Hálózati Architektúrák és Protokollok
GI BSc

Kocsis Gergely
Debreceni Egyetem - Informatikai Kar
Informatikai Rendszerek és Hálózatok Tanszék
2017

Információk

Kocsis Gergely
http://irh.inf.unideb.hu/user/kocsisg

2 zh – mindkettő külön javítható

A zh sikeres, ha az elért eredmény legalább 50%

Követelmény: Legalább 2 sikeres zh
+ a két zh átlaga nagyobb vagy egyenlő, mint 66%

Információk

Maximálisan megengedett hiányzások száma: 3 alkalom

Maximálisan megengedett késés óráról: 20 perc

20 perc késés után a megjelenés engedélyezett, de hiányzásnak minősül

Zh-ról történő igazolatlan hiányzás esetén a zh eredménye 0%

Különösen indokolt esetben, egyéni elbírálás alapján, a zh előtt legalább egy héttel jelezve a zh-t lehetőség van az órán megbeszélttől más időpontban megírni

Információk

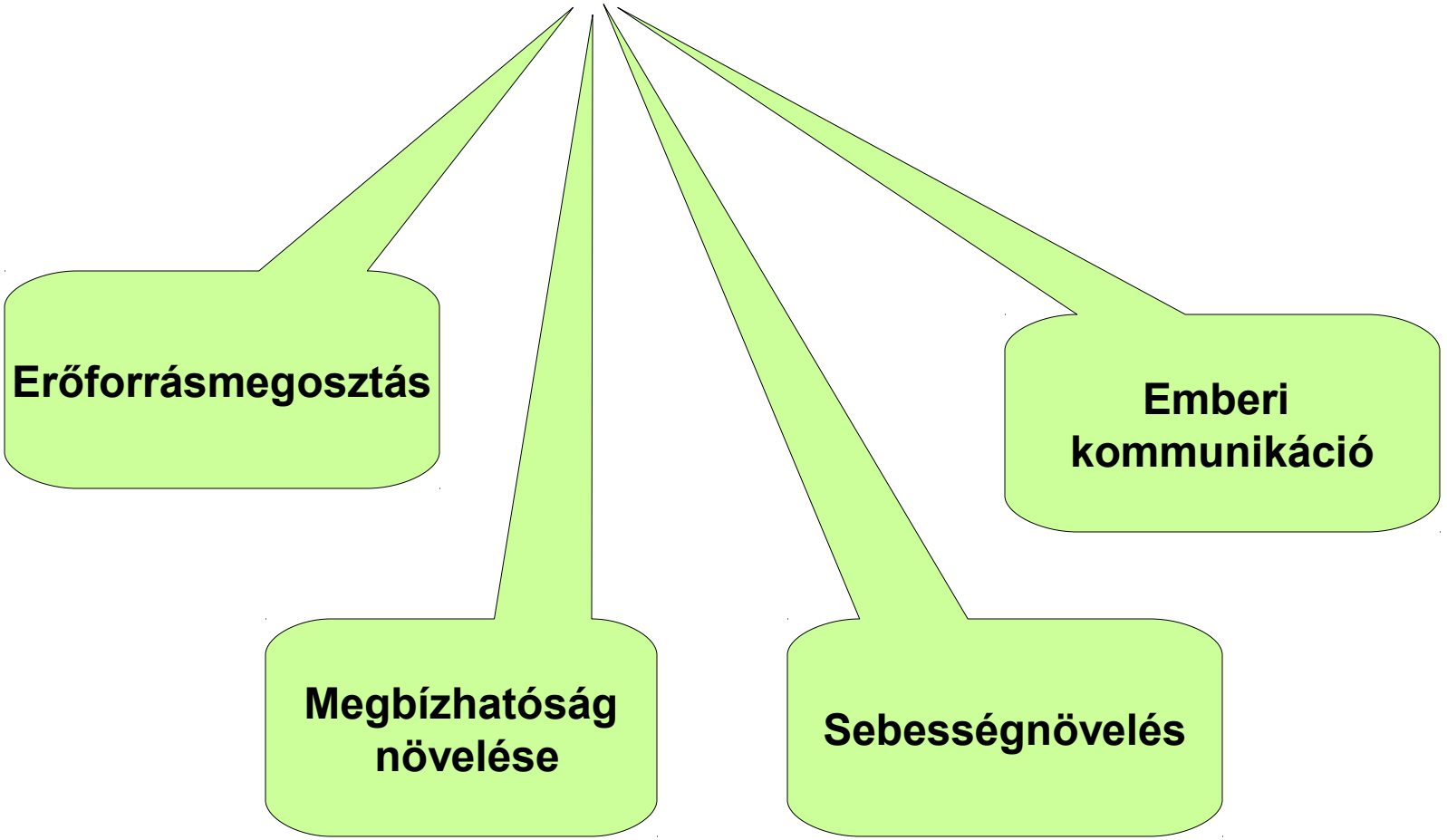
A diasor elkészítéséhez használt és egyben ajánlott irodalom:

- James F. Kurose and Keith W. Ross. Számítógép hálózatok működése: Alkalmazásorientált megközelítés. 4. ed. Pearson Education, 2008, Panem Könyvkiadó 2009.
- Almási Béla, Számítógép Hálózatok oktatási segédlet, Debreceni Egyetem Informatikai Kar, 2011
- Végh János, Hálózati architektúrák és protokollok előadási segédlet, Debreceni Egyetem Informatikai Kar, 2014

Mi az a hálózat?

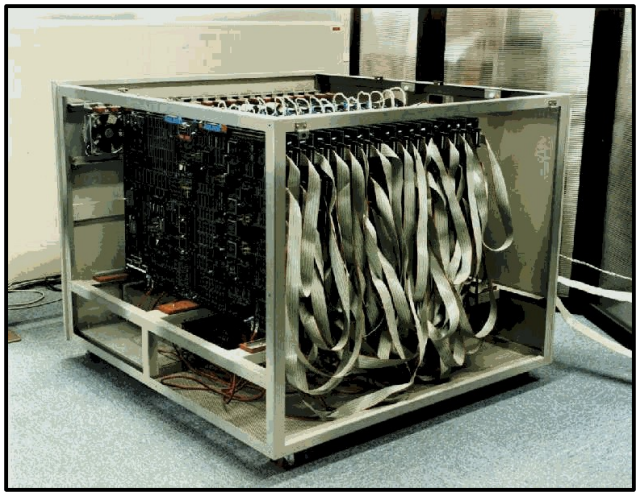
Számítógép hálózat

Számítógép hálózat: Számítógéprendszerek valamilyen információátvitellel megvalósítható **célért** történő összekapcsolása



Csoportosítás méret szerint

~1m → multicomputer



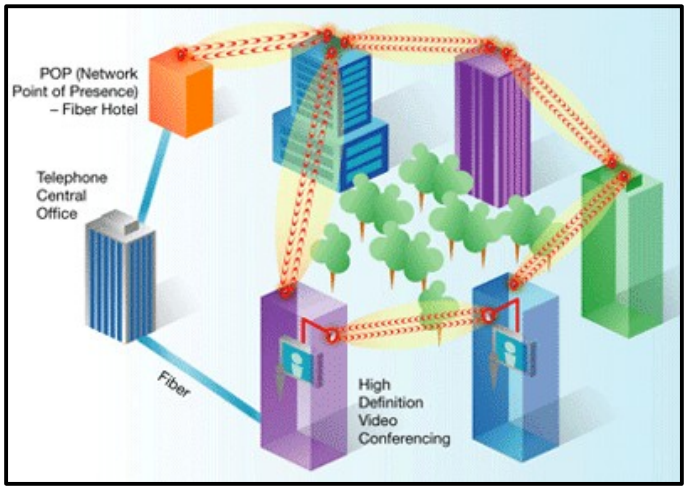
http://aquila.is.utsunomiya-u.ac.jp/~baba/webEnglish.html

~1km → helyi hálózat, LAN

http://blog.triplepointpr.com/wp-content/uploads/2012/03/gaming-huge-lan-party.jpg

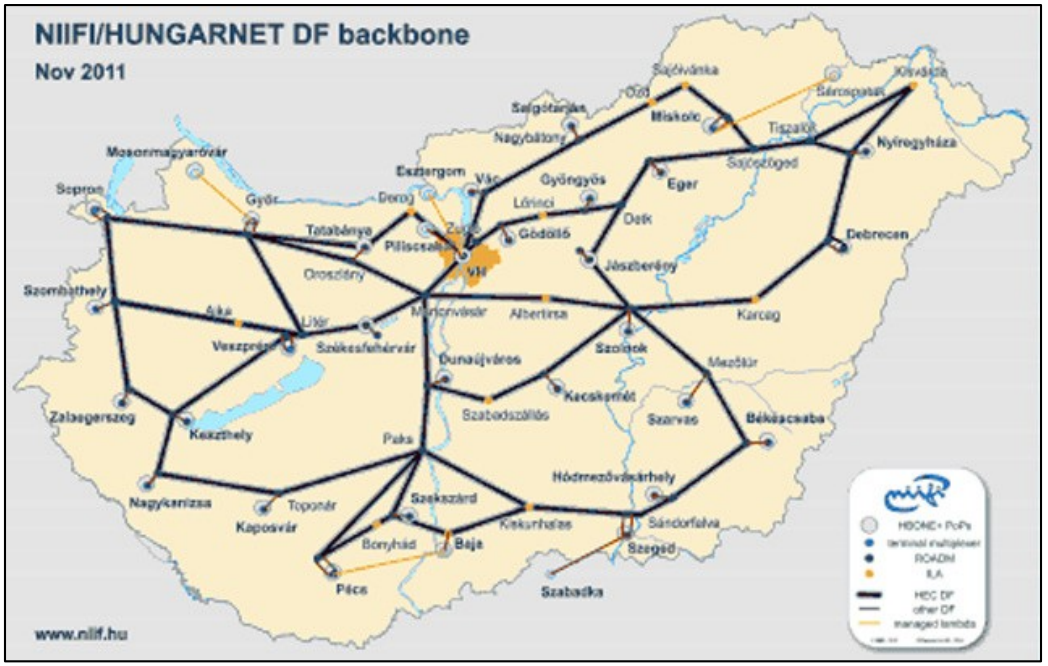
Csoportosítás méret szerint

~10km → városi hálózat, MAN



http://scorea-ict.blogspot.hu/p/computer-networks-f4cd5-and.html

~100+km → nagy kiterjedésű hálózat, WAN



Csoportosítás méret szerint

Kiterjedés	Megnevezés
<1m	Multicomputer
1 km	Helyi hálózat (Local Area Network)
10 km	Városi hálózat (Metropolitan AN)
100 km <	Nagy kiterjedésű hálózat (Wide AN)

Egyéb hálózati kategóriák

(Wireless) Personal Area Network – Személyi hálózatok (W)PAN

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

Csoportosítás méret szerint

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

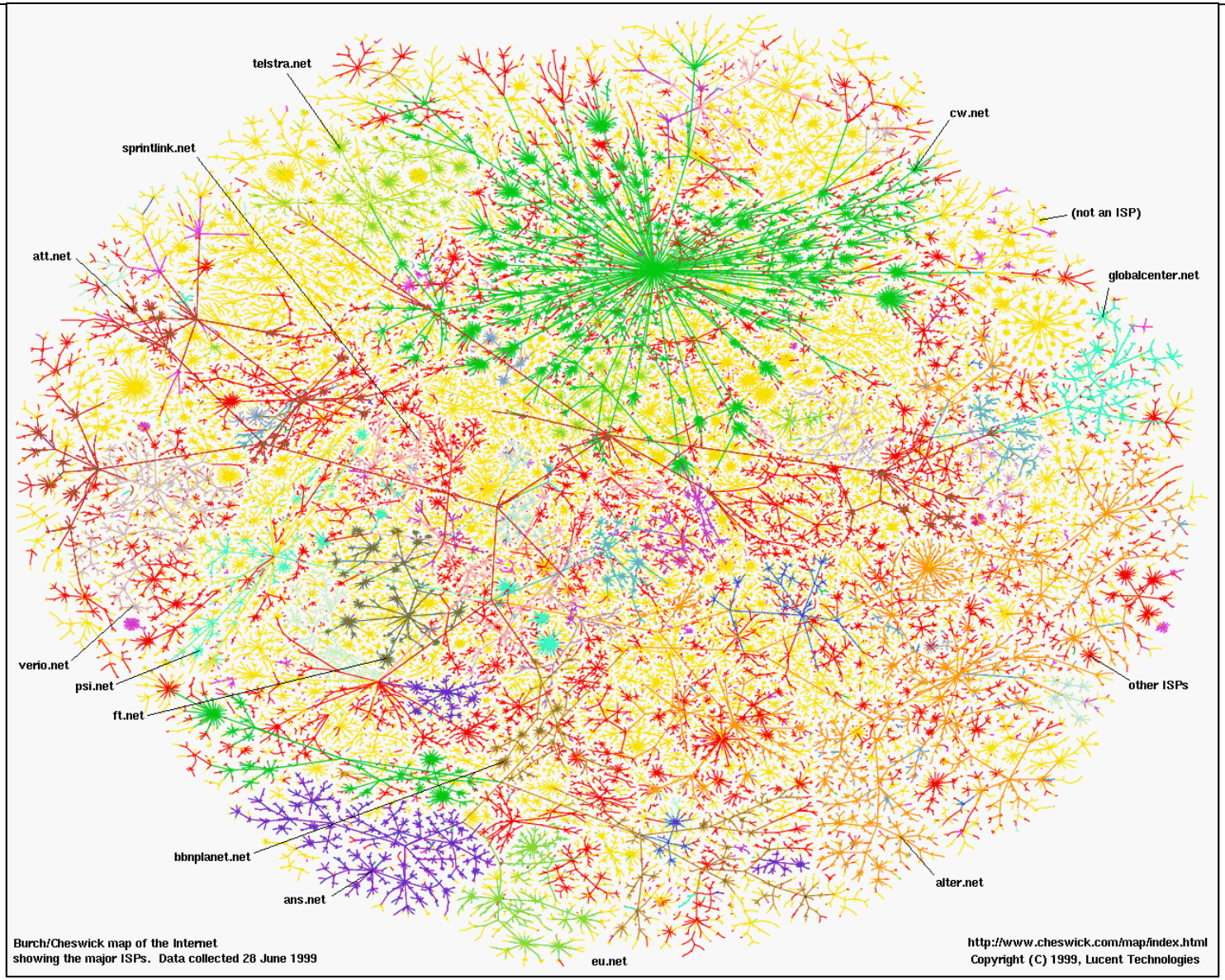
LAN eszközök

- Számítógépek
- Hálózati kártyák
- Perifériás készülékek
- Hálózati átviteli közeg
- Hálózati készülékek

WAN feladatok

- Nagy földrajzi terület lefedése
- (Valós idejű) kommunikáció biztosítása a felhasználók között
- Nonstop hozzáférés a helyi szolgáltatásokhoz csatlakoztatott távoli erőforrásokhoz
- Elektronikus levelezési, internetes, fájlátviteli és e-kereskedelmi szolgáltatások biztosítása

Internet



http://www.cheswick.com/ches/map/gallery/isp-ss.gif

Hogy épül fel az Internet?

Internet

Felépítése: végrendszerek és a köztük lévő információszállítási infrastruktúra, illetve elosztott alkalmazási platform.

Végrendszerek (end systems)

Végrendszer

(magasabb szinten): **hoszt** (gazda) a hálózati alkalmazásoknak helyet adó hálózati egység

Csomópont (alacsonyabb szinten):

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

Szerver-kliens architektúra

Kliens-szerver modell: A hálózati alkalmazások legelterjedtebb modellje.

- **Szerver:** Olyan hálózati csomópont (és szoftver), mely más csomópontok számára valamilyen szolgáltatást nyújt, biztosít. A szerver szolgáltatását valamilyen szerver-szoftver (pl. web-szerver) biztosítja.

  Kliens: Olyan hálózati csomópont (és szoftver), mely a hálózaton valamilyen szolgáltatás használati igényével jelentkezik. A szolgáltatás igénybevételéhez valamilyen kliens szoftvert (pl. web-böngésző) használ.

  A szerver és a kliens kommunikációs együttműködését egy magas szintű protokoll (pl. http) írja le.

Hozzáférési hálózatok

Az a fizikai, vagy adatkapcsolat, mely a végrendszert a hálózat szélén lévő útvonalválasztóhoz csatolja

Otthoni hozzáférés

Vállalati hozzáférés

Vezeték nélküli hozzáférés

Hálózati hozzáférés modem 56kb/s, lefoglalja a telefonvonalat, lassú, már meglévő telefonvonalon működik

DSL (Digital Subscriber Line): Telefontársaságok szolgáltatják a már meglévő vezetéken. FDM (frekvenciaosztásos multiplexelés)

HFC (hybrid fiber-coaxial cable): jellemzően a kábeltv hálózat kiterjesztése. Osztott adatszóró közeg, TDM (időosztásos multiplexelés)

Jellemzően helyi alhálózatokat alakítanak ki csillag topológiával, melyet egészében kapcsolnak az útvonalválasztóhoz. Debrecen FDDI - Fiber Distributed Data Interface

Jellemzően két fajtája van: WiFi, mobilinternet 3G, 4G

Internet szolgáltatók és gerinchálózatok

Az Internet hierarchikus felépítésű. Hálózatok hálózata.

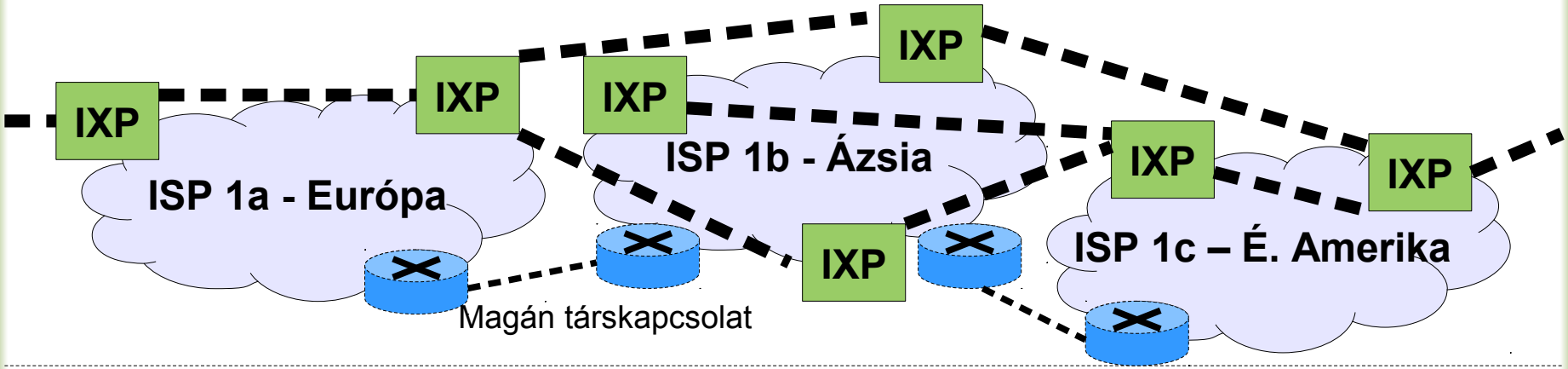
1. rétegű szolgáltatók (Tier 1 ISP): Internet szolgáltató óriásszervezetek, melyek magán társkapcsolaton (*private peering*) keresztül kapcsolódnak egymás gerinchálóihoz, így létrehozva az internet gerinchálózatát.

POP (Point of Presence): A szolgáltatók szolgáltatási pontjai:
IXP (Internet Exchange Point): Internet csatlakozási pont
NAP (Network Access Point): Hálózatelérési pont

A szolgáltatók szolgáltatási pontjaikon (POP) keresztül csatlakoznak egy IXP-hez (vagy NAP-hoz)

Az internet gerince így tulajdonképpen óriásszervezetek gerinchálózatainak csoportja, melyeket IXP-n keresztül magán társkapcsolat közt össze.

Internet szolgáltatók és gerinchálózatok



Internet szolgáltatók és gerinchálózatok

Az Internet hierarchikus felépítésű. Hálózatok hálózata.

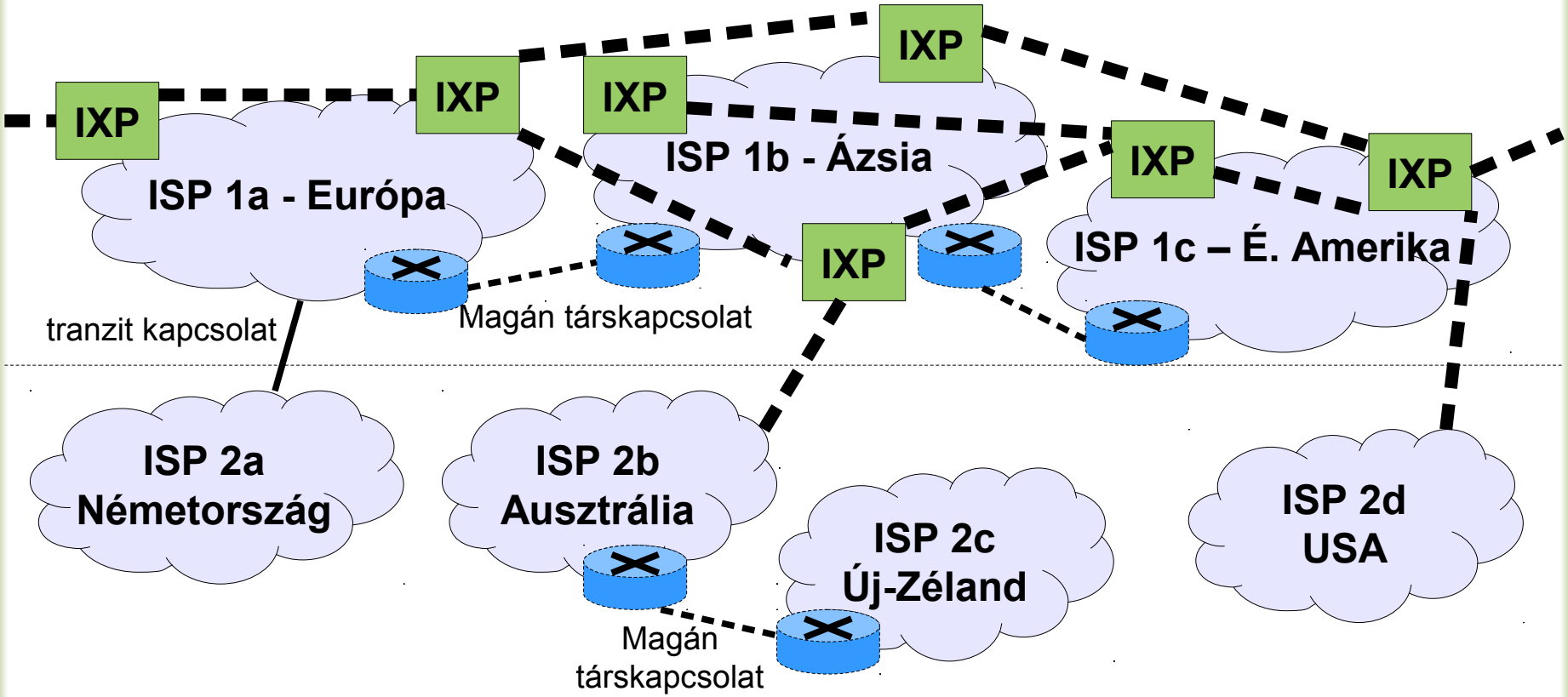
2. rétegű szolgáltatók (Tier 2 ISP): Ezek lehetnek nagyon nagyok is (akár több országon átnyúló hálózattal, de ez a ritkább eset. Különböző megoldásokat használva nyújthatják szolgáltatásaikat:

Egy 2. rétegű ISP

- Fizethet egy első rétegű ISP-nek, hogy rajta keresztül elérje az Internet gerincét és így a világot (tranzit szolgáltatás).
- Egy IXP-n keresztül maga férhet hozzá a világhoz.
- Magán kapcsolattal csatlakozhat egy másik 2. rétegű ISP-hez és rajta keresztül érheti el a világot.

3. rétegű szolgltató (Tier 3 ISP): Ezek vannak a gerinctől a legtávolabb, jellemzően egy-egy városban szolgáltatnak elérést a felhasználóknak. Fizetnek egy Tier 1, vagy egy Tier 2 ISP-nek az elérésért.

Internet szolgáltatók és gerinchálózatok



Internet szolgáltatók és gerinchálózatok

Az Internet hierarchikus felépítésű. Hálózatok hálózata.

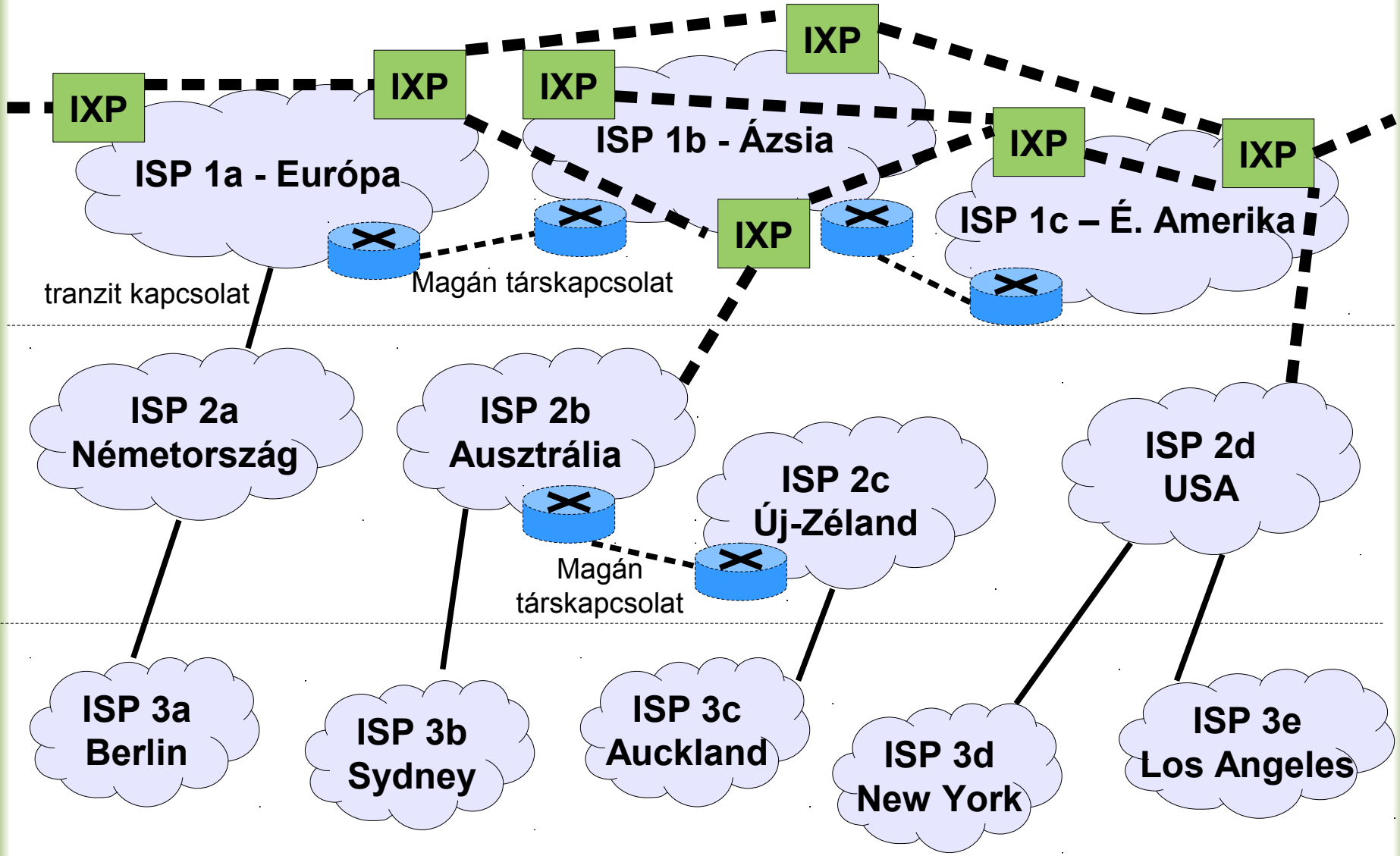
2. rétegű szolgáltatók (Tier 2 ISP): Ezek lehetnek nagyon nagyok is (akár több országon átnyúló hálózattal, de ez a ritkább eset. Különböző megoldásokat használva nyújthatják szolgáltatásaikat:

Egy 2. rétegű ISP

- Fizethet egy első rétegű ISP-nek, hogy rajta keresztül elérje az Internet gerincét és így a világot (tranzit szolgáltatás).
- Egy IXP-n keresztül maga férhet hozzá a világhoz.
- Magán kapcsolattal csatlakozhat egy másik 2. rétegű ISP-hez és rajta keresztül érheti el a világot.

3. rétegű szolgltató (Tier 3 ISP): Ezek vannak a gerinctől a legtávolabb, jellemzően egy-egy városban szolgáltatnak elérést a felhasználóknak. Fizetnek egy Tier 1, vagy egy Tier 2 ISP-nek az elérésért.

Internet szolgáltatók és gerinchálózatok



Internet szolgáltatók és gerinchálózatok

Tier 1 ISP-k például: AT&T, Deutsche Telekom, Level 3 communications
továbbiak listája elérhető a wikipedián)

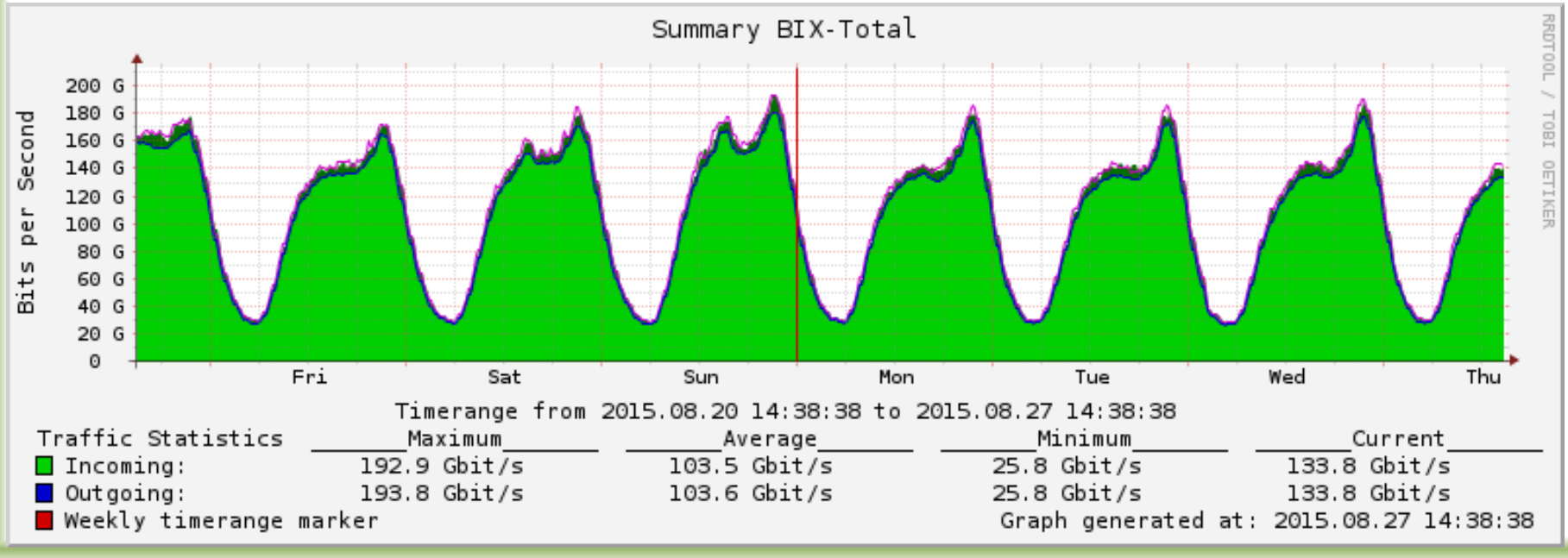
Alsóbb szolgáltatók: pl: Hungarnet, Digi, UPC, Magyar Telekom
továbbiak lekérdezhetők: http://www.whoismyisp.org/)

IXP példa: BIX (Budapest Internet Exchange – http://www.bix.hu/)

Az egyetlen magyarországi IXP (https://www.peeringdb.com 2016)

Összesen 37 taggal rendelkezik (2016) beleértve a fenti példákat is.

A magyar internet forgalom legnagyobb része áthalad rajta.



Hogyan kommunikálunk a hálózatokon?

Csomagkapcsolás ⟷ vonalkapcsolás

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).

Csomagkapcsolás ⟷ vonalkapcsolás

Csomagkapcsolás:

Vonalkapcsolás:

Az internet csomagkapcsolt

Képek forrása: https://blog.openttdcoop.org, http://www.nyugatijelen.com/pictures/xbigs/30160.jpg

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).

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).

Képek forrása: http://tilos.hu/,, http://www.jatekshop.eu/, http://einclusion.hu/

Jel, jelkódolás, moduláció

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

Jelkódolás: A (**digitális**) információ leképezése (**digitális**) vivőjelre (pl. feszültségszintekre, feszültségszint váltásokra).

Moduláció: A (**digitális**) információ leképezése (**analóg**) vivőjelre. A csatornába kerülő (modulált) jel előállítása a forrásból érkező moduláló-jelből és az analóg vivőjelből. Inverz folyamata a demoduláció.
A modem a modulációt és demodulációt végző berendezés.

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 az adatátviteli közegen több csatornát (adatutat) építenek ki.

Ütközés:

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

Adatátviteli sebesség

Adatátviteli sebesség
(hálózati sebesség, sávszélesség, bit ráta):

- Időegység alatt átvitt információ mennyisége. Mértékegysége a bit/másodperc, b/s, bps.
- Az applikációkban mérhető átbocsátó képesség (throughput) mindig alacsonyabb a fizikai átvitel sávszélességénél (bandwidth).

- Nagyobb mértékegységek:

  1 Kbps = 1000 bps

  1 Mbps = 1000 Kbps = 1.000.000 bps

  1 Gbps = 1000 Mbps = 1.000.000.000 bps

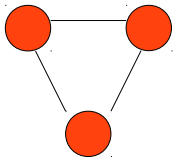
SI szabvány mértékegységek: Babák György, Méréstechnika II. fejezet, Szent István Egyetem, (2011)
http://www.tankonyvtar.hu/hu/tartalom/tamop412A/2010-0019_Merestechnika/pr03.html
u.l. 2016.08.

Internettörténet három dián.

Internettörténet

1961-1972: A csomagkapcsolás kifejlesztése

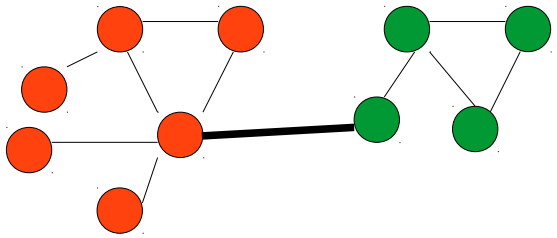
- Leonard Kleinrock – MIT 1964: A csomagkapcsolás előnye a vonalkapcsolással szemben nem kiegyensúlyozott, ún. Löketszerű forgalom esetén.
- Paul Baran – Rand Institute: A csomagkapcsolás használata katonai hálózatokon hangátvitelre.
- Donald Davies és Robert Scantlebury – National Physical Laboratory (NPL): További vélemények a csomagkapcsolásról
- Lawrence Roberts – ARPA (Advenced research Projects Agency): 1967 ARPAnet. 3 csomóponttal indult, majd 1972-re 15 csomópont.



Internettörténet

1972-1980: Egyedi hálózatok és ezek összekapcsolása

- A '70-es évek közepére több kisebb hálózat jelent meg:
  - ALOHANET Hawaii szigeteken működő csomóppontok közötti mikrohullámú hálózat + DARPA (Defense ARPA) műhold
  - Telnet: kereskedelmi csomagkapcsolt hálózat
  - Cyclades: Francia csomagkapcsolt hálózat
  - IBM SNA (System Networks Architecture)
- Vinton Cerf és Robert Kahn – DARPA 1974: Hálózatok összekapcsolása. TCP, UDP, IP



Internettörténet

1980-1990: Hálózatok gyors fejlődése

- '70-es évek vége ARPAnet ~200 csomópont
- '80-as évek vége Internet ~100.000 csomópont
- 1983. január 1. TCP/IP bevezetése
- 1982. DNS leírása, majd 1984 első linux implementáció

1990-: Az Internet rohamos elterjedése

- Megszűnik az ARPAnet
- WWW megjelenése Tim-Berners Lee
- 1992-re kb 200 webszerver működik
- Grafikus böngészők megjelenése és harca
- 1995-2000/2001 “dotcom lufi”: meggondolatlan befektetések akár kockázati tőkebefektetői szinten is. A lufi kidurranásakor több ezer cég ment tönkre, de a túlélők ma óriásira nőttek (Google, Amazon)
- Új technológiák megjelenése (P2P megosztás, stream)
- Internet of Things

Mik azok a protokoll rétegek?

Protokoll

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

Egy protokoll meghatározza a két, vagy több kommunikáló entitás között átadott adatok formátumát és sorrendjét, valamint az üzenetek küldésekor és/vagy fogadásakor vagy más esemény bekövetkezésekor megtett lépéseket.

Röviden a protokoll egy szabály/szabály rendszer.

Request For Comments – RFC

RFC: Az internetszabványokat az Internet Engineering Tast Force (IETF) fejleszti. A IETF szabvány dokumentumait RFC-k (Request For Comments) tartalmazzák.

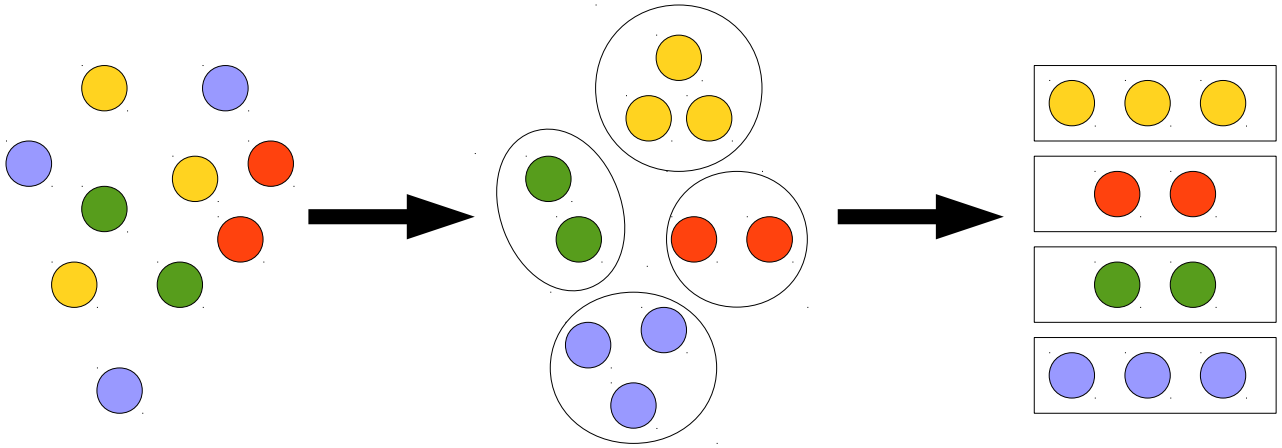
Az RFC-k kezdetben ténylegesen “hozzászólás-kérések” voltak, innen a név. Céljuk, hogy olyan hálózat-, és protokolltervezési problémákat oldajanak meg, amelyek az Internet elődjénél felmerültek. Jelenleg kb a 7900-as RFC sorszámnál tartunk (http://www.rfc-editor.org/rfc-index2.html 2016.08.30.).

Az IETF-en kívül más testületek is foglalkoznak szabványok specifikációjával. Pl.: IEEE 802 LAN/WAN Standards Committee – Ethernet és vezetéknélküli szabványok.

Rétegelt architektúra

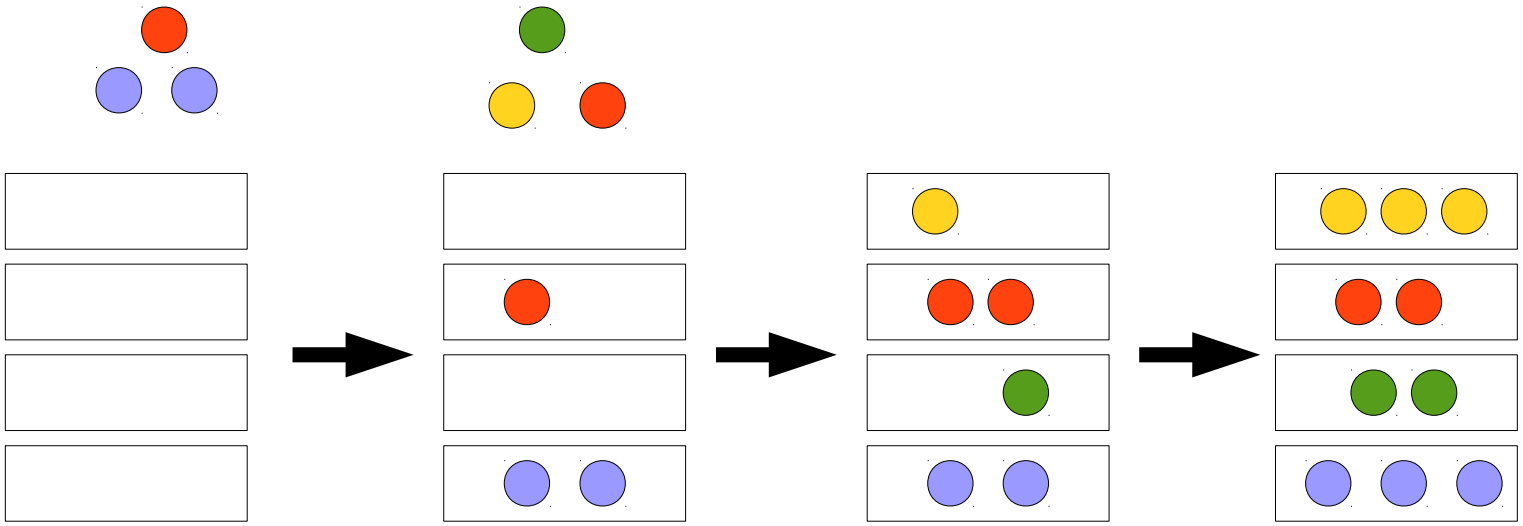
- A protokollok az általuk leírt funkciók szerint csoportokba foglalhatók.
- Ezek a jól definiált csoportok egymással kapcsolatban állnak.
- A csoportok a fizikai világtól való távolság (az absztrakciós szint) szerint egymásnak alá és fölé rendelhetők.

Az így kialakult csoportokat **protokoll réteg**nek hívjuk. A rétegek száma és mérete többféleképpen megválasztható. Egy bizonyos szempont szerint kialakított rétegstruktúrát hívunk **protokoll rétegmodell**nek.



Rétegelt architektúra

A gyakorlatban természetesen a rétegmodellek nem a meglévő prtokollok rendszerezésével jönnek létre, hanem először adnak egy jól használható keretet, amelybe a későbbi protokollokat el lehet helyezni.



Rétegelt architektúra

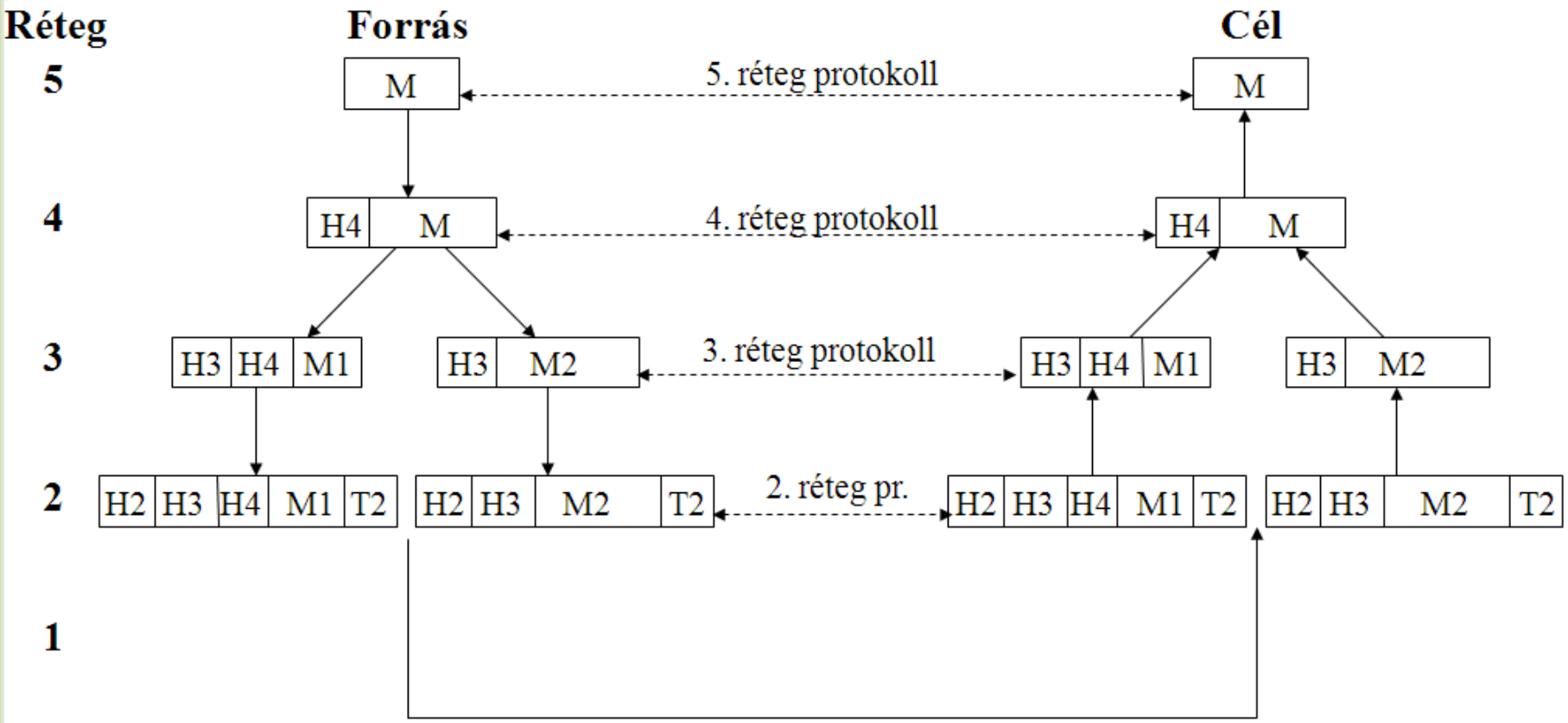
N. réteg protokoll: Az N. réteg (szint) specifikációját leíró protokoll.

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).

Adattovábbítás rétegelt architektúrában

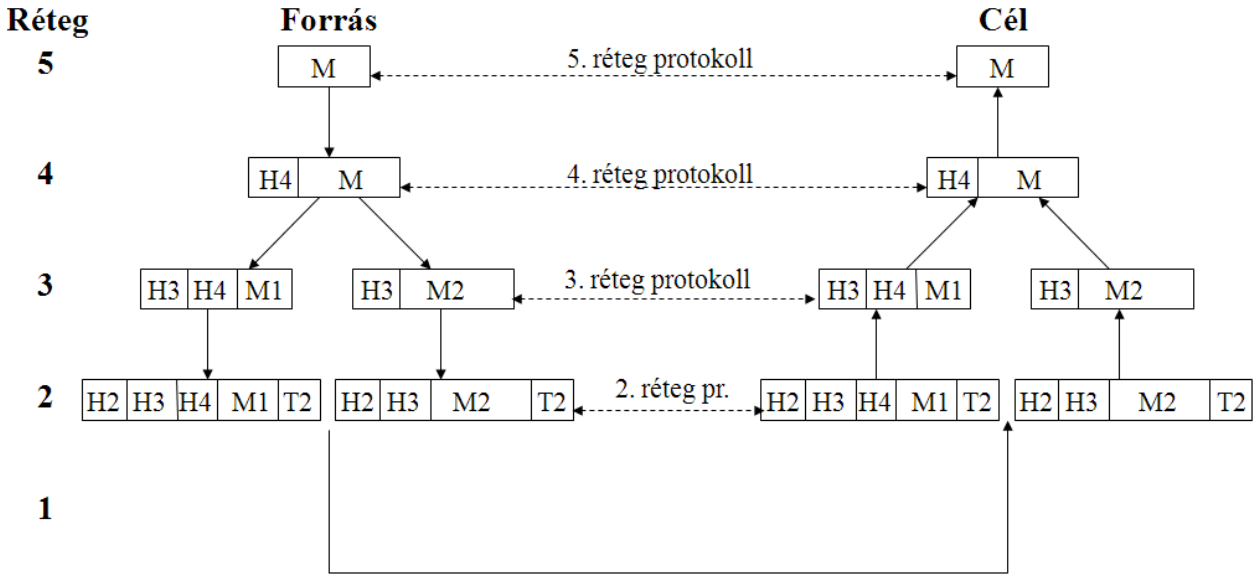


M: Message – üzenet
H: Header – fejléc
T: Tail – lábléc

Adattovábbítás rétegelt architektúrában

A rétegek igénybe veszik az alattuk levő réteg szolgáltatását és szolgáltatást nyújtanak a felettük levő rétegnek (ezt hívják **függőleges avagy fizikai kommunikáció**nak).

A két protokoll oszlop megfelelő rétegei tulajdonképpen egymással váltanak üzenetet (ezt hívják **vízszintes vagy logikai kommunikáció**nak), bár technikailag
az üzenet az összes alattuk levő rétegen keresztül halad



M: Message – üzenet
H: Header – fejléc
T: Tail – lábléc

Az ISO/OSI modell

ISO/OSI: A nemzetközi szabványügyi hivatal (*International Organization for Standardization*) által elfogadott hét rétegű (*nyílt rendszerek összekapcsolási, Open System Interconnection*) modellje.

Sorszám	Réteg neve
7	Alkalmazási réteg (Application layer, Applikációs réteg)
6	Megjelenítési réteg (Presentation layer, Prezentációs réteg)
5	Viszony réteg (Session layer)
4	Szállítási réteg (Transport layer, Transzport réteg)
3	Hálózati réteg (Network layer, IP layer, IP réteg)
2	Adatkapcsolati réteg (Data Link layer)
1	Fizikai réteg (Physical layer)

Az ISO/OSI modell

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

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

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

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

Az ISO/OSI modell

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 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.

1. Fizikai réteg: Elektromos és mechanikai jellemzők procedurális és funkcionális specifikációja két (közvetlen fizikai összeköttetésű) eszköz közötti jeltovábbítás céljából. Bitek csatornára bocsátása.

Protokoll rétegbesorolási modellek

Protokoll → Protokollréteg → Rétegbesorolási modell

ISO/OSI modell	Hibrid modell	TCP/IP modell
Alkalmazási Megjelenítési Viszony		Alkalmazási
Szállítási		Szállítási
Hálózati		Hálózati
Adatkapcsolati Fizikai		Hoszt a hálóhoz

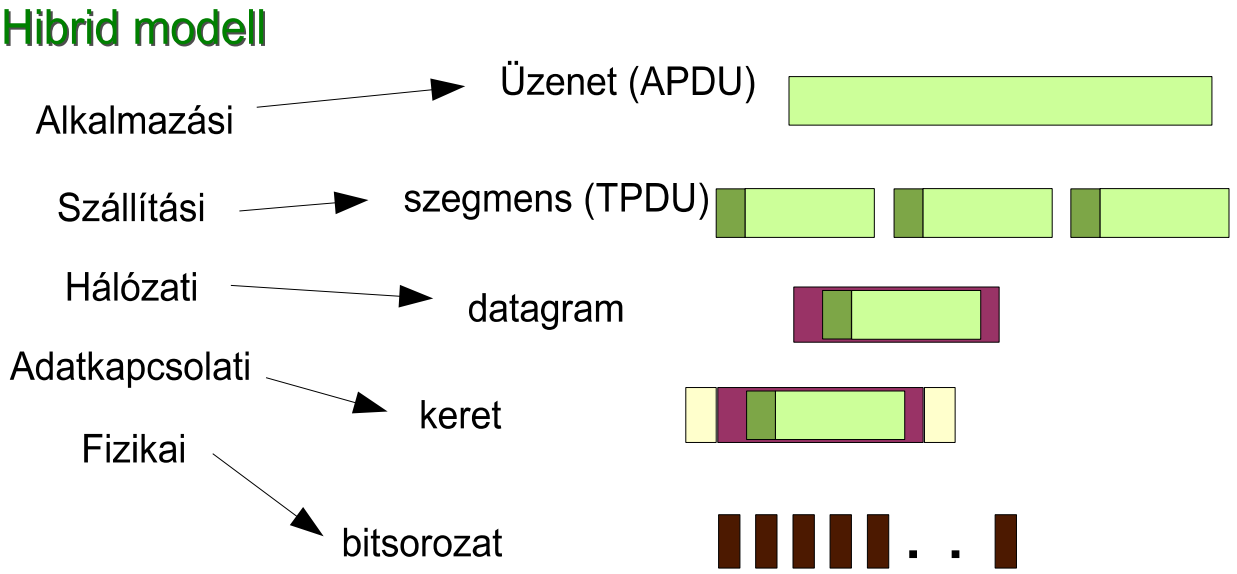
Enkapszuláció, Protocol Data Unit

Beágyazás (enkapszuláció):

- A (felsőbb szintről érkező) információ egy bizonyos protokoll fejléccel történő becsomagolása (mint pl. levél küldésekor a borítékba helyezés és boríték címzés).

Protokoll adatelem (PDU, Protocol Data Unit, csomag):

- Az adott protokoll által kezelt (fejlécből és adatból) álló elem. (Gyakran használt másik megnevezése a csomag.)



Hálózati kapcsolóelemek

Hálózati kapcsolóelemek - alapfogalmak

Ütközési tartomány (Collision domain; Bandwith domain):

- Az a hálózatrész, melyben az ütközés érzékelhető (több állomás által használt közös média).
- Az ütközési tartományban egy időpillanatban csak egy információátvitel folyhat.

Üzenetszórási tartomány (Broadcast domain):

- Az a hálózatrész, ahol az üzenetszórás célcímmel feladott információ megjelenik, érzékelhető.

Hálózati kapcsolóelemek

A részhálózatok - a kapcsolóelem működése alapján - különböző OSI rétegekben kapcsolhatók össze:

OSI réteg	**Kapcsolóelem**
Transzport réteg és felette	Átjáró (gateway)
Hálózati réteg	Forgalomirányító (router)
Adatkapcsolati réteg	Híd (bridge), Kapcsoló (switch)
Fizikai réteg	Jelismétlő (repeater) HUB

Hálózati kapcsolóelemek

Jelismétlő (repeater):

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

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.

Hálózati kapcsolóelemek

Kapcsoló (switch):

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

Forgalomirányító, útválasztó (router):

- Az hálózati rétegben működve szelektív összekapcsolást, útvonalválasztást, forgalomirányítást végez.
- Az összekapcsolt részhálózatok külön ütközési tartományt és külön üzenetszórási tartományt alkotnak.
- Csomópont, saját hálózati címmel rendelkezik.
- Hálózati rétegbeli átjárónak is nevezik (default gateway).

Topológiák

Fizikai topológia:

- A csomópontok térbeli elhelyezési, összeköttetési lehetőségeit vizsgálja. (Kábelezési topológia).

Logikai topológia:

- A csomópontok logikai egymás utáni rendezettségét, sorrendjét vizsgálja.

A fizikai réteg

Topológiák

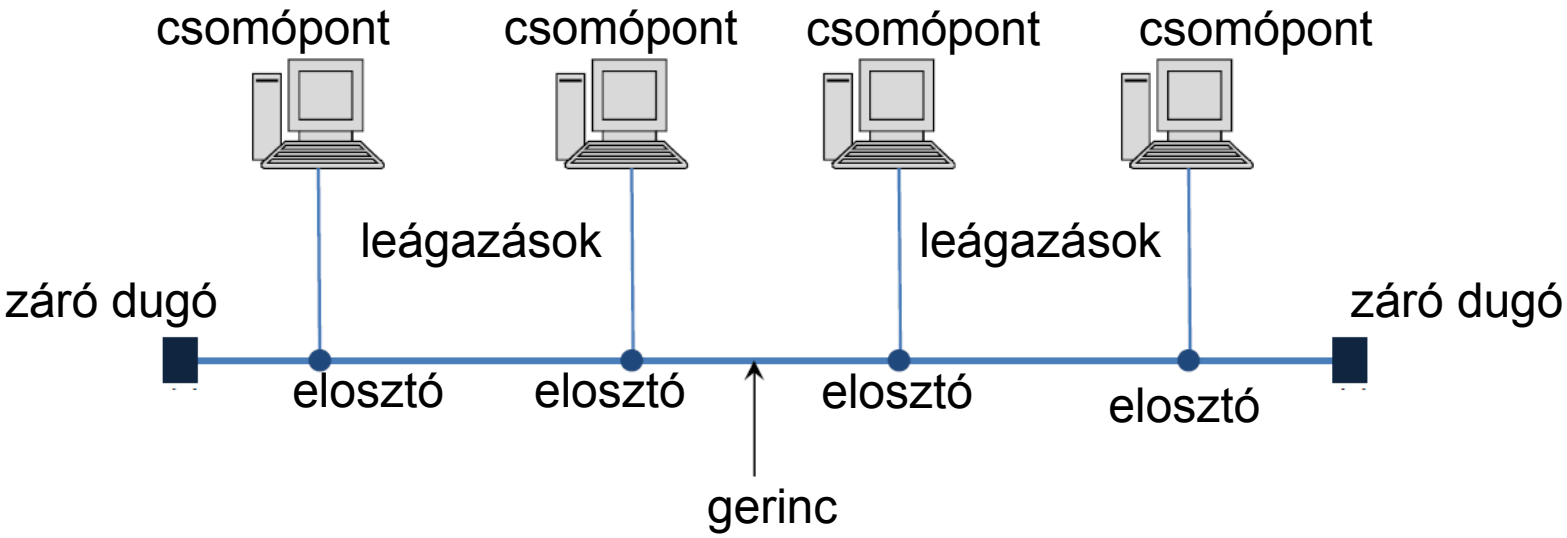
Busz topológia: Egy hosszú kábel szolgál a hálózat gerinceként. A csomópontokat leágazásokkal kapcsoljuk a gerinchez elosztó dugókkal (tap).

Előnyei:

- Könnyű csomópontot hozzáadni
- Egyszerű és olcsó

Hátrányok:

- Nehéz hibakeresés
- Az összes csomópont között osztott sávszélesség



Topológiák

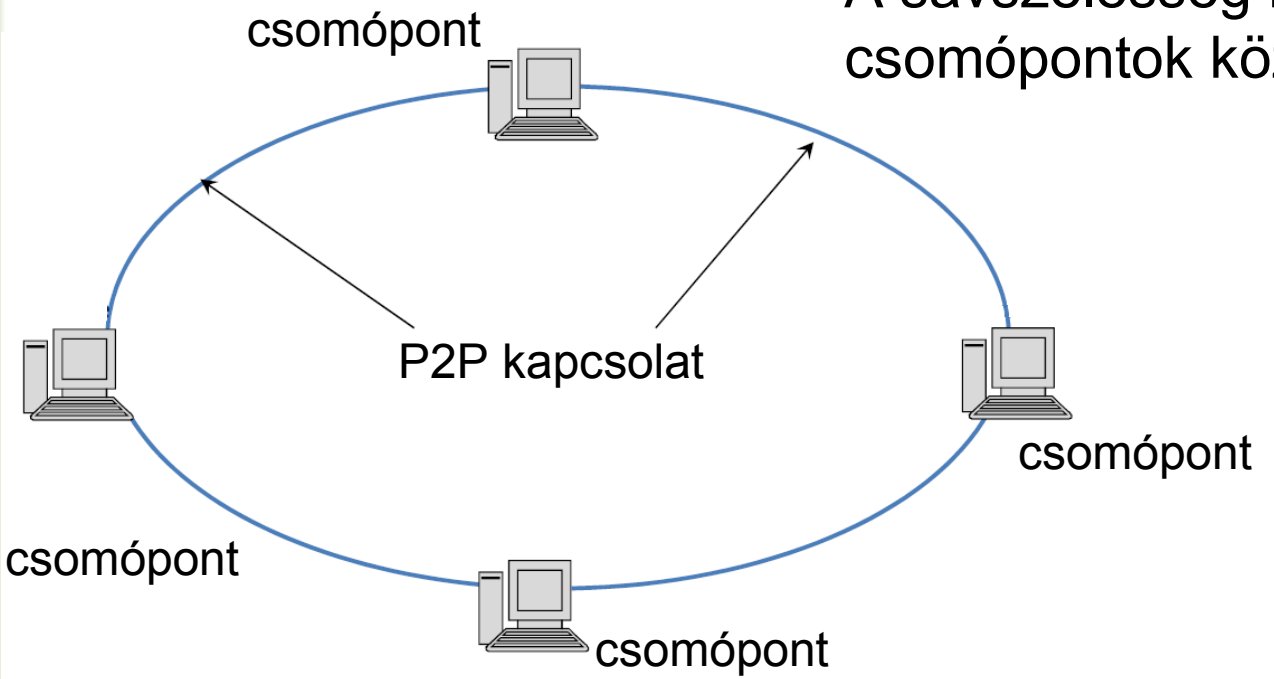
Gyűrű topológia: minden csomópont dedikált P2P vonalon csatlakozik a mellette lévő két szomszédjához

Előnyök:

- Könnyű installálás
- Egyszerűbb hibakeresés

Hátrányok

- Az eszközök cseréje hatással lehet a hálózatra
- A sávszélesség megoszlik a csomópontok között



Topológiák

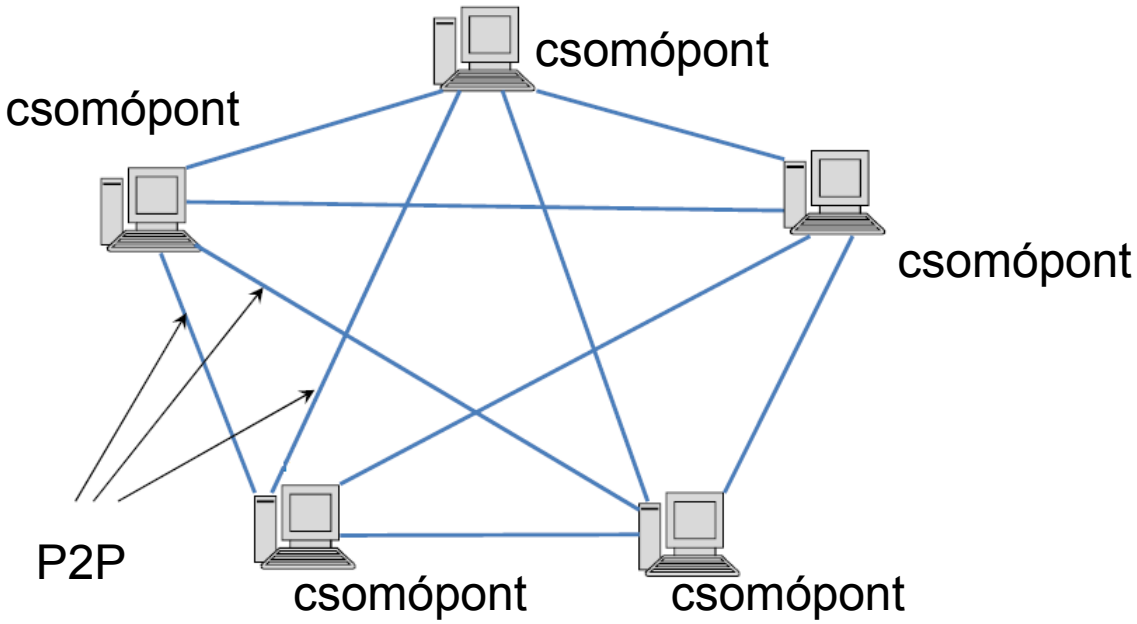
Mesh (háló) topológia: minden csomópont dedikált P2P vonalon csatlakozik majdnem minden további csomóponthoz

Előnyök:

- Robosztus (→ hibatűrő)
- A vonalak (legtöbbször) nem osztottak

Hátrányok:

- A teljes háló kialakításához N csomópont esetén N(N-1)/2 vonal kell.



Topológiák

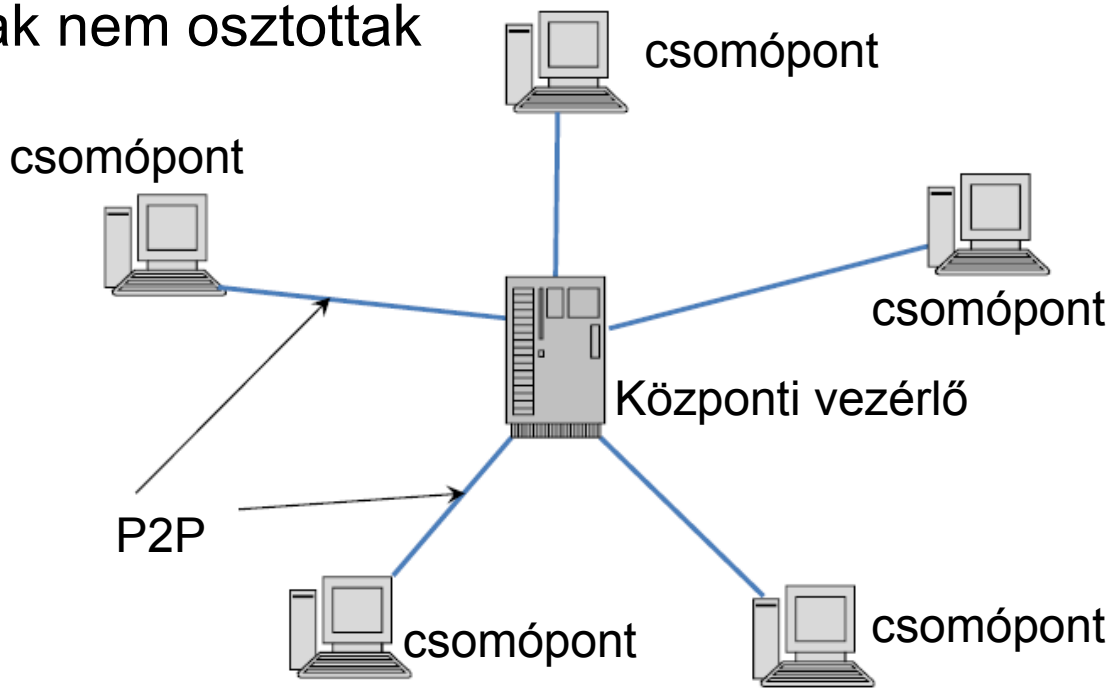
Csillag topológia: minden csomópont dedikált vonalon csatlakozik egy központi elosztóhoz

Előnyök:

- Hiba esetén csak egy adott link esik ki
- A vonalak nem osztottak

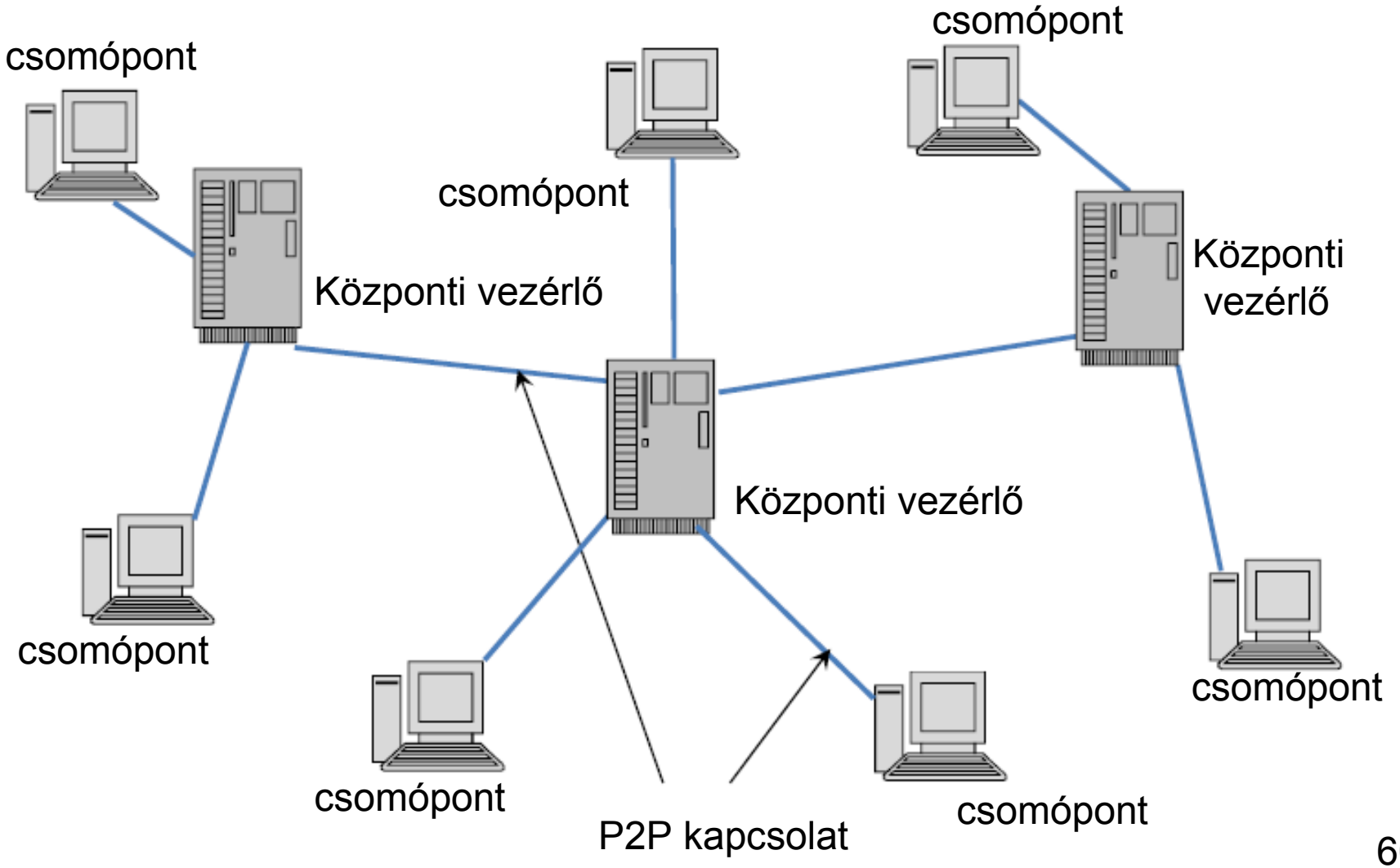
Hátrányok:

- A központi csomópont hibája a teljes hálózatot érinti



Topológiák

Kiterjesztett csillag (fa) topológia



A fizikai réteg protokolljai

1. Fizikai réteg: Elektromos és mechanikai jellemzők procedurális és funkcionális specifikációja két (közvetlen fizikai összeköttetésű) eszköz közötti jeltovábbítás céljából. Bitek csatornára bocsátása.

- **Jeltovábbítás:** a fizikai rétegben valósul meg az információ fizikai továbbítása az átviteli közegen.

- **Jelkódolás:** Az adatkapcsolati rétegből érkező adategység (keret) a fizikai rétegben egyszerű bitsorozatként jelenik meg, melyet a fizikai réteg az adott átviteli közegen (médium) továbbítható jelsorozattá (impulzus sorozattá) alakít: bit-by-bit vagy symbol-to-symbol továbbítás.

Csillapítás

A jel amplitúdója csökken a jel haladása során az átviteli közegben.

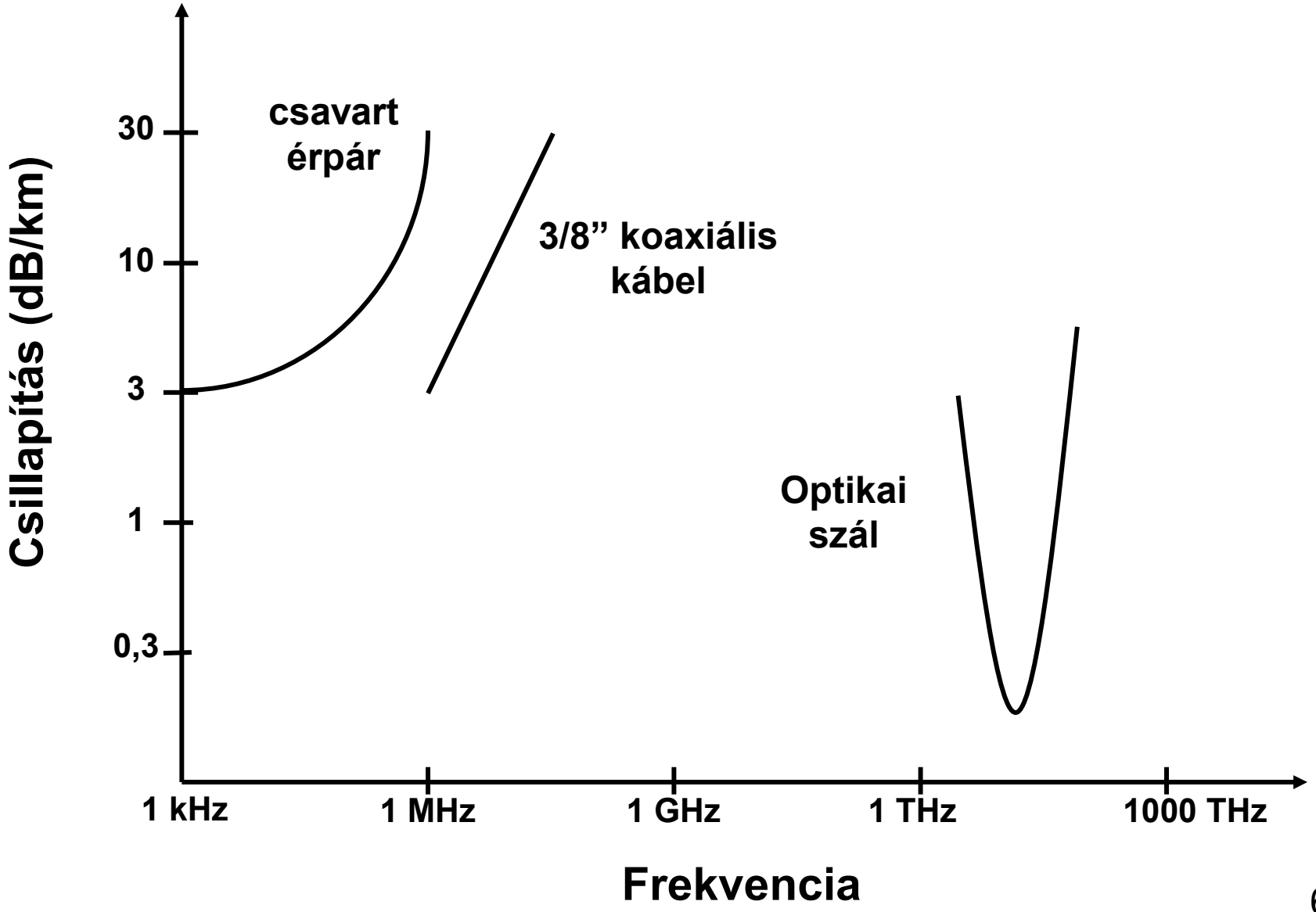
Az átviteli közeg hosszát úgy állapítják meg, hogy a jel biztonsággal értelmezhető legyen a vételi oldalon.

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 logaritmikus skálán *decibel*ben(dB) adják meg.

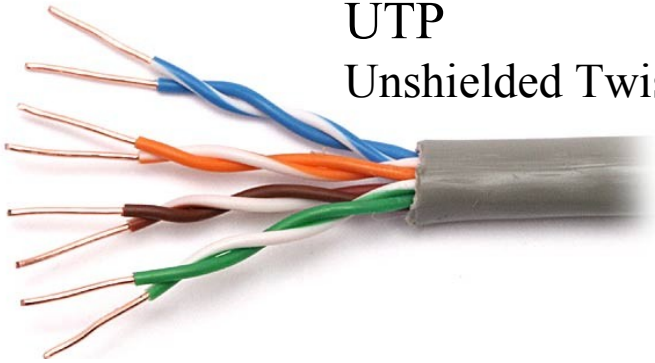
Csillapítás



Csavart érpár

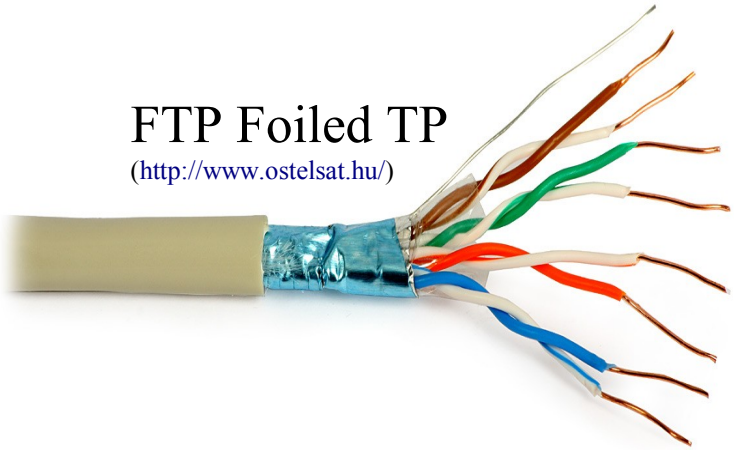
- A legolcsóbb, legelterjedtebben használt átviteli közeg.
- Két szigetelt rézvezetéket szabályos minta szerint összecsavarnak.
- Többnyire néhány csavart érpárt (UTP esetén 4 db-ot) kötegelnek és védőszigeteléssel vonnak be.
- A csavarás csökkenti az áthallást az érpárok között és zajvédelmet biztosít.
- A csavarás hossza kicsit különbözhet az egyes érpárokban, hogy csökkenjen az áthallás.
- A huzal átmérője 0.4 - 0.9 mm .
- A legolcsóbb médium, a legkönnyebb vele dolgozni, de az adatátviteli sebessége és az áthidalható távolság erősen korlátozott.

Csavart érpár

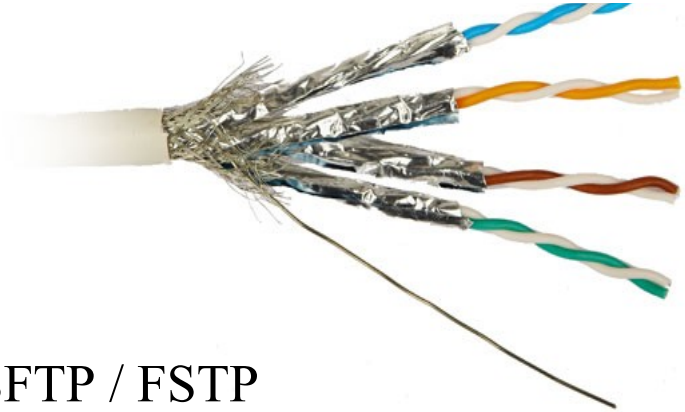


UTP
Unshielded Twisted Pair
(fotohal.hu)

STP
Shielded TP
(www.rieztoshare.com)



FTP Foiled TP
(http://www.ostelsat.hu/)



SFTP / FSTP
Shielded Foiled / Fully Shielded TP
(hyperlinesystems.com)

Csavart érpár

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.
- A zavarások csökkentésére árnyékolást alkalmazhatnak (STP, FTP).
- Különböző csavarási hosszak használata a szomszédos érpárok közötti áthallást (crosstalk) csökkenti.
- Pont-pont analóg jelzéssel (néhányszor) 100KHz sávszélesség is elérhető (több hangcsatorna átvitele).
- Rövid távolságra (néhányszor) 100 Mbps sebesség is elérhető.

Csavart érpár

Category 5. UTP kábel és csatlakozók 100 MHz átvitelre.

Korlátozott távolságra (100 méter) 100 Mbps sebességű átvitelt tesz lehetővé. Az új épületeket gyakran ezzel a kábellel huzalozzák be.

Új szabványok:

Cat5e – a 4 érpár együttes használatát teszi lehetővé, 1GBps

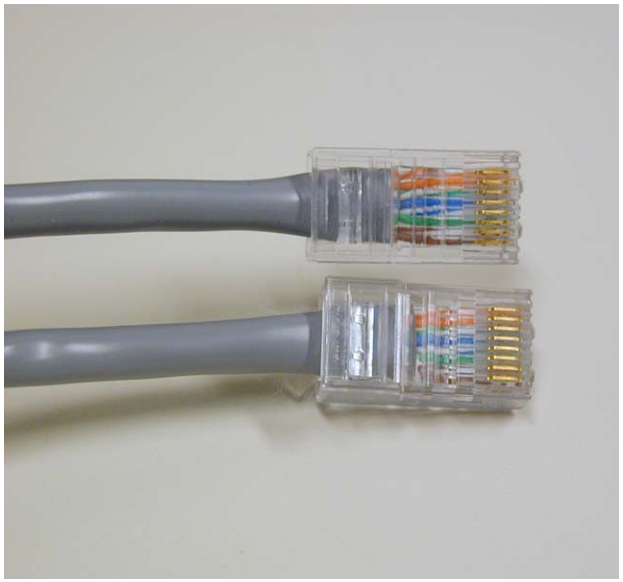
Cat6: ~250MHz 1GBps nagy távolságra, 10GBps kicsire

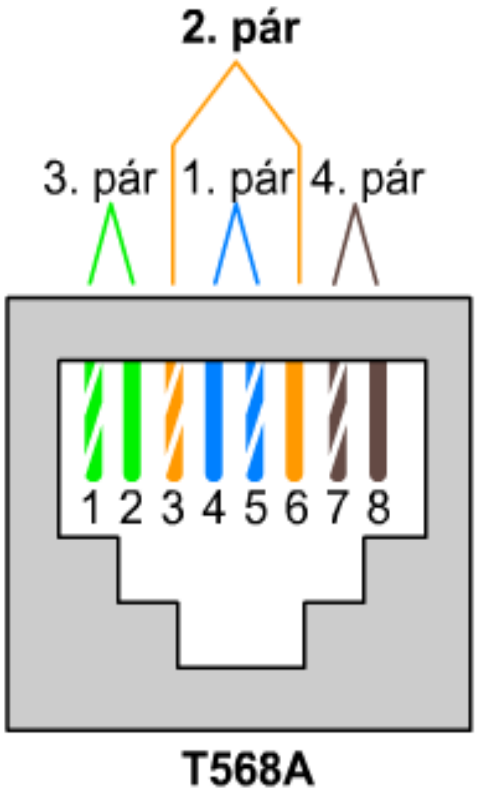
Cat6a: ~500MHz 100m-ig 10GBps

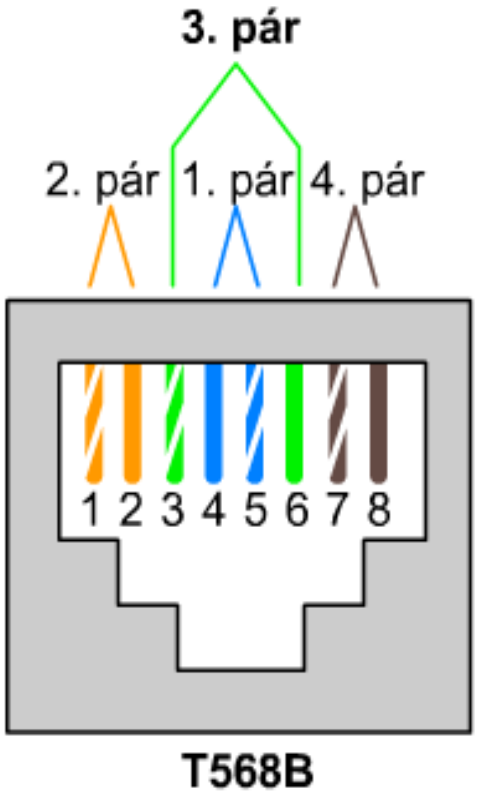
Cat7: STP: ~600MHz.(jelenleg 40GBps, 100GBps tesztelés alatt http://www.ieee802.org/3/hssg/public/nov07/kavehrad_01_1107.pdf 2016.08.30.)

Cat8.1, Cat8.2:

Csavart érpár







Csavart érpár

Egyenes RJ-45 aljzat (PC, router):

Tx+	Tx-	Rv+			Rv-		
1	2	3	4	5	6	7	8

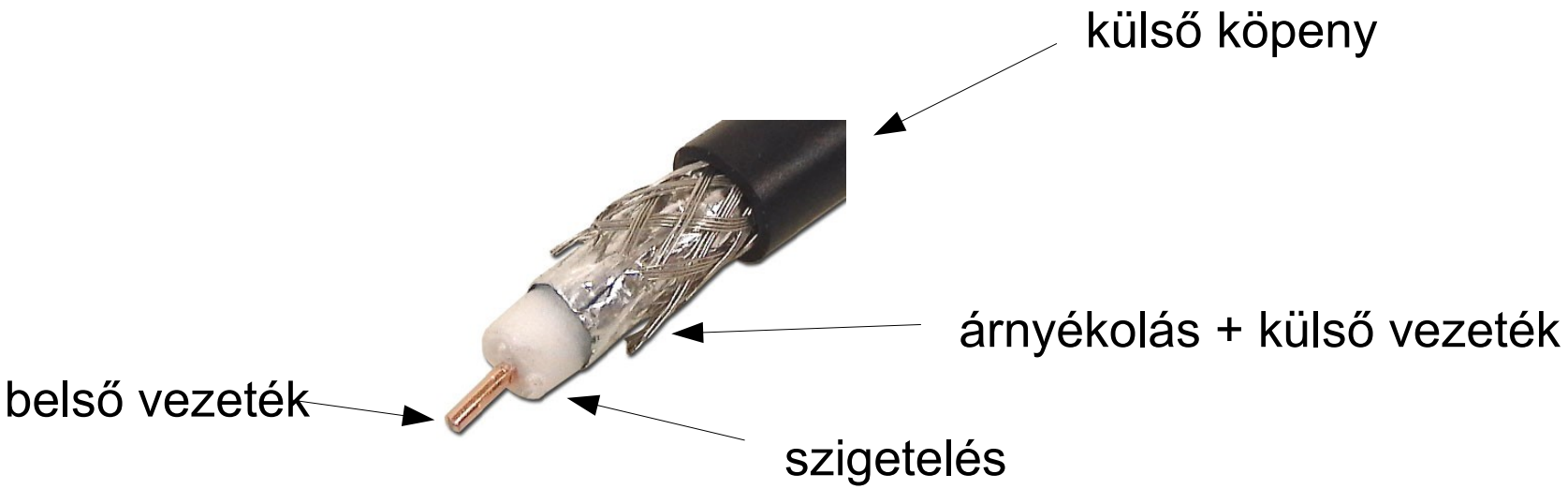
Kereszt RJ-45 aljzat (Switch, Hub):

Rv+	Rv-	Tx+			Tx-		
1	2	3	4	5	6	7	8

- Az azonos kiosztású RJ-45 aljzatokat (pl. pc-pc, hub-hub) keresztkábellel (568A – 568B) kötjük össze.
- A különböző RJ-45 aljzatokat (pl. pc-hub, pc-switch, router-switch) egyenes kábellel (568A – 568A, vagy 568B – 568B) kötjük össze.
- A legtöbb mai eszköz érzékelni tudja a másik oldalon alkalmazott RJ-45 aljzat kiosztását, s ahhoz automatikusan alkalmazkodni képesek (auto sense).

Koaxiális kábel

Koax kábel



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

Koaxiális kábel krempelés: : ://www.youtube.com/watch?v=NEi0SXhqObQ u.l. 2016.08.30.

Koaxiális kábel

Alkalmazásai

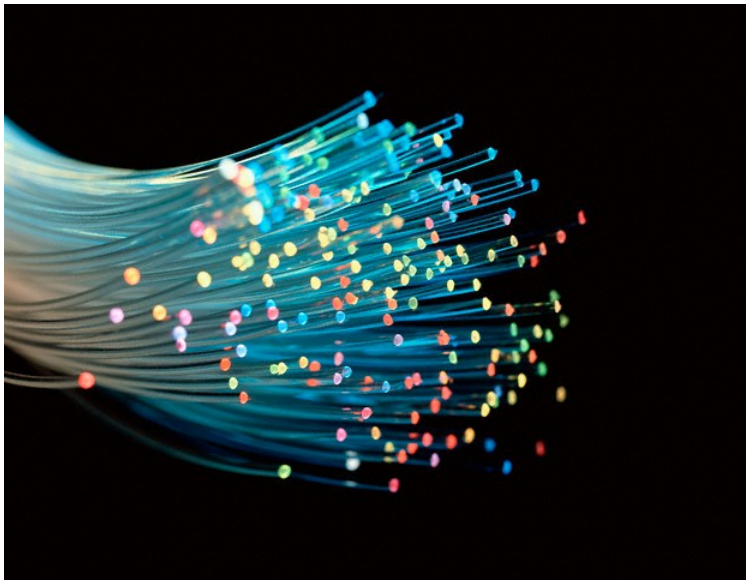
- Televízió adás továbbítása.
- Nagy távolságú telefon átvitel.
- Számítógépek összekapcsolása
- Helyi hálózatok.

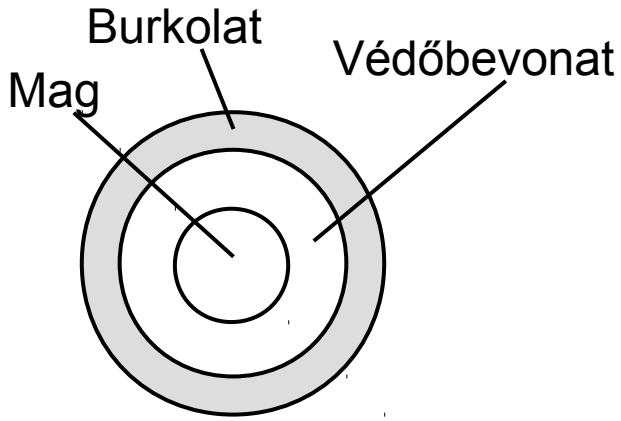
Átviteli jellemzők

- Analóg átvitel esetén néhány km-enként szükséges erősítés. Néhány 100 MHz-ig használható.
- Digitális átvitel esetén km-enként szükséges jelismétlő használata.

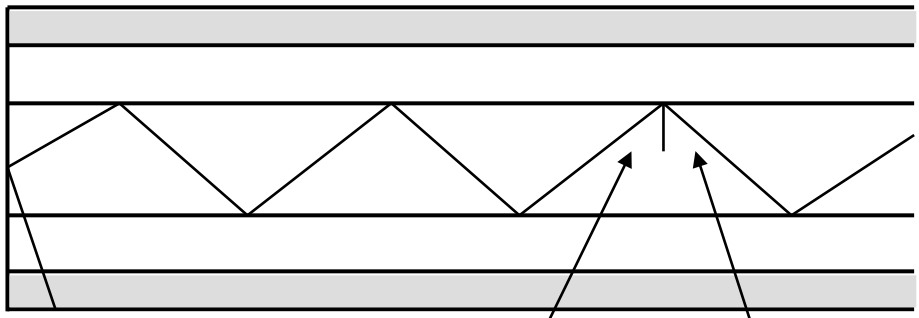
Optikai szál

Fizikai jellemzők





Optikai szál



A kritikus szögnél (határszög) kisebb szögben becsapódó fény-sugarat elnyeli a bevonat

Beesési szög

Visszave-rődési szög

Optikai szál

Fizikai jellemzők

- 2 - 125 μm átmérőjű hajlékony optikai szál fénysugár továbbítására képes.
- Optikai szálat üvegből és műanyagból is készítenek.
- A védőbevonat szintén üveg vagy műanyag, más optikai tulajdonságokkal rendelkezik, mint a mag.
- A külső műanyag burkolat a szennyeződés, kopás és egyéb külső hatások ellen nyújt védelmet.

Optikai szál

Alkalmazásai (pozitívumok):

Nagyobb kapacitás

Nagy adatátviteli sebesség érhető el (2 Gbps több 10 km-en).

Kisebb méret és súly

Kisebb csillapítás

A csillapítás kisebb, és széles frekvencia tartományban 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

Optikai szál

Optikai szálon történő adatátvitel fejlesztések:

pl. 101 TBit/s 165 km-en (2011),

1.05 PetaBit/s 52.4 km-en (2012)
http://www.laserfocusworld.com/articles/slideshow/2014/01/slideshow-technology-review-2013/pg014.html
(2016)

Ugyanakkor a sebesség nem minden. A helyesség is fontos.
http://phys.org/news/2016-03-record-speed-transmission-big-accessible.html (2016)

Optikai szál

Alkalmazásai

Nagyvárosi fővonalak
Vidéki nagy távolságú fővonalak (trunk)
Telefonközpontok fővonalai
Előfizetői hurkok
Helyi hálózatok

Átviteli jellemzők

10^{14} - 10^{15} Hz (infravörös) tartományban működik.

Fényforrás lehet:

LED
Lézer dióda.

Optikai szál - típusok

Átviteli jellemzők

Több módusú szál

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.

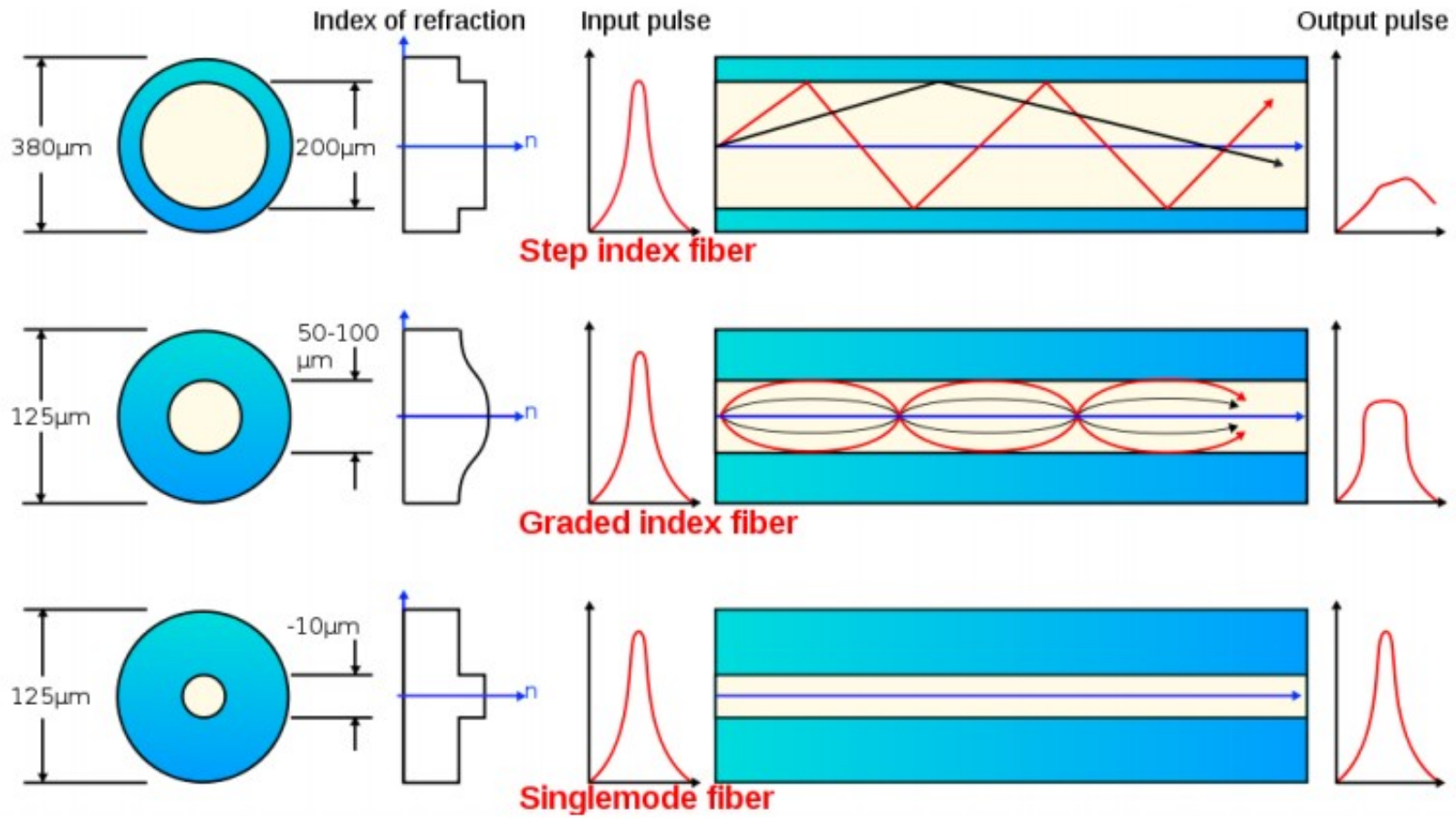
Egy módusú szál

A mag átmérőjét csökkentve a hullámhossz méretére, csak a tengely irányú fénysugár jut át. A fényimpulzusok nem torzulnak, nagyobb adatátviteli sebesség érhető el.

Több módusú, emelkedő törésmutatójú szál

A mag anyagának törésmutatója a tengelytől távolodva növekszik. Ez mintegy fókuszálja a fényt. E típus tulajdonságai az előző kettő közé tehetők.

Optikai szál - típusok



forrás: wikipedia.org

Vezeték nélküli technológiák

Helyi hálózati technológiák (WLAN, Wi-Fi):

- Egy intézményi LAN hálózat vezeték nélküli kiterjesztése.
- Szabadon használható frekvenciák (2.4 GHz, 5 GHz).
  - Fényszerű terjedés.
  - 2.4 GHz a víz rezonancia-frekvencia közelében!
- Mobilitás biztosítása az intézményi adatkommunikációs hálózaton.

Nagy távolságú összeköttetés biztosítása (GPRS, 3G, 4G, 5G).

- Globális hálózati hozzáférést biztosít.
- A mobiltelefonos technológia kiterjesztése adatátviteli célokra.
- Használati (átviteli) díj fizetés.

Vezeték nélküli technológiák

WLAN Üzemmódok:

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

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

Jel, jelkódolás, moduláció

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

Jelkódolás: A (**digitális**) információ leképezése (**digitális**) vivőjelre (pl. feszültségszintekre, feszültségszint váltásokra).

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

Moduláció: A (**digitális**) információ leképezése (**analóg**) vivőjelre. A csatornába kerülő (modulált) jel előállítása a forrásból érkező moduláló-jelből és az analóg vivőjelből.
Inverz folyamata a demoduláció.
A modem a modulációt és demodulációt végző berendezés.

Jelkódolás

NRZ – Non Return to Zero

Az 1 jel teljes idejében alacsony feszültségszint
A 0 jel teljes idejében magas feszültségszint

NRZI – Non Return to Zero Inverted

Az 1 jel esetén történjen feszültségváltás
A 0 jel esetén ne történjen semmi

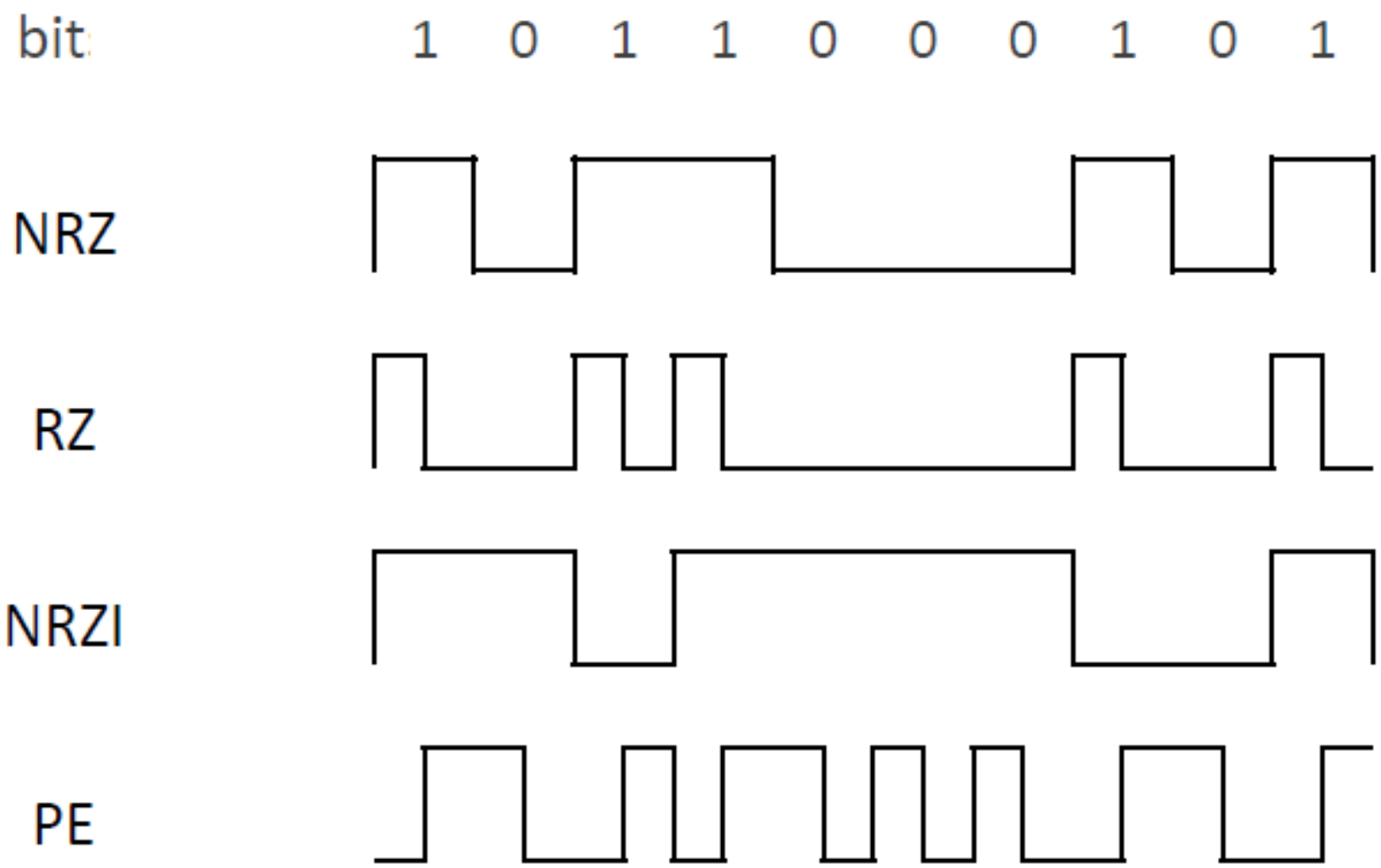
RZ – Return to Zero

Az 1 jel esetén történjen feszültségváltás lefelé az átviteli idő felénél
A 0 jel esetén ne történjen semmi

PE – Phase Encode (Manchester)

Az 1 jel esetén történjen feszültségváltás felfelé az átviteli idő felénél
Az 0 jel esetén történjen feszültségváltás lefelé az átviteli idő felénél

Jelkódolás



Moduláció

Amplitudó billentyűzés (Amplitude Shift Keying): Az (1) értéket a vivőfrekvencia jelenléte; a (0) értéket a vivő hiánya jelzi. Rossz tulajdonsága a diszkrét komponens jelenléte

Frekvencia billentyűzés (Frequency SK): Az (1) értéket a vivőfrekvenciánál egy meghatározott frekvencialökettel kisebb; a (0) értéket pedig a vivőnél a megadott frekvencialökettel nagyobb frekvencia jelzi.

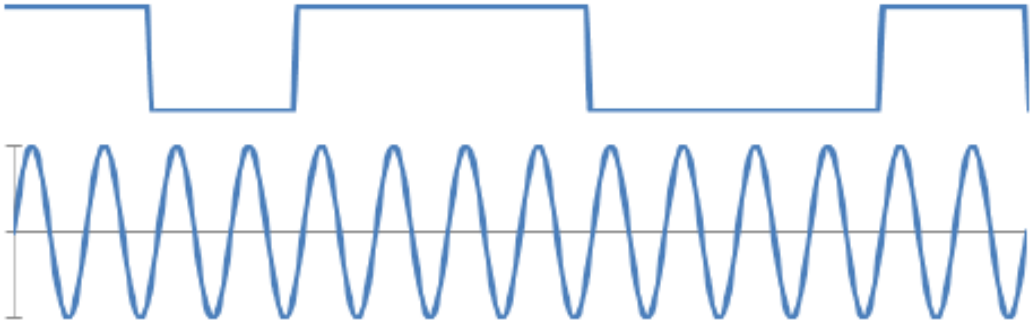
Fázis billentyűzés (Phase SK): Az (1) értéket a vivőfrekvenciával azonos; a (0) értéket pedig a vivőhöz képest ellentétes fázisú jel jelzi.

Többszintű PSK: 180 fok helyett több kisebb eltolási érték alkalmazásával egy átviteli időegységben több bit átvitele is megoldható. (Tipikusan 4 szintet használunk 0° 90° 180° 270° eltolással)

Moduláció

Digitális jel

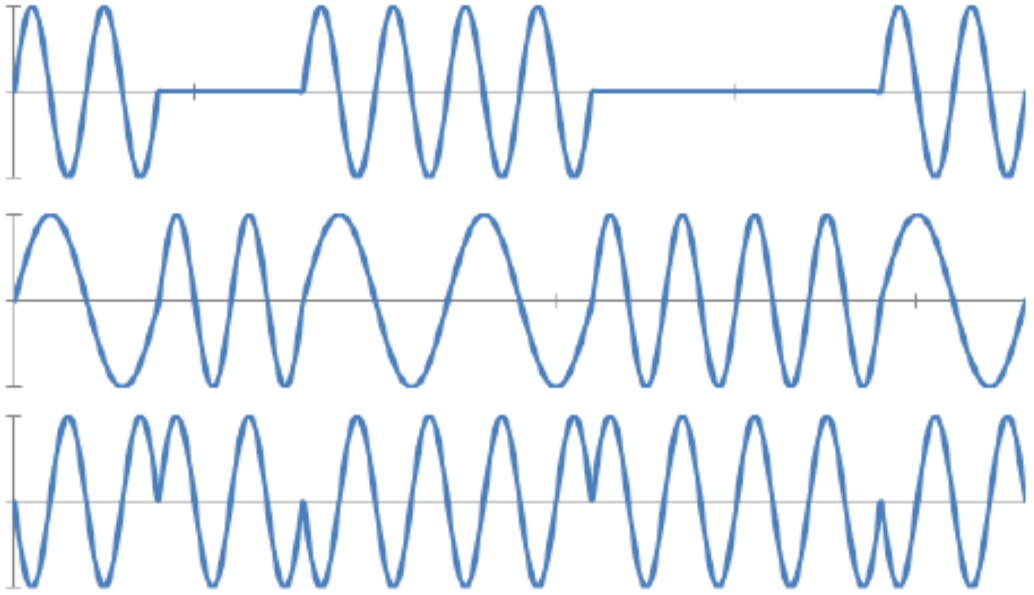
Vivőjel



Amplitudó billentyűzés (ASK)

Frekvencia billentyűzés (FSK)

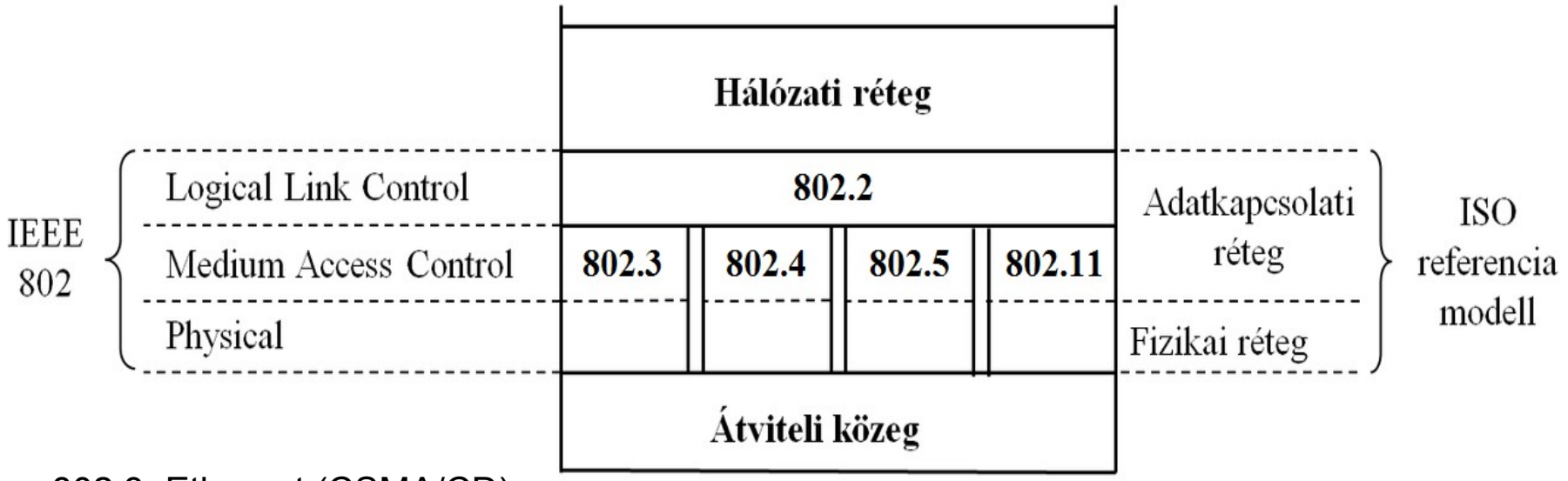
Fázis billentyűzés (PSK)



Az adatkapcsolati réteg

Az adatkapcsolati réteg protokolljai

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.



802.3: Ethernet (CSMA/CD)
802.4: Token Bus
802.5: Token Ring
802.11: Wireless LAN

(Az IEEE 802 protokollcsalád 802.1-802.24-ig tartalmaz protokollokat. Az órán nem ismertetett prrotokollokról lásd: http://www.ieee802.org/)

802.2 Logical Link Control

Feladatai:

A 3. rétegbeli protokoll számára megbízható átvitel biztosítása

- Forgalomszabályozás
- Hibaérzékelés, -javítás
- Protokoll multiplexelés

Szolgáltatások:

- **Nyugtázatlan, összeköttetésmentes (datagram):** 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).
- **Nyugtázott, összeköttetésmentes (datagram):**Nem megbízható (hibás, zajos) fizikai összeköttetés esetén célszerű. Alkalmazása tipikusan a vezeték nélküli technológiáknál a leggyakoribb.
- **Nyugtázott, összeköttetés-alapú:** Keretsorozatok átvitele esetén hatékony, ahol nem minden egyes keretre vonatkozóan történik visszajelzés.

Az LLC jelenléte nem mindig szükséges (pl. Ethernet keret esetén)

Media Access Control

MAC: Közeghozzáférési alréteg.
Fealdata annak eldöntése, hogy egy adott pillanatban ki adhat a csatornán, illteve mi a teendő ütközés esetén.

A feladat ellátására két különböző mód létezik:
- Statikus csatornafelosztás
- Dinamkus közeghozzáférés

(Miért szükséges az adatkapcsolati réteg két rétegre bontása? A logikai alréteg a fizikai közegtől független, sokkal állandóbb, mint a közeg-elérési alréteg. A hardver gyártók számára ez azt jelenti, hogy egy új csatolókártyához csak a MAC alréteg szoftverét kell implementálni.)

Media Access Control

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. *(Frequency Divided Multiple Access)*

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. *(Time Divided Multiple Access)*

Hullámhossz-osztásos multiplexelés (WDMA). Hasonló az FDM-hez, de ezt az optikai átvitelnél, a fény frekvenciatartományában alkalmazzuk. (Wavelength Divided Multiple Access)

Media Access Control

Dinamikus közeghozzáférés

Továbbítás figyelés nélkül (ALOHA)

Időréselt (Time Slot) (Réselt ALOHA)

Továbbítás figyeléssel (CSMA - Carrier Sense Multiple Access)

Ütközésérzékeléses (CSM/CD - Collision Detect)

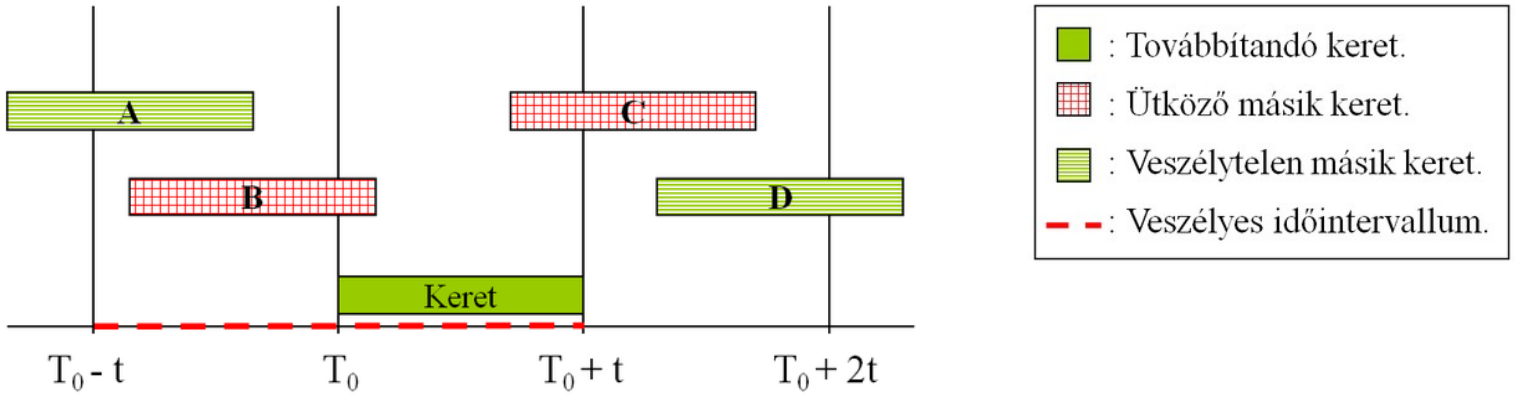
Vezérjeles (Token)

Kódosztásos (Code Divison Multiple Access)

Media Access Control

ALOHA

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

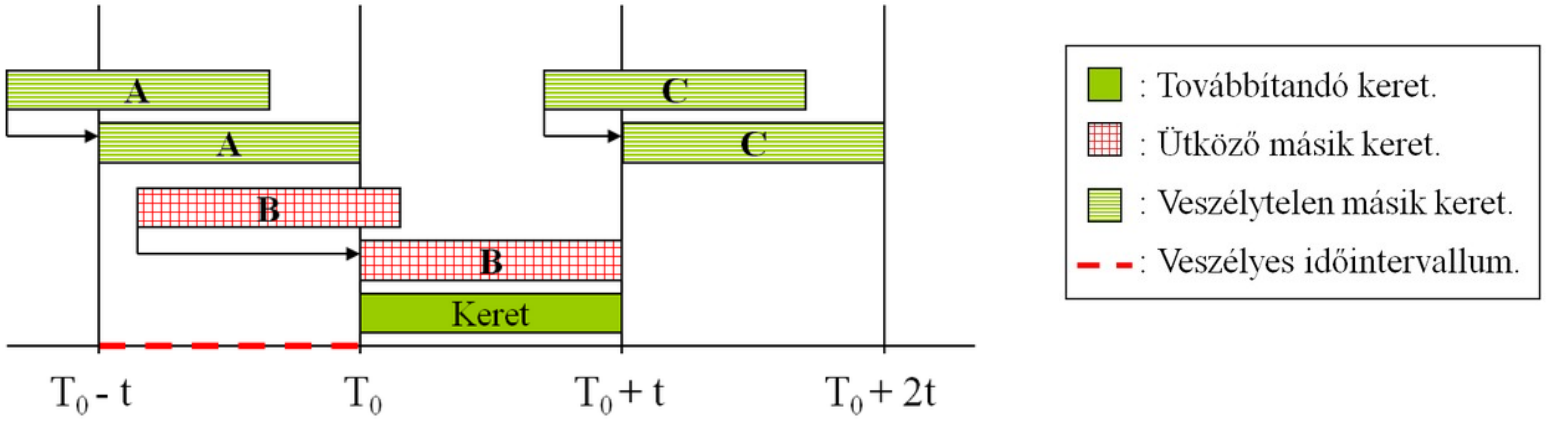


(T0 - a keret küldésének kezdőpillanata; t - egy keret átviteli ideje):

Media Access Control

Réselt ALOHA

- A továbbítandó keret a következő időrés elején kerül a csatornára.
- Ütközés esetén a következő időrésben véletlen valószínűséggel küldök.
- A csatornakihasználtság egyszerűen növelhető (36%).



(T0 - a keret küldésének kezdőpillanata; t - egy keret átviteli ideje):

Media Access Control

CSMA – Carrier Sense Multiple Access

Adás előtt belehallgatunk a csatornába, hogy szabad-e
Ha igen, megkezdjük az adást
Ha nem, véletlen ideig várunk

CSMA/CD – Carrier Sense Multiple Access / Collision Detection

Ha valaki velem azonos időben kezd adni, elhallgatok és véletlen ideig várok

Ezt a típusú hozzáférést használják a 802.3 Ethernet protokollok

Media Access Control

Vezérjeles gyűrű, Token ring 802.5

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.

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.

https://www.youtube.com/watch?v=2ZGfjsQw7_Y Ul:2015.10.04.

Media Access Control

CDMA (Code Divison Multiple Access)

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. **(802.11 Orhogonal FDM)**
- CDMA: A beszélgetők különböző nyelveken beszélgetnek.

Media Access Control

CDMA (Code Divison Multiple Access)

Működés:

Minden állomáshoz egy m bit hosszú kódot (chip-et, töredéket) rendelünk. A kódok ortogonlisak kell, hogy legyenek.

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

A1 = (+1, +1, -1, -1); (1-es bit jelzése). A0 = (-1, -1, +1, +1); (0-ás bit jelzése).
B1 = (+1, -1, +1, -1); (1-es bit jelzése). B0 = (-1, +1, -1, +1); (0-ás bit jelzése).
C1 = (-1, -1, -1, -1); (1-es bit jelzése). C0 = (+1, +1, +1, +1); (0-ás bit jelzése).

Ortogonalitás (a két vektor skaláris szorzata 0):

A1*B1 = a1*b1 + a2*b2 + a3*b3 + a4*b4 =
= 1*1 + 1*-1 + -1*1 + -1*-1 = 1 -1 -1 +1 = 0

Media Access Control

CDMA (Code Divison Multiple Access)

Működés:

Az állomások által egyidőben feladott bitértékek
(a 0-hoz a chip-code ellentettjét rendeljük):

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

A csatornán megjelenő vektor (jelsorozat): A0 + B1 + C0 = (+1, -1, +3, +1)

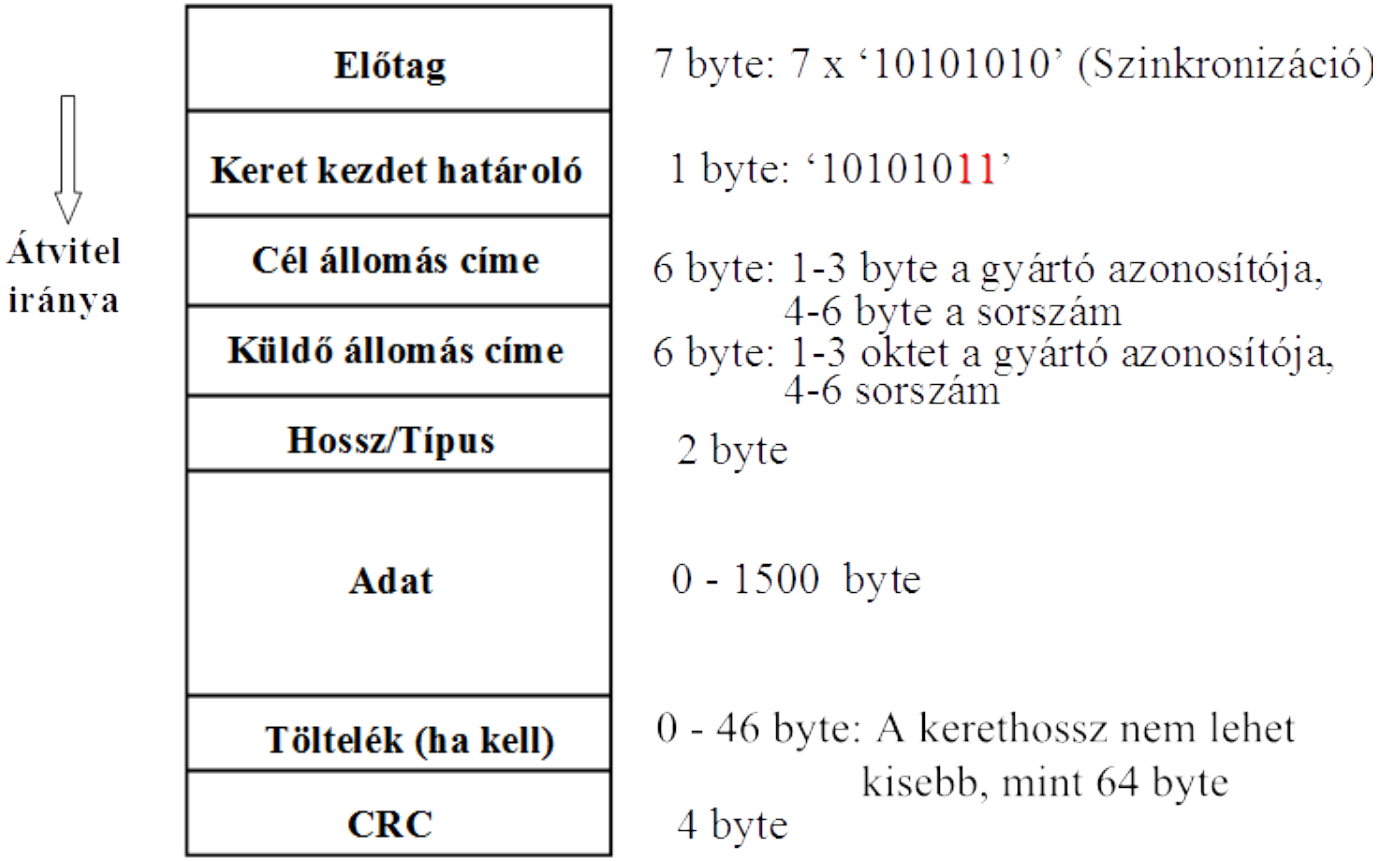
Visszafejtés (a megjelenő vektor skaláris szorzata a chip kóddal):

A partnere: A1 * (A0 + B1 + C0) = A1 * A0 = -, tehát A 0-ás bitértéket küldött.
B partnere: B1 * (A0 + B1 + C0) = B1 * B1 = +, tehát B 1-es bitértéket küldött.
C partnere: C1 * (A0 + B1 + C0) = C1 * C0 = -, tehát C 0-ás bitértéket küldött

(Mivel ha egy vektort önmagával szorzok skalásiran, + -t, míg ha az ellentettjével, - -t kapok.)

Media Access Control

802.3 – Ethernet (CSMA/CD)



IEEE 802.3 / Ethernet keret formátum

Egyéb keretformátumok: http://blog.globalknowledge.com/technology/what-is-the-difference-between-ethernet-ii-and-ieee-802-3/ 2015.10.30.

Media Access Control

802.3 – Ethernet (CSMA/CD)

Működési paraméterek

Átviteli sebesség	**10 Mbps (Manchester kódolás)**
Résidő	**512 bit-idő**
Keretek közti idő	**9,6 μs**
Átviteli kísérletek max. száma	**16**
Zavaró bitek száma (jam size)	**32 bit**
Legnagyobb kerethossz	**1518 byte**
Legrövidebb kerethossz	**512 bit (64 byte)**

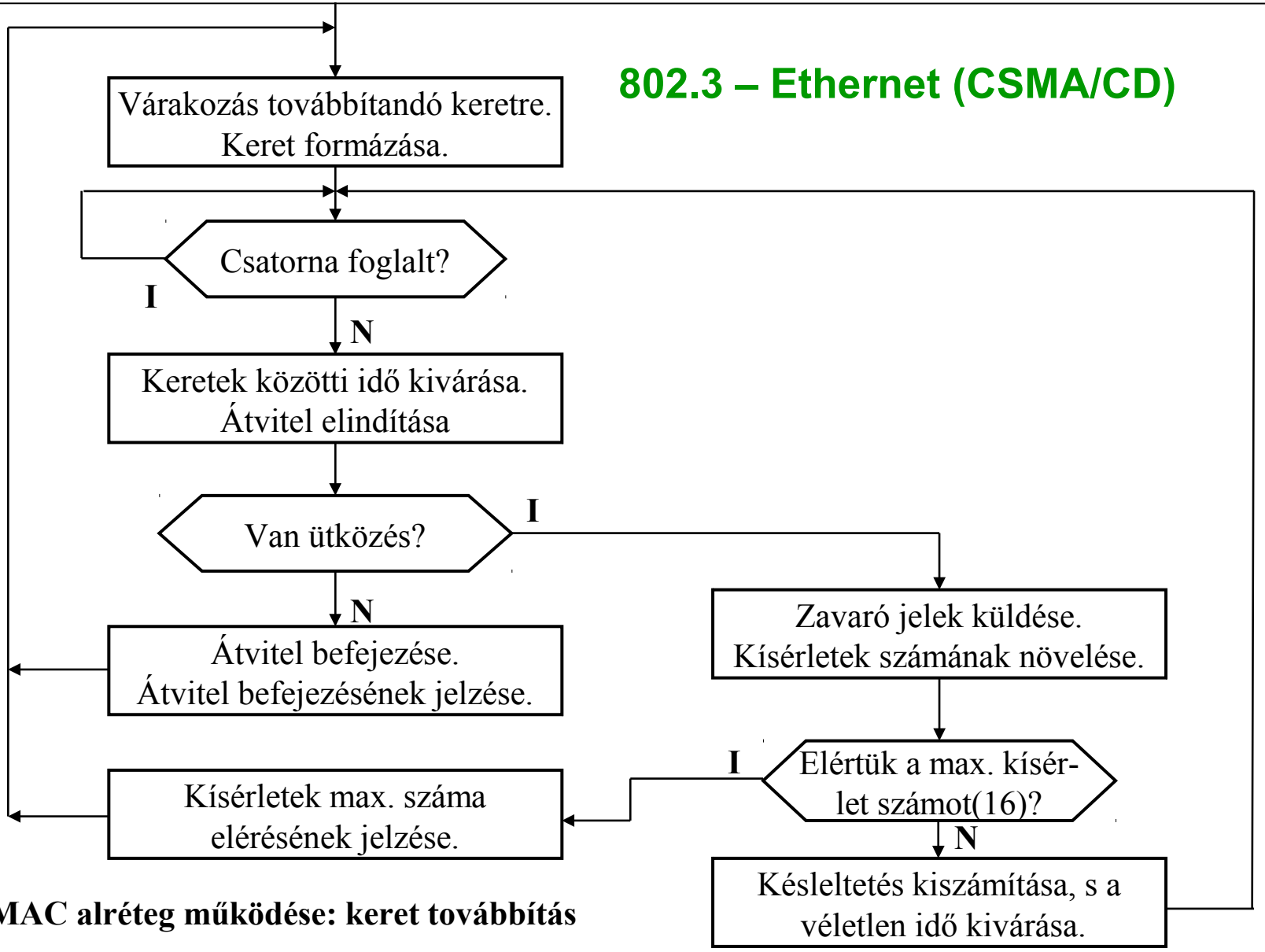
Célcím lehet

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

A küldő állomás címe nem lehet többes cím!

Media Access Control

802.3 – Ethernet (CSMA/CD)



MAC alréteg működése: keret továbbítás

Media Access Control

802.3 – Ethernet (CSMA/CD)

A keret ismételt továbbítása idejének meghatározása:

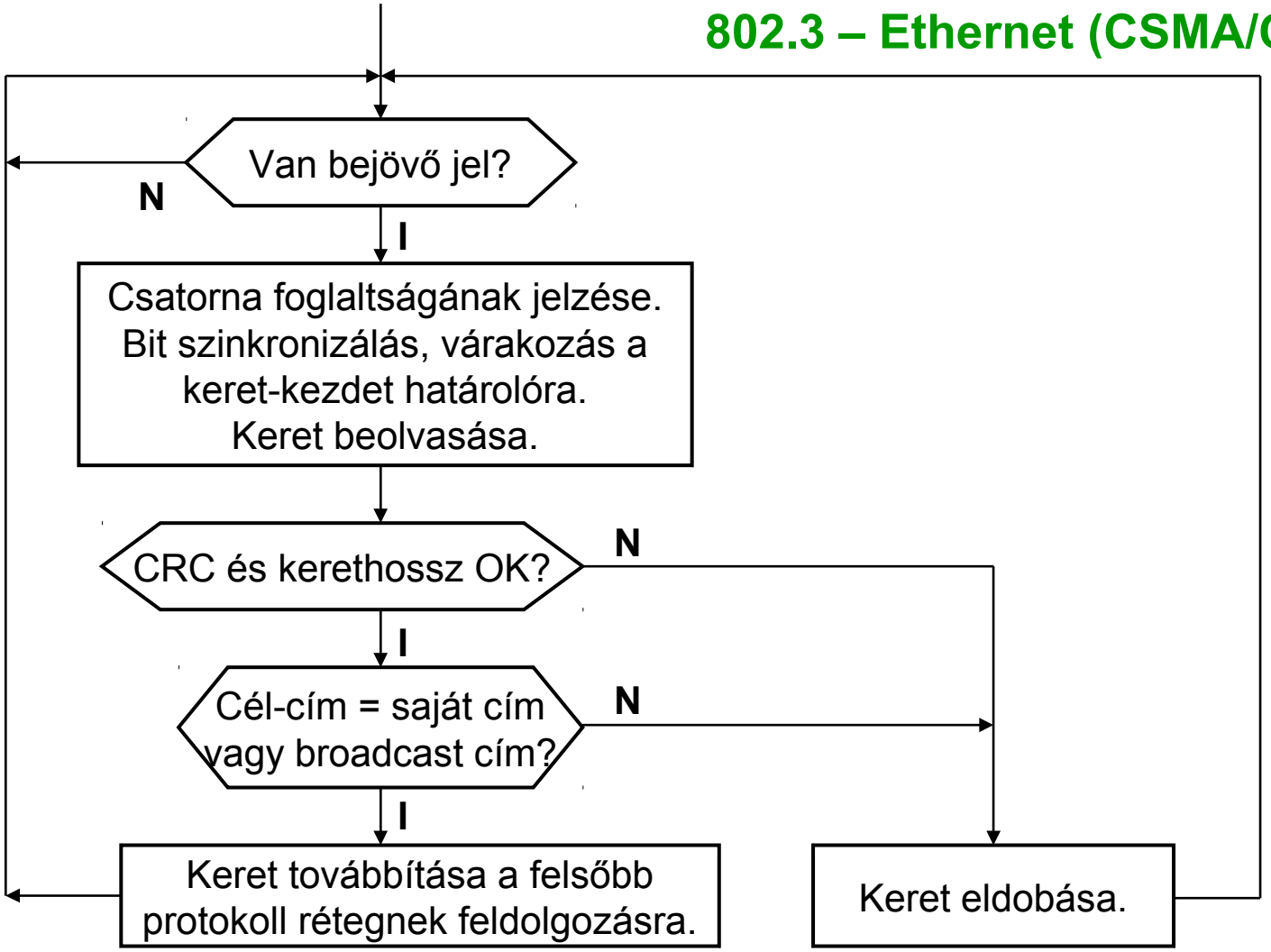
A résidő vagy körbejárási késleltetés az az idő amennyi idő alatt a keret első bitje a két legtávolabbi állomás között kétszer megfordul. Ennyi idő alatt az állomások biztonsággal észlelik az ütközést.

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

1. ütközés 0 vagy 1 résidőnyi várakozás véletlenszerűen
2. ütközés 0, 1, 2 vagy 3 résidőnyi várakozás véletlenszerűen
3. ütközés 0, 1, 2 …7 résidőnyi várakozás véletlenszerűen
.
10. ütközés 0 – (2^{10}-1) résidőnyi várakozás véletlenszerűen
11. ütközés - ” -
. - “ -
15. ütközés - “ -

16. ütközés után nem az interfész kártya nem próbálkozik tovább, jelzi az átvitel sikertelenségét.

Media Access Control



MAC alréteg működése: keret fogadás

Media Access Control

802.3 – Ethernet (CSMA/CD)

	Név	Sávszélesség	Átviteli közeg	Szabvány	Max. szegmenshossz
klasszikus	10BASE-2	10 Mbit/s	koaxiális	802.3 (8)	185 m
klasszikus	10BASE-5	10 Mbit/s	koaxiális	802.3 (10)	500 m
klasszikus	10BASE-T	10 Mbit/s	csavart érpár (Cat3, Cat5)	802.3 (14)	100 m
fast	10BASE-F(L)	10 Mbit/s	optikai	802.3 (15, 18)	2000 m
fast	100BASE-TX	100 Mbit/s	csavart érpár (Cat5)	802.3 (24)	100 m
fast	100BASE-FX	100 Mbit/s	optikai (MM)	802.3 (24)	2000 m
gigabit	100BASE-SX	100 Mbit/s	optikai (MM)	TIA	
gigabit	1000BASE-T	1 Gbit/s	csavart érpár (Cat 5e, Cat6)	802.3ab (40)	100 m
gigabit	1000BASE-SX	1 Gbit/s	optikai (MM)	802.3z	550 m
gigabit	1000BASE-LX	1 Gbit/s	optikai (MM/SM)	802.3z (38)	550 m / 2000 m
gigabit	1000BASE-LX10	1 Gbit/s	optikai (SM)	802.3	10 km
	10GBASE-T	10 Gbit/s	csavart érpár (Cat6a, Cat7)	802.3an	100 m
	10GBASE-SR	10 Gbit/s	optikai (MM)	802.3ae	300 m
	10GBASE-LX4	10 Gbit/s	optikai (MM/SM)	802.3ae	300 m / 10 km
	10GBASE-LR	10 Gbit/s	optikai (SM)	802.3ae	10 km

Adatkapcsolati réteg - WAN

SLIP (**Serial Line Internet Protocol**, RFC 1055) egy régi WAN adatkapcsolati réteg megoldás. 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 autentikáció.

Adatkapcsolati réteg - WAN

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.

Soros vonalon alkalmazott protokoll. A TCP/IP mellett számos protokollt támogat, lehetővé teszi például Novell IPX és Appletalk protokollok átvitelét is.

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. Például IPCP

Adatkapcsolati réteg - WAN

Csomagkapcsolt L2 WAN protokollok:

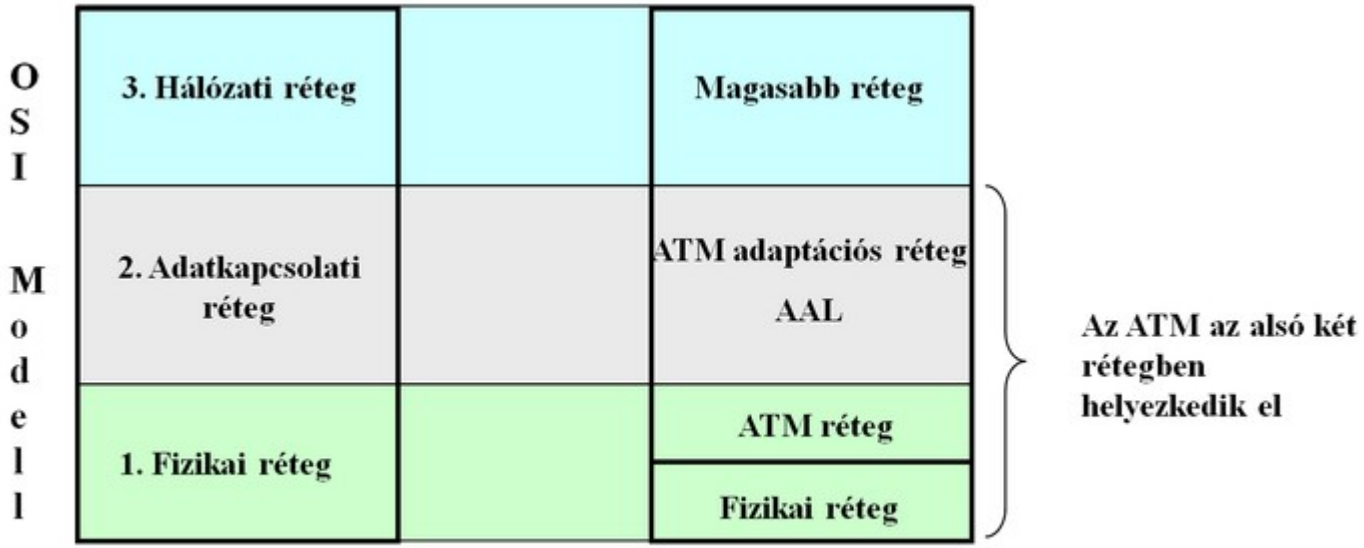
X.25: Eredeti protokollok leírása 1976. Az akkor aktuális hálózati feltételekre szabott protokollkészlet. Többszörös hibaellenőrzés.

Frame relay: Hasonló működésű az X.25-höz, de a technológiai fejlesztéseknek köszönhetően a redundáns hibaellenőrzés már nem szükséges. (Felsőbb rétegben kell megoldani -> TCP)

ATM (Asynchronous Transfer Mode): Fix cellamérettel dolgozik, melynek köszönhetően jelentésen javítható az átvitel sebessége.
Manapság ez a legszélesebb körben használatos megoldás. (2016)

Adatkapcsolati réteg - WAN

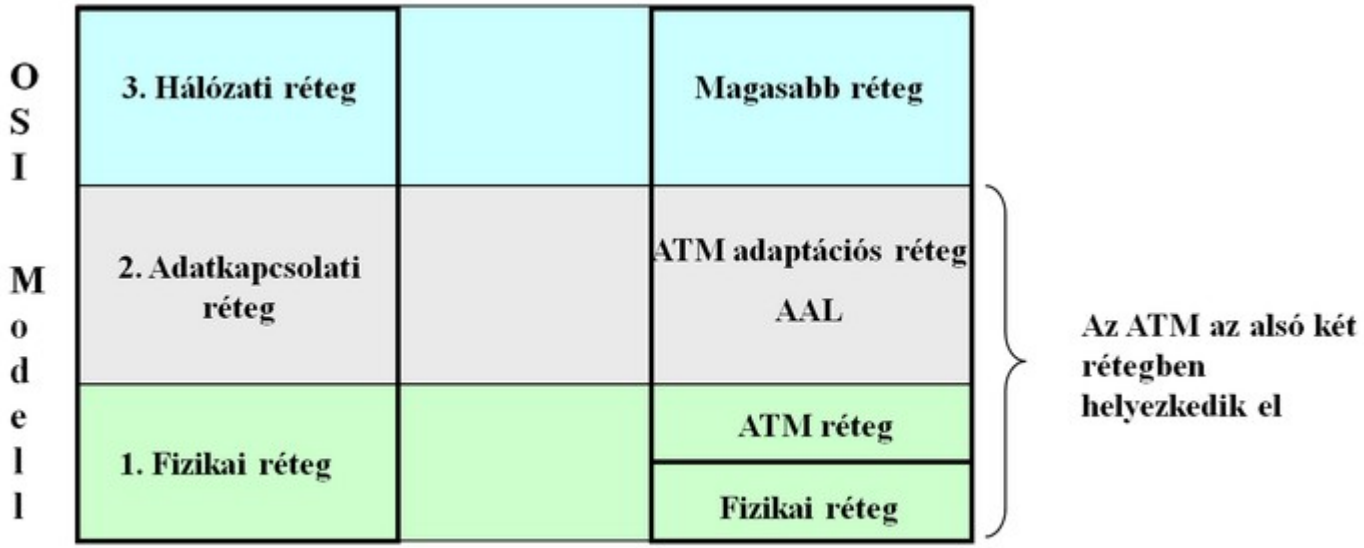
ATM (Asynchronous Transfer Mode): Az ATM hálózat különböző szolgáltatásokat kínál a különböző típusú alkalmazások számára. Az ATM adaptációs réteg kínálja ezeket a szolgáltatásokat az alkalmazások számára, és fedi el a cellakapcsolást, amellyel az átvitelt az alsó két réteg végzi.



Az ATM funkcionális rétegei

Adatkapcsolati réteg - WAN

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.

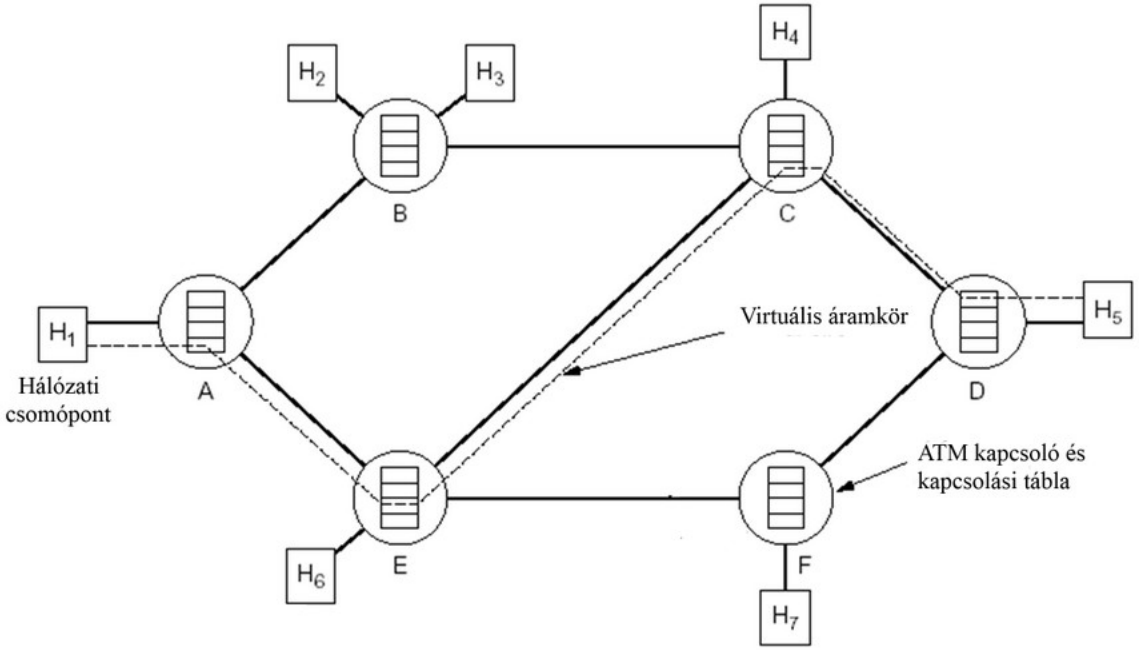


Az ATM funkcionális rétegei

Adatkapcsolati réteg - WAN

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 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).

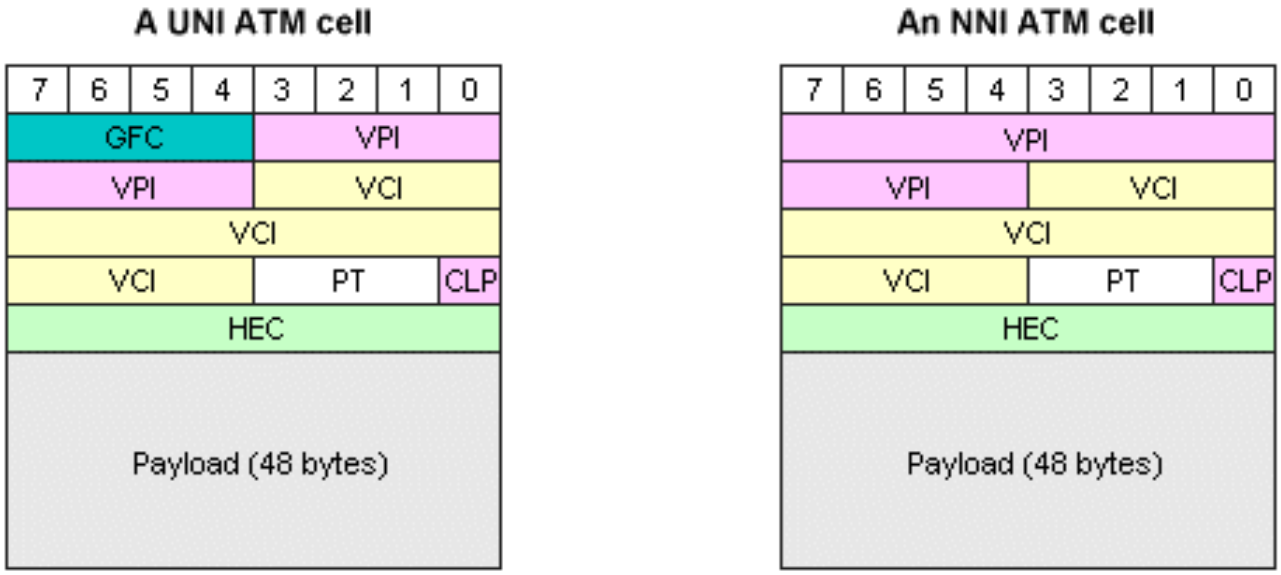


Adatkapcsolati réteg - WAN

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 egy ún. "UNI - User to Network Interface" típusú cellaformátumot használ a szolgáltatói oldal elérésére.
- Az ATM kapcsolók egymás között pedig egy ún. "NNI - Network Node Interface" típusú cellaformátumot használnak.



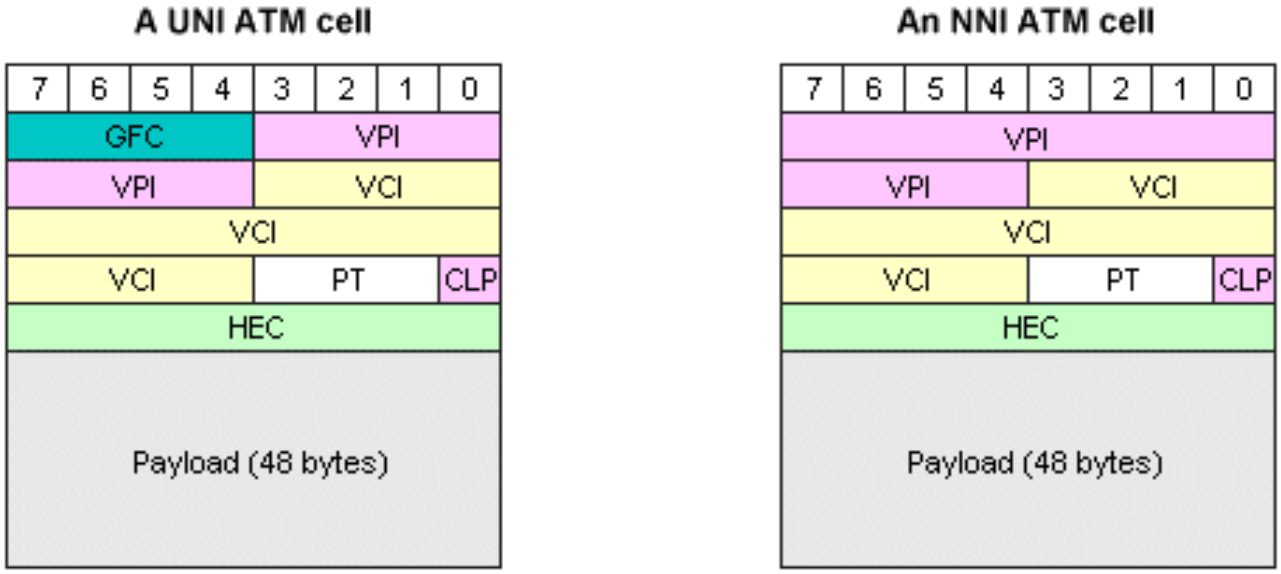
u.l.:2016.03.25.
http://www.technologyuk.net/telecommunications/communication_technologies/asynchronous_transfer_mode.shtml

Adatkapcsolati réteg - WAN

Mindkét cella fejrészében az egyik legfontosabb 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 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.



u.l.:2016.03.25.
http://www.technologyuk.net/telecommunications/communication_technologies/asynchronous_transfer_mode.shtml

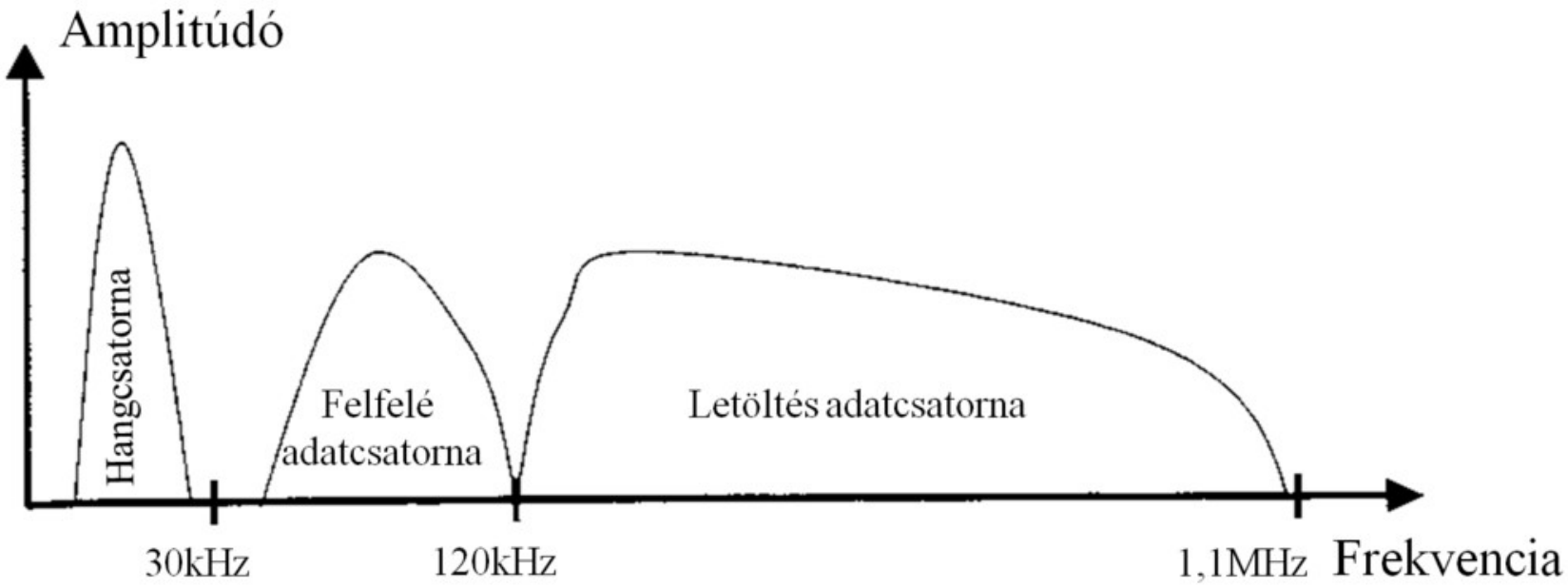
ADSL

ADSL (Asymmetric Digital Subscriber Line)

- A felhasználók letöltéséhez nagy(obb) sávszélesség szükséges.
- Az adatfeltöltéshez kisebb sávszélesség is elegendő.

Ennek következtében a rendelkezésre álló sávszélességet (frekvenciatartományt) aszimmetrikus módon célszerű felosztani.

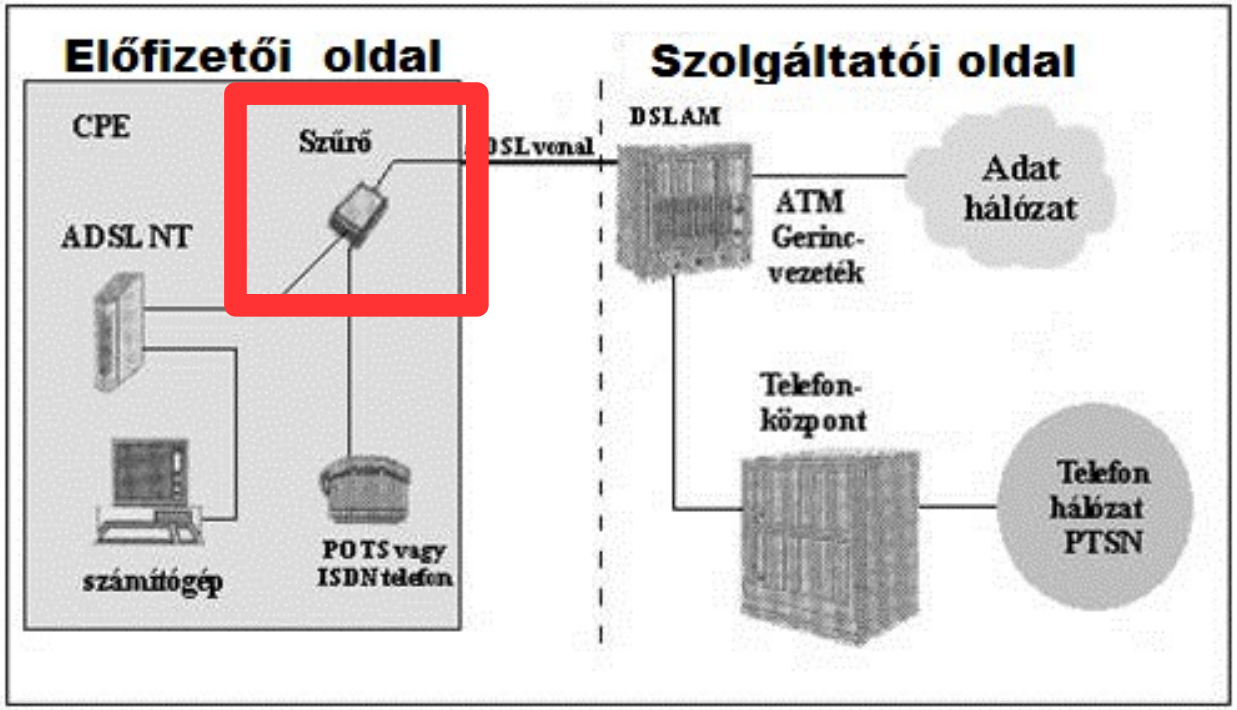
Az ADSL alapvetően FDM alapon osztja fel a csatornát a három kommunikációs cél (hang, adatfeltöltés, adatletöltés) között.



ADSL

Az ADSL rendszertechnikai felépítése

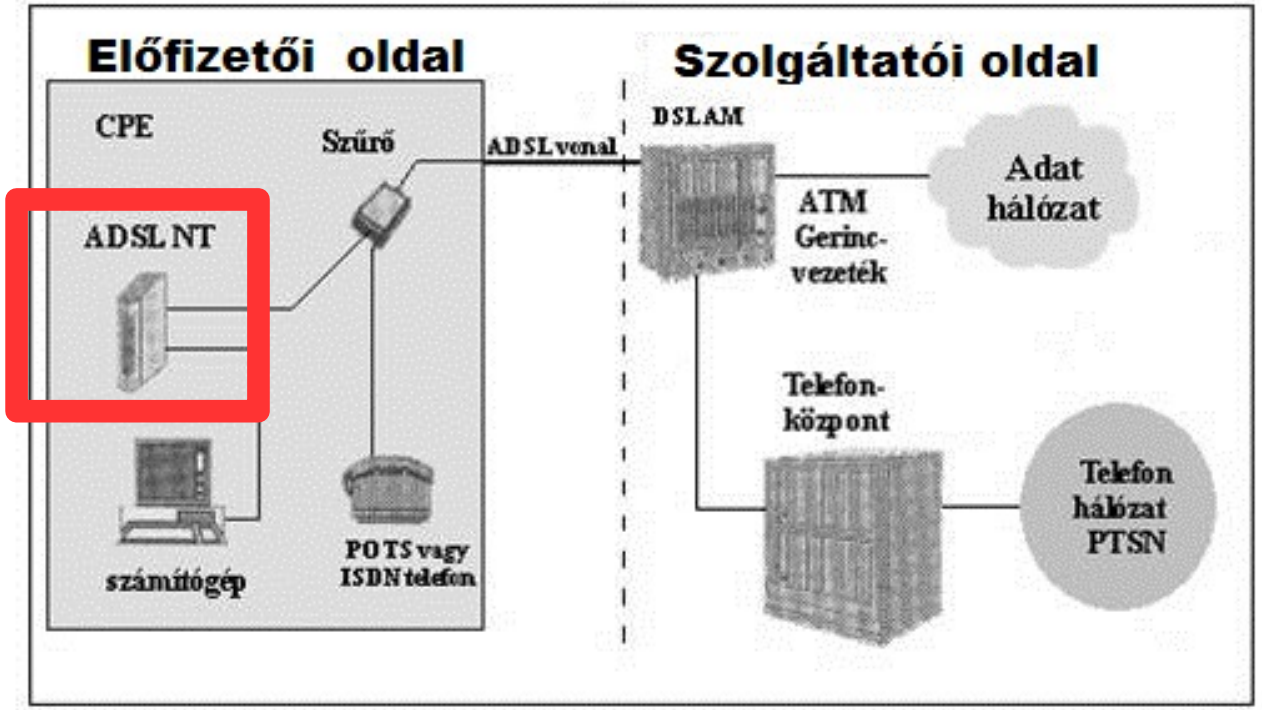
Az ADSL előfizetői oldalán az előfizetői vonal (helyi hurok, local loop) végén egy szűrővel különítik el a hang- és adatátviteli frekvenciatartományokat.



ADSL

Az ADSL rendszertechnikai felépítése

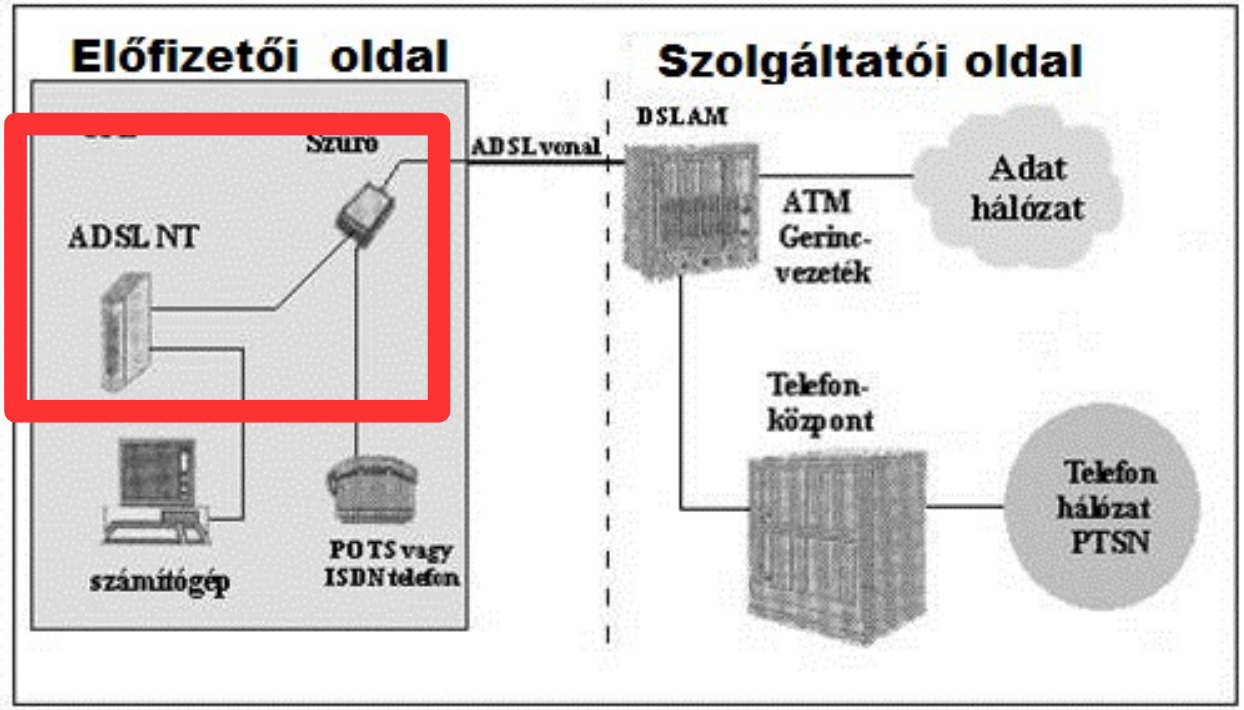
A szolgáltatói hálózat végpontját az ADSL NT (Network Termination, vagy ADSL modem) eszköz képviseli. Ennek kimenete egy hálózati csatlakozásra közvetlen módon használható (tipikusan RJ-45) interfész, melyre az előfizető Ethernet (vagy autentikációs célok miatt PPP over Ethernet) technológiával kapcsolódik.



ADSL

Az ADSL rendszertechnikai felépítése

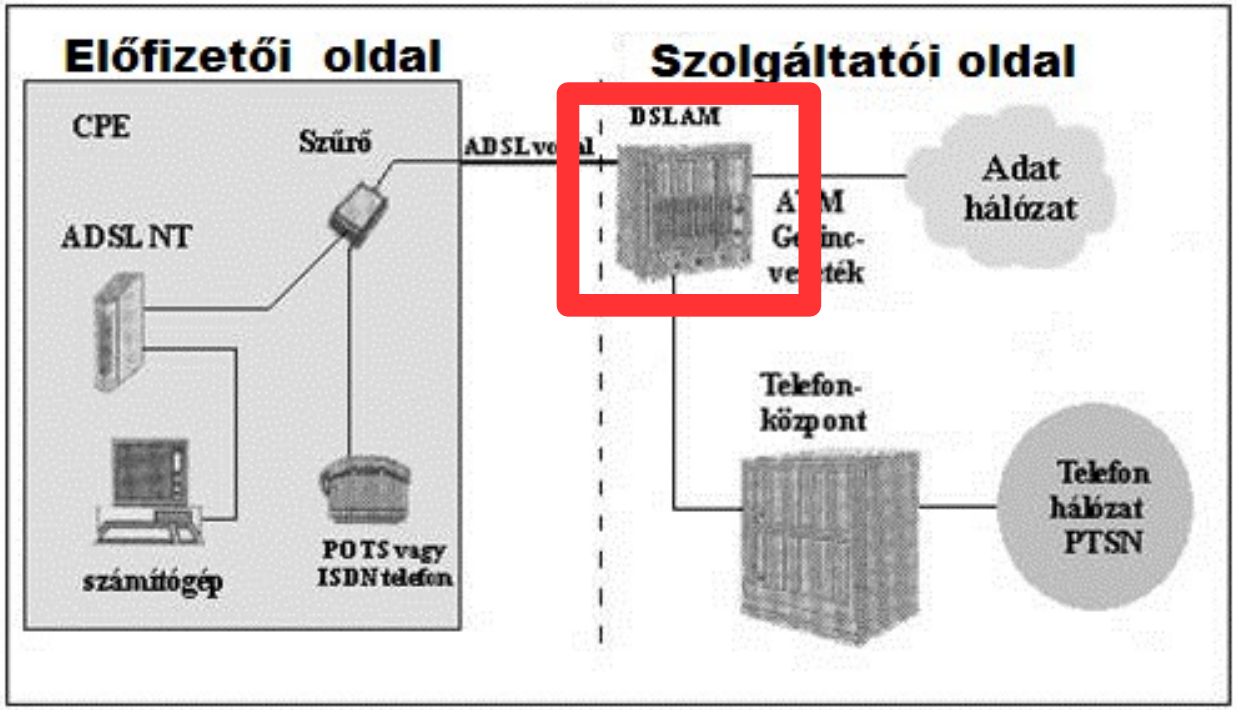
A szűrőt és az ADSL NT-t természetesen egyetlen eszközben is implementálhatják, s esetlegesen további (pl. forgalomirányítási) funkciókkal is kiegészíthetik.



ADSL

Az ADSL rendszertechnikai felépítése

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



MPLS

Multiprotocol Label Switching (MPLS)

Az MPLS egy protokollfüggetlen adatátviteli technológia, amennyiben tetszőleges adatkapcsolati réteg (úgy mint ATM, frame relay) fölött üzemelhet.

Működésének lényege, hogy a hálózaton címkeutakat (label path) alakítanak ki, ahol az egyes MPLS útvonalválasztók csupán a csomagokra rakott címke alapján döntik el, hogy merre továbbítsák azt.

Az útvonalválasztók különböző műveleteket is végezhetnek a címkéken, így újabb címkét tehetnek a csomagra, kicserélhetik a meglévő címkét, vagy el is távolíthatják azt. Az útvonalválasztók egymás között a Label Distribution Protocol (LDP) segítségével alakítják ki az utakat.

(https://hu.wikipedia.org/wiki/Multiprotocol_Label_Switching) u.l. 2016.10.17.

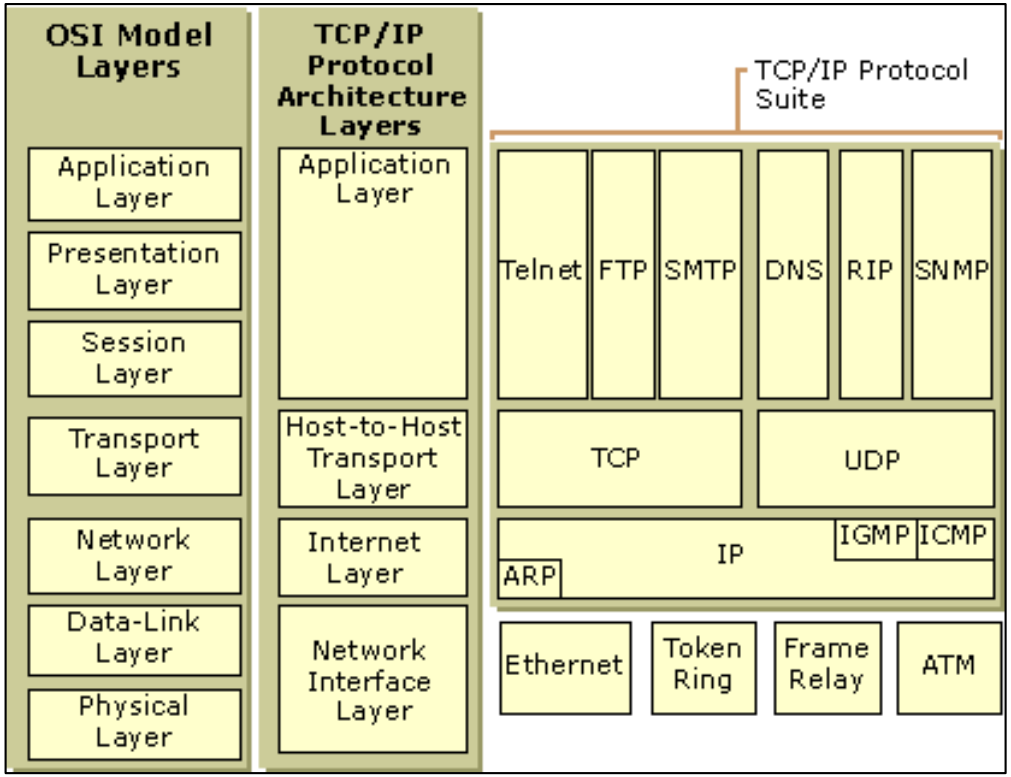
Az MPLS-ről bővebben (ul.: 2016.10.17.):
https://www.nanog.org/meetings/nanog49/presentations/Sunday/mpls-nanog49.pdf

A hálózati réteg

A hálózati réteg protokolljai

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

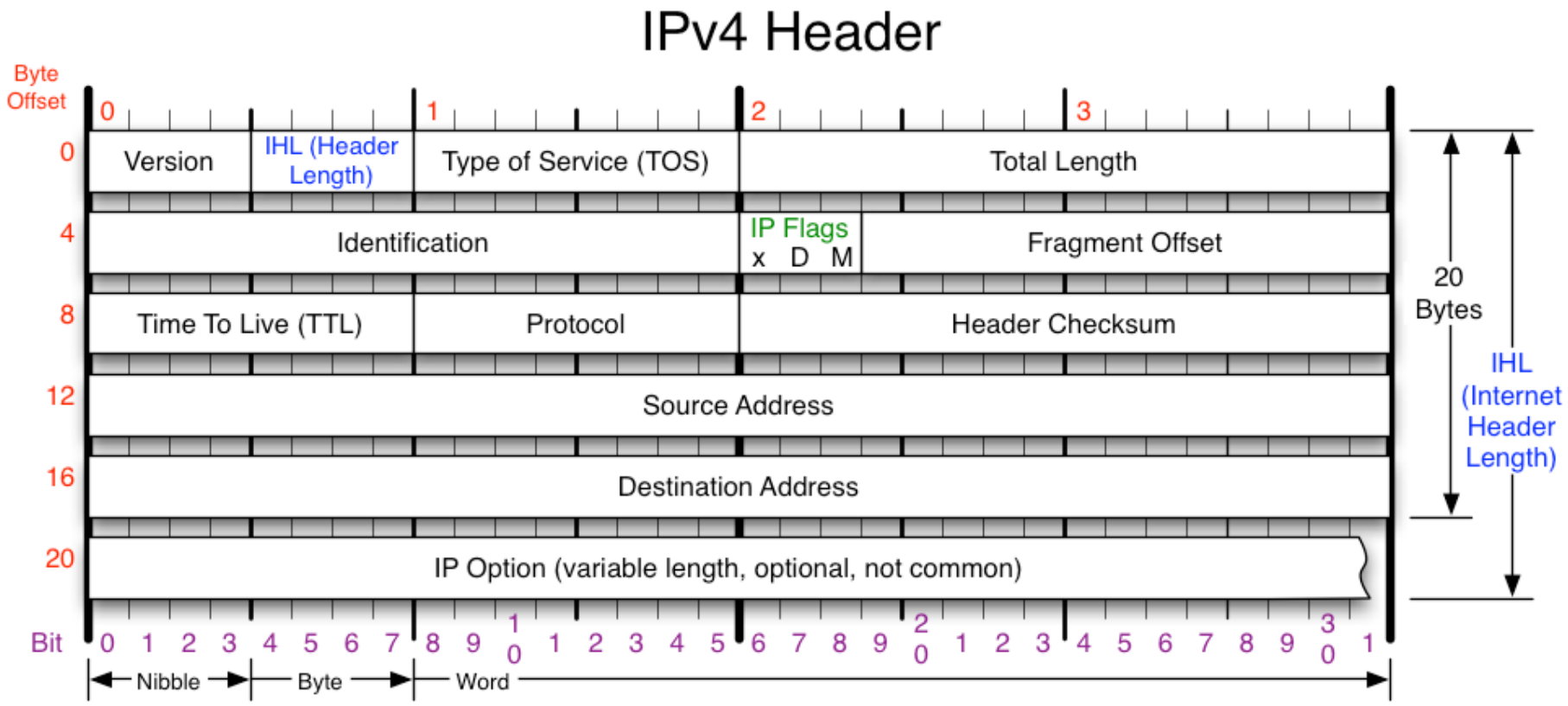
IP protokoll: Az IP (Internet Protocol, RFC 791) a TCP/IP referenciamodell általános adatszállításra szolgáló hálózati réteg protokollja. Összeköttetés mentes (datagram) szolgáltatást nyújt a szállítási réteg felé.



https://technet.microsoft.com
TCP/IP Protocol Architecture (2015.10.)

Az Interet Protokoll

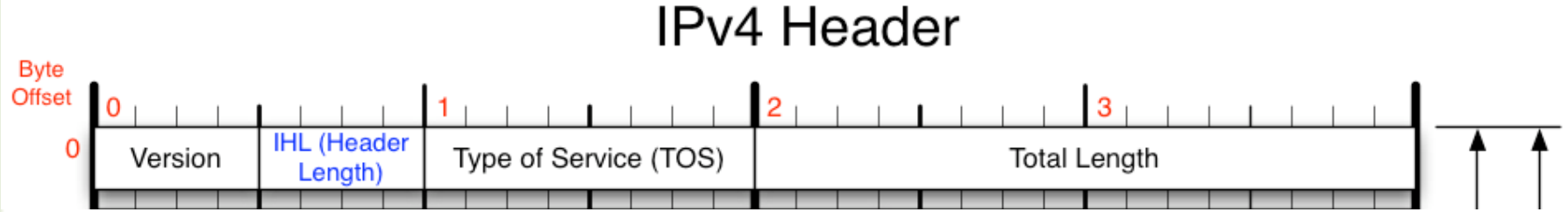
IP



Az IP fejrész minimum 5, maximum 15 db 32 bites szóból áll. Az Ethernet keret típusmezőjének értéke 0x0800 (lásd 99. dia).

https://ask.wireshark.org/questions/32097/how-to-interpret-ipv4-header/32123

IP

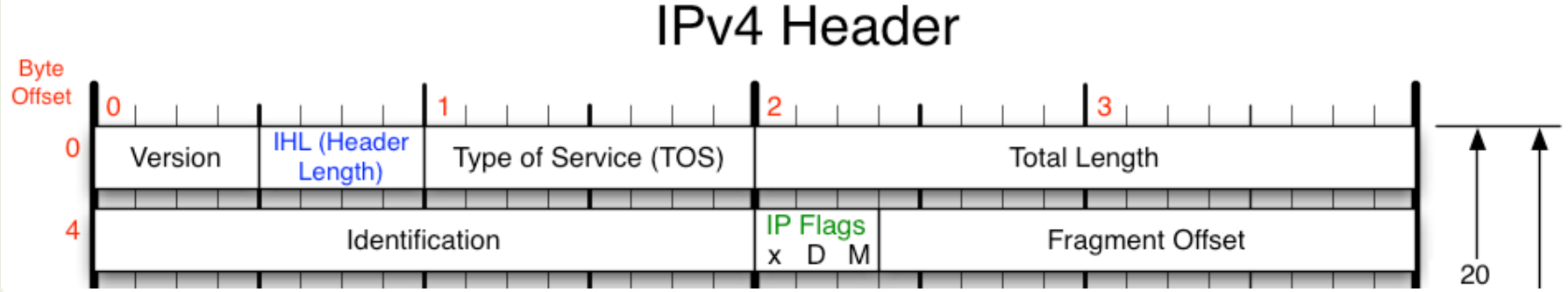


Az első szó általános információkat tartalmaz:

- Verziószám (4 vagy 6)
- IP fejrész hossza (szavakban) (min 5, max 15)
- szolgáltatás típusa (Type of Service) (A szolgáltatással szemben elvárt minőségi szint. Pl: Best effort, prioritásos, kritikus...)
- adatmező hossza (bájtokban mérve).

https://ask.wireshark.org/questions/32097/how-to-interpret-ipv4-header/32123

IP



Második szó: a csomag darabolásával kapcsolatos információk:
Darabolásra akkor van szükség, ha a csomag (túl nagy mérete miatt) nem ágyazható be az adatkapcsolati réteg keret adatmezőjébe. (lásd MTU)

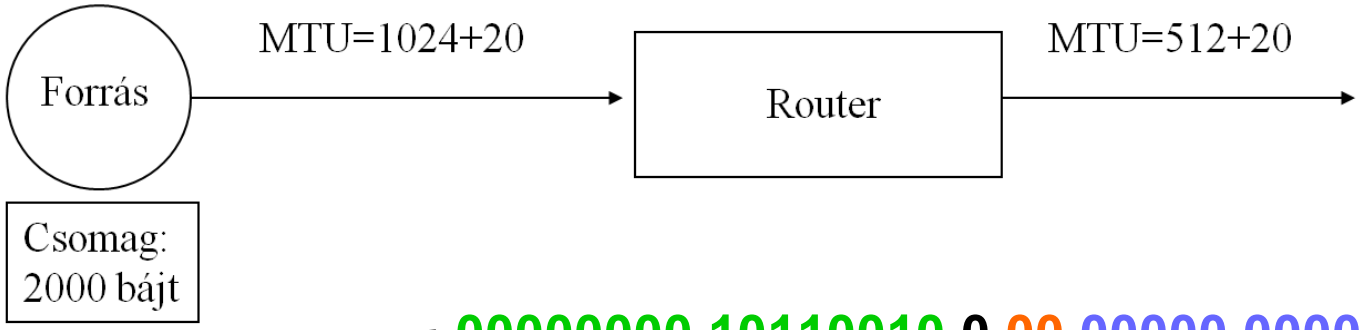
- Az azonosító a csomagdarabok összetartozását jelzi.
- X: 2003 április 1. óta “evil bit” (RFC 3514)
- A DF jelzőbit a csomag darabolhatatlan voltát jelzi.
- Az MF jelzőbit 0 értéke jelzi, hogy az adott darab (fragment) a sorozat utolsó eleme.
- Az offset érték a darab eredeti csomagbeli helyét mutatja (8 bájtos egységben mérve).

https://ask.wireshark.org/questions/32097/how-to-interpret-ipv4-header/32123 u.l. 2016.08.

IP

IP datagram 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.



Az eredeti csomag 2. szava

00000000 10110010 0 00 00000 00000000

A két új csomag második szava

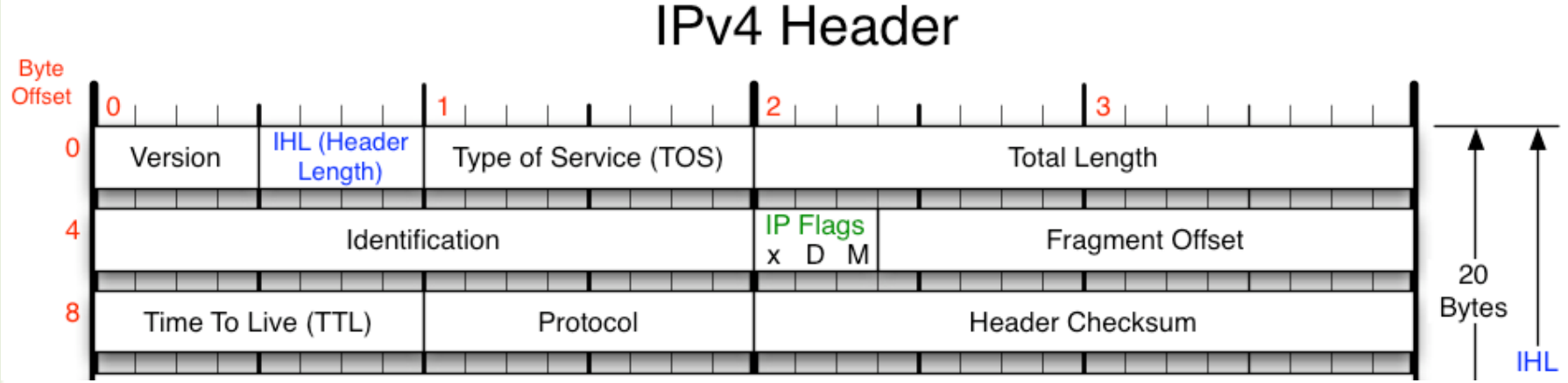
00000000 10110010 0 01 00000 00000000
00000000 10110010 0 00 00000 10000000

offset=128*8=1024

A négy új csomag második szava
offset: 0,, 512, 1024, 1536

00000000 10110010 0 01 00000 00000000
00000000 10110010 0 01 00000 01000000
00000000 10110010 0 01 00000 10000000
00000000 10110010 0 00 00000 11000000

IP

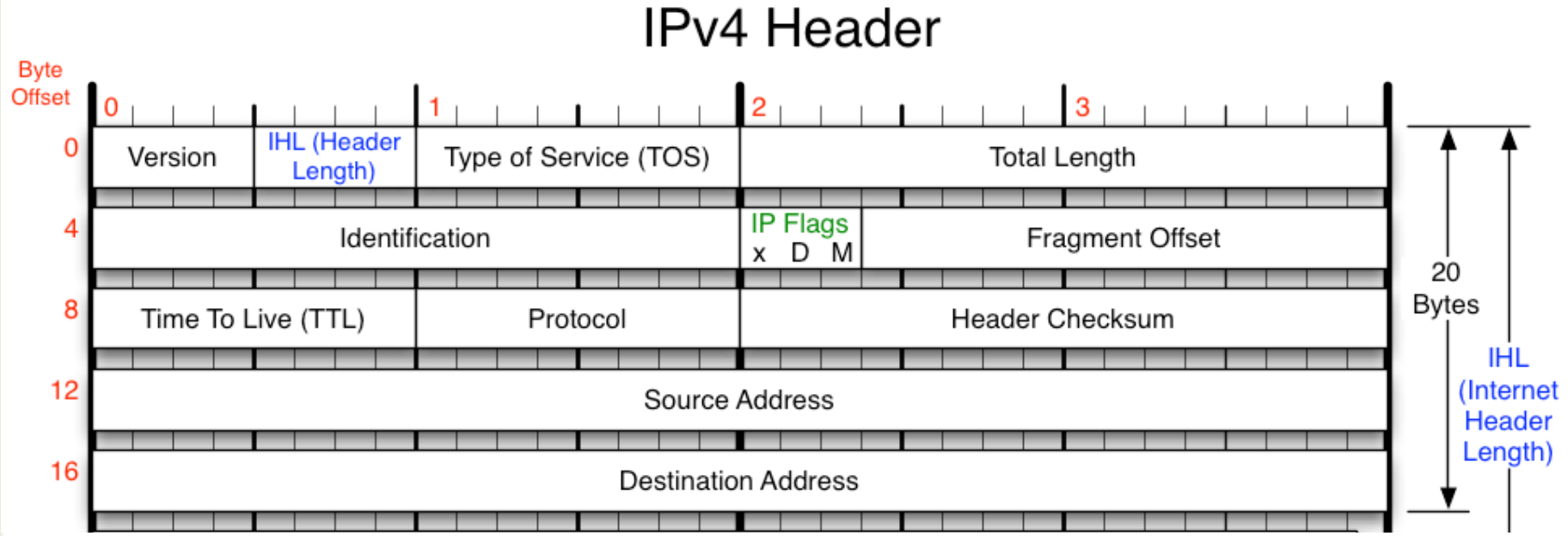


Harmadik szó: általános információk:

- 8 bit: TTL (Time To Live) 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.

https://ask.wireshark.org/questions/32097/how-to-interpret-ipv4-header/32123

IP

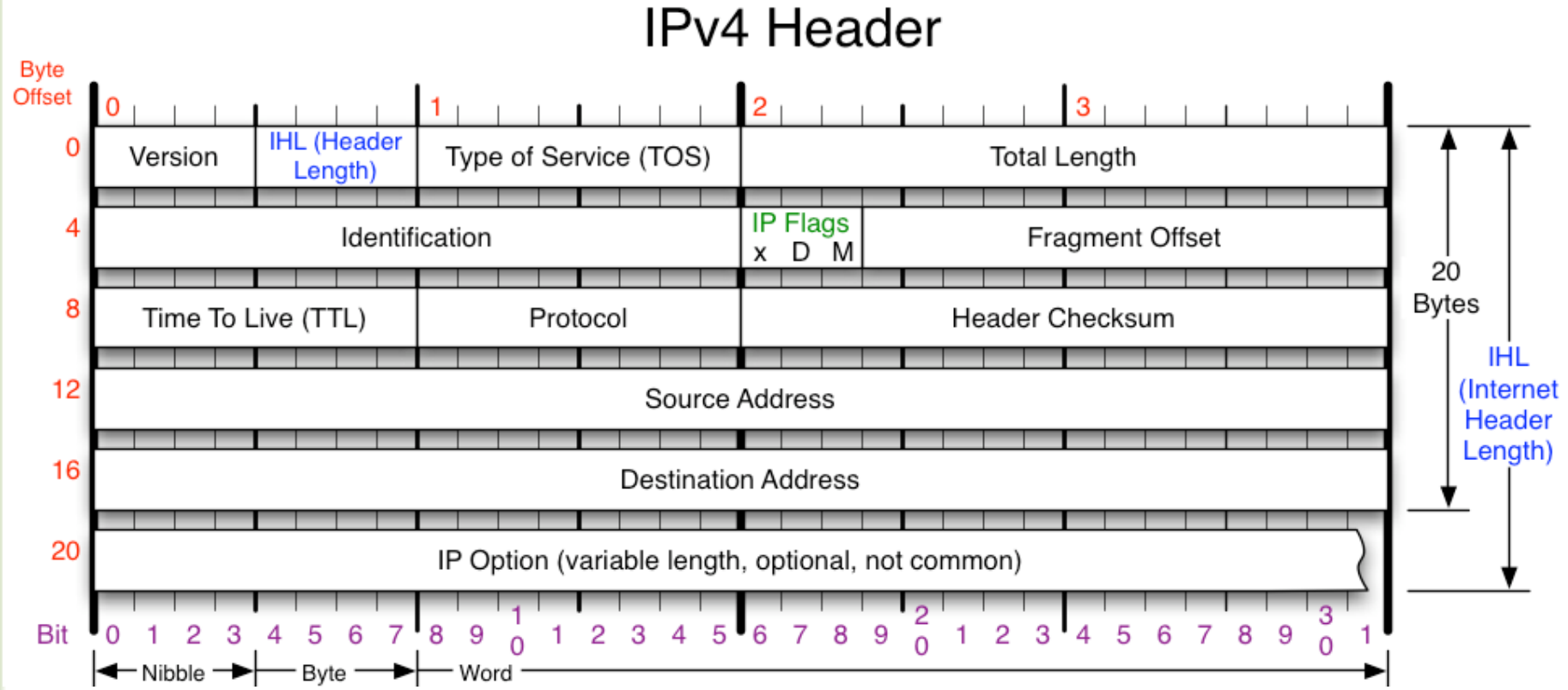


Negyedik és ötödik szó – cím információk:

- A negyedik szó tartalmazza a feladó IPv4 címét,
- Az ötödik szó tartalmazza a címzett Ipv4 címét

https://ask.wireshark.org/questions/32097/how-to-interpret-ipv4-header/32123

IP



Hatodik szótól: 32 bites opcionális információk:

pl.:

Record route - A továbbítás útvonalának naplózása.

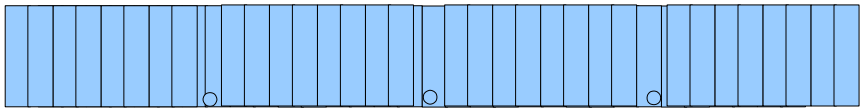
Timestamp - A késleltetési idők naplózása.

https://ask.wireshark.org/questions/32097/how-to-interpret-ipv4-header/32123 u.l. 2016.08.

IP cím

IP cím: hierarchikus logikai azonosító. A hálózaton minden csomópontnak rendelkeznie kell ***legalább egy*** IP-címmel.

Felépítése: 4 bájtos azonosító pontozott decimális formában (8 bitenként)



Netmaszk: Olyan 32 tagú bitsorozat, melyben 1 értékkel helyettesítettük a kapcsolódó IP-cím hálózati azonosító bitjeit és 0-val a csomópont azonosító biteket.

Prefix hossz: a netmaszk elején elhelyezkedő 1-ek száma

Példa: 17 prefix hosszú netmaszk:

```
11111111 11111111 10000000 0000000
```

Címosztályok

Osztály	Prefix	Netmaszk	Első bitek	Tartomány
A	8	255.0.0.0	0..	0-127
B	16	255.255.0.0	10...	128-191
C	24	255.255.255.0	110...	192-223

D – multicast címek

E – speciális célra fenntartva

Speciális IP címek:

0 … 0: aktuális gép (nem lehet célcím)

0 … 0 hoszt: aktuális hálózaton a hoszt (nem lehet célcím)

hálózat 0 … 0: hálózatazonosító

hálózat 1 … 1: üzenetszórás a hálózaton

1 … 1: üzenetszórás saját hálózaton

127.bármi: loopback

ICMP

Az ICMP (Internet Control Message Protocol) az 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

Minden ICMP csomag tartalmaz 3 mezőt (Típus, kód, ellenőrző összeg)
A típus adja meg a csomag jellegét. Nagyságrendileg 30 különböző ICMP típus létezik. ICMP-t használ például a ping (Echo request csaomag küldésével).
A kód a típushoz tartozik, az ellenőrző összeg segítségével pedig a csomag integritását ellenőrizhetjük.

http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml u.l. 2016.08.

IP forgalomirányítás alapok

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

Forgalomirányítási táblázat (routing table): A forgalomirányításhoz szükséges információkat tartalmazó táblázat. Tipikus (legfontosabb) mezők: `célháló, netmaszk, kimenő interfész, következő csomópont (gateway), 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).

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

Forgalomirányítás fogalmak

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) kategória:
– Távolság alapú (költség alapú) metrika.
– Jóság alapú metrika.

Forgalomirányítók (alapvető) működése

1. A router az input interfészen érkező csomagot fogadja. !
2. A router a csomag célcímét illeszti a routing táblázat soraira.
3. Ha a célcím több sorra illeszkedik, akkor a leghosszabb prefixű sort tekintjük illeszkedőnek.
4. Ha nem létezik illeszkedő sor, akkor a cél elérhetetlen, a csomag nem továbbítható.
5. A csomagot a router eldobja és ICMP hibajelzést küld a feladónak.
6. 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

Forgalomirányítók (alapvető) működése

Útválasztás a gyakorlatban:

- netmaszk prefix hossz alapján csökkenő sorrendben haladok a bejegyzéseken
- az IP-t maszkolom a megfelelő netmaszkkal
- ha a megfelelő célhálót kapom vissza, elküldöm a csomagot a megfelelő átjáróra, egyébként lépek a következő sorra
- az alapértelmezett átjáró sora bármely címre megfelel

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
193.6.135.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U     1002   0        0 eth0
0.0.0.0         193.6.135.1     0.0.0.0         UG    0      0        0 eth0
```

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.

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.

IP problémák

Kiosztott hálózati azonosítók száma és aránya 1992 (RFC 1466)

	Összes	Kiosztott	Kiosztott %
A osztály	126	49	38%
B osztály	16383	7354	45%
C osztály	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 eredménye volt, hogy a "B" osztályú hálózatazonosítók a teljes kimerülést közelítették (1992: 45%)

Az Internet gerinchálózati útválasztóinak irányító tábla mérete ebben az időben a kiosztott hálózati azonosítók számával volt arányos..

CIDR

Rövidtávú megoldás: CIDR (Classless Inter Domain Routing)
A hálózat-gép határvonalat nem statikus módon (osztály alapon) helyezzük el, hanem az igényelt csomópont-darabszám alapján az igényeket lefedő legalkalmasabb pozícióra állítjuk

Az irányítási táblák növekedési problémáinak kezelésére területi elrendeződés szerinti címtartomány-zónákat alakítottak ki.

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

CIDR

CIDR 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:
A: 194.24.0.0 - 194.24.7.255; <194.24.0.0, 255.255.248.0> (2048 cím)
B: 194.24.16.0 - 194.24.31.255; <194.24.16.0, 255.255.240.0> (4096 cím)
C: 194.24.8.0 - 194.24.11.255; <194.24.8.0, 255.255.252.0> (1024 cím)

NAT

Középtávú megoldás: NAT (Network Address Translation)

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.

NAT

Középtávú megoldás: NAT (Network Address Translation)

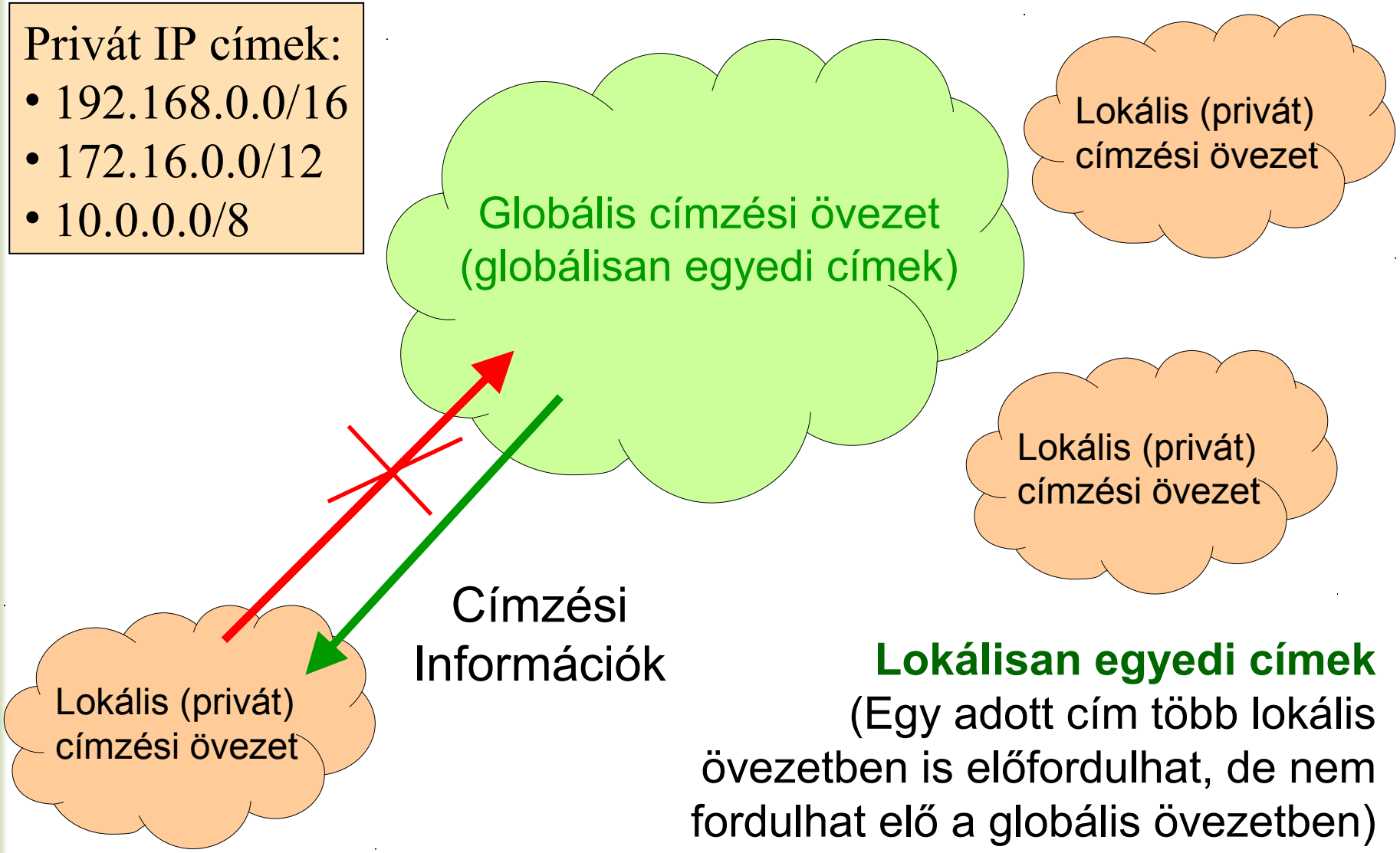
Belső hálózat (Private/Local Network): Az intézmény saját (belső, privát) címzéssel rendelkező címzési övezete. A belső hálózatban használt címek a világon nem egyediek, mert másik intézményben működtetett belső hálózatban ismételten megjelenhetek.

A belső hálózatban használható címtartományokat az RFC 1918 dokumentumban rögzítették:

Méret	Tartomány	Prefix	Osztályok szerinti leírás	Legnagyobb CIDR blokk
24 bites blokk	10.0.0.0-10.255.255.255	/8	1db A osztályú blokk	10.0.0.0/8
20 bites blokk	172.16.0.0-172.31.255.255	/12	16db folytonos B osztályú blokk	172.16.0.0/12
16 bites blokk	192.168.0.0-192.168.255.255	/16	256db folytonos C osztályú blokk	192.168.0.0/16

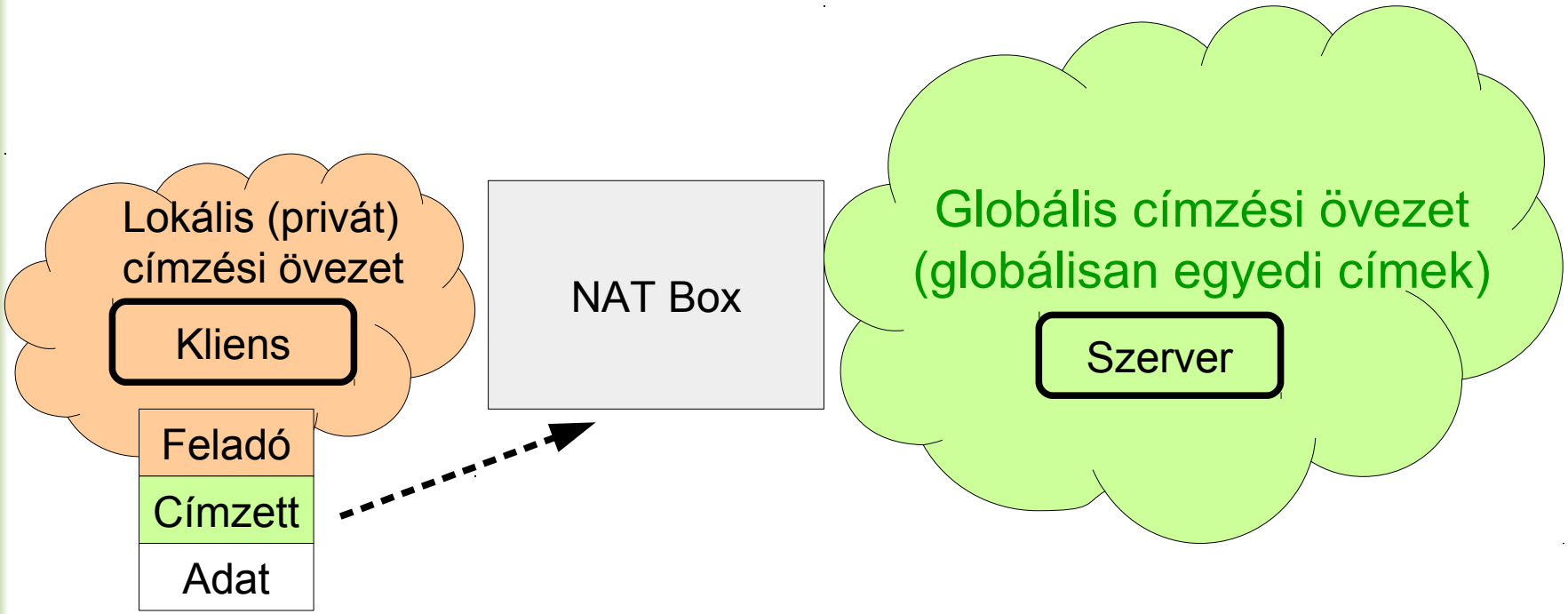
NAT működése

Privát IP címek:
- 192.168.0.0/16
- 172.16.0.0/12
- 10.0.0.0/8



Lokálisan egyedi címek
(Egy adott cím több lokális övezetben is előfordulhat, de nem fordulhat elő a globális övezetben)

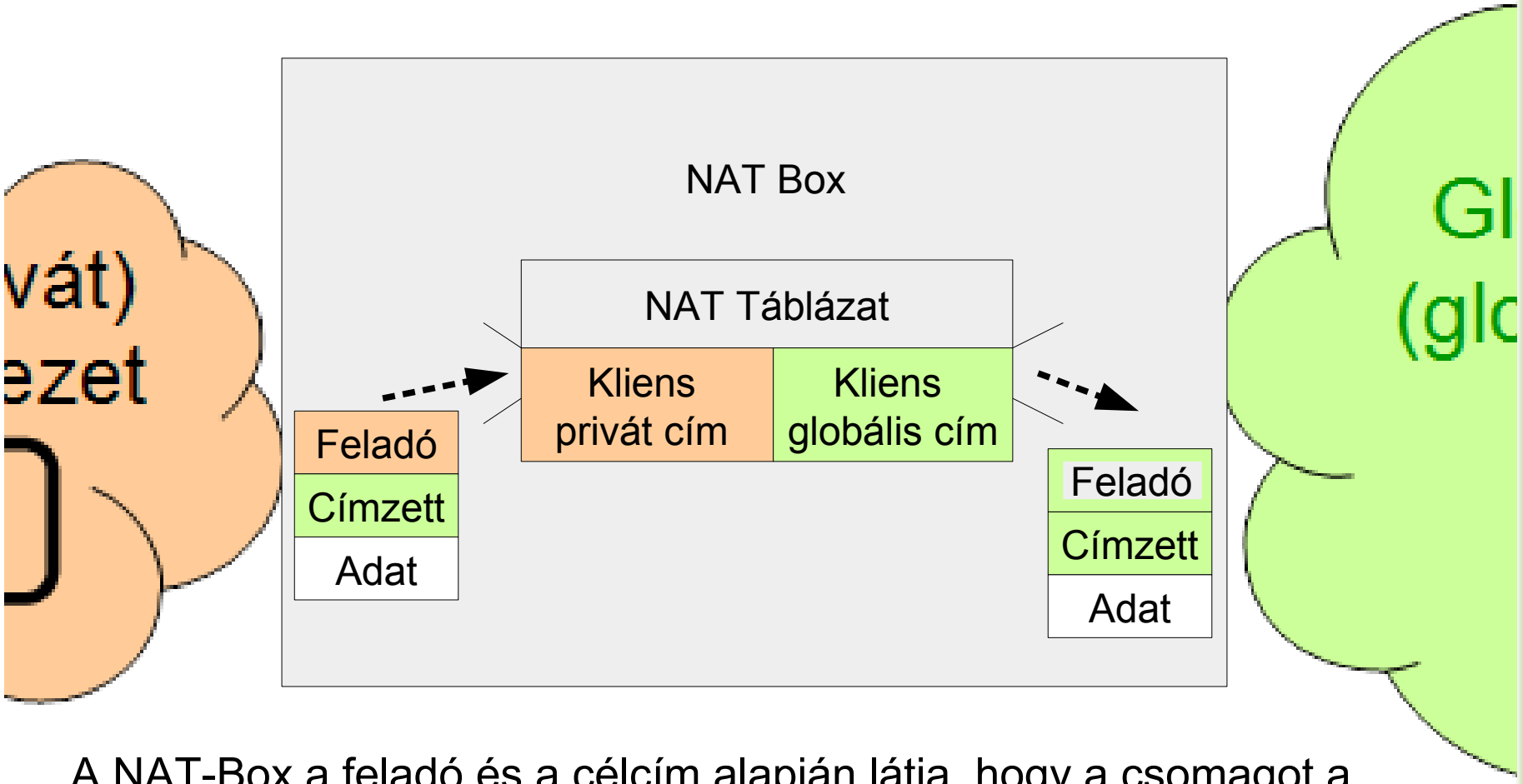
NAT működése



A klasszikus címfordítás (Basic NAT) esetében a kliens egy belső, a szolgáltatást nyújtó szerver pedig a külső, globális hálózatban van.

Az első csomagot a kliens küldi a szerver felé, a csomagban célcímként a szerver globális címe, feladó címként pedig a kliens privát címe szerepel.

NAT működése

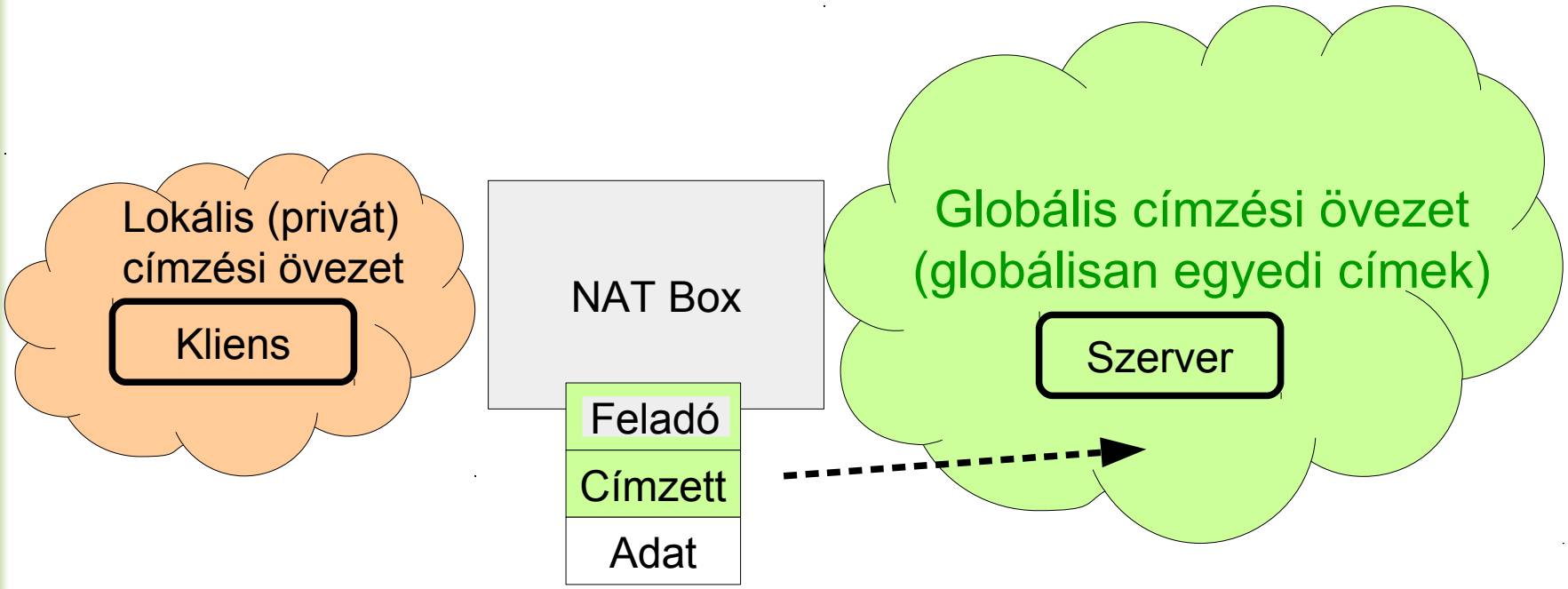


A NAT-Box a feladó és a célcím alapján látja, hogy a csomagot a külső hálózat felé kell továbbítani.

Lecseréli a kliens privát címét egy külső (publikus) címre.

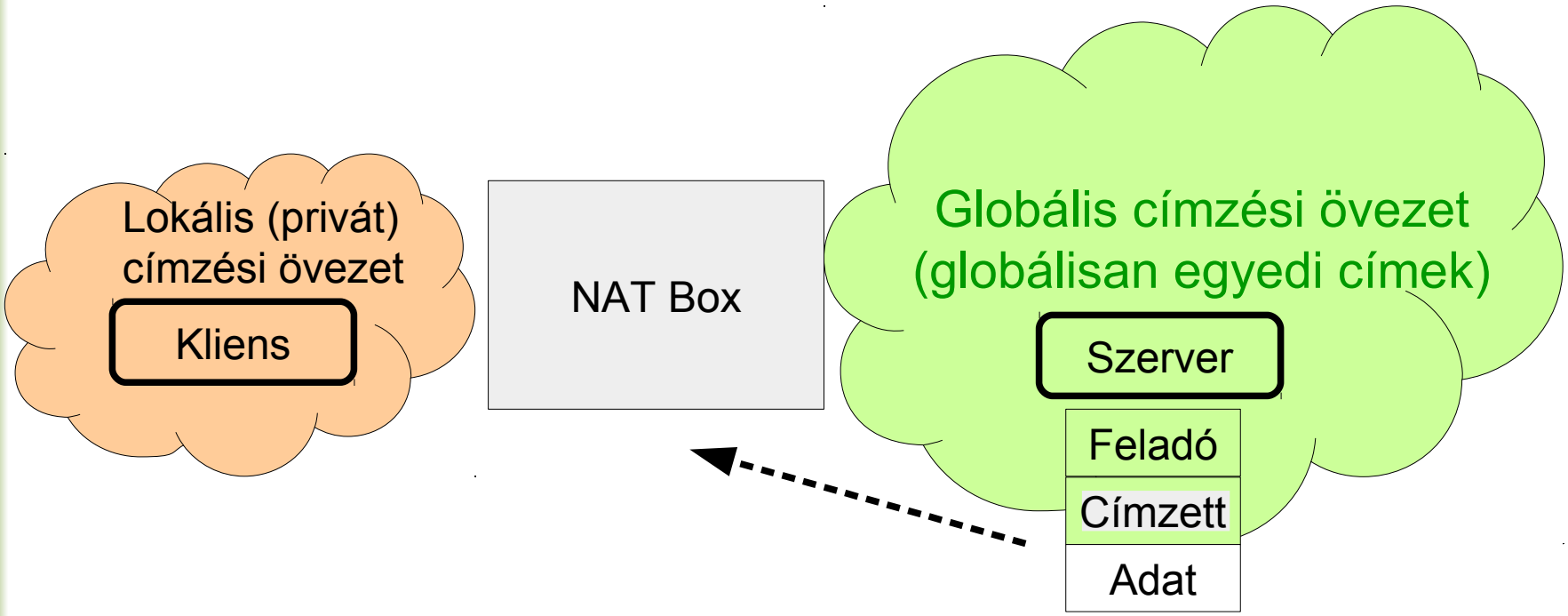
Egy táblázatban (címfordító tábla) feljegyzi a címcserét.

NAT működése



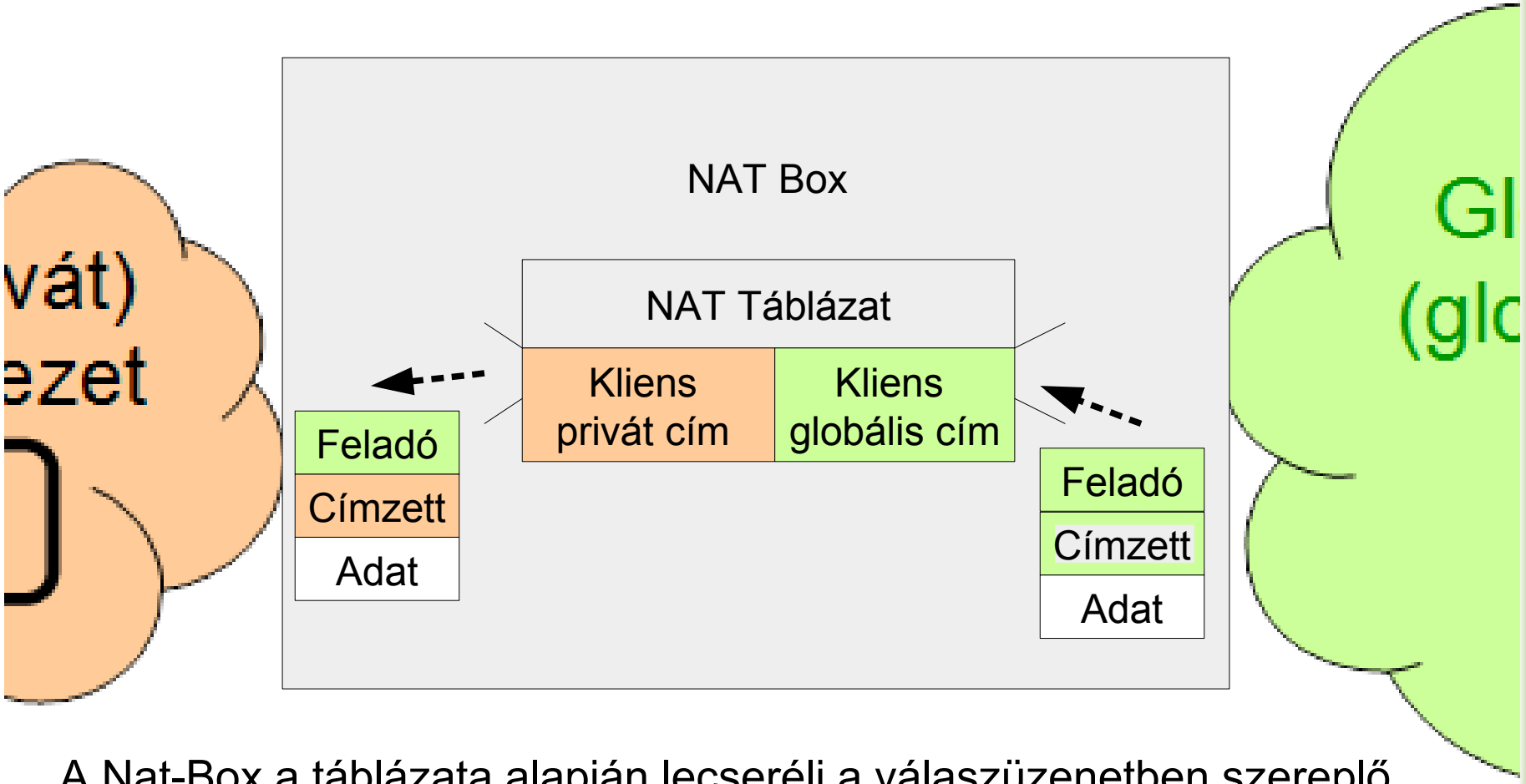
A NAT Box az új feladócímmel indítja a csomagot külső hálózatban a szerver felé.

NAT működése



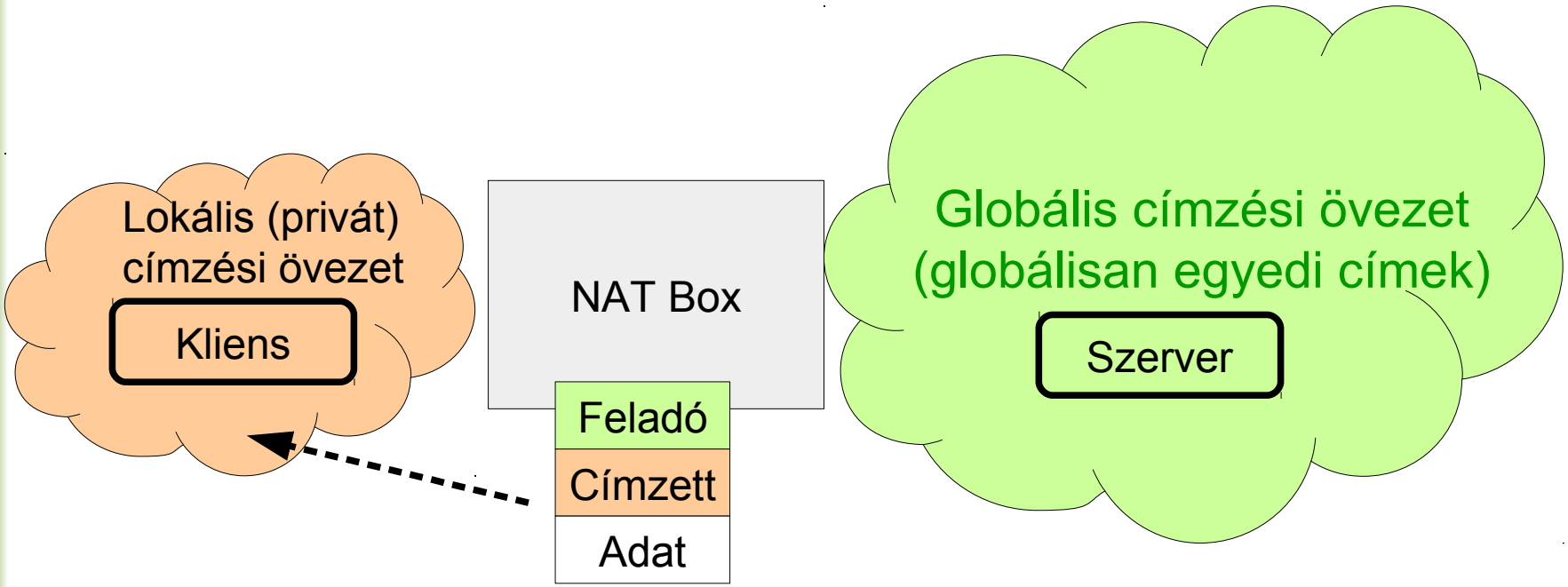
A szervertől érkező válaszüzenet a címfordítóhoz érkezik, s a Nat-Box a válaszüzenetben szerplő célcím alapján felismeri, hogy címtranszlációra van szükség

NAT működése



A Nat-Box a táblázata alapján lecseréli a válaszüzenetben szereplő globális címet a kliens privát címére.

NAT működése



Az így előállított csomagot a NAT Box továbbítja a belső hálózaton a kliens felé.

További magyarázat: http://microchip.wikidot.com/tcpip:nat-translation-table (u.l. 2015.10.)

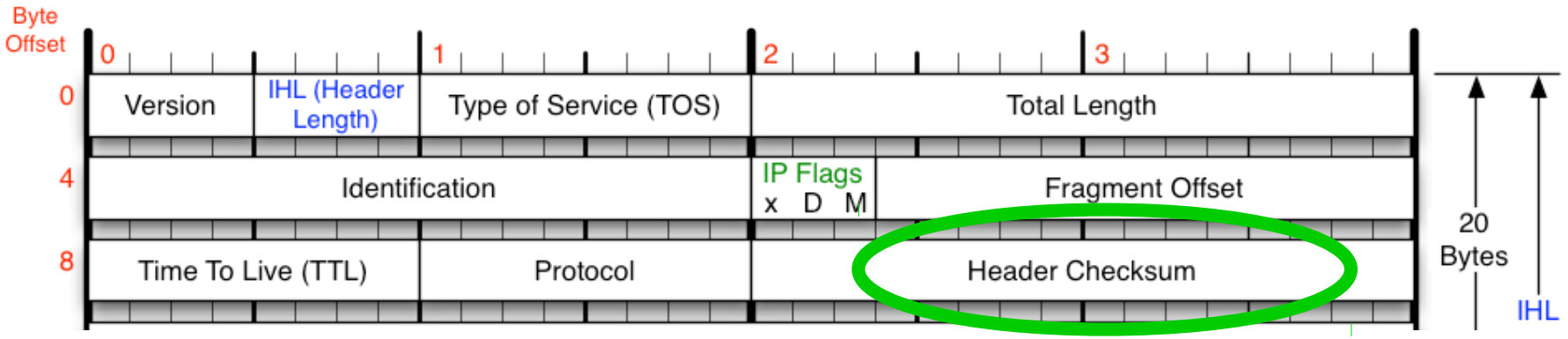
NAT erőforrásigény

A NAT megoldások erőforrás igényesek (processzor).

- Keresés a címtranszformációs táblázatban.
- Címcsere (portszám csere).
- Ellenőrző összegek újraszámítása.

Gyorsítási lehetőség: Nem fontos a teljes PDU-ra elvégezni a számítást:

- Régi ellenőrző összegből „kivonni” a régi címeket.
- A kapott eredményhez az új címek „hozzáadása”.



IPv6

Hosszútávú megoldás: IPv6 (RFC 1883)

Miért van szükség az IPv6-ra?

Az IPv4 korlátozott
- 4,3 milliárd cím, 60% az USA-ban
- egyre növekvő felhasználói populáció
  (pl. ADSL, mobil készülékek, játék konzolok)
- KEVÉS CÍM (a NAT nem megoldás)

Új szolgáltatások IPv6 felett
- pl. mobilitás támogatás

IPv6

Hosszútávú megoldás: IPv6 (RFC 1883)

Újdonságok:

Kiterjesztett címtér
- 128 bit, szemben az IPv4 32 bitjével
- 6,65 * 10^{23} cím/m2 a Földön

Állapotmentes auto-konfiguráció

Egyszerősített fejléc
- összesen 40 byte (16+16+8)
- gyorsabb feldolgozás

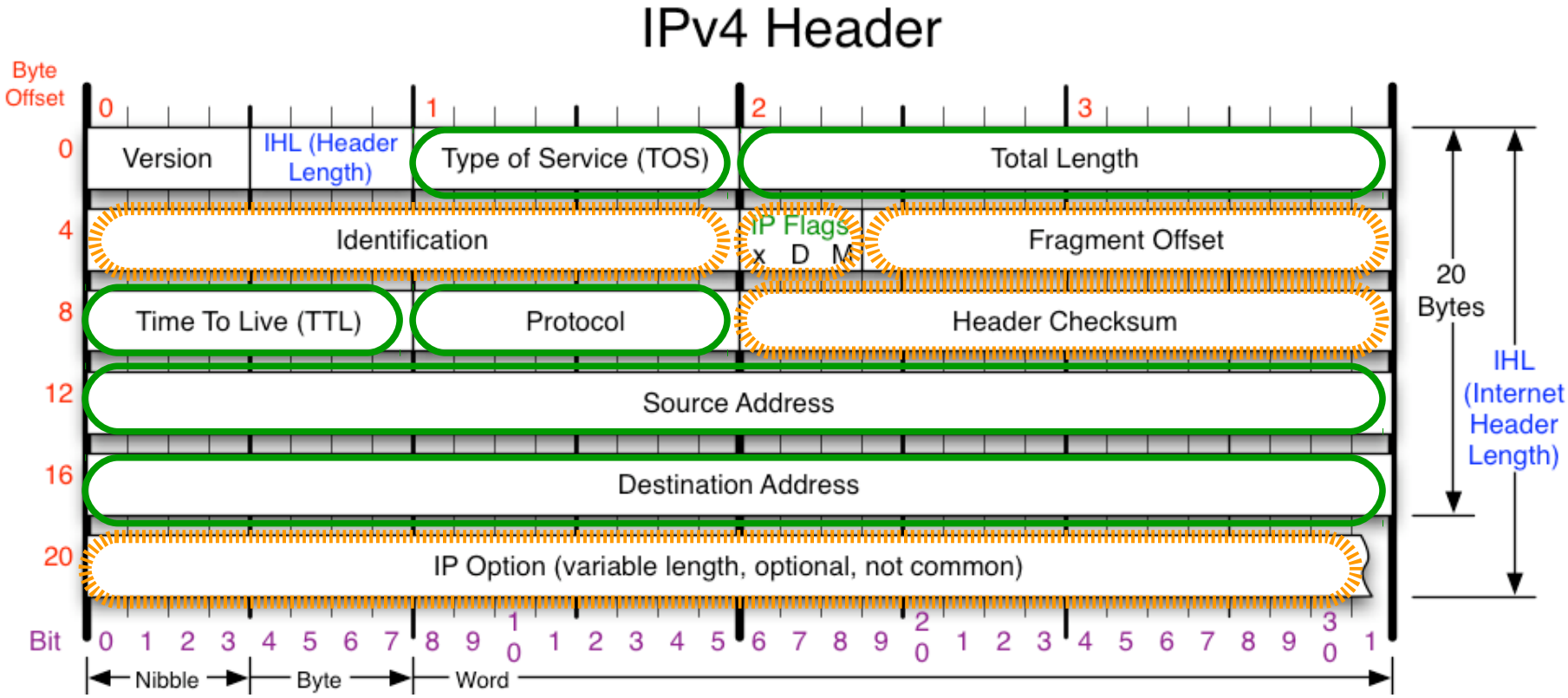
Az opciók és kiterjesztések jobb kezelése
- kiterjesztés fejlécek

IPv6

Változások a fejlécben

törölt

változott



A témáról részletesebben: Szabó Sándor, Bokor László INFOKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK ÉS ALKALMAZÁSOK – IPv6 alapok (2011)

IPv6

Változások a fejlécben

Az alábbi IPv4-es mezık tőntek el:

- Fejléc hossz (fix 40 byte)
- Azonosító
- Flags
- Fragment offset

IPv6-ban nincs darabolás, így ezek a mezők feleslegesek

Fejléc ellenőrző összeg - lassúság

Megváltozott mezők:

Type-of-Service => forgalmi osztály (traffic class)
prioritások kezelése

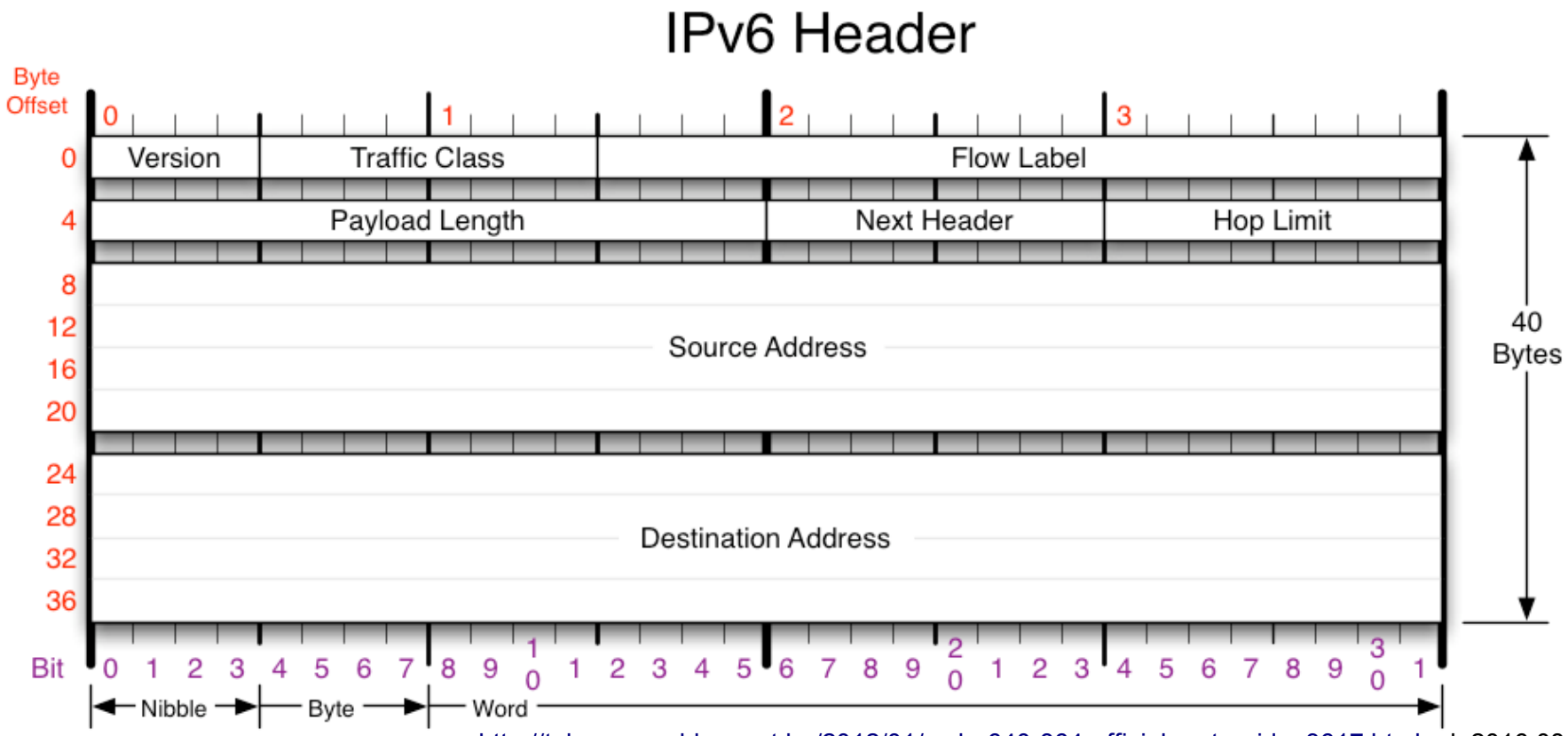
Protocol Type => Next header
TCP, UDP, de kiegészítő fejlécek is, lásd később

Time To Live (TTL) => Hop Limit

Címzett és feladó címe (hosszabb)

Új mező: Folyam azonosító (flow label):
hatékonyabb csomagtovábbítás

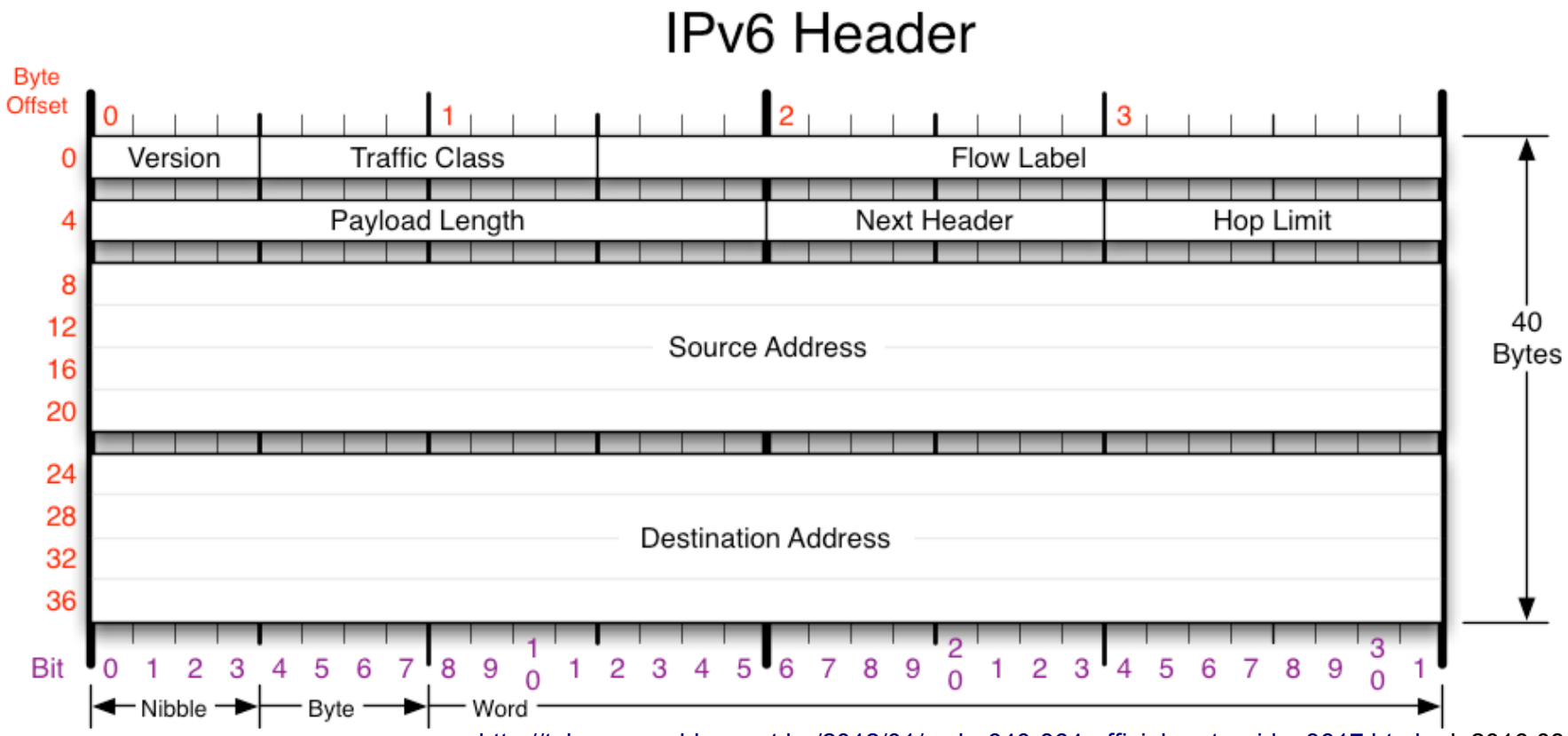
IPv6



http://telecom-sp.blogspot.hu/2012/01/ccda-640-864-official-cert-guide_3617.html u.l. 2016.08.30.

Verzió: Továbbra is 4, vagy 6
Forgalmi osztály (traffic class): prioritások kezelése
Flow label (folyam azonosító): hatékonyabb csomagtovábbítás

IPv6



http://telecom-sp.blogspot.hu/2012/01/ccda-640-864-official-cert-guide_3617.html u.l. 2016.08.30.

Payload length: a datagram fejléc utáni része bájtokban
(a kiegészítő fejlécek is a részét képezik)

Next header: TCP, UDP, de kiegészítő fejlécek is, lásd később

Hop lmiit: TTL

Forrás és cél címe: 128 biten

IPv6

Kiegészítő fejlécek:

A “Next header” jelzi mi következik

Hop-by-Hop Options header (jumbogram): Minden érintett csomópont dolgozza fel

Destination Options header (köztes célnál): Csak a célállomás számára feldolgozandó opciók

Routing header (routing type): laza/szigorú routing megjelölés

Fragment header: Tördelés elősegítő fejléc (csak forrás tördelhet, router nem)

Authentication header: Autentikáció (Valóban a küldő küldte, nem változott a tartalom)

Encrypted Security Payload header: Titkosítás (csak a jogosult olvashatja el)

További részletek: (u.l. 2016.08.30.)
http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

IPv6

IPv6 címek:

128 bit hosszú
Hexadecimális formában ábrázolt
pl: `2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A`
A bevezető nullák elhagyhatók,
illetve csaupa 0 sorozat egyszer ::-tal helyettesíthető
`2001:DB8::2F3B:2AA:FF:FE28:9C5A`

Speciális tartományok:

`2000::/3` global unicast
`FE80::/10` link-local unicast
`FD00::/8` lokális egyedi IPv6 címek
`FF00::/8` multicast

Speciális:

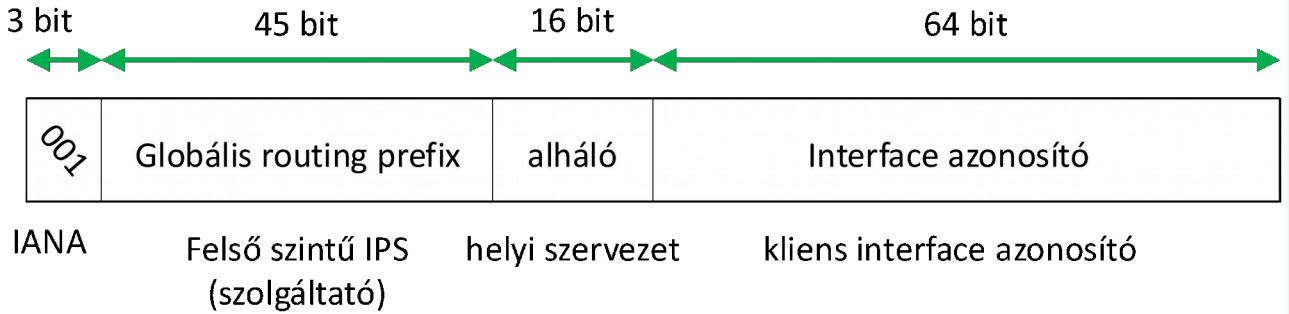
`::` unspecified address (mint 0.0.0.0 az IPv4-ben)
`::1` loopback

IPv6

IPv6 címek:

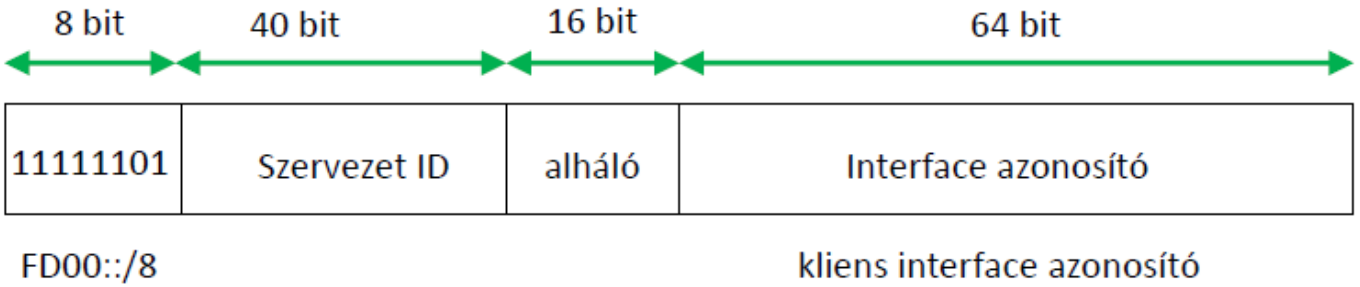
Global unicast címek

Az Ipv6 interneten routolható
16 bit foglalt belső alhálózatok kialakítására
2-vel ,vagy 3-mal kezdődik (2000::/3)



Local unicast címek

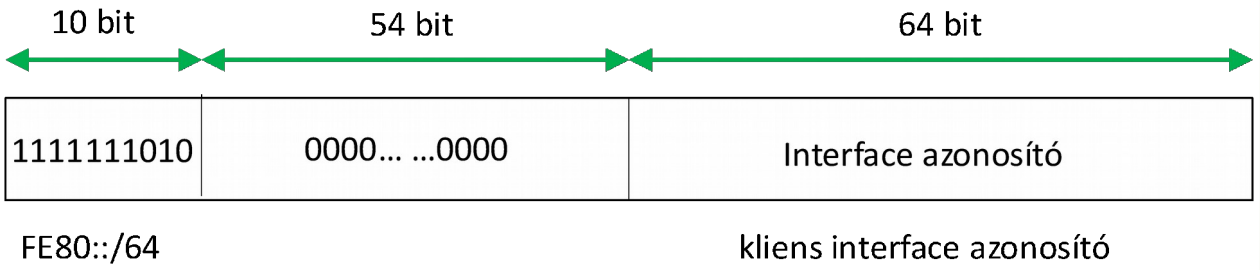
Az Ipv4 privát címtartományok megfelelője
Véletlenszerűen generált szervezeti azonosítót használ
16 bit használható belő hálózatok kialakítására



IPv6

IPv6 címek:

Link lokális autokonfigurált címek



Multicast cím példák:

Minden node a küldővel azonos linken `FF02::1`

Minden router a küldővel azonos linken `FF02::2`

Minden DHCP ügyfél `FF02::1:2`

Minden DHCP szerver `FF05::1:3`

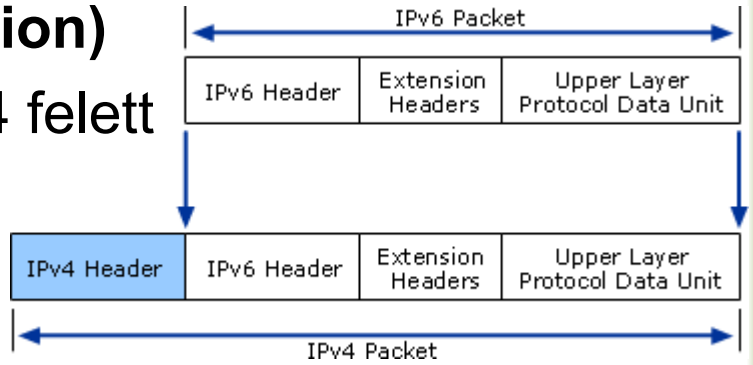
IPv6 és IPv4

Az IPv4 és az IPv6 sokáig együtt fog élni egymás mellett

Három módszer

- **kettős protokoll stack (dual stack):**
  Ez a legáltalánosabb megoldás, a két rendszer egyszerre működik. Ahol lehet, IPv6, ahol nem, ott IPv4

- **alagút (tunneling, vagy encapsulation)**
  IPv6 szigetek összekötése IPv4 felett



https://technet.microsoft.com/en-us/library/dd379548(v=ws.10).aspx u.l. 2016.08.30.

- **fordítás (translation)**
  IPv6 hosztok kommunikációja IPv4 hosztokkal A korábban ismertetett NAT kiterjesztése

A kettős címrendszer problémái

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.

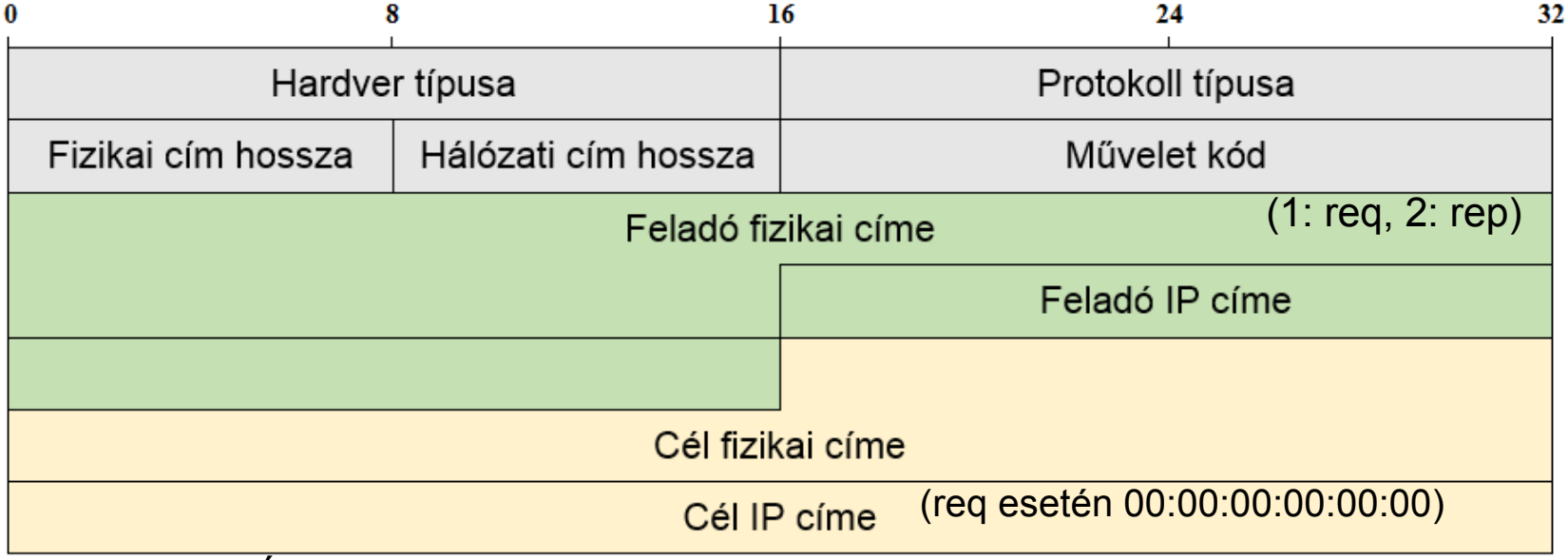
Másrészt felmerült az igény, hogy ne kelljen a csomópontokon külön-külön IP címbeállítást végezni, hanem legyen lehetőség arra, hogy **a csomópont** (az Ethernet címe alapján) **a hálózatról (egy központi helyen tárolt adatbázisból) kaphasson IP címet.**

Hálózati címből fizikai cím (ARP)

Minden csomópontnak van egy **ARP (Address Resolution Protocol)** táblája (mely fizikai cím, IP cím párokat tartalmaz), ha ebben nincs a keresett cím:

Körüzenet az alhálón az FF:FF:FF:FF:FF:FF címre. Az üzenetet mindenki megkapja, de csak az a csomópont válaszol, akinek az IP-je megegyezik a keresettel.

ARP keret fomrátuma:

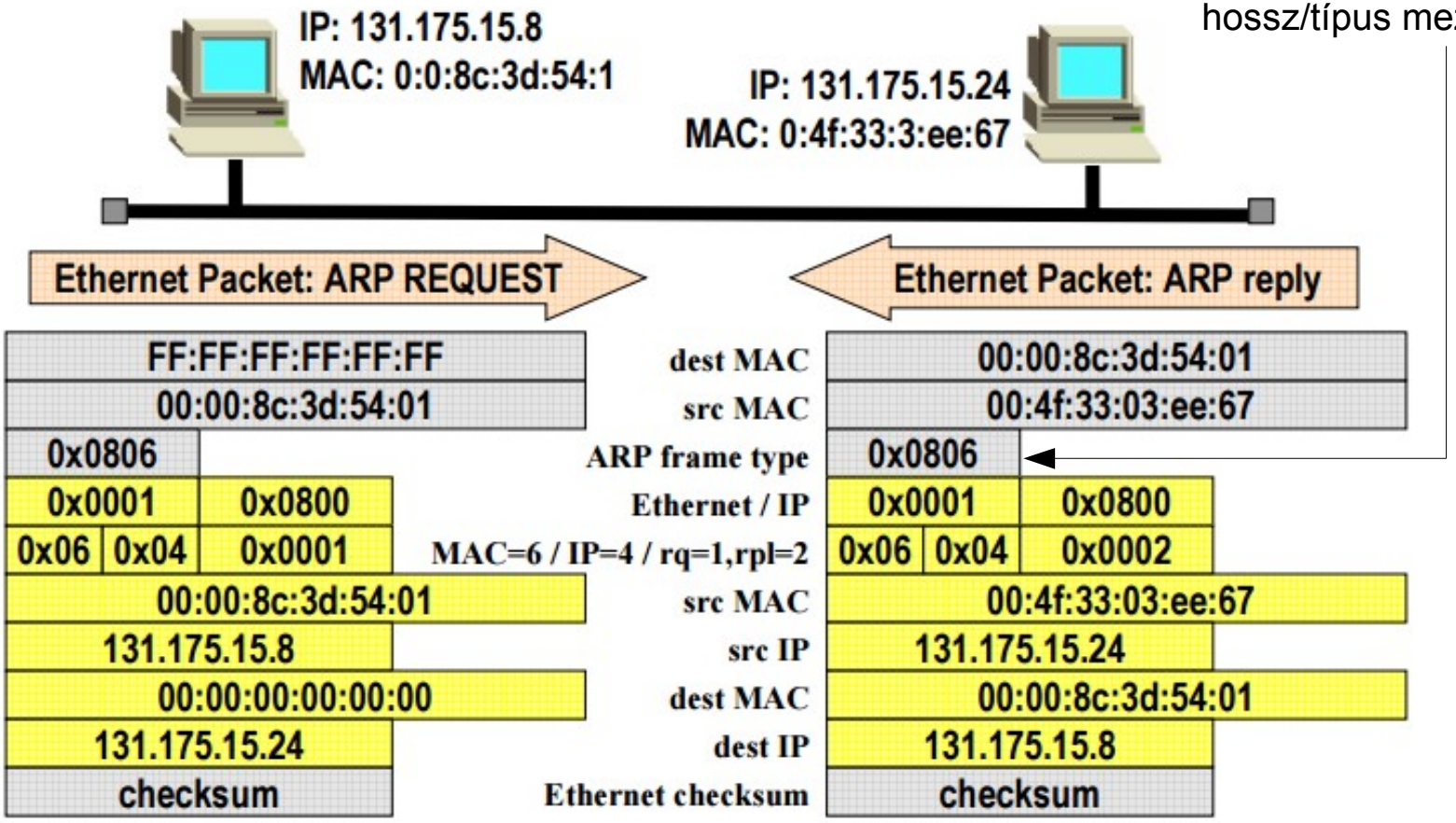


1-2. szó: Általános ARP fej
3-7. szó: IPv4/Ethernet specifikus adatrész.
Az Ethernet-keret típus értéke: 0x0806

Hálózati címből fizikai cím (ARP)

ARP kérés és válasz példa:

Vesd össze: 122. és 99. dia (Ethernet keret: hossz/típus mező)



G.Bianchi, G.Neglia, V.Mancuso, Direct Datagram Forwarding: Address Resolution Protocol (ARP), http://www-sop.inria.fr/members/Vincenzo.Mancuso/ReteInternet/09_arp.pdf u.l. 2016.08.30.

Fizikai címből hálózati cím (RARP)

A RARP **(Reverse ARP)** 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.

- RARP kérdés: Ki tudja az X fizikai cím hálózati címét?
- A kérdés keretét üzenetszórásos küldéssel az alhálózat valamennyi csomópontja megkapja.
- A RARP szerverek feldolgozzák a kérdést: Ha megtalálják a táblázatukban az X fizikai címet, akkor a táblázatban található hálózati címmel megválaszolják a RARP kérdést.

Egytől több üzenetszórási tartományban történő meghatározáshoz használható a BOOTP prtokoll (RFC 951)

Dinamikus IP címmeghatározás (DHCP)

A DHCP (Dynamic Host Configuration Protocol, DHCP RFC 1531) 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 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 (lease) kapják az IP címet. Ha az időszak lejár (s nem sikerül a megújítás) a kliensnek kötelezően el kell engednie az IP címet.

Dinamikus IP címmeghatározás (DHCP)

A DHCP működési vázlata:

1) A kliens **DHCPDISCOVER** csomagot küld szét üzenetszórással, amire csak a DHCP szerverek válaszolhatnak. (*"CL: Ki tud nekem adni egy címet?"*)

2) A DHCP szerverek **DHCPOFFER** csomaggal válaszolnak (Ha van a tartományukban szabad IP), mely a potenciális IP címet tartalmazza. (*"S: Én ezt tudom felajánlani."*)

3) A kliens megkapja a csomagotkat, majd **DHCPREQUEST** csomaggal válaszol (több szerver esetén a kiválasztott szervernek). A csomag tartalmazza a szerverazonosítót (több szerver esetén innen tudni melyik a kiválasztott) (*"CL: Ezt kérném..."*)

4) A kiválasztott szerver regisztrálja a címet az adatbázisában, majd **DHCPACK** csomaggal válaszol. (Ha a cím mégsem osztható ki DHCPNAK). (*"S: Tessék..."*)

Dinamikus IP címmeghatározás (DHCP)

A szervertől kapott IP cím érvénytelenségének jelzése:

DHCPDECLINE

Cím elengedése (nincs tovább rá szükség):

DHCPRELEASE

Lease újrakérése (renewal):

A gyakorlatban a lease érvényességi idejének végét (tipikusan néhány nap pl. MS rendszereken vezetékes LAN esetén 8, vezeték nélküli LAN esetén 3 nap) általában nem szokás megvárni.

Microsoft rendszereknél például a lease érvényességi idejének 50%-ánál a kliens új kérést indít. Mivel ekkor ismeri a DHCP szervert, ez nem broadcastüzetenet. A szerver válaszában tudatja a klienssel az esetleges megváltozott paramétereket.

Ha a szerver nem válaszol, akkor a lejárati idő 87.5%-ánál broadcast DHCPREQUEST üzenetet küld a kliens és egy szookásosleasegenerálás zajlik.

Dinamikus IP címmeghatározás (DHCP)

Foglalt címek (reservation):

A szervereken lehetőség van címek statikus hozzárendelésére MAC cím alapján.
Tipikus használati esetek pl. hálózati nyomtatók, szerverek, stb…

A MAC cím lekérdezhető `ipconfig /all` paranccsal, illetve egyes eszközökre rá is írják.

Fontosabb opciók:

- 1 Subnet mask
- 3 Router
- 6 DNS servers
- 15 DNS domain name
- 31 Perform router discovery
- 33 Static route

További opciók: http://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml

Forgalomirányítás

Forgalomirányítási konfigurációk

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. (pl: default gateway beállítása)

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

Belső forgalomirányítási protokollok (IGP – Interior Gateway Protocol): Egy autonóm rendszeren (AS) belül működik.

Külső forgalomirányítási protokollok (EGP - Exterior Gateway Protocol): Jellemzően autonóm rendszerek közötti forgalomirányítás

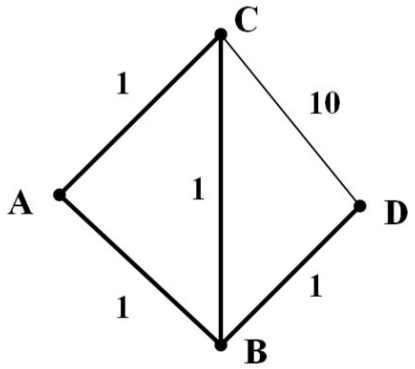
Távolságvektor alapú forgalomirányítás

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?)

Példa: Az ábrán látható hálózati topológiát feltételezve az A csomópont a következő informcáiókat tárolja:

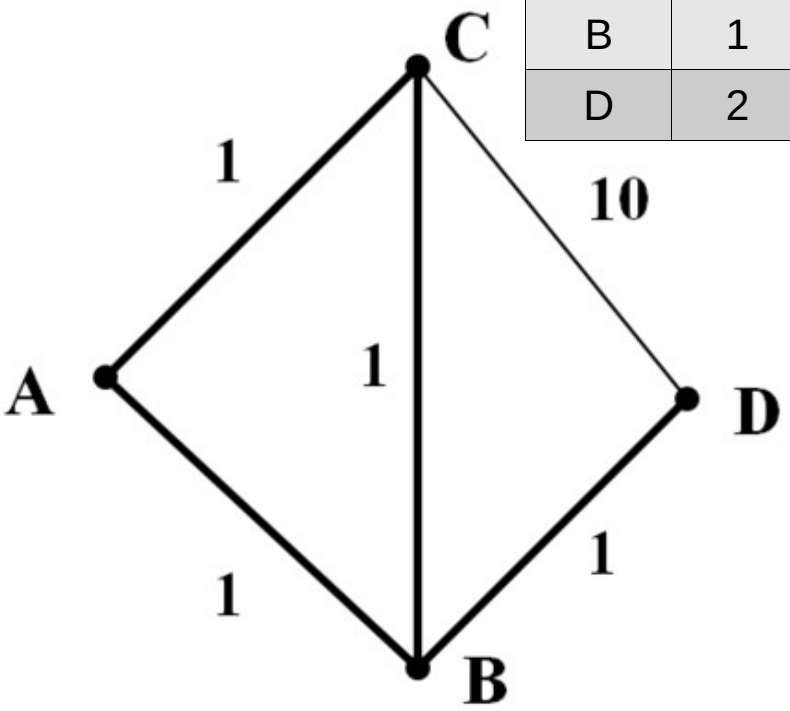
Cél	Távolság	Next hop
B	1	B
C	1	C
D	2	B



Távolságvektor alapú forgalomirányítás

Cél	Táv.	NH
A	1	A
B	1	B
D	2	B

Cél	Táv.	NH
B	1	B
C	1	C
D	2	B



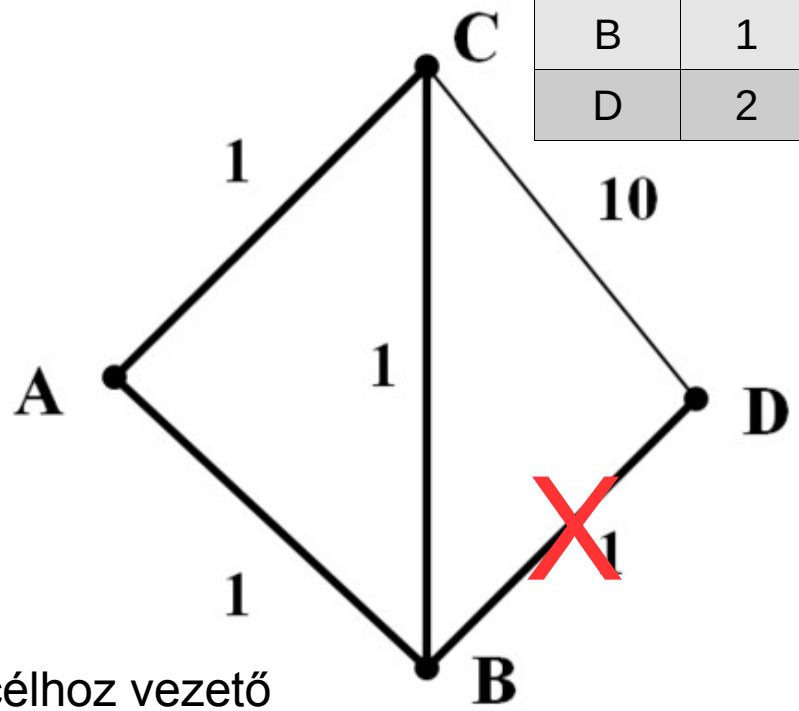
Cél	Táv.	NH
A	2	B
B	1	B
C	2	B

Cél	Táv.	NH
A	1	A
C	1	C
D	1	D

Távolságvektor alapú forgalomirányítás

Cél	Táv.	NH
A	1	A
B	1	B
D	2	B

Cél	Táv.	NH
B	1	B
C	1	C
D	2	B



Cél	Táv.	NH
A	2	B
B	?	?
C	10	C

Mi történik, ha egy célhoz vezető kedvezőbb útvonal megsérül?

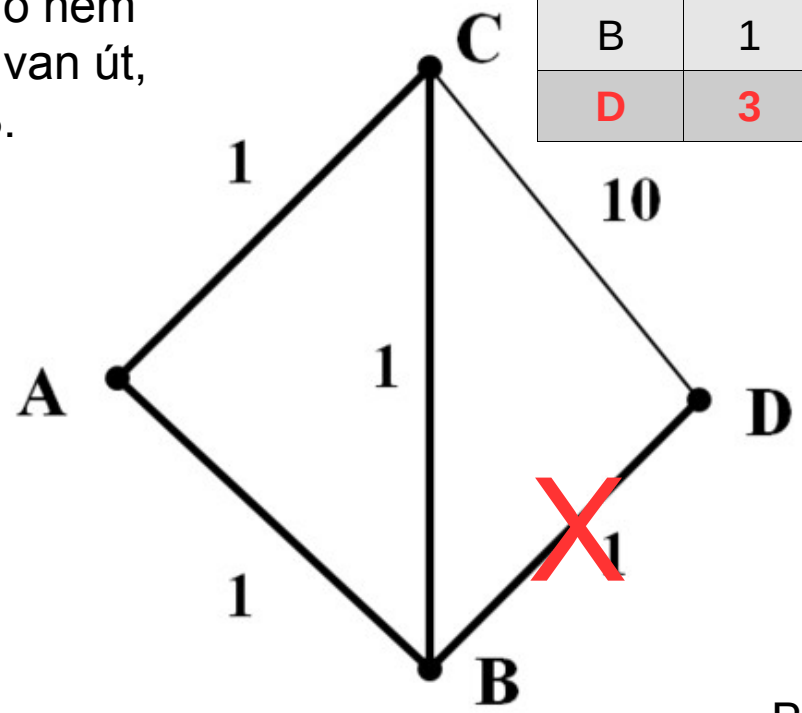
Végtelenig számolás problémája.

Cél	Táv.	NH
A	1	A
C	1	C
D	?	?

Távolságvektor alapú forgalomirányítás

A azt kapta C-től, hogy ő 2 távolságra el tud jutni D-be. B-től meg azt, hogy ő nem tud. → C-n kerestül van út, aminek a költsége 3.

Cél	Táv.	NH
B	1	B
C	1	C
D	**3**	**C**



Cél	Táv.	NH
A	1	A
B	1	B
D	**3**	**A**

C hasonlóan járt, mint A, csak ő A-tól kapott hamis információt

Cél	Táv.	NH
A	11	C
B	11	C
C	10	C

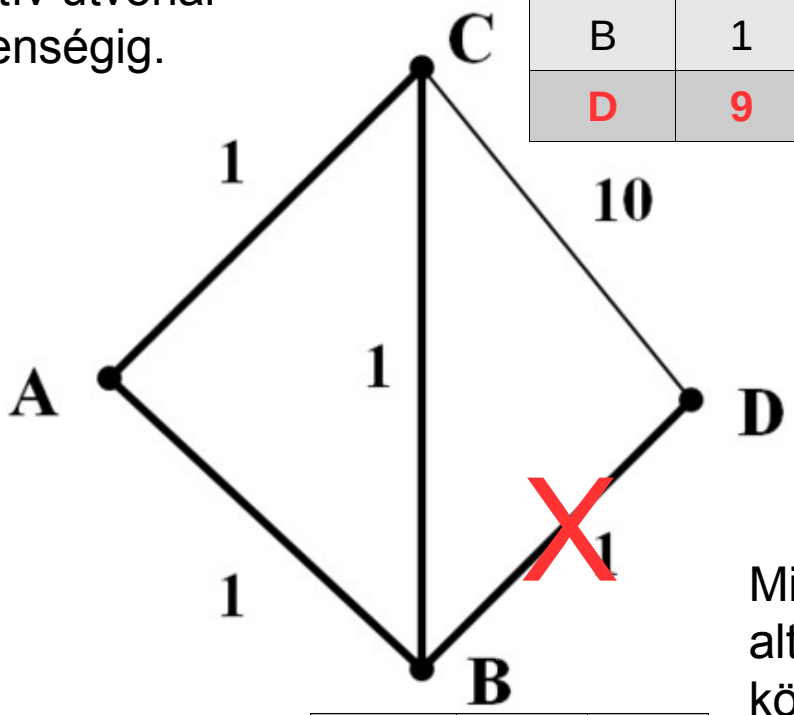
Cél	Táv.	NH
A	1	A
C	1	C
D	**3**	**C**

B az A-tól és C-től kapott két hamis információ közül tulajdonképpen mindegy melyik rosszat választja.

Távolságvektor alapú forgalomirányítás

A routerek egymás között folyamatosan szórják a fals információt. Alternatív útvonal hiányában a végtelenségig.

Cél	Táv.	NH
A	1	A
B	1	B
D	**9**	**A**



Cél	Táv.	NH
B	1	B
C	1	C
D	**9**	**C**

Cél	Táv.	NH
A	11	C
B	11	C
C	10	C

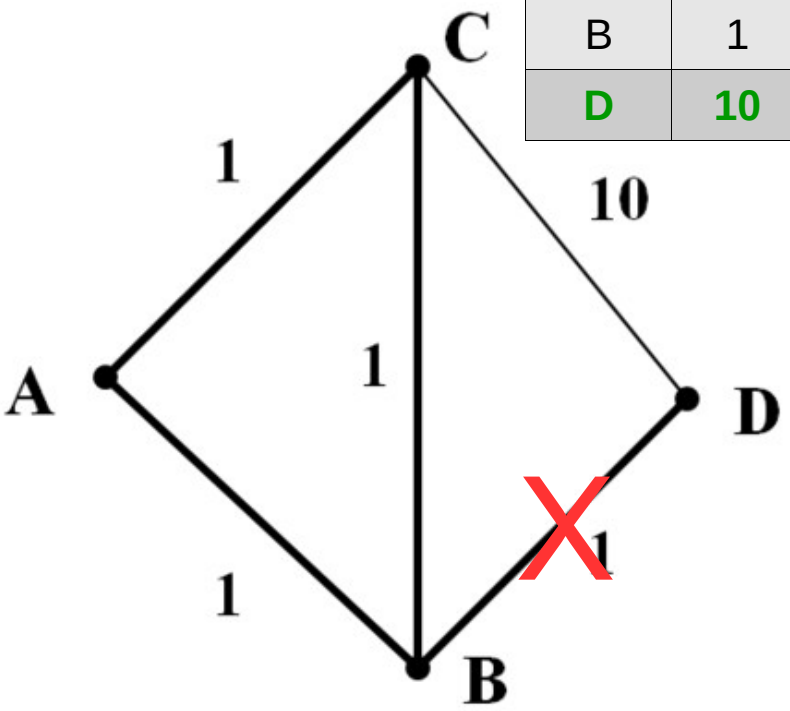
Cél	Táv.	NH
A	1	A
C	1	C
D	**9**	**C**

Mivel ebben a példában van alternatív útvonal, a következő lépésben C táblája már helyreáll. (Azaz nem A- keresztül próbálja D-t elérni.)

Távolságvektor alapú forgalomirányítás

Cél	Táv.	NH
A	1	A
B	1	B
D	10	D

Cél	Táv.	NH
B	1	B
C	1	C
D	10	C



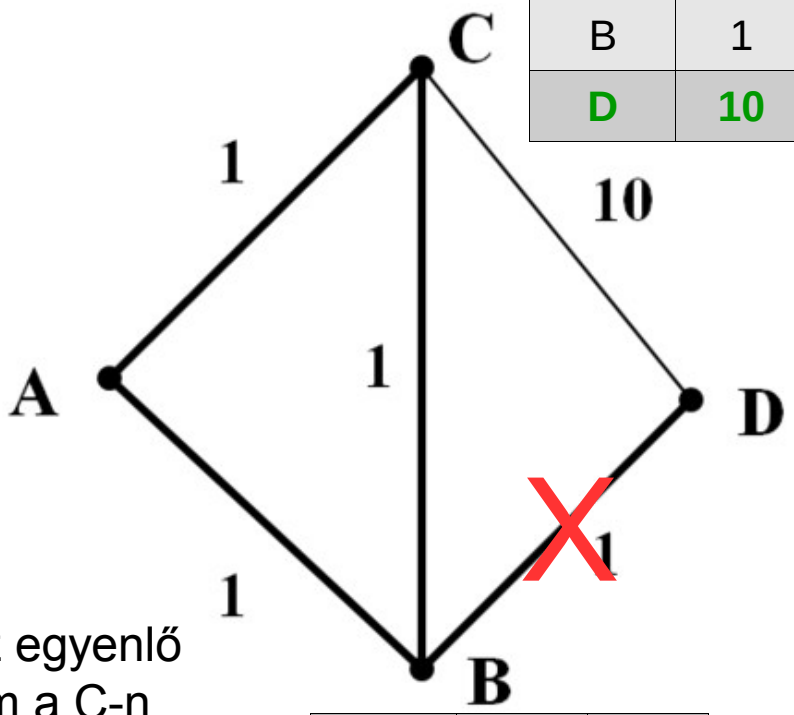
Cél	Táv.	NH
A	11	C
B	11	C
C	10	C

Cél	Táv.	NH
A	1	A
C	1	C
D	10	C

Távolságvektor alapú forgalomirányítás

Cél	Táv.	NH
A	1	A
B	1	B
D	**10**	**D**

Cél	Táv.	NH
B	1	B
C	1	C
D	**11**	**C**



Cél	Táv.	NH
A	11	C
B	11	C
C	10	C

Cél	Táv.	NH
A	1	A
C	1	C
D	**11**	**C**

Ha esetleg A és B az egyenlő költség miatt mégsem a C-n keresztüli útvonalat vette volna át, a következő lépésben akkor is beállína az ábrán most látható rend.

Link-állapot alapú forgalomirányítás

A link-állapot protokollok (Link-state routing) működése 2 részből áll:

1. Minden állomás felderíti a hálózat topológiáját így minden állomás mindig ismeri a teljes hálózat topológiáját
2. A kapott gráfban megkeresi a legrövidebb útvonalat a többiekhez és az azokhoz tartozó első állomást

Előnyök:

Gyorsabban topológiaváltozás követés

Bonyolultabb metrikák használata

- A költségek egyszerűbben tehetők összetetté
- több mint egy metrika használatának lehetősége

Terhelés kiegyenlítés (Load Balancing):

- Többszörös utak figyelembevétele
- Topológia adatbázisból kiszámíthatóak

IGP Routing protokollok

A Routing Information Protocol (RIP) legfontosabb jellemzői:

- **Távolságvektor alapú IGP protokoll.**
- Régi, de folyamatosan fejlesztik, javítják.
- **Metrika: érintett útválasztók száma** (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
- **RIPv2 (RFC 1723): CIDR kompatibilis, a szomszédok közötti kommunikációra authentikáció előírható.**

IGP Routing protokollok

Enhanced Interior Gateway Routing Protocol (EIGRP)

- **Gyártóspecifikus (Cisco) távolságvektor alapú IGP routing protokoll.**
- Szomszédsági viszonyok kiépítése és fenntartása ("update" csak tényleges változás esetén történik, nem ez képezi a szomszéd elérhetőségének a vizsgálatát).
- **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).

IGP Routing protokollok

OSPF (Open Shortest Path First)

- **Link-állapot alapú IGP protokoll**
- **A legszélesebb körben használatos 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 (2016):**
  OSPF V2 (RFC 2178), OSPF V3 – Ipv6 (RFC 2740)

IGP Routing protokollok

OSPF területek

A döntési folyamat alapja a terület (area).

A területek „csillag alakzatot” formáznak, középpontjában a területeket összekötő speciális területtel (backbone).

A terület határ router-ek feladata összetett:

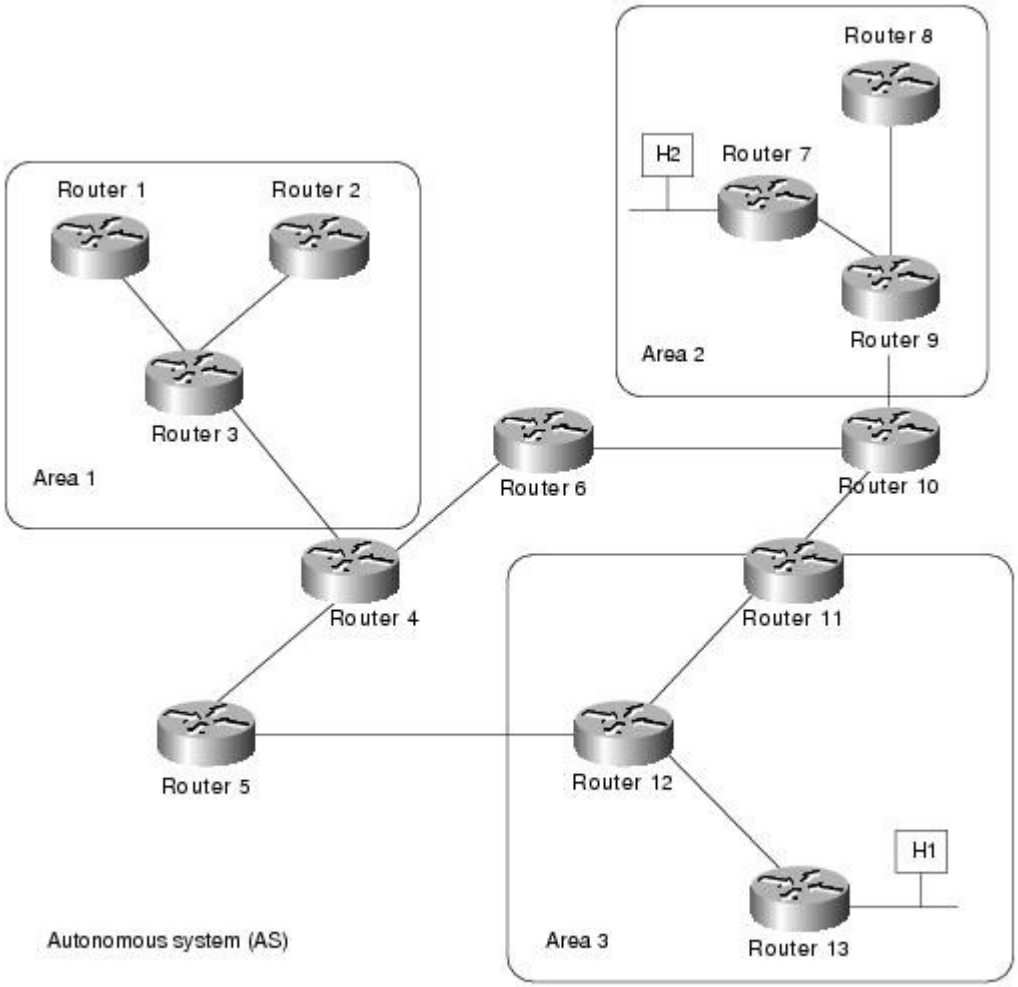
- Minden területhez (külön) döntési folyamat.
- A területekből tanult információk összegzése.
- Az összegzett információk bevitele a többi területbe.

Területek közötti forgalomirányítás (inter area routing):

- Routing a forrás területben a határ router-ig.
- Routing a backbone-on a cél terület határ router-ig.
- Routing a cél területben a cél hálózatig.

IGP Routing protokollok

OSPF



Magyarázat a képhez: http://docwiki.cisco.com/wiki/Open_Shortest_Path_First u.l. 2016.08.30.

IGP Routing protokollok

IS-IS (Intermediate System to Intermediate System – RFC 1142, 7142)

- **Link-állapot alapú IGP protokoll**
- **Az OSPF mellett szintén viszonylag gyakran használt protokoll**
- **Az AS-t szintén területekre osztja**
- Előnyei az OSPF-fel szemben:
  - Nem szigorúan IP alapú, így változtatás nélkül használható Ipv6-ra
  - Nincs kifejezetten gerincnek szánt 0-s terület. Nem kell követni az OSPF szigorú csillag topológiáját.
  - A routereket két különböző szintre osztja (Level 1 és Level 2) intra- és inter area routerek.
  - Több kiegészítési lehetőséggel bír

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a3e6f.shtml#wp39303
u.l. 2016.08.30.

EGP Routing protokoll

BGP (Border Gateway Protocol)

- **Az Internet gerincén használatos standard EGP**
- **Path Vector Routing alapú (Speciális távolságvektor)**
- **CIDR támogatás**
  - Hatékony címtatomány aggregáció
- **Manuális szomszéd beállítás**
  - Nincs automatikus felfedezés
- TCP felett működik (179 port)
  - Megbízható (lásd később – szállítási réteg)
  - Feltételezi a kapcsolat orientált szállítóréteget
- Nincsenek periodikus frissítések
  - Nemműködő útvonalak megjegyzésre kerülnek
- Hurok elkerülése:
  - útvonalvektor
  - AS-ek felsorolása a célig

További információ: Baumann Ferenc, Routing Protokollok - http://alpha.tmit.bme.hu/~baumann/05routingv.pdf

A szállítási réteg

A szállítási réteg protokolljai

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

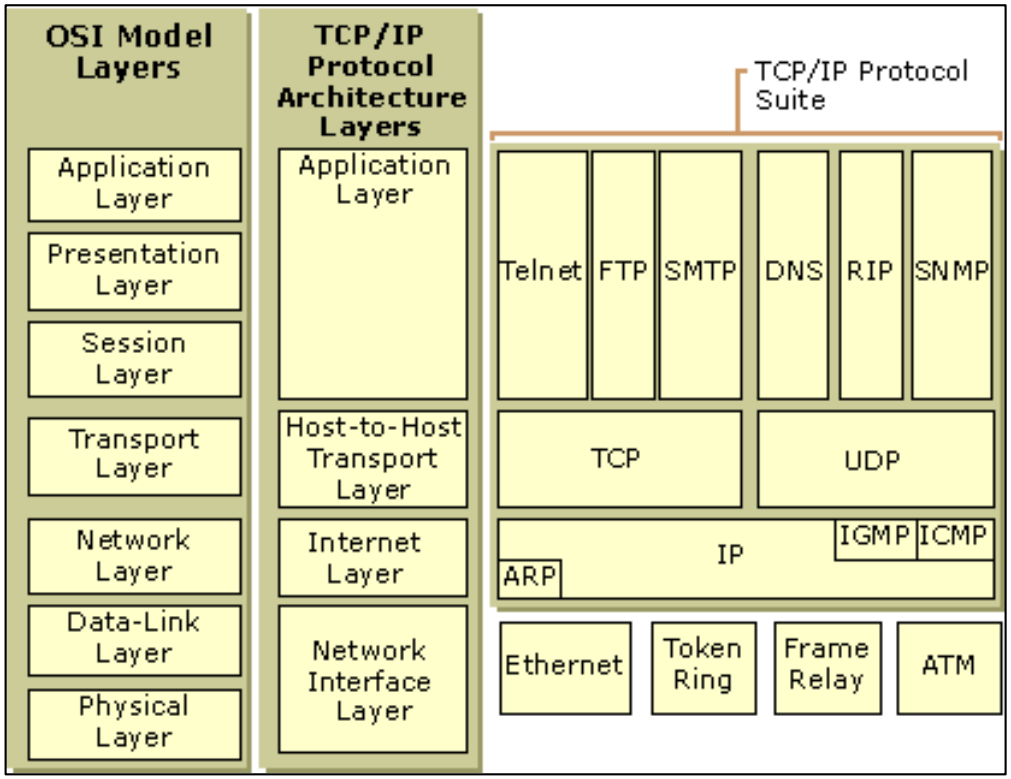
- A szállítási réteg a felette lévő alkalmazási rétegbeli folyamatok számára **logikai kommunikációt valósít meg**, azt a látszatot keltve, mintha a kommunikáló felek közvetlenül összekööttetésben állnának.
- A szállítási réteg **protokolljait csak a végrendszerekben implementálják**, a köztes forgalomirányítókon nem.
- A szálítási réteg adateleme a **szegmens** (vagy TPDU – Transport Layer Protocol Data Unit)

A szállítási réteg protokolljai

A TCP/IP protokoll verem az alkalmazási réteg folyamatai számára két szállítási réteg beli protokoll használatát teszi lehetővé:

User Datagram Protocol (UDP)
(RFC 768) Nem megbízható, össszeköttetés nélküli szolgáltatás.

Transmission Control Protocol (TCP)
(RFC 793) Megbízható, összeköttetés alapú szállítás megvalósítása.



https://technet.microsoft.com
TCP/IP Protocol Architecture (2016.08.)

A szállítási réteg protokolljai

A szállítási réteg beli protokollok által biztosított szolgáltatások:

Nyalábolás (multiplexelés): Míg az IP protokoll a csomópontok közötti szállítást valósítja meg, a szállítási réteg beli protokollok a csomópontokon futó folyamatok közötti kézbesítést végzik. A különböző folyamatoktól érkező szegmenseket a küldő oldalon egy csatornára kell helyezni. A különbőző kommunikációs folyamatok azonosítására szolgál a **port**.

Nyalábbontás (demultiplexelés): A nyalábolás fogadó oldali ellenművelete. Az kommunikációs csatornán érkező szegmenseket a portszám alapján a csomóponton belüli folyamatokhoz rendeli.

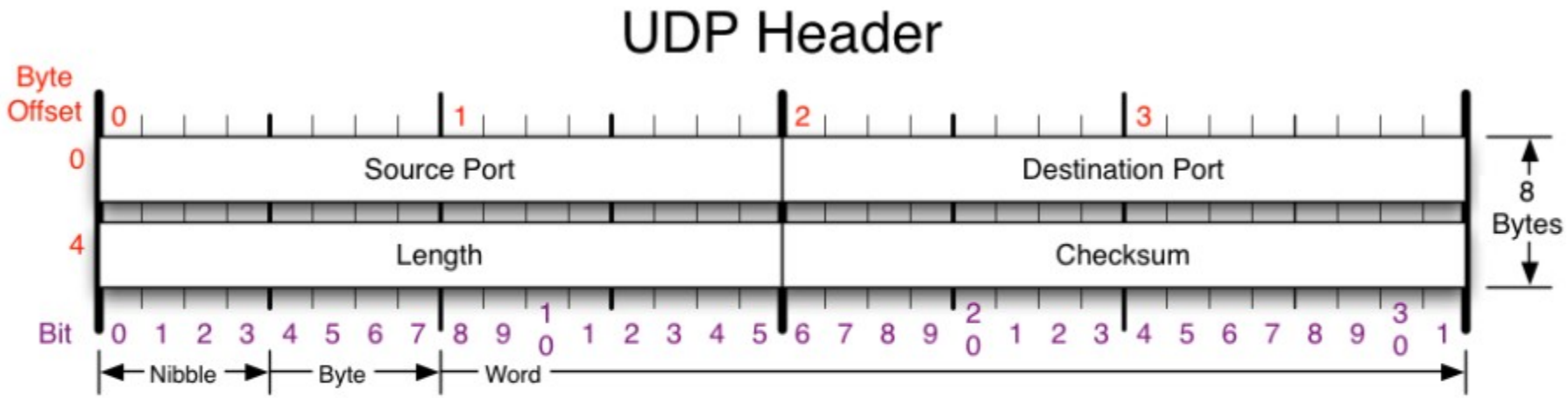
> **(Hálózati) Port:** 16 bites előjel nélküli egész azonosító (0-65536). A 0-1023-ig terjedő tartományban találhatók az ún. Jól ismert szolgáltatások portjai, melyeket az IANA jelölt ki (RFC 1700 https://tools.ietf.org/html/rfc1700 u.l. 2016.08.30.)

Adatintegritás: Mindkét protokoll fejlécében található ellenőrző összeg, mely segítségével ellenőrizhető az adatok sérülésmentessége

UDP

Az UDP protokoll a szállítási rétegben garantálandó szolgáltatásokon kívül semmit nem biztosít előnyei ugyanakkor pont egyszerűségéből adódnak:

- Alkalmazási szinten szabályozható
- Nincs összeköttetés felépítés
- Nincs állapot nyilvántartás
- Kisebb fejléc többletterhelés



Source port (forrás port): A küldő folyamatot azonosító port
Destination port (cél port): A fogadó folyamatot azonosító port
Length (hossz): A fejléc a szállított adat együttes hossza bájtokban
Checksum (ellenőrző összeg): Az adatintegritás ellenőrzésére

http://www.ccnahub.com/ip-fundamentals/understanding-tcp-and-udp-protocols/ u.l. 2016.08.30.

TCP

A TCP protokoll az UDP-vel szemben számos további szolgáltatást nyújt, melyek közül a legfontosabbak:

Megbízható adatszállítás sorszámok, nyugták és időzítők segítségével: Annak biztosítása, hogy a küldőtől az információ garantáltan megérkezik.

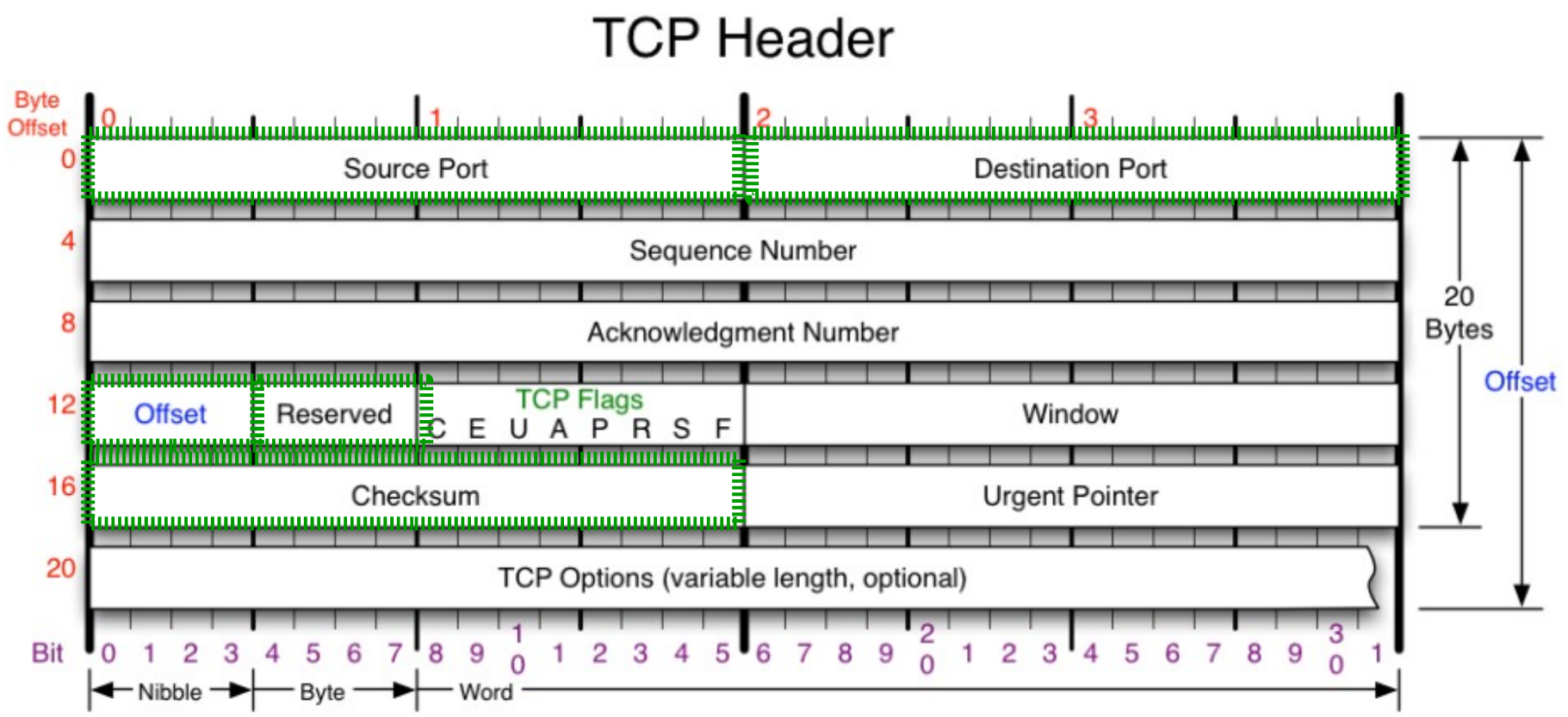
Főbb feladatai:

- az adat részeinek sorrendhelyessége
- Egységek elvesztésének megakadályozása
- Duplikációk elkerülése

Torlódáskezelés: Az adott idő alatt kiküldendő szegmensek számának szabályozása küldő oldalon annak érdekében, hogy a túlterhelt kapcsolatokat ne “árassza el” egy-egy szolgáltatás

A TCP-ről részletesen:
http://alpha.tmit.bme.hu/meresek/lantcp.htm u.l. 2016.08.30.

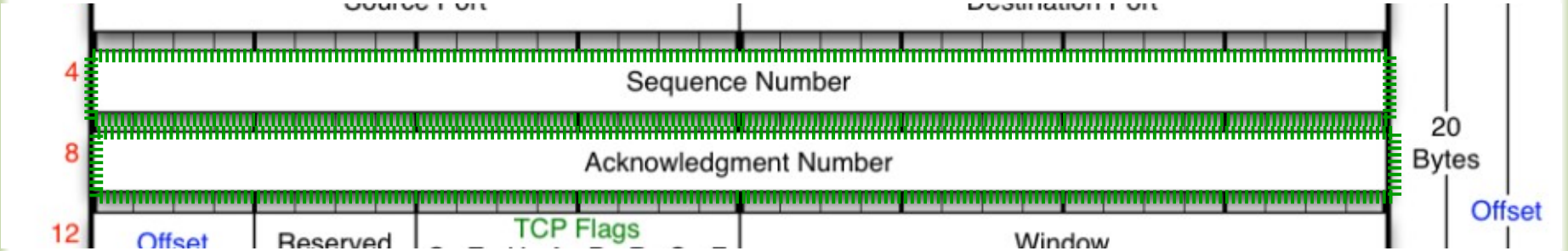
TCP



Source port (forrás port): A küldő folyamatot azonosító port
Destination port (cél port): A fogadó folyamatot azonosító port
Offset: TCP fejrész hossza szavakban
Reserved (foglalt): Későbbi használtra fenntartott 6 bit, értéke kötelezően csupa 0.
Checksum (ellenőrző összeg): Az adatintegritás ellenőrzésére

http://www.ccnahub.com/ip-fundamentals/understanding-tcp-and-udp-protocols/ u.l. 2016.08.30.

TCP



Sequence number (sorszám): 32 bites előjel nélküli egész. E szám távolsága az induló sorszámtól (ISN – Initial SN) megegyezik a szegmens első bájtjának pozíciójával az eredeti bájtfolyamban. Az ISN értéke véletlenszerűen generált. A generálás módja rendszerfüggő.

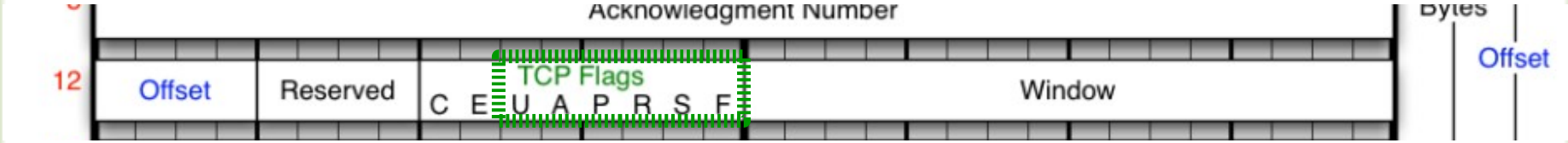
Ha például ISN=84500, a szegmens első bájtának sorszáma pedig az eredeti folyamban 68700, akkor a sorszám értéke a szegmensben e két szám összege → 153200.

Ha az összeadás eredménye nagyobb lenne, mint a 32 biten ábrázolható legnagyobb szám, akkor venni kell az összeg 2^{32}-nel vett maradékát.

Acknovledgement number (nyugtaszám): Ha az ACK vezérlőbit értéke 1, akkor az ebben a mezőben megadott 32 bites szám annak a byte-nak a sorszáma, amit a szegmens küldője a vevőtől vár.

http://www.ccnahub.com/ip-fundamentals/understanding-tcp-and-udp-protocols/ u.l. 2016.08.30.

TCP



Vezérlő bitek (Control Bits vagy Flags) - 6 bit az alábbi sorrendben:

URG - Urgent Pointer - Ha az értéke 1, akkor a vevőnek figyelembe kell vennie a Sürgősségi mutató (Urgent Pointer) mező értékét.

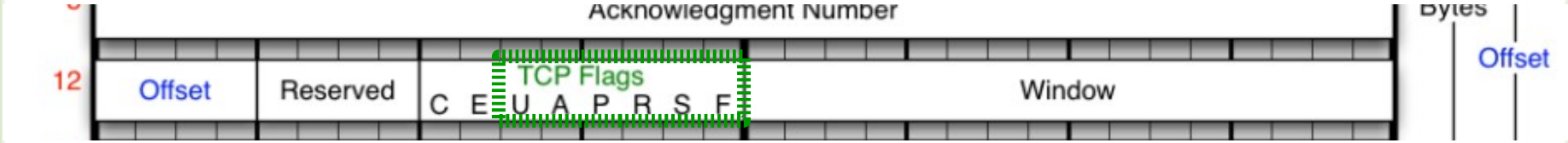
ACK - Acknoledgement - Ha értéke 1, akkor a Nyugta sorszáma (Acknowledgement Number) mező valós értékkel rendelkezik.

PSH - Push Function - Ha az értéke 1, akkor a vevőnek a lehető leghamarabb továbbítania kell a szegmenst a fogadó alkalmazásnak. A szegmens tartalma lehet például egy vezérlő üzenet, aminek meg kell előznie a normál adatfolyamot.

RST - Reset the Connection - Azt jelzi a vevőnek, hogy a küldő törölte az összeköttetést. A sorban álló adatcsomagok törölhetőek és a lefoglalt pufferek felszabadíthatóak. A szegmens sorszáma és a nyugta sorszáma alapján a vevő figyelmen kívül hagyhatja a RST parancsot.

http://www.ccnahub.com/ip-fundamentals/understanding-tcp-and-udp-protocols/ u.l. 2016.08.30.

TCP



Vezérlő bitek (Control Bits vagy Flags) - 6 bit az alábbi sorrendben:

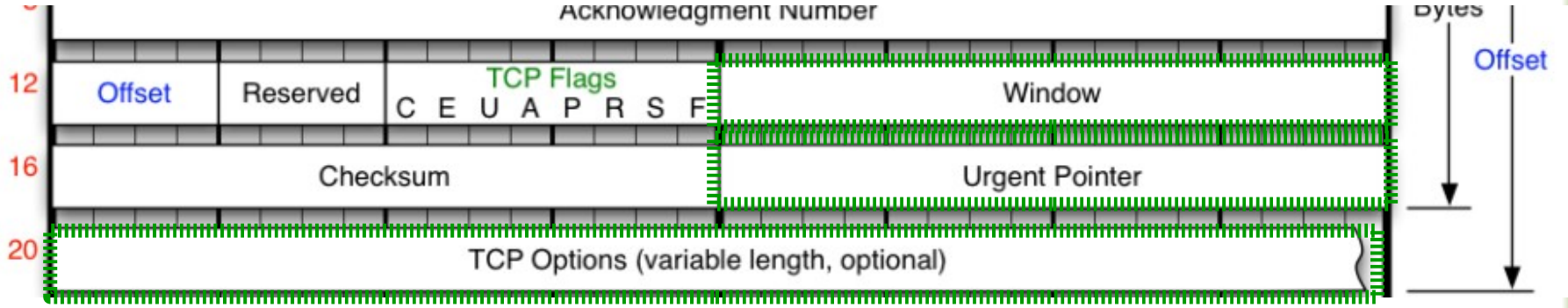
SYN - Synchronize sequence numbers - Ha értéke 1, akkor azt jelzi, hogy a küldő "szinkronizálni" szeretné a sorszámokat. Az összeköttetés létrehozásakor használatos.

FIN - No more data from sender - Ha értéke 1, akkor azt jelzi a vevőnek, hogy ebben az összeköttetésben a küldő nem küld több adatot.

Az RFC 3168 (http://tools.ietf.org/html/rfc3168 u.l. 2015.11.08.) további két jelzőbitet definiált az URG bit elé (így a Fenntartott mezőben csak 4 bitnyi hely maradt), sorrendben a CRW (Congestion Window Reduced) és az ECE (ECN Echo) biteket, amelyeknek a TCP továbbfejlesztett torlódáskezelési mechanizmusával kapcsolatban van jelentősége

http://www.ccnahub.com/ip-fundamentals/understanding-tcp-and-udp-protocols/ u.l. 2016.08.30.

TCP



Window (Ablak) - A TCP forgalomszabályozása során használt változó, megmondja bájtokban, hogy a vevő mennyi adatot képes még fogadni.

Urgent pointer (Sürgősségi mutató) A sürgősen feldolgozandó (a vevő alkalmazás felé mihamarabb továbbítandó) adatok utáni byte-ra mutató pointer. Csak akkor kell értelmezni, ha az URG jelzőbit értéke 1.

Options (opciók): A kapcsolat menedzsmenjéhez haszálatos kiegészítő lehetőségek megadása. (Mérete változó. Hogy a TCP fejrész biztosan 32 bites szóhatáron végződjön esetlegesen **kitöltés** alkalmazható.)

http://www.ccnahub.com/ip-fundamentals/understanding-tcp-and-udp-protocols/ u.l. 2016.08.30.

TCP

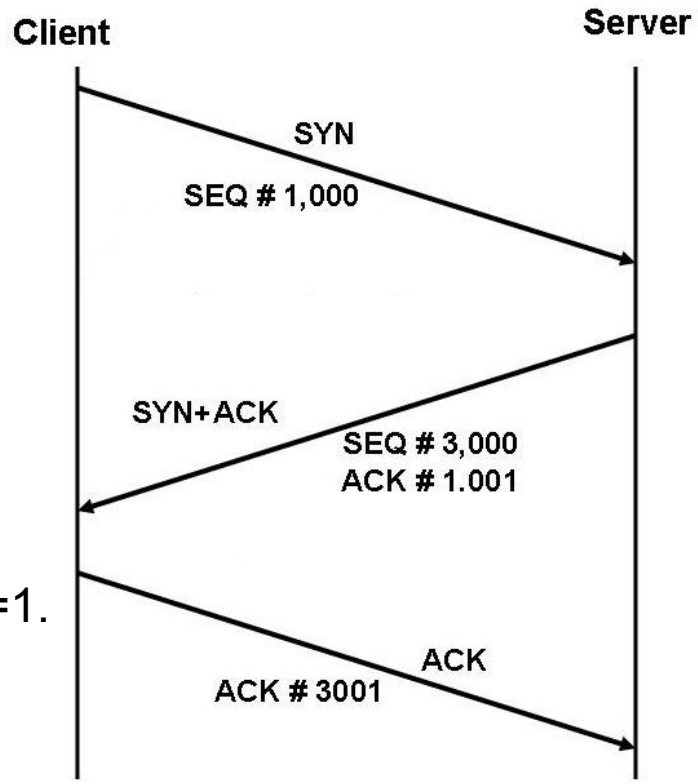
A TCP kapcsolat felépítése – háromutas kézfogás:

1) A kapcsolat kiépítést a kliens kezdeményezi. A kezdősorszám egy véletlen-szám lesz (pl. SEQ_No=1000). 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: Beállítja a saját (véletlen) kezdősorszámát (pl. SEQ_No=3000), a nyugta sorszámot a kapott SEQ érték rákövetkezőjére (ACK_No=1001) állítja. A jelzőbiteknél SYN=1, ACK=1.

3) A kliens megkapja a szerver válaszát, s erre egy jóváhagyást küld a szerver felé. Beállítja a saját szegmes-sorszámát (SEQ_No=1001), a nyugta sorszámot pedig a kapott SEQ érték rákövetkezőjére (ACK_No=3001). A jelzőbiteknél SYN=0, ACK=1.

4) A szerver megkapja a kliens válaszát, s ezzel a kapcsolat kiépült.

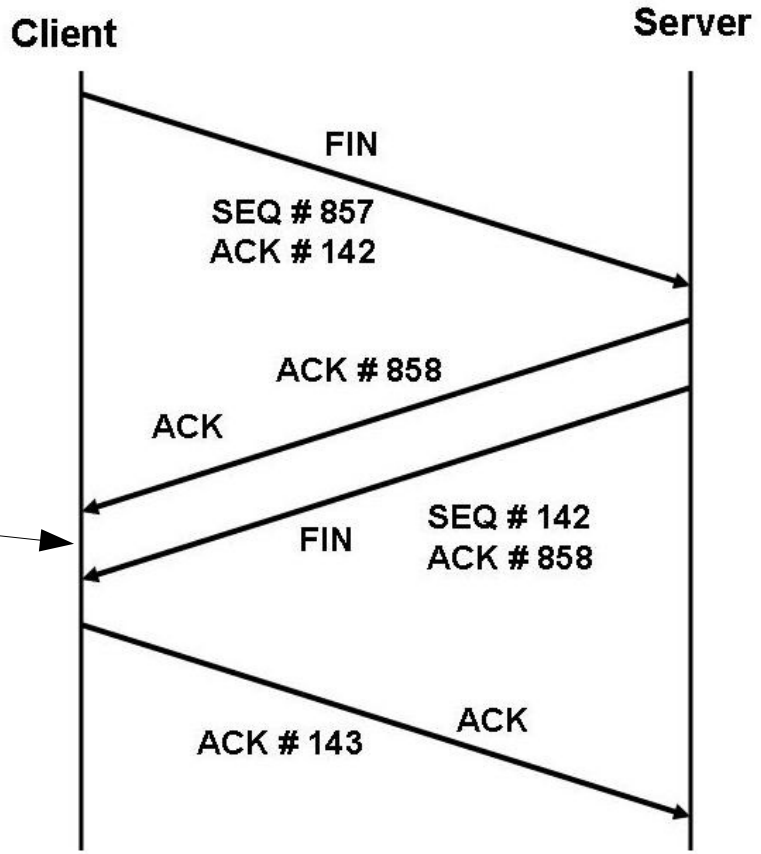


TCP

A TCP kapcsolat bontása:

A lezárás a két fél által kölcsönösen elküldött FIN jelzőbites szegmensekből és az arra adott nyugtákból áll, vagyis alapvetően 4 üzenetet használunk, ami nem is meglepő, ha arra gondolunk, hogy a TCP full-duplex összeköttetést nyújt.

A mai implementációkban gyakran az aktív FIN-re adott nyugta és a passzív FIN egy szegmensben megy.



TCP

Az újraküldés időzítése:

Mivel a TCP megbízható átvitelt nyújt, minden olyan szegmenst újraküldünk, amire egy meghatározott időn belül nem érkezik nyugta. Minden szegmenshez egy újraküldési időzítőt kapcsolunk, amely az **RTO (Retransmission Timeout)** lejárta után újraküldi a szegmenst.

Az RTO-t a kommunikáció két végpontja közötti kétirányú késleltetés **(RTT - Round Trip Time)** alapján határozzuk meg, azonban az Internet két tetszőlegesen kiválasztott végpontja között az több nagyságrendet átfogó tartományba eshet az RTT, sőt két kiválasztott host között időben is jelentős ingadozást mutathat a késleltetés alakulása, vagyis az RTT meghatározása meglehetősen nehéz feladat.

TCP

A TCP forgalomszabályozás:

A TCP a hatékonyság növelése érdekében lehetővé teszi, hogy egyszerre több szegmens is "kint legyen a hálózaton" (a pillanatnyilag maximálisan kint levő nyugtázatlan adatmennyiséget az "Ablak" mező értéke határozza meg),

Az ablak segítségével a vevő megakadályozza, hogy egy gyors küldő elárassza a vevőt (folyamvezérlés - flow control).

A folyamvezérlés eszköze a TCP protokollban az ún. **csúszóablakos technológia,** melynek segítségével elérhető:

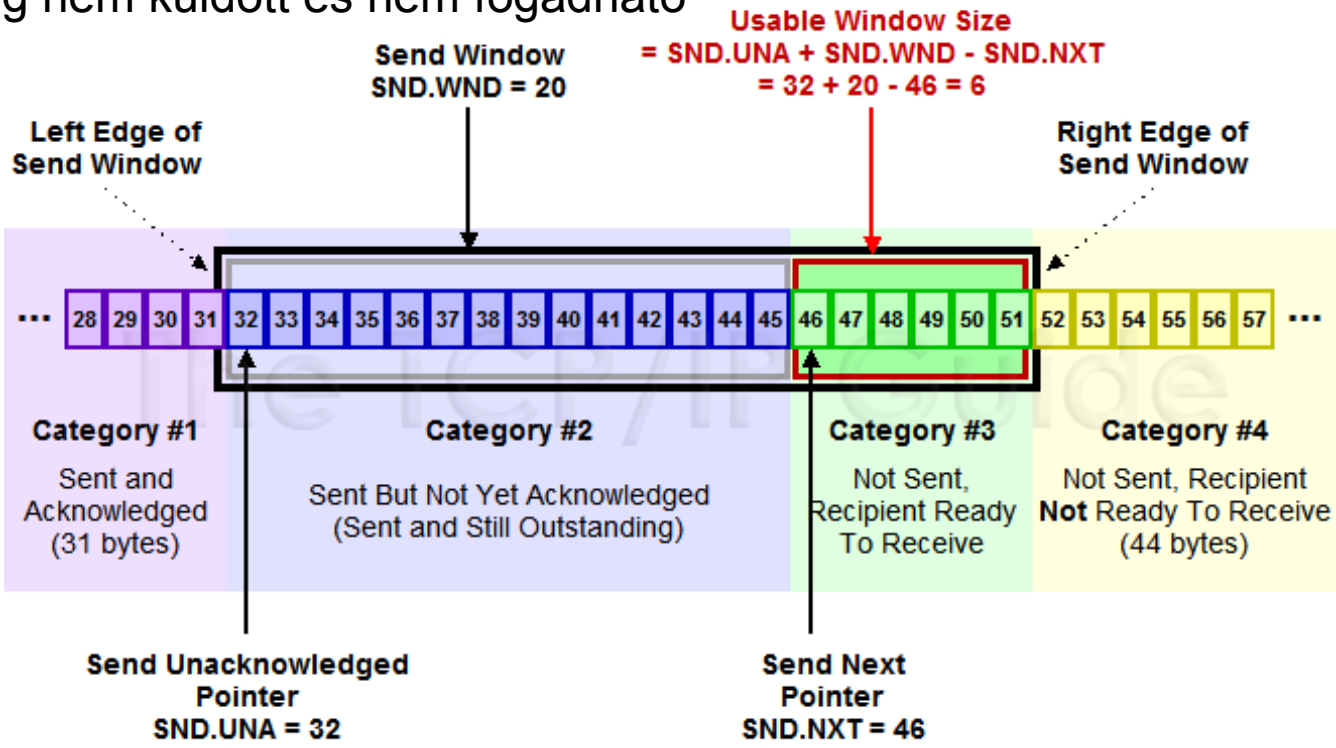
- A sorrendhelyes kézbesítés
- A duplikált csomagok eldobása
- A küldő sebességének korlátozása folyamvezérlés, vagy torlódásszabályozás céljából.

TCP

Csúszóablakos technológia

A technológia a szegmenseket négy csoportra osztja:

1) Elküldött és nyugtázott
2) Elküldött, nyugtázatlan
3) Még nem küldött, de fogadható
4) Még nem küldött és nem fogadható

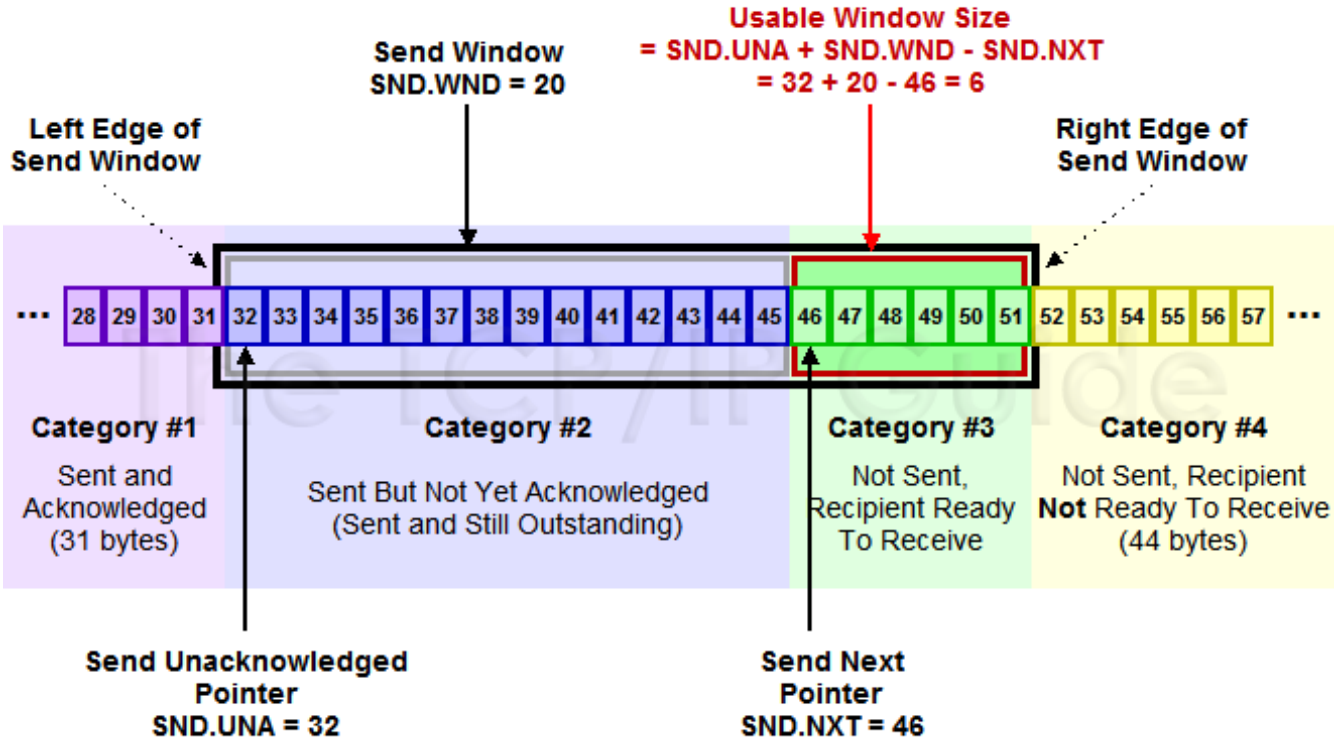


http://www.tcpipguide.com/free/t_TCPSlidingWindowDataTransferandAcknowledgementMech-2.htm u.l. 2016.08.30.

TCP

Csúszóablakos technológia

Az ablak bal széle mindig az utolsó küldött és nyugtázott bájt.
Az ablakon belül tetszőleges pozícióra érkező bájtokat elfogadjuk.
A duplikált és az ablakon kívüli szegmenseket eldobjuk.
A sebesség szabályozása az ablakméret változtatásával lehetséges.



http://www.tcpipguide.com/free/t_TCPSlidingWindowDataTransferandAcknowledgementMech-2.htm u.l. 2016.08.30.

TCP

A TCP protokoll rendkívül összetett, számos fontos de túlontúl komplex lehetőségét és javítását jelen tárgy keretein belül nincs lehetőség tárgyalni.

További áttekintésre ajánlottak a diák alján szereplő források, illetve a diasor elején hivatkozott összefoglaló művek.

Kapcsolódó fontosabb RFC dokumentumok:

- RFC 675 - Internet Transmission Control Program specifikációja (1974. 12)
- RFC 793 - TCP v4
- RFC 1122 - TCP néhány hibajavítását tartalmazza
- RFC 1323 - TCP-Kiegészítések
- RFC 2018 - TCP szelektív nyugtázás
- RFC 2883 - Szelektív nyugtázás kiegészítése (D-SACK)

Az alkalmazási réteg

Az alkalmazási réteg protokolljai

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

Interész (interface): Kapcsolódási felület. Az informatika számos területén előforduló fogalom. Való életből vett példa: Az autót a sofőr egy interészen keresztül irányítja (kormány, pedálok, kapcsolók).

“Az internethez csatlakoztatott végrendszerek egy alkalmazói programinterfészt (**Application Programming Interface – API**) biztosítanak, amely meghatározza, hogy egy végrandszeren futó szoftver hogyan kéri meg az internet infrastruktúrát arra, hogy eljuttasson valamilyen adatot egy bizonyos célszoftverhez, amely egy másik végrendszeren fut.” (Kurose, Ross)

Az alkalmazási réteg protokolljai

Hibrid modell

Alkalmazási

Socket API

Szállítási

Hálózati

Adatkapcsolati

Fizikai

A socket a gyakorlatban egy protokoll + port páros, amelyen keresztül az alkalmazási rétegbeli szolgáltatás kommunikál az alsóbb rétegekkel.

A jól ismert szolgáltatások protokoll port párosai linux rendszeren: **/etc/services**

Ugyanez a file windows rendszerek alatt: C:/WINDOWS/system32/drivers/etc/services

Az alkalmazási réteg protokolljai

Milyen alkalmazási rétegbeli protokollokat ismerünk?

File átvitel:

FTP

TFTP

Névfeloldás

DNS

IRC

SSH

Bittorrent

Böngészés

HTTP

HTML

Levélküldés

e-mail

POP3

IMAP

SMTP

MIME

Telnet

NFS

Névfeloldás

Mivel hálózatok felhasználói emberek, természetes igény, hogy a hálózat csomópontjaira ne csak az IP cím segítségével, hanem valamilyen név megadásával is lehessen hivatkozni.

A legegyszerűbb megoldás egy **szótárfájl** alkalmazása, mely IP cím – név összerendeléseket tartalmaz. (hosts fájl)

A hálózatba kötött csomópontok számának növekedésével a fájl menedzsmentje lokálisan kivitelezhetetllenné válik. Megoldás: fájl letöltése központi **hosts szerver**ekről.

A fájlok méretének növekedésével és a módosítások gyakoriságának emlekedésével a központi fájl is kezelhetetlenné válik. Megoldás: Központi dinamikus elosztott adatbázis alkalmazása → **DNS**.

DNS

A DNS (Domain Name System) egy hierarchikus tartomány-alapú névkiosztási séma, melyet elosztott adatbázis, segítségével valósítanak meg, RFC 1034, 1035

A DNS legszélesebb körben ismert alkalmazása az IP címekhez történő névhozzárendelés az Interneten, ugyanakkor egyrészt segítségével más erőforrások is cimkézhetők, másrészt igen széles körben használatos vállalati és magánhálózatok kialakításakor is.

A tartománynevek rendszere (DNS) három fő komponensből áll:

1) Tartománynevek tere és erőforrásrekordok
2) Névszerverek
3) Címfeloldó (resolver) programok

DNS

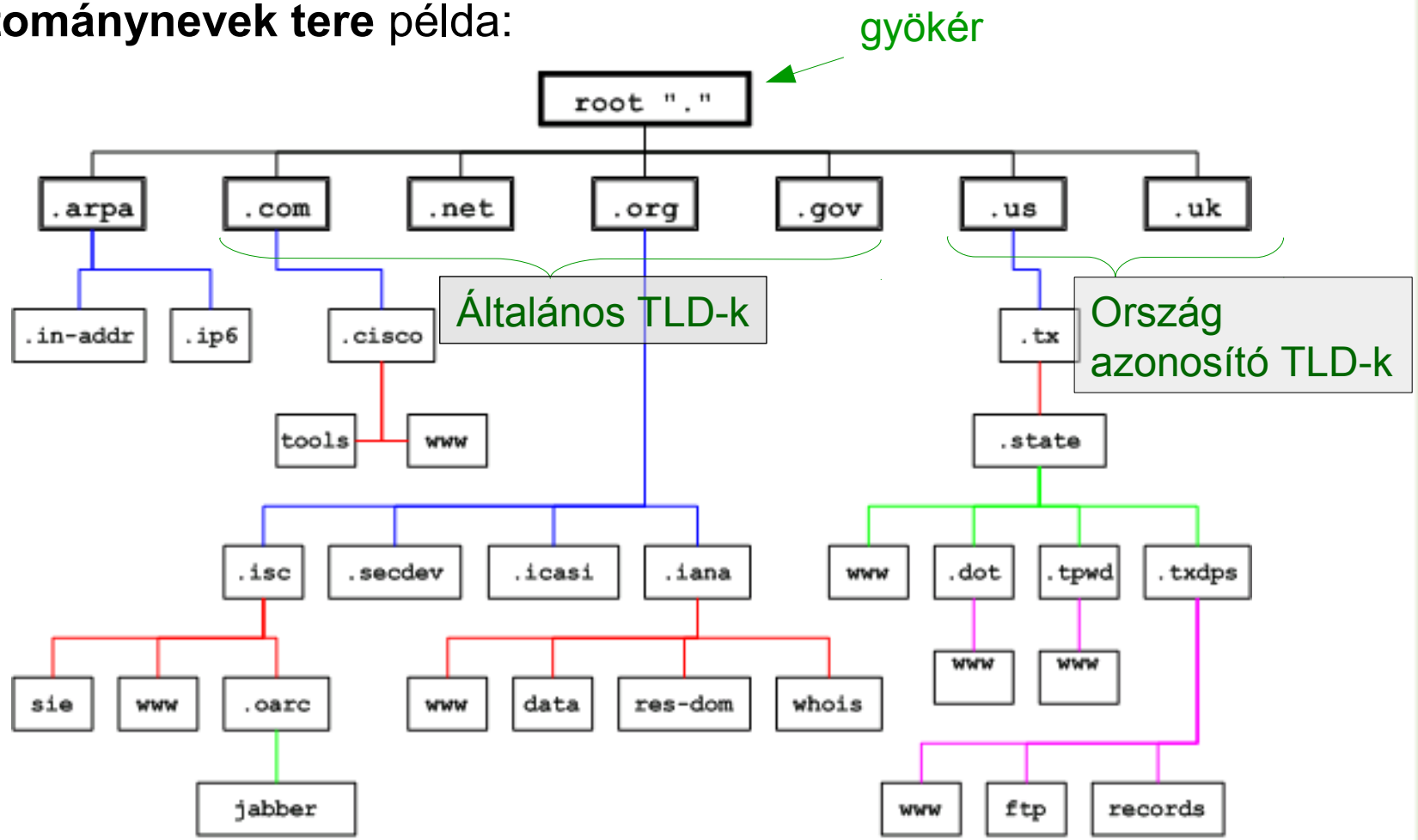
Tartománynevek tere és erőforrásrekordok

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

Abszolút tartománynév: A tartománynevek terében bármely csúcs egyértelműen reprezentálható a csúcstól a gyökérig vezető utat leíró címkesorozattal.

DNS

Tartománynevek tere példa:

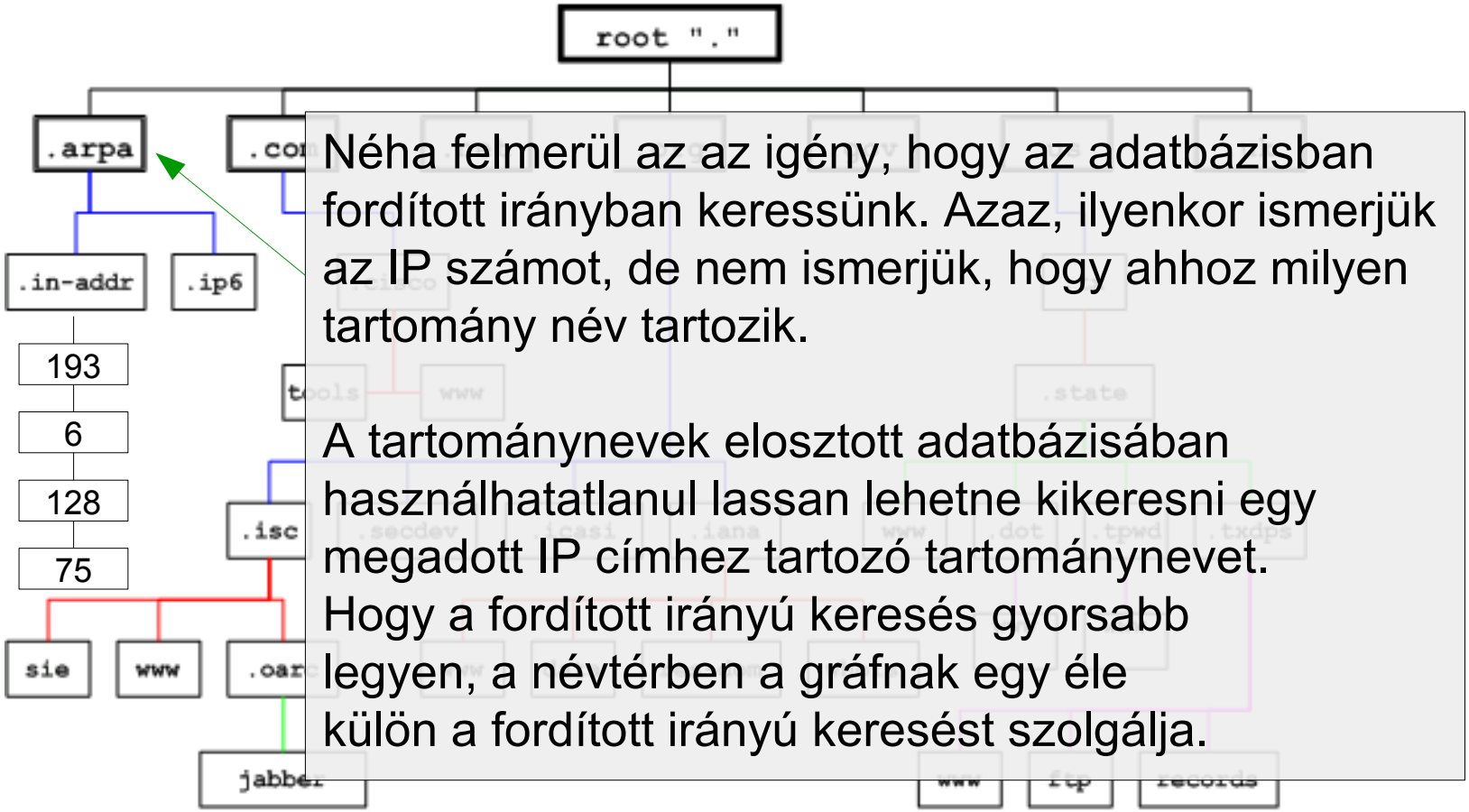


Ebben a gráfban egy abszolút nél pl: www.tped.state.ta.us

http://www.cisco.com/web/about/security/intelligence/dns-bcp.html (u.l. 2016.08.30)

DNS

Tartománynevek tere példa:



Néha felmerül az az igény, hogy az adatbázisban fordított irányban keressünk. Azaz, ilyenkor ismerjük az IP számot, de nem ismerjük, hogy ahhoz milyen tartomány név tartozik.

A tartománynevek elosztott adatbázisában használhatatlanul lassan lehetne kikeresni egy megadott IP címhez tartozó tartománynevet. Hogy a fordított irányú keresés gyorsabb legyen, a névtérben a gráfnak egy éle külön a fordított irányú keresést szolgálja.

http://www.cisco.com/web/about/security/intelligence/dns-bcp.html (u.l. 2016.08.30)

DNS

Tartománynevek tere és **erőforrásrekordok**

- A tartománynevek egy-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: Az a tartománynév, amelyhez a RR tartozik.
Osztály: 16 bites érték, mely egy protokollcsaládot/protokollt azonosít.
IN: az internet protokollcsalád
CH: A Chaos protokollcsalád (Moon A. David, Chaosnet, https://dspace.mit.edu/bitstream/handle/1721.1/6353/AIM-628.pdf?sequence=2)
Élettartam (TTL): 32 bites érték: A RR max. felhasználhatósági ideje (sec).
Típus: 16 bites érték a típus szerinti tagoláshoz.
Adat

DNS

Tartománynevek tere és **erőforrásrekordok**

Legfontosabb RR típusok:

Típus	Adat	Leírás
A	32 bites IP cím (IN osztály esetén).	A tulajdonos hálózati címe
CNAME	Tartománynév	Egy alias névhez kanonikus név rendelése
HINFO	Tetszőleges sztring.	CPU, op. rsz. információk meghatározása
MX	16 bites prioritás érték és egy tartománynév.	Levélforgalmazó (mail exchange) megadása
NS	Egy host tartományneve	Névszerver rendelése a tartományhoz
PTR	Egy tartománynév	Pointer a névtér egy másik területére
SOA	Több mezőből álló rekord	Hitelességi (authority) zóna specifikációja

DNS

Tartománynevek tere és erőforrásrekordok

A tartománynevek tere két (természetes) módon darabolható:

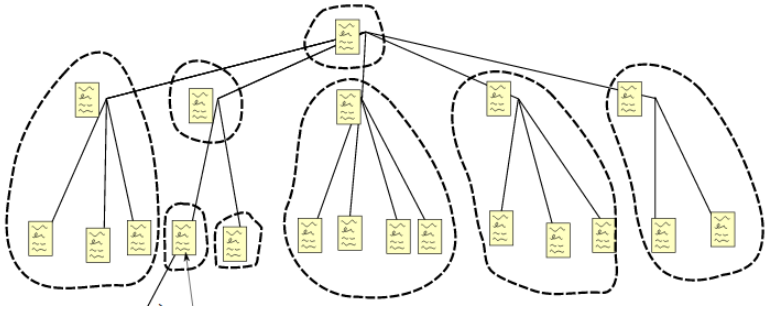
1.) **Az osztálytagozódás alapján.**
A különböző osztályok parallel névtér-faként foghatók fel.

2.) **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.

Az „átvágásokat” nyilván kell tartanunk.



http://courses.ischool.berkeley.edu/i253/f11/internet#(24) (u.l. 2016.08.30)

DNS

Névszerverek

Információt tárolnak a tartománynevek gráfjáról.

Tartománynevekhez tartozó erőforrás rekordokat tárolnak.

Kérdéseket (lekérdezéseket) válaszolnak meg.

Minden szerver **authoritatív** az általa kezelt zónában és **nem authoritatív** az általa csak cachelt információkra.

DNS szerver típusok:

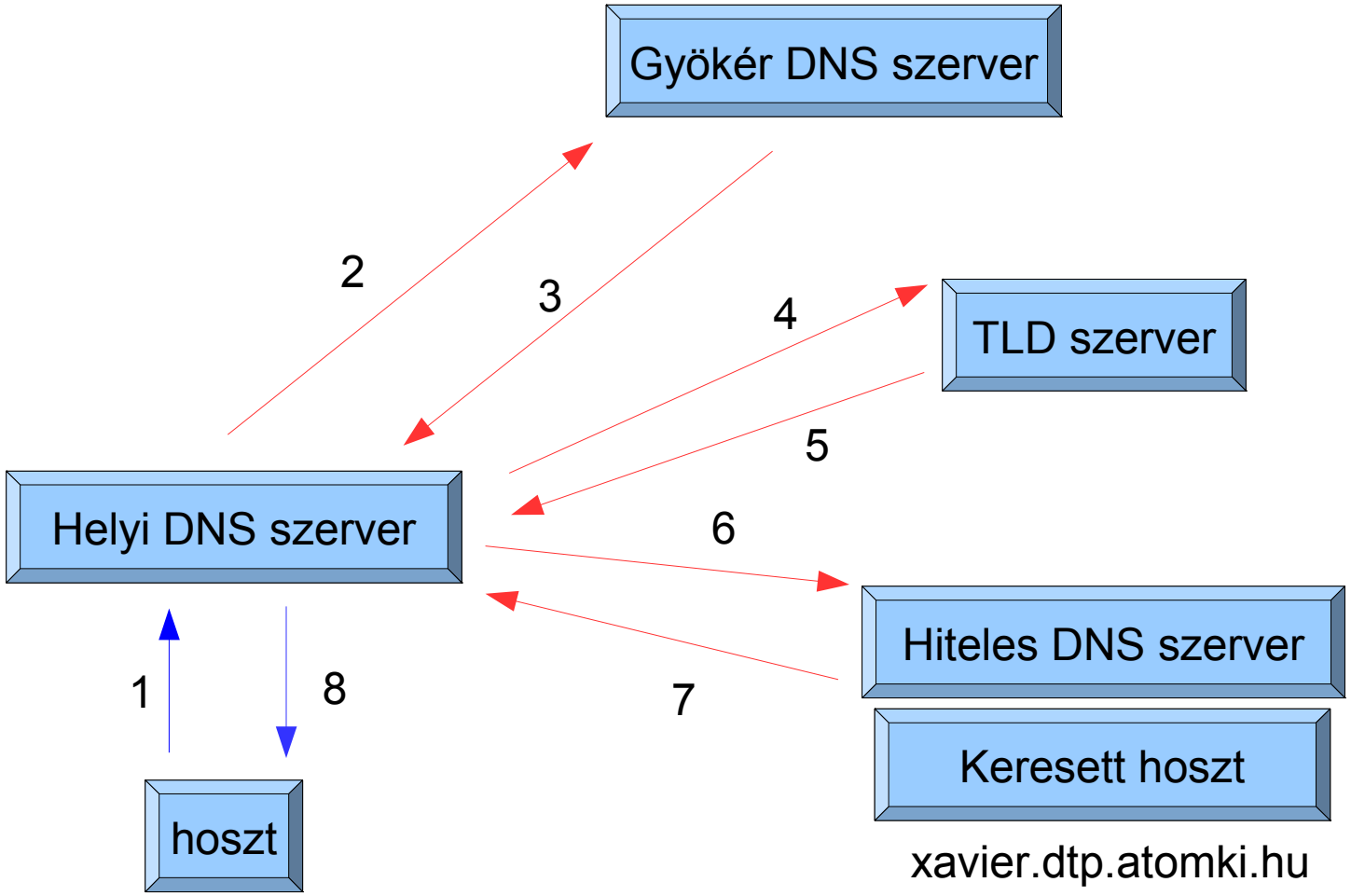
Gyökér DNS szerverek (összesen 13 db. A-M-ig)

TLD (Top Level Domain) szerverei. Pl országok szerverei (hu, fr, com ...)

Hiteles DNS szerverek: minden olyan szervezet, mely nyilvánosan elérhető hosztokat üzemeltet, nyilvános DNS bejegyzéseket kell, hogy szolgáltasson. Ezt saját hiteles DNS szerverén keresztül teheti meg.

Helyi DNS szerver: Nem tartozik szorosan a DNS hierarchiába, ugyanakkor fontos a szerepük pl a chachelés miatt.

DNS lekérdezés működése



Kérdés: xavier.dtp.atomki.hu

DNS lekérdezés működése

Nem rekurzív (iteratív) 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.

DNS

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

HTTP

HyperText Transfer Protocol – RFC 1945, RFC 2616, Port: 80
Alkalmazásszintű protokoll elosztott, kollaboratív hipermédia rendszerekhez.
Jelenlegi verzió (2015.09.): 1.1 Fejlszetés alatt: 2.0

HTTPS: A HTTP és a szállítási rétegbeli TCP közé titkosítást ékelünk

A weboldalak objektumokból állnak. Többnyire egy alap HTML (Hypertext Markup Language) fájl és az ott hivatkozott egyéb objektumok.

Az objektumokat ún. **URL (Uniform Resource Locator)** segítségével hivatkozhatjuk. (*Az URL egy speciális URI (UR Identifier), ahol az objektumokra a helyük alapján hivatkozunk. URI-kat más területeken is alkalmazhatunk.*)

Szintaxis:

```
http://host [':' port] [útvonal] ['?' lekérdezés]
```

Például:

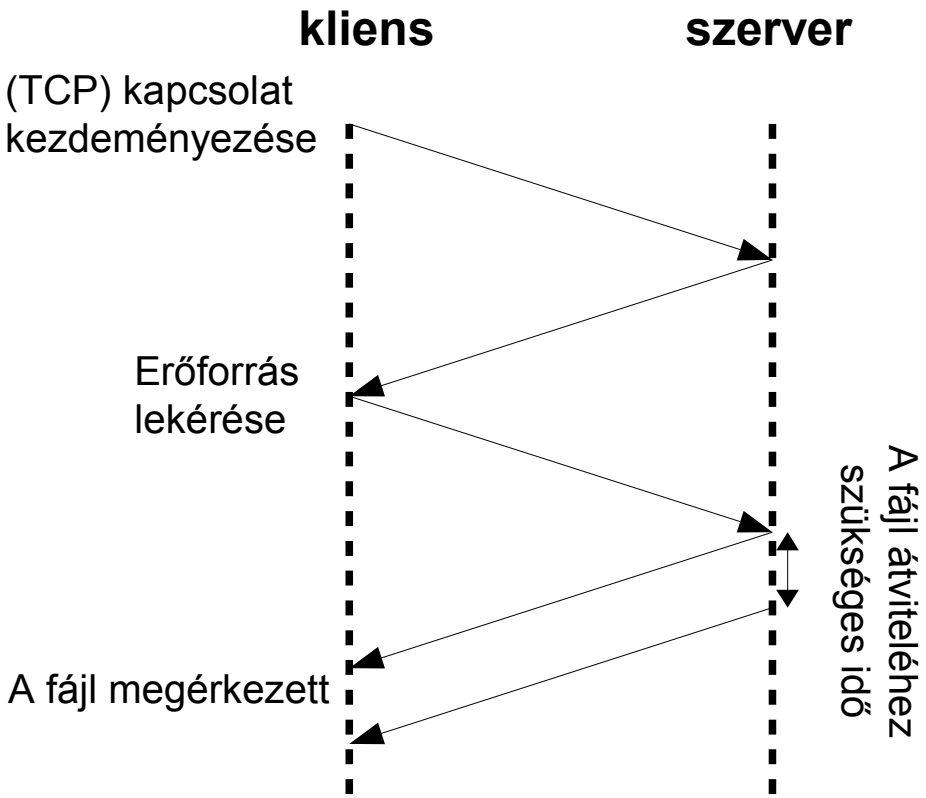
```
https://www.youtube.com:443/watch?v=oHg5SJYRHA0
```

A HTTP-ről sokkal bővebben: http://www.inf.unideb.hu/~jeszy/download/ie/http.pdf (u.l. 2016.08.30.)

HTTP

HTTP kommunikáció során kérés-válasz párok váltják egymást

HTTP lekérdezés menete



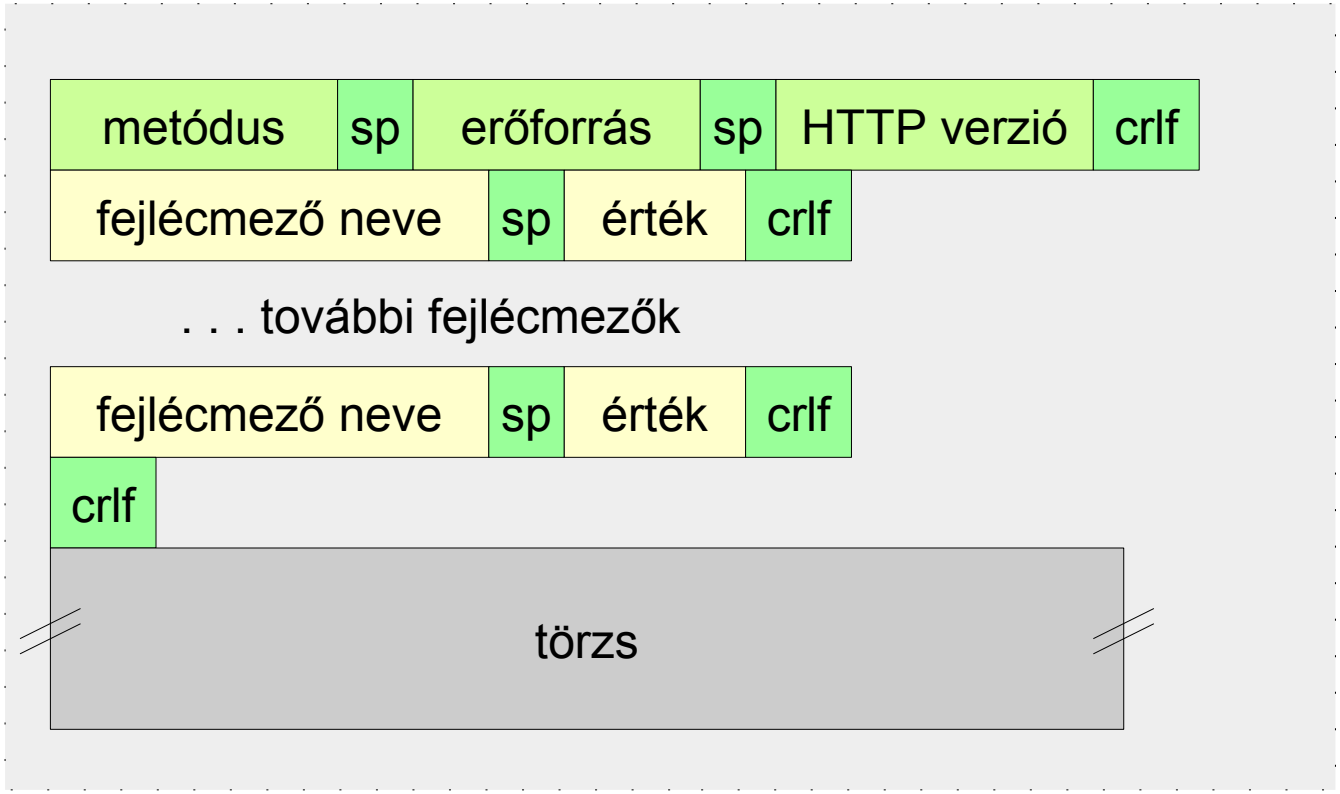
Alapesetben az ábrán látható folyamat a letölteni kívánt tartalom minden objektumára megismétlődik.

Javítás: HTTP 1.1 **perzisztens kapcsolatok**: Egy kiépített kapcsolaton keresztül több kérés is megvalósítható.

HTTP

HTTP kommunikáció során kérés-válasz párok váltják egymást

Kérés formátuma:



sp space (szóköz)

crlf sortörés (carriage return, line feed)

HTTP

HTTP kommunikáció során kérés-válasz párok váltják egymást

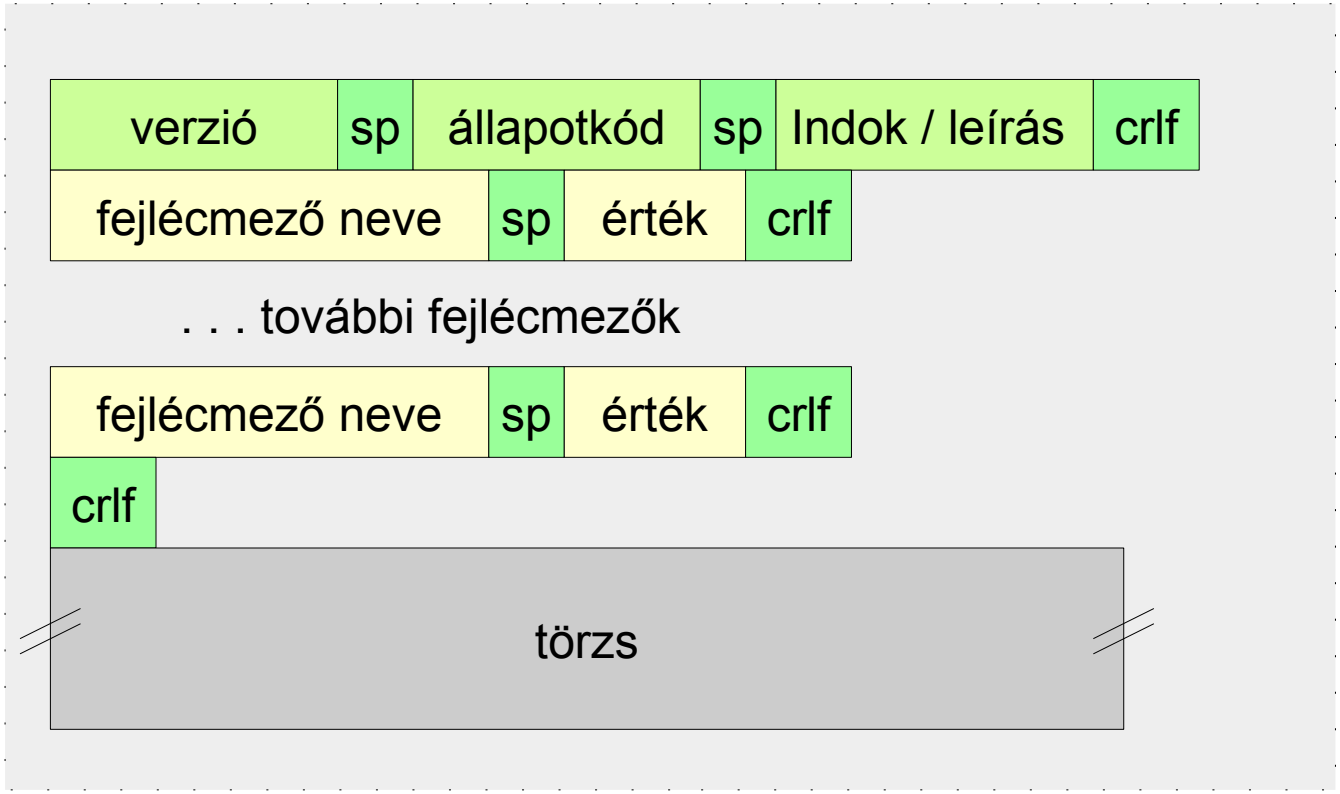
HTTP metódusok:

GET	Erőforrás lekérdezése
HEAD	Törzs nélküli GET (pl. metaadatok elérésére)
POST	A kérésben szereplő adatok feldolgozásának kérése a szervertől (pl. űrlapok)
PUT	Erőforrás feltöltése
DELETE	Erőforrás törlése
OPTIONS	Cél erőforrás kommunikációs opcióinak lekérdezése
TRACE	Kérés visszaküldésének kérése
CONNECT	Proxy kapcsolat alagút létrehozása

HTTP

HTTP kommunikáció során kérés-válasz párok váltják egymást

Válasz formátuma:



sp space (szóköz)

crlf sortörés (carriage return, line feed)

HTTP

HTTP kommunikáció során kérés-válasz párok váltják egymást

HTTP állapotkódok:

Az első számjegy a válasz fajtáját határozza meg. A klienseknek nem szükséges megérteniük minden regisztrált állapotkód jelentését, kötelező azonban az állapotkód fajtájának megértése az első számjegy alapján

1xx: Informational (tájékoztató)
A végső választ megelőző ideiglenes választ jelez A kérés csak az állapotsorból és opcionális fejlécből áll, a végét üres sor jelzi.

2xx: Success (siker)
A szerver megkapta, megértette és elfogadta a kérést

3xx: Redirection (átirányítás)
A kérés kiszolgálásához a felhasználói ágens további művelet kell, hogy végrehajtson, ezt automatikusan elvégezheti

4xx: Client Error (kliens hiba)

5xx: Server Error (szerver hiba)

HTTP

HTTP kommunikáció során kérés-válasz párok váltják egymást

HTTP állapotkódok:

Az első számjegy a válasz fajtáját határozza meg. A klienseknek nem szükséges megérteniük minden regisztrált állapotkód jelentését, kötelező azonban az állapotkód fajtájának megértése az első számjegy alapján

Példák:

200 OK: A kérés sikeres volt

301 Moved Permanently: A kért erőforrást áthelyezték. Az új cím a fejlécben található. A kliens automatikusan az új helyre lép.

400: Bad request: Általános hiba. A szerver nem tudja értelmezni a kérést.

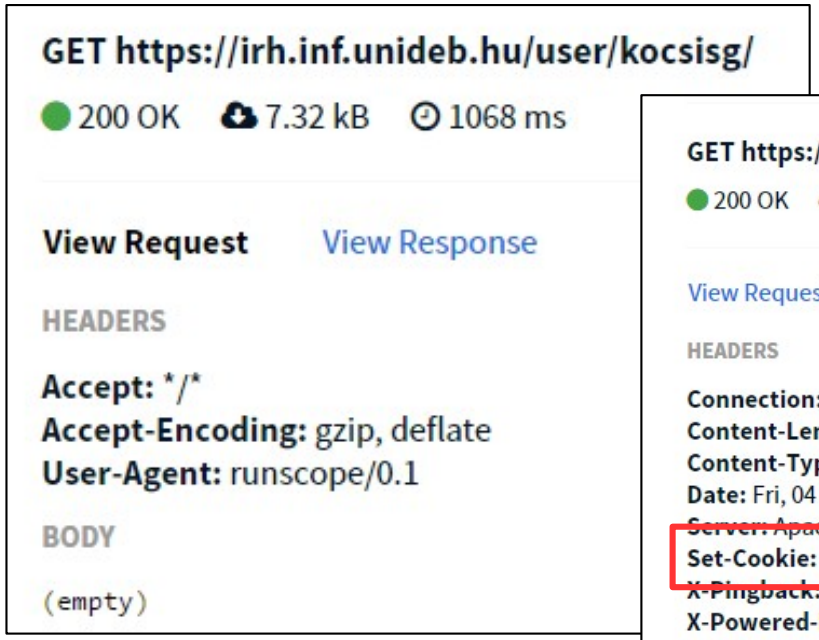
404 Not Found: A kért erőforrás nem található a szerveren.

505 HTTP Version Not Supported: A HTTP protokoll használni kívánt verzióját a szervver nem támogatja

HTTP

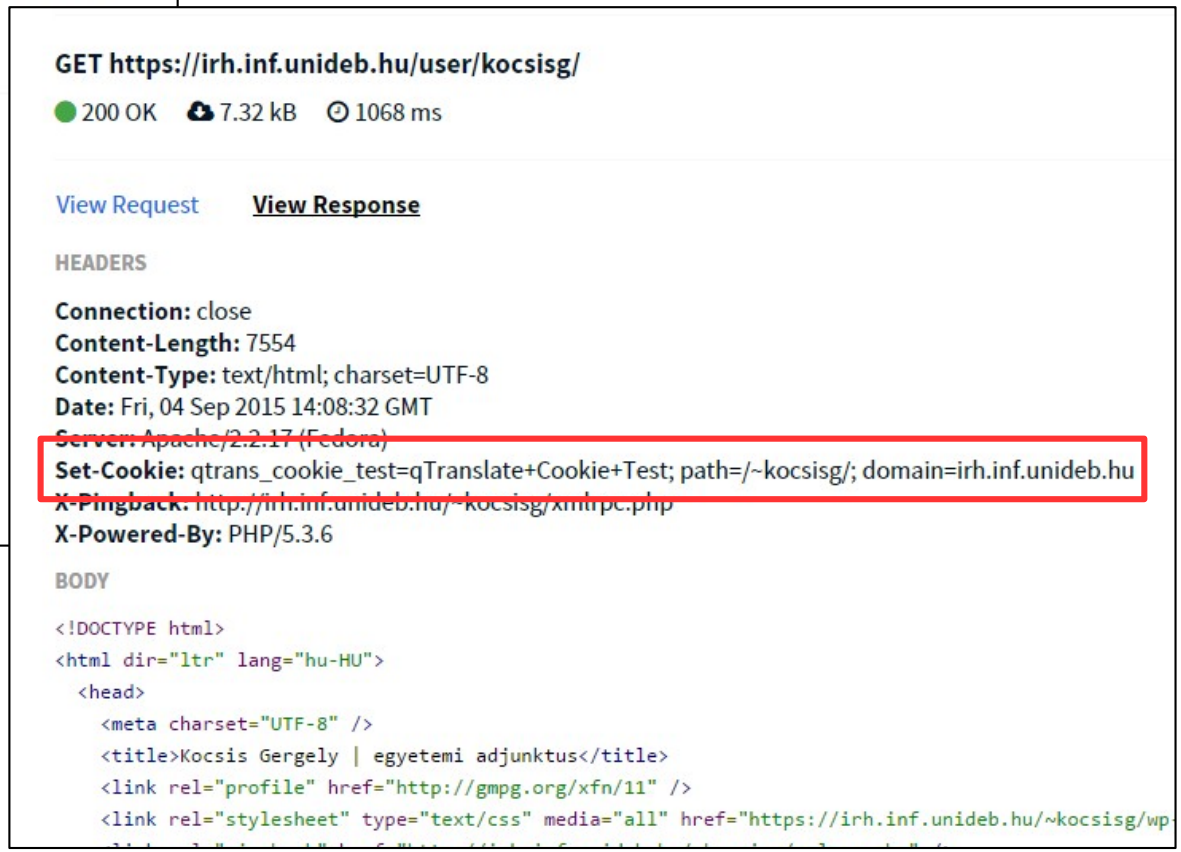
HTTP kérés válasz példa

https://www.hurl.it/



kérés

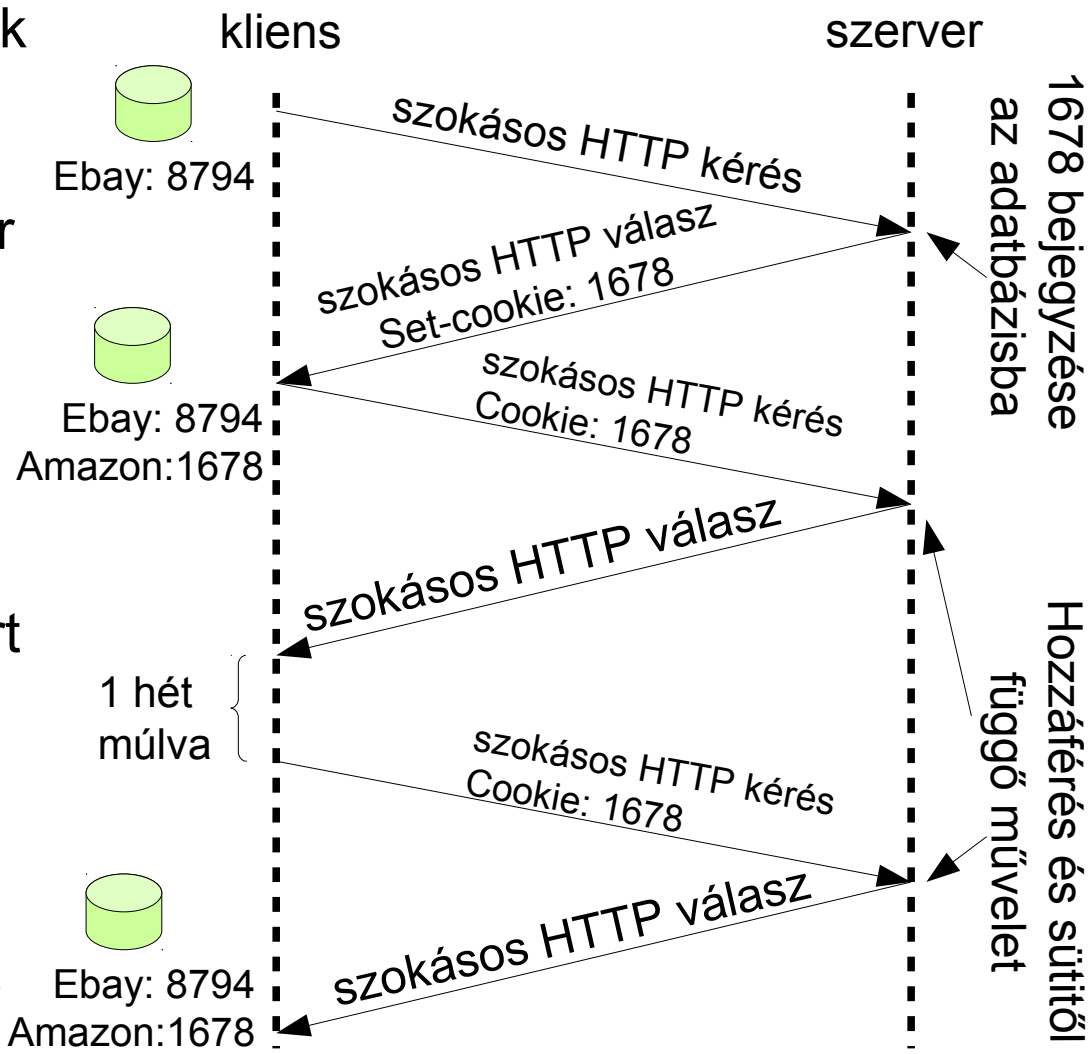
válasz



HTTP

Süti (cookie): Egy név-érték pár és kapcsolódó metaadatok (attribútumok), melyeket egy eredet szerver a válaszok Set-Cookie fejlécmezőjében küld a felhasználói ágenseknek

Az attribútumok révén az eredet szerver egy hatáskört határozhat meg, s a felhasználói ágensek a további kérésekben a név-érték párt a Cookie fejlécmezőben küldik vissza az eredet szervernek



HTML

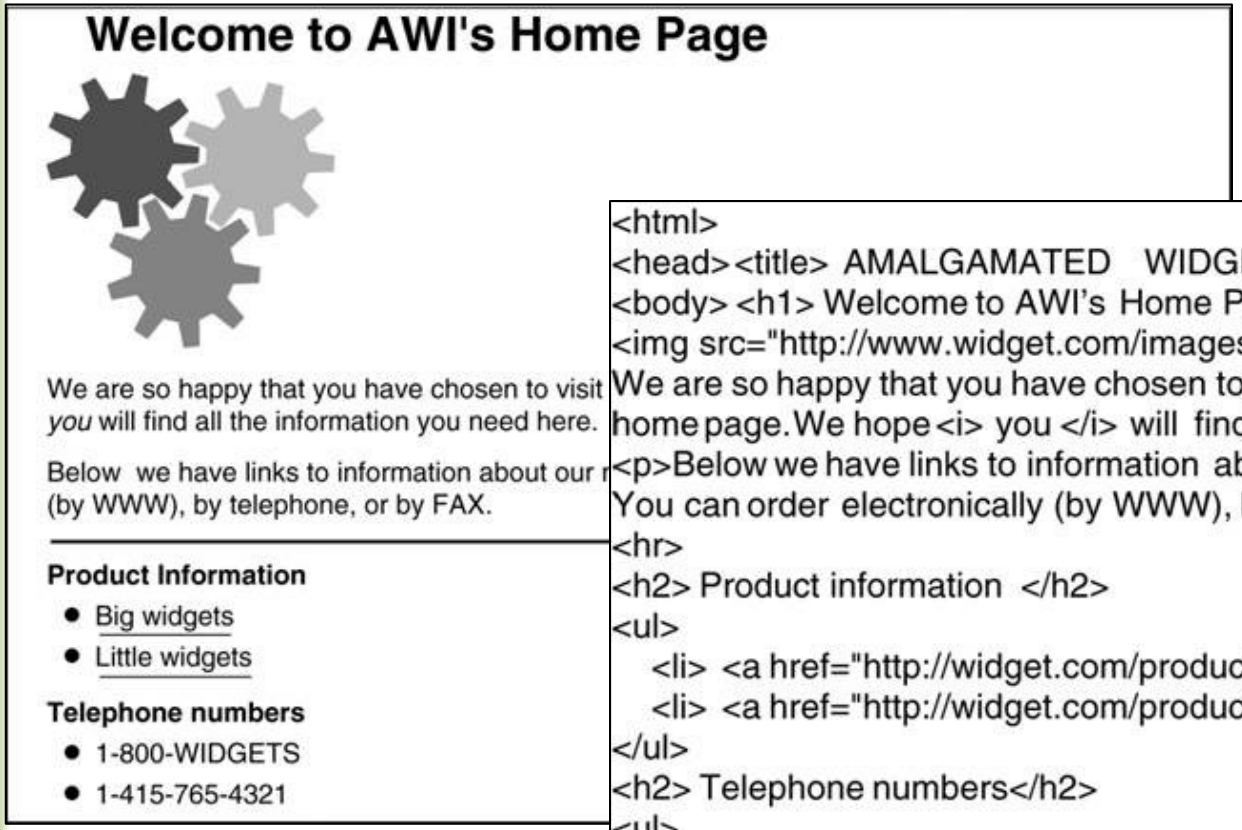
Hiperszöveg/hypertext: “A hypertext olyan interaktív dokumentum, mely linkeket biztosít az olvasónak a szövegek közti átjárhatóság céljából. Ezeken a linkeken tovább lehet haladni más szövegek felé.” (Szűts Zoltán – A Hypertext http://magyar-irodalom.elte.hu/vita/szuts/00beve.html u.l. 2016.08.30.)

HTML (HyperText Markup Language)

- Egy olyan jelölőonyelv, amelyben utasításokkal írjuk le, hogy hogyan kell a tartalmat megjeleníteni
- Őse: ISO standard 8879:1986: Standard Generalized Markup Language (SGML)
- Szöveges utasításai vannak minden olyan szempontra, ami szerint dokumentumokat meg lehet jeleníteni
- Jelenlegi verzió: HTML 5 (2014-)

HTML

HTML példa:




```
<html>
<head><title> AMALGAMATED  WIDGET, INC. </title> </head>
<body> <h1> Welcome to AWI's Home Page</h1>
<img src="http://www.widget.com/images/logo.gif" ALT="AWI Logo"> <br>
We are so happy that you have chosen to visit <b> Amalgamated Widget's </b>
home page. We hope <i> you </i> will find all the information you need here.
<p>Below we have links to information about our many fine products.
You can order electronically (by WWW), by telephone, or by fax. </p>
<hr>
<h2> Product information </h2>
<ul>
   <li> <a href="http://widget.com/products/big"> Big widgets </a>
   <li> <a href="http://widget.com/products/little"> Little widgets </a>
</ul>
<h2> Telephone numbers</h2>
<ul>
   <li> By telephone: 1-800-WIDGETS
   <li> By fax: 1-415-765-4321
</ul>
</body>
</html>
```

(a)

FTP

File Transfer Protocol – RFC 114 (1971) [RFC 959 (1985)], Port: 20, 21

Legegyszerűbb FTP parancsok:
USER name
PASS jelszo
CD, RETRIEVE, STORE, MKDIR, RMDIR, HELP, BYE

Névtelen belépés esetén a felhasználónév szabvány szerint anonymous, a jelszó mezőt pedig üresen kell hagyni

Az FTP protokoll két csatornával dolgozik:

Vezérlő csatorna (Control connection) – Itt folyik a szerver-kliens üzenetváltás

Adat csatorna (Data connection) – Itt történik az adatáramoltatás (minden új adatfolyamhoz új csatorna)

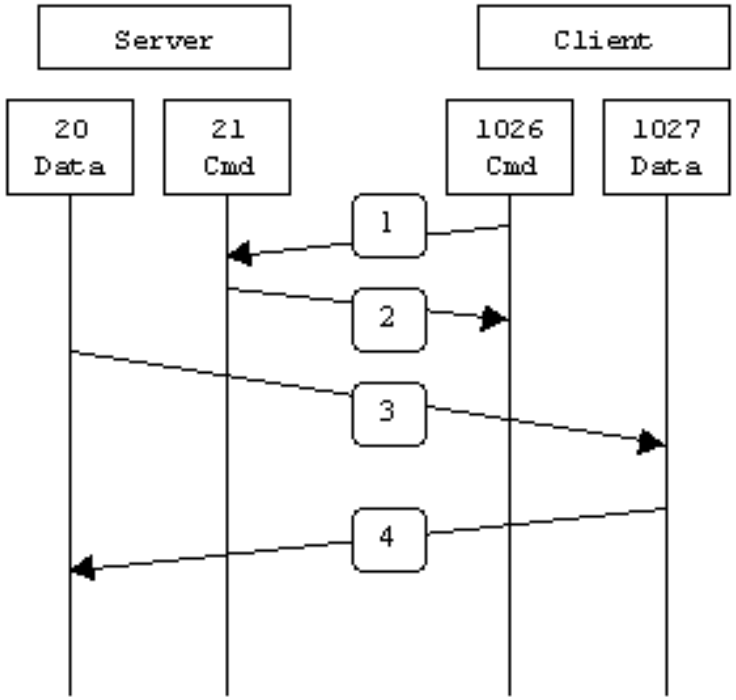
Aktív és passzív FTP

Az FTP kapcsolódás kezdetén kiépül a vezérlő csatorna a kliens egy adott portja és a szerver 21-e portja között.

Az aktív és passzív mód az adatcsatorna kiépítésének módját jelenti.

Aktív módban a kliens nyit egy portot, amihez a szerver csatlakozik (azaz aktív cselekvést végez)

Passzív módban a kliens jelzi adatátviteli szándékát, mire a szerver nyit egy portot, majd (passzívan) várakozik. Emellett a port számát elküldi a kliensnek, ami alapján az csatlakozni tud.



http://slacksite.com/other/ftp.html u.l. 2016.08.30.

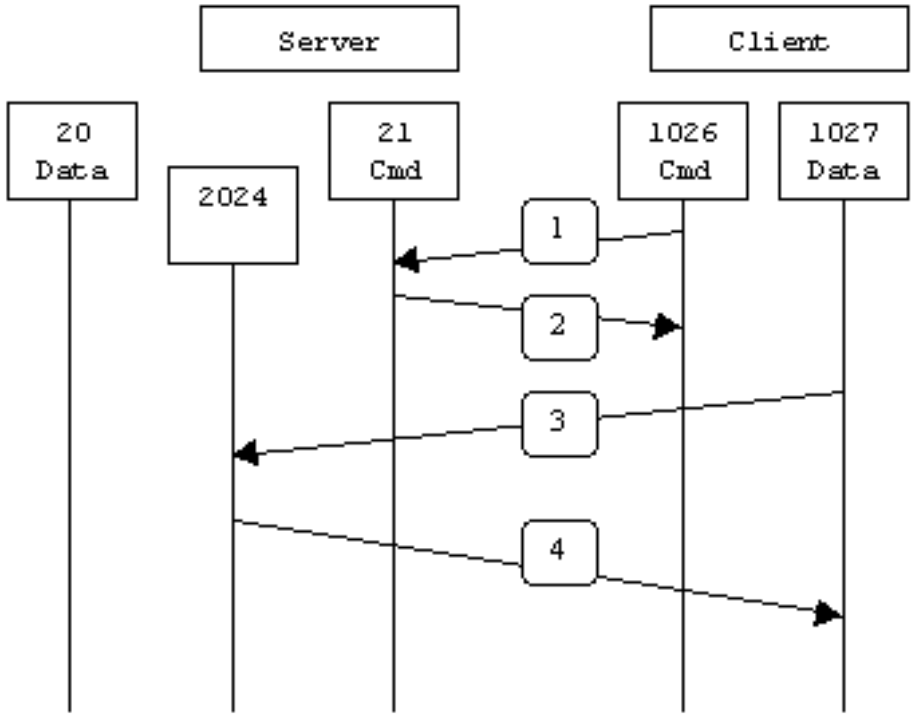
Aktív és passzív FTP

Az FTP kapcsolódás kezdetén kiépül a vezérlő csatorna a kliens egy adott portja és a szerver 21-e portja között.

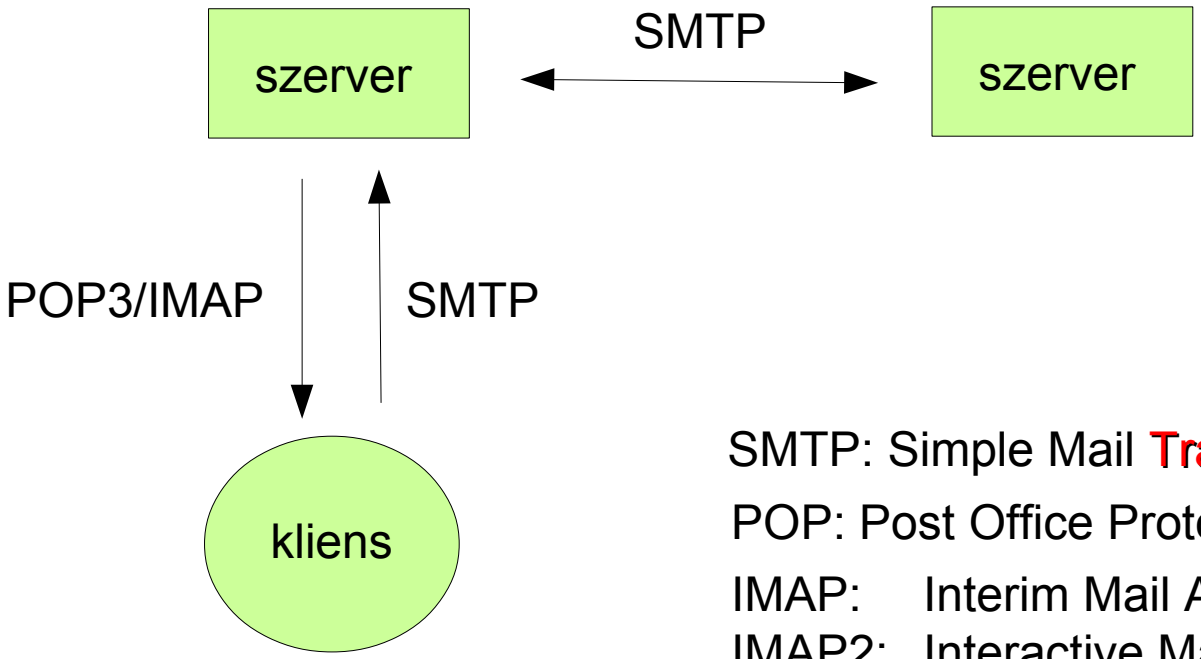
Az aktív és passzív mód az adatcsatorna kiépítésének módját jelenti.

Aktív módban a kliens nyit egy portot, amihez a szerver csatlakozik (azaz aktív cselekvést végez)

Passzív módban a kliens jelzi adatátviteli szándékát, mire a szerver nyit egy portot, majd (passzívan) várakozik. Emellett a port számát elküldi a kliensnek, ami alapján az csatlakozni tud.



e-mail



SMTP: Simple Mail Transfer Protocol

POP: Post Office Protocol

IMAP: Interim Mail Access Protocol
IMAP2: Interactive Mail Access Protocol
IMAP4: Internet Message Access Protocol

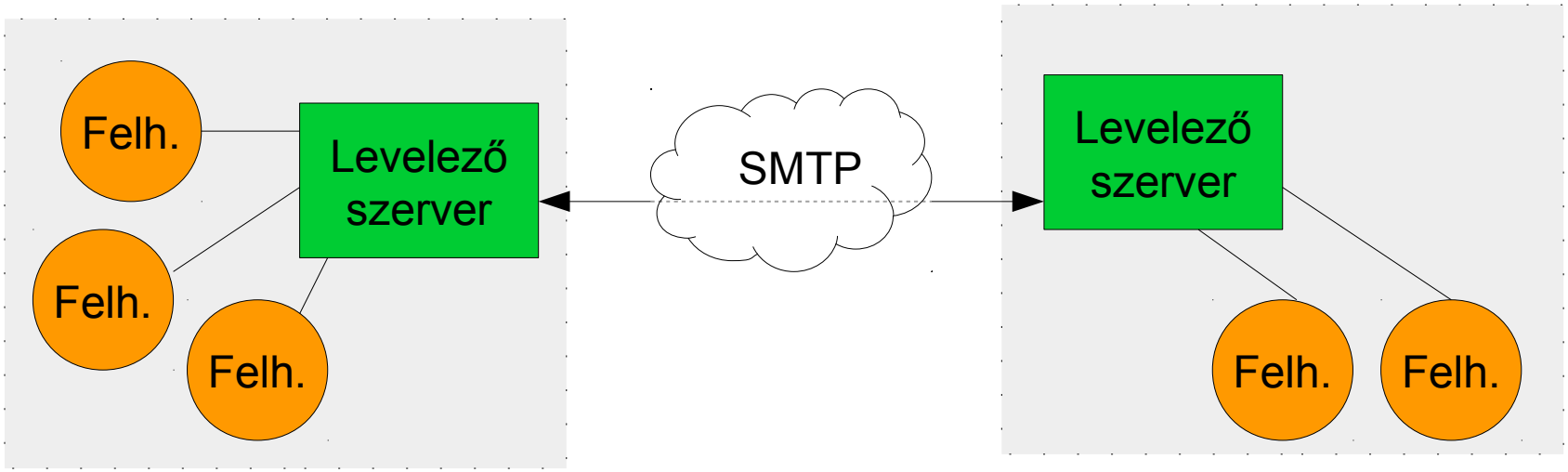
MIME: Multipurpose Internet Mail Extension

e-mail

E-mail cím felépítése: felhasználó @ levelező_szerver

Simple Mail Transfer Protocol – RFC 821 (1981) [RFC 5321 (2008)]
Port: 25

Csak a levelek továbbítására szolgál (felhasználói ügynöktől a szerverhez, illetve szerverek között)



e-mail

Levélküldés menete SMTP segítségével:

1) A küldő feltölti a levelét a saját kiszolgálójára SMTP segítségével.

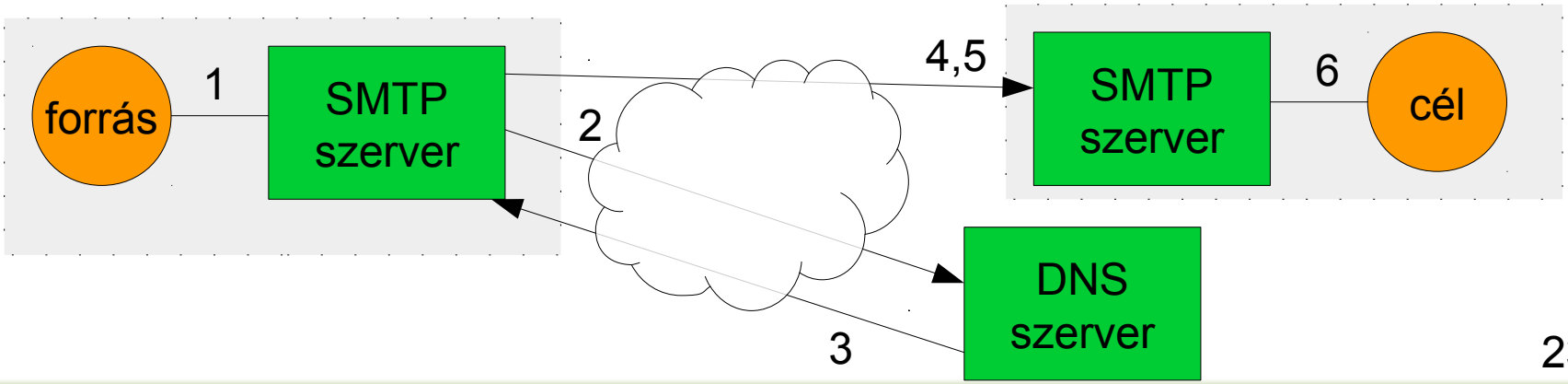
2) A küldő kiszolgáló a célcím @ utáni része alapján DNS lekérdezést indít az adott tartomány levelező kiszolgálójára (MX rekord)

3) A válasz egy, vagy több kiszolgálót mutat a fogadó oldalon.

4) A küldő kiszolgáló kapcsolatba lép (TCP) a cél kiválasztott kiszolgálójával

5) A küldő kiszolgáló átadja a levelet a fogadó kiszolgálónak

6) A fogadó oldalon a célcím @ előtti része azonosítja a felhasználót. A levelet ez a felhasználó tudja megtekinteni POP, vagy IMAP segítségével.

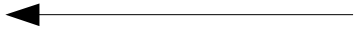


e-mail

http://www.anta.net/misc/telnet-troubleshooting/smtp.shtml u.l. 2016.08.30.

Az SMTP párbeszéd:

> telnet mx1.example.com smtp
Trying 192.0.2.2...
telnet: Connected to mx1.example.com.
telnet: Escape character is '^]'.
220 mx1.example.com ESMTP server ready Tue, 20 Jan 2004 22:33:36 +0200
HELO client.example.com
250 mx1.example.com
MAIL from: <sender@example.com>
250 Sender <sender@example.com> Ok
RCPT to: <recipient@example.com>
250 Recipient <recipient@example.com> Ok
DATA
354 Ok Send data ending with <CRLF>.<CRLF>
From: sender@example.com
To: recipient@example.com
Subject: Test message



Üres sor jelzi a levéltörzs kezdetét

This is a test message.
.
250 Message received: 20040120203404.CCCC18555.mx1.example.com@client.example.com
client: QUIT
server: 221 mx1.example.com ESMTP server closing connection

e-mail

Az SMTP párbeszéd:

Ahogy a példán is látszik, az SMTP egyszerű szöveges protokoll. Nem titkosított kommunikációt végez.
Kifejlesztésének idejében csak egy szűkebb réteg használta, nem volt szükség a felhasználók autentikációjára. Ez az oka annak, hogy **az SMTP protokoll önmagában** a máig **nem képes autentikálni** → spam

Egy lehetséges megoldási mód az **Extended SMTP** (ESMTP) használata, mely további kiterjesztéseket tartalmaz. A két protokoll között a kiszolgálók úgy tesznek különbséget, hgy míg SMTP esetén az üdvözlő üzenet HELO, ESMTP esetén ez EHLO-ra változik.

Az előző dián látható telnet alapú SMTP levélküldést a legtöbb levelező szerver tiltja (nyilvánvaló biztonsági okokból). A fentieket megengedő szervereket szokás open relay szervernek hívni (http://searchnetworking.techtarget.com/definition/open-relay u.l. 2016.08.30.).

e-mail

Levélfogadás

POP

RFC 918 (1984)
[POP3 RFC 1939 (1996)]
Port: 110 (POP3S 995)

Levelek letöltése a szerverről.
Rövid kapcsolatidő.
Levélmenedzsment a kliensen
Beállítható opciók:

Letöltés és:

- Törlés
- Olvasottnak jelölés
- Archiválás

IMAP

RFC 1370 (1984)
[IMAP4 RFC 3501 (2003)]
Port: 143 (IMAP4S 993)

Levelek elérése a szerveren
Állandó kapcsolat
Levélmenedzsment a szerveren
Hatékonyabban használható pl. többeszközös elérésre.

e-mail

MIME (Multipurpose Internet Mail Extension) - RFC 2045, RCF 2049

```
From: elinor@abcd.com
To: carolyn@xyz.com
MIME-Version: 1.0
Message-Id: <0704760941.AA00747@abcd.com>
Content-Type: multipart/alternative; boundary=qwertyuiopasdfghjklzxcvbnm
Subject: Earth orbits sun integral number of times

This is the preamble. The user agent ignores it. Have a nice day.

--qwertyuiopasdfghjklzxcvbnm
Content-Type: text/enriched

Happy birthday to you
Happy birthday to you
Happy birthday dear <bold> Carolyn </bold>
Happy birthday to you

--qwertyuiopasdfghjklzxcvbnm
Content-Type: message/external-body;
        access-type="anon-ftp";
        site="bicycle.abcd.com";
        directory="pub";
        name="birthday.snd"

content-type: audio/basic
content-transfer-encoding: base64
--qwertyuiopasdfghjklzxcvbnm--
```

Lehetővé teszi, hogy az e-mailek ne csak az angol ábécé kisbetűit tartalmazzák.

Az elektronikus levélhez további mezőket csatol (a levél szerkezetét az RFC 822 szabályozza). A mezőkben meghatározza a mező típusát és altípusát (Content-Type: type/subtype) majd paraméterek megadásával pontosítja a mező leírását.

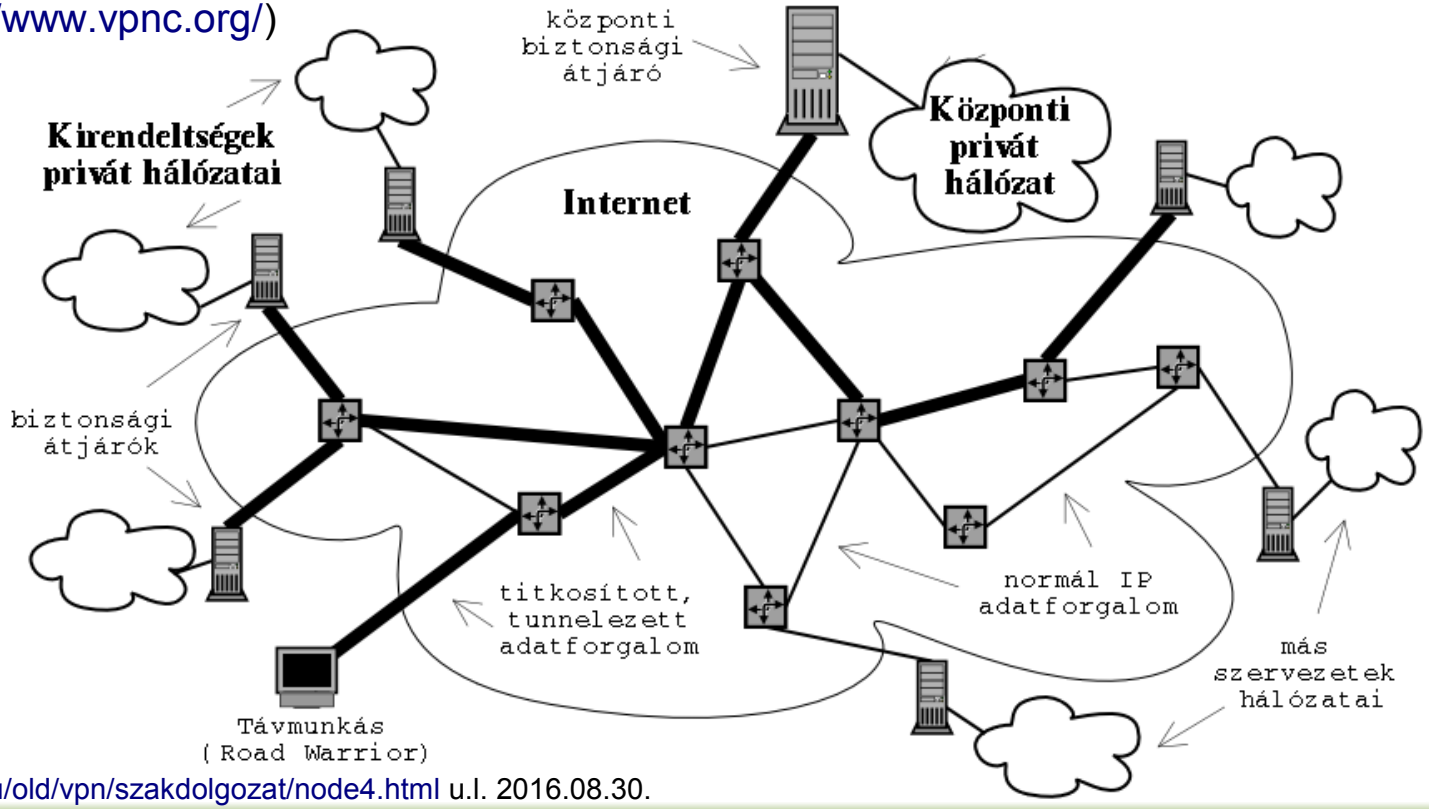
e-mail

MIME (Multipurpose Internet Mail Extension) - RFC 2045, RCF 2049

Fő típus	Altípus	Leírás
Text	Plain Enriched	Formázatlan szöveg Szöveg egyszerű formázással
Image	GIF JPEG	Állókép GIF formátumban Állókép JPEG formátumban
Audio	Basic	Hallható hang
Video	MPEG	Film MPEG formátumban
Application	Octet-stream Postscript	Bájtsorozat Nyomtatható dokumentum PostScript formátumban
Message	RFC 822 Partial External body	MIME RFC 822-es üzenet Több részre bontott üzenet Az üzenetet külön át kell hozni a hálózaton
Multipart	Mixed Alternative Parallel Digest	Független üzenetdarabok Azonos üzenet eltérő fomrátumokban Egyidejűleg megjelenítendő darabok Összefoglaló RFC 822-es üzenetekből lálló üzenet

VPN

A virtuális magánhálózat (Virtual Private Network VPN) olyan technológiák összessége, amelyek azt biztosítják, hogy egymástól távol eső számítógépek és/vagy egy szervezet által kizárólag saját céljaira kialakított és fenntartott privát hálózatok biztonságosan kommunikálhassanak egymással, valamilyen publikus hálózaton keresztül (ez tipikusan az Internet), amelyben nem bíznak meg.
(http://www.vpnc.org/)

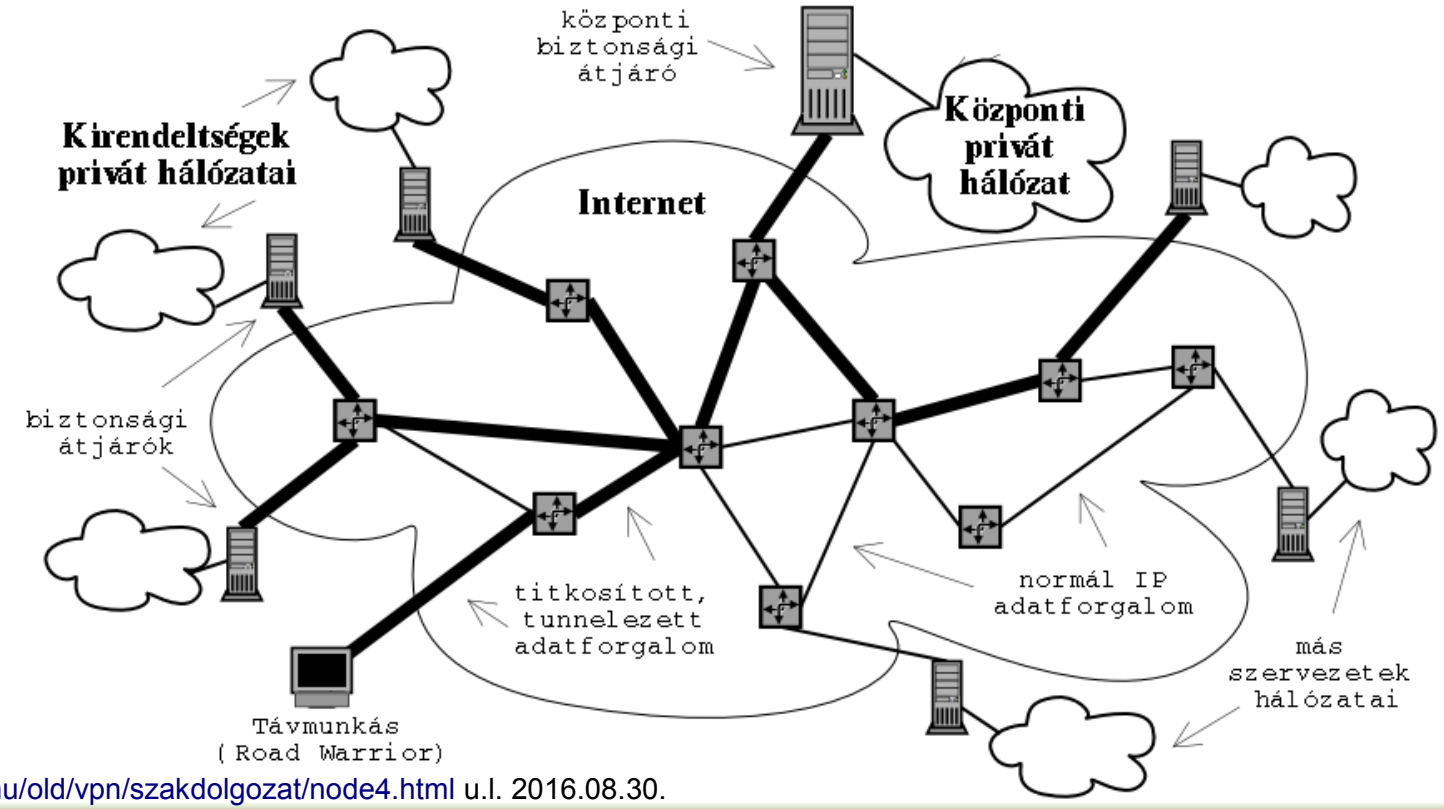


http://hup.hu/old/vpn/szakdolgozat/node4.html u.l. 2016.08.30.

VPN

A VPN megoldások két fajtáját különböztetjük meg:

- **Távoli elérést biztosító Remote Access VPN**
- **Hálózatrészek közötti Site-to-Site VPN**



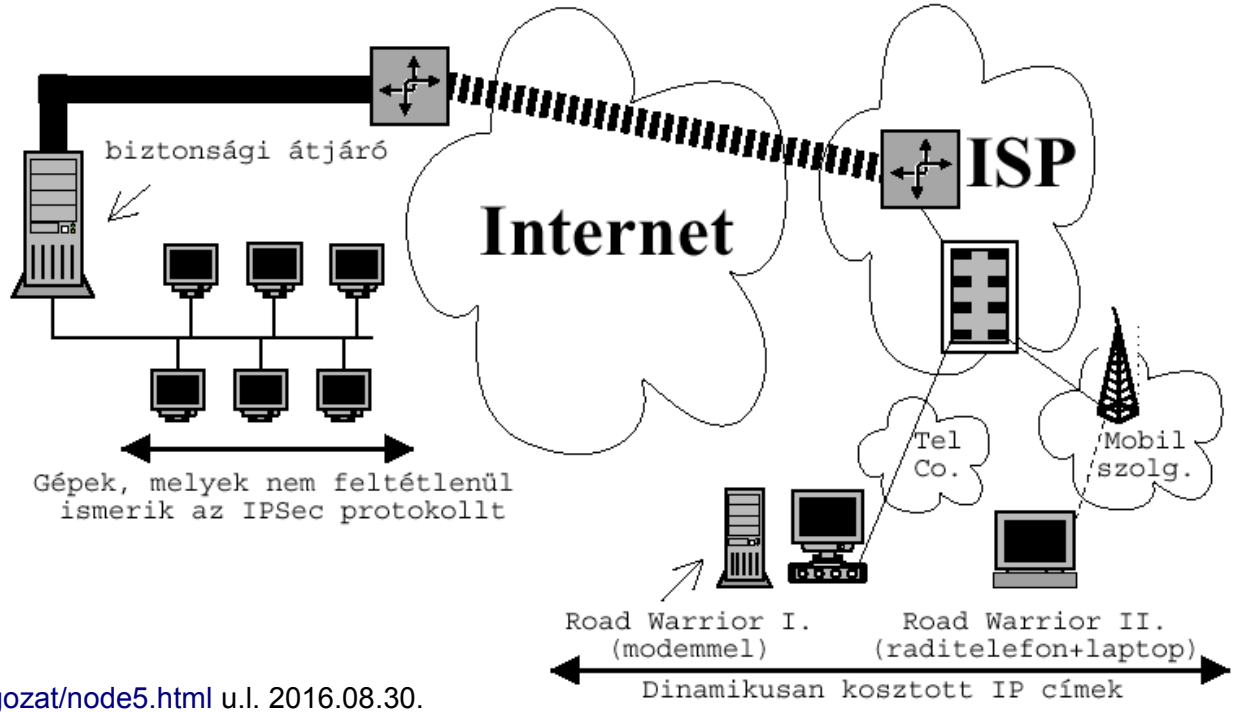
http://hup.hu/old/vpn/szakdolgozat/node4.html u.l. 2016.08.30.

VPN

Távoli elérést biztosító Remote Access VPN

Ez a kapcdsolódási mód távoli kliensek (road warrior) számára segít csatlakozni egy belső hálózathoz. Tipikus esete az otthonról dolgozó alkalmazott.

A VPN kliens a publikus weben keresztük autentikálja magát a vállalati VPN szerveren, majd ffordítva. Ezután a kialakított biztosnságos csatornán folyik tovább a kommunikáció.

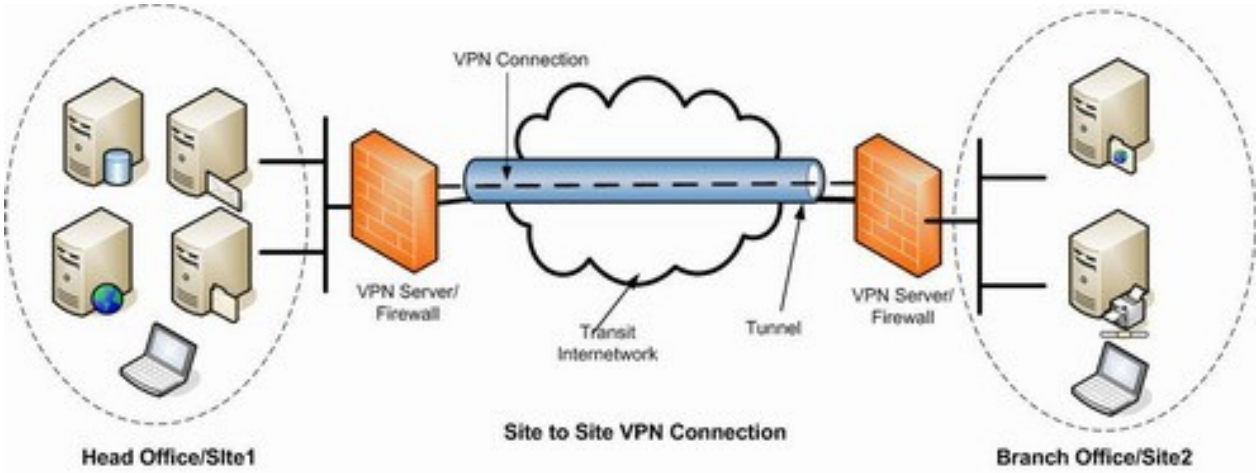


VPN

Hálózatrészek közötti Site-to-Site VPN

Ez a VPN típus jellemzően arra szolgál, hogy egy vállalat kisebb távoli telephelyeit úgy lehessen a szervezeti hálózatba kapcsolni, hogy ahhoz ne kelljen drága dedikált WAN kapcsolatot létesíteni a telephelyek között.

Felépítése után logikailag a kapcsolat ugyanúgy működik, mintha tényleges WAN kapcsolat épült volna ki.



VPN

A VPN megvalósítására négy különböző megoldás terjedt el széles körben:

- **PPTP (Point-to-Point Tunneling Protocol)**
- **L2TP (Layer 2 Tunneling Protocol)**
- **IPSec (IP Security)**
- **SSL VPN (Secure Socket Layer)**

VPN

PPTP (Point-to-Point Tunneling Protocol)

Az alapvető cél az volt, hogy nem TCP/IP-t, mint amilyen az IPX át lehessen vinni az Interneten keresztül GRE (Generic Routing Encapsulation) segítségével.

Több gyártó is készített PPTP-re terméket, de jellemzően Microsoft verziója terjedt el:

- PPTP szerver NT 4.0 vagy újabb verzió
- PPTP kliens, Win 95 vagy újabb

VPN

PPTP (Point-to-Point Tunneling Protocol)

A Windows megoldása nem ajánlott, mert:

- Az azonosítás a WIN domain biztonsági rendszerére korlátozódik
- Gyenge titkosítási módszerek a kulcsok nem véletlenszerűek a kulcsok túl rövidek, és nem is növelhetőek ezért jelszavak a hash kódból könnyen visszafejthetőek
- A jelszókezelés a vegyes környezetben nem körültekintően van megoldva a statikus jelszavak könnyen kompromittálhatóak
- A szerver is túlságosan sebezhető átejthető (például spoofing), mivel a csomag azonosítás nincs megvalósítva könnyen lebéníthatóak a szolgáltatások (DOS : Denial of Services)

VPN

L2TP (Layer 2 Tunneling Protocol) – RFC 2661

Az L2TP protokoll tulajdonképpen a PPTP továbbfejlesztése. Széles körben használatos ISP-ken (Internet Service Provider).

Maga a protokoll a PPTP (Microsoft) protokoll és az L2F (Layer 2 Forwarding - Cisco) protokoll hibridje, néhány IPSec (lásd később) megoldással kibővítve.

Jelenlegi verzió L2TPv3 – RFC 3931

Sajnos nem szolgáltat megfelelő biztosnságot, ezért jellemzően IPSec-kel együtt implementálják.

VPN

IPSec - RFC 1825, 1826, 1827

IPSec alapfogalmak:

Feladó hitelesség (Sender Authentication): Bizonyosság, hogy a feladó valóban az üzenetben jelzett személy (nem álüzenet).

Sértetlenség (Integritás, Integrity): Bizonyosság, hogy a kapott üzenet tartalma megegyezik a feladott tartalommal (nem módosult).

Hitelesség: Feladó hitelesség + Sértetlenség.

Titkosság (Confidentiality): Bizonyosság, hogy az üzenet külső személyek számára nem hozzáférhető.

Titkosítás (Encryption): Titkosságot biztosító mechanizmus.

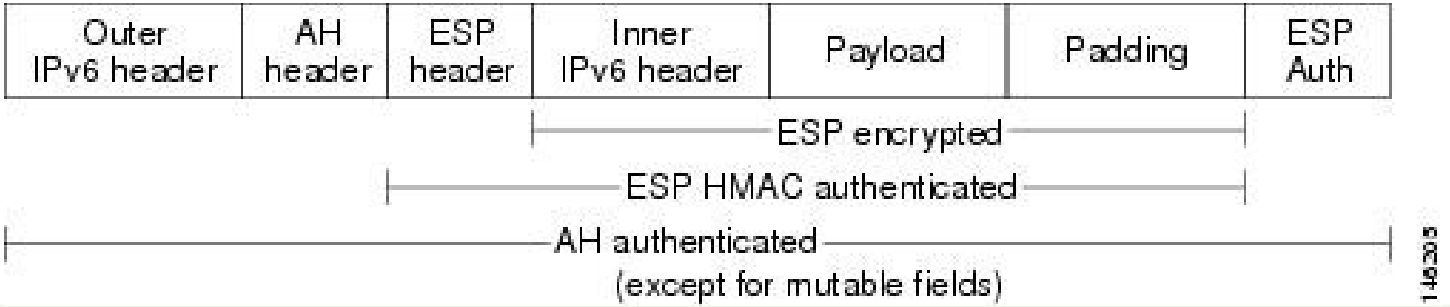
Letagadhatatlanság (Non repudiation): A küldő személyének bizonyíthatósága.

VPN

IPSec - RFC 1825, 1826, 1827

IP Authentication Header (AH)

- Authentikáció
- Letagadhatatlanság (opcionális)
- Egy „pecsét” (a teljes IP datagram alapján készült kód) segítségével látja el feladatát.
- Egyszerűen implementálható, hagyományos rendszerekkel együttműködhet.
- Többféle authentikációs algoritmus használható (MD5)
  - Aszimmetrikus kulcsú algoritmussal a letagadhatatlanság biztosítható.

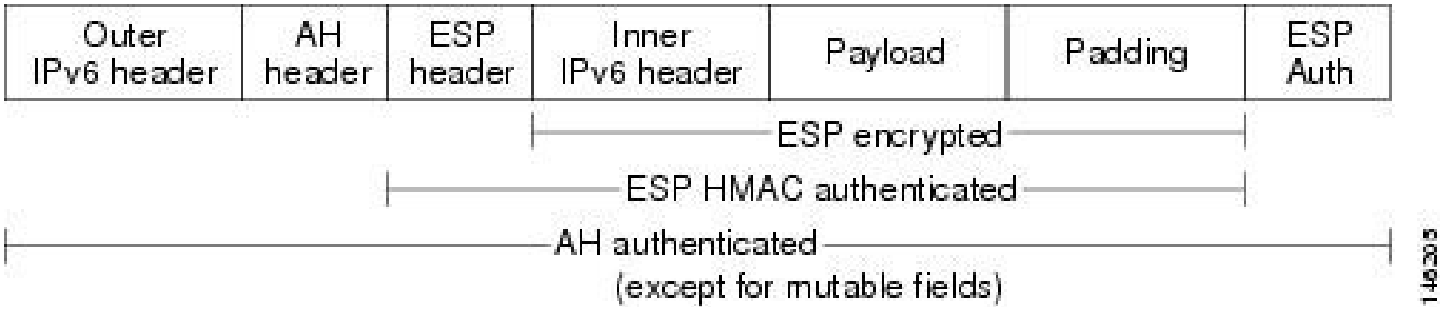


VPN

IPSec - RFC 1825, 1826, 1827

IP Encapsulation Security Payload (ESP)

- Sértetlenség.
- Titkosság.
- Transzport rétegbeli implementáció.
  - Az IP fejléc adataira nem vonatkozik a szolgáltatás.
- Hálózati rétegbeli implementációk.
  - A teljes IP datagramra érvényes a szolgáltatás.
- Titkosítással új PDU-t származtat.
- IP AH-val együtt alkalmazható.



http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book/ip6-ipsec.html u.l. 2016.08.30.

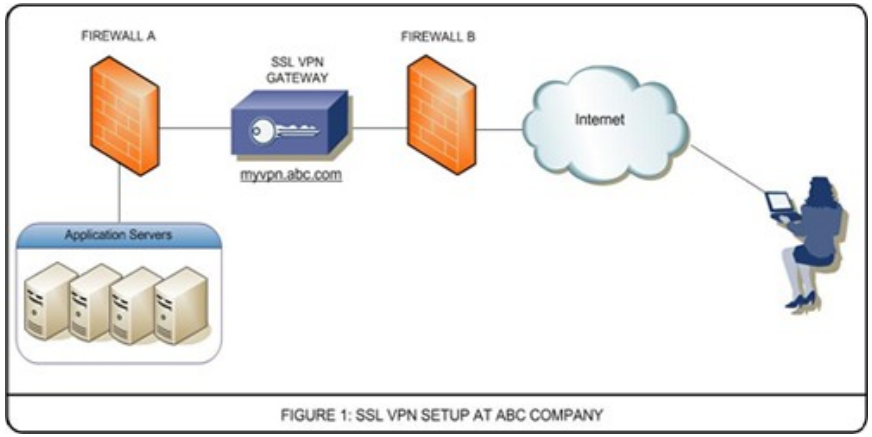
VPN

SSL VPN (Secure Socket Layer)

A korábbiakkal szemben ez nem követi szigorúan a VPN korábbi definícóját. Nem szükséges kliens program telepítése. Tulajdonképpen például a böngésző a kliens.

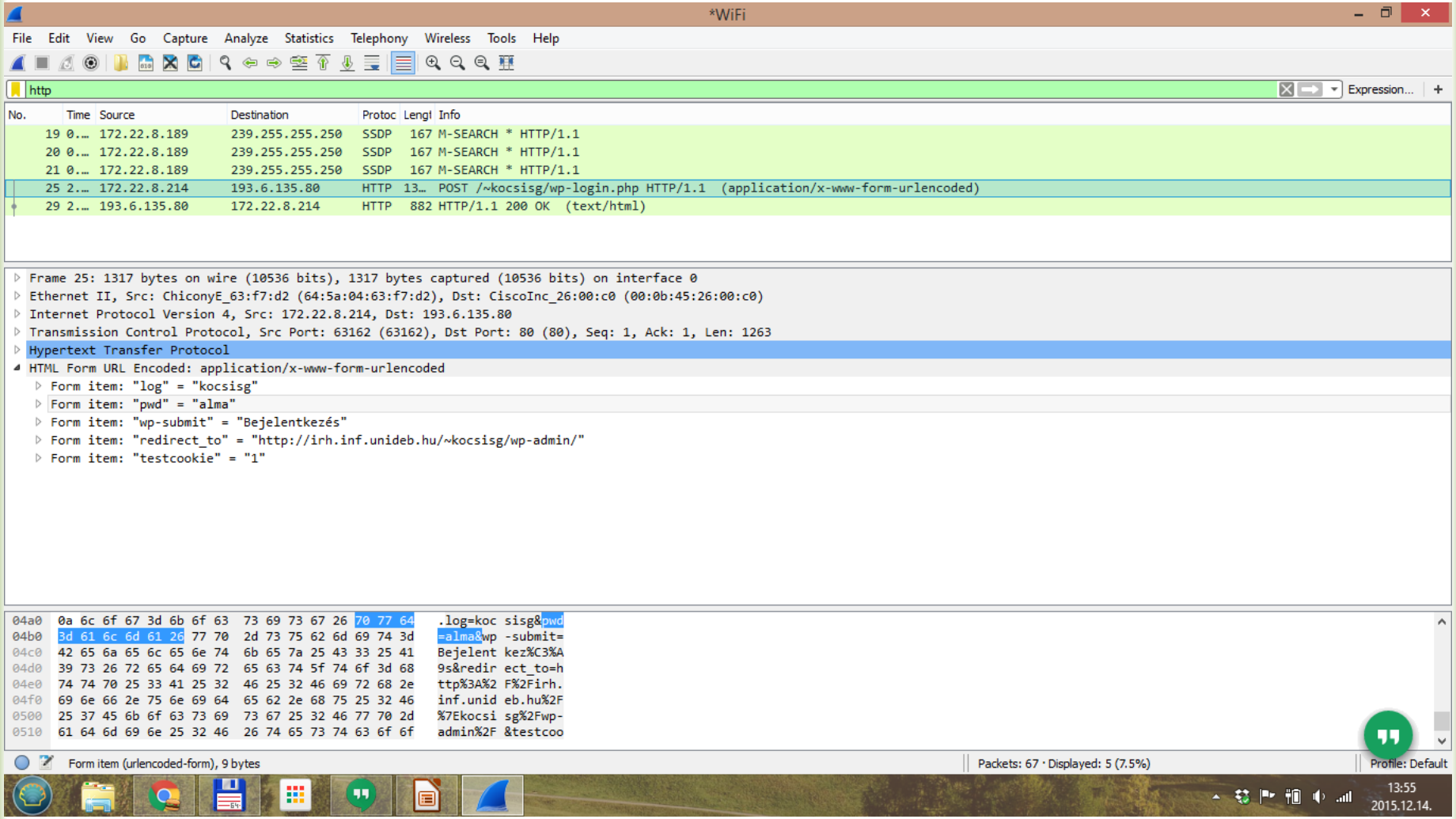
Egyesíti az IPSec biztonságosságát a PPTP és L2TP egyszerű kezelhetőségével.

Nagyon széles körben használatos. Minden olyan alkalommal, amikor a böngészőben. *https* kezdet látszik , a háttérben egy ilyen kapcsolat kiépítése történik.

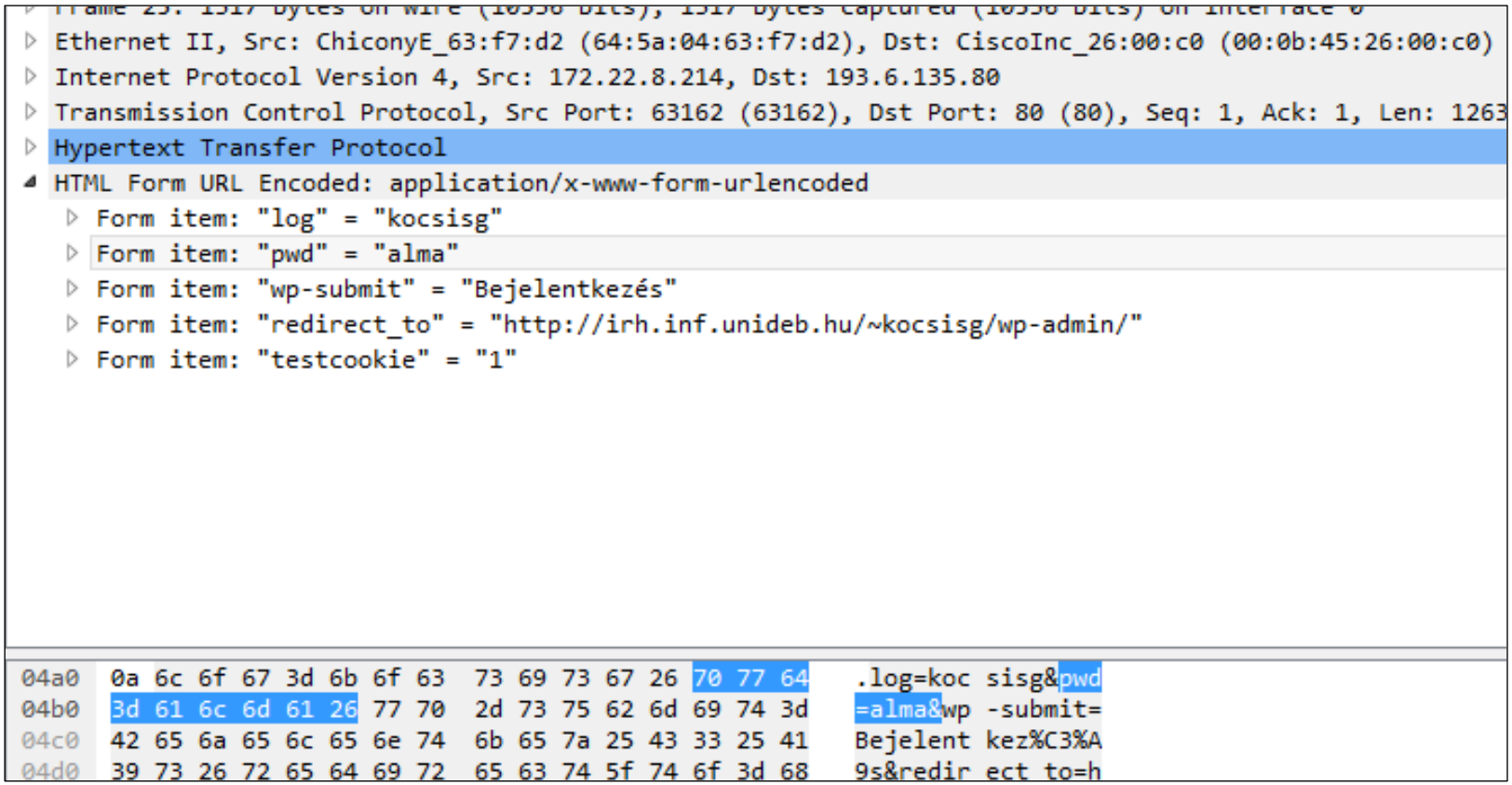


http://www.lumleymedia.co.uk/?p=613 u.l. 2016.08.30.

Wireshark


*WiFi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Source Destination Protoc Lengl Info
19 0.… 172.22.8.189 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
20 0.… 172.22.8.189 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
21 0.… 172.22.8.189 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
25 2.… 172.22.8.214 193.6.135.80 HTTP 13… POST /~kocsisg/wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
29 2.… 193.6.135.80 172.22.8.214 HTTP 882 HTTP/1.1 200 OK (text/html)
Frame 25: 1317 bytes on wire (10536 bits), 1317 bytes captured (10536 bits) on interface 0
Ethernet II, Src: ChiconyE_63:f7:d2 (64:5a:04:63:f7:d2), Dst: CiscoInc_26:00:c0 (00:0b:45:26:00:c0)
Internet Protocol Version 4, Src: 172.22.8.214, Dst: 193.6.135.80
Transmission Control Protocol, Src Port: 63162 (63162), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1263
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "log" = "kocsisg"
Form item: "pwd" = "alma"
Form item: "wp-submit" = "Bejelentkezés"
Form item: "redirect_to" = "http://irh.inf.unideb.hu/~kocsisg/wp-admin/"
Form item: "testcookie" = "1"
04a0 0a 6c 6f 67 3d 6b 6f 63 73 69 73 67 26 70 77 64 .log=koc sisg&pwd
04b0 3d 61 6c 6d 61 26 77 70 2d 73 75 62 6d 69 74 3d =alma&wp -submit=
04c0 42 65 6a 65 6c 65 6e 74 6b 65 7a 25 43 33 25 41 Bejelent kez%C3%A
04d0 39 73 26 72 65 64 69 72 65 63 74 5f 74 6f 3d 68 9s&redir ect_to=h
04e0 74 74 70 25 33 41 25 32 46 25 32 46 69 72 68 2e ttp%3A%2 F%2Firh.
04f0 69 6e 66 2e 75 6e 69 64 65 62 2e 68 75 25 32 46 inf.unid eb.hu%2F
0500 25 37 45 6b 6f 63 73 69 73 67 25 32 46 77 70 2d %7Ekocsi sg%2Fwp-
0510 61 64 6d 69 6e 25 32 46 26 74 65 73 74 63 6f 6f admin%2F &testcoo
Form item (urlencoded-form), 9 bytes
Packets: 67 · Displayed: 5 (7.5%)
Profile: Default
13:55
2015.12.14.

Wireshark


Frame 29: 1517 bytes on wire (10536 bits), 1517 bytes captured (10536 bits) on interface 0
Ethernet II, Src: ChiconyE_63:f7:d2 (64:5a:04:63:f7:d2), Dst: CiscoInc_26:00:c0 (00:0b:45:26:00:c0)
Internet Protocol Version 4, Src: 172.22.8.214, Dst: 193.6.135.80
Transmission Control Protocol, Src Port: 63162 (63162), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1263
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "log" = "kocsisg"
Form item: "pwd" = "alma"
Form item: "wp-submit" = "Bejelentkezés"
Form item: "redirect_to" = "http://irh.inf.unideb.hu/~kocsisg/wp-admin/"
Form item: "testcookie" = "1"
04a0 0a 6c 6f 67 3d 6b 6f 63 73 69 73 67 26 70 77 64 .log=koc sisg&pwd
04b0 3d 61 6c 6d 61 26 77 70 2d 73 75 62 6d 69 74 3d =alma&wp -submit=
04c0 42 65 6a 65 6c 65 6e 74 6b 65 7a 25 43 33 25 41 Bejelent kez%C3%A
04d0 39 73 26 72 65 64 69 72 65 63 74 5f 74 6f 3d 68 9s&redir ect_to=h

BitTorrent

BitTorrent

A BitTorrent, egy p2p (peer-to-peer) alapú fájlcserélő protokoll, amely alkalmas a mások által megosztott adat, adtok le- és feltöltésére.

torrent: (magyarul áradat, özön) A fájlcserélésben résztvevő társak összessége.

A társak a fájl egyenlő méretű **töredékekre** osztják. A letöltés tulajdonképpen ezeknek a töredékeknek az összegyűjtése.

A gyűjtés tetszőleges időpontban félbehagyható, vagy újrakezdhető.

BitTorrent

Peer: Két jelentéssel is bírhat. Elsõként egy összefoglaló szó a seederekre és leecherekre, azaz a le és feltöltõkre. Másodsorban a peer jelentheti ugyanazt, mint a leecher, azaz letöltõt.

Tracker: egy központi szerver program. Tárolja, hogy melyik torrentet melyik peer tölti és statisztikát gyûjt.

.torrent metafájl: ez egy fájl, ami tartalmazza a tracker címét, a megosztott fájlok nevét, a pieces (darabok) számát, méretét és a hash-t.

Seeder: Az a felhasználó, aki rendelkezik az adott torrent-hez tartozó adatok 100%-val. Õ csak feltölt, azaz tõle töltenek a leecherek.

Leecher: Az a felhasználó, aki nem rendelkezik az adott torrent-hez tartozó adatok 100%-val. Õ le és fel is tölt egy idõben. Ha megszerzi az adatok 100%-át, akkor belõle is seeder lesz.

Feltöltõ: az a felhasználó, aki az új dolgokat felteszi az oldalra.

http://torrent-new.atw.hu/fogalmak.html u.l. 2016.08.30.

BitTorrent

A tracker kezeli és osztja szét a kapcsolatokat a felhasználók között. Minél gyorsabban tölt fel a letöltõ, annál gyorsabb felhasználókat oszt ki a tracker a letöltõnek.

A letöltés során a letöltőnek két fontos kérdést kell tisztáznia:

- Melyik töredéket töltse le először?
- Melyik társától töltse le?

Az első kérdésre a válasz: A legritkábbat először.

A második kérdésre egy kereskedő algoritmust használ.

BitTorrent

A BitTorrent kereskedő algoritmusa:

- A letöltő folyamatosan figyeli, hogy kitől milyen gyorsan tölt le.
- A négy leggyorsabb társnak a szolgáltatását viszonozza, és ő is tölt nekik.
- A négy leggyorsabb társ kiválasztása 10 másodpercenként újra megtörténik.
- 30 másodpercenként véletlenszerűen is hozzáad egy társat, akinek szintén küld. (Ha elég gyorsan küld, akkor bekerül az ottani legjobb négybe és új kereskedő kapcsolat épül ki)

Az algoritmus eredményeként a nagyjából azonos sebességgel töltő társak egymásra találnak.

BitTorrent

A BitTorrent használata:

- A megosztani kívánt tartalomról egy leíró .torrent metafájlt kell készíteni.
- Ezt a fájlt kell elhelyezni egy (nyilvános, vagy privát) tracker szerveren
- A fájl létezéséről értesíteni kell a potenciális letöltőket (pl link megadása egy oldalon)
- Az eredeti feltöltőnek elérhetőnek kel lennie legalább amg egyszer minden adatot le nem töltenek tőle (nem feltétlenül egy peer).

http://www.bittorrent.org/beps/bep_0003.html u.l. 2016.08.30