

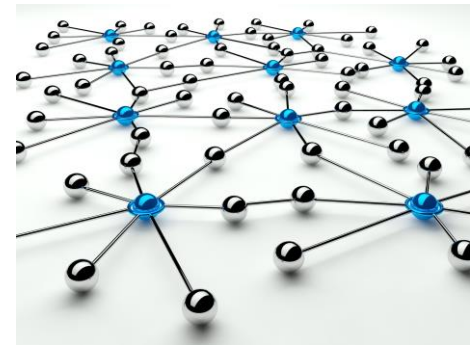
Hálózati architektúrák és protokollok

1. BEVEZETÉS

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Számítógép-hálózat fogalom bevezetése
Definíció, célok, alkotó elemek
- 2) Hálózatok kialakulásának története, mérföldkövek
- 3) Számítógép-hálózatok osztályozási szempontjai
- 4) Kommunikációs alapfogalmak
 - Csomópont
 - Adatátviteli közeg, csatorna, ütközés
 - Jel, kódolás, moduláció, multiplexelés
 - Adatátviteli sebesség
 - Moduláció sebesség
 - Adatátviteli kapcsolat típusok
 - Adatátvitel irányítottsága
 - Kapcsolási módok
 - Címzési alapfogalmak
 - Kommunikációs protokoll és elemei
 - Kommunikáció működési alapelve

1. Számítógép-hálózat fogalom bevezetése

Számítógép-hálózat definíciója:

- Autonóm gépek összekapcsolt rendszere közös alkalmazás céljából.
- Számítógéprendszerek valamilyen adatátviteli módszerrel megvalósított (hardveres és szoftveres) összekapcsolása.

Célok:

- Kommunikáció (ember-ember, ember-gép, gép-gép)
- Erőforrás-megosztás (CPU, tároló, vonal)
- Takarékoság (célfeladatok optimális végrehajtása)
- Skálázhatóság (darabszám, kapacitás módosítás)
- Megbízhatóság növelése (adat <-> hardver)
- Kommunikációs sebesség növelés

Alkotó elemek:

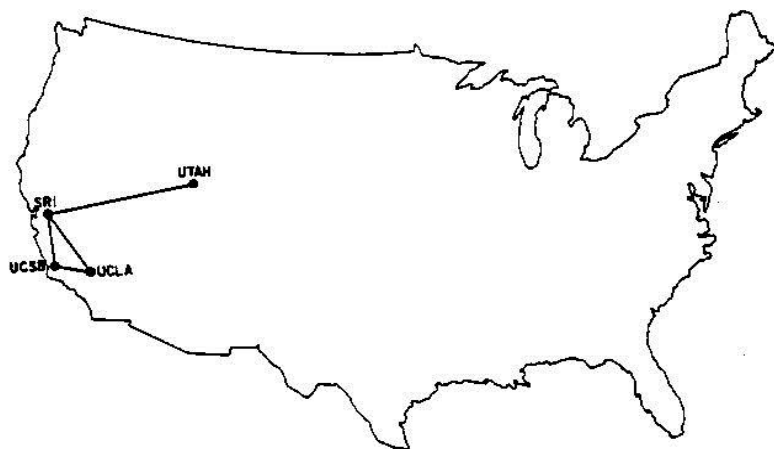
- Számítógépek, perifériák (pl. hálózati nyomtató)
- Hálózati berendezések (hardver: pl. kapcsolóelemek)
- Fizikai összeköttetést megvalósító eszközök (kábelek, vonalak)
- Hálózati alkalmazásokat működtető programok (szoftverek)

2. Hálózatok kialakulásának története

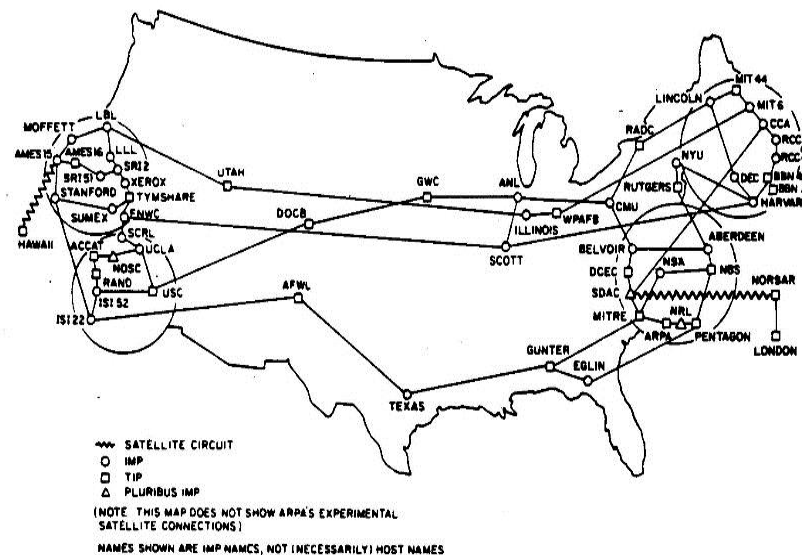
Időpont	Esemény
1900 előtt	Nagy távolságú kommunikáció (futár, füstjel, üzenő, optikai telegráf, elektromos telegráf)
1890-es évek	Bell: telefon feltalálása, szolgáltatás gyors elterjedése
1901	Marconi: első transzatlanti vezeték nélküli átvitel
1920-as évek	AM rádió
1939	FM rádió
1940-es évek	Mikrohullám feltalálása
1947	Shockley, Barden, Brittain: félvezető tranzisztor feltalálása
1948	Claude Shannon: „A Mathematical Theory of Communication”
1950-es évek	Integrált áramkör feltalálása
1957	DoD létrehozza a ARPA-t

2. Hálózatok kialakulásának története

Időpont	Esemény
1960-as évek	Mainframe Computing
1962	Paul Baran: csomagkapcsolás elméletének kidolgozása
1967	Larry Roberts: ARPANET témájú dolgozata
1969	ARPANET létrehozása: UCLA, UCSB, U-Utah, Stanford



1969



1977

2. Hálózatok kialakulásának története

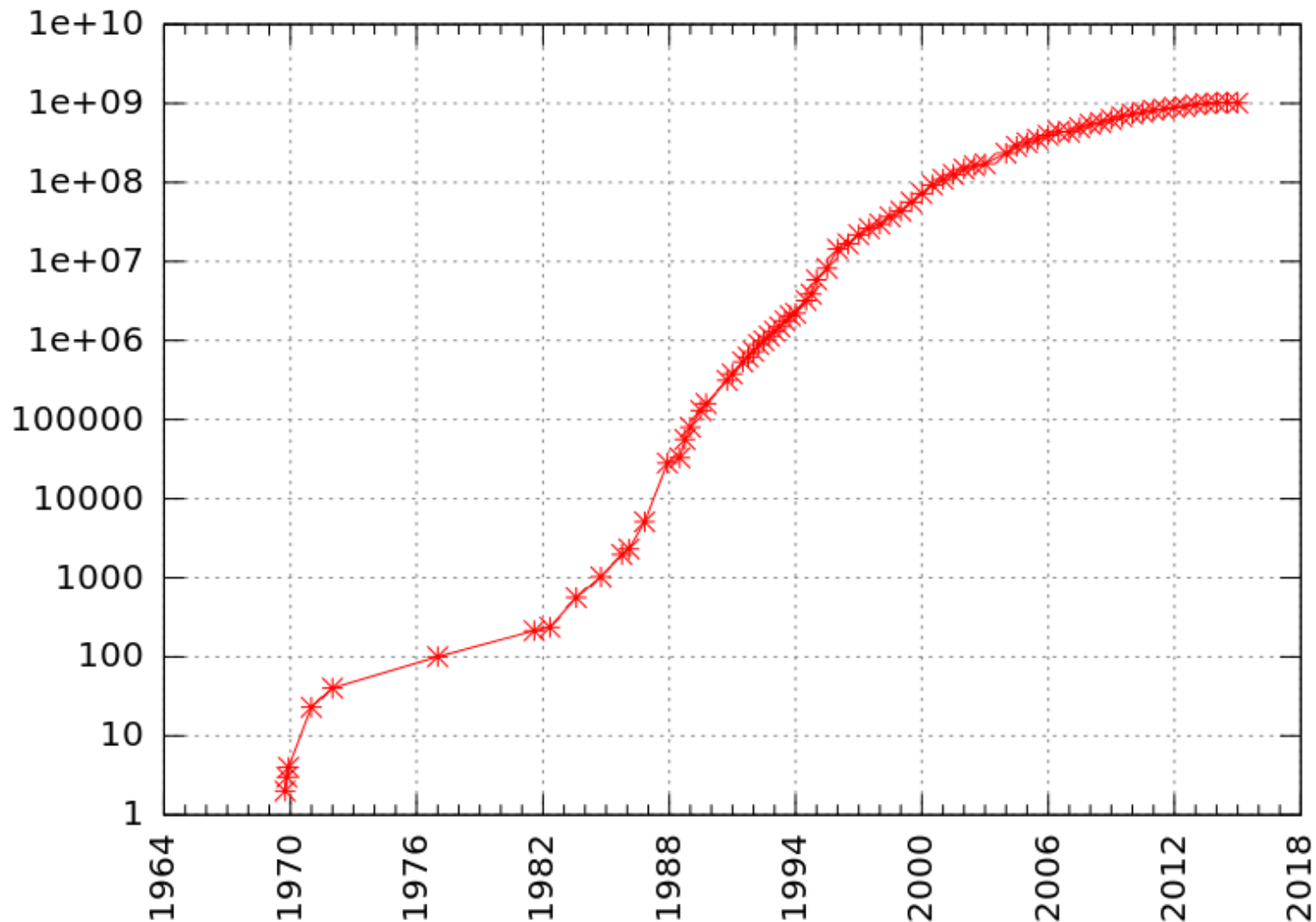
Időpont	Esemény
1970	University of Hawaii: ALOHANET létrehozása
1970-es évek	Digitális IC-k elterjedése, digitális személyi számítógépek
1972	Ray Tomlinson: E-mail küldő program létrehozása
1973	Bob Kahn, Vint Cerf: TCP/IP kidolgozása, ARPANET európai kapcsolata
1974	BBN: Telnet létrehozása (ARPANET üzleti változata)
1980-as évek	Személyi számítógépek és a Unix alapú minigépek elterjedése
1981	Internet fogalom megalkotása: hálózatok halmaza
1982	ISO megalkotja az OSI modellt és protokolljait (utóbbiak elhaltak)
1983	TCP/IP általános nyelve az Internetnek. ARPANET-ből kiválik a MILNET
1984	Cisco Systems cég megalakulása (router). DNS megalkotása, 1000 gép

2. Hálózatok kialakulásának története

Időpont	Esemény
1986	NSFNET létrehozása (56 kbps)
1987	Internet csomópontok száma > 10 k
1988	DARPA létrehozza CERT-et (Computer Emergency Response Team)
1990	ARPANET = Internet, (cs.pont szám > 100 k)
1991	Tim Berners-Lee: World Wide Web megalkotása
1993	Első Web böngésző megalkotása: Mosaic
1994	Netscape navigátor bevezetése
1997	ARIN (American Registry for Internet Numbers) létrehozása, Internet 2 elindítása
1999	Internet 2: IPv6 létrehozása Hang, videó, adat integrálási szándék megfogalmazása

2. Hálózatok kialakulásának története

Internet csomópontok számának növekedése



3. Számítógép-hálózatok osztályozási szempontjai

1) Lefedett fizikai terület mérete szerint:

- Hálózat az emberi testen (BAN: Body Area Net., BCI – Brain Comp. Interf.)
- Személyi hálózat (PAN: Personal Area Network)
- Otthoni/kiscéges hálózat (SOHO: Small Office/ Home Office)
- Helyi hálózat (LAN: Local Area Network)
- Városi/területi hálózat (MAN: Metropolitan Area Network)
- Nagyterületi hálózat (WAN: Wide Area Network)
- Globális hálózat (GAN/Internet: Global Area Network)

2) Adatátviteli ráta szerint:

- Klasszikus hálózatok: kbps ... Mbps
- Nagysebességű hálózatok: 100 Mbps ... Tbps

3) Tulajdonjog szerint:

- Magán hálózat (Private Network)
- Nyilvános hálózat (Public Network)

4) Mobilitás szerint:

- Rögzített (Fixed Network)
- Mobil (Mobile Network)

3. Számítógép-hálózatok osztályozási szempontjai

Helyi hálózatok (LAN)

- Egymással adatkommunikációs kapcsolatban lévő számítógépek együttese.
- Kiterjedésük viszonylag kicsi (néhány km²), egy-egy intézményre terjednek ki.
- Állandó hozzáférés a hálózati szolgáltatásokhoz
- A LAN kiépítését, menedzselését maga az intézmény végzi.
- A LAN-ok átviteli sebessége viszonylag nagy lehet (10 - 100(00) Mbps) a rövid távolságok miatt.
- Az adatátvitel biztonsága a rövid távolságok és a technológiából eredően magas.

LAN típusok:

- Összeköttetéssel működő (huzalozott, pl. csavart érpár, koaxiális kábel, optikai szál)
- Összeköttetés nélküli (nem huzalozott, pl. rádió hullámok)

3. Számítógép-hálózatok osztályozási szempontjai

Helyi hálózatok (LAN)

Tipikus LAN összetevők:

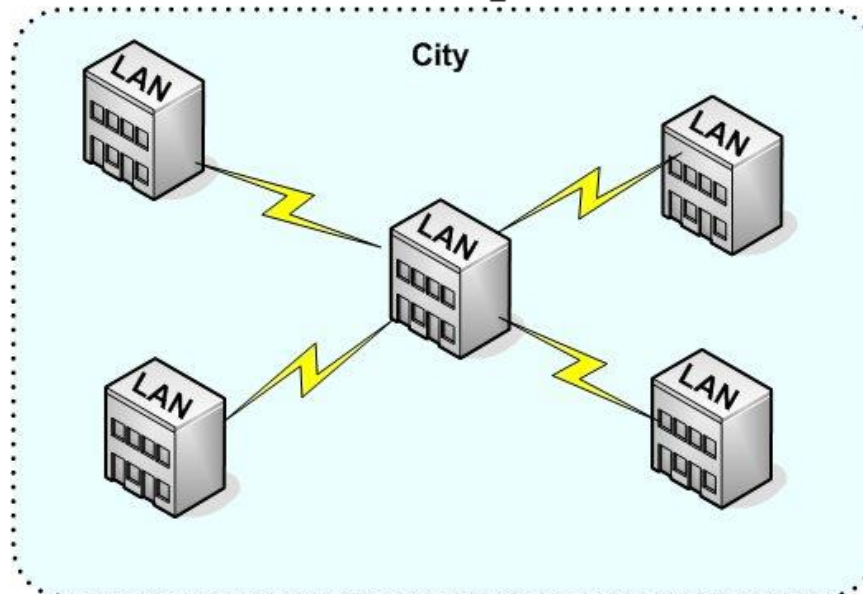
- Számítógépek
- Hálózati interfész kártyák
- Hálózati média (csavart érpár, koaxiális kábel, optikai szál, rádió hullámok)
- Hálózati eszközök: Ismétlő (Hub), Híd (Bridge), Kapcsoló (Switch), Forgalomirányító (Router)



3. Számítógép-hálózatok osztályozási szempontjai

Városi hálózatok (MAN)

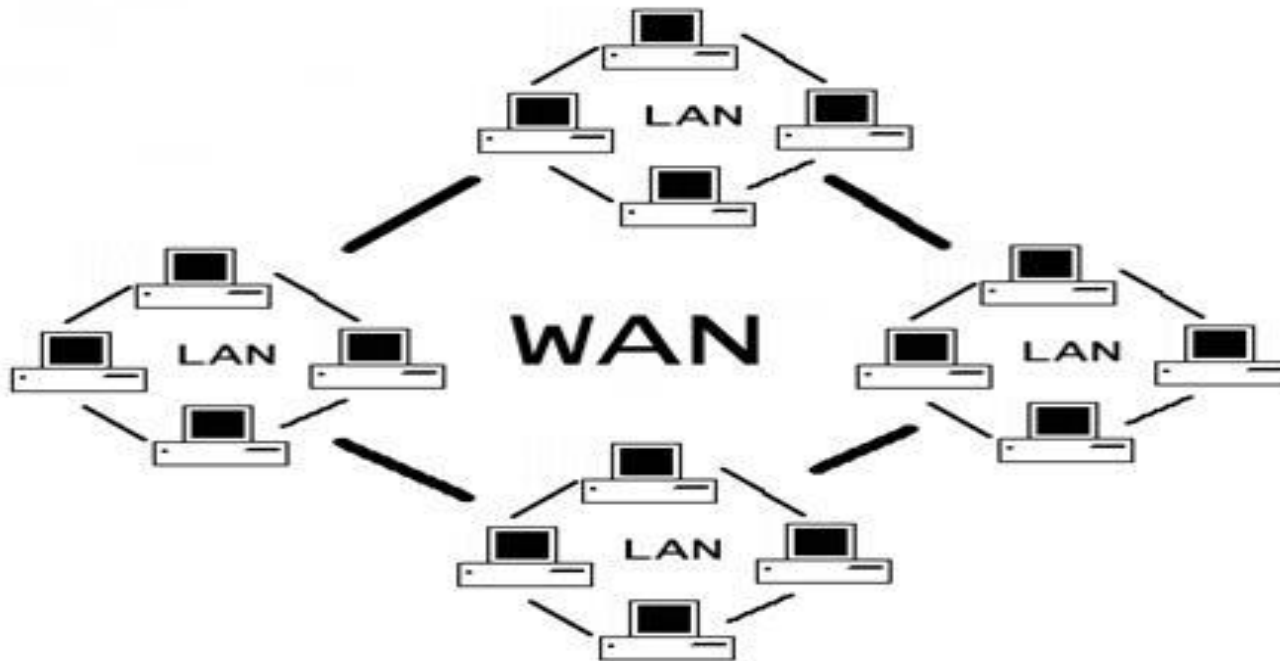
- Kiterjedése egy város vagy néhány kerület
- Két vagy több LAN-t kapcsolnak össze
- Például egy bank, utazási iroda vagy egyetem több telephellyel, irodával
- Tipikusan egy szolgáltató bérelt vonalait veszik igénybe
- Technológiájuk leggyakrabban a LAN-okéval azonos
- Egyes esetekben vezeték nélküli híd technológiát alkalmaznak az összekapcsolásra



3. Számítógép-hálózatok osztályozási szempontjai

Nagy kiterjedésű hálózatok (WAN)

- Nagy, földrajzilag elkülönített területen működnek
- A felhasználók együttműködhetnek valós idejű alkalmazásokban
- Távoli erőforrások igénybevétele
- E-mail, World Wide Web, fájlátvitel és e-commerce szolgáltatások igénybevétele



4. Kommunikációs alapfogalmak

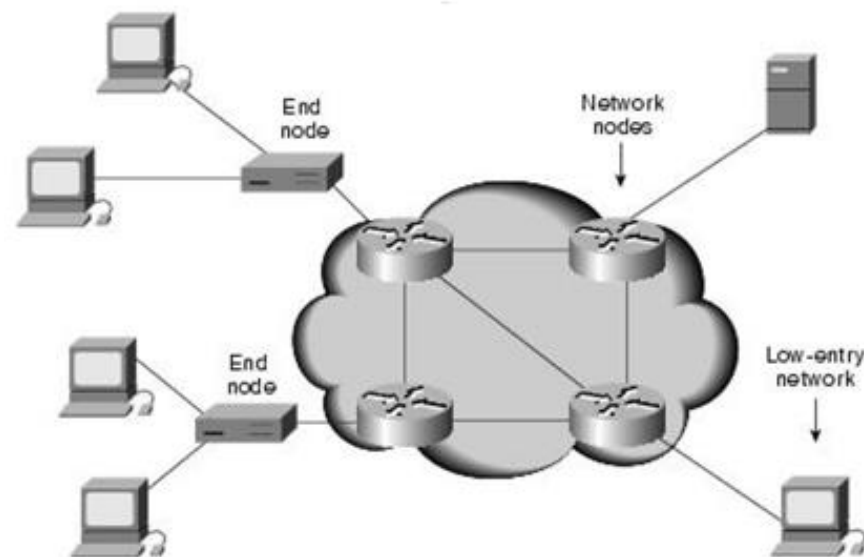
Számítógép-hálózati csomópont (kommunikációs entitás) típusok:

Csomópont (node): Önálló kommunikációra képes, saját hálózati címmel rendelkező eszköz (pl. számítógép, nyomtató, forgalomirányító). Egy kommunikációban egy csomópont működhet adó (forrás, küldő), vevő (nyelő, fogadó), illetve adó-vevő funkcióval. A csomópont kommunikációs ponton (interfészen) keresztül kommunikál.

Felhasználói csomópont (End/User node):

Kommunikációs végpont, amely információt adatként küld (forrás), vagy adatból információt nyer ki (nyelő).

Köztes csomópont (Network/Intermediate node): Csomópont, amely adatot vagy jelet továbbít más csomópontok között.



4. Kommunikációs alapfogalmak

Adatátviteli közeg, csatorna, ütközés:

Adatátviteli közeg (média, vonal): Eszköz, anyag, közeg, melyen keresztül a jel továbbítása történik. (Pl. csavart érpár, koaxiális kábel, optikai kábel, levegő, EM tér).

Adatátviteli csatorna: Jelek továbbítására szolgáló adatút (frekvenciasáv). Gyakran egy adatátviteli közegen több csatorna (adatút) van használatban.

Ütközés: Egy közös adatátviteli csatornán kettő vagy több csomópont egyszerre küld jelet. Általában egy csatornán egyszerre egyetlen adó adhat, a továbbiakban is erre építünk. Léteznek ettől eltérő kommunikációs megoldások is (ld. pl. CDMA).

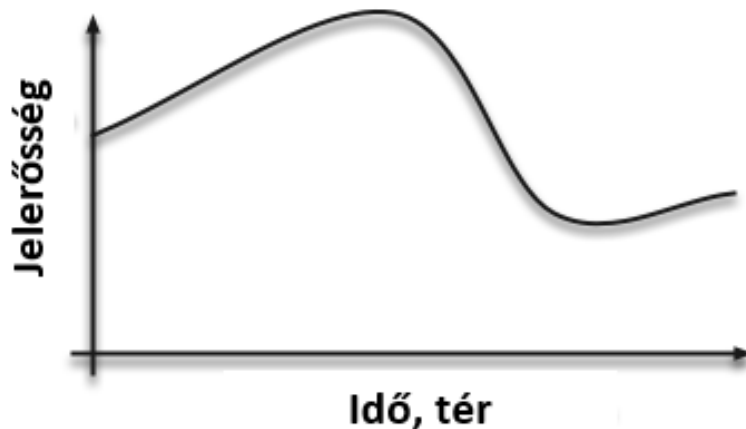
Ütközési tartomány (collision domain, bandwidth domain): Az a hálózatrész, ahol az ütközés megjelenik, érzékelhető. Az ütközési tartományban egyszerre csak egy adatátvitel történhet. Logikailag, egy ütközési tartomány egy közös csatornával rendelkező hálózatrészként reprezentálható. Itt az „egyszerre” jelentése relatív.

4. Kommunikációs alapfogalmak

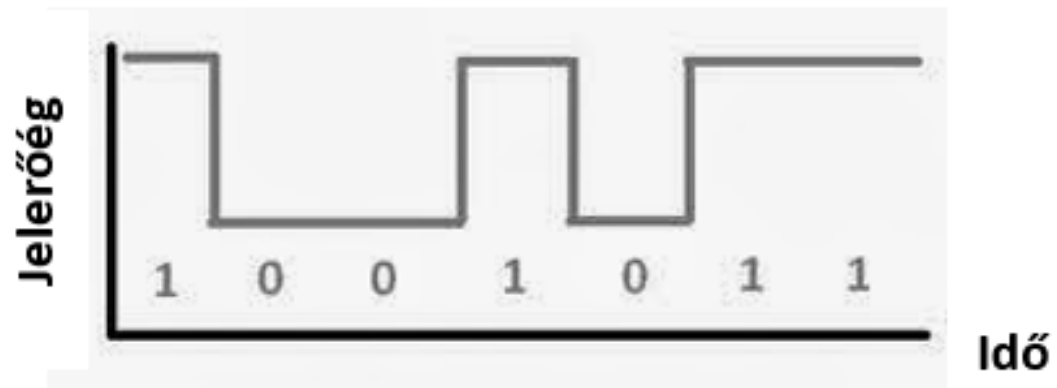
Jel, kódolás, moduláció, multiplexelés:

Jel: Helytől és időtől függő, adatot hordozó fizikai mennyiség(ek). Adathordozó a kommunikációs csatornán. Lehet analóg vagy digitális.

Analóg jel



Digitális jel



4. Kommunikációs alapfogalmak

Jel, kódolás, moduláció, multiplexelés:

Jelkódolás: A (digitális) adat leképezése (digitális) vivőjelre (pl. feszültségszintekre, feszültségszint-váltásokra). (Mi csak digitális kódolással foglalkozunk, de természetesen létezik nem digitális variáns is).

Moduláció/Demoduláció: Az adatátviteli csatorna egy frekvenciasávként jeleníthető meg legegyszerűbben (analóg vivőfrekvencia). A moduláció a továbbítandó (digitális) adatnak az analóg vivőjelre történő leképezése. Tipikusan az analóg vivőfrekvencia valamely paraméterének (pl. amplitúdó, fázis, stb.) jól meghatározott elven történő megváltoztatásával történik. Inverz (vevő oldali) folyamata a demoduláció. A modem a **modulációt** és **demodulációt** végző berendezés.

Multiplexelés/Demultiplexelés: Két (vagy több) jól elkülöníthető (különböző) kommunikációnak azonos vonalon (vagy csatornán) egyidőben történő küldése (multiplexelés). A nyelő (vételi) oldalon a szétválasztás a demultiplexelés.

4. Kommunikációs alapfogalmak

Adatátviteli sebesség (adatátviteli ráta):

Adatátviteli sebesség (hálózati sebesség, sávszélesség, bitráta, bandwidth):

Időegység alatt átvitt bitek mennyisége.

Mértékegysége:

bit/másodperc,

b/s,

bps.

Az adatátviteli sebességet tipikusan a csatorna kapacitásának mérésére, jelzésére használják.

Nagyobb egységek:

1 kbps	1.000 bps				10^3 bps
1 Mbps	1.000 kbps	1.000.000 bps			10^6 bps
1 Gbps	1.000 Mbps	1.000.000 kbps	1.000.000.000 bps		10^9 bps
1 Tbps	1.000 Gbps	1.000.000 Mbps	1.000.000.000 kbps	1.000.000.000.000 bps	10^{12} bps

4. Kommunikációs alapfogalmak

Moduláció sebesség:

Moduláció sebesség (jelváltás sebesség): Időegység alatt bekövetkező jelváltások száma, vagyis a csatornán érvényes szimbólumok közötti átmenetek száma.

Mértékegysége:

jelváltás/másodperc (baud)

A modulációsebesség és az adatátviteli sebesség (természetesen) különböző mennyiségek mérésére szolgál, de egy konkrét, jól meghatározott környezetben a két mennyiség között szoros összefüggés áll fenn.

Nagyobb egységek:

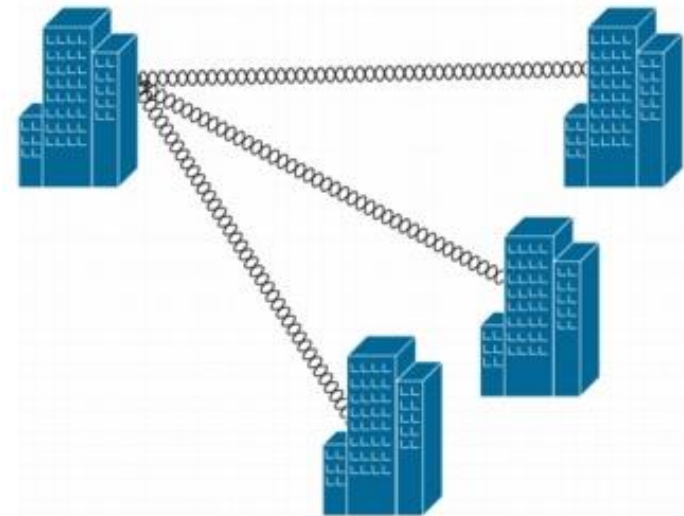
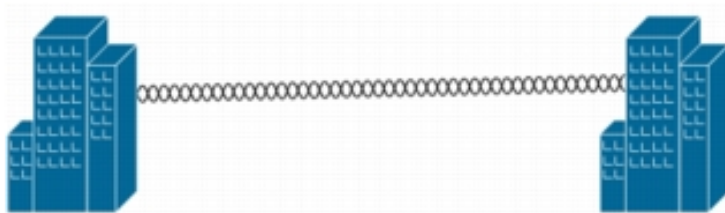
1 kbaud	1.000 baud				10^3 baud
1 Mbaud	1.000 kbaud	1.000.000 baud			10^6 baud
1 Gbaud	1.000 Mbaud	1.000.000 kbaud	1.000.000.000 baud		10^9 baud
1 Tbaud	1.000 Gbaud	1.000.000 Mbaud	1.000.000.000 kbaud	1.000.000.000.000 baud	10^{12} baud

4. Kommunikációs alapfogalmak

Adatátviteli kapcsolattípusok:

Pont-pont kapcsolat (Point-To-Point): Csak két pont (egy adó és egy vevő) között zajlik a kommunikáció (pl. huzal két végén lévő egy-egy gép).

Többpontos kapcsolat, üzenetszórás (point-to-multipoint, broadcast): Egyetlen adó egyszerre több vevőt lát el adattal. Az üzenetszórás olyan többpontos kapcsolat, ahol az adótól egy bizonyos hatósugáron belül minden vevő megkapja az információt (pl. rádiós műsorszórás).



4. Kommunikációs alapfogalmak

Információátvitel irányítottsága:

Egyirányú (szimplex) összeköttetés: Két kommunikációs pont közötti adatátvitel csak egy irányban lehetséges (pl. rádiós műsorszórás).

Kétirányú (duplex) összeköttetés: Két kommunikációs pont közötti adatátvitel mindkét irányban lehetséges (pl. rádiós műsorszórás).

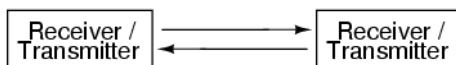
- **Váltakozó irányú (half-duplex) összeköttetés:** Két kommunikációs pont közötti adatátvitel mindkét irányban lehetséges, de egyszerre csak az egyik irányban (pl. CB rádió).

- **Kétirányú (full-duplex) összeköttetés:** Két kommunikációs pont közötti adatátvitel mindkét irányban egyszerre lehetséges (pl. telefon). Ez logikailag két, egymástól független szimplex összeköttetésnek fogható fel.

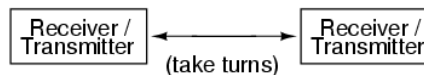
Simplex communication



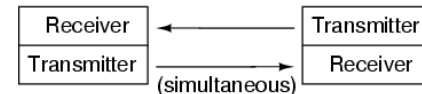
Duplex communication



Half-duplex



Full-duplex



4. Kommunikációs alapfogalmak

Kapcsolási módok:

Vonalkapcsolt (áramkörkapcsolt, circuit switched) technológia: Az adatátvitel előtt dedikált kapcsolat (kommunikációs áramkör) épül ki a két végpont között, s ez folyamatosan fennáll, amíg a kommunikáció tart. (Pl. klasszikus vonalas telefon.)

Üzenetkapcsolt (store and forward) technológia: Nem épül ki áramkör, hanem a teljes üzenet kapcsolóközpontról kapcsolóközpontra halad, mindig csak egy összeköttetés szakaszt terhelve. (Pl. telex)

Csomagkapcsolt (packet switched) technológia: Az adatot korlátozott maximális méretű részekre (csomagokra) darabolják, s ezeket mint önálló elemeket egymás után továbbítják. A módszert a jól tervezhető puffereelési tulajdonsága miatt előszeretettel alkalmazzák.

4. Kommunikációs alapfogalmak

Címzési alapfogalmak:

Kézbesítés érdekében szükség van a csomópontok (gépek) egyértelmű azonosítására (mint pl. a postai kézbesítőrendszerben is). Az üzenetekben tipikusan két azonosító jelenik meg: a feladó, és a cél azonosítója. A cél azonosítója (címe) nem feltétlenül egyetlen csomópont azonosítására szolgál, mivel többféle címkategória létezik:

Egyedi cím (Unicast address): Egy kommunikációs entitás adott kommunikációs pontjára (interfészére) vonatkozó azonosító. Az üzenetekben szereplő feladó cím tipikusan egyedi (unicast) cím. Általában egy hálózati interfész egy egyedi címet kap azonosítási célból, de ez nem kötelező elv minden technológiánál.

Bárki cím (Anycast address): A kommunikációs pontok egy halmazát (tipikusan különböző csomópontokon található interfészek halmazát) azonosító cím. Ha egy csomagot egy „bárki címre” küldünk, akkor azt a halmazból legalább egy interfészre (célszerűen a legközelebbire) kell eljuttatni.

4. Kommunikációs alapfogalmak

Címzési alapfogalmak:

Többes cím (Multicast address): A kommunikációs pontok egy halmazát vagy csoportját (tipikusan különböző csomópontokon található interfészek csoportját) azonosító cím. Erre a címre küldött csomagnak a csoport mindegyik tagjához el kell jutnia.

Üzenetszórási ("mindenki") cím (Broadcast address): Egy jól meghatározott hálózatrészen (ún. üzenetszórási tartományon, broadcast domain) belül elhelyezkedő valamennyi csomópontot (ill. csomópontok interfészét) azonosító cím. Logikailag speciális multicast címnek is felfogható, ahol a csoport az üzenetszórási tartomány valamennyi kommunikációs pontját magába foglalja.

Üzenetszórási tartomány (broadcast domain): Az a hálózatrész, ahol az üzenetszórás célcímmel feladott kommunikációs elem (csomag) megjelenik, érzékelhető.

4. Kommunikációs alapfogalmak

Kommunikációs protokoll és elemei:

Protokoll: Szabályok és konvenciók összességének egy formális leírása, mellyel meghatározzák a hálózati entitások (eszközök, csomópontok) kommunikációját (kommunikációs szabályok halmaza).

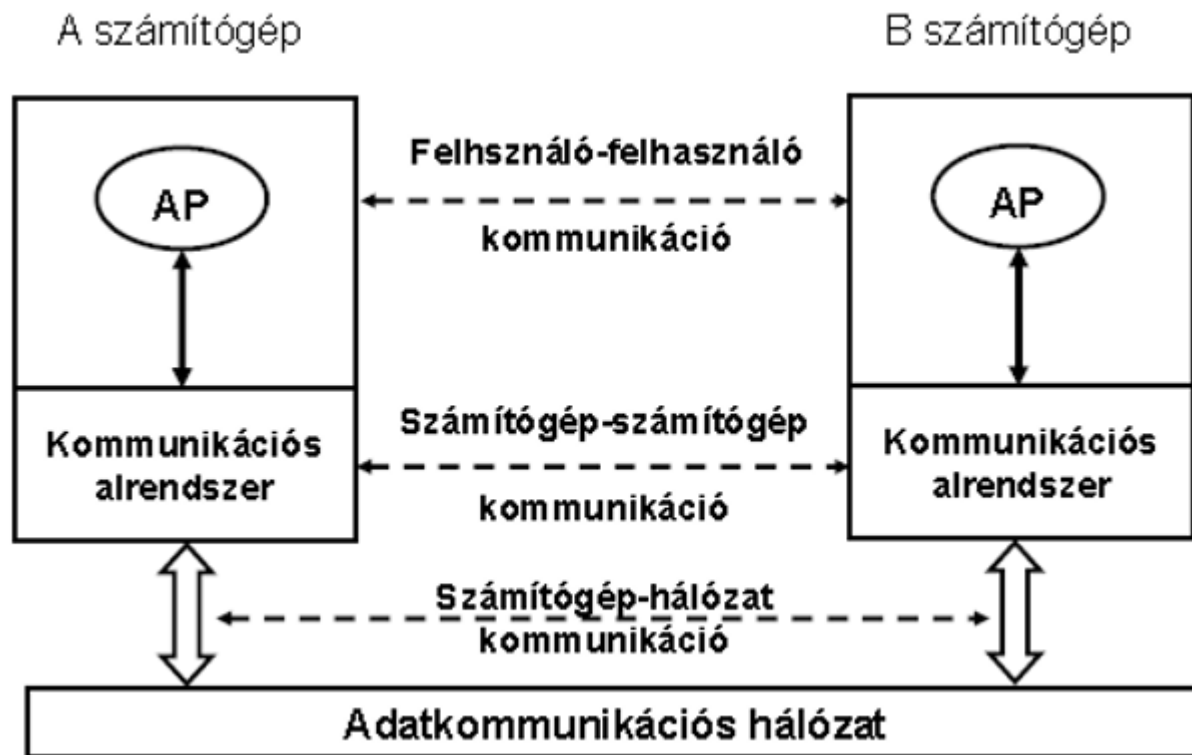
A protokollok pontos leírására általában speciális eszközöket alkalmaznak: pl. kiterjesztett véges automaták, SDL (Specification and Description Language), magasszintű nyelvek.

Protokoll entitás (PE – Protocol Entity): A forrás és/vagy cél kommunikációját megvalósító hálózati entitás (hardver/firmware és/vagy szoftver). Pl. kommunikációs eszköz, kommunikációs program.

Protokoll adatelem (PDU – Protocol Data Unit): A kommunikáció során továbbított adat (rekord), amely a protokoll entitások között a protokoll szabályok szerint továbbítódik. Szerkezete és mérete az adott kommunikációs technológia előírása szerinti.

4. Kommunikációs alapfogalmak

Kommunikáció működési alapelve:



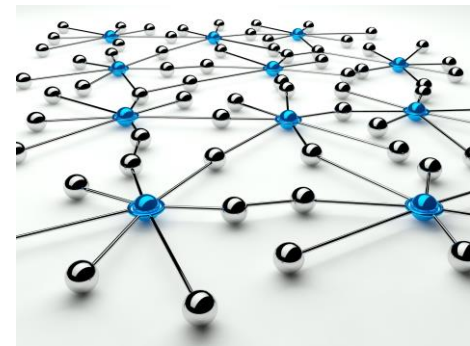
Hálózati architektúrák és protokollok

2. HÁLÓZATI MODELLEK, RÉTEGEK, ESZKÖZÖK

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Rétegelt hálózati architektúra
- 2) OSI referenciamodell és rétegei
- 3) TCP/IP – OSI modell leképezése
- 4) Hibrid referenciamodell
- 5) Hálózati köztes csomópont típusok és funkcióik
 - Jelisméltő
 - Híd/kapcsoló
 - Útválasztó
 - Átjáró

1. Rétegzett hálózati architektúra

Megfontolás:

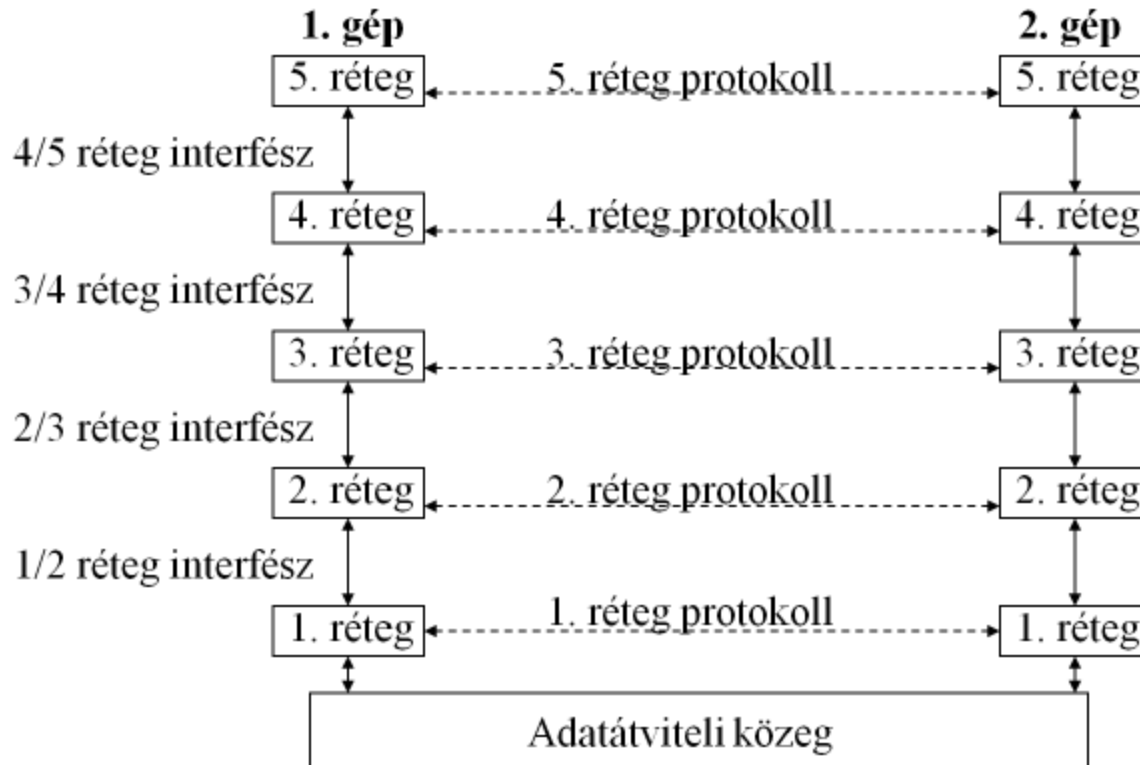
Egy protokoll leírása, pontos specifikációja általában nehéz, komplex feladatot jelent. Hierarchikus rendben felépített protokoll-rendszer könnyebben kezelhető, áttekinthetőbb. Egy ilyen rendszerben a változások könnyebben követhetők, és a hierarchia különböző szintjeit különböző gyártók is implementálhatják anélkül, hogy ez együttműködési problémákat okozna.

Példa: Üzenetküldés távoli cégvezetők között



1. Réteget hálózati architektúra

Rétegek (szintek), protokollok, interfészek:



1. Rétegelt hálózati architektúra

Rétegelt hálózati architektúra - fogalmak

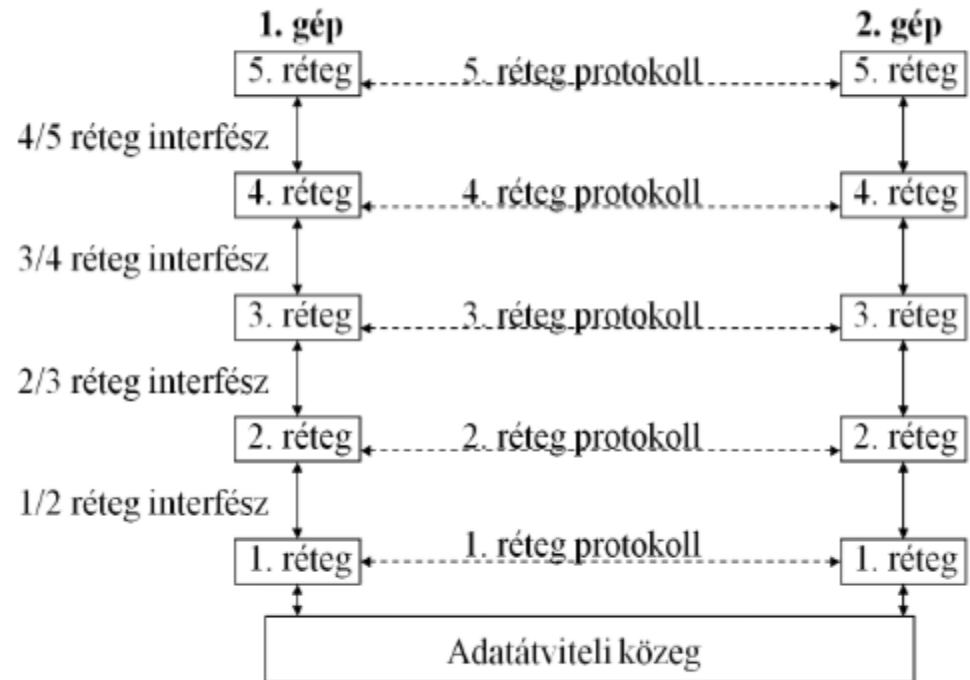
N. réteg protokoll:

Az N. réteg (szint) specifikációját leíró protokoll.

Társ entitások (peer entities):

A két kommunikációs végpont (csomópont) azonos szintjén elhelyezkedő entitások.

Logikailag a társ entitások kommunikálnak egymással a megfelelő réteg protokollját használva.



1. Rétegelt hálózati architektúra

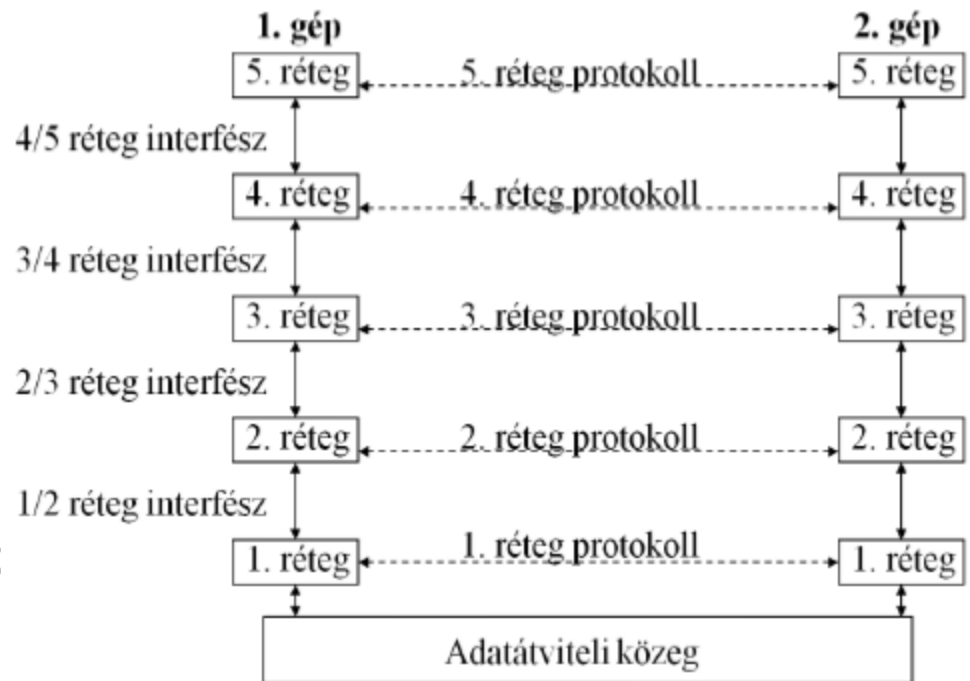
Rétegelt hálózati architektúra - fogalmak

N/N+1 szint interfész:

Az N. és N+1. réteg kapcsolódási felülete, határfelülete. Az interfészen keresztül a kommunikáció tárgyát képező adatok mellett különböző vezérlő információk is továbbíthatók.

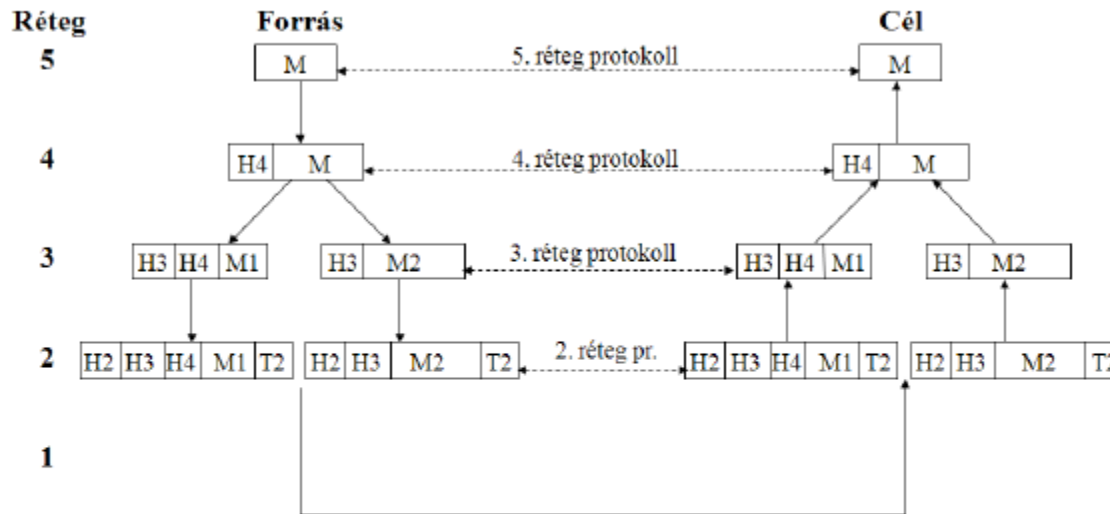
N. réteg szolgáltatása:

Azon művelethalmaz (szolgáltatás), melyet az N. réteg nyújt az N+1. réteg számára (az interfészen keresztül).



1. Réteget hálózati architektúra

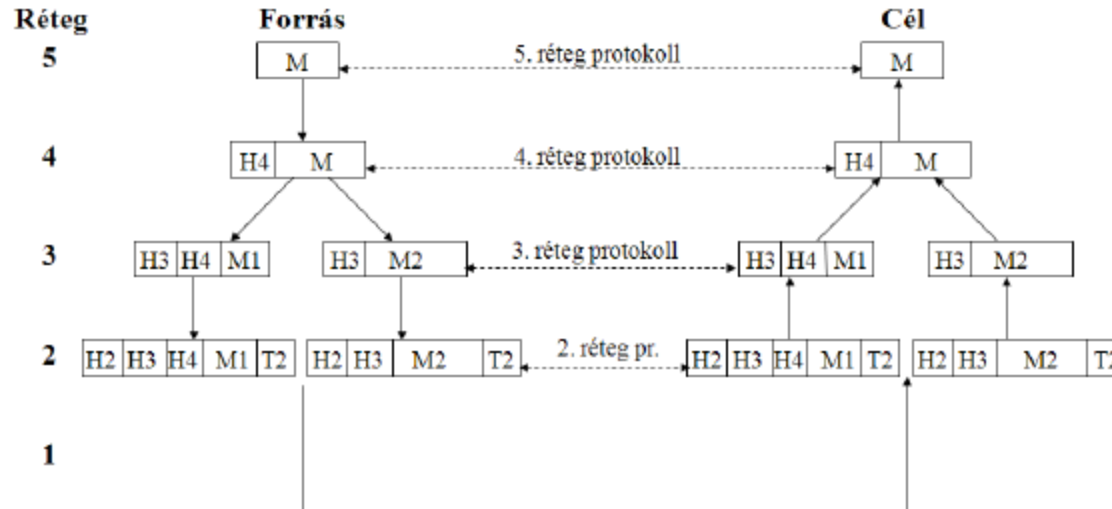
Hálózati kommunikáció vázlata



A legfelső rétegben jelenik meg a kommunikáció tárgyát képező üzenet (M). Logikailag a legfelsőbb rétegbeli (a példában az 5. rétegbeli) entitás az üzenetet a társ entitásnak (5. rétegben) küldi, az adott réteg működését leíró protokoll alapján.

1. Rétegelt hálózati architektúra

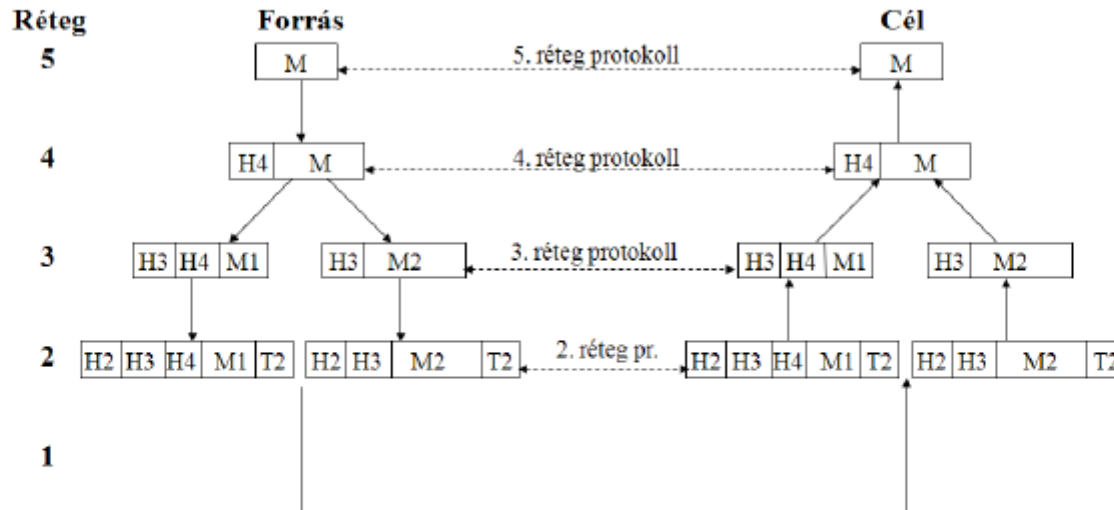
Hálózati kommunikáció vázlata



Valójában az adó (forrás) oldalon egy adott rétegbeli entitás az alatta elhelyezkedő rétegnek adja tovább az üzenetet (az 5. réteg a 4. réteg által nyújtott szolgáltatásokra építve látja el a feladatát). Az alsóbb réteg (4. réteg) a saját funkcionálisainak az ellátásához további mezőket társít a felsőbb rétegtől kapott adatelem elé ("H" fejrész, "header"), vagy esetleg az után ("T" végrész, "tailor", pl. ellenőrző összeg).

1. Rétegelt hálózati architektúra

Hálózati kommunikáció vázlata

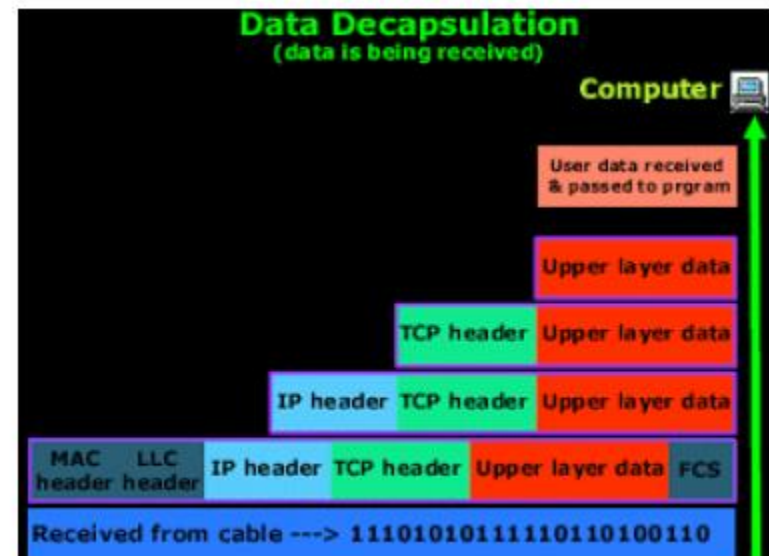
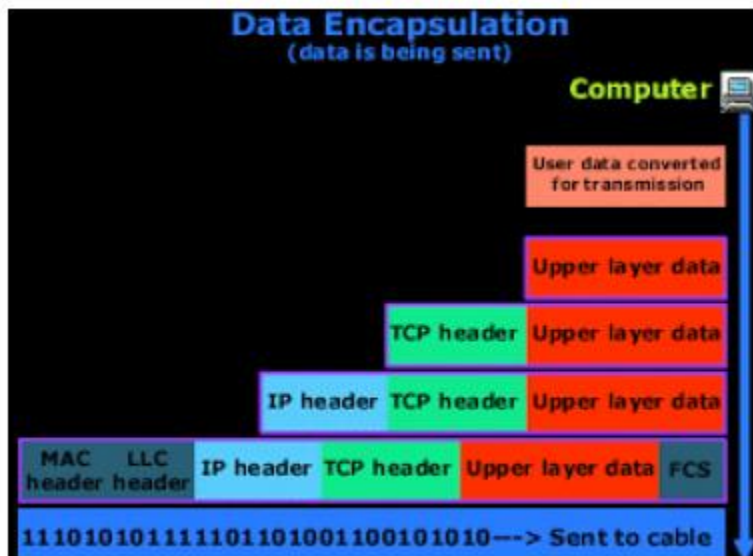


Az egyes rétegekben megadott méretkorlátok miatt előfordulhat, hogy a felsőbb rétegben egy adatelemként megjelenő üzenetet darabolni kell (ld. a példa 3. rétegében). A darabolás (fragmentálás) után létrejött adatelemek külön-külön haladnak a cél felé, s a célhelyen a megfelelő réteg (jelen példában a 3. réteg) a darabokat összeillesztve adja tovább az eredeti adatelemet a felsőbb réteg számára.

1. Rétegelt hálózati architektúra

Hálózati kommunikáció - fogalmak

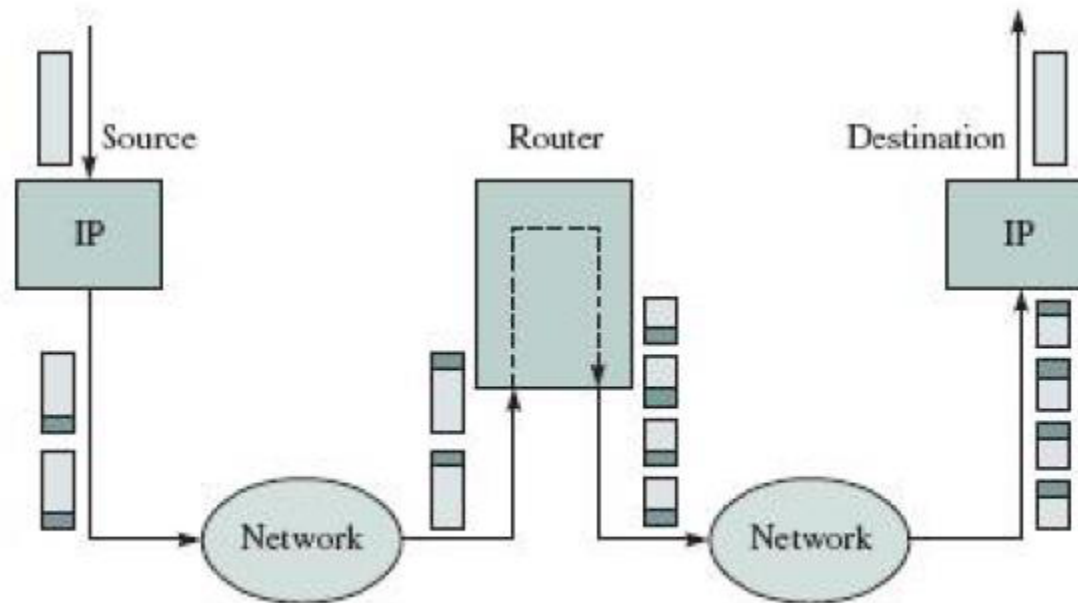
Beágyazás (encapsulation) és kiemelés (decapsulation): A felsőbb szintről érkező, s az adott réteg által már nem módosítható adat (ún. Service Data Unit, SDU) egy bizonyos protokoll fejlécével történő kiegészítése, becsomagolása az aktuális rétegben (mint pl. levél küldésekor a borítékba helyezés és a boríték címezése).



1. Réteget hálózati architektúra

Hálózati kommunikáció - fogalmak

Darabolás (fragmenting) és visszaállítás (reassembly): A felsőbb rétegtől átvett SDU kisebb részenként történő küldése a nagy méret miatt. A kisebb részek öröklék az SDU (módosított) fejrészét. A célnál a folyamat fordítottja a visszaállítás.

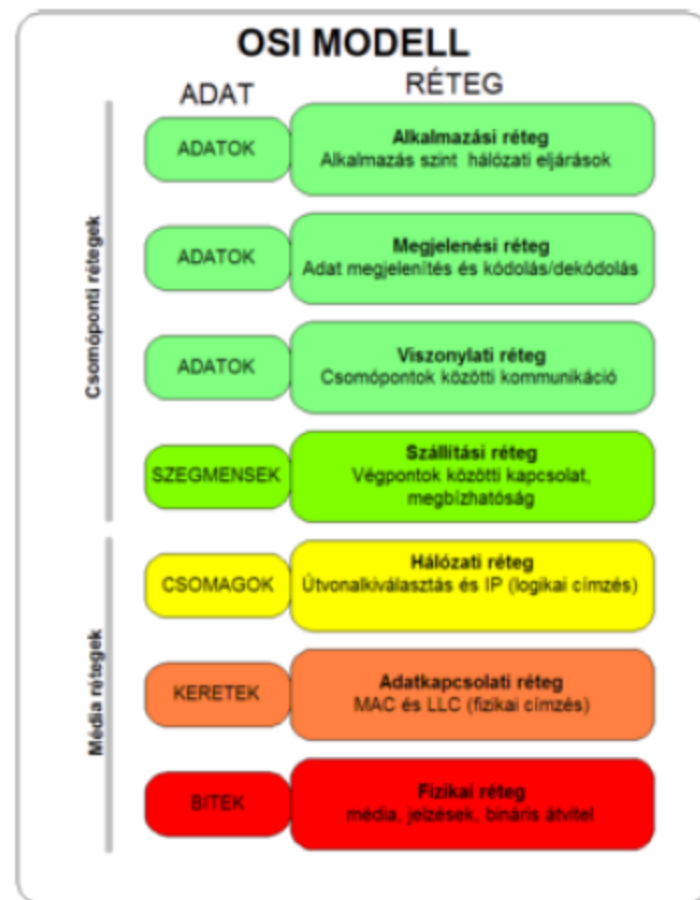


2. OSI referenciamodell és rétegei

ISO OSI

A nemzetközi szabványügyi hivatal (ISO) által elfogadott hét rétegű (ún. nyílt rendszerek összekapcsolási, OSI – Open System Interconnect) modellje.

Sorszám	Réteg neve	PDU neve	
7.	Applikációs réteg (Application Layer)	Üzenet (APDU)	Message
6.	Megjelenítési réteg (Presentation Layer)	Üzenet (PPDU)	Message
5.	Viszonyi réteg (Session Layer)	Üzenet (SPDU)	Message
4.	Szállítási réteg (Transport Layer)	Szegmens (TPDU)	Segment
3.	Hálózati réteg (Network Layer)	Csomag	Packet
2.	Adatkapcsolati réteg (Data Link Layer)	Keret, cella	Frame, cell
1.	Fizikai réteg (Physical Layer)	Bit	Bit



2. OSI referenciamodell és rétegei

Az OSI modell rétegei

- 1. Fizikai réteg:** Elektromos és mechanikai jellemzők procedurális és funkcionális specifikációja két (közvetlen fizikai összeköttetésű) eszköz közötti jeltovábbítás céljából.
- 2. Adatkapcsolati réteg:** Megbízható adatátvitelt biztosít egy fizikai összeköttetésen keresztül. Ezen réteg problémaköréhez tartozik a fizikai címezés, hálózati topológia, közeghozzáférés, fizikai átvitel hibajelzése és a keretek sorrendhelyes kézbesítése. Az IEEE két alrétegre (MAC, LLC) bontotta az adatkapcsolati réteget.
- 3. Hálózati réteg:** Összeköttetést és útvonalválasztást biztosít két hálózati csomópont között. Ehhez a réteghez tartozik a hálózati címezés és az útvonalválasztás (routing).

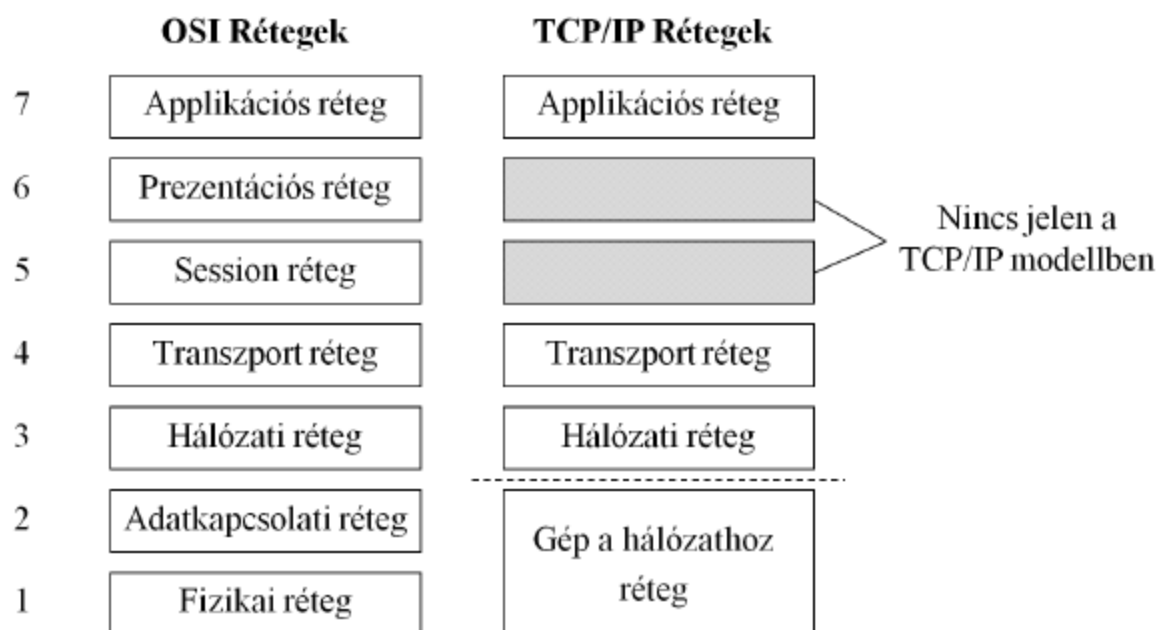
2. OSI referenciamodell és rétegei

Az OSI modell rétegei

- 4. Szállítási réteg:** Megbízható hálózati összeköttetést létesít két csomópont között. Feladatkörébe tartozik pl. a virtuális áramkörök kezelése, átviteli hibák felismerése/javítása és az áramlásszabályozás.
- 5. Viszony réteg:** Ez a réteg építi ki, kezeli és fejezi be az applikációk közötti dialógusokat (session, dialógus kontroll).
- 6. Megjelenítési (prezentációs) réteg:** Feladata a különböző csomópontokon használt különböző adatstruktúrákból eredő információ-értelmezési problémák feloldása.
- 7. Applikációs (alkalmazási) réteg:** Az applikációk (fájltávitel, e-mail stb.) működéséhez nélkülözhetetlen szolgáltatásokat biztosítja.

3. TCP/IP – OSI modell leképezése

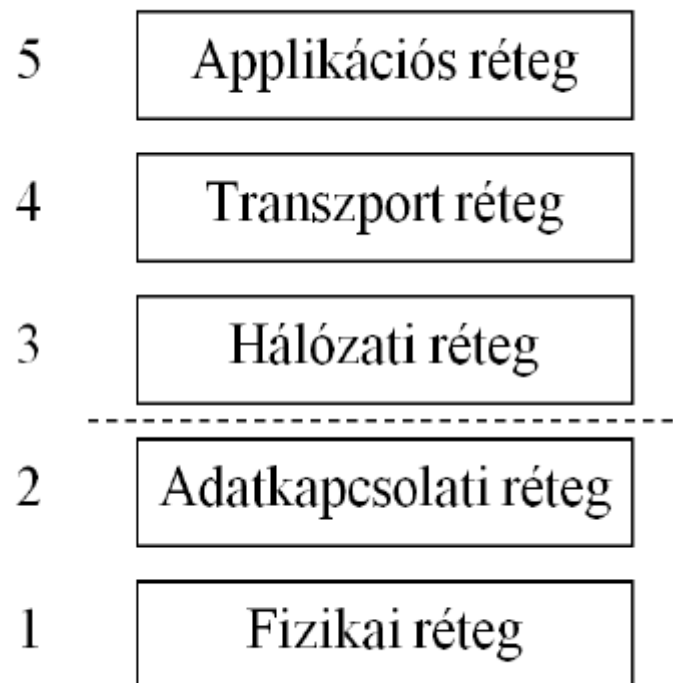
Megfontolás: A hétköznapi életben leginkább elterjedt hálózati technológia a TCP/IP protokollrendszerre épülő hálózat (Internet). A TCP/IP architektúra (korántsem egységes) modellszemlélete eltér az OSI modell szemléletmódjától:



4. Hibrid referenciamodell

Megfontolás: A. S. Tanenbaum (több kiadásban is megjelent) Számítógép-hálózatok c. művében javasolta, hogy a hálózati kommunikáció tanulmányozására egy ún. "hibrid modellt" használjunk: A hibrid modell alsó két rétegében (az OSI modellt követve) a fizikai és adatkapcsolati réteg jelenik meg, a felsőbb rétegeket pedig (a TCP/IP modellt követve) a hálózati, szállítási (transzport), és az applikációs rétegek képviselik.

A továbbiakban a hibrid modell szemléletmódját követve vizsgáljuk a hálózatokat.



5. Hálózati köztes csomópont típusok és funkcióik

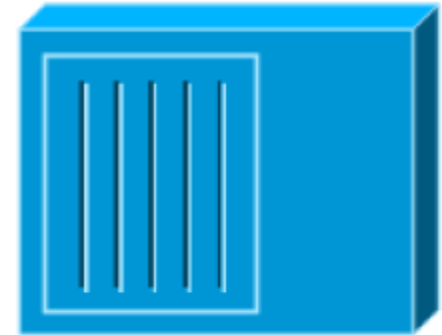
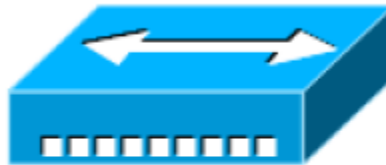
Megfontolás: Az egyes hálózatrészek összekapcsolására szolgáló eszközök különböző OSI rétegekbe sorolhatók. Ez az osztályozás a köztes csomópont működési funkcionalitása alapján történik.

Réteg	Köztes csomópont (eszköz)
Transzport réteg (és felette)	Átjáró (gateway)
Hálózati réteg	Forgalomirányító, útválasztó (router)
Adatkapcsolati réteg	Híd, kapcsoló (bridge, switch)
Fizikai réteg	Jelismétlő (repeater, hub)

5. Hálózati köztes csomópont típusok és funkcióik

Jelismétlő (repeater/hub):

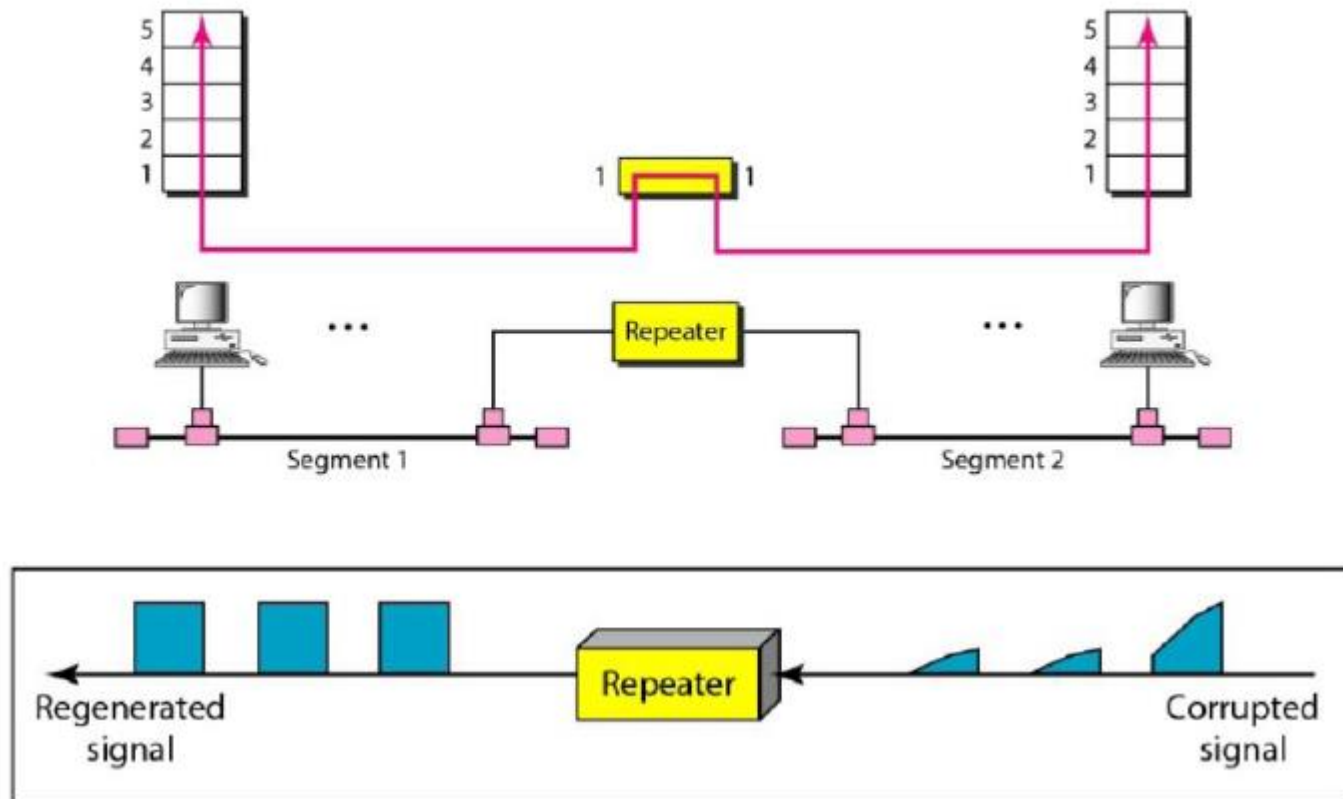
- Az átviteli közegen továbbított jeleket ismétli, erősíti, időzítésüket szabályozza
- Az összekapcsolt részhálózatokat (ütközési tartományokat) nem izolálja
- Strukturált hálózatban alkalmazott változat neve: hub



L1 animáció START

5. Hálózati köztes csomópont típusok és funkcióik

Jelismétlő (repeater/hub):



5. Hálózati köztes csomópont típusok és funkcióik

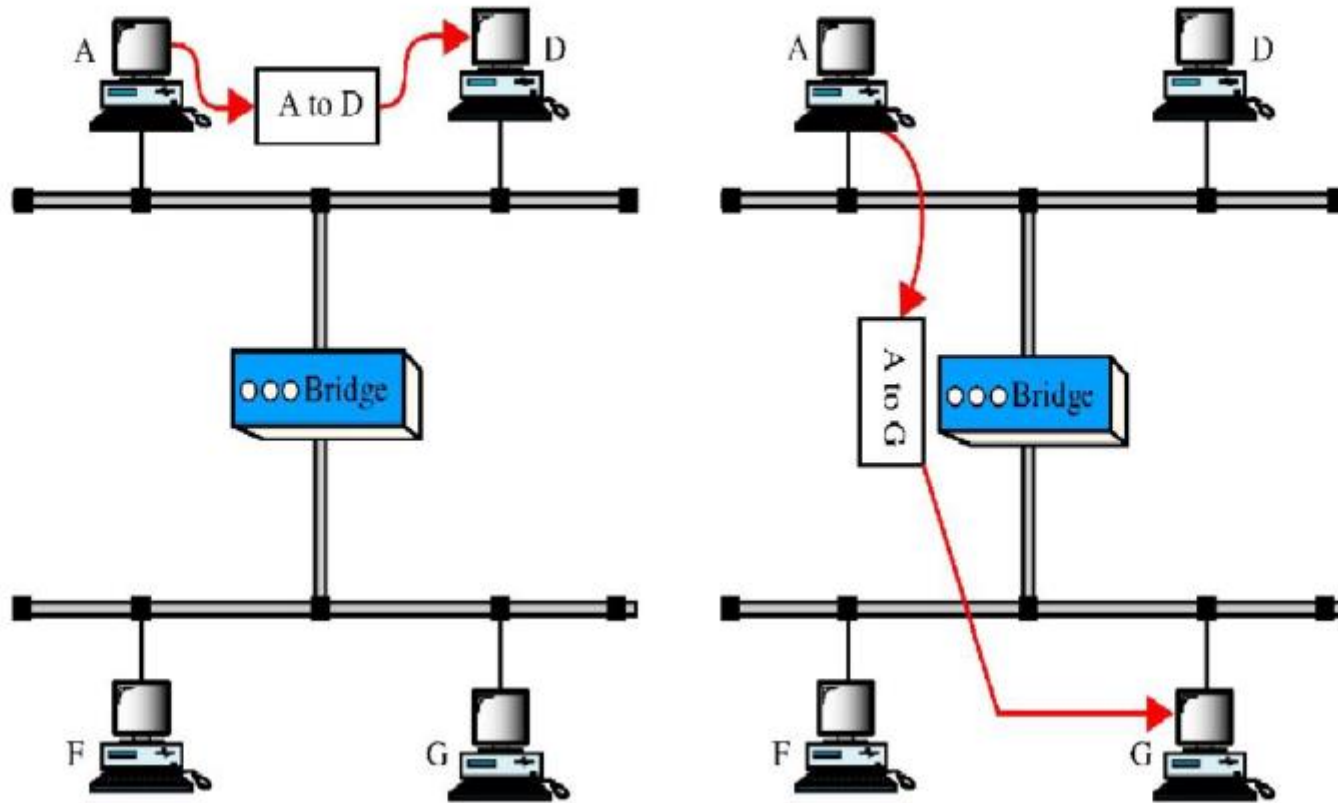
Híd (bridge):

- Fizikai **és** adatkapcsolati rétegben működve szelektív összekapcsolást végez („csak az megy át a hídon, aki a túloldalra tart”).
- Az összekapcsolt részhálózatok külön ütközési tartományt alkotnak.
- Az üzenetszórást általában minden összekapcsolt részhálózat felé továbbítja.
- Egyprocesszoros rendszer, ami a kapcsolást szoftveresen végzi.
- A portok sűrűsége alacsony (2/4).



5. Hálózati köztes csomópont típusok és funkcióik

Híd (bridge):



5. Hálózati köztes csomópont típusok és funkcióik

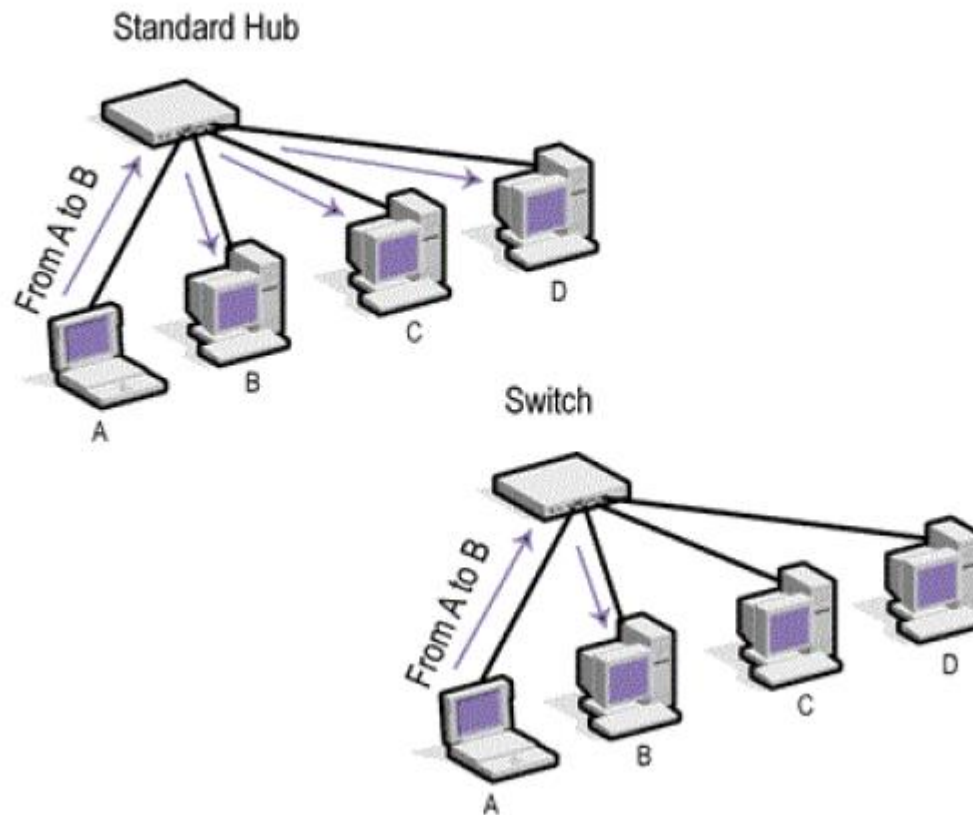
Kapcsoló (switch):

- Olyan többportos eszköz, melynek bármely két portja között híd (bridge) funkcionalitás működik.
- Kapcsoló mátrixból felépített berendezés, ami a kapcsolást firmware vagy hardver szinten végzi.
- A berendezés port-sűrűsége általában nagy (24/48/96) .



5. Hálózati köztes csomópont típusok és funkcióik

Kapcsoló (switch) és jelismétlő összehasonlítása:



5. Hálózati köztes csomópont típusok és funkcióik

Vezeték nélküli hozzáférési pont, bázisállomás (Access Point):

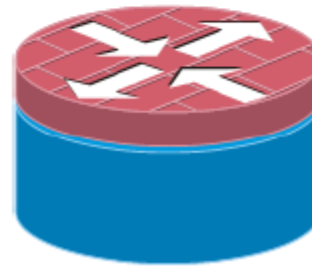
- A vezeték nélküli hozzáférési pont (AP) leggyakrabban speciális híd funkcionalitást megvalósító eszköz.
- Olyan kétportos híd, melynek egyik portja vezetékes, másik portja pedig vezeték nélküli (RF) csatornához csatlakozik.
- Az eszköz módosítja a keretet a portok közötti továbbítás közben.



5. Hálózati köztes csomópont típusok és funkcióik

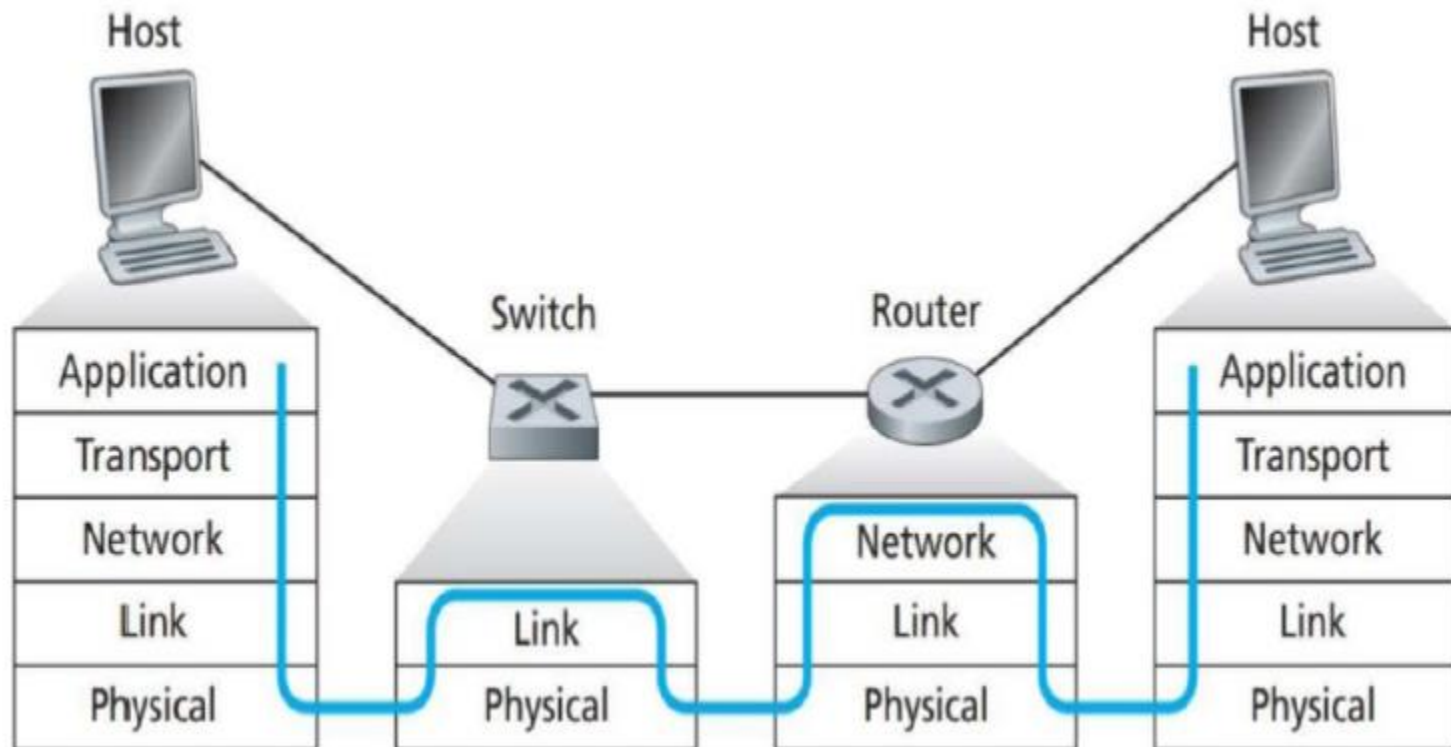
Forgalomirányító (router):

- A fizikai **és** az adatkapcsolati **és** a hálózati rétegben működve szelektív összekapcsolást, útvonalválasztást, forgalomirányítást végez.
- Az összekapcsolt részhálózatok külön ütközési tartományt és külön üzenetszórási tartományt alkotnak.
- Mindegyik interfészén saját hálózati címmel rendelkezik.



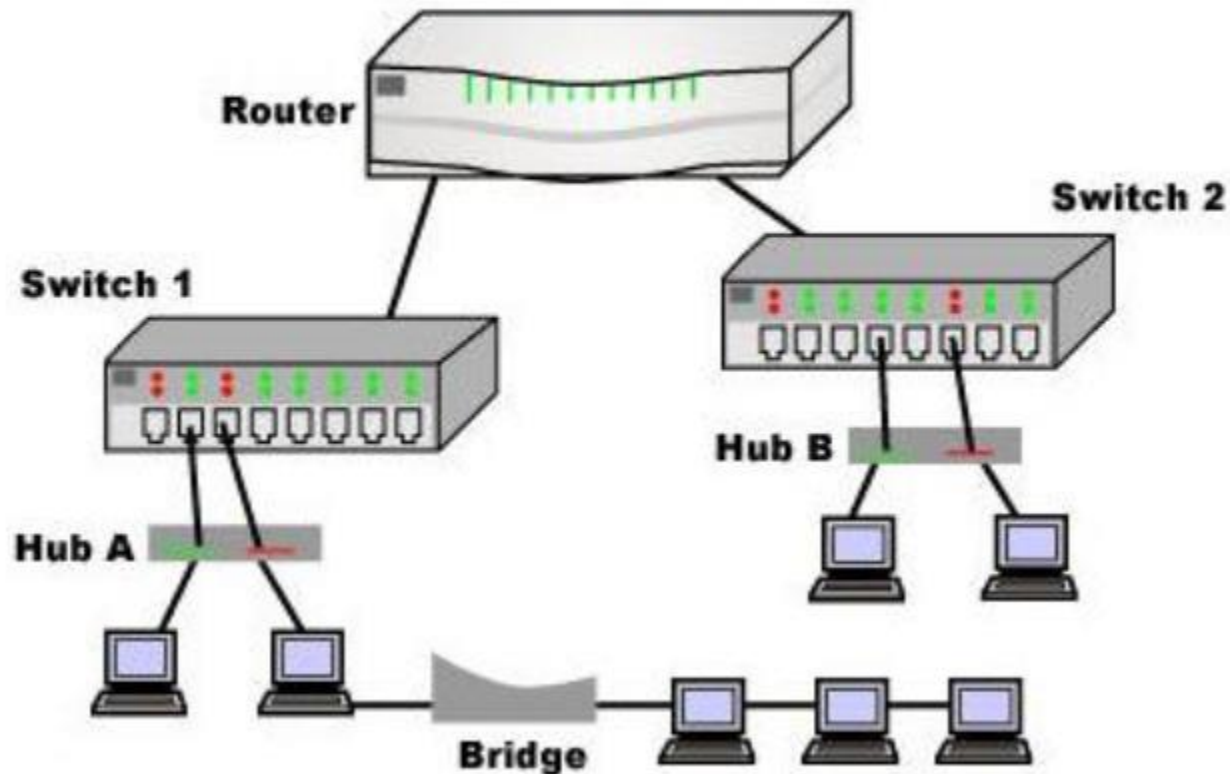
5. Hálózati köztes csomópont típusok és funkcióik

Forgalomirányító és kapcsoló összehasonlítása:



5. Hálózati köztes csomópont típusok és funkcióik

Forgalomirányító, kapcsoló és jelismétlő összehasonlítása:



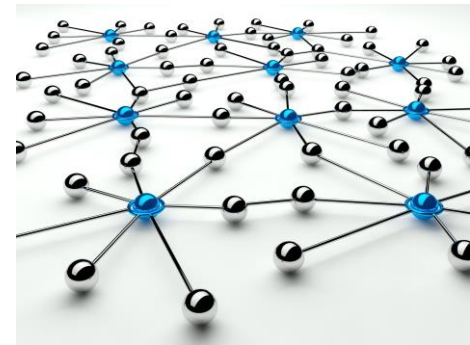
Hálózati architektúrák és protokollok

3. FIZIKAI RÉTEG

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Fizikai réteg általános jellemzése
- 2) Átviteli közegek
 - Vezetékes: sodrott érpár, koaxiális kábel
 - Vezetéknélküli: levelgő, rádiófrekvenciás csatorna
- 3) Jelkódolási technikák
- 4) Modulációs technikák

1. Fizikai réteg általános jellemzése

Megfontolás:

Az impulzuscsomagként küldött jel a csatornán történő továbbítása közben energiát veszít. A csatorna bizonyos frekvencia komponenseket jobban, másokat kevésbé nyel el (csillapít). A csatorna fizikai környezetében jelen lévő más energiaforrások befolyással vannak a csatornán lévő jelek minőségére. Minden csatornán létezik felső korlát a jeltovábbítás rátájára vonatkozóan. Ez a csatorna fizikai jellemzőitől és a környezeti jelektől függ.

Csatorna maximális adatátviteli rátája (sebessége):

Nyquist meghatározta a maximális adatátviteli sebességet zajtalan csatornára.

Ha a csatorna V darab diszkrét érték (jelszint) elkülönítésére képes, akkor:

$$C = 2 \cdot H \cdot \log_2 V$$

ahol

C : maximális adatátviteli ráta [bit/s],

H : csatorna sávszélessége (frekvenciatartománya) [Hz],

V : diszkrét jelszintek száma [Hz].

1. Fizikai réteg általános jellemzése

Vonali zaj (noise):

Az átviteli közeg környezetéből származó energia csomagokat vonali zajnak nevezik.

Az átvitt jelek csillapítása miatt a zajszint összemérhetővé válhat a jelszinttel, és a jelek helyes érzékelése lehetetlenné válhat.

Az átviteli médiumok jellemezhetők az átlagos jelteljesítmény (Signal) és zajteljesítmény (Noise) hányadosával (jel-zaj viszony, általában dB skálán mérve), jele: S/N

Shannon meghatározta a maximális adatátviteli sebességet zajos csatornára:

$$C = H \cdot \log_2 (1 + S/N)$$

ahol

C: maximális adatátviteli ráta [bit/s],

H: csatorna sávszélessége (frekvenciatartománya) [Hz],

S: jel teljesítménye [W],

N: zaj teljesítmény [W].

1. Fizikai réteg általános jellemzése

Csillapítás (A - Attenuation):

A jel amplitúdója csökken a jel haladása során az átviteli közegben. Az átviteli közeg hosszát úgy állapítják meg, hogy a jel biztonsággal értelmezhető legyen a vételi oldalon. Ha nagyobb távolságot kell áthidalni, akkor erősítők (jelismétlők) beiktatásával kell a jelet visszaállítani. A csillapítás frekvenciafüggő, ezért az erősítőknek frekvenciafüggő erősítéssel kell ezt kompenzálniuk.

A csillapítás és az erősítés mértékét decibelben (dB) adják meg:

$$A = 10 \cdot \log_{10} \frac{P_R}{P_T}$$

ahol

PR: vételi oldali teljesítmény [W],

PT: küldési oldali teljesítmény [W],

S: jel teljesítménye [W],

N: zaj teljesítmény [W].

1. Fizikai réteg általános jellemzése

Jelterjedési sebesség (v):

A forrásból küldött energia csomag (impulzus) terjedési sebessége a közegtől és a jel tartományától függ. Ez vonatkozik úgy az EM hullámokra, mint a hangra: $v = \lambda \cdot f$

Átviteli közegek, médiumok:

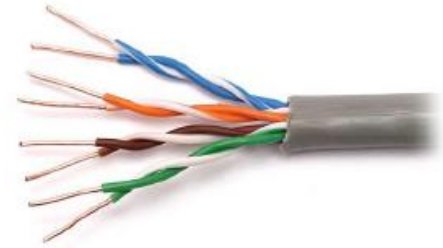
A továbbított jel fizikai megjelenési formája alapján több típust különböztetünk meg:

Jel	Közegtípus	Megjelenési forma	v [m/s]
Elektromos impulzus	Galvanikus (fém huzal)	vezetékes	$\sim 3 \cdot 10^8$
Optikai impulzus	Optikai (fénycábel)	vezetékes	$\sim 3 \cdot 10^8$
Mechanikai hullám	Levegő	vezeték nélküli	~ 340
Elektromágneses impulzus	Rádiófrekvenciás ()	vezeték nélküli	$\sim 3 \cdot 10^8$

A jeltovábbítási jellemzőik szignifikánsan eltérnek egymástól, ezért alkalmazásuk csak jól meghatározott helyen optimális.

2. Átviteli közegek

Vezetékes, galvanikus közegek:



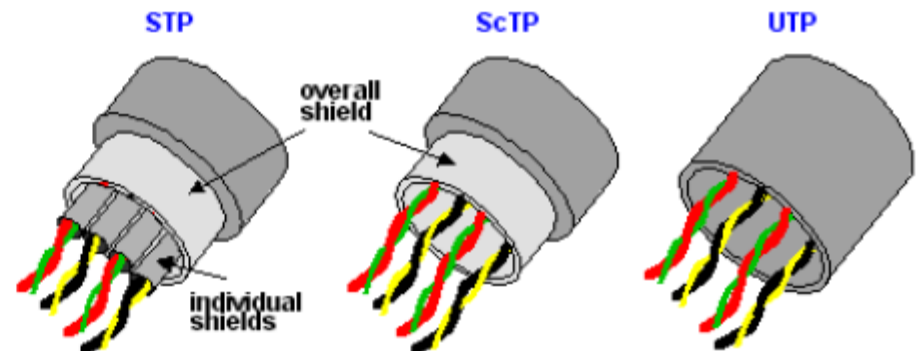
1. Sodrott érpár (Twisted Pair) megjelenési jellemzői:

- Az egyik legolcsóbb, legelterjedtebben használt jelátviteli közeg.
- Két szigetelt rézvezetékot szabályos minta szerint összezsavarnak: érpár (~0,4 / ~0,8 mm)



- A kábelben négy darab érpárt fognak össze egy külső burkolatban.
- További galvanikus árnyékolást alkalmazhatnak az EM zajok kiszűrésére.
- Típusok:

- Árnyékolatlan sodrott érpár
(UTP – Unshielded Twisted Pair)
- Árnyékolt sodrott érpár:
 - ScTP (Screened Twisted Pair),
FTP (Foiled Twisted Pair)
 - STP (Shielded Twisted Pair)



2. Átviteli közegek

Vezetékes, galvanikus közegek:

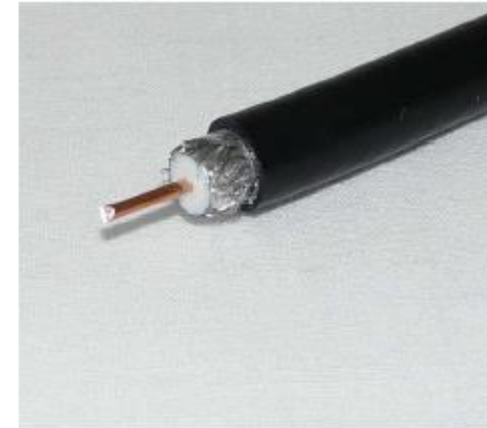
1. Sodrott érpár (Twisted Pair) jeltovábbítási jellemzői:

- A sodrás célja a külső zajok önkioltásának (Cancellation) előidézése
- Az érpárok egymásra zajhatással lehetnek, amit áthallásnak (Crosstalk) nevezünk.
- A szálpárankénti sodrás sűrűségének változása csökkenti az áthallást
- A szálpárankénti árnyékolás gyakorlatilag megszünteti az áthallást.
- Az adatátviteli kategóriák (osztályok): maximális frekvencia és átviteli ráta eltérés.
- LAN technológiáknál használatos hosszúságnál (100 m) létező jellemzők:

Kategória (USA)	Osztály (EU)	Frekvencia [MHz]	Átviteli ráta [Mbps]
Category 3	Class C	16	10
Category 5/5e	Class D	125	100/1.000 2/4 érpáron
Category 6	Class E	250	1.000 2 érpáron
Category 6A	Class EA	500	10.000
Category 7	Class F	600	10.000

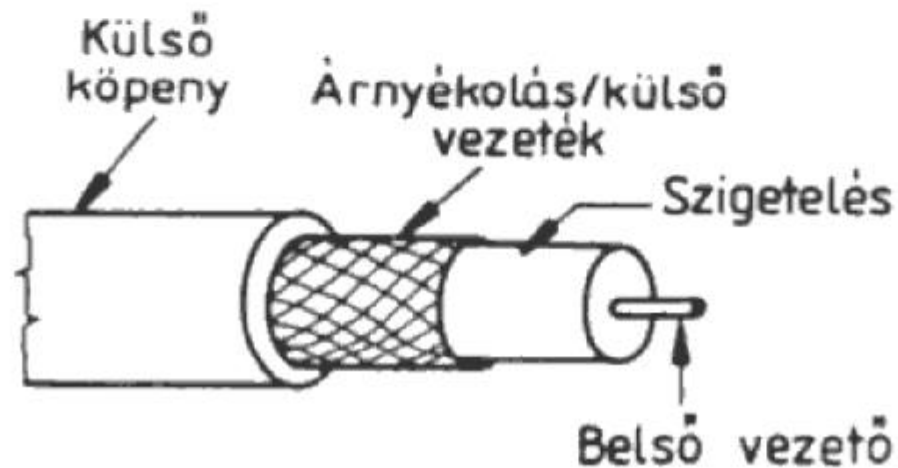
2. Átviteli közegek

Vezetékes, galvanikus közegek:



2. Koaxiális kábel megjelenési jellemzői:

- Merev, koncentrikus felépítésű
- A kábel átmérője:
 - Vékony koaxiális kábel (thin): 5 mm
 - Vastag koaxiális kábel (thick): 25 mm



2. Átviteli közegek

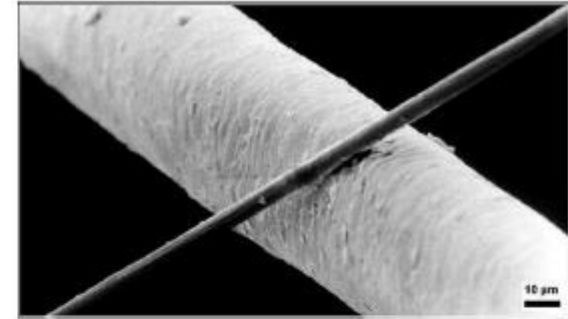
Vezetékes, galvanikus közegek:

2. Koaxiális kábel jeltovábbítási jellemzői:

- Az árnyékolás miatt kevésbé érzékeny a zavarokra, mint a csavart érpár.
- Nagyobb távolságra használható és többpontos alkalmazási változatnál több állomást is képes galvanikusan összekötni.
- Hullámellenállás (impedancia):
 - Alapsávú (baseband): 50 Ω , digitális jelátvitel
 - Szélessávú (broadband) hullámellenállása : 75 Ω , analóg jelátvitel
- Néhány km-enként szükséges erősítés.
- Alkalmazási frekvencia tartomány: ~600 MHz
- A mai (strukturált kábelezési technológiára épülő) LAN környezetben már nem használják új építésű passzív hálózatokhoz.

2. Átviteli közegek

Vezetékes, optikai közegek:

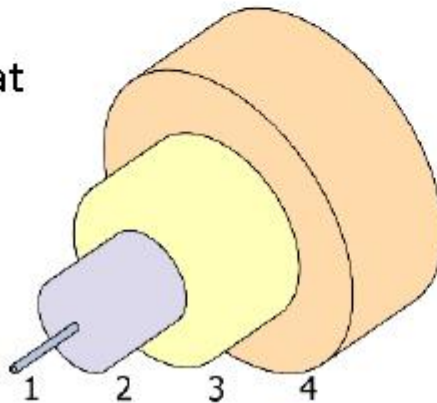


3. Optikai szál megjelenési jellemzői:

- Fénysugár továbbítására alkalmas hajlékony, átlátszó anyag (üveg, műanyag)
- Felépítése: köpeny, puffer, védőburkolat/héj (D), mag (d)
- Több szál együtt: nyaláb, több nyaláb együtt: kábel

Optikai szál

- 1 – Mag
- 2 – Védőburkolat
- 3 – Puffer
- 4 – Köpeny



Optikai kábel



2. Átviteli közegek

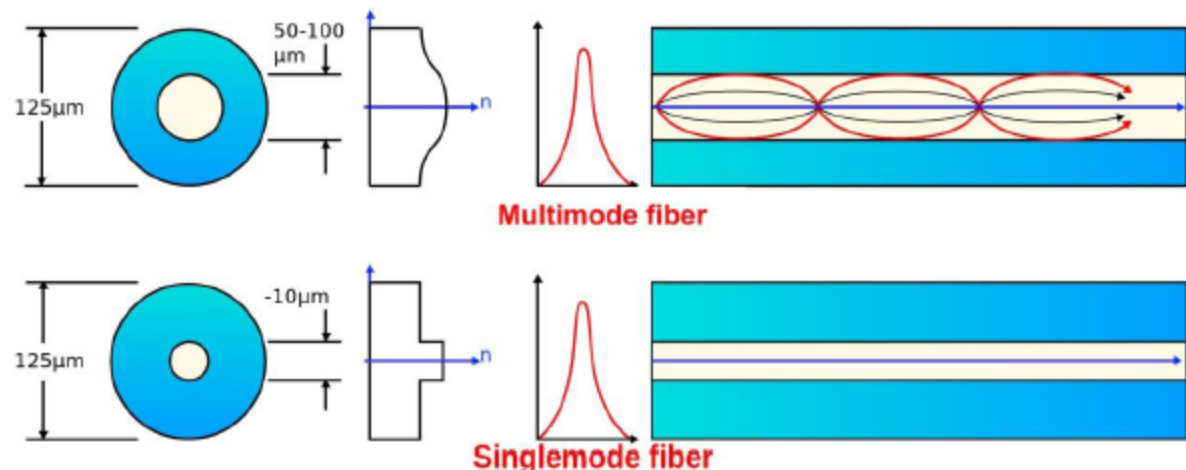
Vezetékes, optikai közegek:

3. Optikai szál jeltovábbítási jellemzői:

- Egy optikai szál egy vagy több optikai csatorna (WDM) számára használható.
- Egy csatornás változatban az oda-vissza pont-pont kapcsolathoz két szál szükséges.
- A fény (egy vagy több) módusokban terjed az optikai szálban

MMF – Multimode Fibre ↔ SMF – Singelmode Fibre

	MMF	SMF
D [μm]	125	125
d [μm]	50; 62,5	9,5
λ [μm]	0,85	1,31; 1,55



2. Átviteli közegek

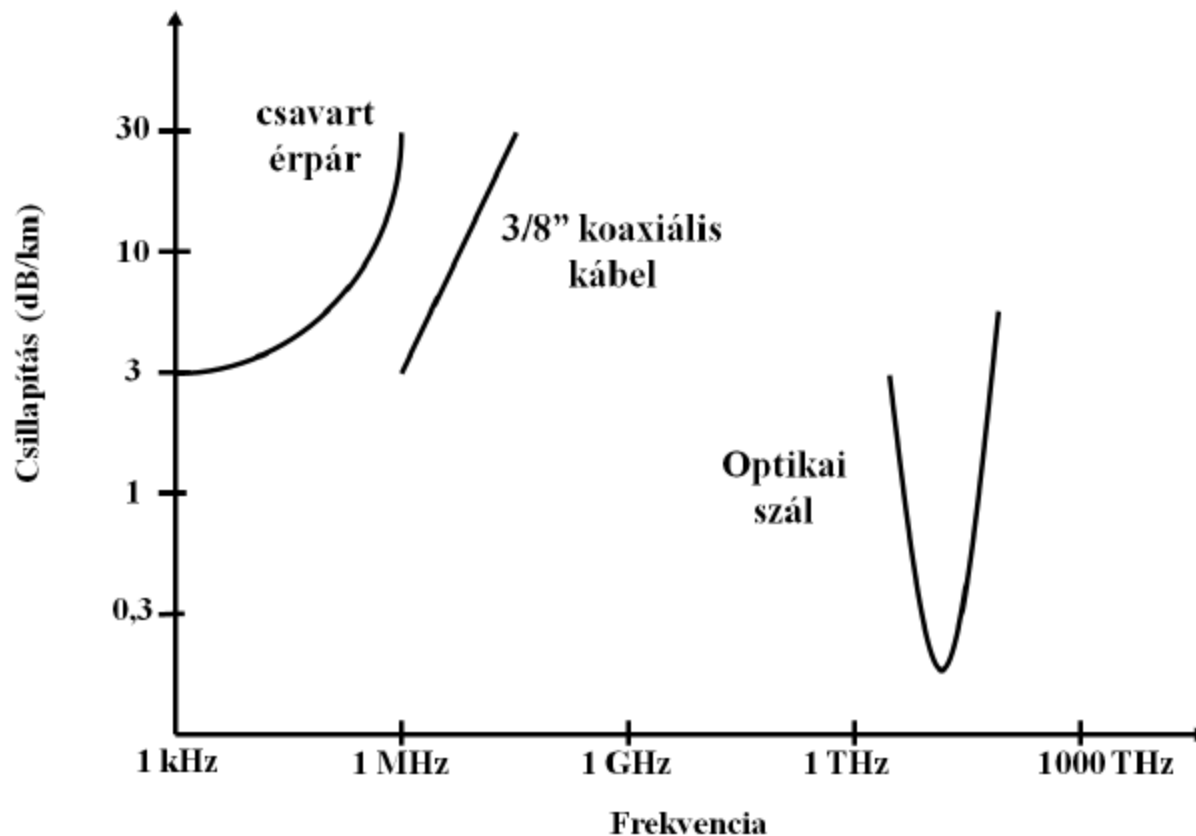
Vezetékes, optikai közegek:

3. Optikai szál alkalmazásának előnyei:

- Nagy adatátviteli ráta: Gbps több 10 km-en).
- Kisebb méret és kisebb tömeg, mint a galvanikus kábeleknél.
- Jelcsillapítás alacsony, és szélesebb frekvenciatartományban állandó.
- Külső elektromágneses hatások nem jutnak be az optikai szálba.
- Nem sugároz energiát, ezért nem hallgatható le. Nehéz az optikai szálát megcsapolni.
- Nagyobb ismétlési távolság miatt kevesebb ismétlő:
kevesebb hibalehetőség, alacsonyabb üzemeltetési költség.

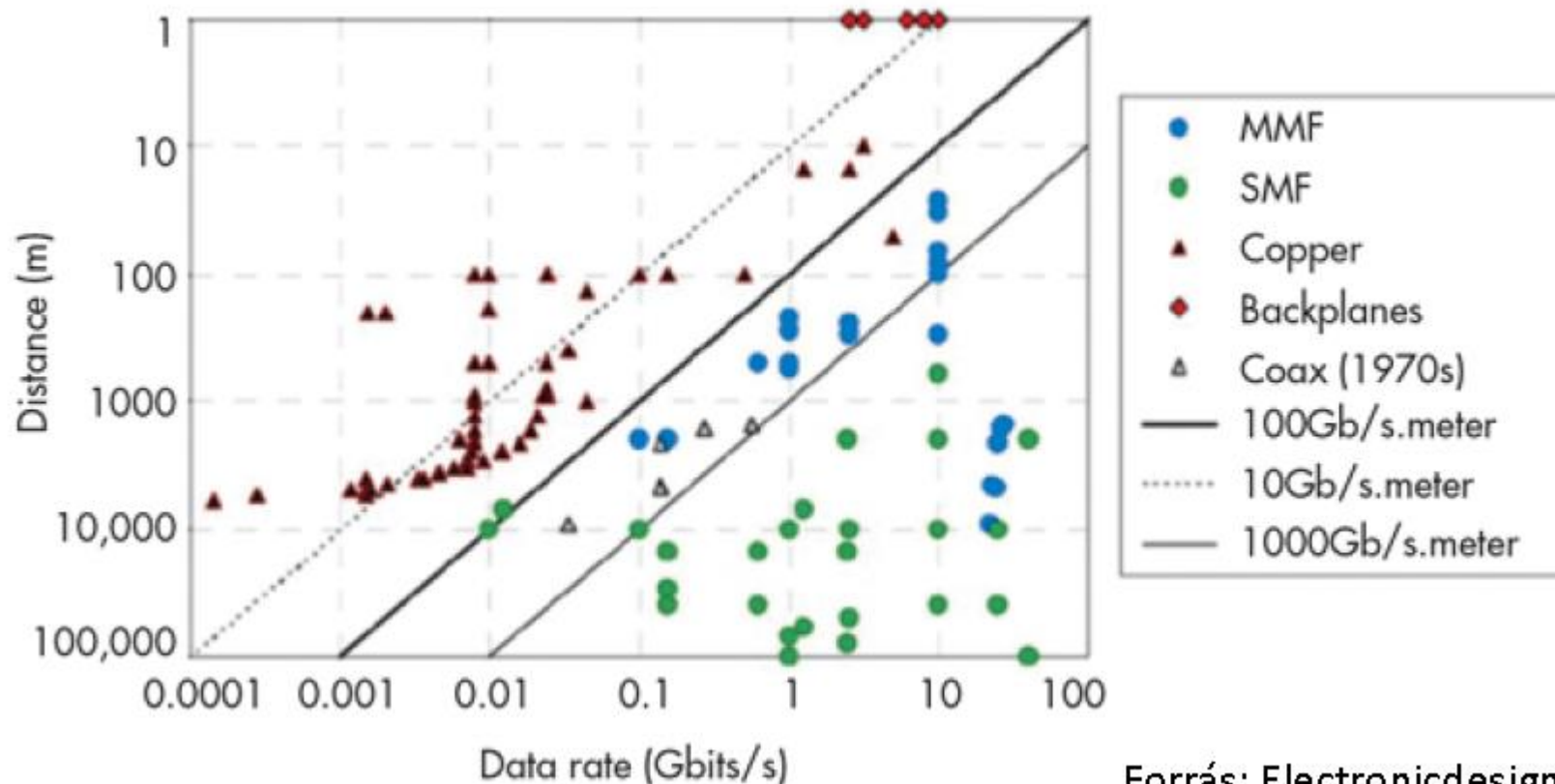
2. Átviteli közegek

Vezetékes átviteli közegek fajlagos csillapítása (A):



2. Átviteli közegek

Vezetékes átviteli közegek hatótávolsága (Távolság és Átviteli ráta szorzat):



Forrás: Electronicdesign.Com

2. Átviteli közegek

Vezetéknélküli közeg: levegő



4. Levegő jelátviteli jellemzői:

- Hangjel továbbítása levegőben: gázmolekulák rezgése
- Hangjel terjedési sebessége levegőben több tényezőtől függ:
gáz összetétele, nyomása, hőmérséklete
- Tipikus hangterjedési sebesség levegőben: 340 m/s
- Emberi fül által érzékelt hang frekvencia tartománya: 20 ... 20.000 Hz (300 ... 12.000 Hz)
- Emberi hangszalagok frekvencia tartománya: 50 ... 3.520 Hz (300 ... 3.400 Hz)
- Infrahang: $f < 20$ Hz (pl. aranyhal, vakond)
- Ultrahang: $f > 20$ kHz (denevér, kutya)
- Hangjel továbbítás levegőben alkalmazási területei:
 - Ember-ember kommunikáció,
 - Ember-gép kommunikáció,
 - Gép-ember kommunikáció.

2. Átviteli közegek

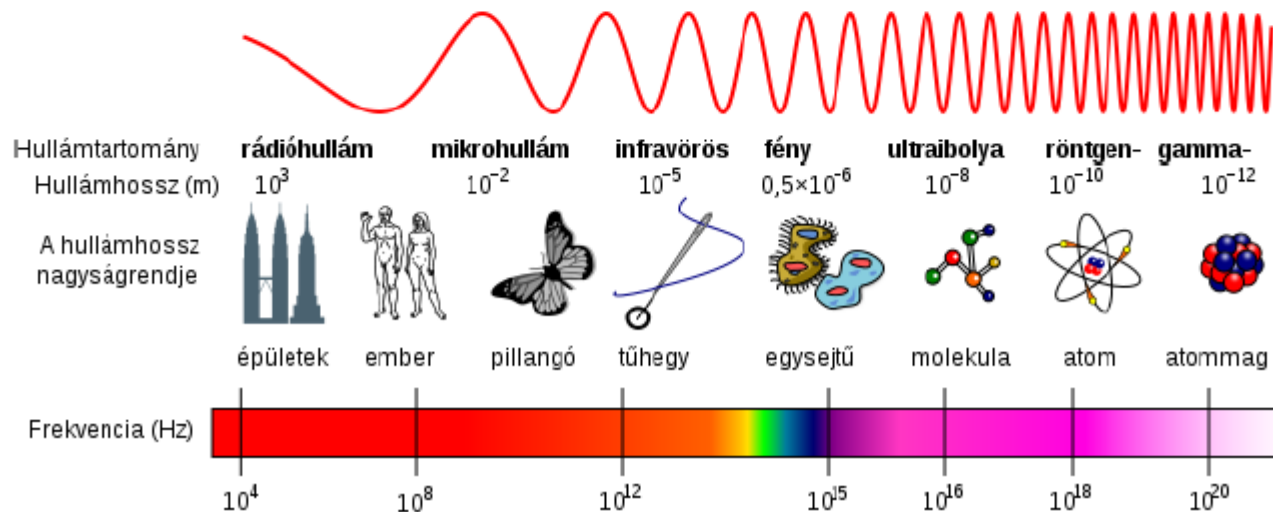
Vezetéknélküli közeg: rádiófrekvenciás csatorna



4. Rádiófrekvenciás csatorna jeltovábbítási jellemzői:

- EM térben egyetlen periodikus jel vagy több periodikus jel összege

$$S_i(t) = A_i \cdot \sin(2\pi \cdot f_i + \varphi_i), \quad S(t) = \sum_{i=0}^n S_i(t), \quad n \in \mathbb{N} \text{ és véges}$$



2. Átviteli közegek

Vezetéknélküli közeg: rádiófrekvenciás csatorna

4. Rádiófrekvenciás csatorna jeltovábbítási jellemzői (folyt.):

- Kiküldött EM jel csillapszik, ezért hatótávolságon belül alkalmazható
- Környezeti EM események befolyásolják a csatorna minőségét
- Lefedett fizikai terület szerinti osztályozás:
 - Irányított: csak két csomópont közötti egyenes mentén
 - Szektor: egy térszögön belül
 - Minden irányban: teljes térszögben (4π sr/szteradián)
- Frekvencia komponensek darabszáma szerinti osztályozás:
 - Alapsávú (baseband): szűk frekvenciatartomány ($n = 1$)
 - Keskenysávú (narrowband): kis frekvenciatartomány (n kicsi)
 - Szélessávú (broadband): tág frekvenciatartomány (n nagy)
- Alkalmazó kommunikációs technológiák:
 - Távközlés (GSM, LTE, 5G, ...)
 - Adathálózatok (WiMax, WiFi, BT, RFID, NFC, ...)

3. Jelkódolási technikák

Fogalmak:

Jelkódolás: A fizikai rétegben megjelenő bitsorozatot az alkalmazott (digitális) csatorna jelkészletére, jelzésrendszerére (szintekre, szint-váltásokra) képezzük le. A jelszint a közeg típusától függ és lehet elektromos feszültség, fényerősség vagy rezgés amplitúdó.

Unipoláris kódolás: A csatornán két jelet (szintet) különítünk el: (+V) és a (0) szimbólumok.

Bipoláris kódolás: A csatornán két jelet (szintet) különítünk el: (+V) és a (-V) szimbólumok.

Szinkron átvitel: A vevő összhangba kerül az adóval és ezt az összhangot végig fenntartja. Az egyes bitek azonos idő nagyság után követik egymást, szigorú rendben.

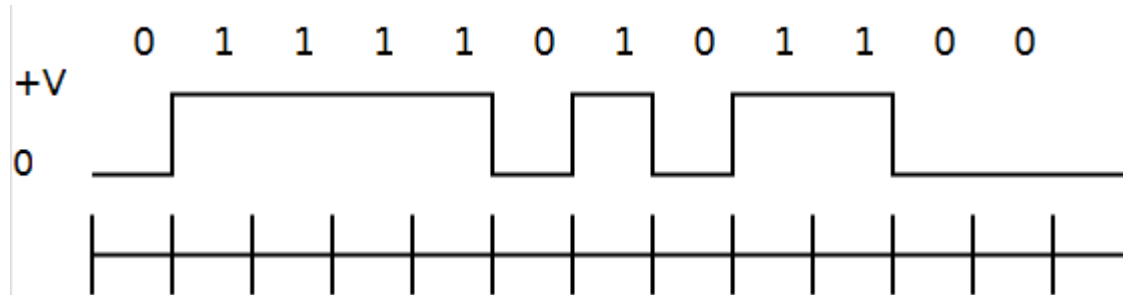
Aszinkron átvitel: Az adó és vevő egymástól függetlenül működik. Ha adatot akar az egyik átvinni, akkor egy összehangolási mintát küld a másik számára.

3. Jelkódolási technikák

1. NRZ (Non-Return to Zero) jelkódolás: Unipoláris szintek.

„0” bit: alacsony jelszint a teljes bitidőben. „1” bit: magas jelszint a teljes bitidőben.
Jelváltás a bitidő elején. Könnyen implementálható, de nem biztosít szinkronizációt több azonos bit érték átvitele során.

Példa:

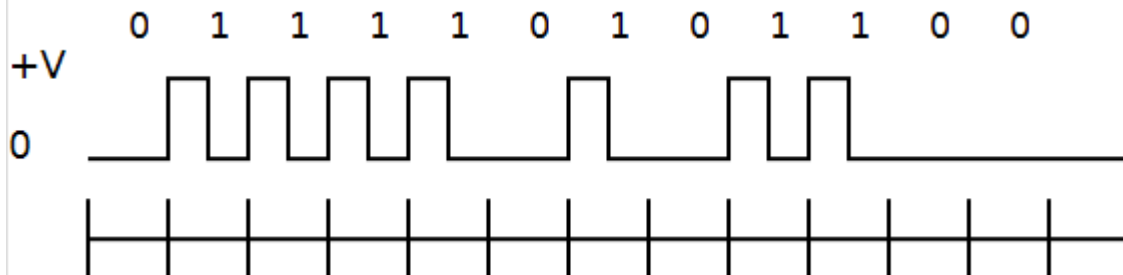


2. RZ (Return to Zero) jelkódolás: Unipoláris szintek.

„0” bit: alacsony jelszint a teljes bitidőben. „1” bit: első félidőben magas jelszint, második félidőben alacsony jelszint.

Jelváltási sebesség duplikáció csupa „1” esetén, szinkronizálatlan jelsorozat sok „0” esetén. Bit beszúrás és kivágás.

Példa:



3. Jelkódolási technikák

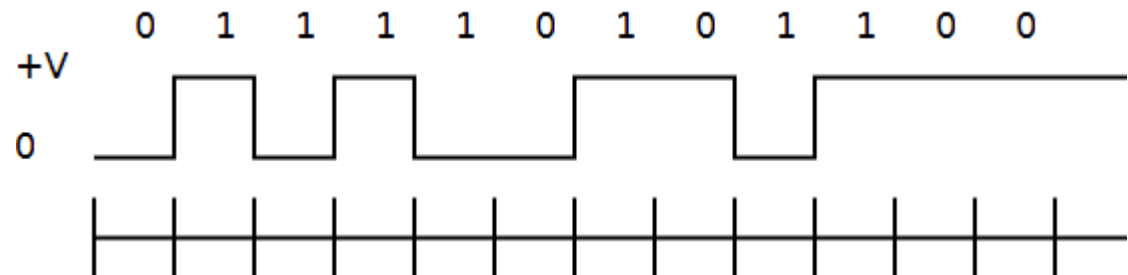
3. NRZI (Non-Return to Zero Invert on One) jelkódolás: Unipoláris szintek.

„0” bit: változatlan jelszint a teljes bitidőben.

„1” bit: jelszint váltás a bitidő elején.

Bit beszúrás és kivágás.

Példa:



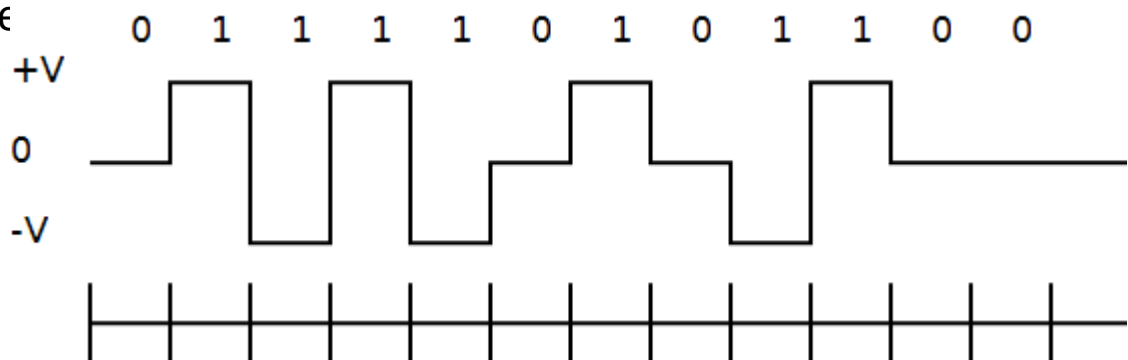
4. AMI (Alternate Mark Inversion) jelkódolás: Bipoláris feszültségszintek.

„0” bit: (0) jelszint a teljes bitidőben.

„1” bit: egymás utáni „1”-esek

Bit beszúrás és kivágás.

Példa:



3. Jelkódolási technikák

5. Manchester (PE – Phase Encoding) jelkódolás: Unipoláris/bipoláris szintek.

„0” bit: negatív jelátmenet bitidő felénél.

„1” bit: pozitív jelátmenet bitidő közepén.

Folyamatos szinkronizációt biztosít, de dupla jelváltás-sebességet igényel.

6. Különbözeti Manchester (DME – Differential Manchester Encoding):

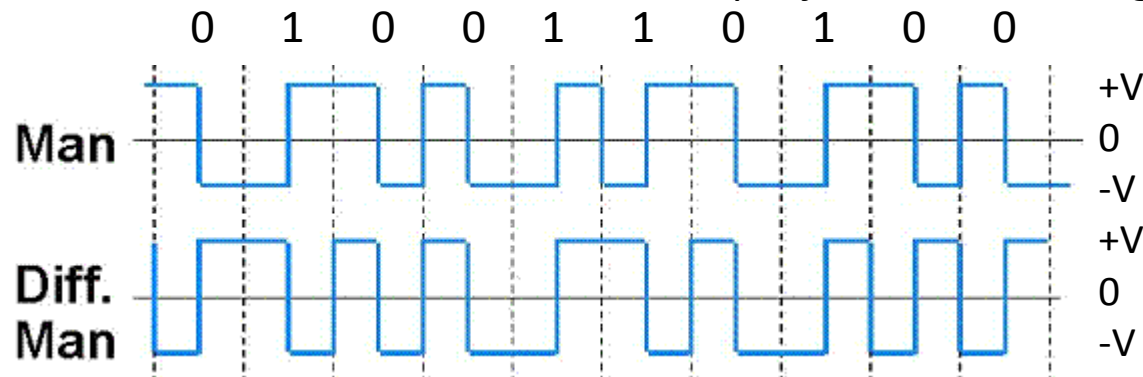
Unipoláris/bipoláris szintek.

„0” bit: bitidő elején és bitidő felénél is van szintváltás.

„1” bit: bitidő elején nincs szintváltás, bitidő felénél van szintváltás.

Folyamatos szinkronizációt biztosít, kevesebb mint dupla jelváltás-sebesség mellett.

Példa:



4. Modulációs technikák

Megfontolások:

A bináris információt sok esetben nem alapsávi impulzusok formájában vesszük át a csatornán, hanem egy (alsó- és felső frekvenciahatár megadásával) jól meghatározott frekvenciatartománnyal rendelkező (sáváteresztő) csatornán.

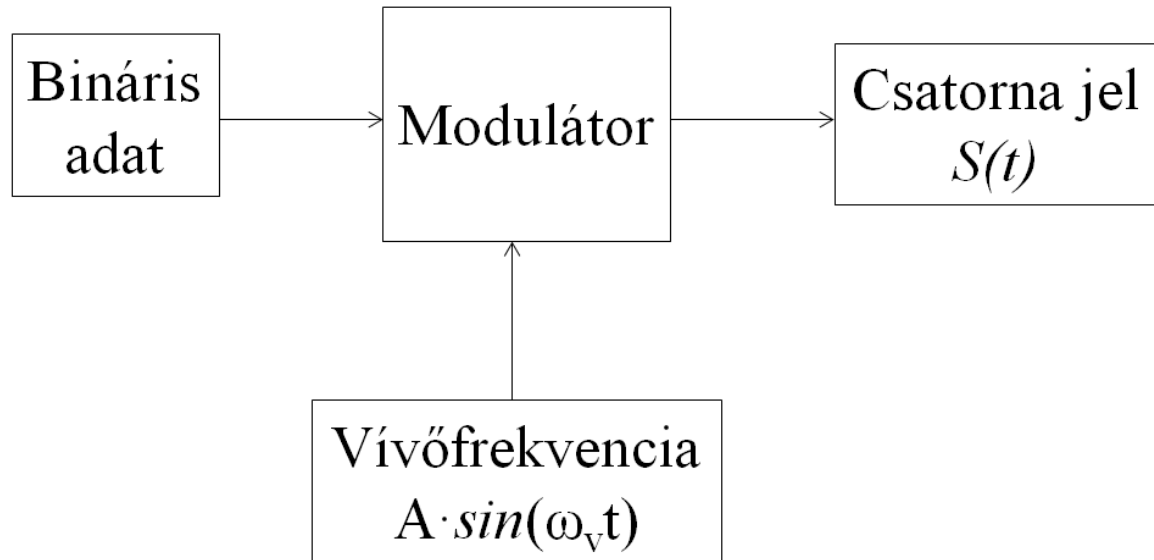
A rendelkezésre álló frekvenciasáv középértéke adja a vivőfrekvenciát, melyen valamilyen modulációs eljárással tudjuk leképezni a továbbítandó bit értékét.

Jelmagyarázat:

A : jel amplitúdó

ω_v : jel szögsebesség

t : idő (folytonos)



4. Modulációs technikák

1. Amplitúdó ugratás (Amplitude Shift Keying, ASK):

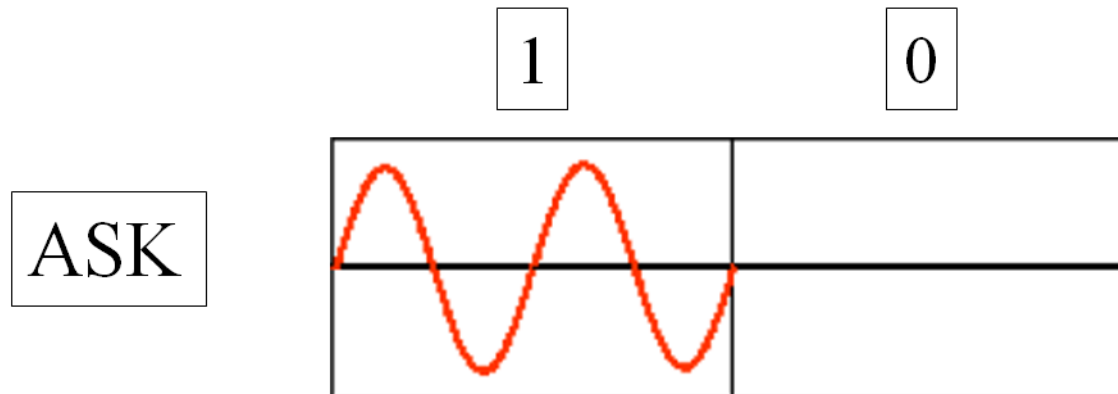
„0” bit értéket a vivőfrekvencia hiánya jelenti ($A = 0$).

„1” bit értéket a vivő jelenléte jelenti ($A \neq 0$).

$$S_{(0)}(t) = 0$$

$$S_{(1)}(t) = A \cdot \sin(\omega_v \cdot t)$$

Előny az egyszerű megvalósíthatóság. Hátrány a diszkrét komponens jelenléte.



4. Modulációs technikák

2. Frekvencia ugratás (Frequency Shift Keying, FSK):

„0” bit értéket a vivőnél megadott frekvencialökettel nagyobb frekvencia jelenti.

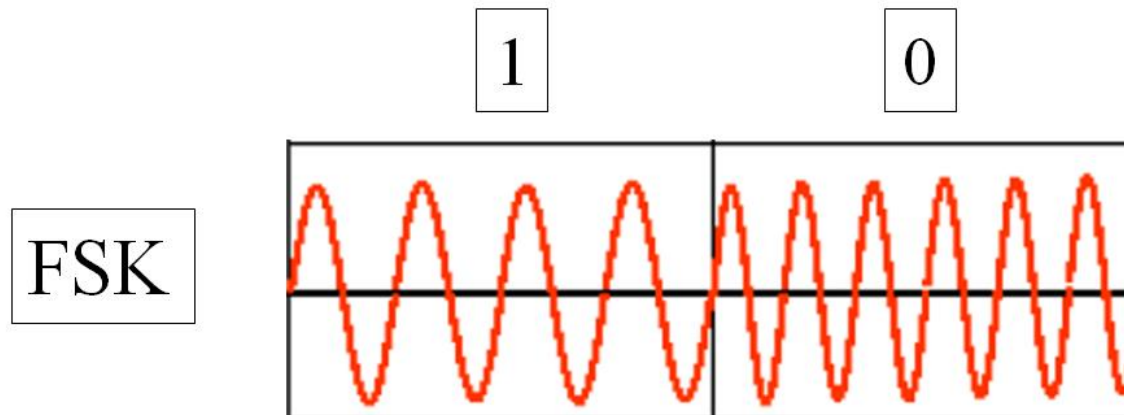
„1” bit értéket a vivőnél megadott frekvencialökettel kisebb frekvencia jelenti.

$$S_{(0)}(t) = A \cdot \sin((\omega_v + \omega_d) \cdot t)$$

$$S_{(1)}(t) = A \cdot \sin((\omega_v - \omega_d) \cdot t)$$

Itt a bit ráta és a baud ráta értéke azonos. A sávszélesség szükséglet: $2 \cdot \omega_d$

Előny az egyszerű dekódolás. Hátrány a nagy sávszélesség igény.



4. Modulációs technikák

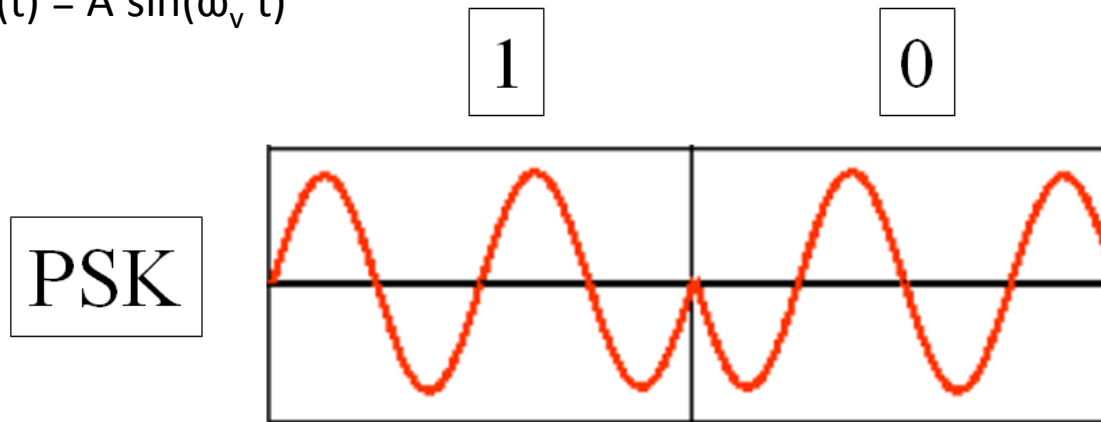
3. Fázis ugratás (Phase Shift Keying, PSK):

„0” bit értéket a vivőhöz képest ellentétes fázisú jel jelenti.

„1” bit értéket a vivőhöz képest azonos fázisú jel jelenti.

$$S_{(0)}(t) = A \cdot \sin(\omega_v \cdot t + \pi) = -A \cdot \sin(\omega_v \cdot t)$$

$$S_{(1)}(t) = A \cdot \sin(\omega_v \cdot t)$$



Ez a felírási forma általánosítási lehetőséget nyit a többszintű PSK alkalmazására: 180° helyett több kisebb eltolási érték segítségével egy átviteli időegységben több bit átvitele is megoldható.

Pl.: 4 szintű PSK (Quadrature PSK, QPSK): 0° , 90° , 180° és 270° fokos eltolások léteznek. Itt egy időegység alatt két bitnyi információ vihető át.

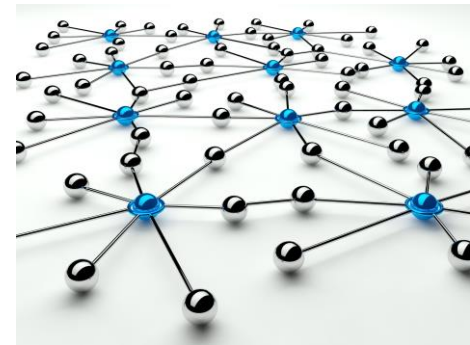
Hálózati architektúrák és protokollok

4. ADATKAPCSOLATI RÉTEG

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Logikai és fizikai hálózati topológiák
- 2) Adatkapcsolati réteg funkciók és szolgálatok
- 3) MAC alréteg technikák
- 4) Kódosztásos többszörös hozzáférés

1. Logikai és fizikai hálózati topológiák

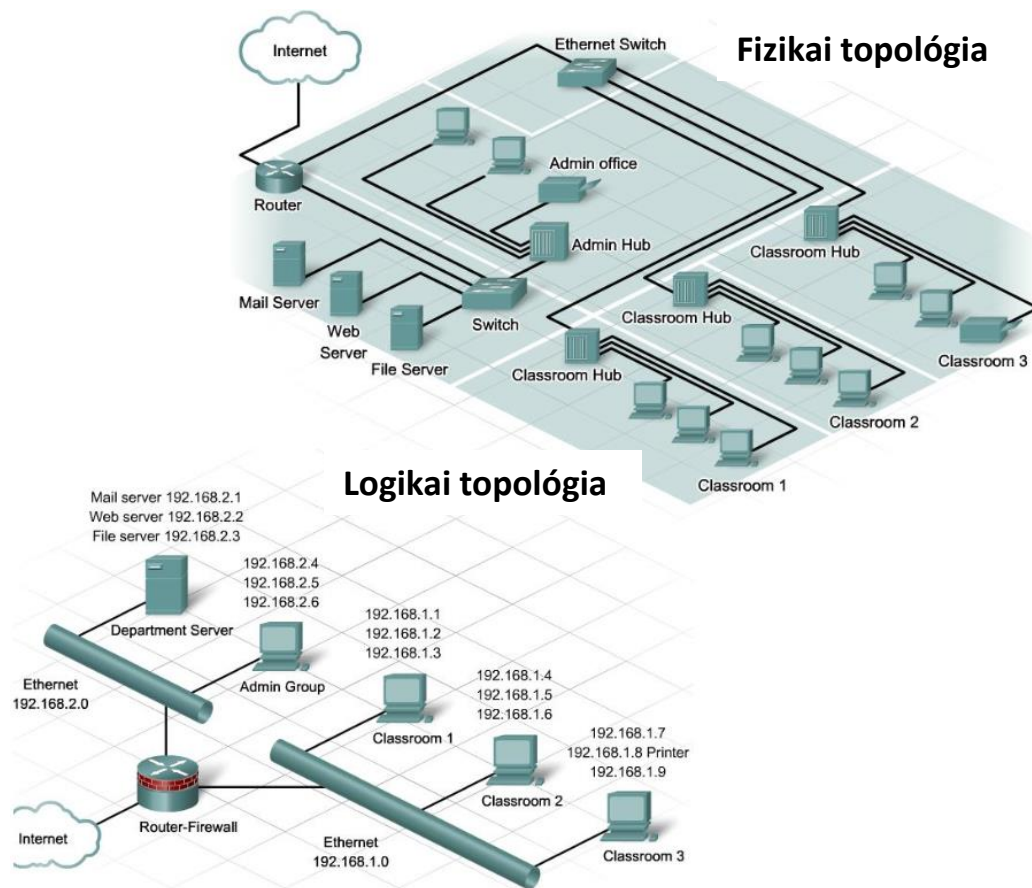
Hálózati topológia:

A hálózati csomópontok térbeli elrendezési, összeköttetési rendszere.

- **Logikai topológia:** Az OSI modell felsőbb rétegeiben reprezentált kapcsolatrendszer.

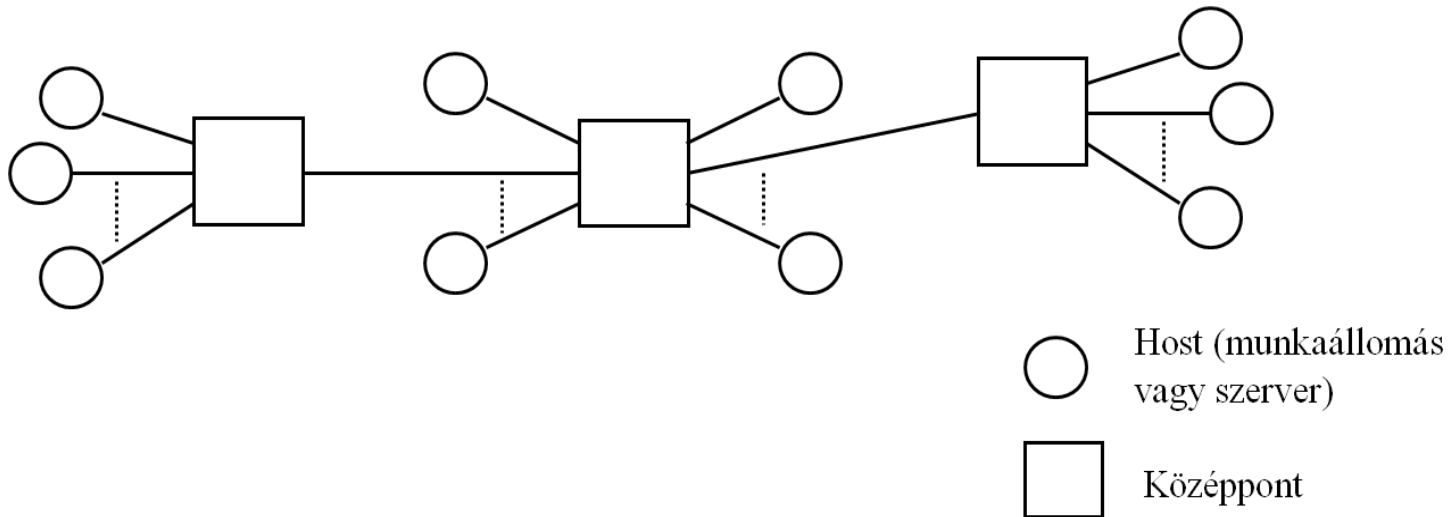
- **Fizikai topológia:** Az OSI modell fizikai rétegében megvalósított kapcsolatrendszer, annak fizikai nyomvonalával együtt.

A legalapvetőbb topológia típusoknál vizsgáljuk, hogy a csatorna esetleges meghibásodása (pl. kábelszakadás) milyen hatást gyakorol az adott kapcsolati rendszer további működésére.



2. Logikai és fizikai hálózati topológiák

1. Csillag topológia, kiterjesztett csillag topológia:



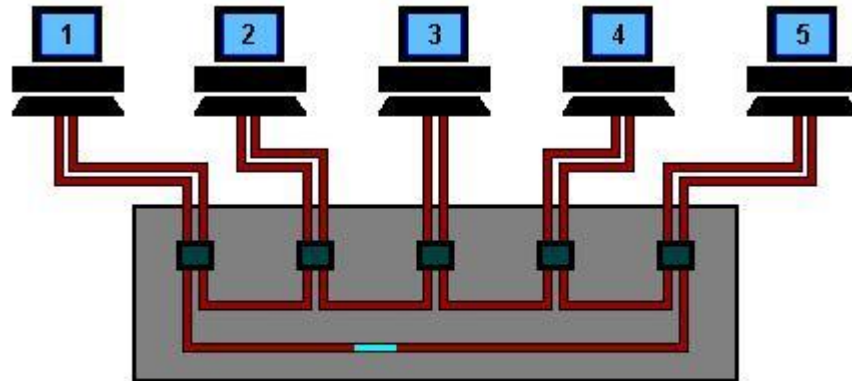
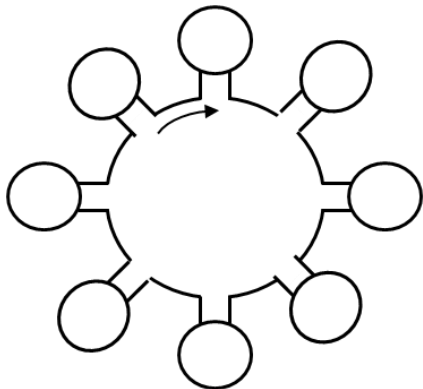
A kiterjesztett csillag topológia az egy középponttal rendelkező klasszikus csillag elrendezés kiterjesztése. Egy eredeti csillag csúcspontot egy újonnan kiépítendő csillagközeppon tulajdonsággal ruházunk fel.

A hierarchia mélysége tipikusan egy-két szint.

Kiterjesztett csillag topológia esetén a csatorna meghibásodása egymástól elkülönülő, de önmagukban működőképes hálózati egységekre bontja fel a hálózatot.

1. Logikai és fizikai hálózati topológiák

2. Gyűrű topológia:



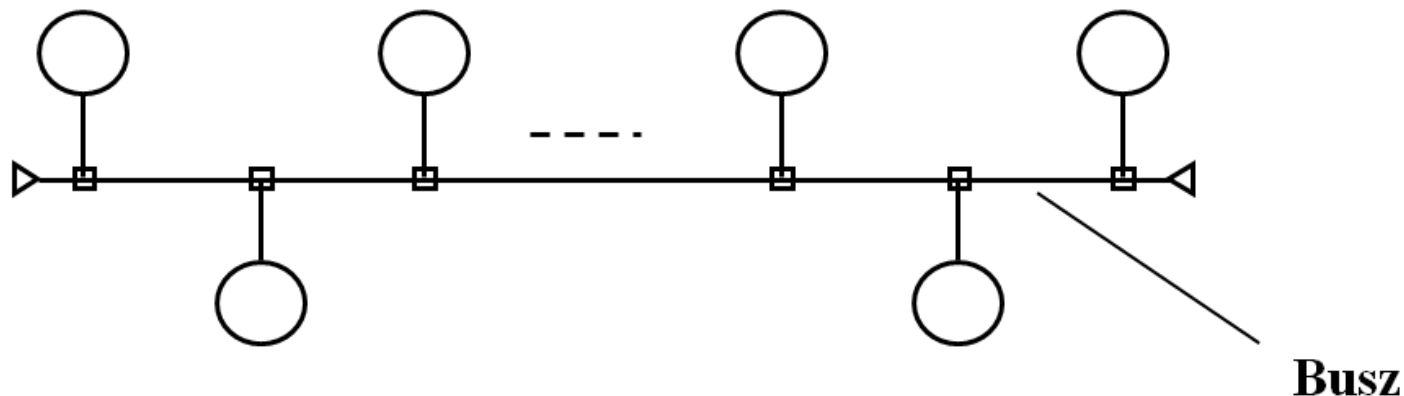
A gyűrű huzalozott koncentrátor növeli a megbízhatóságot, de kritikus meghibásodási pontként jelenik meg.

Gyűrű topológiában az átvitel tipikusan irányított, minden állomásnak van felső és aló szomszédja.

A leggyakrabban használt gyűrű topológiák esetén a feladott keretet az adó állomás távolítja el a gyűrűből. A meghibásodás kezelésére/elkerülésére speciális megoldásokat használnak, pl. kétkörös, ellentétes irányítottságú gyűrű alkalmazása.

1. Logikai és fizikai hálózati topológiák

3. Busz (sín) topológia:



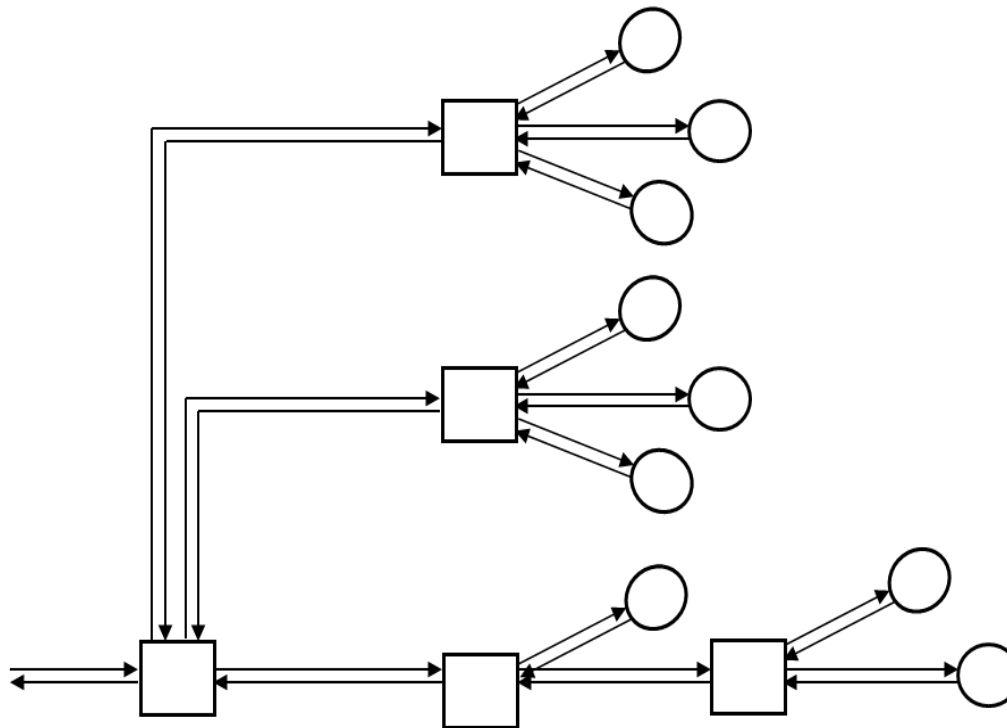
Több csomópont csatlakozik egy közös csatornára (kábelre, buszra).

Léteznek egyik irányba vagy mindkét irányba továbbító sínek.

A közösen használt galvanikus vagy optikai közeg sérülése a teljes rendszer leállítását eredményezheti, mert a szakadási helyen megjelenő jelterjedési inhomogenitás a szakadás helyéről jelvisszaverődést eredményez. Így azon állomások sem tudnak egymással kommunikálni, melyek között a közeg folytonos.

1. Logikai és fizikai hálózati topológiák

4. Fa topológia:



A fa topológia a kiterjesztett csillag topológia általánosításaként is felfogható, ahol a kiterjesztések mélységének száma nem korlátozott. A gyakorlati implementációknál az osztási pontok és a csomópontok száma véges.

Tipikus jellemző: a fa különböző régióiban jelentős forgalomintenzitási eltérések jelenhetnek : pl. a fa gyökerénél és a levél elemeknél.

2. Adatkapcsolati réteg funkciók és szolgálatok

Szolgálat típusok adatkapcsolati rétegben:

- **Nyugtázás nélküli, összeköttetés-mentes:** A vevő semmiféle visszajelzést nem ad az adó felé a keret vételével kapcsolatban. Széles körben alkalmazzák, ahol stabil (megbízható) fizikai összeköttetés létezik. Pl.: vezetékes Ethernet technológiák.
- **Nyugtázásos, összeköttetés-mentes:** A vevő nyugtáz a keret átvétele után. Alkalmazása tipikusan a vezeték nélküli technológiáknál a leggyakoribb. Nem megbízható (hibás, zajos) fizikai összeköttetés esetén célszerű a használata. Pl.: WiFi.
- **Nyugtázásos, összeköttetés-alapú:** Nem minden egyes keretre vonatkozóan történik visszajelzés. Keretsorozatok átvitele esetén hatékony. Hiba esetén csak a legutóbbi blokk újraküldése szükséges.

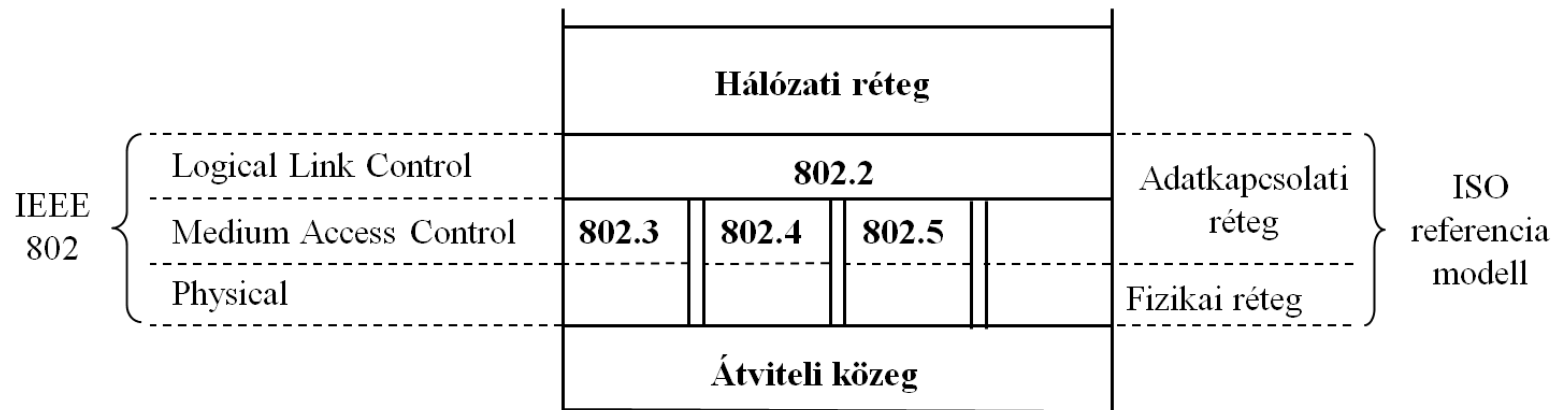
2. Adatkapcsolati réteg funkciók és szolgálatok

Keretezés adatkapcsolati rétegben:

- A hálózati réteg felől érkező SDU (Service Data Unit, szolgáltat adatelem) keretekre bontása.
- Fejrész és adatrész mezők elhelyezése.
- Bitsorozat átadása a fizikai rétegnek.
- A keretek egymástól való elhatárolása több módszerrel lehetséges:
 - Időzítés (IFG - InterFrame Gap): kötelező küldésszünet, technológia függő
 - Keretméret: A keret tartalmazza a saját hosszát bájtokban kifejezve. Gondot jelenthet a hosszmező sérülése.
 - Bitminta: DLE STX és DLE ETX (DataLink Escape/Start of TeXt, End of TeXt, azaz kezdő- és zárókarakterek) alkalmazása karakterbeszúrással. A keretben megjelenő DLE karakter DLE DLE duplikátumként megy át.

2. Adatkapcsolati réteg funkciók és szolgálatok

IEEE LAN adatkapcsolati réteg szabványok:



802.2 = Logical Link Control Protocol
802.3 = CSMA/CD
802.4 = Token bus
802.5 = Token ring

} Közeghozzáférési protokollok

Az IEEE 802 protokoll család

Adatkapcsolati réteg alrétegei:

- Közeghozzáférés vezérlés (MAC – Medium Access Control): HW/FW
- Logikai kapcsolat vezérlés (LLC – Logical Link Control): SW

3. MAC alréteg technikák

1. Statikus csatorna-hozzáférési módszerek:

- **Frekvenciaosztásos többszörös hozzáférés (FDMA):** A csatornát (különböző frekvenciákon alapuló) alcsatornákra osztjuk, így csökkentjük a versenyhelyzetet. Ideális esetben minden adó más-más alcsatornára (frekvenciára) kerül, így az ütközés teljesen eliminálható.
- **Időosztásos többszörös hozzáférés (TDMA):** A közös csatornát előre meghatározott időszelvény-használati besorolással megosztjuk a versenyhelyzetben lévő adók között, ezzel biztosítva, hogy egy időpillanatban csak egy adó küldhessen információt a csatornán.
- **Hullámhosszosztásos többszörös hozzáférés (WDMA):** Hasonló az FDMA-hoz, de a közeg optikai kábel vagy EM tér, a jel pedig fény.

3. MAC alréteg technikák

2. Dinamikus csatorna-hozzáférési módszerek:

- Továbbítás figyelés nélkül
- Időréselt (Time Slot)
- Vivőfigyelés többszörös hozzáféréssel (Carrier Sense Multiple Access)
- Ütközésérzékeléses (Collision Detect)
- Ütközés megelőzéses (Collision Avoidance)
- Vezérjeles (Token)
- Kódosztásos többszörös hozzáférés (Code Divison Multiple Access)



3. MAC alréteg technikák

3. Csatorna alcsatornákra bontásának szempontjai:

- **Ütközés teljes kizárása:** Az alcsatornák száma az adók számával azonos. Egyszerűen implementálható, de a működési hatékonysága alacsony, mivel az éppen nem aktív adók erőforrásfoglalása veszteségként jelentkezik.
- **Átviteli idő (átlagos válaszidő) minimalizálása:** Hangsúly a működési hatékonyság optimalizálása, vagyis a keretek csatornán való átviteli idejének minimalizálása.

Sorbanállási modell N részre osztott csatorna esetén:

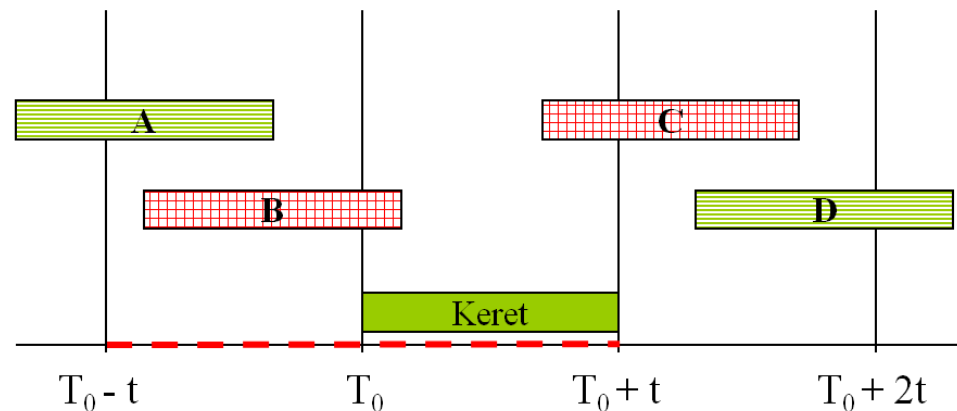
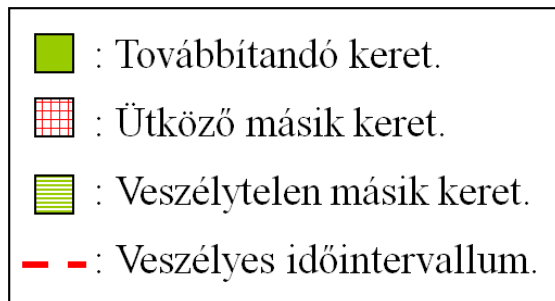
- A keretek érkezési és továbbítási idejét független, exponenciális eloszlású valószínűségi változónak tételezzük fel. Ez a gyakorlatban csak közelítő modell.
 - **Kapacitás:** C/N [b/s] $\rightarrow$ 1 bit átviteli ideje: N/C [s].
 - **Keretérkezési intenzitás:** λ/N [keret/s] $\rightarrow$ keret érkezési időköz: N/λ [s].
 - **Kerethossz:** $1/\mu$ [bit/keret].
 - **Egy keret átviteli ideje:** $N/(\mu \cdot C)$ [s] $\rightarrow$ keret kiszolgálási intenzitás: $(\mu \cdot C)/N$ [Hz].
 - **Little-tétel:** Átlagos válaszidő = $1/(\text{kiszolg. int.} - \text{érk. int.}) = N/(\mu \cdot C - \lambda)$ [s]
- A keret várható továbbítási ideje tehát az alcsatornák számával lineárisan növekszik.

3. MAC alréteg technikák

4. ALOHA:

Továbbítás figyelés nélküli (legegyszerűbb) közeghozzáférés:

- Eredet: Hawai Egyetem – szigetek közötti rádiós kommunikáció.
- A továbbítandó keret azonnal a csatornára kerül.
- Fogadó nyugtázza a keretet, ha nem volt ütközés.
- Ütközés esetén a forrás véletlen ideig vár és újból elküldi a keretet.
- Egyszerű működés, könnyen implementálható.
- Az ütközések miatt a csatorna várható maximális kihasználtsága alacsony (18%).
- Keretátvitelre veszélyes időtartam:



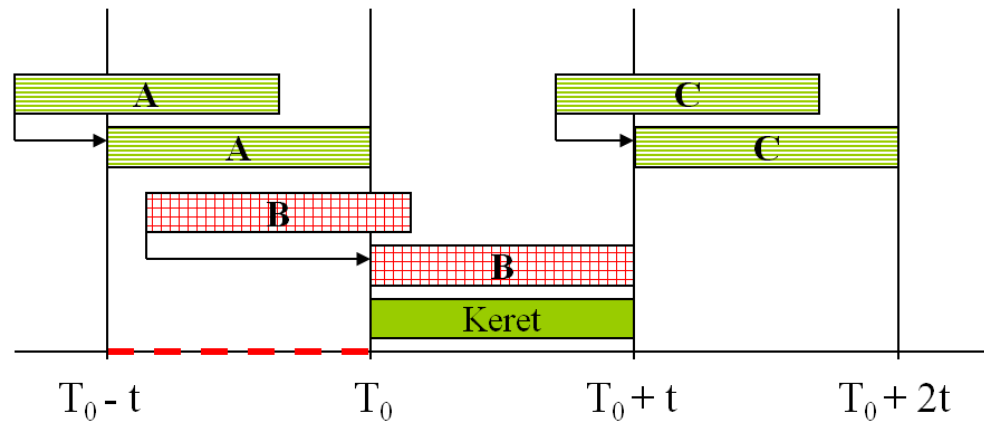
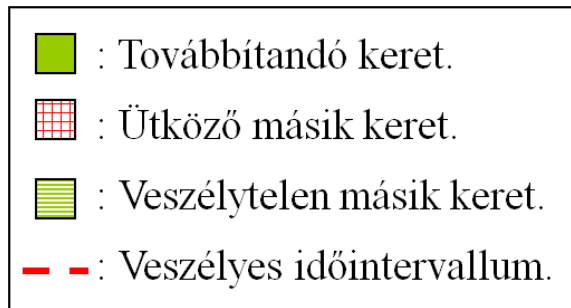
T_0 : a keret küldésének kezdőpillanata

t : egy keret átviteli ideje

3. MAC alréteg technikák

5. Réselt ALOHA:

- Időrészek használata, amiben elfér a keret.
- A továbbítandó keret a következő időrés elején kerül a csatornára.
- Fogadó nyugtázza a keretet, ha nem volt ütközés.
- Ütközés esetén a forrás véletlen ideig vár és újból elküldi a keretet.
- A csatornakihasználtság egyszerűen növelhető (36%).
- Keretátvitelre veszélyes időtartam:



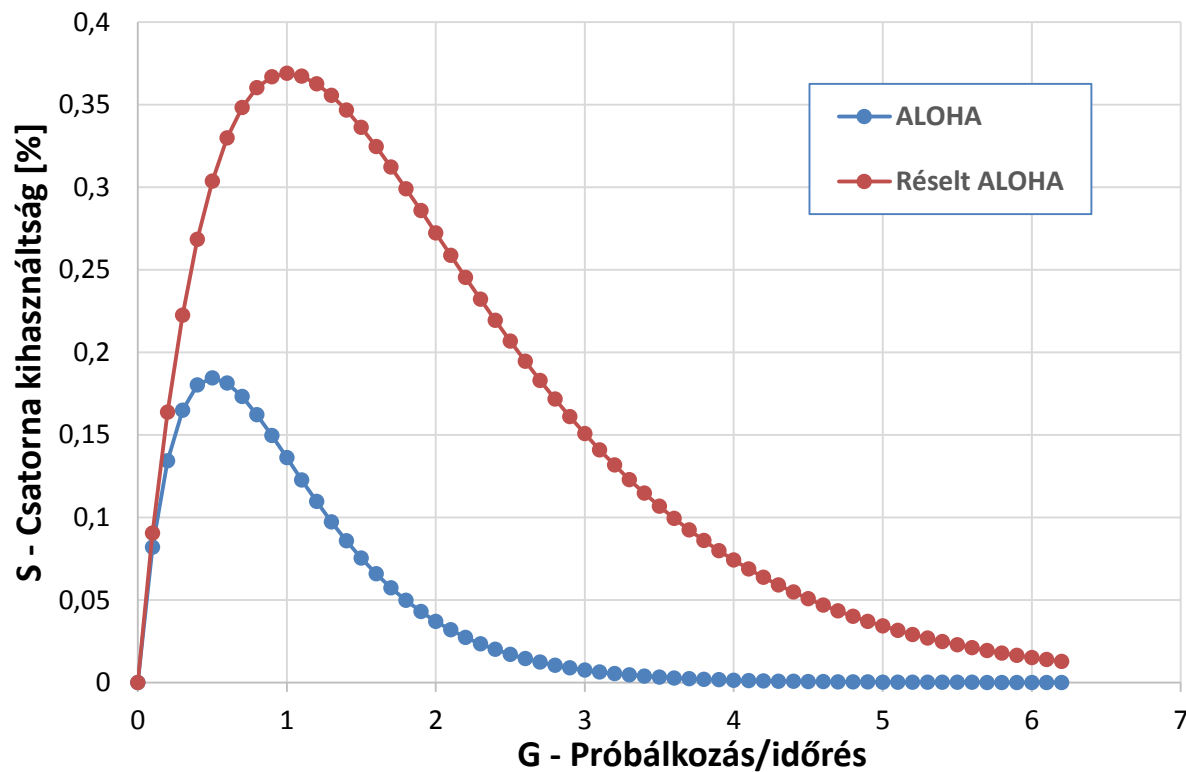
T_0 : a keret küldésének kezdőpillanata

t : egy keret átviteli ideje

3. MAC alréteg technikák

6. ALOHA és Réselt ALOHA csatornakihasználtsága (S):

Poisson eloszlású próbálkozási eloszlást feltételezve:



$$S_{\text{ALOHA}} = G \cdot e^{-2G}$$

$$S_{\text{R_ALOHA}} = G \cdot e^{-G}$$

4. Kódosztásos többszörös hozzáférés (CDMA)

Megfontolások:

Klasszikus esetben adott rádiófrekvenciás csatornán egy időpillanatban csak egyetlen keret küldése lehet folyamatban, mivel egyébként interferencia lép fel. Létezik azonban az interferenciának egy konstruktív változata, amelynél szórt spektrumban történik a jelek küldése. Ez a frekvenciatartomány jóval nagyobb, mint az adatküldéshez szükséges sávszélesség. A különböző források egyidőben küldenek jeleket, amelyek csak részben interferálnak. Mindegyik forrás a bitjeit sajátosan kódolja.

CDMA matematikai háttere:

Kiindulási állapot: Minden állomáshoz egy m bit hosszú bipoláris kód (chip) tartozik. A chip kód egyedi módon jellemzi az adót. A küldött bitek („1”, illetve „0”) kódjai:

$$S_1 = (s_1, \dots, s_m)$$

$$S_0 = (-s_1, \dots, -s_m)$$

$$\text{ahol } s_i = +1, \text{ vagy } s_i = -1, \quad i = 1, \dots, m.$$

Műveletek chip kódokkal:

S és T chipek összege: $S + T = (s_1 + t_1, \dots, s_m + t_m)$

S és T chipek (skaláris) szorzata: $S * T = (1/m) \cdot (s_1 \cdot t_1 + \dots + s_m \cdot t_m)$

4. Kódosztásos többszörös hozzáférés (CDMA)

CDMA matematikai háttere (folyt.):

A bipoláris kódolás miatt érvényesülnek az alábbi összefüggések:

$$S_1 * S_1 = S_0 * S_0 = 1,$$

$$S_1 * S_0 = -1,$$

$$S * (A+B) = (S*A) + (S*B).$$

Működési feltétel:

A különböző állomásokhoz rendelt chip-ek ortogonálisak, azaz skaláris szorzatuk nulla:

$$S_1 * T_1 = S_1 * T_0 = S_0 * T_1 = S_0 * T_0 = 0$$

A feltétel teljesüléséhez szükséges: $\log_2 m \geq \lceil \log_2 N \rceil$, ahol N a populáció számossága.

Vételi folyamat:

A célpontnál vételezett, több forrásból származó egyidejű vektorok összegéből (interferencia) meghatározható a küldött bit értéke. A célpont az adóchip értékkel szorozza az interferencia jelsorozatot. A vételezéshez chipbitek szinkronítására van szükség.

4. Kódosztásos többszörös hozzáférés (CDMA)

CDMA példa:

Három állomás (A, B, C) egyidejű adását vizsgáljuk. Legyen $m = 4$, és az ortogonális chip kódok:

$$A_1 = (+1, +1, -1, -1);$$

$$A_0 = (-1, -1, +1, +1);$$

$$B_1 = (+1, -1, +1, -1);$$

$$B_0 = (-1, +1, -1, +1);$$

$$C_1 = (-1, -1, -1, -1);$$

$$C_0 = (+1, +1, +1, +1);$$

Az állomások által egy időben küldött bitértékek legyenek pl.:

A: 0 (-1, -1, +1, +1); **B: 1** (+1, -1, +1, -1); **C: 0** (+1, +1, +1, +1)

Csatornán megjelenő interferencia jelsorozat: $A_0 + B_1 + C_0 = (+1, -1, +3, +1)$

A partnere: $A_1 * (A_0 + B_1 + C_0) = (+1-1-3-1)/4 = -1$, vagyis $A_1 * X = -1$ egyenletből

$X = A_0$, tehát A forrás „0” bitértéket küldött.

B partnere: $B_1 * (A_0 + B_1 + C_0) = (+1+1+3-1)/4 = 1$, vagyis $B_1 * X = +1$ egyenletből

$X = B_1$, tehát B forrás „1” bitértéket küldött.

C partnere: $C_1 * (A_0 + B_1 + C_0) = (-1-1-1-1)/4 = -1$, vagyis $C_1 * X = -1$ egyenletből

$X = C_0$, tehát C forrás „0” bitértéket küldött.

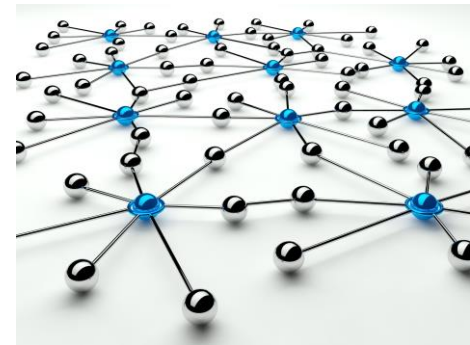
Hálózati architektúrák és protokollok

5. LAN ÉS MAN ÁTVITELTECHNIKÁK

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

1) Ethernet átviteltechnika

- Topológia, keretszerkezet

- Jellemző paraméterek

- MAC mechanizmus (CSMA/CD)

- Kapcsolás, szegmentálás

2) Token Ring átviteltechnika

- Topológia, keretszerkezet

- Jellemző paraméterek

- MAC mechanizmus (vezérjeles gyűrű)

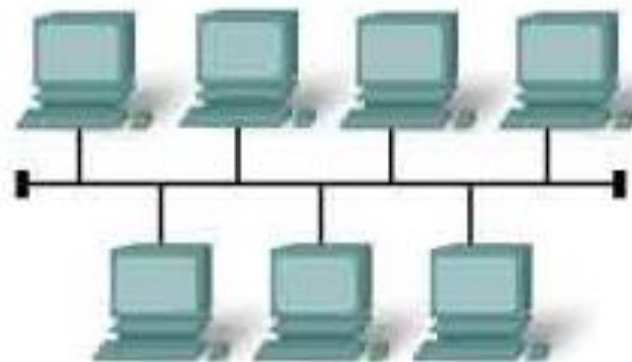
1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3):

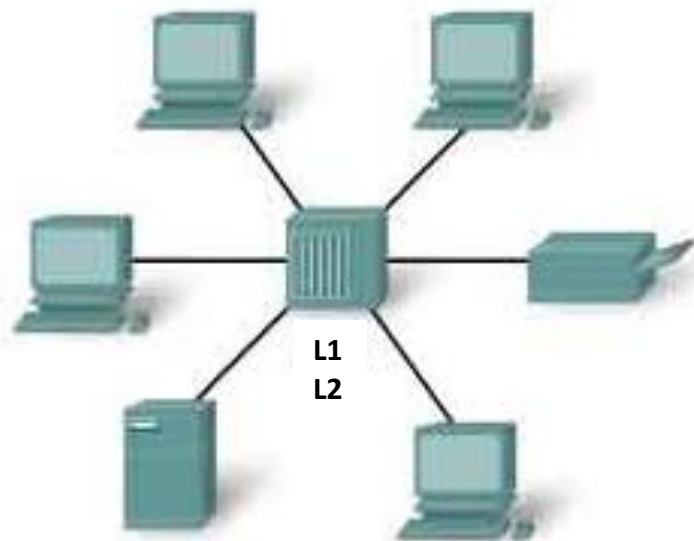
Lehetséges topológiák:

Sín

Fa (repeater)



Csillag (hub, switch)



1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3):

IEEE 802.3 Ethernet keretformátum:

↓
**Átvitel
iránya**

Előtag
Keret kezdet határoló
Cél állomás címe
Küldő állomás címe
Hossz/Típus
Adat
Töltelék (ha kell)
CRC

7 bájt: 7 x '10101010' (Szinkronizáció)

1 bájt: '10101011'

6 bájt: 1-3 bájt a gyártó azonosítója,
4-6 bájt a sorszám

6 bájt: 1-3 bájt a gyártó azonosítója,
4-6 sorszám

2 bájt: hossz/típus jelzése

0 - 1500 bájt adat

0 - 46 bájt: A kerethossz nem lehet
kisebb, mint 64 bájt

4 bájt: ellenőrző összeg

1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3) (folyt.):

IEEE 802.3 Ethernet működési paraméterek:

Paraméter	Érték
Átviteli sebesség	10 Mbps (Manchester kódolás)
Résidő	512 bitidő
Keretek közti idő (IFG)	9,6 μ s
Átviteli kísérletek max. száma	16
Zavaró bitek száma (jam size)	32
Legnagyobb kerethossz	1518 bájt
Legkisebb kerethossz	64 bájt

Célcím lehetséges értékei:

- Egy állomás pontos címe
- Csupa '1' bit: üzenetszórás (broadcast) - az üzenetet minden állomás veszi.
- A küldő állomás címe nem lehet többes cím!

1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3) (folyt.):

IEEE 802.3 Ethernet kerettovábbítás (CSMA/CD):

1. Várakozás továbbítandó keretre, majd a keret formázása.

2. Csatorna foglalt?

Igen: Ugrás a 2-re.

Nem: Keretek közötti idő kivárása, majd a kerettovábbítás megkezdése.

3. Van ütközés küldés közben?

Igen: Zavarójelek küldése. Továbbítási kísérletek számának növelése. Ugrás 4-re.

Nem: Átvitel befejezése. Sikeres átvitel jelzése. Ugrás az 1-re.

4. Elértük a max. kísérletszámot (16)?

Igen: Sikertelen továbbítás jelzése. Ugrás az 1-re.

Nem: Késleltetés kiszámítása és az idő kivárása. Ugrás a 2-re.

1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3) (folyt.):

IEEE 802.3 Ethernet kerettovábbítás (CSMA/CD) (folyt.):

A keret késleltetési idejének meghatározása:

- A résidő vagy körbejárési késleltetés az az idő, ami alatt a keret első bitje a két legtávolabbi állomás között kétszer megfordul. Ennyi idő alatt az állomások biztonsággal észlelik az ütközést. Kábelkésleltetés: $\sim 5 \mu\text{s}/1000 \text{ m}$.
- Résidő = $2 * (\text{kábelkésleltetés} + \text{ismétlők késleltetése}) + \text{tartalék idő}$
- Résidő = $51,2 \mu\text{s} (2 * (2,5 \text{ km} + 4 \text{ ismétlő késleltetése}), 512 \text{ bit átvitelének ideje})$

1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3) (folyt.):

IEEE 802.3 Ethernet kerettovábbítás (CSMA/CD) (folyt.):

A várakozási idő küldésnél:

A résidő véletlen számú többszöröse, amely az átviteli kísérletek számának függvénye.

Ütközési próbálkozás sorszáma	Véletlenszerű várakozási időtartam [résidő]
1	{0, 1}
2	{0, 1, 2, 3}
3	{0, 1, 2, 3, 4, 5, 6, 7}
i	{0, 1, 2, ..., (2^i-1) }
15	{0, 1, 2, ..., 32767}
16	Próbálkozás leállítása, küldési sikertelenség jelzése

1. Ethernet átviteltechnika

1. Ethernet (IEEE 802.3) (folyt.):

IEEE 802.3 Ethernet keretfogadás (CSMA/CD):

1. Van bejövő jel a közegen?

Van: Csatorna foglaltságának jelzése. Bitszinkronizálás, keretkezdet azonosítás, keret beolvasás.

Nincs: Ugrás az 1-re.

2. Ellenőrző összeg (CRC) és kerethossz rendben?

Igen: Tovább 3-ra.

Nem: Keret eldobása. Ugrás az 1-re.

3. Célcím = saját cím vagy csoportcím?

Igen: A vett adat továbbítása a felsőbb protokollrétegnek, majd ugrás az 1-re.

Nem: Keret eldobása, majd ugrás az 1-re.

1. Ethernet átviteltechnika

2. Fast Ethernet (IEEE 802.3u):

Kifejlesztésének célja:

- 10BASE-T Ethernethez (IEEE 802.3) képest 10-szeres átviteli sebesség elérése.
- Kábelezési rendszer megőrzése.
- MAC módszer és keretformátum megtartása

A 10BASE-T hálózatok nagy része 100 m-nél rövidebb kábelekkel csatlakozott a hálózathoz. Két állomás távolsága legfeljebb 200 m (egy jelismétlő alkalmazásával).

100 Mbps átviteli sebesség esetén 512 bit átviteli ideje alatt a legtávolabbi állomások is érzékelik az ütközést, így a maximális hosszak lerövidítésével a CSMA/CD MAC módszer megtartható.

A szabvány változatai:

100BASE-TX fél-duplex módban 100 Mbit/s, duplex módban pedig 200 Mbit/s ráta.

100BASE-FX különálló adási (Tx) és vételi (Rx) útvonalai összesen 200 Mbit/s ráta.

1. Ethernet átviteltechnika

2. Fast Ethernet (IEEE 802.3u) (folyt.):

100BASE-X (100BASE-TX, 100BASE-FX).

Különböző médiumokra (X) tervezték:

- Category 5 árnyékolatlan (UTP) kábel
- Category 5 árnyékolt (STP) kábel
- Optikai szál (MM, SM)
- Az FDDI hálózatra kifejlesztett 4B5B (4B/5B) bitkódolást adaptálták a 100BASE-X-re.

4B/5B kódolási mechanizmus:

- Az adat minden 4 bitjét (nibble) 5 biten kódolják.
- Csak olyan 5 bites szimbólumokat használnak, amelyben legfeljebb két '0' bit van egymás mellett.
- A garantált 2 bitenkénti jelátmenet jó bitszinkronizálást biztosít.
- A 100BASE-X változat 4B/5B kódolást használ, mely réz kábelezésnél többszintű átvitelt (Multi-Level Transmit, MLT-3) alkalmaz.

1. Ethernet átviteltechnika

2. Fast Ethernet (IEEE 802.3u) (folyt.):

4B/5B kódolási mechanizmus (folyt.):

Adat		4B/5B kód
(Hexa)	(Bináris)	
0	0000	11110
1	0001	01001
2	0010	10100
3	0011	10101
4	0100	01010
5	0101	01011
6	0110	01110
7	0111	01111

Adat		4B/5B kód
(Hexa)	(Bináris)	
8	1000	10010
9	1001	10011
A	1010	10110
B	1011	10111
C	1100	11010
D	1101	11011
E	1110	11100
F	1111	11101

1. Ethernet átviteltechnika

3. Gigabit Ethernet (IEEE 802.3ab, IEEE 802.3z):

1000BASE-TX:

- Cat5e UTP kábel (802.3ab) négy érpár szükséges a 125 MHz/szálpár átvitel miatt.
- Duplex átvitelt lehetővé tévő hibrid áramkörökkel a sávszélesség 250 Mbit/s/szálpár.
- Résidő 4096 bit (512 bájt).

1000BASE-SX:

- 850 nm-es lézer vagy LED-es fényforrás többmódusú optikai szálon működik.
- Olcsóbb, kisebb távolságok (550 m) áthidalására alkalmas.
- Az adásra (Tx) és a vételre (Rx) külön optikai szál, ezért összeköttetés full duplex.

1000BASE-LX:

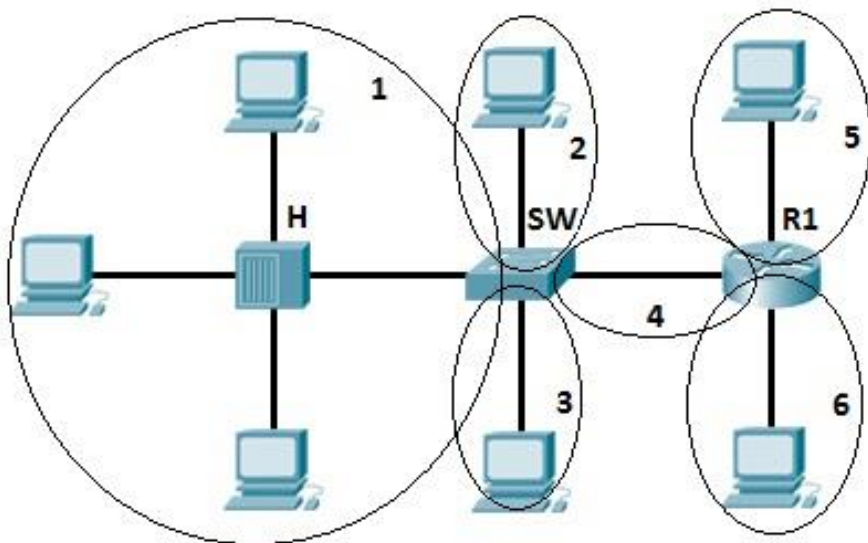
- 1310 nm-es lézerforrások egymódusú vagy többmódusú optikai szálon.
- Egymódusú optikai szálon az áthidalt távolság: 5.000 m.
- Az adásra (Tx) és a vételre (Rx) külön optikai szál, ezért összeköttetés full duplex.

1. Ethernet átviteltechnika

4. Ethernet kapcsolat, szegmentálás:

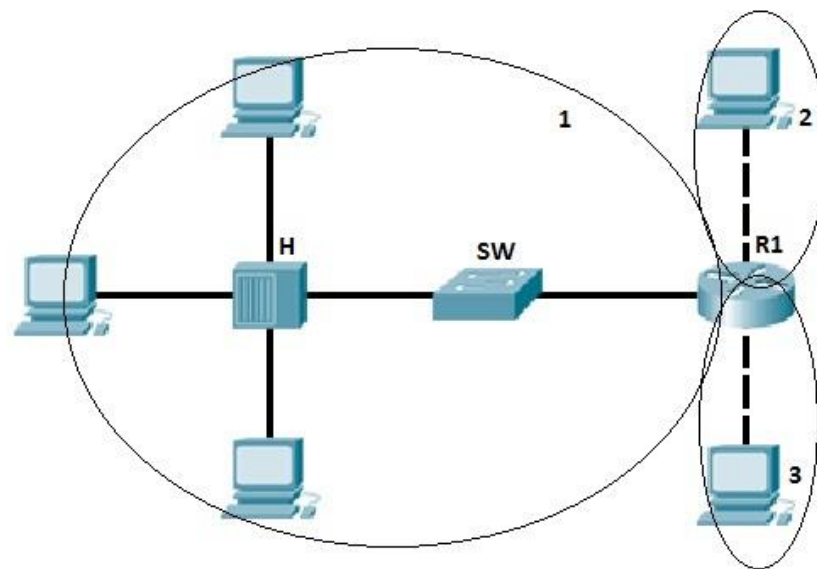
Ütközési tartomány:

Jelismétlőkkel (repeater, hub)
összekapcsolt azonos típusú közeg.



Üzenetszórési tartomány:

L3 PDU útválasztó nélküli
kézbesítésének tartománya.



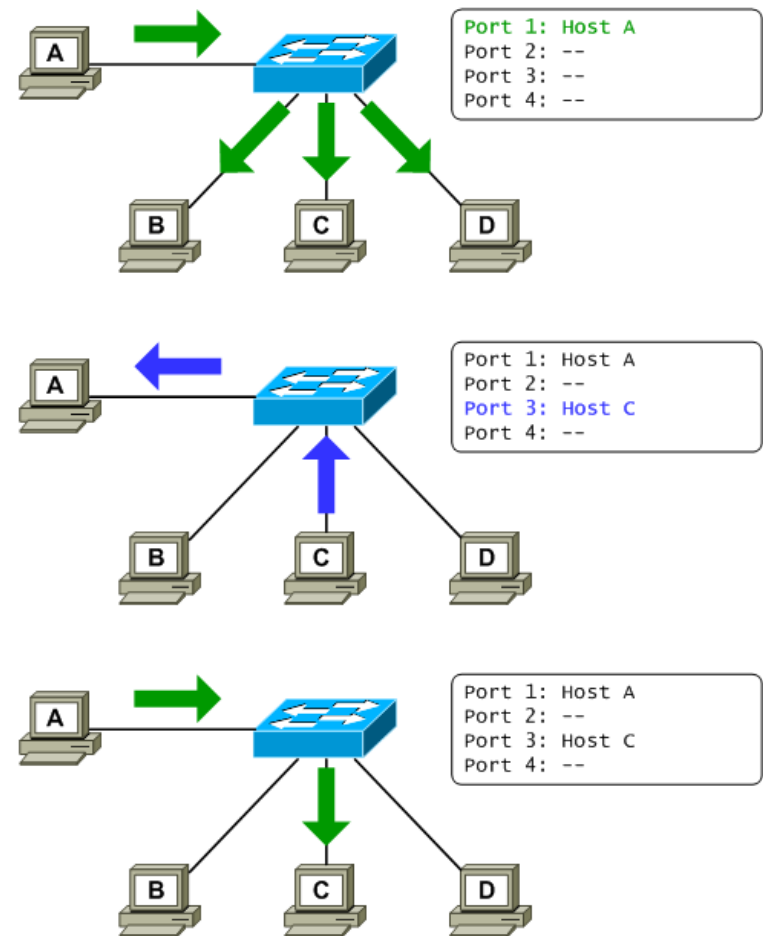
- Az L2 eszközök (híd, kapcsoló) fizikai interfészenként szeparálják az ütközési tartományokat, de az Ethernet végpontok egyedi MAC-címe alapján szabályozzák a keretek továbbítását.
- A második és harmadik rétegbeli készülékek az ütközéseket nem továbbítják.

1. Ethernet átviteltechnika

4. Ethernet kapcsolás, szegmentálás (folyt.):

Ethernet kapcsolás folyamata (Ethernet switching):

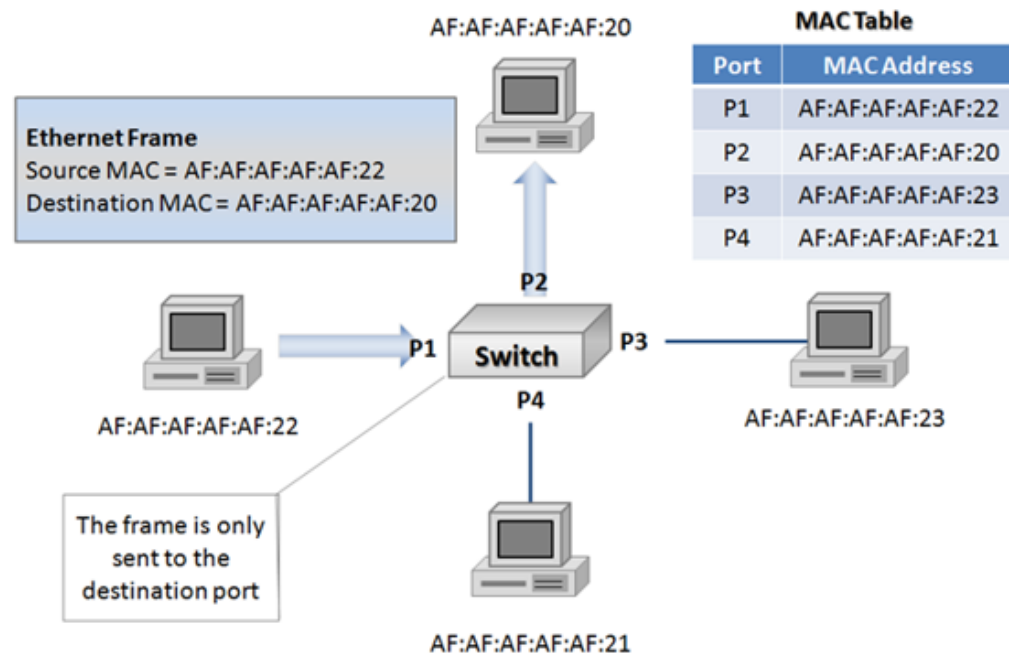
- A kapcsolók dinamikusan töltik fel és tartják karban kapcsolási táblájukat (az érkező keretek forráscíme alapján).
- A kapcsolási táblát tartalom szerint címezhető memóriában tárolják (Content Addressable Memory, CAM).
- A kapcsoló a beérkező Ethernet keret célcímét keresi a kapcsolási táblájában.
- **Kereső algoritmus:** Ha a célcím nem található meg a kapcsolási táblában, akkor valamennyi portján továbbítja a keretet (kivéve az érkezési portot).



1. Ethernet átviteltechnika

4. Ethernet kapcsolás, szegmentálás (folyt.):

- A CAM révén a kapcsoló kereső algoritmus futtatása nélkül is meg tudja találni az adott MAC címhez tartozó saját fizikai interfészét.
- Ha a célcím újcímzési cím (FF:FF:FF:FF:FF:FF), akkor a keretet a kapcsoló valamennyi portján továbbítja (kivéve az érkezési porton).
- Ha a célcím megtalálható a kapcsolás táblában, akkor a hozzá tartozó portra továbbítja a keretet (ha nem azonos a keret érkezési portjával).



1. Ethernet átviteltechnika

4. Ethernet kapcsolás, szegmentálás (folyt.):

Ethernet kapcsolási módszerek:

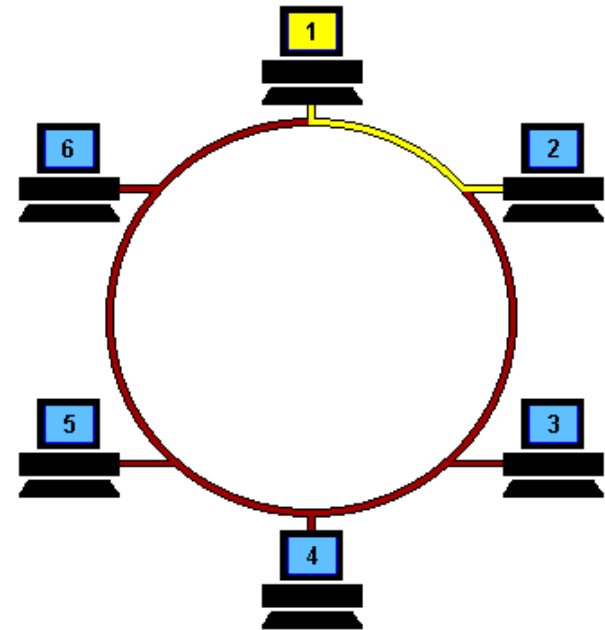
- **Tárol és továbbít:** A keret továbbítása a teljes keret megérkezése után kezdődik meg. A kapcsoló újraszámítja a keretellenőrző összeget (CRC – Cyclical Redundancy Code, FCS - Frame Control Sequence), s ha a keret hibás, eldobja.
- **Közvetlen kapcsolás:** A célcím (6 bájt) megérkezése után azonnal megkezdődik a keret továbbítása a kimeneti porton.
- **Töredékmentes kapcsolás:** A minimális keretméret (64 bájt) megérkezése után kezdődik a keret továbbítása a kimeneti porton. Esetlegesen ütköző keret nem kerül továbbításra.
- **Adaptív kapcsolás:** A fenti három közül a legelőnyösebb üzemmód dinamikus választása.

2. Token Ring átviteltechnika

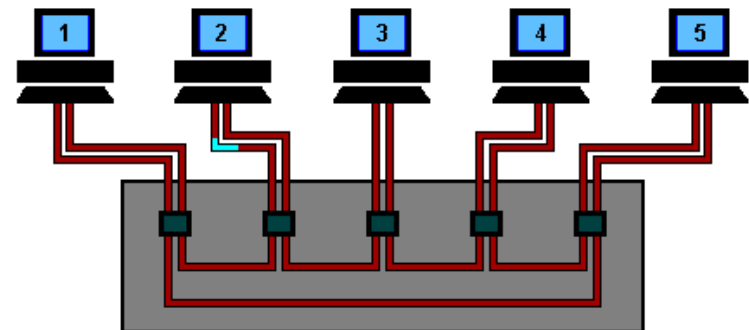
Token Ring (ISO/IEEE 802.5):

Lehetséges topológiák:

Gyűrű (repeater)



Gyűrű huzalozott csillag (repeater, switch)



2. Token Ring átviteltechnika

Token Ring (ISO/IEEE 802.5) (folyt.):

Zseton szerkezete

Start Delimiter (SD)	Access Control (AC)	End Delimiter (ED)
1 B	1 B	1 B

Keret szerkezete

SD	AC	FC	DA	SA	Data	CRC	ED	FS
1 B	1 B	1 B	6 B	6 B	max. 4500 B	4 B	1 B	1 B

FC – Frame Control

ED- Ending Delimiter

FS – Frame Status

2. Token Ring átviteltechnika

Token Ring (ISO/IEEE 802.5):

- A vezérjeles gyűrű eliminálja az ütközést.
- Egy speciális keret (vezérjel, zseton, token) a topológia által adott sorrendben egy-egy csomóponthoz kerül.
- A zseton birtoklása a csomópont számára egyetlen keret elküldését engedélyezi.
- Az állomás az adás után a vezérjelet továbbadja a soron következő állomásnak.
- A logikai topológia: gyűrű, a fizikai topológia: csillag.
- A középpontban lévő TCU (Trunk Coupling Unit) berendezés szervezi a logikai gyűrű működését és biztosítja a gyűrű folytonosságát állomás vagy kapcsolat meghibásodása esetén is.

2. Token Ring átviteltechnika

Token Ring (ISO/IEEE 802.5) (folyt.):

Vezérjeles gyűrű működési elve:

- Adatküldés előtt a csomópont megvárja a zseton beérkezését.
- A zseton birtokló csomópont elküldi a keretét a gyűrűben lévő célcsomópontnak a következő csomóponton keresztül.
- A zsetont nem birtokló csomópontok mindegyike továbbadja a beérkező keretet és összehasonlítja a cél fizikai címet a saját címével.
- Ha illeszkedés van (vagyis ez a címzett), akkor értelmezi a keretet, egyébként nem értelmezi a keretet.
- A célcsomópont a keret végére állapotinformációt helyez el az átvétel automatikus nyugtázása céljából.
- A keretet a forrásállomás távolítja el a gyűrűből és feldolgozza a nyugta állapotinformációt is.
- A feladó állomás továbbküldi a vezérjelet.

2. Token Ring átviteltechnika

Token Ring (ISO/IEEE 802.5) (folyt.):

Token Ring változatok:

TR (4 Mbps)

- Egyszerre csak 1 keret van a gyűrűben.
- A vezérjelet a feladó állomás csak a keret visszaérkezése után továbbítja.
- Max. 72 csomópont azonos gyűrűben.

ETR (Early TR, 16 Mbps)

- Egyszerre több keret van a gyűrűben.
- A vezérjelet a feladó állomás a keret elküldése után azonnal továbbítja a rákövetkező állomásnak (early token release).
- Max. 125 csomópont azonos gyűrűben.

FTR (Fast TR, 100 Mbps): IEEE 802.5t (2000)

GTR (Gigabit TR, 1 Gbps): IEEE 802.5v (2003)

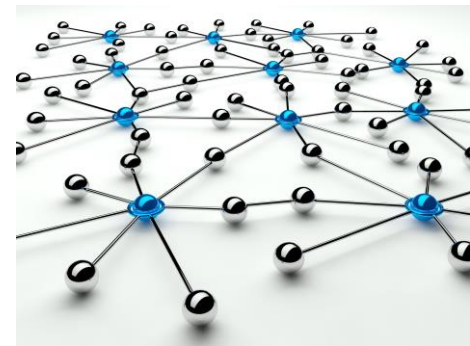
Hálózati architektúrák és protokollok

6. WAN ÁTVITELTECHNIKÁK

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) SLIP átviteltechnika
- 2) PPP átviteltechnika
- 3) ISDN átviteltechnika
- 4) ATM átviteltechnika
- 5) DSL átviteltechnika

1. SLIP átviteltechnika

Általános leírás:

- SLIP: Serial Line Internet Protocol, első verzió: RFC 1055.
- Célja az IP csomagok küldése soros (pont-pont) linken keresztül.
- Aszinkron, karaktert továbbító protokoll: 8 bit, paritásbit nincs.
- Számos kellemetlen előírása/hiányossága miatt ma már kevésbé használják:
 - Csak az IP csomagokat továbbít.
 - Statikus IP címkiosztást feltételez.
 - Nincs keretcímzés.
 - Nincs hibajelzés, nincs hibajavítás, nincs tömörítés.
 - Nincs autentikáció.
- Bájt beszúrás (Byte Stuffing) miatt a keret hossza függ a tartalomtól.
- Tömörített SLIP (CSLIP, Compressed Serial Line Internet Protocol) változat:
 - TCP szegmens fejrészét 20 bájtról 7 bájtra csökkenti.
 - Csak 16 darab különféle egyidejű TCP kapcsolatot tud kezelni.

1. SLIP átviteltechnika

SLIP keretformátum:

- Vezérlő bájtok:

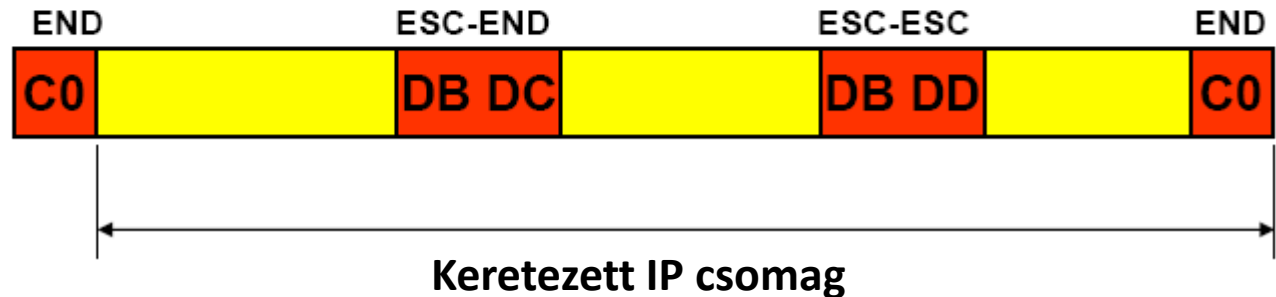
Hexa érték	Bájt név	Bájt funkció
0xC0	END	Keretlezáró
0xDB	ESC	Keret ESC
0xDC	ESC_END	Módosított keretlezáró
0xDD	ESC_ESC	Módosított keret ESC

IP csomag



Bájt beszúrás

SLIP keret



2. PPP átviteltechnika

Általános leírás:

- PPP: Point to Point Protocol, első verzió: RFC 1661, 1662, 1663.
- Célja bármilyen L3 datagram továbbítása full-duplex soros vonalon.
- Szinkron és aszinkron átvitelre képes. Keret jelzők: kezdet- és véghatároló (0x7E).
- Két funkcióhalmazból áll:
 - Kapcsolat vezérlő protokoll (**LCP**, Link Control Protocol): egy darab/link
 - Keret szintű logikai kapcsolat felépítés,
 - Keret szintű logikai kapcsolat konfigurálás,
 - Keret szintű logikai kapcsolat tesztelés.
 - Hálózat vezérlő protokoll (**NCP**, Network Control Protocol): több darab/link
 - L3 hálózati kapcsolat felépítés,
 - L3 hálózati kapcsolat konfigurálás, tömörítés
 - Adott link-en egyidőben működő minden egyes hálózati réteg protokollhoz egy-egy támogató NCP szükséges.

2. PPP átviteltechnika

Általános leírás (folyt.):

- Alap enkapszuláció: HDLC (High-Level Data Link Control)
 - Keretezés és átviteli hiba detektálás
 - Csak számozatlan adatkeretek továbbítása
- PPP keret tartalma:
 - Fejrész (2-8 bájt) + Datagram + Lezáró rész
 - Az L2 fejrész (2-8 bájt) összetétele: HDLC fejrész + PPP fejrész
- Bájt beszúrás (Byte Stuffing) miatt a keret hossza függ a tartalomtól.
- Támogatott autentikáció típusok:
 - **PAP** (Password Authentication Protocol):
 - titkosítatlan (cleartext) jelszóátvitel a kommunikáció kezdetén
 - **CHAP** (Challenge-Handshake Authentication Protocol):
 - titkosított jelszóátvitel, bármikor kérhető.

2. PPP átviteltechnika

PPP keretformátum:

↓
**Továbbítási
sorrend**

Flag
Address
Control
Protocol
Adat
Checksum
Flag

1 bájt: '01111110' (Kezdethatároló).
1/0 bájt: '11111111' (Broadcast).
1/0 bájt: pl. keretszámozás kialakítására.
2/1 bájt: pl. LCP, NCP, IP, IPX.
0 - 1500 bájt (tipikusan).
2 bájt (Létezik 32 bites kiterjesztés).
1 bájt: '01111110' (Végthatároló).

- LCP opciókkal a mezők mérete csökkenthető (hatékonyságnövelés, pl. Protocol 2/1).

Hexa érték	Bájt név	Bájt funkció
0x7E	FLAG	Kerethatároló (kezdet, vég)
0x7D	ESC	Keret ESC
0xAE	ESC_END	Módosított lezáró
0xAD	ESC_ESC	Módosított ESC

3. ISDN átviteltechnika

Általános leírás:

- ISDN: Integrated Services Digital Network
- Célja digitális adat, hang, videó forgalmak integrációja azonos technológián.
- Áramkörkapcsolást használ a tartalom továbbításához.
- **Szabványos csatornatípusok:**
 - A: 4 kHz analóg telefoncsatorna.
 - B: 64 kbps digitális hang vagy adatcsatorna.
 - C: 8/16 kbps digitális csatorna.
 - D: 16/64 kbps digitális csatorna (jelzés, signaling).
- **Három szabványos csatorna kombináció (interfész):**
 - BRI, Basic Rate Interface: $2 \cdot B + 1 \cdot D_{(16)}$ (144 kbps)
 - PRI, Primary Rate Interface: $T1: 23 \cdot B + 1 \cdot D_{(64)}$ (USA: 1,544 Mbps),
 $E1: 30 \cdot B + 1 \cdot D_{(64)}$ (EU: 2,048 Mbps)
 - HRI, Hibrid Rate Interface: $1 \cdot A + 1 \cdot C$ (ritka alkalmazás)

3. ISDN átviteltechnika

Általános leírás (folyt.):

- Jelzésrendszer: ITU-T Q.931 (QSIG)
- Gyors kapcsolat felépítés és kapcsolat lebontás a D csatornán.
- Átviteli ráta növelés $n \cdot 64$ kbps lépésekben.
- Több egyidejű áramkör építhető ki adott interfészen

Pl.:

- BRI: $\text{hang}_{(64)} + \text{adat}_{(64)}; \text{adat}_{(128)}$

- PRI: $\text{cs1}_{(bw1)} + \text{cs2}_{(bw2)} + \dots + \text{csk}_{(bwk)}$

$$bwi = ni \cdot 64 \text{ kbps}, i = 1, 2, \dots, k$$

$$bw1 + bw2 + \dots + bwk \leq r \cdot 64 \text{ kbps (USA: } r = 23, \text{ EU: } r = 30)$$

- A 64 kbps-os csatornára épülő megoldás elnevezése:
Keskenysávú ISDN (Narrowband ISDN, N-ISDN).
- Ma a gyakorlatban nagyobb átviteli ráta igények léteznek.

3. ISDN átviteltechnika

Általános leírás (folyt.):

- Alkalmazott hangkódolási technika: **PCM (Pulse Code Modulation)**
 - Analóg jel amplitúdójának átalakítása digitálisra (A/D)
 - Mintavételezési frekvencia: 8 kHz
 - Mintavételi mélység: 8 bit
 - Átviteli ráta: 64 kbps
- Mivel az emberi hallószerv érzékenyebb az alacsony hangerő skálán bekövetkező változásra, ezért a $[-2^7, 2^7]$ amplitúdó tartományt átkódolják önmagára nem lineáris törvény szerint.
- Kódolási törvények:

A-law (EU: $A = 87,6$):

$$F(x) = \text{sgn}(x) \begin{cases} \frac{A|x|}{1+\log(A)}, & |x| < \frac{1}{A} \\ \frac{1+\log(A|x|)}{1+\log(A)}, & \frac{1}{A} \leq |x| \leq 1, \end{cases}$$

μ -law (USA, JP: $\mu = 255$):

$$F(x) = \text{sgn}(x) \frac{\ln(1 + \mu|x|)}{\ln(1 + \mu)} \quad -1 \leq x \leq 1$$

4. ATM átviteltechnika

Megfontolások:

- A mai hálózatoknál sokféle szolgáltatási igény létezik: adattovábbítás, hang- és videoátvitel, multimédia tartalmak átvitele, számítógéppel segített oktatás (Computer Aided Learning = CAL).
- Ezeket a szolgáltatásokat egyidőben nyújtó hálózati rendszereket **Szélessávú, integrált szolgáltatású hálózatoknak** nevezzük: Broadband ISDN, **B-ISDN**.
- A B-ISDN hálózatok követelményei messze meghaladják az adathálózatokkal szemben támasztott követelményeket.

Különböző tartalmak átviteli ráta szükségletei:

- Az audió és videó átvitele állandó bitsebességet, és alacsony késleltetést igényel.
- Videokonferencia rendszerekben az egymás utáni képkockák keveset változnak, így hatékony képtömörítés lehetséges.
- Hang, kép és videó átvitele esetén a tömörítés lehetséges információvesztő is, amely viszont jelentősen csökkenti a továbbított bájtok számát.
- Az állandó átviteli rátát igénylő tartalmak az eddig tárgyalt (minőségi garanciákat nem támogató) technikákkal nem továbbíthatók hálózaton.
- Olyan új technológiára van szükség, amely az adatátvitelen kívül a többi médiatípus átvitelére is alkalmas. Az egyik ilyen hálózat az **ATM (Asynchronous Transfer Mode)**.

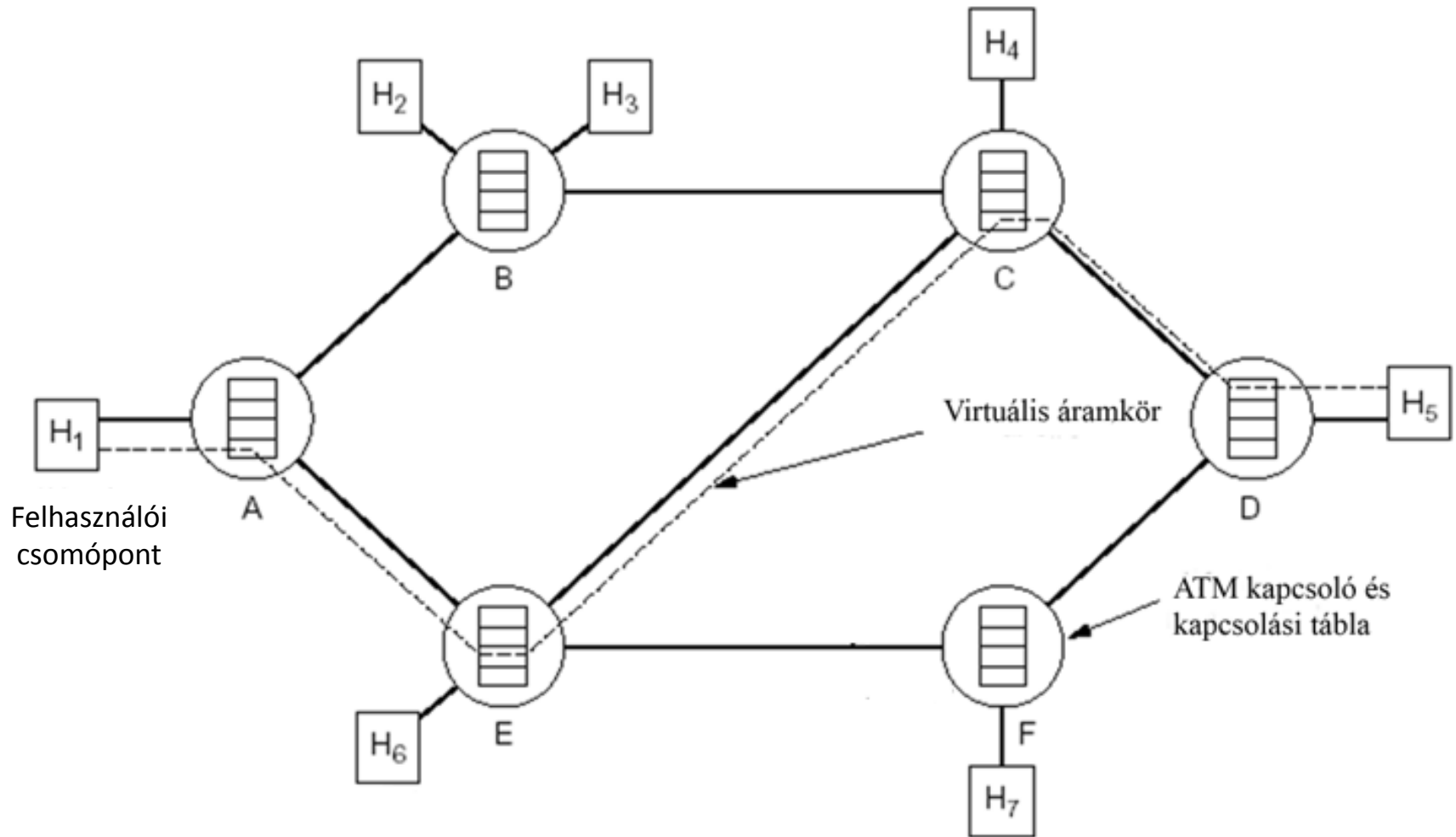
4. ATM átviteltechnika

Általános leírás:

- Az átviteltechnika kifejlesztését az ATM Forum koordinálta. Sok (150) ipari képviselő közös munkájának eredménye az 1990-es években.
- Cellakapcsolt technológia, a PDU mérete rögzített.
- A cellák kis méretűek (53 bájt), ezért a csomagkapcsolás előnyeit örökli.
- Cellák továbbítása: statisztikus multiplexálási módszerrel, hatékony csatorna kihasználás.
- Áramkör kapcsolási technika alapján történik a cellák útjának kiválasztása:
 - Hardver szintű kapcsolat (nagyon gyors),
 - Hierarchikus útvonal azonosítás.
- Az előfizetők számára kommunikációs garanciákat (QoS, Quality of Service) nyújt:
 - Késleltetés,
 - Átviteli ráta,
 - Késleltetés ingadozás (dzsitter),
 - Hibaarány, stb.
- A rendszer nagyon jól skálázható különböző szempontok alapján:
 - Átviteli ráta,
 - Csomópontszám,
 - Időérzékenység.

4. ATM átviteltechnika

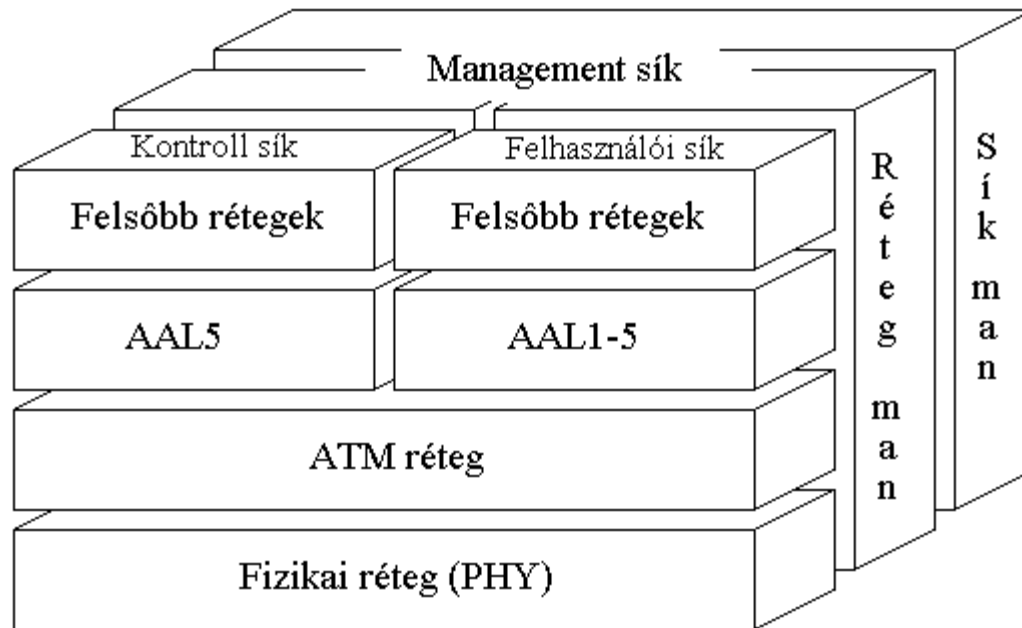
Felépítés és működési modell:



4. ATM átviteltechnika

Általános leírás:

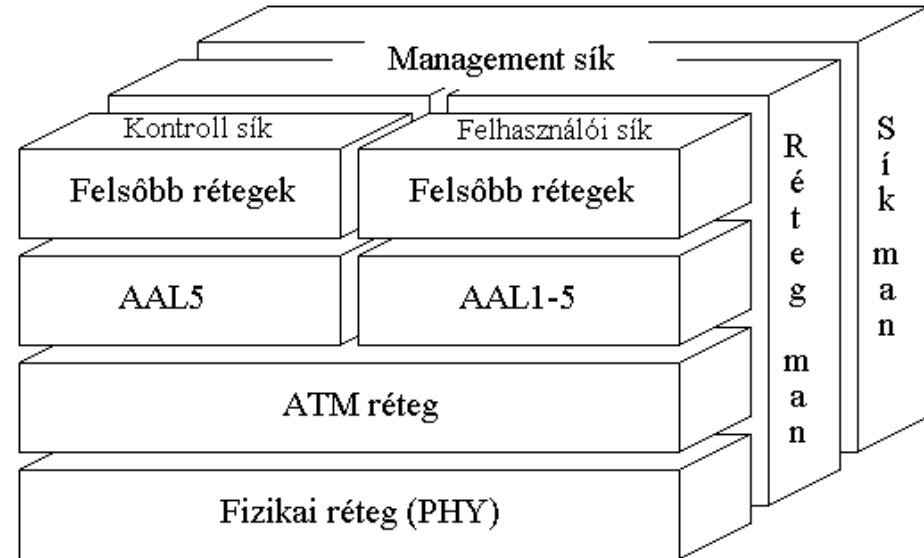
- A koncepció lényegesen eltér az OSI modelltől, mivel a kommunikációs rétegek között transzparens erőforrás menedzsment történik.
- Rétegekbe és síkokba szervezett funkciók csak részben hasonlítanak az OSI rétegek funkcióihoz.



4. ATM átviteltechnika

Általános leírás (folyt.):

- Síkok:
 - Felhasználói sík: adatok átvitele
 - Kontroll sík: jelzésrendszer
 - Réteg menedzsment sík
 - Sík menedzsment sík
- Rétegek:
 - Fizikai réteg (két alréteg):
 - Közegfüggő alréteg (PMD, Physical Medium Dependent): jelek továbbítása
 - Átvitel konvergencia alréteg (TC, Transmission Convergence): cella keretek képzése
 - ATM réteg:
 - Cellák létrehozása (fejrész, hibaellenőrzés)
 - Cella multiplexálás és demultiplexálás
 - Cellakapcsolás
 - ATM Adaptációs réteg (AAL)
 - Szolgáltat típusok (időzítés, enkapszuláció/dekapszuláció)



4. ATM átviteltechnika

Általános leírás (folyt.):

- ATM Adaptációs réteg (AAL) (folyt.):
 - Osztályok:

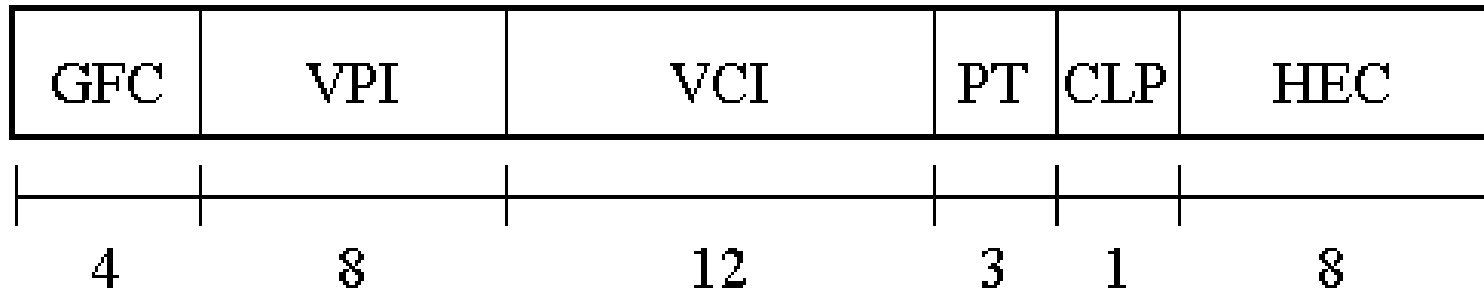
Jellemző	Class A	Class B	Class X	Class C	Class D
Időzítés	Időzítésre érzékeny		Időzítésre nem érzékeny		
Bitráta	Állandó (CBR)	Változó (VBR)			
Kapcsolat	Kapcsolatorientált				Kapcsolat nélküli
Alkalmazás	Áramkör emuláció	Tömörített videó	Cella átadás	Bőrsztös adat	Datagram
AAL	AAL 1	AAL 2	AAL 0	AAL 3/4, 5	AAL 3/4, 5

- AAL3 C osztály, AAL4 D osztály, ezért egyben kezelik: AAL 3/4
- AAL 5: IP over ATM (IPoA), Ethernet over ATM (EoA), LAN emuláció (LANE)

4. ATM átviteltechnika

Cella struktúra:

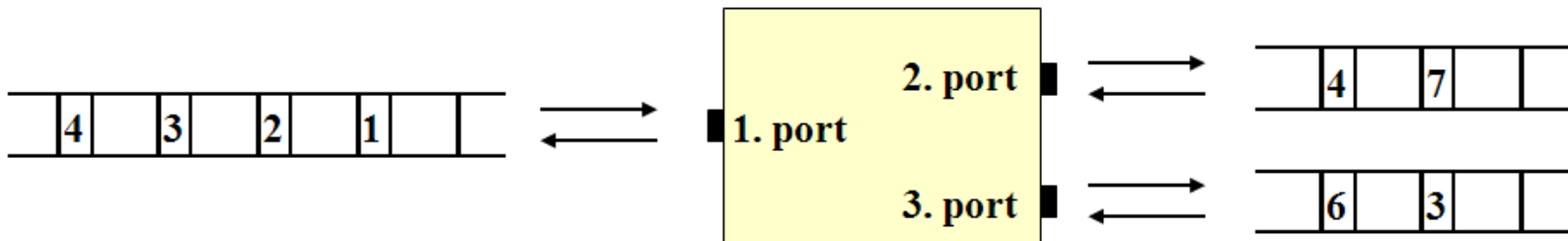
- **Fejrész** (Header): 5 bájt, két változat



- GFC (Generic Flow Control): multiplexálás és mobil kommunikáció támogatása
 - UNI (User-Network Interface) esetén létezik
 - NNI (Network-Network Interface) esetén nem létezik
- VPI/VCI (Virtual Path Identifier / Virtual Channel Identifier): virtuális áramkört azonosít
- PT (Payload Type): rakrész tartalom típusa
- CLP (Cell Loss Priority): eldobható cella jelölése
- HEC (Header Error Control): fejrész hibaellenőrző kód
- **Rakrész** (Payload): 48 bájt
- Lezáró rész (Tail): nincs

4. ATM átviteltechnika

Cellakapcsolás példa:



1. port
kapcsolási táblázat

Be		Ki	
Port	KA	Port	KA
1	1	2	7
1	2	2	4
1	3	3	3
1	4	3	6

2. port
kapcsolási táblázat

Be		Ki	
Port	KA	Port	KA
2	7	1	1
2	4	1	2

3. port
kapcsolási táblázat

Be		Ki	
Port	KA	Port	KA
3	3	1	3
3	6	1	4

KA = Kapcsolat azonosító (VPI+VCI)

5. DSL átviteltechnika

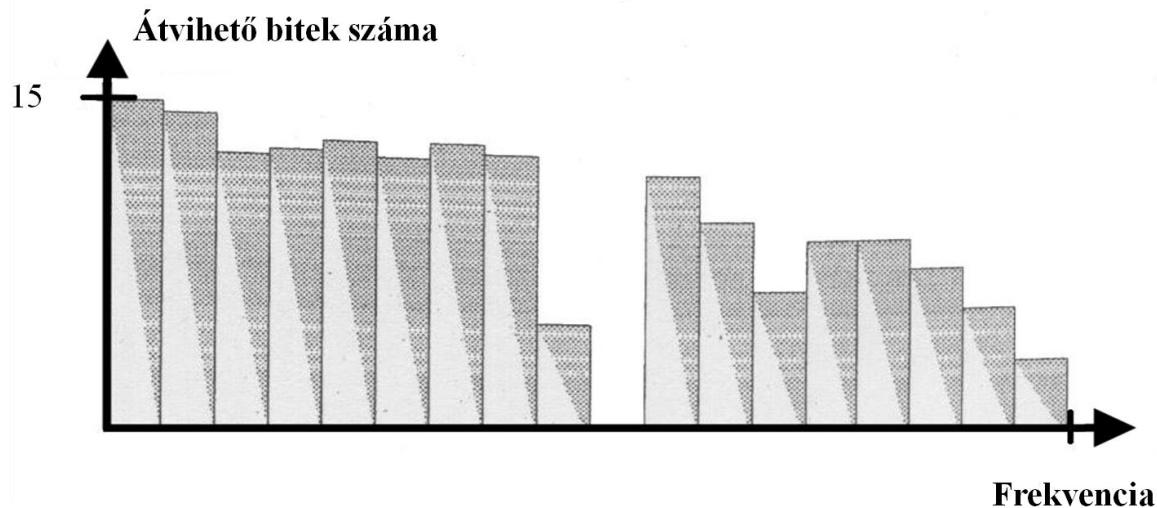
Megfontolások:

- A klasszikus telefon technológiában a végfelhasználók csatlakoztatására használatos réz érpár lehetővé teszi 1-2 MHz-es sáv szélesség alkalmazását kilométer nagyságrendű távolságra. Így a telepített telefonvezetékeken kialakítható Mbps nagyságrendű átviteli ráta.
- Az árnyékolatlan érpár érzékeny a környezeti zajokra, ezért az átvitel során hibajavítás szükséges.
- Frekvenciaosztásos közeghozzáférés esetén a frekvenciatartomány tetszőleges diszjunkt tartományokra bontható.
- A felhasználók a nagytömegű letöltéshez nagyobb sáv szélességet igényelnek, míg a várhatóan lényegesen kisebb mennyiségű adatfeltöltéshez kisebb sáv szélesség is elegendő.
- Megfontolható a rendelkezésre álló sáv szélesség (frekvenciatartomány) irányonkénti aszimmetrikus felosztása.

5. DSL átviteltechnika

Zajforrások hatásának enyhítése:

- A huzal közelében működő nagyteljesítményű középhullámú rádióadók viszonylag keskeny sávban, de nagy teljesítménnyel sugároznak: Pl. a Solton működő rádióadó 540 kHz-en 3 MW (megawatt!) teljesítménnyel sugározza a Kossuth rádió műsorát. Az adó közelében ez nagyon rossz jel-zaj viszonyt eredményez ("a zaj erősebb a jelnél").
- Megoldás: DMT (Discrete MultiTone) modulációs technika: a rendelkezésre álló frekvenciatartomány nagyon kicsi (4,3 kHz) sáv szélességű alcsatornákból áll. Az egyes alcsatornákon külön-külön meghatározható a jel-zaj viszony, és erre építve a dinamikus bitráta.



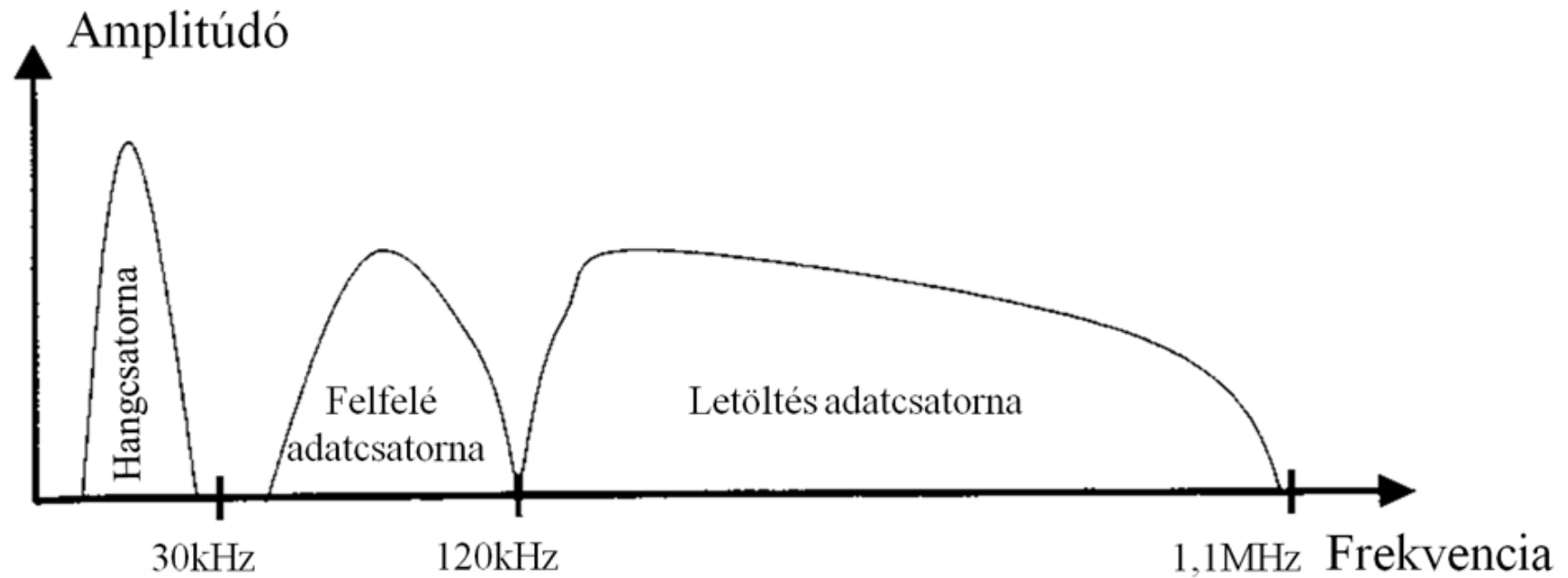
5. DSL átviteltechnika

DSL (Digital Subscriber Line) változatok:

DSL típus	Átviteli mód	Letöltés [Mbps]	Feltöltés [Mbps]	Távolság [km]	Megjegyzés
ADSL	Analóg	8	1	6	1,1 MHz
ADSL2	Analóg	12	3	4	1,1 MHz
ADSL2+	Analóg	24	3	4	2,2 MHz
HDSL	Digitális	1,544	1,544	4	2 érpár
SDSL	Digitális	1,544	1,544	3	1 érpár
IDSL	Digitális	144 kbps	144 kbps	15	ISDN
VDSL	Analóg	50	5	1,5	50 Mbps, 300m
VDSL2	Analóg	100	100	1,5	igény: 30 MHz

5. DSL átviteltechnika

Aszimmetrikus frekvenciatartományok (ADSL):



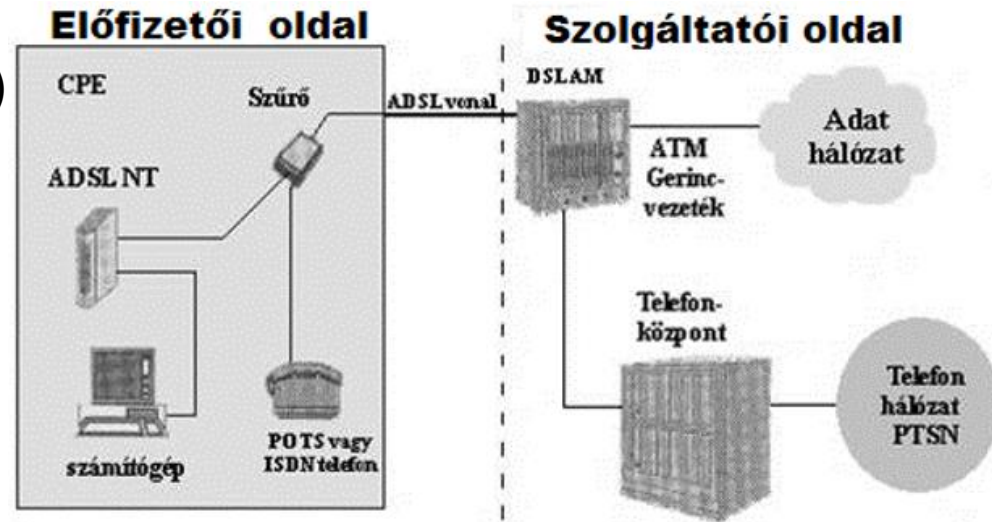
- Csatornák:
 - Hang (~ 30 kHz)
 - Adat feltöltés (~ 80 kHz)
 - Adat letöltés (~ 1000 kHz)

5. DSL átviteltechnika

ADSL rendszer felépítése:

- Előfizetői oldal:

- Előfizetői vonal (helyi hurok, Local Loop)
- Szűrő (hangcsatorna, adatcsatornák)
- ADSL NT (Network Termination, vagy ADSL modem), RJ-45 interfésszel, Ethernet vagy autentikációs célok miatt PPP over Ethernet.



- Szolgáltatói oldal:

- DSLAM (Digital Subscriber Line Access Multiplexer):
Nagy kapacitású trónk vonalon multiplexálja az előfizetők forgalmát az Internet felé.

- Jelenleg az ADSL-t a szolgáltatók széles körben nyújtják az előfizetők számára.

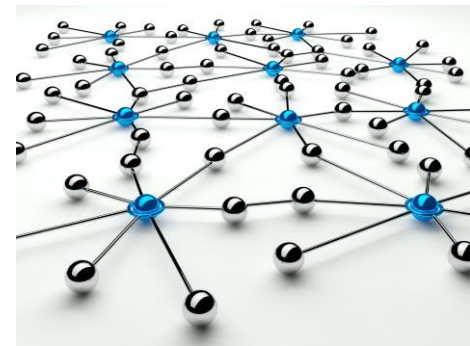
Hálózati architektúrák és protokollok

7. IP TECHNOLÓGIA HÁLÓZATI RÉTEGE

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) IP protokoll adatelem szerkezete
- 2) IP címezési rendszer
- 3) IP vezérlő mechanizmus (ICMP)
- 4) IP forgalomirányítási alapok
- 5) IP alhálózatok és IP aggregált hálózatok

1. IP protokoll adatalem szerkezete

Általános leírás:

- Vint Cerf és Bob Kahn (USA): 1974
- Az IP (Internet Protocol, RFC 791) a TCP/IP referenciamodell általános adatszállításra szolgáló hálózati réteg protokollja.
- Összeköttetés mentes (datagram) szolgáltatást nyújt a szállítási réteg felé.
- Datagram: önálló adatcsomag, amely az azonosításhoz és a kézbesítéshez szükséges összes elemet tartalmazza.
- IP csomag: fejrész (Header) + rakrész (Payload)
- Típusazonosító az L2 (pl. Ethernet) keretekben: 0x0800
- IP csomag fejrész:
 - A datagram kézbesítéséhez szükséges információk (címek, vezérlő és ellenőrző mezők)
 - 4 bájtos (32 bites) szavakból áll
 - Szavak száma: minimum: 5, maximum: 15.
- IP csomag rakrész:
 - Szállítási réteg adatalemét foglalja magába
 - Maximális méret: 64 kB
 - Nincs hibaellenőrző kód

1. IP protokoll adatalem szerkezete

IP csomag darabolás és összerakás:

- A max. 64 kB méretű IP csomag adatkapcsolati réteg technológiával továbbítódik az üzenetszórási tartományon belül.
- Az L2 technológia keretének rakrész mérete: MTU (Maximum Transmission Unit).
 - Ethernet MTU: 1500 B
 - Ethernet Jumbo MTU: 1501...9198 B
 - Token Ring MTU: 4464 B
 - WiFi MTU: 7981 B
- Küldő csomópontnál beágyazás (enkapszuláció) előtt a túl nagy IP csomagot darabolni (fragmentálni) és a darabokat sorszámozni kell.
- Fogadó csomópontnál a dekapszuláció után bájtrend pontosan össze kell rakni (reassembly) részekből a nagy IP csomagot.
- A részek is szabványos felépítésű IP csomagok.
- Darabolást végező csomópont: forrás, vagy köztes (útválasztó).
- Darabolás engedélyezés hatáskör: forrás csomópont, csomagonként.
- Útvonal menti MTU meghatározása (IPv4: RFC 1191, IPv6: RFC 1981): a legkisebb MTU érték beazonosítása a forrás és cél csomópontok közti útvonalon (ld. ICMP később).

1. IP protokoll adatalem szerkezete

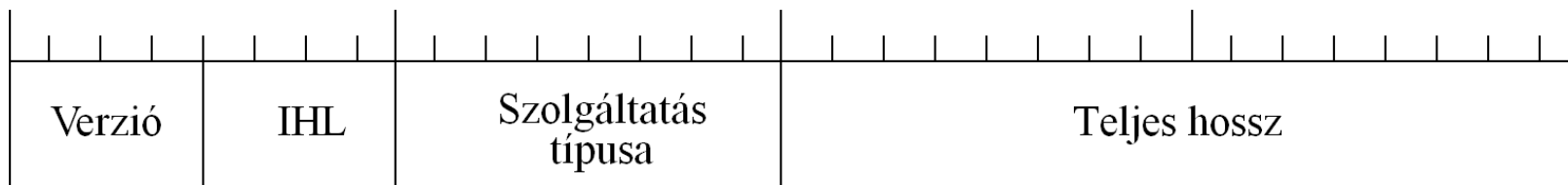
IP csomag fejrésze (Header):

Verzió	IHL	Szolgáltatás típusa	Teljes hossz
Azonosító		D F	M F
TTL	Transzport réteg protokoll	Fejrész ellenőrző összeg	
Feladó (forrás) IP címe			
Címzett (cél) IP címe			
Opcionális mező(k)			

1. IP protokoll adatalem szerkezete

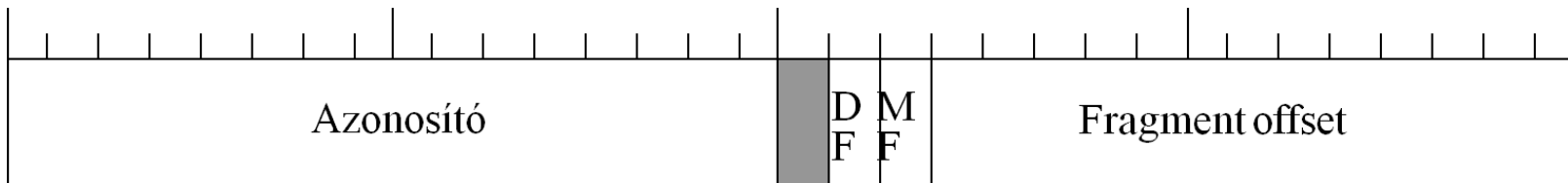
IP csomag fejrésze (Header):

1. szó:



- Verzió: IPv4 (0x4), IPv6 (0x6)
- IHL: IP csomag fejrészének hossza [szó]
- ToS: Szolgáltatás típusa, minőségi jellemzők (QoS)
- SoD: Adatmező+fejrész hossza [Bájt]

2. szó:

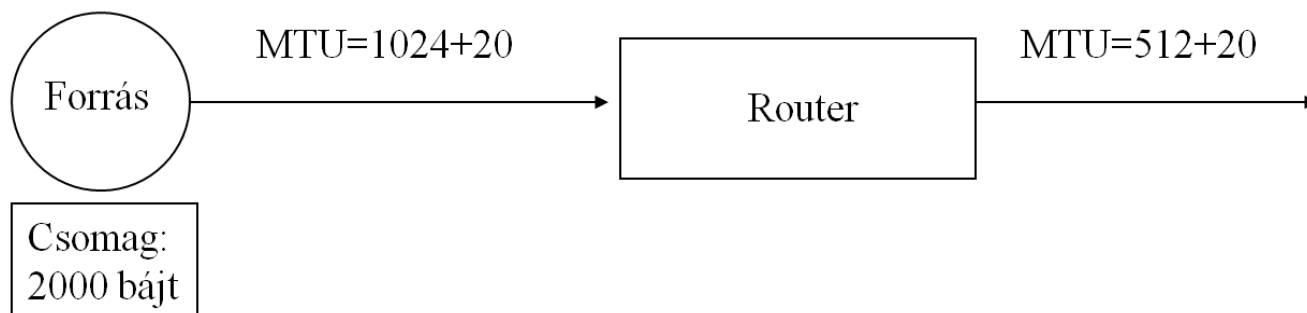


- Csomag darab (fragmentum) azonosító
- DF (Don't Fragment): darabolás tiltás
- MF (More Fragment): további csomagdarab létezik
- Fragmentum offset: csomagdarab helye a nagy csomagban

1. IP protokoll adatalem szerkezete

IP csomag darabolás és összerakás: Példa

- A forrás állomáson küldésre vár egy 2020 B teljes méretű IP csomag (20 bájt IP fejrész).
- A forrás üzenetszórási tartományon MTU = 1024+20 B.
- Az első forgalomirányító távolabbi interfészén MTU = 512+20 B.



Darabolási folyamat:

- Az eredeti (darabolatlan) nagy IP csomag fejrészének 2. szava:

Offset = 0

00000000	10110010	0 00 00000	00000000
----------	----------	------------	----------

- A forrás által feladott IP csomagok fejrész információi (2. szó):

Offset = 0

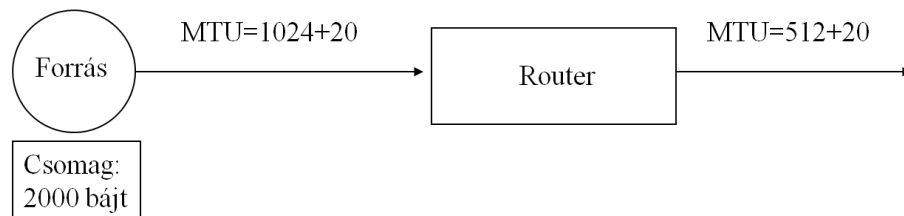
00000000	10110010	0 01 00000	00000000
----------	----------	------------	----------

Offset = 0 + 1024/8 = 128

00000000	10110010	0 00 00000	10000000
----------	----------	------------	----------

1. IP protokoll adatalem szerkezete

IP csomag darabolás és összerakás: Példa



Darabolási folyamat (folyt.):

- A router által továbbküldött IP csomagok fejrészének 2. szava:

Offset = 0

00000000 10110010 0 01 00000 00000000

$$\text{Offset} = 0 + 512/8 = 64$$

00000000 10110010 0 01 00000 01000000

$$\text{Offset} = 64 + 512/8 = 128$$

00000000 10110010 0 01 00000 10000000

$$\text{Offset} = 128 + 512/8 = 192$$

00000000 10110010 0 00 00000 11000000

3. szó:

TTL	Transzport réteg protokoll	Fejrész ellenőrző összeg
-----	-------------------------------	--------------------------

- TTL a csomag „hátralevő életidejének” jelzése. Az útválasztó csökkenti, ha pozitív.
- Szállítási réteg adatelemének típuskódja (RFC 1700).
- Fejrész ellenőrző összeg (HCS): minden útválasztó újraszámolja (kétszer).

1. IP protokoll adatalem szerkezete

IP csomag fejrésze (Header) (folyt.):

4. szó:

Feladó (forrás) IP címe

5. szó:

Címzett (cél) IP címe

- Forrás (feladó) IP cím: 32 bit
- Cél (címzett) IP cím: 32 bit

6. szótól:

Opcionális mező(k)

- Opcionális információk:
 - Továbbítási útvonal naplózása (Record route)
 - Késleltetési idők naplózása (Timestamp)

2. IP címzési rendszer

Megfontolások:

- Az IP címzés a hálózati rétegben logikai azonosításként működik.
- A logikai cím egy hálózati interfészt egyértelműen azonosít.
- Az egyetlen interfészes csomópontnál ez „host cím” megnevezésként használatos.
- IP címmel azonosított interfészek:
 - A végfelhasználói (host) csomópontnál,
 - Az L3 típusú köztes (router) csomópontnál.
- Az azonosítók nyilvántartását nemzetközi szervezetek látják el: (IANA, InterNIC, RIPE).
- Az IP cím kódoltan azonosítja az üzenetszórási tartományt és a host címet is.
- IP címek használata:
 - Szervezet vagy Internet szolgáltató (ISP): IP címtartomány(ok) (hálózat azonosító(k)),
 - Előfizető gép: IP host azonosító.
- Az IP cím hossza bájtok 4^k típusú többszöröse:
 - IPv4: $k = 1$,
 - IPv6: $k = 2$.
- IP címek formátuma:
 - IPv4: decimálisan reprezentált bájtok, pont („.”) karakterrel elválasztva,
 - IPv6: hexadecimálisan reprezentált (ld. később).

2. IP címzési rendszer

IP címkezelés:

- Az IP címzésnél használt kódolási módszer: maszkolás
- Maszk:
 - Hossza megegyezik az IP cím méretével.
 - Formája: 1111 ... 1100 ... 0 = „N(1)”, „H(0)”
 - N: hálózat (halmaz) azonosító rész,
 - H: host (interfész) azonosító rész.
- Szabályok:
 - „0” bit után csak „0” bit lehet,
 - „1” bit után bármi lehet.
- Jelölések:
 - Bináris: 111111111111111111111111111110000000
 - Decimális: 255.255.255.0
 - Prefix: /24 (N: 24 db bit, H: 32-24 = 8 bit)
- Konverzió jelölések között:

Bin	Dec	Bin	Dec	Bin	Dec	Bin	Dec
10000000	128	11100000	224	11111000	248	11111110	254
11000000	192	11110000	240	11111100	252	11111111	255

/n	Decimális	/n	Decimális
/1	128.0.0.0	/17	255.255.128.0
/2	192.0.0.0	/18	255.255.192.0
/3	224.0.0.0	/19	255.255.224.0
/4	240.0.0.0	/20	255.255.240.0
/5	248.0.0.0	/21	255.255.248.0
/6	252.0.0.0	/22	255.255.252.0
/7	254.0.0.0	/23	255.255.254.0
/8	255.0.0.0	/24	255.255.255.0
/9	255.128.0.0	/25	255.255.255.128
/10	255.192.0.0	/26	255.255.255.192
/11	255.224.0.0	/27	255.255.255.224
/12	255.240.0.0	/28	255.255.255.240
/13	255.248.0.0	/29	255.255.255.248
/14	255.252.0.0	/30	255.255.255.252
/15	255.254.0.0	/31	255.255.255.254
/16	255.255.0.0	/32	255.255.255.255

2. IP címzési rendszer

IP címkezelés (példák, IPv4):

	IP	M	N	H	Megjegyzés
a)	13.194.58.11	255.0.0.0	13.0.0.0	0.194.58.11	N és H
b)	13.194.58.12	/8	13.0.0.0	0.194.58.12	N és H
c)	13.194.58.255	/24	13.194.58.0	0.0.0.255	N és speciális H
d)	13.194.58.16	/28	13.194.58.16	0.0.0.0	N és speciális H
e)	192.168.31.107	255.192.0.0	192.128.0.0	0.40.31.107	N és H
f)	192.169.31.108	/10	192.128.0.0	0.41.31.108	N és H
g)	192.170.31.255	/20	192.170.0.0	0.0.31.255	N és speciális H
h)	192.170.32.0	255.255.224.0	192.170.32.0	0.0.0.0	N és speciális H
i)	201.69.254.255	255.255.128.0	201.69.128.0	0.0.126.255	N és H
j)	223.69.255.255	/16	223.69.0.0	0.0.255.255	N és speciális H

2. IP címzési rendszer

IP címkezelés:

- Maszkolás: bitpozíciónkénti ÉS művelet: $N = IP \wedge M$, $H = IP - N$
- Prefix (/n) méretének hatása:
 - Nagy prefix: sok kisméretű (kevés host) különböző üzenetszórési tartomány,
 - Kis prefix: kevés nagyméretű (sok host) különböző üzenetszórési tartomány.
 - Cél: a tartományok (hálózatok) kihasználtsági szintjének növelése, tartalékkal.
- Speciális IP host címek:
 - IP hálózat (halmaz) azonosító: $IP = NH$, ahol H = „csupa bináris 0” (legkisebb érték).
 - IP üzenetszórás (broadcast): $IP = NH$, ahol H = „csupa bináris 1” (legnagyobb érték).
- A speciális IP host címek nem rendelhetők interfészhez.
- Az IP hálózatban kiosztható IP címek száma = $Bcast - N - 1$.

2. IP címzési rendszer

IP címkezelés (Példa címkiosztásra):

Feladat: Legyen IP = 193.6.128.38 és M = 255.255.255.128 paraméterekkel rendelkező IP gép. Határozzuk meg az adott hálózatban a host-okhoz rendelhető (kiosztható) IP címeket!

Megoldás:

$$\begin{aligned} \text{IP} &= 193.6.128.38 &= 11000001.00000110.10000000.00100110 \\ \text{M} &= 255.255.255.128 &= 11111111.11111111.11111111.10000000 \text{ (25 bit prefix)} \\ \text{N} = \text{IP} \wedge \text{M} &= 193.6.128.0 &= 11000001.00000110.10000000.00000000 \\ \text{H} = \text{IP} - \text{N} &= 0.0.0.38 &= 00000000.00000000.00000000.00100110 \\ \text{Bcast} &= 193.6.128.127 &= 11000001.00000110.10000000.01111111 \end{aligned}$$

Kiosztható IP címek darabszáma: $\text{Bcast} - \text{N} - 1 = 193.6.128.127 - 193.6.128.0 - 1 = 126$

Kiosztható IP címek a tartományban (hálózatban): 193.6.128.1 ... 193.6.128.126

Jelen esetben a tartományból már egy cím (193.6.128.38/25) az IP géphez van rendelve.

2. IP címzési rendszer

IP címosztályok:

1 7 24

A osztály:

0	Network #	Host #
---	-----------	--------

1 1 14 16

B osztály:

1	0	Network #	Host #
---	---	-----------	--------

1 1 1 21 8

C osztály:

1	1	0	Network #	Host #
---	---	---	-----------	--------

- Osztályozási (első bájt) szabály:

Osztály	Kezdőbit(ek)	1. Bájt értéke	Prefix	Hálózat	Bcast	N számossága	H számossága
A	0	0 - 127	/8	N.0.0.0	N.255.255.255	126 !!!	$256 * 256 * 256 - 2$
B	01	128 - 191	/16	N.N.0.0	N.N.255.255	$64 * 256$	$256 * 256 - 2$
C	110	192 - 223	/24	N.N.N.0	N.N.N.255	$32 * 256 * 256$	$256 - 2$

3. IP vezérlő mechanizmusa (ICMP)

Általános megfontolások:

- Az IP datagram továbbítása nem megbízható.
- Bármikor felléphet az útvonal mentén torlódás vagy szakadás.
- Különböző IP datagramok különböző utakon továbbíthatnak a forrás és cél között.
- A különböző üzenetszórási tartományok egymástól eltérő MTU-val dolgozhatnak.
- A forrás IP csomópontot értesíteni kell az útvonal mentén bekövetkezett problémákról.

ICMP mechanizmus (Internet Control Message Protocol):

- Az ICMP IP-re épülő (logikailag felsőbb szintű) protokoll, de funkciója miatt a hálózati réteghez soroljuk.
- Célja: IP datagramok továbbítása során előforduló problémák (hibák) jelzése, jelzőüzenetek küldése.
- Az IP-vel együtt létezik és működéséhez elengedhetetlenül szükséges.
- Az IP fejrész protokoll típus mező értéke: 1
- ICMP üzenetek (továbbítási) hibáira nem generálunk ICMP üzenetet.

3. IP vezérlő mechanizmusa (ICMP)

ICMP csomag szerkezete:

Típus	Kód	Ellenőrző összeg
Típus specifikus adat		

- Típus: az üzenet „oka”:
 - *Destination unreachable*
 - *Redirect*
 - *Time exceeded*
 - *Echo request*
 - *Echo reply*
- Kód: a típushoz tartozó kiegészítő kód, pl.: *Destination unreachable típus esetén*
 - *Network unreachable*
 - *Host unreachable*
 - *Fragmentation needed and DF set*
- Adat: Tipikusan címezési (és egyéb) információk az üzenettel kapcsolatosan

3. IP vezérlő mechanizmusa (ICMP)

ICMP mechanizmus működési példák:

3.1) Útvonal menti MTU meghatározása:

- Forrás IP csomópont 1500 B méretű IP csomagot próbál küldeni a cél IP csomópontnak, de az IP csomag fejrészében (2. szó) DF = 1.
- Ha az útvonal mentén bármely üzenetszórási tartományban (link-en) $MTU < 1500$, akkor az adott router ICMP üzenetet küld a forrás IP címre: „*Fragmentation needed and DF set*” jelentéssel.
- A forrás IP host csökkenti lépcsőzetesen az IP csomag méretét addig, amíg a legszűkebb link-en is átfér az IP csomag.

3.2) Útvonal feltérképezése forrás és cél között (traceroute):

- Forrás IP csomagot küld a célnak, az IP csomag fejrészében (3. szó) TTL = 1.
- Az első router visszajelez „*ICMP Time Exceeded*” jelentéssel.
- A forrás feljegyzi az első router IP címét.
- Forrás egyesével növeli a TTL értéket és ismétli az IP csomagok küldését ugyanarra a célcímre, miközben tanulja a következő router IP címét.
- Addig ismétli a folyamatot, amíg a cél IP címről jön vissza az IP válasz.

4. IP forgalomirányítási alapok (routing)

Alapfogalmak:

- **Forgalomirányítás (routing):** Csomagok (IP datagramok) továbbítási irányának meghatározásával kapcsolatos döntések meghozatala. Ez megvalósul host (saját csomagok) és router (saját ÉS mástól származó csomagok) szinten is.
- **Forgalomirányítási táblázat (routing table):** A forgalomirányításhoz szükséges információkat tartalmazó táblázat. Tipikus (legfontosabb) mezők:

Célhálózat	Netmask	Kimenő interfész	Következő csomópont (next hop)	Metrika
------------	---------	------------------	--------------------------------	---------

- Hálózati protokollok típusai forgalomirányítás szerint:
 - **Forgalomirányított protokoll (routed protocol):** Hálózati réteghez kötődő, host-ok közötti általános protokoll, melynek csomagjait a forgalomirányító (router) irányítja és továbbítja
Pl: IP, IPX, AppleTalk, Banyan Vines, ISO CLNS, Apollo Domain, XNS, DECNet.
 - **Forgalomirányítási protokoll (routing protocol):** A forgalomirányítási táblázat(ok) felépítéséhez szükséges információkat (routerek közötti cseréjét) továbbító protokoll (pl. RIP, OSPF, BGP).
 - **Egyéb protokoll:** Az előzőekhez nem sorolható hálózati protokoll (pl. ICMP).

4. IP forgalomirányítási alapok (routing)

Forgalomirányítás (alapvető) működése:

- Csomópont a csomag célcímét illeszti a routing tábla soraira.
- Ha a célcím több sorra illeszkedik, akkor a leghosszabb prefixű sort tekinti illeszkedőnek.
- Ha nem létezik illeszkedő sor, akkor a cél elérhetetlen, a csomag nem továbbítható.
- Ha létezik illeszkedő sor, akkor a csomagot az ebben szereplő kimeneti interfészen továbbítja (adatkapcsolati keretben).

A) Host szintű forgalomirányítás:

- Csak saját forráscímű csomagot küld.
- Üzenetszórási tartományon belül keretben küldi közvetlenül a célnak a csomagot.
- Üzenetszórási tartományon kívülre keretben küldi az illeszkedő útválasztónak (hop).

B) Útválasztó (router) szintű forgalomirányítás:

- Idegen ÉS saját forráscímű csomagot kezel.
- Üzenetszórási tartományon belül: a csomagot keretben küldi közvetlenül a célnak.
- Üzenetszórási tartományon kívülre: a csomagot keretben küldi a következő illeszkedő útválasztónak (hop).

4. IP forgalomirányítási alapok (routing)

Forgalomirányítás (alapvető) működése (folyt.):

IP célcím illesztési algoritmus:

1. A routing tábla sorait prefix hossz szerint csökkenő sorrendbe rendezi. $N = 1$. Ezzel biztosítja, hogy több illeszkedő sor esetén a leghosszabb prefixút fogja eredményként kapni.
2. Ha nem létezik a táblázatban az N . sor, akkor nincs illeszkedő sor, és vége.
3. A csomag célcíme és az N . sor hálózati maszkja között bitenkénti AND műveletet hajt végre.
4. Ha a bitenkénti AND művelet eredménye megegyezik az N . sor célhálózat értékével, akkor a cím az N . sorra illeszkedik és vége.
5. $N := N + 1$; folytatja a 2. pontnál.

5. IP alhálózatok és aggregált hálózatok

Megfontolások:

- Az Internet felhasználói szervezetek (cégek, intézmények) a logikai működésük, vagy térbeli elhelyezkedésük alapján kisebb (azonos méretű) részekre oszthatják az IP címtartományukat.
- A felosztás eredményeként kisebb, könnyebben kezelhető üzenetszórási tartományok alakulnak ki.

Alapfogalmak:

Alhálózat (SN: subnet): Az osztályos IP cím host részének legmagasabb helyiértékű bitjeiből k darabot az alhálózat azonosítására csoportosítunk át. Az új network-host azonosító határvonal pozícióját $(N \mid SN \mid H)$ a hálózati maszk jelöli.

Aggregált hálózat (SN: supernet): 2^k darab osztályos IP hálózatot egyetlen csoportban kezelünk. Az IP cím network részének legalacsonyabb k bitje a host rész legmagasabb helyiértékű bitjei elé kerül. Az új hálózat-host azonosító határvonal pozícióját $(N \mid SN \mid H)$ a hálózati maszk jelöli.

5. IP alhálózatok és aggregált hálózatok

5.1. Alhálózat (subnet) példa:

Feladat: Legyen a 197.45.112.0/24 osztályos címtartomány. Alakítsunk ki nyolc darab azonos méretű alhálózatot!

Megoldás:

- Eredeti hálózat jellemzői:

$$N = 197.45.112.0 = 11000101.00101101.01101100.00000000$$

$$M = 255.255.255.0 = 11111111.11111111.11111111.00000000 = /24$$

- Nyolc alhálózathoz három SN bit szükséges, ezért:

$$M' = 255.255.255.224 = 11111111.11111111.11111111.11100000 = /27$$

- Alhálózati azonosítók: $SN_0 = 000$, $SN_1 = 001$, ..., $SN_6 = 110$, $SN_7 = 111$

SN (Dec)	Alhálózati cím	Pre- fix	Bcast	H' számossága	SN (Dec)	Alhálózati cím	Pre- fix	Bcast	H' számossága
0	197.45.112.0	/27	197.45.112.31	$2^5 - 2 = 30$	4	197.45.112.128	/27	197.45.112.159	$2^5 - 2 = 30$
1	197.45.112.32	/27	197.45.112.63	$2^5 - 2 = 30$	5	197.45.112.160	/27	197.45.112.191	$2^5 - 2 = 30$
2	197.45.112.64	/27	197.45.112.95	$2^5 - 2 = 30$	6	197.45.112.192	/27	197.45.112.223	$2^5 - 2 = 30$
3	197.45.112.96	/27	197.45.112.127	$2^5 - 2 = 30$	7	197.45.112.224	/27	197.45.112.255	$2^5 - 2 = 30$

5. IP alhálózatok és aggregált hálózatok

5.2. Aggregált hálózat (supernet) példa:

Feladat: Legyen négy darab szomszédos osztályos hálózat az alábbiak szerint: 197.45.112.0/24, 197.45.113.0/24, 197.45.114.0/27, 197.45.115.0/24. Alakítsunk ki egyetlen supernet hálózatot!

Megoldás:

- Eredeti hálózatok jellemzői:

$$N_0 = 197.45.112.0 = 11000101.00101101.011011\mathbf{00}.00000000$$

$$N_1 = 197.45.113.0 = 11000101.00101101.011011\mathbf{01}.00000000$$

$$N_2 = 197.45.114.0 = 11000101.00101101.011011\mathbf{10}.00000000$$

$$N_3 = 197.45.115.0 = 11000101.00101101.011011\mathbf{11}.00000000$$

$$M = 255.255.255.0 = 11111111.11111111.111111\mathbf{11}.00000000 = /24$$

- Négy szomszédos hálózat különböző bitjeinek száma: 2, vagyis SN = 2, ezért:

$$M' = 255.255.252.0 = 11111111.11111111.111111\mathbf{00}.00000000 = /22$$

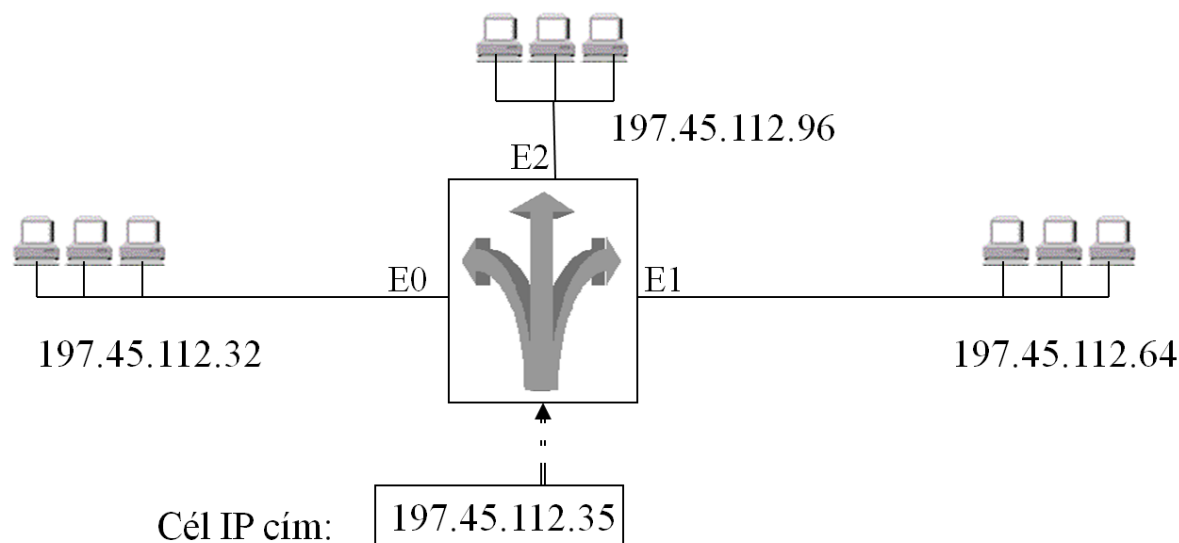
- Aggregált (supernet) hálózat:

SN (Dec)	Supernet cím	Prefix	Bcast	H' számossága
0	197.45.112.0	/22	197.45.115.255	$2^{10} - 2 = 1022$

5. IP alhálózatok és aggregált hálózatok

5.3. Forgalomirányítás azonos méretű alhálózatok között (példa):

Feladat: Legyen a 197.45.112.0/24 osztályos címtartomány nyolc azonos méretű alhálózata. Készítsük el az Internethez, valamint az SN_1 , SN_2 , SN_3 subnet-ekhez közvetlenül kapcsolódó útválasztó forgalomirányítási tábláját és magyarázzuk az N_1 alhálózatba címzett csomag irányítási folyamatát!

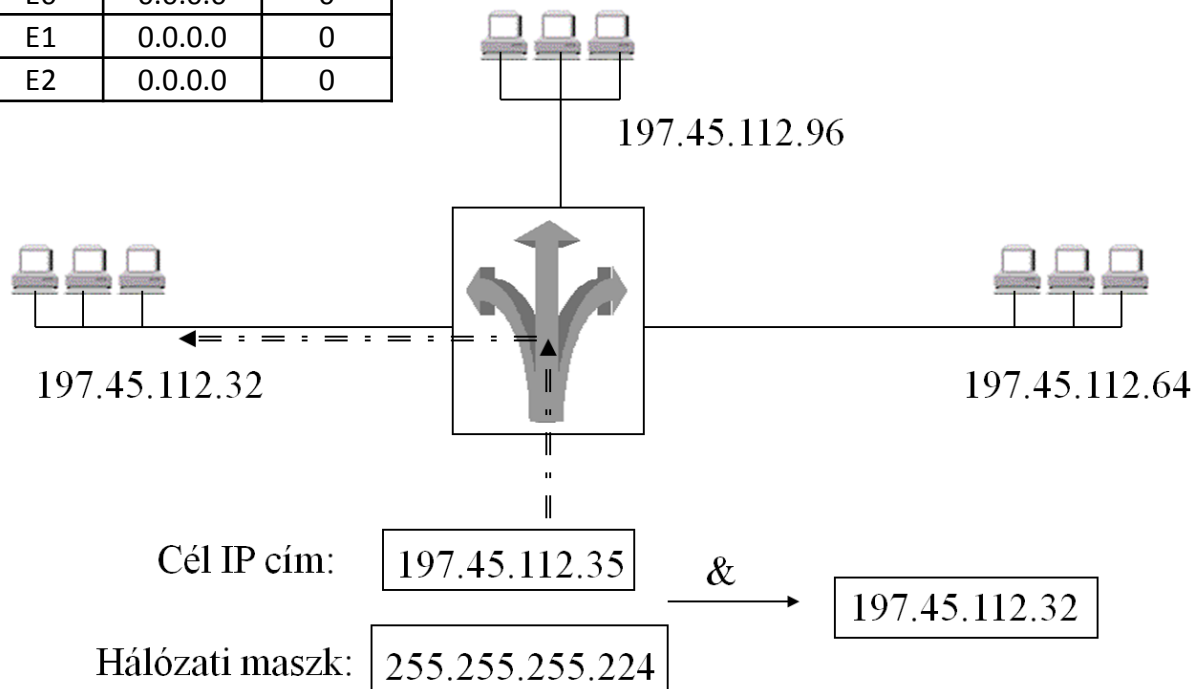


5. IP alhálózatok és aggregált hálózatok

5.3. Forgalomirányítás azonos méretű alhálózatok között (példa):

Megoldás: (Az IP alhálózatok az 5.1 példa szerintiek)

Célhálózat	Netmask	Interfész	Next-hop	Metrika
197.45.112.32	255.255.255.224	E0	0.0.0.0	0
197.45.112.64	255.255.255.224	E1	0.0.0.0	0
197.45.112.96	255.255.255.224	E2	0.0.0.0	0



5. IP alhálózatok és aggregált hálózatok

Forgalomirányítás osztály nélküli hálózatok között (CIDR):

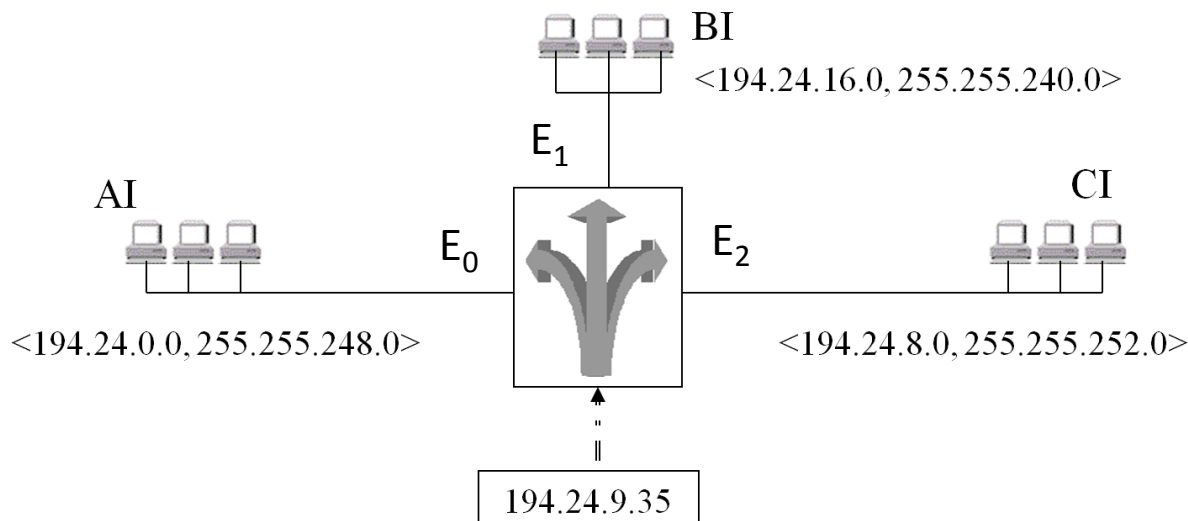
- CIDR: Classless Inter-Domain Routing
- A hálózat-host határvonal pozíció nem osztály, hanem az igényelt csomópont-darabszám alapján kerül meghatározásra.
- A hálózat-host határvonal pozíció jelzésére kötelező a prefix hossz, vagy a hálózati maszk megadása.
- Egy adott tartományon kívül eső hálózatokra vonatkozóan elegendő összegző (aggregált) irányítási információ tárolása, mivel a távoli címzési zóna részletinformációit nem szükséges ismerni.
- Az irányítási táblák növekedési problémáinak kezelésére földrajzi elhelyezkedés szerint címtartomány-zónákat alakítottak ki (RFC 1366, 1466):

Kontinens	Címtartomány
Európa	194.0.0.0 - 195.255.255.255
Észak-Amerika	198.0.0.0 - 199.255.255.255
Közép- és Dél-Amerika	200.0.0.0 - 201.255.255.255
Ázsia és Ausztrália	202.0.0.0 - 203.255.255.255

5. IP alhálózatok és aggregált hálózatok

5.4. Forgalomirányítás különböző méretű hálózatok között (példa):

Feladat: Legyen három, AI, BI, CI intézmény az ábra szerinti IP hálózati felosztással. Magyarázza az Internet szolgáltató (ISP) útválasztójának tevékenységét az IP csomag irányítása során!



5. IP alhálózatok és aggregált hálózatok

5.4. Forgalomirányítás különböző méretű hálózatok között (példa):

Megoldás:

Intézmény	Célhálózat	Netmask	Interfész	Next-hop	Metrika
AI	194.24.0.0	255.255.248.0	E0	0.0.0.0	0
BI	194.24.16.0	255.255.240.0	E1	0.0.0.0	0
CI	194.24.8.0	255.255.252.0	E2	0.0.0.0	0

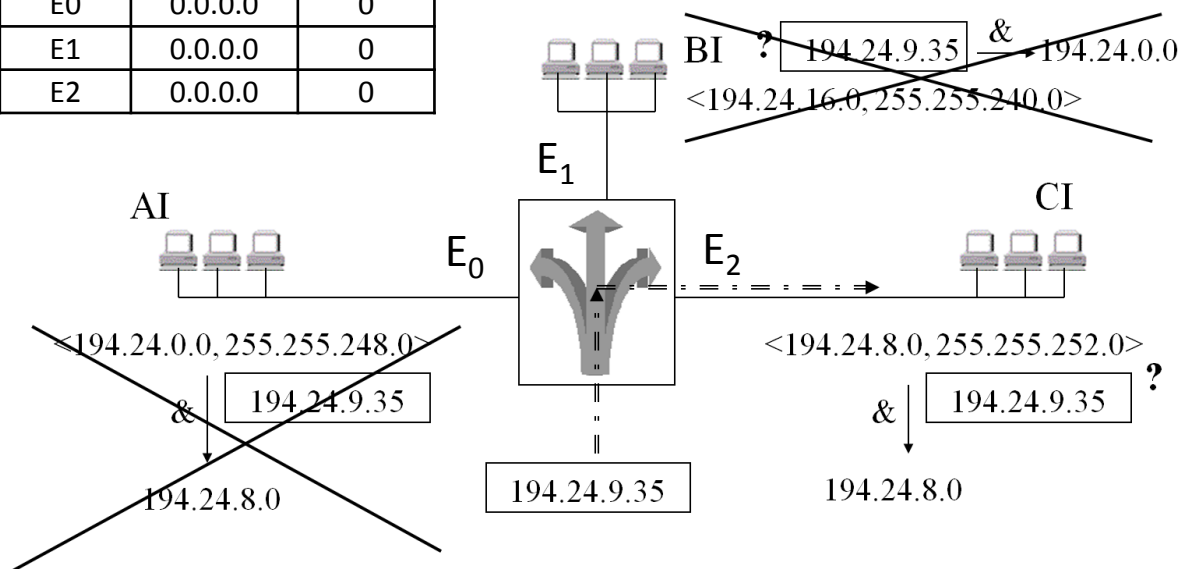
Cél IP cím = 194.24.9.35

Műveletek:

$IP \wedge M_{AI} = 194.24.8.0 \neq 194.24.0.0 = N_{AI}$ ezért IP csomag nem távozik E_0 interfészen.

$IP \wedge M_{BI} = 194.24.0.0 \neq 194.24.16.0 = N_{BI}$ ezért IP csomag nem távozik E_1 interfészen.

$IP \wedge M_{CI} = 194.24.8.0 = 194.24.8.0 = N_{CI}$ ezért IP csomag E_2 interfészen távozik.



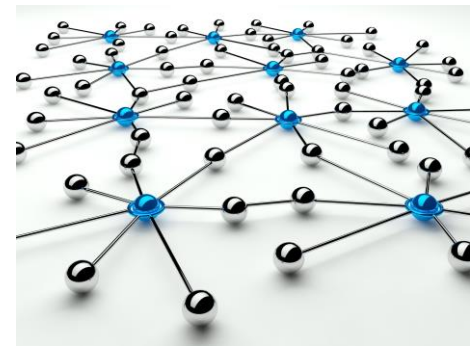
Hálózati architektúrák és protokollok

6. IP CÍMKONVERZIÓS MEGOLDÁSOK, IPv6 ALAPOK

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Hálózati címcseré (NAT)
- 2) Hálózati portcím csere (PAT)
- 3) Hálózati címből fizikai cím meghatározása (ARP)
- 4) Fizikai címből hálózati cím meghatározása
RARP, BOOTP, DHCP
- 5) Csomag felépítése és címzés IPv6 esetén

1. Hálózati címcseré (NAT)

Megfontolások:

- Az IPv4 címtartomány mérete ma már nem elégséges a jelenlegi Internet összes csomópontjának egyedi címzéséhez.
- A csomópontok jelentős része csak kiszolgálást kér (kliens), nem szolgáltat (szerver).

NAT alapfogalmak:

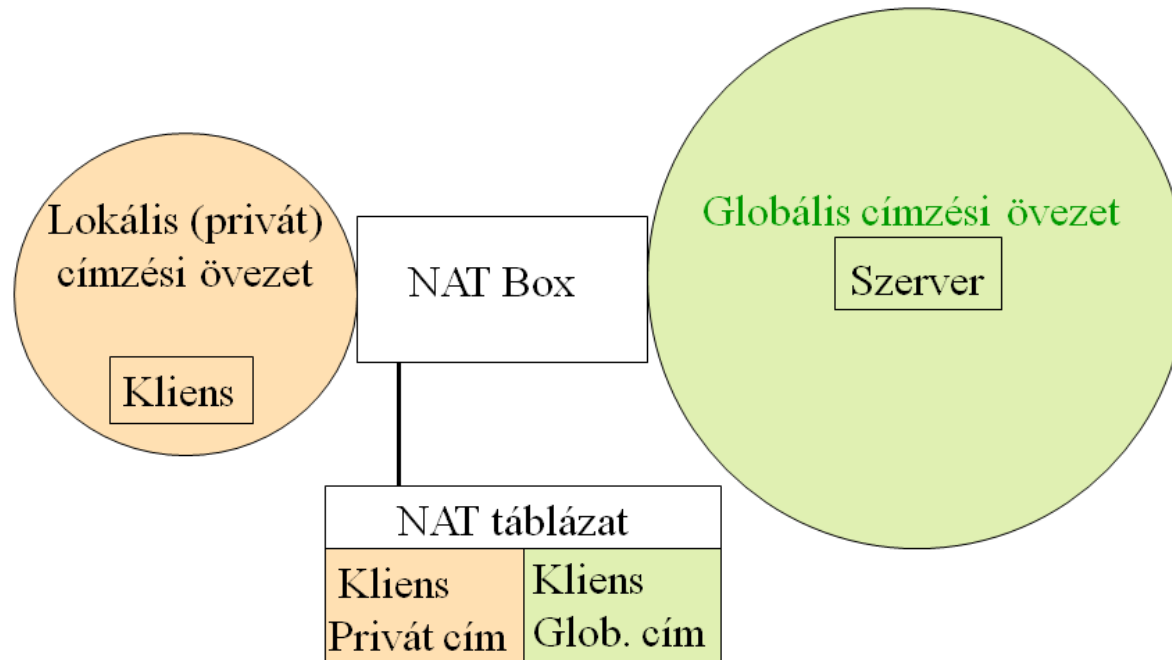
- **Címzési övezet (Address Realm):** Az a hálózatrész, amelyben biztosítani kell az IP-címek egyediségét.
- **Külső hálózat (Public/Global/External Network):** Az IANA által kezelt címtartománnyal rendelkező címzési övezet. A külső, globális hálózatban használatos címek a teljes Internetre vonatkozóan egyediek.
- **Belső hálózat (Private/Local Network):** Előfizető cég saját (belső, privát) címzéssel rendelkező címzési övezete.
- **Privát címtartomány (RFC 1918):** A belső hálózatban használt címek, amelyhez tartozó csomagokat a szolgáltatói routerek nem irányítják. A privát címek a világon nem egyediek, mert másik cég belső hálózatában ismételten megjelenhetnek.

Osztály	Privát címtartomány	Megjegyzés
A	10.0.0.0/8	Hálózat
B	172.16.0.0/12	Aggregált hálózat (supernet)
C	192.168.0.0/16	Aggregált hálózat (supernet)

1. Hálózati címcseré (NAT)

NAT működési mechanizmus:

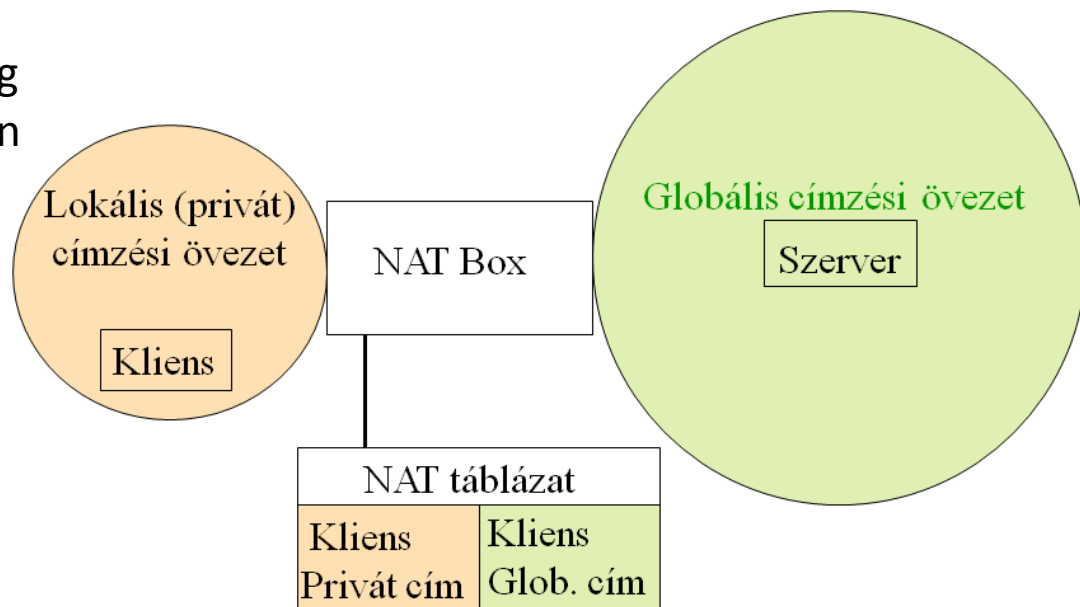
- Kliens (esetleg belső szerver) csomópont: helye a belső (lokális) hálózat, privát IP címmel.
- Külső szerver csomópont: helye a külső, globális hálózat, publikus IP címmel.
- A címzési övezet határán egy speciális eszköz, a címcserélő (NAT-Box) biztosítja, hogy (bizonyos korlátoktól eltekintve) valamennyi applikáció számára a szolgáltatások elérhetőek legyenek.



1. Hálózati címcseré (NAT)

A klasszikus IP címcseré (Basic NAT):

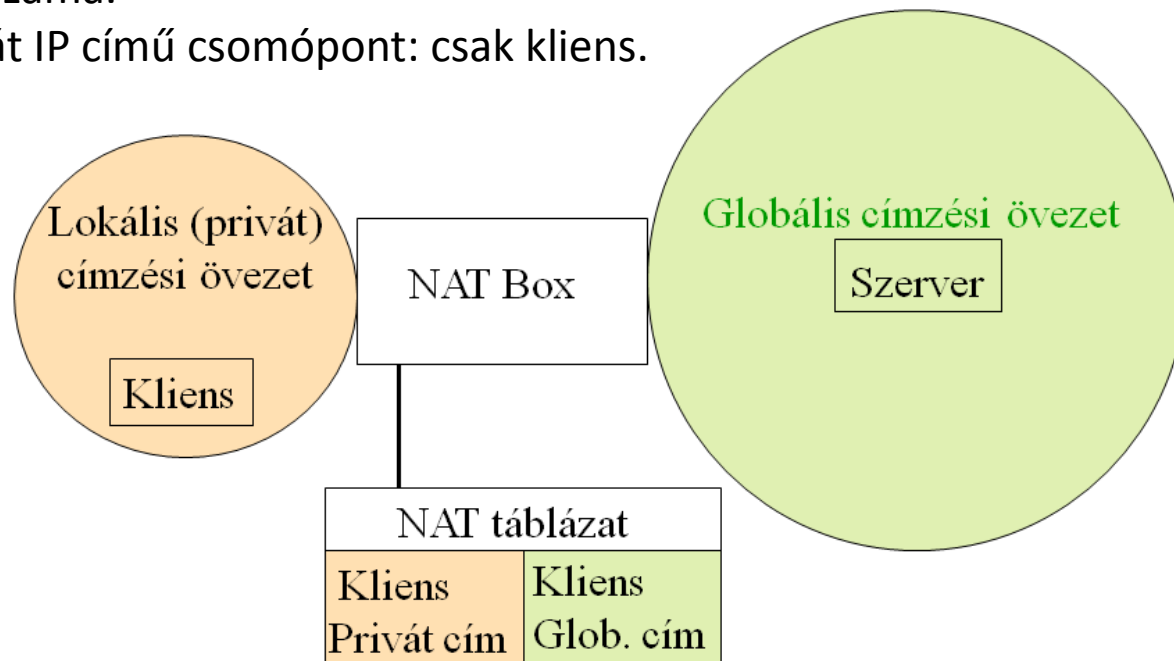
- Az első IP csomagot a kliens küldi a szerver felé, a csomagban célcímként a szerver globális IP címe, feladó címként pedig a kliens privát IP címe szerepel.
- Az IP csomag a belső hálózat forgalomirányítása alapján a két címzési övezet határához (a címcserélőhöz, Nat-Boksz-hoz) jut.
- A NAT-Box az IP csomag forrás címmezőjében privát $\leftrightarrow$ publikus címcserét végez, és ezzel a feladócímmel továbbítja a csomagot külső hálózati szerver felé.
- A Nat-Box NAT táblázatban (címcserélő, címfordító, címtranszlációs tábla) feljegyzí a címcserét.
- A szervertől érkező válasz IP csomag célcímét a Nat-Boksz a NAT táblában megtalálja és publikus $\leftrightarrow$ privát IP címcserét végez, majd az így előállított csomagot továbbítja a belső hálózaton a kliens felé.



1. Hálózati címcseré (NAT)

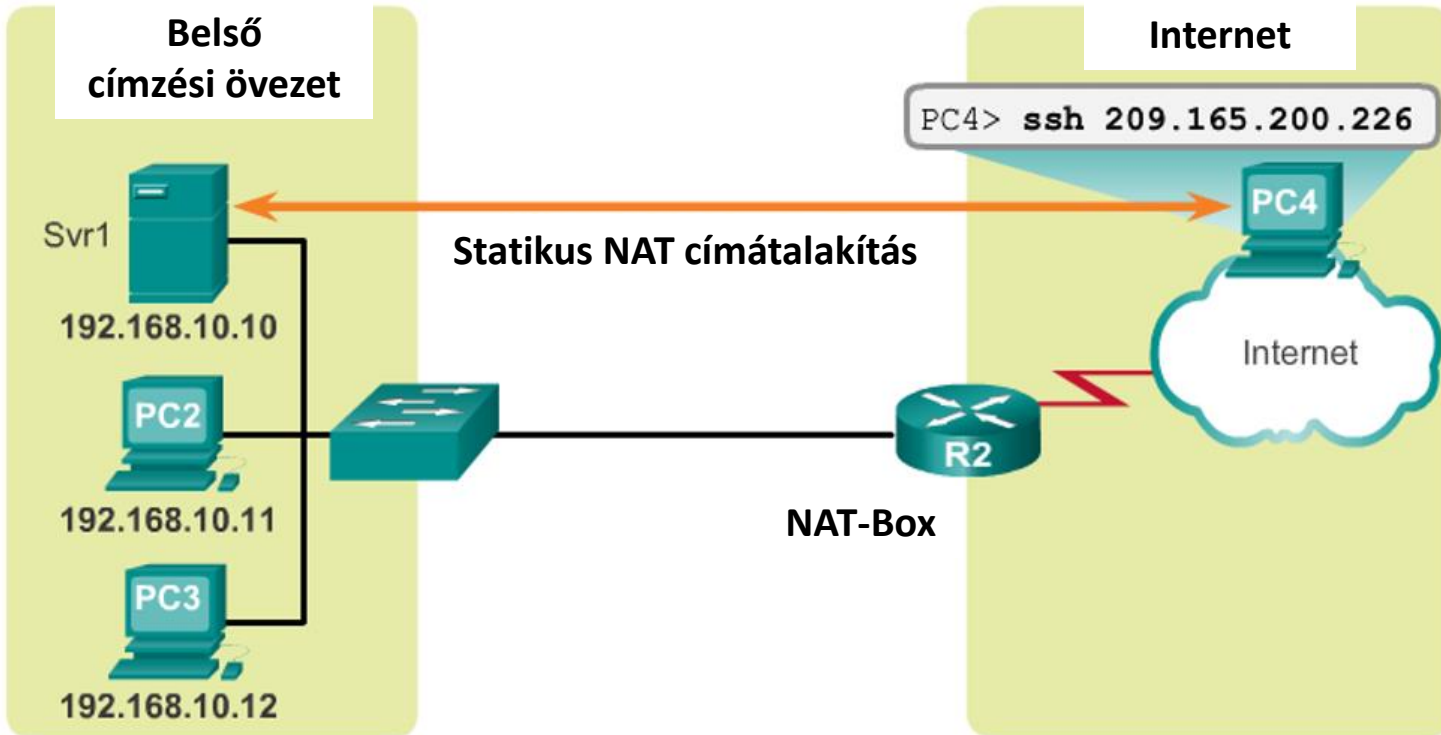
NAT típusok:

- Statikus NAT: n db lokális IP cím $\leftrightarrow$ n globális IP cím rögzített összerendelése
 - Privát IP című csomópont: kliens vagy szerver.
- Dinamikus NAT: n db lokális IP cím $\leftrightarrow$ m db globális IP cím változó összerendelése ($n \geq m$).
 - n : privát IP című csomópontok maximális száma.
 - m : publikus IP című gépek száma = szimultán viszonyban lévő belső csomópontok száma.
 - Privát IP című csomópont: csak kliens.



1. Hálózati címcseré (NAT)

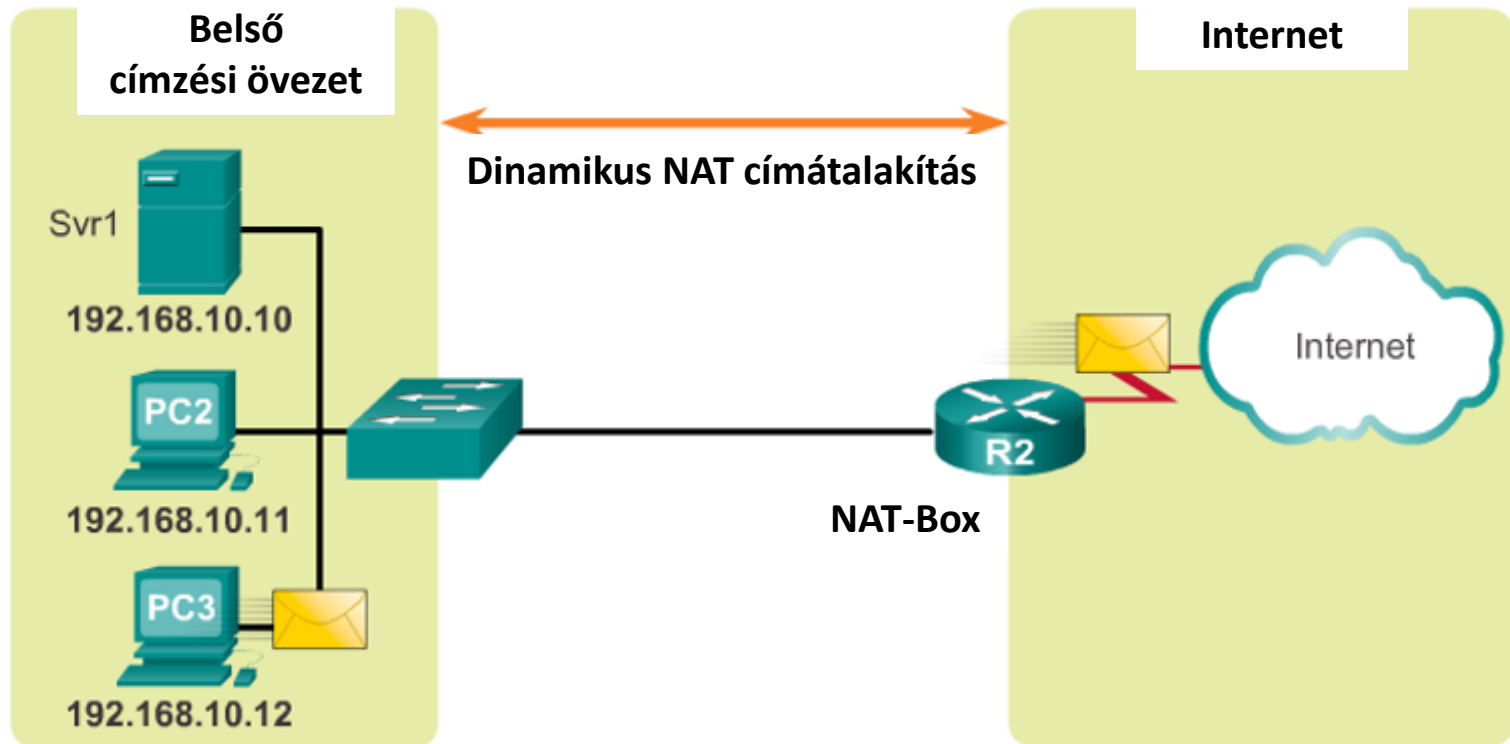
Példa statikus NAT címátalakításra:



R2 statikus NAT tábla	Belső lokális IP cím	Belső globális IP cím
Gép 1	192.168.10.10	209.165.200.226
Gép 2	192.168.10.11	209.165.200.227
Gép 3	192.168.10.12	209.165.200.228

1. Hálózati címcseré (NAT)

Példa dinamikus NAT címtálcakításra:



R2 dinamikus NAT lista	Belső lokális IP cím	Belső globális IP cím
Aktív kliens 1	192.168.10.12	209.165.200.226
Passzív kliens i	Rendelkezésre áll	209.165.200.227
Passzív kliens j	Rendelkezésre áll	209.165.200.228
Passzív kliens k	Rendelkezésre áll	209.165.200.229

2. Hálózati portcím csere (PAT)

PAT működési mechanizmus:

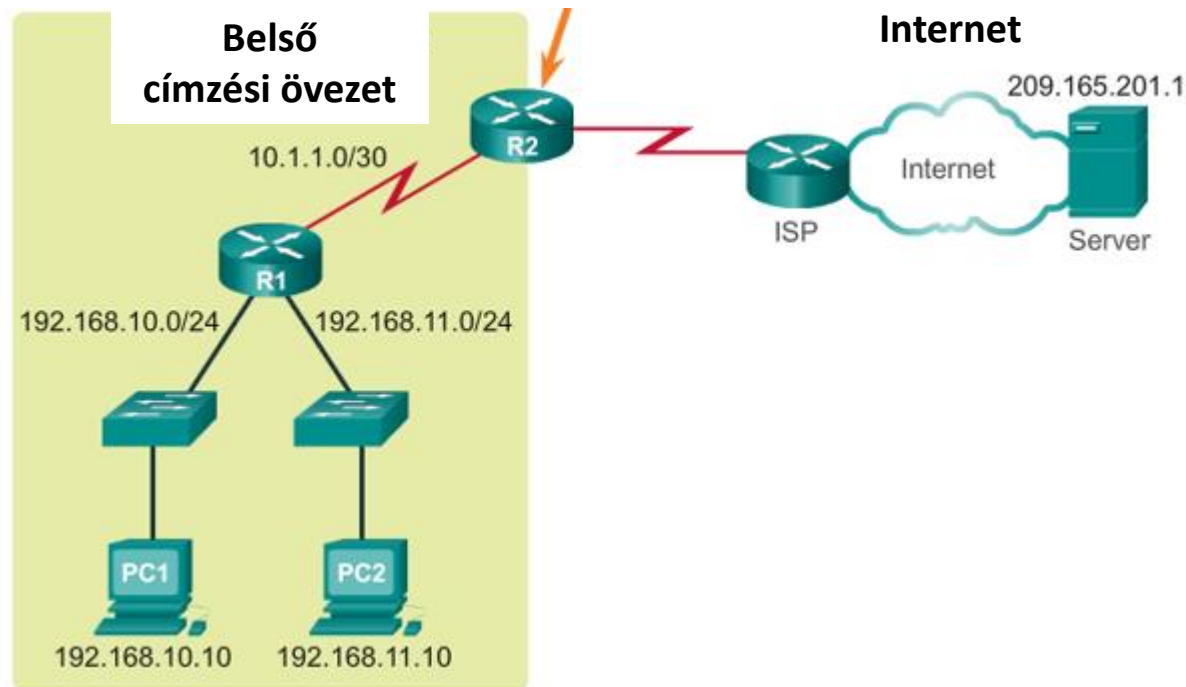
- Kliens csomópont: helye a belső (lokális) hálózat, privát IP címmel.
- Szerver csomópont: helye a külső, globális hálózat, publikus IP címmel.
- A belső és külső hálózat közötti NAT-Box L3 és L4 szinteken egyszerre végez címcserét (NAT overload):
 - $(IP_L, Port_L) \leftrightarrow (IP_G, Port_G)$
- Képes olyan protokoll számára is címcserét is végezni, amely nem használ port címet (pl. ICMP).
- Speciális tulajdonság: hálózati biztonság funkció.

NAT/PAT erőforrásigénye:

- Több processzálas szükséges, mint a klasszikus routing esetén:
 - Keresés a címtranszformációs táblázatban.
 - Címcseré / címcseré és portszám csere.
 - Ellenőrző összegek újraszámítása.
- Gyorsítási lehetőségek az ellenőrző összegek újraszámításánál:
 - Az eredeti ellenőrző összegből a régi cím „kivonása”.
 - A kapott eredményhez az új cím „hozzáadása”.

2. Hálózati portcím csere (PAT)

Példa PAT címtalakításra:



R2 NAT tábla	Kliens		Szerver	
	Belső lokális <IP, Port> cím	Belső globális <IP, Port> cím	Külső lokális <IP, Port> cím	Külső globális <IP, Port> cím
Viszony 1	192.168.10.10:1440	209.165.200.226:1440	209.165.201.1:80	209.165.201.1:80
Viszony 2	192.168.10.10:2222	209.165.200.226:2222	209.165.201.1:80	209.165.201.1:80
Viszony 3	192.168.11.10:2222	209.165.200.226:3333	209.165.201.1:23	209.165.201.1:23

3. Hálózati címből fizikai cím meghatározása (ARP)

Megfontolások:

- A forrás csomópont adatkapcsolati szinten a keret fejrésében fizikai címazonosítókat helyez el, amihez tudnia kell a **cél hálózati cím** → **cél fizikai cím** összerendelést.
- Ezt az információt a forrásnak lokálisan kell tárolnia.

ARP (Address Resolution Protocol) működése:

- 1) ARP kérdés küldése mindegyik csomópontnak az üzenetszórási tartományon belül:
Ki tudja az X hálózati cím fizikai címét?
- 2) Az üzenetszórási tartomány valamennyi csomópontja megkapja és feldolgozza a kérdést.
- 3) Csak az a csomópont válaszol egyes (unicast) formában, amelynek logikai címe X.
- 4) Az ARP válasz csomagban a címösszerendelés szerepel:
X hálózati cím fizikai címe - MAC_X .

3. Hálózati címből fizikai cím meghatározása (ARP)

ARP csomag szerkezete:

Hardver típusa										L3 protokoll típusa									
Fiz. cím hossza					Hál. cím hossza					Művelet kód									
Feladó fizikai címe																			
Feladó fizikai címe										Feladó L3 címe									
Feladó L3 címe										Cél fizikai címe									
Cél fizikai címe																			
Cél L3 címe																			

Művelet kód	ARP Üzenet típus
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply
5	DRARP Request
6	DRARP Reply
7	DRARP Error
8	InARP Request
9	InARP Reply

- Szavak hossza: 32 bit

1. szó: Hardver (L2) típus, L3 protokoll típus

2. szó: L2/L3 címek hossza [B]

3-7. szó: L2/L3 címek értéke

- ARP csomag típusazonosító L2 szinten: 0x0806

Hardver típuskód	Hardver (L2) típusa
1	Ethernet (10 Mbps)
6	IEEE 802
15	Frame Relay
17	HDLC
18	Fibre Channel
19	ATM
20	Soros vonal

4. Fizikai címből hálózati cím meghatározása (RARP)

Megfontolások:

- A forrás csomópont hálózati szinten a csomag fejrészában logikai címazonosítókat helyez el, amihez tudnia kell a **saját fizikai cím → saját logikai cím** összerendelést.
- Ezt az információt a forrásnak lokálisan kell tárolnia.
- A logikai címinformációt hálózati szolgáltatásként dedikált szerver/szerverfarm biztosítja.

RARP (Reverse Address Resolution Protocol) működése:

- 1) RARP kérdés küldése mindegyik csomópontnak az üzenetszórési tartományon belül:
Ki tudja a MAC fizikai címhez tartozó hálózati címet?
- 2) Az üzenetszórési tartomány valamennyi csomópontja megkapja, de csak a RARP szerver/szerverfarm feldolgozza fel a kérdést.
- 3) Ha megtalálja valamelyik RARP szerver a táblázatában a MAC fizikai címet, akkor egyes (unicast) válasz érkezik a hálózati címmel a kérdezőhöz.
- 4) Több válasz esetén az időben első érvényes.

4. Fizikai címből hálózati cím meghatározása (RARP)

RARP csomag szerkezete:

Hardver típusa										L3 protokoll típusa									
Fiz. cím hossza					Hál. cím hossza					Művelet kód									
Feladó fizikai címe																			
Feladó fizikai címe										Feladó L3 címe									
Feladó L3 címe										Cél fizikai címe									
Cél fizikai címe																			
Cél L3 címe																			

Művelet kód	ARP Üzenet típus
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply
5	DRARP Request
6	DRARP Reply
7	DRARP Error
8	InARP Request
9	InARP Reply

- Szavak hossza: 32 bit

1. szó: Hardver (L2) típus, L3 protokoll típus

2. szó: L2/L3 címek hossza [B]

3-7. szó: L2/L3 címek értéke

- RARP csomag típusazonosító L2 szinten: 0x0806

Hardver típuskód	Hardver (L2) típusa
1	Ethernet (10 Mbps)
6	IEEE 802
15	Frame Relay
17	HDLC
18	Fibre Channel
19	ATM
20	Soros vonal

4. Fizikai címből hálózati cím meghatározása (BOOTP)

Megfontolások:

- Boot-olható szoftverrel lokálisan (HDD) nem rendelkező gép számára a hálózatnak kell az image fájlt szolgáltatni.
- A RARP csak egy üzenetszórési tartományon belül működik, ezért minden üzenetszórési tartományban RARP szervert kell üzemeltetni.
- Egy céges hálózatban sok üzenetszórési tartomány létezik: nehézkes lenne a sok RARP szerver szeparált üzemeltetése.
- Olyan megoldás szükséges, amely cég szinten bármely kliense számára egyben kezeli le a hálózatra kapcsolódás összes szükséges elemét:
 - Kliens hálózati paraméterek: IP cím, Maszk, alapértelmezett átjáró IP címe, DNS címe.
 - Kliens boot image: a boot fájlt (operációs rendszer) szolgáltató szerver IP címe.

BOOTP (BOOTstrap Protocol, RFC 951) működése:

- Szállítási rétegben működő mechanizmus (IP / UDP:67/68).
 - BOOTP Relay Agent: L3 ügynök szoftver (tipikusan a kliens útválasztójában).
- a) Ha kliens és a BOOTP szerver **azonos üzenetszórési tartományban** van:
- IP cím megszerzésének működési elve hasonló a RARP - nál ismertetettel.
 - Egyéb elemek megszerzése: saját IP cím birtokában interaktívan, szerverektől.

4. Fizikai címből hálózati cím meghatározása (BOOTP)

BOOTP (BOOTstrap Protocol, RFC 951) működése (folyt.):

- b) Ha kliens és a BOOTP szerver **különböző üzenetszórési tartományban** van:
- BOOTP Relay Agent: egyes (unicast) kérelem küldése BOOTP szerverhez.
 - Kliens kérdés csomagjában értékadások:
 - Forrás IP címmező := BOOTP RA IP címe.
 - Cél IP címmező := BOOTP szerver IP címe.
 - BOOTP szerver válaszában értékadások:
 - Keret célcím : = Kliens MAC címe.
- BOOTP RA által **statikusan** tárolt objektumok:
- BOOTP szerver IP címe.
 - Kliens MAC címe - BOOTP RA IP címe.
- Alkalmazott portazonosítók:
- Kliens: UDP(68)
 - Szerver: UDP(67)

4. Fizikai címből hálózati cím meghatározása (DHCP)

Megfontolások:

- BOOTP esetén MAC cím - IP cím összerendelés: csak statikus.
- A céges hálózatban kliensek hálózati elemekkel való kiszolgálási igénye:
 - Időben változó (dinamikus).
 - Az IP címelemek csak megújítható ideig legyenek használhatók (változás követése).
- A megoldás legyen visszafelé kompatibilis a BOOTP szolgáltatással: intelligencia és csomag formátum.

DHCP (Dynamic Host Configuration Protocol, RFC 1531) működése:

- 1) Broadcast DHCP kérdés: Ki tud adni egy IP címet? (DHCPDISCOVER).
- 2) Az üzenetszórási tartomány valamennyi csomópontja megkapja.
- 3) DHCP szerverek feldolgozzák a kérdést: Ha a kezelt címtartományukban még van szabad IP cím, akkor azzal megválaszolják a DHCP kérdést. (DHCPOFFER).
- 4) A kliens a hozzá érkező DHCP válaszokból választ egyet, s visszajelzi a választását a megfelelő DHCP szervernek. (DHCPREQUEST).
- 5) A DHCP szerver „könyveli” a címválasztást (foglalt lett a cím), s a könyvelésről megerősítést küld a kliensnek. (DHCPACK/DHCPNAK).

4. Fizikai címből hálózati cím meghatározása (DHCP)

DHCP csomag felépítése:

Op. kód	Hardver típusa	Fiz. cím hossza	Hop
Tranzakció azonosító			
Folyamat ideje (sec)	B	Nem használt (zéró)	
Kliens IP címe (DHCPREQUEST ell.)			
Kliens IP címe (DHCPOFFER)			
Szerver IP címe (DHCPOFFER, DHCPACK, DHCPNAK)			
DHCP Relay agent IP címe			
Kliens fizikai címe (16 byte)			
Szerver DNS neve (64), Boot file neve (128), Opciók(312)			

1. szó: Op. kód (kérelem/válasz/stb.), Hardver típusa (ld. RARP), Hop (IP TTL)

2. szó: Tranzakció azonosító

3. szó: Folyamat ideje [s], B: szerver válaszána típusát (unicast/broadcast) kéri a kliens

4. szó: Kliens IP címe (kérelemnél)

5. szó: Kliens IP címe (válasznál)

6. szó: DHCP szerver IP címe

7. szó: DHCP Relay IP címe

8. szó: Kliens fizikai címe

9-11 szó: DNS szerver neve, Boot fájl azonosító, Opciók

5. Csomag felépítése és címzés IPv6 esetén

Megfontolások:

- Az IPv4 címzési terület szűkössége fejlesztést igényelt.
- Az IP technológia irányába támasztott QoS elvárások erősödése 1990-től.

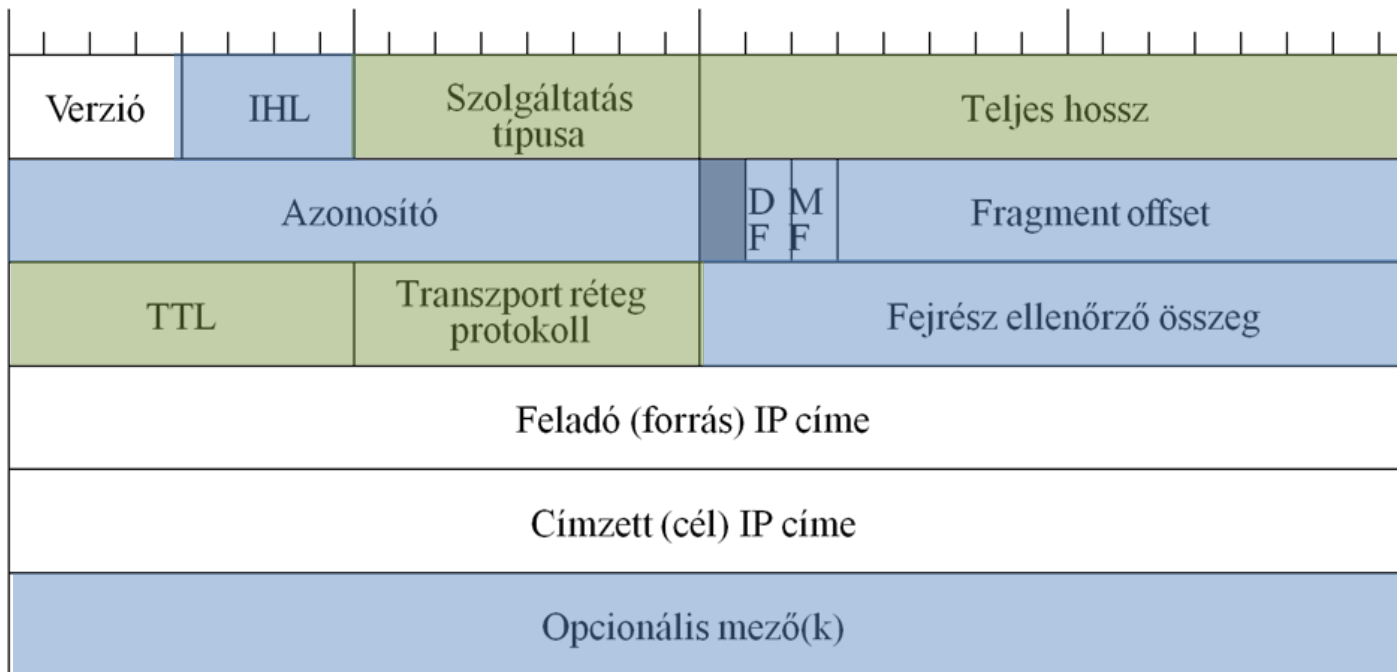
IPv6 tulajdonságok:

- Címzési tartomány: 128 bit (IPv4-nyi oldalhosszúságú kockarács mindegyik rácspontja egy-egy IPv4 halmaz).
- Intelligensebb csomagkezelés, mint IPv4 esetén.
- NAT igényének mellőzése (habár létezik NAT64 is).
- Egyszerűbb csomagfejrész, nincs hibaellenőrző kód:
 - Kevesebb számolás.
 - Gyorsabb útválasztás.
- Adatfolyam azonosító mező a csomag fejrészben:
 - Áramkörök egyszerűbb azonosítása.
- IPv4 és IPv6 együttműködés:
 - Kettős (duális) stack: mindkét protokoll párhuzamosan működik a csomóponton.
 - Alagút: IPv4 csomagban IPv6.
 - Címcseré (NAT64): átjárás IPv4 és IPv6 hálózatok között.

5. Csomag felépítése és címzés IPv6 esetén

IPv6 csomag felépítése:

- Fejrész (H) + Rakrész (P, max. 64 kB)
- IPv6 csomag fejrészének kialakítása: egyszerűsítés az IPv4-hez képest.



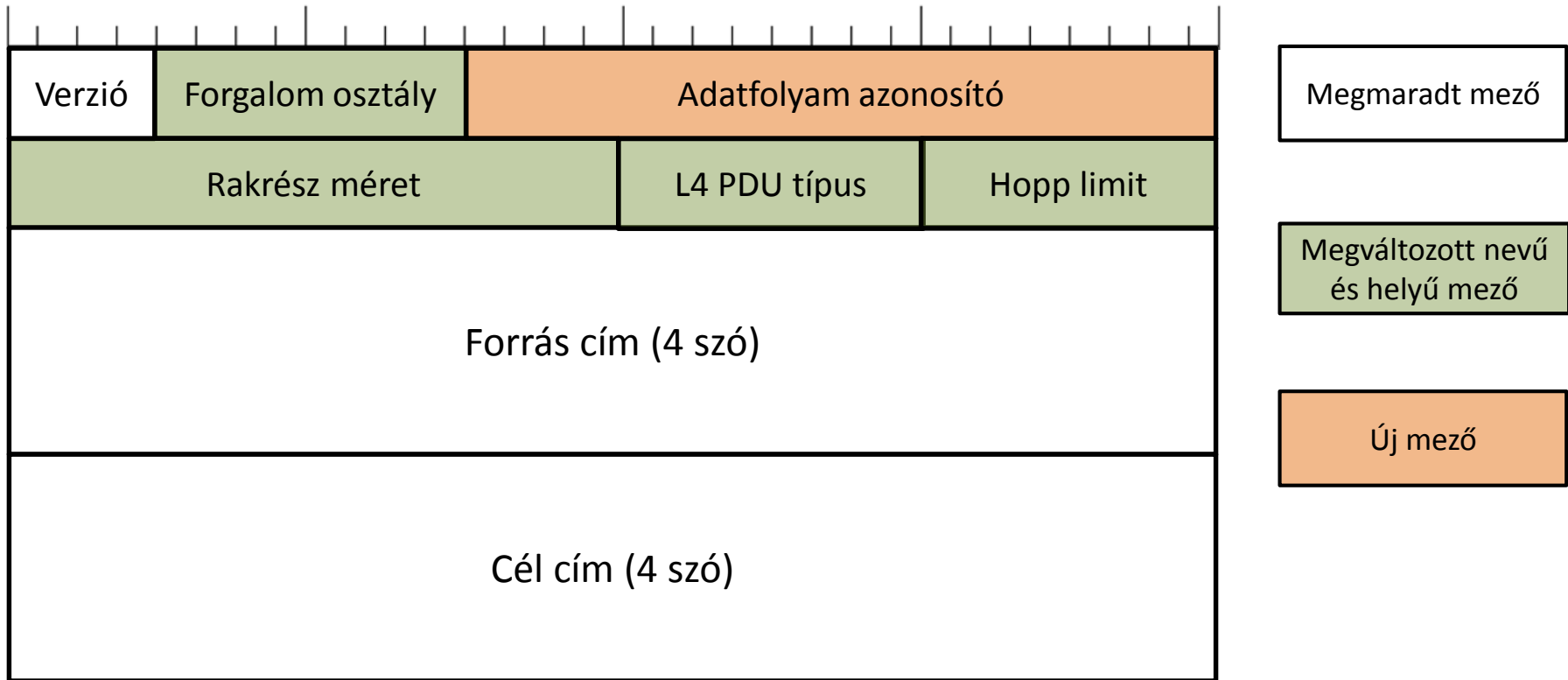
Megmaradt mező

Megváltozott nevű
és helyű mező

Megszűnt mező

5. Csomag felépítése és címzés IPv6 esetén

IPv6 csomag fejrészének felépítése:



- Forgalom osztály: Prioritás
- Adatfolyam azonosító: Azonos adatfolyam, azonos kezelési mód
- Hopp limit: Azonos az IPv4 TTL funkcióval

5. Csomag felépítése és címzés IPv6 esetén

IPv6 címek:

- Jelölés: 8 db hextet segítségével (16 bit)

Pl: AAAA:BBBB:CCCC:DDDD:AAAA:BBBB:CCCC:DDDD

- Jelölés egyszerűsítési szabályai:

1) Vezető 0-ák elhagyása:

Pl1: AAAA:0000:CCCC:0000:AAAA:0000:0000:DDDD

AAAA: 0:CCCC: 0:AAAA: 0: 0:DDDD

Pl2: AAAA:B000:0000:00DD:AAA0:0000:0000:00D0

AAAA:B000: 0 : DD:AAA0: 0: 0: D0

2) Egy darab nulla szegmens elhagyása:

Pl3: AAAA:0000:0000:0000:AAAA:0000:0000:DDDD

AAAA: :AAAA:0000:0000:DDDD = AAAA::AAAA:0:0:DDDD

Pl4: 0000:0000:0000:0000:0000:0000:0000:0000 = ::

5. Csomag felépítése és címzés IPv6 esetén

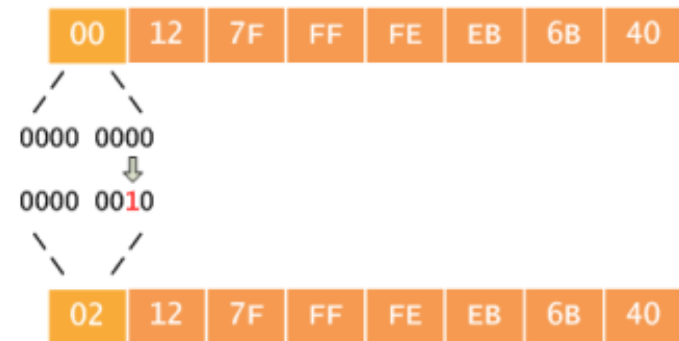
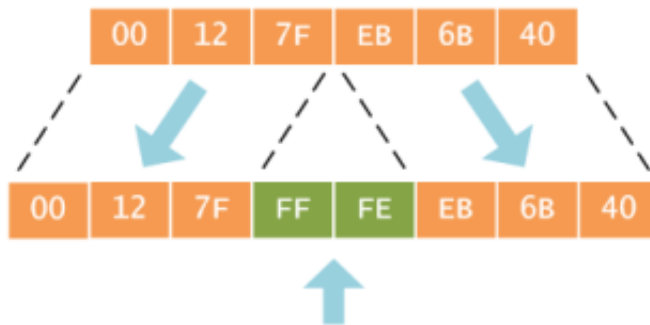
IPv6 címtípusok:

- Három címtípus: nincs üzenetszórás (broadcast).
 - Egyes (Unicast):
 - Globális egyes: 2000:: ... (4000:: - ::1) PI: 3FFF::10/64
 - Link-local: FE80::/10 PI: FE80::1/64
 - Loopback: ::1/128
 - Határozatlan: ::/128
 - Egyedi lokális: FC00::/7 ... FD::/7 PI: FCFF::F/7
 - Beágyazott IPv4 ::FFFF:/96 PI: ::ffff:192.1.56.10/96
 - Fenntartott: ::/8
 - Többes (Multicast): FF00::/8
 - Csoportazonosítók (IANA):
 - Link-local minden csomópont az üzenetszórási tartományban: FF02::1
 - Link-local minden router az üzenetszórási tartományban: FF02::2
 - Link-local minden router a telephelyen belül: FF02::3
 - Bármelyik a célok közül (Anycast):
 - Unicast, csak a használata eltér a szokásostól.
 - Ugyanaz a cím több interfészhez is hozzá van rendelve.
 - A routing mechanizmus dönt, hogy melyik címpéldányhoz küldi a csomagot.

5. Csomag felépítése és címzés IPv6 esetén

IPv6 címtípusok (folyt.):

- Prefix:
 - Tartomány: /0 ... /128
 - Tipikus hálózat: /64
 - Tipikus alhálózat: /48 és /64 közötti bitek
- Interfész azonosító generálás 48 bites MAC címből (EUI-64 szabály): 3 lépés
 1. MAC cím felezése OUI – DI határnál.
 2. 0xFFFFE beszúrása középre (6 bájtos azonosító).
 3. Első bájtban U/L (Universal/Local) jelzőbit (bit 7) komplementálása.



Indoklás:

- Lokálisan generált MAC cím: U/L = 1 → IPv6 interfésznél U/L = 0.
- Soros link, alagút vége esetén: ::2, ::3

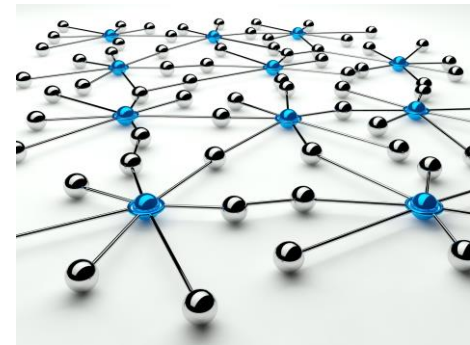
Hálózati architektúrák és protokollok

9. IP FORGALOMIRÁNYÍTÁS

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Útválasztás és forgalomirányítás osztályok
- 2) Távolságvektor alapú forgalomirányítás (DVR)
RIP, EIGRP
- 3) Link-állapot alapú forgalomirányítás (LSR)
IS-IS, OSPF
- 4) Vektor-állapot alapú forgalomirányítás (VSR)
BGP

1. Útválasztás és forgalomirányítás osztályok

Megfontolások:

- Útválasztás szükséges úgy a végpontokon, mint a köztes csomópontokon.
- Host csak saját csomagjai számára végez útválasztást.
- Útválasztó (router) idegen és saját csomagjai számára is végez útválasztást.
- Útválasztás szükséges eszköze a routing tábla, amibe bejegyzések kerülnek.
- Dinamikus routing üzenet hitelessége hálózatbiztonsági szempont.

Forgalomirányítási osztályok:

1) Minimális routing: Teljesen izolált, router nélküli megoldás.

2) Statikus routing: A forgalomirányítási táblázat manuális feltöltése a rendszergazda által.

Pl: default router (default gateway) beállítása, fix irány beállítása.

3) Dinamikus routing: A forgalomirányítási táblázat(ok) bejegyzéseit valamilyen routing protokoll végzi.

- **Belső forgalomirányítás:** Egy autonóm rendszeren belül a legelőnyösebb útvonal meghatározása speciális algoritmusokkal: távolságvektor vagy link-állapot alapon.

Pl.: RIP, EIGRP, OSPF, IS-IS

- **Külső forgalomirányítás:** Autonóm rendszerek közötti útvonal meghatározása útvonalvektor (üzemeltetési politika) alapján.

Pl.: BGP

1. Útválasztás és forgalomirányítás osztályok

Routing információ komponensek:

- A routing tábla bejegyzései: a távoli IP cím lehetséges elérési útjainak minősítése egyesével.

Célhálózat	Netmask	Kimenő interfész	Következő csomópont (Next Hop)	Metrika
------------	---------	------------------	--------------------------------	---------

- Az útvonalat jellemző metrika jellemzője:
 - Dimenziója: egy (skaláris érték) vagy több (összetett).
 - Hatásköre: egyetlen link vagy a teljes útvonal.
- A metrika lehetséges jelentése:
 - Hatékonyság
 - Minőség
 - Jóság
 - Megbízhatóság
 - Költség
 - Távolság
 - Átviteli ráta
 - Késletetési idő, stb.

2. Távolságvektor alapú forgalomirányítás (DVR)

Működési alapelv:

- Routing tábla egy-egy bejegyzése: adott elérhető célhoz a legjobb küldési irány.
- Elérhető cél: csomópont vagy hálózat.
- Metrika: távolság (távolságvektor).
- A szomszédos forgalomirányítók közötti párbeszéd: bejegyzésekről értesítés (update) küldése meghatározott időközönként.
- Routing update kiértékelése routerben: legjobb út módosítása, ha létezik még jobb új út.

Távolságvektor alapú forgalomirányítás algoritmus (Bellman-Ford):

- Közvetlen távolság i és j csomópontok között: $d(i, j)$

$$d(i, j) = \begin{cases} \text{a hálózat használati költsége, ha } i \text{ és } j \text{ egy hálózatban vannak,} \\ \infty, \text{ egyébként.} \end{cases}$$

- Legrövidebb út i és j csomópontok között: $D(i, j)$

$$D(i, j) = \begin{cases} 0, \text{ ha } i = j, \\ \min_k \{d(i, k) + D(k, j)\}, \text{ egyébként.} \end{cases}$$

ahol k : i szomszédjai

2. Távolságvektor alapú forgalomirányítás (DVR)

Távolságvektor alapú forgalomirányítás algoritmus (Bellman-Ford, folyt.):

- Kiindulási állapot:

- Mindegyik csomópont_{*i*} ismeri elsődleges szomszédjai $d(i, k)$ távolságát.
- Mindegyik magasabb rendű szomszéd végtelen távolságra van.

$$D(i, j) = \begin{cases} 0, & \text{ha } i = j, \\ \infty, & \text{egyébként.} \end{cases}$$

- Algoritmus lépései:

1. Csomópont_{*i*} mindegyik k szomszédjától megkapja a $D(k, j)$ értéket.
 2. Mindegyik csomópont_{*k*} szomszédjától érkezett $D(k, j)$ érték alapján távolság metrika számolás: $X_{i,k,j} := d(i, k) + D(k, j)$
 3. Ha $X_{i,k,j} < D(i, j)$, akkor csomópont_{*k*} előnyösebb úton van, ezért $D(i, j) := X_{i,k,j}$
 4. Ciklusidő várakozás, majd folytatás 1. lépésnél.
- Az eljárás véges számú lépés után optimális utat szolgáltat a forrás és cél csomópontok között.

2. Távolságvektor alapú forgalomirányítás (DVR)

Távolságvektor alapú forgalomirányítás – routing tábla problémák:

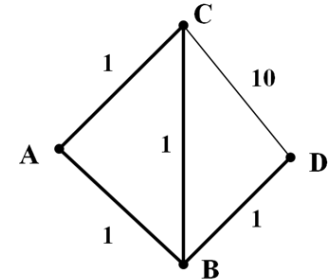
1) Túl kicsi kezdőérték probléma: Ha az optimális út megsérül, akkor nagyobb költségű (hosszabb) út nem léphet helyébe.

Megoldás: Kötelező felülírni a korábbi (kisebb) metrika értéket az optimális út irányából érkező nagyobb költséggel.

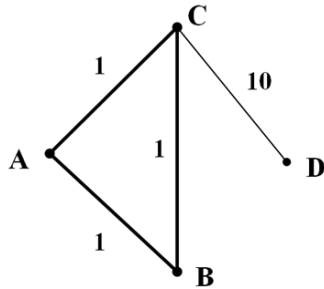
2) Végtelenig számlálás (Counting to Infinity) probléma: Az eljárás bizonyos esetekben nagyon lassan reagál a topológia változására.

Példa: Legrövidebb távolság meghatározása D-be küldéshez:

$$D(A,D) = X_{A,B,D} = 2, \quad D(B,D) = d(B,D) = 1, \quad D(C,D) = X_{C,B,D} = 2$$



Routing táblák a B-D kapcsolat megsérülése esetén:



Forrás	Ciklus 1	Ciklus 2	Ciklus 3	Ciklus 4	...	Ciklus 9	Ciklus 10	Ciklus 11
A → D	B, 2	C, 3	C, 4	C, 5	...	C, 10	C, 11	C, 11
B → D	---	C, 3	C, 4	C, 5	...	C, 10	C, 11	C, 11
C → D	B, 2	A, 3	A, 4	A, 5	...	A, 10	D, 10	D, 10

2. Távolságvektor alapú forgalomirányítás (DVR)

1. Routing Information Protocol (RIP, RFC 1058):

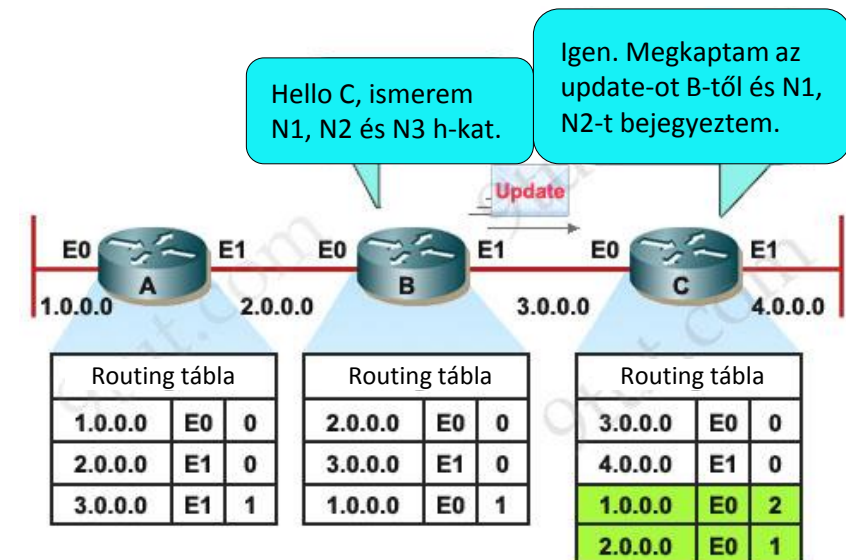
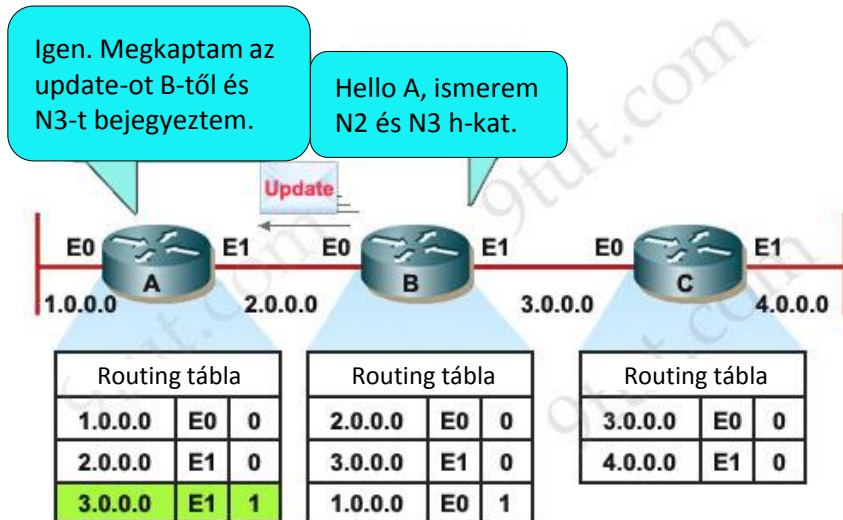
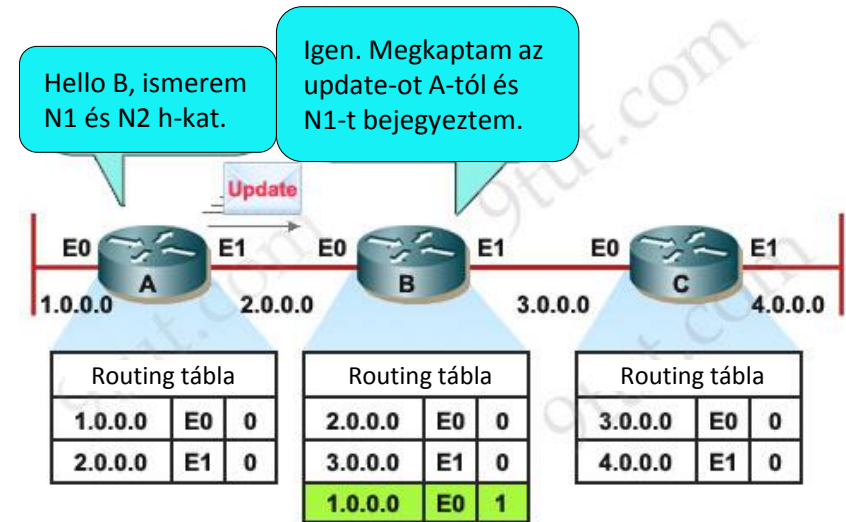
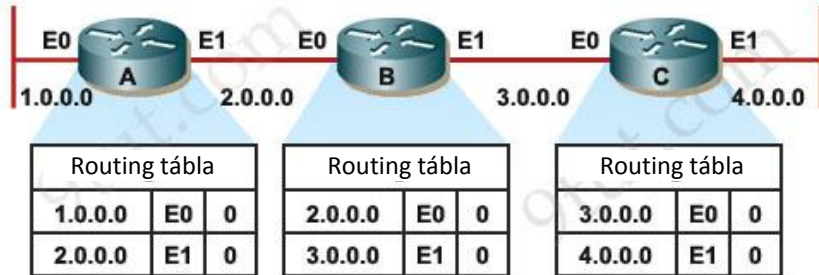
- Távolságvektor alapú IGP routing protokoll.
- Régi, de folyamatosan fejlesztik, javítják.
- Kisméretű hálózatokban használható.

- Metrika: érintett útválasztók (hop-ok) száma, minden kapcsolat költsége 1.
- Maximum 15 hop hosszúságú optimális útvonal esetén használható (16 = ∞ távolság).
- Routing update ciklusidő: 30 s.
- Szomszédos útválasztó elérhetetlen státusz: ha 6 x 30 s-ig nincs routing update.

- Végtelenig számlálás idejének csökkentése:
 - Link változása esetén azonnali routing update küldése
 - Speciális állapotjelző bitek (flag) és időzíteni információk nyilvántartása szükséges
- RIP: csak osztályos hálózatok kezelése, nincs autentikáció.
- RIPv2 (RFC 1723): CIDR kompatibilis, a szomszédok közötti kommunikációra autentikáció előírható.

2. Távolságvektor alapú forgalomirányítás (DVR)

Routing Information Protocol példa:



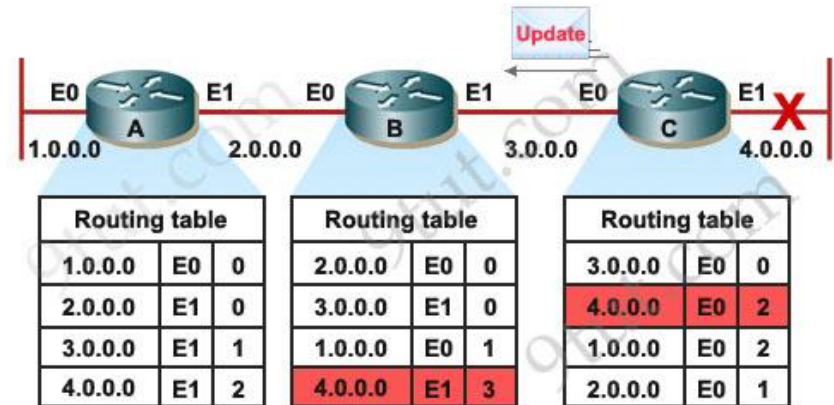
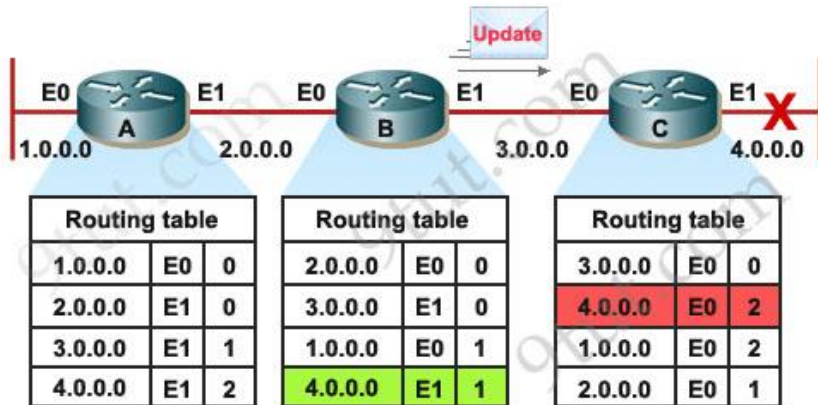
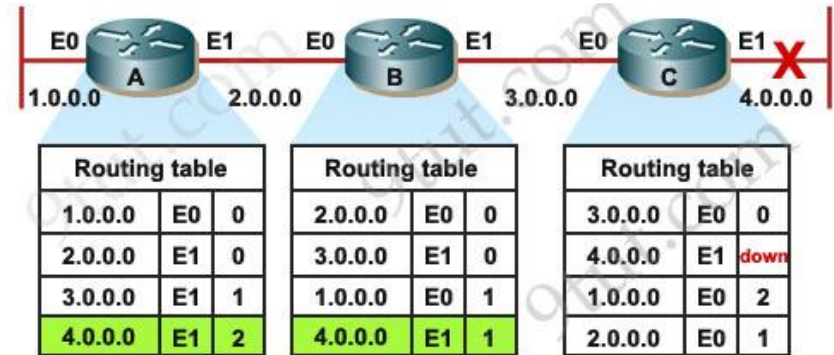
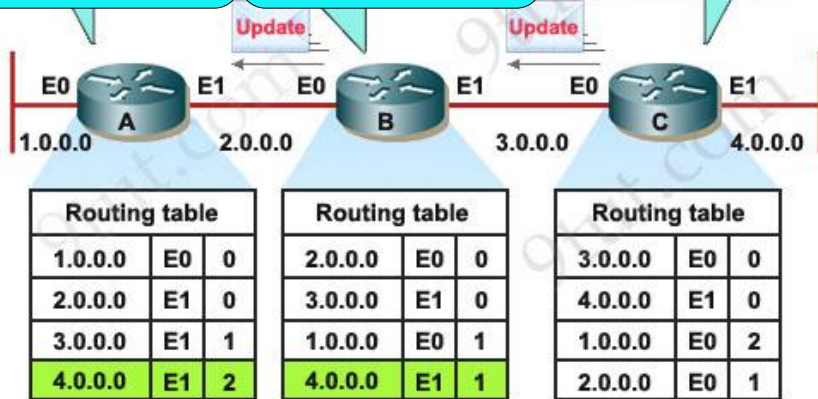
2. Távolságvektor alapú forgalomirányítás (DVR)

Routing Information Protocol példa:

Igen. Megkaptam az update-ot B-től és N4-t bejegyeztem.

Igen. N4 hálózatot bejegyeztem és update-ot elküldtem A-nak.

Hello B, ismerem N1, N2, N3 és N4 h-kat.



2. Távolságvektor alapú forgalomirányítás (DVR)

2. Enhanced Interior Gateway Routing Protocol (EIGRP):

- Gyártóspecifikus (Cisco Systems) távolságvektor alapú IGP (hibrid) routing protokoll.
- LAN hálózatokban alkalmazzák.
- Sokcélú, flexibilis, skálázható, CIDR és VLSM kompatibilis, autentikációt támogat.
- Szomszédsági viszonyok kiépítése és fenntartása: update csak tényleges változás esetén és csak a változást terjeszti.
- Metrika: összetett, öt darab változóból súlyozással számított:
 - Alapértelmezett változók: átviteli ráta [b/s], késleltetés [s].
 - Opcionális változók: terhelés [%], megbízhatóság [%], MTU [B].
- Megbízható távolság adott hálózathoz (DR): legkisebb metrika érték az adott hálózatig.
- Végtelenig számlálás kezelése több módszerrel:
 - Trigger-elt update: hálózati változás okoz frissítés küldést.
 - Látóhatár felosztás (Split Horizon): router nem küld vissza update-ot forrásnak.
 - Lefogó (Hold down) időzítő: a legjobb út keresése előtt kis ideig várakozás, hogy minden útválasztó értesüljön a módosult helyzetről.
- Potenciális helyettesítő útvonalak nyilvántartása egy háttér, topológia adatbázisban.
- Integrált routing: több fajta irányított protokollra alkalmazható.

2. Távolságvektor alapú forgalomirányítás (DVR)

1) Enhanced Interior Gateway Routing Protocol (EIGRP) példa: Útvonal: R1 → N

R1-R2-R3-R5 útvonal paramétereit:

$$b = \min\{56, 56, 10000, 10000\} = 56$$

$$d = 2000 + 2000 + 100 + 100 = 4200$$

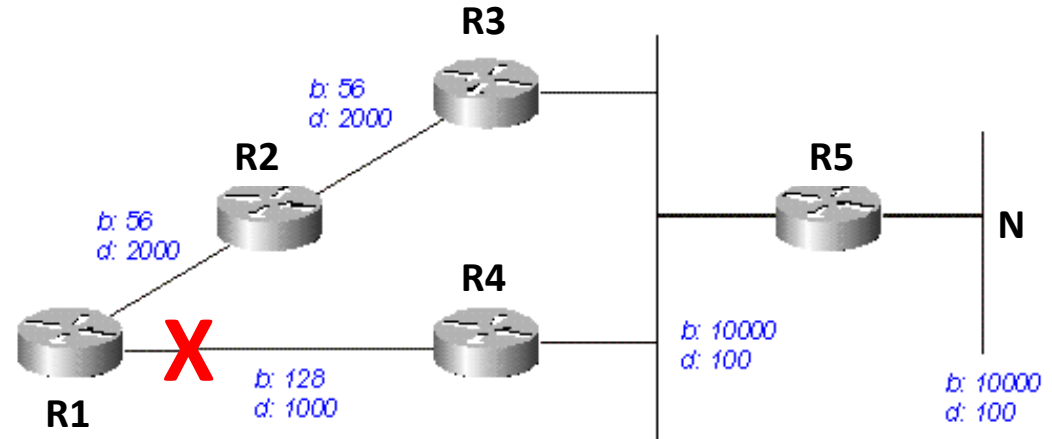
$$\text{metrika} = b + d = 4256$$

R1-R4-R5 útvonal paramétereit:

$$b = \min\{128, 10000, 10000\} = 128$$

$$d = 1000 + 100 + 100 = 1200$$

$$\text{metrika} = b + d = 1328$$



R1-ben routing tábla bejegyzés: (N, R4) és DR = 1328

R1-ben topológia tábla bejegyzések: (N, R4); (N, R2)

2) Enhanced Interior Gateway Routing Protocol (EIGRP) példa: Útvonal: R3 → N, No Split Hori.

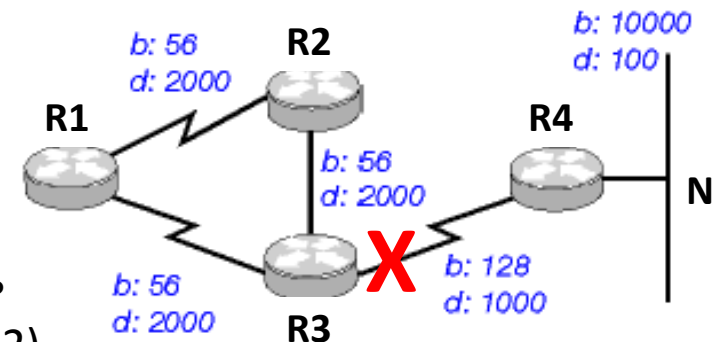
R3-R1-R2-R3-R4-N útvonal metrika = $56 + 7100 = 7156$

R3-R2-R1-R3-R4-N útvonal metrika = $56 + 7100 = 7156$

R3-R4-N útvonal metrika = $128 + 1100 = 1228$

R3-ban routing tábla bejegyzés: (N, R4) és DR = 1228 → ∞

R1-ben topológia tábla bejegyzések: (N, R4); (N, R1); (N, R2)



3. Link-állapot alapú forgalomirányítás (LSR)

Működési alapelv:

- Routing tábla egy-egy bejegyzése: adott elérhető célhoz a legjobb küldési irány.
- Elérhető cél: csomópont vagy hálózat.
- Metrika: link-állapot.
- A szomszédos forgalomirányítók között állapotváltozás jelzés: értesítés (update) küldése a teljes tartományon belül a teljes tartományra vonatkozóan.
- Routing update kiértékelése routerben: legjobb út módosítása, ha létezik még jobb új út.

Mechanizmus ismételt lépései:

1. Szomszédok felfedezése.
2. A szomszédok felé vezető kapcsolat (link) költségének mérése (érzékelés és számolás).
3. PDU készítése a mérési eredményekről.
4. A készített PDU küldése (update) a hálózati forgalomirányítási tartomány összes útválasztójának, többes formájában (elárasztás).
5. Minden router ismeri a teljes hálózati topológiát, és ki tudja számítani (pl. Dijkstra algoritmussal) a többi routerhez vezető optimális utat (feszítőfa, spanning tree számítás).

3. Link-állapot alapú forgalomirányítás (LSR)

Dijkstra algoritmus: (A. S. Tanenbaum Számítógép-hálózatok c. könyve alapján.)

```
#define MAXNODES 1024                                /* maximum number of nodes */
#define INFINITY 1000000000                          /* larger than every maximum path */

int dist[MAXNODES][MAXNODES];                       /* dist[i][j] is the distance from i to j */

void shortestpath(int n, int s, int t, int path[]) {
    struct state {
        int predecessor;                             /* the path being worked on */
        int length;                                  /* previous node */
        enum {permanent, tentative} label;           /* length from source to this node */
    } state[MAXNODES];                               /* label state: permanent, tentative */

    int i, k, min;
    struct state *p;

    for (p = &state[0]; p < &state[n]; p++)          /* initialize state */
        { p->predecessor = -1;  p->length = INFINITY; p->label = tentative; }

    state[t].length = 0; state[t].label = permanent; k = t; /* k is the initial working node */
}
```

3. Link-állapot alapú forgalomirányítás (LSR)

```

    /******* Continue void shortestpath(int n, int s, int t, int path[]) *****/

do {
    for (i = 0; i < n; i++)
        if (dist[k][i] != 0 && state[i].label == tentative)
            if (state[k].length + dist[k][i] < state[i].length)
                { state[i].predecessor = k; state[i].length = state[k].length + dist[k][i]; }

    /******* Find the tentatively labeled node with the smallest label. *****/
    k = 0; min = INFINITY;
    for (i = 0; i < n; i++)
        if (state[i].label == tentative && state[i].length < min)
            { min = state[i].length; k = i; }
    state[k].label = permanent;
} while (k != s);

    /******* Copy the path into the output array. *****/
i=0; k=s;
do { path[i++] = k; k = state[k].predecessor; } while (k >= 0);

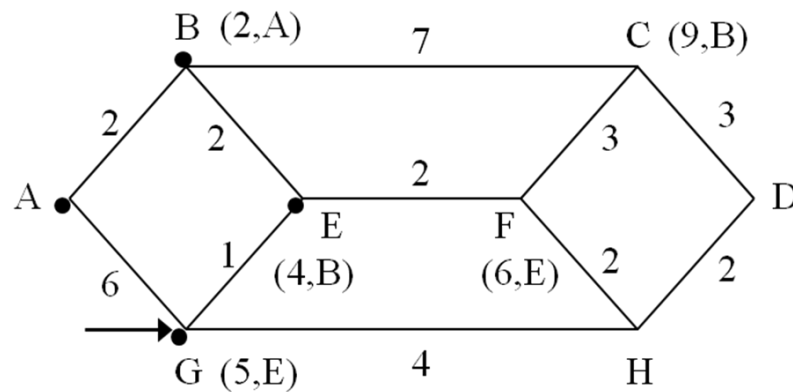
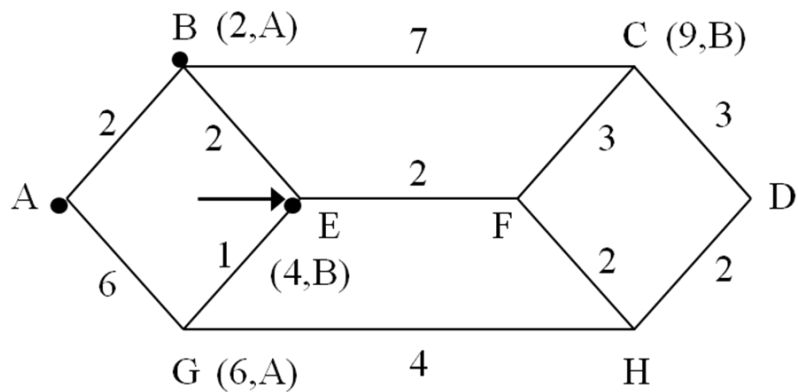
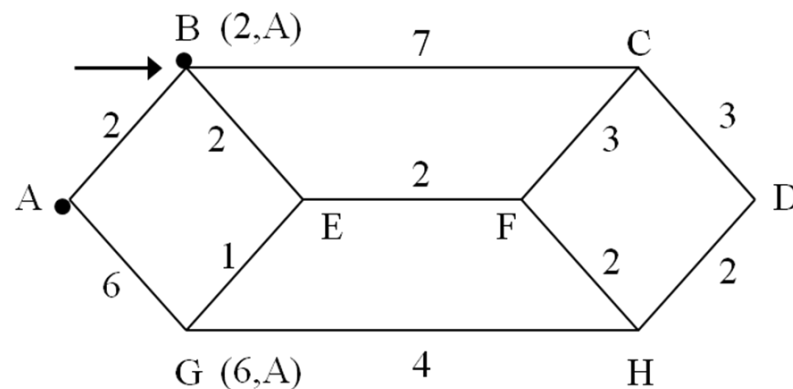
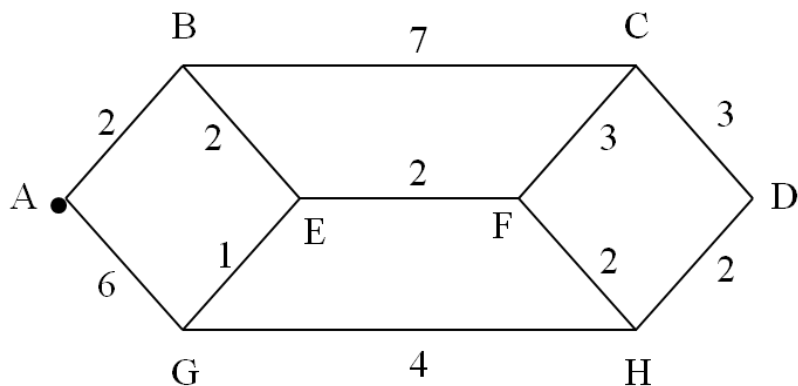
}

    /******* End of shortestpath. *****/
```

3. Link-állapot alapú forgalomirányítás (LSR)

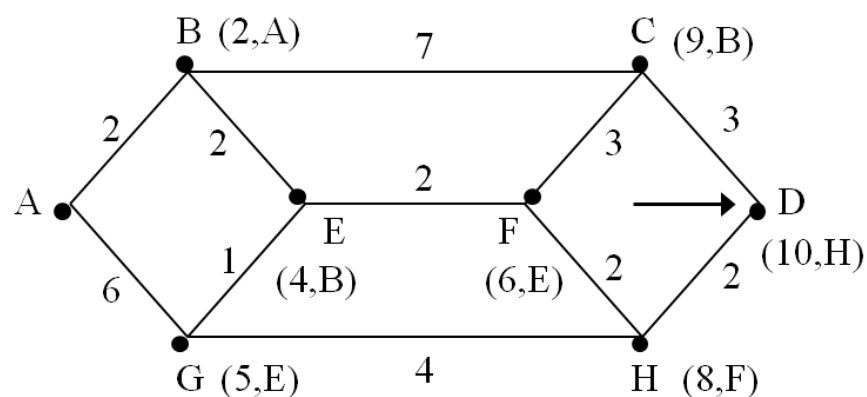
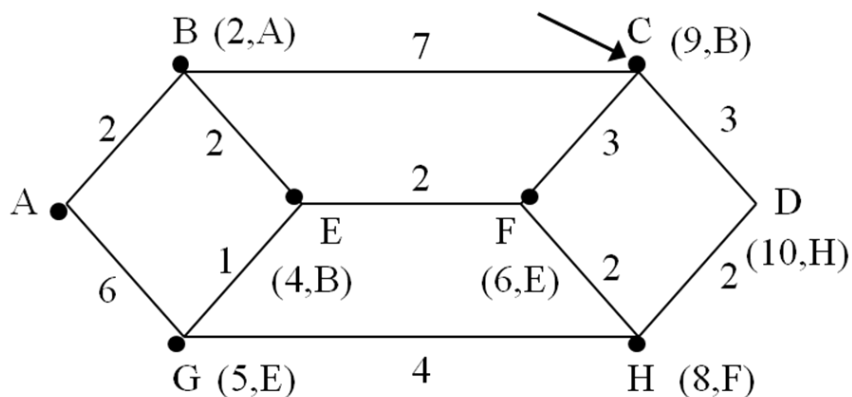
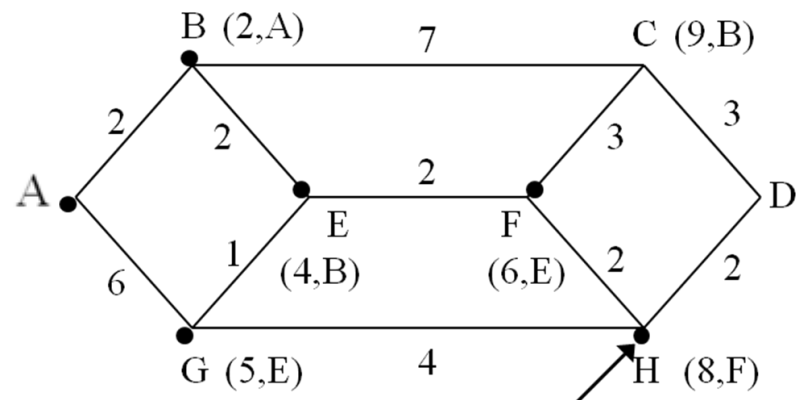
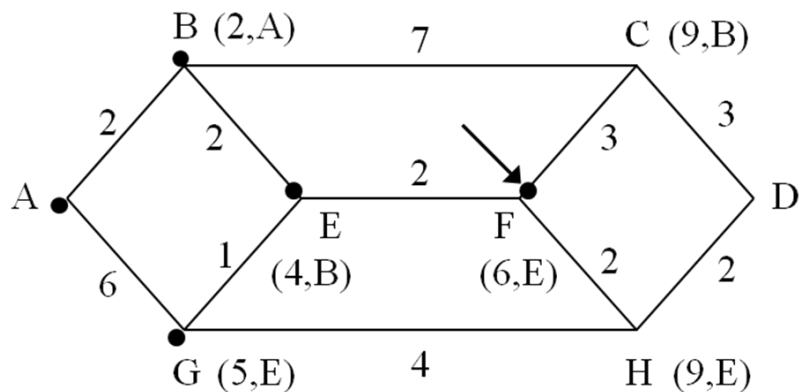
Dijkstra algoritmus példa: $A \rightarrow D$ optimális útvonal keresése a gráfban

- Fa gyökere: A
- Csúcsponst státusz: ● lezárt; → aktuális



3. Link-állapot alapú forgalomirányítás (LSR)

Dijkstra algoritmus példa (folyt.): $A \rightarrow D$ optimális útvonal keresése a gráfban

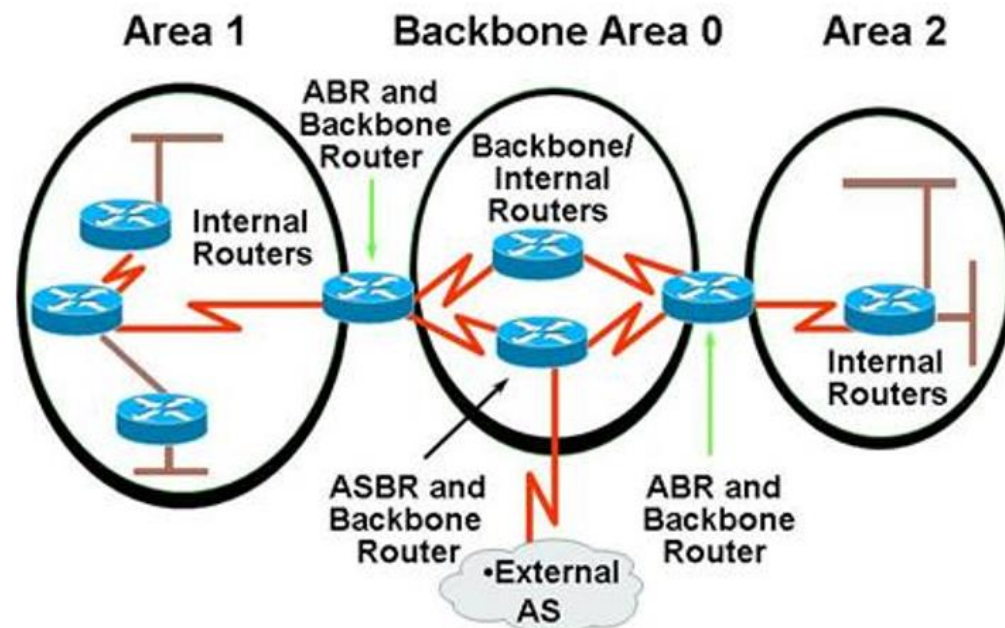


- Optimális $A \rightarrow D$ útvonal: $A \rightarrow B \rightarrow E \rightarrow F \rightarrow H \rightarrow D$
- Optimális $A \rightarrow D$ út költsége: 10

3. Link-állapot alapú forgalomirányítás (LSR)

1. Open Shortest Path First (OSPF) routing protokoll (RFC 1131, IP: RFC 1247):

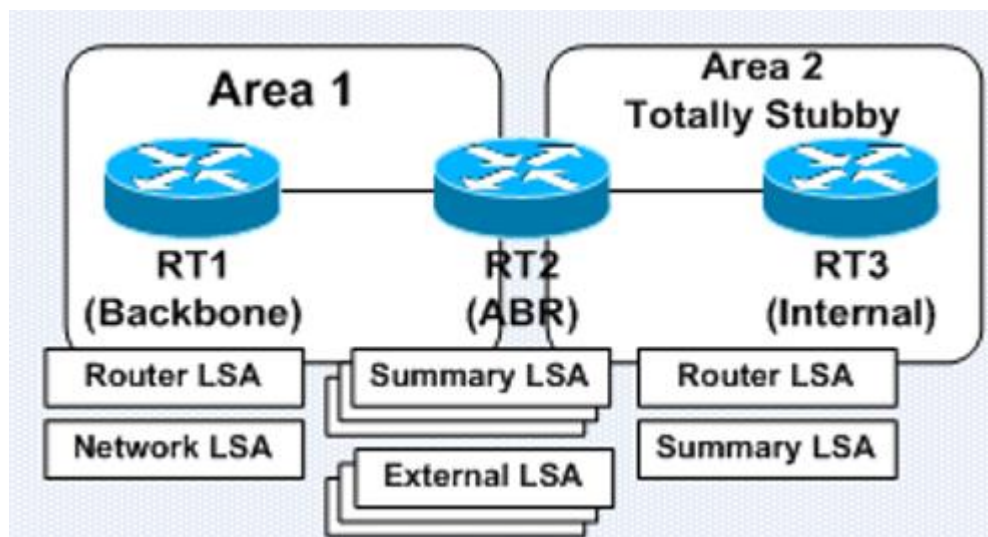
- Nyílt szabványú, link-állapot alapú IGP routing protokoll.
- Működési környezet: tipikusan IP technológia felett.
- Használat: hierarchikus szervezésű LAN/MAN hálózatokban.
- Többcélú, flexibilis, skálázható, CIDR és VLSM kompatibilis, autentikációt támogat.
- Terület (Area): felügyelt L3 hálózatok csoportja: Non-backbone Area / Backbone Area.
- Terület elemei: L3 hálózatok (link-ek).
- Autonóm rendszer (AS): azonos üzemeltetési érdekeltségű Area-k halmaza.
- Router típusok:
 - Internal Nonbackbone Stub Area
 - Area Border Router (ABR)
 - Autonomous System Boundary Router (ASBR).



3. Link-állapot alapú forgalomirányítás (LSR)

1. Open Shortest Path First (OSPF) routing protokoll (RFC 1131, IP: RFC 1247):

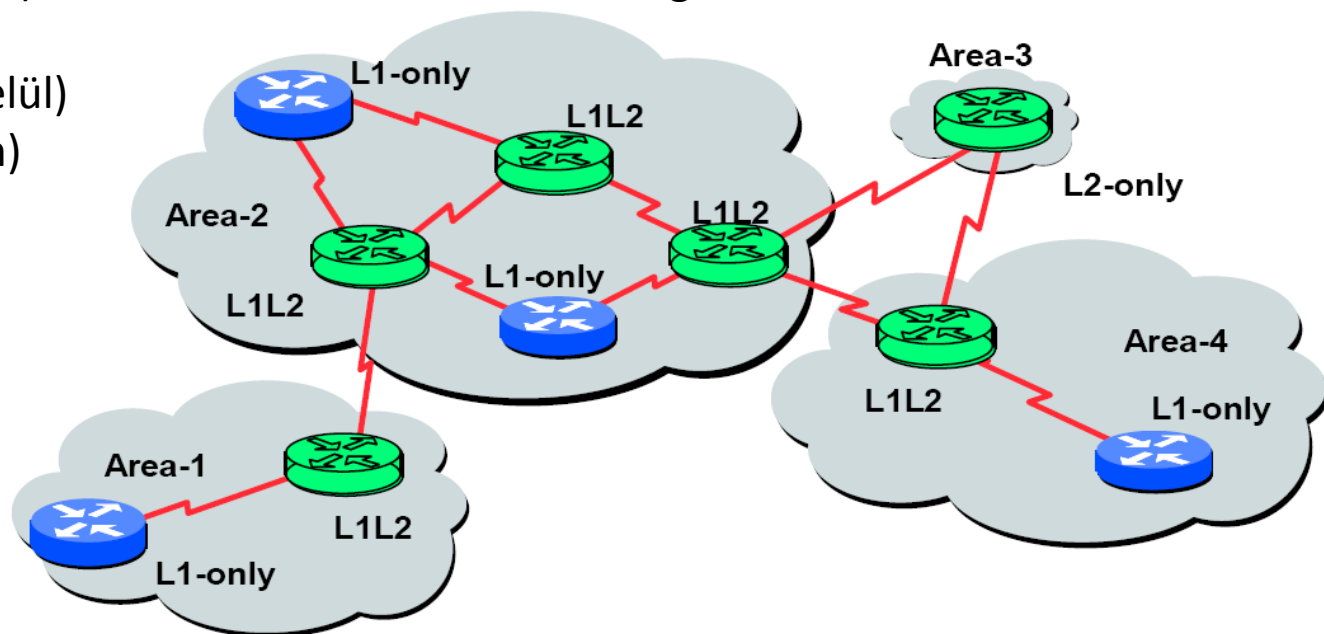
- Routing update: AS útválasztói között a link-állapot információk (LSA) szétküldése elárasztásos módszerrel.
- Gerinchálózati Area: kötelezően Area0.
- Mindegyik OSPF router magának építi fel AS-en belül az SPF (Shortest Path First) fa adatbázist az aggregált link-állapot információk alapján.
- Legjobb útvonal meghatározása: Dijkstra algoritmus



3. Link-állapot alapú forgalomirányítás (LSR)

2. Intermediate System to Intermediate System (IS-IS) routing prot. (ISO10589, IP: RFC1195):

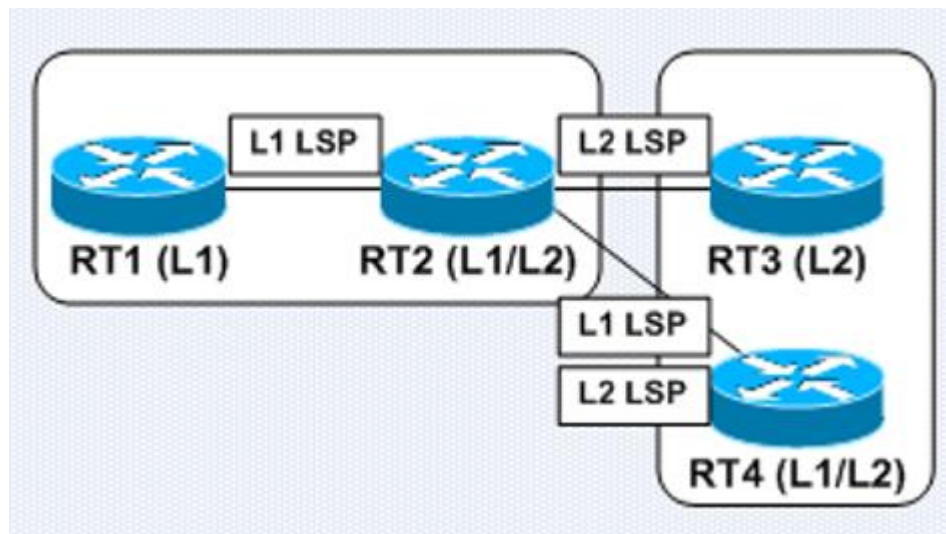
- Nyílt szabványú, link-állapot alapú IGP routing protokoll.
- Működési környezet: tipikusan adatkapcsolati átviteltechnika felett.
- Használat: nagy ISP gerinchálózatokban (2 hierarchia szint).
- Sokcélú, flexibilis, skálázható, CIDR és VLSM kompatibilis, autentikációt támogat.
- Terület (area): felügyelt L3 hálózatok csoportja.
- Terület elemei: L3 hálózatok ÉS útválasztók.
- Autonóm rendszer (AS): azonos üzemletetési érdekeltségű area-k halmaza.
- Router típusok:
 - L1 (Stub Area-n belül)
 - L1-2 (Area határán)
 - L2 (Gerinc)



3. Link-állapot alapú forgalomirányítás (LSR)

2. Intermediate System to Intermediate System (IS-IS) routing prot. (ISO10589, IP: RFC1195):

- Routing update: AS útválasztói között a link-állapot információk (LSP) szétküldése elárasztásos módszerrel.
- Gerinchálózati Area: L2 útválasztók.
- Mindegyik IS-IS router magának építi fel AS-en belül az SPF (Shortest Path First) fa adatbázist az aggregált link-állapot információk alapján.
- Legjobb útvonal meghatározása: Dijkstra algoritmus



3. Link-állapot alapú forgalomirányítás (LSR)

OSPF és IS-IS routing protokollok összehasonlítása:

Tulajdonság	OSPF	IS-IS
Routing protokoll	Dijkstra SFP	
VLSM/CIDR	Igen	
Update	Elárasztásos	
Area	Link-ek	Útválasztók
Update szállítás	IP csomagban	Adatkapcsolati keretben
Gerinc	Area 0	Több router közösen
Rugalmasság	Alacsony	Magas
Komplexitás	Magas	Nagyon magas
Security	Magas	Nagyon magas
Megbízhatóság	Magas	Nagyon magas
IPv6 támogatás	OSPFv3	Alapból, bármit

3. Link-állapot alapú forgalomirányítás (LSR)

Belső routing protokollok (IGP) jellemzői:

- Konvergencia sebesség: topológia és/vagy terhelés változásának követési sebessége.
- Méret skálázhatóság: router-ek és L3 hálózatok száma.
- VLSM/CIDR képesség: IPv4 esetén osztályos/nem osztályos hálózatok hirdetése.
- Erőforrás igény: router hardver (RAM, CPU) és átviteli ráta erőforrások.
- Komplexitás: beüzemeléshez és üzemeltetéshez szükséges rendszergazdai know-how.

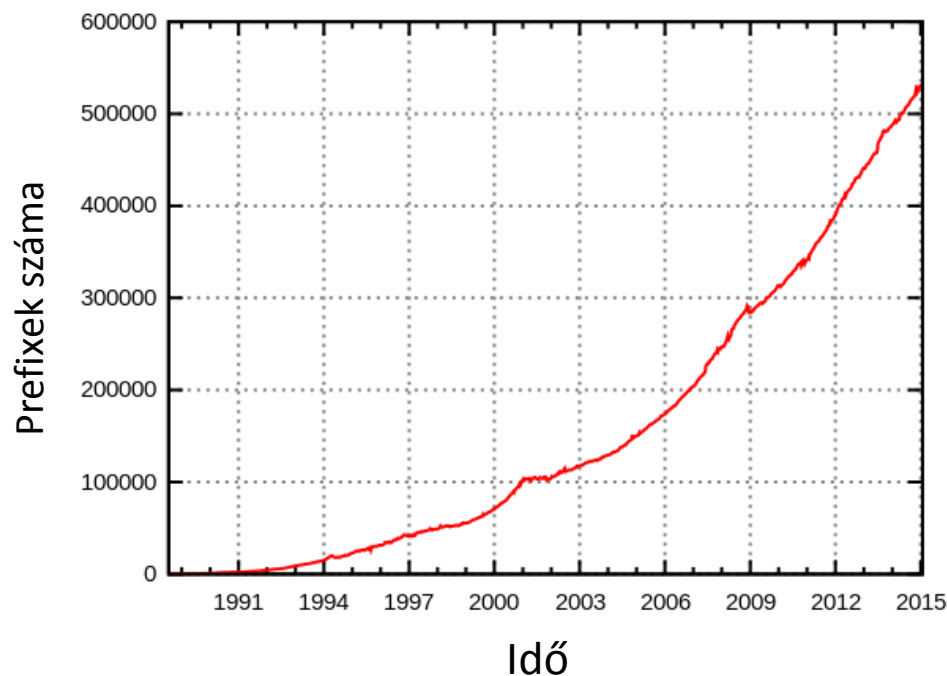
Jellemző	Távolságvektor alapú				Link-állapot alapú	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Konvergencia sebessége	Alacsony	Alacsony	Alacsony	Magas	Magas	Magas
Méret skálázhatóság	Alacsony	Alacsony	Alacsony	Magas	Magas	Magas
VLSM/CIDR képesség	Nem	Nem	Nem	Igen	Igen	Igen
Erőforrás igény	Alacsony	Alacsony	Alacsony	Közepes	Magas	Magas
Komplexitás	Alacsony	Alacsony	Alacsony	Magas	Magas	Magas

4. Vektor-állapot alapú forgalomirányítás (VSR)

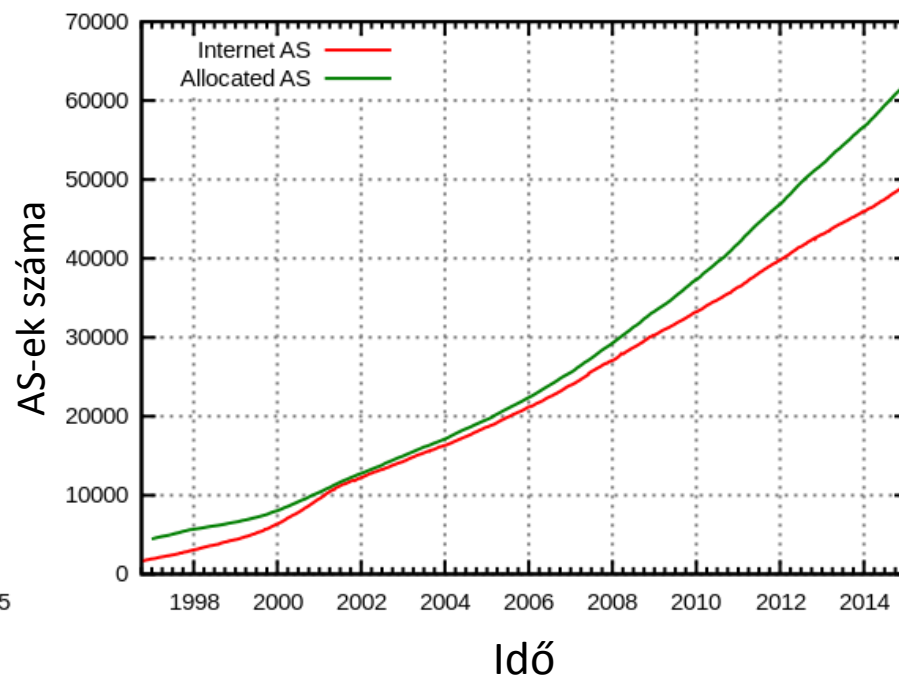
Megfontolások:

- Minden egyes IP csomag útválasztása routerben a routing tábla alapján történik.
- IP hálózatok számának növekedése a routing táblák bejegyzéseinek számát növeli.
- Internet méretének növekedése a távoli gerinc útválasztók teljesítményét is rontja.
- Cél: routing bejegyzések számának optimális csökkentése.

IP prefixek száma az Interneten



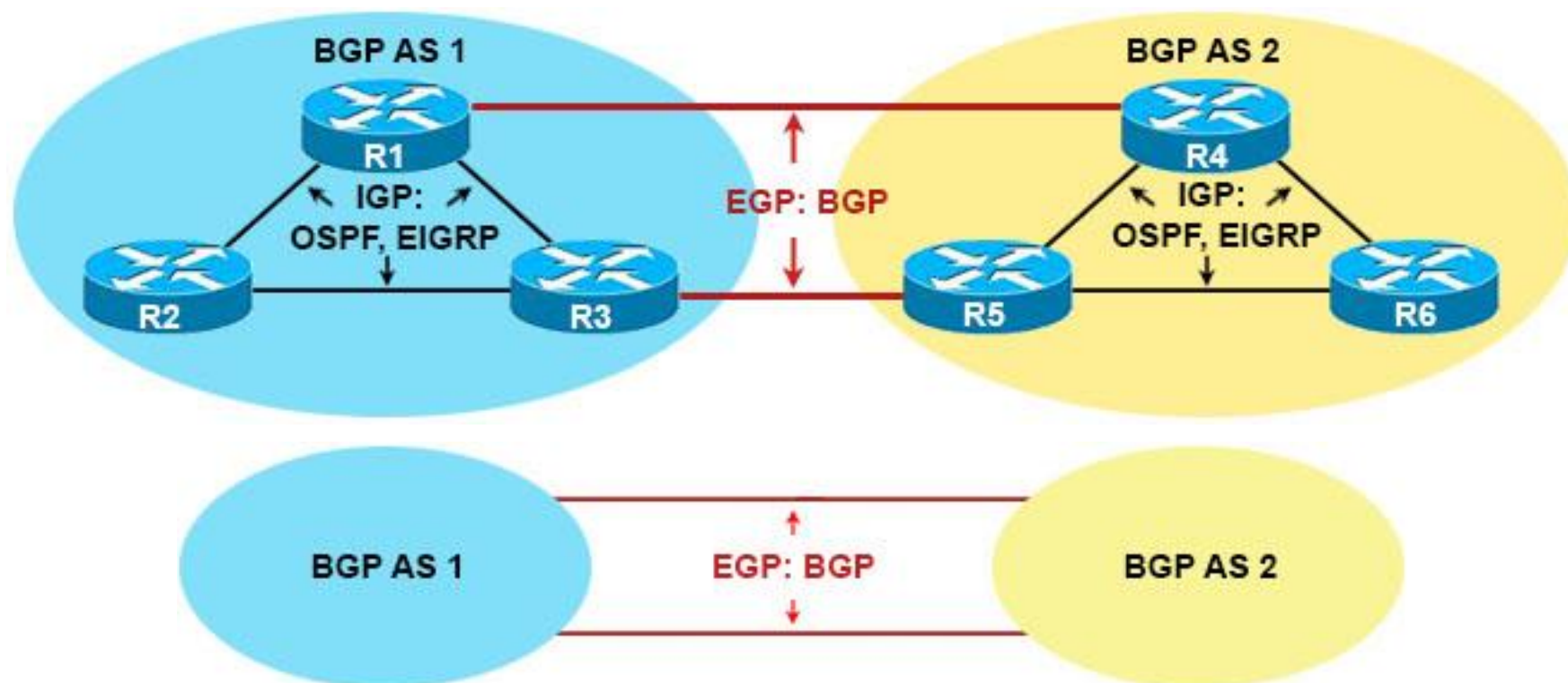
AS-ek száma az Interneten



4. Vektor-állapot alapú forgalomirányítás (VSR)

Border Gateway Protocol (BGP) routing protokoll (RFC 1771, RFC 4271):

- IGP: AS-en belüli routing protokoll.
- EGP: különböző AS-ek közötti routing protokoll.
- AS: világon egyedi azonosítójú (16 bit), egyetlen adminisztratív tartomány.
- ISP: egy vagy több AS üzemeltetése.



4. Vektor-állapot alapú forgalomirányítás (VSR)

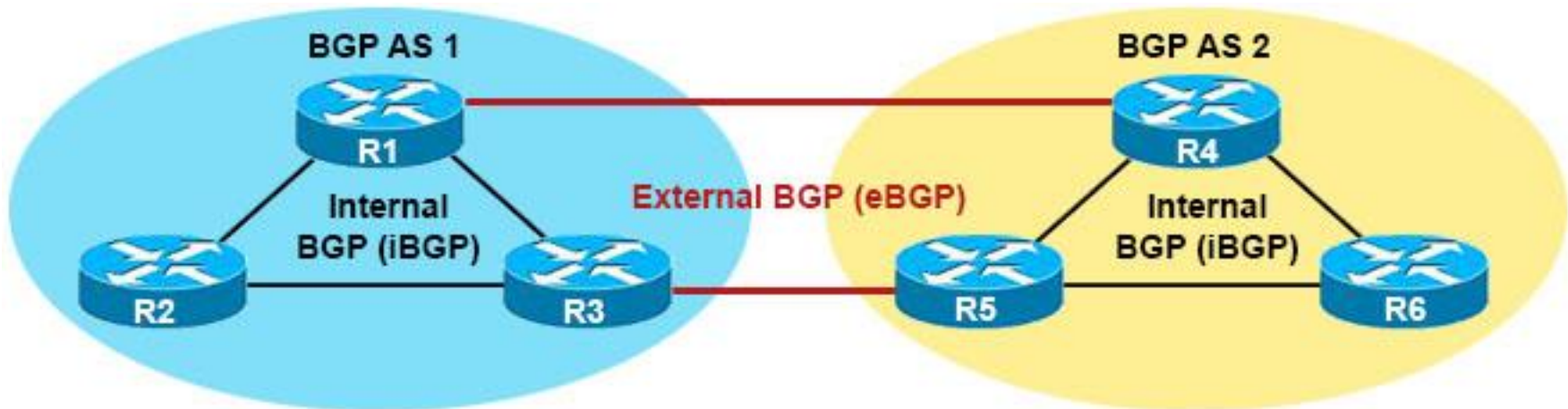
Border Gateway Protocol (BGP) routing protokoll (RFC 1771, RFC 4271) (folyt.):

- BGP fogalmak:

- BGP router: BGP protokollt beszélő útválasztó.
- BGP pár / BGP szomszéd: TCP:179 kapcsolatban lévő BGP router pár.
- Prefix: alhálózat vagy aggregált hálózat.

- BGP router típusok:

- Internal BGP (iBGP): AS-en belüli BGP pár (pl.: R1-R2, R1-R3, R2-R3, R4-R5, R4-R6, R5-R6).
- External BGP (eBGP): különböző AS-ek közötti BGP pár (pl.: R1-R4, R3-R5).



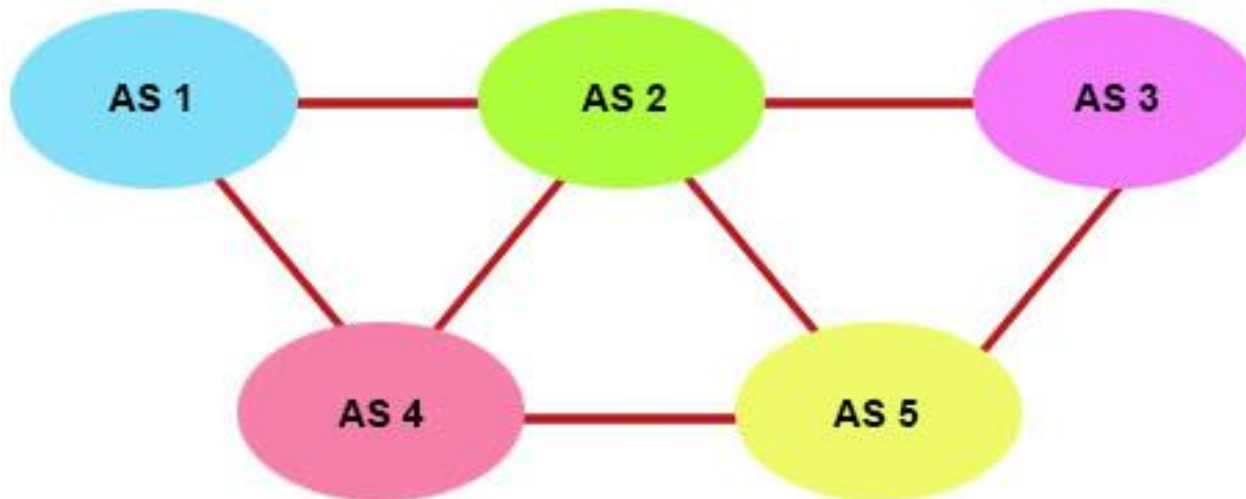
4. Vektor-állapot alapú forgalomirányítás (VSR)

Border Gateway Protocol (BGP) routing protokoll (RFC 1771, RFC 4271) (folyt.):

- BGP egyedi routing tulajdonsága:

- Routing: útvonalvektor alapján, legelőnyösebb AS útvonal.
- Forgalom átviteli ráta szabályozása link-enként.
- Nagyon nagy méretű routing táblákat képes kezelni.
- Jól igazodik a VPN (Virtual Private Network) megoldásokhoz (MPLS VPN).

- Példa: AS1 → AS3 útvonala különböző routing megoldások esetén



- IGP (OSPF, EIGRP): AS1 → AS2 → AS3
- BGP: AS1 → AS4 → AS5 → AS3 (de lehet más is)

A blue world map with a glowing circuit board pattern overlaid on it, representing global connectivity and technology.

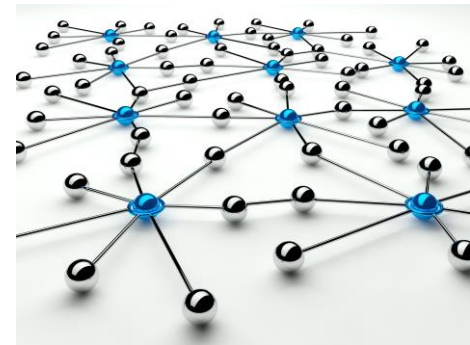
SZÁLLÍTÁSI RÉTEG PROTOKOLLOK

IP FELETT: TCP/UDP

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2018. március 20.



SZÁLLÍTÁSI RÉTEG PROTOKOLLOK

IP FELETT: TCP/UDP

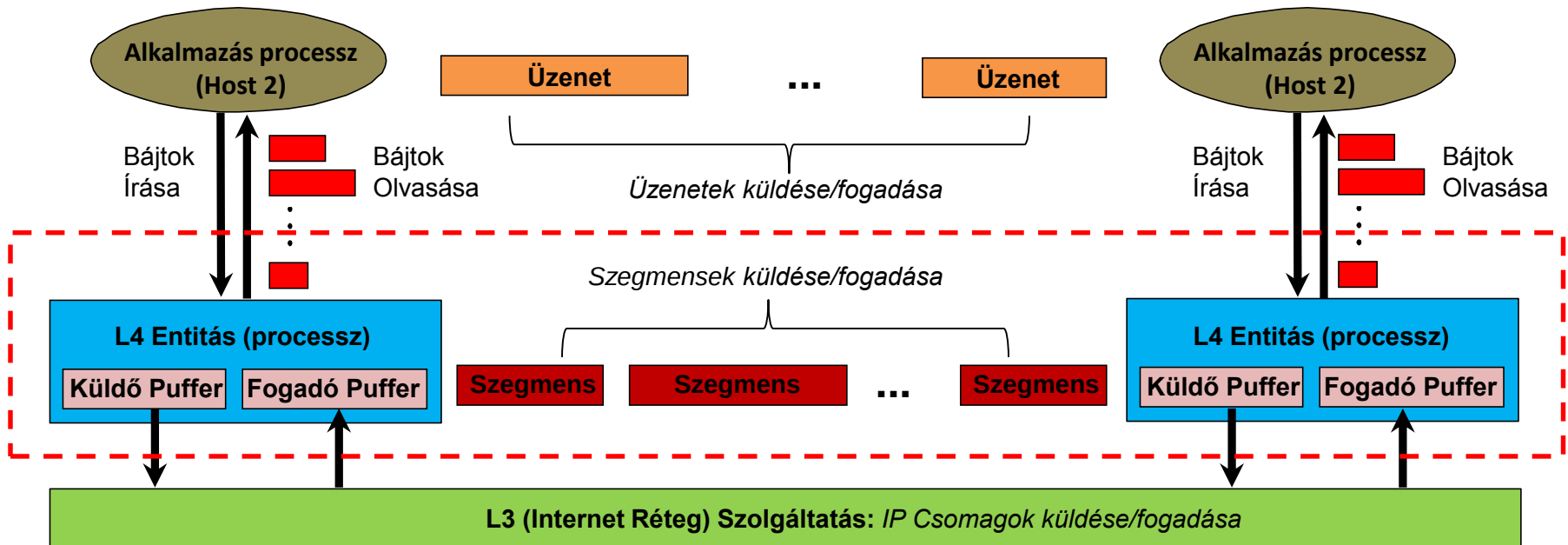
Tartalom

- 1) Transzport protokollok IP felett
- 2) User Datagram Protocol (UDP)
- 3) Transmission Control Protocol (TCP)
- 4) Transzport protokollok összehasonlítása

1. Transzport protokollok IP felett

Megfontolások:

- Alkalmazás réteg számára kommunikációs szolgáltatás.
- A különböző számítógépek processz szintű kapcsolata párban történik.
- Elvárás a klasszikus szolgáltatások egyértelmű azonosítása.
- A kommunikáció ezen a szinten is szabványos kell, hogy legyen.
- A kommunikáló processzek ideiglenesen, egy vagy több PDU küldése céljából kapcsolódhatnak egymáshoz.
- Szállítási réteg PDU (szegmens) nem módosítható átvitel közben a hálózaton (pl. darabolás nem megengedett szállítási rétegben).



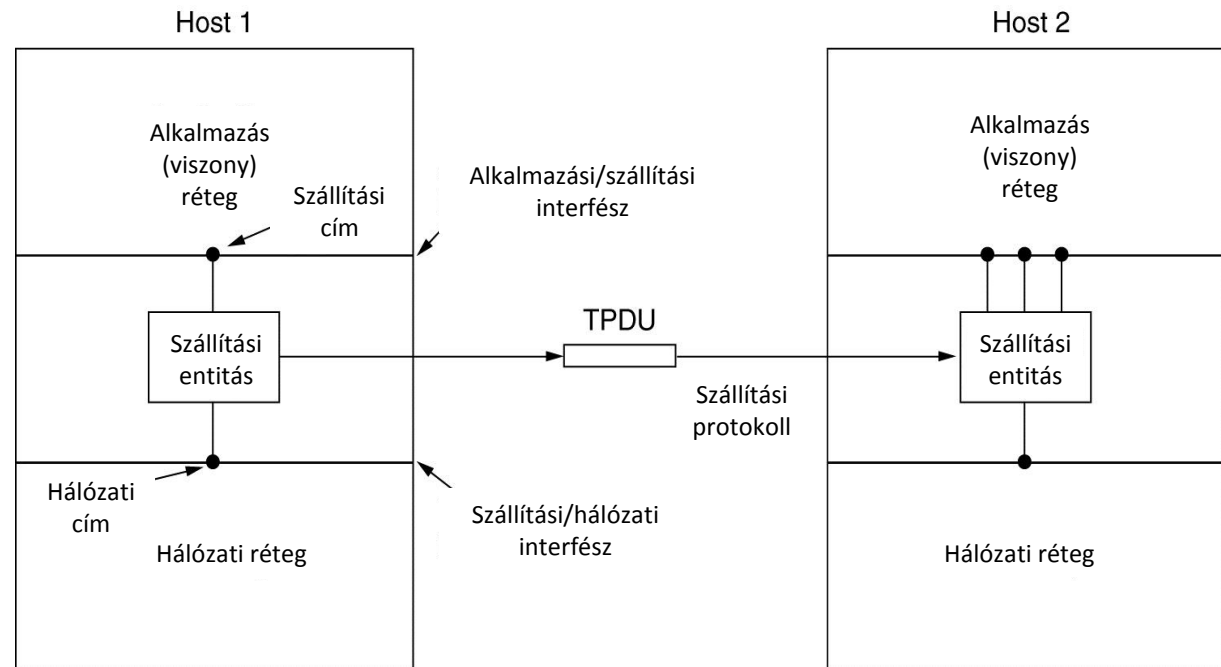
1. Transzport protokollok IP felett

Transzport réteg funkciók:

- **Címzés:** végponti kommunikáló programok egyértelmű azonosítása.
- **Kapcsolat felépítés:** szegmens sorozat küldésének előkészítése.
- **Kapcsolat lebontás:** szegmens sorozat küldésének befejezése.
- **Adatfolyam szabályozás és pufferezés:** torlódások kezelése.
- **Multiplexálás:** hálózati réteg hatékony felhasználása.
- **Forgalom elakadás kijavítása, kezelése:** alsóbb rétegek képességeihez való dinamikus alkalmazkodás.

Összetevők:

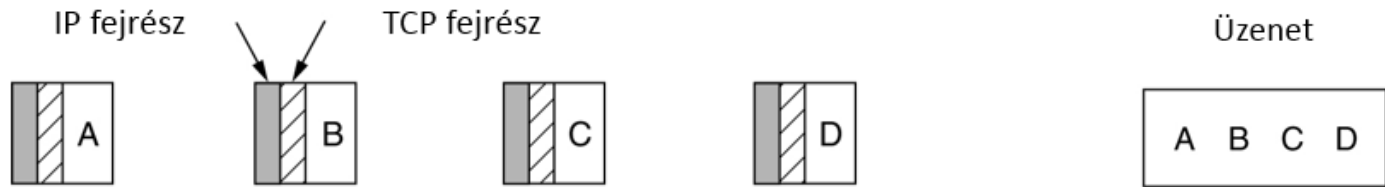
- Interfészek
- Pufferek, adatelemek
- Entitások, protokollok
- Címek, azonosítók.



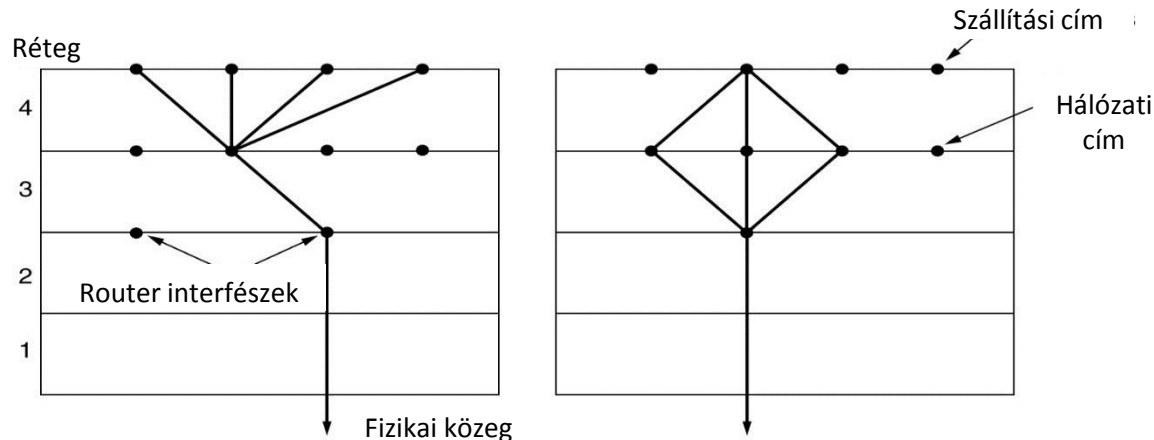
1. Transzport protokollok IP felett

Transzport protokollok szolgáltatásai:

- **Kapcsolatorientált/kapcsolat nélküli adatfolyam:** Szegmens(ek) kézbesítése (sorrendben).
- **Megbízhatóság:** Az elküldött szegmens vagy szegmens sorozat kézbesítése.
 - Megbízhatóság szintje a szolgáltatás típusától függ.
 - Pl.: Bináris fájl letöltése $\leftrightarrow$ Videó tartalom mozgatása.



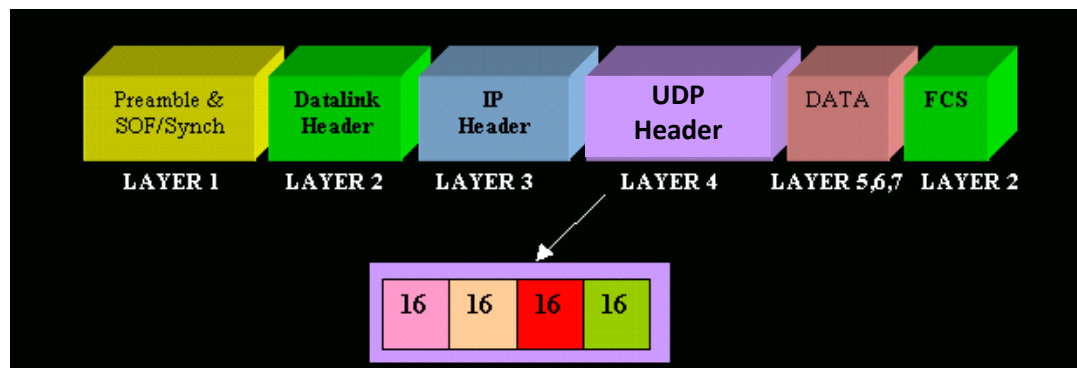
- **Adatfolyam vezérlés:** Időegység alatt küldött bájtok mennyiségének szabályozása.
- **Multiplexálás/demultiplexálás:** Hálózati rétegen több fajta szegmens küldése/fogadása.
 - Különböző forgalmak időben összefésült módon továbbítódnak: hatékonyság.



2. User Datagram Protocol

User Datagram Protocol (UDP, RFC 768):

- Összeköttetés nélküli (CL) szállítási réteg protokoll.
- Nem megbízható, nyugta nélküli kapcsolat a szegmens küldésének idejére.
- Hibajavítási funkció: alkalmazás szinten.
- Felhasználó alkalmazás jellemzői:
 - Adatvesztés tolerancia.
 - Átviteli ráta érzékenység.
- Funkciók:
 - UDP datagram küldése.
 - UDP datagram fogadása.
- UDP szegmens: Fejrész + Rakrész.
- Tipikus alkalmazások: DNS, SNMP, TV multicast, multimédia kommunikáció (VoIP, IoT).



2. User Datagram Protocol

UDP szegmens fejrész szerkezete:

Forrás portszám	Cél portszám
Hossz (bájt)	Ellenőrző összeg

1. szó: Forrás portszám (16 bit), Cél portszám (16 bit).

2. szó: UDP szegmens hossza (16 bit), Fejrész ellenőrző összeg (16 bit).

UDP szegmens rakrész:

- Tetszőleges tartalom (bármilyen réteg PDU).
- Előnyös tűzfalakon továbbított protokollok áthidalására.
- Bithiba javítását, illetve egynél több vagy kevesebb példányos kézbesítés kezelését a rakrészben szállított PDU protokolljára bízva.

UDP-Lite (RFC 3828) változat:

- Fejrészben az Hossz mező jelentése megváltozik: Checksum Coverage.
- Ellenőrző összeg csak fejrészre vonatkozik (rakrész hibáit nem érzékeli: előny/hátrány).
- Felhasználás: multimédia hálózatok (hang, videó).

2. User Datagram Protocol

Szegmens fejrész ellenőrző összeg számolási algoritmus (UDP és TCP esetén):

- Socket = (IP cím, Port) azonosítópár.
- Biztonsági funkció célja: a kapcsolathoz tartozó Socket pár ellenőrzése
Forrás_Socket(Forrás IP cím, Forrás Port) és Cél_Socket(Cél IP cím, Cél Port).
- Ellenőrző kód kiszámolása álfejrész segítségével.

Álfejrész (Pseudo Header) szerkezete:

- IP fejrészből származó mezők:
 - Forrás IP cím (32 bit)
 - Cél IP cím (32 bit)
 - Töltelék (0x00)
 - Protokoll ID (TCP: 0x06, UDP: 0x17)
- Szegmens fejrészből származó mezők:
 - L4 PDU hossz (fejrész + rakrész)
- Ellenőrző összeg: 12 B összege



3. Transmission Control Protocol

Transmission Control Protocol (TCP, RFC 793):

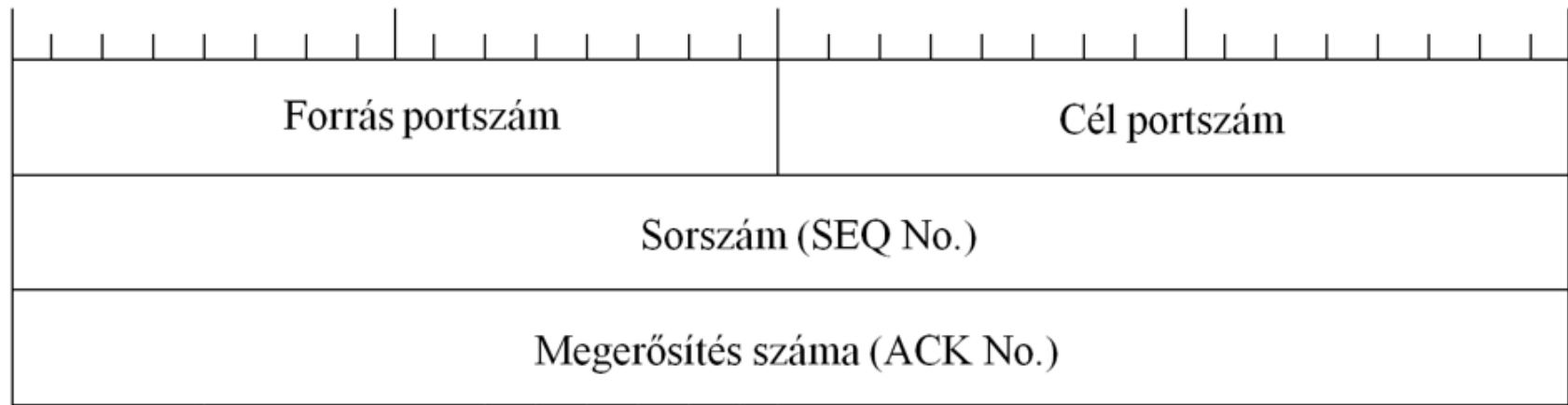
- Összeköttetés alapú (CO) szállítási réteg protokoll (Setup/Transfer/Release).
- Megbízható, nyugtázott kapcsolat a szegmenssorozat idejére.
- Minden elküldött adatbájt sorszámozása.
- Soron következő várt bájt sorszámanak visszaküldése a társa felé.
- Áramlásszabályozás: a legközelebbi szegmens méret visszajelzése a társ processzhez.
- TCP szegmens: Fejrész + Rakrész.

TCP szegmens fejrész szerkezete:

Forrás portszám										Cél portszám									
Sorszám (SEQ No.)																			
Megerősítés száma (ACK No.)																			
Data Offset	Foglalt	U	A	P	R	S	F	Ablakméret											
		R	C	S	S	Y	I												
		G	K	H	T	N	N												
Ellenőrző összeg								URG pointer											
Opciók												Kitöltés							

3. Transmission Control Protocol

TCP szegmens fejrész szerkezete (folyt.):



1. szó: Forrás portszám (16 bit), Cél portszám (16 bit).

2. szó: Szegmens sorszáma (32 bit):

- Ha SYN = 0: első bájt sorszáma a szegmensben.
- Ha SYN = 1: kezdeti szekvencia szám (ISN – Initial Segment Number) és első adatbájt = ISN + 1.

3. szó: A partner által várt következő szekvencia szám (32 bit).

3. Transmission Control Protocol

TCP szegmens fejrész szerkezete (folyt.):

Data Offset	Foglalt	U R G	A C K	P S H	R S T	S Y N	F I N	Ablakméret	
Ellenőrző összeg								URG pointer	
Opciók								Kitöltés	

4. szó: Adat offset (4 bit): TCP fejrész szavainak száma.

Fenntartott mező (6 bit): 000000

Kontroll bitek:

URG: Urgent Pointer mezőt értelmezni kell (1) vagy sem (0).

ACK: Acknowledgement (a nyugta sorszám értéke érvényes(1) vagy sem (0)).

PSH: Push Function (a szegmenst azonnal továbbítani/fogadni kell)

RST: Reset (kapcsolat lezárása hiba miatt)

SYN: Szekvencia szám (kapcsolat kiépítés, szinkronizálás).

FIN: Adat vége a küldőtől (kapcsolat bontás).

Ablakméret (16 bit): nyugtázott bájtok száma.

5. szó: Ellenőrző összeg (16 bit); Urgent Pointer (prioritásos adat kezdete, offset-je).

6-15. szó: Opciók (MSS - Maximum Segment Size; CWND Scaling; SACK; Timestamps; Nop).

3. Transmission Control Protocol

1. TCP kommunikációs mechanizmusok: Összeköttetés fázisai:

A. Felépítés (Setup) fázis: háromutas kézfogás (three-way handshake): SYN - SYN/ACK - ACK

1. Kliens: kapcsolat kiépítésének kezdeményezése:

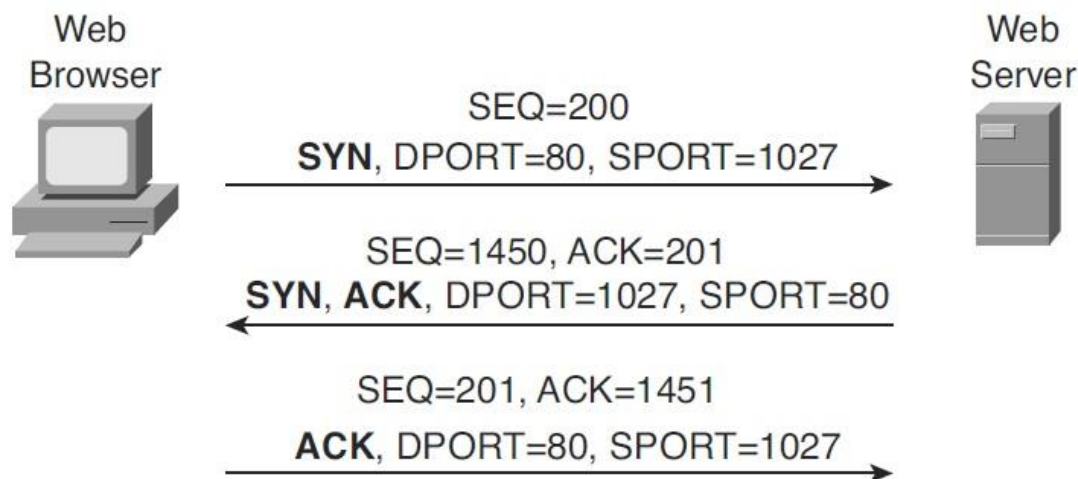
- Portsámok és kezdősorszám beállítása (pl. SEQ_No = 200); Jelzőbitek: SYN=1, ACK=0.

2. Szerver: jóváhagyó válasz-üzenetet küldése:

- Portsámok felcserélése; Saját kezdősorszám beállítása (pl. SEQ_No = 1450).
- Nyugta sorszám beállítása: kapott SEQ érték+1 (pl. ACK_No = 201). SYN = 1; ACK = 1.

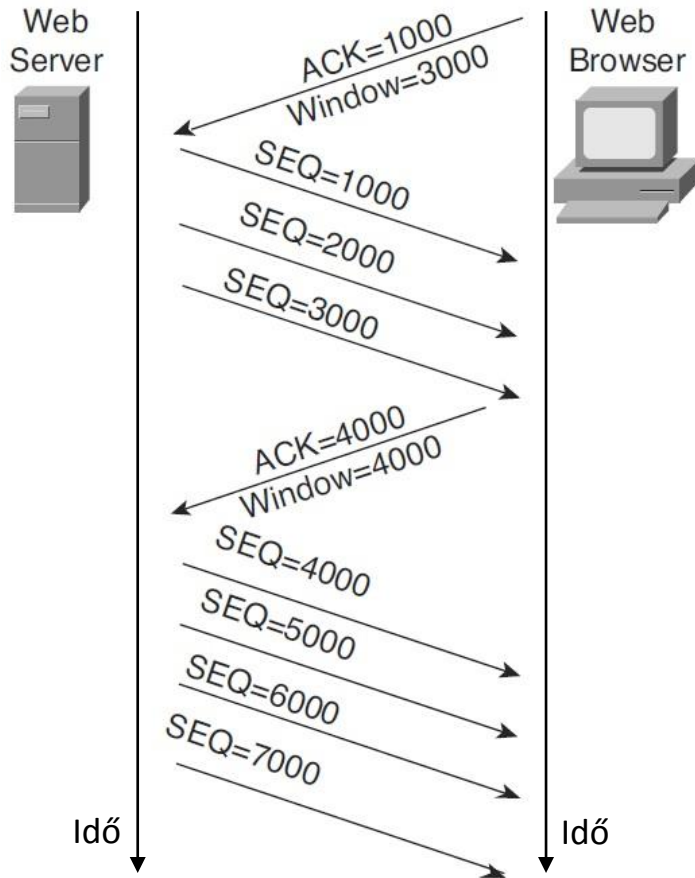
3. Kliens: jóváhagyás küldése:

- Portsámok felcserélése; Saját szegmens-sorszám beállítása (pl. SEQ_No = 201).
- Nyugta sorszám beállítása: kapott SEQ érték+1 (pl. ACK_No = 1451); SYN = 0; ACK = 1.

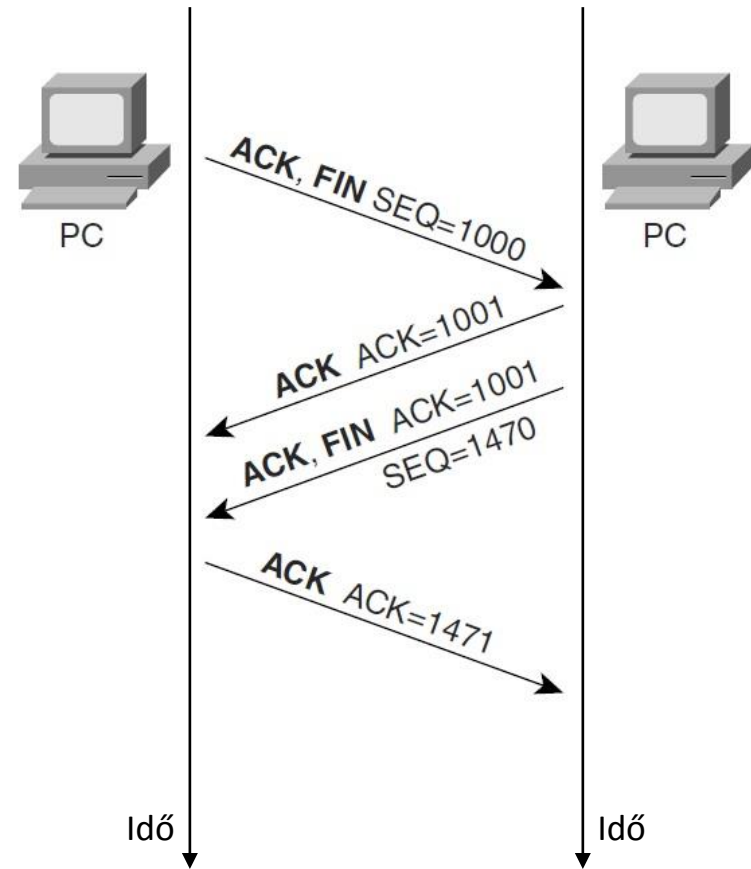


3. Transmission Control Protocol

1. TCP kommunikációs mechanizmusok: Összeköttetés fázisai (folyt.):



B. Adatátvitel (Transfer) fázis



C. Lebontás (Release) fázis (négy-utas)

- Kapcsolat lebontás sérülése: „Két hadsereg - probléma” kezelése időzítéssel.

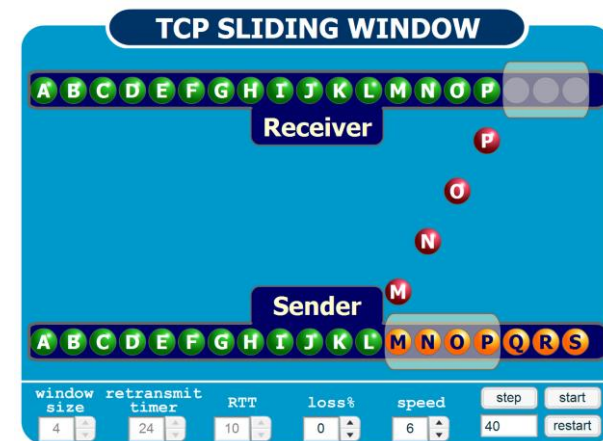
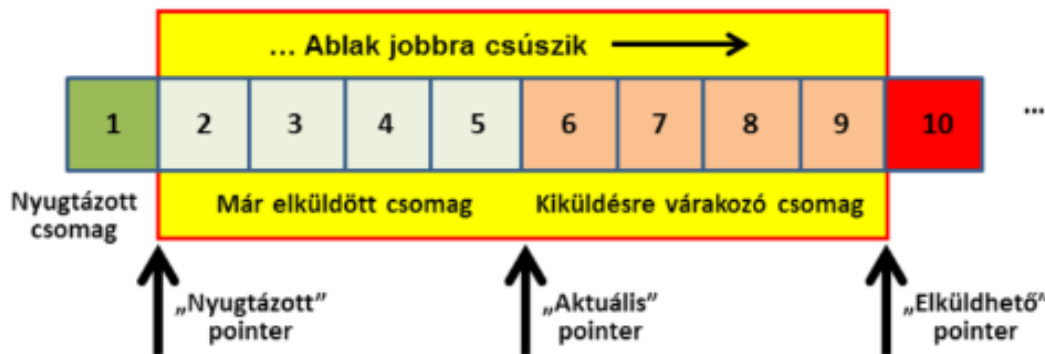
3. Transmission Control Protocol

2. TCP kommunikációs mechanizmusok: Csúszó ablak (Sliding Window):

- Tartalom küldése és fogadása: pufferek és ablak segítségével.
- Nyugta (ACK) válaszidejének figyelése szegmens újraküldés céljából.



Egy nyugta beérkezése hatására az ablak és a pointerok jobbra lépnek



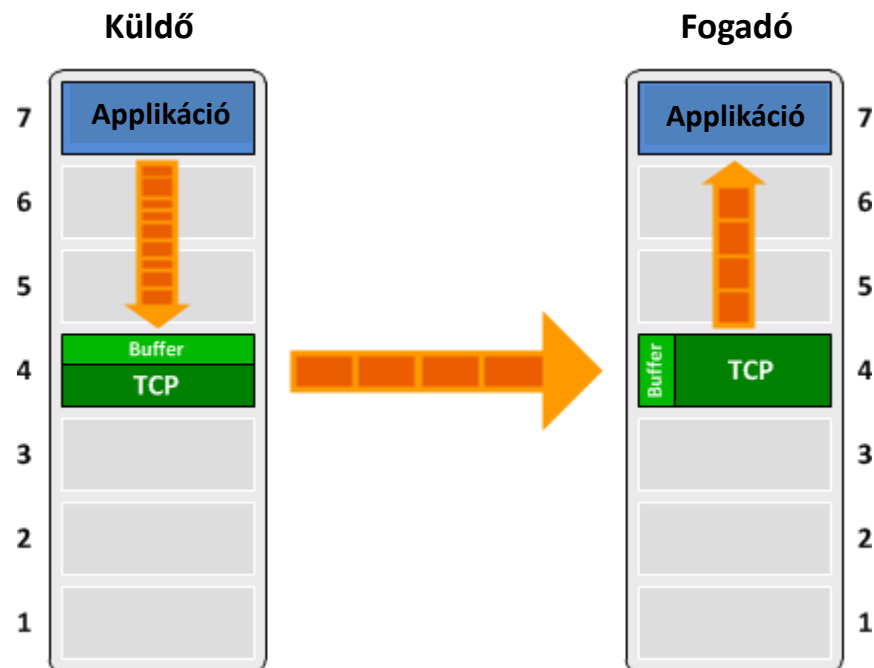
Demó:

http://www2.rad.com/networks/2004/sliding_window/demo.html

3. Transmission Control Protocol

3. TCP kommunikációs mechanizmusok: Rövid szegmens küldése (Push Segment):

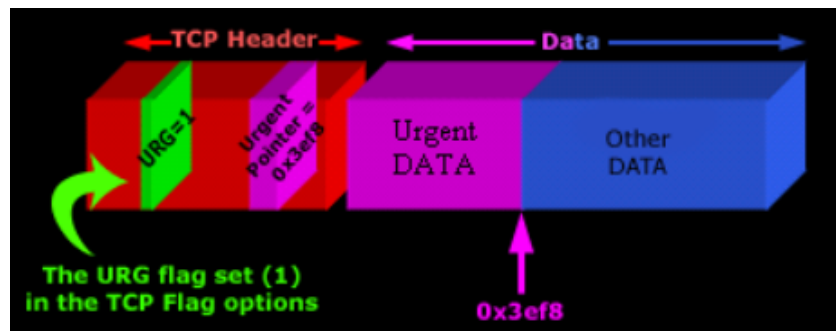
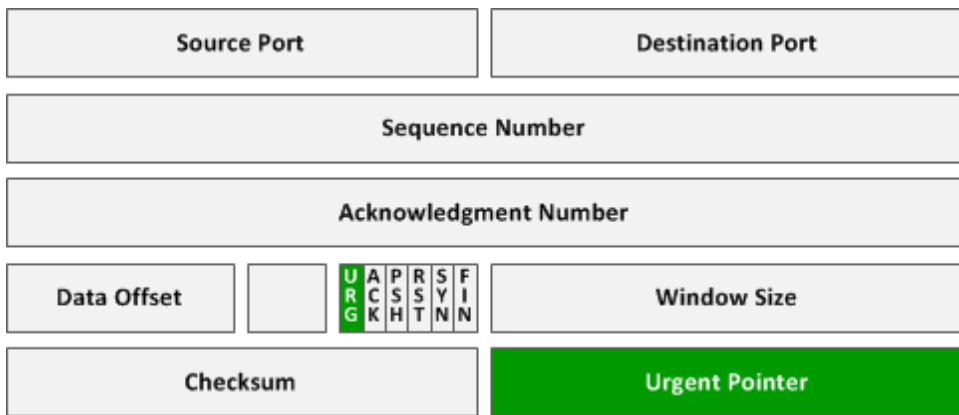
- Tartalom küldése és fogadása: pufferek segítségével.
- Küldő puffer: küldésre várakozó, vagy elküldött és még nem nyugtázott szegmens.
- Fogadó puffer: fogadott és még nem továbbított szegmens felsőbb rétegnek.
- MSS (Maximum Segment Size) méretet meghaladó tartalom: várakozás a pufferben.
- Szegmens generálás feltétele küldőnél: alkalmazás szintű adatbájtból minimális darabszám létezen.
- PSH = 1: aktuális szegmens küldése/fogadása azonnal, mérettől függetlenül, pufferben várakoztatás nélkül.
- Alkalmazási esetek:
 - Internet böngészésnél „HTTP GET” parancs elküldése
 - Fájl végének küldése.



3. Transmission Control Protocol

4. TCP kommunikációs mechanizmusok: Sürgős adat küldése (Urgent Data):

- Szegmensek küldésének alapértelmezés szerinti sorrendje: növekvő SEQ_No alapján.
- URG szegmens küldése prioritás alapján: URG_Flag = 1.
- URG_Pointer érték felhasználása: prioritásos adat utolsó bájtnak címe (offset).



- Alkalmazási esetek:
 - Telnet billentyűleütések küldése szerverhez.
 - Távoli asztal egérmozgatás állapotok, illetve billentyűleütések küldése szerverhez.

3. Transmission Control Protocol

5. TCP kommunikációs mechanizmusok: TCP teljesítmény szabályozása kapcsolat közben:

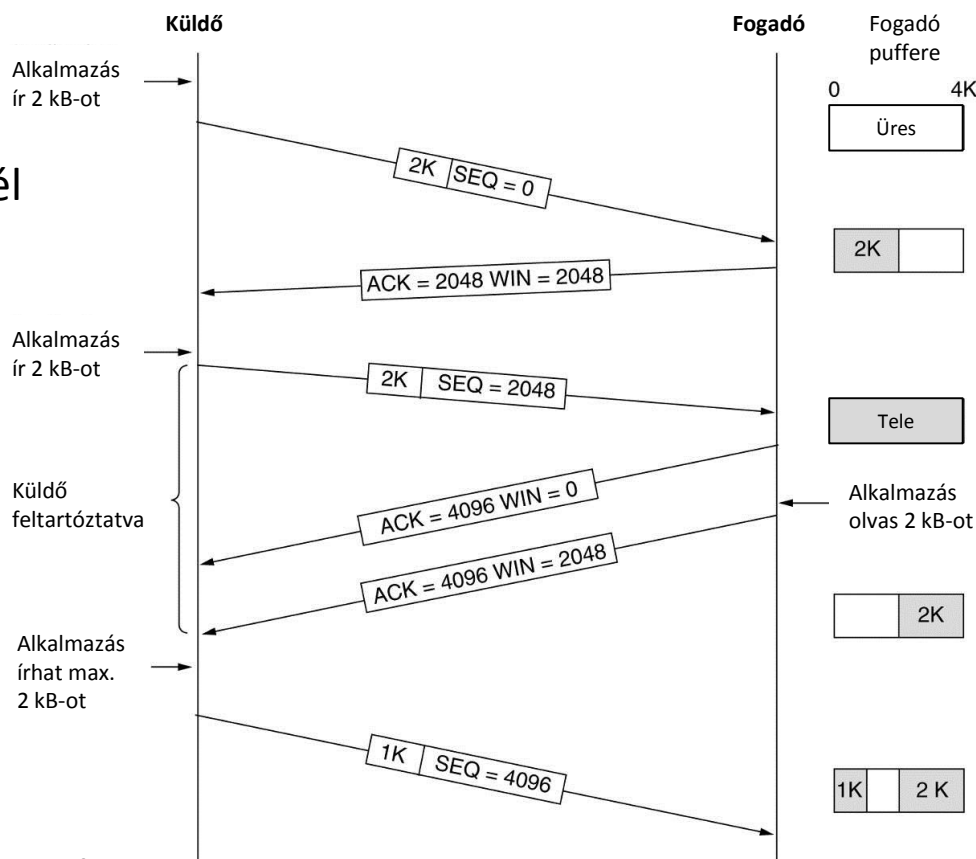
- Lehetséges torlódási helyek:
 - Hálózaton belül (router, vonal)
 - Fogadó csomópont (CPU, RAM)

4.1. Hálózati torlódás szabályozás:

- CWND (Congestion Window) küldőnél
- Torlódási ablak opcionális skálázása
$$CWND_{MAX} = 2^{16} * 2^{14} B = 1 GB !$$
- Torlódási „Ablakméret”-nyi adatbajt fogadása után adatküldő felé kötelező a nyugta-válasz (ACK).

4.2. Adatfolyam szabályozás:

- RWND (Receiver Window) fogadónál
 - Flow control fogadónál
 - Adatfolyam ablak (puffer): max. 1 GB.
- Alkalmazási esetek: nagyméretű fájlok átvitele



3. Transmission Control Protocol

6. TCP kommunikációs mechanizmusok: TCP teljesítményszabályozás kapcsolat idején:

„Slow Start” mechanizmus:

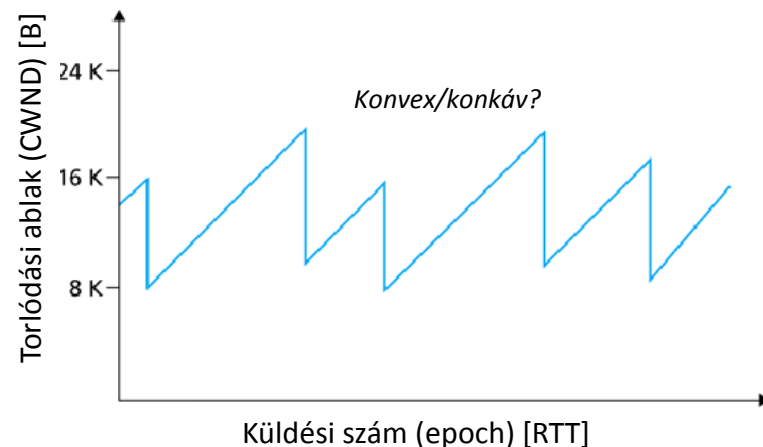
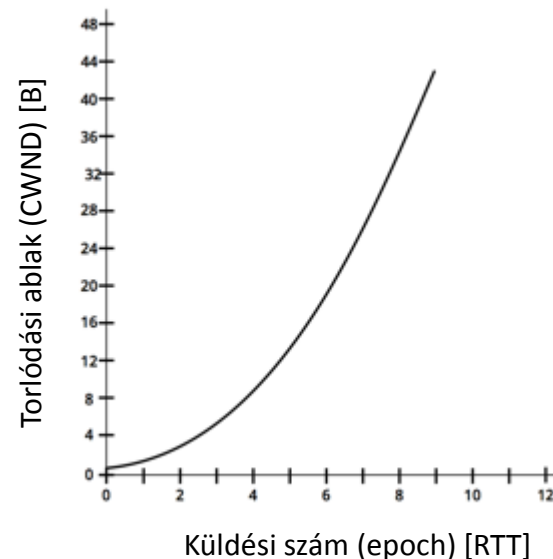
- Forgalom indítása kis átviteli rátával:
 $CWND := 1$
- Lépésenként duplázás:
 $CWND := 2 * CWND$
- Nyugtázás időtúllépése esetén újratezdés:
 $CWND := 1$

„Additive Increase Multiplicative Decrease (AIMD)” mechanizmus:

- Lépésenként additív növelés:
 $CWND := CWND + MSS * MSS / CWND$
- Nyugtázás időtúllépése esetén felezés:
 $CWND := CWND / 2$

„Fast Retransmit” mechanizmus:

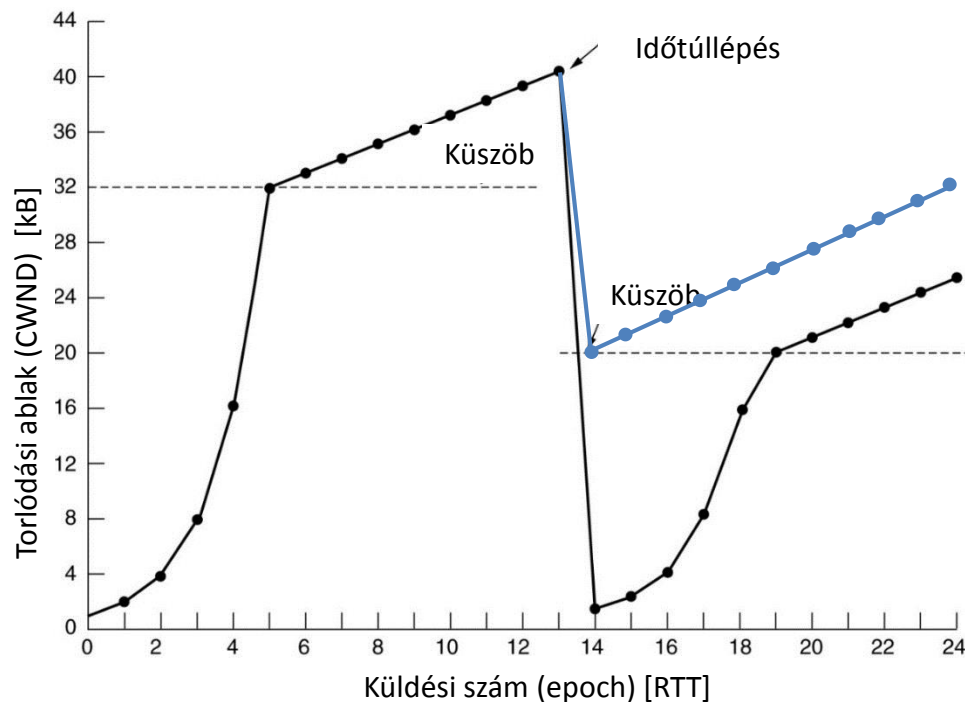
- Kiesett szegmensek soron kívüli pótlása



3. Transmission Control Protocol

7. TCP kommunikációs mechanizmusok: TCP teljesítményszabályozási változatok:

TCP implementáció	Gyártó/Felhasználó
<u>TCP Tahoe</u>	Unix
<u>TCP Reno</u> , TCP New Reno	Unix
TCP Vegas	Unix
TCP Westwood	Unix
TCP BIC, TCP CUBIC	Linux
TCP Hybla	Satellite Radio
TCP Agile-SD	Linux
Compound TCP	Microsoft
TCP PRR	Google
TCP BBR	Google
Fast TCP	Akamai Technologies
High-Speed TCP	IETF
Stb.	



4. Transzport protokollok összehasonlítása

Port tartományok:

0 – 1023:

jól ismert portok (WKP
Well-Known Port):
hivatalos szolgáltatások

1024 – 49151:

regisztrált
szolgáltatások

49152 – 65535:

privát és/vagy
dinamikus processz
portok.

Szolgáltatás (példák)	TCP port	UDP port
Echo	7	7
Wake-on-LAN	9	9
File Transfer Protocol (FTP)	20 (data) 21 (command)	20 (data) 21 (command)
Telnet	23	23
Simple Mail Transfer Protocol (SMTP)	25	25
Domain Name System (DNS)	53	53
Trivial FTP (TFTP)	69	69
Hipertext Transfer Protocol (HTTP)	80	80
Network Time Protocol	123	123
Internet Message Access Protocol (IMAP)	143	143
Simple Network Management Protocol	161 (get, getnext) 162 (trap)	161 (get, getnext) 162 (trap)
Internet Relay Chat (IRC)	194	194
Hypertext Transfer Protocol over TLS/SSL (HTTPS)	443	443
Syslog	-	514
Email Message Transfer Protocol	587	-

4. Transzport protokollok összehasonlítása

Hasonlóságok, különbségek:

Szempont	TCP	UDP
Kapcsolat típusa	Összeköttetés alapú	Összeköttetés mentes
Felhasználó alkalmazás	Magas megbízhatóság, korlátos időérzékenység	Rövid kérelmek, időérzékeny jelleggel
Tipikus alkalmazások	HTTP, HTTPS, FTP, SMTP, Telnet, SSH	DNS, DHCP, TFTP, SNMP, RIP, VoIP
Szegmens sorrend tartás	Igen	Nem
Átviteli sebesség	Alacsonyabb, mint UDP esetén	Magasabb, mint TCP esetén
Szegmens overhead	20 ... 60 B	8 B
Hasonló mezők fejrészben	Forrás port, Cél port, Ellenőrző összeg	Forrás port, Cél port, Ellenőrző összeg
Adatok stream-elése	Bájtsorozat szinten	Üzenet szinten
Költség	Kapcsolat felépítés miatt magas	Alacsony (datagram-szerű)
Adatfolyam szabályozás	Igen	Nem
Nyugtázás	Igen	Nem
Kézfogás	Három-utas (Setup), Négy-utas (Release)	Nincs
IPv6 felhasználás	Igen	Igen
Tárgyak Internete (IoT)	Korlátozottan	Igen

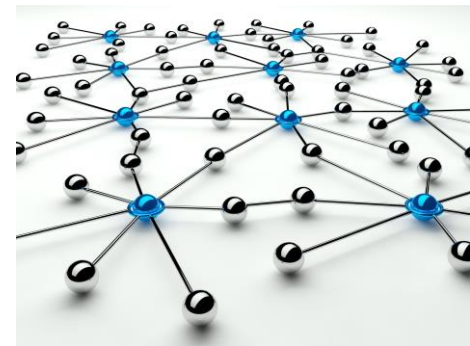
Hálózati architektúrák és protokollok

11. ALKALMAZÁSI RÉTEG MECHANIZMUSOK

Előadó: Dr. Gál Zoltán

Debreceni Egyetem Informatikai Kar

2017. február 16.



Tartalom

- 1) Alkalmazási réteg protokollok IP felett
- 2) Tartománynév feloldó rendszer (DNS)
- 3) Fájllátviteli protokoll (FTP, TFTP, SFTP)
- 4) Távoli bejelentkezés (TELNET, SSH)
- 5) Hipertext transzport protokoll (HTTP, HTTPS)
- 6) Elektronikus levélküldés (SMTP, MIME, POP, IMAP)
- 7) Hálózatmenedzsment (SNMP, RMON)

1. Alkalmazási réteg protokollok IP felett

Megfontolások:

- A hálózati alkalmazás által nyújtott szolgáltatás több csomóponton fut párhuzamosan.
- Bizonyos szolgáltatások háttérben működnek a felhasználói alkalmazások számára.
- Szerver-kliens modell jól használhatóvá teszi a szolgáltatásokat.
- Szerver gépek is vehetnek igénybe szerver szolgáltatásokat.
- Szerver szolgáltatás címezése: (IP cím, Port cím, URL).
- Üzenet tartalma könnyen hozzáférhető, ezért szükséges bizonyos esetekben:
 - Az üzenet titkosítása.
 - A feladó és az üzenet hitelességének ellenőrzése.
 - Az üzenet időbeni kézbesítése.
- Bizonyos alkalmazási protokollok éppen a titkossághoz és a hitelességhez szükséges azonosítókat, kulcsokat továbbítanak.
- Szabványos programozói felületen (API – Application Programming Interface) keresztül lehet tartalmat továbbítani.

1. Alkalmazási réteg protokollok IP felett

Alkalmazási réteg funkciók:

- Alkalmazás entitások között PDU (üzenet) kézbesítése.
- Kézbesítés: hiteles és hibamentes.
- Bizonyos alkalmazásoknál: sorrendiség és időbeliség.
- Hálózati objektum egyértelmű azonosítása.
- API felület biztosítása operációs rendszer függő:
 - Linux/Unix: /etc/services
 - Windows: c:\Windows\system32\drivers\etc\services

Pl.:

```
echo          7/tcp
echo          7/udp
discard       9/tcp      sink null
discard       9/udp      sink null
sysstat       11/tcp      users           #Active users
sysstat       11/udp      users           #Active users
daytime       13/tcp
daytime       13/udp
qotd          17/tcp      quote          #Quote of the day
qotd          17/udp      quote          #Quote of the day
chargen       19/tcp      ttytst source  #Character generator
chargen       19/udp      ttytst source  #Character generator
ftp-data      20/tcp
ftp           21/tcp      #FTP, data
ftp           21/tcp      #FTP. control
ssh           22/tcp      #SSH Remote Login Protocol
telnet        23/tcp
smtp          25/tcp      mail           #Simple Mail Transfer Protocol

.....

directplaysrvr 47624/tcp      #Direct Play Server
directplaysrvr 47624/udp      #Direct Play Server
```

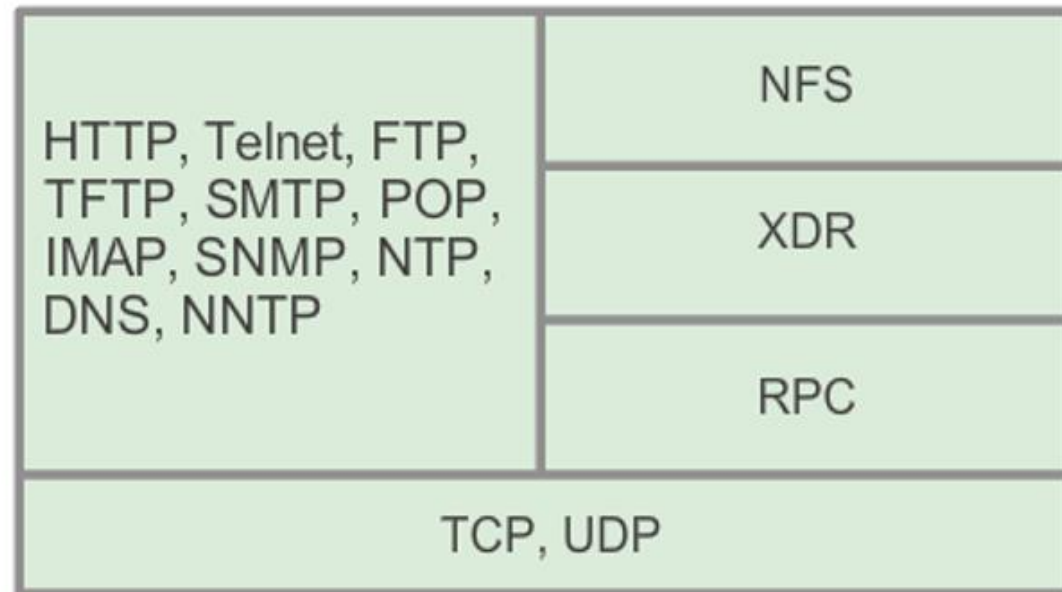
1. Alkalmazási réteg protokollok IP felett

Alkalmazás szintű protokollok:

OSI referencia modell



TCP/IP referencia modell



Név	Protokoll	Név	Protokoll	Név	Protokoll
HTTP	HiperText Transfer P	SMTP	Simple Mail Transfer P	NTP	Network Time P
TELNET	Telnet	POP	Post Office P	DNS	Domain Name System
FTP	File Transfer Protocol	IMAP	Internet Message Access P	NNTP	Network News Transfer P
TFTP	Trivial FTP	SNMP	Simple Network Management P		

2. Tartománynév feloldó rendszer (DNS)

Megfontolások:

- A felhasználók neveket könnyebben észben tartanak, mint számokat (IPv4, IPv6).
- Bizonyos szolgáltatások szöveges azonosítója kitalálható (cég neve, szolgáltatás típusa, stb.)
- Protokollok számok segítségével azonosítják a hálózati objektumokat.
- Alkalmazás programok igénye: névazonosító → számazonosító.
- Üzemeltetők és biztonsági alkalmazások: számazonosító → névazonosító.
- Több névazonosítóhoz tartozhat ugyanazon számazonosító.
- Adott számazonosító egyértelműen azonosítja az interfészt.
- Összerendelések, változások gyors érvényesítése az Interneten.

Domain Name System (DNS, RFC 1034, 1035) funkciók:

- Feloldások: névazonosító → számazonosító; számazonosító → névazonosító.
- Hierarchikus névtér: fa struktúra.
- Osztott adatbázis: felhasználói tartományonként/csoportonként kiszolgáló.
- Hierarchikus kiszolgálói struktúra: szigorú összerendelés a névtérrel.
- Kiszolgáló: DNS szerver átmeneti tárolási (cache) lehetőséggel.
- Névfeloldás érvényessége: elévülési idő (viszonylag lassú változás).
- Szolgáltatás biztonság: redundancia.

2. Tartománynév feloldó rendszer (DNS)

DNS rendszer architektúra elemei:

1. DNS névtér és erőforrások
2. DNS adatbázis
3. DNS kiszolgálók és protokoll

1. DNS névtér és erőforrások:

- Internet név: egyedi erőforrás azonosításra alkalmas, max. 253 karakteres sztring.
- DNS névtér: azonosító tagok gráfja.
 - Topológia: fa.
 - Gyökér: „üres” karakter.
 - Csomópont: max. 63 karakter hosszúságú sztring.
 - Él: „.” karakter.
- Legfelső szintű azonosító tag (TLD, Top Level Domain, RFC 920): felelős az IANA.
 - Ország Pl.: hu, au, it, gr, fr, uk
 - Generikus tartomány Pl.: com, edu, gov, mil, org, arpa, bitnet, int, net, info
- Második szintű azonosító tag: felelős az országos szervezet, max. 61 karakter.
 - Tartomány (szervezet, cég) Pl.: unideb.hu, funet.fi
- Harmadik és további szintű azonosító tag: felelős a tulajdonos
 - Tartomány (szervezet, témakör) Pl.: inf.unideb.hu, www.unideb.hu
 - Hosztnév Pl.: ftp.funet.fi

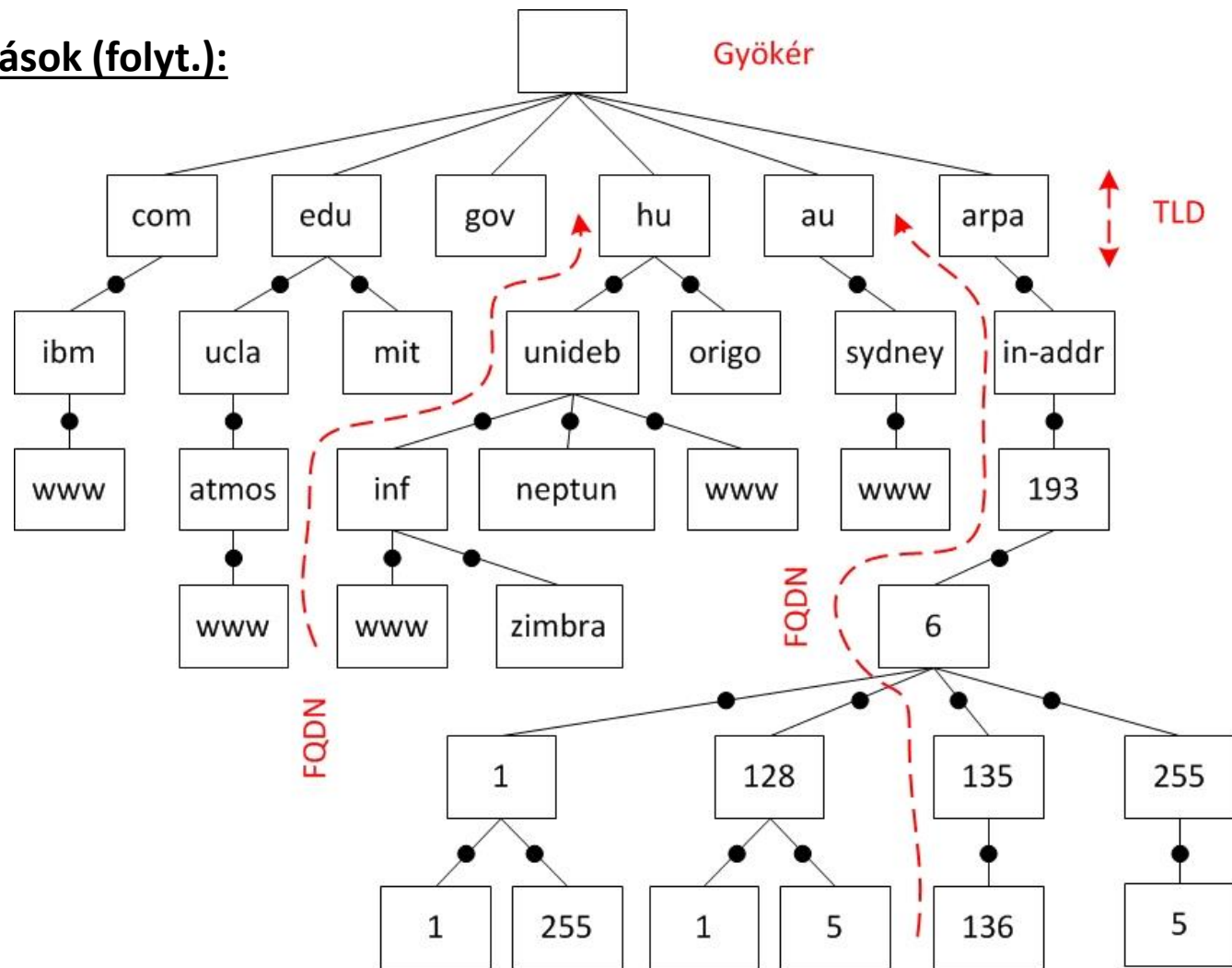
2. Tartománynév feloldó rendszer (DNS)

1. DNS névtér és erőforrások (folyt.):

- Internet erőforrás név szerkezete:
 - „.” karakterrel elválasztott azonosító tagok listája.
 - „ ” karakter tiltott.
- Azonosításra használható karakterek:
 - „a” ... „z” (kis/nagy betű ekvivalens): azonosító tag, hosztnév
 - „0” ... „9” azonosító tag, hosztnév
 - „-” azonosító tag, hosztnév belsejében
 - „_” csak azonosító tag (korlátozottan)
- Erőforrás azonosítása Interneten:
 - Hosztnév (relatív azonosítás) Pl.: webszerver
 - Teljes név (FQDN, Fully Qualified Domain Name): Pl.: webszerver.unideb.hu
- DNS névtér és erőforrás FQDN összerendelési szabálya:
Internet név: azonosítók és élek összeolvasása levéltől gyökérig haladva.

2. Tartománynév feloldó rendszer (DNS)

1. DNS névtér és erőforrások (folyt.):



- FQDN példák:

www.ibm.com

www.inf.unideb.hu

neptun.unideb.hu

136.135.6.193.in-addr.arpa

2. Tartománynév feloldó rendszer (DNS)

2. DNS adatbázis:

- Osztott adatbázis: tartományonkénti szervezés.
- Tartalom hitelesség: IANA-nál (EU: RIPE, www.ripe.net) regisztrált DNS szerver

domain: [6.193.in-addr.arpa](#)
descr: Hungarnet class C block
admin-c: [KG229-RIPE](#)
tech-c: [NH320-RIPE](#)
zone-c: [NH320-RIPE](#)
mnt-by: [NIIF-MNT](#)
created: 2002-08-21T09:41:15Z
last-modified: 2013-04-26T06:33:40Z
source: RIPE
nserver: ns.ripe.net
nserver: ns5.univie.ac.at
nserver: ns2.sztaki.hbone.hu
nserver: ns2.iif.hu
nserver: kubiak.iif.hu

person: Zoltan Gal
address: Debreceni Egyetem
address: University of Debrecen
address: Egyetem ter 1
address: H-4032 Debrecen
address: Hungary
phone: +36 52 52 512900 ext 2509
fax-no: +36 52 533680
e-mail: zgal@unideb.hu
nic-hdl: [ZG4-RIPE](#)
created: 1970-01-01T00:00:00Z
last-modified: 2004-02-19T12:37:00Z
mnt-by: [RIPE-NCC-LOCKED-MNT](#)
source: RIPE

role: NIIF Hostmaster
address: NIIF Office
address: NIIF Intézet
address: Victor Hugo u. 18-22.
address: H-1132 Budapest
address: Hungary
phone: +36 1 450-3070
fax-no: +36 1 2709650
e-mail: hostmaster@iif.hu
abuse-mailbox: abuse@iif.hu
admin-c: [NP3129-RIPE](#)
tech-c: [NP3129-RIPE](#)
nic-hdl: [NH320-RIPE](#)
remarks: hostmaster on duty
created: 2002-08-21T09:30:04Z
last-modified: 2016-04-05T11:56:14Z
mnt-by: [RIPE-NCC-LOCKED-MNT](#)
source: RIPE

person: Katalin Ganzler
address: Information Infrastructure Development Program
address: IIF
address: Pf. 498.
address: H-1396 Budapest 62
address: Hungary
org: [ORG-HHAN1-RIPE](#)
abuse-mailbox: abuse@iif.hu
phone: +36 1 4503060
fax-no: +36 1 3506750
e-mail: hostmaster@iif.hu
notify: hostmaster@iif.hu
nic-hdl: [KG229-RIPE](#)
mnt-by: [NIIF-MNT](#)
created: 1970-01-01T00:00:00Z
last-modified: 2009-12-21T16:23:52Z
source: RIPE

organisation: [ORG-UA110-RIPE](#)
e-mail=csirt@unideb.hu, abuse-mailbox=csirt@unideb.hu

person: [KE357-RIPE](#)
e-mail=ecsedi@unideb.hu

person: [ZG4-RIPE](#)
e-mail=zgal@unideb.hu

2. Tartománynév feloldó rendszer (DNS)

2. DNS adatbázis (folyt.):

- Adatbázis: zónafájlban felsorolt erőforrásrekordok.
- Erőforrásrekord (RR, Resource Record): névtartomány információk.
 - Tulajdonos (sztring): szülő elem a fa struktúrában.
 - Osztály (16 bit): protokollcsalád azonosító (IN: Internet, CH: Chaosnet).
 - Elévülési idő (TTL, 32 bit): érvényesség időtartama [sec].
 - Típus (16 bit) – Adat értékek: összerendelések.

Típusazonosító	Adat	Leírás
A	32 bites IPv4 cím decimális formátumban	Tulajdonos hálózati címe
AAAA	128 bites IPv6 cím hexadecimális formátumban	Tulajdonos hálózati címe
CNAME	Tartománynév	Alias név - kanonikus név összerendelés
HINFO	Magyarázó szöveg	Hardver/szoftver jellemzők
MX	16 bites prioritás érték és tartománynév	Levelező szerver megadása
NS	Zóna (részfá) tartományneve	Tartomány DNS szerverének neve
PTR	Tartománynév	Visszirányú fordítás
SOA	Leíró mezők	Hitelességi jellemzők zóna fájlként

2. Tartománynév feloldó rendszer (DNS)

2. DNS adatbázis (folyt.):

- SOA rekord: zónafájlönkénti hitelesítő leírás.
 - Elsődleges kiszolgáló neve.
 - Kiszolgáló elektronikus levelezési címe.
 - Zóna fájl sorozatszám: frissítés másodlagos kiszolgáló számára.
 - Frissítési periódus: másodlagos kiszolgáló számára.
 - Újrapróbálkozási periódus: másodlagos kiszolgáló számára.
 - Elévülési idő: másodlagos kiszolgálók számára.
 - Elévülési idő: lekérdezők számára.

ibm.com

```
primary name server = asia3.akam.net
responsible mail addr = hostmaster.akamai.com
serial = 1481923691
refresh = 43200 (12 hours)
retry = 7200 (2 hours)
expire = 604800 (7 days)
default TTL = 3600 (1 hour)
```

unideb.hu

```
primary name server = domser.unideb.hu
responsible mail addr = dns.unideb.hu
serial = 201612180
refresh = 43200 (12 hours)
retry = 14400 (4 hours)
expire = 604800 (7 days)
default TTL = 86400 (1 day)
```

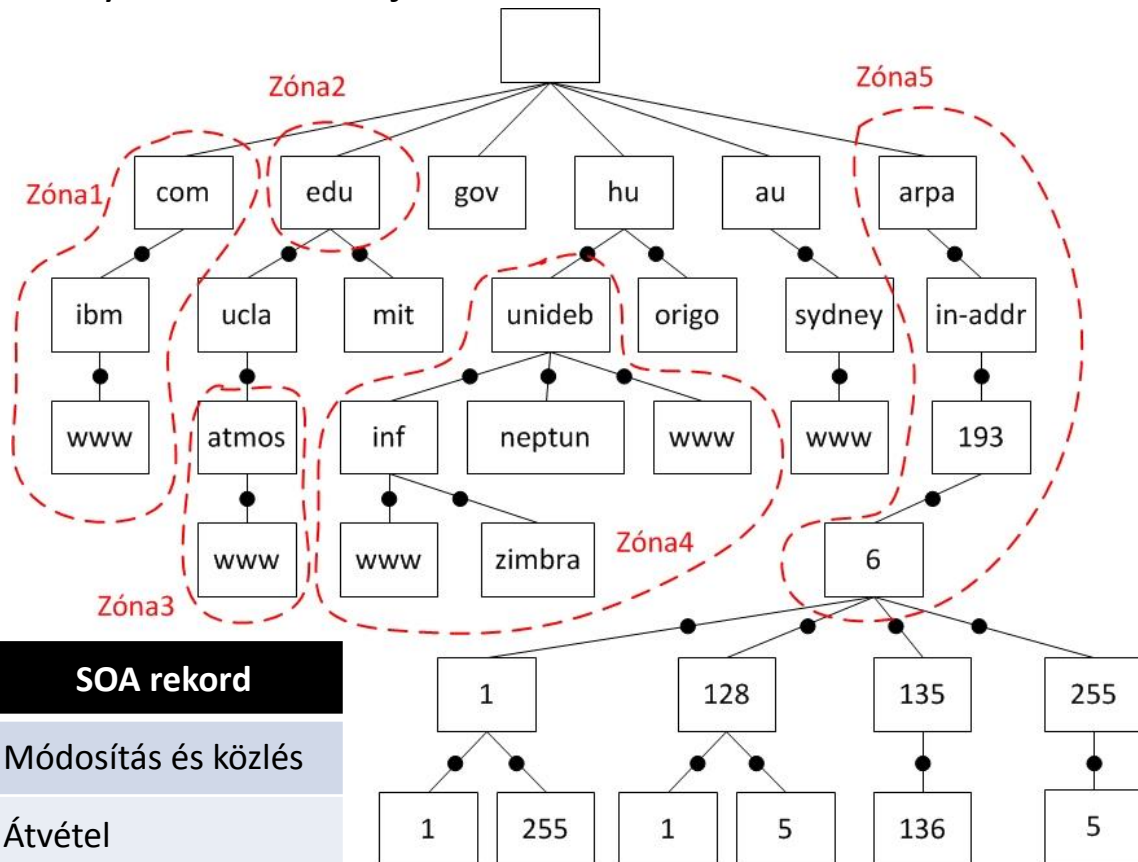
128.6.193.in-addr.arpa

```
primary name server = domser.unideb.hu
responsible mail addr = dns.domser.unideb.hu
serial = 201612180
refresh = 43200 (12 hours)
retry = 14400 (4 hours)
expire = 604800 (7 days)
default TTL = 86400 (1 day)
```

2. Tartománynév feloldó rendszer (DNS)

3. DNS kiszolgálók és protokoll:

- DNS kiszolgáló: lefedett névtartomány adatai zónafájlokban.
- DNS kiszolgáló típusok:
 - Elsődleges: csak egy darab.
 - Másodlagos: bármennyi.
 - Cache: bármennyi
- DNS funkció halmozás:
 - Több zónanév kezelése.
- DNS zóna delegálása:
 - Zónafájl átadása másik NS-hez.



DNS kiszolgáló típus	Zónafájl	SOA rekord
Elsődleges	Módosítás és közlés	Módosítás és közlés
Másodlagos	Átvétel	Átvétel
Cache	Átvétel	Átvétel

2. Tartománynév feloldó rendszer (DNS)

3. DNS kiszolgálók és protokoll (folyt.): Gyökér (Root) DNS kiszolgálók (IANA)

Gyökér DNS kiszolgáló	IP címek	Üzemeltető
a.root-servers.net	198.41.0.4, 2001:503:ba3e::2:30	VeriSign, Inc.
b.root-servers.net	192.228.79.201, 2001:500:84::b	University of Southern California (ISI)
c.root-servers.net	192.33.4.12, 2001:500:2::c	Cogent Communications
d.root-servers.net	199.7.91.13, 2001:500:2d::d	University of Maryland
e.root-servers.net	192.203.230.10, 2001:500:a8::e	NASA (Ames Research Center)
f.root-servers.net	192.5.5.241, 2001:500:2f::f	Internet Systems Consortium, Inc.
g.root-servers.net	192.112.36.4, 2001:500:12::d0d	US Department of Defense (NIC)
h.root-servers.net	198.97.190.53, 2001:500:1::53	US Army (Research Lab)
i.root-servers.net	192.36.148.17, 2001:7fe::53	Netnod
j.root-servers.net	192.58.128.30, 2001:503:c27::2:30	VeriSign, Inc.
k.root-servers.net	193.0.14.129, 2001:7fd::1	RIPE NCC
l.root-servers.net	199.7.83.42, 2001:500:9f::42	ICANN
m.root-servers.net	202.12.27.33, 2001:dc3::35	WIDE Project

2. Tartománynév feloldó rendszer (DNS)

3. DNS kiszolgálók és protokoll (folyt.):

- DNS kérdések és válaszok:
 - Entitáspárok: kliens-kiszolgáló, kiszolgáló-kiszolgáló.
 - PDU: kérdés üzenet, válasz üzenet.
 - Kérdés üzenet: szabványos formátum (pl.)

Fejrész	OPCODE=Standard Query
Kérdés	QNAME=IBM.COM. CLASS=IN TYPE=MX
Válasz	
Hiteles	
További	

- Válasz üzenet(ek): szabványos formátum (pl.)

Fejrész	OPCODE=Standard Query, Response, AA
Kérdés	QNAME=IBM.COM. CLASS=IN TYPE=MX
Válasz	IBM.EDU 3600 IN MX mx0a-001b2d01.pphosted.com MX mx0b-001b2d01.pphosted.com
Hiteles	
További	mx0a-001b2d01.pphosted.com IN A 148.163.156.1 mx0b-001b2d01.pphosted.com IN A 148.163.158.5

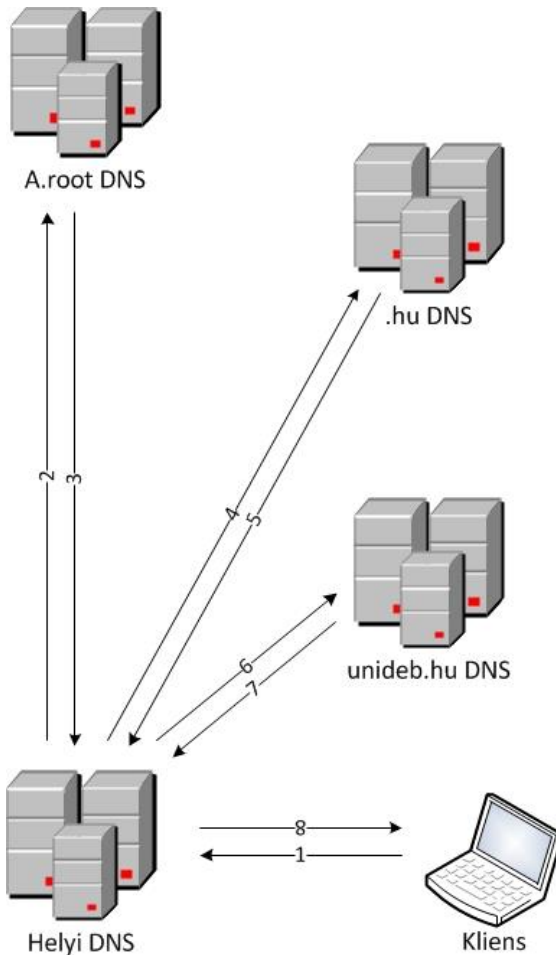
2. Tartománynév feloldó rendszer (DNS)

3. DNS kiszolgálók és protokoll (folyt.):

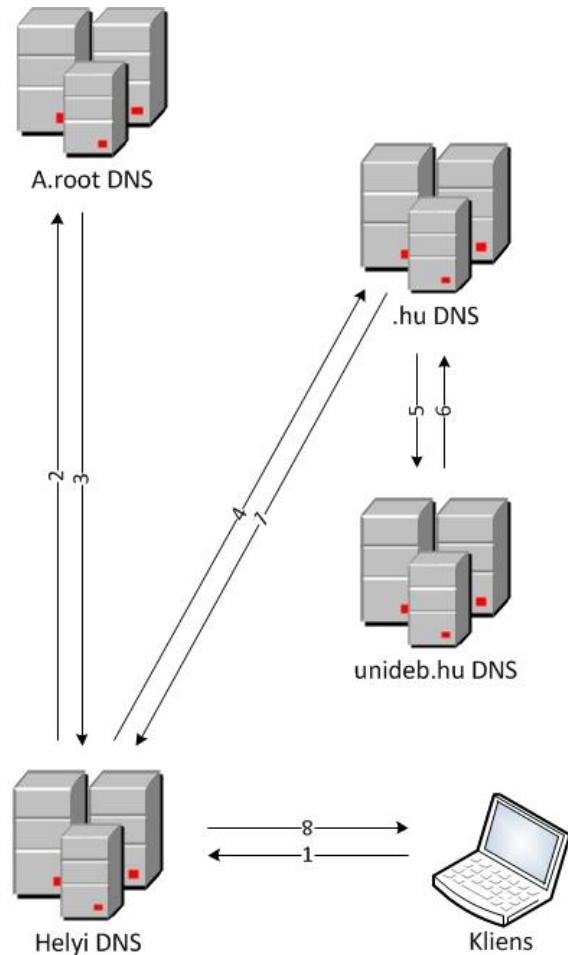
- DNS lekérdezési módszerek:
 - Iteratív: helyi kiszolgáló ismételi.
 - Szerver oldalon a legegyszerűbb megvalósítás.
 - Bármelyik névszerverben implementált.
 - A kliensnek lehetősége nyílik az információk értékelésére.
 - Rekurzív: helyi kiszolgáló csak egyszer kérdez.
 - Kliens oldalon a legegyszerűbb megvalósítás.
 - A szerveren megvalósítható átmeneti tárolás (cache).
 - Opcionális, mind a szerveren, mind a kliensen implementált-nak kell lennie.
- Szerver válaszolási módszer típusa: RA bit minden válaszban.
- Kliens lekérdezési módszer típusa: RD bit a kérdésben.
- Válasz tartalma: egy vagy több RR rekord
 - Sikeres feloldás: érték vagy lista.
 - Sikertelen feloldás: név nem létezik; név létezik, de adat nem; másik NS-re irányítás.

2. Tartománynév feloldó rendszer (DNS)

3. DNS kiszolgálók és protokoll (folyt.):



Iteratív lekérdezési módszer

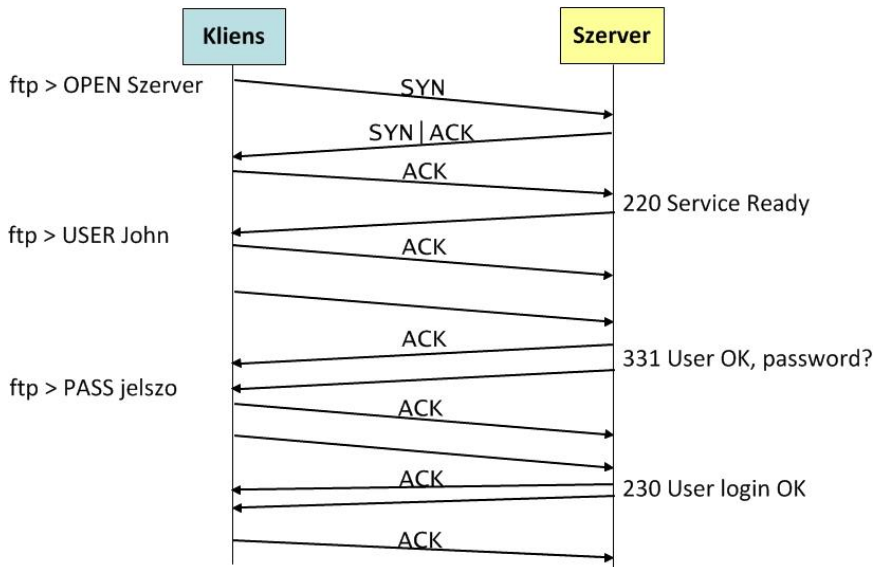


Rekurzív lekérdezési módszer

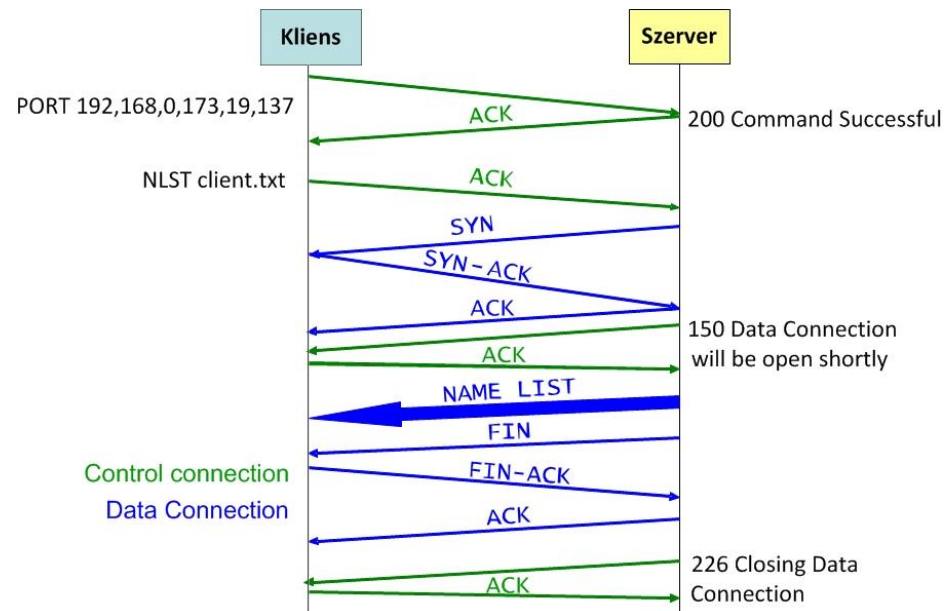
3. Fájlátviteli protokoll (FTP, TFTP, SFTP)

Funkciók:

- Fájlok biztonságos (SFTP) (TFTP-nél nem biztonságos) és hatékony megosztása (RFC 959).
- Távoli gépek közvetett felhasználása.
- Különböző operációs rendszerek lokális reprezentációja közötti konverzió:
 - Címzés fájlrendszerben (fájlnevek, alkönyvtár utak)
 - Fájlok belső szerkezete (Pl. ASCII, EBCDIC karakter készlet).
- Szerver-kliens architektúra: kapcsolat felépítés, adatátvitel, kapcsolat lebontás.



Kapcsolat felépítés



Nyugtázott adatátvitel

3. Fájlátviteli protokoll (FTP, TFTP, SFTP)

FTP kapcsolat csatornái:

- Kontroll csatorna (folyamatos):
 - Szerver: passzív OPEN a TCP 21 porton.
 - Kliens: aktív OPEN rövididejű TCP porton.
 - Szerver: lezárja a kapcsolatot.
- Adat csatorna (rövididejű):
 - Kliens: passzív OPEN rövididejű porton.
 - Kliens: rövididejű portazonosító elküldése szerverhez PORT paranccsal.
 - Szerver: aktív OPEN a TCP 20 porton.

TFTP működése:

- Fájl írása/olvasása távoli szerverrel (tipikusan konfigurációs és image fájlok).
- Nincs alkönyvtár listázás.
- UDP felett működik.
- Továbbítási protokoll egyetlen csatornán: „Stop and Wait”.
- Nincs autentikációs eljárása.
- Öt különböző üzenet formátum: RRQ (Read Remote Query), WRQ (Write Remote Query, DATA, ACK, ERROR).

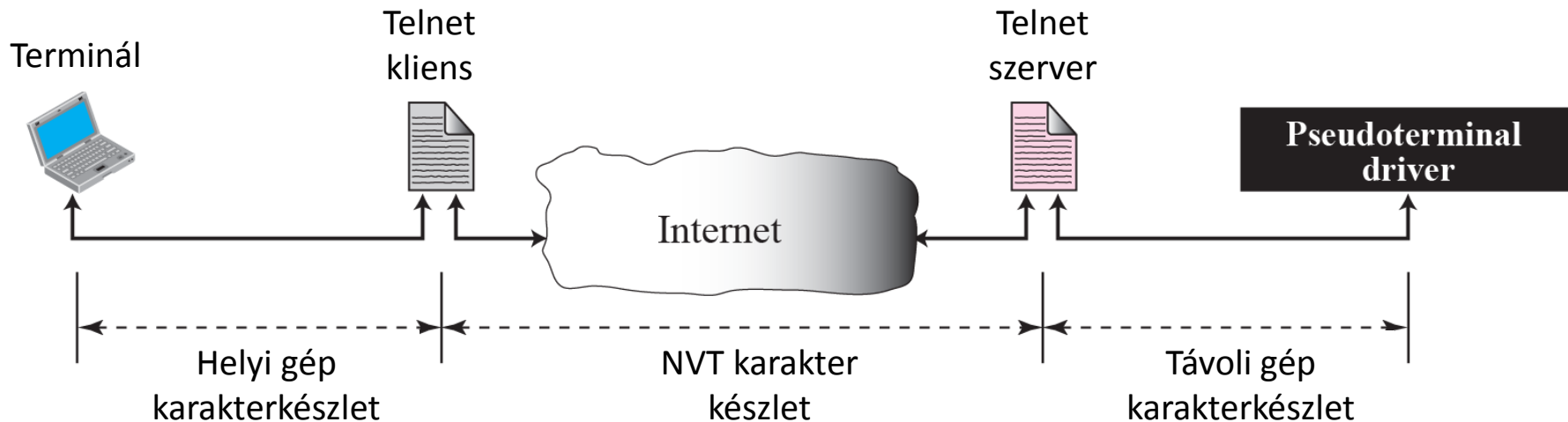
4. Távoli bejelentkezés (TELNET, SSH)

Megfontolások:

- Távoli gépekre bejelentkezés parancsok/alkalmazások végrehajtása céljából.
- Szerver-kliens architektúra.
- Alkalmazástól függően a kommunikáció biztonsága magas vagy alacsony lehet.

TELNET (Terminal NETwork, RFC 854):

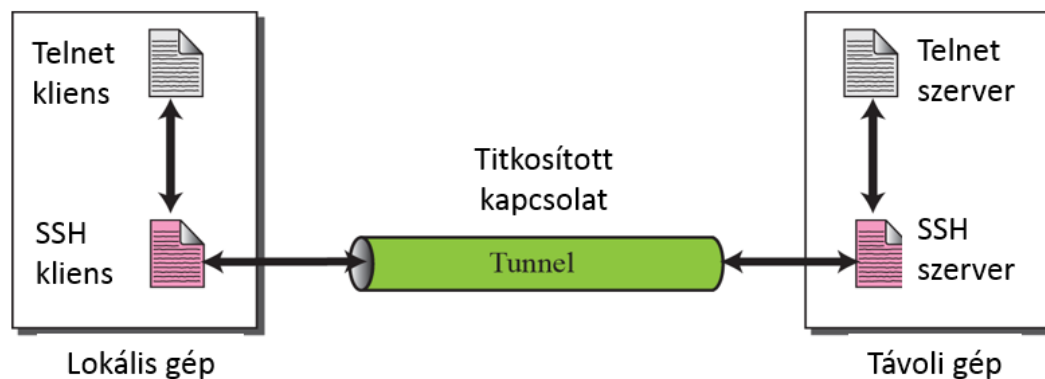
- NVT (Network Virtual Terminal): hálózati virtuális terminál
- Szállítási réteg: TCP.
- Tartalom karakter: adat 0XXX.XXXX
- Parancs karakterrel: kontroll 1XXX.XXXX



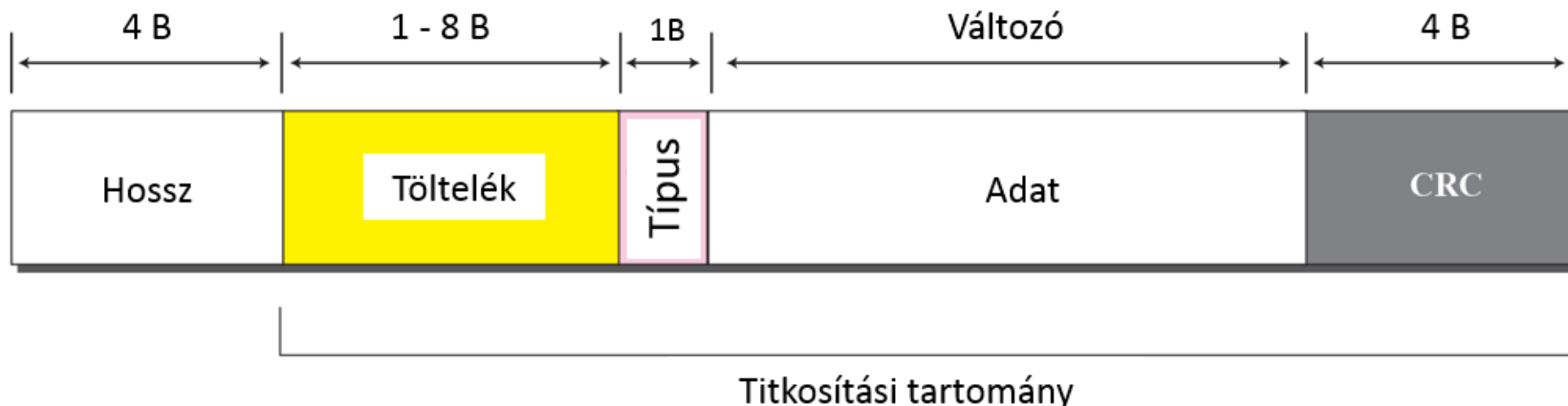
4. Távoli bejelentkezés (TELNET, SSH)

SSH (Secure Shell, RFC 4252):

- NVT (Network Virtual Terminal): hálózati virtuális terminál.
- Szállítási réteg: TCP.
- Funkciók: több, mint a Telnet.
- Kommunikáció: titkosított.



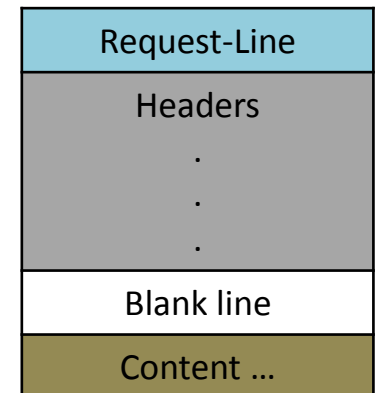
SSH PDU üzenet szerkezete: hossz, töltelék, típus, adat, CRC.



5. Hipertext transzfer protokoll (HTTP, HTTPS)

Funkciók és működés:

- RFC 1945 (HTTP 1.0), RFC 2616 (HTTP 1.1).
- Hálózati objektumok továbbítása kliens-szerver között.
- Objektum azonosítás:
 - URL (Universal Resource Locator): hálózati hely.
 - Pl.: `http://www.inf.unideb.hu`
`https://ugyfelkapu.magyarorszag.hu/`
 - URI (Universal Resource Identifier): objektum (fájl) abszolút vagy relatív azonosítója.
 - Pl.: `http://hostname[:port]/path` `http://www.inf.unideb.hu:80/a/b/szerver/a/b`
- PDU üzenet: titkosítatlan (HTTP), titkosított (HTTPS).
 - HTML (Hypertext Markup Language) oldal: hivatkozott objektumok és formátum.
- Szállítási réteg: TCP:80, TCP:443; UDP:80, UDP:443.
- PDU üzenet: **Kérelem**.
 - **Request-Line**: ASCII szöveg: GET, HEAD, POST, *CRLF*.
PUT, DELETE, OPTIONS, TRACE.
 - **Headers**: kliens jellemzői szerver felé, *CRLF*.
 - **Blank line**: elválasztó jel a Header és a Content között.
 - **Content**:



5. Hipertext transzfer protokoll (HTTP, HTTPS)

Funkciók és működés (folyt.):

Kérelem (Request) fejrészek:

Header név	Leírás
Accept	Böngésző által elfogadott tartalom típusa (Pl.: text/html).
Accept-Charset	Böngésző által várt karakterkészlet
Accept-Encoding	Böngésző által elfogadott adatkódolás
Accept-Language	Böngésző által várt nyelv (default: angol)
Authorization	Böngésző azonosítása a szervernél

5. Hipertext transzfer protokoll (HTTP, HTTPS)

Funkciók és működés (folyt.):

- Pl. GET Request:

GET /~pictures/list.html HTTP/1.1

Accept: */*

Host: www.valami.valahol.hu

User-Agent: Internet Explorer

From: valaki@levelcim.hu

Referer: http://ott.hu



Üres sor itt!

- Pl. POST Request:

POST /~pictures/list.html HTTP/1.1

Accept: */*

Host: www.valami.valahol.hu

User-Agent: Internet Explorer

Content-length: 35

Referer: http://www.gogle.hu/id



Üres sor itt!

stuid= 1234567890&item=test1&grade=99

5. Hipertext transzfer protokoll (HTTP, HTTPS)

Funkciók és működés (folyt.):

- PDU üzenet: **Válasz**.
 - **Status-Line**: HTTP-Version Status-Code Message.
Status Code: 3 számjegyű szám.
Message: ember által értelmezhető szöveg.
 - **Headers**: válasz entitás leírása (típus, méret, kódolás, dátum)
 - **Blank line**: elválasztó jel a Header és a Content között.
 - **Content**: bármilyen tartalom, típusazonosító fejrészsel együtt.

- Pl.: Válasz header

Date: Tue, 20 Dec 2016, 15:43:17 CET

Server: Apache/1.17

Content-Type: test/html

Content-Length: 1756

Content-Encoding: gzip

Tartalom



Üres sor itt!

Status-Line
Headers . . .
Blank line
Content ...

5. Hipertext transzfer protokoll (HTTP, HTTPS)

Funkciók és működés (folyt.):

Válasz (Response) fejrészek:

Header név	Leírás
Content-Encoding	Válasz tartalomrészének kódolási típusa
Content-Language	Válasz tartalomrészének nyelve (default: angol)
Content-Length	Válasz tartalomrészének mérete [B]
Content-Type	Válasz tartalomrészének típusa (Pl.: text/html)
Date	Adatküldés kezdődik.
Expires	Adat érvényességi dátuma
Forwarded	Böngésző és szerver közötti köztes gép továbbít
Location	Dokumentum új URL-jéhez átirányítás
Server	Választ küldő szerver tulajdonságai

- **Szerver terhelésének megosztása: proxy/cache szerver (forwarder)**

6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Megfontolások:

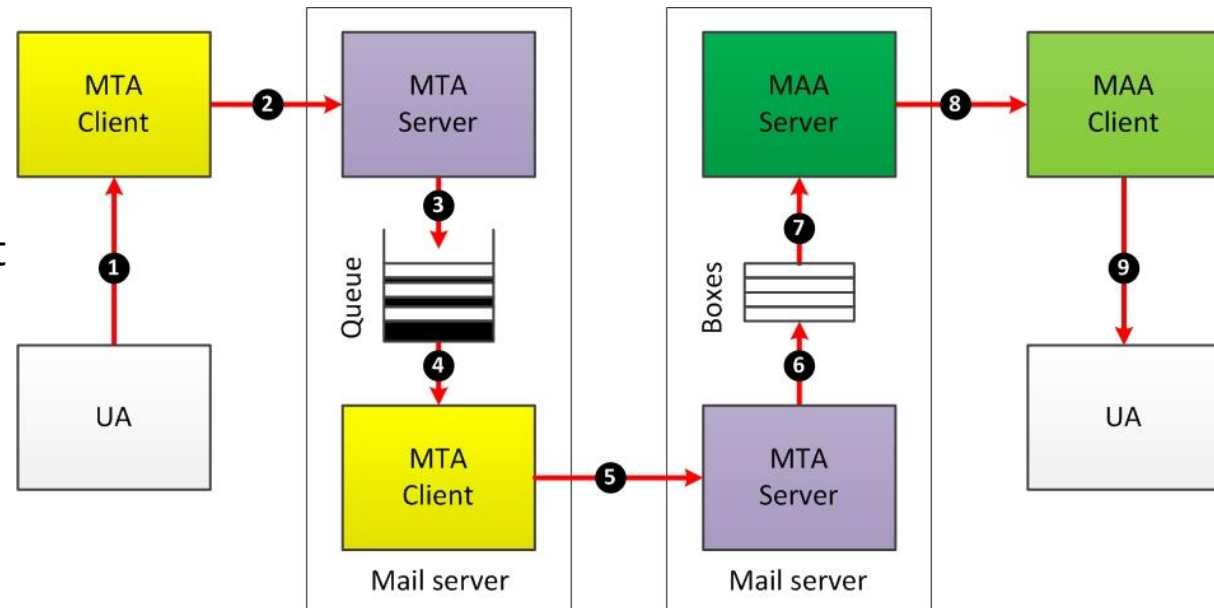
- Emberek közötti információcsere: valós idejű (online), késleltetett (offline).
- Elektronikus levelezés: alkalmazás szintű offline információcsere.
- Szállítási réteg: TCP
- Felhasználás (intenzitás, penetráció) egyre növekszik.
- Leginkább támadott Internet alkalmazás: spam, vírus.
- Biztonsági megoldások: DNS, tűzfal, spam-szűrő.

Elektronikus levélküldési rendszer felépítése:

UA – User Agent

MTA – Message Transfer Agent

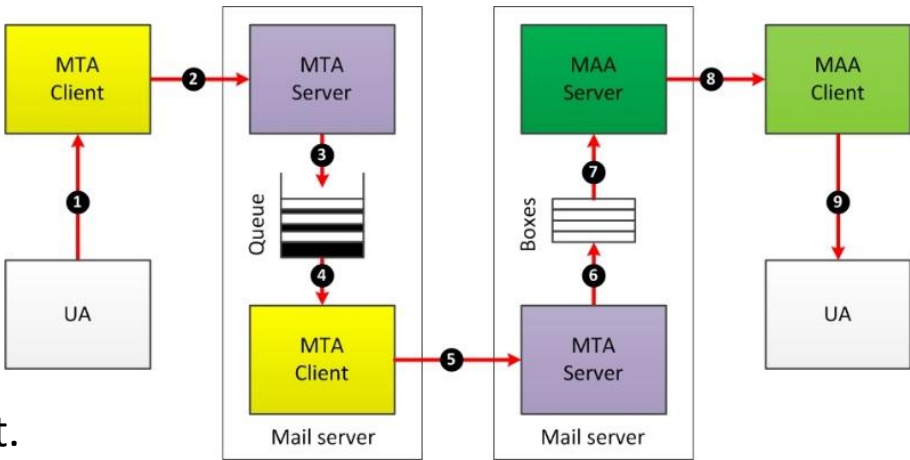
MAA – Message Access Agent



6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus levélküldési rendszer működése:

- Üzenet átvadási formák:
 - MTA kliens → MTA szerver (**PUSH**):
Üzenet: MTA kliens → MTA szerver
 - MAA szerver → MAA kliens (**PULL**):
Kérelem: MAA kliens → MAA szerver
Válasz: MAA szerver → MAA kliens
- Felhasználói ügynök (UA): felhasználói felület.
- Levéltovábbító ügynök (MTA):
 - MTA kliens: üzenetfogadás (1, 4), üzenetküldés (2, 5).
 - MTA szerver: üzenetfogadás (2, 5), üzenetküldés (3, 6).
- Levélkézbesítő ügynök (MAA):
 - MAA kliens: üzenetfogadás (8), üzenetküldés (9).
 - MAA szerver: üzenetfogadás (7), üzenetküldés (8).
- Levelező szerver: postafiók és/vagy gateway funkciók.
- Kommunikációs viszonylatonkénti protokollok:
 - SMTP, MIME, HTTP, POP3, IMAP4.

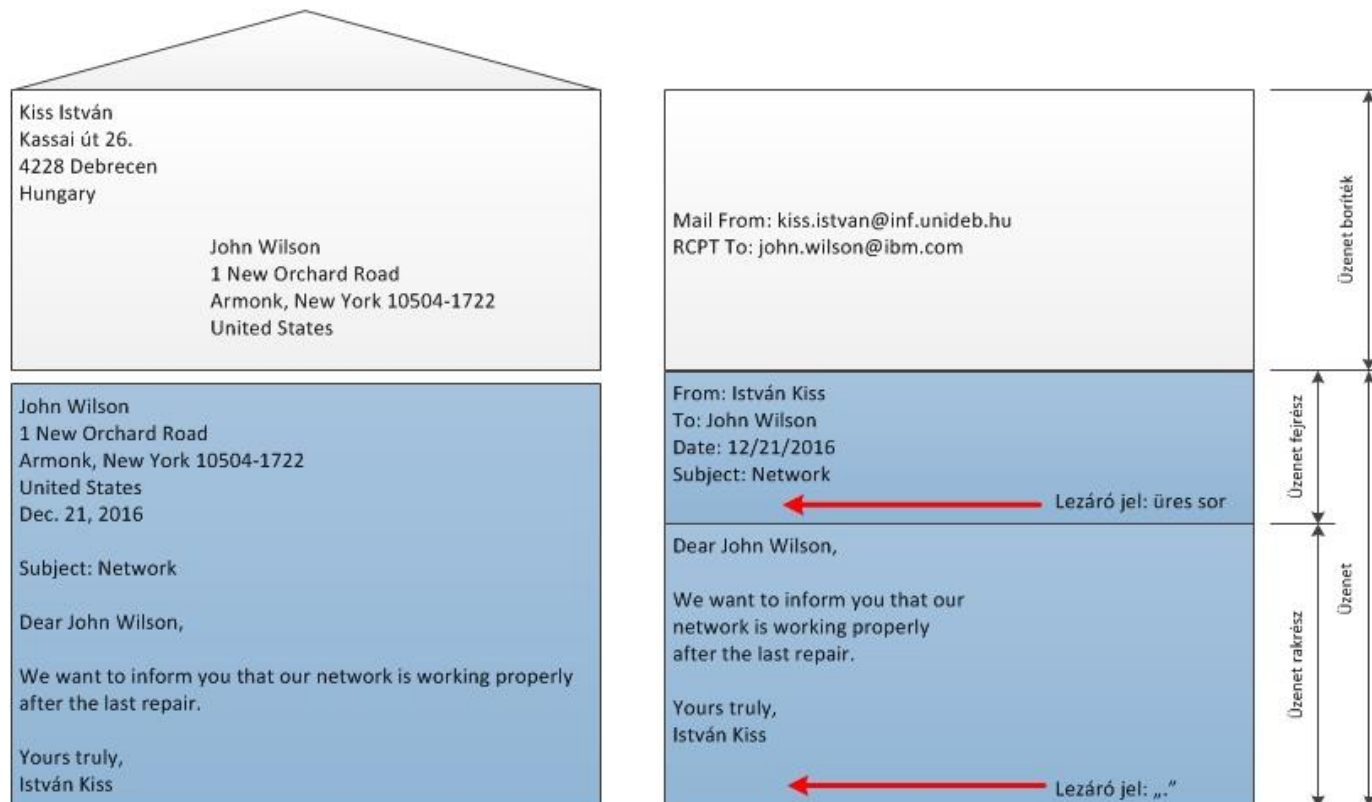


Protokoll	Viszonylat	Port
SMTP	2, 3, 4, 5, 6, 7, 8	TCP:25
MIME	2, 8	SMTP
HTTP	2, 8	TCP:80
POP3	7, 8	TCP:110
IMAP4	7, 8	TCP:143

6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus üzenet szerkezete:

- Boríték: üzenet elején, MTA/MAA szervereknek szóló információk.
- Üzenet:
 - Üzenet fejrész: címzett e-mail címe, feladó e-mail címe, dátum, téma, stb.
 - Üzenet rakrész: szöveg és/vagy csatolmány (állományok).



6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus levél szerkezete: Példa

Szerver postaláda:

```
From kissel@mail.acad.ece.udel.edu Tue Oct 25 20:27:21 2005
Return-Path: <kissel@mail.acad.ece.udel.edu>
X-Original-To: kissel@cis.udel.edu
Delivered-To: kissel@cis.udel.edu
```

Szerver és levél útvonal:

```
Received: by mail.eecis.udel.edu (Postfix, from userid 62)
        id 8EC8D18D; Tue, 25 Oct 2005 20:27:21 -0400 (EDT)
Received: from mail.acad.ece.udel.edu (devil-rays.acad.ece.udel.edu
[128.4.60.10])
        by mail.eecis.udel.edu (Postfix) with ESMTP id 59888C9
        for <kissel@cis.udel.edu>; Tue, 25 Oct 2005 20:27:20 -0400 (EDT)
Received: by mail.acad.ece.udel.edu (Postfix, from userid 62)
        id 344482045; Tue, 25 Oct 2005 20:27:20 -0400 (EDT)
Received: from nimbus.acad.ece.udel.edu (nimbus.acad.ece.udel.edu [128.4.63.34])
        by mail.acad.ece.udel.edu (Postfix) with ESMTP id 3932E1ECA
        for <kissel@cis.udel.edu>; Tue, 25 Oct 2005 20:27:19 -0400 (EDT)
Date: Tue, 25 Oct 2005 20:27:19 -0400 (EDT)
```

Fogadó postaláda:

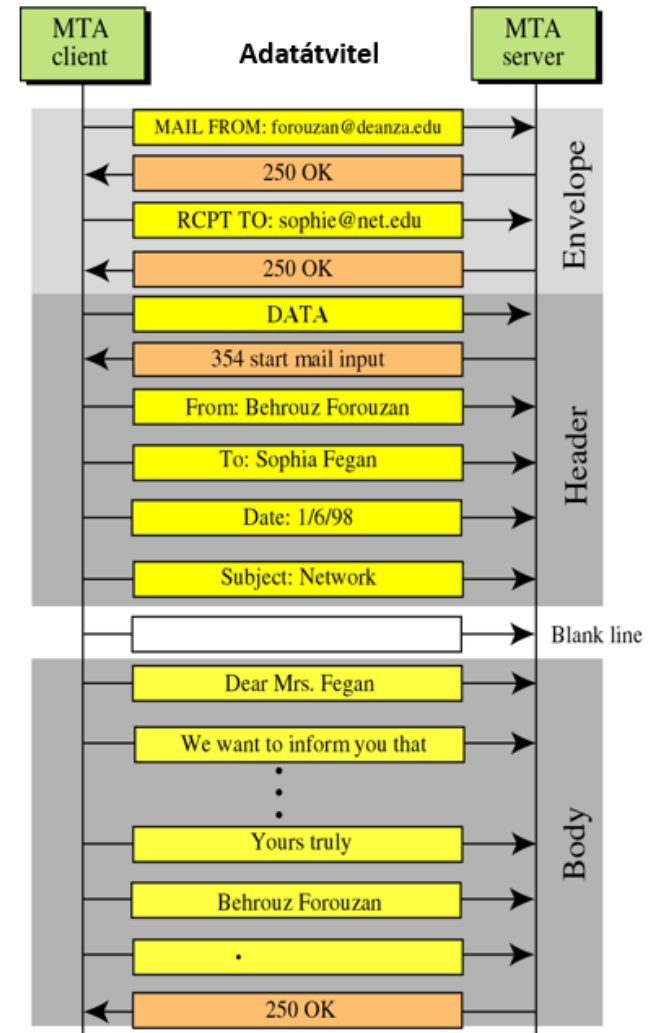
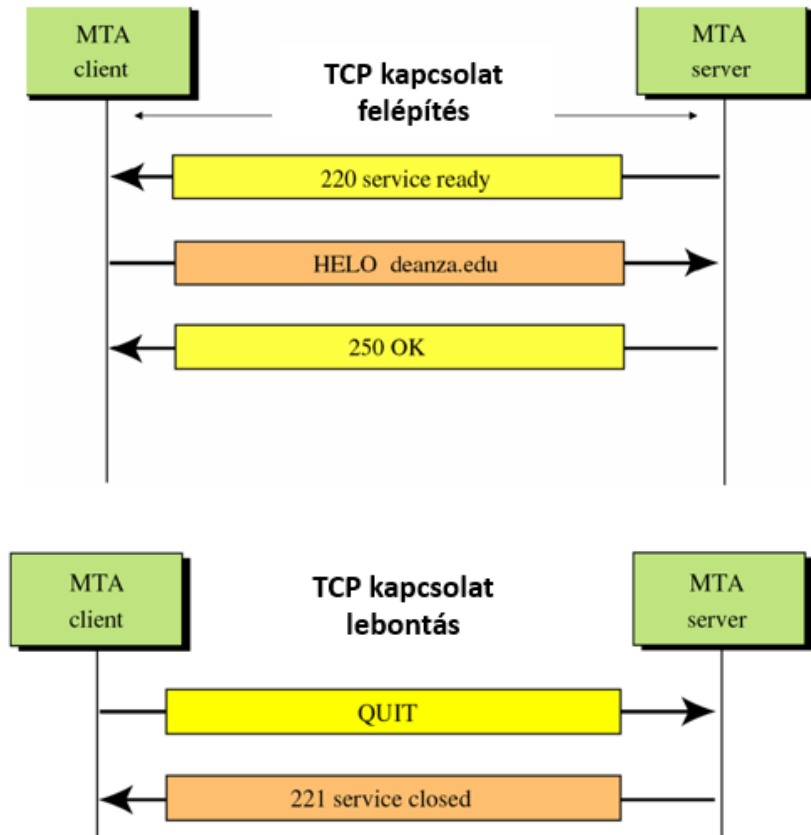
```
From: Ezra Kissel <kissel@mail.acad.ece.udel.edu>
X-X-Sender: kissel@nimbus.acad.ece.udel.edu
To: kissel@cis.udel.edu
Subject: email test
Message-ID: <Pine.LNX.4.62.0510252026550.4176@nimbus.acad.ece.udel.edu>
X-Sanitizer: This message has been sanitized!
X-Sanitizer-URL: http://mailtools.anomy.net/
X-Sanitizer-Rev: UDEL-ECECIS: Sanitizer.pm,v 1.64 2002/10/22 MIME-Version: 1.0
X-Spam-Checker-Version: SpamAssassin 3.0.4 (2005-06-05) on louie.udel.edu
X-Spam-Level:
X-Spam-Status: No, score=-3.8 required=4.1 tests=ALL_TRUSTED,BAYES_00
        autolearn=ham version=3.0.4
X-Sanitizer: This message has been sanitized!
X-Sanitizer-URL: http://mailtools.anomy.net/
X-Sanitizer-Rev: UDEL-ECECIS: Sanitizer.pm,v 1.64 2002/10/22 MIME-Version: 1.0
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset="US-ASCII"; format=flowed
Status: RO
X-Status:
X-Keywords:
X-UID: 50

This is a test message.
```

6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus üzenetküldés SMTP-vel:

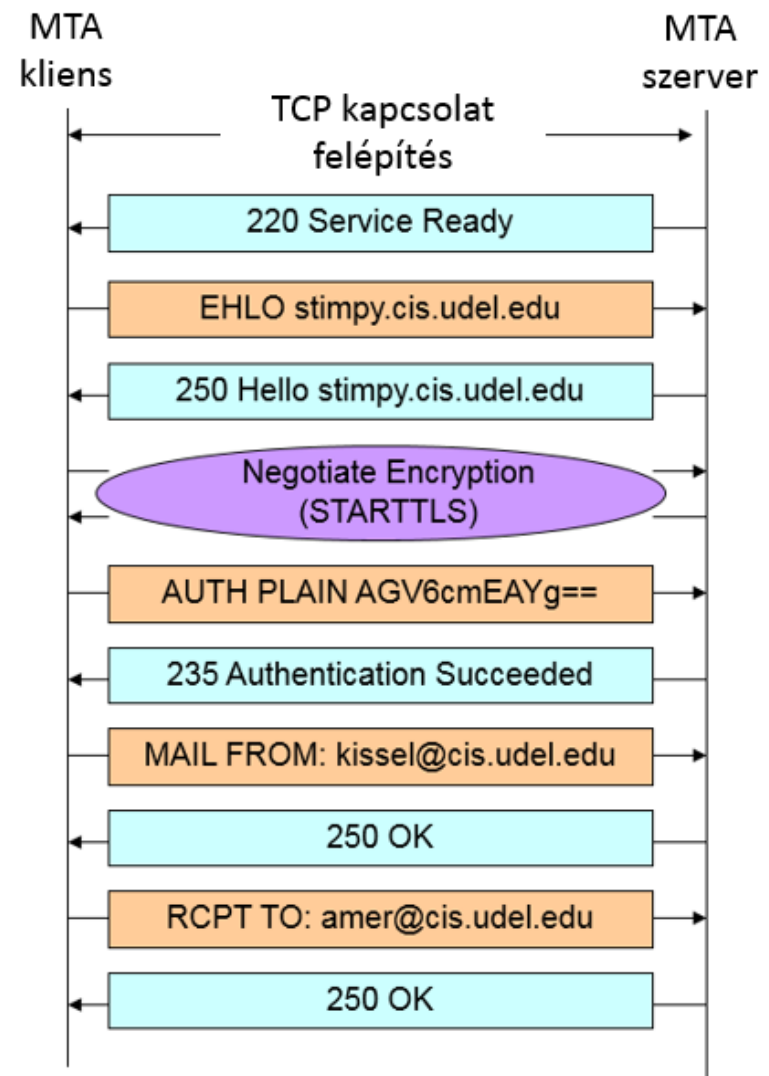
- Üzenet küldése: TCP kapcsolaton.
- Adat: 7 bites NVT (Network Virtual Terminal) ASCII kód.
- Nincs titkosítás.



6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus üzenetküldés SMTP-vel (folyt.):

- Authentikáció (AUTH):
 - Opcionális lehetőség.
 - Módszerek: PLAIN, LOGIN, CRAM-MD5, stb.
 - Szükséges a használata (spam, címhamisítás).



6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus üzenetküldés MIME-vel (Multipurpose Internet Mail Extensions):

- Üzenet küldése: SMTP üzenetben.
- Adat: tetszőleges kódolású (text, alkalmazás, kép, hang, videó), majd kódolása 7 bites NVT (Network Virtual Terminal) ASCII formátumra.

- MIME üzenet: fejrész, rakrész
- MIME üzenet fejrész mezők:

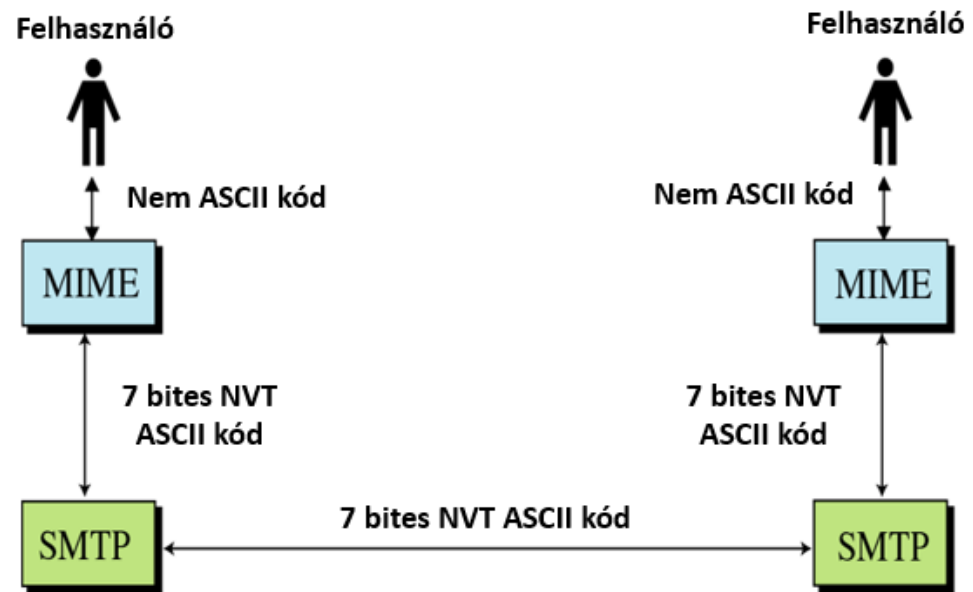
MIME-Version: 1.1

Content-Type: tartalom típus/altípus.

Content-Transfer-Encoding: kódolás neve.

Content-Id: üzenet azonosítója.

Content-Description: nemszöveges tartalom szöveges leírása.



6. Elektronikus levélküldés (SMTP, MIME, POP, IMAP)

Elektronikus üzenetküldés: postafiók hozzáférés

- Postafiók tartalom lekérdezési módszerek:
 - Mindegyik üzenet listában: POP (Post Office Protocol).
 - Csak egyetlen üzenet: IMAP (Internet Mail Access Protocol).

POP v3 (Post Office Protocol):

- Egyszerű, üzenetlista lekérdezése.
- Üzenetek törlése vagy meghagyása a szerveren.
- Szerver erőforrásainak megkímélése.

IMAP v4 (Internet Mail Access Protocol):

- Üzenet letöltése előtt fejrész lekérdezése.
- Üzenetek hozzáférése egyesével.
- Sztring keresés üzenet letöltés előtt.
- Üzenetrész letöltési lehetőség.
- Postafiók adminisztráció a szerveren (létrehozás, törlés, módosítás).

7. Hálózatmenedzsment (SNMP, RMON)

Megfontolások:

- Nagyon sok hálózati objektum együttműködése szükséges a hálózati szolgáltatásokhoz. Szolgáltatások minőségét a kommunikáció erőteljesen befolyásolja.
- Gyors közbeavatkozás szükséges az ISP részéről hiba esetén.
- Minőségi jellemzők lekérdezése és működési paraméterek módosítása igény a felhasználó és a szolgáltató részéről is.
- Szabványos, bővíthető megoldás szükséges: hálózat menedzsment módszerek, hardver és szoftver eszközök (alkalmazások).

Hálózatmenedzsment SNMP-vel:

- SNMP (Simple Network Management Protocol, RFC 1098): v1, v2, v3.
- Alkalmazás szintű protokoll.
- Megjelenítési réteg: ASN.1 (objektumok szervezése)
- Szállítási réteg: UDP:161 (üzenet), UDP:162 (trap üzenet)
- IP címmel rendelkező hálózati objektumok olvasása, írása.
- Kommunikációs komponensek (entitások):
 - Ügynök (Agent): adatot gyűjtő szerver (!).
 - Menedzser (Manager): menedzsment gépen futó kliens (!).
 - Tolmács/átjáró (Proxy/Gateway): köztes csomóponton futó szoftver.
 - SNMP – nemSNMP átjárás; verziók közti átjárás; védelmi szűrés; csoportképzés.

7. Hálózatmenedzsment (SNMP, RMON)

Hálózatmenedzsment SNMP-vel (folyt.):

- Működési módszerek SNMP-nél:
 - Client Pull: menedzsment szoftver lekérdezi az ügynök adatait.
 - Server Push: ügynök értesítést (trap) küld a menedzsment szoftvernek.
- SNMP architektúra elemek:
 - Protokoll: üzenetek formátuma és műveletek: Get, GetNext, GetBulk(v2-től), Set, Trap.
 - Menedzsment információ struktúrája (SMI, BER): objektumok formátuma.
 - Menedzsment információ adatbázis (MIB): hierarchikus szervezés és hozzáférés.
- Menedzselt tartomány (Community): hozzáférési jog (system, read only, read/write).
- SNMP ügynök típusok:
 - Bővíthető: MIB fa részekkel (pl. operációs rendszer).
 - Monolitikus: rögzített MIB struktúra (pl. digitális hőmérő).
- SMI v1/v2 fa struktúra (RFC 1155, RFC 1212, RFC 1215 / RFC 1442, RFC 1443, RFC 1444):
Pl.: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).ibm(2) 1.3.6.1.4.1.2
iso(1).org(3).dod(6).internet(1).mgmt(2).system(1).sysDescr(1) 1.3.6.1.2.1.1

7. Hálózatmenedzsment (SNMP, RMON)

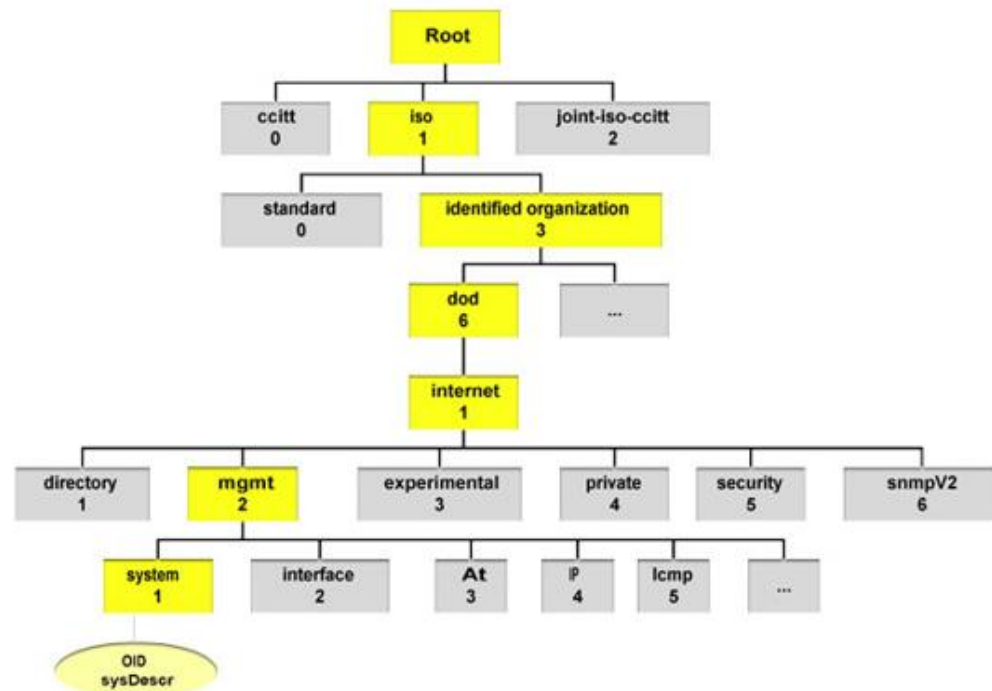
Hálózatmenedzsment SNMP-vel (folyt.):

SMI v1:

```
-- RFC1155 MIB
RFC1155-SMI DEFINITIONS ::= BEGIN
-- the path to the root
org OBJECT IDENTIFIER ::= { iso 3 }
dod OBJECT IDENTIFIER ::= { org 6 }
internet OBJECT IDENTIFIER ::= { dod 1 }
directory OBJECT IDENTIFIER ::= { internet 1 }
mgmt OBJECT IDENTIFIER ::= { internet 2 }
experimental OBJECT IDENTIFIER ::= { internet 3 }
private OBJECT IDENTIFIER ::= { internet 4 }
enterprises OBJECT IDENTIFIER ::= { private 1 }
mib-2 OBJECT IDENTIFIER ::= { mgmt 1 }
END
```

SMI v2:

```
-- RFC 1902
SNMPv2-SMI DEFINITIONS ::= BEGIN
-- the path to the root
org OBJECT IDENTIFIER ::= { iso 3 }
dod OBJECT IDENTIFIER ::= { org 6 }
internet OBJECT IDENTIFIER ::= { dod 1 }
directory OBJECT IDENTIFIER ::= { internet 1 }
mgmt OBJECT IDENTIFIER ::= { internet 2 }
mib-2 OBJECT IDENTIFIER ::= { mgmt 1 }
transmission OBJECT IDENTIFIER ::= { mib-2 10 }
experimental OBJECT IDENTIFIER ::= { internet 3 }
private OBJECT IDENTIFIER ::= { internet 4 }
enterprises OBJECT IDENTIFIER ::= { private 1 }
security OBJECT IDENTIFIER ::= { internet 5 }
snmpV2 OBJECT IDENTIFIER ::= { internet 6 }
-- transport domains
snmpDomains OBJECT IDENTIFIER ::= { snmpV2 1 }
-- transport proxies
snmpProxys OBJECT IDENTIFIER ::= { snmpV2 2 }
-- module identities
snmpModules OBJECT IDENTIFIER ::= { snmpV2 3 }
-- definitions for information modules
END
```



SMI példa:

Nominális formátum:

iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1).system(1).sysname(5).0

Numerikus formátum:

1.3.6.1.2.1.1.5.0

7. Hálózatmenedzsment (SNMP, RMON)

Hálózatmenedzsment SNMP-vel (folyt.):

- ASN.1 programozási nyelv:

- Objektum azonosítók leírása

- ASN.1 példa:

```
-- Két kötőjel a komment
MostSevereAlarm ::= INTEGER                -- MostSevereAlarm típusa Integer
circuitAlarms MostSevereAlarm ::= 3        -- MostSevereAlarm circuitAlarms = 3;
MostSevereAlarm ::= INTEGER (1..5)         -- Értékkészlet
ErrorCounts ::= SEQUENCE {
    circuitID      OCTET STRING,
    erroredSeconds INTEGER,
    unavailableSeconds INTEGER
}      -- adat struktúrák SEQUENCE kulcsszóval hozhatók létre
```

- BER (Basic Encoding Rules) programozási nyelv (CCITT X.209):

- SNMP üzenetek bináris alakra konvertálása.

- SNMP – programozás analógia: ASN.1 ~ forráskód, BER ~ gépi kód.

- SNMP adat típusok:

Típus	Jelentés
INTEGER	32 bites egész
OCTET STRING	Bájtos sztring
OBJECT IDENTIFIER (OID)	Objektum azonosító
NULL	Típus nélküli adatérték
IpAddress	4 bájtos OCTET STRING

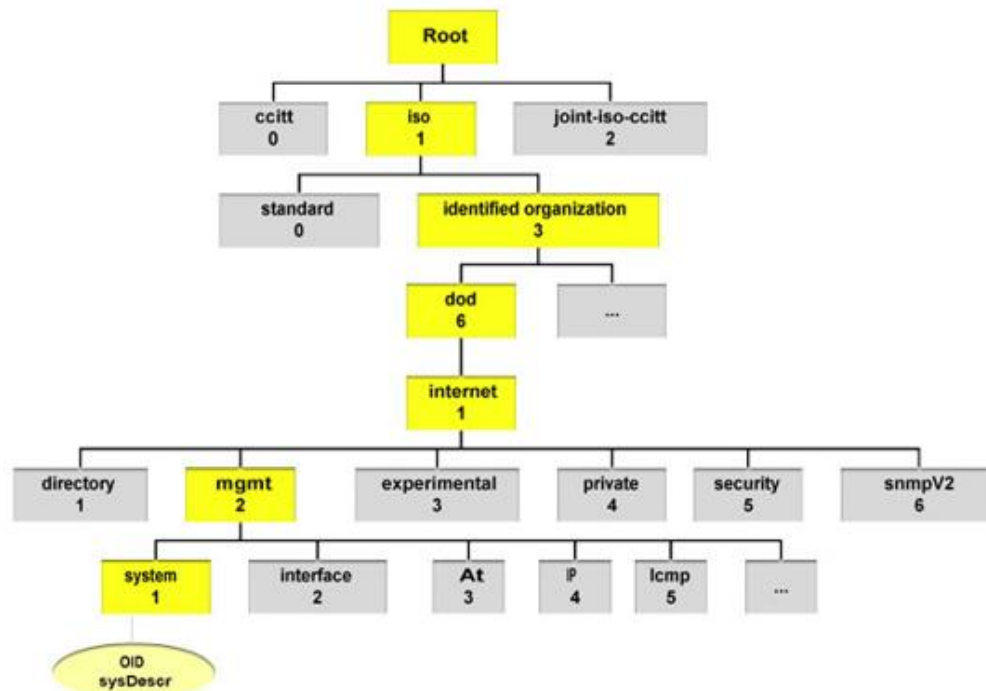
Típus	Jelentés
Counter	32 bites előjel nélküli egész (ciklikus)
Gauge	32 bites előjel nélküli egész
TimeTicks	32 bites előjel nélküli egész (1 ms darabszám)
Opaque	NemSNMPv1-es adat
DateAndTime, DisplayString, ...	Szöveges típusok

7. Hálózatmenedzsment (SNMP, RMON)

Hálózatmenedzsment SNMP-vel (folyt.):

- Példa MIB változó létrehozására:

```
sysContact OBJECT-TYPE -- OBJECT-TYPE is a macro
    SYNTAX      DisplayString (SIZE (0..255))
    ACCESS      read-write -- or read-write, write-only, not-accessible
    STATUS      mandatory  -- or optional, deprecated, obsolete
    DESCRIPTION
        "Chris Francois
         cfrancois@acm.org
         (360)650-0000"
    ::= { system 4 }
```



Mi lesz a numerikus formátuma az új objektumnak?

7. Hálózatmenedzsment (SNMP, RMON)

Hálózatmenedzsment SNMP-vel (folyt.):

- SNMP üzenet formátuma:

- Üzenet előtag:

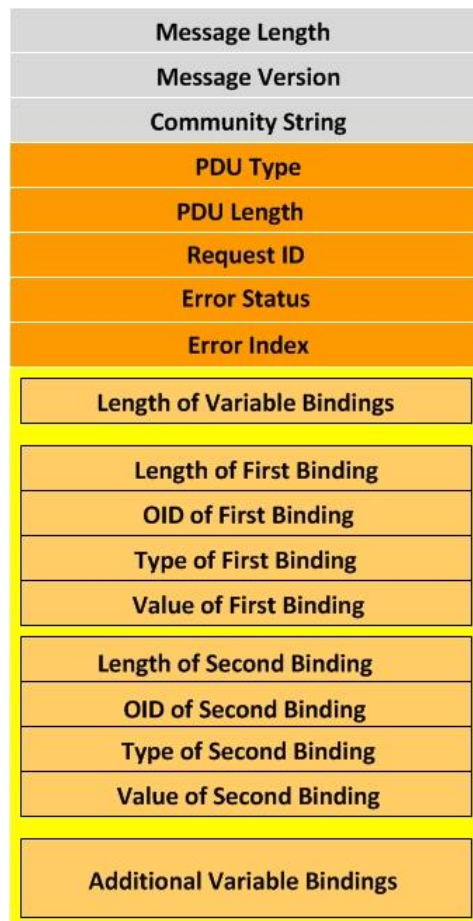
- Üzenet hossza
- Üzenet verziója
- Community sztring

- Üzenet fejrész:

- Típustól függő (!)
 - Kérdés
 - Válasz

- Üzenet rakrész:

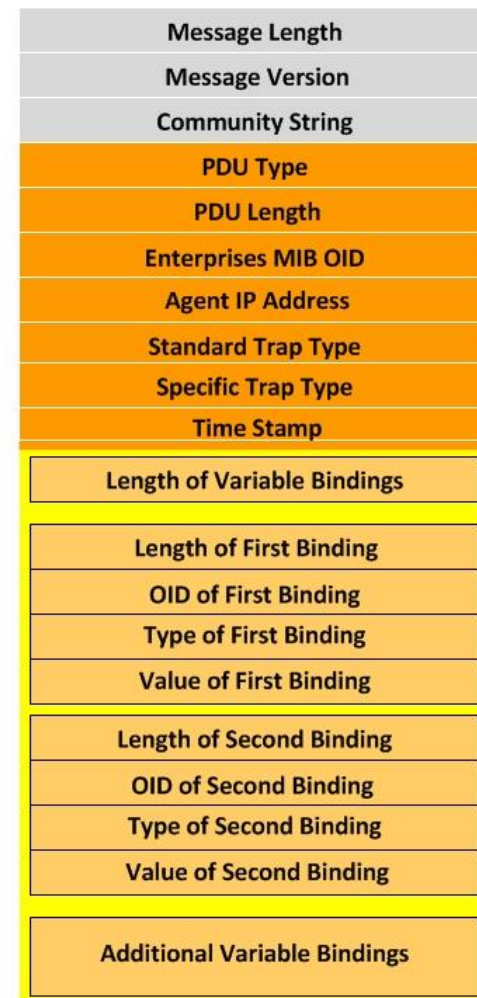
- Rakrész hossza
- Rekordok
 - Rekord hossza
 - Változó ID
 - Változó típusa
 - Változó értéke



SNMP
üzenet
előtag

SNMP
üzenet
fejrész

SNMP
üzenet
rakrész



7. Hálózatmenedzsment (SNMP, RMON)

Hálózatmenedzsment RMON-nal:

- RMON (Remote Monitoring, RFC 2819, RFC 4502): v1, v2.
- Hálózati objektumok lekérdezése és beállítása alkalmazási rétegben.
- SNMP kiegészítés: RMON1 MIB, RMON2 MIB.
- RMON csoportok: egyedi és csoportos adatforgalmak lekérdezési eszközei.

RMON1 csoport	Elemzés
1. Statistics	Valós idejű LAN statisztikák, pl. terhelés, ütközés, CEC hibák
2. History	Kiválasztott statisztikák historikus listája
3. Alarm	RMON SNMP trap definíció küszöbértékei
4. Hosts	Hoszt specifikus LAN statisztikák, pl. küldött/fogadott bájtok, küldött/fogadott keretek
5. Hosts top N	Adott időintervallumban a legaktívabb N kapcsolat
6. Matrix	Rendszerek közötti küldött-fogadott forgalom mátrix
7. Filter	Csomag mintázat, pl. MAC címérték, TCP portszám
8. Capture	A Filter szűrési feltételnek megfelelő megfigyelt és továbbított csomagok
9. Event	Trap küldése Alarm csoport esetén
10. Token Ring	Token Ring specifikus kiterjesztés

RMON2 csoport	Elemzés
1. Protocol Directory	Monitorozott protokollok listája
2. Protocol Distribution	Forgalom statisztika protokollonként
3. Address Map	Hálózati réteg (IP cím) és adatkapcsolati réteg (MAC cím) összerendelése
4. Network-Layer Host	Hosztönkénti L3 forgalom
5. Network-Layer Matrix	Hoszt forrás-pár szintű L3 forgalom statisztika
6. Application-Layer Host	Alkalmazás és hoszt szintű protokoll statisztika
7. Application-Layer Matrix	Alkalmazás és forrás-cél hoszt szintű protokoll statisztika
8. User History	Felhasználó specifikus változók periodikus mintavételezése
9. Probe Configuration	Mintavételek távoli konfigurálása
10. RMON Conformance	RMON2 MIB megfelelés elvárások