## Itt a listája azon kérdéseknek amiket ez a jegyzet válaszol

**BOLD – mindig / majdnem mindig szerepel**

Szín az, hogy szubjektívségemben mennyire találtam nehéznek :P

Ne ijedj meg, mert nagyonkönnyű, max első ránézésre nehéz - Közepes - Szar. Fos. >\_<

Speciális szín: ez a tétel csak egyszer jelent meg az példavizsgák közt.

1. [**Számítógépes hálózatok osztályozása négy szempont szerint( lefedett fizikai méret ...)**](#_A_számítógép_Hálózat)
2. [**Lefedett fizikai méret szerint osztályozza a hálózatokat (csak az első szempontja az első résznek!)**](#_Lefedett_fizikai_terület)
3. [**Három kapcsolási mód**](#_Kapcsolási_Módok)
4. [**Kommunikációs protokoll elemei (a három def. simán)**](#_Kommunikációs_protokoll_és)
5. [**A rétegelt hálózati modellek *(három típúsa)* ( OSI, TCP/IP, Hibrid) – mindegyikhez felrajozolod a kis szerkezetét, OSI-t ki kell fejteni, a TCP-hez félmondat, a hibridhez egy bekezdés tartozik.**](#_OSI_Referenciamodell_és)
6. [Ismertesse a három alsó réteg köztes hálózati csomópont változatait és működését! (a repeater/hub, híd, switch, meg routerre, meg talán access pointra kíváncsi itt)](#_Hálózatti_köztes_csomópont)
7. [Útválasztó protokollok (egy-egy mondat) – itt mindegyikről egy kevés amit megjegyzel](#_Útválasztás_és_forgalomirányítás)
8. [Ismertesse a vektor-állapot alapú forgalomirányítást (rajz és szöveg)](#_Vektor-Állapot_alapú_forgalomirányí)
9. [Modulációs sebbeség, és adatátviteli sebbesség (kell hozzá a digitális / analóg jel rajz!)](#_Számítógép-hálózati_csomópont_(komm)
10. [802.3 ellenőrző mechanizmus (rajz, jellemző, magyarázat)](#_Ethernet(IEEE_802.3))
11. [805.2 ellenőrző mechanizmus (rajz – itt csak a topológiák lehetnek szerintem, jellemző, magyarázat) – TOKEN RING](#_802.5_Token_Ring)
12. [VLSM és CIDR](#_Forgalomirányítás_osztály_nélküli)

Megkell tanulni az IP-t (v4 és v6-ot), mert ezek a kérdések mind jöhetnek:

1. Címzett és címző alapján ismertesse az IPv4 és IPv6-ot (leírás róluk)
2. [IPv4 szerkezete! (igen, kell a táblázat, lehetőleg figyelve a cellák méreteit, azért színeztem!)](#_IP_protokoll_adatelem)
3. [IPv6 szerkezete](#_Csomag_felépítése_és)
4. IPv4 és v6 táblázatos összehasonlítása ( mi változott , ez az IPv6 nál a narancs meg zöld mezők dolog)
5. [TCP felépítése](#_Transmission_Control_Protocol)
6. [UDP felépítése](#_User_Datagram_Protocol)
7. [Táblázatosan hasonlítsa össze a TCP és UDP protokollokat](#_TCP_VS_UDP)

[**Hasonlítsa össze táblázatosan az OSPF / RIP / IS – IS / EIGRP ( közül kettőt ).**](#_AZ_összehasonlító_táblázat!)

1. [NAT vagy PAT (NAThoz kell az a rajz)](#_Hálózati_címcsere_(NAT)) - a PAT már volt PTI 2. Vizsgán, NAT ot mindenképp érdemes
2. [ALOHA és réselt ALOHA](#_ALOHA) - már volt a PTI második vizsgán
3. [DSL](#_DSL:_Digital_Subscriber) még PTI-n nem volt, olvasd el a nagyjegyzetből ha kell (szerintem ez a legeasybb közülük)
4. PPP még PTI-n nem volt, olvasd el a nagyjegyzetből ha kell , egyik se nagyon nehéz tho.
5. ICMP még PTI-n nem volt, olvasd el a nagyjegyzetből ha kell
6. [**ISDN**](#_ISDN:_Integrated_Services) **– első 2őn volt, most legútóbbin nem. Idk wat to tell you.**
7. [SNMP mechanizmus PTI-n még nem volt, de itt van ebben, ment ugyanaz a kategória mint az RMON](#_Hálózatmenedzsment_SNMP-vel:)
8. [RMON (RMON1 / RMON2) mechanizmus](#_RMON) első két vizsgán volt, 1 dia, de sok info ☹
9. [Email – a mi vizsgánkon volt, elvileg a kategóriákról kellet írkálni röviden + rajz. GZ diákban érdemes átnézni, én nem bírtam megjegyezni.](#_Elektronikus_üzenetküldés:_postafió)
10. Soroljon fel 10 darab protokollt az alkalmazás rétegből(rövidítés, angol neve, funkciója, tömör bemutatása) – nagyjából hasonló az emaileshez PTI-n még nem volt
11. Ismertesse Nyquist és Shannon fizikai réteghez vonatkozó állítását(szabályok és összetevők magyarázata). – most volt nekünk. It stinks :P

## A számítógép Hálózat elemei, fogalmak Osztályozási szempontok

### Lefedett fizikai terület mérete szerint:

* Hálózat az emberi testen (**BAN: Body Area Net**., BCI – Brain Comp. Interf.)
* Személyi hálózat (**PAN: Personal Area Network**)
* Otthoni/kiscéges hálózat (**SOHO: Small Office/ Home Office**)
* Helyi hálózat (**LAN: Local Area Network**)
* Egymással adatkommunikációs  
   kapcsolatban lévő számítógépek együttetese.
* Állandó hozzáférés a hálózati szolgáltatásokhoz.
* A LAN kiépítését és kezelését az intézmény végzi.
* A LAN-ok átviteli sebessége viszonylag nagy lehet (10 – 100(00) Mbps) a rövid távolságoknak köszönhetően.
* Az adatátvitel biztonsága a rövid távolságok és a technológiából eredendően magas.

LAN típusok:

* Összeköttetéssel működő (huzalozott, pl. csavart érpár, koaxiális kábel, optikai szál)
* Összeköttetés nélküli (nem huzalozott: rádióhullámok)

Tipikus LAN összetevők

* Számítógépek
* Hálózati interfész kártyák
* Hálózati média (csavart érpár, koaxiális kábel, optikai szál vagy rádióhullámok)
* Hálózati eszközök:Ismétlő (Hub) , Híd (Bridge) , Kapcsoló (Switch), Forgalomirányító (Router)
* Városi/területi hálózat **(MAN: Metropolitan Area Network)**
* Kiterjedése egy város vagy néhány kerület
* Két vagy több LAN-t kapcsolnak össze
* Technológiájuk általában a LAN-éval azonos
* Nagyterületi hálózat **(WAN: Wide Area Network)**
* Nagy, földrajzilag elkülönített területen működnek
* E-mail, World Wide Web szolgáltatások igénybevétele
* Globális hálózat **(GAN/Internet: Global Area Network)**

### Adatátviteli ráta szerint:

* Klasszikus hálózatok: **kbps … Mbps**
* Nagysebességű hálózatok: **100 Mbps … Tbps**

### Tulajdonjogszerint**:**

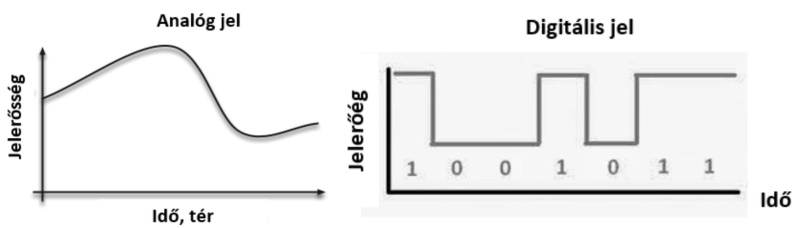
* + Magán hálózat (Private Network)
  + Nyilvános hálózat (Public Network)

### Mobilitás szerint:

* + Rögzített (Fixed Network)
  + Mobil (Mobile Network)

## Kommunikációs Alapfogalmak

### Sebbeséges kérdés :P



#### Moduláció/Demoduláció:

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

#### Multiplexelés/Demultiplexelés:

Két vagy több különböző kommunikációnak azonos vonalon (vagy csatornán) egyidőben történő küldése (multiplexelés). A nyelő (vételi) oldalon a szétválasztás a demultiplexelés.

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

Időegység alatt átvitt bitek mennyisége. Mértékegysége: bit/másodperc Jel: b/s, bps.

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

#### Moduláció sebesség (jelváltás sebesség):

Időegység alatt bekövetkező jelváltások száma, vagyis a csatornán érvényes szimbólumok közötti átmenetek száma.

Mértékegysége: jelváltás/másodperc (baud)

## Kapcsolási Módok

### Vonalkapcsolt (áramkörkapcsolt, circuit switched) technológia:

Azadatátvitel előttdedikált kapcsolat (kommunikációs áramkör) épül ki a két végpont között, s ez folyamatosan fennáll, amíg a kommunikáció tart. (Pl. klasszikus vonalas telefon.)

### Üzenetkapcsolt (store and forward) technológia:

Nem épül ki áramkör, hanem a teljes üzenet kapcsolóközpontról kapcsolóközpontra halad, mindig csak egy összeköttetés szakaszt terhelve. (Pl. telex)

### Csomagkapcsolt (packet switched) technológia:

Azadatot korlátozott maximális méretű részekre (csomagokra) darabolják, s ezeket mint önálló elemeket egymás után továbbítják. A módszert a jól tervezhető pufferelési tulajdonsága miatt előszeretettel alkalmazzák.

**! Az internet csomagkapcsolt.**

## Kommunikációs protokoll és elemei:

#### Protokoll:

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

A protokollok pontos leírására általában speciális eszközöket alkalmaznak: pl.

kiterjesztett véges automaták, SDL (Specification and Description Language),

magasszintű nyelvek.

#### Protokoll entitás (PE – Protocol Entity):

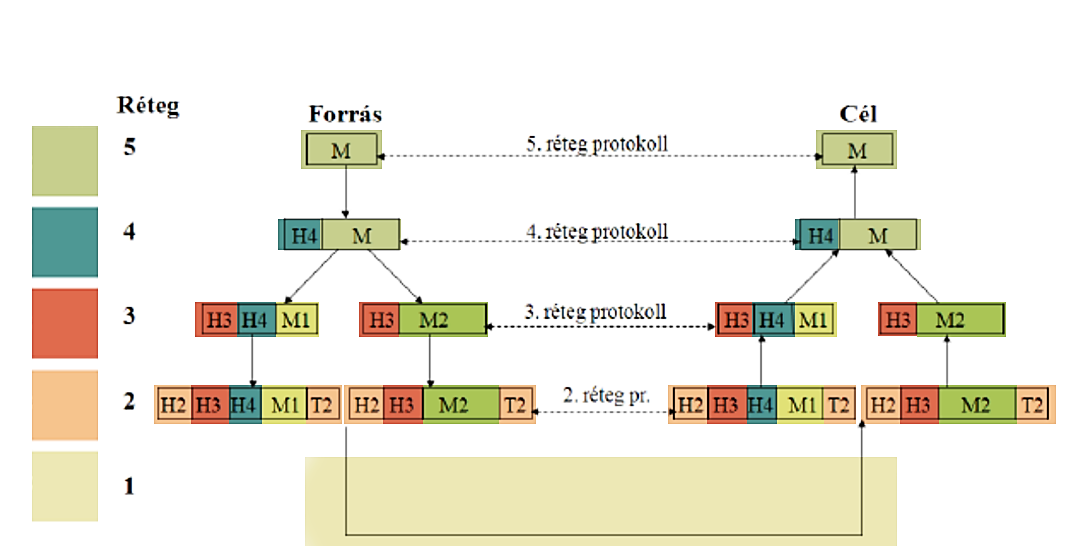
A forrás és/vagy cél kommunikációjátmegvalósító hálózati entitás (hardver/firmware és/vagy szoftver). Pl. kommunikációs eszköz, kommunikációs program.

#### Protokoll adatelem (PDU – Protocol Data Unit):

A kommunikáció során továbbított adat(rekord), amely a protokoll entitások között a protokoll szabályok szerint továbbítódik. Szerkezete és mérete az adott kommunikációs technológia előírása szerinti.

## C:\Users\Bernkastel\AppData\Local\Microsoft\Windows\INetCache\Content.Word\retegek.pngRétegelt hálózati architektúra \_ btw ez a rajz nem kell csak szép lett ☺

## Hálózati Kommunikáció vázlata, rétegmodell



Réteg5 Réteg4 Réteg3 Réteg2 Réteg1

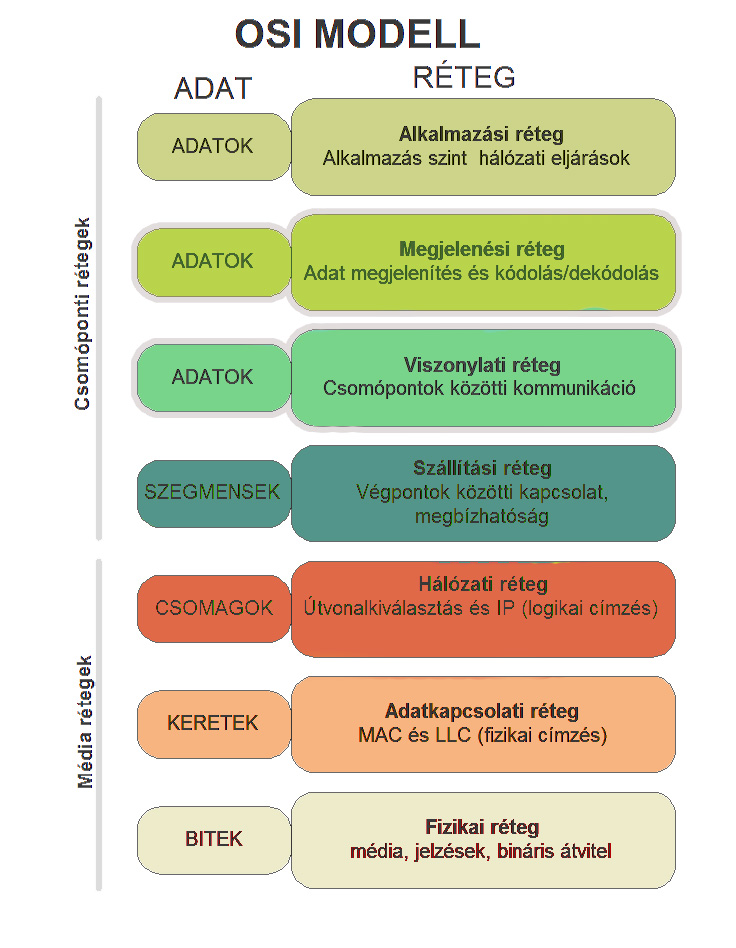
RÉTEGMODELL, A legfelső rétegben jelenik meg a kommunikáció tárgyát képező üzenet ( M ). Logikailag a legfelsőbb rétegbeli (a például az 5. rétegbéli) entitás az üzenet a társ entitásnak (5. Rétegben ) küldi, az adott réteg működését leíró protokoll alapján.

Valójában a forrás oldalon egy adott rétegbéli 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 ellátásához további mezőket társít a felsőbb rétegtől kapott adatelem elé ( “H” fejrész “header” ), vagy után (“T” végrész, “tailor” , pl. az ellenőrző összeg, a *checksum* ilyen ).

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

## OSI Referenciamodell és rétegei, rétegmodell

A nemzetközi szabványügyi hivatal (ISO) által elfogadott 7 rétegű (ún. *Nyílt rendszerek összekapcsolási*, OSI – Open System Interconnect) modellje.

**7. Applikációs (Alkalmazási ) réteg**

Az applikációk (fájlátvitel, e-mail, stb) működéséhez nélkülözhetetlen szolgáltatásokat biztosítja.

### **6. Megjelenítési réteg**

Feladata a különböző csomópontokon használt különböző adatstrúktúrákból eredő információ-értelmezési problémák feloldása.

### **5.Viszony réteg**

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

### **4.Szállítási réteg**

Megbízható hálózati összeköttetést létesít két csomópont között. Feladatkörébe tartozik pl. A virtuális áramkörök kezelése, átviteli hibák felismerése, javítása és áramlásszabályozás.

### **3.Hálózati réteg**

Összeköttetést és útvonalválasztást biztosít két hálózati csomópont között. Ehhez a réteghez tartozik a hálózati címzés és az útvonalválasztás (routing).

### **2.Adatkapcsolati réteg**

Megbízható adatátvitelt biztosít egy fizikai összekötettésen 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.  
**1.Fizikai réteg**

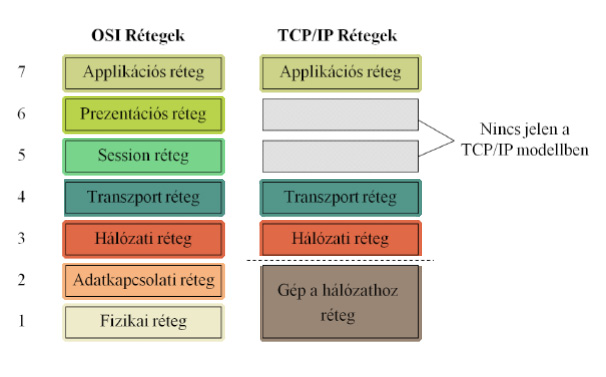
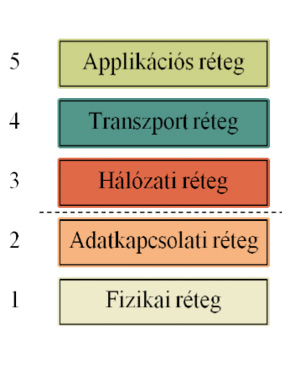
Elektromos és mechanikai jellemzők procedurális és funkcionális specifikációja két (közvetlen fizikai összeköttetésű) eszköz közötti jeltovábbítás céljából.

BTW ez a táblázat NEM KELL, csak írja, hogy melyik rétegnek milyen PDU típúsa van.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Szám | Réteg neve |  | PDU neve | |
| 7. | Applikációs | (Application) | Üzenet (APDU) | Message |
| 6. | Megjelenítési | (Presentation) | Üzenet (PPDU) |
| 5. | Viszony | (Session) | Üzenet (SPDU) |
| 4. | Szállítási | (Transport) | Szegmens (TPDU) |
| 3. | Hálózati | (Network) | Csomag | Packet |
| 2. | Adatkapcsolati | (Datalink) | Keret, cella | Frame, cell |
| 1. | Fizikai | (Physical) | Bit | Bit |

#### Megfontolás:

A hétköznapi életben leginkább elterjedt hálózati technológia a TCP/IP protokollrendszerre épülő hálózat (Internet). A TCP/IP architectúra (korántsem egységes) modellszemlélete eltér az OSI modellétől (a prezentációs és Session réteg nincs jelen a TCP/IP modellben)

S. Tanenbaum javaslata alapján a hálózati kommunikáció tanulmányozására az ún. hibrid modellt használjuk: alsó két rétegében az OSI modell szerinti fizikai és adatkapcs. Réteg jelenik meg, felsőbb rétegeket pedig TCP/IP szerint a hálózati, szállítási és applikációs rétegek képviselik.

Hibrid modell

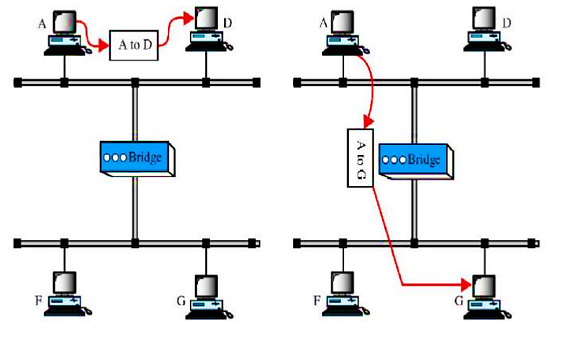
## Hálózatti köztes csomópont típúsok és funkcióik

|  |  |  |
| --- | --- | --- |
| Köztes csomópont (eszköz) | Réteg száma | Réteg neve |
| Átjáró (gateway) | 4. | Szállítási |
| Forgalomirányító, útválasztó (router) | 3. | Hálózati |
| Híd (bridge), kapcsoló (switch) | 2. | Adatkapcsolati |
| Jelismétlő (repeater, hub) | 1. | Fizikai |

Jelismétlő

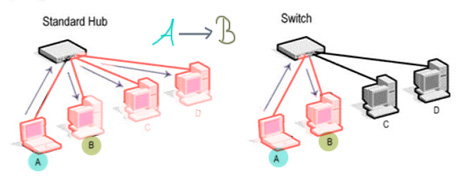
Az átviteli közegen továbbított jeleket ismétli, erősíti, időzítésüket szabályozza.

* Az összekapcsolt részhálózatokat (ütközési tartományokat) **nem** **izolálja**!
* Strukturált hálózatban alkalmazott változat neve: **HUB**

Híd(Bridge)

* Fizikai **ÉS** adatkapcsolati rétegben működve *szelektív* összekpacsolást végez
* “*Csak az megy át a hídon, aki a túloldalra tart.”*
* Az összekapcsolt részhálózatok külön ütközési tartományokat alkotnak.
* Az üzenetszórást általában minden összekapcsolt részhálózat felé továbbítja.
* A portok sűrűsége alacsony (2 / 4)

Kapcsoló (Switch)

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

Vezeték nélküli hozzáférési pont, bázisállomás (Access Point)

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

Forgalomirányító (Router)

* A fizikai **ÉS** az adatakpacsolati **ÉS** a hálózati rétegben működve *szelektív* összekapcsolást, *útvonalválasztást*, *forgalomirányítást* végez.
* Az összekapsolt részhálózatok külön ütközési tartományt és külön üzenetzórási tartományt alkotnak.
* Mindegyik interfészen saját hálózati címmel rendelkeznek.

## ALOHA

Eredet: Hawai Egyetem – szigetek közötti rádiós kommunikáció.

* A továbbítandó keret azonnal a csatornára kerül.
* Fogadó nyugtázza a keretet, ha nem volt ütközés.
* Ütközés esetén a forrás *véletlen* ideig vár és újból elküldi a keretet.
* Egyszerű működés, könnyen implementálható.
* Az ütközések miatt a csatorna várható maximális kihasználtsága alacsony (18%).
* Keretátvitelre veszélyes időtartam (lásd illusztráció).

## Réselt ALOHA

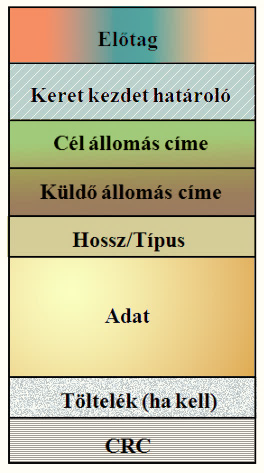
* Időrések használata, amiben elfér a keret.
* A továbbítandó keret a következő időrés elején kerül a csatornára.
* Fogadó nyugtázza a keretet, ha nem volt ütközés.
* Ütközés esetén a forrás véletlen ideig vár és újból elküldi a keretet.
* A csatornakihasználtság egyszerűen növelhető (36%).
* Keretátvitelre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

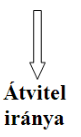
## Ethernet(IEEE 802.3)

Lehetséges topológiák:

* Sín
* Fa (Repeater)
* Csillag (Hub, Switch)

## Ethernet keretformátum



**7 bájt:** 7x ‘1010 1010’ szinkronizációs

**1 bájt:** ‘1010 1011’

**6 bájt:** 1-3 gyártó azonosító, 4-6 sorszám

**6 bájt: -||-**

**2 bájt:** hossz/típús jelzése

**0-1500 bájt**  adat

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

**4 bájt:** ellenörző összeg

Célcím lehetséges értékei:

1. Egy állomás pontos címe
2. Csupa ‘1’ bit üzenetzórás (broadcast) – az üzenetet minden állomás veszi.

! A küldő állomás címe nem lehet többes cím!

## IEEE 802.3 Ethernet Kerettovábbíttás (CSMA / CD) lépései

1. Várakozás továbbítandó keretre, majd a keret formázása.
2. Csatorna foglalt-e?

IGEN: ugrás 2-re.

NEM: keretek közötti idő kivárása, majd kerettovábbítás megkezdése.

1. Van ütközés küldés közben?

IGEN: zavarójelek küldése. Továbbíási kísérletek számának növelése. Ugrás 4-re.

NEM: átvitel befejezése. Sikeres átvitel jelzése. Ugrás 1-re.

1. Elértük a max. kísérletszámot (16)?

IGEN: sikertelen továbbítás jelzése. Ugrás az 1-re.

NEM: késleltetés kiszámítása és az idő kivárása. Ugrás 2-re.

## IEEE 802.3 Ethernet Keretfogadás (CSMA / CD) lépései

1. Van bejövő jel a közegen?

VAN: Csatorna foglaltságának jelzése. Bitszinkronizálás, keretkezdet azonosítás, keretbeolvasás.

NINCS: Ugrás 1-re.

1. Ellenőrző összeg (CRC) és kerethossz rendben?

IGEN: tovább a 3-ra.

NEM: Keret eldobása. Ugrás 1-re.

1. Célcím = ( saját cím vagy csoportcím )?

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

NEM: Keret eldobása, majd ugrás 1-re.

## 802.5 Token Ring átviteltechnika

Lehetséges topológiák:

* Gyűrű (Repeater)
* Gyűrű huzalozott csillag

(Repeater, Switch)

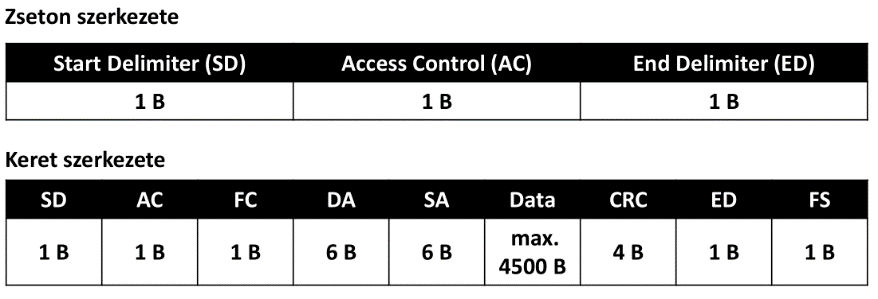
Gyűrű huzalozott csillag

Gyűrű

Token Ring (ISO/IEEE 802.5):

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

Vezérjeles gyűrű működési elve:

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

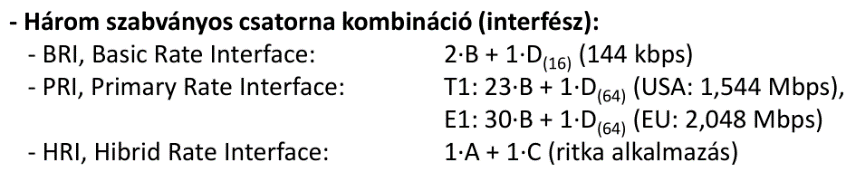
Token Ring változatok:

* TR (4 Mbps):Egyszerre csak 1 keret van a gyűrűben. A vezérjelet a feladó állomás csak akeret visszaérkezése után továbbítja. Max. 72 csomópont azonos gyűrűben.
* ETR (Early TR, 16 Mbps):Egyszerre több keret van a gyűrűben. A vezérjelet a feladóállomás a keret elküldése után azonnal továbbítja a rákövetkező állomásnak (early token release). Max. 125 csomópont azonos gyűrűben.
* FTR (Fast TR, 100 Mbps):IEEE 802.5t

## ISDN: Integrated Services Digital Network

Általános leírás

1. Célja digitális adat, hang, videó forgalmak integrációja azonos technológián.

Áramkörkapcsolást használ a tartalom továbbításához.

1. **Szabványos csatornatípusok:**

A: 4 kHz analóg telefoncsatorna.

B: 64 kbps digitális hang vagy adatcsatorna.

C: 8/16 kbps digitális csatorna.

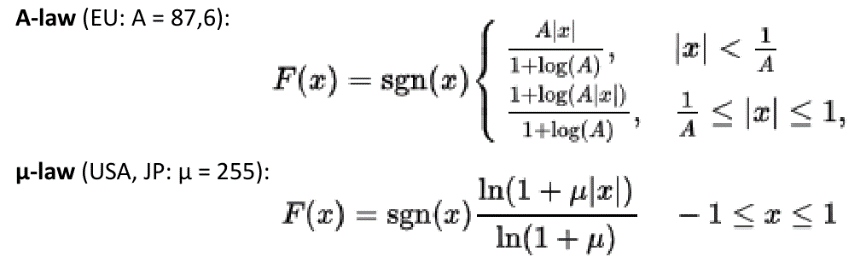
D: 16/64 kbps digitális csatorna (jelzés, signaling).

1. **Jelzésrendszer: ITU-T Q.931 (QSIG)**

* Gyors kapcsolat felépítés és kapcsolat lebontás a D csatornán.
* Átviteli ráta növelés n·64 kbps lépésekben.
* Több egyidejű áramkör építhető ki adott interfészen

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

Alkalmazott hangkódolási technika: **PCM (Pulse Code Modulation)**

* 1. Analóg jel amplitúdójának átalakítása digitálisra (A/D)
  2. Mintavételezési frekvencia: 8 kHz
  3. Mintavételi mélység: 8 bit
  4. Átviteli ráta: 64 kbps
  5. Mivel az emberi hallószerv érzékenyebb az alacsony hangerő skálán bekövetkező változásra, ezért a [-27, 27] amplitúdó tartományt átkódolják önmagára nem lineáris törvény szerint.
  6. **Kódolási törvények (ne jegyezd meg, de itt vannak :P )**

# IP technológia Hálózati Rétege, IP technológia címzési rendszere

## IP protokoll adatelem szerkezete

1. Vint Cerf és Bob Kahn (USA): 1974
2. Az IP a TCP/IP referenciamodell általános adatszállításra szolgáló hálózati réteg protokollja.
3. Összeköttetés mentes (datagram) szolgáltatást nyújt a szállítási réteg felé.
4. Datagram: önálló adatcsomag, amely az azonosításhoz és a kézbesítéshez szükséges összes elemet tartalmazza.

**Felépítése:**

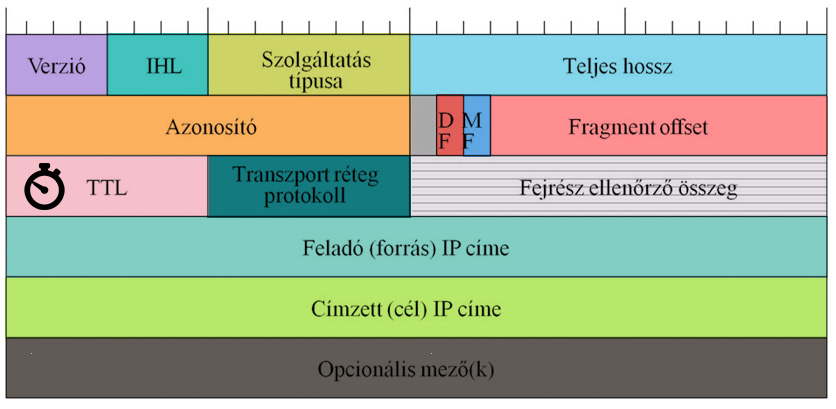
1. IP csomag: fejrész (Header) + rakrész (Payload)
2. Típusazonosító az L2 (pl. Ethernet) keretekben: 0x0800

IP csomag fejrész:

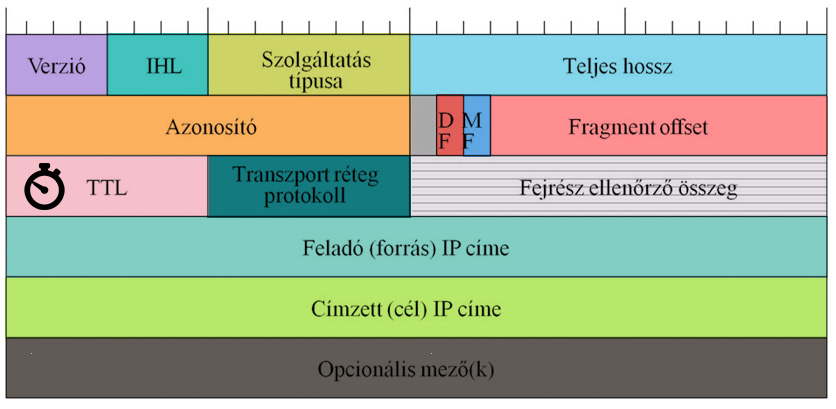
* 1. A datagram kézbesítéséhez szükséges információk (címek, vezérlő és ellenőrző mezők)
  2. 4 bájtos (32 bites) szavakból áll
  3. Szavak száma: minimum: 5, maximum: 15.

IP csomag rakrész:

* 1. Szállítási réteg adatelemét foglalja magába
  2. Maximális méret: 64 kB
  3. Nincs hibaellenőrző kód



1. 1. szó
2. **Verzió**: IPv4 (0x4), IPv6 (0x6)
3. **IHL**: IP csomag fejrészének hossza [szó]
4. **ToS**: Szolgáltatás típusa, minőségi jellemzők (QoS)
5. **SoD**: Adatmező+fejrész hossza [Bájt]

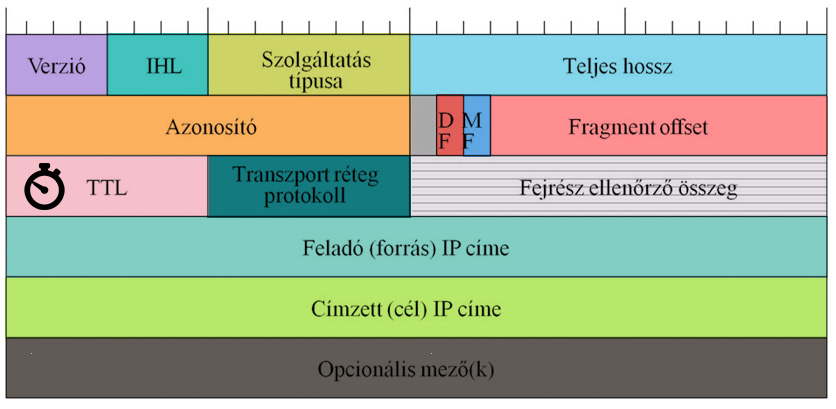


2.szó

1. Csomag darab (fragmentum) azonosító

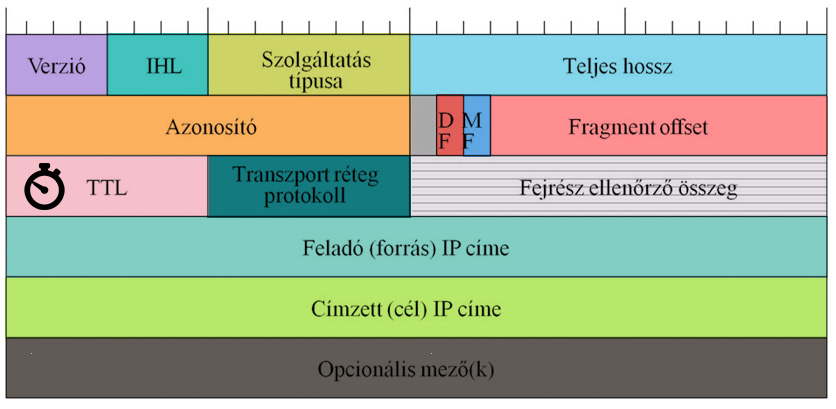
DF (Don’t Fragment): darabolás tiltás

1. MF (More Fragment): további csomagdarab létezik
2. Fragmentum offset: csomagdarab helye a nagy csomagban



3.szó

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



4.szó

5.szó

1. **Forrás (feladó)** IP cím: 32 bit
2. **Cél (címzett)** IP cím: 32 bit
3. **Opcionális információk**: továbbítási útvonal naplózása (Record route) , Késleltetési idők naplózása (Timestamp)

Az IP cím hossza bájtok 4k típusú többszöröse:

* IPv4: k = 1,
* IPv6: k = 2.

IP címek formátuma:

* IPv4: decimálisan reprezentált bájtok, pont („ . ”) karakterrel elválasztva,
* IPv6: hexadecimálisan reprezentált (ld. később).

## IP címkezelés:

1. Az IP címzésnél használt kódolási módszer: maszkolás

Maszk:

* 1. Hossza megegyezik az IP cím méretével.
  2. Formája: 1111 … 1100 … 0 = „N(1)”„H(0)”
     1. **N**etwork: hálózat (halmaz) azonosító rész,
     2. **H**ost: host (interfész) azonosító rész.
  3. Szabályok:
     1. „0” bit után csak „0” bit lehet,
     2. „1” bit után bármi lehet.
  4. Jelölések:
     1. Bináris: 11111111111111111111111100000000
     2. Decimális: 255.255.255.0
     3. Prefix: /24 (N: 24 db bit, H: 32-24 = 8 bit)

1. Maszkolás: bitpozíciónkénti ÉS művelet: N = IP Λ M, H = IP - N
2. Prefix (/n) méretének hatása:

* Nagy prefix: sok kisméretű (kevés host) különböző üzenetszórási tartomány,
* Kis prefix: kevés nagyméretű (sok host) különböző üzenetszórási tartomány.
* Cél: a tartományok (hálózatok) kihasználtsági szintjének növelése, tartalékkal.

Speciális IP host címek:

* 1. IP hálózat (halmaz) azonosító: IP =NH, ahol H = „csupa bináris 0” (legkisebb érték).
  2. IP üzenetszórás (broadcast): IP = NH, ahol H = „csupa bináris 1” (legnagyobb érték).

## Forgalomirányítás osztály nélküli hálózatok között (CIDR):

CIDR: Classless Inter-Domain Routing

1. A hálózat-host határvonal pozíció nem osztály, hanem az igényelt csomópont-darabszám alapján kerül meghatározásra.
2. A hálózat-host határvonal pozíció jelzésére kötelező a prefix hossz, vagy a hálózati maszk megadása.
3. Egy adott tartományon kívül eső hálózatokra vonatkozóan elegendő összegző (aggregált) irányítási információ tárolása, mivel a távoli címzési zóna részletinformációit nem szükséges ismerni.
4. Az irányítási táblák növekedési problémáinak kezelésére földrajzi elhelyezkedés szerint címtartomány-zónákat alakítottak ki (RFC 1366, 1466):
5. VLSM: CIDR encompasses several concepts. It is based on the **variable-length subnet masking** (VLSM) technique with effective qualities of specifying arbitrary-length prefixes. CIDR introduced a new method of representation for IP addresses, now commonly known as **CIDR notation**, in which an address or routing prefix is written with a suffix indicating the number of bits of the prefix.
6. Röviden VLSM ( variable-length subnet masking) – mikor prefixet írsz hozzá, és nem a 3 osztály szerint állapítod meg, hogy hány bit a Network, hány bit a HOST.

# 

## Hálózati címcsere (NAT)

**N**etwork **A**ddress **T**ranslation

Megfontolások:

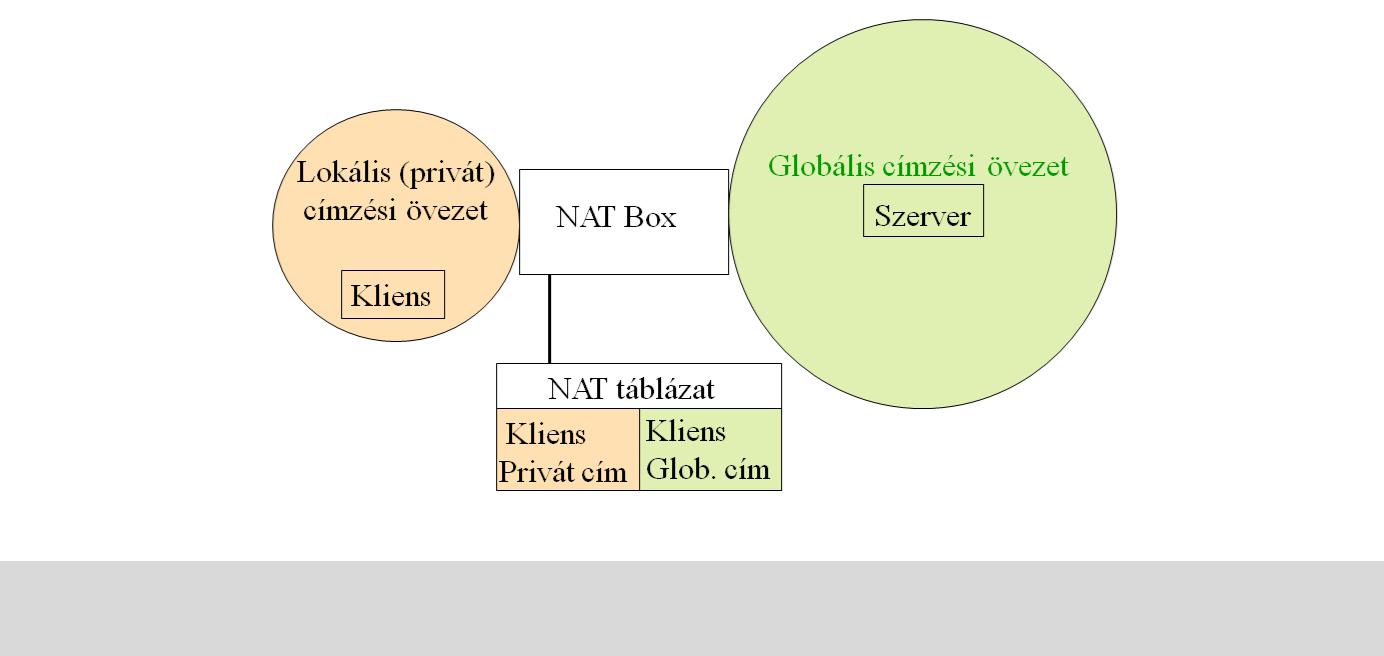
1. Az IPv4 címtartomány mérete ma már nem elégséges a jelenlegi Internet összes csomópontjának egyedi címzéséhez.
2. A csomópontok jelentős része csak kiszolgálást kér (kliens), nem szolgáltat (szerver).

NAT alapfogalmak – ez a 4 def. nem hiszem, hogy kell!

1. Címzési övezet (Address Realm):Az a hálózatrész, amelyben biztosítani kell az IP-címekegyediségét.
2. Külső hálózat (Public/Global/External Network):Az IANA által kezelt címtartománnyalrendelkező címzési övezet. A külső, globális hálózatban használatos címek a teljes Internetre vonatkozóan egyediek.
3. Belső hálózat (Private/Local Network):Előfizető cég saját (belső, privát) címzésselrendelkező címzési övezete.
4. Privát címtartomány (RFC 1918):Abelső hálózatban használt címek, amelyhez tartozócsomagokat a szolgáltatói routerek nem irányítják. A privát címek a világon nem egyediek, mert másik cég belső hálózatában ismételten megjelenhetek.

NAT működési mechanizmus:

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

A klasszikus IP címcsere (Basic NAT):

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

NAT típusok:

1. Statikus NAT: n db lokális IP cím ↔ n globális IP cím rögzített összerendelése

Privát IP című csomópont: kliens vagy szerver.

Dinamikus NAT: n db lokális IP cím ↔ m db globális IP cím változó összerendelése (n ≥ m).

n: privát IP című csomópontok maximális száma.

m: publikus IP című gépek száma = szimultán viszonyban lévő belső csomópontok száma.

Privát IP című csomópont: csak kliens.

## Hálózati Portcím csere (**P**ort **A**ddress **T**ranslation)

PAT működési mechanizmus:

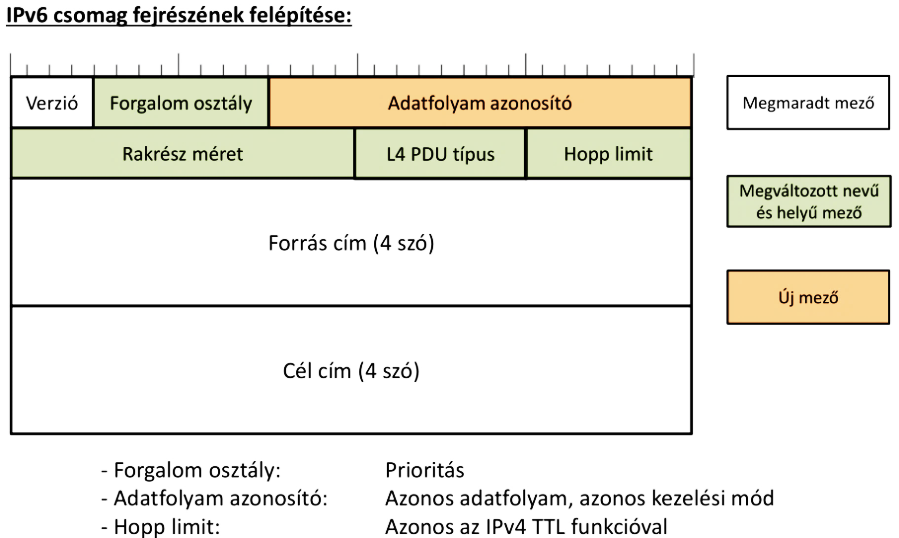
1. Kliens csomópont: helye a lokális hálózat, privát IP címmel.
2. Szerver csomópont: helye a globális hálózat, publikus IP címmel.
3. A belső és külső hálózat közötti NAT-Box L3 és L4 szinteken egyszerre végez címcserét

(NAT overload):

(IPL,PortL) ↔ (IPG, PortG)

1. Képes olyan protokoll számára is címcserét is végezni, amely nem használ port címet (pl. ICMP).
2. Speciális tulajdonság (.): hálózati biztonság funkció.

## Csomag felépítése és címzés IPv6 esetén

Megfontolások:

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

IPv6 tulajdonságok:

1. Címzési tartomány: 128 bit (IPv4-nyi oldalhosszúságú kockarács mindegyik rácspontja egy-egy IPv4 halmaz).
2. Intelligensebb csomagkezelés, mint IPv4 esetén.
3. NAT igényének mellőzése (habár létezik NAT64 is).
4. Egyszerűbb csomagfejrész, nincs hibaellenőrző kód:

Kevesebb számolás.

Gyorsabb útválasztás.

Adatfolyam azonosító mező a csomag fejrészben:

Áramkörök egyszerűbb azonosítása.

IPv4 és IPv6 együttműködés:

Kettős (duális) stack: mindkét protokoll párhuzamosan működik a csomóponton.

Alagút: IPv4 csomagban IPv6.

Címcsere (NAT64): átjárás IPv4 és IPv6 hálózatok között.

IPv6 csomag felépítése:

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

- Három címtípus: nincs üzenetszórás (broadcast).

# IP forgalomirányítás

## Útválasztás és forgalomirányítás osztályok

Routing információ komponensek:

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

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

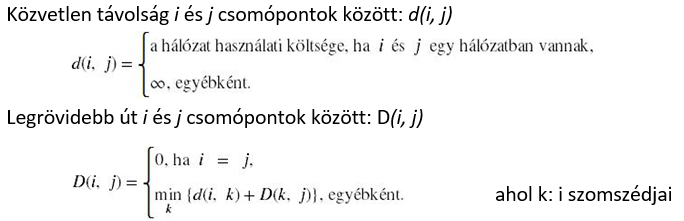
## **Útválasztási kategóriák (az összes világoskék zárójelben)**

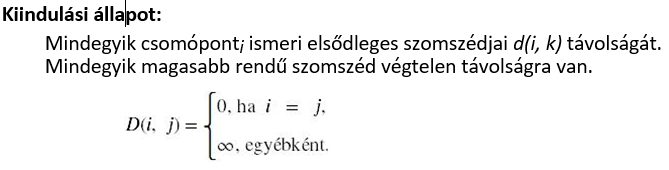
## Távolságvektor alapú forgalomirányítás (DVR)

Működési alapelv:

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

Távolságvektor alapú forgalomirányítás algoritmusa (Bellman-Ford):





Algoritmus lépései:

1. Csomópont*i* mindegyik *k* szomszédjától megkapja a *D(k, j)* értéket.
2. Mindegyik csomópont*k* szomszédtól érkezett *D(k, j)* érték alapján távolság metrika számolás: *Xi,k,j* *:= d(i,k) + D(k, j)*
3. Ha *Xi,k,j* < *D(i, j)*, akkor csomópont*k* előnyösebb úton van, ezért *D(i, j)* := *Xi,k,j*
4. Ciklusidő várakozás, majd folytatás 1. lépésnél.

Az eljárás véges számú lépés után optimális utat szolgáltat a forrás és cél csomópontok között.

**IMPORTANT NOTE HERE: ne kezd el ezeket tanulni, bőven sok a nevüket, azt, hogy távvektor, link vagy vekt-állapot alapúak tudni, meg épp egy félmondatot. Nem lesznek ÍGY feltéve, csak a Vektor-állapot és távolságvektor KATEGÓRIA szerepelt kérdésként.**

## Routing Information Protocol (RIP):

1. Távolságvektor alapú IGP routing protokoll.
2. Régi, de folyamatosan fejlesztik, javítják.
3. Kisméretű hálózatokban használható.
4. Metrika: érintett útválasztók (hop-ok) száma, minden kapcsolat költsége 1.
5. Maximum 15 hop hosszúságú optimális útvonal esetén használható (16 = ∞ távolság).
6. Routing update ciklusidő: 30 s.
7. Szomszédos útválasztó elérhetetlen státusz: ha 6 x 30 s-ig nincs routing update.
8. RIP: csak osztályos hálózatok kezelése, nincs authentikáció.
9. RIPv2 (RFC 1723): CIDR kompatibilis, a szomszédok közötti kommunikációra authentikáció előírható.

## Enhanced Interior Gateway Routing Protocol (EIGRP):

1. Gyártóspecifikus (Cisco Systems) távolságvektor alapú IGP (hibrid) routing protokoll.
2. LAN hálózatokban alkalmazzák.
3. Sokcélú, flexibilis, skálázható, CIDR és VLSM kompatibilis, autentikációt támogat.

Szomszédsági viszonyok kiépítése és fenntartása: update csak tényleges változás esetén és csak a változást terjeszti.

1. Metrika: összetett, öt darab változóból súlyozással számított:
2. Alapértelmezett változók: átviteli ráta [b/s], késleltetés [s].
3. Opcionális változók: terhelés [%], megbízhatóság [%], MTU [B].
4. Megbízható távolság adott hálózathoz (DR): legkisebb metrika érték az adott hálózatig.

## Link-állapot alapú forgalomirányítás (LSR):

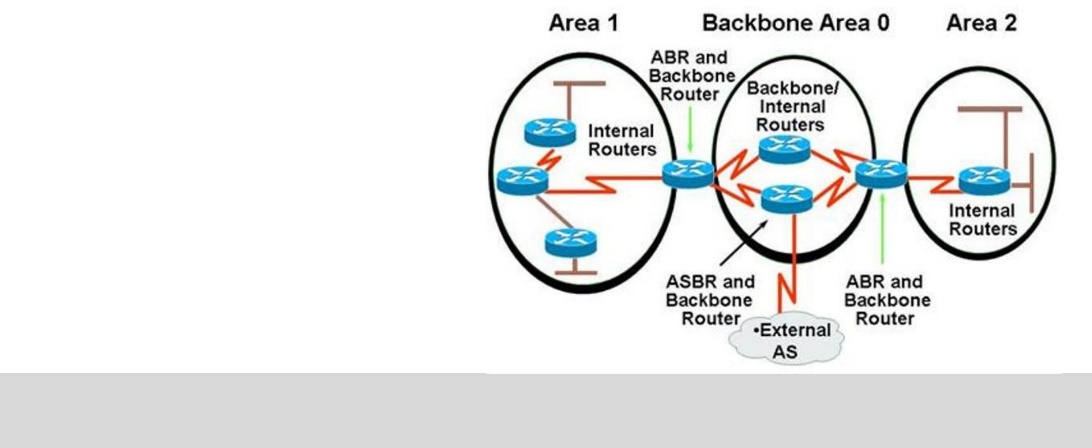
Működési alapelv:

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

Mechanizmus ismételt lépései:

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

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

1. Nyílt szabványú, link-állapot alapú IGP routing protokoll.
2. Működési környezet: tipikusan IP technológia felett.
3. Használat: hierarchikus szervezésű LAN/MAN hálózatokban.
4. Többcélú, flexibilis, skálázható, CIDR és VLSM kompatibilis, autentikációt támogat.
5. Autonóm rendszer (AS): azonos üzemletetési érdekeltségű Area-k halmaza.

Mindegyik OSPF router magának építi fel AS-en belül az SPF (Shortest Path First) fa adatbázist az aggregált link-állapot információk alapján.

Legjobb útvonal meghatározása: Dijkstra algoritmus

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

1. Nyílt szabványú, link-állapot alapú IGP routing protokoll.
2. Működési környezet: tipikusan adatkapcsolati átviteltechnika felett.
3. Használat: nagy ISP gerinchálózatokban (2 hierarchia szint).
4. Sokcélú, flexibilis, skálázható, CIDR és VLSM kompatibilis, autentikációt támogat.
5. Autonóm rendszer (AS): azonos üzemletetési érdekeltségű area-k halmaza.

Routing update: AS útválasztói között a link-állapot információk (LSP) szétküldése elárasztásos módszerrel.

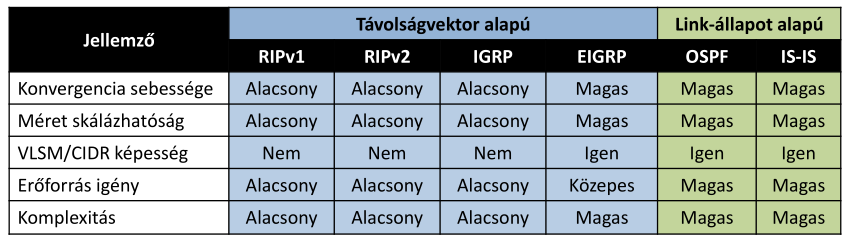
Gerinchálózati Area: L2 útválasztók.

Mindegyik IS-IS router magának építi fel AS-en belül az SPF (Shortest Path First) fa adatbázist az aggregált link-állapot információk alapján.

Legjobb útvonal meghatározása: Dijkstra algoritmus

## AZ összehasonlító táblázat!

CSAK A TÁBLÁZAT KELL. Itt a leírás, hogy minden szempont mit jelent, de nem KELL tudni!

Konvergencia sebesség: topológia és/vagy terhelés változásának követési sebessége.

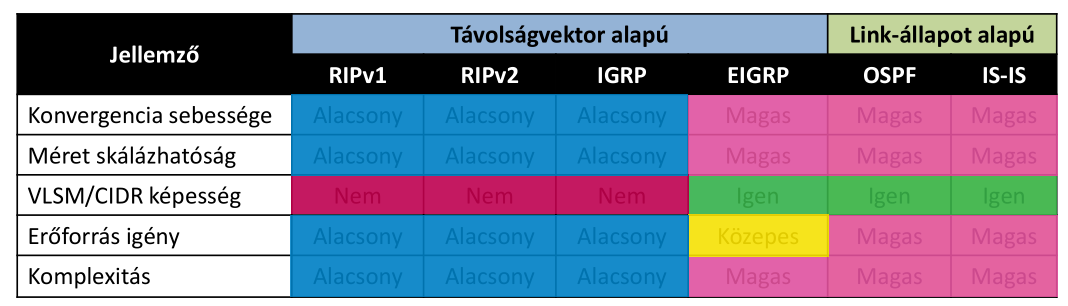
Méret skálázhatóság: router-ek és L3 hálózatok száma.

VLSM/CIDR képesség: IPv4 esetén osztályos/nem osztályos hálózatok hirdetése.

Erőforrás igény: router hardver (RAM, CPU) és átviteli ráta erőforrások.

Komplexitás: beüzemeléshez és üzemeltetéshez szükséges rendszergazdai know-how.

**TIPP, így jegyezd meg:**



## Vektor-Állapot alapú forgalomirányítás (VSR)

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

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

IGP: AS-en belüli routing protokoll.

EGP: különböző AS-ek közötti routing protokoll.

AS: világon egyedi azonosítójú (16 bit), egyetlen adminisztratív tartomány.

ISP: egy vagy több AS üzemeltetése.

BGP fogalmak:

* 1. BGP router: BGP protokollt beszélő útválasztó.
  2. BGP pár / BGP szomszéd: TCP:179 kapcsolatban lévő BGP router pár.
  3. Prefix: alhálózat vagy aggregált hálózat.

BGP router típusok:

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

BGP egyedi routing tulajdonsága:

Routing: útvonalvektor alapján, legelőnyösebb AS útvonal.

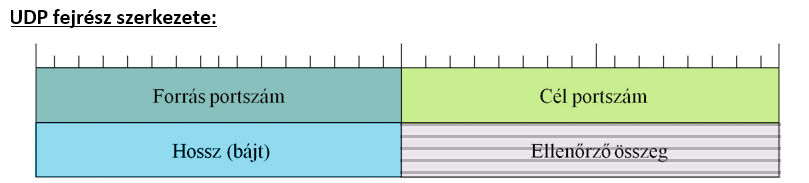
Forgalom átviteli ráta szabályozása link-enként.

Nagyon nagy méretű routing táblákat képes kezelni.

Jól igazodik a VPN (Virtual Private Network) megoldásokhoz (MPLS VPN).

## User Datagram Protocol (UDP, RFC 768):

1. Összeköttetés nélküli (CL) szállítási réteg protokoll.
2. Nem megbízható, nyugta nélküli kapcsolat a szegmens idejére.
3. Hibajavítási funkció: alkalmazás szinten.

Felhasználó alkalmazás jellemzői:

* + 1. Adatvesztés tolerancia.
    2. Átviteli ráta érzékenység.

Funkciók:

* 1. UDP datagram küldése.
  2. UDP datagram fogadása.

1. UDP szegmens: Fejrész + Rakrész.
2. Tipikus alkalmazások: DNS, SNMP, multicast, multimédia kommunikáció.

UDP fejrész:

1. **1. szó:** Forrás portszám (16 bit), Cél portszám (16 bit).
2. **2. szó:** UDP szegmens hossza (16 bit), Fejrész ellenőrző összeg (16 bit).

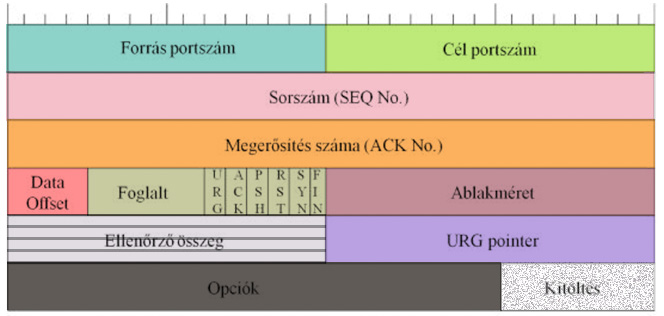
UDP rakrész:

* 1. Tetszőleges tartalom (bármilyen réteg PDU).

Előnyös tűzfalakon továbbított protokollok áthidalására.

Bithiba javítását, illetve egynél több vagy kevesebb példányos kézbesítés kezelését a rakrészben szállított PDU protokolljára bízza.UDP-Lite (RFC 3828): Fejrészben a Hossz mező a csak fejrészre vonatkozik (rakrész hibáit nem érzékeli: előny/hátrány).

## Transmission Control Protocol

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

Fejrész szerkezete

1. **1. szó|szó:** Forrás portszám (16 bit), Cél portszám (16 bit).
2. **2.szó:** Szegmens sorszáma (32 bit):
   * 1. Ha SYN = 0: első bájt sorszáma a szegmensben.
   1. Ha SYN = 1: kezdeti szekvencia szám (ISN) és első adatbájt = ISN + 1.
3. **3.szó:** A partner által várt következő szekvencia szám (32 bit).
4. **4. szó:** Adat offset(4 bit): TCP fejrész szavainak száma.

Fenntartott mező (6 bit): 000000

**Kontroll bitek:**

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

**ACK:** Acknowledgement (a nyugta sorszám értéke érvényes(1) vagy sem (0)). PSH: Push Function (a szegmenst azonnal továbbítani/fogadni kell)

**RST:** Reset (kapcsolat lezárása hiba miatt)

**SYN:** Szekvencia szám (kapcsolat kiépítés, szinkronizálás). FIN: Adat vége a küldőtől (kapcsolat bontás).

Ablakméret (16 bit): nyugtázott bájtok száma.

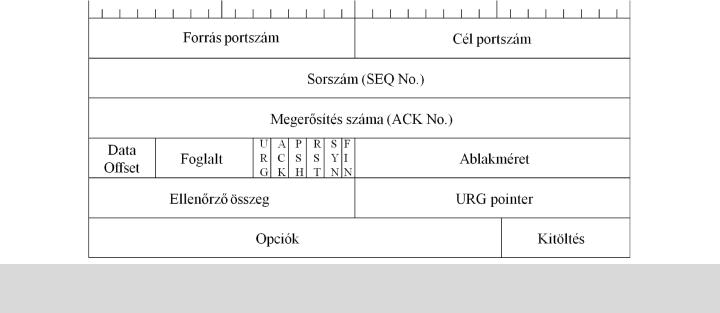
1. **5.szó:** Ellenőrző összeg (16 bit); UrgentPointer (prioritásos adat kezdete,offset-je).
2. **6.szó:** Opciók;Kiegészítés egész szóra.

## 

## **Transmission Control Protocol (TCP)**

**Transmission Control Protocol (TCP, RFC 793):**

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

**TCP fejrész szerkezete:**

**TCP fejrész szerkezete (folyt.):**

1. **szó:** Forrás portszám (16 bit), Cél portszám (16 bit).
2. **szó:** Szegmens sorszáma (32 bit):
   1. Ha SYN = 0: első bájt sorszáma a szegmensben.
   2. Ha SYN = 1: kezdeti szekvencia szám (ISN) és első adatbájt = ISN + 1.
3. **szó:** A partner által várt következő szekvencia szám (32 bit).
4. **szó:** Adat offset(4 bit): TCP fejrész szavainak száma.

Fenntartott mező (6 bit): 000000

Kontroll bitek:

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

ACK: Acknowledgement (a nyugta sorszám értéke érvényes(1) vagy sem (0)). PSH: Push Function (a szegmenst azonnal továbbítani/fogadni kell)

RST: Reset (kapcsolat lezárása hiba miatt)

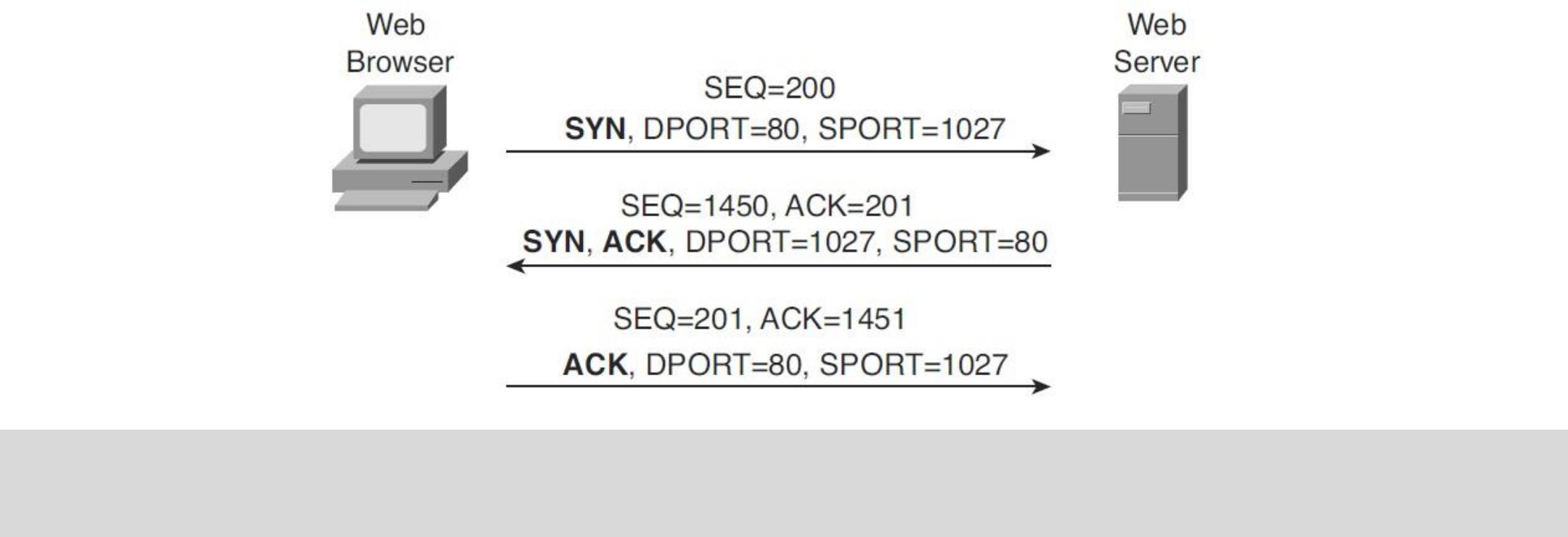
SYN: Szekvencia szám (kapcsolat kiépítés, szinkronizálás). FIN: Adat vége a küldőtől (kapcsolat bontás).

Ablakméret (16 bit): nyugtázott bájtok száma.

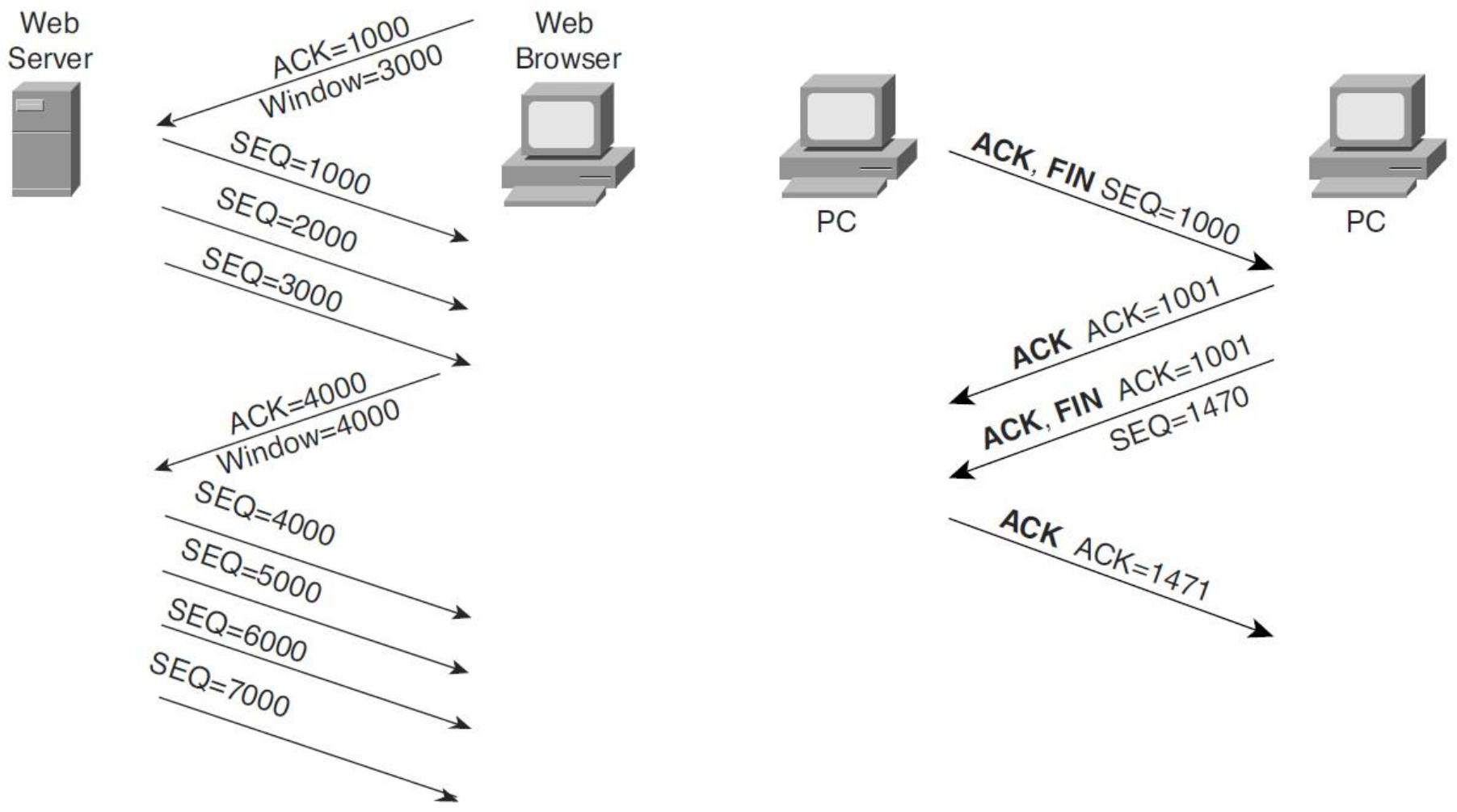
1. **szó:** Ellenőrző összeg (16 bit); UrgentPointer (prioritásos adat kezdete,offset-je).
2. **szó:** Opciók;Kiegészítés egész szóra.
3. **TCP kommunikációs mechanizmusok: Összeköttetés fázisai:**

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

1. Kliens: kapcsolat kiépítésének kezdeményezése:
   1. Portszámok és kezdősorszám beállítása (pl. SEQ\_No = 200); Jelzőbitek: SYN=1, ACK=0.
2. Szerver: jóváhagyó válasz-üzenetet küldése:
   1. Portszámok felcserélése; Saját kezdősorszám beállítása (pl. SEQ\_No = 1450).
   2. Nyugta sorszám beállítása: kapott SEQ érték+1 (pl. ACK\_No = 201). SYN = 1; ACK = 1.
3. Kliens: jóváhagyás küldése:
   1. Portszámok felcserélése; Saját szegmens-sorszám beállítása (pl. SEQ\_No = 201).
   2. Nyugta sorszám beállítása: kapott SEQ érték+1 (pl. ACK\_No = 1451); SYN = 0; ACK = 1.



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

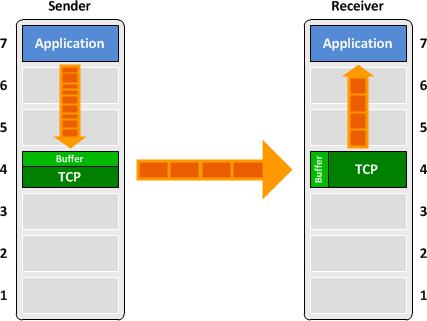
****

**Adatátvitel (Transfer) fázis** **Lebontás (Release) fázis**

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

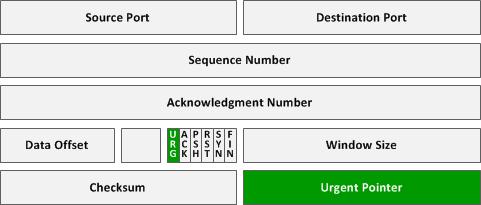
1. **TCP kommunikációs mechanizmusok: Rövid szegmens küldése (Push):**
2. Tartalom küldése és fogadása: pufferek segítségével.
3. Küldő puffer: küldésre várakozó, vagy elküldött és még nem nyugtázott szegmens.
4. Fogadó puffer: fogadott és még nem továbbított szegmens felsőbb rétegnek.
5. MSS (Maximum Segment Size) méretet meghaladó tartalom: várakozás a pufferben.
6. Szegmens generálás feltétele küldőnél: alkalmazás szintű adatbájtból minimális

|  |  |  |
| --- | --- | --- |
| darabszámú bájt létezzen. | **Küldő** | **Fogadó** |
| - PSH = 1: aktuális szegmens |  |  |
| küldése/fogadása azonnal, mérettől |  |  |
| függetlenül, puffer nélkül. |  |  |



## - Pl.: Internet böngészésnél HTTP GET parancs elküldése; Valósidejű forgalom segítése

1. **TCP kommunikációs mechanizmusok: Sürgős adat küldése (Urgent Data):**
2. Szegmensek alapértelmezés szerinti küldési sorrendje: növekvő SEQ\_No alapján.
3. Szegmensek sorrendjének küldése prioritás alapján: URG\_Pointer alapján.
4. URG Pointer érték felhasználása: prioritásos adat első bájtjának címe (offset).



- Pl.: Telnet program paraméterei (méret, kódolás) módosításának küldése szerverhez

1. **TCP kommunikációs mechanizmusok: TCP teljesítmény szabályozása kapcsolat közben:**
2. Lehetséges torlódási helyek:
   1. Hálózaton belül (router, vonal)
   2. Fogadó csomópont
3. **Hálózati torlódás szabályozás:**
   1. Congestion control küldőnél
   2. Torlódási ablak: max. 64 kB.
   3. Torlódási „Ablakméret”-nyi adatbájt fogadása után adatküldő felé kötelező a nyugta-válasz.

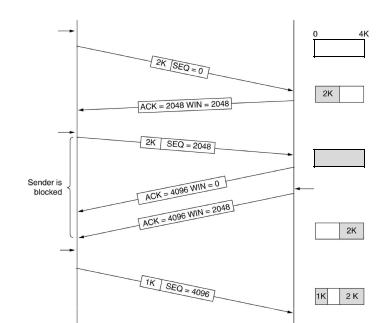
**Küldő**

Alkalmazás ír 2 kB-ot

Alkalmazás ír 2 kB-ot

|  |
| --- |
| Küldő |
| feltartóztatva  Alkalmazás  írhat max  2kb-ot. |

**Fogadó** Fogadó

puffere

Üres

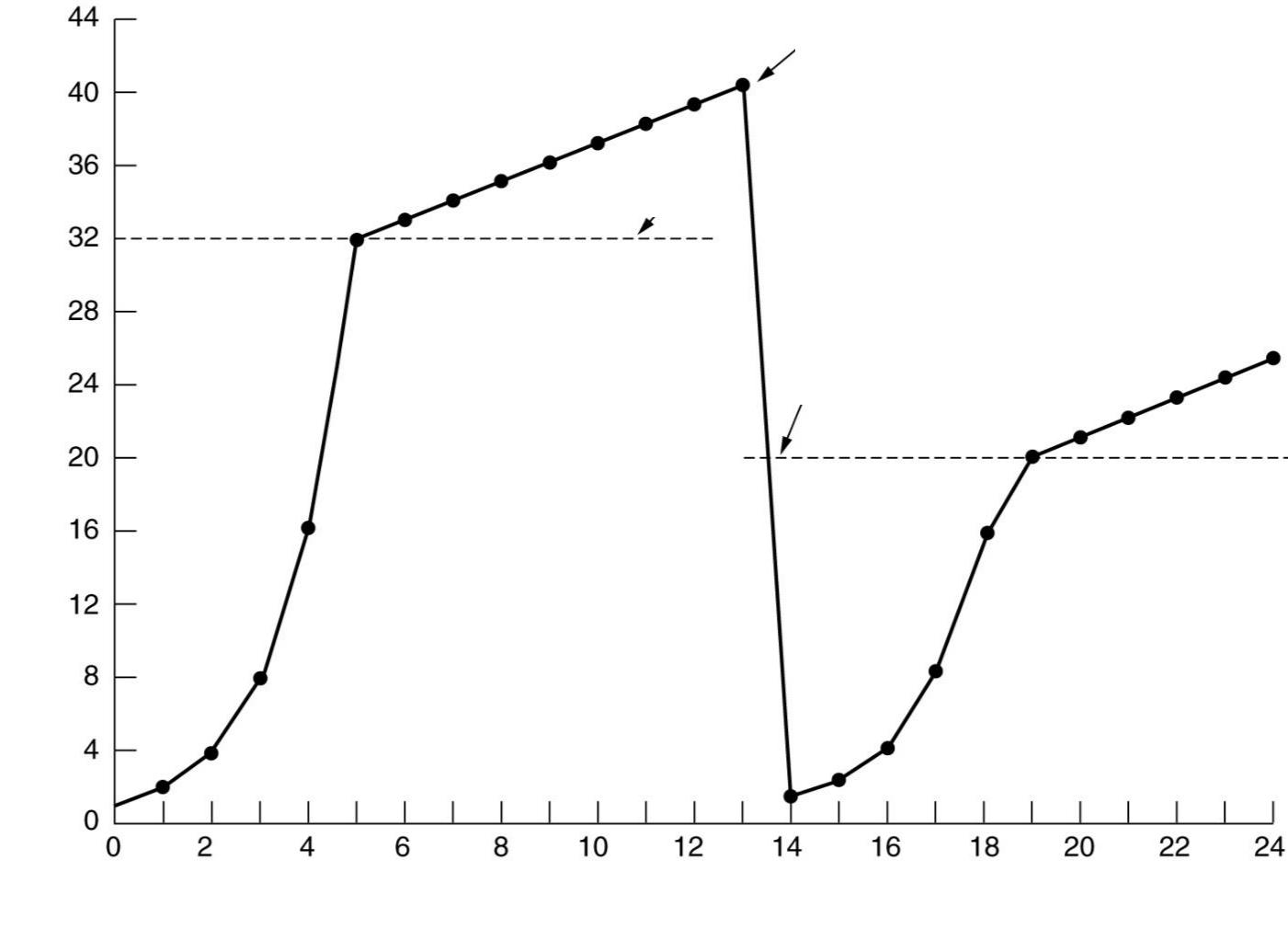
Tele

|  |  |
| --- | --- |
|  |  |
| **4.2. Adatfolyam szabályozás:** |  |
|  |
|  |

1. Flow control fogadónál
2. Adatfolyam ablak (puffer): max. 1 GB.

- Pl.: Web böngészés (kliens – szerver).

1. **TCP kommunikációs mechanizmusok: TCP teljesítmény szabályozás kapcsolat elején:**
2. Forgalom indítása kis átviteli rátával
3. Ablakméret lassú növelése (slow starting)
4. Implementációk:
   1. Tahoe,
   2. Reno,
   3. Vegas,
   4. Westwood,
   5. Cubic (BIC),[kB]
   6. stb.abla



Időtúllépés

Küszöb

Küszöb

Küldési szám

1. **TCP kommunikációs mechanizmusok: Forgalom elakadás kijavítása, kezelése:**
2. Kapcsolatot befolyásoló tényezők:
   1. Időtartamok
      1. Újraküldési időkorlát (RTO – Retransmission Timeout
      2. Körbeforgási idő (RTT – Round Trip Time)
   2. Szegmens bithiba

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Fogadó stratégiája** | |  |  |
| **TCP\_Crash Recovery** | |  | | |  | | |
| **Előbb ACK, utána írás** | | | **Előbb írás, utána ACK** | | |
|  |  |  |  |  |  |  |  |
|  |  | **AC(W)** | **AWC** | **C(AW)** | **C(WA)** | **WAC** | **WC(A)** |
|  |  |  |  |  |  |  |  |
| **stratégiája** | **Mindig újraküld** | OK | Duplum | OK | OK | Duplum | Duplum |
|  |  |  |  |  |  |  |
| **Soha nem küld újra** | Adatvesztés | OK | Adatvesztés | Adatvesztés | OK | OK |
|  |  |  |  |  |  |  |
| **Újraküld S0-ban** | OK | Duplum | Adatvesztés | Adatvesztés | Duplum | OK |
| **Küldő** |
|  |  |  |  |  |  |  |
| **Újraküld S1-ben** | Adatvesztés | OK | OK | OK | OK | Duplum |
|  |
|  |  |  |  |  |  |  |  |

## TCP VS UDP táblázat, TCP VS UDP összehasonítás

