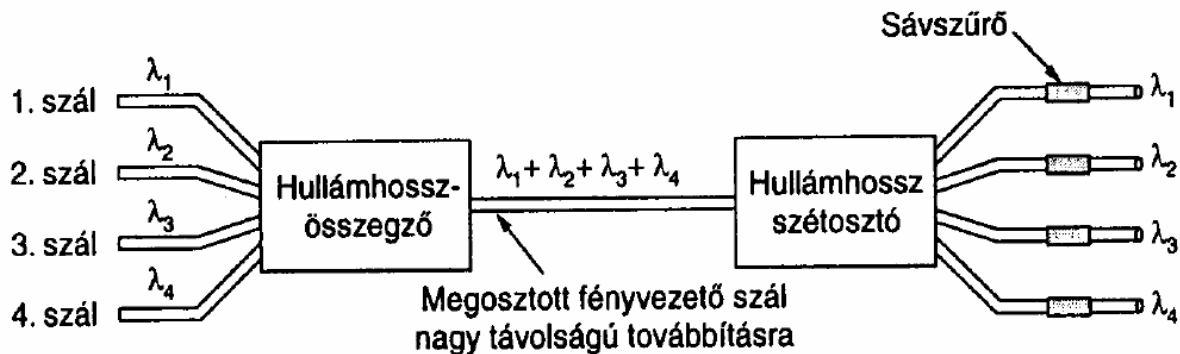
Fix méretű idődarabokra osztjuk az időtartományt, ahol az első adatfolyam az 1., a második a 2. időrészben fut, stb.



Wavelength Division Multiplexing (WDM):

Speciális frekvenciaosztásos multiplexelés, amit fényvezető szálaknál alkalmaznak.

Ld. Kapcsolás rész



Code Division Multiplexing (CDM):

A multiplexálás egy formája (és nem egy modulációs séma), amely nem osztja a csatornát idő alapján, mint a TDMA, vagy frekvencia alapján, mint a FDMA, hanem **az adatokhoz csatornánként speciális kódokat rendel, és kihasználja a konstruktív interferencia tulajdonságot** a multiplexáláshoz, spektrumszórást alkalmaz. Katonaságnál használják, nehéz zavarni.

Hírközlő csatornák a gyakorlatban

Mindegyik közegnek megvan a maga sajátossága a sáv szélességet, a késleltetést, az árat, a kiépítés nehézségeit és az üzemeltetést illetően. Az átviteli közegeknek két nagy csoportja van: az egyik a vezetékes közegek csoportja, a másik pedig a vezeték nélküli közegek csoportja.

Jeltovábbítás fémvezetőkkel

Két fémvezető és köztük dielektromos szigetelés (levegő is lehet). Szakszerű elnevezés: **TEM-hullámvezető** (Transzverzális Elektromos-Mágneses)

Sodrott(csavart) érpár (Twisted Pair):

A legrégebbi, de még ma is a legelterjedtebb átviteli közeg. Két szigetelt rézhuzalból áll, amelyek tipikusan 1 mm vastagságúak. A rézhuzalok a DNS-hez hasonlóan spirálszerűen egymás köré vannak tekerve. A két eret azért sodorják össze, hogy csökkentsék a kettő közötti elektromágneses kölcsönhatást. A vezetékek sáv szélessége néhány Mb/s pár kilométeres távolságon belül.

A **3-as kategóriájú** csavart érpár (kb. **16 MHz-ig**) két finoman egymás köré tekert, szigetelt vezetékből áll. Általában négy ilyen érpárt fognak össze egy műanyag köpennyel, ami védi, és egyben tartja a vezetéket. A fejlettebb, **5-ös kategóriájú** csavart érpár (kb. **100 MHz-ig**) lényegében megegyezik a 3-as kategóriájú vezetékekkel, a különbség csak annyi, hogy egységnyi hosszon többet csavarodott, és teflonos szigeteléssel látták el. Ez a megoldás a vezetékek között kisebb áthallást, és nagyobb távolság esetén is jobb minőségű jelátvitelt eredményezett. Ezt a két kábelfajtát gyakran **árnyékolatlan csavart érpárnak** (Unshielded Twisted Pair, **UTP**) is hívják. Telefon- és számítógép hálózatoknál használják.

Strukturált kábelezés

Döntően UTP -kábelezést használ

Strukturált: központi elosztókból (ún. rendezőkből) minden végponthoz külön kábel megy, szemben pl. a végpontok felfűzésével egy kábelre

Általános célú, telefon-és számítógép hálózat kialakítására egyaránt alkalmas

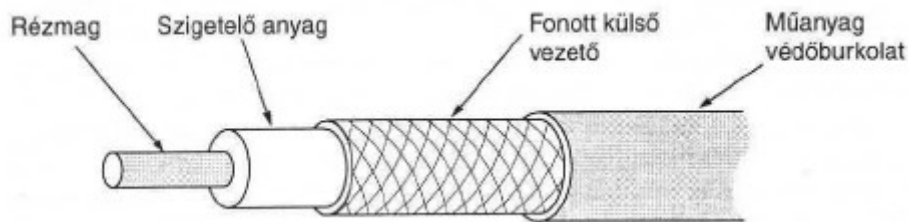
A végpontról nem kell előre eldönteni, hogy mit fogunk arra csatlakoztatni

Könnyű átkonfigurálhatóság

Felépítése:

- Főrendező: az épület központi rendezője, itt csatlakozik pl. a telefon-alközpont
- Gerinckábelezés (újabban gyakran fényvezetős)
- Alrendezők: a szintenkénti kábelezés elosztói
- Vízszintes kábelezés: többnyire sodrott érpáras, de helyettesíthető vezeték nélküli megoldással is, lásd később a vezeték nélküli lokális hálózati technikákat
- Csatlakozók

Koaxiális kábel (coaxial cable):

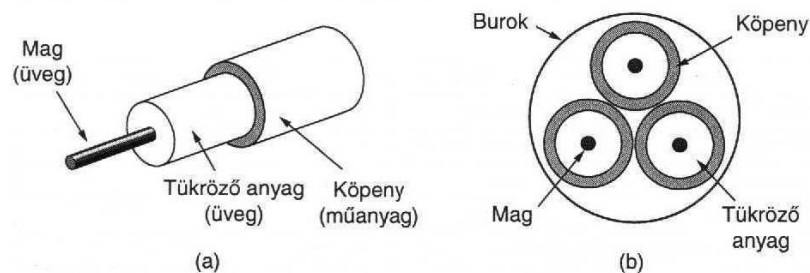


A koaxiális kábel közepén tömör rézhuzal mag van, amelyet szigetelő vesz körül. A szigetelő körül sűrű szövésű hálóból álló vezető található. A külső vezetőt mechanikai védelmet is biztosító műanyag burkolattal vonják be.

Két végén lezárás a hullámimpedanciával (50 Ohm).

- Jó zavarvédetség és nagy sáv szélesség
- Számítógéphálózatokban ma már kevésbé használják (**kábeltelevíziós rendszerekben, a távközlő hálózatok nagytávolságú átviteli rendszereiben fordul elő**, régen a PSTN betárcsázós hálózatok is ezt használták). Vagy az optikai (fényvezetős) átvitel szorítja ki, vagy kis távolságok esetén a sodrott érpár.

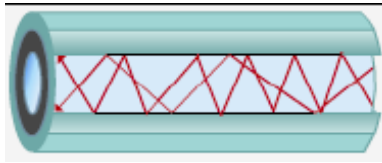
Száloptikai kábel:



(a) Fényvezető szál oldalnézetben. (b) Három fényvezető szálból álló kábel

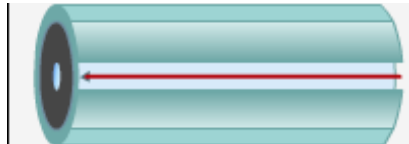
A tükröző anyag idegen neve a cladding. Core/cladding viszonyban jellemzik a kábeleket.

A fényvezető szál as adatátviteli rendszernek három fő komponense van: a fényforrás (LED/lézer), az átviteli közeg és a fényérzékelő (fotodióda) (adó, vevőerősítő, szűrő)



A fény kilépését az optikai kábelből az optikában jól ismert teljes visszaverődés jelensége akadályozza meg. Ha a közeg határfelületére érkező fénysugár beesési szöge eléri egy kritikus értéket, akkor a fénysugár már nem lép ki a levegőbe, hanem visszaverődik az üvegbe. Az üvegszálaban az adóból

kibocsátott fénysugár fog ide-oda verődni, az ilyen optikai szálakat **többszálú üvegszálabnak** (multimode fiber) nevezik. Itt a core/cladding arány kb 0,6



Ha azonban a szál átmérőjét a fény hullámhosszára csökkentjük, akkor a fénysugár már csak a kábel hosszanti tengelye mentén, verődés nélkül terjed. Ez az **egyszálú üvegszálab** (single (mono) mode fiber). Itt a core/cladding arány kb 0,1.

Csillapítás és torzítások

Az optikai szálab áthaladó fény különbözőoptikai hatásoknak van kitéve. Ezek lehetnek lineáris és nemlineáris hatások:

- Lineáris csillapítás: a teljesítmény csökkenése a távolság függvényében
- Lineáris diszperzó: az optikai impulzus alakjának torzulása
- Nemlineáris: a törésmutató függése az elektromos tér intenzitásától,

Optikai átvitel szabad térben:

Az összeköttetéshez közvetlen rálátásra van szükség. A terjedést nagymértékben befolyásolják a légkör jellemzői: eső, pára, köd. Legfeljebb pár km-es távolságokat lehet megbízhatóan áthidalni. A nyomvonalat körültekintően kell megválasztani (vízfelületek, nagyméretű fémfelületek felett aggályos)

Optikai hálózati elemek

- Adók: LED, lézer
- Vevők: fotodióda
- Erősítő
- Szűrő
- Szétosztó-összegző

Jeltovábbítás vezeték nélkül

Rádiócsatornák:

Az elektromágneses hullámtartománynak az ultrahang- és a látható fény tartományai között része. Igen széles, és nem teljesen kihasznált sáv: ~10 kHz-től ~1 THz-ig. Az elektromos jel átalakítása elektromágneses hullámmá és viszont: adó- és vevőantennák.

A hullámterjedést befolyásoló jelenségek

szabadtéri csillapítás

a távolság négyzetével fordítottan arányos

visszaverődés (reflexió)

bármilyen közegről, amely az adott frekvenciasávban visszaverő felületként szerepel (pl. légköri réteg a dekaméteres tartományban, épület a cm-es tartományban)

törés (refrakció)

elhajlás (diffrakció)

szóródás (scattering)

az adott hullámhossznak megfelelő méretű részecskéket tartalmazó közegben, pl. troposzféra

Zajok a rádiócsatornában:

- Termikus zaj a vevő bemenetén
- Atmoszférikus zajok
- Kozmikus zaj, galaktikus zaj

Zavarok:

- ipari zajok, zavarok
- más rádiórendszerekből származó zavarok

A rádiócsatorna nyitottsága miatt kritikus a frekvenciasávok felosztása a felhasználók között
Általában: engedély kell, kivétel: ISM-sáv (industrial, scientific, medical)

Mikrohullámú átvitel:

100 MHz felett az elektromágneses hullámok egyenes vonal mentén terjednek, és ezért jól fókuszálhatók. Ha ezeket a hullámokat egy parabolaantenna segítségével egy keskeny nyalábbá fogjuk össze, akkor a jel-zaj viszony sokkal jobb lesz, viszont ehhez az adó és a vevő antennát nagyon pontosan egymáshoz kell igazítani.

Mivel a mikrohullámok egyenes vonal mentén terjednek, ezért a földfelszín görbülete problémát jelent, ha az adótornyok túlságosan messze vannak egymástól. Ezért meghatározott távolságoként ismétlőkre van szükség.

Az alacsony frekvenciás rádióhullámokkal szemben a mikrohullámok nem képesek áthatolni az épületek falain. A hullámok egy kis része megtörhet az alacsonyabb légköri rétegeknél, ezek a hullámok valamivel később érnek célba, mint a közvetlen beérkező hullámok. A megtört hullámok fázisa nem egyezik meg a közvetlen beérkező hullámokéval, így ezek akár ki is olthatják egymást (ha a Fresnel zónában akadályba ütközik a jel). Ez a jelenség az **elhalkulás (multipath fading)**. A többutas terjedés hatásának csökkentése: többszörös vétel (diversity):

- Több antenna és vevő egyidejűleg, és optimális kombinálás (tér-diversity)
- Adás és vétel párhuzamosan több frekvencián (frekvencia-diversity)

2. Többszörös Hozzáférés

A többszörös hozzáférés szerepe, jelentősége

- *Takarékoskodás az átviteli közeggel*
- *Rugalmas hálózati elérés biztosítása*
- *A rugalmas, kötetlen, akár mobil elérés rádiócsatornán valósítható meg*

Hátrány:

- *Bonyolult algoritmusok*
- *Biztonsági kérdések*

A csatorna átviteli képességének megosztása: FDMA, TDMA, CDMA

- **FDMA:** Ortogonális, de technikailag hátrányos, alkalmazása elsősorban valódi idejű esetben()
- **TDMA:** Ortogonális, rugalmas megosztásra kiváló (GSM)
- **CDMA:** Nem ortogonális, de elvileg a legjobb (nehéz zavarni)

Kétirányú kommunikáció:

- **Frequency Division Duplex**
- **Time Division Duplex**

A hozzáférési módszerek teljesítőképességének jellemzése:

- **Átvitel (throughput):** kiszolgált információ - a fellépő igény függvényében. Optimális esetben az átvitel egyenesen arányos az igény növekedésével.
- **Kiszolgálási késleltetés:** az igény jelentkezése és kiszolgálása közötti idő
- **Igazságosság (fairness):** teljesül-e a jogosultság szerinti kiszolgálás
- **Stabilitás:** reakció a túlterhelésre, a forgalom dinamikus változására

A többszörös hozzáférés fajtái

Közösen használt erőforrás igénybevétele:

- Szabad: igény szerint
- Vezérelt: engedély szerint

A vezérlés módja:

- Centralizált: egy vezérlő felügyeli a hozzáférést
- Elosztott: a résztvevők nyílt / rejtett mechanizmus révén végzik a hozzáférés vezérlését

A kiszolgálás kötöttsége:

- Merev: „ami jár az jár”
- Rugalmas: igény szerinti

Körbefordulási idő (Turnaround-Time):

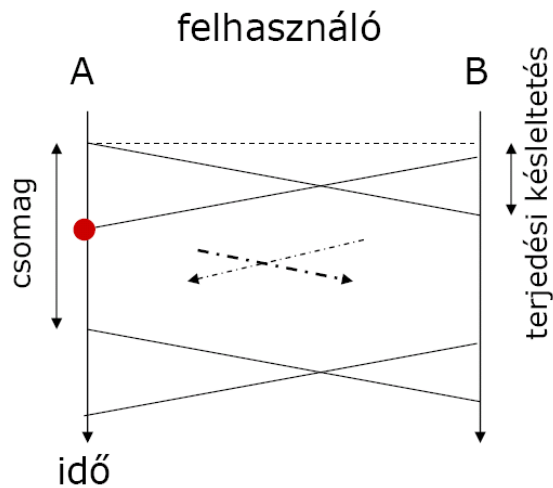
A hozzáférést elsődlegesen meghatározó paraméter:

$$\alpha = \frac{D}{T}$$

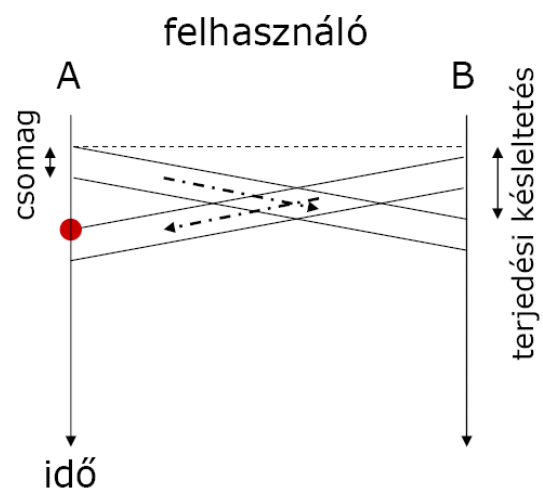
D a terjedési idő két állomás között

T egy átlag-hosszú csomag továbbítási ideje.

□ Kis α érték



□ Nagy α érték



Függ:

az átviteli sebességtől,
2 pont közti távolságtól
a csomag méretétől.

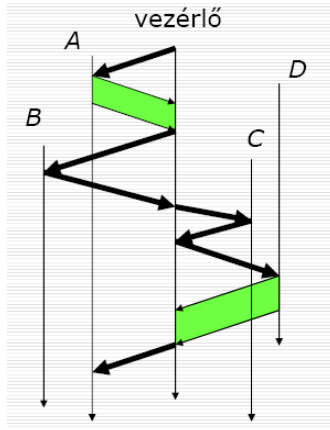
Nagy α esetén csak az egész csomag elküldése után érezhetjük meg a hibát. Ekkor $\alpha=2D$.

Kis α esetén a csomag küldése közben érzékelhető a hiba. Ekkor $\alpha=2T$.

Round-Trip Time= $2(D+T)$

Centralizált vezérlés:

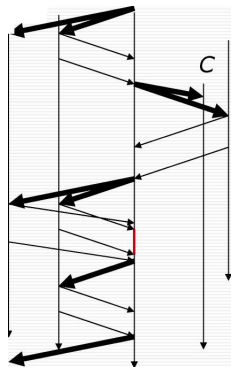
Lekérdezés (Polling):



A vezérlő egyenként lekérdezi a hálózati elemeket, hogy van-e küldeni valójára. Ha van, elküldi, ha nincs, visszaigazolja ezt a vezérlőnek. Két állomás csak a vezérlőn keresztül képes kommunikálni

- Kihasználtság: Hasznos adatátviteli idő/szervezési idő
- Késleltetés: Körbefordulási idő/2
- A módszer fair és stabil (ha állandóan van üzenet).
- Nem léphet fel ütközés
- A vezérlő meghibásodásával a hálózat megbénul

Próbálkozás (Probing):

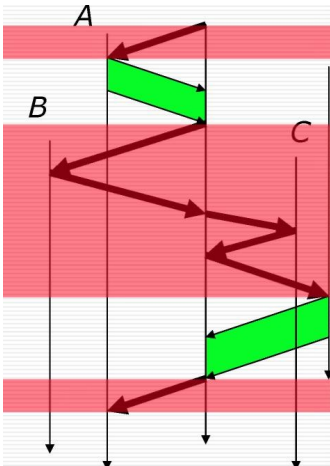


Csoportos lekérdezés: egyszerre több állomást kérdez meg a vezérlő, ha többen is küldenek, ütközéskezelés kell (részekre bontás).

- Kihasználtság javul
- Kiszolgálási késleltetés csökken
- Stabil
- Fair

Foglalás (Reservation, Roll Call Polling):

Az átviteli csatornát foglalási és átviteli részre osztják. A vezérlő a foglalási részben az érkező igények alapján csatornahasználati jogosultságot jelöl ki.



Az igények gyűjtése:

- Egyedi „csatornákon”
- „versenyben”
- Ha nagy a körbefordulási idő, akkor a lekérdezés hatékonysága romlik
- Külön foglalási és átviteli rész
- Szélessáv: átvitelre
- Rövidsáv: foglalásra
- Dedikált csatornarészek foglalásra
- Verseny alapú elérés
- A vezérlő a beérkezett igények alapján engedélyt küld a felhasználónak

Elosztott vezérlés:

A vezérlés szinte megszűnik, így nő a kihasználtság, bár biztonsági kérdések merülnek fel.

Centralizált: Terminálhálózatok (Master-Slave)

Elosztott: LAN (peer-to-peer)

Elosztott lekérdezés, és próba:

Polling: explicit kérdés nélkül, de merev időkiosztással. Mint a TDM, de itt a felhasználók maguk dolgoznak

Probing: a felhasználók csoportjai együtt kísérik meg a csatornahasználatot, ha nem kapnak nyugtát, akkor a csoport részenként folytatja, akár addig, míg egyedül maradnak. A csoportok, és tördelésük előre rögzített.

Mindkét esetben fontos az órák együttfutása

Vezérjel átadás (token passing):

Ez a leggyakrabban használt közeghozzáférés vezérlési módszer a gyűrű topológiájú hálózatoknál. A gyűrűben egy speciális üzenet, a **vezérjel (token)** halad körbe-körbe a hosztok között. A vezérjel hordozza magában a hálózat foglaltságát. Amikor egy állomás veszi a tokent, megvizsgálja, hogy foglalt-e. Amennyiben szabad jelzést észlel, foglaltra állítja, majd az üzenetével együtt továbbküldi. Az üzenetet minden állomás veszi, majd megvizsgálja, hogy neki szól-e. Amennyiben igen, veszi az üzenetet, majd feldolgozza. Ha nem, továbbküldik. A küldő állomás veszi a saját üzenetét, kivonja azt a vezérjelből, szabadra állítja, majd továbbküldi. Így kerül a küldési jog ahhoz az állomáshoz, amely a küldést befejező után helyezkedik el.

- Kifinomult együttműködést igényel az állomások között.
- Jó kihasználtságot ér el, korlátozott késleltetéssel, hasonlóan a lekérdezéshez.
- Az igazságos csatornamegosztás biztosítható.

Vivőérzékelés (Carrier Sensing):

- Csak foglaltságot ellenőriz
- Nagy hatékonyság
- Nagy érzékenység a terjedési késleltetésre
- Nagy körbefordulási idő esetén nagyon rossz
- Instabil lehet: túlterheltség esetén sok ütközés
- Fair

1-perzisztens Carrier Sensing Multiple Access (CSMA):

Amikor egy állomás adni készül, először belehallgat a csatornába, hogy az foglalt-e. Ha a igen, akkor addig vár, amíg az ismét szabad nem lesz. Amikor az állomás szabad csatornát érzékel, elküld egy keretet. Ha ütközés következik be, akkor az állomás véletlen hosszúságú ideig vár, majd újból előlről kezdi a keret elküldési procedúrát.

Nemperzisztens (nonpersistent) CSMA:

Küldés előtt az állomás megfigyeli a csatornát. Ha senki sem forgalmaz, akkor az állomás elkezdhet adni. Ha azonban foglalt a csatorna, nem folytatja folyamatosan a megfigyelést, hogy a forgalom megszűntével azonnal megkezdje az adást, hanem véletlen hosszúságú ideig várakozik, és ekkor előlről kezdi az algoritmust. Jobb kihasználtsághoz, de nagyobb késleltetéshez vezet, mint az 1-perzisztens CSMA.

p-perzisztens (p-persistent) CSMA:

Amikor egy állomás adásra kész állapotba kerül, megvizsgálja a csatornát. Ha szabad, akkor p valószínűséggel forgalmazni kezd, vagy $q = 1 - p$ valószínűséggel visszalép szándékától a következő időrésig. Ha a következő időrésben a csatorna még mindig szabad, akkor ismét p , illetve q valószínűséggel ad vagy visszalép.

CSMA/Collision Detection:

Az állomások az ütközés érzékelése után azonnal befejezik az adásukat, majd véletlen ideig vár, mielőtt újra megvizsgálná a vivőt.

Az ütközés-detekció csak vezetékes csatornán lehetséges, rádió csatornán nem lehet ütközést érzékelni.

Aki éppen használja a csatornát, az nem tud ütközést észlelni.

- **Árnyékolt (hidden)** terminál: Nem hall mindenki mindenkit, egy folyamatban lévő adást megzavarhatunk.
- **Exponált (exposed)** terminál: Idegen rendszerből észlelhet adást egy állomás, ezért nem használja a sajátját
- LAN-ra jellemző

CSMA/Collision Avoidance:

- Megpróbálja elkerülni az ütközéseket.
- Sűrűsödés esetén p-perzisztens CSMAként működik
- Árnyékolt: nem mindenki hall a hálózatban mindenkit.
- Exponált: előforulhat az, hogy egy állomás túl jó helyzetbe kerül az áthallások miatt.
- **Széleskörben használt**
-

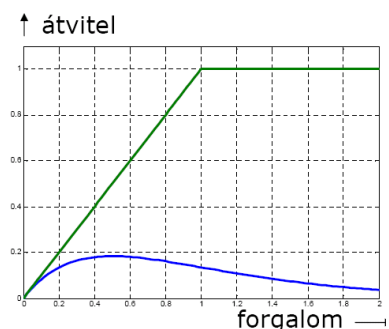
Busy Tone Multiple Access (BTMA)

- Az árnyékolt vagy exponált terminál probléma kiküszöbölésére
- A vevő kiad egy foglalt jelzést egy frekvenciában elkülönített részcsatornán.
- Igénybejelentés (RTS)
- Nyugta (CTS)
- Csak ezek után történik információ átvitel
- Az átvitel hosszát tartalmazza a két üzenet

Egyszerű Aloha:

Teljesen kötetlen hozzáférés, aki akar, az küld. Ütközéskor keretek vesznek el.

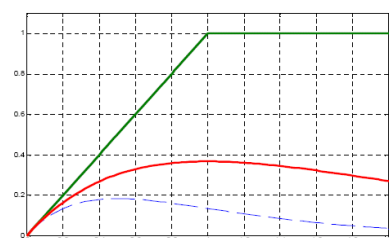
- Kihasználtsága rossz
- Alapvetően instabil.
- Késleltetése nem korlátos
- Hosszútávon fair



Réselt Aloha:

Az állomások nem adhatnak bármikor, csak bizonyos időközönként.

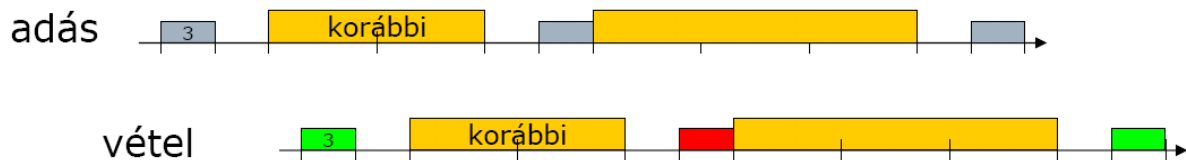
- **Csak a kihasználtság javul.**
- Ütközésnél teljes fedés
- A jellemzők javítására foglalatást használhat



Helyfoglaló Aloha:

Két részből áll a folyamat: A foglalási részben az állomások réselt Aloha használatával kis méretű foglaló kereteket küldenek. Az az állomás, amely ütközés nélkül képes küldeni, megkapja a csatorna használatának jogát. Egy állomás addig küld foglaló keretet, amíg nem sikerül ütközésmentesen továbbítania azt. Ezután az adatokat szabadon küldheti, hisz kizárólagos joga van a csatorna használatára.

- Ütközésfeloldás: Probing szerű, az ütközést produkálók csoportja résztvevőnként véletlen időközönként újrapróbálkozik.
- Mindenki visszahallja az igénybejelentést.
- **Műholdas kommunikáció esetén használják**
- Függs a használt közegtől
- A biztonsági problémákat kezelni kell



Ütközések feloldására egy gyakorlati példa a Capetanakis fa algoritmus.

- Olyan algoritmusokat használ, ami a konfliktus mihamarabb való megszüntetésére törekszik
- A felhasználók tudják a csatornáról, hogy üres, sikeres, vagy ütközött

3. Kapcsolás

Kapcsolás: azon eljárások, technikák összessége, amelyek kapcsolt számítógép-ill. távközlési hálózatokban két, nem szomszédos csomópont között összeköttetést hoznak létre

*A kapcsolással létrehozott összeköttetés **nem feltétlenül közvetlen és nem feltétlenül fizikai.***

Hálózat: jel-átviteli csatornák szövevénye

Három alkotóelem:

- (felhasználói) végpont
- összekötés (link)
- (hálózati) csomópont

Hálózat alapvető funkciója:

- Kommunikációs csatorna végpontok között
- Pont – pont
- Pont – multipont
- Multipont - multipont

Hálózat(-építés, -működés)i alapelvek

A végpontok közötti kommunikációs csatornák:

Időben

- Permanensek
- Időszakosak (kapcsoltak)

Módszerükben

- Valóságosak (fizikaiak)
- Virtuálisak (logikaiak)

Csatornák létrehozásának alapvető eszköze: KAPCSOLÁS a csomópontokon

Számítógép-hálózatokban az éppen aktív állomás (csomópont) az adatokat/üzeneteket továbbíthatja:

- az összes többi állomáshoz, ez az **adatszóró(üzenetszóró) hálózat**
- egy bizonyos (v. néhány) állomáshoz, ez a **kapcsolt hálózat**: ezzel foglalkozunk
- A kapcsolt hálózatnak magának kell gondoskodnia az információnak a célállomáshoz történő eljuttatásáról

Kapcsolás fajták:

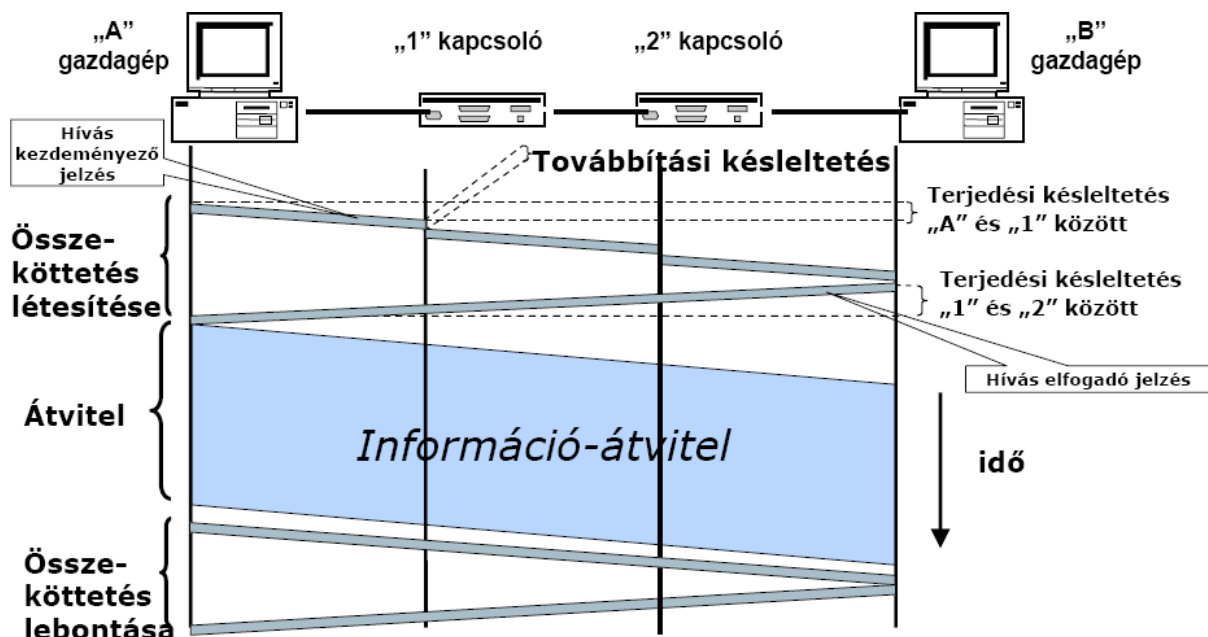
- Mindenki mindenkivel: egyszerű, drága, irreális
- Csak bizonyosakkal: kitüntetett csomópont(kapcsoló), bonyolult, de gazdaságos

Összeköttetés-alapú hálózat: a kommunikáló csomópontok a tényleges adatátvitel előtt végpontok közötti összeköttetést (end-to-end connection) létesítenek.

Összeköttetés-mentes hálózat: a kommunikáló csomópontok között az adatátvitel előzetes összeköttetés létrehozása nélkül történik

A kapcsolás elvégezhető, ha vannak nevek, címek, igény-bejelentési szabályok

Áramkörkapcsolás/Vonalkapcsolás (fizikai kapcsolat):



A telefóniázás tipikus folyamata

A kapcsolatot fel kell építeni, majd le kell bontani.

Minden adat egy dedikált fizikai vonalon halad, az adatátvitel során nem léphet fel ütközés, csak kapcsolás közben.

A kapcsolóelem a tényleges kapcsolást végzi.

A kapcsoló-vezérlő kiválasztja az(oka)t a kapcsolóelem(ek)e(t), amely(ek) működésbe lép(nek) kapcsoláskor.

A kapcsolóelemek MUX/DEMUX alapúak.

Továbbítás alatt a csomópontok az adatokat **nem** tárolják.

Valós idejű információátvitelre kiváló

Ütközés csak a kapcsolás során léphet fel, adatátvitel során nem.

Kapcsolótípusok (áramkörkapcsolásnál):

Tér-osztásos (Space Division Multiplexing - SDM) kapcsoló:

Minden beérkező minta a rendeltetési helytől függően más és más térbeli (fizikai) útvonalon halad. Legegyszerűbb megvalósítása a keresztpontos (crossbar) kapcsológép – régi telefonközpont.

Előny: egyszerű

Hátrány: nagy méret: N bemenet, N kimenet $\rightarrow N \times N$ kapcsoló

Belső blokkolódás: a kimenet szabad, de nincs szabad útvonal a két állomás között

Külső blokkolódás: két hívó fél $\rightarrow$ ütközés a vevőnél, az egyik hívó blokkolva lesz

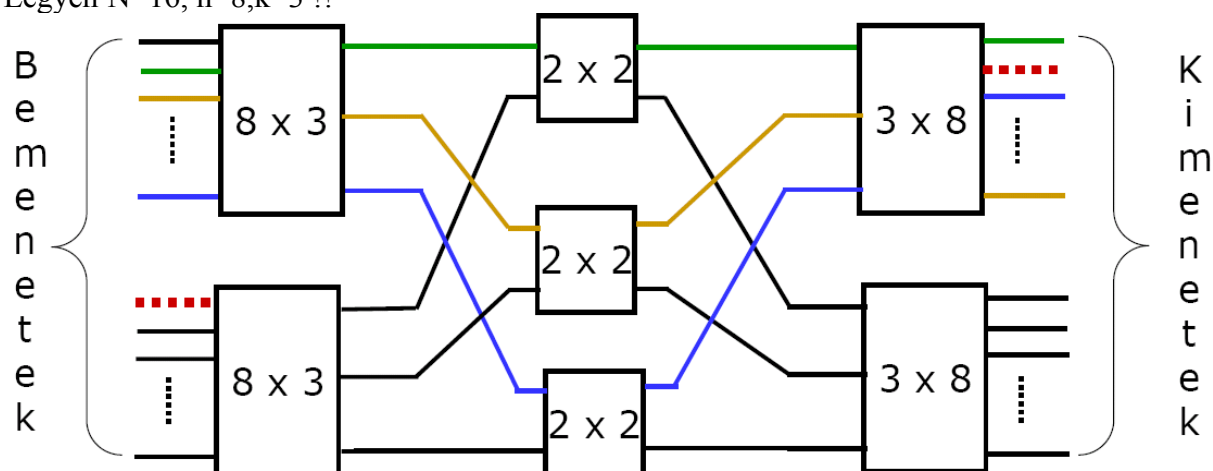
Egyszerű crossbar kapcsolóban nincs belső blokkolás

Többszintű tér-osztásos kapcsoló:

Cél: méretek csökkentése, kihasználtság növelése (egy lezárt kapcsoló sorában és oszlopában a többi kapcsoló kihasználatlan)

Megoldás: N^2 kapcsoló helyett az N bemenetet multiplexerrel leosztjuk, majd egy belső, kisebb kapcsolóval (MUX/DEMUX) továbbítjuk, hogy a kimeneti demultiplexer továbbítsa a megfelelő címzettnek.

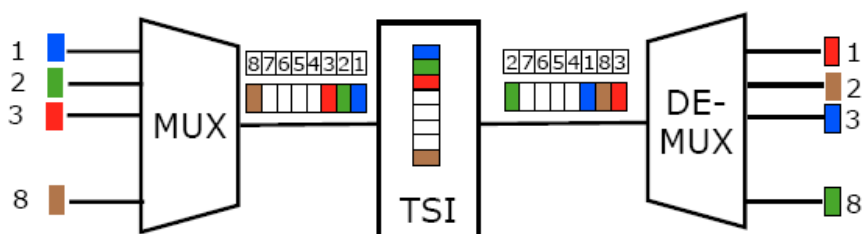
Egy háromfokozatú kapcsoló első fokozata álljon N/n darab $n \times k$ méretű, a második fokozat k darab $N/n \times N/n$ méretű és a harmadik ismét N/n darab $k \times n$ méretű kapcsolótömbből. Legyen $N=16, n=8, k=3$!!



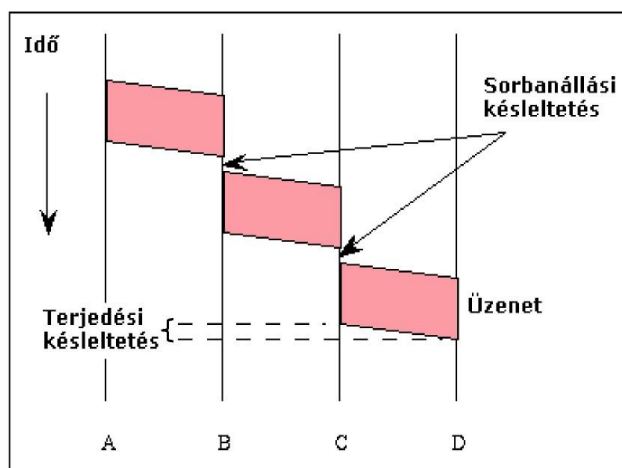
- Kapcsolók száma 108, nem 256!
- A bemeneti tömbök két független úton kapcsolódnak a kimeneti tömbökhöz
- Kis k értékek esetén belsőblokkolás lehetséges! (piros pontvonal)

Időosztásos (Time Division Multiplexing - TDM) kapcsoló:

Egy N sebességű csatorna van, bemenete egy multiplexer, amire N darab egységnyi sebességű bemenet kapcsolódik, a kimeneten pedig egy demultiplexer osztja szét az adatokat. Az időosztások kapcsolók időrés-cserélővel (**Time Slot Interchanger, TSI**) végzik a kapcsolást. A TSI egy rögzített méretű puffermemória, amelybe a bemeneti csatornákról érkező multiplexelt minták beírása cím szerinti sorrendben, kiolvasása viszont ettől eltérően történik. 125 μ s ismétlődési idővel és 40 ns hozzáférési idővel számolva 1560 vonal kapcsolható, ez nem túl sok. Vannak épp ezért ST és TST ((Time), Space, Time) kapcsolók.



Üzenetkapcsolás:



Ennél a kapcsolódási módnál a küldő és a vevő között nem jön létre fizikai rézvezetékes összeköttetés (összeköttetésmentes), hanem amikor egy küldő egy adatblokkot akar továbbítani, akkor az az első kapcsolóközpont (azaz router) eltárolja, majd **valamikor később** továbbküldi a következő központnak és így tovább. Azokat a hálózatokat, amelyek ezt az eljárást használják, **tárol-és-továbbít (store-and-forward)** hálózatoknak nevezzük. Megvalósításához puffer tár kell. Két szomszédos csomópont közt dedikált csatorna vagy akár vonalkapcsolás is lehet

Ilyen volt pl. az Arpanet.

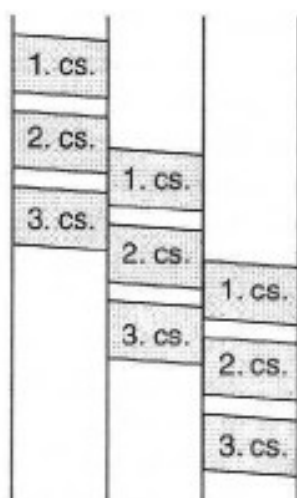
Előnyök:

- Az adatcsatornákat a kommunikáló eszközök megosztva használják, javul a csatorna kihasználtsága
- Az átmeneti tárolás képessége csökkenti a torlódásokra való érzékenységet
- Az üzenetekhez elsőbbség (prioritás) rendelhető
- Támogatja az üzenetszórást (broadcast)

Hátránya:

- A fellépő késleltetések miatt általában nem képes valós idejű átvitelre (élő hang, mozgókép). De nem is erre találták ki, hanem adatátvitelre, amikor a késleltetésre kevésbé vagyunk érzékenyek

Csomagkapcsolás (Logikai kapcsolat):



- Az üzenetet a küldő csomópont kisebb részekre, csomagokra tördeli.
- A csomag tartalmazza:
 - a küldő csomópont azonosítóját/címét,
 - a címzett csomópont azonosítóját/címét
 - a csomag helyét az üzenetben.
- A csomagokat a küldő egymás után elküldi a hálózaton át a címzettnek.
- A közbeeső csomópontok a bennük lévő cím alapján továbbítják a csomagokat, akár egymástól különböző útvonalon.
- A csomagok az eredetitől eltérő sorrendben is érkezhettek a címzethez.
- A címzett a csomagokban található információ alapján visszaállítja a helyes csomagsorrendet

A csomópontok eszközei:

- Switch (lokális) – olyan csomópont, amely a csomagokat ugyanazon helyi hálózaton belül továbbítja
- Router (globális) – két vagy több hálózat közt továbbít

Csomagkapcsolás megvalósítható:

- **Összeköttetés-mentes** módon, ezt nevezik röviden **datagram** kapcsolásnak is, vagy
- **Összeköttetés alapú** módon, amire a **virtuális áramkörkapcsolás** elnevezést is használják

Áramkörkapcsolás vs Csomagkapcsolás

Jellemző	Vonalkapcsolás	Csomagkapcsolás
Dedikált vezetékes útvonal	Van	Nincs (több összeköttetés is használhatja ugyanazt a csatornát)
Rendelkezésre álló sávszélesség	Állandó	Dinamikusan változó
Kihasználatlan sávszélesség	Van	Nincs
Tárol-és-továbbít típusú adatátvitel	Nem	Igen
Minden csomag ugyanazon az útvonalon halad	Igen	Nem
Kapcsolatfelépítés	Szükséges	Nem szükséges
Torlódás lehetséges ideje	Kapcsolatfelépítés során	Bármelyik csomagnál

- Az **áramkörkapcsolás** ideális, amikor az **adatokat gyorsan, sorrendhelyesen és állandó sebességgel** kell továbbítani, például telefonátvitelre
- A **csomagkapcsolás** előnyösen alkalmazható a **lökésszerű átvittel járó és a késleltetéseket jól tűrő adatok**, például elektronikus levelek, web-oldalak továbbítására
- **Csomagkapcsolásnál** a csomagok **késleltetése lecsökken, a hálózat átbocsátóképessége pedig megnő**

Datagram kapcsolás:

- Egy datagram alapú alhálózatban nincsenek előre meghatározott útvonalak, még akkor sem, ha maga a szolgált összeköttetés alapú.
- Minden egyes csomagot az előzőektől függetlenül irányítanak, a csomagok önálló egységet képviselnek.
- Az egymás után következő csomagok más-más útvonalat követhetnek, minden csomag tartalmazza a cél teljes globális címét.
- A két végpont közötti csomópontok megvizsgálják a csomag fejrészét és kiválasztják az útvonal következő szakaszát, vagyis azt a kimeneti kapcsolatot (port), ahová a csomagot továbbítják.

A választás során két tényezőt kell figyelembe venni:

- a csomag a lehető legrövidebb úton érjen rendeltetési helyére
- hol található szabad csomópont, amely képes a csomag fogadására

Ez a port leképezés (port mapping):

a csomag fejrészében található címhez megkeresi a legjobb kimenő kapcsolatot az útvonalválasztó táblázat alapján, amely minden lehetséges cél-címhez tartalmazza a következőket:

- a cél-cím (destination address, DA)
- a kimeneti kapcsolat (output port)
- az adott kimenethez tartozó „költség” típusú mezőt

Belső és kimeneti blokkolás egyaránt lehetséges. Elkerülésének módjai:

- túltartalékolás (overprovisioning), a belső kapcsolatok gyorsabbra választása, mint a bemenetek sebessége
- pufferek, a csomagok késleltetésére
- visszaduzzasztás(backpressure): küldő kényszerítése a küldés felfüggesztésére (ideigl.)
- párhuzamos kapcsolás, több párhuzamos útvonal kialakítása a bemenetek és a kimenetek között, a túltartalékolás térbeli megfelelője
- Nincs kiszolgálási garancia

Virtuális áramkörkapcsolás:

- A cél, hogy elkerüljük azt, hogy minden elküldött csomagnak vagy cellának újra útvonalat kelljen választani.
- Ehelyett, amikor egy összeköttetés felépül, ennek a felépülésnek a részeként egy útvonalat is kiválasztanak a forrásgéptől a célgépig. Ezt az útvonalat használják a teljes, ezen az összeköttetésen keresztül folyó forgalom számára, amely pontosan ugyanúgy működik, ahogyan a telefonrendszer.
- Amikor a kapcsolatot lebontják, a virtuális áramkör is megszakad.
- A virtuális áramköröket egy helyi, az adott csomóponton érvényes azonosítóval a virtuális áramkör azonosítóval (**Virtual Circuit Identifier, VCI**) azonosítjuk.

Címzési információk a csomagban:

- kapcsolatfelvételi (**Call Request, CR**) csomag
- kapcsolat nyugtázó (**Call Confirm CC**) csomag
- A CR és CC csomagban a VCI mellett megtalálható a hívást kezdeményező és a cél-csomópont teljes, globális címe is, ez a rendeltetési cím (**Destination Address, DA**), illetve a forrás cím (**Source Address, SA**)
- Az adatcsomagokban csak a virtuális áramkör azonosító, a VCI található, nem kell címzett/küldő adatokat tárolnia.

A kapcsolat felépítése:

A virtuális áramkör felépítéséhez a CR csomagot a hálózat csomópontjai a hálózati útválasztó tábla (**Network Routing Table, NRT**) információi alapján továbbítja. Az NRT bejegyzései tartalmazzák - többek között - az adott csomópontból elérhető rendeltetési helyek címét (DA) és az ezekhez vezető útvonal következő útválasztójának címét (next hop/gateway), és a kimeneti port címét (interface), amelyen a csomagot tovább kell küldeni.

A CR csomag továbbításához a csomópont:

- keres egy szabad logikai csatornát
- bejegyzést készít a kimenő porthoz tartozó virtuális áramkör táblába (VCI_{in} , $PORT_{out}$, VCI_{out})
- a csomagban felcseréli a bemeneti VCI-t a kimenetivel
- elküldi a csomagot a kimeneti porton át

Az adatcsomagok továbbítása a kapcsolatfelépítés során kialakított virtuális csatorna (**Virtual Channel - VC**) táblák alapján történik:

- a kapcsoló megkeresi a beérkezett adatcsomag bemeneti portjának és VCI-jének megfelelő bejegyzést a VC táblában
- a csomagban felcseréli a VCI-t a táblában talált kimeneti VCI-vel
- a csomagot a táblában talált számú porton továbbküldi

Datagram vs Virtuális Áramkörkapcsolás

Kérdés	DG alhálózatokban	VÁ alhálózatokban
Áramkörfelépítés	Nem szükséges	Megkövetelt
Címzés	Minden csomag tartalmazza a teljes forrás- és célcímet	Minden csomag egy rövid VÁ számot tartalmaz
Állapotinformáció	Az alhálózat nem tartalmaz állapotinformációkat	Minden VÁ táblázat helyet követel az alhálózatban
Forgalomirányítás	Minden csomagot függetlenül irányítanak	Az útvonalat akkor választják ki, amikor a VÁ felépül
A forgalomirányítók meghibásodásainak hatása	Semmi, eltekintve az összeomlás során elveszett csomagoktól	Minden VÁ megszakad, amely a csődöt mondott forgalomirányítón keresztülhaladt
Torlódásvédelem	Bonyolult	Könnyű, ha elég puffert lehet előre lefoglalni mindegyik VÁ számára

Hullámhossz-kapcsolás (Wavelength Division Multiplexing, WDM):

A legújabb kapcsolási technika: Egy optikai szálon, több optikai vivőt multiplexel a hullámhosszuk alapján (vagyis különböző hullámhosszú vivőket csinál). A veszteségek miatt periódikusan jel-regenerálókat kell elhelyezni, ahol a regenerálás optikai-elektronikus-optikai átalakítással történik, egyetlen hullámhosszon.

Elvileg kihasználható sáv szélesség: ~25 THz. Hullámhossz-érzékeny (hangolható) eszközökkel a jelek útvonala is megváltoztatható, ez tkp. kapcsolat.

WDM-nél a jel hullámhossza jelenti a forrásra, az útvonalra és a rendeltetési helyre vonatkozó információt.

Kissűrűségű hullámhossz-kapcsolás (Coarse WDM, CWDM):

- Legfeljebb 16 különböző hullámhossz egy szálon
- Hullámhosszak 1310 és 1610 nm között, 20 nm-es térközökkel elválasztva
- A viszonylag nagy térköz miatt egyszerű eszközökkel kezelhető
- Még mindig nem igazán hatékony a szál kihasználtsága

Nagysűrűségű hullámhossz-kapcsolás (Dense WDM, DWDM):

Az erbium-adalékolású optikai erősítő (Erbium-Doped Fiber Amplifier, EDFA) kifejlesztése lehetővé tette, hogy sok, egymáshoz viszonylag közeli hullámhosszú (1.6~0.8 nm térköz) fényt lehessen multiplexálni egyetlen üvegszállra, ez a sűrű WDM.

Optikai keresztkapcsoló (Optical cross-Connect – OXC):

Optikailag kapcsolja valamennyi bejövő szál valamennyi hullámhosszát a kimeneti szálak hullámhosszaira. Ha konvertereket is tartalmaz, akkor a k-adik bemeneti szál X_i hullámhosszát képes az m-edik kimeneti szál X_k hullámhosszára is kapcsolni.

A wavelength routing hálózatok áramkörkapcsolt hálózatok. Egy összeköttetés tulajdonképpen egy hullámhossz hozzárendelését jelenti az összeköttetés útvonalának minden szakaszán („Fényút”). Ha egy OXC kimenetén a továbbítandó hullámhossz foglalt, akkor átkonvertálja néhány nm-rel különböző hullámhosszba a jelet és így továbbítja

4. Hívásvezérlés, Címzés

Hívásvezérlés

A „hívások”(kapcsolatok) létrehozása, fenntartása, lebontása, az ehhez szükséges jelzések rendszere. Hívásvezérlő protokollok (valamely szabvány szerint).

Jelzésrendszerek:

- a hívásokat vezérlő jelzések rendszere
- „sávon belüli” (**in-band**) – belső „előfizetői hurokban”
- „sávon kívüli” (**out-of-band** – külön csatornán/hálózaton) jelzésátvitel
- „közös csatornás” jelzésátvitel - **Common Channel Signaling (CCS)**
- rugalmasság, jobb sávszélesség-kihasználás
- a közös csatornás jelzhálózat üzenet- vagy csomagkapcsolt

ISDN (Integrated Services Digital Network) jelzésrendszerek:

- végpontok közötti átlátszó digitális csatornák
- univerzális interfészek

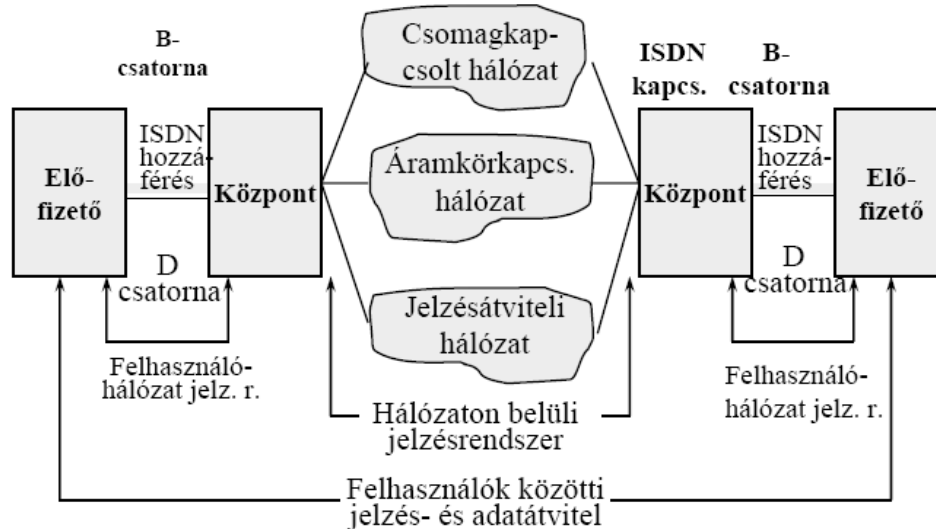
Common Channel Signaling (CCS):

- Közös virtuális/fizikai jelzéscsatornák
- Üzenet- vagy csomagkapcsolt
- Észak-Amerikában különálló csatornaként valósult meg
- felhasználó és hálózat közötti jelzésátvitel: UNI (user-network interface)
- BRI (basic rate interface): 2B+D,
- PRI (primary rate interface): 30B+D
- (B = 64 kbit/s, D = 16, 64 kbit/s)
 - hálózaton belüli jelzésátvitel: No7, CCS7
 - Service Switching Points (SSPs)
 - Signal Transfer Points (STPs)
 - Service Control Points (SCPs)

az ISDN-ben az UNI-n alkalmazott ITU Q.931-es protokoll:

- Call Reference
 - 1-15 byte hosszú egyedi azonosító az ugyanazon D-csat-n folyó hívások megkülönböztetésére
- Message Type
 - 1 byte hosszú, ez mondja meg, h. milyen jelzésüzenet
- Information Elements
 - Az adott jelzésüzenethez szükséges információk

Az ISDN felépítése:



Elnevezés, címzés

Elnevezés: egyedi név hozzárendelése a hálózat végpontjaihoz: diana.create-net.it

Címzés: egyedi cím hozzárendelése a hálózat végpontjaihoz: 213.21.183.196

A nevek kiosztási módjai:

- hierarchikus: magasabbrendű névadó ad prefixet és jogot az az utáni névadásra
- névtér (name space)
- tartományok (domains)

Címek kiosztása:

- a címek is globálisan egyediek
- hierarchikusan célszerű ezeket is szervezni
- A hierarchikus szervezésnek további oka az, hogy a hálózatokban egyszerűbbé tesszik az útvonalválasztást:
 - „lapos”, egyszintű címezésnél minden csomópontban kell útvonalirányító tábla (routingtábla), és abban n-1 bejegyzés
 - hierarchikus címezésnél nem kell mindenhol és mivel alhálózatok alakíthatók ki, csak a határokon kellenek routingtáblák

Névhasználat az Interneten:

- DNS - Domain Name System: név-cím-összerendelések
- IANA - Internet Assigned Names Authority: adminisztrálja a neveket
- ccTLD - country code top-level domains, pl. .hu
- gTLD generic top-level domains():pl. .org, .edu, .net, .com, .gov, .mil
eredetileg: a szervezetek egy-egy csoportja az USA-ban, ma már világszerte csaknem szabadon felhasználható, a .gov és a .mil csak az USA-ban
- itld -infrastructure top-level domains: egy van, az .arpa(megemlítjük később)

Root domain: az üres string a záró pont után: hit.bme.hu.

Top level domains: a név utolsó része (.hu, .org, .gov, .arpa, ...)

Van olyan globális, hierarchikus címzés, amely nem prefix jellegű, ilyen az Ethernet lokális hálózatokban használt címzés

Ethernet-cím: az Ethernet adapter(kártya) egyedi címe: 6 byte

Ebből a gyártó kódja: 3 byte, a másik három az adapteré

Címek aggregálása

Hierarchia nélküli (flat) címzés

- Minden csomópontban kell irányítótábla
- Minden táblában n-1 bejegyzés

Hierarchikus címzés

- Címek csoportosíthatók (c)
- Néhány csomópontban kell irányítótábla • Minden táblában c-1 bejegyzés

Címzés az adatkapcsolati rétegben

- Az eddigiekben kimondtunk, vagy feltételeztük, hogy a címzés, lehetővé teszi a hálózatok közötti útvonalválasztást és a csomagtovábbításhoz szükséges
- Az egyes hálózatokon belül gyakran egy másik szinten is van címzés, pl. lokális hálózatban, pl. az Ethernet LAN-ban a hálózati kártyáknak saját címzésük van
- Tehát többszintű a címzés, címeket kezelünk a hálózati architektúra különböző rétegeiben (később a rétegezett architektúrákat részletesen tárgyaljuk)
- Az Ethernet LAN címzését az IEEE 802.3 szabványa határozza meg
- hierarchikus, de nem prefix tulajdonságú címzés
- 3 byte a gyártót, 3 byte az adapterkártyát jelöli
- később részletesen (55. oldal)

Adatkapcsolati- (hardver) címek keresése

- A DNS leképezi a nevet hálózati címre, ez egyértelműen azonosítja a végpontot
- Ha azonban a végpont egy LAN-on van, az csak pl. Ethernet-címet ért meg
- Ezért a célponthoz legközelebbi hálózati csomópontnak (routernek) le kell fordítania a hálózati címet hardver-(Ethernet)címre, és azt a csomaghoz kell csatolnia a továbbításhoz
- Szimmetrikusan: ha a LAN-végpont küld egy csomagot kifelé, tehát a routeren keresztül, akkor a router LAN-címét kell használnia
- Az IP-ben ezeket az átalakításokat az ARP (Address Resolution Protocol) és a RARP (reverse ARP) végzi,
- lásd később (66. oldal)

Telefonhálózat címzési rendszere

E.164-es telefonszám:

- .1 CC –countrycode(1...3 számjegy)
- .2 NDC –nationaldestinationcode(opcionális)
- .3 SN –subscribernumber
- .4 NDC+SN=15-CC

általában a „+” prefix-szel írjuk, ami a nemzetközi elválasztást jelenti, pl. „00”, vagy „011” általában valamilyen elválasztót használunk a CC után és a szám további részében a körzetszám elválasztására (a szabvány szerint az elválasztó a szóköz!)

ENUM (Telephone Number Mapping):

Lehetővé teszi, hogy az Internet domain név rendszerét (DNS), mint egy világméretű elosztott adatbázist felhasználva valamely E.164(telefonhálózati) szabvány szerinti telefonszámhoz internetes és hagyományos távközlési szolgáltatásokat rendeljünk, és azt a telefonszám alapján elérjük. Átváltás:

Telefonszám fordítva, pontokkal elválasztva, végére .e164.arpa

+36-30-595-1329 → 9.2.3.1.5.9.5.0.3.6.3.e164.arpa

Címzés az interneten:

IP-címek (jelenleg Ipv4) 0.0.0.0 – 255.255.255.255

A osztályú címek: 0-val kezdődik 8+24

B osztályú címek: 10-gyel kezdődik 16+16

C osztályú címek: 110-val kezdődik 24+8

Dinamikus hoszt-konfigurálás (Dynamic Host Configuration Protocol - DHCP):

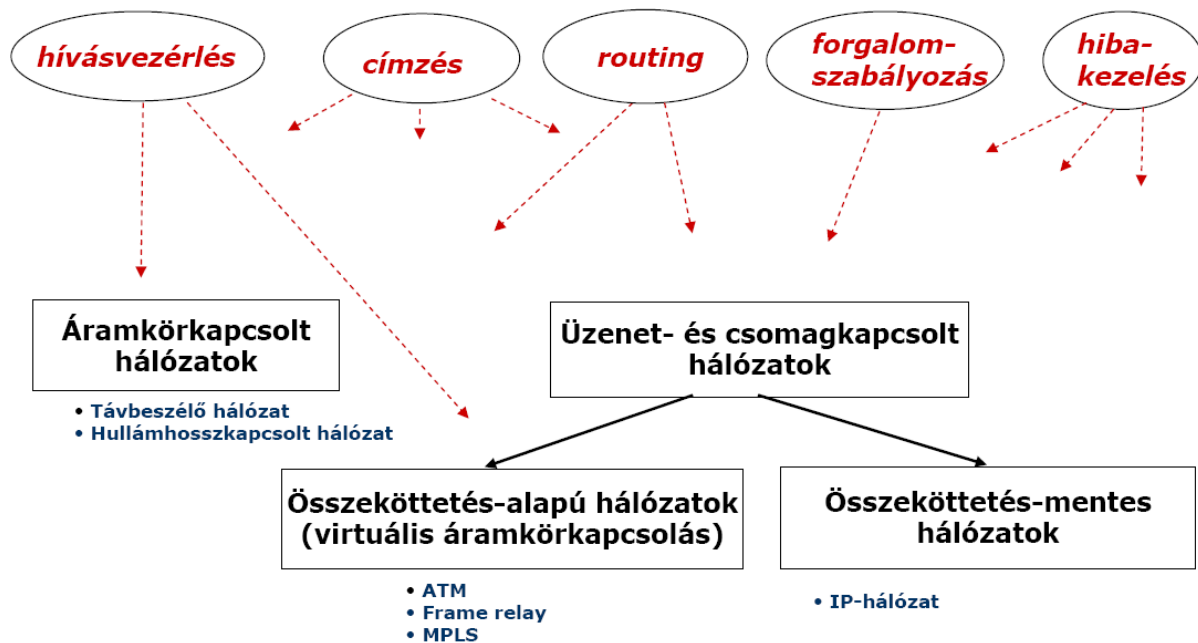
Dinamikus IP-cím allokálás végpontoknak. A végpontnak gyakran csak akkor van szüksége IP-címre, amikor aktív, és nem kell, hogy mindig ugyanaz legyen → ugyanaz az IP-cím több végpont között megosztható, ha azok nem egyszerre aktívak. Az újonnan bekapcsolódó végpont IP-címet kér (és jó esetben kap) egy DHCP szervertől, ami DHCP protokollal végzi az allokálást (pl DSL)

Névfeloldás – name resolution:

Az Interneten a hierarchikus név- és címrendszer felhasználásával a DNS -Domain Name System végzi. Elvileg először a rootnak megy a kérés, az továbbítja az aktuális tartományba, az azt kezelő névszervernek.

5. Routing

A hálózati réteg fő feladata, hogy a csomagokat a forrásgéptől a célgépig irányítsa. A legtöbb hálózatban a csomagoknak ehhez több routeren kell keresztülhaladni, több átugrást kell megtenni. Az útválasztás (routing) az a művelet, amelynek során a rendszer egy helyi hálózat valamely számítógépétől az adatcsomagokat különböző vonalszakaszokon keresztül eljuttatja azokhoz a címzettekhez is, amelyek nem részei a helyi hálózatnak.



Az összeköttetés alapú útvonalkijelölés, összeköttetésmentes útvonalválasztás csomópontok táblázatai alapján történnek, melyek tartalmazzák egy célponthoz éréshez szükséges következő lépést (tágabb értelemben idetartozik a továbbítás is).

Feladat:

- Kitöltés adaptív módon (nincs globális kép nagy hálózatok esetén)
- Algoritmusok, protokollok megalkotása
- Megismerni és nyilvántartani a hálózat felépítését
- Biztosítani a csomópontok számára az útvonalválasztáshoz szükséges információt
- Összeköttetés alapú: lépésről lépésre választunk csomópontot, dedikált (virtuális) csatornákon. A csomópontok megjegyzik az útvonalinformációt.
- Összeköttetés-mentes: nincs előre kialakított útvonal, minden csomópont választ útvonalat. Minden csomagra újra elvégzik az útvonalirányítást

Útvonaltábla:

- cél-végpont
- következő csomópont

Ennek kitöltése történhet

- manuálisan
- automatikusan:
 - **centralizáltan**: egy ponton összegyűjtjük a hálózatról megszerezhető valamennyi ismeretet, majd meghatározzuk az egyes csomópontok útvonaltábláinak bejegyzéseit, és továbbítjuk azokat a csomópontokhoz. (telefonhálózatok)
 - **elosztottan**: mindenki egyénileg gyűjtöget és készít táblát (nem garantált az egységes kép) (számítógép-hálózatok)

Két eltérő koncepció az útvonal-adatbázis kialakítására:

A tapasztalatok alapján előre becsült forgalmi viszonyoknak megfelelő útvonaltáblák centralizált kialakítása és szétosztása (telefonhálózat)

Statikus eset

Az aktuális forgalmi helyzet állandó figyelése, az annak legjobban megfelelő útvonaltáblák kialakítása (adathálózat)

Dinamikus eset, pl számítógép hálók

Információgyűjtés:

- csomópontok, végpontok, linkek
- topológiai információk
- várakozási sor
- terhelés
- kiszolgálási díj

Követelmények (minél kisebb útvonaltáblát adjon, mert):

- Kisebb tár, olcsóbb csomópont
- Gyorsan működő csomópont kis keresőtáblával
- Kis routing forgalom
- Robusztusság a hibás tábla esélyének minimalizálására
- Optimális útvonal kijelölése igénytől függően

Megoldások csoportosításra:

- | | | |
|-------------------------------|---|-------------------|
| • Centralizált - | - | Szétosztott |
| • Tényleges forgalomtól függő | - | Forgalomfüggetlen |
| • Egyutas | - | Többutas |
| • Lépésenkénti | - | Forrás általi |

Elosztott Routing:

Az útvonal táblák kialakítását végezzék maguk a csomópontok.
Valójában nem információ gyűjtés, hanem terítés történik

Két alapvető módszer ismert:

Távolság-vektor (distance-vector) - Bellman-Ford algoritmus:

□ Példa:

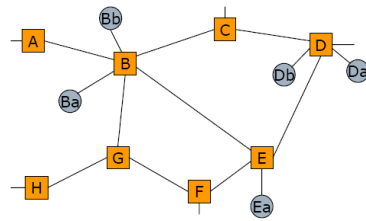
A	B,1				
B	A,1	C,1	E,1	G,1	∞
C	B,1	D,1			
D	C,1	E,1			
E	B,1	D,1	F,1		

B-hez megérkezik
C üzenete:

B	A,1	C,1	D,2	E,1	G,1	∞
C	B,1	D,1				

B-hez megérkezik
E üzenete:

B	A,1	C,1	D,2	E,1	F,2	G,1	∞
E	B,1	D,1	F,1				

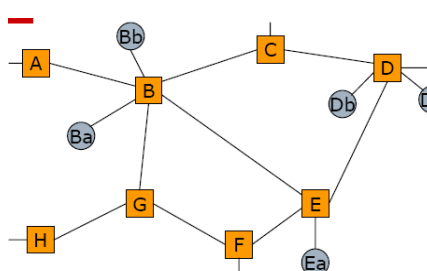


A csomópontok elmondják a hálózatról alkotott elképzeléseiket a szomszédaiknak.

Alapja, hogy minden routernek egy táblázatot (vagyis egy vektort) kell karban tartania, amelyben minden célhoz szerepel a legrövidebb ismert távolság, és annak a vonalnak az azonosítója, amelyiken a célhoz lehet eljutni. A táblázatokat a szomszédokkal való információcsere útján frissítik.

A távolság-vektor módszer alapproblémája a végtelenig számolás. Ha A-B-C pontokat vesszük, A-B = 1, B-C = 1, A-(B)-C = 2. Ha B-C összekötés megszakad, (B,C) távolsága ∞ . Amint A és B (mint szomszédok) információt cserélnek, A-(B)-C ∞ lesz, de B-C 3 lesz, mert A-(B)-C az információcsere pillanatában még 2 volt. Javítás: kiegészítő információ, hogy melyik csomóponton keresztül érvényes a távolság.

	C táv	Köv. lépés
A	2	B
B	1	C
A	2	B
B	∞	-
A	∞	-
B	3	A
A	4	B
B	∞	-



C	B	2
C	D	1
D	C	2
D	E	1
E	B	2
E	D	1
E	F	1

Összekötés-állapot (Link-state) módszer – Dijkstra algoritmus:

A csomópontok elmondják mindenkinek a szomszédaikról nyert tapasztalataikat.

A „tapasztalatok”: a szomszédokhoz vezető linkek aktuális állapota (ez pontosan ismerhető).

Ennek a módszernek a neve elárasztás (flooding), amelyben minden bejövő csomagot minden kimenő vonalon kiküldünk, kivéve azon, amelyiken beérkezett. Az elárasztás nyilván nagyszámú kettőzött csomagot eredményez. Ennek elkerülésére módszer, hogy legyen minden csomag fejrészében egy ugrásszámláló, amely minden ugráskor csökken eggyel, és ha eléri a nullát, a csomagot eldobjuk. Ideális esetben az ugrásszámláló kezdeti értékének a forrástól a célig vezető út hosszát kell beállítani. Ha a küldő nem tudja, hogy milyen hosszú az út, beállítja a legrosszabb esetre, nevezetesen az alhálózat teljes átmérőjére.

Hierarchikus routing:

Ha egy hálózatnak N csomópontja és E összekötése van, akkor kimutatható:

A legrövidebb út számítása: $O(E \log E)$

Az útvonal tábla mérete: $O(N)$

# csomópont	Tábla-hely	Számítási idő
1	1	$O(1)$
1.000	1.000	$O(3.000)$
1.000.000	1.000.000	$O(6.000.000)$
100.000.000	100.000.000	$O(800.000.000)$
10.000.000.000	10.000.000.000	$O(100 \text{ millárd})$

Ahogy a hálózat mérete nő, a routerek forgalomirányító táblázatai is arányosan nőnek. Nemcsak a routerek memóriáját fogyasztják az egyre növekvő táblázatok, hanem több CPU időre is van szükség az átvizsgálásukhoz, és nagyobb sávszélesség szükséges ahhoz, hogy elküldjük ezek állapotjelentéseit. Ha a hálózat akkorára nő, hogy már nem lehetséges minden egyes routerben minden más router számára egy bejegyzést fenntartani, akkor a forgalomirányítást hierarchikusan kell elvégezni, ekkor a routereket tartományokra osztjuk.

Az autonóm rendszer (AS):

- olyan egység, amelyen belül egységes routing policy érvényesül
- egyetlen hálózat, vagy hálózatok csoportja
- közös hálózataadminisztrátor (vagy azok csoportja) kezeli
- egyetlen szervezeti egység (pl. egyetem, üzleti vállalkozás) megbízásából
- az egész csoport egyetlen bejegyzés lesz az útvonal-táblában

Kiegészítések szükségesek:

- Mobil végpontokat megengedő routing
 - A végpontok más csomópontok közelébe vándorolhatnak
 - A mobil routing feladata nyomon követni a pontot
 - Kiegészítések: Home Agent/Foreign Agent
- Multicast routing (konferencia bezélgetés)
 - Egyidejűleg több címre juttatjuk el a csomagot
 - Megoldandó feladatok:
 - Címzés
 - Csoportkezelés
 - Útválasztás segítése
 - Egy csoportot egy logikai címhez hasonló azonosító azonosít
 - Sűrű elhelyezkedés: Elárasztás + Lemondás:
 - Legrövidebb útvonalfa alkalmazása
 - Csoportlemondás
 - Forráslemondás
 - forráslemondás
 - Ritka elhelyezkedés: Explicit csatlakozás
 - Gerinc fa alkalmazása
 - Elhelyezkedés független: a kettő ötvözte

6. Feladatütemezés, csomagkezelés

Több területen is megjelenő problémára megoldás. Sokszor van véges erőforrással dolgunk amelyet időnként nagyobb mértékben kellene igénybe venni, mint amekkorára az képes, máskor viszont nincs eléggé leterhelve, viszont igaz, hogy hosszú idejű átlagban képes az igények kiszolgálására. Milyen elvek, stratégiák alapján képezzünk sort, sorokat a várakozókból, ahhoz, hogy adott kiszolgálási feltételek, elvárások a lehető legjobban teljesüljenek?

Egy hálózati csomópontban várakozás fennállhat

- a linkek átviteli képessége
- a csomópontok tárolási képessége (tárolás, sorbaállítás, átrendezés)
- a csomópontok feldolgozási képessége miatt

Feltételezzük, hogy nagyszámú igény adja össze a teljes igénybevételt és azok általában kiegyenlítik egymást, eltekintve kilógó esetekről, amelyekre jó becslést lehet adni, ez a **statisztikus multiplexelés**.

Így jobban járunk, mintha a csúcsra méreteznénk (és általában az igények is), ez a **statisztikus nyereség**.

A triviális ütemezés az FCFS (puffer). Sok esetben ez nem elég. Legalább kétféle alkalmazást kell kiszolgálni.

- **Rugalmas** (elasztikus) vagy késleltetés-tűrő: elviselik a véges és változó ábocsátóképességet, pl. file-átvitel. Igényei:
 - Igazságos
 - Best-effort (legjobb szándékú)
- **Merev, vagy intoleráns**: garantált szolgáltatást igényelnek, pl. beszéd: állandó 64 kbit/s-os csatornát. Igényei:
 - korlát a késleltetésre, garantált átviteli sebesség, korlát a veszteségi arányra
 - garantált szolgáltatásra

Megőrzési törvény (Conservation Law):

Az átlagos késleltetések forgalom-részaránnyal súlyozott összege = konstans. $\sum_1^N p_i q_i =$

konstans. Valakinek előnyt csak mások rovására lehet biztosítani.

Alapvető követelmények:

Egyszerű megvalósíthatóság (mindkét esetben):

Nagysebességű hálózatokban gyakori csomagtovábbítás, csomagonként csak néhány műveletre van lehetőség. Ezeket lehetőleg hardverben lehessen megvalósítani

Ha N a kiszorgálandó összeköttetések száma: A csomagonkénti feldolgozási időigény ne exponenciálisan, hanem lineárisan nőjön N függvényében.

Elsődleges korlát az állapotok nyilvántartásához szükséges memória és elérési idő.

Igazságosság (fairness) és védelem (protection) biztosítása („best effort” kiszorgálásnál):

Bármely ütemezési módszer valamilyen módon elosztja az erőforrásokat. Alapvető követelmény, hogy ez igazságos legyen: A részesedés a költség-viselés arányában történjen. Amennyiben valaki megkísérel jogosulatlan előnyhöz jutni, legyen megakadályozva, védve a többiek.

Teljesítménykorlátok (performance bounds) biztosítása (garantált kiszorgálásnál)

Gyakori eset: egyenlő jogosultságok, de vannak, amelyek igénye kisebb a többiekénél. A „kis” felhasználóknak adjuk oda, amennyit akarnak, a fennmaradót osszuk szét igazságosan a nagyok között. Ez a max-min igazságos megosztás elve (**max-min algoritmus**):

- Erőforrás-kiosztás a növekvő igények szerint
- Senki sem kap többet a kértnél
- A kielégítetlen igények egyenlően osztoznak a maradékon

Példa: 4 forrás, 2, 2.6, 4, 5, igényekkel, 10 kapacitású erőforrással.

1. lépés: mindenki 2,5.

A 2 miatt maradó 0,5-öt egyenlően elosztjuk a 3 között, ez 2.66-ot ad, a 2.6 miatt maradó 0.06-ot a 2 között, végül az 1-es 2-t, a 2-es 2,6-ot, a 3-as és 4-es 2,7-et kap

Van még: Súlyozott max-min. Súlyaik arányában szétosztjuk, és utána osztjuk vissza a felesleget.

Például 15 egységnyi erőforrásra 5 pályázó

Jogosultságaik aránya

Igényeik:

Normalizált súlyok:

Az E kivételével mindenki elégedetlen:

Szétosztjuk súlyaik

arányában, D is OK:

A	B	C	D	E
1/15	2/15	3/15	4/15	5/15
2	4	7	5	2
1	2	3	4	5

+3

$$1,3+2,6+3,9+5,2+2=15$$

$$+0,2$$

Ez még szétosztható

Teljesítménykorlátok:

Akár felhasználónként kiszolgálási teljesítménykorlát garantálása (a megőrzési törvényen belül), szerződéssel a felhasználó és szolgáltató között. Egyrészt kiszolgálási garancia, másrészt használati kötelezettség-vállalás.

Fajtái:

- **Determinisztikus:** Az összeköttetés valamennyi csomagjára teljesülnie kell. Egyszerű ellenőrzés, de rossz kihasználtság.
- **Statisztikus:** A csomagok adott hányadára teljesül N egymásutáni csomagból egyre nem teljesül. Bonyolult ellenőrzés, de jó kihasználtság

Szolgáltatási minőség-paraméterek (Quality of Service - **QoS**):

- **Sávszélesség**
 - garantált minimális sávszélesség az összeköttetésre
- **Késleltetés**
 - Legrosszabb eset
 - minden más összeköttetés a lehető legrosszabbul „viselkedik”
 - Átlagos érték
 - elvileg a minden további összeköttetés lehetséges forgalmi viszonyoknak a halmazára kellene átlagolni, ez lehetetlen, ezért az adott összeköttetés csomagjainak késleltetését átlagoljuk
 - Csomagok adott hányadára vonatkozó jellemző
 - pl. a csomagok 99%-a kisebb késleltetésű lesz, mint a 99-percentilis késleltetésérték
- **Késleltetés-ingadozás**
 - kiegyenlítési lehetőség a vevőben, de nem lehet akármekkora
- **Csomagvesztés**

Megj.: Legrosszabb eset és az átlagolás a többi jellemzőnél is!

Egyszerű és hatékony beengedésszabályozás (garantált kiszolgálásnál):

A teljesítménykorlátok (QoS paraméterek) csak beengedés-szabályozás (admission control) alkalmazásával biztosíthatók. Gyorsan kell eldönteni, hogy újabb igény még kiszolgálható-e. Nem eredményezheti azt, hogy a hálózat nem lesz kihasználva a lehetséges mértékben.

Négy alapvető választási lehetőségünk van a tervezésnél:

Prioritási szintek száma:

n szint esetén a k-adik szintű igényt akkor elégíti ki csak az ütemező, ha nincs nála nagyobb prioritású igény.

Magas prioritás = kisebb késleltetés

- Egyszerű a megvalósítása
- Jól számolható a teljesítőképessége
- Probléma: „kiéhezteti” az alacsonyabb szintűeket
- Megoldás: megfelelő beengedés-szabályozás (ill. öregítés)

Az egyes szinteken munkamegőrző (work-conserving) vagy nem munkamegőrző (non work-conserving) módot használjunk-e?:

Work-conserving: csak akkor üres a kiszolgáló, ha nincs várakozó igény (csomag)

Non-work-conserving: vannak üres időszakai akkor is, ha van várakozó igény

- A kivárási előnyös lehet a forgalmi jellemzőkre
- Csak az „esedékessé” váló csomagokat továbbítjuk – pl „rate descriptor” alapján
 - Csökken a tároló iránti igény
 - Csökken a késleltetés-ingadozás
 - Egyszerűsödik a vállalható teljesítmény-korlát meghatározása
- korrekt forgalomjellemezést kíván meg a forrásoktól, és azt, hogy ahhoz tartsák is magukat
- ellenérv: csak a késleltetésingadozást küszöböli ki, azt viszont a vevőben is megtehetjük <-> a kapcsolók tárigényét is csökkenti
- a késleltetés ingadozást az átlagos késleltetés megnövelése árán csökkenti <-> a vevőpuffer is, de sok alkalmazásnál ez kevésbé kritikus
- viszont korrekt forgalomjellemezést kíván meg a forrásoktól, és azt, hogy ahhoz tartsák is magukat

Igények csoportosítási (aggregálási) mértéke az egyes szinteken belül:

Két véglet:

- valamennyi igény együttes jellemzése - ugyanazt a szolgáltatásminőséget kapják
- minden egyes összeköttetésre saját QoS biztosítása - Csomagkapcsolt hálózaton technikailag nem lehet erőforrással győzni az egyedi igények kezelését, szemben a telefonhálózattal, ahol azonosak az igények.

Közbenső eset: osztályokba sorolás: az adott osztályba sorolt összeköttetések ugyanazt a szolgáltatásminőséget kapják („együtt sírnak, együtt nevetnek”) → a csoportosításból következik, hogy nincsenek védve egymástól. „Csalás” esetén az egész csoport bűnhődik

Kiszolgálási sorrend az egyes szinteken belül:

FCFS hátrányai:

- Nincs prioritás
- Nem biztosít védelmet, nem max-min elvű
- Erőszakosságra ösztönöz

GPS - Generalized Processor Sharing:

A max-min igazságosság megvalósítása. Alapelv: úgy lehetne igazságosan megosztani az erőforrást, ha sorban mindenkinek egy 0-hoz tartóan kicsiny elemi „szeletét” végeznék el a feladatából. Elvileg megoldjuk a GPS-szel az igazságos kiszolgálás problémáját, gyakorlatban közelítő-GPS.

Mindenki egymás után kap egy parányi kiszolgálást, majd „körben” folytatódik. Akinek nincs igénye az kimarad. Különböző jogosultságok esetén a nullához tartóan kis kiszolgálás a súlyok arányában különböző lesz. Kimutatható, hogy a GPS max-min értelemben fair kiszolgálást nyújt.

Közelítő megvalósítása:

Súlyozott körbekérdezés (Weighted-Round-Robin - WRR)

Egy körben a prioritásnak megfelelő egész számú darab csomagot fogad egy kapcsolattól.

Jó, ha azonos csomaghosszak és azonos súlyú összeköttetések mellett, a kiszolgálási körben csomagonként különböző súlyokkal, különböző csomaghosszakkal érkeznek az adatok.

Átlagos csomaghossz jó közelítésű ismerete kell.

Példa: három összeköttetés A, B, C

	átlagos csomaghossz byte-ban	súly	súly/csmghossz	egészre normálva(×6000)	byte-ban
A	50	0.5	1/100	60 csomag/round	3000
B	500	0.75	3/2000	9 csomag/round	4500
C	1500	1	1/1500	4 csomag/round	6000

Deficit round-robin:

A WRR fejlesztett változata, előre ismeretlen átlagos csomaghosszra.

Definiálunk

- egy kiszolgálási adagot, kvantumot (byte-okban mérve)
- egy számlálót, amely a felhasználó 'hitelét' számolja (deficit counter), kezdeti értéke 0

A sor elején álló csomagot akkor szolgáljuk ki, ha annak mérete nem nagyobb, mint a kvantum. Ekkor a kapcsolat DC-je kvantum-csomaghossz lesz. Ha nagyobb, az adagot hozzáadjuk a számlálóhoz és a következő körben ennek vizsgálata alapján döntünk. Ha egy kapcsolatnak nincs csomagja DC = 0.

Példa:

	A	B	C	Kvantum: 100
Csomaghossz	150	80	120	
Deficit-counter 1.kör	100	20	100	
Deficit-counter 2.kör	50	0	80	
Deficit-counter 3.kör	0	0	0	

WFQ - Weighted Fair Queueing vagy PGPS - Packet-by-packet GPS:

Alapötlet: kiszámítjuk (szimuláljuk) a csomagok távozási időpontjait, mintha GPS szerint szolgáltuk volna ki azokat, és ezt a **sorrendet**(vagyis nem az időpontját) alkalmazzuk a kiszolgálásra. Ez a távozási jellemző érték a befejezési szám.

Legyen bitenkénti kiszolgálás

Ciklusszám (round number) - pozitív valós szám

Ciklushossz: arányos az aktív felhasználók számával

Ha ismerjük a ciklusszámot, a befejezési szám kiszámolható:

$$F(i, k, t) = \max[F(i, k - 1, t), R(t)] + P(i, k, t)$$

- $F(i, k, t)$ - az i-edik felhasználó k-adik csomagjának befejezési száma t időpontban
- $P(i, k, t)$ - az i-edik felhasználó k-adik csomagjának átviteli ideje t időpontban, i sávzélességén
- $R(t)$ - ciklusszám a t-ben

Inaktív felhasználónál a befejezési szám:

- az aktuális ciklusszám plusz a csomagméret
- pl. ha egy 10 bites csomag érkezik, amikor a ciklusszám 3, a kiszolgálása akkor befejeződik be amikor a ciklusszám 13 lesz

Aktív felhasználó csomagja beérkezésekor annak befejezési száma:

- A sorában lévő csomagok közül a legnagyobb befejezési számú plusz a csomagméret
- pl. ha a 10 bites csomag beérkezésekor a sorban van egy 20-as befejezési számú, akkor 30 lesz

Kombinálva ezt a két állítást jön ki a fenti összefüggés $F(i,k,t)$ -re

Súlyozott WFQ:

$$F(i,k,t) = \max[F(i,k-1,t), R(t)] + P(i,k,t) / w(i)$$

Ahol $w(i)$ az i -edik kapcsolat súlya

- Az aktuális ciklusszám meghatározása jelent gondot
- Egyre általánosabban használt korszerű routerekben

További módszerek:

- Virtuális óra
- Legkorábban esedékes (Earliest-Due-Date - EDD)
- Sebesség vezérelt

Csomageldobás

Nem csak a kiszolgálási sorrendről, hanem a tárolhatatlan csomagok kezeléséről is dönteni kell

Milyen alapon működjön a csomageldobási stratégia?

- Csoportosítás (aggregálás): összeköttetésenként, vagy csoportonként?
- Eldobási prioritások... mikor dobjunk el csomagot?
- Korai eldobási stratégiák (Early Random Drop, Random Early Detection)

7. Forgalom Szabályozás (Flow Control)

Fontos tervezési kérdés, amely megjelenik az adatkapcsolati rétegben az, hogy mit tegyünk azzal az állomással, amelyik rendszeresen gyorsabban akarja adni a kereteket, mint a vevő azokat fogadni tudná. Az adó folyamatosan pumpálja kifelé a kereteket egészen addig, míg a vevőt teljesen el nem árasztja. Még ha az átvitel hibamentes is, a vevő egy bizonyos ponttól kezdve nem lesz képes kezelni a folyamatosan érkező kereteket, és néhányat el fog veszíteni.

Forgalomszabályozás: Módszerek, amelyek lehetővé teszik, hogy egy adatforrás az aktuális átviteli sebességét illessze a vevőnél és a hálózatban rendelkezésre álló kiszolgálási sebességhez.

Torlódásvezérlés (congestion control): Azok a módszerek, amelyekkel linkek, csomópontok időszakos túlterheltségét megkíséreljük megszüntetni, avagy azok a módszerek, amelyekkel meg is lehet előzni a torlódásokat.

Ebben az értelemben a flow control tekinthető a congestion control eszközének (előzzük meg a torlódást, mielőtt az bekövetkezne)

Két jelentős forgalomszabályozási fajta:

Nyílthurkú (vezérlés):

A kommunikáció előtt a felhasználó és a hálózat forgalmi paramétereit egyeztet.

A hálózat dönt az új összeköttetés elfogadásáról.

Ennek megfelelően a hálózat erőforrásokat dedikál, a működés során paraméter-ellenőrzés.

Forgalomleírók (traffic descriptors): Egy paraméterkészlet, amely jellemzi az adatforrás viselkedését. Bemenő adatok:

- forgalomszabályzó (**regulator**) - tipikusan késlelteti a túlzott forgalmat
- felügyelő (**policer**) - inkább eltávolítja azt.

Követelmények a forgalomleírókkal szemben:

„Megjelenítési képesség” (representativity): képesek legyenek a forgalmat hosszútávon megjeleníteni → megfelelő mennyiségű erőforrás fenntartása

Ellenőrizhetőség (verifiability): A hálózat legyen képes olcsón, és gyorsan ellenőrizni a forgalom „megfelelőségét”

Megőrizhetőség (preservability): Az út mentén való megőrizhetőség

Használhatóság (usability): A felhasználó képes legyen megmondani, a hálózat képes legyen mérlegelni

Zárthurkú szabályozás:

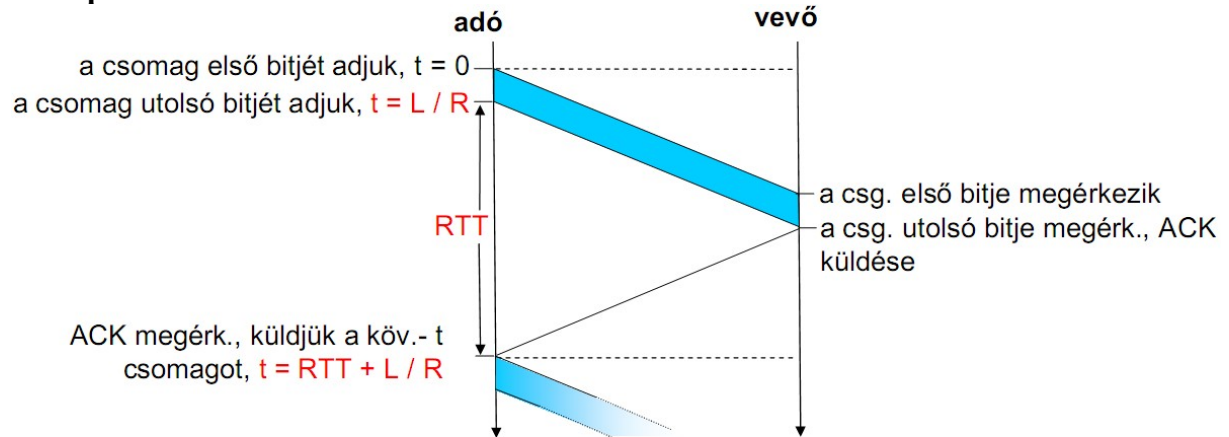
Feltétlenül szükséges, ha

- nincs erőforrásfoglalás
- túlfoglalást (overbooking) alkalmazunk

Módszerek (nyelő oldali):

- On-off: a nyelő engedélyezi az adást
- Stop-and-wait: a küldő egy csomag után vár a nyugtára
- Statikus ablak: a küldő az ablak méretével megadott számú csomag elküldése után vár csak nyugtára. Az adónak lehet több, adásban lévő, még nem nyugtázott csomagja
 - sorszámozásra van szükség
 - tárolásra van szükség az adóban

A Stop-and-Wait működése:



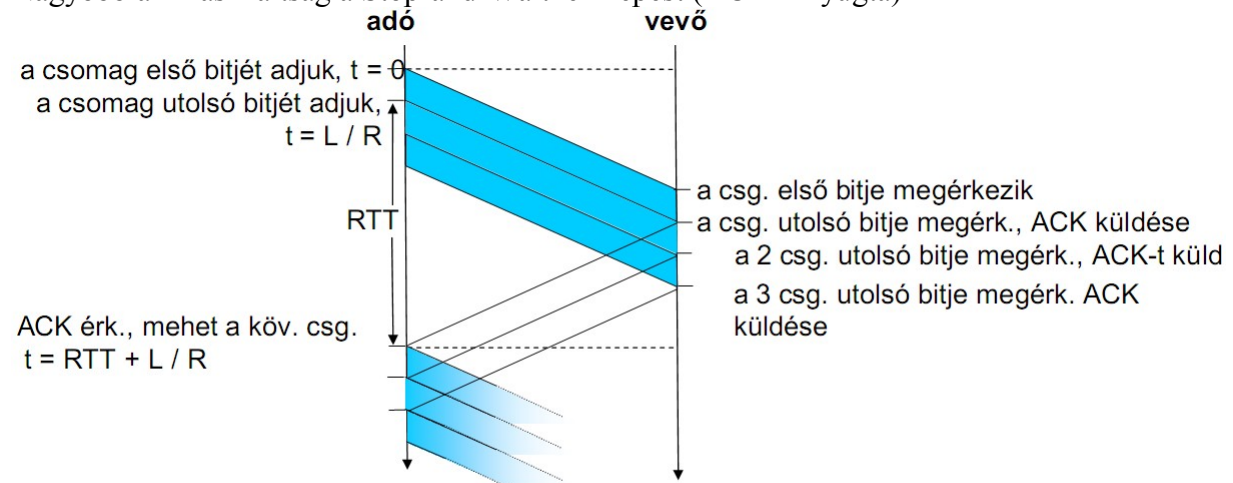
A kihasználtság:
$$U = \frac{L/R}{RTT + L/R}$$

Statikus ablak működése:

Az adónak lehet több, adásban lévő, még nem nyugtázott csomagja

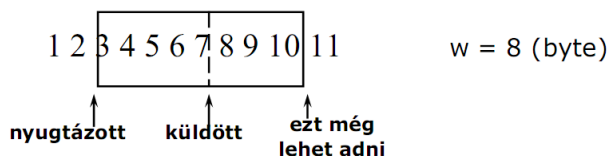
- sorszámozásra van szükség
- tárolásra van szükség az adóban

Nagyobb a kihasználtság a Stop-and-Waithez képest (ACK = nyugta)



$$U_{\text{sender}} = \frac{3 * L/R}{RTT + L/R}$$

Csúzóablakos frogalomszabályozás:



Teljes terjedési időhöz kötik az ablakméretet

8. Hibakezelés (Error Control)

A hibakezelés az a folyamat, amellyel a bármelyik szinten jelentkező hiba észlelhető és javítható.

Bithiba kezelése

Bithiba:

A végpontok közötti (end-to-end) átvitel során két szinten történhet hiba:

- bithiba: $0 \rightarrow 1$, $1 \rightarrow 0$ (törlési hiba)

Bithibák okai: Az információt a fizikai közegen valamilyen jel állapotának (pl. feszültségének, frekvenciájának, fázisának, intenzitásának) megváltoztatásával továbbítjuk. A vételi oldalon a jel értékét előre meghatározott referenciákkal összehasonlítva nyerjük vissza az információt, a vett jel ugyanakkor csak ideális átvitel esetén egyezik meg pontosan valamelyik referenciával.

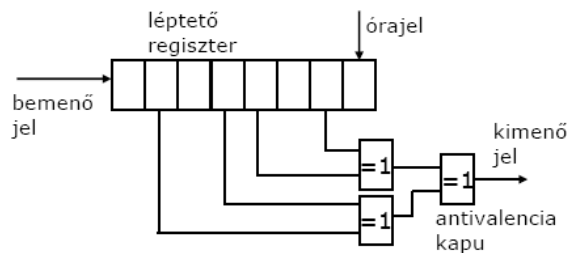
Negatív hatások: zajok, zavarok, csillapítás, jelalaktorzulás

- „véletlen zaj”: tipikusan a termikus zaj ilyen. Egymástól független bithibákat okoz
- impulzus zaj: tipikus forrásai erősáramú berendezések, amelyek pl. szikrákat bocsátanak ki. Hibacsomókat okoz.

Hibák a szinkron elvesztése miatt: A vevő periódikusan mintavételezi a vett analóg jelet, tipikusan jelátmeneteket keres. Ha a vett jelben túl kevés az átmenet, az előállított órajel elcsúszik az adó órajeléhez képest, így a vevő nem a megfelelő időpontban mintavételez, ez hibacsomósodást okoz.

Ennek megoldásai:

- Kódolási technikák (pl. Manchester-kód)
- Bitkeverés (Scrambling):



- a bemeneti adatot egy léptetőregiszterbe léptetjük be
- a regiszter különböző mélységű bitjeiről adatokat csatolunk ki, ezek kizáró vagy kapcsolata lesz az adó kimeneti jele
- a vételi oldalon egy azonos felépítésű áramkörrel állítjuk vissza az eredeti adatokat

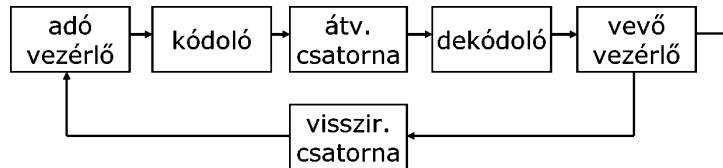
Bithibák mobil rádióhálózatokban

- Cellás mobil rádióhálózatokban a cellaváltás és elhalkulás hibálöketeket eredményez
- a cellaváltás tipikusan mintegy 150 ms időtartamú, ezalatt a vett jel szinte teljes egészében hibás
- ez megelőzhető, ha előbb létrehozunk az új kapcsolatot és csak azután bontjuk a régit, de ez rontja a frekvenciák kihasználtságát
- A vezeték nélküli átvitel során a terjedés útjában lévő közeg jelerősség-csökkenést okoz, a különböző tereptárgyak visszaverődést okoznak
- ezek összefoglaló neve „fading”, hatása különböző struktúrájú bithibák

Hibajavítási stratégiák:

Visszirányú hibajavítás (Backward Error Correction - BEC), más néven automatikus ismétléskérés (**Automatic Repeat Request, ARQ**):

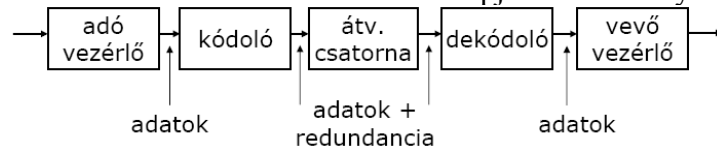
Automatikus ismétléskérés esetén a vevő észleli a hibát és ismétlést kér az adótól



Az adatcsomagokat a küldő hibafelfedő kódolással (**error-detecting code**) kódolja. A vevő dekódolja a vett csomagokat. Minden hibásnak talált csomagot eldob és a visszirányú csatornán kéri újbóli elküldését.

Megelőző hibajavítás (Forward Error Correction, FEC) ~ hibajavító kódolás:

Megelőző hibajavítás esetén a hiba a vett információ alapján a vétel helyén kijavítható.



A kódoló az adatokat redundáns információval egészíti ki, ez a hibafelfedést, hibajavítást szolgálja. A dekódoló dekódolja a vett információt, megállapítja hogy történt-e hiba, és javítja, ha igen.

- Az eljárás gyors, hatékony, nem igényli az adó és a vevő együttműködését.
- Hátránya, hogy a redundáns kiegészítés mérete jelentős, az adatok méretével összehasonlítható lehet

Mindkét módszer alapja redundáns információ továbbítása a tényleges adatokkal együtt, a hiba észlelése/javítása céljából.

Csomaghibák kezelése

Csomaghibák kezelésére kihasználják a bit- valamint a csomagszintű hibadetektálás módszereit, hogy a vevőnél azonosítsák és figyelmen kívül hagyják a hibás csomagokat, vagy megismételtessék azokat az adóval.

Csomaghiba oka lehet:

Csomagvesztés:

- A javíthatatlan (mert sokszoros, burst-ös) bithibák miatti csomagvesztés a vezeték nélküli hálózatokban gyakori (akár 40%-os is lehet).
- Vezetékes hálózatokban a csomagvesztés oka inkább a hálózati csomópontok időleges túlterhelése.
 - kiegyenlített terhelés esetén a túlterhelés ritka, a csomagvesztés aránya alacsony
 - ingadozó, lökésszerű terhelés esetén a csomagvesztés aránya növekedik

Csomagtöbbszöröződés:

A csomagok ismételt elküldése a csomagvesztés gyakori ellenszere. Az adó a csomag elküldése után bizonyos ideig várakozik a vétel nyugtázására, és ha az nem érkezik meg, ismét elküldi a csomagot. Lehet, hogy a csomag már először is hibátlanul megérkezett, csak erről az adó nem értesült, mert

- a nyugta elveszett, vagy
- csak a várakozási idő letelte után érkezik meg

Helytelen csomagsorrend:

- Ugyanazon kapcsolathoz tartozó csomagok sorrendje felborulhat, ha azok különböző útvonalakon érkeznek a vevőhöz.
- Csomagbeszúrás történhet akkor, amikor a csomag fejrésze észlelhetetlenül hibásodik meg:

Csomaghibák észlelése: **sorszámozás**

A küldő minden csomag fejrészébe beilleszt egy csomagonként növekvő sorszámot, ennek segítségével felismerjük az átszortrendeződést és a csomagtöbbszöröződést, a csomagvesztés hézagként jelentkezik a sorszámokban, a csomagbeszúrás is jelezni lehet

A csomagok sorszámai korlátos méretűek, ezért kellően sok csomag továbbítása esetén körülfordulhatnak.

A sorszám a csomag fejrészenek része, mérete -különösen rövid csomagok esetén- kihat az átviteli kapacitás kihasználtságára. A sorszám n -nel jelölt hosszát (bitekben) befolyásolja:

- a csomag maximális élettartama (Maximum Packet Lifetime, *MPL*) [sec]
- az a T_{max} idő, amelyen belül egy nyugtára várakozó küldő állomás ismétli a csomagokat [sec]
- a leghosszabb A idő egy csomag vétele és a rá vonatkozó nyugta elküldése között, [sec]
- a küldő állomás R csomagtovábbítási sebessége, [csomag/s]

Ezekkel az adatokkal $2^n \geq (2MPL + T_{max} + A)R$

Az adó T_{max} ideig folytatja a csomagja ismétlését az első kísérlettől kezdve

Legrosszabb esetben a vevő közvetlenül a csomag élettartamának lejártá előtt, tehát $T_{max} + MPL$ idő elteltével kapja meg azt.

A idő elteltével küldi a nyugtát, az legfeljebb MPL idő múlva érkezik meg az adóhoz. Ezalatt az adó legfeljebb $(2MPL + T_{max} + A)R$ csomagot, így sorszámot generálhatott

A csomagvesztés észlelése történhet:

Időzítéssel (timeout):

Kritikus pont az időzítés mértéke:

- túl kis érték esetén sok felesleges ismétlés jelentkezik
- túl nagy érték esetén lassú, vontatott lesz a hibajavítás folyamata

Az időzítés mértéke lehet:

- rögzített, általában a teljes körülfordulási idő (**Round Trip Time, RTT**) 1-2-szerese
- változó, a mért RTT értéktől illetve annak valamilyen átlagától függő

Negatív nyugtázással (negative acknowledgement):

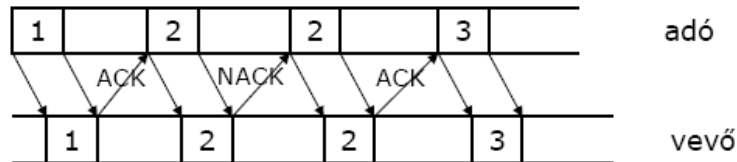
A vevő NACK-ot küld, ha hibás csomagot vagy hézagot észlel a vett csomagok sorszámában. NACK vételekor a küldő ismételten elküldi a kért csomagokat. Problémák:

- csomagvesztés általában torlódáskor lép fel, az ilyenkor küldött NACK csomagok csak növelik a hálózat terhelését
- a NACK is elveszhet, ilyenkor a vevőnek kell ismételnie, de ehhez a vevőnél kell időzítést alkalmazni

Csomagismétlési módszerek:

Megállás és várakozás(Stop-and-Wait)

Az adó minden csomag elküldése után leáll a továbbítással, és a vevőtől érkező nyugtára vár. A vevő minden csomagot nyugtáz, a hibátlanokat pozitív (ACK), a hibásakat/hiányzókat negatív (NACK) nyugtával. NACK esetén az adó ismételten elküldi a csomagot. Egyszerű, de nem hatékony eljárás (adó sokat vár, sok a visszairányú csomag).



Visszalépés n-nel – go-back-n:

Ablak-típusú, amire már láttunk példát a forgalomszabályozásnál. A hibakezelő ablak azon csomagok sorszámait tartalmazza, amelyeket az adó már elküldött, de még nem nyugtáztak. A hibakezelő ablak legnagyobb mérete rögzített. Minden elküldött csomag eggyel növeli, minden ACK csökkenti az ablak méretét. Ha az ablak mérete eléri a rögzített maximumot, az adó leáll.

A visszalépés n-nel azt jelenti, hogy amikor egy csomag ismétlését kéri a vevő, az adó a hibakezelő ablakban található összes csomagot ismételten elküldi.



- Biztonságra törekszik, mivel egy csomag hibája esetén is több csomagot ismételt, ezért jobban kezeli a hibacsomókat.
- Egyszerűbb, mert a vevőnek nem kell tárolni a már beérkezett csomagokat.
- Sávszélesség-veszteséget okoz, mivel többet ismételt a szigorúan szükségesnél
- Ha az eredeti hibát túlterhelés okozta, a fölös ismétlések csak rontanak a helyzeten
- Külső ellenőrzés nélkül ez odáig fokozódhat, hogy a hálózat csak csomagismétlést végez, valódi forgalom nincs, ez a torlódás miatti összeomlás (congestion collapse)
- p csomaghiba-valószínűség és W maximális hibakezelő ablakméret mellett az adó legfeljebb $(1-p)/(1-p+Wp)$ százalékban használja a sávszélességet nemismételt csomagok továbbítására

Szelektív csomagismétlés:

A küldő állomás csak a kért csomagokat ismétli, a vevő csak a hibásan vett csomagokat dobja el. A hibásan vett csomag utáni jó csomagokat egy külön pufferben tárolja, a helyesen vett ismételt csomag után a külön puffer tartalmát bemásolja a vételi pufferbe.

Nagyon hatékony módszer, bonyolultabb algoritmussal és nagy puffermemória-igénnyel.



9. Forgalommenedzselés (Traffic control)

Szabályok, intézkedések, tennivalók (policies and mechanisms) összessége, amely lehetővé teszi a különféle kiszolgálási igények hatékony kielégítését.

A forgalommenedzselés kiindulópontja:

Tételezzük fel, hogy a felhasználóknak vannak hasznosság vagy megelégedettség függvényei (utility functions). Ezeket kell maximalizálni, mivel a hasznossági függvény - ha megadható - pontosan jellemzi a felhasználó elvárásait.

Általában nincs ilyen, de a felhasználói igények, preferenciák alapján lehet készíteni, bár lehet, hogy matematikailag nem lesznek kezelhetők. Kapcsolatot kell létesíteni a hasznossági függvény és a QoS paraméterek között, mert az utóbbira lehet méretezni.

Forgalommodellezés:

A forgalom-modell egy alkalmazás összegzett viselkedésének várható jellemzőit tartalmazza

Két alapvetően eltérő fajta:

matematikailag kezelhető modell

tapasztalati modell, a hálózaton végzett mérések alapján (ritkán kezelhető matematikailag)

Internet-forgalommodellek:

Legalább az alábbi négy paraméter együttesével jellemezhető:

- a „session”-ök közötti beérkezési idő
- egy-egy session (összeköttetés) időtartama
- egy-egy session-ban továbbított adatmennyiség
- egy-egy session-on belül a csomagok közötti időköz

Két fő forgalmi osztály → két fő kiszolgálási típus (Garantált/Best effort)

ATM Forum alosztályok:

- garantált: CBR (Constant Bit Rate) és VBR (Variable ...)
- best-effort: ABR (Available Bit Rate) és UBR (Unspecified...)

IETF alosztályok

- Tolerant: Controlled-load / Intolerant: Guaranteed service
- Best-effort

A forgalommenedzselés időskálája és eszközeinek kapcsolata:

Időtartam	Eszközök	Hálózat	Végpont
< Körbefordulás (csomag)	Feladatütemezés	X	X
	Szabályozás és ellenőrzés	X	X
	Routing (ö.k. mentes hál.)	X	X
	Hibakezelés	X	X
Néhány körbef. (börszt)	Flow control	X	X
	Ismétlés		X
	Újratárgyalás	X	X
Session (hívás)	Jelzés	X	X
	Beengedésszabályozás	X	
	Tarifálás	X	
	Routing (ö.k. alapú hál.)	X	
Egy nap	Csúcsidőszak tarifálása	X	
Egy hét vagy	Kapacitástervezés	X	

10. Aszinkron Átviteli Mód (Asynchronous Transfer Mode, ATM)

Az ATM egy nemzetközileg szabványosított multiplexelési és kapcsolási technológia, és az ezen alapuló távközlőhálózati rendszertechnika. Az ATM az ún. gyors csomagkapcsolási módszerek családjába tartozik és több fontos alapszabványt alkalmaz, amellyel az eddigiekben megismertünk

Az ATM-et az ITU-T szabványosította 1988-ban, a B-ISDN átviteli módjaként.

Fő célkitűzések:

- különböző típusú forgalmak átvitelére tervezték: beszéd, állókép, video, adat
- Tág átvitelisebesség-tartomány: néhány száz kbit/s-tól egészen nagy sebességekig (2.4 Gbit/s-ig)

Az ATM „gyors csomagkapcsolási” technika

- gyors: rövid csomagok, **nincs forgalomszabályozás, nincs linkenkénti hibajavítás**
- rövid, fix hosszúságú adatsomagok hordoznak mindenféle típusú adatot
- minden összeköttetéshez képes specifikus QoS-t biztosítani

Az ATM (virtuális) összeköttetés-alapú csomagkapcsolt hálózat.

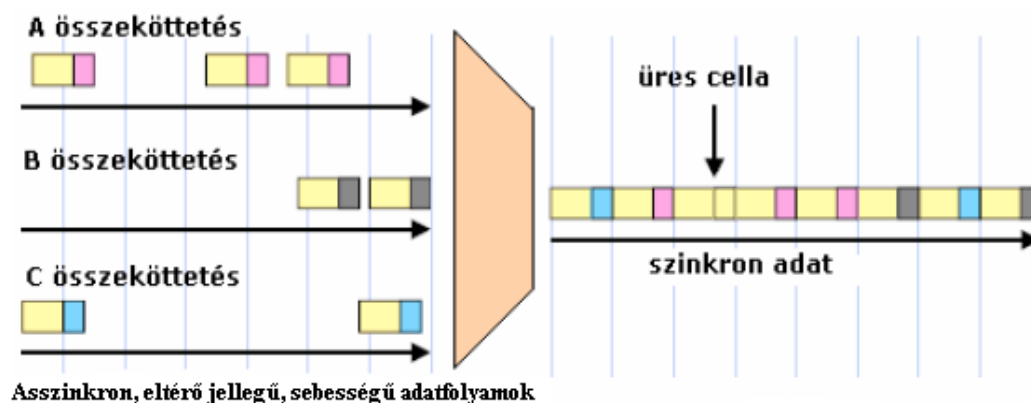
Funkciói: hívásvezérlés (összeköttetés alapú), címzés, routing, ütemezés, forgalommenedzsment

A cellamultiplexálás elve:

A bemeneti adatfolyam byte-jaiból rövid, állandó hosszúságú adategységeket, ATM cellákat képzünk (**fejrész 5 byte, hasznos rész (payload) 48 byte**). A multiplexer bemeneteire - aszinkron módon - számos, eltérő jellegű adatfolyam (hang, adat, kép,...) érkezik, egy vagy több felhasználói végberendezéstől (az egyes adatfolyamok adatsebessége eltérő lehet).

A cellák az ATM multiplexer bemenetére véletlenszerű időközönként érkeznek.

A multiplexer egy pufferben átmenetileg tárolja a cellákat, majd FCFS vagy más előre meghatározott eljárás szerint beilleszti a kimenő szinkron ATM adatfolyamba.



Az ATM-cella fő jellemzői:

A cella mérete 48+5 byte (hasznos rész + fejrész, payload + header). A cellaméret megválasztásának szempontjai, kompromisszum:

Beszédátvitelnél 125 µs-onként 1 minta (1 byte), 48 byte tehát 6 ms-nak felel meg.

A fej- és hasznos rész aránya elég nagy, nagy az „overhead”, a járulékos (de fontos!) információ átvitelére szolgáló rész.

Az ATM cella fejrészének felépítése:

Kétféle van:

UNI (User-Network Interface)

NNI (Network-Network Interface)

GFC (általános áramlásvezérlés): nem használt, mert nincs megfelelő protokoll

VPI (virtuális útvonal-azonosító): két ATM csomópont közötti virtuális útvonal azonosítója.

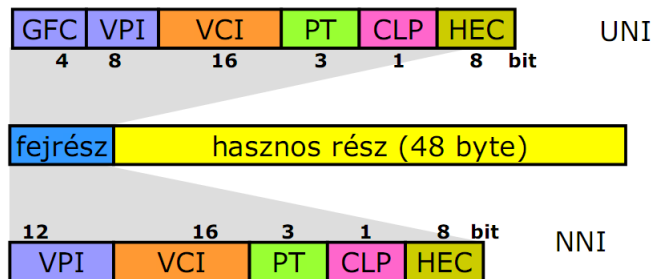
VCI (virtuális csatorna azonosító): azonosít egy virtuális csatornát két ATM csomópont között, vagy egy virtuális útvonalon belül.

PT (hasznos rész típusa): alapvetően a hasznos adatot hordozó és a menedzseléshez szükséges cellatípusok megkülönböztetése

CLP (cellavesztési prioritás): 0 magas (adatátvitel), 1 alacsony (adatvesztésre kevésbé érzékeny kép, hang), eldobható, ha torlódás

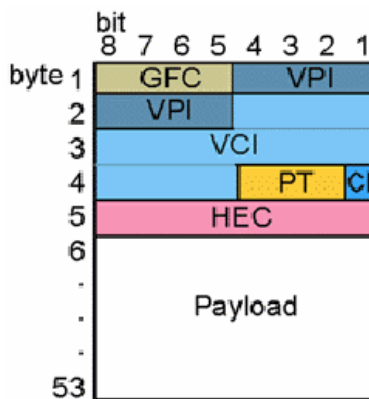
HEC (fejrész-hibaellenőrzés): CRC-ellenőrzőösszeget képezünk a fejrészre (egyszeres hibát javítunk, többszörös hibát jelzünk, ez esetben

Tehát UNI-ban van 4 bites GFC,
NNI-ben nincs, helyette +4 byte VPI

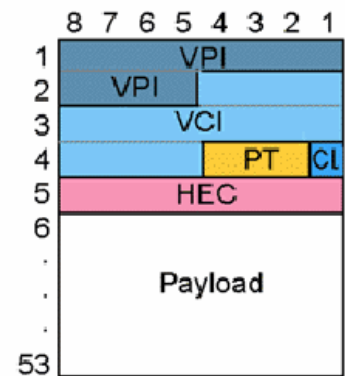


GFC: általános áramlásvezérlés
VPI: virtuális útvonal azonosító
VCI: virtuális csatorna azonosító
PT: hasznos rész típusa
CLP: cellavesztési prioritás
HEC: fejrész-hibaellenőrzés

UNI: felhasználó-hálózat interfész
NNI: hálózat-hálózat interfész



UNI format



NNI format

Az ATM-összeköttetéseket a VPI-VCI-pár definiálja:

VPI mező: 256 virtuális út a UNI-n és 4096 virtuális út az NNI-n

VCI mező: maximum 65 536 VCI

Ezt a kettőt nevezik együttesen címkének

Egy VPI/VCI kettős lokális érvényű, azaz két szomszédos csomópont közötti viszonylatra vonatkozik.

Több pont-pont kapcsolatból álló összeköttetésen ugrásonként különböző VPI/VCI értékeket használ, amihez az ATM kapcsológépek kapcsolótáblákat tartanak fenn (útvonalkijelölés!).

Ezek minden összeköttetésre vonatkozóan összerendelik a bejövő és kimenő VCI/VCI értékeket és az in/out portokat.

Virtuális csatorna (Virtual Channel - VC), virtuális útvonal (Virtual Path - VP) és virtuális csatorna-összeköttetés (Virtual Channel Connect - VCC):

- A VP kapcsoló (szokás ATM keresztpontnak is nevezni) a cellákat a virtuális útvonal szintjén kapcsolja → hatékonyságnövelő, mert a kapcsolásnál nem kell a VCI-vel foglalkozni.
- A VC kapcsoló a virtuális csatorna szintjén kapcsol, rendszerint megváltoztatja a VPI és VCI értékét egyaránt.

Az összeköttetés lehet:

Permanent Virtual Connection (PVC - állandó virtuális áramkör):

- A PVC-ket a rendszermenedzsment állítja be, hosszú ideig fennmaradnak

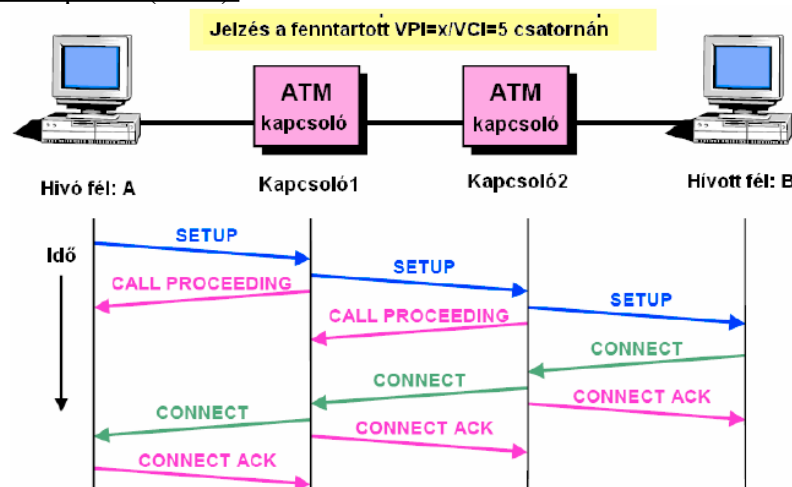
Switched Virtual Connection (SVC - kapcsolt virtuális áramkör):

- Az SVC-ket az ATM-jelzésrendszer segítségével építi fel a hálózat, valódi időben, tetszőleges időtartamra.

ATM címkekapcsolás (ATM label switching):

A kapcsoló beolvassa egy beérkező cellát egy adott bemeneti porton, annak fejrészből kiolvassa a VPI/VCI címkét, majd megkeresi a bemeneti port és a címke értékéhez tartozó kimeneti port számát és egy új címkeértéket a kapcsolótáblájában. A kapcsoló a bemeneti címkeértéket felcseréli a táblázatban talált kimeneti címkeértékkel, majd a táblázatban megadott kimeneti porton továbbküldi.

ATM kapcsolat felépítése (SVC):



Bontáskor *RELEASE*, *RELEASE COMPLETE*.

Az ATM átviteli és kapcsolási mód fő funkciói:

- Összeköttetés-alapú csomagkapcsolás
 - Nincs linkenkénti hibavédelem és flow control
 - A cellavesztés vagy a téves célbajuttatás valószínűsége alacsony
 - Az adatok visszaállítása elveszett vagy hibás cellák esetén a magasabb rétegbeli protokollok (pl. TCP) feladata
- Címzés
 - Minden ATM végkészüléknek és ATM kapcsolónak egyedi ATM címe van
 - Szolgáltatásminőség - Quality of Service - biztosítása
 - Minden ATM összeköttetéshez QoS kategória kapcsolódik, az ATM hálózat garantálja a megállapodás szerinti QoS-t minden összeköttetés számára

QoS, szolgáltatási kategóriák és torlódásvezérlés ATM hálózatokban

Forgalmi jellemzők:

Peak Cell Rate (PCR) ATM Forum, ITU-T szabvány - csúcs-cellasebesség, amelyet a forrás bebocsáthat az ATM hálózatba

Sustained Cell Rate (SCR) ATM Forum szabvány - tartósan fennálló cellasebesség:

Kiszámítjuk az egymást követő rövid T hosszú időszakokra az átlagos cellaszámokat, ezeknek az átlagoknak a maximuma az SCR. A T időt nem definiálják a szabványokban, a gyakorlatban 1 sec-nak veszik

Maximum Burst Size (MBS) ATM Forum szabvány - maximális burst-méret: maximális cellaszám, amelyet a forrás a csúcs-cellasebességgel (PCR) küldhet

Burstiness – börsztösség: Ez a fogalom azt jellemzi, hogy milyen mértékben csomósodik a forrás által kibocsátott cellafolyam (aktív átvitel/szünet aránya)

Inter-Arrival Times - beérkezési időközök

Szolgáltatásminőség (Quality of service - QoS) paraméterek:

Cell Loss Rate (CLR): Cellavesztési arány, könnyű számszerűsíteni

Jitter (Cell Delay Variation - CDV): Azt jellemzi, hogy mennyire ingadoznak a beérkezési időközök a célnál. Videó és hang esetén fontos paraméter.

Cell Transfer Delay (CTD): Amennyi idő alatt a cellát átviszi a hálózat végponttól végpontig, azaz a küldő eszköztől a vételi oldali végkészülékig

- Fix Cell Delay: terjedési késleltetés, feldolgozási idő
- Peak-to-Peak Cell Delay Variation (max CDV): sorbanállási késleltetés

Maximum Cell Transfer Delay (max CTD): Statisztikus felső korlát a CTD-re

Cell Error Rate (CER): Egy összeköttetésen a hibás cellák számaránya a forrás által leadott teljes cellaszámhoz képest. Hibás cella az, amelynek a payload-ja meghibásodott.

Cell Misinsertion Rate (CMR): Tévesen célba szállított cellák aránya adott időszak alatt

ATM szolgáltatási kategóriák:

Constant Bit Rate (CBR): Real-time alkalmazások számára, amelyek szigorúan rögzített késleltetés és késleltetés-ingadozást igényelnek

Real time Variable Bit Rate (rt-VBR): Real-time alkalmazások számára, amelyek korlátozott késleltetés és késleltetés-ingadozást igényelnek

Non-real time Variable Bit Rate (nrt-VBR): Változó bitsebességű és börsztös források, amelyek nem igényelnek real-time jellegű korlátokat

Unspecified Bit Rate (UBR): Késleltetést tűrő alkalmazások számára, nem garantál szolgáltatásminőséget.

Available Bit Rate (ABR): Visszacsatolás-alapú, olyan források számára, amelyek képesek adási sebességüket a rendelkezésre álló átbocsátóképességhez igazítani

Guaranteed Frame Rate (GFR): olyan források számára, amelyek egy minimális cellasebességet igényelnek, tudnak ennél többet is adni, amelyet azonban a hálózat nem garantál.

A CBR, rt-VBR, nrt-VBR, UBR szolgáltatások jellemzésére használt forgalomleírók és QoS-paraméterek

CBR

- Forgalomleírók: PCR, CDVT
- QoS jellemzők: maxCDV, MaxCTD, CLR

rt-VBR

- Forgalomleírók: PCR, CDVT, SCR, MBS
- QoS jellemzők: maxCDV, MaxCTD, CLR

nrt-VBR

- Forgalomleírók: PCR, CDVT, SCR, MBS
- QoS jellemzők: CLR

UBR

- PCR specifikálva van, de nem használja a CAC és a policing
- Nincsenek QoS paraméterek jelezve

Forgalomleírók és QoS-paraméterek az ABR és a GFR számára

ABR

- Forgalomleírók: PCR, CDVT, MCR
- QoS jellemzők: CLR (lehetséges, hálózathatófüggően)

GFR

- Forgalomleírók: PCR, CDVT, MCR, MBS, MFS, CDVT
- QoS jellemzők: CLR (lehetséges, hálózathatófüggően)

Torlódásvezérlés- Congestion control:

Preventív torlódásvezérlés: Megelőzi a torlódást.

Egy új összeköttetésre vonatkozó kérés esetén minden, az útvonal mentén levő ATM switch el kell döntse, hogy elfogadja-e vagy sem

A döntéshez két kérdést kell megválaszolni:

- Befolyásolja-e az új összeköttetés a kapcsológép által már kezelt összeköttetések szolgáltatásminőségét?
- Képes-e a kapcsoló az új összeköttetés által igényelt szolgáltatásminőség nyújtására?

Call admission control (CAC):

A legtöbb CAC algoritmus a CLR-en (Cellavesztési Arány) alapul.

Az új összeköttetés elfogadást nyer, ha a switch képes nyújtani a kért cellavesztési arányt anélkül, hogy az hatással lenne a meglevő összeköttetésekre. A jittert vagy CTD-t nem vesszük figyelembe.

Reaktív torlódásvezérlés

A hálózat által adott visszacsatoláson alapul, szabályozza az adási sebességet

Az összeköttetés felépítésekor az adó minimum cell rate-et (MCR) kér. Megadja a maximum cell rate-et is, amely a PCR-je (csúcs-cellasebesség).

A hálózat elfogadja, ha a kért MCR-t teljesíteni tudja. A forrás túl is lépheti a kért MCR-t, ha a hálózatban van ehhez szabad kapacitás

Ha torlódás kezdődik, az adónak csökkentenie kell az adási sebességét

Összefoglalva, az ATM:

- 1. Összeköttetés alapú** (connection oriented) üzemmódban működik. Mielőtt a hálózat egy terminálja információt küldene, egy logikai kapcsolatfelépítési fázis a szükséges erőforrásokat lefoglalja. Ez az összeköttetés alapú működési mód **minimális csomagvesztést és így maximális minőséget garantál.**
- Adatkapcsolati szinten nincs hibavédelem vagy forgalomirányítás. A nagyon jó minőségű hálózati kapcsolatok miatt olyan kevés a hiba, hogy ez elhanyagolhatóvá teszi a hibavédelmet. Az egyetlen megelőző típusú védelem a preventív torlódásvezérlés.
- 3. A fejrészben foglalt hálózati feladatok minimálisak.** A hálózati gyorsaság garantálása érdekében az ATM fejrésznek csak nagyon korlátozott funkciója van. **Fő feladata a virtuális kapcsolat azonosítása** (VCI/VPI címke) és minden adatsomag számára **megfelelő útvonalválasztás garantálása.**
- 4. Az információmező viszonylag rövid.** Mivel a rögzített hosszúságú csomagok kisebb hálózati késleltetést és egyszerűbb kapcsolást eredményeznek, valamint lehetővé teszik bármilyen szolgáltatás továbbítását, az ATM „celláknak” nevezett rögzített hosszúságú csomagokat használ (48 byte-os hasznos adat, 5 byte-os fejrész). A kisméretű, rögzített hosszúságú adatcellák alkalmassá teszik az ATM hálózatokat a különböző típusú kevert adatforgalom (hang, videokép és más adat) problémamentes továbbítására.
- 5. Rugalmasan alkalmazkodó, a jövő változó követelményeinek is megfelel.** Hatékonyan kihasználja a rendelkezésre álló erőforrásokat. Minden szolgáltatás osztozik a hálózat minden rendelkezésre álló erőforrásán, így **megvalósul az erőforrások optimális elosztása.**

11. Protokoll Architektúrák

Annak érdekében, hogy csökkentsék a hálózatok bonyolultságát, a legtöbb hálózatot rétegekbe (layers) vagy szintekbe (levels) szervezik. Minden réteg vagy szint az alatta levőre épül. A rétegek száma, neve, tartalma és funkciója minden hálózatban más és más. Az egyes rétegek célja viszont minden hálózatban az, hogy a felettük levő réteg számára szolgáltatásokat nyújtson oly módon, hogy közben a szolgáltatások implementálásának részleteit azok elől elrejtse.

Előnyök:

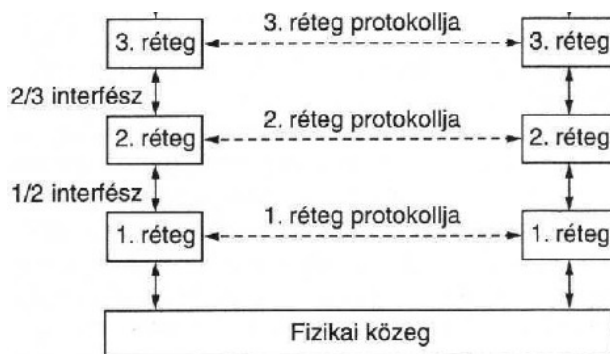
- Nagyon összetett feladat kezelhető részekre bontható
- Az egyes részek megvalósítása független más részekétől, így könnyen módosítható
- Feljebb lévő feladatoknak közös kiszolgálást nyújthat egy lejjebb lévő rész

Hátrányok:

- Adott réteg működéséhez szükséges információk egy másik rétegben - megsérül a rétegstruktúra
- Feladatok duplikálása elkerülhetetlen, ez a hatékonyság rovására megy (pl. hibavédelem több rétegben is)

Az egyik gép n -edik rétege párbeszédet folytat egy másik gép n -edik rétegével. A párbeszéd írott és íratlan szabályait együttesen az n -edik réteg protokolljának nevezzük. A protokoll lényegében olyan megállapodás, amely az egymással kommunikáló felek közötti párbeszéd szabályait rögzíti.

A rétegek és protokollok halmazát hálózati architektúrának (network architecture) nevezzük.



A szolgáltatásokat a szolgálatelérési pontokon (Service Access Points, SAP) keresztül lehet igénybe venni. Az n -edik réteg szolgálatelérési pontjai azok a helyek, ahol az $(n + 1)$ -edik réteg igénybe veheti a rendelkezésére álló szolgáltatásokat.

Protokoll-adategységek (PDU – protocol data unit)

Ezek kerülnek továbbításra a szomszédos rétegek között

A PDU-k általános felépítése, tartalma:

- Header, Payload, Trailer

Fejben és farokban található kiegészítő információk:

- Címek, sorszámok, hibavédelem, egyéb opcionális paraméterek

ISO OSI referenciamodell

A fizikai réteg (physical layer) feladata, hogy továbbítsa a biteket a kommunikációs csatornán. A rétegnek biztosítania kell azt, hogy az egyik oldalon elküldött 1-es bit a másik oldalon is 1-ként érkezzen meg, és ne pedig 0-ként. Ez a réteg tipikusan olyan kérdésekkel foglalkozik, hogy mekkora feszültséget kell használni a logikai 1, és mekkorát a logikai 0 reprezentálásához, mennyi ideig tart egy bit továbbítása, az átvitel megvalósítható-e egyszerre mindkét irányban, miként jön létre az összeköttetés, hogyan bomlik le az összeköttetés, ha már nincs szükség rá (jelzések a küldése a csatornára, ill. fogadása onnan).

Az adatkapcsolati réteg (data link layer) feladata, hogy a fizikai szint szolgáltatásainak igénybevételével a hálózati réteg számára fel nem ismert átviteli hibáktól mentes átvitelt biztosítson. A forgalomszabályozás és a hibakezelés is rendszerint eleme az adatkapcsolati rétegnek. Az adatszóró hálózatok esetén felmerül még egy kérdés az adatkapcsolati réteget illetően, hogy hogyan szabályozzuk az osztott csatornához való hozzáférést. Ezzel a problémával az adatkapcsolati rétegnek egy speciális alrétege, a közeghozzáférési alréteg foglalkozik. További feladata a csomagok összeállítása, hibaellenőrzéshez szükséges adatok előállítása, vétel esetén ellenőrzése, esetleg javítás.

A hálózati réteg (network layer). A legfontosabb kérdés itt az, hogy milyen útvonalon kell a csomagokat a forrásállomástól a célállomásig eljuttatni. Ha egyszerre túl sok csomag tartózkodik az alhálózatban, akkor egymást akadályozzák a továbbhaladásban, és ilyenkor torlódás alakul ki. A torlódások kivédése szintén a hálózati réteg feladata. További feladata, hogy lehetővé tegye az egymástól eltérő hálózatok összekapcsolását (címezés, protokoll, csomagméret, stb).

A szállítási réteg (transport layer) legfontosabb feladata az, hogy adatokat fogadjon a viszony rétegtől, feldarabolja azokat kisebb egységekre - ha szükséges -, továbbítsa ezeket a hálózati rétegnek és biztosítsa azt, hogy minden kis egység hibátlanul megérkezzen a másik oldalra. A szállítási réteg azt is meghatározza, hogy milyen szolgáltatásokat kell a viszony rétegnek, és végső soron a hálózat felhasználóinak nyújtani. Az információ áramlásának szabályozására is kell valamilyen mechanizmus, amely arra ügyel, hogy a gyorsabb hosztok ne árásszák el a lassab-bakat. Ezt a mechanizmust **forgalomszabályozásnak (flow control)** nevezzük. A hosztok közötti forgalomszabályozás nem ugyanaz, mint a routerek közötti forgalomszabályozás. Forgalomirányítás, útvonalkeresés.

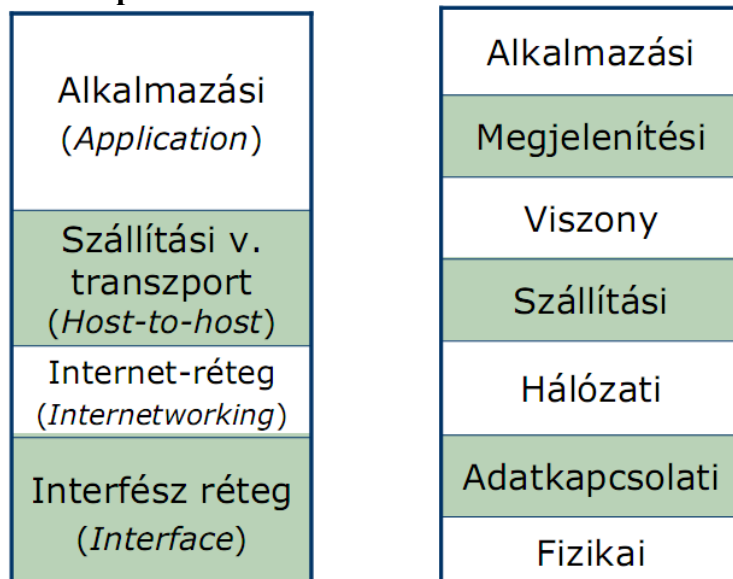
A viszony réteg (session layer) feladata az, hogy a felhasználók között viszony (session) létesítését tegye lehetővé. Továbbá feladata a **vezérjelkezelés (token management)** is. A viszony réteg **szinkronizálást (synehronization)** is végez (ellenőrzési pontokat beszűrása az adadfolyamokba)

A megjelenítési réteg (presentation layer) olyan feladatokkal foglalkozik, amelyek elég gyakran fordulnak elő ahhoz, hogy megérje azokra egy általános megoldást kidolgozni, és így ne kelljen a felhasználóknak minden alkalommal maguknak megoldani azt. A megjelenítési réteg egyik tipikus feladata az adatok szabványos módon történő kódolása.

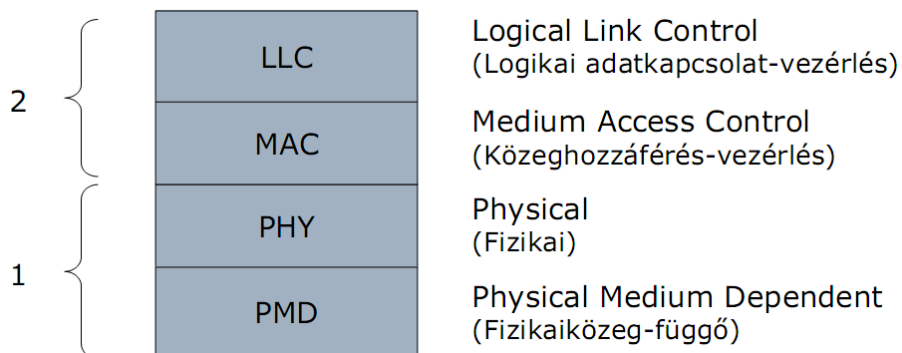
Az alkalmazási réteg (application layer) számos olyan protokollt tartalmaz, amelyet széles körben használnak. Például a világon több száz egymással nem kompatibilis terminál létezik. Az alkalmazási réteg egy másik feladata a fájlátvitel (file transfer). A különféle fájlrendszerek más és más módon nevezik el a fájlokat, eltérő módon ábrázolják a szövegsorokat stb.

Az architektúra nem valósul meg teljesen soha, ma már a legtöbb réteg, főleg a felsőbb rétegekben nincs használatban. Referenciamodellként viszont továbbra is hasznos

TCP/IP protokoll architektúra

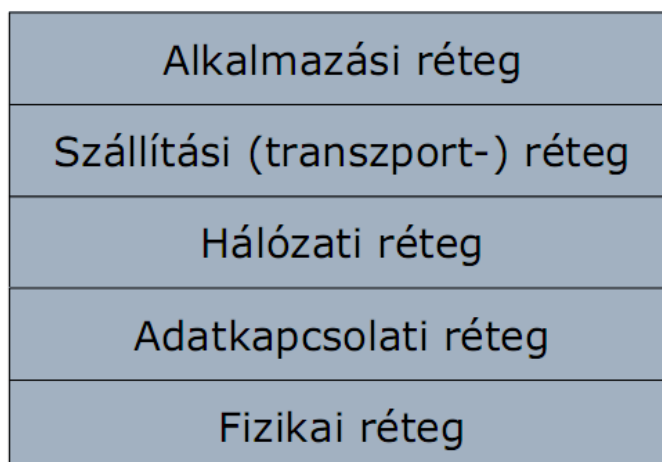


IEEE szerinti LAN architektúra



Kombinált referenciamodell

5 réteg, a felső három a TCP/IP-nek, az alsó 2 az OSI-nak felel meg



12. Adatkapcsolati rétegbeli kommunikáció

Az adatkapcsolati réteg:

- szolgáltatásokat nyújt a hálózati rétegnek
- használja a fizikai réteg szolgáltatásait
- nagyterjedésű hálózatok két szomszédos csomópontja, illetve helyi hálózatok csomópontjai közötti adatátvitelt biztosítja
- tartalmazhat hibadetektálási/hibajavítási funkciókat, a fizikai rétegben jelentkező hibák kezelésére

Egyes hálózatokban két alrétegre oszlik:

- logikai kapcsolat vezérlés (Logical Link Control, LLC)
- közeg hozzáférés vezérlés (Media Access Control, MAC)

Adatkapcsolati rétegbeli protokollok:

Magasszintű adatkapcsolat vezérlés (High-Level Data Link Control - HDLC):

- bit orientált szinkron adatkapcsolati protokoll
- az ISO (13239) az IBM által definiált SDLC protokoll továbbfejlesztésével definiálta
- egyaránt támogatja az összeköttetés alapú és az összeköttetés mentes szolgáltatásokat
- számos további protokoll alapja a HDLC
- adategysége a keret (frame) (Minden keretet egy speciális bitsorozat határol, amely a 01111110 (0h7E)).

HDLC protokollt alkalmazó hálózatban háromféle állomás (csomópont) létezhet:

- **elsődleges**, amely a kapcsolat vezérlője
 - vezérli az össze többi állomást
 - szervezi az adatátvitelt
- **másodlagos**, amelynek léteznie kell, ha van elsődleges és amely az elsődleges felügyelete alatt áll
 - csak az elsődleges kérésére aktiválódik
 - nem felel a kapcsolat vezérléséért
- **kombinált**, amely egyesíti az elsődleges és a másodlagos funkcióit

A HDLC protokoll a három állomástípusra alapozva háromféle konfigurációt, kiépítést ismer:

- kiegyenlítetlen: egy elsődleges és egy v. több másodlagos állomásból áll
- kiegyenlített: kettő v. több kombinált állomásból áll, az állomások egyenrangúak
- szimmetrikus: minden fizikai állomás két logikai állomásból áll, az egyik elsődleges a másik másodlagos

A HDLC működési módjai (két adatcserét folytató állomás közötti viszony)

Normál válasz mód (Normal Response Mode, NRM):

A szabályos elsődleges-másodlagos viszony megvalósulása. A másodlagos állomás csak az elsődleges engedélyével adhat, az engedély birtokában a másodlagos állomás egy v. több, adatot tartalmazó keretből álló válasz továbbítását kezdeményezheti.

Aszinkron válasz mód (Asynchronous Response Mode, ARM):

A másodlagos állomás az elsődleges engedélye nélkül maga is kezdeményezhet átvitelt, ha a vonal tétlen. Az ARM nem változtatja meg az állomások közötti elsődleges-másodlagos viszonyt. Az elsődleges állomástól minden üzenet még mindig a másodlagoshoz jut, és csak azután kerülhet további eszközökhöz.

Aszinkron kiegyenlített mód (Asynchronous balanced Mode, ABM):

Minden állomás egyenrangú → csak kombinált állomások között, pont-pont kapcsolatban. Bármelyik kombinált állomás kezdeményezhet átvitelt a másik engedélye nélkül.

HDLC keretek:

- információs (Information, I), felhasználói adatok, illetve ezekre vonatkozó vezérlési információk továbbítására
- felügyeleti (Supervisory, S) az átvitel vezérlését szolgáló információkhoz (nincs hozzá információ rész)
- számozatlan (Unnumbered, U), a rendszermenedzsment számára fenntartva

Jelző	Cím	Vezérlés	Információ	FCS	Jelző
Flag	Address	Control	Information		Flag

Jelző (Flag): minden keret elején és végén (01111110)

- a vevő szinkronizálására szolgál
- ez a minta adatok közt nem fordulhat elő:
- 5 db egymásutáni 1-es adatbit után az adó automatikusan beszúr egy 0-t
- a vevő az 5 egyes utáni 0-t automatikusan törli
- a keretek közötti szünetben jelzők folytonos továbbítása történik

További speciális jelző sorozatok:

- 7 v. több, de 15-nél kevesebb egymás utáni 1-es bit jelzi a forgalom megszakítását (abort)
- 15 vagy több egymásutáni 1-es jelzi a tétlen csatornát (hunt mode)

Cím (Address): 8 bit v. annak többszöröse, a hálózattól függően

- több byte-os címnél az utolsó byte utolsó bitje 1, a többi 0
- minden állomásnak egyedi címe van
- kiegyenlített konfigurációban a cím a parancs és a válaszkkeretben is a másodlagos állomásra vonatkozik
- kiegyenlített konfigurációban a parancskeretben a célállomás címét, a válaszkkeretben a küldő állomás címét tartalmazza
- a cím első bitje jelzi, hogy egy (=0) vagy több (=1) állomásra vonatkozik

Vezérlés (Control): meghatározza a keret típusát

- Információ („I”) keretben végfelhasználói információt szállít a két állomás között
- felügyeleti („S”) keretben vezérlő funkciókat lát el (nyugta/ismétlés-kérés/adatfolyam felfüggesztésének kérése).
- számozatlan („U”) keretben kapcsolatvezérlési funkciók (kapcsolat inicializálása/bontása/egyéb kapcsolatvezérlő funkciók)
- P/F bit:
 - ha elsődleges küldi másodlagosnak, akkor állapotlekérdezés
 - ha másodlagos küldi az elsődlegesnek, akkor az állapotot küldi
 - normálválasz módban a másodlagos ezzel jelzi az adás végét

Kód (vezérlés része)

Kódmező értelmezése felügyeleti („S”) keretben:

- 00: vevő készenlétben
- 01: visszautasítás
- 10: vevő nincs készenlétben
- 11: szelektív visszautasítás

Kódmező értelmezése számozatlan („U”) keretben:

- SNRM: normál válasz mód beállítása
- SARM: aszinkron válasz mód beállítása
- SABM: kiegyenlített válasz mód beállítása
- DISC: kapcsolat bontása
- UA: számozatlan nyugtázás
- FRMR: keret visszautasítása

Információ:

- csak az információs és a számozatlan keretben található - tényleges adatbitek
- mérete hálózathoz tartozó, de egy adott hálózaton belül állandó

Keretellenőrző összeg (Frame Check Sequence – FCS): a HDLC hibadetektálást szolgáló mezője - a cím-, vezérlési és információs mezőkre vonatkozik. 16 vagy 32 bites CRC lehetséges.

(2008 tavaszán nem vettük)

Szinkron Adatkapcsolati Vezérlés (Synchronous Data Link Control – SDLC):

- szinkron adatkapcsolati vezérlés terminál és számítógép között
- bitorientált szinkron adatátviteli protokoll
- fél-duplex vagy duplex adatátvitel
- többféle topológia: pont-pont közötti/pont-többpont közötti/hurokba szervezett/középponti (hub) szervezésű
- kapcsolt vagy kapcsolásmentes hálózatokban

Lényegében megfelel a kiegyenlített konfigurációjú NRM HDLC-nek

Eltérések a HDLC-től:

- csak egy átviteli mód, az NRM (Normál válasz mód)
- csak 16 bites CRC
- HDLC támogatja a hurokba szervezett és központosított hálózatokat

Link Access Protocol - Balanced, LAPB:

Kiegyenlített kapcsolathozzáférési protokoll: az X.25 protokollkészlet adatkapcsolati szintű tagja. Keretekbe szervezett adatokat továbbít egy adatvégberendezés (**Data Terminating Equipment, DTE**) pl. egy számítógép és egy adatkapcsolati végberendezés (**Data Circuit Terminating Equipment, DCE**), pl. egy modem között.

LAPB kapcsolatot akár a DTE, akár a DCE kezdeményezhet, a kezdeményező lesz az elsődleges állomás.

Működése megfelel az aszinkron kiegyenlített módban működő HDLC-nek.

Ugyanaz a három kerettípus, mint a HDLC-nél.

Két érvényes LAPB cím létezik: DTE cím (0x03) és DCE cím (0x01), ezek egyben az átvitel irányát is meghatározzák

Link Access Protocol - D channel, LAPD:

Kapcsolathozzáférési protokoll a csatorna számára: az ISDN csatorna protokollja

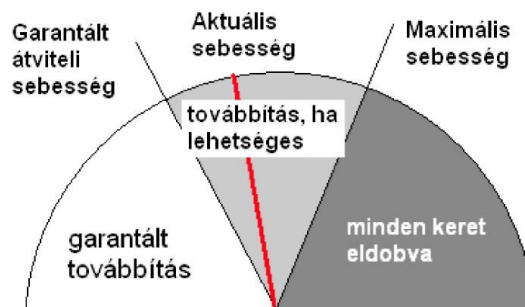
Link Access Protocol - Frame Mode Services, LAPF:

Kapcsolathozzáférési protokoll kerettovábbítás számára (végpontok közötti jelzésre)

A legfontosabb mag- (core) funkciói:

- kerethatárolás és -igazítás
- transzparens átvitel
- virtuális áramkörök nyálábolása és kibontása
- bájtok/oktettek határra igazítás (nulla beszúrás előtt egész számú bájt)
- keret méretének ellenőrzése
- hibakezelés
- torlódásvezérlés

LAPF áramlásvezérlés:



A garantált átviteli sebesség [keret/sec] alatt minden keretet továbbít a hálózat. Efölött, de a maximum alatt a garantált sebesség felett érkező keretek DE(keret-eldobhatóság) bitjét 1-be állítjuk. A maximális sebesség felett minden keretet eldobunk.

13.Lokális Hálózatok (Local Area Network - LAN)

A számítógép hálózatok klasszikus osztályozása:

WAN 802.1 – Wide Area Network – nagy kiterjedésű hálózat

- távolsági megkötés nélküli, tetszőleges kiterjedésű hálózat
- akár globális méretű is lehet

MAN 802.10– Metropolitan Area Network – városi/nagyvárosi hálózat

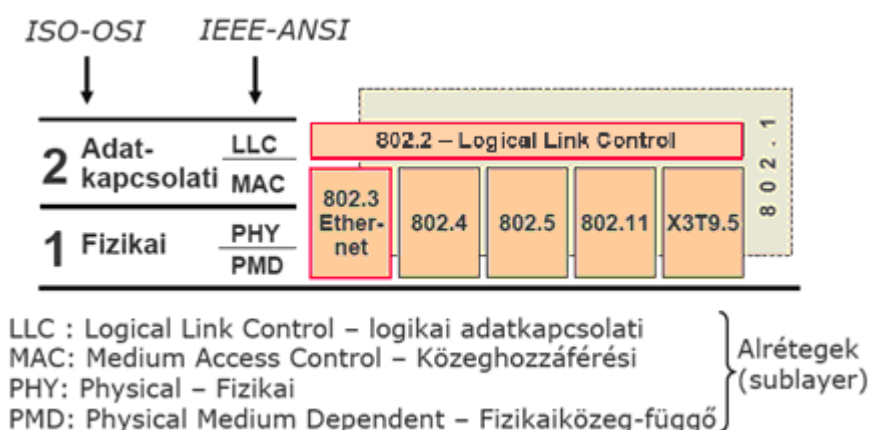
- eredetileg: egy tipikus USA-beli metropolitan area, de nem feltétlenül város
- néhány tíz km

LAN 802.3 (vezeték nélküli LAN 802.11)– Local Area Network – helyi v. lokális hálózat

- tipikusan vállalaton, intézményen belüli hálózat
- max. néhány km-es távolságok

PAN 802.15– Personal Area Network – személyi hálózat

Lokális hálózatok architektúrája:



Az Ethernet (IEEE 802.3)

Az Ethernet napjaink legelterjedtebb adatkapcsolati szintű technológiája. Rendkívül elterjedt helyi hálózati technika, amely 10 Mbit/s névleges átviteli sebességet biztosít koaxiális kábelben. Az Ethernet jelzőt sokan általánosságban az összes CSMA/CD alapú eljárás megnevezésére használják. Az Ethernet az OSI hivatkozási modell két legalsó rétegét kielégítő protokoll gyűjtemény.

Jelölésrendszer:

A	B	C
10	Base	5
1000	Broad	-T

A: adatsebesség [Mbit/s]

B: Base = alapsávi, Broad = szélessávú átvitel

C: Átviteli közeg (T2 – 2 Twisted Pair, stb), Szegmenshossz

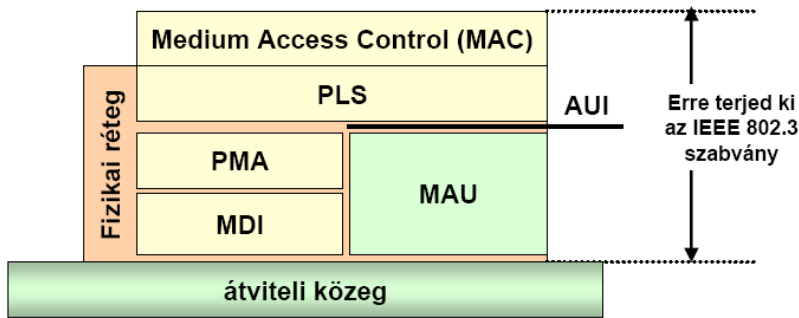
Kábelezési megoldások:

„Eredeti” vastag (yellow) kábeles (10Base5)

Vékony kábeles (10Base2)

Aktív hubos (10BaseT)

Fizikai réteg – architektúra:



PLS Physical Signalling Sub-layer

AUI Attachment Unit Interface

PMA Physical Medium Attachment

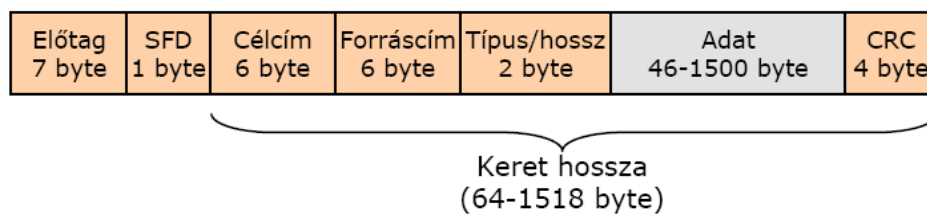
MDI

MAU

Medium Dependent Interface

Medium Attachment Unit

Medium Access Control (MAC) – az Ethernet-keretek felépítése



- SF: keret kezdete (1 byte)
- Típus/hossz (2 byte): az adatmező típusa és hossza
- CRC - ellenőrző összeg (4 byte)

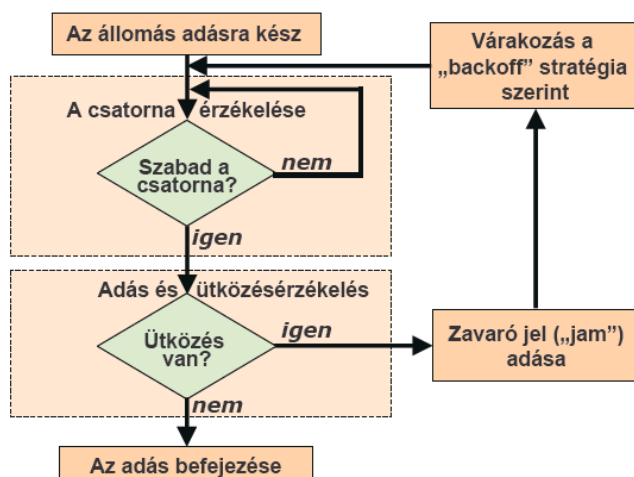
Min. csomaghossz, „résidő”: az ütközések biztos érzékeléséhez:

Legkedvezőtlenebb esetben is (két állomás a busz két végén) minden állomás érzékeli az ütközést

$$T = \frac{C}{2L}$$

L: szegmens (busz) hossza C: jelterjedési sebesség T: „résidő”

Medium Access Control - CSMA/CD:



Az állomás figyeli a csatornát, a „vivőt” (carrier sense), ha nem érzékel adást, elkezd küldeni a keretet.

Ha kettő vagy több állomás ad, mindegyik abbahagyja az adást (ütközésetekció - collision detection), valamekkora (véletlen) késleltetést („backoff” time) követően az állomás újból megkísérli az adást. A CSMA/CD-hoz szükséges, hogy:

adás előtt vivőt érzékeljünk (carrier sensing - CS)
adás alatt érzékeljünk, hogy más is ad (collision detection - CD)

Példa: *A* és *B* egy-egy hálózati interface. *A* elkezd adni, *B* áll. *B* megvizsgálja a közeget, de *A* adása még nem ért el *B*-hez (szabadnak látja a csatornát), ezért elkezd *B* is adni. A hálózat jelterjedési idején belül *B* észleli *A* adását, de *A* még nem kapta meg *B* adását, így az nem tud az ütközésről. *B* folytatja az adását egy **32 bites JAM** – zavaró jellel, amelyet mindenki megkap a hálózatban. A hálózati elemek ezt a *B*-től kapott csomag **32 bites CRC** mezőjének helyén kapják meg (a keret végén), így CRC-error miatt mindenki eldobja *B* keretét. Az ütközés észlelése után *A* is elküld egy JAM – zavaró jelet.

Megj: Slideokban a JAM:

„Jam (zavarás): 48 bitnyi ideig, hogy minden állomás biztosan érzékelje az ütközést.”

Kapcsolt Ethernet:

Nagyobb forgalom kezelése a buszsebesség növelése nélkül.

Ethernet-kapcsoló (switch), több vonali kártyával. Ld. majd: LAN-ok összekapcsolása

Nagysebességű Ethernet szabványok:

Fast Ethernet IEEE 802.3u:

Minden gyors Ethernet kapcsolt, UTP vagy üvegszál.

Gigabit Ethernet IEEE 802.3z:

- Megőrizték a 802.3 keretformátumot. Lefelé kompatibilis a klasszikus és a gyors Ethernettel
- Rézvezeték és üvegszál
- Manchester helyett 8B/10B kódolás
- Félduplex működés: még mindig CSMA/CD
- Duplex működés: Egyidejű kétirányú adás-vétel → Nincs ütközés
- Felhasználás:
 - Nagyforgalmú „dedikált” állomások (szerverek)
 - Gerinchálózat
- Flow Control – forgalomszabályozás - Opcionális flow control a vételi puffer túlsordulásának elkerülésére
- 802.1Q szerinti VLAN-ok kezelése itt jelent meg először mint lehetőség (VLAN = virtuális LAN)

„Félduplex” üzemmód (megnyújtott keretformátum):

Mint a klasszikus Ethernet (CS, CD), de sokkal rövidebb keretidők

Két megoldási lehetőség:

- Megnövelt kerethossz
- „Carrier-extension” bitek hozzáadása a keretekhez → Ezt választották, mert ezzel nem változott a szabvány

Frame bursting: másik lehetőség az adási időszak megnyújtására

Az állomás (rövid) csomagok sorozatát küldheti el anélkül, hogy egy adott burst időkorlátig, anélkül, hogy elengedné a csatornát („jumbo” keret)

- A keretek közé „interframe”-eket kell elhelyeznie
- Az időkorlát leteltekor az utolsó keretet befejezheti

További lokális hálózatok:

Token Ring - IEEE 802.5:

- Gyűrű topológia - látszólag csillag
- Sodrott érpáras kábel
- Differenciális Manchester-kódolással
- Minden állomás aktív ismétlő
- MAC (közeghozzáférés vezérlés):
 - TOKEN (vezérjel) segítségével

A tokenes protokoll működése:

Az állomások tétlensége esetén, a vezérjeles gyűrűn egy speciális bitminta, a **vezérjel (token)** jár körbe. Amikor egy állomás keretet akar küldeni, akkor még az adás megkezdése előtt meg kell szereznie a vezérjelet, és el is kell távolítania azt a gyűrűből. Mindezt úgy teheti meg, hogy a 3 bájtos vezérjel egyik bitjét invertálja, és e három bájtot az elküldendő normál adatkeret első 3 bájtjává változtatja. A címzett beolvassa a neki szóló csomagot, a küldő kivonja a saját csomagját, majd új token-t enged el.

Token bus: IEEE 802.4:

Fizikai sintonológián - logikai gyűrű, az állomások duplán láncolt listán. Ma már nem létezik.

FDDI - Fiber Distributed Data Interface:

- A LAN-okhoz képest nagyobb sebességgel és területi lefedéssel (100 Mbit/s, 100 km)
- Tokenes közeghozzáférési protokoll
- Logikai gyűrű, fizikai gyűrű- és fa-topológia
- Az átviteli közeg üvegszál és a gyűrű egy öngyógyító kettős gyűrű

Működése:

A token-t lefogó állomás az adatállomány elküldése után rögtön elindít egy új token-t, amit az állomány megérkezése előtt is lefoglalhat egy másik állomás → Egyszerre több állomástól származó adat is lehet a gyűrűn.

A „timed token ring” protokoll:

TRT (Token Rotation Time) = a gyűrű teljes késleltetése + adási idők

Gyűrű késleltetése = állomások késleltetése + terjedési késleltetés

Limitálni kell mindkettőt :

Egy állomás maximális késleltetése = 600 ns (szabvány)

Terjedési késleltetés: 5 μ s/km

Példa: 1.6 ms késleltetés = 0.6 ms + 1 ms

→ 1000 (0.6 ms / 600 ns) állomás és max. 200 km (1 ms / 5 μ s) kábel

T_{opr} (Token OPeRative) = TTRT (Target TRT - megcélzott TRT)

Szinkron/aszinkron FDDI:

Némelyik állomás adási “kvótával” rendelkezik

- A hozzá érkező tokent a kvóta idejéig megtarthatja, ezalatt adhat
- Ez a „szinkron” forgalom

A kvótán felül csak akkor adhat egy állomás, ha a $TRT < T_{opr}$

- Ez az „aszinkron” adás

802.2 – Logical Link Control

Feladatai:

- A 3. rétegbeli protokoll számára megbízható átvitel biztosítása
- Forgalomvezérlés
- Hibaérzékelés, -javítás
- Nagymértékben épít a HDLC-re (Magasszintű adatkapcsolat vezérlés)

Szolgáltatások:

- Nyugtázatlan, összeköttetés nélküli (datagram)
- Nyugtázott, összeköttetés nélküli (datagram)
- Nyugtázott, összeköttetés-alapú

Nem biztos, hogy szükség van LLC-re (pl. az IP nem igényli) Protokoll-overhead: a MAC-kerethez LLC fejléc adódik hozzá

LAN-ok összekapcsolása

A LAN-ok korlátai:

- távolság
- állomások száma → Megoldás: Átjátszók
- állomások típusa

Bridge-ek és switch-ek - Hidak és kapcsolók:

Mindkettő LAN-szegmenseket köt össze, az adatkapcsolati rétegben. Először volt a híd, aztán a kapcsoló a LAN-okban, a kapcsolt Ethernetben.

A híd elvileg LAN-szegmenseket köt össze, a kapcsoló portjaira gyakran egyedi munkaállomások csatlakoznak. A híd elvileg képes különböző LAN-okat összekötni, pl. Ethernetet token ringgel, de ennek ma már nincs jelentősége.

Switch - kapcsoló:

Adatkapcsolati rétegbeli eszköz, ami

- tárolja és továbbítja az Ethernet-kereteket
- megvizsgálja a keretfejrészt és szelektíven továbbítja a keretet a MAC célcím alapján, amennyiben a keretet a saját szegmensre kell továbbítani, CSMA/CD-t használ
- transzparens → a végpontok nem tudnak a kapcsolók jelenlétéről
- plug-and-play, self-learning → a kapcsolókat nem kell konfigurálni

A kapcsolók felépítése:

- Kapcsolómátrix
- Nagysebességű hátlap (1 Gbit/s)
- Vonali kártyák (4-32 db) - Kártyánként 1-8 port

Működés:

- A kártya portjai belső LAN-okat alkotnak, minden port egy ütközési tartomány (CSMA/CD).
- A kapcsoló belsejében nincs ütközés.
- Portok pufferelek, képesek a duplex működésre.

Manapság:

- Több Gbit/s átvitel
- Integráltak

Kapcsolótábla feltöltése - öntanulás:

- Bejegyzés a táblában: MAC Address, Interface, Time Stamp
- Megtanulja, hogy melyik végpontokat melyik interfészen keresztül tudja elérni
- Amikor vesz egy keretet, megtanulja azt, hogy hol, melyik szegmensen van a küldő
- Bejegyzik a küldő/szegmens párokat a táblába
- Ha nincs bejegyzés az adott MAC-címre → elárasztás

Vezeték nélküli LAN-ok – WLAN (IEEE 802.11 család)

*Pár száz méter, 1-2 Mbit/s - 100 Mbit/s, a 2.4 GHz-es ISM sávban.
Épületeken belüli LANok*

Direct Sequence Spread Spectrum – DSSS:

A DSSS (Direct Sequence Spread Spectrum) kódolásnál minden átvinni kívánt bitet egy redundáns bitmintával helyettesítenek. Minél hosszabb ez a bitminta, annál nagyobb a valószínűsége, hogy az átviteli torzulások ellenére az eredeti jel helyreállítható. Illetéktelen megfigyelő számára a DSSS jel szélessávú kisenergiájú zaj. A legtöbb vezeték nélküli LAN eszközöket gyártó cég a DSSS eljárást választotta a kódoláshoz.

Frequency Hopping Spread Spectrum – FHSS:

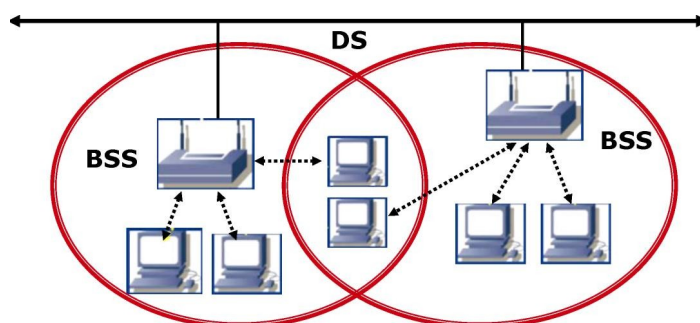
Az FHSS (Frequency Hopping Spread Spectrum) kódolásnál egy keskenysávú vivőt használnak, aminek pillanatnyi frekvenciáját egy adott minta szerint változtatják. Ezt a kódmintát ismeri az adó és a vevő is. Megfelelő szinkronozás esetén az adó és a vevő között létrejön a logikai csatorna. Illetéktelen megfigyelő számára az FHSS jelek kisenergiájú impulzus zajnak látszanak.

Orthogonal Frequency Division Multiplexing – OFDM:

A sáv felosztása sok részsávra, ezekben továbbítjuk a párhuzamosított jelfolyamot. A spektrum hatékony kihasználás: „ortogonális” vivőkkel

A sávok nem diszjunktak, a spektrumok „össze vannak tolva”, egymásba átlógnak, viszont szétválaszthatók, mert eleget tesznek az időtartományban megismert Nyquist-elv frekvenciatartománybeli megfelelőjének

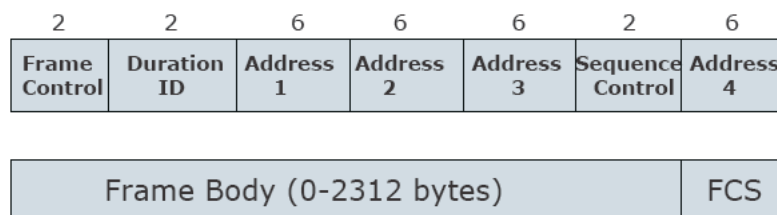
WLAN-ok topológiája:



- Basic Service Set (BSS) – egy cella
- Extended Service Set (ESS) – több cella
- Distribution System (DS) – elosztóhálózat (gerinc)

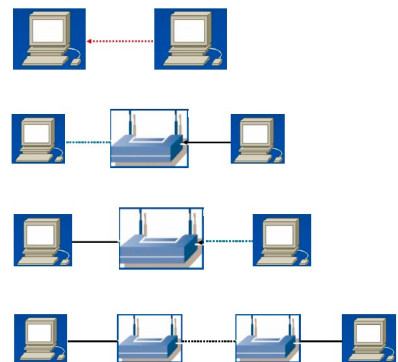
A WLAN-ok és Vezetékes LAN-ok Wireless Access Point-on keresztül kapcsolódnak.

802.11 keretformátum:



Miért van 4 címmező?

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	Sending AP	SA	N/A
1	0	Receiving AP	SA	DA	N/A
1	1	Receiving AP	Sending AP	DA	SA



DS: Distribution System DA: Destination Address (Célcím)
 BSSID: Basic Service Set ID SA: Source Address (Forráscím)

DS: 0 – vezetékes, 1 – vezeték nélküli

802.11 MAC-réteg Hozzáférési módszerek:

Carrier Sense Multiple Access/Collision Avoidance - CSMA/CA

- Vezeték nélküli LAN-okban nem lehet ütközést detektálni (Az állomások nem képesek észlelni a máshonnan érkező jelek által létrehozott ütközést)

Két hozzáférési módszer:

Distributed Coordination Function (DCF):

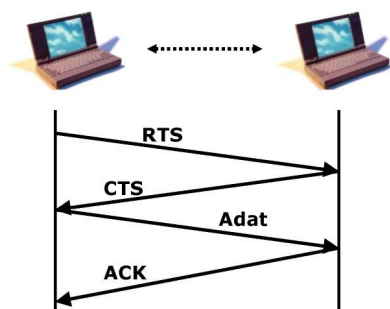
A MAC alsó alrétege

Collision Avoidance - Ütközés-elkerülés

Különböző értékű IFS-ek (InterFrame Space)

Ha a csatorna szabad, az állomás vár, hogy szabad marad-e IFS ideig. Ha igen, ad.

Ha a csatorna foglalt (vagy már az elején, vagy azzá válik az IFS alatt), az állomás tovább figyel. Amikor a csatorna szabaddá válik, az állomás vár IFS ideig, majd egy véletlen késleltetést választ. Amikor az letelik, megkezdje az adását.



Handshaking - opcionális eljárás:

- Request To Send (RTS)
- Clear To Send (CTS)
- Acknowledgement (ACK)

Erőforrásokat igényel, és jelentős késleltetést visz be.

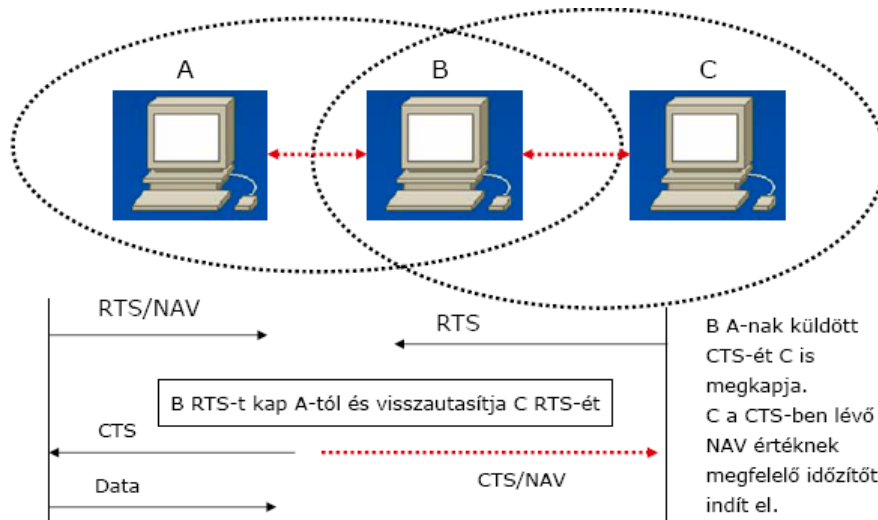
Akkor kell használni, amikor nagy verseny van a hálózaton.

Network Allocation Vector (NAV):

Minden RTS keret tartalmazza azt az időt, ameddig az állomás el akarja foglalni a csatornát. NAV: számláló a többi állomásnál, amelyeknek NAV ideig várniuk kell, mielőtt megnéznék, hogy a csatorna szabad-e.

Rejtett állomás problémája: A kommunikál B-vel. C nem tud erről, ezért ő is elkezd B-nek üzeneteket továbbítani. Ez B-nél ütközéshez vezet.

Megoldás:



Egy csatorna lehet fizikailag foglalt (az állomás foglaltnak érzékeli a rádiócsatornát), és virtuálisan foglalt (az állomás RTS-t vagy CTS-t vesz, amely jelzi hogy a csatorna foglalt lesz a NAV időtartamán)

Point Coordination Function (PCF):

- Opcionális és ha van, a DCF „felett”, azzal együttesen valósítják meg
- Egyetlen AP vezérli a hozzáférést
- Az AP által küldött jelzőüzenet (beacon) hatására az állomások beszüntetik a DFC működést
- Az AP lekérdezi sorban az állomásokat → Garantált a maximális késleltetés
- Egy állomás csak akkor adhat, ha kérdezik
- Prioritásokat is lehet az állomásokhoz rendelni, így időérzékeny alkalmazások is támogathatók

A WLANok teljesítőképessége:

	802.11b	802.11a	802.11g
Elméleti maximális sebesség [Mbit/s]	11	54	54
UDP [Mbit/s]	7,1	30,5	30,5
TCP [Mbit/s]	5,9	24,4	24,4

14.BWA – Broadband Wireless Access -szélessávú vezeték nélküli hozzáférés

Wireless Personal Area Networks – WPAN – IEEE 802.15.1 (Bluetooth)

Alapja a Bluetooth specifikáció

- Bluetooth: az Ericsson kezdeményezése 1998-1999-ben, majd csatlakozott az IBM, Toshiba, Nokia, Intel,...
- Bluetooth SIG (Special Interest Group)

Célkitűzések:

- olcsó eszközök (1-2 cm-es modul, pár \$)
- rövidtávú kommunikáció (10 m)
- max. 1 Mbit/s

A Bluetooth alkalmazása:

Bluetooth a mobilban: telefonhívások „least-cost routing”-gal

- telefonhívás házon belül a mobilról, de Bluetooth-kapcsolat segítségével a vezetékes telefonról

Internet-elérés mobilról és PDA-ról

- Bluetooth-csatlakozás a notebookhoz, vagy desktop-hoz, ami LAN-ra vagy WLAN-ra csatlakozik, vagy ADSL-lel a nyilvános hálózaton keresztül

Vezeték nélküli csatlakozások széles köre

- Fejhallgató (headset), mobil kihangosító az autóban, fényképezőgép és notebookm ...

A rádiós interfész paramétereit:

- 10 m, 1 mW telj. (opcionálisan: 100 m, 100mW)
- A 2,4 GHz-es ISM-sávban
- 3 db duplex 64 kbit/s-os hangcsatorna, 1 Mbit/s adatcsatorna
- Frekvencia-ugratás, 1600-szor mp-nként, álvéletlen jelsorozattal a kb. 2,4 GHz-nél kezdődő 79 MHz-es sávon belül, 79 x 1 MHz
- TDD, 625 µs-os időrések, adás-vétel idGben egymás után, felváltva

Hálózatszervezés & kommunikáció: Piconet

legfeljebb 8 állomás: 1 master, a többi slave

Scatternet: piconet-ek hálózata, dinamikus, ad-hoc alapon

Van olyan node, amely >1 piconet-hez tartozik

A Bluetooth nem rendelkezik a scatternet-ek kiépítésének módjáról

Szinkronizációs eljárás az elején, a slave-ek megtudják a master azonosítóját, és órájukat összevetik, hogy képessé váljanak a közös frekvenciaugratásos sorozat előállítására

A master megmondja, hogy melyik slave melyik időrésben

Hívásfelépítés az inquiry és page eljárásokkal:

- Inquiry: megtudni, hogy mik a további Bluetooth-eszközök a hatótávolságon belül
- Page: felépíteni a kapcsolatot

Kétféle összeköttetés:

- SCO (Synchronous Connection Oriented) – hangátvitel, előre lefoglalt időrések
- ACL (Asynchronous Connectionless) - adat

Architektúra

Saját rétegzett architektúra

- „Transport protocols” és a magasabb rétegbeli protokollok („middleware protocols”)
- „Transport protocols”
 - Radio (fr. sáv, rádiós jellemzők, adatsebességek, duplexelés, FH jellemzők)
 - Baseband (hálózatszervezés és kommunikáció)
 - Link manager protocol (authenticáció, titkosítás)
 - Logical Link Control & Adaptation Protocol (LLCAP) – csomaginterfész a felső rétegek felé

Middleware protocols

- SDP - Service Discovery Protocol
- RFCOMM – soros interfész (RS232)
- TCS – Telephony Control Signaling: modem vezérlő jelek

Nagysebességű PAN-ok -> IEEE 802.15.3

Célkitűzés: médiakommunikáció

- digitális kamera – tv, MP3 ide-oda, videójátékok

Új PHY specifikáció 55 Mbit/s-ig (11,22,33,44,55 Mbit/s), kb. 10 m-ig

Másik munkacsoport: még nagyobb sebességek (110, 200, 480 Mbit/s) – házimozik, játékok

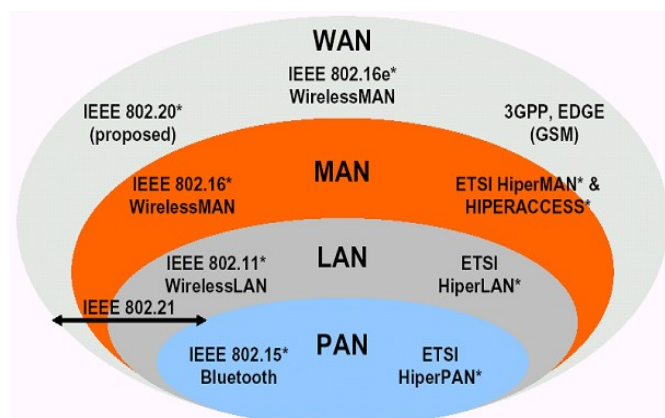
A rádiós rétegre több lehetőség, a legígéretesebb az UWB

UWB – Ultra-WideBand

- Igen nagy sáv szélesség, sokkal nagyobb, mint a CDMA-nál
- Nincs vívő, igen rövid (pár ns) impulzusok, kis teljesítmény, nincs azonos csatornás zavar
- FCC (USA) a 3,1...10,6 GHz-es sávban engedélyezi, feltéve, ha UWB, azaz ha a relatív sáv szélesség nagyobb, mint 0.2
- ETSI, CEPT (Európa) hasonlóan
- MAC: fejlesztés alatt, megoldandó problémák (pl. nem lehet üres csatornát érzékelni)

Nagyvárosi vezeték nélküli hálózat

- WMAN – Wireless Metropolitan Area Network – IEEE 802.16
- WiMAX - Worldwide Interoperability for Microwave Access



WLAN: IEEE 802.11x

- Wi-Fi – WiFi Alliance (Wi-Fi – „wireless fidelity” a Hi-Fi mintájára)

WMAN: IEEE 802.16x

- WiMAX – WiMAX Forum – „Worldwide Interoperability of Microwave Access”

Wi-Fi Alliance és WiMAX Forum: együttműködés a gyártók és a piac más szereplői között

- a technikák bevezetésére,
- a szabványokkal való kompatibilitás tanúsítására
- a különböző gyártók közötti együttműködés tanúsítására

LOS környezet (Line of Sight)

- Közvetlen rálátás
- Nincs takarás a Fresnel-zónában

NLOS környezet (No Line of Sight)

- Nincs közvetlen rálátás, reflektált hullámok, több jelút
- A WiMAX-ban: speciális technika a reflektált hullámok felhasználásával történő vételre, ha nincs is direkt út
- Terjedés városi környezetben

A WiMAX alkalmazási lehetőségei

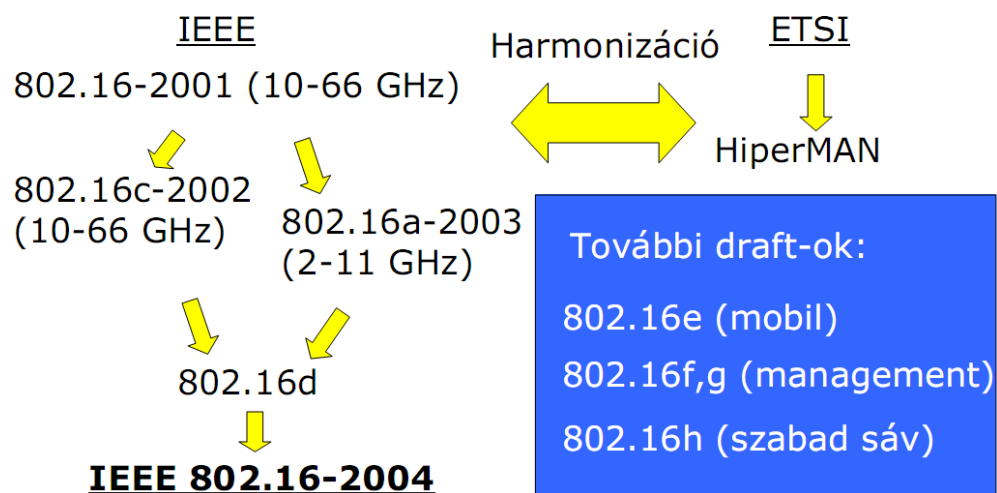
WiMAX szolgáltatók

- új belépők,
- a területen már jelen lévő, inkumbens szolgáltatók lehetnek.
- mobil szolgáltatók, amelyek a meglévő infrastruktúrájukkal összhangban használják a WiMAX-ot.

A WiMAX alkalmazási területei:

- a meglévő vezetékes infrastruktúra kiegészítése,
- olyan helyeken, ahol technológiai, gazdasági akadályai vannak a vezetékes szélessávú elérési hálózat további bővítésének, vagy a szabályozási helyzet nem teszi lehetővé. (pl. konkurens helyi szolgáltató – LTO - területe),
- vezetéknélküli szélessávú hozzáférés biztosítására, vezetéknélküli „hot-spot”-ok, „hot-zone”-ok kiépítése.

Szabványok, Verziók



A WiMAX működése

Fizikai réteg : OFDM

- Ortogonális frekvencia multiplexálás
- Többvivős modulációs/multiplexálási technika
- A rendelkezésre álló sávszélességet alvivőkre osztják
- A felhasználói adat soros-párhuzamos átalakítás és szimbólumformálás után külön alvivőkön kerül továbbításra
- Többutas terjedés (ISI) ellen védőidő alkalmazása
- A több ivő miatt ellenáll a frekvencia-szelektív elhalkulásnak
- Alvivők: Ahol az egyik vivőnek maximuma van, ott a többi vivő eltűnik.
Vivők közötti távolság $\Delta f = 1/T_s$

Időosztásos duplex (Time Division Duplex – TDD)

- Ezt az esetet más néven félduplex (half-duplex) kapcsolatnak is szokták nevezni. Ekkor egyetlen egy csatorna áll rendelkezésre a kommunikációhoz, ez időben megosztva használják a kommunikáló felek.

Frekvenciaosztásos duplex (Frequency Division Duplex – FDD)

- Az előbbi esettel ellentétben nem egy csatornát – frekvenciát – használunk a kommunikációra, hanem két egymástól eltérő – WiMAX esetén 50 vagy 100 MHz-re lévő - frekvenciát. Ekkor tehát valódi duplex (full-duplex) módról beszélhetünk.

Frekvenciasávok:

3,4 – 3,6 GHz (ETSI) EU – QoS garantált

5,7 – 5,8 GHz (U -NII) – egyelőre csak katonai célokra, QoS nem garantált

MAC réteg

Közeghozzáférési mechanizmus biztosítása

Topológia

- kétirányú PMP (pont-multipont)
- „mesh”-módot definiálja.

Kapcsolatorientált

- Kapcsolat-azonosító (Connection ID - CID), mely 16 bites
- Előfizető (Subscriber Station - SS) azonosítása
- 48 bites MAC címmel

További funkciók

- Címzés
- MAC header illetve PDU kialakítása
- Fragmentáció
- Ütemezési feladatok
- Sávszélesség-allokálás
- PHY réteg támogatása (duplexálási technikák)

Forgalmi paraméterek és előírások

MIR – Maximum Information Rate, Maximum Reserved Traffic Rate, Maximum Sustained Traffic Rate, Excess Burst

- Ez az érték felülre korlátozza egy forgalom adatsebességét annak érdekében, hogy a korlátozott csatorna kapacitás miatt ki ne szorítson más forgalmat. Értékét bit/s-ban kell megadni.

CIR – Committed Information Rate, Minimum Reserved Traffic Rate, Committed Burst

- Ezzel az adott forgalom átlagos adatsebességét definiáljuk. Sok kis forgalom ingadozása – forgalomtípus esetén ezzel jól lehet számolni. Értéke bit/s-ban értendő.

CT – Committed Time, Polling Time Interval, Unicast Polling

- Maximum ilyen időközönként kerül frissítésre a sáv szélesség igény – csatorna idejének/frekvenciájának felosztása – a tényleges forgalomnak megfelelően. Egyúttal ez jelenti azt is, hogy milyen időtartamra történik az átlagolás a CIR és MIR kiszámításánál. A paraméter gyakran csak rövid, közepes vagy hosszú értékeket vehet fel, melyekhez a később bemutatott forgalmi osztálytól függően más-más időértékek tartoznak. Tipikusan 50-1000 ms.

Prioritás – Traffic Priority

- Azonos forgalmi osztályon belül az egyes forgalmakat prioritizálásukkal elgynyben lehet részesíteni. A prioritás érték 0-7 közötti egész lehet.

Késleltetési ingadozás – Normal Grant Jitter, Tolerated Jitter (jitter = delay variation)

- Megadja, maximum mekkora késleltetési ingadozás megengedett. Értékét ms-ban kell megadni.

Maximális késleltetés – Maximum latency

- A ms-ban megadott értéket nem meghaladó késleltetést kell biztosítani a forgalom számára.

Megengedett méret – Unsolicited grant size

- Azt határozza meg, hogy tipikusan milyen méretűek a csomagok.

Forgalmi osztályok

UGS – Unsolicited Grant Service, Continuous Grant (CG)

- Olyan valósidejű szolgáltatások számára alkalmas, melyek konstans adatsebességet igényelnek, konstans méretű csomagokkal kommunikálnak. Tipikusan ilyen lehet egy beszédcsatorna – VoIP – vagy CBR – constant bit rate – videóátvitel. ATM és E1 vonalak helyettesítésére is jól használható.

rtPS – real-time Polling Service, RT-VR – Real Time Variable Rate

- Olyan valósidejű szolgáltatások esetén érdemes ezt az osztályt használni, ahol bár nem konstans az adatsebesség, mégis valósidejűséget kell biztosítani. Ide tartoznak azok az ingadozó adatsebességű – VBR, Variable Bit Rate – alkalmazások, melyek tipikusan egyes tömörített hang- és videó-adatfolyamok. Pl: MPEG

nrtPS – non-real-time Polling Service, NRT-VR – Non Real Time Variable Rate

- Azon forgalmak sorolhatók ide, melyekre nem kell valósidejűséget biztosító garanciát vállalni, de mégis egy adott sáv szélességet kívánunk számukra allokálni. Ilyen lehet egy internetes böngészés, letöltés, ahol a szolgáltató minden esetben biztosítani kíván egy minimális sáv szélességet a felhasználók számára.

BE – Best Effort

- Hasonló az nrtPS osztályhoz, de itt semmilyen garancia sem biztosított. A rendszer ezen forgalmakat a többi QoS osztálybeli által meghagyott, fennmaradó sáv szélességben próbálja kiszolgálni.

Összeszedve:

<i>Paraméter</i>	<i>QoS osztály</i>			
	UGS	rtPS	nrtPS	BE
MIR	(✓)	(✓)	✓	✓
CIR	✓	✓	✓	
CT		✓	✓	✓
Tolerated jitter	✓			
Maximum latency	✓	✓		
Traffic priority			✓	✓
Unsolicited grant size	✓			

Table 4- Comparison of WiMax and Wi-Fi Technologies			
	WiMax (802.16a)	Wi-Fi (802.11b)	Wi-Fi (802.11a/g)
Primary Application	Broadband Wireless Access	Wireless LAN	Wireless LAN
Frequency Band	Licensed/Unlicensed 2 G to 11 GHz	2.4 GHz ISM	2.4 GHz ISM (g) 5 GHz U-NII (a)
Channel Bandwidth	Adjustable 1.25 M to 20 MHz	25 MHz	20 MHz
Half/Full Duplex	Full	Half	Half
Radio Technology	OFDM (256-channels)	Direct Sequence Spread Spectrum	OFDM (64-channels)
Bandwidth Efficiency	≤5 bps/Hz	≤0.44 bps/Hz	≤2.7 bps/Hz
Modulation	BPSK, QPSK, 16-, 64-, 256-QAM	QPSK	BPSK, QPSK, 16-, 64-QAM
FEC	Convolutional Code Reed-Solomon	None	Convolutional Code
Encryption	Mandatory- 3DES Optional- AES	Optional- RC4 (AES in 802.11i)	Optional- RC4 (AES in 802.11i)
Access Protocol	Request/Grant	CSMA/CA	CSMA/CA
- Best Effort	Yes	Yes	Yes
- Data Priority	Yes	802.11e WME	802.11e WME
- Consistent Delay	Yes	802.11e WSM	802.11e WSM
Mobility	Mobile WiMax (802.16e)	In development	In development
Mesh	Yes	Vendor Proprietary	Vendor Proprietary

15. Internet Protocol – IP

Az a ragasztó, amely az Internetet egybetartja, az IP (Internet Protocol - hálózatközi protokoll). Ez a protokoll gondoskodik a csomagok átviteléről a hálózaton. Az összes kommunikáció a hosztok között IP csomagok formájában történik. Ez egy kapcsolat nélküli protokoll, azaz a kommunikációhoz nem szükséges előzetes kapcsolatfelvétel. Ebből adódik, hogy tartalmaznia kell a kézbesítéssel összefüggő információkat, a teljes és pontos címet. Adátvitel szempontjából nem megbízható, a csomagokkal bármi megtörténhet: elveszhetnek, megsérülhetnek, sorrendjük összekeveredhet.

TCP/IP architektúra:

ISO/OSI	TCP/IP	Gyakorlatias
Alkalmazás	Alkalmazás	Alkalmazás
Megjelenítési		
Viszony	Szállítási / Host-to-host (TCP/UDP/...)	TCP/UDP/...
Szállítási	Internet (IP)	IP
Hálózati		LLC
Adatkapcsolati	Hálózati interface/ Hálózati hozzáférési	MAC
Fizikai		PCS & PMA
		PMD

Az IP feladata:

Adattovábbítás a hálózat végpontjai között

- Címzés (addressing) és forgalomirányítás (routing)
- Tördelés/fragmentálás (fragmentation)

NEM feladata:

- Torlódáskezelés
- Ütemezés
- Titkosítás és hitelesítés

Címzés:

Az IP-cím felépítése:

4 bájtos cím (32 bit) $\rightarrow 2^{32} \approx 4 \cdot 10^9$

Cím = Hálózatazonosító + Egyedi azonosító

Jelölések:

- Bináris: 10110000 10010011 00111110 11100001
- „Dotted decimal”: 176.147.62.225

Címosztályok:

Az IP-címeket kezelő szervezet (IANA: Internet Assigned Numbers Authority) osztja ki

	0	1	2	3	4	8	16	24	31	
A	0					Network ID				Host ID
B	1	0				Network ID				Host ID
C	1	1	0			Network ID				Host ID
D	1	1	1	0		Multicast address				
E	1	1	1	1	0	Reserved				

A és B osztályú címeket országok, egyetemek, ISP szolgáltatók kapnak
A, B, C osztályú címek egyedi címzésre
D osztály: multicast címzés
E osztály: fenntartott címtartomány

A – 0... B – 128. ... C – 192. ... D – 224. ... E – 240. ...

Előtag: Ez azonosítja a címosztályt. A címosztály mutatja meg, hogy az előtag után hány bitet kell hálózati címként, és hány bitet kell hosztcímként értelmezni.

Hálózati cím (Network Address): Az egyes hálózatok megkülönböztetésére szolgál, valamint a központi adminisztrációt segíti elő, azaz ne lehessen két gépnek azonos IP-címe. A hálózati címet központilag kell igényelni, és központilag utalják ki az igénylőnek.

Host Address: A 32 címbit maradékát teszi ki. Ezt szabadon állíthatja be a címtartományt igénylő a saját gépein.

Speciális címek:

- Host ID csupa 0: Hálózat címe, amit az adott hálózat eszközei opcionálisan kezelhetik
- Host ID csupa 1: Broadcast cím - A hálózaton mindenkinek szól
- 127.0.0.0 - 127.255.255.255: Loopback cím, a helyi gépet azonosítja
- Léteznek privát IP-címtartományok, csak helyi hálózaton (Interneten nem) érvényes címek.

Címosztályok általánosítása:

Subnetting:

Alhálózatokra osztás vagy aggregálás

- 1 db A osztályú → 256 db B osztályú
- 1 db B osztályú → 256 db C osztályú

CIDR - Classless Inter-Domain Routing:

A módszer lényege, hogy a router-ekben egy bejegyzés nem csupán egy, hanem több hálózat felé való továbbítási irányt írjon le. Azaz a célpontok ne egyes hálózatok, hanem hálózatok csoportjai legyenek. Így az azonos irányba eső hálózatok egy bejegyzésben megjeleníthetők és nem kell mindegyikhez külön-külön letárolni a továbbítási irányt.

Alhálózati maszk:

	0	1	2	3	4	N	31	
IP-cím						Network ID		Host ID
Alhálózati maszk						111...111		000...000
Hálózatazonosító						Network ID		000...000

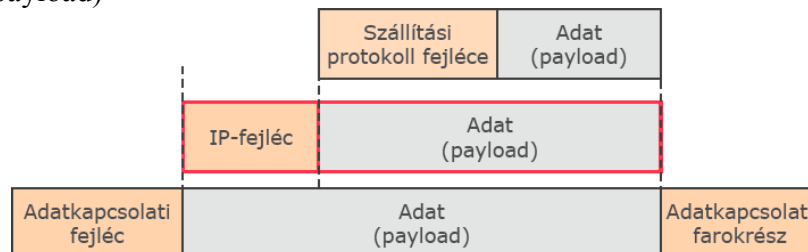
Bitenkénti **ÉS**

Jelölés a hálózat egyértelmű azonosítására: <hálózat IP-címe> / <alhálózati maszk egyeseinek a száma>

Az IP-csomag szerkezete

Az IP-csomag két része:

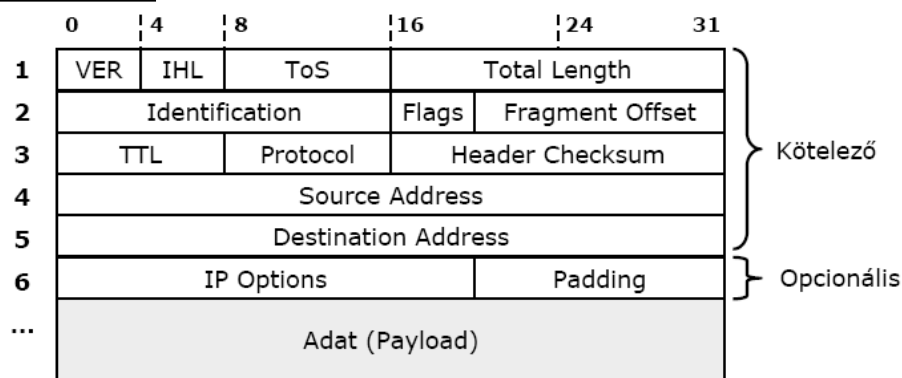
- IP-fejléc / fejrész (IP header)
- Adat (payload)



Az IP-csomag alsóbb rétegbeli protokoll adat részébe ágyazódik be.

Az IP-csomag adat részébe magasabb rétegbeli protokollüzenet (PDU) kerül.

Az IP-fejléc szerkezete:



VER - Version (4 bit): Az Internet Protocol verziójának száma

IHL - Internet Header Length (4 bit): Az IP fejléc mérete 32 bites egységekben
Minimum: 5 (20 byte) Maximum: $2^4 - 1 = 15$ (60 byte)

ToS - Type of Service (8 bit): QoS osztályok, paraméterek jelzésére

Total Length (16 bit): A teljes IP csomag mérete bájtokban

Minimum: 576 (IP-fejléc 20 + 512 adat + 44 IP-opciók és az alsóbb réteg fejlécei)

Maximum: $2^{16} - 1 = 65535$ (max. 65515 bájt adat)

Identification (16 bit): Az IP-töredékek egyedi azonosítása

Flags (3 bit):

- 0: Fenntartott/nem használt
- 1: DF - Don't Fragment – „Ne darabold”: routereknek szóló parancs
- 2: MF - More Fragment – „Több darab”: minden darabban, kivéve az utolsóban '1'

Fragment Offset (13 bit): Ez az adat mondja meg, hogy a töredék az eredeti datagram melyik része. Ez nélkül nem lehetne összerakni a csomagot.

TTL – Time To Live (8 bit): Csomag élettartama, minden továbbításnál csökkenteni kell ez értékét legalább 1-gyel. Ha a csökkentés után az értéke nem > 0 , akkor el kell dobni.

Protocol (8 bit): Az adat (payload) részben lévő protokoll azonosítója (ICMP/TCP/UDP/stb)

Header Checksum (16 bit): Az IP fejléc minden 16 bites szavának összegére számolt egyes komplementum. A csomag érkezésekor ellenőrizni kell a helyességét, és továbbítás esetén újra kell számítani (pl a TTL mező biztos változik)

Source / Destination Address (2 x 32 bit) Az IP-csomag feladójának és címzettjének az IP-címe

IP Options: Ritkán használt opcionális része a fejlécnek

Padding: az IP Options részt egészíti ki 32 bit többszörösére

IP – Útvonalválasztás:

„Hot potato”-elv:

- Minél gyorsabban továbbítsuk
- Csak a következő csomópont kell ismernünk (hop-by-hop)

Kinek küldjük tovább?

- Cél címe alapján → csomag tartalmazza
- Saját ismeret alapján → útvonal-irányítási táblázat (routing table)
 - Hova tart a csomag? Merre küldjük tovább?
 - Ki a következő csomópont? → Melyik interfészen keresztül?

Keresés az útválasztó táblában (általában bináris fában tárolják – $O(\log[\text{cím hossz}])$):

Ha a keresett cím több hálózatra is illeszkedik, akkor a leghosszabb egyezőséget kell választani! (leghosszabb hálózati maszk)

Alapértelmezett útvonal (Default route): Erre megy a csomag, ha nem ismeri a célhálózatot

Ez is elérhető megfelelő bejegyzéssel

Teendők helyi és távoli hálózat esetén:

Közvetlenül kapcsolódó (helyi) hálózat esetén a címzettnek közvetlenül küldeni.

Ehhez a címzett adatkapcsolati rétegbeli címére van szükség.

Nem közvetlenül kapcsolódó (távoli hálózat) esetén az útválasztónak kell küldeni.

Csak adatkapcsolati rétegben kell az útválasztónak címezni

Címet tilos módosítani.

Kapcsolat az adatkapcsolati címek felé

ARP – Address Resolution Protocol: IP címhez adatkapcsolati (fizikai) címet

Feladata a hálózati szinten lévő (IP) címeket a kapcsolati szint megfelelő címeivé alakítani. A hálózati szinten IP-címet használnak, de a kapcsolati és fizikai rétegben fizikai (kártya)címet kell használni.

Ha egy gép egy másikhoz akar kapcsolódni - amelyről tudja, hogy vele azonos alhálózaton van -, először egy cache-ben keresi a fizikai címet. Ha nem találja, akkor elküld egy üzenetszórásos(broadcast) ARP-kérélmeket tartalmazó keretet, amelybe beteszi a keresett IP-címét, a fizikai címnek hagy egy üres mezőt, majd beteszi a saját IP-címét és fizikai címét és megkérdezi, hogy ki is az XY IP-címmel rendelkező számítógép és mi az ő fizikai címe. Az üzenetet mindenki veszi, de csak az válaszol rá, aki az adott IP-cím tulajdonosa, az kitölti a fizikai címre szolgáló helyet, és visszaküldi a csomagot. Közben a csomagból ő is ki tudja venni a feladó IP-címét, és fizikai címét, és azt be tudja építeni a saját cache-be. Ezután a kezdeményező elhelyezi a címzettre vonatkozó információkat egy gyorsítótárba (ARP Cache) és legközelebb, ha ugyanazzal a címzettel akar kommunikálni, akkor már abból veszi az adatokat. A cache-ben lévő adatok pár percen belül elévülnek.

RARP – Reverse ARP: Adatkapcsolati rétegbeli címből IP-címet

Az előbbivel ellentétes folyamatot végez, vagyis a kapcsolati címeket, mint pl. egy Ethernet címet IP-címmé alakít át. A hálózati azonosítót kérő számítógép egy broadcast csomagban teszi közzé az adatkapcsolati címet, amely eljut a hálózaton levő RARP szerverhez. A szerver, amennyiben a kérő csomópont adatkapcsolati címe benne van a nyilvántartásban, a csomópontnak szánt hálózati címmel válaszol. Miután a válaszcsoport megérkezett, a hálózati cím felkonfigurálása után a kérő végpont megkezdheti az adatkommunikációt. A legfőbb probléma vele, hogy csak az adatkapcsolati rétegben tud működni, a hálózati rétegbeli eszközök nem továbbítják az adatkereteit, így minden hálózathoz szükséges egy RARP szerver üzemeltetése.

IP – Útvonalválasztó protokollok

Útválasztó protokollok feladatai:

- Útvonal-irányítási információk begyűjtése
- Hurokmentes útvonal-irányítás
- Újabb csomópontokat és hálózatok csatlakoztatásának biztosítása
- Csomópontok és hálózatok leválasztásának kezelése

Útválasztó protokollok:

Ad hoc routing protokollok:

Kis és gyorsan változó hálózatokra, szenzor és egyéb vezeték nélküli hálózatokra

- Distance-Vector (Távolság-vektor) módszer: (szomszédoknak mindenkiről)
- Link-State (Összeköttetés-Állapot) módszer: (mindenkinek szomszédokról)

Interior Gateway Protocols (IGPs):

- Autonóm rendszereken (AS) belül

Exterior Gateway Protocols (EGPs):

- Autonóm rendszerek (AS) között

Autonóm rendszerek

Egy autonóm rendszer a többi autonóm rendszer számára jelzi az általa képviselt csoport(ka)t

Az egész csoport egyetlen bejegyzés lesz az útvonal-táblában AS_3

IGP – Interior Gateway Protocol

EGP – Exterior Gateway Protocol. Már nem használt

BGP – Border Gateway Protocol. EGP helyett 1995 óta

Címaggregáció miatt gyorsabb keresés és terjedés

IP – Tördelés

Tördelés szükségessége:

Hálózatok alsóbb rétegei meghatározzák az általuk fogadható maximális keretméretet.

- Az adatkapcsolati réteg fej- és farokrészét leszámítva ez az MTU (Maximum Transmission Unit) (Ethernetnél 1500 byte)

Eltérő technológiák → eltérő MTU-jú kapcsolatok → tördelni kell

Tördeléssel kapcsolatos mezők az IP-fejlécben:

Tördelés után minden keletkezett csomag kap fejléct

Identification (16 bit): Az IP-töredékek egyedi azonosítása

Flags (3 bit):

- 0: Fenntartott/nem használt
- 1: DF - Don't Fragment – „Ne darabold”: routereknek szóló parancs
- 2: MF - More Fragment – „Több darab”: minden darabban, kivéve az utolsóban '1'

Fragment Offset (13 bit): Ez az adat mondja meg, hogy a töredék az eredeti datagram melyik (hányadik) része. Ez nélkül nem lehetne összerakni a csomagot.

IP-fejléc változása tördelés közben:

- Adat tördelése 8 bájt többszöröse méretű egységekre – a küldő, vagy egy router teheti ezt meg
- Ha nem volt Identification mező érték, akkor generálni kell
- A tördelésnek megfelelő „fragmentation offset”-et beállítani az új csomagokban
- Minden csomagban az MF bitet 1-re kell állítani, kivéve annak a csomagnak az utolsó töredékét, amelyben MF 0 volt.
- Total Length mező is változik, hisz a tördelt csomagok egymástól független csomagokká válnak, és kerülnek továbbításra (akár más útvonalon)
- Header Chechsum: minden töredékre újra kell számolni

A töredékek összeállítása:

- Csak a címzett végezheti el
- Ha valamely darab nem érkezik meg, akkor a többi is eldobja
- Csak teljesen összeállított csomagokat továbbít a felsőbb réteg felé

ICMP (Internet Control Message Protocol - Internet vezérlőüzenet protokoll):

Az Internet működését a routerek szorosan figyelemmel kísérik. Amikor valami váratlan esemény történik, azt az ICMP segítségével jelentik (hibaüzenetek, kérdések, válaszok). Az ICMP-t az Internet tesztelésére is használják. Körülbelül egy tucat ICMP üzenetet definiáltak.

IGMP - Internet Group Management Protocol: IP-t futtató csomópontok kezelésére.

IP – Ipv6 – A következő generációs Internet Protokoll

Az IPv4-gyel kapcsolatosan felmerült problémák:

- Kicsi a címtér. Pontosabban fogalmazva kevés a hálózati szám (32 bites).
- 4,3 milliárdból (minek 87,5% használható ki) 1,7 már ki van osztva
- A routing táblák túl nagy mérete (erőforrásigény)
- Kevés a lehetőség egy IP csomag tartalmának vagy feladójának hitelesítésére
- Nem vesz figyelembe olyan szempontokat, mint: mobilitás vagy autokonfiguráció
- Tördelés a köztes csomópontokban
- Mobilitástámogatás csak külön protokollal

IPv6 címek ábrázolása:

128 bites címek

8x16 bites hexadecimális számként ábrázolják

- FEDC:BA94:7654:3210:FEDC:BA98:7654:3210

A vezető nullák elhagyhatók:

- FEDC:0094:0004:0000:000C:BA98:7654:3210 → FEDC:94:4:0:C:BA98:7654:3210

A 16 bites nullákat tartalmazó részek kihagyhatók, ha egymás után vannak (maximum egy ilyen blokk hagyható ki):

- FEDC:0000:0000:0000:000C:BA98:0000:3210 → FEDC::C:BA98:0000:3210

Címtípusok az IPv6-ban:

Unicast:

- Az IPv4-hez hasonlóan egyedi cím (pontosan egy csomóponthoz tartozik)
- Minden IPv6 csomópontnak legalább egy ilyen címe van
- Globális, Link local, Site local



Multicast

- Csoportot azonosít
- Minden csoporton belüli csomópont megkapja az erre a címre küldött adatot (broadcast helyett is ezt használjuk)



Anycast

- Csoportot azonosít
- Biztosított, hogy a csoport egy csomópontja megkapja az címre küldött üzenetet



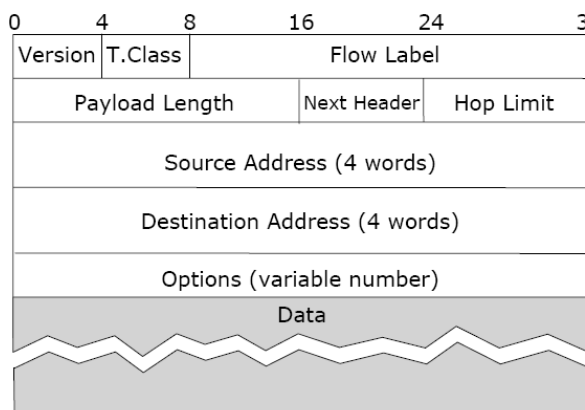
erre a

Broadcast (IPv6-ban NINCS)

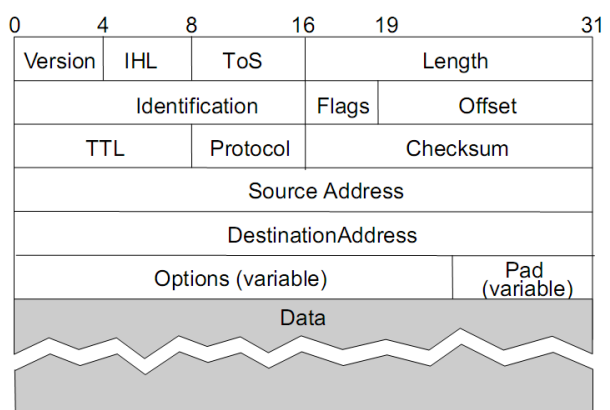
- Elárasztás



IPv6 csomag szerkezete:



IPv4 csomag szerkezete:



Az IPv6 fejléc mezői:

Version - verzió (4 bit): IPv6 esetén 6 (IPv4: 4)

Traffic Class - forgalmi osztály(4 bit): QoS lehetőség biztosítása IPv4 Type of Service mezőjével megegyező módon

Flow Label - folyam azonosító (24 bit): Arra használható, hogy megjelölje azon csomagokat, amelyek számára speciális kezelést kér az IPv6-os routerektől.

Payload Length (16 bit): csak az adat mérete (max 64 kbyte)

Hop Limit - ugrás korlát: megegyezik az IPv4 TTL mezőjével

Source/Destination Adress (2×128 bit): A fejléc jelentős része (32 byte a 40ból)

Next Header - következő fejléc (8 bit):

- A beágyazott PDU típusát adja meg, hasonlóan az IPv4 Protocol mezőjéhez vagy
- Az IPv6 fejléc kiterjesztését jelentő „Extension header” típusát adja

Ami az IPv6 fejlécből kimaradt...:

Nincs ellenőrzőösszeg (checksum)

- Általában kevés a hiba (jó minőségű kapcsolatok)
- Nem kell minden routernek ellenőriznie → nő a feldolgozási sebesség

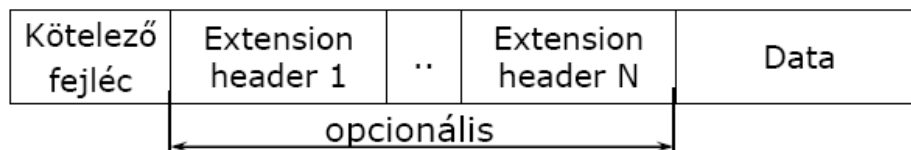
A fejléc mérete fix

- Rögzített méret → nő a feldolgozási sebesség
- Nem kell IHL (Internet Header Length) mező (IPv4-ben az opcionális mező ha volt, akkor az a fejléc része volt, ezért kellett IHL, itt ha van, nem az) → kisebb fejléc

Nincs ugrásonkénti tördelés (csak a forrás tördelhet!)

- Nő a feldolgozási sebesség
- Nem kell ehhez használt mező → kisebb fejléc
- MTU felderítés (Path MTU Discovery) kell!

IPv6 Header Extensions - Az egyszerű fejléc kiegészítése opcionális lehetőségekkel:



Hop-by-hop Options Header:

- Különböző információ, amelyet minden csomópont meg kell vizsgáljon
- Jumbogramok támogatása (óriás-datagrammok)
- QoS támogatása

Routing Header:

- Routers felsorolása, amelyeket útba kell ejteni (max 24 cím)
- Következő csomópont megtalálása anycast címmel

Fragmentation Header:

- Mint a v4-ben, de csak a forrás darabolhat (ehhez kell az Path MTU Discovery)
- 13 bites Fragmentation offset
- More fragment bit (MF) (2 nem használt bit)
- 16 bites helyett 32 bites Fragment ID mező, amely a töredéksorozatot azonosítja

Destination Options Header:

- Csak a célállomás vizsgálja
- Meghatározható, hogy mit kell a célállomának elvégeznie a csomag fogadása után

Authentication Header (AH) (IPSec-ből):

- Valóban a látszólagos feladó küldte-e
- Lett-e módosítva a csomag?

Encapsulation Security Payload Header (ESP) (IPSec-ből)

- A csomag titkosítására vonatkozó adatok

Az IPv6 infrastruktúra szolgáltatásai:

Neighbor Discovery: Feltérképezi a „szomszédokat”

Router Discovery: Automatikusan kiválasztja az átjárót

Stateless Autoconfiguration:

- Automatikusan minden beállítást megkap
- Duplikált cím észlelése

Path MTU Discovery: Meghatározható a teljes úton az MTU, így nincs szükség tördelésre (csak a feladónál)

IPv4 → IPv6 áttérési lehetőségek:

- Óraütésre, Címzés, Alagutazás, Dual Stack csomópontok

16.Mobil IP

Módosítás az IP-rétegben, amikor is a csomópontok attól függetlenül képesek folyamatosan adatok fogadására/küldésére, hogy éppen hol kapcsolódnak a hálózatra. A mobil IP-t olyan mozgó végpontoknak találták ki, amelyek legfeljebb kb. másodpercenként változtatják hozzáférési pontjukat. Vagyis a protokoll jól működik, amíg a mozgás sebessége nem éri el a mobil IP vezérlő üzeneteinek oda-vissza idejét.

Fogalmak:

Mobile node: kapcsolódási pontját változtató (mobil) eszköz

Home agent (honos ügynök): a mobil végpont otthoni hálózatában lévő router, amely tunnelezi az adatokat, így juttatva el azokat a távolban lévő mobil végponthoz.

Foreign agent (idegen ügynök): egy router a végpont jelenlegi hálózatában, mely felelős az adatok továbbításáért a végpont felé, amíg az a hálózatban tartózkodik.

Home address: a mobil végpont otthoni IP címe (~permanens IP cím)

Care-of address: cím az idegen hálózatban

Becsomagolás (encapsulation): A home agent a csomópont számára érkező IP csomagot új fejrésszel látja el és úgy küldi tovább

Tunneling: A home agent továbbítja a Care of Address-ra a mobilnak szóló csomagot, egyfajta alagutat hozva létre a hálózatban. A küldő úgy látja, hogy ezen az alagúton keresztül a címzettet közvetlenül eléri a csomag.

Absztrakt Mobil IP modell

Két IP cím tartozik minden mobil nodehoz, ezeket tárolni kell (home- és care-of address)

Ha csomag érkezik:

- a node otthon van: továbbítjuk neki
- nincs otthon: továbbítjuk a care-of address címre.

Ha a node távol van, regisztráltatnia kell care-of address-ét a home agent-nél.

A home agent vagy elfogadja, ekkor frissíti a CoA-node - IP-cím összerendelést, vagy visszautasítja a túl hosszú igényelt időtartam, elérhetetlen otthoni hálózat, elérhetetlen honos ügynök port, túl sok összeköttetés, stb. miatt.

Kétféle módon lehet care-of address-t szerezni:

- care-of address = a foreign agent címével. Ekkor a tunnel vége a foreign agent.
- egy helyi IP címet utalunk ki a mobil node-nak (colocated care-of address), dinamikusan (DHCP). Ekkor a tunnel vége a mobil node.

A Mobil IP protokoll működése:

A home/foreign ügynökök meghirdetik szolgáltatásukat, amikről a mozgó végpontok értesülnek.

Ha a végpont otthon van, akkor mobilitást támogató funkciók nélkül kommunikál, ha hazatért egy másik hálózathoz, akkor egy de-registration-t hajt végre a home agent-jével.

Ha a végpont új hálózat területére téved, care-of address-t igényel. Ez lehet vagy a foreign agent címe, vagy egy colocated(helyi IP) cím. Az otthonától távol lévő node regisztráltatja új care-of címét a home agent-tel. Ehhez esetleg igénybe veszi a foreign agent segítségét.

A mobil végpont otthonába küldött adatokat a home agent továbbküldi a care-of címre, egy tunnel segítségével.

17.Szállítási protokollok: UDP és TCP

Hálózati réteg: végpontok („host”-ok) közötti logikai kapcsolatok

Szállítási réteg: alkalmazások (processzek) közötti logikai kapcsolatok

Az UDP és TCP közös képességei:

Portok kezelése

Multiplexelési képesség

Alapvető különbség az UDP és a TCP között:

- *Az UDP kapcsolatmentes (connectionless) transzport-szolgáltatást nyújt (best-effort)*
- *A TCP összeköttetés-orientált (connection-oriented)*
- *Az UDP sokkal gyorsabb protokoll, mint a TCP, viszont nem megbízható adatátvitel szempontjából, míg a TCP lassabb, de sorrendhelyes és hibamentes.*

UDP - User Datagram Protocol

Portok kezelése:

Az IP-rétegben a csomagok végpontnak, „host”-nak vannak címezve.

A végpontokon belül több alkalmazás, folyamat, megkülönböztetésük: portok használatával

Foglalt (reserved) és rendelkezésre álló (available) portszámok

- Foglalt portok: ide mindig lehet küldeni datagrammokat. Pl. 21: FTP

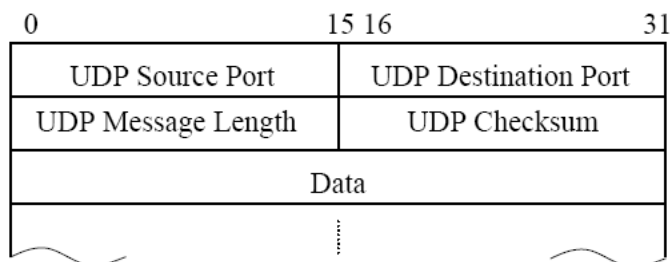
Az UDP-n belül megállapításra kerülnek az alkalmazandó port-számok

Socket = IP cím + portszám

Multiplexelés/demultiplexelés

A port-mechanizmus segítségével. A beérkező UDP datagramot az UDP a különböző portokra demultiplexálja. Ezáltal több alkalmazást tud egyidejűleg kezelni.

UDP Datagram:

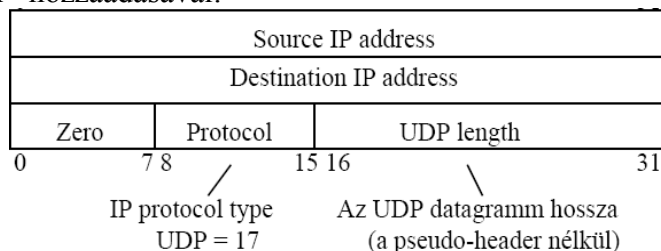


Source port opcionális (nem használt: 0)

Message Length - üzenethossz: minimum: 8 byte

Checksum: opcionális (nincs: 0)

- számítási elve: Tartalmazza az IP-címeket is (annak ellenőrzésére, hogy a datagramm elérte a helyes címzettet, nemcsak a helyes portot) – egyetlen hibajelző funkció „Pseudo-header” hozzáadásával:



TCP - Transmission Control Protocol

Megbízható szállítási szolgáltatás nyújtása az IP nem megbízható datagram-szolgáltatásán

Jellemzői:

Virtuális összeköttetések: összeköttetés épül fel és marad fenn a kommunikáció tartamára

Stream-típusú szolgáltatás: bit- (byte-) stream-ek sorrendhelyes átvitele

Strukturálatlan stream: nincsenek határolók a stream-en belül

Pufferelt átvitel: a stream-ből a datagramm megtöltéséhez szükséges mennyiséget várja össze

Duplex kapcsolatok: két független stream (egyidejűleg mindkét irányú forgalom lehetséges)

Vezérlő információk küldése: az ellenkező irányban folyó stream-be ágyazva

TCP megbízható transzport-szolgáltatás:

Csúszóablakos („sliding window”) mechanizmus

Ablak-módszer; az ablak mérete megadja a „kintlevő”, nyugtázatlan csomagok max. számát.

A TCP-ben: az ablak-mechanizmus oktett-eken (8-as egységeken) működik

→ jó hatékonyság, egyben forgalomszabályozási (flow control) módszer is (biztosítja azt a sebességet, amit a vevő képes feldolgozni)

TCP PDU (Protocol Data Unit):

0	4	10	16	19	24	31
SOURCE PORT			DESTINATION PORT			
SEQUENCE NUMBER						
ACKNOWLEDGEMENT NUMBER						
HLEN	RESERVED	CODE BITS	WINDOW			
CHECKSUM			URGENT POINTER			
OPTIONS (IF ANY)					PADDING	
DATA						
...						

Sequence no: a szegmensben levő adat első byte-jának pozíciója a küldő byte stream-jében

Ack no: annak a byte-nak a sorszáma, amelyet a forrás legközelebb vár

Header length: hány 32 bites szóból áll a TCP fejrész

Code bits: a szegmens tartalmára utal

URG bit értéke 1, ha *sürgősségi mutatót* használ.

ACK bit 1 értéke jelzi a *nyugta* mező érvényességét.

PSH bit jelzi a késedelem nélküli adattovábbítást (PUSH).

RST bit egy hoszt összeomlása, vagy más okból összezavart összeköttetés helyreállítására szolgál.

SYN bit összeköttetés létesítésére szolgál.

FIN bit szolgál egy összeköttetés bontására.

Window: a küldő ismertté teszi a vételi pufferének méretét

Checksum: mint az UDP-ben

Urgent pointer: „out of band” adatok küldésére

Torlódásvezérlés a TCP-ben

Módszer: növeljük az adatsebességet, ha úgy érezzük, hogy van elég átbocsátó képesség, amíg torlódásra utaló jelet nem tapasztalunk

Megvalósítás:

- Növeljük az ablakozás méretét amíg veszteséget nem tapasztalunk
- Minden vesztéskor felére csökkentjük az ablakot
- Adaptive Increase – Multiplicative Decrease módszer

Torlódás észlelése:

- Timeout letelt
- Többszörös nyugta érkezett

Adatsebesség = ablak méret / körbefordulási idő

Összefoglalás:

<i>Alkalmazás</i>	<i>Alkalmazási rétegbeli protokoll</i>	<i>Használt transzport-protokoll</i>
<i>E-mail</i>	SMTP	TCP
<i>Távoli elérés</i>	Telnet	TCP
<i>Web-elérés</i>	HTTP	TCP
<i>File-átvitel</i>	FTP	TCP
<i>Routing</i>	RIP	UDP
<i>Hálózatmenedzsment</i>	SNMP	UDP, TCP
<i>VoIP, média-streaming</i>	Többnyire nem szabványos	UDP

Hiányzik: az angol TCP rész, amit előadáson leadtak (Kurose_Ch3_TCPkieg.ppt)

18.Multimédia továbbítása IP felett (RTP, RTCP, RTSP)

Multimédia, v. egyszerűen média (beszéd, videó, adat) továbbítása IP-hálózatokban . Ezek a protokollok a multimédia-továbbítás mellett a kapcsolódó vezérlő információval is foglalkoznak, de nem hívásvezérléssel!

Szolgáltatásminőség-igényeik pont ellentétesek az adatkommunikációval:

- Késleltetésre érzékenyek
- Adatvesztésre kevésbé érzékenyek

Többsíkú architektúra

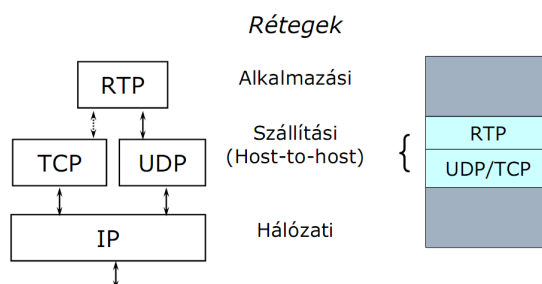
A B-ISDN szabványaként vezették be, 3 réteg van

- Felhasználói sík
- Vezérlő sík
- Menedzsment sík

Az NGN architektúra (New Generation Network)

- egységes gerinchálózat, három gerinc-réteg: transzport, vezérlés és szolgáltatás.
- Csomagalapú

RTP – Real Time Protocol



- A payload-jában média-, pl. beszédinformációt hordoz
- UDP felett működik (közvetlenül IP felett is lehetséges, de ritkán alkalmazzák)
- nem nyújt QoS garanciát
- Különböző UDP portokat használnak párban az RTCP-vel:
 - RTP: páros számú portot
 - RTCP: a következő páratlant

RTP Fejrész formátum:

0	1	2	3	8		16		31
V=2	P	X	CC	M	PT	Sequence number		
Timestamp								
Synchronization Source Identifier (SSRC)								
Contributing Source Identifiers (CSRC)								

Fejrész kompresszió:

Cél: az overhead csökkentése

Kezeljük együtt mindhárom protokollt (IP + UDP + RTP)!

Elv: a kapcsolat kezdete után kis változások a fejrészekben

- Redundáns információ (pl. megvan a data link header-ben)
- Sok mezőben nincs változás a kapcsolat alatt
- Vannak mezők, amelyek változnak, de jósolható módon, pl. sequence number

Először tömörítetlen és teljes header elküldése, utána a kompresszor és a dekompresszor.

Megállapodnak egy Context Session ID-ben (CID); (8/16 bit hosszú)

RTCP – Real-time Transport Control Protocol

End-to-end QoS-monitoring-ot nyújt

Különböző UDP portokat használnak párban az RTP-vel:

- RTP: páros számú portot
- RTCP: a következő páratlant

RTCP csomagtípusokban átvitt információ:

SR (Sender Report): Aktív adók statisztikái

- Egy „session” minden résztvevőjét informálja

RR (Receiver Report): Nem aktív adóktól származó információk

Sávszélesség-hozzárendelés az SR/RR forgalom számára: Elvileg: a teljes sávszélesség 5%-a

SDES: Helyi jellemzőket szolgáltat (hely, telefonszám, e-mail cím)

BYE: Egy forrás elhagyja a konferenciát

APP: A végpontok alkalmazásai közötti kommunikáció

RTP és RTCP: összefoglalás:

RTP a média-transzport-protokoll a VoIP-rendszerekben (is)

- UDP felett működik
- Különböző média-kódolási formátumokat támogat
- Az átvitelért felelős, a QoS-ért nem
- A fejrészt (az UDP+IP-vel együtt) kompresszióval lehet csökkenteni

RTCP az RTP társ-protokollja

- Nem jelzésprotokoll
- Nem QoS protokoll
- Hasznos segédeszköz a QoS megvalósításához

19.Hívásvezérlő Protokollok

SIP – Session Initiation Protocol

Alkalmazási rétegbeli protokoll a TCP-IP architektúra szerint. (A SIP UDP vagy TCP felett működhet). Session-ök létrehozása, módosítása, befejezése egy vagy több partnerrel.

„**Session**”: Kommunikáció küldők és fogadók csoportja között, ahol a kommunikáció állapotait a küldők és fogadók tárolják az átvitel alatt.

Session-leírókat (descriptors) visz át a különböző médiatípusokra vonatkozóan képesség-egyeztetés céljából.

Kezeli a felhasználók helyzetinformációit, támogat pl. hívásátadást

Támogatja a mobilitást

Multipoint control unit (MCU) funkció

A SIP text-alapú protokoll (a HTTP-hez hasonló) → a SIP-üzeneteket könnyen generálhatják emberek vagy programok (CGI, Perl vagy Java)

SIP Uniform Resource Locators (URLs):

Hasonlók az e-mail URL-ekhez sip: szabo@hit.bme.hu sip: +3614633261@hit.bme.hu

A SIP architektúrája: építőelemek

User agent – UA: „Request”-eket kezdeményeznek és azok címzettjei: IP-telefon, PC, konferencia-szerver. Lehet hardware és software alapú. Két logikai részből áll:

- User Agent Client (UAC): Request-eket küld és response-okat vesz
- User Agent Server (UAS): Response-okat küld és request-eket fogad

Proxy server: A SIP request-eket és response-okat route-olják a kliensek (UA-k) megbízásából. Két típusa van:

- Állapotmentes: Egyszerű és gyors üzenettovábbítók
- Állapot-alapú: Forking - egy üzenet vételekor 2 v. több üzenetet küld ki

Registrars: Nyilvántartják a felhasználókat (név-cím-összerendelések) egy domain-en belül

Redirect servers: Request-re megadják a felhasználó címét, de nem kezelnek hívásvezérlést és nem továbbítanak SIP request-eket. Vagyis ha egy UA INVITE -ot küld a Redirect Servernek (RS), akkor az kapcsolatba lép a location service-szel, majd ha megvan a cél UA címe, akkor azt visszaküldi a hívó félnek. Ezután hívó UA ACK az RS-nek, majd INVITE a cél UA-nak, aki ACK-kal válaszol.

Forking:

Más jelzésprotokolloknál ilyen nincs: a híváskérések elágaztatása. A szerver két vagy több request-et küld különböző címzetteknek egy beérkező request-re

SIP üzenetek:

Két fő kategória: Request-ek és Response-ok

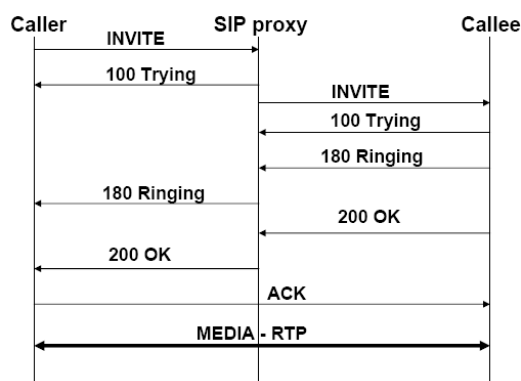
Nagyon hasonlít a HTTP/1.1-hez

Ugyanaz a request-ek és response-ok formátuma, az első sor kivételével

Tartalmazhatnak üzenettörzset:

- Session description
- ASCII vagy HTML

INVITE továbbítása proxy segítségével (ábra):



20.QoS: a Best Effort-on túl - IntServ, DiffServ

QoS összeköttetés alapú hálózatokban: ATM

- Minden ATM összeköttetéshez QoS kategória kapcsolódik, és a hálózat garantálja a megállapodás szerinti QoS-t minden összeköttetés számára
- önmagában finom felbontású módszer, ugyanakkor a QoS-t nem a hálózati rétegben valósítja meg, hanem a hálózati rétegben: az ATM-et gyakran használják IP routerek összeköttetésére -> lehet összefogott (aggregált) csomagfolyam egyetlen VC-n



Best-Effort: megkülönböztetés nélkül továbbítja a csomagokat

DiffServ: különböző kiszolgálást biztosít csomagfolyamok csoportjainak (osztály) (durva felbontású)

IntServ: a csomagfolyamokat egyedileg szolgálja ki, igényeiknek megfelelően (finom felbontású)

A szolgáltatásosztályok:

Best Effort

Guaranteed Quality: garantált korlátok bármely csomag késleltetésére

Controlled-Load: függetlenül a többi forgalomtól, terheléstől, törekszik kb. ugyanolyan szolgáltatást nyújtására, mint amelyet a folyam kapna, ha terheletlenek lennének a hálózati csomópontok.

IntServ

Az alkalmazások igényei és az IntServ-szolgáltatások:

1. „Elastic applications”: nincs késleltetési vagy bármilyen korlát

→ Best effort service

- interactive burst (pl. WEB)
- interactive bulk (pl. FTP)
- asynchronous (pl. e-mail)

2. „Real-time tolerant (RTT)” alkalmazások: gyenge késleltetési korlátok, alkalmanként csomagvesztés megengedett → Controlled load service

3. „Real-time intolerant (RTI)” alkalmazások: minimális késleltetés és késleltetés-ingadozás → Guaranteed service

Az IntServ-ben használt mechanizmusok

A felhasználó (alkalmazás) specifikálja a forgalmát a hálózat számára, és meghatározott szolgáltatást kér a hálózattól, melynek alapján a hálózat eldönti, hogy tudja-e ezt vállalni, beengedi-e az új folyamatot a hálózatba (admission control, beengedésszabályozás).

A felek információt cserélnek az erőforrásfoglalásról (jelzésátvitel, az IntServ-ben az RSVP-protokoll segítségével). Áramkörkapcsolt és összeköttetés-alapú hálózatokban a hívásvezérlő protokollok csinálhatják

A hálózat gondoskodik arról, hogy a forrás forgalma ne térjen el a megadottól (traffic policing), majd meghatározza a csomagok sorbaállítását és kiszolgálását a csomópontokon (scheduling, ütemezés).

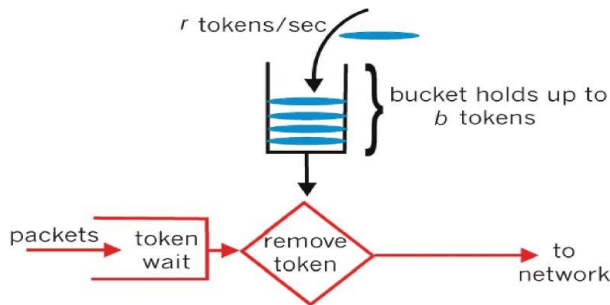
A csomagfolyam-specifikáció (flowspec):

Két eleme van:

Tspec (Traffic Specification): leírja a folyam forgalmi jellemzőit, informálva ezzel a hálózatot a szükséges sávszélességről

Rspec (Request Specification): leírja a kiszolgálási igényt

Forgalomleírás és policing:



A policing és a forgalomleírás eszköze: a **token bucket** (tokenvödör).

A vödör formálja (szűri) a forgalmat: küldhetünk b méretű borsztöt, de az átlagsebesség csak r lehet

A vödörbe r sebességgel töltődnek a tokenek. Legfeljebb b token lehet benne, ha már tele van, a beérkező tokenek törlődnek.

Beengedés-szabályozás (admission control):

Megvizsgálja a forgalomleírást (TSpec) és a kiszolgálási igényt (RSpec), ezután dönt az igényelt szolgáltatás teljesíthetőségéről.

Jelzésátvitel – RSVP (Resource ReSerVation Protocol):

Vevőoldali erőforrás-foglalás: Nem az adó „erőlteti” a képességeit, hanem a vevő foglalja le azt az igényei szerint → kedvező a többescímzésnek (multicast).

A vevőnek ismernie kell, hogy az adó milyen forgalom generálására képes: tudnia kell az adó TSpec jellemzőjét, valamint tudnia kell a forgalom (csomagok) útját, hogy erőforrást foglaljon az út mindegyik csomópontjánál.

„Soft state”: igények „elhalnak”: nem igényli a session explicit lezárását → a lezárásból adódó hibák kiküszöbölése.

Csak egyirányú (szimplex) csatorna, csak a vevő üzen.

RSVP – „út”: egy adó ↔ egy vevő (a folyamat ismertetése):

PATH üzenet a vevőnek, hogy a vevő ismerje a csomagok útját így azt, hogy hol foglaljon erőforrást az általa kívánt szolgáltatáshoz. A PATH üzenet által érintett routerek feljegyzik a vissz-irányt (reverse path).

Amikor a vevő kap egy PATH üzenetet, visszaküld egy RESV választ, benne TSpec és Rspec. A reverse path-on lévő routerek megkísérlik a RESV üzenetben lévő RSpec-nek megfelelő erőforrás-foglalást megcsinálni. Siker esetén továbbítják a RESV üzenetet. Ellenkező esetben hiba a vevőnek. Ha egy router kiesik, új útvonal kell. Mivel a foglalásokat 30 mp-enként meg kell erősíteni, a régi RevPATH-on lévő routerek elengedik a lefoglalt erőforrásokat.

RSVP: egy adó ↔ több vevő:

Ha az új vevő RevPATH-ja találkozik a régi vevőéjével:

- Új vevő elvárása kisebb, mint a régié → nincs teendő.
- Ha nagyobb, akkor tovább kell folytatni a foglalás

RSVP: több adó ↔ több vevő:

A vevőknek össze kell gyűjteni az adók TSpec-eit, ezután a foglalást az összesített TSpec-ek alapján kell kialakítani.

IntServ scalability (skálázhatóság, „növekedési” képesség):

Bár az IntServ nagyon jelentős előrelépés a best effort kiszolgáláshoz képest, nem teljesíti az Internet egyik alapvető célkitűzését: a növekedési képességet. Az IntServ-nél: lényegében összeköttetés-alapú szolgáltatást csináltunk annak minden nehézségével együtt, de anélkül, hogy annak előnyét, a lokális címezést kihasználtuk volna.

DiffServ:

A gerinchálózatra kell megoldást találni, ahol nagy volumenű, aggregált forgalmat viszünk át. A DiffServ módszer kisszámú forgalomosztályhoz rendel erőforrásokat: pl.: Premium/Regular. Ahelyett, hogy külön jelzéssel (pl. RSVP-vel) értesítenénk a routereket egy folyam igényéről, egyetlen bit a csomagfejben megegyezhet ezt. (Ezt az adó, az első DiffServ Router, vagy egy Edge Router teheti meg).

A DiffServ architektúrája:

Edge route:

- folyamonkénti forgalom-menedzselést végez
- megjelöli a csomagokat in-profile ill. out-profile -ként

Core router:

- osztályonkénti forgalommenedzselést végez
- pufferezés és ütemezés a széleken történt megjelölésnek megfelelően
- elsőbbség adása az in-profile csomagoknak

A csomagok megjelölése az edge-routerben:

profile: egyeztetett A sebesség és B vödörméret

osztály szerinti: a különböző osztályokhoz tartozó csomagokat eltérően jelöljük

osztályon belüli: a folyam konform (a profilnak megfelelő) és nem konform részei eltérő
Megfigyeljük a forgalmat (meter) és a nem konform csomagokat formáljuk (shaping) vagy eldobjuk (dropping).

DiffServ - csomópontok viselkedése:

A különböző szolgáltatásokat a DiffServ különböző csomóponti viselkedéssel PHB = Per-Hop-Behavior) éri el, vagyis nincs együttműködés a végpontok között, mint az IntServ-nél. A különböző PHB-k kiválasztására az IP fejléc ToS (type of Service) 8 bites mezijében 6 bit szolgál (az IPv4-nél – ez 64 különböző PHB). Ez a 6 bit a „**DiffServ Code Points**” (DSCP).

Alapvető PHB-k:

Expedited Forwarding (EF): virtuális bérelt vonal, állandó bitsebesség

Ez a legegyszerűbb PHB: a csomagok továbbítása minimális késleltetéssel kis csomagvesztéssel történik. Célszerű ha az EF-forgalom érkezési ütemét csak a csomópontok link-sebessége korlátozza.

Assured Forwarding (AF): kevesebb garancia, de megengedi a bősztös forgalmat.

A legnépesebb osztály: 12 elemmel

DiffServ – előnyök:

- Mivel a **DiffServ módszer a 3. rétegben működik**, bármely 2. rétegbeli - IP-re alkalmas -infrastruktúrán működhet változtatás nélkül.
- Nem igényel jelzést valamennyi csomóponton.
- Megszünteti a gerinchálózati csomópontokon a csomagfolyamokénti állapotnyilvántartást.
- Az elkerülhetetlenül szükséges bonyolultságot a hálózat szélére (hozzáférési rész) tolja.

Problémák:

- önmagában nem biztosít végpontok közötti QoS-t
- nem DiffServ-képességű csomópontok az útban

Az IntServ és a DiffServ összehasonlítása:

Jellemző	IntServ Elérési hálózat	DiffServ Gerinc-hálózat
Szolgáltatások kezelési módja	Végpontok közötti	Helyi (lépésenkénti)
Szolgáltatások kezelésének hatóköre	Egyedi- vagy többes-című út	Bárhol a hálózatban
A skálázhatóság (scalability) korlátja	Csomagfolyamok száma	Szolgáltatás-osztályok száma
Számlázás alapja	Forgalom- és QoS jellemzők	Forgalmi osztály használat
Forgalommenedzsment fajtája	Hasonló, mint az áramkörkapcsolt	Hasonló, mint az IP hálózaté
Tartományokon átívelő megvalósítás feltétele	Többoldalú megállapodás	Kétoldalú megállapodás

21.MPLS – Multi-Protocol Label Switching

Összeköttetés-alapú hálózatok

A csomópontok csomagtovábbítási tevékenysége (packet forwarding) egyszerű, ezáltal gyors működést tesznek lehetővé, és a csomagtovábbítási tevékenység teljesen független az útvonalirányítási (vezérlési) tevékenységtől. Az összeköttetés felépítése során sokféle szempont figyelembe vételével lehet az útvonalat kialakítani (csak egyszer kell megtenni, így viszonylag körülményesebben járhatunk el, mintha minden csomagra meg kellene ismételni), így könnyen lehet forgalom- és hálózat-menedzsment szempontokat is tekintetbe venni.

Összeköttetésmentes hálózatok

Nem kell várni az információtovábbításnál az összeköttetés kiépítésére, robosztusabb a meghibásodások kezelésben (útvonalváltás), rendkívül jók a csomagok „túlélési esélyei”. A két rendszer jó tulajdonságait próbálja ötvözni az MPLS!

Milyen az IP-csomagtovábbítás és milyen az MPLS-é?

Az **IP-csomagtovábbítás** nem elég hatékony: az összeköttetésmentes működés miatt mindegyik router függetlenül végez lépésenkénti (hop-to-hop) csomagtovábbítási döntést. Az **MPLS** felosztja a címetet Forward Equivalence Class (FEC)-ekre (a továbbítás szempontjából azonosan kezelendő csomagok osztályaira) és azoknak megfelelő, rövid, helyi érvényű címeket, címkéket (label) használ a továbbításra (Az útvonaltáblák bejegyzéseiben szereplő globális azonosítók (mellett) most elhelyezünk lokális azonosítókat is melynek előnye, hogy a csomagok routolása helyett lehetséges azok kapcsolása).

Az MPLS alapvető jellemzői:

- mechanizmusokat határoz meg a különféle összefogottságú csomagfolyamok kezelésére
- függetlenül működik a 2. és 3. rétegbeli protokolloktól
- módszert biztosít az IP címeknek a leképezésére az egyszerű, fix hosszúságú címkékre
- csatlakozik a használt protokollokhoz (pl. RSVP, OSPF)
- együttműködik az IP-vel, az ATM-mel, és a Frame Relay 2. rétegének protokolljával

Az MPLS működése:

A címke-kapcsoló-router (Label Switching Router = **LSR**) a csomagokat a rájuk „ragasztott” fix hosszúságú címkék alapján továbbítja. Az LSR átírja a címkét, mielőtt elküldi a csomagot lényegesen egyszerűbb, mint a leghosszabb egyezés (alvál. maszk-nál volt ez)

- az LSR adott teljesítmény esetén olcsóbb a hagyományos routernél
- a csomagtovábbítási döntések összetettebbek lehetnek
- csomagfolyamok összevont kezelése is lehetséges

A csomagtovábbítás címkekapcsolt utakon (Label Switched Path = LSP) történik

Az LSP-t LSR-ek és LER-ek alkotják:

- Az LSR (Label Switching Router) egy gyors útvonalirányító az MPLS gerincében
- Az LER (Label Edge Router) egy útvonalirányító az MPLS és a hozzáférési hálózat határán: elsődleges eszköze a csomagok címkézésének (kilépő/belépő LER)

A címkék kiosztását a Label Distribution Protocol (LDP), vagy az RSVP, vagy valamely routing protokoll végzi.

Hardver is alkalmas a csomagok kapcsolására

Az MPLS csomagtovábbítás előnyei

Csomag FEC-be sorolása csak a belépésnél:

- „buta”, de gyors gépek a csomópontokon
- a besorolásnál IP fejen kívüli szempontok is → pl. melyik interfészen érkezett a csomag
- ugyanaz a csomag eltérő módon sorolható be a belépő (ingress) routertől függően
- a besorolási procedúra bonyolultsága nincs hatással a csomópontokra (mivel ők nem számolják ezt semmikor)
- ha forrás általi útvonalat akarunk, akkor a csomagnak nem kell magával vinni azt

A FEC és a címkék:

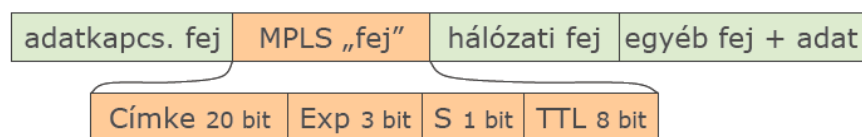
FEC (Forward Equivalence Class): a csomagoknak egy csoportját képviseli, amelyek továbbítása azonos. FEC-be sorolás csak egyszer, a belépésnél

Címkék (Label):

- A címkét a csomag magával viszi egy 2. réteg jelölként
- A közbelső router a címke tartalma alapján határozza meg a csomag következő lépését
- Ha egyszer egy csomagot „felcímkéztünk”, akkor útjának hátralévő részén a csomópontok már ennek alapján kezelik
- A címkék értéke lokális jelentésű

A címkék elhelyezése:

Közbeiktatott (ún. shim vagy generic) header:



Ha az adatkapcsolati rétegbeli protokoll összeköttetés-alapú, akkor annak címkéjét lehet használni (ATM cellák esetén: VPI/VCI)

Honnan tudja egy küldő, hogy milyen címkét használjon?

Az MPLS-ben több protokoll is használható erre a célra:

- A BGP-t kibővítették, így címkeinformációt is szállíthat a „saját” adatok mellett
- Ugyanez történt az RSVP-vel is
- Az IETF azért kidolgozott egy új protokollt is: az LDP-t (Label Distribution Protocol)
- címkék szétosztására és „karbantartására”. Az LDP-nek kidolgozták egy kiterjesztését is, hogy képes legyen a forgalommenedzsment és a szolgáltatási minőség igényeinek is megfelelni

A címkelosztás szabályai:

Az MPLS képességű eszközök egy csoportja MPLS tartományt (domain) képez. Egy-egy ilyen tartományban képezzük a FEC-ekhez kötött utakat. Ezeket nevezzük LSP-eknek (Label Switched Path). Az LSP létrehozása megelőzi az adatátvitelt. Az MPLS két módot határoz meg LSP képzésére:

- lépésenkénti: mindegyik LSR függetlenül választ következő lépést egy adott FEC számára. Az LSR bármilyen routing protokollt használhat
- explicit: forgalommenedzsment vagy szolgáltatási minőség szempontjai szerint létrehozott LSP-k

MPLS összefoglaló:

Az IP hálózat csomópontjai a routing révén rendelkeznek valamennyi lehetséges útra vonatkozó információval.

A lehetséges utakat „rögzíthetjük”, mielőtt bármelyik felhasználó igényelné azokat.

Különböző „minőségű” utak igény szerint is kialakíthatók

A hálózati rétegben kialakított utakon (LSP) a csomagtovábbítás az adatkapcsolati rétegben történik (címkekapcsolás)

A GMPLS (általánosított MPLS)

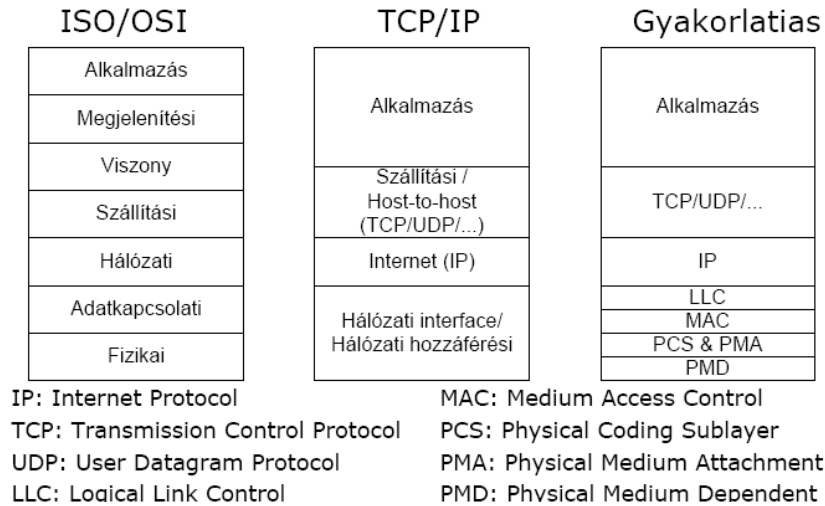
Lehet, hogy az MPLS-nek nem is a csomagtovábbítási módszer a lényege?

Valójában az LSP-k létrehozása a jelentős!

A csomaghálózat címke-kapcsolt útjai (LSP) a csomaghálózat csomópontjait összekötő linkeken jönnek létre. Ezeknek a linkeknek a kialakítása idő-, hullámhossz-, és térosztású fizikai hálózatokon történik. A fizikai átviteli utak vezérlése (jelzése) történhet meg a GMPLS révén a csomaghálózat hálózati szintjéről.

22.Hálózati alkalmazások

TCP/IP és ISO/OSI rétegek áttekintése:



Kliens-szerver architektúra:

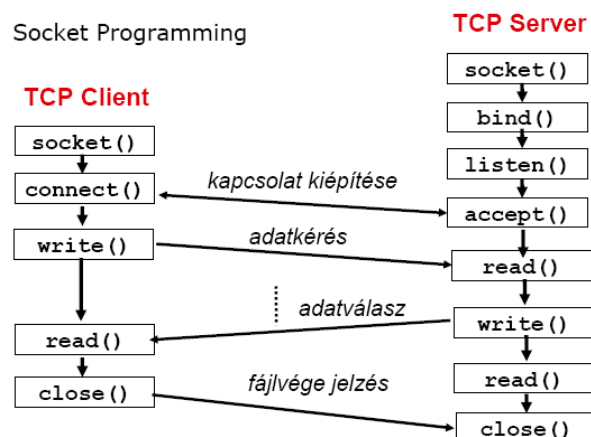
Kliens: kapcsolatot kezdeményező ügyfél

Porthozzárendelés: Dinamikusan kerül kiosztásra a még nem használtak közül (beleértve a szolgáltatásokat) 1-65536 tartományból 1024-65535-ig

Szerver: Szolgáltatást nyújtó kiszolgáló

Porthozzárendelés: Szolgáltatást azonosítja, egy port maximum egy szolgáltatáshoz lehet hozzárendelve (statikusan) tipikusan 1-1023-ig

TCP kommunikáció socket-hívásokkal:



Telnet

Egyik legrégebbi alkalmazás. Távoli parancssor, feladata:

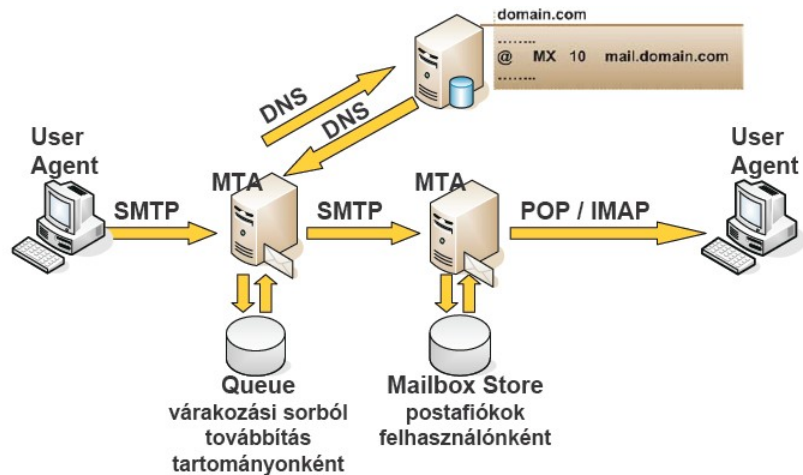
- Parancsok elküldése
- Visszajelzések megjelenítése

Még ma is alkalmazzák főként hálózati eszközök egyszerű hálózati adminisztrációjára. Nem biztonságos (jelszavak védelem nélkül) → helyette SSH (Secure Shell).

FTP – File Transfer Protocol:

Az egyik legelső fájlátvitelre tervezett protokoll. TCP 21-es port
Adattípus figyelembevétele (megjelenítési réteg): ASCII/Bináris

Levelező rendszerek:



Komponensek:

- **User Agent** (levelező kliens)
- **MTA** (Mail Transfer Agent) (SMTP szerver)

POP3: Post Office Protocol ver 3

Levelek lekérdezésére. Parancsorientált

IMAP4: Internet Message Protocol ver 4

Levelek lekérdezésére. Parancsorientált, de intelligensebb a POP3-nál:

- Könyvtárstruktúra támogatása
- Keresés támogatása
- Nem törli automatikusan a szerveren tárolt leveket (csak másolja azokat)

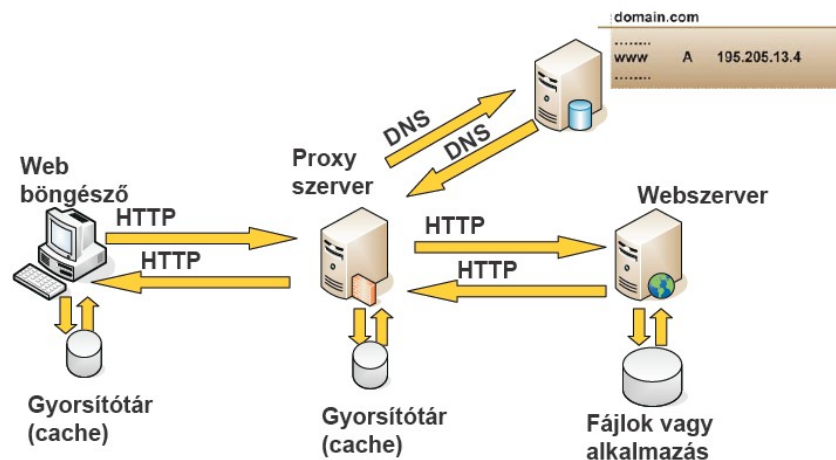
SMTP: Simple Mail Transfer Protocol

Levelek továbbítására (első „killer application”), parancsorientált állapotkódokkal

SMTP relay: Nem közvetlen továbbítás, egy (vagy több) SMTP (relay) szerver közbeiktatásával

Webes rendszerek:

HTTP - HyperText Transfer Protocol:



Proxy (ha van) kliens nevében jár el, főként a hatékony gyorsítótárazás miatt.

Gyakori http parancsok: GET, HEAD, POST, PUT, DELETE

HTTP alkalmazási területei: HTML, PHP, ASP, JSP, CGI, DHTML, ASPX, (ActiveX Control), Fájl le- és feltöltés, prototcol alagút (Tűzfalak kijátszása (HTTP 80-as port mindenhol engedélyezve))

HTTP biztonság: Hitelesítés, Tanúsítvány (Certificate), HTTPS (SSL)

Hálózatbiztonság:

A hálózatbiztonság építőkövei

AAA

- Authentication: hitelesítés
- Authorization: jogosultság-hozzárendelés
- Accounting: számlázás

Hitelesítés:

Kerberos

- Adott tartományon belül működik
- Időbélyeget használ

Public Key Infrastructure (PKI)

- Nyilvános kulcsú titkosítás felhasználásával
- Digitálisan aláírt tanúsítványokat kiállító szervezetek (CA: Certificate Authority)

Titkosítás:

- Szimmetrikus kulcsú
- Nyilvános kulcsú

NAT – Network Address Translation - Hálózati címfordítás

A belső (magán-) hálózat és az Internet összekötésére Csak hálózati rétegbeli átalakítás - címcserevel

NAT – Cím-összerendelési stratégia

Statikus: Probléma:

- Több mint egy belső cím jut egy külsőre
- Hogyan talál vissza a belső állomáshoz a vissza-irányú kommunikáció?

Dinamikus:

- Használjuk a következő szabad IP-címet
- Probléma: Nincs minden állomás számára elegendő IP-cím

Valójában nem csak az IP-címeket, hanem a portokat is módosítjuk: Network Address Port Translation (NAPT)

Problémák:

A NAT táblában a bejegyzések dinamikusan kerülnek hozzáadásra és törlésre. Ha létezik egy porthoz tartozó bejegyzés, és e portra bárki csomagot küld, akkor azt A állomás a portjára továbbítódik (port scan, Denial of Service), vizsgálat nélkül.

Megoldás:

A NAT táblát bővíteni kell a külső fél IP és port címével A NAT router eldob minden más állomástól jövő csomagot. Ezt a módszert maszkolásnak (masquerade) hívják.

NAT – Virtual server:

Belső szerver közzététele statikus NAT tábla bejegyzéssel. Úgy tűnik, mintha a szolgáltatás a NAT routeren lenne. Két típus:

- Minden IP-forgalom továbbításra kerül
- Csak az adott portra érkező forgalom kerül továbbításra A belső kiszolgálókat védi más forgalmaktól

Erőforrások megosztása:

Több mint egy belső kiszolgáló

- Terheléselosztás - a forgalom megosztása a belső szerverek között
- Magas rendelkezésreállás - ha egy meghibásodik, a többi még kiszolgál

Több mint egy külső interfész

- Terheléselosztás - a több kapcsolaton kifelé
- Magas rendelkezésreállás - ha egy kapcsolat meghibásodik, még mindig működhet

Problémák a NAT-tal

Másodlagos kapcsolatok hibája (Pl. FTP (TCP 20/21: vezérlő-/adatcsatorna) – egy alkalmazáshoz egy port)

- IP-cím az alkalmazásrétegben (a hálózatban lenne helye)
- Megoldás
 - Az alkalmazás-rétegbeli IP-cím cseréje - Az ISO OSI koncepció felrúgása
 - Proxy alkalmazás a NAT routeren

- További probléma:
 - Nincs lehetőség a csatornák tartalmának, de általában még az IP-címek megváltoztatására sem
- Megoldás: NAT-T (Traversal): Becsomagolás (encapsulation) és továbbítás az UDP 4500-as porton. A másik félnek is támogatnia lett a NAT-T-t a kicsomagoláshoz és a becsomagolt válaszhoz

Tűzfalak

Szabály alapú forgalomszűrés és továbbítás

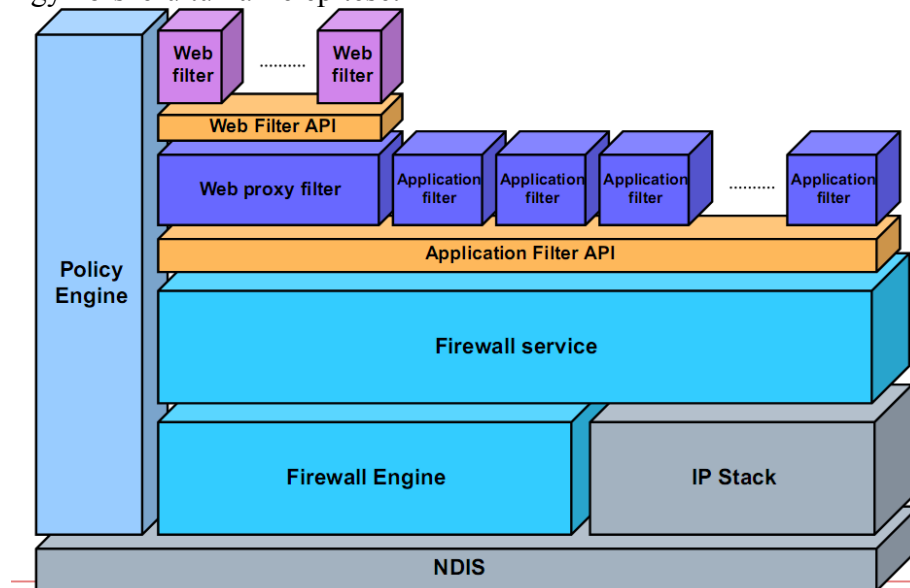
Tűzfal működési típusok

- állapotalapú (stateful) vagy állapotmentes (stateless)
- NAT vagy routing
- Közzététel (publishing) támogatása
- Protokoll és alkalmazás szintű szűrés támogatása (tűzfal, mint alkalmazás)

Egyéb funkciók

- Proxy
 - Gyorsítótárral
 - HTTP és FTP forgalomra
 - VPN kiszolgáló
 - Monitorozás, naplózás, riasztás, jelentések
- Szabály alapú forgalomszűrés és továbbítás
(automatikus szabályok, user által beállított)

Egy korszerű tűzfal felépítése:



VPN Virtual Private Network

Tunneling protokollok (közvetlen rálátás a címzettre, mindenki mást kizárva)