SZÁMÍTÓGÉP-HÁLÓZATOK BEVEZETŐ ELŐADÁS 1.

Mérnök-informatikus szak, BSc, 4. félév
2012/13 2.félév

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2012.február 12.
Budapest

A tárgy mottója

„Mondd el és elfelejtem. Mutasd meg és megjegyzem. Vonj be és megértem.”

Konfuciusz

SZÁMÍTÓGÉP-HÁLÓZATOK?

Új tudomány/technika... egy régi egyetemen...

Milyen régi a Műegyetem?

- 1777: Mária Terézia „Ratio Educationis”–a a mérnökképzés fontosságáról
- *1782: II. József megalapítja a BME-t : „Institutum Geometricum Hydrotechnicum”*
- 1871: „Királyi József Nádor Műegyetem” – a világ első műszaki oktatási intézménye „egyetemi” rangban

És a Villamoskar?

- Csak 64!

Milyen régi a számítógép-hálózat?

44 éves!

1969 – 2013

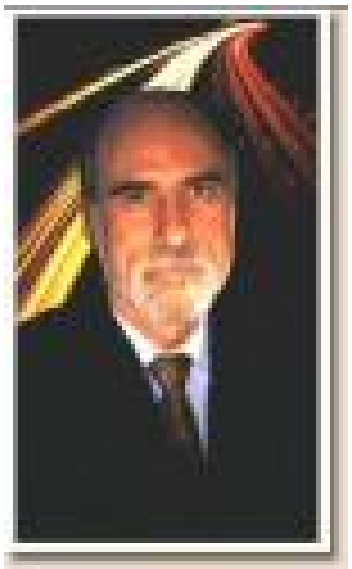
1969: az ARPANET, az első számítógép-hálózat születése

Milyen régi az Internet?

Attól függ, mit értünk „Internet”-en!

Mi az Internet?

Vinton Cerf, one of the „Fathers of Internet”:



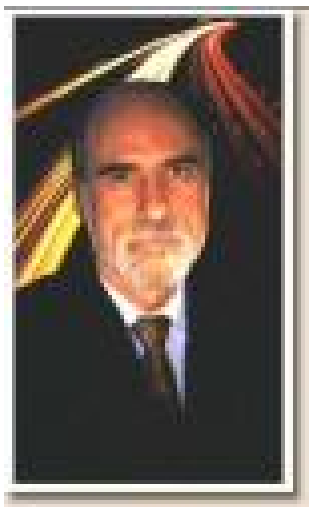
- **The largest network of networks in the world.**
- **Uses TCP/IP protocols and packet switching .**
- **Runs on any communications substrate.**

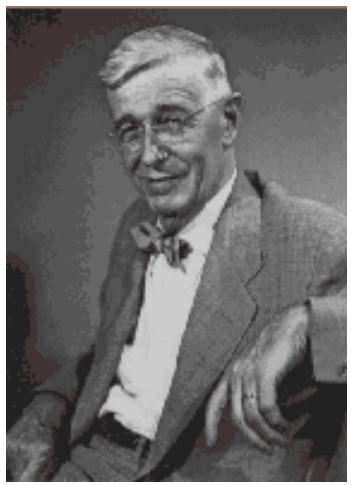
Mi az Internet?

- Számítógép-hálózat
  - 44 éves: az ARPANET-től számítva
  - 30 éves: 1983-ben lett a TCP/IP protokoll a működésének alapja, ekkor nevezték el Internet-nek

- WWW (World Wide Web), világháló
  - 24 éves: 1989-ben találta fel *Tim Berners-Lee* a WWW-t

Nagy emberek, akiknek a számítógéphálózat és az Internet köszönhető





J. C. R. Licklider

ARPA (DARPA) – (Defense) Advanced Research Projects Agency
(of the Department of Defense, USA)

„Man-Computer Symbiosis”, 1960
„The Computer as a Communication Device”, 1968

- Az összekapcsolt számítógépek elve
- A szerves ember-gép kapcsolat víziója

Paul Baran (ARPA) és a decentralizált hálózat alapelve

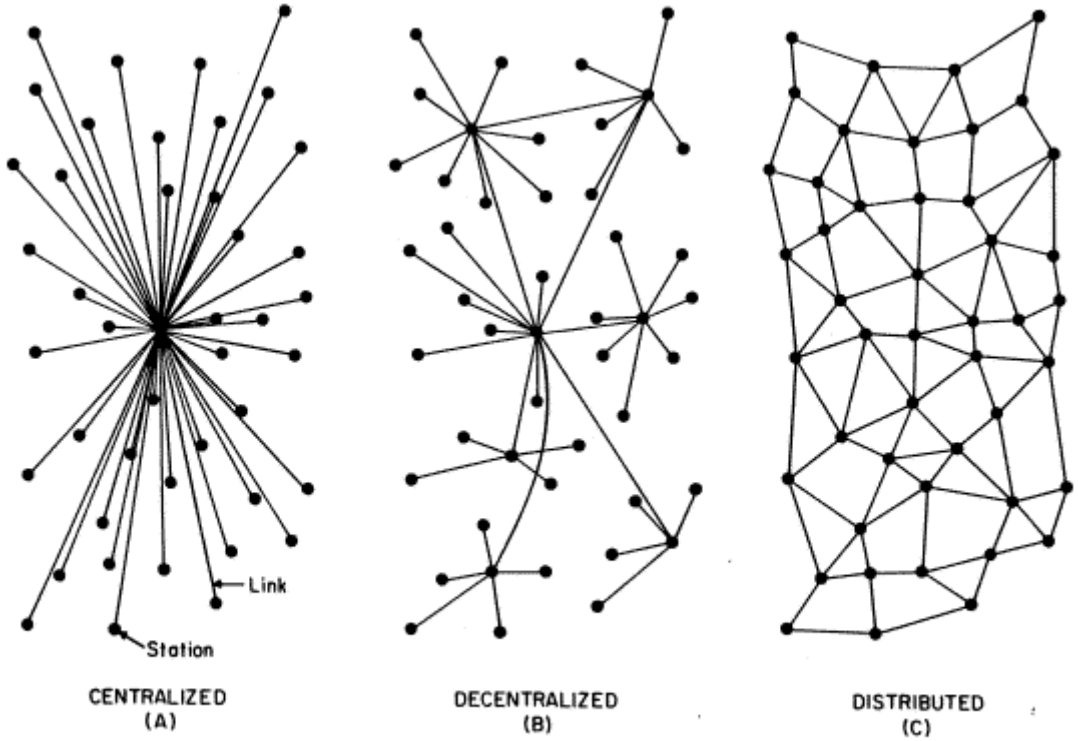
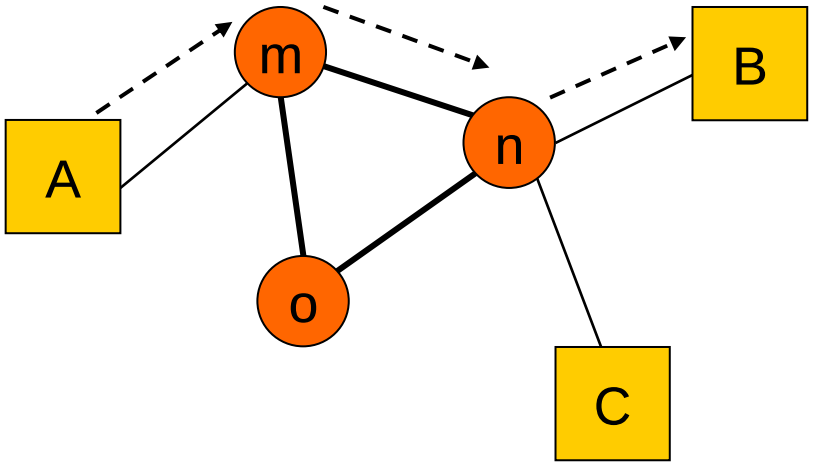


FIG. 1 — Centralized, Decentralized and Distributed Networks

Leonard Kleinrock

- A csomagkapcsolás elvét ő fogalmazta meg először (1961): MIT doktori
- A 60-as évek elején három kutatói csoport egyidejűleg és egymástól függetlenül vetette fel a csomagkapcsolás elvét
  - Kleinrock, Baran, Donald Davies
- Kleinrock meggyőzte az ARPA-t: a létrehozandó ARPANET hálózat csomagkapcsolt elven alapuljon
- Hierarchikus routing kidolgozója

Csomagkapcsolás???



- Az addig természetes **vonalkapcsolás** helyett
  = összeköttetés kiépítése és fenntartása A és B között, az adatkommunikáció idejére

A telefonhálózat alapelve!

- **Csomagkapcsolás:**
  - adatok továbbítása kis „adagokban”
  - egymástól függetlenül
  - csomópontból csomópontba („store-and-forward” elv)

Analógia: posta

Számítógépek közötti kommunikáció burst-ös jellegű!

Az ARPANET

ARPANET csomópont, eredeti rajz

THE ARPA NE[illegible]

SEPT. 1969

I NODE

FIGURE 6.1 Drawing of September 1969
(Courtesy of Alex McKenzie)

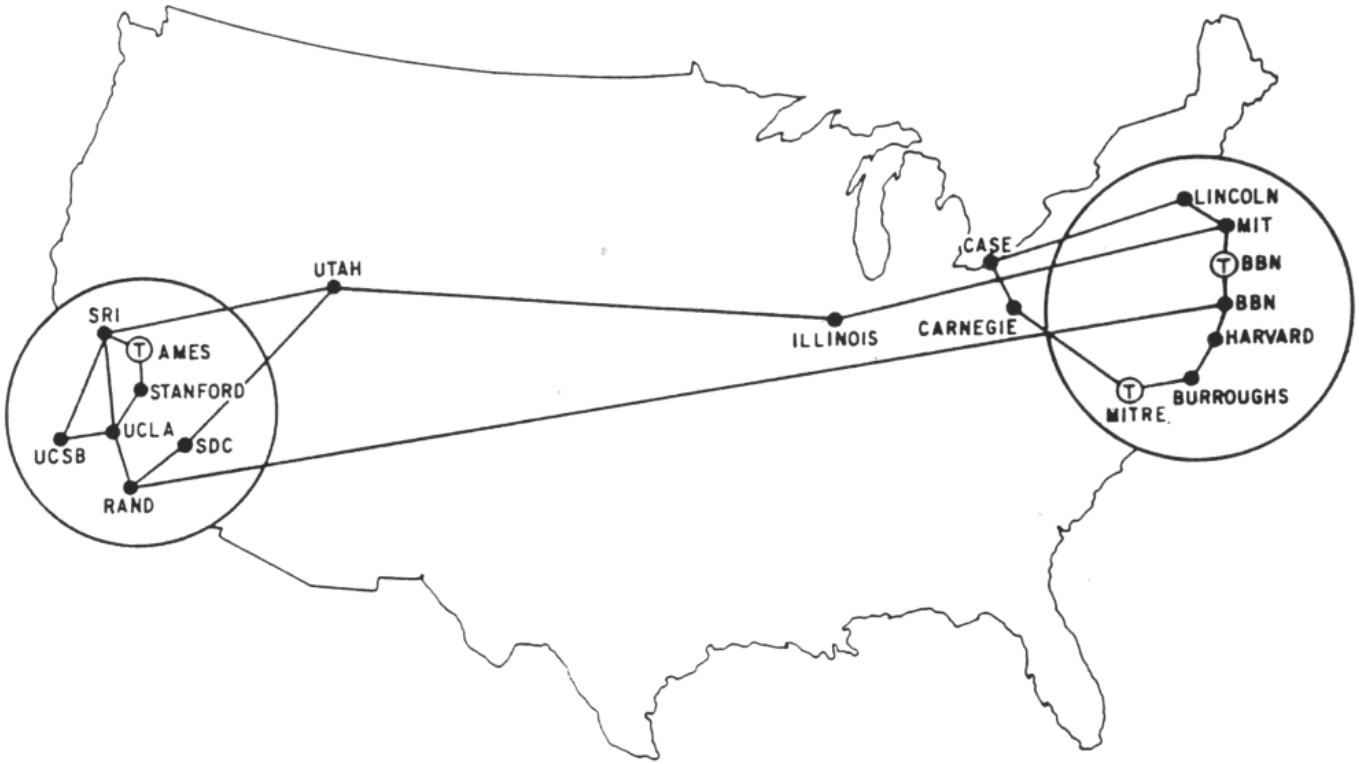
Az első ARPANET csomópont tesztelése 1969-ben (Leonard Kleinrock)

1969-70-ben az első négy végpont összekapcsolása:
UCLA, Stanford, UC Santa Barbara, Univ. of Utah

Az első távoli számítógép-kapcsolat...
(Részlet egy Leonard Kleinrock-kal készített interjúból.)

- "We set up a telephone connection between us and the guys at **SRI**...„
  (UCLA – Stanford Research Institute, mindkettő Kaliforniában)
- "We typed the **L** and we asked on the phone, "Do you see the **L**?„
- "Yes, we see the **L**," came the response.
- "We typed the **O**, and we asked, "Do you see the **O**.„
- "Yes, we see the **O**.„
- "Then we typed the **G**, and the **system crashed**"...
- Yet a **revolution had begun**"...

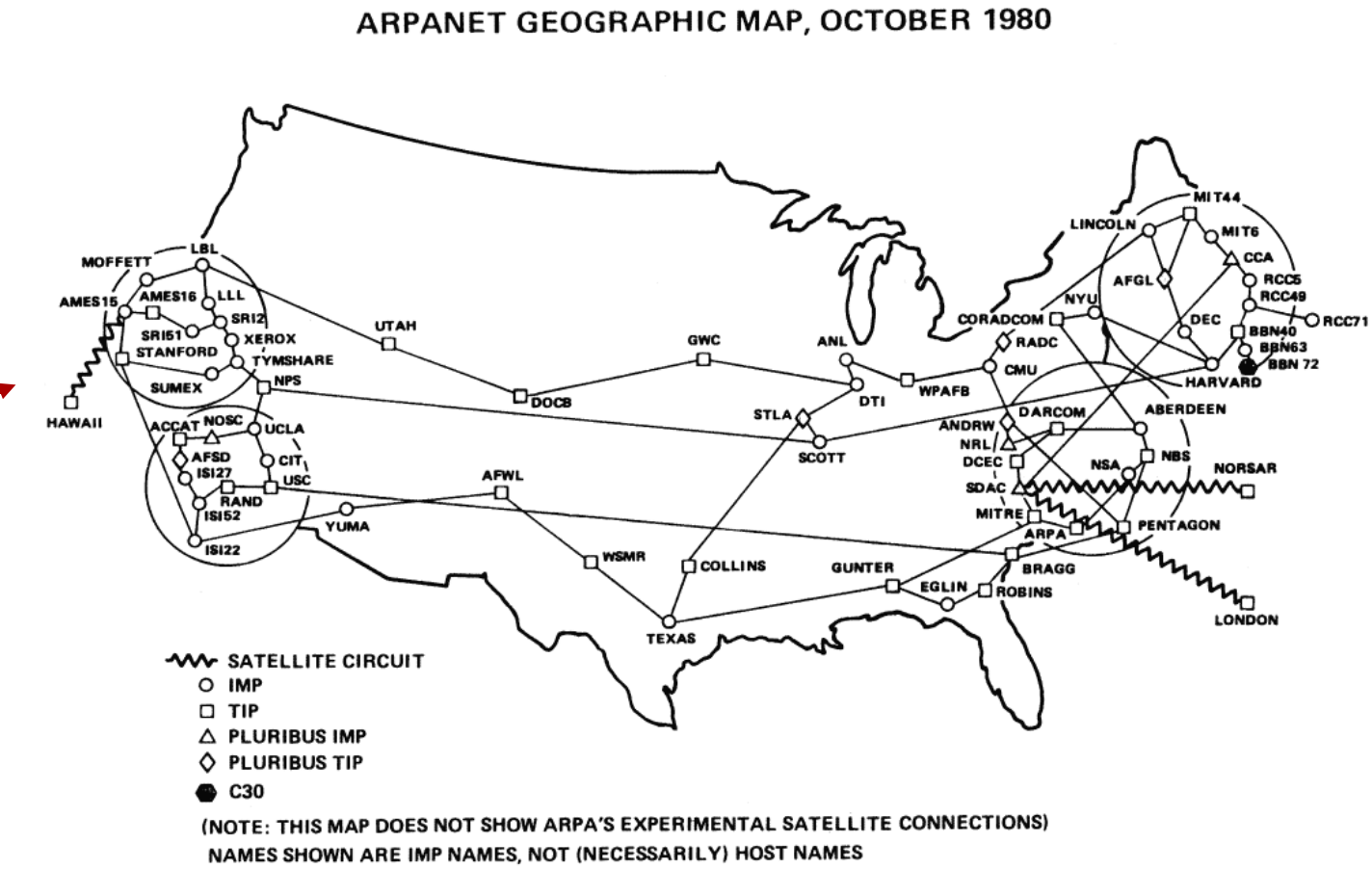
ARPANET, 1971 szeptember



MAP 4 September 1971

ARPANET, 1980 október

erről még lesz szó később

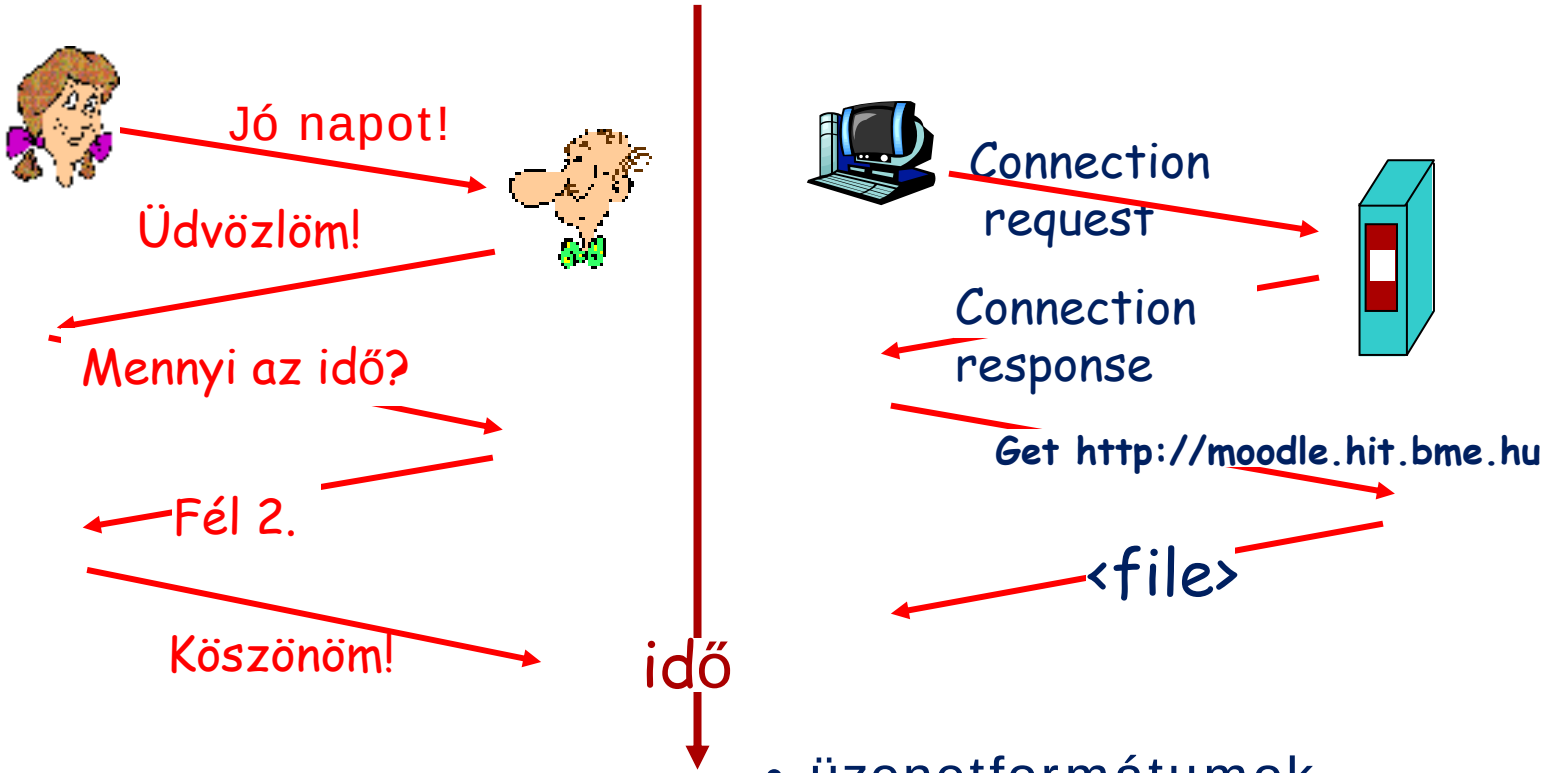


A működésről

- Hogyan végezzék a hálózati csomópontok (az IMP-ek) a csomagok továbbítását?
- Hogyan hozzunk létre kapcsolatokat a végpontok (a számítógépek) között?
- Ehhez megfelelő protokollok kellettek

- Eredetileg: NCP (Network Control Program)
  - Kétirányú, megbizható kommunikáció alkalmazások között
- Később lecserélve (1983, **flag day**):
  - az Interneten ma is használt IP (Internet Protocol) és TCP (Transmission Control Protocol)
  - Együttesen: **TCP/IP**

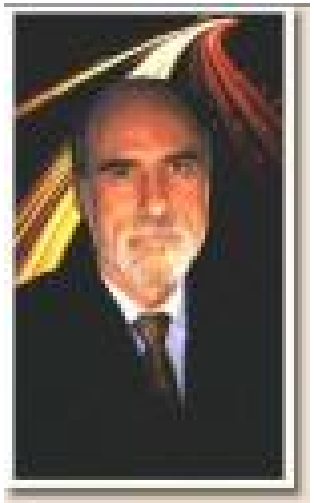
Protokollok az emberi és a gépek közötti kommunikációban



Viselkedési szabályok, előírt viselkedési minták

- üzenetformátumok
- azok cseréjének módja
- az egyes üzenetekre adott válaszok

Robert Kahn és Vinton Cerf, a TCP/IP protokoll kitalálói (1974)



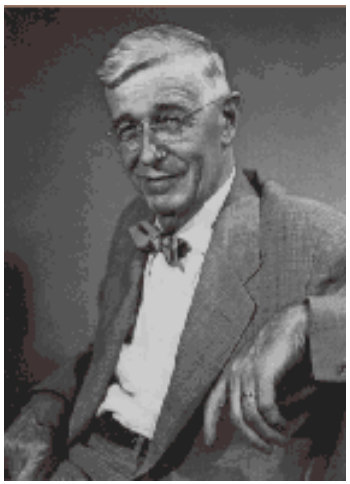
- Több független csomagkapcsolt hálózat jött létre
  - ARPANET
  - ALOHANET (Hawai-i egyetemek, mikrohullámú kapcsolat)
  - IBM
- **Internetting!**

- IP – Internet Protocol
  - a hálózat csomópontjainak viselkedését szabályozza
  - Ún. **best effort** szolgáltatást nyújt a csomagok továbbítását illetően
- TCP – Transmission Control Protocol
  - a hálózat végpontjai közötti kommunikáció
  - **megbízható** adatátvitelt nyújt
  - később UDP
- Alapelv: **intelligencia a hálózat szélére, a végpontokba**
- **Router** koncepciója

Internet: a hálózati kommunikáción túl...

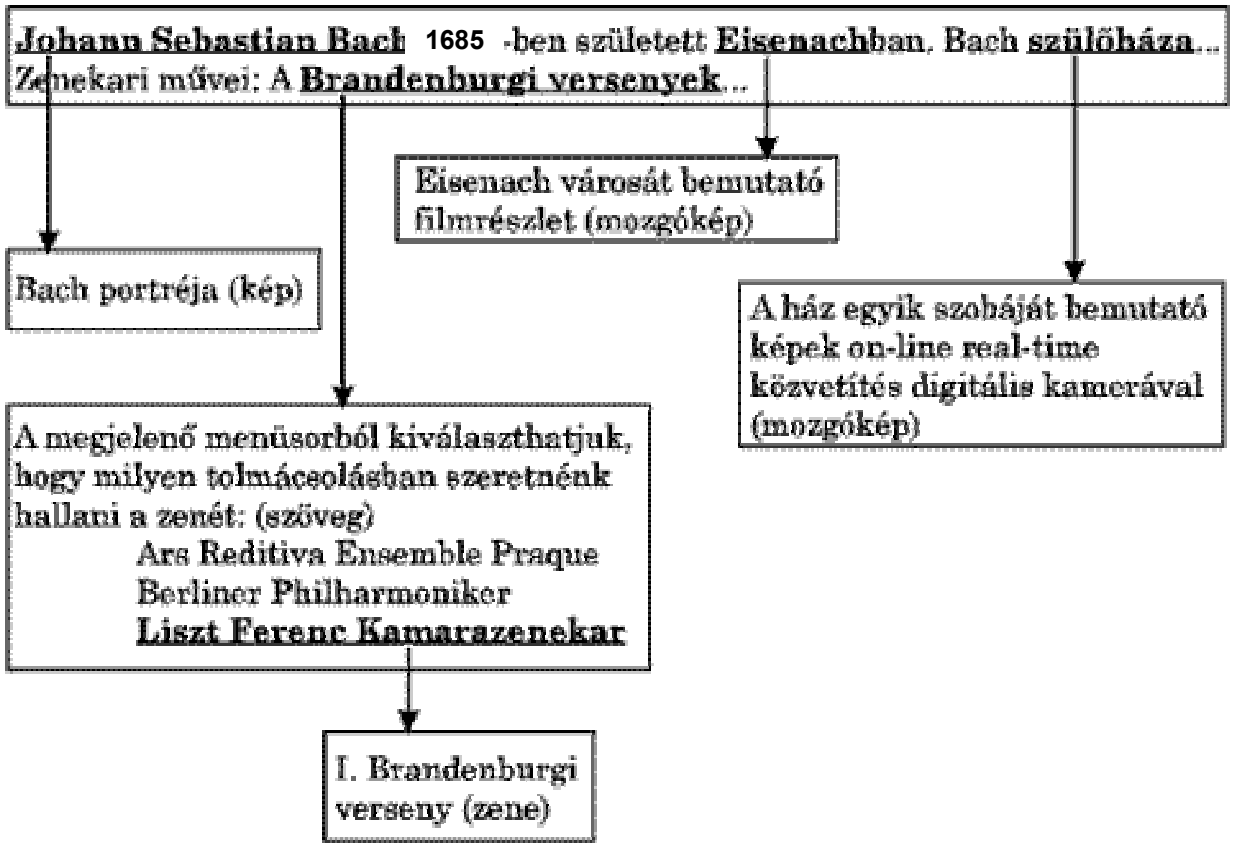
Hipertext, hipermédia, web-szerver, WWW, a WWW újabb generációi (Web2.0, Web3.0)

Vannevar Bush



- A II. világháború alatt és után: National Defense Research Committee
- *As We May Think*; Atlantic Monthly; July 1945
  - Első elképzelések az asszociatív keresésről.
  - Memex jövőbeli gép:
    - képes megjeleníteni bármit egy könyvtári archívumból
    - képes bennük szavakra keresni, mint hiperhivatkozás
- Nem a hagyományos könyvtári keresőrendszer szerint: az emberi agyhoz hasonlóan
  - asszociációk létesítése alapján

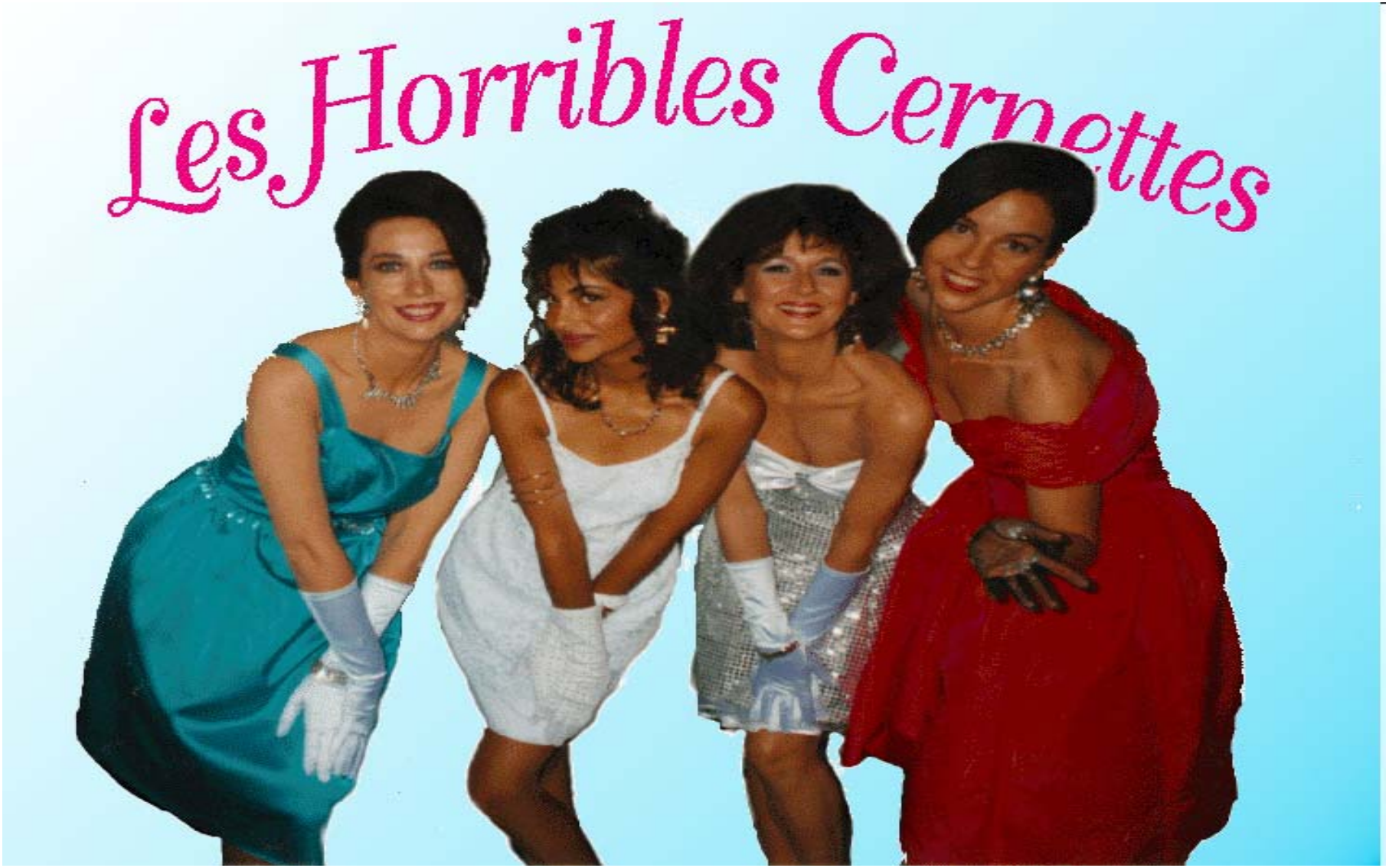
Hipertext, hipermédia: példa



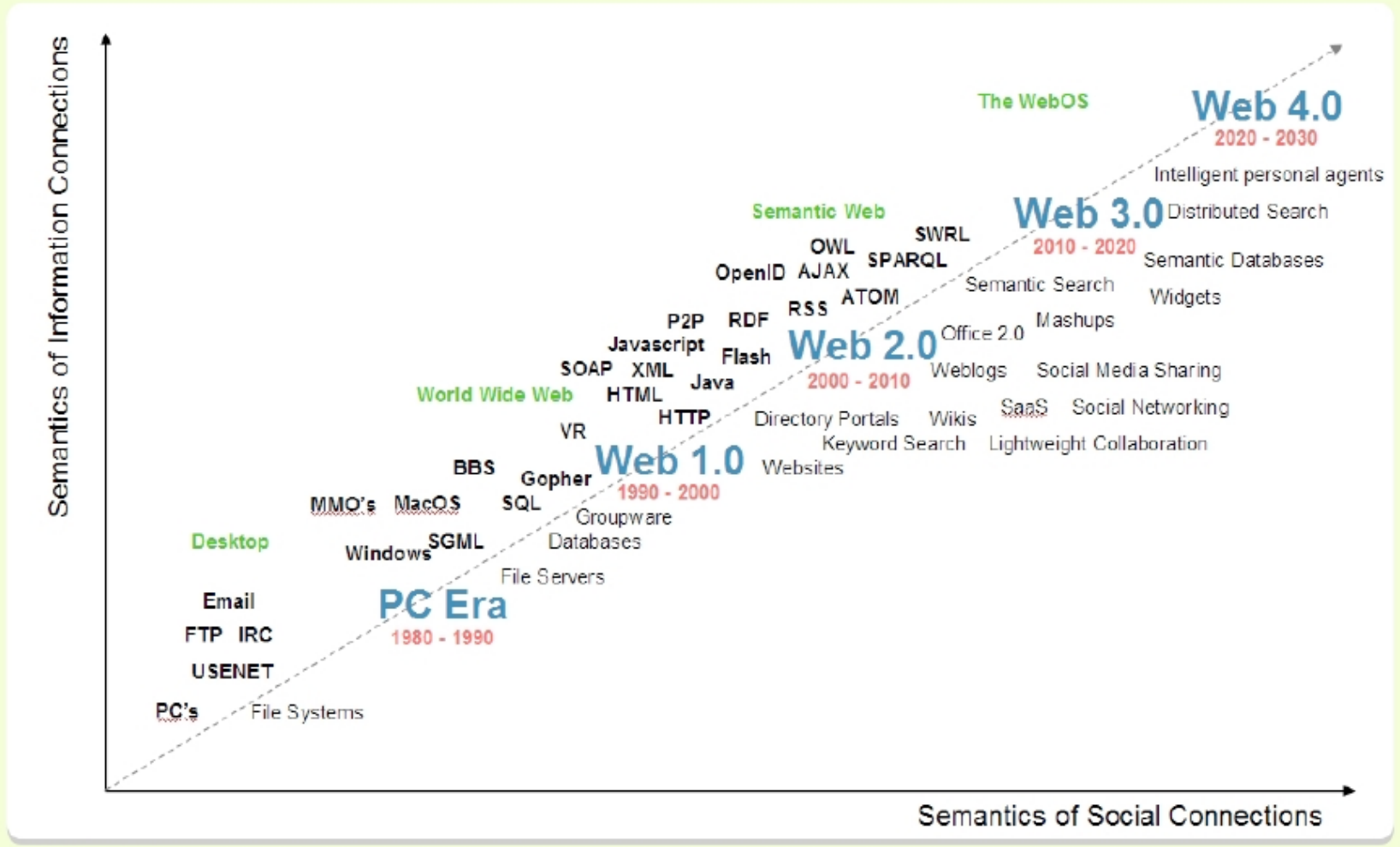
(Sir) Tim Berners-Lee, a WWW feltalálója

- Először a CERN belső hálózatán valósult meg (1990):
  - Böngésző (WWW néven)
  - Webszerver
    - Könyvtárszerkezet az Interneten
      - HTML oldalak
      - közöttük linkekkel lehetett navigálni.
  - HTML (HyperText Markup Language)
  - HTTP (HyperText Transfer Protocol)
- Kiterjesztése az Internetre: WWW
- Új projektje: Semantic Web

Első kép a WWW-n



Web-”generációk”



SOME RIGHTS RESERVED

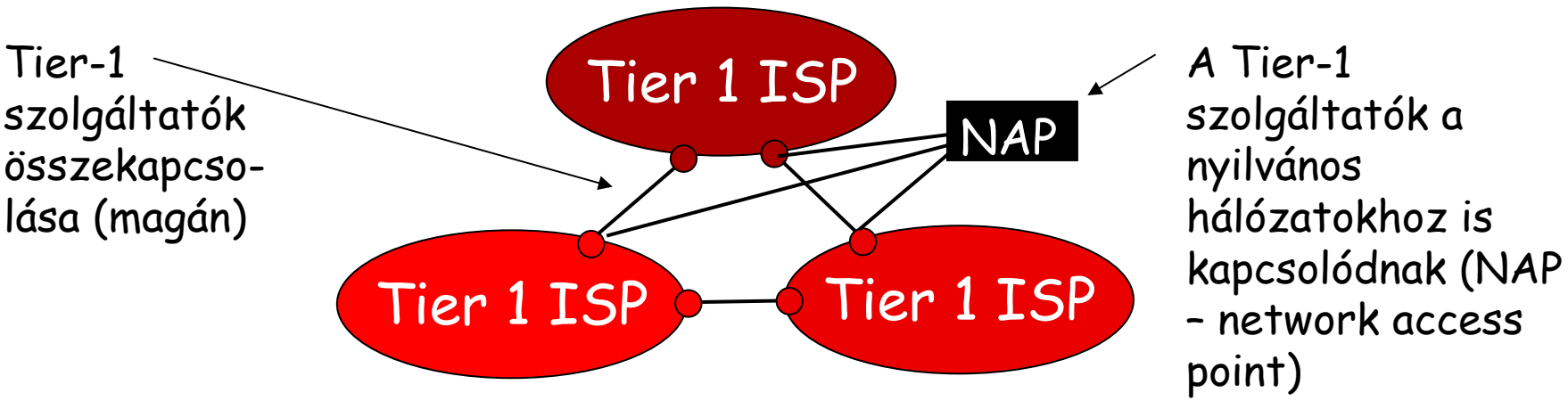
Source: Radar Networks & Nova Spivack, 2007 – www.radarnetworks.com

Példák számítógép-hálózatokra

- A mai Internet
- Az európai kutatói gerinchálózat (GEANT)
- Magyarországi kutatói gerinchálózat, H-Bone
- A PlanetLab
- Helyi hálózat
- Vezetéknélküli hot-spot

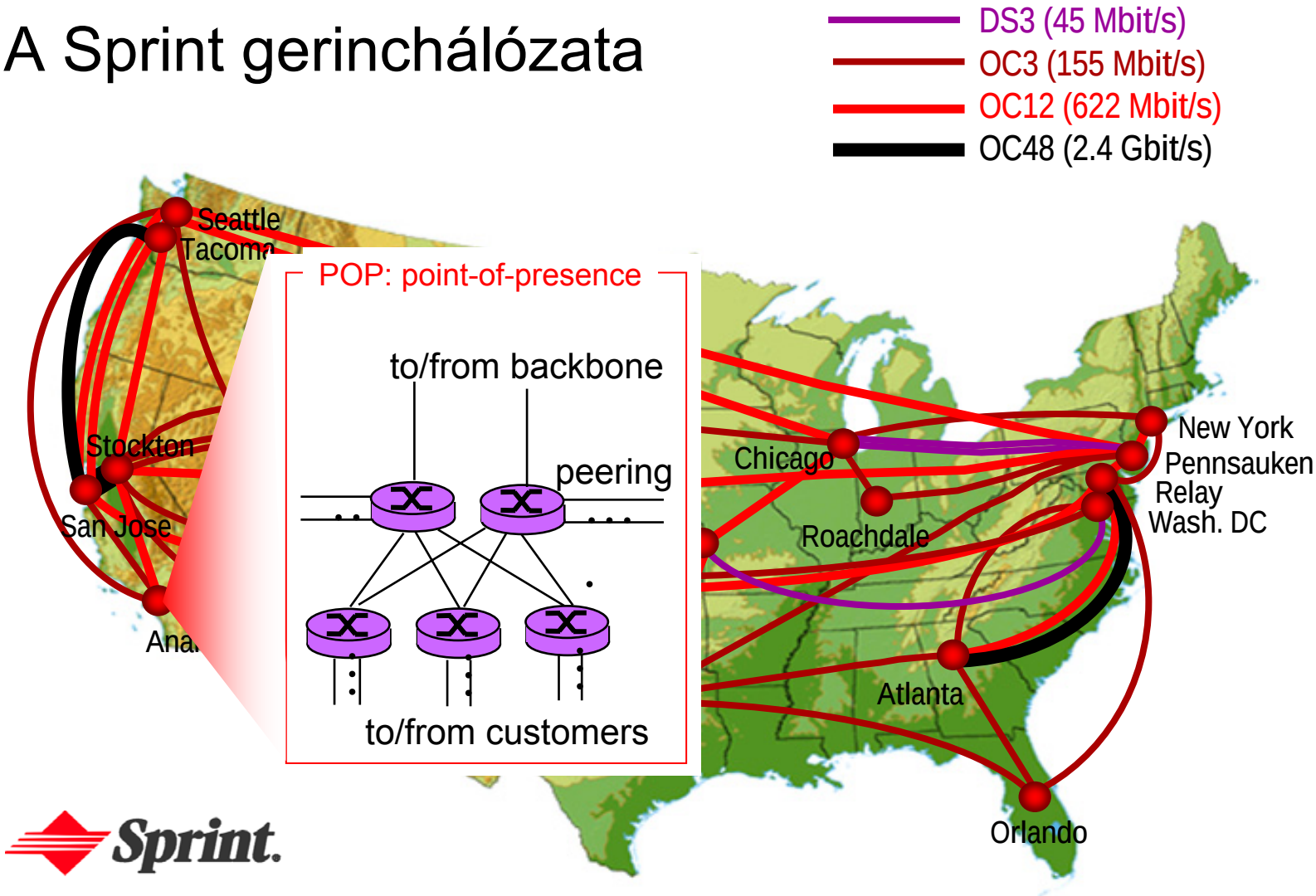
Az Internet: hálózatok hálózata

- Kezdetben egyszintű, elosztott, ma alapvetően hierarchikus
- A középpontban: “tier-1” ISP-k (pl. Sprint, AT&T, Tata Communications, NTT), nemzeti/nemzetközi lefedés, egyenrangúak



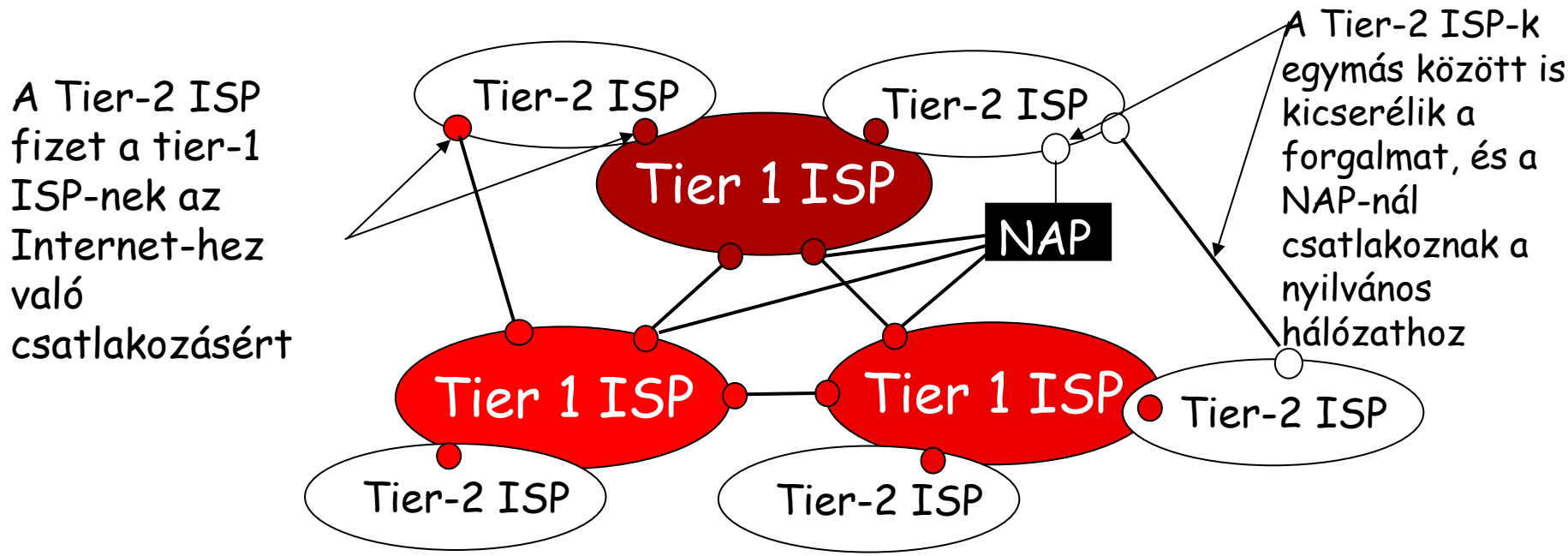
USA példa Tier-1 ISP-re: Sprint

A Sprint gerinchálózata



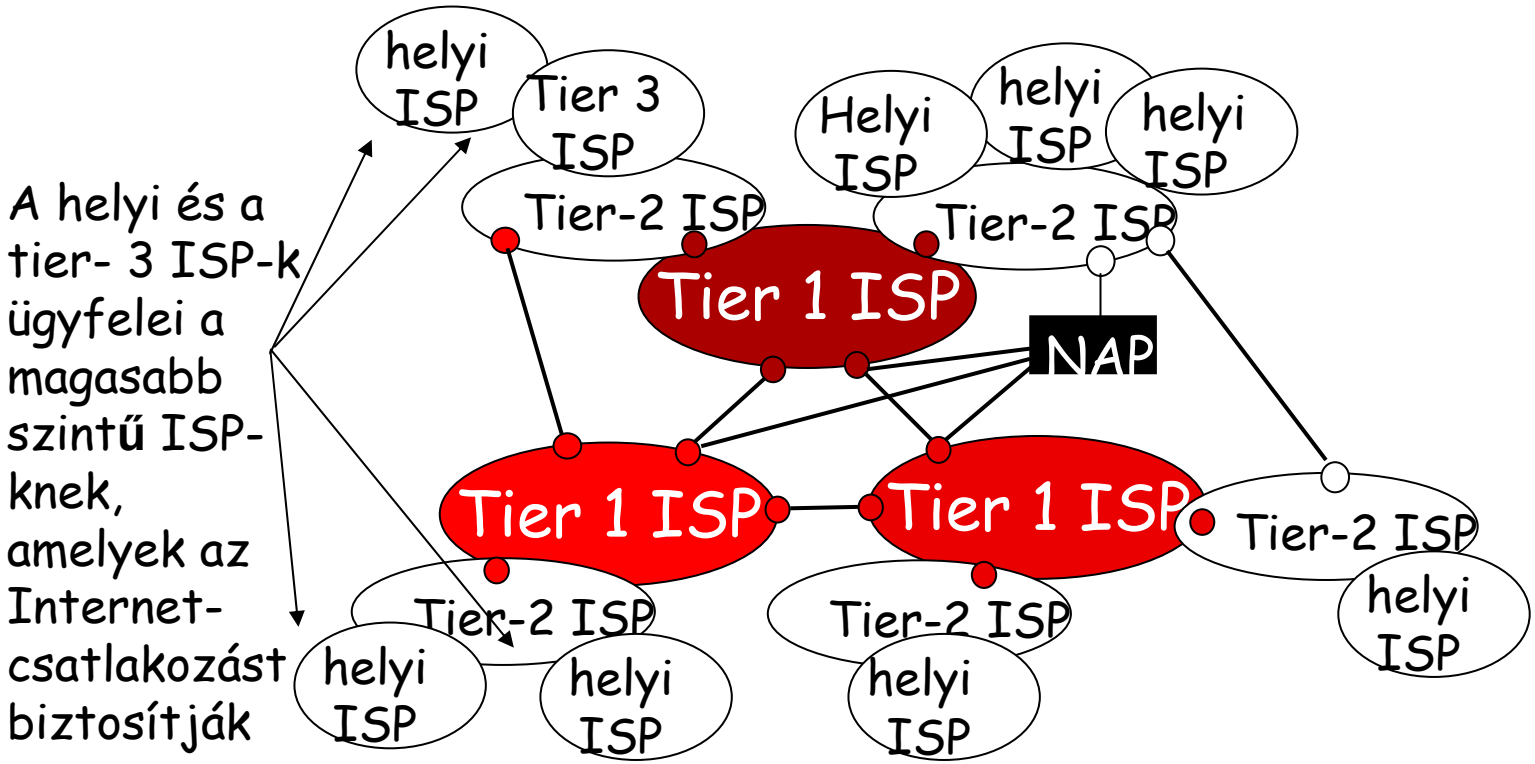
Az Internet: hálózatok hálózata

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



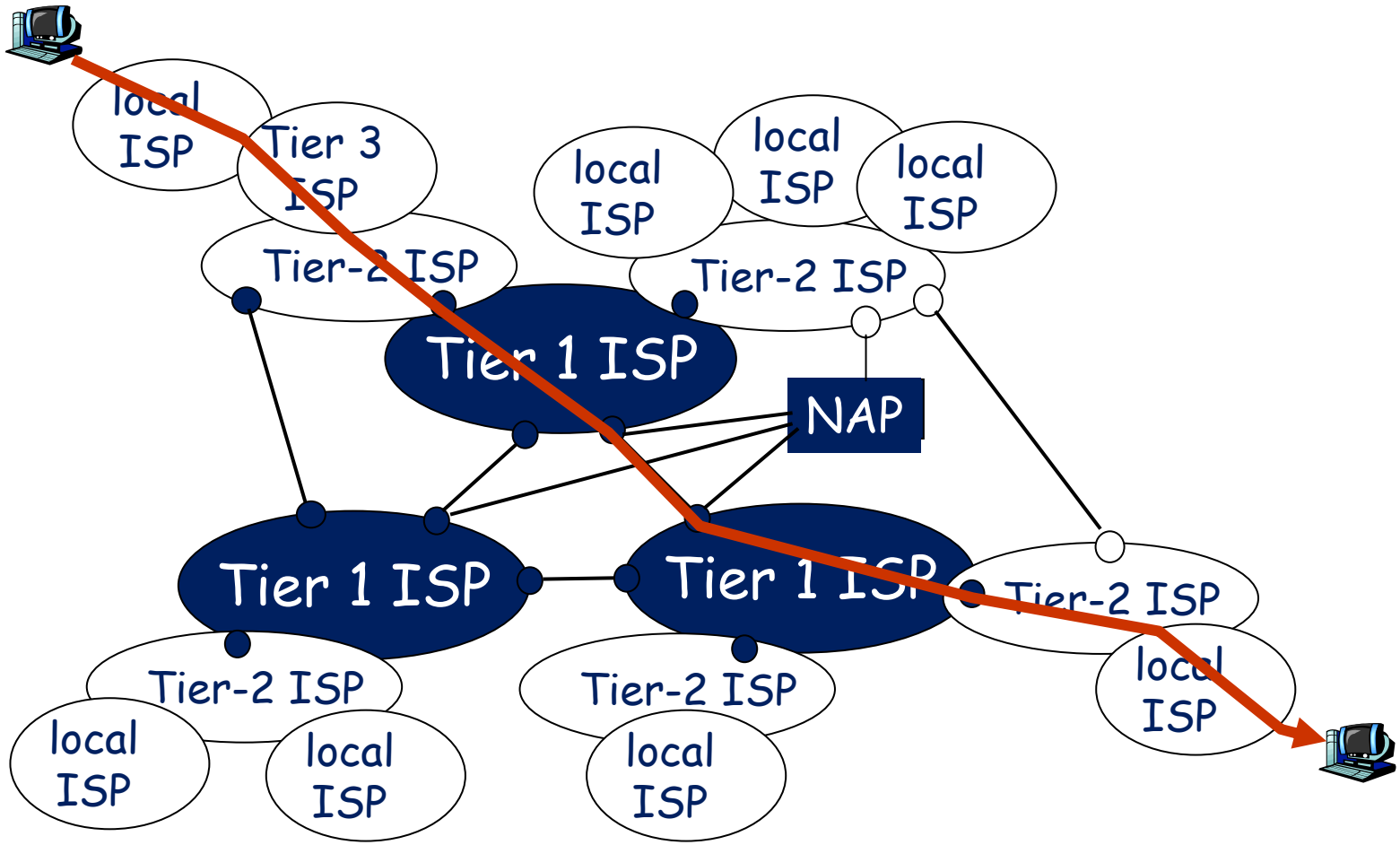
Az Internet: hálózatok hálózata

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

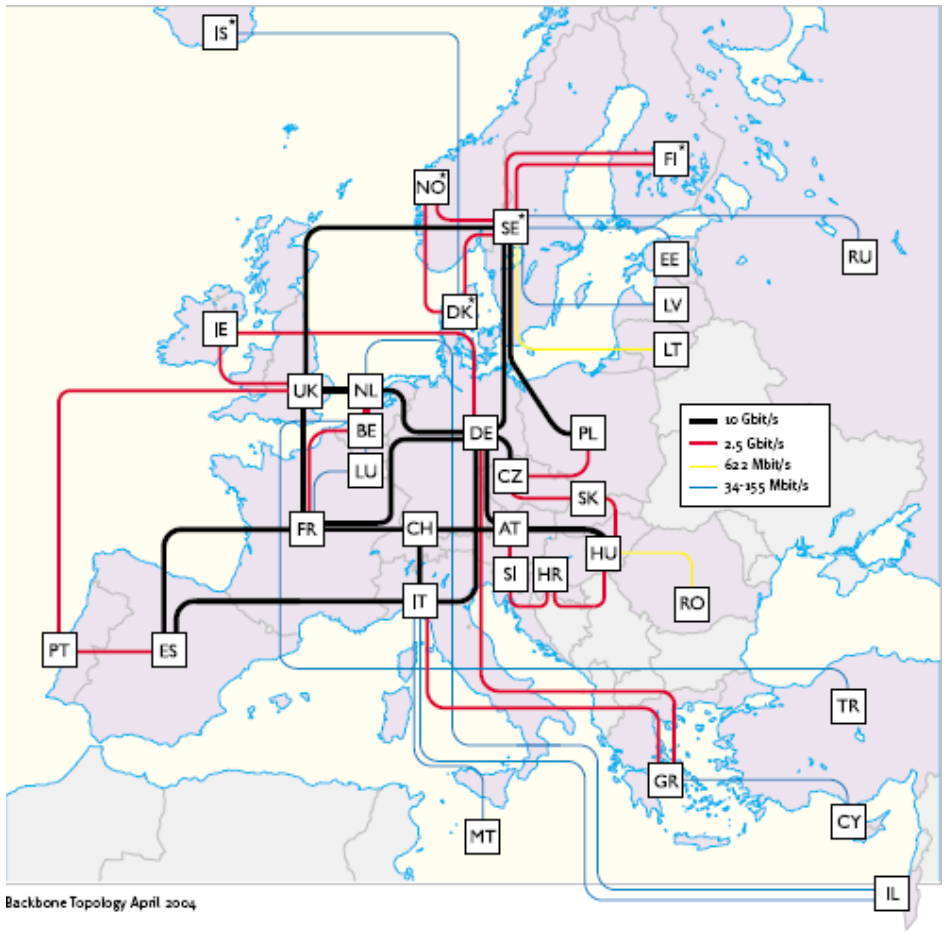


Az Internet: hálózatok hálózata

- Egy adatcsomag sok hálózaton halad át!



Az európai kutatói gerinchálózat (GEANT)



fekete vonal: 10 Gbit/s

piros vonal: 2,5 Gbit/s

sárga vonal: 622 Mbit/s

Magyarország a legizmosabb kapcsolattal rendelkezők közé tartozik

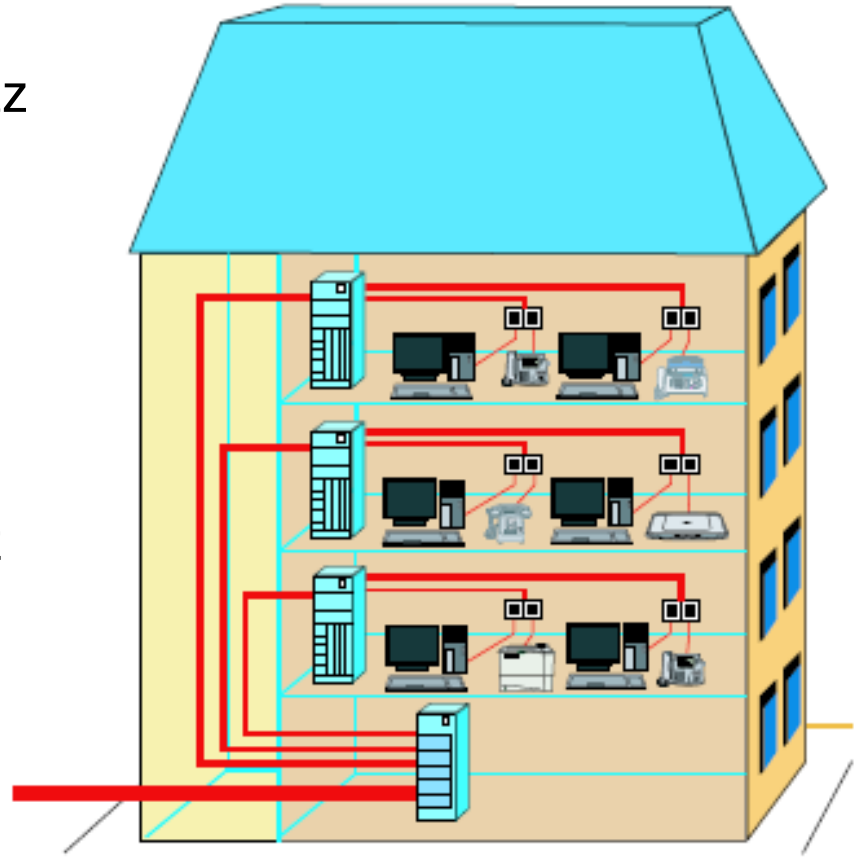
Helyi hálózat (local area network)

Többszintes irodaház

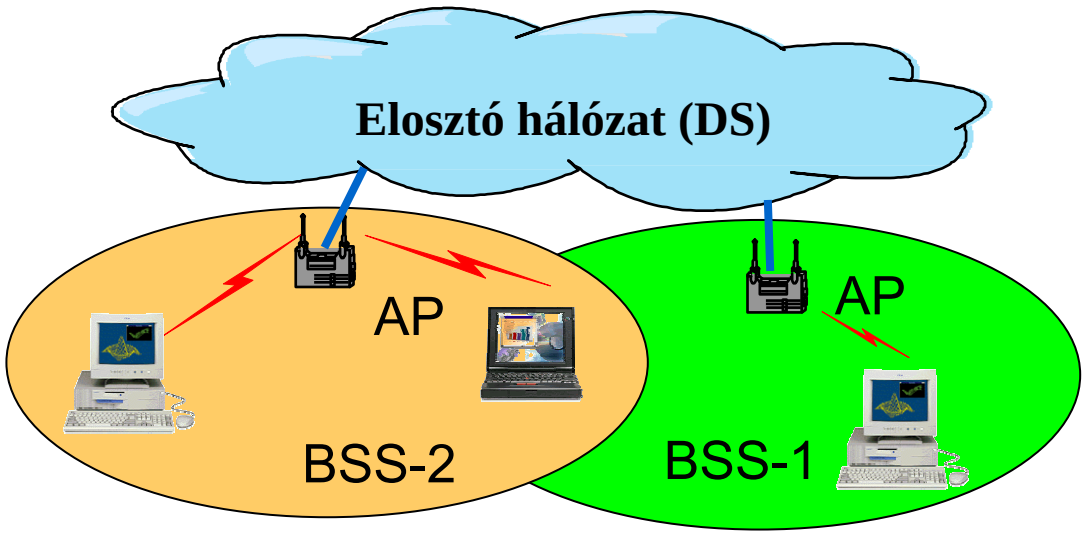
Szétosztó szekrény

Gerinchálózat az emeletek között

LAN-szegmensek az egyes szinteken



A vezeték nélküli hot-spot-ok technikája, a WLAN (wireless LAN, vezeték nélküli LAN)



ESS

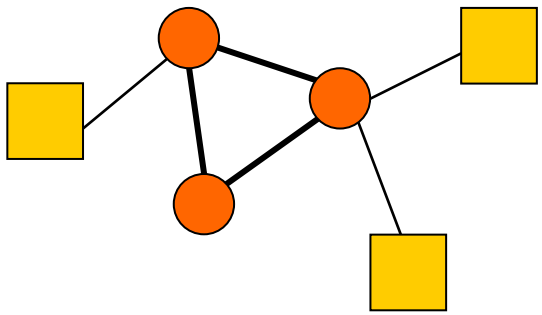
Rendszertechnika
(meg fogjuk ismerni részletesen)

AP – access points

WLAN-kártya

Mi tehát a számítógép-hálózat?

- Eredetileg: számítógépek összekapcsolása
- Ma: sokkal tágabb értelemben használt („kommunikációs hálózat”)
- Elméletben: topológia, gráf…
- Gyakran „infrastruktúra” értelemben, hálózati infrastruktúra, mint pl. az úthálózat, vasúthálózat, közművek



- Végkészülékek (end system)
- Csomópontok (node)
- Összekötések (link)

A cél: összeköttetések (connectivity) biztosítása végkészülékek között

Infrastruktúra és alkalmazások!

- A számítógép-hálózat azért van, hogy azon alkalmazások, szolgáltatások működjenek

- Ezért fontos:
  - megismernünk a számítógép-hálózati és Internet-alkalmazásokat
  - megvizsgálnunk, hogy azok milyen követelményeket támasztanak a hálózattal szemben

És mi ez a Számítógép-hálózatok tárgy?

- „Computer Networks”, standard BSc tárgy minden rendes egyetem informatika (computer science) szakán, plusz:
- Határozott hangsúly a
  - korszerű vezetéknélküli és mobiltechnológiákon
  - multimédia és Internet-alkalmazásokhoz szükséges feltételek biztosításán, plusz:
- Bizonyos alapok nyújtása az erre épülő „Távközlő hálózatok és szolgáltatások” tárgyhoz
- A tárgy címe a fentieket nem fejezi ki elég jól, de ez vált általánossá történetileg és mi is így hívjuk.

Összefoglalás: miről volt szó ezen a bevezető előadáson?

- Mi a számítógép-hálózat, mi az Internet?
- Kis történeti visszatekintés:
  - kiknek köszönhető az, ahol tartunk?
  - milyen új elveket fedeztek fel és technikákat hoztak létre
- Példák számítógép-hálózatokra
  - az ARPANET-től a Wi-Fi-ig
- *Legközelebb:*
  - *Jellegzetes alkalmazások és igényeik a hálózattal szemben. Mivel foglalkozunk a tárgyban, hogyan épül fel?*
  - *Szabványosítás, szabványosítási szervezetek*
    - *IETF és társai*

Adminisztráció...

Fontos tudnivalók

- Félévközi követelmény: ZH
  - **ZH: április 8, 8-10h**
  - **pótZH: május 22, 10-12h**
    - Két részből áll (ahogy a vizsga is):
      - tesztkérdések (beugró)
      - ZH-t megelőző gyakorlatok számítási példái, kiegészítős kérdések
    - A ZH eredménye nem számít bele az év végi vizsgajegybe
- ZH: papíron
- Vizsga: elektronikusan, a HSzK-ban

Segédanyag

- Segédanyag:
  - ***Az előadások slide-sorozatai,***
  - ***James F. Kurose - Keith W. Ross: Számítógép-hálózatok működése, Panem, 2008***
  - ***Lencse G.: Számítógép-hálózatok, Széchenyi István Egyetem, az anyag jelentős részéhez segédanyagként használható,***
  - ***Tanenbaum: Számítógéphálózatok, Panem, 2004, kijelölt fejezetek segédanyagként használhatók***
  - ***További közzétett segédanyagok***

Technikai tudnivalók

- ZH, vizsgázás, előadás anyagainak elérése, hirdetések kizárólag az általunk működtetett Moodle* site-on keresztül:

  http://moodle.hit.bme.hu/

- Ezt mindenki eléri, aki felvette a tárgyat

* *Moodle: a világban és Magyarországon is széleskörűen használt e-learning keretrendszer*

A Moodle site-unk használata

Bejelentkezés:

- Felhasználónév = Neptun kód (kis betűvel)
- Jelszó generálása= a Neptunban megadott e-mail címre lehet kérni (mindenkinél ez az e-mail cím lesz a default)

Leonard Kleinrock idézet

„Don’t be constrained by today’s technology. Reach out and imagine what could be and then make it happen!”

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

SZÁMÍTÓGÉP-HÁLÓZATOK BEVEZETŐ ELŐADÁS 2.

Mérnök-informatikus szak, BSc, 4. félév

2012/13 2.félév

Dr. Simon Vilmos

adjunktus

BME Hálózati Rendszerek és Szolgáltatások Tanszék

svilmos@hit.bme.hu

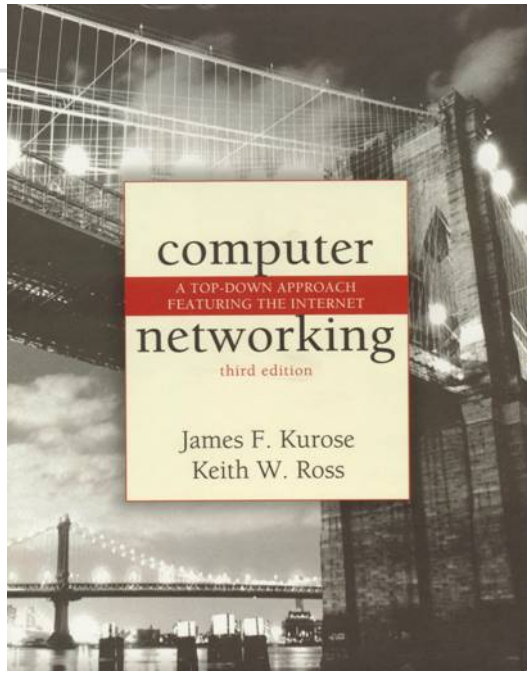
2012.február 14

Miről volt szó az előző előadáson és mi lesz ma?

- Ez volt:
  - Mi a számítógép-hálózat, mi az internet?
  - Kis történeti visszatekintés:
    - kiknek köszönhető az, ahol tartunk?
    - milyen új elveket fedeztek fel és technikákat hoztak létre
  - Példák számítógép-hálózatokra
    - az ARPANET-től a Wi-Fi-ig
- Ez lesz ma:
  - Szabványosítás, szabványosítási szervezetek
    - IETF és társai
  - Jellegzetes alkalmazások és igényeik a hálózattal szemben
  - Mivel foglalkozunk a tárgyban, hogyan épül fel a tárgy anyaga?

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Copyright”-megjegyzés: slide-ok és ábrák időnként ebből a könyvből:



A note on the use of these ppt slides:

We’re making these slides freely available to all (faculty, students, readers). They’re in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we’d like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

All material copyright 1996-2006
J.F Kurose and K.W. Ross, All Rights Reserved

Computer Networking: A Top Down Approach Featuring the Internet, 3rd edition.
Jim Kurose, Keith Ross
Addison-Wesley, July 2004.

Hálózati és Internet-szabványok...

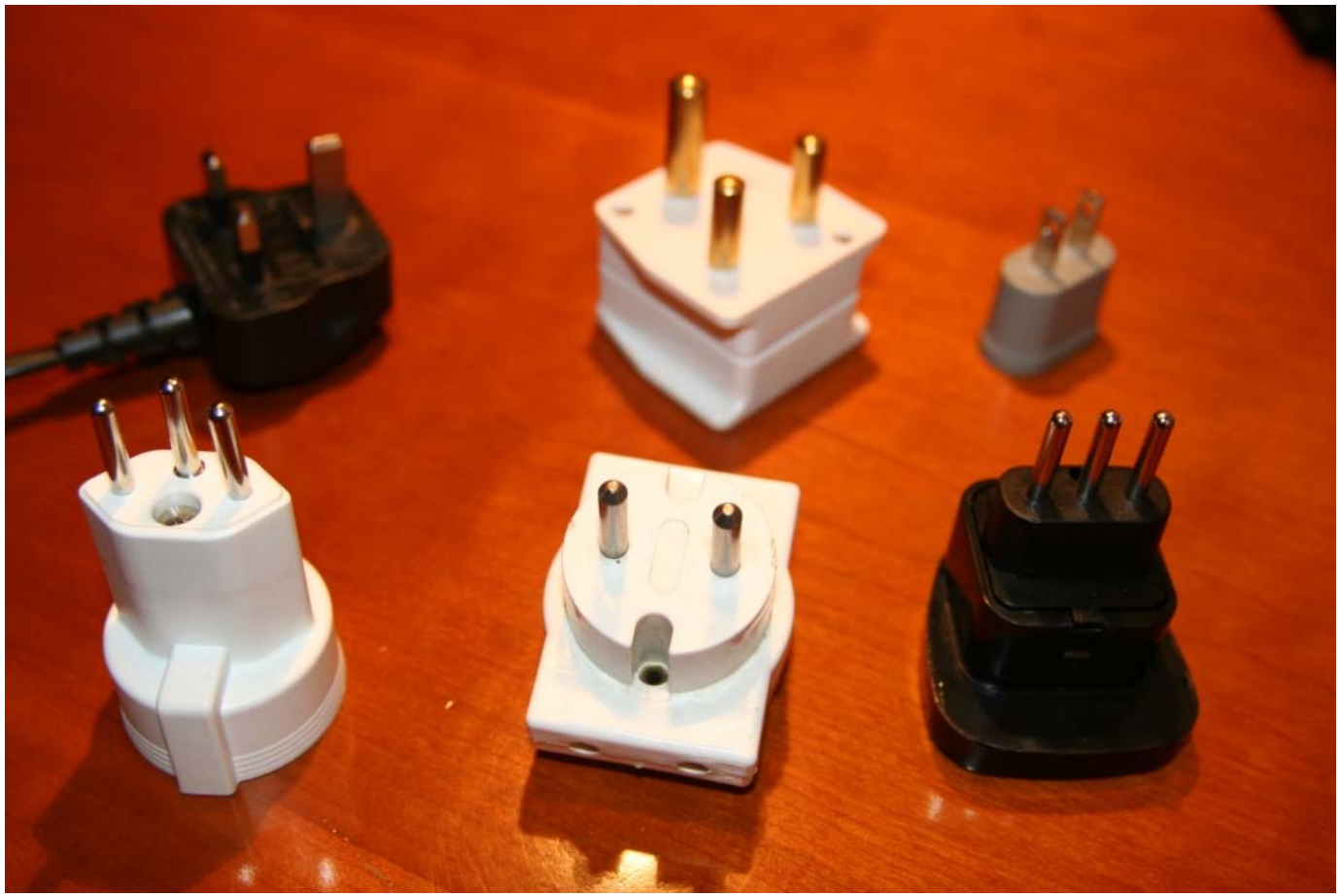
...és szabványosítási szervezetek

2012.február 14

Szabvány, szabványosítás, a szabványosítás fontossága

- Az adott eszköz, rendszer vagy – rész legfontosabb **fizikai, elektromos és procedurális jellemzőinek lerögzítése**
- Mikor történjék meg a szabványosítás?
- A szabványnak megfelelés – **a konformancia**
  - biztosíték arra, hogy az eszköz „tudja”, amit szeretnénk
  - de önmagában nem biztosíték arra, hogy két különböző gyártó eszköze együttműködik!
- A szabvány sok mindent specifikál, a termék ennek **részhalmazát** tudja
  - alaposan meg kell vizsgálni, amikor azt mondják, a termék „szabványos”
  - ha a specifikáció **azonos részhalmazát tudják, akkor együttműködnek**
- Gyári és nyilvános szabványok
- **De facto** és **de jure** szabványok

Nemzetközi szabványok kellenek!



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A számunkra fontos szabványosítási szervezetek

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

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IETF: Internet Engineering Task Force

Nagy, nyitott szervezet:

- gyártók, szolgáltatók, kutatók, ...

- Munkacsoportokban (Working Group), levelezőlisták segítségével
- Dokumentumai az RFC-k (Request for comments)
- Hagyományhűen textformátumúak az RFC-k
- Lassú fázis (önkéntesek, viták, konszenzus), pl. SMTP
- De gyakorlatiasabb, mint pl. ISO
  - Internet Draft ⟹ Proposed Standard ⟹ *Internet Standard*
- Április elsejei vicces RFC-k: evil bit, IPv6 over Facebook

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IEEE: néhány aktív munkacsoport

- A világ legnagyobb, USA-központú villamosmérnök-egyesülete

- 802.1 Higher Layer LAN Protocols Working Group
- 802.3 Ethernet Working Group
- 802.11 Wireless LAN Working Group
- 802.15 Wireless Personal Area Network (WPAN) Working Group
- 802.16 Broadband Wireless Access Working Group
- 802.17 Resilient Packet Ring Working Group
- 802.20 Mobile Broadband Wireless Access (MBWA) Working Group
- 802.22 Wireless Regional Area Networks

- de facto *szabványból* de jure *szabványt csinálnak*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

Jellegzetes internet-alkalmazások és igényeik a hálózattal szemben

2012.február 14

Minden alkalmazás alapvető igénye: hálózati összeköthetőség - *connectivity*

Az úthálózat analógiája:

- el lehessen jutni A városból B városba
  - útszakaszok és csomópontok (kereszteződések, elágazások) sorozatán keresztül
  - megfelelő útjelző táblák segítségével
- jó utak legyenek (széles, aszfaltos, síkosságmentesített, jelzett stb.)
- ha valamely szakaszon v. csomópontban forgalmi dugó támad, ezt kezelni kell (információ, elterelés stb.)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hálózati összeköthetőség - *connectivity*

- A számítógép-hálózatban:
  - A és B végpont összeköthető legyen
    - linkek és hálózati csomópontok sorozatán keresztül
    - megfelelő útvonalválasztó és –irányító módszerek és protokollok segítségével
  - “jó” linkjeink legyenek
    - kellő sebességűek
    - megfelelő fizikai paraméterekkel
      - pl. hibaarány, késleltetés
  - ha valamely linken v. csomópontban forgalomtorlódás támad, kezelni kell
    - a forgalom elterelése
    - a forrás szabályozása
    - megelőző módszerek

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Elegendő-e az összeköthetőség biztosítása?

- Az úthálózat analógiája: elegendő-e mindez, hogy egy A városból induló kamion biztosan eljusson B városba (adott időn belül?)
  - Nyilván nem: pl. eltévedés, baleset, műszaki hiba estén.
  - Folyamatos kommunikáció kell a kamionos cég központjával
    - megszervezni a javítást, mentést, csereautó küldését.

- A számítógép-hálózatban sem!

  - Csomagok **eltérülnek, elvesznek, eldobásra kerülnek** a csomópontok minden igyekezete („best effort”) ellenére.

  - Kell tehát **kommunikációs eljárás és protokoll** amely a végpontok közötti adatcserét támogatja.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Ez már elég sok internetes alkalmazás működtetéséhez elegendő!

Ilyen alkalmazások:

- webszerver elérése
- fájlátvitel
- elektronikus levelezés
- peer-to-peer fájlcsere

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

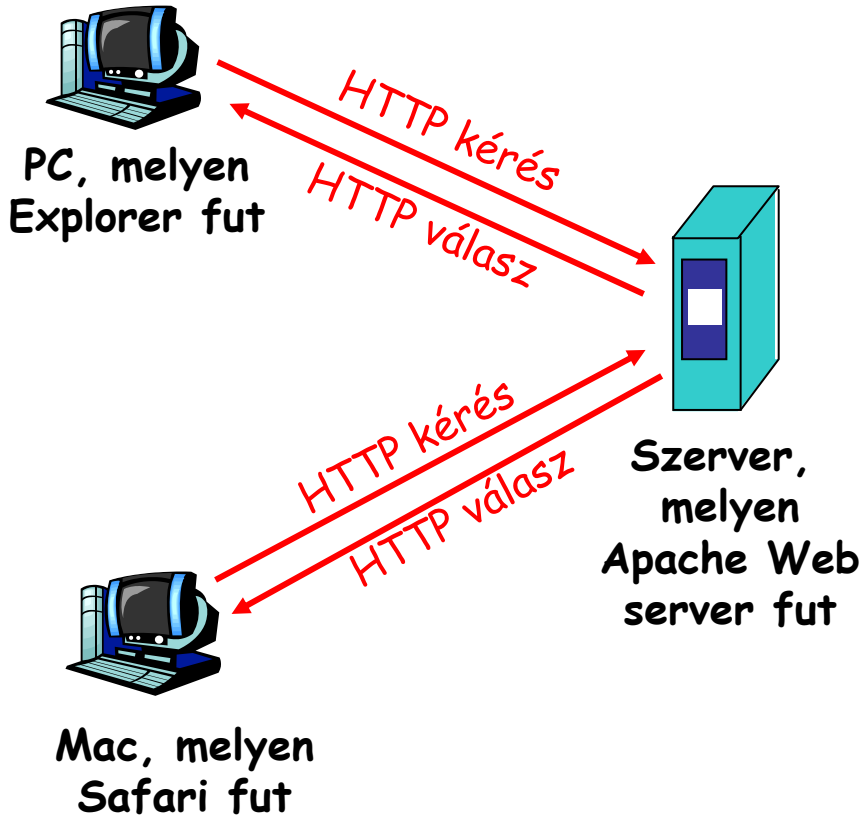
Web és HTTP

- A weblap objektumokat tartalmaz
  - Pl. HTML (*HyperText Markup Language*) file, JPEG kép, Java alkalmazás, hangfile,…
- A weblap tartalmaz egy HTML file-t, amely magában foglal számos objektumot
- Minden objektum címezhető a saját URL-ével
- Példa URL-re: http://moodle.hit.bme.hu/mod/resource/view.php?id=1666

HTTP: bevezető áttekintés

HTTP: HyperText Transfer Protocol

- Kliens-szerver modell
  - *kliens:* a böngészője kéréseket küld, válaszokat fogad, és megjeleníti a webes objektumokat
  - *szerver:* kérésre a web-szerver válaszként objektumokat küld vissza
- HTTP 1.0: RFC 1945
- HTTP 1.1: RFC 2068



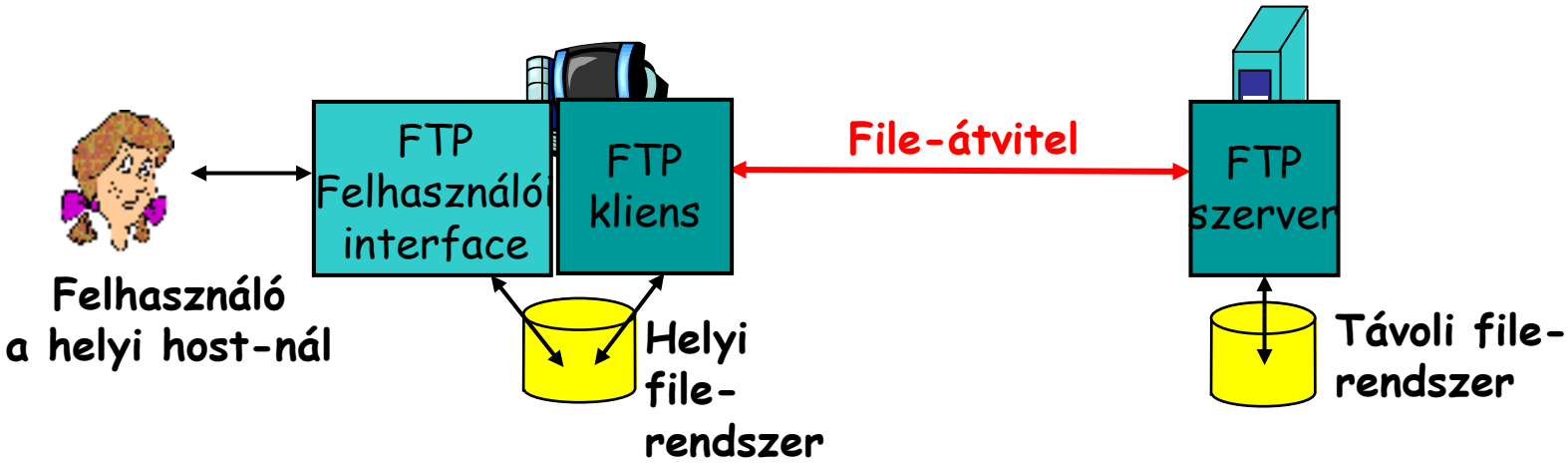
HTTP

- Megalkotása az előző előadásban megismert Tim-Bernes Lee és az IETF nevéhez fűződik
- **Független az átviteli rétegtől**, de általában TCP/IP réteg felett van
- HTTP 1.1 újdonságok:
  - **Perzisztens kapcsolat**: felette már stream is továbbítható
    - Chunked Transfer-Encoding
  - **Pipelining**: kliens elküldhet több kérést is egymás után anélkül, hogy megvárná a választ
  - **Byte serving**: a kért erőforrásnak csak a kliens által kijelölt darabját küldi el a szerver.

HTTP jövője

- Következő verzió: HTTP 2.0, IETF fejlesztésben
- A Google SPDY protokolljának lényeges elemeit használja
  - De facto szabvány?
- Csökkenti a web oldalak betöltési idejét:
  - multiplexált stream-ek egy TCP kapcsolaton belül
  - kérések priorizálása
  - kérés és válasz fejtészek tömörítése, a statikusok nincsenek újraküldve
  - szerver push és hint funkció

FTP: a file-átviteli protokoll



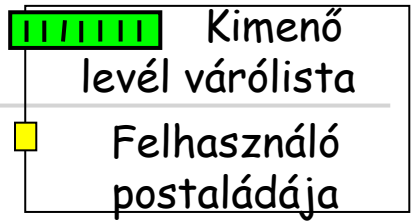
- File-átvitel a távoli hostra/hostról
- Kliens/szerver modell
  - *kliens:* az átvitelt indító oldal (akár felmásol, akár leszed adatot a távoli hostra/hostról)
  - *server:* távoli host
- ftp: RFC 959

FTP

- Két párhuzamos kapcsolat: egy vezérlési illetve egy adatátviteli csatorna (más porton)
  - out-of-band vs. in-band protokoll (HTTP)

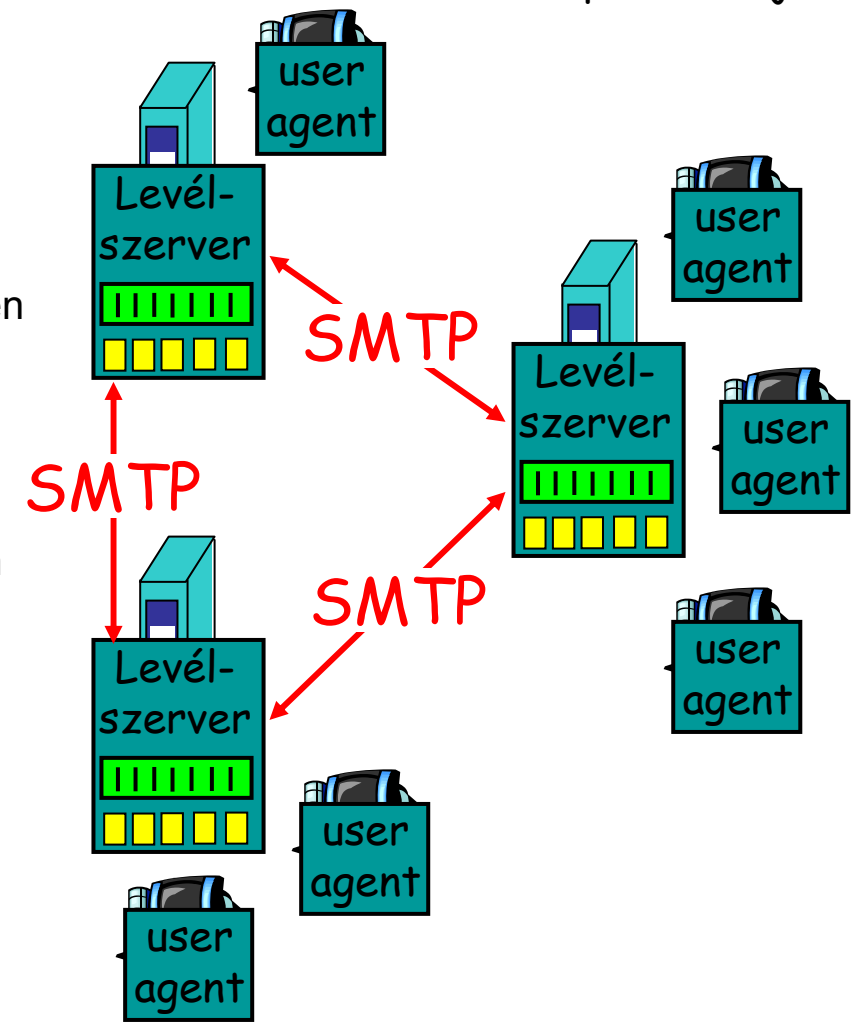
- Aktív/passzív adatátvitel

Elektronikus levelezés

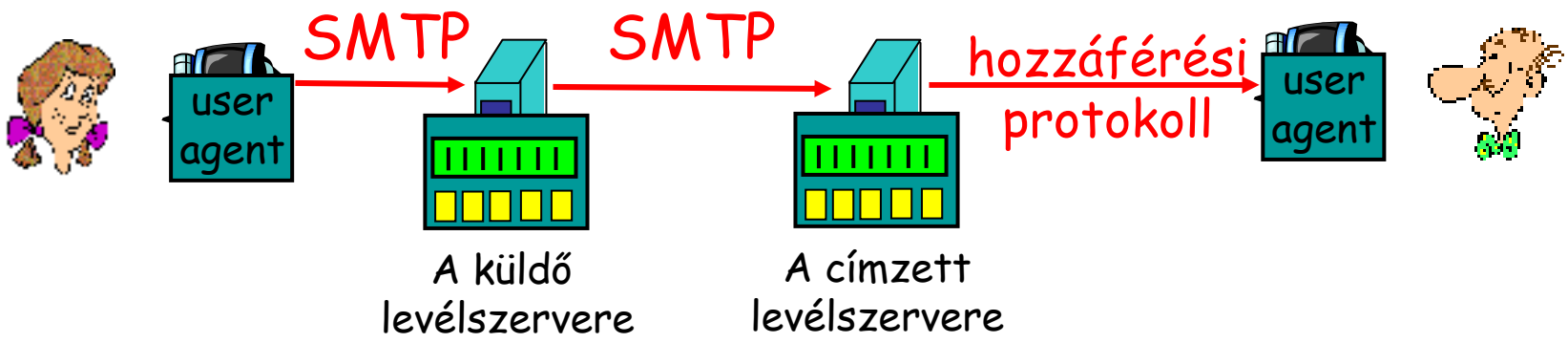


Három fő alkotóelem:

- **User Agent**
  - Levelek írása, szerkesztése, olvasása
  - Pl: Mozilla Thunderbird, Outlook
  - A kimenő és bejövő levelek a szerveren vannak tárolva
- **Levélszerverek**
  - A postaláda tartalmazza a felhasználó bejövő leveleit
  - Kimenő levelek várólistája a szerveren
- **Levelező protokoll (SMTP)** a levelező szerverek között az e-mailek továbbítására
  - Kliens:küldő
  - Szerver: fogadó levélszerver



Protokollok a levelekhez való hozzáférésre

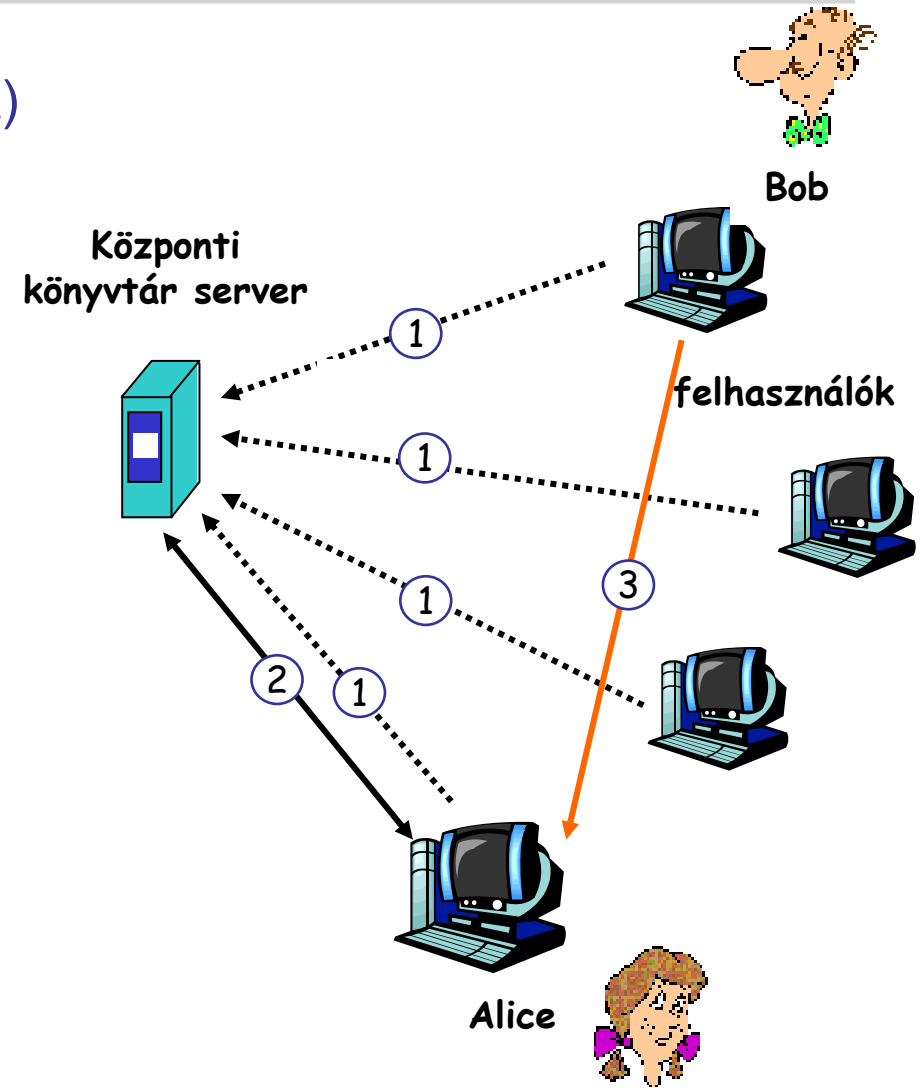


- SMTP: tárolja és továbbítja a leveleket a címzett szerverének
- Levelek lekérése a szerverről
  - POP: Post Office Protocol [RFC 1939]
    - **Azonosítás (levelezőprogram <--> szerver) és letöltés**
  - IMAP: Internet Mail Access Protocol [RFC 1730]
    - **Több beállítási lehetőség (összetettebb)**
    - **Egyszerre több kliens is hozzáférhet, észleli mások módosításait (flag-ek)**
  - HTTP: Gmail, Hotmail , Yahoo! Mail, stb.

P2P fájlcsere

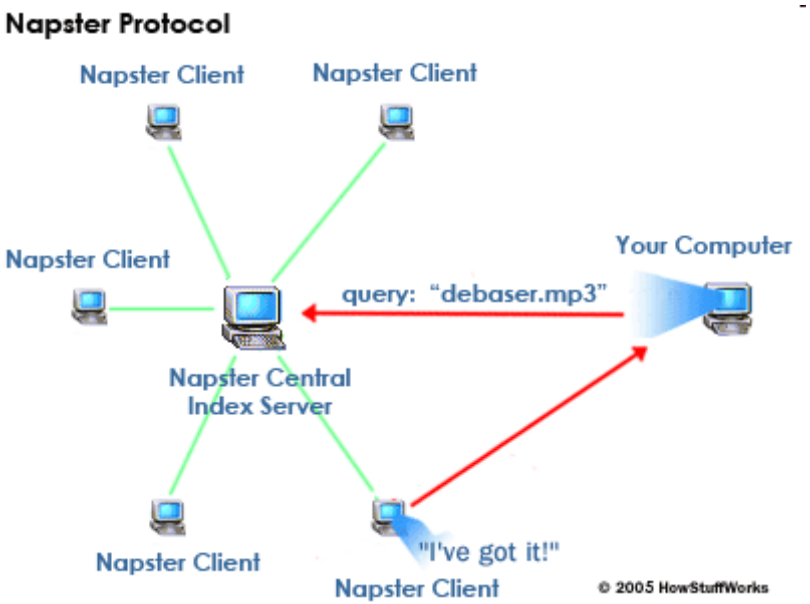
Eredeti „Napster” típusú (centralizált)

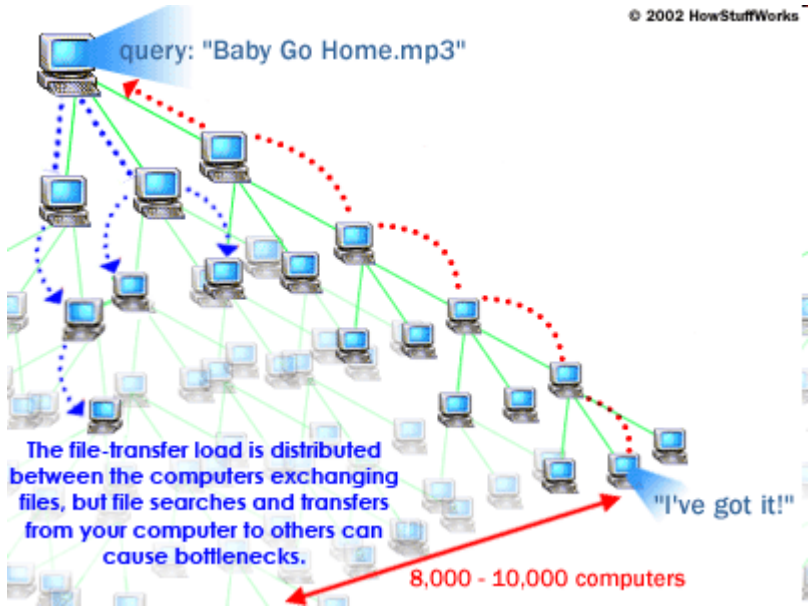
1) Ha egy felhasználó csatlakozik, akkor tudatja a szerverrel:
   - Az IP címét
   - Megosztani kívánt tartalmát
2) Alice megnézi, kinek van meg a letölteni kívánt zeneszám
3) Majd „elkéri” a file-t Bobtól



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

P2P topológiák





Centralizált (Napster)

Teljesen elosztott (Gnutella, v.04 előtti)

P2P generációk

1.generáció: hibrid, központi szerverrel (pl.Napster)

2. generáció: teljesen elosztott, nincs központi szerver (pl.Gnutella)

előny: robusztusabb mint az 1.generáció

hátrány: exponenciális forgalom növekedés elárasztás miatt

3.generáció: párhuzamos kommunikáció egyszerre több csomóponttal (pl. BitTorrent)

- seed, tracker, leech csomópontok

P2P: előnyök, hátrányok

- FTP-vel ellentétben nem szerver-kliens, mindenki lehet szerver és kliens is
- Előnye: robusztusabb, jobban skálázódik
- Hátránya: nagy sávszélesség igény
  - Megoldás: P2P caching
  - P2P forgalom blokkolása, rosszindulatú szeletek injektálása, erre BitTorrent titkosítás

- Internet forgalmának komoly hányadát már a fájlcserélő (főképp a BitTorrent) hálózatok adják

- Jövőben: a többszereplős online játékok is használhatják

Web-elérés, ftp, e-mail, p2p fájlcsere:

Az eddigi alkalmazások igényei a hálózattal szemben:

- alapvetően „csak” **megbízható kapcsolat** végpontok között
- valamekkora **átbocsátóképesség** („sávszélesség”)

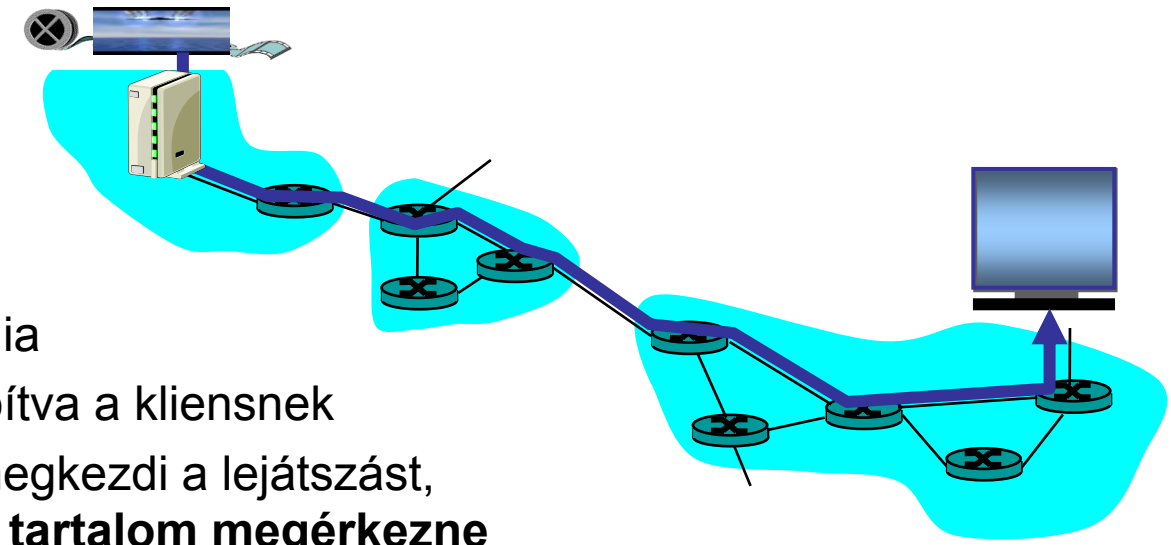
- az Internet IP és TCP protokollja elég,
- de kell is a TCP, amely a végpontok közötti megbízható kommunikációt biztosítja (ha kell, ismétlések stb. árán).

További, már nem ennyire „igénytelen” (sőt!) alkalmazások

- Audió-videó- (multimédia) streaming
  - tárolt (on-demand)
  - élő (live / real-time)
  - interaktivitás
- Élő beszéd (Internet-telefónia, Voice over IP)
- Élő videókonferencia (audió-videókonferencia természetesen)

NÉZZÜK MEG, MIK ITT A KÖVETELMÉNYEK A HÁLÓZATTAL SZEMBEN?

Multimédia streaming



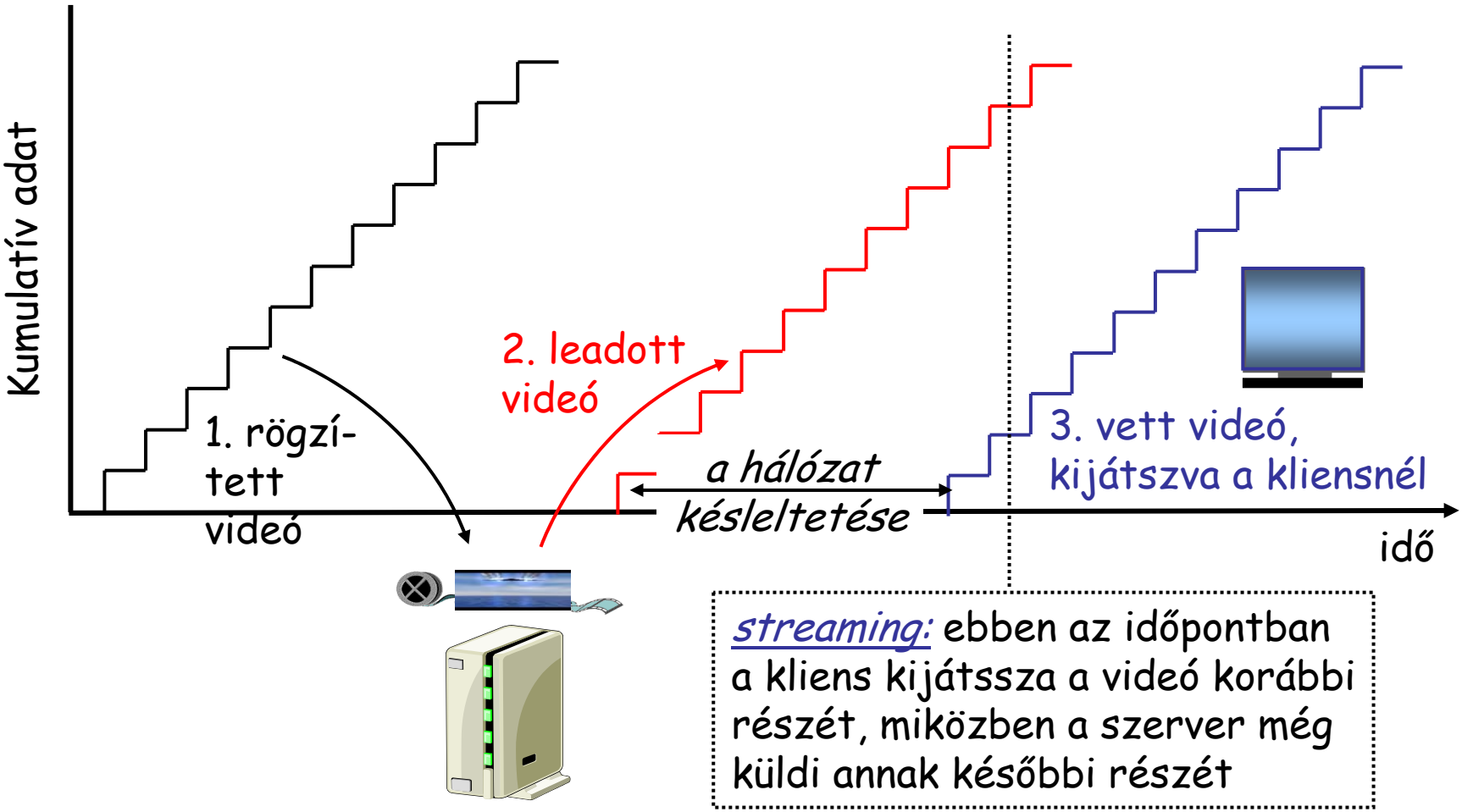
Streaming:

- a forrásnál tárolt média
- a hálózat által továbbítva a kliensnek
- streaming: a kliens megkezdi a lejátszást, **még mielőtt a teljes tartalom megérkezne**

- **időbeli követelmény a még továbbítandó adatokra: időben érkezzen meg a kijátszáshoz (playout)**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

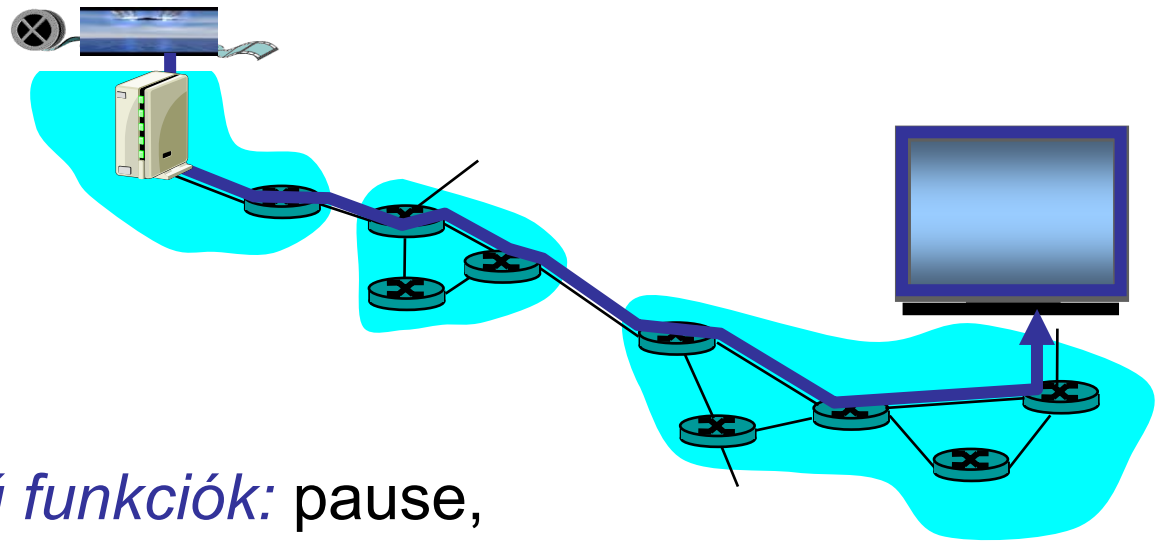
Multimédia streaming: a késleltetés kérdése



streaming: ebben az időpontban a kliens kijátssza a videó korábbi részét, miközben a szerver még küldi annak későbbi részét

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Multimédia streaming: interaktivitás



- *Videómagnó-szerű funkciók:* pause, rewind, fast forward, etc.
  - komolyabb késleltetés-követelmények

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Élő multimédia streaming

Példa:

- Internetes rádió, tv
- Élő sportközvetítések

Streaming:

- lejátszási puffer (playback buffer)
- néhány mp késleltetés elviselhető

Korlátozott interaktivitás:

- gyors vissza, pillanat állj lehetséges
- gyors előre nyilván lehetetlen

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Élő beszéd (Internet-telefónia, Voice over IP)

- Miért IP-n?
- Ma már ez triviális, mit mondtunk néhány éve?
- „Everything over IP”, nézzük meg, mi mindent lehet IP felett továbbítani?
  - *RFC3251 “Electricity over IP”, April 1, 2002*
  - *“Scents over IP”: France Telecom R&D*
    Multimédia bortúra Burgundiában
  - *ScentMail: illatos mail*

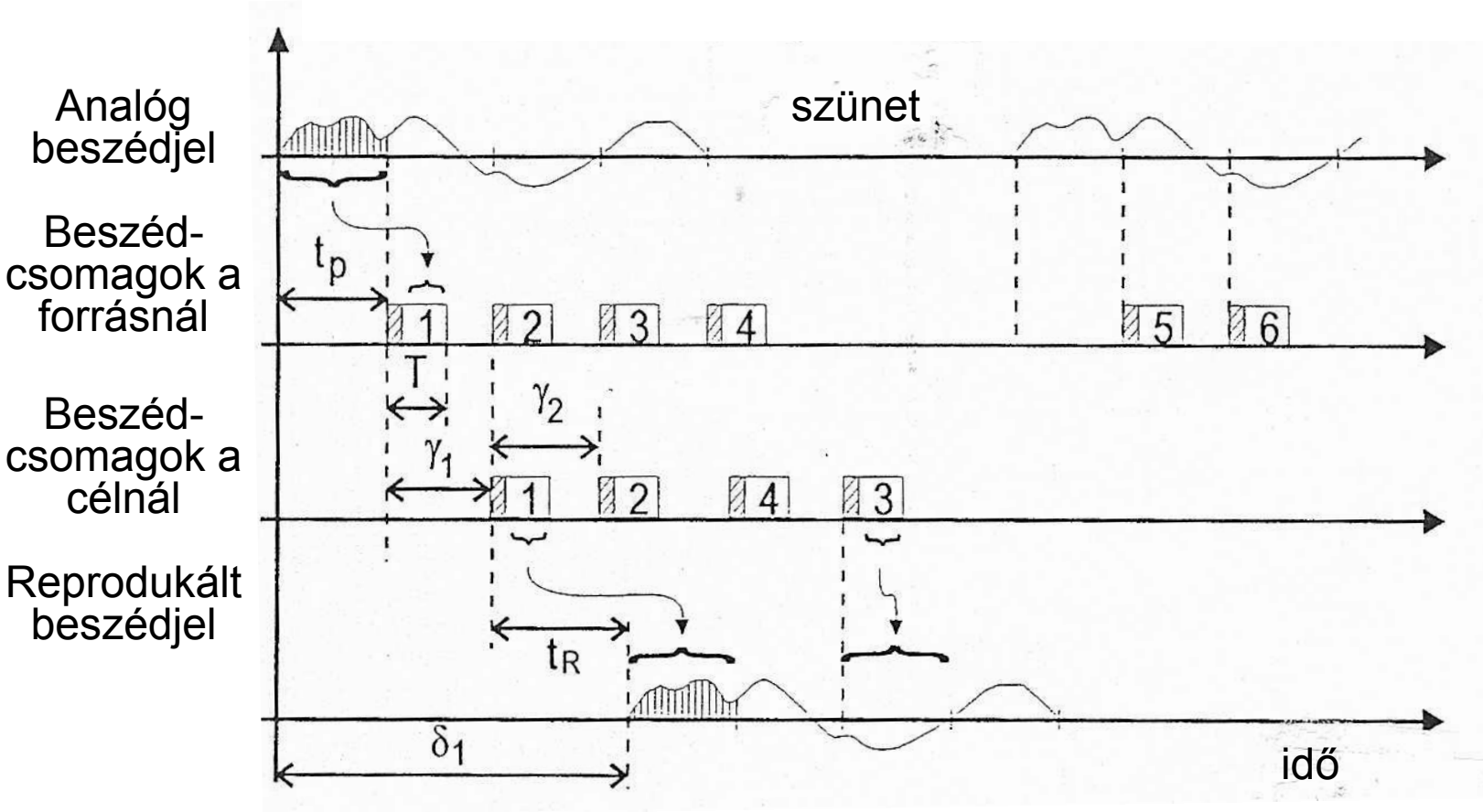
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Ma már nem kell magyarázni...

Két meggyőző példa az IP feletti beszéd- és általánosan: IP feletti multimédia-forgalom elterjedtségére:

- Skype
  - 45 millió felhasználó volt egyszerre on-line!
- A 3. generációs mobil hálózatokban (UMTS) Release5-től kezdve a beszédforgalom IP felett megy!

Beszédcsomagolás és -visszaállítás



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A beszédminőséget befolyásoló tényezők csomagkapcsolt hálózatokban

- Késleltetés (delay)
  - Megengedett maximum: **150 ms** körül
- Késleltetés-ingadozás (packet delay variance)
  - Megengedett maximum: **néhány tíz ms**
- Csomagvesztés
  - Megengedett maximum: néhány %, feltéve ha:
    - A kiesett beszédszegmensek rövidek
      - 10 ms nagyságrendben
    - **Véletlenszerűen** oszlanak meg az időben

Video over IP: még szigorúbb követelmények!

A megbeszélt multimédia alkalmazások igényei: összefoglalás

- A multimédia alkalmazások igényei:
  - *érzékenyek a késleltetésre* (delay sensitivity)
    - a késleltetés nagyságára
    - a késleltetés ingadozására
  - *de tűrik az adatvesztést* (loss tolerance)

- Szemben az első csoport „egyszerű” internetes alkalmazásaival (adatátvitellel), amelyek
  - *nem tűrik az adatvesztést*
  - *de tolerálják a késleltetést*

- *Tehát a multimédia alkalmazásoknál*
  - *nem kell feltétlenül megbízható kommunikáció a végpontok között (TCP protokoll)*
  - *sőt az okozott késleltetés miatt általában nem is szabad használni!*

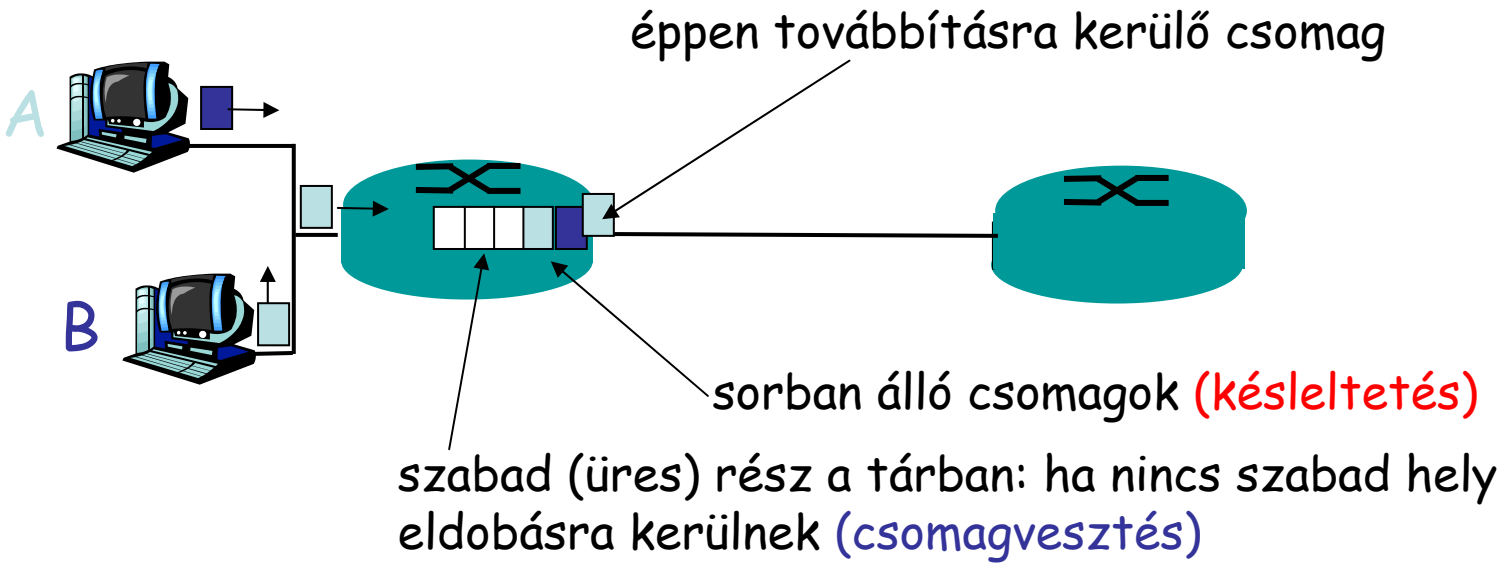
Ezek tehát az igények,

és mi a helyzet az Interneten (és általában a csomagkapcsolt számítógép-hálózatokban)?

Mik a csomagvesztés és késleltetés okai?

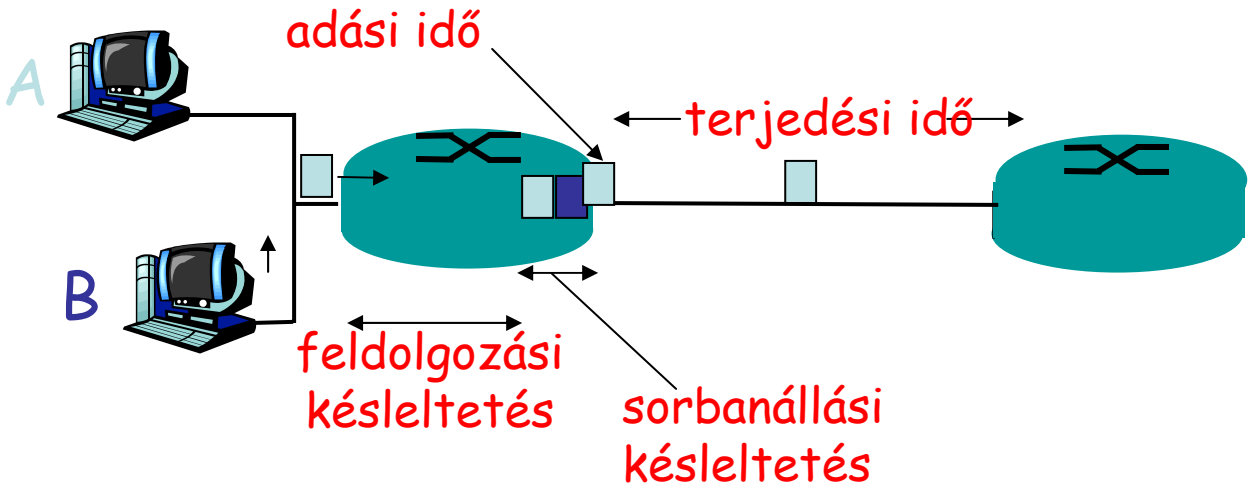
a csomagok sorban állnak a csomóponti gépek (routerek) tárolóiban

- a csomagok beérkezési sebessége meghaladja a kimenő link átbocsátóképességét
- a csomagok beállnak a sorba (sorokba?) és várnak a sorukra



A csomagok késésének négy fő oka (1)

- 1. Feldolgozás a csomópontban:
  - hibaellenőrzés
  - a kimenő link meghatározása
- 2. Sorbanállás
  - várakozás továbbításra az adott kimenő linken
  - a router terheltségétől függ



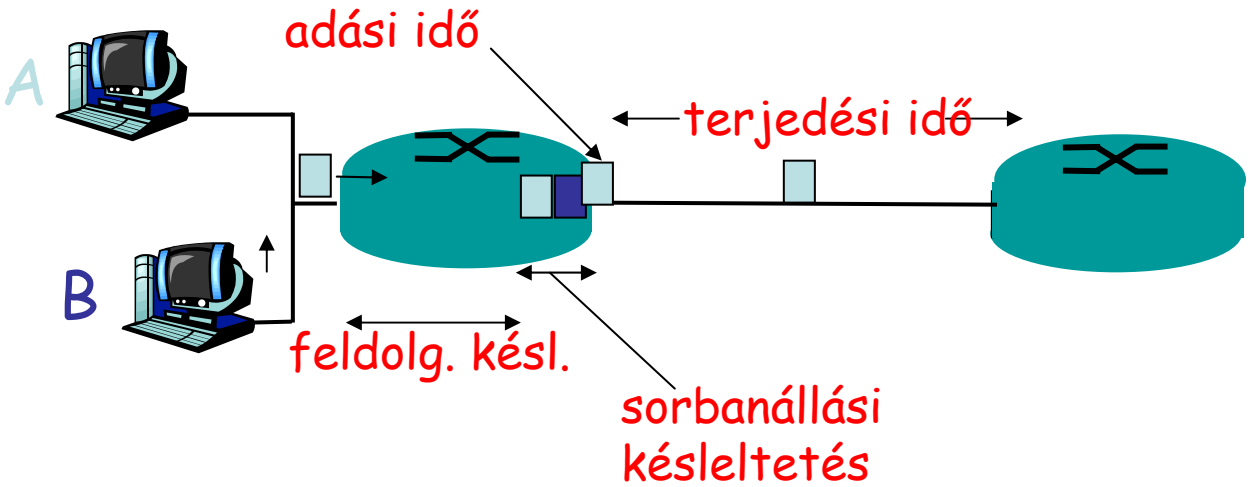
A csomagok késésének négy fő oka (2)

3. Adási idő:

- R= a link adatátviteli sebessége (bit/s)
- L=csomaghossz (bit)
- az adási idő = L/R

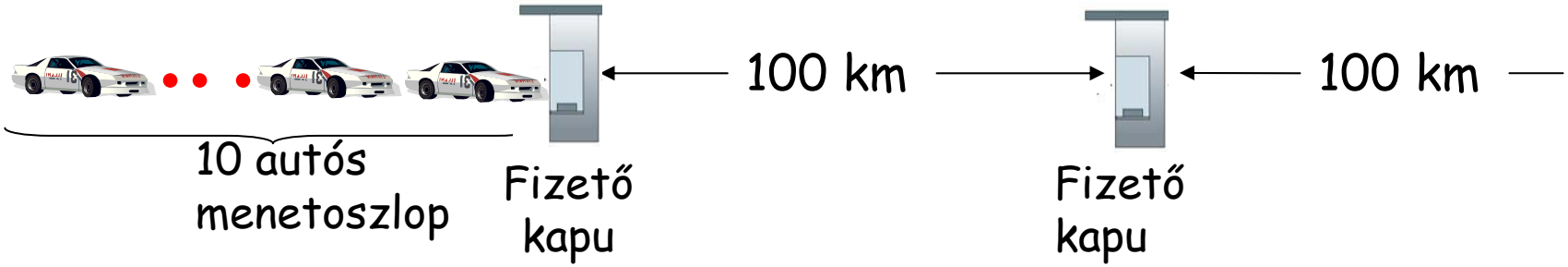
4. Terjedési idő:

- d = a link fizikai hossza
- s = terjedési sebesség az átviteli közegben (~$2x10^8$ m/sec)
- terjedési idő = d/s



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Menetoszlop analógia



- autók sebessége: 100km/óra
- 12 mp a fizetőkapu egy autóra (adási idő)

autó~bit; menetoszlop ~ csomag

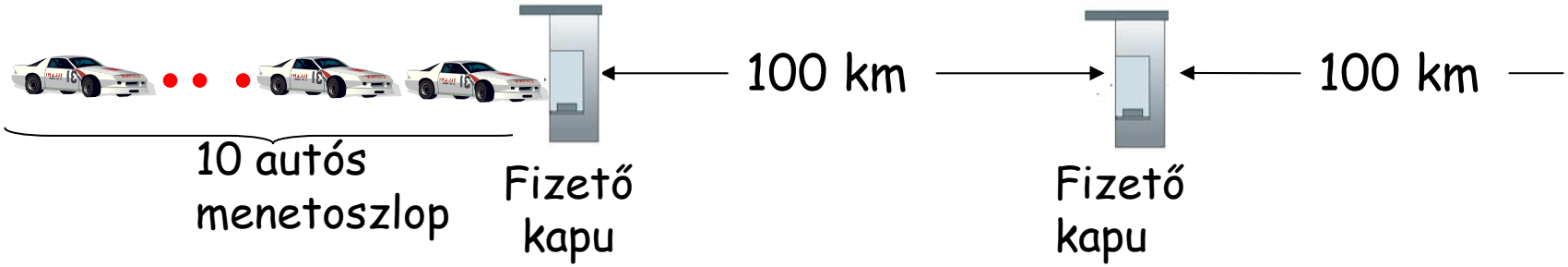
Kérdés: Mennyi idő múlva ér a menetoszlop a 2.fizetőkapuhoz?

- A teljes menetoszlop átengedési ideje a kapun = 12*10 = 120 mp (adási idő analógia)

- Utolsó autó megérkezése a 2.kapuhoz: 100km/(100km/óra)= 1 óra (terjedési idő analógia)

Válasz: 62 perc

Menetoszlop analógia (2)



- Autók most 1000km/órával haladnak
- 1 perc a kapunál autónként

Kérdés: Érkezhet-e autó a 2.kapuhoz mielőtt kiszolgálnák mindegyiket az 1.kapunál?

Igen! 7 perc után az 1.autó a 2.kapunál, míg 3 autó még az 1.kapunál

Csomag első bitje megérkezik a 2.routerhez, mielőtt a teljes csomag áthaladt volna az 1.routeren!

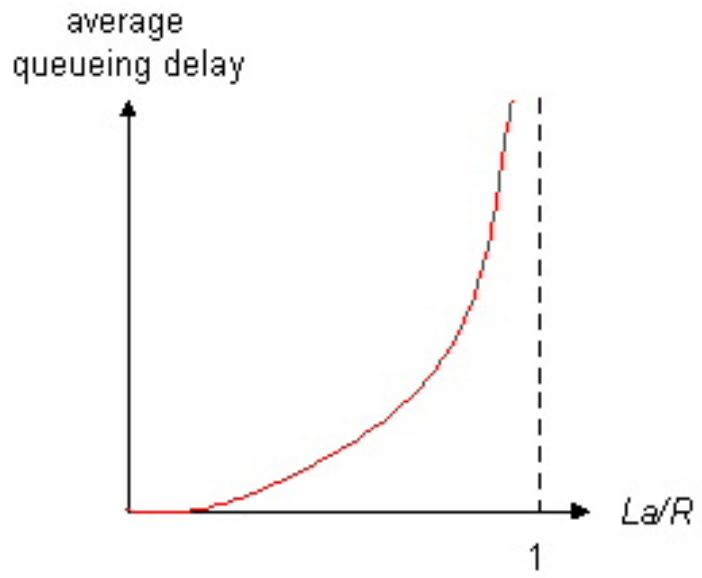
Csomóponti késleltetés, összefoglalva:

$$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

- d_{proc} = feldolgozási (processzálási) idő
  - tipikusan pár mikroszekundum
- d_{queue} = sorbanállási idő/késleltetés
  - a forgalomtól függ
- d_{trans} = adási idő
  - = L/R, kis sebességű linkeken jelentős lehet
- d_{prop} = terjedési idő
  - =d/s, pár mikroszekundumtól mp-ig

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Sorbanállási késleltetés



- R=link sávszélesség (b/s)
- L=csomaghossz (bit)
- a= átlagos csomag érkezési ráta

Forgalom intenzitása = La/R

La/R ~ 0: nincs sorbanállás, kis késleltetés
La/R -> 1: nagy késleltetés
La/R > 1: több igény érkezik mint amit ki lehet szolgálni, átlagos késleltetés végtelen lesz!

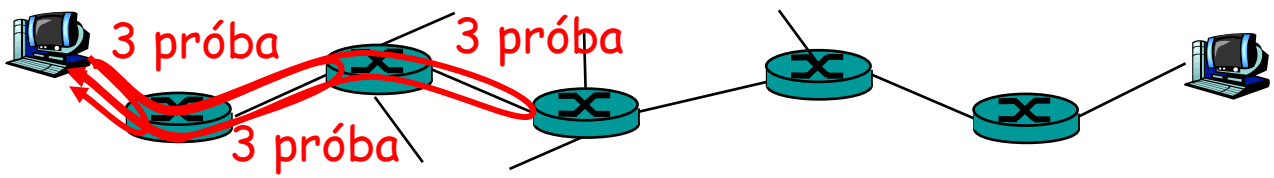
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Valós késleltetések és utak az Interneten

- Traceroute: otthon kipróbálni!

```
1  cs-gw (128.119.240.254)  1 ms  1 ms  2 ms
2  border1-rt-fa5-1-0.gw.umass.edu (128.119.3.145)  1 ms  1 ms  2 ms
3  cht-vbns.gw.umass.edu (128.119.3.130)  6 ms 5 ms 5 ms
4  jn1-at1-0-0-19.wor.vbns.net (204.147.132.129)  16 ms 11 ms 13 ms
5  jn1-so7-0-0-0.wae.vbns.net (204.147.136.136)  21 ms 18 ms 18 ms
6  abilene-vbns.abilene.ucaid.edu (198.32.11.9)  22 ms  18 ms  22 ms
7  nycm-wash.abilene.ucaid.edu (198.32.8.46)  22 ms  22 ms  22 ms
8  62.40.103.253 (62.40.103.253)  104 ms 109 ms 106 ms
9  de2-1.de1.de.geant.net (62.40.96.129)  109 ms 102 ms 104 ms
10  de.fr1.fr.geant.net (62.40.96.50)  113 ms 121 ms 114 ms
11  renater-gw.fr1.fr.geant.net (62.40.103.54)  112 ms  114 ms  112 ms
```

Transz-atlanti link



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csomagvesztés

- A sor (tár, puffer) **kapacitása véges**
- Ha a csomag olyankor érkezik, amikor a puffer tele van, eldobásra kerül: **csomagvesztés**
- Az elveszett csomagok vagy újraküldésre kerülhetnek, vagy nem
  - mikor igen, mikor nem?
- Csomagvesztés akkor is ha: a hibaellenőrzés a csomagot **hibásnak** találja
  - bithibák az átvitel során a nem ideális linkek miatt, zajok, zavarok, torzítások stb.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hogyan egyeztessük az alkalmazások igényeit és a hálózat problémáit?

- Az alapvető csomagkommunikációs és végpontok közötti kapcsolatokat kezelő protokollok mellett kellenek ún.
  - szolgáltatásminőséget (QoS – quality of service) biztosító módszerek és protokollok
- Egy ötlet, foglaljunk erőforrásokat:
  - csomóponti képességeket
  - link-kapacitásokat

  egy adott kommunikációs viszonylat (session) számára a hálózatban
- Egy másik ötlet: jelöljük meg a csomagokat a különböző igények szerint és a csomópontok ennek megfelelően kezeljék azokat
  - pl. prioritást biztosítva a beszédcsomagok számára

Hogyan épül fel a tárgy anyaga?

A házépítés analógiája:

- Alapozás
  - talajmechanika
- Szerkezetépítés
  - szilárdságtan, statika
- Épületgépészet
  - pl. hőtan

Hogyan tanuljunk házépítést?

- Először talajmechanikát, szilárdságtant, hőtant stb., utána alapozást, szerkezetépítést stb.
- Az alapvető tudományokból egyszerre mindig csak annyit, amennyi a következő gyakorlati részhez kell, tehát: talajmechanika, alapozás, szilárdságtan, szerk. ép.

Hogyan épül fel a tárgy anyaga?

- A második módszerrel:
  - elv(ek) és utána technikák, protokollok, rendszerek
  - aztán ismét bizonyos elvek, alapmódszerek, és utána...
- Előadások és gyakorlatok
  - az előadások egy része gyakorlati jellegű anyagot fog tartalmazni
  - de lesznek dedikált gyakorlati órák is, minden 3-4 „elméleti” előadást követően
  - az ezeken bemutatott számítási példák lesznek a ZH-n, vizsgán is!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az anyag beosztása (1)

- Bevezető áttekintés, hálózatok és rendszerek példái.
- Alkalmazások és szolgáltatások. Követelmények a hálózattal szemben.
- Protokollarchitektúrák, referenciamodellek.
- A fizikai szintű kommunikáció alapjai.

Gyakorlat.

- Többszörös hozzáférés.
- LAN-ok, LAN-ok összekapcsolása.
- BWA (WPAN, WLAN, WMAN).
- Áramkörkapcsolás, csomagkapcsolás, hívásvezérlés, címzés.

Gyakorlat.

- Routing.
- Ütemezés.
- IP.

Gyakorlat.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az anyag beosztása (2)

- Forgalomszabályozás. Hibakezelés.
- Szállítási réteg, TCP, UDP.
- Multimédia 1.r. Médiakezelés (RTP, RTCP, RTSP).
- Multimédia 2.r. Hívásvezérlés (SIP).

Gyakorlat.

- Szolgáltatásminőség (QoS).
- Multimédia 3.r. Szolgáltatásminőség biztosítása (IntServ, DiffServ).
- MPLS.
- Alkalmazások.

Gyakorlat.

Számítási példa

Mikor kapunk nyugtát a központban, ha az ADSL linken (rézkábelen) a sorbanállási idő a felhasználónál 3 ms, a feldolgozási idő 1 ms (feltételezve hogy a másik oldalon elhanyagolhatóak ezek a késleltetések), miközben:

- Letöltés: 4 Mbit/s
- Feltöltés: 512 kbit/s
- Távolság: 4 km
- Csomagunk 1000 bájt
- Nyugta 64 bájt
- Terjedési sebesség $2 \cdot 10^8$ m/s

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

Ennyi volt mára...
Legközelebb: protokollarchitektúrák, referenciamodellek.

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások
svilmos@hit.bme.hu

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

PROTOKOLLARCHITEKTÚRÁK

Mérnök-informatikus szak, BSc, 4. félév
2012/13 2.félév

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.február 19.

Az anyag beosztása (1)

- Bevezető áttekintés, hálózatok és rendszerek példái.
- Alkalmazások és szolgáltatások. Követelmények a hálózattal szemben.
- Protokollarchitektúrák, referenciamodellek.
- A fizikai szintű kommunikáció alapjai.

Gyakorlat.

- Többszörös hozzáférés.
- LAN-ok, LAN-ok összekapcsolása.
- BWA (WPAN, WLAN, WMAN).

Gyakorlat.

- Áramkörkapcs., csomagkapcs., hívásvezérlés, címzés.
- Routing.
- Ütemezés.
- IP.

Gyakorlat.

Tartalom

- Bevezetés, motiváció
- A protokollok kialakulása, jelölések
- Megvalósítás
- A protokollok szerepe a hálózatok leírásában

Bevezetés 1.

- „Protokoll”?
  - Más területeken: ***orvosi protokollok***, ***diplomáciai protokollok***

- A számítógép-hálózatoknál is szükség van **viselkedési szabályok**, azaz **protokollok**
  - lerögzítésére
  - betartására

- Definíció:

  A protokoll két vagy több kommunikáló egység közötti üzenetcsere **formátumait** és az **üzenetek sorrendjét** határozza meg, valamint az üzenetek vételéhez kapcsolódó és egyéb események által kiváltott **tevékenységeket**.

Bevezetés 2.

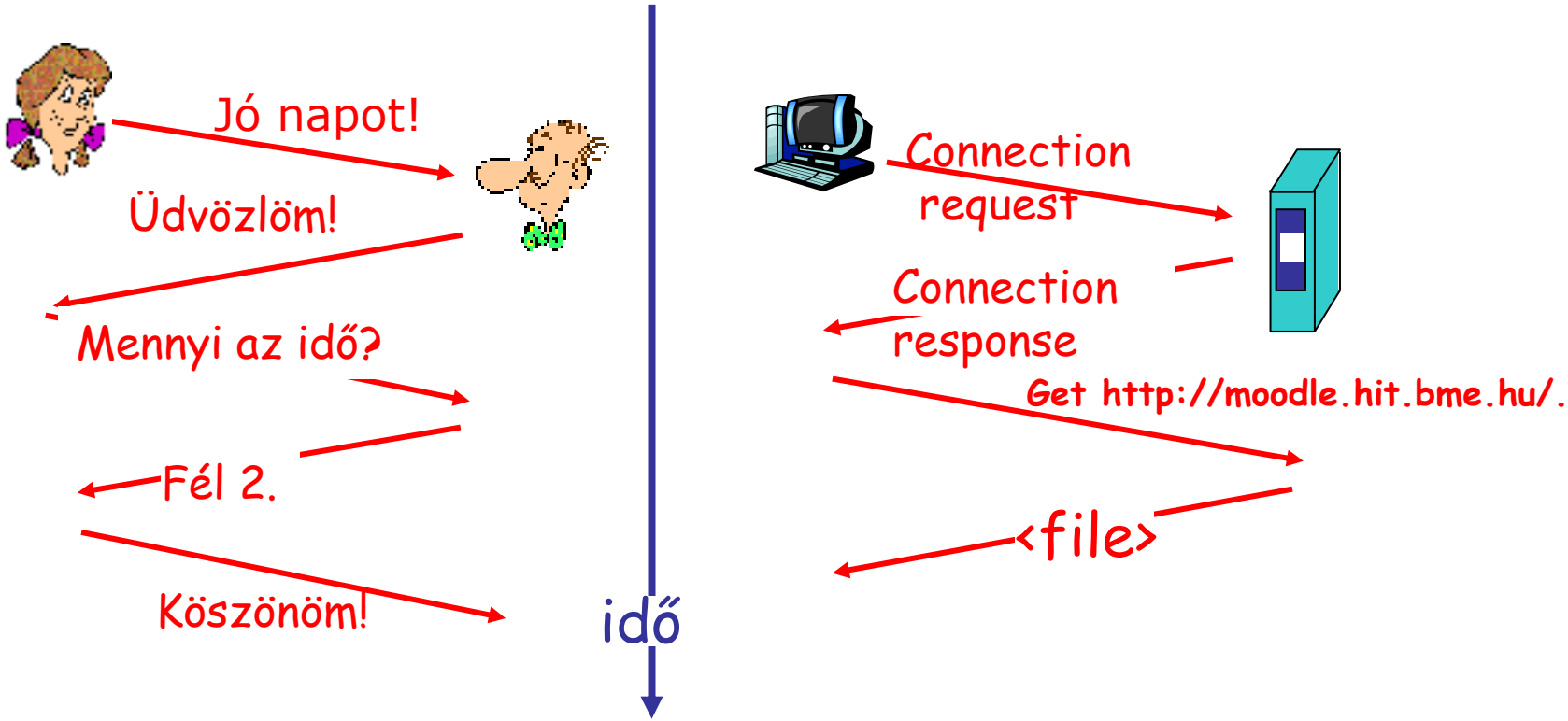
- Röviden:
  - Szintaxis (*syntax*) (formátum): adategységek formai leírása
  - Szemantika (*semantics*) (jelentés): az adatelemek értelmezése
  - Viselkedés (*behavior*): mit kell tenni valamely üzenet vételekor, küldésekor

- Helyesírás: protokoll és *protocol*

- **Módszer -> algoritmus –> protokoll** (l. pl. majd a routingnál: *linkállapot-módszer – Dijkstra-alg. – OSPF protokoll*)

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Protokollok az emberi és a gépek közötti kommunikációban



Ábrázolás forma: **Message Sequence Chart**

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A protokoll két fő része

Két elkülöníthető rész:

- A továbbított információ alakja, formája
  - A protokoll **statikus** része
  - **Protocol Data Unit** (protokoll-adategység)
- Mi történik a továbbításkor?
  - A protokoll **dinamikus** része
  - Mit kell tenni az adott protokollüzenet vételekor
  - Rendellenes esetek kezelése is

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Miért „protokollok”?

- Miért nem elég egyetlen protokoll?
  - Történelmi okai
  - Részfeladatokra tördelés
    - tevékenységek részekre bontása
    - az egyes részekre önálló szabályok
- Miért részekben, miért nem egyben?
  - egyszerűbb a tennivalók elvégzése
  - részenként lehet továbbfejleszteni
- Hogyan bontsuk részekre?
  - hány rész legyen?
  - hogyan viszonyuljanak egymáshoz?
  - vannak-e „természetes” határok?

Részekre bontás …

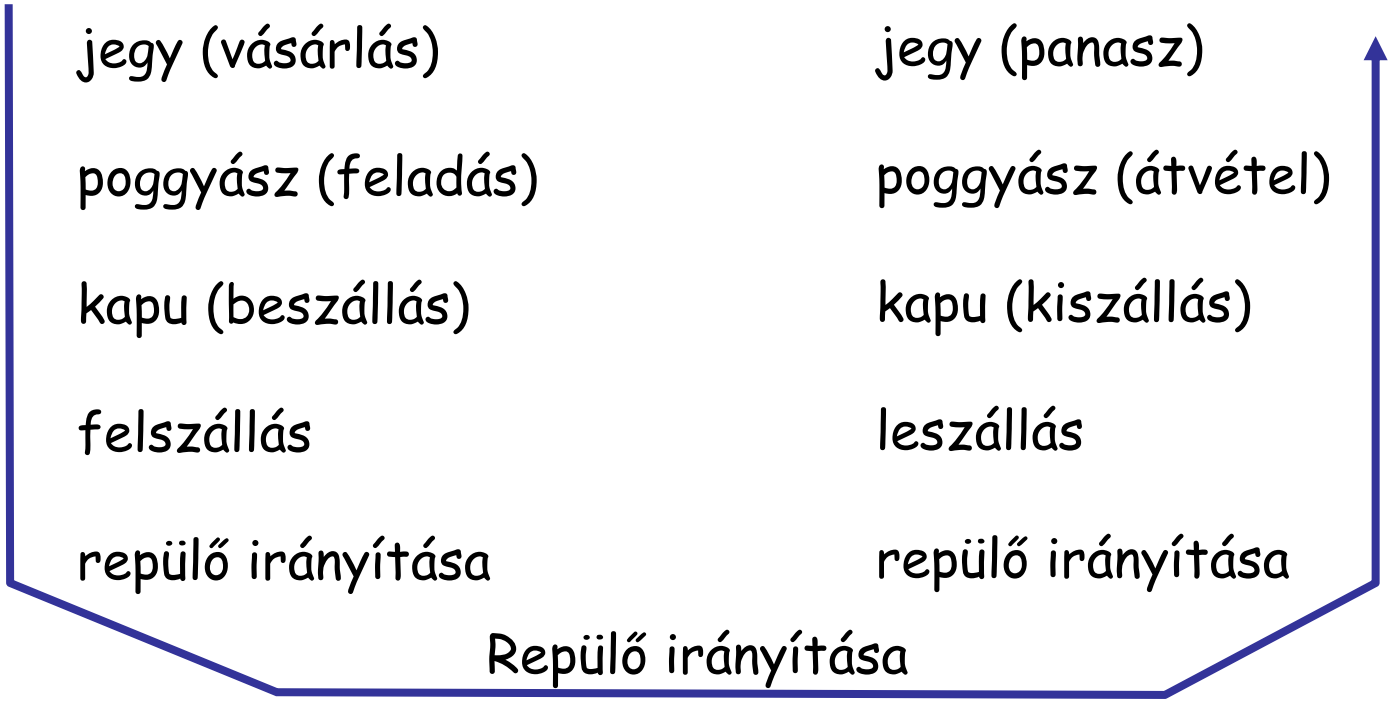
- Önálló, jellegzetes, gyakori feladatok (pl):
  - illeszkedés a jelátvivő közeghez
    - hardware-közeli feladatok megoldása, problémák kezelése
  - összeköttetéseken megbízható adattovábbítás
  - végpontok közötti információtovábbítás
  - kívánt végpontok azonosítása
  - kedvezőtlen forgalmi állapot kezelése

- Mindezekkel kapcsolatban az előforduló hibák kezelése is

- Részek – funkcionalitások – **„rétegek”**

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

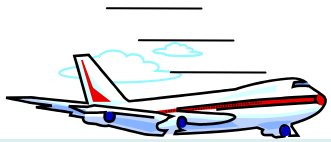
Analógia: légi közlekedés szervezése



- Lépések sorozata

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Analógia: légi közlekedés rétegezve



jegy(vásárlás)			jegy (panasz)	jegy
poggyász (feladás)			poggyász (átvétel)	poggyász
kapu (beszállás)			kapu (kiszállás)	kapu
pálya (felszállás)			pálya (leszállás)	fel/leszállás
repülő irányítás	repülő irányítás	repülő irányítás	repülő irányítás	repülő irányítás
Repülőtér	**Légi irányító központok**		**Repülőtér**	

Rétegek: minden réteg egy szolgáltatást valósít meg

- a saját rétegen belüli tevékenységével
- támaszkodva az alatta lévő réteg által nyújtott szolgáltatásra

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hálózati architektúra és referenciamodell

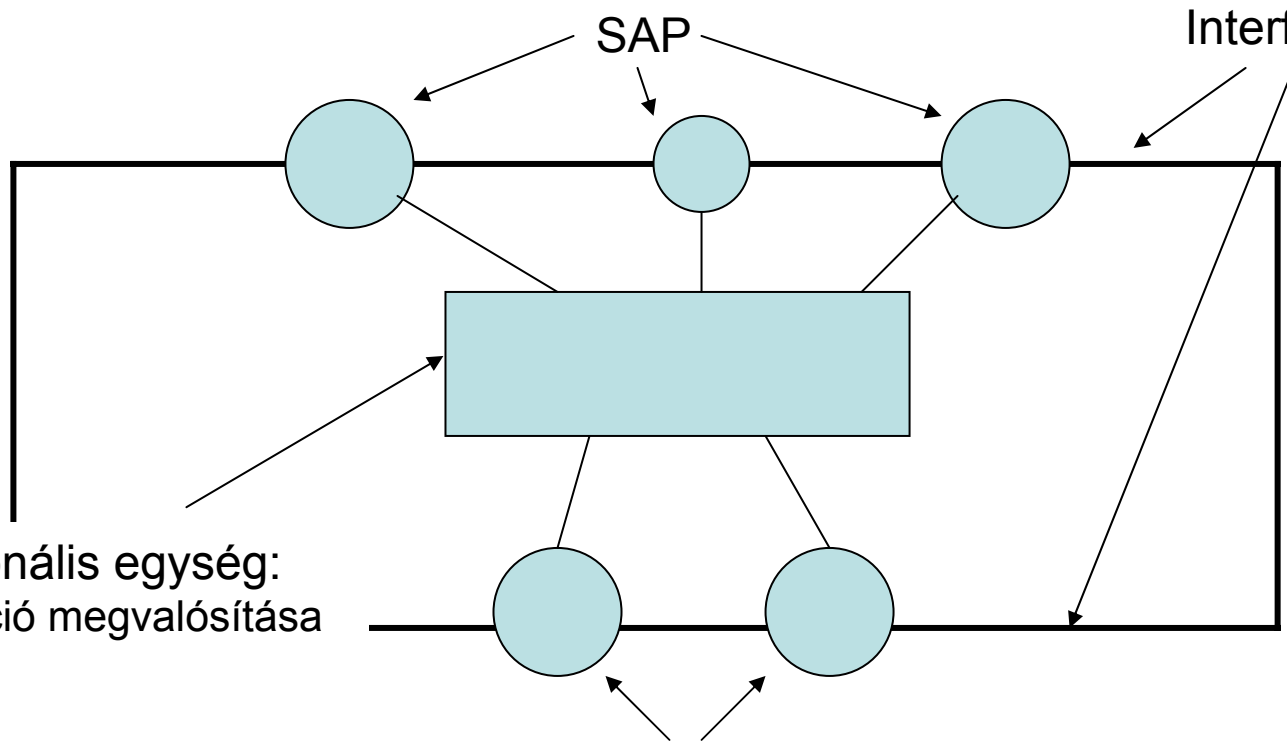
- Hálózati architektúra: **protokollrétegek egymásra épülése**
  - számítógép-architektúra, szoftverarchitektúra
- Referenciamodell
  - csak a rétegek és azok feladatai, **maguk a protokollok nem**
- Szabványosításig jutott el az ún. **OSI-referenciamodell**
  - OSI: az ISO-ban kidolgozott referenciamodell (1983)
  - ISO – International Standardization Organization
  - OSI – Open System Interconnection – nyílt rendszerek összekapcsolása
  - 7 feladatcsoport, 7 réteg
  - a protokollok nem részei az OSI-nak, de kidolgoztak és szabványosítottak protokollokat is az egyes rétegekhez

A rétegezett protokollarchitektúrák előnyei és hátrányai

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

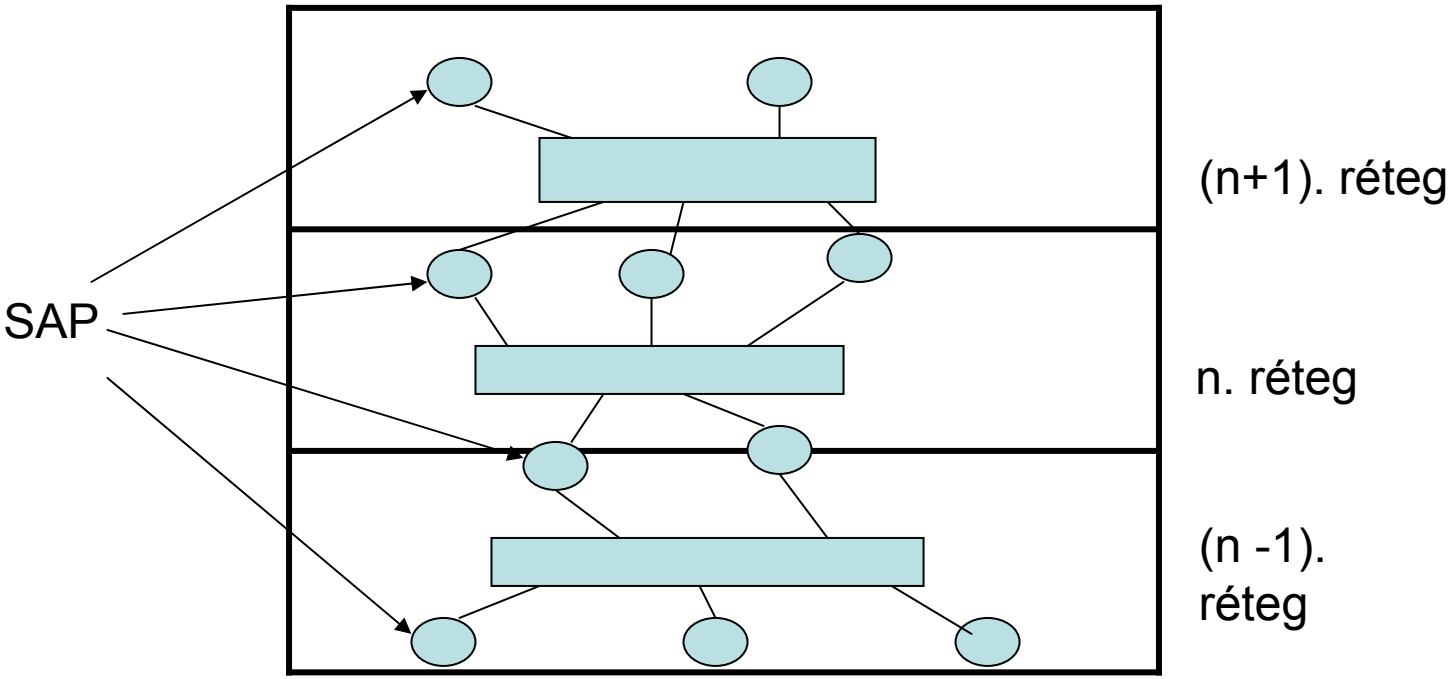
- Hátrány:
  - Adott réteg működéséhez szükséges információk egy másik rétegben → megsérül a rétegstruktúra
  - **Feladatok duplikálása** elkerülhetetlen
    - hatékonyság rovására megy (pl. hibavédelem több rétegben is)

A réteg elve

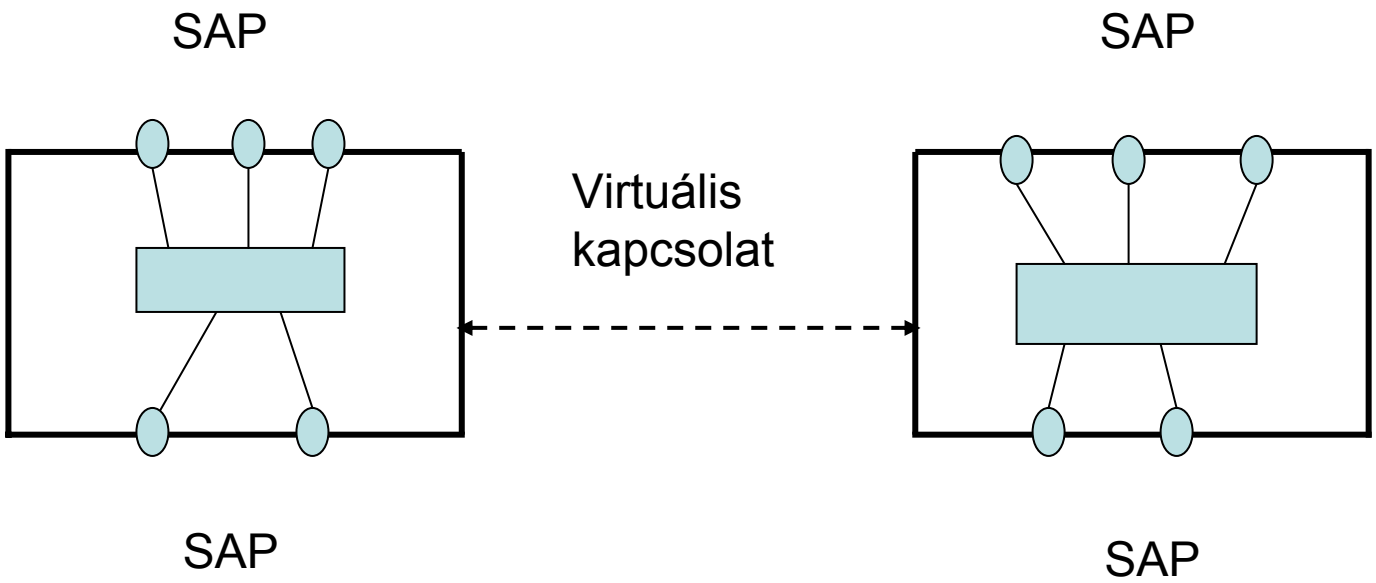


- Interfész-elv
- A megvalósítás elrejtése

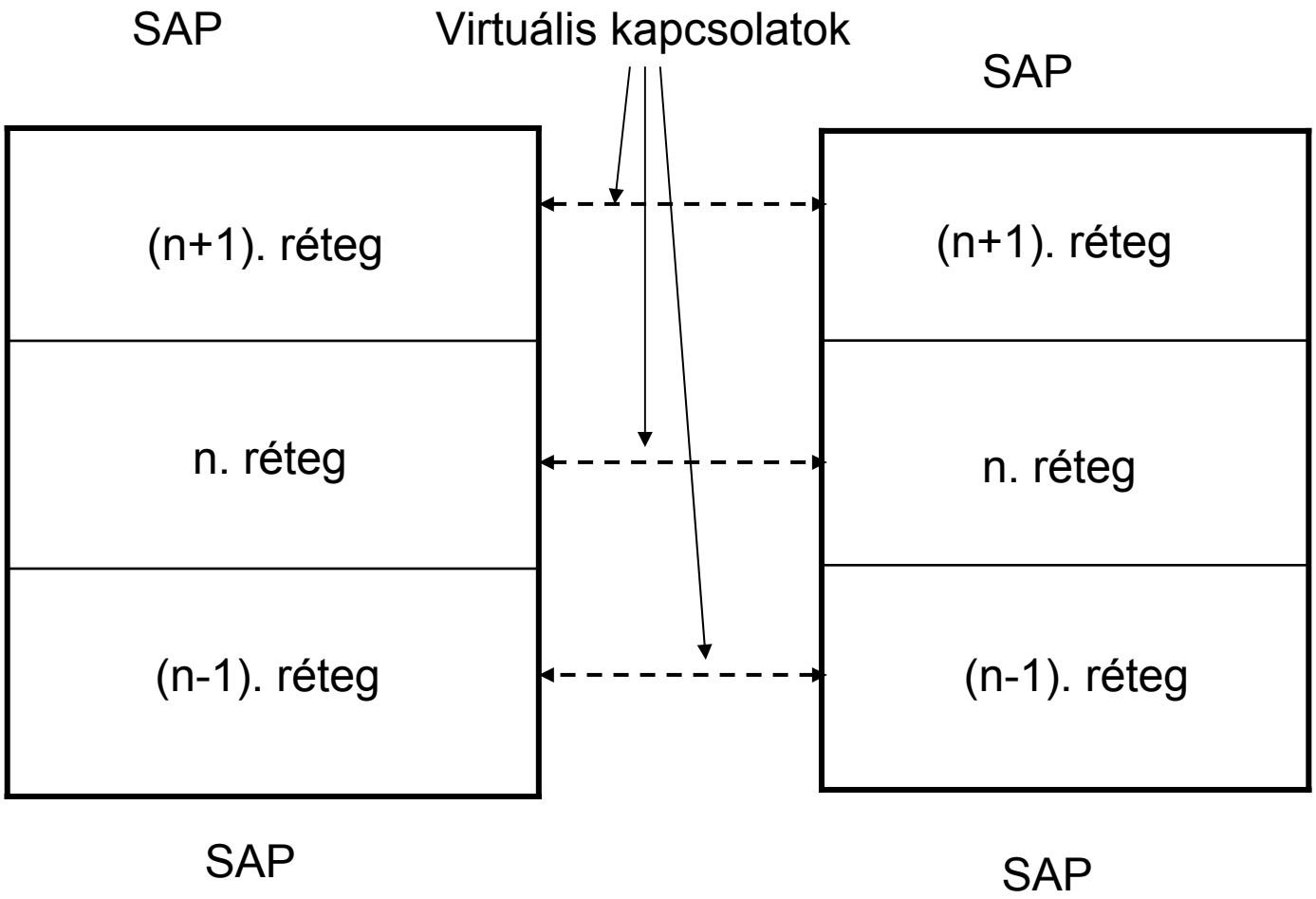
Rétegek



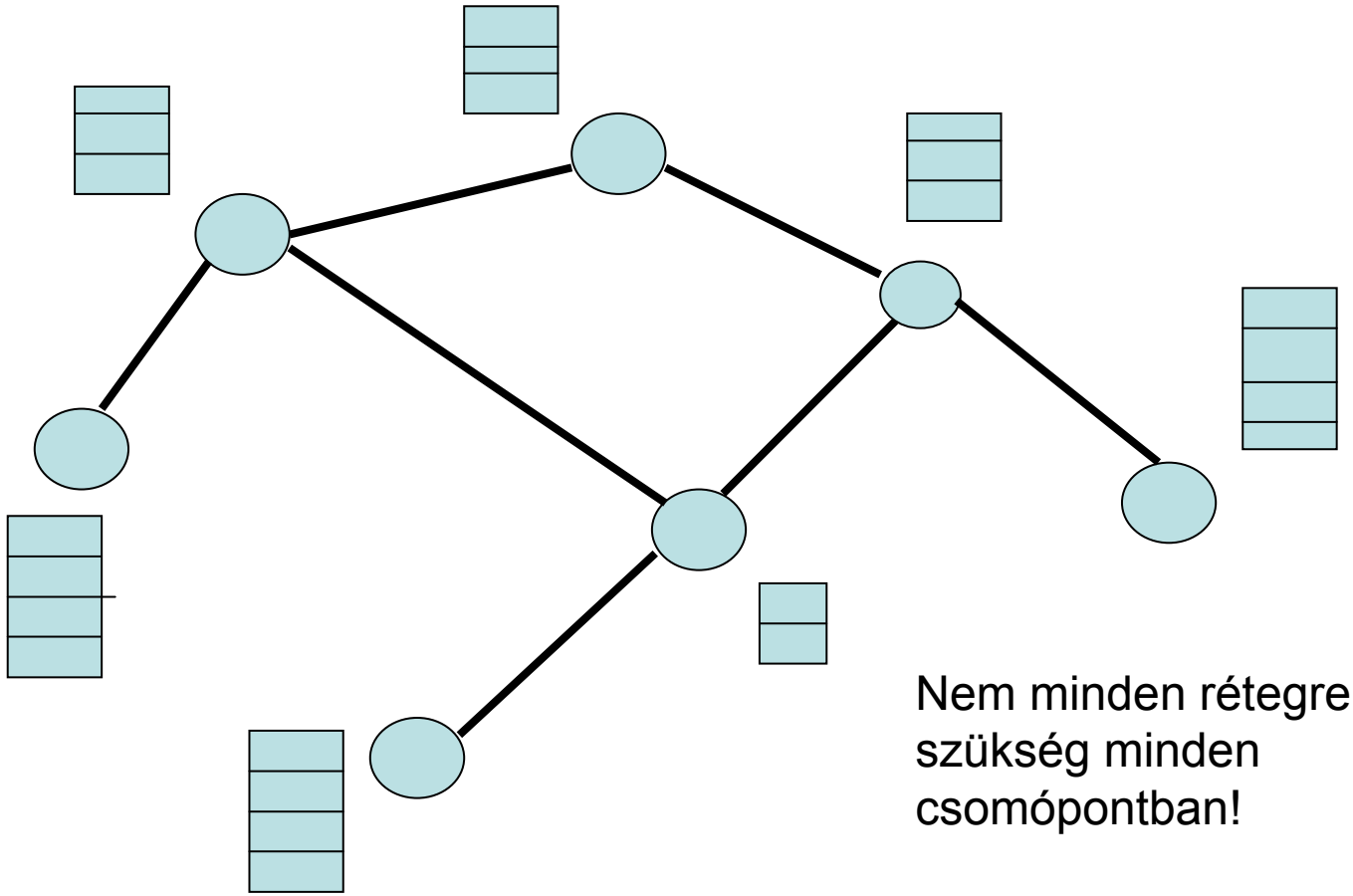
Kommunikáció azonos rétegek között



Protokollrétegek

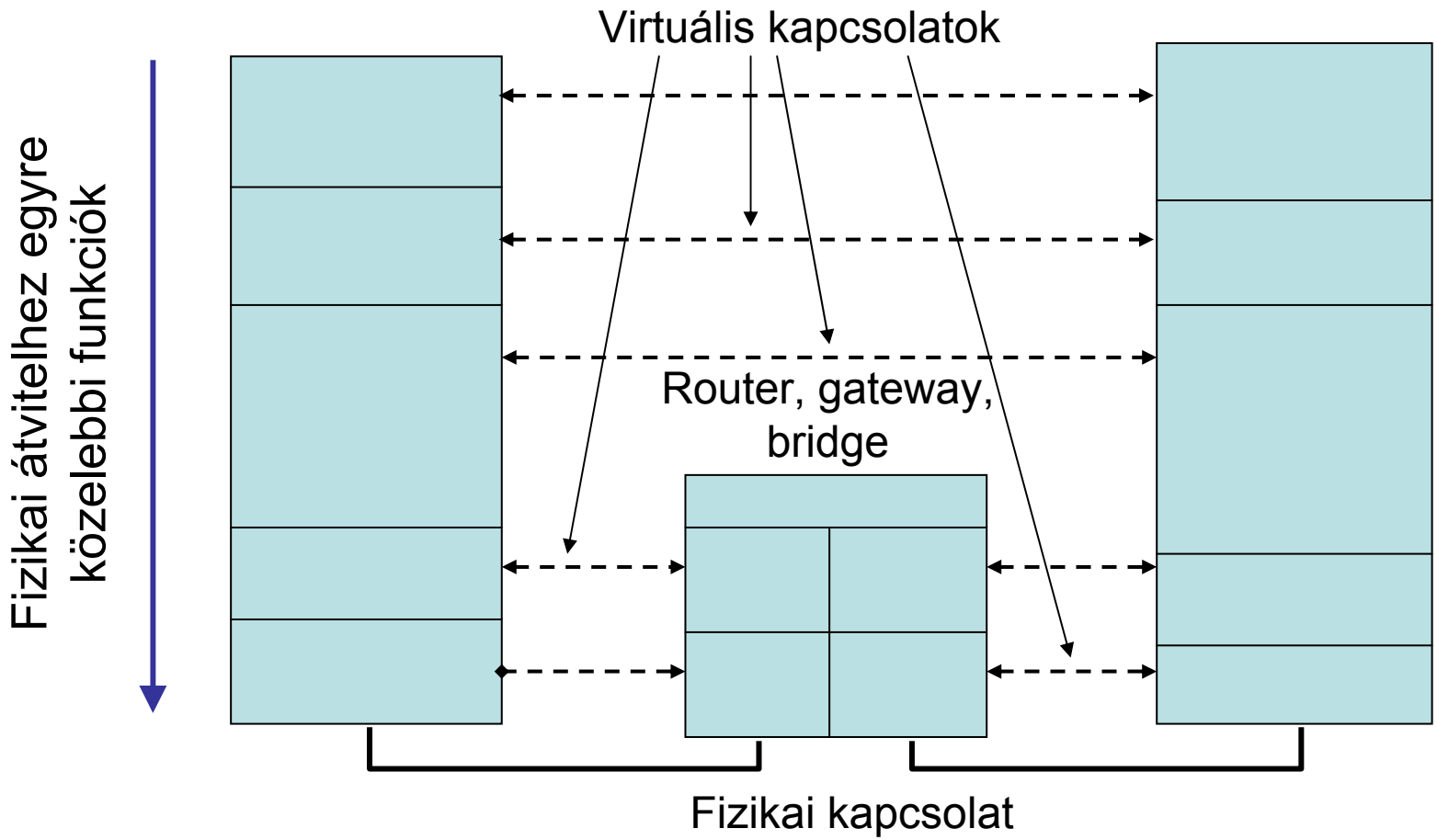


Protokollrétegek a hálózati csomópontokban

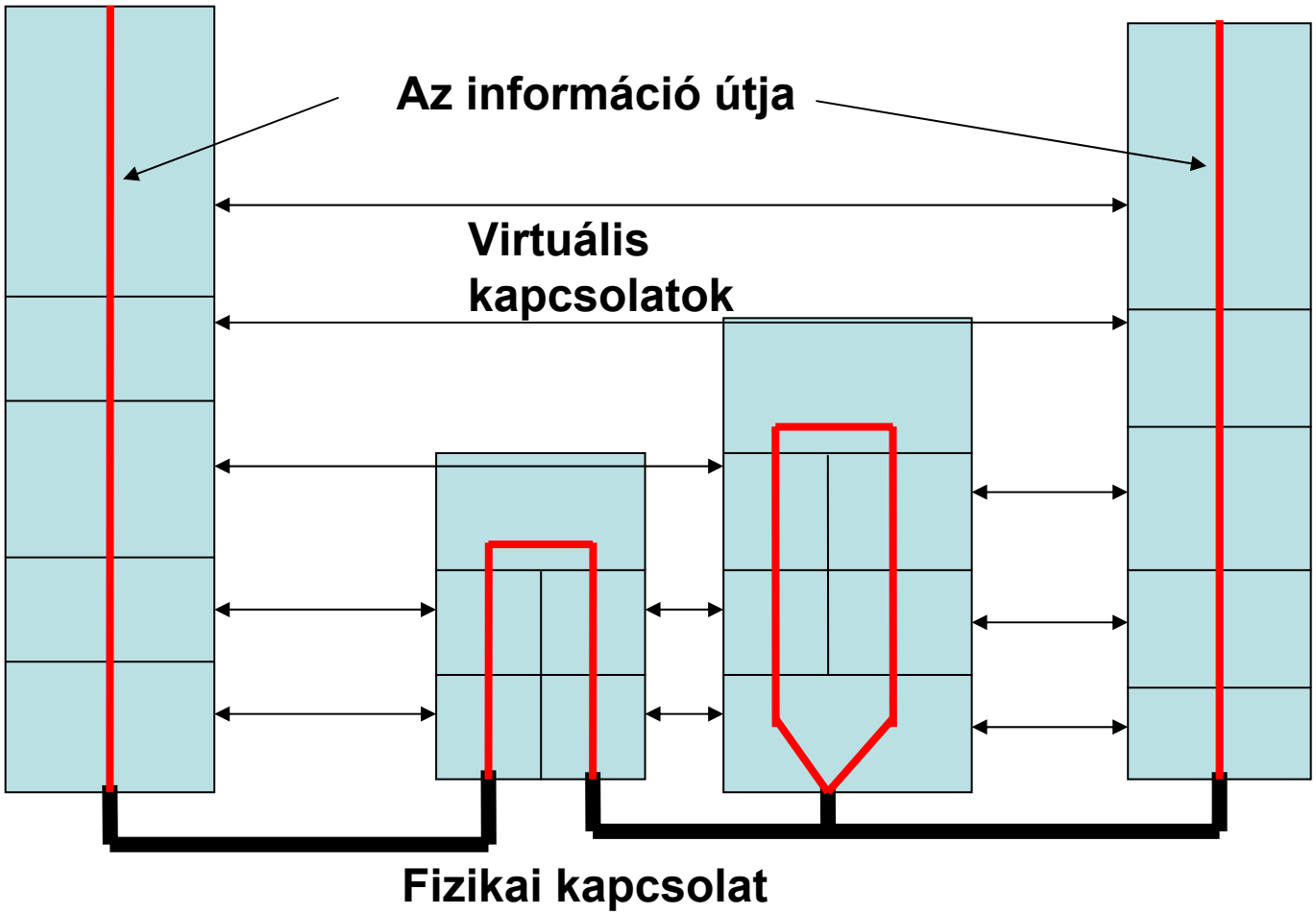


Nem minden rétegre van szükség minden csomópontban!

Protokollrétegek (1)

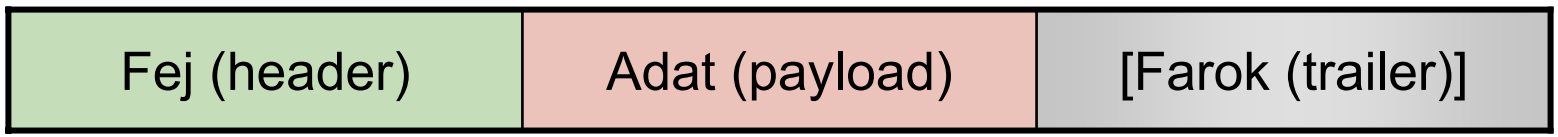


Protokollrétegek (2)



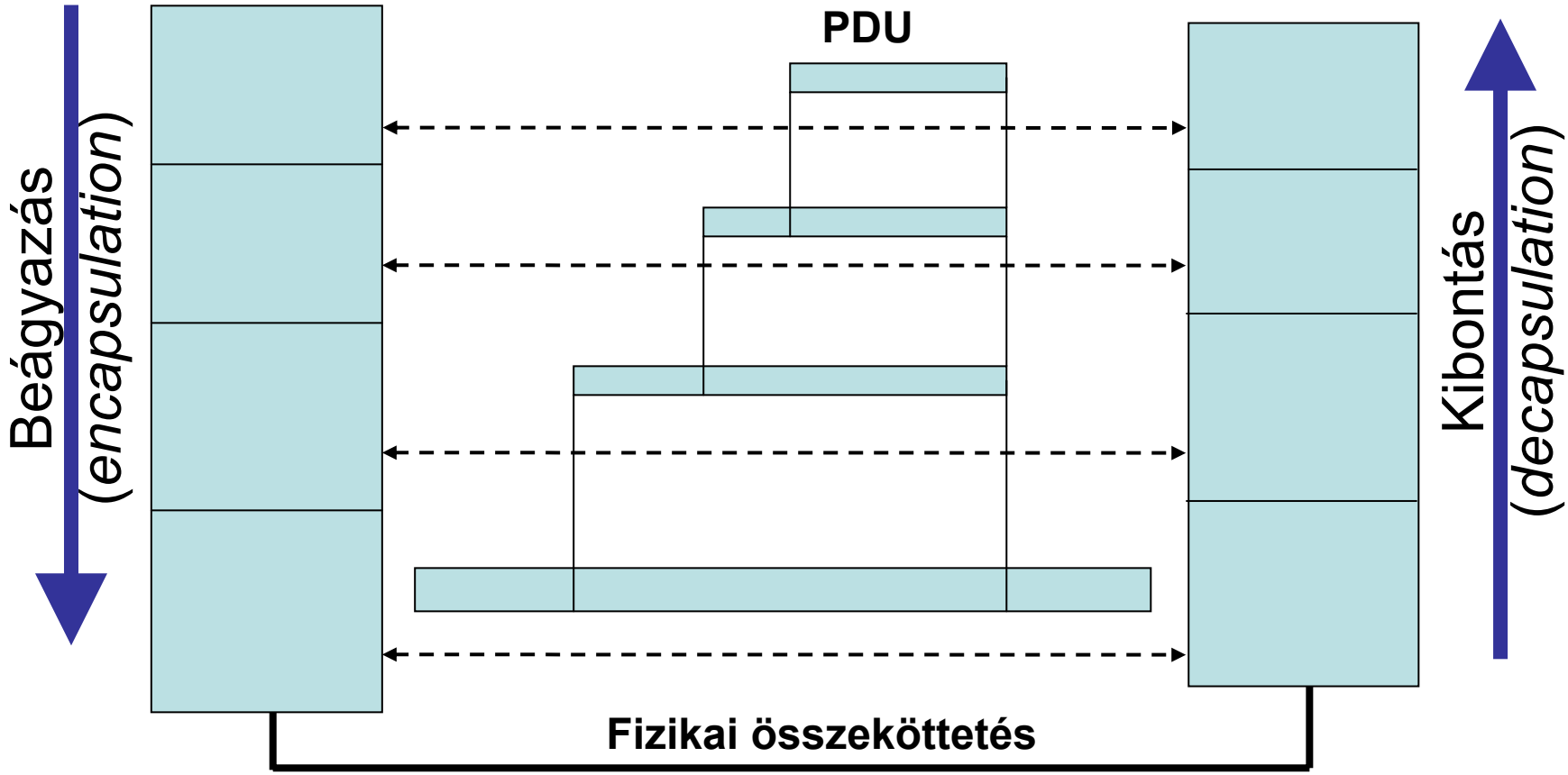
Protokoll-adategységek (PDU – protocol data unit)

- Ezek kerülnek továbbításra a szomszédos rétegek között
- A PDU-k általános felépítése, tartalma



- A fejrészben és farokrészben található kiegészítő információk:
  - Címek, sorszámok, hibavédelem, egyéb opcionális paraméterek

„Borítékolás” - beágyazás (encapsulation)



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

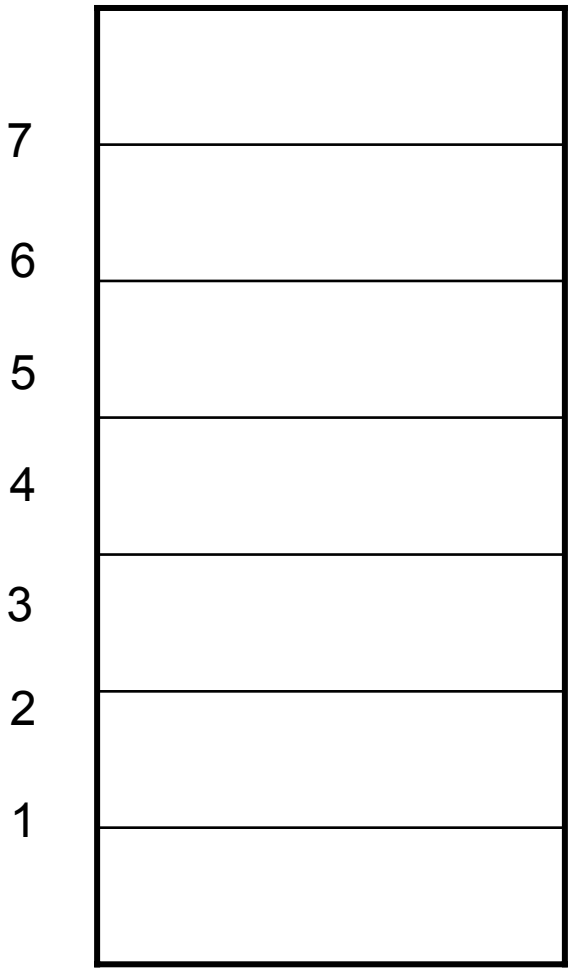
Service Data Unit (SDU)

- Olyan adategység, amelyet egy OSI réteg egy alsóbb rétegnek küld és amit az még nem borítékol egy PDU-vá
- Ezt kapja meg a vele virtuális kapcsolatban álló réteg
- Az n. réteg PDU-ja: az n-1. réteg SDU-ja
  - Vagyis az SDU a PDU payload-ja
- Az n-1.réteg fejlécet és farokrészt ad rá, ezzel lesz az n-1.réteg PDU-ja

ISO OSI referenciamodell

ISO - International Organization for Standardization

OSI - Open Systems Interconnection



- **Alkalmazási réteg (*Application layer*)**
- **Megjelenítési réteg (*Presentation layer*)**
- **Viszonyréteg (*Session layer*)**
- **Szállítási réteg (*Transport layer*)**
- **Hálózati réteg (*Network layer*)**
- **Adatkapcsolati réteg (*Data link layer*)**
- **Fizikai réteg (*Physical layer*)**

PDU elnevezések az OSI-modellben

- Szigorúan véve:
  - az adott réteg protokoll-adategysége
  - vannak/voltak „szabványos” elnevezések
    - 2. réteg: keret (*frame*)
    - 3. réteg: csomag (*packet*)
    - 4. réteg: szegmens (*segment*)
    - Feljebb (főként alk. réteg): üzenet (*message*)

- Az egyszerűség kedvéért gyakran: mindent „csomag”-nak nevezünk

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fizikai réteg

- A fizikai közeg specifikációja
  - pl. érintkezők kiosztása, használatos feszültség szintek, kábel specifikációk stb.
- Bitek, bitcsoportok továbbítása a fizikai csatornán
  - vonali kódolás: szimbólumreprezentáció
  - moduláció: vivő viszi át az információt
- Egyéb jelzések küldése a csatornára, ill. fogadása onnan
- Bitszinkronizáció végzése
- Csatlakozók típusának, méretének rögzítése

Adatkapcsolati réteg

- Bitsorozatok „keretezése”
  - Csomagok összeállítása
- Hibaellenőrzéshez szükséges adatok előállítása, vétel esetén ellenőrzése, esetleg javítása
- Adatkapcsolati címek kezelése (MAC címek)
- Közeghozzáférés vezérlése (Media Access Control)
- Forgalomszabályozás itt is lehet (manapság ritkán)
- Tipikusan itt működik: bridge, switch

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fizikai-Adatkapcsolati összehasonlítás

- Fő különbség:
  - fizikai: egy készülék interakciója a fizikai médiummal
  - Adatkapcsolati: több készülék interakciója egy osztott médiummal

- Fizikai megmondja:
  - a készülék hogyan adjon a médium felett és egy másik készülék ezt hogyan fogadja
  - De nem mondja meg hogyan férjen a médiumhoz!

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hálózati réteg

- Egyedi linkek logikai összefűzése végpontok közötti csatornává
  - Akár több hálózaton át
  - Meghatározott QoS-t biztosítva a felsőbb rétegnek
- Logikai címzés: hálózati eszközök közötti kapcsolásokhoz
- Útvonalkeresés a hálózaton belül
- Forgalomirányítás, csomagjavítás
- Tipikusan itt működnek: útvonalválasztók

Adatkapcsolati-Hálózati összehasonlítás

- Adatkapcsolati: **fizikai címzés**
  - MAC címek: gyártó fixen
- Hálózati: **logikai címzés**
  - hálózattervező határozza meg az értékeket

- Adatkapcsolati réteg egy hálózaton belül teremt kapcsolatot, hálózati réteg több hálózaton át!

Szállítási réteg

- **Végpontok közötti megbízható kommunikáció**

- A hálózati réteg „nyers” csomagtovábbítása felett:
  - Hibamentes összeköttetés létrehozása:
    - Hibás csomagok ismétlése
    - Duplikált csomagok eldobása
    - Csomagsorrend helyreállítása
  - Forgalomszabályozás
  - Alkalmazások adatfolyamainak multiplexálása

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Szállítási réteg analógia

- Posta: kiküldi és rendszerezi a leveleket, csomagokat
- Megbízható szolgáltatást nyújt: nem veszhetnek el levelek következmények nélkül
- Viszont: csak a borítékát látja a levélnek, a tartalmát nem

Viszonyréteg

- Kapcsolat irányának kezelése
  - Duplexitás kezelése
- Összeköttetés kezelése
  - Kapcsolat felépítése, lebontása
- Adatfolyam-szinkronizáció
  - az összefüggő adatfolyamok összehangolása
- Manapság: általában a szállítási rétegben implementálják

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Duplexitás

- Duplex: kétirányú kommunikáció a két fél között
  - Pl. telefónia (mobil, vezetékes), távfelügyelet
  - Frekvenciaosztás, Full-duplex Ethernet
- Szimplex: egyirányú
  - Broadcast
  - Rakétavezérlés
  - Sputnik1, Pioneer 6
- Félduplex: kétirányú, de nem lehet egyszerre használni
  - Pl. Walkie-Talkie
  - Lehetnek allokált időrések is

Full duplex előnyei

- Nincs ütközés: nem kell újraadni
- Nagyobb adatátviteli ráta
- A kommunikáló feleknek nem kell várni egymásra: kisebb késleltetés

- Ha meg kell osztani a fizikai médiumot: emulált full duplex
  - Idő osztásban (TDD): igazából fél-duplex csatorna
  - Frekvencia osztásban (FDD)
  - Előny-hátrány?

Megjelenítési réteg

- Míg az előző rétegek a fejben lévő meta-adatokat kezelik, ez a réteg a felhasználói adatokat
- Adatábrázolás
  - az átvitt felhasználói információ szintaktikai ellenőrzése
    - „Syntax réteg”
  - szükség szerinti konvertálása
    - adatábrázolás
    - operációs rendszer miatti különbségek
- Adattömörítés
- Adattitkosítás
- Általában az alkalmazási rétegben van megvalósítva

Alkalmazási réteg

- A végpontokon futó alkalmazási programok
- Felhasználják az alsóbb rétegek szolgáltatásait, ők maguk csak a felhasználót szolgálják ki

- Fő feladatai:
  - kommunikációs partnerek azonosítása, elérhetősége
  - hálózati erőforrások elérhetősége
  - szinkronizáció a felhasználók között
  - formátum, biztonsági egyeztetés
- Implementációi: HTTP, FTP, SMTP

Az OSI referenciamodell szerepe, jelentősége

- Architektúraként nem valósult meg teljesen soha, és ma már a legtöbb OSI-protokoll sincs használatban

- Referenciamodellként továbbra is hasznos
  - a különböző létező architektúrák megértéséhez, bemutatásához
  - mintegy „mérőléc”-ként használva

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

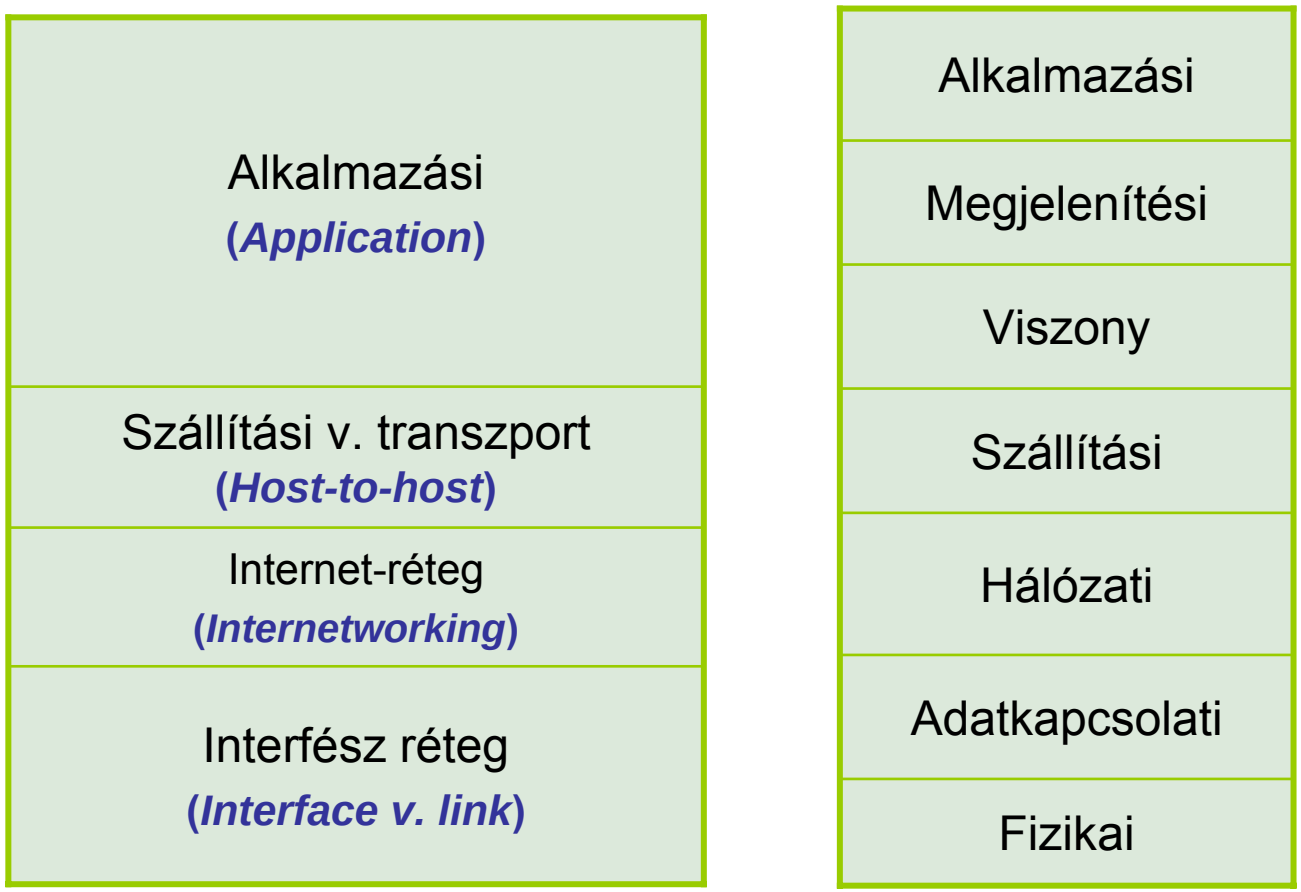
Nem OSI-szerinti protokollarchitektúrák

- OSI: túl sok réteg a felső szinteken
  - *TCP-IP architektúra*
    - *Transmission Control Protocol – Internet Protocol*
- OSI: túl kevés réteg az alsó szinteken
  - *IEEE (PAN) – **LAN** – (MAN) architektúra*
    - *(Personal – Local – Metropolitan Area Networks)*

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

1.példa: a TCP/IP protokoll-architektúra

- Rétegek és viszonyítás az OSI modellhez



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

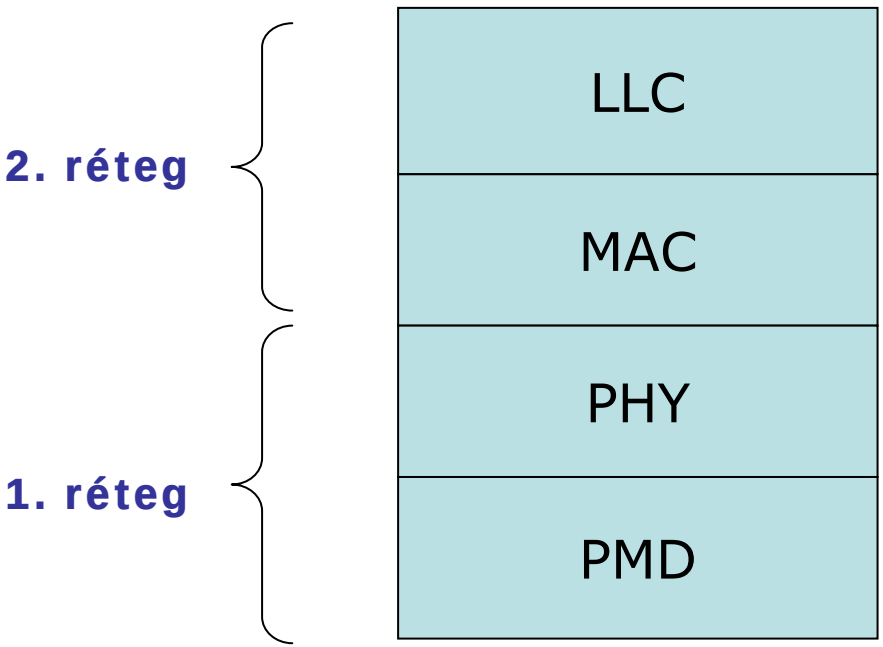
TCP/IP protokoll-architektúra

- RFC 3439 kimondja: „A rétegezés károsnak tekinthető!”
- Az IETF által koordinált protokoll-architektúra
- Már az OSI modell előtt használták, Internet világát tükrözi
  - Összeköttetésmentes csomagkommunikáció
- A protokolloknak nem kell megfelelni szigorúan rétegeknek, hogy el legyenek fogadva szabványként
- Az operációs rendszerek többsége mind TCP/IP-t használ

2. példa: az IEEE szerinti LAN-architektúra

IEEE – Institution of Electrical and Electronic Engineers
802-es szabványosítási bizottság

OSI



Logical Link Control
(Logikai adatkapcsolat-vezérlés)

Medium Access Control
(Közeghozzáférés-vezérlés)

Physical
(Fizikai)

Physical Medium Dependent
(Fizikaiközeg-függő)

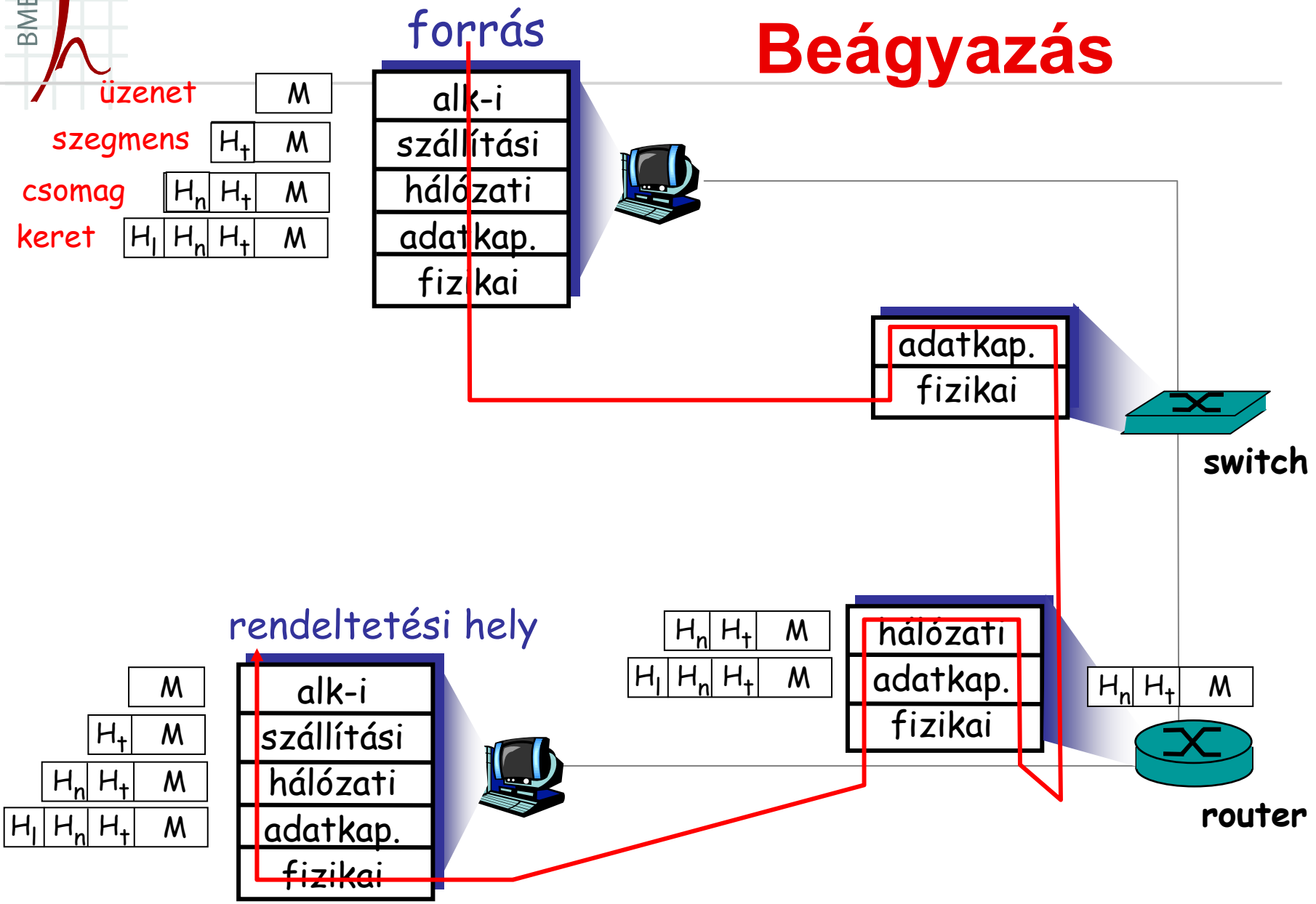
© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A gyakorlatban jól használható kombinált referenciamodell

[Tanenbaum: Számítógép-hálózatok],
[Kurose-Ross: Computer Networking]

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

Beágyazás


forrás
üzenet
M
szegmens
H_t M
csomag
H_n H_t M
keret
H_l H_n H_t M
alk-i
szállítási
hálózati
adatkap.
fizikai
adatkap.
fizikai
switch
rendeltetési hely
M
H_t M
H_n H_t M
H_l H_n H_t M
alk-i
szállítási
hálózati
adatkap.
fizikai
H_n H_t M
H_l H_n H_t M
hálózati
adatkap.
fizikai
H_n H_t M
router

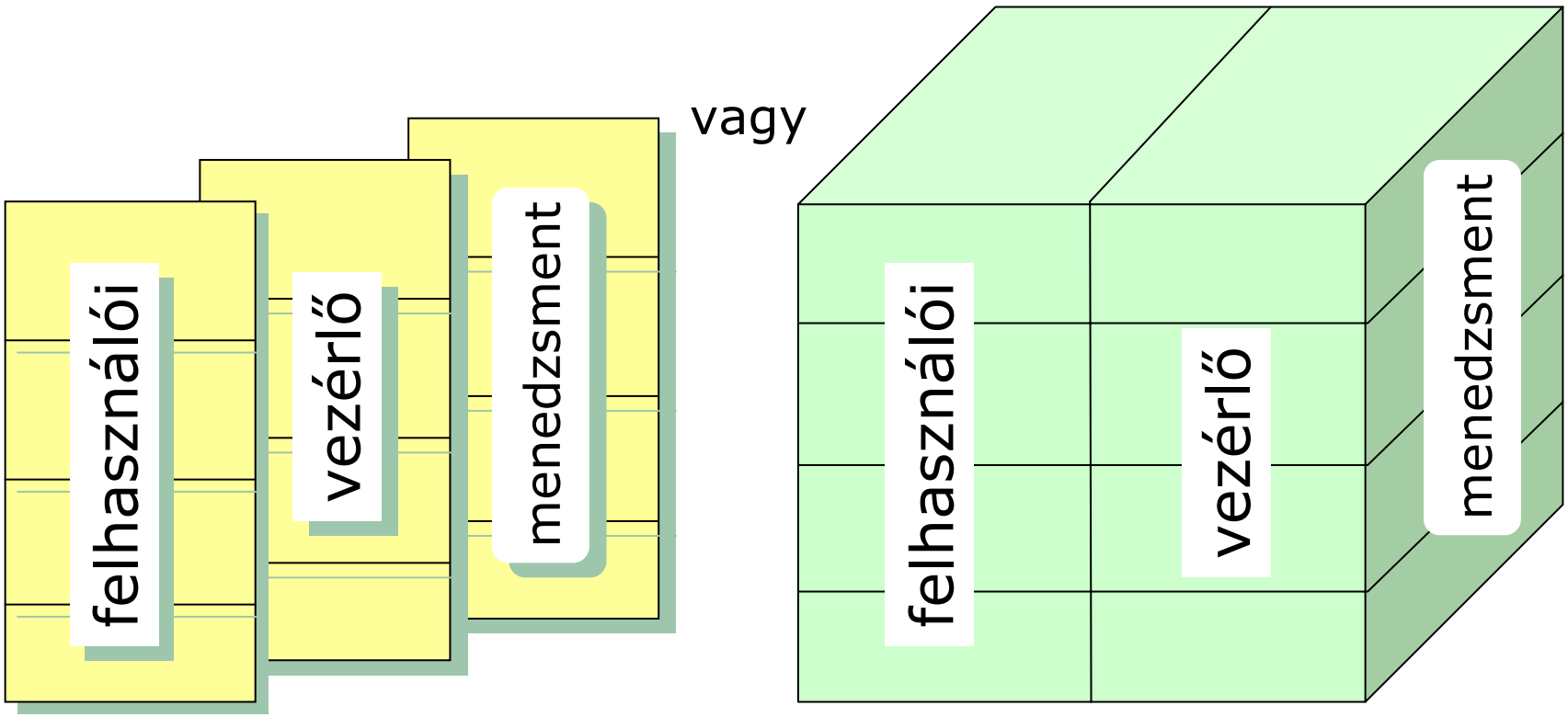
„Többsíkú” architektúrák

- Bizonyos feladatok egymásra épülnek, de vannak eltérő jellegűek
  - pl. az adatforgalom és a forgalomszabályozás
- Feladatcsoportok:
  - *felhasználói információ továbbítása*
  - *a felhasználói információ továbbításához szükséges ismeretek cseréje*
  - *a felhasználói információ továbbítására való képesség fenntartása, ellenőrzése*
- Felhasználói-, vezérlő- és menedzsment feladatcsoportok → „síkok”

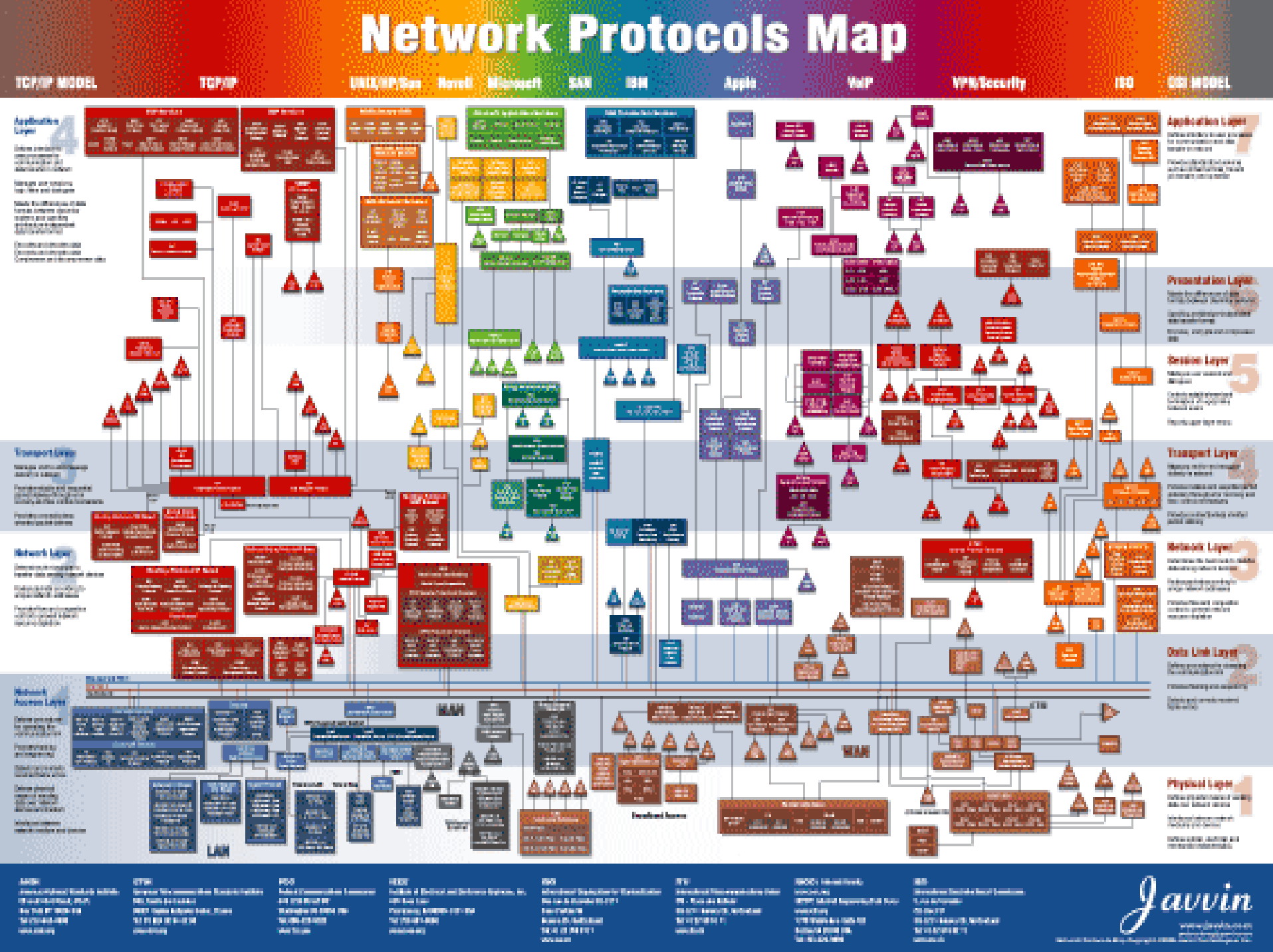
© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A háromsíkú protokollarchitektúra

- Mint egy épület …

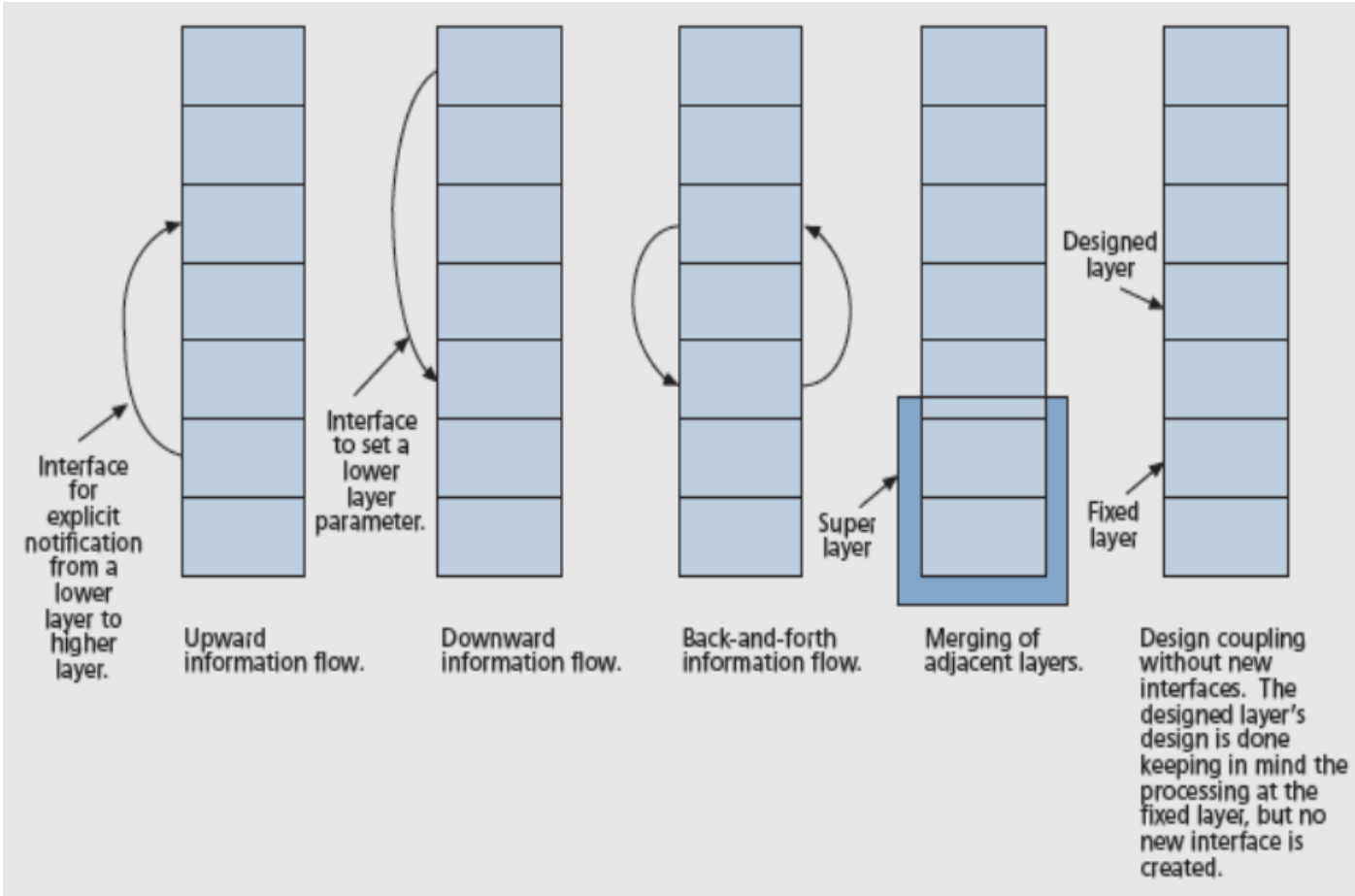


Network Protocols Map



Cross-layer megközelítés

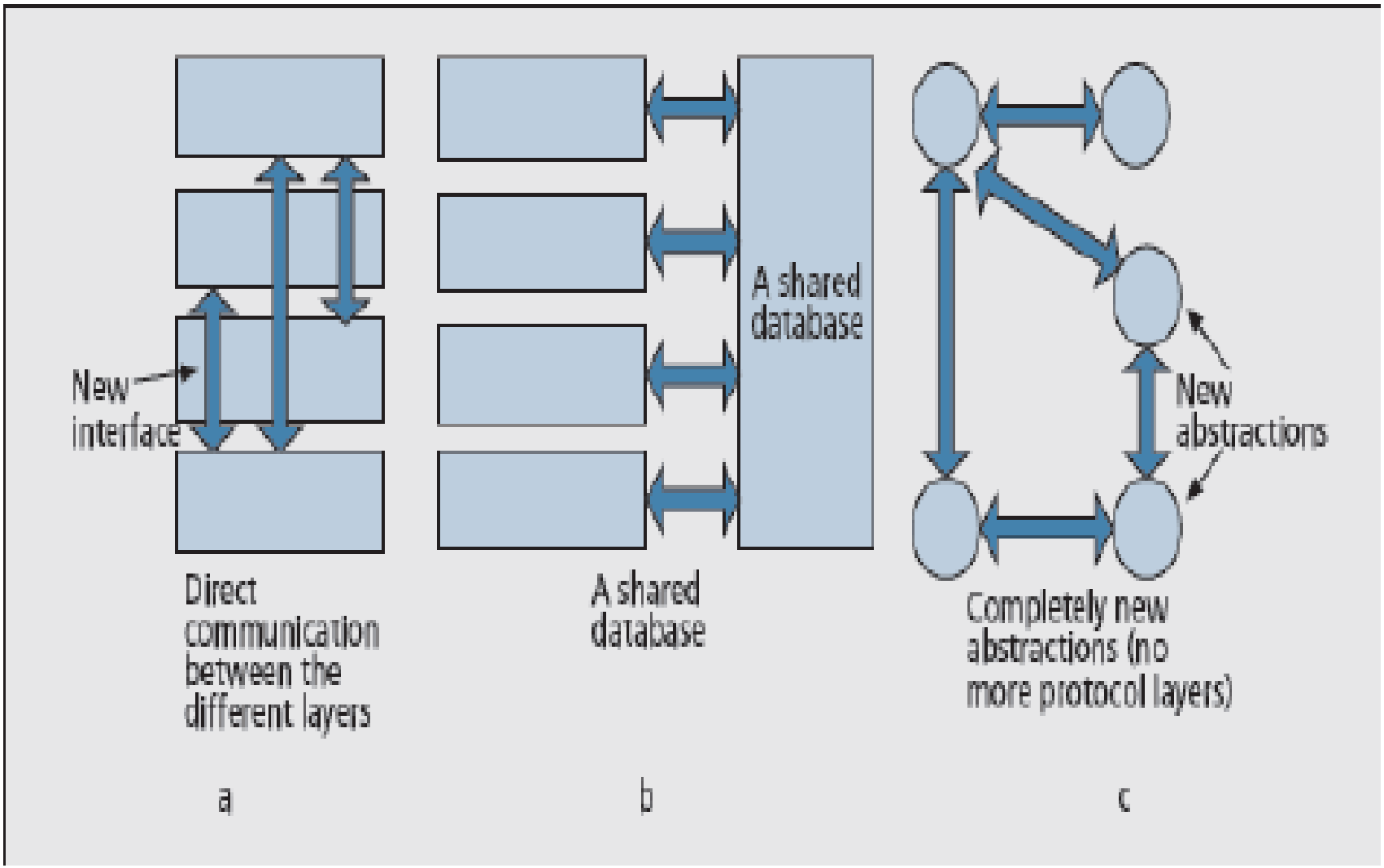
- Rétegezés: nincs közvetlen kommunikáció a nem-szomszédos rétegek között
- Cross-layer ezt az elvet sérti meg!



Cross-layer példák

- Infó felfelé:
  - TCP nem tudja megkülönböztetni, hogy hibás csomagok vagy torlódás miatt van-e a csomagvesztés
  - Mondja meg ezt a szállítási rétegnek az alsóbb réteg
- Infó lefelé:
  - Alkalmazási réteg megmondja a fizikai rétegnek, hogy milyen késleltetést vár el

Megvalósítás



Összefoglalás

- Protokollarchitektúra
  - rétegek, rétegek közötti kommunikáció, adategységek, beágyazás
- Az OSI referenciamodell
- Protokollarchitektúrák
  - TCP/IP
  - IEEE
- Többsíkú modellek

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A következő anyagrész:

Fizikai szintű kommunikáció

(most már mondhatjuk így is: fizikai rétegbeli kommunikáció)

2013.február 19.

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

„FIZIKAI SZINTŰ” KOMMUNIKÁCIÓ 1.

Bitfolyamok továbbítása hírközlő csatornákon

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.február 21.

Az anyag beosztása (1)

- Bevezető áttekintés, hálózatok és rendszerek példái.
- Alkalmazások és szolgáltatások. Követelmények a hálózattal szemben.
- Protokollarchitektúrák, referenciamodellek.
- A fizikai szintű kommunikáció alapjai.

Gyakorlat.

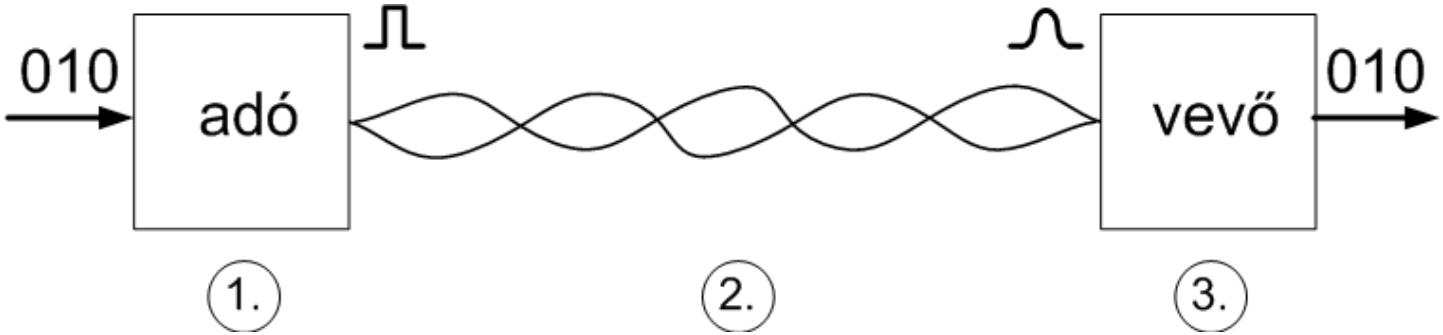
- Többszörös hozzáférés.
- LAN-ok, LAN-ok összekapcsolása.
- BWA (WPAN, WLAN, WMAN).

Gyakorlat.

- Áramkörkapcsolás, csomagkapcsolás, hívásvezérlés, címzés.
- Routing.
- Ütemezés.
- IP.

Gyakorlat.

Mi az, hogy „fizikai szintű” átvitel?



- A hálózatnak az a funkcionalitása, amely két csomópont között szimbólumok (bitek) továbbításával foglalkozik.
- *Az adó a **szimbólumok**at **jelalakok**kal reprezentálja.*
- Ezek kerülnek továbbításra a kommunikációs csatornán.
- A továbbítás során **torzulnak** és **zajok, zavarok** adódnak hozzájuk.
- A vevő feladata: a vett jelet kiértékelve, a kapott szimbólumsorozat a lehető legjobban megfeleljen az adó által küldött sorozatnak.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Miről lesz szó ebben a részben?

- **Bitfolyamok továbbítása hírközlő csatornákon**
  - *Alapfogalmak*
  - *Átvitel sávhatárolt csatornán*
  - *Átvitel zajos csatornán*
- **Digitális modulációs eljárások**
  - *ASK, FSK, PSK*
- **Többcsatornás átvitel multiplexeléssel**
  - *FDM, TDM*
- **Hírközlő csatornák a gyakorlatban**
  - *(Réz)vezetékes csatornák*
    - *Sodrott érpáras kábelek, strukturált kábelezés*
    - *Koaxiális kábelek*
  - *Fényvezetős (üvegszálas) csatornák*
  - *Vezeték nélküli csatornák*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Szimbólumok átvitele hírközlő csatornán: alapfogalmak

- ***bit, bitsebesség*** (információátviteli sebesség) – bit/s
- ***szimbólum, szimbólum-sebesség, jelzési sebesség*** – baud, Bd
- ***összefüggés a bitsebesség és a szimbólum-sebesség között:*** hány bitnyi információt hordoz egy szimbólum?
  - *Bináris jelátvitel esetén: a két sebesség megegyezik.*
  - *Többszintű jelátvitel esetén: a bitsebesség többszöröse lehet a jelzési sebességnek.*
  - *Pl. 4-szintű impulzusoknak bitpárokat lehet egyértelműen megfeleltetni:*
    - *1. szint: 00*
    - *2. szint: 01*
    - *3. szint: 10*
    - *4. szint: 11*

    tehát kétszerese a jelzési sebességnek a bitsebesség.

    Példa: telefonos modem, 2400bit/s, 600 baud

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Növelhetjük-e tetszőlegesen a szintek számát?

- Elvileg igen, de

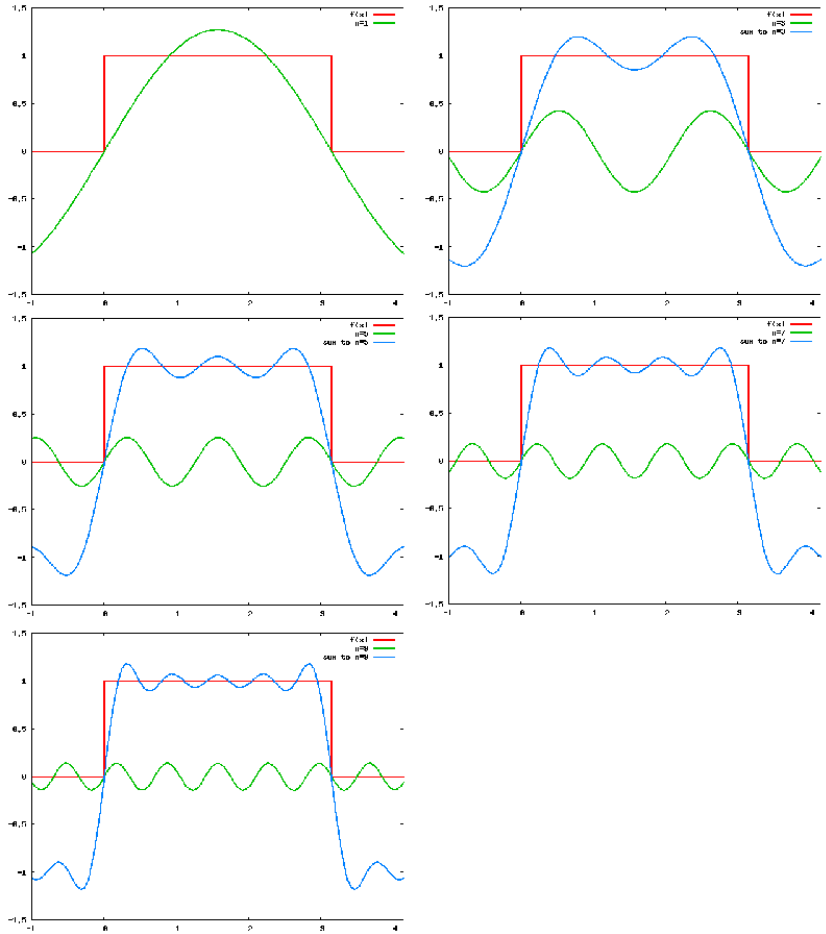
  a gyakorlatban a csatornák
  - ***sávkorlátozottak**, ezért torzítják, elkenik a jeleket*
  - ***zajok és zavarok forrásai**: döntéskor hibákat okoznak*

- Minél több szint: annál kisebb a „távolság” a szomszédos szintek között, és annál nagyobb az esély a tévesztésre

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fourier-sorfejtés*

Négyszögjel közelítése szinuszos hullámokkal



•Minden periodikus függvény: előállítható szinuszos és koszinuszos függvények összegekként

• A legkisebb összetevő frekvenciája megegyezik az eredeti jel ismétlődési frekvenciájával

•Az egyes összetevők frekvenciája ennek az alapfrekvenciának egész számú többszöröse

*:nem lesz számonkérve

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fourier-sorfejtés matematikája*

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty}[a_n \cos(n2\pi f_0 t) + b_n \sin(n2\pi f_0 t)] = \frac{a_0}{2} + \sum_{n=1}^{\infty}[a_n \cos(n\omega_0 t) + b_n \sin(n\omega_0 t)]$$

Ahol

T_0 jelenti a függvény periódus idejét,

$f_0 = \frac{1}{T_0}$ a periodikus jel alapharmonikusa,

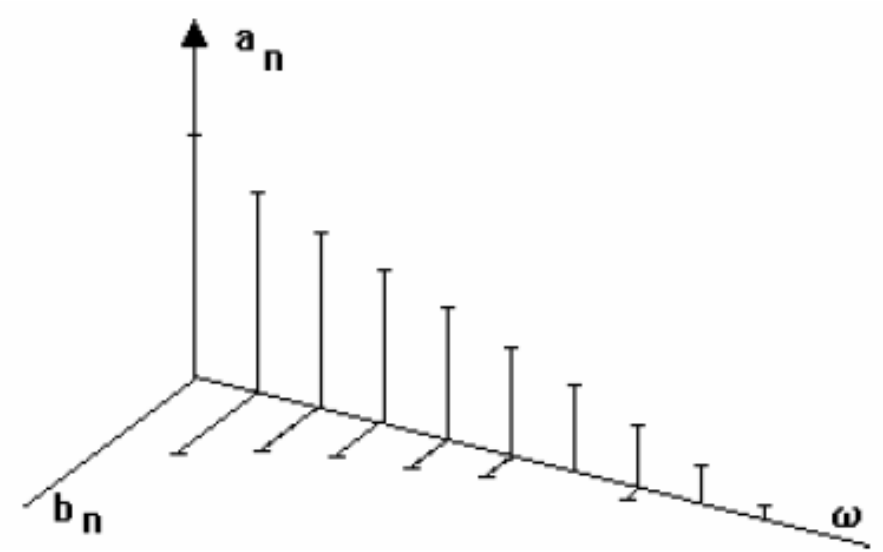
$\omega_0 = \frac{2\pi}{T_0}$ a periodikus jel alap körfrekvenciája.

Az egyes együtthatók az alábbi módon határozhatók meg:

$$a_0 = \frac{1}{T_0}\int_{-\frac{T_0}{2}}^{\frac{T_0}{2}} f(t)dt \qquad a_n = \frac{2}{T_0}\int_{-\frac{T_0}{2}}^{\frac{T_0}{2}} f(t)\cos(n\omega_0 t)dt \qquad b_n = \frac{2}{T_0}\int_{-\frac{T_0}{2}}^{\frac{T_0}{2}} f(t)\sin(n\omega_0 t)dt$$

Fourier-sorfejtés*

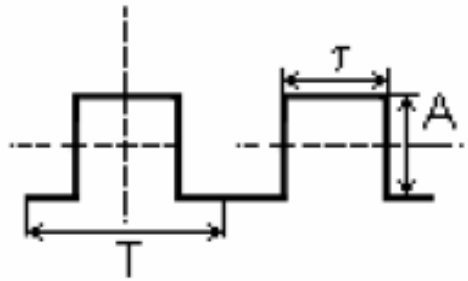
- Folytonos, periodikus időfüggvényekhez egy sorozat pár rendelhető, és egyben megadható az oda-vissza transzformáció is
- A sorozatok frekvenciákhoz köthetők, tehát az idő (t) tartományból itt lehet áttérni az ω illetve az f tartományba



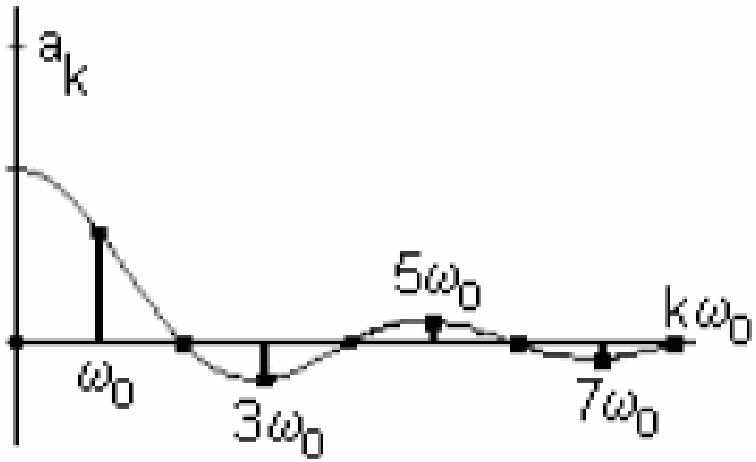
Négyszögjel esetén*

- Csak koszinus összetevők (ha origóhoz képes szimmetrikus):

$$a_k = \frac{2}{T}\int_{-\frac{\tau}{2}}^{\frac{\tau}{2}} A\cos\left(\frac{2\pi}{T}kt\right)dt$$



- Frekvenciaspektrum felharmonikusokból:

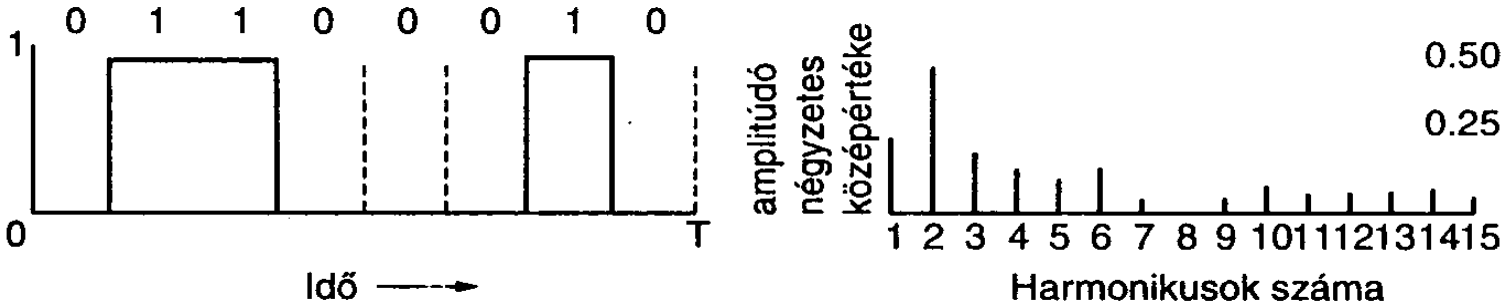


© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

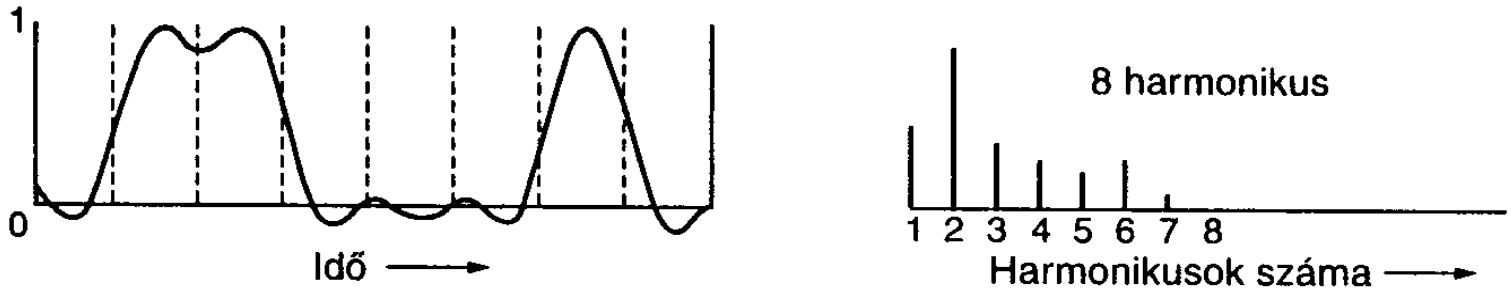
Négyszögjelek átvitele sávhatárolt csatornán

Fourier-sorfejtés:
tagjai a „harmonikusok” (alap- és felharmonikusok)

Eredeti jel (nem sávhatárolt csatorna)



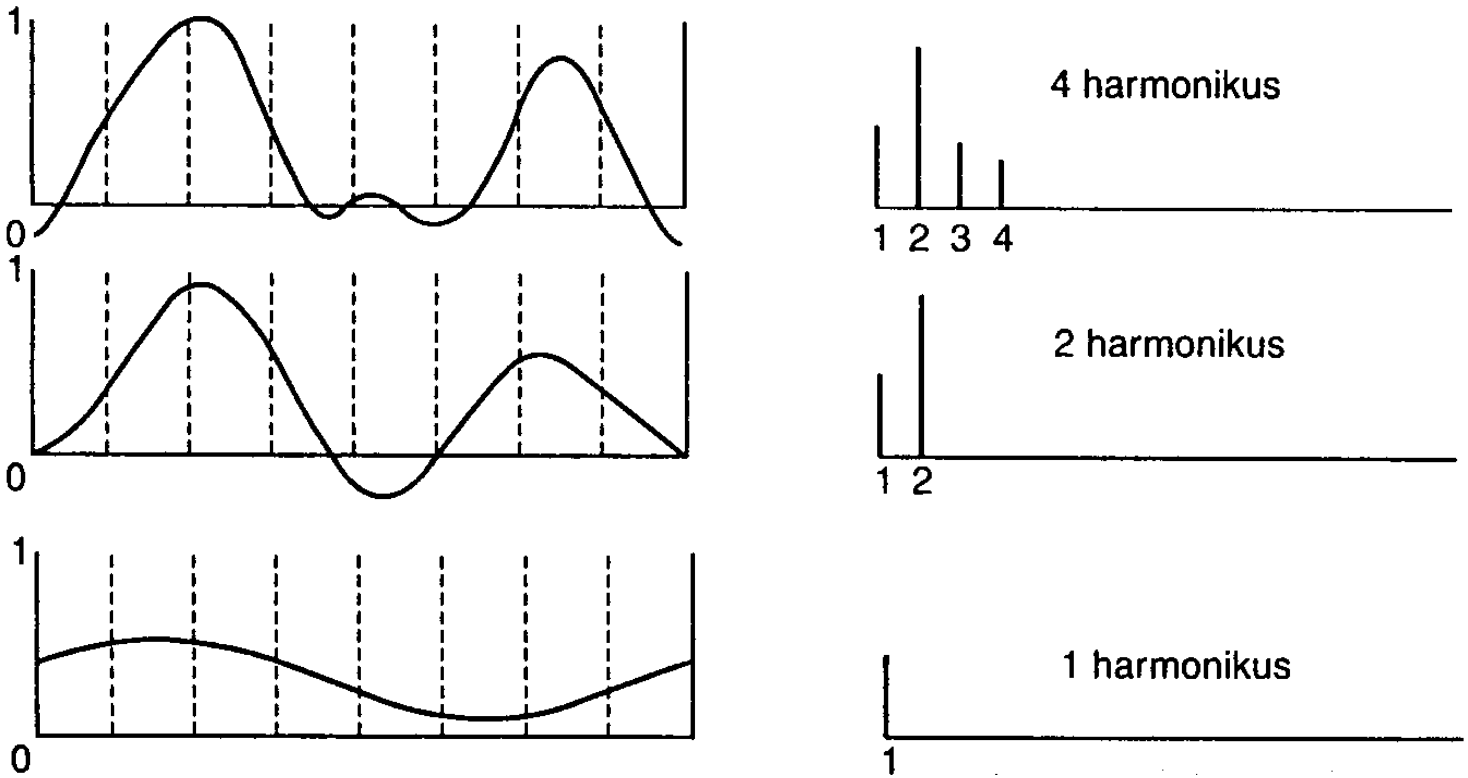
Sávhatárolt csatorna (csak 8 harmonikus)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Négyszögjelek átvitele sávhatárolt csatornán

Diszperzív csatorna

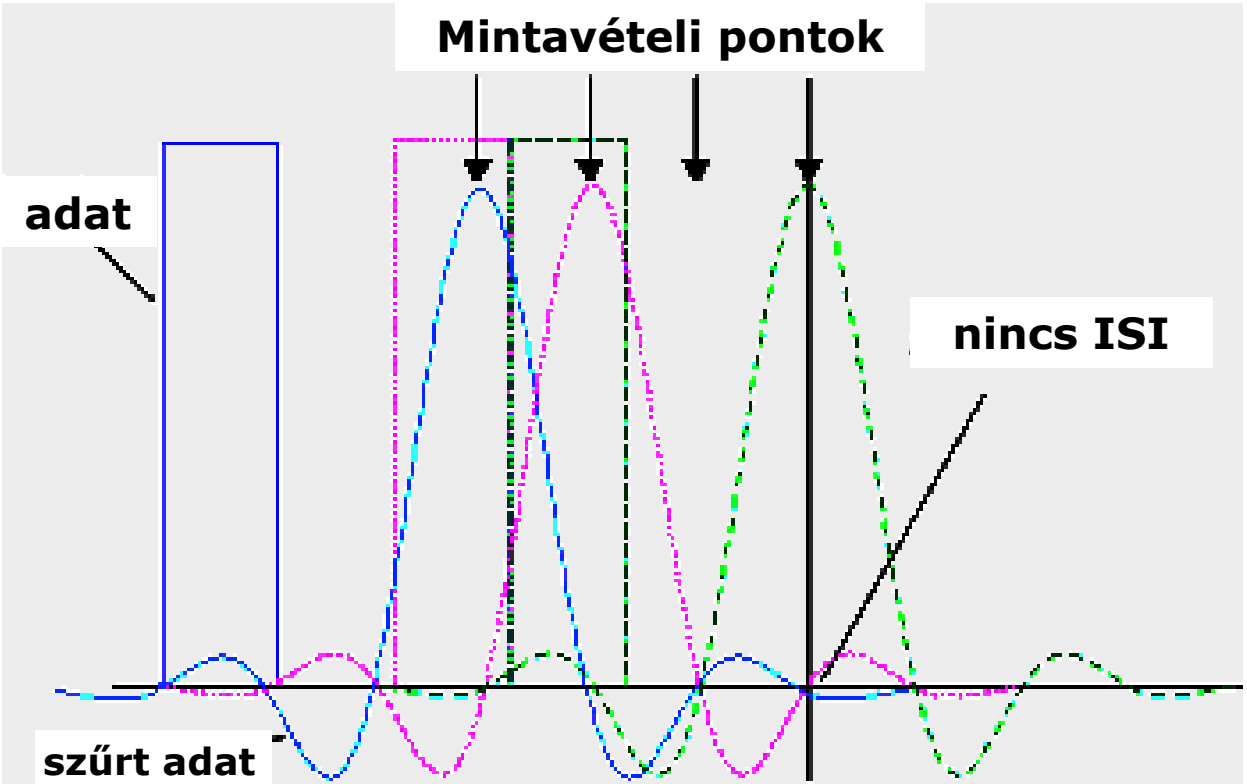


Mekkora sávszélességre van szükség a jel átviteléhez?

- Mi a probléma?
  - *Minél kisebb a sávszélesség, annál jobban „elkenődik” a jel:* ***diszperzív csatorna***
  - *Ha csak egy impulzusunk lenne*
    - *elég nagy szétkenődést is megengedhetnénk*
    - *elég lenne, ha a jel közepén vett minta jól megkülönböztethető lenne a jel hiányától*
  - *Impulzussorozat esetén a szomszédosak egymásra hatnak és elrontják a döntést*
  - A jelenség neve: **szimbólumközi áthallás – inter-symbol interference (ISI)**
- A megoldás elve (**Nyquist-módszer**):
  - *Úgy csökkentsük a sávszélességet, hogy közben tartsuk kézben a szimbólumközi áthallást*
  - *Nem baj, ha van, de ne befolyásolja a helyes döntést*

A szimbólumközi áthallásmentesség feltétele az időtartományban

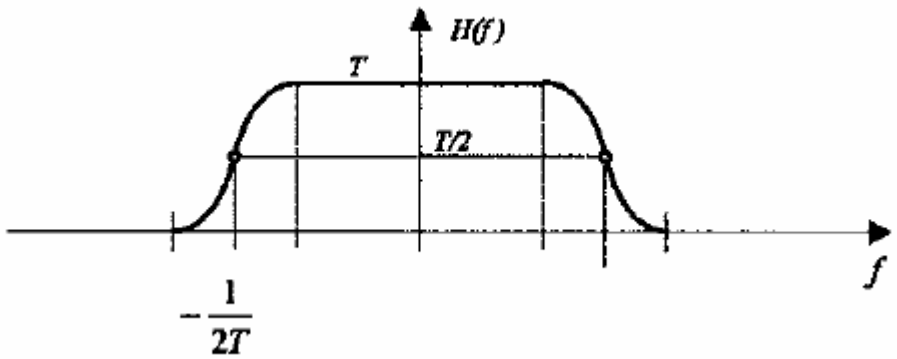
A mintavételi időpontban valamennyi szomszédos jelből származó minta értéke legyen zérus!



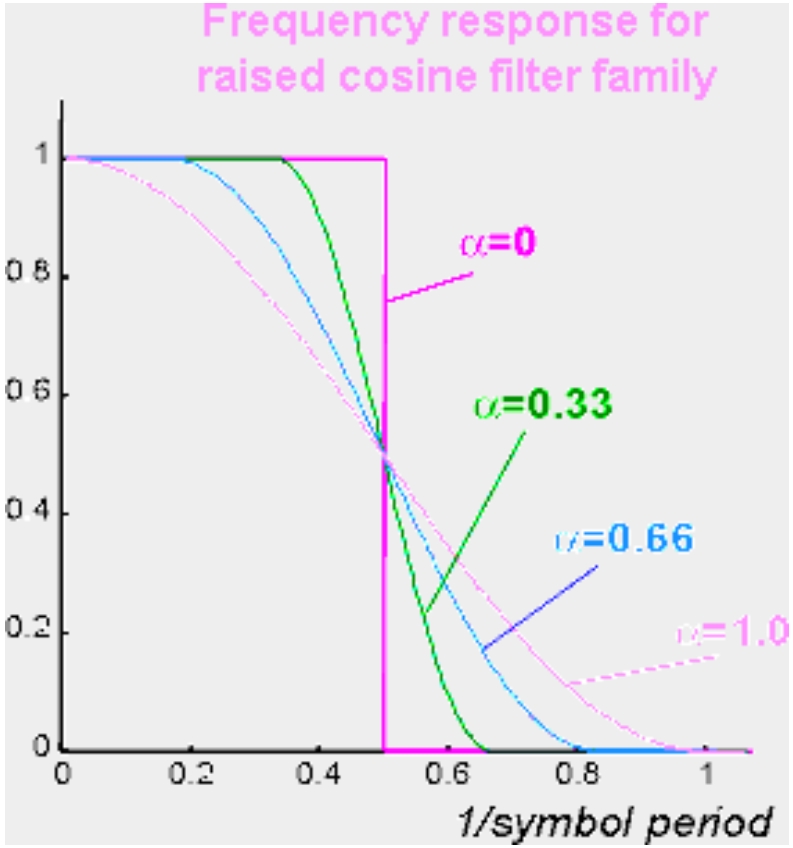
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A szimbólumközi áthallás-mentesség feltétele a frekvenciatartományban

A jel spektruma a döntés előtt legyen szimmetrikus a jelzési frekvencia felére (Nyquist-frekvencia)



A Nyquist-kritériumnak eleget tevő spektrumalakok



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A szimbólumközi áthallás-mentesség feltétele a frekvenciatartományban

- Megjegyzés
  - *az előbbi feltétel egy bebizonyítható tétel, amellyel azonban itt nem tudunk foglalkozni*

- Hogyan teljesítsük a Nyquist-feltételt?
  - *a döntésre kerülő jel spektrumára kell, hogy teljesüljön*
  - *az átviteli úton több helyen formálódik a spektrum*
  - *a vevőben lévő szűrővel kell „helyretenni” az alakját, amelynek emiatt nem feltétlenül Nyquist-alakúnak kell lennie*

- **A szükséges legkisebb sávszélesség tehát a jelzési frekvencia felének felel meg**, pl.
  - *1 MBaud-os átviteli sebesség – 0,5 MHz elvi sávszélesség*
  - *pl. a szabványos telefoncsatornán, melynek sávszélessége 3100 Hz, 6200 Baud-dal lehet elvileg kommunikálni*
  - *ez többszintű jelátvitelnél ...*

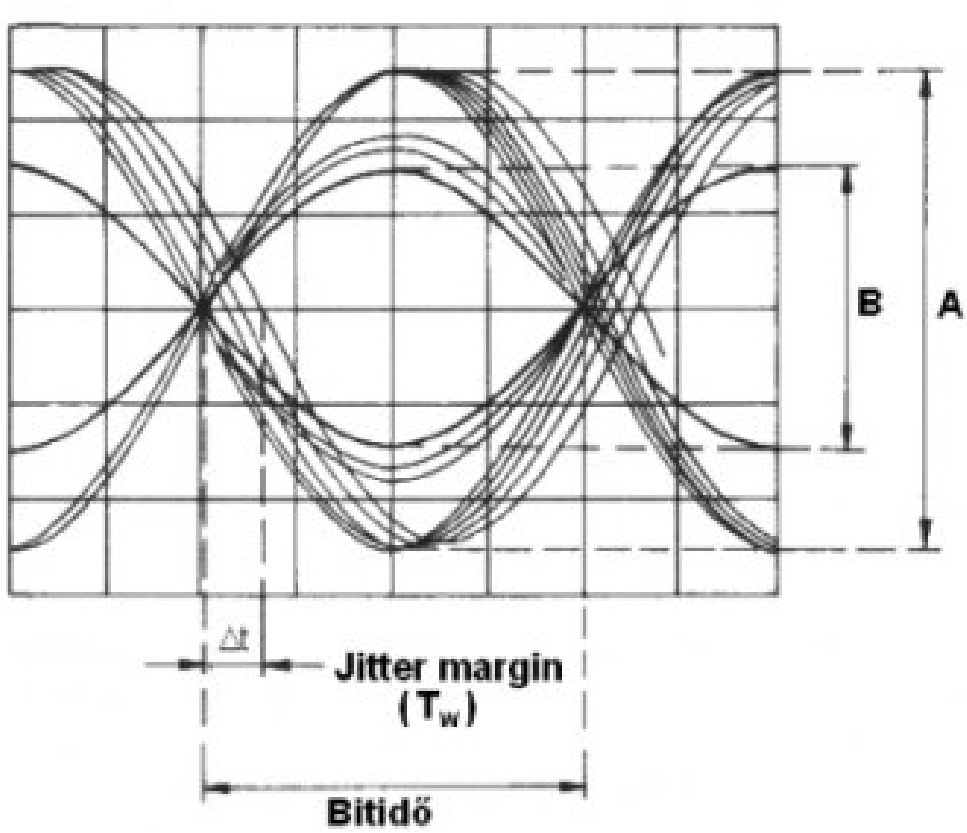
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A szemábra (eye diagram)

- **Oszcilloszkópos megfigyelés: egymás utáni jelalakok egymásra rajzolódnak**

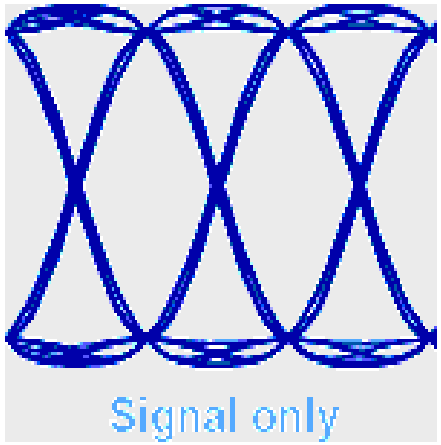
- **Ha egy szimbólumidőre húzzuk szét a vízszintes tengelyt: szemre emlékeztet**

- **A szem tisztasága, nyitottsága a mintavételi időpontban jelzi, hogy mekkora esélyünk van a helyes döntésre**



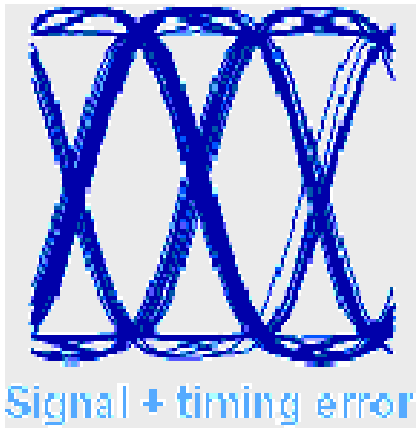
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Szemábrák”

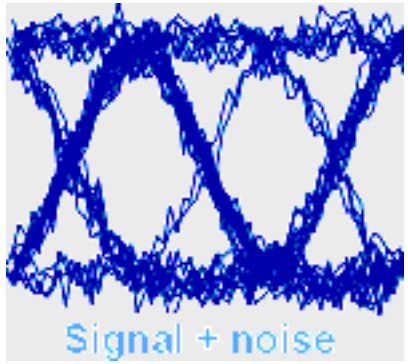


csak hasznos jel

jel és időzítési hiba



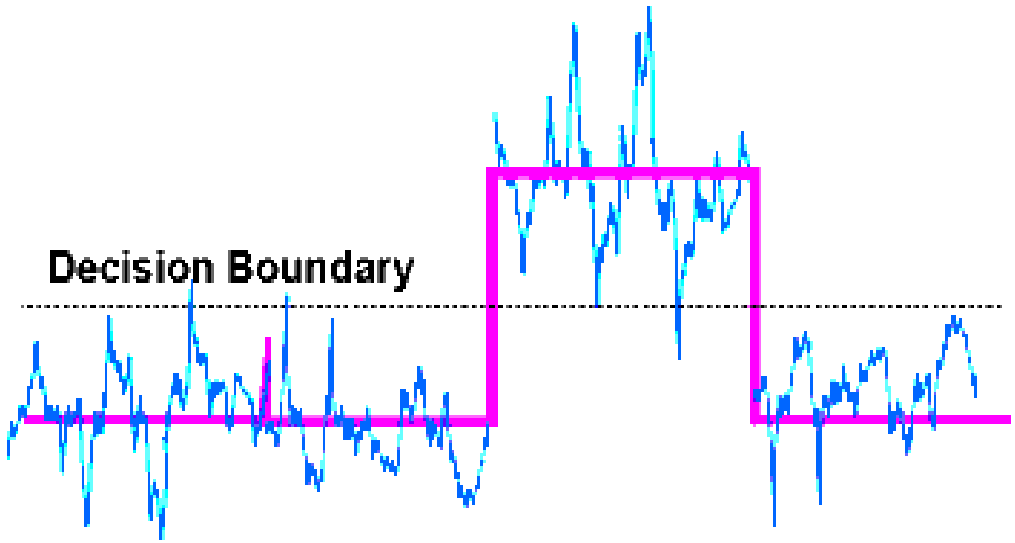
jel és zaj



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Átvitel zajos csatornán

- *Az ábra bináris: szimmetrikus jel és „ráülő” 0-átlagú additív zaj*
- *Ésszerű: döntési küszöb a fél jelmagasságon, ezzel összehasonlítva a mintákat döntünk*
- *Az additív zaj miatt tévesztések, minél nagyobb a zaj, annál többször.*



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Átvitel zajos csatornán, hibavalószínűség (1)

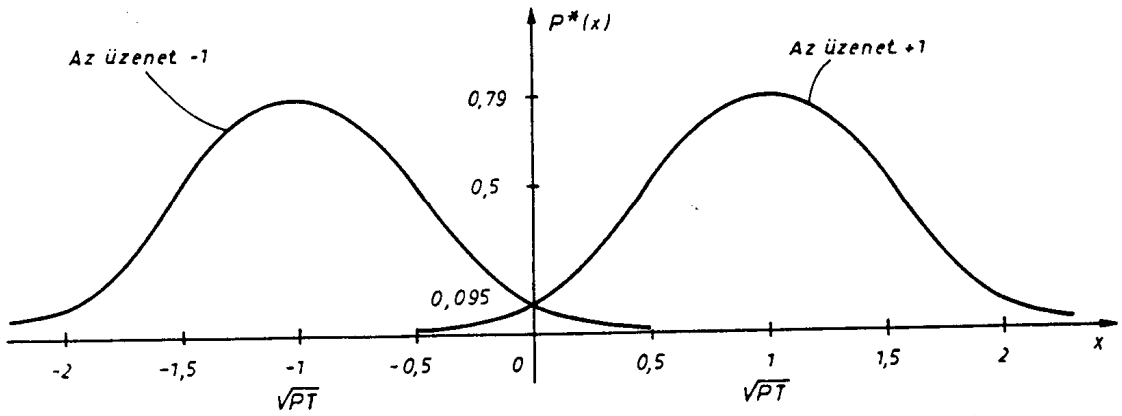
- A hibavalószínűség könnyen kiszámítható, ha a modellünk

  - *additív zaj*
  - *a zajminták nulla várható értékű, Gauss-i eloszlásúak*
  - *a zaj teljesítménysűrűség-spektruma konstans („additív fehér Gauss zaj”-modell)*
    - *Teljesítménysűrűség-spektrum: S [W/Hz]*

- Hibavalószínűség: sűrűségfüggvények „farkai” alatti területek (l. az ábrát)

Átvitel zajos csatornán, hibavalószínűség (2)

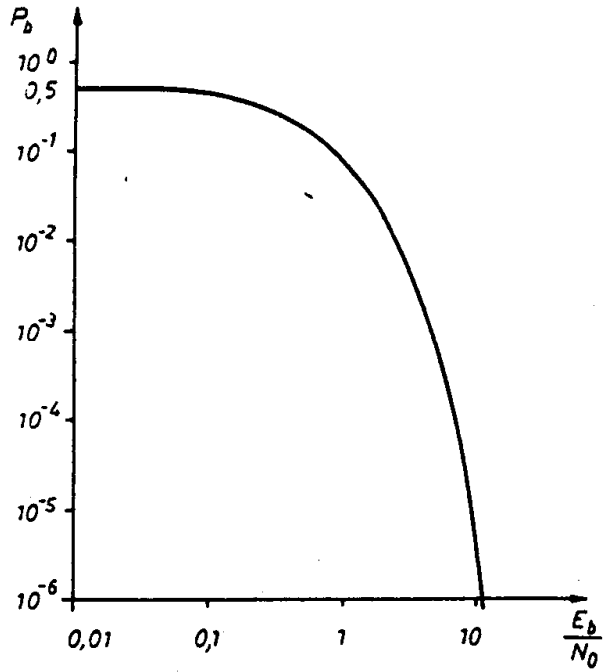
- A jel+zaj valószínűség-sűrűségfüggvényei a jel nagyságával eltolt Gauss-sűrűségfüggvények
- A döntési küszöb ebben az esetben 0
- A küszöb alatt -1-re, felette +1-re döntünk
- Az ellentétes jelalakra „ráült” zaj-sűrűségfv.-ek „átlógó” része alatti terület a hibavalószínűség



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Átvitel zajos csatornán, hibavalószínűség (3)

A hibavalószínűség kiszámítható és a Gauss-hibaintegrál segítségével kiértékelhető a jelenergia/zajteljesítmény sűrűségfüggvényében



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

További gyakorlati kérdések impulzusátvitelnél

- Nullafrekvenciás komponens
  - Ne legyen DC tartalma a jelnek
  - Ezért kell bipoláris kódolás: AMI (Alternate Mark Inversion), értékkészlet: -1, 0, +1.

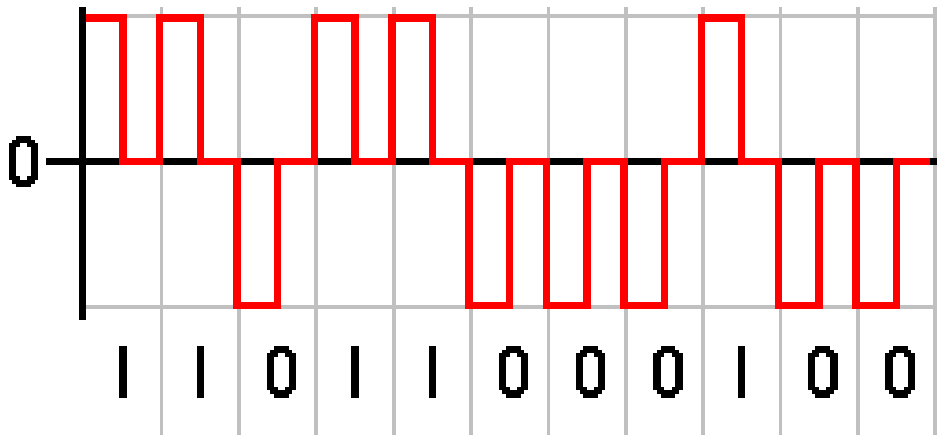
- Bitszinkron biztosításához órajel kinyerése
  - Ezért ne legyenek hosszú egyforma bitsorozatok

- Néhány, a gyakorlatban használt „vonali” kódolás (a következő ábrán)
- Vonali kódolás: **digitális alapsávi moduláció**!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

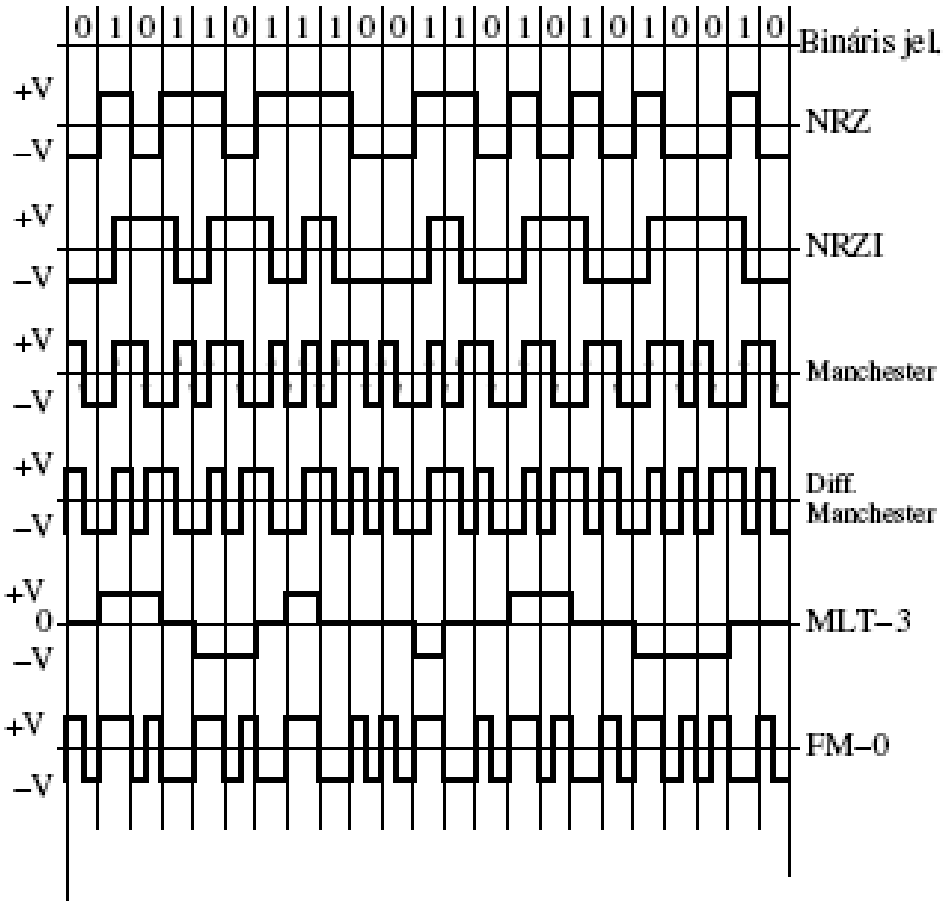
Return-to-zero (RZ)

- Két impulzus között mindig visszatér a nulla jelszintre
  - Még ha több 1 vagy 0 is jön egymás után
- Szinkron biztosított, de kétszer akkora sávszélesség kell ugyanakkora adatátviteli sebességhez, mint pl. a NRZ-nek
- Van DC komponens hosszú 0 vagy 1 sorozatok esetén



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Vonali” kódolások (1)



non-return-to-zero (NRZ)

NRZ inverted (NRZI)

Manchester

Diff. Manchester

más kód 1.

más kód 2.

„Vonali” kódolások (2)

- **RZ**
  +: megoldott a szinkron
  -: kétszeres sávszélesség kell mint NRZ-nek

- **NRZ**
  +: fele annyi sávszélességre van szüksége mint pl. a Manchesternek vagy RZ-nek
  - : hosszú 1-es, v. 0-ás sorozat esetén a váltások hiánya miatt szinkronvesztés

- **NRZI**
  + : ugyanaz
  - : Az 1-eseknél mindig van váltás a bitidő közepén, hosszú 0-ás sorozat itt is problémát okoz
    - Megoldás: bit stuffing pl. USB (6 1-es után 0)

- **Manchester**
  - 1-esnél felfelé, 0-ásnál lefelé váltás a bitidő közepén, egymás utáni azonos biteknél a bithatáron mindig váltás
  - Pl. Ethernetnél, RFID-nél használják
  + : jól szinkronizálható, nincs DC komponens
  - : kétszeres bitsebességet igényel mint NRZ

- **Differenciális Manchester**
  + : polaritás nem fontos, csak tranzíció: hibavédettebb
  - 0-nál a bitidő elején is és közepén is van váltás
  - Optikai tárolásra, token ring

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Vonali” kódolások (3)

- MLT (Multi-Level Transmit)-3
  - 3 feszültségszint: ciklusban mozog ha 1, 0-nál marad ugyanazon a szinten

  \+ : kevesebb EM interferencia, kisebb sávszélesség

- FM-0
  - minden bit határon váltás, 0-nál középen is

  \+ : szinkron, nincs DC komponens

  \- : több sávszélesség

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

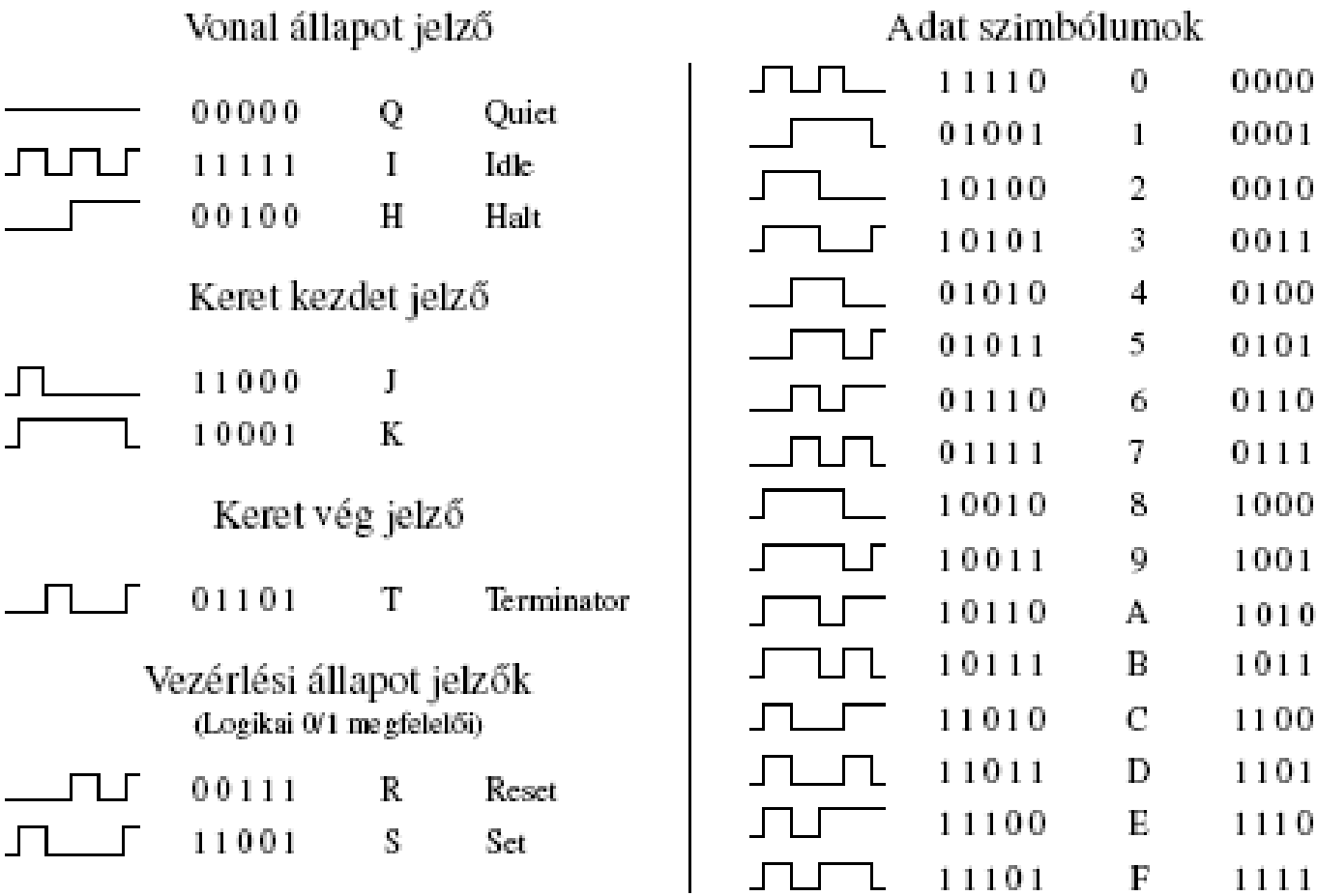
4B/5B kódolás

- Hatékonyabb kódolás: összeegyeztetni a jó szinkronizálhatóság és a kis sávszélesség-növekedés feltételeit

- 4B/5B kódolás
  - a bemeneti bitfolyam minden bit-négyesét 5 bites kóddal helyettesítjük
  - a 16 helyett 32 kombinációnk van, ezért megtehetjük, hogy:
    - csak azokat használjuk, amelyek jó tulajdonságú sorozatot eredményeznek
      - legalább 2 váltás a blokkban
    - a többiből 8-at használunk speciális jelzésekre, a fennmaradó 8-at nem használjuk fel (köv. ábra)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A 4B/5B kódolás illusztrációja (+NRZI)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

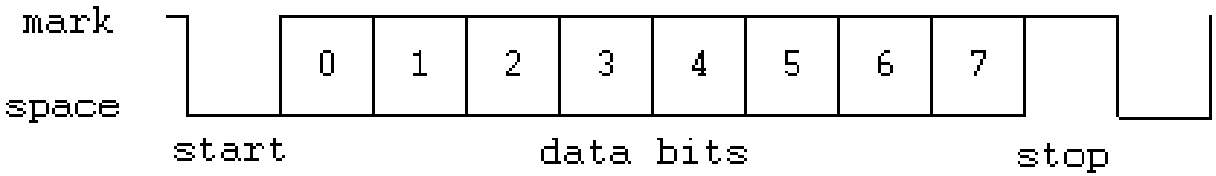
Bitfolyamok strukturálása

- Keretezés hibavédelmi és szinkronizálási célokra
- Szinkronizálás
  - bitszinkron
  - byte-szinkron
  - keretszinkron
- Hibajelzés, hibajelző kódok
  - Paritásellenőrzés
  - Ciklikus redundancia-ellenőrzés (CRC)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

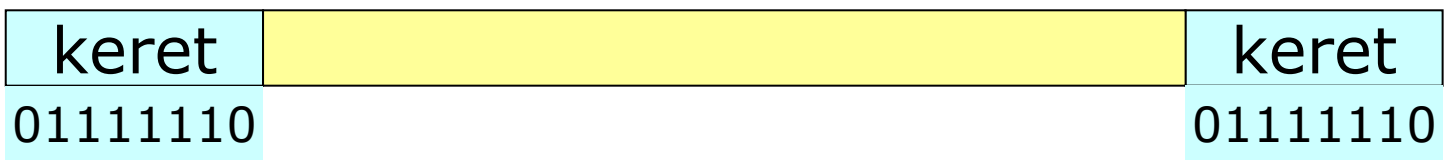
Aszinkron és szinkron átvitel

- A „start-stop” átvitel: aszinkron mód, órajel nem kerül továbbításra



  - jól használható például text továbbításhoz (pl. telex gép), csak kis sebességre

- Szinkron átvitel



  - bitbeszúrás

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

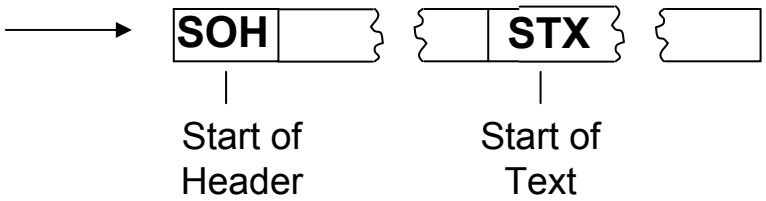
Szinkronizálás, hibajelzés

Byte-szinkronizálás

Vezérlő és ellenőrző információ átvitele

HEADER – fejrész
TRAILER – pl. **ellenőrző kód**
PAYLOAD – „hasznos teher”

Fejrész azonosítása



Hibajelző kódok: -paritás

- ciklikus kód

(CRC – cyclic redundant code)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Miről volt eddig szó?

- Alapfogalmak
  - bitsebesség, jelzési sebesség, többszintű jelzések
- A véges sávszélesség hatása impulzussorozat átvitelénél
  - szimbólumközi „áthallás”
  - a szimbólumközi áthallástól mentesség feltétele: Nyquist-kritérium, minimálisan szükséges sávszélesség
- A zaj hatása
- További gyakorlati kérdések

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Fizikai szintű” kommunikáció

Bitfolyamok továbbítása hírközlő csatornákon

2. rész: Modulációs eljárások

2013.február 21.

Modulációs eljárások, digitális moduláció

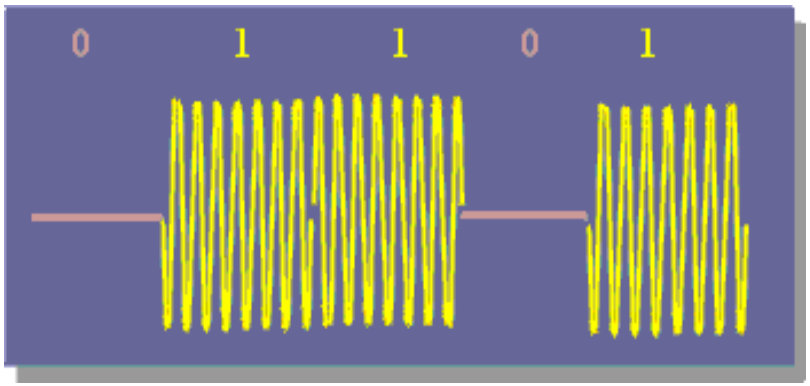
- „Moduláció”: a szimbólumsorozat továbbítására egy – a jelzési sebességnél általában nagyobb frekvenciájú - **szinuszos vivőt** használunk.

- A vivő valamely jellemzőjét változtatjuk a szimbólumoknak megfelelően, így
  - amplitúdóját: **ASK** (amplitude-shift-keying) – ki-bekapcsolásos moduláció (eredetileg: „billentyűzés”),
  - frekvenciáját: **FSK** (frequency-shift-keying),
  - fázisát: **PSK** (phase-shift-keying).

- A jel spektruma áthelyeződik **az „alapsávból” a vivő környezetébe**.

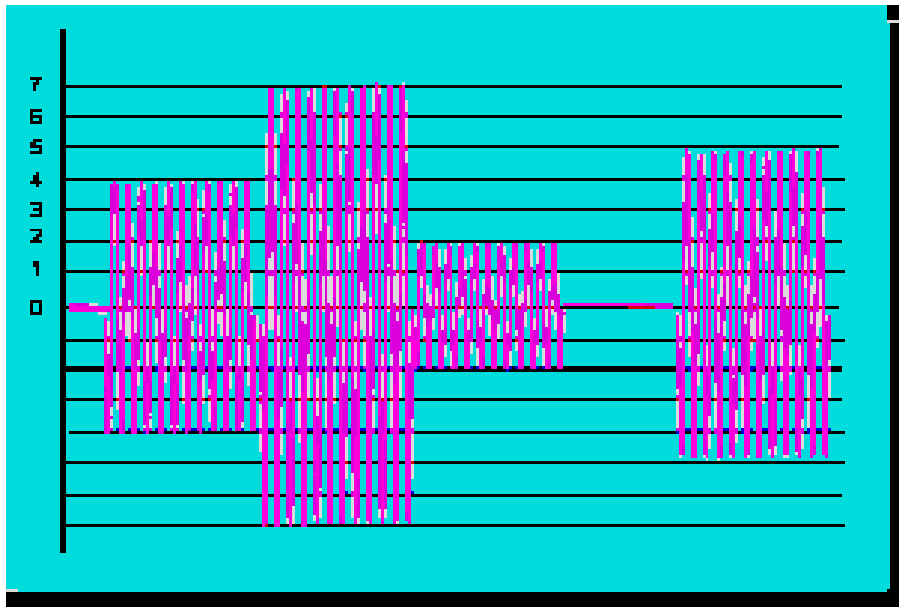
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ASK (Amplitude Shift Keying) - amplitúdó moduláció



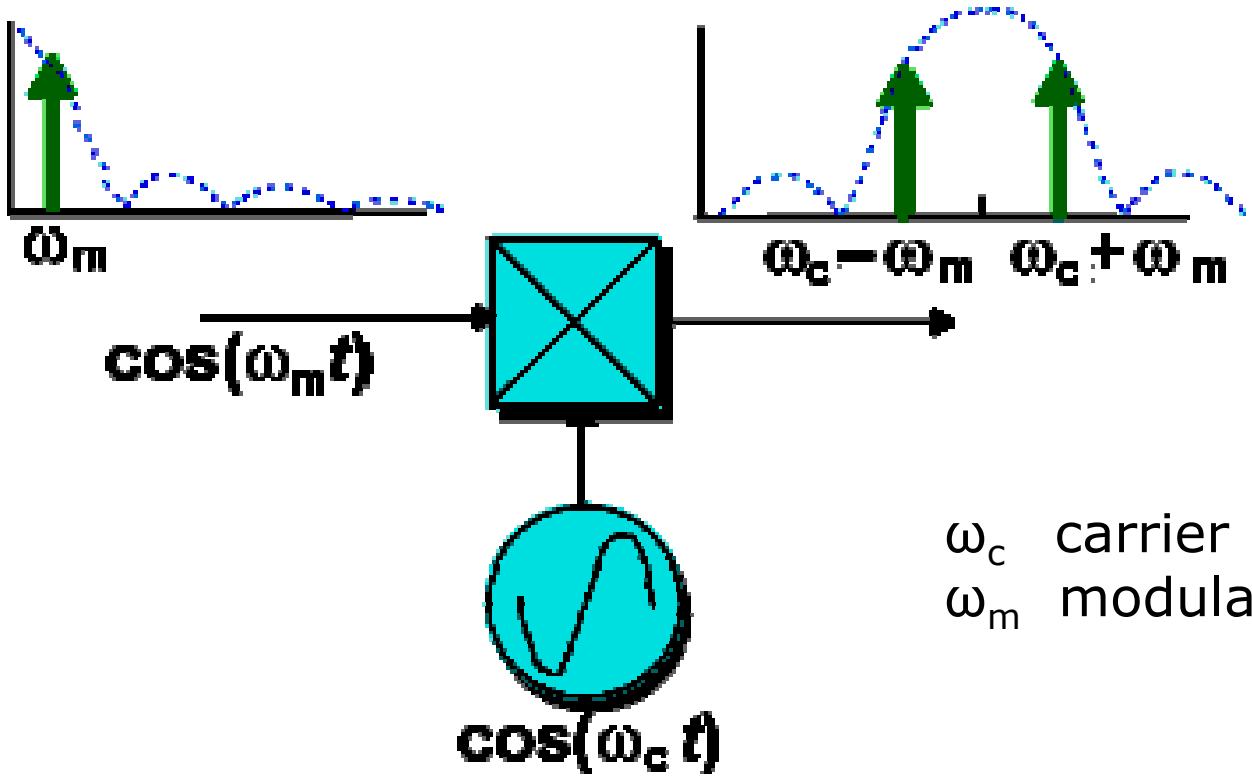
„0”: nincs vivő, „1”: van
(on-off-keying,
ki-bekapcsolásos moduláció)

Többszintű
ASK
-magas jel-zaj
viszony kell hozzá!



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ASK jel spektruma: illusztráció szinuszos jelkomponenssel

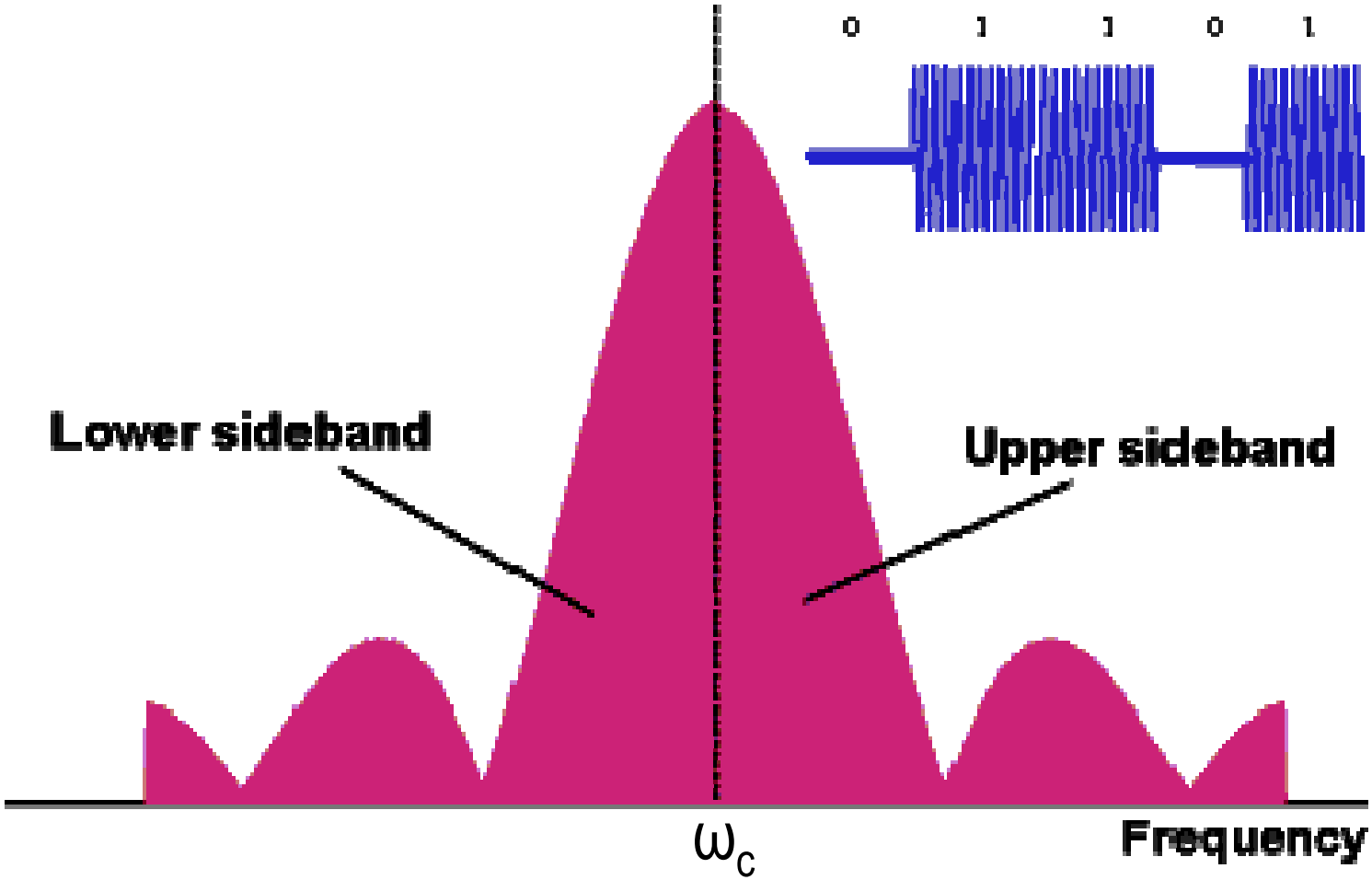


ω_c carrier (vivő)
ω_m modulator

$$\cos \omega_m t \times \cos \omega_c t = 0{,}5 \cos (\omega_c - \omega_m)t + 0{,}5 \cos (\omega_c + \omega_m)t$$

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ASK jel spektruma



ASK előnyei-hátrányai

+:

- ASK moduláció és demoduláció is egyszerű, olcsó

-:

- Érzékeny a zajokra, a különböző terjedési utak körülményeire

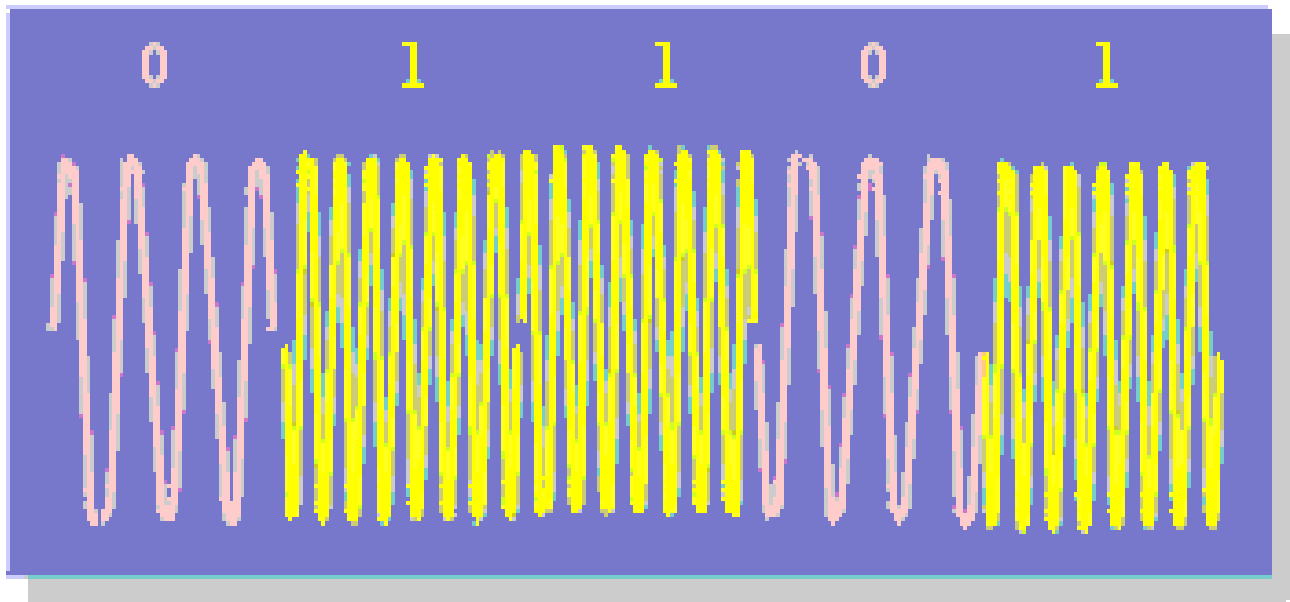
- Felhasználás:
  - Digitális adat átvitele optikai kábelen
    - LED adónál 1: rövid fényimpulzus, 0: nincs fény
    - Lézernél 1: magas amplitúdójú fényhullám, 0: alacsony

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

FSK

„0” szimbólumnak f1 frekvenciájú vivő
„1”-es szimbólumnak f2 frekvenciájú felel meg

digitális frekvenciamoduláció: a vivő frekvenciáját változtatjuk a moduláló jel szerint



FSK előnyei-hátrányai

+ :

- Egyszerű előállítás és demodulálás

- Érzéketlenség a nem-lineáris erősítők torzítására
  - jó hatásfokú erősítők alkalmazásának lehetősége
  - gazdaságos akkumulátorhasználat a mobil készülékekben

- : Sávszélesség kihasználása nem olyan jó mint PSK-nak

- Népszerűek változatai:
  - AFSK (Audio FSK): telefonmodemek, alapsávban
  - GMSK (Gaussian Minimum Shift Keying): GSM!

    Használat: pl. távoli mérőóra leolvasás

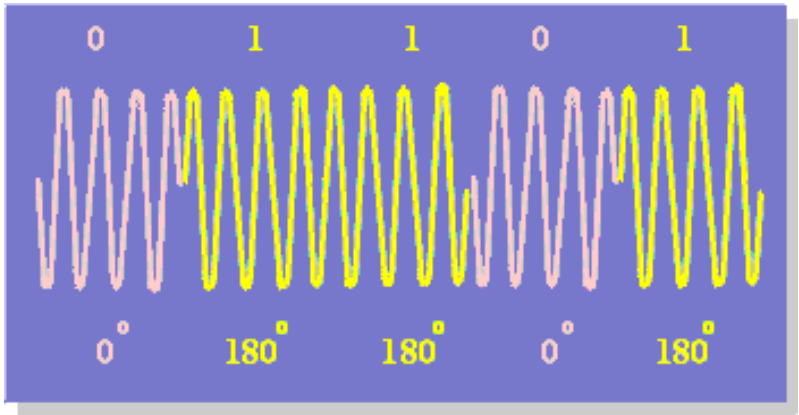
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

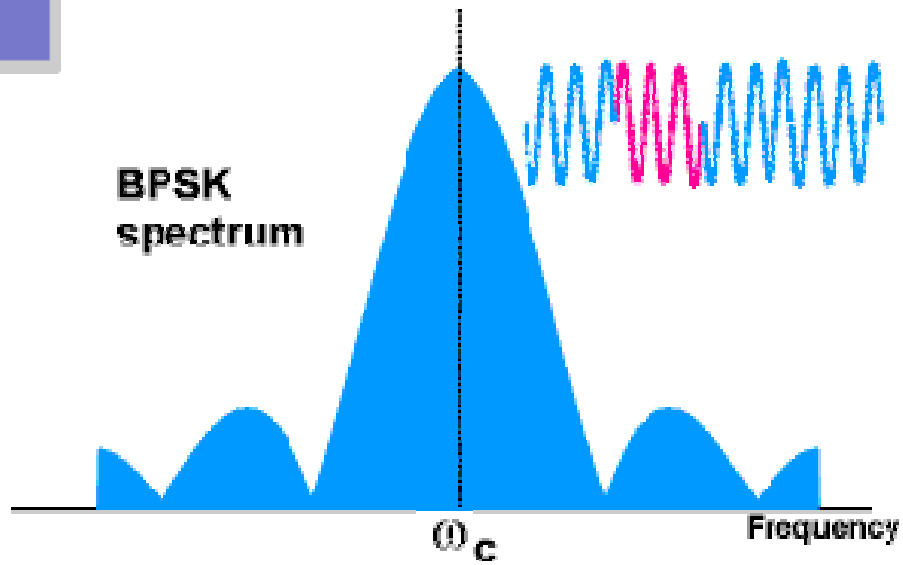
GMSK

- **Folyamatos fázismoduláció**: nem ugrik vissza a kezdeti értékre, van memóriája a fázisnak
  - +: kisebb energiafogyasztás
  - +: magas spektrális hatékonyság
  - -: ismerni kell az előéletét
- Jel **Gauss szűrőn** megy át a modulátor előtt
  - kisebb oldalsáv, csökken a szomszédos frekvencia csatornák közötti interferencia

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

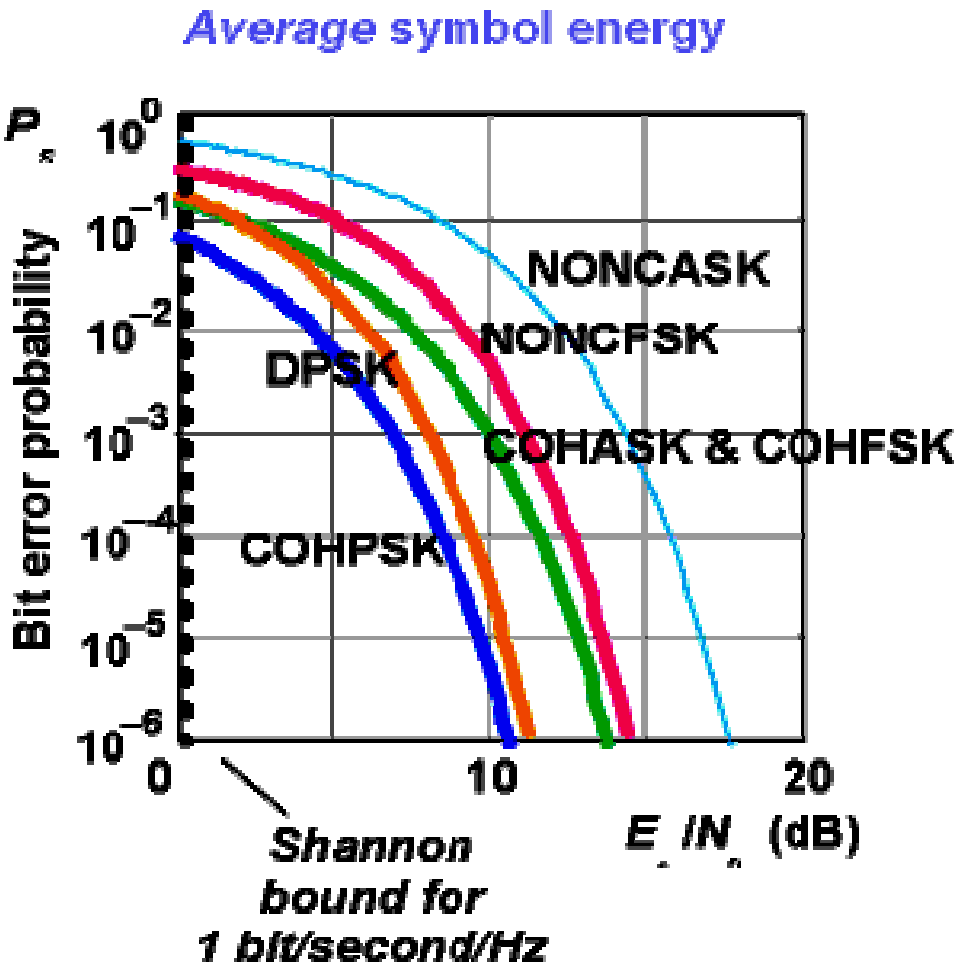
(Bináris) PSK jel az időtartományban és a spektruma





© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

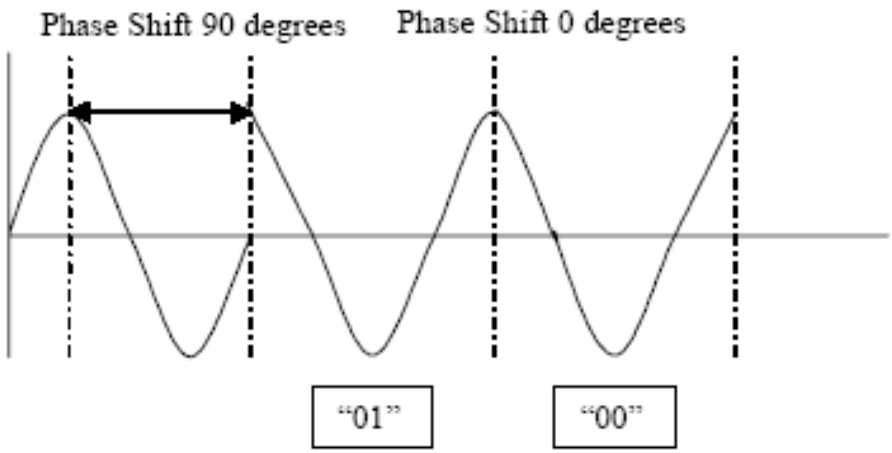
ASK, FSK és PSK hibavalószínűségei



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Többszintű PSK: QPSK (Quadrature PSK)

Symbol	Phase Shift
00	0 degrees
01	90 degrees
11	180 degrees
10	270 degrees

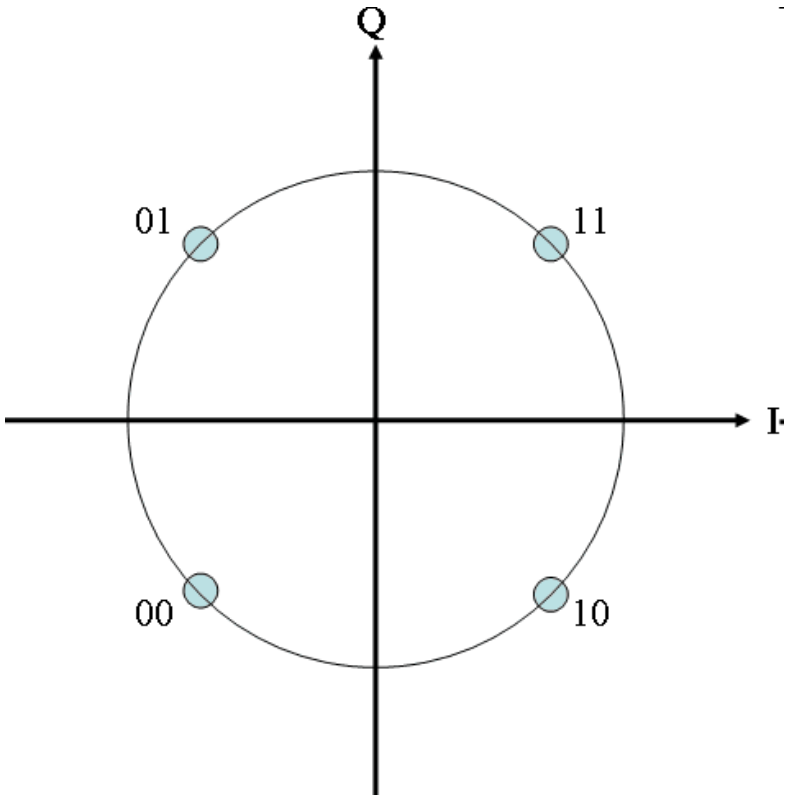


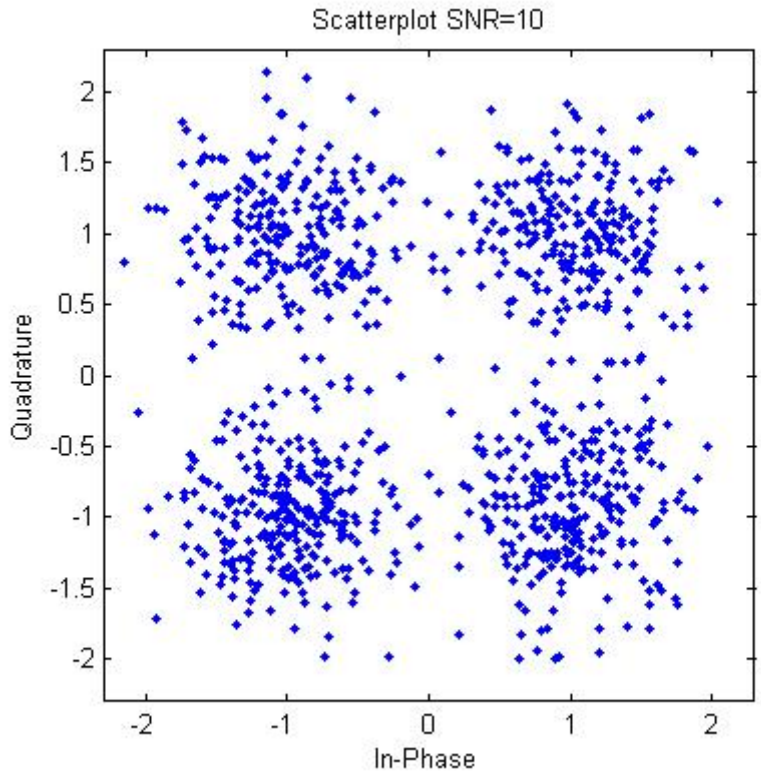
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Konstellációs diagram

- Konstellációs diagramon komplex számmal ábrázoljuk az átviendő szimbólumot
- Kvadratúra vivők: modulálva a valós és képzetes résszel a sin illetve cos vivőt, mindkettőt átvisszük ugyanazon a frekvencián
  - kvadratúra moduláció
- Vevő: arra a szimbolúmra választ, amelyhez a vett szimbólumnak a **legkisebb az euklidészi távolsága**
  - Hibás döntés: zaj másik konstellációs ponthoz viszi közelebb
- Olyan mint a szemábra

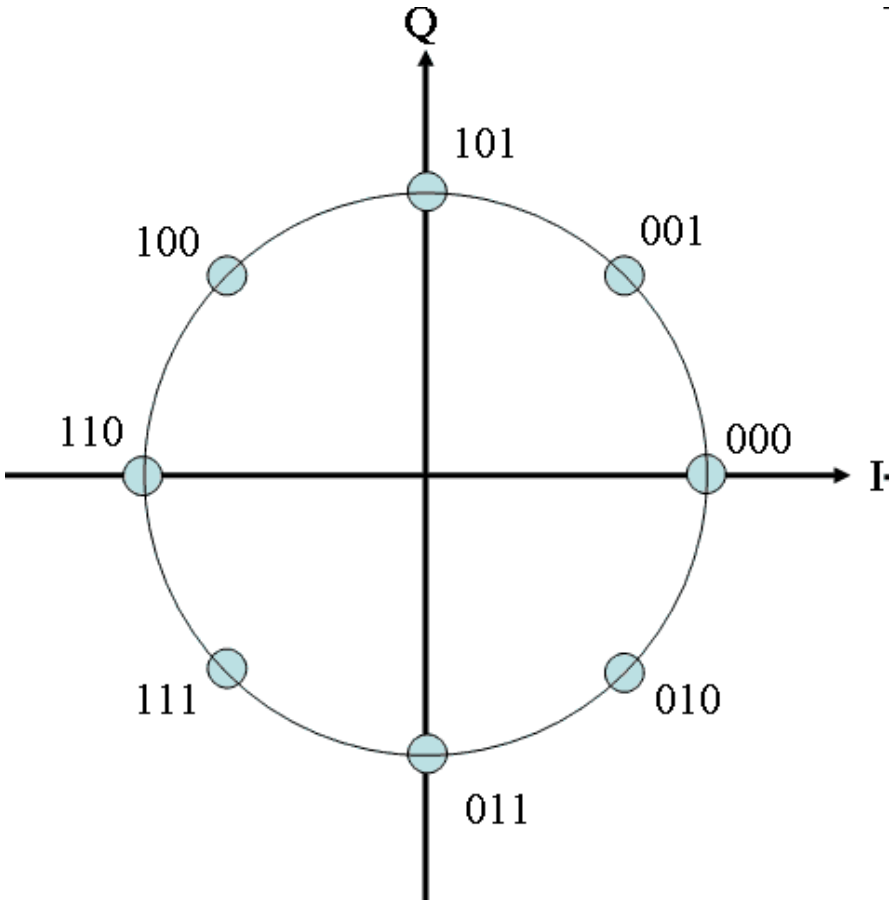
QPSK konstellációs diagram





© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

8PSK

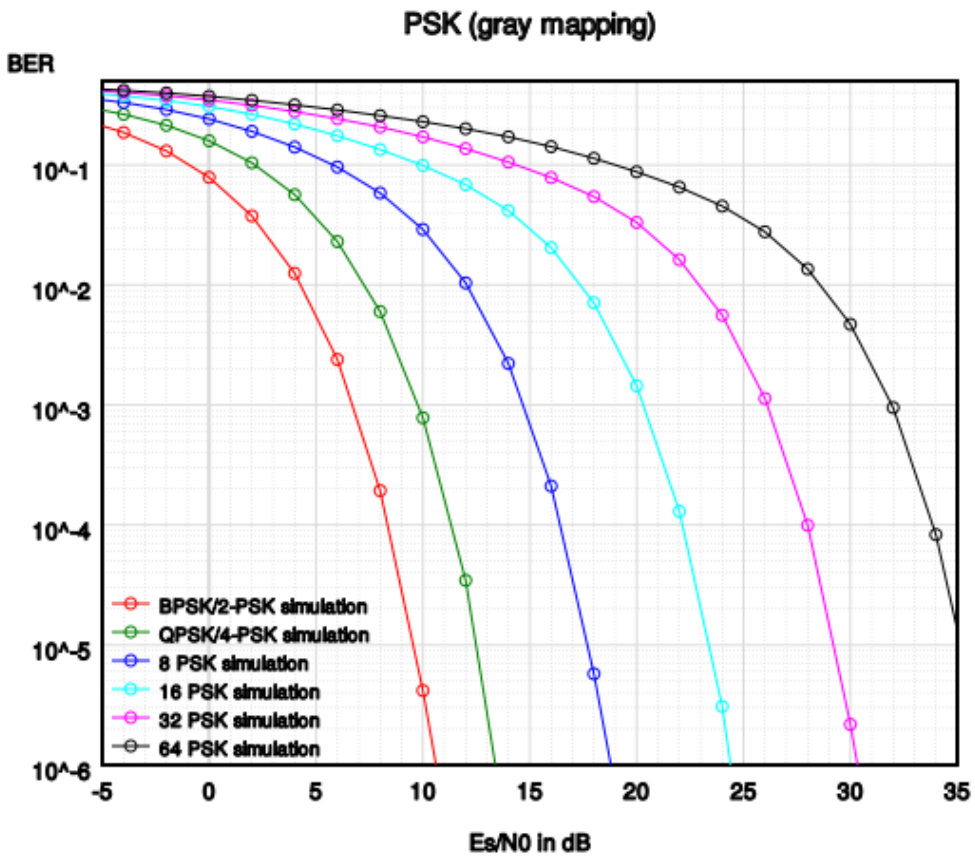


BPSK-QPSK-8PSK

- QPSK megduplázza a BPSK adatsebességét
- Viszont nagyobb adóteljesítményre van szüksége ugyanahhoz a jel-zaj viszonyhoz!
- BPSK: hibatűrő, de alacsony adatsebesség
- 8PSK: legmagasabb szintű PSK
  - 8 szint felett már magas a hibaarány, erre jobb a QAM

PSK hibaarányok

- 8 PSK felett már túl nagy a hibaarány!



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazási terület

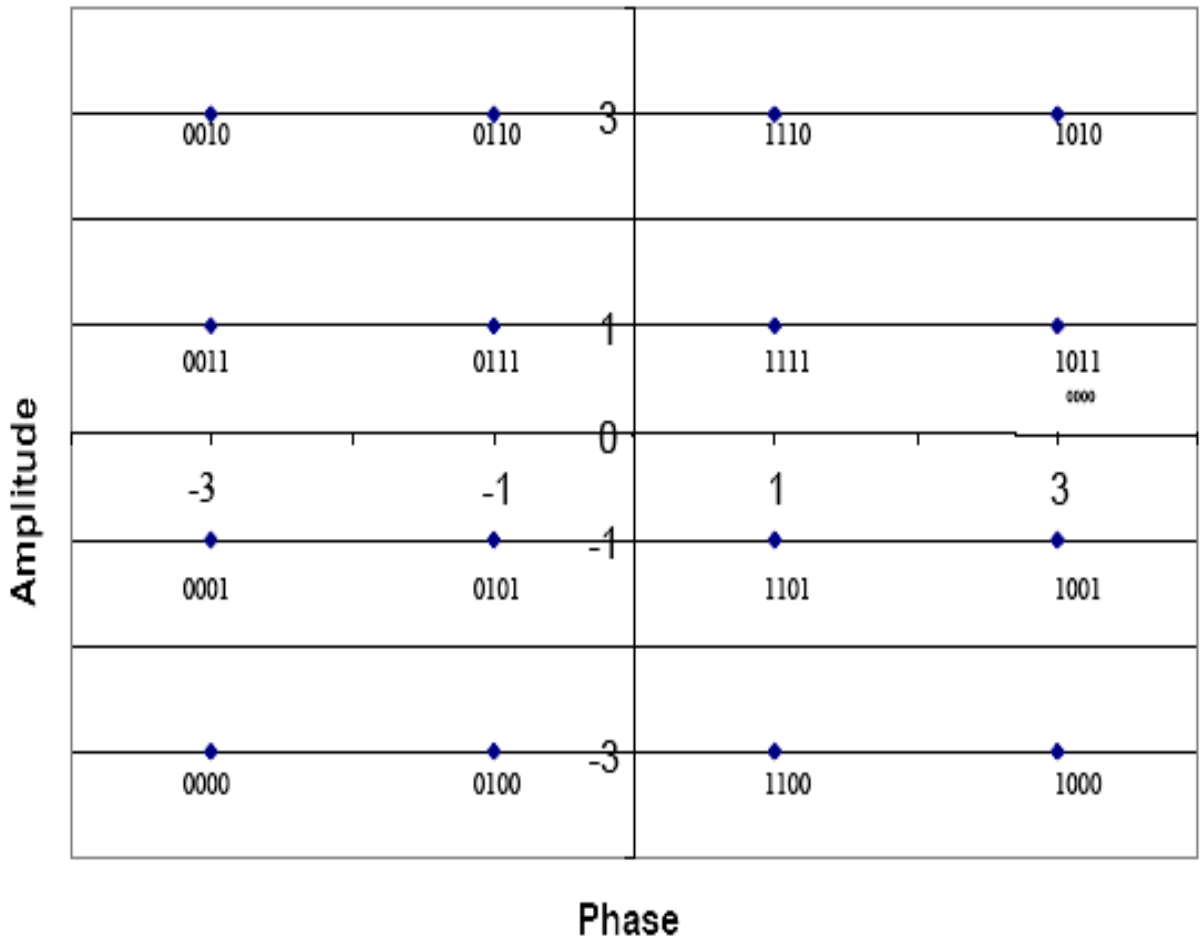
- **BPSK**: RFID (biometrikus útlevelek, American Express)
- **QPSK**: Bluetooth 2 (DQPSK)
- **8PSK:** Enhanced Data rates for GSM Evolution (EDGE), 2.5G

QAM

- Két, 90 fokkal eltolt vivőnek egyszerre moduláljuk az amplitúdóját, majd összeadva átküldjük a csatornán
- Olyan, mintha egy vivőnek egyszerre modulálnánk az amplitúdóját és fázisát is
- Leggyakoribb 16-QAM, 64-QAM, 128-QAM és 256-QAM
  - egyre nagyobb adatsebesség, de rosszabb hibaarány!

QAM konstellációs diagramm

Példa: 16QAM



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazás

- 8PSK felett már érdemes áttérni a 16QAM-re
  - 8PSK csak 0.5dB-el ad jobb hibaarányt, de adatsebessége csak ¾-e
  - Így néha QPSK után már 16QAM jön
- 64-QAM és 256-QAM: digitális kábel és földfelszíni tv

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Adaptív moduláció

- A rádiós link állapotától függően vált modulációt
  - más adók interferenciája, vevő érzékenysége, adóteljesítmény
  - Ehhez szükség van az adónak csatornainformációra

- Pl. 3G mobil rendszereknél HSPA (High Speed Packet Access)
  - Zajos csatornánál QPSK
  - „Tisztább” csatornánál 16QAM

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Multiplexelés (nyalábolás)

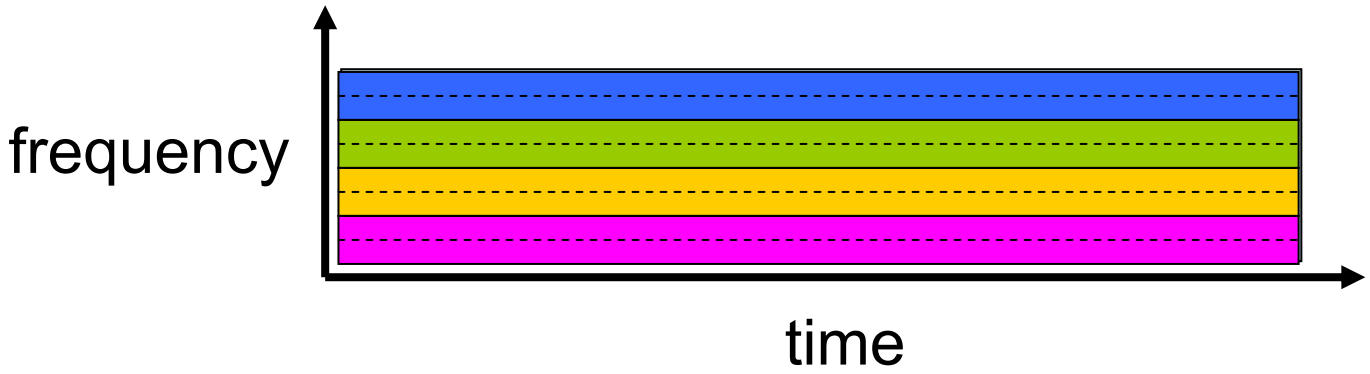
- Több csatorna jelét egyetlen jellé alakítani egy osztott csatornán
- Egy kommunikációs csatornát több magasabb szintű logikai csatornává
  - Minden jelfolyamhoz egy logikai csatorna
- Demultiplexelés: vevő oldalon elő tudják állítani az eredeti csatornákat

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

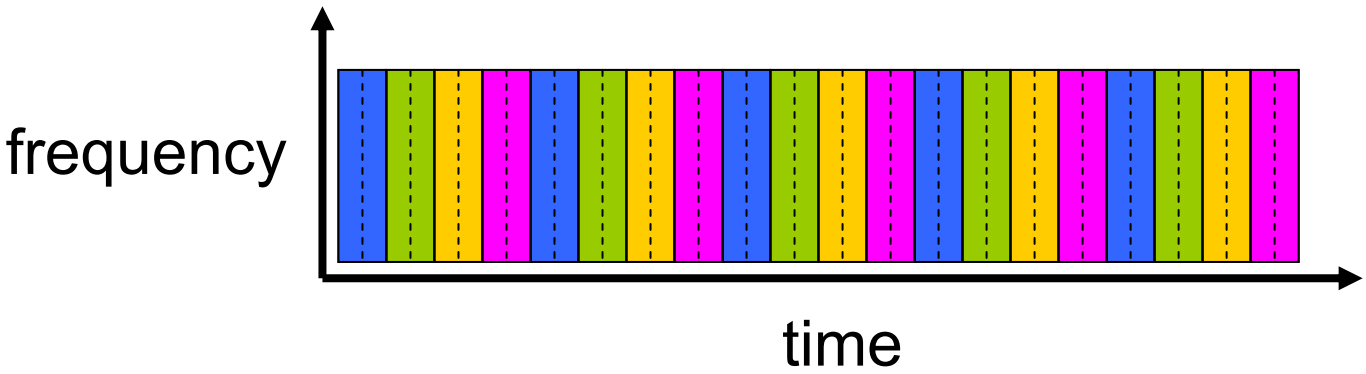
Multiplexelés: FDM és TDM

FDM

Példa:
4 felhasználó

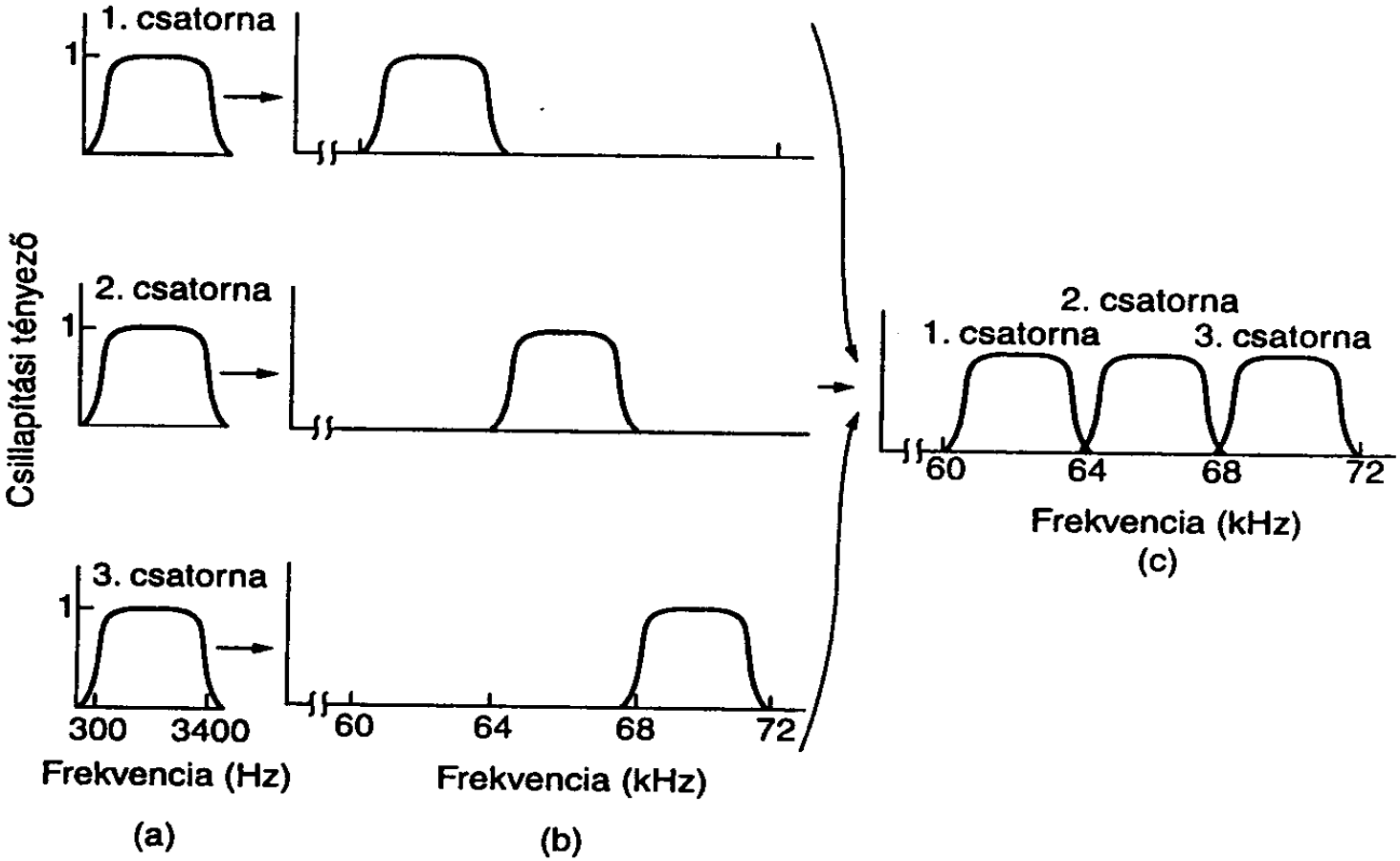


TDM



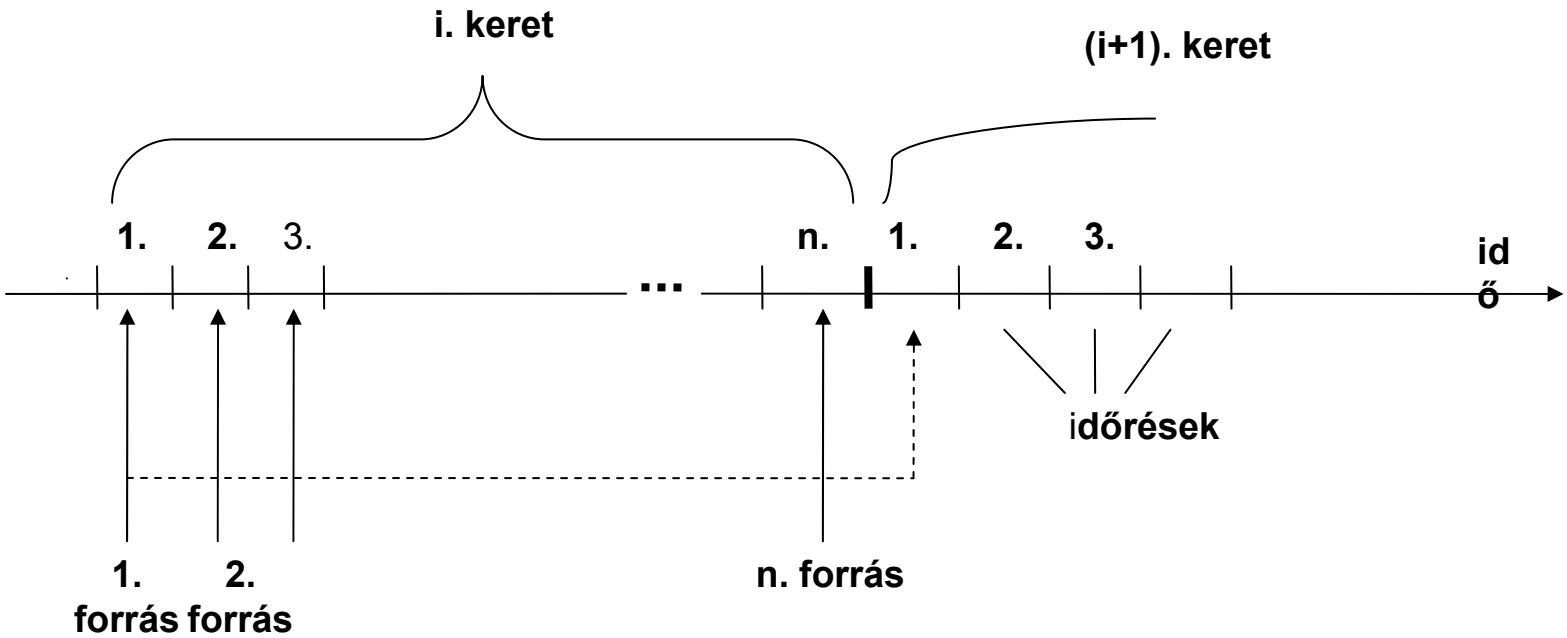
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A frekvenciaosztású nyalábolás elve – - FDM – frequency division multiplexing



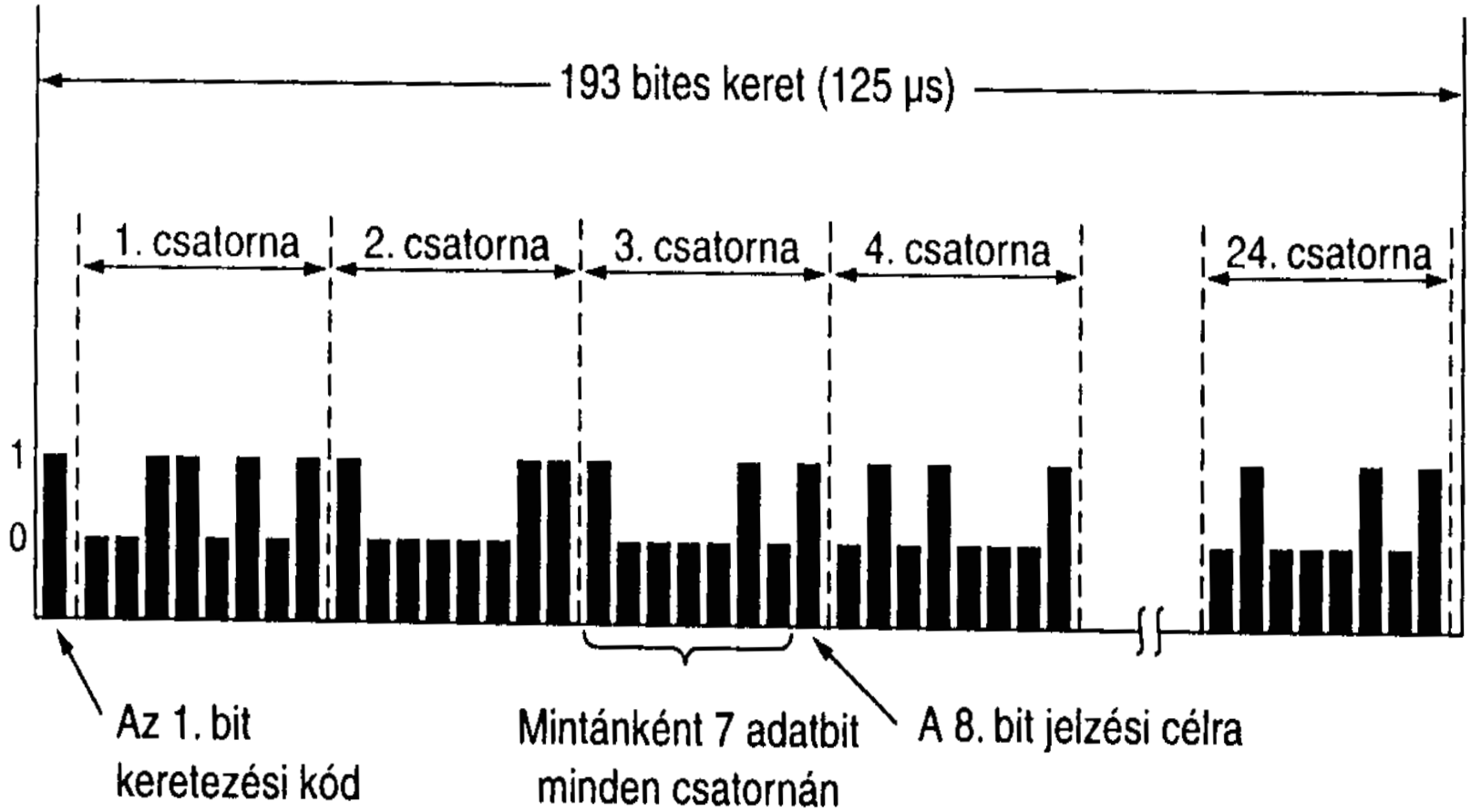
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Időosztású multiplexelés – - TDM – time division multiplexing



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa időosztású nyalábolásra beszédátviteli rendszerben (24 csatorna egyenként 8 bitjének multiplexelése)



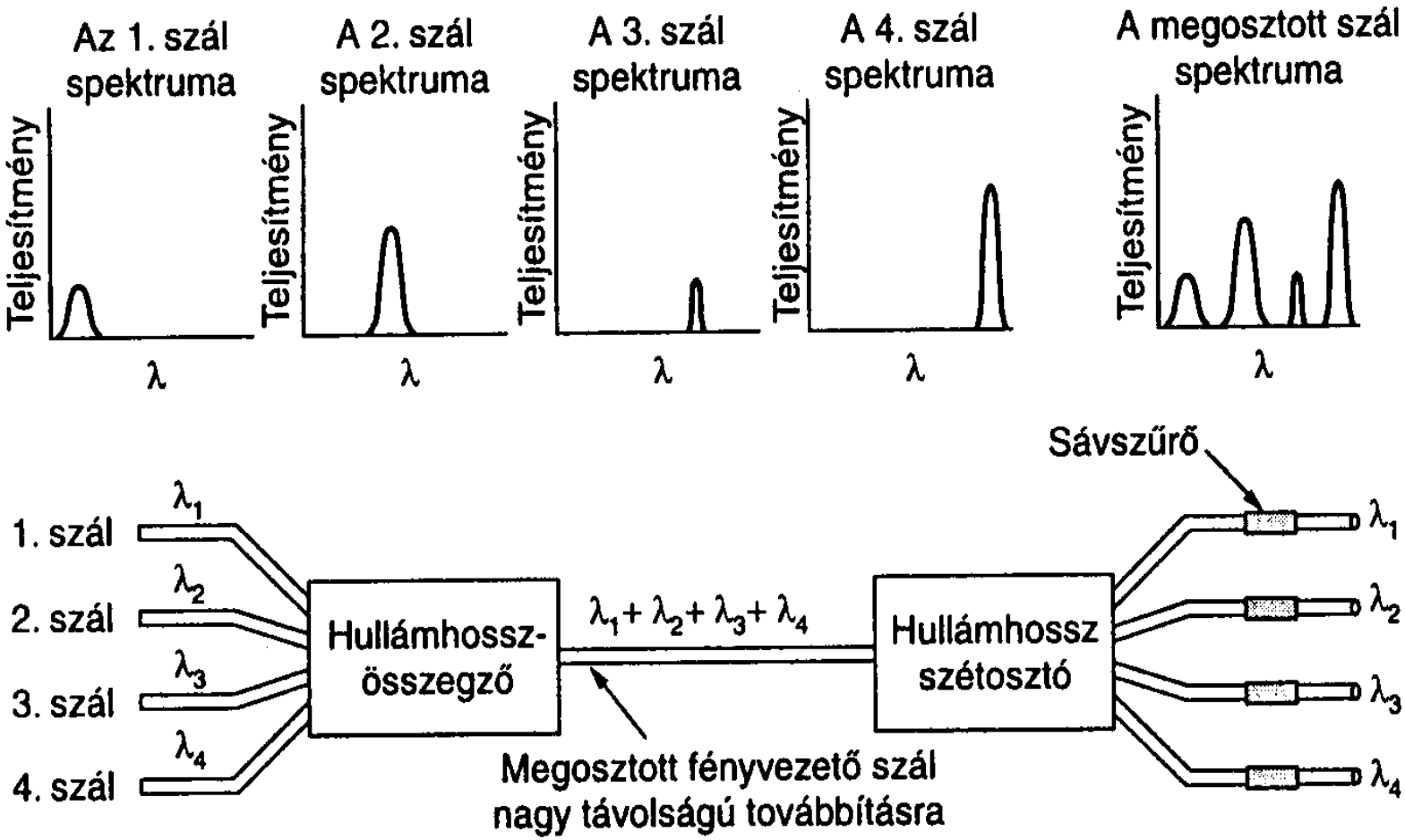
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hullámhossz-osztású multiplexelés

- Üvegszálon több eltérő hullámhosszú fényt viszünk át: több csatorna alakítható ki egy üvegszálon
- Végülis egy FDM technika, de üvegszálon WDM-nek nevezzük (rádiós csatornán FDM)
- Népszerű a szolgáltatóknál: újabb optikai kábelek lefektetése nélkül kapacitásnövekedés
  - Pl. mai rendszereknél 160 jel összefogásával 10Gbit/s helyett 1.6Tbit/s

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hullámhossz-osztású nyalábolás (multiplexelés)



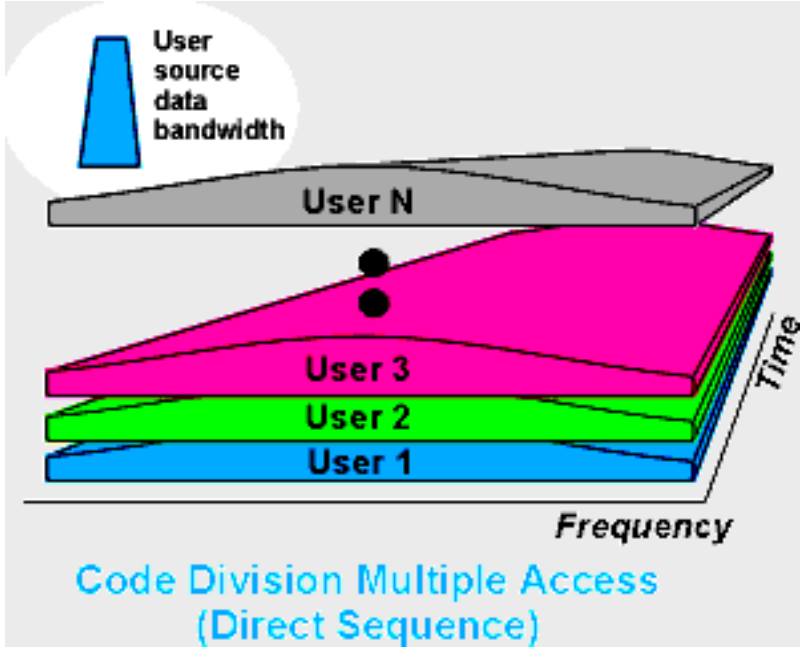
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kódosztású nyalábolás (CDM – code division multiplexing)

- A egyes csatornák jele sem frekvenciában, sem az időben nem különül el

- Hogy lehet ez?
- Akkor hogyan különböztetjük meg azokat?
- És mi az értelme ennek a furcsa „osztás”-nak?

- Nézzük az egyik módját, az ún. direct sequence CDM-et!

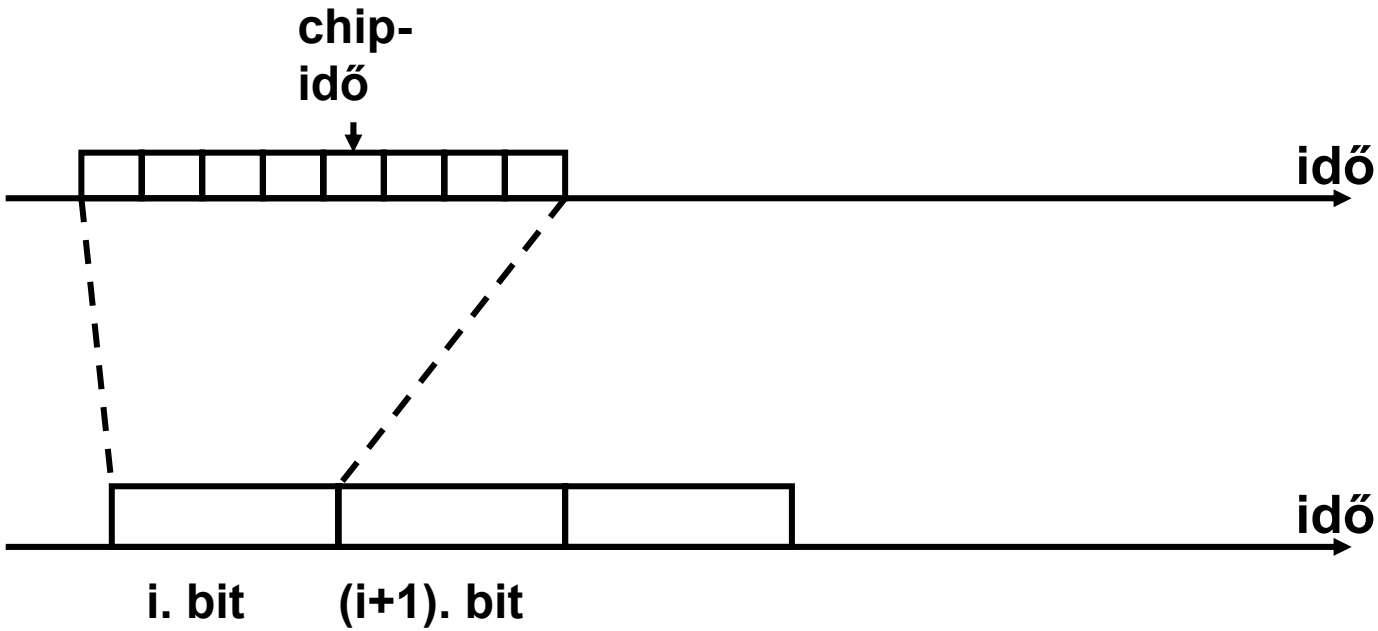


Kódosztású nyalábolás elve

- Analógia: beszélgető emberek egy helységben
  - TDM: egymást felváltva beszélnek
  - CDM: más nyelven beszélnek
- Alapelv: adatokhoz csatornánként speciális kódokat rendel (chip kód)
- Ezzel a szórt, széles sávú jellel (pszeudozaj) kerül többszörözve átvitelre a jel, vevő oldalon visszaszorozzák vele (XOR művelet)
- Minden felhasználónak saját chip kódja, legyen ortogonális a többitől

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A CDM elve és a „spektrumszórás” (spread spectrum)



Szórt spektrum előnyei-hátrányai

- +:
  - Nehezen lehallgatható, zajnak tünik a chip kód miatt
  - Nehezen blokkolható
  - Nem érzékeny a keskenysávú interferenciára illetve többutas terjedésre
  - Frekvencia újrafelhasználás pl. cellás rendszerekben
- -:
  - Nagyon pontos teljesítményszabályozás kell (közel-távol probléma)
  - Interferencia: ha nem pontos a szinkronizáció a chip határoknál
  - Bonyolultabb adó-vevő: ma már nem gond

Hol tartunk?

- Megismertük szimbólumok jelekkel történő továbbításának alapvető problémáit:
  - Véges sávszélességű csatorna → diszperzió
  - Elektromos jelek feldolgozása → additív zaj
- A forrás által küldött szimbólumok nem mindig azonosak a nyelőbe jutó szimbólumokkal
- Megismertük a jeleknek a csatorna rendelkezésre álló frekvenciasávjához történő illesztését:
  - Vonali kódolás
  - Moduláció
  - Nyalábolás (multiplexálás / multiplexelés)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

„FIZIKAI SZINTŰ” KOMMUNIKÁCIÓ

Hírközlő csatornák a gyakorlatban

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

Az előző előadáson

- Megismertük szimbólumok jelekkel történő továbbításának alapvető problémáit:
  - Véges sávszélességű csatorna → diszperzió
  - Elektromos jelek feldolgozása → additív zaj
- A forrás által küldött szimbólumok nem mindig azonosak a nyelőbe jutó szimbólumokkal
- Megismertük a jeleknek a csatorna rendelkezésre álló frekvenciasávjához történő illesztését:
  - Vonali kódolás
  - Moduláció
  - Nyalábolás (multiplexálás / multiplexelés)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hírközlő csatornák a gyakorlatban

- (Réz)vezetékes csatornák
- Fényvezetős (üvegszálas) csatornák
- Vezetéknélküli csatornák
  - szabadtéri fényátvitel
  - infravörös átvitel
  - rádiós átvitel
    - földfelszíni
    - műholdas
    - ezen belül mobil

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Jeltovábbítás fémvezetőkkel

- Két fémvezető és köztük dielektromos szigetelés
  - levegő is lehet: légvezeték
- Szakszerű elnevezés: TEM-hullámvezető (**t**ranszverzális **e**lektromos-**m**ágneses)
- Fő típusai:
  - Szimmetrikus érpár
    - sodrott érpár
  - Koaxiális kábel

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Sodrott érpár (Twisted pair)

- Két szigetelt, egymásra spirálisan felcsavart rézvezeték
  - UTP: árnyékolatlan (unshielded)
- A csavarás a két ér egymásra hatását küszöböli ki, illetve más külső EMI zavarokat
  - belső: crosstalk EMI
  - külső: pl. másik UTP pár
- Minél sűrűbb a csavarás, annál nagyobb az adatátviteli sebesség (és a méterenkénti ár is)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Sodrott érpárak

3-as kategóriájú sodrott érpár, árnyékolatlan
Cat3 UTP (unshielded twisted pair) – kb. 16 MHz-ig

4 érpár egy kábelben

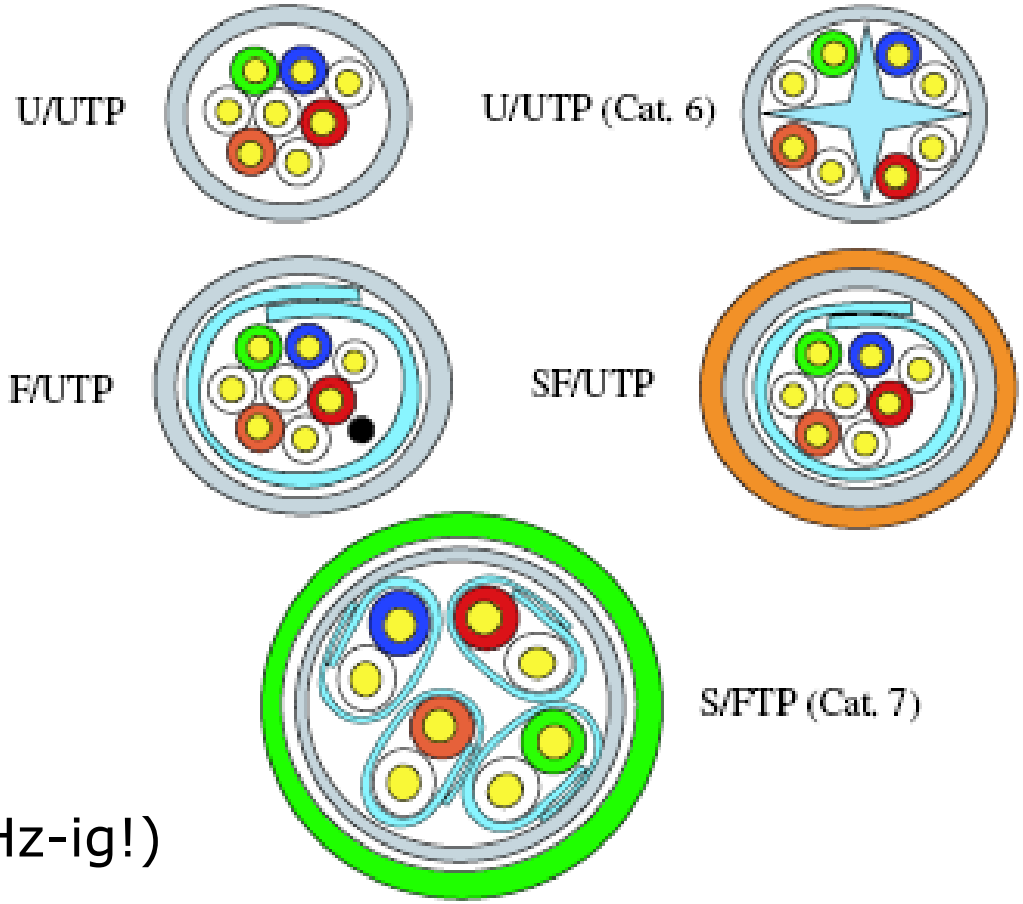
5-ös kategóriájú árnyékolatlan sodrott érpár
- kb. 100 MHz-ig

sűrűbb sodrás, jobb átviteli jellemzők

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Sodrott érpáras kábelek

Jelölések:
S – shielded (fémhálóval)
F – foiled (árnyékolás fémlemezzel)



Cat6, Cat7:
újabb, még nagyobb sávsz.
nem terjedtek el
(250 illetve 600 MHz-ig!)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

UTP előnye-hátránya

- +:
  - Vékony, rugalmas kábel: könnyű szerelés
  - Mérete miatt sok fér el belőle egy burkoló csatornában
  - A legolcsóbb LAN kábel
- -:
  - Komoly előírások a szereléskor az EMI miatt
  - Video átvitelnél a különböző hosszak miatt késleltetés
    - Átvitel párhuzamosan több éren: színtorzulás, szellemkép
    - Túloldalon kompenzálni kell a változó hosszakat, bonyolult

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Strukturált kábelezés

- Döntően UTP-kábelezést használ
- Strukturált: központi elosztókból (ún. rendezőkből) minden végponthoz külön kábel megy
  - szemben pl. a végpontok felfűzésével egy kábelre
- Általános célú, telefon- és számítógép-hálózat kialakítására egyaránt alkalmas
- A végpontról nem kell előre eldönteni, hogy mit fogunk arra csatlakoztatni
- Könnyű átkonfigurálhatóság

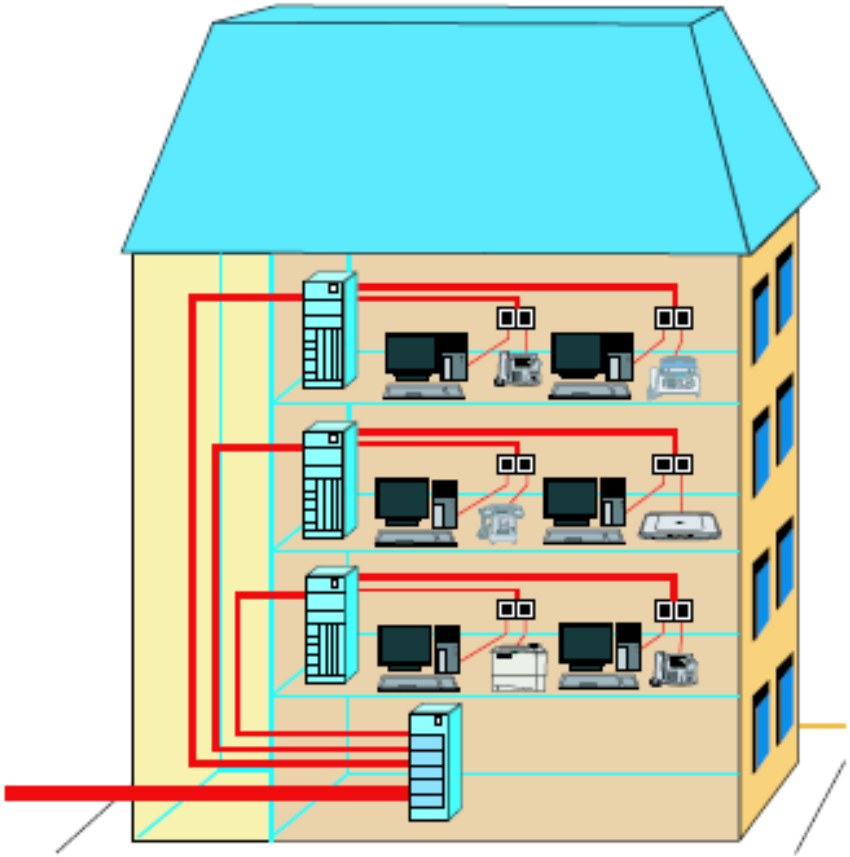
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A strukturált kábelezés fő elemei

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

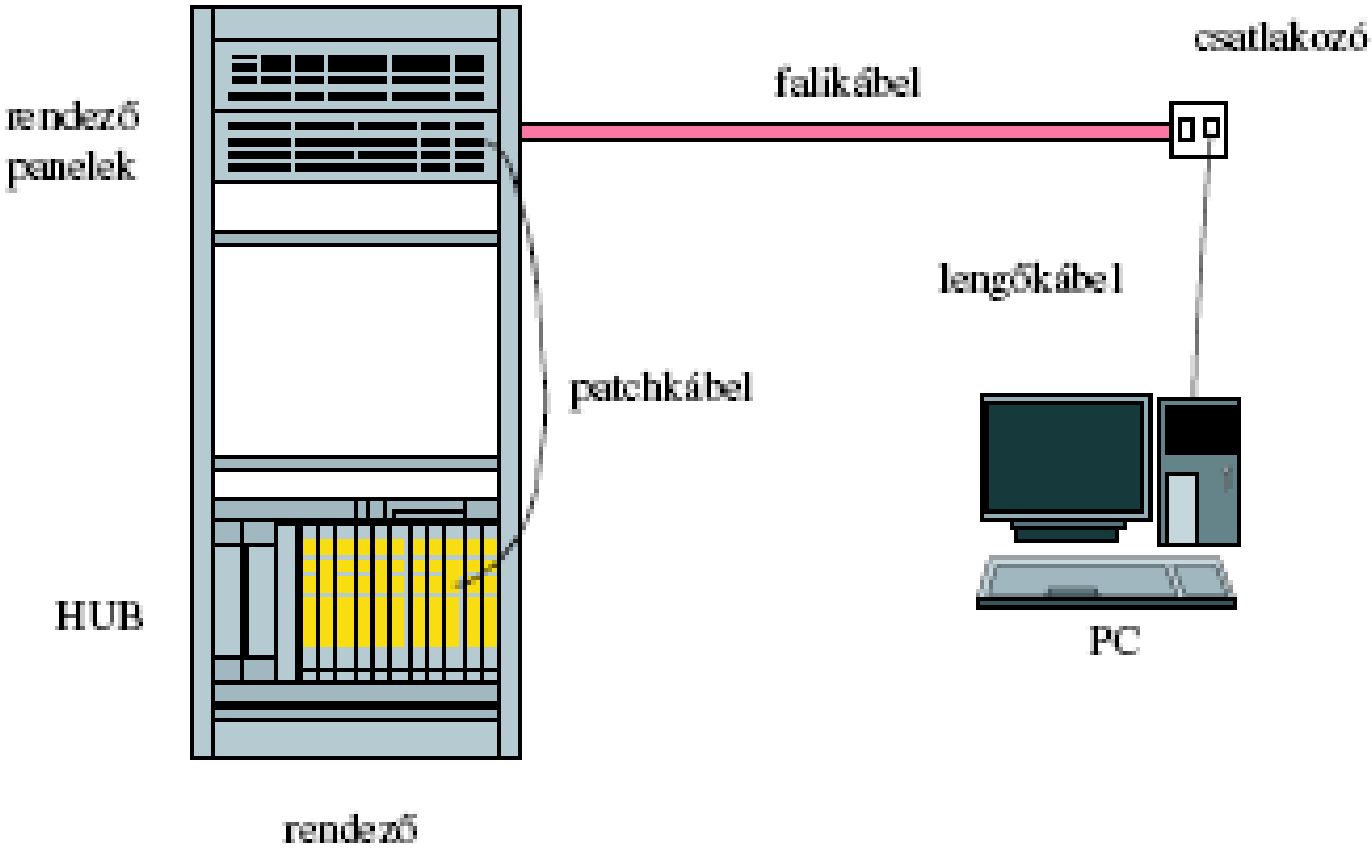
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Illusztráció:
Strukturált kábelezés többszintű épületben



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Illusztráció: a strukturált kábelezési rendszer elemei



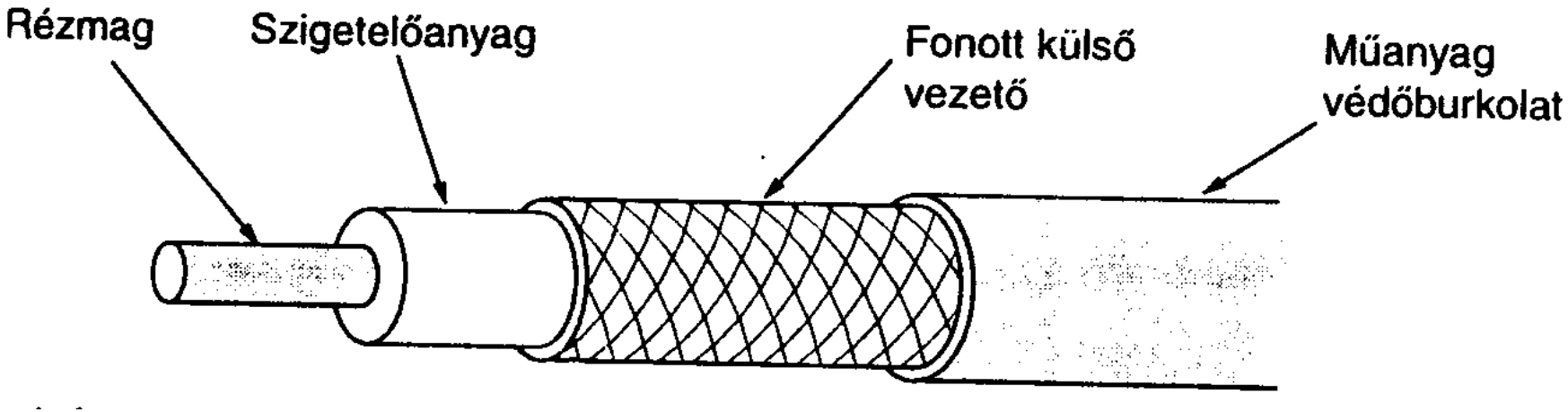
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Koaxiális kábelek

- Amennyiben egy vezeték magas frekvenciájú áramot visz át: antenna viselkedés
- Koaxiális kábel: egyik vezető körüleli a másikat, nincs kimenő rádió hullám a belsőből
  - Külső pedig le van földelve
- Ha változik a külső és belső közötti távolság: állóhullám alakulhat ki
  - Ezért közöttük félmerev műanyag dielektrikum

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Koaxiális kábelek

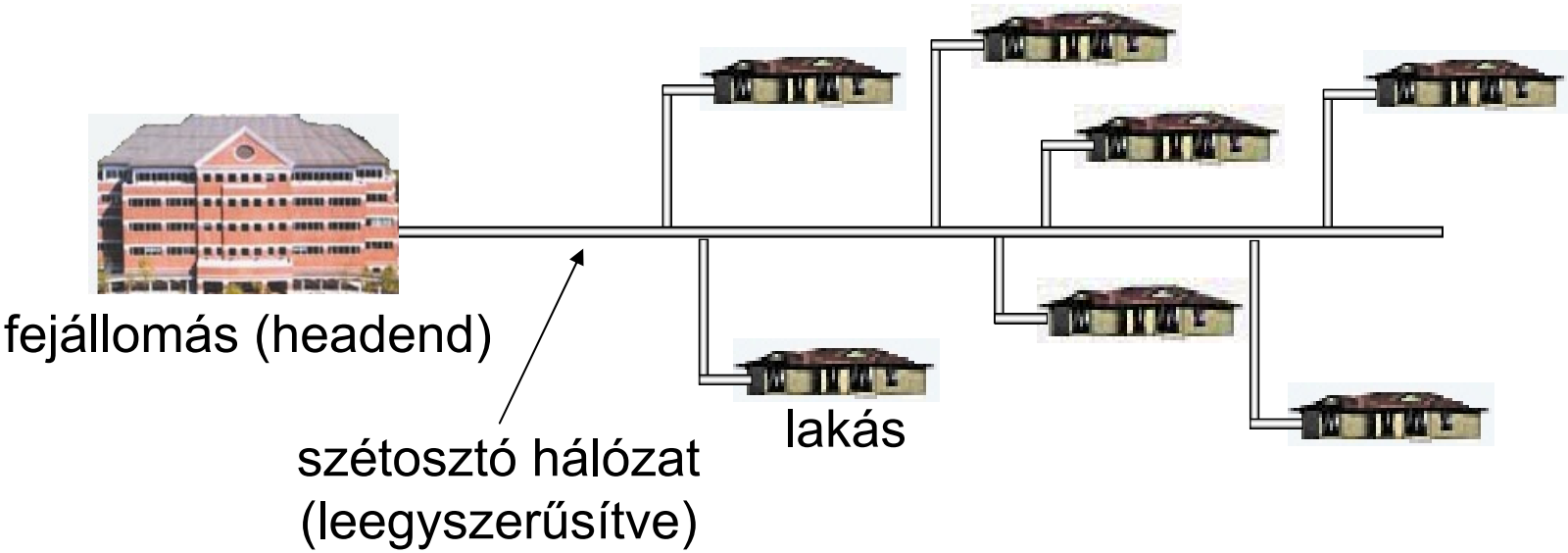


- Két végén lezárás a hullámimpedanciával (50 Ohm Ethernet, 75 Ohm kábel tv)
- Jó zavarvédettség és nagy sávszélesség
- Számítógép-hálózatokban ma már kevésbé használják
  - kábeltelevíziós rendszerekben fordul elő
  - vagy az optikai (fényvezetős) átvitel szorítja ki, vagy kis távolságok esetén a sodrott érpár

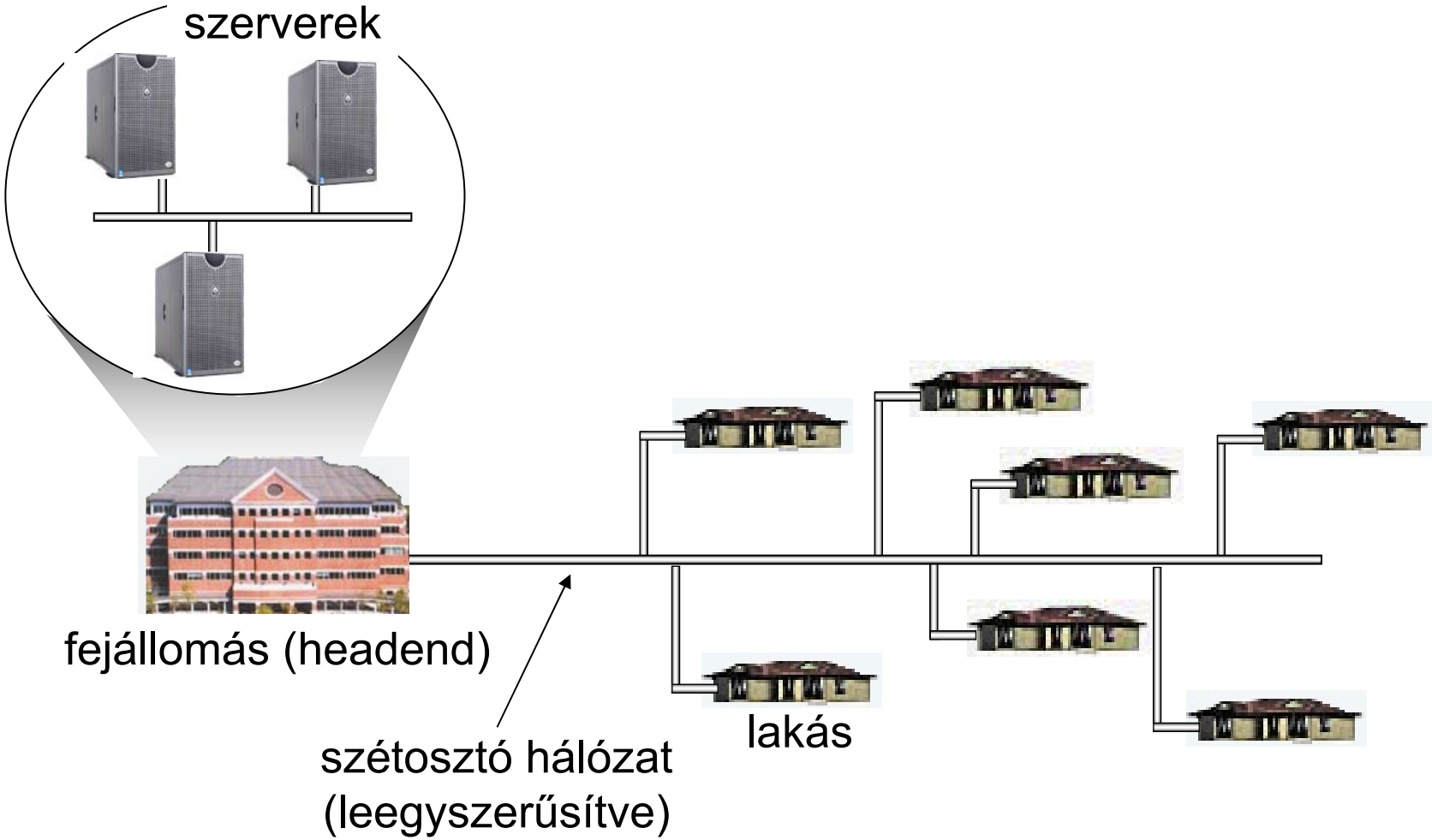
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kábeltévé-hálózat

Tipikusan 500...5000 lakás

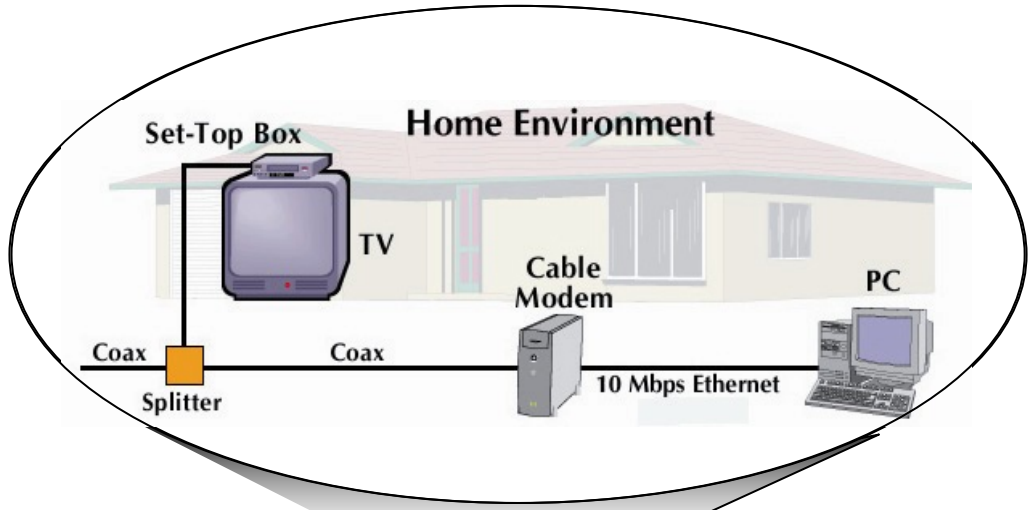


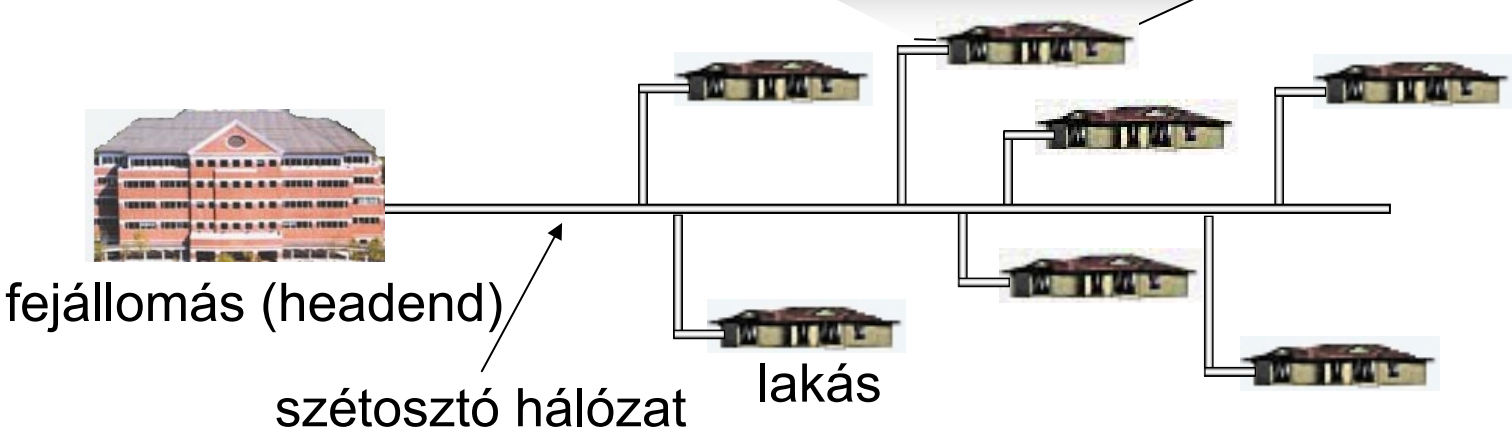
Kábeltévé-hálózat



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

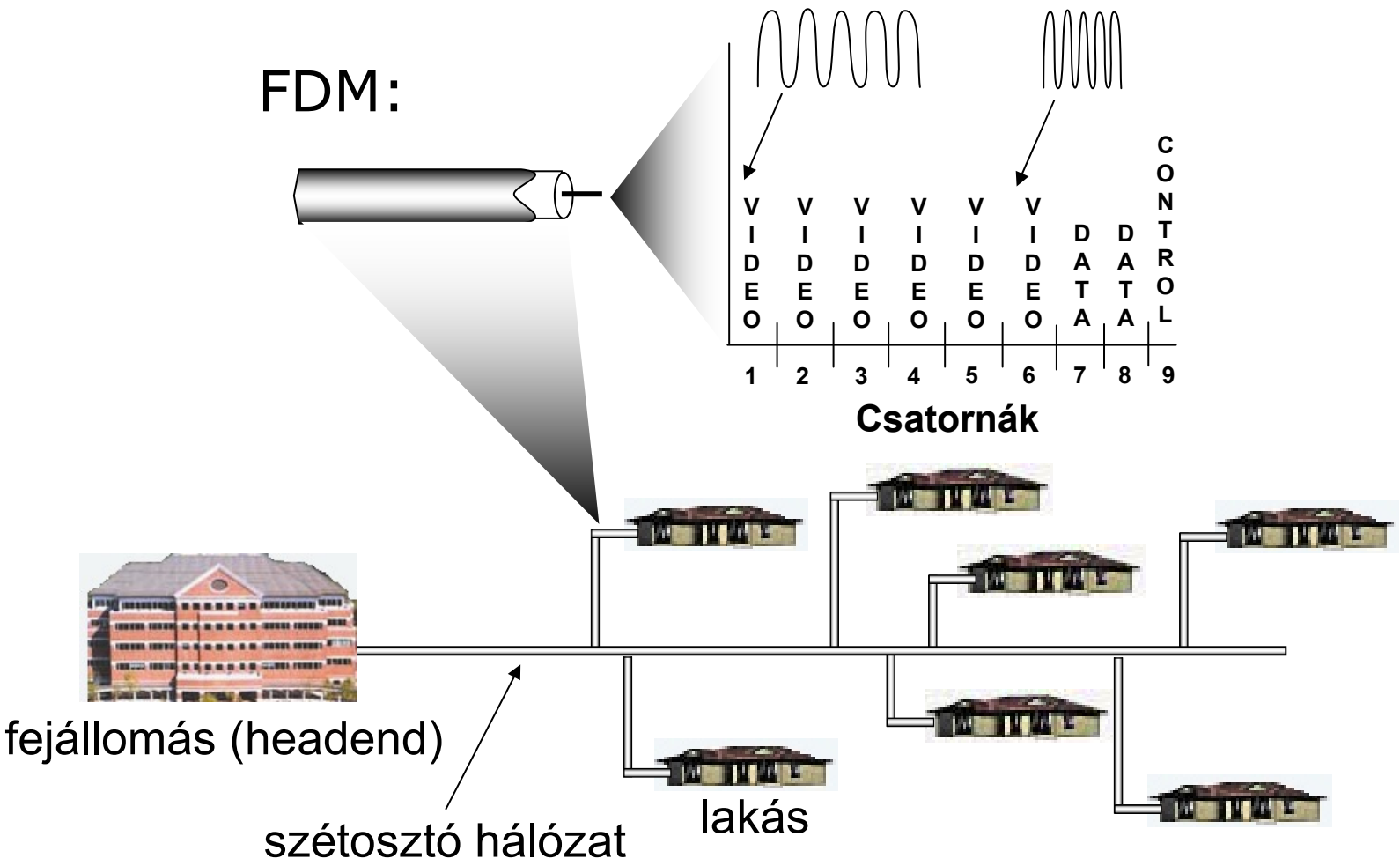
Kábeltévé-hálózat





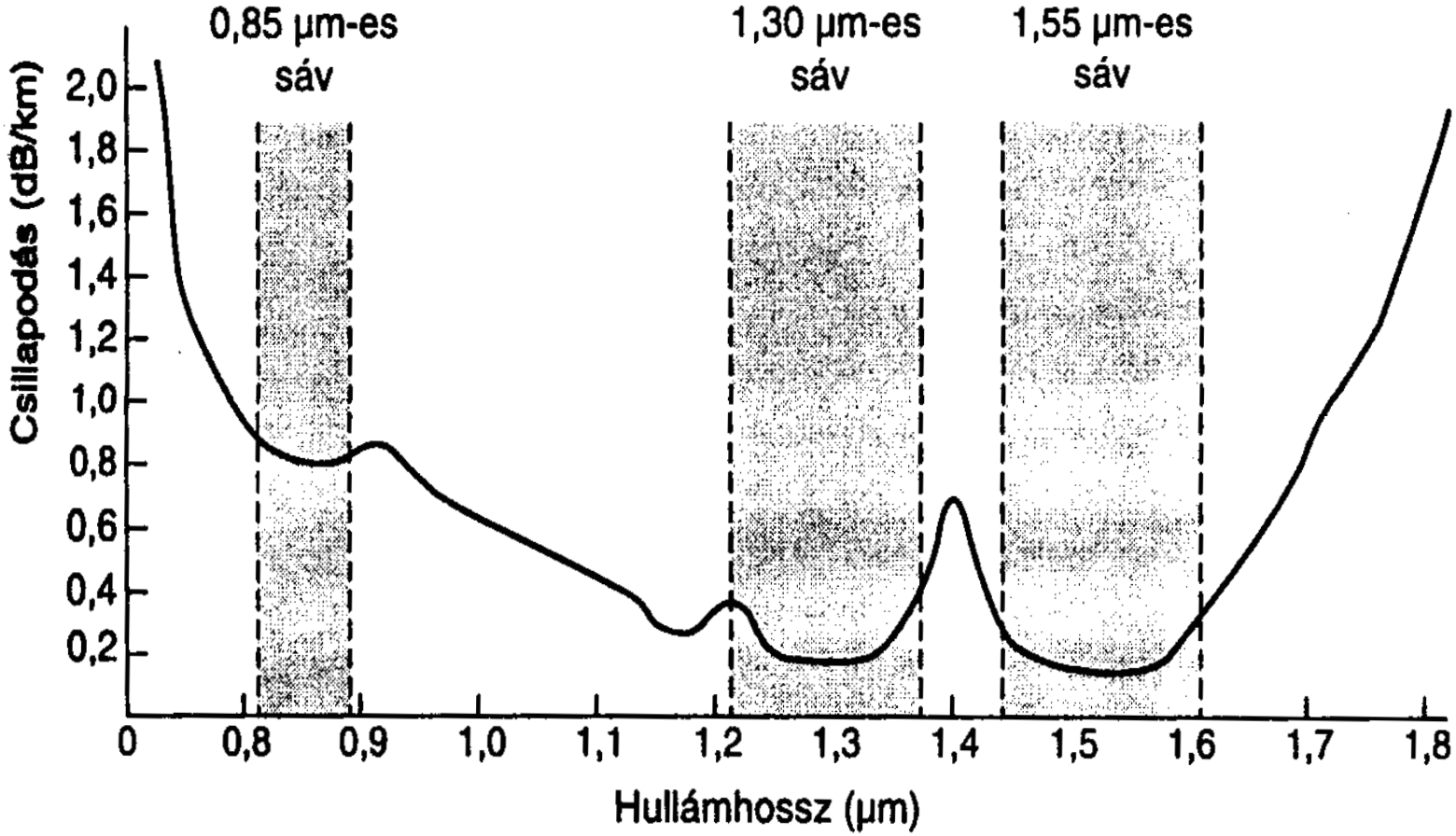
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kábeltévé-hálózat



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Átvitel a látható fény tartományában: optikai „ablakok”



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Optikai „ablakok”

- **850 nm**
  - optikai távközlő rendszerek első generációja a 70-es évek végén.
  - 2-3 dB/km-es szálcsillapítás jellemzi
  - elérhető modulációs sebesség 100Mbit/s nagyságrendű
- **1310 nm**
  - a 80-as évek közepére második generációs rendszerek
  - 0.5 dB/km-es szálcsillapítás
  - átviteli sebesség Gbit/s-os nagyságrendbe nőtt
  - optikai szálnak itt van diszperziós minimuma
- **1550 nm**
  - ideális abszorbció szempontjából
  - 0.2 dB/km-es szálcsillapítás
  - néhányszor 10 Gbit/s-os nagyságrendű sebesség
  - hullámhosszosztásos (WDM – Wavelength Division Multiplex) rendszerek
    - sávszélesség 120 nm, ami 15 THz frekvenciasávnak felel meg!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

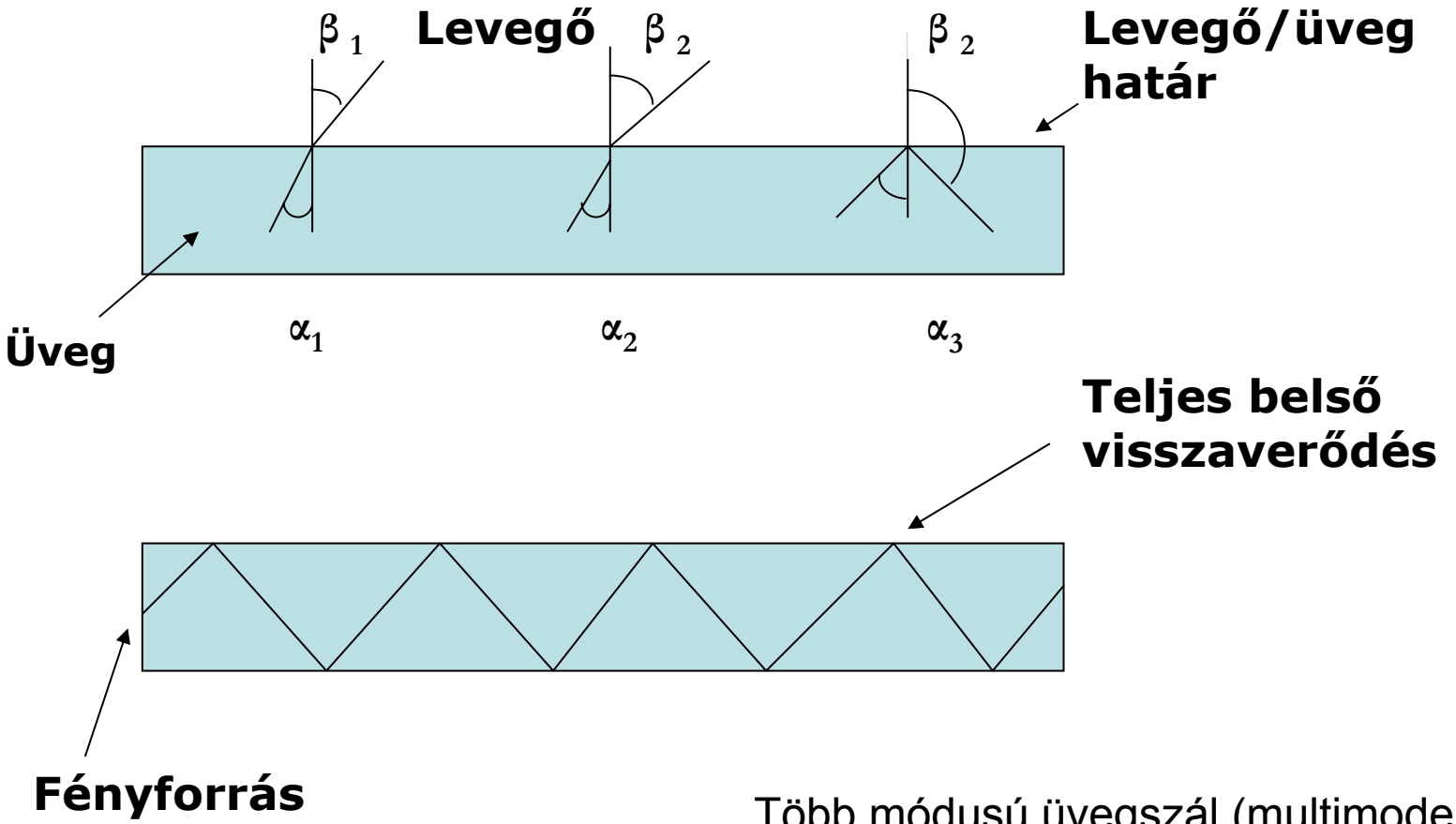
Veszteségek

A fényveszteség három részből áll:

- Két közeg határán bekövetkező visszaverődés (reflexió)
  - határfelületek gondos összeillesztésével minimálisra csökkenthető
- Közegben létrejövő csillapítás
  - megfelelő anyagválasztással minimalizálható
- Közegek határfelületén átlépő fénysugarak
  - fénytörés (refrakció)
  - teljes visszaverődés jelensége!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

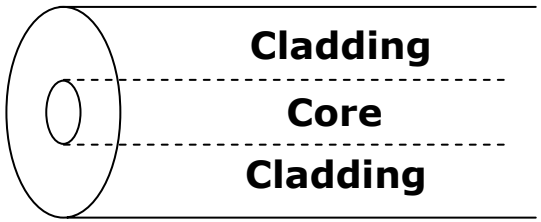
Terjedés üvegszálban



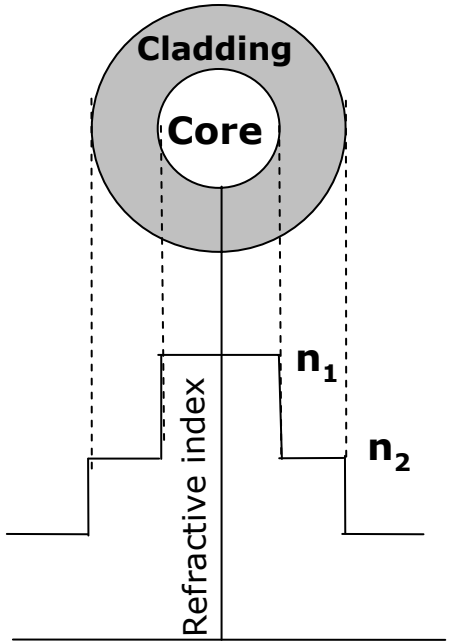
Több módusú üvegszál (multimode fiber)

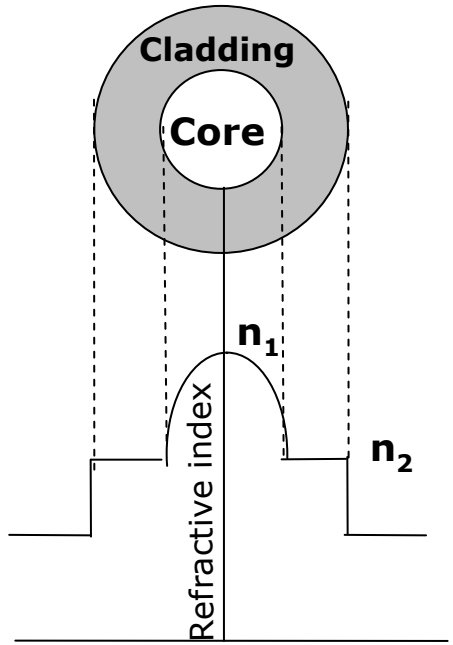
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Optikai szál



Core and cladding
(Mag és héj)

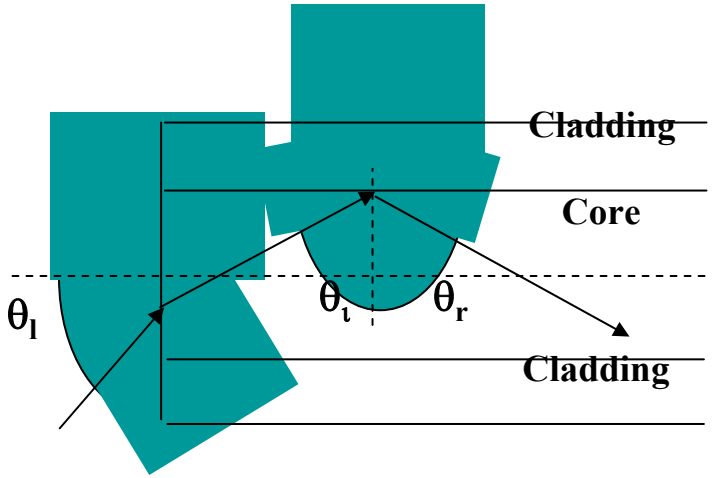


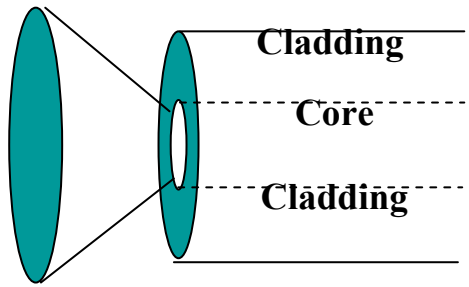


a) step-index fiber (ugrásszerű törésmutató változás)
b) graded-index fiber (fokozatos törésmutató változás)

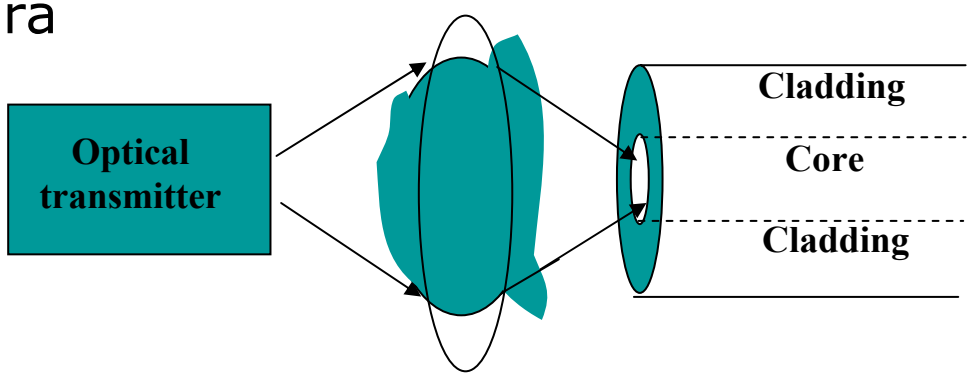
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A fénysugár betáplálása a szálba





Numerikus apertúra



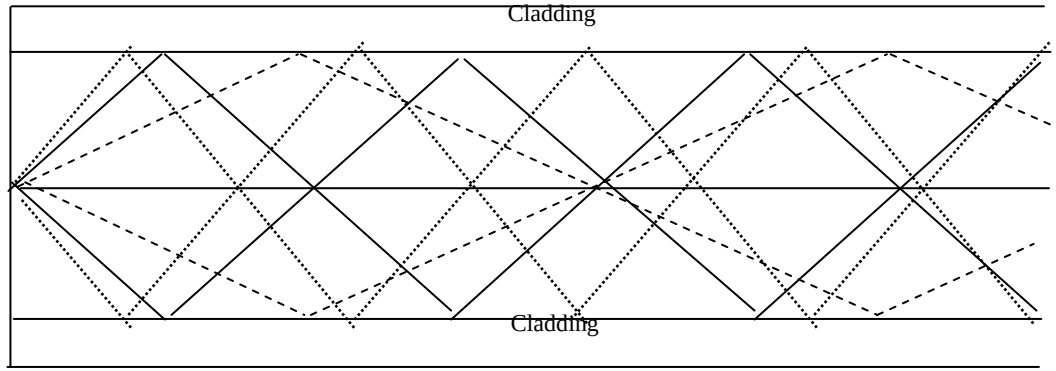
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Multimódusú és monomódusú szálak

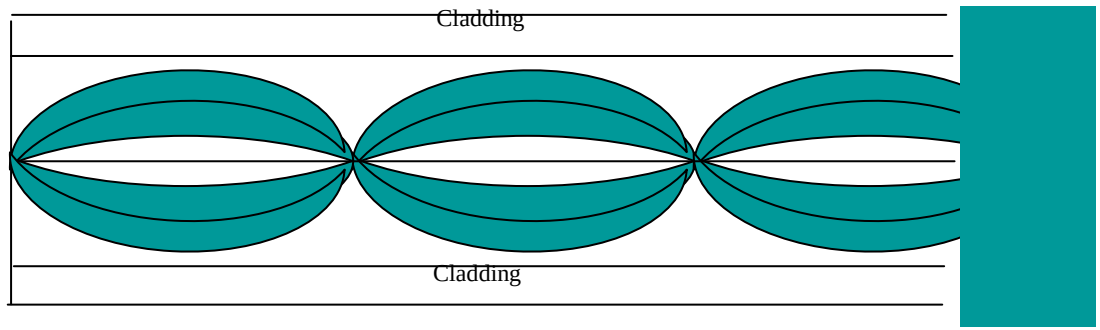
- A mag/héj (core/cladding) értékek a multimódusú szálban:
  - 50/125 μm,
  - 62,5/125 μm,
  - 100/140 μm
- Monomódusú szál esetén:
  - 9 vagy 10 / 125 μm

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A módusok kialakulása

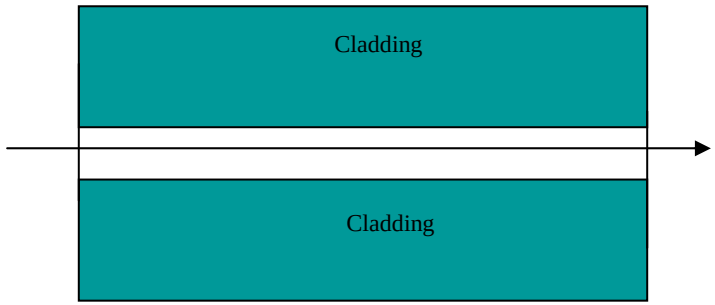


a) step-index fiber



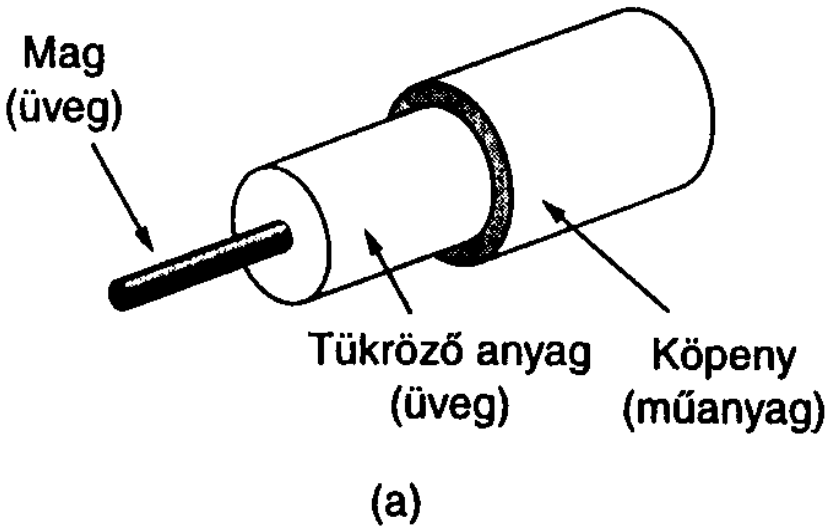
b) graded-index fiber

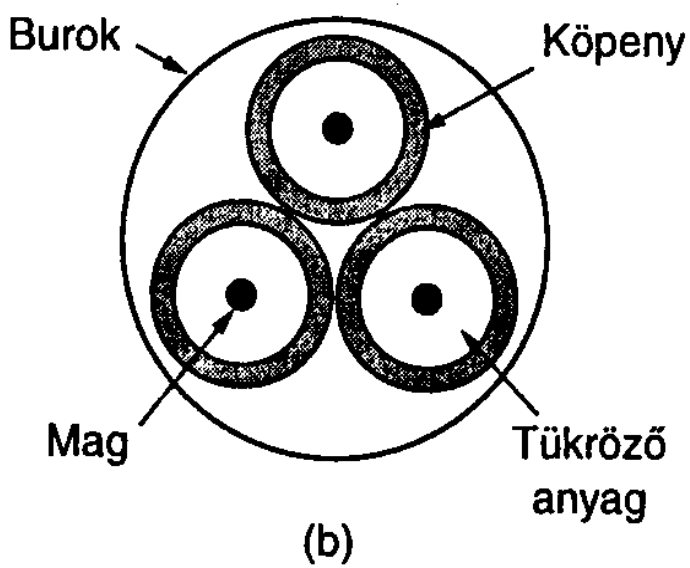
Monomódusú szál



Ha a **mag átmérõjét a fény hullámhosszára** csökkentjük, akkor a fénysugár már verődés nélkül terjed: csak alapmódus terjed!

Üvegszálas kábelek konstrukciója





© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

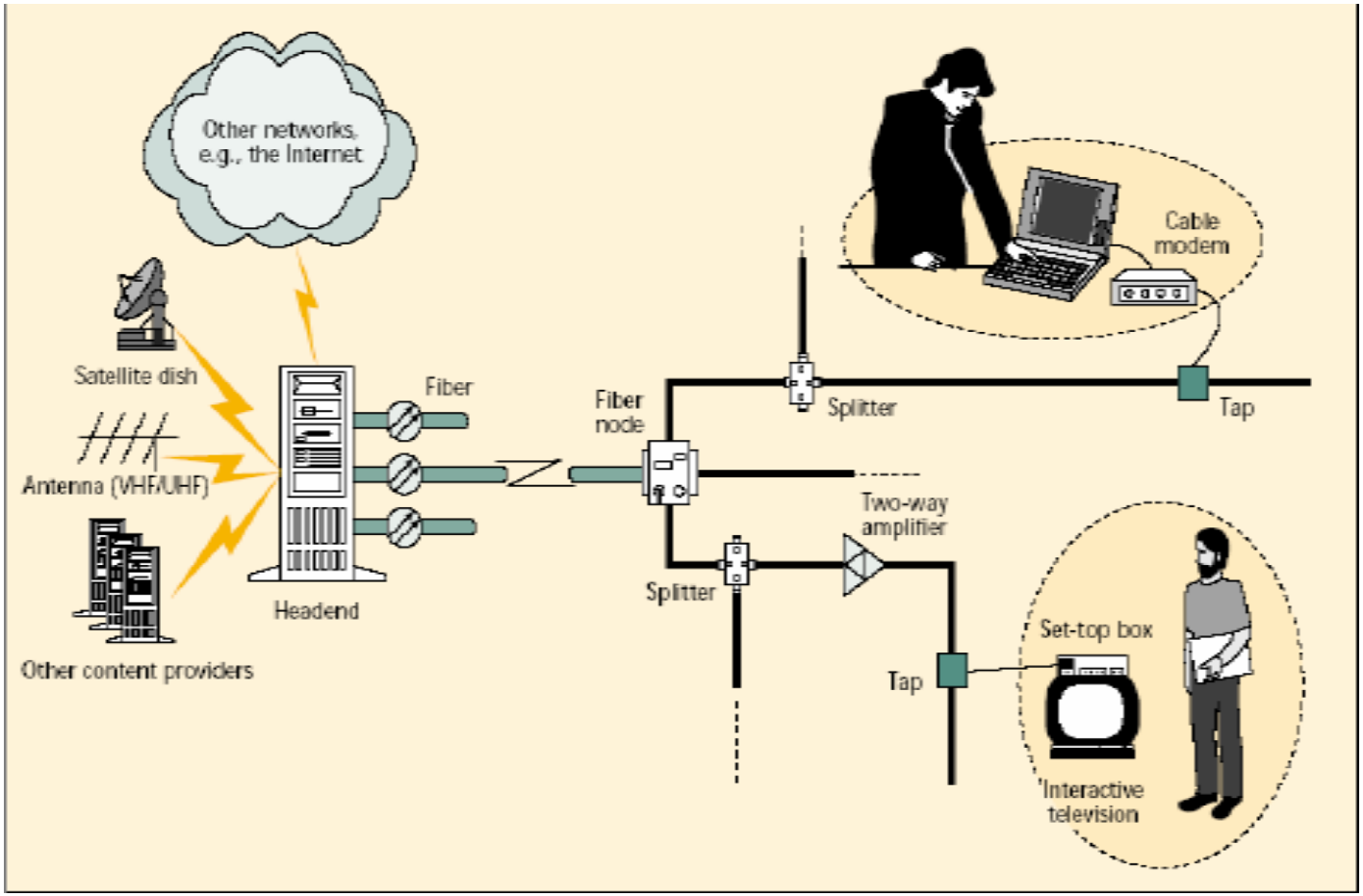
Optikai hálózati elemek

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

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

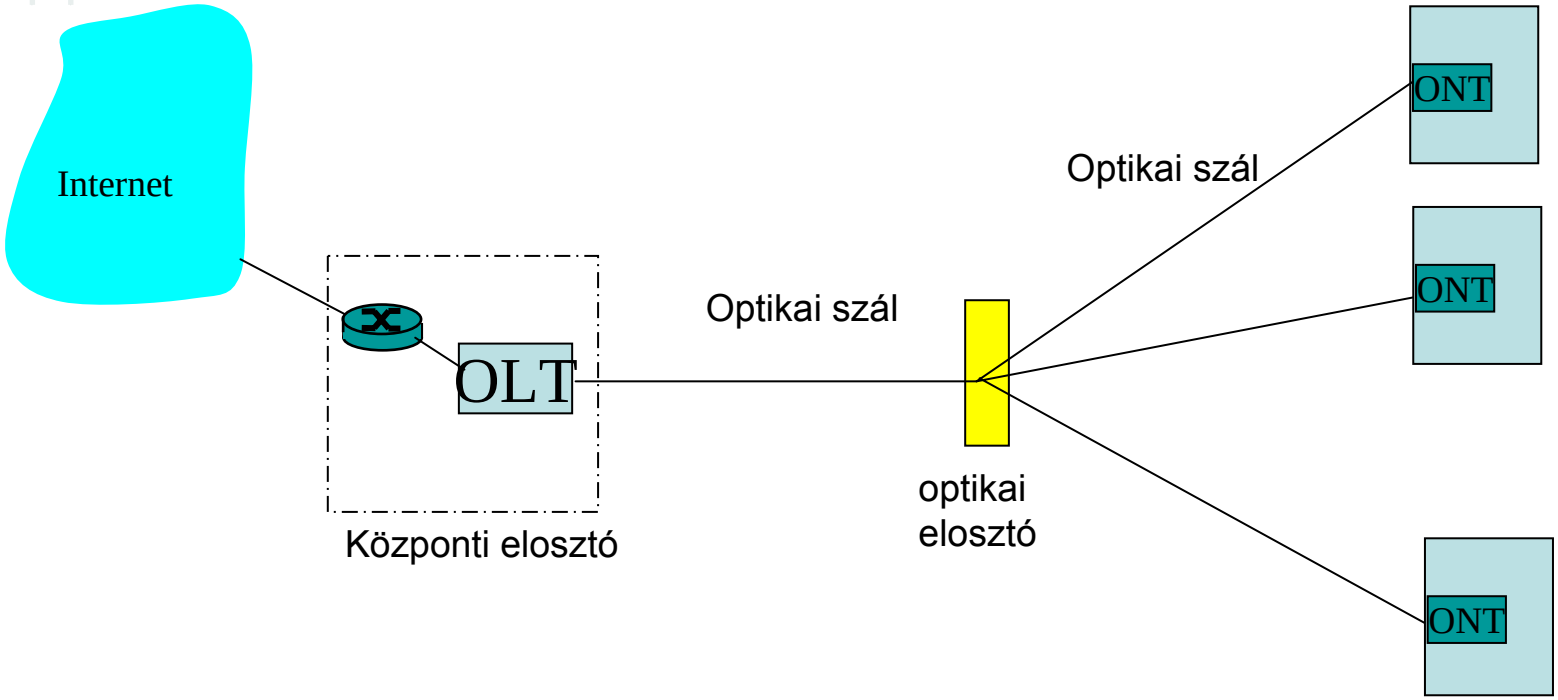
Példa üvegkábeles hálózatra: HFC

Hybrid fiber coax



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fiber to the Home (FTTH)



- Optikai szál a központi elosztótól az otthonig
- ONT: Optical network terminator
- OLT: Optical line terminator
- Magas adatátviteli sebességek: TV szolgáltatás, telefon, Internet

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mono vs. multimódusú

Monomódusú

+

- : nincs módusdiszperzió
  - de van kromatikus és polarizációs!

-:

- kábel olcsóbb, de adó-vevővel drágább
- nagy optikai teljesítmény esetén szálégés

- Általában: kis távolságokra multimódusú (<500m), nagyobbra mono

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Optikai átvitel előnyei

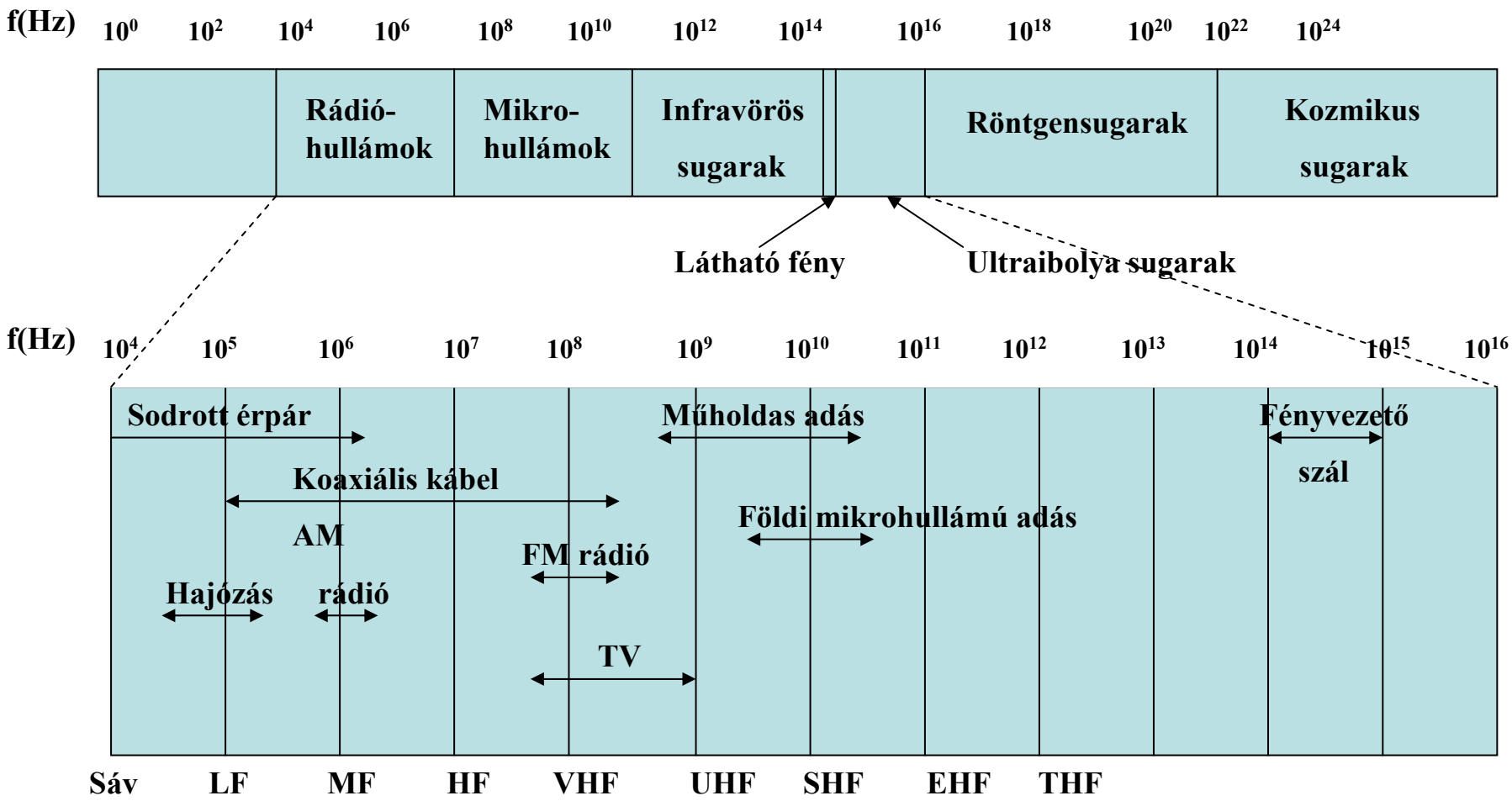
- +:
  - Nagy távolságokra nagy sávszélesség
  - Nincs EMI, kisebb csillapitás mint fémvezetéknél: kevesebb ismétlőállomás
  - Megbízhatóbb, mint a fémvezeték, lehallgatása költséges, könnyen felfedezhető
- -:
  - Diszperzió
    - Kromatikus
      - különböző hullámhosszú nyalábok különböző sebességgel terjednek
    - Módus
      - eltérő utak
    - Felső korlátot jelent az átvihető sávszélességre és maximális távolságra!
      - Mhz km
      - Rekord: Bell Labs (Fr): 155 multiplexelt csatorna, egyenként 100 Gb/s, 7000 km-en (100 Petabit/s/km, 400 DVD másodpercenként Párizs és Chicago között☺)

Rádiócsatornák

- Az elektromágneses hullámtartomány: az ultrahang- és a látható fény tartományai között rész
- Igen széles, és nem teljesen kihasznált sáv: ~10 kHz-től ~1 THz-ig (terahertz: 10^{12} Hz)
- Hullámterjedés a szabadban
- Az elektromos jel átalakítása elektromágneses hullámmá és viszont: adó- és vevő-antennák
- A hullámhossz nagyságrendjébe eső méretű antennák kellenek
- Az antennák fő jellemzője: **antennanyereség**
  - az antenna a fő sugárzási irányában hányszoros teljesítménysűrűséggel (térerővel) sugároz egy ugyanakkora teljesítménnyel táplált izotrop antennához képest (dB-ben)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az elektromágneses hullámtartomány



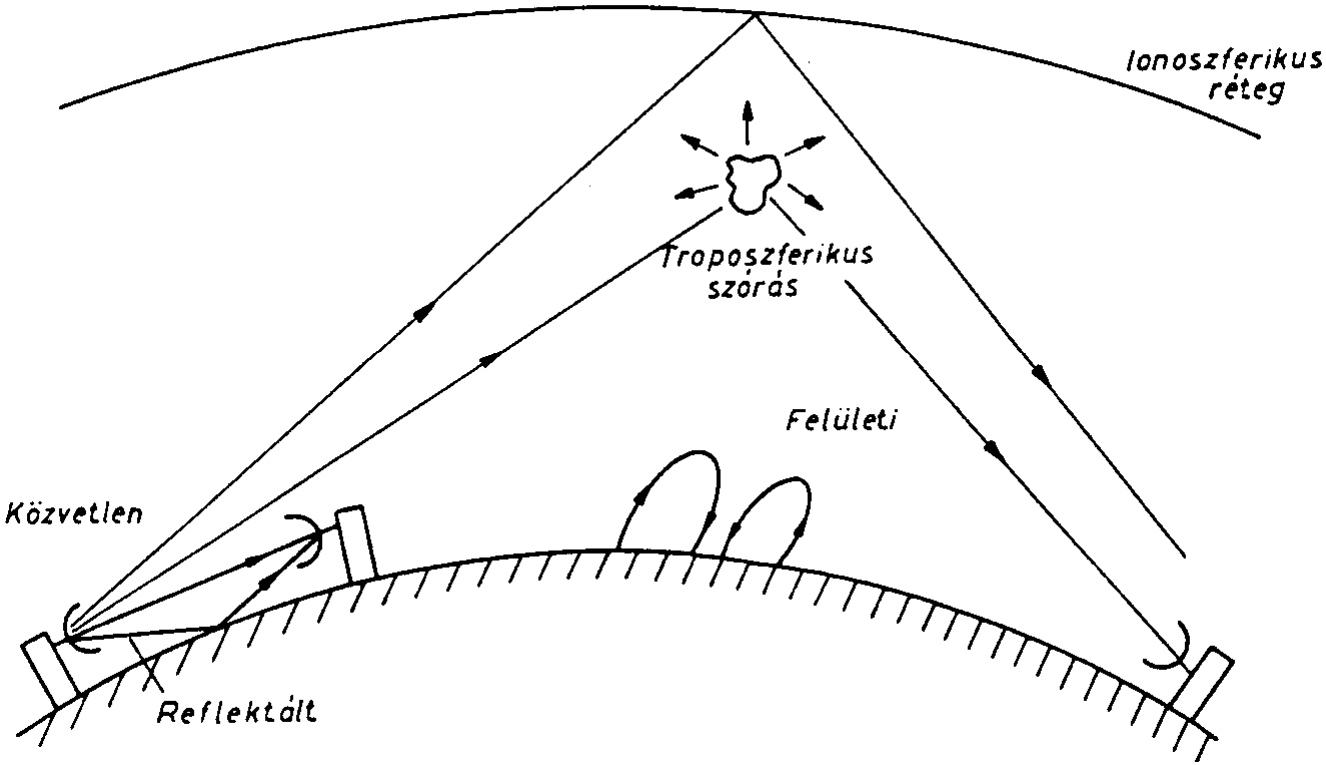
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A hullámterjedést befolyásoló jelenségek

- szabadtéri csillapítás
  - a távolság négyzetével fordítottan arányos
- visszaverődés (reflexió)
  - bármilyen közegről, amely az adott frekvenciasávban visszaverő felületként szerepel
- törés (refrakció)
- elhajlás (diffrakció)
- szóródás (scattering)
  - az adott hullámhossznak megfelelő méretű részecskéket tartalmazó közegben, pl. troposzféra

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fő hullámterjedési módok



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Zajok és zavarok a rádiócsatornában

- A rádiócsatorna „nyitottsága”
- Zajok
  - termikus zaj a vevő bemenetén
  - atmoszférikus zajok
  - kozmikus zaj, galaktikus zaj
- Zavarok
  - ipari zajok, zavarok
  - más rádiórendszerekből származó zavarok
- Sokszor ezek együttes hatásával kell számolni

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Műholdas rádiócsatorna: csillapítás- és zajviszonyok

- A vett jel nagyságát alapvetően a szabadtéri csillapítás befolyásolja
- Az adó- és a vevőantennák nyereségével lehet javítani
  - az antennák „irányítottak”
  - antennanyereség: a fő sugárzási irányba eső telj. sűrűség per az izotróp sugárzó telj. sűrűsége
- A zaj döntően a vevőkészülék bemenetén jelentkező termikus zaj
  - kismértékben a vett jelhez a csatornában adódott zajok és zavarok (kozmikus zaj, ipari zajok és zavarok)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Frekvenciagazdálkodás

- A rádiócsatorna nyitottsága miatt kritikus a frekvenciasávok felosztása a felhasználók között

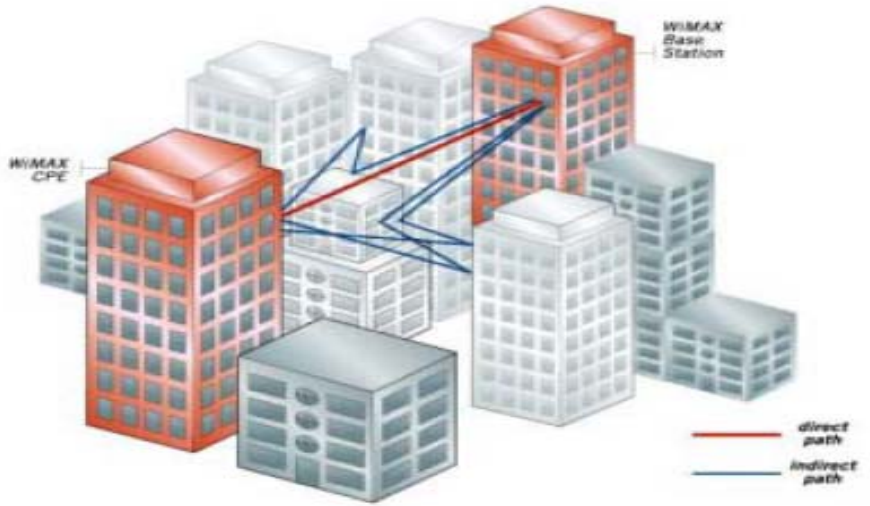
- Engedélyköteles és engedélyhez nem kötött sávok
  - Általában: engedély kell, kivétel:
  - ISM-sáv (industrial, scientific, medical)
    - ~2,4 GHz, ~5,6 GHz

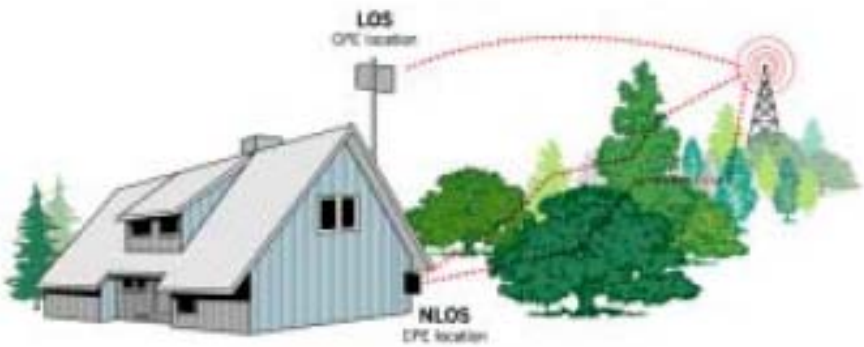
- A szabályozás többszintű:
  - globális, Nemzetközi Rádiószabályzat
  - regionális, pl. EU irányelvek
  - nemzeti, Mo-n az NMHH (Nemzeti Média- és Hírközlési Hatóság)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Közvetlen rálátásos és rálátás nélküli összeköttetések

Nagyvárosi környezet: visszaverődések az épületekről, az épületek árnyékoló hatása

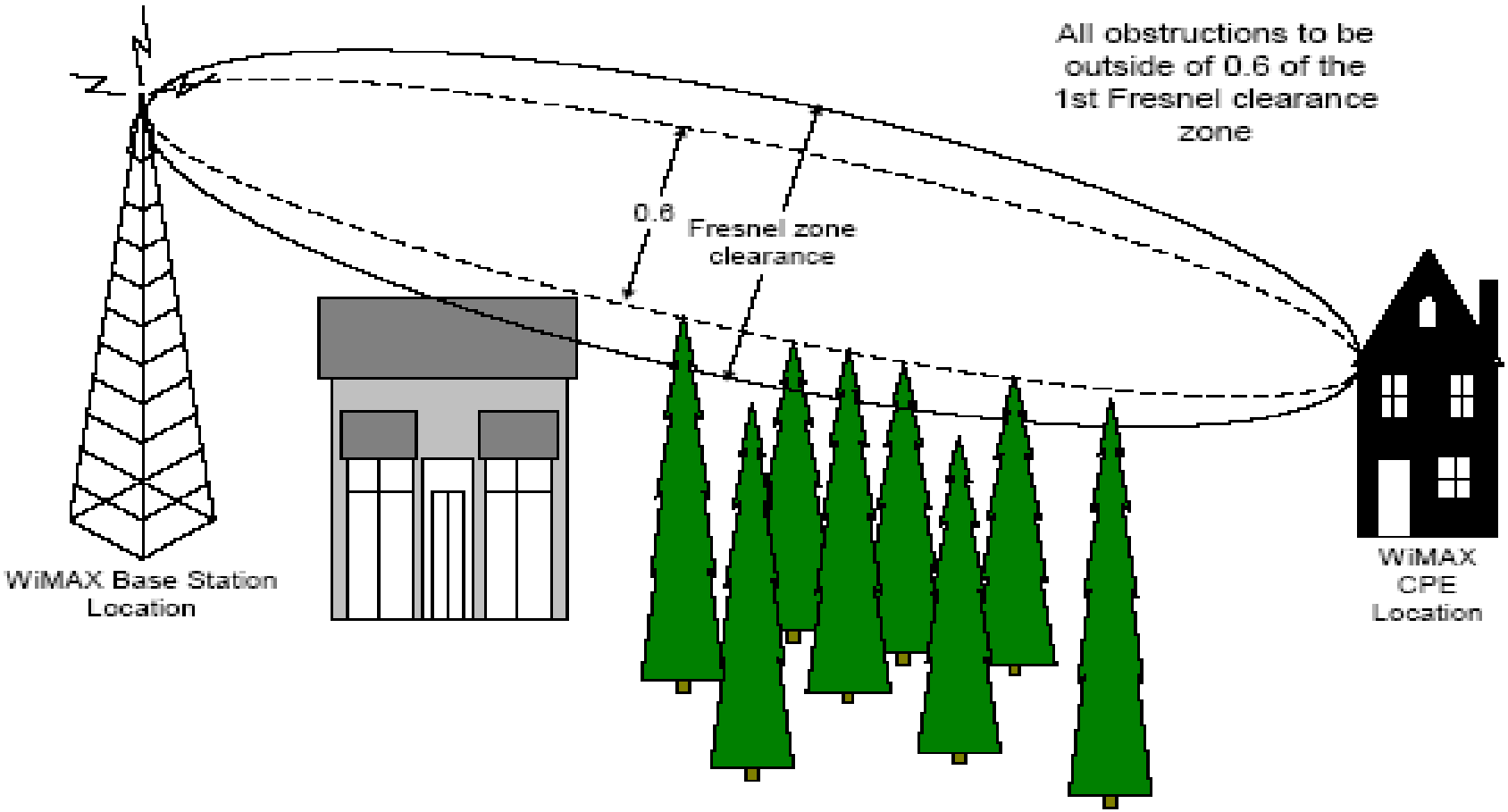




Rurális környezet: csillapítás a növényzet miatt

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A közvetlen rálátás definíciója a Fresnel-zónák alapján



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

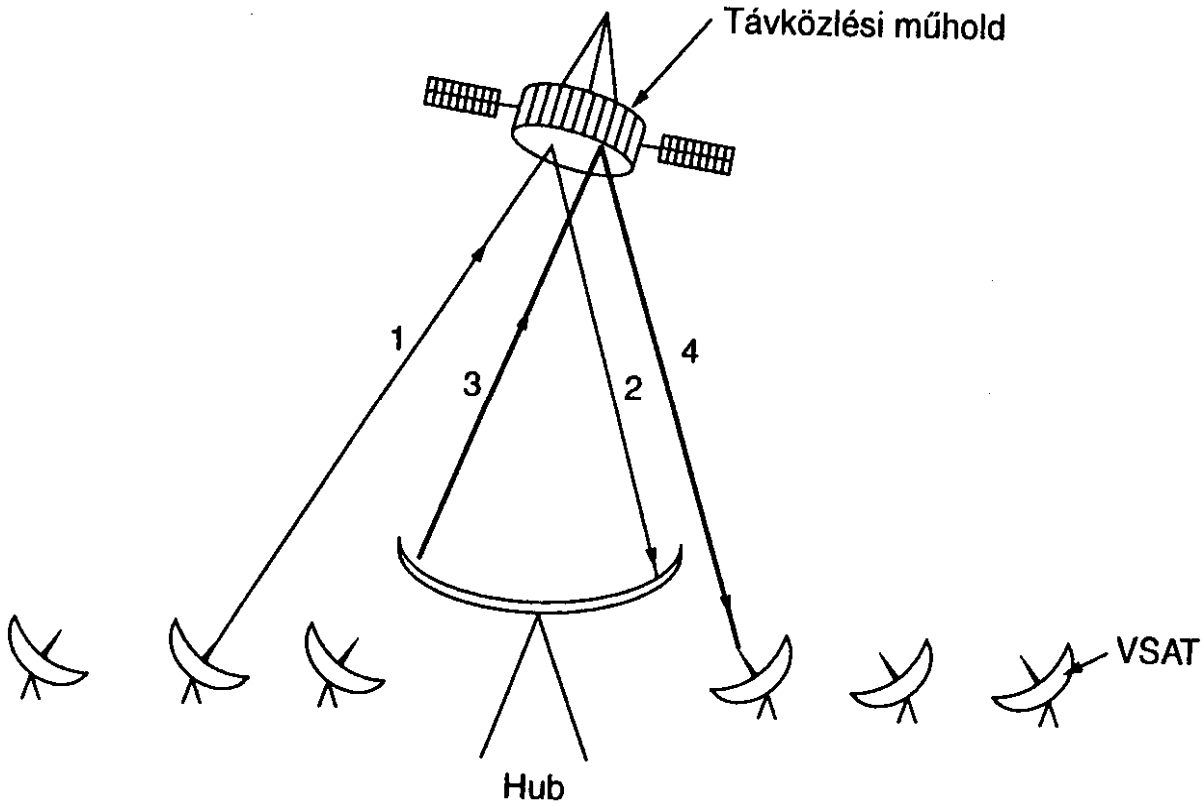
A többutas terjedés és következményei

- A különböző utakon terjedő jelek időben eltolva érkeznek a vevőbe, gyengítik egymást
  - a jelenség régi ismerős: **fading** (elhalkulás) a rövidhullámú rádiózásnál

- A többutas terjedés hatásának csökkentése: többszörös vétel
  - **diversity** az eljárás neve
  - több antenna és vevő egyidejűleg, és optimális kombinálás: **tér-diversity**
  - adás és vétel párhuzamosan több frekvencián: **frekvencia-diversity**

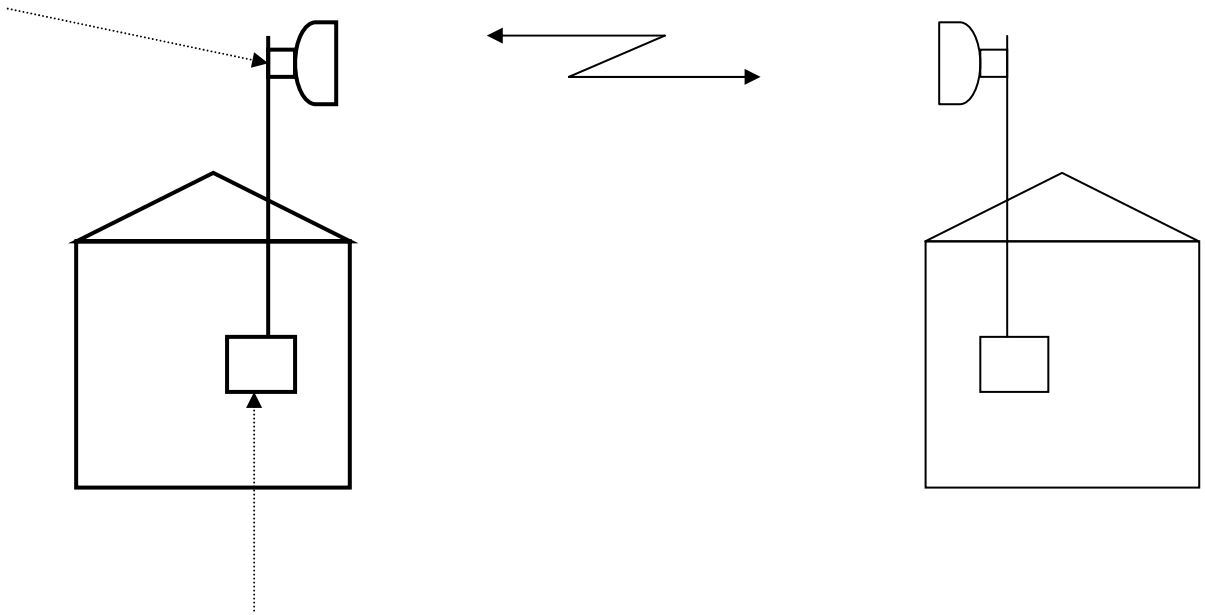
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa: műholdas terminálhálózat, „hub” alkalmazásával



Példa: földfelszíni pont-pont mikrohullámú összeköttetés

Kültéri egység



Beltéri egység

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

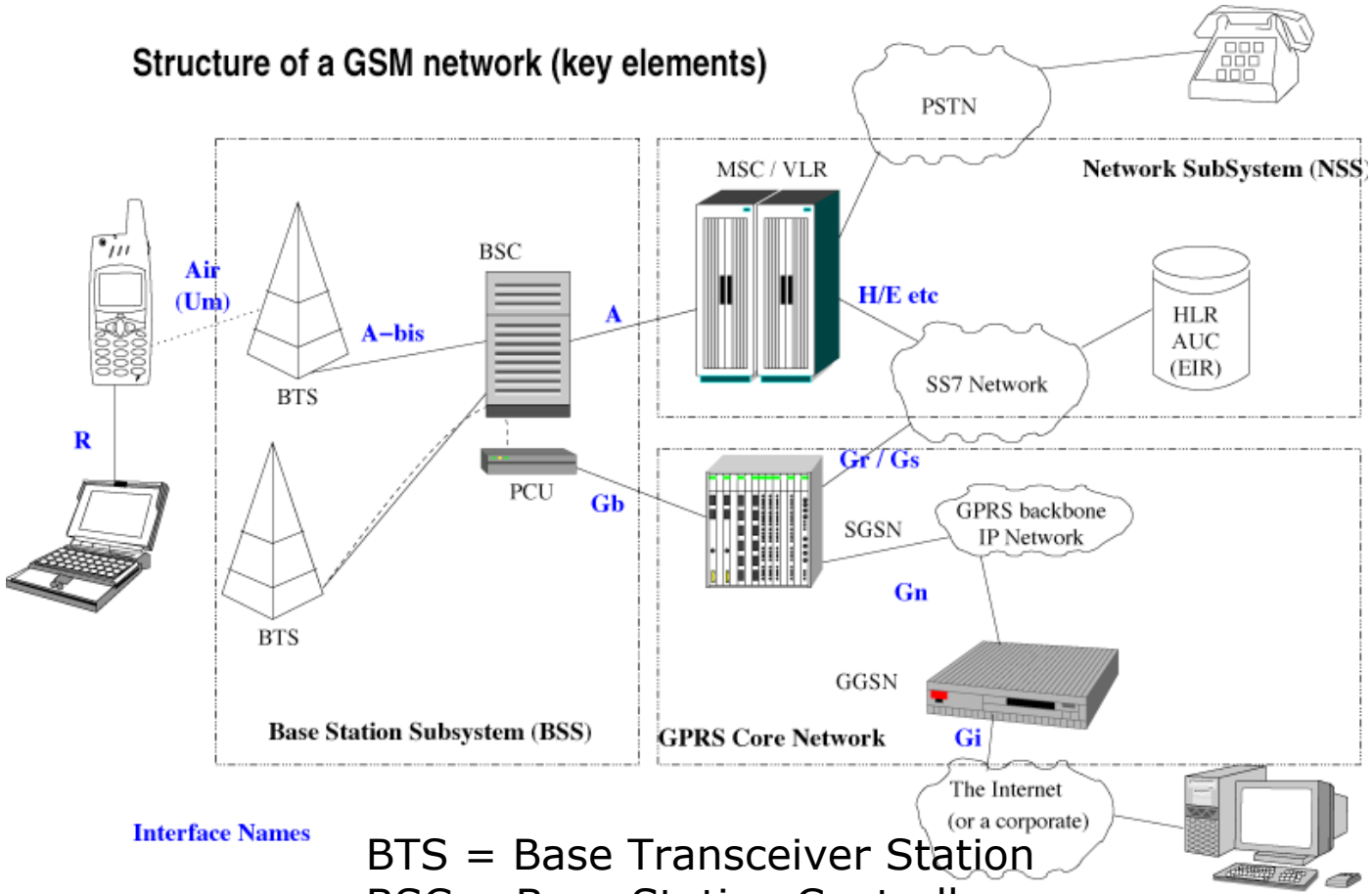
Példa: földfelszíni pont-pont mikrohullámú összeköttetés

Kültéri egység

Beltéri egység

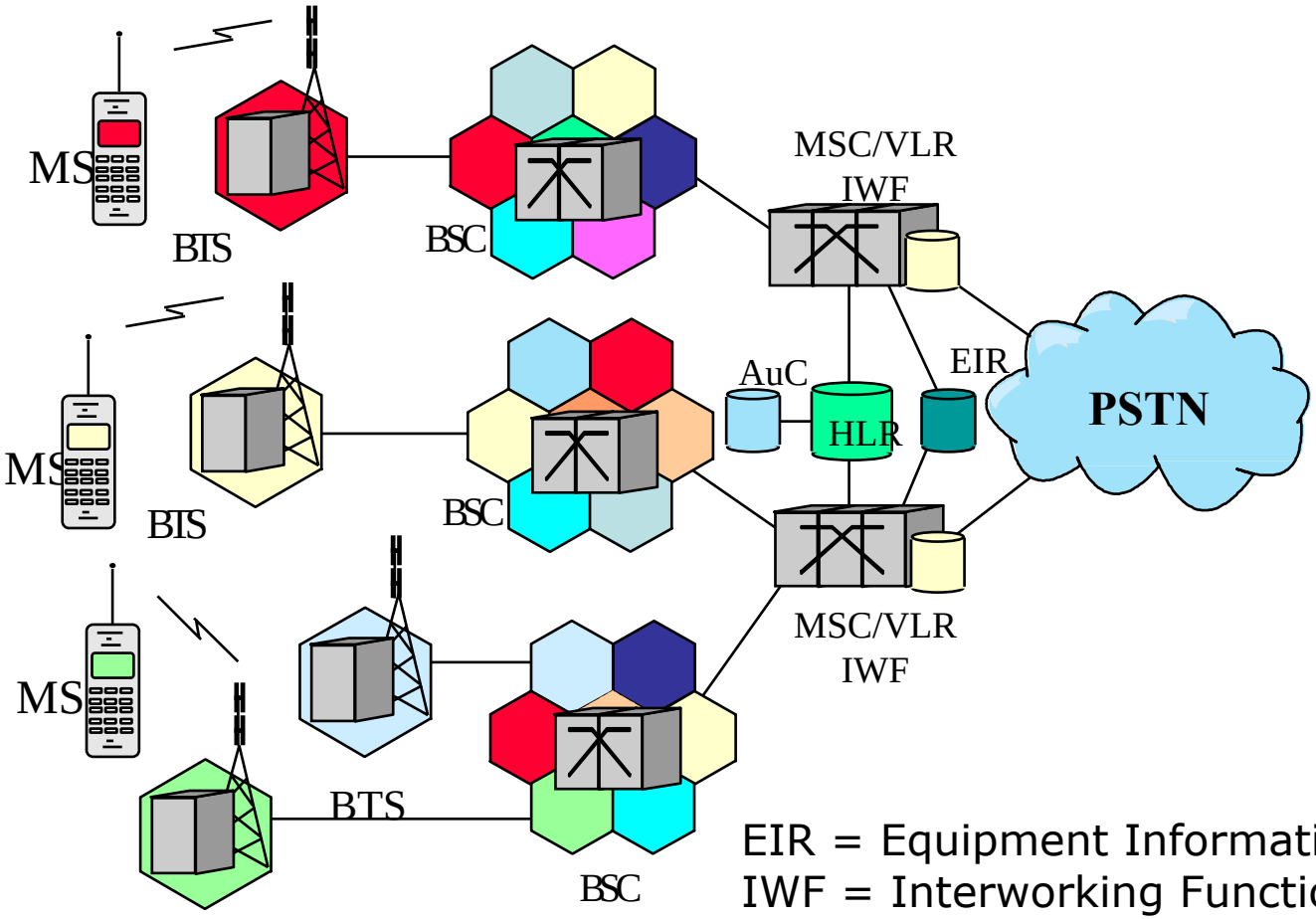
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa: cellás mobil rádióhálózat



BTS = Base Transceiver Station
BSC = Base Station Controller

Példa: cellás mobil rádióhálózat



EIR = Equipment Information Register
IWF = Interworking Function

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás: milyen fogalmakkal és tudnivalókkal ismerkedtünk meg?

- Bitfolyamok továbbítása hírközlő csatornákon
  - Alapfogalmak – ***bit/s, Baud, jelalakok tulajdonságai***
  - Átvitel sávhatárolt csatornán – ***mekkora sávszélességre van szükség adott szimbólumsebességhez?***
  - Átvitel zajos csatornán – ***hogyan kell jól dönteni, hogyan jelentkezik a zaj hatása (hibavalószínűség)***
- Digitális modulációs eljárások
  - ASK, FSK, PSK – ***alapeljárások, többszintű moduláció***
- Többcsatornás átvitel multiplexeléssel
  - FDM, TDM – ***több jelforrás egyetlen csatornán való átvitelének módszerei***
- Hírközlő csatornák a gyakorlatban
  - (Réz)vezetékes csatornák - ***felépítés, jellemzők***
    - Sodrott érpáras kábelek, strukturált kábelezés
    - Koaxiális kábelek
  - Fényvezetős (üvegszálas) csatornák
  - Vezetéknélküli csatornák – ***frekvenciatartomány, terjedés, földfelszíni és műholdas rádiócsatornák***

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás: hol használjuk fel ezeket az ismereteket?

- A tárgyban a későbbiekben megismerendő számítógép-hálózati technológiák mindegyike valamilyen fizikai közegen történő adatátvitelt használ
- Az adott technológia tárgyalásának ismertnek tételezzük fel az itt elmondottakat és hivatkozunk ezekre
- Ezen túlmenően több olyan alapfogalommal ismerkedtünk meg, amelyek későbbi tárgyakhoz, pl. a *„Távközlő hálózatok és szolgáltatások”* közös tárgyhoz és a *szakirány-tárgyakhoz* szükségesek

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csütörtökön gyakorlat, izgalmas példákkal!

- Késleltetés számítások
- Modulációk
- Többutas terjedés

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

TÖBBSZÖRÖS HOZZÁFÉRÉS

Mérnök-informatikus szak, BSc, 4. félév
2012/13 2.félév

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013. március 5.

Az anyag beosztása (1)

- Bevezető áttekintés, hálózatok és rendszerek példái.
- Alkalmazások és szolgáltatások. Követelmények a hálózattal szemben.
- Protokollarchitektúrák, referenciamodellek.
- A fizikai szintű kommunikáció alapjai.

Gyakorlat.

- Többszörös hozzáférés.
- LAN-ok, LAN-ok összekapcsolása.
- BWA (WPAN, WLAN, WMAN).

Gyakorlat.

- Áramkörkapcsolás, csomagkapcsolás, hívásvezérlés, címzés.
- Routing.
- Ütemezés.
- IP.

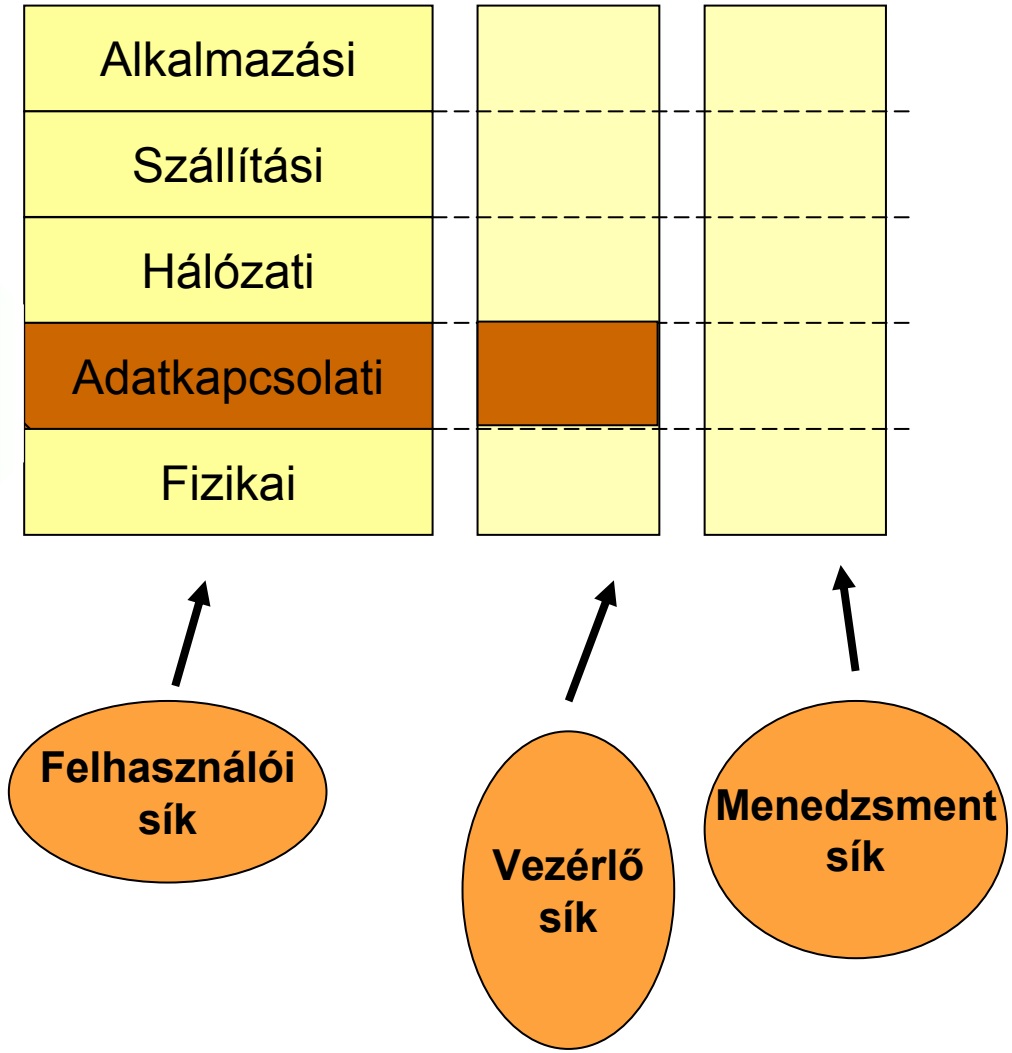
Gyakorlat.

Elv:

Többszörös hozzáférés

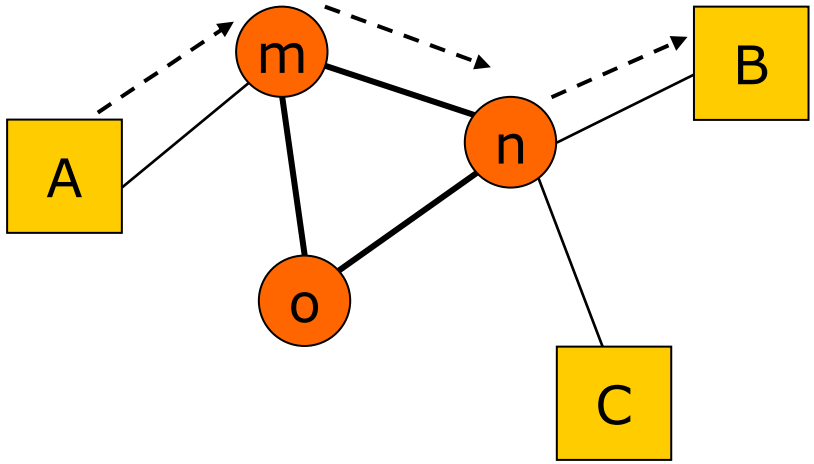
Módszer:

Aloha,
CSMA/CD,
CSMA/CA....



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mi az, hogy többszörös hozzáférés (multiple access)?



- Nemcsak ilyen hálózat van, hanem:

egy közös átviteli közeg, amelyhez minden végpont hozzáfér.

- Ez lehet vezetékes vagy rádiócsatorna.

Multiplexelés ⟺ többszörös hozzáférés

- Multiplexelés:
  - közös csatorna
  - több forrás
  - mindegyik egy helyen, a csatorna bemenetén
- Többszörös hozzáférés:
  - közös csatorna
  - több forrás
  - szétszórtan, akár nagy területen is
  - Nevezik MAC-nek is (Medium Access Control)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A többszörös hozzáférés szerepe, jelentősége

- A többszörös hozzáférés szerepe:
  - Takarékoskodás az átviteli közeggel,
    - különösen rádiócsatorna esetén.
  - Rugalmas hálózati elérés biztosítása.
- Mibe kerül ez nekünk?
  - szervezési („hozzáférési”) módszerek alkalmazása,
  - valamekkora erőforrás-felhasználás a szervezésre
    - sebességben
    - időben
    - frekvenciában

A közös csatorna fix megosztásának fő lehetőségei

- A megismert multiplexálási (nyalábolási) módszerek ...hozzáférési (... access) megfelelői:
  - FDMA TDMA CDMA

- FDMA
  - Ortogonális, de technikailag bonyolult
  - Hatékonyságát rontja a védősávok szükségessége
  - Alkalmazása elsősorban valós idejű átvitel esetben
- TDMA
  - Ortogonális, rugalmas megosztásra kiváló, mert könnyű különböző nagyságú rész-csatornákat kialakítani
- CDMA
  - Nem ortogonális, de bebizonyítható, hogy információelméleti értelemben a legjobb

- *SDMA (Space ...): térben választjuk el a felhasználókat*
  - *Irányított antenna nyalábok (fázisvezérelt antennarács, smart antenna: pl. MIMO)*

Példa: FDD-FDM-FDMA

- FDD (.....Duplex)
  - Pl. csatorna megosztása uplink-downlink irányba
- FDM (.....Multiplexing)
  - Fizikai rétegben több, kisebb sávszélességű csatorna átvitele egy közös nagyobb sávszélességű csatornán
- FDMA (.....Multiple Access)
  - Adatkapcsolati rétegben a felhasználók hozzáférése a csatornához, különböző földrajzi helyekről

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

FDMA előnyök-hátrányok

+:

- Nincsenek időzítési problémák mint TDMA-nál
  - megfelelő pl. stream alapú átvitelre
- Nincs közel-távol probléma, mint CDMA-nál
- Fix mellett igény szerinti frekvenciasáv kiosztás is

-:

- Magas teljesítményű szűrők a hw-ben
- Frekvenciák közötti interferencia
  - védősávok használata

TDMA előnyök-hátrányok

+:

- Egy frekvenciacsatornát oszt meg több felhasználó között
- Itt sincs közel-távol probléma
- Dinamikus TDMA: igény szerinti időrés kiosztás
  - Pl. Bluetooth, WiMAX

-:

- Interferencia a használt frekvencián
- Szinkronizációs problémák
  - terminál mozgása esetén különösen nehéz, megkötés a cellaméretre
  - szinkronizációs időrések: rosszabb kihasználtság

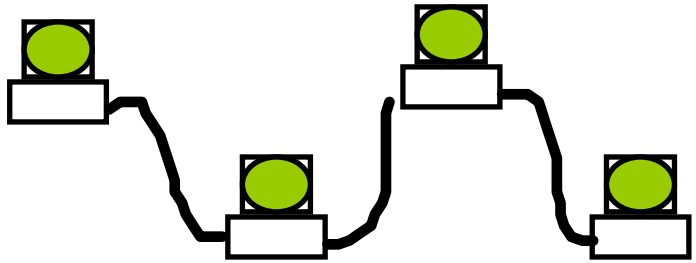
TDMA kiemelése

- Az előadás további részében TDMA típusú megosztással foglalkozunk
  - mivel csomagkapcsolású számítógép-hálózatokban ez terjedt el

- De sok más rendszerben ezek keverékét használják:

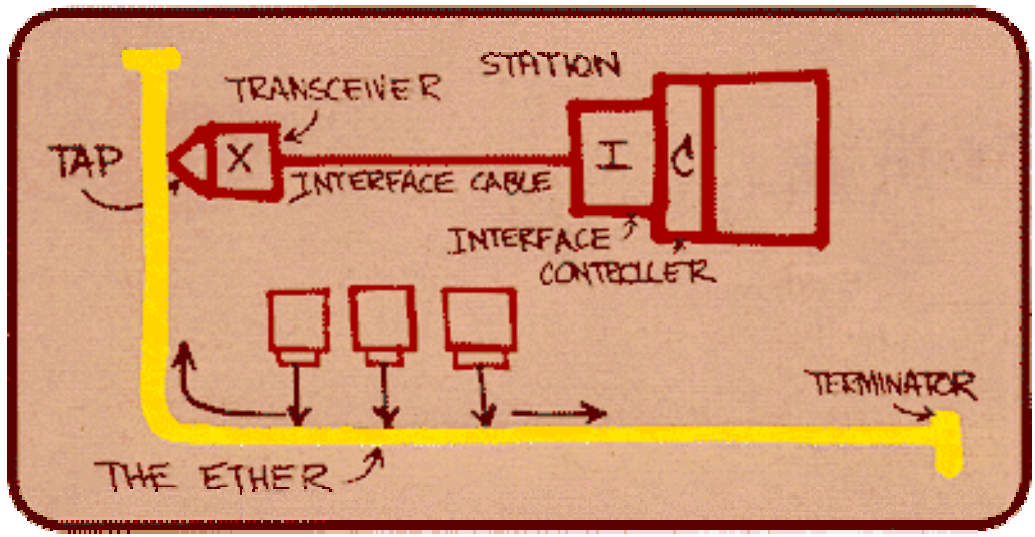
  - TDMA+FDMA+FDD: GSM mobil rendszerek
  - CDMA+FDD: UMTS mobil rendszerek

Példák közös csatornára: vezeték (koaxiális kábel)

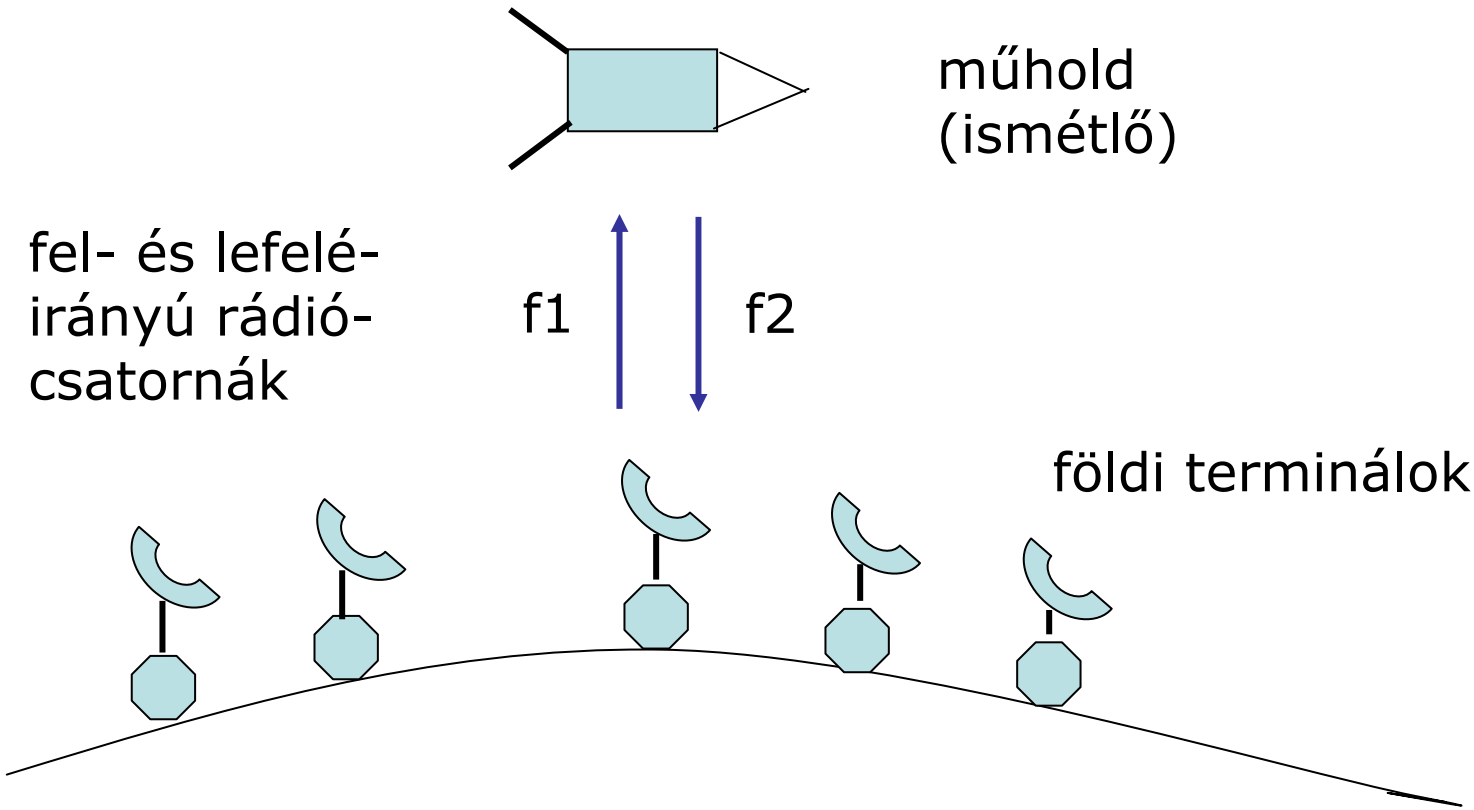


- „Vékony Ethernet”-kábelezés

- „Vastag” Ethernet,
  Az Ethernet elve
  Robert M. Metcalfe
  (1976)



Példák közös csatornára: műholdas ismétlőállomás

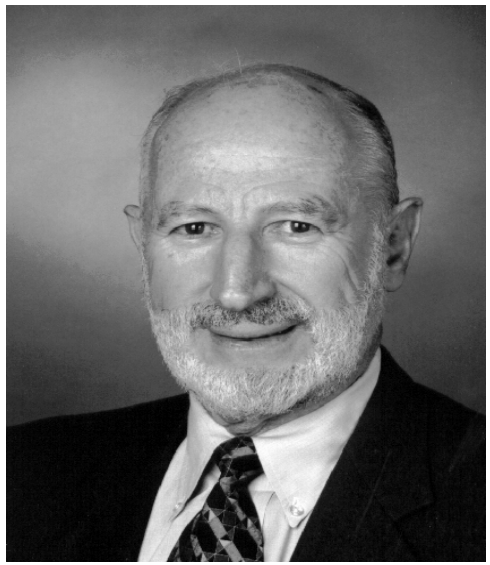


Eddig fix kiosztású hozzáférési technikák, következnek a véletlenszerű hozzáférési módszerek!

ALOHA? Hawaii köszöntés!

- ALOHA from Hawai: Elvis Presley koncertje (1973)
- Minden idők legnézetebb műholdas adása ami egy előadóhoz köthető

ALOHA?



- Norman Abramson, Univ. of Hawaii, HI, USA
- Aloha-eljárás és rendszer
- Az első rádiós csomagkapcsolt számítógép-hálózat, 1970!

ALOHAnet

- Világ első csomagkapcsolt vezetéknélküli hálózata!
- Már nem használják ezt a hálózatot, de az itt használt eljárás volt az Ethernet egyik ötletadója (Metcalfe)
  - Sőt az ALOHA módszert továbbra is használják!
- Ötlet: összekötni amatőr rádiós linkekkel az egyetem távoli részet (szigetcsoport)
- Rávilágított, hogy meg kell oldani a közös csatorna hatékony megosztását
- 1973-ban elsőként kötötték össze az ARPANET-el

ALOHAnet

- 2 frekvencián (uplink-downlink): elosztó (hub)/csillag (star) topológia elrendezésben

- Kimenő csatorna: szórt adás (broadcast), hub->kliensek
  - Csomagokban címekkel: csak a címzett kliens fogadta a csomagot
- Bejövő csatorna: kliens->hub
  - nyugtázva a sikeres vétel a hub által
  - nem érkezik nyugta: véletlenszerű idő után újraadás-> ütközések felderítése
- ARPANET-ben végpont-végpont kapcsolat: itt minden kliens egy frekvencián kommunikált a hubbal!
- Börsztös forgalomra

Szabad hozzáférés – random access

- Egyszerű (pure) Aloha-eljárás: teljesen kötetlen hozzáférés

Az egyszerű Aloha-eljárás tulajdonságai (1)

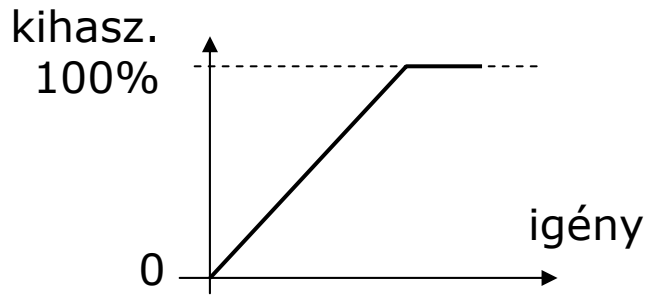
- A szabály tehát:
  - mindenki akkor ad, amikor akar
  - óhatatlanul lesznek ütközések, ekkor egyik adása sem sikeres
  - az ütközésben résztvettek ismét próbálkoznak
    - Véletlen késleltetés múlva!
  - adás előtt **nem ellenőrzik** a csatorna foglaltságát

- Egyszerű, semmi szervezést nem igényel
- Ütközés detektálás: nyugtával (uplink-downlink frekvencia)

Nézzük meg ehhez, hogy általában mik a hozzáférési módszerek legfontosabb jellemzői!

A hozzáférési módszerek teljesítőképességének jellemzése

- **Kihasználtság (throughput):**
  kiszolgált információ –
  a fellépő igény függvényében



- **Kiszolgálási késleltetés:**
  - az igény jelentkezése és kiszolgálása közötti idő

- **Igazságosság** (***fairness***):
  - egyformán részesülnek-e az átbocsátóképességből, illetve
  - teljesül-e a jogosultság szerinti kiszolgálás?

- **Stabilitás**: reakció a túlterhelésre, a forgalom dinamikus változására

Gondok az egyszerű Alohával

- **Egyik terminál sem figyeli**, hogy foglalt-e a csatorna adás előtt: ütközés!
- Véletlenszerű várakozás miatt egyetlen állomás sem kezdeményez adást: rossz kihasználtság!

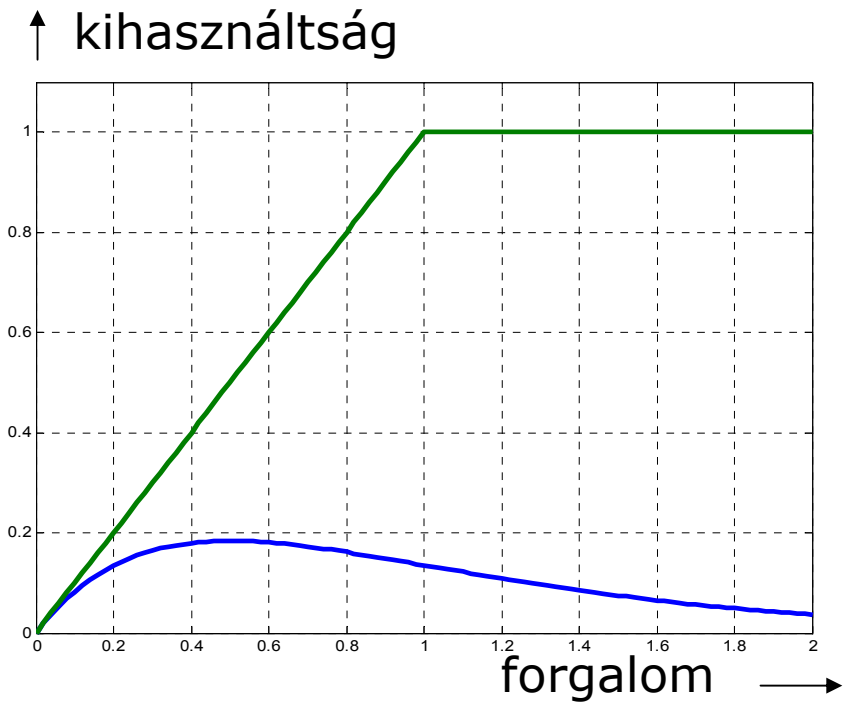
- Ütközés után ismét próbálkoznak, a **visszatartó mechanizmus (backoff)** nagyban befolyásolja a
  - protokoll hatékonyságát
  - a csatorna kapacitását

- Tanenbaum: legjobb esetben az idő 18,4%-van hasznos átvitel:

$$\Pr[k] = \frac{G^k e^{-G}}{k!} \quad \Rightarrow \quad S_{pure} = G \cdot e^{-2 \cdot G}$$

Az egyszerű Aloha-eljárás tulajdonságai

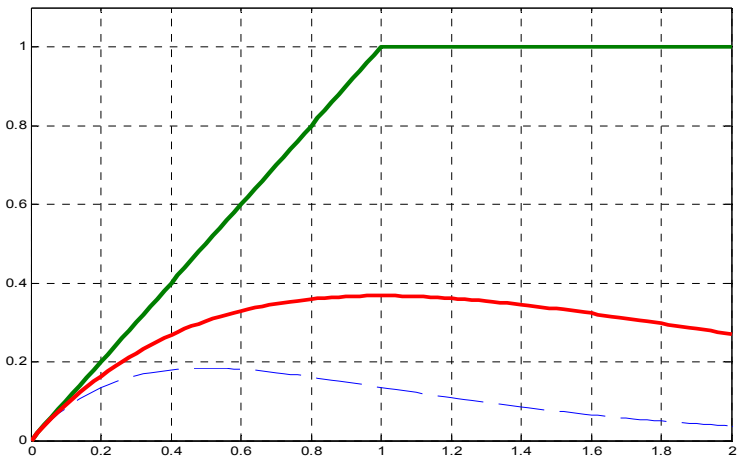
- A kihasználtsága rossz
- Alapvetően instabil
- Késleltetése nem korlátos
- Fairness: egyenlősdi hosszútávon



Réselt (slotted) Aloha

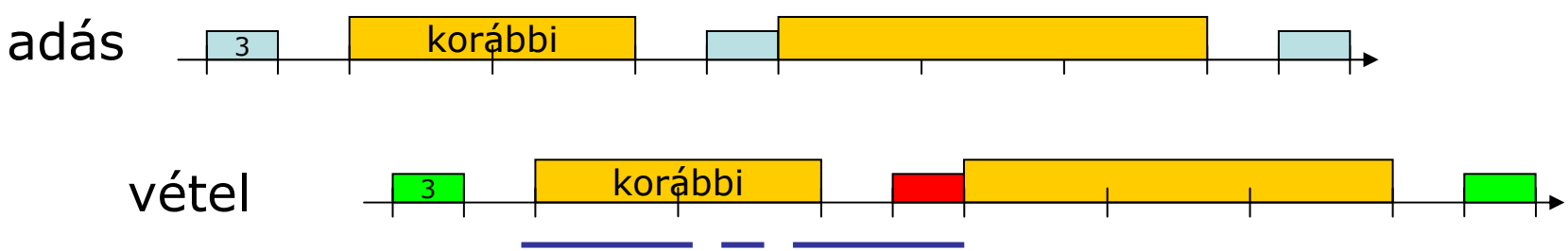
- Azonos hosszúságú csomagok időréshatárokon (szinkronjel):

- Ennek köszönhetően csak egy időrésen belül lehet ütközés, nem nyúlnak át a következőbe
- A kihasználtság javul
- Késleltetés alig változik
- A stabilitási probléma változatlanul fennáll
- Fairness: mint előbb



Helyfoglaló Aloha

- A jellemzők javítására használjunk „helyfoglalást” (reservation)
- A csatorna egy részén igénybejelentés
- A felhasználók „visszahallják” az igényeket
- Mindegyikük egységes döntésre jut a hallottakból az átviteli csatorna használati jogosultságát tekintve
- Késleltetés szempontjából sokkal jobb mint a réselt Aloha



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Aloha alkalmazása

- Ahogy növekszik a felhasználók száma és a forgalom: **rohamosan romlik a kihasználtsága**
- De börsztös forgalom esetén jobb mint fix kiosztású
  - 10%-os csatornaterhelés alatt
- Felhasználás (Réselt Aloha):
  - Műholdas rendszerekben (katonai)
  - RFID
  - Más eljárásokkal együtt: réselt-helyfoglaló Aloha (pl. GSM-GPRS)

Vivőérzékeléses többszörös hozzáférés (Carrier Sense Multiple Access)

- A többszörös hozzáférés „vezérlése” a csatorna foglaltságának ellenőrzésére korlátozódik
- Szabad csatorna esetén:
  - a csatorna igénybevétele
- Foglalt csatorna esetén:
  - *majd később megpróbáljuk* (**nemperzisztens**)
  - várakozás a csatorna felszabadulására:
    - felszabaduláskor rögtön igénybe vesszük (**1-persisztens**)
      - Ütközés: várakozás véletlenszerű ideig
  - p valószínűséggel adja a keretet ha szabadnak érzékeli a csatornát, időrés elején (**p-perzisztens**)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A vivőérzékelés jellemzői

- Egyszerű megvalósítás: csak a foglaltságot kell érzékelni
- Nagy kihasználtság: az átvitel egészen közel juthat a 100%-hoz
- Nagy érzékenység a terjedési késleltetésre: ameddig nem ér hozzánk a jel, nem észlelhetjük
- Túlterheltség esetén instabil lehet
- Az igazságos kiszolgálás megvalósítható

CSMA/CD

- Újabb visszacsatolás a csatornából adás közben: ütközés – Collision Detection - CD
- Vivőérzékelés ütközésdetekcióval: észlelt ütközés esetén leállás
- Az ütközésdetekció vezetékes csatornán lehetséges
- Rádiócsatornán nem tudja az éppen használó detektálni az ütközést

CSMA/CD működése

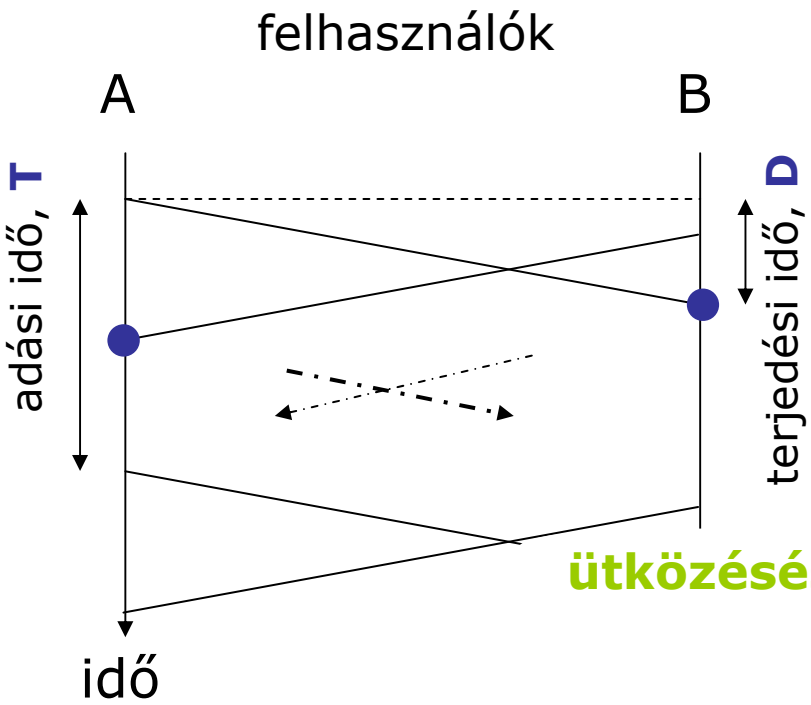
- Vivőérzékelés: terminál csak akkor ad ha szabadnak érzékeli a csatornát
- Ha időközben ütközést detektál: küld egy **foglaltsági jelzést**, hogy ne legyen több ütközés
- Majd vár **exponenciális backoff** ideig (részletek Ethernetnél) és csak utána ad

CSMA/CD hatékonysága

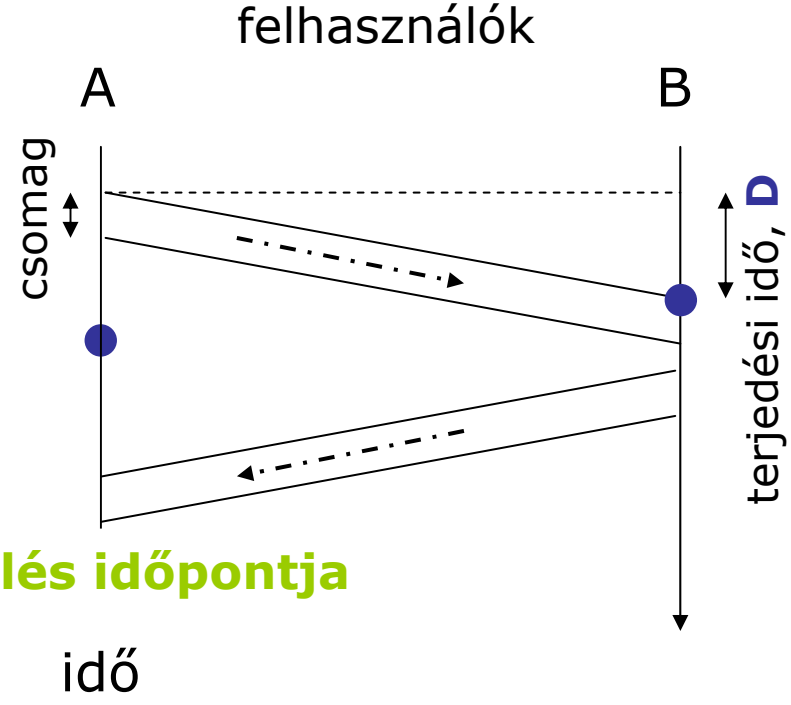
- CSMA hatékonyágának javítása:
  - Az ütközésdetektálás után rögtön leáll az adás
    - **Jam signal**: minden adó leáll
  - Újraadás csak **exponenciális backoff** után: csökkenti az újabb ütközés lehetőségét
  - Megvalósítása: lehet teljesen szoftver vagy hardver is
  - Csak fél-duplex esetén van értelme
    - full-duplexnél nem használják

Az $a=D/T$ paraméter értékének hatása

Kis a érték



Nagy a érték



ütközésészlelés időpontja

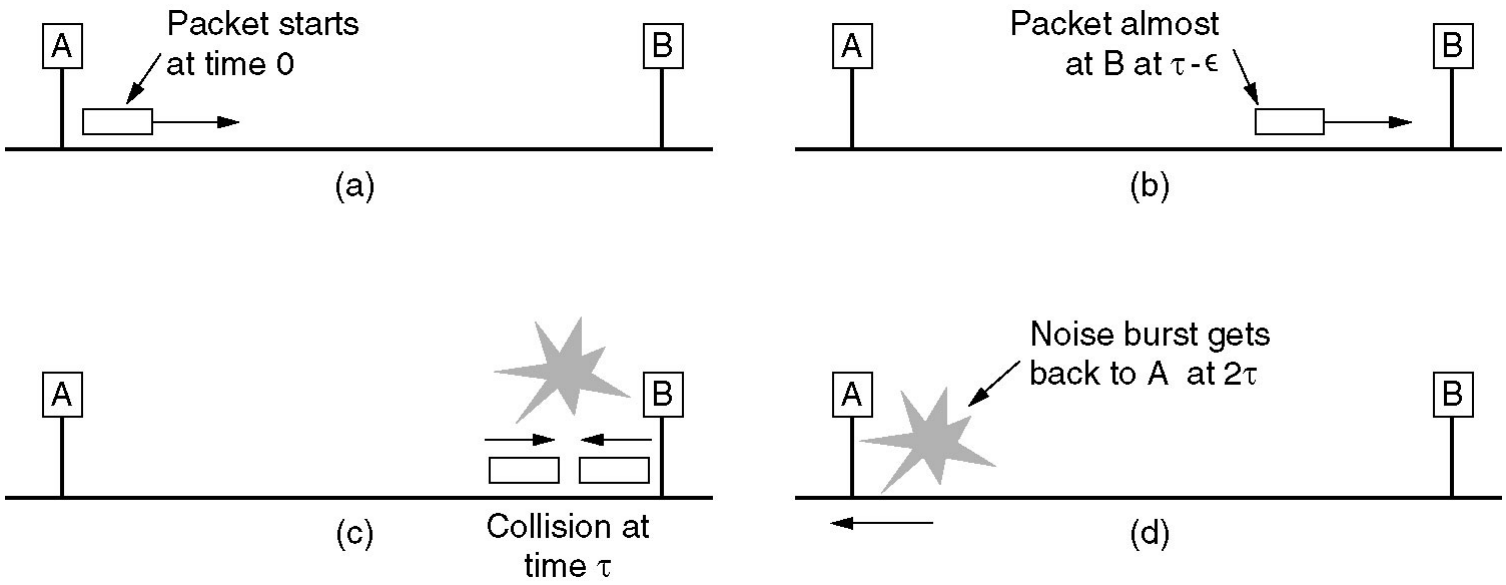
T: adási idő

D: terjedési idő

2D ~ Round Trip Time, RTT

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Legrosszabb eset



Akár 2τ ideig is eltarthat az ütközés detekció!

CSMA/CA (Collision Avoidance)

- Vivőérzékelés ütközéselkerülés (Collision Avoidance, CA): készülünk az ütközésveszélyes helyzetekre

- Ha szabad a csatorna:
  - küld egy jelzést a többi állomásnak, hogy adni készül

    vagy
  - vár egy további ideig és ha az idő lejárta után is még szabad a csatorna, akkor ad csak

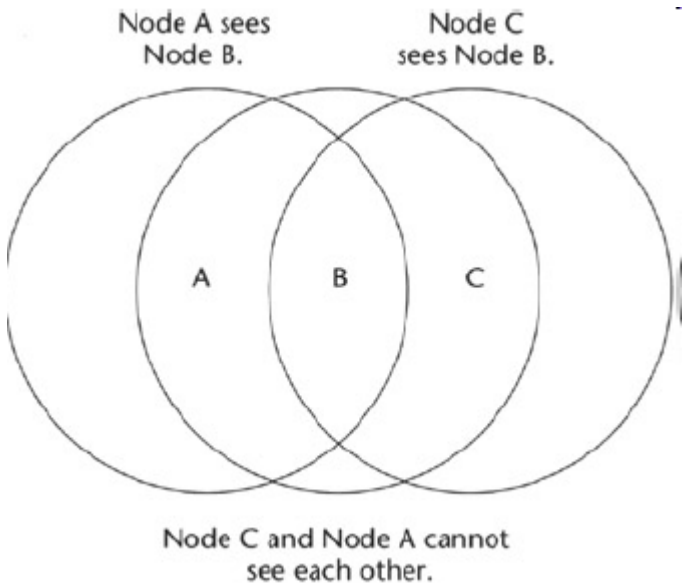
- Ha foglalt a csatorna:
  - exponenciális backoff ideig elhalasztja az adást

CSMA/CA használata

- Kevésbé „mohó” adók
- Ott használják, ahol a csatorna nem alkalmas CSMA/CD-re
  - pl. WLAN-ok
- rádiós átvitel esetén az adó nem tudja adás közben „hallgatni” a csatornát: nem lehetséges az ütközés detekció
- Vagy rejtett terminál probléma!

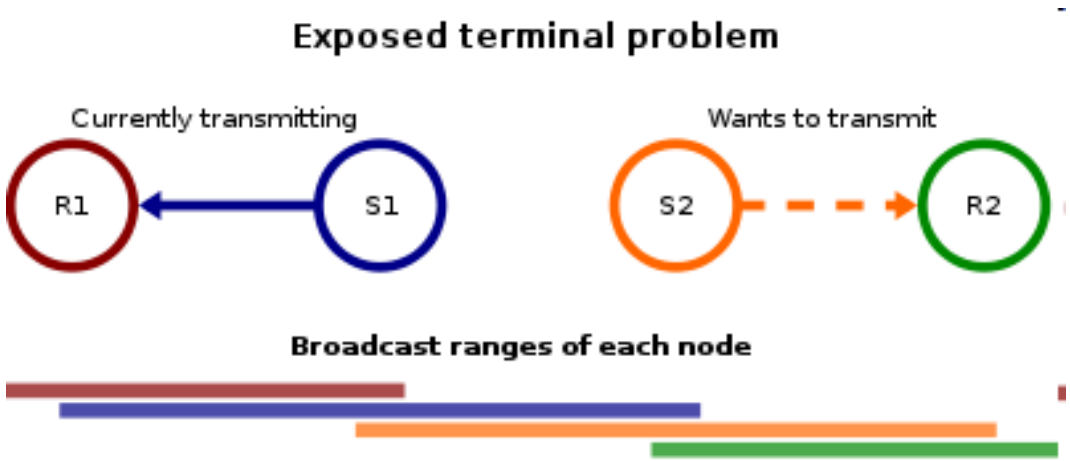
A „rejtett” terminál probléma

- Az „árnyékolt” felhasználó problémája: nem mindenki hall mindenkit
- Ha egy adást nem észlelünk, azt akaratlanul megzavarhatjuk



„Exponált” terminál probléma

- Túl „jó helyzetű” felhasználó:
  - szomszédos (idegen) rendszerekből is észlelhet adást
  - nem meri használni a csatornát, mert úgy véli ütközést okoz



Megoldások rejtett és exponált terminálra

RTS-CTS

- Egy igénybejelentés (RTS) és egy nyugta (CTS) párbeszéd után történik adatátvitel
- Az átvitel hosszát tartalmazza a két üzenet (lásd majd a vezeték nélküli LAN-oknál)

Versenymentes MAC protokollok

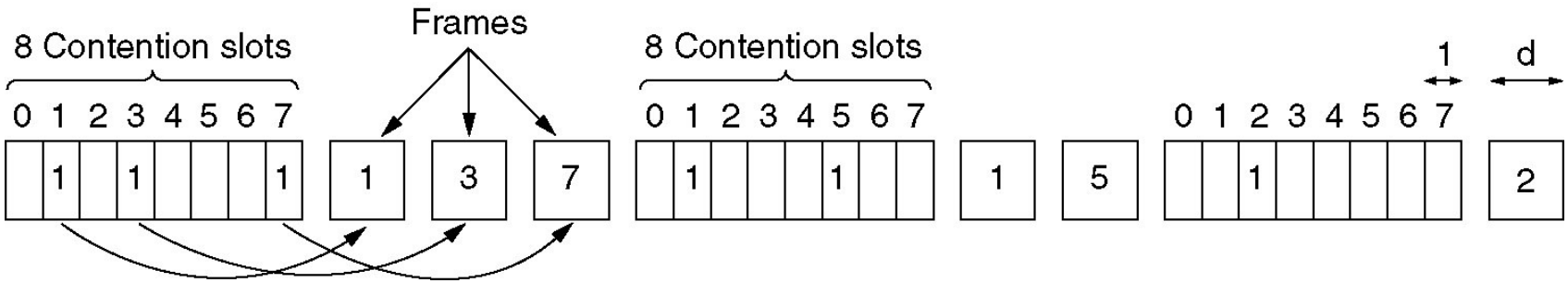
- CSMA/CD esetén nincs ütközés amikor az egyik állomás már lefoglalta a csatornát
- Viszont lehet ütközés a verseny helyzet idején
- Ezen ütközések kihatnak az átvitel hatékonyságára
- Ezért fejlesztettek ki verseny-mentes protokollokat (contention free):
  - Bit-térkép módszer
  - Bináris visszaszámlálás

Bit-térkép módszer

- N időrés: j. terminál a j. időrésben egy 1-es bittel jelzi, ha szeretne keretet adni
- Miután minden terminál nyilatkozott, minden egyes terminál tudja ki akar majd adni
- Így numerikus sorrendben adnak, **nem lehet ütközés**
- Hátránya: **alacsony forgalom** esetén **nem hatékony**
  - Pl. csak egy terminál szeretne adni, senki más, de ki kell várnia a bit-térkép végét
  - Sávszélesség pocsékolás kevés adó terminál esetén

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

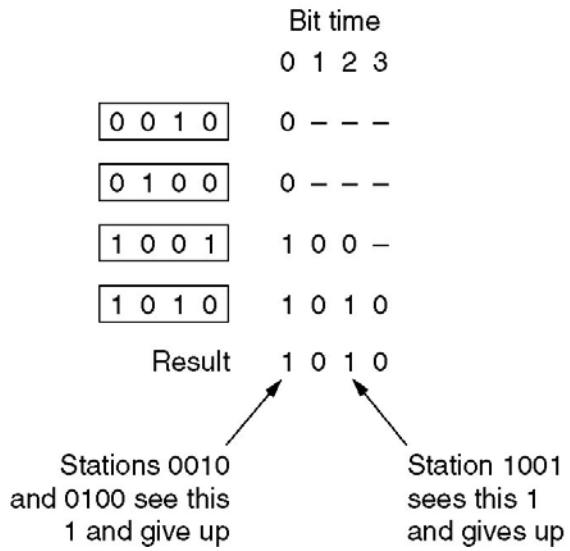
Bit-térkép módszer



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Bináris visszaszámlálás

- Azon terminál amelyik keretet szeretne forgalmazni: bináris számként beírja a címét a fejlécbe
- Ha látja egy másik terminál, hogy a magasabb helyértéken az ő O-ja helyén másnál 1 van, lemondja az adást
- Végén megmarad ki adhat, ez a folyamat ismétlődik
- Hátrány: nagyobb értékű címmel rendelkező adóknak előnye van
  - Sérül a fairness elv



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Verseny vs. versenymentesség

- Alacsony forgalom esetén a verseny javasolt: alacsony késleltetés
- Ahogy növekszik a forgalom egyre kevésbé jó a verseny: sok erőforrást emészt fel
- Ötvözni kell a verseny-mentes és verseny-alapú protokollokat!
  - Alacsony forgalom esetén verseny, magasabbnál nincs: protokollok korlátozott versennyel!
- Cél:
  - kis késleltetés alacsony terhelés esetén
  - nagy átvitel (throughput) nagy terhelés esetén

Protokollok korlátozott versennyel

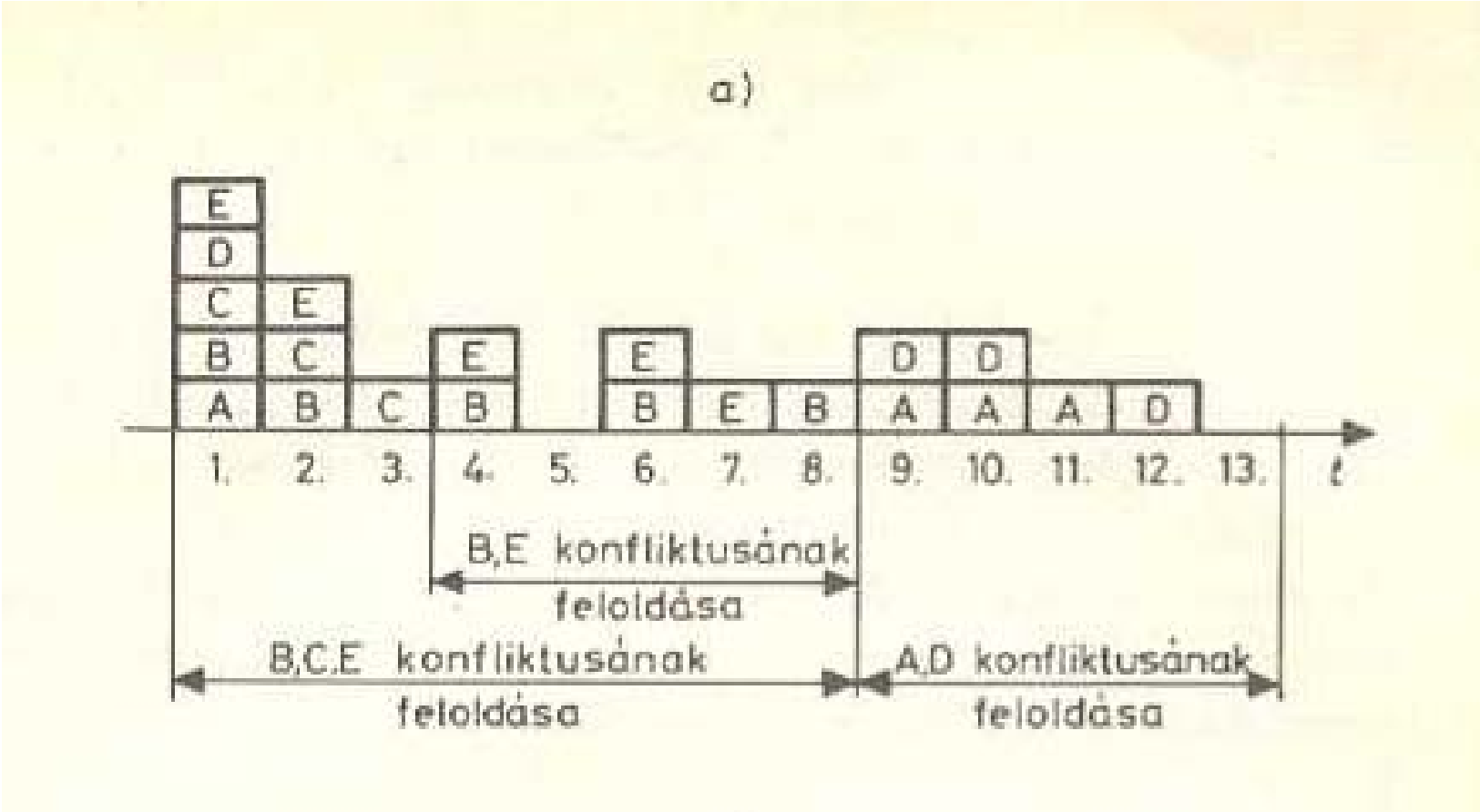
- A terminálok esélyét a csatornaszerzéshez úgy lehet növelni, hogy csökkentjük a versenyt
- Terminálok csoportokba (nem feltétlenül diszjunkt) sorolódnak
- Csak a j.csoport tagjai versenyezhetnek a j.időrésért
- Ha ütközés történt vagy senki sem akar küldeni a j.csoportból, akkor jön a j+1.csoport a j+1.időrésért

Adaptív fa protokoll

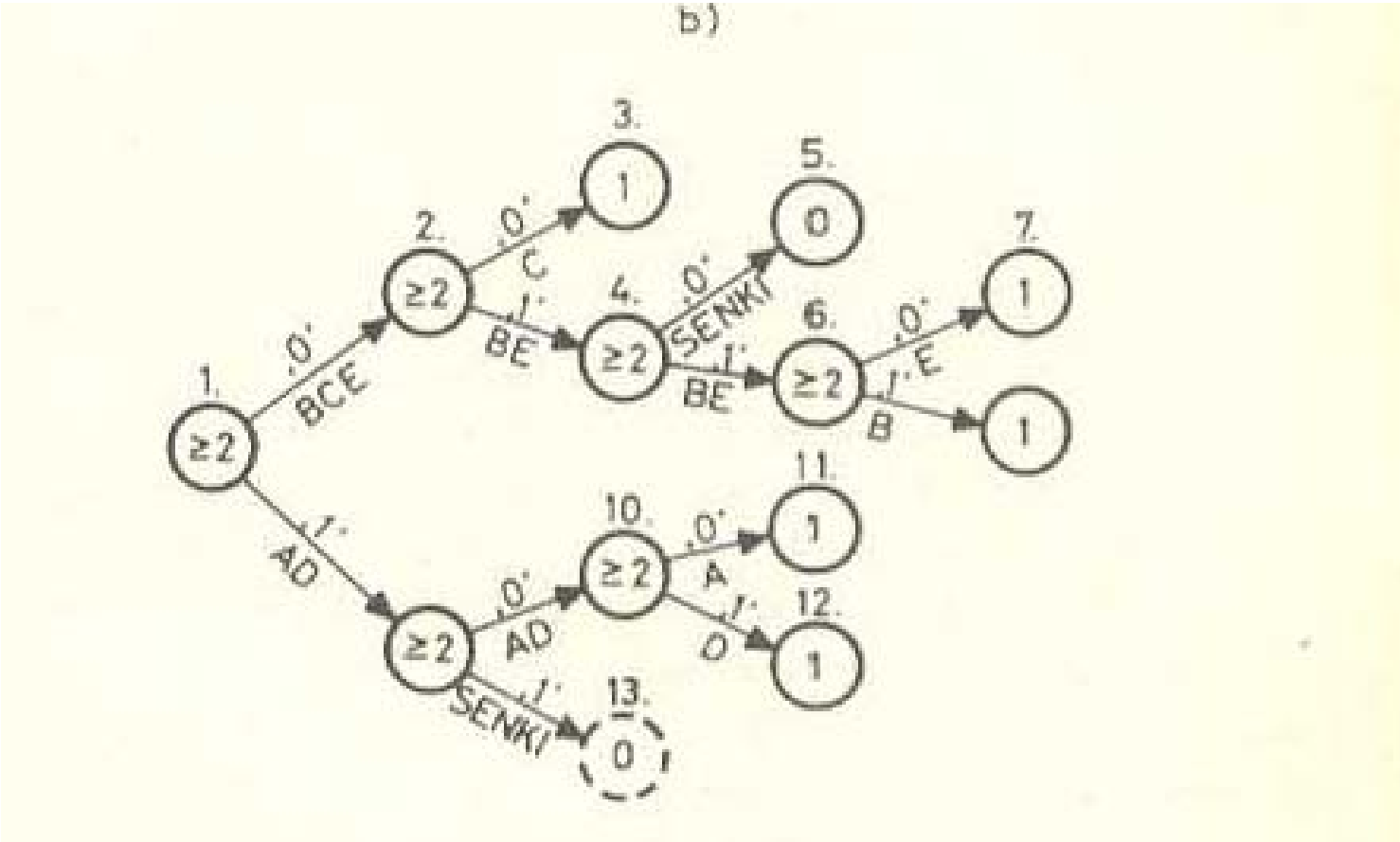
- Minden terminál versenyezhet a csatornáért
- Ha ütközés, két egyforma csoportra osztódnak a terminálok
  - Csak az egyik versenyez a következő időrésért
- Ha valaki megszerzi közülük, következő időrését a következő csoport versenyez
- Ha újra ütközés: újabb csoportfelezés

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A Capetanakis-algoritmus működése - illusztráció



A Capetanakis-algoritmus működése – illusztráció



Milyen többszörös hozzáféréses módszerekről volt szó eddig?

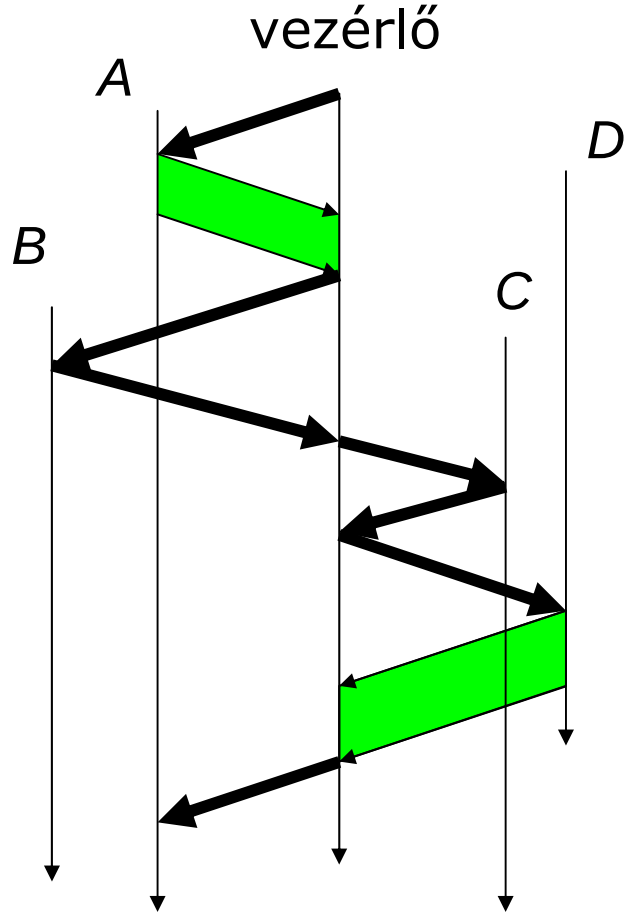
- Teljesen (vagy majdnem teljesen) szabad (véletlen) hozzáférés:
  - Egyszerű Aloha
  - Réselt Aloha
  - Ezeknél: egyszerű visszacsatolás a csatornából (sikeres/nem sikeres)
- Vivőérzékeléses módszerek
  - visszacsatolás itt is + „a priori” információ („vivő” érzékelés)
- Közös jellemző: **nincs központi vezérlés**, koordináció

Központilag vezérelt többszörös hozzáférési módszerek

- Lekérdezés (polling): a vezérlő kérdése jelenti a csatornahasználati jogot
- Csoportos lekérdezés (probing): felhasználók nagyobb csoportját kérdezi a vezérlő
  - több igény esetén kezelni kell az ütközést
- Foglalás (reservation): a vezérlő az érkező igények alapján csatornahasználati jogosultságot jelöl ki.
  - Az igények gyűjtése:
    - egyedi „csatornákon”
    - „versenyben”

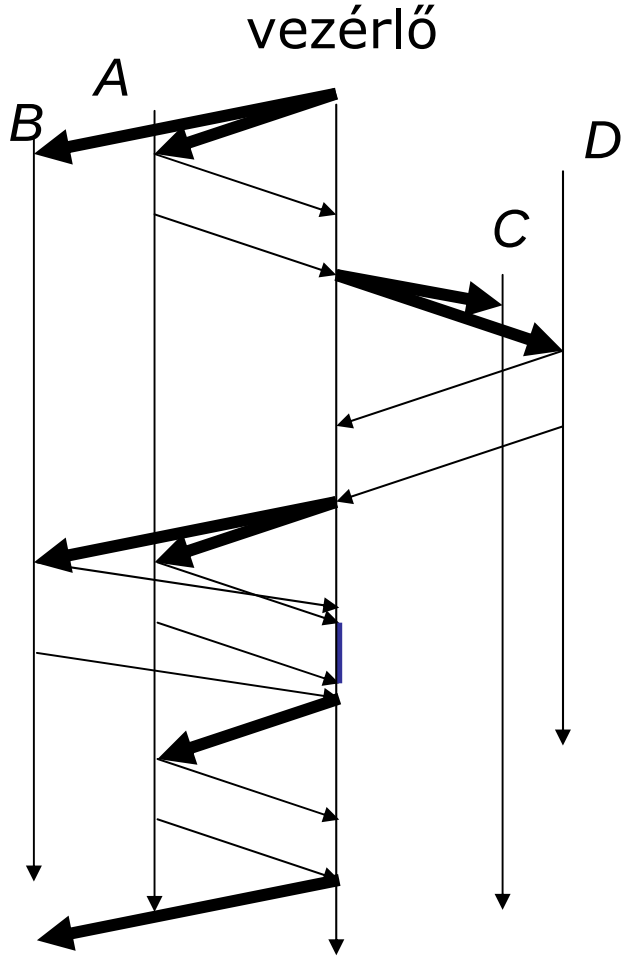
Lekérdezés (Roll-call polling)

- „körbekérdezés”: akinek van csomagja, az elküldi
- A csatorna információ-átvitelre használt a csomagtovábbítás alatt
- Egyébként a hozzáférés szervezése folyik
- Kihasználtság: a két időszak aránya
- Kiszolgálási késleltetés: a körbejárási idő fele
- A módszer stabil és fair



Csoportos lekérdezés (Probing)

- Csoportos lekérdezés:
  - Ütközés esetén:
    - részekre bontás
- Kihasználtság javul
- Kiszolgálási késleltetés csökken
- Stabilitás megmarad
- Igazságosság biztosítható



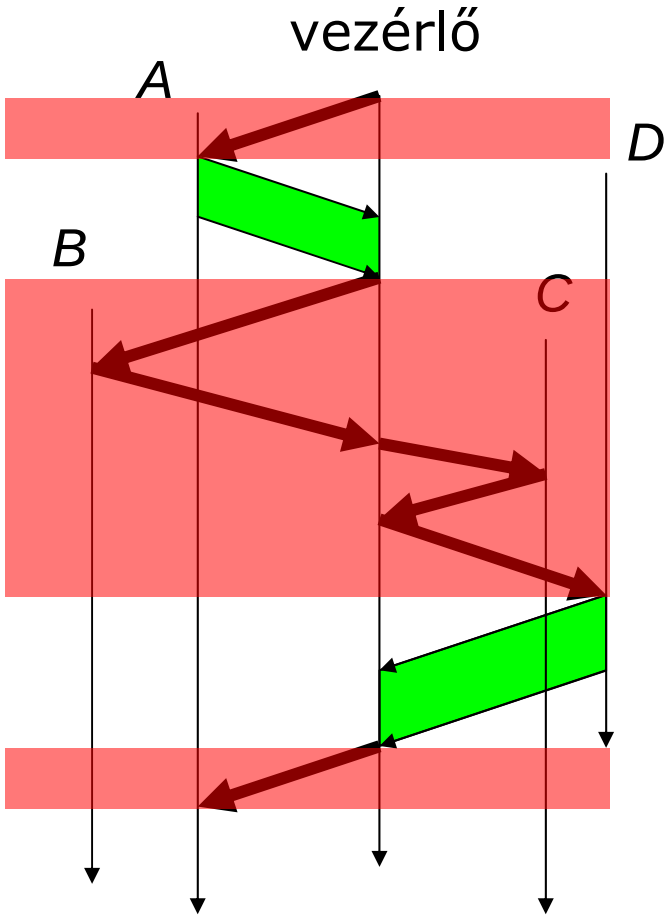
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Helyfoglalás (Reservation)

- Ha nagy a körbefordulási idő, akkor a lekérdezés hatékonysága rossz
- Célszerű az átviteli csatornát megosztani:
  - foglalási és
  - átviteli részre
- A (hely)foglalási részben (kis hányad):
  - dedikált csatornarészek:
    - zavartalan igénybejelentés
  - verseny alapú elérés
- A vezérlő a beérkező igények alapján engedélyeket küld a felhasználóknak

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Foglalás: a csatorna megosztása



Polling elosztott vezérléssel: token passing (vezérjelátadás)

- A csatorna használatára való jogosultságot egy speciális üzenet (token) birtoklása jelenti
- Megfelelő szabályok alkalmazásával nagyon rugalmas kiszolgálást biztosít
- Kifinomult együttműködést igényel az állomások között
- Jó kihasználtságot ér el, korlátozott késleltetéssel, hasonlóan a lekérdezéshez
- Az igazságos csatornamegosztás biztosítható

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A többszörös hozzáférés előnyei,hátrányai

- Előnyök: (nagyon függ a használt közegtől)
  - Gazdasági: pl. kevesebb vezeték
  - Technikai: jobb teljesítőképesség
  - Rádiócsatorna esetén szinte nélkülözhetetlen

- Hátrányok:
  - Bonyolultabb algoritmusok (nem jelentős)
  - Illetéktelen hozzáférés az információhoz (kezelendő)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás

- Megismertük a multiplexeléstől (xDM) eltérő feladatot, a többszörös hozzáférést (xDMA)
- Megtanultuk, hogy vannak:
  - elosztott vezérléssel működő módszerei, és
  - centralizált módszerek
- Rádiócsatorna használata esetén meghatározó szerepük van
- Vezetékes csatorna esetén is lehet fontos szerepük, ahol a felhasználók busz, vagy gyűrű topológián helyezkednek el

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

LOKÁLIS HÁLÓZATOK 1.RÉSZ

Az Ethernet (IEEE 802.3)

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013. március 7.

A számítógép-hálózatok klasszikus osztályozása területi lefedés szerint

- WAN – *Wide Area Network* – nagy kiterjedésű hálózat
  - távolsági megkötés nélküli, ***tetszőleges kiterjedésű*** hálózat
    - akár ***globális méretű*** is lehet
- MAN – *Metropolitan Area Network* – városi/nagyvárosi hálózat
  - eredetileg: egy tipikus USA-beli ***metropolitan area***, de nem feltétlenül város
    - ***néhány tíz km***
- LAN – *Local Area Network* – helyi v. lokális hálózat
  - tipikusan ***vállalaton, intézményen belüli*** hálózat
    - max. ***néhány km-es*** távolságok
- PAN – *Personal Area Network* – személyi hálózat

Lokális hálózatok – tartalom

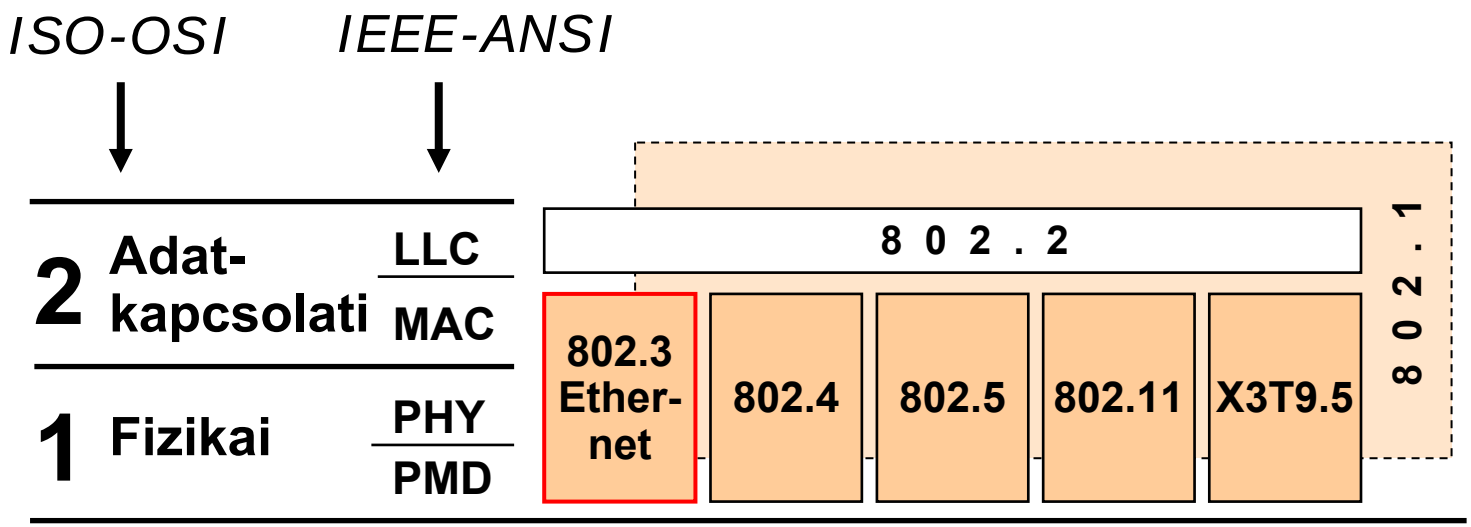
I. Az „Ethernet”
- IEEE 802.3 Ethernet (a „klasszikus” E.)
- *IEEE 802.3u Fast Ethernet*
- *IEEE 802.3z Gbit/s Ethernet*
- *IEEE 802.3ae 10 Gbit/s Ethernet*

II. További LAN-ok
- „Token ring” – 802.5
- FDDI (ANSI)

III. LAN-ok összekapcsolása

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A lokális hálózatok architektúrája

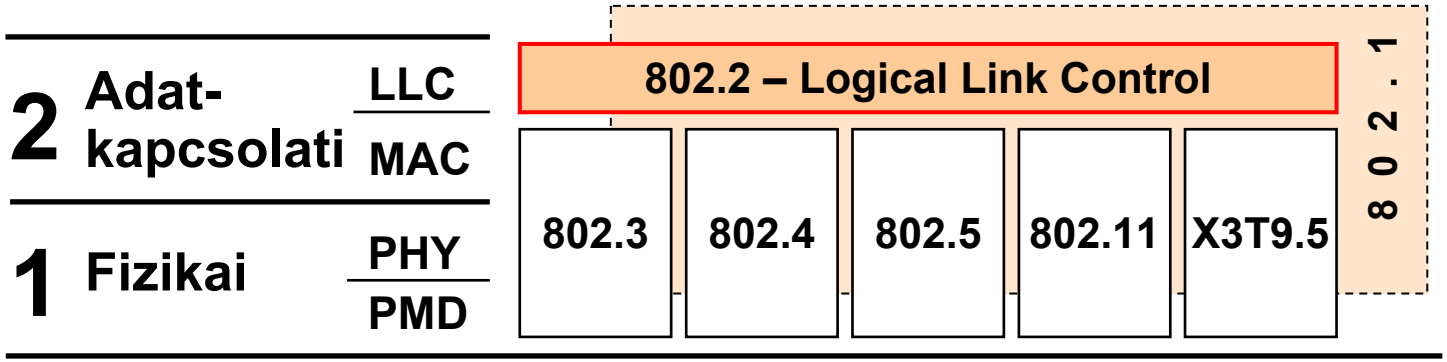


- LLC : Logical Link Control – Logikai adatkapcsolati
- MAC: Medium Access Control – Közeghozzáférési
- PHY: Physical – Fizikai
- PMD: Physical Medium Dependent – Fizikaiközeg-függő
- *802.1: közös funkciók valamennyi LAN-ra és MAN-ra pl. együttműködés, biztonság (interworking, security)*

} Alrétegek (sublayer)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IEEE 802.2 LLC – Logical Link Control



- Feladatai:
  - **A 3. rétegbeli protokoll számára megbízható átvitel biztosítása**
    - Forgalomszabályozás
    - Hibaérzékelés, -javítás
- Szolgáltatások:
  - Nyugtázatlan, összeköttetésmentes (datagram)
  - Nyugtázott, összeköttetésmentes (datagram)
  - Nyugtázott, összeköttetés-alapú
- **Nem biztos, hogy szükség van LLC-re (pl. az IP nem igényli)**
- Protokoll-overhead: a MAC-kerethez LLC fejléc adódik hozzá

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

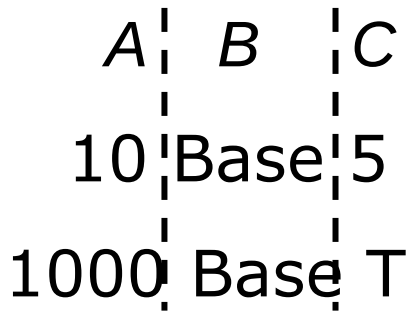
A 802.3 szerinti fizikai és MAC réteg: az Ethernet

- A Xerox Palo Alto Research Center fejlesztette ki: Robert Metcalfe
- A Digital Equipment, Intel, és Xerox mint DIX közös gyártói szabványa lett
  - Az IEEE az IEEE 802.3-ban szabványosította (jelentős változtatásokkal)
- Ezért két változat létezik:
  - Ethernet version 2 (DIX)
  - IEEE 802.3
  - Különbségek elsősorban a MAC keretben
- Topológia: logikailag (és eredetileg fizikailag is) busz

Ethernet vs. Token bus-Token ring

- Komoly verseny volt a három között (80-as évek)
- Ethernet sikere: CSMA/CD
  - Előny: mindenki hallott mindenkit a csatornán
  - Hátrány: minimum csomagméret és útvonalhossz összerendelve
- Metcalfe sikertörténete: 3Com

Ethernet – jelölésrendszer



- „A” rész: Adatsebesség
  - **1 = 1 Mbit/s**
  - **10 = 10 Mbit/s, ...**
- „B” rész:
  - **Base = alapsávi (baseband) átvitel**
  - **Broad = „szélessávú” (broadband) átvitel**
- „C” rész:
  - Átviteli közeg:
    - T = twisted pair
    - FX/LX/SX = fibre optics
    - CX = shielded balanced copper
    - T4 = 4 pair twisted pair
    - T2 = 2 pair twisted pair
  - Szegmenshossz:
    - 2=185 m
    - 5=500 m

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

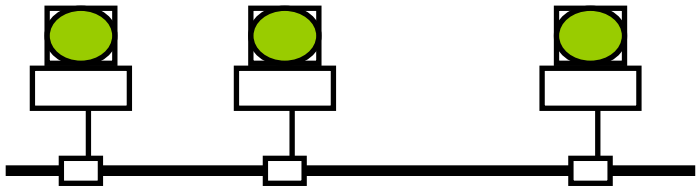
A fizikai réteg feladatai

- Bitfolyamok adása és vétele
- Vivőérzékelés
- Ütközésészlelés
- A jelek kódolása és dekódolása
- „Előke” / „előtag” (preamble) generálása
- Órajel generálása a szinkronizáláshoz

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

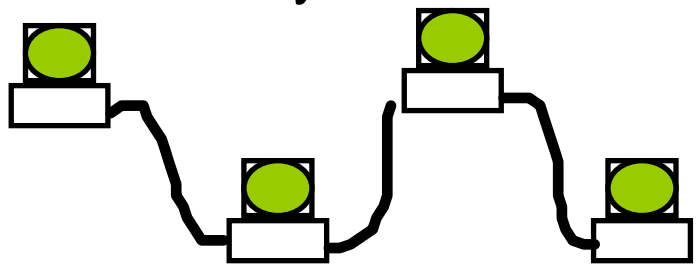
Kábelezési megoldások

„Eredeti” vastag (yellow) kábeles



10 BASE5

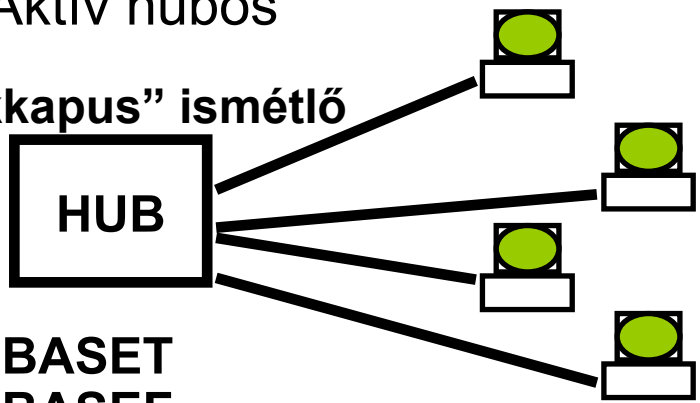
Vékony kábeles



10BASE2

Aktív hubos

hub = „sokkapus” ismétlő



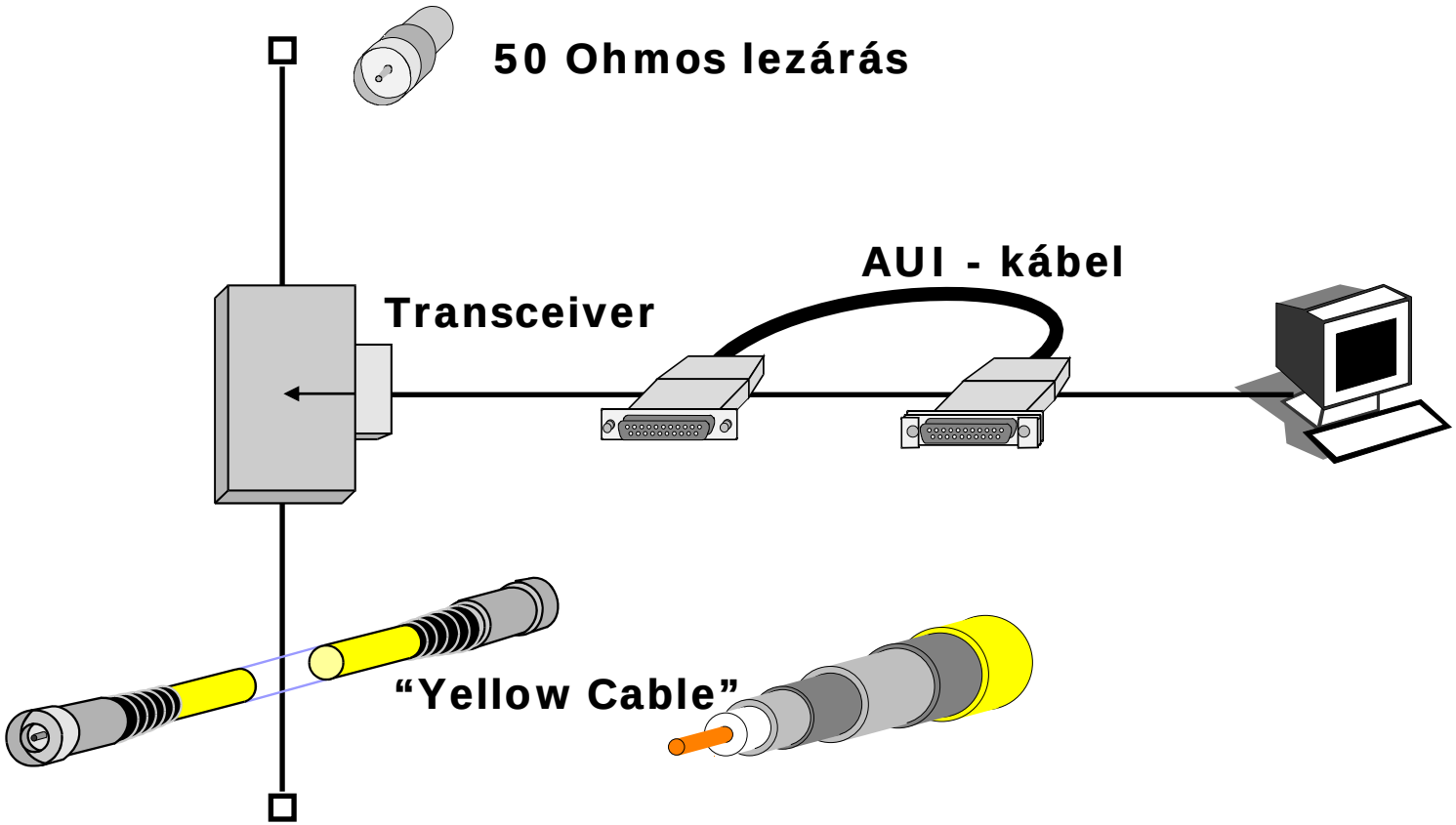
10BASET
10BASEF

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

10 Base 5 (Vastag Ethernet)

- Első kábelezési megoldás: koaxiálisra tervezve
  - „Kerti locsolócső”: tűzvédelem
- Állomás csatlakoztatása: vámpír csatlakozóval
- Alapsávú, de létezett szélessávú változat is
  - 10Board36, eltünt
- CSMA/CD
- Rövid maximális szegmens: időzítés és jelcsillapítás miatt
  - Max 100 adó; 2.5 méterenként

Ethernet kábelezés: 10 Base 5

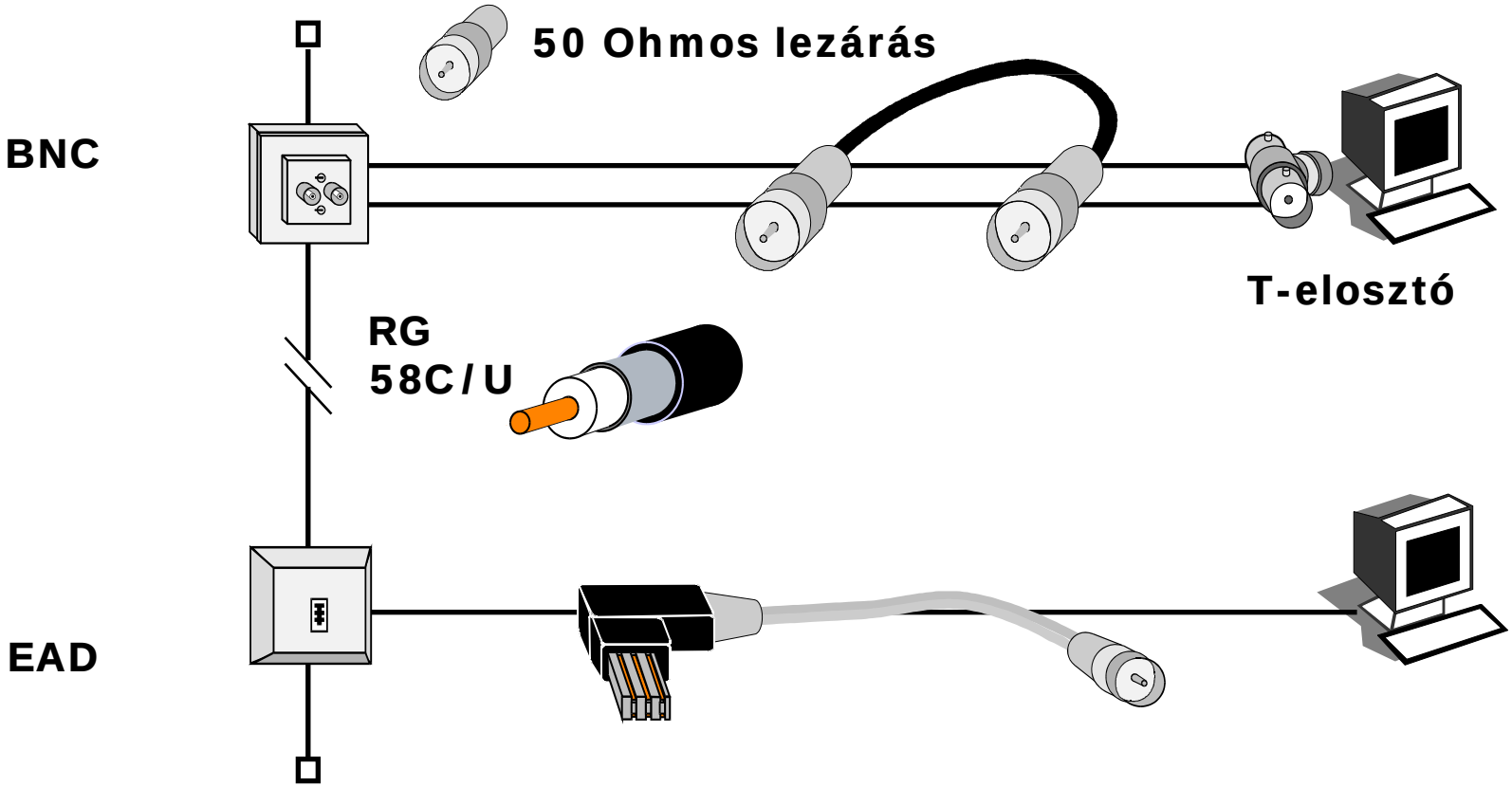


10 Base 2 (Vékony Ethernet)

- BNC csatlakozók, T elosztók, vékony koaxiális kábel
- Max. 30 adó per szegmens
- Sok csatlakozó: sérülékeny, ilyenkor teljes kommunikáció leáll!
  - Kiváltotta a 10BaseT (hubos megoldás)
  - Előnye: olcsóbb mint a hubos megoldás
  - Hátránya: nehéz lenyomozni a hibát
- Kis otthoni hálózatokra jó lenne, de már teljesen eltünt, ahogy a 10Base5 is

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

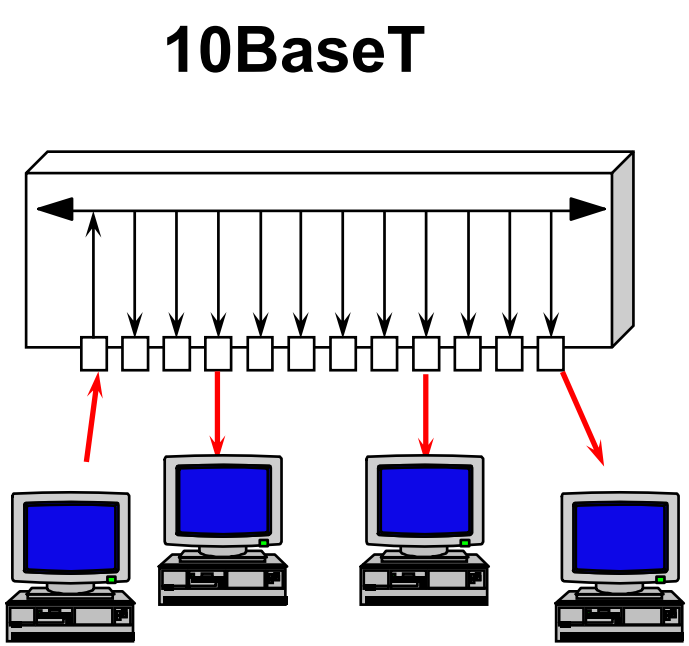
Ethernet kábelezés: 10 Base 2



Ethernet jelismétlő (repeater)

- Több szegmens összekötése
- 5-4-3 szabály (10Mb/s)
  - 5 szegmens
  - 4 ismétlő
  - 3 szegmensen terminálok
- Ütközés: minden porton jam jelzés (ütközési tartomány)
- Kábel meghibásodás: csak az adott szegmensen
  - Rosszul csatlakozott terminál blokkolása
- Nem ismétlik a preamble-t, újat generálnak

10Base T



- Sokkapus ismétlő (multiport repeater) / hub
- Valamely porton észlelt jel a hátlapra jut, onnan minden egyes porton adásra kerül
- Csavart érpárok (2 pár), RJ45 csatlakozó

Az esetleges ütközés a hubban jön létre !

Ethernet hubok alkalmazása

Half-duplex: CSMA/CD

+:

- Tudja kezelni az ütközéseket
  - jam jelet sugároz ki
  - letilt portokat

-:

- Minden keret minden portra
  - Korlátozott terminálszám
- Korlátozott hubszám
- Minden összekötött szegmens **egy sebességen és ugyanazon keretezéssel** működhet csak

- Megoldás: **bridge** (híd) és **switch** (kapcsoló) az adatkapcsolati rétegben

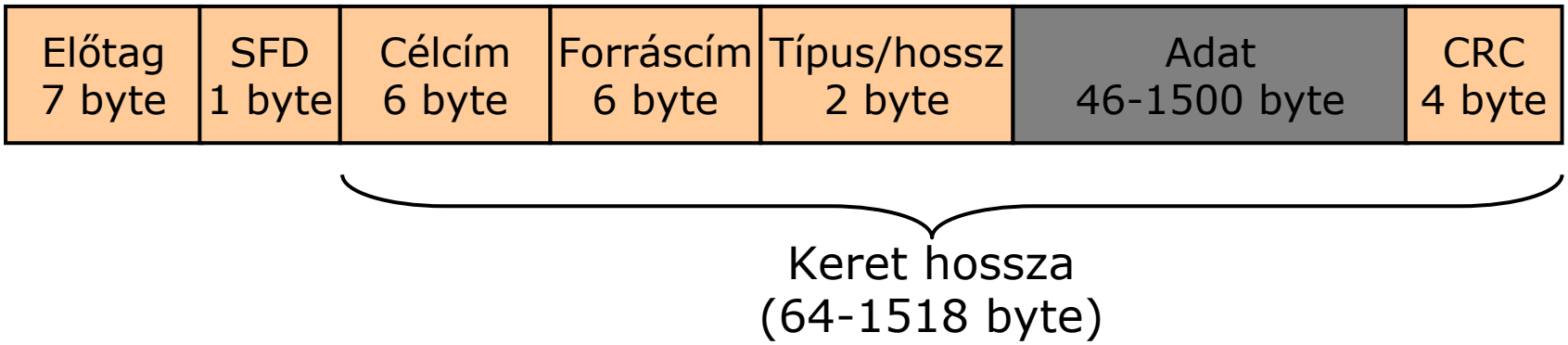
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hubok alkalmazása

- A switchek olcsóbbá válásával elvesztették jelentőségüket

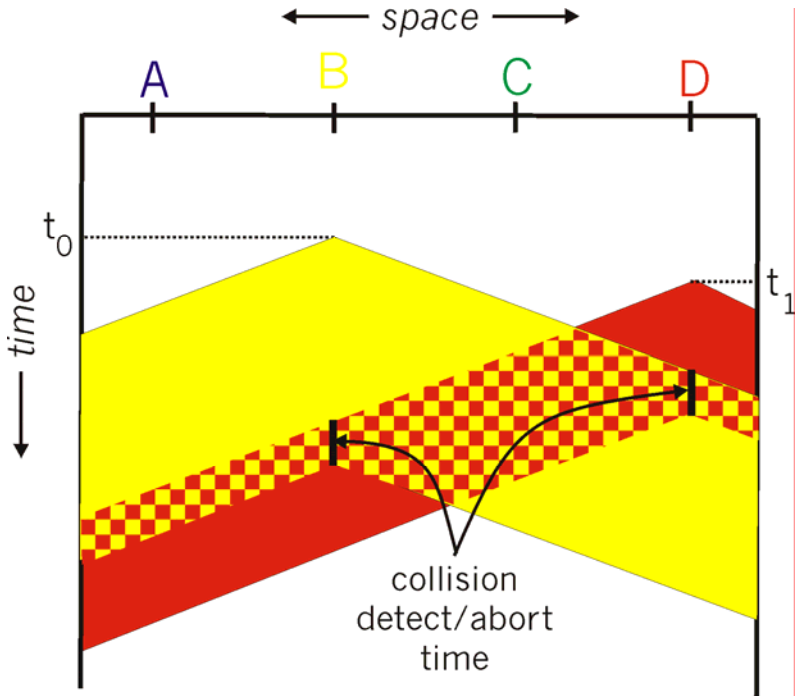
- Pár helyen alkalmazzák még őket:
  - Régi 10Base2 és 10Base5 szegmensek illesztése a mai hálózathoz
  - Protokoll analizátor illesztése a hálózathoz
  - Olyan switch-nél hol nincs STP (Spanning Tree Protocol), 2 port összekötése megbénítja a hálózatot, hubnál csak ez a rész esik ki

Medium Access Control – az Ethernet-keretek felépítése



- Előtag, preamble (7 byte): 10101010…
- SFD (Start Frame Delimiter) – keret kezdete (1 byte)
- Célcím (6 byte), pl. 00:DA:07:9B:43:1B
- Forráscím (6 byte)
- Típus/hossz (2 byte): az adatmező hossza vagy típusa (1500 alatt vagy 1536 felett)
- Adat: min. 46 byte, max. 1500 byte
- CRC - ellenőrző összeg (4 byte)

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



- Grafikus ábrázolás: az ütközési területnek folytonosnak kell lennie a busz mentén

- Legkedvezőtlenebb esetben is (két állomás a busz két végén) minden állomás érzékelje az ütközést:

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

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

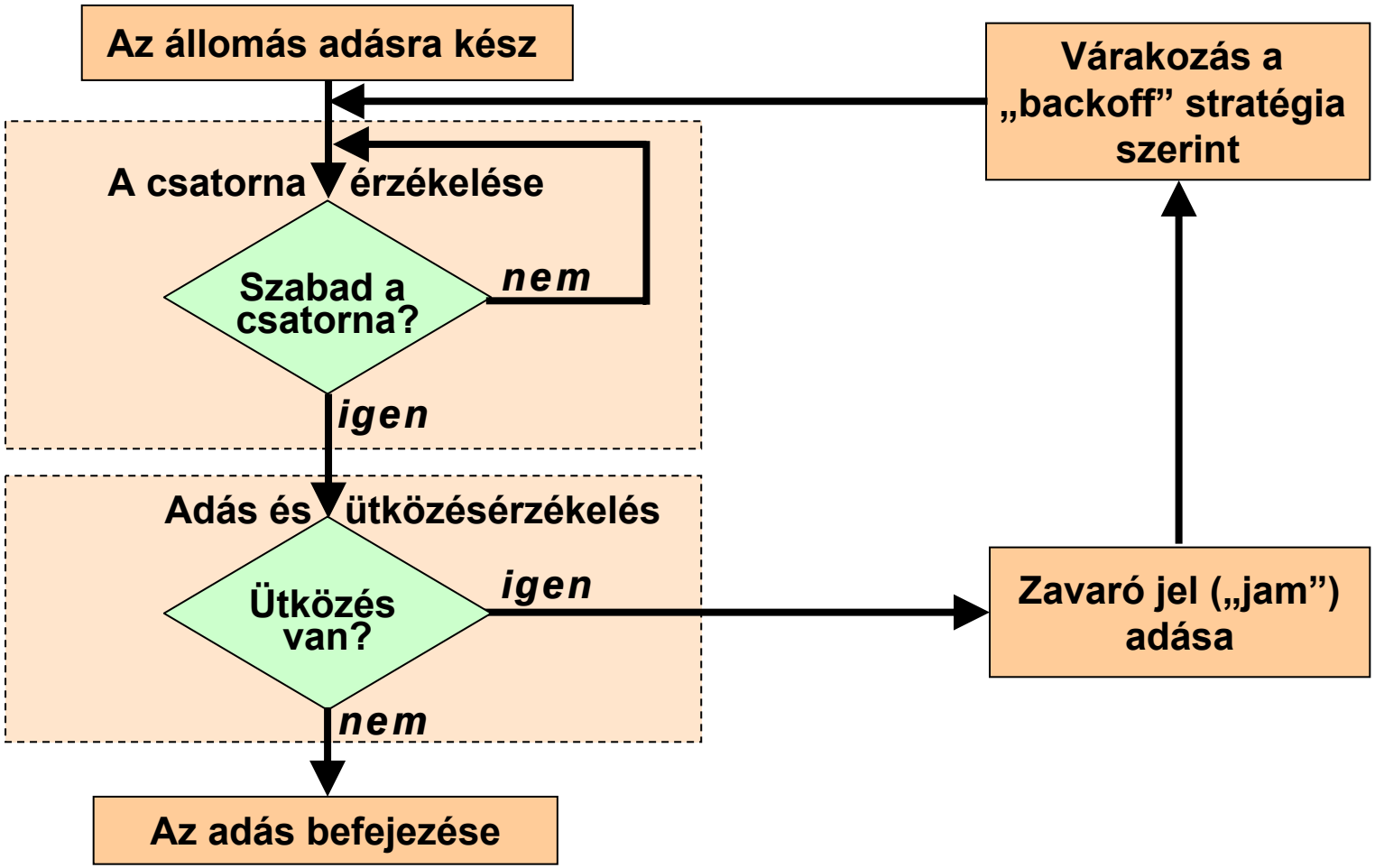
- Résidő = 51.2 µs (2 * (2.5 km + 4 ismétlő késleltetése), 512 bit átvitelének ideje 10 Mb/s Ethernet esetén
- Ezért minimális kerethossz 64 byte

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Medium Access Control – CSMA/CD

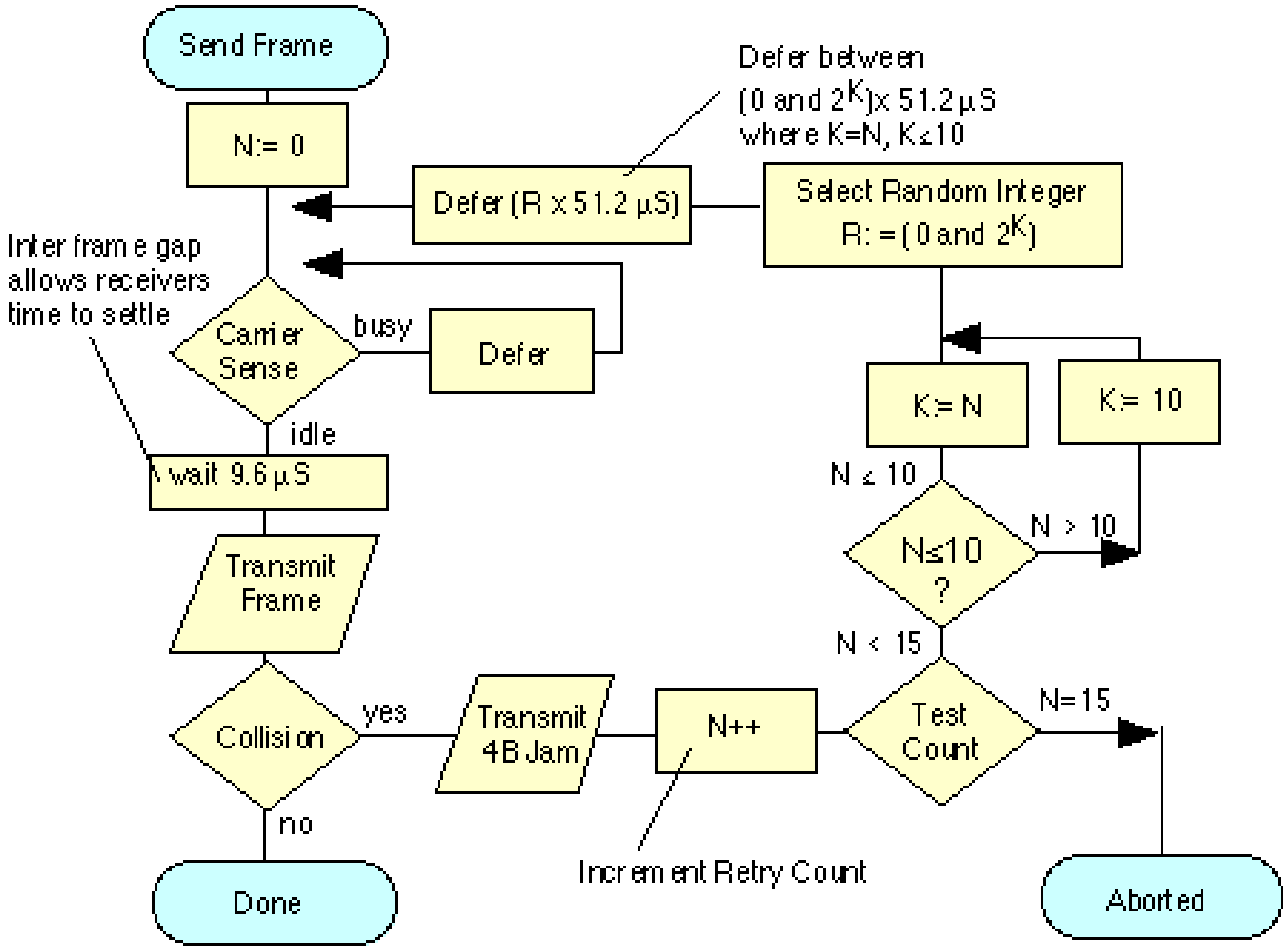
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - Az állomás figyeli a csatornát, a „vivőt” (carrier sense)
  - Ha nem érzékel adást, elkezdi küldeni a keretet
  - Ha kettő vagy több állomás ad, mindegyik abbahagyja az adást: ütközésérzékelés (collision detection)
  - Valamekkora (véletlen) késleltetést („backoff” time) követően az állomás újból megkísérli az adást
- A CSMA/CD-hoz szükséges, hogy
  - **adás előtt** vivőt érzékeljünk (carrier sensing – CS)
  - **adás alatt** érzékeljük, hogy más is ad (collision detection - CD)

Medium Access Control – a CSMA/CD elvi folyamatábrája



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az Ethernet MAC-protokollja



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Magyarázatok a MAC-protokollhoz

- Interframe gap (keretek közötti idő): 96 bit (9,6 µs 10 Mbit/s-nél)
- Retry count (ismétlésszám): N, N=1…15
- Véletlen késleltetésszám: R
  - *R*-et a $0,2^K - 1$ intervallumból sorsoljuk, ahol *K=N*, ha *N<=10,* és *K=10*, ha *N>10*
  - 1. ütközés után: sorsoljuk *R*-et a *{0, 1}*-ből; a késleltetés *R*512* bitidő (1 bitidő 0,1 µs 10 Mbit/s-nál)
  - 2. ütközés után: *R*-et a *{0, 1, 2, 3}*-ből
  - …
  - 10. ütközés után: *R*-et a *{0, 1, 2, 3, 4, …, 1023}*-ből (Ez kb. max. 52,4 ms-ot ad.)
- Jam (zavarás): 32-48 bitnyi ideig, hogy minden állomás biztosan érzékelje az ütközést (CRC hiba)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

LAN-ok - tartalom

- *I. Az „Ethernet”*
  - *IEEE 802.3 Ethernet (a „klasszikus” E.)*
  - IEEE 802.3u Fast Ethernet
  - IEEE 802.3z Gbit/s Ethernet
  - IEEE 802.3ae 10 Gbit/s Ethernet

II. További LAN-ok
  - „Token ring” – 802.5
  - FDDI (ANSI)

III. LAN-ok összekapcsolása

Kapcsolt Ethernet

- Nagyobb forgalom kezelése a buszsebesség növelése nélkül
- Bridge (híd), kapcsoló (switch) bevezetése: nagyobb sebességű Ethernet
- MAC címek alapján szűrik/irányítják a szegmenseken belüli/közötti forgalmat
- Több szegmens összekapcsolása, eltérő szegmensebességek
- Kicsit többet a kapcsolókról a „LAN-ok összekapcsolása” részben

Nagysebességű Ethernet szabványok

- Fast Ethernet
  - **(IEEE 802.3u)**
- Gigabit Ethernet
  - **(IEEE 802.3z)**
- 10Gb Ethernet
  - **(IEEE 802.3ae)**

Jellemzők	**10/100 Mbit/s**	**1 Gbit/s**	**10 Gbit/s**
Fizikai közeg	▪ **UTP** ▪ **üvegsz.**	▪ **koax** ▪ **UTP** ▪ **üveg**	▪ **üveg** ▪ **(rézv.)**
Résidő (slot time) [byte]	64	512	**NINCS CSMA/CD MAC PROT.**
Küldési próbálkozás	16		
Visszalépési algoritmus korlátja	10		
Minimális keretméret [byte]	64		
Maximális keretméret [byte]	1518		

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fast Ethernet

100 Base-X

- Különböző médiumokra (X) tervezték:
  - Category 5 árnyékolatlan (UTP) kábel
  - Category 5 árnyékolt (STP) kábel
  - Optikai szál

- Mindegyik más fizikai médiumfüggő alréteggel rendelkezik

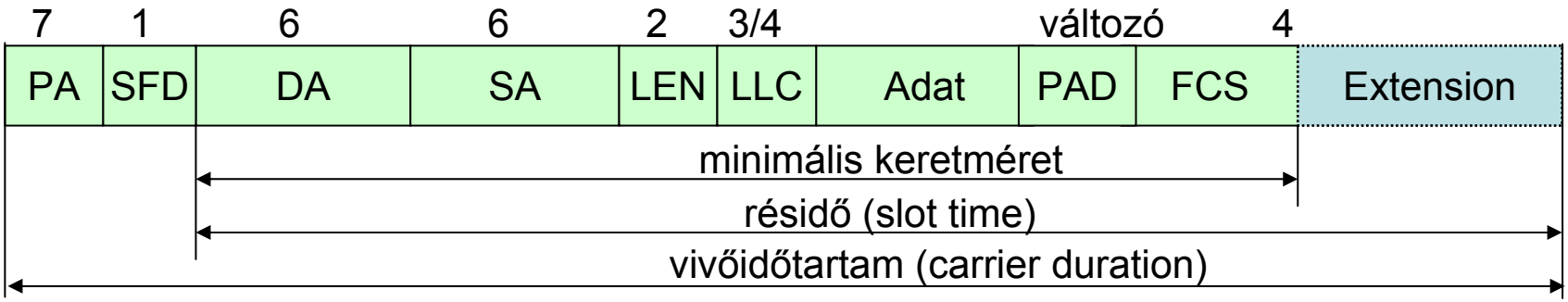
- Az FDDI hálózatra kifejlesztett **4B5B** (4B/5B) **bit kódolás**t adaptálták rá

- Különböző sebességű linkek: bridge-k megjelenése

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IEEE 802.3z Gigabit Ethernet – Megnyújtott keretformátum

- „Félduplex” üzemmód:
  - Mint a klasszikus Ethernet, de sokkal rövidebb keretidők
  - Két megoldási lehetőség:
    - Megnövelt kerethossz
    - Vivő kiterjesztés (Carrier-extension) bitek hozzáadása a keretekhez
      - Ezt választották, mert ezzel nem változott a szabvány
- Ma tipikusan full duplex switchekkel



PA	Preamble	LLC	Logical Link Control
DA	Destination Address	PAD	Padding
SA	Source Address	FCS	Frame Check Sequence (CRC-32)
SFD	Start Frame Delimiter	LEN	Length

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IEEE 802.3ae - 10 Gbit/s Ethernet (XGE) - Áttekintés

- Ez a legújabb az Ethernet-családban, 2002 közepén hagyták jóvá
- 10 Gigabit-Ethernet Alliance (http://www.10gea.org)
- IEEE 802.3ae:
  - további 10-szeres sebességnövelés a GbE-hez képest
  - az Ethernet alkalmazási területének kiterjesztése a WAN-okra
- Kizárólag full duplex switchekkel, nincs többé CSMA/CD
- Főként üvegszál, de van rézvezetékes változata is
  - 7 különböző PHY-réteg

Ethernet jövője

- 10 Gb Ethernet elterjedőben, pl. adatközpontok összekötésére
- 40 Gb és 100 Gb Ethernet: megszületett a szabvány 2010-ben, 802.3ba
- Metcalfe próféta: 2015-ig Terabit Ethernet, viszont ehhez teljesen új féle Ethernet szabványok

IEEE 802.3 Ethernet – összefoglalás

- Az Ethernet nagy fejlődésen ment át
  - Sebességben 3 nagyságrend!
  - Lefedési/alkalmazási területet illetően: LAN-tól a WAN-ig
- A különböző IEEE 802.3 szabványok közös tulajdonságai:
  - Keretformátum
  - Címzés
- Különböző lehet
  - a közeghozzáférés
    - a CSMA/CD fokozatos kivonása
  - a fizikai közegek
    - koaxiális kábeltől a monomódusú üvegszálig
- Megvalósítás szempontjából mindegyik változatra igaz:
  - Könnyű telepítés
  - Költséghatékonyság

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

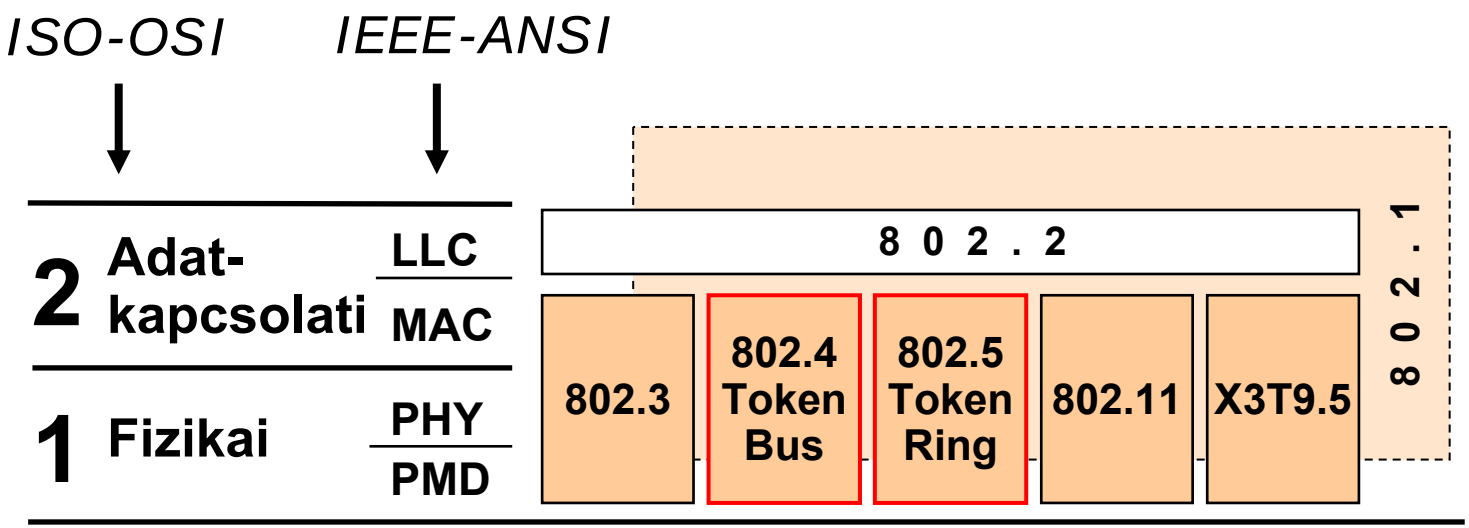
Lokális hálózatok II. rész

További lokális hálózatok:

- *Token bus (IEEE 802.4)**
- *Token ring (IEEE 802.5)*
- *FDDI (ANSI)*
- *FiberChannel (ANSI)**

* nem tárgyaljuk

A lokális hálózatok architektúrája



- LLC : Logical Link Control
- MAC: Medium Access Control
- PHY: Physical
- PMD: Physical Medium Dependent

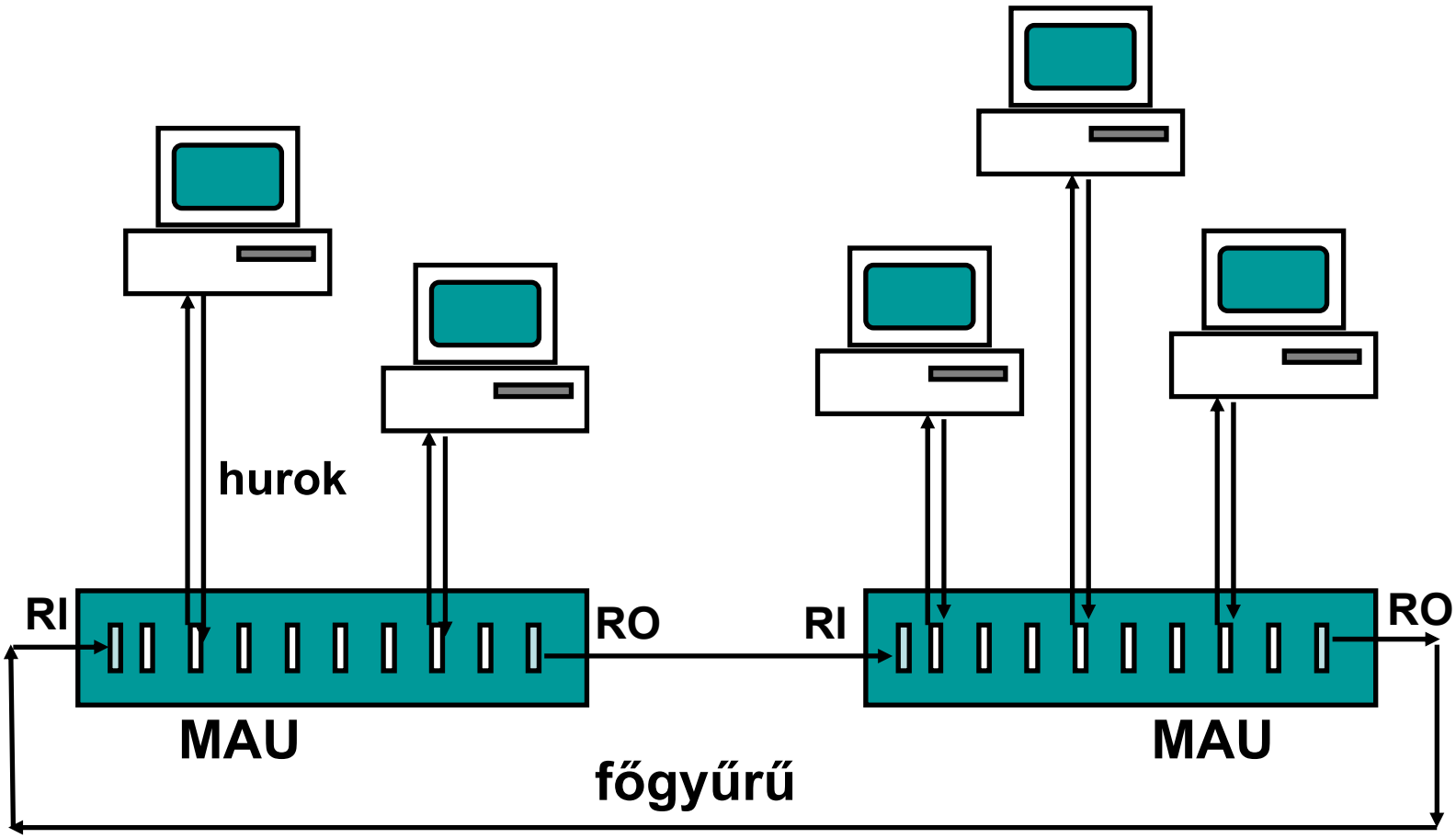
- *802.1: közös funkciók valamennyi LAN-ra és MAN-ra*
- *pl. együttműködés, biztonság (interworking, security)*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

További LAN-ok

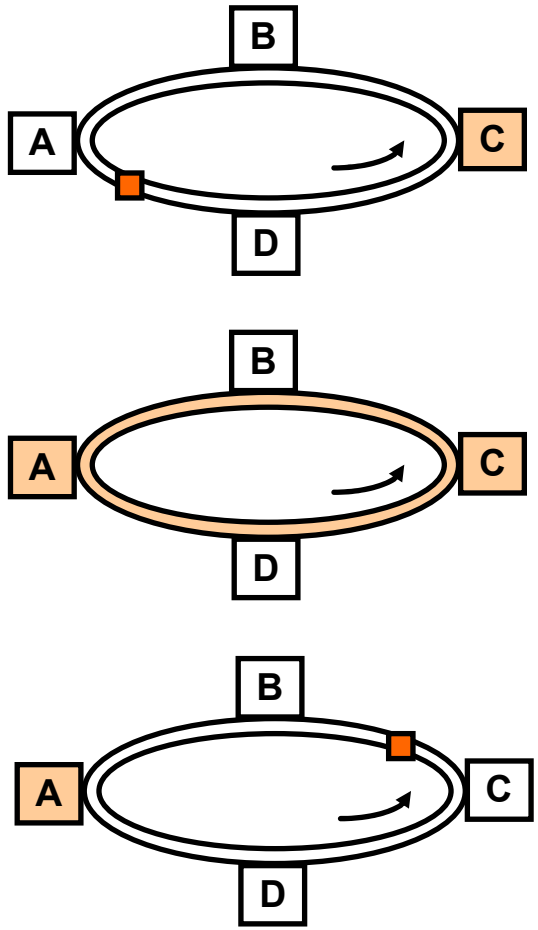
- 802.4: Token bus (vezérjeles busz)
  - Talán a legjobb MAC protokoll, de bonyolult
  - A kezdeti ipari alkalmazások után kihalt (General Motors)
- 802.5: Token ring (vezérjeles gyűrű)
  - Az IBM hatására szabványosították
  - Még létezik, de csak nagyon kevés helyen
- ANSI FDDI
  - FDDI – Fiber Distributed Data Interface
  - A LAN-oknál egy nagyságrenddel nagyobb sebességet és lefedettséget biztosít
  - Gyűrű-topológia és MAC-protokoll
  - Még létezik pár helyen, de kifutóban
- *Mivel az alkalmazott megoldások és közeghozzáférési protokollok érdekesek és tanulságosak, röviden foglalkozunk ezekkel is*

Token ring az IBM kábelezési rendszerén



Az IEEE 802.5 szerinti tokenes protokoll működése

- Az adni kívánó állomás kivárja, míg megérkezik hozzá a token
  - a token egy speciális rövid keret, 3 Byte
  - megsérti a differenciális Manchester kódolást
- A tokent átírja üzenetkeretre, és kiegészíti az adatokkal
- Az állomások kimenetükre másolják a bemeneten jött adatokat
- A címzett feldolgozza a neki szóló keretet, továbbítja, mint a többi állomás
  - azzal a különbséggel, hogy a címzett a válasz biteket is beállítja a keret végén.
- A küldő kivonja a csomagot a gyűrűről
- A küldő új tokent indít útra



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Monitor állomás

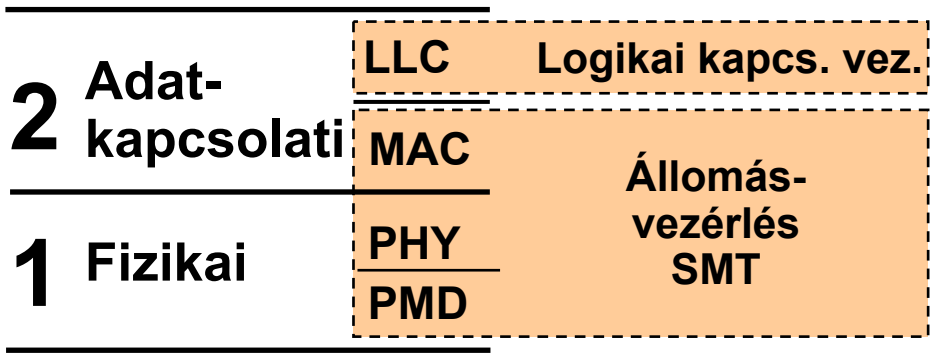
- Egy monitor állomás, többi standby állomás
- Monitor felügyeli:
  - egy token a gyűrűn
  - órajel biztosítása
  - levenni sokáig keringő kereteket
- Új monitor kijelölése versennyel ha:
  - nincs token vagy
  - nincs monitor

A vezérjel továbbadása

- **Lassú gyűrű: (4 Mbps)**
  - Egyszerre csak 1 keret van a gyűrűn
  - A vezérjelet a feladó állomás csak a keret visszaérkezése után továbbítja
- **Gyorsabb gyűrű: (16 Mbps)**
  - Egyszerre több keret van a gyűrűben
  - A vezérjelet a feladó állomás a keret elküldése után azonnal továbbítja (early token release)

FDDI - Fiber Distributed Data Interface

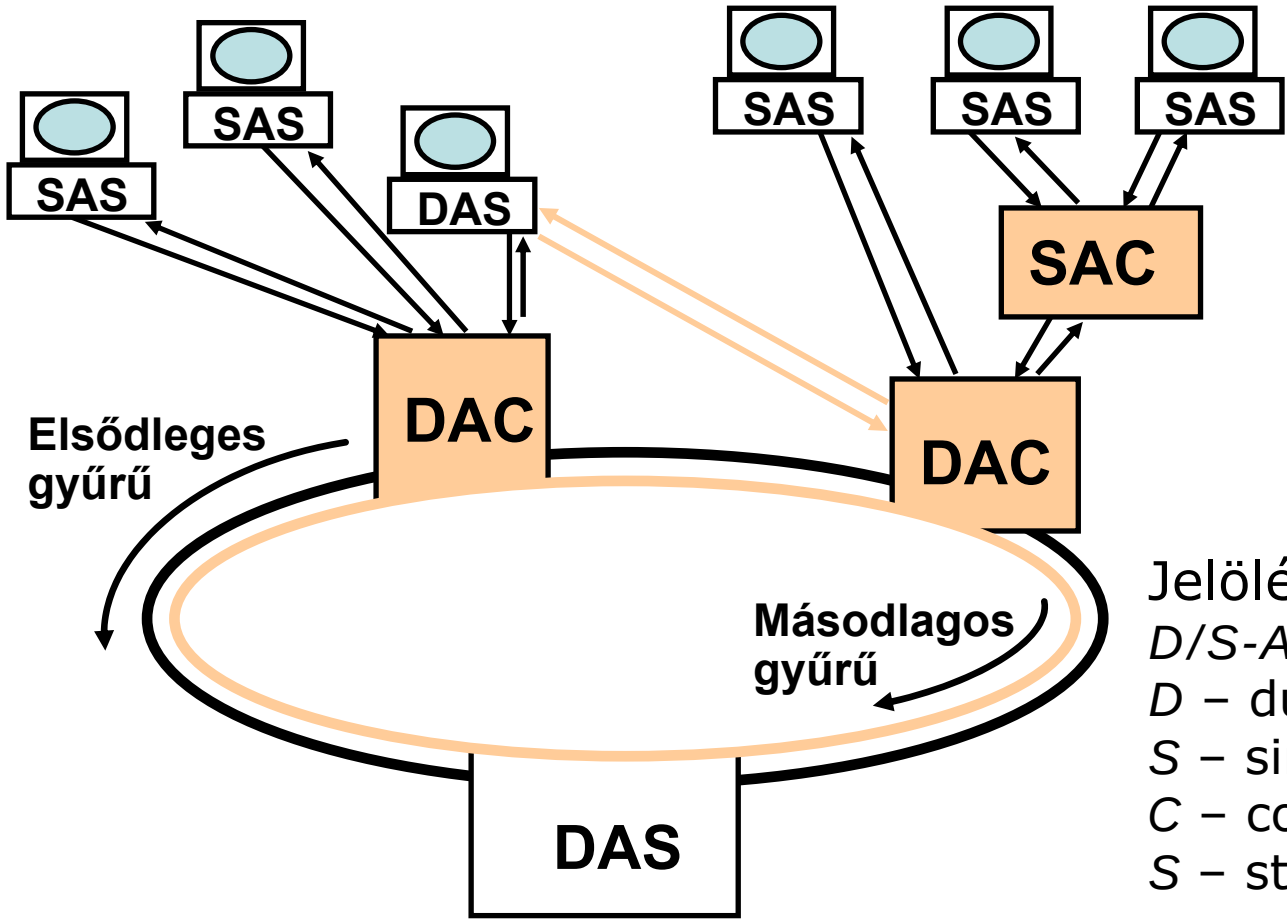
- Két optikai szálas gyűrű, melyekben az adatforgalom ellentétes irányú (tartalék meghibásodás esetén)
- Több-módusú üvegszálak, 4B/5B kódolás
- A LAN-okhoz képest nagyobb sebességgel és területi lefedéssel (100 Mbit/s, 100-200 km), MAN-ra is jó
- Tokenes közeghozzáférési protokoll
- Logikai gyűrű, fizikai gyűrű- és fa-topológia



SMT Station Management
MAC Medium Access Control
PHY Physical
PMD Physical Medium Dependent

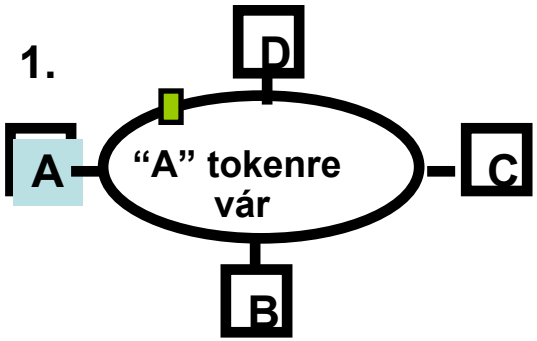
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

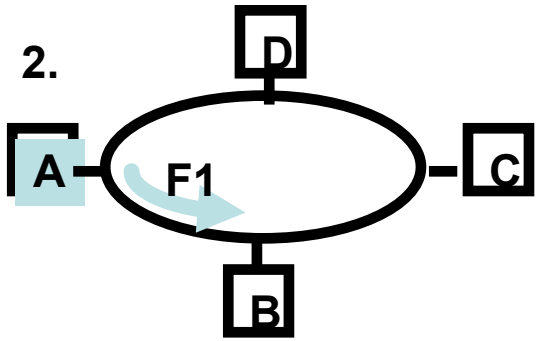
Az FDDI topológiája



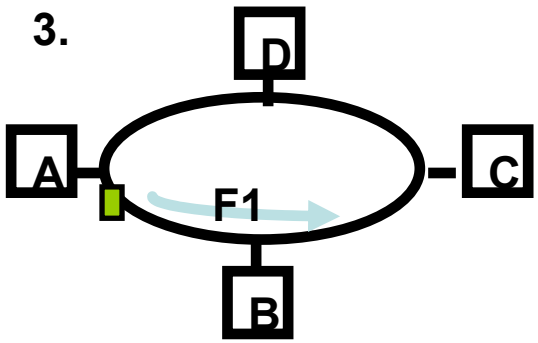
Jelölés:
D/S-A-C/S
D – dual
S – single
C – concentrator
S – station

Az FDDI tokenes protokolljának működése

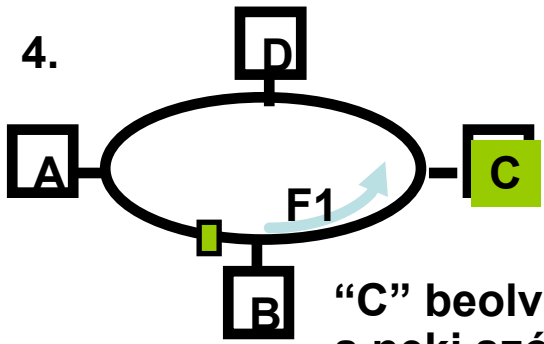




“A” a token helyett F1-et küldi C-nek



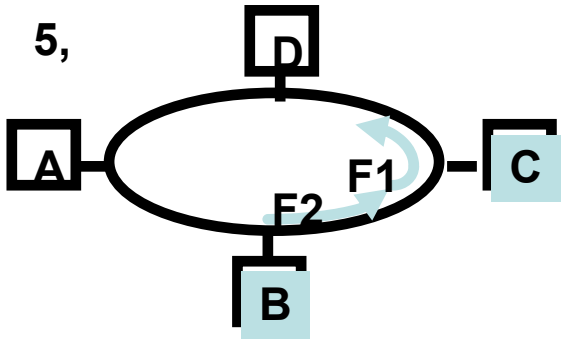
F1 után azonnal továbbadja a tokent



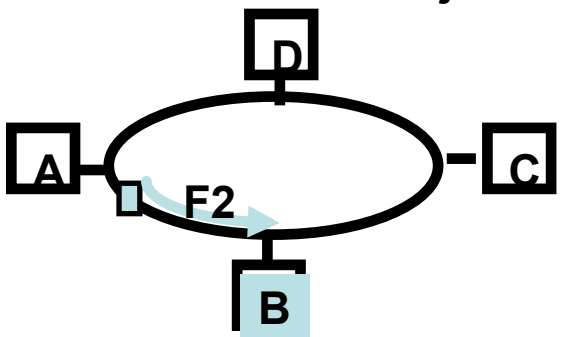
“C” beolvassa
a neki szóló
F1-et és másol

Az FDDI tokenes protokolljának működése

5,

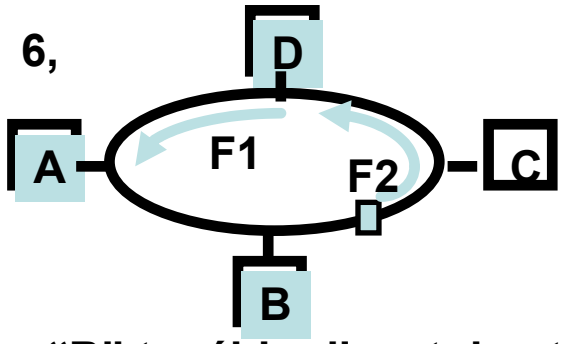


“C” tovább másol
“B” a tokent kivonja és ad

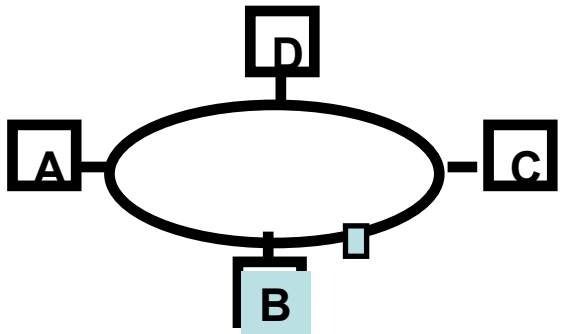


“B” kivonja F2-t

6,



“B” továbbadja a tokent, “D” másol
“A” kivonja F1-et



“B” elengedi a kapott tokent

FDDI vs. token ring

- Token ring: egy állomás addig nem állít elő új vezérjelet, amíg kerete a gyűrű körbejárása után vissza nem ért (lassú gyűrű)

- FDDI: a keret elküldésének pillanata után már új vezérjelet bocsáthat ki a gyűrűre
  - Pl.1000 állomás, 200 km optikai szál: jelentős késleltetés lenne enélkül
  - egy nagy gyűrűben akár több keret is keringhet egyszerre

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az FDDI MAC protokollja a „timed token ring” protokoll

- Az állomások megállapodnak egy megcélzott TRT-ben (Token Rotation Time)
  - TRT = a gyűrű teljes késleltetése + adási idők
- Ez felső korlátot ad a késleltetésre
- Némelyik állomás adási “kvótával” rendelkezik
  - A hozzá érkező tokent a kvóta idejéig megtarthatja, ezalatt adhat
  - Ez a „szinkron” forgalom
- A kvótán felül csak akkor adhat egy állomás, ha „belefér” TRT-be
  - Ez az „aszinkron” adás

FDDI alkalmazása

- 90-es évek elején népszerű volt
  - Ethernet akkor csak 10Mb/s, token ring 4Mb/s vagy 16Mb/s
- Fast Ethernet már jóval olcsóbb volt, Gigabit Ethernet pedig gyorsabb és olcsóbb

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

Lokális hálózatok III. rész

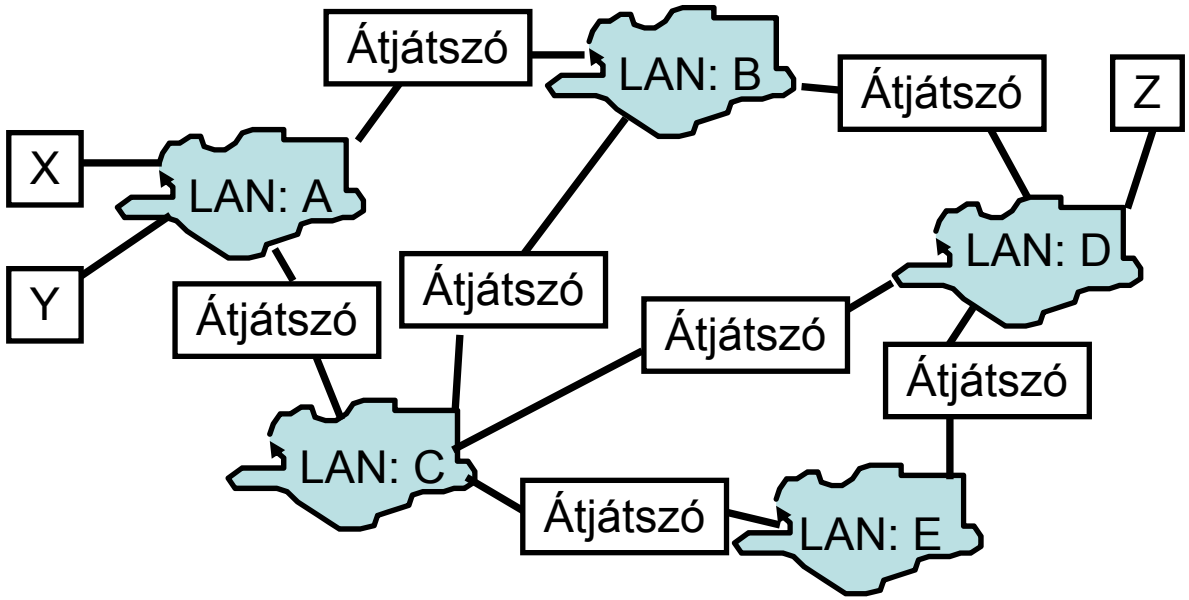
LAN-ok összekapcsolása

2013. március 7.

A LAN-ok korlátainak átlépése

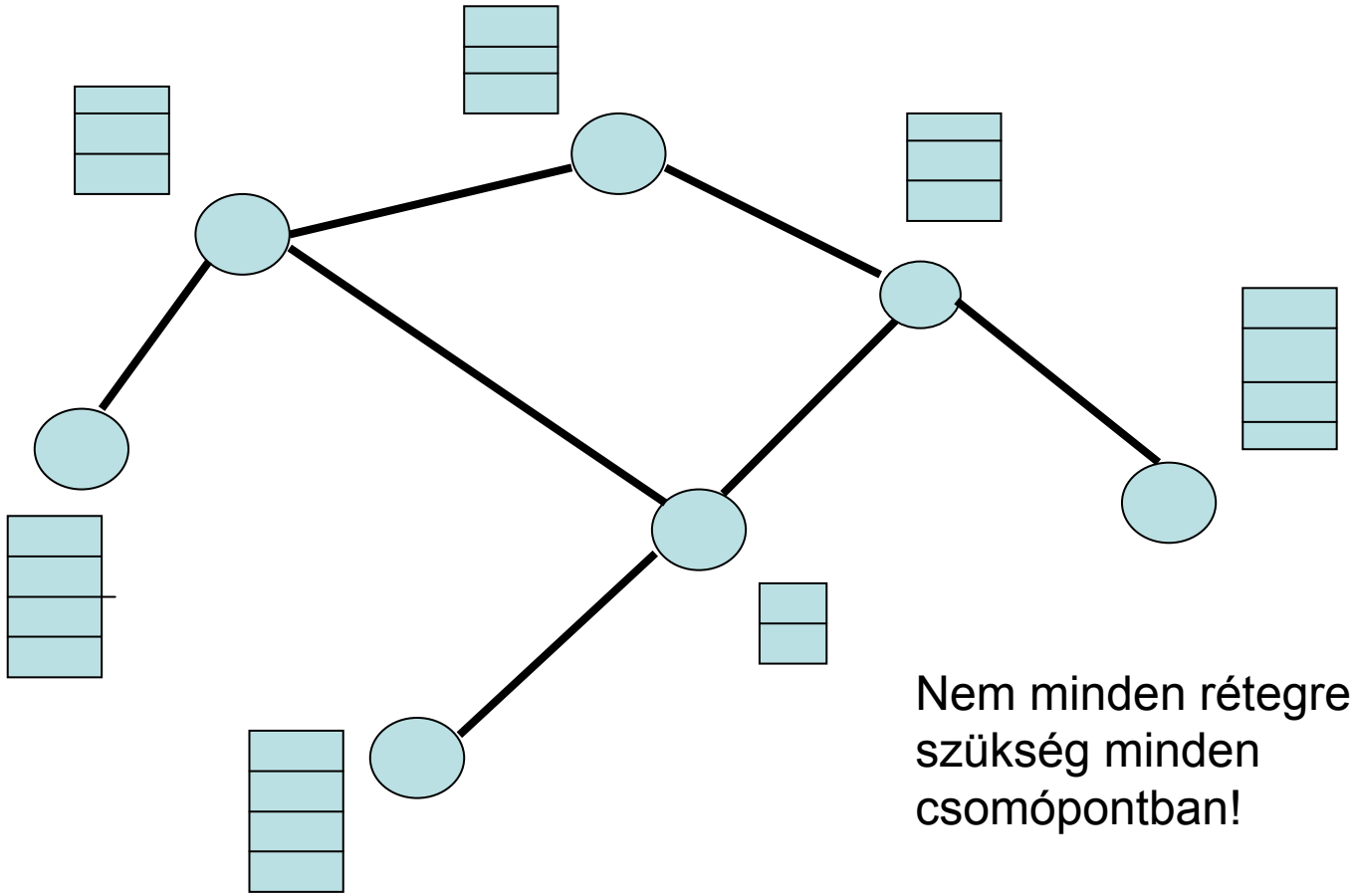
- Korlátok:
  - távolság
  - állomások száma
  - állomások típusa

- LAN-ok kiterjesztése:
  - A LAN-korlátokat egy **átjátszó** segítségével átléphetjük



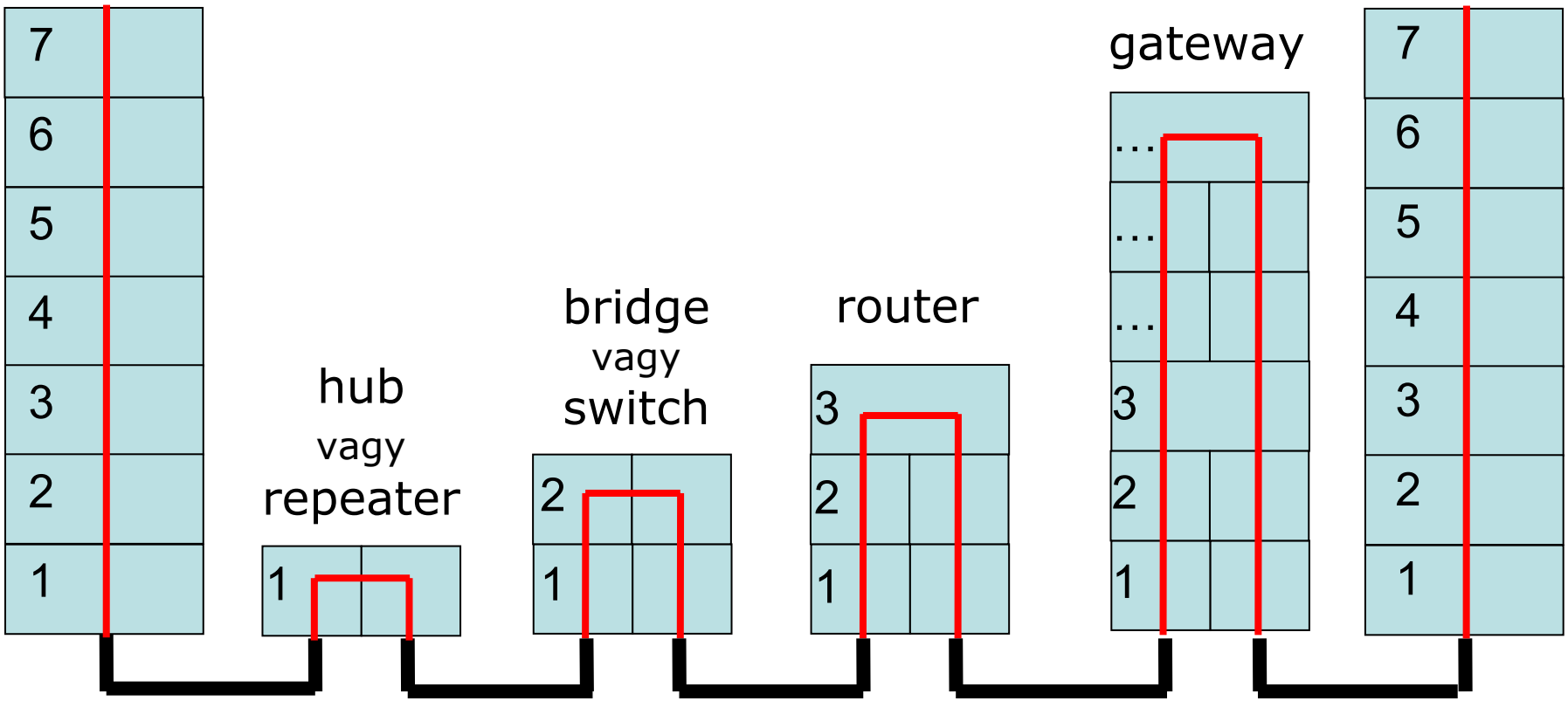
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Protokollrétegek a hálózati csomópontokban



Nem minden rétegre van szükség minden csomópontban!

Különböző képességű átjátszók



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Átjátszó eszközök megnevezése

Angol név	Magyar név	OSImax. réteg	Tipikus port-szám	Funkcionalitás
repeater	jelismétlő	L1	2	jelerősítés, -továbbítás
hub	többportos jelismétlő	L1	4-16	jelerősítés, -továbbítás minden porton; több eszköz összekapcsolása
bridge	híd	L2	2-8	nem ütköző szegmensek összeköttetése; továbbítás csak a szükséges porton; átviteli közegek közötti konverzió újrakeretezéssel
switch	kapcsoló	L2	4-32	nem ütköző szegmensek összeköttetése; továbbítás csak a szükséges porton, azonos közegen, újrakeretezés nélkül
router	útválasztó	L3	2-10	útválasztás L3 címek alapján
gateway	átjáró	>L3	2-4	protokollkonverzió, -együttműködés

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Bridge-ek és switchek

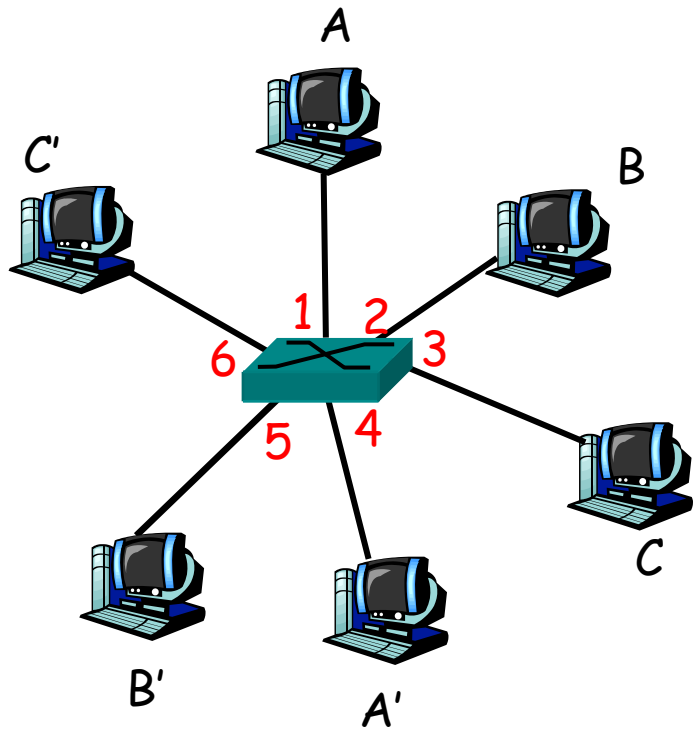
- Nagyon hasonló a kettő:
  - Adatkapcsolati rétegbeli összeköttetés
  - Többféle sebességet is képesek kezelni
- Történetileg:
  - Először: híd
  - Később: kapcsoló a LAN-okban (kapcsolt Ethernetben)
- Az összeköttetés
  - Híd: tipikusan LAN-szegmenseket köt össze
  - Kapcsoló: LAN-szegmensek és egyedi munkaállomások is összeköthetők
- A híd képes lehet különböző LAN-okat összekötni
  - pl. Ethernetet token ringgel
- Az eszközök megvalósítása tipikusan „tárolj és továbbíts” (store and forward) (közös memória, kapcsolómátrix nélkül)

Switch - kapcsoló

- Adatkapcsolati rétegbeli eszköz
  - tárolja és továbbítja az Ethernet-kereteket
  - megvizsgálja a keretfejrészt és szelektíven továbbítja a keretet a MAC célcím alapján
  - a keretek továbbításakor CSMA/CD-t használ (ha nem full duplex)
- Transzparens
  - a végpontok nem tudnak a kapcsolók jelenlétéről
- Plug-and-play, self-learning
  - a kapcsolókat nem kell konfigurálni

Switch: több kapcsolat egy időben

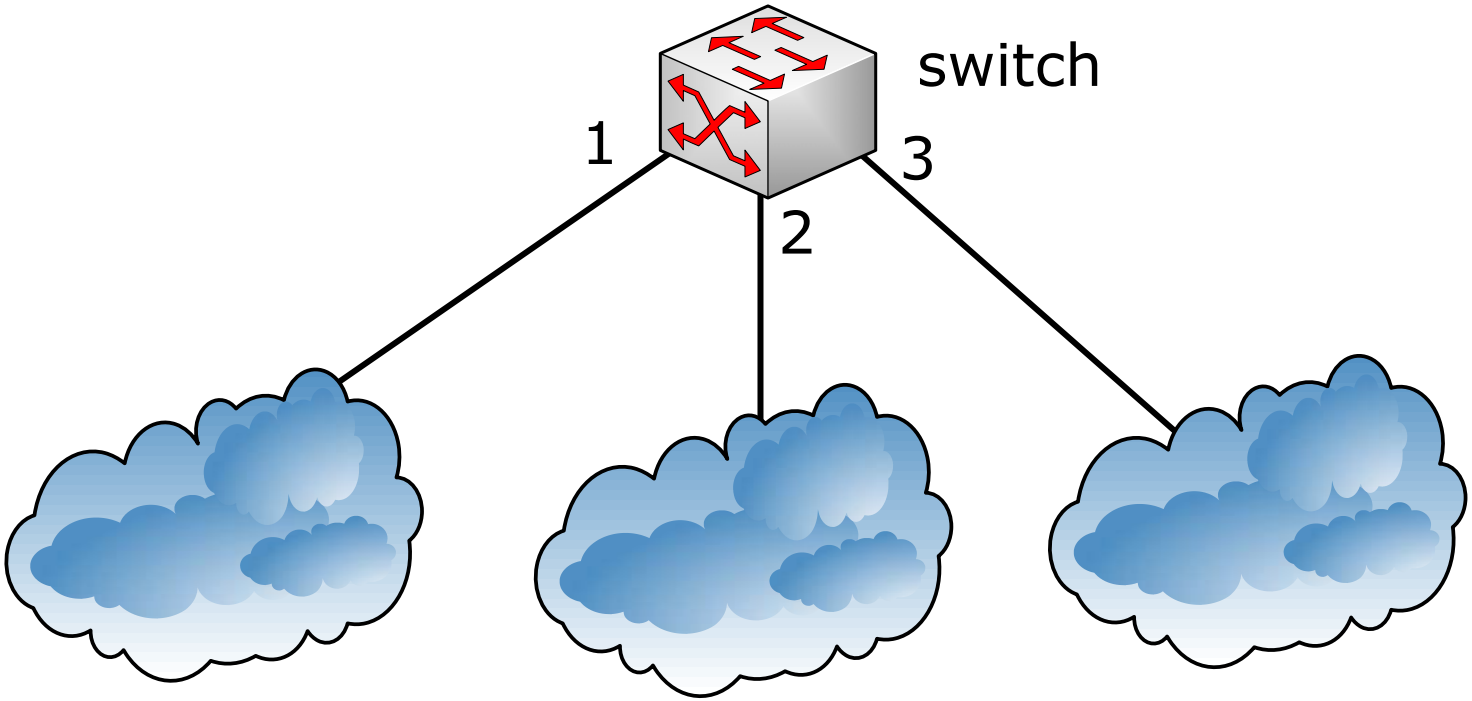
- Hosztok számára dedikált, közvetlen kapcsolat a switch-hez
- Switch puffereli a csomagokat
- Ethernet protokoll van alkalmazva minden bejövő linken, de nincs ütközés, full duplex
  - Minden link egy saját ütközési tartomány
- *switching:* A-A' és B-B' között kapcsolat egyidőben, ütközés nélkül
  - Hub-al nem lehetséges



switch 6 interfésszel (1,2,3,4,5,6)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kerettovábbítás szegmensek között



Hogyan határozza meg a kapcsoló, hogy melyik szegmensre kell továbbítania?

Öntanulás – self-learning

- Van kapcsolótáblája (switching table)
- Bejegyzés a táblában:
  - (MAC Address, Interface, Time Stamp)
  - régi bejegyzéseket eldobja
- Megtanulja, hogy melyik végpontokat melyik interfészen keresztül tudja elérni
- Amikor vesz egy keretet, megtanulja azt, hogy hol, melyik szegmensen van a küldő
  - bejegyzi a küldő/szegmens párokat a táblába

Szűrés/továbbítás

Amikor a kapcsoló vesz egy keretet:

megnézi a switching table-t a MAC cél-cím alapján

if van bejegyzés az adott MAC cél-címre

then{

if a cél azon a szegmensen van, ahonnan jött a frame

then eldobja a keretet

else továbbítja a megadott interfészre

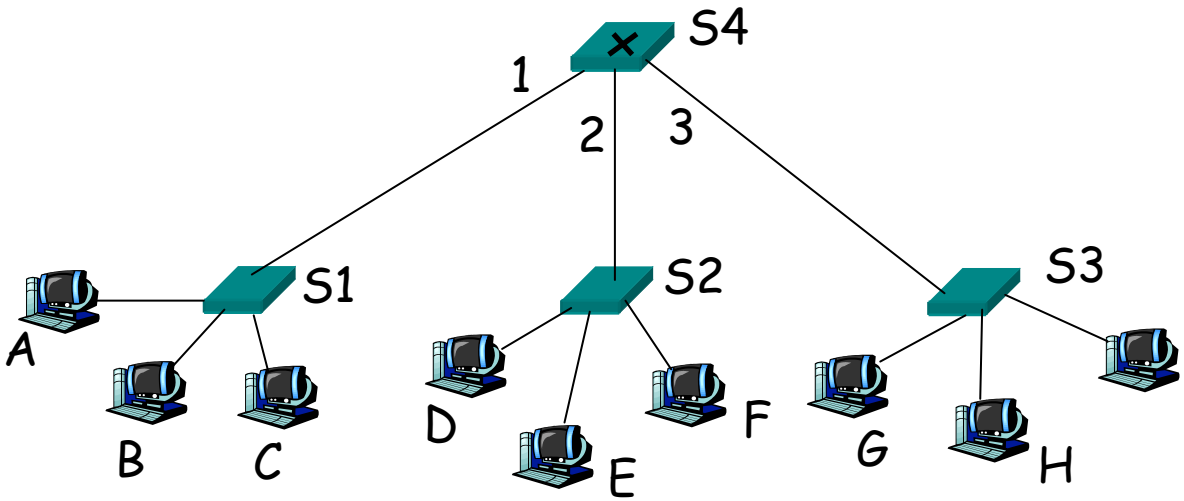
}

else elárasztás

továbbítás minden interfészre, kivéve azt, amelyről érkezett

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa

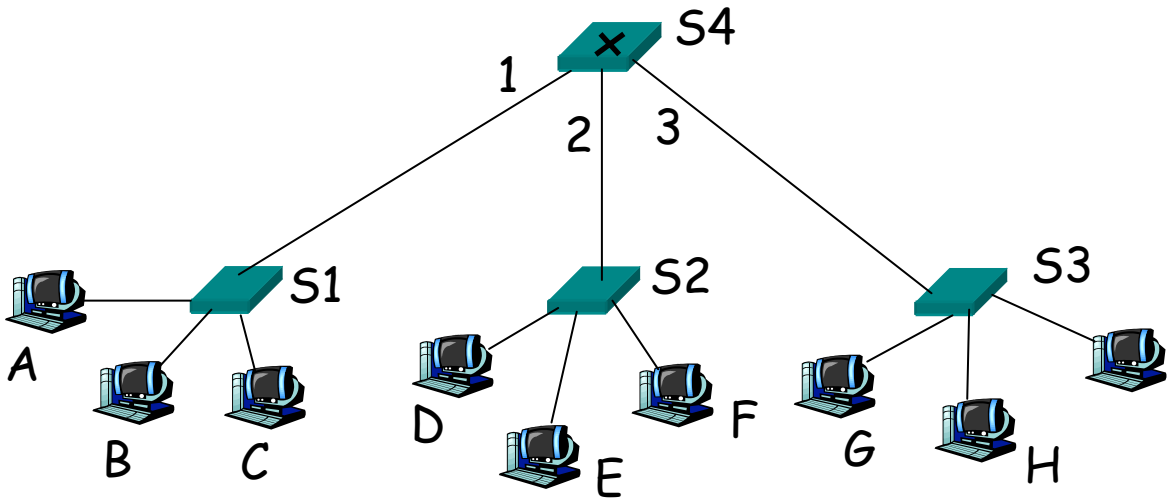


address	interface
A	1
B	1
E	2
G	3
I	

- A kapcsoló vesz egy C-től D-nek menő keretet
  - bejegyzi a táblába, hogy C az 1-es interfészen érhető el
  - mivel D nincs benne a táblában, továbbítja a keretet a 2 és 3 interfészre
- D veszi a keretet

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa (folyt.)



address	interface
A	1
B	1
C	1
E	2
G	3

I

- A kapcsoló veszi a keretet D-től
  - bejegyzi a táblába, hogy D a 2-es interfészen érhető el
  - mivel C benne van a táblában, továbbítja a keretet az 1-es interfészre (csak oda)
- C veszi a keretet

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

Vezeték nélküli LAN-ok IEEE 802.11

WLAN –Wireless Local Area Network
Wi-Fi – Wireless Fidelity

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

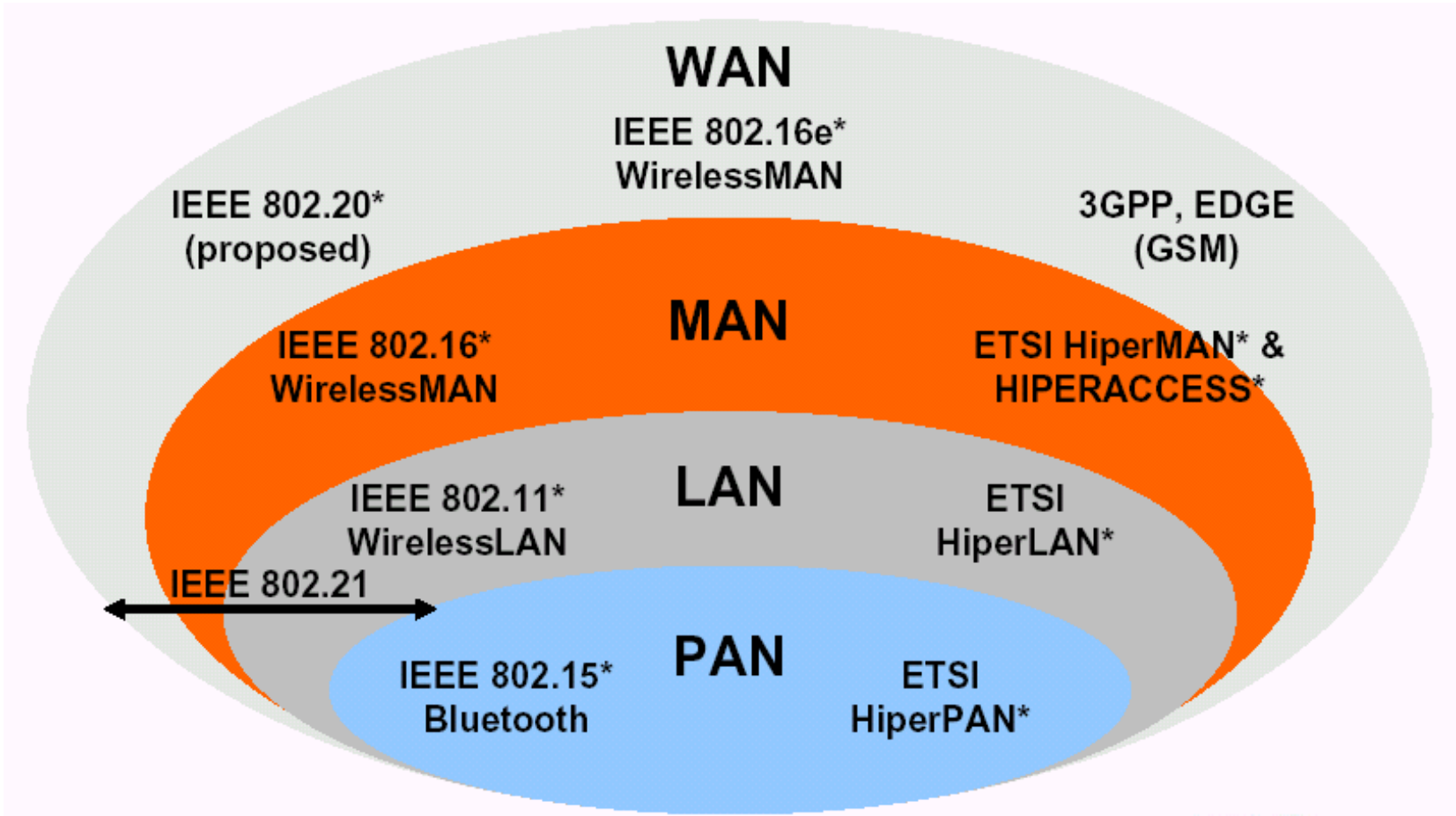
2013.március 14.

A számítógép-hálózatok klasszikus osztályozása területi lefedés szerint

- WAN – *Wide Area Network* – nagy kiterjedésű hálózat
  - távolsági megkötés nélküli, tetszőleges kiterjedésű hálózat
    - akár ***globális méretű*** is lehet
- MAN – *Metropolitan Area Network* – városi/nagyvárosi hálózat
  - eredetileg: egy tipikus USA-beli metropolitan area, de nem feltétlenül város
    - ***néhány tíz km***
- LAN – *Local Area Network* – helyi v. lokális hálózat
  - tipikusan vállalaton, intézményen belüli hálózat
    - max. ***néhány km-es*** távolságok
- PAN – *Personal Area Network* – személyi hálózat

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Vezetéknélküli hálózatok osztályozása kiterjedésük szerint



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A wireless LAN-ok jellemzői

WLAN jellemzők:

- pár száz méter
- 1-2 Mbit/s-től a 100 Mbit/s-ig
- ISM sávban (engedélymentes): 2,4 GHz, 5,8 GHz

Jellegzetes alkalmazások:

- Épületen belüli LAN-ok részeként
  - kórházak, áruházak, hotelek, egyetemi campus, műemlék-épületek
- Közeli épületek közötti kapcsolat, pl. utca felett
- Otthoni iroda, kisvállalati iroda (SOHO – small office – home office)
- Nyilvános Internet-elérési pont

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

WLAN-eszközök

WLAN-kártya

asztali számítógépekbe (PCI, ISA)

hordozható eszközökbe (PCMCIA)

AccessPoint (AP)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

802.11-es szabványok

- ***Különböző alszabványok***
  - 802.11 – 1-2 Mbit/s, 2,4 GHz, FHSS/(DSSS/infra)
  - 802.11a – 54 Mbit/s, 5 GHz, OFDM
  - 802.11b – 11 Mbit/s, 2,4 GHz, DSSS, 11-13 csatorna
  - 802.11g – 54 Mbps, 2,4 GHz, OFDM / DSSS, 13 csatorna
  - 802.11n – akár 600 Mbit/s, 2,4/5 GHz, OFDM MIMO
  - 802.11ac- fejlesztés alatt, 5GHz, max 1Gbps, multi-user MIMO, 256QAM
- ***További alszabványok fontos kiegészítő funkciókra***
  - 802.11e – QoS-támogatás
  - 802.11h – automatikus teljesítményszabályozás (ATPC) és dinamikus csatornaválasztás (DFS)
  - 802.11i – adatbiztonság, titkosítás (pl: AES titkosítás)
  - 802.11j – 802.11a - HiperLAN2 együttélés
  - 802.11s – mesh-üzemmódú működés

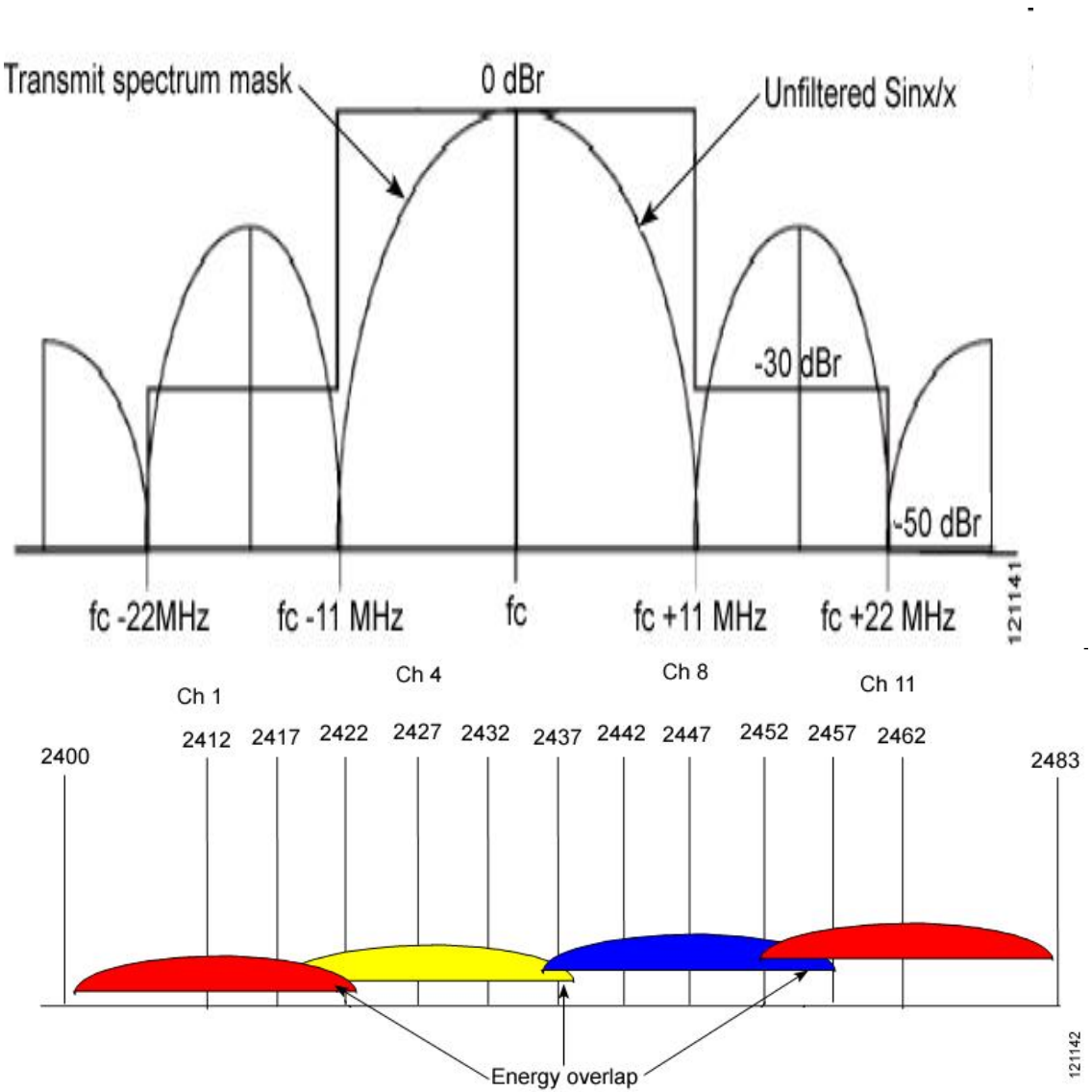
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csatornák (2,4Ghz)

- Pl. egy felosztás: 2.4000–2.4835 GHz sávban:
  - 13 db 22 MHz-es csatorna, egymástól 5 MHz-re a középfrekvencia
- Spektrális maszk minden csatornára (átlapolódás miatt)
  - Frekvencia közepétől 30dB-es csillapítás +/-11Mhz-re
- Egyszerre lehet használni pl. 1.,6.,11.csatornát átlapolodás nélkül
  - Közel-távol probléma akkor is gond lehet!
- Így is interferencia: mikrosütő, cordless telefon, Bluetooth
- 5Ghz-es sávban 23 nem átlapolódó csatorna

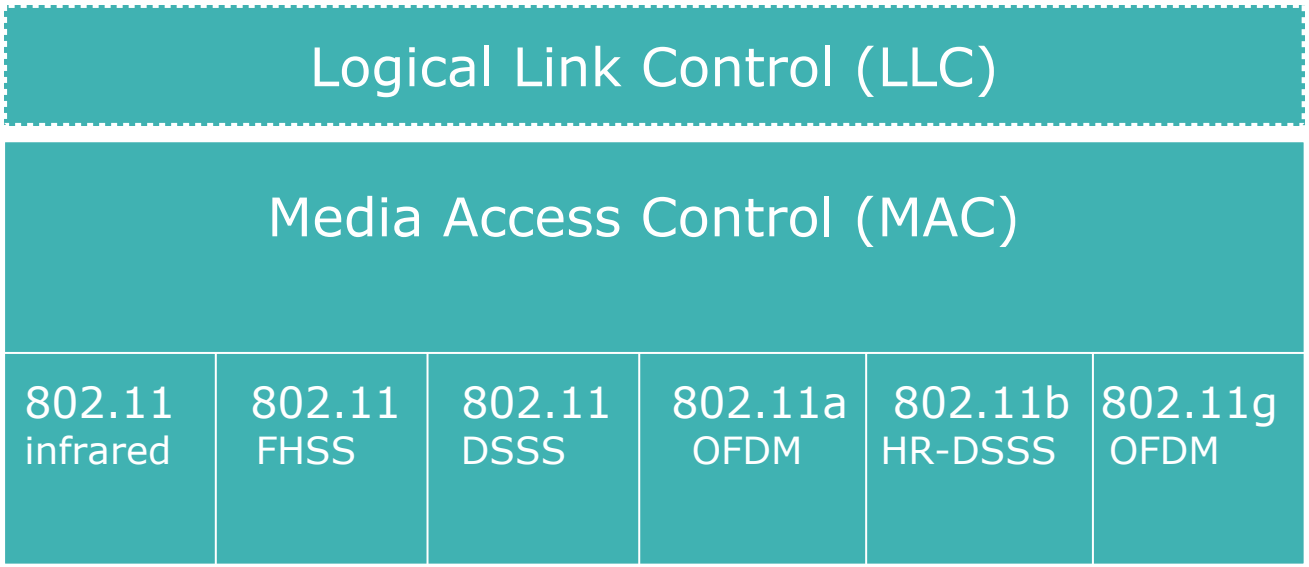
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Spektrális maszk, 802.11b



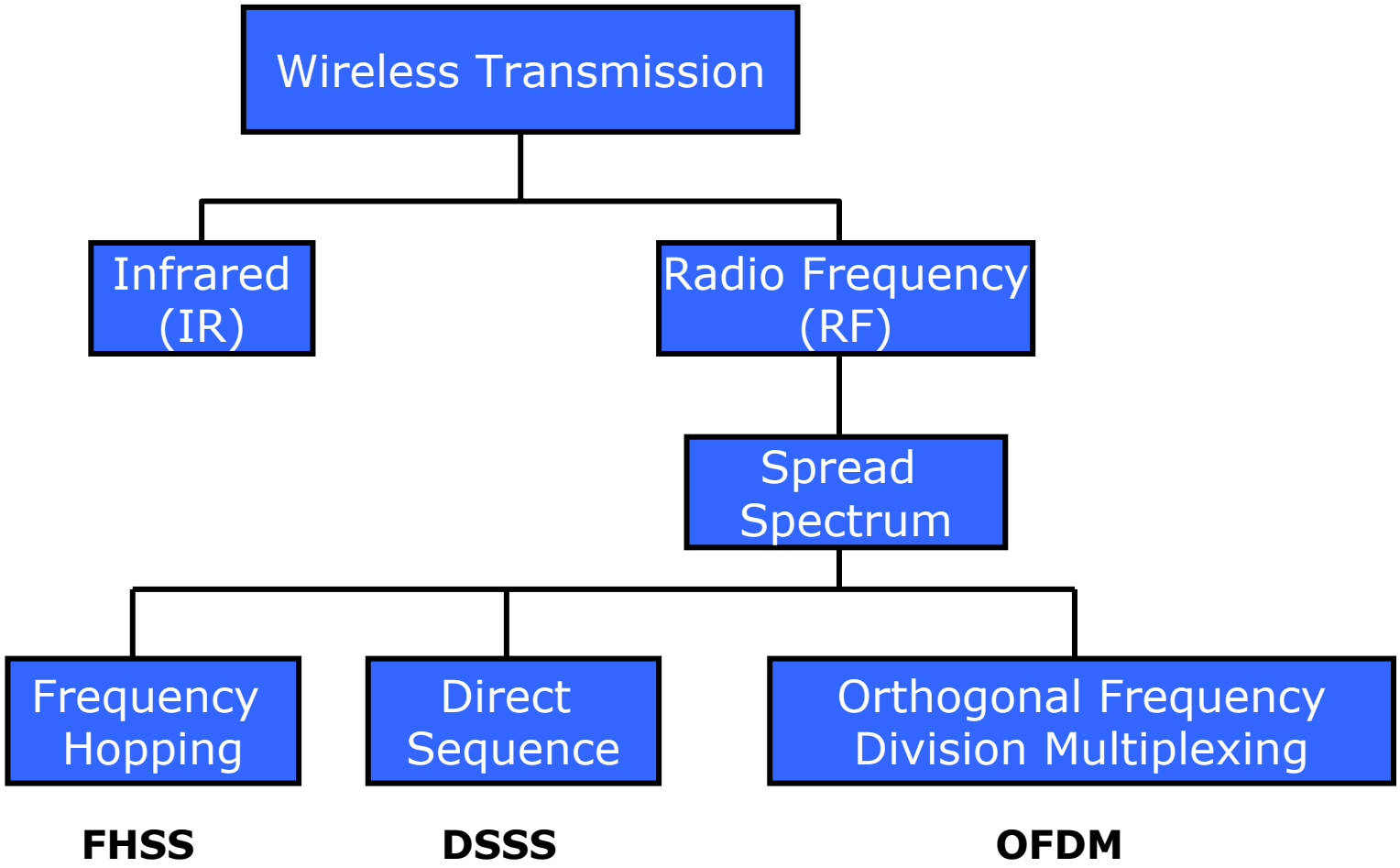
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

802.11 szabványok



Szabványváltozatok a különböző rétegeknek megfelelően

A vezetéknélküli kommunikáció fizikai formái

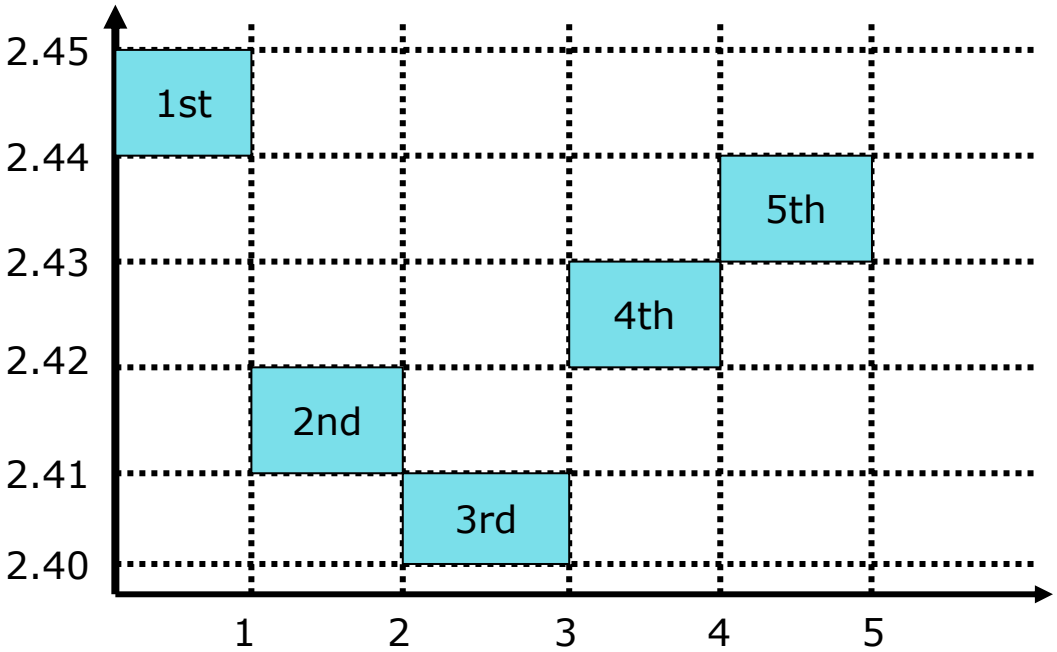


DSSS: detekció, zavarvédettség

- Detekció: korrelációs vevő, a kódolásnál alkalmazott álvéletlen jelsorozattal, szinkronban
  - A korrelációs detektor maximumot ad az adott chip-időn belül és alacsony értékeket más helyeken
  - A zajjal, zavarokkal nincs korreláció
  - Többutas terjedés esetén az interferáló jelekkel kicsi a korreláció
- A chip-frekvencia („processing gain”) megválasztása
  - Hosszú kód: jó zavarvédettség
  - Rövid kód: kisebb sávszélességigény
- IEEE 802.11 : 11 bites szórás
  - FCC: min. 10 az ISM sávban
  - 11-es érték nem túl nagy: mérsékelt zavarvédettség, de jó sávszélesség-gazdálkodás

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Frequency Hopping Spread Spectrum (FHSS) *



- Több frekvenciát használ
- Példa:
  - 10 MHz helyett 50 MHz-et használ
  - Az első bit (vagy bitek egy csoportja) 2,44 GHz-en, a második bit 2,41 GHz-en, míg a harmadik bit 2,30 GHz-en kerül kiküldésre

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

FHSS: fő paraméterek

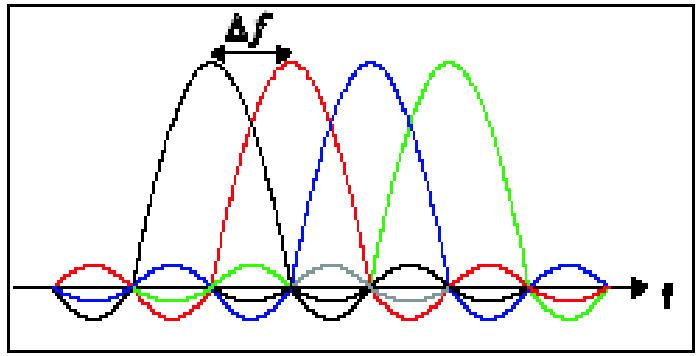
- Lassú és gyors frekvenciaugratás
  - Bitsebesség > vagy < a hopping-sebességnél

- A 2.4 GHz ISM sávban:
  - Min. 75 frekvencia használata
  - Max. 400 ms egy frekvencián, ha 400, akkor 2,5 ugrás/s;
  - FHSS ⇔ DSSS
    - Különböző sávszélesség igény és adatsebességek
    - FHSS védettebb a keskenysávú zavarokkal szemben
      - mivel az egész ISM sávra kiterjed, a DSSS csak egy részére

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

OFDM

Ortogonal Frequency Division Multiplexing

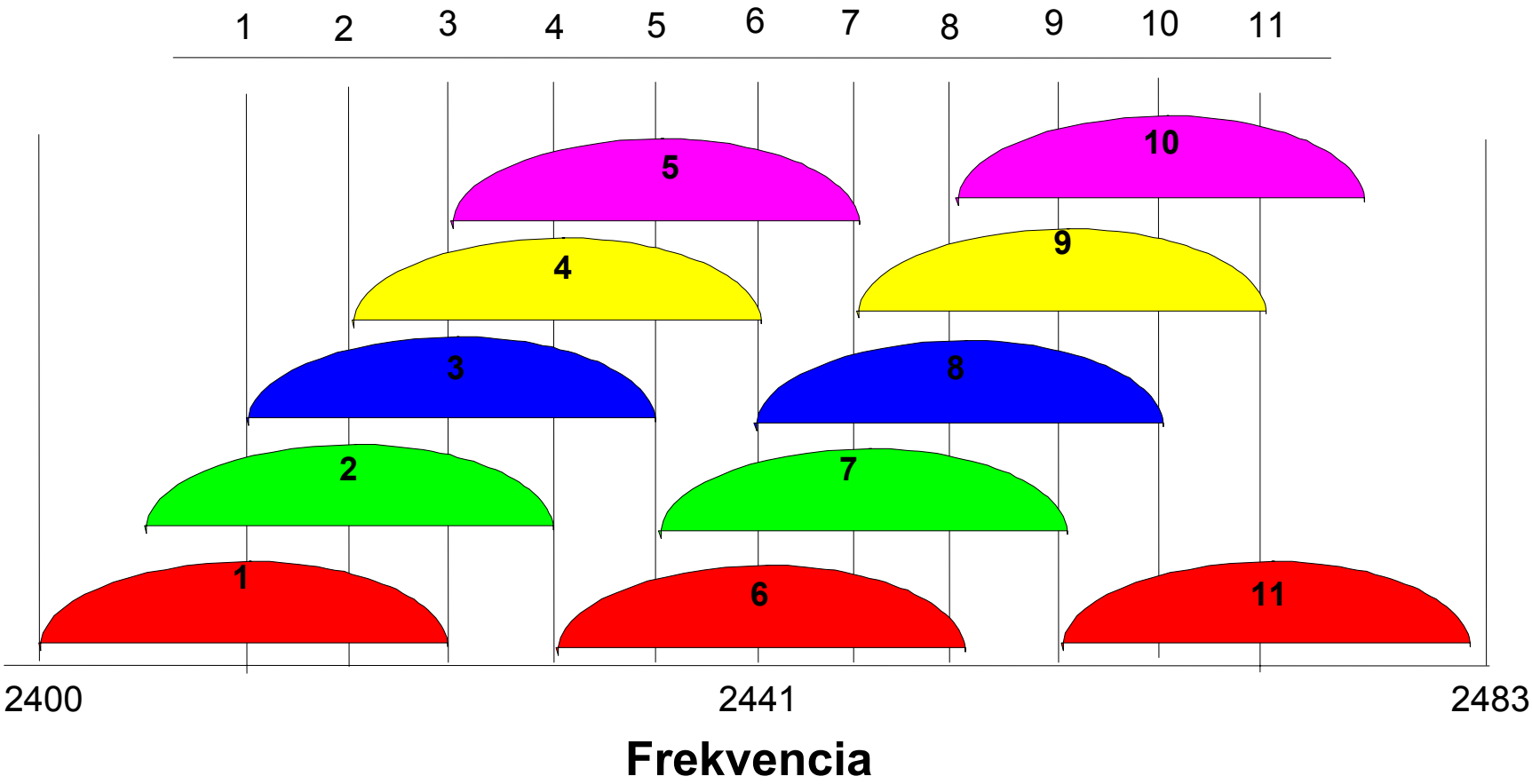


- A sáv felosztása sok részsávra
  - ezekben továbbítjuk a párhuzamosított jelfolyamot
  - részsávon belül QAM (16 v. 64) vagy PSK (B v. Q)

- A spektrum hatékony kihasználása: **„ortogonális” vivőkkel**
  - a sávok nem diszjunktak, a spektrumok „össze vannak tolva”, egymásba átlógnak
  - viszont szétválaszthatók, mert eleget tesznek a **Nyquist-elv**nek

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csatornakiosztás



OFDM előnyei-hátrányai

+:

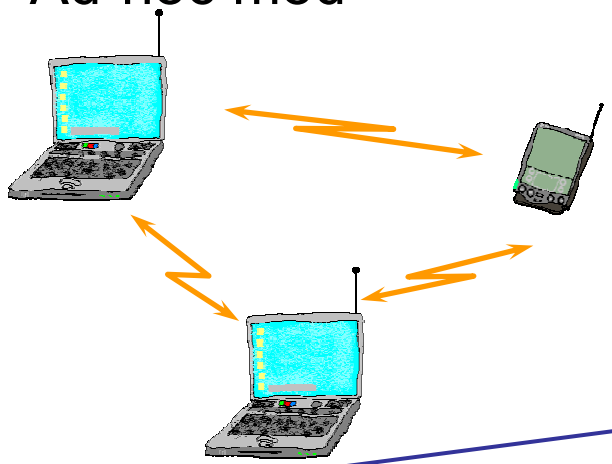
- Jó védettség a ISI, keskenysávú interferencia és frekvencia szelektív fading ellen
- Magas spektrális hatékonyság

-:

- Érzékeny a Doppler-effektusra és frekvencia szinkronizációra

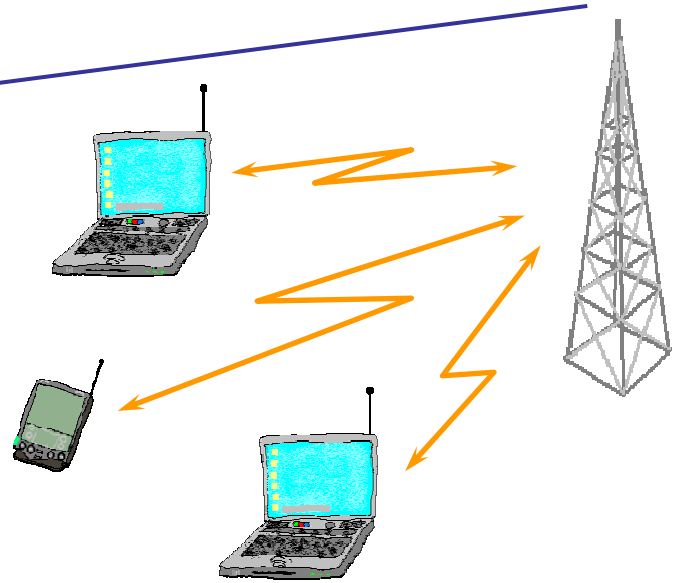
Működési módok

- Ad-hoc mód



- Részei: csak kliensek
- Kommunikáció: peer-to-peer
- Eseti hálózatok esetén

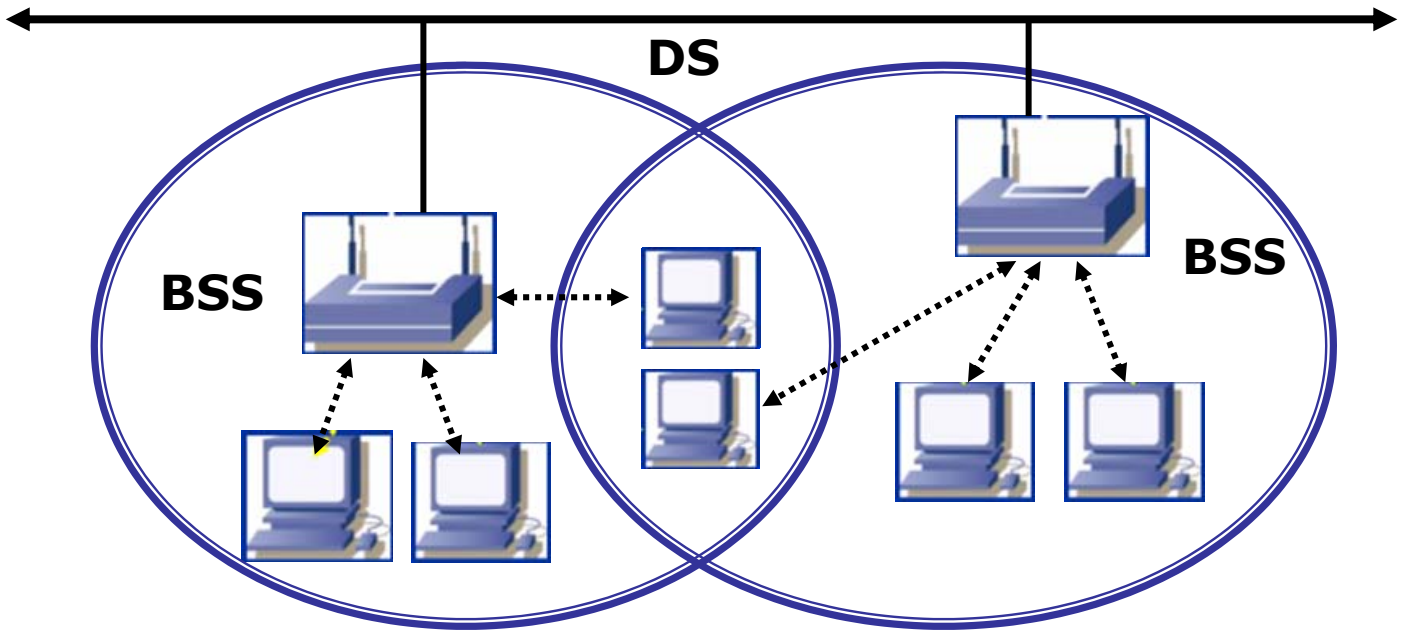
- Infrastruktúra mód



- Részei: Access Point (AP) + kliensek
- Kommunikáció: csak **AP-kliens**
- AP: kapcsolat a vezetékes és a vezetéknélküli hálózat között

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

WLAN-ok topológiája (BSS és ESS)



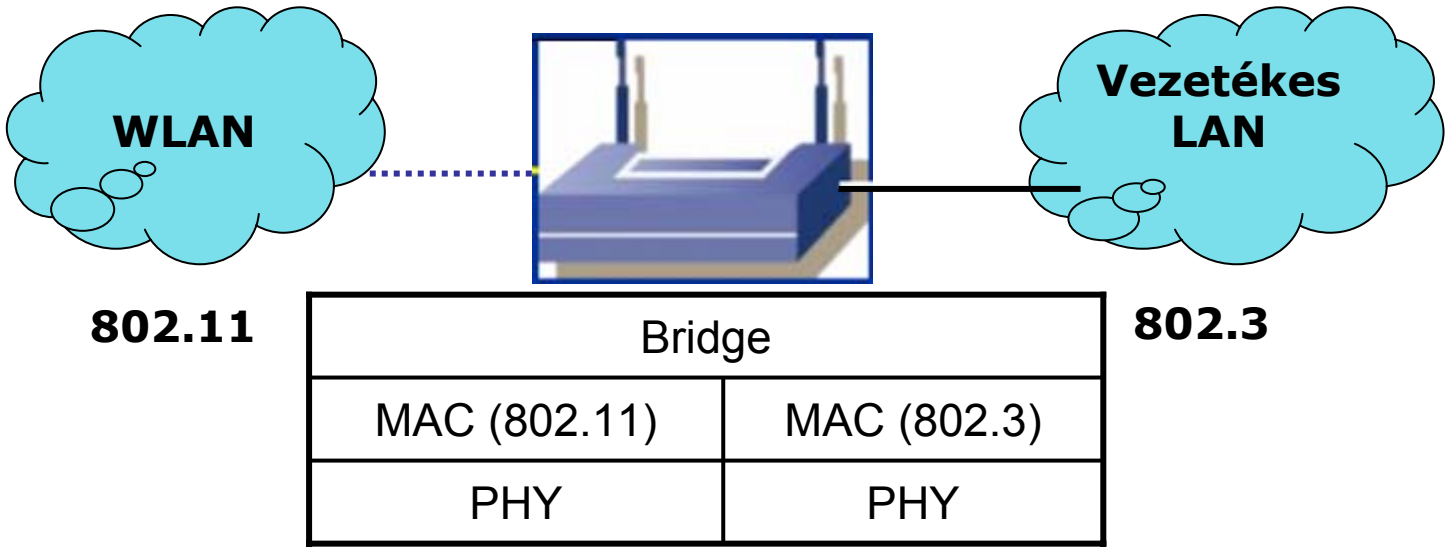
Basic Service Set (BSS) – egy cella

Extended Service Set (ESS) – több cella

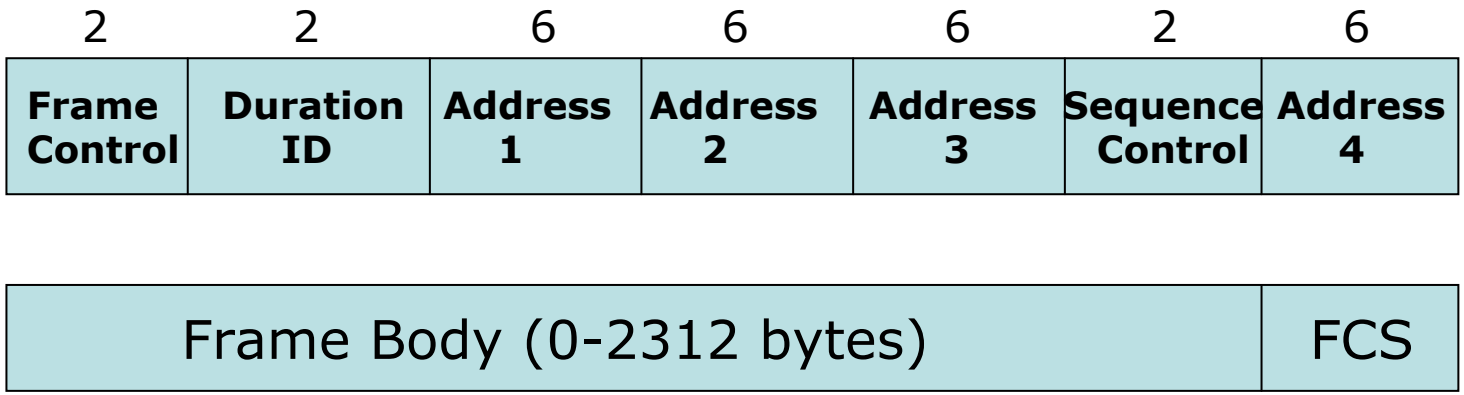
Distribution System (DS) – elosztóhálózat (gerinc)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Wireless Access Point (WAP) – Bridge



802.11 keretformátum



Vezérlési keretmező (Frame control)

- Protokoll verzió (2bit)
- Típus (2 bit): vezérlési, adat vagy menedzsment keret
- ToDS-FromDS (1-1 bit): elosztóhálózatba/ból
  - BSS-en belüli kommunikáció esetén 00
- További bitek:
  - fragmentáció
  - újraadott keret
  - teljesítményszabályozás stb.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

802.11 címek

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

DS: Distribution System
BSSID: Basic Service Set ID

DA: Destination Address (Célcím)
SA: Source Address (Forráscím)

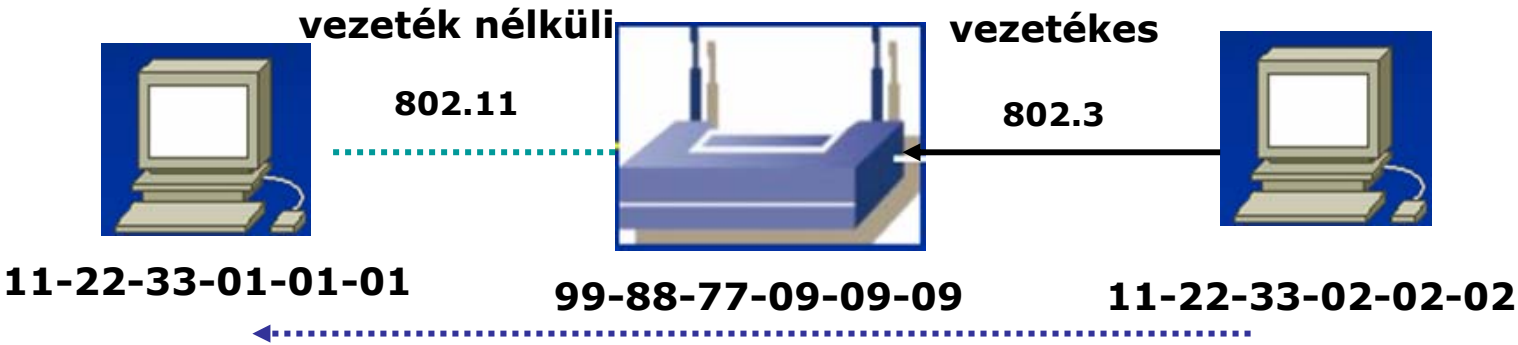
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„00”-eset

11-22-33-01-01-01 11-22-33-02-02-02

A1: 11-22-33-01-01-01	DA
A2: 11-22-33-02-02-02	SA
A3: BSS ID	
A4: nem használt	

„01”-eset (vezetékesből vezetéknélkülibe)

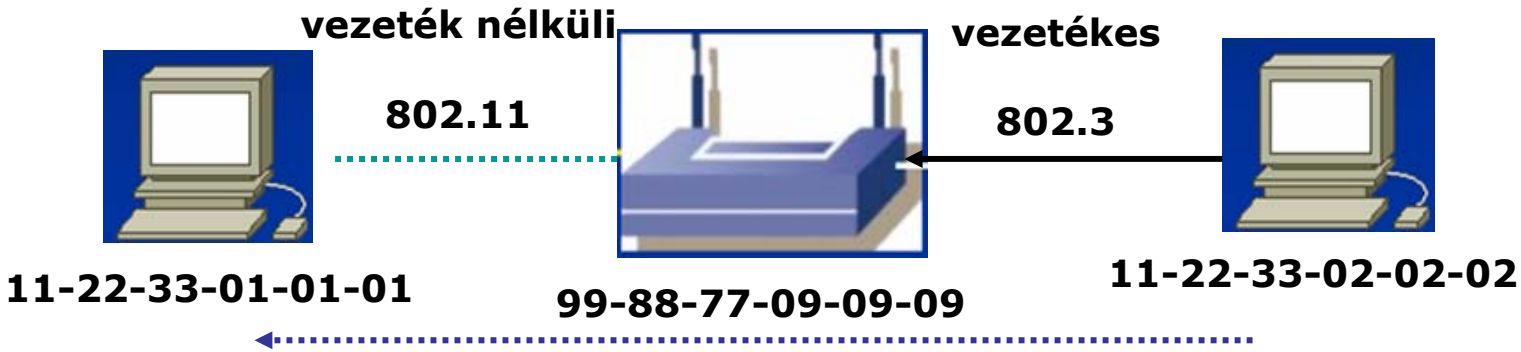


A1: 11-22-33-01-01-01
A2: 99-88-77-09-09-09
A3: 11-22-33-02-02-02
A4: nem használt

DA: 11-22-33-01-01-01
SA: 11-22-33-02-02-02

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„10”-eset (vezetéknélküliből vezetékesbe)



A1: 99-88-77-09-09-09
A2: 11-22-33-01-01-01
A3: 11-22-33-02-02-02
A4: nem használt

DA: 11-22-33-02-02-02
SA: 11-22-33-01-01-01

„11”-eset (vezeték nélküli összekapcsolás)

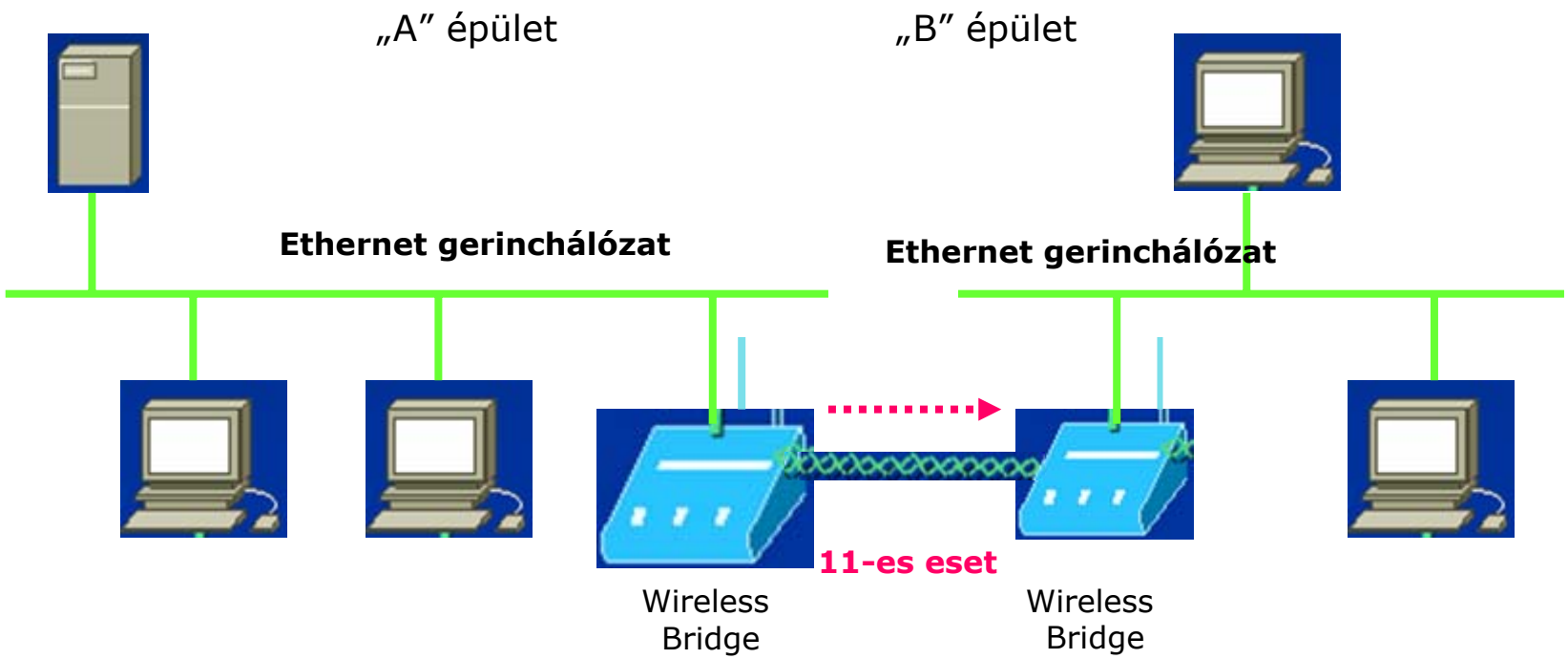
DA: 11-22-33-02-02-02
SA: 11-22-33-01-01-01

A1:99-88-77-08-08-08
A2:99-88-77-09-09-09
A3:11-22-33-02-02-02
A4:11-22-33-01-01-01

DA: 11-22-33-02-02-02
SA:11-22-33-01-01-01

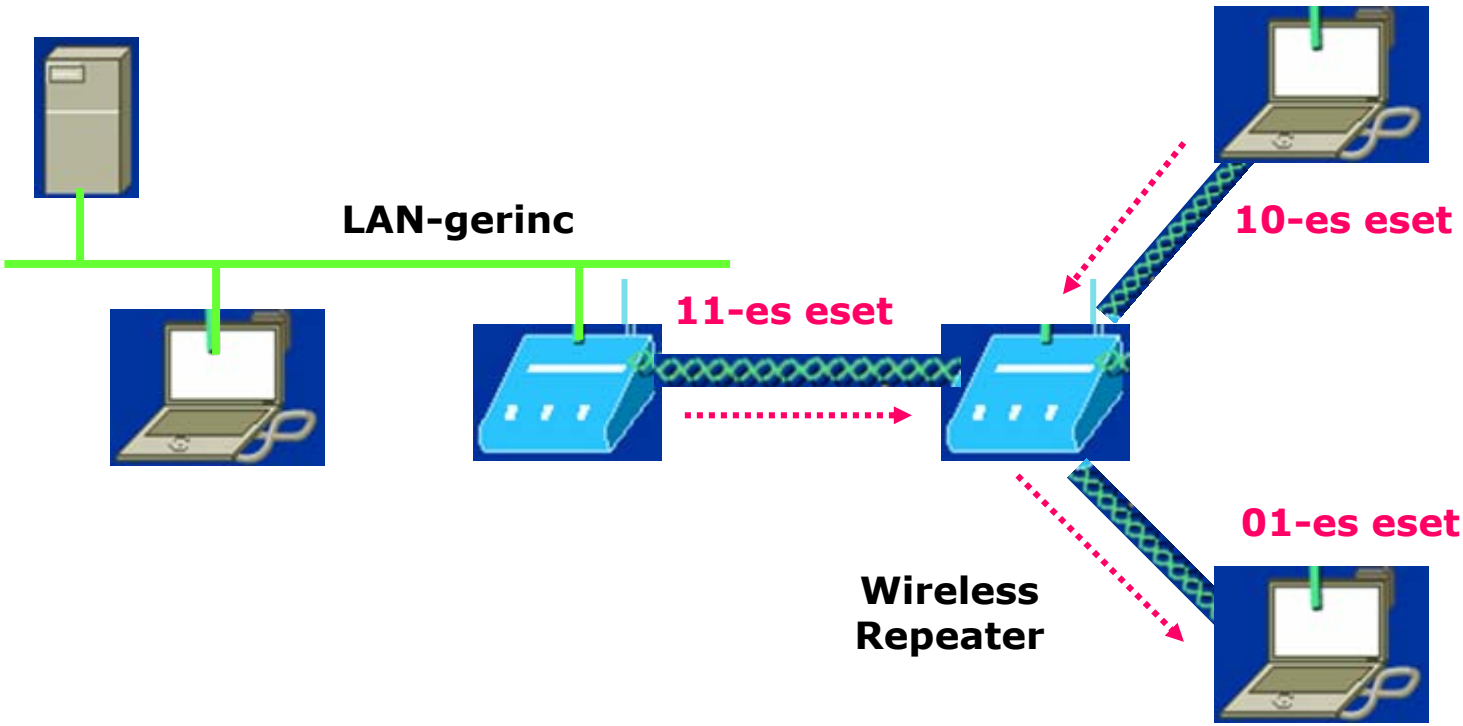
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Vezeték nélküli híd (bridge)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Vezeték nélküli ismétlő (repeater)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

802.11 MAC-réteg- Hozzáférési módszerek

- Carrier Sense Multiple Access/Collision Avoidance – CSMA/CA
  - Nem CSMA/CD (802.3), CS, de nem CD
  - Vezeték nélküli LAN-okban nem lehet ütközést detektálni
- Két hozzáférési módszer:
  - Distributed Coordination Function (DCF)
  - Point Coordination Function (PCF)

Distributed Coordination Function (DCF)

- A MAC alsó alrétege
- CSMA/CA
  - Collision Avoidance – Ütközés-elkerülés
- Nincs ütközésdetekció
  - az állomások nem képesek észlelni a máshonnan érkező jelek által létrehozott ütközést
- Különböző értékű IFS-ek (Inter Frame Space)
  - Short IFS (SIFS) – rövid IFS vezérlőüzenetek számára
  - PCF IFS (PIFS)
  - DCF IFS (DIFS) – adatkeretek számára

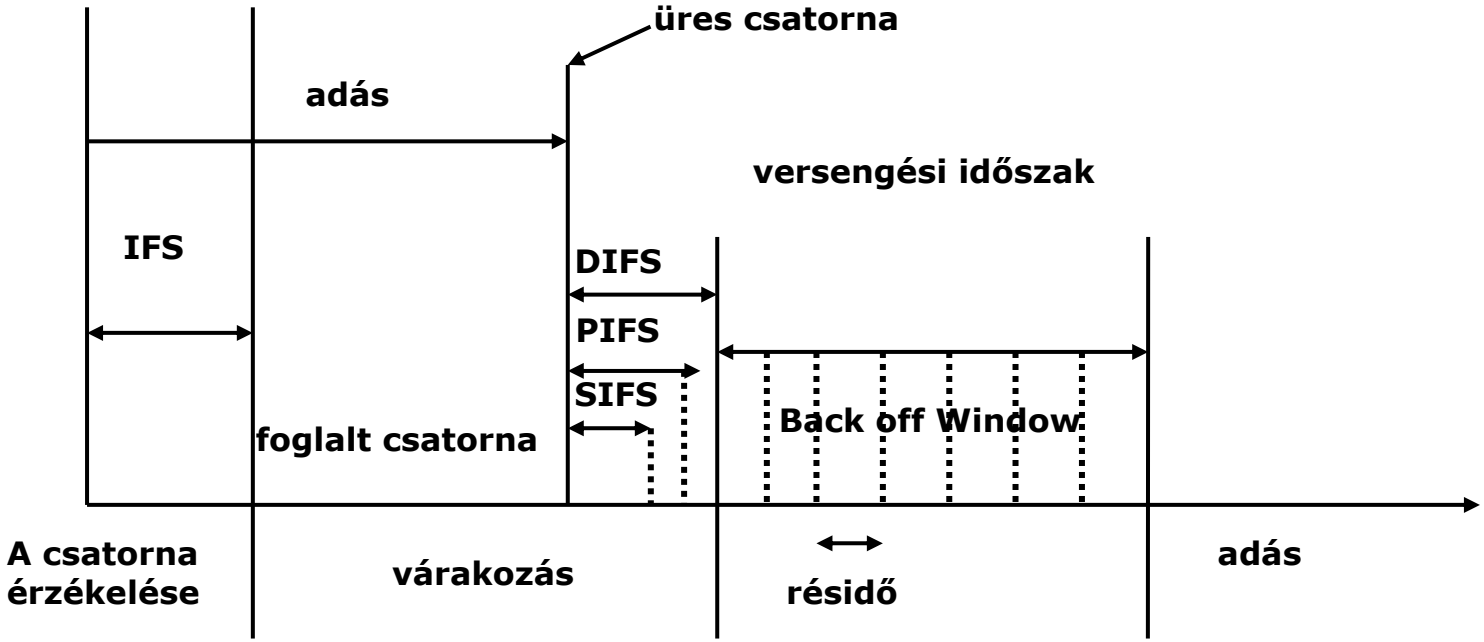
SIFS-PIFS-DIFS

- SIFS:
  - Magas prioritású adások esetén: ők férnek legelőbb a csatornához
  - Pl. SIFS után: ACK, CTS
  - Konstans értékű (10 v.16 μs)
  - Reduced IFS (RIFS): 802.11n szabványban, még rövidebb
- PIFS: PCF képes AP várakozási ideje
  - PIFS = SIFS + Résidő
- DIFS: adatkereteknek
  - DIFS = SIFS + (2 * Résidő)

DCF algoritmus

- Ha a csatorna szabad, az állomás vár, hogy szabad marad-e (D)IFS ideig. Ha igen, ad.
- Ha a csatorna foglalt (vagy már az elején, vagy azzá válik az IFS alatt), az állomás tovább figyeli.
- Amikor a csatorna szabaddá válik, az állomás vár (D)IFS ideig, majd egy véletlen késleltetést választ. Amikor az letelik, megkezdi az adását.
- Sikeres adás esetén ACK-ot vár a vevőtől.

CSMA/CA (DCF)



DIFS: DCF IFS

PIFS: PCF IFS

SIFS: Short IFS

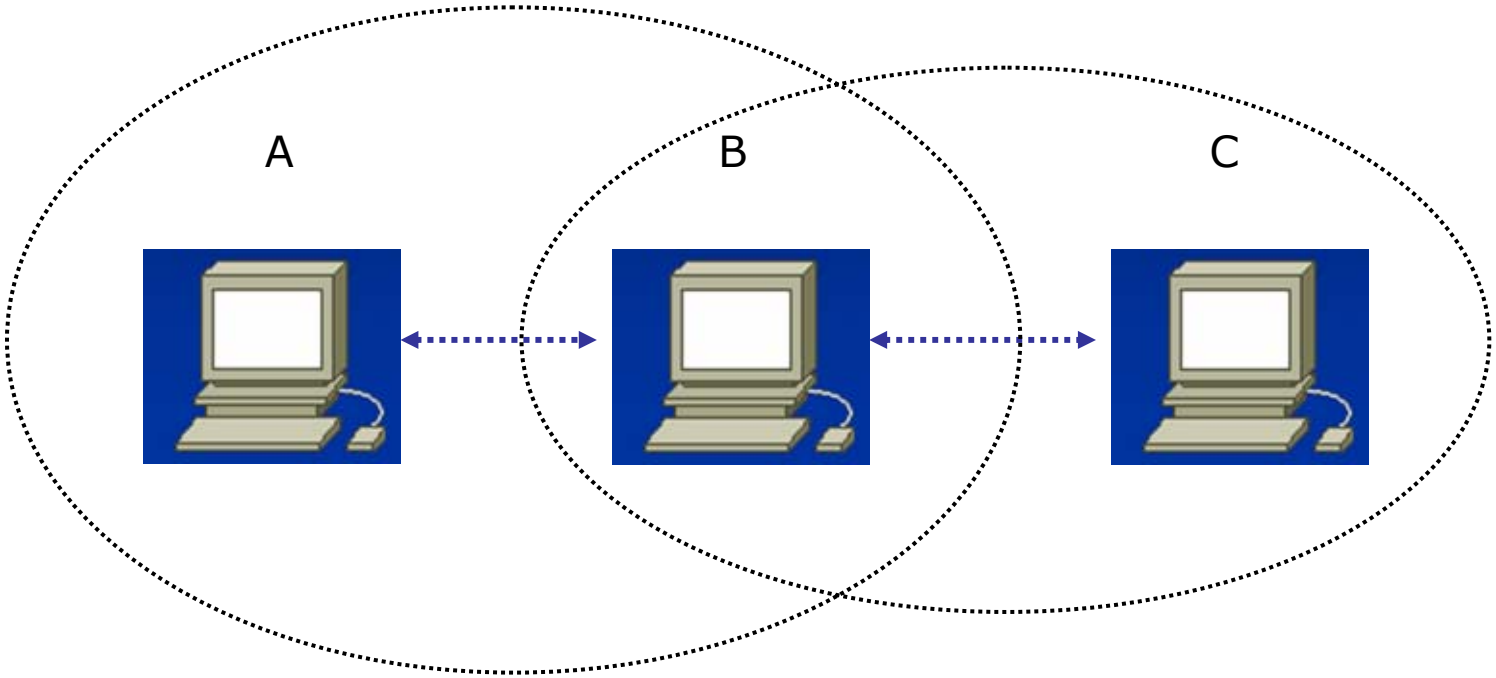
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az exponenciális backoff algoritmus

- Backoff_Time=INT(CW*RND())*Slot_Time
  - CW – Contention Window
    - Kezdetben 31, majd 63, 127 stb. A késleltetést itt résidőben (Slot_Time) mérjük
  - Résidő
    - Úgy kerül megválasztásra, hogy azalatt az állomás biztosan érzékelhesse a csatorna foglaltságát
      - 20 µs (DSSS), 50 µs (FHSS)
  - RND()
    - Véletlen számot generáló függvény 0 és 1 között

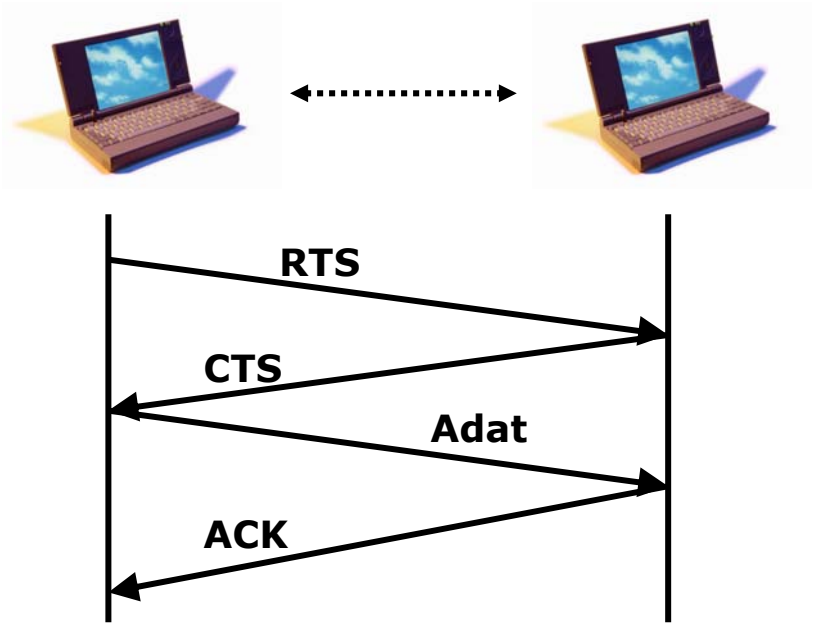
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A rejtett állomás problémája



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

Megoldás: RTS/CTS Handshaking

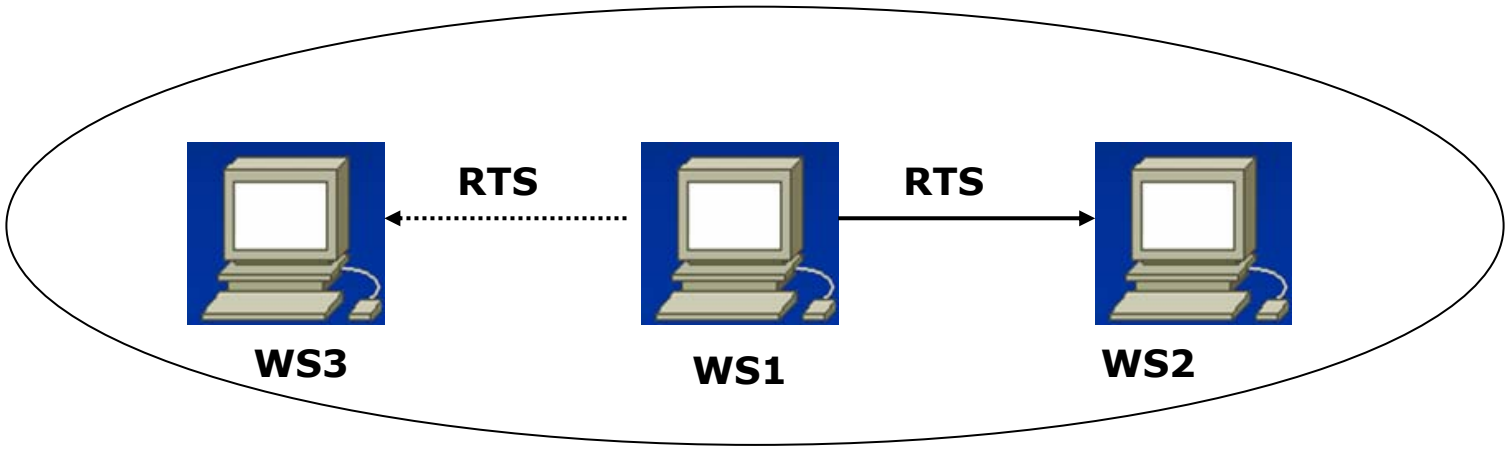


RTS – Request To Send
(küldés kérése)
CTS – Clear To Send
(szabad küldeni)
ACK – ACKnowledgement
(nyugta)

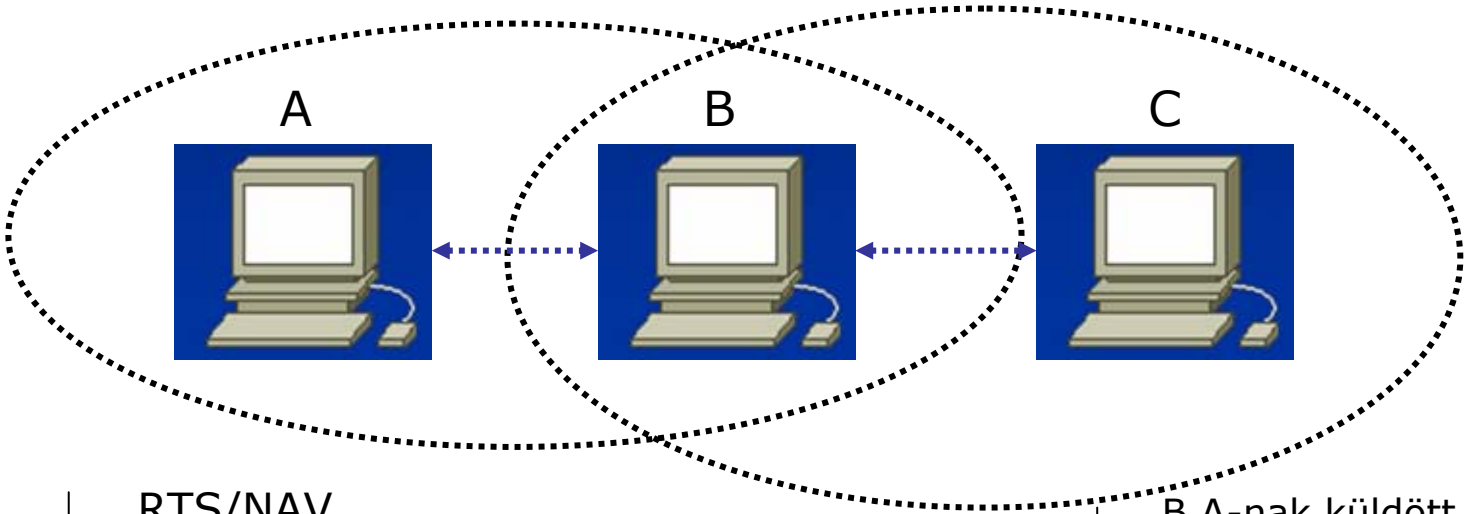
- A WLAN-oknál opcionális eljárás

Network Allocation Vector (NAV)

- Minden RTS keret tartalmazza azt az időt, ameddig az állomás el akarja foglalni a csatornát
- NAV: számláló a többi állomásnál, amelyeknek NAV ideig várniuk kell, mielőtt megnéznék, hogy a csatorna szabad-e
- Amikor az állomás (WS1) RTS-t (vagy CTS-t) küld, a többi (WS2 és WS3) elindítják a NAV-ot



RTS/CTS + NAV: Megoldás a rejtett állomás problémájára



RTS/NAV

RTS

B RTS-t kap A-tól és visszautasítja C RTS-ét

CTS

CTS/NAV

Data

B A-nak küldött CTS-ét C is megkapja.
C a CTS-ben lévő NAV értéknek megfelelő időzítőt indít el.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

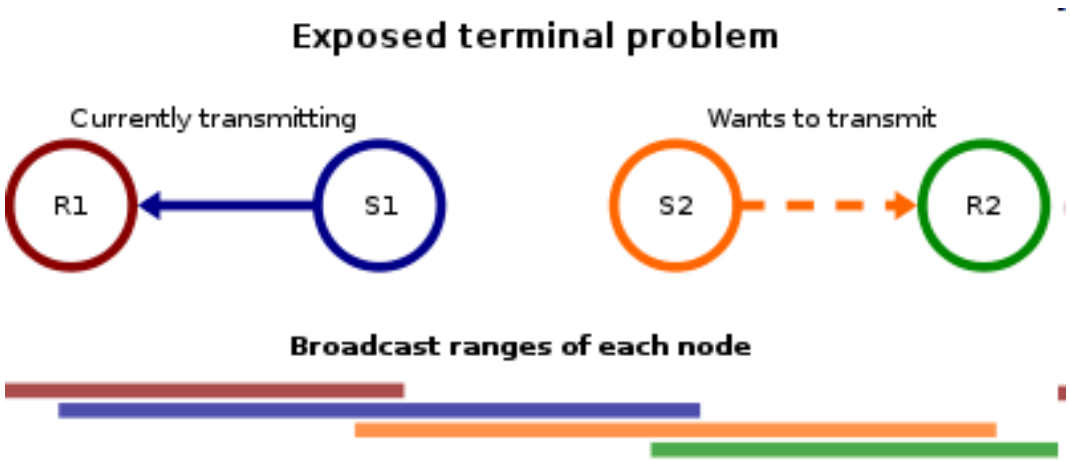
Foglalt közeg

- Fizikailag foglalt
  - Az állomás foglaltnak érzékeli a rádiócsatornát
- „Virtuálisan” foglalt
  - Az állomás RTS-t vagy CTS-t vesz, amely jelzi hogy a csatorna foglalt lesz a NAV időtartamán

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Exponált terminál probléma

- RTS/CTS csak akkor oldja meg, ha az állomások szinkronizáltak és egyezik a csomagméretük és adatrátájuk
- Ha hall a szomszédos állomástól RTS-t, de CTS-t nem: exponált terminál lehet, így adhat
- Gyakorlatban nem oldja meg



RTS/CTS értékelése

- WLAN-oknál opcionális eljárás

- Előnyös használni, ha
  - a rejtett állomás probléma fennállhat
  - nagy verseny van
    - sok nagy forgalmú állomás
    - a rövidebb keretek (RTS/CTS) ütköznek, nem a hosszabb adatkeretek

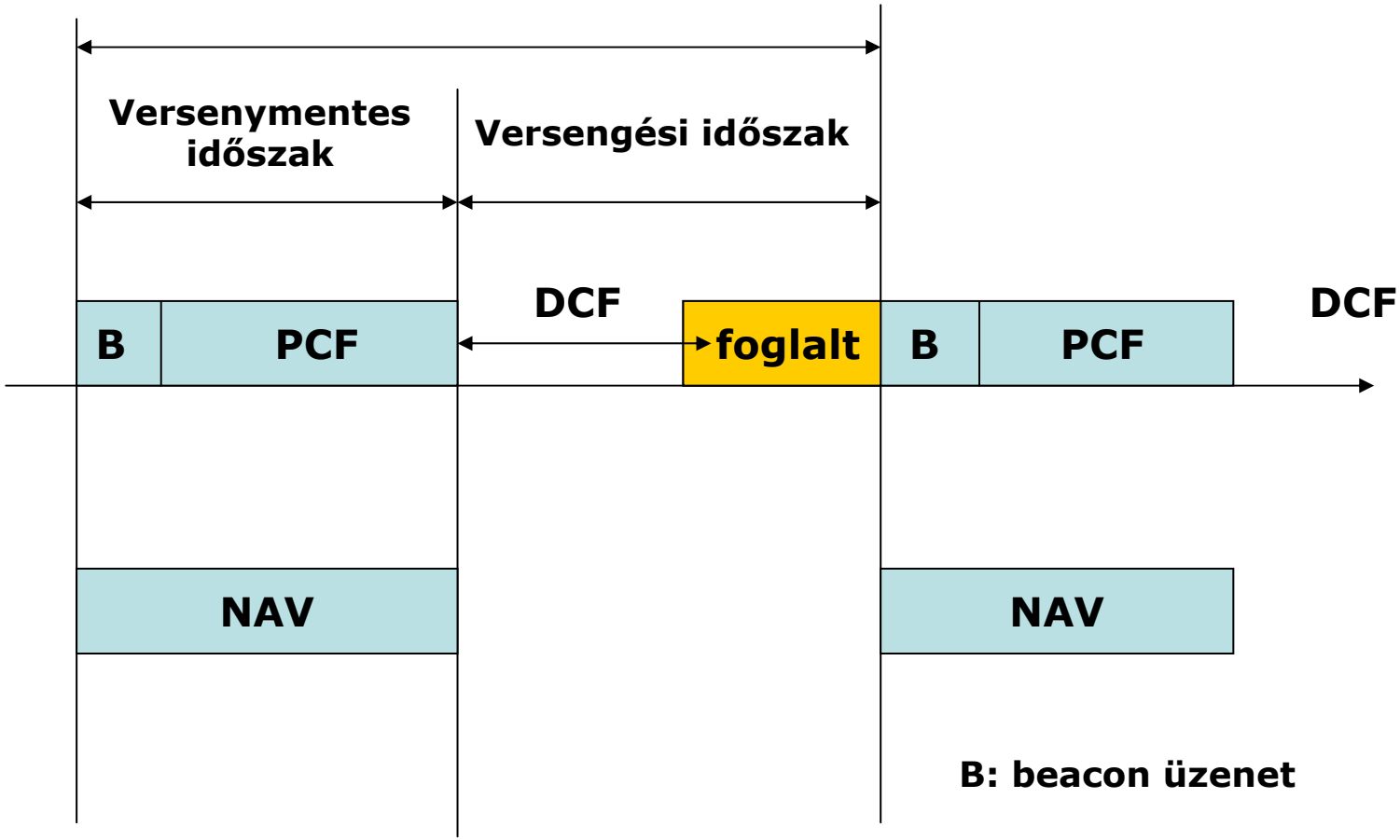
- Hátrány
  - Kisebb a felhasználható adatsebesség
    - RTS/CTS-re fordított idő kiesik
  - Jelentősen megnőhet a késleltetés

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Point Coordination Function (PCF)

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

A PCF időbeli működése



DCF vs. PCF

- DCF hátrányai:
  - Sok kommunikáló terminál esetén sok ütközés
  - Nincsenek proritások, nincs QoS
  - Ha egyszer megszerzi egy terminál a csatornát, sokáig tarthatja
- PCF:
  - Van QoS, de nem elterjedt

Szolgáltatásminőség biztosítása (QoS) a WLAN-okban: a 802.11e szabvány

- **HCF – Hybrid Coordination Function**

- Kétféle MAC-módszer, DCF-PCF analógia
- Forgalmi osztályok (Traffic Category): pl. e-mail alacsony, Voice over WLAN magas prioritású

  - **EDCA – Enhanced Distributed Channel Access**
    - Versenyzés: prioritásos kevesebb ideig vár
    - Van itt is versenymentes idő: hang és video számára

  - **HCCA – HCF Controlled Channel Access**
    - Mint PCF, de AP bármikor elrendelhet versenymentes periódust, egyébként EDCA verseny
    - Nem csak állomás, hanem **forgalomosztály ütemezés** is
    - Előre veszi a magasabb prioritású osztályt (**per-session service**)
    - Legbonyolultabb CF, állomásokon DCF felett is működhet, AP-n új ütemező kell, ritkán valósítják meg

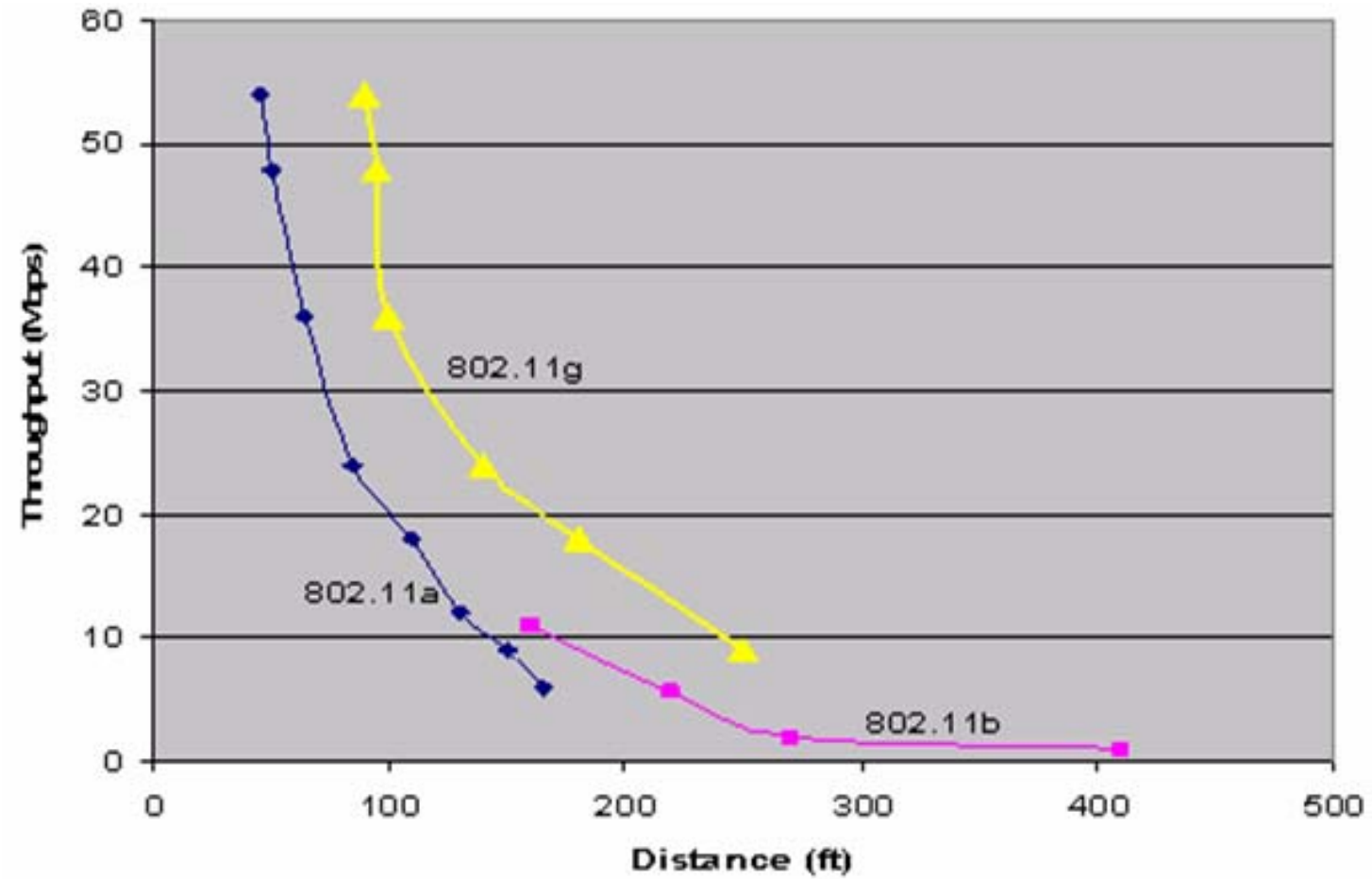
WLAN-ok teljesítőképessége

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

A teszt laboratóriumi körülmények között zajlott 10 m-nél kisebb távolságból.

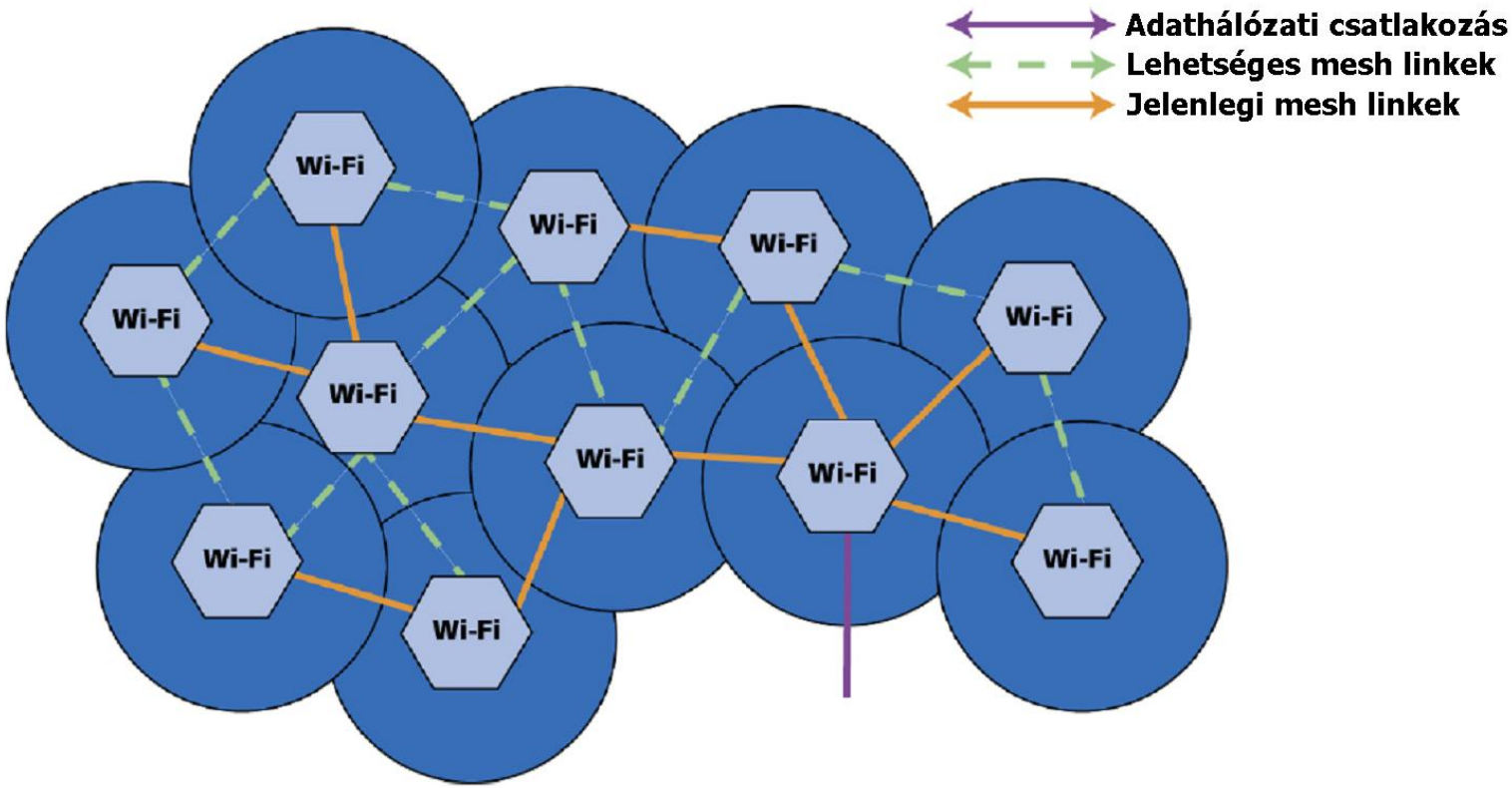
"WLAN Testing with IXIA IxChariot", IXIA White Paper

A WLAN teljesítőképessége (átvitel)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

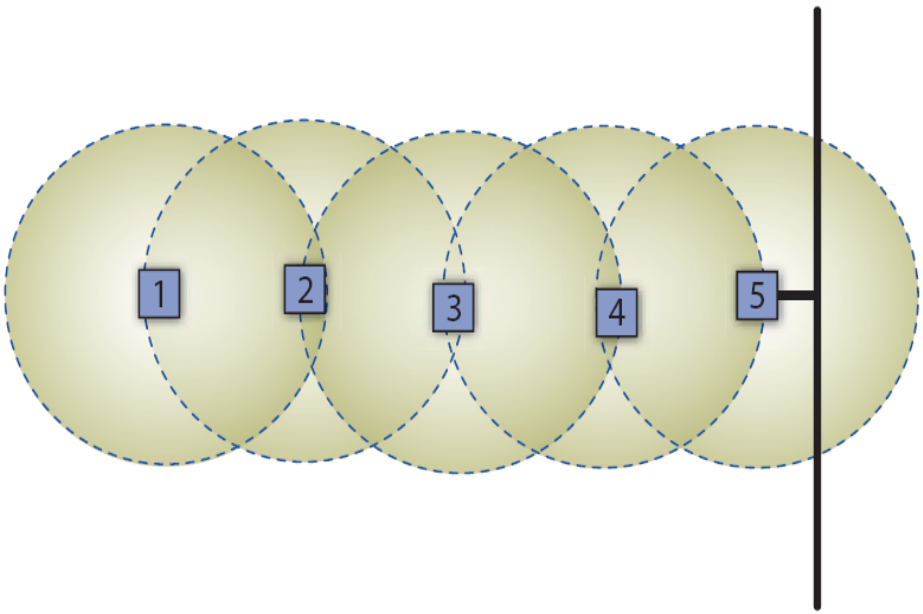
Mesh-hálózatok kialakítása WLAN- eszközökből: a 802.11s szabvány

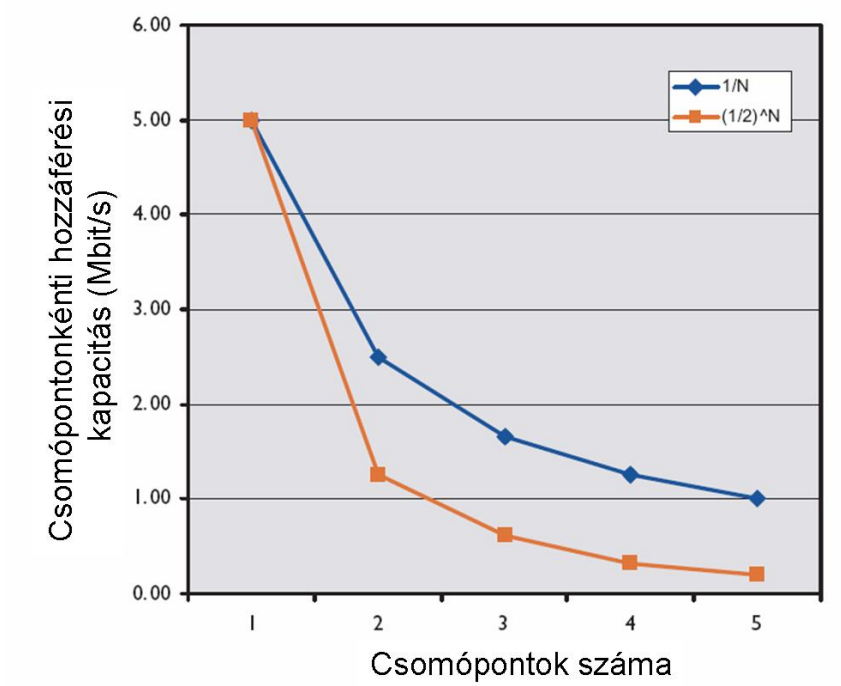


Az ad-hoc mód továbbfejlesztésének tekinthető.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Láncba kapcsolt mesh csomópontok: a hozzáférési kapacitás csökkenése





Megoldás: duális ill. többszörös rádiók

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Igen nagy sebességű WLAN: a 802.11n szabvány

- Elméletileg akár 600 Mbit/s
  - 4 adatfolyam, 64QAM, 40Mhz csatorna esetén
- MIMO technikával
  - Több adó és több vevő antenna
  - 2X2:2, 3X3:2, 4X4:4 (adó/vevőantenna/adatfolyam száma)
- Keret aggregáció (overhead csökkenés)
- Zajosabb csatornán illetve nem közvetlen rálátás (NLOS) esetén jobb vétel

Az eddigi szabványok és az ‘n’

	802.11a	802.11b	802.11g	802.11n
Standard approved by IEEE	January 2000	December 1999	June 2003	Expected in 2007
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Different data rate configurations	8	4	12	576
Typical range	75 feet	100 feet	150 feet	150 feet
Modulation technologies (1)	OFDM	DSSS, CCK	DSSS, CCK, OFDM	DSSS, CCK, OFDM+
RF band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz and 5 GHz
Number of spatial streams and antennas	1	1	1	Up to 4
Channel width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz
Number of channels	23	3	3	26

802.11 b, g, n együttélése

- Az ‘n’ szabványra az 5MHz-es sáv a javasolt (de nem írja elő kizárólagosan a szabvány)
- ‘n’ hálózatnak együtt kell élnie a ‘b/g’ meglévő hálózatokkal
- Praktikus megoldás: duál rádiós AP
  - 5MHz: ‘n’
  - 2,4MHz: ‘b/g’

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

WLAN biztonság

- Evolúció
  - WEP (Wired Equivalent Privacy): kezdeti könnyen feltörhető titkosítás
  - WEP2, WPA (Wi-Fi Protected Access) : WEP továbbfejlesztései, kicsit erősebbek annál, de nem kell a WEP-hez képest hardverváltoztatás
  - WPA2: erős titkosítás és hitelesítés új hardveren, 802.11i definiálja
- Jótanácsok
  - Használaton kívüli WLAN-eszközök kikapcsolása
  - SSID közzététel tiltása
  - MAC-cím alapú szűrés
  - WEP, WEP2, WPA, WPA2 engedélyezése
    - lehetőleg egyéni (nem PSK) kulccsal

Összefoglalás a lokális hálózatokról

- I. Az „Ethernet”
  - IEEE 802.3 Ethernet (a „klasszikus” E.)
  - IEEE 802.3u Fast Ethernet
  - IEEE 802.3z Gbit/s Ethernet
  - IEEE 802.3ae 10 Gbit/s Ethernet
- II. Két további IEEE 802-es szabványú LAN és egy ANSI-szabványú, amely átmenet volt a MAN felé
  - „Token bus” – 802.4
  - „Token ring” – 802.5
  - FDDI (ANSI)
- III. LAN-ok összekapcsolása

- Vezeték nélküli LAN-ok
  - az IEEE 802.11-es család

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

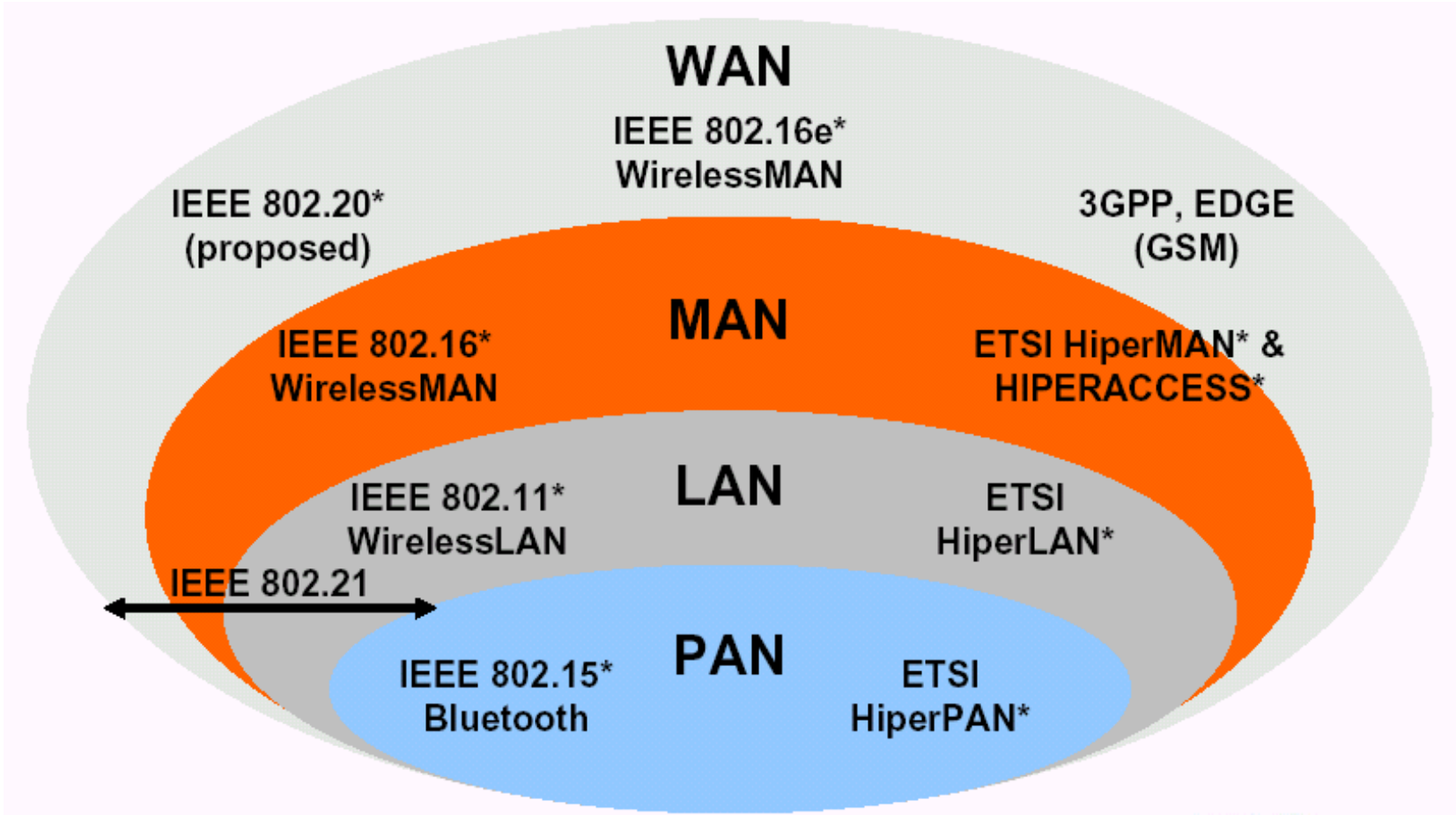
BWA- Broadband Wireless Access- szélessávú vezetéknélküli hozzáférés

WLAN – Wireless LAN
WPAN – Wireless PAN
WMAN – Wireless MAN

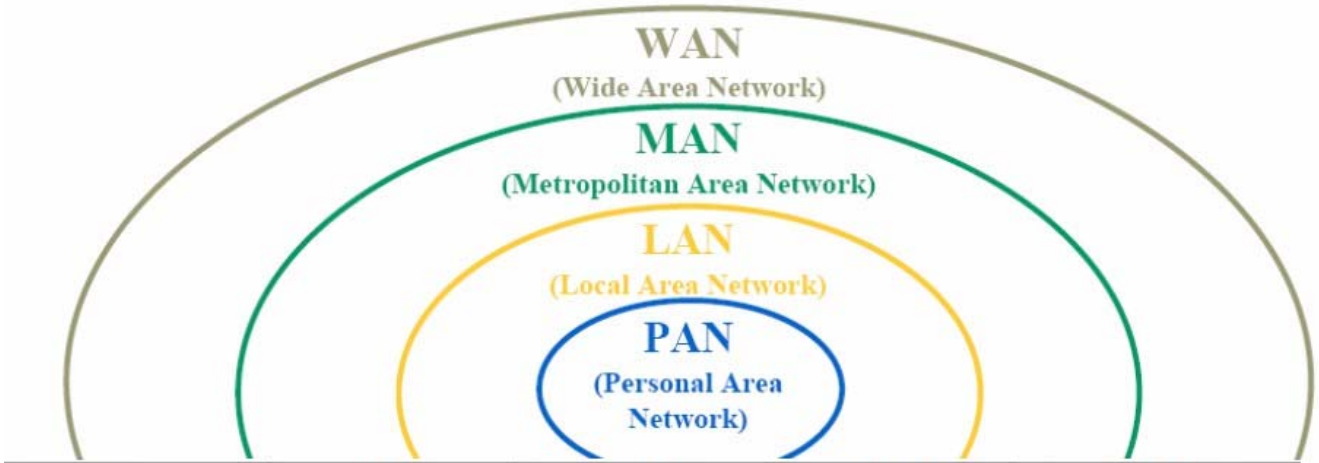
Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.március 19.

Vezeték nélküli hálózatok osztályozása kiterjedésük szerint

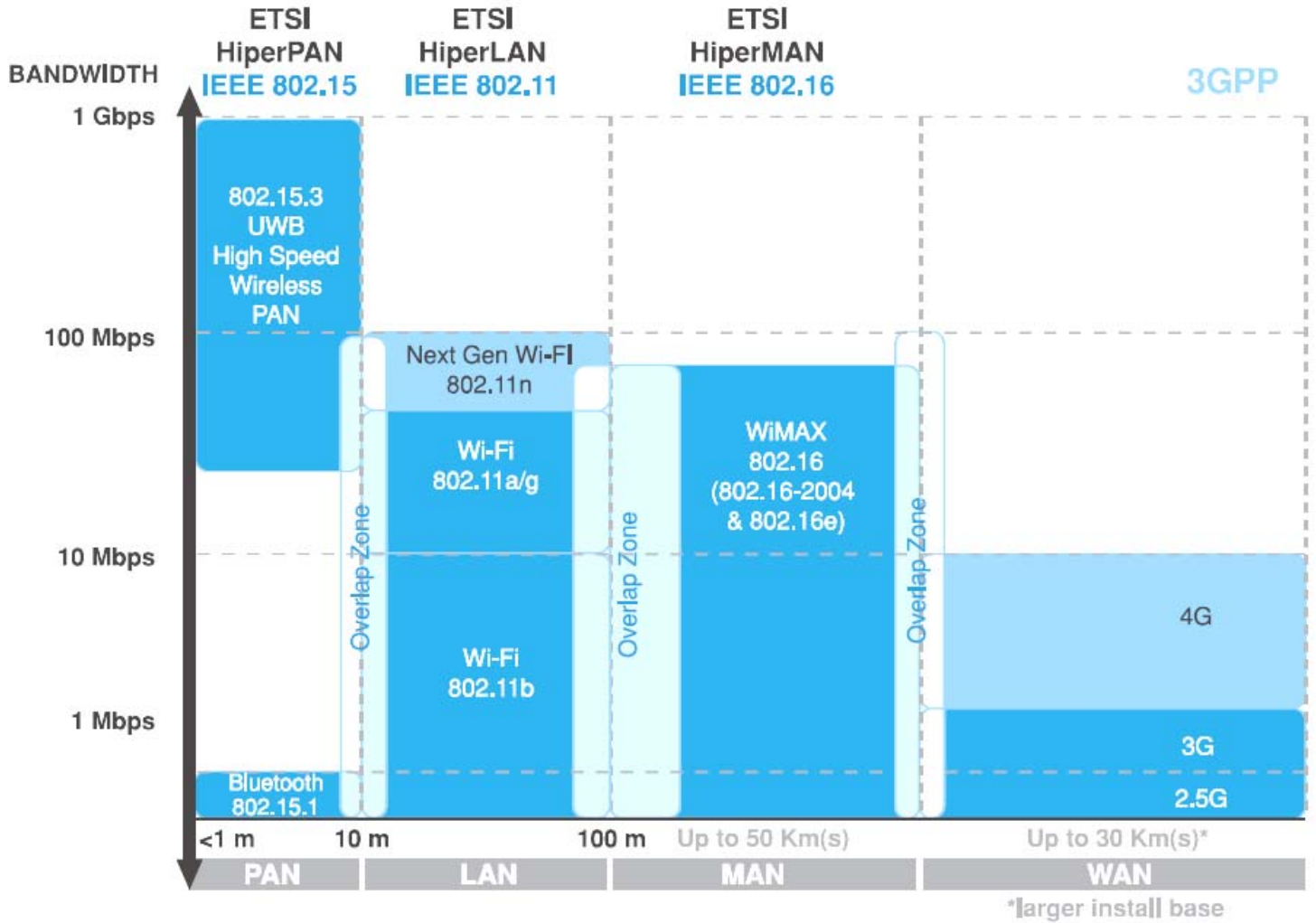


PAN, LAN, MAN, WAN



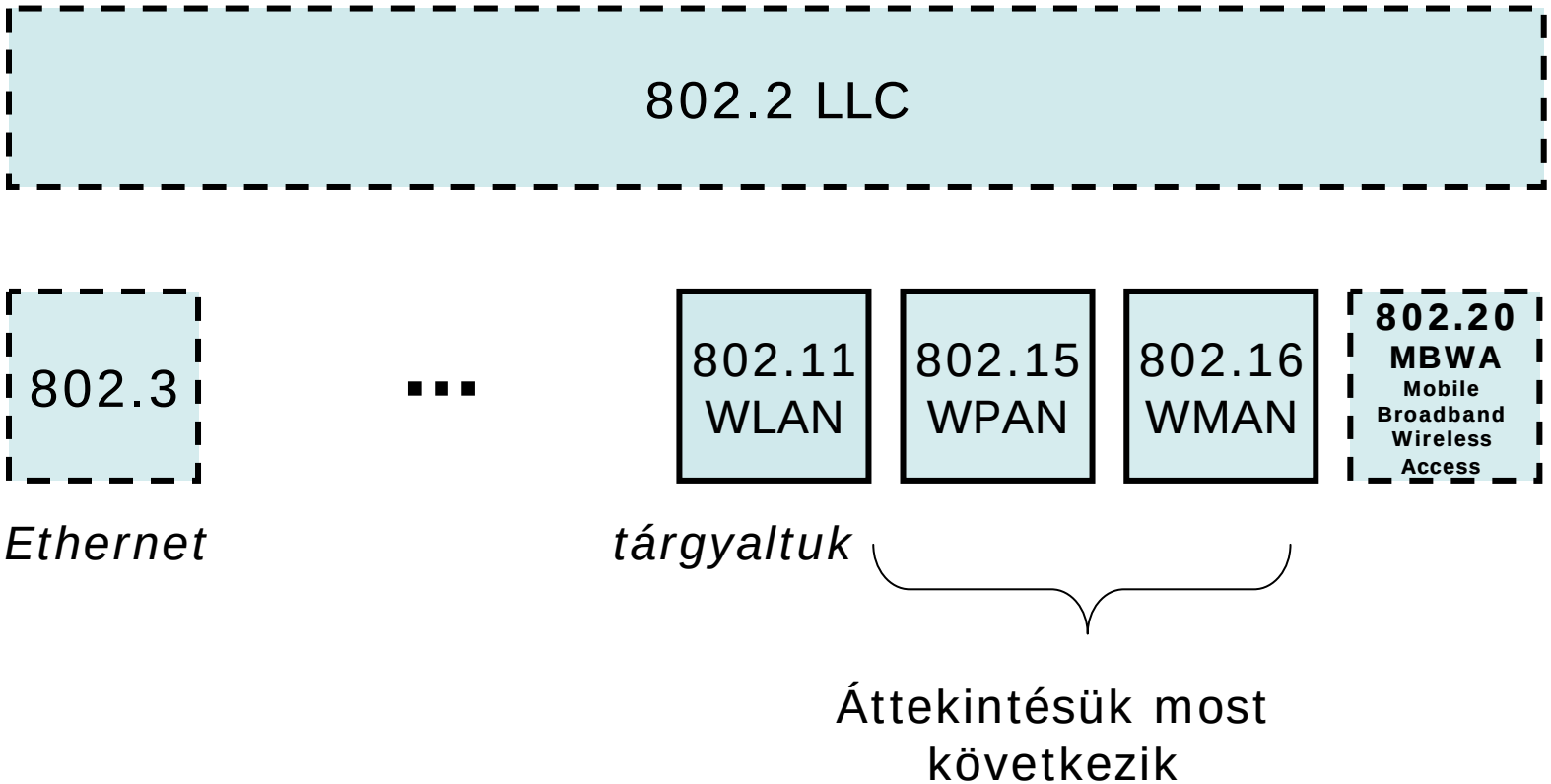
	PAN	LAN	MAN	WAN
Szabványok	Bluetooth	802.11a,b,g Hiperlan2	802.16, MMDS, LMDS	GSM, GPRS, UMTS
Sebesség	< 1 Mbps	2 – 54+ MBPS	22+ Mbps	10-384 kps
Távolság	Rövid	Közepes	Közepes-hosszú	Hosszú
Alkalmazások	Peer-to-peer és eszközök közötti	Magán és vállalati hálózatok	Gyors, „last mile” elérés	PDA, mobiltelefonok, cellás elérés

Szélessávú vezetéknélküli hozzáférési technikák összehasonlítása



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IEEE.802.xx BWA-k architektúrája



MŰEGYETEM 1782

BME

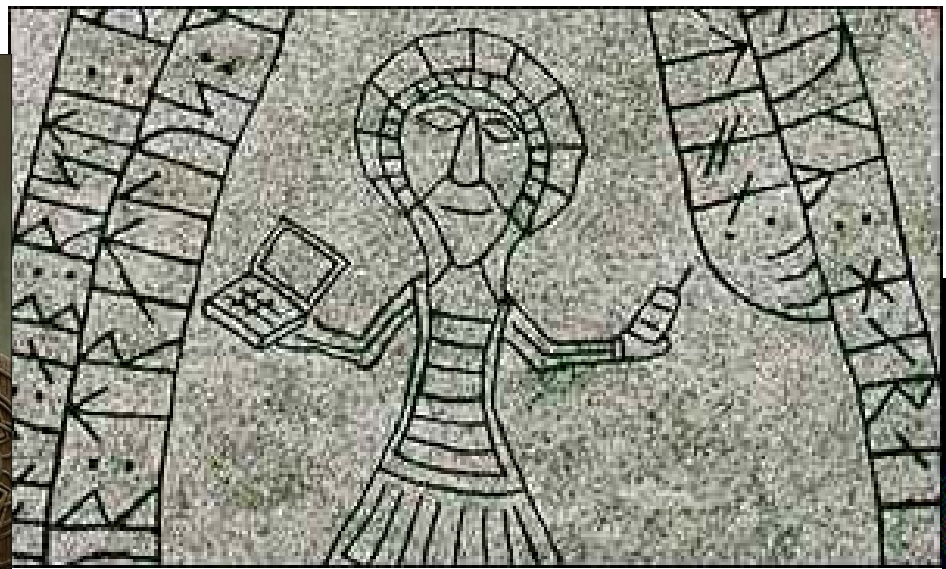
Bluetooth – IEEE 802.15.1

Bluetooth™

2013.március 19.

Bluetooth névadás

- **Kékfogú (‘bla-tand’) Harald**
  (Harald Blatand Gormsen) (940 - 981)
  középkori viking király
  (hasonló mint nálunk Szent István)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

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

- Alapja a Bluetooth specifikáció
  - Bluetooth: az Ericsson kezdeményezése 1998-1999-ben, majd csatlakozott az IBM, Toshiba, Nokia, Intel,...
  - Bluetooth SIG (Special Interest Group)
    - Ma 18 ezer cég a tagja!
- Célkitűzések:
  - olcsó eszközök (1-2 cm-es modul, pár $)
  - rövidtávú kommunikáció (10 m)
  - max. 1 Mbit/s

Bluetooth-alkalmazások

- Bluetooth a mobilban: telefonhívások „least-cost routing”-gal
  - telefonhívás házon belül a mobilról, de Bluetooth-kapcsolat segítségével a vezetékes telefonról
- Internet-elérés mobilról és PDA-ról
  - Bluetooth-csatlakozás a notebookhoz, vagy desktop-hoz, ami LAN-ra vagy WLAN-ra csatlakozik, vagy ADSL-lel a nyilvános hálózaton keresztül
- Vezetéknélküli csatlakozások széles köre
  - fejhallgató
  - mobil kihangosító az autóban
  - fényképezőgép és notebook
  - PDA és notebook szinkronizálása
- Iparban: gyógyászati műszerek, bar kód olvasók, vezérlésben: infravörös kapcsolat kiváltása, lokalizációs rendszerek (RTLS), szenzorhálózatok

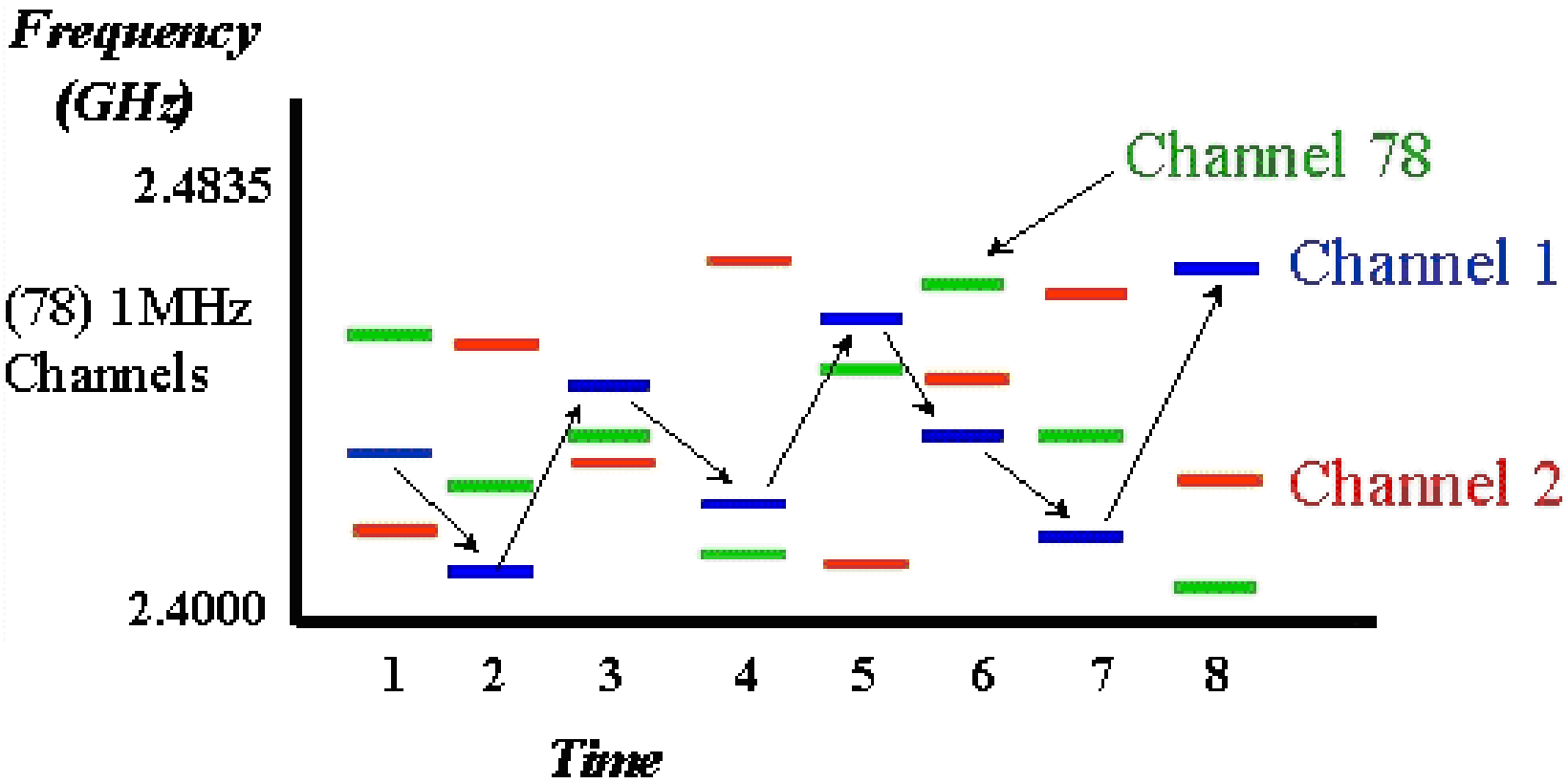
A rádiós interfész jellemzői

- Teljesítmény és távolság

Megnevezés	Teljesítmény [mW]	Teljesítmény [dBm]	Távolság [m]
Class 1	100	20	100
Class 2	2,5	4	10
Class 3	1	0	1

- **A 2,4 GHz-es ISM-sávban**
- **Frekvencia-ugratás**
  - 1600-szor mp-nként
  - álvéletlen jelsorozattal a kb. 2,4 GHz-nél kezdődő 79 MHz-es sávon belül: 79 x 1 MHz
- **TDD**, 625 µs-os időrések, adás-vétel időben egymás után
  - master-slave, felváltva
  - Master órája alapján: páros időrésben master, páratlanban slave ad

Frekvenciaugratás a Bluetoothban

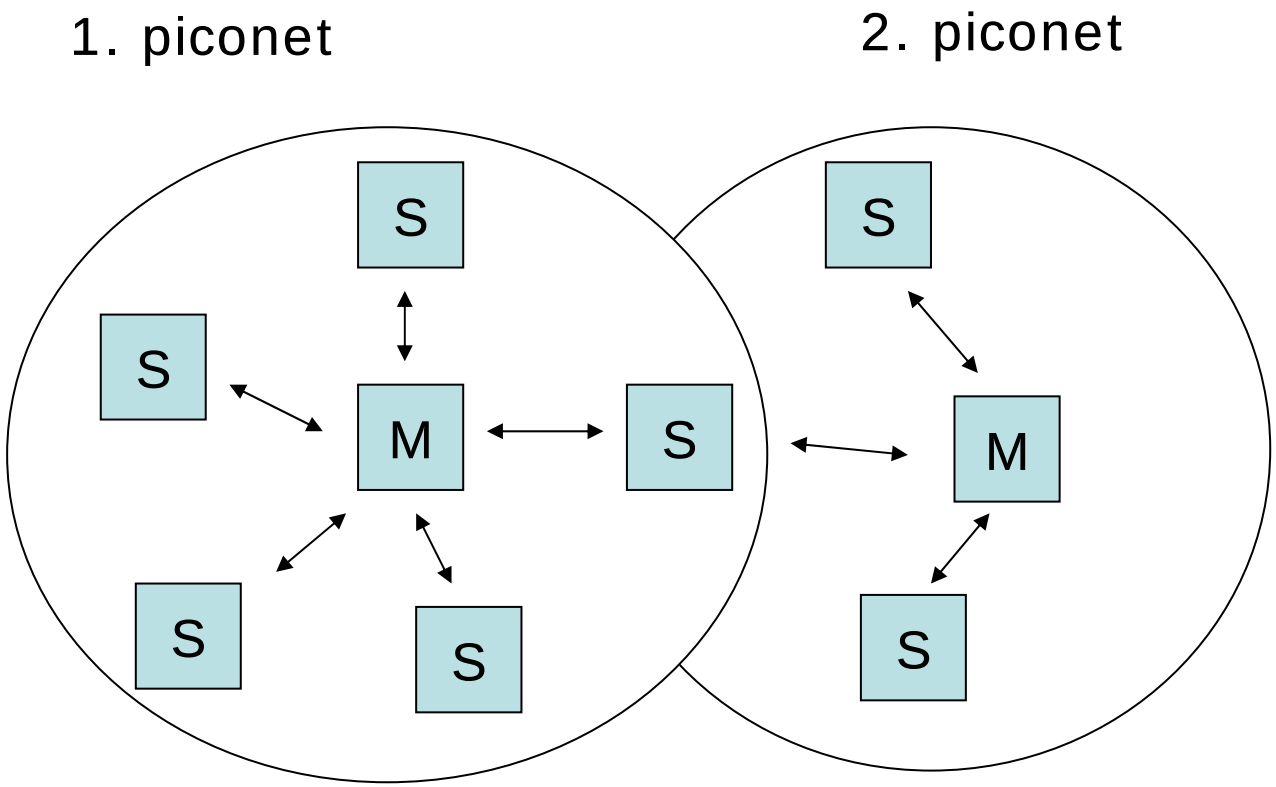


© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Használt modulációk

- Alapráta (Base Data Rate):
  - GFSK (Gaussi FSK): 1Mbit/s
- Megnövelt adatráta (Enhanced Data Rate)
  - Bluetooth 2.0
    - π/4-DQPSK: 2Mbit/s
    - 8DPSK: 3Mbit/s
- A kettő kombinációja BR/EDR radio

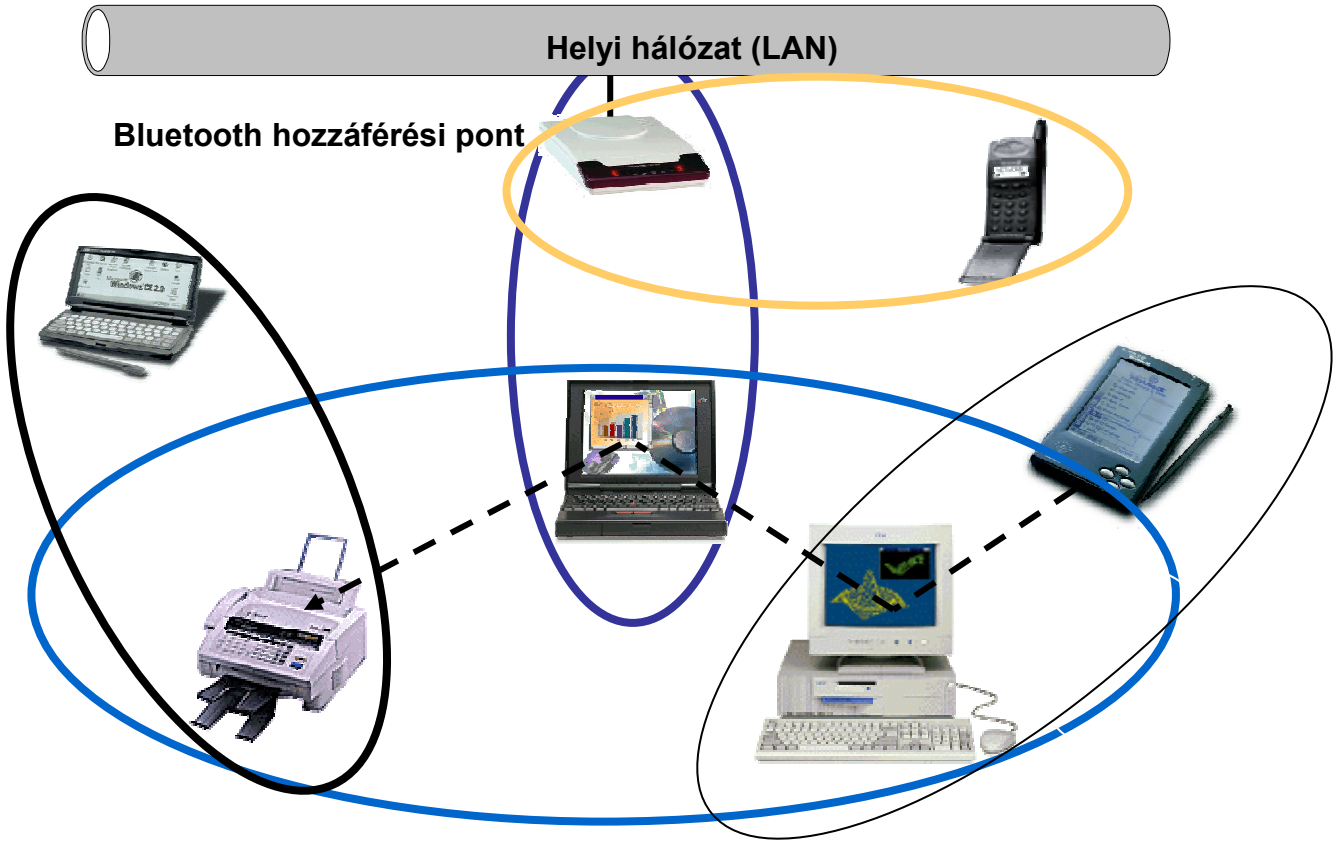
Hálózatszervezés, kommunikáció



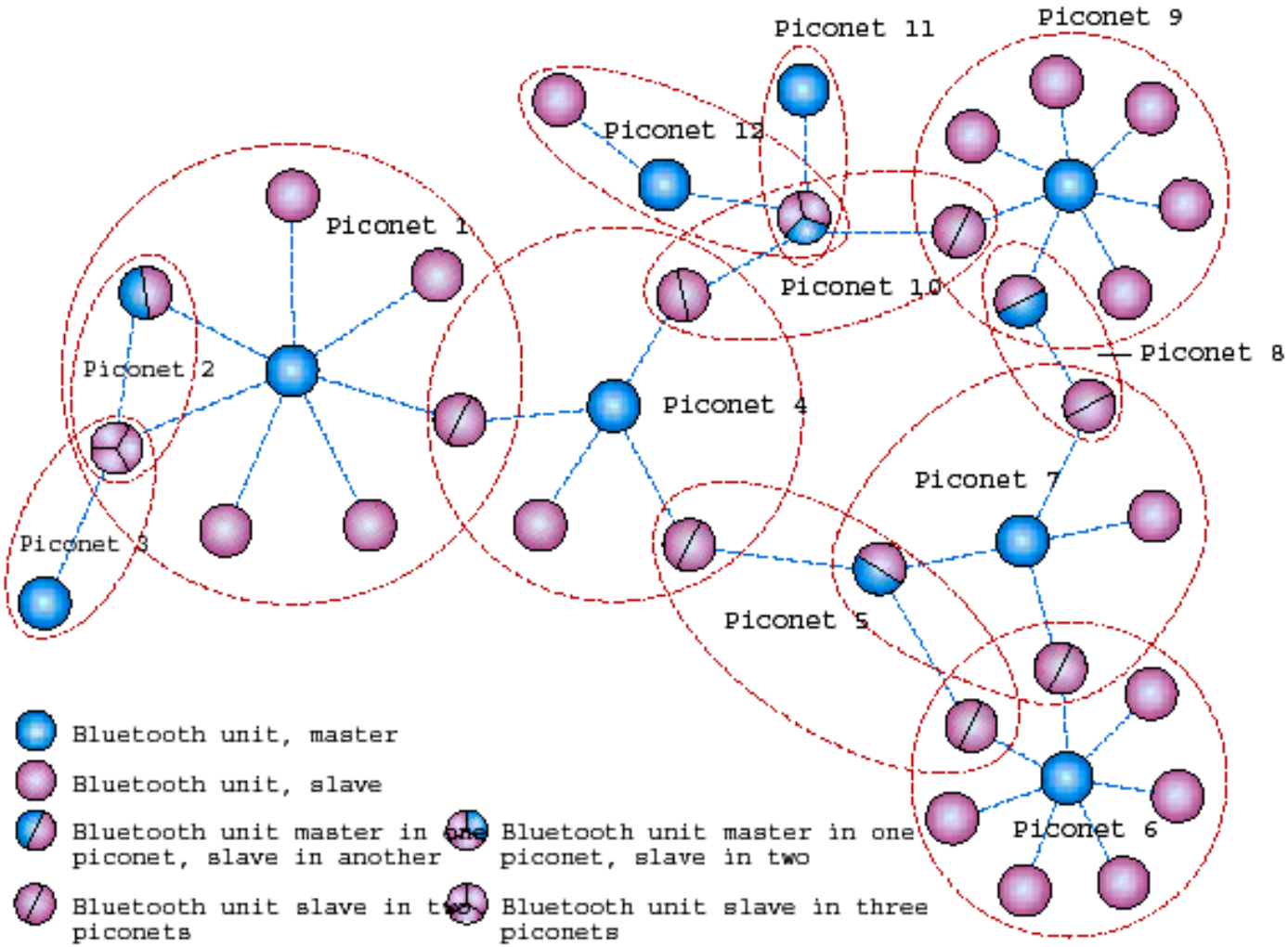
Max. 8 aktív állomás (255 „parkolt”)

M - master
S - slave

Piconet-ek



Scatternet


Piconet 11
Piconet 9
Piconet 12
Piconet 1
Piconet 10
Piconet 8
Piconet 2
Piconet 4
Piconet 7
Piconet 3
Piconet 5
Piconet 6
Bluetooth unit, master
Bluetooth unit, slave
Bluetooth unit master in one piconet, slave in another
Bluetooth unit master in one piconet, slave in two
Bluetooth unit slave in two piconets
Bluetooth unit slave in three piconets

Hálózatszervezés, kommunikáció

- Piconet: legfeljebb 8 aktív állomás egyszerre
- 1 master, a többi slave
- Scatternet: piconetek hálózata, dinamikus, ad-hoc alapon
- Van olyan node, amely >1 piconethez tartozik
- A Bluetooth nem rendelkezik a scatternetek kiépítésének módjáról

Hálózatszervezés, kommunikáció (folyt.)

- Szinkronizációs eljárás az elején
  - a slave-ek megtudják a master azonosítóját
  - órájukat összevetik: képessé váljanak a közös frekvencia-ugratásos sorozat előállítására

- Master megmondja: melyik slave melyik időrésben
- Hívásfelépítés:
  - *Inquiry*: további Bluetooth- eszközök felderítése a hatótávolságon belül
  - *Page*: felépíteni a kapcsolatot
    - pairing
- Kétféle összeköttetés:
  - SCO (*Synchronous Connection Oriented*) – hangátvitel, előre lefoglalt időrések
  - ACL (*Asynchronous Connectionless*) - adat

Bluetooth verziók

- Bluetooth 1.0
  - Interoperabilitási problémák
- 1.2
  - adaptív frekvencia ugratás
- 2.0
  - Enhanced Data Rate: 3Mbit/s!
  - kisebb energiafogyasztás
- 3.0
  - 24Mbit/s-ig, HS: vezérlési infók Bluetooth linken, adat WLAN-on
- 4.0
  - alacsony fogyasztású, orvosi és sportfelügyelet
    - Bluetooth Smart
- Jövő
  - Broadcast hirdetések pull módon
  - Automatikus scatternet konfiguráció
  - QoS: audio és video

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Nagysebességű PAN-ok → IEEE 802.15.3

- Célkitűzés: médiakommunikáció
  - digitális kamera – tv, MP3 ide-oda, videójátékok
- Új PHY specifikáció 55 Mbit/s-ig (11,22,33,44,55 Mbit/s), kb. 10 m-ig
- Másik munkacsoport: még nagyobb sebességek (110, 200, 480 Mbit/s) – házimozi, játékok
- A rádiós rétegre több lehetőség, egyik lehetőség az UWB

Nagy sávszélesség vs. SNR

- Shannon csatorna-kapacitással összefüggő egyenlete

$$C = B*\log(1+SNR)$$

- Sávszélesség növelésével az adatátviteli sebesség lineárisan, míg a jel-zaj viszony növelésével csak logaritmikusan növekszik

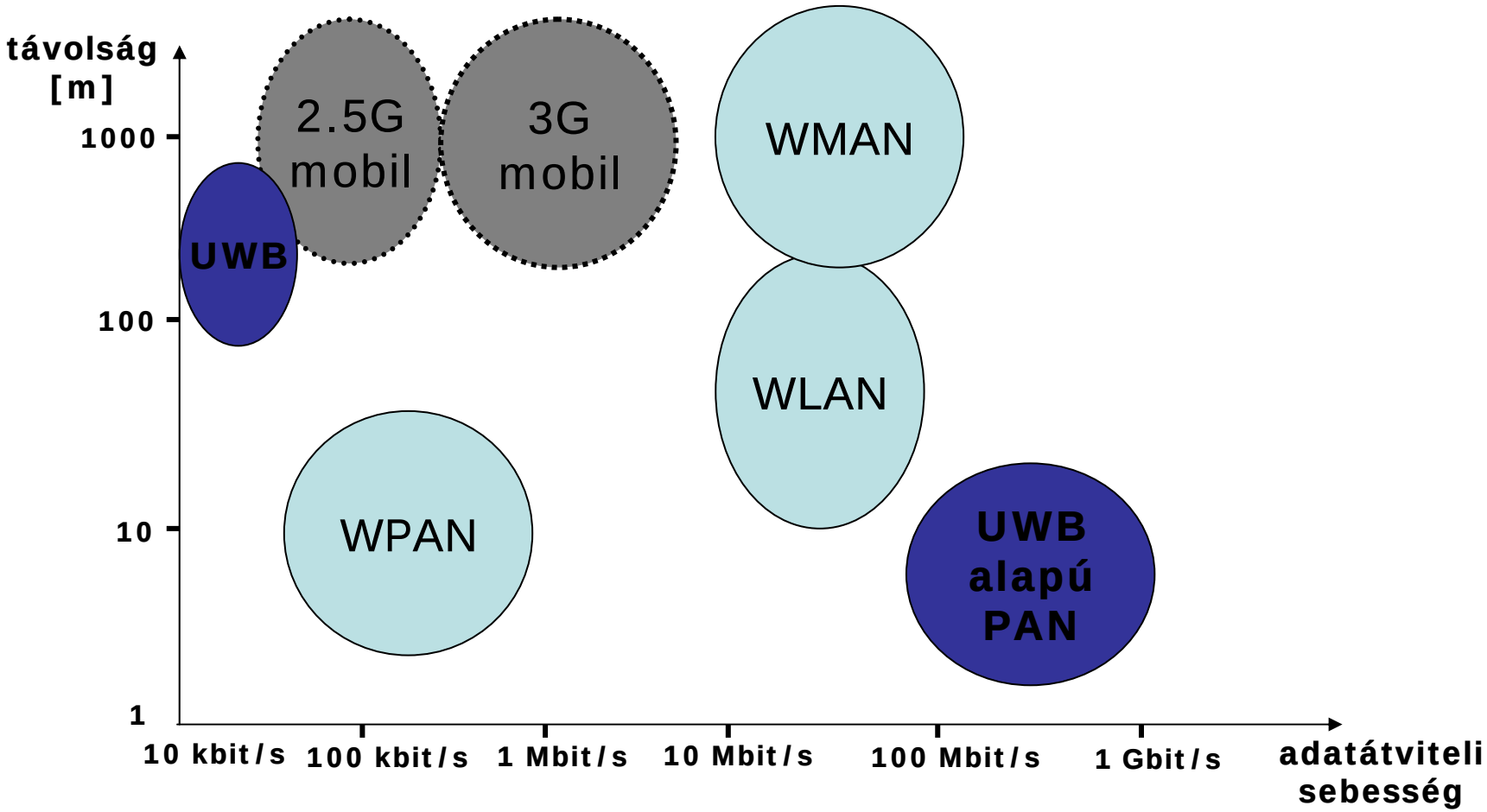
- Konklúzió: „jobban megéri” a sávszélességet növelni, mint az SNR-t

UWB (Ultra-Wideband)

- Nagy sávszélesség: min (>500 Mhz, sávközép+20%)
- Nincs vivő, igen rövid (pár ns), széles spektrumú impulzusok, kis teljesítmény
- Jelentős mértékben ellenáll a többutas terjedésnek
- FCC (USA) a 3,1...10,6 GHz-es sávban engedélyezi
- ETSI, CEPT (Európa) hasonlóan
- Széleskörű elterjedésétől még évekre vagyunk

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

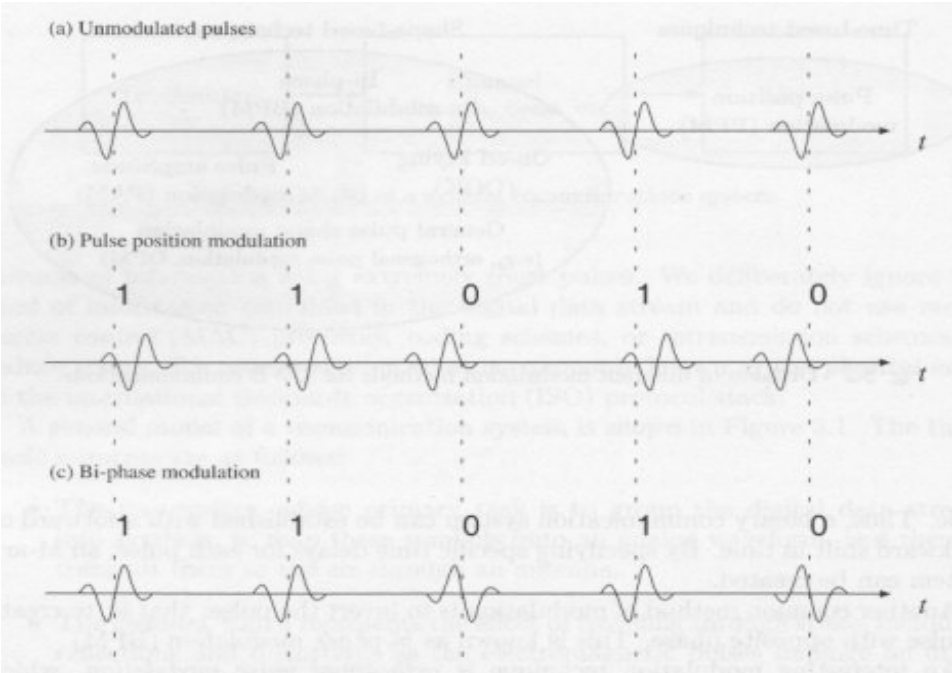
Az UWB helye – a kétféle UWB



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

UWB modulációs technikák

- Time-based (idő-alapú)
  - UWB impulzusokat adott egyenlőközű időintervallumokhoz képest korábban, vagy késleltetve küldjük
  - egyszerű, de az impulzusok nanoszekundum pontosságú előállítása szükséges
- Shape-based (jelforma-alapú)
  - ellenfázisú impulzusokkal



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Adatátviteli sebesség

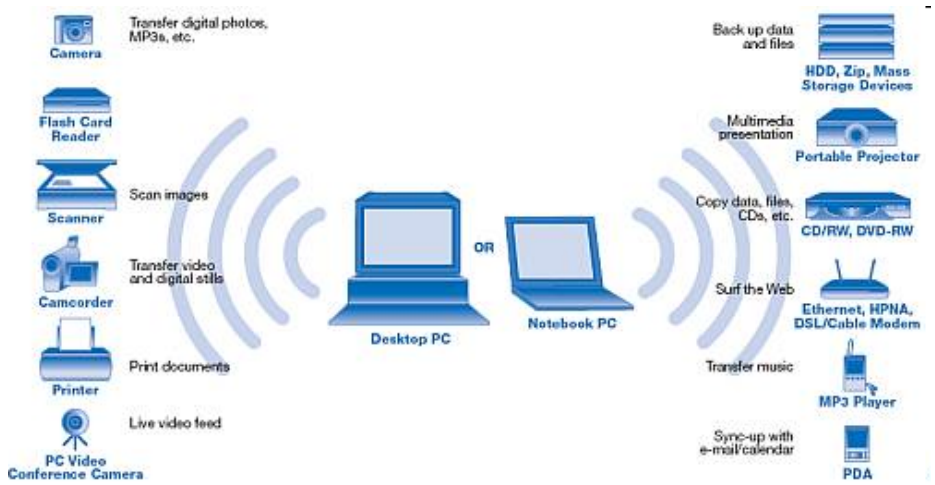
- Tipikus adatátviteli sebesség: 100 - 500 Mbps (~vezetékes Ethernet vagy az USB sebessége)

- Három szabványos adatátviteli sebesség létezik:
  - 110 Mbps 10 m-es minimális távolság esetén
  - 200 Mbps 4 m-es
  - 480 Mbps, ha kisebb

- Alacsony spektrális hatékonyság [bps/Hz], de magas területi hatékonyság [bps/m2]

UWB alkalmazások

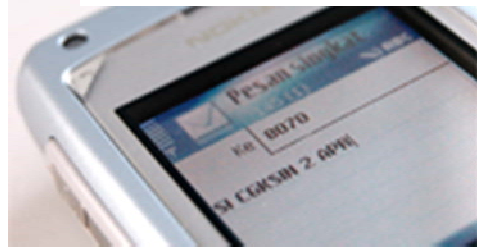
- Digitális Otthon
  - Wireless USB



- "Road Side Markers" (útszéli adóvevők)
  - információk az autósoknak pl. az időjárásról, az útviszonyokról vagy az aktuális útépítési munkálatokról
- "Through-the-wall Intrusion Sensor"
  - 1 W-os impulzusok segítségével képes érzékelni embereket akár több falon keresztül
- Eddig főleg katonai célokra használták

EMC összeférhetőség

- Legnagyobb nehézség: az impulzusok sávközép-frekvenciájának és sávszélességének pontos kézben tartása
- WLAN sávval átlapolódnak
- Ha a távolság > 50cm => nem tapasztalható szignifikáns csökkenés az IEEE 802.11b csatorna jel-zaj viszonyában.
- Ha a távolság < 50cm => az IEEE 802.11b csatorna jel-zaj viszonya 10-15 dB-el csökken



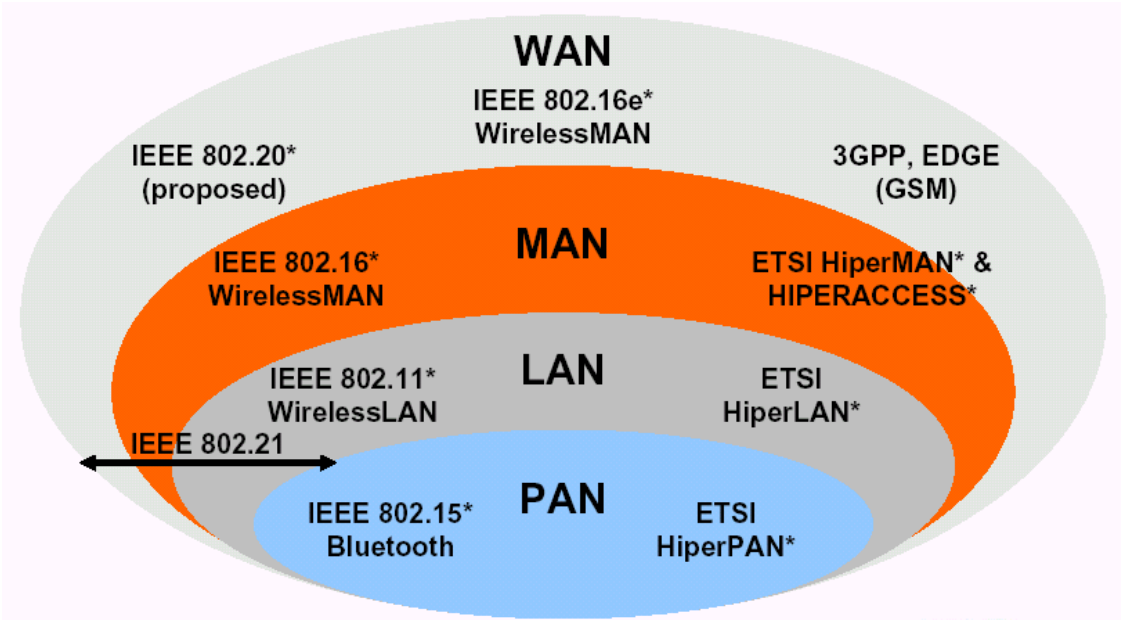
WiMAX – IEEE 802.16

Egy WMAN technológia

2013.március 19.

Nagyvárosi vezetéknélküli hálózat – WMAN és WiMAX

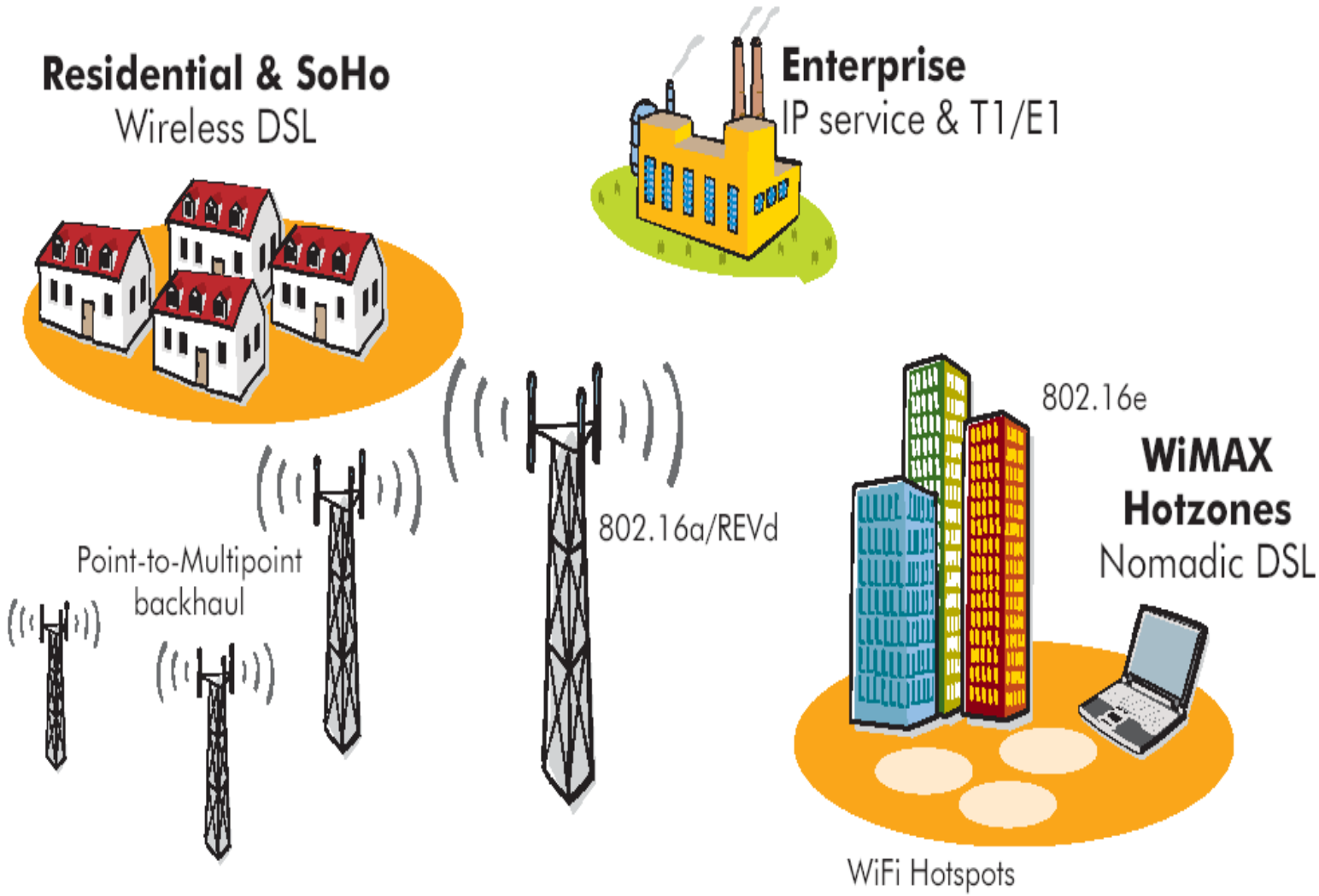
- WMAN – Wireless Metropolitan Area Network – IEEE 802.16
- WiMAX - Worldwide Interoperability for Microwave Access



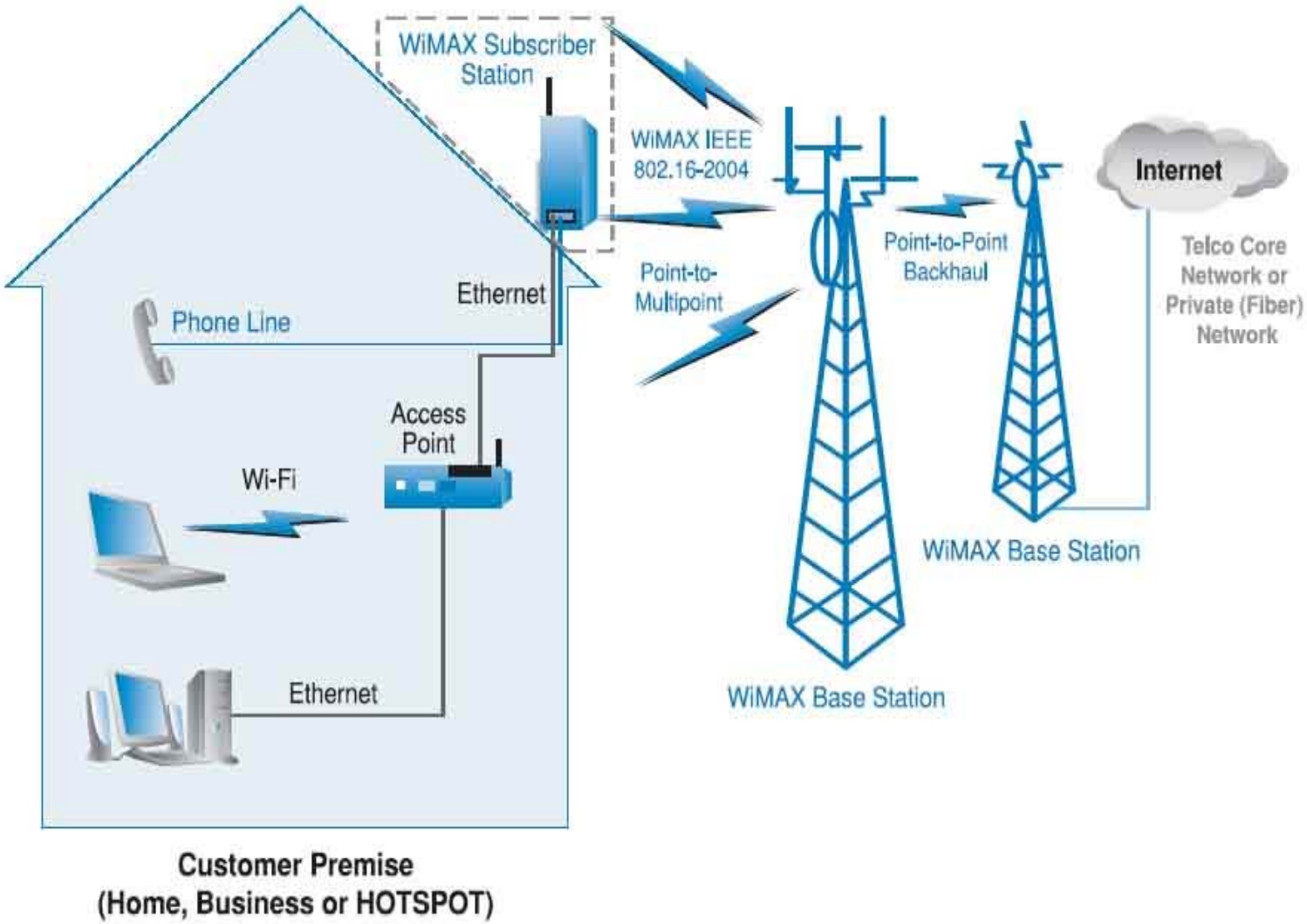
WMAN - WiMAX

- WLAN: IEEE 802.11x
  - Wi-Fi – WiFi Alliance (Wi-Fi – „wireless fidelity” a Hi-Fi mintájára)
- WMAN: IEEE 802.16x
  - WiMAX – WiMAX Forum – „Worldwide Interoperability of Microwave Access”
- *Wi-Fi Alliance és WiMAX Forum:* együttműködés a gyártók és a piac más szereplői között
  - a technikák bevezetésére,
  - a szabványokkal való kompatibilitás tanúsítására
  - a különböző gyártók közötti együttműködés tanúsítására

A WIMAX alkalmazási területei



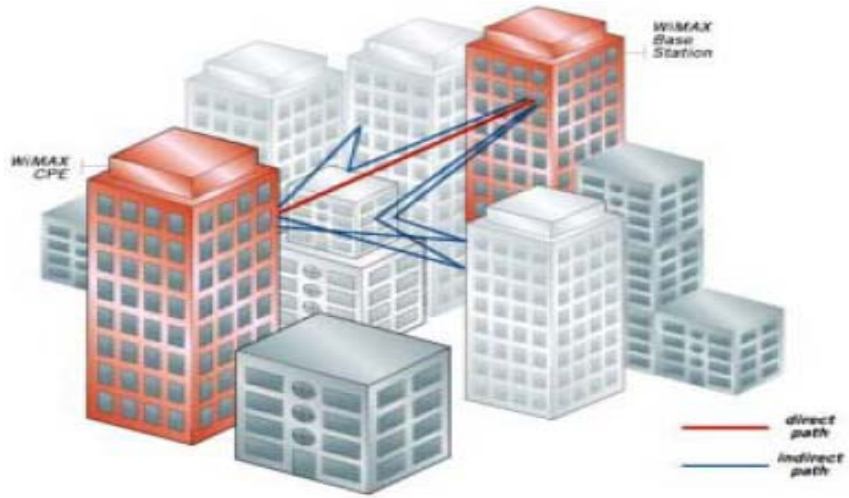
WIMAX alkalmazási területei: „hot zone”



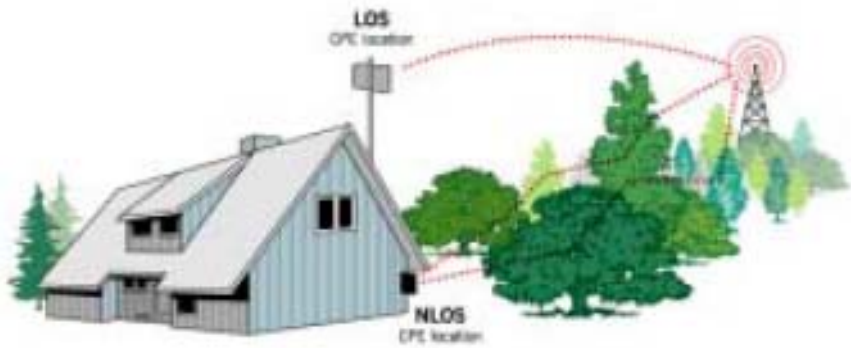
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

LOS – NLOS környezet

- LOS (line-of-sight)
  - Közvetlen rálátás
  - Nincs takarás a Fresnel-zónában
- NLOS (non-line-of-sight)
  - Nincs közvetlen rálátás (direkt jelút) csak reflektált hullámok
  - Így több jelút: többutas terjedés
- WiMAX-ban
  - speciális technikával a reflektált hullámok felhasználásával történik a vétel, ha nincs is direkt út (NLOS)

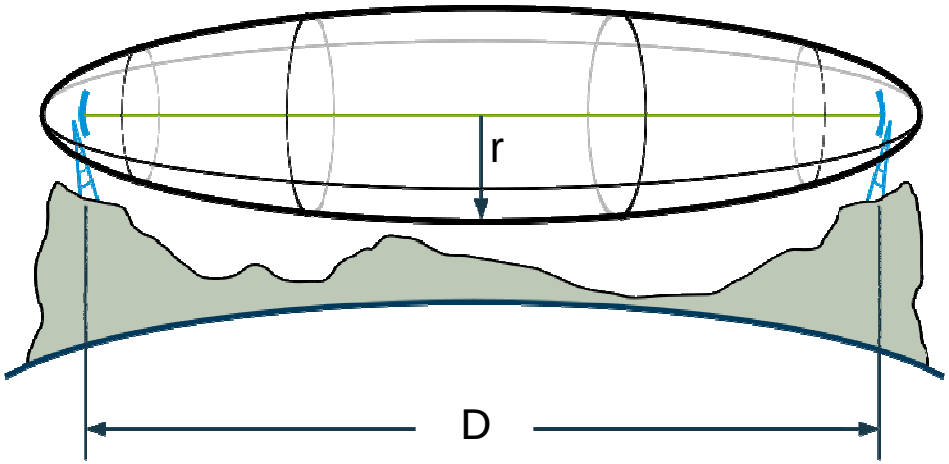


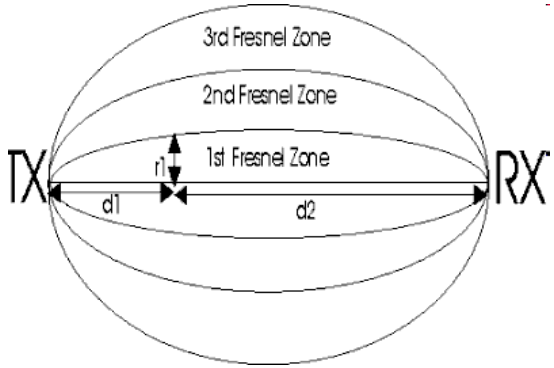
Közvetlen és többutas terjedés városi és rurális környezetben

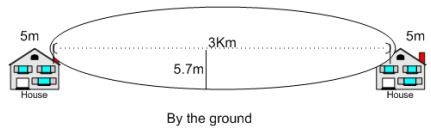


© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

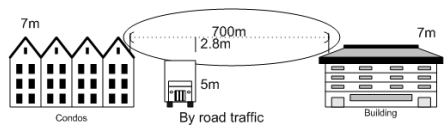
Fresnel zóna *







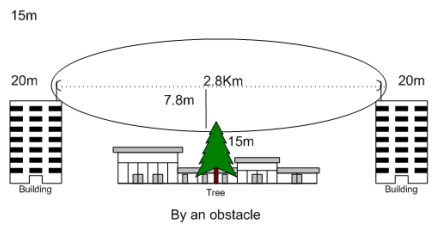
$$r = 17.32\sqrt{\frac{D}{4f}}$$



r: Fresnel zóna sugara [m]

D: távolság [km]

f: frekvencia [GHz]



WiMAX szabványok, verziók

- „Fix” WiMAX
  - 802.16d, vagy IEEE 802.16-2004
  - OFDM
- „Mobil” WiMAX
  - 802.16e
  - +MIMO

MŰEGYETEM 1782

BME

A WIMAX működése

Fizikai és közeghozzáférési réteg

2013.március 19.

Fizikai réteg: OFDM

- Többvivős modulációs/multiplexálási technika
- A rendelkezésre álló sávszélességet alvivőkre osztják
- A felhasználói adat soros-párhuzamos átalakítás és szimbólumformálás után
  - Külön alvivőkön kerül továbbításra
  - Ezeken alacsonyabb szimbólumsebességű moduláció
  - Kiküszöbölhető az ISI
- **Adaptív moduláció**:
  - BPSK-QPSK-16QAM-64QAM

MAC

- A WLAN-al ellentétben: ütemező algoritmus
- Csak egyszer kell versenyezni, utána minden állomásnak a bázisállomás fog időrést biztosítani
- Időrés csökkenhet-nőhet, de csak az adott felhasználó használhatja
- Így lehet QoS-t is biztosítani
  - pl. VoIP-ot előnyben részesíteni a web böngészéssel szemben
- Beengedés-szabályozás: biztosítja, hogy az új adatfolyam ne rontsa a meglevők minőségét

TDD - FDD

- Időosztásos duplex
  (Time Division Duplex – TDD)
  - félduplex kapcsolat
  - egyetlen csatorna: időben megosztva használják a kommunikáló felek.

- Frekvenciaosztásos duplex
  (Frequency Division Duplex – FDD)
  - WiMAX esetén 50 vagy 100 MHz-re lévő - frekvenciák
  - duplex (full-duplex)

Frekvenciasávok

- Engedélyköteles:
  - 2,500-2,690 GHz (MMDS) – csak USA
  - 3,410-3,600 GHz (ETSI) – csak EU

Szolgáltatás minősége garantálható

- Engedélymentes:
  - 5,725-5,850 GHz (U-NII)
    - Egyelőre katonai célokra használt

QoS nem garantált

  - Automatikus teljesítményszabályozás (TPC) ajánlott

MAC réteg

Biztonság, közeghozzáférés, QoS

Majd későbbi QoS előadásnál!

2013.március 19.

Wi-Fi - WiMAX összevetés

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

A WiMAX összefoglalása

- „Wi-Fi nagyban”
  - Eddiginél nagyobb adatsebesség (~70 Mbit/s)
  - Nagy távolságok (~50 km) áthidalása
- Minőségi különbségek
  - Közvetlen rálátás nélkül is jól működik
  - Többutas terjedés ellen „véd”
  - QoS-támogatás

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

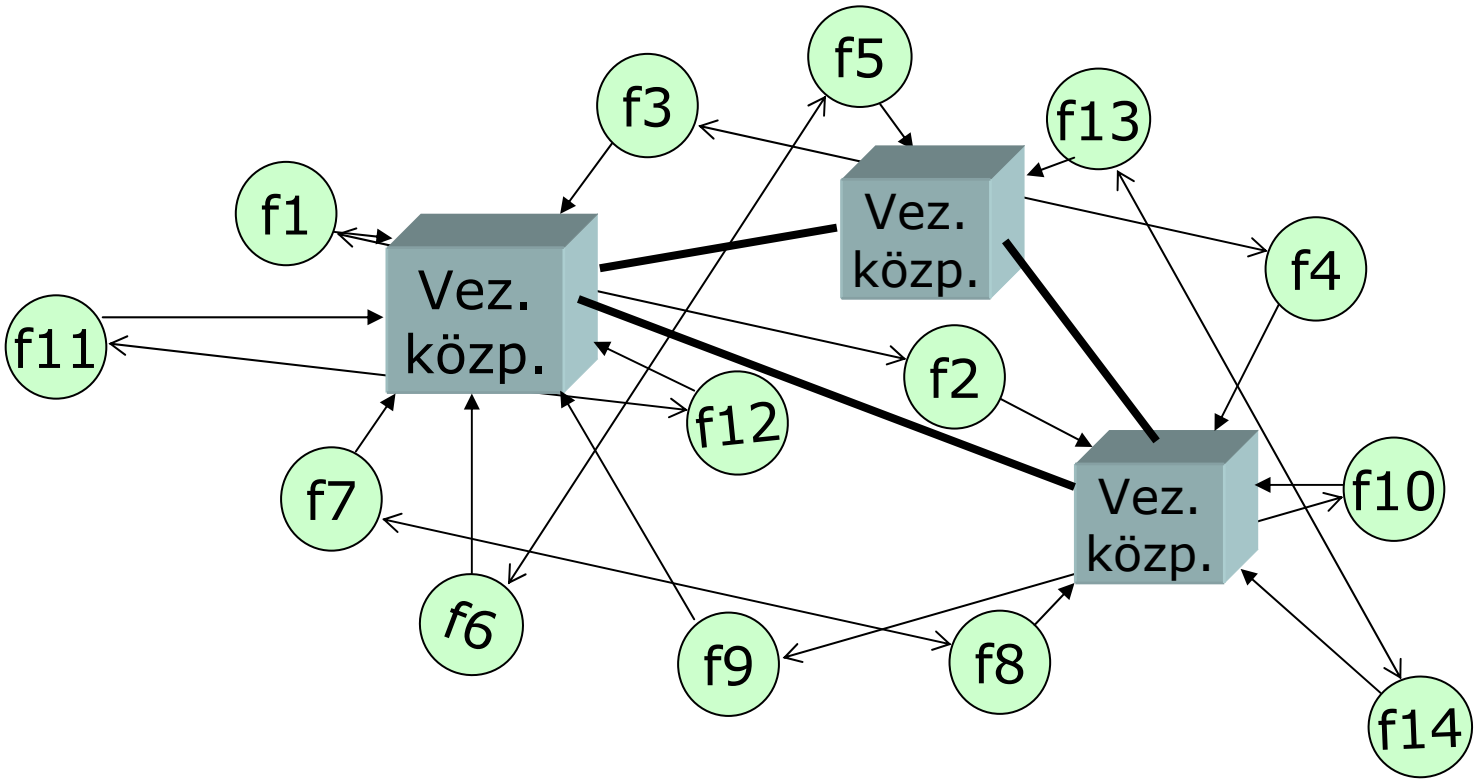
KAPCSOLÁS, JELZÉS, CÍMZÉS

(„Elmélet”, alapelvek és módszerek)

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.március 21

Hálózat?



Szövevényes kuszaság!

De hogyan működik?

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

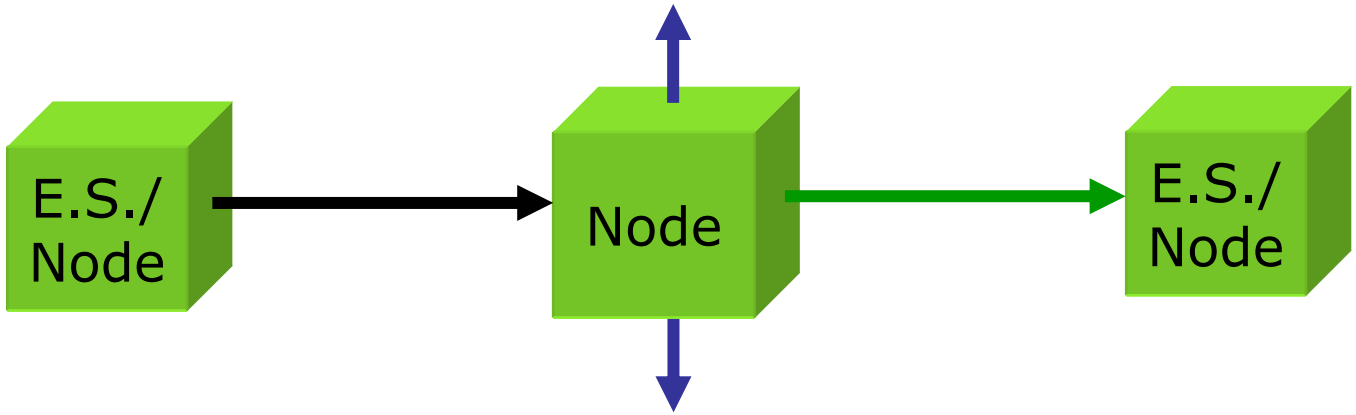
Kapcsolás

Áramkörkapcsolás,
hullámhossz-kapcsolás,
üzenetkapcsolás,
csomagkapcsolás,
virtuális áramkörkapcsolás.

2013.március 21

Kapcsolás

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



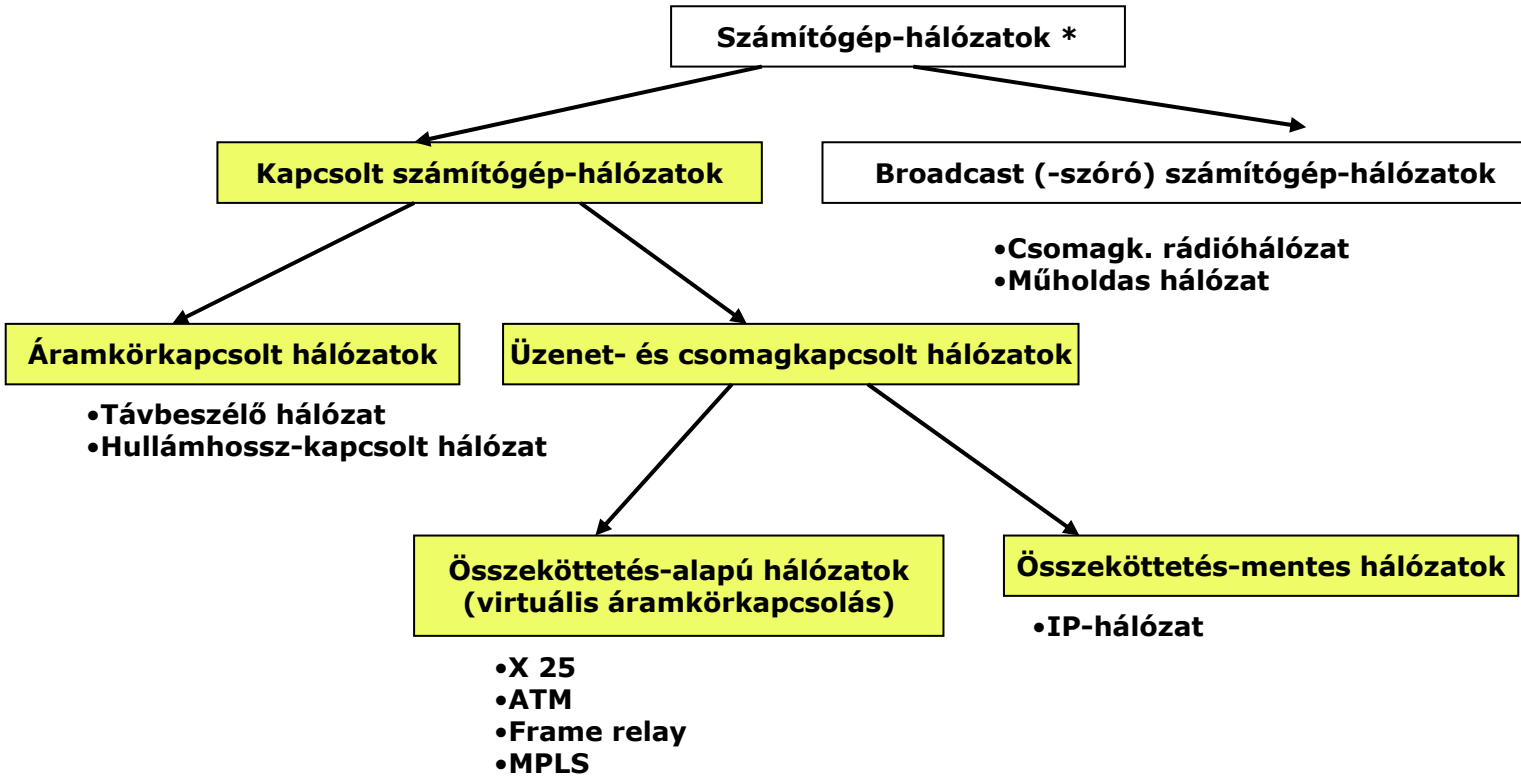
* E.S. =End System, végpont, felhasználói végpont

Milyen fajta kapcsolások léteznek?

- Áramkörkapcsolás – circuit switching
- Hullámhossz-kapcsolás *(~áramkörkapcsolás)*
- Üzenetkapcsolás – message switching
- Csomagkapcsolás – packet switching
  - *az üzenet- és a csomagkapcsolás rokonok*
- Virtuális áramkörkapcsolás
  (üzenet- ill. csomagkapcsoláson belül)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Áttekintés

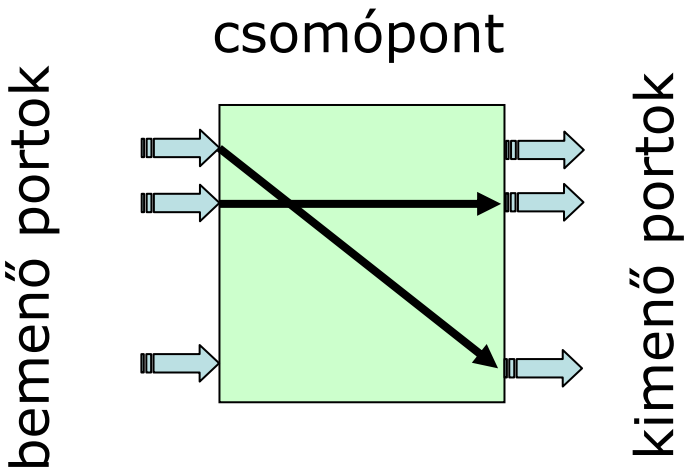


** általánosan: kommunikációs hálózatok – communication networks*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

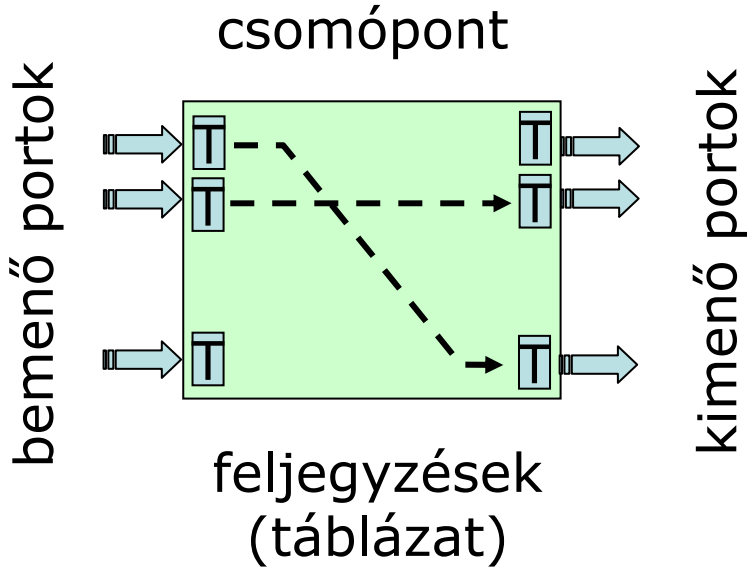
Az áramkör- és a csomagkapcsolás

- Áramkör-kapcsolás



- **Fizikai kapcsolat**

- Csomagkapcsolás



- **Logikai kapcsolat**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összeköttetés alapú és összeköttetés-mentes hálózatok

- Összeköttetés alapú hálózat
  - a tényleges adatátvitel előtt

    végpontok közötti összeköttetés

    (end-to-end connection)
  - ehhez külön jelzések!
- Összeköttetés-mentes hálózat
  - végpontok közötti adatátvitel előzetes összeköttetés létrehozása nélkül történik

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Áramkörkapcsolás/**vonalkapcsolás**

- Fizikai kapcsolat a küldő és a célállomás között
- A kapcsolat jellemzően nem állandó
  - **fel kell építeni** és az összeköttetés végén **le kell bontani**
- Minden felhasználói információ ugyanazon a **dedikált fizikai útvonalon** halad
- Valós idejű információátvitelre kiváló
- Továbbítás alatt a csomópontok **az adatokat nem tárolják**
- **Torlódás csak az összeköttetés felépítése során** léphet fel, az adatátvitel során nem

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Áramkörkapcsoló csomópontok

- Fizikai szintű kapcsolatokat kell létesíteni
- Kapcsolók általános felépítése
  - **kapcsolóelem**
    - a tényleges kapcsolást végzi
    - változatos megvalósítási módok, ezek szerint osztályozzák is a kapcsolókat
  - **kapcsolóvezérlő**
    - kiválasztja az(oka)t a kapcsolóelem(eke)t, amely(ek) működésbe lép(nek) kapcsoláskor
- Blokkoló és blokkolásmentes kapcsológépek
  - belső és külső blokkolás
  - többfokozatú kapcsológépek

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

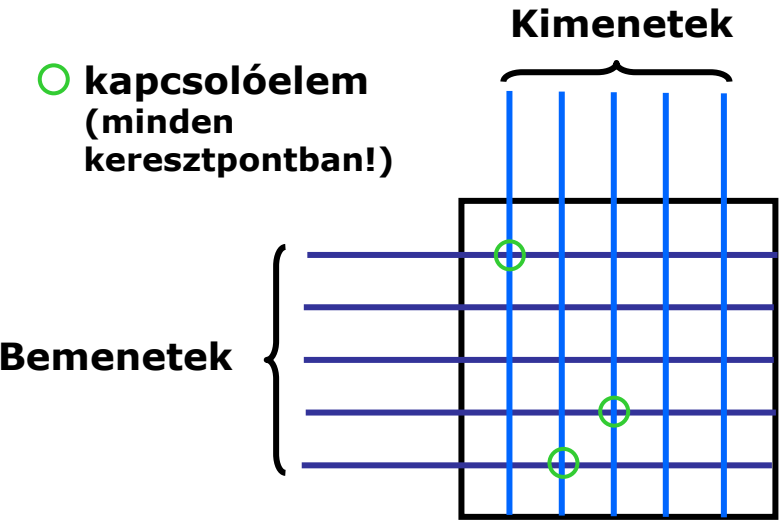
„Blokkolás” a kapcsolókban

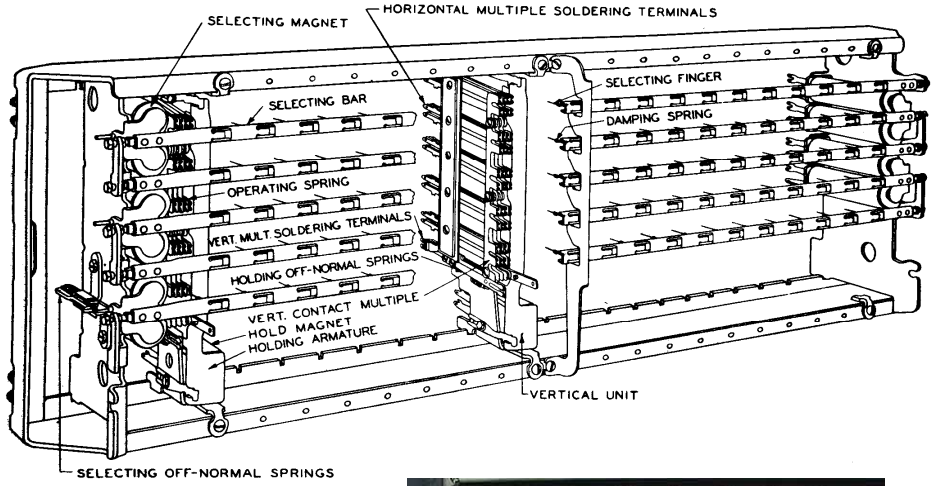
- **belső blokkolás** (internal blocking): a kért kimenet szabad, de nincs útvonal a bemenettől a kimenetig
- **kimeneti blokkolás** (output blocking): két bemenet ugyanazt a kimenetet akarja használni, ilyenkor az egyik kimenet blokkolt lesz
- az egyszerű crossbar (keresztpontos) kapcsolóban nincs belső blokkolás
- ha megengedünk blokkolást, akkor hatékonyabb kapcsológépeket készíthetünk
  - több fokozat alkalmazásával és a ki-bemenetek közötti útvonalak létesítésével

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

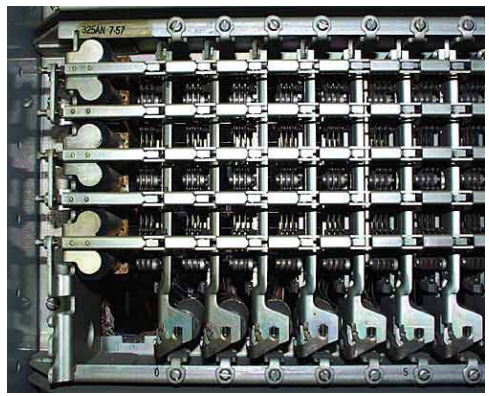
Egy régi kapcsológép: a keresztpontos (crossbar) kapcsoló

- kapcsolóelem (minden keresztpontban!)



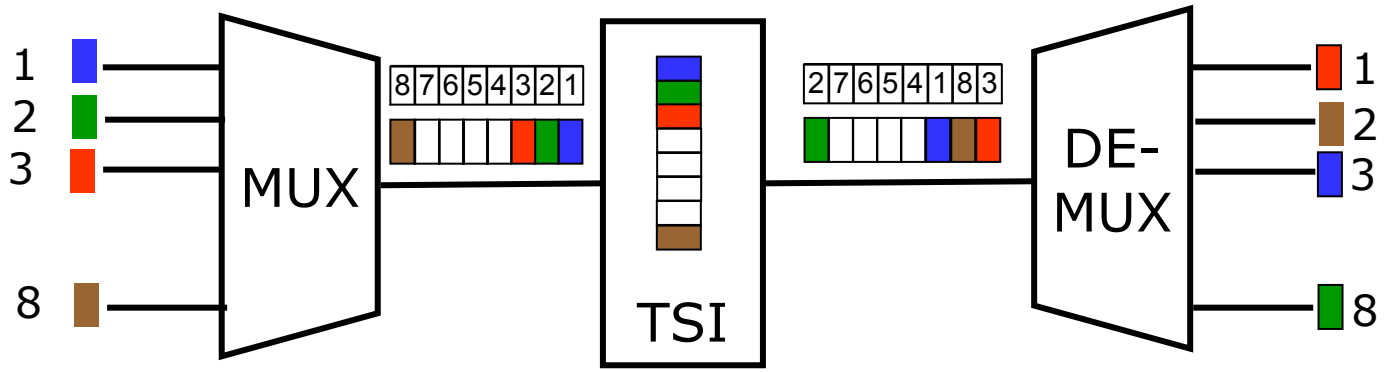


5 x 5-ös kapcsoló elvi rajza, korai elektromechanikus (jelfogós) kapcsoló szerkezeti rajza és fényképe



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Időosztású kapcsológépek: kapcsolás időréscseréléssel



TSI – Time Slot Interchanger

- Az **időosztású multiplexálás** elvének felhasználása
- A TDM jel beírása memóriába adott sorrendben, kiolvasás eltérő sorrendben = kapcsolás
- Korlátos számú csatornát tud csak kapcsolni, ezért kombinálják a térosztású elvvel

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hullámhossz-kapcsolás

- WDM emlékeztető:

- A felső adó λ_1, az alsó pedig λ_2 hullámhosszú fényt bocsát ki, ezeket a multiplexer egyetlen üvegszálra multiplexálja, majd az átviteli út végén a demultiplexer a λ_1 hullámhosszúságú jelet a felső, a λ_2 -t pedig az alsó vevőhöz irányítja

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

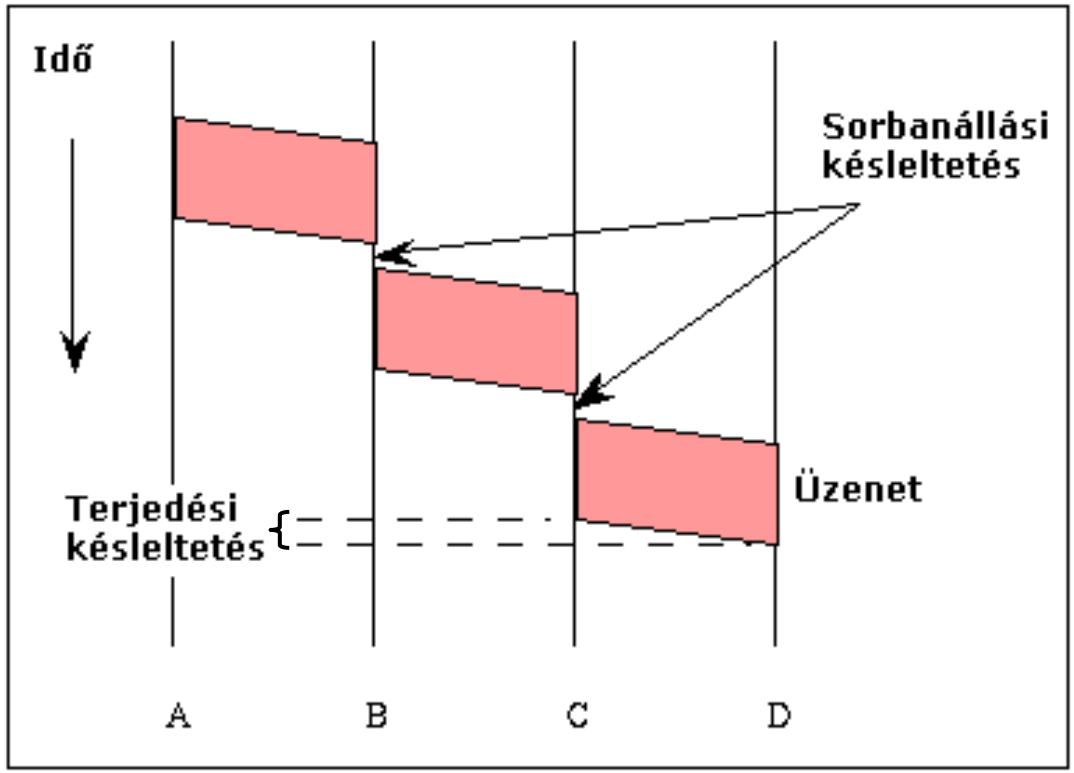
Üzenetkapcsolás

- Az egész üzenet egyetlen egységként egyik csomóponttól a szomszédos másikig
- A csomópontok időlegesen tárolják, majd továbbítsák az üzenetet: store-and-forward
- Megvalósításához
  - az üzenetben **címrész**
  - a csomópontokban **átmeneti tárolás** kell

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az átvitel folyamata üzenetkapcsolással

- **Egy üzenet átvitele A és D csomópont között három lépésben: az AB, BC és CD szomszédos állomások közötti kapcsolatok sorozatán keresztül**
- **B és C csomópont esetleg nem azonnal továbbítja az üzenetet, várakozási sorba helyezi, majd a kimeneti csatorna felszabadulásakor továbbküldi**



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Üzenetkapcsolás

- Előnye:
  - az adatcsatornákat a kommunikáló eszközök megosztva használják, **javul a csatorna kihasználtsága**
  - **késleltetés blokkolás helyett**
  - az üzenetekhez elsőbbség (**prioritás**) rendelhető
  - támogatja az üzenetszórást (**broadcast**)

- Hátránya:
  - a fellépő késleltetések miatt gond a valós idejű átvitel (élő hang ☹, mozgókép ☹)
  - adatátvitelre jó, amikor a késleltetésre kevésbé vagyunk érzékenyek

- Tulajdonképpen ez a fajta kapcsolás volt az ARPANET hálózatban

Csomagkapcsolás

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

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csomagkapcsolás

- Csomagkapcsolt hálózatok csomóponti eszközei:
  - kapcsoló (switch): olyan csomópont, amely a csomagokat ugyanazon helyi hálózat más csomópontjaihoz továbbítja
  - útválasztó (router): két vagy több hálózat között továbbítja a csomagokat

- Csomagkapcsolás megvalósítható:
  - összeköttetés-mentes módon: datagram kapcsolás
  - összeköttetés alapú módon: virtuális áramkörkapcsolás

Datagram-kapcsolás

- Minden csomag önálló egység
- Minden csomag tartalmazza a rendeltetési hely teljes (**globálisan egyedi**) címét
- A két végpont közötti csomópontok
  - megvizsgálják a csomag **fejrészét**
  - kiválasztják az útvonal **következő szakaszát**
- A választás során két tényező:
  - melyik az a csomópont, amely a csomagot a lehető legrövidebb úton juttatja rendeltetési helyére
  - hol található szabad csomópont, amely képes a csomag fogadására

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Blokkolás” a csomagkapcsolókban

- **Belső és kimeneti torlódás** egyaránt lehetséges
- A torlódás átmeneti, fellépte előre nem látható
- Elkerülésének módozatai:
  - túlbiztosítás (overprovisioning): a belső kapcsolatok gyorsabbra választása, mint a bemenetek sebessége
  - pufferelés: csomagok késleltetésére
  - visszaduzzasztás (backpressure): kapcsoló vezérlő arra kényszeríti a csomagok küldőjét, hogy ideiglenesen függessze fel a küldést
    - csak korlátozott ideig hatásos
  - párhuzamos kapcsolás: több párhuzamos útvonal kialakítása a bemenetek és a kimenetek között
    - a túltartalékolás térbeli megfelelője

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Virtuális áramkörkapcsolás

- A küldő és a cél végpontok között egy, a hálózat csomópontjai közötti **szakaszokból álló összeköttetés** létesül

- Analógia az áramkörkapcsolással:
  - két végpont között **minden csomag ezt az útvonalat** használja
  - viszont nem valódi fizikai kapcsolat, innen a virtuális áramkörkapcsolás (virtual circuit switching) elnevezés

- A virtuális áramkörkapcsolásnál is megtalálható a
  - ***kapcsolat felépítés***
  - ***adatátvitel***
  - ***kapcsolat lebontás***

- A virtuális áramkörhöz egy helyi, az adott csomóponton érvényes azonosító
  - **virtuális áramkör azonosító** (Virtual Circuit Identifier, VCI)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csomagkapcsolás vs. áramkörkapcsolás

- Áramkörkapcsolás
  - dedikált használat, más nem használhatja
  - ideális: ha adatokat sorrendhelyesen és állandó sebességgel kell továbbítani, például telefonátvitel

- Csomagkapcsolás
  - az átviteli csatornák és egyéb erőforrások használata nem dedikált, több összeköttetés is használhatja ugyanazt a csatornát
  - ideális: lökésszerű átvitellel járó és a késleltetéseket jól tűrő adatok
    - például elektronikus levelek, weboldalak továbbítására

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

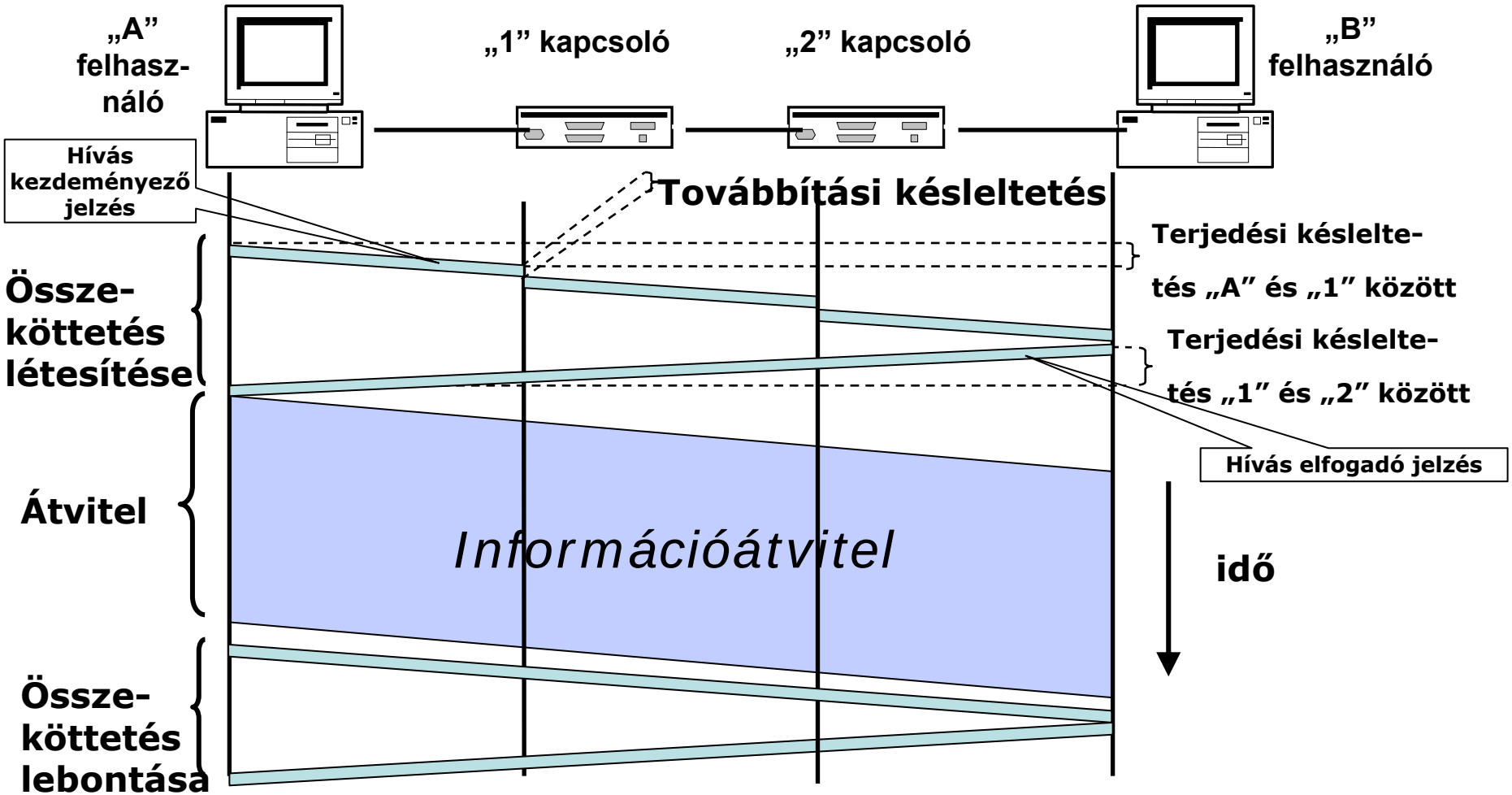
Jelzés

Signaling

Áramkörkapcsolásnál és virtuális áramkörkapcsolásnál

2013.március 21

A működés fázisai áramkörkapcsolásnál



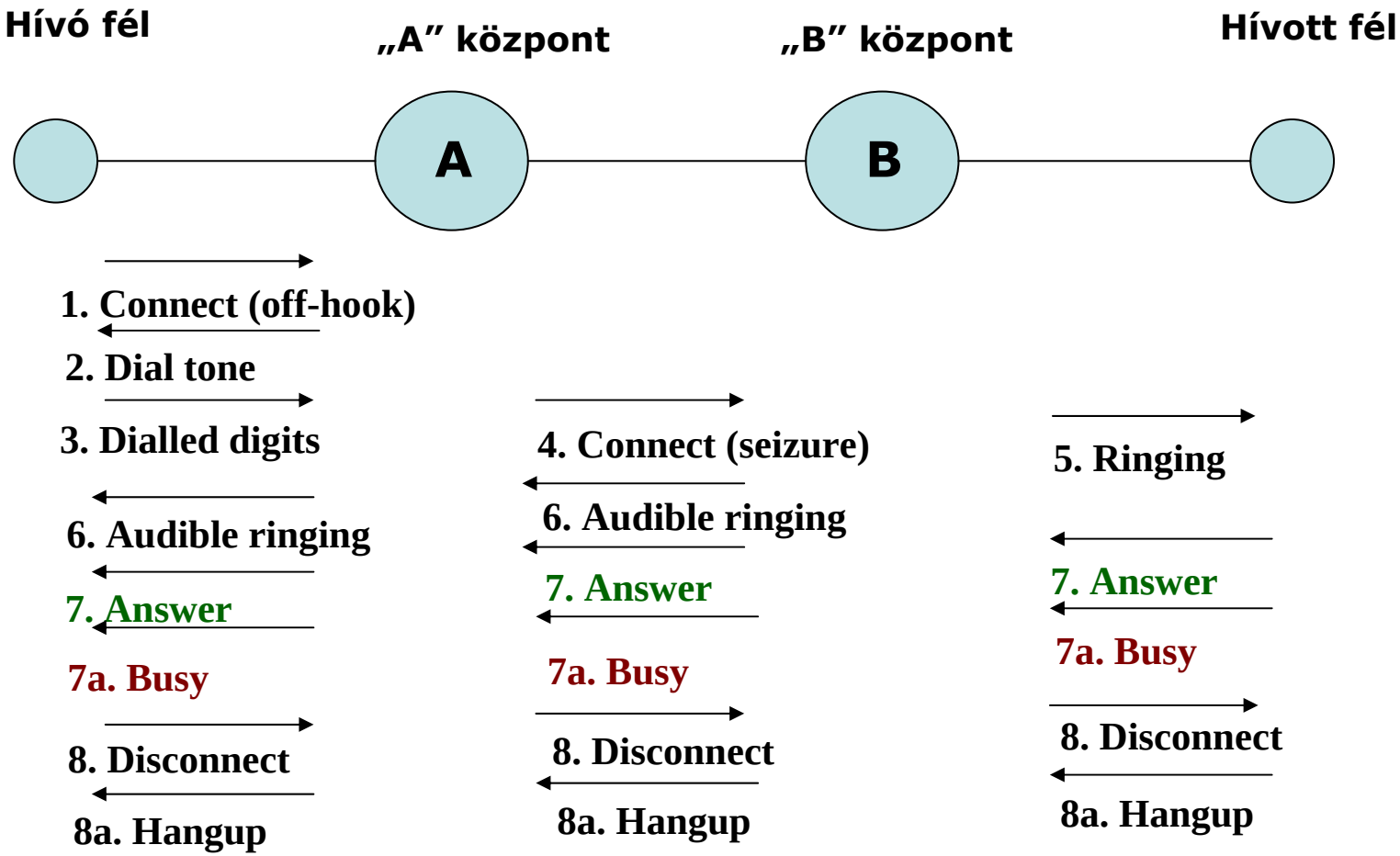
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hívásvezérlés

- „Hívások” (kapcsolatok, **összeköttetések**) létrehozása, fenntartása, lebontása
- Az ehhez szükséges jelzések rendszere
- Hívásvezérlő protokollok (valamely szabvány szerint)
- Angolul: call processing, call control systems/algorithms/protocols

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Jelzésátvitel, közönséges telefonhívás



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Jelzésrendszerek

- 2 féle jelzésátvitel:
  - Sávon belüli (in-band)
    - hagyományosan a telefóniában, ma is megvan még az analóg előfizetői vonalon (előf. „hurokban”)
  - Sávon kívüli (out-of-band)
    - a jelzések továbbítása külön csatornákon/hálózaton
- sávon kívüli jelzésátvitel → „közös csatornás” jelzésátvitel - common channel signaling (CCS)
  - rugalmasság, jobb sávszélesség-kihasználás
  - Észak-Amerikában különálló hálózatként valósult meg
  - az ISDN-ben: külön digitális csatornákon

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Elnevezés és címzés

Naming and addressing

2013.március 21

Elnevezés és címzés – *naming and addressing*

- Elnevezés (naming): egyedi név hozzárendelése a hálózat végpontjaihoz
  - Pl.: *diana.create-net.it*
- Címzés: egyedi cím hozzárendelése
  - Pl.: *213.21.183.196*
- Név-cím átalakítás: címfeloldás
- Miért kell mindkettő?
  - emberi tényező
  - előnyös a nevek és címek „szétcsatolása”

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Nevek hierarchikus használata

- Hogyan osszuk ki a neveket?

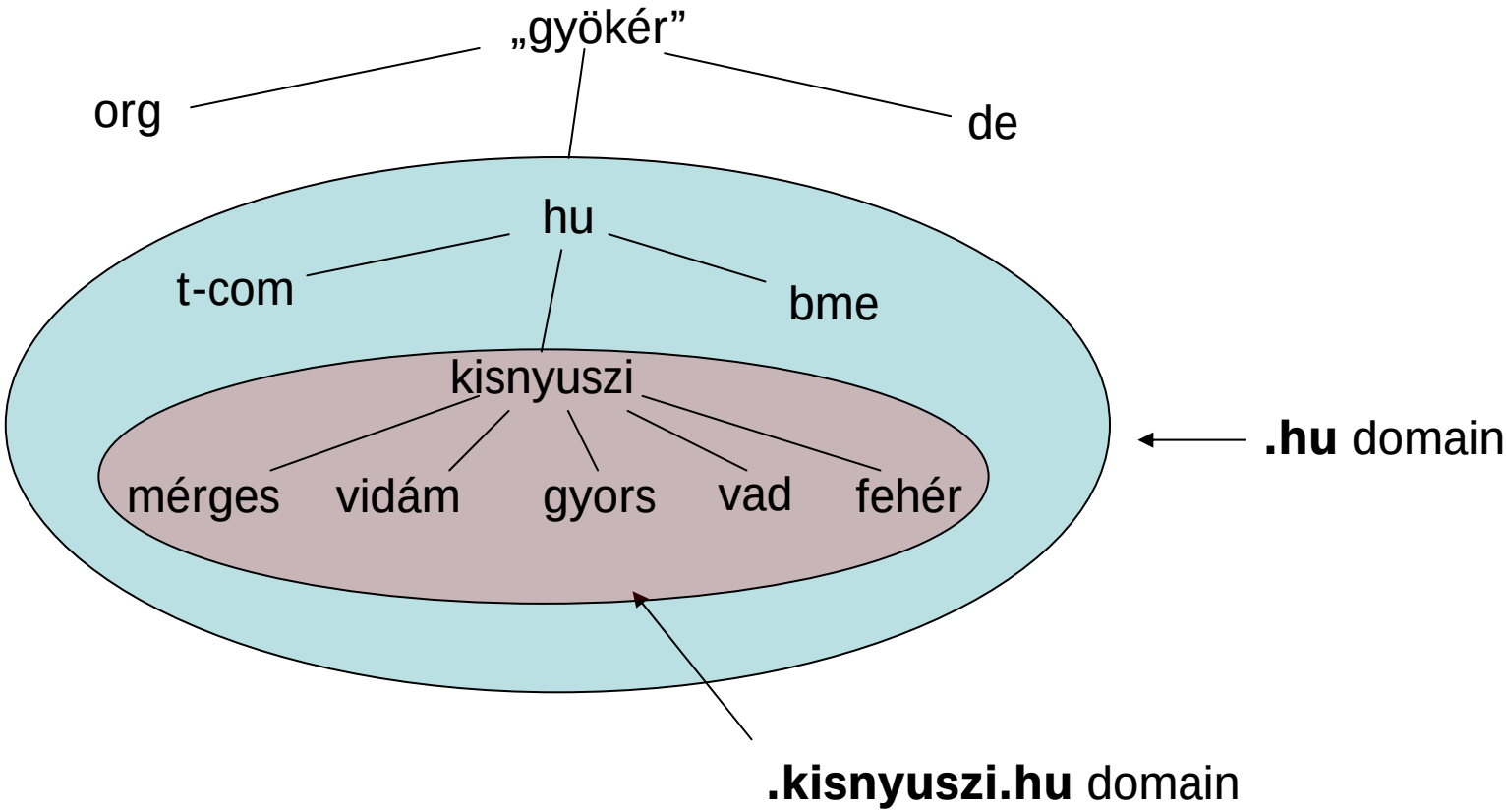
- Hierarchikus névadás
  - egy és több névadó
  - magasabb rendű névadó **prefixet** és **jogot ad** a további névadásra
  - pl. „a”, a.a, a.b, a.c (elválasztás pontokkal)

- Névtér (name space)
  - Tartományokra bontása (**domains**)

- Globális hatóság a csúcsszintű tartományban (**top-level domain**)
- Névadó hatóságok az egyes tartományokra
- Ezt használja a telefonhálózat és az Internet is

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Névtér, tartományok (*name space, domains*)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Névhasználat az Interneten

- Internet: DNS – Domain Name System
- Root domain: az üres string a záró pont után:
  hit.bme.hu.
- Top level domains: a név utolsó része
  - Az IANA adminisztrálja (Internet Assigned Numbers Authority)
  - **country code top-level domains (ccTLD), pl. .hu**
  - **generic top-level domains** (gTLD): pl. .org, .edu, .net, .com, .gov, .mil
    - eredetileg: a szervezetek egy-egy csoportja az USA-ban, ma már világszerte csaknem szabadon felhasználható, a .gov és a .mil csak az USA-ban
  - **infrastructure top-level domains**: egy van, az .arpa

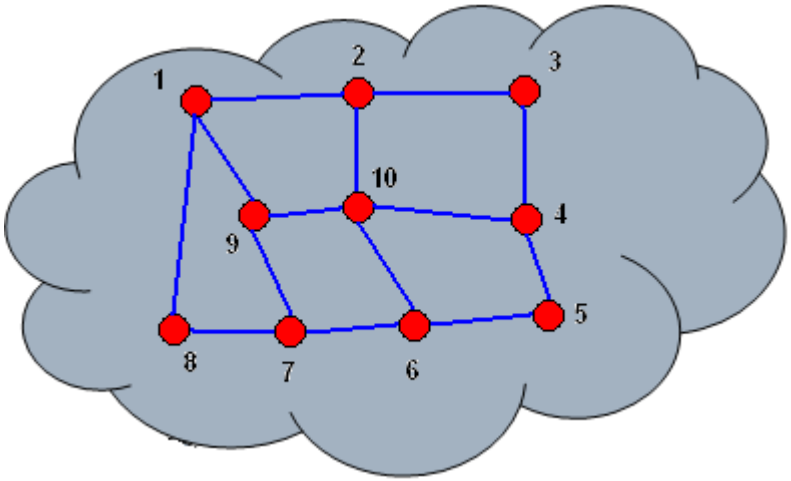
Címzés

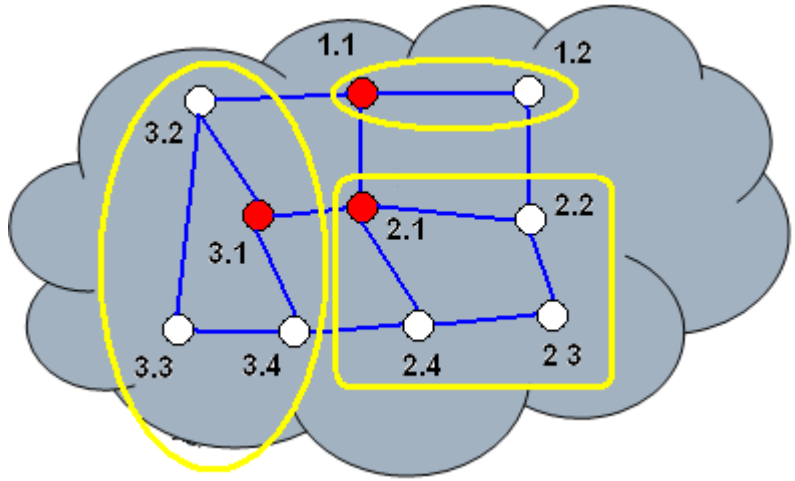
- A névhez hasonlóan
  - a címek is globálisan egyediek
  - hasonló okból célszerű ezeket is hierarchikusan szervezni

- A **hierarchikus** szervezésnek további oka az, hogy a hálózatokban egyszerűbbé teszik az
  útvonalválasztást
  - „lapos”, egyszintű címzésnél minden csomópontban nagy útvonalirányító tábla kell (routingtábla)
  - hierarchikus címzésnél nem mindenhol kell nagy
    - mivel alhálózatok alakíthatók ki,
    - csak a határokon kell nagy routingtábla

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Címek aggregálása





Hierarchia nélküli (flat) címzés

- Minden csomópontban nagy irányító tábla
- Minden táblában 9 bejegyzés

Hierarchikus címzés

- Címek csoportosíthatók
- Néhány csomópontban kell csak nagy irányító tábla

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csoportosítás nélküli hierarchia

- Van olyan globális, hierarchikus címzés, amely nem prefix jellegű
- Ilyen az Ethernet lokális hálózatokban használt címzés
- Ethernet-cím: az Ethernet adapter(kártya) egyedi címe
- 6 byte, 48 bit
- 3 byte-os része a gyártó kódja, a másik három az adapteré

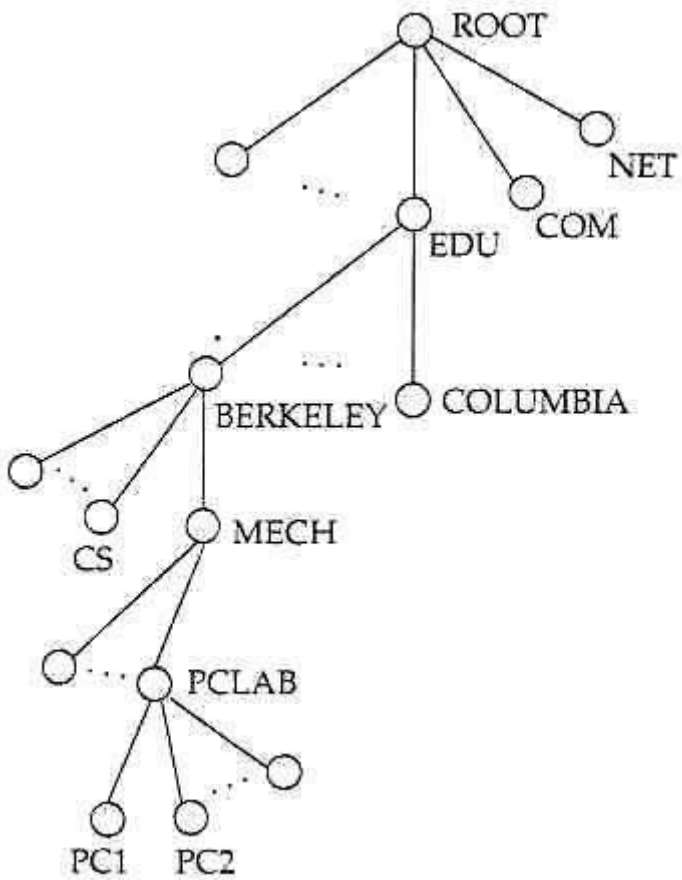
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Névfeloldás – *name resolution*

- **Névszerverek – name servers**
- Az Interneten a hierarchikus név- és címrendszer felhasználásával a **DNS – Domain Name System** végzi.

- Elvileg először a rootnak megy a kérés, az továbbítja az aktuális tartományba, az azt kezelő névszervernek

- A terhelés csökkentése:
  - szerver-replikáció: a DNS-ben egyazon tartományban több névszerver kezeli a kéréseket
  - cache-elés: amikor a végpont vagy ügynöke felold egy nevet, tárolja az eredményt az ismételt kérések számára



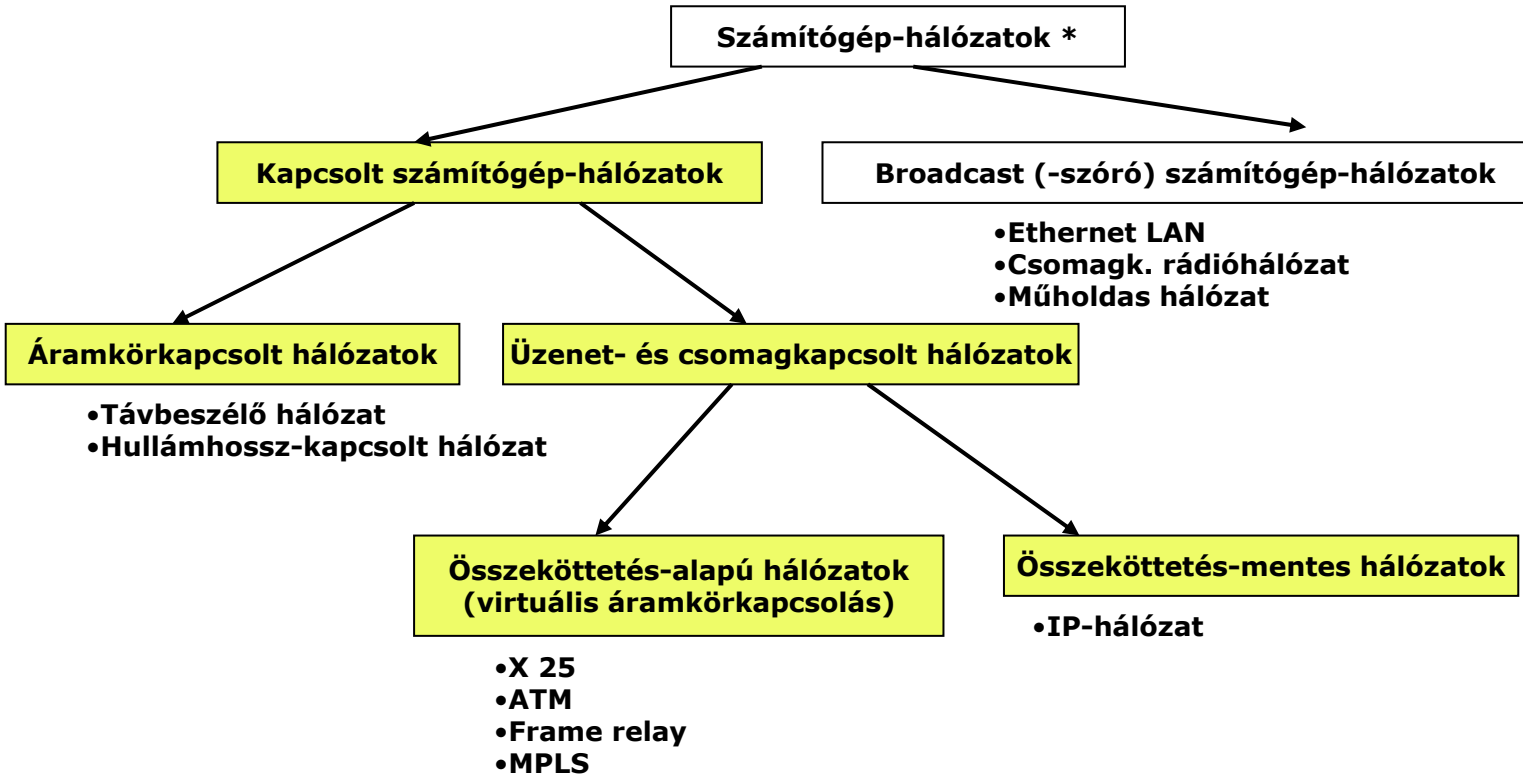
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Címzés több szinten

- Címzés lehetővé teszi a hálózatok közötti útvonalválasztást és csomagtovábbításhoz szükséges
- Az egyes hálózatokon belül gyakran egy másik szinten is van címzés
  - pl. az Ethernet LAN-ban a hálózati kártyáknak saját címzésük van
- *Tehát többszintű a címzés*
  - *címeket kezelünk a hálózati architektúra különböző rétegeiben*
- Az Ethernet LAN címzését az IEEE 802.3 szabványa határozza meg
  - hierarchikus, de nem prefix tulajdonságú címzés
- Átalakítás kell a hálózati és adatkapcsolati rétegbeli címek között: címfeloldás (l. később az IP-részben)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás



** általánosan: kommunikációs hálózatok – communication networks*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

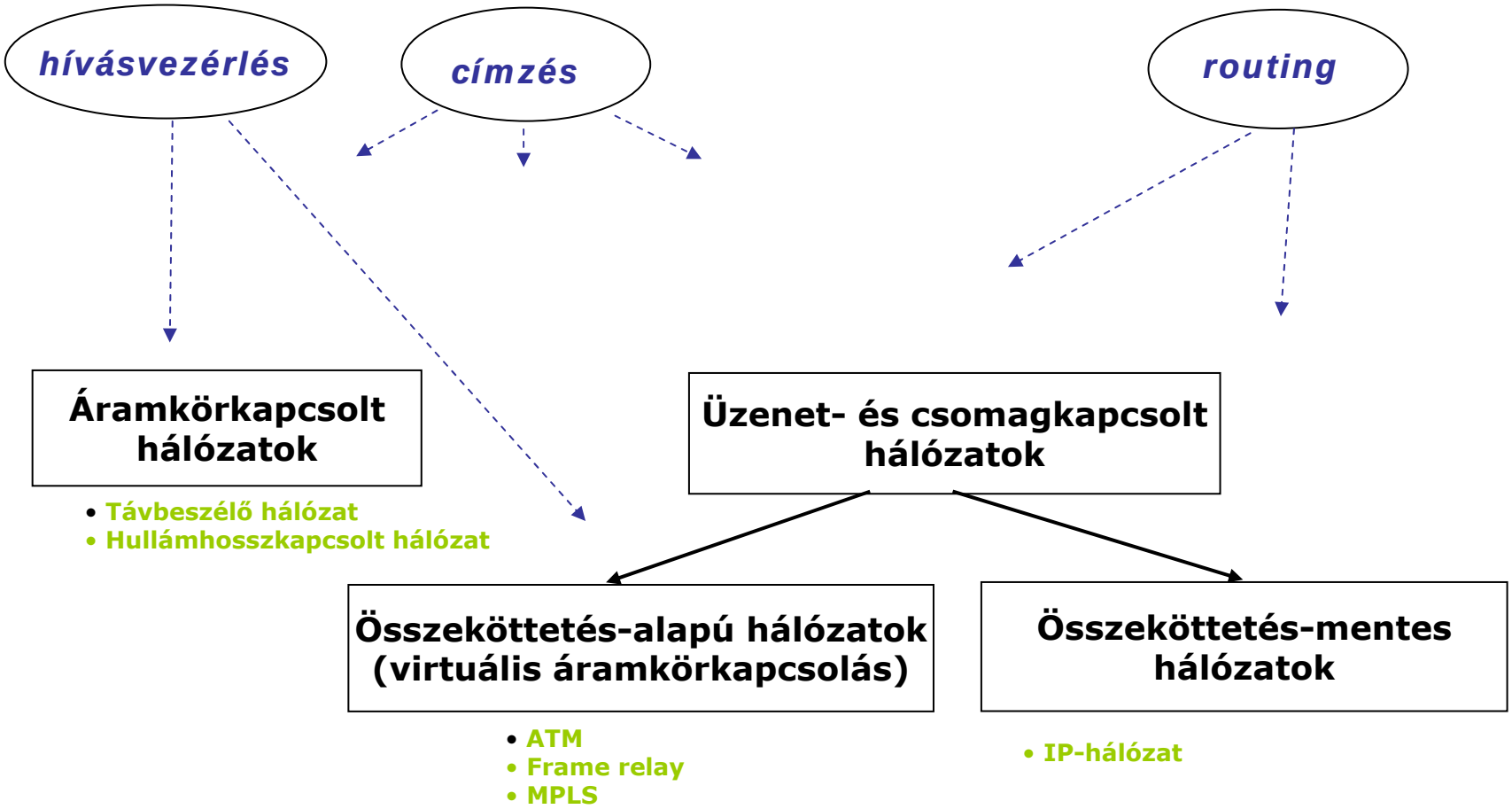
ROUTING

Útvonalválasztás

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.március 26.

További nagyon fontos funkció a kapcsolt hálózatok működtetéséhez



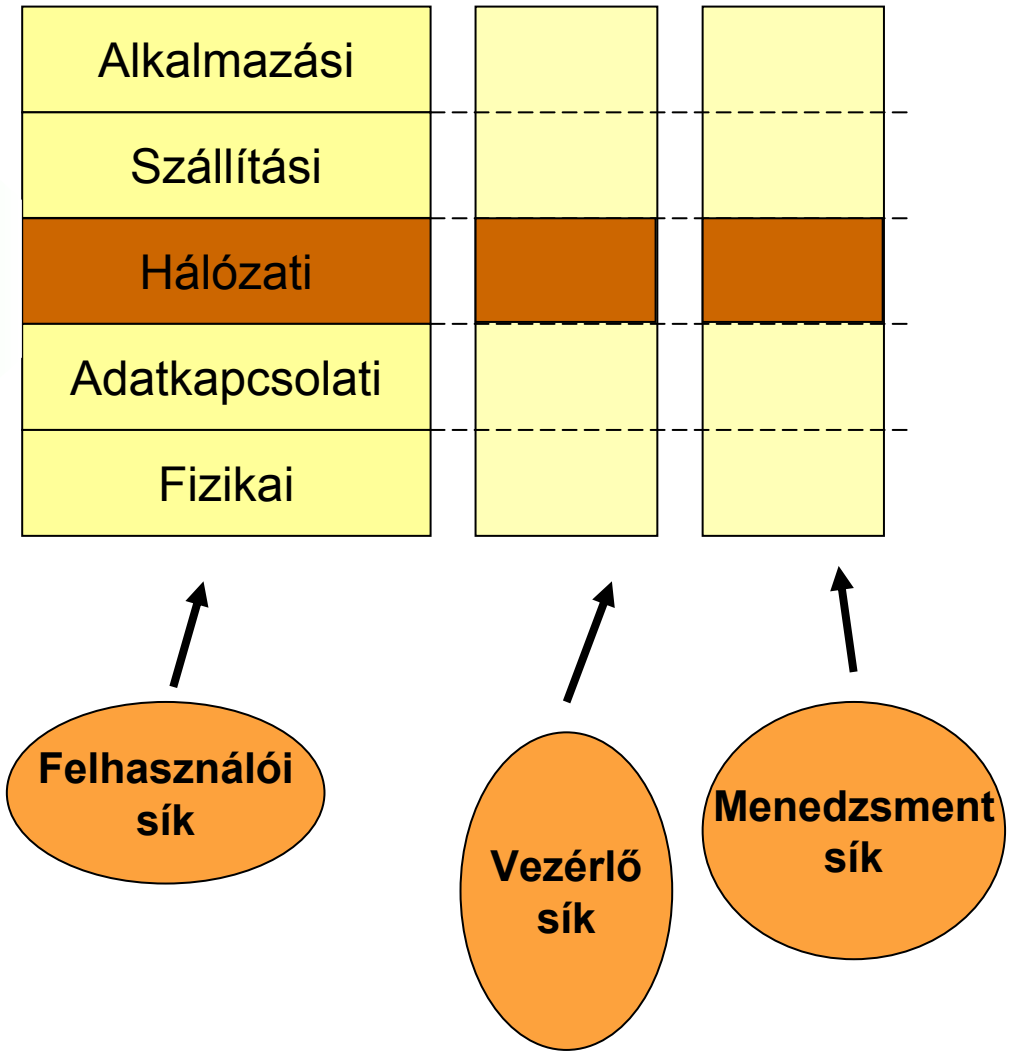
Elv, módszer, protokoll

Elv:

Routing

Módszerek:
Távolságvektor
Linkállapot

Protokollok: későbbiekben



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az elnevezésről...

.fr Routage

.de Routing

.ru Маршрутизация (marshrutizatsiya)

A Tanenbaum: Computer Networks könyv magyar fordításában: „forgalomirányítás”

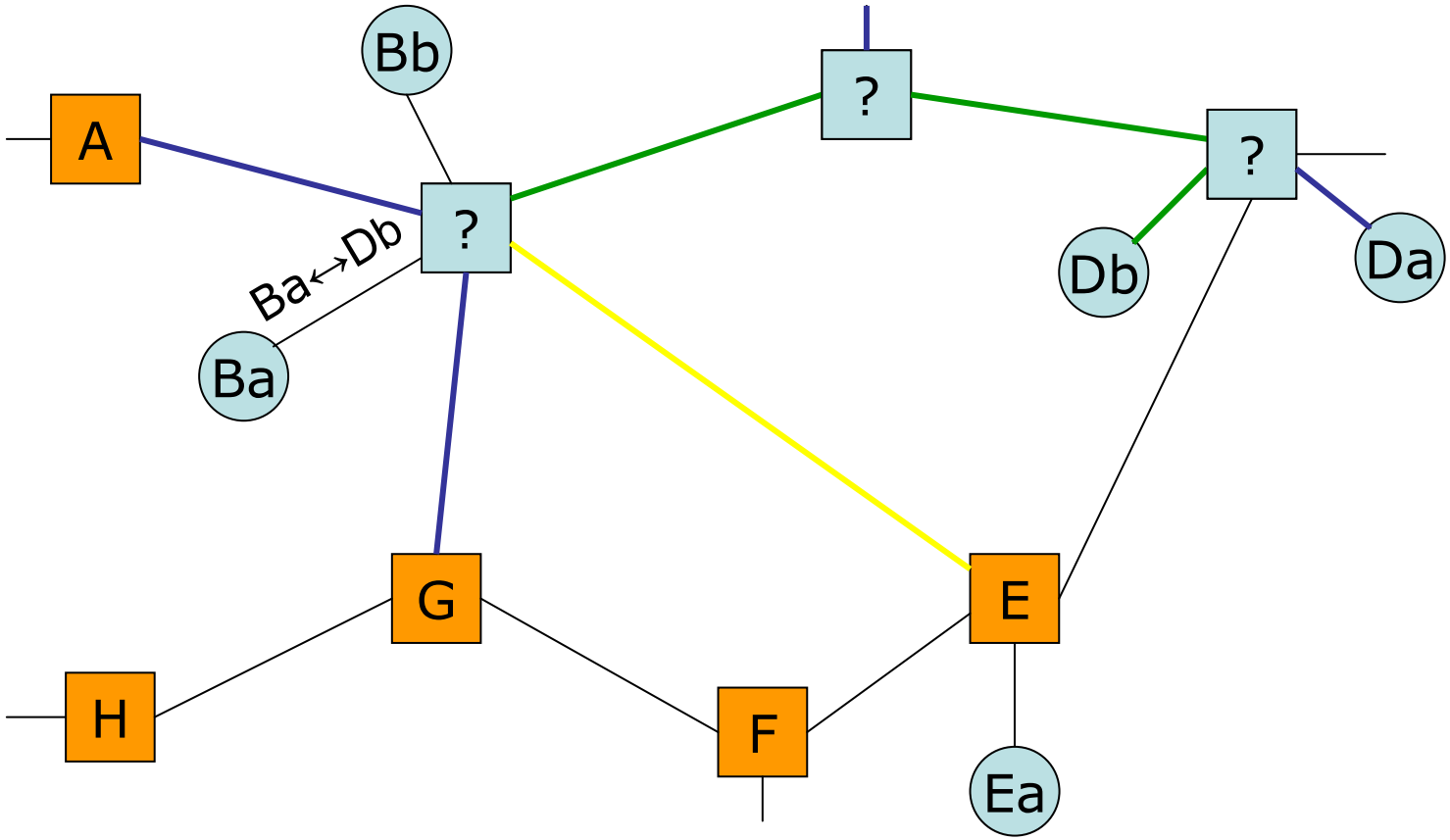
Nálunk (általában): routing

Mi a routing?

- *Az a mechanizmus, mely segítségével a szállítandó információ a **megfelelő útón** kerül továbbításra a végpontok között*
  - *szűkebb értelemben: csak az útvonalválasztás, útvonalkijelölés*
  - *tágabb értelemben: ideértjük a csomópontokban a csomagok **továbbítását** is*
- A feladat érdekessége:
  - Általában ***nem állandó*** a hálózat felépítése: adaptív módon
  - Gyakran **„nagy" a hálózat mérete**: nincs pontos és aktuális információ a hálózat állapotáról.
- Ez a feladat egyaránt felmerül az összeköttetés-alapú és –mentes hálózatokban
  - ö. a.: útvonalkijelölés
  - ö. m.: útvonalválasztás
- Ide tartoznak az útvonalválasztó **módszerek**, **algoritmusok** és az azokat megvalósító **protokollok**

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Bevezetés: a feladat értelmezése

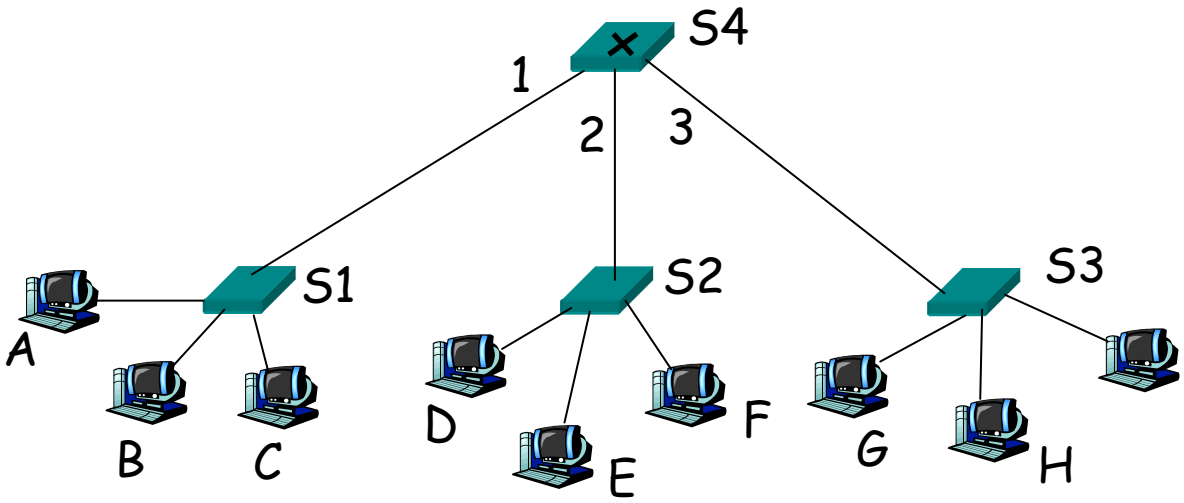


Különbség bridging és routing között

- Bridging (bridge vagy switch által végezve):
  - Nem tudja hol van pontosan az adott cím
  - A fogadott keretek forráscíme alapján bejegyzés a táblában:
    - MAC Address, Interface, Time Stamp
    - régi bejegyzéseket eldobja
  - Megtanulja, hogy melyik végpontokat melyik interfészen keresztül tudja elérni

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa bridging-re (LAN előadásról)

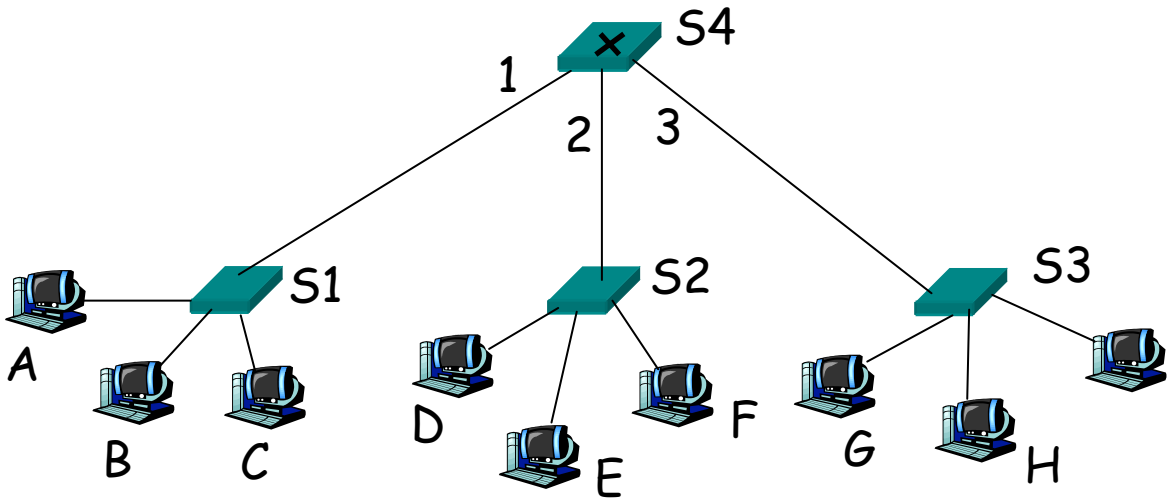


address	interface
A	1
B	1
E	2
G	3
I	

- A kapcsoló vesz egy C-től D-nek menő keretet
  - bejegyzi a táblába, hogy C az 1-es interfészen érhető el
  - mivel D nincs benne a táblában, továbbítja a keretet a 2 és 3 interfészre
- D veszi a keretet

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa bridging-re (folyt.)



address	interface
A	1
B	1
C	1
E	2
G	3

I

- A kapcsoló veszi a keretet D-től
  - bejegyzi a táblába, hogy D a 2-es interfészen érhető el
  - mivel C benne van a táblában, továbbítja a keretet az 1-es interfészre (csak oda)
- C veszi a keretet

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Bridging fajtái

- **Transzparens (vagy tanuló) bridging:** előző példában bemutatott
  - pl. Ethernetnél

- **Forrás által vezérelt bridging + transzparens**
  - A küldött csomag fejlécében fel vannak sorolva az útvonal bridge-i és szegmensei, amit érinteni kell
  - Vezérjeles gyűrűnél használatos

  - Első küldés esetén:
    - **Broadcast csomag** minden irányban, feljegyzik az útvonalat sorban, visszaküldik
    - Ahány lehetséges útvonal, annyi csomag jön vissza, pl. **legrövidebbet** választja
    - **Maximális hopszám** után eldobás (hurok elkerülése)
    - **Forgalom kiegyenlítés**: leterhelt eszközök nem vesznek részt benne

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Különbség bridging és routing között

- Bridging:
  - Adatkapcsolati rétegben MAC címek alapján
  - Nem tud különbséget tenni hálózatok között
  - Elárasztást használ: csak helyi hálózatokban

- Routing:
  - Hálózati rétegben, IP címek alapján
  - Skálázhatóbb megoldás
  - Erről lesz szó a továbbiakban!

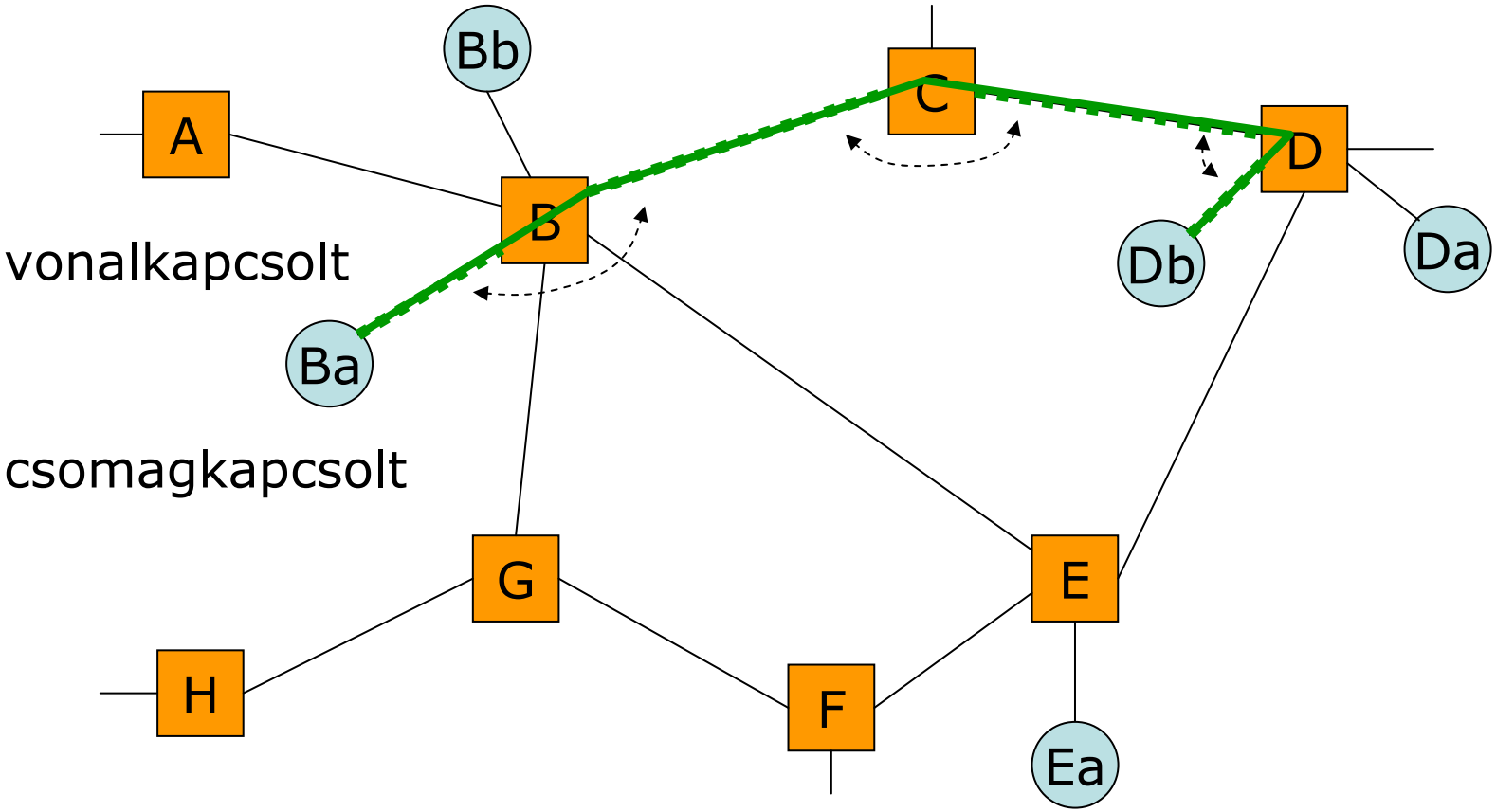
© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mi tehát a feladat?

- **Megismerni, nyilvántartani** a hálózat felépítését:
  - csomópontok
  - összekötések (link)
  - lehetséges útvonalak

- **Összeköttetés-alapú eset:**
  - Csomópontokban felhalmozott ismeretek alapján
    - az útvonal kiválasztása lépésről-lépésre
    - **feljegyzése** az érintett csomópontokban
    - értesítés a kommunikáló végekhez, hogy elkészült az útvonal, megkezdhető a kommunikáció.
- **Összeköttetés-mentes**:
  - nincs külön útvonalkialakítás előre
  - a csomópontok a megfelelő útvonalat a csomag továbbításával **egyidejűleg** választják meg

Összeköttetés-alapú /-mentes



Mi tehát a feladat?

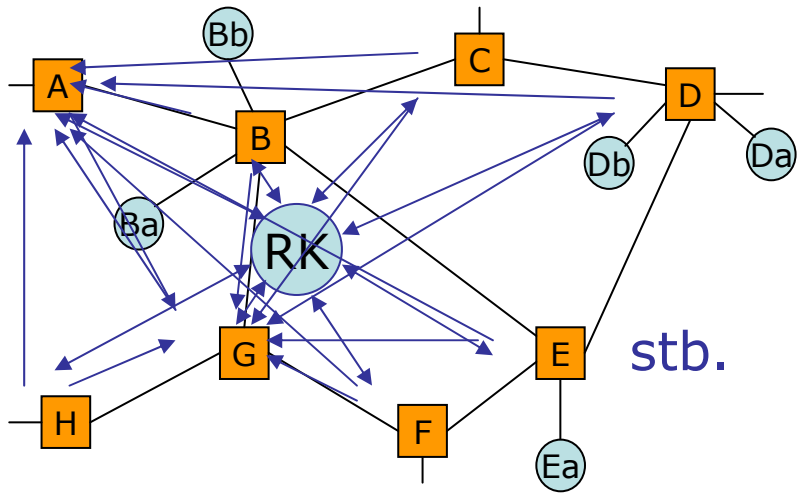
- **Áramkörkapcsolt eset:**
  - állandó átviteli csatorna létrehozása az összeköttetés időtartamára
- **Összeköttetés-alapú eset**
  - virtuális csatorna létrehozása a csomópontokban történt feljegyzésekkel
    - honnan hová kell tenni a csomagot
- **Összeköttetés-mentes eset:**
  - a csomópontok minden egyes csomagra újból elvégzik az útválasztást
  - nincsenek állandó feljegyzéseik
- *Utóbbi esettel foglalkozunk, a teljesség kedvéért megemlítve az előző kettőt*
- Mi kell az útválasztáshoz?
  - A hálózat felépítésének (csomópontjainak és linkjeinek) megismerése és nyilvántartása
  - Ezen ismeretek biztosítása a csomópontok számára

Útvonaltáblák

- Útvonalkijelölés ill. útvonalválasztás:
  - a csomópontok táblázatai alapján

Cél-végpont	következő csomópont
…	…

- A táblák kitöltése:
  - manuálisan
  - automatikusan:
    - centralizáltan
    - elosztottan



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Centralizált **kontra** *elosztott* **módszer**

- **Centralizált:**
  - egy ponton összegyűjtjük a hálózatról megszerezhető valamennyi ismeretet
  - meghatározzuk az egyes csomópontok útvonaltábláinak bejegyzéseit
  - továbbítjuk azokat a csomópontokhoz.

- **Elosztott esetben**
  - valamennyi csomópont egyénileg gyűjt információt a hálózatról
  - saját útvonaltábláját készíti el

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Centralizált előnyei-hátrányai

+

- egyetlen kép a hálózatról, minden útvonal-tábla „**konzisztens**” lesz
  - De nem valós helyzetre!

-

- nagy hálózatnál közben megváltozhat az állapota
- sérülékenység *(„single point of failure”)*
  - Megoldás lehet: tartalékolás

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Elosztott **előnyei-hátrányai**

+

- Kevésbé sérülékeny

-

- Nincs egységes kép a hálózatról
- Eltérő „nézőpontok” a csomópontokban

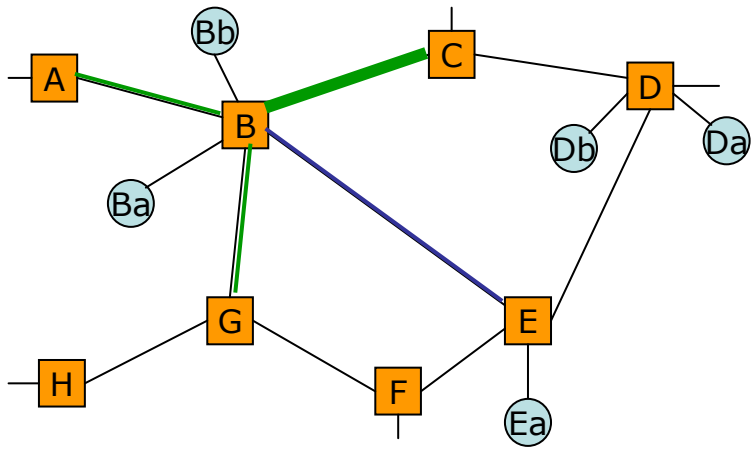
Az útvonal-adatbázis kialakítása

- **Statikus routing**
  - Előre becsült forgalmi viszonyok alapján útvonaltáblák centralizált kialakítása és szétosztása
  - A hagyományos telefonhálózatokra alkalmazható
    - mivel itt a forgalom jól előrejelezhető
    - a hálózat amúgy is központilag menedzselt
- **Dinamikus, adaptív routing**
  - Az aktuális forgalmi helyzet állandó figyelése és az annak legjobban megfelelő útvonaltáblák kialakítása
  - Adathálózatokra jellemző
    - az Internet esetén elosztott változatban
    - a forgalom nem jósolható jól előre
    - nincs egységes hálózatfelügyelet

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A gyűjthető információ

- Csomópontok közötti összekötések, linkek:
  - pl.: *B-A, B-C, B-E, B-G*
    - nem működik: pl.: *B-E*
    - *B->Ba,->Bb*
- Linkek jellemzői:
  - *átv. seb., pl.*
    - *B-A:* 2 Mbit/s
    - *B-C:* 10 Mbit/s
    - *B-E:* 2 Mbit/ s
  - *Forgalom (sorhossz):*
    - *B-A:* 2
    - *B-C:* 0
  - *Terhelés %-ban*
  - *Kiszolgálási díj*



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Információ -> routingtáblák

- Ha a hálózat valamennyi csomópontjáról megvan az információ: meghatározható, hogy **bármely két felhasználót milyen útvonalon célszerű összekötni**.

- Célszerű: pl. legrövidebb

- A célszerű utakból
  - **kiolvashatjuk az egyes csomópontok által kialakítandó útvonal darabot**
  - meghatározhatjuk az **útvonaltáblákat**, amelyek bejegyzései lényegében útvonaldarabokat képviselnek.

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A routing módszerrel szembeni követelmények

- ***Minél kisebb méretű útvonaltábla:***
  - Kisebb tár, olcsóbb csomópont
  - Gyorsabb keresés a táblában, gyorsabban működő csomópont
  - Kisebb routingforgalom

- ***Robosztusság:***
  - Hibás tábla esélyének minimalizálása, mert a hibás tábla okozhat:
    - „fekete lyukat”
    - hurkot
    - oszcillációt

- ***Optimális útvonalak kijelölése:***
  - az út optimalitása az igénytől függő, lehet optimális a
    - legrövidebb *(miben mérjük?)*
    - legmegbízhatóbb
    - legolcsóbb

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

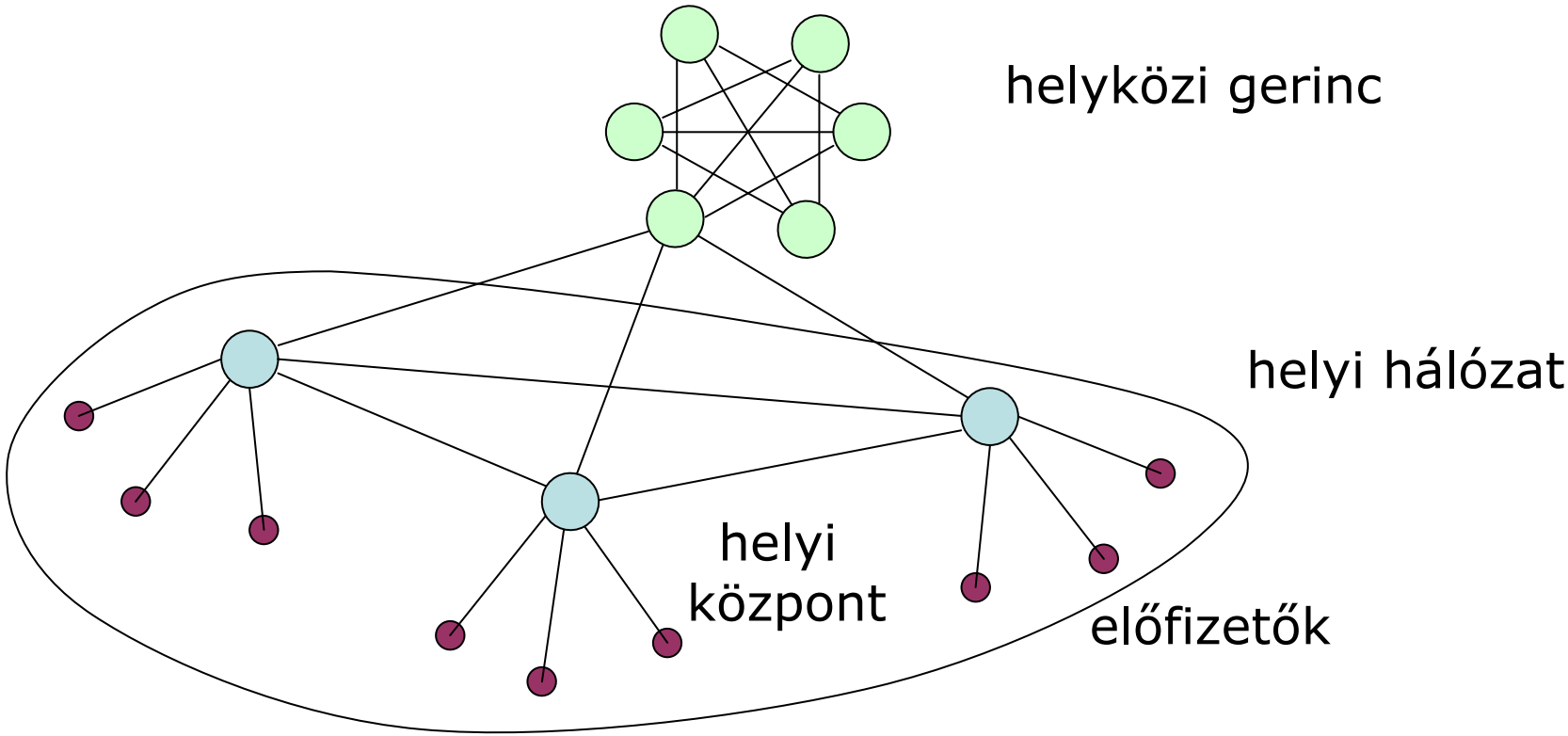
A megoldások csoportosítása

- Centralizált
- Tényleges forgalomtól függő
- Egyutas
- Lépésenkénti
- *Elosztott*
- *Forgalomfüggetlen*
- *Többutas*
- *Forrás általi*

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Routing a telefonhálózatokban

- A telefonhálózat leegyszerűsített struktúrája



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Routing a telefonhálózatokban: a blokkolás minimalizálása

- **Útvonalkijelölés**
  - helyi hívások: nincs útvonal
  - a helyi központok szintjén közvetlen útvonal, vagy kétlépéses egy helyközin keresztül
  - távolsági hívás
    - mindkét helyi központ ugyanahhoz a távolságihoz van bekötve
    - másik távolsági központon keresztül

- **Az alkalmazott routing:**
  - centralizált táblakitöltés, a becsült forgalom függvényében
  - két útvonal a távolsági központ számára:
    - közvetlen a hívott távolsági központjával
    - közvetett utak
      - **tartaléknak, ha a közvetlen út trönkvonalai foglaltak**, ezért a hívást blokkolni kellene

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Routing a számítógép-hálózatokban

- „Routing az összekötöttség – **connectivity** – **maximalizálására**”: katonai célok eleinte!

- Legyen a módszer **elosztott**!
  - Az útvonaltáblák kialakítását végezzék maguk a csomópontok

- Két alapvető módszer:
  - „distance-vector” – *Bellman-Ford algoritmus*
  - „link-state” – *Dijkstra algoritmus*
- A módszerek különböznek abban, hogy:
  - milyen információt gyűjtenek
  - hogyan gyűjtik az információt
  - hogyan terítik ezt később

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A módszerek lényege

- Információgyűjtés, és -terítés történik
- „Kinek, mit mondunk?”:
  - „Távolságvektor” módszer (*distance-vector*):

  A csomópontok elmondják a **hálózatról alkotott *elképzeléseiket* a szomszédaiknak**
  - „Linkállapot” módszer (*link-state*):

  A csomópontok elmondják **mindenkinek a szomszédaikról nyert *tapasztalataikat***

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A „távolságvektor” módszer

- A gyűjtött információ és a gyűjtés módja:
  A csomópontok elmondják a hálózatról alkotott elképzeléseiket a szomszédaiknak

- Az „elképzelések”:
  - melyik csomópont milyen távol van
  - egy lista (vektor) melynek elemei
    - csomópontazonosító – távolság párok

- A távolságvektorát közli mindegyik csomópont valamennyi szomszédjával
- A távolság mérése?

A „távolságvektor” módszer: a távolság mérése

- Legegyszerűbb esetben ez lehet *a **lépések** (ugrások, hop-ok) száma*

- Súlyozás:
  - *a link átviteli sebességével*
  - *a sorbanállási hosszal*
  - *a költséggel*

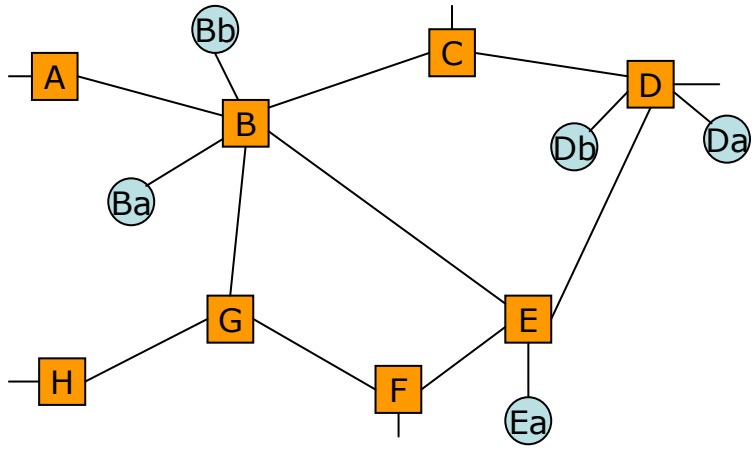
- *Szóhasználat: távolság = költség*
- Így a távolságvektor elemei az adott csomópont által elképzelt költségek a hálózat többi (ismert) csomópontjához

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A Bellman – Ford algoritmus (1)

- Példa:

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



B-hez megérkezik *C* üzenete:

B	A,1	C,1	D,2	E,1	G,1	∞
C	B,1	D,1				

B-hez megérkezik *E* üzenete:

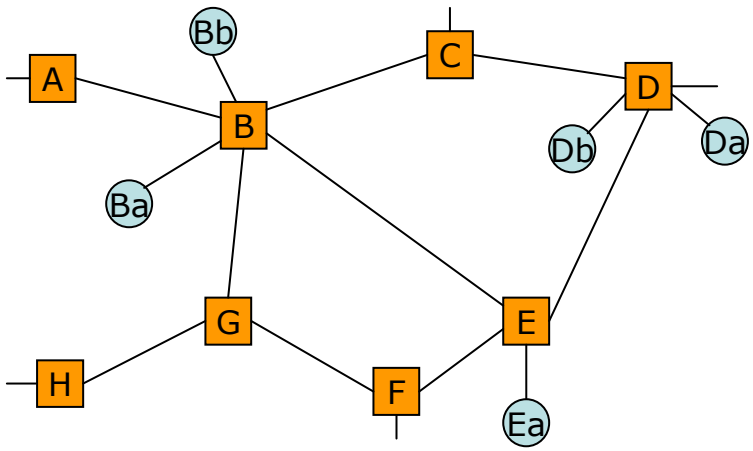
B	A,1	C,1	D,2	E,1	F,2	G,1	∞
E	B,1	D,1	F,1				

(∞ - a hálózat még nem látott része)

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A Bellman – Ford algoritmus (2)

- Ha a csomópont a beérkező üzenetből kideríti, hogy rövidebb útra van lehetőség, akkor végrehajt egy cserét a vektorban.
- Példa: *D* üzenete eljutott *E*-hez, majd *F*-hez, majd *G*-hez, és innen *B*-hez.
  - *F* táblázatába bekerült *D* két lépéssel,
  - *G* táblázatába így *D* már 3 lépéssel szerepel,
  - ezért *B* úgy látja, hogy *D* a *G*-n keresztül 4 lépéssel érhető el.
- Ha ezután érkezik hozzá *E* vagy *C* üzenete, amelyekben *D* egy lépéssel szerepel, akkor nyilván lecseréli a bejegyzést, mert 2 < 4.
- Bebizonyítható, hogy a fenti algoritmus konvergens, de vannak tranziensei

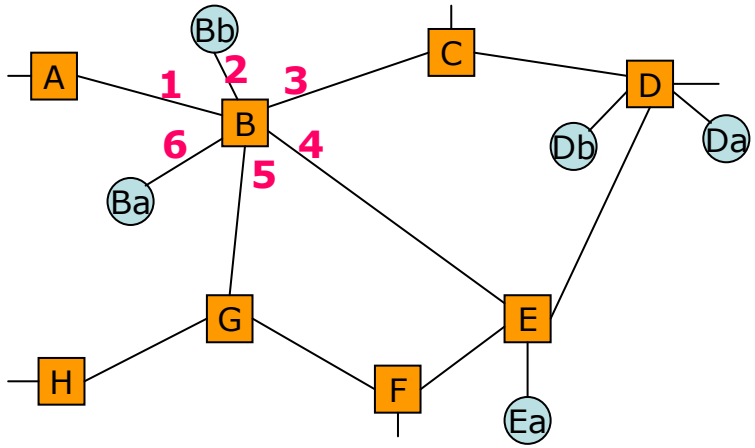


© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az útvonaltábla kialakítása a távolságvektor alapján

- Például:
  - *B* távolságvektora

B	A,1	C,1	D,2	E,1	F,2	G,1	∞



  - Sorszámoztuk *B* portjait
  - Kitölthetjük *B* útvonaltábláját:

Ba	6	közvetlen
Bb	2	közvetlen
Da	3	
Db	3	
Ea	4	

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

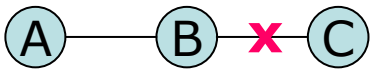
A távolságvektor módszer alapproblémája (1)

- **A végtelenig számolás**
  - meghibásodások léphetnek fel
  - a csomópontok tévesen korrigálhatják távolságvektorukat
    - nem tudják, hogy a kapott távolságvektorokat a szomszédaik milyen módon, lépésekkel hozták létre
      - ‘routing by rumor’
  - egyre növelik egy adott csomóponthoz való távolságukat
    - elvileg végtelenig
    - konkrét megvalósításoknál véges számig

- Következmény: egymásnak irányítják az el nem érhető csomóponthoz tartó forgalmat, ezzel túlterhelnek linkeket

A távolságvektor módszer alapproblémája (2)

- Példa a *végtelenig számolásra*:



- A *B*-*C* link megszakad
- *B* kijavítja a bejegyzését
- *B* és *A* kicserélik elképzeléseiket és korrigálnak:
- Ha ismét cserélnek és korrigálnak:

	C táv	Köv. lépés
A	2	B
B	1	C

A	2	B
B	∞	-

A	∞	-
B	3	A

A	4	B
B	∞	-

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A távolságvektor módszer javítási lehetőségei

- Split horizon: megtiltja a csomópont számára az útvonal hirdetését azon interfész felé, ahonnan tanulta
- Route poisoning: hirdeti a csomópont, hogy elérhetetlen az útvonal, törölni kell a táblákból
  - Pl. ha maximális hopszám 15, 16-ra állítja
- Kettőt együtt alkalmazzák
- Holddown timer: amikor értesül a csomópont, hogy elérhetetlen egy útvonal, indít egy időzítőt
  - amíg le nem jár, nem foglalkozik azon útvonal hirdetményeivel
  - vagy megjavul ez idő alatt az útvonal, vagy új útvonalat keres
- Növekszik a konvergencia idő, további komplexitás!

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

További problémák

- Nem jól skálázódik
  - Ezért tipikusan egy területen belül használják (később lesz róla szó)
  - Pl. egy ISP hálózatán belül
- A hálózati topológia változását nem elég gyorsan követi
  - Mivel a frissítések csomópontról csomópontra terjednek

A „linkállapot” módszer

- A gyűjtött információ és a gyűjtés módja:
  A csomópontok elmondják **mindenkinek a szomszédaikról nyert tapasztalataikat**

- A „tapasztalatok”:
  - a **szomszédokhoz vezető linkek aktuális állapota**: ez pontosan ismerhető!
  - a link költsége valamilyen mérték szerint

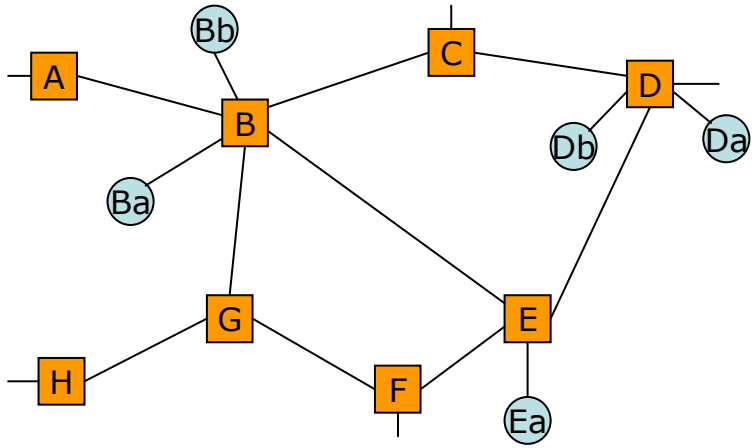
- Az **információ elküldése mindenkinek *„elárasztással”*:**
  - elküldik a szomszédokhoz, amelyek továbbadják (kivéve azon a linken, amelyen érkezett)

- *A linkállapot-információk alapján a legrövidebb utak kiválasztása*

A küldött információ és „védelme”

- Például: a *B* csomópont

B	A	1
B	C	1
B	E	2
B	G	1
B	Ba	0
B	Bb	0



- Védelem a téves információ ellen:
  - **sorszám és életkor**, növelés/csökkentés
  - régi bejegyzések elévülése
- Védelem a hibák és rosszakarat ellen:
  - hibavédő kódolás és autentikáció (hitelesítés), jelszavas azonosítással
- Hogyan történik a linkállapotok alapján az utak kiszámítása?
  A Dijkstra-algoritmussal

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

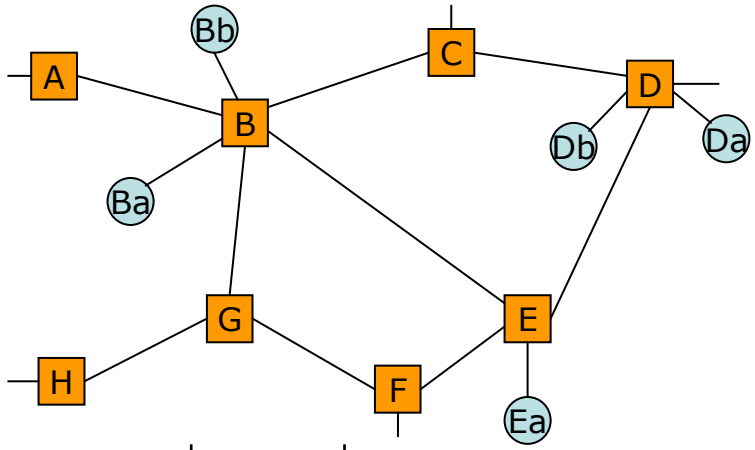
A Dijkstra algoritmus

- Példa: *B* csomópont

  - *P* és *T* halmazok

B	C(B,1) E(B,2)
	D(C,2) ~~D~~**(E,3)**

  - Ha *T* halmaz üres, akkor vége van



C	B	2
C	D	1

D	C	2
D	E	1

E	B	2
E	D	1
E	F	1

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Magyarázat a Dijkstra-algoritmus illusztrációjához

- *P* (permanent) és *T* (temporary) halmazok nyilvántartása az adott csomópontban.
- Induláskor csak **B** van a *P*-ben.
- *T*-be betesszük az ismert szomszédainkat.
- Akkor teszünk be egy szomszédot *T*-be
  - ha még nincs ott
  - vagy ott van, de kisebb költséggel is elérhető, ekkor lecseréljük.
- *T*-ből a legkisebb költségűt átvisszük *P*-be, ha még nincs ott.
- Ha *T* kiürül, készen vagyunk

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Távolságvektor vs. Linkállapot

- Távolságvektor alapú protokollok:
  - Rosszabbul skálázódnak
  - Lassabb konvergencia
  - Hopszámban adják meg a költséget, nem veszik figyelembe az egyéb paramétereket
    - pl. linkkapacitás
  - Kisebb hálózatokban használják őket

  - Manapság a linkállapot alapú módszerek dominálnak tartományon belüli routing esetén

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Routing tábla metrikák

- A metrika az adott routing algoritmustól függ
  - Linkkapacitás
  - Késleltetés
  - Hopszám
  - Megbízhatóság
  - Csomagvesztési ráta
  - MTU stb. kombinációja

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A hierarchikus routing

- Kiterjeszthetőek („skálázhatóak”) a routing-algoritmusok egyszintű (flat) hálózat esetén?
- *N* csomópontja és *E* linkje esetén kimutatható:
  - A legrövidebb út számítása: $O(E \log E)$
  - Az útvonaltábla mérete: $O(N)$
  - Nem lehet hierarchia nélkül egy Világháló:

# csomópont	Táblahely	Számítási idő
1	1	$O(0)$
1.000	1.000	$O(3.000)$
1.000.000	1.000.000	$O(6.000.000)$
100.000.000	100.000.000	$O(800.000.000)$
10.000.000.000	10.000.000.000	$O(100$ milliárd$)$

Az autonóm rendszerek

- Megoldás: a hálózat szegmentálása

- ***Autonóm rendszerek*** kialakítása
  - *önállóan oldanak meg routingfeladatokat*
  - *a külvilág felé egyetlen elérési pontként szerepelnek*

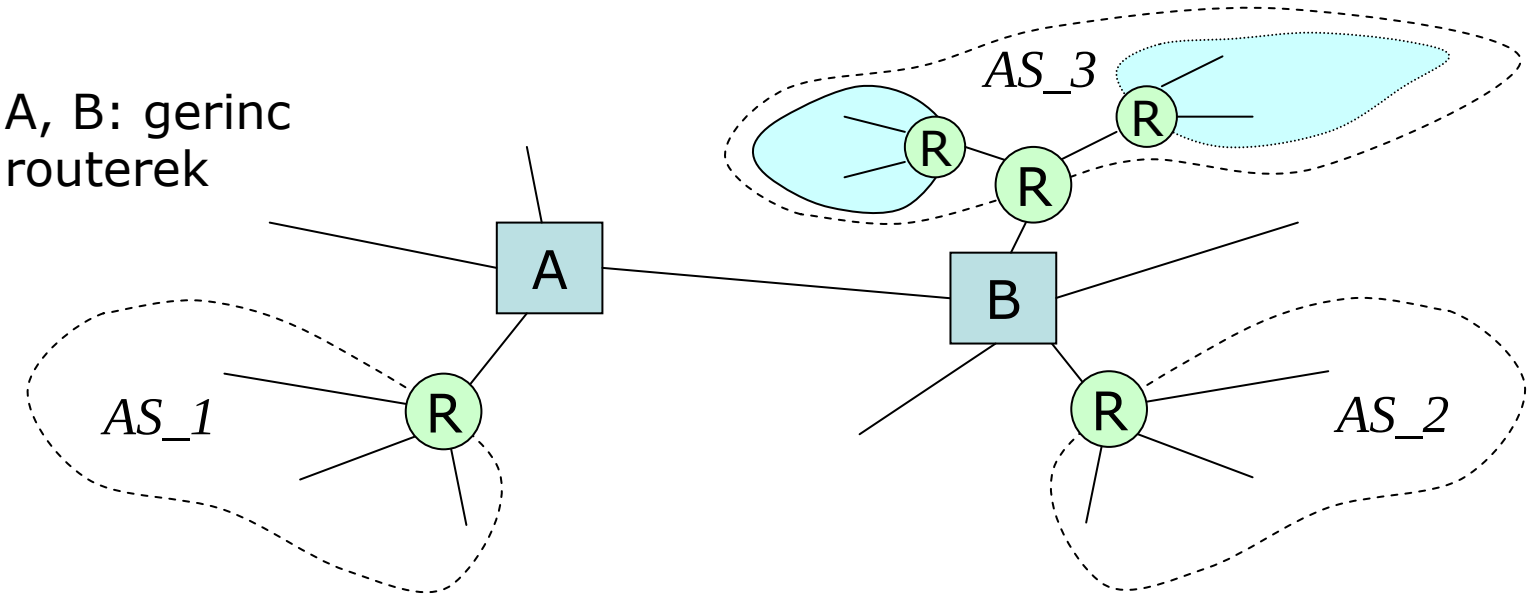
- Az autonóm rendszer (AS)
  - olyan egység, amelyen belül **egységes routing policy** érvényesül
  - egyetlen hálózat, vagy hálózatok csoportja
  - közös hálózatadminisztrátor kezeli
  - egyetlen szervezeti egység (pl. egyetem, üzleti vállalkozás) megbízásából
- Gyakran **routing-domain**-nek is nevezzük
- Globálisan egyedi azonosító: **ASN (Autonomous System Number),** a IANA-tól

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Autonóm rendszerek

- Egy autonóm rendszer a többi autonóm rendszer számára képviseli az általa képviselt csoporto(ka)t
  - az ún. **határ-routereken** keresztül érhető el

- Az egész csoport **egyetlen bejegyzés** lesz az útvonaltáblákban



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

AS típusok

- Multihomed AS
  - Több mint egy AS-el van összekötve
  - Meghibásodás esetén sem lesz elvágva
  - Viszont nem enged átmenő forgalmat más AS-ek között
- Stub (csonk) AS
  - Csak egy másik AS-el van összekötve
    - Gyakorlatban többel is van peering, csak nem nyilvános
- Tranzit AS
  - Csak átmenő forgalmat szolgálnak ki
  - Összes ISP ilyen

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

AS-k közötti útvonalválasztás

- Multihomed és tranzit AS esetén több útvonal közül választhat más AS-ek felé
- Sok esetben nem a linkkapacitás vagy késleltetés számít, hanem az üzleti kapcsolatok a szomszédos AS-el

- Hot-potato (forró krumpli) elv:
  - minél rövidebb legyen az út a saját AS-én belül
  - annak ellenére, hogy lehet összeségében így hosszabb lesz az út
- Cold-potato:
  - minél hosszabb ideig a saját hálózatán belül akarja tartani a forgalmat, szinte a felhasználóig
  - szolgáltatás minőségi garanciákat nyújthat

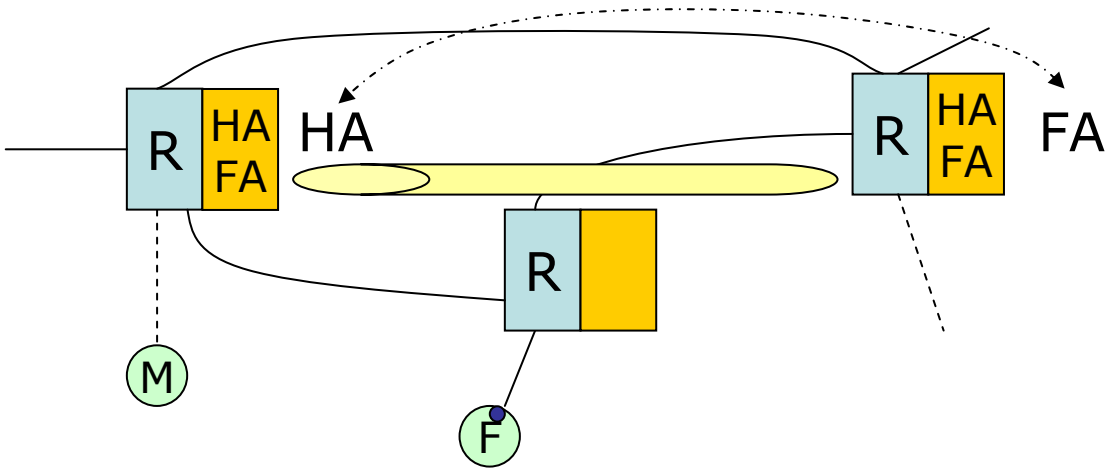
Mobil végpontok kezelése

- Eddig: egy végpontot a csomóponthoz való kapcsolata definiálja
  - pl. Ba, Bb: a B csomóponthoz kapcsolódó végpontok
- A végpontok átmozoghatnak más csomópont környezetébe, más autonóm rendszerbe
  - mozgás: vándorló (nomádikus) végpont, mobil végpont
- A többi végpont csak a mozgó csomópont eredeti (pl. Ba) címét ismeri
  - jó lenne, ha nem is kellene tudnia, hol van aktuálisan Ba
- Ezért a hálózatnak kell kezelnie Ba mozgását – ez a mobil routing feladata

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Konkrét megvalósítás az IP protokollnál: mobil IP (lásd később)

- Elv: „kiegészítések” a csomópontokon:
  - Mobil ügynök:
    - Home agent = hazai ügynök
    - Foreign agent = idegen ügynök



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Multicast routing

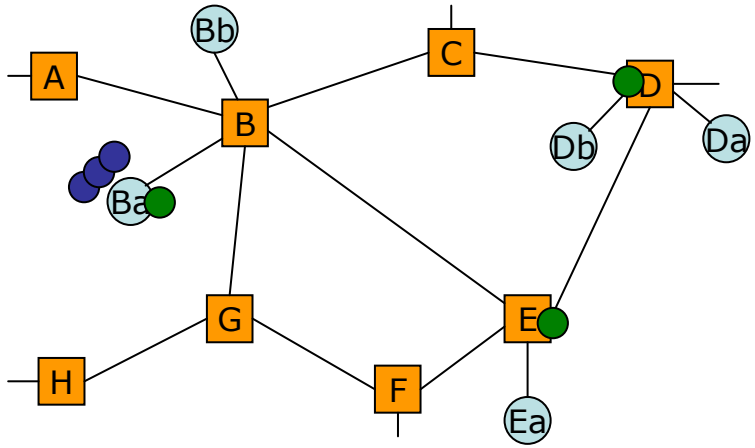
- Egy másik érdekes járulékos feladat az alap routinghoz képest: ***multicast routing***
- Nem egyetlen végponthoz/címre kell eljuttatni a csomagokat, hanem egyidejűleg többre
  - a gyakorlatban: adat-beszéd-videókonferencia
- *Elnevezés:*
  - *broadcast - (műsor)szórás mintájára, mindenkinek a hálózaton*
  - *multicast: egy csoportnak*
  - *anycast: egy valakinek a csoportból (pl. aki a legközelebb van a forráshoz)*
  - *unicast: egy adott végpontnak*

- Magyarul: *többesadás*

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A multicast routing: példa és megoldandó feladatok

- Példa:
  - *Ba* -> *Da, Db* és *Ea*
    - Három unicast
    - Multicast



- Megoldandó feladatok:
  - Címzés
  - Csoportkezelés
  - Útválasztás segítése

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A többescímzés, csoportazonosítás

- Azonosítsuk a csoportot!

- A hálózat végpontjait azonosítják a
  - Fizikai címeik
  - Logikai címeik
    - ezt tartják a csomópontok nyilván az útvonaltábláikban
- A csoport azonosítására használhatnánk a csoport tagjainak címlistáját is...
- Jobb: a csoportot **egy**, az egyedi logikai címhez hasonló **azonosító** különbözteti meg: **csoport-cím**!
- A csoport létezésének feltétele: legalább egy aktív információforrása legyen

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Multicast routing, módszerek

- A csoport résztvevői a hálózatban:
  - Sűrű elhelyezkedés:
    - Elárasztás + lemondás (flood-and-prune)
      - Legrövidebb útvonalfa alkalmazása
      - Csoportlemondás
      - Forráslemondás
  - Ritka elhelyezkedés:
    - Explicit csatlakozás
      - Gerincalapú fa alkalmazása (Core Based Tree)
- Elhelyezkedés-független
  - A kettő ötvözete

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás

- Routing:
  - **Az a mechanizmus, mely segítségével a szállítandó információ a megfelelő úton kerül továbbításra a végpontok között**
  - szűkebb ételemben: az a folyamat, amelynek eredményeként a csomópontokban létrejönnek az útvonaltáblák

- Két fő módszer és két algoritmus az útvonaltáblák létrehozására:
  - Távolságvektor (distance-vector) – Bellman-Ford
  - Linkállapot (link-state) - Dijkstra

- Kiegészítések szükségesek:
  - Mobilitás biztosítására
  - Pont-multipont, multipont-multipont kommunikáció esetén

- A routingot megvalósító *protokollokat* később tárgyaljuk

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

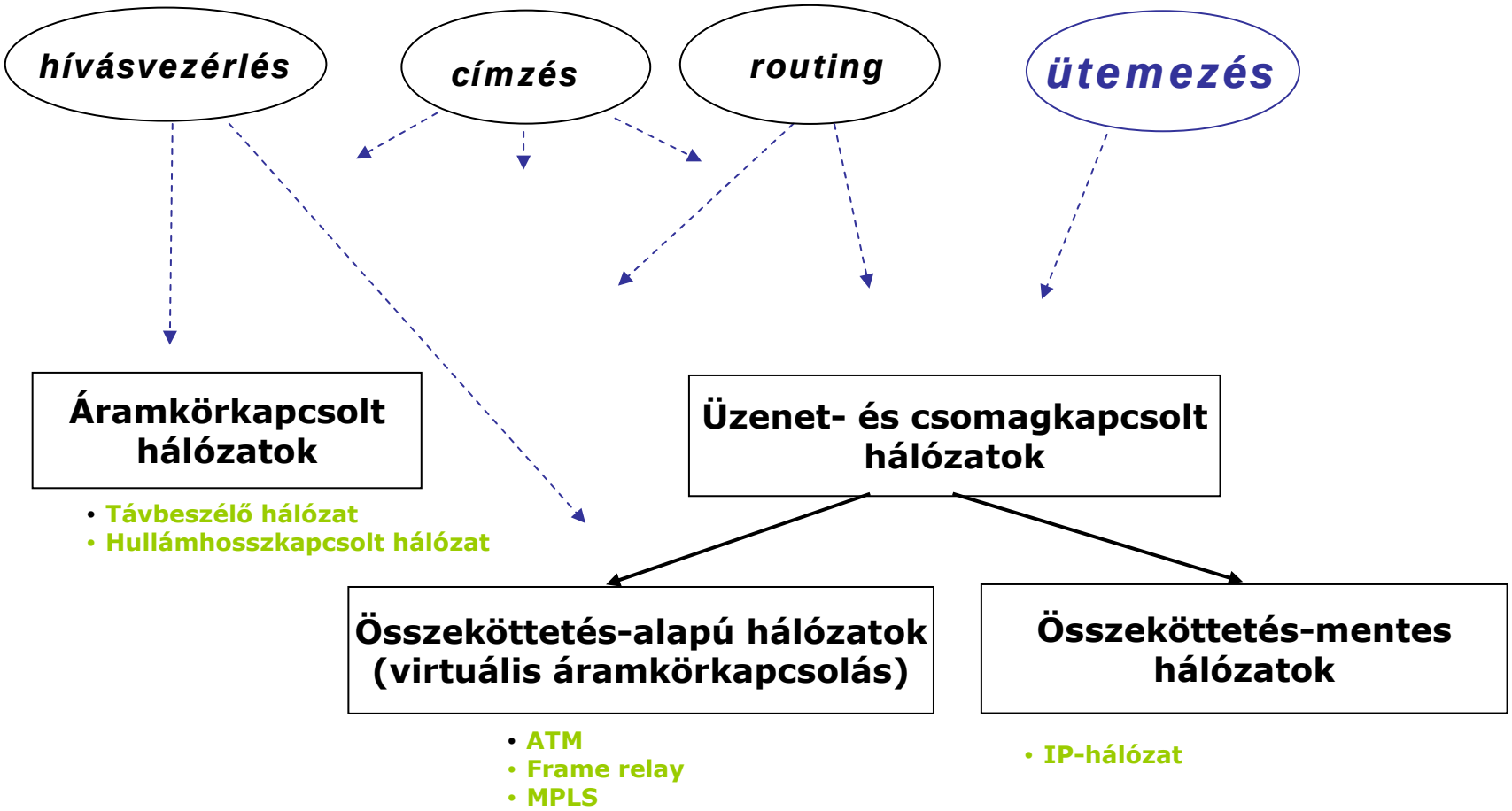
FELADATÜTEMEZÉS, CSOMAGKEZELÉS

Scheduling

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013. március 27.

További nagyon fontos funkció a kapcsolt hálózatok működtetéséhez



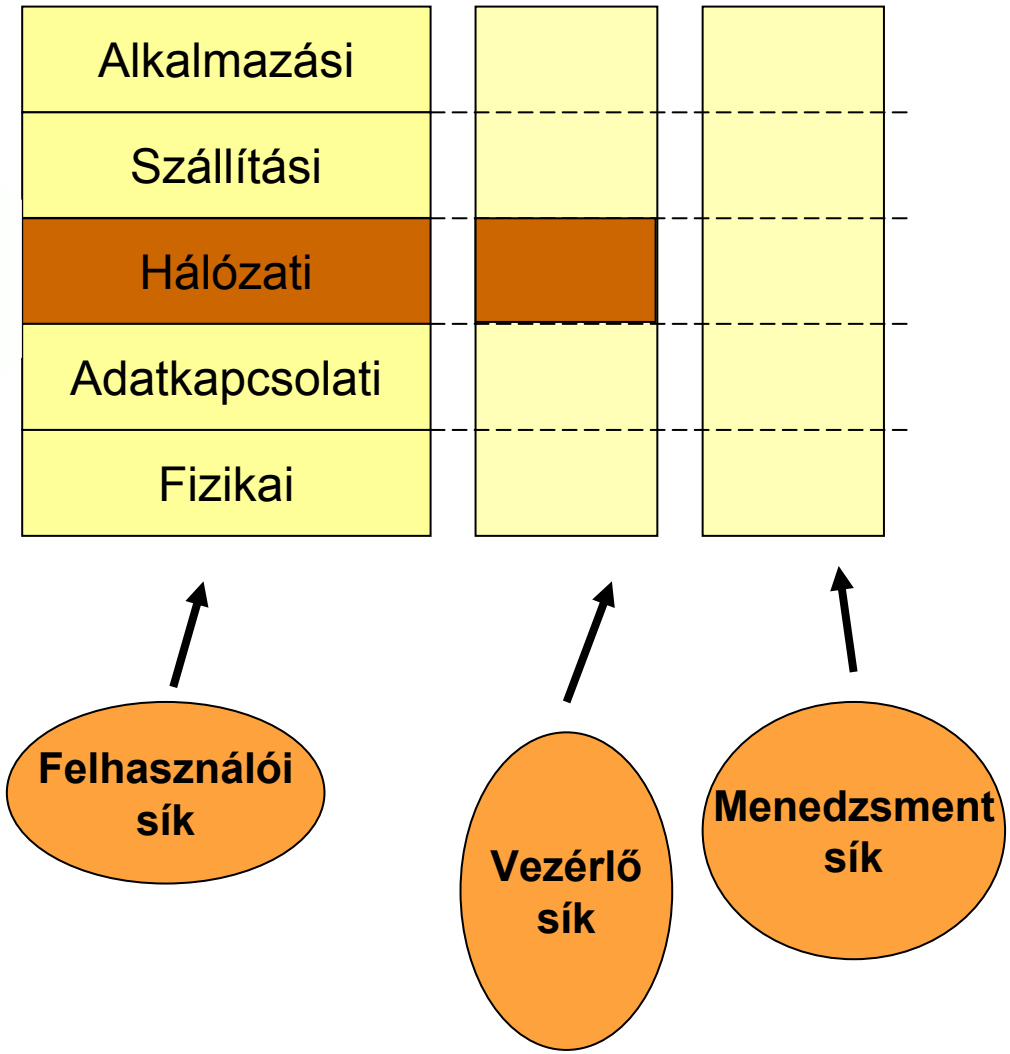
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Elv:

Ütemezés (packet scheduling)

Módszerek:

GPS
Weighted round robin
Deficit round robin
WFQ



Meg kell jegyezni, hogy cross-layer megoldásai is vannak!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mi az, hogy „scheduling”, ütemezés?

- Több területen is megjelenő problémára megoldás
- **Véges erőforrás:**
  - **időnként nagyobb mértékben kellene igénybe venni**, mint amekkorára az képes
  - máskor viszont nincs eléggé leterhelve
  - **Ha igaz, hogy hosszú idejű átlagban képes az igények kiszolgálására: ütemezés!**

    *(ha nem akkor **erőforrás bővítés** kell)*
- Időnként tehát **várakozni kell** az erőforrásra
  - Milyen **elvek, stratégiák alapján** képezzünk sort, sorokat a várakozókból, ahhoz, hogy
  - **adott kiszolgálási feltételek, elvárások** a lehető legjobban teljesüljenek

Scheduling a hálózatokban

- Csomagkezelés a hálózat csomópontjaiban
  - **Csomag jön → cél-cím → csomag megy**

- Véges erőforrások:
  - **A linkek átviteli képessége**
  - **A csomópontok tárolási képessége**
    - **tárolás, sorbaállítás, átrendezés**
  - **A csomópontok feldolgozási képessége**

- Jól van méretezve az a hálózat, amelynél ez előfordul?
  - nagyszámú igény adja össze a teljes igénybevételt
  - általában kiegyenlítik egymást
  - eltekintve kilógó esetekről, amelyekre jó becslést lehet adni, ez a
  - **statisztikus multiplexelés**
- és így jobban járunk, mintha a csúcsra méreteznénk ez a
  - **statisztikus nyereség**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Miről lesz szó ebben a részben?

- *Bevezetés*
- *Követelmények*
- *Lehetőségek*
- *A „best effort” kiszolgálás ütemezői*
- *Ütemezés garantált kiszolgálás esetén*
- *Csomageldobás*

Bevezetés

- **Verseny** az osztott használatú erőforrásokért
  - Miért verseny, miért nem FCFS (**f**irst-**c**ome-**f**irst-**s**erved)?

- Feladatütemezési módszer kell:
  - Az **igazságos megosztáshoz**
    - lehet egyenlő, de nem feltétlenül az egyenlősdi az igazságos
  - A **kiszolgálási minőség** garantálásához
    - különböző típusú forgalomnak különböző elvárásai vannak

- A módszer két független összetevője:

  - **Kiszolgálási sorrend meghatározása - késleltetés**
  - **Kiszolgálásra várakozók túlcsordulásánál igényeldobási „stratégia” - vesztési arány**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Miről van szó tehát, amikor ütemezésről beszélünk hálózatokban?

- A hálózatokban osztott:
  - az átviteli képesség
  - a csomópontok tárolói
- A feladatütemezés helye:
  - a csomópontok tárolóiban
- A forgalom statisztikus ingadozását kezeljük az ütemezéssel

Miért van szükség (nem triviális) ütemezésre?

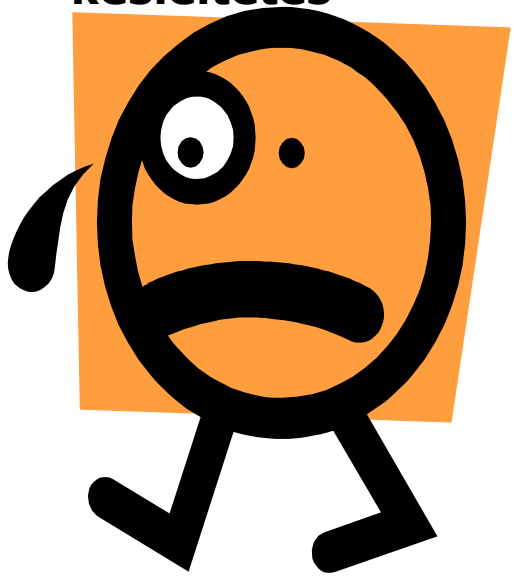
- **Legalább** kétféle alkalmazást kell kiszolgálni
  - ***Rugalmas (elasztikus) vagy késleltetéstűrő alkalmazások***
    - *elviselik a véges és változó ábocsátóképességet (pl. file-átvitel)*
    - igazságos megosztás
    - *„best effort" igény* (~ legjobb szándékú)
  - ***Merev, vagy intoleráns alkalmazások***
    - *garantált szolgáltatást igényelnek*
      - *pl. a beszéd állandó 64 kbit/s-os csatornát*
    - korlát a késleltetésre, garantált átviteli sebesség, korlát a vesztési arányra
    - *garantált szolgáltatású igény*

Megőrzési törvény (Conservation Law)

- Triviális ütemezés: FCFS
- de mindenfajtára igaz, hogy:
  az átlagos késleltetések forgalom részaránnyal súlyozott összege = konstans
- *Valakinek előnyt csak mások rovására lehet biztosítani*
- Bármely ***munkamegőrző* (work-conserving)** ütemező csak ugyanazt az összeget osztogathatja
- „Szorgalmas” vs. „Lusta” ütemező

$$\sum_{i=1}^{N} \rho_i \cdot q_i = \text{konstans}$$

forgalom-részarány **átlagos késleltetés**



Alapvető követelmények

- Egyszerű megvalósíthatóság
- „Best effort” kiszolgálásnál:
  - **Igazságosság (fairness)** biztosítása
  - **Védelem (protection)** biztosítása
- Garantált kiszolgálásnál:
  - **Teljesítménykorlátok (performance bounds)** biztosítása
  - Egyszerű és hatékony **beengedés-szabályozás (admission control)**

Egyszerű megvalósíthatóság

- Nagysebességű hálózat → gyakori csomagtovábbítás
- Csomagonként csak néhány műveletre van lehetőség
- Ha *N* a kiszolgálandó igények száma:
  - a csomagonkénti feldolgozási időigény **ne exponenciálisan**, hanem **lineárisan** nőjön *N* függvényében
- Elsődleges korlát az állapotok nyilvántartása (pl. pointer a sorban):
  - az ehhez szükséges memória és
  - elérési idő

Igazságosság és védelem

- Erőforrás elosztás *igazságos* legyen:
  - A részesedés **a költségviselés arányában** történjen
- Amennyiben valaki megkísérel **jogosulatlan előnyhöz** jutni, legyen megakadályozva ebben → *védelem* a többieknek

Igazságosság és védelem

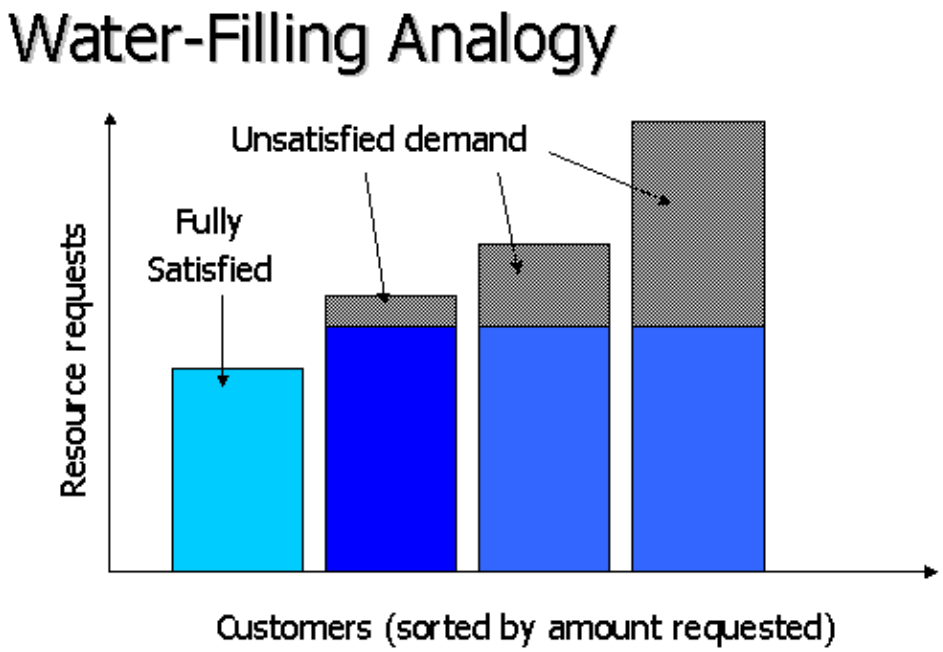
- Gyakori eset: egyenlő jogosultságok, de vannak, amelyek igénye kisebb a többiekénél
  - logikus, hogy a „kis” felhasználóknak adjuk oda, amennyit akarnak
  - a fennmaradót igazságosan a nagyok között
- Ez a max-min igazságos megosztás elve:
  - Erőforrás-kiosztás az igények növekedése szerint
  - Senki sem kap többet a kértnél
  - A kielégítetlen igények egyenlően osztoznak a maradékon
- Ezt formalizálva, kapjuk a **max-min algoritmust**

Példa max-min algoritmusra

- 4 forrás: 2; 2,6; 4; 5 igényekkel
- 10 kapacitású erőforrással.
  - **1. lépés: mindenki 2,5.**
  - **a 0,5-öt egyenlően elosztjuk a 3 között, ez ~2,66-ot ad**
  - **a ~0,06-ot a 2 között,**
  - **végül az 1-es 2-t, a 2-es 2,6-ot, a 3-as és 4-es ~2,7-et kap**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Max-min szemléltetése



Eltérő jogosultságok: súlyozott max-min megosztás

- Például 15 egységnyi erőforrásra 5 pályázó

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

- Jogosultságaik aránya
- Igényeik:
- Normalizált súlyok:
- Az E kivételével mindenki elégedetlen:
- Szétosztjuk súlyaik arányában, D is OK:

1,3+2,6+3,9+5,2+2=15
+0,2

Ez még szétosztható

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Igazságosság és átbocsátóképesség

- Eljárások hol nem teljesül az igazságosság (fairness):
  - Néha magas átbocsátóképesség
  - De instabil szolgáltatásminőség
    - Felhasználók viselkedésének függvényében
  - Ha gyakran instabil: elégedetlen felhasználók

Max-min előnyei

- Összehasonlítva az egyenlő felosztással:
  - Jobb erőforráskihasználtság
    - mivel egyenlő felosztás esetén nem használjuk az egyes felhasználók maradékát
- Egyéb előnyök:
  - „Rosszul” viselkedő (nagy méretű csomagok vagy börsztös átvitel) felhasználók magukat büntetik, nem mást
- Ezt az elvet használja (lásd később):
  - Round robin
  - Far Queuing

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Maximális átbocsátóképességű ütemezés

- **Maximum throughput scheduling**
- Prioritás azon folyamok számára, amelyek a „legolcsóbbak” a hálózat szempontjából
  - „Legolcsóbb”: legkisebb hálózati erőforrás/átvitt információ
  - Pl. rádiós hálózatoknál: prioritás az alacsony csillapítású felhasználóknak (magas SNR)
    - „Drága” felhasználó: távol van a bázisállomástól
- Költségfüggvényt számol, pl. csillapítást felhasználókhoz
- Legjobb erőforrás kihasználás, de !

Gondok a maximális átbocsátóképességű ütemezéssel

- Többi felhasználó folyamának meg kell várni míg a „legolcsóbbak” kiszolgálásra kerülnek
  - **Éheztetés (starvation)**

- Hiába ad jobb erőforrás kihasználást mint a max-min, nem teljesül a fairness elv
  - Elégedetlen felhasználók
  - Szolgáltató profitja ettől is függ

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Proportional fair

- Kompromisszum a max-min és maximális átbocs.ü. között
- Előnye van az „olcsóbb” folyamoknak, de „drágábbak” is kapnak egy adott kiszolgálási szintet
- Minden felhasználóhoz egy prioritási szint
  - Fordítottan arányos a várható erőforrás használatukkal
  - Pl. Weighted Far Queuing (lásd később)

„Merev” alkalmazások: teljesítménykorlátok biztosítása

- Teljesítmény, teljesítőképesség - *performance*
- Akár felhasználónkénti kiszolgálási **teljesítménykorlát garantálása**
  - a megőrzési törvényen belül
- Szerződés: felhasználó ↔ szolgáltató
- Egyrészt kiszolgálási garancia, másrészt használati kötelezettségvállalás
- Garancia nem csak egyetlen ütemezőre, hanem elvileg az egész hálózatra
  - **végpontok közötti garancia, igen nehéz feladat**
  - **mivel ütemezés csomópontokon**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Teljesítménykorlátok fajtái

- Determinisztikus:
  - Az összeköttetés valamennyi csomagjára teljesülnie kell

  Egyszerű ellenőrzés, de rossz kihasználtság

- Statisztikus:
  - A csomagok adott hányadára teljesül
  - *N* egymás utáni csomagból egyre nem teljesül

  Bonyolult ellenőrzés, de jó kihasználtság

Gyakran használt teljesítménykorlátok (teljesítőképesség-jellemzők, QoS-paraméterek)

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

Egyszerű és hatékony beengedésszabályozás

- A teljesítménykorlátok (QoS paraméterek) csak **beengedésszabályozás (admission control)** alkalmazásával biztosíthatók
- Gyorsan kell eldönteni, hogy újabb igény még kiszolgálható-e
- Nem eredményezheti azt, hogy a hálózat nem lesz kihasználva a lehetséges mértékben
- Például FCFS esetén
  - Legnagyobb késleltetésre garancia:
    - Létszámkorlát és limitált börszt-méret

    Kis kihasználtság!

Miről volt szó eddig és mi következik?

- *Bevezetés*
  - *fogalmak, a megőrzési törvény*
- *Követelmények*
  - *megvalósíthatóság*
  - *igazságosság*
  - *teljesítménykorlátok, beengedésszabályozás*
- *Lehetőségek*
  - *prioritások...*
- *A „best effort” kiszolgálás ütemezői*
  - *GPS elv*
  - *Round-robin, súlyozott round-robin*
  - *Weighted Fair Queueing*
- *Ütemezés garantált kiszolgálás esetén*
- *Csomageldobási stratégiák*

Alapvető választási lehetőségek az ütemezés tervezésénél

- Négy alapvető szabadsági fokunk van a tervezésnél
  - Prioritási szintek száma (A)
  - Az egyes szinteken
    - munkamegőrző (work-conserving) vagy nem munkamegőrző (non-work-conserving) módot használjunk-e? (B)
  - Igények csoportosítási (aggregálási) mértéke az egyes szinteken belül (C)
  - Kiszolgálási sorrend az egyes szinteken belül (D)

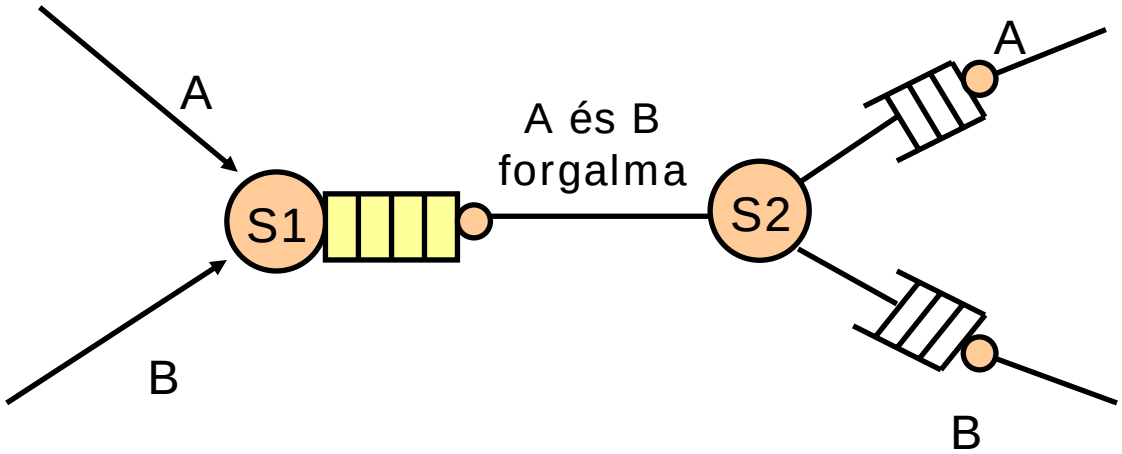
(A) Prioritás

- *n* szint esetén a *k*-adik szintű igényt akkor elégíti ki csak az ütemező, ha nincs kiszolgálásra váró igény a *k+1, k+2, …, n* szinteken
- Magasabb prioritási szint = kisebb késleltetés
- Egyszerű a megvalósítása
- Jól számolható a teljesítőképessége
- Probléma: minden áron előnyben részesítés, a magasabb szintű igény **„kiéhezteti”** az alacsonyabb szintűeket
- Megoldás: megfelelő beengedésszabályozás
- **Gyakorlatban: max. 3 prioritási szint**

(B) Work-conserving és non-work-conserving kiszolgálás („szorgalmas” vagy „lusta” kiszolgáló)

- **Work-conserving**: csak akkor tétlen a kiszolgáló, ha nincs várakozó igény (csomag)
- **Non-work-conserving**: vannak tétlen időszakai akkor is, ha van várakozó igény
- Miért jöhet egyáltalán szóba a „lusta”?
- A kivárás előnyös lehet a forgalmi jellemzőkre
- Csak az „esedékessé” váló csomagokat továbbítjuk
  - Csökken a tároló iránti igény
  - Csökken a késleltetés ingadozás
  - Egyszerűsödik a vállalható teljesítménykorlát meghatározása
  - De nagyobb teljes késleltetés

Példa: amikor a nem munkamegőrző kiszolgálás hasznos lehet



- „A” beérkezési folyamata az S2 kimeneti pufferébe attól is függ, milyen „B” viselkedése az S1-nél
- „B” forgalma feltartóztathatja „A” csomagjait, így amikor azok végre elhagyják S1-et, csomósodva érkeznek meg az S2 kimenetére

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Nem-munkamegőrző kiszolgáló

- Az esedékessé válás időpontjainak meghatározása
  - pl. a „rate descriptor” alapján
- Szükség van-e ilyen kiszolgálóra?
  - Viszonylag új technika, egy évtizeddel ezelőtt még kutatási kérdés volt
  - Értékelés:
    - csökkenti a *késleltetés ingadozást* az átlagos késleltetés megnövelése árán és a *kapcsolók tárigényét*
    - **korrekt forgalomjellemzést** kíván meg a forrásoktól, és azt, hogy **ahhoz tartsák is magukat**

Nem-munkamegőrző kiszolgáló alkalmazása

- Csomagformázás (packet shaping):
  - Korlátozza a folyam „kijátszásának” rátáját a kimenő interfészre
  - Pl. multimédia forgalom esetén néha nem éri meg siettetni a továbítást
    - Hang nem lesz előbb kijátszva, mint ahogy felvették
- Gyakorlatban nem alkalmazzák
- Lehetséges ötvözni a munkamegőrzővel
  - Munkamegőrző használja a kapacitását ameddig a nem-munkamegőrző szünetel

Hol tartottunk: tervezési lehetőségek

- Négy alapvető szabadsági fokunk van a tervezésnél
  - Prioritási szintek száma (A)
  - Az egyes szinteken
    - munkamegőrző (work-conserving) vagy nem munkamegőrző (non-work-conserving) módot használjunk-e? (B)
  - Igények csoportosítási (aggregálási) mértéke az egyes szinteken belül (C)
  - Kiszolgálási sorrend az egyes szinteken belül (D)

(C) Igények csoportosítása

- Összeköttetések összevonása (aggregation) és közös kezelése
- Két véglet:
  - **valamennyi igény együttes jellemzése** – ugyanazt a szolgáltatásminőséget kapják
  - **minden egyes összeköttetésre saját QoS** biztosítása
- Csomagkapcsolt hálózaton technikailag nem lehet erőforrással győzni az egyedi igények kezelését
  - szemben a telefonhálózattal, ahol azonosak az igények
  - mindenekelőtt a kapcsolók ütemezői által kezelt állapotváltozók mennyisége a kritikus
    - ha összeköttetésenkénti, akkor megengedhetetlenül nagy lehet

Igények csoportosítása: osztályba sorolás

- Közbenső eset: osztályokba sorolás
  - az adott osztályba sorolt összeköttetések ugyanazt a szolgáltatásminőséget kapják
- Nincsenek védve egymástól
  - mivel ütemező nem tud különbséget tenni az osztály összeköttetései között, ha egy megsérti a „szerződést”, mindenki rosszabb kiszolgálást kap → **kiszolgáltatottság**
- Torlódás kezelése
  - mivel ..., ha egy csoporttag okozza is a torlódást, mindegyik jelzést kap, hogy fogja vissza magát
- Jó lenne megoldani, hogy csak az értelmezze, amelyik okozta

(D) Kiszolgálási sorrend (prioritási szinten és csoporton belül)

- Érkezési sorrendben történő kiszolgálás (FCFS) ↔ érkezéstől eltérő sorrendű kiszolgálás
- A FCFS hátrányai:
  - Nem engedi meg a kivételt, pl. késleltetés érzékeny összeköttetések csomagja számára
  - Nem biztosít védelmet, nem *max-min* elvű
  - Erőszakosságra ösztönöz

- A nem-FCFS ütemező előnyös, de bonyolult
  - Meg kell határozni, és jelezni a sorrendet (tagging)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A „best effort” kiszolgálás ütemezői

- Általánosított processzormegosztás (GPS) - elmélet
- Súlyozott „round-robin” – innentől gyak. közelítések
- „Deficit round-robin”
- A WFQ – weighted fair queueing *vagy*
  PGPS – Packet-by-packet GPS
  ~ súlyozott igazságos sorképzés ill.
  csomagonkénti GPS

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A GPS (Generalized Processor Sharing) elve

- A **max-min** igazságosság megvalósítása
- Egy **alapelv** kimondása csupán: úgy lehetne igazságosan megosztani az erőforrást, ha sorban mindenkinek egy 0-hoz tartóan kicsiny elemi „szeletét” végeznénk el a feladatából
- **Elvileg megoldjuk** a GPS-szel az igazságos kiszolgálás problémáját, de mit lehet tenni **a gyakorlatban**?
- **A GPS közelítéseit** alkalmazhatjuk, és a GPS-hez viszonyíthatjuk azok tulajdonságait

A GPS

- Mintha mindegyik csomag **külön logikai sorban** lenne
- Mindenki **egymás után kap egy parányi kiszolgálást**, majd **„körben”** folytatódik
- Akinek nincs igénye az kimarad
- Különböző jogosultságok esetén a nullához tartóan kis kiszolgálás a súlyok arányában különböző lesz
- Kimutatható, hogy a GPS max-min értelemben **fair kiszolgálást** nyújt
- A GPS egy **absztrakció**
- A kérdés: mennyire közelíti egy valóságos ütemező a GPS-t?

Súlyozott körbekérdezés (Weighted round-robin)

- A round-robin a GPS legegyszerűbb közelítése
- Jó, ha azonos csomaghosszak és azonos súlyú összeköttetések
- Kiszolgálás körben **csomagonként,**
  - különböző súlyokkal,
  - különböző csomaghosszakkal

Hátrányai

- Átlagos csomaghossz jó közelítésű ismerete kell
  - IP hálózatokban ez nem könnyű, változó csomagméretek!
- *Rövid időszakra nagyon igazságtalan lehet*

Példa súlyozott körbekérdezésre

- Pl. három összeköttetés:
  A, B, C
- átlagos csomaghosszak:
  50, 500, 1500 byte
- súlyok: 0,5:0,75:1
- Hány csomagot/byte-ot szolgáljunk ki az egyes összeköttetésekből egy körben?
- súly/csomaghossz:
  1/100; 3/2000; 1/1500
- normalizált súly/csomaghossz:
  60, 9, 4
  (3000, 4500, 6000 byte)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

„Deficit round-robin”

- Előre ismeretlen átlagos csomaghosszra
- Definiálunk
  - egy ***kiszolgálási adagot***, *kvantumot* (byte-okban mérve)
  - egy ***számlálót***, amely a felhasználó „hitelét” számolja
- A sor elején álló csomagot akkor szolgáljuk ki, ha az nem hosszabb, mint az adag
  - ha hosszabb, az adagot hozzáadjuk a számlálóhoz
  - és a következő körben ennek vizsgálata alapján döntünk

Példa deficit round robinra

- *Példa:*

		A	B	C
Kiszolgálási adag: 100				
Csomaghossz:		*150*	*80*	*120*
Hitelszámláló:	*1. kör*	*100*	*20*	*100*
	2. kör	*50*	*0*	*80*

- *1. kör: B (marad 20 hitele), A és C kimarad*
- *2. kör: A és C, mert*
  megmaradó hitel: hitel + adag – csomaghossz

- *akinek nincs igénye, az elveszti a hitelt*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A WFQ (Weighted Fair Queueing)

- Alapötlet: kiszámítjuk (szimuláljuk) a csomagok távozási időpontjait, mintha GPS szerint szolgáltuk volna ki azokat, és ezt a sorrendet alkalmazzuk a kiszolgálásra
- Nem a távozási időpont, hanem a sorrend érdekes
  - **ezért a távozást jellemző értéket így *befejezési számnak* (*finish number*) nevezik**
- (Legyen bitenkénti kiszolgálás)
- **Ciklusszám** (***round number***) – pozitív nem egész szám
  - az aktív felhasználók számának reciprokával arányos
- **Ciklushossz:** arányos az aktív felhasználók számával
- Ha ismerjük a ciklusszámot, a **befejezési szám** kiszámolható:
- $F(i,k,t) = \max[F(i,k-1,t),R(t)]+P(i,k,t)$
  - $F(i,k,t)$ – az ***i***-edik felhasználó befejezési száma ***t*** időpontban
  - $P(i,k,t)$ – az ***i***-edik felh. ***t***-ben beérkező ***k***-adik csomagjának hossza
  - $R(t)$ – ciklusszám a ***t***-ben

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hogy jön ki a WFQ összefüggés?

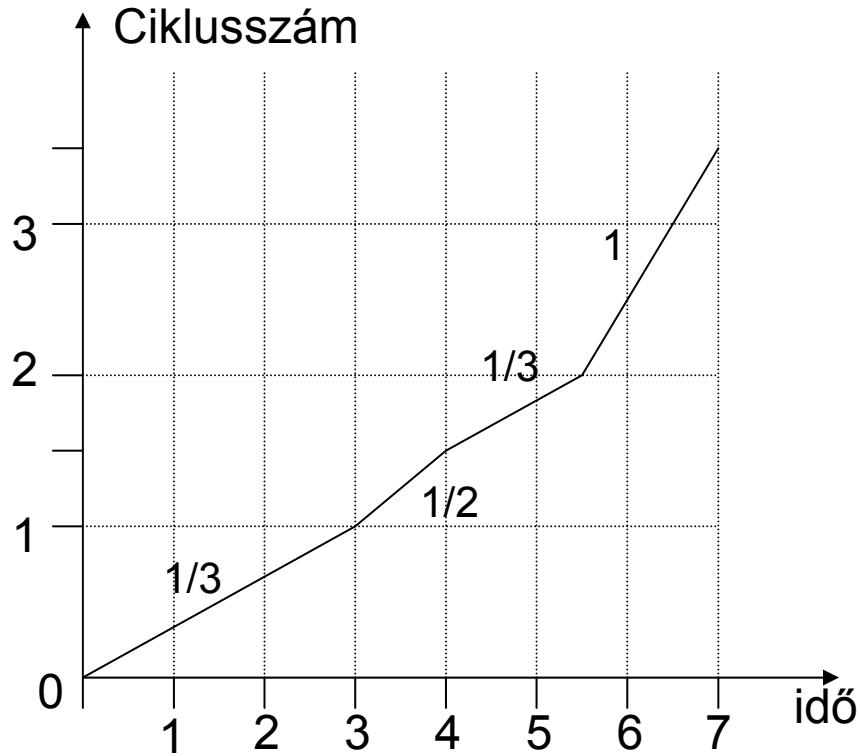
- *Inaktív* felhasználónál a befejezési szám:
  - az aktuális ciklusszám plusz a csomagméret
  - pl. ha egy 10 bites csomag érkezik, amikor a ciklusszám 3, a kiszolgálása akkor befejeződik be, amikor a ciklusszám 13 lesz

- *Aktív* felhasználó csomagja beérkezésekor annak befejezési száma:
  - a sorában lévő csomagok közül a legnagyobb befejezési számú plusz a csomagméret
  - pl. ha a 10 bites csomag beérkezésekor a sorban van egy 20-as befejezési számú, akkor 30 lesz
- Kombinálva ezt a két állítást:

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

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

- A, B, C, 1; 2; 2 a csomaghosszak t=0-ban és A még generál egy 2 hosszút t=4-ben
- Kiszolgálás: 1 csomageység/időegység
- $R(0)=0$
- $F(A,1,0) = \max[F(A,0,0),R(0)]+ P(A,1,0)=\max[0,0]+1=1$
- $F(B,1,0) = F(C,1,0) = 2$
- *A* első csomagjával kezdjük
- majd B vagy C, ami t=3-ban fejeződik be
- a harmadikat t=3-ban kezdjük és 5-ben fejeződik be
- t=4-ben *A* második csomagja
- *A* második csomag finish no-hoz kell tudnunk a round no-t, t=4-ben
- A görbe menetéből...



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A WFQ értékelése

- Súlyozott esetben a befejezési szám:

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

- Az aktuális ciklusszám meghatározása jelent gondot:

  egy kieső (kiszolgált) felhasználó megváltoztatja a ciklus-szám változási sebességét → felgyorsul a kiszolgálás → „láncreakció” következik/-het be

- Egyre általánosabb a használata a korszerű routerekben

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csomageldobás

- Nem csak a kiszolgálási sorrendről, hanem a tárolhatatlan csomagok kezeléséről is dönteni kell
  - csomageldobás
- Milyen alapon működjön a csomageldobási stratégia?
  - Csoportosítás (aggregálás): összeköttetésenként, vagy csoportonként
- Eldobási prioritások
  - Előbb dobja el az alacsony prioritású csomagokat
- Korai eldobási stratégiák
  - Early Random Drop
  - Random Early Detection

Early Random Drop és Random Early Detection

- Korai véletlen eldobás
  - Sorhossz nagyobb, mint *eldobási küszöb* →
    - azonos és állandó valószínűségű eldobás
- Véletlen korai detektálás
  - küszöb az átlagsorhosszra
    - börsztökre nem érzékeny
  - az eldobás valószínűsége arányos a sorhosszal
  - nem-kooperatív felhasználók csomagjainak jelölése

Miről volt szó a scheduling részben?

- *Bevezetés*
  - *fogalmak, a megőrzési törvény*
- *Követelmények*
  - *megvalósíthatóság*
  - *igazságosság*
  - *teljesítménykorlátok, beengedésszabályozás*
- *Lehetőségek*
  - *prioritások...*
- *A „best effort” kiszolgálás ütemezői*
  - *GPS elv*
  - *Round-robin, súlyozott round-robin*
  - *Weighted Fair Queueing*
- *Ütemezés garantált kiszolgálás esetén*
- *Csomageldobási stratégiák*

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

IP – Internet Protocol

IP címzés, routing, IPv6, IP mobilitás

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.Április 4.

IP - Áttekintés

- Bevezetés
  - A TCP/IP protokollarchitektúra
  - Az IP feladata és jellemzői
- Címzés
- Az IP csomag szerkezete
- Routing
- IP segédprotokollok
- IPv6
- Mobil IP megoldások

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

IP – Bevezetés

Az IP, mint hálózati protokoll

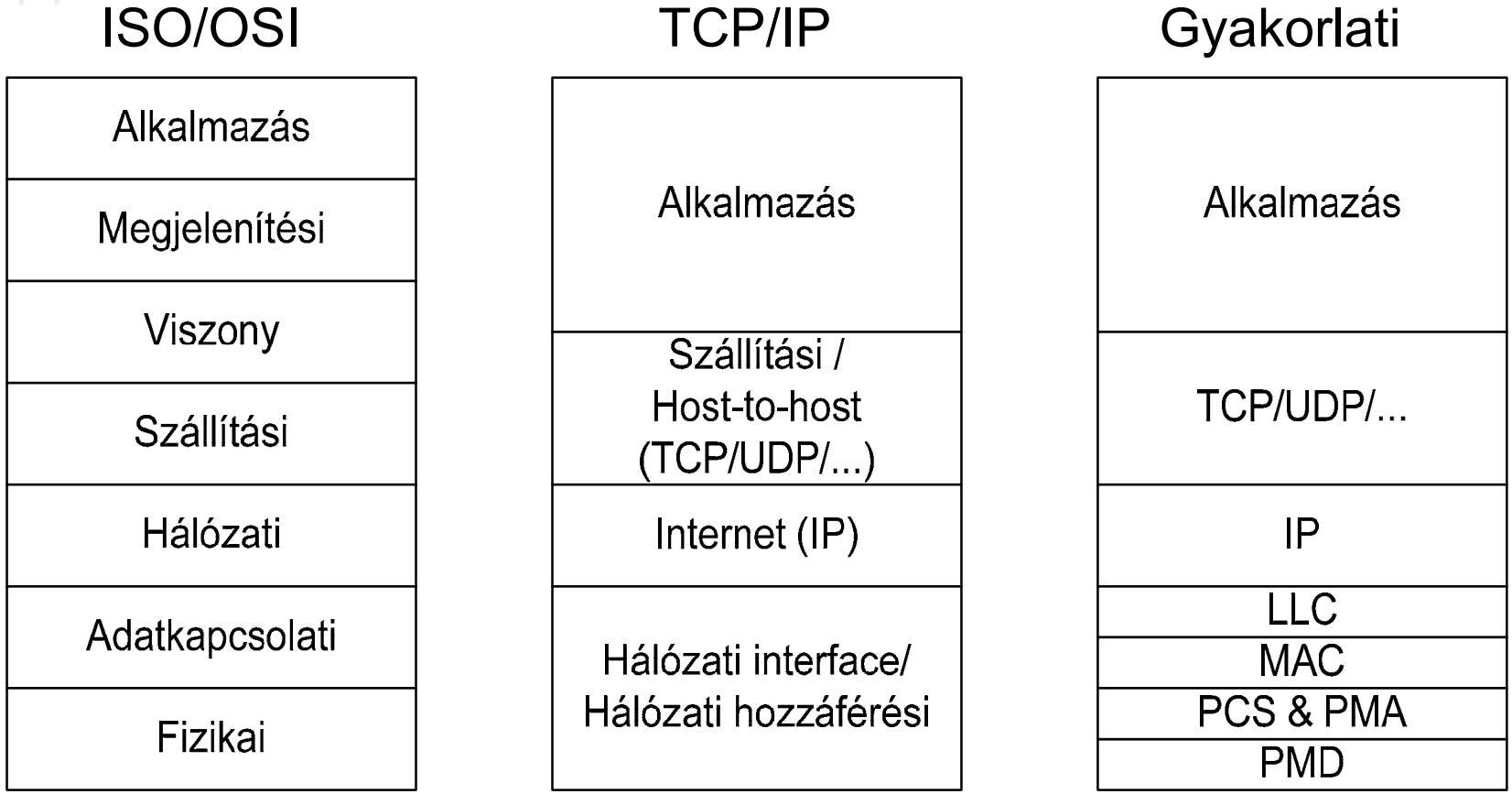
2013.Április 4.

Az Internet és az IP rövid története

- 1969 – ARPANET, „az Internet őse”
- 1974 – Az IP és a TCP alapgondolata
  - Protokollarchitektúra az NCP kiváltására az ARPANET-en
  - „A Protocol for Packet Network Interconnection” (Vinton G. Cerf, Robert E. Kahn)
  - Az „Internet” kifejezés megjelenése (Internet Protocol Suite)
- 1980 – IPv4 (Internet Protocol version 4)
  - Az első, széles körben használt IP és TCP verziók megalkotása
  - DoD (Department of Defense) által támogatott szabványok: IP (RFC 760), TCP (RFC 761)
  - 1983. január 1: Flag day, NCP → TCP/IP
- Alapvetően ma is ezt használjuk!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

TCP/IP architektúra és az ISO/OSI rétegmodell



IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
LLC: Logical Link Control

MAC: Medium Access Control
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

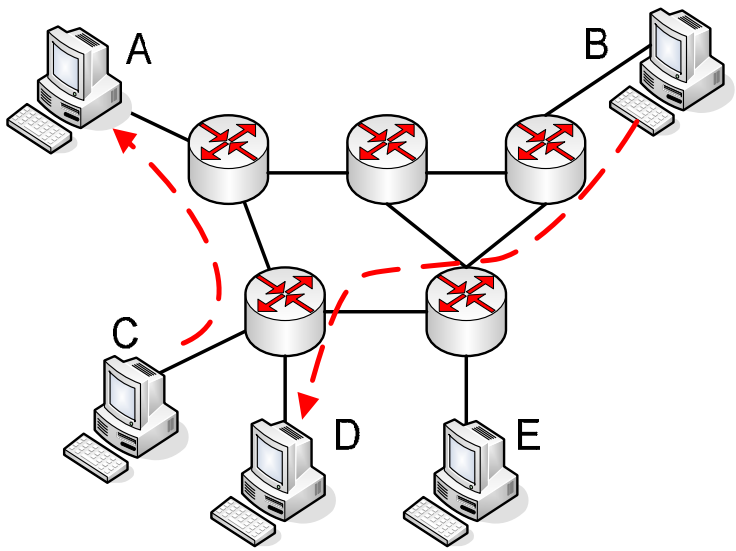
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ISO OSI vs. IETF

- OSI 7 rétegét a gyakorlatban nem szokták megvalósítani
- IETF szerint: Internet protokolljainak és architektúrájának fejlesztése továbbra sem lesz OSI alapú!
- Nálunk: 5 réteg, TCP/IP modell használata, de
  - interface réteg= adatkapcsolati réteg + fizikai réteg

Az IP feladata

- Hálózati protokoll
  - Adattovábbítás a hálózat végpontjai között
- Két fő funkció
  - **Címzés (addressing) és útvonalválasztás (routing)**
  - Tördelés/fragmentálás (fragmentation)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IP jellemzői

- Csomagkapcsolt
- Összeköttetés-mentes (connectionless)
- „Best effort” – nincs garancia

} Datagram típusú

  - A csomagokra igaz:
    - Elveszhetnek
    - Duplikálódhatnak
    - Sorrendjük megváltozhat
    - Meghibásodhatnak (nincs hibaészlelés és -javítás)
- Egyéb **NEM** nyújtott szolgáltatások:
  - Torlódáskezelés
  - Ütemezés
  - Titkosítás és hitelesítés

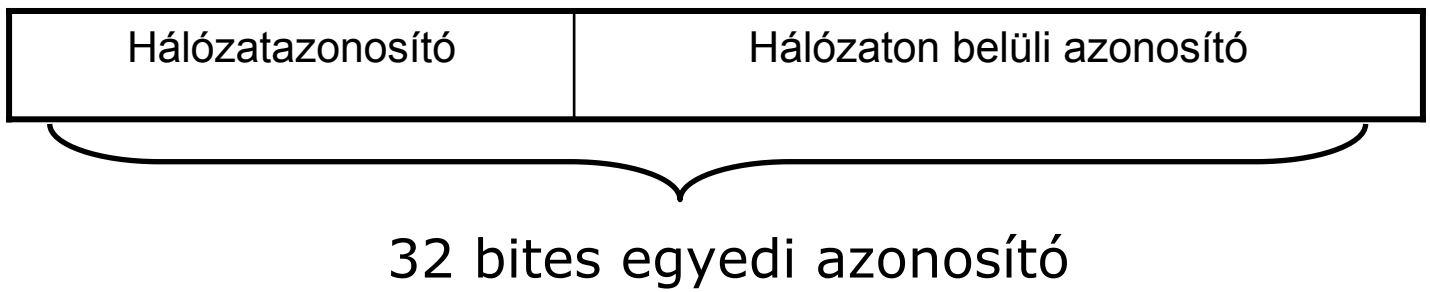
IP – Címzés

IP-címek és címosztályok

2013.Április 4.

Az IPv4-cím felépítése

- 4 bájtos cím (32 bit)
  - $2^{32} \approx 4 \cdot 10^9$ ⇨ kimerült!
- Jelölések
  - Bináris: 10110000 10010011 00111110 11100001
  - „Dotted decimal”: 176.147.62.225
- Cím = Hálózatazonosító + Egyedi azonosító



Címosztályok

- Eleinte első 8 bit hálózati, majd bevezették a címosztályokat (1981)
- Különböző méretű hálózatoknak más méretű IP-cím tartományok

Osztály	Hálózatazonosító bitjeinek száma*	Hálózatok száma*	Hálózaton belüli címek száma*
A	8	126	16777214
B	16	16382	65534
C	24	2097150	254

- Az IP-címeket kezelő szervezet (IANA: Internet Assigned Numbers Authority) osztja ki
- Alatta 5 Regional Internet registry
  - A és B osztályú címet kaphatnak tipikusan:
    - Országok
    - Internet-szolgáltatók (ISP: Internet Service Provider)
    - Egyetemek

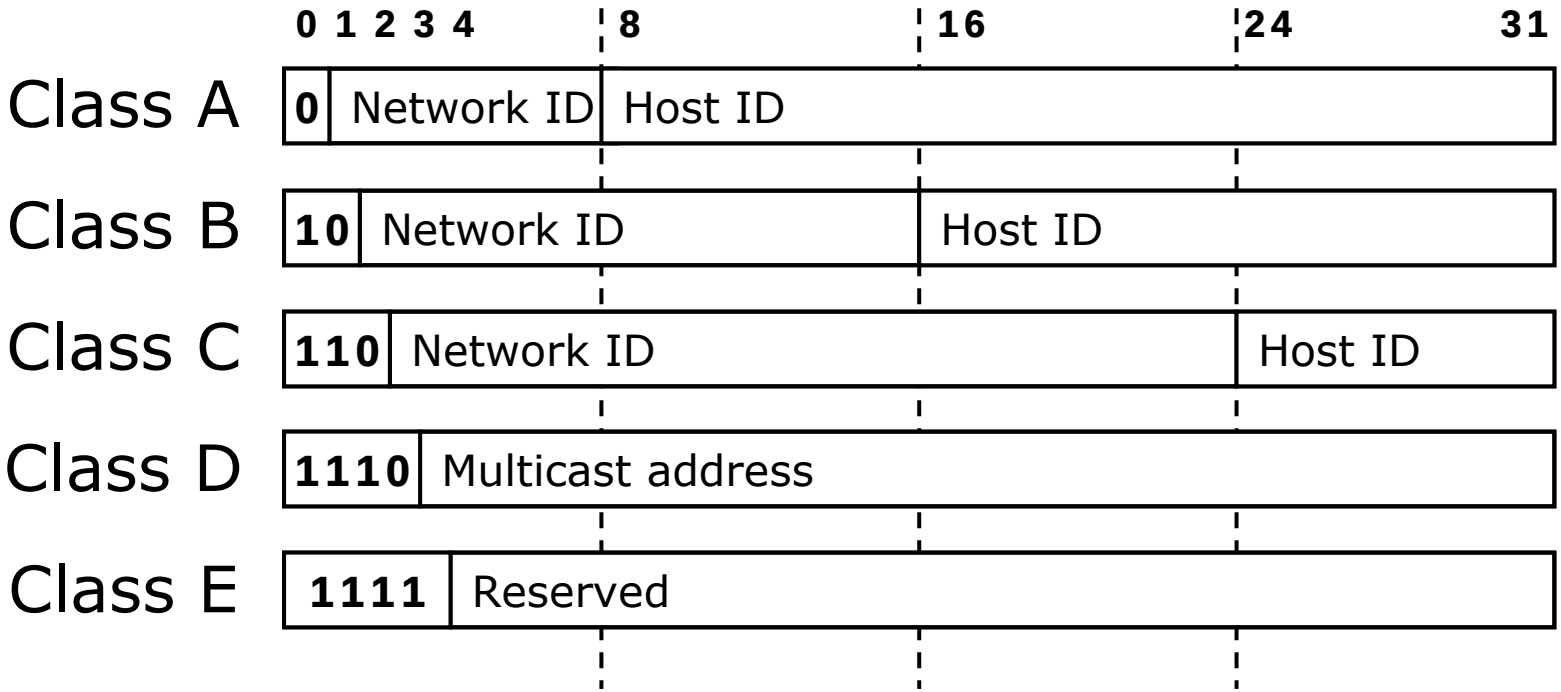
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Címosztályok

- A, B és C osztályú címek
  - Egyedi címzésre (unicast)
- D osztály
  - Többes címzésre (multicast) (később részletesen)
  - Fenntartott címtartomány:
    224.0.0.0-től 239.255.255.255-ig
- E osztály
  - Fenntartott osztály és címtartomány
    240.0.0.0-től 255.255.255.255-ig

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A címosztályok címkiosztása



- Osztályazonosító prefix
- Diszjunkt címtartományok

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Speciális címek

- Host ID: csupa 0
  - Hálózat címe
  - Az adott hálózat eszközei opcionálisan kezelhetik
- Host ID: csupa 1
  - Broadcast cím
  - A hálózaton mindenkinek szól

- E kettő miatt csak $2^{N_{host}} - 2$ számú terminált lehet megcímezni

- 127.0.0.0 - 127.255.255.255
  - Loopback cím
  - A helyi gépet azonosítja: localhost
  - Pl. vonaltesztelésre

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Problémák a címosztályokkal

- Egyes nagy cégeknek, egyetemeknek *A* osztályú címek, amit nem használtak ki (16 millió cím)
  - B kicsi lett volna nekik
- Ugyanez középcégeknél: *C* túl kicsi, *B* túl nagy
- Gond a routing aggregációval
- Nem skálázható az osztályokon alapuló rendszer!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Privát címtartományok

- Első megoldás az IPv4 címtartomány kimerülésre
- Ötlet: pl. cégen belül nem kell globálisan egyedi IP cím ha nem kommunikál kifelé
- Nem kell hozzá RIR jóváhagyás
- Ha kifelé is szeretne: Network Address Translation (NAT)
- Privát IP-címtartományok (RFC 1918)
  - Csak helyi hálózaton (Interneten nem) érvényes címek
  - 10.0.0.0 – 10.255.255.255 (1 db A osztály)
  - 172.16.0.0 - 172.31.255.255 (16 db B osztály)
  - 192.168.0.0 - 192.168.255.255 (256 db C osztály)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Gondok privát címtartománnyal

- Késleltette az IPv6 bevezezését
- Megsérti a végpont-végpont konnektivitás elvét
  - Sőt egyes Internet protokollokra nem is működik
- Privát hálózatok egyesítése: címduplikáció
  - Újracímezés
  - NAT közöttük
- Privát címek kiszivárgása az Internetre
  - Rosszul konfigurált privát hálózat
  - Komoly terhelés a névszervereknek
    - Blackhole anycast névszerverek
  - Határ routerek szűrik

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példák: IP-címek

- Milyen IP-címek az alábbiak?
  - 152.66.115.35 (www.bme.hu)
    - Első bitjei: 10… ⇨ B osztályú cím
    - Utolsó 16 bitje nem csupa 0 vagy 1 ⇨ egyedi cím
  - 195.199.23.255
    - Első bitjei: 110… ⇨ C osztályú cím
    - Utolsó 8 bitje csupa 1 ⇨ broadcast cím
  - 10.97.15.255
    - Első bitje: 0… ⇨ A osztályú cím
    - Utolsó 24 bitje nem csupa 0 vagy 1 ⇨ egyedi cím
    - Privát címtartománybeli ⇨ globálisan nem használható
- Mi legkisebb és legnagyobb C osztályú cím?
  - 11000000 00000000 00000000 00000000 ⇨ 192.0.0.0
  - 11011111 11111111 11111111 11111111 ⇨ 223.255.255.255

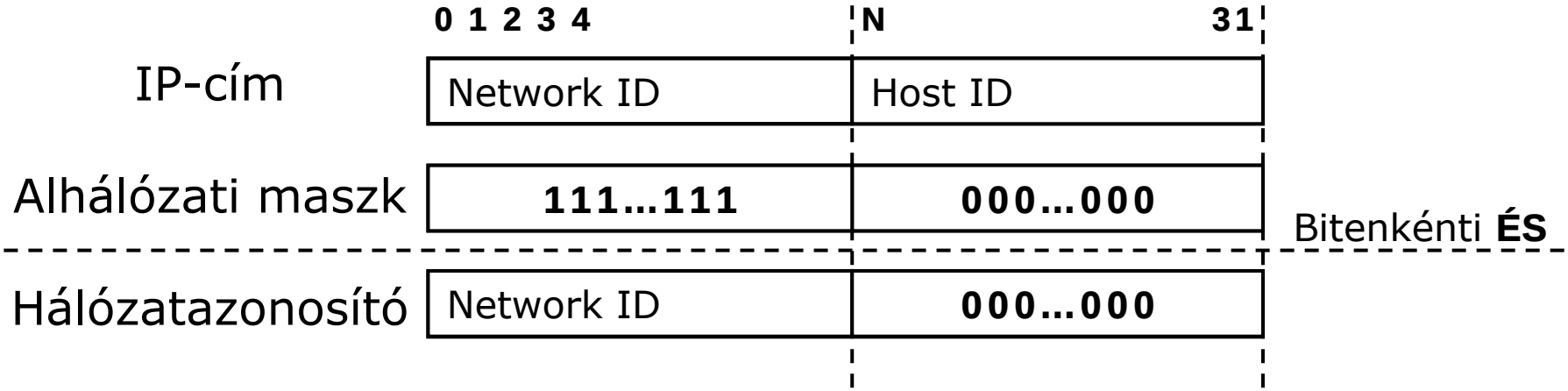
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Címosztályok általánosítása

- Osztály alapú nem skálázható, plusz IPv4 címtartomány kimerülés
- CIDR – Classless Inter-Domain Routing
  - VLSM – Variable Length Subnet Mask
    - Osztályok eltörlése: a cím 32 bitje tetszőleges helyen lehet kettéosztva hálózat- és végponti azonosítóra
  - A címből nem lehet megállapítani, hol lett kettéosztva ⇨ alhálózati maszk
- Subnetting
  - Alhálózatokra osztás vagy aggregálás
    - 1 db A osztályú ⇔ 256 db B osztályú
    - 1 db B osztályú ⇔ 256 db C osztályú
  - Már nem lehet a prefix alapján megállapítani

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alhálózati maszk (Subnet mask)



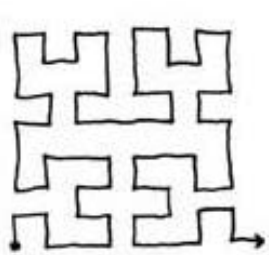
- Jelölés a hálózat egyértelmű azonosítására
  - <hálózat IP-címe> / <alhálózati maszk egyeseinek a száma>
  - Így pl. a BME hálózata: 152.66.0.0 /16 (alhálózati maszkja 255.255.0.0)
  - Hasonlóan:
    - A osztály: /8
    - B osztály: /16
    - C osztály: /24

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MAP OF THE INTERNET

THE IPv4 SPACE, 2006

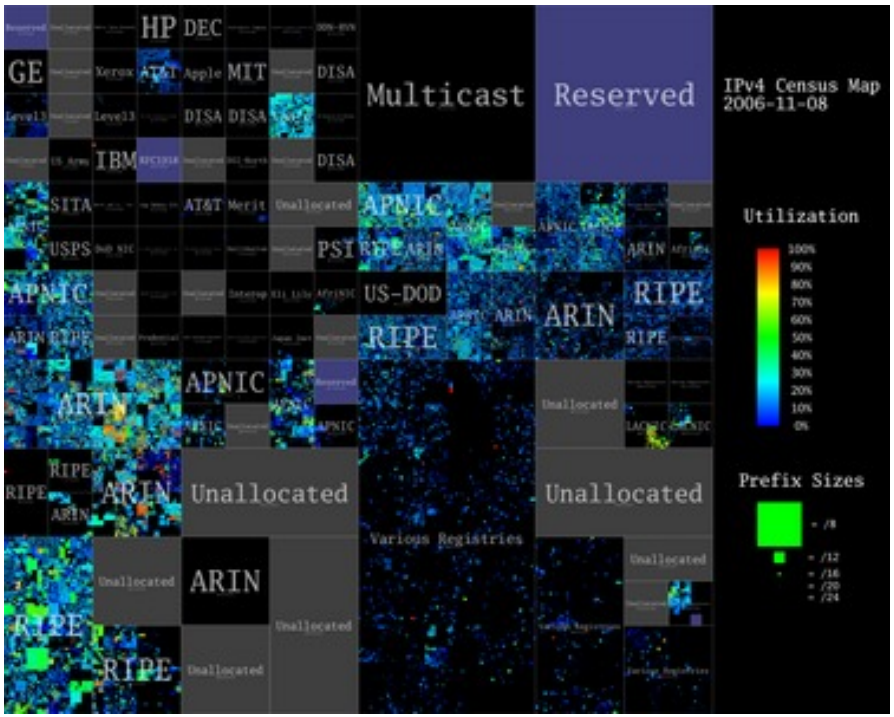
THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IPs WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IPs THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIRs TOOK OVER ALLOCATION.



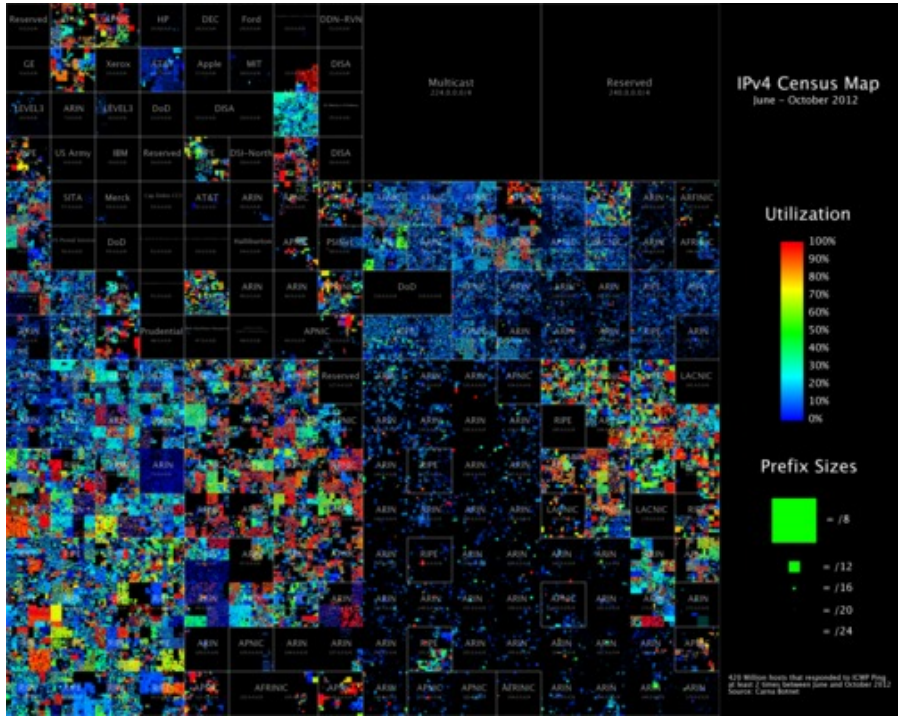
= UNALLOCATED BLOCK

IPv4 címtartomány kimerülése

2006



2012



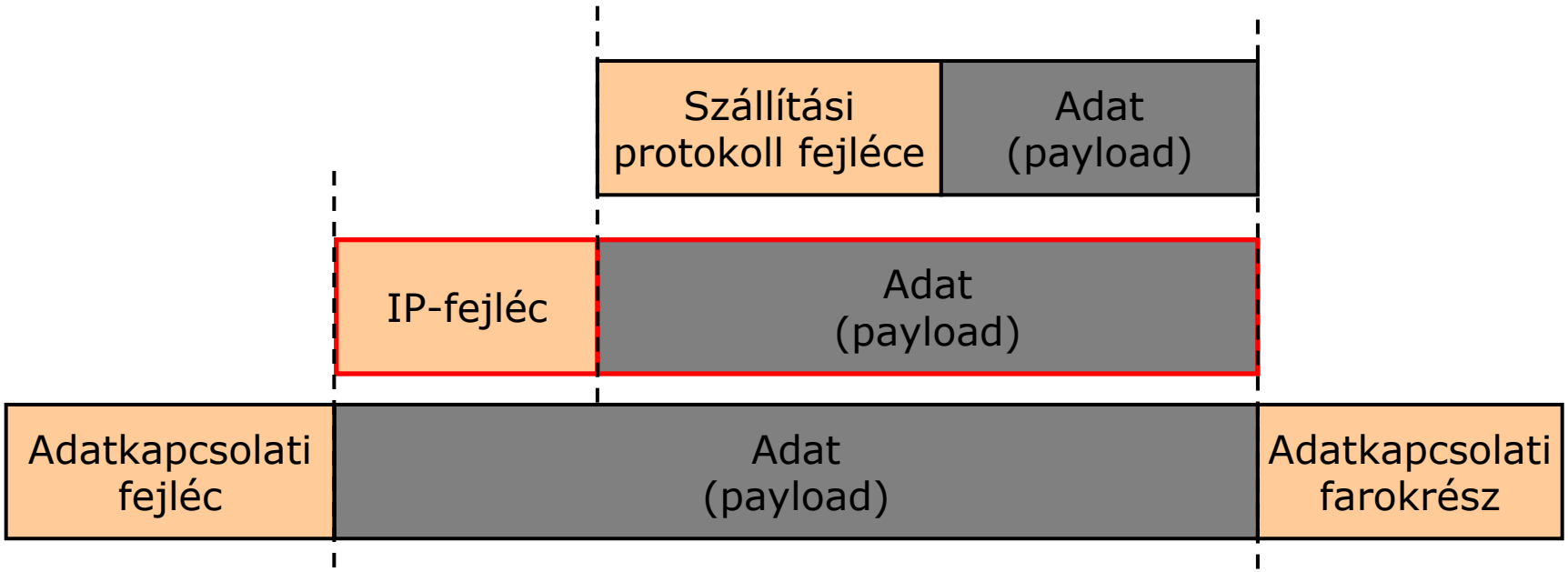
IP - Áttekintés

- Bevezetés
  - A TCP/IP protokollarchitektúra
  - Az IP feladata és jellemzői
- Címzés
- Az IP csomag szerkezete
- Routing
- IP segédprotokollok
- IPv6
- Mobil IP megoldások

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IP-csomag szerkezete és „helye”

- Az IP-csomag két része:
  - IP-fejléc / fejrész (IP header)
  - Adat (payload)
- Az IP-csomag alsóbb rétegbeli protokoll adatrészébe ágyazódik be
- Az IP-csomag adatrészébe magasabb rétegbeli protokollüzenet (PDU) kerül



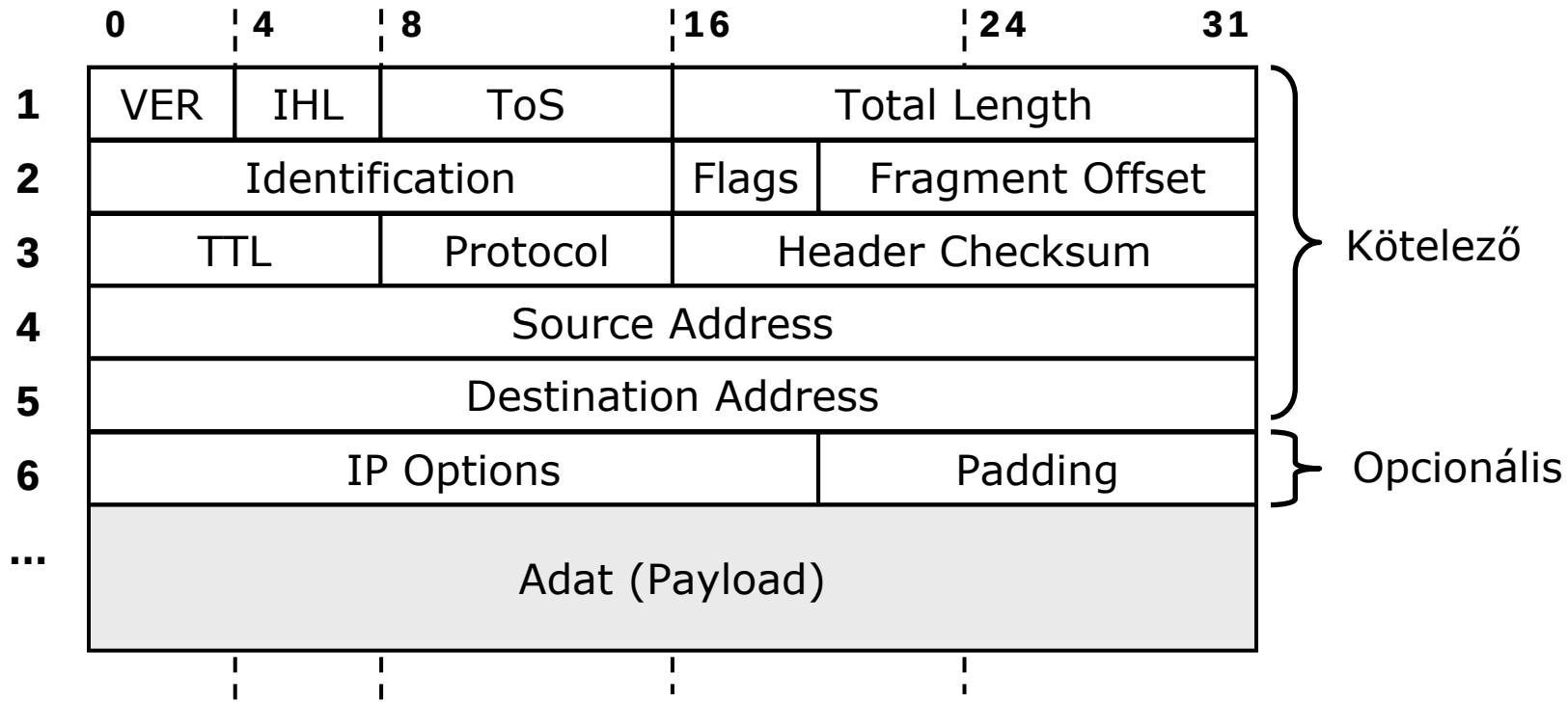
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IP - Fejléc

Az IP fejléc szerkezete

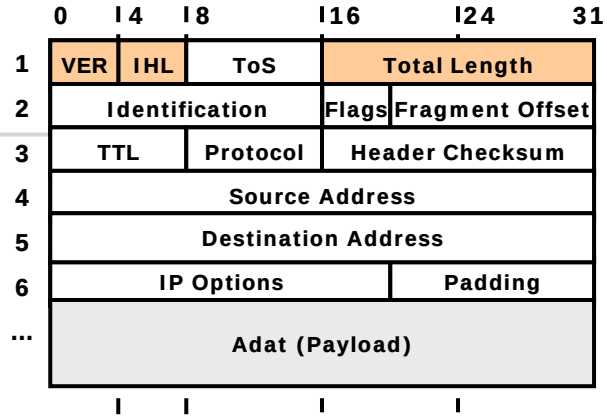
2013.Április 4.

Az IP fejléc szerkezete



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

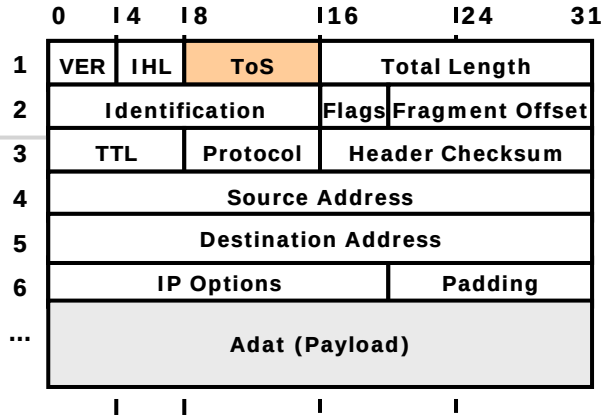
Az IP fejléc mezői I.



- VER – Version (4 bit)
  - Az Internet Protocol verziójának száma
  - Tipikus értéke: IPv4: 4, IPv6: 6
- IHL – Internet Header Length (4 bit)
  - Az IP fejléc mérete **32 bites szavakban**
  - Értéke:
    - Minimum: 5 (20 byte)
    - Maximum: 2^4-1=15 (60 byte)
- Total Length (16 bit)
  - A teljes IP csomag mérete **bájtokban**
  - Értéke:
    - Minimum: 576 (IP-fejléc 20 + 512 adat + 44 IP-opciók és az alsóbb réteg fejlécei)
      Ilyen méretű csomagot tördeletlenül kell továbbítani!
    - Maximum: 2^{16}-1=65535 (max. 65515 bájt adat)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IP fejléc mezői II.



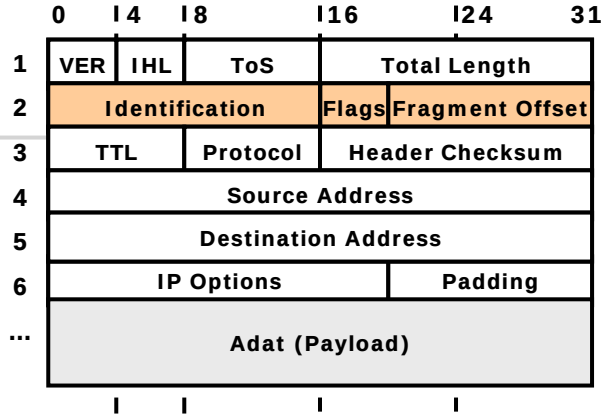
- ToS (Type of Service) (8 bit)
  - QoS osztályok, paraméterek jelzésére (RFC 791)

Bitek	Jelentés
0-2	Precedencia Példák: „network control” „priority” „routine”
3	Késleltetés (normal/low)
4	Throughput (normal/light)
5	Reliability (normal/high)
6-7	Fenntartott

  - A legtöbb router nem támogatja, de jövőben várható
  - Leggyakrabb felhasználás:
    - DSCP – Differentiated Services Code Point (RFC 2474)- 6bit: **DiffServ** (lesz róla szó később!)
    - ECN – Explicit Congestion Notification (RFC 3168)- 2bit

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

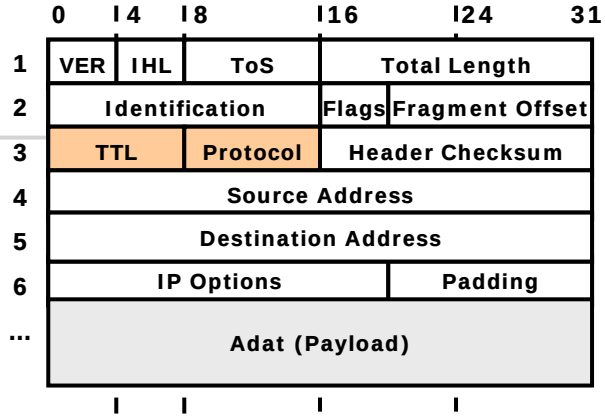
Az IP fejléc mezői III.



- **Identification (16 bit)**
  - Az IP-töredékek egyedi azonosítása
- **Flags (3 bit)**
  - 0: Fenntartott
    - 0-nak kell lennie
    - „Evil bit” (RFC 3514) (áprilisi tréfa 2003-ban)
  - 1: DF – Don’t Fragment
    - 1: ha tördelni kellene, el kell dobni
    - Ezt használják az MTU (Maximum Transmission Unit) Path Discovery néhány TCP verzióban és az IPv6-ban
  - 2: MF – More Fragment
    - 1: ha nem az utolsó töredék
    - 0: utolsó töredék vagy nem tördelt csomag
- **Fragment Offset (13 bit)**
  - Az eredeti csomagban lévő kezdőpozícióját adja meg e töredékben lévő adatnak **8 bájtos egységekben**
  - $(2^{13}-1)x8=65528 > 65515$ bájt (max. adat)
    (így a maximális méretű csomag is tördelhető)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

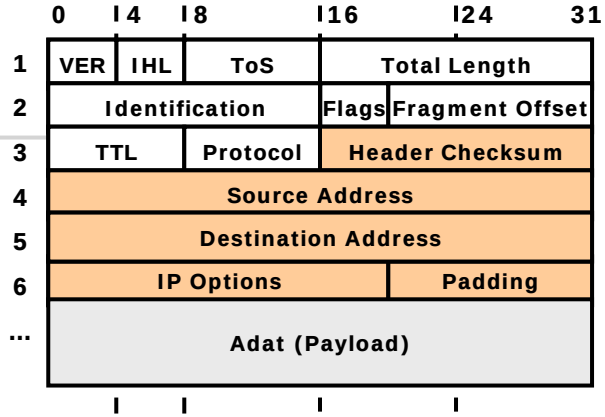
Az IP fejléc mezői IV.



- **TTL – Time To Live (8 bit)**
  - Csomag élettartama
  - Eredetileg másodpercben
  - Gyakorlatban **hopszámban** mérve (hop count)
    - Minden továbbításnál csökkenteni kell ez értékét legalább 1-gyel
    - Ha a csökkentés után az értéke nem >0, akkor el kell dobni
- **Protocol (8 bit)**
  - Az adatrészben lévő protokoll azonosítója
  - Pl: (kezdeti lista az RFC 790-ben)
    1: Internet Control Message Protocol (ICMP)
    2: Internet Group Management Protocol (IGMP)
    6: Transmission Control Protocol (TCP)
    8: Exterior Gateway Protocol (EGP)
    17: User Datagram Protocol (UDP)
    89: Open Shortest Path First (OSPF)
    132: Stream Control Transmission Protocol (SCTP)
  - Az IANA felügyeli ezeket az azonosítókat

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IP fejléc mezői V.



- **Header Checksum (16 bit)**
  - Az **IP fejléc** minden 16 bites szavának összegére számolt egyes komplemens
  - A csomag érkezésekor ellenőrizni kell a helyességét, és továbbítás esetén újra kell számítani
    - Új TTL minden lépésben, és fragmentáció is lehet
- **Source / Destination Address (2 x 32 bit)**
  - Az IP-csomag feladójának és címzettjének az IP-címe
    - NAT miatt lehet nem a feladó tényleges címe
- **IP Options**
  - Ritkán használt opcionális része a fejlécnek
  - Segítségével például a csomag útjának lehet kijelölni
    - SSRR: Strict Source (Record) Route – pontos út kijelölése
    - LSSR vagy LSRR: Loose Source (Record) Route – kötelező útba ejtendő csomópontok kijelölése
    - Legtöbb router biztonsági okokból eldobja
- **Padding**
  - Az IP Options részt egészíti ki 4 bájt többszörösére

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

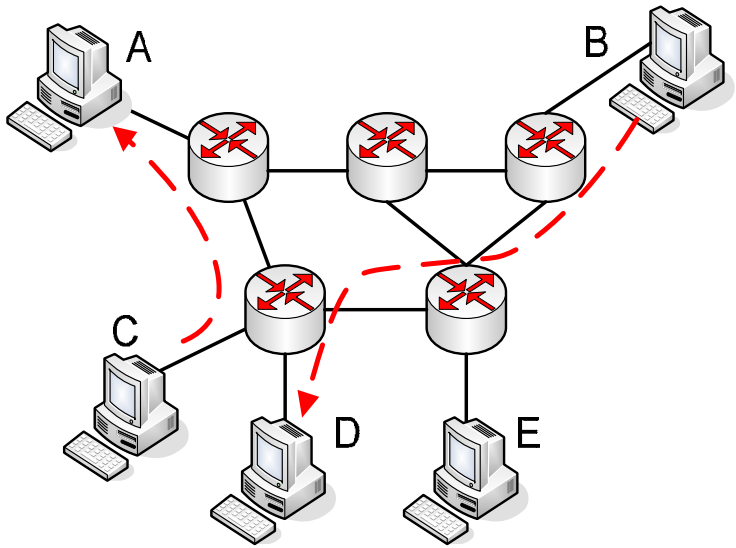
IP - Útvonalválasztás

Az IP routing működése

2013.Április 4.

Az IP feladata

- Hálózati protokoll
  - Adattovábbítás a hálózat végpontjai között
- Két fő funkció
  - **Címzés (addressing) és útvonalválasztás (routing)**
  - Tördelés (fragmentation)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A csomagtovábbítás alapelve

- Az IP jellemzői
  - Csomagkapcsolt
  - Összeköttetés-mentes (connectionless)
  - „Best effort” – nincs garancia

} Datagram típusú

- **„Hot potato”-elv**
  - Minél gyorsabban továbbítsuk
  - Csak a következő csomópontot kell ismernünk (**hop-by-hop**)
  - Előnyei:
    - Kis erőforrásigény
      - Egyszerű, ezért gyorsan továbbítható
      - Gyors, ezért nem kell tárolnunk a csomagokat
        - » kis memóriaigény
    - „Kevés” ismeret a hálózatról
    - Datagram szolgáltatásra tökéletesen alkalmas
      - nem vállal garanciát, nincs szükség nyugtázásra és egyéb hibakezelésre ⇨ gyorsasága megmarad

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Továbbításhoz szükséges információk

- Kinek küldjük tovább?
  - Cél címe alapján ⇨ csomag tartalmazza
  - Saját ismeret alapján ⇨ **útvonal-irányítási táblázat** (routing table)
- Hogyan küldjük tovább?
  - Mekkora egységekben?
    - Mekkora érkezik? ⇨ csomag határozza meg
    - Mekkora továbbítható? ⇨ **a következő hálózat MTU-ja** (Maximum Transmission Unit) határozza meg
  - Milyen QoS biztosításával?
    - „Best effort” – nincs garancia
    - Opcionális megoldás: **ToS mező** felhasználásával egyéb protokollok és mechanizmusok

Routing (útválasztás, útvonal-irányítás)

Tördelés (fragmentation)

QoS

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

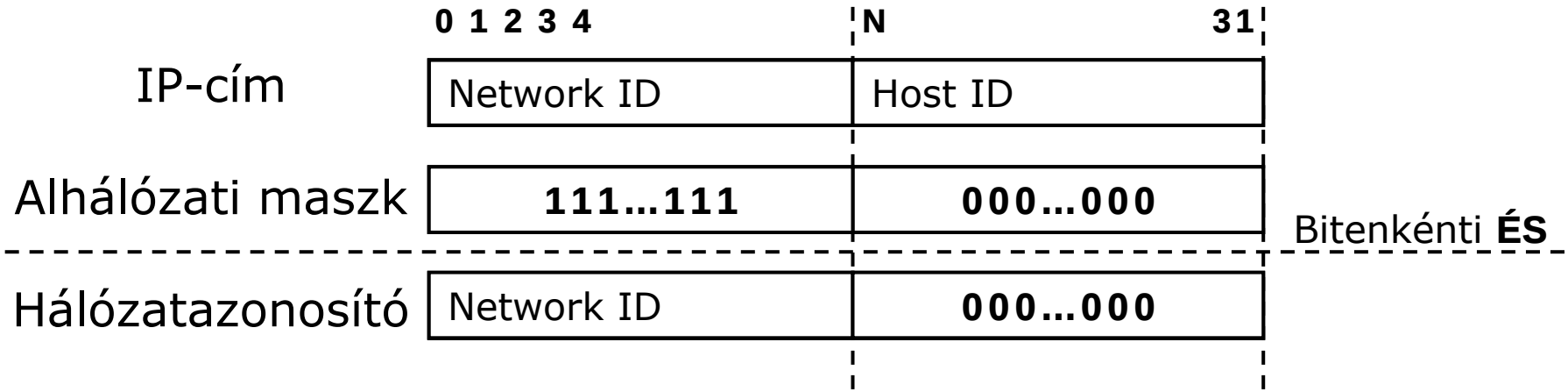
Útválasztó tábla (Routing table)

- Szükséges információk
  - Hova tart?
  - Merre küldjük tovább?
    - Ki a következő csomópont?
    - Melyik interfészen kell továbbítani?

Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alhálózati maszk (Subnet mask)



- Jelölés a hálózat egyértelmű azonosítására
  - <hálózat IP-címe> / <alhálózati maszk egyeseinek a száma>
  - Így pl. a BME hálózata: 152.66.0.0 /16 (alhálózati maszkja 255.255.0.0)
  - Hasonlóan:
    - A osztály: /8
    - B osztály: /16
    - C osztály: /24

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

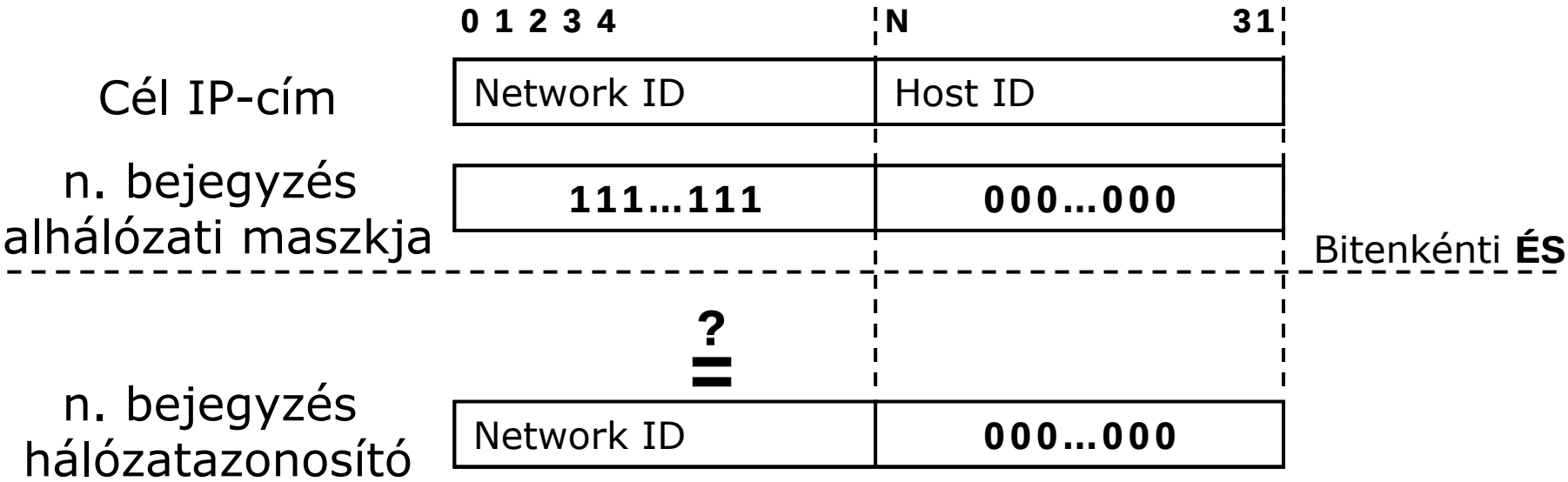
Útválasztó tábla (Routing table)

Merre megy?		Merre küldjük?		
Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

- Táblázatban szereplő hálózatok közül melyikbe megy?
- Az ahhoz tartozó interfészre küldjük ki

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hálózat kiválasztása



- A cél IP-cím akkor tartozik egy hálózatba, ha a hálózatazonosító résszel megegyezik

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Keresés az útválasztó táblában

- Ha több hálózatra is illeszkedik: **leghosszabb egyezőséget** kell választani!
  - leghosszabb hálózati maszk
- Az útválasztó tábla összes bejegyzését végig kell nézni ⇨ rosszul skálázódik
  - Általában bináris fával implementálják
    ⇨ *n* számú bejegyzésben lineáris keresés helyett csak a cím hosszában logaritmikus
- Keresés csak akkor, ha az nem saját cím

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alapértelmezett útvonal (Default route)

- Erre megy a csomag, ha nem ismeri a célhálózatot
- Minden címet tartalmazó hálózat
  - Ehhez a hálózati cím: 0.0.0.0/0
- Az alapértelmezett átjáró és elnevezése
  - A fenti bejegyzéshez tartozó következő csomópont IP-címe
  - **Alapértelmezett átjáró (default gateway, DG)** név nem szerencsés
    - Átjáró: általában alkalmazás rétegbeli továbbító
    - Helyette inkább a router / útválasztó/ útvonalválasztó
- Nem feltétlenül van ilyen
  - Ha másra nem illeszkedik, akkor a célhálózat ismeretlen, így a csomagot eldobja
- Végpontokon gyakran csak két bejegyzés szerepel:
  - Helyi hálózat (helyi végpont közvetlenül elérhető)
  - Alapértelmezett útvonal (minden más távoli hálózaton)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Metrikák szerepe az útválasztásban

- Metrika (mérték): Egy számérték, amely a hálózati utak közötti preferenciát adja meg
- Metrika alapja lehet például:
  - Elérhetőség
  - Terheltség
  - Késleltetés
- Metrika típusa
  - Statikus
    - Manuálisan megadott
  - Dinamikus
    - A link vagy a hálózat állapotától függően automatikusan változó
- A jobb metrikával rendelkező kapcsolaton küldjük ki a csomagot!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Megfelelő bejegyzés kiválasztva

Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

- Mi a stratégia, ha
  - Közvetlenül (nincs következő csomópont!)

  vagy
  - nem közvetlenül

  kapcsolódik a hálózat?

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Teendők helyi és távoli hálózat esetén

- Közvetlenül kapcsolódó (helyi) hálózat
  - A címzettnek közvetlenül küldeni
    - Ehhez a címzett **adatkapcsolati rétegbeli címére** van szükség
- Nem közvetlenül kapcsolódó (távoli hálózat)
  - Az útválasztónak kell küldeni
    - Az IP-címet tilos módosítani
    - Csak **adatkapcsolati rétegben** kell az útválasztónak címezni
      - Ehhez szükség van az adatkapcsolati címére

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

IP – ARP/RARP

Kapcsolat az adatkapcsolati címek felé

2013.Április 4.

ARP – Address Resolution Protocol

- Ha ismerjük az IP-címet, és a hozzá tartozó adatkapcsolati rétegbeli címre van szükség
  - RFC826
- Szinte minden adatkapcsolati és hálózati réteget támogat
  - Token Ring, FDDI, ATM, IEEE802.3, IEEE802.11
- Működése:
  - **Broadcast** kérés: „Kinek az IP-címe a …?”
  - Az IP-cím tulajdonosa válaszol
- Az ARP üzeneteket közvetlenül az adatkapcsolati réteg protokolljának küldjük (**Nem IP-csomag**!)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az ARP fejléce

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		
RARP header structure		

- Hardware Type
  - Ethernet: 0x0001
- Protocol Type
  - IP: 0x8000
- HLen
  - Ethernet: 6 byte
  - TokenRing: 2 vagy 6 byte
  - FDDI: 2 vagy 6 byte
- PLen
  - IP: 4 byte

- Operation
  - ARP request = 1
  - ARP reply = 2
  - RARP request =3
  - RARP reply =4
- Sender Hardware Address
  - <MAC-cím>
- Sender Protocol Address
  - <IP-cím>
- Target Hardware Address
- Target Protocol Address

Névfeloldás ARP-vel

- „A” szeretné megtudni „B” MAC-címét
  - 1. „A” üzenete
    - Operation: ARP Request = 1
    - Sender HA: <A MAC-címe>
      - **Megegyezik a keret fejlécében** találhatóval
    - Sender PA: <A IP-címe>
    - Target HA: 00:00:00:00:00:00 (ismeretlen)
      - A keret MAC címében FF:FF:FF:FF:FF:FF !!! (broadcast)
    - Target PA: <B IP-címe>
  - 2. „B” válasza
    - Operation: ARP Reply = 2
    - Sender HA: <B MAC-címe>
      - Most már nem 00:00:00:00:00:00 (ismeretlen)
      - Megegyezik a keret fejlécében találhatóval
    - Sender PA: <B IP-címe>
    - Target HA: <A MAC-címe>
    - Target PA: <A IP-címe>

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ARP tábla

- Címpárok: Adatkapcsolati rétegbeli és IP-címek
- Két bejegyzéstípus
  - Statikus
    - Manuálisan felvitt bejegyzés
  - Dinamikus
    - ARP címfeloldás eredménye
    - **Gyorsítótár (cache)** funkció: ne kelljen mindig lekérdezni
    - Egy idő után elévül és törlődik

HW-cím	*IP-cím*	*típus*
<MAC-cím1>	<IP-cím1>	statikus
<MAC-cím2>	<IP-cím2>	dinamikus

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ARP egyéb alkalmazásai

- ARP próba (probe)
  - Mielőtt használni kezdene egy IPv4 címet, felderíti, hogy nem használja-e más
  - Broadcast ARP kérés, küldő IP címe csupa nulla, saját címét kérdezi le
  - *IPv4 Address Conflict Detection* (RFC 5227)

- ARP hirdetmény
  - Ha változik MAC vagy IP címe, küld egy *gratuitous ARP* üzenetet, hogy mások tudják frissíteni az ARP táblájukat
  - TPA=SPA és THA=0 (request) vagy TPA=SPA, THA=SHA (reply)
    - Pl. operációs rendszer betöltésnél ha változott a hálózati kártya
    - vagy terheléselosztásra (több hálókártyánál)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

RARP – Reverse ARP

- Adatkapcsolati rétegbeli címből IP-címet
- Felhasználási terület
  - Hálózatmenedzsment
  - Permanens tár nélküli eszközök
    - Semmi ismeretük nincs a hálózatról
    - Hálózatról töltődik be az operációs rendszer
    - IP-cím nélküli kezdeti kommunikáció
- RARP kiszolgálók
  - RARP broadcast üzenetekre válaszolnak
- RARP helyett ma sokkal elterjedtebb megoldások
  - Bootstrap Protocol (BOOTP): hálózatról történő betöltésre
  - Dynamic Host Configuration Protocol (DHCP): IP-cím kérésére

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Útválasztó tábla karbantartása

- Manuálisan
  - Minden hálózati operációs rendszer által támogatott
- Automatikusan
  - A tábla felépítéséhez szükséges információkat az útválasztók megosztják egymással
    ⇨ útválasztó protokollok (routing protocols)

IP – Útvonalválasztó protokollok

Útvonalválasztó táblák építése automatikusan

2013.Április 4.

Útválasztó protokollok feladatai

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

Útvonalválasztó protokollok funkcionális osztályozása

- Ad hoc routing protokollok
  - Kis és gyorsan változó hálózatokra
    - Szenzor és egyéb vezeték nélküli hálózatokra
- Interior Gateway Protocols (IGPs)
  - Autonóm rendszereken (AS) belül
    - Kisebb hálózatokon
- Exterior Gateway Protocols (EGPs)
  - Autonóm rendszerek (AS) között
    - Az Internet routing protokollja

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Ad hoc routing protokollok osztályozása *

- Működési mód szerint
  - Proaktív
    - Folyamatosan karbantartott táblákkal
  - Reaktív
    - Igény szerinti célfelderítés
  - Hibrid
    - A fenti kettő együttes alkalmazása
- Alkalmazási terület szerint
  - Hierarchikus
  - Földrajzi elhelyezkedés alapján
  - Multicast
  - Energiatakarékos

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IGP routing: A „távolság-vektor” módszer

- A gyűjtött információ és a gyűjtés módja:

  A csomópontok elmondják a hálózatról alkotott elképzeléseiket a szomszédaiknak

- Az „elképzelések”:
  - melyik csomópont milyen távol van
  - egy lista (vektor) melynek elemei
    - csomópont azonosító – távolság párok

- A távolság-vektorát közli mindegyik csomópont valamennyi szomszédjával

IGP routing: Az „összekötés-állapot” módszer

- A gyűjtött információ és a gyűjtés módja:

  A csomópontok elmondják mindenkinek a szomszédaikról nyert tapasztalataikat

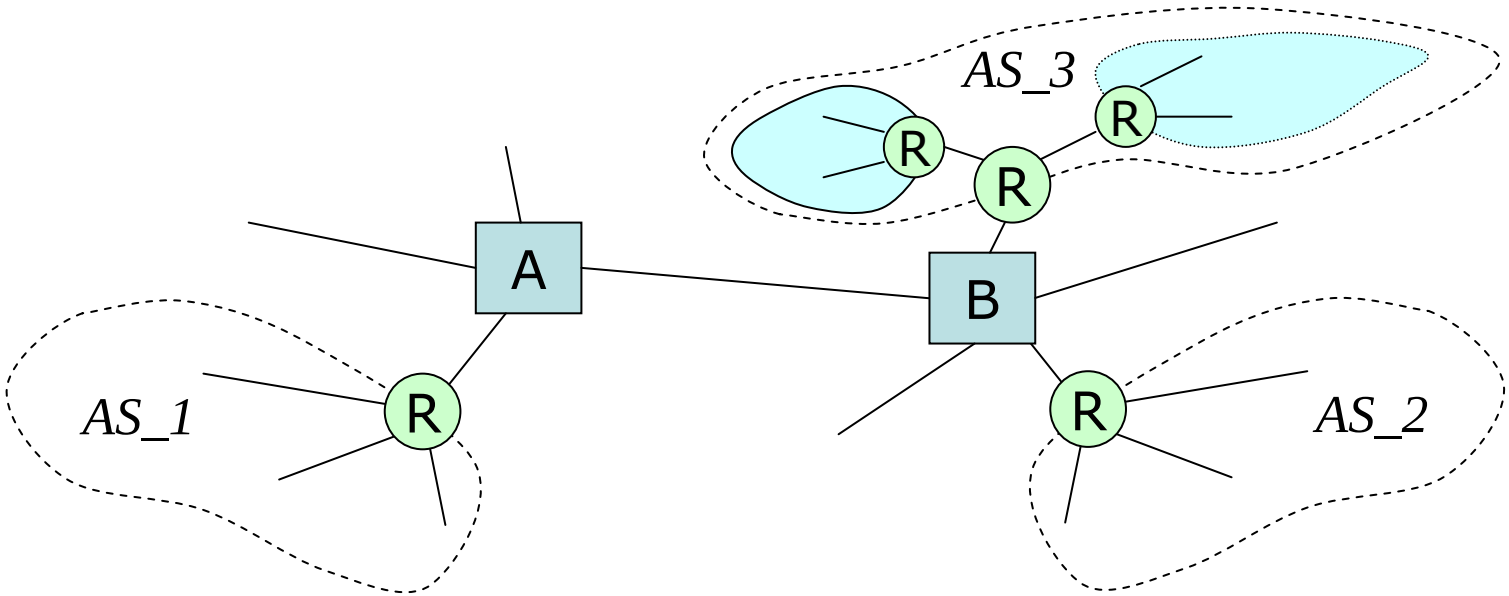
- A „tapasztalatok”:
  - a szomszédokhoz vezető linkek **aktuális állapota** (ez pontosan ismerhető)

- Az információ elküldése „mindenkinek” a korlátozott (felügyelt) *elárasztás*-sal:
  - elküldik a szomszédokhoz, akik továbbadják
  - kivéve azon a linken, amelyen érkezett

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Autonóm rendszerek

- Egy autonóm rendszer a többi autonóm rendszer számára jelzi az általa képviselt csoporto(ka)t
- Az egész csoport egyetlen bejegyzés lesz az útvonal-táblában



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Interior Gateway Protocols (IGPs)

- Autonóm rendszereken (AS) belül
  - Távolság-vektor:
    - RIP (Routing Information Protocol)
    - IGRP (Interior Gateway Routing Protocol)
    - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - Összekötés-állapot:
    - OSPF (Open Shortest Path First)
    - IS-IS (Intermediate System to Intermediate System)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazásuk

- **RIP:** nem preferált
  - Lassan konvergál, nem skálázódik jól
    - Update: 30s
  - Hopszám limit korlátozza a hálózat méretét
    - Max 15
  - De könnyen konfigurálható
  - Metrika: hopszám
- **IGRP**: Cisco specifikus
  - Javította RIP hibáit
    - Max 255 hop
    - Többféle metrika figyelembe vétele
    - Már nem használják
- **EIGRP:** IGRP javítása (VLSM)
  - Gyorsabb konvergencia
  - Hurokmentes működés
  - 6 metrika kombinációja

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazásuk

- Elterjedtebbek az összeköttetés-állapot módszerek
  - OSPF: nagy céges hálózatokban
    - Nagyon gyorsan konvergál
    - Többféle metrika
    - Hierarchikus: gerinc - routing tartományok, köztük határ routerek
  - IS-IS: nagy kiterjedésű ISP hálózatokban

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

OSPF vs. IS-IS

- OSPF (2-es verzió):
  - IPv4 forgalom irányítására tervezték: népszerűbb
    - több fejlesztés, alkalmazás
  - Át kellett specifikálni IPv6-ra (OSPFv3)

- IS-IS:
  - OSI fejlesztés, nem IP csomagokban
  - Nagyobb kiterjedésű hálózatokra (ISP)
    - Több routert támogat adott területen
  - Mivel nem IPv4 specifikus, könnyebb átállás IPv6-ra

Exterior Gateway Protocols (EGPs)

- Autonóm rendszerek (AS) között
- Példák:
  - EGP (Exterior Gateway Protocol)
    - Sokáig az Internet EGP-je, ma már nem használt
  - BGP (Border Gateway Protocol)
    - 1995-től használt EGP (BGPv4)

- Címaggregáció (supernet)
  - Gyorsabb keresés
  - Gyorsabb terjesztés

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

BGP routing alapelv

- **Path vector protocol (Útvonal-vektor protokoll)**

- Routing tábla bejegyzés:
  - Célhálózat
  - Következő router
  - **Útvonal a célhálózatig**

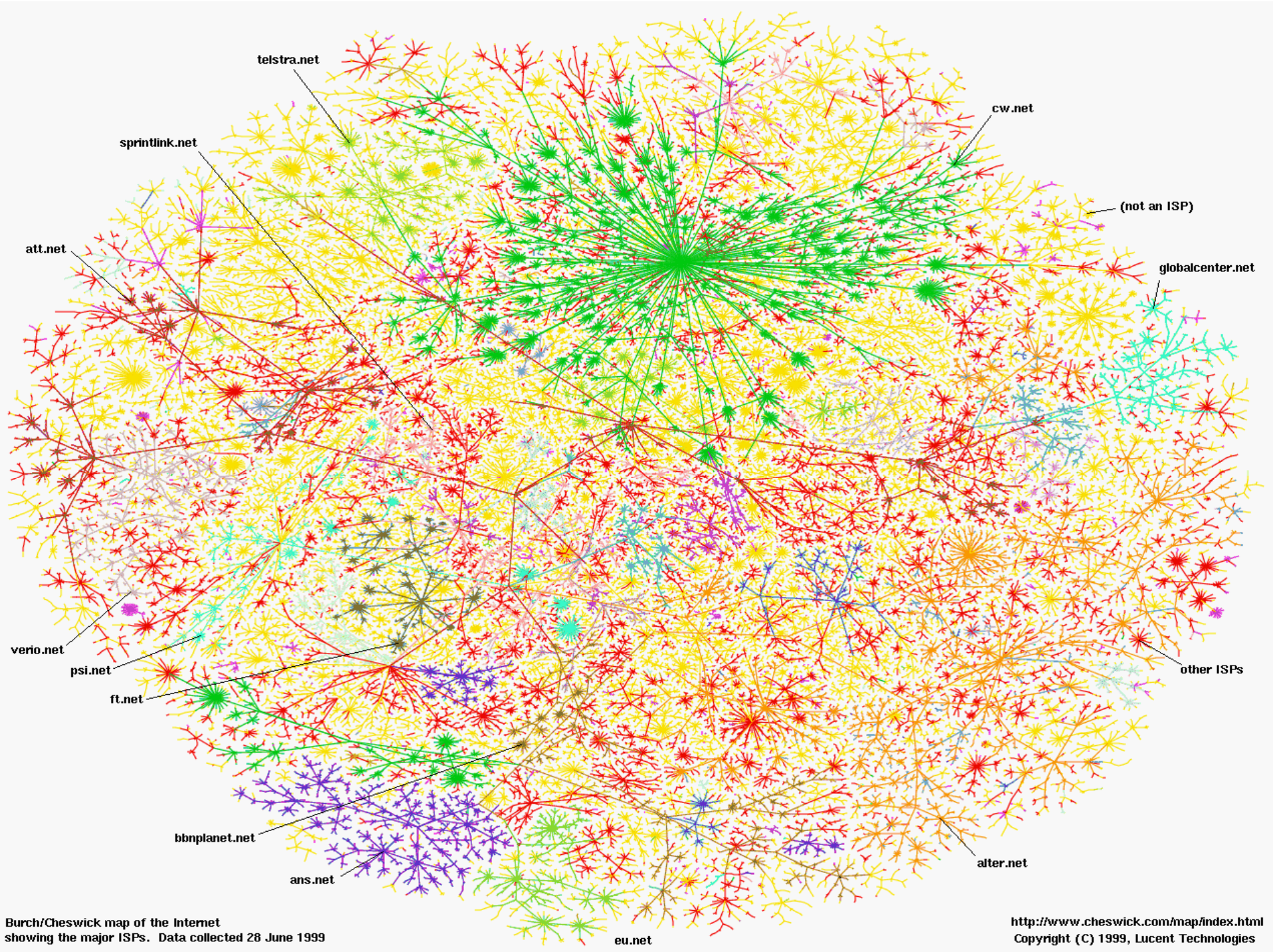
- A **teljes útvonal** dinamikus nyilvántartása
  - AS határ routerek végzik: útvonal-vektor üzenetekkel (Path Vector Message) frissítés, hirdetve a többi AS elérhetőségét
  - **Útvonal-vektor üzenet**: AS-ek sorozata a célhálózat felé
  - Minden AS határ router fogadáskor megnézi megfelel-e a saját szabályainak
    - Ha igen, módosítja a routing tábláját és az útvonal-vektor üzenetet
    - Következő router: saját ID-je, illetve útvonal-vektorba AS száma

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hogyan néz ki az Internet?

Valóban decentralizált?

2013.Április 4.

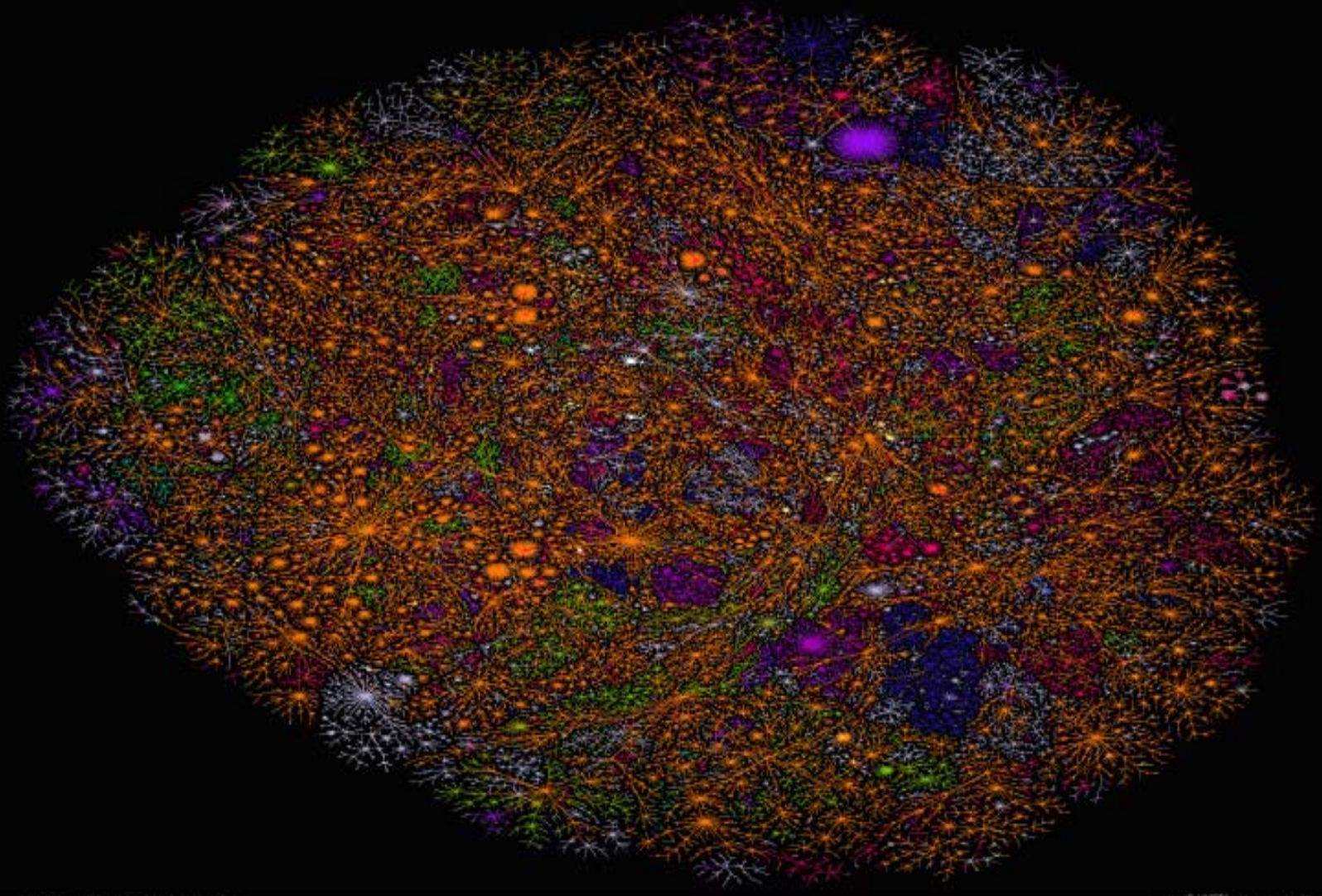


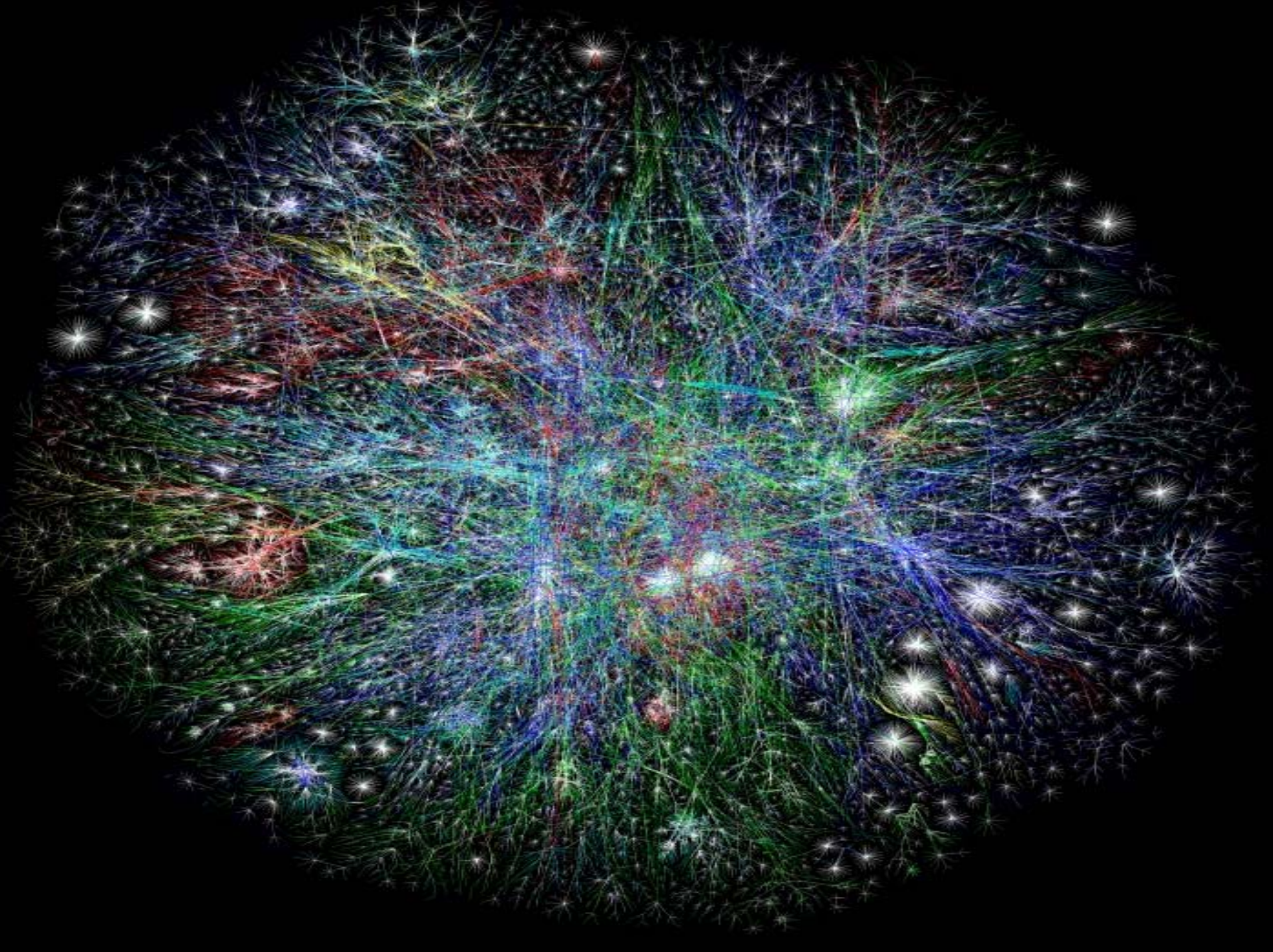
Burch/Cheswick map of the Internet
showing the major ISPs. Data collected 28 June 1999

http://www.cheswick.com/map/index.html

Copyright (C) 1999, Lucent Technologies

The Internet: 2002





IP - Tördelés

Darabolás és összeállítás

2013.Április 4.

Tördelés szükségessége

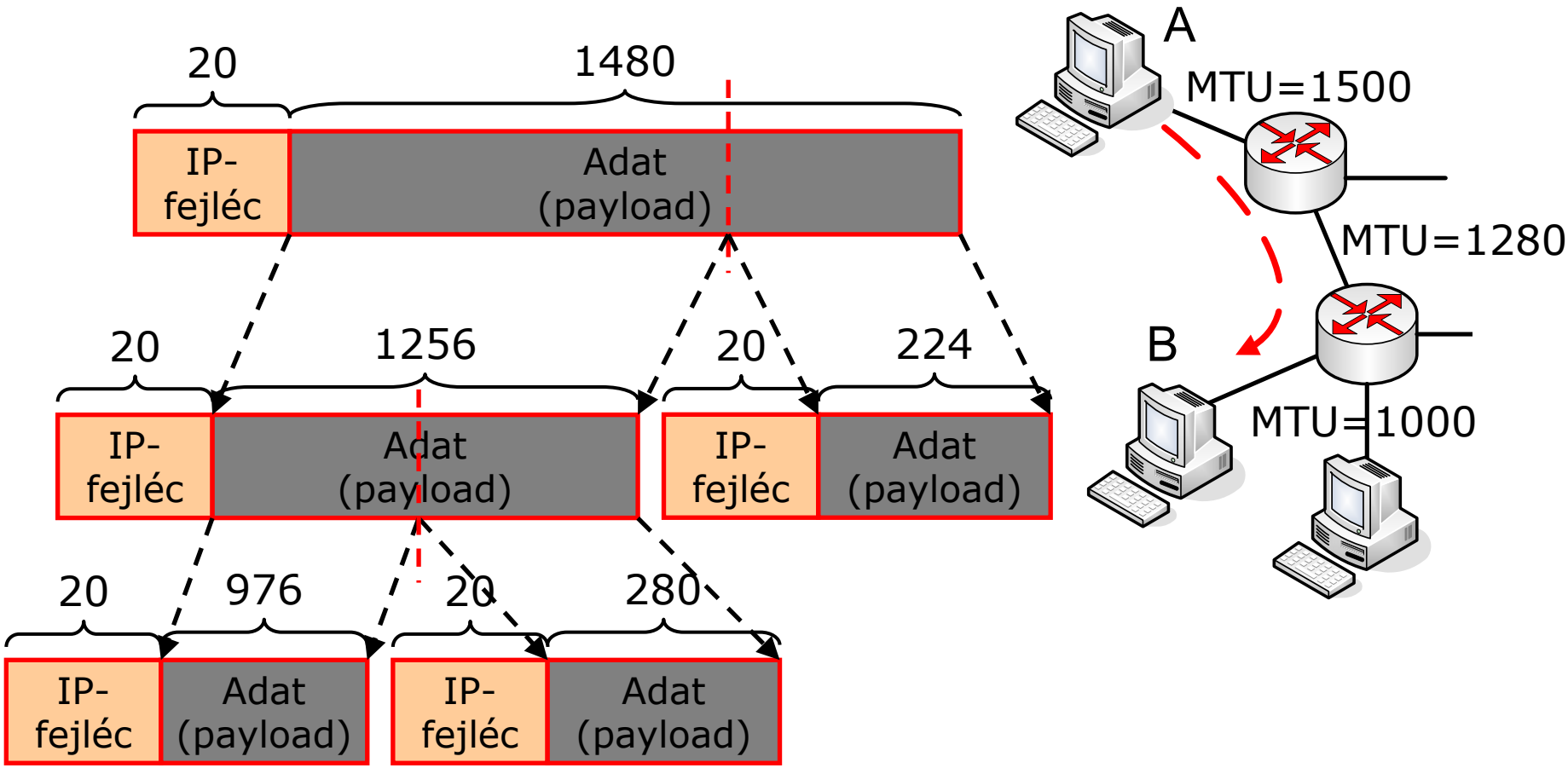
- A hálózatok alsóbb rétegei meghatározzák a keret maximális méretét
  - Az adatkapcsolati réteg fej- és farokrészét leszámítva ez az MTU (Maximum Transmission Unit)
    - Ethernetnél 1500 byte

- Eltérő technológiák ⇨ eltérő MTU-jú kapcsolatok ⇨ tördelni kell

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

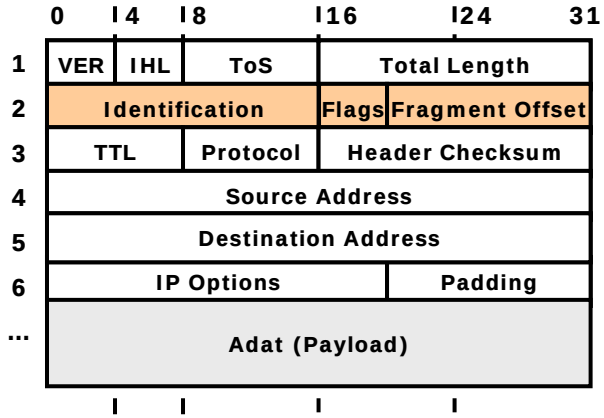
A tördelés menete

- Minden csomagnak kell fejléc (itt minimális fejléccel)!



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Tördeléssel kapcsolatos mezők az IP-fejlécben



- Identification (16 bit)
  - Az IP-töredékek egyedi azonosítása
- Flags (3 bit)
  - 0: Fenntartott
    - 0-nak kell lennie
    - „Evil bit” (RFC 3514) (áprilisi tréfa 2003-ban)
  - 1: DF – Don’t Fragment
    - 1: ha tördelni kellene, el kell dobni
    - Ezt használják az MTU (Maximum Transmission Unit) Path Discovery néhány TCP verzióban és az IPv6-ban
  - 2: MF – More Fragment
    - 1: ha nem az utolsó töredék
    - 0: utolsó töredék vagy nem tördelt csomag
- Fragment Offset (13 bit)
  - Az eredeti csomagban lévő kezdőpozícióját adja meg e töredékben lévő adatnak **8 bájtos egységekben**
  - $(2^{13}-1)x8=65528 > 65515$ bájt (max. adat)
    (így a maximális méretű csomag is tördelhető)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

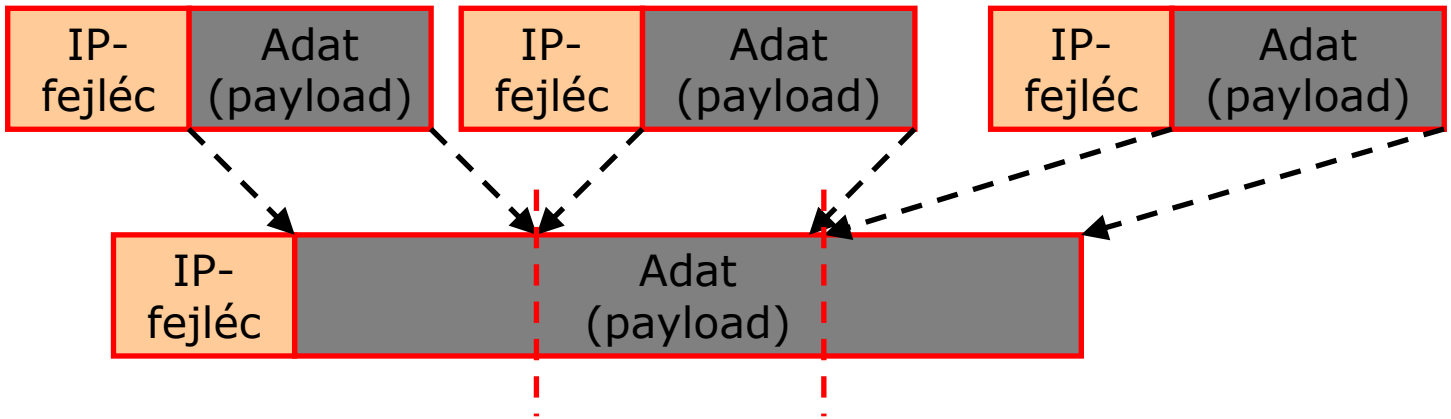
IP-fejléc változása tördelés közben

- Ha tördelés szükséges:
  - Total Length mezőt a töredék méretére állítani
  - Ha nem volt Identification mező érték, akkor generálni kell
  - Adat tördelése 8 bájtos egységekre
  - A tördelésnek megfelelő fragmentation offset-et beállítani az új csomagokban
  - Minden csomagban az MF bitet 1-re kell állítani, kivéve annak a csomagnak az utolsó töredékénél
  - Ellenőrző összeg változása

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A töredékek összeállítása

- Csak a címzett végezheti el
  - Kivéve pl. NAT
- Ha valamely darab nem érkezik meg, akkor a többit is eldobja
- Csak teljesen összeállított csomagokat továbbít a felsőbb réteg felé
- A „fragment offset”-ekből a töredék helye meghatározható



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A router feladatai

- Hibás-e a csomag (fejléce)?
- Nekem címezték-e?
- Ismerem-e a címzett hálózatát?
- A TTL érték csökkentés után >0?
- Kell-e tördelni? Lehet-e tördelni?
- Kell-e visszajelzést küldeni?

ICMP és IGMP

Az IP jelzés- és menedzsmentüzenetei

- *ICMP: Internet Control Message Protocol*
- *IGMP: Internet Group Management Protocol*

2013.Április 4.

ICMP - Internet Control Message Protocol

- Jelzés- és menedzsmentüzenetek
  - Visszajelzés a „best effort” hálózattól
- IP felett (0x01-es protokollazonosító)
- Üzenettípusok
  - Hibaüzenetek
  - Kérdések
  - Válaszok
- Gyakran használt ICMP üzenetek:
  - Echo request – Echo reply ⇨ Ping (RTT)
  - Echo request – Echo reply + TTL ⇨ Traceroute

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ICMP csomag és fejléce

- IP csomagba ágyazva, IPv4 fejléc után következik a fejléce (8 byte)
- Így best-effort szolgáltatás, de különleges elbánást kap a feldolgozásnál
  - Kötelező értesíteni a forrás címet, amely okozta a hibaüzenet generálását

- Fejléc:
  - Típuson belül kód, pl. típus: *címzett elérhetetlen*, ezen belül kód:
    - *címzett hálózat/host/protokoll/port elérhetetlen*
    - *tördelésre van szükség*
    - *letiltott hálózat/host*
  - Ellenőrzőösszeg egész ICMP üzenetre
  - Hibaüzenetnél: a hibás üzenet fejléce és adatmezőjéből az első 8 byte

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ICMP – Cél elérhetetlen

- Gyakran előforduló üzenet:
  „Destination unreachable” (ICMP Message Type: 0x03)

  Hibakódok:

0 = net unreachable
1 = host unreachable
2 = protocol unreachable
3 = port unreachable
4 = fragmentation needed and DF set
5 = source route failed
6 = destination network unknown
7 = destination host unknown
8 = source host isolated
9 = communication with destination network administratively prohibited
10 = communication with destination host administratively prohibited
11 = network unreachable for type of service
12 = host unreachable for type of service

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Traceroute

- Először TTL=1, majd TTL=2 ...
- Sorban eldobják a routerek és ICMP üzenetet küldenek róla (Time Exceeded)
- Megadja a csomópontok listáját, amelyeket érint a csomag a célig
- Nem mindig a realitást tükrözi a traceroute lista
- Alkalmazás:
  - Hibaelhárításra
  - Tűzfal felderítésre
  - Letöltésnél (mirror)
  - Penetráció tesztelésre
- Hackerek is szeretik☺

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

További érdekes ICMP üzenetek

- Source Quench: felszólítás a küldőnek a forgalma visszafogására
- Redirect: felszólítás a küldőnek másik útvonal használatára
- Address Mask Request: host lekéri a router-től az alhálózati maszkot

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IGMP – Internet Group Management Protocol

- IP-t futtató csomópont-csoportok kezelésére
  - Pl. online streaming video, játékok
  - IP csomagokban
- Főként multicast csoportok kezelése
  - Csoportok lekérdezése
  - Csoporthoz csatlakozás
- A TTL értéke általában 1
  (csak a helyi hálózaton érvényes)
- Csak IPv4-hez, IPv6 máshogy oldja meg

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás

- Bevezetés
  - A TCP/IP protokollarchitektúra
  - Az IP feladata és jellemzői
- IP címzés
  - Címosztályok
  - Speciális címek
- Az IP fejrész szerkezete
- Routing protokollok
- Routingtáblák, subnet mask
- Továbbítás
- Címfeloldás: ARP, RARP
- MTU, tördelés
- Segédprotokollok: ICMP, IGMP

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

IPv6

A következő generációs Internet Protocol

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.Április 9.

IPv6 - Áttekintés

- Motivációk – az IPv4 hibái
- Címzés
- IPv6-fejléc
- Migráció és együttélés
- IPv6 biztonság

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Motivációk

Az IPv4 hibái

2013.Április 9.

Motiváció – problémák az IPv4-gyel

- 32 bites címtartomány kimerülése
- Erőforrás-igényes
  - Sok felesleges mező a fejlécben
  - Tördelés a köztes csomópontokban
- Nem biztonságos
  - Nem támogatja a hitelesítést és a titkosítást
- Mobilitás támogatás csak külön protokollal

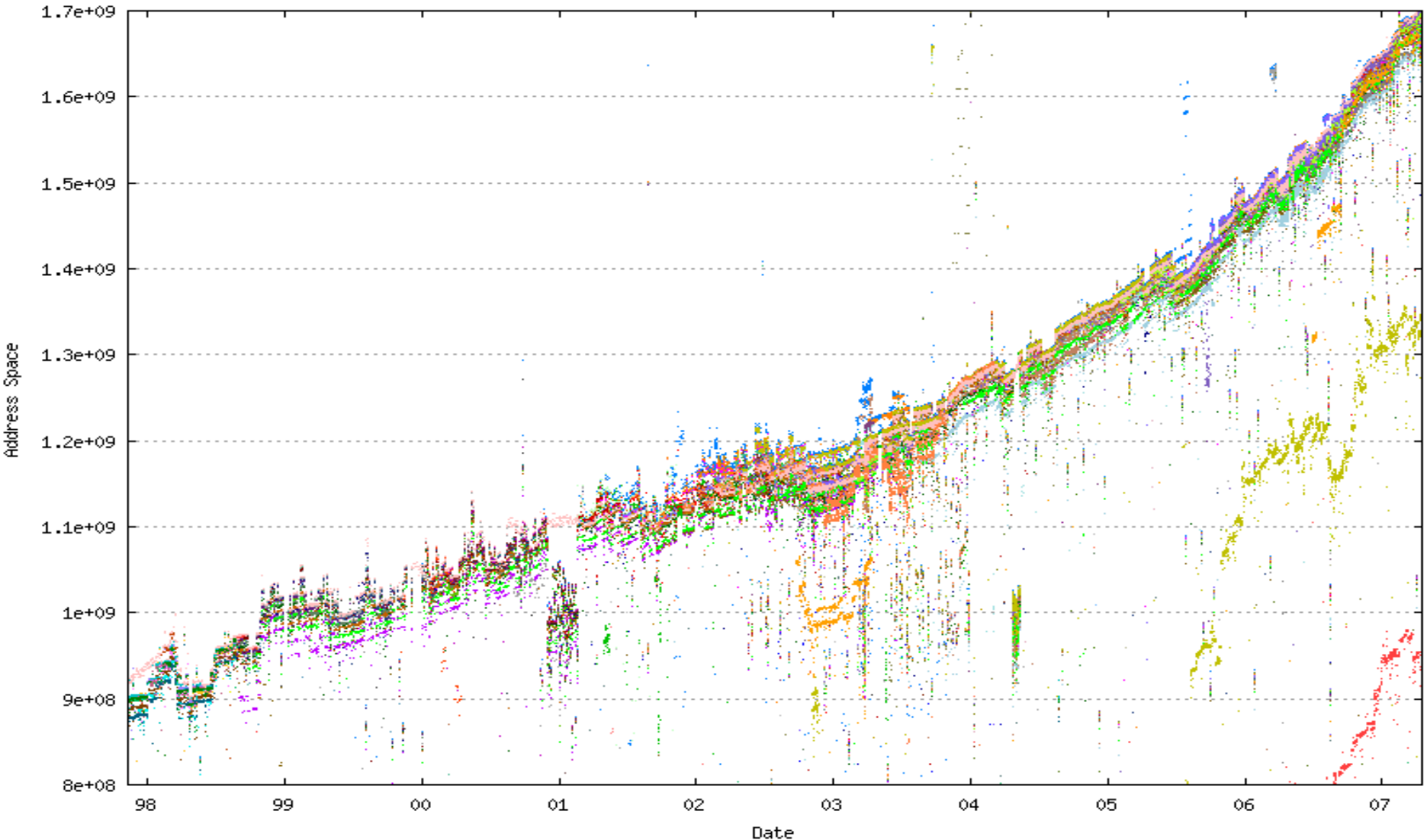
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Címtartomány kimerülés okai

- Egyre nagyobb az Internet elterjedtsége
  - Fejlődő népes országok (Kína, India, Afrika)
- Egyre több eszköz
  - Mobiltelefonok: 4G-ben már IPv6!
  - Szenzorok (intelligens otthon, biometrikus ~)
  - TV-készülékek, hűtők, mosógépek, …
- Pazarló címfelhasználás
- Always-on elterjedése
  - dial-up helyett
- Virtualizáció

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kiosztott címtartományok tere



Híres ember híres kijelentése

„32 bits should be enough address space for Internet”

- Vint Cerf, 1977 (Honorary Chairman of IPv6 Forum 2000)

Hol tartunk most? Mennyi IP-cím szabad?

- Már a 80-as végétől felmerült a címkimerítés lehetősége
- Történelmi pillanat: 2011. februárjában osztotta ki a IANA az utolsó 5 blokkot az 5 RIR-nek
  - egyenként 16 millió címmel
- 2011 áprilisára az ázsiai-csendes-óceáni RIR kimerítette ezt a cím blokkját!

- 2001-ben 2007-re a címtartomány kimerülését jósolták
- Miért nem következett be?
  - NAT (Network Address Translation)
  - Privát IP-címtartományok
  - CIDR
    - VLSM
    - Címek újraosztása
  - RIR-ek, ISP-k IP-címgazdálkodása
  - Virtuális hosting
    - Név, IP illetve port alapú

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

IPv6 címzés

Hatalmas címtartomány újdonságokkal

2013.Április 9.

Milyen hosszú az ideális cím?

- 64 bites
  - Sokkal tovább elég, mint a 32 bites
  - Nem túl nagy növekedés az IP fejlécben
- Változó méretű 160 bitig
  - Kezdetben lehet 64 bites is, majd szükség esetén lehet növelni
- Megállapodás: 128 bites legyen!
  - Kompromisszum
  - 340 282 366 920 938 463 463 374 607 431 768 211 456 ≈ $3{,}4 \cdot 10^{38}$ cím kezelésére
  - Minden lakosra 2^{95} cím

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv6 címek ábrázolása

- 128 bit
- 8x4 hexadecimális számként ábrázolják
  - FEDC:BA94:7654:3210:FEDC:BA98:7654:3210
- A vezető nullák elhagyhatók
  - FEDC:0094:0004:0000:000C:BA98:7654:3210
  - FEDC:94:4:0:C:BA98:7654:3210
- A 16 bites nullákat tartalmazó részek kihagyhatóak, ha egymás után vannak (maximum egy ilyen blokk hagyható ki):
  - FEDC:0000:0000:0000:000C:BA98:0000:3210
  - FEDC::C:BA98:0:3210
  - Pl. localhost: (0:0:0:0:0:0:0:1) helyett ::1

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv6 címek ábrázolása

- Egyes IPv6-os címek IPv4-ből származnak. Ekkor megengedett:
  - 0:0:0:0:0:0:A00:1
  - ::10.0.0.1
- Hálózati címek (prefixek) jelölése
  - FEDB:ABCD:ABCD::/48
  - FEDB:ABCD:AB00::/40
- Hivatkozásként
  - http://[FEDC::C:BA98:0000:3210]/index.html
  - RFC 2732

Cím prefixek

0000 0000	Reserved
0000 0001	Unassigned
0000 001	Reserved for NSAP (non-IP addresses used by ISO)
0000 010	Reserved for IPX (non-IP addresses used by IPX)
0000 011	Unassigned
0000 1	Unassigned
0001	Unassigned
001	**Unicast Address Space**
010	Unassigned
011	Unassigned
100	Unassigned
101	Unassigned
110	Unassigned
1110	Unassigned
1111 0	Unassigned
1111 10	Unassigned
1111 110	Unassigned
1111 1110 0	Unassigned
1111 1110 10	**Link Local Use addresses**
1111 1110 11	**Site Local Use addresses**
1111 1111	**Multicast addresses**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Címtípusok az IPv6-ban

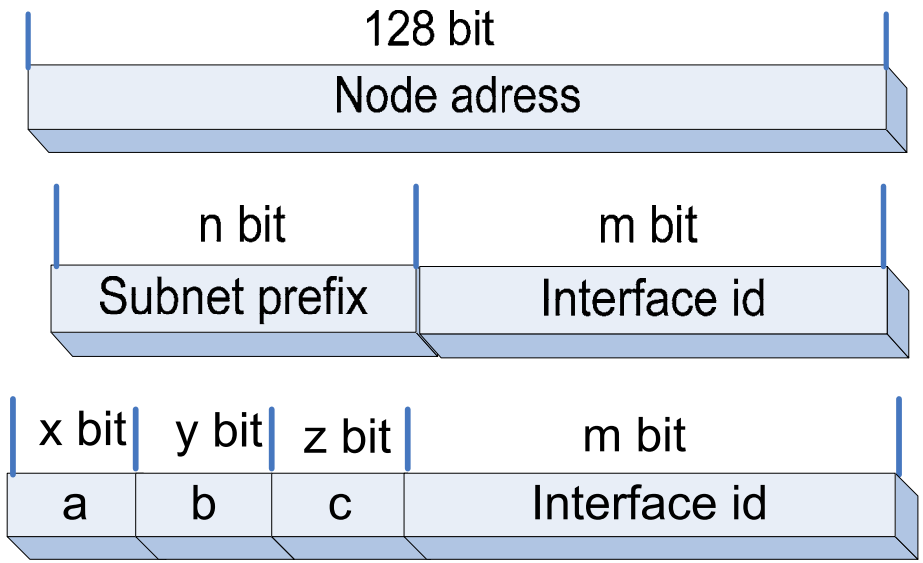
- Unicast
  - Az IPv4-hez hasonlóan
  - Egyedi cím: pontosan egy csomóponthoz tartozik
  - Minden IPv6 csomópontnak legalább egy ilyen címe van
- Multicast
  - Csoportot azonosít
  - Minden csoporton belüli csomópont megkapja az erre a címre küldött adatot
  - Broadcast helyett is ezt használjuk
- Anycast
  - Csoportot azonosít
  - Biztosított, hogy a csoport egy csomópontja megkapja az erre a címre küldött üzenetet
    - pl. a küldőhöz legközelebbi

Unicast címek

- Típusai:
  - Globális
    - Aggregálható

    vagy
    - IPv4 kompatibilis
  - Link local
    - Prefix után a hálózati cím végig nulla, nem route-olható
  - Site local (valószínűleg a gyakorlatban ezt nem fogják használni)
  - Beágyazott IPv4 címet tartalmazó

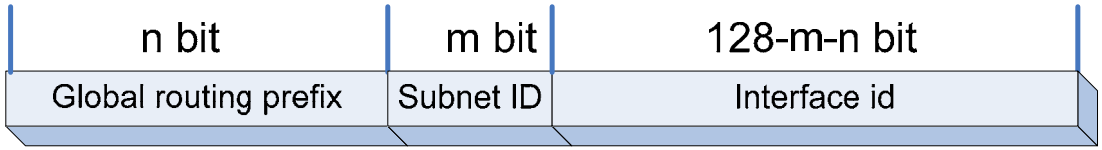
- Strukturált cím



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Globális unicast cím

- Felépítése:



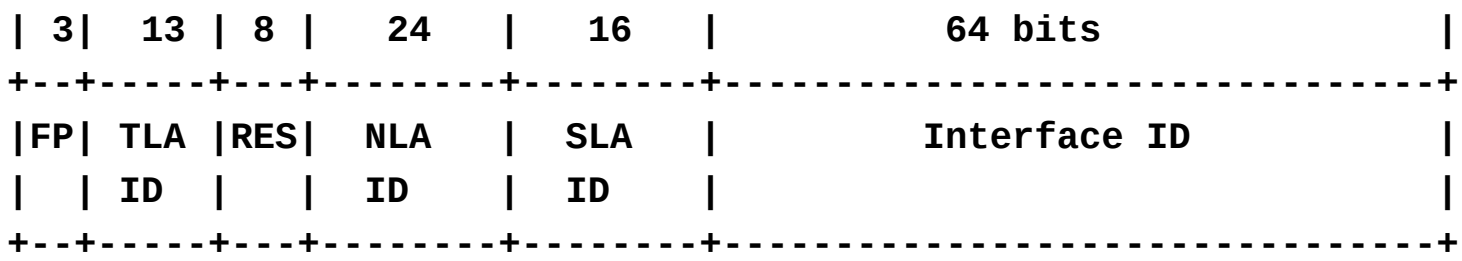
- A „ki vagy ” szétválasztása a „hová kapcsolódsz”-tól
  - Routing Prefix
    - Routing topológia
  - Subnet ID
    - Hálózati adminisztrátor
  - Csomópont azonosítás
    - Interface Identifier

- Interface ID
  - Megegyezés alapján 64 bit
  - Az adatkapcsolati rétegbeli címből képződik
    - Egyediséget biztosítja, ha hardverhez kötődik a cím
    - Ethernet MAC címből: 48 bit →64 bit
  - Vagy DHCP szervertől random

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Aggregálható globális unicast címzés

- Aggregatable Global Unicast Address Structure [RFC 2347]

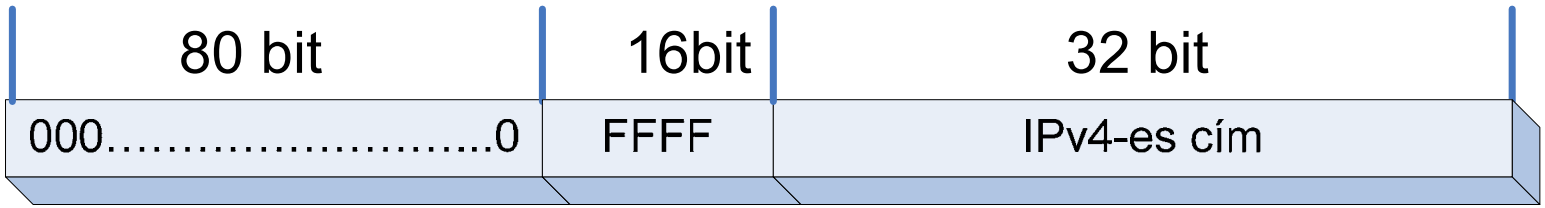


- FP Format Prefix (001)
- TLA ID Top-Level Aggregation Identifier (régió)
- RES Reserved for future use
- NLA ID Next-Level Aggregation Identifier (szolgáltató)
- SLA ID Site-Level Aggregation Identifier (előfizető és alhálózat)
- INTERF. ID Interface Identifier

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv4 kompatibilis címek

- 000-val kezdődők
  - IPv4 kompatibilis IPv6 címek
    - Pl. ::10.0.0.1
  - IPv6-ra képezett IPv4-os címek
    - Pl: ::FFFF:10.0.0.1



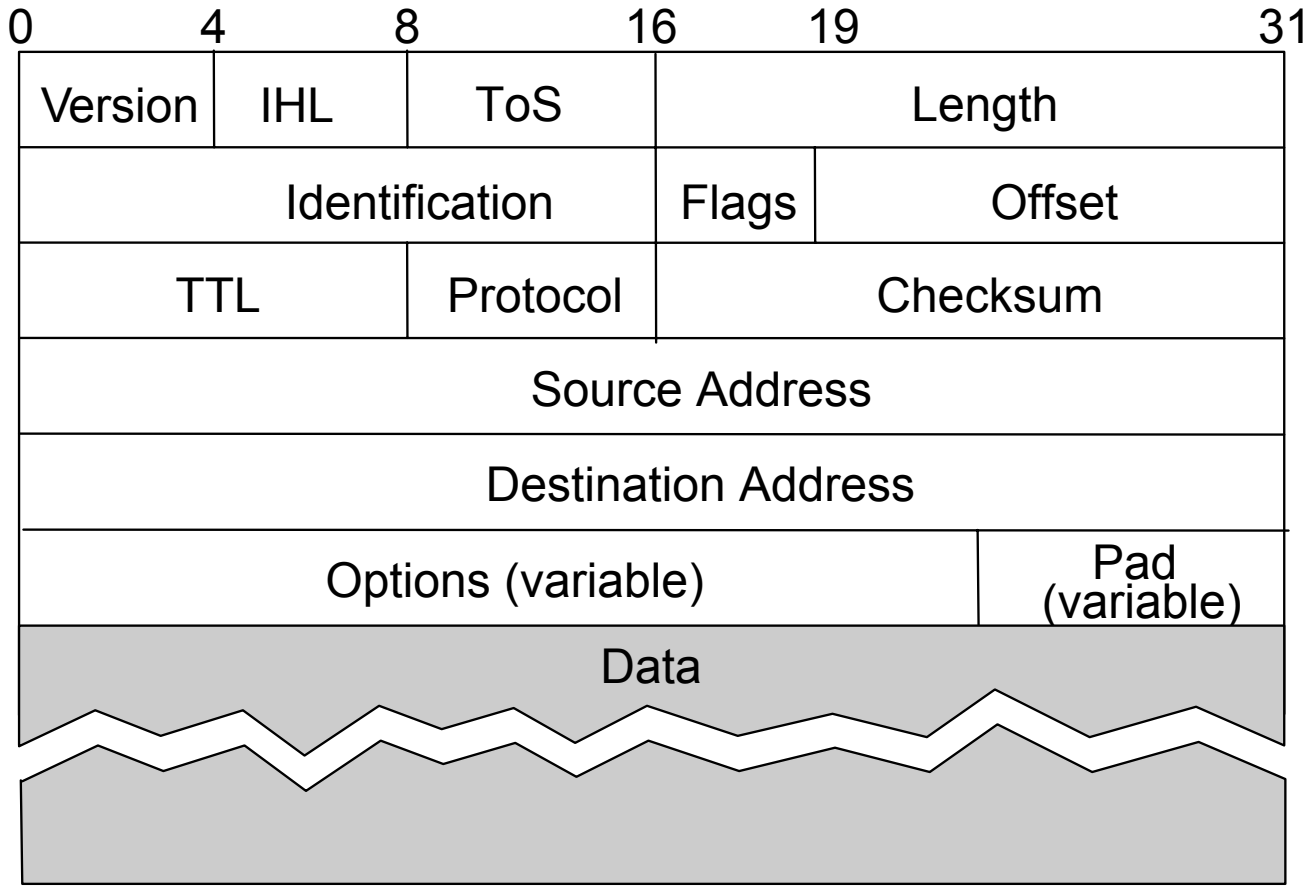
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv6 csomag szerkezete

Egyszerűség és univerzalitás

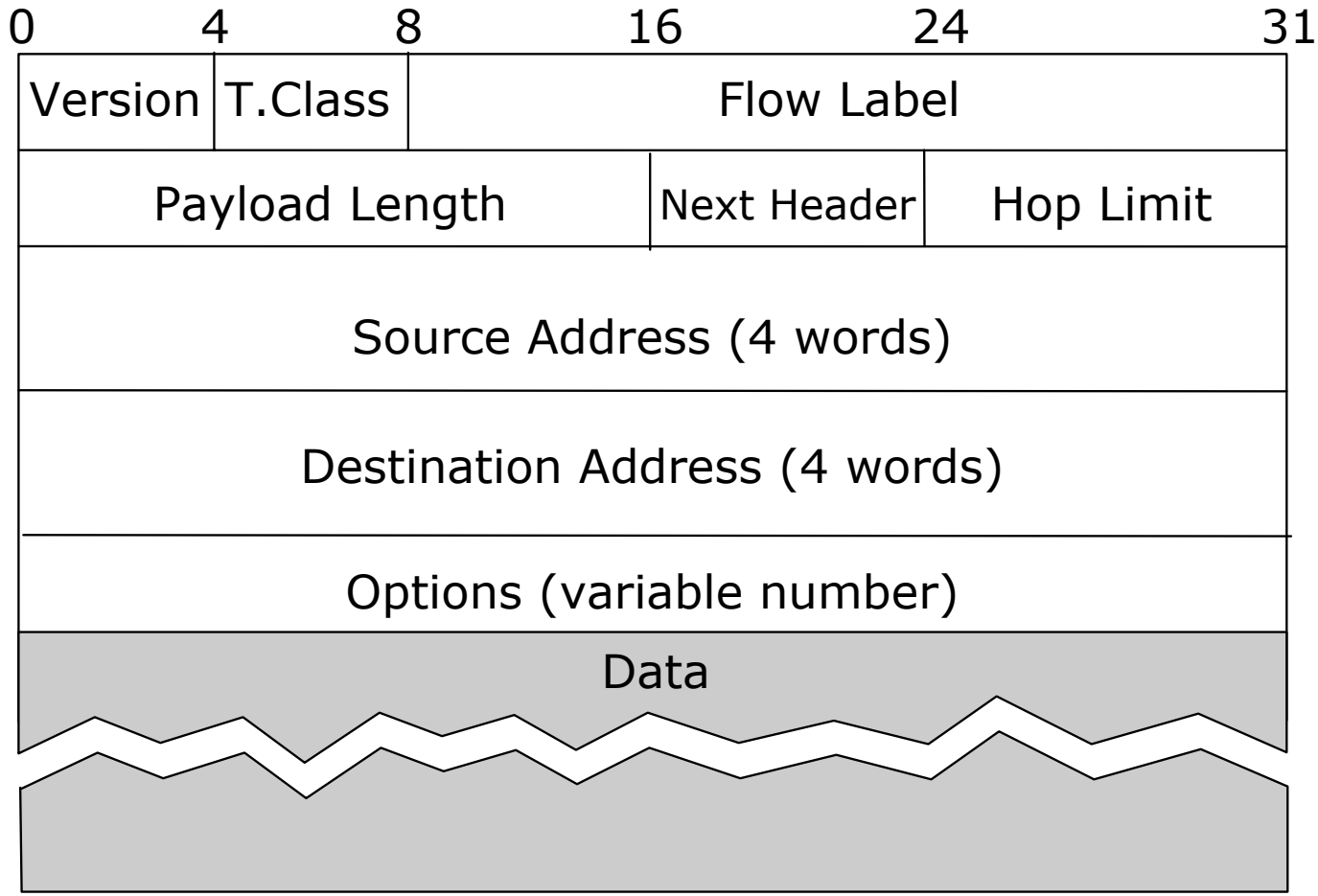
2013.Április 9.

Az IPv4 csomag szerkezete



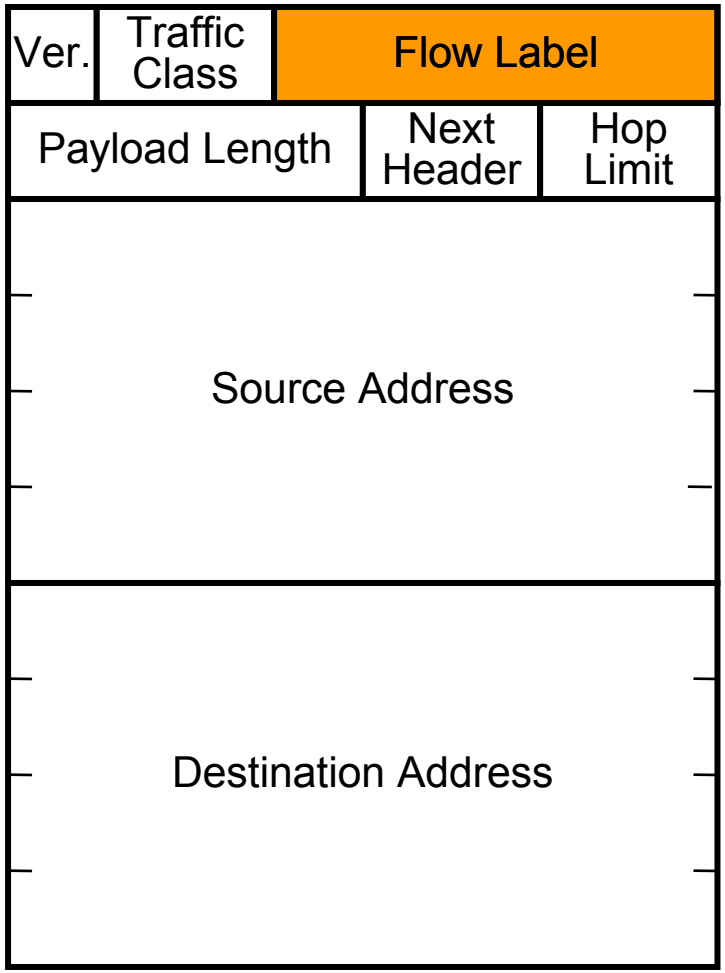
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

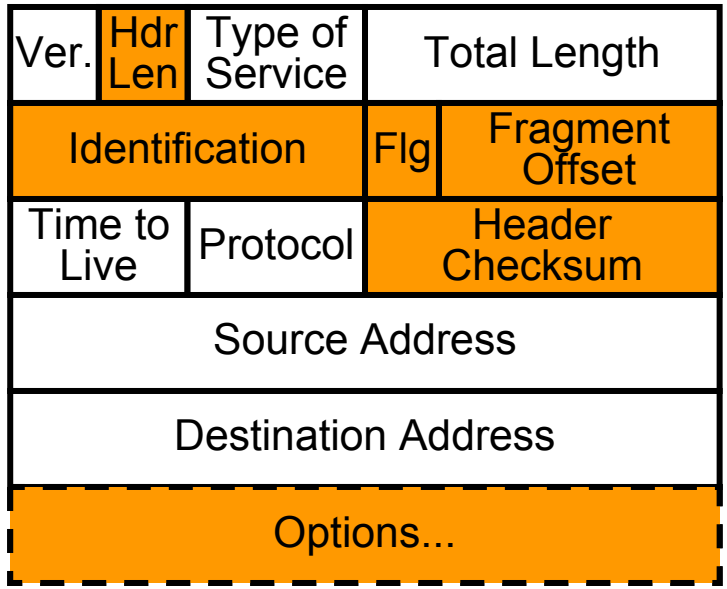
IPv6 csomag szerkezete



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv6 és IPv4 fejrészek összehasonlítása





A kiemelt részek a másik verzióban nem találhatók meg!

IPv6 fejrész kétszer hosszabb (40 byte), mint a minimális IPv4-es (20 byte)!!!

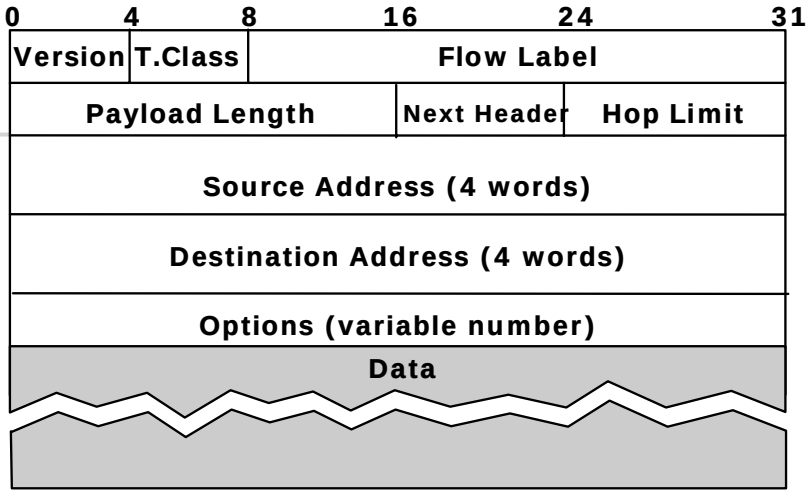
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Ami az IPv6 fejrészből kimaradt…

- Nincs ellenőrzőösszeg (checksum)
  - Nem kell minden routernek ellenőriznie
    ⇨ nő a feldolgozási sebesség
  - Általában kevés a hiba (jó minőségű kapcsolatok)
- Nem változik a fejrész mérete
  - Rögzített méret ⇨ nő a feldolgozási sebesség
  - Nem kell IHL mező ⇨ kisebb fejrész
- Nincs ugrásonkénti tördelés
  - ⇨ nő a feldolgozási sebesség
  - Nem kell ehhez használt mező ⇨ kisebb fejrész
  - MTU felderítés (Path MTU Discovery) kell!!!

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

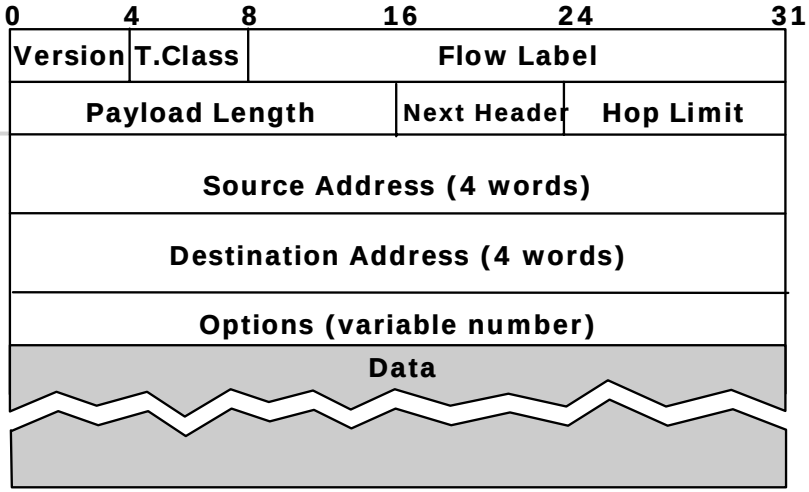
Az IPv6 fejrész mezői I.



- Version – verzió (4 bit)
  - IPv6 esetén 6 (IPv4: 4)
- Traffic Class – forgalmi osztály
  - QoS lehetőség biztosítása az IPv4 Type of Service (ToS) mezőjével megegyező módon
  - Használt elnevezés még a Priority
- Flow Label – folyam azonosító címke (24 bit)
  - Adott kapcsolatot azonosító generált mező
    - Nem független datagrammok!
  - QoS és igazságos adatsebesség megosztást tesz lehetővé
  - Egy forrás-célállomás pár esetén **több folyam** is lehet
    - Adatfolyamot a **cím és a flow label együtt** azonosítja

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IPv6 fejrész mezői II.



- Payload Length – adathossz
  - Nem tartalmazza a fejrészt
  - Maximum 64 KB-os csomag
    - de: jumbogram opció
- Hop Limit – ugrás korlát (8 bit)
  - Megegyezik az IPv4 TTL mezőjével
- Címmezők (2 x 128 bit)
  - 2 128 bites cím
  - A fejrész jelentős része
- Next Header – következő fejléc (8 bit)
  - 2 lehetőség:
    - A beágyazott PDU típusát adja meg
      - Hasonlóan az IPv4 Protocol mezőjéhez
    - Az IPv6 fejléc kiterjesztését jelentő „Extension header” típusát adja

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv6 „opciók” – Header Extensions I.

Célja:

- Az egyszerű fejléc kiegészítése opcionális lehetőségekkel

Típusai:

- **Hop-by-hop Options Header** (0)
  - **Minden közbülső** csomópont is meg kell, hogy vizsgálja
  - Jumbogrammok (óriás-datagrammok)
  - QoS támogatása
- **Routing Header** (43)
  - Routerek felsorolása, amelyeket útba kell ejteni
  - Az IPv4 opciókhoz hasonlóan
    - Laza forrás forgalomirányítás
    - Szigorú forrás forgalomirányítás

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

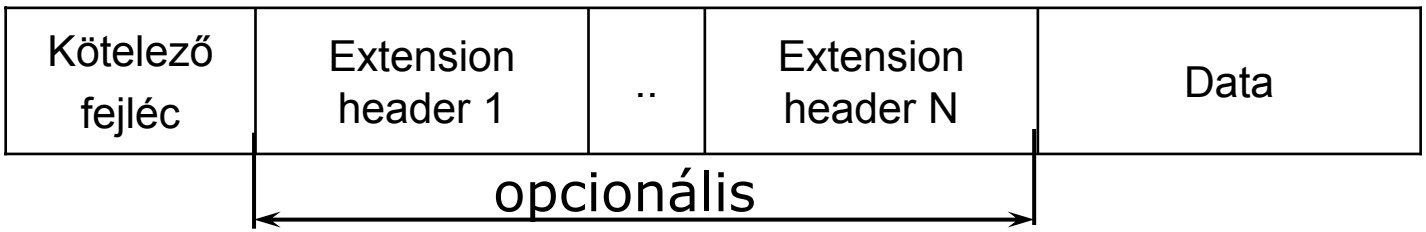
IPv6 „opciók” – Header Extensions II.

- Fragmentation Header (44)
  - Mint az IPv4-ben, de csak a forrás darabolhat
- Authentication Header (AH) (IPSec-ből) (51)
- Encapsulation Security Payload Header (ESP) (50) (IPSec-ből)

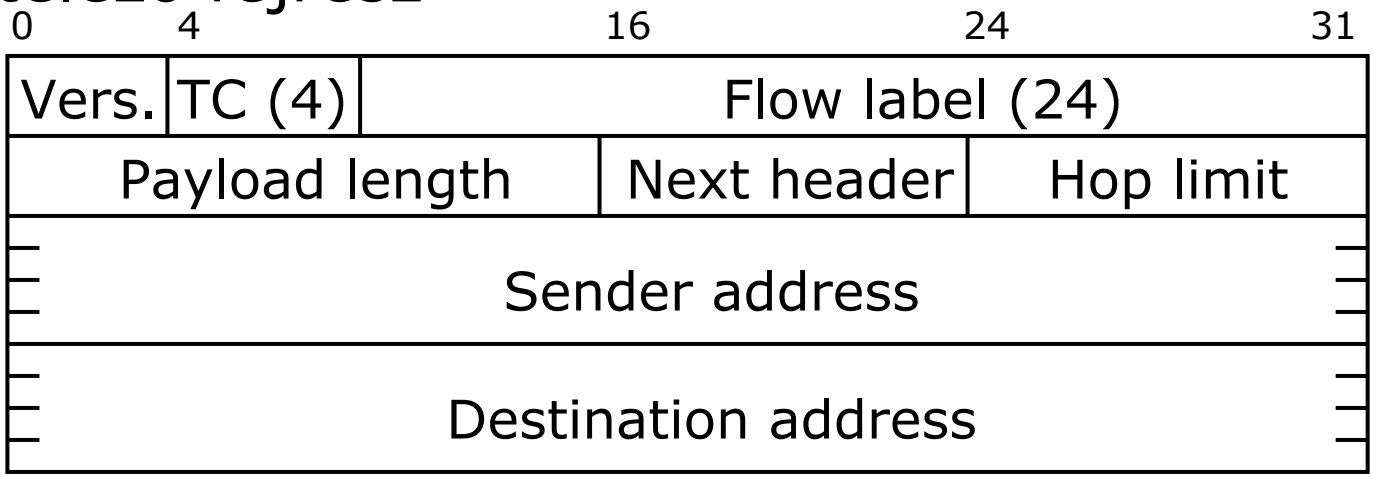
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Az IPv6 fejrész kiterjesztése

Általános fejlécformátum



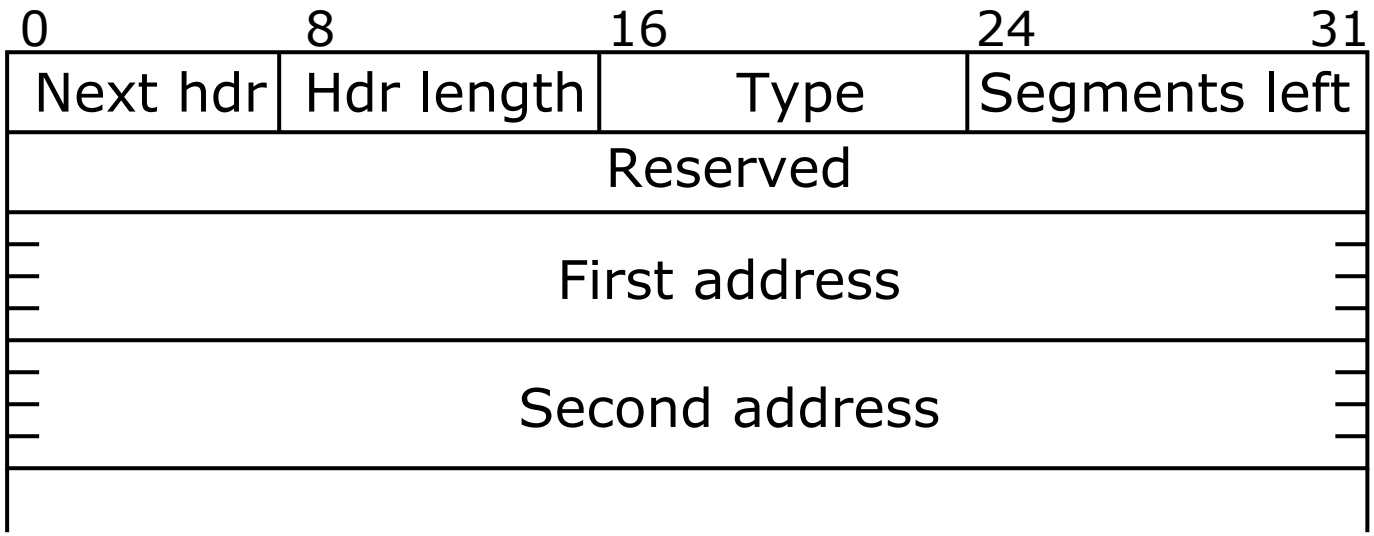
A kötelező fejrész



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Routing Extension

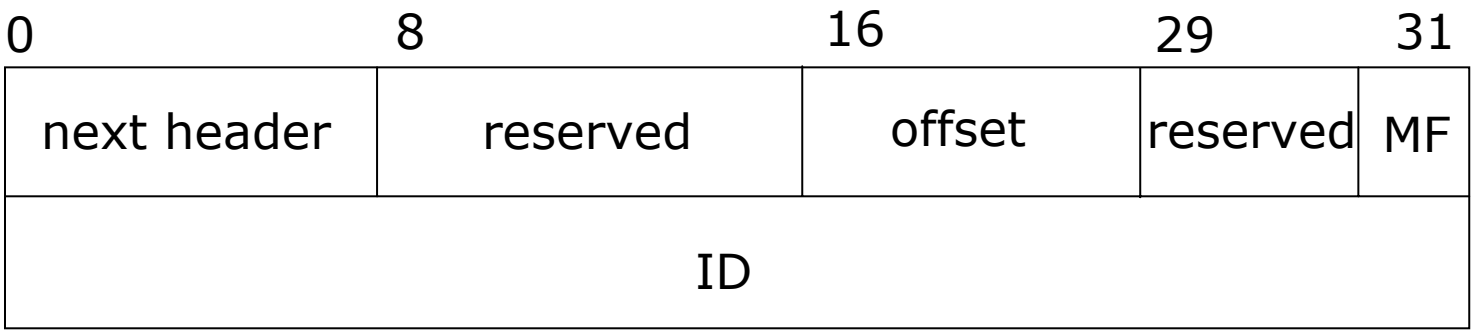
- Az IPv4 opcióhoz hasonlóan
- Header length – fejrész hossza (64 bites szavakban mérve)
- Type - típus
- Az érintendő csomópontok IPv6 címét tartalmazó lista
  - Maximum 24 cím
  - Következő csomópont megtalálása anycast címzéssel



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fragmentation Extension

- Hasonló az IPv4-ben megtalálhatóhoz
  - 13 bites Fragmentation offset
  - More fragment bit (MF)
  - Már 2 nem használt bit
  - 16 bites helyett 32 bites Fragment ID mező, amely a töredéksorozatot azonosítja
- Tördelni csak a feladó fog
- Összeállítani csak a fogadó fog

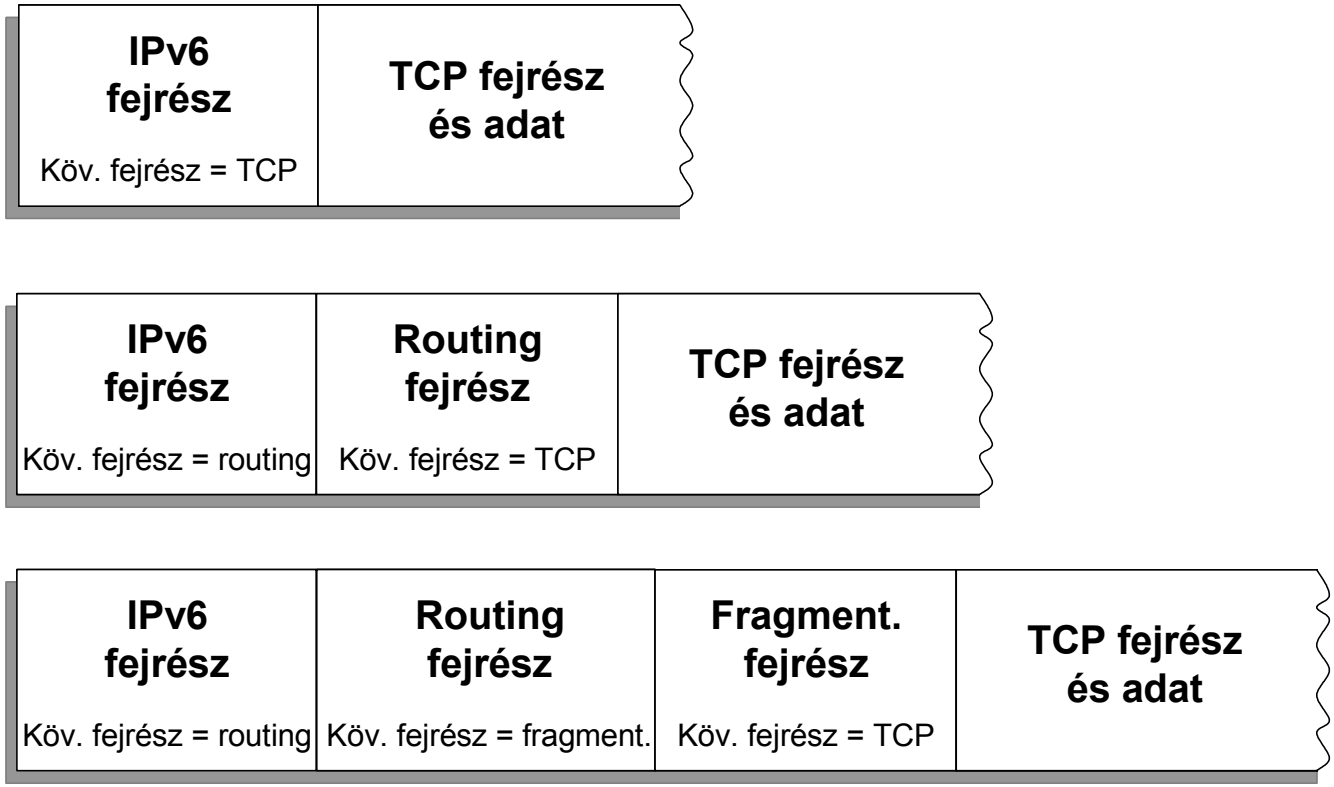


© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPsec az IPv6-ban

- Két Extension Header a biztonság növelésére
- IPSec-re minden IPv6 csomópontnak képesnek kell lennie
- *Authentication Header (RFC 2402)*
  - Valóban a látszólagos feladó küldte-e?
  - Lett-e módosítva a csomag?
- *Encapsulating Security Payload Header (RFC 2406)*
  - Titkosított a csomag tartalma

Példák az IPv6 fejlécre



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IPv6 koncepció

- Megnövelt címtartomány
- Egyszerűbb és rugalmasan bővíthető fejrészformátum
  - Alapfejrész: kevesebb funkció
  - Bővíthetőség opcionális funkciókkal
  - Gyorsabb feldolgozás a csomópontokban
- Erőforrás-allokáció támogatása
- Biztonságos kommunikáció támogatása
- Mobilitás támogatása

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Neighbor Discovery Protocol (NDP)

- IPv4-nél erre szolgált az ARP, ICMP Router Discovery, Redirect
  - Itt egy protokollban minden!
- Szomszédok, routerek felderítése a környezetben
  - ICMPv6 üzenetekkel
- Automatikus címkonfiguráció (Stateless Autoconfiguration)
  - Automatikusan minden beállítást megkap, nem kell DHCP!
  - Stateful: DHCP
- Duplikált cím észlelése

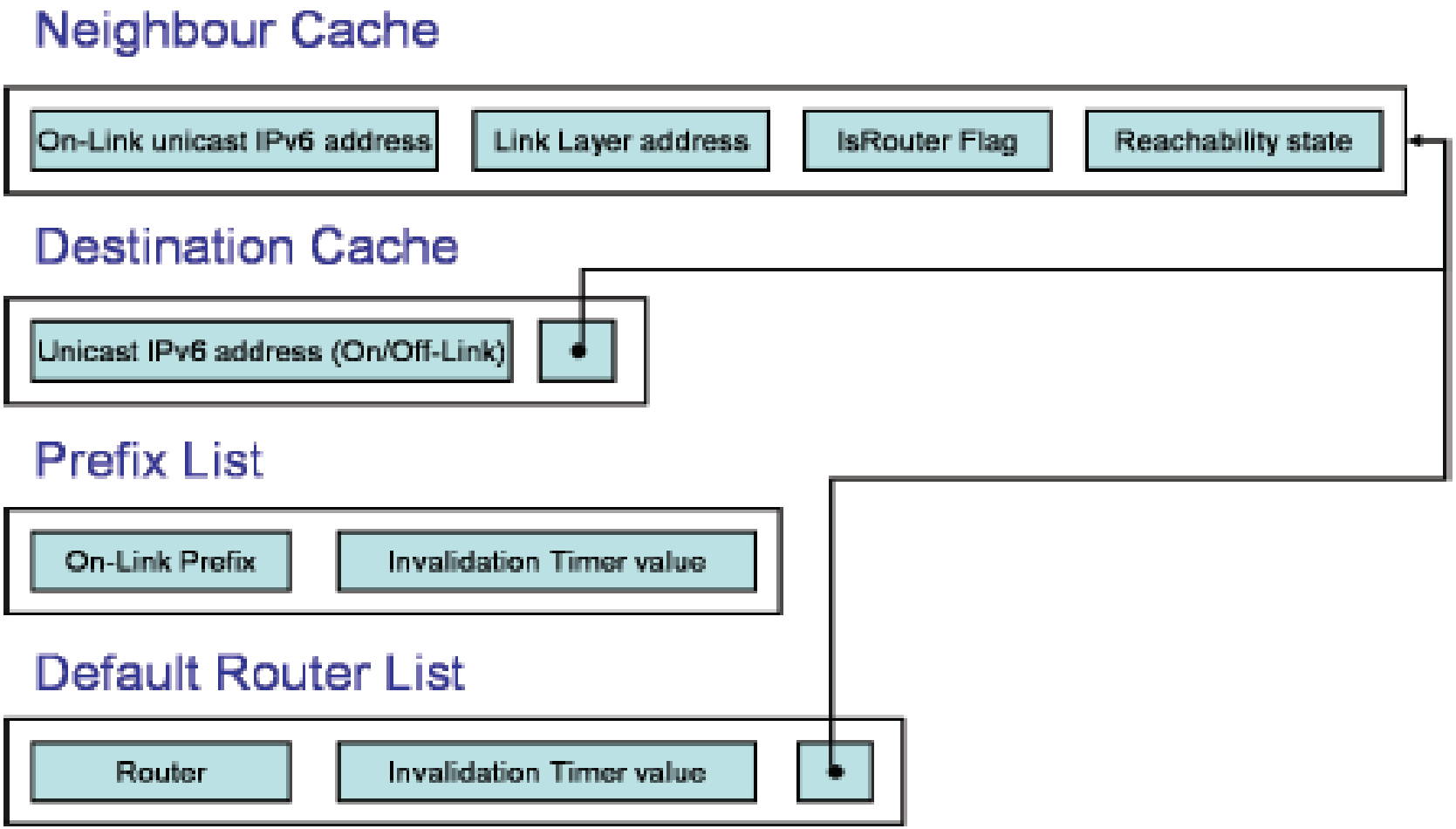
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

ICMPv6 üzenetek NDP-hez

- Router hirdetés (Router Advertisement)
  - Routerek terjesztik a környezetükben
  - Host automatikusan kiépíti a default router listáját
    - Link prefix, link MTU terjesztése
    - Nem manuális konfiguráció, mint IPv4-ben
- Router kérelmezés (Router Solicitation)
- Redirect
  - Routerek megmondják a jobb útvonalakat a hostoknak
- Szomszéd kérelmezés (Neighbor Solicitation)
  - Része az automatikus címkonfigurációnak (ARP helyett)
  - Szomszédok elérhetősége
  - Cím duplikáció felderítés
- Szomszéd hirdetés (Neighbor Advertisement)
  - Pl. új adatkapcsolati cím hirdetése

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

NDP adatbázisok



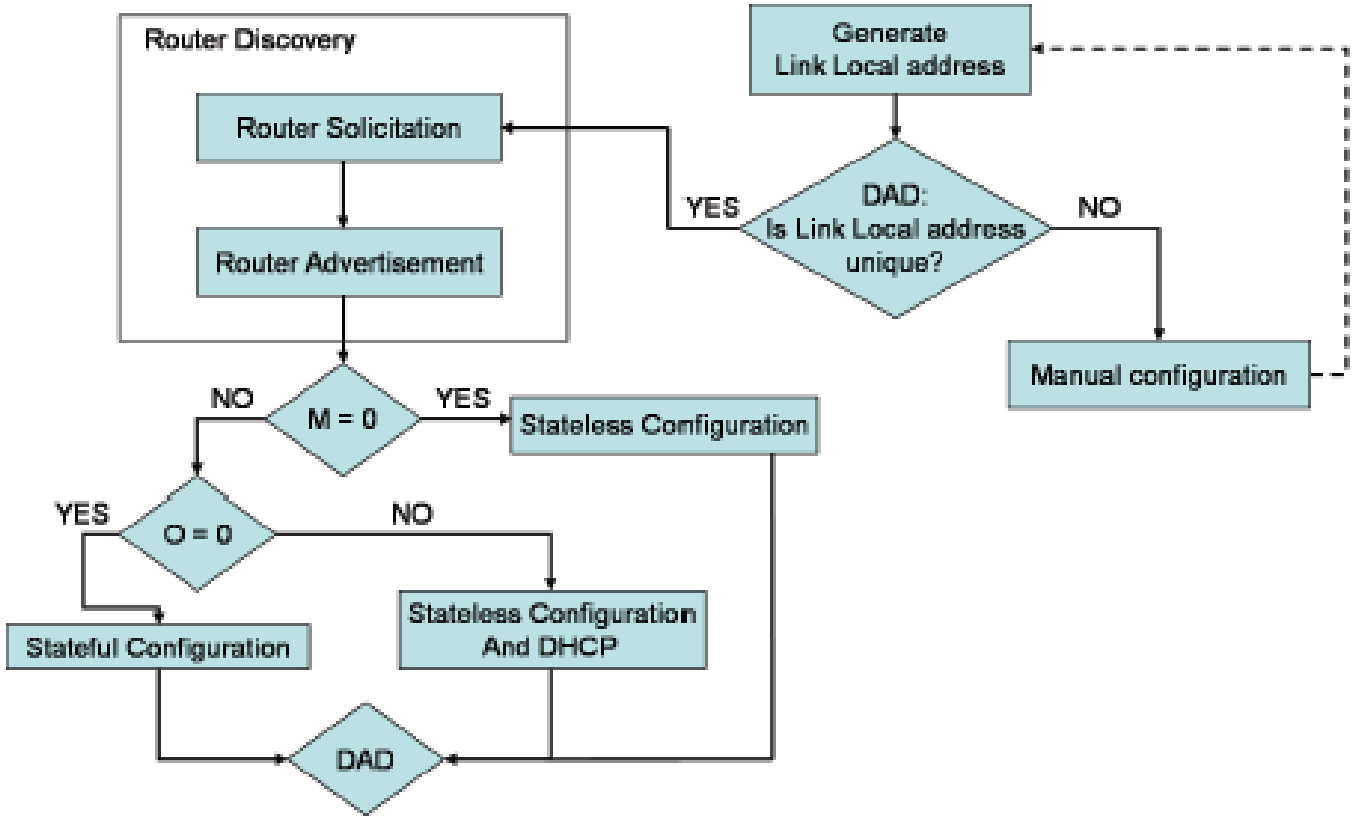
© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Állapotmentes automatikus címkonfiguráció

- Először duplikáció ellenőrzése a host link-local címét illetően
  - multicast szomszéd kérelmezéssel
- Ha egyedi a linken: link-local multicast típusú router kérelmezés
- Routerek hirdetéssel felelnek konfigurációs paraméterekkel
- Cím: **routerek által közölt prefix+link local cím**
- Ha alkalmazásnak nem felel meg: lehet állapotfüggő konfiguráció (DHCPv6)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Állapotmentes automatikus címkonfiguráció



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A szolgáltatásokat lehetővé tevő „eszközök”

- „Okos” routerek
  - DHCP-funkcionalitás
    - IP-címkiosztás koordinálása
    - Hálózati beállítások nyilvántartása
- Anycast címzés
  - Szolgáltatás elérésére
    - Pl.: „Valamely router mondja meg, hogy…”
- Multicast címzés
  - Azonos szolgáltatásokat nyújtó egységek egymás közötti kommunikációja
    - Pl.: „Én már nem vagyok többé router”

IPv6 Routing

Routing protokollok:

- RIPng
- OSPFv3
- IS-IS Extensions for IPv6
- EIGRP for IPv6

- MP-BGP

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MŰEGYETEM 1782

BME

Áttérés IPv6-ra

Rengeteg megoldás, mégse megy gyorsan?

2013.Április 9.

Pillanatnyi helyzet

- 2008-ban ünnepelték az IPv6 10 éves születését
- Az IPv6-os forgalom aránya elérte az Interneten 1 % -ot (2012 november)

- Okok:
  - Kevés IPv6-os szolgáltató (ISP)
  - Kevés IPv6 kompatibilis alkalmazás és szolgáltatás
  - Még mindig nincs igazi kényszer az áttérésre!
    - Már van☺

- Nagy lökések az áttéréshez:
  - Pekingi olimpia 2008
  - 4G mobil cellás rendszerek: hang VoIPv6

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Már létező IPv6 alkalmazások

- Hálózatban:
  - Routing protokollok
  - DNS (A6, AAAA és DNAME rekordokkal)
  - DHCP6
  - …
- Operációs rendszerekben régóta (az alábbiakban és ennél újabbaknál):
  - Windows XP SP1, Windows Server 2003
  - Mac OS X 10.2
  - Debian Linux 2.1.8, Redhat 2.1, Solaris 8
  - FreeBSD 4.0, OpenBSD 2.7, NetBSD 1.5, BSD/OS 4.2
- Tűzfalak:
  - ip6fw (FreeBSD)
  - E-Border (kereskedelmi)
  - …
- Alkalmazások:
  - JAVA IPv6 (JDK1.4 óta)
  - 3GPP
  - …

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

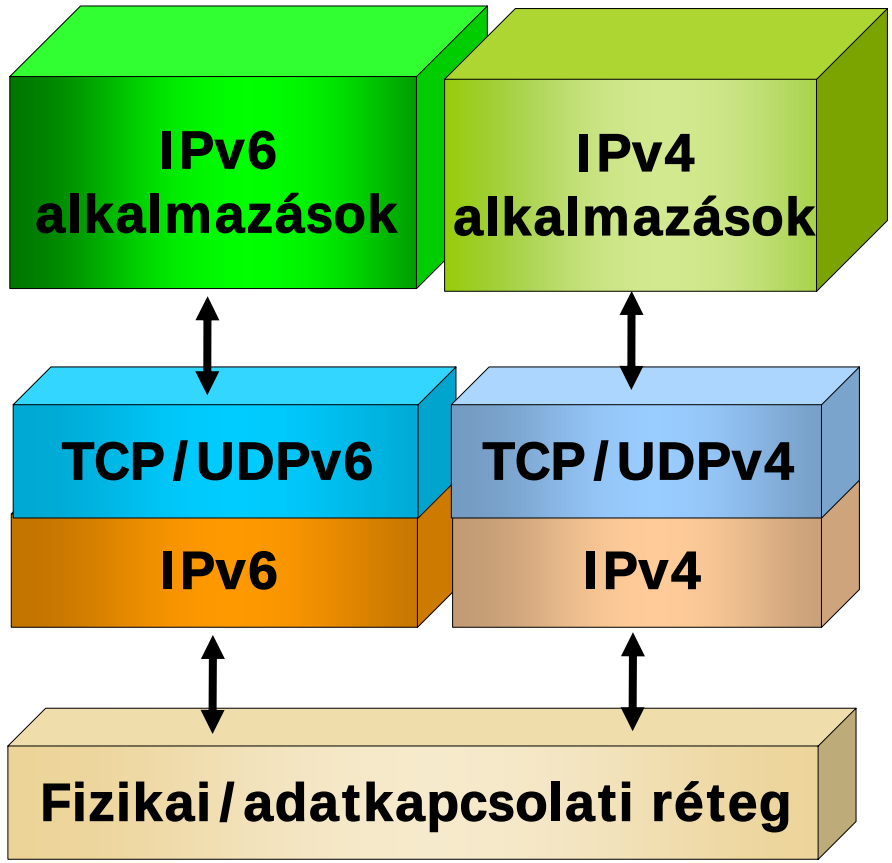
IPv6 kompatibilis IPv4 címzés

- „Compatible”
  - 96 0 bit után az IPv4 cím
- „Mapped”
  - 80 0 bit után 16 1-es bit, majd az IPv4-cím
- Címfordítás menet közben

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Áttérés Dual Stackkel

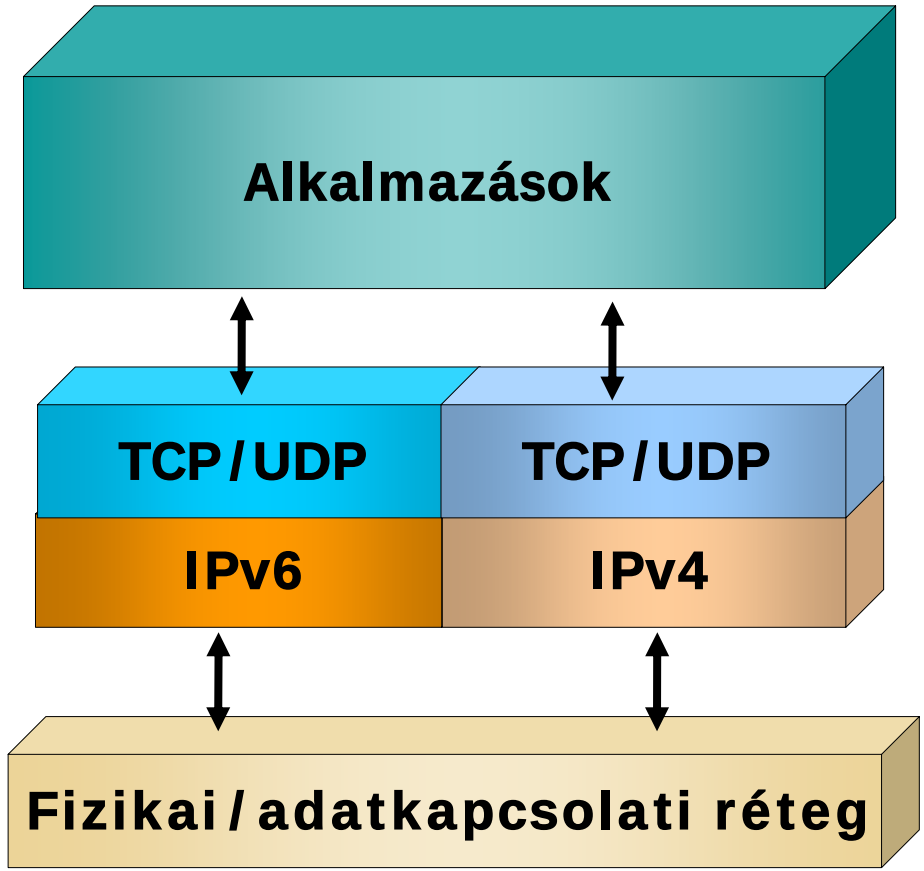
- A csomópontok egyszerre IPv4 és IPv6 csomópontok
- IPv6 más IPv6 rendszerekkel való kommunikációhoz, de képesek visszalépni IPv4 módba régi rendszerekhez
- Protokollválasztás: DNS szerver IPv6 vagy IPv4 címmel válaszol
- A legtöbb IPv6 implementáció ezt használja



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Áttérés Dual Layerrel

- A csomópontok egyszerre IPv4 és IPv6 csomópontok.
- De a szállítási réteg megmarad.
- Így több alkalmazás működne, ha nem használ IP-címeket.

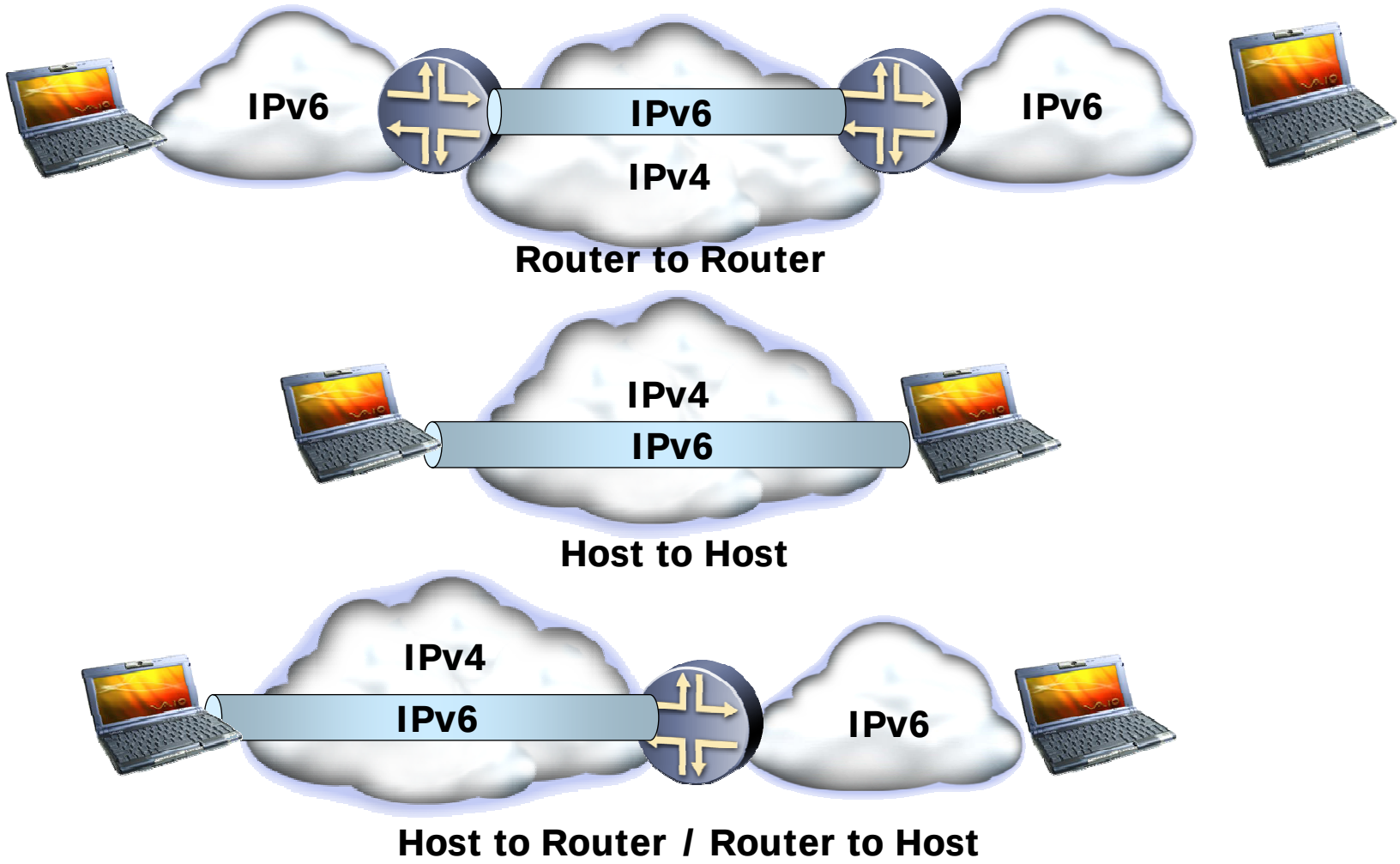


Áttérés alagutazással (Tunneling)

- Beágyazása az egyik protokoll változatú csomagnak a másikba
  - Mintha adatkapcsolati rétegbeli protokoll lenne az egyik
- IPv4 hálózaton IPv6-os csomagokat szállítunk
  - Végpontok már IPv6-képesek, de a hálózat még nem
  - 6to4: IPv4-es célcím cím az IPv6-os cím prefixében
    - elterjedt
  - 6in4: statikus alagút-végpont konfiguráció
- IPv6 hálózaton IPv4-es csomagokat szállítunk
  - Hálózat már IPv6-os, de a végpontok még nem

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alagutazás lehetőségei (Tunneling)



Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

IP - Mobil IP

Hogyan érnek utol a csomagok?

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

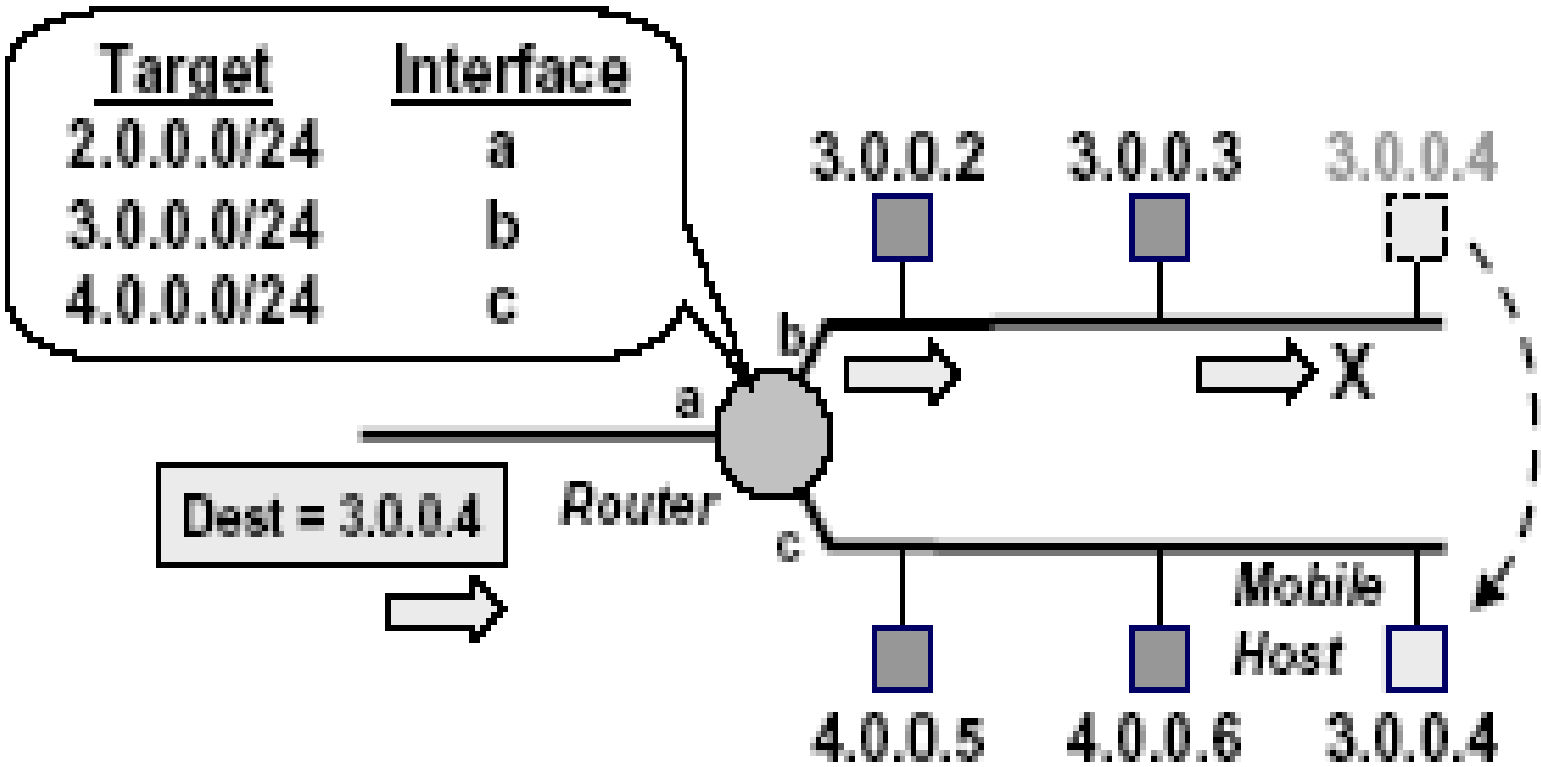
2013.Április 11.

Probléma

- Gyakori a mozgó vagy nomád Internet-felhasználás
- Az IP-címét a felhasználó meg kívánja tartani
  - viszont az IP-cím fizikailag kötött
  - ennek alapján történik a routing
- Így az IP cím egyszerre *azonosító és helymeghatározó* (lokátor) is
- Hogyan kaphatja meg mégis a csomagot?

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Hagyományos routing mobil csomópont esetén



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mobil IP - áttekintés

- Mi az a mobil IP?
  - Módosítás az IP-rétegben
    - csomópontok attól függetlenül képesek folyamatosan adatok fogadására/küldésére, hogy éppen hol kapcsolódnak a hálózatra
- Mobilitás?
  - Olyan mozgó csomópontoknak találták ki, amelyek **legfeljebb kb. másodpercenként** változtatják hozzáférési pontjukat
  - A protokoll jól működik, amíg a mozgás sebessége nem éri el a mobil IP vezérlő üzeneteinek oda-vissza idejét
  - Mobilitás: nem csupán mobil állomások, hanem egész **mobil hálózatok**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mobilitás kezelése IPv4-ben

- Hierarchikus címzés: egyszerre globális azonosító és hely azonosító
- Megoldás: az otthontól távol lévő *mobil állomás két címmel* rendelkezik
  - home address (HA)
  - care of address (CoA)
- Két új hálózati funkcionalitás bevezetése
  - home agent (HA) (otthoni ügynök)
  - foreign agent (FA) (idegen ügynök)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Terminológia

- ***Mobile node:*** kapcsolódási pontját változtató (mobil) eszköz
- ***Home agent*** *(otthoni ügynök):*
  - a mobil csomópont otthoni hálózatában lévő ügynök
  - „tunnelezi” a csomagokat a távolban lévő mobil csomóponthoz
- ***Foreign agent*** *(idegen ügynök)*
  - ügynök a csomópont jelenlegi hálózatában
  - felelős az adatok továbbításáért a csomópont felé, amíg az ebben a hálózatban tartózkodik
- ***Home address:*** a mobil csomópont otthoni IP címe (**~permanens IP cím**)
- ***Care-of address:*** az idegen hálózatban kapott cím

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Regisztráció

- Ha a mobil csomópont távol van:
  - regisztráltatnia kell a care-of címét az otthoni ügynökénél
    - történhet közvetlenül, vagy az idegen ügynök igénybevételével is
    - **regisztrációs kérelem: HA címe, saját cím, igényelt CoA, ennek élettartama**
- Ha a FA a HA-nak továbbítja, ez
  - elfogadja, ekkor frissíti a **CoA-node – IP-cím** összerendelést, vagy
  - visszautasítja:
    - túl hosszú igényelt időtartam
    - elérhetetlen otthoni hálózat
    - elérhetetlen otthoni ügynök port
    - túl sok összeköttetés, stb.

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mi lesz a care-of address?

Kétféle módon lehet „care-of address”-t szerezni:

- care-of address = a foreign agent címével, ekkor a tunnel vége a foreign agent
  - Előnyös, mert kevés címet használ fel a szűkös címtartományból
  - Ekkor a FA saját listán tárolja a csatlakozott idegen mobilok IP címét
- egy helyi IP címet utalunk ki a mobil csomópontnak: co-located care-of address
  - dinamikusan (DHCP)
  - ekkor a tunnel vége a mobil csomópont

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mobil IPv4 alapműveletek 1.

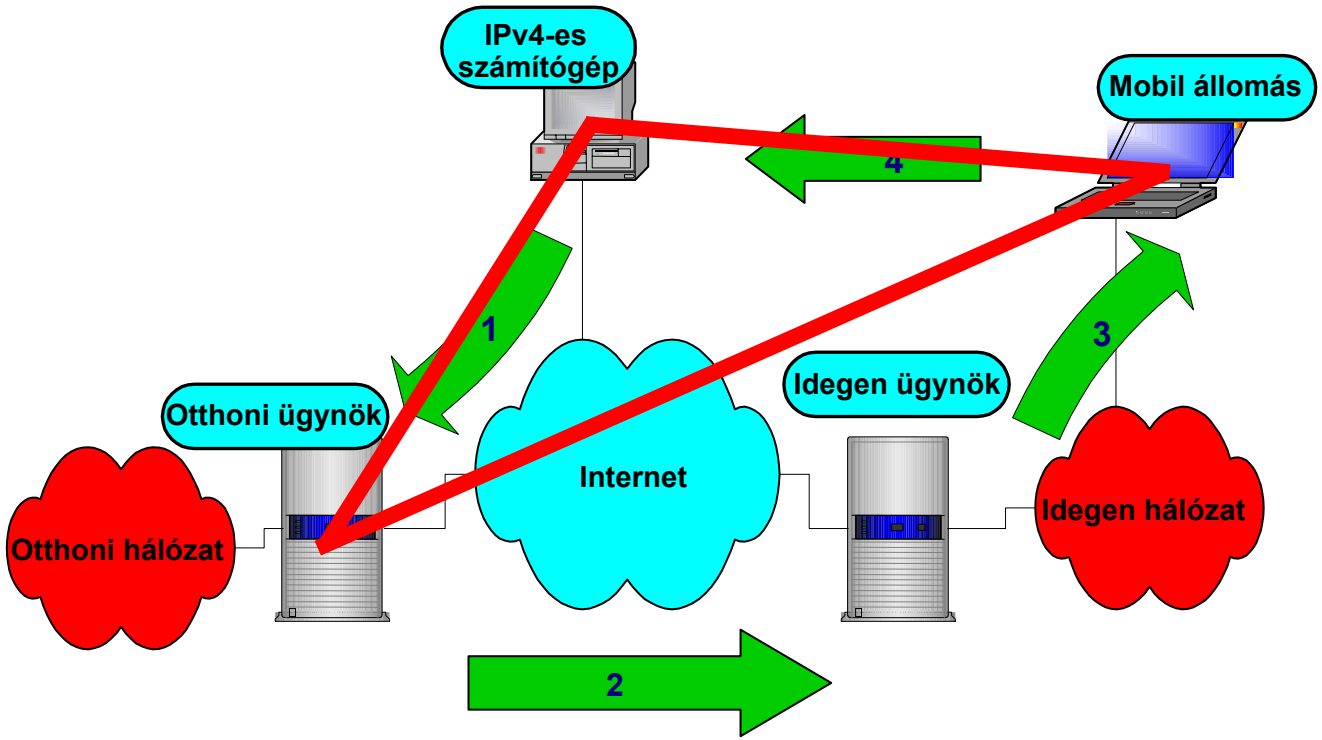
- A mobil (idegen és otthoni) ügynökök hirdetik magukat
  - ICMP Router Discovery
- Mobil csomópont veszi a hirdetéseket és eldönti, hogy otthoni vagy idegen hálózatban tartózkodik
- Amennyiben hazatért: **kiregisztrálja** magát az otthoni ügynökénél
- Ha idegen hálózatban van, care-of címet igényel:
  - Idegen ügynök care-of cím
  - Co-located care-of cím

Mobil IPv4 alapműveletek 2.

- Azt észleli, hogy idegen hálózatban van: a mobil csomópont regisztrálja az új care-of címét az otthoni ügynöknél
  - lehetőleg idegen ügynökön keresztül
- Otthoni ügynök fogadja a neki címzett üzeneteket és a **regisztrált care-of címére „alagutazza” (tunneling) őket**
- Megjön a csomag
  - az idegen ügynökön keresztül
  - közvetlenül (co-located)
- A mobil csomagjai visszafelé mehetnek közvetlenül is

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A Mobil IPv4 működési elve

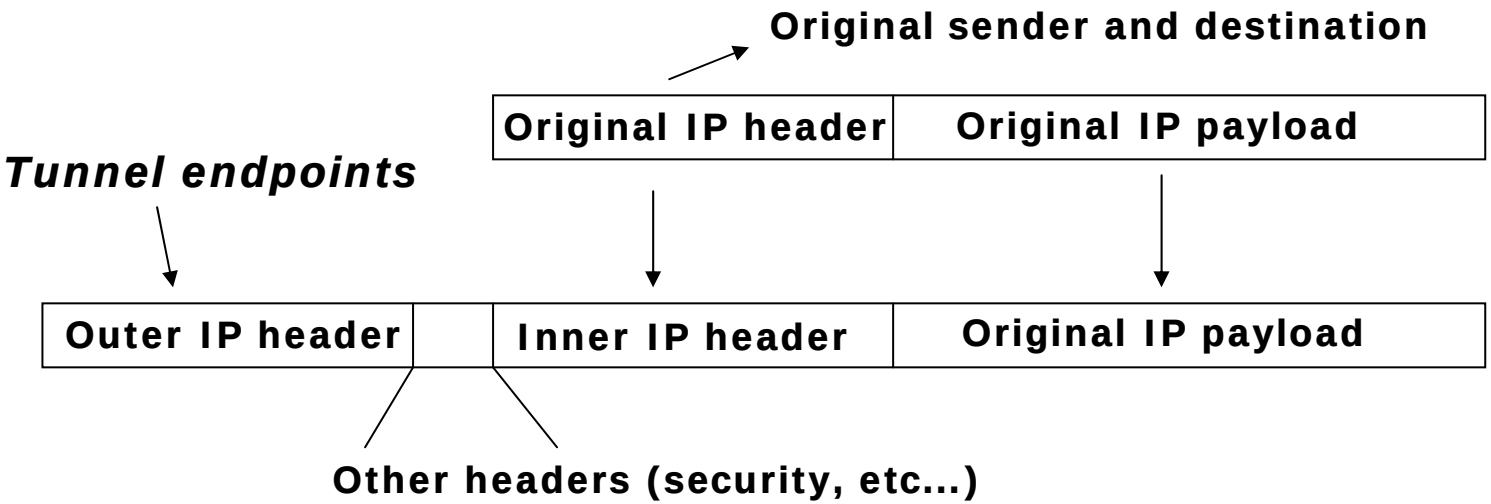


© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Becsomagolás & alagútazás

- *Becsomagolás (encapsulation):*
  - a HA a node számára érkező IP csomagot új fejrésszel látja el és úgy küldi tovább
- *Alagútazás (tunneling):*
  - a HA továbbítja a CoA–ra a mobilnak szóló csomagot
    - egyfajta alagutat hozva létre a hálózatban
    - a küldő úgy látja, hogy ezen az alagúton keresztül közvetlenül eléri a címzettet a csomag

Becsomagolás



Ez a legegyszerűbb becsomagolás
Nem hatékony, mert ismételt mezők a belső és külső fejben
Megoldás: „minimal encapsulation”

Minimális becsomagolás

- A „belső” fejlécből csak pár mezőt tartunk meg:
  - Protokoll (változatlan)
  - Eredeti forrás- és célcím
  - Ellenőrző összeg: csak „belső fejlécre”
  - S flag: tartalmazza-e az eredeti forrás címet
    - Ennek függvényében 8 vagy 12 byte

- „Külső fejléc”:
  - változó forrás- és célcím
    - alagút végpontjai
  - inkrementált Total Length
    - 8 vagy 12 byte

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Gond a Mobil IPv4-el

- Háromszög probléma

- Érdekes eset:
  - A mobil csomópont és a vele kommunikáló csomópont egy hálózatban vannak, de nem a mobil otthoni hálózatában
  - Minden alkalommal az otthoni ügynökön keresztül kell kommunikálni: jelentős késleltetés!

- Megoldás: Route Optimization

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Útvonal optimalizálás (Route Optimization)

- A mobillal kommunikáló csomópontban:
  - Binding Cache (kötéstár) mobil otthoni és CoA címének összerendelése
  - Így közvetlenül neki küldheti a csomagot a HA kikerülésével
  - Minden ilyen bejegyzésnek élettartama van

- Amennyiben nincs ilyen bejegyzés
  - a HA-nek küldi, majd az értesíti egy Binding Update (BU) üzenettel a mobil CoA címéről

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Gond a Mobil IPv4-el

- **Ingress filtering**: a hálózat csak akkor fogadja vagy adja tovább a csomagot ha jóváhagyott címről érkezik
  - Egress filtering: kifelé menő forgalomra

- Amennyiben a hálózat gateway routere ilyen szűrést használ:
  - megköveteli hogy MN forráscíme az idegen ügynök alhálózatához tartozzon
  - Vagy eldobja ellenkező esetben

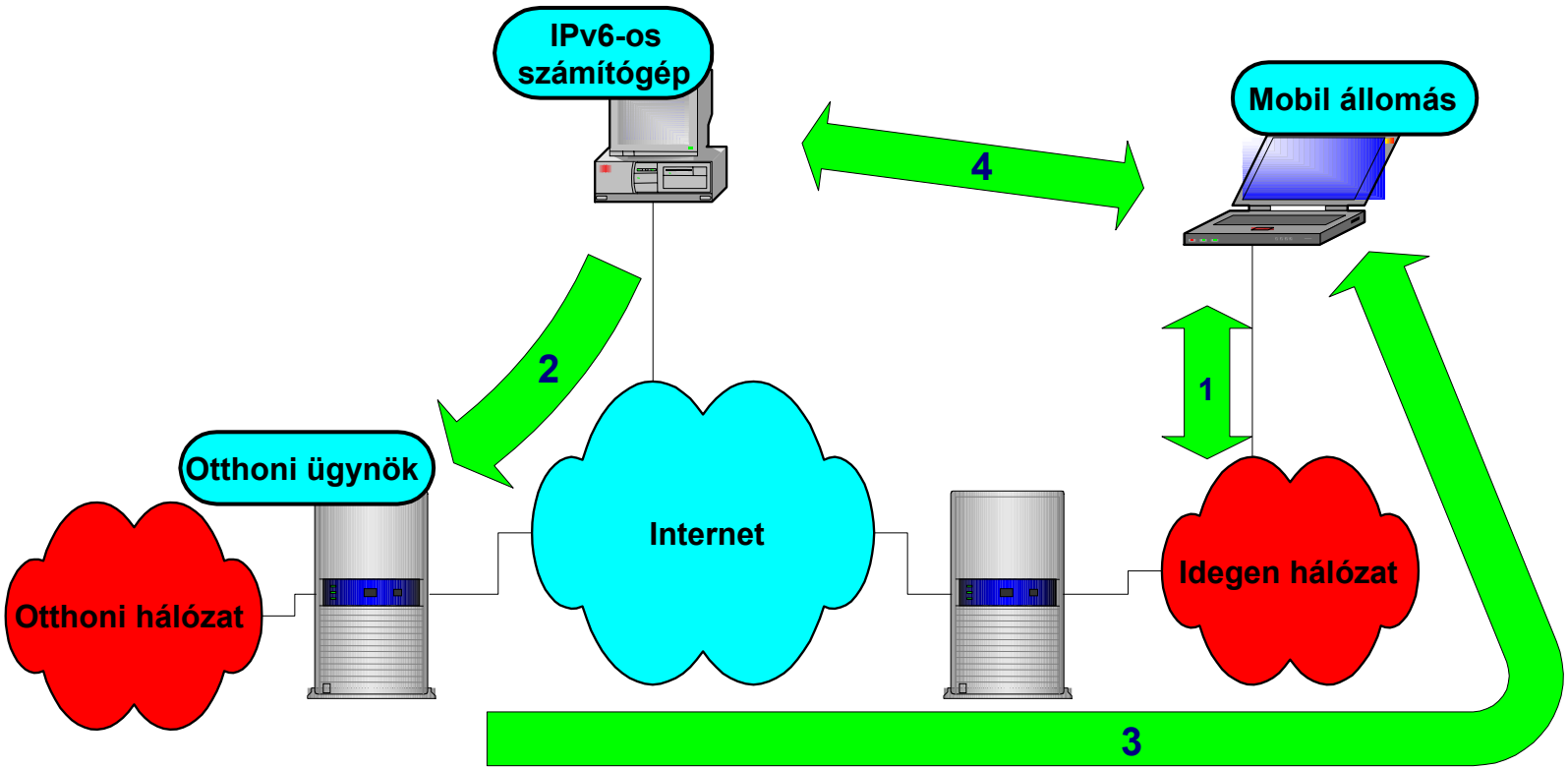
- Megoldás: **reverse tunneling**
  - FA visszaalagútazza a MN csomagjait a HA-nek, az továbbítja a vele kommunikáló csomópontnak
  - Komoly késleltetést jelenthet

Mobil IPv6

- Az **útvonal optimalizálás** az IPv6-ban nem opcionális kiegészítés hanem alapvetővé lépett elő
  - nem minden csomópont támogatja IPv4-ben
- A háromszög probléma leküzdése
  - Kommunikáló állomás: Kötés tároló (Binding Cache)
  - Mobil állomás: Kötés lista (Binding List)
- Kötések (Binding) létrehozása
  - Kötés frissítés (Binding Update)
  - Kötés nyugta (Binding Acknowledgement)
  - Kötés kérés (Binding Request)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Mobil IPv6 alapvető működése



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A Mobil IPv6 egyéb előnyei

- Nem kell idegen ügynök
  - Address autoconfiguration, Neighbor Discovery

- MN automatikusan észleli, hogy új hálózatba került:
  - új router hirdetésekből
  - vagy lejárt a régi routerek hirdetése és nem kapott tőlük újat
- Utóbbi esetben MN router kérelmezést küld
  - erre jövő hirdetésekből megszerzi a CoA címet
    - hirdetett prefixből

- Regisztrálja a CoA címét az otthoni ügynökénél Binding Update-el
- Otthoni ügynök felel majd a neki érkező Neighbor Solicitation üzenetekre is

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A Mobil IPv6 egyéb előnyei

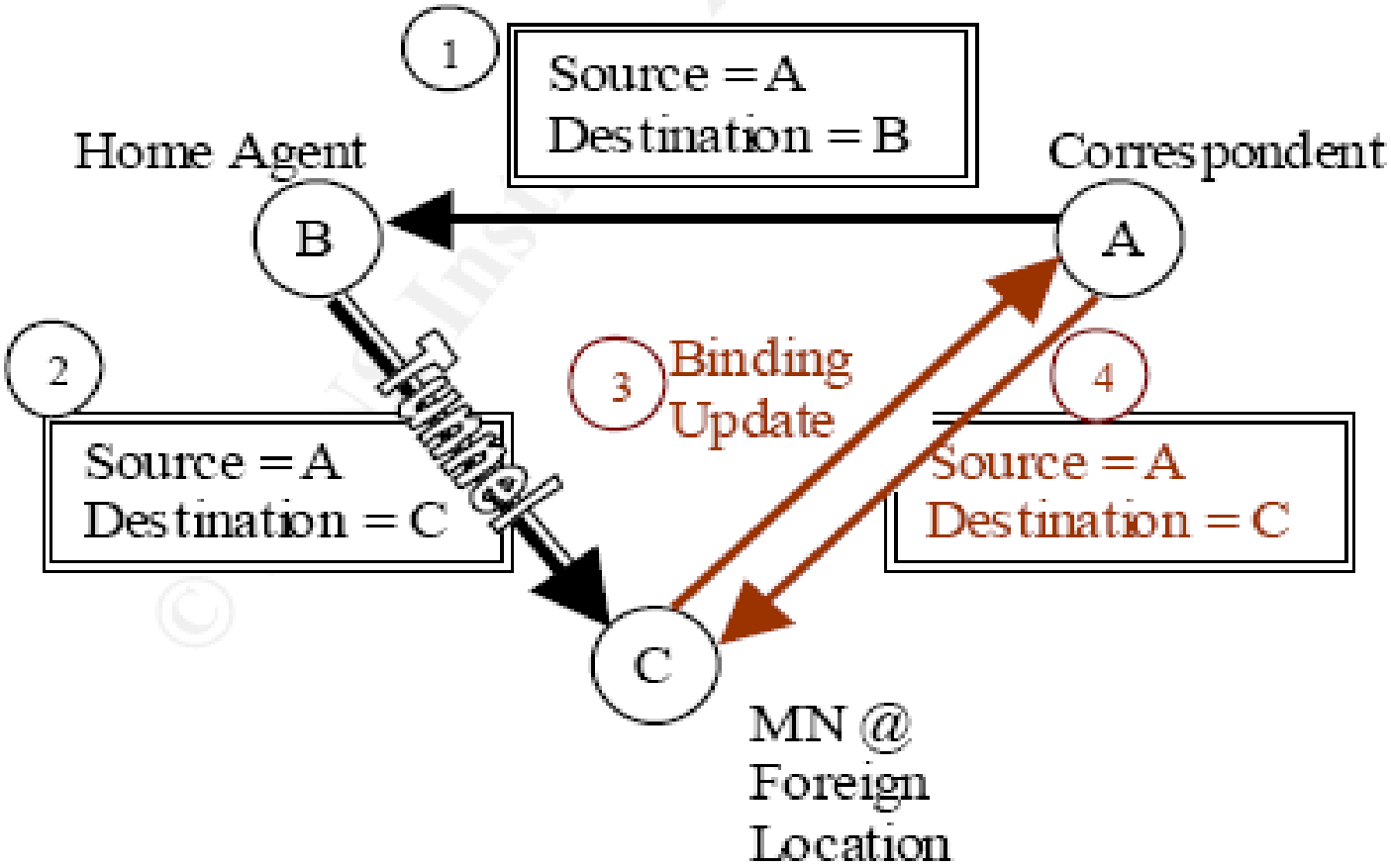
- Mobil IPv4-ben a MN amikor másik csomóponttal kommunikál:

  csomag forráscím=otthoni cím

  - Nincs ingress filtering probléma
  - Mobil IPv6-ban forrás cím=care of cím
  - A mobil csomópont otthoni címe egy Otthoni Cím cél opcióban kerül továbbításra

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Route optimization



Új üzenetek MIPv6-ban?

- Nem kell új üzenetformátum: Destination Options fejléc kiterjesztés
- Csak a csomag címzettje vizsgálja

  - Binding Update
  - Binding Acknowledgement
  - Binding Request

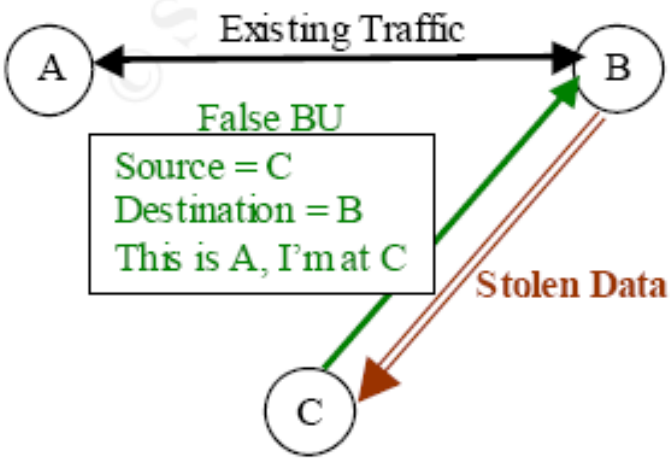
Otthoni ügynök felderítés

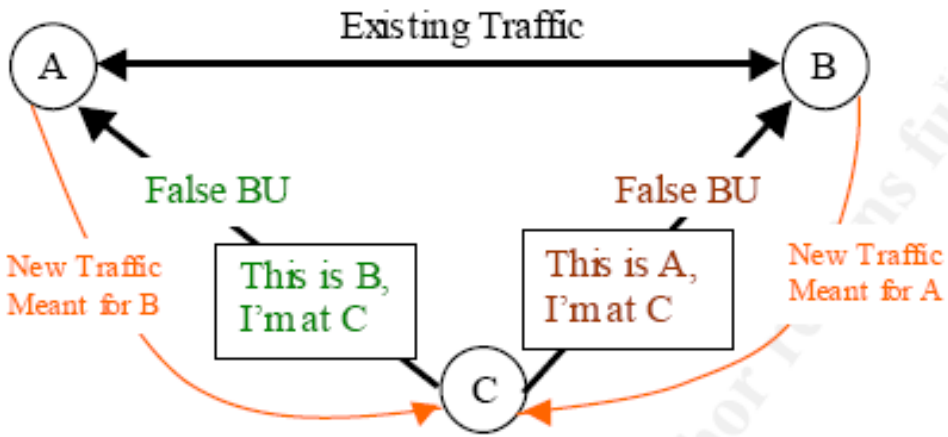
- MN egy Binding Update üzenetet küld az otthoni ügynök anycast címre
- Binding Acknowledgement jön vissza az otthoni ügynökök listájával és preferenciájukkal
  - legközelebbi válaszol
- Ezekből választ a MN a preferencia alapján

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Biztonság Mobil IPv6-ban

- Biztonság aggály Mobil IPv6-al szemben:
  - Binding Update-k hamisítása
    - ***Man-in-the-Middle támadás***
    - ***Denial-of-Service támadás***





© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Biztonság Mobil IPv6-ban

- Eltérően az IPv4-től, a Mobil IPv6-ban IPsec alkalmazása Binding Update esetén:
  - küldő hitelesítés (sender authentication)
  - adatintegritás-védelem (data integrity protection)

- A Mobil IPv4-nél saját biztonsági mechanizmus
  - statikusan konfigurált ”mobilitás biztonsági összerendelések (mobility security associations)”

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Becsomagolás - Tunneling

- Nem IP becsomagolás (encapsulation), hanem IPv6 Útvonalválasztó fejléc (Routing header) használata

- A Mobil IPv4 valamennyi csomagot becsomagolással továbbítja
- Az útvonalválasztó fejléc használata kevesebb fejléc bájtot igényel: csökkenti az overheadet

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Problémák a mobil IP-vel

- Hozzáférési pont váltások miatt nagy jelzésforgalom (BU üzenetek), adminisztráció
- A jelzési üzenetek késleltetése nem megfelelő real-time (késleltetés-kritikus) alkalmazásokhoz
- Magas csomagvesztési arány (QoS)
- Felesleges hálózati többletterhelés

Megoldási lehetőségek

Jelzésforgalom csökkentése, a címváltozások kezelése „helyben”

Handover gyorsítása (QoS növelés)

Helyzetinformáció titkossága

- Makro – mikro mobilitás (CIPv6)
- Handoverek javítása (FMIPv6)
- Hierarchikus mobilitáskezelési megoldások (HMIPv6)
- Mobil hálózat mozgásának kezelése (NEMO)

Mobil IP pillanatnyi alkalmazása

- Vezetéknélküli LAN-ok közötti váltásnál IP felett (WLAN, WiMAX)
- 3G mobil rendszerekben nem használják cellaváltásnál
  - adatkapcsolati megoldások vannak
  - de különböző domainek közötti váltásnál igen
- A 4G-ben is számolnak vele
  - Pl. az LTE demonstráción HDTV streaming (>30 Mbit/s) Mobile IP alapú váltás LTE és HSPA hálózat között

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

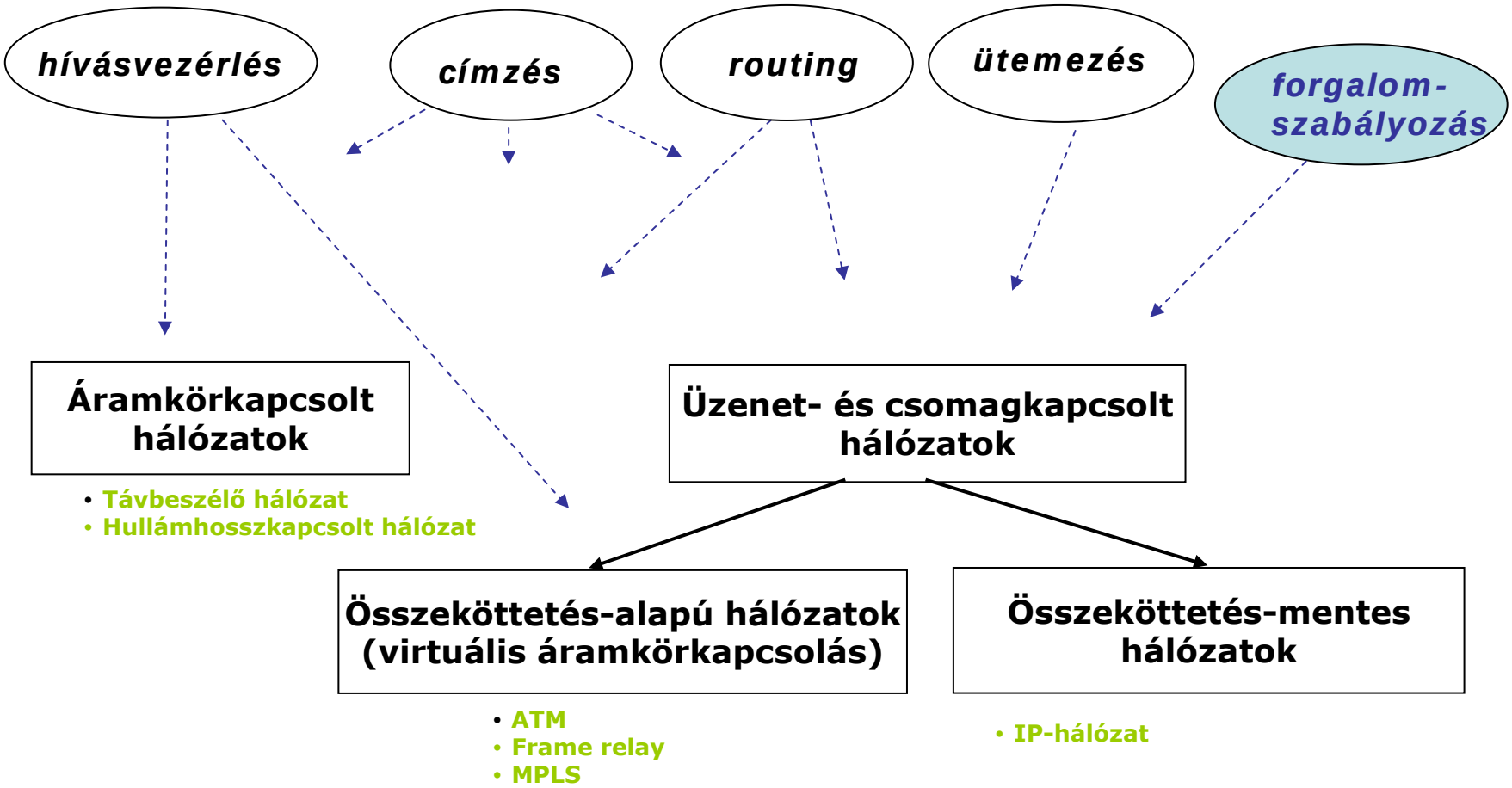
FORGALOMSZABÁLYOZÁS

Flow control

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.Április 16.

Újabb fontos funkciók és alapelvek



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Definíció és a feladat meghatározása

- Két rokon feladat:

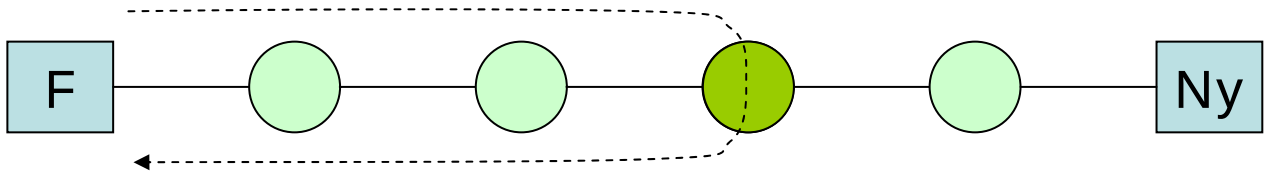
- Forgalomszabályozás (*flow control*):
  - Módszerek, amelyek lehetővé teszik, hogy egy adatforrás az **aktuális átviteli sebességét illessze** a vevőnél és a hálózatban rendelkezésre álló kiszolgálási sebességhez

- Torlódásvezérlés (*congestion control*):
  - Azok a módszerek, amelyekkel linkek, csomópontok időszakos túlterheltségét megkíséreljük megszüntetni
    - A torlódásvezérlést értelmezhetjük általánosabban is: azok a módszerek, amelyekkel meg is lehet előzni a torlódásokat
    - Ebben az értelemben a *flow control* tekinthető a *congestion control* eszközének
      - előzzük meg a torlódást, mielőtt az bekövetkezne

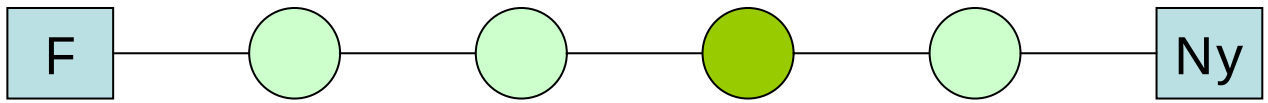
© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A működés egyszerűsített vizsgálata

- Korlátozódjunk egyetlen forrásra:
  - A csomagok több csomóponton jutnak a nyelőhöz



  - Az út mentén valahol kialakul egy szűk keresztmetszet, „bottleneck”
  - A többi csomópont elfelejthető a forgalomszabályozás modellezése szempontjából



(A késleltetéshez természetesen valamennyi csomópont hozzájárul)

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A forgalomszabályozás kívánatos jellemzői

- Az alapvető cél megvalósításán túl:
  - Legyen egyszerűen megvalósítható
  - Lehető legkevesebb hálózati erőforrást vegyen igénybe
  - Hatékonysága ne függjön a szabályozott források számától
  - Biztosítsa a szabályozott források **igazságos részesedését** az igénybe vett erőforrásokon
  - Stabil legyen a működése

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A forgalomszabályozás fajtái

- Két jelentős csoport:
  - „Nyílthurkú” – nincs visszacsatolás
  - „Zárthurkú” – van visszacsatolás
- Lehetséges a kettő kombinációja is (hibrid)

- Nyílthurkú:
  - A kommunikáció előtt a felhasználó és a hálózat forgalmi paramétereket egyeztet
  - A hálózat dönt az új összeköttetés elfogadásáról
    - *admission control, beengedésszabályozás*
  - Ennek megfelelően a hálózat **erőforrásokat dedikál**
  - A működés során a **paraméterek ellenőrzése**

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Nyílthurkú szabályozás

- **Forgalomleírók (traffic descriptors):**
  - Egy paraméterkészlet, amely jellemzi az adatforrás viselkedését, továbbá
  - alapját képezi egy *szolgáltatási szerződés forgalmi részének*

- Egyszerű példák forgalomleírókra:
  - csúcssebesség
  - átlagsebesség

- A forgalomleírók bemenő adatai:
  - a forgalomszabályozónak (regulator), valamint
  - a felügyelőnek (policer)

A *regulátor* tipikusan késlelteti a túlzott forgalmat, míg a *policer* inkább eltávolítja

Zárthurkú szabályozás

- Feltétlenül szükséges, ha:
  - nincs erőforrás-foglalás
  - túlfoglalást (*overbooking*) alkalmazunk statisztikus nyereség elérése érdekében
- Típusai:

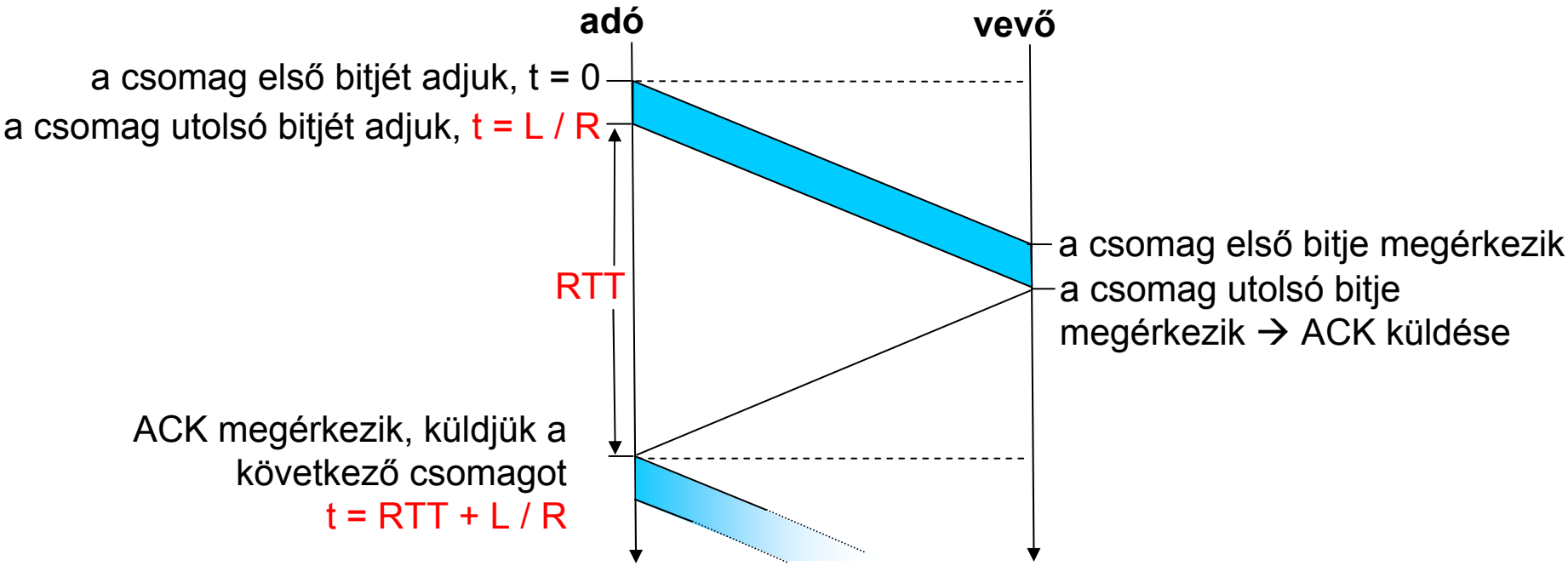
1. generáció (csak a nyelő képessége)	**ki – bekapcsolás (on-off)**		
	stop-and-wait		
	statikus ablak (static window)		
2. generáció (a nyelő és a hálózat képessége)	**állapot vizsgálat**	**vezérlés módja**	**vezérlés helye**
	explicit	**din. ablak**	**végpont**
	implicit	**din. seb.**	**lépések**

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A felsorolt módszerek

- *On-off:*
  - a nyelő engedélyezi az adást
- *Stop-and-wait:*
  - a küldő egy csomag után vár a nyugtára
- *Statikus ablak:*
  - a küldő az ablak méretével megadott számú csomag elküldése után vár csak nyugtára
- *Második generációs módszerekre a protokolloknál látunk majd példát*

A stop-and-wait működése



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

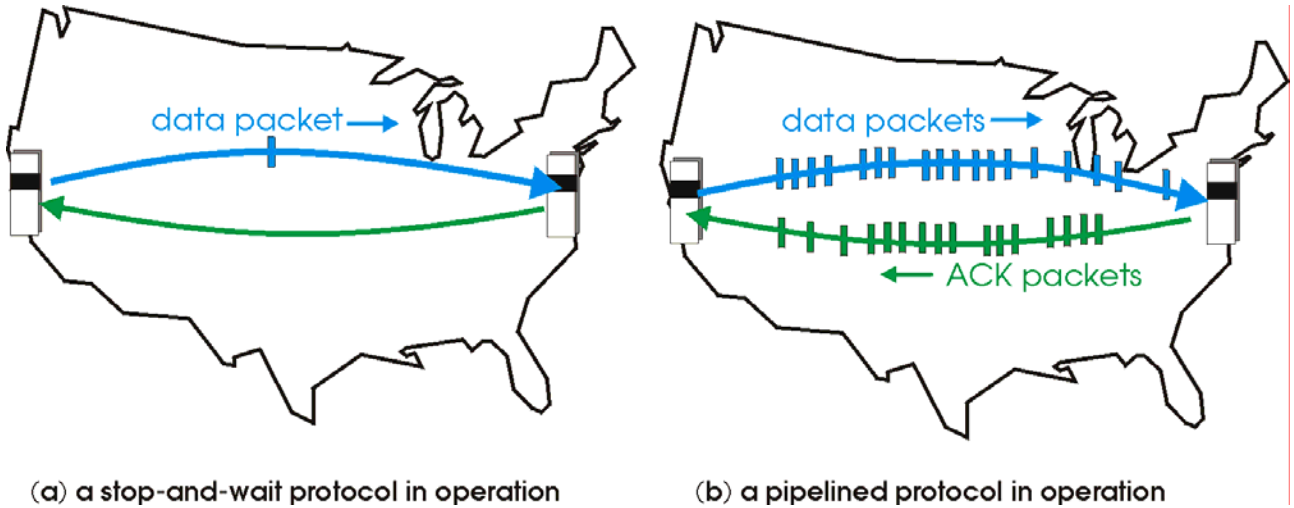
RTT: round-trip-time (teljes körbefordulási idő)

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Statikus ablak: több egymás utáni, még nem nyugtázott csomag adása

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

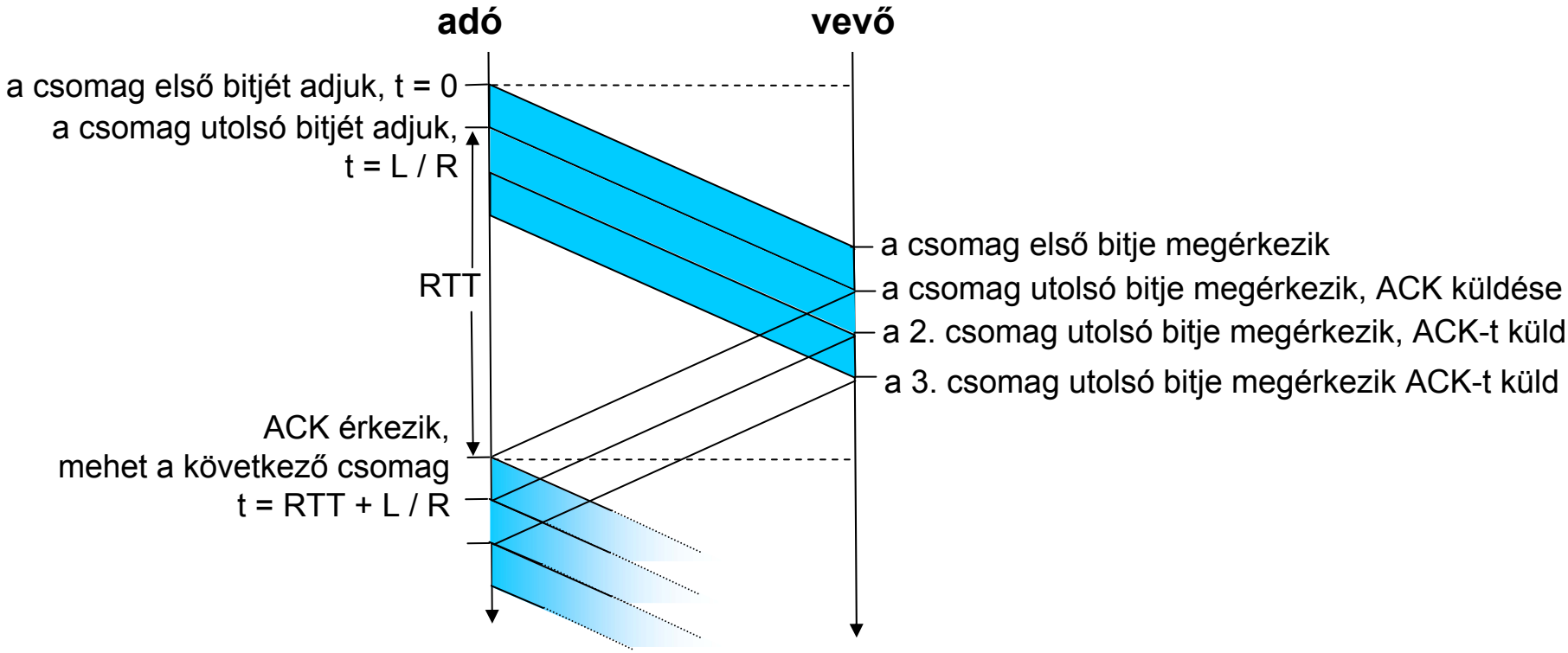
- sorszámozásra van szükség
- tárolásra van szükség az adóban



(a) a stop-and-wait protocol in operation

(b) a pipelined protocol in operation

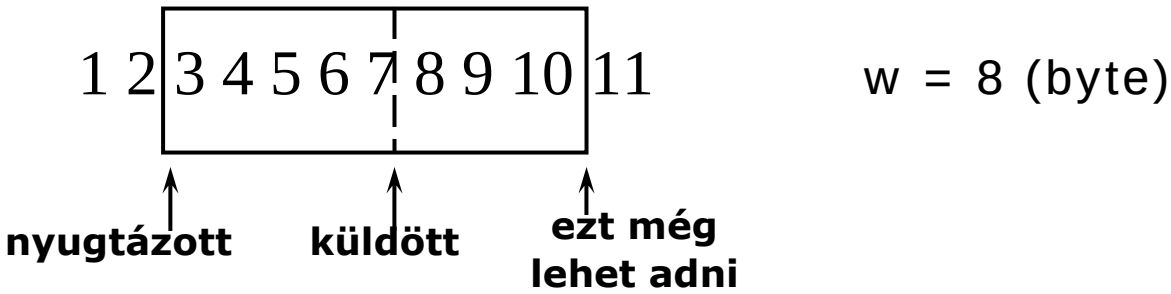
Nagyobb kihasználtság a stop-and-wait-hez képest



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

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csúszóablakos („sliding window”) forgalomszabályozás



Várakozás ACK-ra: **time–out**

- Mekkorára válasszuk a time–out-ot?
- Probléma a túl kicsivel és a túl naggyal
- Megoldás: a teljes körbefordulási időhöz (RTT) igazítani
  - **adaptívvá** tenni
- Szabályok arra, hogy mit tegyünk, ha nem jön ACK a time-out alatt

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglalás

- A küldő által kibocsátott adatátviteli sebességet kordában kell tartani, mert
  - a vevő nem győzi annak feldolgozását
  - a hálózatban képződő szűk átviteli keresztmetszetek torlódáshoz vezethetnek

- Két alapvetően eltérő megközelítés:
  - az információtovábbítást megelőzi egy szerződéskötés
  - folyamatosan befolyásoljuk a küldőt

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

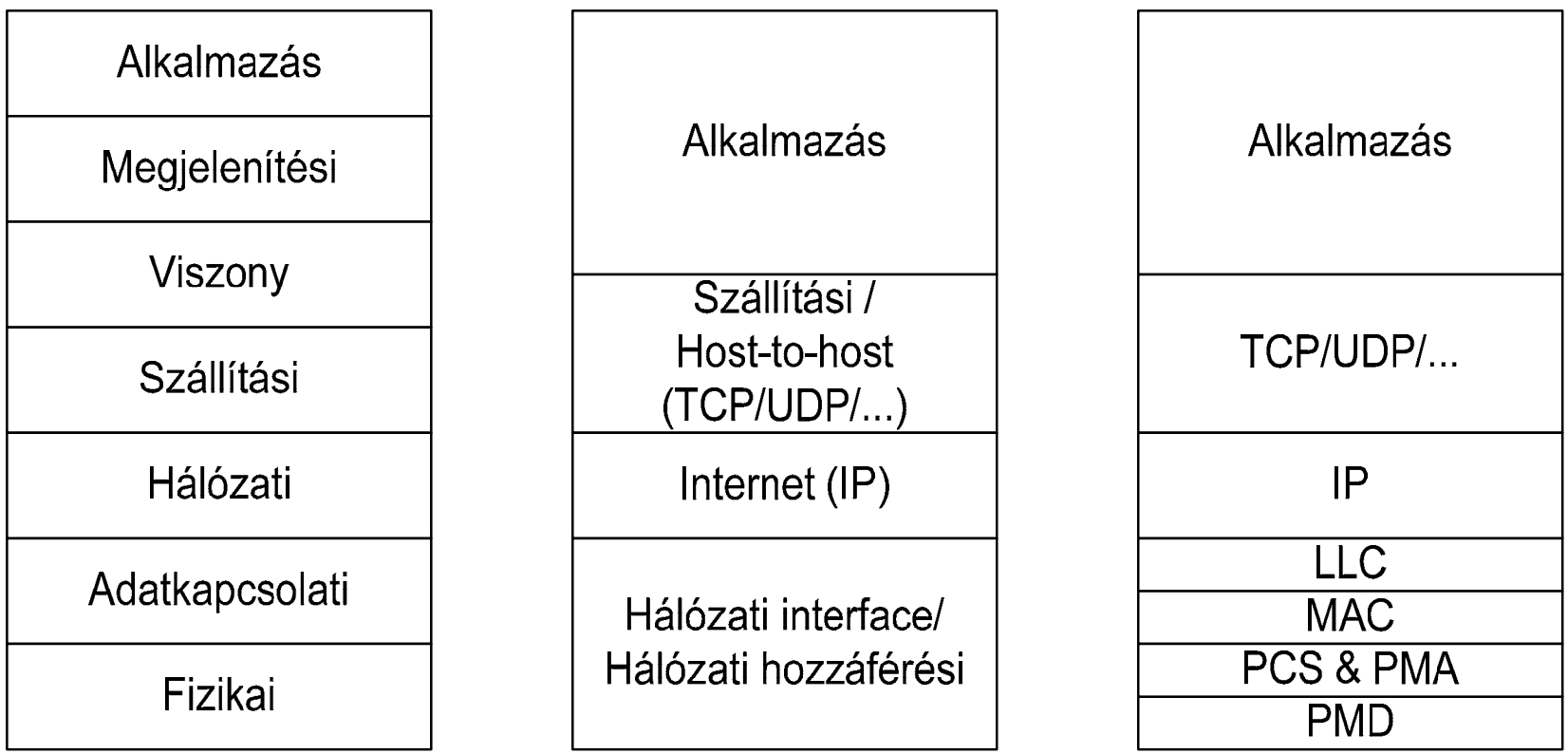
SZÁLLÍTÁSI (TRANSPORT, HOST-TO-HOST) PROTOKOLLOK

UDP és TCP

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

2013.Április 16.

A TCP/IP architektúra és az ISO/OSI rétegmodell



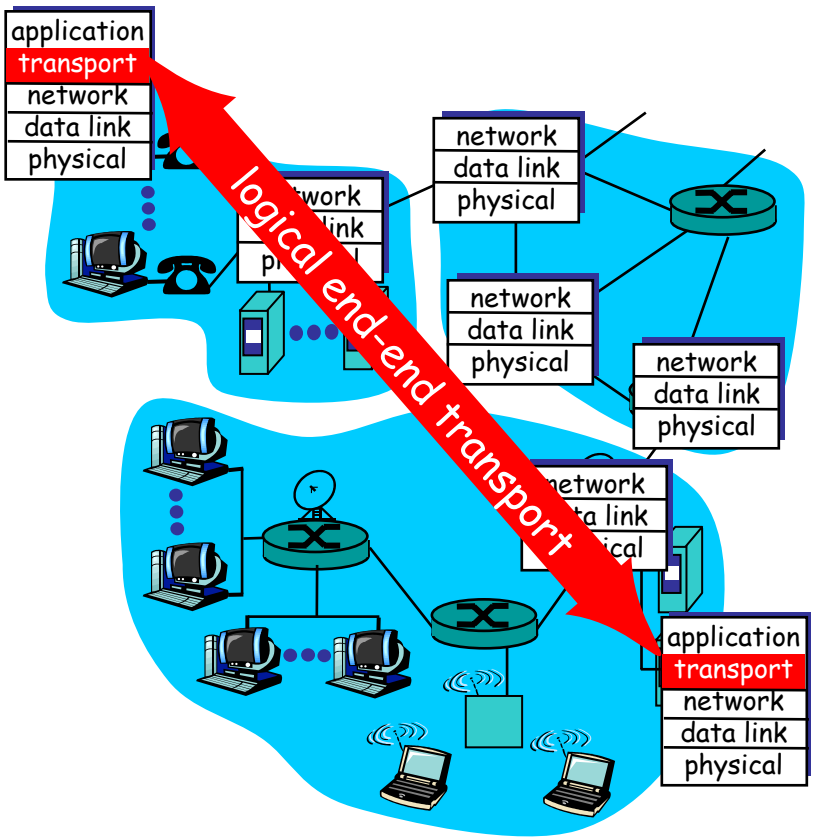
IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
LLC: Logical Link Control

MAC: Medium Access Control
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

A hálózati és a szállítási réteg

- *hálózati réteg:* végpontok („host”-ok) közötti logikai kapcsolatok
- *szállítási réteg:* alkalmazások (process) közötti logikai kapcsolatok
  - a hálózati réteg szolgáltatásainak igénybevételére alapozva **megbízható** átvitel a **transzport entitások** között (transport entity)
  - Feladatai:
    - forgalom szabályozás
    - multiplexelés
    - hibadetektálás, javítás (pl. Automatic Repeat reQuest – ARQ)
    - sorrendhelyes átvitel
    - csomagképzés (szegmensek) és csomagok visszaállítása a felsőbb rétegek számára
      - – byte alapú átvitel

A szállítási réteg



Logikai kapcsolatok a végpontokban futó **alkalmazások között**

A szállítási protokollok a **végpontokban futnak**, a csomópontokban nem

Az alkalmazások adategységeit szállítási protokoll-adategységekbe tördeljük, a kapottakból pedig összerakjuk

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Szállítási protokollok: UDP és TCP

- **UDP – User Datagram Protocol**
- **TCP – Transmission Control Protocol**

- Az UDP és TCP közös képességei:
  - Portok kezelése
  - Multiplexelési képesség

- Alapvető különbség az UDP és a TCP között:
  - UDP összeköttetésmentes (connectionless),
  - TCP összeköttetés-alapú (connection–oriented)

  transzport-szolgáltatást nyújt

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

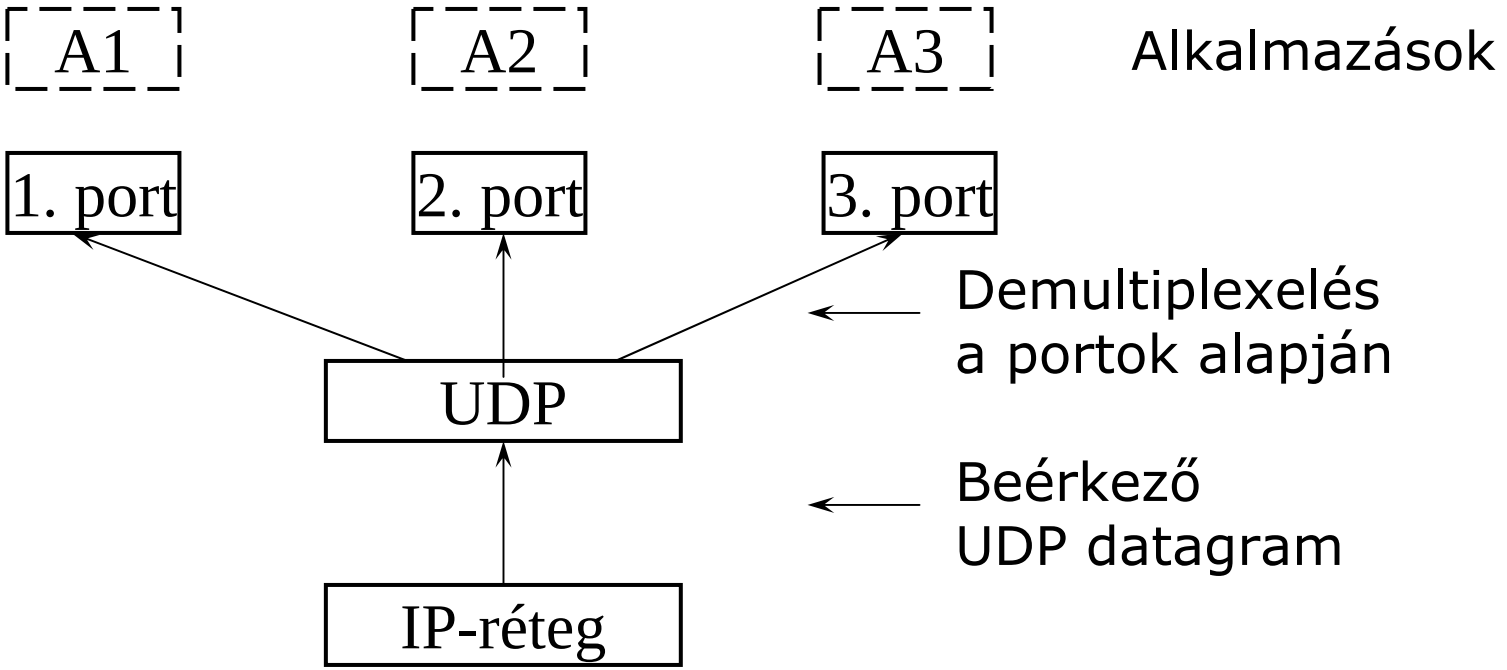
Az UDP és TCP közös képességei (1)

- Portok kezelése:
  - Az IP-rétegben a csomagok végpontnak, „host”-nak vannak címezve
  - A végpontokon belül: több alkalmazás, folyamat
  - Megkülönböztetésük: portok használatával
  - **Foglalt** (reserved, „well-known”) és **rendelkezésre álló** (available) portszámok
  - Foglalt portok: ide mindig lehet küldeni datagrammokat
    - 0...1023 közötti portszámok
    - pl. 80: HTTP, 21: FTP, 69: TFTP (ezek főként TCP-re)
  - Az UDP-en belül megállapításra kerülnek az alkalmazandó portszámok
- Multiplexelés /demultiplexelés
  - A portmechanizmus segítségével

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

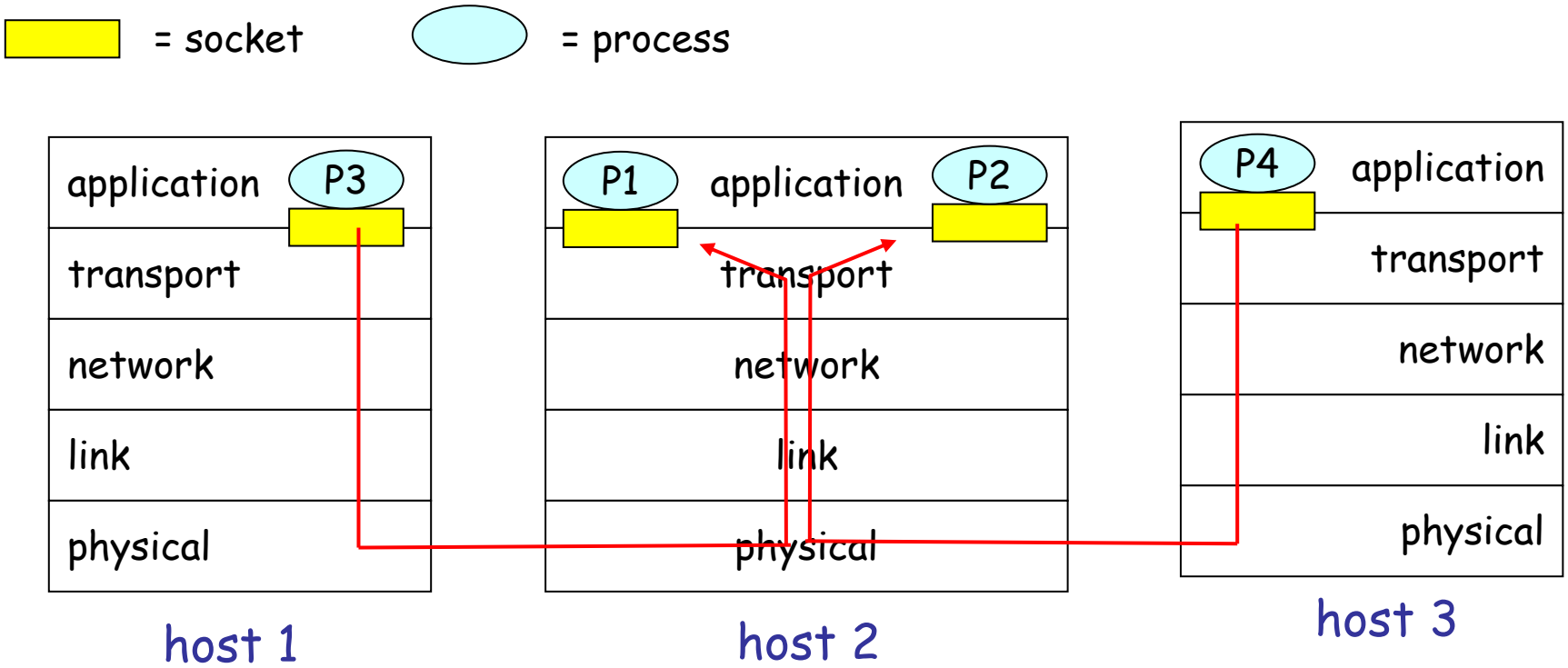
Az UDP és TCP közös képességei (2)

Multiplexelés és demultiplexelés
Példa:



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Multiplexelés-demultiplexelés



Socket: magyarázat

- Socket: interfész, „ajtó” az alkalmazás és a hálózat között
- A socket-et az alábbiak jellemzik:
  - transzportprotokoll (UDP v. TCP)
  - saját IP cím
  - saját portszám

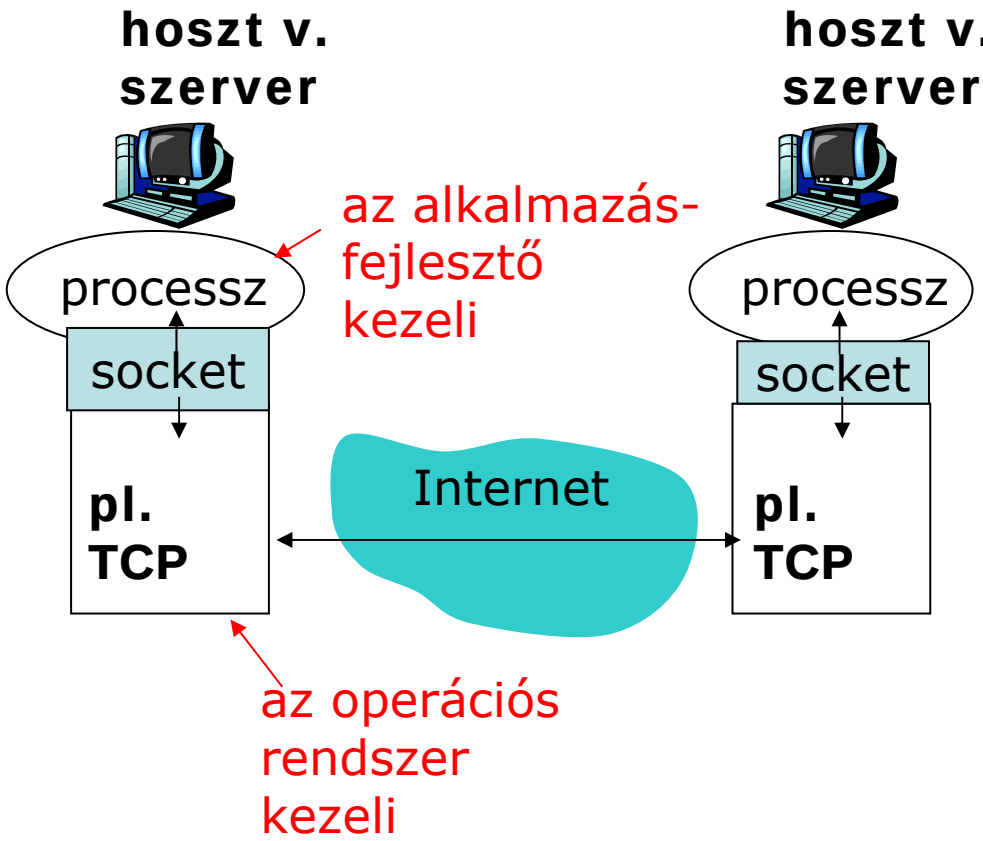
  } helyi socket cím
  - *(opcionális) távoli host IP címe*
  - *(opcionális) távoli alkalmazás portszáma*

  } távoli socket cím

  } socket pár
- Leegyszerűsítve: socket = IP cím + portszám
- Az operációs rendszer a bejövő IP csomagokat a fentiek alapján továbbítja az alkalmazásnak, kiszedve ezeket a megfelelő PDU-kból

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

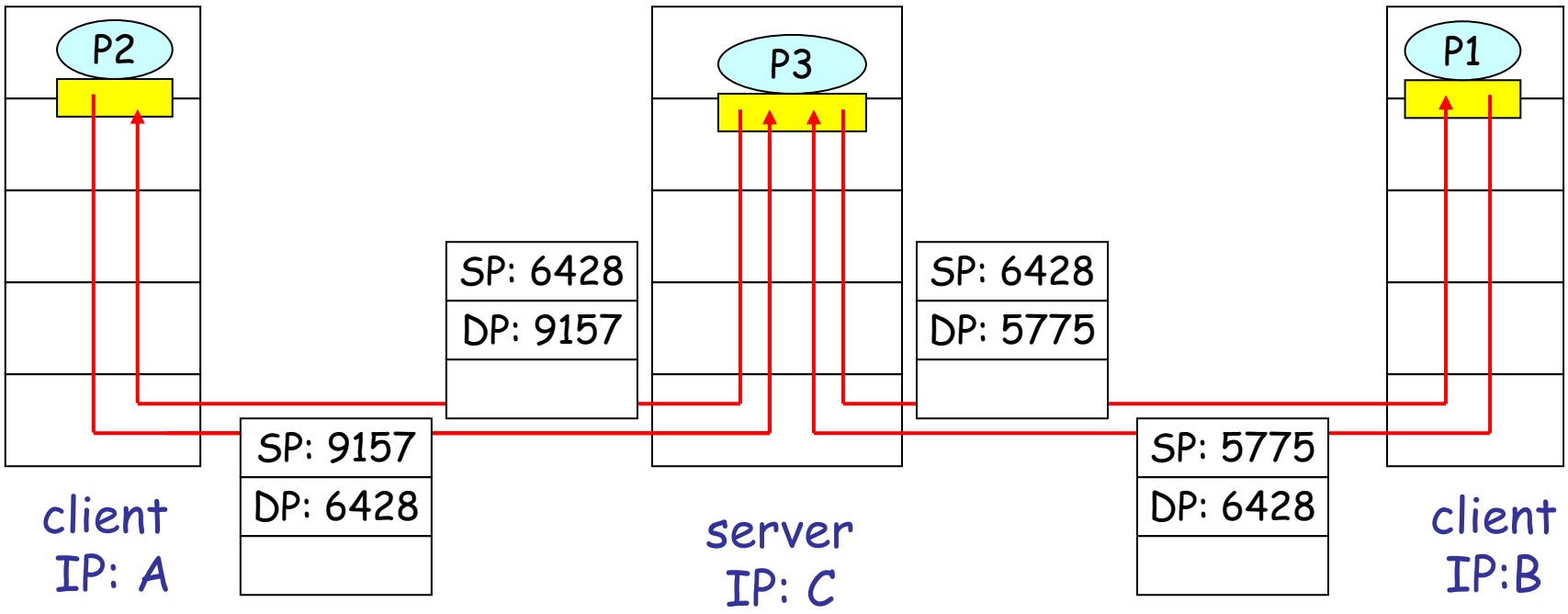
Socket: illusztráció



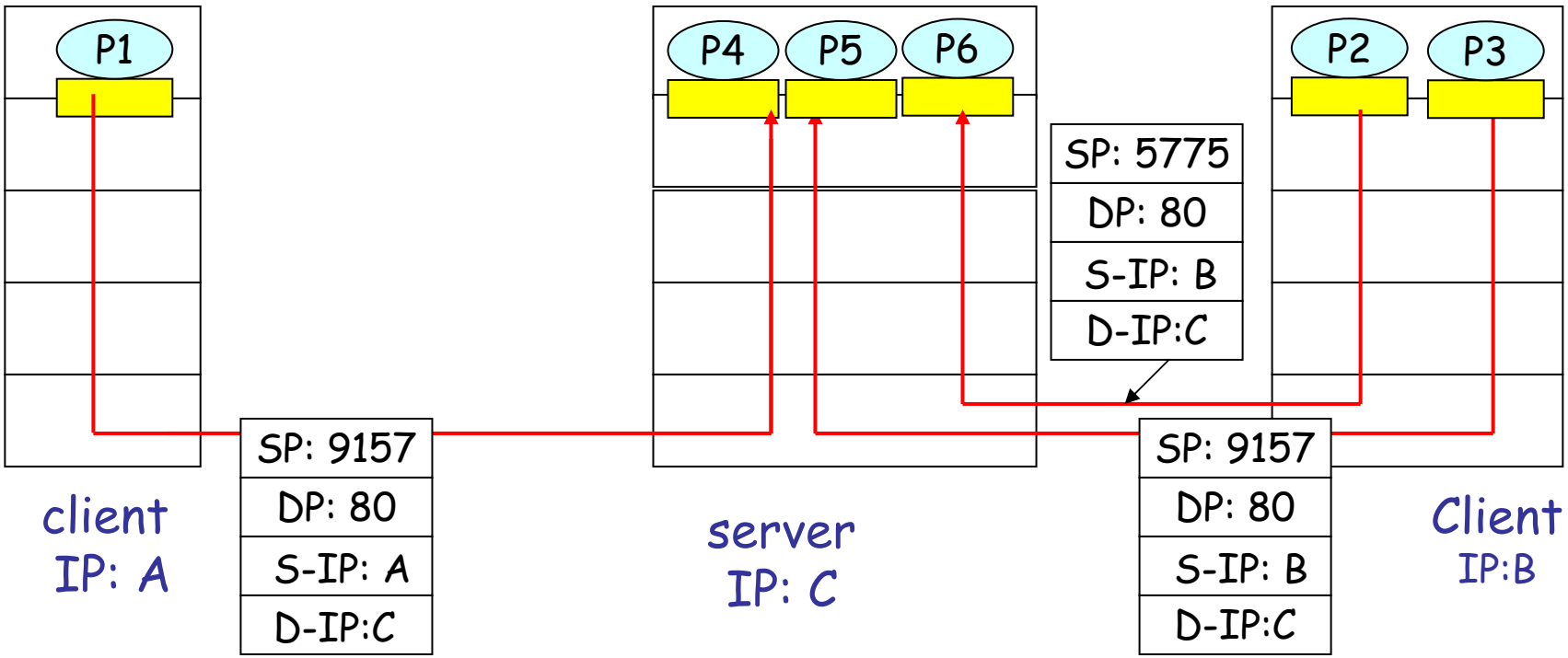
Socket típusok

- Datagramm socket
  - Összeköttetésmentes socket, UDP használja
- Stream socket
  - Összeköttetés-alapú socket, TCP használja
- Raw (IP) sockets
  - Routerekben és hálózati eszközökben
  - Pl. ICMP, IGMP, OSPF

Multiplexelés-demultiplexelés, összeköttetésmentes eset (UDP)



Multiplexelés-demultiplexelés, összeköttetés-alapú eset (TCP)



TCP kliens-szerver socket kezelés

- Szerver létrehoz **„hallgató” módban** lévő socketeket
  - várja a kliensek kapcsolatfelvételét
  - ilyenkor távoli cím: 0.0.0.0, távoli port: 0
- Kapcsolatfelvétel után: **dedikált socket** minden kapcsolathoz
  - Socket-socket közötti virtuális áramkörkapcsolás: TCP kapcsolat, duplex byte folyam
- Szerver különböző TCP socketeket hozhat létre ugyanazzal a helyi IP címmel és port számmal
  - mivel a távoli host IP címével, portjával **más socket párt alkot**
  - szerver gyerek processz összerendelése a kliens processzével
- UDP-ben **nincs dedikált socket**
  - Nincs külön gyerek processz minden távoli processzhez, egy processz kommunikál velük

És ahol nincs transzport réteg implementálva?

- Egyes hálózati elemekben nincs implementálva a transzport réteg
  - Router hálózati rétegben
  - Switch adatkapcsolati rétegben
- De tűzfalak, NAT-ok és proxy szerverek figyelik az aktív socket párokat és fenntartanak socket interfészeket
- Továbbá: ütemezéshez (WFQ), QoS támogatáshoz routerekben a csomagfolyamokat a socket párokkal lehet azonosítani

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Megoldás: Egyszerű (raw) socket

- **Közvetlenül** az alkalmazásnak továbbítja a csomagot a **fejléccel**
  - Nincs TCP/IP feldolgozás, alkalmazás látja el fejléccel/veszi le a fejlécet
  - Pl. routerekben ICMP-hez

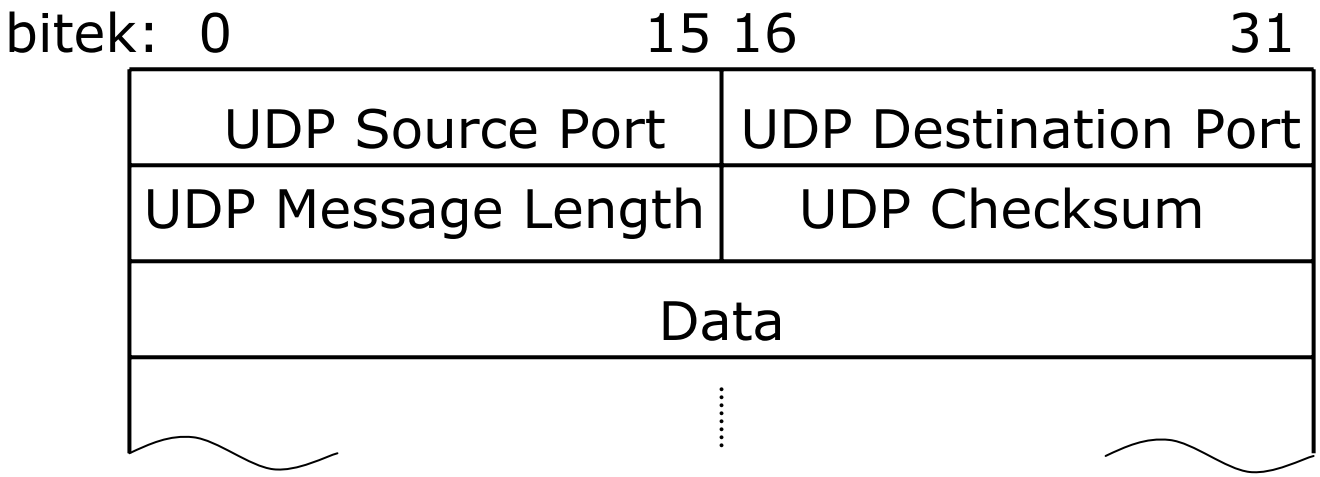
- Windows XP-ben 2001-ben jelent meg: biztonsági aggályok (Unixban régóta)
  - Félelem **TCP reset támadástól**: „lelövi” a TCP kapcsolatot
    - +:gyanús kapcsolatok megszakítása
    - -: harmadik fél beékelődve megszakítja a kapcsolatot
    - +/- ? Peer-to-peer forgalom szűrése (Comcast-NNSquad eset)

UDP (User Datagram Protocol)

- Nincs kapcsolatfelépítés, kézfogás
- Semmi garancia:
  - a csomagok sorrendjére
  - adatintegritására
  - elvesztésének detekciójára
- A megbízható átvitel garantálását az alkalmazási rétegre bízza
- *Unreliable* Datagram Protocol ☺
- Multiplexálást és opcionálisan adatintegritás ellenőrzést nyújt

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

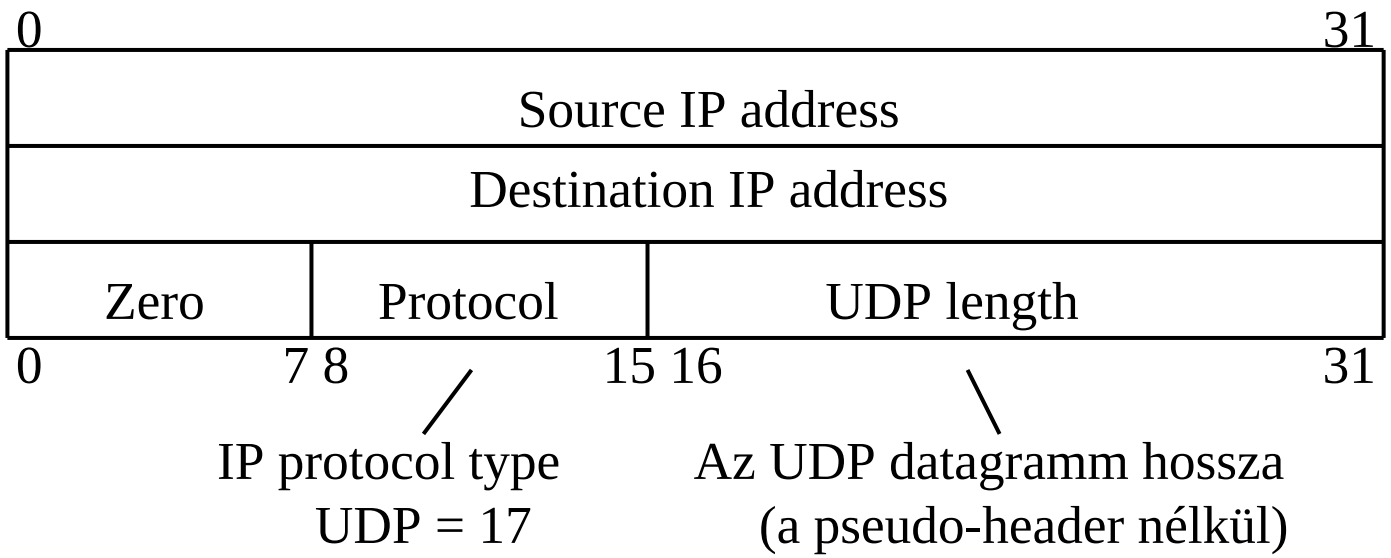
UDP – User Datagram Protocol (2)



- **Source port** opcionális
- **Length**: oktettben, max (65 535-8-20)
- **Checksum**: opcionális (nincs: 0, IPv6-nál már nem opcionális)
- Az UDP checksum az egyetlen lehetőség annak ellenőrzésére, hogy a datagram helyesen érkezett-e meg
  - adatra és fejlécre!
  - az IP-csomag ellenőrzése csak a fejrészt fogja át

UDP – User Datagram Protocol (3)

- A checksum számítási elve
  - 1-es komplemens 16 bites szavakra
- Tartalmazza az IP-címeket is
  - annak ellenőrzésére, hogy a datagramm elérte a helyes címzettet, nemcsak a helyes portot
- „Pseudo-header” hozzáadásával (IPv4-re):



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

UDP – User Datagram Protocol
Összefoglalás: funkcionalitás és a költsége

- Portkezelés
  - a különböző alkalmazások/folyamatok megkülönböztethetők
- Több alkalmazás egyidejű kezelése
  - port-hozzárendeléssel és multiplexeléssel/demultiplexeléssel
- Hibajelzés az UDP datagram tartalmára és az IP csomag további részeire
- A fentiek költsége:
  minimum 8 oktettnyi overhead

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

UDP alkalmazása

- Broadcast, multicast (TCP nem képes rá)
- Média: streaming, valós idejű játékok, VoIP, IPTV
- Gyors és rövid lekérdezések:
  - DNS
  - DHCP
  - RIP
- Tipikusan a hálózati forgalom pár százaléka
  - De növekszik a részaránya és nincs torlódás szabályozás: aggályok!
  - Datagram Congestion Control Protocol (DCCP)

TCP –Transmission Control Protocol
Fő jellemzői

- **Célkitűzés:** megbízható szállítási szolgáltatás nyújtása az IP nem megbízható datagram-szolgáltatásán

- **Jellemzői:**
  - ***Virtuális összeköttetések:*** összeköttetés épül fel és marad fenn a kommunikáció tartamára
  - ***Stream–típusú szolgáltatás:*** byte- (oktett-) streamek sorrendhelyes átvitele
  - ***Strukturálatlan stream:*** nincsenek határolók a streamen belül
  - ***Pufferelt átvitel:*** a streamből a datagramm megtöltéséhez szükséges mennyiséget várja össze
  - ***Duplex kapcsolatok:*** két független stream
  - ***Vezérlő információk küldése:*** az ellenkező irányban folyó streambe ágyazva (**piggybacking**)

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

TCP – Transmission Control Protocol
Miről lesz szó?

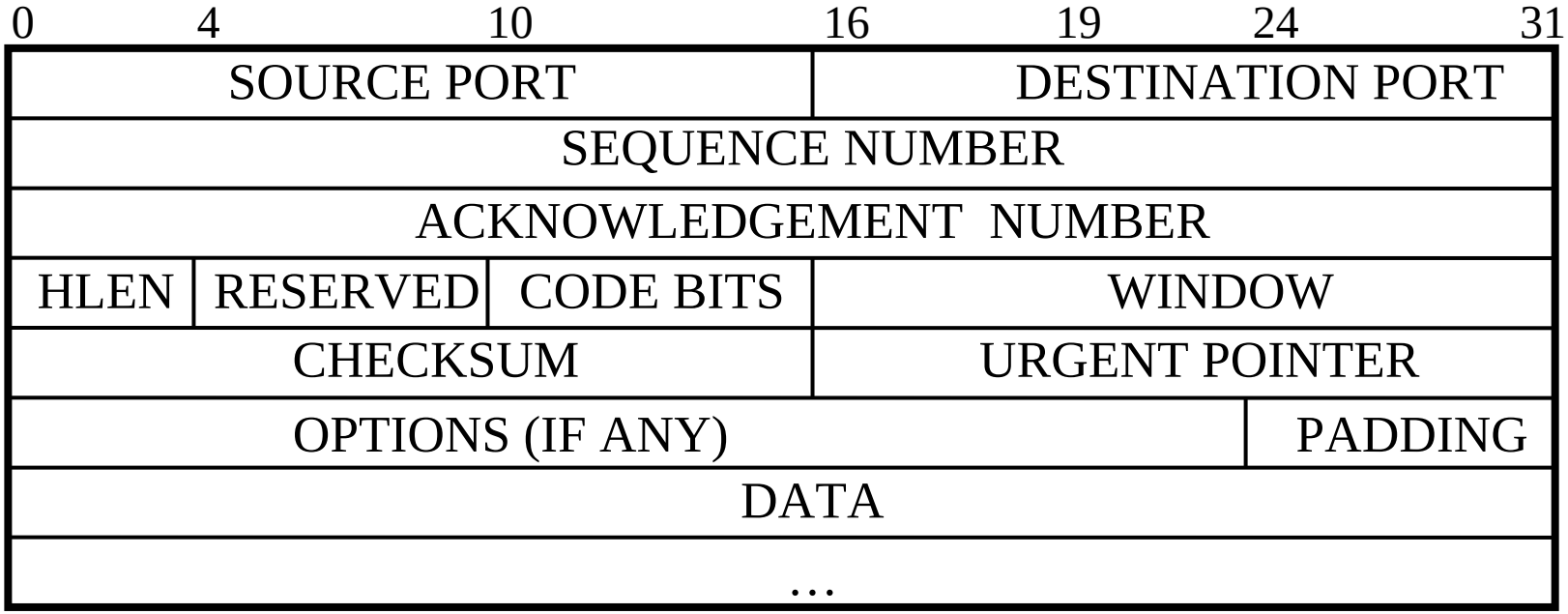
- **Adategység**: szegmens; szegmensstruktúra
- **Megbízható átvitel** sorszámozás és pozitív nyugtázás segítségével
- Összeköttetés-alapú kommunikáció: **kapcsolatfelépítés és -lebontás**
- **Forgalomszabályozás** (flow control) ablakmechanizmus segítségével
- **Torlódásvezérlés** (congestion control)

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

TCP kialakulása

- 1974: "*A Protocol for Packet Network Interconnection.*" Vint Cerf és Bob Kahn
- Itt vezetik be a *Transmission Control Program*-ot, ez válik szét később TCP-re és IP-re
- Eleinte Internet Protocol Suite, majd TCP/IP elnevezés

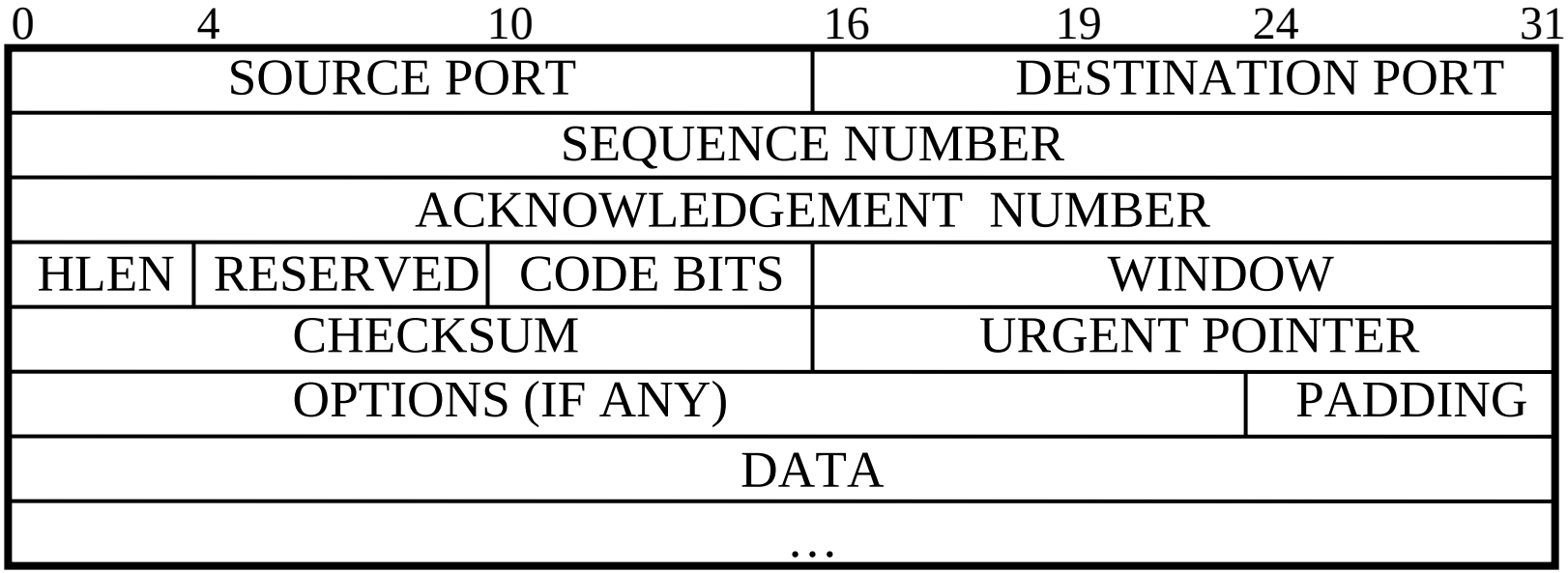
A PDU – Protocol Data Unit (a TCP-ben: „segment”) struktúrája



- **Sequence no**.: a szegmensben levő adat első byte-jának pozíciója a küldő byte stream-jében
- **Ack no**.: annak a byte-nak a sorszáma, amelyet a forrás legközelebb vár

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

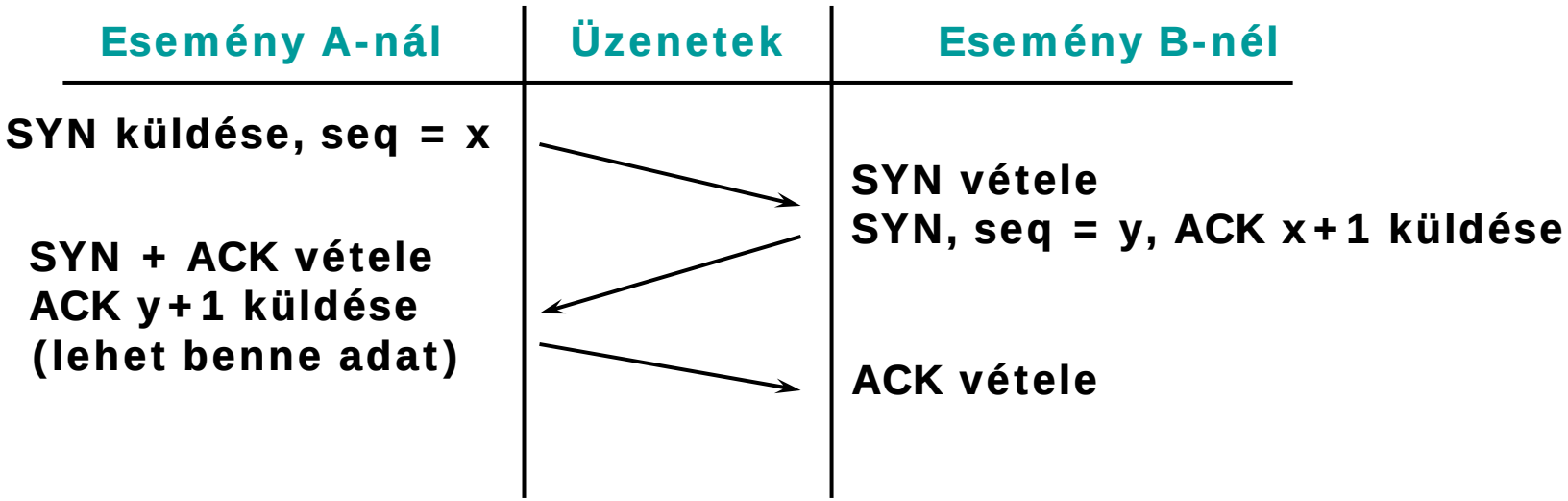
TCP – Transmission Control Protocol
Szegmensformátum (folyt.)



- **HLEN**: fejléc mérete, minimum 20 byte, max 60 byte
- **Code bits** (flags): URG, PSH, ACK, RST, SYN, FIN bitek
  a kapcsolat kezeléséhez használt jelzőbitek
- **Window**: a küldő ismertté teszi a **vételi pufferének méretét**
- **Checksum**: mint az UDP-ben (pszeudorandom)
- **Urgent pointer**: ha URG=1, a szegmens „urgent” részt tartalmaz, ilyenkor a végére mutat (pl. jelszóküldés)

Hívásfelépítés a TCP-ben

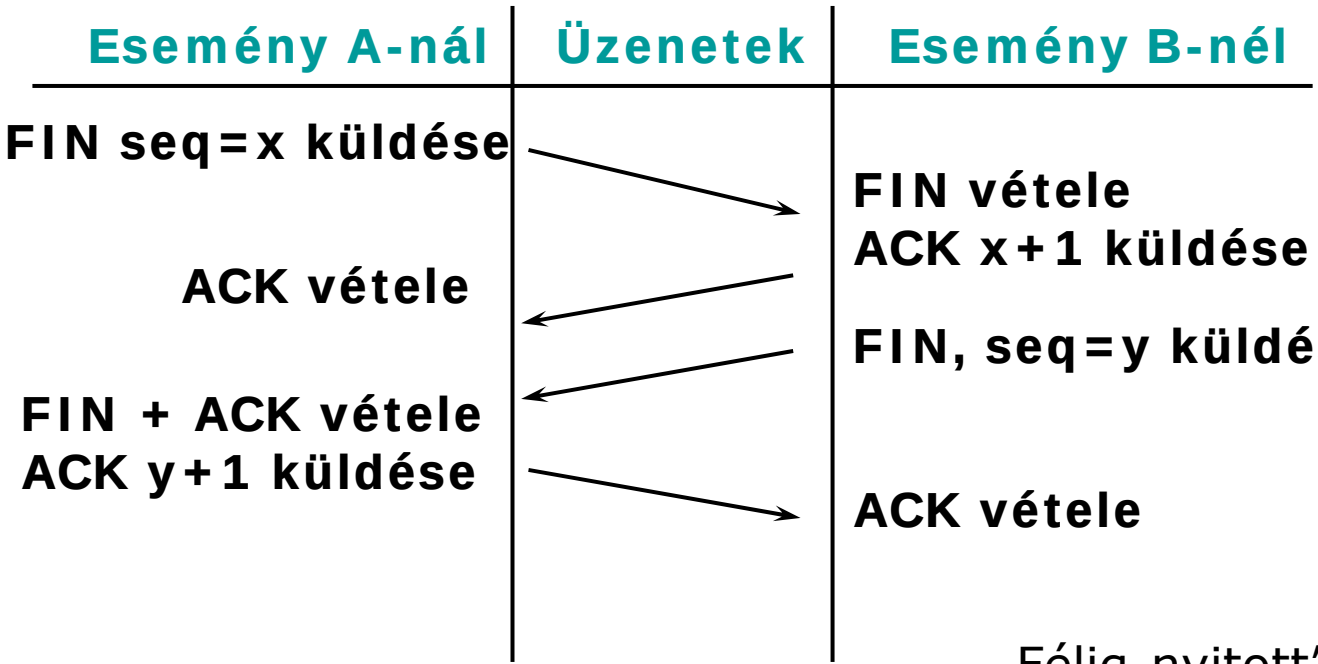
„3-way handshake” eljárás (3 utas kézfogás)



Elején véletlenszerű sorszám: a TCP sorszám predikciós támadás elkerülése

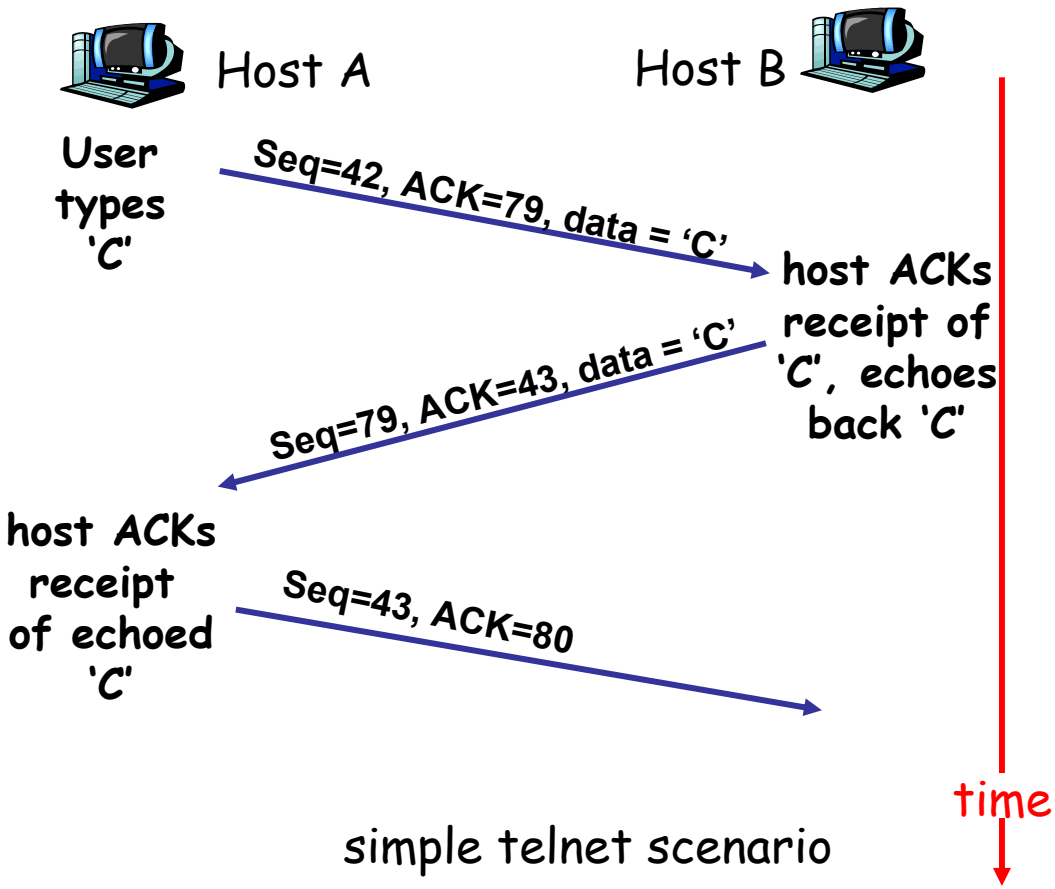
Híváslebontás a TCP-ben

„Modified 3-way handshake” eljárás



„Félig-nyitott” kapcsolat elkerülése

Sorszámok és nyugtaszámok használata a TCP-ben



simple telnet scenario

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

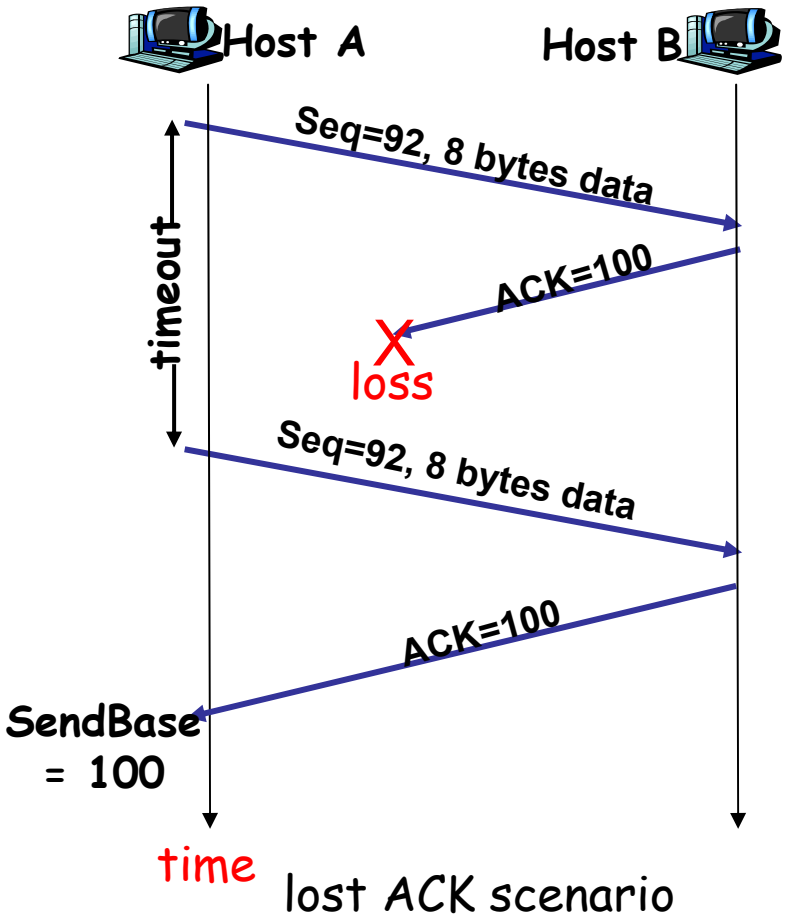
Várakozás nyugtázásra

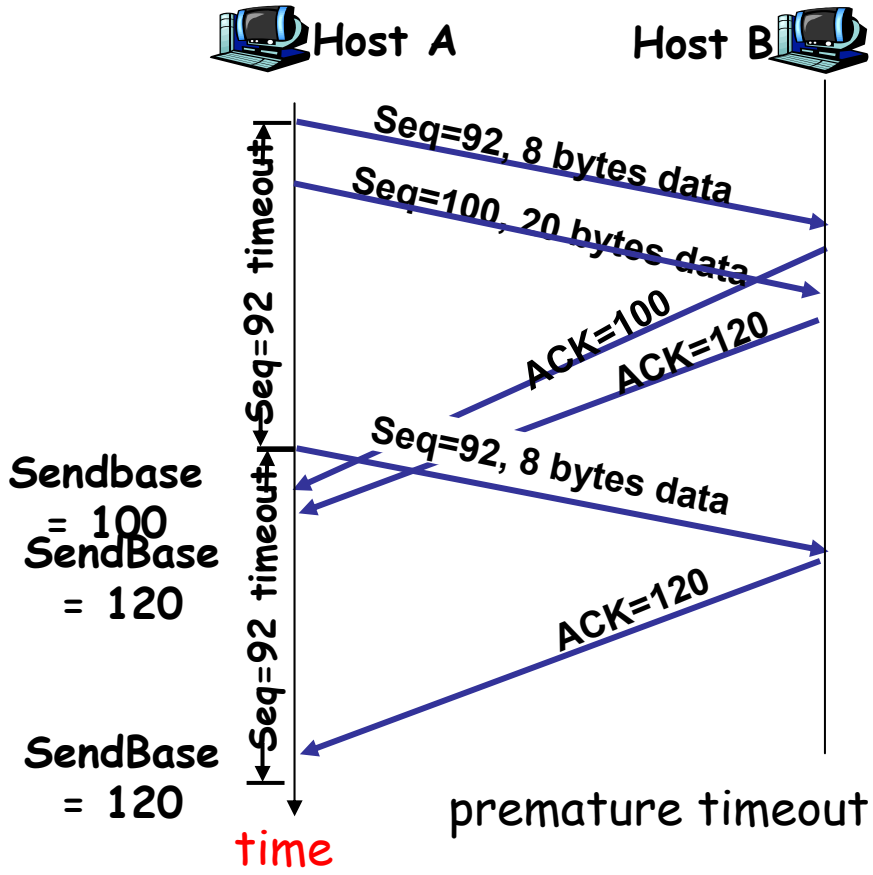
- Várakozás ACK-ra: **time–out**
- Mekkorára válasszuk a time–out-ot?
- Probléma a túl kicsivel és a túl naggyal

- Megoldás:
  a teljes terjedési időhöz
  (RTT - round-trip time) igazítani, **adaptívvá** tenni

- Szabályok arra, hogy mit tegyünk, ha nem jön ACK a time-out alatt

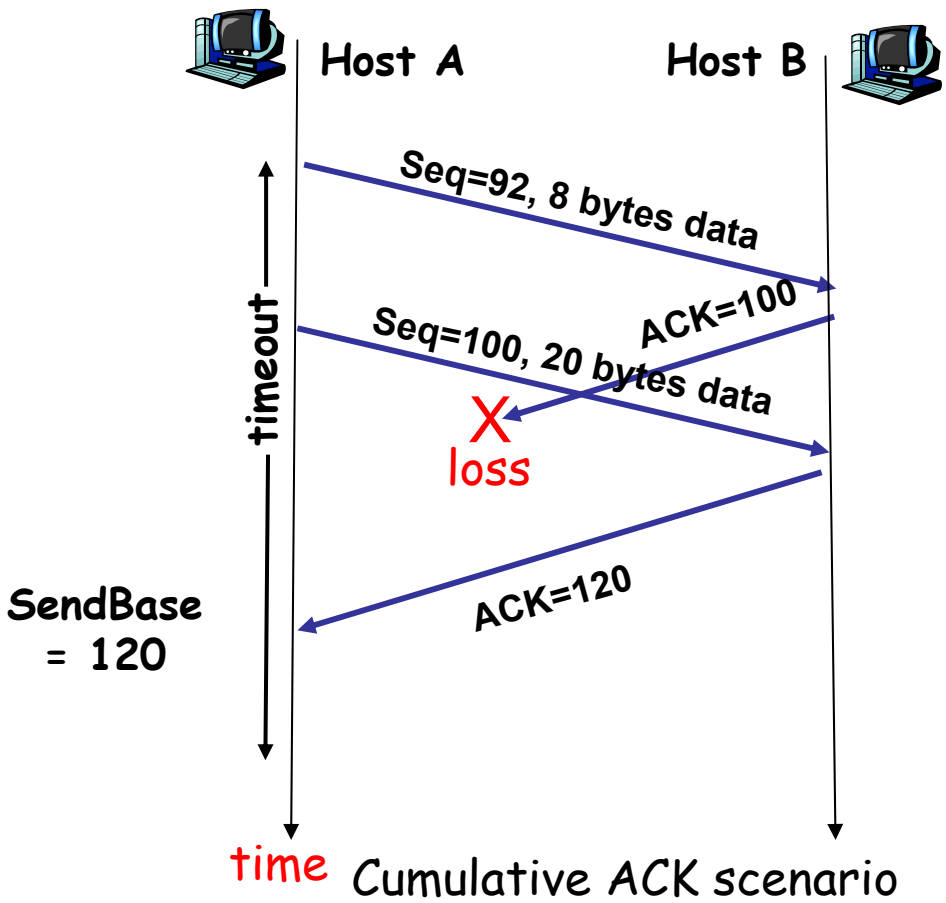
Újraküldési esetek a TCP-nél: elveszett nyugta és korai timeout





© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Újraküldési esetek a TCP-nél: összevont nyugta



Cumulative ACK scenario

Gond összevont nyugtával

- Pl. 1000 bájt kerül elküldésre 10 szegmensben
  - Ha elveszik az első szegmens, a fogadó nem tudja visszajelezni, hogy 100-999 megjött, de 0-99 nem
  - Újra elküldi a teljes 1000 bájtot

- Megoldás: **szelektív nyugtázás**
  - SACK-ban meg tudja mondani, hogy 100-999 megjött sikeresen
  - Opcionális fejrészmezőben
  - Népszerű, minden TCP implementációban

Gond sorrend keveredéssel

- Sorrendkeveredés miatt elveszett csomagnak hiszi a küldő ->újraküldés->forrás visszafogás

- Megoldás: **D-SACK (duplikált nyugta)**
  - Fogadó szól, hogy az újraküldött csomag duplikátum

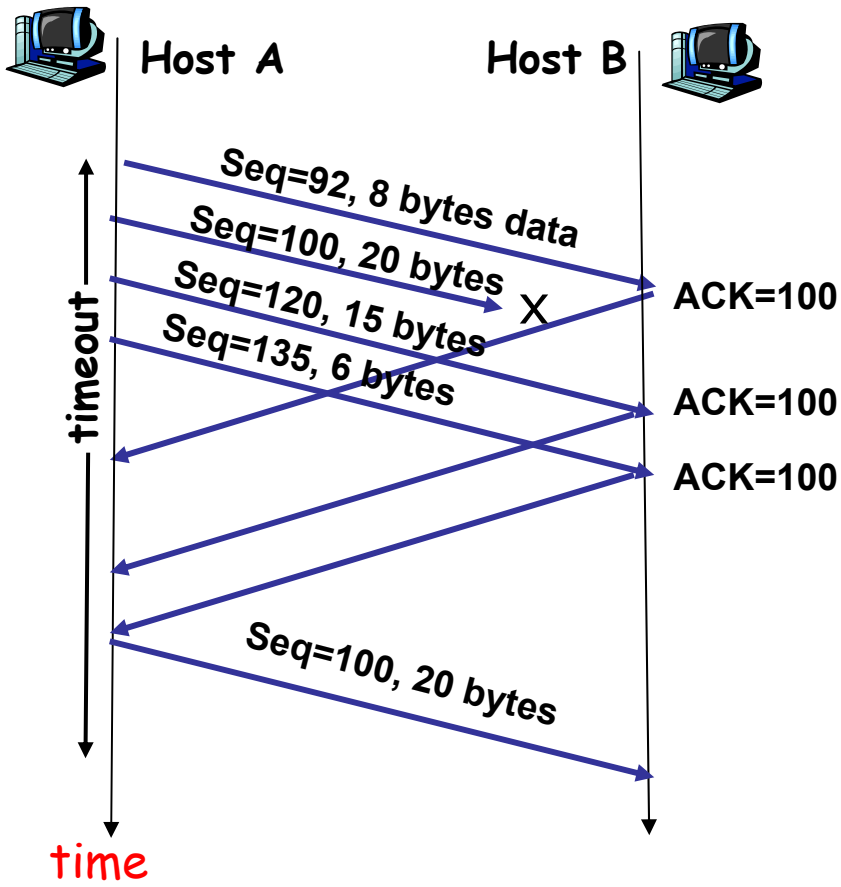
  ->visszagyorsul a forrás

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Fast retransmit (1)

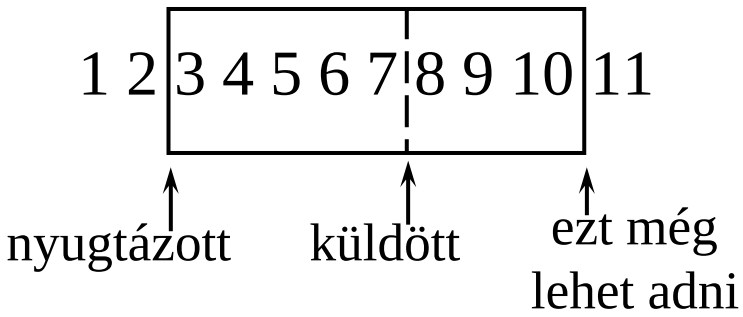
- A time-out idő gyakran túl hosszú:
  - nagy késleltetés mielőtt az elveszett csomagot az adó újra tudná küldeni.
- De hogy értesülhetne az elveszett csomagról előbb, mintsem hogy letelt volna a timeout?
  - Az elveszett szegmensekre utalhatnak a duplikált ACK-ok
  - Ha a vevő hézagot vesz észre a vett szegmensek sorozatában (elveszett csomag) akkor újból lenyugtázza a megelőző helyesen vett szegmenst.
  - Több egymást követő duplikált ACK érkezhet.
- Fast retransmit szabály: ha az **adó 3 egymást követő ACK-t kap** ugyanarra a szegmensre, feltételezi, hogy az azt követő szegmens elveszett és
  - **újraküldi azt még mielőtt lejárna a timeout**.

Fast retransmit (2)



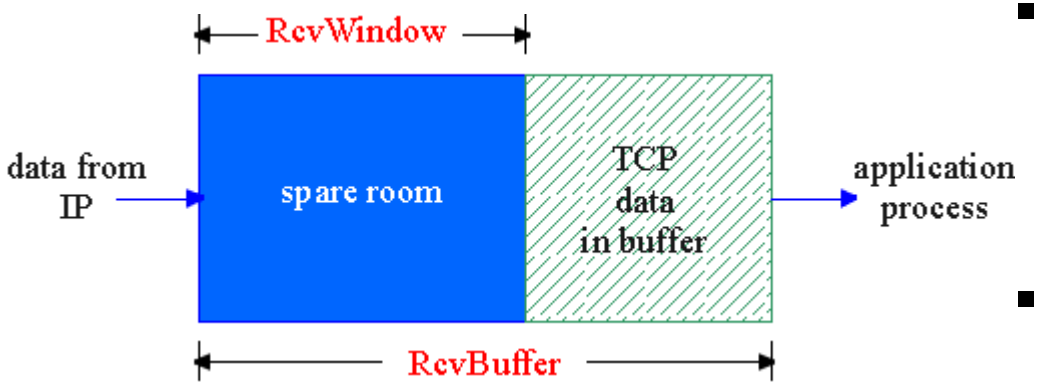
© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Flow control: a „sliding window” módszer elve



- Csúszóablakos („sliding window”) mechanizmus
  - az ablak mérete megadja a „kintlevő”, nyugtázatlan csomagok max. számát. (Pl.: w=8)
- A TCP-ben: az ablak-mechanizmus oktetteken működik

TCP Flow control: hogy működik?



- Spare room:

= **RcvWindow**

= **RcvBuffer-[LastByteRcvd - LastByteRead]**

- A vevő közli a szabad helyének a méretét (**RcvWindow**) a küldött szegmensben
- Az Adó legfeljebb **RcvWindow** mennyiségű nyugtázatlan adatot küld

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

MSS (Maximum Segment Size)

- A legnagyobb adatméret bátjban, amit a TCP hajlandó küldeni egy szegmensben
- Össze kell egyeztetni az adatkapcsolati réteg MTU-jával
  - elkerülendő a tördelést
- TCP kapcsolatfelépítésnél kell egyeztetni, **MSS opció a fejlécben**
- TCP adó használhat Path MTU discovery-t is: dinamikus MSS változtatás

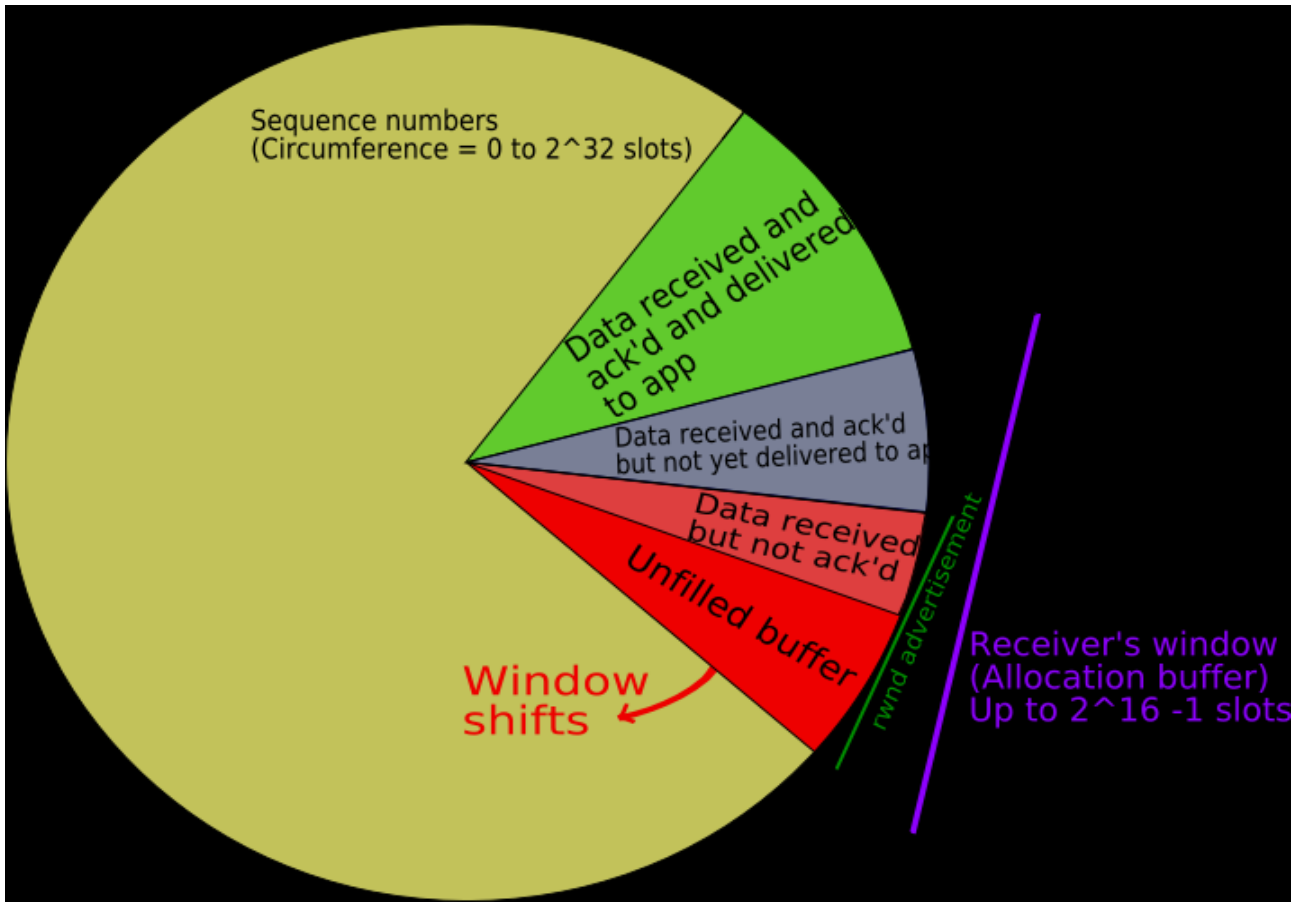
Csúszóablakos problémák

I. Ha a vevő **nullás csúszóablak** méretet hirdet: adó leáll a küldéssel
- Ha **elveszik a vevő csomagja az új csúszóablak méretről**: adó vár hiába
- Megoldás: adó egy **timert** indít, lejárta után felkéri a vevőt, hogy küldjön ACK-ot az új ablakméretről

II. **Buta ablak jelenség**
- Ha a vevő oldalon kicsi (akár 1 byte) szabadul fel, lehet 1 byte az ablak
- A küldő 1 byte-ot küld, a vevő megint 1 byte-tal nyit
- Erőforráspocsékolás: kisebb az adat mint a fejléc!
- Megoldás:
  - A vevő nem nyitja az ablakot, csak akkor, **ha MSS nagyságrendűt nyithat**
- A küldő nem küld, hacsak nem
  - MSS-nyit küldhet
  - Mindent küldhet, amit az alkalmazás kért

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A TCP „óra”



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Torlódásvezérlés a TCP-ben

- A torlódásvezérlésről általában:
  - Azok a módszerek, amelyekkel linkek, csomópontok időszakos túlterheltségét megkíséreljük megszüntetni.
- Két fő módszer:
  - „Hálózat által segített” (**network assisted**) torlódásvezérlés
    - A hálózati elemek szolgáltatnak információt a túlterhelésről az adónak
  - Végpontok közötti (**end-to-end**) torlódásvezérlés
    - nincs visszacsatolás a hálózatból, a végpont következtet arra, hogy torlódás léphetett fel
- A TCP az utóbbit csinálja!

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

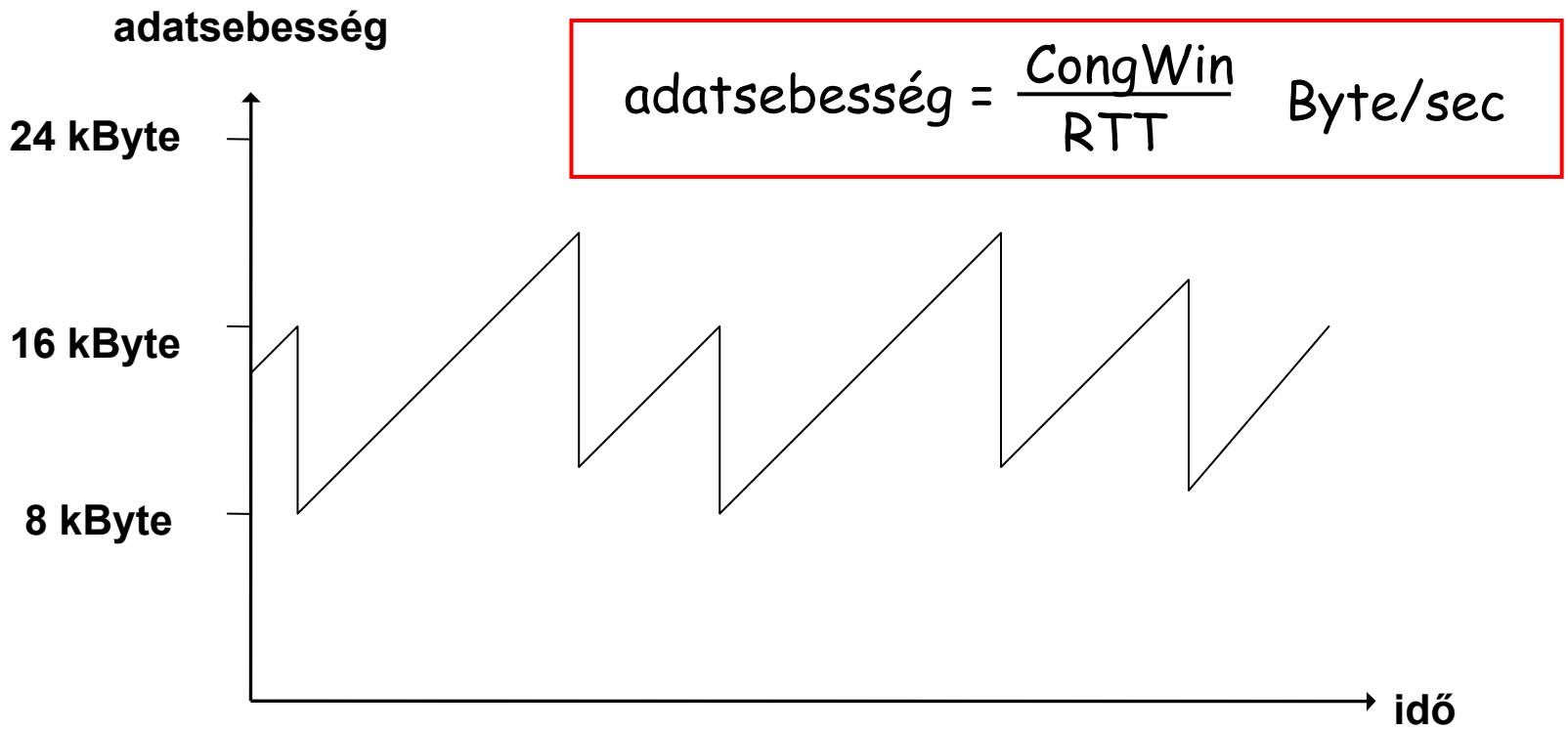
Torlódásvezérlés a TCP-ben

- Módszer:
  - **növeljük az adatsebességet**, ha úgy érzékeljük, van elég átbocsátóképesség
  - amíg **torlódásra utaló jeleket** nem tapasztalunk, ha igen, csökkentsük.

- Hogyan:
  - congestion window, **CongWin**
  - növeljük a CongWin-t minden RTT alatt MSS-sel, amíg vesztést nem érzékelünk
  - csökkentsük a CongWin-t felére minden vesztéskor
  - = **Additive increase – multiplicative decrease (AIMD)** módszer

- Hogyan érzékeljük a torlódást (vesztést)?
  - timeout letelt, nem jött nyugta
  - többszörös nyugta érkezett ugyanarra a szegmensre

Az adatsebesség alakulása AIMD esetén



$$\text{adatsebesség} = \frac{\text{CongWin}}{\text{RTT}} \quad \text{Byte/sec}$$

TCP torlódásvezérlés: további részletek

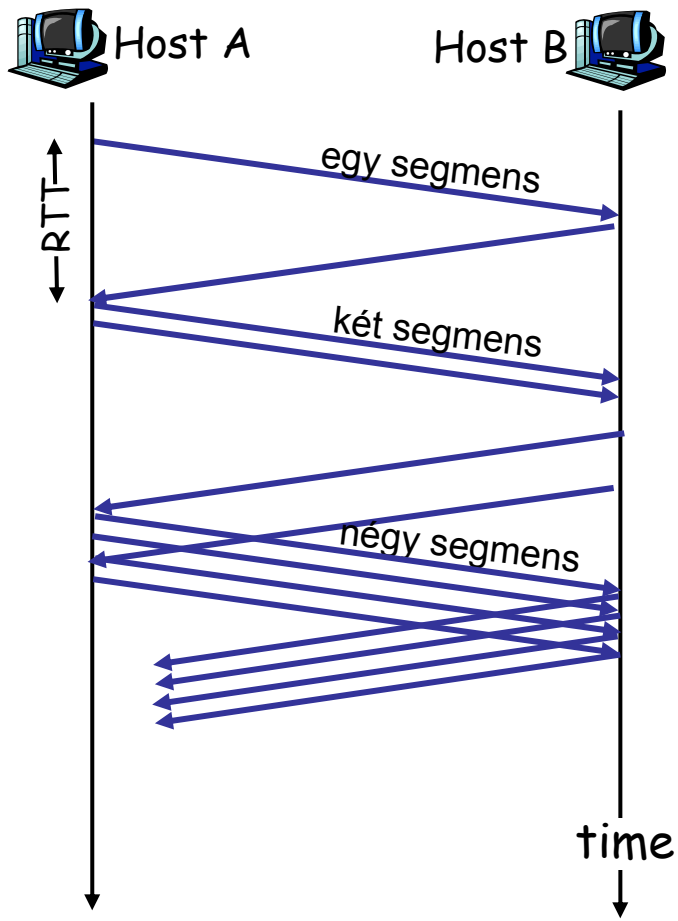
- Az AIMD kiegészítései:

- „Slow Start”
  - az összeköttetés kezdetén a sebesség gyors (exponenciális) növelése az első vesztésig, utána AIMD
  - Gyors növelés: minden ACK után kétszerezzük

- Eltérő viselkedés timeout és többszörös (3-szoros) nyugták esetén

TCP Slow Start

- Az elején: **`CongWin`** = 1 MSS
  - Példa: MSS = 500 byte & RTT = 200 msec
  - kezdeti sebesség = 20 kbps
- Mivel a rendelkezésre álló átb. képesség >> CongWin/RTT lehet,
  - célszerű gyorsan elérni, ezért
  - induláskor exponenciálisan növelni az első vesztésig



© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Csomagvesztés

- 3 duplikált ACK után:
  - **`CongWin`** felére csökken
  - Utána lineáris növekedés
    - torlódás elkerülés
- De timer lejárta esetén:
  - **`CongWin`** 1 MSS lesz;
  - Utána exponenciálisan nő,
  - Egy korlátig, majd onnan lineáris

Filozófia:

- timer lejárta rosszabb torlódási helyzetet jelez, mint a 3 duplikált ACK

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Összefoglaló: TCP torlódás szabályozás

- Ha a **CongWin** egy korlát alatt van, adó slow-start fázisban, exponenciális ablak növelés
- Ha **CongWin** a korlát felett, az adó torlódás elkerülési fázisban, lineáris ablak növelés
- Ha 3 duplikált ACK, a korlát **CongWin/2** lesz és a **CongWin** pedig a korlát
- Ha timer lejárt, a korlát **CongWin/2** lesz, míg a **CongWin** 1 MSS lesz

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

TCP sender congestion control *

State	Event	TCP Sender Action	Commentary
Slow Start (SS)	ACK receipt for previously unacked data	CongWin = CongWin + MSS, If (CongWin > Threshold) set state to “Congestion Avoidance”	Resulting in a doubling of CongWin every RTT
Congestion Avoidance (CA)	ACK receipt for previously unacked data	CongWin = CongWin+MSS * (MSS/CongWin)	Additive increase, resulting in increase of CongWin by 1 MSS every RTT
SS or CA	Loss event detected by triple duplicate ACK	Threshold = CongWin/2, CongWin = Threshold, Set state to “Congestion Avoidance”	Fast recovery, implementing multiplicative decrease. CongWin will not drop below 1 MSS.
SS or CA	Timeout	Threshold = CongWin/2, CongWin = 1 MSS, Set state to “Slow Start”	Enter slow start
SS or CA	Duplicate ACK	Increment duplicate ACK count for segment being acked	CongWin and Threshold not changed

TCP átbocsátóképessége

- TCP átlagos átbocsátó képessége az ablak méret és RTT függvényében?
  - Nem foglalkozunk slow-start-al

- *W* az ablakméret a csomagvesztés pillanatában
- Csomagvesztés előtt az átbocsátás *W/RTT*
- Vesztés után az ablak *W/2* lesz, átbocsátás *W/2RTT*.
- Átlagos átbocsátás: *.75 W/RTT*

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

TCP és UDP: összefoglalás

- Mindkettő host layer/transport layer protokoll
- Mindkettő portokat kezel
  - multiplexelés/demultiplexelés
  - ezáltal interface nyújtása az alkalmazói folyamatok felé
- Az UDP összeköttetés-mentes, best effort szolgáltatás
  - nem garantál célba juttatást, csak hibajelzést nyújt
  - gyorsan célba juttat
- A TCP összeköttetés-alapú, megbízható transzport szolgáltatás
  - sorrendhelyes, hibamentes szállítást nyújt
  - ára: késleltetés

© Dr.Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Néhány gyakori alkalmazás és az használt transzportprotokollok

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

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

MULTIMÉDIA TOVÁBBÍTÁSA AZ IP FELETT

1. rész
Bevezető áttekintés
Médiakezelő protokollok (RTP, RTCP, RTSP)

Dr. Szabó Csaba Attila
egyetemi tanár
BME Híradástechnikai Tanszék
szabo@hit.bme.hu

April 23, 2013
Budapest

Multimédia alkalmazások

- *A multimédia alkalmazások fő csoportjai:*
  - Tárolt audió- és videóstreaming
  - Élő audió- és videóstreaming
  - Interaktív real-time audió és videó

- *Milyen igényeik vannak a hálózattal szemben („szolgáltatásminőség”: l. kicsit később)*
  - Késleltetés-érzékenyek
    (késleltetés és késleltetés-ingadozás)
  - Adatvesztésre általában nem érzékenyek
  - Éppen ellentétesen az adatkommunikációval

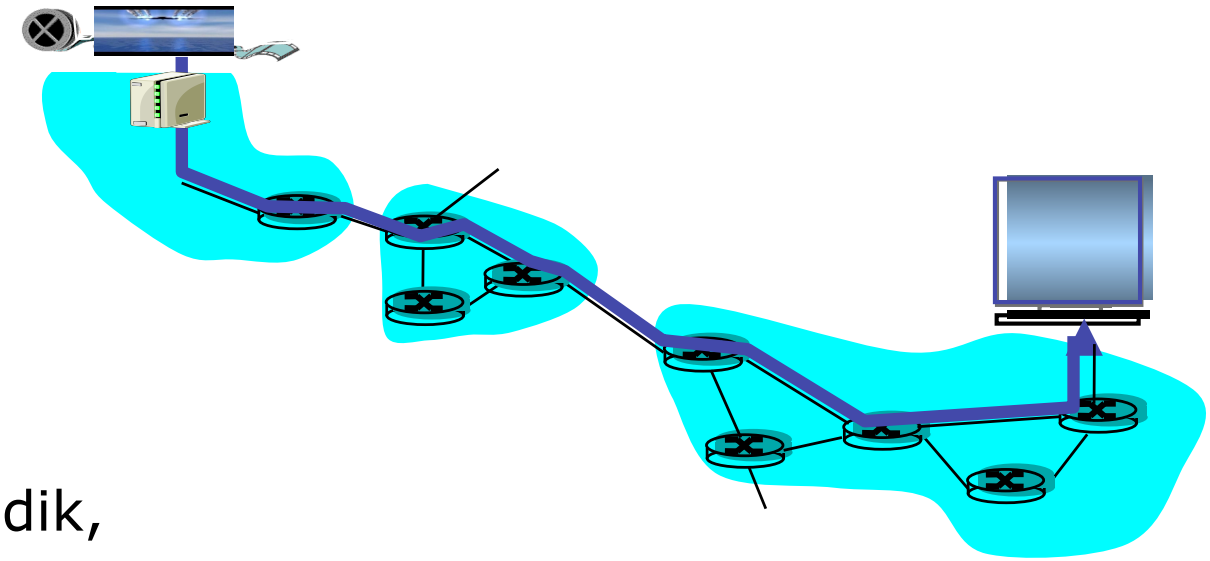
Tárolt média letöltése streaminggel

Streaming?
Szemben a hagyományos médiafájl-letöltéssel, amikor egyetlen nagy csomagban töltődik le a tartalom, itt folyamatos csomagküldés és közben feldolgozás a vevőben

A tartalom a forrásnál tárolódik (médiaszerver)

Lejátszásra kerül a kliensnek

A lejátszás elkezdődik, mielőtt a teljes anyag megérkezik



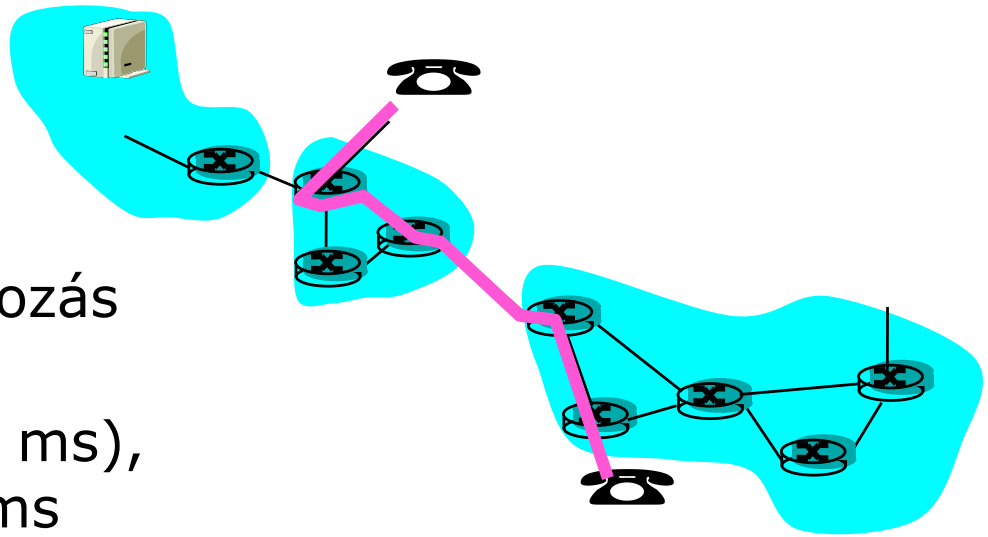
Interaktivitás: videomagnó-szerű funkciók szükségesek (előre-hátra, szünet, állj stb.)

Élőmédia-streaming

- Alkalmazási példák:
  - rádió-, TV-állomások az interneten
  - élő előadások („webinar”)
  - élő sportesemények
- Streaming:
  - playback-tár
  - lejátszás késleltetéssel
- Interaktivitás:
  - néhány, a tárolt média lejátszásánál használt funkció (persze pl. gyors előre nincs)

Interaktív real-time audió és videó

- Alkalmazási példák:
  - VoIP, IP feletti telefonálás
  - videokonferencia
- Igények:
  - kis késleltetés,
  - kis késleltetésingadozás
  - pl. beszédnél:
    150 ms (max. 300 ms),
    ingadozás pár 10 ms



- Új funkció: hívásvezérlés

Szolgáltatásminőség
QoS – Quality of Service

- Mi a **QoS** = végpontok közötti garanciák, adott időszakra és adott forgalom mellett, az alábbi és hasonló paraméterekre vonatkozóan:
  - Rendelkezésreállás
  - Átviteli sebesség, „sávszélesség”
  - Késleltetés, késleltetésingadozás
  - Adatvesztés
- **QoS-paraméterek** – pl. csomagkésleltetés, csomagvesztés
- **Forgalomleírók** – pl. csomagsebesség (csúcs-, átlagos)
- **QoS- (szolgáltatási) osztályok** (IP: best effort?)
- **A QoS biztosításának eszközei:**
  - Torlódásvezérlés
  - Preventív: beengedésszabályozás
  - Reaktív: torlódásvezérlés

Példa: beszéd-csomagkommunikáció, beszédátvitel IP felett

April 23, 2013
Budapest

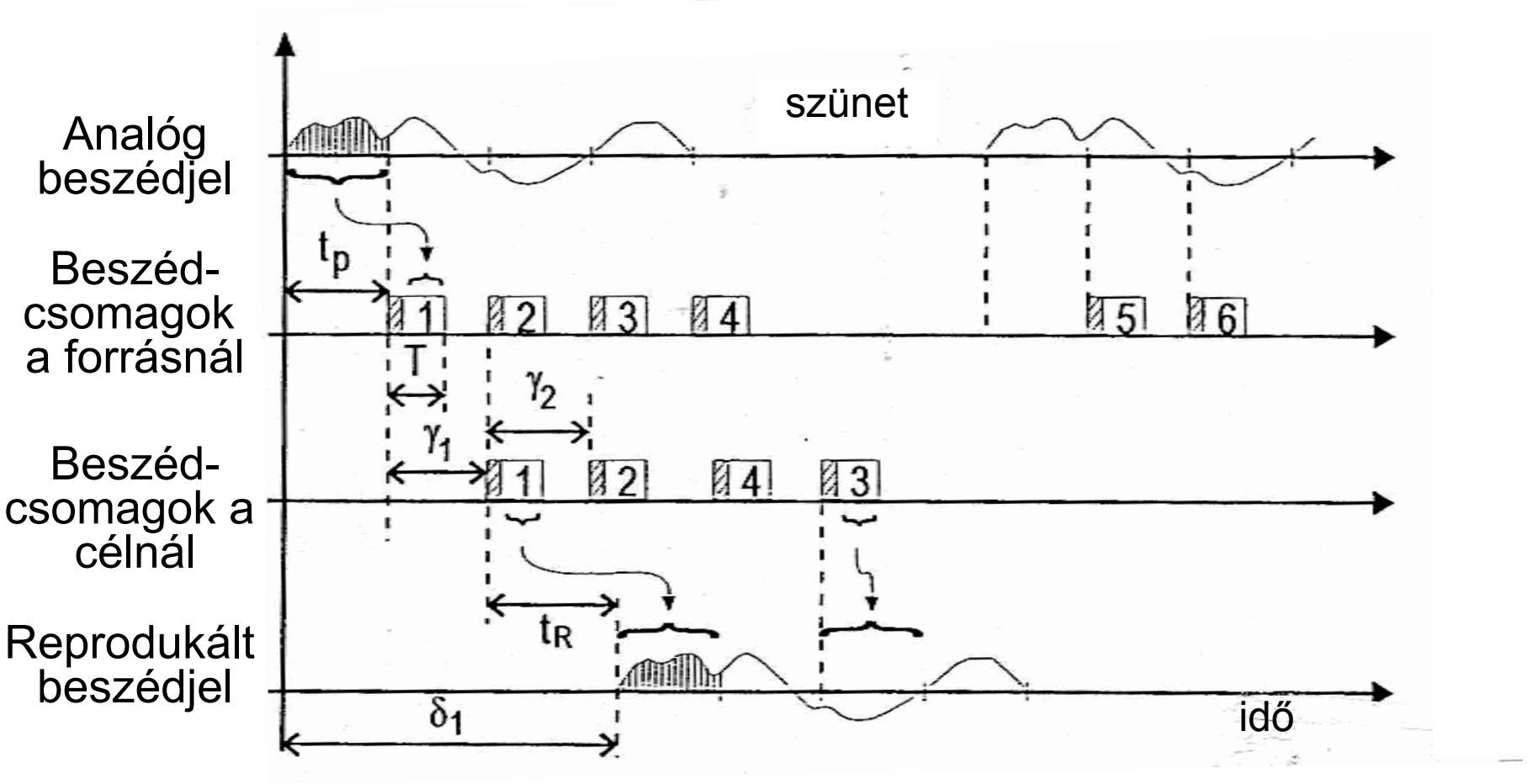
Beszédfeldolgozás beszédcsomag-kommunikációs rendszerekben

- Analóg-digitális átalakítás
  - A 64 kbit/s-os beszéd:
    - mintavétel 8 kHz-cel, azaz 125 mikroszekundumonként
    - a minták ábrázolása 8 biten (kerekítése 256 szintre)
    - tehát 8 bit 125 μs-nként
  - „PCM” – pulse code modulation, az eljárás neve a klasszikus digitális telefóniában
- Redundanciák kivonása a beszédminta-folyamból
  - Tömörítési eljárások: PCM-DPCM-ADPCM-CELP
- Az inaktív szakaszok kivonása
  - Szünet/aktivitás detektálás (VAD - Voice Activity Detection)
- Csomagokká alakítás
  - A beszédcsomag mérete függ a forrássebességtől és hogy milyen hosszú beszédszakaszt teszünk bele egy csomagba.

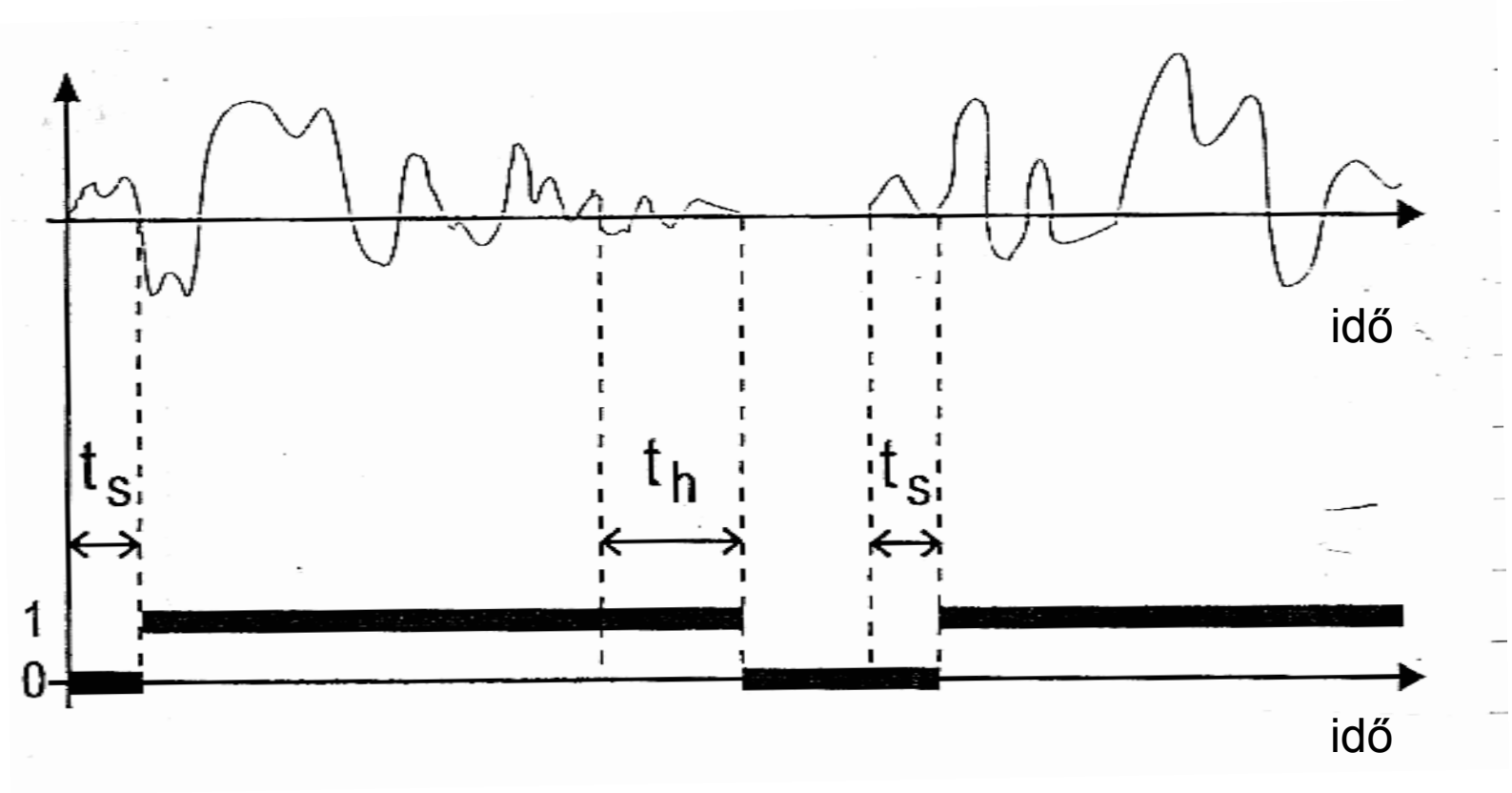
Néhány beszédtömörítés-szabvány összehasonlítása *

ITU-T szabvány	Kódolási módszer	Bitsebesség [kbit/s]	Bonyolultság	Késleltetés [ms]
G.711	PCM	64	1	0,125
G.726	ADPCM	32	10	0,125
G.728	Low Delay-CELP	16	50	0,625
G.729	CS-ACELP	8	30	15
G.723.1	ACELP	6,3/5,3	25	37,5

Beszédcsomagolás és -visszaállítás



Szünet/aktivitás-detektálás



Tipikus beszédcsomagméretek

- Pontosabban: payload-méretek
- Tipikus beszédszakasz, amelyet egy csomaggá alakítunk át: néhánytól ms-tól néhány 10 ms-ig
  - a csomagolás fix kezdeti késleltetési komponenst okoz
  - ha a csomag elveszik (nincs pótlás): viszonylag rövid szakasz essen csak ki

- 1. példa: 10 ms és tömörítés nélkül 80 byte.
- 2. példa: 20 ms és 2-szeres tömörítés esetén 80 byte.
- 3. példa: 6 ms és tömörítetlen beszéd esetén 48 byte.

Multimédia kommunikáció: Mire van még szükségünk az eddig megismert protokollokon túl?

- IP:
  - „best effort”-szolgáltatás, datagram átvitel a hálózaton a végpontok között
  - nincs késleltetésgarancia, sőt semmilyen garancia arra, hogy a csomagok egyáltalán eljutnak a címzetthez

- TCP vagy UDP:
  - kommunikáció támogatása a végpontok alkalmazásai között
  - eddig még a payload bármi lehetett, nem kezeltük, hogy milyen
  - IP, UDP összeköttetésmentes,
    TCP összeköttetés-alapú, de ez még nem „hívásvezérlés”

Mire van még szükségünk?
Feladatcsoportok és jellegzetes protokollok

- Médiakezelés – médiaformátumok kezelése, médiaátvitel „támogatása”
  - RTP, RTCP, RTSP (1. rész)
- Hívásvezérlés – kapcsolatok létrehozása, bontása, menedzselése a kommunikáló felek/alkalmazások között
  - (H.323) és SIP (2. rész)
- Szolgáltatásminőség biztosítása – a médiakommunikáció igényeinek kielégítése
  - IntServ*, DiffServ*, RSVP (3. rész)

  ** nem protokoll, hanem módszer*

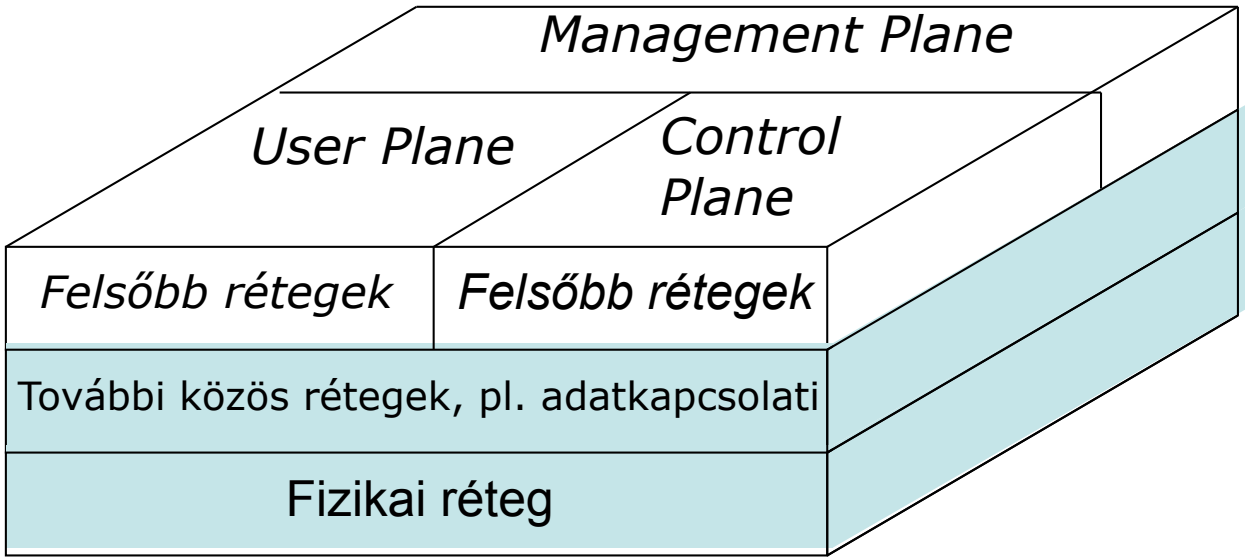
Egy kis „rendcsinálás”: továbbfejlesztett architekturális modellre lenne szükség *

- Egyre feljebb megyünk az architektúrán:
  - egyre kevésbé lesznek tisztán besorolhatók a funkciók egy-egy rétegbe az OSI szerint, ill.
  - mostantól kezdve minden az alkalmazási réteg része, a TCP/IP szerint.
- Az egyes funkcionalitások nem is homogének:
  - nem mindegyik közvetlen része a felhasználói adatkommunikáció folyamatának,
  - vannak olyanok, amelyek ehhez segítséget nyújtanak,
  - vannak olyanok, amelyek magának a hálózatnak a fenntartásához szükségesek.
- Ezért „többsíkú” modelleket találtak ki, amiről már beszéltünk a hálózati architektúrák bevezetésekor.

A távközlésben használatos rétegezett (és többsíkú) architektúra *

A B-ISDN szabványosítási környezetében vezették be *User, Control, Management Planes*

Felhasználói (adat) sík
Vezérlő sík
Menedzsment sík



Az egyes síkok közös alsóbb rétegekre támaszkodhatnak és saját felsőbb rétegekkel rendelkeznek

Vezérlősík: pl. hívásvezérlő protokollok

Menedzsmentsík: hálózatmenedzsment

Multimédia kommunikáció 1. rész: Médiakezelő protokollok

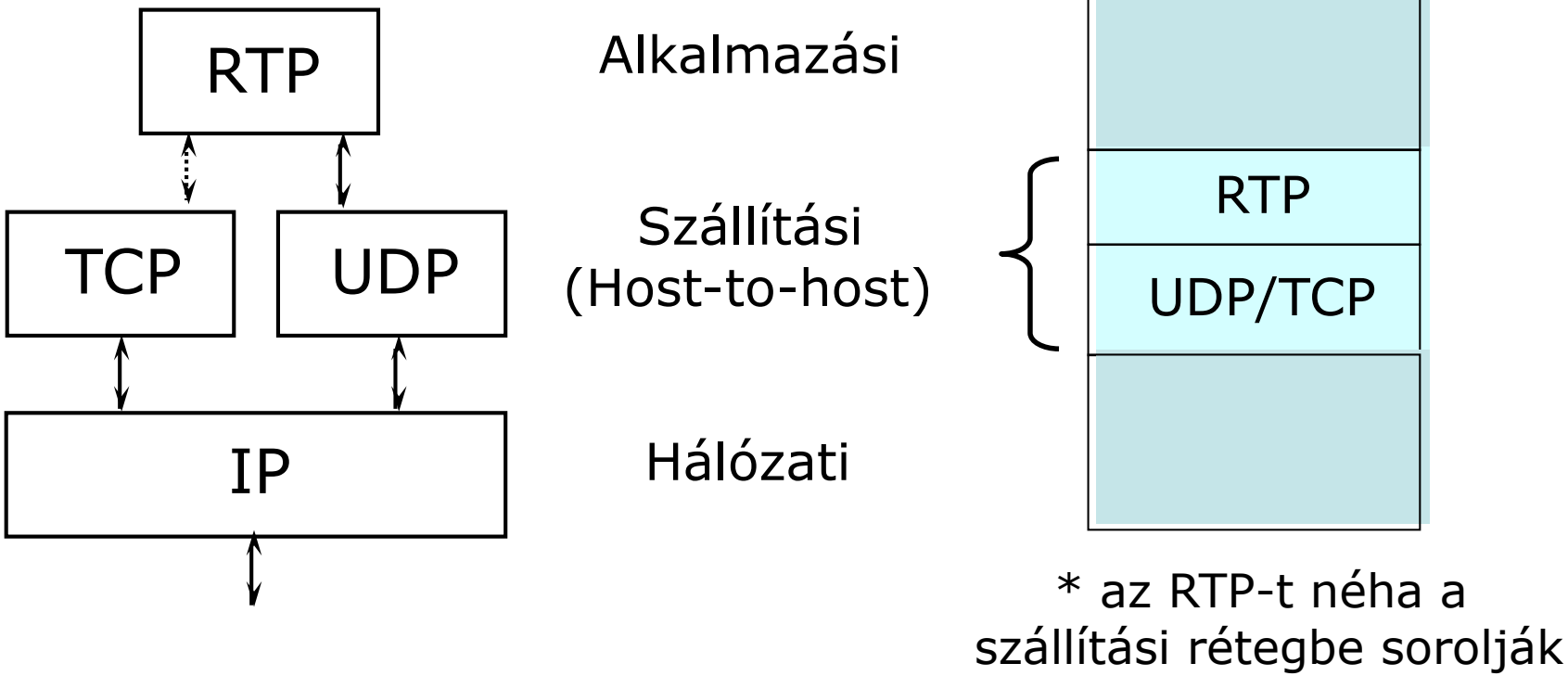
- **RTP – Real-time Transport Protocol**
- RTCP – Real-Time Transport Control Protocol
- RTSP – Real-Time Streaming Protocol

- *Ezek mind IETF-protokollok, RFC-kben vannak definiálva*

RTP és RTCP

- Mi az **RTP** és mi nem:
  - a payloadjában média-, pl. beszédinformációt hordoz
  - szállítási protokoll felett működik
  - „támogatja” a médiafolyamok (streamek) szállítását
  - de önmagában nem nyújt QoS-garanciát
- RTCP:
  - végpontok közötti QoS-monitorozás eszköze
- Különböző UDP portokat használnak párban
  - RTP: páros számú portot
  - RTCP: a következő páratlant
- RTP, RTCP: az RFC 1889-ben specifikálták

Az RTP helye az IP protokollcsaládban

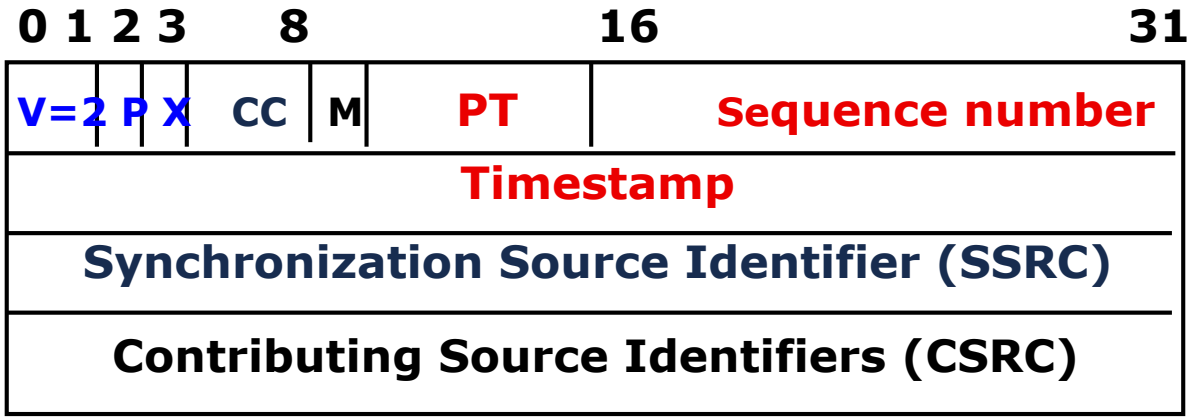


Az RTP szolgáltatásai

- Payload-típusok (médiatípusok, tartalomtípusok) kezelése
- Sorszámozás
- Időbélyeg - a médiafolyam jellegzetes időpontjainak megadása

- Mivel a szabvány párban definiálja az RTP-t és RTCP-t, utóbbi:
  - QoS-monitorozási szolgáltatás
  - Médiastreamek közötti szinkronizálás
- 5% RTCP forgalom, többi RTP

RTP: csomagfejrész-formátum (1)



A legfontosabb mezők a pirossal jelzettek, de azért nézzük a többit is.

Version (V, 2 bits)

Az RTP verziószáma; az RFC 1889-ben definiált módon

Padding (P, 1 bit)

Ha 1-es: van padding az RTP csomag végén

Padding - utolsó byte: hányat kell figyelmen kívül hagyni

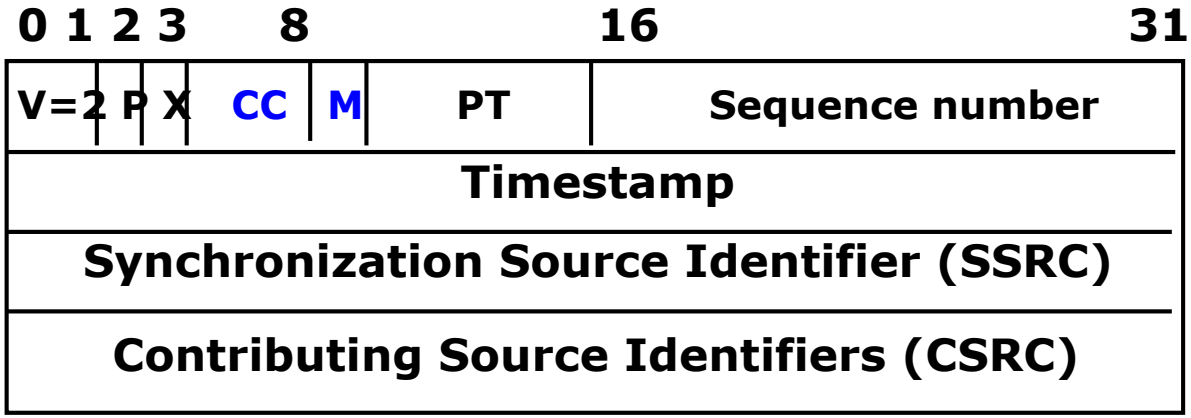
Extension (X, 1 bit)

Ha 1-es: a fejrész után változó hosszúságú fejrész kiterjesztés.

Ha van kiterjesztés: első 2 byte a hosszát adja meg

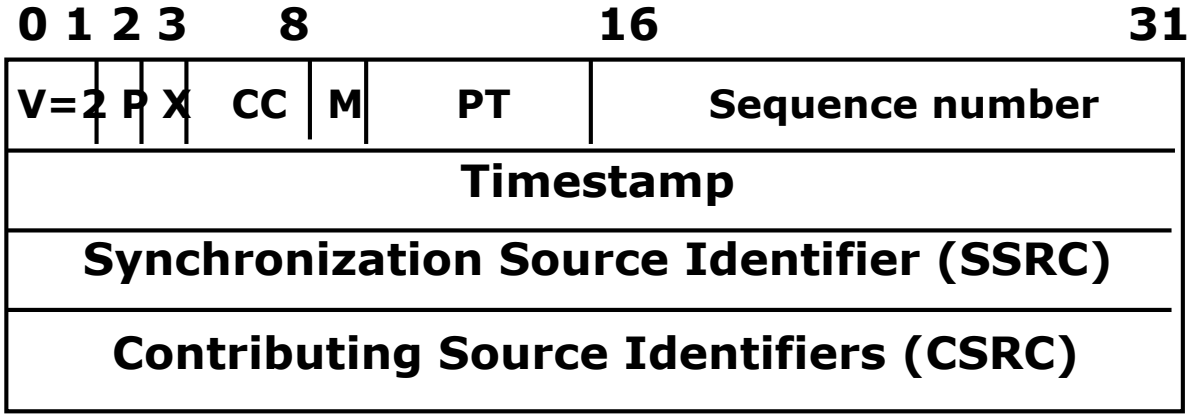
A kiterjesztés a fix fejrész utolsó érvényes mezője után következik

RTP: csomagfejrész-formátum (2)



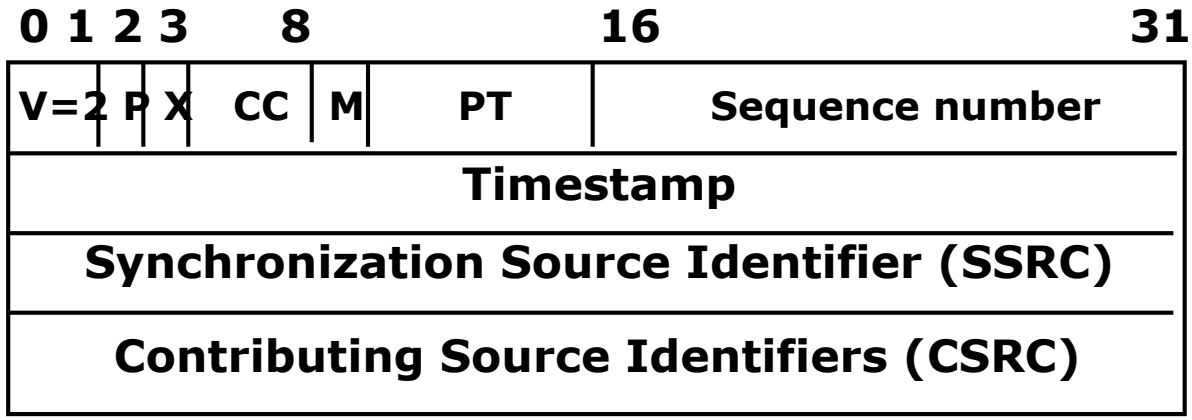
- CSRC count (CC, 4 bits)
  - a CSRC azonosítók száma = a multiplexált források száma (a források megadása: a CSRC mezőben)
  - csak egy forrás: CC = 0
- Marker (M, 1 bit)
  - a csomagfolyam szignifikáns eseményeinek megjelölése
  - példák:
    - kerethatárok a különféle kódolási módszereknél
    - a beszéd aktív időszakainak kezdete/vége
  - az aktuális interpretációt a “profile” adja meg

RTP: csomagfejrész-formátum (3)



- Payload type (PT, 7 bit)
  - “profile”, amely legtöbbször a médiakódolási típusokat kezeli, azoknak payload-formátumokat feleltet meg
- Sequence number (16 bit)
  - lehetővé teszi az elveszett csomagok detektálását és a csomagsorrend helyreállítását
  - kezdőértéke véletlen szám (l. később); minden elküldött RTP csomag után eggyel növelődik
- Timestamp (32 bit)
  - Az RTP csomag első oktettjének megfelelő pozíció valódi ideje a médiafolyamban

RTP: csomagfejrész-formátum (4)



- SSRC (32 bit)
  - Az RTP csomagfolyam forrását azonosítja, az RTCP rendeli hozzá, véletlenszerűen
- CSRC (0…15-ször 32 bit)
  - contributing source: az „RTP mixer” által létrehozott kombinált csomagfolyam komponensét azonosítja

RTP „profile”-ok

= A médiakódolást felelteti meg payload-formátumoknak
Példák beszédátvitelnél (továbbiakat specifikál az RFC):

Média kódolás	Mintavételi seb., kHz	Adatsebesség, kbit/s	RTP payload type
G.711 *)	8	64	0
G.722 *)	16	48-64	9
G.728 *)	8	16	15
GSM	8	13	3
„Comfort noise”	-	-	19

Videó-payloadok pl.: 26: JPEG, 33: MPEG2
**) ezek ITU-T beszédkódolási szabványok*

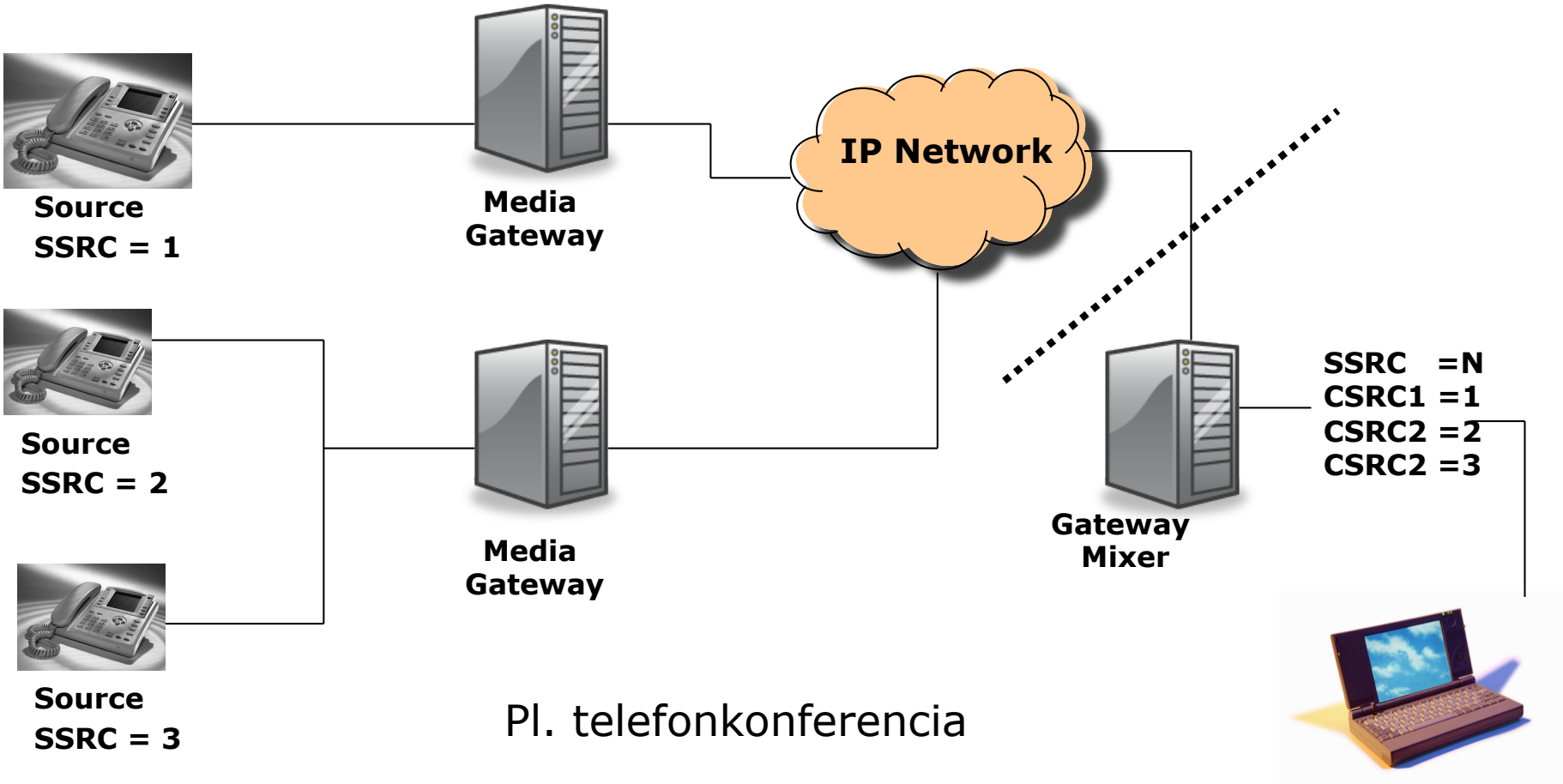
SSRC, Synchronization source

- A stream forrását azonosítja, független a hálózati címtől
  - Véletlen szám, egyedi kell hogy legyen a session-on belül
  - Pl. mikrofon, kamera, vagy akár mixer
- Ha több streamet generál ugyanazon forrás egy session-ön belül: mindegyikhez más SSCR-t rendel hozzá
  - Pl. több kamerától
- A vevő ennek alapján válogatja egy csoportba a csomagokat pl. playback esetén

RTP mixer

- Közbülső rendszer, amely fogadja az RTP csomagokat egy vagy több forrásból
  - megváltoztathatja az adatformátumot
  - kombinálja a csomagokat
  - új RTP csomagként továbbítja
  - kombinált streamre új időzítés
- Mixer által összerakott új csomagok SSRC-je a mixer lesz
- Viszont CSRC-ben felsorolja az eredeti forrásokat

RTP Mixer



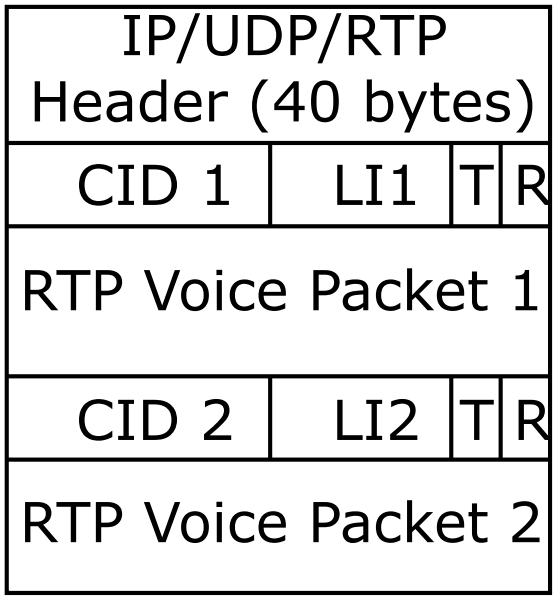
Pl. telefonkonferencia

RTP csomag megjelenítése hálózatmonitoron

```
RTP Header

RTP: Version = 2
RTP: P Bit = 0 (Padding Does Not Exist)
RTP: X Bit = 0 (No Extension Header Follows)
RTP: CSRC Count = 0
RTP: Marker Bit = 0
RTP: Payload Type = MU-Law Scaling (PCMU) (0)
RTP: Sequence Number = 19382
RTP: Time Stamp = 7241.899 seconds
RTP: Synchronization Source Indentifier = 0x1C1A054A
RTP: 160 Bytes Of PCMU Payload Data

00 90 a0 00 00 73 00 90   a0 00 00 95 08 00 45 00  .....s.. ......E.
00 c8 00 37 00 00 78 11   a1 cb 0a 01 46 11 0a 01  ...7..x. ....F...
46 10 04 02 04 05 00 b4   00 00 80 00 4b b6 03 74  F....... ....K..t
05 58 1c 1a 05 4a ff ff   ff ff ff ff ff ff ff ff  .x...J.. ........
...
```

RTP payload-multiplexelés

Javítja a sávszélesség-kihasználást
Példa: 2 beszédforrás



CID: Channel ID, LI: Length Indicator,
T: Transmit bit, R: Reserved

RTP-t használó alkalmazások

- *QuickTime (Apple)* – audió- és videóstreaming
- *RealAudio, RealVideo* (RealNetworks) – médiastreaming
- *NetMeeting (Microsoft)* – IP telefónia, whiteboard, text chat, alkalmazásmegosztás
- *CU-SeeMe* – a NetMeeting-hez hasonló
- *IP/TV (Cisco)* – jó minőségű videó/audió, élő, VoD

RTSP – Real Time Streaming Protocol

- Kapcsolat felépítése és ellenőrzése a session végpontjai között
- VCR-jellegű funkciók, azaz lejátszás-vezérlés:
  - elindítás tetszőleges pozícióból
  - előre, hátra, megállás, folytatás
  - különböző lejátszási sebesség kérése
  - különböző bitsebesség beállítása
- RTSP szerverek nagy része RTP-t használ

RTSP

- Hasonló mint a HTTP, de ez állapotfüggő protokoll, több kérés típussal
  - kliens-médiaszerver kapcsolat
- Pl. kérésekre:
  - SETUP: specifikálja hogy kell átvinni az adott média stream-et (PLAY kérés előtt)
    - Portszámok RTP-re és RTCP-re
    - Szerver: jóváhagyja és elküldi saját portszámait
  - PLAY: egy vagy több médiastream lejátszása
    - Megadható a lejátszási intervallum is

RTCP – Real-time Transport Control Protocol

- Végpontok közötti információt szolgáltat a minőségről a kapcsolat résztvevőinek:
  - késleltetés
  - jitter
  - vett csomagok, elveszett csomagok stb.
  - RTT – round trip time – teljes átviteli idő
- RTCP = nem jelzésátviteli protokoll!
- Hatására az alkalmazás módosíthatja a session jellemzőit (kódolás váltása, folyam korlátozása)
- Minden session résztvevőnek CNAME egyedi azonosítót biztosít
  - SSRC azonosító változhat végpontonként, de ez nem
  - 3. fél is monitorozhat végig

RTCP csomagtípusok

- SR (Sender Report)
  - Aktív adók statisztikái
  - Egy session minden résztvevőjét informálja
  - Abszolút időbélyeggel: audió és videó stream szinkronizálása
- RR (Receiver Report)
  - Passzív résztvevőktől (nem forgalmaznak RTP csomagokat) származó információk

Sávszélesség-hozzárendelés az SR/RR forgalom számára

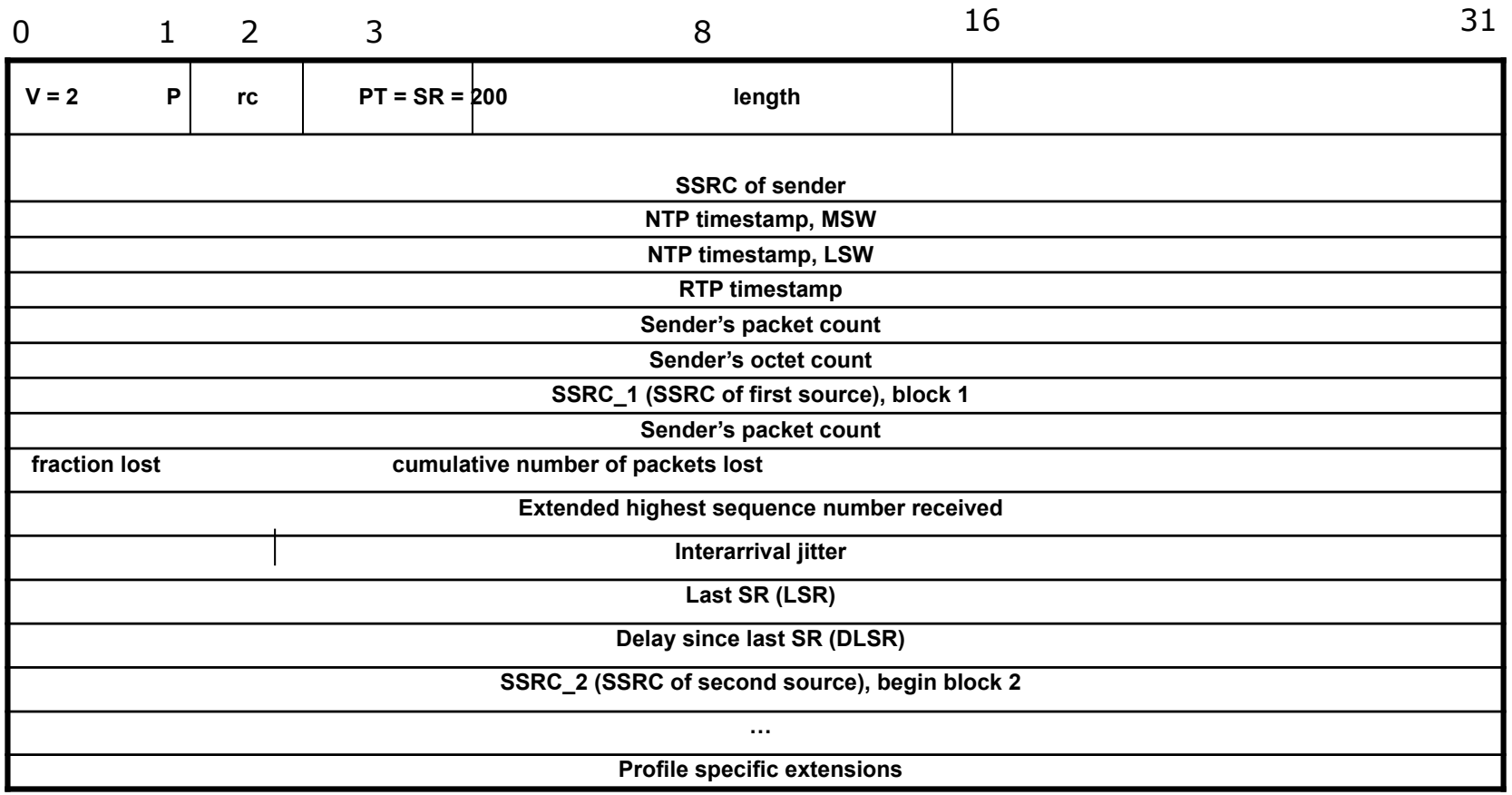
- *Max: a teljes sávszélesség 5%-a*
- *Ennek 75%-a az RR számára, 25%-a az SR-nek*

- SDES: Source description
  - CNAME elküldése a session résztvevőinek
  - További infók a forrás tulajdonosáról (név, e-mail cím, telefon)
- BYE: End of participation
  - Pl. a forrás közli, hogy elhagyja a konferenciát, mindenki hallja

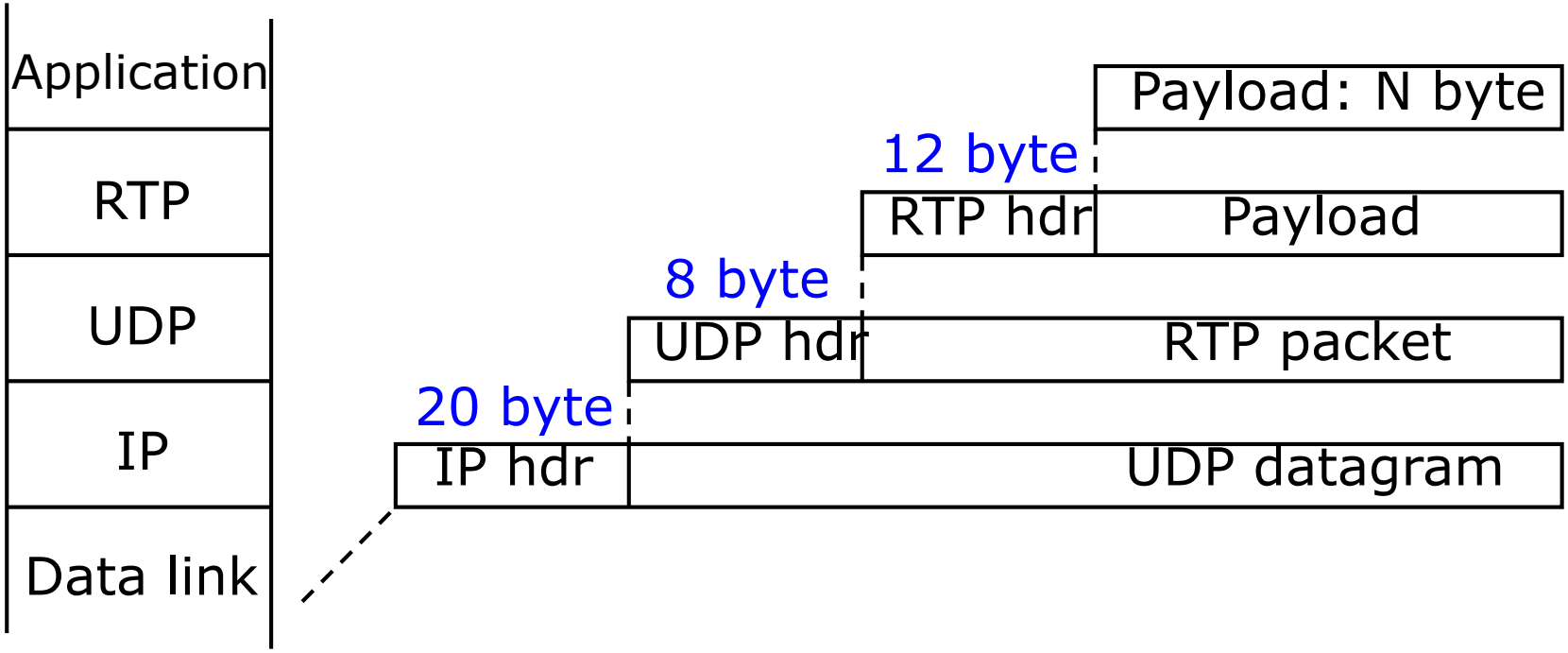
Gondok az RTCP-vel

- Ha sok felhasználó és hosszú sessionok: ritkán jön RTCP jelentés (5% korlát miatt)
  - Pl. IPTV esetén, több perc vagy akár óra után csak, miközben 10 mp az elfogadható
- Elavult jelentések miatt a forrás rossz intézkedéseket hozhat QoS szempontjából
- Megoldás: hierarchikus aggregáció
  - Több jelentés összevonása egy összefoglaló jelentésbe
  - Összevonás: node-ok hierarchiája, fastruktúra

RTCP Sender Report formátum *

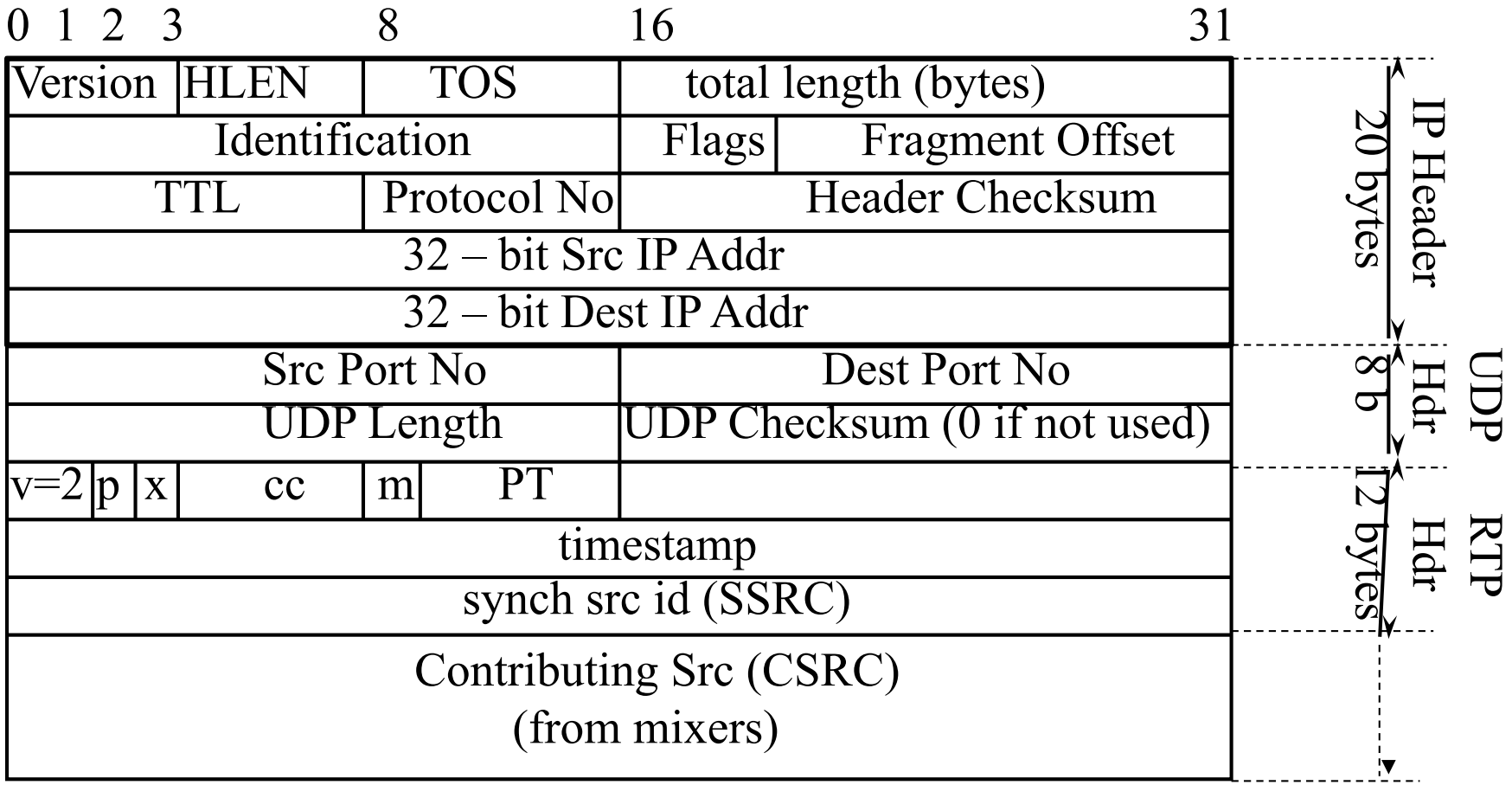


Most már túl sok protokollunk van ☺
Átvitelisebesség-igény a fejrész-halmozódás miatt?



Overhead = 40 byte plusz az adatkapcsolati réteg fejrésze
Egy médiacsomag hossza = 40+N+ link layer header

Fejrésztömörítés (1)
Nézzük meg az együttes fejrészt!



Fejrésztömörítés (2)

- Cél: az overhead csökkentése
- Kezeljük együtt mindhárom protokollt (IP + UDP + RTP)!
- Elv: a kapcsolat kezdete után kis változások a fejrészekben
  - Sok mezőben nincs változás a kapcsolat alatt
  - Vannak mezők, amelyek változnak, de jósolható módon, pl. sequence number
- Továbbá: redundáns információ (pl. megvan az adatkapcsolati fejlécben)
- Először tömörítetlen és teljes fejrész elküldése
- Utána a kompresszor és a dekompresszor megállapodnak egy Context Session ID-ben (CID);
  (8/16 bit hosszú) és a tömörítés formátumában
  - CID: IP címek, UDP portok, RTP SSCR halmazát azonosítja

Fejrésztömörítés (3)

- Csak a következők változnak
  - IP:
    - Teljes hossz: ezt az adatkapcsolati fejléc is tartalmazza, nem kell átvinni
    - Header checksum: elhagyható, adatkapcsolatira bízva
    - ID: inkrementálódik, IPv6-nál már nincs
  - UDP:
    - Ugyanaz az első kettő, mint IP-nél
  - RTP:
    - Seq. number: inkrementálódik
    - Időbélyeg: mintavételi időkkel növekszik
    - M bit
    - CSRC lista ritkán, csak akkor kell átvinni

Fejrésztömörítés (4)

- Compressed RTP (cRTP) protokoll
- 4 formátum
  - FULL_HEADER: teljes tömörítetlen fejrészek plusz CID és Sequence No
    - Seq. No: csomagvesztés ellen kom. és dekom. között
  - COMPRESSED_UDP:
    IP + UDP tömörített (2 v 6 byte), RTP tömörítetlen
    - Ha változik az RTP payload típus
  - COMPRESSED_RTP:
    normál eset, minden fejrész tömörítve
    - Delta kódolás
  - COMPRESSED_NON_TCP:
    IPv4 ID mező tömörítetlen
    - védekezés nagy csomagvesztés esetén

Fejrésztömörítés alkalmazása

- Kis sebességű linkeken érdemes csak használni, és
- ahol alacsony a hibaarány
  - Pl. vezeték nélküli környezetben nem
- Szolgáltatások:
  - Interaktív: videokonferencia, IP telefónia

Voice over RTP adatátviteli-sebesség számolása (adatkapcsolati réteg nélkül)

Payload-formátum	Névleges sebesség	Csomagolási idő [ms]	Payload méret [byte]	Átvitelisebesség-igény, tömörítetlen fejrészek [kbit/s]	Átvitelisebesség-igény, tömörített fejrészek [kbit/s]
G.711	64 kbit/s	20	160	80	64.8
G.711		10	80	96	65.6
G.729	8 kbit/s	20	20	24	8.8
G.729		10	10	40	9.6

RTP/RTCP, RTSP: összefoglalás

- RTP - médiakezelő protokoll
  - UDP felett működik
  - Különböző médiakódolási formátumokat támogat
  - Az átvitelért felelős, a QoS-ért nem
  - A fejrészt (az UDP+IP-vel együtt) kompresszióval lehet csökkenteni
- RTCP az RTP társprotokollja
  - Nem jelzésprotokoll
  - Nem QoS protokoll
  - Hasznos segédeszköz a QoS megvalósításához
- RTSP: VCR-jellegű funkciók

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Híradástechnikai Tanszék

Dr. Szabó Csaba Attila
egyetemi tanár
BME Híradástechnikai Tanszék
szabo@hit.bme.hu

MULTIMÉDIA-TOVÁBBÍTÁS AZ IP FELETT

2. rész

Hívásvezérlő protokollok:
H.323 – az ITU protokollcsaládja
SIP – Session Initiation Protocol, az IETF hívásvezérlő protokollja

Szabó Csaba Attila
egyetemi tanár
szabo@hit.bme.hu

Apr 25, 2013,
Budapest

Mire van még szükségünk?
Feladatcsoportok és jellegzetes protokollok

- Médiakezelés – médiaformátumok kezelése, médiaátvitel „támogatása”
  - RTP, RTCP, RTSP (1. rész)
- **Hívásvezérlés – kapcsolatok létrehozása, bontása, menedzselése a kommunikáló felek/alkalmazások között**
  - **(H.323) és SIP (2. rész)**
- Szolgáltatásminőség biztosítása – a médiakommunikáció igényeinek kielégítése
  - IntServ*, DiffServ*, RSVP (3. rész)

  ** nem protokoll, hanem módszer*

Mi volt az első részben?

Médiakezelés, továbbítás (media transport)

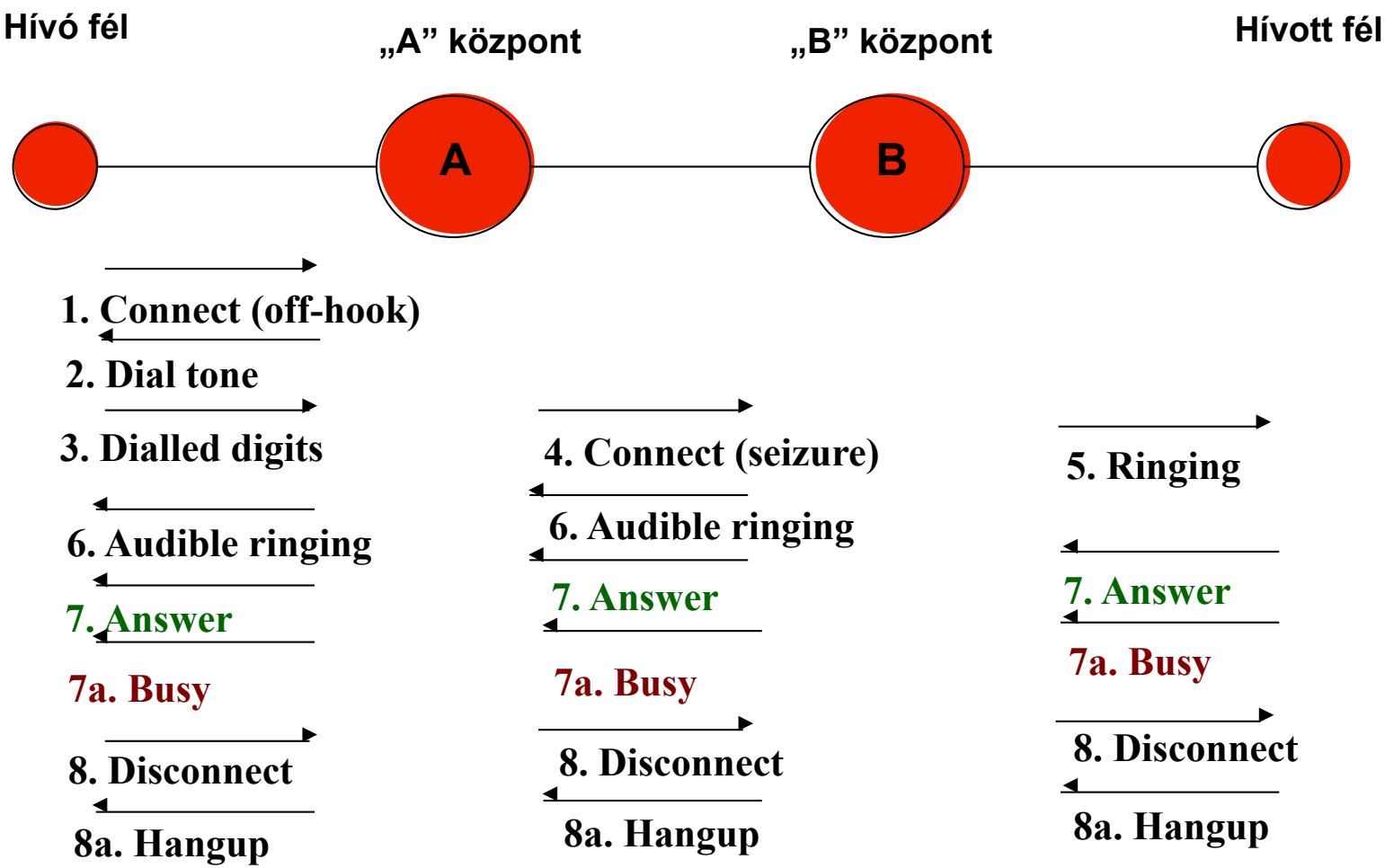
- RTP – Real Time Transport Protocol
  - Mi a feladata, mit tud nyújtani és mit nem?
  - Médiaátvitel „támogatása” (QoS-t önmagában nem)
  - Médiatípusok kezelése, sorszámozás, időbélyeg
- RTCP – ez mi?
  - Segítség QoS megvalósításához: a kapcsolatok minőségének monitorozása (pl. késleltetés, csomagvesztés)
- RTSP – és ez mi?
  - Streaming-tartalom lejátszásának vezérlése

Mi az, hogy hívásvezérlés?

- „Hívások” (kapcsolatok, **összeköttetések**) létrehozása, fenntartása, lebontása
- Az ehhez szükséges jelzések rendszere
- Hívásvezérlő protokollok (valamely szabvány szerint)
- Angolul: call processing, call control systems/algorithms/ protocols
- *Azóta van, amióta telefonálunk*
- *Ma: multimédia session*-ök menedzseléséhez, konferenciák is, akár sok végpont között*

** Mi az, hogy „session”?*

Példa hívásvezérlésre: közönséges telefonhálózat



Multimédia-hívásvezérlés IP-alapú hálózatokban

- Amit a klasszikus hívásrendszerek tudnak, továbbá
- több fontos, új elvárás (többek között):
  - multimédia-tartalmak kezelése
  - többrésztvevős összeköttetések vezérlése (konferencia)
  - helyzetinformáció kezelése, pl. hívásátadás
  - mobilitás kezelése
  - könnyű integrálhatóság a web-alapú szolgáltatásokkal
- Fő rendszertechnikák és protokollok
  - **H.323**
  - **SIP**

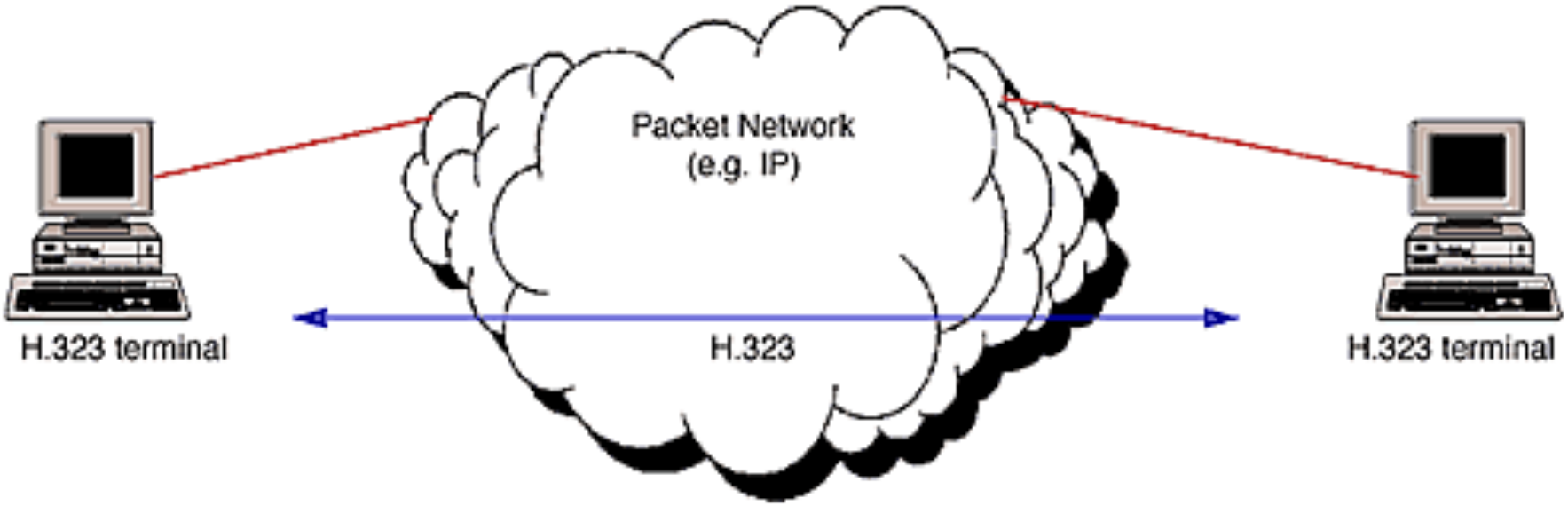
Miért két rendszer?

- (Nem kettő, több is volt ill. van...)
- A távközlési és az internetes világ sokáig párhuzamosan fejlesztette a szabványait
  - Távközlési szabványosítás: ITU – International Telecommunications Union
  - Számítógéphálózatok, IP és Internet: IETF – Internet Engineering Task Force
- Eltérő megközelítések, rendszertechnikák és megvalósítások
- **ITU: H.323**
- **IETF: SIP**
- Mit tud e két rendszer? Ezzel foglalkozunk.
- Mi lesz a jövő? Marad a két rendszer? A végén erre visszatérünk!

H.323 – az “esernyőszabvány” (umbrella standard)

- ITU-protokollcsalád, amelyet széles körben használnak a mai VoIP- és videókonferencia-rendszerekben
- = Procedúrák **csomagkapcsolt hálózatok (pl. IP)** feletti konferencia-alkalmazásokra:
  - *Pont-pont és multipont összeköttetések*
  - *Audió-, videó- és adatkommunikáció*
- Meghatározza a csomag- és áramkörkapcsolt hálózatok közötti együttműködést is
- Komplett szabványdokumentáció:
  - *Audió-, videókódolás, médiastreaming*
  - *Hívásfelépítés és –vezérlés, az ehhez szükséges jelzésátviteli protokollokkal*
  - *Regisztráció és hozzáférés-szabályozás*

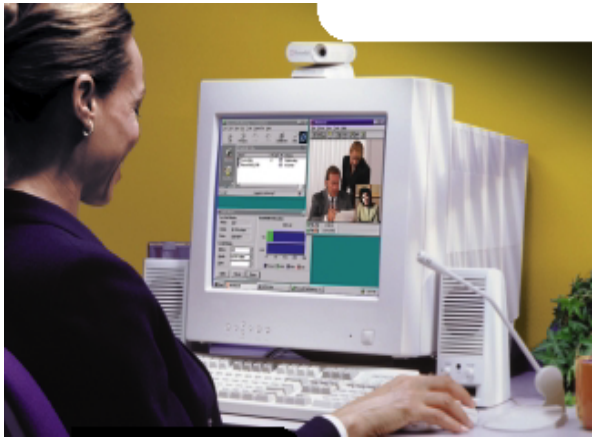
H.323 a legegyszerűbben: két terminál kommunikál csomaghálózaton



A H.323 szerinti hálózat funkcionális egységei

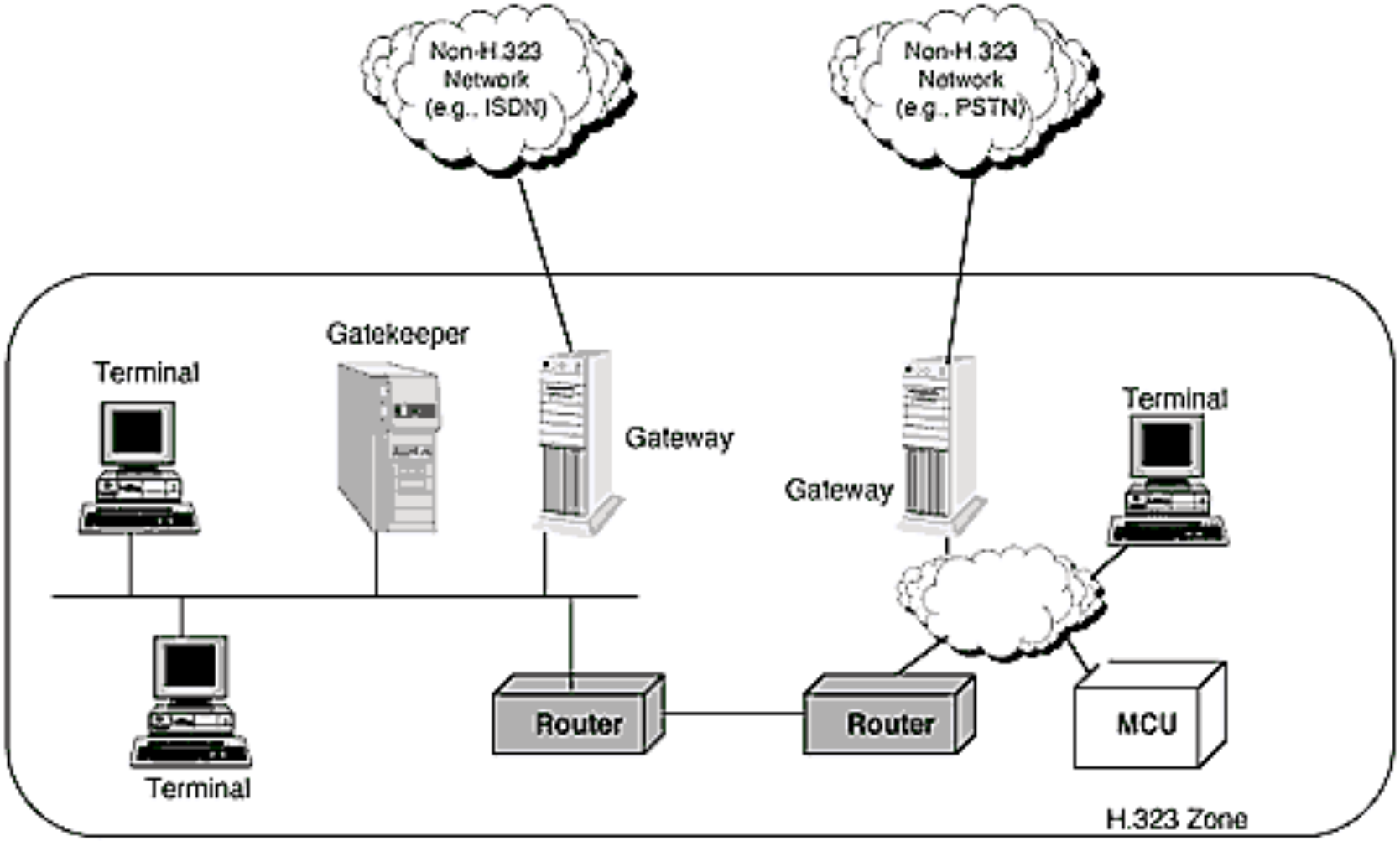
- Terminal
  - felhasználói végpont
  - lehet multimédia, de lehet csak beszéd
- Gateway
  - A H323 és más típusú terminálok közötti együttműködést biztosítja. Gyakorlatban csak az ISDN-nel (H.320).
  - Konverzió a különböző kódolások, jelzésrendszerek stb. között
- Gatekeeper
  - Opcionális, ha van: központi “intelligencia”
  - Beengedés-szabályozás, maga a hívásvezérlés opcionálisan mehet a GK-en keresztül (a média nem), erőforrás-menedzsment, autentikáció
- Multipoint Control Unit (MCU)
  - 3 vagy több terminál közötti konferencia lebonyolítására

Példák H.323 terminálokra: videókonferencia-rendszerek

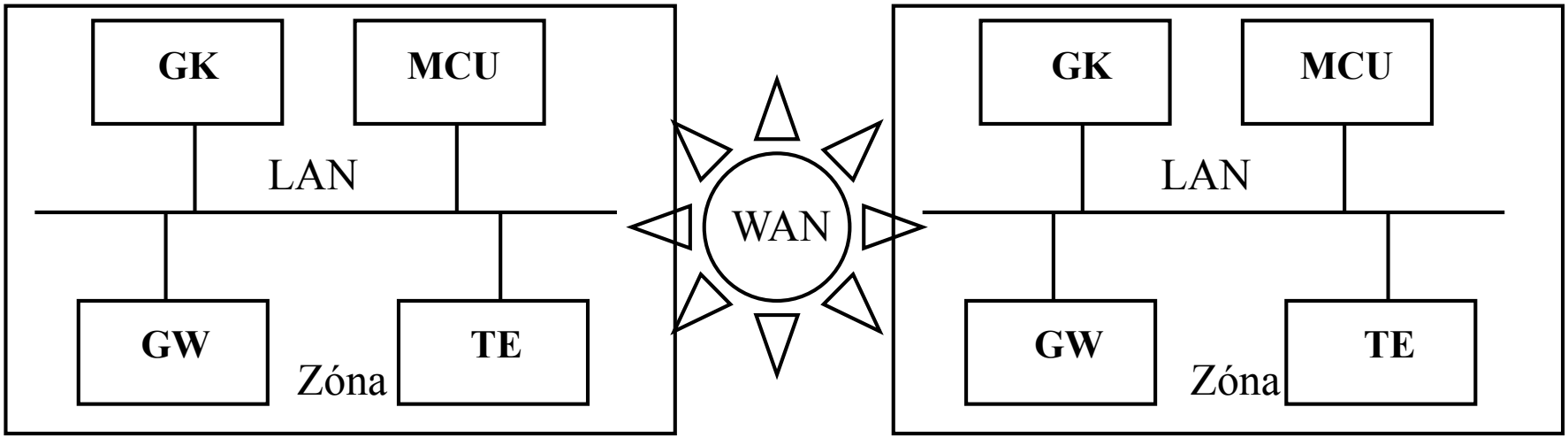


Továbbá szoft kliensek, pl. MIRIAL softphone

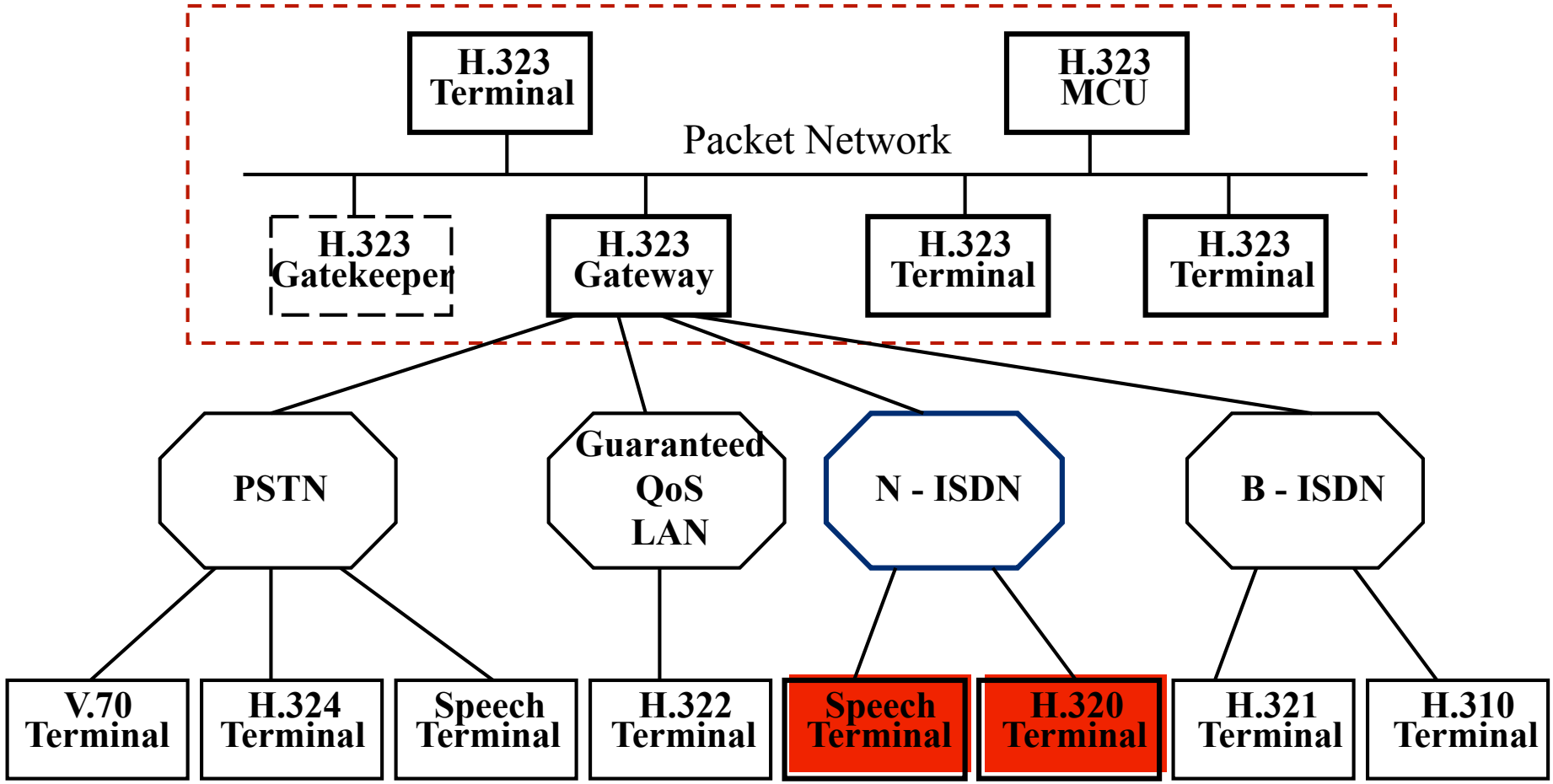
Egy H.323 szerinti hálózat



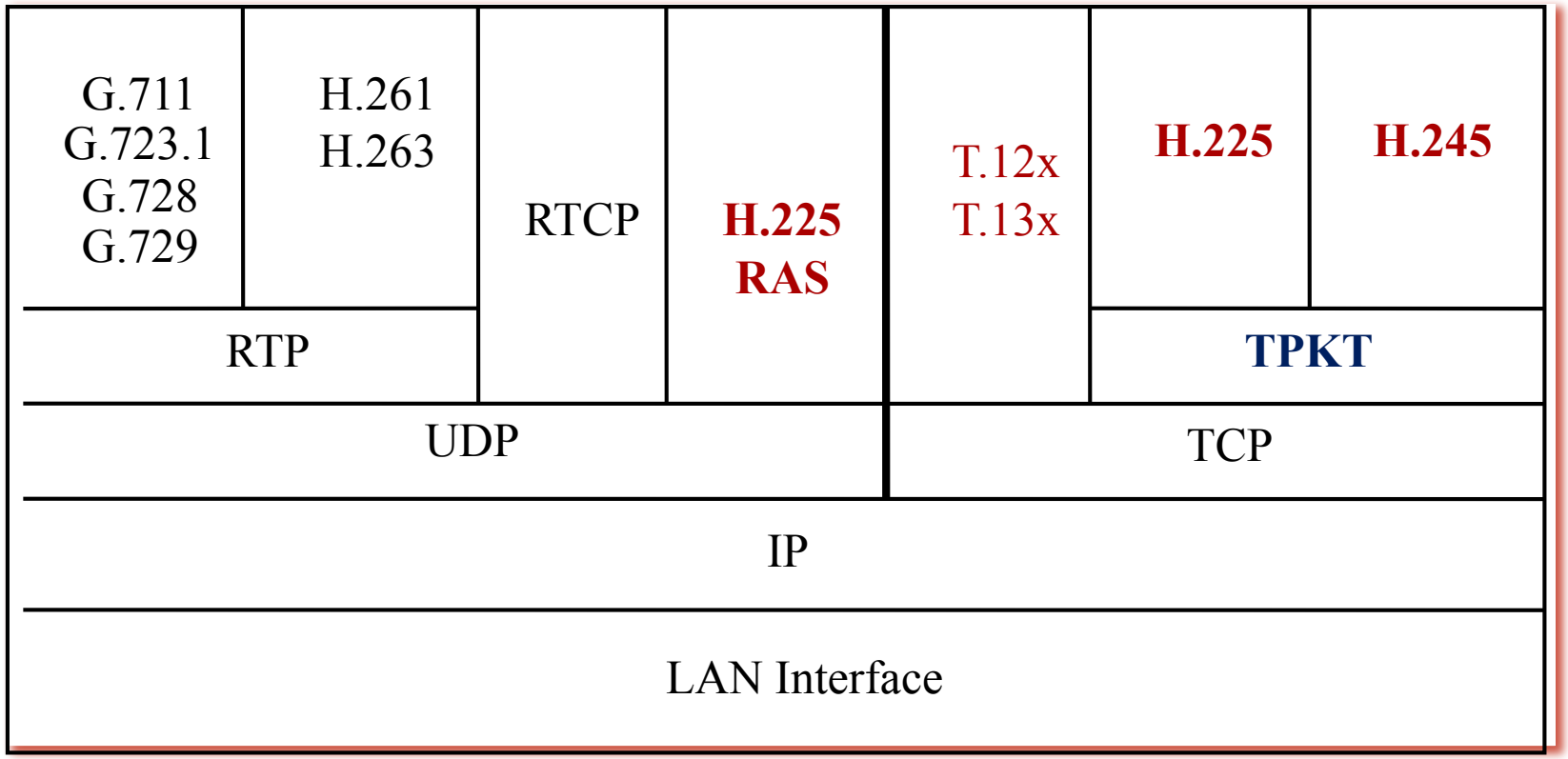
A H.323 funkcionális egységei, „zónák”



A teljes H.323 architektúra



A H.323 protokollcsalád: hívásvezérlő protokollok

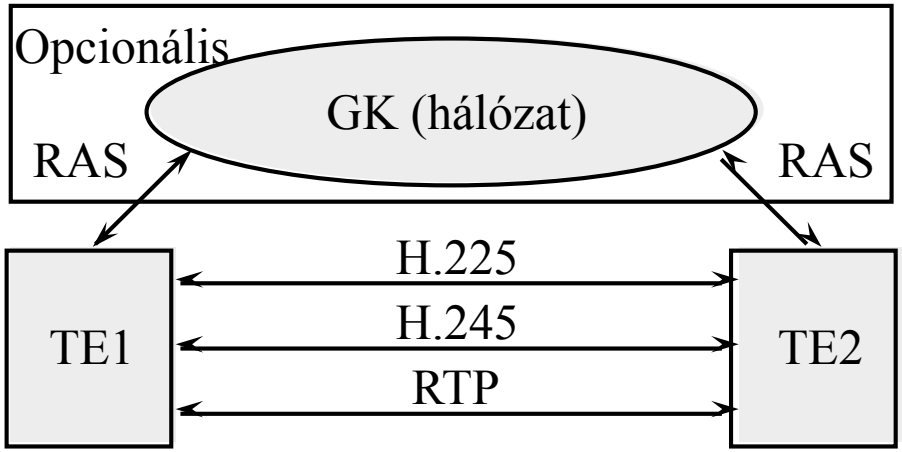


A H.323 hívásvezérlő protokolljainak áttekintése

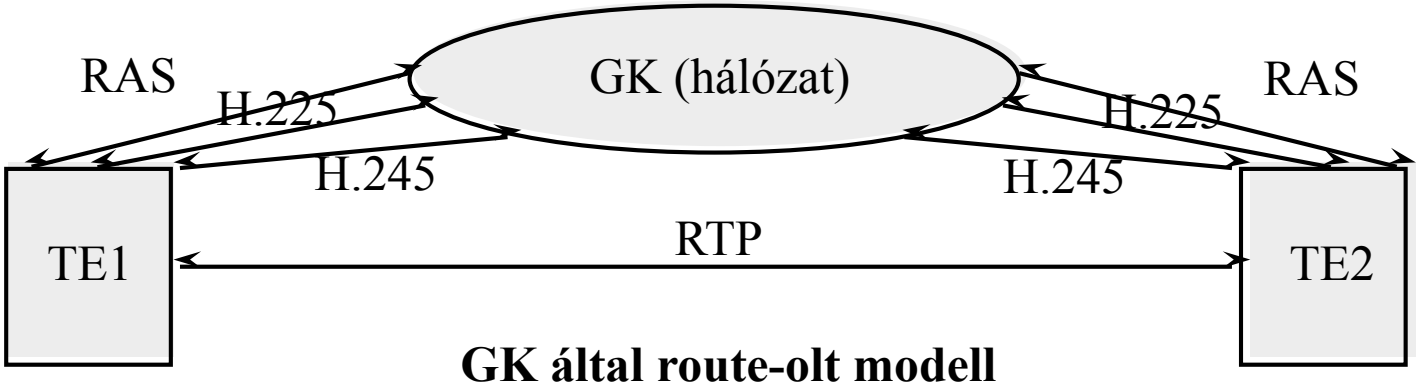
- H.225
  - A H.323 jelzésátviteli protokollja
  - TCP felett működik
- H.245
  - Hívásvezérlő protokoll
  - TCP-t felett működik (egy TPKT nevű protokoll közbeiktatásával)
- *A H.225 és a H.245 ugyanannak a hívásfolyamatnak különböző fázisait vezérlik*

- H.225.RAS *(RAS: registration-authentication-status)*
  - Gatekeeper-protokoll
  - Nem megbízható szállítási protokollt használ (UDP)

Két hívásfelépítési modell

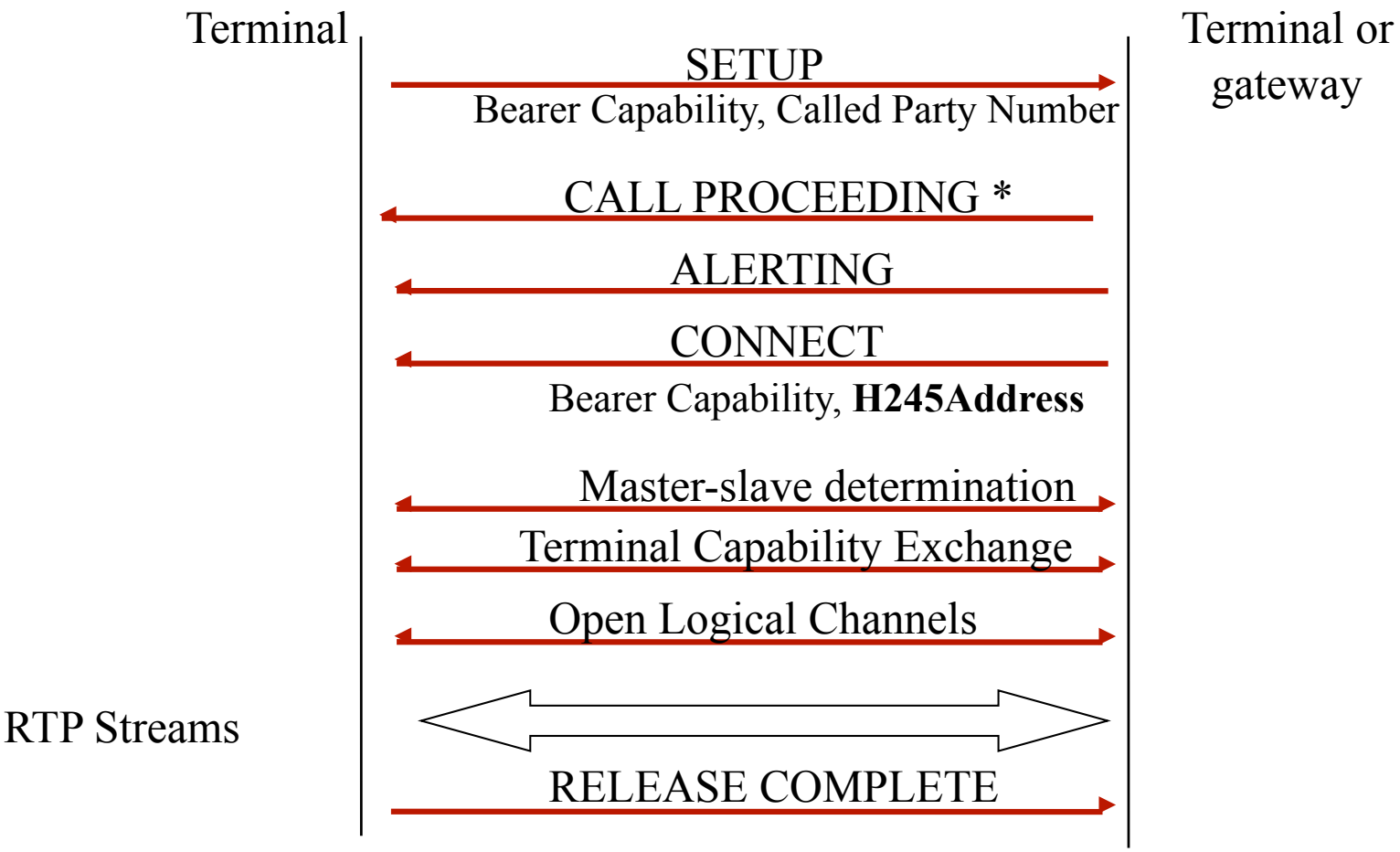


Közvetlen hívásmodell



GK által route-olt modell

A hívásfelépítés részletesebben



H.323: összefoglalás

- ITU szabvány
  - Több mindent átvett a távközlésből (pl. ISDN jelzésprotokoll)
  - Internet-protokollokat is használ (RTP, RTCP)
- Széles spektrumú szabvány
  - médiák (adat, hang, beszéd) kódolási szabványai
  - protokollok (hívásvezérlés, de ide vettek média-feldolgozási és QoS-protokollokat is)
- Funkcionális egységei a T, GK, GW, MCU
- Hívásvezérlő protokollok p-p és mp kapcsolatokhoz (p-p és konferencia)
- Állapotalapú és bináris protokoll
- Széles körben alkalmazzák
- Hátrányai (késleltetés, processzálási igény)

Az NIIF H.323-alapú videókonferencia-hálózata

Nemzeti Információs Infrastruktúra Fejlesztési Intézet
National Information Infrastructure Development Institute

Home Desktop konferencia

Kollaborációs szolgáltatások

- Aktualitások
- Bemutatás
- Dokumentumok
- Elérhetőségek
- Linkek

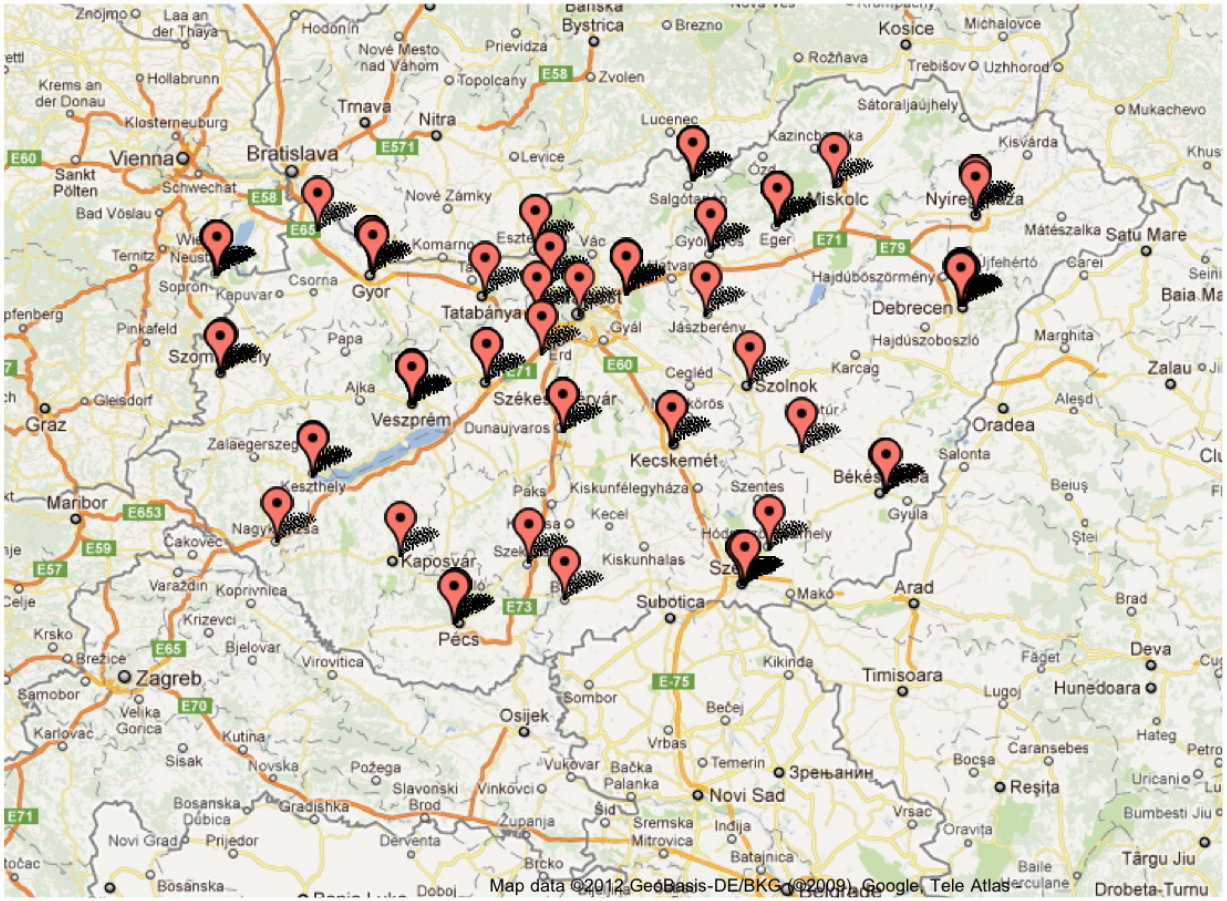
VoIP / IP telefónia

- Általános információk
- Műszaki információk
- Csatlakozás feltételei
- Nem hívható számok
- wiki
- Dokumentumok
- IP PBX projekt
- VoIP kapcsolattal rendelkező intézmények
- VOIP intézmények a térképen

Videokonferencia

- Általános információk
- Csatlakozás feltételei
- Végpontok
- Eszközök
- Forgalmi adatok
- wiki
- **VIDKONF intézmények a térképen**

VIDKONF intézmények a térképen



SIP: bevezető áttekintés (1)

- Session Initiation Protocol: alkalmazási rétegbeli protokoll a TCP-IP architektúra szerint (IETF - RFC 3261)
- Session-ök létrehozása, módosítása, befejezése egy vagy több partnerrel. Mi az, hogy „session”? (Vö.: Session Layer az OSI architektúrában.)
  - *Szótár: Ülés, összejövetel, kocsmázás (biz.)*
  - ***SIP: „Session: a set of senders and receivers that communicate and the state kept in those senders and receivers during the communication.”***
- Session-öket hoz létre 2 v. több fél között
- Session-leírókat (descriptors) visz át a különböző médiatípusokra vonatkozóan képességegyeztetés céljából
- Kezeli a felhasználók helyzetinformációit, támogatja a mobilitást
- Multipoint Control Unit (MCU) funkció

Emlékeztető: a TCP/IP protokoll-architektúra

Ez a homokóra hogy kerül ide?

Alkalmazási (***Application***)	Rengeteg alkalmazási rétegbeli protokoll: HTTP, RTP, RTCP stb., és itt van a **SIP** is
Szállítási v. transzport (***Host-to-host***)	TCP, UDP
Internet-réteg (***Internetworking***)	IP
Interfész réteg (***Interface v. link***)	Itt vannak a LAN-protokollok, a pont-pont-protokollok stb.

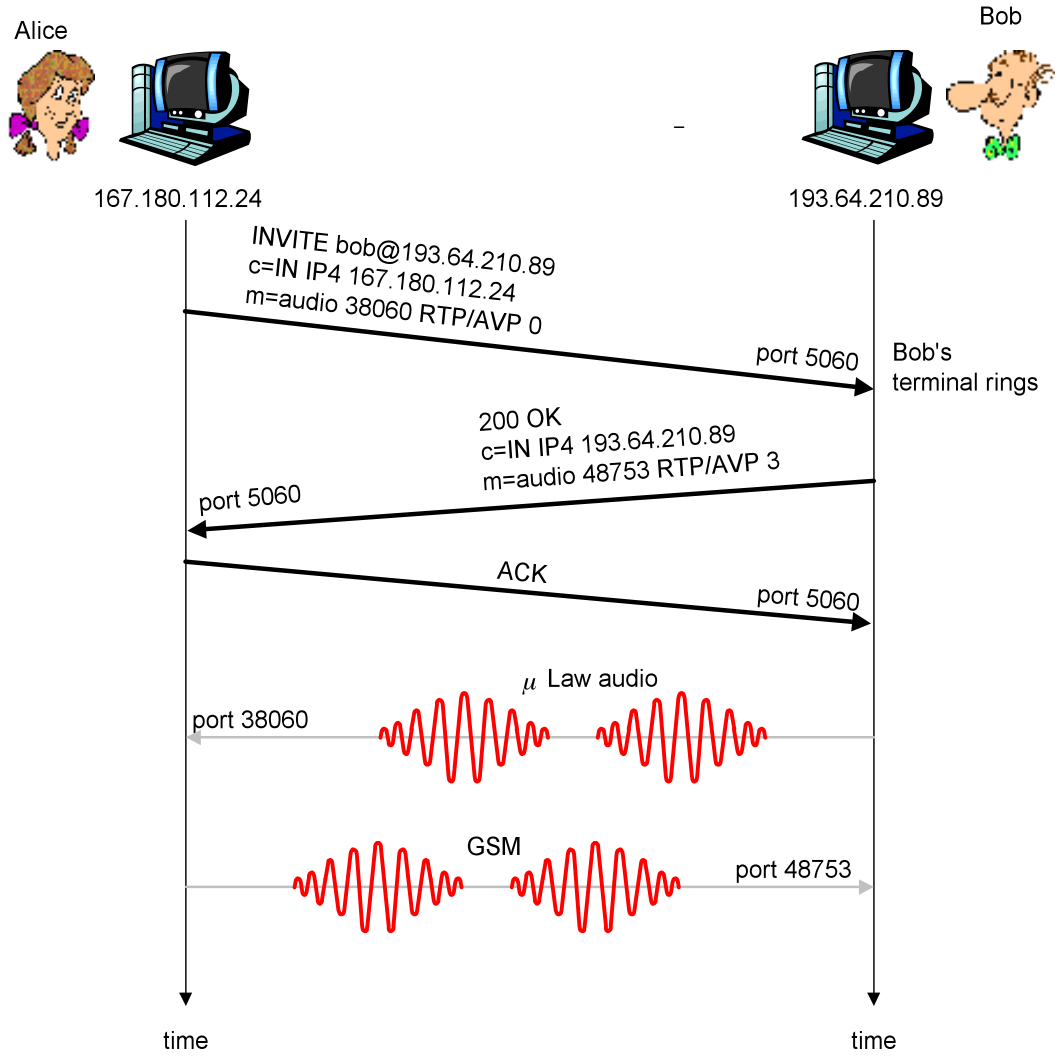
SIP bevezető áttekintés (2)

- A SIP a következő TCP-IP protokollcsaládbeli protokollokkal működik együtt ill. használja azokat:
  - RTP/RTCP/RTSP a médiatartalom továbbítására és támogató feladatokra (mint a H.323-ban) - *tárgyaltuk*
  - Session Announcement Protocol (SAP) - multimédia session-ök hirdetésére – *nem foglalkozunk vele*
  - Session Description Protocol (SDP) - multimédia session-ök leírására – *nem foglalkozunk vele*
  - RSVP - erőforrás-foglalásra – *lásd majd a következő részben*

SIP bevezető áttekintés (3)

- A SIP text-alapú protokoll (a HTTP-hez hasonló)
  ⇒ a SIP-üzeneteket können generálhatják emberek vagy programok
- SIP Uniform Resource Locators (URLs):
  Hasonlók az e-mail URL-ekhez
  sip: szabo@hit.bme.hu
  sip:+36 1 463 2049@hit.bme.hu
- A SIP *UDP* vagy *TCP* felett működhet, ma többnyire UDP felett

Példa hívásfelépítésre, legegyszerűbb eset: Alice ismeri Bob e-mail címét



Alice: **INVITE** (request)
IP-cím, portszáma, médiakódolás módja (AVP0), küldi az 5060-as well-known portra

Bob: **200 OK** (response)
IP-cím, portszám, médiakódolás módja (AVP3)

(mi van, ha Bob nem tudja az AVP0-ás kódolást...)
(mi van, ha Bob nem elérhető, vagy foglalt...)

Hívásfelépítés: mi van, ha Alice csak Bob nevét, vagy e-mail-címét ismeri?

- Meg kell tudnia a hívott aktuális IP-címét, ez miért kihívás?
  - A hívott mozog
  - Rendelkezhet különböző IP-eszközökkel
- A SIP szolgáltatásai ehhez:
  - Regisztráció
  - Proxy-zás, átirányítás

A SIP architektúrája: építőelemek

- *User agent - UA*
  - „Request”-eket kezdeményeznek és azok címzettjei
  - IP-telefon, PC, konferenciaszerver
- *Proxy server*
  - A kliensek (UA-k) megbízásából tevékenykednek
  - A SIP request-eket és response-okat route-olják
- *Registrars*
  - Nyilvántartják a felhasználókat egy domain-en belül
  - Név-cím-összerendeléseket kezelnek
- *Redirect servers*
  - Request-re megadják a felhasználó címét
  - De nem kezelnek hívásvezérlést és nem továbbítanak SIP request-eket

User Agents (UA)

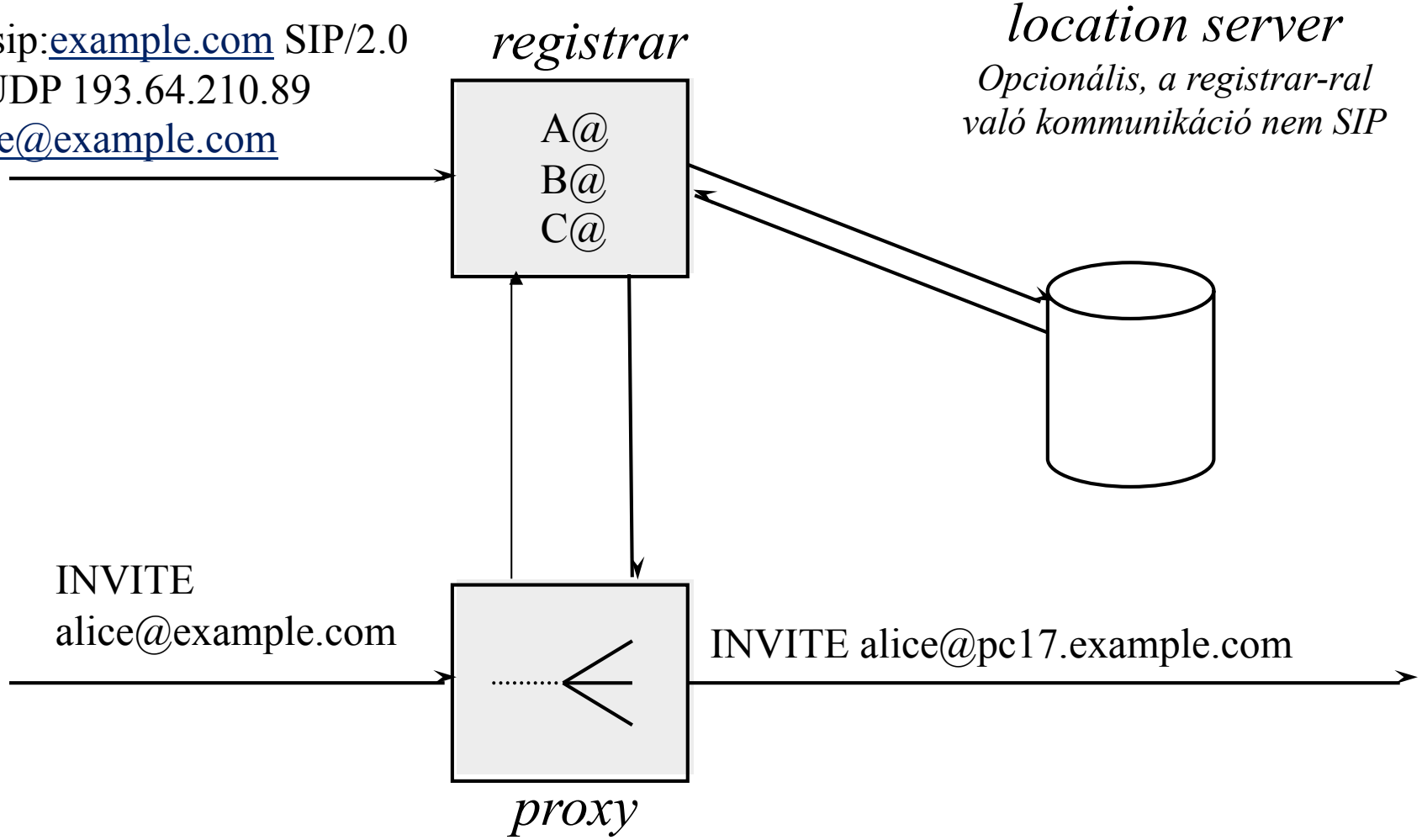
- Lehet hardware-alapú IP-telefon (pl. Cisco7960)
- vagy software-alapú – softphone (pl. Mirial, Windows Messenger)
- Softphone futhat PDA-n vagy mobiltelefonon is
- Két logikai részből állnak:
  - User Agent Client (UAC)
    - ***Request-eket küld és response-okat vesz***
  - User Agent Server (UAS)
    - ***Response-okat küld és request-eket fogad***

Proxy Server

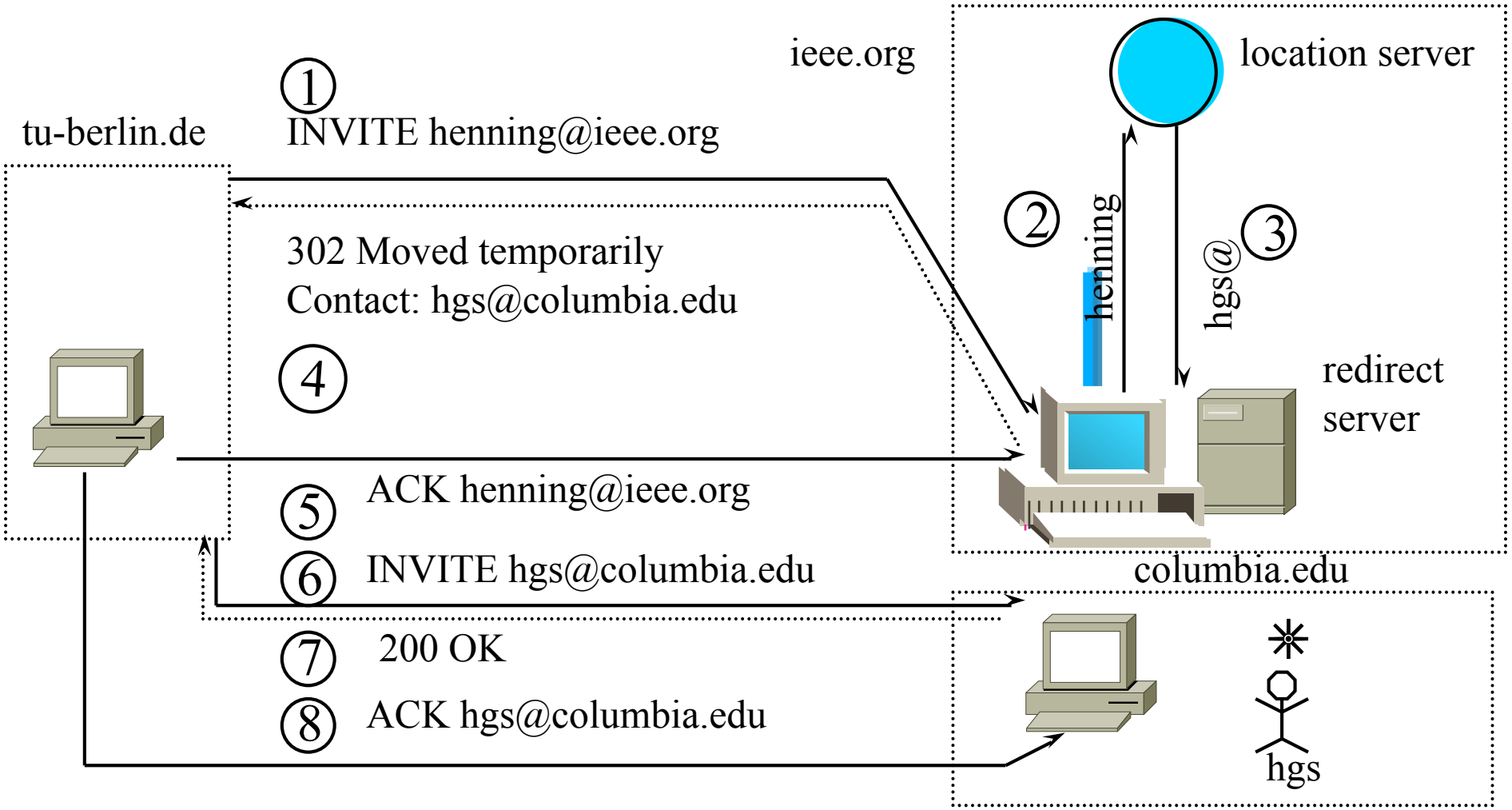
- A session invitation-okat továbbítja a hívott közelébe
- Két típusuk van:
  - Állapotmentes
    - **Egyszerű és gyors üzenettovábbítók**
  - Állapotalapú
    - **Forking-ra – egy üzenet vételekor 2 v. több üzenetet küld ki**

Registrar és Location Server

REGISTER sip:example.com SIP/2.0
Via: SIP/2.0/UDP 193.64.210.89
From: sip:alice@example.com
...
Expires: 3600



Redirect Server



A SIP működése Redirect-módban

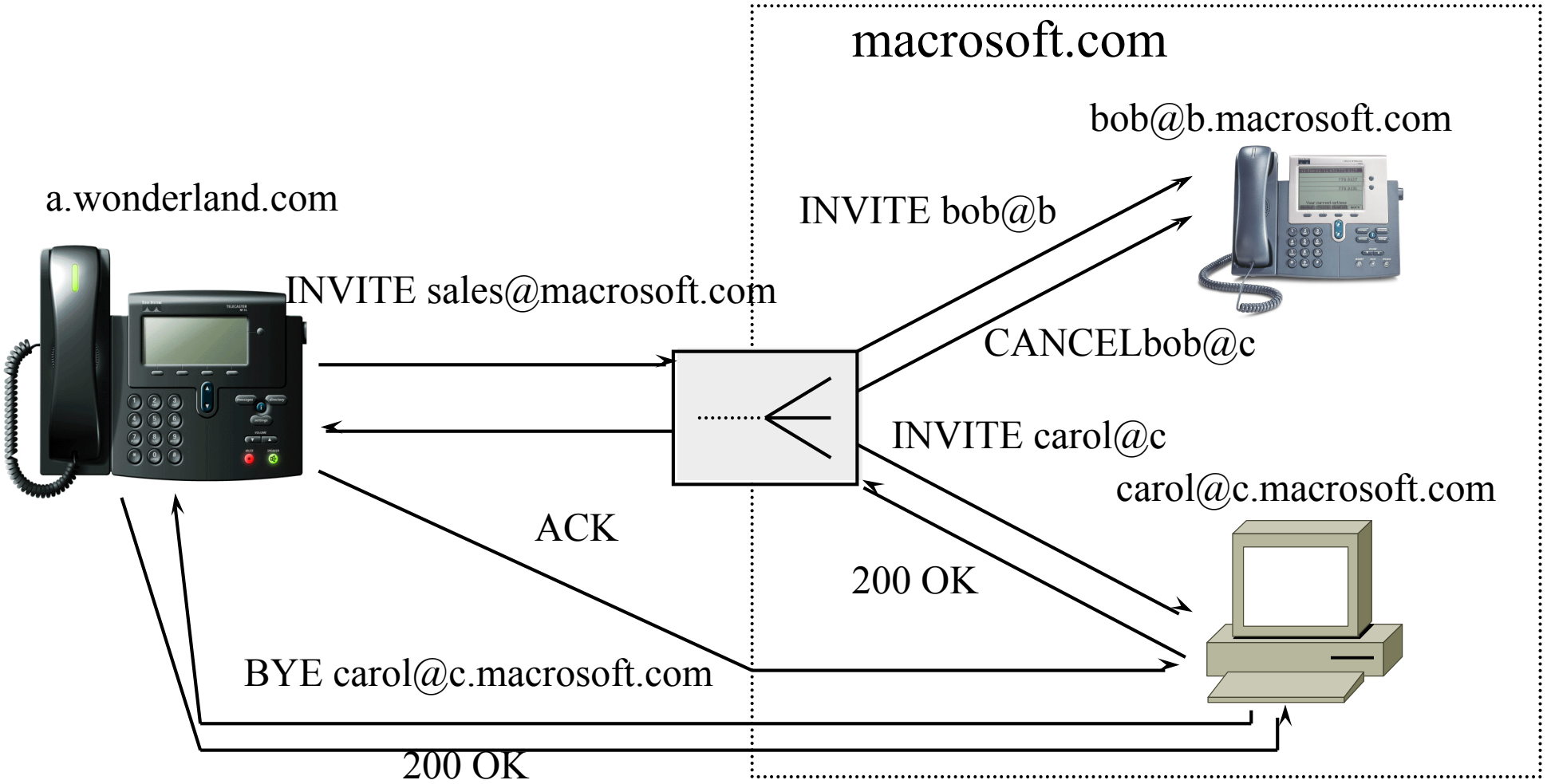
LÉPÉSEK:

- A Redirect server fogadja az INVITE-ot és kapcsolatba lép a location service-szel
- Ha megvan a felhasználó, a redirect server visszaküldi a címet a hívó félnek (nem ő generál új INVITE-ot!)
- A hívó UA ACK-t küld a redirect server-nek
- Az UA új INVITE-ot küld közvetlenül a kapott címre
- A hívott UA jelzi a sikert (200 OK) és a hívó UA ACK-t küld

Forking

- Más jelzésprotokolloknál ilyen nincs: a híváskérések elágaztatása
  - = a szerver két vagy több request-et küld különböző címzetteknek egy beérkező request-re
    - egyidejűleg
    - egymás után
- Ezzel valósít meg a SIP különböző „emeltszintű” szolgáltatásokat
  - hívástovábbítás hangpostára
  - automatikus hívásszétosztás

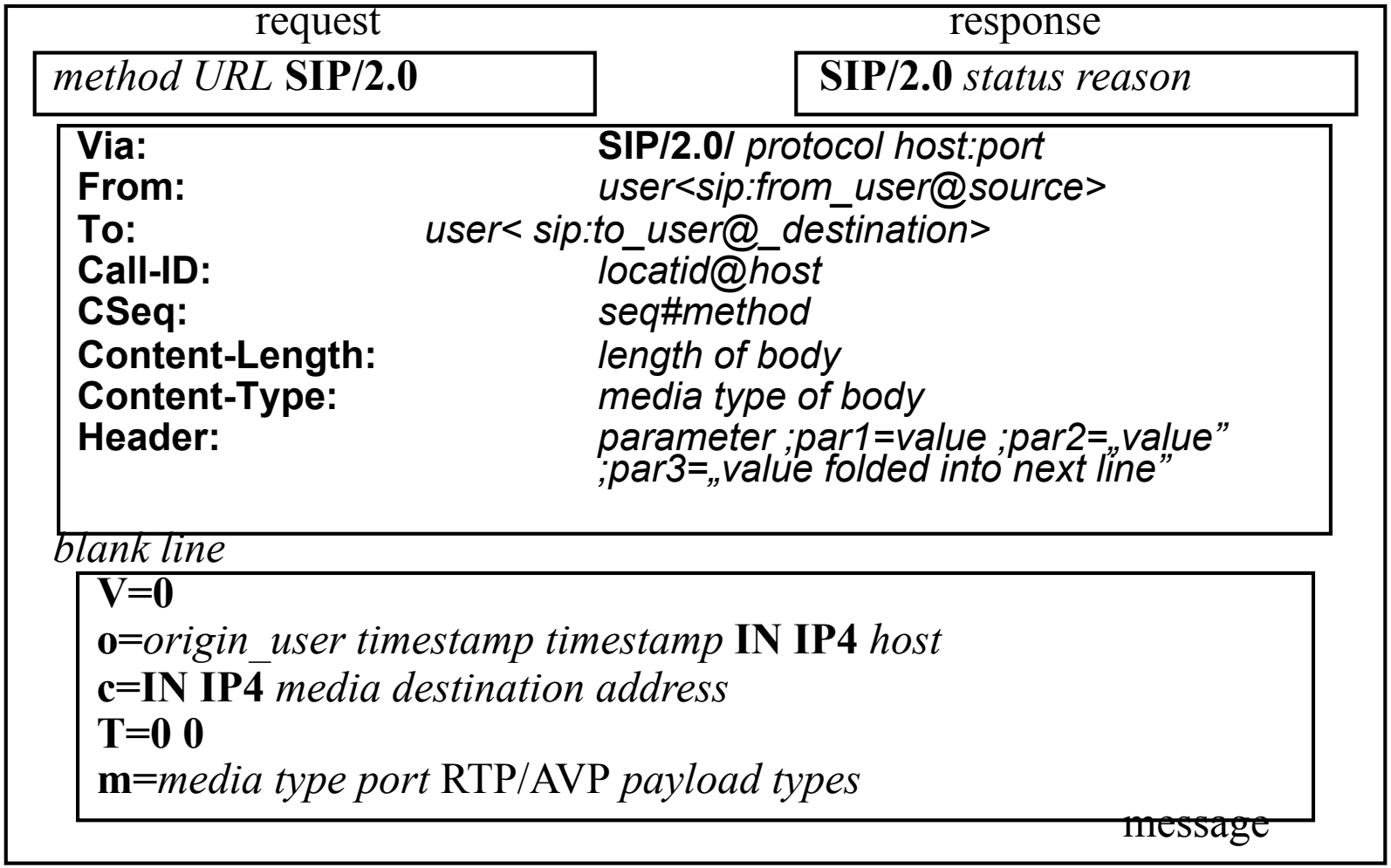
SIP request forking



SIP-üzenetek

- Két fő kategória: **Request**-ek és **Response**-ok
- Nagyon hasonlít a HTTP/1.1-hez
- Ugyanaz a request-ek és response-ok formátuma, az első sor kivételével
- Tartalmazhatnak üzenettörzset
  - Session description
  - ASCII vagy HTML

SIP-üzenetek



SIP Request-ek

- INVITE – hívás kezdeményezése
- ACK – válasz nyugtázása
- BYE – hívás befejezése (és továbbítása)
- CANCEL – keresés és „csengetés” törlése
- OPTIONS – a másik fél által támogatott tulajdonságok
- REGISTER - regisztráció a location service-szel

Request-példa: INVITE *)

INVITE

INVITE sip:godor@10.3.113.75 SIP/2.0
Via: SIP/2.0/UDP 10.3.119.239:8990
From: "392" <sip:392@10.3.113.75>;
tag=99982b0d-24c7-422d-971c-1c55
a00073d2

To: <sip:godor@10.3.113.75>
Call-ID:
95d2c362-4594-40ff-9d4f-92ace3aaf
81a@10.3.119.239
CSeq: 1 INVITE
Contact: <sip:10.3.119.239:8990>
User-Agent: Windows RTC/1.0
Content-Type: application/sdp
Content-Length: 533

v=0
o=matav-endre 0 0 IN IP4 10.3.119.239
s=session
c=IN IP4 10.3.119.239
b=CT:1000
t=0 0
m=audio 35528 RTP/AVP 97 111 112 6 0 8 4
5 3 101
a=rtpmap:97 red/8000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:6 DVI4/16000
a=rtpmap:3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
m=video 11518 RTP/AVP 34 31
a=rtpmap:34 H263/90000
a=rtpmap:31 H261/90000

SIP Response-ok *)

Informational	*Success*	*Redirection*	*Request Failure*
100 Trying **180 Ringing** **181 Call forwarded** **182 Queued** **183 Session Progress**	**200 OK** – *positive final response*	**300 Multiple Choices** **301 Moved Perm.** **302 Moved Temp.** **380 Alternative Serv.**	**400 Bad Request** **401 Unauthorized** **403 Forbidden** **404 Not Found** **405 Bad Method** **415 Unsupp. Content** **420 Bad Extensions** **486 Busy Here**

Server Failure	*Global Failure*
500 Server Error **501 Implemented** **503 Unavaiable** **504 Timeout**	**600 Busy Everwhere** **603 Decline** **604 Doesn't Exit** **606 Not**

A SIP összefoglalása

- IETF-szabványú (RFC...) multimédia hívásvezérlő protokoll
- IP-központú,
- állapotmentes protokoll,
- szöveges protokoll,
- jól kombinálható mindenféle web-alapú szolgáltatással.

A SIP és a H.323 összehasonlítása

- A H.323 komplett, vertikális protocollcsalád multimédia konferenciára. Jelzésfunkciók, regisztráció, beengedésszabályozás, átvitel, kodekek...
- A SIP egyetlen protokoll. Működik RTP-vel, de nem kötelezően. Más protokollokkal és szolgáltatásokkal kombinálható.
- A H.323 a távközlési világ terméke, ITU-szabvány. A digitális távközlésben használt jelzésprotokollokat integrálja magában.
- A SIP IETF-szabvány. Sok mindent vett kölcsön a HTTP-ből.

A H.323 – SIP összehasonlítása a képességek szempontjából

Összehasonlítási szempontok

- Hívásfelépítés
- Konferenciahívások
- Multimédia-kommunikáció
- Teljesítőképesség, skálázhatóság
- Integráció web-es alkalmazásokkal

SIP a jövő! Miért?

- A 3GPP által a 3. generációs mobil rendszerek számára bevezetett IMS (IP Multimedia Subsystem) alapja
  - IMS: szolgáltatások nyújtásának támogatása IP felett a mobil hálózatokban
  - Támogatás: olyan közös szolgáltatások az alkalmazások számára, mint a hívásvezérlés (ilyenek még az AAA, vagy a számlázás)
- A mobil szabványosítási világból az ITU is beemelte az IMS-t (és ezzel a SIP-et) az NGN szolgáltatásnyújtó platformjaként

NGN – next generation networks, újgenerációs hálózat

AAA – authentication, authorization, accounting

Az IP-hálózatokon történő multimédia-továbbítás eszközei

Az eddigiek összefoglalása:

- Médiakezelés (1. rész)
  - RTP, RTCP, RTSP
- Hívásvezérlés (2. rész)
  - (H.323), SIP

JÖN MÉG:

- Szolgáltatásminőség-biztosítás
  - IntServ*, DiffServ*, RSVP (3. rész)

**) nem protokoll, hanem módszer*

QoS IP-hálózatokban: túl a Best Effort-on

IntServ, DiffServ

Dr. Szabó Csaba Attila
egy. tanár
BME Hálózati Rendszerek és Szolgáltatások Tanszék
szabo@hit.bme.hu

2013. április 30.
Budapest

Mi a QoS?

- QoS = végpontok közötti garanciák
  - adott időszakra és adott forgalom mellett
  - alábbi paraméterekre:
    - Rendelkezésreállás
    - Átviteli sebesség, „sávszélesség”
    - Késleltetés, késleltetésingadozás
    - Vesztés
- A QoS biztosításának eszközei:
  - Forgalmi méretezés
  - Protokollválasztás
  - Hálózati architektúra megválasztása, hálózati biztonság
  - Tárak menedzselése

A QoS biztosításának módszerei

- „Nyers erő” (over-provisioning)
- ATM
  - Összeköttetés-alapú kommunikáció
    - virtuális utak és áramkörök
    - plusz felhasználó-hálózat közötti szerződés
    - beengedésszabályozás
    - erőforrás-menedzselés
- Folyamonkénti (per-flow) QoS-biztosítás
  - IETF’s Integrated Services (IntServ) módszer
- Forgalomosztály-alapú (class-based) QoS-biztosítás
  - IETF’s Differentiated Services (DiffServ) módszer
- LAN-okban
  - WLAN: 802.11e „soft QoS”
- MAN-okban
  - 802.16 WiMAX: QoS osztályok, erőforrás-allokálás

QoS összeköttetés-alapú hálózatban: ATM

- Az elv:
  - **Minden ATM összeköttetéshez QoS-osztály** kapcsolódik
  - A hálózat garantálja a megállapodás szerinti QoS-t minden összeköttetés számára
- Megvalósítás:
  - A forgalom jellemzése, forgalomleírók
  - QoS-paraméterek készlete
  - ATM szolgáltatási osztályok
  - Torlódásvezérlés
    - Legfontosabb a preventív módszer – CAC (Call admission control) – beengedésszabályozás
    - Van reaktív mechanizmus is

Mi az ATM? (1)

- ATM – Asynchronous Transfer Mode
- Az ATM-et az ITU-T szabványosította 1988-ban, a B-ISDN átviteli módjaként
  - B-ISDN: a (keskenysávú) ISDN fejlettebb, „szélessávú” utódjának szánták
- Fő célkitűzések:
  - különböző típusú forgalmak átvitelére tervezték:
    - **beszéd**
    - **állókép, video**
    - **adat**
  - Tág átvitelisebesség-tartomány: néhányszor 64 kbit/s-tól egészen nagy sebességekig (2,4 Gbit/s-ig)
- *A B-ISDN nem valósult meg, az ATM-rendszertechnika azonban ma a távközlő hálózatokban több helyen használt, de a felhasználó általában nem „látja” (pl. 3G mobil rendszerek hozzáférési hálózatában, vagy ADSL-vezérlőegységben). Számunkra elsősorban egy nagyon hasznos példa a QoS-re.*

Mi az ATM? (2)

- *Az elnevezés magyarázata:*
  - *„Asynchronous”* a távközlésben addig egyeduralkodó, ún. *Synchronous* Transfer Mode (STM) ellentéte
  - *„Transfer Mode”* – átviteli mód, általános megjelölés
- Ami a mi számunkra most lényeges:
  - az ATM **„gyors csomagkapcsolási”** technika
    - gyors: **rövid csomagok („cellák”), nincs forgalomszabályozás, nincs linkenkénti hibajavítás**
    - ezek a rövid, fix hosszúságú adatcsomagok hordozzák az összes típusú adatot
  - **Összeköttetés-alapú** elven működik
  - **Minden összeköttetéshez specifikus szolgáltatásminőséget képes biztosítani**

ATM szolgáltatásminőségi (QoS) osztályok

- **CBR –continuous bit rate**
  - **Forgalomleírók**:
    - PCR *(peak cell rate)*
    - CDVT (*cell delay variation tolerance)*
  - **QoS jellemzők**:
    - maxCDV (*maximum cell delay variation)*
    - MaxCTD (*maximum cell transfer delay)*
    - *CLR (cell loss rate)*
- **rt-VBR – real-time variable bit rate**
  - **Forgalomleírók:**
    - PCR, CDVT
    - SCR (*sustained cell rate*)
    - MBS (*maximum burst size)*
  - **QoS jellemzők:**
    - maxCDV, MaxCTD, CLR

ATM szolgáltatás-minőségek (QoS)

- **nrt-VBR – non-real-time variable bit rate**
  - **Forgalomleírók:**
    - PCR, CDVT, SCR, MBS
  - **QoS jellemzők:**
    - CLR
- **UBR – unspecified bit rate**
  - PCR specifikálva van, de nem használja a CAC és a policing
  - Nincsenek QoS paraméterek jelezve

Módszerek QoS biztosítására összeköttetés-mentes hálózatokban

- IP-alapú megoldások:
  - Integrated Services (IntServ)
    - QoS az egyedi csomagfolyamokra: **„finom felbontású”** módszer
  - Differentiated Services (DiffServ)
    - QoS folyamosztályokra: **„durva felbontású”** módszer

- *Az ATM-ben kitalált forgalomosztályok, forgalomleírók, QoS-biztosítási módszerek itt visszaköszönnek*

Integrated Services (IntServ)

- Integrated Service Working Group
  - 1995-97 szolgáltatás-osztályok specifikálása
  - az RSVP (Resource reSerVation Protocol) használata
  - Nem protokoll, hanem módszer!
- Több RFC-ben specifikálták: 1633, 2211, 2212, 2215, 2216

- A szolgáltatásosztályok:
  - **Best Effort**
  - **Guaranteed Quality** (RFC 2212):
    - garantált korlátok bármely csomag **késleltetésére és a sávszélességre**
  - **Controlled-Load** (RFC 2211):
    - függetlenít a többi forgalomtól, terheléstől
    - törekszik **kb. ugyanolyan** szolgáltatást nyújtására, mint amilyet a folyam kapna, ha terheletlenek lennének a hálózati csomópontok
    - beengedés-szabályozást használ
  - Ütemezés!

Az alkalmazások igényei és az IntServ-szolgáltatások

1. „Elastic applications”
   - nincs késleltetési vagy bármilyen korlát
   - tipikus TCP/IP adat-alkalmazások

Best effort service

3 alosztály:

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

ATM-analógia: UBR – unspecified bit rate

Az alkalmazások igényei és az IntServ-szolgáltatások (folyt.)

2. „Real-time tolerant (RTT)” alkalmazások
   - gyenge késleltetéskorlátok, alkalmanként csomagvesztés megengedett
   - pl.: tárolásos videóalkalmazások

   Controlled load service
   - átlagos késleltetés garantált
   - mennyiségi biztosítékok nélkül

   ATM analógia: nrt-VBR – non-real time variable bit rate
3. „Real-time intolerant (RTI)” alkalmazások
   - min. késleltetés és késleltetés-ingadozás
   - Pl.: beszéd, élő videókonferencia

   Guaranteed service
   - Átvitelisebesség- és késleltetéskorlátok

   ATM analógia: rt-VBR, CBR (continuous bit rate)

Az IntServ-ben használt mechanizmusok

- A forgalom és a kért szolgáltatásminőség leírása
  - *a **Tspec és Rspec** paraméterekekkel*
- **Erőforrás-foglalás jelzésátvitellel**
- **Beengedés-szabályozás** - *admission control*
- A forrás forgalmának ellenőrzése és formálása - ***traffic policing***
- **Ütemezés** - *scheduling*

Az IntServ-ben használt mechanizmusok (1)

- A forgalom **leírása, kérése, engedélyezése**
  - a felhasználó (alkalmazás) specifikálja a forgalmát a hálózat számára
  - meghatározott **szolgáltatást kér** a hálózattól
  - ez alapján a **hálózat eldönti**, hogy tudja-e ezt vállalni
  - beengedi-e az új folyamot a hálózatba (beengedés-szabályozás)

Az IntServ-ben használt mechanizmusok (2)

- **Foglalás, forgalom-ellenőrzés, ütemezés**
  - információt cserélnek az erőforrásfoglalásról
    - jelzésátvitel
    - IntServ-ben az ***RSVP-protokoll*** segítségével
    - az összeköttetés-alapú hálózatokban ez a hívásvezérlő protokollok feladata
  - a hálózat gondoskodik arról, hogy a forrás forgalma ne térjen el a megadottól
    - **traffic policing**
  - a hálózat meghatározza a csomagok sorbaállítását és kiszolgálását a csomópontokon
    - **scheduling, ütemezés**

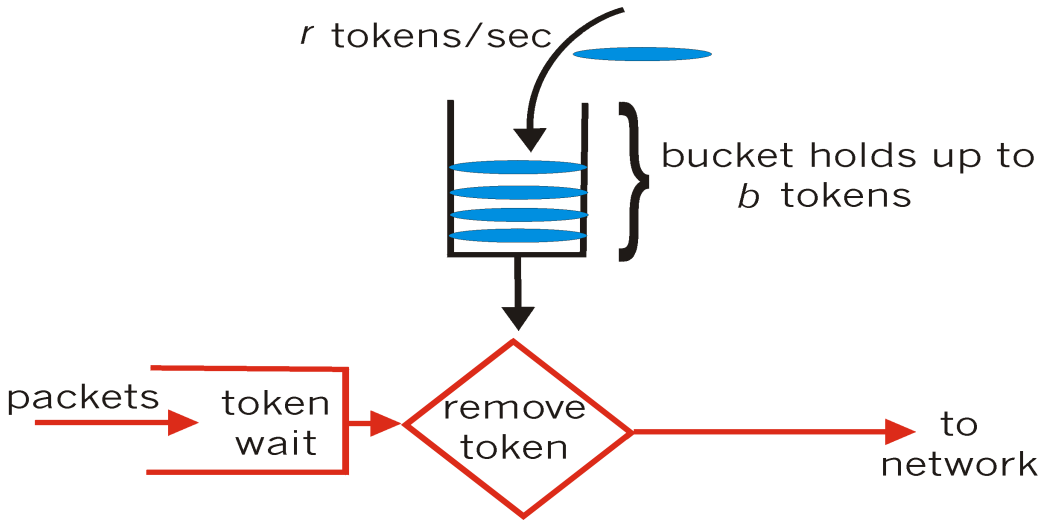
Flowspec: csomagfolyam specifikáció

- Két eleme van:
  - ***Tspec***:
    - leírja a folyam forgalmi jellemzőit, informálva ezzel a hálózatot a szükséges sávszélességről
    - lehetővé téve a döntést a beengedés-szabályozás részére
    - **token bucket** algoritmus
    - *TSpec: a Traffic Specification-ból jön*
  - ***Rspec***:
    - leírja az igényelt szolgáltatásminőséget
      - *Pl. controlled load (soft QoS)*, vagy *guaranted* (késleltetési korlát)
    - *RSpec: a Reservation vagy Request Specification-ból*

Forgalomleírás és policing

A policing és a forgalomleírás eszköze: a **token bucket** (tokenvödör)
A vödör formálja a forgalmat: küldhetünk *b* méretű börsztöt, de az átlagsebesség csak *r* lehet
Ezeket a paramétereket (is) használjuk a TSpec-ben

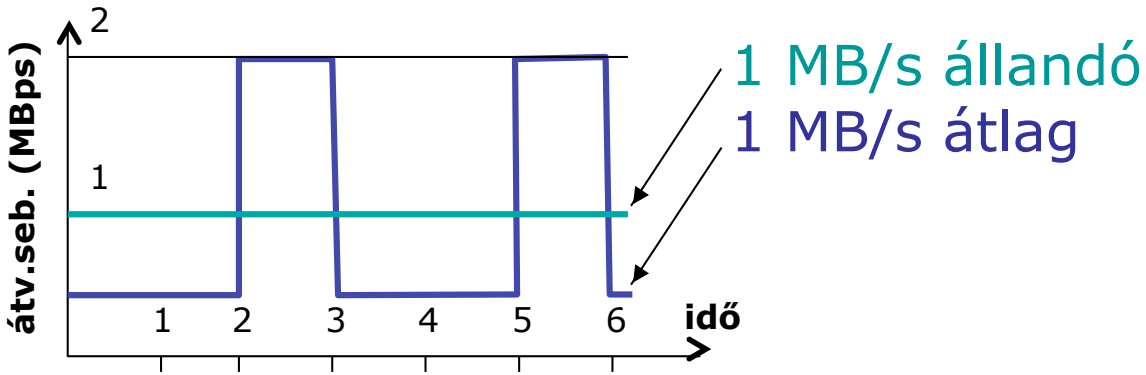
- A vödörbe ***r* sebességgel** töltődnek a tokenek
- Legfeljebb ***b* token** lehet benne, ha már tele van, a beérkező tokenek elvesznek, túlcsordulnak
- Ha egy *n* hosszú csg érkezik, kivesz *n* tokent a vödörből (ha van annyi) és továbbításra kerül
- Ha kevesebb mint *n* token van: nem kerül kiszolgálásra



Token Bucket (TB) az IntServ-ben

- Az IntServ *b*-t byte-ban, *r*-et pedig byte/sec-ban méri
  - Igen tág határok a *b*-re és az *r*-re
    - 1 byte...250 Gbyte és 1 byte/s...40 Tbyte/s

- A TB hatása:



Példa tokenvödörre

- Két különböző forgalomtípus: CBR videó és beszédátvitel
- CBR videó: 75 keret/s, 10 csomag/keret
  - TSpec: token ráta 750 Hz, a vödör mélysége 10
- Beszéd TSpec:
  - Kisebb tokenráta
    - mivel a beszéd közötti szüneteket nem viszik át
  - De nagyobb vödörmélység: börsztösebb átvitel

Börsztös átvitel: könnyebben okoz torlódást!

Beengedés-szabályozás (admission control)

- Minden csomópont megvizsgálja
  - **forgalomleírást (*Tspec*)** és a
  - **QoS-igényt (*Rspec*)**

  ezután dönt az igényelt szolgáltatás teljesíthetőségéről

- Eltérő a *Controlled Load* és a *Guaranteed*:
  - *Controlled Load*: heurisztikus is jó lehet
    - Pl. eddig a hasonló esetek jók voltak, engedjük meg most is
    - vagy korábban hasonló esetben már nem felelt meg a kiszolgálás, ezért tagadjuk meg
  - *Guaranteed* esetben ennél sokkal szigorúbb vizsgálat szükséges

- **Az admission control konkrét módszerei nem képezik az IntServ specifikáció részét**

Jelzésátvitel – az RSVP

- **R**esource Re**S**er**V**ation **P**rotocol
  - *R.S.V.P.: "Répondez/Réservez s'il-vous-plaît"*

- Lényeges jellemzői :
  - **Vevőoldali erőforrás-foglalás**:
    - Nem az adó „erőlteti" a képességeit, hanem a vevő foglalja le azt az igényei szerint *
  - **„Soft state":** igények „elhalnak", ha nem …
    - nem igényli a session explicit lezárását **
    - viszont időnként „frissíteni" kell a foglalást

- Eredmény: robusztusság
  - * kedvező a multicast-címzés esetén
  - ** megkíméli a hálózatot a végkészülék esetleges hibáitól

- Specifikáció: az RFC 2210-ben

- Az RSVP-t nemcsak az IntServ használja (említettük a H.323-nál is)

RSVP – alapvető jellemzők, lépések

- Alapötlet:
  - a vevőnek ismernie kell, hogy az adó milyen forgalom generálására képes → tudnia kell az adó ***Tspec*** jellemzőjét, valamint
  - tudnia kell a **forgalom (csomagok) útját**, és
  - így **erőforrást foglalhat az út mindegyik csomópontjánál**

1. Az adó *PATH* üzenetet küld, benne a *Tspec*
   - az úton lévő valamennyi csomópont feljegyzi

2. A vevő *RESV* üzenettel foglal, benne *Rspec*

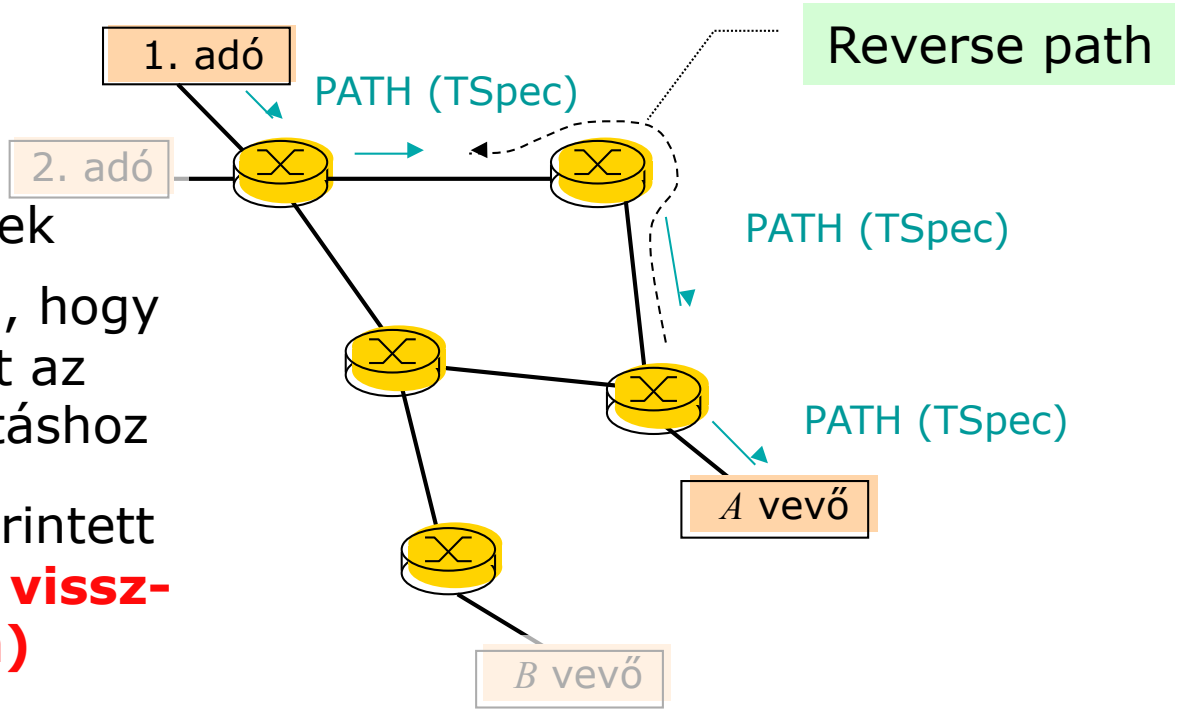
RSVP – „út”: egy adó <-> egy vevő

- Első fázis:

•a vevőnek ismerni kell az adó jellemzőit (**TSpec)**
•PATH üzenet a vevőnek

•a vevőnek tudnia kell, hogy hol foglaljon erőforrást az általa kívánt szolgáltatáshoz

•a PATH üzenet által érintett routerek **feljegyzik a vissz-irányt (reverse path)**

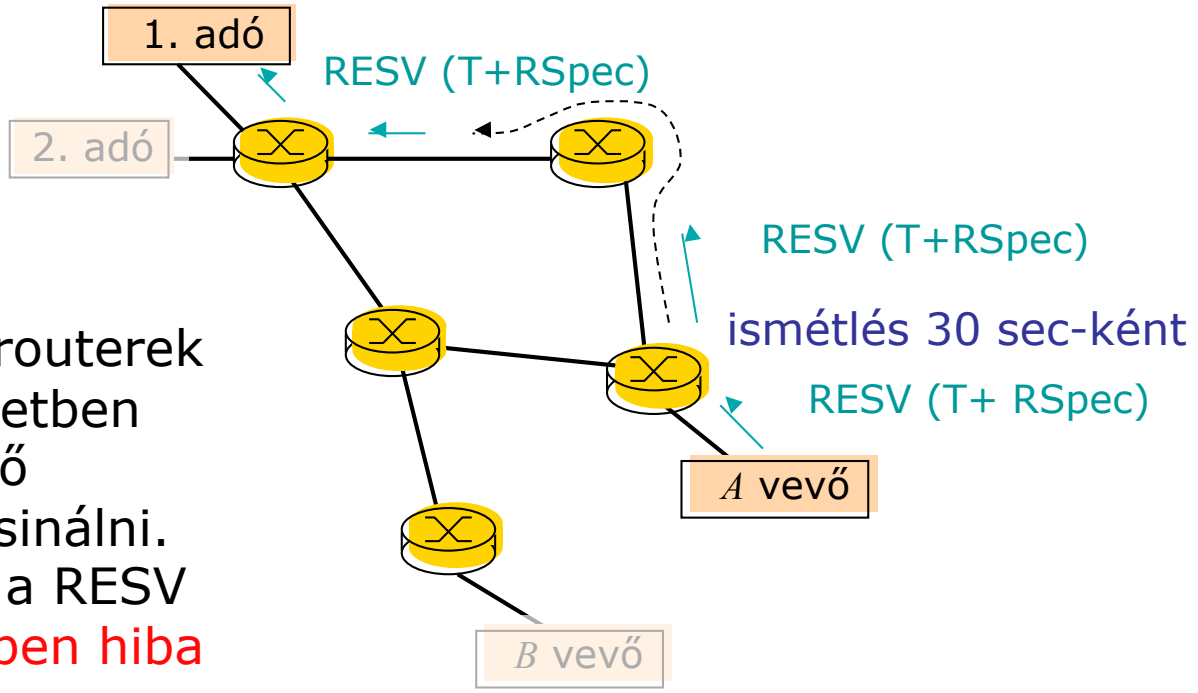


RSVP –”foglalás”: egy adó <-> egy vevő

- 2. fázis:

•amikor a vevő kap egy PATH üzenetet, visszaküld egy RESV választ, benne **TSpec és RSpec**

•a reverse path-on lévő routerek megkísérlik a RESV üzenetben lévő RSpec-nek megfelelő erőforrás-foglalást megcsinálni. Siker esetén továbbítják a RESV üzenetet. Ellenkező esetben hiba a vevőnek.



•ameddig a vevő fenn kívánja tartani a foglalást, 30 sec-ként meg kell ismételje a RESV üzenetet („soft-state”)

RSVP – „hiba”: egy adó <-> egy vevő

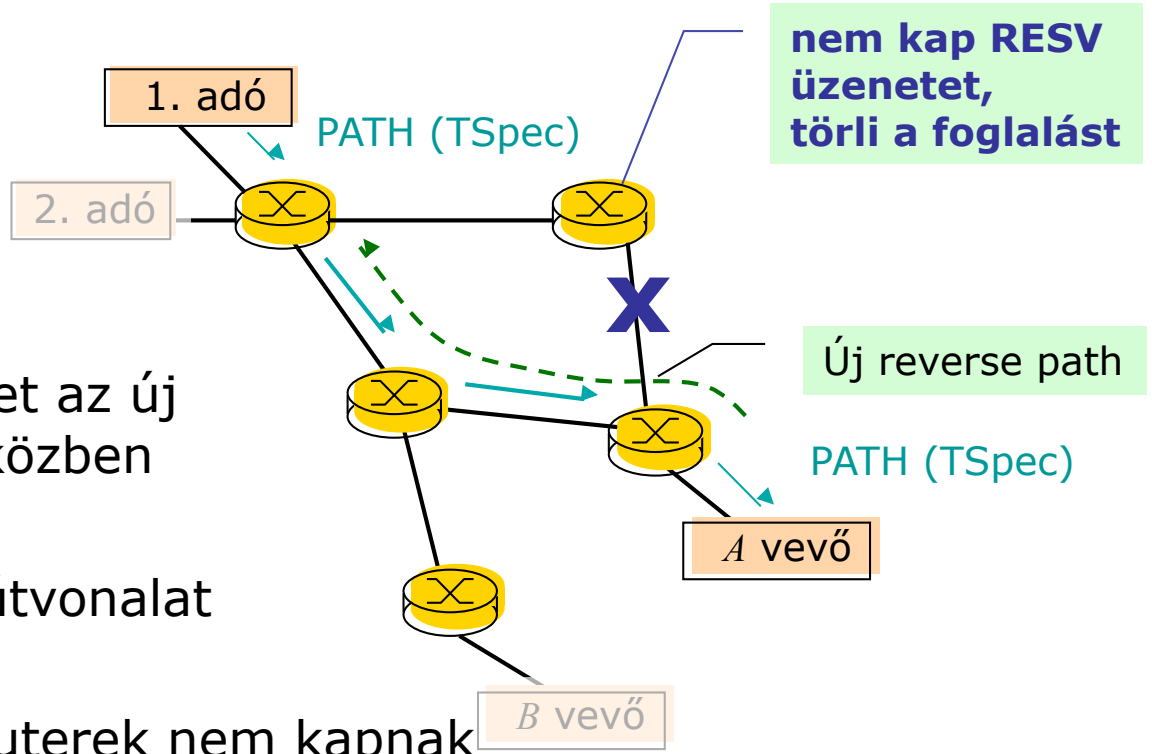
- Hálózati hiba esetén:

•élő útvonalon történő kommunikáció közben kieső link vagy router esetén a routing új útvonalat keres

•az ismétlődő PATH üzenet az új útvonalon eléri a vevőt, közben új reverse path képződik

•a vevőtől a RESV az új útvonalat követve végzi a foglalást

•a régi útvonalon lévő routerek nem kapnak tovább RESV üzenetet, lejár az időzítés, és törlik a foglalást (soft state)



RSVP: egy adó <-> több vevő

- Új vevő csatlakozása:

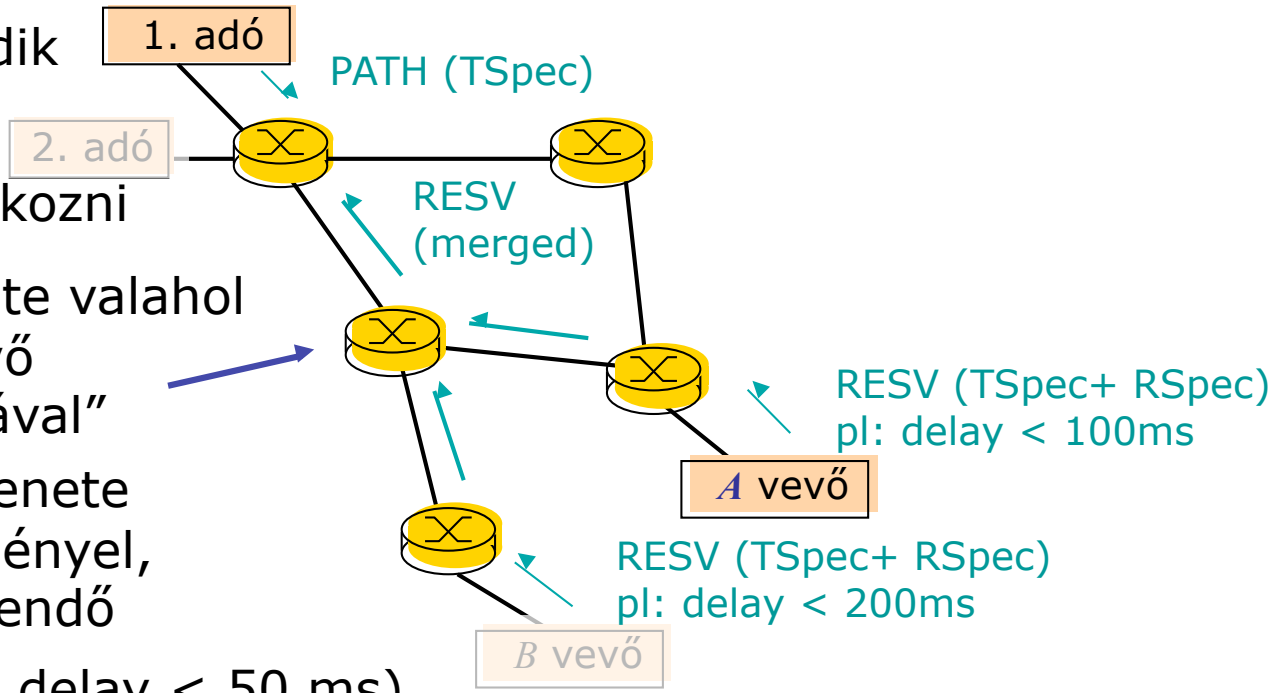
•az *A* vevő már működik egy ideje

•a *B* vevő kíván csatlakozni

•a *B* vevő RESV üzenete valahol találkozni fog az *A* vevő kiszolgálását végző „fával”

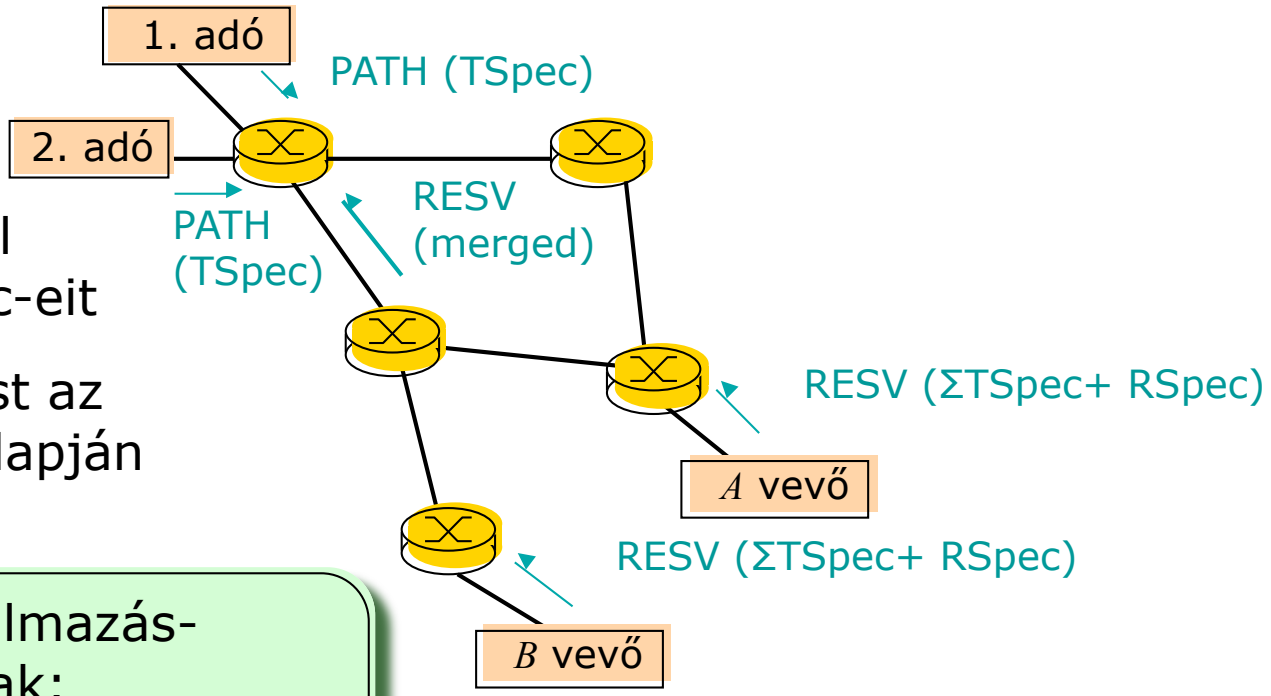
•ha a *B* vevő RESV üzenete kevesebb erőforrást igényel, mint *A*, akkor nincs teendő

•ellenkező esetben (pl delay < 50 ms) az új foglalást tovább kell küldeni, amely azonban mindenképpen összevont (merged) lesz



RSVP: több adó <-> több vevő

- Konferencia:



•a vevőknek össze kell gyűjteni az adók Tspec-eit

•a vevőknek a foglalást az összesített Tspec-ek alapján kell kialakítani

A Tspec-ek alkalmazás-specifikusak:
Az **RSVP különböző foglalási "stílusokkal" működik**

Visszatekintés: az IntServ-ben használt mechanizmusok

- a felhasználó (alkalmazás) specifikálja a forgalmát a hálózat számára (**TSpec**)
- meghatározott szolgáltatást kér a hálózattól (**RSpec**)
  - melynek alapján a hálózat (csomópontonként!) eldönti, hogy beengedi-e az új folyamot a hálózatba (*admission control*, **beengedés-szabályozás**)
- információt cserélnek az erőforrásfoglalásról
  - IntServ-ben az ***RSVP-protokoll*** segítségével
- a hálózat gondoskodik arról, hogy a forrás forgalma ne térjen el a megadottól (***traffic policing***)
- a hálózat meghatározza a csomagok sorbaállítását és kiszolgálását a csomópontokon (***scheduling,* ütemezés**)
  - *megnéztük az általános módszereknél*

Az IntServ csomagkezelése

1. **Csomagminősítés (*packet classification*):**
   - mindegyik csomagot hozzá kell rendelni az arra vonatkozó foglaláshoz
     - vizsgálva a source address, destination address, protocol number, source port, destination port értékeket
   - ezzel meghatározzuk a csomag kezelését a csomópontokon

2. **Csomagkezelés (*packet scheduling*) a sorokban:**
   - Guaranteed service esetén:
     - Weighted Fair Queue biztosítani fogja a végpontok közötti késleltetést
   - Controlled-load kiszolgálásnál egyszerűbb módszerek is megfelelnek

Filterspec: csomagminősítés*

- ***Filterspec:*** definiálja a csomagok mely halmazára vonatkozik az adott ***flowspec (TSpec, RSpec)***
- E szelekció a csomag attribútumaitól függ, pl. IP cím, portszám

- RSVP foglalási stílusok:

  - **Fix filter** – adott folyamhoz foglal erőforrásokat
  - **Explicit osztás** – több folyamhoz foglal erőforrásokat, ezen osztoznak
  - **Wildcard filter** – egy általános folyamtípusnak foglal erőforrásokat, mindannyian ezen osztoznak a típuson belül

  - RSVP RESV kérés: ***flowspec + filterspec = flowdescriptor*.**

IntServ skálázhatóság, bővíthetőség, „növekedési” képesség

- Bár az IntServ nagyon jelentős előrelépés a *best effort* kiszolgáláshoz képest,
- **nem teljesíti** az Internet egyik alapvető célkitűzését: a **növekedési képességet**
  - *best effort* kiszolgálásnál nincs folyamhoz kötött állapot-nyilvántartás a routereknél
  - így a hálózat növekedésével elég, ha a routerek a linkek sebességének növekedésével lépést tudnak tartani
- Az IntServ-nél: lényegében összeköttetés-alapú szolgáltatást csináltunk
  - annak minden nehézségével együtt,
  - de anélkül, hogy annak előnyét, a lokális címzést kihasználtuk volna

Az IntServ bővíthetősége, kiterjeszthetősége

- Pl. 64 kbit/s beszédcsatornák egy „STM-16” (2,5 Gbit/s) összekötésen:

  $2.5 \times 10^9 / 64 \times 10^3 = 39000$

  - mindegyik foglalás igényel valamennyi memóriát,
  - valamint periodikus frissítést.

- Mindegyik folyamot osztályozni, ellenőrizni kell és sorbaállítani (*classification, policing, scheduling*)
- *Admission control* döntést kell végezni mindegyik igényre
- Meg kell akadályozni indokolatlanul hosszú foglalást

- Mindezek a feladatok együtt akadályát jelentik az “Integrated Service” növekedési képességének
- **Olyan módszer kell, amely nem egyedi folyamokat kezel!**

Differentiated Services (DiffServ)

2013. április 30.
Budapest

A DiffServ alapötlete (1)

- A gerinchálózatra kell megoldást találni, ahol nagy volumenű, aggregált forgalmat viszünk át

- A DiffServ módszer kisszámú **forgalomosztály**-hoz rendel erőforrásokat:
  - osztály, pl.:
    - *Premium*
    - *Regular*

- Ahelyett, hogy külön jelzésekkel (pl. RSVP-vel) értesítenénk a routereket egy folyam pl. *Premium* igényéről,

  egyetlen bit a csomagfejben megteheti ezt!

DiffServ alapötlete (2)

- Két kérdés az előző ötlethez:
  - Ki állítsa be a „premium” bitet, és mikor?
    - történjék a beállítás az ***„adminisztratív” határon***
  - Mit csinál a router másképpen, ha egy olyan csomagot kap, ahol ez a bit be van állítva?
    - különféle router-viselkedéseket ***követ***, meghatározta az *IETF DiffServ WG*
- Előbb nézzük meg, hogyan működik a DiffServ!

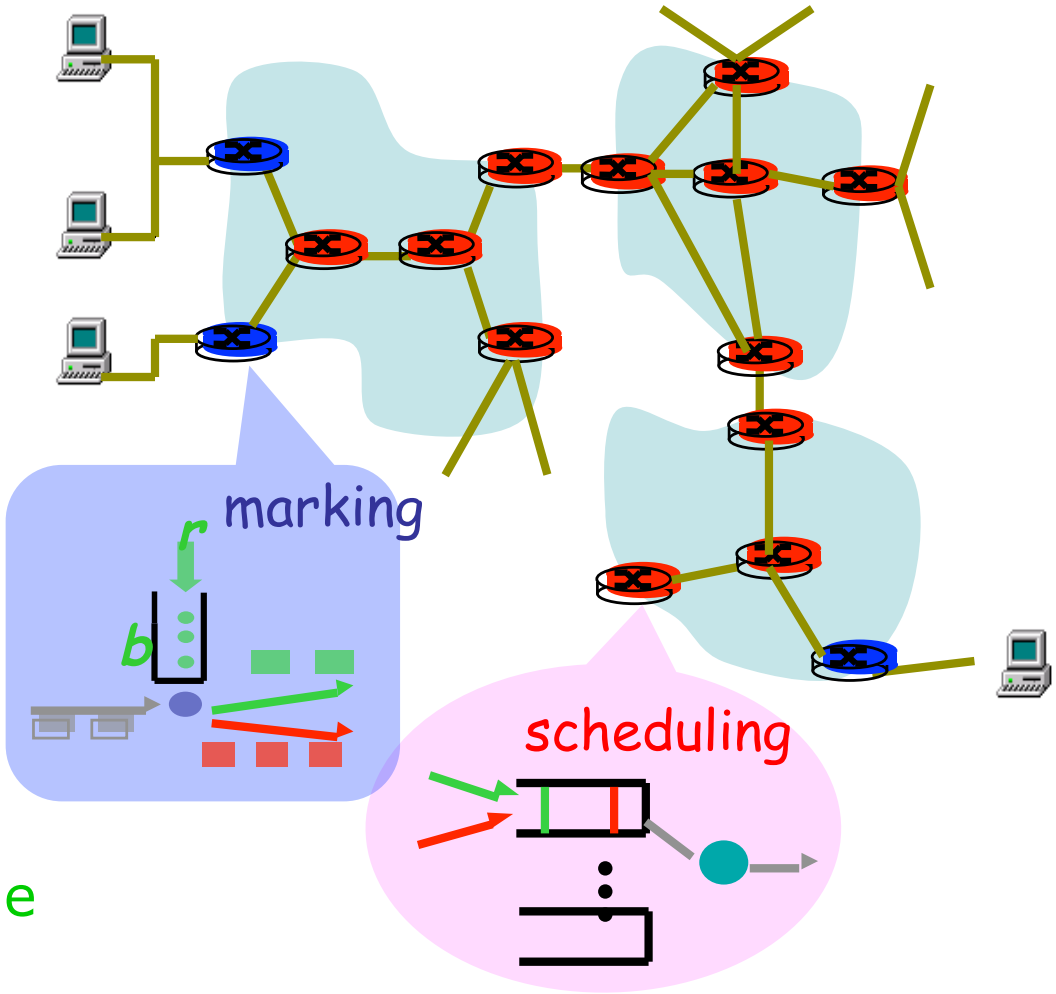
A DiffServ működése

Edge router:

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

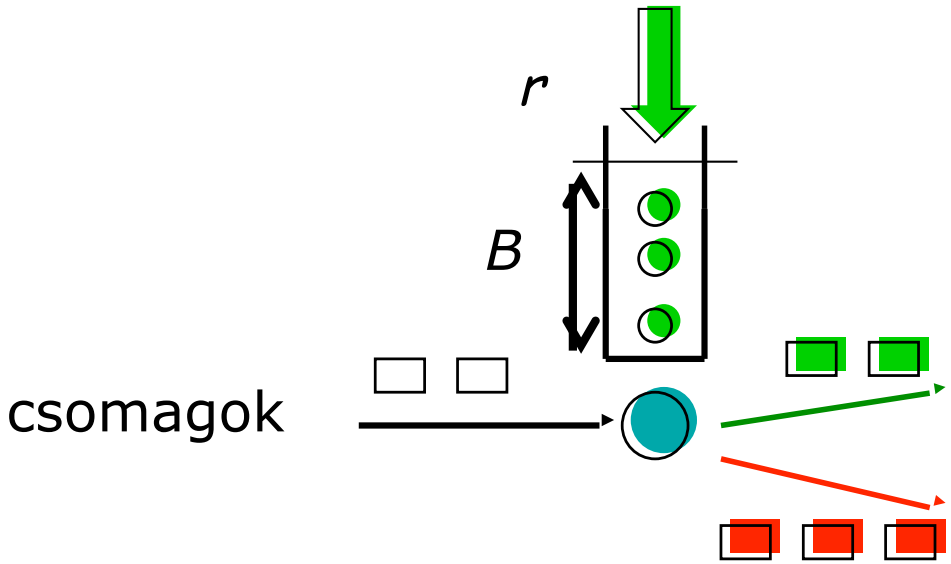
Core router:

- osztályonkénti forgalom-menedzselést végez
- pufferelés és ütemezés a széleken történt megjelölésnek megfelelően
- elsőbbség adása az in-profile csomagoknak



A csomagok megjelölése az edge-routerben

- profil: egyeztetett *r* sebesség és *B* vödörméret
- a csomagok megjelölése a széleken a folyamonkénti profil szerint

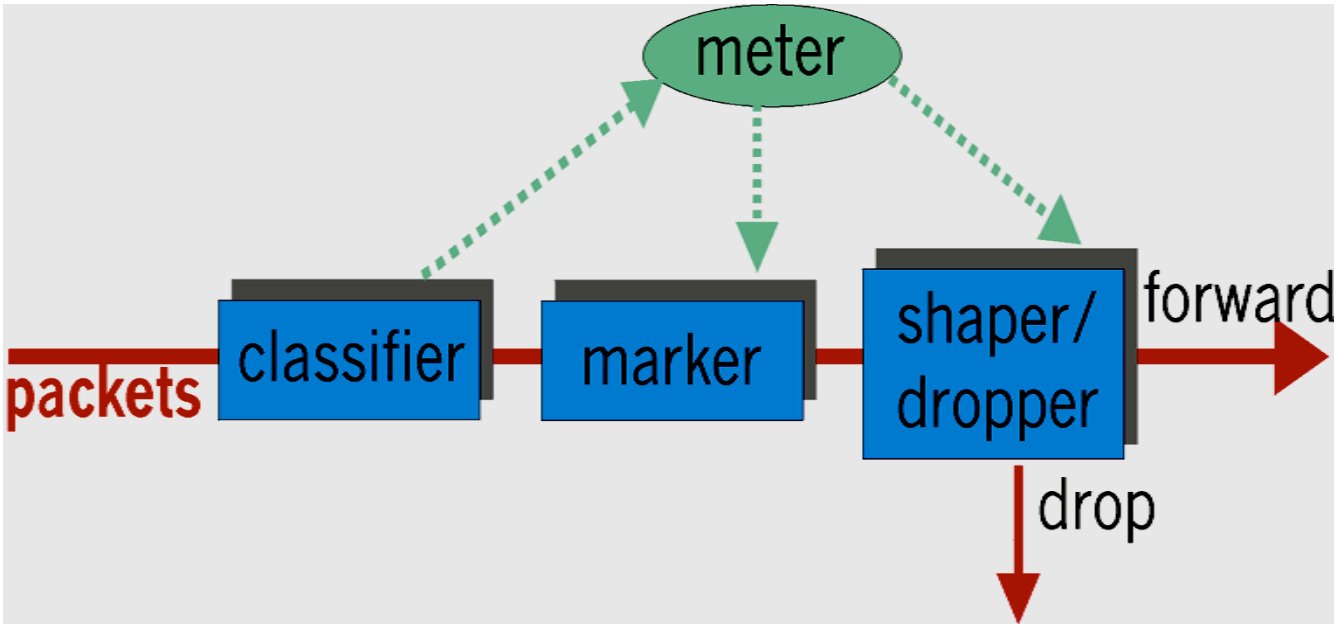


Megjelölés:

- osztály szerinti: a különböző osztályokhoz tartozó csomagokat eltérően jelöljük
- osztályon belüli: a folyam konform (a profilnak megfelelő) és nem konform részei eltérő jelölést kapnak

Mérés, osztályozás, megjelölés, és „kondícionálás”

- megfigyeljük a forgalmat (meter) és a nem konform csomagokat
  - formáljuk (shaping)
  - eldobjuk (dropping)

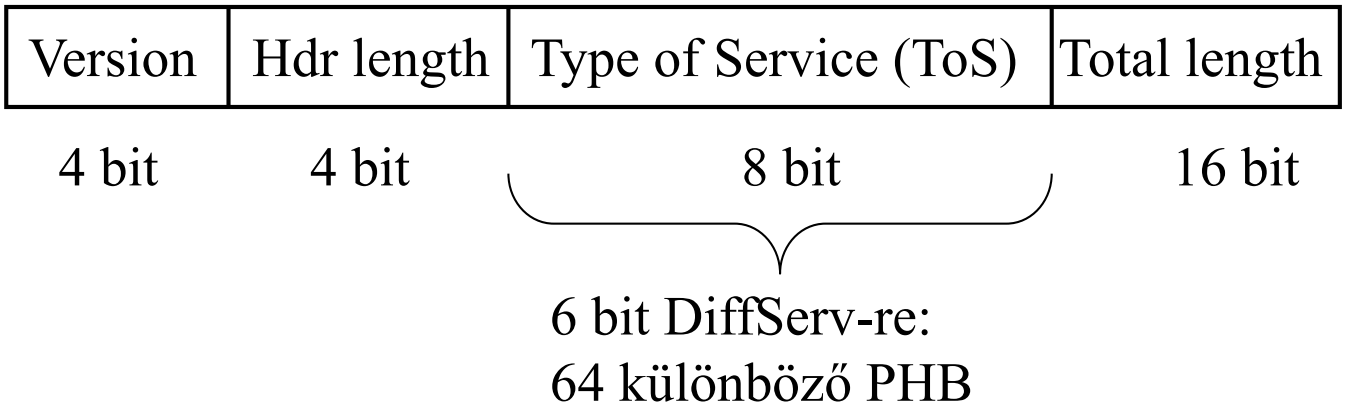


DiffServ – a csomópontok viselkedése

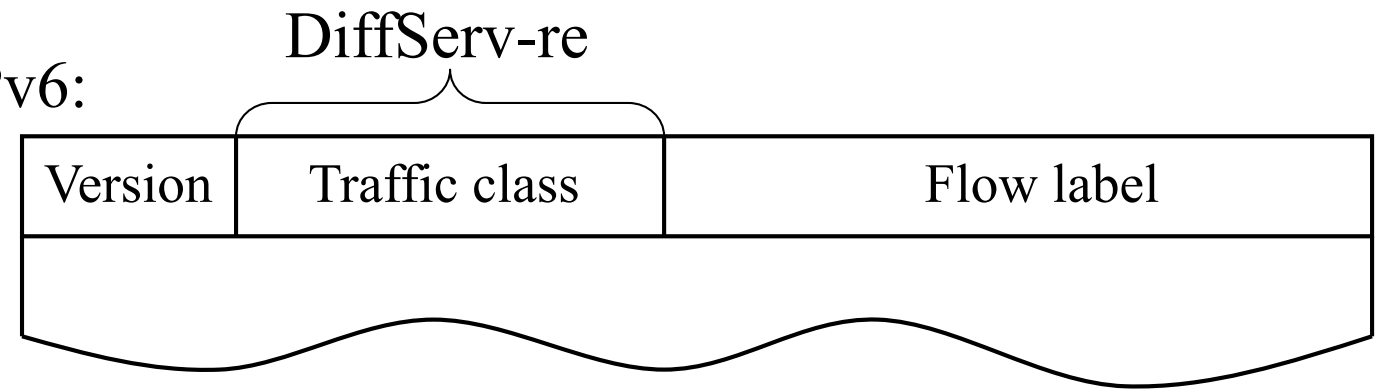
- *Természetesen nem csak 2 osztály van*
- ***Per-Hop-Behavior (PHB):*** *a forgalomosztályhoz tartozó csomagtovábbítási elveket definálja*
- Nincs együttműködés a végpontok között, mint az IntServ-nél
- A különböző PHB-k megadására:
  - IPv4-nél: IP fejrész ToS mezőjében 6 bit
  - IPv6-nál: ugyanaz Traffic Class néven
- Ez a 6 bit: “DiffServ Code Points” (DSCP)
  - A mező további 2 bitje: Explicit Congestion Notification (torlódásjelzés)
- Két alapvető PHB-típus:
  - **“*expedited forwarding*” (EF)**
  - **“*assured forwarding*” (AF)**
- Plusz default PHB: **best effort**
  - minden idekerül ami nem felel meg a fenti kettőnek

A “DiffServ Code Points”-ok (DSCP-k) elhelyezése

IPv4:



IPv6:



DiffServ – *expedited forwarding* (EF)

- Ez a legegyszerűbb PHB:
  - a csomagok továbbítása
    - minimális késleltetéssel
    - kis csomagvesztéssel történik
- Célszerű ha az EF-forgalom érkezési ütemét csak a csomópontok link-sebessége korlátozza
  - Ütemezőben: olyan sorhoz rendeljük hozzá, amelynek a kiszolgálási üteme legalább a csomagok beérkezési ütemével egyezik meg
    - Ezért elhanyagolható lesz a késleltetés és csomagvesztés
- Az EF („expressz” továbbítás) más típusú forgalommal szembeni szigorú prioritással garantálható
- Alkalmazások: beszéd, videó

DiffServ – *expedited forwarding* (EF)

- Gond az EF-fel: túl nagy EF forgalom **sorbanállási késleltetést okoz**
- Osztályon belül: késleltetés és jitter leromlása
- Szigorú beengedés-szabályozás kell erre az osztályra!
- A szolgáltató korlátozza, pl. max. 30%-a lehet a link kapacitásának

DiffServ – *assured forwarding* (AF)

- A legnépesebb osztály: 12 elemmel (**AF$_{xy}$**)
  - 4 csoport, az *x* (1 ÷ 4) sort választ
    - ezekben 3 – 3 elem, *y* (1 ÷ 3) „eldobási stílust” határoz meg

- Így az összesen 14 kiszolgálás közül a DSCP mező 6 bitje választja a megfelelőt:
  - - A*ssured Forwarding* DSCP: a köv. tábl. szerint
  - - *Expedited Forwarding* DSCP: 101 110
  - - *Best Effort (Default PHB):* 000000

- **Prioritásos sorok és eldobási jellemzők** valósítják meg a megfelelő kiszolgálást

Assured forwarding (AF) alosztályok

Drop Precedence	Class 1	Class 2	Class 3	Class 4
Low *Medium* *High*	010 000 … …	… … …	… … …	… … …

Osztályok közötti torlódás: az osztály prioritása dönti el

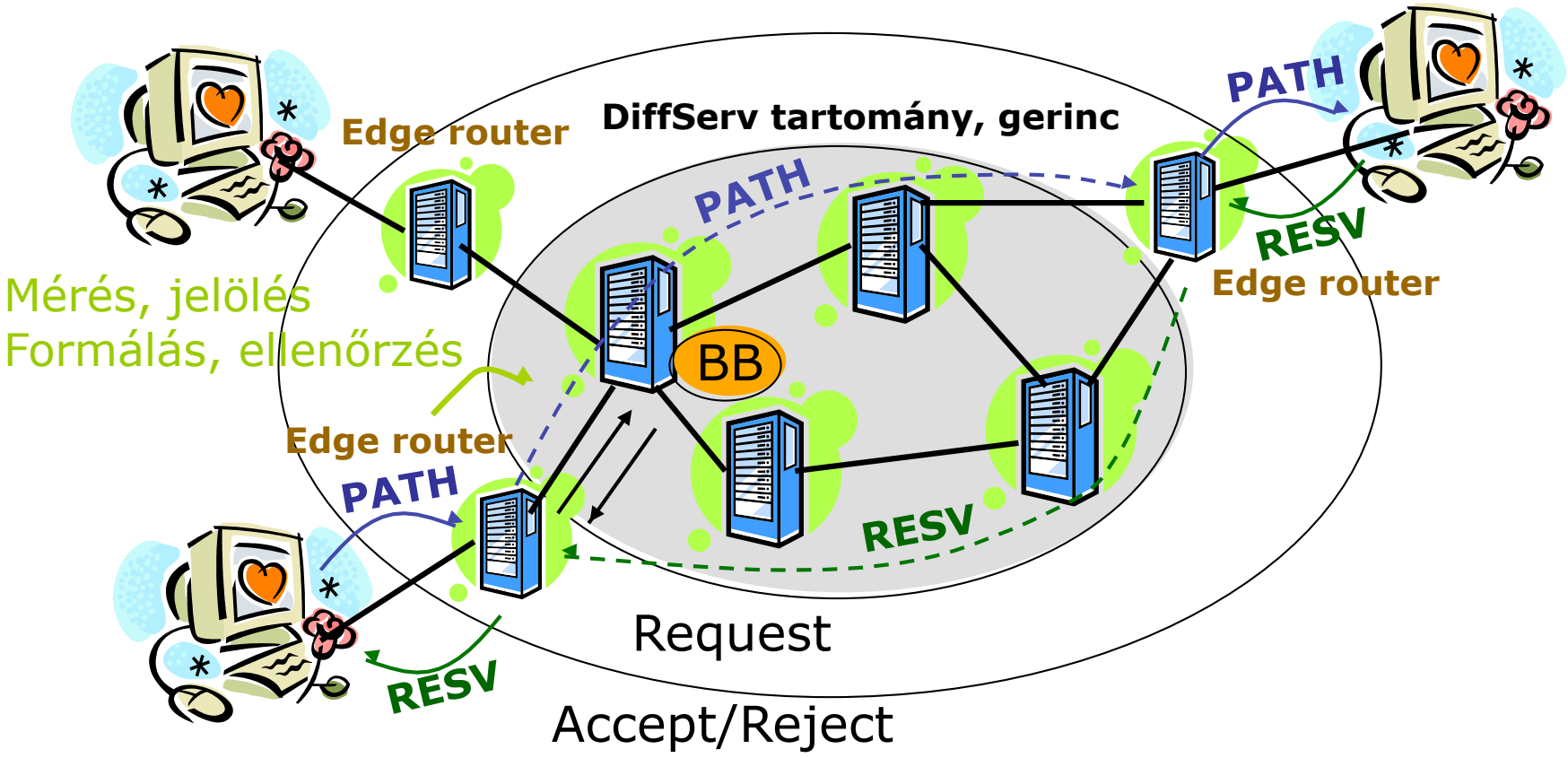
Osztályon belüli torlódás: a legkisebb eldobási valószínűségű élvez előnyt

Eldobási valószínűség szolgáltatónál: elég alacsony mindegyik eleinte, amelyik csomagok túllépik a „szerződött” átviteli rátát, azoknál növelik

Az IntServ és a DiffServ összehasonlítása

Jellemző	IntServ	DiffServ
Szolgáltatások kezelési módja	Végpontok közötti	Helyi (lépésenkénti)
Szolgáltatások kezelésének hatóköre	Egyedi- vagy többes-című út	Bárhol a hálózatban
A skálázhatóság (scalability) korlátja	Csomagfolyamok száma	Szolgáltatás-osztályok száma
Számlázás alapja	Forgalom- és QoS jellemzők	Forgalmi osztály használat
Forgalommenedzsment fajtája	Hasonló, mint az áramkörkapcsolt	Hasonló, mint az IP hálózaté
Megvalósítás helye	Hozzáférési hálózat	Gerinchálózat

DiffServ és IntServ: IntServ szolgáltatás DiffServ-hálózaton



DiffServ és IntServ (folyt.)

1. Az adó PATH üzenete eljut a vevőhöz
2. A vevő RESV válasza megérkezik az adóoldali *Edge router*-hez
3. Ez a router a DiffServ ***Bandwidth Broker*-éhez** fordul egy igénnyel
4. Ha a *BB* elfogadja, akkor értesíti az adót (RESV)
5. Az adó megkezdi a csomagküldést, az *Edge router* jelöli a csomagokat a megfelelő **DSCP (*differentiated services code point*) értékkel**
6. Az ***Edge router* ellenőrzi az adó forgalmát**: megfelel-e a szolgáltatási szerződésnek (SLA - *service level agreement*). „Kilógó” csomagokat vagy eldobja, vagy alacsony prioritásúnak jelöli.
7. **A *Core routerek* csak a DSCP-t nézik**, végzik a PHB-t

Hol, milyen eszközökben valósítják meg az IntServ-et és a DiffServ-et?

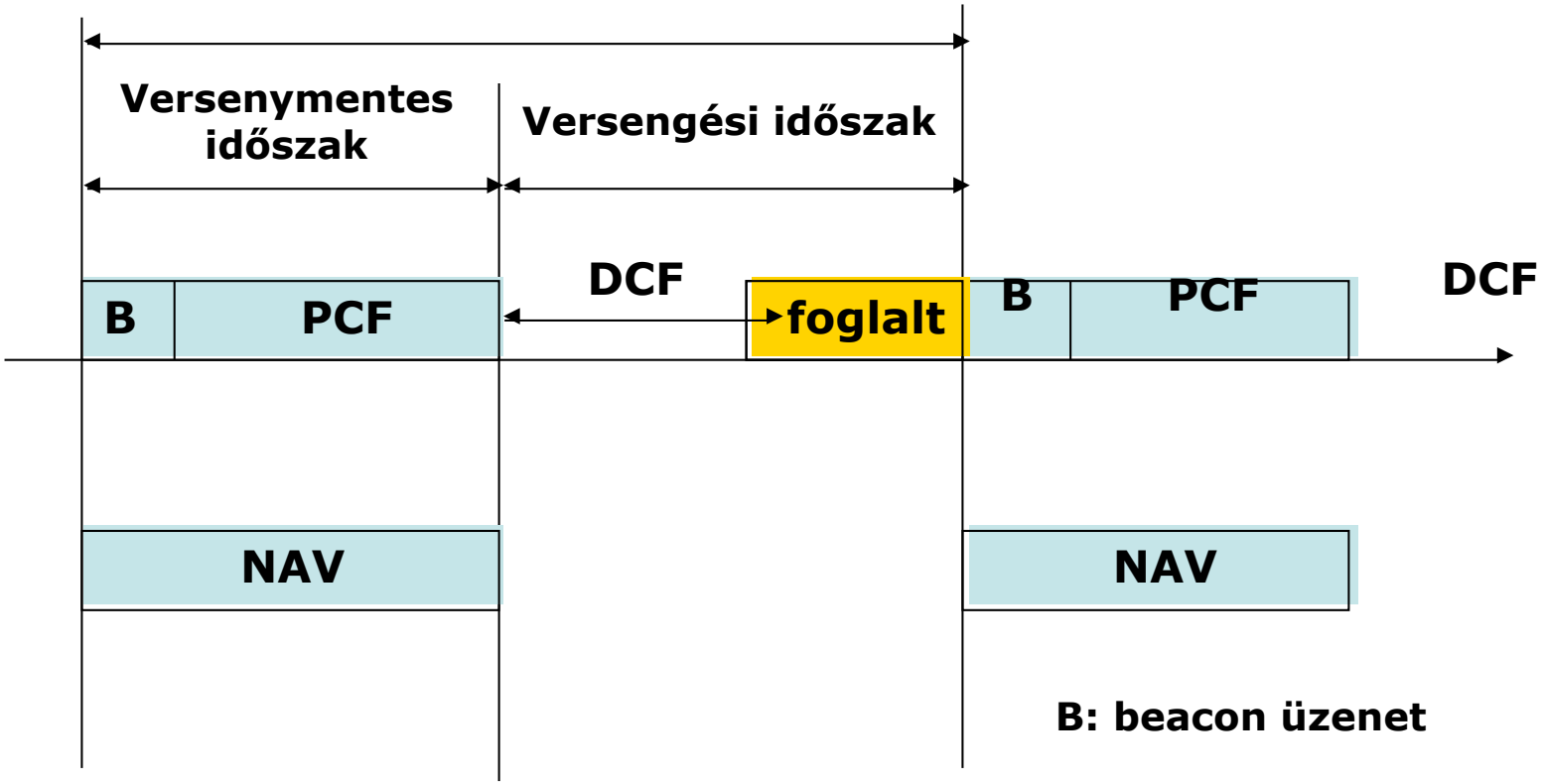
- IntServ: végponti eszközökben és az edge routerekben
- DiffServ: valamennyi routerben
  - Pl.: a Cisco IOS része
- Alkalmazás a szolgáltatóknál:
  - Eleinte, amíg van elég kapacitás, nemigen
  - Később, a forgalom növekedtével, egyre inkább

Röviden a QoS-biztosításról a vezeték nélküli LAN-okban és MAN-okban

2013. április 30.
Budapest

WLAN: a PCF lehetőséget ad QoS biztosítására

Mi is volt a PCF – Point Coordination Function?



Általában nem implementálják, csak a DCF-et…

Szolgáltatásminőség biztosítása (QoS) a WLAN-okban: a 802.11e szabvány

- **HCF – Hybrid Coordination Function**

- Kétféle MAC-módszer, DCF-PCF analógia
- Forgalmi osztályok (Traffic Category): pl. e-mail alacsony, Voice over WLAN magas prioritású

  - **EDCA – Enhanced Distributed Channel Access**
    - Versenyzés: prioritásos kevesebb ideig vár
    - Van itt is versenymentes idő: hang és videó számára

  - **HCCA – HCF Controlled Channel Access**
    - Mint PCF, de AP bármikor elrendelhet versenymentes periódust, egyébként EDCA verseny
    - Előre veszi a magasabb prioritású osztályt (per-session service)
    - Legbonyolultabb CF, állomásokon DCF felett is működhet, AP-n új ütemező kell, ritkán valósítják meg

WiMAX: a MAC rétegben “igazi” QoS

Alkalmazások, QoS-osztályok és QoS-paraméterek

QoS Category	Applications	QoS Specifications
UGS Unsolicited Grant Service	VoIP	• Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance
rtPS Real-Time Polling Service	Streaming Audio or Video	• Minimum Reserved Rate • Maximum Sustained Rate • Maximum Latency Tolerance • Traffic Priority
ErtPS Extended Real-Time Polling Service	Voice with Activity Detection (VoIP)	• Minimum Reserved Rate • Maximum Sustained Rate • Maximum Latency Tolerance • Jitter Tolerance • Traffic Priority
nrtPS Non-Real-Time Polling Service	File Transfer Protocol (FTP)	• Minimum Reserved Rate • Maximum Sustained Rate • Traffic Priority
BE Best-Effort Service	Data Transfer, Web Browsing, etc.	• Maximum Sustained Rate • Traffic Priority

QoS- osztályok és paraméterek

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

QoS-biztosítási módszerek összefoglalása

- QoS összeköttetés-alapú hálózatokban
  - ATM
- QoS összeköttetésmentes hálózatokban
  - módszerek a hálózati rétegben, az IP-protokoll alapján
  - **IntServ**: folyamonkénti QoS-biztosítás, az összeköttetés-alapú megoldásokhoz hasonlóan, nem jól skálázható
  - **DiffServ**: osztályonkénti QoS-biztosítás, alkalmas gerinchálózati megvalósításra
  - A végpontok közötti (end-to-end) QoS-hez mindkét módszerre szükség van

Multimédia IP-hálózatokban, összefoglalás

- *Feladatcsoportok és*
  - *jellegzetes protokollok*
- Médiakezelés
  - RTP, RTCP, RTSP (1. rész)
- Hívásvezérlés
  - SIP (2. rész)
- Szolgáltatásminőség-biztosítás
  - IntServ*, DiffServ*, RSVP (3. rész)

*) *nem protokoll, hanem módszer*

HÁLÓZATI ALKALMAZÁSOK

Dr. Simon Vilmos
adjunktus
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu

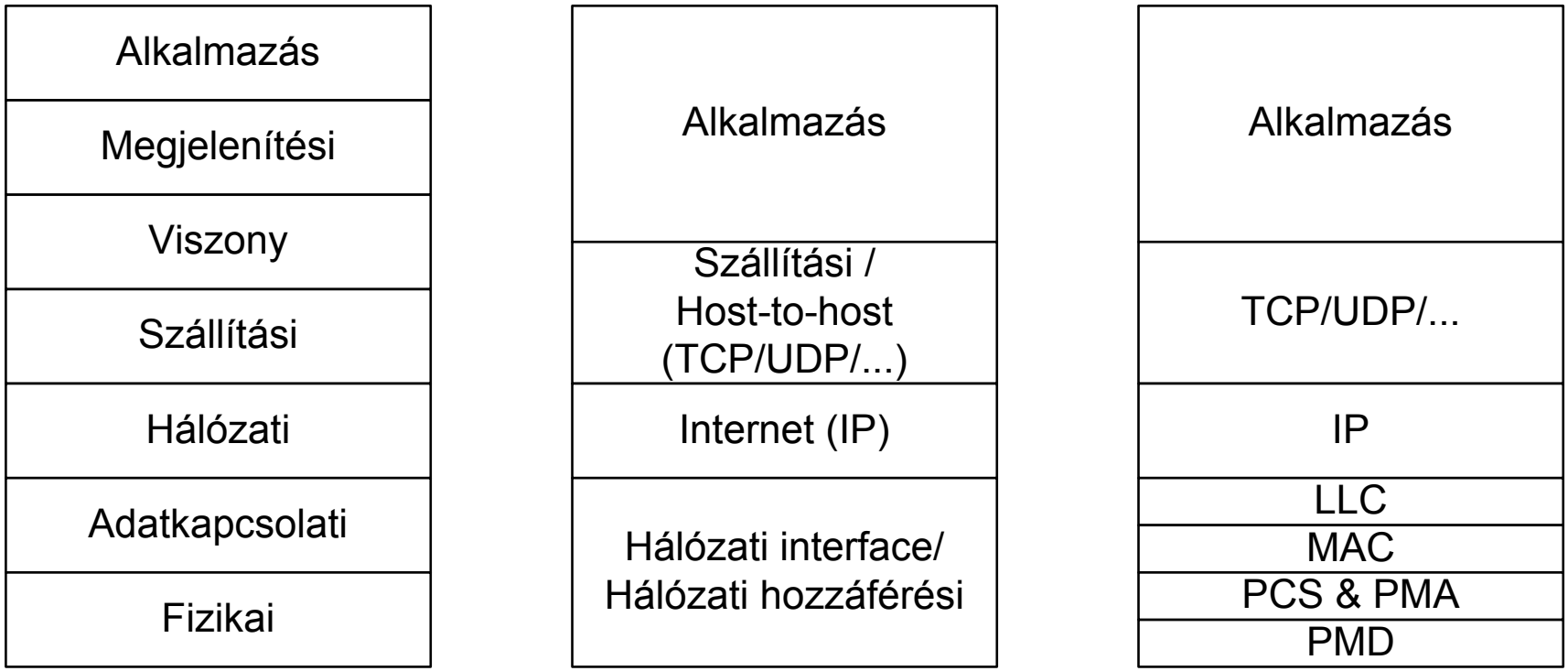
2013.Május 7.

A tartalomból

- Hálózati alkalmazások
- Alkalmazásprotokollok
- Infrastrukturális szolgáltatások
- Névfeloldási szolgáltatás
- Levelezési rendszerek
- Webes rendszerek

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

TCP/IP architektúra és az ISO/OSI rétegmodell



IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

LLC: Logical Link Control

MAC: Medium Access Control

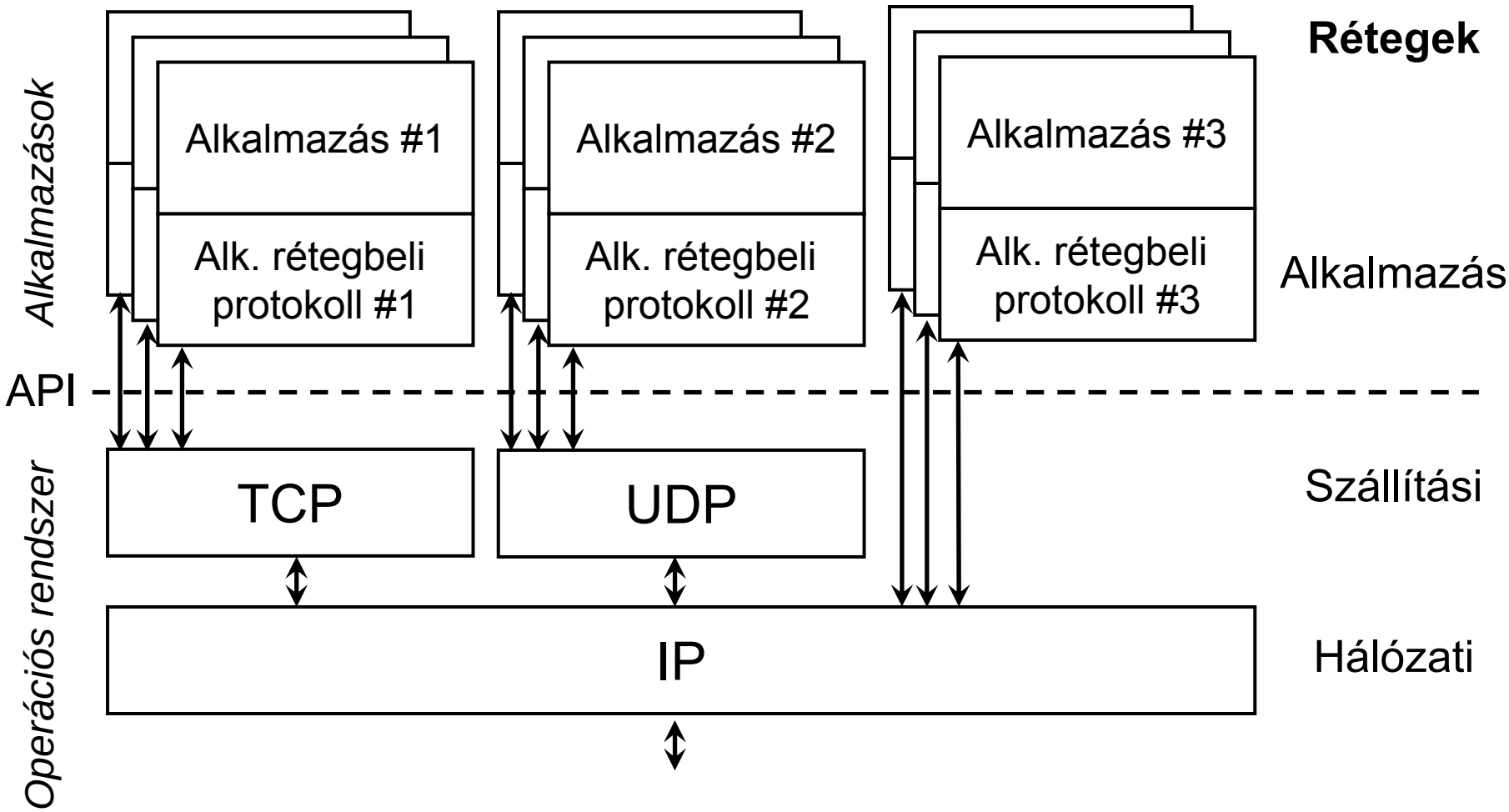
PCS: Physical Coding Sublayer

PMA: Physical Medium Attachment

PMD: Physical Medium Dependent

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

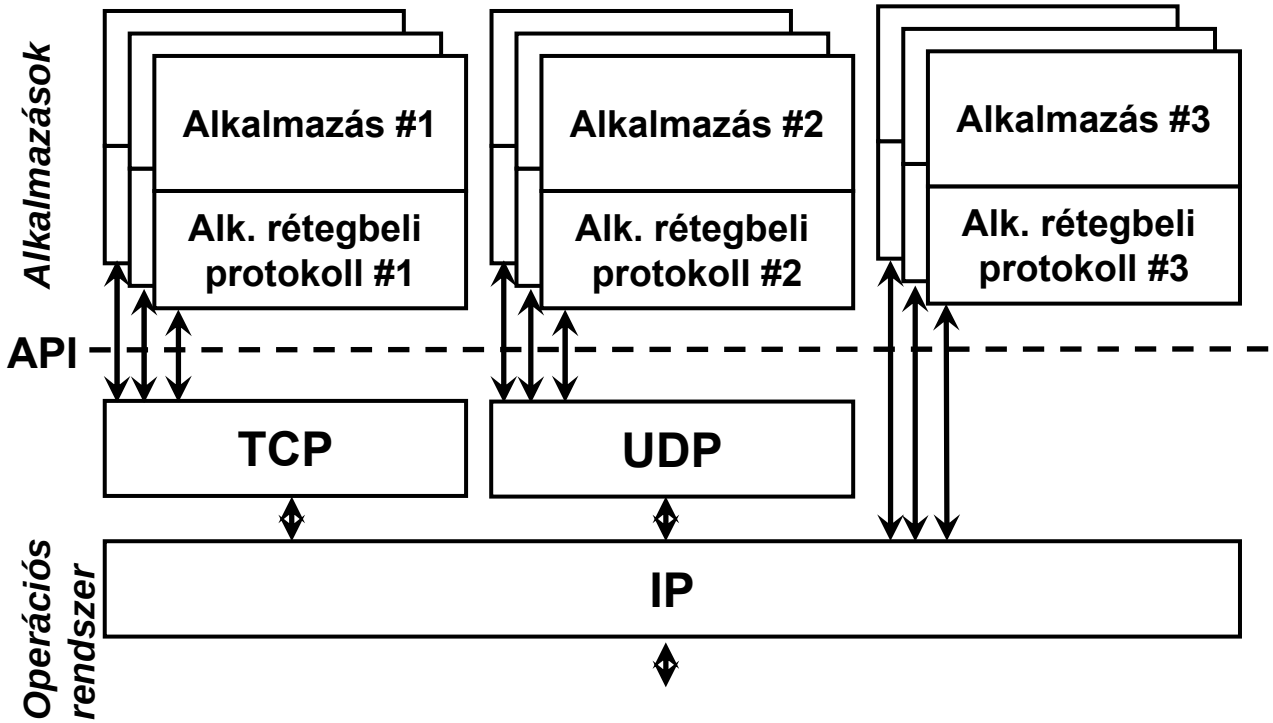
Alkalmazások kapcsolata az alsóbb rétegekkel



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazás-rétegbeli protokollok

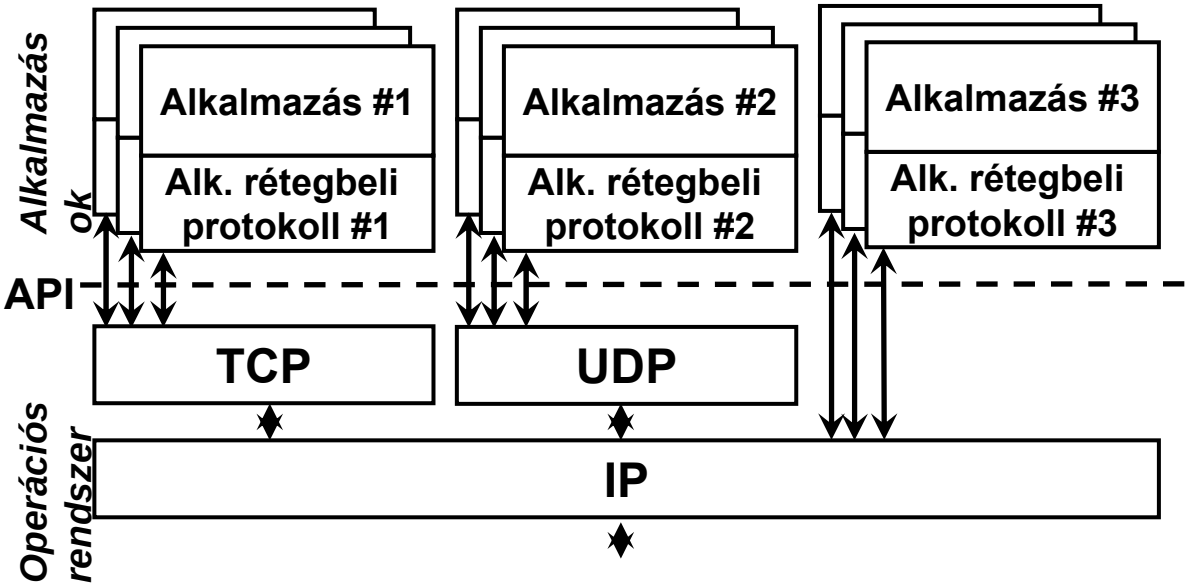
- Legtöbbször az alkalmazásban kerül implementálásra
  - Alkalmazás logikájához szorosan kapcsolódik
  - Egy alkalmazás-rétegbeli protokollt tipikusan kevés alkalmazás használja
- Mégis szükséges szabványosítani (lásd RFC-k)
  - Alkalmazások együttműködése



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazások környezete

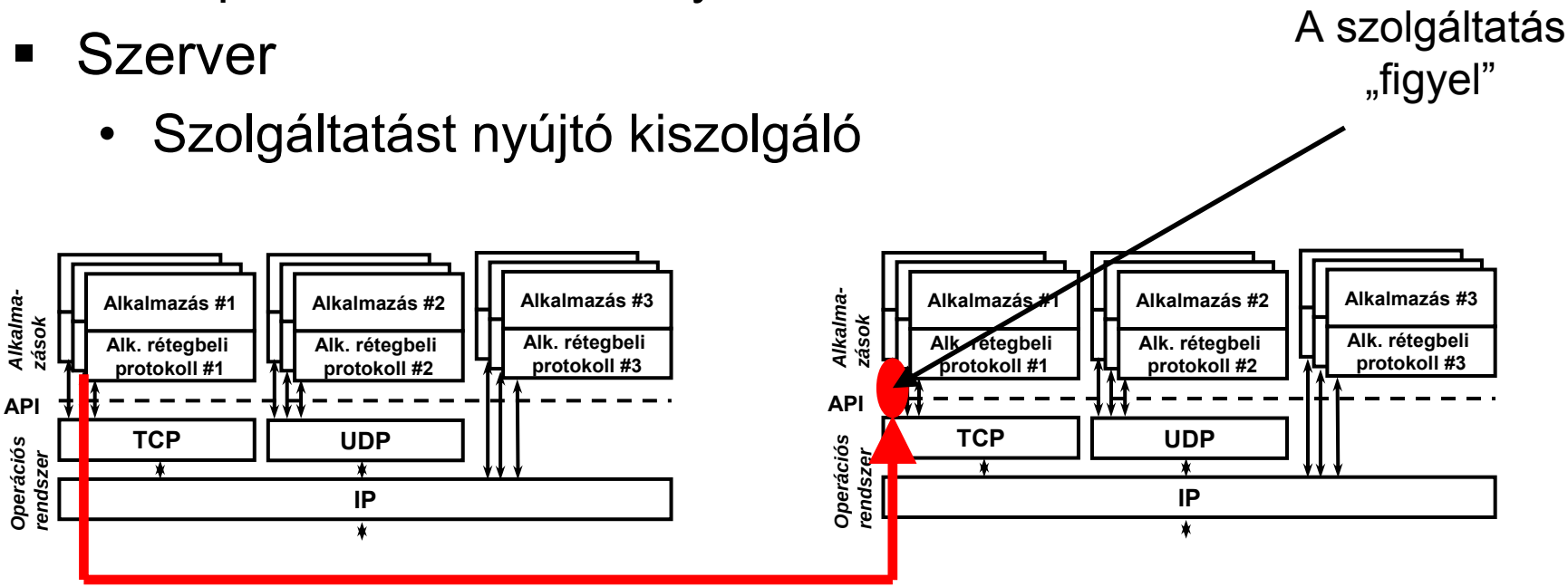
- **Alsóbb rétegeket** – mint szolgáltatásokat – az **operációs rendszer** biztosítja
- **Elfedi** a tényleges rétegeket
- Csak egy interfészt (API: Application Programming Interface) biztosít
  - SAP (Service Access Point)
- Ennek rendszerhívásait használva létrehozható a kívánt kommunikációs csatorna
  - az alkalmazás által használható végződése: **socket**



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Kliens-szerver architektúra

- Kliens
  - Kapcsolatot kezdeményező fél
- Szerver
  - Szolgáltatást nyújtó kiszolgáló



- Kliensnek a szolgáltatást meg kell címeznie
  - IP-cím (vagy DNS név) + szállítási protokoll + portszám

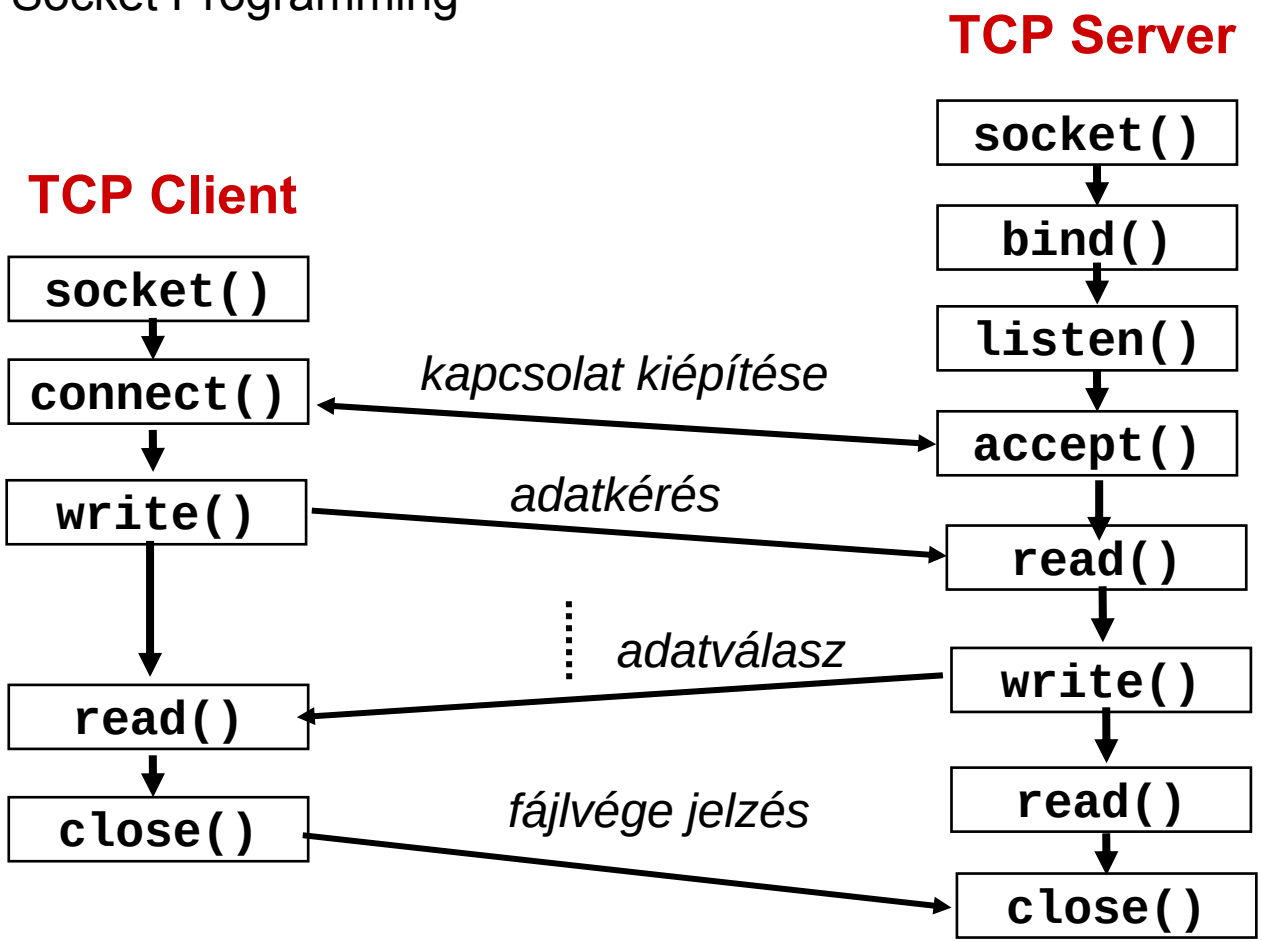
Port-hozzárendelés

- Szerveren
  - Szolgáltatást azonosítja
    - egy port maximum egy szolgáltatáshoz lehet hozzárendelve
  - Statikus
  - 1-65536 tartományból tipikusan 1-1023-ig
    - ***well-known ports***
    - privilegizált szerver programok kapcsolódhatnak csak

- Kliensen
  - Dinamikusan kerül kiosztásra a még nem használtak közül
  - 1-65536 tartományból 1024-65535-ig
    - Regisztrált (1024-49151) illetve dinamikus portok (49152-65535)

TCP kommunikáció sockethívásokkal

Socket Programming



UDP: egyszerűbb, kevesebb hívás

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Socket létrehozása

- Meg kell adni a socket:
  - Típusát
    - Stream: TCP-vel, megbízható kétirányú kapcsolat
    - Datagram: UDP-vel, kapcsolatmentes, nem megbízható
    - Raw: hozzáférés a hálózati szintű protokollhoz
  - Domain-t
    - Unix: helyi kommunikáció
    - Internet: IPv4 vagy IPv6

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Milyen alkalmazás milyen szállítási rétegbeli protokollon?

	Natív IP	UDP	TCP
Kapcsolatorientált	✘	✘	✓
Megbízható	✘	✘	✓
Üzenetméret (tipikus)	rövid	rövid	hosszú
Adattovábbítás jellege	datagram	datagram	bitstream pipe
Portkezelés	✘	✓	✓
Overhead	minimális	kicsi	nagy
Alkalmazások	vezérlési és menedzsment •ICMP, IGMP •Routing	multimédia -átvitel, névfeloldás	fájlátvitel, web, levelezés

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazások, protokollok és portszámok – natív IP felett

- Natív IP szolgáltatást igénybevevő protokollok és az IP Protocol mező értéke*:
  - Vezérlés:
    1: ICMP (Internet Control Message Protocol)
    2: IGMP (Internet Group Management Protocol)
  - Routing:
    8: EGP (Exterior Gateway Protocol)
    89: OSPF (Open Shortest Path First)
  - Egyéb:
    132: SCTP (Stream Control Transmission Protocol)
  - Valódi szállítási rétegbeli protokollok:
    6: TCP (Transmission Control Protocol)
    17: UDP (User Datagram Protocol)

* kezdeti lista az RFC 790-ben

* a mező értékeit **az IANA** (Internet Assigned Numbers Authority) felügyeli

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazások, protokollok és portszámok – UDP felett

- UDP szolgáltatásait igénybevevő protokollok és a tipikus **szerveroldali** UDP portszám értéke*:
  - **53 DNS (Domain Name System)**
    - névfeloldás
  - 67 BOOTP (Bootstrap Protocol) (Server)
    DHCP (Dynamic Host Configuration Protocol)
    - konfigurálás
  - 68 BOOTP (Bootstrap Protocol) (Client)
    DHCP (Dynamic Host Configuration Protocol)
    - konfigurálás
  - 69 TFTP (Trivial File Transfer Protocol)
    - fájlátvitel
  - 123 NTP (Network Time Protocol)
    - időszinkronizáció
  - 161 SNMP (Simple Network Management Protocol)
    - hálózatmenedzsment
  - 520 RIP (Routing Information Protocol)
    - routing

* a portszámokat az IANA (Internet Assigned Numbers Authority) felügyeli

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Alkalmazások, protokollok és portszámok – TCP felett

- TCP szolgáltatásait igénybevevő protokollok és a tipikus szerveroldali TCP portszám értéke*:
  - **20 és 21 FTP (File Transfer Protocol)**
    - Ugyanahhoz a protokollhoz két port is!
  - **22 SSH (Secure Shell)**
  - **23 Telnet**
  - **25 SMTP (Simple Mail Transfer Protocol)**
  - **53 DNS (Domain Name System)**
    - Ugyanahhoz a protokoll UDP-n és TCP-n is!
  - **80 HTTP (HyperText Transfer Protocol)**
  - **110 POP3 (Post Office Protocol version 3)**
  - **143 IMAP4 (Internet Message Protocol version 4)**
  - **443 HTTPS (HTTP Secure)**
  - **465 SMTPS (SMTP Secure)**
  - **993 IMAP4S (IMAP4 Secure)**
  - **995 POP3S (POP3 Secure)**

* a portszámokat az IANA (Internet Assigned Numbers Authority) felügyeli

DNS – Domain Name System

DHCP – Dynamic Host Configuration Protocol

INFRASTRUKTURÁLIS SZOLGÁLTATÁSOK

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

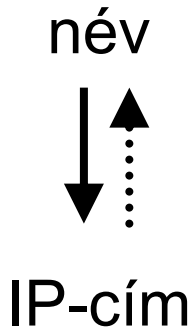
DNS – Domain Name System

NÉVFELOLDÁSI RENDSZER

A névfeloldás szerepe és követelményei

- Eltérő reprezentációk közötti megfeleltetés
  - Humán: könnyen megjegyezhető, beszédes nevek
  - Gépi: IP-címek

  → névfeloldás
- Követelmények:
  - Jó skálázhatóság
  - Hibatűrés
  - Aktuális (friss) információk

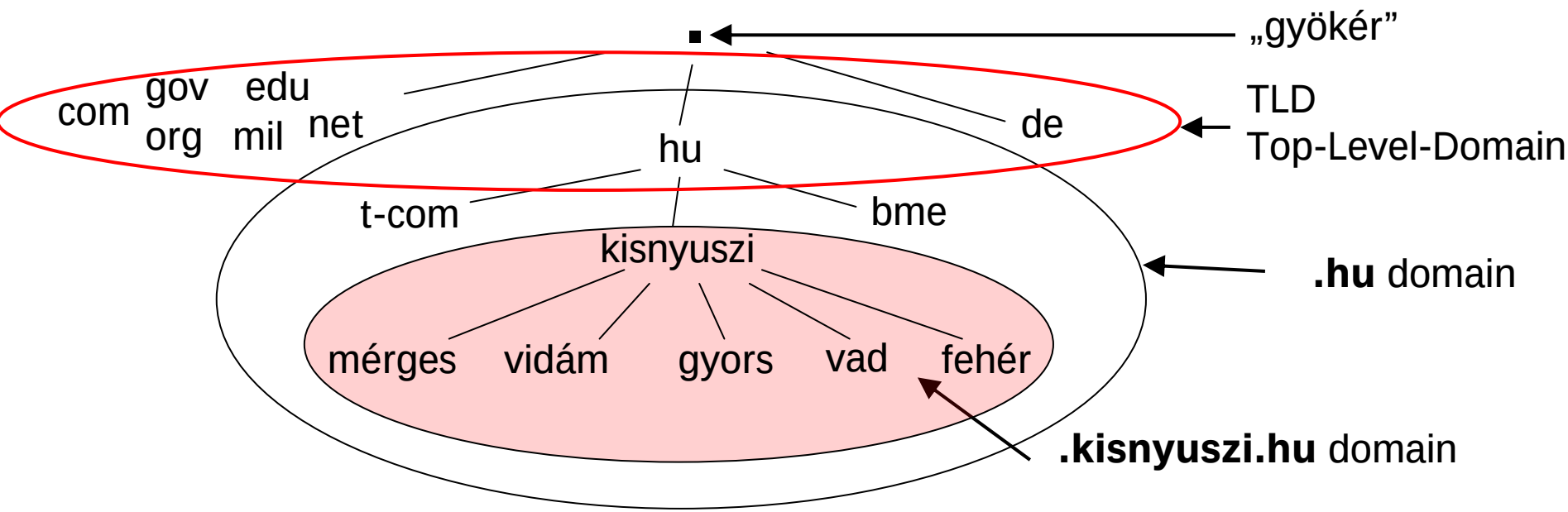


A DNS (Domain Name System) névtere

- Hierarchikus
- Állomások azonosítása: FQDN (Fully Qualified Domain Name)

vad.kisnyuszi.hu.

host neve | tartomány neve (FQDN suffix)



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

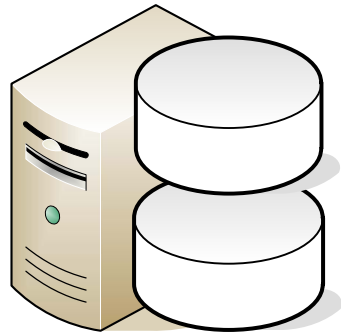
A DNS névtér „csúcsa”

- Root (gyökér):
  - „.” – ponttal jelölik
  - Elméletileg minden FQDN emiatt ponttal zárul
  - **Gyökérzóna**: legmagasabb szintű DNS zóna
    - Valójában világszerte kb. 16 DNS szerver szolgáltatja
  - **Anycast címzés** előnye!
- Top level domains: a név utolsó része
  - Az IANA adminisztrálja
    (Internet Assigned Numbers Authority)
  - country code top-level domains (ccTLD): pl. .hu
  - generic top-level domains (gTLD): pl. .org, .edu, .net, .com, .gov, .mil
  - infrastructure top-level domains: egy van, az .arpa

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

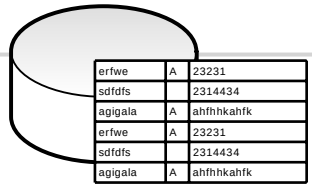
A DNS zóna és névszerverek

- Zóna
  - Minden tartomány csúcsának vagy egészének adatit tároló adatbázis
  - A DNS nevével azonosítjuk (pl. kisnyuszi.hu.)
- DNS szerver
  - Egy vagy több zónát tárol, szolgál ki
- Elsődleges/másodlagos DNS szerver
  - Egy adott zónára vonatkozóan
    - Elsődleges: írható és olvasható
    - Másodlagos: csak olvasható
  - Minden esetben pontosan 1 elsődleges és legalább 1 másodlagos kell
    - → hibatűrés
    - → terheléselosztás és skálázhatóság
  - Szinkronizálás monoton növekvő verziószám alapján
    - Egyre elfogadottabb a verziószám: YYYYMMDDnn



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

A zóna elemei: rekordok



Az erőforrásrekordok (Resource Records - RR) gyakori típusai:

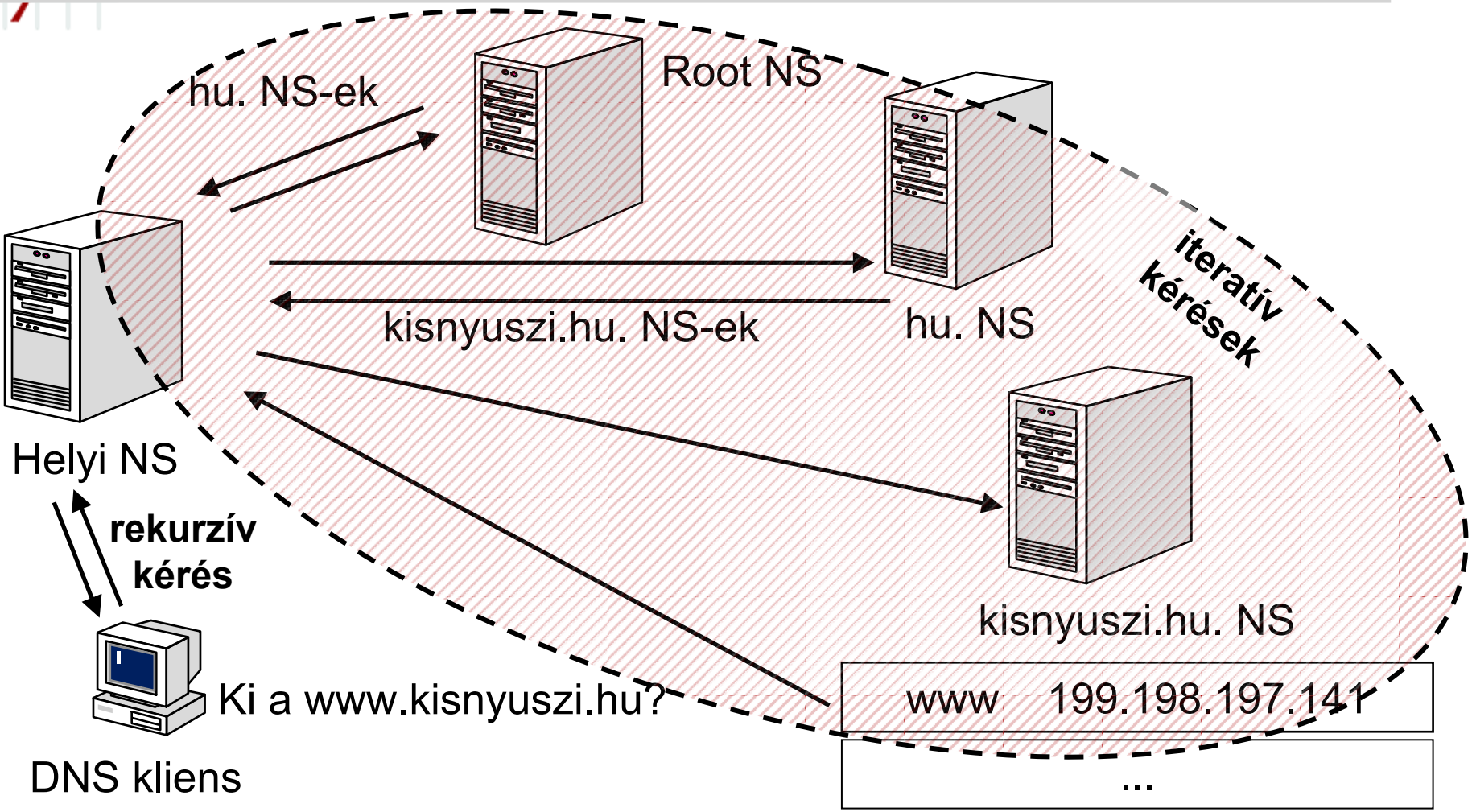
- SOA (Start of Authority)
  - adminisztratív adatok
    - az elsődleges DNS szerver neve
    - zóna verziószáma (ez alapján a szinkronizálás)
    - kapcsolattartó e-mail címe
- A (Address)
  - név – IP-cím
  - a legtipikusabb felhasználás
- CNAME (Canonical Name)
  - más néven „alias”
  - név – név összerendelés
- PTR (Pointer)
  - IP-cím – név
  - ún. reverse zónában

- NS (Name Server)
  - az adott zónát kiszolgáló DNS szerverek
  - legalább kettő kell
- MX (Mail Exchange)
  - SMTP kiszolgálót azonosít
  - Több is megadható preferenciával (prioritással)
- SRV (Service Locator)
  - MX általánosítása
  - tetszőleges szolgáltatásra

Altartományok (subdomain)

- delegálhatóság

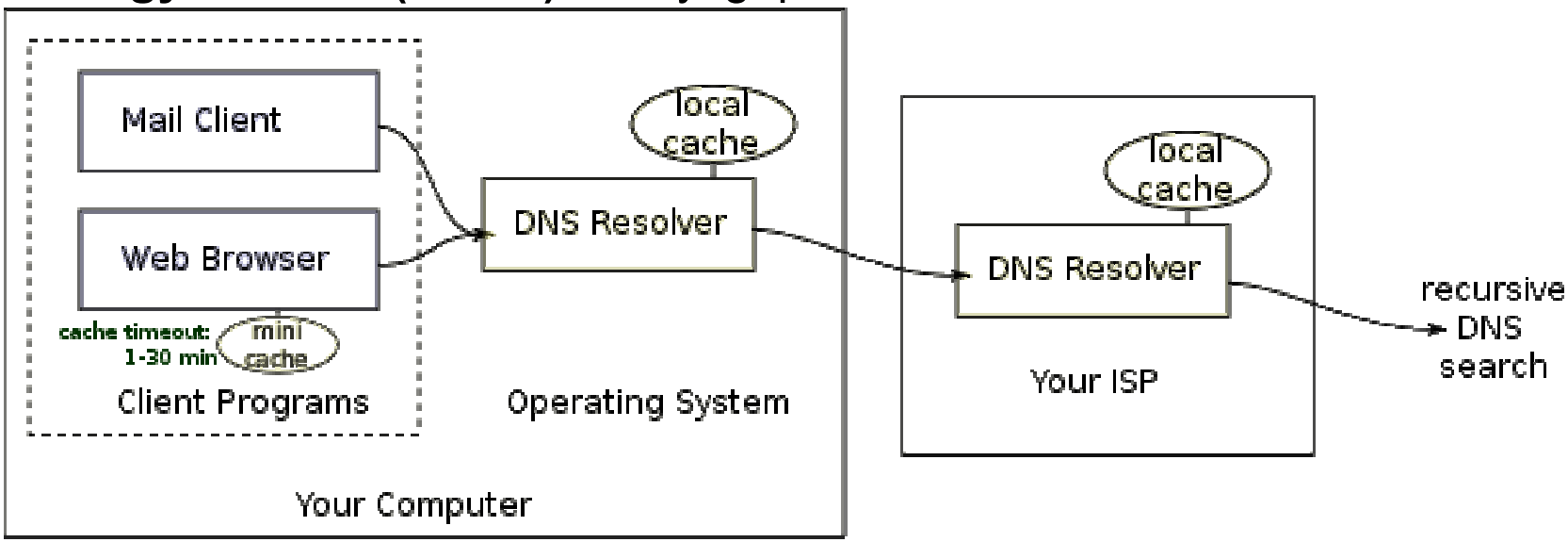
Névfeloldás menete



- Rekurzív kérés: a konkrét (vagy a negatív) választ várja, a címzettnek a feladata a névfeloldás
- Iteratív kérés: a minél közelebbi felelős megtalálása, arra egy hivatkozást ad vissza (referral)

Névfeloldás gyorsítótárral

- A DNS-kéréseket a helyi gépen az operációs rendszer oldja fel egységesen
- **DNS gyorsítótár (cache)** a helyi gépen és a DNS szerveren



- Minden rekordnak **TTL-je (Time To Live**) valódi másodpercben megadva → elévülés

- **Authoritatív válasz**: ha a rekordért felelős szerverek valamelyikétől származik a válaszol
- **Nem autoritatív**: ha gyorsítótárból származik

Névfeloldás menete

(0. Böngésző gyorsítótára)

1. Helyi gép gyorsítótára
2. Helyi gépen „hosts” fájl
3. Lekérdezés DNS szerverektől
   - Ha van DNS szerver megadva
     - Lekérdezés az elsődleges DNS szervertől, ha elérhető (rekurzív)
       - Az a cache-ből kiszolgál vagy névfeloldást végez (iteratív)
     - Lekérdezés a másodlagos DNS szervertől, ha meg van adva és az elsődleges nem érhető el (rekurzív)
   - Ha nincs DNS szerver megadva vagy nem elérhetők, akkor lekérdezés valamely root NS-től, majd a hivatkozott NS-ektől (iteratív)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

DNS mint protokoll: kapcsolatok

- A DNS protokoll felhasználási területei:
  - Lekérdezés:
    - DNS kliens ⇔ DNS szerver
    - UDP 53 ← rövid, gyors üzenetváltás

      (TCP 53)
  - Zónaletöltés
    - Elsődleges DNS szerver ⇨ másodlagos DNS szerver
    - TCP 53 ← hosszabb, megbízhatóbb

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

DNS mint protokoll: üzenetek

- Kérés elemei
  - Kért rekord típusa(i)
  - Feloldandó név vagy IP-cím
  - **Rekurzív kérés esetén** RD (Recursion Desired) bit beállítva
- Válasz
  - Pozitív válasz: egy vagy több elemű lista
    - Ebből „véletlenszerűen” (round-robin) választ
  - **Authoritatív válasz esetén** az AA (Authoritative Answer) bit beállítva
  - **Referral** válasz (egy vagy több elemű lista)
    - Kiegészítő hivatkozásokat tartalmaz, mely közelebb visz a feloldáshoz
      - pl.: illetékesebb NS; A rekord helyett azonos nevű CNAME rekord
  - Negatív válasz: nem található bejegyzés, nem oldható fel
    - Nincs válasz ≠ negatív válasz

Dynamic Host Configuration Protocol

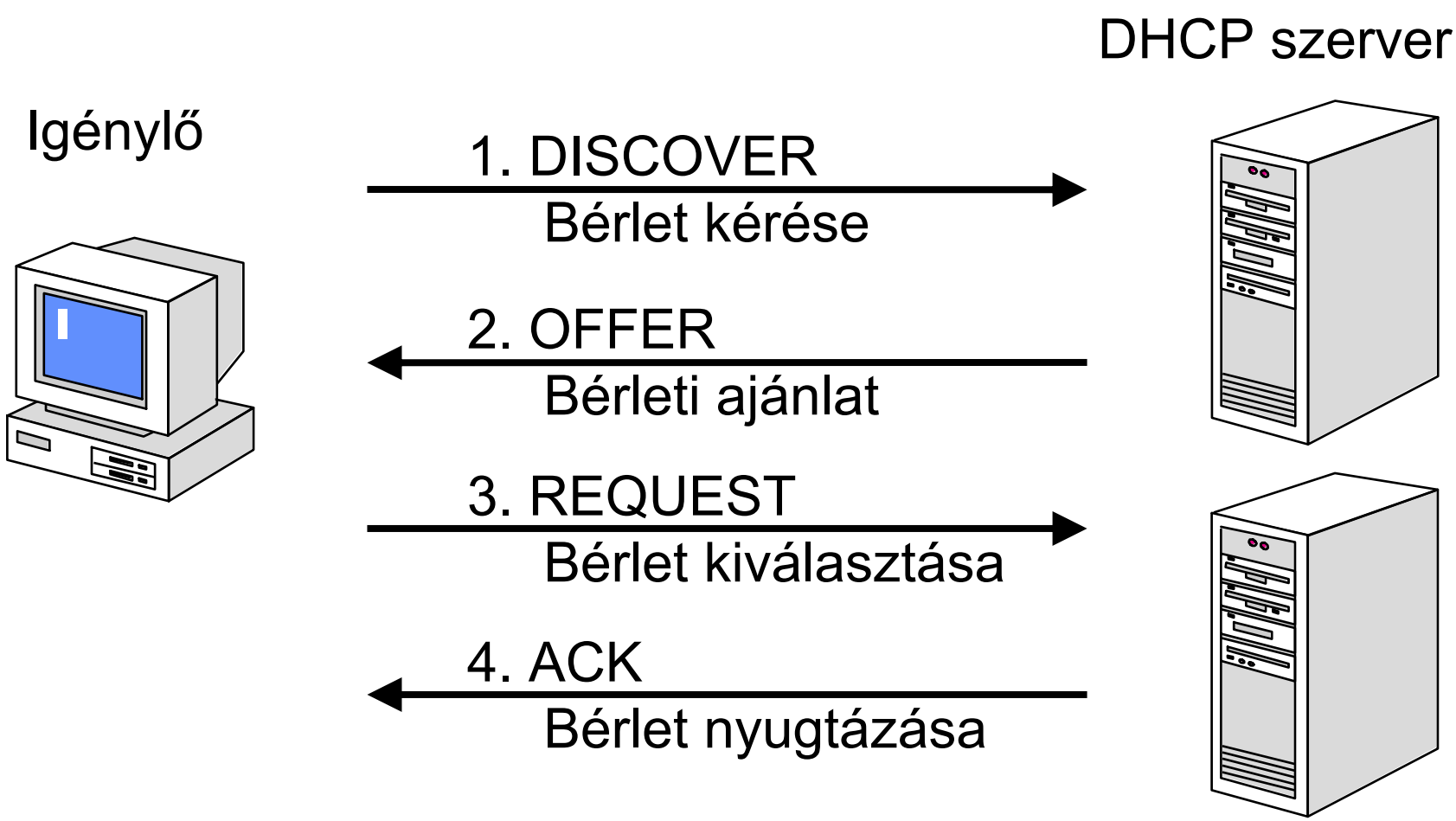
DHCP

Általában a DHCP-ről

- Mi a DHCP?
  - IP-beállításokat oszthatunk ki vele dinamikusan
- Előnyei:
  - Nem kell tudni, hogy milyen címeket osztottunk már ki
  - Kliensek egyszerű beállítása
  - Módosítások központilag
  - Mobilitás hálózatok között (eltérő beállítások)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

IP cím igénylése



DISCOVER és OFFER
Bérlet kérése és felajánlása

- Kérés:

  0.0.0.0-tól (még nincs IP-címe) → 255.255.255.255-nek (bárkinek)

- Ajánlat:

  255.255.255.255-nek ← (bárkinek; nem címezhető) 192.168.1.1-től (egy DHCP szerver címe)

- Ajánlat tartalma
  - IP-cím
  - Alhálózati maszk
  - Bérleti idő
  - DHCP szerver IP címe
  - **Igénylő MAC címével!**

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

REQUEST és ACK
Bérlet kiválasztása és nyugtázása

- Kiválasztás
  - az első ajánlatot (pl. ha több DHCP szerver)
  - Kiválasztási üzenet:
    - 0.0.0.0-tól 255.255.255.255-nek
    - Az üzenet tartalma
      - **kért IP-cím**
      - **DHCP szerver IP-címe**
- Nyugta
  - 192.168.1.1-től, 255.255.255.255-nek
  - Nyugtázó üzenet tartalma
    - **kiosztott IP-cím**
    - **alhálózati maszk**
    - **bérleti idő**

Bérleti idő (TTL)

- Bérleti időbeli kezelése
  - Félidőben hosszabbítási kérés
  - 7/8 TTL-nél új igénylése
- Hosszú vagy rövid TTL?
  - Rövid mellett
    - Ha a kliens szabálytalanul távozik a hálózatból
      - a bérletét nem adja vissza
    - Ha a kliens szabálytalanul újraindul
      - nem adja vissza a bérletét, és még újat is igényel
    - A beállításváltozások gyorsan életbe lépjenek
  - Hosszú mellett
    - Ne legyen nagy hálózati forgalom

Ami DHCP-vel beállítható…
DHCP opciók, paraméterek

- **0x01 Subnet Mask (alhálózati max)**
- **0x0F Domain Name (FQDN suffix)**
- **0x03 Router (alapértelmezett átjáró(k))**
- **0x06 DNS (DNS szerver(ek))**
- **0x0C Host Name (gép neve is kioszthető)**
- 0x1F Router Discovery
- 0x21 Static Route
- 0x2B Vendor Specific (gyártófüggő beállítások)
- 0x2C WINS
- 0x2E NBT
- 0x2F Node Type
- **0x32 Requested Address (igényelt IP-cím)**
- **0x33 Lease Time (TTL)**
- **0x36 DHCP Server (DHCP szerver IP-címe)**
- **0x37 Parameter Request List (igényelt paraméterek listája)**
- **0x3A Renewal Time (megújítási idő)**
- 0x3B Rebinding Time
- 0x3C Client Class Information
- 0x4D User Class Information
- 0xF9 Static Route CIDR

Stb…

DHCP egyéb alkalmazása

- DHCP hibatűrés
  - Több DHCP használata egy hálózatban, de **diszjunkt IP-címtartományok osztása**!
- DHCP kiterjesztése több hálózati szegmensre
  - A routerek nem engedik át a DHCP üzeneteket
  - A routerekre ún. „**DHCP Relay Agent**”-et telepítve az továbbítja a DCHP forgalmat a DHCP szerverek és kliensek között
- IPv6-ban minden router egyben DHCP szerver is

Telnet

FTP – File Transfer Protocol

SZÖVEG- ÉS FÁJLÁTVITEL

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Telnet

- Egyik legrégebbi alkalmazás
- Távoli parancssor
  - Parancsok elküldése
  - Visszajelzések megjelenítése
- Még ma is alkalmazzák főként hálózati eszközök egyszerű hálózati adminisztrációjára
- Nem biztonságos (jelszavak védelem nélkül)
  - SSH (Secure Shell) helyette

FTP – File Transfer Protocol

- Az egyik legelső fájlátvitelre tervezett protokoll
  - RFC 959
- TCP 21-es port
  - Ha a TCP 20-as portot használjuk adatcsatornaként, akkor ez csak vezérlés
- Parancsok
  - open – kapcsolat létrehozása
  - ls – aktuális könyvtár listázása
  - put – feltöltés
  - get – letöltés
  - delete – törlés
  - bye – kapcsolat lebontása
  - …

SMTP – Simple Mail Transfer Protocol

POP3 – Post Office Protocol v3

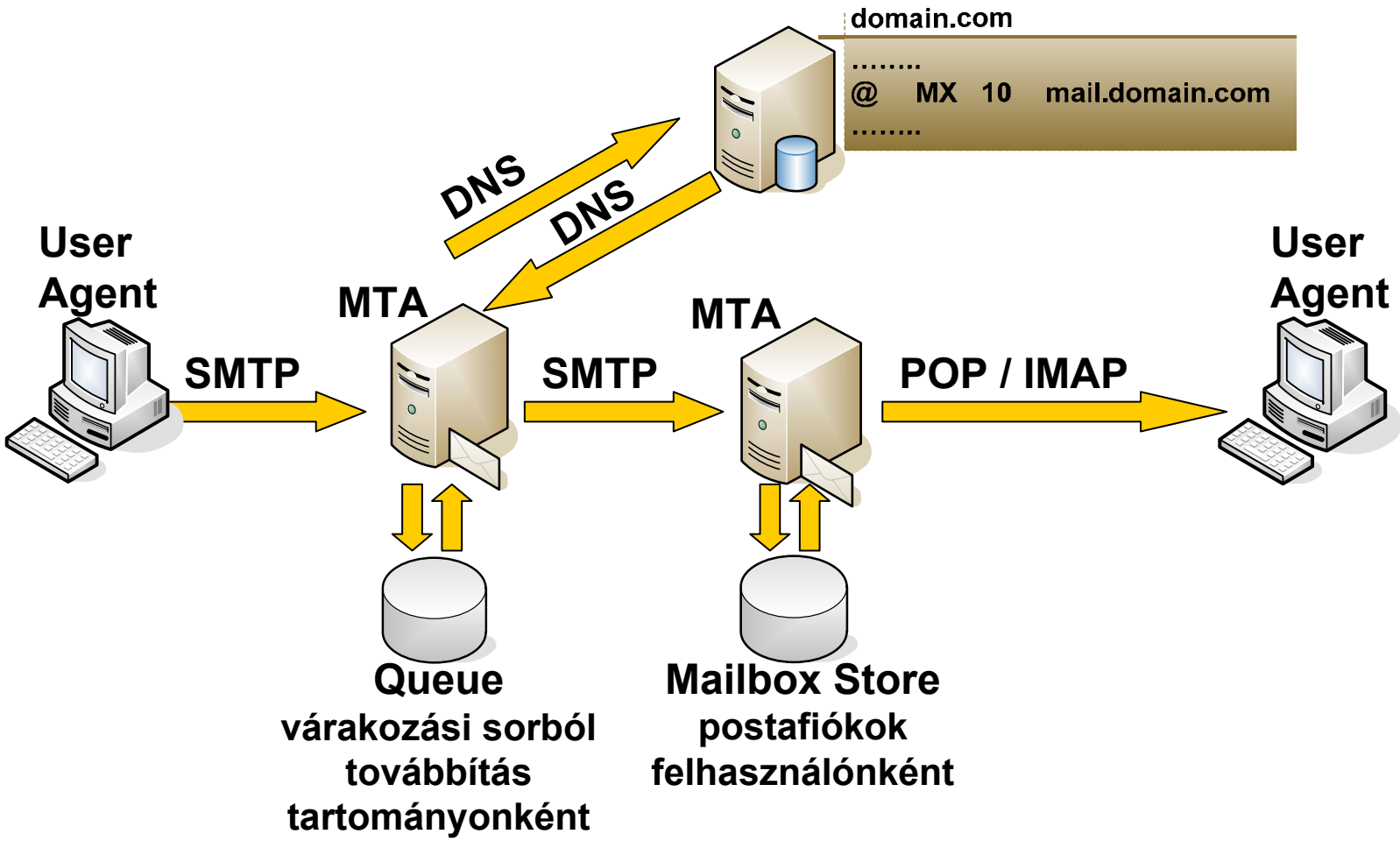
IMAP4 – Internet Message Protocol v4

LEVELEZŐ RENDSZEREK

Levelező rendszerek

- Komponensek
  - (Mail) User Agent ((M)UA) (levelező kliens)
  - Mail Transfer Agent (MTA) (SMTP szerver)
- Használt protokollok
  - SMTP: levél továbbításra
  - POP3: levelek lekérdezése
  - IMAP4: levelek lekérdezése
- Címzett meghatározása
  - DNS segítségével (MX rekord)

Levelező rendszerek



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Levelek lekérdezése – POP3 és IMAP4

POP3

- Post Office Protocol version 3
- RFC 1939, 1957, 1725
- Parancsorientált
- TCP 110-es port
- Levelek lekérdezésére
- POP3S
  - POP3 TLS tikosítással
  - TCP 995

IMAP4

- Internet Message Protocol version 4
- RFC 2060, 1731, 1730
- Parancsorientált
- TCP 143-as port
- Levelek lekérdezésére
- IMAP4S
  - IMAP4 TLS tikosítással
  - TCP 993
- Intelligensebb a POP3-nál:
  - Könyvtárstruktúra támogatása
  - Keresés támogatása
  - Nem törli automatikusan a szerveren tárolt leveleket

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

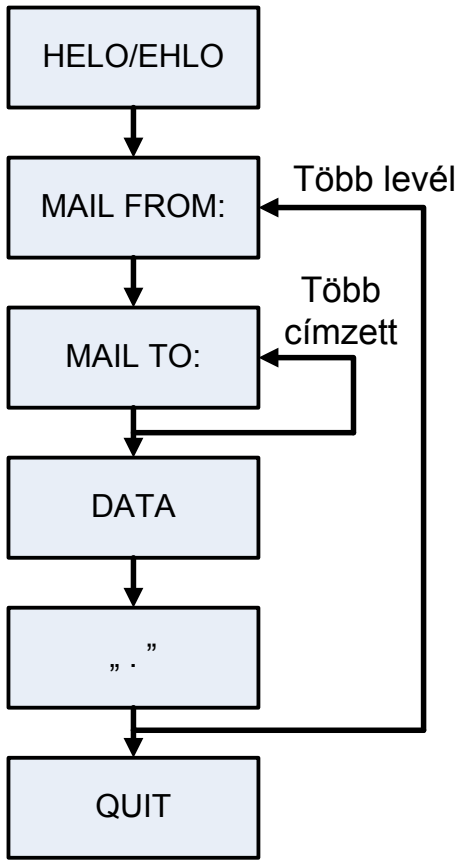
SMTP – Simple Mail Transfer Protocol

- RFC 821, 822
- Levelek továbbítására (első „killer application”)
- Parancsorientált állapotkódokkal
- TCP 25-ös port
- SMTP relay
  - Nem közvetlen továbbítás
  - Egy (vagy több) SMTP (relay) szerver közbeiktatásával
- SMTPS (SMTP Secure)
  - SMTP TLS csatornában
  - TCP 465

A leggyakoribb SMTP parancsok

- HELO
  - Üdvözlés
  - ESMTP esetén EHLO
- MAIL FROM:<feladó e-mail címe>
- RCPT TO:<címzett e-mail címe>
- DATA
  - Adat következik
- <CR><LF>.<CR><LF>
  - Adat vége
- QUIT
  - SMTP kapcsolat bontása
- VRFY <e-mail cím>
  - Létezik-e az adott e-mail cím
- HELP
- NOOP
  - Kapcsolat ellenőrzése, fenntartása

Tipikus kapcsolat folyamatábrája



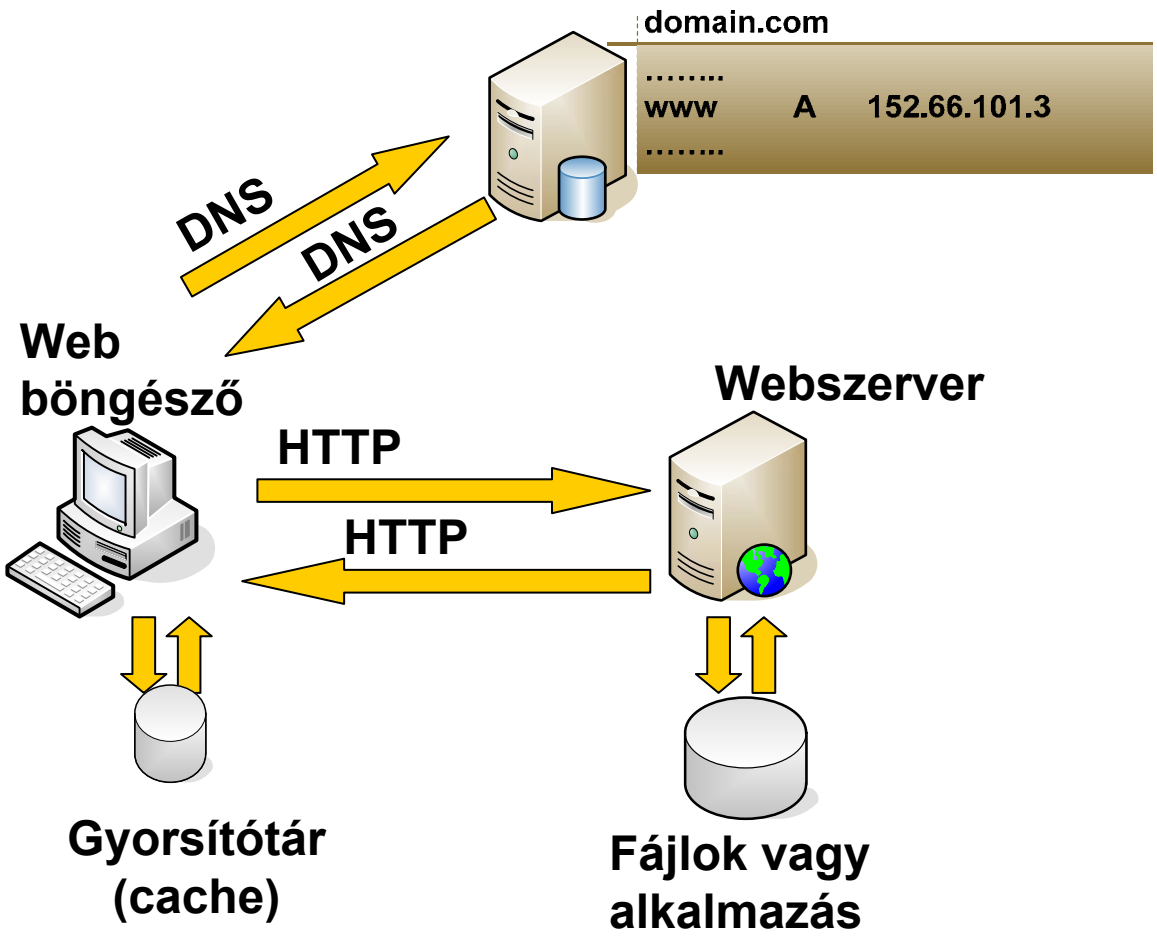
Példa egy SMTP kommunikációra

S: 220 lappfold.fi
C: HELO bme.hu
S: 250 Hello bme.hu, pleased to meet you
C: MAIL FROM: <jogyerek@bme.hu>
S: 250 jogyerek@bme.hu... Sender ok
C: RCPT TO: <mikulas@lappfold.fi>
S: 250 mikulas@lappfold.fi ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Kedves Mikulás!
C: Jó gyerek voltam. Hozzál sok csokit!
C: Köszönöm,
C: Jógyerek Jóska
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 lappfold.fi closing connection

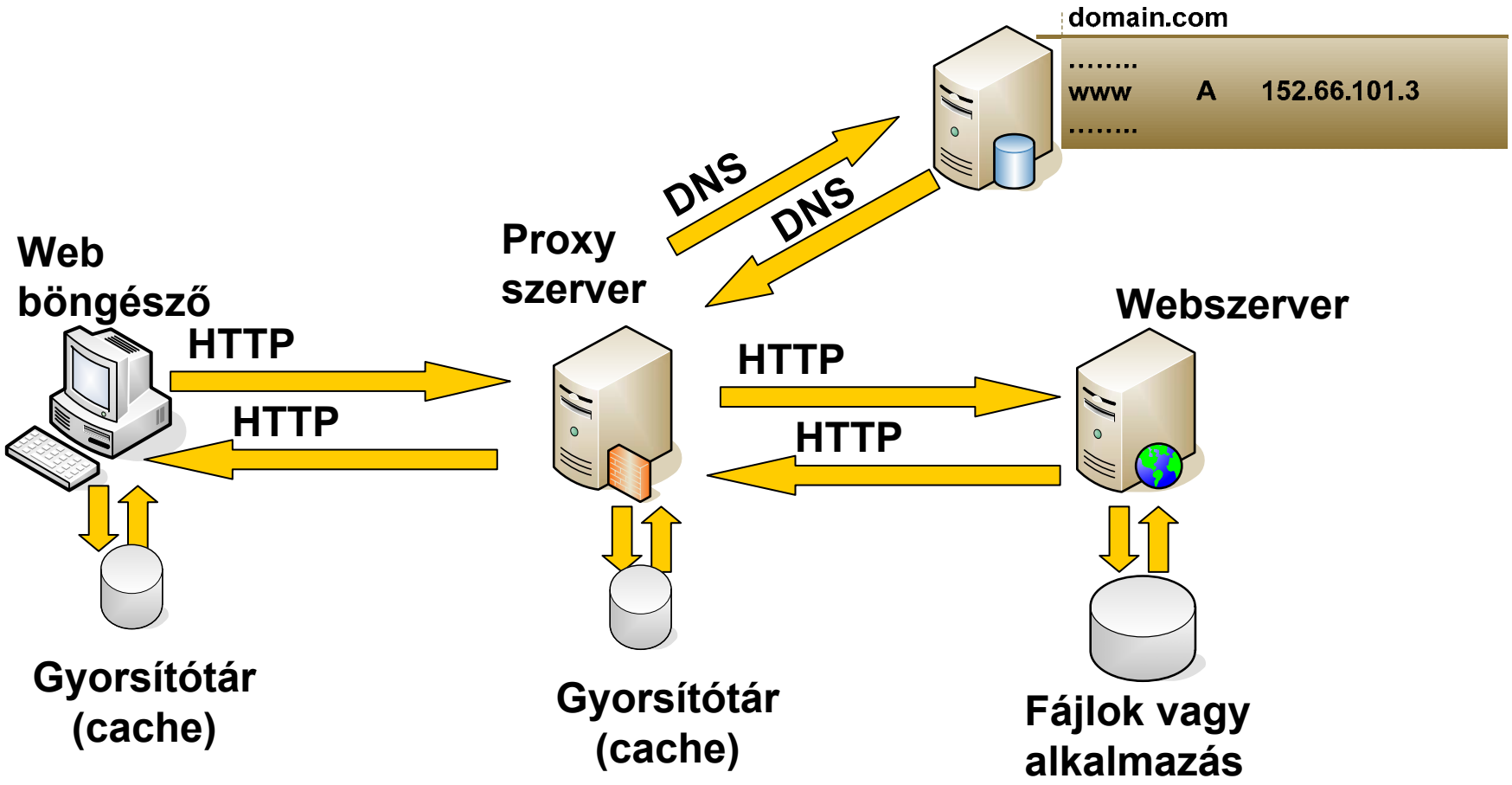
HTTP – HyperText Transfer Protocol

WEBES RENDSZEREK

Webes rendszerek



Webes rendszerek proxyval



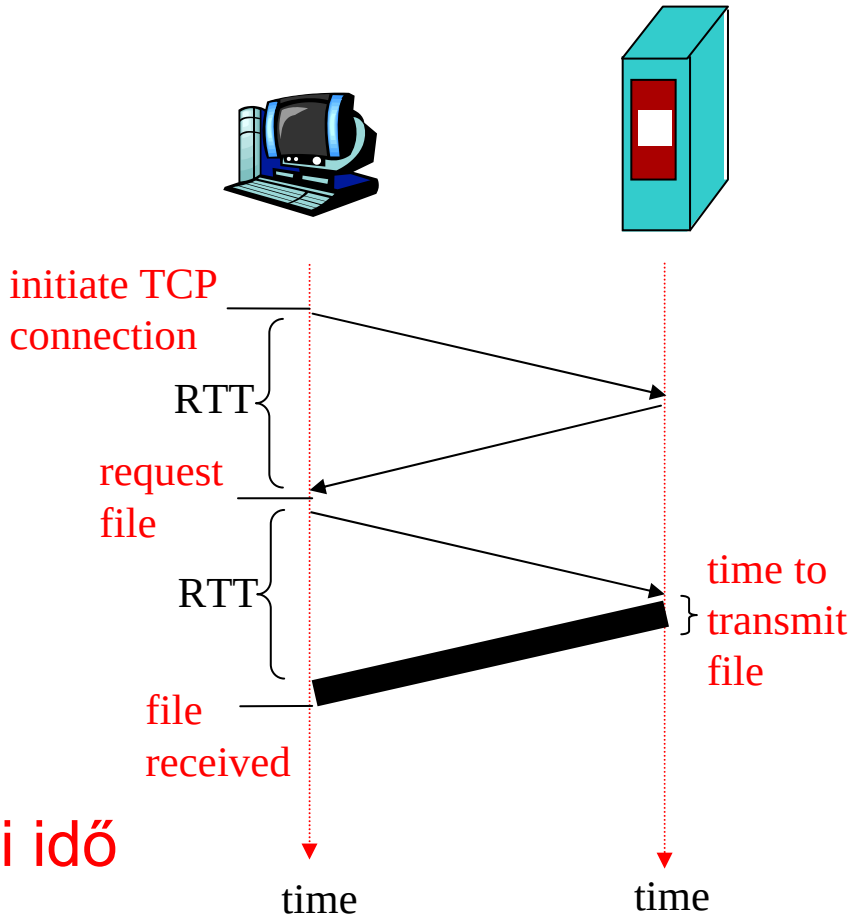
HTTP – HyperText Transfer Protocol

- RFC 2068
- Web
  - Tim Berners-Lee, CERN
  - a második „killer application”
- Parancsorientált állapotkódokkal
- Speciális fejlécek
- Állapotmentes protokoll
- TCP 80
- Proxy
  - Kliens nevében jár el
  - Főként a hatékony gyorsítótárazás miatt

Perzisztens HTTP

- *Nem-perzisztens*:
  - minden kérés/válasz pár egy **külön** TCP kapcsolaton keresztül
  - Legfeljebb egy objektumot visz át egy TCP kapcsolaton
  - HTTP/1.0
- *Perzisztens*:
  - **egy TCP kapcsolaton belül** több kérés/válasz pár
  - Alapbeállítás HTTP1.1-nél

Késleltetés nem perzisztens kapcsolatnál



Teljes késleltetés = 2RTT+adási idő

Perzisztens HTTP

Nonperzisztens HTTP:

- 2 RTT/objektum
- + TCP kapcsolat overhead
- Böngészők használhatnak **párhuzamos TCP kapcsolatokat** a különböző objektumok letöltésére

Persiztensz HTTP

- Server **nyitva hagyja a kapcsolatot** a válasz elküldése után
- HTTP üzenetek sorozata ugyanazon kliens és szerver között **egy kapcsolaton belül**

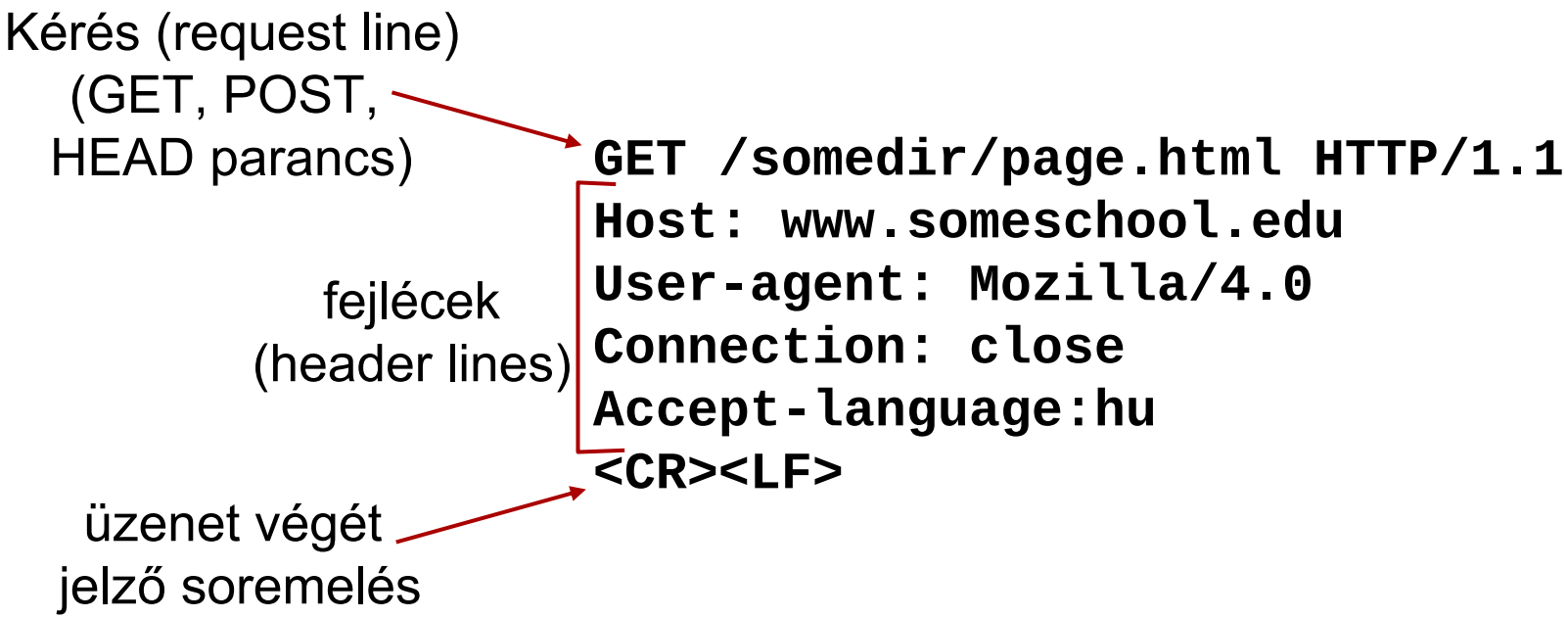
Perzisztens pipelining nélkül:

- Kliens csak akkor küld új kérést, ha előzőre **megjött a válasz**
- Egy RTT/objektum

Perzisztens + pipelining:

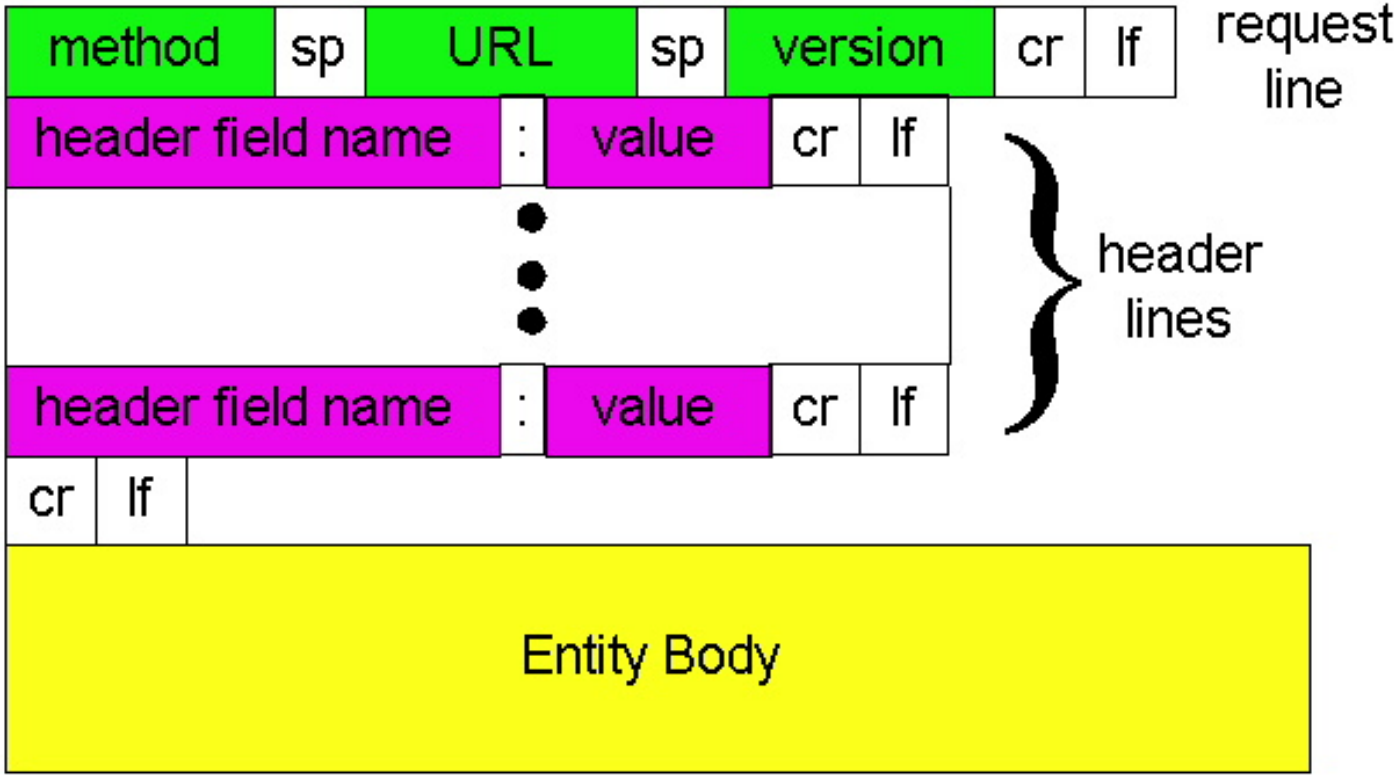
- Alapbeállítás HTTP/1.1-nél
- Kliens elküldhet több kérést is egymás után **anélkül, hogy megvárná a választ**
- Egy RTT minden objektumra

Példa egy HTTP kérésre



© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Általános HTTP kérés üzenet formátum



Entity Body: POST-nál van értelme!

Gyakori HTTP parancsok

- GET <URL> HTTP/1.1
  - adott URL tartalmának lekérése
- HEAD
  - mint a GET, de csak a metaadatokat adja vissza
- POST
  - a kliens ezzel tud adatokat küldeni a szervernek
- PUT
  - a POST-hoz hasonló, fájlfeltöltésre alkalmas
- DELETE
  - adott URL tartalmának törlése

Gyakori HTTP fejlécek

- Accept: elfogadható MIME típus
- Accept-Charset: elfogadható karakterkészlet
- Allow: szerver által támogatott parancsok
- Authorization: támogatott hitelesítési módok
- Content-Encoding: tömörítés típusa
- Content-Length: tartalom mérete
- Content-Type: MIME típus
- Date: lekérés dátuma és ideje
- From: a látogató e-mail címe (nem authentikációra)
- Pragma: nem meghatározott paraméter (pl. „no-cache”)
- Referer: a hivatkozó oldal URL-je
- Retry-After: 503 utáni újrapróbálkozási idő
- Server: szerver neve és verziója
- User-Agent: böngésző neve és verziója
- WWW-Authenticate: Hitelesítési információk (credentials)

© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Példa egy HTTP válaszüzenetre

állapotkód

fejlécek

adat (pl. a kért HTML fájl)

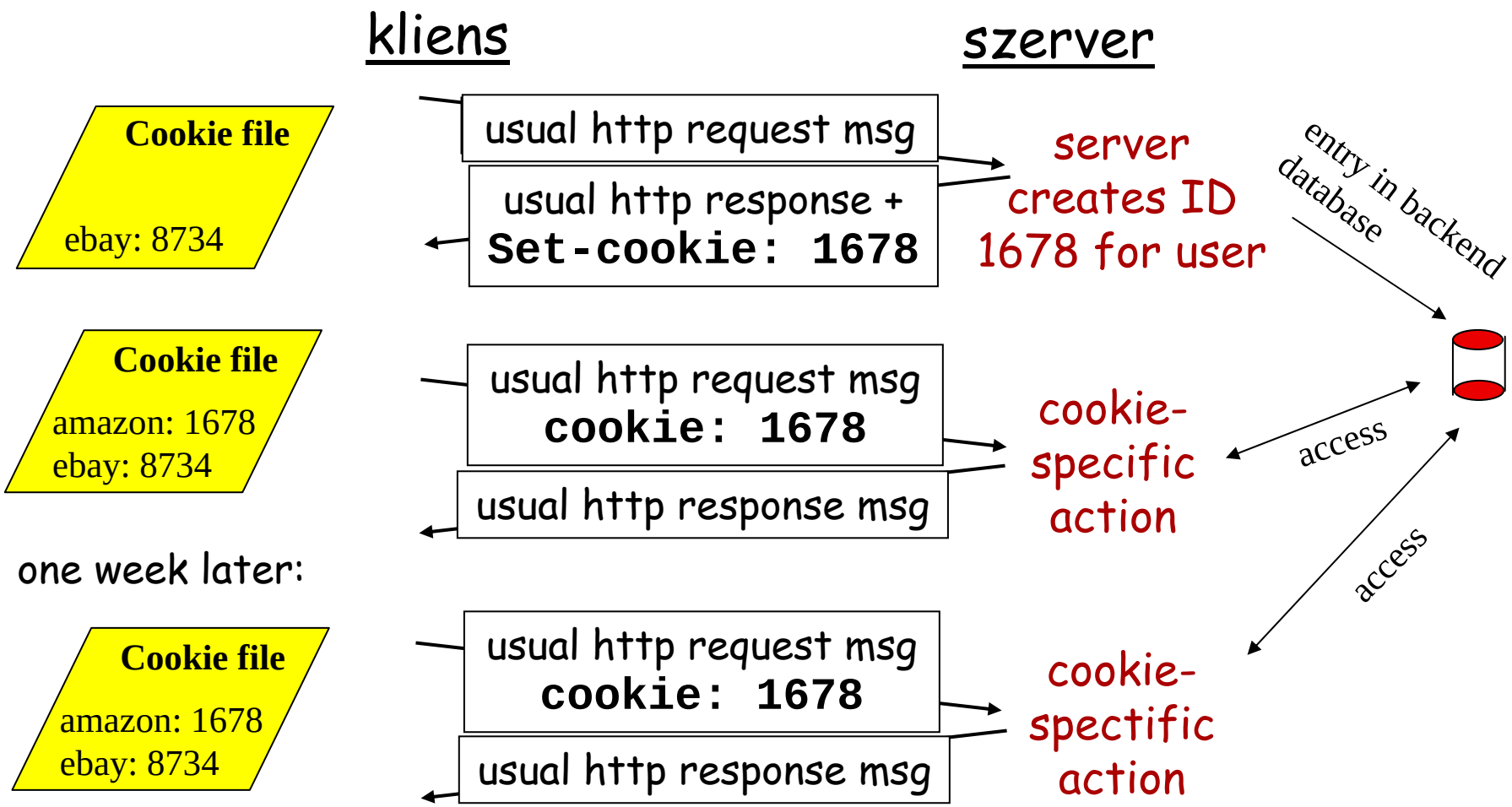
```
HTTP/1.1 200 OK
Connection close
Date: Thu, 14 May 2013 12:00:15 GMT
Server: Apache/1.3.0 (Unix)
Last-Modified: Mon, 22 Jun 2012 …...
Content-Length: 6821
Content-Type: text/html

data data data data data ...
```


© Dr. Simon Vilmos, Hálózati Rendszerek és Szolgáltatások Tanszék

Gyakori HTTP állapotkódok

Kód	Jelentés	Leírás
200	OK	
201	Created	POST sikeres
202	Accepted	Kérés elfogadva
204	No content	Nincs semmi a kliensnek
400	Bad request	Hibás kérés
401	Unauthorized	Hitelesítés szükséges
403	Forbidden	Hozzáférés megtagadva
404	Not found	Nem található
500	Internal Server Error	Belső szerver hiba
503	Service Unavailable	Pillanatnyilag nem szolgálható ki

Cookie-k használata



HTTP jövője

- Következő verzió: HTTP 2.0, IETF fejlesztésben
- A Google SPDY protokolljának lényeges elemeit használja
  - De facto szabvány?
- Csökkenti a web oldalak betöltési idejét:
  - multiplexált stream-ek egy TCP kapcsolaton belül
  - kérések priorizálása
  - kérés és válasz fejtészek tömörítése
    - a statikusok nincsenek újraküldve
  - szerver push és hint funkció

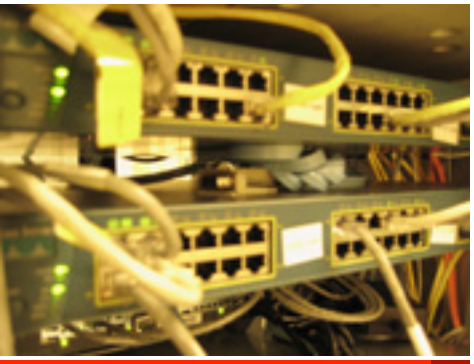
Összefoglalás

- Alkalmazások hálózati kapcsolata
  - Portok és socketek használata
- Infrastrukturális szolgáltatások
  - DNS – Névfeloldási szolgáltatás
  - DHCP
- Szöveg- és fájlátvitel
  - Telnet, FTP
- Levelezési rendszerek
  - SMTP, POP3, IMAP4
- Webes rendszerek
  - HTTP

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos
BME Hálózati Rendszerek és Szolgáltatások Tanszék
svilmos@hit.bme.hu



Introduction

Security

Mark Felegyhazi
assistant professor
CrySyS Lab.

BME Department of Telecommunications
(Híradástechnikai Tanszék)
mfelegyhazi(atat)crysys(dot)hu

First look – quick overview

- What is security?
- Prevent or detect/block?
- Security techniques
  - crypto
  - protocols
- Why do we care about economics here?
  - How much is enough to invest in defense?
  - We work together, or not?
- Who is responsible?

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

- Concepts and definitions
- Attacks
- Cryptography
- Security defense mechanisms
- Security economics

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

biztonság

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

biztonság

safety

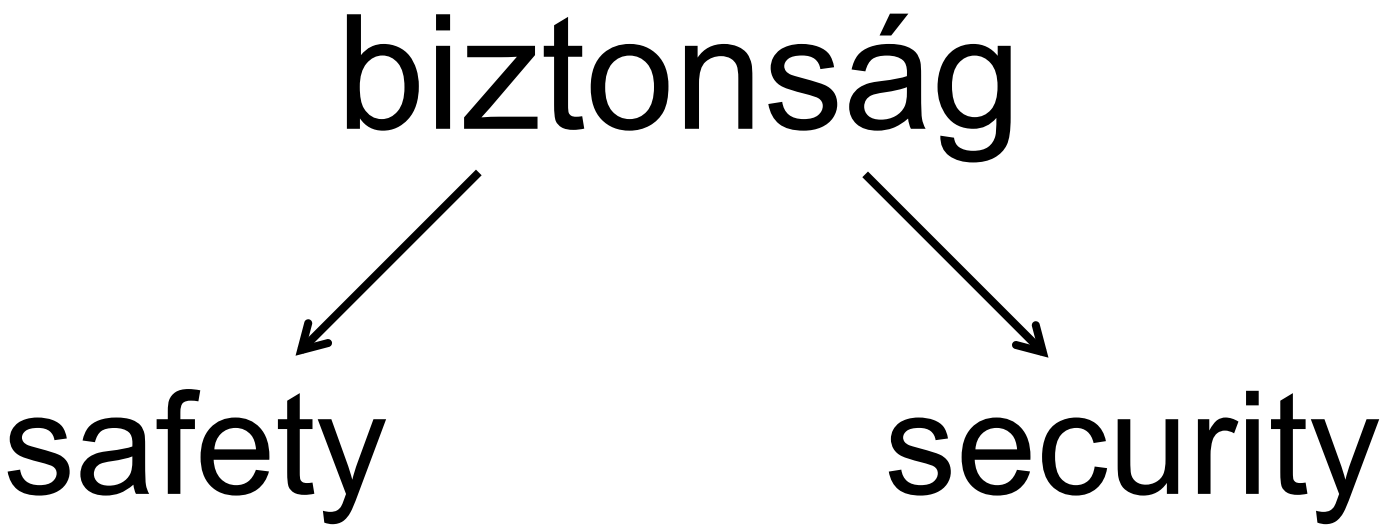
the condition of being protected against the consequences of failure, damage, error, accidents, harm or any other event, which could be considered non-desirable

security

the **process** of delaying, preventing, and otherwise protecting against external or internal defects, dangers, loss, criminals, and other individuals or actions that threaten the steady state of a system

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

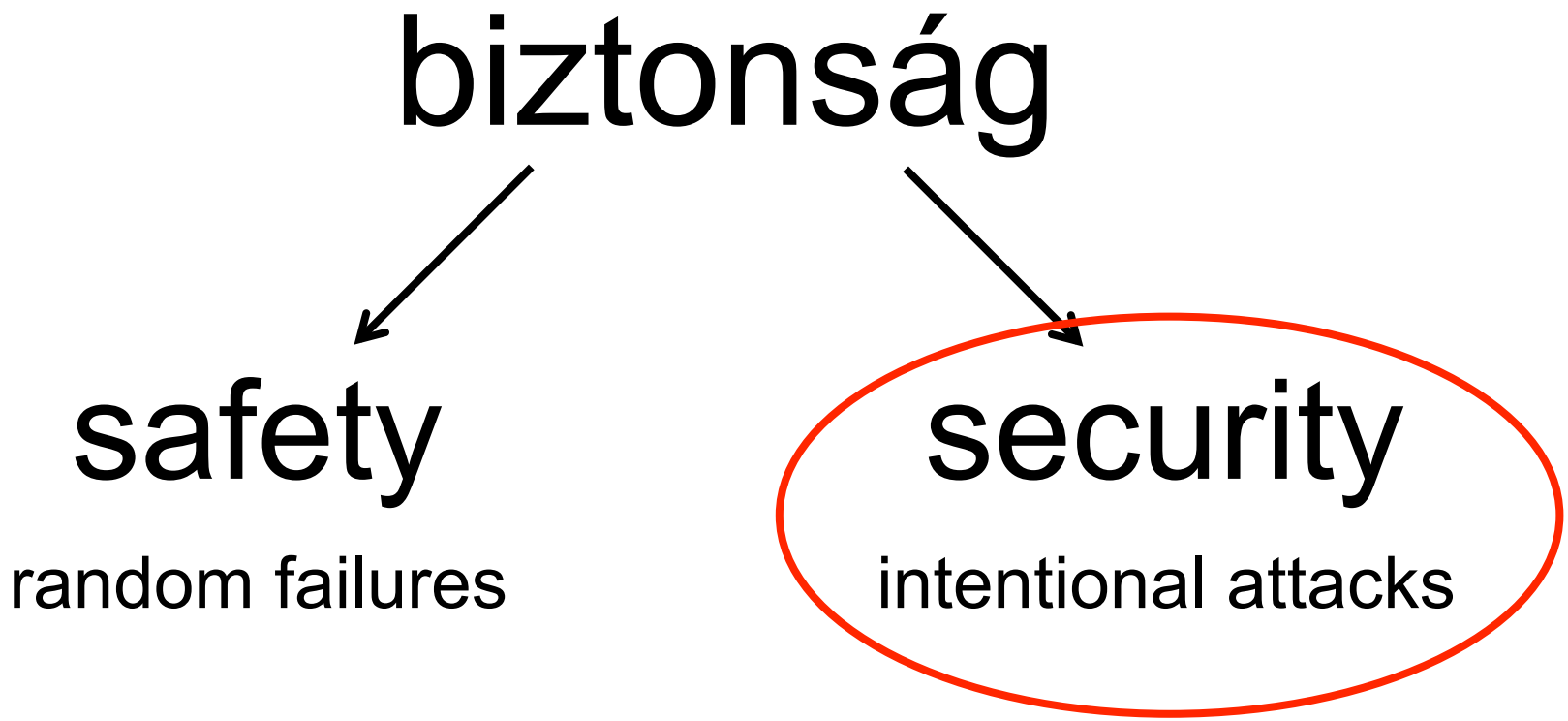
Concepts



achieve an acceptable level of risk

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

megbízhatóság

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

megbízható

reliable

able to perform and maintain its functions in routine, as well as in unexpected circumstances

trustworthy

does what people expect it to do – and not something else – despite environmental disruption, human user and operator errors, and attacks by hostile parties

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Concepts

megbízható

reliable

random failures

trustworthy

+ intentional attacks

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

adatbiztonság

vs.

adatvédelem

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Concepts

adatbiztonság

↓

data **security**

the practice of **protecting** information from unauthorized access, use, disclosure, disruption, modification, or destruction

adatvédelem

↓

data **privacy**

the ability to **control** what information one reveals about oneself, and who can access that information

control can be preserved by protection against disclosure

↓

data security mechanisms can be used to achieve data privacy

but, in general, privacy is a broader (social) concept

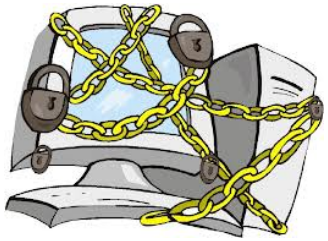
© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Concepts

information security?

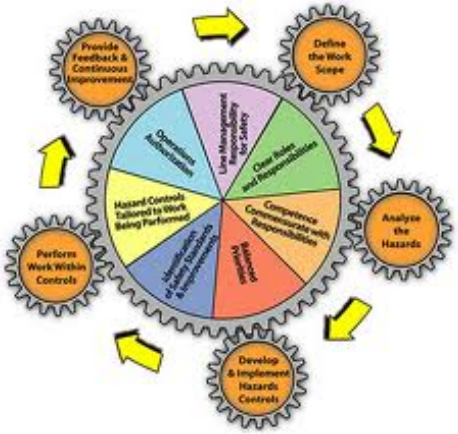
© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

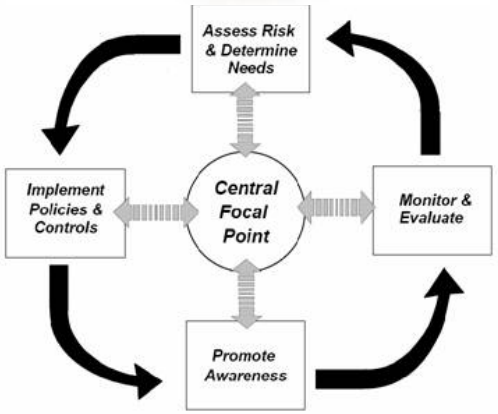
... is about protecting data (transmitted and stored)



... is protecting data processing systems (computers and networks)

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME





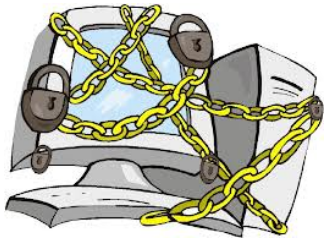
... is a process (aiming at reducing risk)

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

= cryptography

κρυπτός = "hidden, secret";
γράφειν = "writing"

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME



= computer and network security

user authentication (e.g., passwords)
protection against malware (e.g., virus scanners)
vulnerablity detection and patching
network perimeter defense (e.g., firewalls)
network intrusion detection systems (IDS)
DoS resistance
...

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Security

- Merriam-Webster, [4b, (1)]:
  - measures taken to guard against espionage or sabotage, crime, attack, or escape
- Dictionary.com, [1]:
  - freedom from danger, risk, etc.; safety
- Wikipedia.com:
  - **Security** is the degree of protection against danger, damage, loss, and crime.
  - **Information security** means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
  - **Communications security** is the discipline of preventing unauthorized interceptors from accessing telecommunications in an intelligible form, while still delivering content to the intended recipients.
  - **Computer security** can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Our definition

- **security**: prevention or detection of an attack on the computer system
  - attack: deliberate attempt to compromise the intended use of a computer system

- a few important points
  - attacker: a malicious entity whose aim is to prevent the users of the computing system from achieving their goal (primarily privacy, integrity, and availability of data)
  - **security vs. safety**
- Why economics of computer security?
  - strategic adversary: rational, profit-seeking
  - in general: see “Security Protocols” course from Prof. Levente Buttyan (Hírközlõ rendszerek biztonsága szakirány)

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Secure protocols

- in a very general sense, secure protocols are distributed algorithms – involving message passing between participants – that try to reach a certain goal, even in the presence of attackers
- examples:
  - secure communication protocols (for wired and wireless networks)
  - secure key exchange protocols
  - secure routing protocols
  - secure neighbor discovery protocols (in wireless networks)
  - …
- security of a protocol is always evaluated w.r.t. an attacker model
- different types of protocols call for different attacker models

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

More definitions

- vulnerability
  - attacks usually exploit vulnerabilities
  - a vulnerability is a flaw or weakness in the system's design, implementation, or operation and management
  - most systems have vulnerabilities, but not every vulnerability is exploited
  - whether a vulnerability is likely to be exploited depends on the difficulty of the attack and the perceived benefit of the attacker

- threat
  - a possible way to exploit vulnerabilities
  - a potential attack

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

More on attacks

- passive attack
  - requires no intervention into the operation of the system
  - typically consists in the passive acquisition of some information that should not be available to the attacker
  - typical examples:
    - eavesdropping message contents
    - traffic analysis
      - gaining knowledge of data by observing the characteristics of communications that carry the data
      - even if message content is encrypted, an attacker can still
        - » determine the identity and the location of the communicating parties
        - » observe the frequency and length of the messages being exchanged
        - » guess the nature of the communication
  - difficult to detect, should be prevented

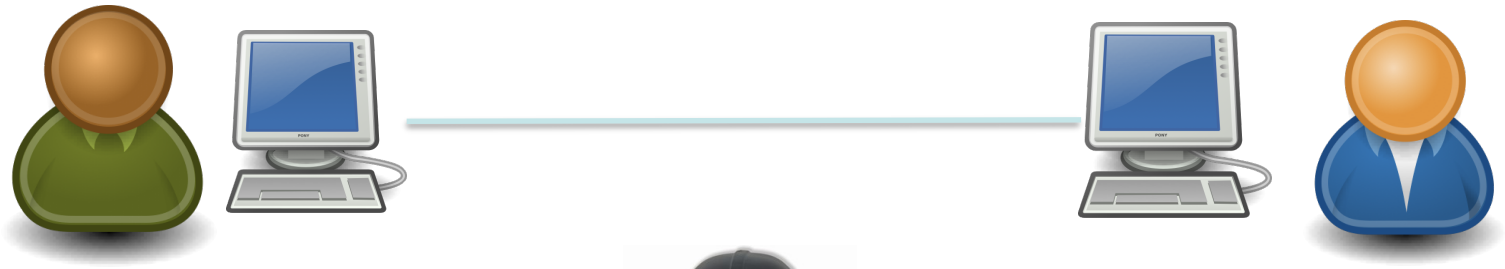
© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

More on attacks

- active attack
  - requires an active intervention into the operation of the system
  - typical examples:
    - masquerade (spoofing)
      - an entity pretends to be a different entity
    - replay
      - capture and subsequent retransmission of data
    - modification (substitution, insertion, destruction)
      - (some parts of the) legitimate messages are altered or deleted, or fake messages are generated
      - if done in real time, then it needs a “man in the middle”
    - denial of service
      - normal use or management of the system is prevented or inhibited
      - e.g., a server is flooded by fake requests so that it cannot reply normal requests
  - difficult to prevent, should be detected

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Communication security – a simple view



Alice

Malice

Bob

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

(Bob is not) living next door to Alice

- the motivation, operation, and analysis of security protocols are often presented as tales about two strange characters, Alice and Bob, and their “friends”
- Alice and Bob
  - they live far from each other and communicate only via Internet, e-mail, or telephone
  - they have actually never met, but for some reason, they frequently need to conduct all sorts of business with each other
  - they rarely trust anyone else, sometimes not even each other
  - their history of interactions include exchanging secret e-mails, playing poker over the phone, using electronic coins to buy digital content from each other, remotely signing contracts, running auctions and elections over the Internet, …

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Friends

- Carol / Carlos / Charlie is a third participant in communications
- **Eve** is an eavesdropper (a passive attacker)
- Gordon is a government agent
- Isaac is an Internet Service Provider (ISP)
- Justin / Julian is from the justice system
- **Mallory** is a malicious attacker; unlike Eve, Mallory can modify messages, substitute her own messages, replay old messages, and so on (active attacker)
- Oscar is an opponent, usually taken as equivalent to Mallory
- Pat / Peggy is a prover and Victor is a verifier; in their interactions, Peggy always tries to convince Victor that she knows some information without actually revealing that information (zero-knowledge protocols)
- Trent is a trusted arbitrator, some kind of neutral third party, whose exact role varies with the protocol under discussion
- Trudy, is an intruder; another alternative to Mallory
- Zoe, often the last party to be involved in a cryptographic protocol

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Communication security services

CIA principles

- confidentiality
  - protection of information from unauthorized disclosure
  - information can be
    - content of communications → (content) confidentiality
    - meta-information (derived from observation of traffic flows) → traffic flow confidentiality
- integrity protection
  - aims to detect message modification and replay
  - provides assurance that data received are exactly as sent by the sender
    - in case of a stream of messages (connection oriented model), integrity means that messages are received as sent, with no duplication, modification, insertion, deletion, reordering, or replays
- availability
  - the service is reachable for the users

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Communication security services

- authentication
  - aims to detect masquerade (spoofing)
  - provides assurance that a communicating entity is the one that it claims to be
    - peer entity authentication
    - data/message origin authentication
- non-repudiation
  - provides protection against denial by one entity involved in a communication of having participated in all or part of the communication
    - non-repudiation of message origin
    - non-repudiation of message delivery

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Placement of security services

- some services can more naturally be implemented at the application layer (e.g., non-repudiation)
- some services better fit in the link layer (e.g., traffic flow confidentiality)
- but many services can be provided at any layer (e.g., authentication, confidentiality, integrity)
  - lower layer (e.g., link-by-link encryption):
    - services are generic, can be used by many applications
    - protection mechanisms are transparent to the user
  - higher layer (e.g., end-to-end authentication):
    - services are more application specific
    - more user awareness

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Attacks

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Examples of attacks

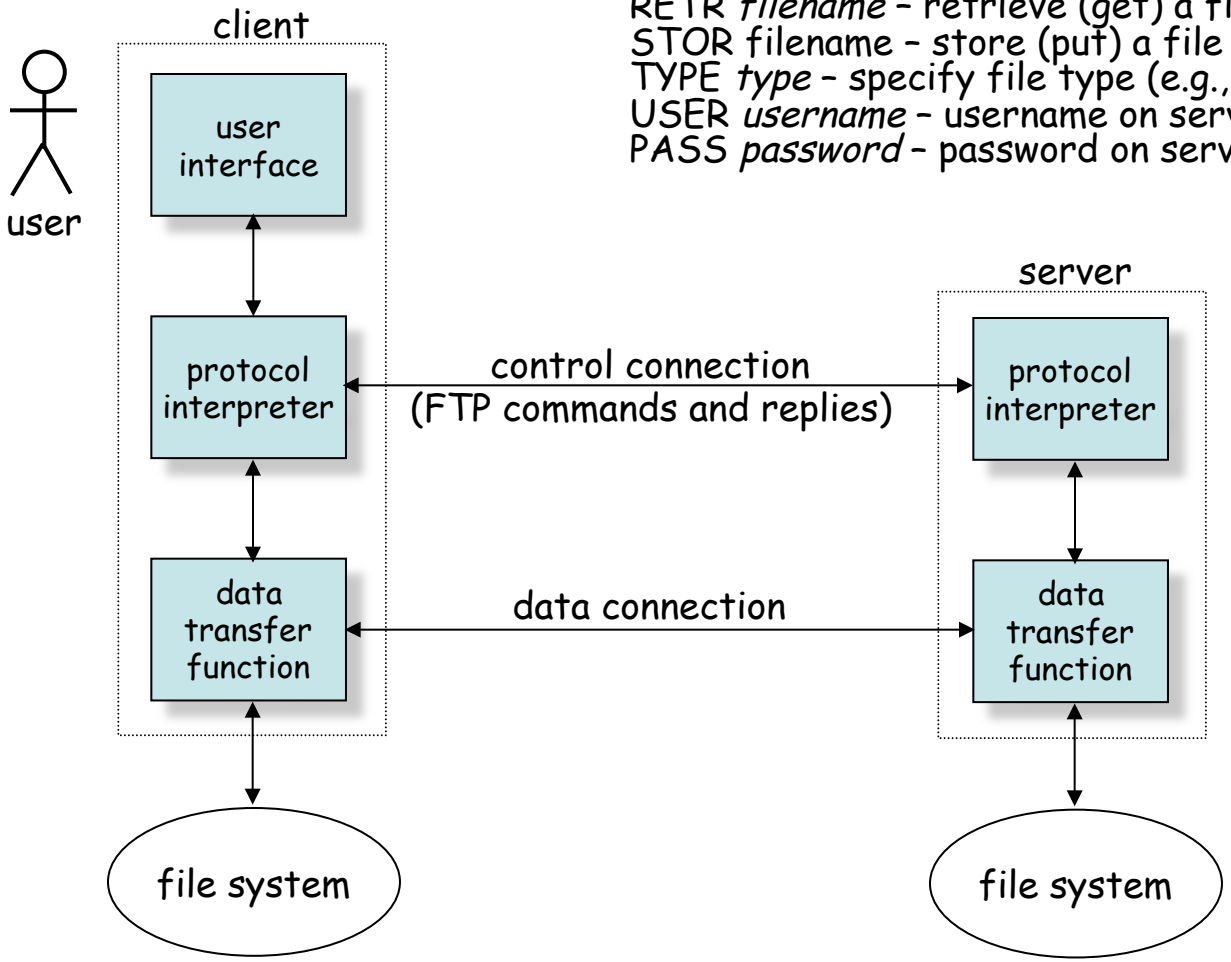
- password sniffing in FTP
- password sniffing in TELNET
- mail forging with SMTP
- ARP spoofing
- DoS against a web server
- spam

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

FTP – File Transfer Protocol

typical FTP commands:

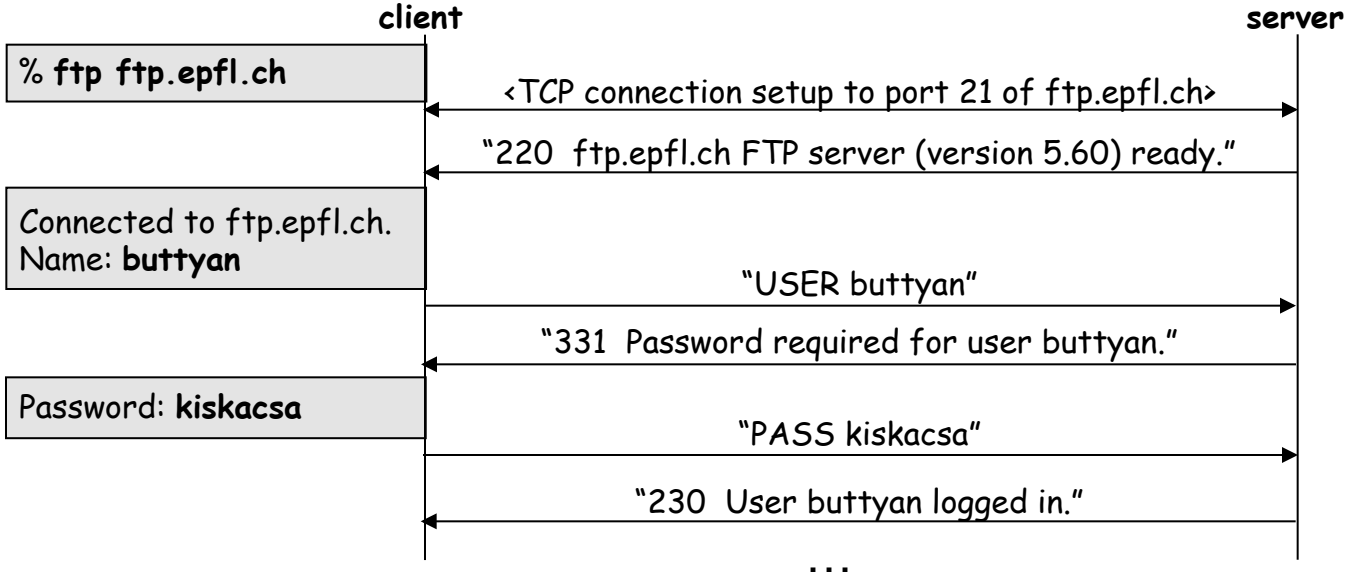
RETR *filename* – retrieve (get) a file from the server
STOR filename – store (put) a file on the server
TYPE *type* – specify file type (e.g., A for ASCII)
USER *username* – username on server
PASS *password* – password on server



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

FTP security problems

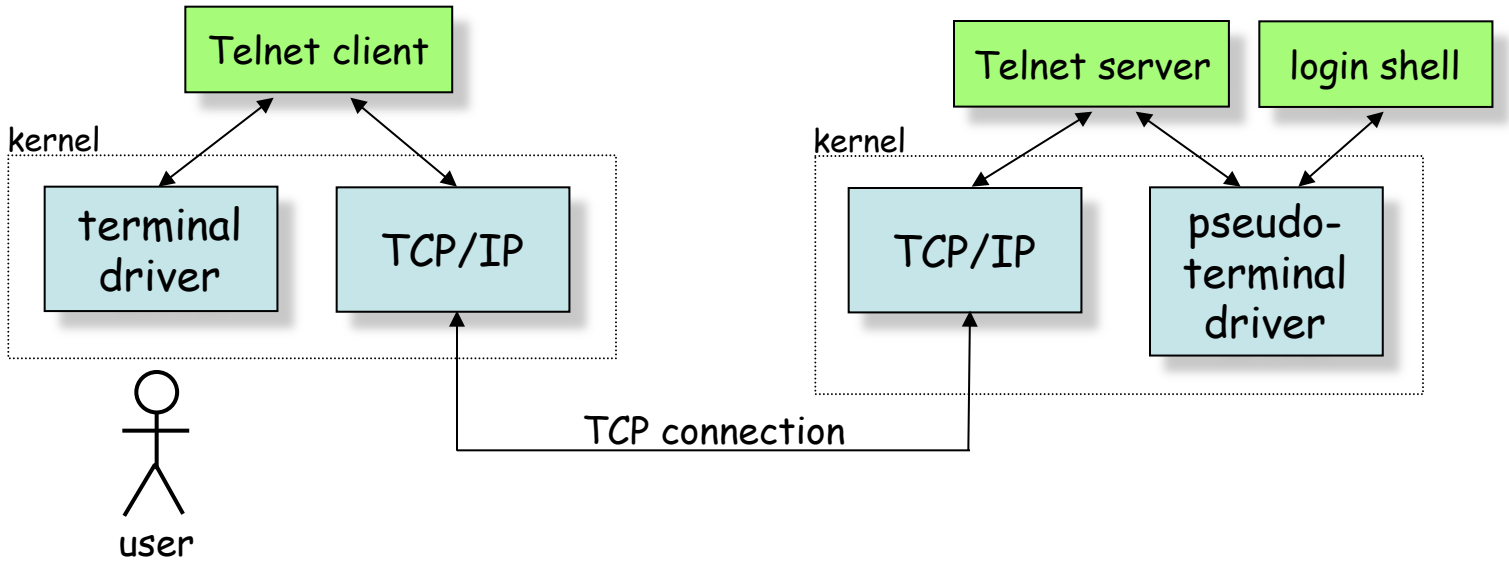
- neither the control nor the data connection is protected
  - passwords can be eavesdropped
    - FTP is a text(ASCII) based protocol, which makes password sniffing even easier
  - files transmitted over the data connection can be intercepted and modified



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Telnet

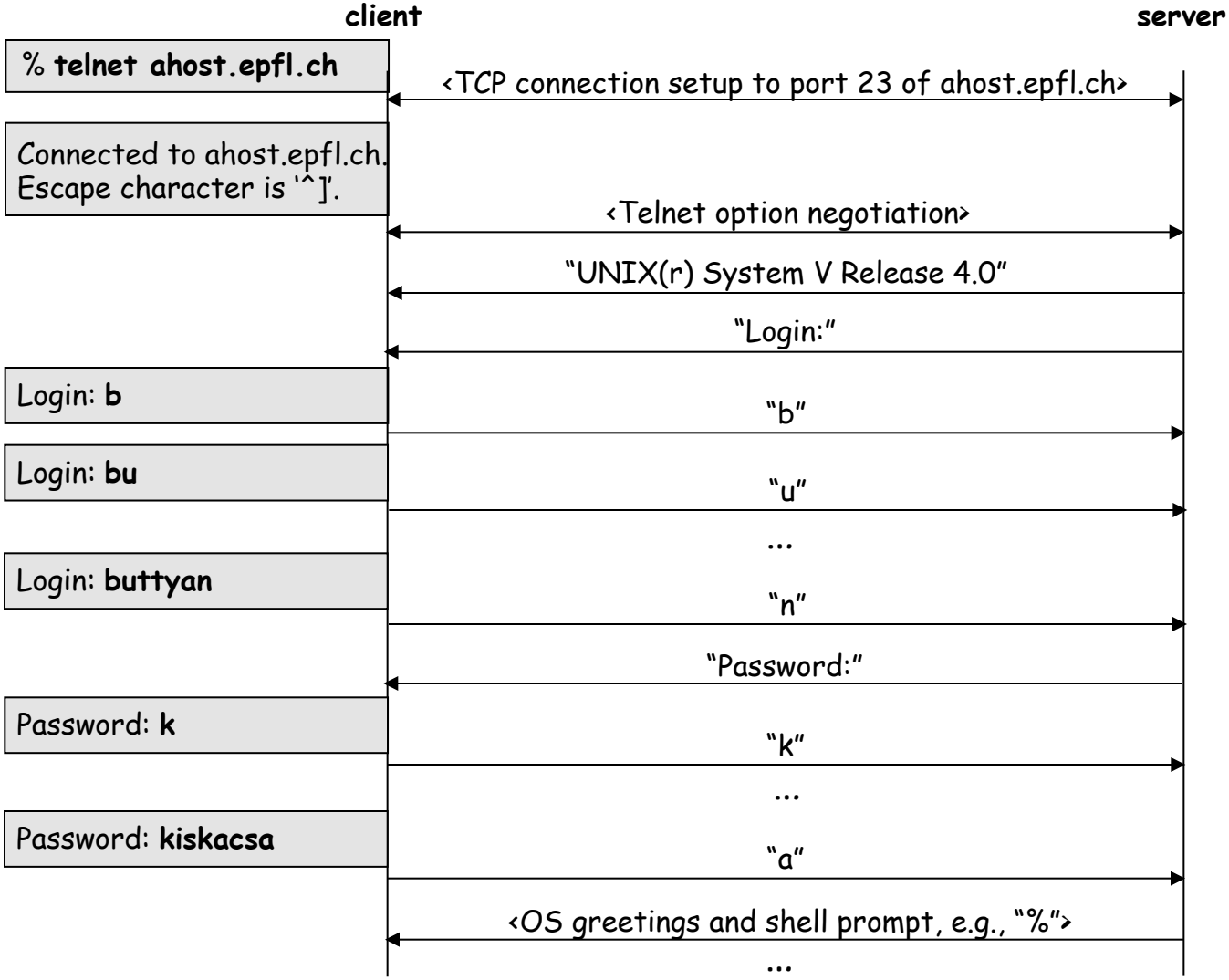
- provides *remote login* service to users
- text (ASCII) based protocol



© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

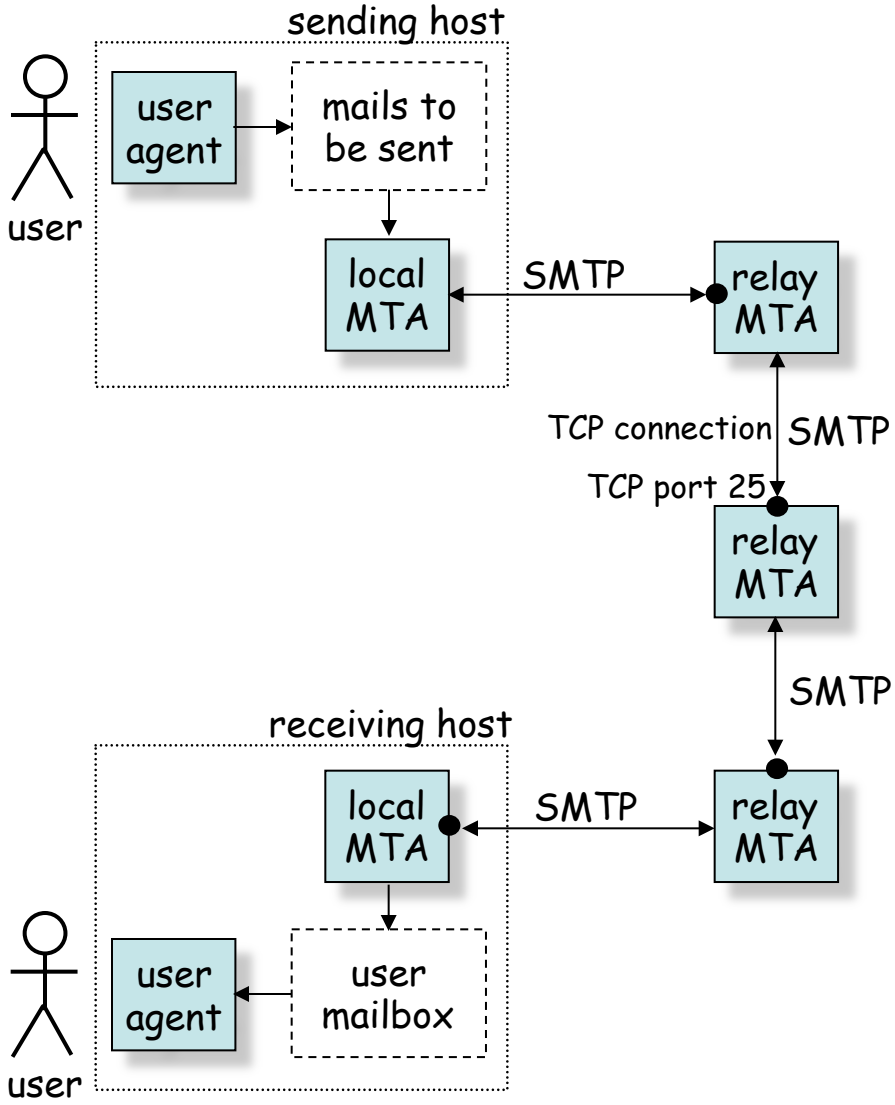
Telnet security problems

- passwords are sent in clear



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

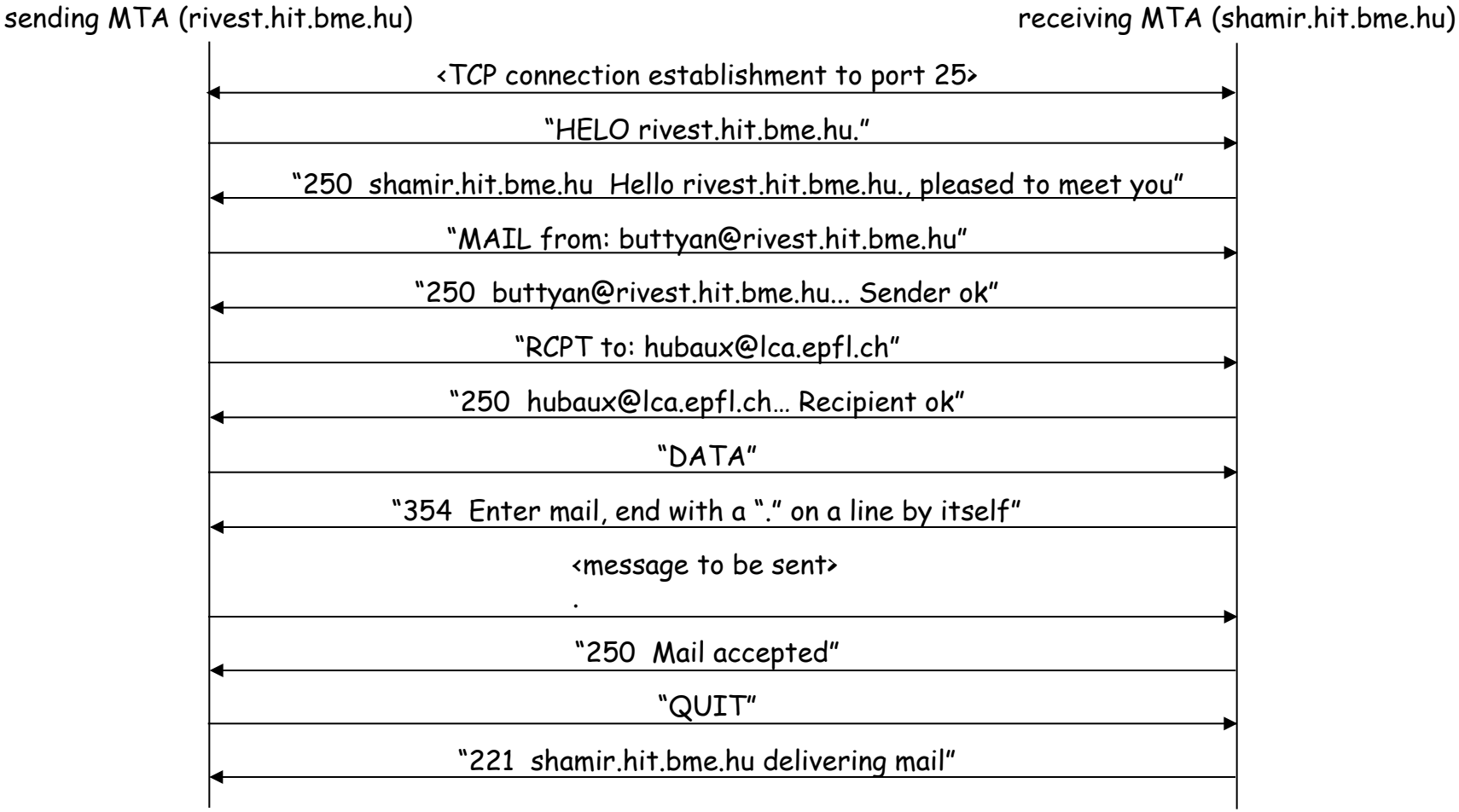
SMTP – Simple Mail Transfer Protocol



© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

SMTP cont'd

- SMTP is used by MTAs to talk to each other
- SMTP is a text (ASCII) based protocol



© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

SMTP security problems

- SMTP does not provide any protection of e-mail messages
  - messages can be read and modified by any of the MTAs involved
  - fake messages can easily be generated (e-mail forgery)
- Example:

```
% telnet frogstar.hit.bme.hu 25
Trying...
Connected to frogstar.hit.bme.hu.
Escape character is '^['.
220 frogstar.hit.bme.hu ESMTP Sendmail 8.11.6/8.11.6;
Mon, 10 Feb 2003 14:23:21 +0100
helo abcd.bme.hu
250 frogstar.hit.bme.hu Hello [152.66.249.32], pleased to meet you
mail from: bill.gates@microsoft.com
250 2.1.0 bill.gates@microsoft.com... Sender ok
rcpt to: buttyan@ebizlab.hit.bme.hu
250 2.1.5 buttyan@ebizlab.hit.bme.hu... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Your fake message goes here.
.
250 2.0.0 h1ADO5e21330 Message accepted for delivery
quit
221 frogstar.hit.bme.hu closing connection
Connection closed by foreign host.
%
```


© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Be careful, though!

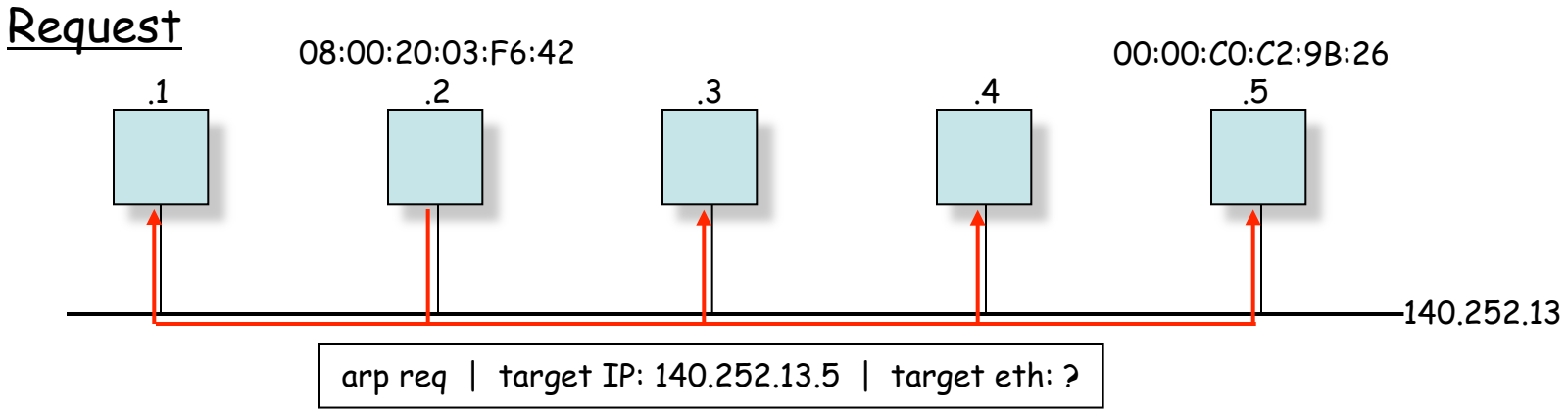
Return-Path: <bill.gates@microsoft.com>
Received: from frogstar.hit.bme.hu (root@frogstar.hit.bme.hu [152.66.248.44])
by shamir.ebizlab.hit.bme.hu (8.12.7/8.12.7/Debian-2)
with ESMTP id h1ADSsxG022719
for <buttyan@ebizlab.hit.bme.hu>; Mon, 10 Feb 2003 14:28:54 +0100
Received: from abcd.bme.hu ([152.66.249.32])
by frogstar.hit.bme.hu (8.11.6/8.11.6) with SMTP id h1ADO5e21330
for buttyan@ebizlab.hit.bme.hu; Mon, 10 Feb 2003 14:25:41 +0100
Date: Mon, 10 Feb 2003 14:25:41 +0100
From: bill.gates@microsoft.com
Message-Id: <200302101325.h1ADO5e21330@frogstar.hit.bme.hu>
To: undisclosed-recipients:;
X-Virus-Scanned: by amavis-dc
Status:

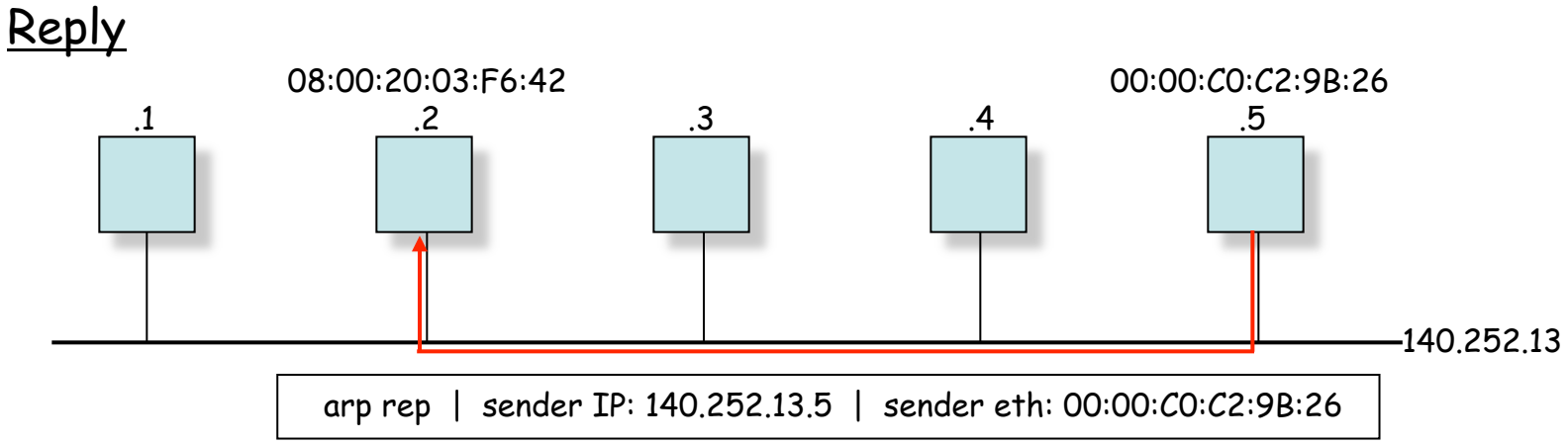
Your fake message goes here.

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

ARP

- mapping from IP addresses to MAC addresses

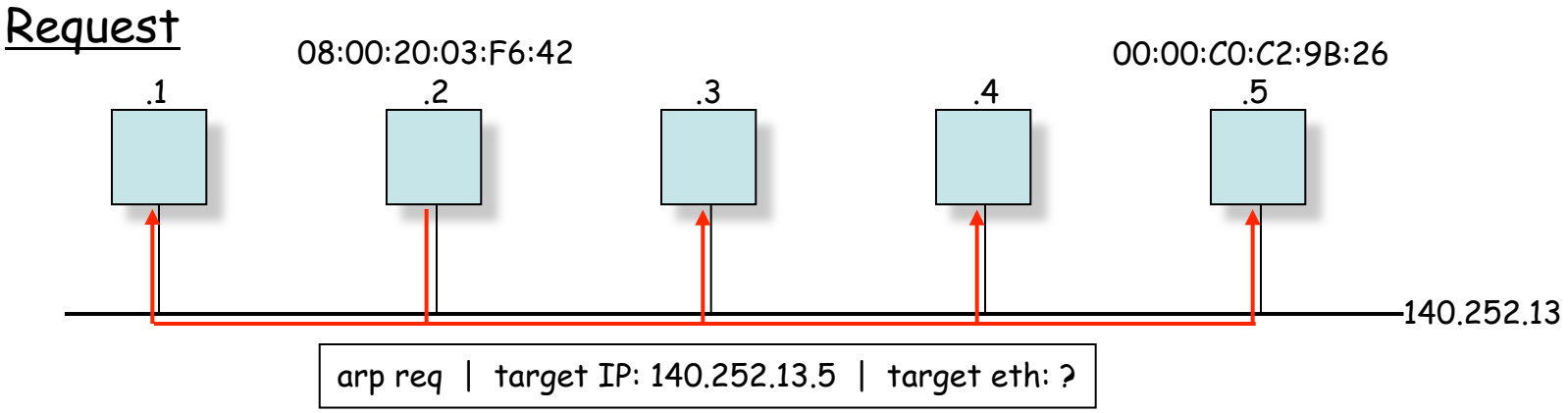


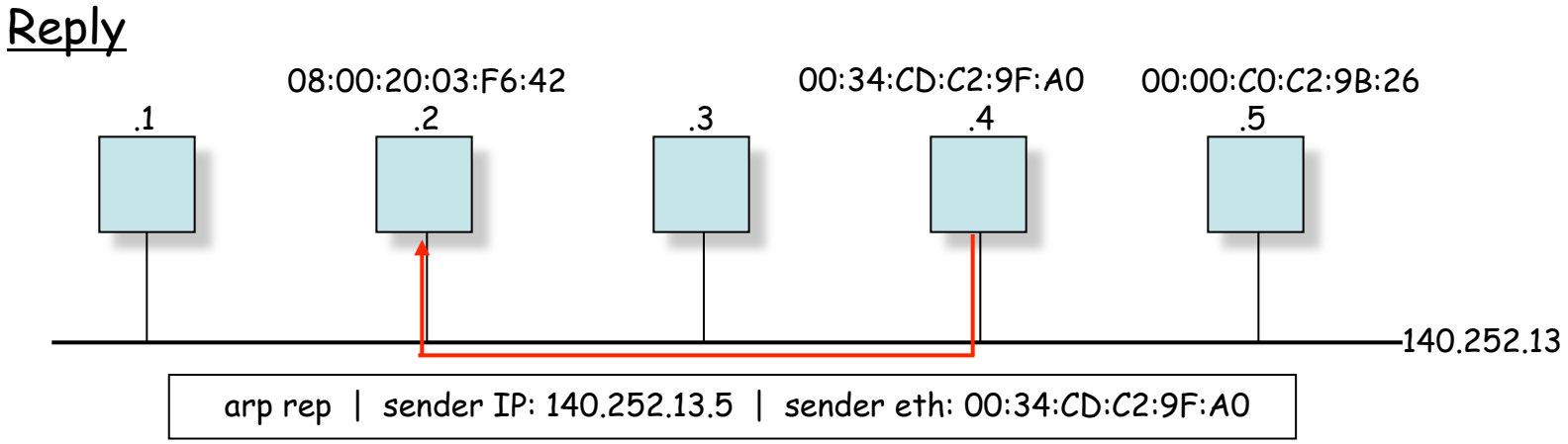


© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

ARP spoofing

- an ARP request can be responded by another host



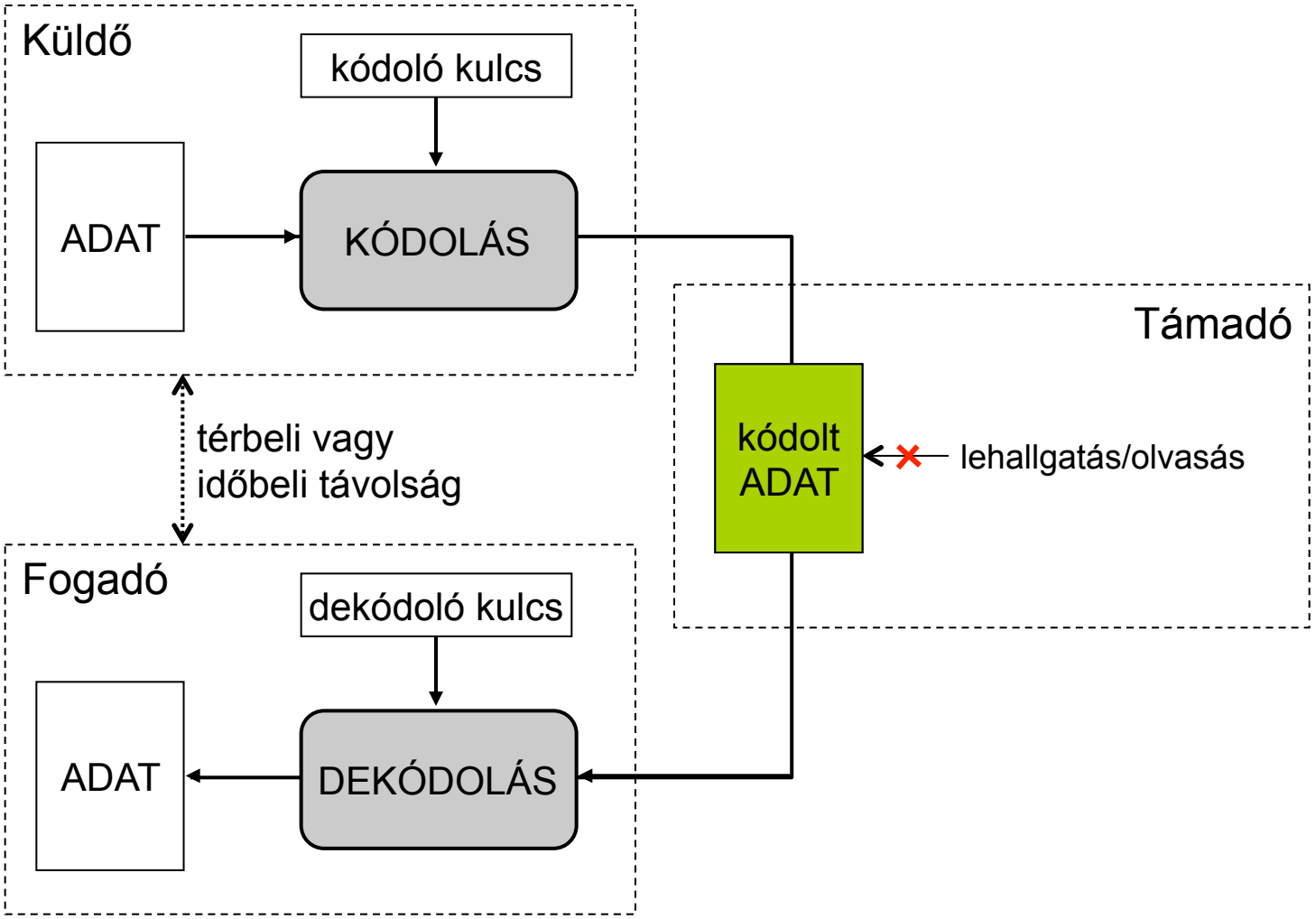


© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Crypto

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Encryption model



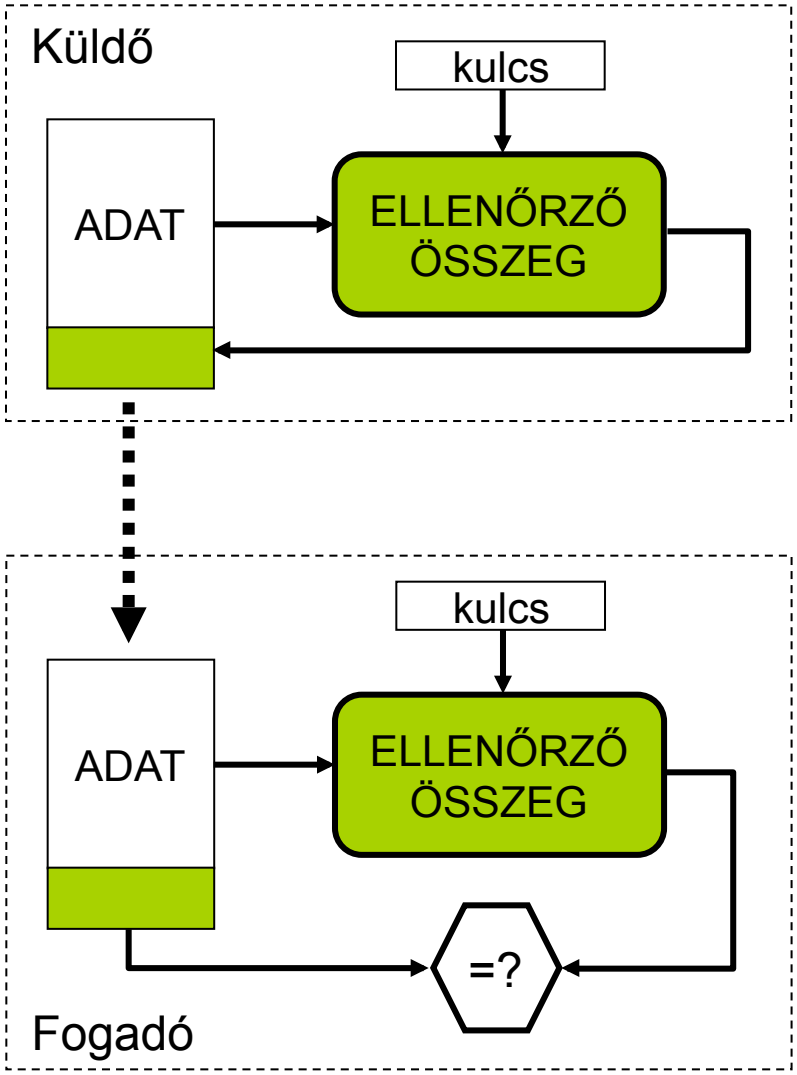
© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Algorithms for symmetric and asymmetric crypto

- symmetric key
  - DES
  - 3DES
  - AES
  - RC4
- asymmentric (public) key
  - RSA (factorization)
  - elliptic curve
- key agreement
  - Diffie-Hellman
  - PKI and CAs

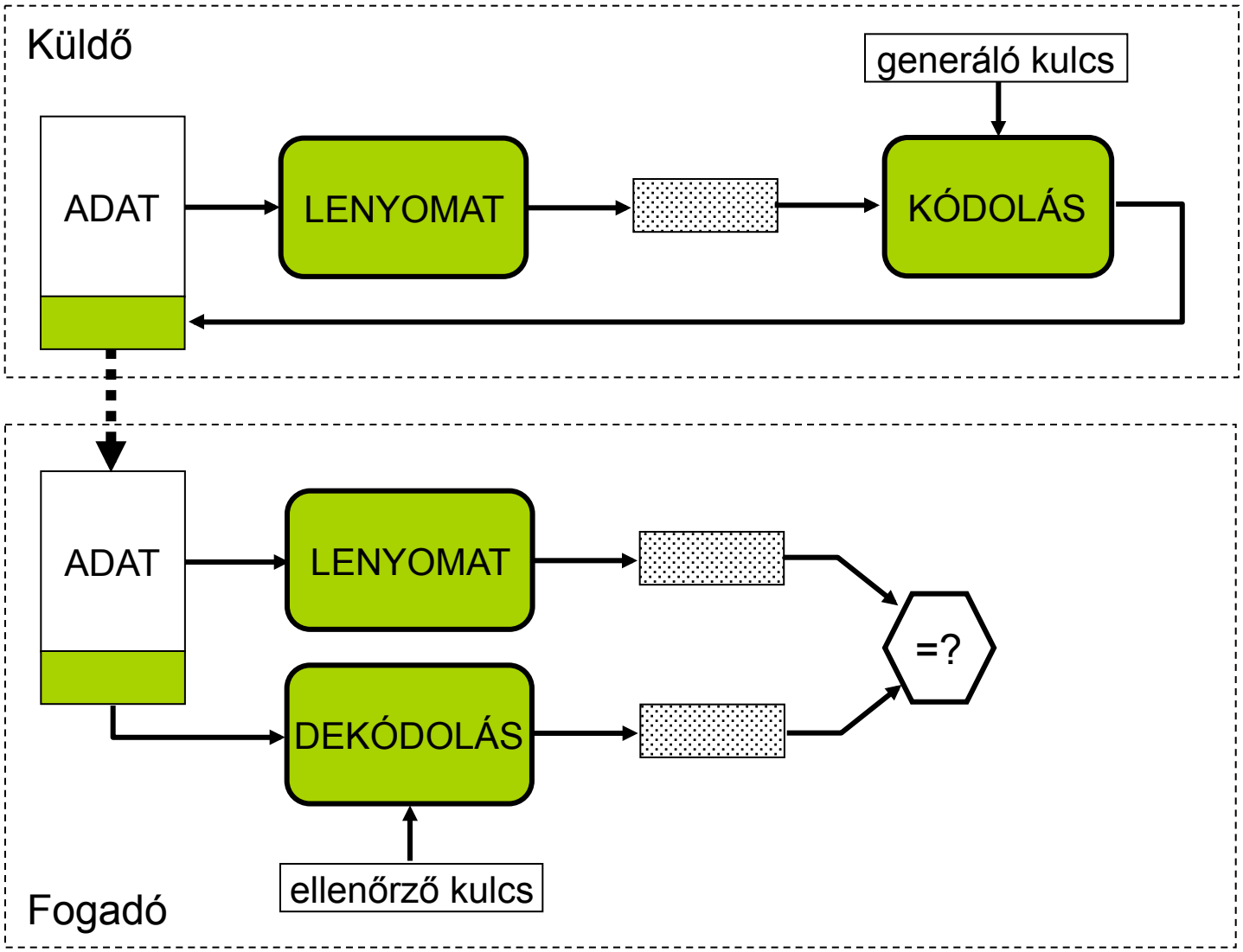
© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Authentication and integrity protection



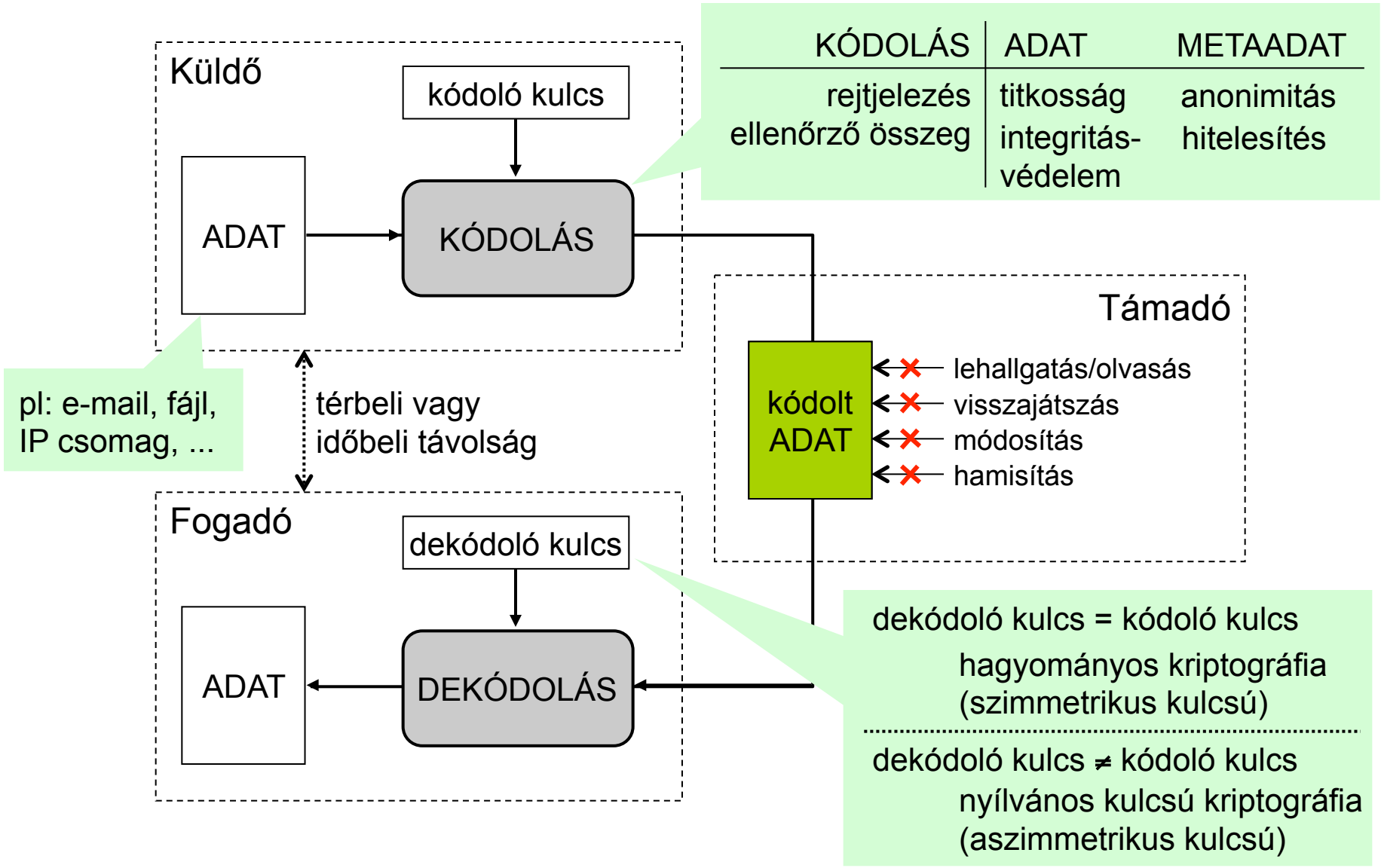
© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Digital signature



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Crypto summary



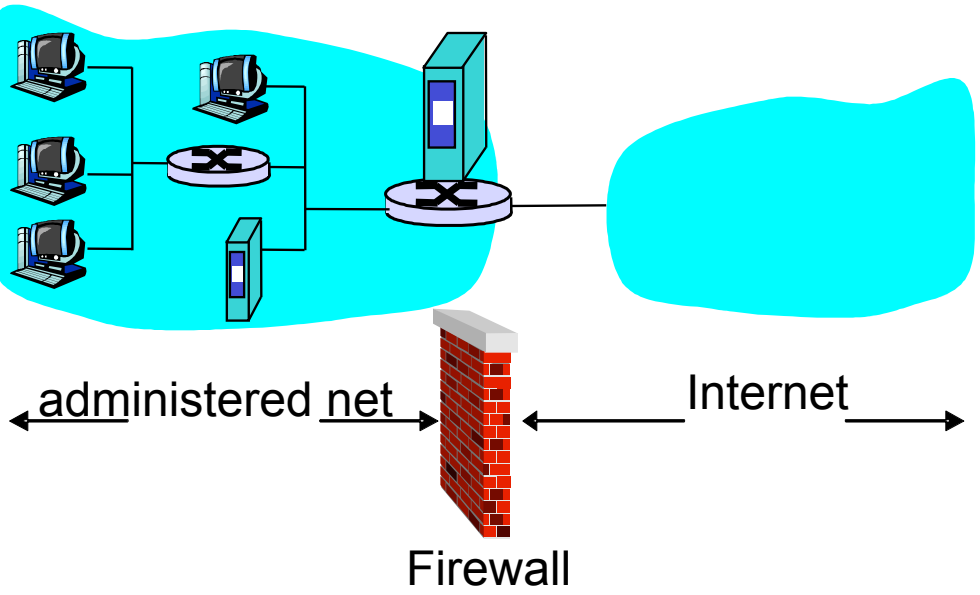
© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Network defenses

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Firewalls

- separates the internal network from the Internet
- some packets can pass, other are dropped



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Firewalls: Why?

Denial-of-Service attack defense:

- SYN-Flooding: attacker initiated several useless TCP connections, not enough resources for legit connections

illegal access or manipulation if internal data:

- website defacement

unauthorized access to the internal network

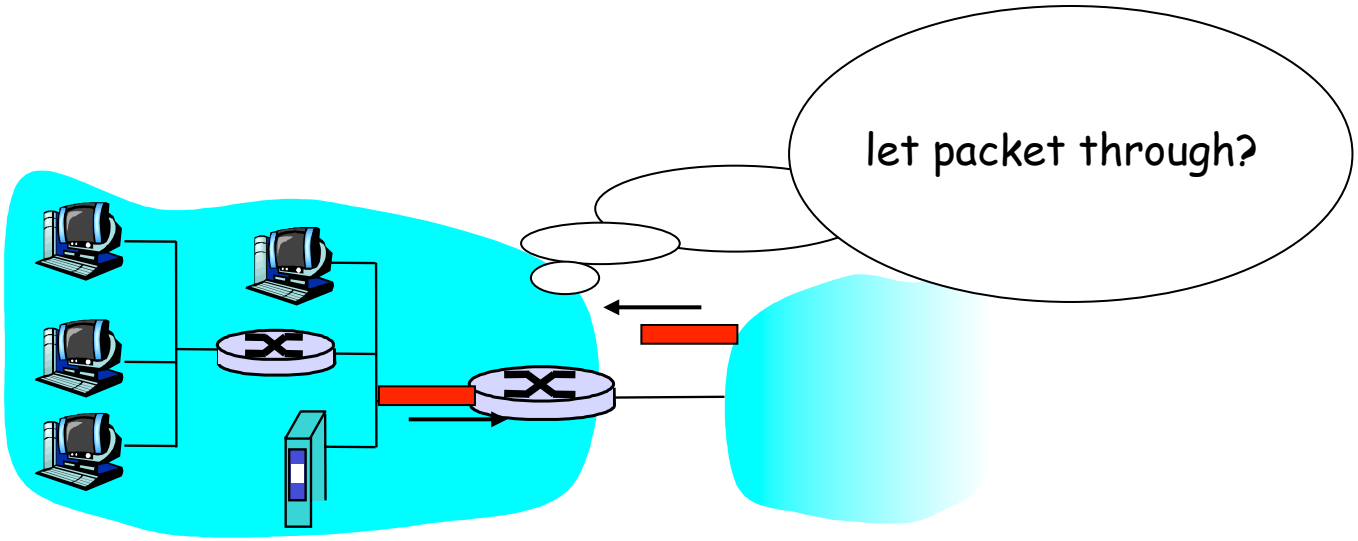
- passing through access control, privilege escalation

3 firewall types (depending on the filtering layer)

- stateless packet filter (L3)
- stateful packet filter (L4)
- application gateway (L7)

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Stateless packet filter



- Router-Firewall separates the internal network and the public Internet
- the router processes each packet, and decides to let it through based on:
  - source and dest IP
  - TCP/UDP source and dest port
  - ICMP data type
  - TCP-SYN- and ACK-Bits

© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Stateless packet filter - examples

goal	Firewall rule
no web access to the outside	drop all incoming packets to all IP addresses to port 80
no incoming TCP connections unless they go to the own webserver	drop all incoming TCP-SYN packets, except if they go to the IP address 130.207.244.203, Port 80.
aviod that a web radio consumes all bandwidth	drop all UDP packets, except for DNS and Router-Broadcasts.
protect network from Smurf-DoS attacks	drop all incoming ICMP broadcast packets (ex. 130.207.255.255)
block net discovery by traceroute	drop outgoing ICMP-TTL-Expired packets

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Access Control Lists

- *ACL:* list of rules aplied to all packets on an interface
- in or out
- criterium - action

action	source IP	dest IP	protocoll	source port	dest port	Flags
allow	222.22/16	nicht in 222.22/16	TCP	> 1023	80	egal
allow	nicht in 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	nicht in 222.22/16	UDP	> 1023	53	---
allow	nicht in 222.22/16	222.22/16	UDP	53	> 1023	----
drop	alle	alle	alle	alle	alle	alle

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Stateful packet filter

- stateless packet filters often let useless traffic pass:
  - ex. packets with port 80, ACK flag set, but no TCP connection exists

action	source IP	dest IP	protocoll	source port	dest port	Flags
allow	not in 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* follow TCP connections
  - read SYN and FIN packets
  - timeout for inactive connections on the firewall

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Stateful packet filter

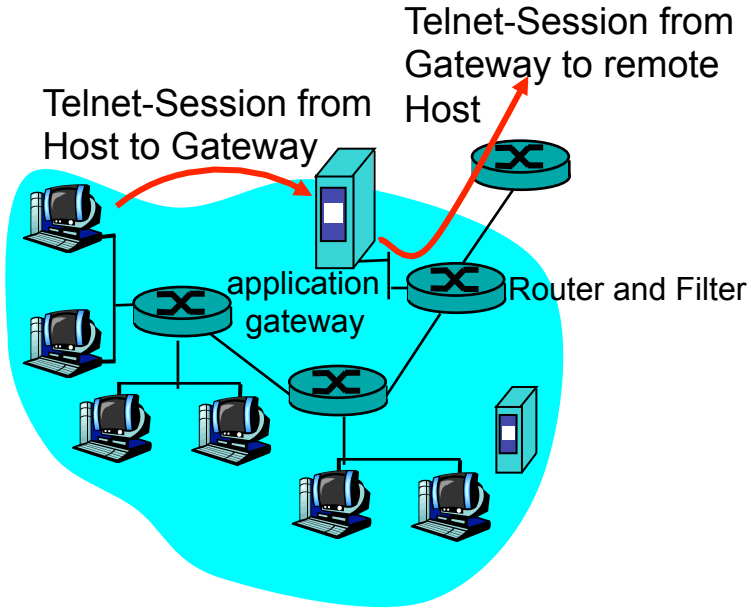
- ACL is extended to check the connection status

action	source address	dest address	proto	source port	dest port	flag bit	check conn
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Application gateway

- filtering packets based on application info and TCP/ UDP/IP fields
- example: only some users can Telnet to the outside



1. require each Telnet connection to pass the gateway
2. establish a Telnet session for authorized users with the remote host; Gateway used as a proxy to relay data
3. router firewall blocks all Telnet connection not originating from the gateway

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Limits of firewalls and gateways

- IP-Spoofing: a router cannot know if the data comes from the source IP
- we need an application gateway for each special application
- Client software has to know which gateway to access:
  - need to set an address of the web proxy
- "all or nothing" rules for UDP
- communication possibilities vs. security level
- even well protected networks are targeted by attacks

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

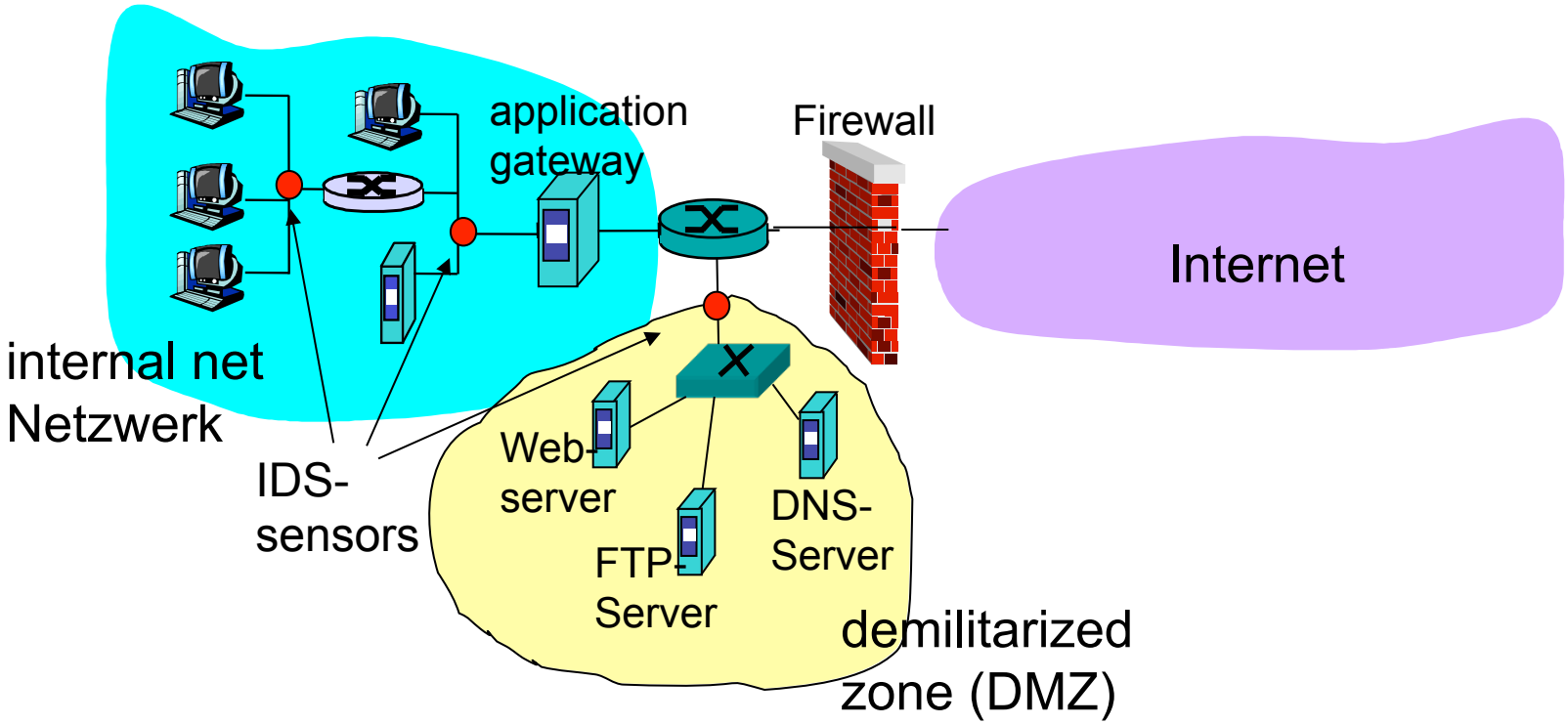
Intrusion detection systems (IDS)

- packet filters:
  - applied only on TCP/IP headers
  - data from different sessions cannot be correlated
- Intrusion detection systems (IDS)
  - *Deep Packet Inspection:* analyze the content of packets (ex. for patterns signalling a well-known attack)
  - correlation of multiple packets
    - Port-Scanning
    - network mapping
    - DoS attacks

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME

Intrusion detection systems

- multiple IDS: various tests at different locations



© Mark Felegyhazi, CrySyS Lab,
Department of Telecommunications, BME

Security concepts summary

- basic concepts
  - security, attack, vulnerability, threat
  - passive vs. active attacks
  - eavesdropping, traffic analysis, masquerade (spoofing), modification, replay, denial of service
  - main communication security services: confidentiality, integrity, availability, authentication, non-repudiation
- some real world attacks
  - ARP spoofing, e-mail forgery, eavesdropping Telnet and FTP passwords, DDoS attacks
- network defenses

© Mark Felegyhazi, CrySyS Lab, Department of Telecommunications, BME