Számítógép-hálózatok oktatási segédlet

Almási, Béla

Számítógép-hálózatok oktatási segédlet

Almási, Béla

Publication date 2011.

Előszó

A Számítógép-hálzatok oktatási segédanyag célja, hogy egy jól használható vázlatot adjon a hálózatok (elsősorban IP alapú kommunikációs hálózatok) működésének vizsgálatához. A hálózatok témakör igen nagy mennyiségű anyagot ölel fel. A segédlet ebben az óriási ismeretanyagban egy egyetemi szemeszterre (kb. 30 óra előadás + gyakorlat követésére) tervezve, elsősorban a fizikai, adatkapcsolati és hálózati réteg kommunikációs technológiáira fókuszál. Igyekeztünk jól felépített, tiszta fogalomrendszerrel és (amennyire lehet magyar nyelvű) terminológiával dolgozni. Az angol nyelvű szakkifejezések (elsősorban az elterjedt használatuk és szakmai körökben elfogadott egyértelműbb jelentésük miatt) minden lényeges helyen említésre kerülnek. Az elektronikus megjelenési forma lehetőségeit kihasználva számos kép és interaktív animáció segíti az anyag elsajátítását.

A tananyag a TÁMOP-4.1.2-08/1/A-2009-0046 számú Kelet-magyarországi Informatika Tananyag Tárház projekt keretében készült. A tananyagfejlesztés az Európai Unió támogatásával és az Európai Szociális Alap társfinanszírozásával valósult meg.

Nemzeti Fejlesztési Ügynökség http://ujszechenyiterv.gov.hu/ *06 40 638-638*

Tartalom

I. rész - Alapfogalmak

Ebben a fejezetben egy rövid áttekintést adunk a számítógép-hálózatok területéhez kapcsolódó legfontosabb fogalmakról. Az itt szereplő rövid definíciókban csak a legfontosabb jellemzők kerülnek említésre.

1. fejezet - Számítógép-hálózatok alapfogalmai

1. Számítógép-hálózat

Számítógép-hálózat: Számítógéprendszerek valamilyen információátvitellel megvalósítható cél érdekében történő (hardveres és szoftveres) összekapcsolása.

Célok:

- Erőforrás-megosztás
- Megbízhatóság növelése
- Sebességnövelés
- Emberi kommunikáció

A számítógép-hálózat tipikusan számítógépekből és perifériás elemekből (pl. hálózati nyomtató), hálózati kapcsolóelemekből, a fizikai összeköttetést megvalósító eszközökből (kábelekből) és a különböző hálózati alkalmazásokat megvalósító programokból (szoftverekből) épül fel.

2. Számítógép-hálózatok osztályozása méretük szerint

Kiterjedés	Megnevezés
< 1 m	Multicomputer
1 km	Helyi hálózat (LAN)
10 km	Városi hálózat (MAN)
100 km <	Nagy kiterjedésű hálózat (WAN)

A LAN és a WAN nem csak méretben, hanem kommunikációs technológiában is jelentős eltérést mutat. A méretkategóriák nem pontos, hanem inkább nagyságrendi információk.

3. Számítógép-hálózati csomópont

Csomópont (node): Önálló kommunikációra képes, saját hálózati címmel rendelkező eszköz (pl. számítógép, nyomtató, forgalomirányító).

Egy kommunikációban egy csomópont működhet adó (forrás) illetve vevő (nyelő) funkcióval.

4. Adatátviteli közeg, csatorna, ütközés

Adatátviteli közeg (média, vonal): Olyan eszköz, anyag, közeg, melyen keresztül az információ (jel) továbbítása történik. (Pl. csavart pár, koax kábel, optikai kábel vagy levegő).

Adatátviteli csatorna: Jelek továbbítására szolgáló adatút (frekvenciasáv). Gyakran egy adatátviteli közegen több csatornát (adatutat) építenek ki.

Ütközés: Ütközésről beszélünk, ha egy közös adatátviteli csatornán két (vagy több) csomópont egy időpillanatban továbbít információt.

Alapvetően az "egy csatornán egy időpillanatban egy adó adhat" elv érvényesül, s alapvetően a továbbiakban is erre építünk, bár megjegyezzük, hogy léteznek ettől eltérő kommunikációs technológiai ötletek (ld. pl. CDMA).

Ütközési tartomány (collision domain, bandwidth domain): Az a hálózatrész, ahol egy bizonyos előforduló ütközés érzékelhető, megjelenik.

Az ütközési tartományban egy időpillanatban csak egy információátvitel folyhat. (Logikailag egy ütközési tartomány egy közös csatornával rendelkező hálózatrészként reprezentálható.)

5. Jel, kódolás, moduláció, multiplexelés

Jel: Helytől és időtől függő, információt hordozó fizikai mennyiség(ek). Információhordozó a kommunikációs csatornán, lehet analóg vagy digitális.

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

Moduláció: Az információátviteli csatorna egy frekvenciasávként jeleníthető meg legegyszerűbben (analóg vivőfrekvencia). A moduláció a továbbítandó (digitális) információnak az analóg vivőjelre történő leképezése. Tipikusan az analóg vivőfrekvencia valamely paraméterének (pl. amplitúdó, fázis, stb) jól meghatározott elven történő megváltoztatásával implementálható. Inverz (vevő oldali) folyamata a demoduláció.

A modem a modulációt és a demodulációt végző berendezés.

Multiplexelés: Két (vagy több) jól elkülöníthető (különböző) kommunikációnak egy vonalon (vagy csatornán) való párhuzamosan történő működtetése (végrehajtása).

6. Adatátviteli sebesség

Adatátviteli sebesség (hálózati sebesség, sávszélesség, bitráta, bandwidth): Időegység alatt átvitt információ mennyisége. Mértékegysége a bit/másodperc, b/s, bps. Az adatátviteli sebességet tipikusan a csatorna kapacitásának mérésére, jelzésére használják.

Nagyobb egységek:

1 kbps	1000 bps
1 Mbps	1000 kbps
1 Gbps	1000 Mbps

7. Modulációsebesség

Modulációsebesség (jelváltás sebesség): Időegység alatt bekövetkező jelváltások (a csatornán érvényes szimbólumok közötti átmenetek) száma. Mértékegysége a jelváltás/másodperc.

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

8. Információátviteli kapcsolattípusok

Pont-pont kapcsolat (Point-To-Point): Ha az információközlés csak két pont (egy adó és egy vevő) között zajlik, akkor pont-pont kapcsolatról beszélünk.

Többpontos kapcsolat, üzenetszórás (broadcast): Többpontos kapcsolatról (pl.) akkor beszélünk, ha egy adó egyszerre több vevőt lát el információval. Az üzenetszórás olyan többpontos kapcsolat, ahol az adótól egy bizonyos hatósugáron belül minden vevő megkapja az információt (pl. rádiós műsorszórás).

9. Információátvitel irányítottsága

Egyirányú (szimplex) összeköttetés: Ha két kommunikációs pont között az információközlés csak egy irányban lehetséges, akkor egyirányú (szimplex) összeköttetésről beszélünk (pl. rádiós műsorszórás).

Váltakozó irányú (half-duplex) összeköttetés: Az információátvitel mindkét irányban lehetséges, de egy időpillanatban csak az egyik irányban (pl. CB rádió).

Kétirányú (full-duplex) összeköttetés: Az információátvitel egy időpillanatban mindkét irányban lehetséges (pl. telefon). (Logikailag két, egymástól függetlenül működő szimplex összeköttetésnek fogható fel).

10. Kapcsolási módok

Vonalkapcsolt (áramkörkapcsolt, circuit switched) technológia: Az információátvitel 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 összeköttetést terhelve. (Pl. telex.)

Csomagkapcsolt (packet switched) technológia: Az információt (korlátozott maximális méretű) részekre (csomagokra) darabolják, s a csomagokat (mint önálló egységeket) üzenetkapcsolt elven továbbítják. (A számítógép-hálózatoknál a jól tervezhető pufferelési tulajdonsága miatt előszeretettel alkalmazzák).

11. Címzési alapfogalmak

A számítógép-hálózatokban történő sikeres információkézbesítés érdekében szükség van a csomópontok (gépek) egyértelmű azonosítására (mint pl. a postai kézbesítőrendszerben is). Az üzenetekben tipikusan két azonosító jelenik meg: a feladó csomópont, és a cél azonosítója. A cél azonosítója (címe) nem feltétlenül egyetlen csomópont azonosítására szolgál, ezen az alapon többféle kategóriát is megkülönböztethetünk:

Egyedi cím (Unicast address): Egy csomópont egy hálózati csatlakozójára (interfészére) vonatkozó azonosító. Az üzenetekben szereplő feladó cím tipikusan egyedi (unicast) cím. Általában egy hálózati interfész egy egyedi címet kap azonosítási célból, de természetesen ez nem kötelező megszorítás.

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

Többes cím (Multicast address): Interfészek egy halmazát vagy csoportját (tipikusan különböző csomópontokon található interfészek csoportját) azonosító cím. Ha egy csomagot egy „többes címre” küldünk, akkor a csoport minden elemére el kell juttatnunk.

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 (a csoport az üzenetszórási tartomány valamennyi interfészét magába foglalja).

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

12. Számítógép-hálózati protokoll

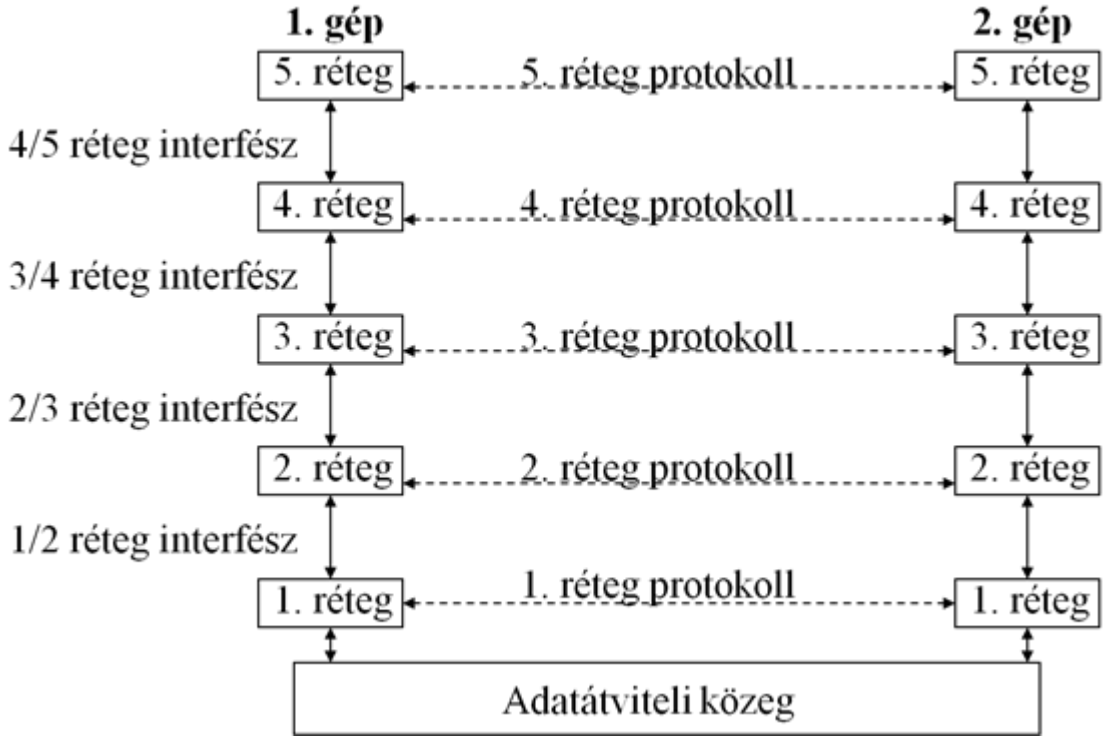
Protokoll: Szabályok és konvenciók összességének egy formális leírása, mellyel meghatározzák a hálózati eszközök (csomópontok) kommunikációját (kommunikációs szabályok halmaza).

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

2. fejezet - Rétegelt hálózati architektúra

Egy protokoll leírása, pontos specifikációja általában nagyon nehéz, óriási feladatot jelent. Egy hierarchikus rendben felépített protokoll-rendszer könnyebben kezelhető, áttekinthetőbb. Egy ilyen rendszerben a változások is könnyebben követhetők, s a hierarchia különböző szintjeit különböző gyártók is implementálhatják (anélkül, hogy ez együttműködési problémákat okozna).

1. Rétegek (szintek), protokollok, interfészek



2. Rétegelt hálózati architektúra - fogalmak

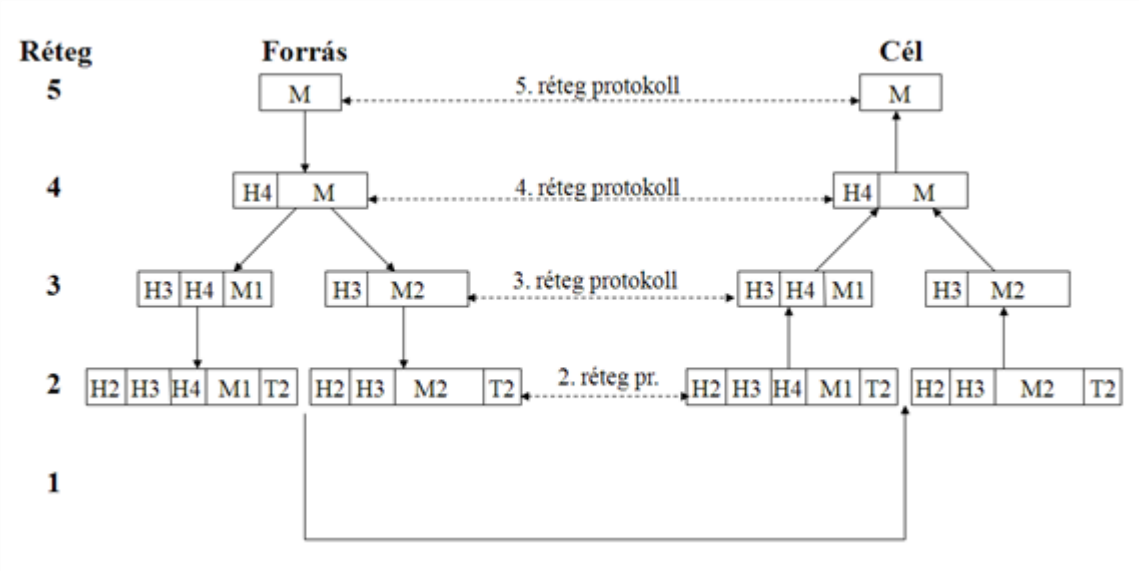
N. réteg protokoll: Az N. réteg (szint) specifikációját leíró protokoll.

Társak (peers): A két kommunikációs végpont (csomópont) azonos szintjén elhelyezkedő entitások. Logikailag a társak kommunikálnak egymással a megfelelő réteg protokollját használva.

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).

3. 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 (peer) legfelsőbb rétegbeli entitásának küldi, az adott réteg működését leíró protokoll alapján. 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 funkcionalitásainak az ellátásához további információkat társíthat a felsőbb rétegtől kapott információs egység elé ("H" fejrész, "header" információ), vagy esetleg az után ("T" végrész, "tailor" információ; pl. ellenőrző összeg). Az egyes rétegekben megadott méretkorlátok miatt előfordulhat, hogy a felsőbb rétegben egy egységként megjelenő információt darabolni kell (ld. a példa 3. rétegében). A darabolás (fregmetálás) után létrejött információs egységek külön-külön entitásként haladnak a cél felé, s a célhelyen a megfelelő réteg (jelen példában a 3. réteg) a darabokat összeilesztve adja tovább a felsőbb réteg számára az eredeti (nagyméretű) információt.

4. Hálózati kommunikáció - fogalmak

Beágyazás (enkapszuláció): A felsőbb szintről érkező, s az adott réteg által már nem módosítható információ (ún. Service Data Unit, SDU) egy bizonyos (alsóbb rétegbeli) protokoll fejlécével történő kiegészítése, becsomagolása (mint pl. levél küldésekor a borítékba helyezés és a boríték címzése).

Protokoll adategység (PDU, Protocol Data Unit, csomag): Az adott réteg protokollja által kezelt (fejlécből és adatból álló) egység. A PDU adatrészében tipikusan a felsőbb réteg SDU-ja található. (A PDU gyakran használt másik megnevezése a csomag.)

5. OSI referenciamodell

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

Sorszám	Réteg neve	PDU neve
7.	Applikációs réteg (Application layer)	APDU
6.	Megjelenítési réteg (Presentation layer)	PPDU
5.	Viszony réteg (Session layer)	SPDU
4.	Szállítási réteg (Transport layer)	Szegmens, TPDU
3.	Hálózati réteg (Network layer)	Csomag
2.	Adatkapcsolati réteg (Datalink layer)	Keret, cella

Sorszám	Réteg neve	PDU neve
1.	Fizikai réteg (Physical layer)	Bit

6. 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 címzés, 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 címzés és az útvonalválasztás (routing).

4. Szállítási réteg: Megbízható hálózati összeköttetést létesít két csomópont között. Feladatkörébe tartozik pl. a virtuális áramkörök kezelése, átviteli hibák felismerése/javítása és az áramlásszabályozás.

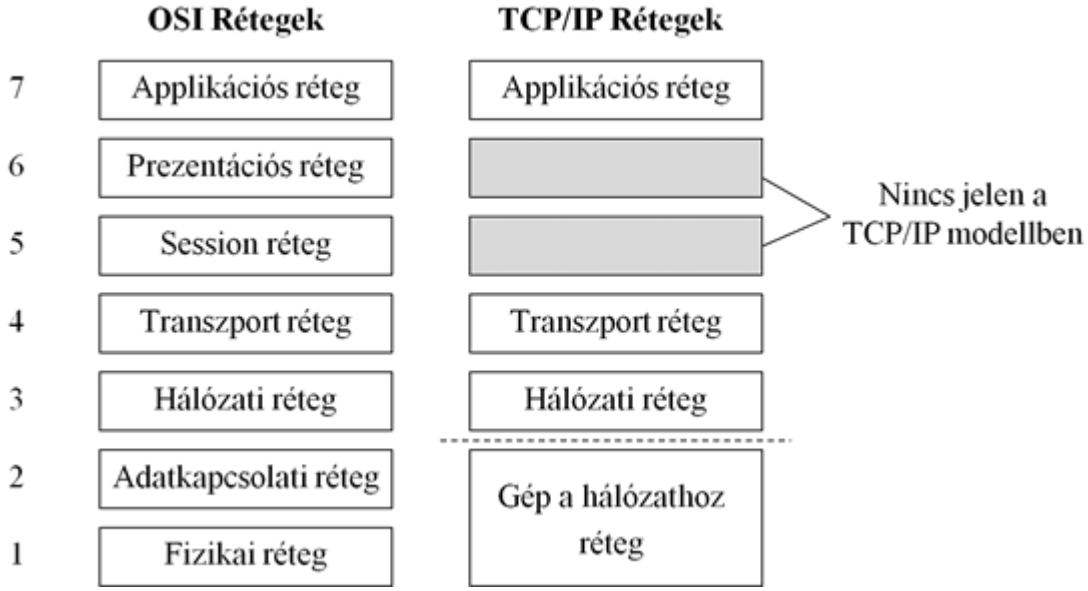
5. Viszony réteg: Ez a réteg építi ki, kezeli és fejezi be az applikációk közötti dialógusokat (session, dialógus kontroll).

6. Megjelenítési (prezentációs) réteg: Feladata a különböző csomópontokon használt különböző adatstruktúrákból eredő információ-értelmezési problémák feloldása.

7. Applikációs (alkalmazási) réteg: Az applikációk (fájlátvitel, e-mail stb.) működéséhez nélkülözhetetlen szolgáltatásokat biztosítja.

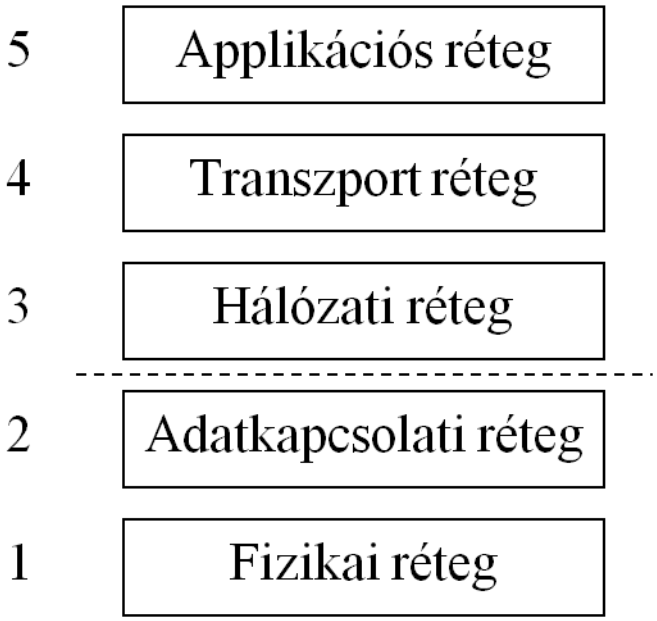
7. TCP/IP - OSI modell leképezése

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:



8. Hibrid referenciamodell

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.

9. Hálózati kapcsolóelemek

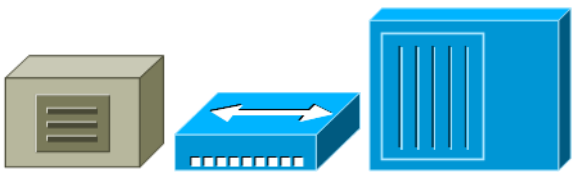
Az egyes hálózatrészek összekapcsolására szolgáló eszközök - a kapcsolóelem működési funkcionalitása alapján - különböző OSI rétegekbe sorolhatók.

Réteg	**Eszköz**
Transzport réteg (és felette)	Átjáró (gateway)
Hálózati réteg	Forgalomirányító, útválasztó (router).
Adatkapcsolati réteg	Híd, kapcsoló (bridge, switch)
Fizikai réteg	Jelismétlő (repeater, HUB)

Jelismétlő (repeater):

- Az átviteli közegen továbbított jeleket ismétli, erősíti.
- Az összekapcsolt részhálózatokat nem választja el.
- Többportos változatát szokás HUB-nak nevezni.

A HUB működése (interaktív animáció)



Híd (bridge):

- Az 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.

Kapcsoló (switch):

- Olyan többportos eszköz, melynek bármely két portja között híd (bridge) funkcionalitás működik.

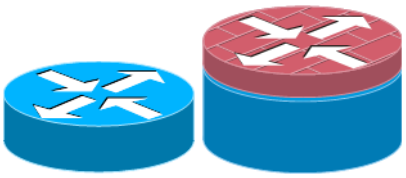
  A kapcsoló működési vázlata (interaktív animáció)

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.

Forgalomirányító (router):

- A hálózati rétegben működve szelektív összekapcsolást, útvonalválasztást, forgalomirányítást végez.
- Az összekapcsolt részhálózatok külön ütközési tartományt és külön üzenetszórási tartományt alkotnak.
- Csomópont, saját hálózati címmel rendelkezik.



II. rész - Fizikai réteg

A fizikai réteg feladata a bitátvitel megvalósítása két (csatornával közvetlen módon összekötött) csomópont között.

3. fejezet - Fizikai réteg

1. Korlátozott sávszélesség

Csatorna maximális adatátviteli sebessége

Nyquist (1924) és Shannon (1948) elméleti összefüggései a csatorna maximális adatátviteli sebességére.

Nyquist meghatározta a maximális adatátviteli sebességet zajtalan csatornára:

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

$$\mathbf{C} = 2H\log_2 V \ \mathbf{bit/s}$$

ahol C a maximális adatátviteli sebesség, H az átviteli csatorna sávszélessége.

2. Vonali zaj (noise)

Az átviteli közeg környezetéből származó zavarokat 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:

$$\mathbf{C} = H\log_2(1 + S/N) \ \mathbf{bit/s}$$

ahol C a maximális adatátviteli sebesség, H az átviteli csatorna sávszélessége, S az átlagos jelteljesítmény, N az átlagos zajteljesítmény.

3. Csillapítás

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.

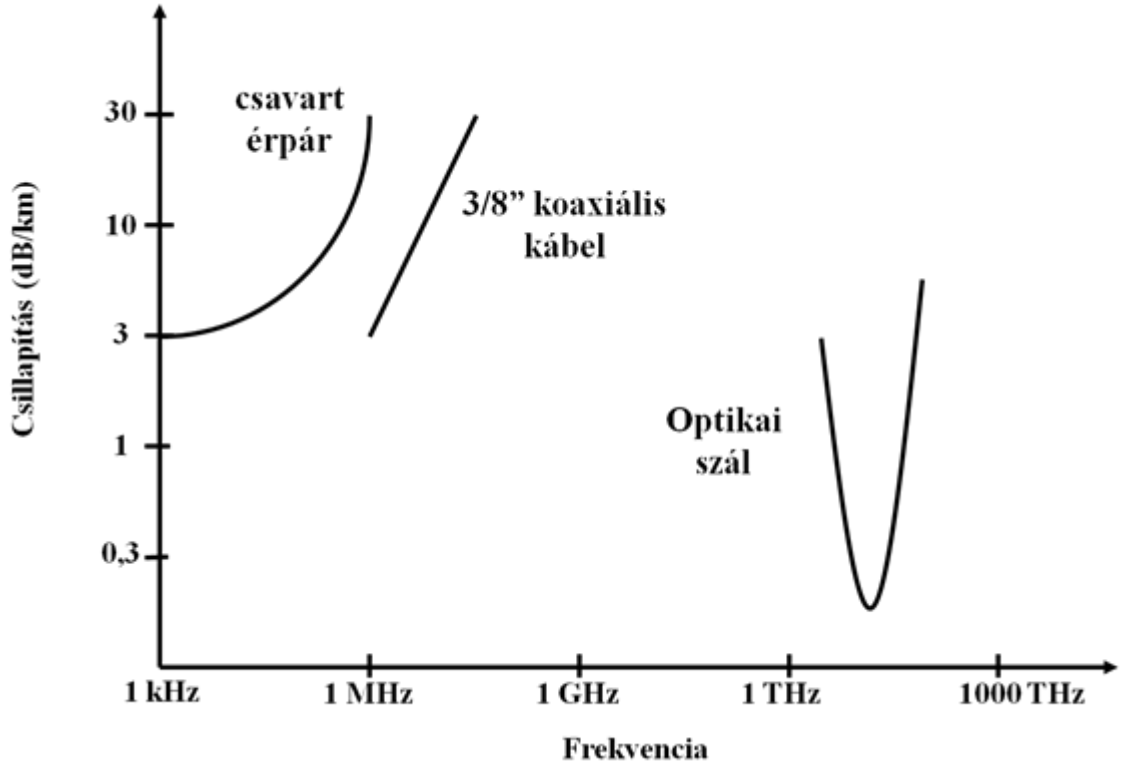
A csillapítás és az erősítés mértékét decibelben (dB) adják meg:

$$\mathbf{Csillapítás} = 10\log_{10}\frac{P_1}{P_2} \ \mathbf{dB}$$

ahol P1 és P2 az átviteli közeg elején és végén mért teljesítmény (Watt).

4. fejezet - Átviteli közegek, médiumok

1. Vezetékes médiumok csillapítása



2. Csavart érpár

2.1. Fizikai jellemzők

A csavart érpár (Twisted Pair) az egyik legolcsóbb, legelterjedtebben használt átviteli közeg. Két szigetelt rézvezetéket szabályos minta szerint összecsavarnak. Több csavart érpárt (4) fognak össze, és külső szigeteléssel látnak el. Az összefogott érpárokat külön-külön (STP) ill együttesen árnyékolhatják (FTP), vagy (olcsóbb megoldásként) árnyékolás nélkül is használhatják (UTP). A csavarás csökkenti az áthallást az érpárok között és (némi) zajvédelmet biztosít. A csavarás sűrűsége különbözhet az egyes érpárokban, hogy csökkenjen az áthallás. A huzal átmérője ~0,4 / ~0,8 mm (AWG 26 - 22).

2.2. Átviteli jellemzők

A csavart érpár csillapítása erősen függ a frekvenciától. Érzékeny az interferenciára és a zajra. Például a párhuzamosan futó AC hálózatból könnyen fölveszi az 50Hz energiát.

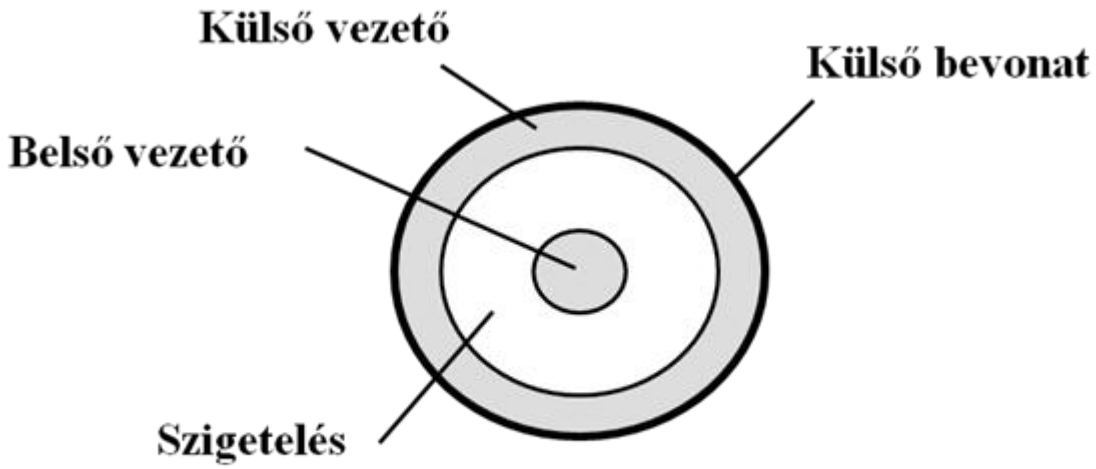
Az adatátviteli kábelspecifikációk különböző kategóriákat (osztályokat) különítenek el, melyek elsősorban a LAN technológiáknál használatos hosszúság (100m) esetén elérhető maximális frekvenciában különböznek:

Kategória (USA)	Osztály (EU)	Frekvencia	Sebesség
Category 3	Class C	16 MHz	10 Mbps

Kategória (USA)	Osztály (EU)	Frekvencia	Sebesség
Category 5/5e	Class D	125 MHz	100 Mbps / 1000 Mbps 4 érpáron
Category 6	Class E	250 MHz	1000 Mbps 2 érpáron
Category 6A	Class EA	500 MHz	10.000 Mbps
Category 7	Class F	600 MHz	10.000 Mbps

3. Koaxiális kábel

3.1. Fizikai jellemzők



Koaxiális kábel keresztmetszete

A kábel átmérője: 5 - 25 mm. A koncentrikus felépítés miatt kevésbé érzékeny a zavarokra és az áthallásra, mint a csavart érpár. Nagyobb távolságra használható és többpontos alkalmazásban több állomást is képes támogatni (egy közös vonalon).

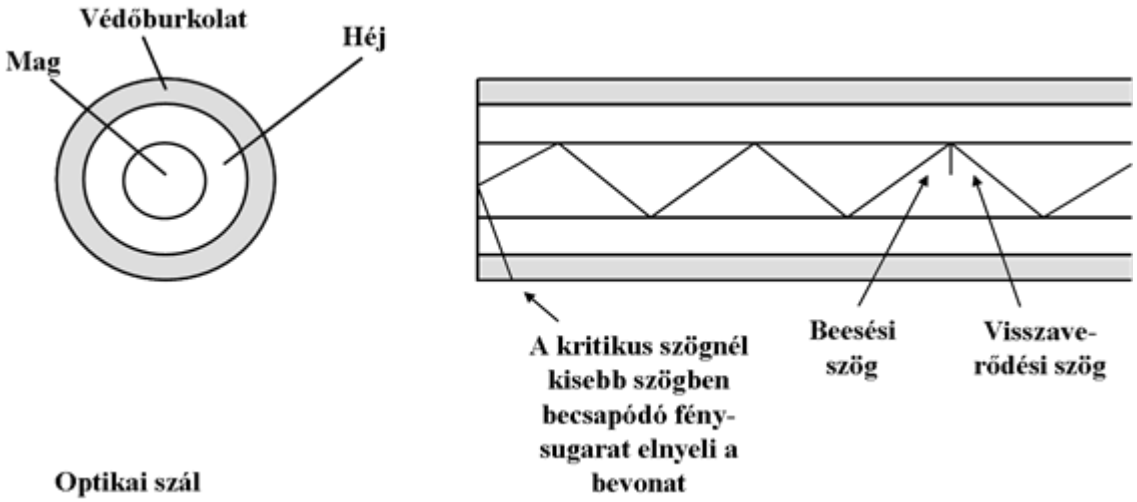
3.2. Átviteli jellemzők

Analóg átvitel esetén néhány km-enként szükséges erősítés. Mintegy 600 MHz-ig használható. Digitális átvitel esetén km-enként szükséges jelismétlő használata.

A mai (struktúrált kábelezési technológiára épülő) LAN környezetekben már nem használják új építésű passzív hálózatokhoz.

4. Optikai szál

4.1. Fizikai jellemzők



Tipikusan 8,3µm, 50µm vagy 62,5µm magátmérőjű, hajlékony optikai szál, ami fénysugár továbbítására képes. Optikai szálat üvegből és műanyagból is készítenek. A köpeny (vagy más néven héj), mely tipikusan125µm átmérőjű szintén üveg vagy műanyag, más optikai tulajdonságokkal rendelkezik mint a mag. A külső burkolat (védőburkolat, 250µm átmérő) a szennyeződés, kopás és egyéb külső hatások ellen nyújt védelmet. Egy optikai összeköttetés tipikusan 2 db optikai szálra épül (külön szál az egyik ill. másik irányú átvitelre). Az optikai kábelben több optikai szál fut, valamint merevítésre és további mechanikai védelemre szolgáló elemek is helyet kapnak.

4.2. Előnyök

- Nagy adatátviteli sebesség érhető el (Több Gbps több 10 km-en).
- Kisebb méret és súly
- A csillapítás kisebb, és széles frekvenciatartományban állandó.
- Elektromágneses izoláltság. Külső elektromágneses hatásokra nem érzékeny, nincs áthallás. Nem sugároz energiát, ezért nem hallgatható le. Nehéz az üvegszálat megcsapolni.
- Nagyobb ismétlési távolság. Kevesebb ismétlő kevesebb hibalehetőséggel és alacsonyabb költséggel jár. A technológia egyre fejlődik: pl. 3,5 Gbps adatátviteli sebesség 318 km távolságra ismétlés nélkül (AT&T, 1990-es évek!!!).

4.3. Alkalmazásai

- Nagyvárosi, nagytávolságú fővonalak (trunk)
- Épületek ill. épületszintek közötti összeköttetések (LAN).
- Előfizetői hurkok

4.4. Átviteli jellemzők

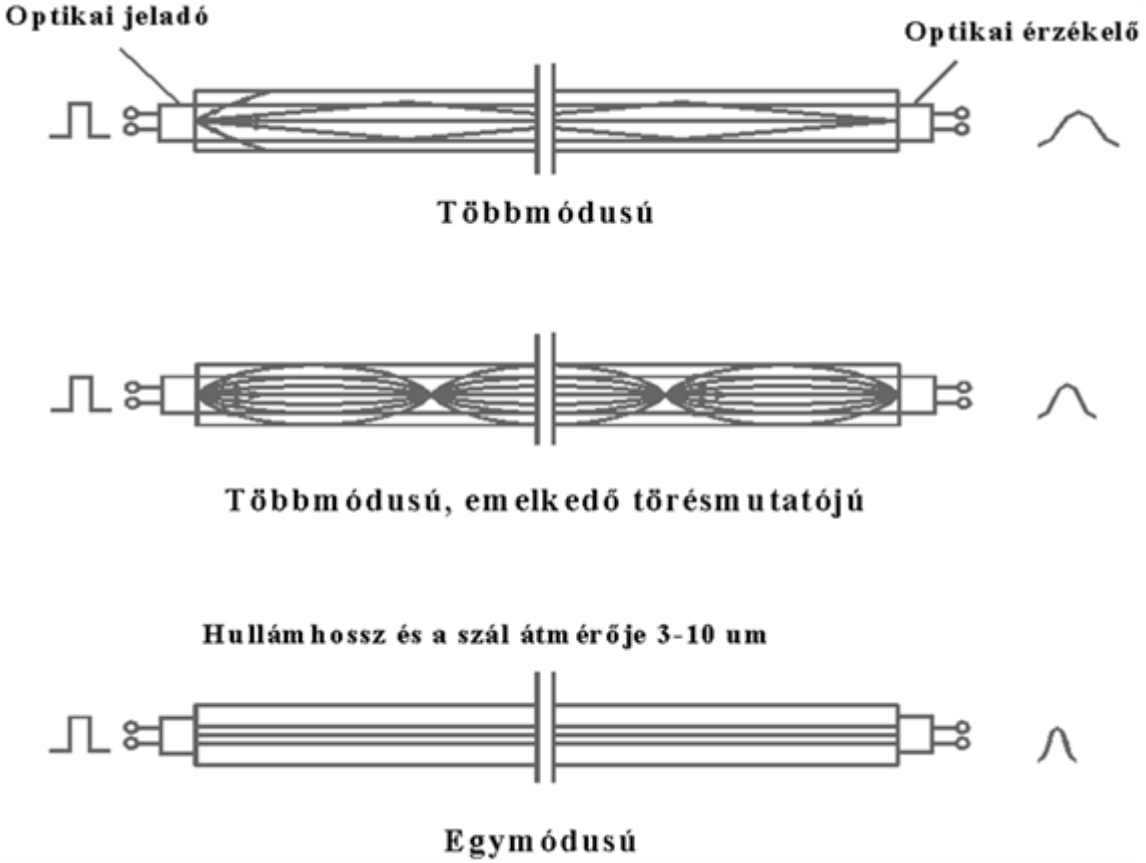
- 800 - 1500 nm (infravörös) hullámhossz tartományban működik.
- Fényforrás lehet: LED vagy lézer.

4.5. Típusok

Többmódusú szál (MultiMode): A fényforrásból különböző szögben kilépő fénysugarak különböző szögben verődnek vissza a két optikai közeg határáról, ezért különböző utat tesznek meg különböző idő alatt. Ezért a fényimpulzusok torzulnak. Emiatt az adatátviteli sebesség csökken. Jellemzők: 50/125µm ill. 62.5/125µm átmérő; 850nm, 1310nm hullámhossz.

Egymódusú szál (SingleMode): A mag átmérőjét csökkentve a hullámhossz nagyságrendjére csak a tengelyirányú fénysugár jut át. A fényimpulzusok nem torzulnak, nagyobb adatátviteli sebesség érhető el. Jellemzők: 9/125µm átmérő; 1310nm, 1550nm hullámhossz.

Többmódusú, emelkedő törésmutatójú szál (MultiMode Graded): A mag anyagának törésmutatója a tengelytől távolodva növekszik. Ez mintegy fókuszálja a fényt. E típus tulajdonságai az előző kettő közé tehetők.



5. Rádiófrekvenciás (vezeték nélküli) adatátvitel

A vezeték nélküli átvitel során a közeghozzáférés és az átvitel biztonsága tekintetében teljesen egyedi (a kábel alapú összeköttetésekhez képest teljesen más) megoldási mechanizmusok működnek. Ezen alapozó segédletben nem foglalkozunk ezekkel a speciális közeghozzáférési és biztonsági megoldásokkal

Méret (távolság) alapján alapvetően két kategóriát kell elkülönítenünk:

- **Kistávolságú átvitel (WLAN, Wi-Fi).** Egy intézményi LAN-hálózat vezeték nélküli kiterjesztése. Szabadon használható frekvenciák (2.4 GHz, 5 GHz). A magas frekvencia miatt fényszerű terjedés. (2.4 GHz a víz rezonancia-frekvencia közelében!) Célja: Mobilitás biztosítása az intézményi adatkommunikációs hálózaton.

- **Nagytávolságú összeköttetés biztosítása (GPRS, EDGE, UMTS).** Globális hálózati hozzáférést biztosít. A mobiltelefonos technológia kiterjesztése adatátviteli célokra. Frekvencia-használati (átviteli) díjfizetés.

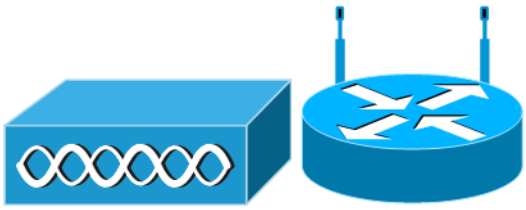
WLAN technológiák

- **Infrastruktúra üzemmód:** A mobil eszközök az intézményi (vezetékes) hálózathoz kapcsolódnak egy rádiós bázisállomáson keresztül (Access Point, AP). A mobil eszközök egymással közvetlen rádiós kommunikációt nem folytatnak.

- **Ad-hoc üzemmód:** A mobil eszközök közvetlenül egymáshoz kapcsolódnak a rádiós interfészükön keresztül. Sok gép esetén nem hatékony.

WLAN logikai architektúrák

- **BSS (Basic Service Set):** Egy rádiós interfész (bázisállomás, AP) hatósugarában működő hálózati környezet. A hálózati környezet azonosítására egy szöveges azonosítót (SSID) használnak.
- **IBSS (Independent BSS):** Több, egymástól függetlenül működő BSS. Tipikusan Ad-hoc hálózatoknál elterjedt a használata.
- **DS (Distributed Systam):** Több BSS összekötése (rádiós vagy vezetékes infrastruktúrán keresztül).
- **ESS (Extended Service Set):** Több BSS olyan speciális összeköttetéssel, mely biztosítani tudja a BSS-ek közötti átjárás lehetőségét a hálózati kapcsolat megszakadás nélkül (Roaming).



5. fejezet - Jelkódolási technológiák

1. Jelkódolás

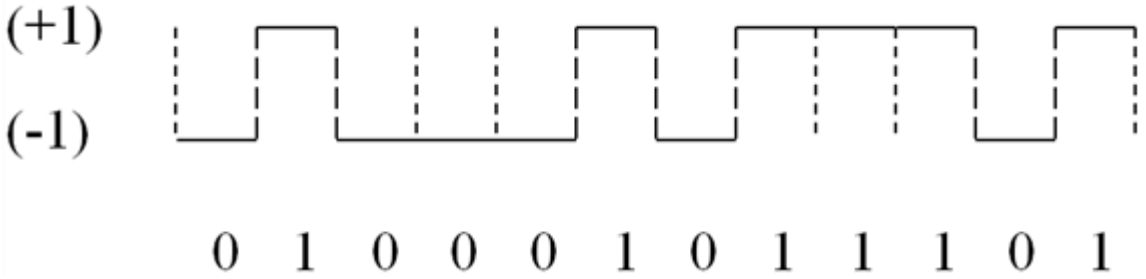
Jelkódolás: A fizikai rétegben megjelenő bitsorozatot az alkalmazott (digitális) csatorna jelkészletére, jelzésrendszerére (feszültségszintekre, feszültségszint-váltásokra) képezzük le.

Bipoláris kódolás: A csatornán két jelet (feszültségszintet) különíthetünk el, s az egyszerűség kedvéért a (+1) és a (-1) szimbólumokkal jelöljük őket.

2. NRZ jelkódolás

A (+1) feszültségszintet tartjuk az „1” bit érték átviteli idejében, s a (-1) feszültségszintet pedig a „0” bit érték átviteli idejében. Könnyen implementálható, de nem biztosít szinkronizációt több azonos bit érték átvitele során.

Példa:

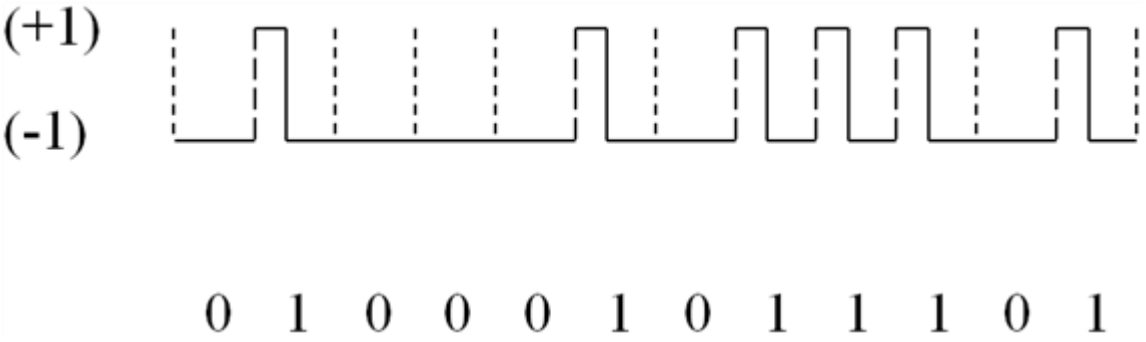


3. RZ jelkódolás

A (+1) feszültségszintet tartjuk az „1” bit érték átviteli idejének első felében és (-1)-et a második felében. A „0” bit érték esetén a teljes bit időtartamban (-1) feszültségszintet tartunk.

Jelváltás sebesség duplikáció és szinkronizálatlan „0” bitsorozat átvitel jellemzi.

Példa:

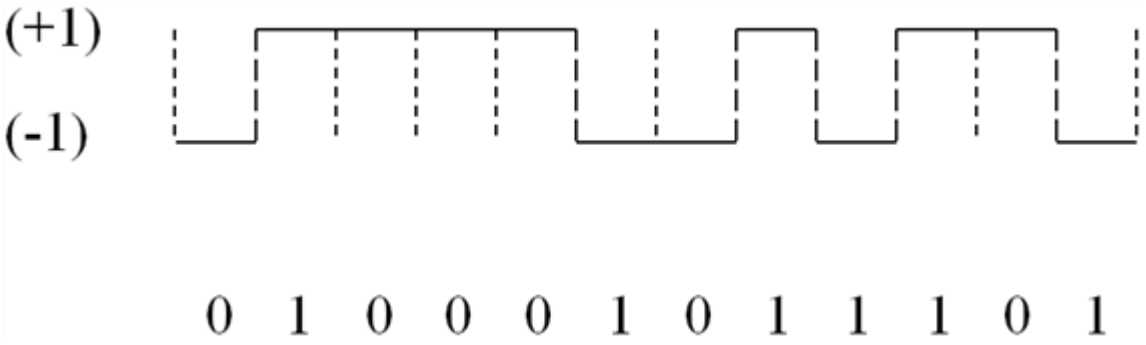


4. NRZI jelkódolás

Az „1” bit érték átviteli idejében a megelőző időtartamban alkalmazott feszültségszint ellentettjét alkalmazzuk, a „0” bit érték átviteli idejében pedig tovább tartjuk a megelőző bit időtartamban alkalmazott feszültségszintet.

Sok „0” bit átvitele során nem biztosít szinkronizációt.

Példa:

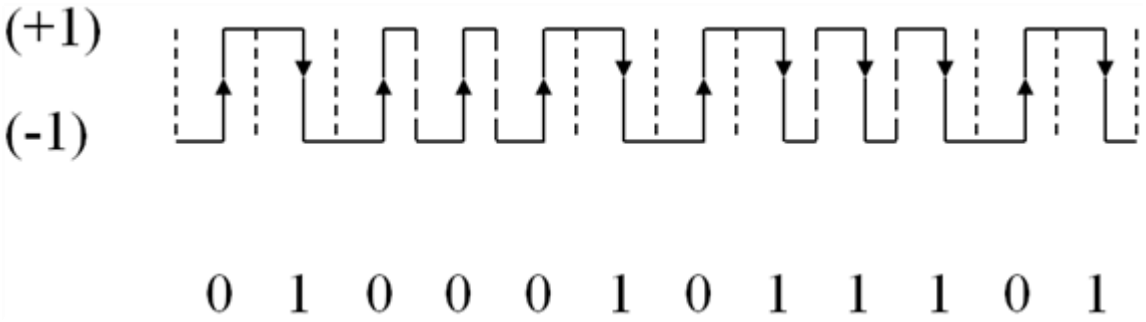


5. Manchester (PE) jelkódolás

Az „1” bit értéket az átviteli idejének közepén bekövetkező (+1) → (-1) feszültségszint-váltás reprezentálja. A „0” bit értéket pedig az átviteli idejének közepén bekövetkező (-1) → (+1) feszültségszint-váltás reprezentálja.

A folyamatos szinkronizáció biztosított, de dupla jelváltás-sebességet igényel.

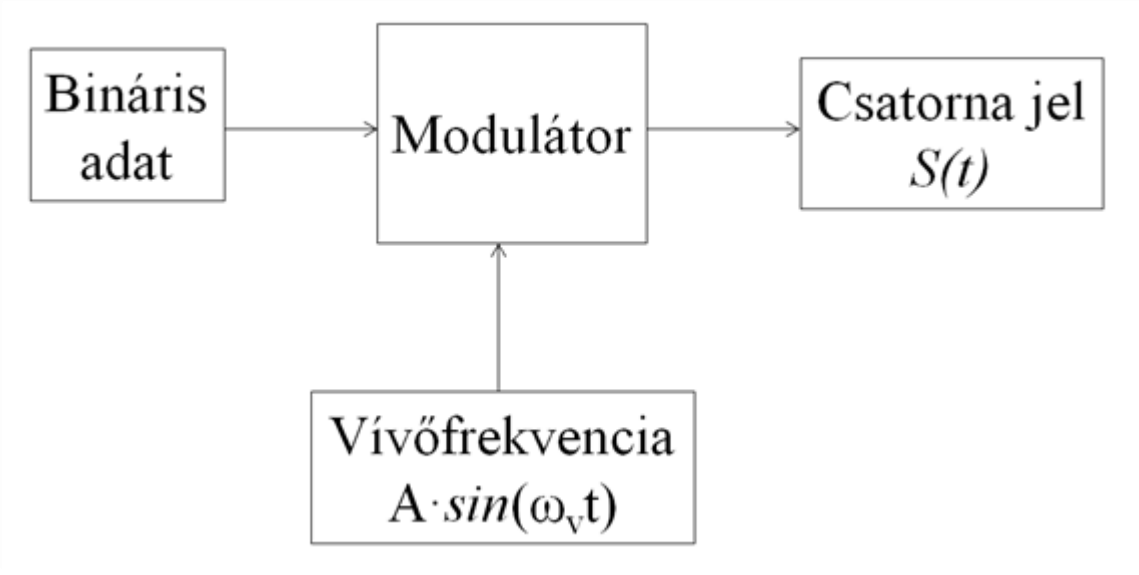
Példa:



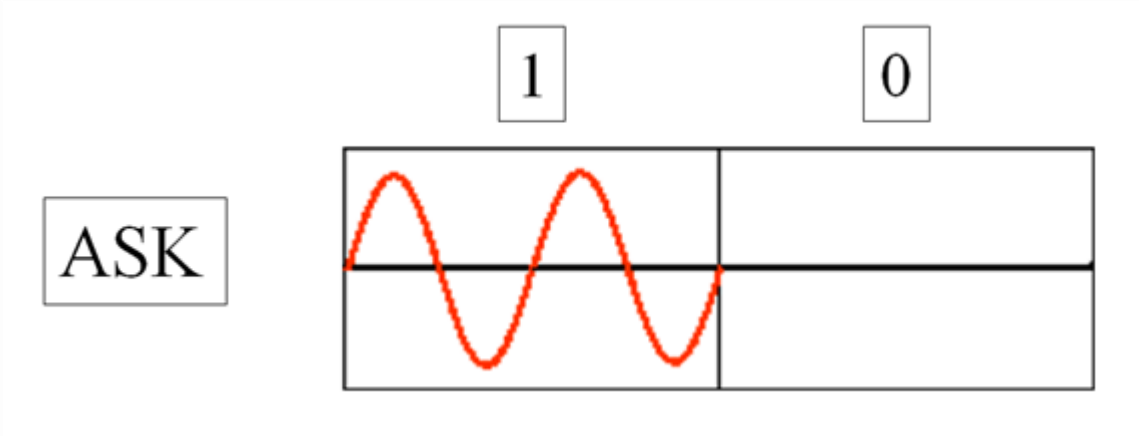
6. fejezet - Modulációs technológiák

1. Szinuszos vivőjű digitális moduláció

A bináris információt sok esetben nem alapsávi impulzusok formájában visszük át a csatornán, hanem egy (alsó- és felső frekvenciahatár megadásával) jól meghatározott frekvenciatartománnyal rendelkező (sávátereszto) csatornán kell továbbítanunk. A rendelkezésre álló frekvenciasáv középértéke adja a vivőfrekvenciát, melyen valamilyen modulációs eljárással tudjuk megjeleníteni a továbbítandó bit értékét (Jelmagyarázat: A-amplitúdó, ω_v - vivőfrekvencia leírója, t - egy bit átviteli időtartamon belüli időpillanat jezője):



1.1. Amplitúdó billentyűzés (Amplitude Shift Keying, ASK)

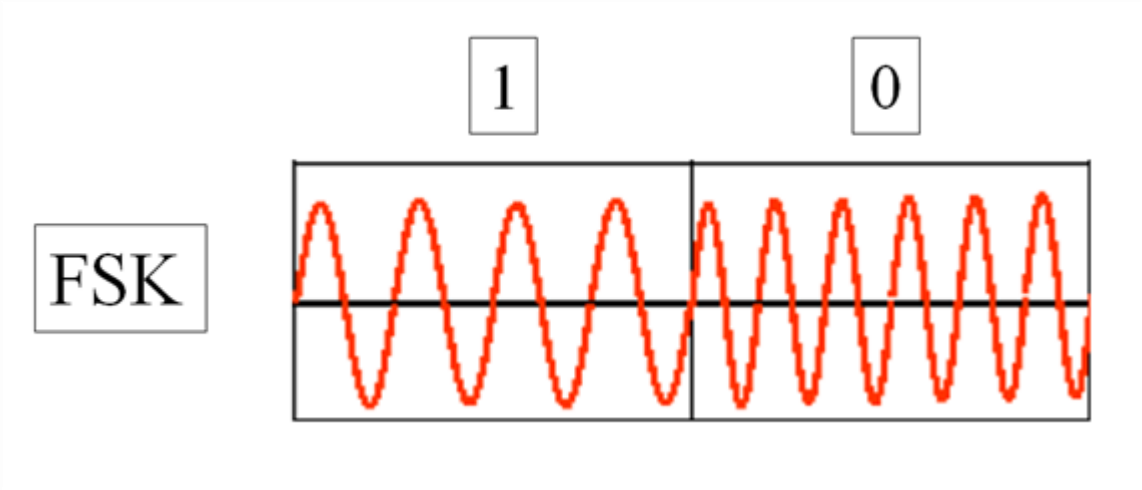


Az (1) értéket a vivőfrekvencia jelenléte; a (0) értéket a vivő hiánya jelzi. Rossz tulajdonsága a diszkrét komponens jelenléte.

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

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

1.2. Frekvencia billentyűzés (Frequency Shift Keying, FSK)

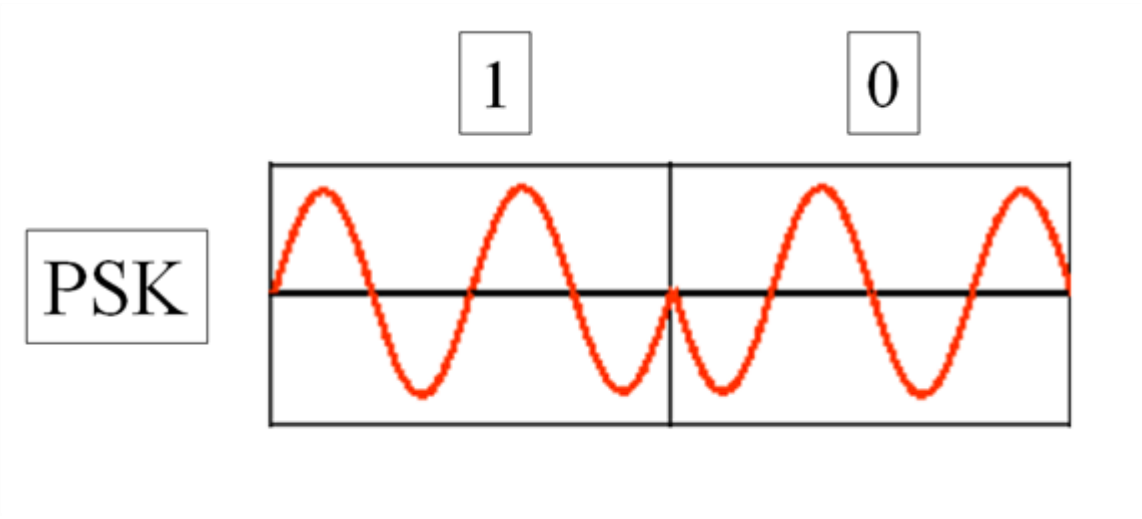


Az (1) értéket a vivőfrekvenciánál egy meghatározott frekvencialökettel (ω_d) kisebb; a (0) értéket pedig a vivőnél a megadott frekvencialökettel nagyobb frekvencia jelzi.

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

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

1.3. Fázis billentyűzés (Phase Shift Keying, PSK)



Az (1) értéket a vivőfrekvenciával azonos; a (0) értéket pedig a vivőhöz képest ellentétes fázisú jel jelzi.

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

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

A jelfüggvény fázisszögeltolással is felírható:

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

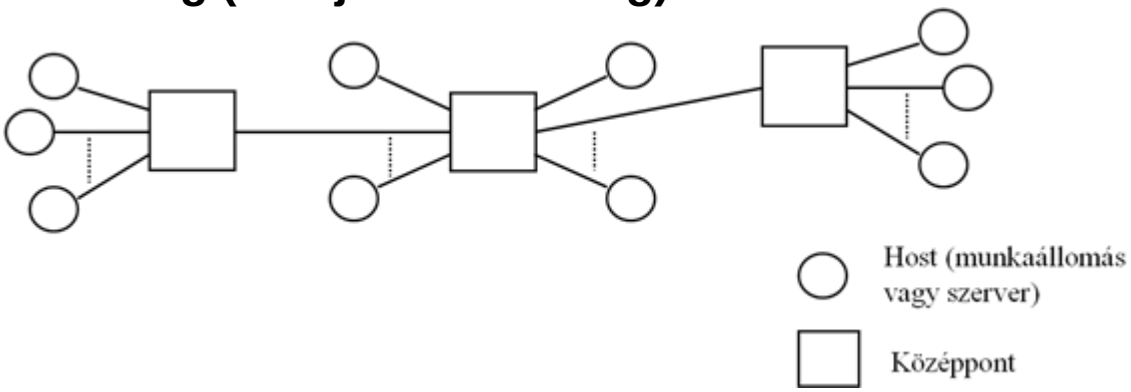
$S_{(0)}(t)= A\cdot\sin(\omega_v\cdot t+\pi)$

Ez a felírási forma általánosítási lehetőséget nyit a többszintű PSK alkalmazására: 180 fok helyett több kisebb eltolási érték alkalmazásával egy átviteli időegységben több bit átvitele is megoldható. Különösen gyakran alkalmazott a 4 szintű PSK (Quadrate PSK, QPSK), ahol 0, 90, 180 és 270 fokos eltolásokat alkalmaznak. ("Egy időegység alatt két bitnyi információ vihető át!")

7. fejezet - Topológiák

A topológiák a csomópontok térbeli elrendezési, összeköttetési lehetőségeit vizsgálják. A következőkben a legfontosabb (legalapvetőbb) topológiatípusokat tekintjük át, s vizsgáljuk, hogy egy esetleges csatorna meghibásodás (pl. kábelszakadás) milyen hatást gyakorol az adott topológia további működésére.

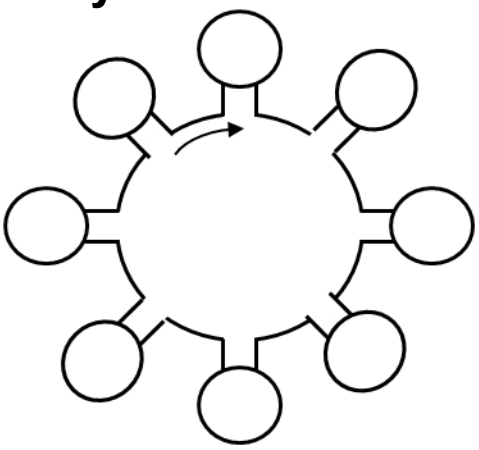
1. Csillag (kiterjesztett csillag)



A kiterjesztett csillag topológia az egy középponttal rendelkező klasszikus csillag elrendezés kiterjesztése. (Egy eredeti csillag csúcspontot egy újonnan kiépítendő csillagközéppont tulajdonsággal ruházunk fel). A kiterjesztés "mélysége" tipikusan egy-két szint.

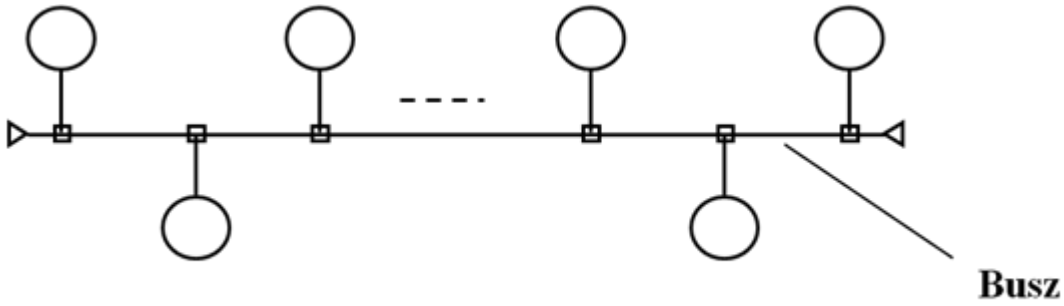
Kiterjesztett csillag topológia esetén a csatorna meghibásodása tipikusan egymástól elkülönülő, de önmagukban működőképes hálózati egységekre bontja fel a hálózatot.

2. Gyűrű



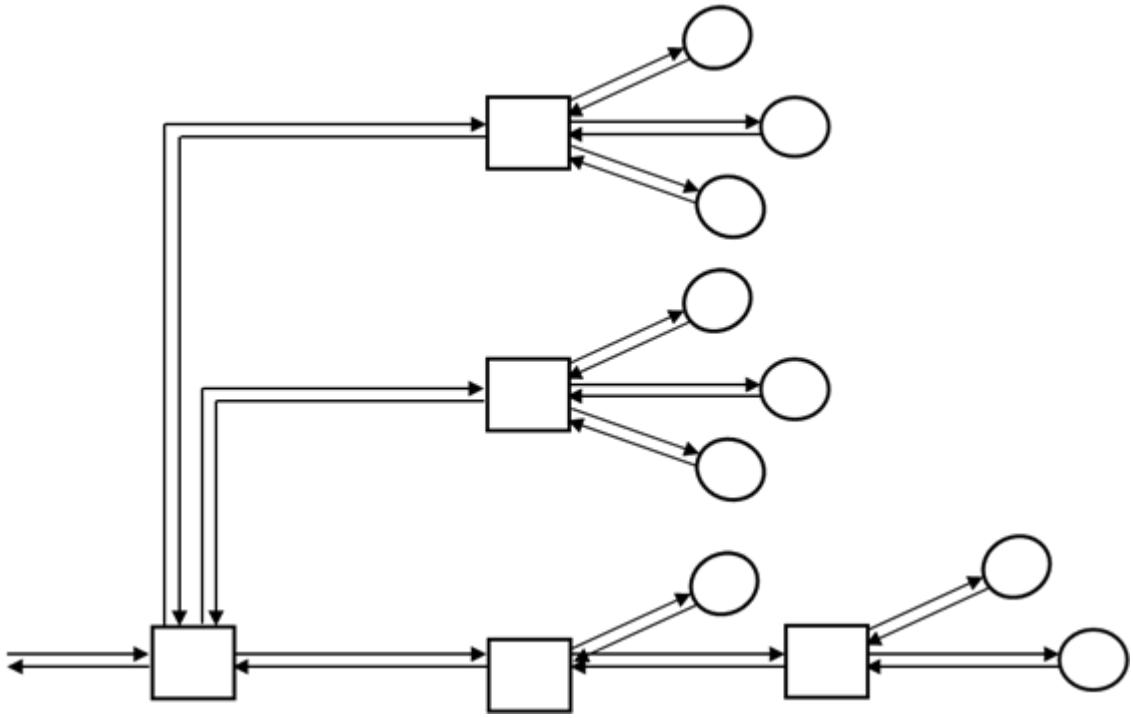
Gyűrű topológiában az átvitel tipikusan irányított, minden állomásnak van "megelőzője" és "rákövetkezője". A leggyakrabban használt gyűrű topológiák esetén a feladott keretet az adó állomás távolítja el a gyűrűből, így a gyűrű sérülése a teljes rendszer leállását okozhatja. Ennek a problémának a kezelésére/elkerülésére speciális megoldásokat használnak (pl. kétkörös, ellentétes irányítottságú gyűrű kiépítése).

3. Busz (sín)



Busz (vagy más néven sín) topológia esetében tipikusan több csomópont csatlakozik egy közös csatornára (kábelre, buszra). A közösen használt kábel sérülése a teljes rendszer leállását eredményezheti, mert a szakadási helyen megjelenő (nagymértékű) impedancia-homogenitási különbség a szakadás helyéről igen erős jelvisszaverődést eredményez (azaz, azon állomások sem tudnak egymással kommunikálni, melyek között a galvanikus kapcsolat még megmaradt).

4. Fa



A fa topológia a kiterjesztett csillag topológia általánosításaként is felfogható, ahol a "kiterjesztések" mélységének száma nem korlátozott (de a valóságban történő implementációknál természetesen véges). Tipikus jellemzője, hogy jelentős forgalomintenzitási eltérések jelenhetnek meg benne (pl. a fa "gyökerénél" ill a "levél" elemeknél.)

III. rész - Adatkapcsolati réteg

Ebben a részben az adatkapcsolati réteg működését vizsgáljuk. Az általános funkcionalitások áttekintése után konkrét implementációkat tanulmányozunk LAN és WAN adatkapcsolati réteg megoldásokra. Az egyik leglényegesebb, legfontosabb fejezet a LAN megoldások területén szinte egyeduralkodó Ethernet technológiák áttekintése.

8. fejezet - Adatkapcsolati réteg általános jellemzői

1. Szolgáltatások

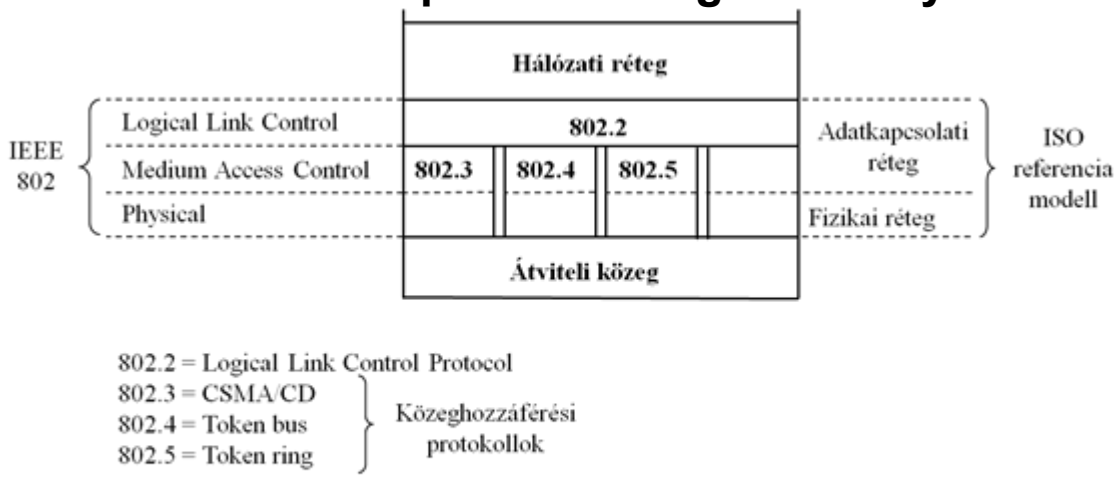
- **Jóváhagyás nélküli, összeköttetés-mentes:** Jó (megbízható) fizikai összeköttetés esetén célszerű alkalmazni. A vevő semmiféle visszajelzést nem ad az adó felé a keret vételével kapcsolatban. Igen sok implementáció használja (pl. tipikusan a vezetékes Ethernet technológiák alkalmazásai).
- **Jóváhagyásos, összeköttetés-mentes:** Nem megbízható (hibás, zajos) fizikai összeköttetés esetén célszerű. Alkalmazása tipikusan a vezeték nélküli technológiáknál a leggyakoribb.
- **Jóváhagyásos, összeköttetés-alapú:** Keretsorozatok átvitele esetén hatékony, ahol nem minden egyes keretre vonatkozóan történik visszajelzés.

2. Keretezés

Keretezés: A hálózati réteg felől érkező bitfolyamot keretekre kell tördelni, s a kereteket kell továbbítani (a fizikai rétegre támaszkodva). A keretek egymástól való elhatárolására (azaz arra, hogy az egyik keret vége, s a következő keret eleje ne olvadjon egybe) több megoldási ötletet alkalmazhatnak:

- Keretek közötti szünetek alkalmazása (időzítés!)
- Karakterszámlálás - a keret elején szerepel a keret hossza. Gondot jelenthet a hossz mező sérülése.
- 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.

3. IEEE LAN adatkapcsolati réteg szabványok



Az IEEE 802 protokoll család

9. fejezet - Közeghozzáférési alréteg (MAC)

1. MAC osztályozás

Statikus csatornafelosztás

- Frekvenciaosztásos multiplexelésen alapuló 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 multiplexelésen alapuló hozzáférés (TDMA). A közös csatornát előre meghatározott időszelet-használati besorolással megosztjuk a versenyhelyzetben lévő adók között, ezzel biztosítva, hogy egy időpillanatban csak egy adó küldhessen információt a csatornán.
- Hullámhossz-osztásos multiplexelés (WDM). Hasonló az FDM-hez, de ezt az optikai átvitelnél, a fény frekvenciatartományában alkalmazzuk.

Dinamikus közeghozzáférés

- Továbbítás figyelés nélkül
- Időréselt (Time Slot)
- Továbbítás figyeléssel (Carrier Sense Multiple Access)
- Ütközésérzékeléses (Collision Detect)
- Vezérjeles (Token)
- Kódosztásos (Code Divison Multiple Access)

Megjegyezzük, hogy maga a multiplexelés (FDM, TDM) a fizikai réteghez kötődő fogalom, de erre alapozva (egyszerű, statikus) közeghozzáférési mechanizmus alakítható ki, s ez a funkcionalitás már az adatkacsolati réteghez (MAC) tartozik.

2. Frekvenciaosztásos multiplexelés (FDM)

Hány részre (alcsatornára) osszuk fel a csatornát?

- Ütközés teljes kizárása: Az alcsatornák száma az adók számával azonos. Egyszerűen implementálható, de a működési hatékonysága alacsony (az éppen nem aktív adók erőforrásfoglalása veszteségként jelentkezik).
- Átviteli idő (átlagos válaszidő) minimalizálása: A működési hatékonyság optimalizálására helyezzük a hangsúlyt: A keretek csatornán való átviteli idejét szeretnénk minimalizálni.

  Sorbanállási modell N részre osztott csatornára:

  A keretek érkezési és továbbítási idejét független, exponenciális eloszlású valószínűségi változónak tételezzük fel.

  Kapacitás: C/N bps → 1 bit átviteli ideje: N/C sec.

  Keretérkezési intenzitás: λ/N keret/sec → N/λ másodpercenként érkezik keret.

  Kerethossz: 1/μ bit/keret

  Egy keret átviteli ideje: N/(μ·C) sec → (μ·C)/N az ún. "kiszolgálási intenzitás".

Little-tétel: Átlagos válaszidő = 1/(kiszolg. int. - érk. int.) = N/(μ·C-λ)

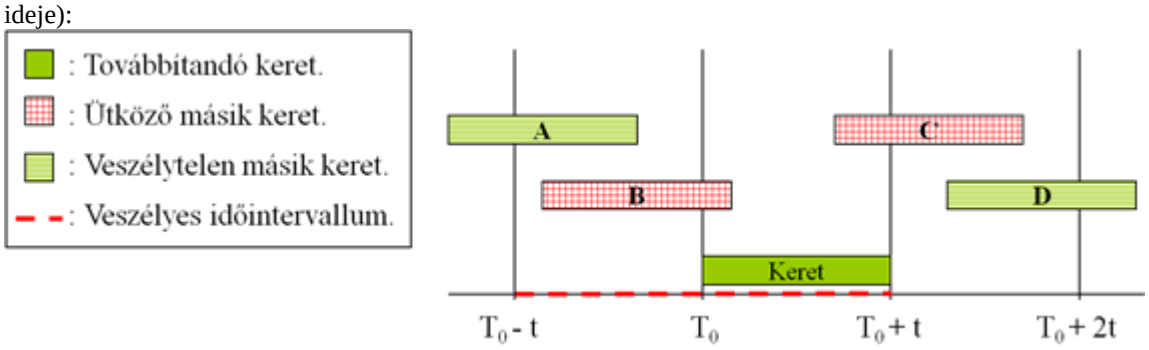
A keret várható továbbítási ideje tehát az alcsatornák számával lineárisan növekszik.

3. ALOHA

Továbbítás figyelés nélküli (legegyszerűbb) közeghozzáférés:

- A továbbítandó keret azonnal a csatornára kerül.
- Eredet: Hawai Egyetem – szigetek közötti rádiós kommunikáció.
- Egyszerű működés, könnyen implementálható.
- Az ütközések miatt a csatorna várható maximális kihasználtsága alacsony (18%).

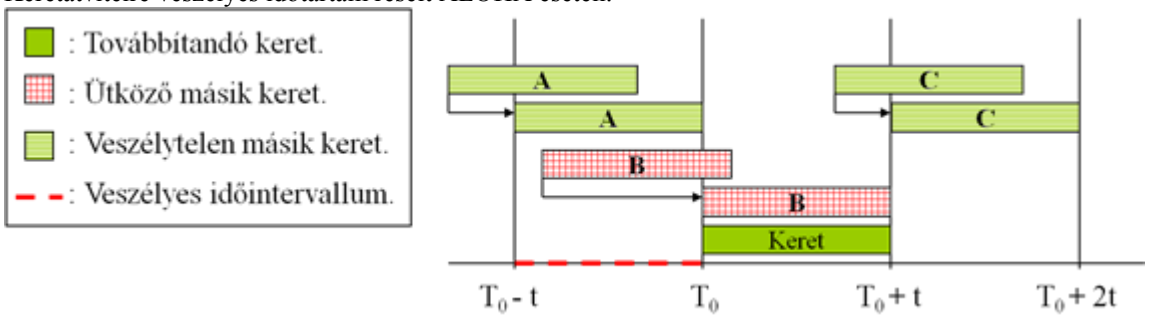
Keretátvitelre veszélyes időtartam ALOHA esetén (T_0 - a keret küldésének kezdőpillanata; t - egy keret átviteli ideje):



4. Réselt ALOHA

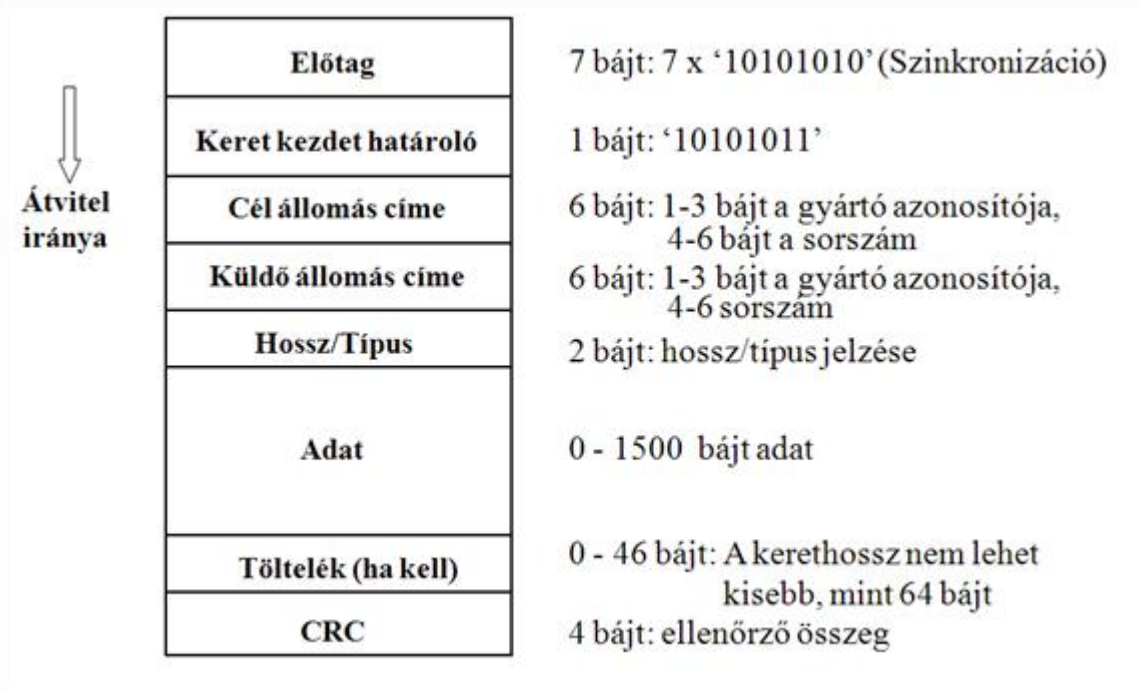
- A továbbítandó keret a következő időrés elején kerül a csatornára.
- A csatornakihasználtság egyszerűen növelhető (36%).

Keretátvitelre veszélyes időtartam réselt ALOHA esetén:



10. fejezet - Ethernet (CSMA/CD)

1. Ethernet (802.3) keretformátum



2. Ethernet

Klasszikus Ethernet - működési paraméterek:

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

Célcím lehet:

- Egy állomás pontos címe
- Csupa '1' bit: üzenetszórás (broadcast) - az üzenetet minden állomás veszi.

A küldő állomás címe nem lehet többes cím!

3. Ethernet kerettovábbítás (CSMA/CD)

1. Várakozás továbbítandó keretre, majd a keret formázása.
2. Csatorna foglalt?
    - **Igen:** Ugrás a 2. lépésre.

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

3. Van ütközés?
   - **Igen:** Zavarójelek küldése. Továbbítási kísérletek számának növelése. Folytatás a 4. lépéssel.
   - **Nem:** Átvitel befejezése. Sikeres átvitel jelzése. Ugrás az 1. lépésre.
4. Elértük a max. kísérletszámot (16)?
   - **Igen:** Sikertelen továbbítás jelzése. Ugrás az 1. lépésre.
   - **Nem:** Késleltetés kiszámítása és az idő kivárása. Ugrás a 2. lépésre.

A keret késleltetési idejének meghatározása:

A résidő vagy körbejárási 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: ~5 μs/1000 m)

Résidő = 2 * (kábelkésleltetés + ismétlők késleltetése) + tartalék idő

Résidő = 51,2 μs (2 * (2,5 km + 4 ismétlő késleltetése), 512 bit átvitelének ideje)

A várakozási idő a résidő véletlen számú többszöröse, amely az átviteli kísérletek számának függvénye:

1. ütközés után	0 vagy 1 résidőnyi várakozás véletlenszerűen
2. ütközés után	0, 1, 2 vagy 3 résidőnyi várakozás véletlenszerűen
3. ütközés után	0, 1, 2 … 7 résidőnyi várakozás véletlenszerűen
i. ütközés után	0, … (2^i-1) résidőnyi várakozás véletlenszerűen
10. ütközés után	0, … 1023 résidőnyi várakozás véletlenszerűen
11. ütközés után	- " -
.	- " -
15. ütközés után	- " -
16. ütközés után	az interfész kártya nem próbálkozik tovább, jelzi az átvitel sikertelenségét.

4. Ethernet keret fogadása

1. Van bejövő jel?
   - **Van:** Csatorna foglaltságának jelzése. Bitszinkronizálás, várakozás a keretkezdet-határolóra. Keret beolvasása.
   - **Nincs:** Ugrás az 1. lépésre.
2. Ellenőrző összeg (CRC) rendben (és kerethossz rendben)?
   - **Igen:** Tovább.
   - **Nem:** Keret eldobása. Ugrás az 1. lépésre.
3. Célcím = saját cím vagy csoportcím?
   - **Igen:** A vett adat továbbítása a felsőbb protokollrétegnek, majd ugrás az 1. lépésre.
   - **Nem:** Keret eldobása, majd ugrás az 1. lépésre.

5. Fast Ethernet (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:

- **100BASE-TX** fél-duplex módban 100 Mbit/s, duplex módban pedig 200 Mbit/s sebességű adatátvitelre képes.
- **100BASE-FX** különálló adási (Transmit, Tx) és vételi (Receive, Rx) útvonalai összesen 200 Mbit/s sebességű átvitelt tesznek lehetővé.

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

Különböző médiumokra (X) tervezték:

- Category 5 árnyékolatlan (UTP) kábel
- Category 5 árnyékolt (STP) kábel
- Optikai szál

Az FDDI hálózatra kifejlesztett 4B5B (4B/5B) bitkódolást adaptálták a 100BASE-X-re. 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, melyet réz kábelezésnél többszintű átvitellel (Multi-Level Transmit, MLT-3) továbbítanak.

6. 4B/5B bitkódolás

4B/5B adatszimbólumok:

4 bites adatcsoport	5 bites szimbólum
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011

4 bites adatcsoport	5 bites szimbólum
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

7. Gigabit Ethernet (802.3ab, 802.3z)

1000BASE-TX:

- Cat5e UTP kábelre (802.3ab)
- A Cat5e kábelek megbízhatóan legfeljebb 125 MHz-es átvitelre képesek egy érpáron.
- A Gigabites sávszélesség biztosítására mind a négy érpárt használatba vették.
- Egyetlen érpáron is duplex átvitelt lehetővé tévő áramkörökre (ún. hibrid áramkörökre) van szükség; segítségükkel a sávszélesség 250 Mbit/s-ra nőtt.
- A négy érpár alkalmazásával elérhetővé vált a kívánt 1000 Mbit/s sebesség.
- 1000 Mbit/s sebességű Ethernetnél a résidő 4096 bit, vagyis 512 oktett.

1000BASE-SX:

- 850 nm-es lézer vagy LED-es fényforrás többmódusú optikai szálon
- Olcsóbb, kisebb távolságok áthidalására alkalmas.

1000BASE-LX:

- 1310 nm-es lézerforrások egy- vagy többmódusú optikai szálon
- Az egymódusú optikai szálakon lézert használva akár 5000 méteres távolságra is továbbíthatók a jelek.

Az adásra (transmit, Tx) és a vételre (receive, Rx) külön optikai szál szolgál, az összeköttetés eleve duplex jellegű.

8. Ethernet kapcsolás, szegmentálás

Ütközési tartomány akkor jön létre, ha több számítógép is csatlakozik ugyanahhoz a megosztott átviteli közeghez, médiához (HUB).

A második rétegbeli készülékek felosztják az ütközési tartományokat. Ezek az Ethernet készülékekhez rendelt MAC-címek alapján szabályozzák a keretek továbbítását. Második rétegbeli készüléknek a hidak és a kapcsolók számítanak.

A második és harmadik rétegbeli készülékek az ütközéseket nem továbbítják. Az ütközési tartományokat a harmadik rétegbeli készülékek is kisebb tartományokra osztják.

9. Kapcsolók (switchek)

A kapcsoló lényegében egy gyors működésű többportos (2. rétegbeli) híd. Mindegyik port külön ütközési tartományt hoz létre. (Pl. egy 24 portos kapcsoló 24 különálló ütközési tartományt hoz létre.)

A kapcsolók minden portjukhoz egy táblázatban (ún. kapcsolási táblában) tárolják le az adott porton elérhető gépek Ethernet (vagy más néven MAC) címét. A kapcsolók dinamikusan töltik fel és tartják karban kapcsolási táblájukat (az érkező keretek forráscíme alapján). A kapcsolási táblát egy ún. tartalom szerint címezhető memóriában tárolják (content-addressable memory, CAM).

A CAM olyan memória, amely a hagyományos memóriákhoz képest fordítottan működik: ha valamilyen adatot táplálunk be (Ethernet cím), a hozzá tartozó memóriacímet adja kimenetként. A CAM révén a kapcsolók kereső algoritmus futtatása nélkül is meg tudják találni az adott MAC címhez tartozó portot.

10. Ethernet kapcsolás folyamata (Ethernet switching)

A kapcsoló a beérkező Ethernet keret célcímét keresi a kapcsolási táblájában:

- Ha a célcím üzenetszórási cím (48 db 1-es bit érték), akkor a keretet a kapcsoló valamennyi portján továbbítja (kivéve az érkezési portot).
- Ha a célcím nem található meg a kapcsolási táblában, akkor valamennyi portján továbbítja a keretet (kivéve az érkezési portot).
- Ha a célcím megtalálható a kapcsolási táblában, akkor a hozzá tartozó porton továbbítja a keretet (feltéve, hogy az nem azonos a keret érkezési portjával).

Kapcsolási módszerek:

- **Tárol és továbbít:** A keret továbbítása a teljes keret megérkezése után kezdődik meg. A kapcsoló újraszámítja a keretellenőrző összeget (CRC, vagy más néven Frame Control Sequence, FCS), 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.)

Az Ethernet kapcsolás működési vázlata (interaktív animáció)

11. fejezet - Vezérjeles közeghozzáférés, Token ring

1. Vezérjeles gyűrű, Token ring (ISO/IEEE 802.5)

A vezérjeles gyűrű eliminálja az ütközést: van egy speciális keret (vezérjel, token), s egy állomás csak akkor adhat keretet, ha birtokolja a vezérjelet. Az állomás az adás után a vezérjelet továbbadja a soron következő állomásnak.

Az állomások logikailag gyűrű topológia alapján működnek (megelőző, rákövetkező csomópont), de fizikailag a csomópontok egy ún. TCU (Trunk Coupling Unit) egységhez csatlakoznak (fizikailag csillag topológia). A TCU reléket és működtető elektronikát tartalmaz, a logikai gyűrű szervezése a TCU feladata. Ez biztosítja, hogy egy állomás kikapcsolásakor (esetleg meghibásodásakor) a gyűrű záródjék.

Ma már kevésbé elterjedt, de a működési filozófiát célszerű áttekinteni.

Vezérjeles gyűrű működési elve:

1. Ha egy állomás keretet akar továbbítani, először meg kell várnia vezérjelet (token-t).
2. Ha megjött a vezérjel, a továbbítandó keretet (amely tartalmazza a feladó és a célcímet) bitenként továbbítja.
3. Minden állomás bitenként veszi és (a rákövetkező felé) továbbküldi a keretet.
4. A címzett állomás a beolvasott keretet feldolgozza, s ugyanúgy továbbítja, mint a többi állomás, azzal a különbséggel, hogy a címzett a válasz biteket is beállítja a keret végén (jelezve a sikeres, vagy sikertelen átvitelt).
5. A keretet a feladó állomás távolítja el a gyűrűből. A feladó a válasz biteket is feldolgozza.
6. A feladó állomás továbbküldi a vezérjelet.

A vezérjel továbbadásának alternatív megoldásai:

- **Lassú gyűrű (4 Mbps):** Egyszerre csak 1 keret van a gyűrűben. A vezérjelet a feladó állomás csak a keret visszaérkezése után továbbítja.
- **Gyorsabb gyűrű (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).

12. fejezet - Kódosztásos közeghozzáférés (CDMA)

1. Alapötletek

Klasszikus probléma: Egy rádiófrekvenciás csatornán egy időpillanatban csak egy adás folyhat.

Hogyan lehetne egy csatornán párhuzamosan több adást is folytatni?

Megoldási ötletek, analógiák:

- **TDMA:** Egyszerre csak egy valaki beszélhet.
- **FDMA:** A beszélgetők különböző helyekre vonulva (egymást nem zavarva) beszélgetnek.
- **CDMA:** A beszélgetők különböző nyelveken beszélgetnek.

2. Matematikai háttér

Kiindulási állapot: Minden állomáshoz egy m bit hosszú kódot (chip-et, töredéket) rendelünk (bipoláris kódolással reprezentálva). Ez a chip reprezentálja az állomástól feladott 1 bitértéket, a 0 bitértéket pedig az inverze. Jelölés:

$S_1 = (s_1, ..., s_m)$,

$S_0 = (-s_1, ..., -s_m)$; $s_i = +1$, vagy -1, $i=1,...,m$.

S és T chip összege: $S + T = (s_1 + t_1, ..., s_m + t_m)$

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

A bipoláris kódolást kihasználva a szorzás és összeadás definíciójának felhasználásával az alábbiak könnyen beláthatók:

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

$S_1 * S_0 = -1$,

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

Működési feltétel: A külöböző állomásokhoz rendelt chip-ek ortogonálisak, azaz skaláris szorzatuk zéró:

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

Vételi folyamat: A vett (érzékelt) vektorösszegből az adóchippel szorozva a nekünk küldött bitérték meghatározható.

Példa a CDMA működésére.

Három állomás (A, B, C) egyidejű adását vizsgáljuk. Legyen m = 4.

A_1 = (+1, +1, -1, -1); (1-es bit jelzése). A_0 = (-1, -1, +1, +1); (0-ás bit jelzése).

B_1 = (+1, -1, +1, -1); (1-es bit jelzése). B_0 = (-1, +1, -1, +1); (0-ás bit jelzése).

C_1 = (-1, -1, -1, -1); (1-es bit jelzése). C_0 = (+1, +1, +1, +1); (0-ás bit jelzése).

Az állomások által egyidőben feladott bitértékek:

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

A csatornán megjelenő vektor (jelsorozat): $A_0 + B_1 + C_0 = (+1, -1, +3, +1)$

A partnere: $A_1 * (A_0 + B_1 + C_0) = A_1 * A_0 = -1$, tehát A 0-ás bitértéket küldött.

B partnere: $B_1 * (A_0 + B_1 + C_0) = B_1 * B_1 = +1$, tehát B 1-es bitértéket küldött.

C partnere: $C_1 * (A_0 + B_1 + C_0) = C_1 * C_0 = -1$, tehát C 0-ás bitértéket küldött.

13. fejezet - WAN adatkapcsolati réteg megoldások

1. SLIP

A SLIP (Serial Line Internet Protocol, első verzió: RFC 1055) egy régi WAN adatkapcsolati réteg megoldás. Célja az IP csomagok küldése soros (pont-pont) linken keresztül. Számos kellemetlen előírása/hiányossága miatt ma már kevésbé használják:

- Csak IP hálózati protokoll támogatott.
- Statikus IP címkiosztást feltételez.
- Nincs hibajelzés, -javítás.
- Nincs authentikáció.

2. PPP

A PPP (Point to Point Protocol, első verzió: RFC 1661, 1662, 1663) az egyik legelterjedtebb nyílt, gyártófüggetlen standard (többprotokollos) WAN adatkapcsolati réteg protokoll. A keretezést eleje és vége jelzőkarakterekkel oldja meg.

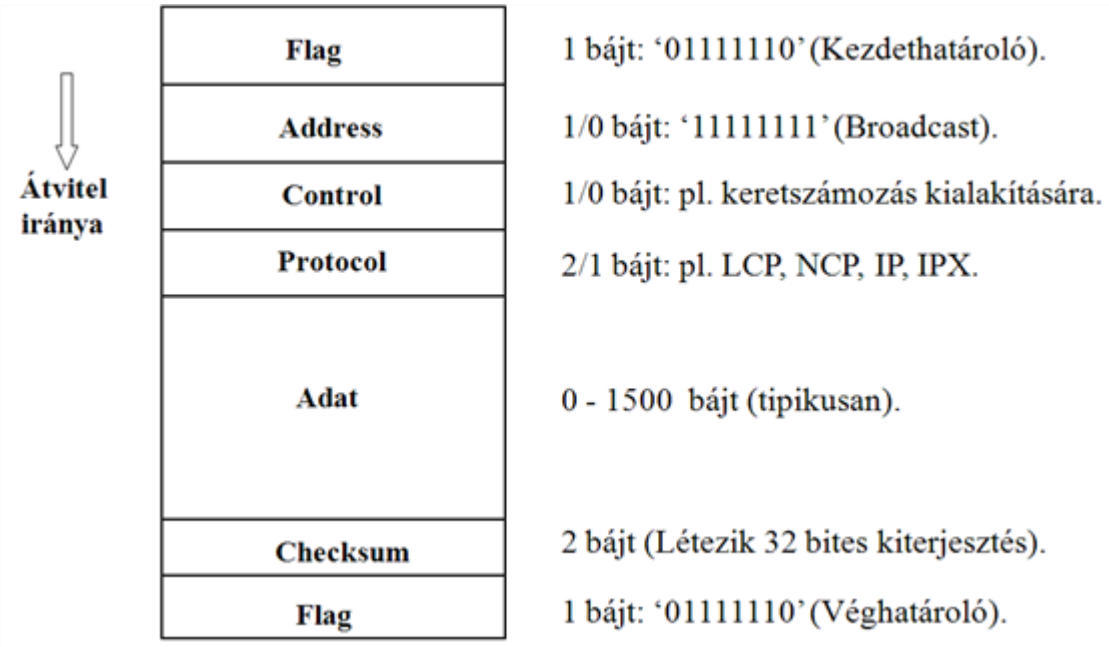
Két részből áll:

LCP (Link Control Protocol): Link felépítés, tesztelés, leállítás.
NCP (Network Control Protocol): Hálózati protokoll támogatás. Minden hálózati réteg protokollhoz kell egy azt támogató NCP.

Többféle autentikációt támogat:

PAP (Cleartext jelszóátvitel a kommunkáció kezdetén.)
CHAP (Titkosított jelszóátvitel, bármikor kérhető.)

PPP keretformátum.



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

3. N-ISDN technológia

ISDN: Integrated Services Digital Network. Kísérlet az analóg telefonok digitális leváltására.

Standard 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 (signaling).

Három standard kombináció:

- Basic: 2B + $1D_{(16)}$
- Primary: 23B + $1D_{(64)}$ (USA), 30B + $1D_{(64)}$ (EU)
- Hibrid: 1A + 1C (kevésbé elterjedt)

Ez a 64 kbps-os csatornára fókuszáló megoldás a Narrowband ISDN.

Ma már nagyobb sávszélesség igények tapasztalhatók.

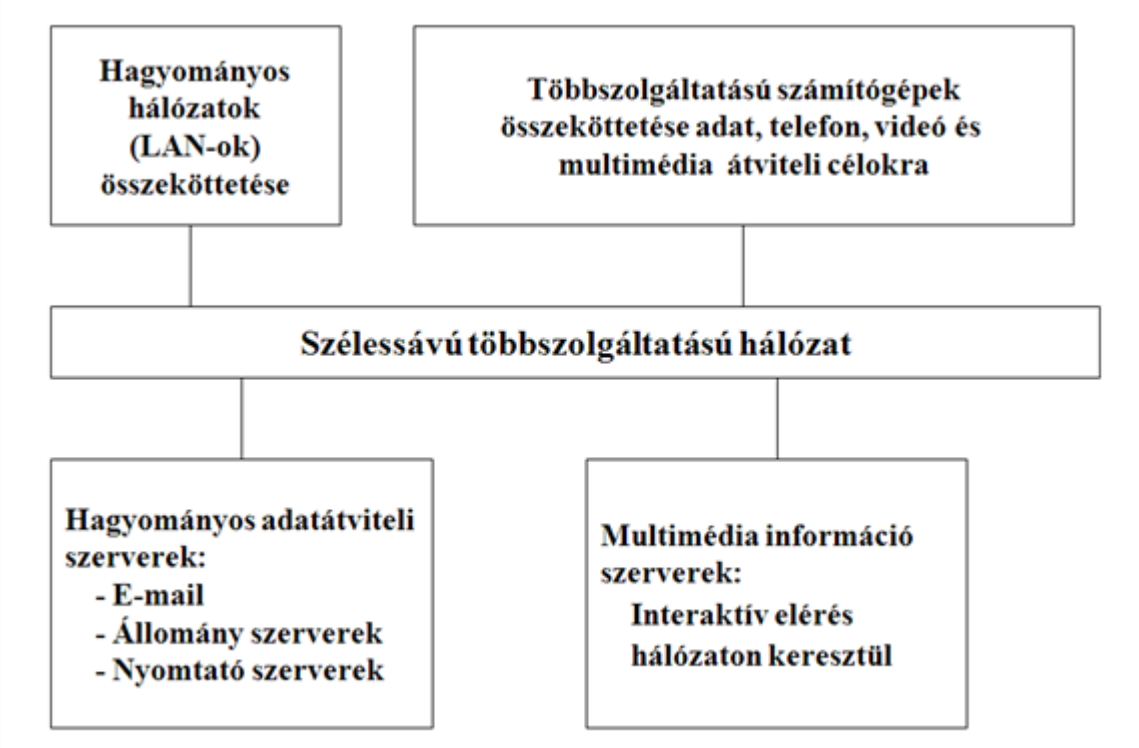
4. Szélessávú, többszolgáltatású hálózatok (B-ISDN)

A mai hálózatoknál sokféle szolgáltatási igénnyel találkozhatunk:

Adattovábbítás, hang- és videoátvitel, multimédia dokumentumok átvitele, számítógéppel segített oktatás (Computer Aided Learning = CAL)

Ezeket a szolgáltatásokat nyújtó számítógépeket szoktuk többszolgáltatású munkaállomásoknak nevezni. A hálózatokat pedig, amelyek összekapcsolják őket, **szélessávú, többszolgáltatású hálózatoknak** (B-ISDN) nevezzük.

A követelmények messze meghaladják az adathálózatokkal szemben támasztott követelményeket.



Különböző applikációs médiatípusok sávszélesség-szükségletei:

- Az audió és videó átvitele állandó bitsebességet, s kicsi késleltetést igényel.
- Videókonferencia rendszerekben az egymás utáni képkockák keveset változnak, képtömörítés lehetséges.
- Hang, kép és videó átvitele esetén a tömörítés lehet információvesztő, amely jelentősen csökkenti az átviendő információt.

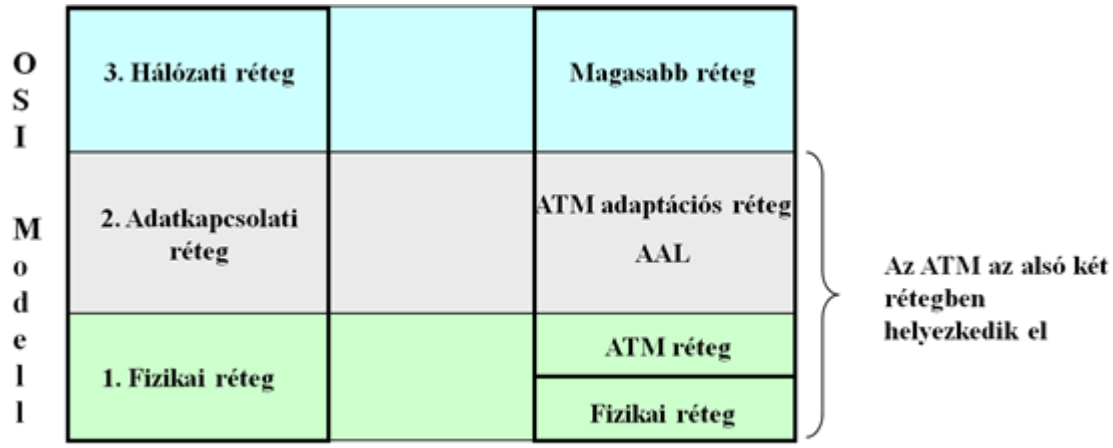
Az állandó bitsebességet igénylő médiatípusok az eddig tárgyalt (minőségi garanciákat nem támogató) hálózatokkal nem vihetők át biztonsággal.

Olyan új technológiára van szükség, amely az adatátvitelen kívül a többi médiatípus átvitelére is alkalmas. Az egyik ilyen hálózat az **ATM (Asynchronous Transfer Mode)** cellakapcsolt hálózat.

5. ATM (Asynchronous Transfer Mode)

5.1. Az ATM protokoll architektúrája

Az ATM három réteggel rendelkezik, amelyek az OSI 1-2 rétegének felelnek meg:



Az ATM funkcionális rétegei

Az ATM hálózat különböző szolgáltatásokat kínál a különböző típusú alkalmazások számára. Az ATM adaptációs réteg kínálja ezeket a szolgáltatásokat az alkalmazások számára, és fedi el a cellakapcsolást, amellyel az átvitelt az alsó két réteg végzi.

5.2. ATM

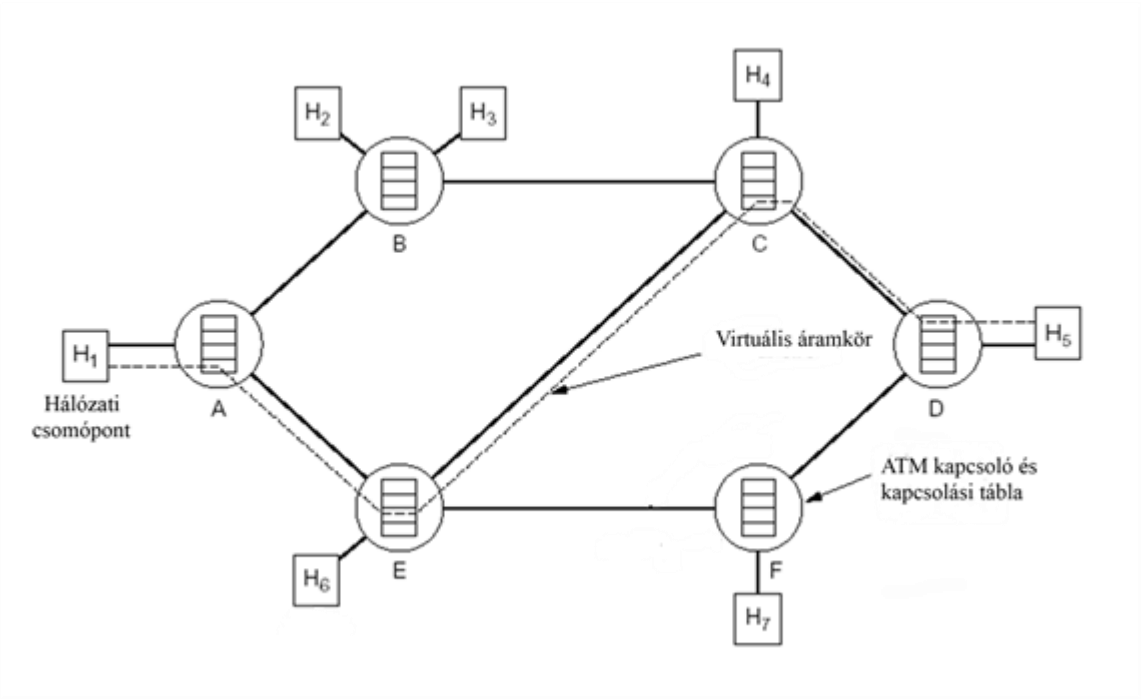
A különféle átviendő médiatípusok miatt, amelyeknek egy része minőségi szolgáltatást követel meg a hálózattal szemben, nem lehet osztott használatú átviteli közeget használni. Az ATM hálózat hálószerű (mesh) topológiát követ, amelyben egymással összeköttetésben lévő kapcsolók (ATM switch-ek) biztosítják az átvitelt a kommunikáló állomások között. Az elv hasonlítható a telefon hálózathoz.

Mielőtt két állomás kommunikálna egymással, a kapcsolókon keresztül egy útvonalat kell felépíteniük. Minden cella, amely az adott híváshoz tartozik, ezen az útvonalon halad keresztül. Az útvonalat (ill. az azon működtetett kommunikációs kapcsolatot) virtuális áramkörnek, vagy virtuális összeköttetésnek nevezzük (Virtual Circuit: VC). Két típusa van:

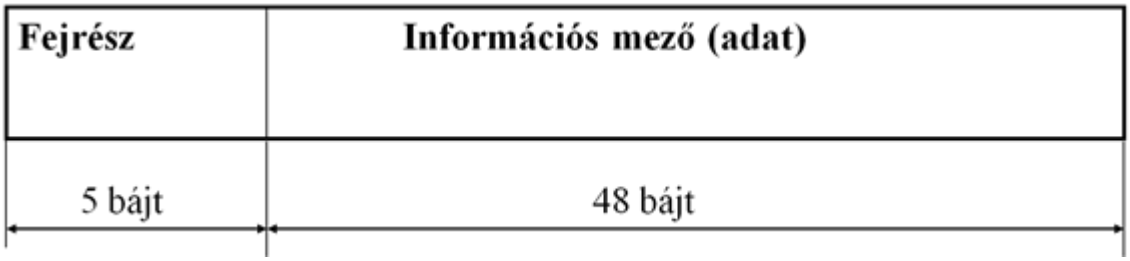
PVC (Permanent VC): Kézi konfigurációval alakítják ki.
SVC (Switched VC): A kommunikáció előtt alakítják ki (majd a végén lebontják).

A kapcsolat felépítése során az igényelt szolgáltatástípusnak megfelelő átviteli kapacitás lesz lefoglalva a kapcsolókban. Van olyan szolgáltatás, amely rögzített bit sebességet igényel; van olyan, amelyik változó bit sebességgel dolgozik, de az átvitt adatok átlagos mennyisége rögzített; és van olyan, amelynél nincs semmilyen megkötés a szolgáltatás minőségére.

5.3. Működési váz

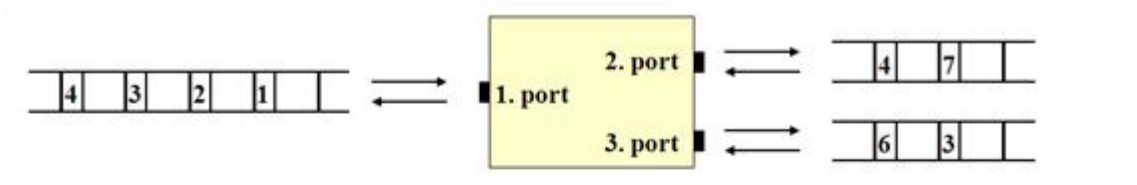


5.4. Az ATM cella felépítése



Az ATM cella (fix, 53 bájt hosszúságú keret) 5 bájtos fejrészből és 48 bájtos adatmezőből áll. A fejrész alapján két különböző ATM cellatípust különíthetünk el: A felhasználói végberendezés (ami tipikusan forgalomirányító, vagy más "DTE" eszköz) egy ún. "UNI - User to Network Interface" típusú cellaformátumot használ a szolgáltatói oldal (tipikusan ATM switch, vagy más DCE eszköz) elérésére. Az ATM kapcsolók egymás között pedig egy ún. "NNI - Network Node Interface" típusú cellaformátumot használnak. Mindkét cella fejrészében az egyik legfontosabb (legtöbb bitet használó) információt a kapcsolat azonosítására szolgáló VPI (Virtual Path Identifier) és VCI (Virtual Channel Identifier) mezők adják. A VPI ugyanazon végponthoz menő csatornákat (VCI-ket) fogja össze. A VPI és VCI mezők együttesen látják el az azonosítási funkciót. Értékük tipikusan nem globális (ATM felhő egészére érvényes) azonosító, hanem csak az adott ATM kapcsolóra érvényes azonosító. Az ATM kapcsolók a cella fejrészében lecserélhetik a VPI és VCI értékeket a cella továbbítása során.

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

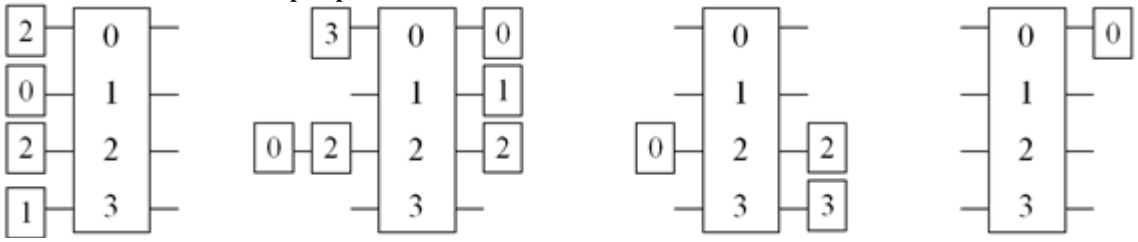
KA = Kapcsolat azonosító (VPI+VCI)

5.5. Az ATM kapcsolás hatékonysági vizsgálata

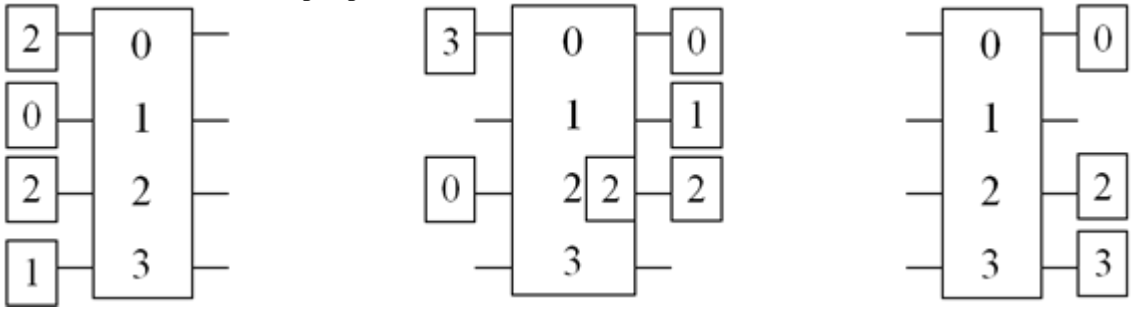
A kapcsolástechnikában (switching) egy nagyon fontos hatékonyságot befolyásoló kérdés, hogy az esetleges forgalmi túlterhelések esetén hogyan képezzük a várakozási sorokat. A cellák sorrendhelyes kézbesítését az ATM technológiának garantálnia kell egy áramkörön belül. Azonban a több bemenetről ugyanarra a fizikai kimenetre tartó cellák továbbításánál többféle továbbítási elv is vizsgálható.

A következőkben egy kis példán keresztül vizsgáljuk az ATM kapcsoló működését: Az első esetben a várakoztatási sort a bemeneti oldalon képezzük, a második esetben pedig a várakoztatási sort a kimeneti oldalon hozzuk létre.

ATM switch működése input puffer alkalmazásával:



ATM switch működése output puffer alkalmazásával:



Eredmény: Kevesebb kapcsolási ciklus szükséges, ha a várakoztatási sort a kimeneti oldalon (output puffer) képezzük.

Karol, Hluchyj és Morgan 1987-ben "Input Versus Output Queueing on a Space-Division Packet Switch," című cikkükben bebizonyították, hogy az output pufferek alkalmazása hatékonyabb.

14. fejezet - ADSL (Asymmetric Digital Subscriber Line)

1. Alapötletek

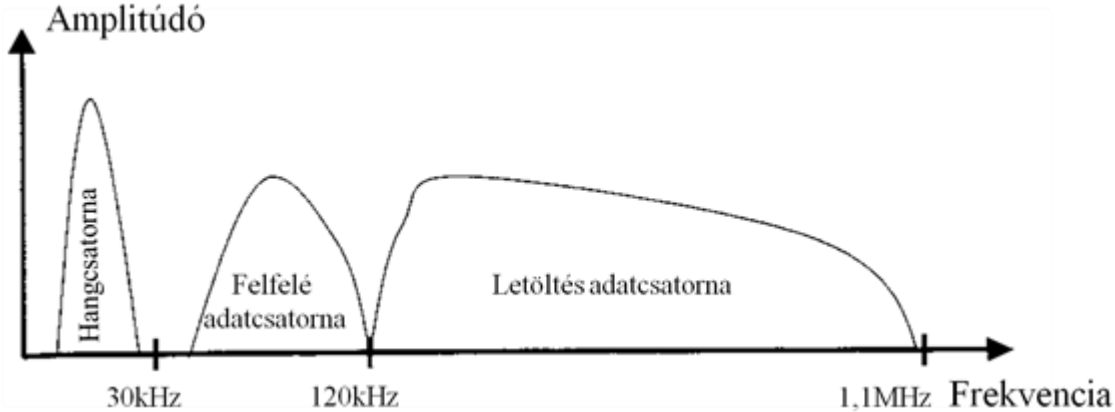
1.1. Az ADSL működésének jellemzői/ötletei

A felhasználók nagytömegű letöltéséhez nagy(obb) sávszélesség szükséges. A (várhatóan lényegesen kisebb mennyiségű) adatfeltöltéshez kisebb sávszélesség is elelgendő. Ennek következtében a rendelkezésre álló sávszélességet (frekvenciatartományt) aszimmetrikus módon célszerű felosztani.

A telefonos technológiában a végfelhasználók csatlakoztatására használatos réz érpár már lehetővé teszi 1-2MHz-es sávszélesség használatát km nagyságrendű távolságra, így ez már a gyakorlatban is alkalmazható telefonvezetéken kialakítandó nagysebességű kapcsolat létrehozására.

1.2. ADSL frekvenciatartományok

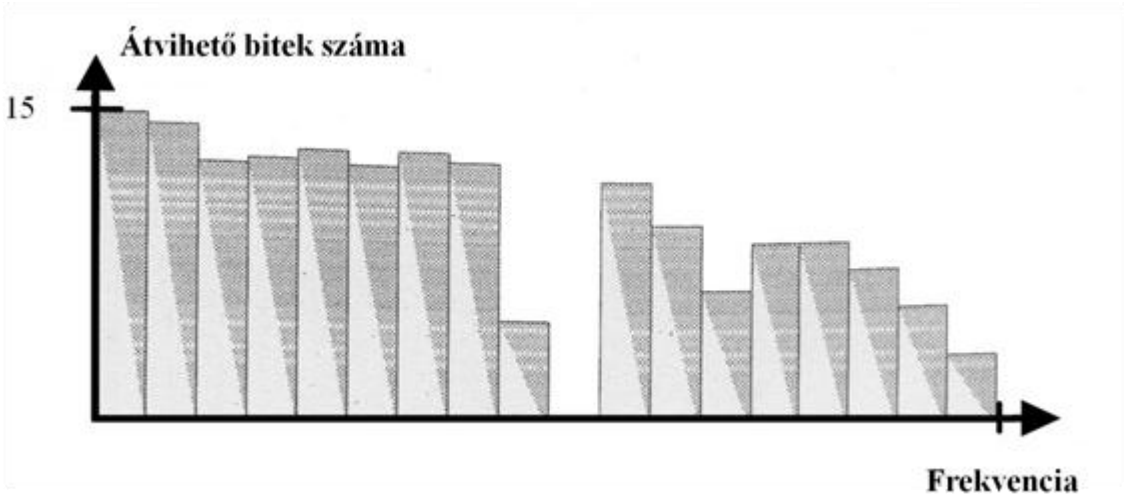
Az ADSL alapvetően FDM alapon osztja fel a csatornát a három kommunikációs cél (hang, adatfeltöltés, adatletöltés) között. A telefonos hangkommunikáció számára néhány kHz sávszélesség szükséges, erre a célra foglalják le az alsó ~30 kHz-es tartományt (melyet a tényleges hangátvitel nem használ ki teljesen). A következő ~80 kHz-es tartományt az adatfeltöltési célra alkalmazzák. A megmaradó ~1000 kHz-es tartomány pedig az adatletöltési célt szolgálja:



1.3. Zavarforrások az ADSL adatátvitelben

Az ADSL letöltési irányban komoly zavarforrásként jelennek meg a közelben működő nagyteljesítményű középhullámú rádióadók: Pl. a Solton működő rádióadó 540 kHz-en 3MW (megawatt!) teljesítménnyel sugározza a Kossuth rádió műsorát. Az adó közelében ez nagyon rossz jel-zaj viszonyt eredményez ("a zaj erősebb a jelnél").

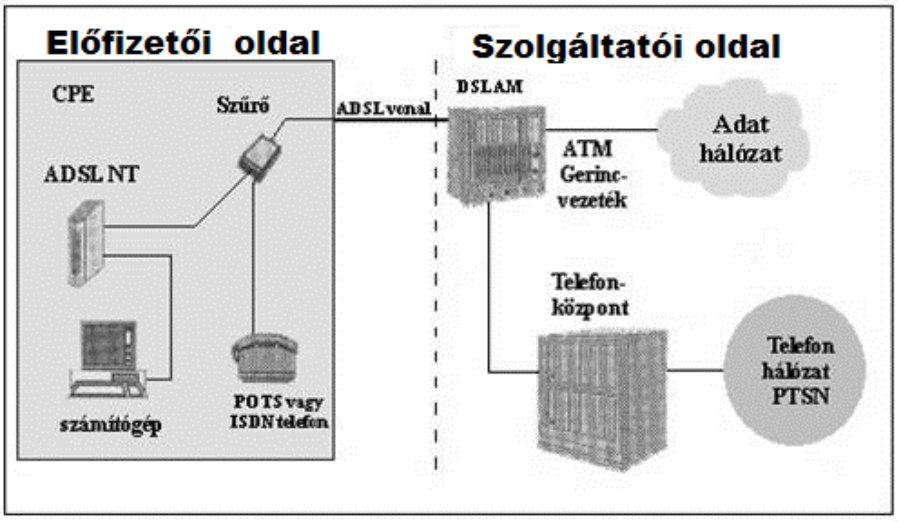
A probléma kezelésére egy széleskörűen alkalmazott megoldás a DMT (Discrete MultiTone) modulációs technológia: A rendelkezésre álló frekvenciatartományt nagyon kicsi (4,3 kHz) sávszélességű alcsatornákra bontják, s az egyes alcsatornákon külön-külön meghatározzák a jel-zaj viszonyt (ill. erre épülve a bitrátát):



1.4. Az ADSL rendszertechnikai felépítése

Az ADSL előfizetői oldalán az előfizetői vonal (helyi hurok, local loop) végén egy szűrővel különítik el a hang- és adatátviteli frekvenciatartományokat. A szolgáltatói hálózat végpontját az ADSL NT (Network Termination, vagy ADSL modem) eszköz képviseli. Ennek kimenete egy hálózati csatlakozásra közvetlen módon használható (tipikusan RJ-45) interfész, melyre az előfizető Ethernet (vagy authentikációs célok miatt PPP over Ethernet) technológiával kapcsolódik. A szűrőt és az ADSL NT-t természetesen egyetlen eszközben is implementálhatják, s esetlegesen további (pl. forgalomirányítási) funkciókkal is kiegészíthetik.

A szolgáltatói oldalon az előfizetői vonalakat (több száz előfizetői vonalat) egy DSLAM (Digital Subscriber Line Access Multiplexer) eszközbe csatlakoztatják. A DSLAM egység egy nagykapacitású ("trönk") vonalon multiplexálja az előfizetők forgalmát az Internet felé.



Az ADSL technológiák (ill. ezek szimmetrikus variánsai) óriási fejlődésen mentek keresztül. Ennek következtében számos DSL verzió létezik. A következő táblázat egy rövid áttekintést ad a legfontosabb technológiák jellemzőiről:

Megnevezés	Letöltési sebesség (Mbps)	Távolság (m)	Megjegyzés
ADSL	8	6000	1.1 MHz
ADSL2	12	4000	1.1 MHz
ADSL2+	24	4000	2.2 MHz

Megnevezés	Letöltési sebesség (Mbps)	Távolság (m)	Megjegyzés
SDSL	1.5	3000	Szimmetrikus
VDSL	50	1500	50Mbps - 300m
VDSL2	100	1500	30MHz

IV. rész - Hálózati réteg

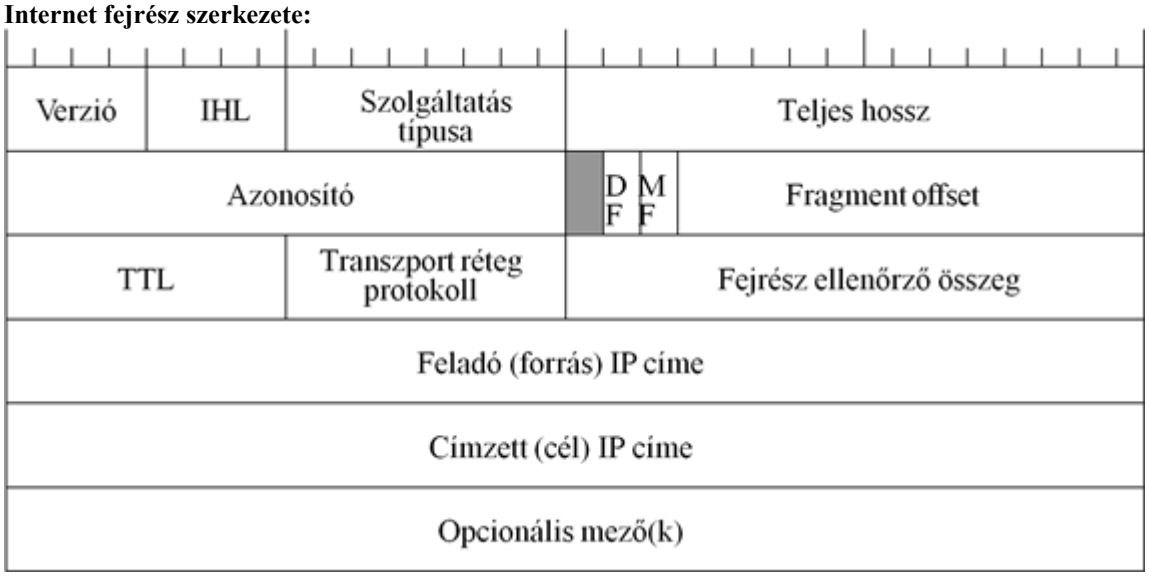
A hálózati réteg feladata a kommunikációs kapcsolat (adatátvitel) megvalósítása olyan csomópontok között is, melyek között nem áll fenn közvetlen csatorna (vagy adatkapcsolati rétegbeli) összeköttetés. A legfontosabb feladat a hálózati rétegben a címzési rendszer kialakítása és a forgalomirányítás. Ebben a részben az IP hálózati technológiát tekintjük át.

15. fejezet - Az IP technológia hálózati rétege

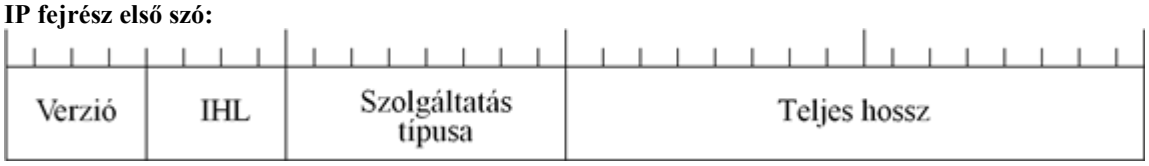
1. Az IP hálózati protokoll

IP (Internet Protocol, RFC 791) a TCP/IP referenciamodell általános adatszállításra szolgáló hálózati réteg protokollja. Összeköttetés mentes (datagram) szolgáltatást nyújt a szállítási réteg felé. Az IP fejrész minimum 5, maximum 15 db 32 bites szóból áll. Az Ethernet keret típusmezőjének értéke 0x0800.

Internet fejrész szerkezete:

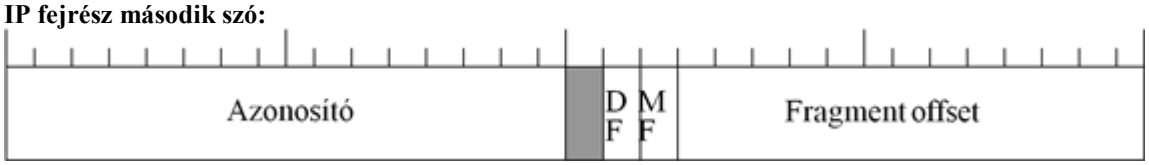


IP fejrész első szó:



Az első szó általános információkat tartalmaz: Verziószám; IP fejrész hossza (szavakban); szolgáltatás típusa (TOS); adatmező hossza (bájtokban mérve).

IP fejrész második szó:



Az IP fejrész második szava a csomag darabolásával kapcsolatos információkat tartalmazza. Darabolásra akkor van szükség, ha a csomag (túl nagy mérete miatt) nem ágyazható be az adatkapcsolati réteg keret adatmezőjébe. Az azonosító a csomagdarabok összetartozását jelzi. A DF jelzőbit a csomag darabolhatatlan voltát jelzi. Az MF jelzőbit 0 értéke jelzi, hogy az adott darab (fragment) a sorozat utolsó eleme. Az offset érték a darab eredeti csomagbeli helyét mutatja (8 bájtos egységben mérve).

IP csomagok darabolása (fregmentálás):

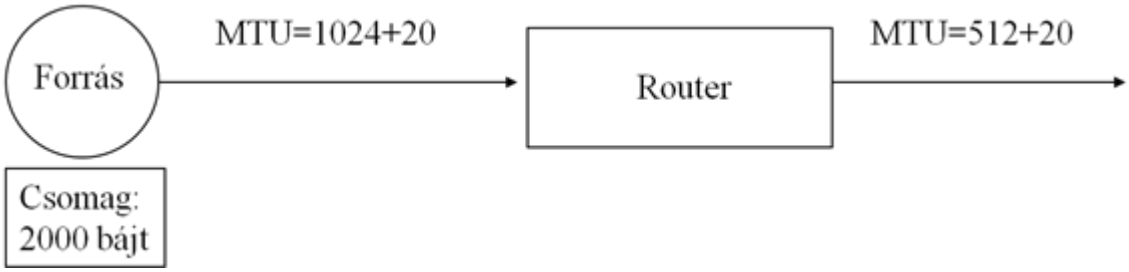
Az azonosítót az adó állomás adja, és minden fregmentben változatlan marad. Az offset kezdetben nulla étékű. Darabolást bármely állomás (router) végezhet a csomag ill. csomagdarab küldése előtt. (Datalink MTU miatt). Darabolás az adatmező valamely 8 bájtos egységhatárán következhet be. Az offset értékben a fregment első bájtjának az eredeti (nem darabolt) csomagbeli helyét jelezzük 8 bájtos egységben számolva. A darabok összeillesztését a célállomás végzi az IP fejrész második szavának adatai alapján.

Darabolás példa:

A forrás állomáson küldésre vár egy 2000 bájt méretű csomag (+20 bájt IP fej).

A forrás 1024+20 bájt MTU értékű linkhez kapcsolódik.

Az első forgalomirányító 512+20 bájt MTU értékű linken küldi tovább a csomagot.



1. **Az eredeti (darabolatlan) csomag IP fejrészének 2. szava:**

00000000 10110010 0 00 00000 00000000

Offset = 0

2. **A forrás által feladott csomagok információi (2. szó):**

00000000 10110010 0 01 00000 00000000

Offset = 0

00000000 10110010 0 00 00000 10000000

Offset = 0 + 1024/8 = 128

3. **A router által továbbküldött csomagok információi (2. szó):**

00000000 10110010 0 01 00000 00000000

Offset = 0

00000000 10110010 0 01 00000 01000000

Offset = 0 + 512/8 = 64

00000000 10110010 0 01 00000 10000000

Offset = 128

00000000 10110010 0 00 00000 11000000

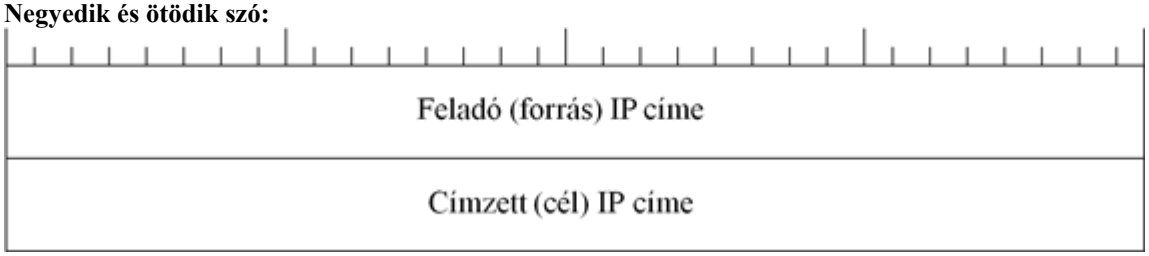
Offset = 128 + 512/8 = 192

Harmadik szó:

A harmadik szó adatai - általános információk:

- 8 bit: TTL a csomag „hátralevő életidejének” jelzése. Az útválasztónak kötelező legalább 1-et levonni a rajtuk áthaladó csomag TTL értékéből. Ha a TTL mező értéke nullára csökken, akkor a csomag "halottnak" tekintendő, s el kell dobni.
- 8 bit: Felsőbb (transzport) rétegbeli protokoll kódja – RFC 1700.
- 16 bit: A fejrész ellenőrző összege.

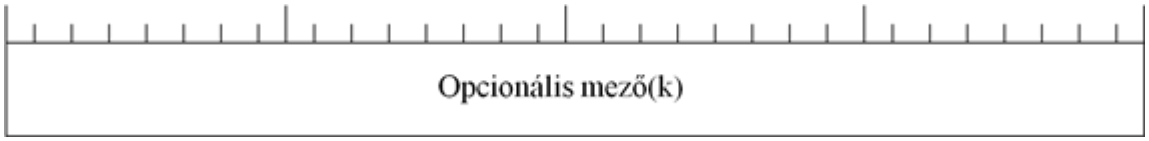
Negyedik és ötödik szó:



A negyedik és ötödik szó adatai - címzések:

- 32 bit: A „forrás” IP címe.
- 32 bit: A „cél” IP címe.

Hatodik szótól:



A hatodik szótól - 32 bites opcionális információk, pl.:

- Record route - A továbbítás útvonalának naplózása.
- Timestamp - A késleltetési idők naplózása.

2. IP címek

Az IP cím a csomópont interfészének hálózati rétegbeli azonosítója. A bájt értékeket ponttal elválasztva (ún. pontozott decimális megjelenítési formában) szoktuk felírni: pl. 157.45.190.57. Az azonosítók kezelését nemzetközi szervezet (IANA, InterNIC) látja el, a végfelhasználók internet szolgáltatóktól kaphatnak IP címet. Az intézmények nem egyedi címeket, hanem címtartományokat (hálózat azonosítókat) kapnak.

Az IP cím eleje a hálózat (vagy intézmény) azonosítója, a vége pedig a csomópont azonosítója a hálózaton belül. Az IP forgalomirányítás a hálózati azonosítókra épül (nem kell minden csomópont címét letárolnunk a forgalomirányítási táblában).

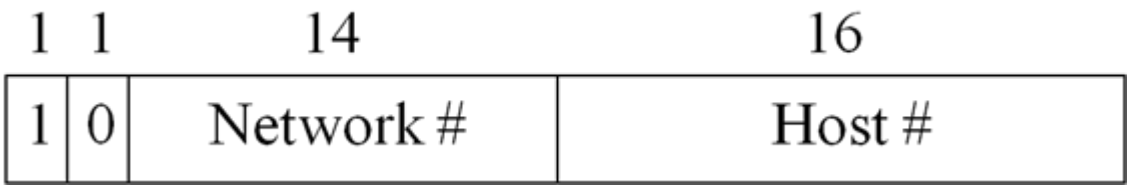
Hány bit hosszú legyen a hálózat azonosítója?

Ha túl kicsi, akkor a nagy tartományok kihasználatlanok.
Ha túl nagy, akkor csak kis alhálózatok kezelhetők.

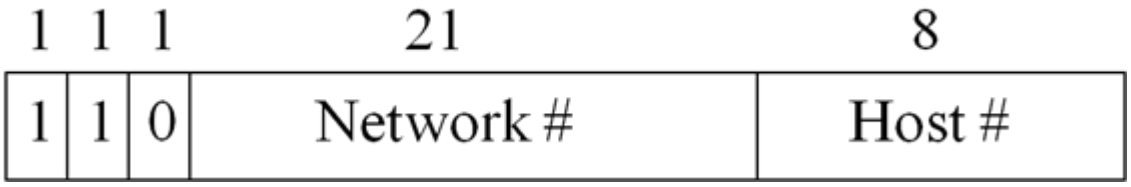
2.1. IP címosztályok

A osztály

B osztály



C osztály



A mezők feletti számok a bitek számát jelentik.

2.1.1. Első bájt szabály

Kezdőbit(ek)	1. bájt értéke	Osztály
0	0 - 127	A
10	128 - 191	B
110	192 - 223	C

2.2. Hálózati maszk

A hálózati maszk (netmask): Egy olyan 32 bites maszk, mely 1-es bit értékeket tartalmaz a hálózat és alhálózat azonosításában résztvevő bithelyeken, és 0-ás bit értékeket tartalmaz a csomópont azonosítására szolgáló bithelyeken.

A hálózati maszk segítségével az eredetileg az osztályba sorolás által (statikusan) meghatározott hálózat-gép határ módosítható.

Prefix hossz: A hálózati maszkban szereplő 1-es értékek darabszáma (a hálózat azonosító bithelyek darabszáma).

Az egyes osztályokhoz tartozó alapértelmezett hálózati maszkok:

- **A osztály:** Hálózati maszk: 255.0.0.0 Prefix hossz: 8
- **B osztály:** Hálózati maszk: 255.255.0.0 Prefix hossz: 16
- **C osztály:** Hálózati maszk: 255.255.255.0 Prefix hossz: 24

2.3. Speciális IP címek

A speciális IP címek nem általános csomópont azonosítási funkciót látnak el, hanem valamilyen (definíció alapján meghatározott) speciális funkciót látnak el.

Nem definiált IP cím (aktuális gép): 32 db "0" bitérték. A csomópont saját magára való hivatkozásként használhatja, ha nincs ennél alkalmasabb címe (pl. DHCP címkéréskor feladó IP címként szerepelhet).

Loopback IP cím (egy gépen belüli kommunikáció): A 127.0.0.0/8 címtartomány "loopback" célra használt. A loopback interfész egy speciális (valódi hardverhez nem kötődő) interfész, melynek célja, hogy egy csomóponton belül is lehessen szabályos IP kommunikációt folytatni. A csomag ebben az esetben nem hagyhatja el a csomópontot (nem jelenhet meg a tényleges hálózati vonalon/csatornán).

Hálózat azonosító IP cím: A hálózat azonosító IP cím csomópont azonosító bitpozícióiban mindenütt "0" érték szerepel (a hálózat azonosító bithelyeken pedig a hivatkozott hálózat azonosítója). Ezt a címet (tipikusan) nem rendeljük hozzá csomóponti interfészhez, hanem az egész hálózati egység hivatkozására használjuk. (Leggyakrabban a forgalomirányítási táblázatokban találkozunk ilyen címmel).

Aktuális hálózaton belüli üzenetszórás IP címe: 32 db "1" bitérték. Az aktuális üzenetszórási tartomány valamennyi csomópontja számára szóló üzenet célcímeként használható.

Irányított üzenetszórás IP címe (directed broadcast): Az irányított üzenetszórás esetén egy megadott azonosítójú hálózat valamennyi csomópontja számára küldünk csomagot. Az irányított üzenetszórási IP cím hálózat azonosító részében az elérni kívánt csomópontok közös hálózat azonosítója szerepel, a csomópont azonosító részben pedig mindenütt "1" bitérték.

16. fejezet - Internet Control Message Protocol

1. Az ICMP protokoll

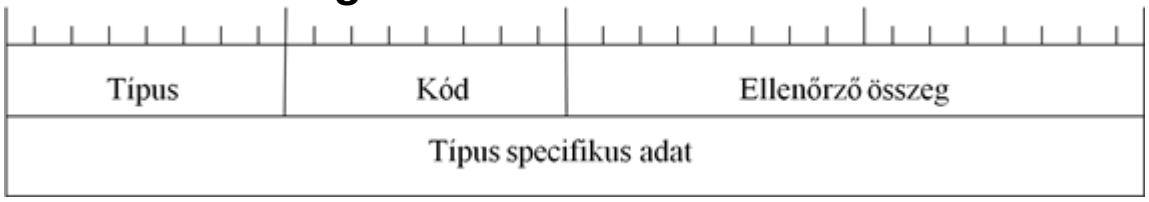
Az ICMP IP-re épülő (logikailag felsőbb szintű) protokoll, de funkciója miatt a hálózati réteghez soroljuk.

Az IP-vel együtt **kötelező** implementálni.

Célja: Az IP datagramok továbbítása során előforduló problémák (hibák) jelzése, jelzőüzenetek küldése.

Az IP csomagtovábbítás nem megbízható.
Az IP fejrész protokoll mezőjének értéke *1*.
A forrást informáljuk a bekövetkező problémákról.
ICMP üzenetek (továbbítási) hibáira nem generálunk ICMP üzenetet.

2. ICMP csomagszerkezet



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 címzési (és egyéb) információk az üzenettel kapcsolatosan

17. fejezet - IP forgalomirányítási alapok

1. Forgalomirányítási alapfogalmak

Forgalomirányítás (routing): Csomagok (IP datagramok) továbbítási irányának meghatározásával kapcsolatos döntések meghozatala.

Forgalomirányítási táblázat (routing table): A forgalomirányításhoz szükséges információkat tartalmazó táblázat. Tipikus (legfontosabb) mezők:

Célhálózat	Netmask	Kimenő int.	Következő csomópont (next hop)	Metrika

2. Hálózati protokollok forgalomirányítási felosztása

Forgalomirányított protokoll (routed protocol): Olyan hálózati réteghez kötődő általános adatszállító protokoll, amelyet a forgalomirányító (router) irányítani képes (pl. IP, IPX).

Forgalomirányítási protokoll (routing protocol): A forgalomirányítási táblázat(ok) felépítéséhez szükséges információk továbbítását (routerek közötti cseréjét) leíró protokoll (pl. RIP, OSPF, BGP).

Egyéb protokoll: Az előzőekhez nem sorolható hálózati protokoll (pl. ICMP).

3. Forgalomirányítók (alapvető) működése

1. A router az input interfészen érkező csomagot fogadja.
2. A router a csomag célcímét illeszti a routing táblázat soraira.

   Ha a célcím több sorra illeszkedik, akkor a leghosszabb prefixű sort tekintjük illeszkedőnek.
3. Ha nem létezik illeszkedő sor, akkor a cél elérhetetlen, a csomag nem továbbítható.

   A csomagot a router eldobja és ICMP hibajelzést küld a feladónak.
4. Ha létezik illeszkedő sor, akkor a csomagot az ebben szereplő kimeneti interfészen továbbítjuk (adatkapcsolati rétegbeli beágyazással) a következő hopként megadott szomszédhoz, ill. a célállomáshoz, ha már nincs több hop.

4. IP cím illesztés

1. A routing tábla sorait prefix hossz szerint csökkenő sorrendbe rendezzük. N=1.

   Ezzel biztosítjuk, hogy több illeszkedő sor esetén a leghosszabb prefixűt fogjuk 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 hajtunk 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; folytassuk a 2. pontnál.

18. fejezet - IP alhálózatok

1. IP alhálózatok

Az intézmények logikai működésük, vagy térbeli elhelyezkedésük alapján kisebb (azonos méretű) részekre oszthatják a hálózati címtartományukat. A felosztás eredményeként kisebb, könnyebben kezelhető üzenetszórási tartományokat tudunk kialakítani.

Alhálózatok kialakítása (subnetting): Az IP cím host részének legmagasabb helyiértékű bitjeiből néhányat az alhálózat (subnet) azonosítására használunk. Az új hálózat-csomópont azonosító határvonal pozícióját a hálózati maszk megadásával jelöljük.

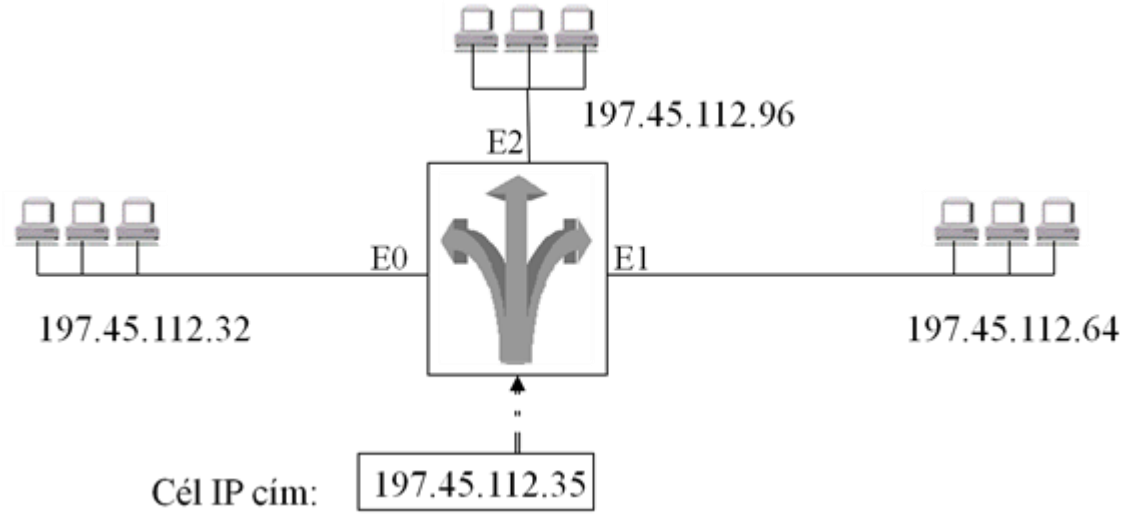
Alhálózat kialakítási példa:

- Hálózat IP címe: 197.45.112.0
- Alapértelmezett hálózati maszk: 255.255.255.0
- Használjunk 3 bitet alhálózat azonosításra.
- Hálózati maszk: 255.255.255.224
- Összesen 8 alhálózat kialakítására van lehetőség.

Az alhálózatok címei:

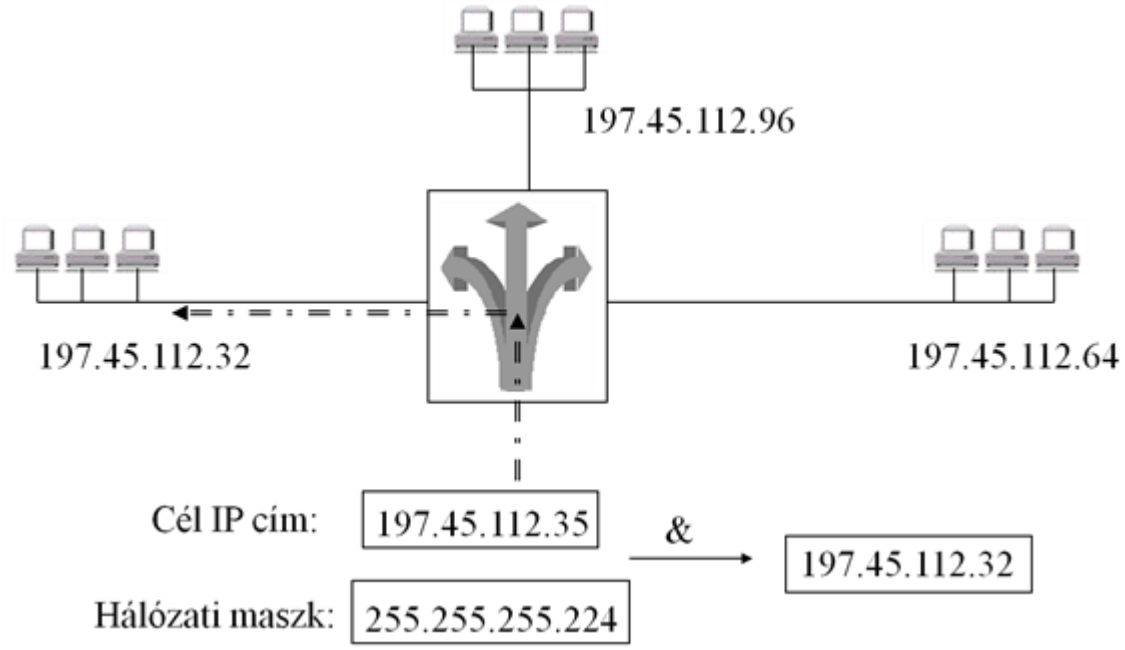
Sorszám	Alhálózat címe	Alhálózati gépcímek
1.	197.45.112.0	197.45.112.1-30
2.	197.45.112.32	197.45.112.33-62
3.	197.45.112.64	197.45.112.65-94
4.	197.45.112.96	197.45.112.97-126
5.	197.45.112.128	197.45.112.129-158
6.	197.45.112.160	197.45.112.161-190
7.	197.45.112.192	197.45.112.193-222
8.	197.45.112.224	197.45.112.225-254

2. Forgalomirányítás alhálózatok között



Forgalomirányítási tábla:

Cél	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



19. fejezet - IPv4 problémák – 1990

1. Az osztály alapú IP címkiosztási rendszer problémái

Irányítási tábla bejegyzéseinek száma:

1990. január	927
1990. április	1525
1990. július	1727
1990. október	2063
1991. január	2338
1991. április	2622
1991. július	3086
1991. október	3556
1992. január	4526

Osztályos IP-címek kiosztási helyzete 1992-ben (RFC 1466):

	Összes	Kiosztott	Kiosztott (%)
Class A	126	49	38 %
Class B	16383	7354	45 %
Class C	2097151	44014	2 %

Az 1990-es években tömegesen jelentek meg Internet csatlakozási igénnyel néhány ezer (~5000) csomóponttal rendelkező intézmények. Ezt a méretkategóriát az osztályos címrendszer nem tudja jól kezelni: a "B" osztály túl nagy, a "C" osztály túl kicsi.

A tömeges csatlakozás miatt a kiosztott hálózati azonosítók száma exponenciális növekedést mutatott. Az Internet gerinchálózati útválasztóinak irányító tábla mérete ebben az időben a kiosztott hálózati azonosítók számával volt arányos. Ha nem történik változtatás, akkor az irányítási táblák kezelhetetlen méretűre növekednek.

Ugyancsak a tömeges csatlakozás eredménye volt, hogy a "B" osztályú hálózatazonosítók a teljes kimerülést közelítették (1992: 45%).

2. CIDR - Az IP címosztály-problémák rövidtávú megoldási ötlete

A hálózat-gép határvonalat nem statikus módon (osztály alapon) helyezzük el, hanem az igényelt csomópont-darabszám alapján az igényeket lefedő legalkalmasabb pozícióra állítjuk. (Azaz, az osztályos határvonalat tetszőleges bitszámmal balra (supernetting), vagy jobbra (subnetting) tolhatjuk.) A határvonal pozíció jelzésére kötelező a prefix hossz, vagy a hálózati maszk megadása.

Az irányítási táblák növekedési problémáinak kezelésére területi elrendeződés szerinti címtartomány-zónákat alakítottak ki. Egy adott tományon kívül eső irányítási információkra elegendő összegző (aggregált) irányítási információkat letárolni. (A másik címzési zóna részletinformációit nem kell letárolnunk.)

2.1. Kontinensek IP címtartományai

A legnagyobb területű IP-címtartományokat kontinentális alapon osztották ki, s RFC-ben rögzítették (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

3. CIDR címkiosztási példa

Egy internetszolgáltató 2048 db „C” osztályú hálózatazonosító IP-cím kiosztásáról rendelkezik: 194.24.0.0 - 194.31.255.255

A szolgáltatót (kívülről) specifikáló információ: <194.24.0.0, 255.248.0.0>

A szolgáltatóhoz 3 intézménytől érkezik internet-csatlakozási igény:

A Intézmény: 2000 csomópont
B Intézmény: 4000 csomópont
C Intézmény: 1000 csomópont

A kiosztott címtartományok:

AI: 194.24.0.0 - 194.24.7.255; <194.24.0.0, 255.255.248.0> (2048 cím)
BI: 194.24.16.0 - 194.24.31.255; <194.24.16.0, 255.255.240.0> (4096 cím)
CI: 194.24.8.0 - 194.24.11.255; <194.24.8.0, 255.255.252.0> (1024 cím)

A példa működtetéséhez szükséges forgalomirányítási információk:

- Az európai (aggregált) forgalomirányításhoz:

  <194.24.0.0, 255.248.0.0>

  Egy bejegyzéssel 2048 db „C” osztályú cím kezelhető.

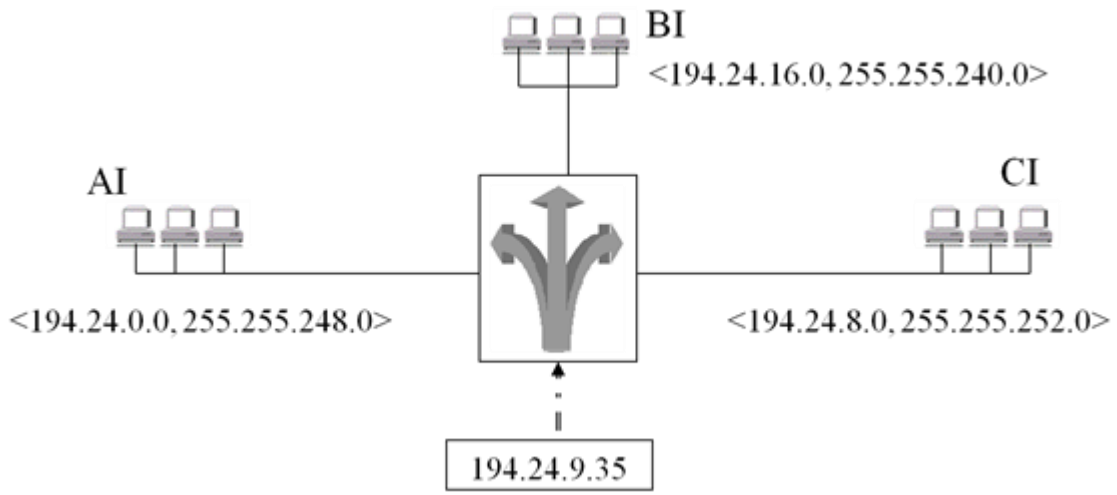
- Az internetszolgáltató belső forgalomirányításához:

  <194.24.0.0, 255.255.248.0>
  <194.24.16.0, 255.255.240.0>
  <194.24.8.0, 255.255.252.0>

  Három bejegyzéssel 28 db „C” osztályú cím kezelhető.

3.1. CIDR példa - routing

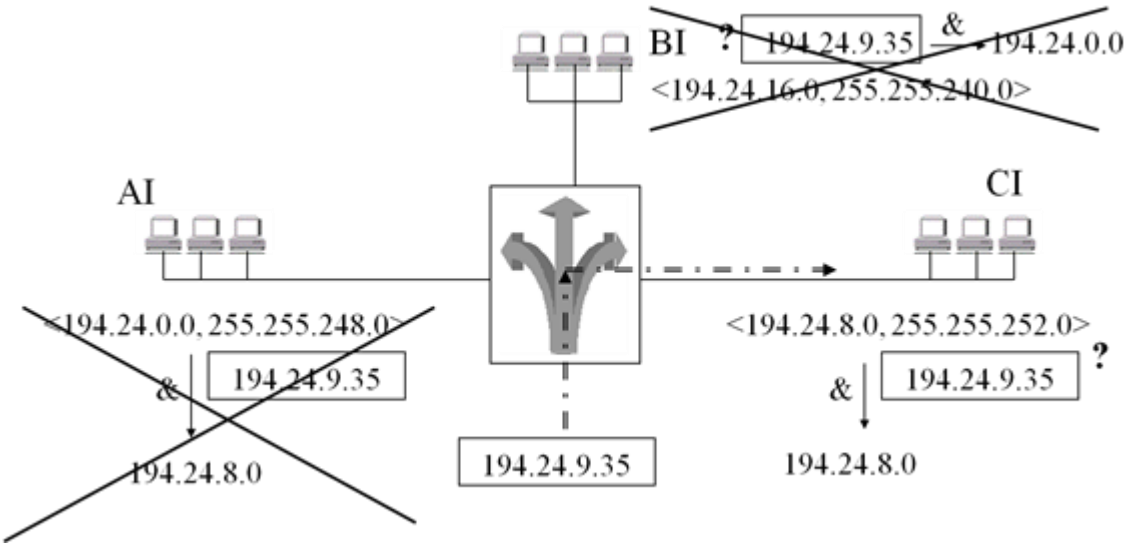
A szolgáltatóhoz az Internet felől érkezik egy csomag, melynek célcíme 194.24.9.35. Nézzük meg hogyan továbbítja a szolgáltató útválasztója a csomagot:



Az "A" intézmény vizsgálata: Bitenkénti ÉS művelet az "A" intézmény netmaszkja (255.255.248.0) és a célcím (194.24.9.35) között. A művelet eredménye 194.24.8.0, ami nem egyezik meg az "A" intézmény hálózatazonosítójával (194.24.0.0), így a csomag nem erre továbbítódik.

A "B" intézmény vizsgálata: Bitenkénti ÉS művelet a "B" intézmény netmaszkja (255.255.240.0) és a célcím (194.24.9.35) között. A művelet eredménye 194.24.0.0, ami nem egyezik meg a "B" intézmény hálózatazonosítójával (194.24.16.0), így a csomag nem erre továbbítódik.

A "C" intézmény vizsgálata: Bitenkénti ÉS művelet a "C" intézmény netmaszkja (255.255.252.0) és a célcím (194.24.9.35) között. A művelet eredménye 194.24.8.0, ami megyezik a "C" intézmény hálózatazonosítójával (194.24.8.0), így a csomag erre továbbítódik.



Megjegyzés: A tényleges forgalomirányítás során az útválasztó tábla prefixhossz szerint csökkenőbe rendezett, így a vizsgálat a "C" intézmény azonosítójával kezdődik.

20. fejezet - NAT – Network Address Translation (középtávú megoldás)

A csomópontok jelentős része „csak” kliensként vesz részt a hálózati kommunikációban. A címzési struktúra kialakítása során figyelembe vehetjük, hogy a kliensek elérhetőségét ("megszólíthatóságát") nem kell biztosítanunk, elegendő a kliensek számára a szolgáltatások elérhetőségét garantálni.

Applikációfüggő megvalósítás: Proxy, ALG. Ebben az esetben egy applikációs rétegbeli átjáró biztosítja az adott szolgáltatás (applikáció) elérhetőségét.
Applikációfüggetlen megvalósítás: Címfordítás (Címtranszláció, NAT, PAT). Ebben az esetben az intézmény határán egy speciális eszköz, a címfordító (NAT-Box) biztosítja, hogy (bizonyos korlátoktól eltekintve) valamennyi applikáció számára a szolgáltatások elérhetőek legyenek.

1. 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 (világméretű) hálózatra vonatkozóan egyediek.

Belső hálózat (Private/Local Network): Az intézmény saját (belső, privát) címzéssel rendelkező címzési övezete. A belső hálózatban használt címek a világon nem egyediek, mert másik intézményben működtetett belső hálózatban ismételten megjelenhetek. A belső hálózatban használható címtartományokat az RFC 1918 dokumentumban rögzítették:

10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

2. NAT – működési elv

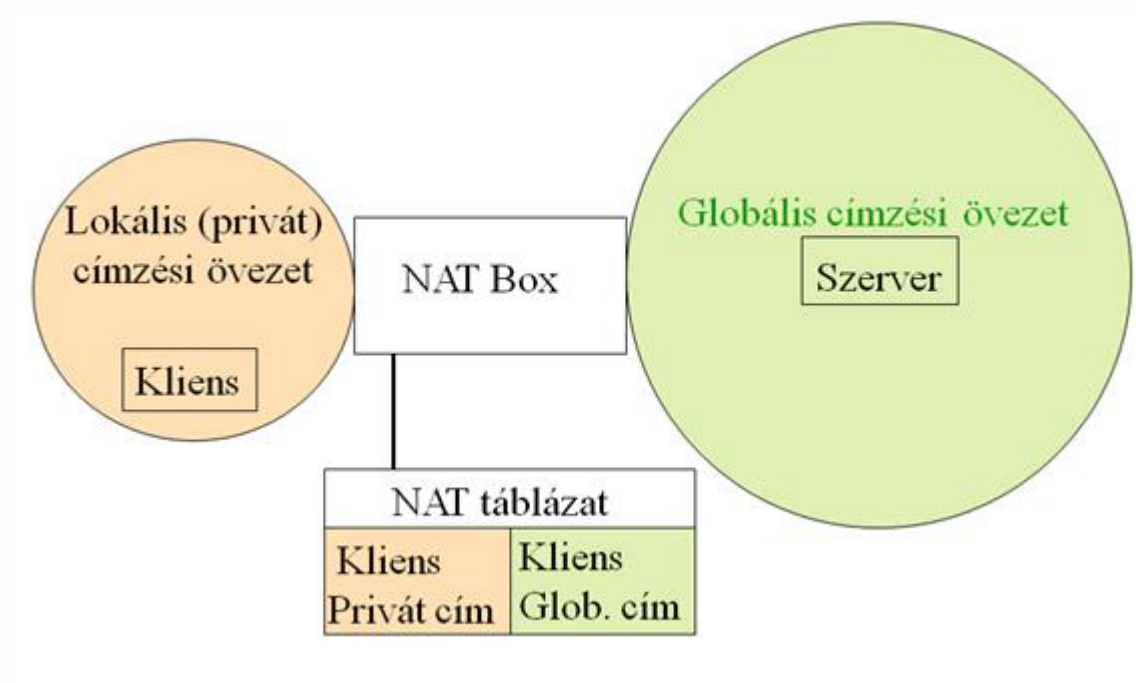
1. A klasszikus címfordítás (Basic NAT) esetében a kliens egy belső, a szolgáltatást nyújtó szerver pedig a külső, globális hálózatban helyezkedik el. Az első csomagot a kliens küldi a szerver felé, a csomagban célcímként a szerver globális címe, feladó címként pedig a kliens privát címe szerepel.

2. A csomag a belső hálózat forgalomirányítása alapján a két címzési övezet határához (a címfordítóhoz) jut. A NAT-Box a feladó és a célcím alapján látja, hogy a csomagot a külső hálózat felé kell továbbítani.

3. A csomagban feladócímként szereplő kliens privát címe nem továbbítható a külső hálózatba, mert ott elveszítené az egyediségét. A NAT-Box lecseréli a kliens privát címét egy külső (publikus) címre, s ezzel a feladócímmel indítja a csomagot külső hálózatban a szerver felé. A Nat-Box egy táblázatban (címfordító, vagy címtranszlációs tábla) feljegyzi a címcserét.

4. A szervertől érkező válaszüzenet a címfordítóhoz érkezik, s a Nat-Box a válaszüzenetben szerplő célcím alapján felismeri, hogy címtranszlációra van szükség.

5. A Nat-Box a táblázata alapján lecseréli a válaszüzenetben szereplő globális címet a kliens privát címére, s az így előállított csomagot továbbítja a belső hálózaton a kliens felé.



A klasszikus nat (Basic NAT) esetében a "cím" fogalom az IP címre vonatkozik. A címtranszláció valójában egy kommunikációs viszonyhoz tartozó azonosító funkcionalitást igényel a "cím"-től, így a cím fogalom általánosításával, újra értelmezésével egy új NAT működés (portszám transzláció, NAPT, PAT) definiálható: A kommunikációs viszony azonosítóját az IP cím és a portszám együttesen alkotja (48 bites azonosító); a felírt NAT működési váz ezzel a címfogalommal változatlan módon működtethető. Ezzel a megoldással egy globális cím felhasználásával több privát gép kommunikációja is megoldható különböző kliens oldali portszámok alkalmazásával.

3. A NAT erőforrásigénye

A NAT megoldások általában erőforrásigényesek (elsősorban processzor oldalon):

- Keresés a címtranszformációs táblázatban
- Címcsere (portszámcsere)
- Ellenőrző összegek újraszámítása

  Nem fontos a teljes PDU-ra elvégezni a számítást:

  Az eredeti ellenőrző összegből „kivonjuk” a régi címeket.
  A kapott eredményhez az új címeket „hozzáadjuk”.

21. fejezet - A kettős címrendszer problémái

A "kettős címrendszer problémája" alatt az adatkapcsolati (Ethernet) és a hálózati (IP) címrendszer együttműködési problémáit értjük: Egyrészt az adó oldalon a továbbítandó IP csomagban szereplő cél IP címhez meg kell határoznunk a hozzá tartozó Ethernet címet, acélból, hogy az adatkapcsolati réteg enkapszulációt el tudjuk végezni. Másrészt felmerült az igény, hogy ne kelljen a csomópontokon külön-külön IP címbeállítást végezni, hanem legyen lehetőség arra, hogy a csomópont (az Ethernet címe alapján) a hálózatról (egy központi helyen tárolt adatbázisból) kaphasson IP címet.

1. Hálózati címből fizikai cím meghatározása (ARP)

ARP (Address Resolution Protocol), RFC 826:

A cél IP cím alapján keressük a hozzátartozó Ethernet címet. Minden csomópont egy táblázatban (ARP táblázat) tartja nyilván a hálózati címekhez tartozó fizikai címeket. A táblázat új bejegyzéseit emberi beavatkozás nélkül kell létrehozni:

1. ARP kérdés: Ki tudja az X hálózati cím fizikai címét?

2. A kérdés keretét üzenetszórásos küldéssel az alhálózat valamennyi csomópontja megkapja és feldolgozza.

3. Ha valamely csomópont “magára ismer“ az X hálózati címben, akkor a saját fizikai címével megválaszolja az ARP kérdést.

1.1. ARP keret szerkezete

1-2. szó: Általános ARP fej
3-6. szó: IPv4/Ethernet specifikus adatrész.
Az Ethernet-keret típus értéke: 0x0806

2. Fizikai címből hálózati cím meghatározása (RARP)

RARP (Reverse Address Resolution Protocol), RFC 903:

A RARP protokoll alkalmazása speciális esetekben szükséges (tipikusan hálózati boot, vagy hálózatról történő IP cím meghatározása esetén.) Egy (vagy több) RARP szerver egy táblázatban (RARP táblázatban) tartja nyilván a fizikai címekhez tartozó hálózati címeket. A táblázatot a rendszeradminisztrátor tartja karban. Az IP cím - Ethernet cím összerendelés statikus (azaz egy Ethernet címhez mindaddig ugyanaz az IP cím lesz hozzárendelve, amíg a rendszeradminisztrátor meg nem változtatja azt). Ha több RARP szervert üzemeltetünk, akkor mindegyiken ugyanazt az összerendelési táblázatot kell alkalmaznunk.

Működési vázlata:

1. RARP kérdés: Ki tudja az X fizikai cím hálózati címét?

2. A kérdés keretét üzenetszórásos küldéssel az alhálózat valamennyi csomópontja megkapja.

3. A RARP szerverek feldolgozzák a kérdést: Ha megtalálják a táblázatukban az X fizikai címet, akkor a táblázatban található hálózati címmel megválaszolják a RARP kérdést.

BOOTP (BOOTstrap Protocol), RFC 951:

A RARP csak egy üzenetszórási tartományon belül működik, minden üzenetszórási tartományban RARP szervert kell üzemeltetni. A BOOTP egy IP/UDP csomagformátumot alkalmazó protokoll, ahol az IP címet igénylő kliens és a kérését kiszolgáló szerver külön üzenetszórási tartományban is lehet. A folyamat működési váza lényegét tekintve azonos a RARP folyamat vázával.

Ha a kliens és a szerver különböző üzenetszórási tartományban van, akkor a kliens üzenetszórási tartományábn egy BOOTP ügynökre (BOOTP Relay Agent) van szükség. A BOOTP ügynök feladata, hogy a kliens kérését továbbítsa a szerverhez, ill. a szervertől jövő válaszokat továbbítsa a klienshez. Címösszerendelési táblázat nincs az ügynököknél.

A BOOTP ügynök feladata nem túl bonyolult, hiszen a kliens által üzenetszórással küldött keretben egy szabályos IP csomag szerepel; a BOOTP ügynöknek csak az IP csomag feladó és célcímét kell lecserélnie a saját ill. a BOOTP szerver IP címére, s a csomag már továbbítható is a másik üzenetszórási tartományban lévő szerver felé.

Dinamikus IP címmeghatározás (Dynamic Host Configuration Protocol, DHCP), RFC 1531:

A DHCP egy IP címtartomány dinamikus kiosztását teszi lehetővé az igénylők között. A "dinamikus kiosztás" azt jelenti, hogy egy bizonyos kliens nem biztos, hogy mindig ugyanazt a címet kapja. Statikus (BOOTP-vel kompatibilis) kiosztásra is alkalmas, de ennek nagyon nehézkes és munkaigényes adminisztrációja miatt előszeretettel alkalmazzák a dinamikus (véletlenszerű) címkiosztást. A kliensek a DHCP esetén egy (megújítható) időszakra kapják az IP címet. Ha az időszak lejár (s nem sikerül a megújítás) a kliensnek kötelezően el kell engednie az IP címet (azaz, az ezzel az IP címmel folytatott kommunikációs viszonyai megszakadnak).

A folyamat működési váza módosult a BOOTP-hez képest, bár nagyon sok ötletet "örökölt" onnan (pl. Relay Agent, IP/UDP csomagszerkezet).

A DHCP működési vázlata:

1. DHCP kérdés: Ki tud adni egy IP címet? (DHCPDISCOVER)

2. A kérdés keretét üzenetszórásos küldéssel az alhálózat valamennyi csomópontja megkapja.

3. A 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)

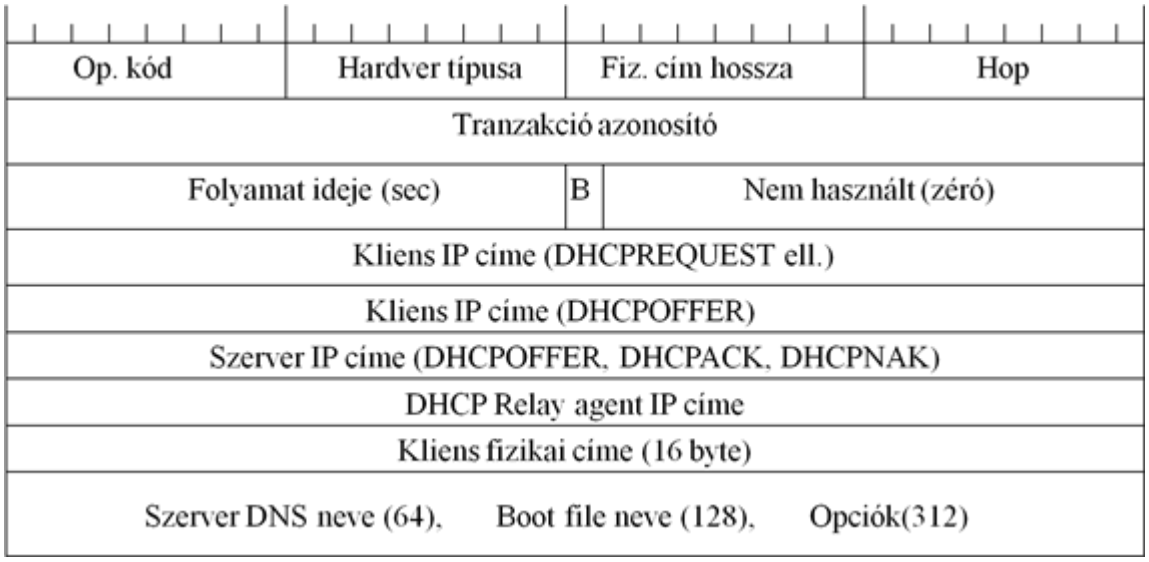
5. A DHCP szerver „könyveli” a címválasztást (foglalt lett a cím), s a könyvelésről megerősítést küld a kliensnek. (DHCPACK/DHCPNAK)

DHCPDECLINE: A szervertől kapott IP cím érvénytelen (használt).

DHCPRELEASE: A kliensnek nincs tovább szüksége az IP címre.

2.1. DHCP fejrész szerkezete

Szemléltetési célból (külön elemzés nélkül) mellékeljük a DHCP fejrész vázlatát:



V. rész - IP forgalomirányítás

Tartalom

22. fejezet - Forgalomirányítási alapismeretek

1. Forgalomirányítási alapfogalmak

Forgalomirányítás (útválasztás, útvonal választás; routing): Csomagok (IP datagramok) továbbítási irányának meghatározásával kapcsolatos döntések meghozatala.

Forgalomirányítási táblázat (routing table): A forgalomirányításhoz szükséges információkat tartalmazó táblázat. Tipikus (legfontosabb) mezők:

Célhálózat	Hálózati maszk	Kimenő interfész	Következő csomópont (next hop)	Metrika

Forgalomirányított protokoll (routed protocol): Olyan hálózati réteghez kötődő általános adatszállító protokoll, amelyet a forgalomirányító (router) irányítani képes (pl. IP, IPX).

Forgalomirányítási protokoll (routing protocol): A forgalomirányítási táblázat(ok) felépítéséhez szükséges információk továbbítását (routerek közötti cseréjét) leíró protokoll (pl. RIP, OSPF, BGP).

Autonóm rendszer (AS): Hálózatok forgalomirányítási adminisztrációs egysége, amelyben egy közös forgalomirányítási stratégia (routing protocol) érvényesül.

Metrika: Egy adott forgalomirányítás eredményeként előálló útvonal minőségének mérési módja, alapvetően két (egymásba transzformálható) kategóriában vizsgálható:

- Távolságalapú (költségalapú) metrika.
- Jóság alapú metrika.

2. Az útválasztás alapvető működése

1. Az útválasztó a bemeneti interfészen érkező csomagot fogadja.
2. A routing tábla sorait prefix hossz szerint csökkenő sorrendbe rendezzük. N=1.

   Ezzel biztosítjuk, hogy több illeszkedő sor esetén a leghosszabb prefixűt fogjuk eredményként kapni.
3. Ha nem létezik a táblázatban az N. sor, akkor a cél elérhetetlen, a csomag nem továbbítható.

   A csomagot a router eldobja és esetlegesen ICMP hibajelzést küld a feladónak. A folyamat befejeződik.
4. A csomag célcíme és az N. sor hálózati maszkja között bitenkénti AND műveletet hajtunk végre.
5. Ha a bitenkénti AND művelet eredménye megegyezik az N. sor célhálózat értékével, akkor a cím az N. sorra illeszkedik; ebben az esetben az N. sorban szereplő kimenő interfészen küldjük tovább a csomagot, s a folyamat befejeződik.
6. N=N+1, és folytassuk a 3. pontnál.

3. Forgalomirányítási konfigurációk osztályozása

Minimális routing: Teljesen izolált (router nélküli) hálózati konfiguráció. Forgalomirányítási döntés nem csak a forgalomirányítókon történik, hanem minden csomóponton a csomag küldése előtt.

Statikus routing: A forgalomirányítási táblázatot a rendszeradminisztrátor tartja karban. Tipikus példa a végfelhasználói csomópontokon az alapértelmezett útválasztó (default router, vagy más néven default gateway) beállítása.

Dinamikus routing: A forgalomirányítási táblázat(ok) valamilyen routing protocol segítségével kerülnek karbantartásra.

- **Belső forgalomirányítási protokollok (IGP, például RIP, OSPF).** Egy autonóm rendszeren belül működik, legfőbb alapelv a „legjobb útvonal” meghatározása ún. távolságvektor alapú vagy kapcsolat-állapot (link-állapot) alapú módszerrel
- **Külső forgalomirányítási protokollok (EGP, például EGP, BGP).** Nem feltétlenül a legjobb útvonal meghatározása a cél (politika alapú forgalomirányítás - BGP)

23. fejezet - Távolságvektor alapú forgalomirányítás (Distance Vector Routing)

Működési alapelv:

- A routerek minden elérhető célra (gép vagy hálózat) nyilvántartják, hogy a legjobb úton milyen irányban milyen távolsággal érhető el az adott cél (távolságvektor).
- A szomszédos forgalomirányítók ezen információkat meghatározott időközönként kicserélik egymással.
- Az új információk birtokában a routerek ellenőrzik, hogy szükséges-e változás valamelyik eddig ismert legjobb úttal kapcsolatban. (Található-e az eddig ismertnél jobb útvonal?)

1. Távolságvektor alapú forgalomirányítás - matematikai háttér

Definíció: *d(i, j)* jelölje az *i* és *j* entitások közvetlen elérési költségét (közvetlen távolságát):

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

Definíció: *D(i, j)* jelölje az *i* és *j* entitások legrövidebb úton történő elérésének távolságát:

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

A minimumot elegendő a szomszédos *k* entitásokra számítani.
D(i, j) számítási formulájának helyessége indukcióval bizonyítható.

Routing tábla felépítés (Bellman-Ford algoritmus).

Kiindulási helyzet:

Minden *i* entitás ismeri a *d(i, k)* távolságot minden *k* szomszédjára vonatkozóan.

Legyen továbbá

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

Működési algoritmus (tetszőleges $i \rightarrow j$ ($i \neq j$) útra vonatkoztatva):

1. Az *i* entitás minden *k* szomszédjától megkapja a *D(k, j)* értéket.
2. A *k* szomszédtól érkezett *D(k, j)* értéket felhasználva az *i* entitás kiszámítja a $X_{i,k,j} = d(i,k) + D(k, j)$ értéket.
3. Ha a kapott $X_{i,k,j}$ érték kisebb, mint az eddig ismert *D(i, j)*, akkor a *j* entitás *i*-ből aktuálisan az új minimumot szolgáltató *k* szomszédon keresztül lesz elérhető, a már kiszámított $X_{i,k,j}$ értéket használva *D(i, j)* metrika értékként.

4. Egy meghatározott ciklusidő eltelte után folytassuk az 1. lépésnél.

Bellmann és Ford bebizonyította, hogy az eljárás véges sok lépés után az optimális utat szolgáltatja (ezért szokás ezt a módszert Bellman-Ford algoritmusnak is nevezni).

2. Távolságvektor alapú forgalomirányítás - routing tábla problémák

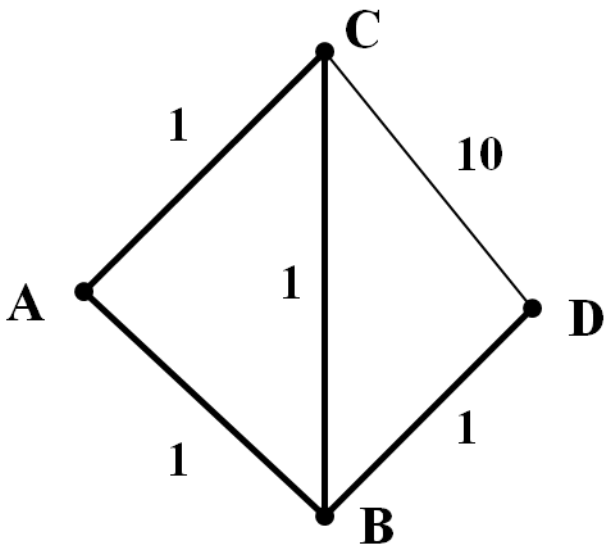
Túl kicsi kezdőérték probléma: Ha az optimális út „megsérül” nagyobb költségű (hosszabb) út nem léphet helyébe.

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

Végtelenig számlálás (counting to infinity) probléma: Az eljárás bizonyos esetekben igen lassan reagál a topológia változására.

Végtelenig számlálás példa:

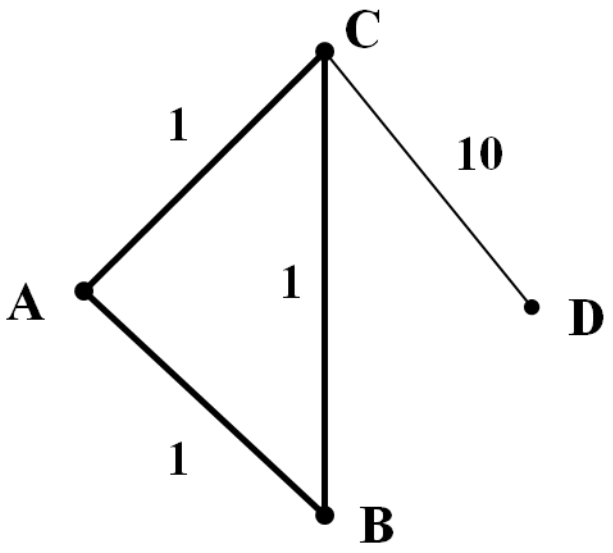
Tekintsük a D-be irányuló forgalomirányítást a következő hálózati környezetben:



Kiinduló forgalomirányítási táblázat bejegyzések a "D" célra vonatkozóan (Az optimális út irányában a "D" felé vezető szomszédot, s azon keresztül "D" optimális távolságát jegyezzük fel):

A: B szomszédon keresztül 2 távolságra.
B: D szomszédon keresztül 1 távolságra.
C: B szomszédon keresztül 2 távolságra.

Tekintsük a routing táblák alakulását a B-D kapcsolat megsérülése esetén:



A	B, 2	C, 3	C, 4	C, 5	...	C, 10	C, 11	C, 11
B	---	C, 3	C, 4	C, 5	...	C, 10	C, 11	C, 11
C	B, 2	A, 3	A, 4	A, 5	...	A, 10	D, 10	D, 10

A példa jól mutatja, hogy egy ilyen egyszerű hálózati környezetben is a meghibásodás bekövetkezte után 9 ciklus kellett a forgalomirányítás helyreállásához.

3. Routing Information Protocol (RFC 1058)

A Routing Information Protocol (RIP) legfontosabb jellemzői:

- Távolságvektor alapú IGP protokoll.
- Régi, de folyamatosan fejlesztik, javítják.
- Metrika: érintett útválasztók (hop-ok) száma (azaz minden kapcsolat költsége 1).
- Max. 15 router hosszúságú optimális útvonalak esetén használható (16 = végtelen távolság).
- 30 másodpercenkénti routing információ küldés.
- A szomszédos útválasztó elérhetetlenségét hat hirdetési cikluson (180 sec.) keresztül történő "csendben maradása" jelzi.
- „Triggered update” a végtelenig számlálás idejének csökkentésére: Változás esetén nem várjuk ki a ciklusidőt, hanem azonnal továbbküldjük a változás információját (A változás "update"-et "triggerel"). (Speciális "flag"-ek és időzítési információk nyilvántartása szükséges)
- RIPv2 (RFC 1723): CIDR kompatibilis, a szomszédok közötti kommunikációra authentikáció előírható.

4. Enhanced Interior Gateway Routing Protocol (EIGRP)

Legfontosabb jellemzők:

- Gyártóspecifikus (Cisco) távolságvektor alapú routing protokoll.

- Szomszédsági viszonyok kiépítése és fenntartása ("update" csak tényleges változás esetén történik, nem ez képezi a szomszéd elérhetőségének a vizsgálatát).
- Sokcélú, flexibilis, skálázható.
- Metrika: összetett (öt változóból számított, súlyozható; alaphelyzetben a "bandwidth"-re és a "delay"-re épül):

  bandwidth
  delay
  load
  reliability
  MTU

- CIDR kompatibilis, authentikáció előírható.
- Számos javítás alkalmazása a végtelenig számlálás kezelésére:

  Triggered update, Split horizon (nem küldjük vissza az információt oda, ahonnan tanultuk), holddown timer (a legjobb út keresése előtt várakozunk egy kicsit, hogy minden útválasztó értesüljön a módosult helyzetről) Potenciális helyettesítő útvonalak nyilvántartása

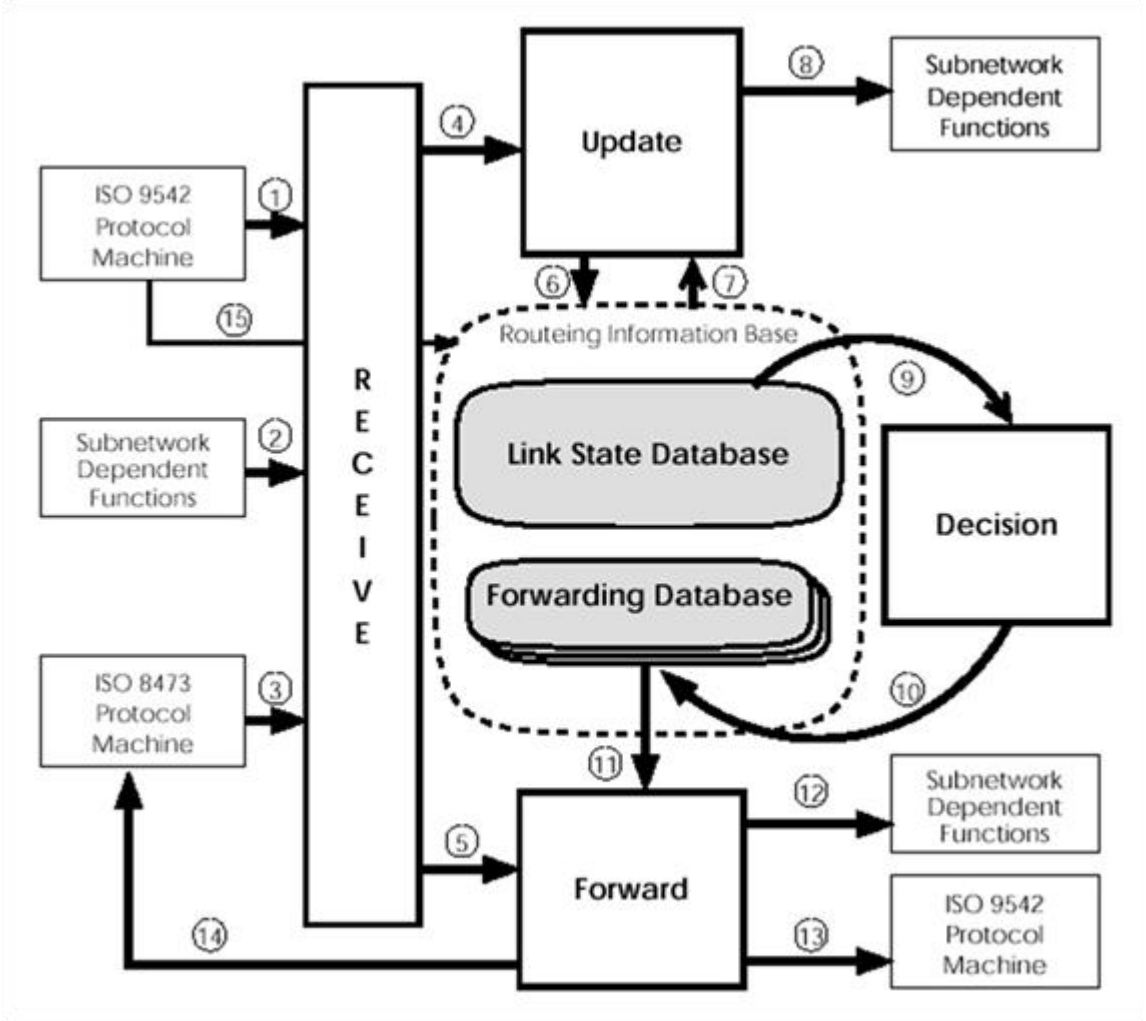
- Update: Csak a tényleges változási információkat küldi (nem a teljes táblázatot).
- Integrált routing (több irányított protokollra alkalmazható).

24. fejezet - Kapcsolat-állapot (link-állapot) alapú forgalomirányítás (Link State Routing)

A kapcsolat-állapot alapú útválasztás működési vázlata:

1. Szomszédok felfedezése.
2. A szomszédok felé vezető kapcsolat (link) költségének mérése.
3. Csomagkészítés a mérési eredményekről.
4. A készített csomag küldése a hálózati forgalomirányítási egység összes útválasztójának.
5. Minden router ismeri a teljes hálózati topológiát, s ki tudja számítani (pl. Dijkstra algoritmussal) a többi routerhez vezető optimális utat (feszítőfa, spanning tree számítás).

LSR folyamatok (IS-IS protokoll specifikációból):



1. A legrövidebb út számítása (Dijkstra algoritmus)

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

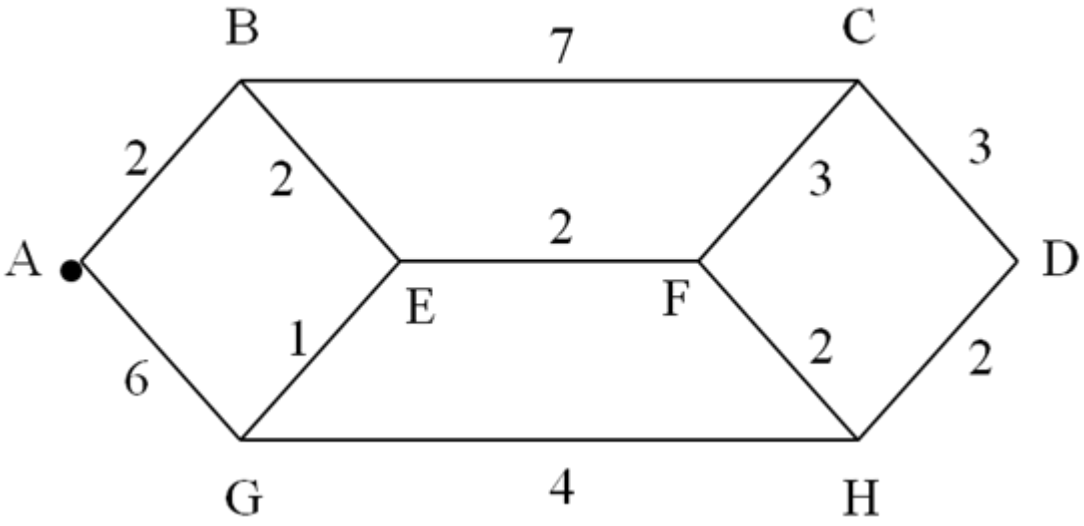
```
#define MAXNODES 1024                               /* maximum number of nodes */
#define INFINITY 1000000000                         /* larger than every maximum path
*/

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 {                                  /* the path being worked on */
        int predecessor;                            /* previous node */
        int length;                                 /* length from source to this node
*/
        enum {permanent, tentative} label;          /* label state: permanent,
tentative */
    } state[MAXNODES];

    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 */

    do {                                            /* Is there a better path from k?
*/
        for (i = 0; i < n; i++)                     /* this graph has n nodes */
            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 */
```

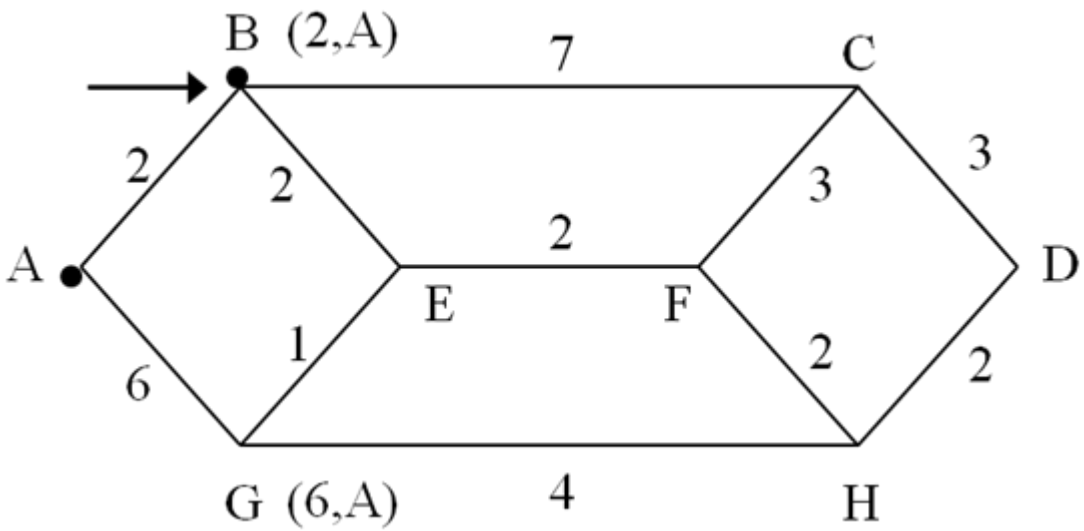
Példa a Dijkstra algoritmusra:

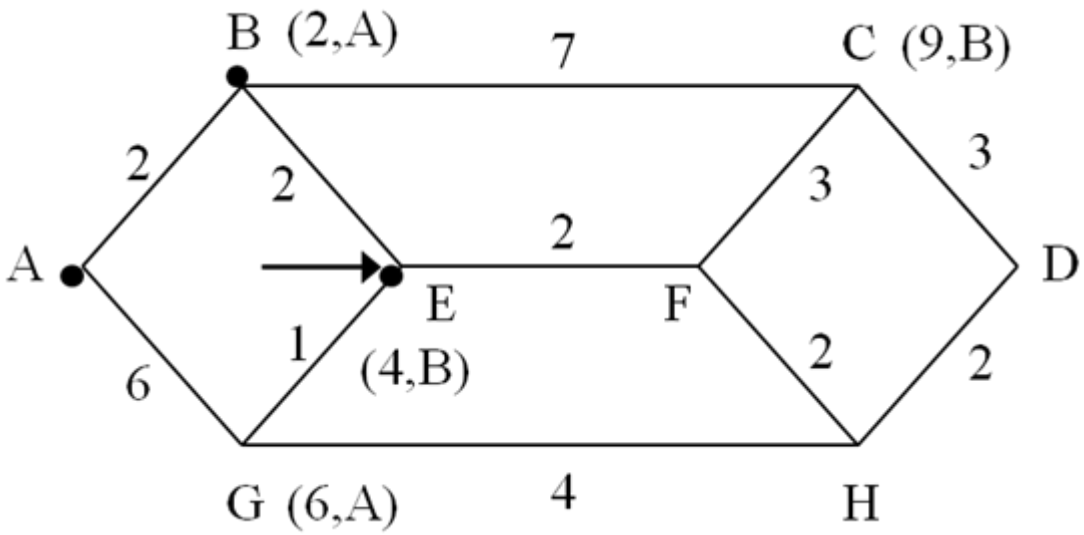
Az "A"-ból a "D"-be vezető optimális utat keressük. A gáfcsúcspontokhoz feljegyezzük, hogy "A"-ból mely szomszédján keresztül, s milyen költséggel érhető el ("A"-t tekintjük a fa gyökerének). Ahol nem szerepel jelzés, az azt jelenti, hogy még nem találtunk oda vezető utat (elérhetetlennek tekintjük a gráfcsúcspontot). A ponttal jelzett gráfcsúcspont az adott gráfcsúcspont "lezárt" állapotát jelzi. Ez azt jelenti, hogy a gráfcsúcspontba

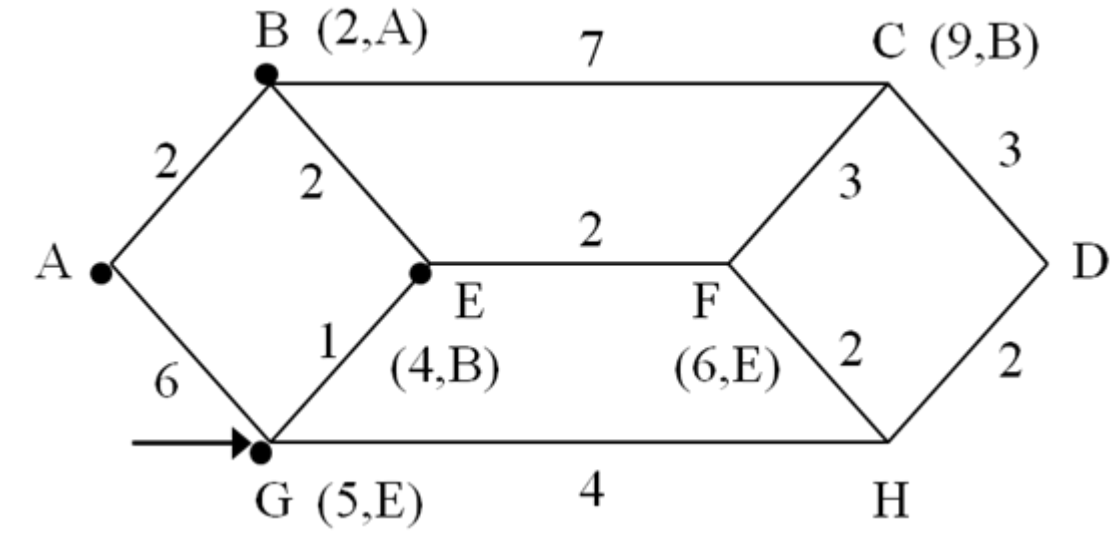
vezető legjobb utat már megtaláltuk, s megvizsgáltuk, hogy az adott gráfcsúcspontból merre lehet továbblépni optimális úton haladva.

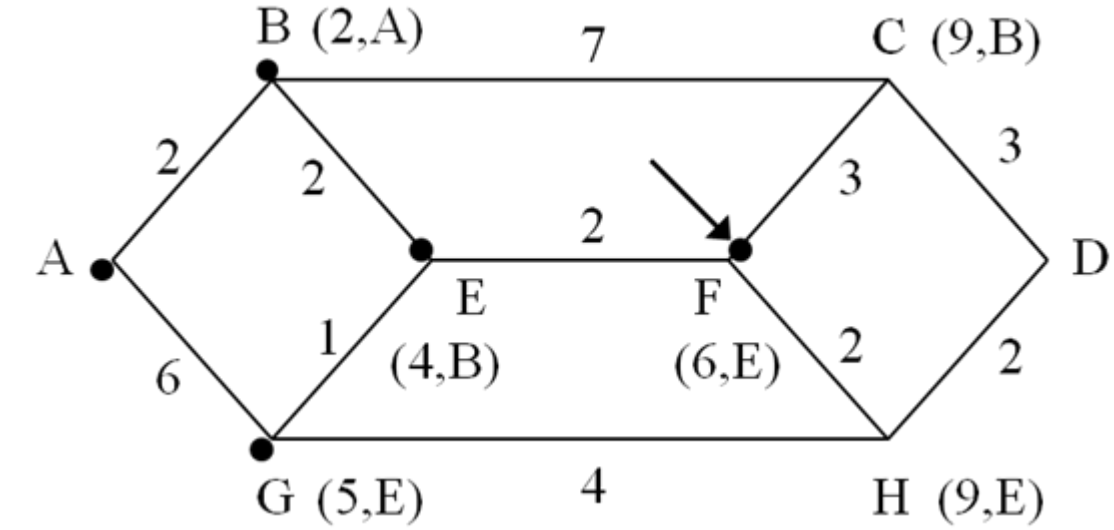
A nyíllal jelölt gráfcsúcspont az ún. "aktuális" pont, erre vonatkozóan vizsgáljuk, hogy milyen (nem zárt) továbblépési lehetőségek vannak innen. Kiinduló helyzetben az "A" gráfcsúcspont az aktuális pont.

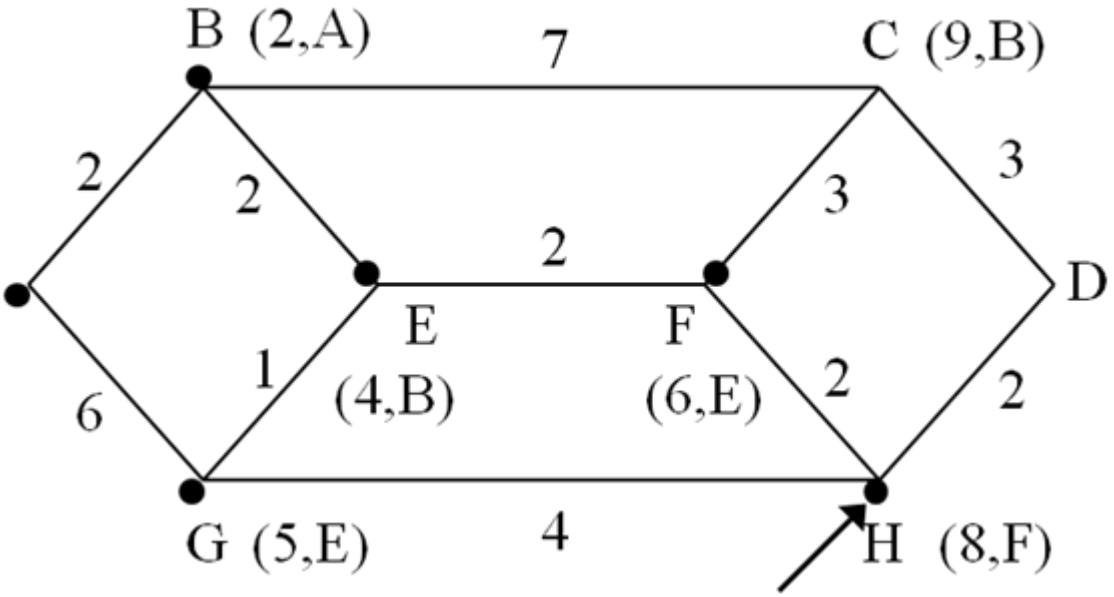


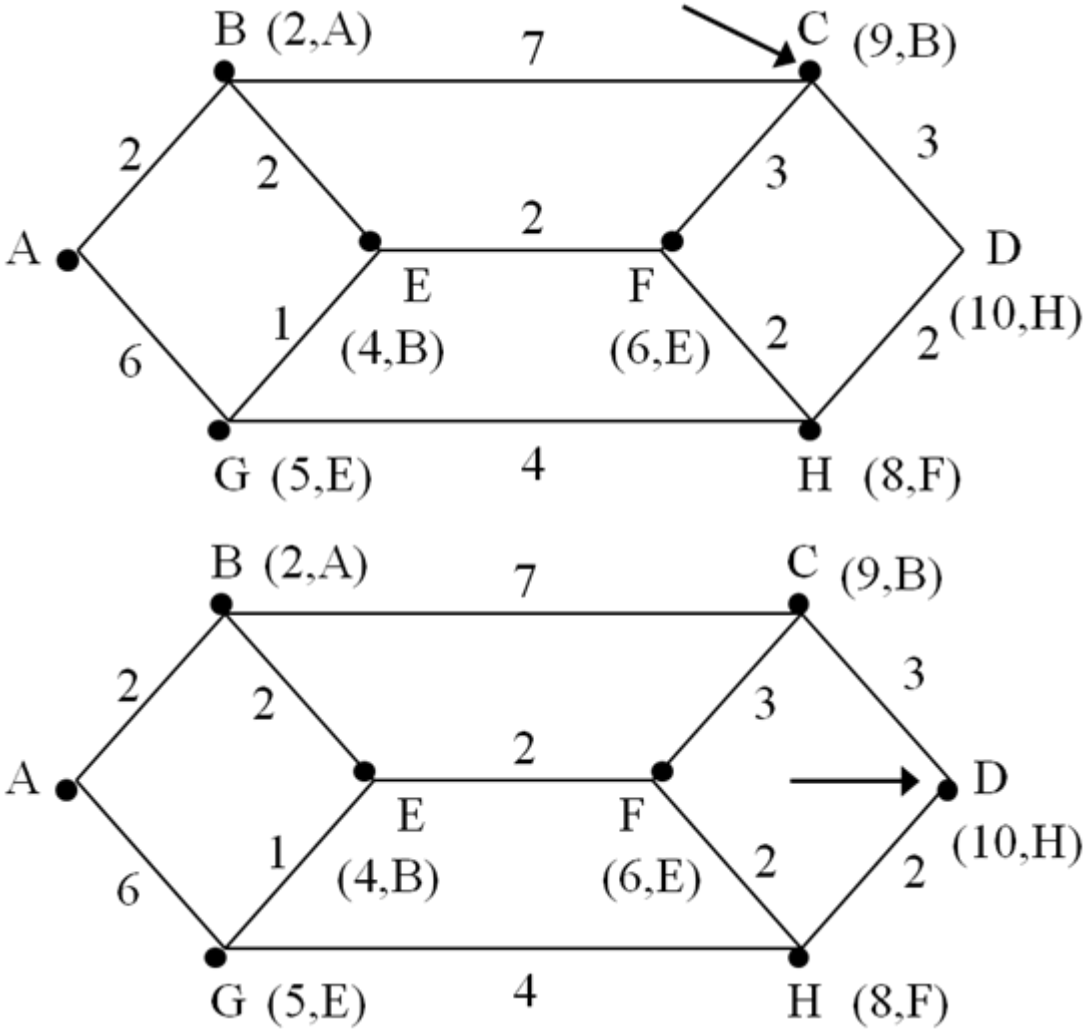












2. Open Shortest Path First (RFC 1131)

Az Open Shortest Path First (OSPF) legfontosabb jellemzői:

- Link-állapot alapú IGP protokoll
- Új, a 90'-es évektől alapértelmezettként javasolt
- AS-nél kisebb hálózati egység: terület (area) használata
- Forgalomirányítók (nem diszjunkt) osztályozása:

  - Területen belül működő forgalomirányítók
  - Területek határán álló forgalomirányítók
  - Gerinchálózaton (backbone) üzemelő forgalomirányítók
  - AS határon működő forgalomirányítók

- Egyenlő költségű többutas irányítás lehetősége
- Mai verzió: OSPF V2 (RFC 1583)

2.1. OSPF Specialitások (hatékonyságnövelő ötletek)

OSPF területek:

A döntési folyamat (Dijkstra algoritmus) alapja a terület (area). A területek „csillag alakzatot” formáznak, középpontjában a területeket összekötő speciális területtel (backbone, azonosítója a 0).

A területek egy terület-határ útválasztó (Area Border Router) segítségével kapcsolódnak a backbone-hoz. A területhatár router-ek feladata összetett:

- Minden területhez külön döntési folyamatot (Dijkstra algoritmust) futtatnak.
- A terület(ek)ből tanult információkat összegzik, s a másik terület(ek)be injektálják.
- A területek "belső térképe" más terület felé nem kerül átvitelre.

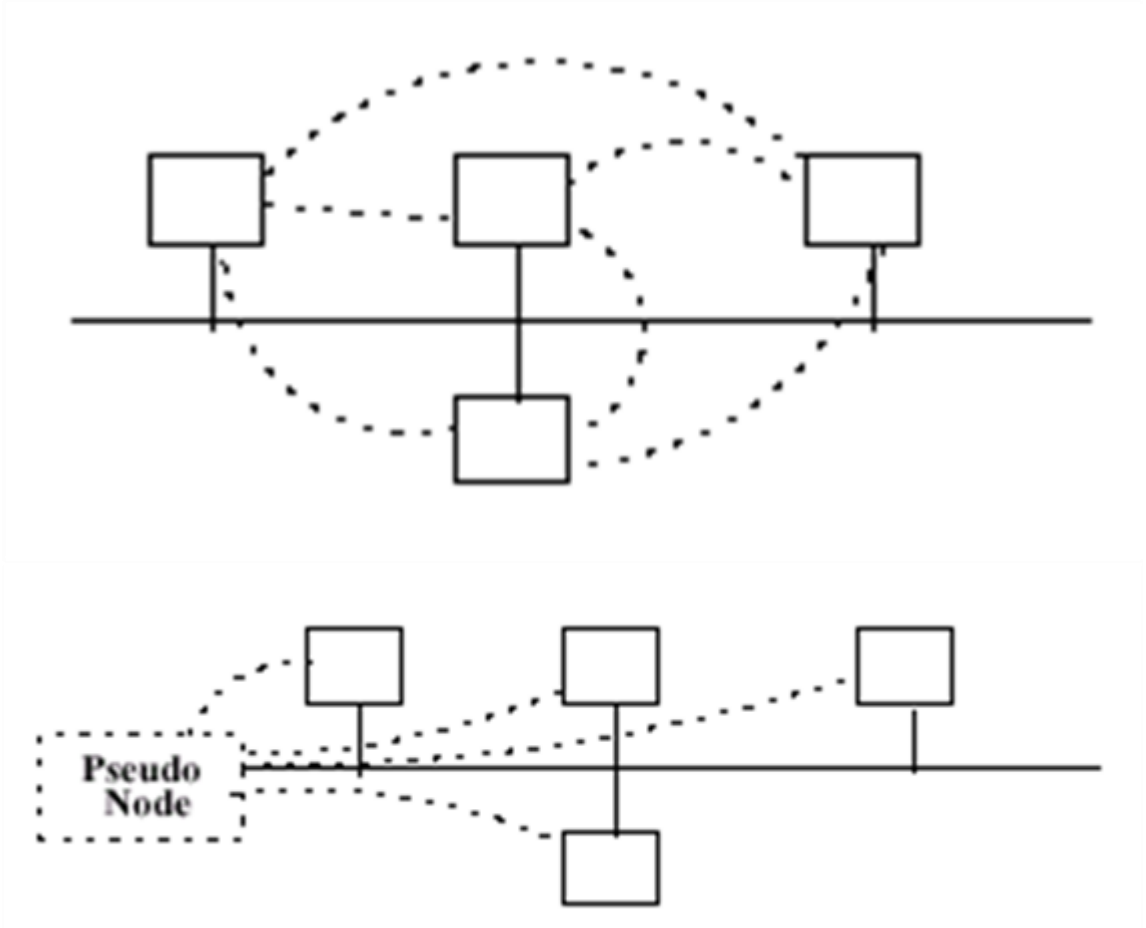
Területek közötti forgalomirányítás (inter-area routing) működése:

- Útválasztás a forrásterületen belül egy területhatár irányítóig.
- Útválasztás a backbone-on a célterület egy határ útválasztójához.
- Útválasztás a célterületen belül a célhálózatig.

A területekre való bontással az OSPF jól skálázható protokollá válik: a területhatár funkciók helyes kijelölésével hatékonyan működő rendszerek építhetők ki (a kisebb erőforrású eszközök kisebb, a nagobb erőforrású eszközök nagyobb feladatokat kaphatnak).

Kijelölt útválasztó (Designated Router, DR):

Olyan útválasztó, amely egy LAN (többhozzáférésű link) nevében propagál link-állapot (LSA) információkat. Az adott LAN-on belül minden útválasztó csak a DR-rel épít ki szomszédsági viszonyt. (A DR egy LAN-t képviselő "pszeudonode" funkcionalitását látja el. A szükséges információcserék száma n^2 nagyságrendről 2n nagyságrendre csökkenthető.)



VI. rész - Szállítási réteg

A szállítási (transzport) réteg funkcionalitása a bitfolyam-átvitel biztosítása az applikációk számára. Feladatai közé tartozik az átvitel vezérlése ill. szabályozása (pl. torlódás elkerülés, torlódási helyzetek kezelése). Két protokollt vizsgálunk: az (egyszrűbb) UDP és az (összetettebb) TCP protokollt.

25. fejezet - UDP (User Datagram Protocol)

Az UDP protokoll (RFC 768) egyszerű, nem megbízható (nem nyugtázott), összeköttetés mentes szállítási réteg protokoll.

Az UDP fejrész szerkezete:

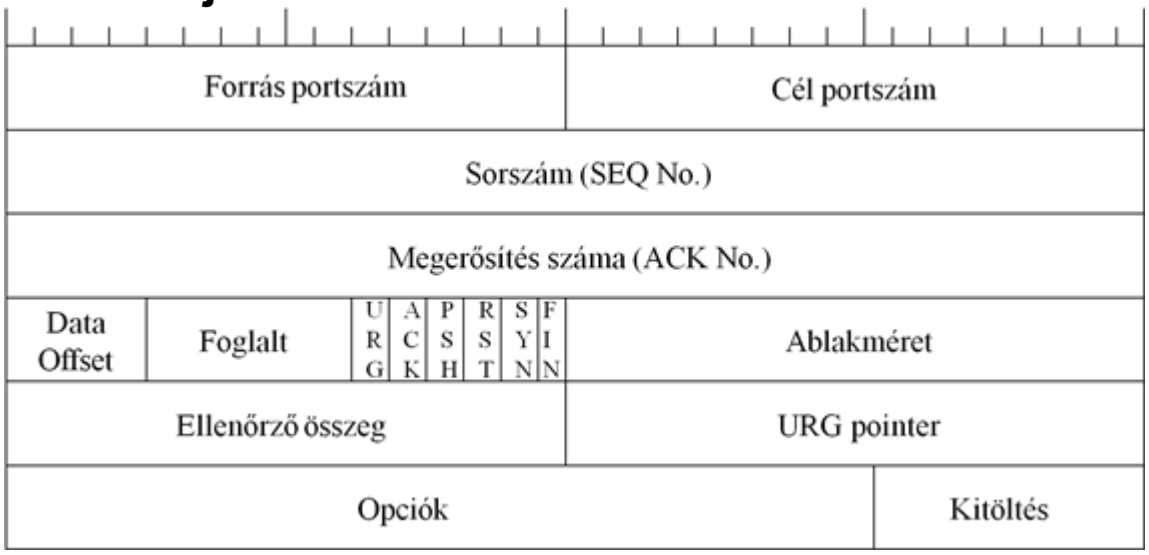
- 16 bit feladó portszám
- 16 bit célportszám
- 16 bit hossz (bájtokban)
- 16 bit ellenőrző összeg

Az UDP nagyon egyszerű protokoll. A fejrész legfontosabb két mezője a két portszám, melyek a kommunikációs adatfolyam azonosítását végzik. Nincs benne kötelező visszajelzési mechanizmus, s az áramlásszabályozást gyakorlatilag az applikációk végzik.

26. fejezet - TCP (Transmission Control Protocol)

Az TCP protokoll (RFC 793) megbízható (nyugtázott), összeköttetés alapú szállítási réteg protokoll. Az adatkommunikáció megkezdése előtt kapcsolat (TCP összeköttetés) épül ki a felek között. A kommunikáció során pedig folyamatos áramlásszabályozást lát el.

1. TCP fejrész



A TCP fejrész legfontosabb mezői:

- 16 bit feladó portszám
- 16 bit célportszám (A két portszám együttesen azonosítja a kommunikációs viszonyt)
- 32 bit szegmens sorszám (bájt sorszám modulo 2^{32})
- 32 bit nyugta sorszám (a következőként várt bájt sorszáma)
- 4 bit (Data offset) TCP fejrész hossza (szavakban)
- Legfontosabb jelzőbitek:

  SYN: Kapcsolat kiépítés (szinkronizáció)

  FIN: Kapcsolat bontás (finish)

  ACK: Érvényes a nyugta sorszám mező értéke
- 16 bit Ablakméret - (A következőként várt szegmens maximális mérete)

A szegmens hossza nincs benne a fejrészben, ez a TCP/IP interfészen adódik át az IP felé. A TCP minden bájtot sorszámoz, s a nyugtában jelzi vissza a társa felé a soron következőként várt bájt sorszámát.

A TCP áramlásszabályozást is végez: az ablakméret mezőben jelzi vissza a társának, hogy az maximum milyen hosszú szegmenst küldhet legközelebb.

2. Portszámok

A széleskörben használt szolgáltatások szerver oldali portszámait rögzítik (RFC 1700). A kliens oldali portszámokat tipikusan nem rögzítik.

Néhány példa szerver oldali portszámra:

Szolgáltatás	Portszám
HTTP	80
SMTP	25
SSH	22
DNS	53

3. TCP háromutas kézfogás

A TCP az applikációk közötti adatátvitel megkezdése előtt egy TCP összeköttetést (TCP kapcsolatot) épít ki, ezt a kapcsolatkiépítést hívjuk TCP háromutas kézfogásnak (3 way handshake).

A háromutas kézfogás működési vázlata:

1. A kapcsolat kiépítést a kliens kezdeményezi. A TCP fejrészben a portszámok megfelelően beállításra kerülnek; a kezdősorszám egy (bizonyos feltételeknek eleget tevő) véletlen-szám lesz (pl. SEQ_No=450). A jelzőbiteknél SYN=1, ACK=0.

2. A szerver megkapja a kliens üzenetét. A TCP fejrészből (jelzőbitekből) látja, hogy új kapcsolat kiépítése indult. A szerver jóváhagyó válasz-üzenetet küld: A válasz TCP fejrészben a kapott üzenet portszámait felcseréli; beállítja a saját (véletlen) kezdősorszámát (pl. SEQ_No=870), a nyugta sorszámot a kapott SEQ érték rákövetkezőjére (ACK_No=451) állítja. A jelzőbiteknél SYN=1, ACK=1.

3. A kliens megkapja a szerver válaszát, s erre egy jóváhagyást küld a szerver felé. A TCP fejrészben a kapott üzenet portszámait felcseréli; beállítja a saját szegmes-sorszámát (SEQ_No=451); a nyugta sorszámot pedig a kapott SEQ érték rákövetkezőjére (ACK_No=871) állítja. A jelzőbiteknél SYN=0, ACK=1.

4. A szerver megkapja a kliens válaszát, s ezzel a kapcsolat kiépült. Ezután megindul az applikációs rétegben használt protokollnak megfelelő adatátviteli kommunikáció.

Megjegyzés: A háromutas kézfogás üzenetei tipikusan nem szállítanak adatot; ha mégis, akkor azokat pufferelni kell, s a feldolgozásuk csak a kapcsolat kiépülése (4. pont) után kezdődhet el.

Animáció a háromutas kézfogásra

VII. rész - Alkalmazási réteg

Az alkalmazási rétegben számos protokoll működik, melyekről külön-külön is óriási irodalom áll rendelkezésre. Ebben a segédletben csupán egy példa rövid, vázlatos áttekintésével foglalkozunk. Példánkban a tartománynév-kezelő rendszert (Domain Name System, DNS) választottuk a vizsgálat tárgyának. A DNS egy nagyon alaposan átgondolt, jól felépített rendszer: több mint 20 éve fejlesztették ki a rendszer alapjait, s (bár változások történtek a rendszer működésében, de) alapvetően ugyanazon váz alapján működik napjainkban is.

27. fejezet - DNS - Tartománynév-kezelő rendszer

1. Nevek használata - kezdeti megoldások

Természetes emberi igény IP számok helyett nevek használata.

- Kezdeti megoldás: hosts.txt állomány letölthető a NIC-től.
- Néhány 100 csomópont esetén működtethető.
- Internet növekedése (’80-as évek): új megoldás szükséges.

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

- Hierarchikus tartományalapú névkiosztási séma.
- Osztott adatbázisban történő implementáció.

2. DNS tervezési szempontok

- Alapvető cél: nevekhez erőforrások rendelése.
- Nagyméretű adatbázis elosztott kezelése.

  Átmeneti tárolás (cache) lehetőség biztosítása.
- Általános célú megoldásnak kell lennie.

  név → hálózati cím
  név → postafiók-információ
  Egyéb (előre nem ismert) applikációk támogatási lehetősége.
- Tagolás: osztály és típus szerint.
- A lekérdezési tranzakció független a kommunikációs eszköztől.
- Platformfüggetlen megvalósíthatóság.

3. DNS alkalmazási feltételezések

- Adatok (többségének) lassú változása.
- Adminisztratív határok (zónák) kialakítása.

  Általában a zónák intézményeket reprezentálnak.
  Névszerver(eke)t üzemeltetnek.
  Felelősek a tartománynevek egy halmazáért.
- Biztosítani kell a kliensek névszerverhez kapcsolódási lehetőségét.
- Adathozzáférés kiemelt prioritása (konzisztenciával, naprakészséggel szemben).
- Más névszerveren tárolt adatra vonatkozó kérdés megválaszolása.

  Iteratív módszer (kötelező).
  Rekurzív módszer (opcionális).

4. DNS komponensek

A tartománynevek rendszerének három fő komponense:

- Tartománynevek (körzetnevek) tere és erőforrás rekordok
- Névszerverek
- Címfeloldó (resolver) programok

4.1. Tartománynevek tere

Fa típusú gráf, melyben minden csúcs egy erőforráshalmazt reprezentál.

A csúcsokhoz egy (max. 63 bájt hosszúságú) címkét rendelünk.

- Két testvér csúcs címkéje nem lehet azonos.
- A zéró hosszúságú címke („null címke”) a gyökér számára kizárólagosan foglalt.
- Címke belső reprezentációja:

  A címke hossza egy bájton.
  A megfelelő karaktersorozat (bájtsztring).

- A kis- és nagybetűk között nem teszünk különbséget, de célszerű megtartani a forrás írásmódját.

4.1.1. Abszolút tartománynevek

Gráfelméleti alapok DNS alkalmazása:

- A tartománynevek terében bármely csúcs egyértelműen reprezentálható a csúcstól a gyökérig vezető utat leíró címkesorozattal (abszolút tartománynév).

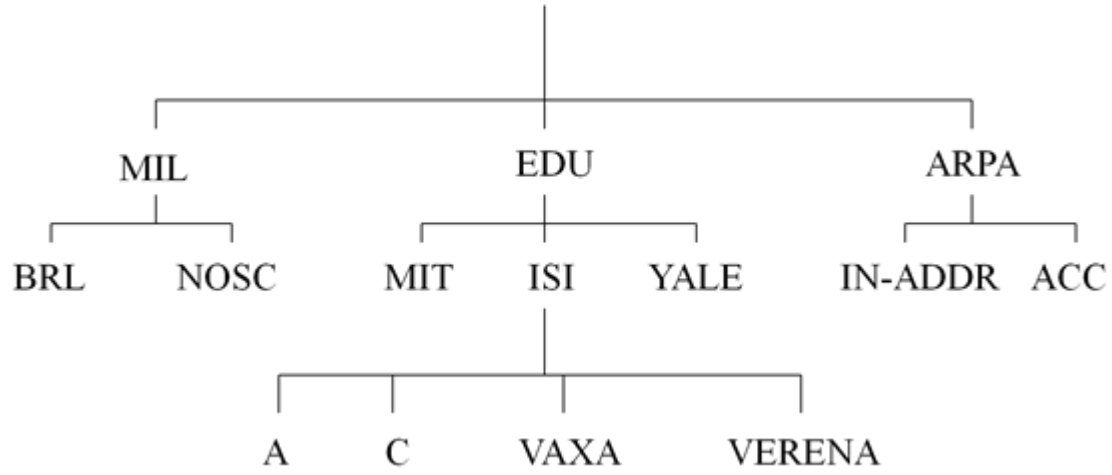
Abszolút tartománynév belső reprezentációja:

- Maximum 255 bájt hosszúságú.
- A címkéket sorrendhelyesen konkatenáljuk.
- Szükségképpen NULL karakterrel (0 bájttal) végződik.

Tartománynevek reprezentációja felhasználói interfészeknél:

- Címkesztring sorozat, elválasztó karakter a pont (.)
- Lehet abszolút és relatív.

4.1.2. Tartománynév-tér példa



Abszolút név felhasználói specifikációja pl.:

vaxa.isi.edu.

Relatív név felhasználói specifikációja pl.:

vaxa (relatív az isi.edu.-hoz képest)
vaxa.isi (relatív az edu.-hoz képest)

vaxa.isi.edu. belső reprezentációja (hexadecimális forma):

04	76	61	78	61	03	69	73	69	03	65	64	75	00

4.2. Erőforrás rekordok

A tartománynevek egy csomópontot specifikálnak.

A csomópontokhoz egy erőforrás-halmaz társítható.

Az információs erőforrások ún. erőforrás rekordokban (Resource Record, RR) tárolódnak.

Az erőforrás rekordok sorrendje lényegtelen.

Az erőforrás rekordok mezői:

tulajdonos
osztály
típus
élettartam
adat

4.2.1. Erőforrás rekordok szerkezete

Tulajdonos: Az a tartománynév, amelyhez a RR tartozik.

Osztály: 16 bites érték, mely egy protokollcsaládot, vagy egy protokollt azonosít.

IN: az internet protokollcsalád
CH: A Chaos protokollcsalád

Élettartam (TTL): 32 bites érték: A RR max. felhasználhatósági ideje (sec).

Típus: 16 bites érték a típus szerinti tagoláshoz.

A legfontosabb erőforrásrekord-típusok és jelentésük:

A	A tulajdonos hálózati címe.
CNAME	Egy alias névhez kanonikus név rendelése.
HINFO	CPU, op. rsz. információk meghatározása.
MX	Levélforgalmazó (mail exchange) megadása.
NS	Névszerver rendelése a tartományhoz.
PTR	Pointer a névtér egy másik területére.
SOA	Hitelességi (authority) zóna specifikációja.

Érték (RDATA): A típustól függően értelmezendő bitsorozat (adat).

Típus	**Adat**
A	32 bites IP cím (IN osztály esetén).
CNAME	Tartománynév.
HINFO	Tetszőleges sztring.
MX	16 bites prioritás érték és egy tartománynév.
NS	Egy host tartományneve.
PTR	Egy tartománynév.
SOA	Több mezőből álló rekord.

4.3. A tartománynév-tér partícionálása

A tartománynevek tere két (természetes) módon darabolható:

- Az osztálytagozódás alapján.

  A különböző osztályok parallel névtér-faként foghatók fel.

- A tartománynév-tér (fa) éleinek átvágásával.

  Ha a tartománynevek terében bizonyos éleket „átvágunk”, akkor a maximálisan összefüggő részgráfok szintén fa struktúrájúak.
  Egy ilyen maximálisan összefüggő részgráfot zónának nevezünk.
  Egy zóna reprezentálható a gyökérhez legközelebbi csúcsának tartománynevével.
  A zónák közötti „átvágásokat” nyilván kell tartanunk.

4.4. Névszerverek

A névszerverek olyan szerverprogramok, melyek:

- Információt tárolnak a tartománynevek gráfjáról.
- Tartománynevekhez tartozó erőforrás rekordokat tárolnak.
  - Egy (vagy több) zónához tartozó valamennyi csomópont hiteles (authoritative) erőforrás rekordját.

    A zóna gyökérhez legközelebbi csúcsát leíró adatokat.

  - Szomszéd (gyermek) zónákhoz (és ezek névszervereihez) vezető információkat.
  - Időlegesen más zónákhoz tartozó RR-t (cache).
- Kérdéseket (lekérdezéseket) válaszolnak meg.

Rekurzív módon
Nem rekurzív (iteratív) módon

4.4.1. DNS kérdések

A lekérdezések és válaszok egy standard formátumot követnek:

- **Fejrész.** Egy bitkombináció a különböző kérdések (pl. standard query, status query stb.) elkülönítésére.
- **Kérdés.** A kérdéses név, és a kérdés egyéb paraméterei.
- **Válasz.** A kérdéshez tartozó direkt válasz.
- **Hitelesség.** A hiteles szerverek adatait leíró rekordok.
- **További adatok.** A kérdéshez kapcsolódó egyéb információk (RR).

DNS kérdés példa.

Fejrész	OPCODE=Standard Query
Kérdés	QNAME=ISI.EDU. CLASS=IN TYPE=MX
Válasz	
Hiteles	
További	

DNS válasz példa.

Fejrész	OPCODE=Standard Query, Response, AA
Kérdés	QNAME=ISI.EDU. CLASS=IN TYPE=MX
Válasz	ISI.EDU 86400 IN MX VAXA.ISI.EDU.
Hiteles	
További	VAXA.ISI.EDU IN A 10.2.0.27 A 128.9.0.33

4.4.2. Rekurzív és nem rekurzív módszer

Nem rekurzív módszer:

- Szerver oldalon a legegyszerűbb megvalósítás.
- Minden névszerverben implementált.
- A kliensnek lehetősége nyílik az információk értékelésére.

Rekurzív módszer:

- Kliens oldalon a legegyszerűbb megvalósítás.

- A szerveren megvalósítható átmeneti tárolás (cache).
- Opcionális, mind a szerveren, mind a kliensen implementált-nak kell lennie.

  A szerver minden válaszában egy bit (RA) jelzi az implementációt.
  A kliens a kérdésben egy bittel (RD) jelzi a rekurzív igényt.

4.5. Címfeloldó (resolver) programok

A címfeloldó programok a felhasználói programok és a névszerverek közötti interfészek.

A címfeloldás ideje lehet kicsi (millisec.) pl. helyi adatokból felépített válasz esetén, de lehet nagy (több sec.) névszerverek adatait kérdezve.

A címfeloldás kliens oldala általában platformfüggő.

Általános funkciók:

Gépnév → gépcím meghatározás
Gépcím → gépnév meghatározás
Általános lekérdezési funkció

4.5.1. Címfeloldási eredmények

A címfeloldók az igényelt tevékenység elvégzése után (általában) a következő eredményekkel térhetnek vissza:

- Egy vagy több RR, a választ tartalmazva
- Névhiba (Name Error, NE)

  A kérdezett név nem létezik.
- Adat nem található (Data Not Found)

  A név létezik, de a kérdezett adat (vagy típus) nem.
- Átmeneti hiba

  Például valamilyen hálózati hiba (vonalhiba) miatt a kérdezett zóna nem elérhető.
  Gyakran nem implementálják külön válaszként.

Irodalomjegyzék

Tanenbaum, Andrew S. *Számítógép-hálózatok* Bővített, átdolgozott kiadás 978-9635453849 Panem Prentice Hall Kiadó 2003

Tanenbaum, Andrew S. *Computer Networks* 4th edition 978-0130661029 Prentice Hall 2002

Halsall, Fred *Computer Networking and the Internet* 5th edition 978-0321263582 Addison Wesley 2005

Stallings, William *Data and Computer Communications* 8th edition 978-0132433105 Prentice Hall 2006

Géher, Károly *Híradástechnika* 2. kiadás 963 16 3065 X Műszaki Kiadó 2000

Thomas, Stephen A. *IP kapcsolás és útválasztás* 978-9639301412 John Wiley & Sons – Kiskapu Kft 2002

RFC Dokumentumok http://www.rfc-editor.org