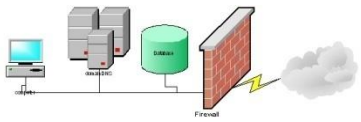
Információs rendszerek üzemeltetése

BME VIK TMIT

Mérnök-informatikus BSc szak



Áttekintés és menetrend

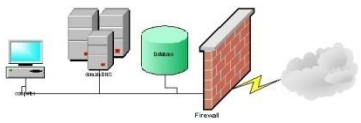
Információs

Rendszerek

Üzemeltetése

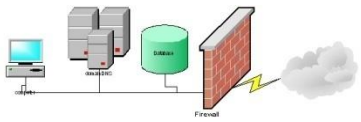
- Desktop, Szerver,
- IP hálózatok,
- Adattárolás, mentés, archiválás, virtualizáció, cloud
- Szabványok, SLA-k
- Információs szolgáltatások üzemeltetési feladatai,
- IT biztonság,

Sok esettanulmányon keresztül.

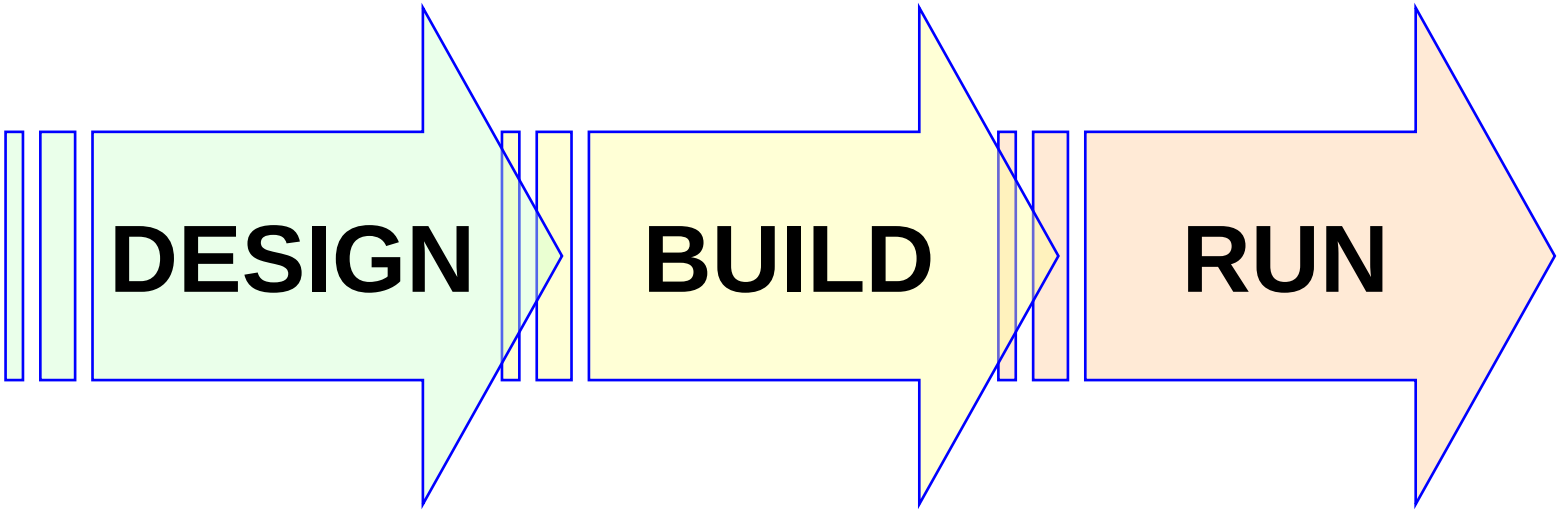


A tárgy célja

A tárgy célja a számítógépek illetve összetett, hálózatba kapcsolt információs rendszerek működtetési és rendszer-adminisztrációs feladatainak megismertetése. A tantárgy rendszer-szemléletű áttekintést ad az információs rendszerekről és a széles értelemben vett rendszergazdai feladatokról.



IT fejlesztés funkcionális életciklusa



Szabványok (Best Practice), folyamatok

Hosszú- és középtávú stratégiai alapok

Előadók

Dr. Magyar Gábor (TMIT)

Dr. Adamis Gusztáv (TMIT)

Dr. Varga Pál (TMIT)

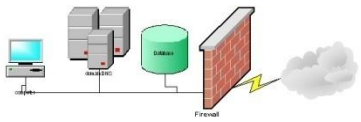
Jankó Árpád (KFKI)

Témakidolgozás ++

Maradi István (Magyar Telekom)

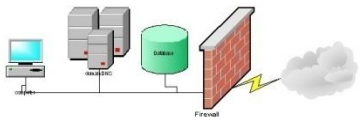
Piszker György (Magyar Telekom)

Kocsis Zsolt (IBM)



Fontosabb időpontok

- Előadás:
  - Csütörtök *minden hét* 14:15-17:00 – I.B.028
- Laboratóriumi gyakorlat:
  - Jelentkezés: http://medialab.bme.hu/ -> „Laborjelentkezés”
  - Első lehetőség: március 5-én
    - mindenkinek **kettő** alkalom; egyetlen pótlási lehetőség
  - Szerda 14:15 - 17:25 (R4J, R4K)
  - Péntek 8:15 - 11:25 (R4J, R4K)
- Zárthelyi dolgozat - 04.01.; 8:15-10:00,
- PótZH - 04.18.; 14:15-16:00



Hasznos források

- Tantárgyi adatlap:

https://www.vik.bme.hu/kepzes/targyak/VITMA314/

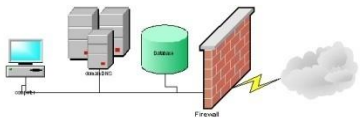
- Tantárgy honlapja:

http://medialab.bme.hu/index.php?page=7&subpage=VITMA314

- Hasznos könyvek:

Tom Limoncelli, Christina J. Hogan, Strata R. Chalup:
The Practice of System and Network Administration

Evi Nemeth, Garth Snyder, Trent R. Hein, Ben Whaley:
UNIX and Linux System Administration Handbook

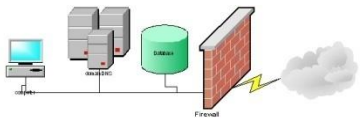


Opcionális Házi Feladat

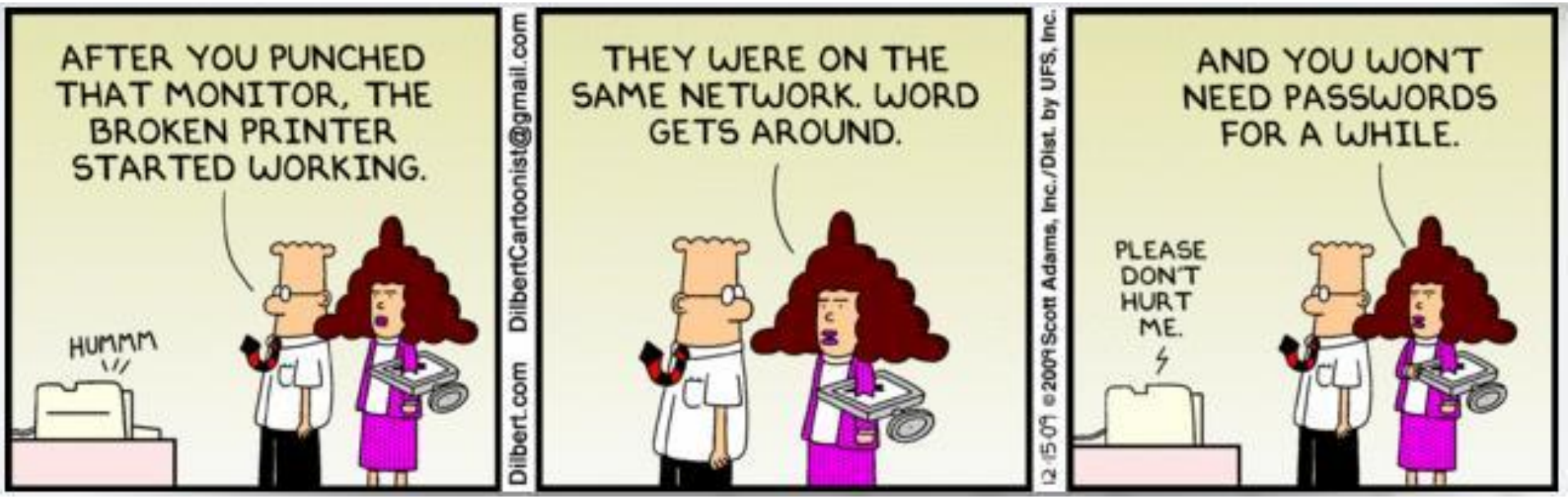
- Az IRÜ témaköréhez kapcsolódó újdonságokból házi dolgozat: min. 8 max. 10 oldal, forrásmegjelöléssel
- Ide kapcsolódó célfeladatok megvalósítása Linux környezetben "script nyelvek" segítségével:
  - awk, perl, python, ruby,…

- A feladatok hirdetése és kiadása
  - A következő hetekben az előadáson
  - „First Come First Served”

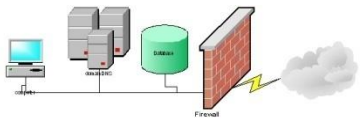
- Előny: az 50 pontos vizsgán max. 8 extra ponttal
- Hátrány: elvállalt, de el nem végzett feladat -2 ponttal



Még nincsenek jövőbeli módszerek

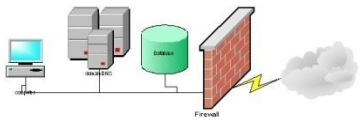


Egy komplex esettanulmány
- felvezetés -



Esettanulmány: TÜK

- **TÜK**: Telefonos Ügyfélközpont: „Call Center”
- Egy nagyvállalat **szervezeti átalakulásakor** a **szétszórt** ügyfélközpontok egységesítése is a feladatok közé tartozik
  - Telephelyek összehangolása
  - IT infrastruktúra
    - Desktop gépek
    - Közös perifériák: nyomtatók
    - Hálózat
  - Alkalmazások kezelésének ésszerűsítése

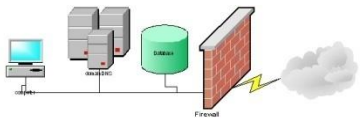


Ráhangolás: - Miről is van szó?

- Mire szolgál a Telefonos Ügyfél Központ (TÜK)?

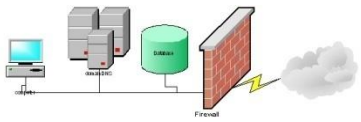
- Mi az „IT crowd” feladata egy TÜK-ben?
  - Műszaki tervező, megoldásszállító
  - Szolgáltatási szintek (SLA: Service Level Agreement) szerinti belső/háttérszolgáltató

- Milyen nézőpontból közelítjük meg a feladatot?
  - Műszaki, szolgáltatási vagy/és szervezési/szervezeti vetület

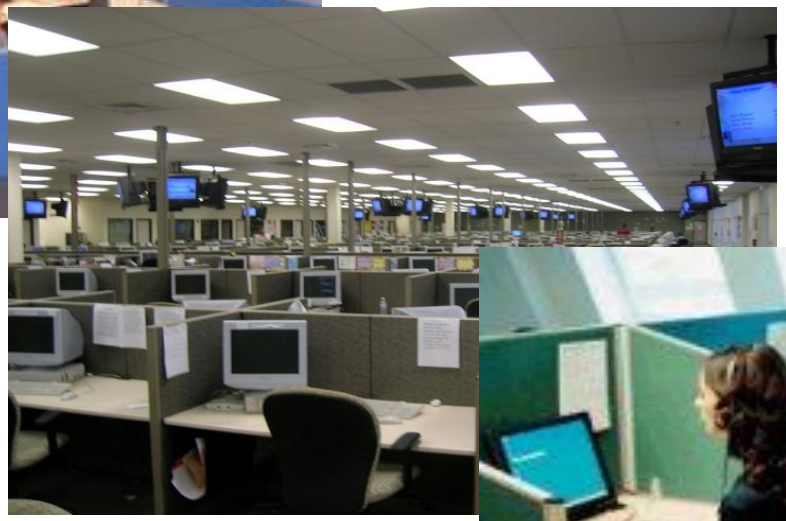


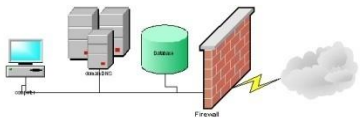
Mire szolgál a TÜK?

- Fő funkciók
  - Ügyfélszolgálat
  - Tudakozó
  - Hibabejelentő
- „Informatikai osztály” által támogatott konkrét tevékenységek
  - Számlázás
  - Levelezés
  - IVR: Interactive Voice Response (opcionális)
  - Standard Office működtetése



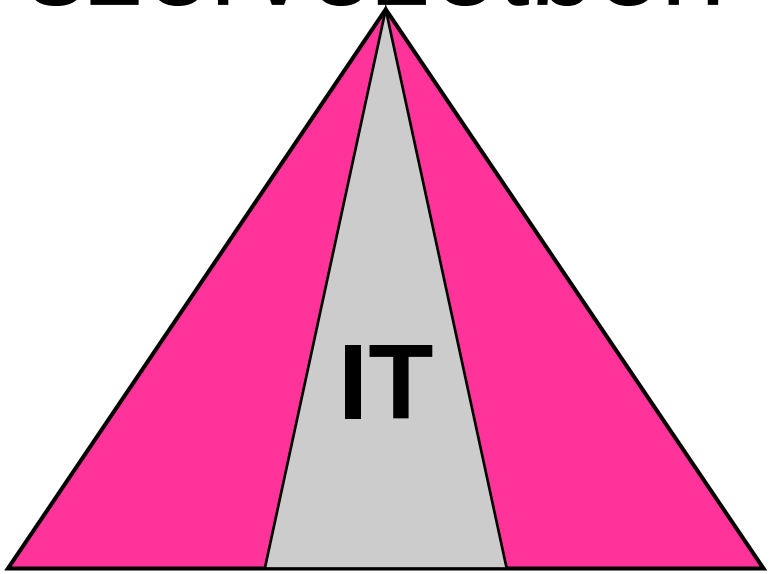
Telefonos Ügyfél Központ a valóságban



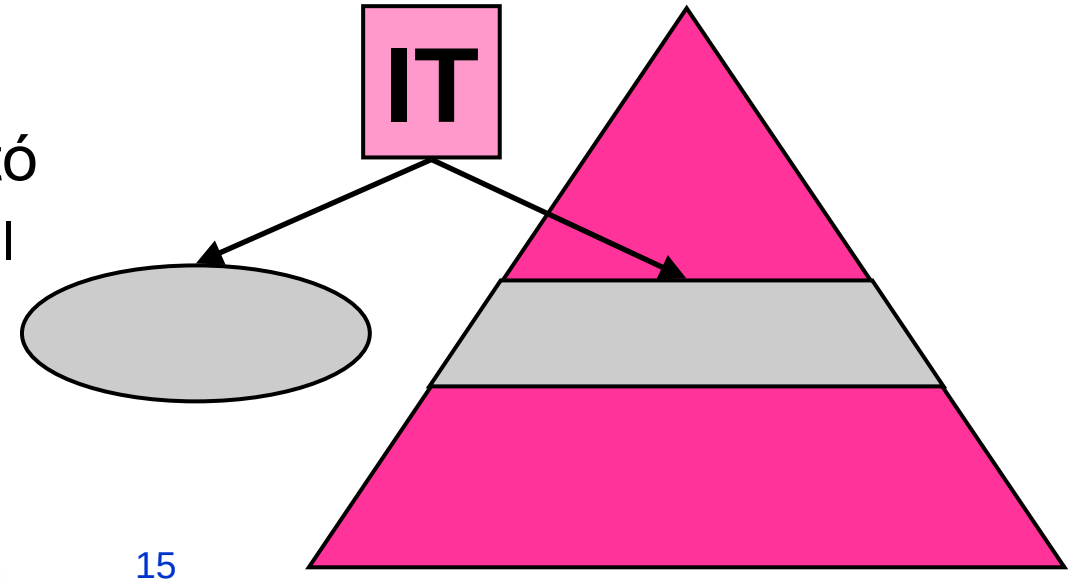


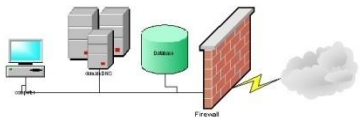
Az IT helye a szervezetben

- A cég főtevékenysége
  - Az IT szolgáltatás maga az üzlet (bevételi felelősség)
  - A cégen belül is szolgáltat (költséghely)

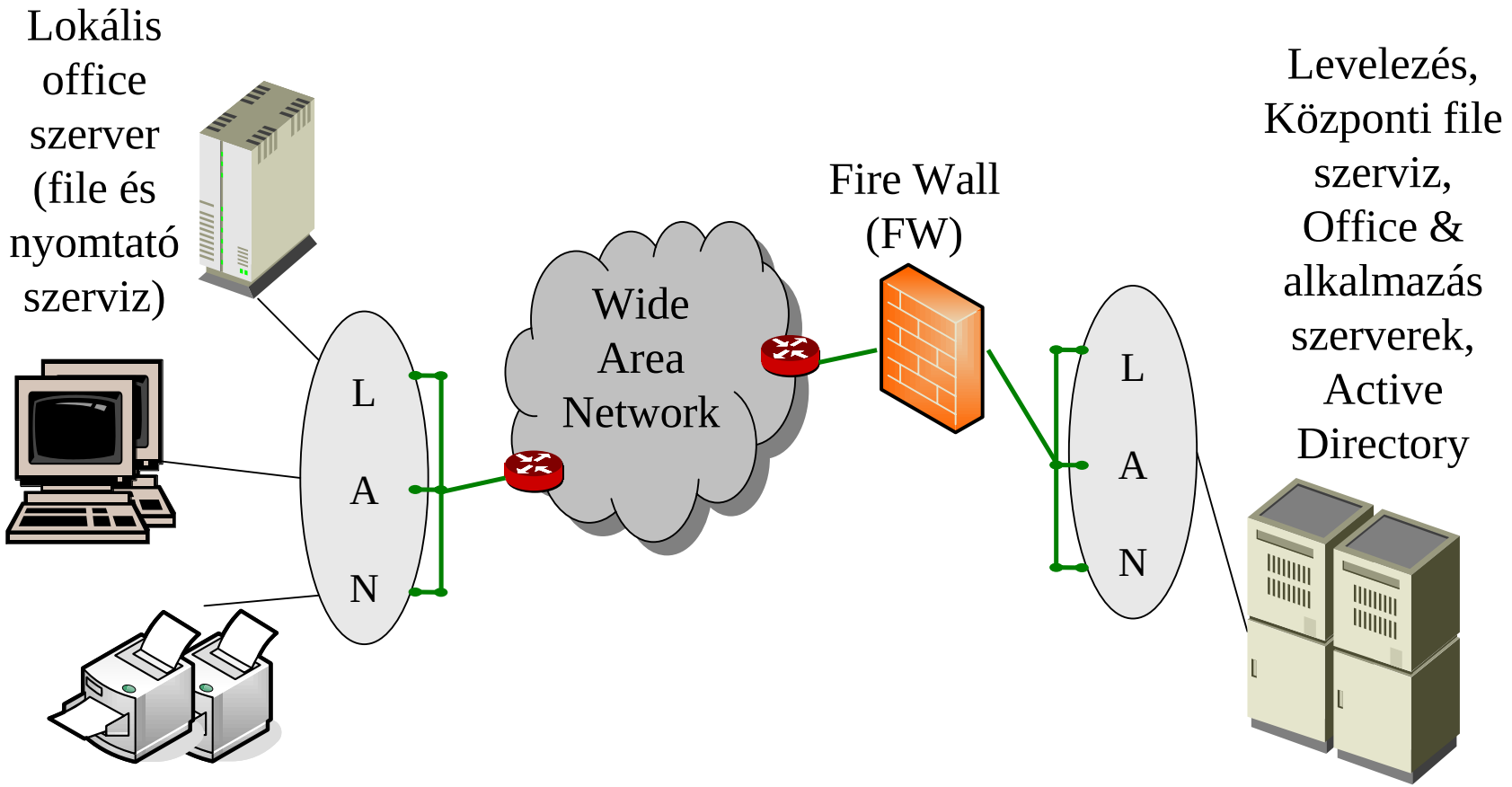


- „Csak” belső szolgáltató
  - Belső erőforrást használ
  - Kintről veszi meg

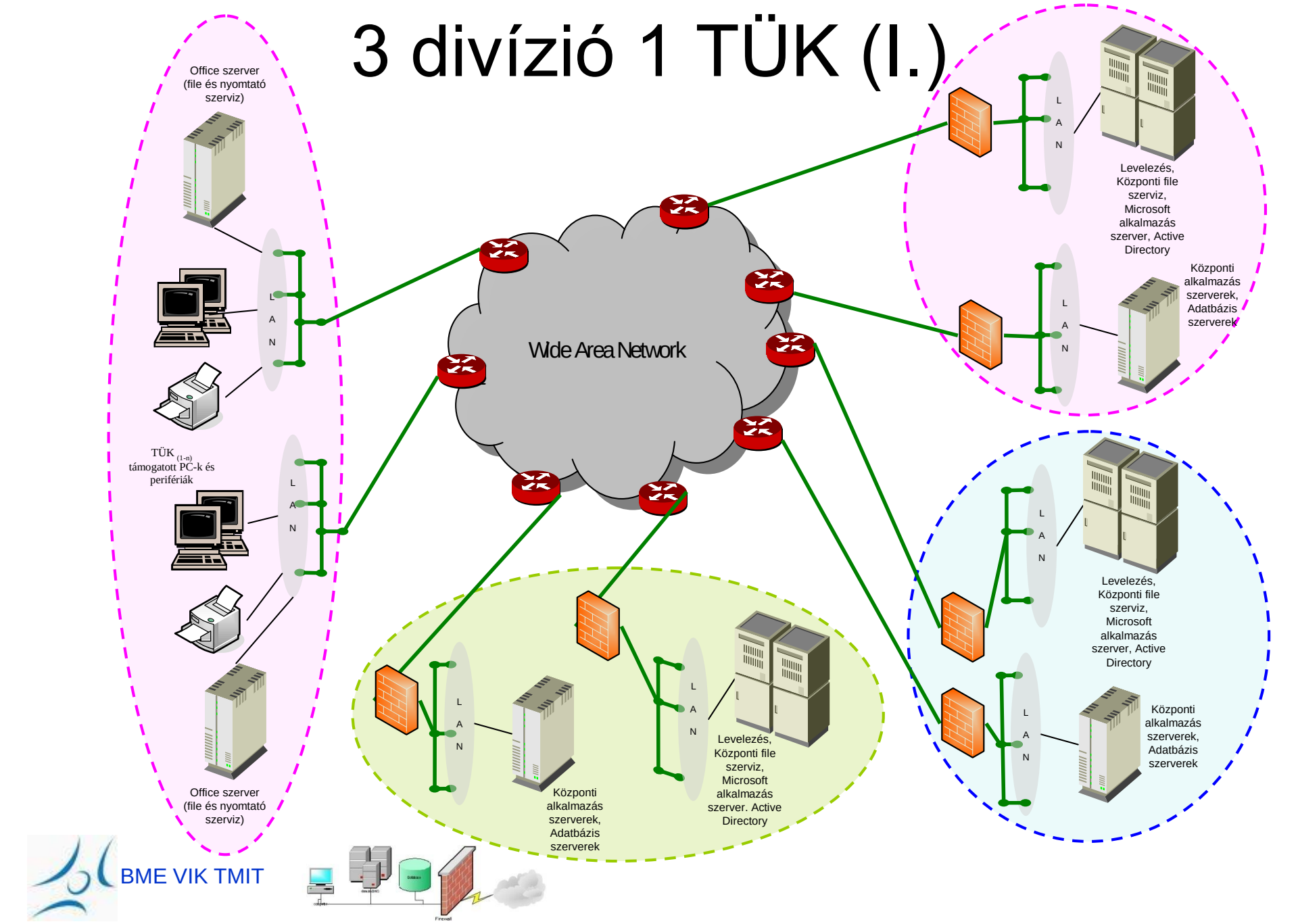


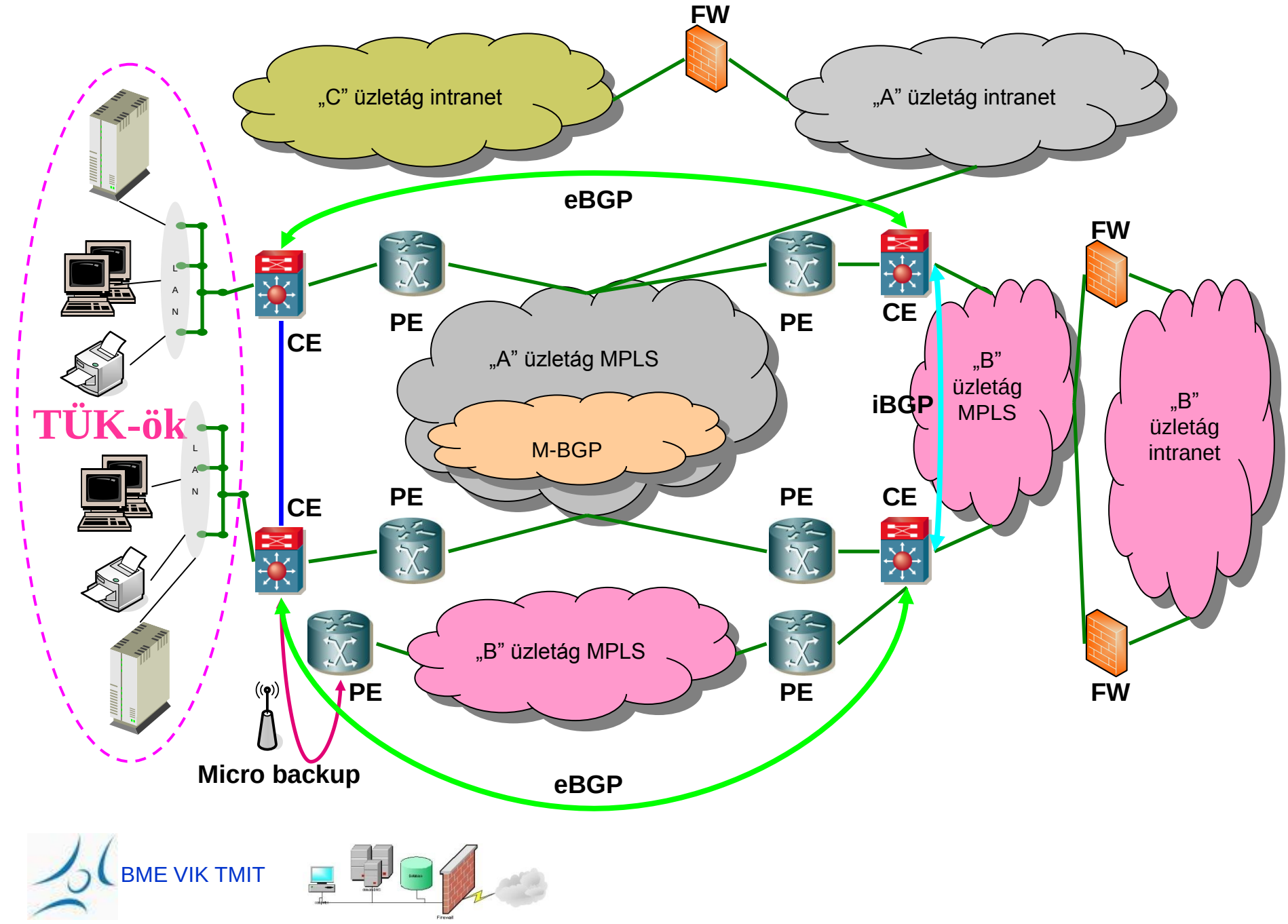


TÜK IT architektúra

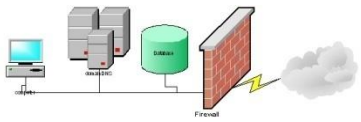


3 divízió 1 TÜK (I.)



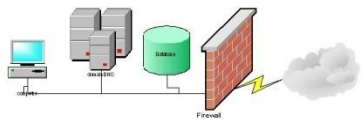

FW
„C” üzletág intranet
„A” üzletág intranet
eBGP
TÜK-ök
LAN
CE
PE
„A” üzletág MPLS
M-BGP
iBGP
„B” üzletág MPLS
„B” üzletág intranet
FW
Micro backup
„B” üzletág MPLS
eBGP

Útmutató a tantárgyi gyakorlat sikeres elvégzéséhez



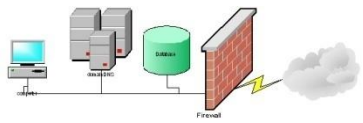
Áttekintés

- A gyakorlat helye, ideje, időtartama
- Követelmények
- Felkészülési anyagok
- A VMWARE használata
- *Két-két* eszköz – *külön* gyakorlati alkalmakon
  - **IBM Tivoli**
    - **Storage Manager FastBack**
    - **Monitoring Version 6.2**
  - **Linux adminisztráció**
    - **Alap Linux, tűzfal, MySQL, címtár (LDAP)**
    - **bash, apache**



A gyakorlatok...

- Helye:
  - HSzK, R épület 4. Emelet
  - J és K termek
- Ideje:
  - Szerda 14:15 - 17:25 (R4J, R4K)
  - Péntek 8:15 - 11:25 (R4J, R4K)
  - Pótlásként:
    - A pótlási héten szerdán és pénteken a fenti időkben
    - A két gyakorlatból csak egy pótlására van lehetőség a félévben
- Időtartama:
    - 4 tanóra - 3 óra 10 perc – egy 10 perces szünettel számolva

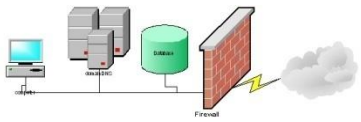


Követelmények

- Legalább ‘elégséges’ (2) érdemjegy mindkét gyakorlaton
- Tivoli: mindkét eszköz megismerése
  - Ennek bizonyítása:
    - a gyakorlati segédletben jelzett lépésekig eljutni,
    - ott a megfelelő képernyőképeket elmenteni,
    - azokat a gyakorlat befejezése előtt e-mailben (tömörített csatolmány!) eljuttatni az

      iru.bme@gmail.com

      címre, a tárgymezőben a **saját névvel**.
- Linux alaptémák
  - ellenőrző script eredményét kell elküldeni



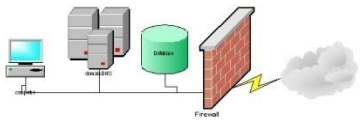
Pótlási lehetőség

Ha valaki nem jelenik meg, vagy sikertelen a gyakorlata,

EGYETLEN

alkalommal van lehetőség pótlásra.

A pótlást egyénileg kell egyeztetni (pvarga@tmit.bme.hu); a feljelentkező felületen újra kell jelentkezni.



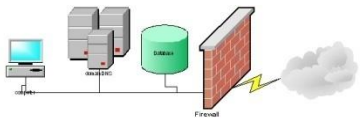
Felkészülési anyagok

- Segédletek a tantárgyi honlapon:

http://medialab.tmit.bme.hu/index.php?page=7&subpage=VITMA314

- VMWARE workstation - virtuális gép:

http://www.vmware.com/products/workstation/

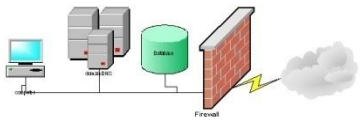


Felkészülési anyagok (2)

- IBM Tivoli Storage Manager FastBack

Marketing:
http://www-01.ibm.com/software/tivoli/products/storage-mgr-fastback/
Dokumentáció:
http://publib-b.boulder.ibm.com/abstracts/sg247685.html?Open innen
http://www.redbooks.ibm.com/redbooks/pdfs/sg247685.pdf
- Innen az 1. és az 5. fejezet az érdekes a gyakorlathoz

  – Magyar nyelvű anyag a tantárgyi honlapra lesz feltöltve
  - rövid összefoglaló
  - mérési útmutató

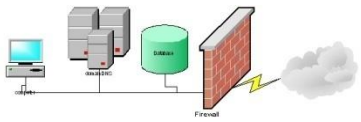


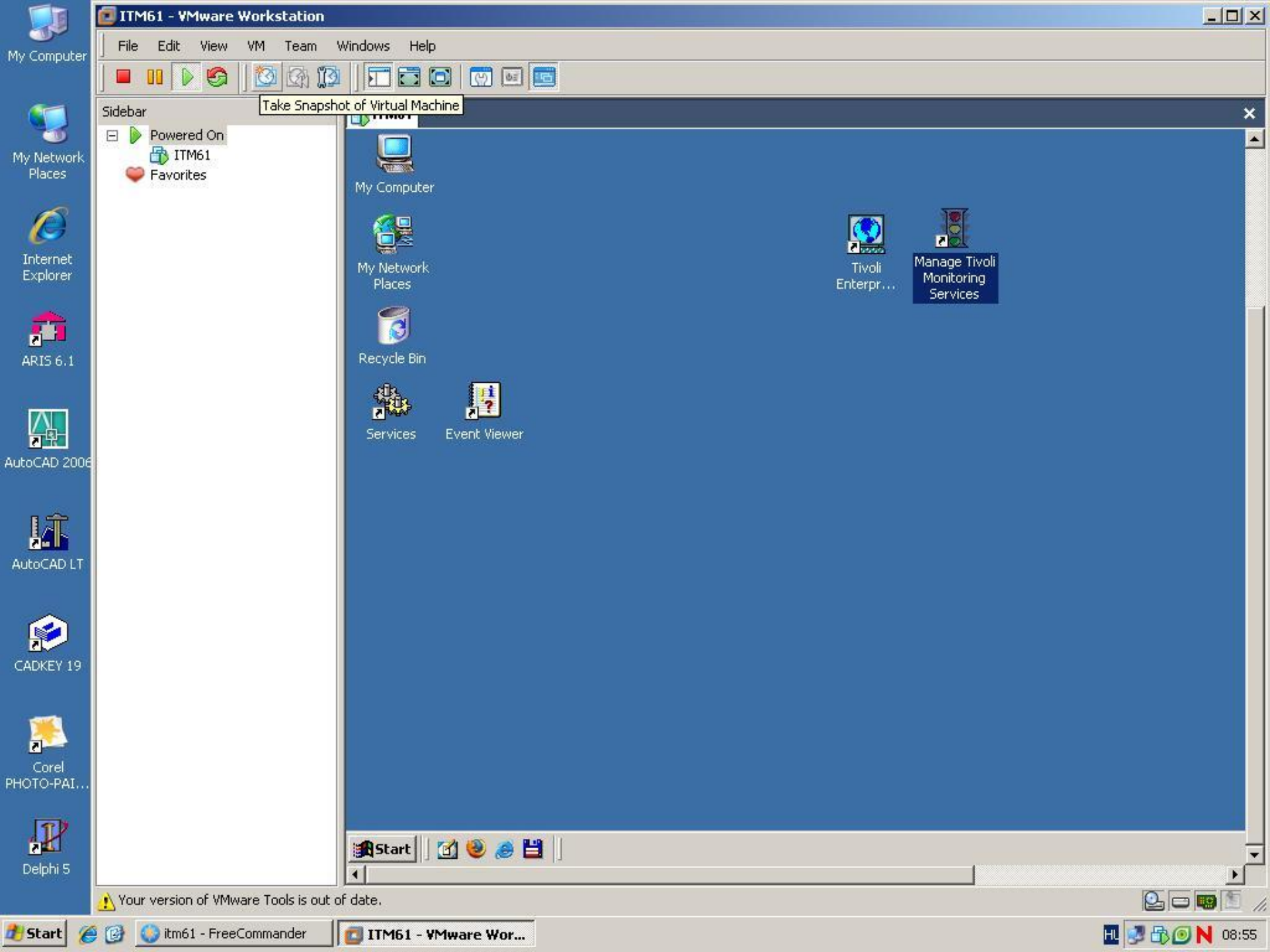
Felkészülési anyagok (3)

- IBM Tivoli Monitoring Version 6.2

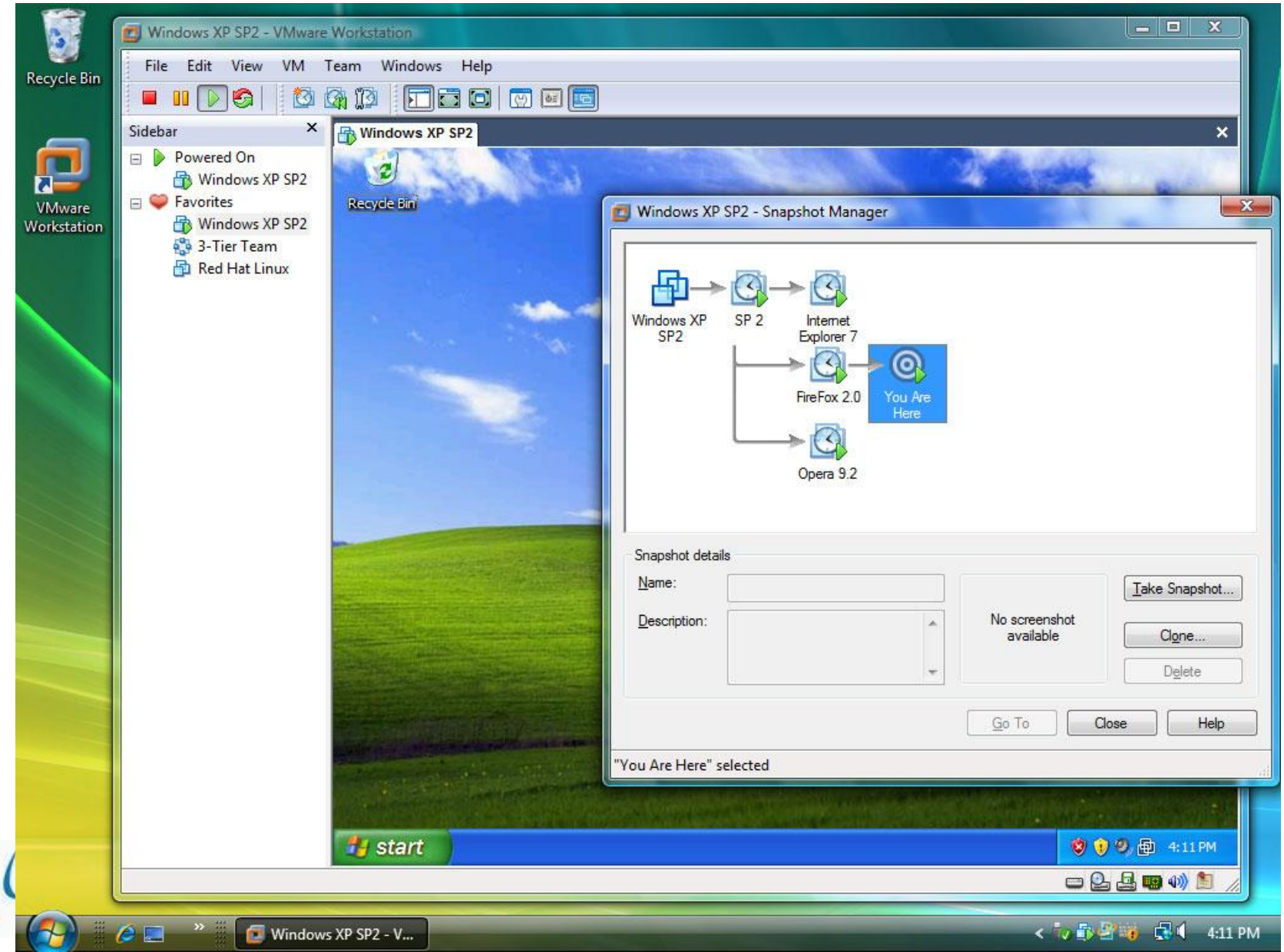
http://www.redbooks.ibm.com/abstracts/sg247444.html?Open innen
http://www.redbooks.ibm.com/redbooks/pdfs/sg247444.pdf

Chapter 1.5 &
Chapter 3 eleje (3.2 után nem kell) &
Chapter 4 az elolvasandó.



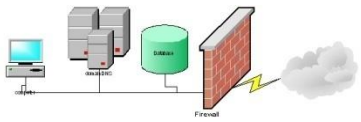

My Computer
My Network Places
Internet Explorer
ARIS 6.1
AutoCAD 2006
AutoCAD LT
CADKEY 19
Corel PHOTO-PAI...
Delphi 5
ITM61 - VMware Workstation
File Edit View VM Team Windows Help
Take Snapshot of Virtual Machine
Sidebar
Powered On
ITM61
Favorites
My Computer
My Network Places
Recycle Bin
Services
Event Viewer
Tivoli Enterpr...
Manage Tivoli Monitoring Services
Start
Your version of VMware Tools is out of date.
Start
itm61 - FreeCommander
ITM61 - VMware Wor...
08:55

A VMWARE használata



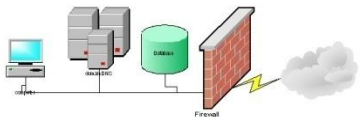
Néhány VMWARE trükk

- .vmx indítja a virtuális gépet
- Wmware ablakba kattintás: a virtuális gép aktív
- ..azon kívül kattinás: *host OS*-be visszatérés
- A Wmware képernyő teljes képernyő-nagyságúra is nagyítható



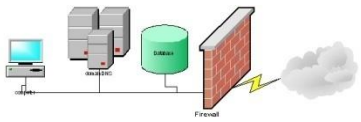
IBM Tivoli Storage Manager FastBack

- Struktúra
- Feladatok a gyakorlatokon
- A teljesítés ellenőrzése

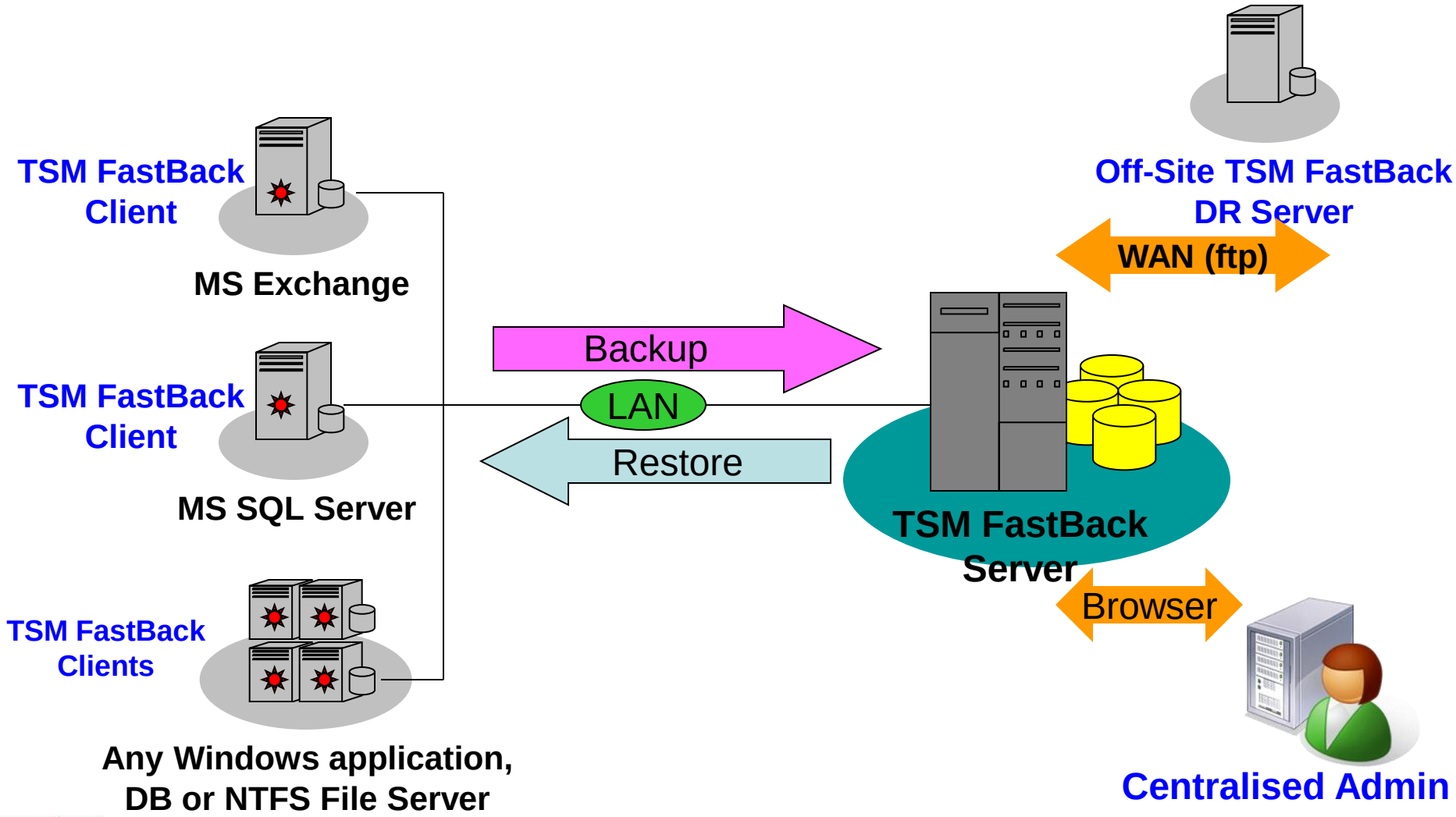


IBM Tivoli Storage Manager (TSM) FastBack

- Struktúra
  - Mentési szerver (*FastBack Server*)
  - Kliensek (*FastBack Client*)
  - Központi adminisztrátor
  - Távoli Katasztrófa utáni -visszaállító *(Disaster Recovery Server)*

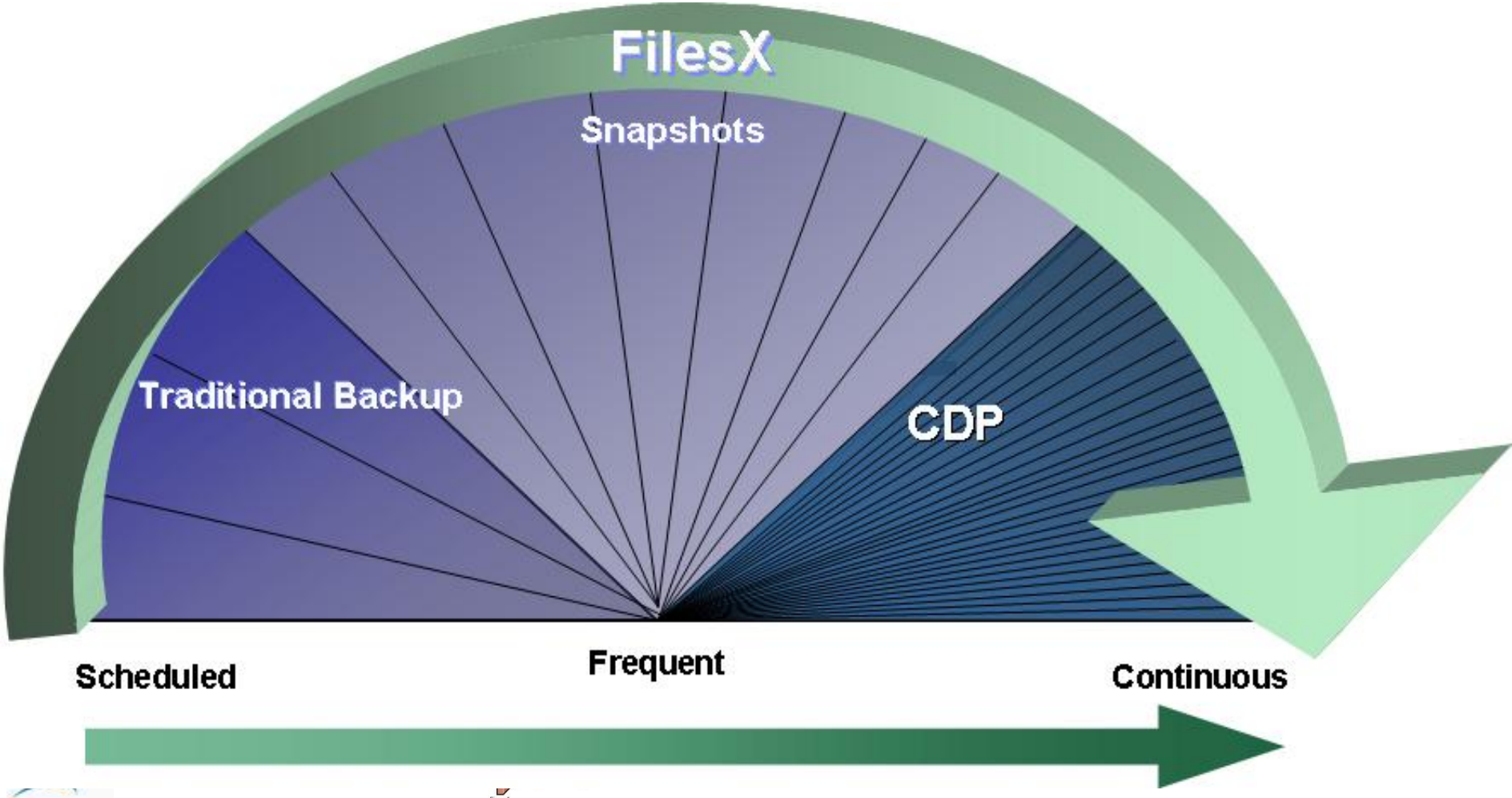


IBM TSM FastBack - struktúra

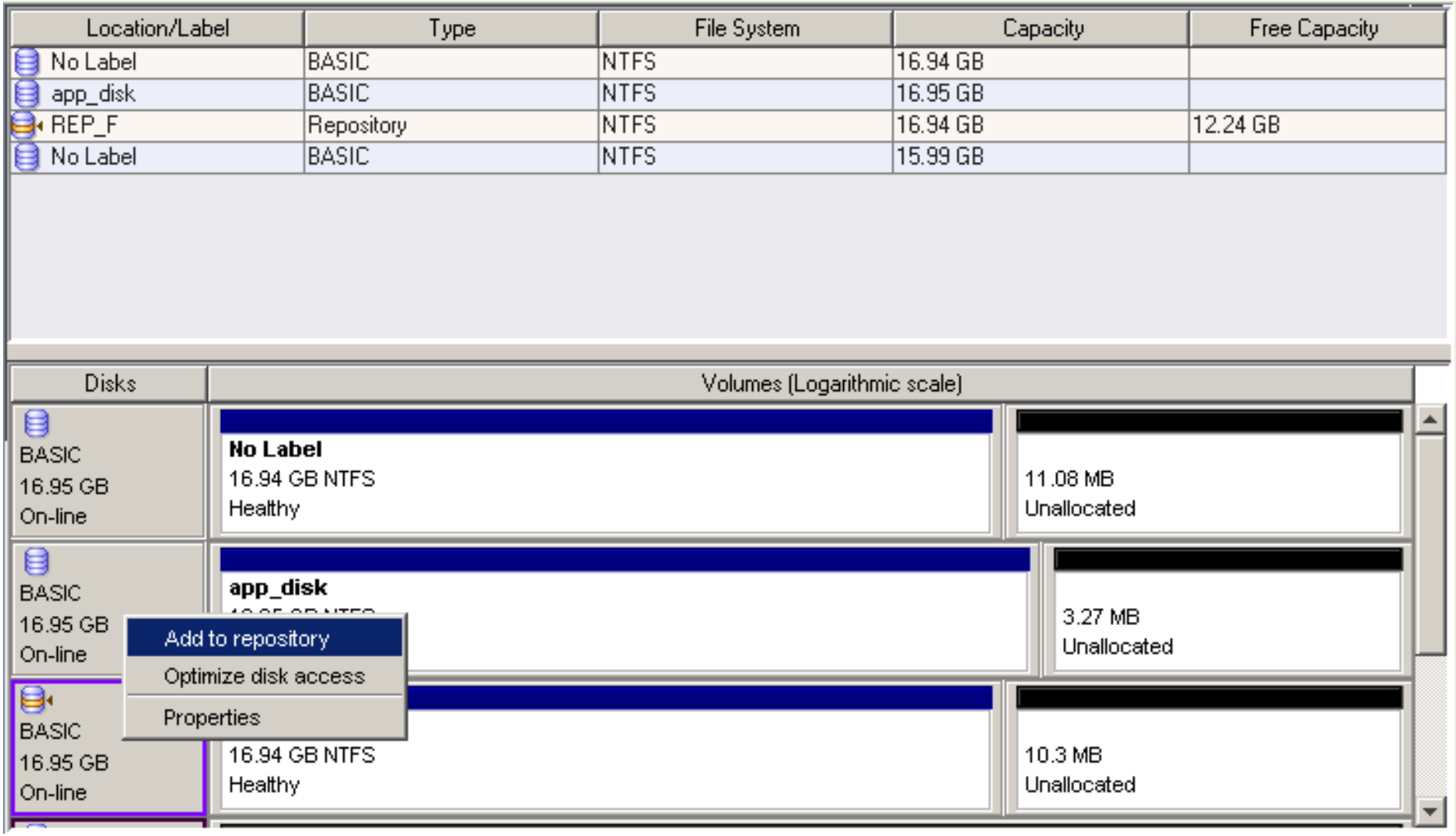


IBM TSM FastBack

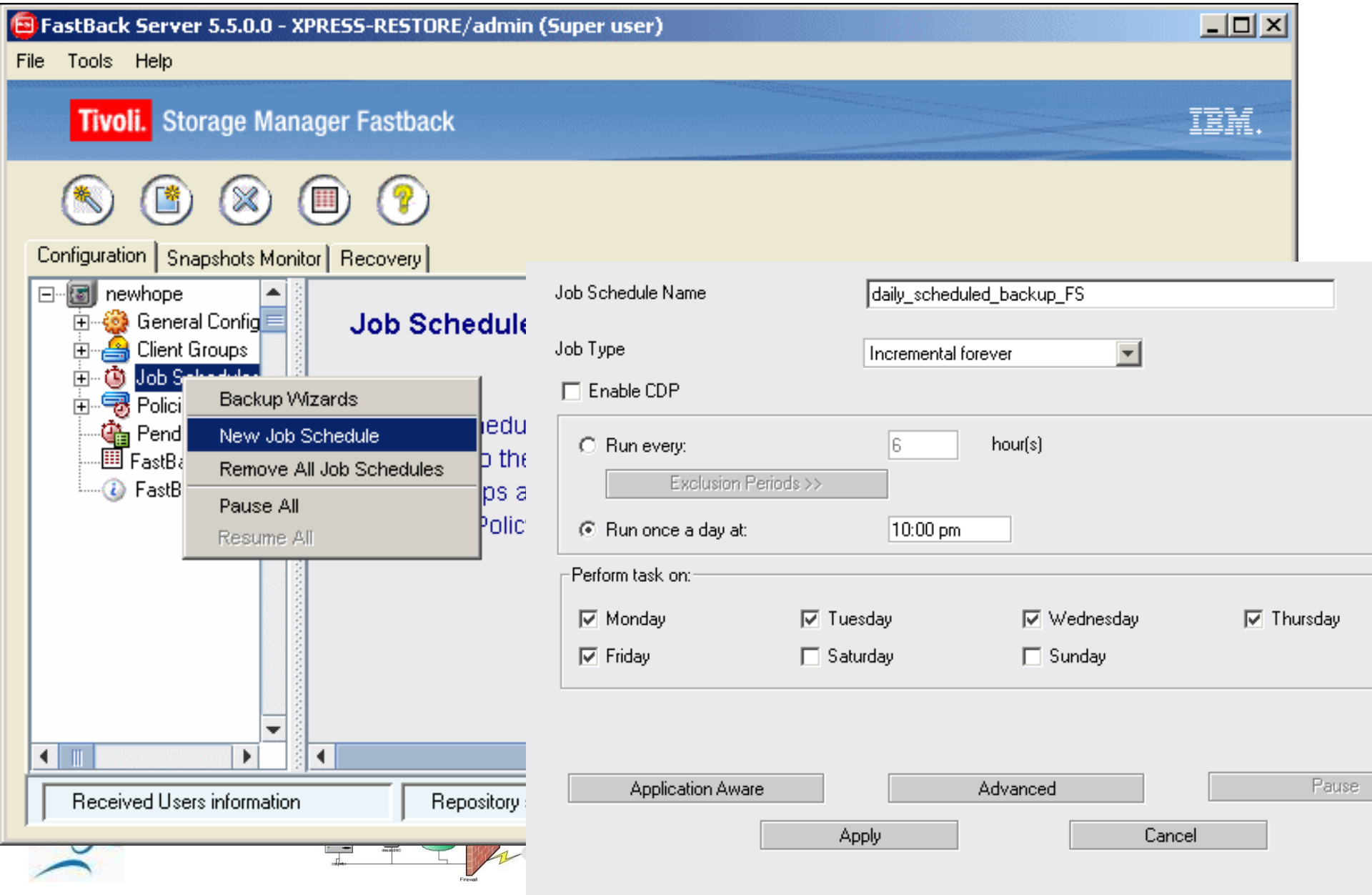
- Mentési stratégiák- hagyományostól a folyamatosig (Continuous Data Protection)



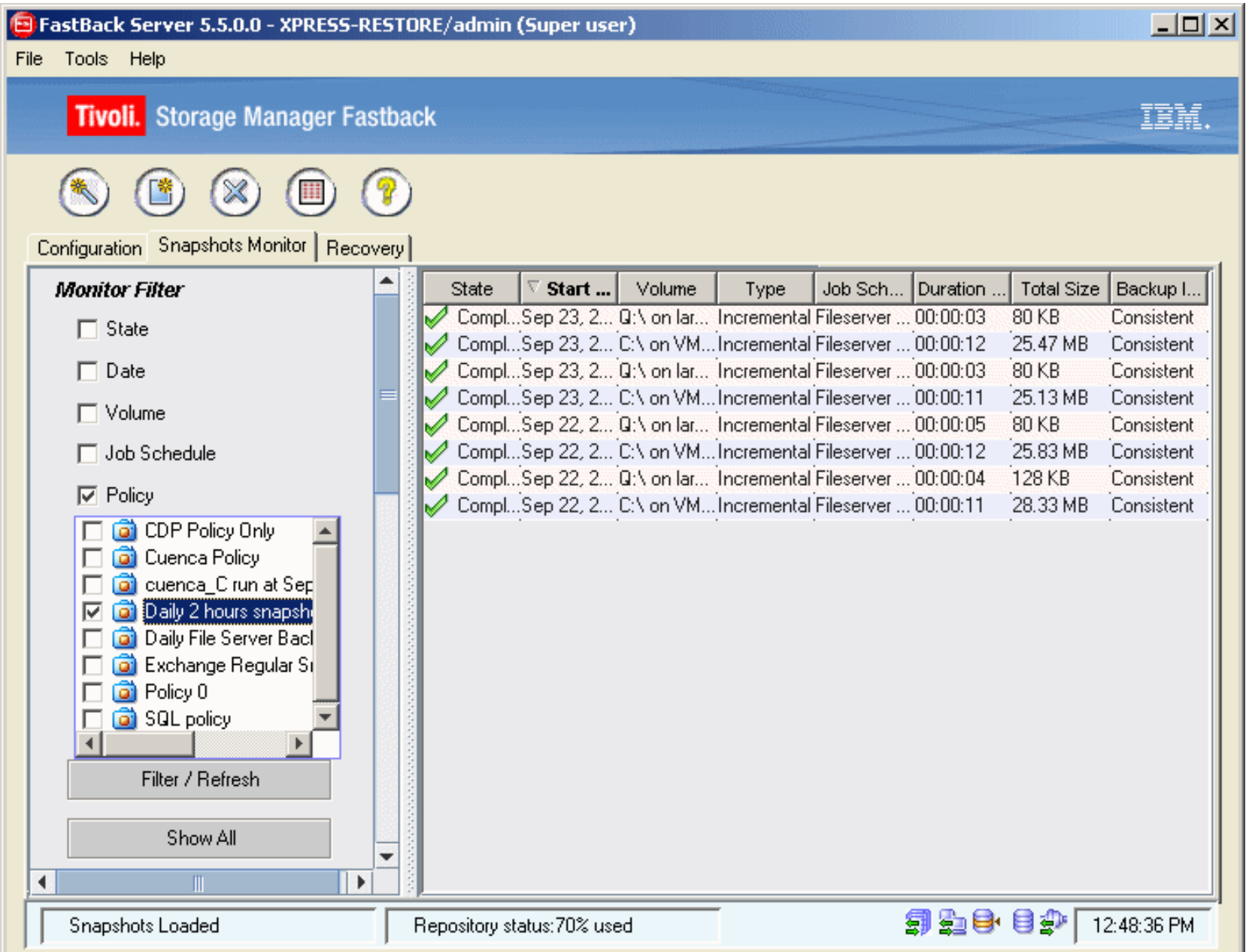
IBM TSM FastBack Manager – repository



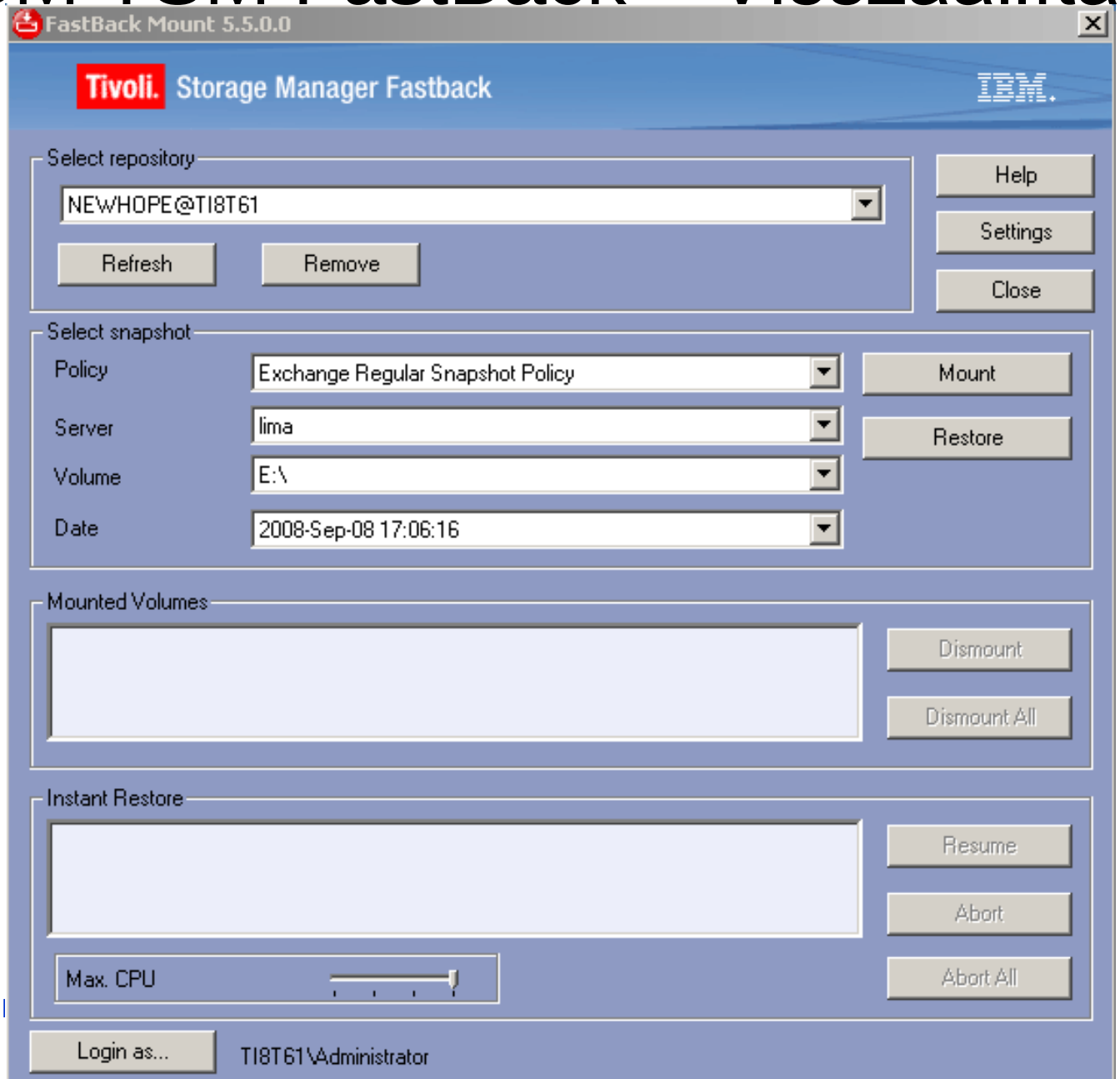
IBM TSM FastBack – Mentési ütemezés



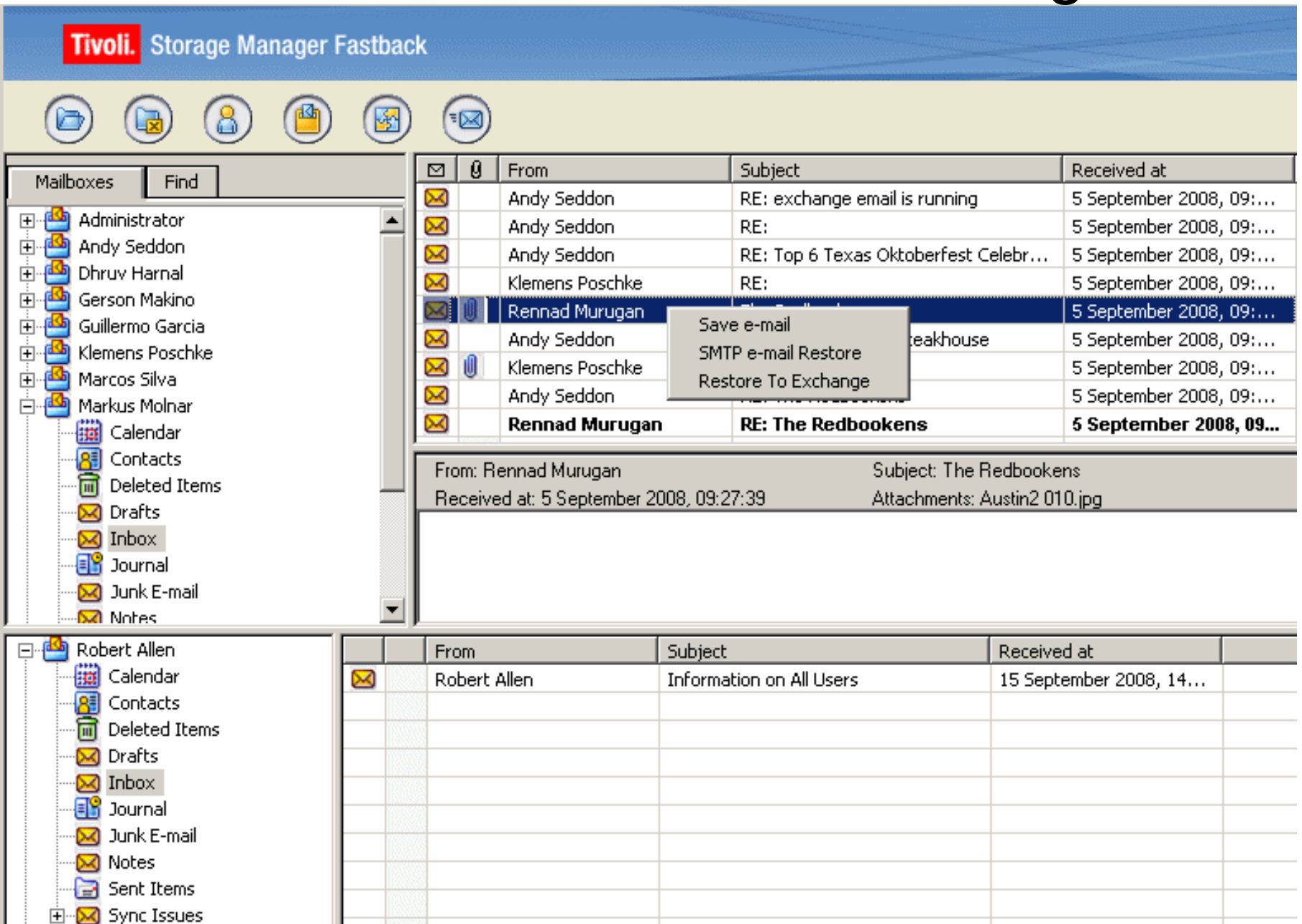
IBM TSM FastBack – Mentési „policy”



IBM TSM FastBack – Visszaállítási példa

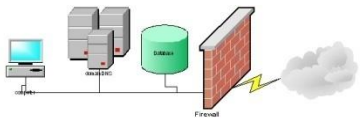


IBM TSM FastBack – MS Exchange restore



IBM Tivoli Storage Manager FastBack

- ... a gyakorlaton még néhány, az előzőekhez hasonló feladat...

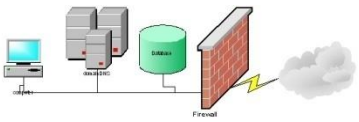


IBM TSM FastBack

- A teljesítés ellenőrzése...:

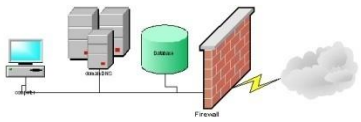
A mérés során bizonyos pontokról képernyőképet kell készíteni, és azt adott néven elmenteni.

- ‘Alt’ + ‘Prt Scr’
- Paint -> ‘Ctrl’ + ‘V’ -> Save…
- Ennél a mérésnél lehet a virtuális gépen…, de jobb a *host OS* alatt..



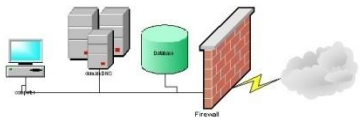
IBM Tivoli Monitoring

- Struktúra
- Feladatok a gyakorlatokon
- A teljesítés ellenőrzése

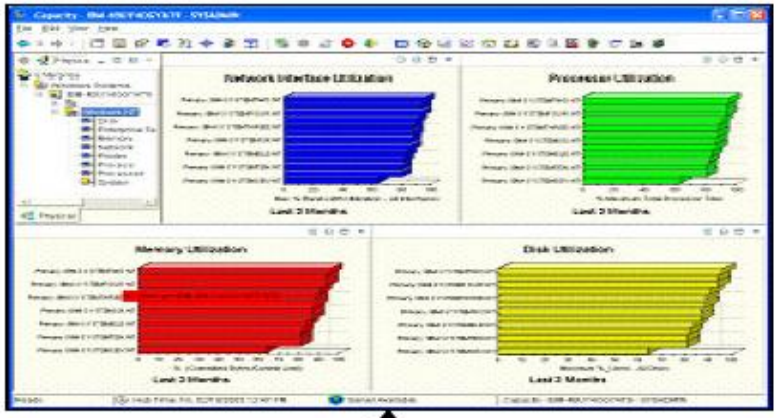


IBM Tivoli Monitoring

- Struktúra
  - Tivoli Enterprise Monitoring Agent
  - Tivoli Enterprise Monitoring Server
  - Tivoli Enterprise Portal Server
  - Tivoli Enterprise Portal



Monitoring Portal
(user or browser based)
with
Tivoli Enterprise Portal



Monitoring and Portal Server

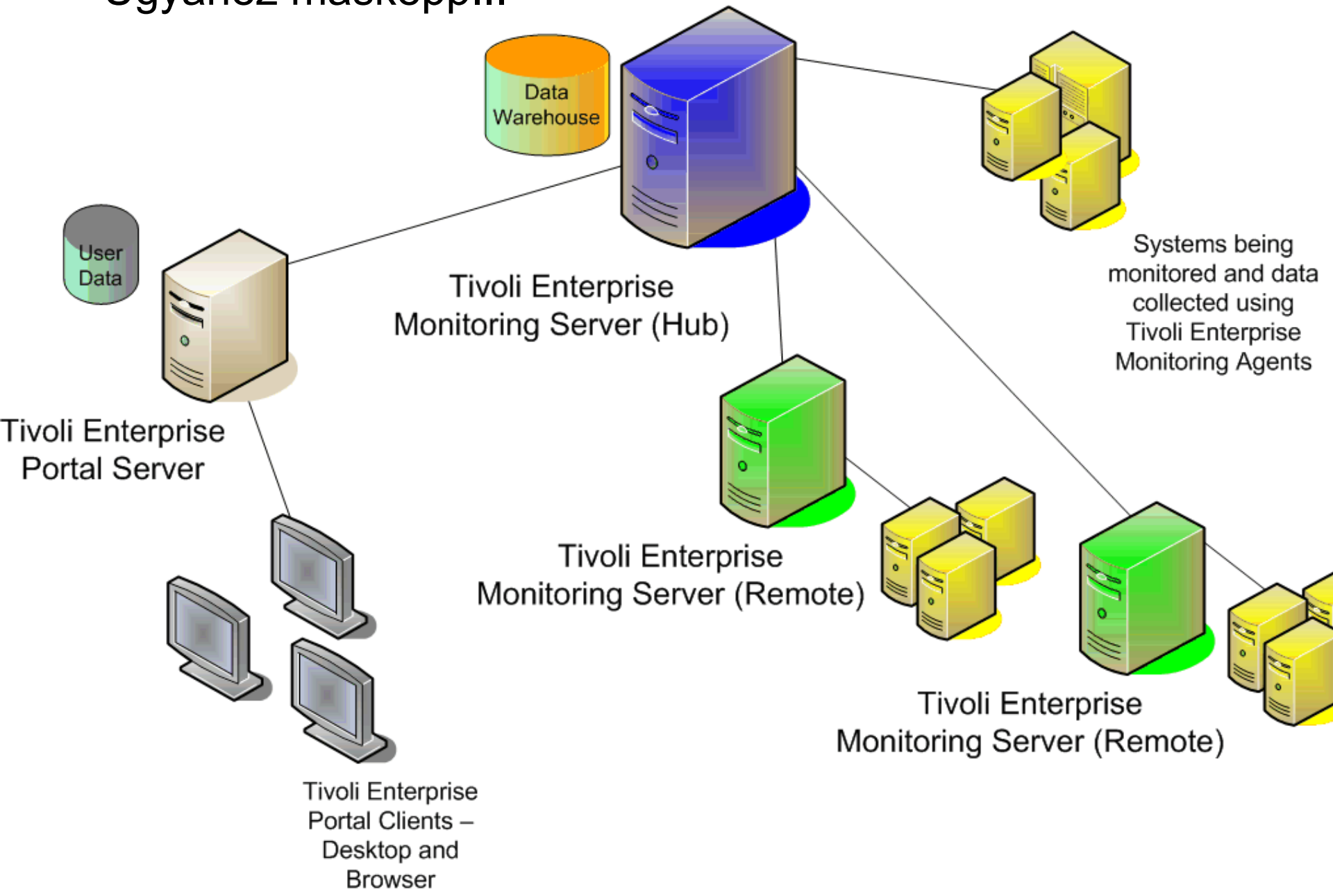
Tivoli Enterprise Monitoring Server
Tivoli Enterprise Portal Server
Warehouse Proxy
Tivoli Data Warehouse

Agents

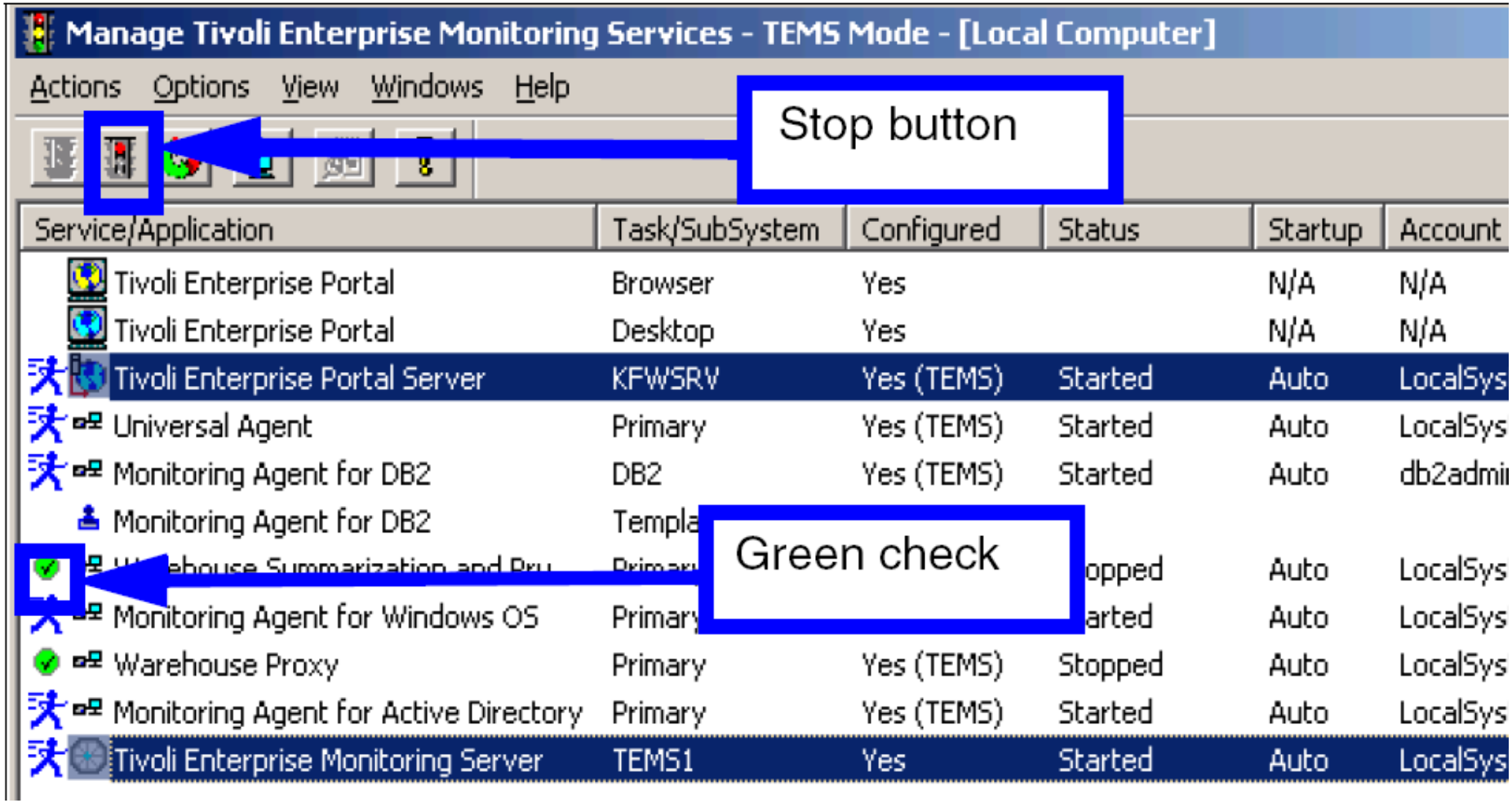
OS Agent
Universal Agent
Unix Log agent
Active Directory

500
Monitoring
Agents

Ugyanez másképp...

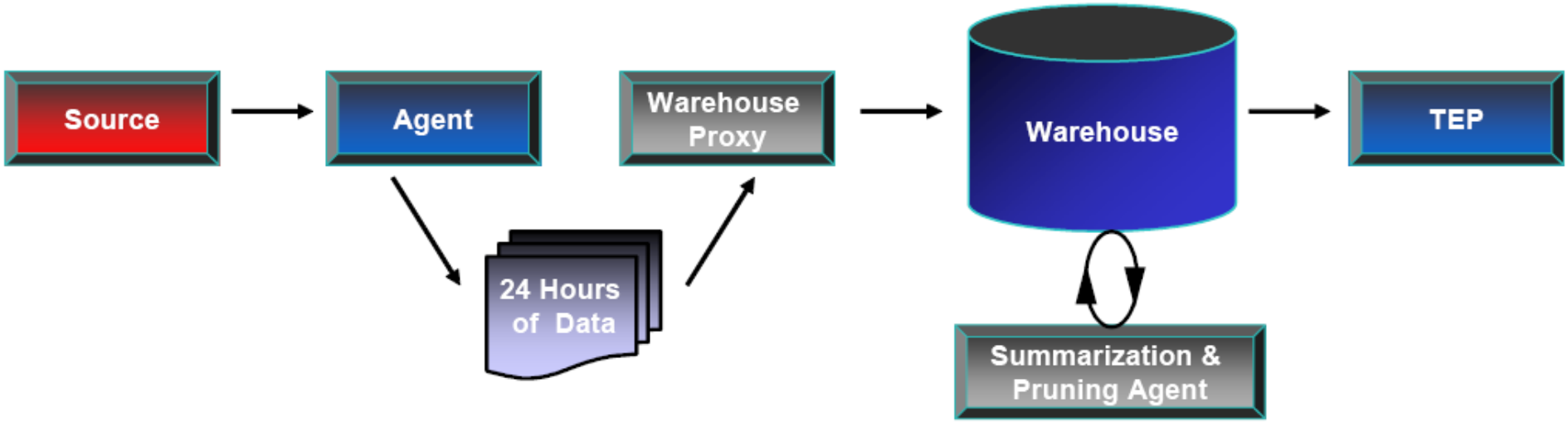


IBM Tivoli Monitoring - services



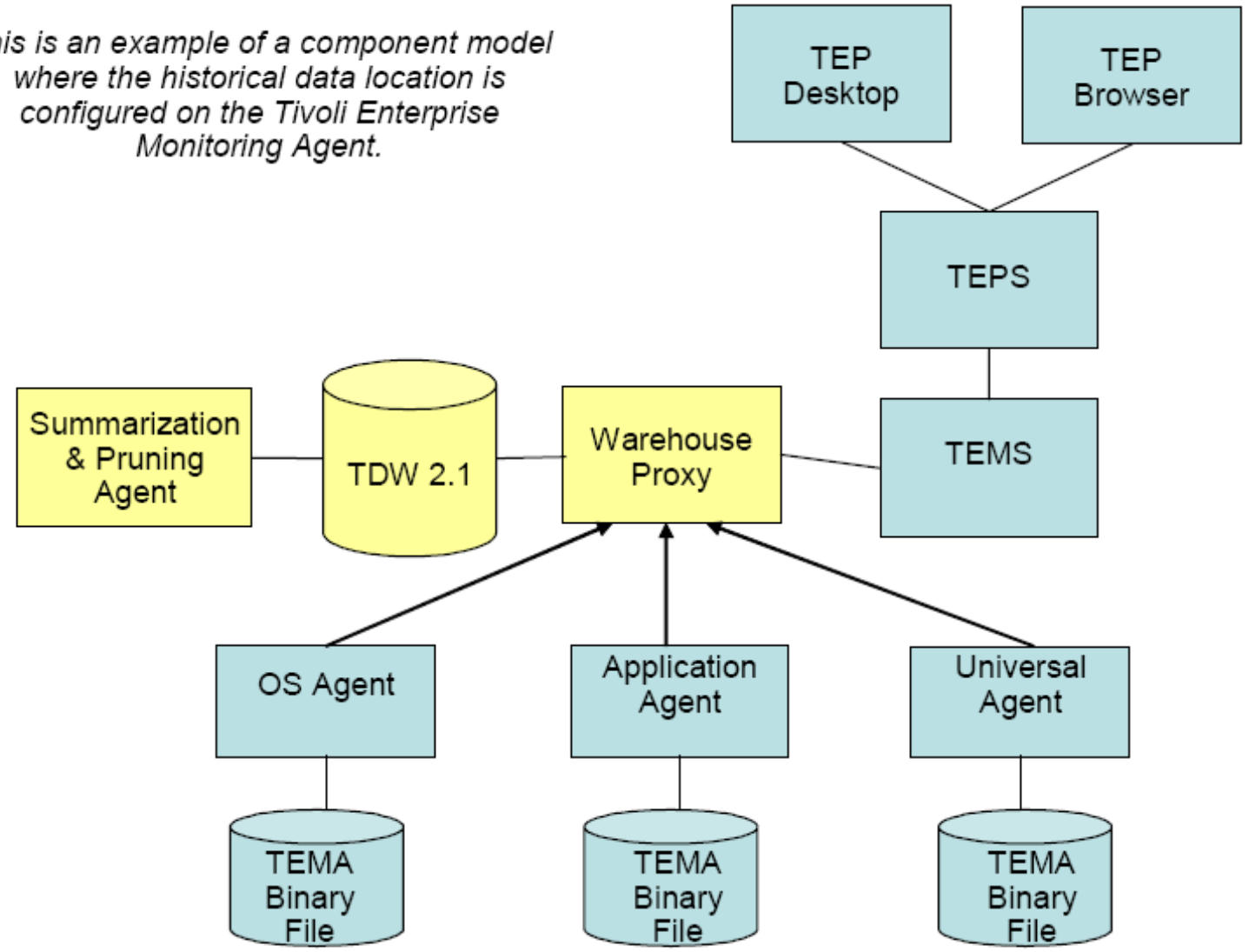
IBM Tivoli Monitoring

Historical Data Collection



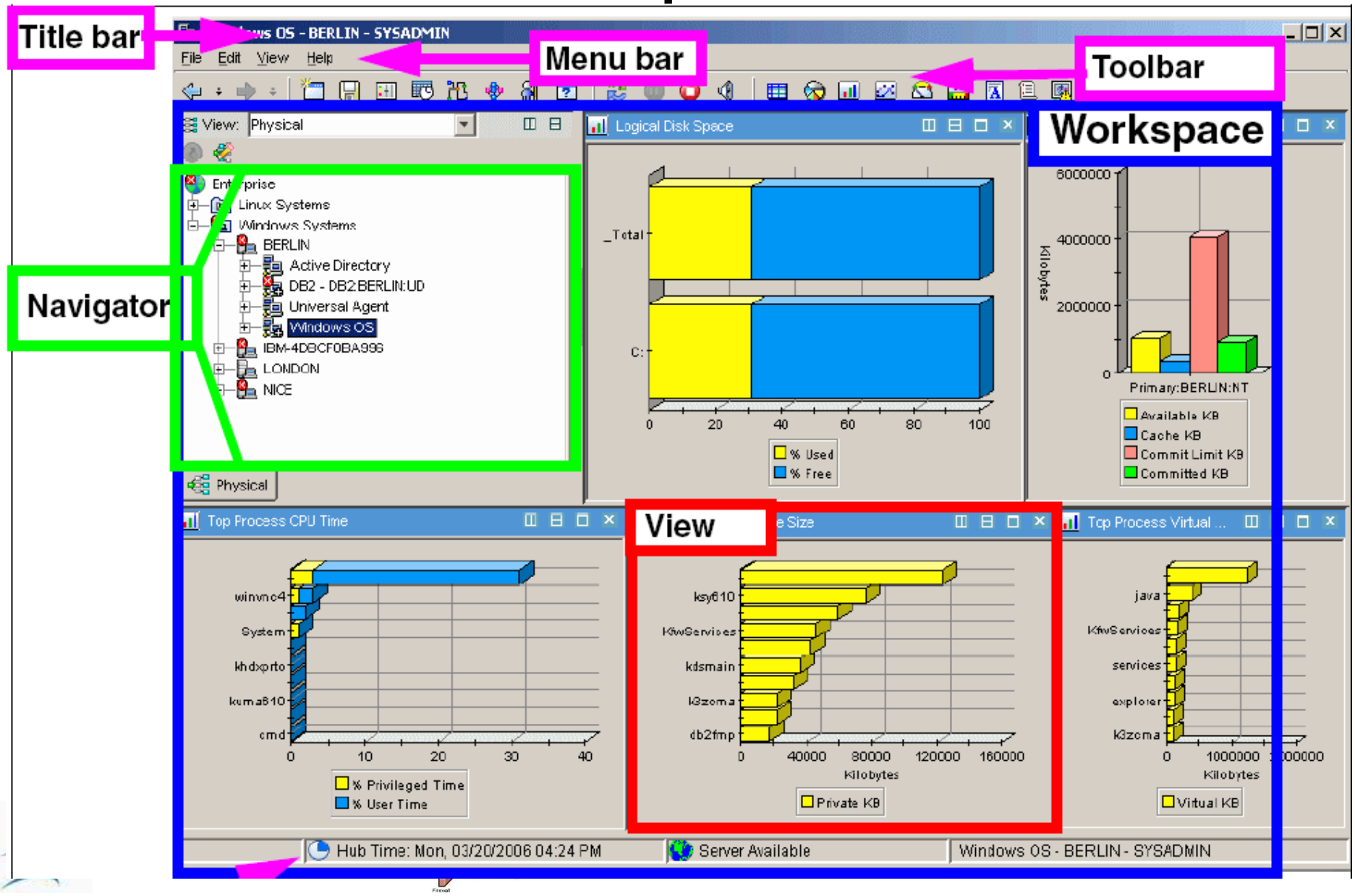
TEP = Tivoli Enterprise Portal

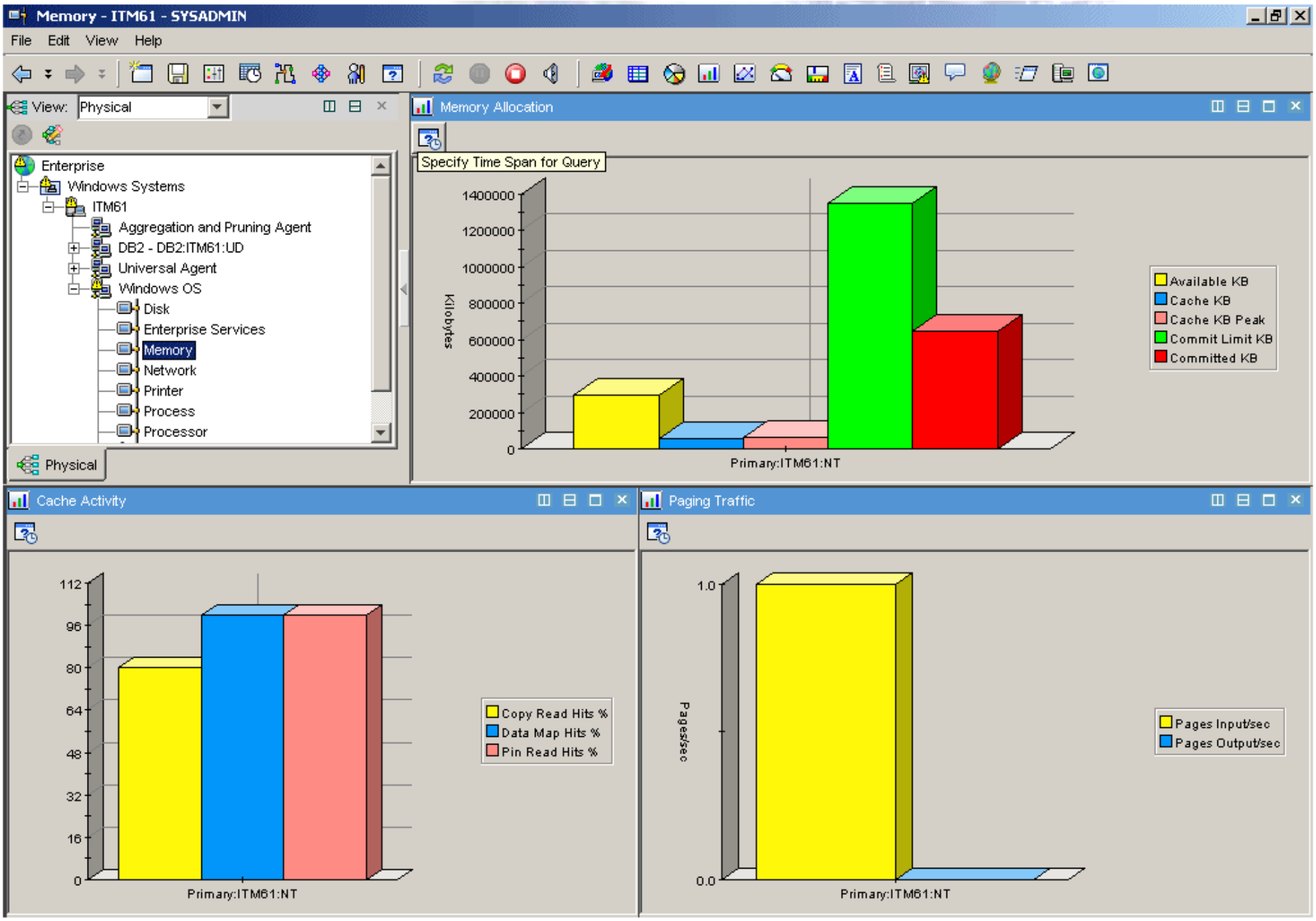
This is an example of a component model where the historical data location is configured on the Tivoli Enterprise Monitoring Agent.



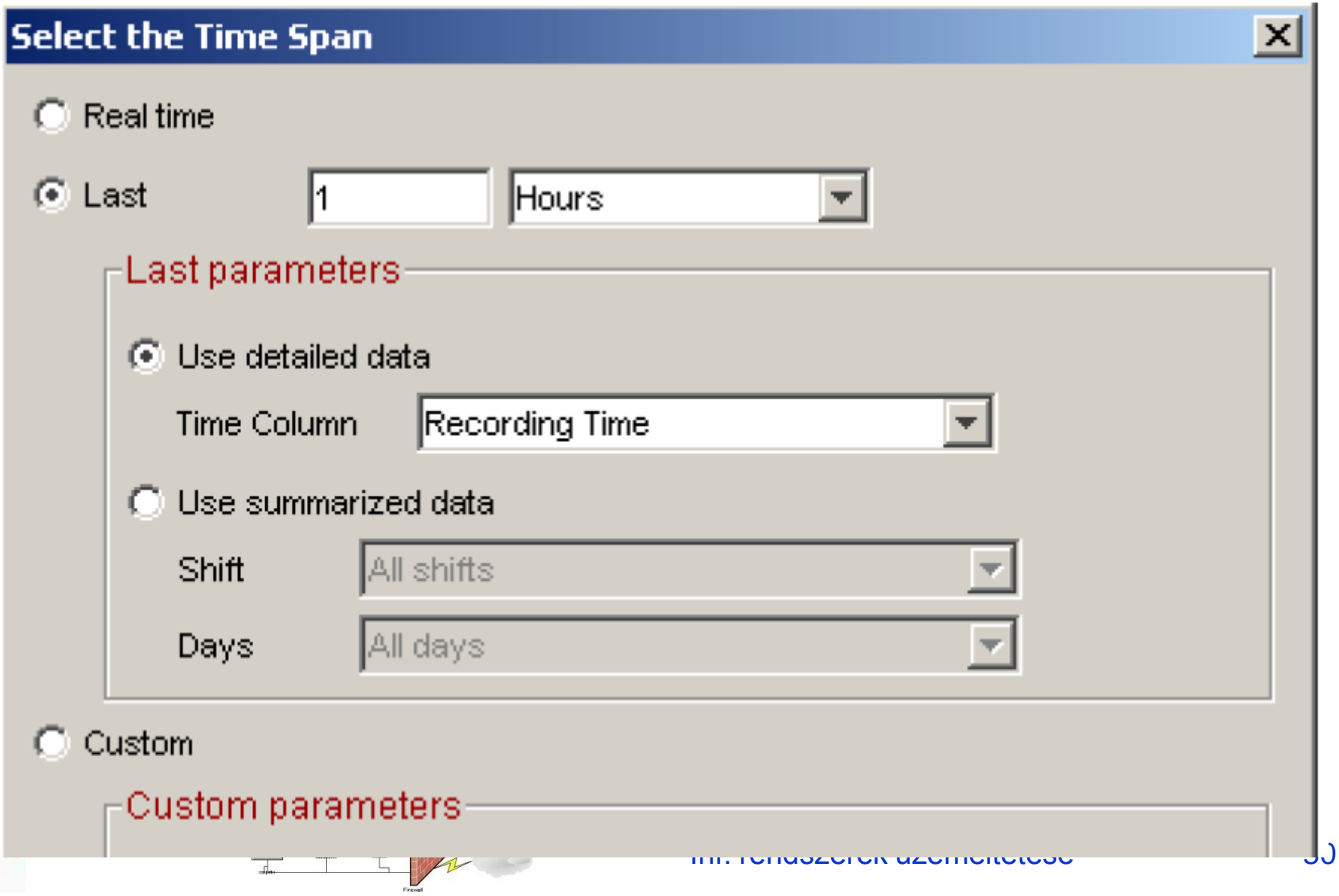
TEMA = Tivoli Enterprise Monitoring Agent
TDW = Tivoli Data Warehouse
TEPS = Tivoli Enterprise Portal Server
TEMS = Tivoli Enterprise Monitoring Server

Tivoli Enterprise Portal

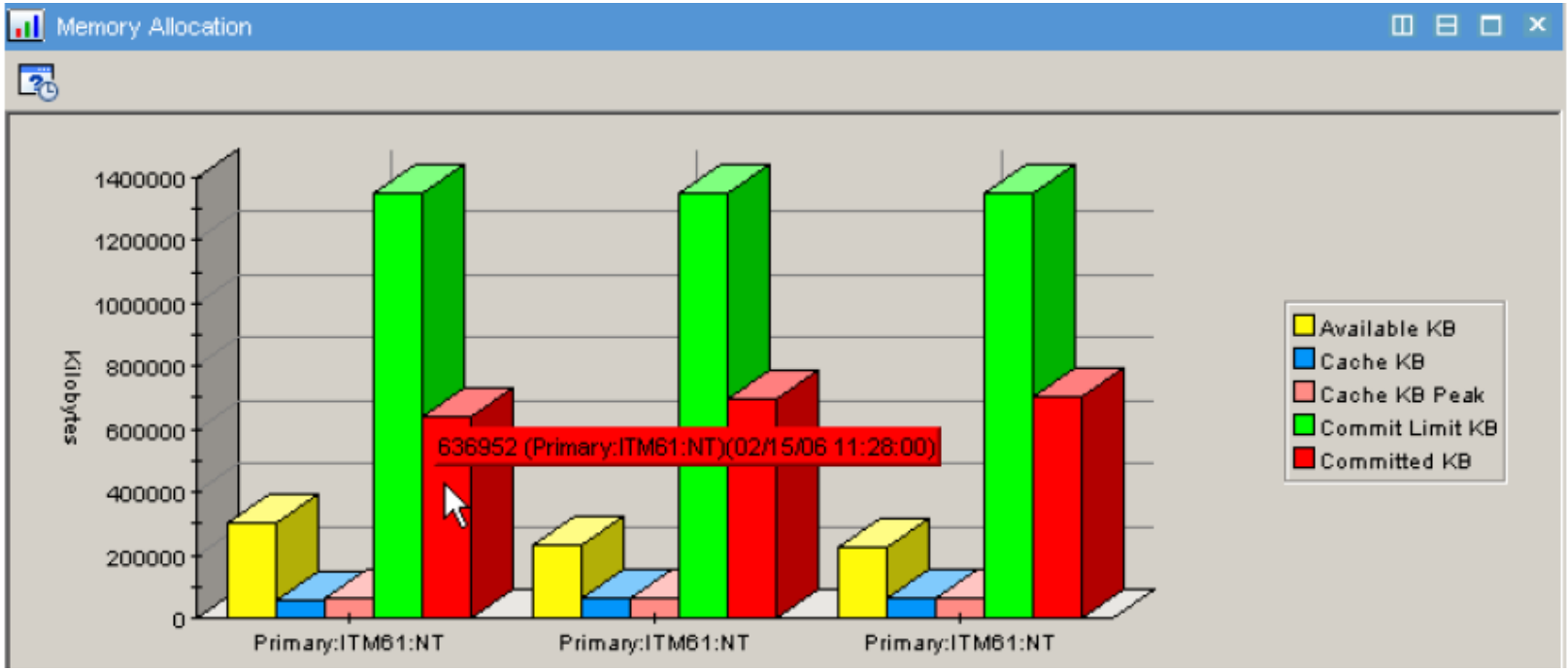



Memory - ITM61 - SYSADMIN
File Edit View Help
View: Physical
Enterprise
Windows Systems
ITM61
Aggregation and Pruning Agent
DB2 - DB2:ITM61:UD
Universal Agent
Windows OS
Disk
Enterprise Services
Memory
Network
Printer
Process
Processor
Physical
Memory Allocation
Specify Time Span for Query
1400000
1200000
1000000
800000
600000
400000
200000
0
Kilobytes
Primary:ITM61:NT
Available KB
Cache KB
Cache KB Peak
Commit Limit KB
Committed KB
Cache Activity
112
96
80
64
48
32
16
0
Primary:ITM61:NT
Copy Read Hits %
Data Map Hits %
Pin Read Hits %
Paging Traffic
1.0
0.0
Pages/sec
Primary:ITM61:NT
Pages Input/sec
Pages Output/sec

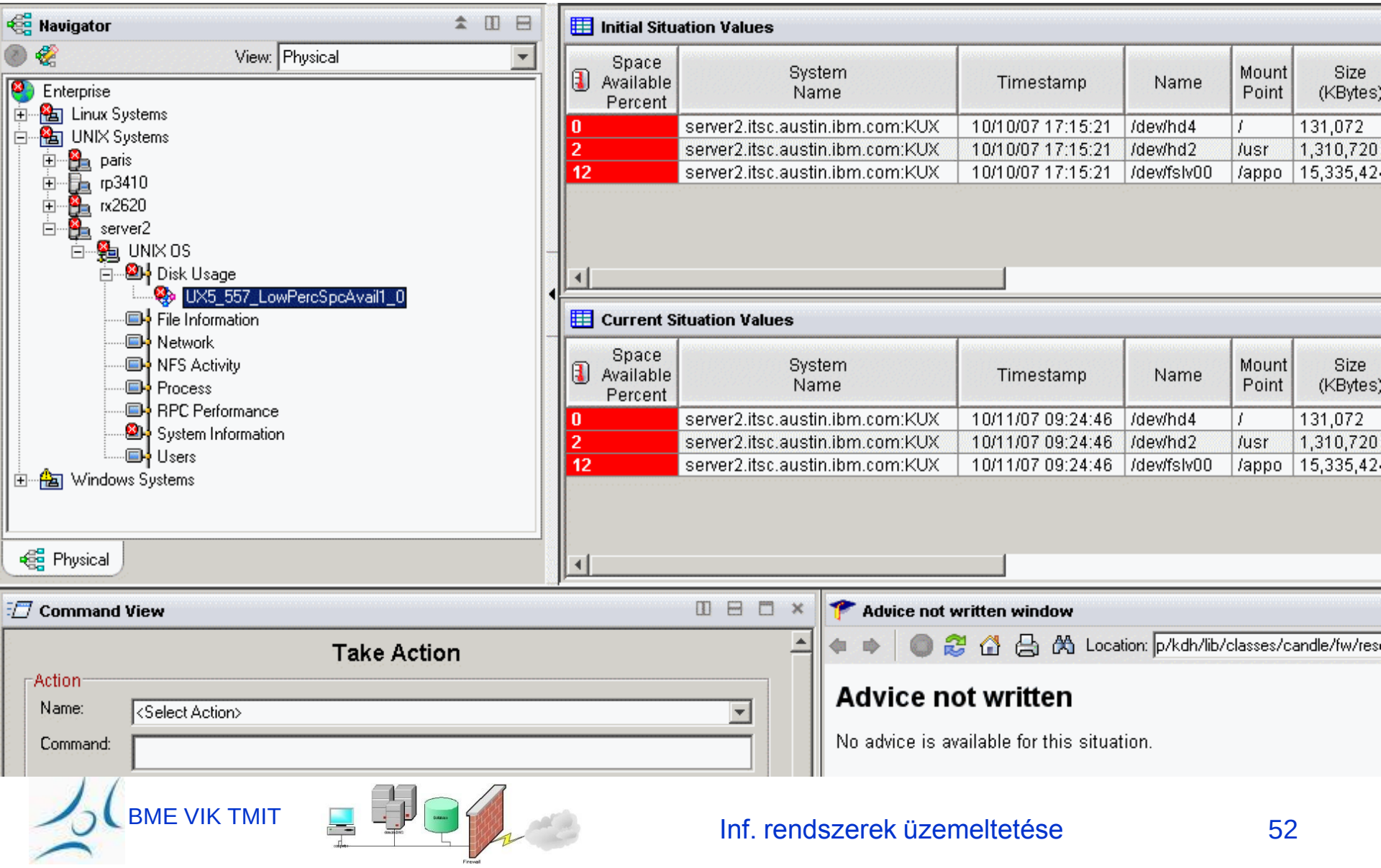
Tivoli Enterprise Portal – megjelenítési időszak

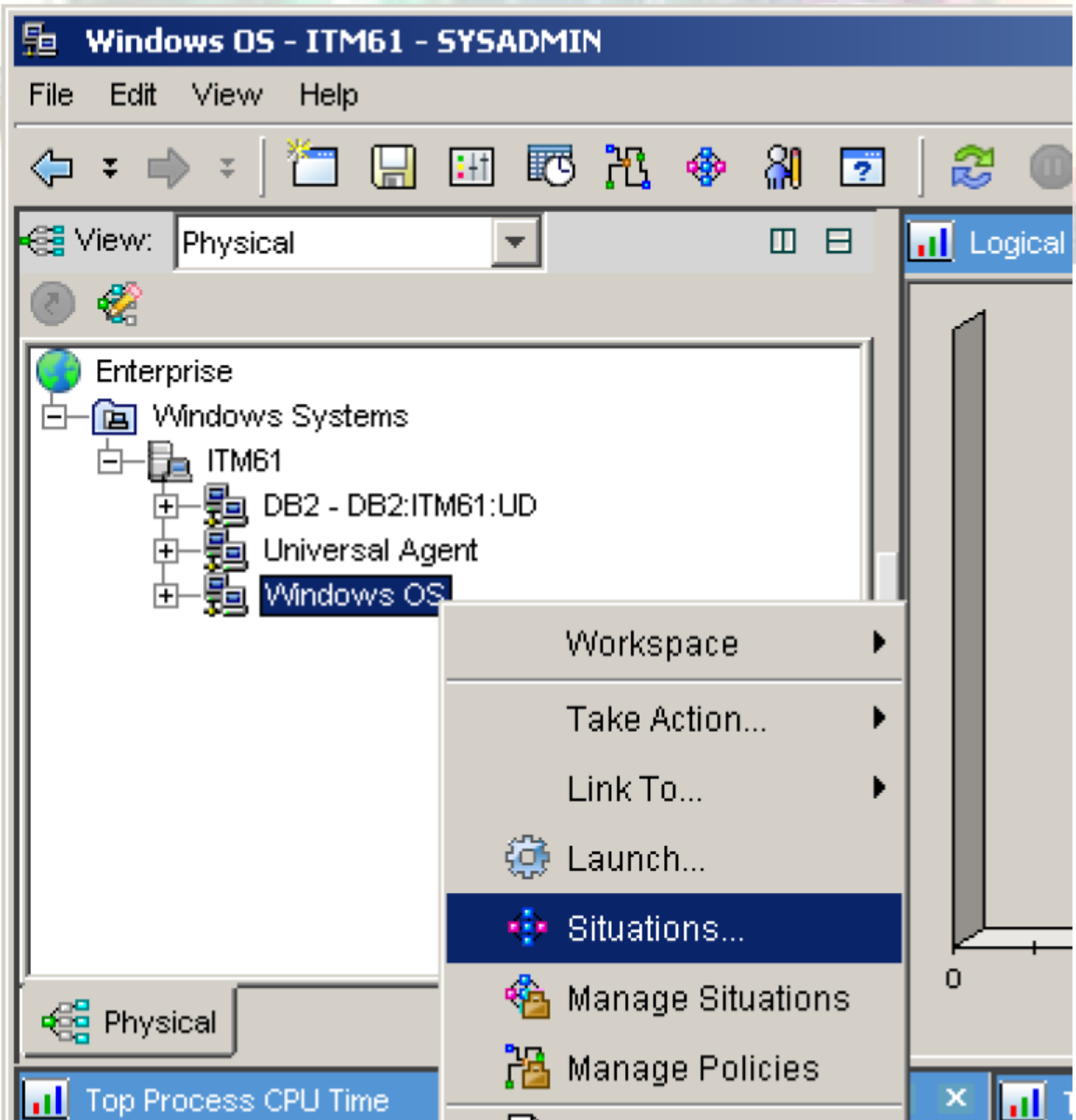


Tivoli Enterprise Portal – több mérés megjelenítése



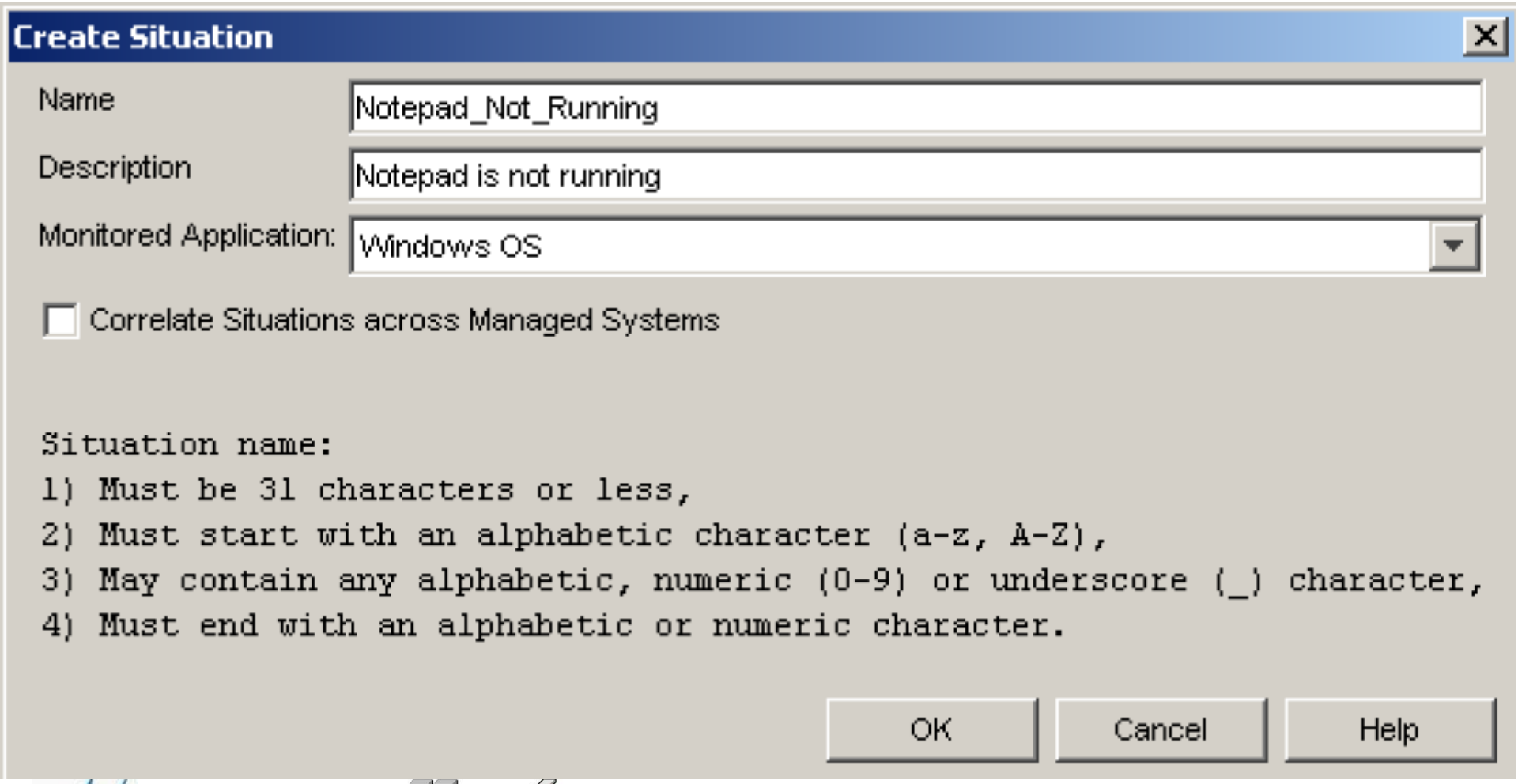
TEP – szitu. (esemény) bekövetkezése

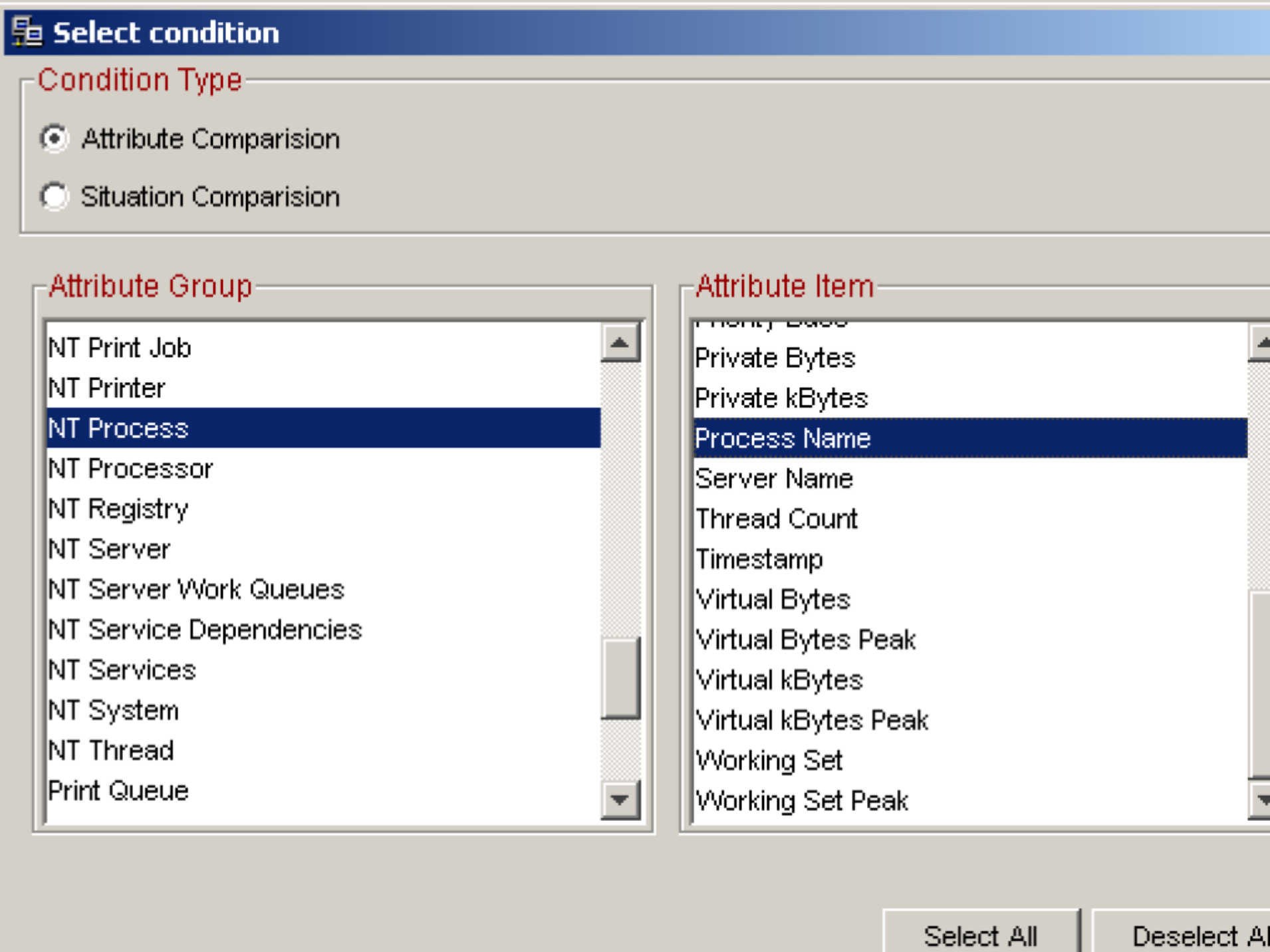




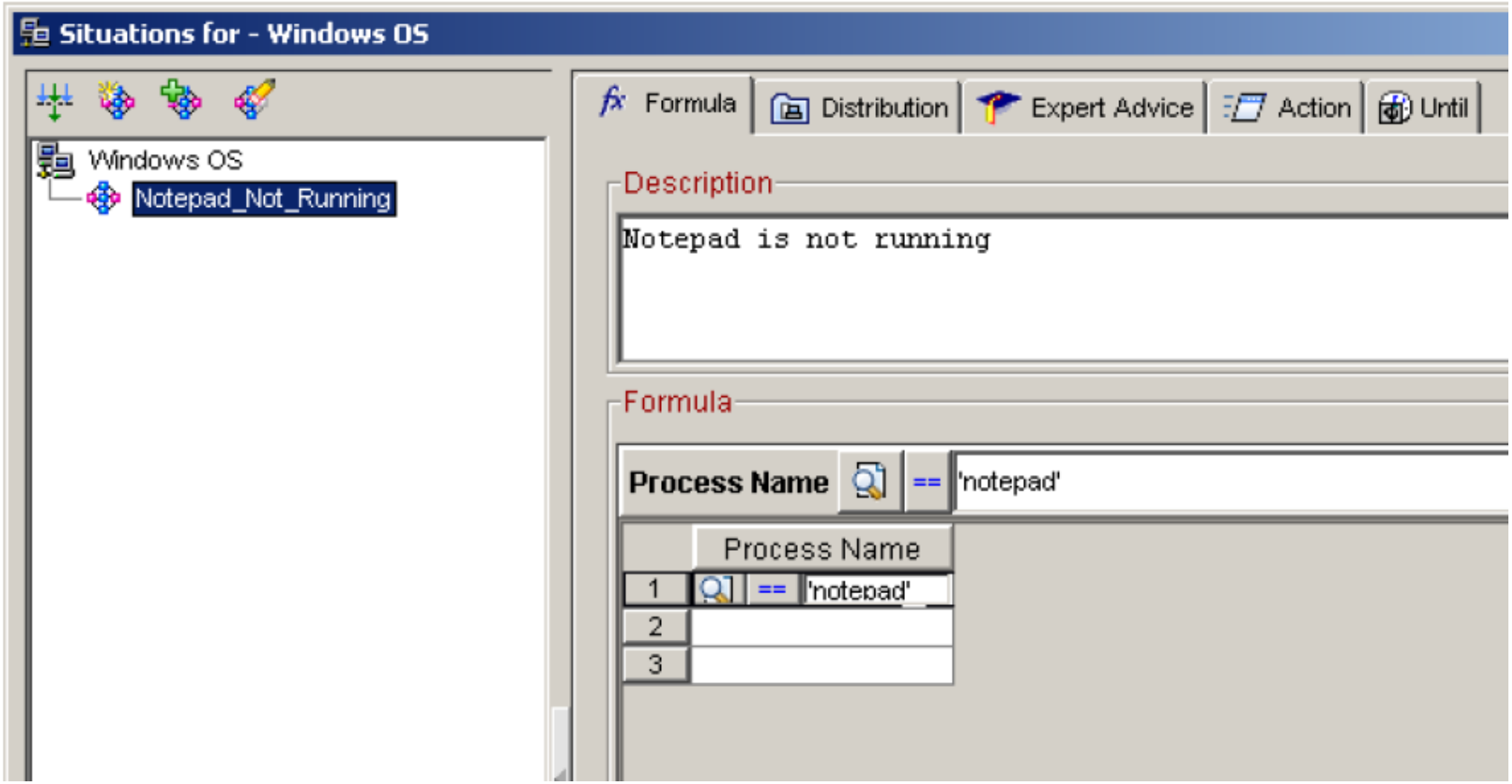
Tivoli Enterprise Portal – szituáció létrehozása

Tivoli Enterprise Portal – szituáció létrehozása 2



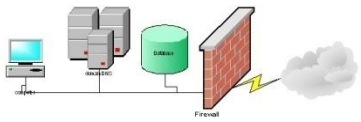

Select condition
Condition Type
Attribute Comparision
Situation Comparision
Attribute Group
NT Print Job
NT Printer
NT Process
NT Processor
NT Registry
NT Server
NT Server Work Queues
NT Service Dependencies
NT Services
NT System
NT Thread
Print Queue
Attribute Item
Private Bytes
Private kBytes
Process Name
Server Name
Thread Count
Timestamp
Virtual Bytes
Virtual Bytes Peak
Virtual kBytes
Virtual kBytes Peak
Working Set
Working Set Peak
Select All
Deselect Al

Tivoli Enterprise Portal – szituáció létrehozása 4



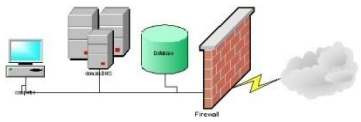
A képernyőképek elküldése

- A *host OS* alól...
- Bármilyen webmail-es alkalmazásból
- Tömörítve! (.zip)
- iru.bme@gmail.com



1.

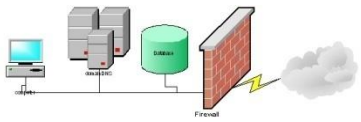
Az információs rendszerek életciklusa



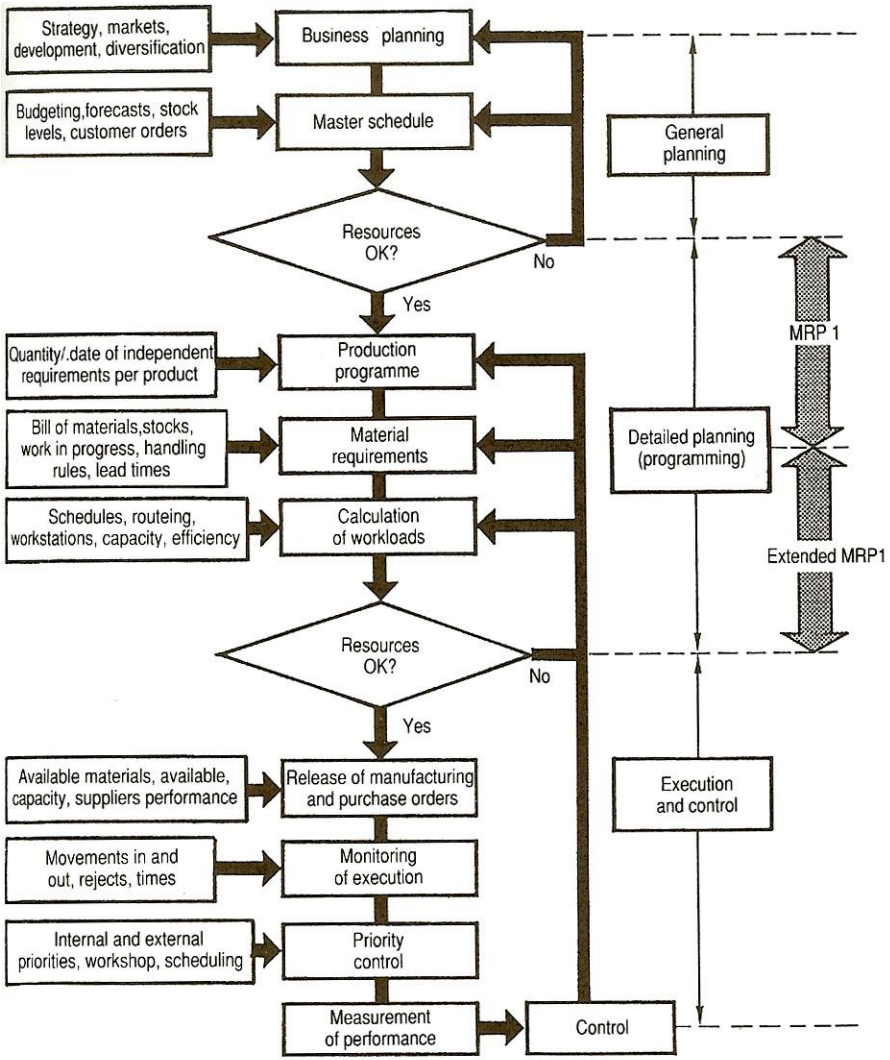
Vállalatirányítási rendszerek

- Mit jelent egy vállalat-irányítási rendszer?
  - Ismerni a pénzügyeket
  - Követni az anyagmozgást, gyártást, szállítást
  - Modellezni a piaci változásokat, stb.

- Ma már kizárólag számítógépes hálózatokon megvalósított információs rendszereket használunk



- Egy vállalatirányítási rendszer sematikus folyamatábrája.
- Mindezt komplex számítástecnika támogat(hat)ja.

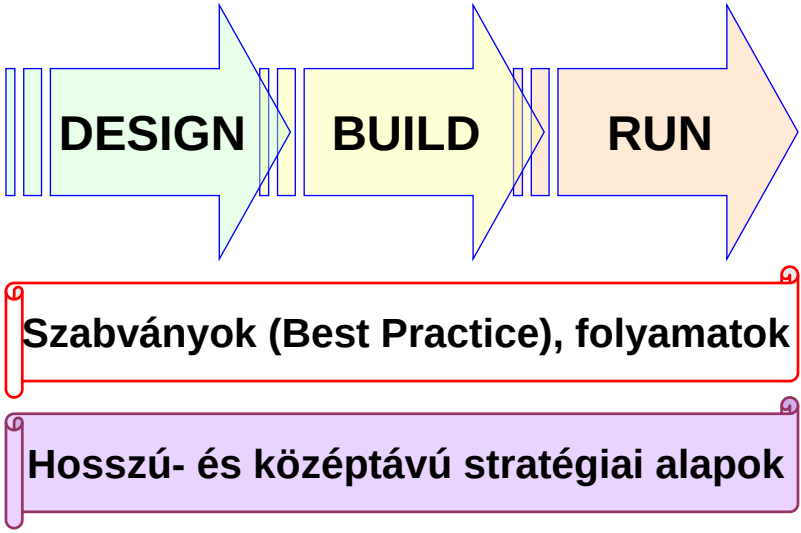


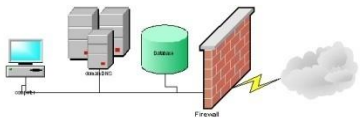
Around 1980, over-frequent changes in sales forecasts, entailing continual reajustments in production, as well as the unsuitability of the parameters fixed buy the system, led MRP (Material Requirement Planning) to evolve into a new concept : Manufacturating Resource Planning or MRP2

Source : "CIM: Principles of Computer Integrated Manufacturing", Jean-Baptiste Waldner, John Wiley & Sons, 1992. Reproduced with author's authorization

Egy információs rendszer nem magától alakul ki...

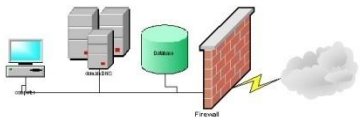
- Sok lépcső kell ahhoz, hogy egy információs rendszer elkészüljön.
- Ha elkészült, önálló életet él: változik, elromlik, kiváltják esetleg egy másikkal (jobbal)
- Információs rendszer csak felhasználóval és támogatóval (rendszergazda, rendszertervező) együtt értelmezhető.





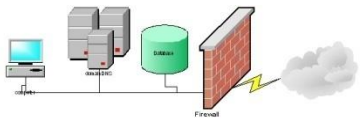
Az információs rendszerek kialakulásának fontosabb lépései

- Felhasználói igénybejelentés („szükségem lenne egy…)
- Igényfelmérés, amikor a felhasználótól még az ő nyelvén begyűjtjük hogy mit is szeretne
- Specifikáció, amikor az igényéből már egy informatikai és felhasználói nyelven megírt anyagot kapunk. (Ez még nem programnyelv.)
- Megvalósíthatósági tanulmány. Ebben az esetben már informatikai emberek készítik el a kért alkalmazás lehetséges alternatíváit. Ez esetleg több iterációs lépcsőn mehet át a felhasználóval.
- Specifikáció lezárása. Ezen fázis után már IT emberek dolgoznak a feladaton.



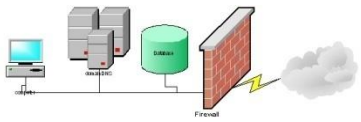
Az információs rendszerek kialakulásának fontosabb lépései (2)

- Alkalmazás megtervezése, amikor IT szakemberek (tervezők és leendő üzemeltetők közösen) megtervezik hogyan és milyen módon épüljön fel az alkalmazás.
- Kódolás. Programozók, esetleg sok csapatban, megfelelő változásmenedzsmenttel megtámogatva, elkezdik elkészíteni az alkalmazást.
- Belső tesztelések.
- Felhasználói tesztelés. Több lépcsőben, többszörös iterációval a felhasználók egy kiválasztott csoportjával készül.



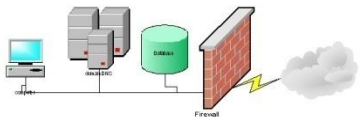
Az információs rendszerek kialakulásának fontosabb lépései (3)

- Üzemeltetői tesztelés (a fentivel együtt is mehet)
- Korrekciók.
- Végső tesztelés, átvétel.
- Üzembe helyezési terv elkészítése (visszaállási tervekkel)
- Go live.
- Babysitting: az esetleges felmerülő hibák azonnali megoldására IT szakemberek folyamatos jelenléte.
- Üzemeltetés.



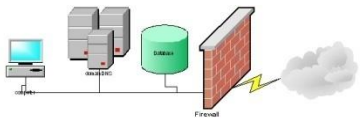
Az információs rendszerek kialakulásának fontosabb szereplői

- Felhasználó (körülötte forog a világ)
- Folyamattervező (inkább business mint IT)
- Rendszertervező (valahol az IT és a business között, IT beütéssel)
- Programozó
- Tesztelő
- Üzemeltető (rendszer adminisztrátor)



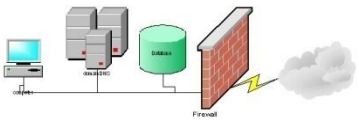
Életciklus

Egy rendszer teljes élettörténete az ötlet megszületésétől a használatból való kivonásig.

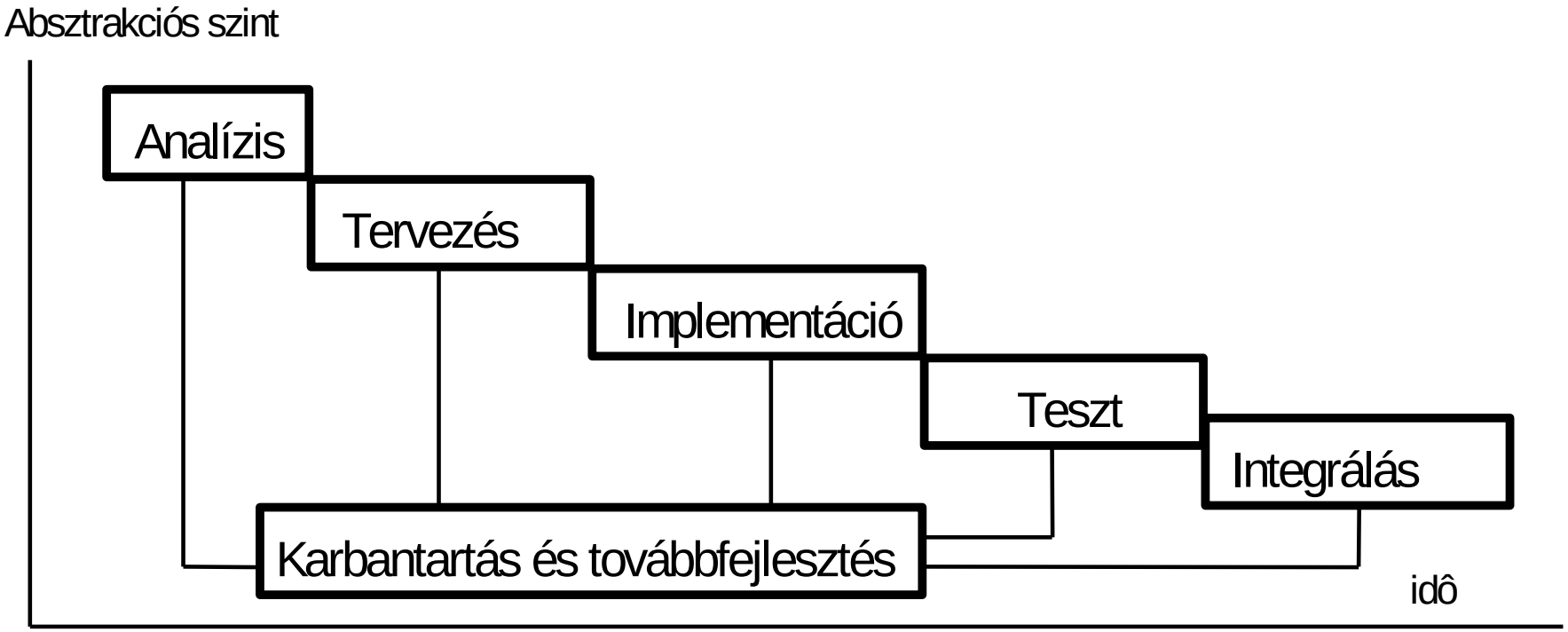


Életciklusban gondolkodó módszertanok

- Az életciklus valamennyi fázisában:
  - a rendszer kezelhető részekre bontása,
  - munkafázisok elkülönítése,
  - megtervezése,
  - átgondolt dokumentálás.



Vízesés modell



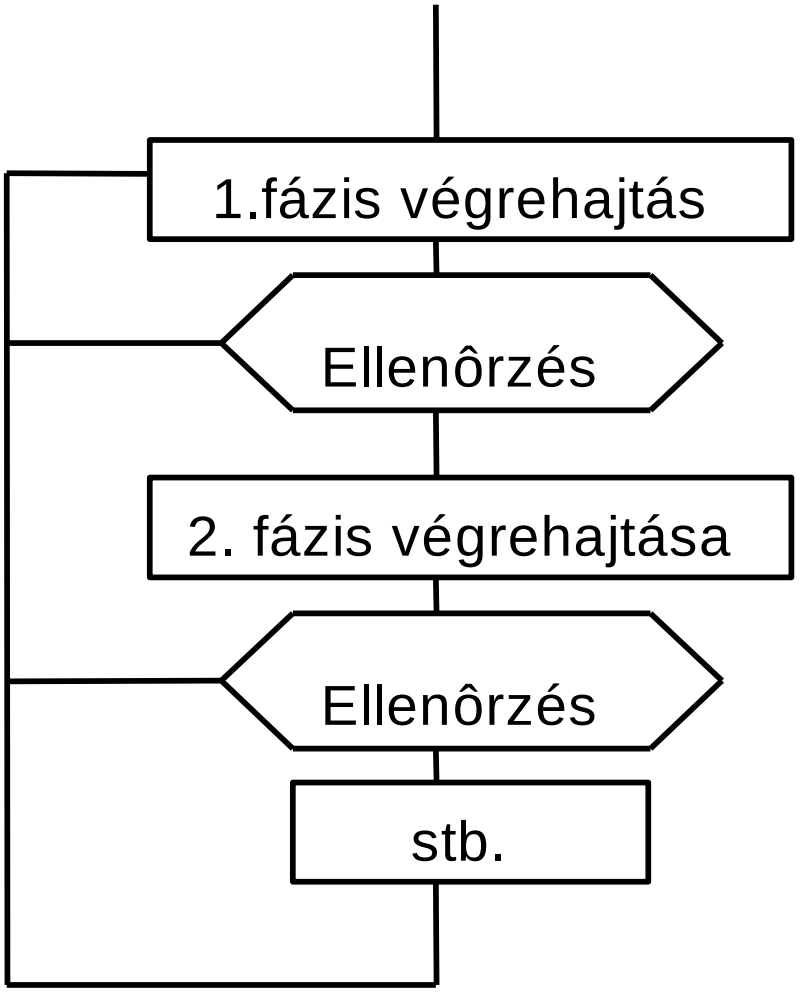
Vízesés modell

- Az egyes fázisok végén döntési pontok (mérföldkövek):

  - helyesek-e az addigi megoldások,

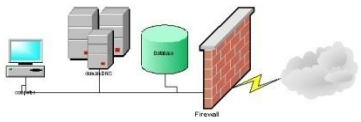
  - folytatható-e a munka a következő fázissal?

  (top-down megközelítés)



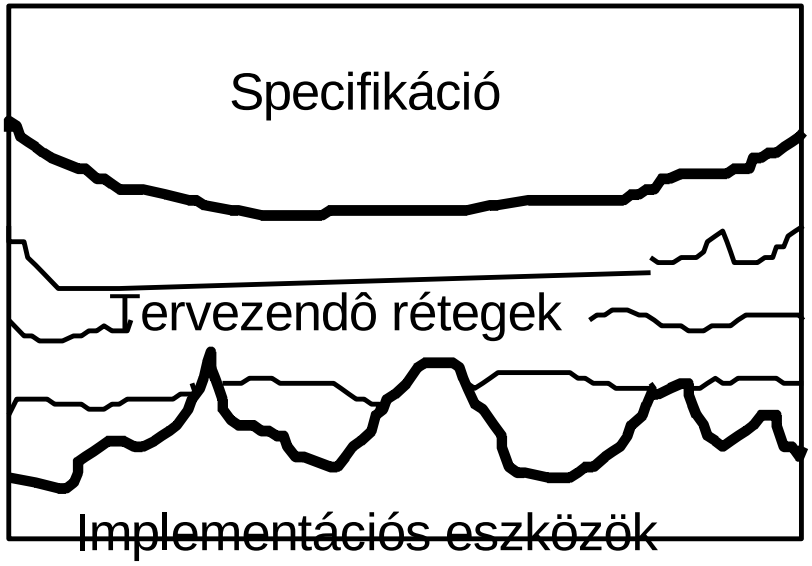
Vízesés modell

- A fázisok szigorúan egymást követik, különállóak, éles határvonal választja el őket. Egy tevékenység csak akkor kezdődhet, ha az őt megelőző már véget ért.
- Módosított változatok
  - az egyes lépések után ellenőrzés (validáció, verifikáció, visszalépési lehetőség)
  - a fázisok után mérföldkövek, előírt dokumentáció
  - kiterjesztés a rendszerfelügyeletre
  - logikai és fizikai tervezés szétválasztása

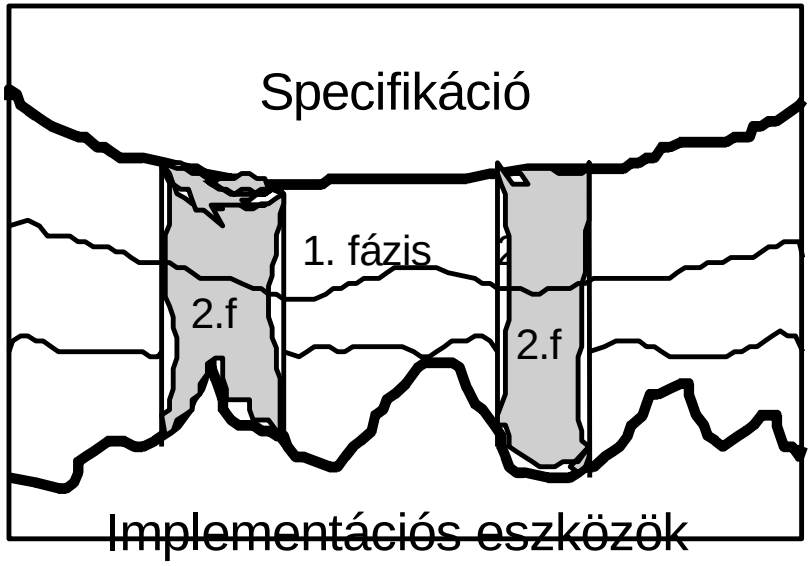


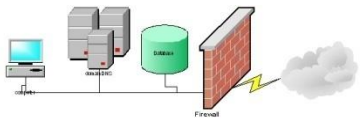
Prototípus modell

Vízesés modell

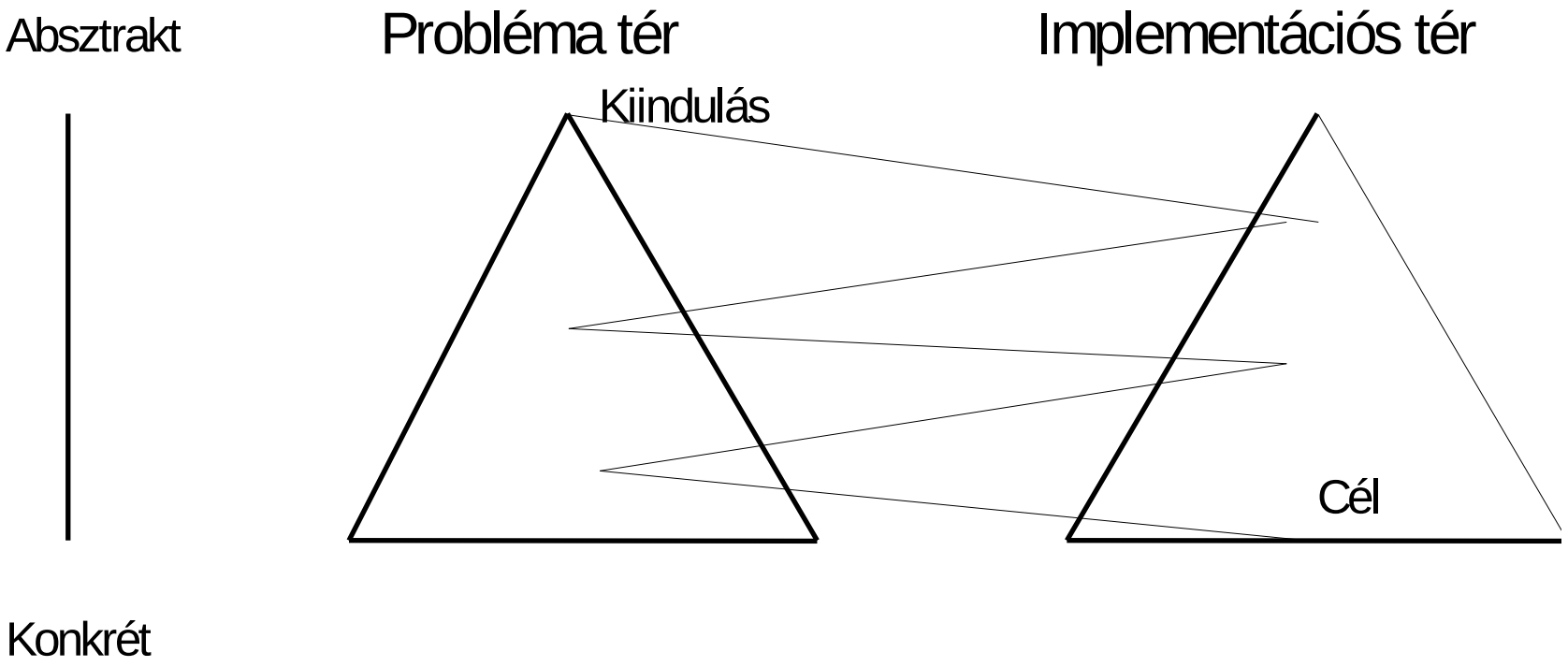


Prototípus modell

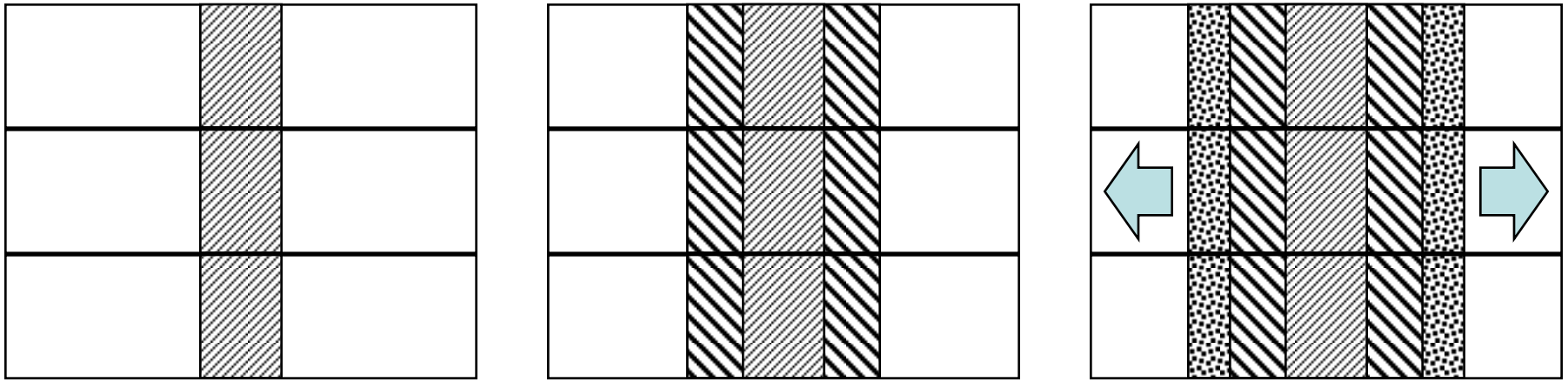




Inkrementális modell

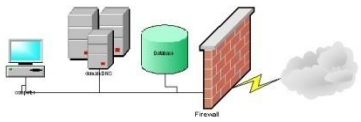


Inkrementális modell

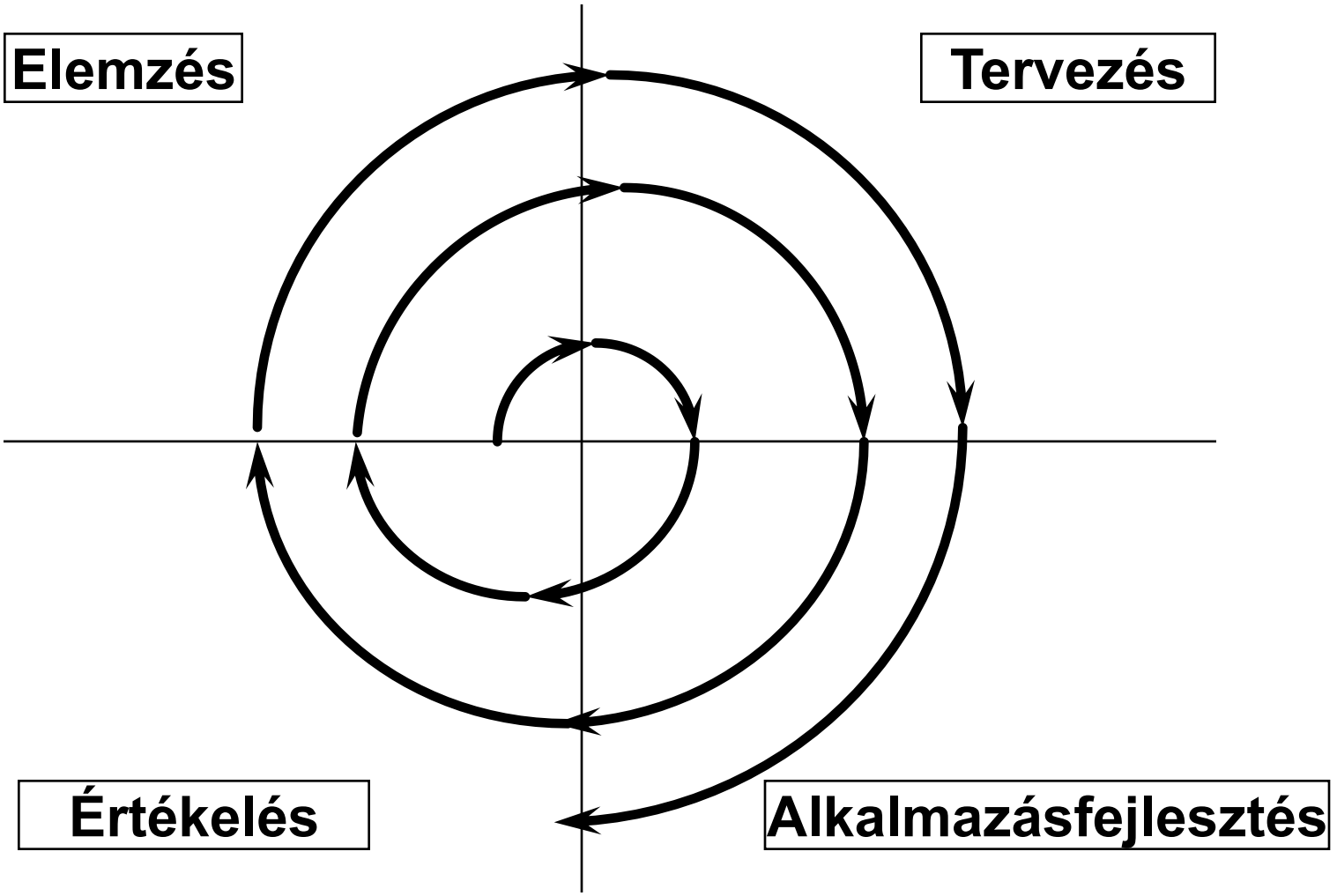


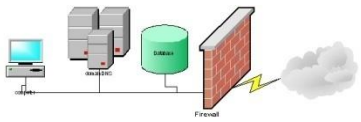
Inkrementális modell

- Előnyök
  - gyorsan készül működő rész
  - kisebb kockázat, az igények fokozatos közelítése
  - bizonytalan esetben is alkalmazható
- Hátrányok
  - Lassan készül el teljes rendszer
  - Soklépéses folyamat



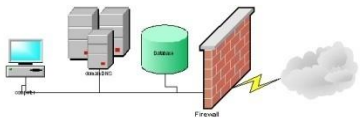
Spirálmodell





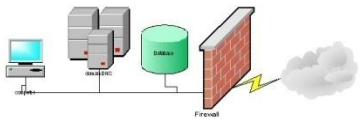
Spirálmodell

- Előnyök
  - kis kockázat
  - kezelhető a felhasználó bizonytalansága
  - kezelhető a fejlesztő bizonytalansága
- Hátrányok
  - hosszabb tervezési szakasz
- Alkalmazás
  - kockázatos, sok alternatívát tartalmazó esetekben



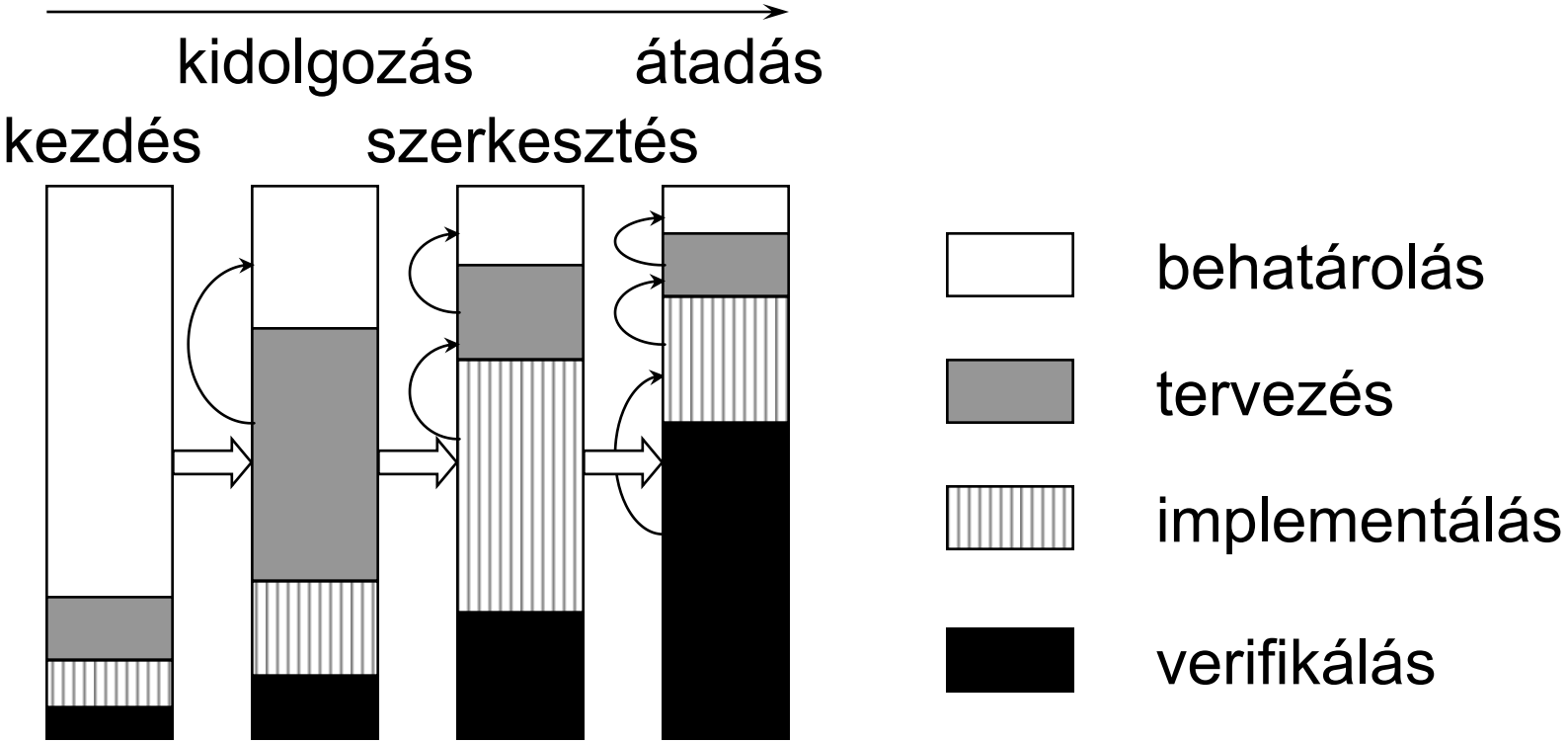
Érettség modell

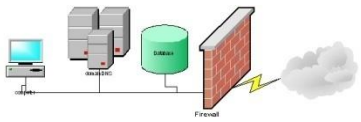
- Alapötlete:
  „érettségi átmenet” a probléma-megoldási fázisok között.
- Ellenőrzött iteráció



Érettség modell

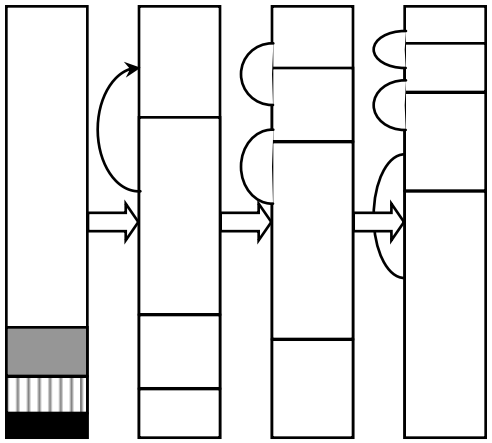
- Fázisok és átmeneteik (érettség alapján):
  - Fázis tevékenység
  - („a problémamegoldás fázisai”)

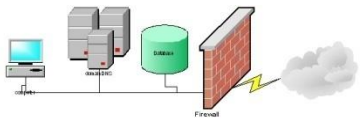




Érettség modell / 1. fázis: kezdés

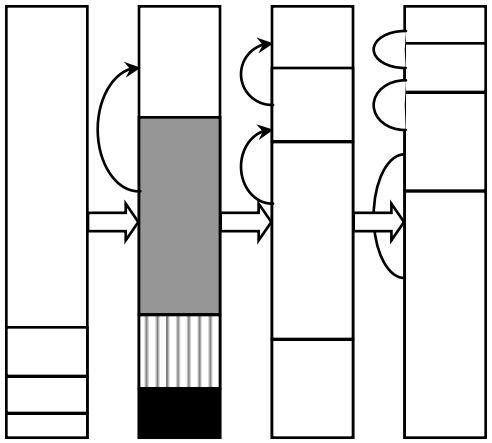
- Cél: a feladat megértése illetve behatárolása
- Bemenet:
  a feladatról fellelhető információk
- Kimenet:
  elsődleges elképzelés a megoldásról, közös definíciók

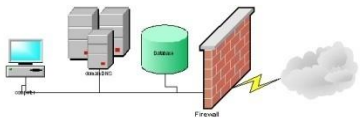




Érettség modell / 2. fázis: kidolgozás

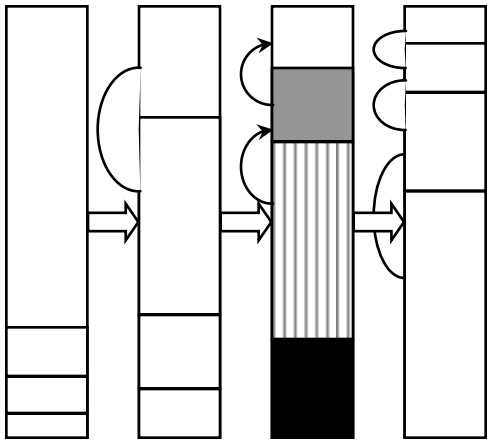
- Cél: a megoldás menetének kidolgozása
- Bemenet: 1. fázis + tervezési adatok, elemzések, stb.
- Kimenet: véleményegyezés, tervek (logikai, fizikai) + az implementálás első lépései (!)
- Iterációs lehetőségek.

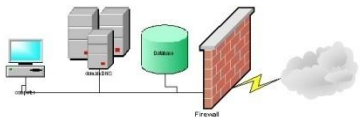




Érettség modell / 3. fázis: szerkesztés

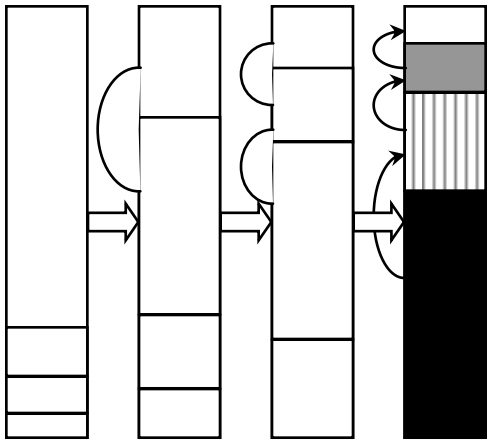
- Cél: a probléma megoldása
- Bemenet:
  2. fázis + újabb adatok
- Kimenet:
  implementálás (működő verzió) + részleges tesztelés, verifikálás

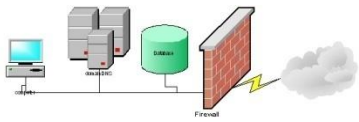




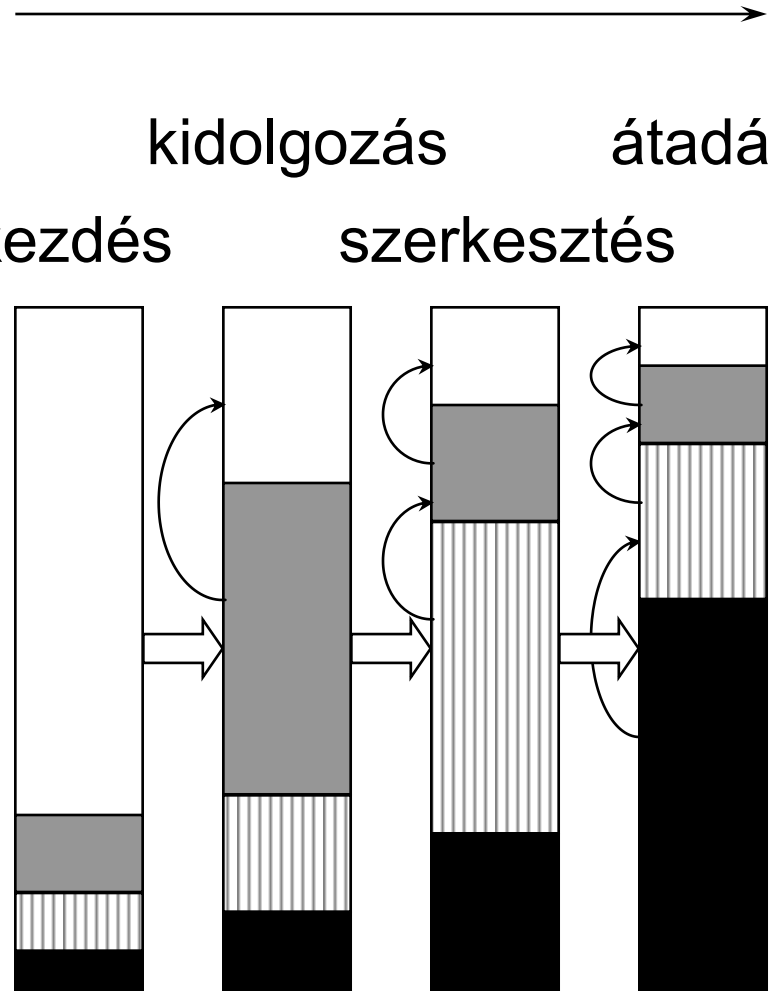
Érettség modell / 4. fázis: átadás

- Cél: a megoldás átadása a megrendelőnek
- Bemenet: 3. fázis + próbák, tesztek eredményei, felhasználói reakciók
- Kimenet: átalakított, bevezetett termék, illesztések a megrendelőnél



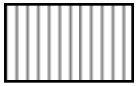


Érettség modell / Összefoglalás

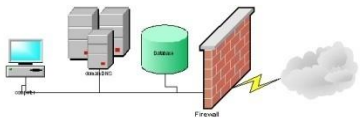



behatárolás

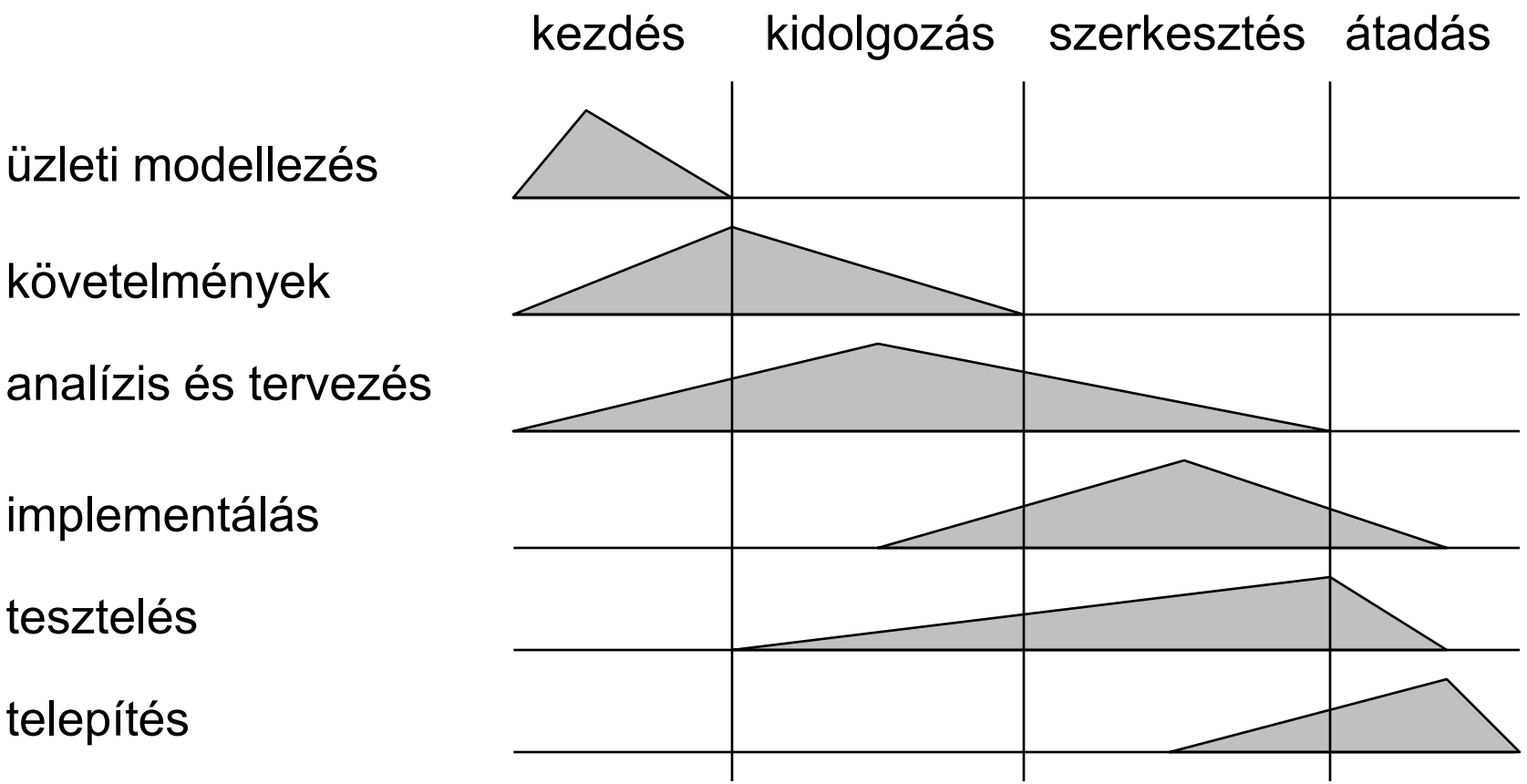

tervezés

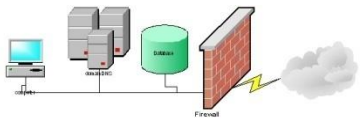

implementálás


verifikálás



Érettség modell / Ütemezés





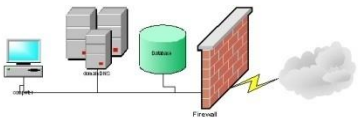
Tanulságok

Az életciklusban gondolkodás azért hasznos, mert

- mások tapasztalatára építhetünk,
- módszeresen végig gondoljuk keretében a feladatokat.

Különböző típusú feladatokhoz más-más életciklus modell illik

(más egy prototípus létrehozása, más egy nagy rendszer kisebb továbbfejlesztése).

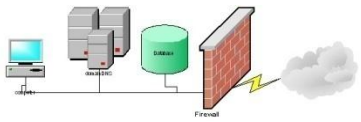


Információs rendszerek üzemeltetése

Adamis Gusztáv – TMIT

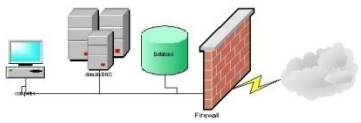
IE 344

adamis@tmit.bme.hu



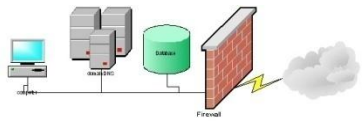
I. rész

Korábban tanultak áttekintése



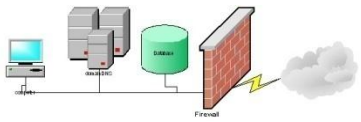
Korábban tanultak áttekintése

- Korábbi tárgyakban tanultak
  - amik az IRÜ-ben is fontosak
- Persze, mindannyian tudjátok
  - biztos???



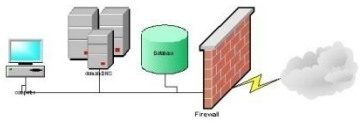
Ismétlés

- Referencia modell, protokollok
- IP alapok
  - címek, címosztályok
  - DHCP
  - ARP/RARP
  - NA(P)T
  - DNS
  - ICMP



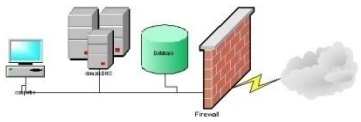
Ismétlés

- Referencia modell, protokollok
- IP alapok
  - címek, címosztályok
  - DHCP
  - ARP/RARP
  - NA(P)T
  - DNS
  - ICMP



OSI referencia modell

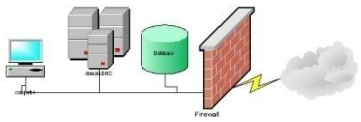
- Hét réteg
  - számítógépek kommunikációjához szükséges hálózati protokollok feladatait határozza meg
  - fő cél: együttműködés különböző gyártók termékei között
- Minden réteg CSAK az alatta levő réteg szolgáltatásaira támaszkodik és a felette levő réteg számára nyújt szolgáltatást
  - protokoll verem (protocol stack)
  - SW / HW / kombinált megvalósítás



Réteg Layer	Név		Funkció
7	Alkalmazási Application	ADATOK	Alkalmazási protokollok, pl. SMTP (e-mail – Simple Mail Transfer Protocol), HTTP (web), FTP (fájl transzfer)
6	Megjelenítési Presentation	ADATOK	Adat megjelenítése és kódolása Adatformátumok (pl. MPEG), karakterkódolás, tömörítés, titkosítás
5	Viszony Session	ADATOK	Kommunikációs viszonylatok vezérlése (SCP – Session Control Protocol)
4	Szállítási Transport	SZEG-MENSEK	Végpontok közötti adatátvitel, megbízhatóság, virtuális áramkörök (pl. TCP kapcsolatok, port számok)
3	Hálózati Network	CSOMA-GOK	Logikai címzés (pl. IP címek) és azon alapuló irányítás, útvonalválasztás (routerek)
2	Adat-kapcsolati Data Link	KERE-TEK	Interfész (MAC) szintű címzés, folyamvezérlés, (bit)hibadetektálás, hibajavítás (bridge, switch)
1	Fizikai Physical	BITEK	Az eszközök közötti fémes vagy optikai átvivő közeg (hub)

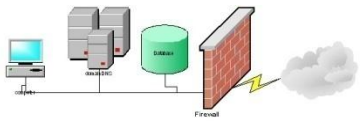
Réteg karakterisztikák

- Minden egyes réteg az alsóbb réteg szolgáltatásait használja valamint saját szolgálatait felajánlja a felsőbb rétegek felé
- Interfész meghatározza a lehetséges kölcsönhatást
- Implementációs részletek rejtve maradnak
  - Megváltoztatható anélkül, hogy befolyásolná a többi réteget (fekete doboz)
- Példák
  - Hálózati topológia és fizikai konfiguráció
  - Útválasztás
  - Új alkalmazások

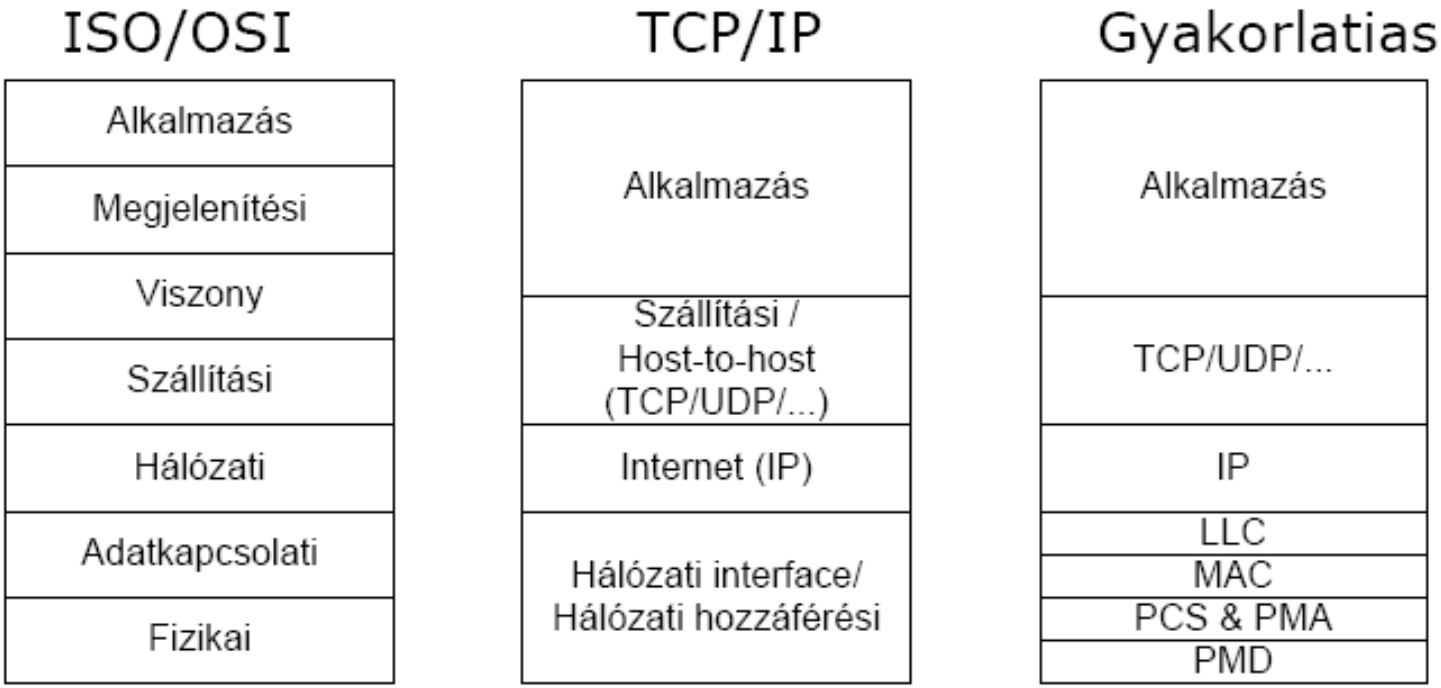


Protokollok

- Modul a réteges struktúrában
- Szabályok gyűjteménye, mely vezényli a kommunikációt hálózati elemek között
- Meghatározzák:
  - Interfészüket magasabb rétegek felé (API)
  - Interfészüket az egyenrangú felek felé (peer)
    - Formátumok (statikus)
    - Üzenet sorrendek, üzenetek kiváltotta cselekvéssorozat (dinamikus)



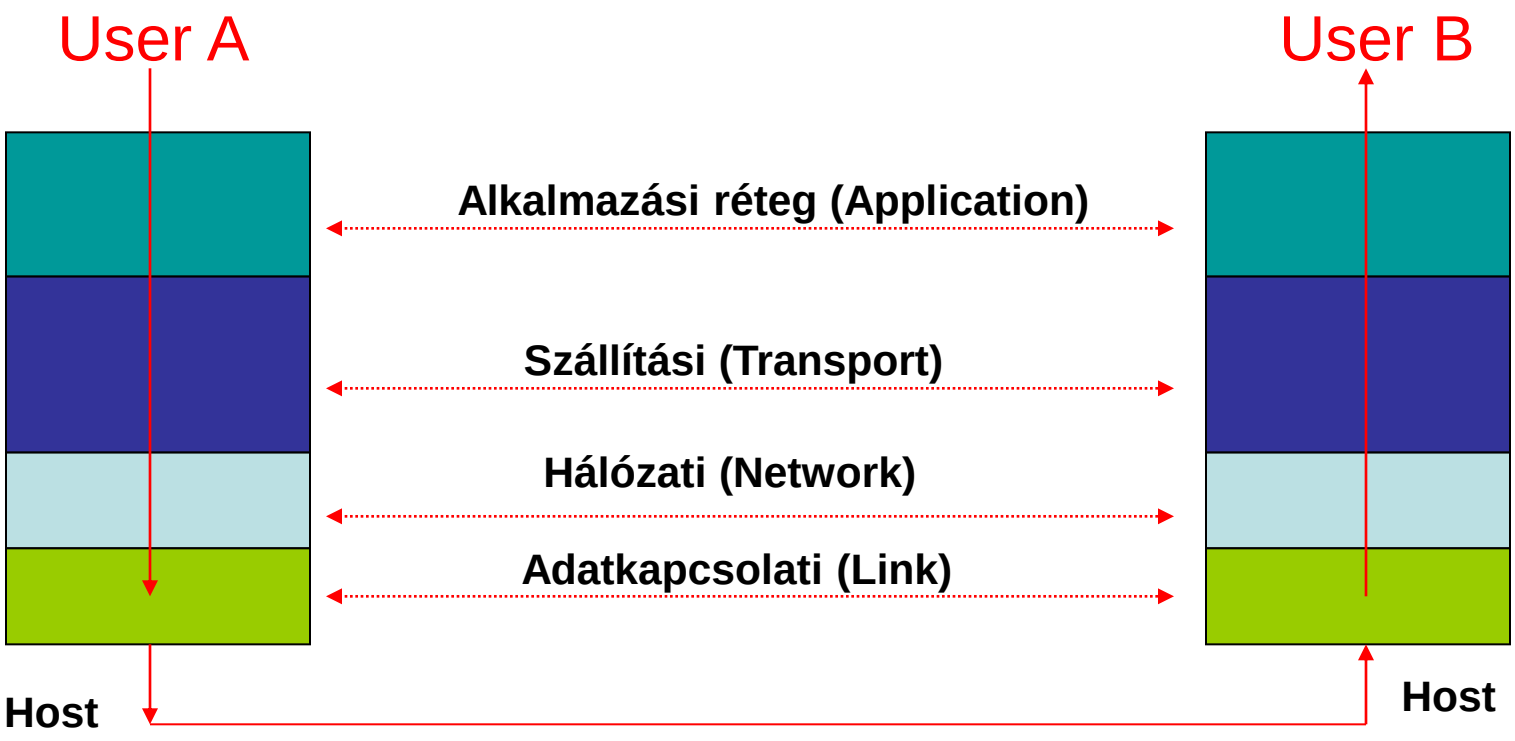
OSI – IP architektúra



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

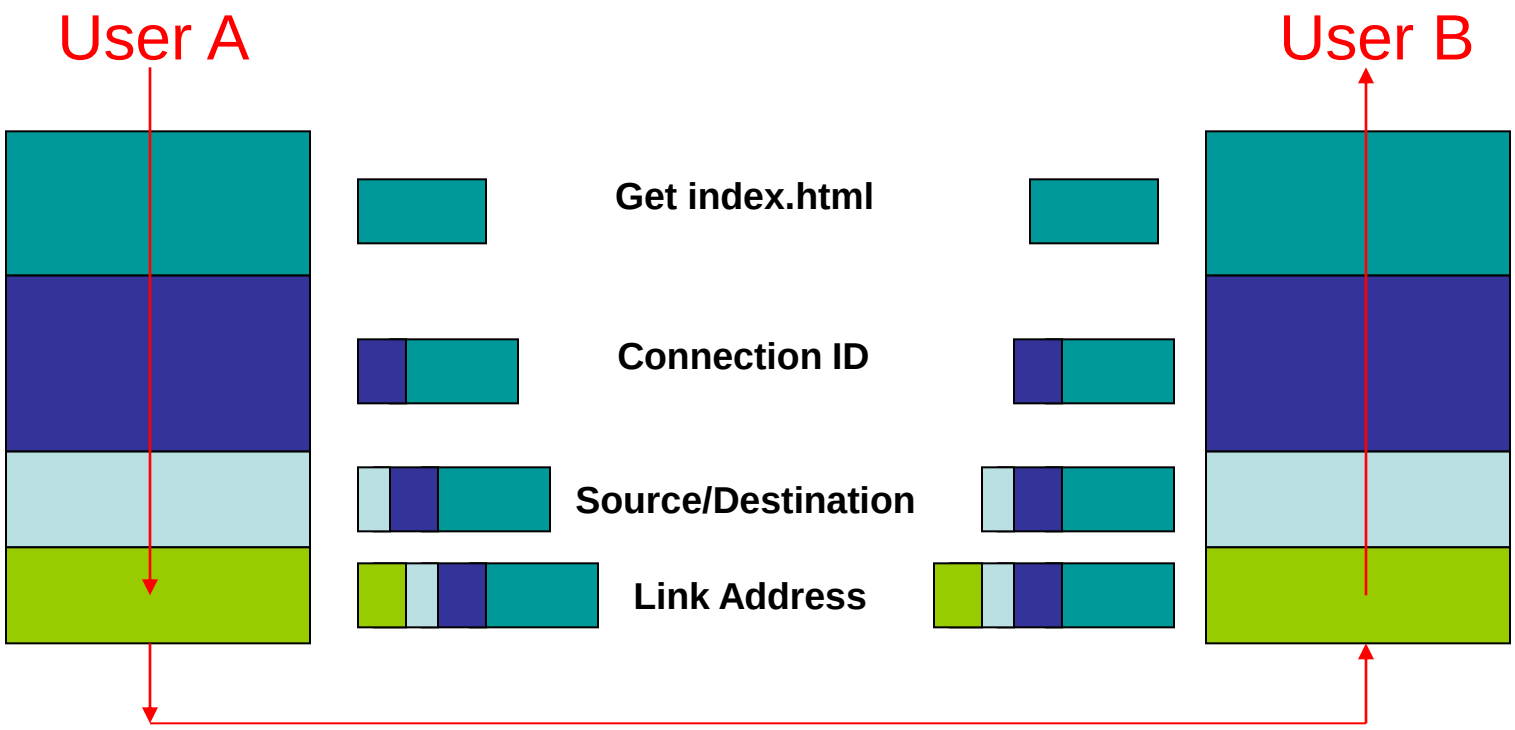
MAC: Medium Access Control
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

Rétegezés



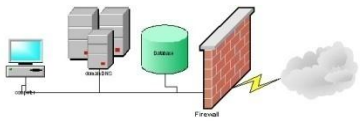
Rétegezés: bonyolult rendszerek egyszerűsítése céljából

Rétegek: egymásba ágyazás



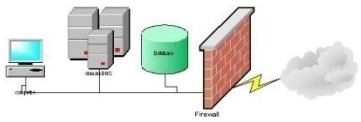
Hub, bridge, router, switch

- Hub
  - 1. (fizikai) réteg
  - broadcast eszköz
  - bejövő jel az összes többi portra, nincs jelfeldolgozás (gyors)
  - hubbal rendelkező Ethernet hálózat – tkp. megosztott medium -> ütközés detektálás



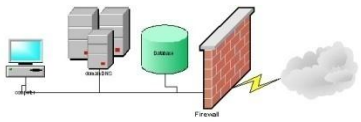
Hub, bridge, router, switch

- Bridge (híd)
  - 2. (adatkapcsolati) réteg
  - keretanalízis, MAC (fizikai) cím alapú irányítás
    - nincs ütközés, de lassabb
    - transzparens (adaptív hidak)
    - forrás által irányított
  - de mikor jobb a hub???



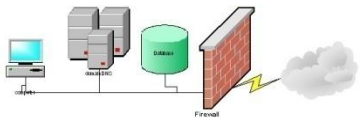
Hub, bridge, router, switch

- Router (irányválasztó)
  - 3. (hálózati) réteg
  - IP (!!) cím alapú irányítás
  - két vagy több IP alhálózatot köt össze
  - tkp. speciális célú nagyszámítógép

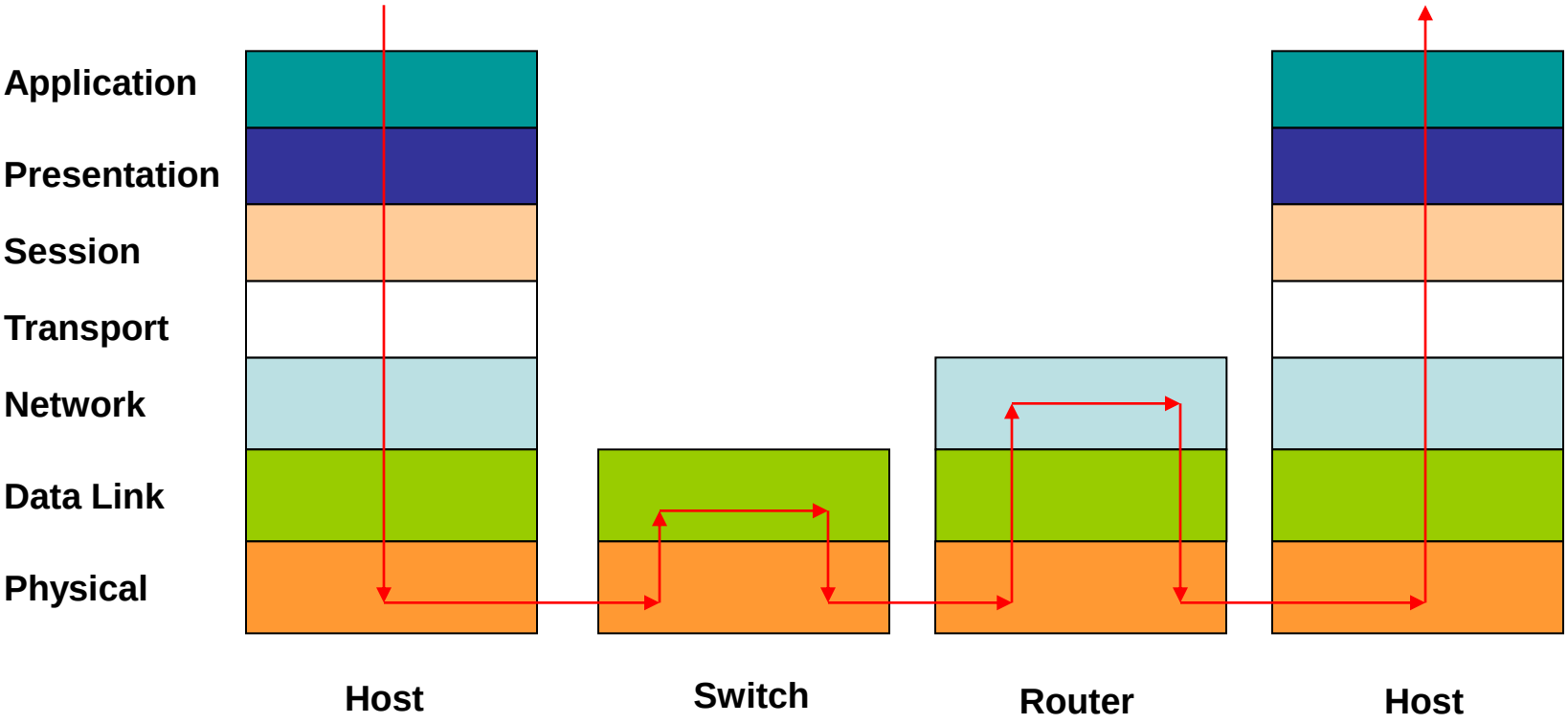


Hub, bridge, router, switch

- Switch
  - kommerciális kifejezés
  - ált. a híd (bridge) helyett használják
  - de vannak felsőbb rétegbeli switch-ek is
    - 4. (szállítási) réteg:
      - NAT
      - terhelésmegosztás TCP session alapján
      - állapotgépes tűzfal
    - 7. (alkalmazási) réteg
      - URL alapú terhelésmegosztás
      - alkalmazás szintű tranzakció kezelés

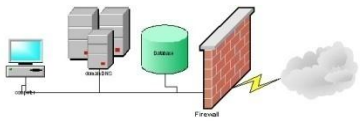


Hálózati eszközök helye a rétegekben



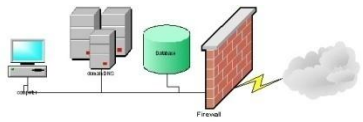
Rétegezés

- Most ez jó dolog?
  - általában igen, de
  - néha...
    - az N. réteg duplikálja az alsóbb rétegek funkcióját (pl.: hiba helyreállítás),
    - rétegeknek ugyanarra az információra van szükségük
      (pl.: időbélyeg, maximálisan továbbítható egység - MTU),
    - a teljesítmény rovására mehet

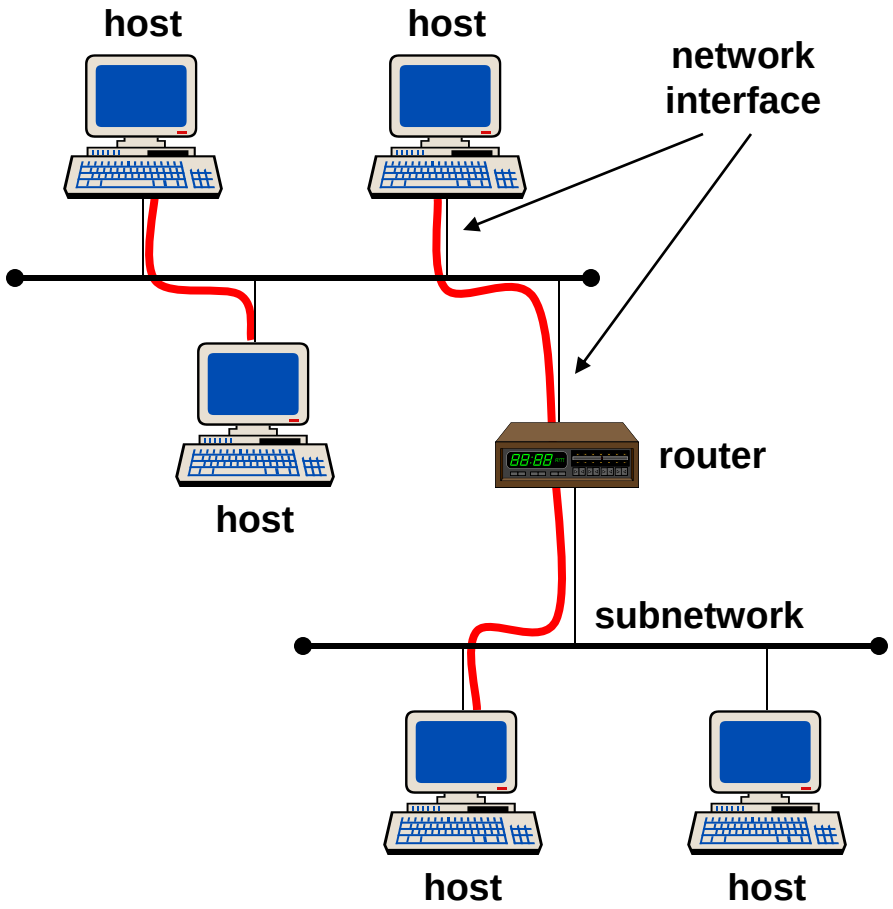


Ismétlés

- Referencia modell, protokollok
- IP alapok
  - címek, címosztályok
  - DHCP
  - ARP/RARP
  - NA(P)T
  - DNS
  - ICMP



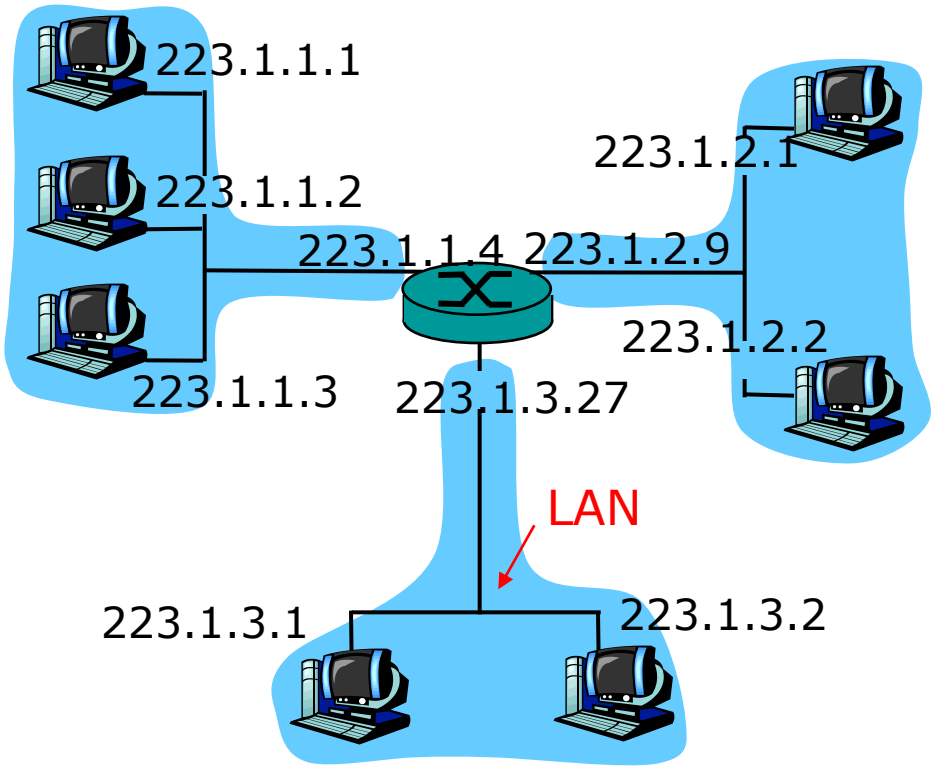
IP hálózati elemek



- **Hoszt (host)**: kommunikációs végpont
- **Alhálózat (subnetwork)**: fizikai hálózat, a hozzákapcsolt csomópontok közvetlenül tudnak kommunikálni
- **Útválasztó (router)**: közvetítő a külön alhálózaton található, kommunikáló hosztok között
- **Interfész (interface)**: csomópont kapcsolódási pontja az alhálózathoz

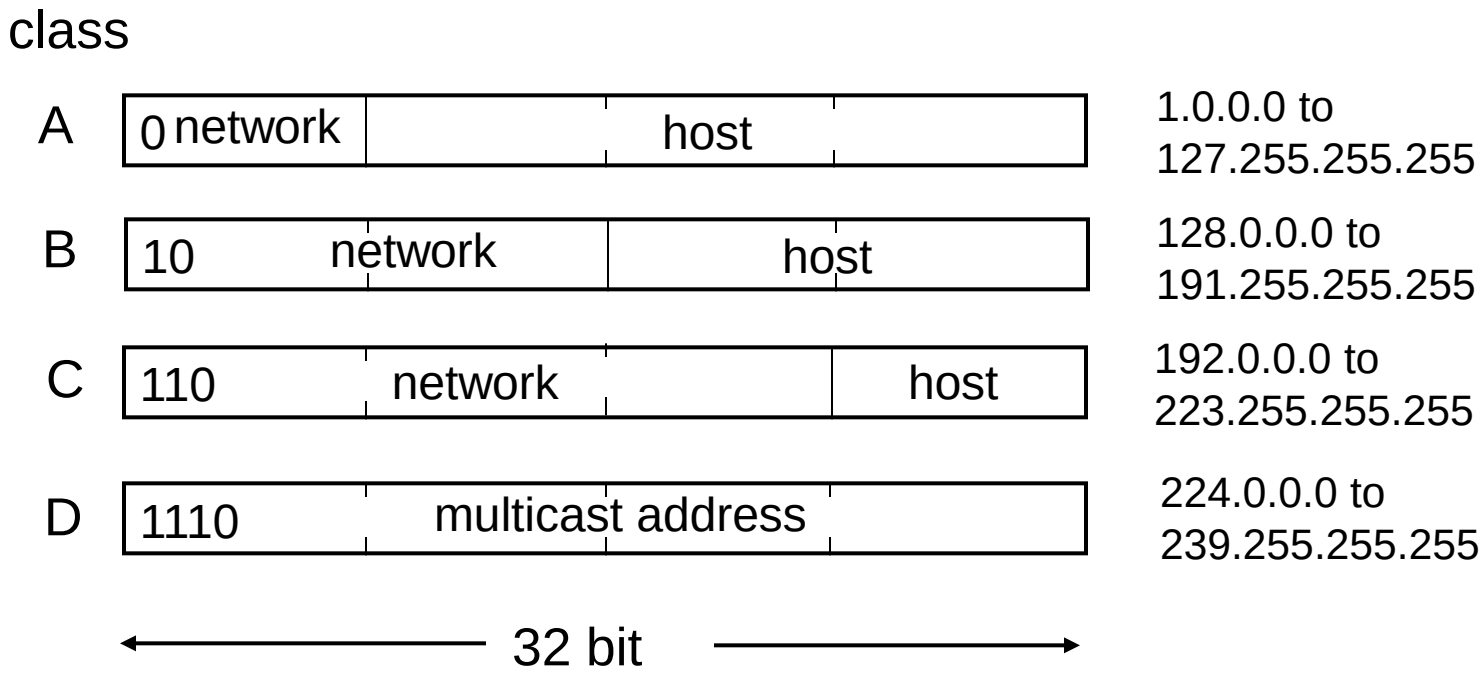
IP címek

- IP cím:
  - hálózati cím (high order bits)
  - host cím (low order bits)
- *Hálózat?* (IP szempontból)
  - eszköz illesztő u. azzal a hálózati címrésszel
  - útválasztó nélküli összeköttetés ezen eszközök között



24 bites hálózati címek

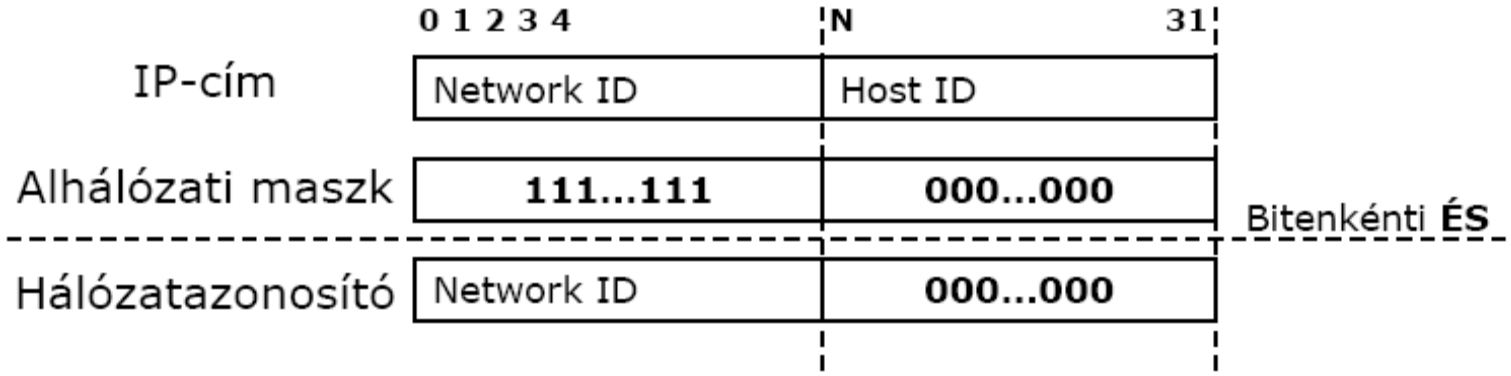
IP címosztályok



- Nem elég flexibilis – túlságosan fogyasztja az IP címeket ☹
- CIDR: Classless Inter-Domain Routing

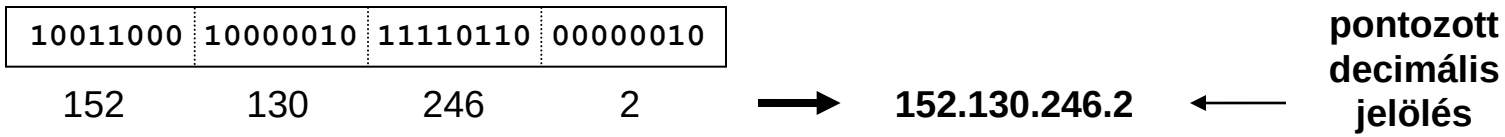
Alhálózati maszk (Netmask)

- Az alhálózatok méretét a netmask adja

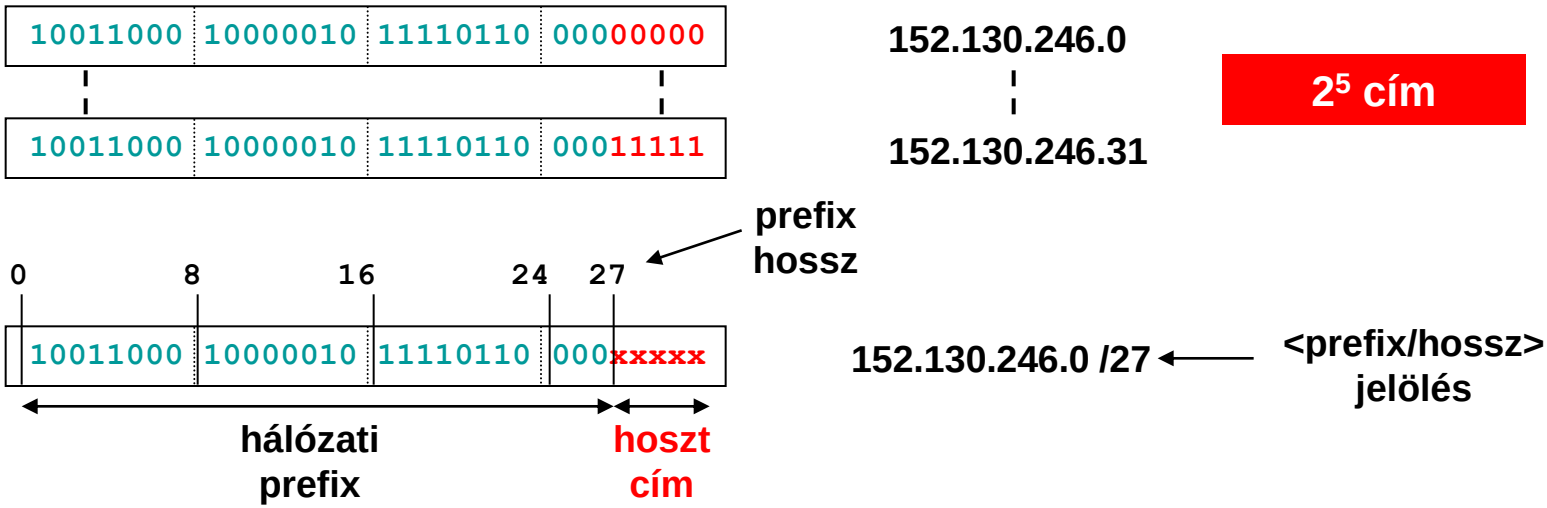


- Példa:
  - BME hálózat
    - IP címtartomány: 152.66.x.x : 255.255.0.0
  - TMIT alhálózat
    - IP címtartomány: 152.66.244.x : 255.255.255.0
- 255.255.255.0 –> 24 bites netmask : C osztály

Variable Length Subnet Mask

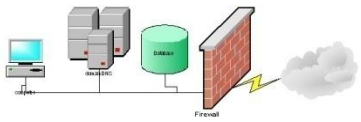


Alhálózatokhoz összefüggő IP címblokkokat rendelünk



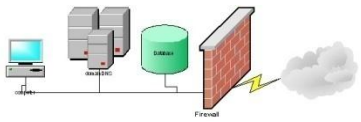
Speciális IP címek

- Host ID csupa 0: a hálózat címe
  - Hálózati cím: 152.66.244.0
    - Olyan gépek számára akik nem ismerik saját IP címüket
- Host ID csupa 1: broadcast cím
  - Broadcast – Üzenetszórás
    - Az alhálózat utolsó címe: pl. 152.66.244.255
    - A szabvány engedi a 255.255.255.255 használatát
    - Az alhálózat minden gépének szól
- 127.0.0.0-127.255.255.255: loopback network (a gép saját magának kézbesíti)
    - 127.0.0.1: helyi gép saját címe



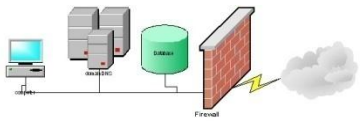
Private IP címek

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



Példa

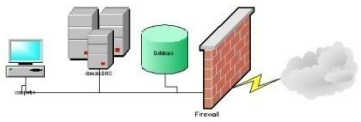
- 152.130.246.128/28
  - hány IP címet tartalmaz?
  - max. hány gépet tartalmaz?
  - mi a broadcast cím?
- Netmask 28 bites -> 32-28=4 bit
  - 2^4=16 IP cím
  - 16-2=14 gépcím (hálózati + broadcast cím!)
    - Ebből 1 cím a router
  - 10001111 -> 128+15=143 -> 152.130.246.143



DHCP

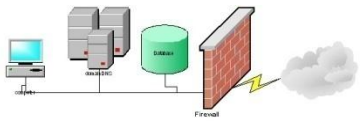
- Dynamic Host Configuration Protocol
  - Lehetővé teszi hogy egy gép IP címet kérjen a hálózattól
  - Megadhatja a többi hálózati paramétert is:
    - Átjáró, DNS szerver

- Hátrány: mindig más IP cím



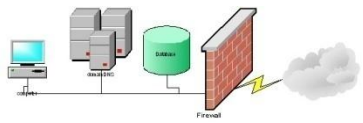
MAC cím

- Media Access Control (Extended Unique Identifier)
  - EUI-48 ill. MAC-48: 48 bites,
  - EUI-64: 64 bites cím
  - 12 hexa formában: **00-09-6B**-26-ED-37
  - Gyártók adják a kártyáknak (**IEEE alapján**)
  - OUI: Organizational Unique Identifier
  - 2^{48} kombináció (281 ezer milliárd)
    - Ethernet
    - Bluetooth
    - ATM
  - EUI-64: IPv6

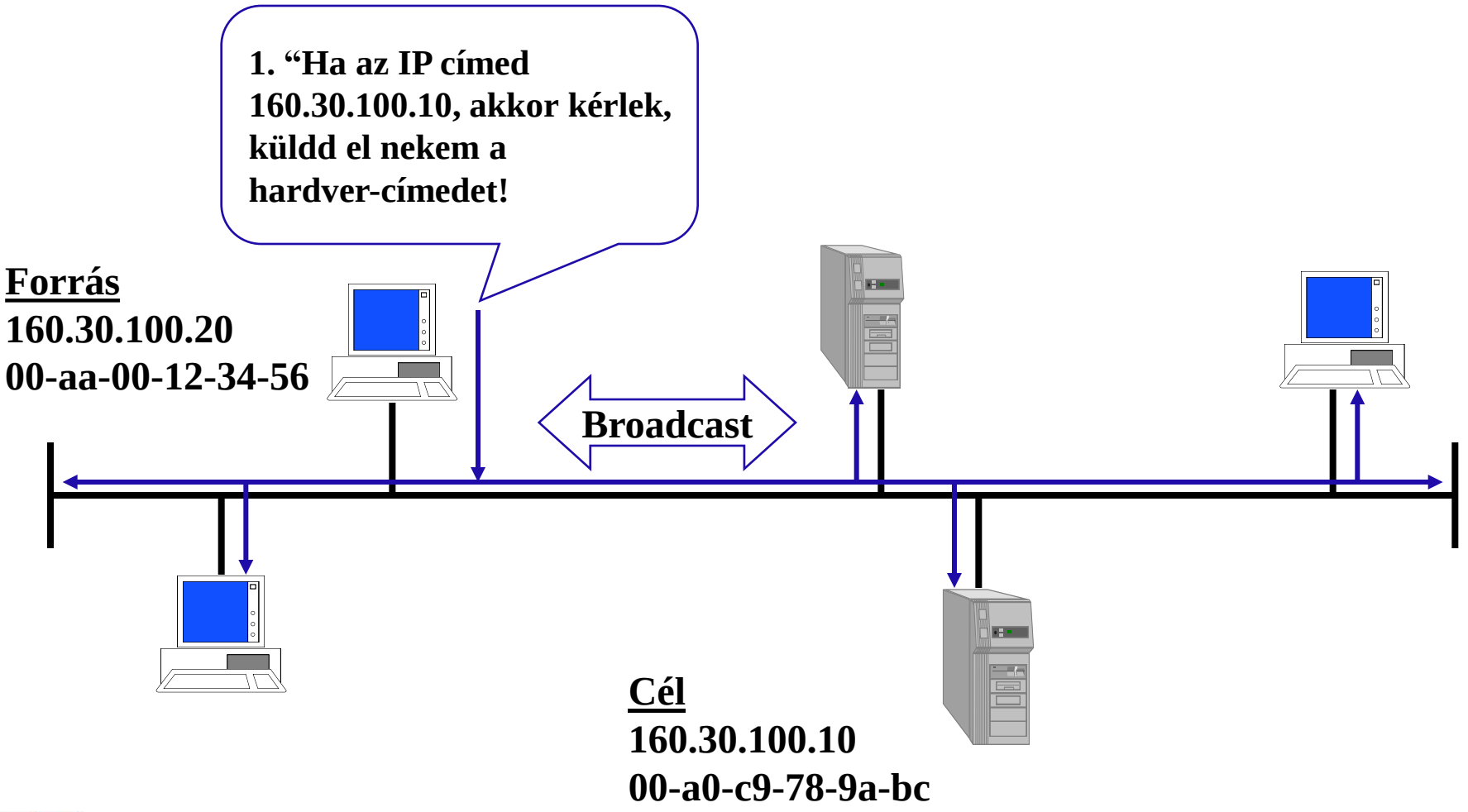


Címfeloldási Protokoll
(ARP – *Address Resolution Protocol*)

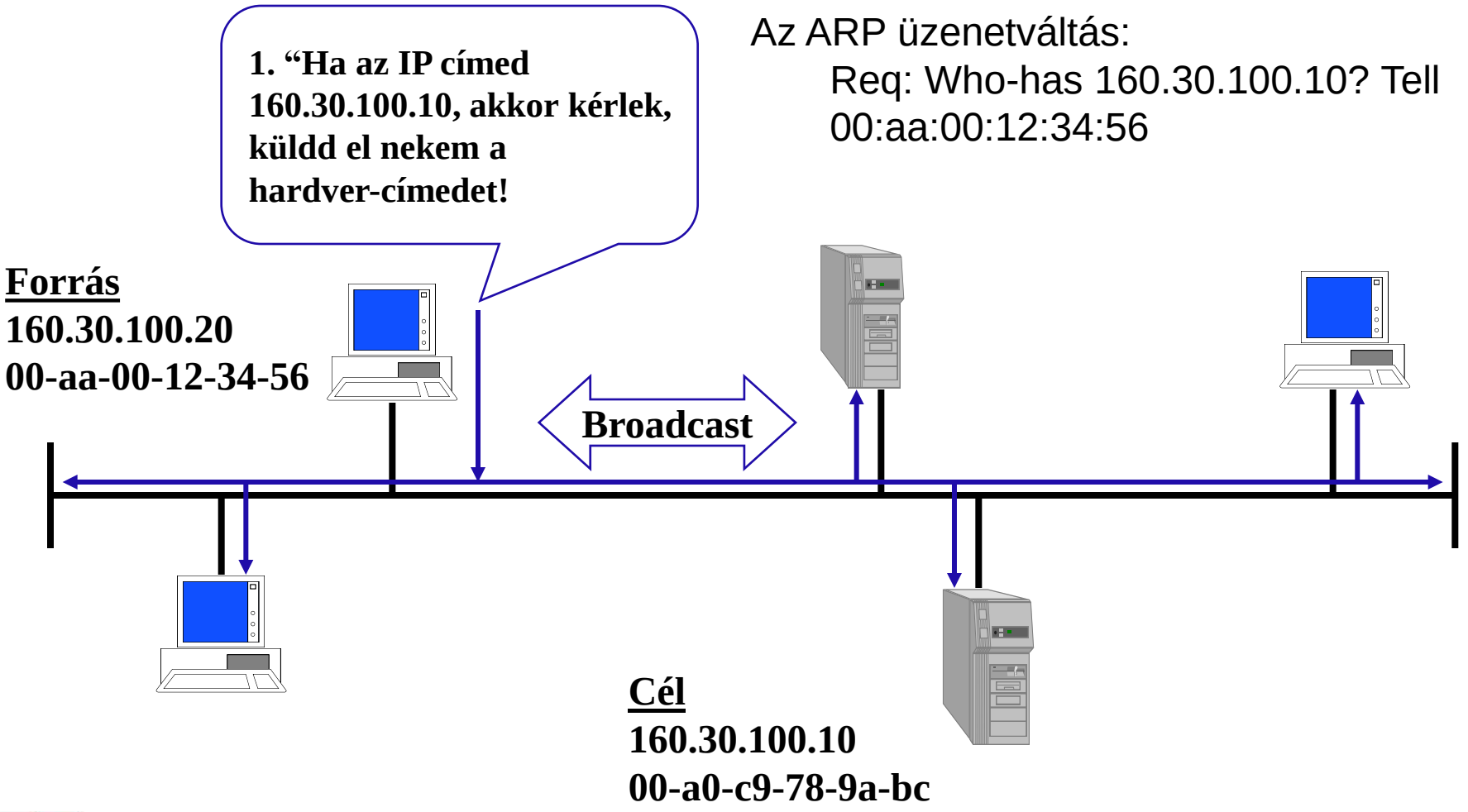
- A forrásnak tudnia kell a cél hardver-címét (MAC address) mielőtt IP csomagokat küldhetne neki
- Az ARP egy eljárás, mely hardver-címet rendel IP címhez
- Az ARP a helyi hálózaton küldött üzenetszórás (broadcast) segítségével állapítja meg a kérdéses IP címhez tartozó hardver-címet
- Az ARP gyorsítótárban (cache) tárolja az összerendeléseket, hogy később használhassa (ez kiíratható az **`arp -a`** paranccsal Windows alatt)



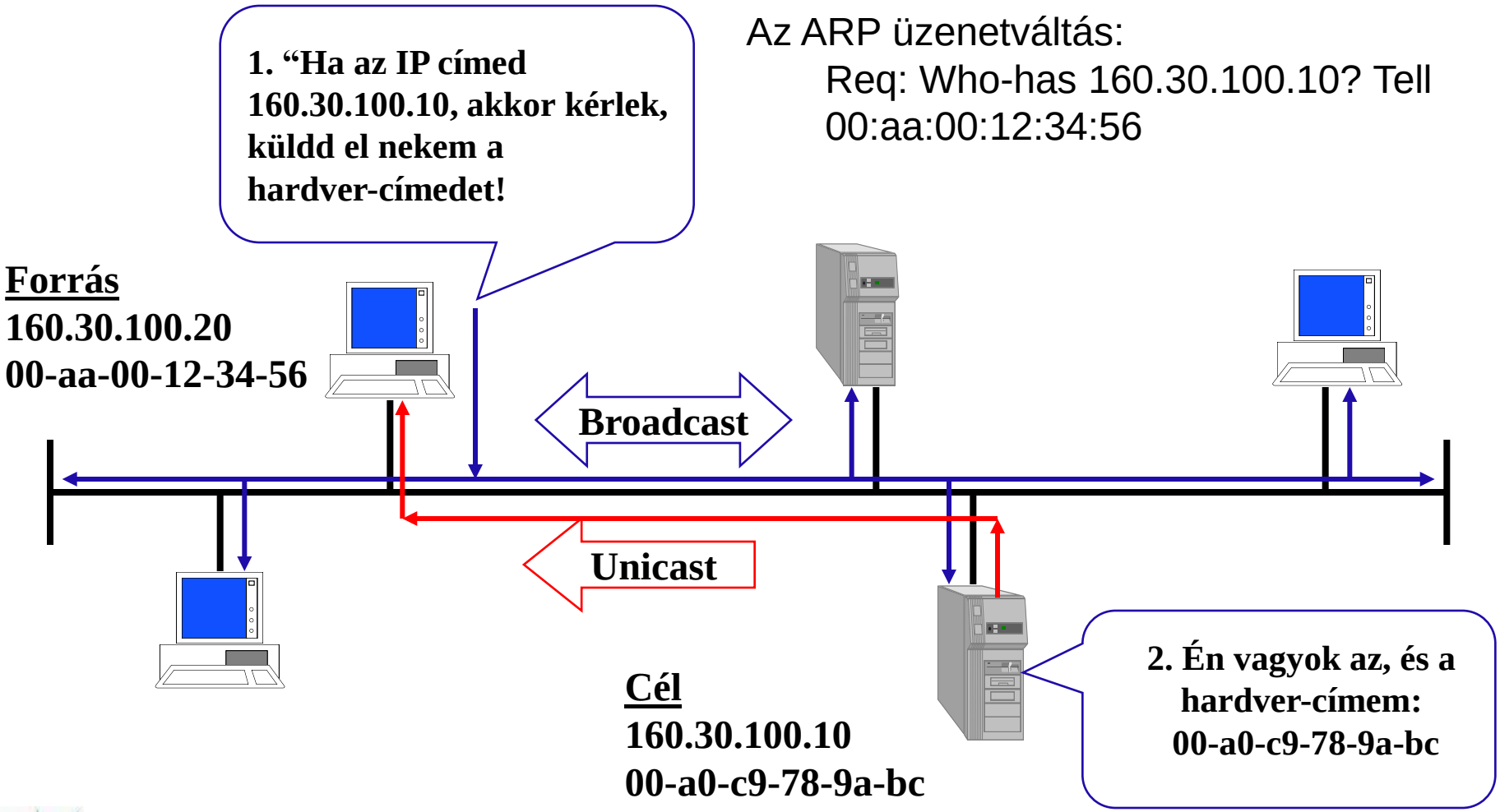
Címfeloldási Protokoll (ARP)



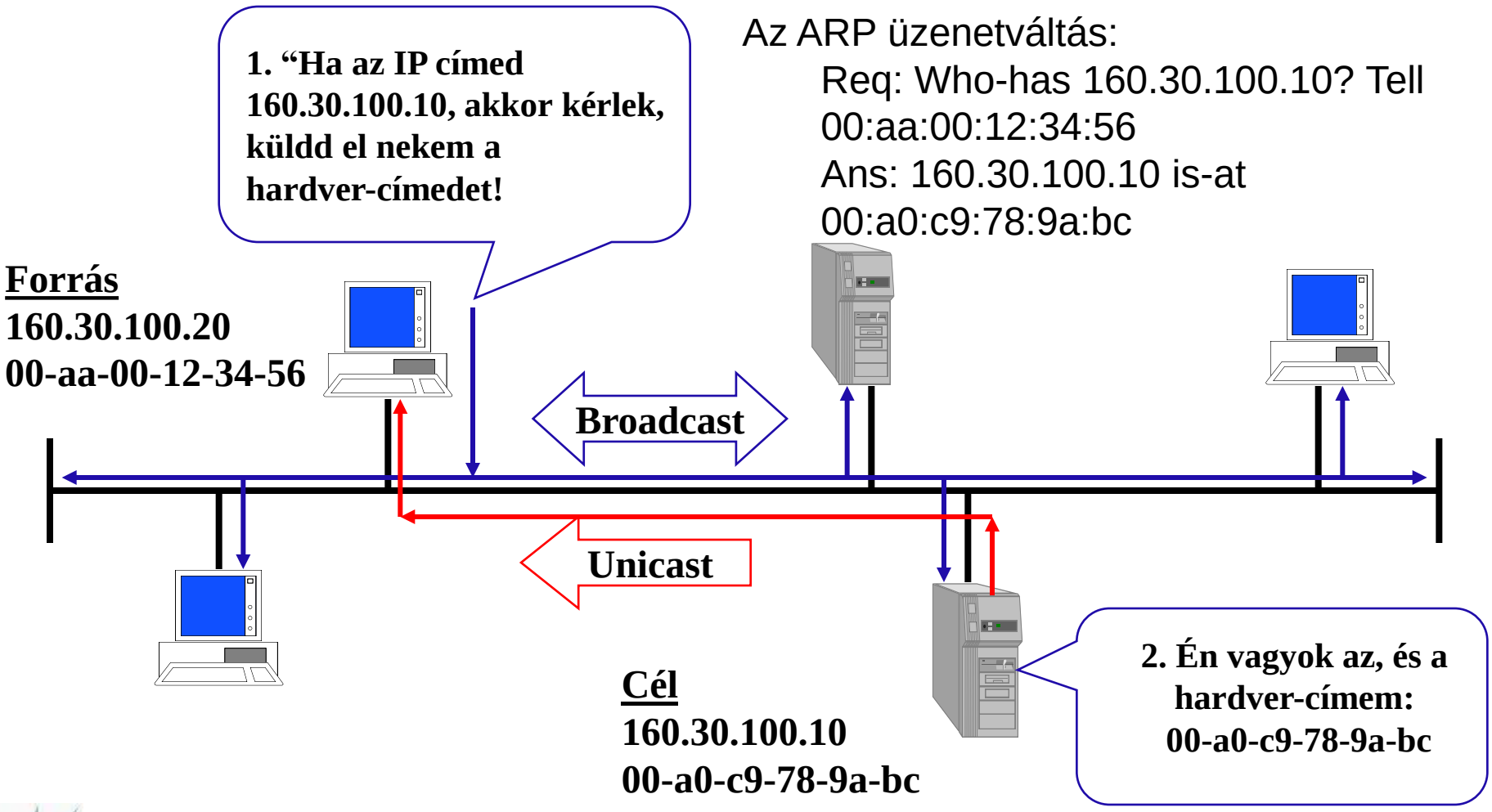
Címfeloldási Protokoll (ARP)



Címfeloldási Protokoll (ARP)

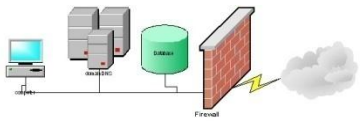


Címfeloldási Protokoll (ARP)



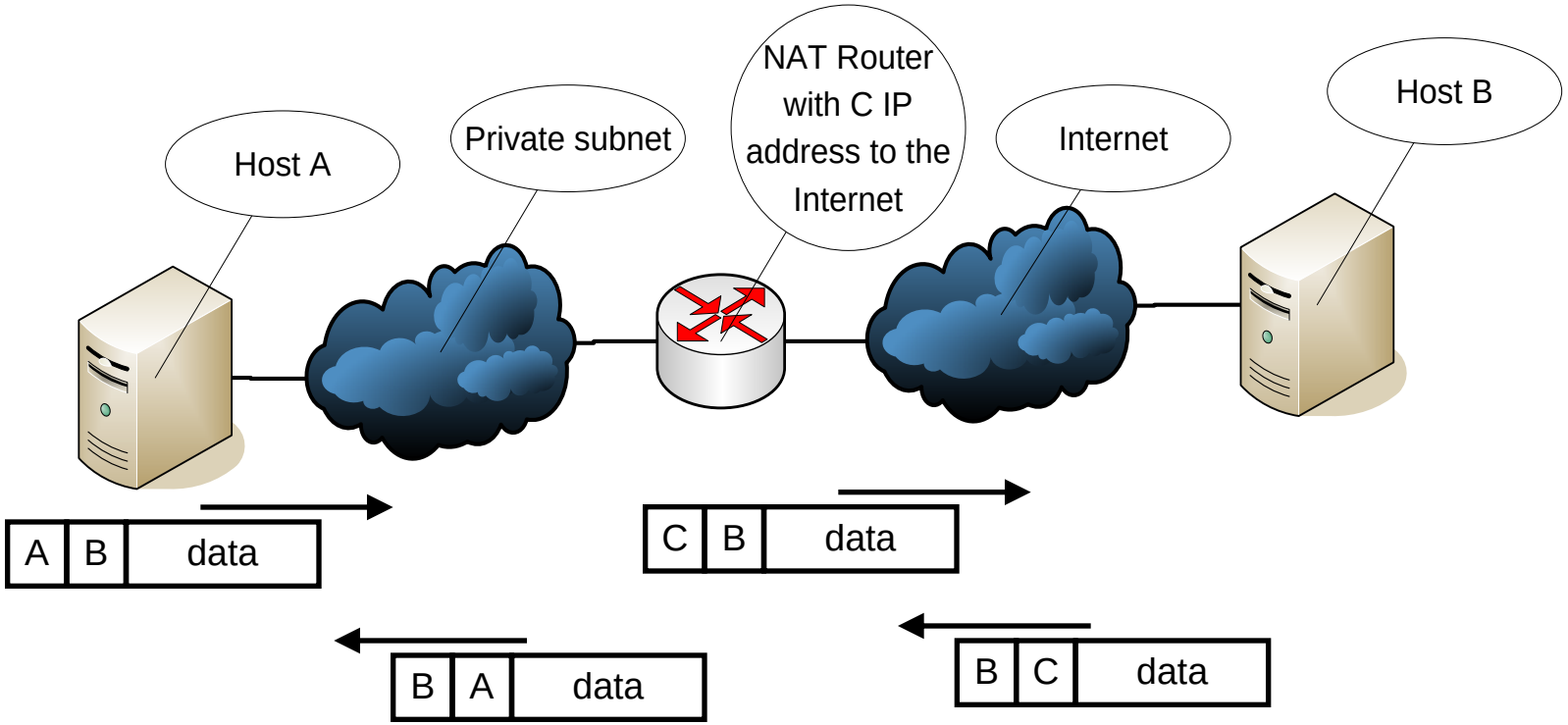
Fordított címfeloldási protokoll (RARP – Reverse Address Resolution Protocol)

- A RARP hardver-címhez rendel IP címet
- A RARP lehetőséget teremt egy újonnan indult gépnek, hogy üzenetszórással kihirdesse Ethernet címét egy kérés formájában
  - „My 48-bit Ethernet address is 00-a0-c9-78-9a-bc. Does anyone know my IP address?”
- A RARP szerver észleli a kérést, és visszaküldi a megfelelő IP címet

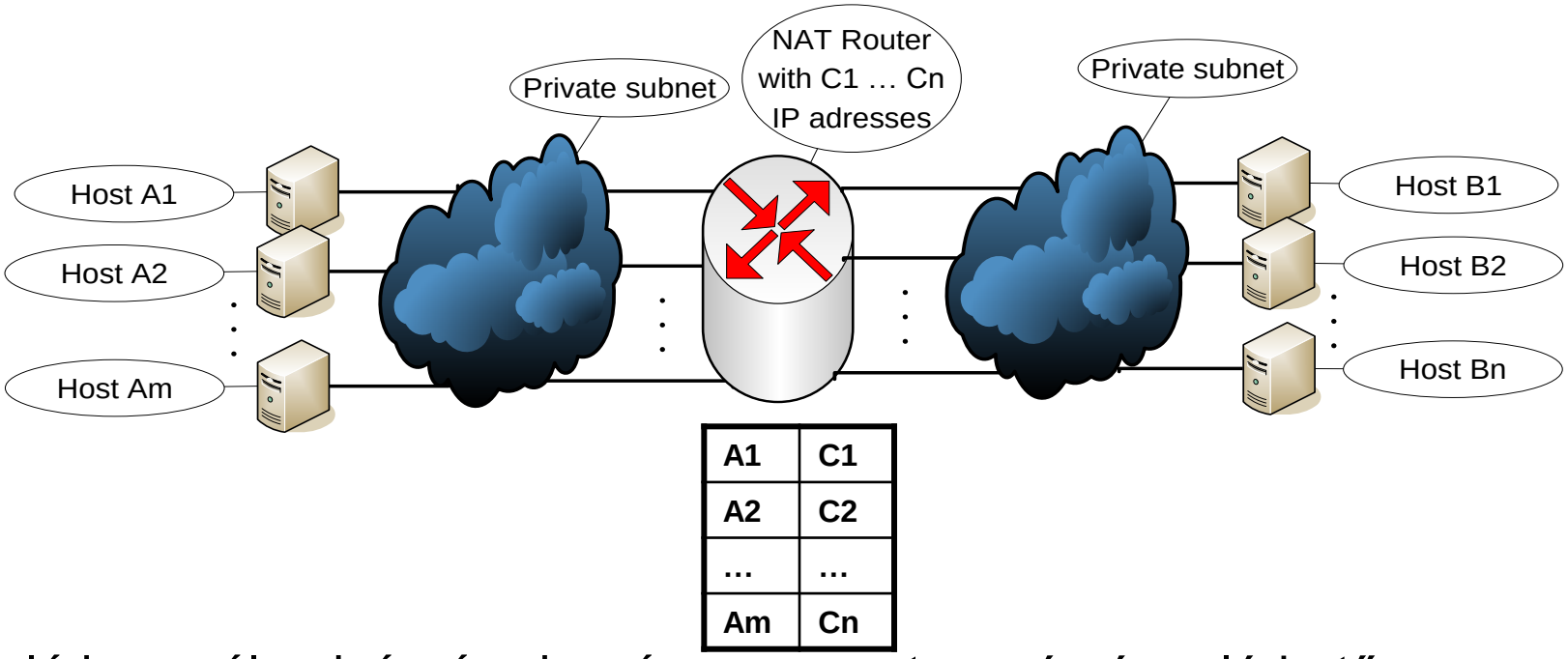


NAT

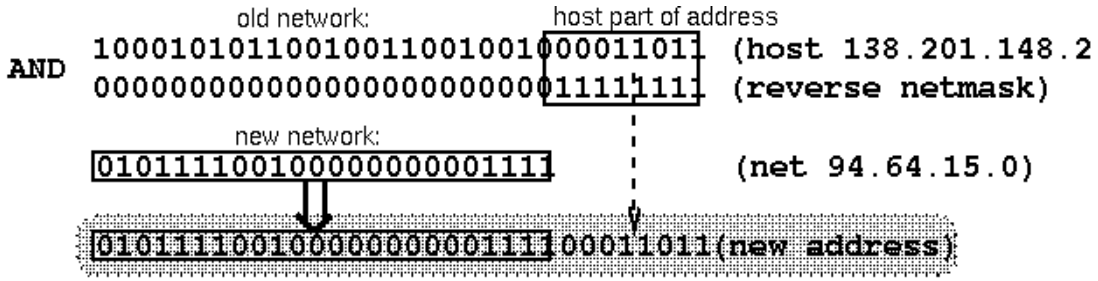
- The IP Network Address Translator (RFC1631) (1994)
- Privát hálózatok Internetre kapcsolására
- L3 (IP szinti) átalakítás
- Végpontoknak transzparens
  - bizonyos esetekben



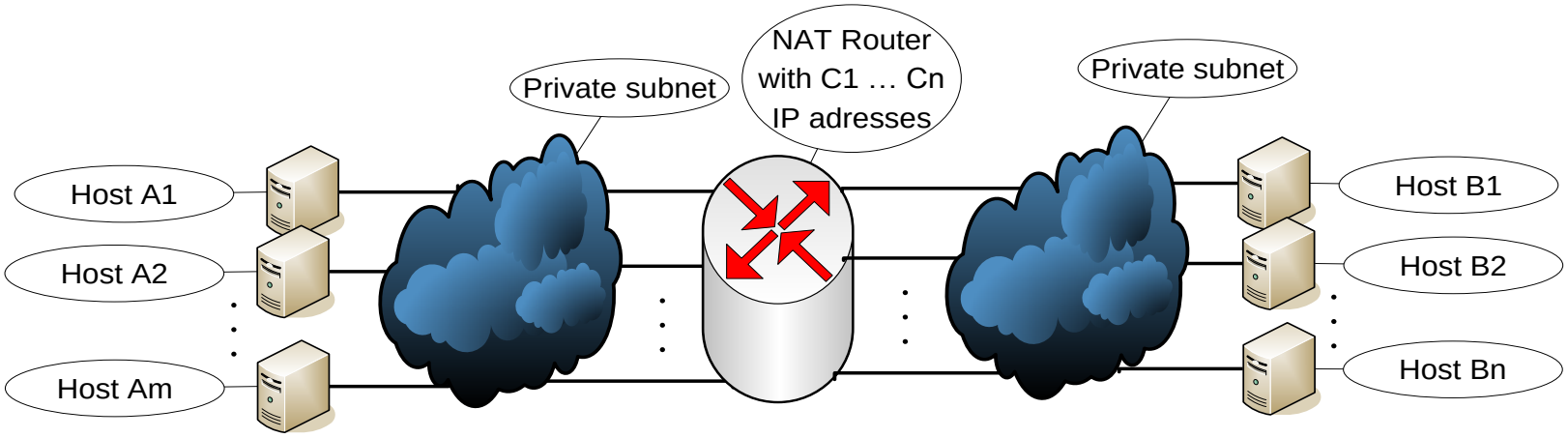
NAT – több hoszttal (m=n)



- Kifelé használt privát címek száma = a router számára elérhető publikus IP címek száma
- Hozzárendelés
  - statikus
  - dinamikus
    - biztonság növelésére



NAT – több hoszttal (m>n)

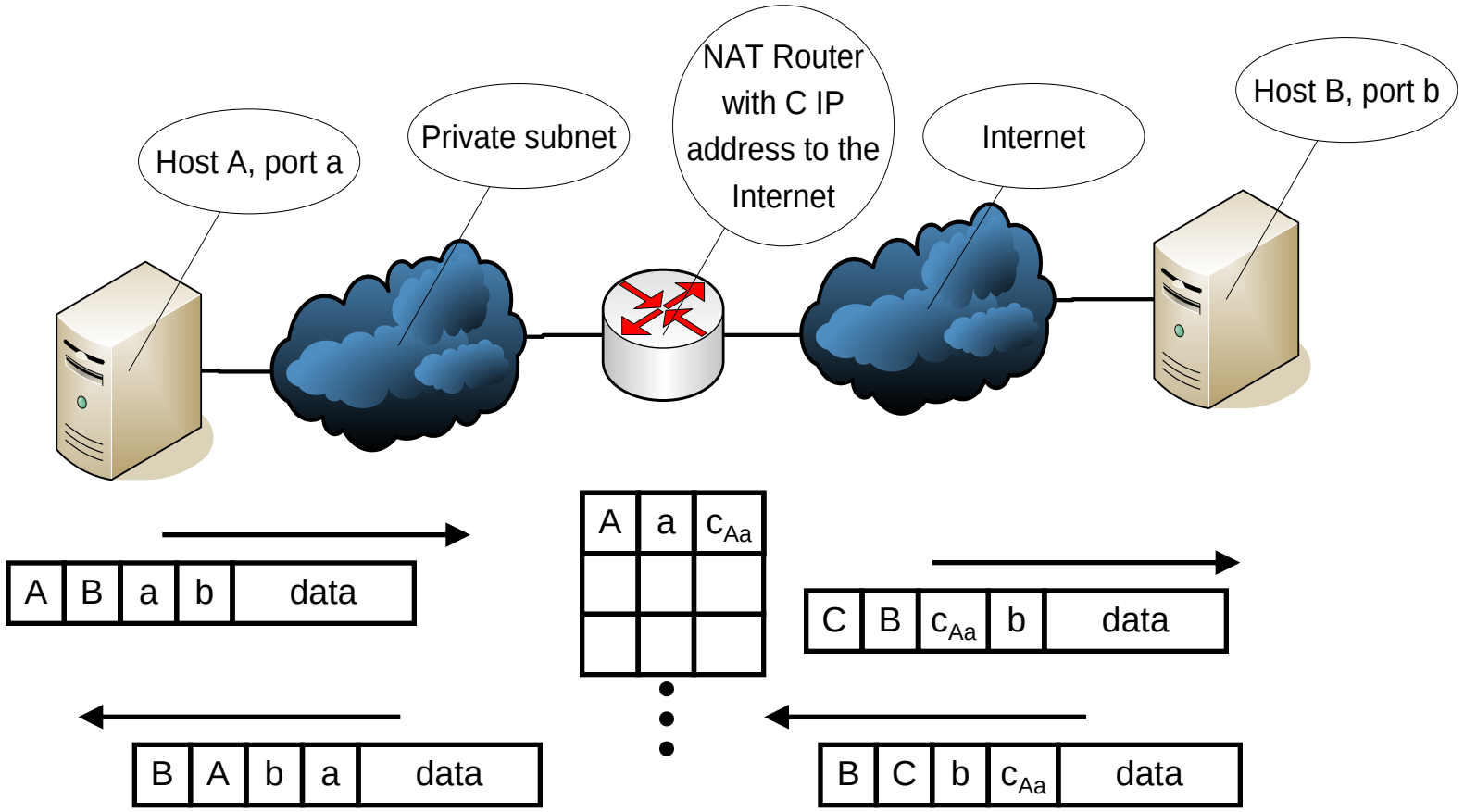


A1	C1
A2	C2
…	…
Am	Cn

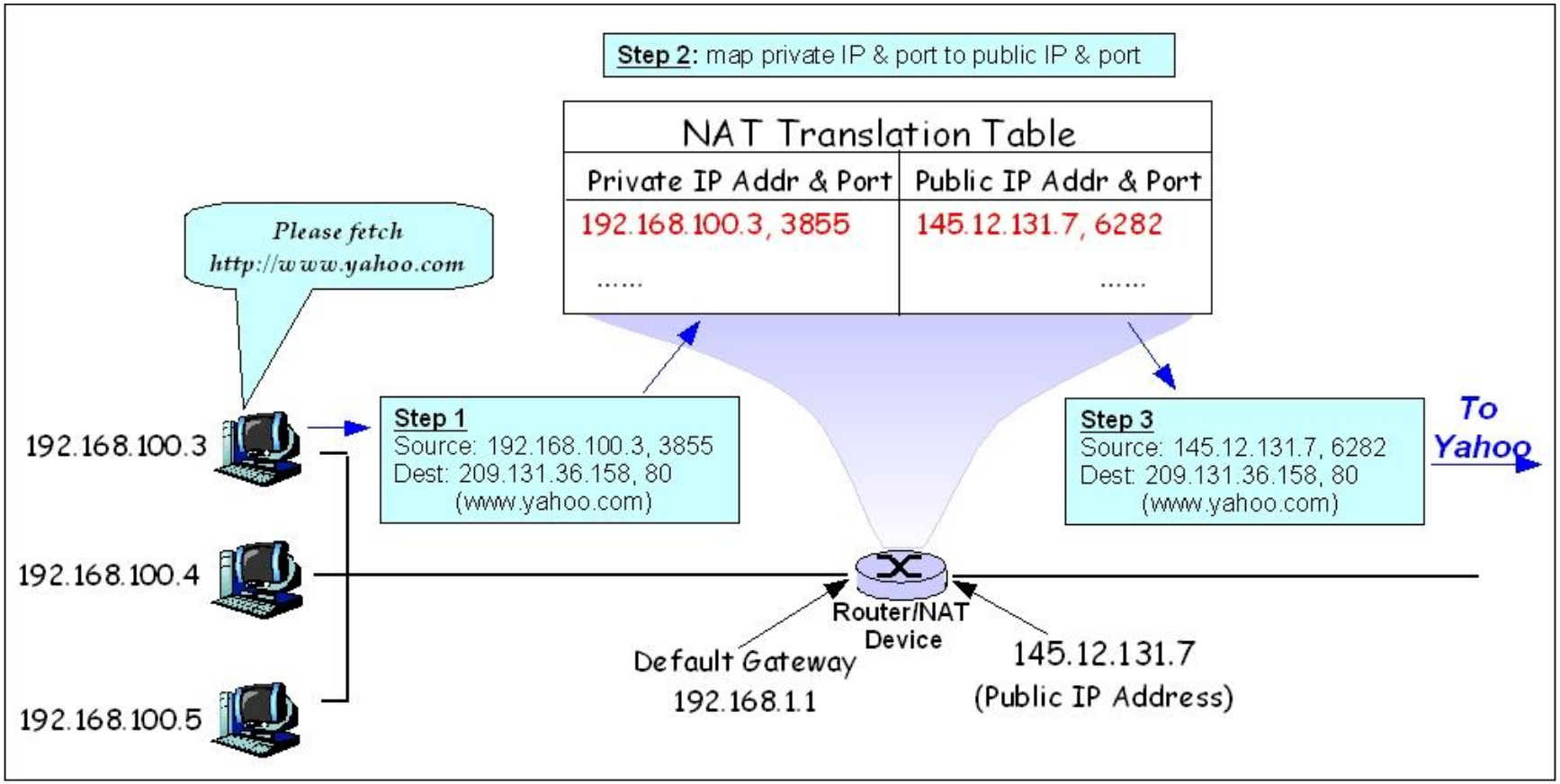
- Hozzárendelési stratégia kell
  - ha nincs elég (m>n)???
  - statikus: probléma: több, mint egy belső cím jut egy külsőre
    - hogyan talál vissza a belső állomáshoz a visszairányú kommunikáció?
  - dinamikus: használjuk a következő szabad IP címet
    - nincs minden állomás számára (egyszerre!) elegendő IP cím
- Tipikusan: n = 1 (szerver szolgáltatás)

NAT + port transzláció

- Network Address Port Translation (NAPT)

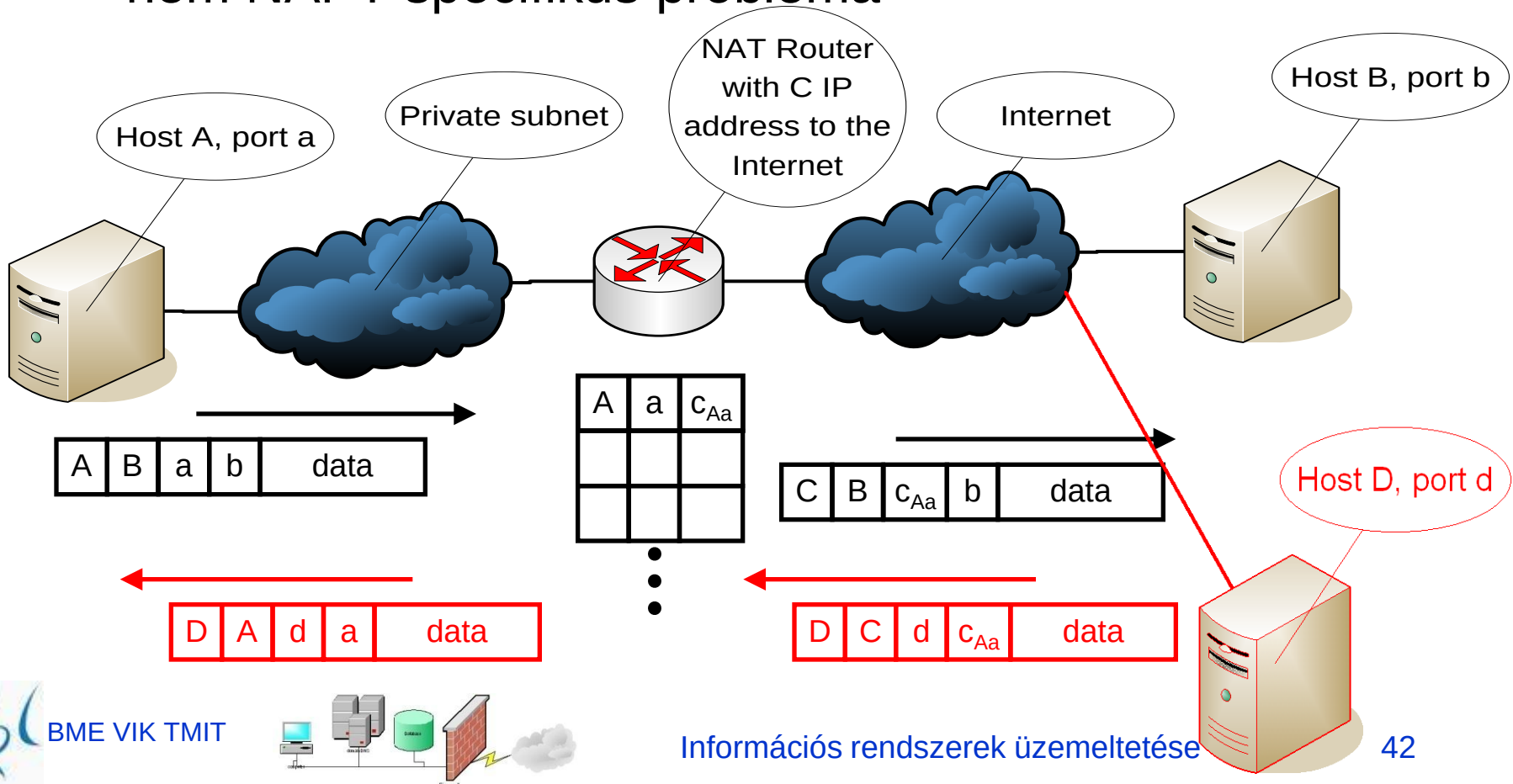


NAT + port transzláció példa



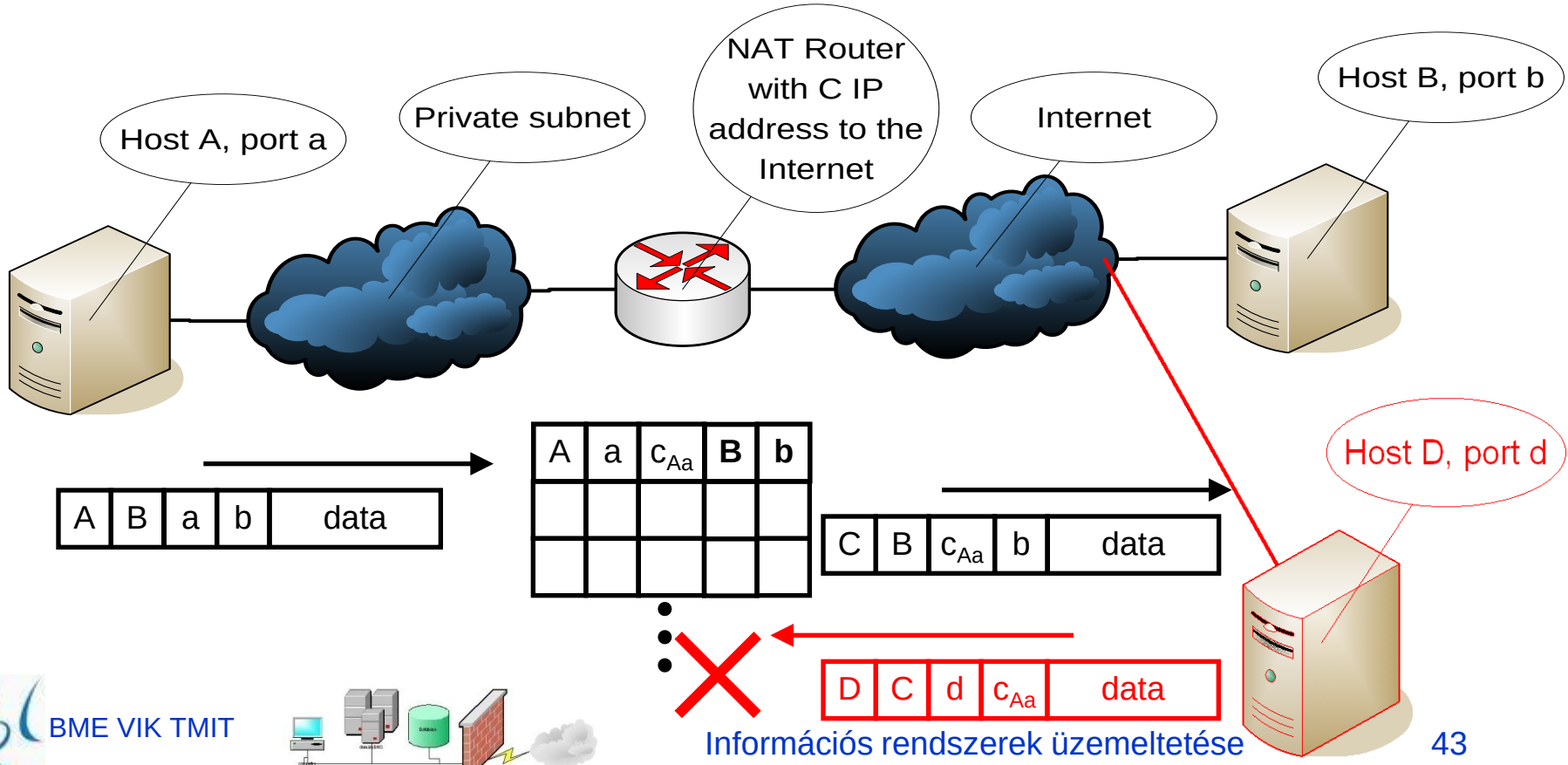
NAPT – biztonság

- Dinamikus bejegyzések
  - de az élettartam alatt scannelhető és elérhető
  - nem NAPT specifikus probléma



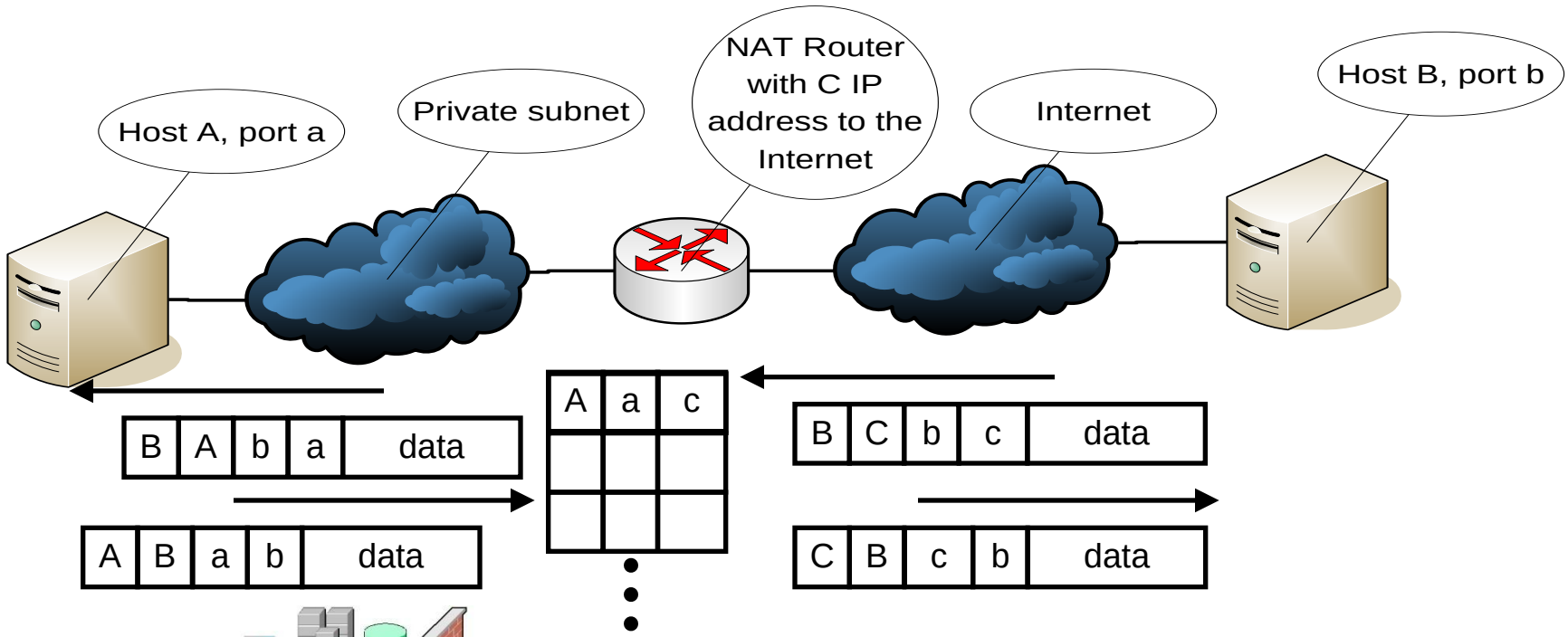
NAPT – biztonsági kiegészítés

- Távoli IP címmel kiegészítve
- Egyszerű tűzfal megoldás



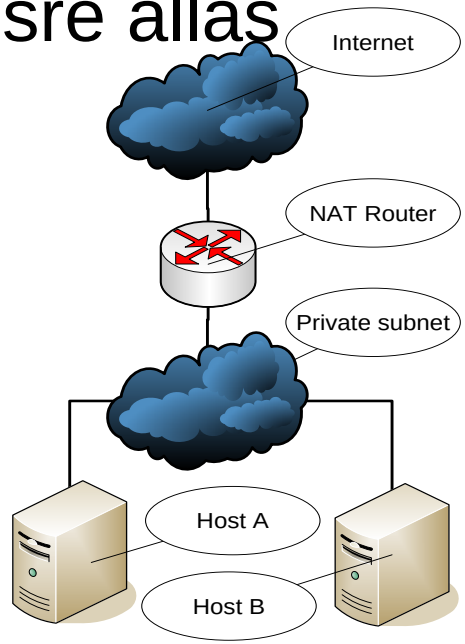
NAPT – virtuális szerver

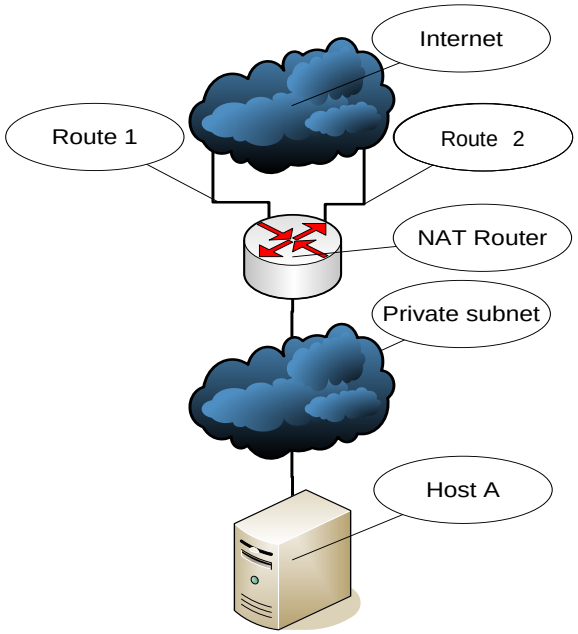
- Belső szervert statikus hozzárendeléssel kiexportálni
  - mintha a NAPT routeren volna a szolgáltatás
    - minden portra
    - kiválasztott portokra
      - megvédhetjük bizonyos forgalmaktól



NAT – optimalizációk

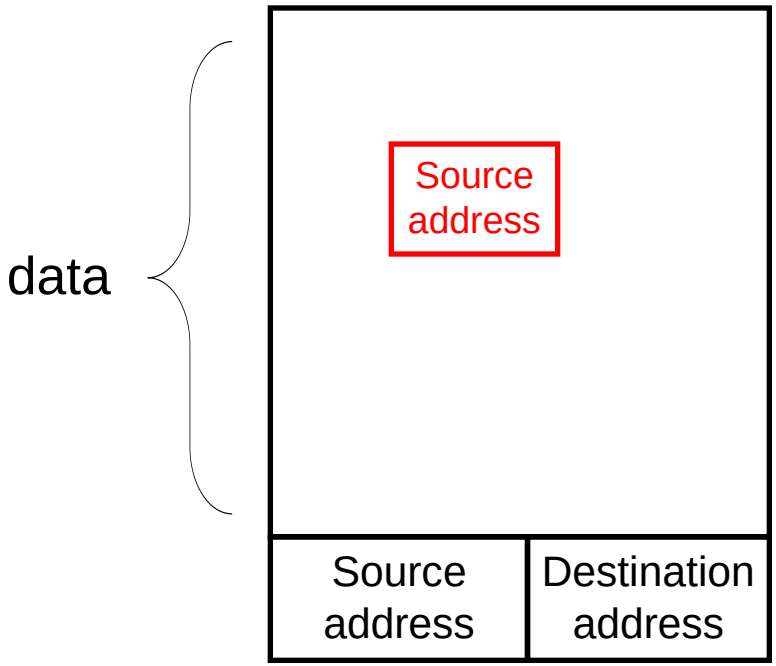
- Több belső szerver / külső interfész
  - terhelésmegosztás
  - rendelkezésre állás



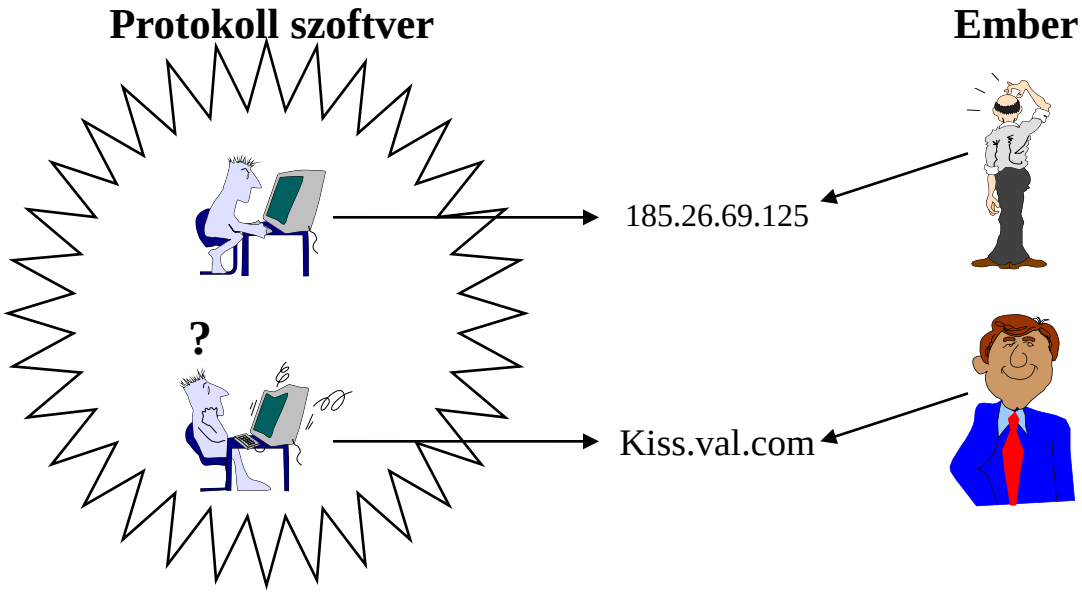


NAT problémák

- Másodlagos kapcsolatokat nem lehet megnyitni
  - kívülről nem lehet kezdeményezni
- IP cím az alkalmazási rétegben
  - útválasztó protokollok
  - DNS
  - FTP
  - H.323
  - SIP
  - HTTP (absolute URL)
  - stb…
- Megoldás
  - az alkalmazási rétegben is le kell cserélni az IP címet
    - OSI szabály megsértése
    - alkalmazás proxy a NAT útválasztón



Domain Name System (DNS)

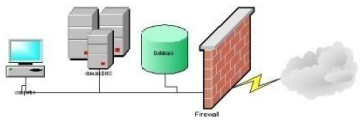


- Az IP címeket az ember nehezen jegyzi meg
  - A protokollt használó szoftverek viszont jól tudják használni
- A szimbolikus nevek használata természetesebb
  - A protokollt használó szoftverek küzdenek vele

DNS folyt.

Számítógépnév – IP cím adatbázis
Hierarchikus szerkezetű
Elosztott adatbázis, elosztott felügyeletű
Összetett nevek
A különböző operációs rendszerek széleskörűen támogatják
Két fő osztály:
- Általános (összesen 7, mindegyik hárombetűs)
- Országok (kétbetűsek)

Hátrány: statikus, kézi adminisztráció

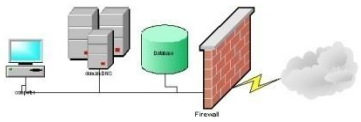


DNS névtér

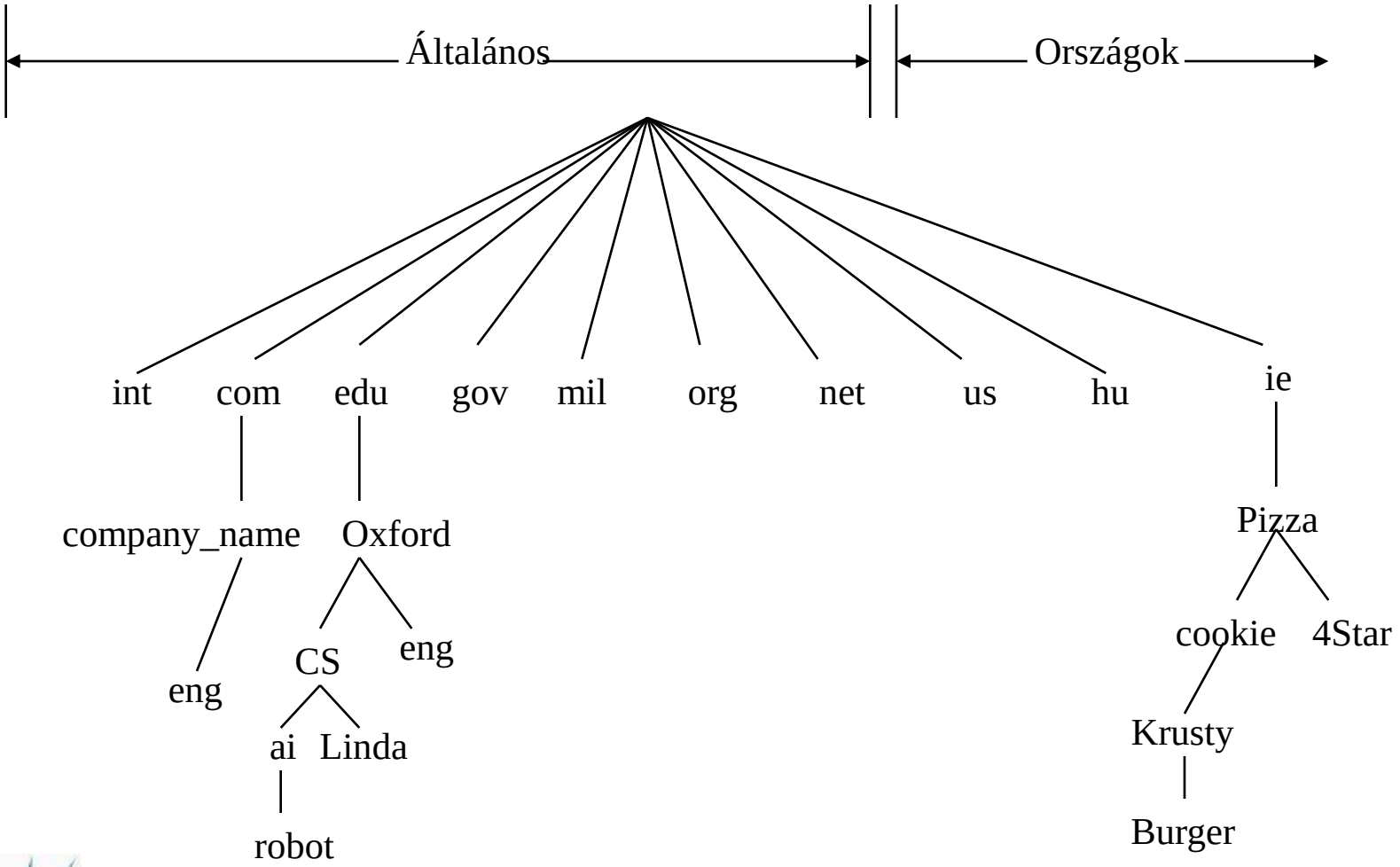
- Általános csoportok:
  - (Nagyrészüket csak az USA-ban lehet regisztrálni, de a .com pl. szabadon regisztrálható)

Domain	*Meghatározás*
.com	Kereskedelmi szervezetek
.edu	Oktatási intézmények
.gov	Kormányzati intézmények
.mil	Katonai csoportok
.net	Főbb hálózati szolgáltatók
.org	Szervezetek a fentieken kívül
.int	Nemzetközi szervezetek

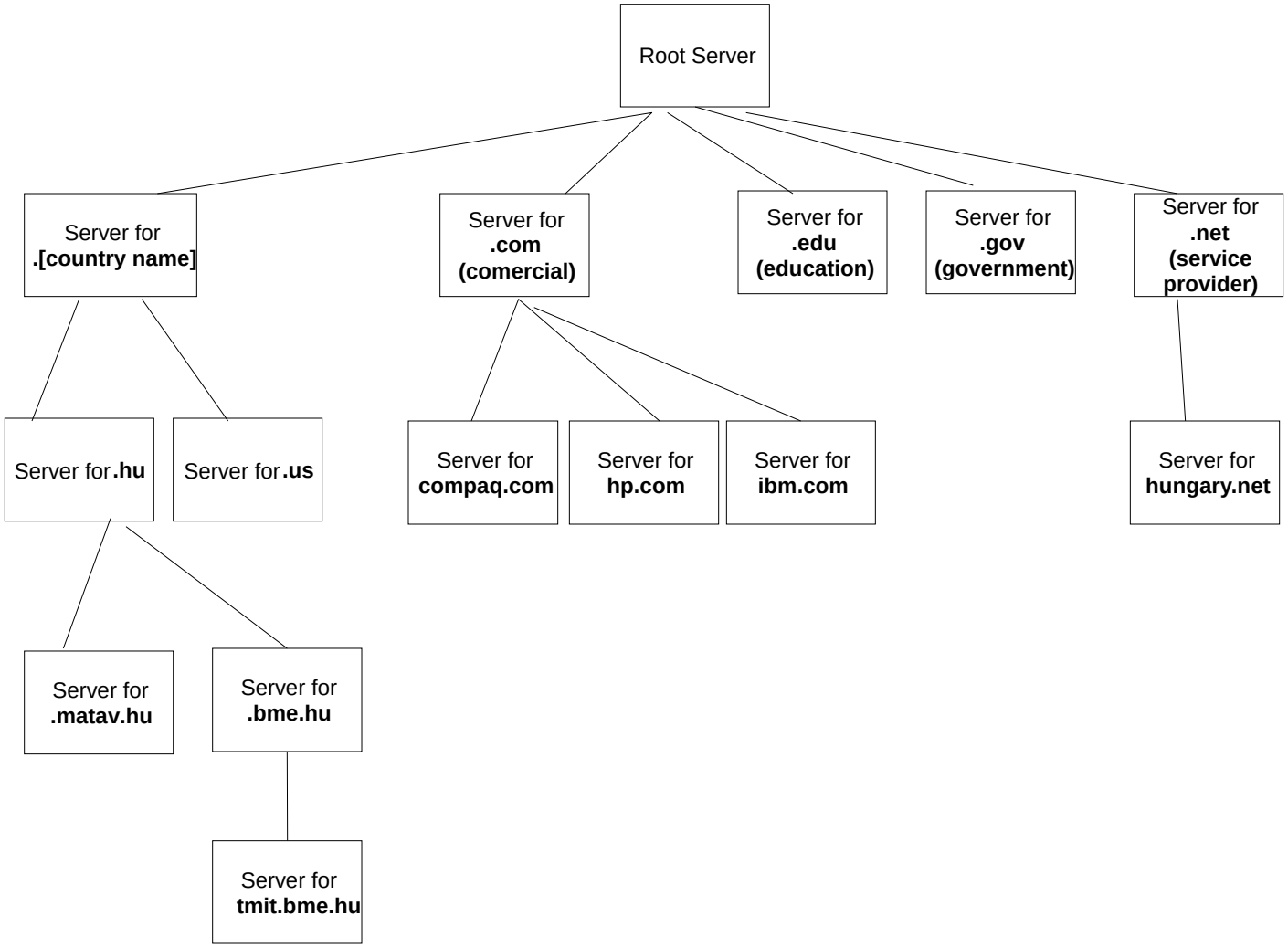
- Országok
  - pl: .hu .us .fr .de



Internet domain névtér

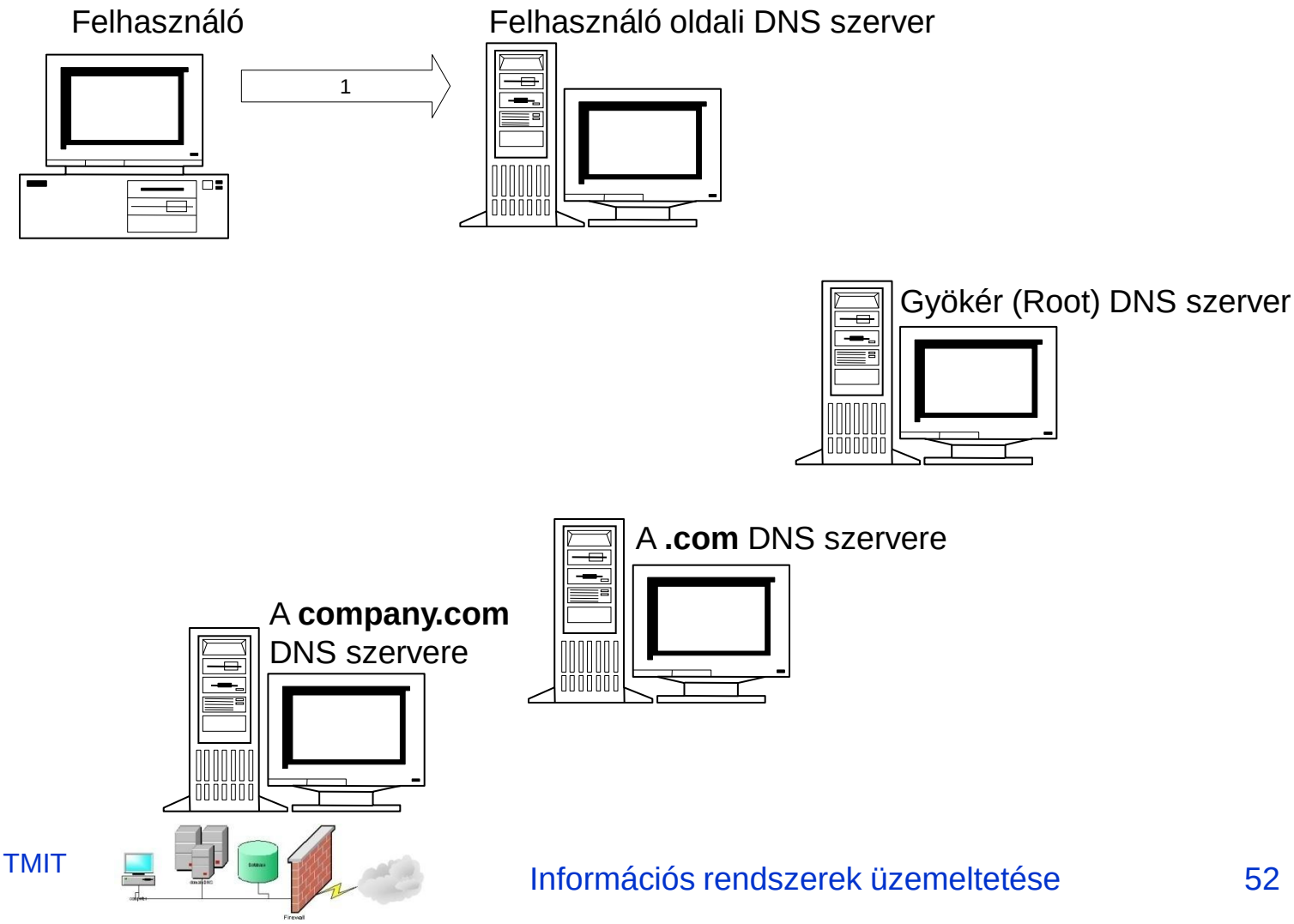


Domain név feloldása



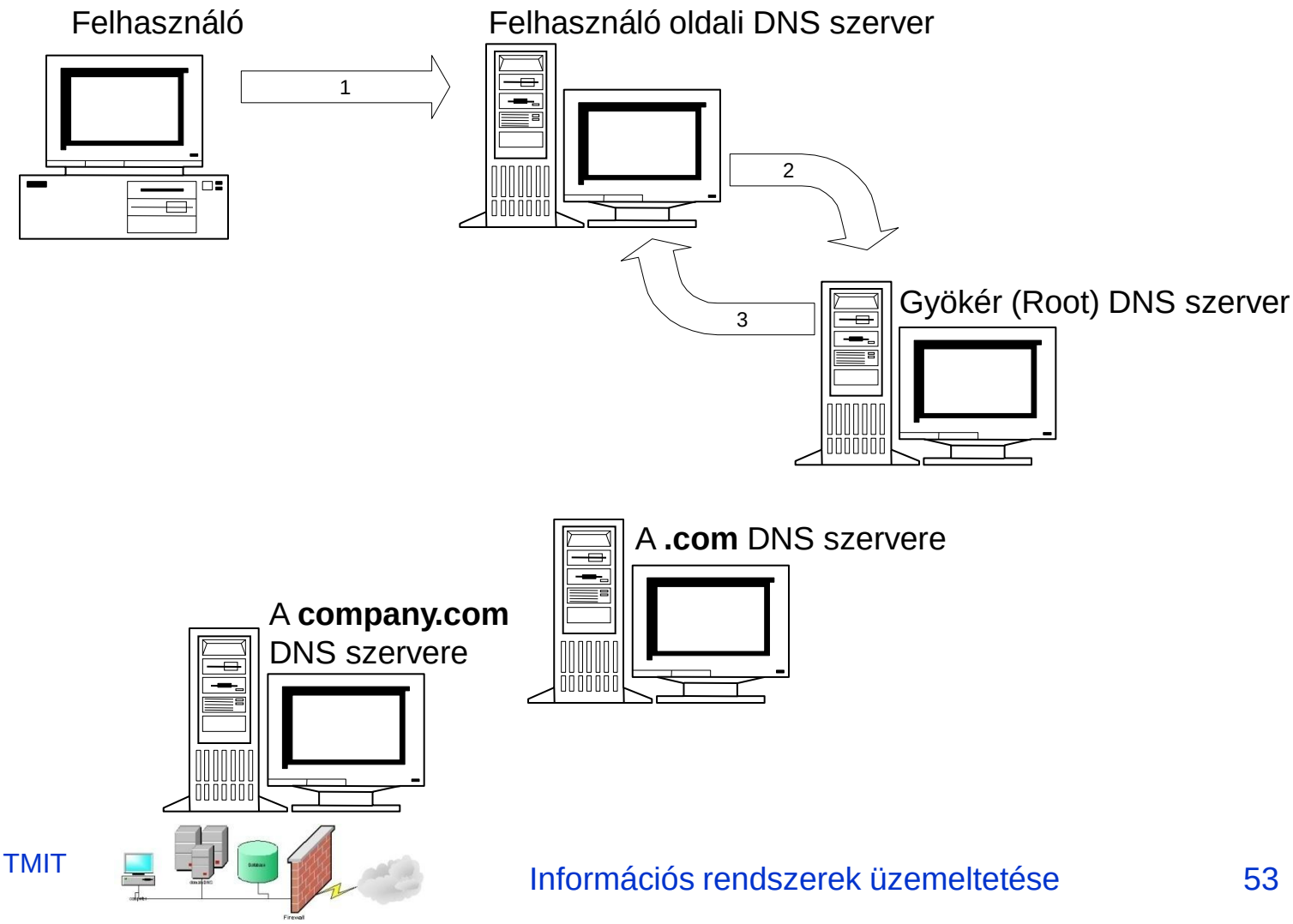
A DNS működése

(Az akarmi.company.com **domain név feloldásának lépései)**



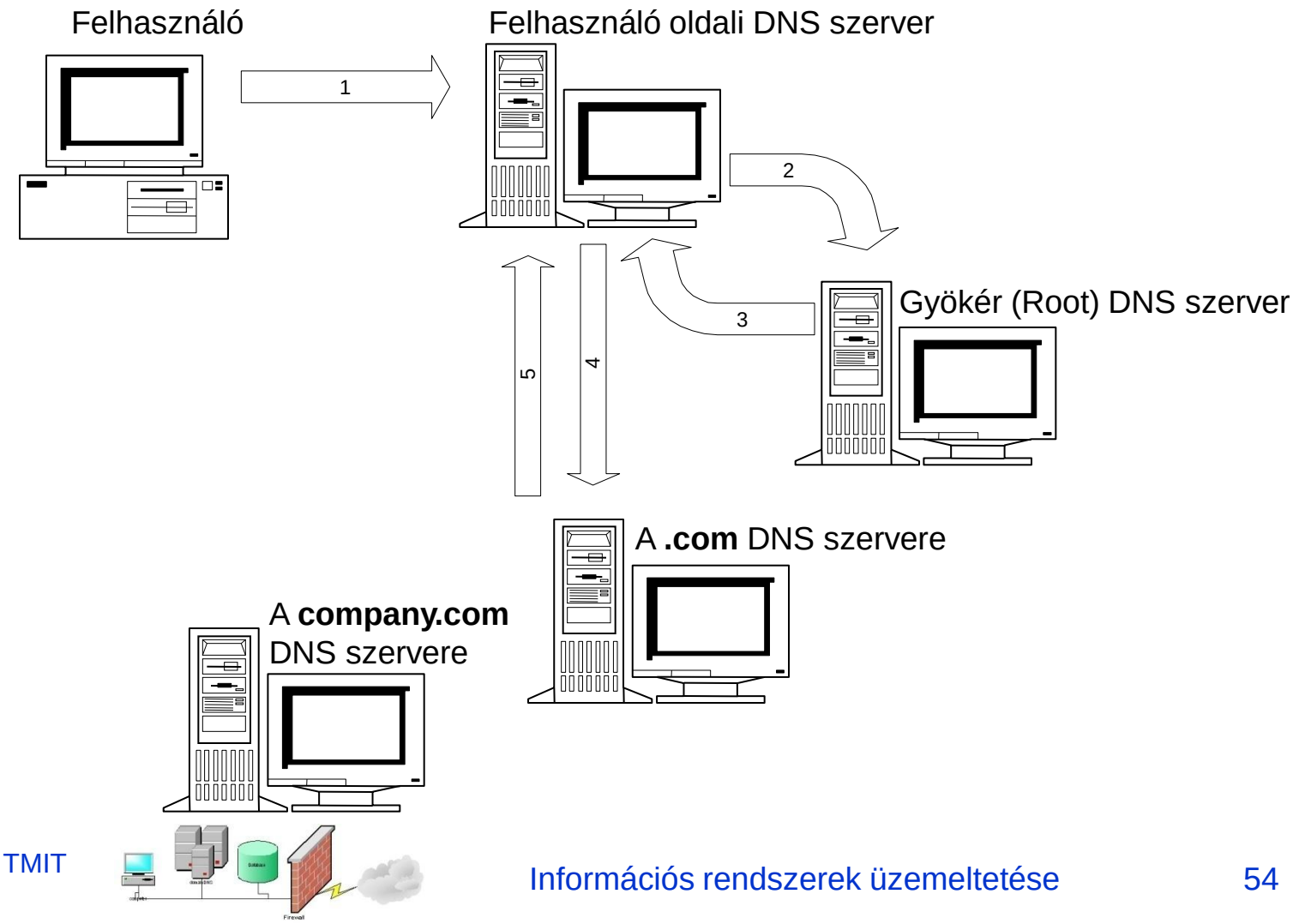
A DNS működése

(Az akarmi.company.com **domain név feloldásának lépései)**



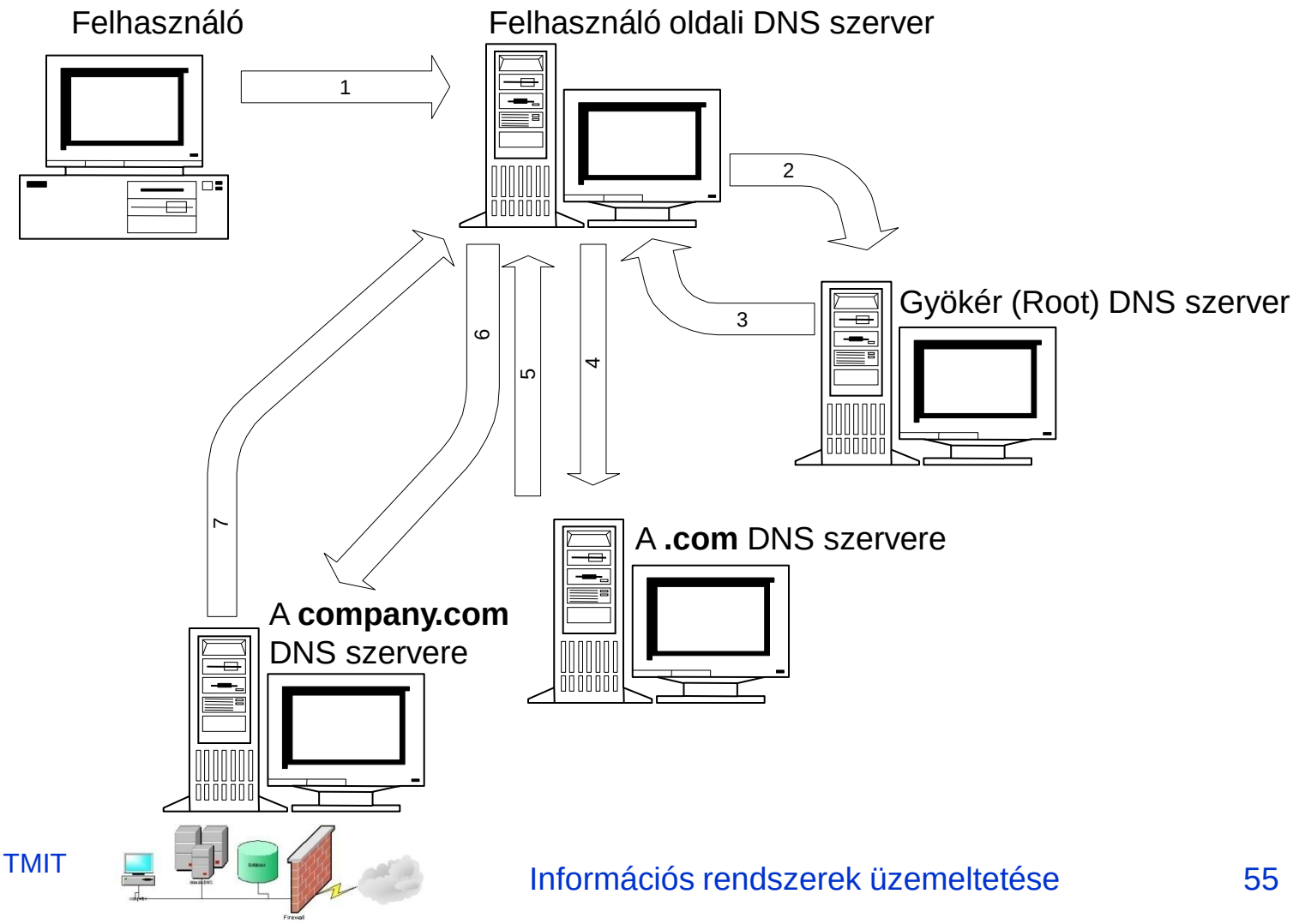
A DNS működése

(Az akarmi.company.com **domain név feloldásának lépései)**



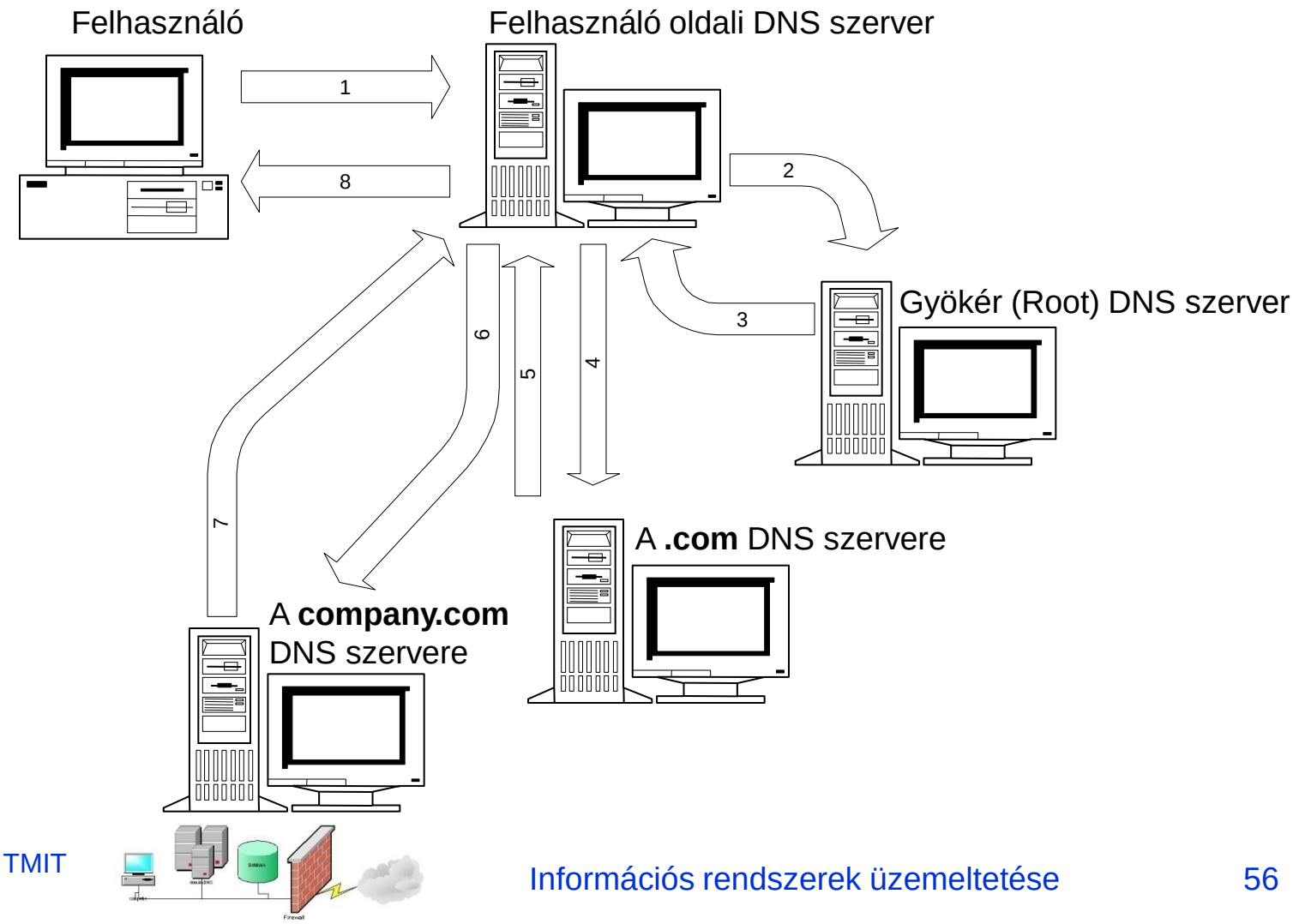
A DNS működése

(Az akarmi.company.com **domain név feloldásának lépései)**



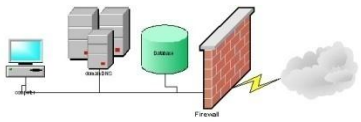
A DNS működése

(Az akarmi.company.com **domain név feloldásának lépései)**



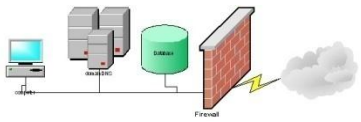
DNS Gyorsítótár (DNS Caching)

- Nemrég feloldott nevek - helyi gyorsítótárba
- A szerver visszaadja a kliensnek a gyorsítótárban lévő információt,
  - nem mérvadó (non-authoritative)
- Ha fontos a hatékonyság,
  - a kliens a nem mérvadó válasszal is megelégszik
- Ha a hitelesség a fontos
  - a kliens a hivatalos DNS szerverhez fordul:
    - a kapcsolat a név és az IP cím között még mindig érvényes?
- Hivatalos DNS szerver válaszol
  - TTL (Time To Live)

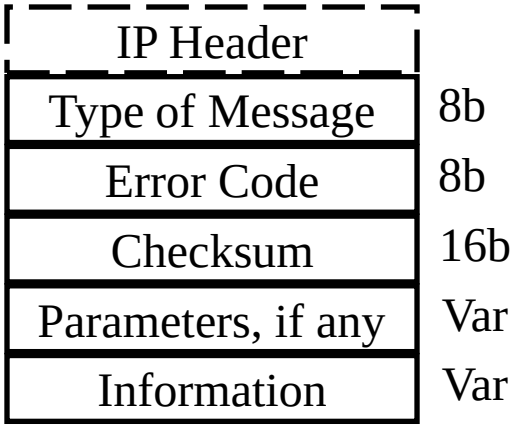


Internet Control Message Protocol (ICMP)

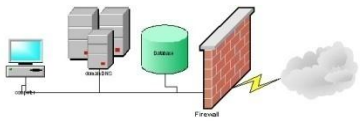
- Hibajelentésekre és IP szintű kontroll üzenetek továbbítására
- Direkt IP csomagokban
- Leggyakrabban használt debuggoló eszköz
  - Ping, traceroute



Üzenetformátum és -típusok



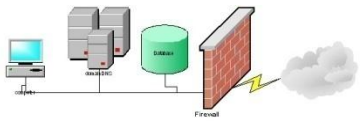
TYPE FIELD	ICMP Message Types
0	**Echo Reply (válasz adás)**
3	Destination Unreachable
4	Source Quench
5	Redirect (change a route)
8	**Echo Request (válasz kérés)**
11	**Time exceeded for a packet (TTL lejárt)**
12	Parameter problem on a packet
13	Timestamp request
14	Timestamp reply
15	Information request (obsolete)
16	Information reply (obsolete)
17	Address mask request
18	Address mask reply



Ping

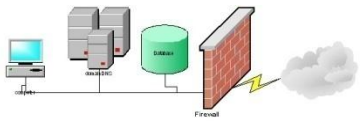
- Ping: tesztelésre
  - végpont elérhetőségét
  - körbefordulási idő – round trip time (RTT)
  - útvonal hossz (hop-okban)
  - esetlegesen record route opció

```
Ping alpha [152.66.246.10] with 32 bytes of data:

Reply from 152.66.246.10: bytes=32 time=114ms TTL=250
Reply from 152.66.246.10: bytes=32 time=26ms TTL=250
Reply from 152.66.246.10: bytes=32 time=23ms TTL=250
Reply from 152.66.246.10: bytes=32 time=27ms TTL=250

Ping statistics for 152.66.246.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 23ms, Maximum = 114ms, Average = 47ms
```



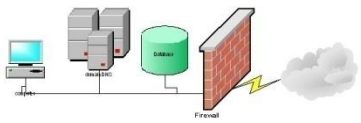
IP beállítások

- Alapvető beállítások egy gépen
  - IP cím/netmask
  - Default gateway
  - DNS szerver
- A beállítások kiegészíthetők
  - Alapértelmezett domain név megadása
  - Több DNS szerver



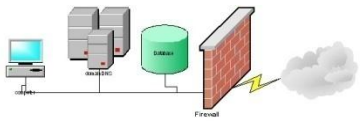
II. rész

Hálózatok

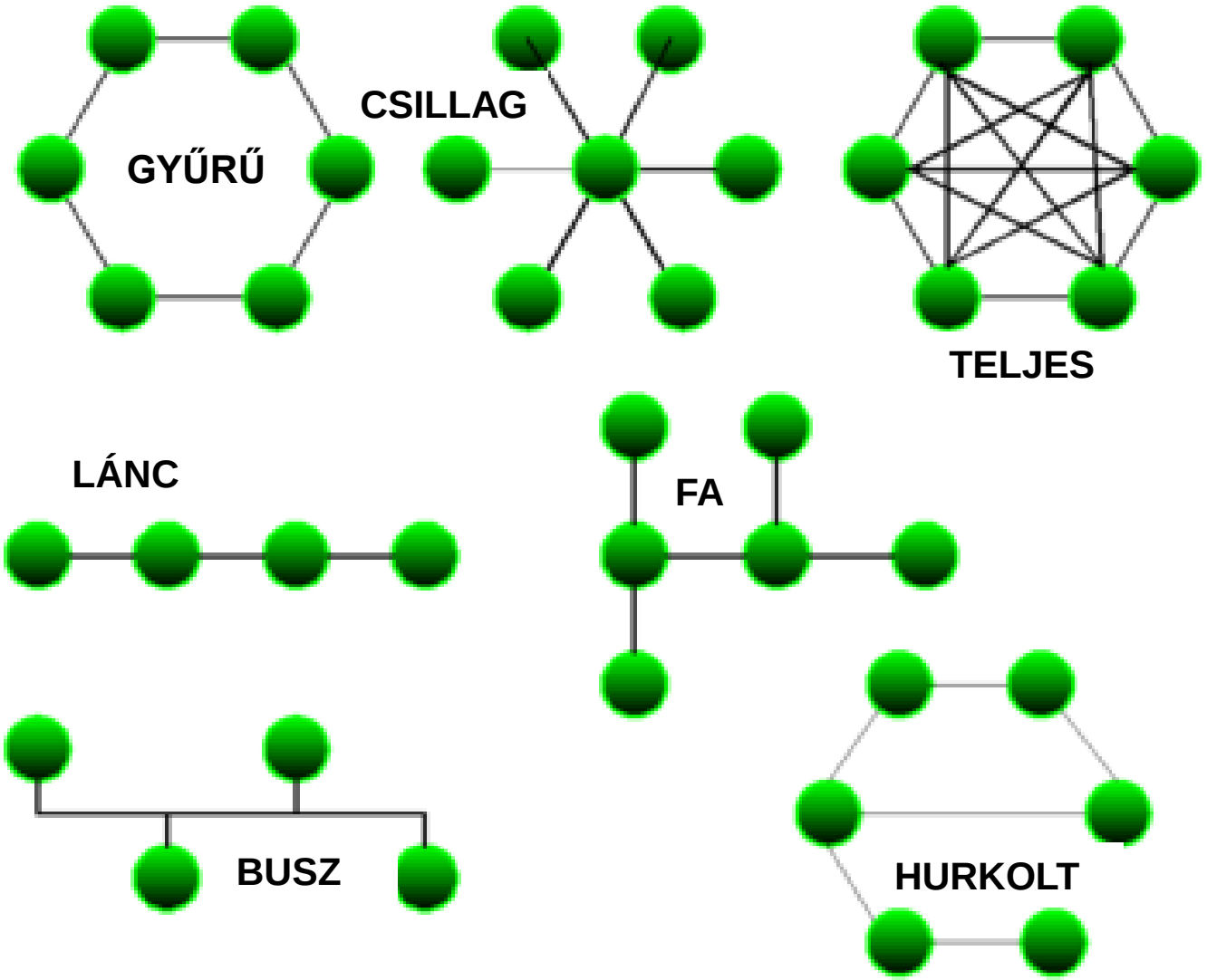


Hálózatok, hálózatok üzemeltetése

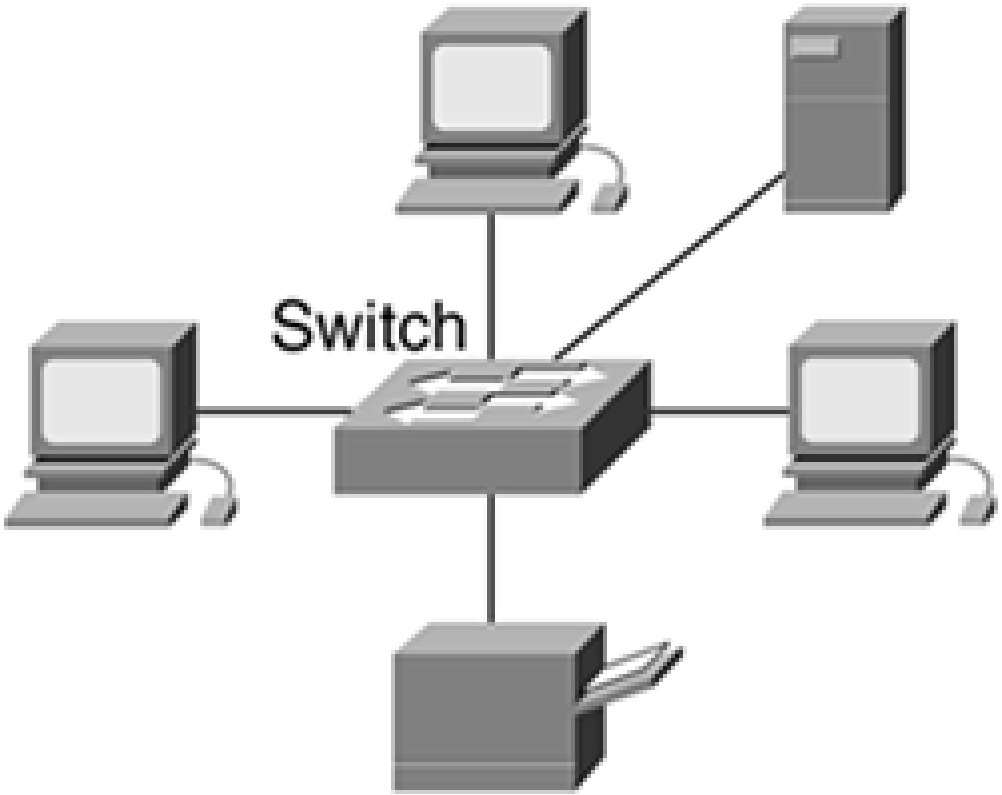
- Ez a tantárgy épít
  - Számítógép-hálózatok
  - Távközlő hálózatok tantárgyak ismereteire
- Ebben a fejezetben olyan hálózati témákat érintünk csak, amelyek az üzemeltetési feladatok megértéséhez fontosak
  - Hálózati topológiák
  - Fizikai és logikai hálózati térképek
  - Demarkációs pontok



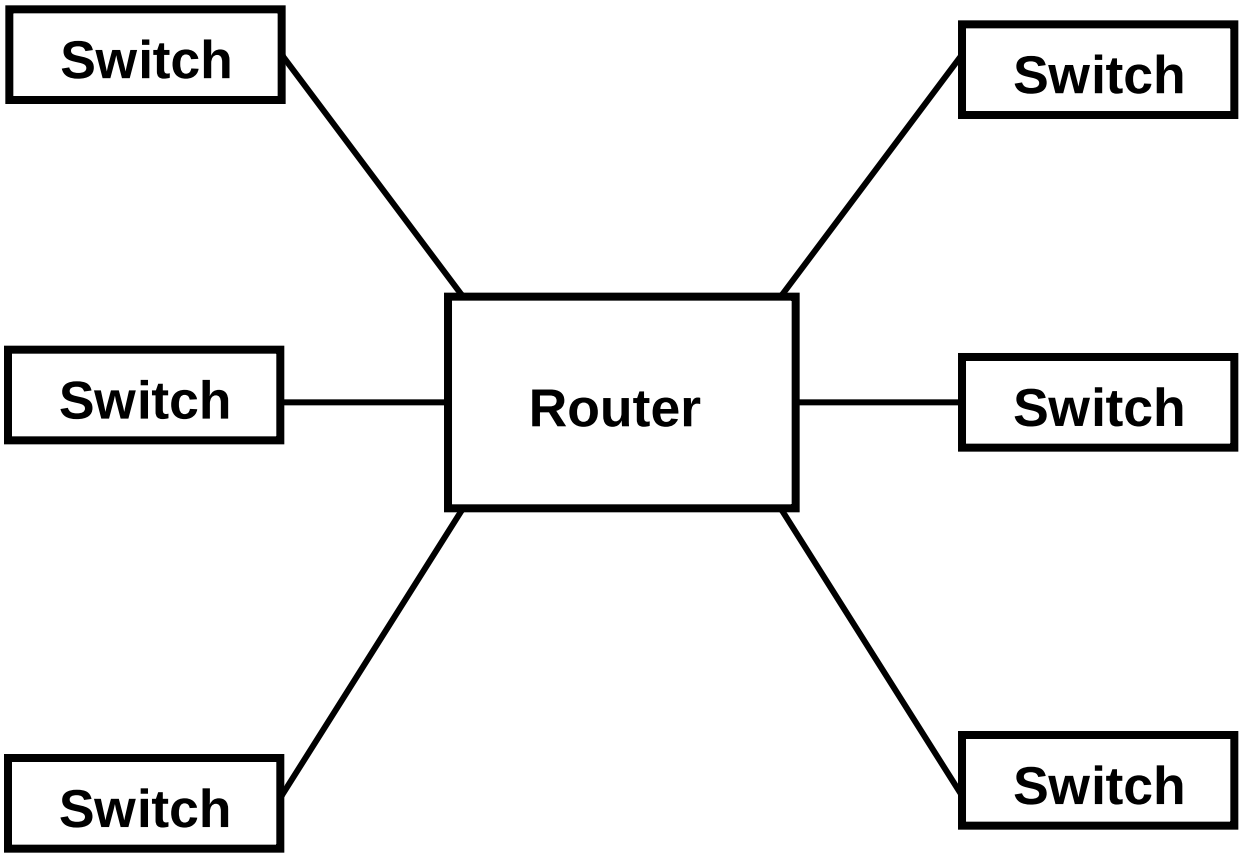
Hálózati topológiák



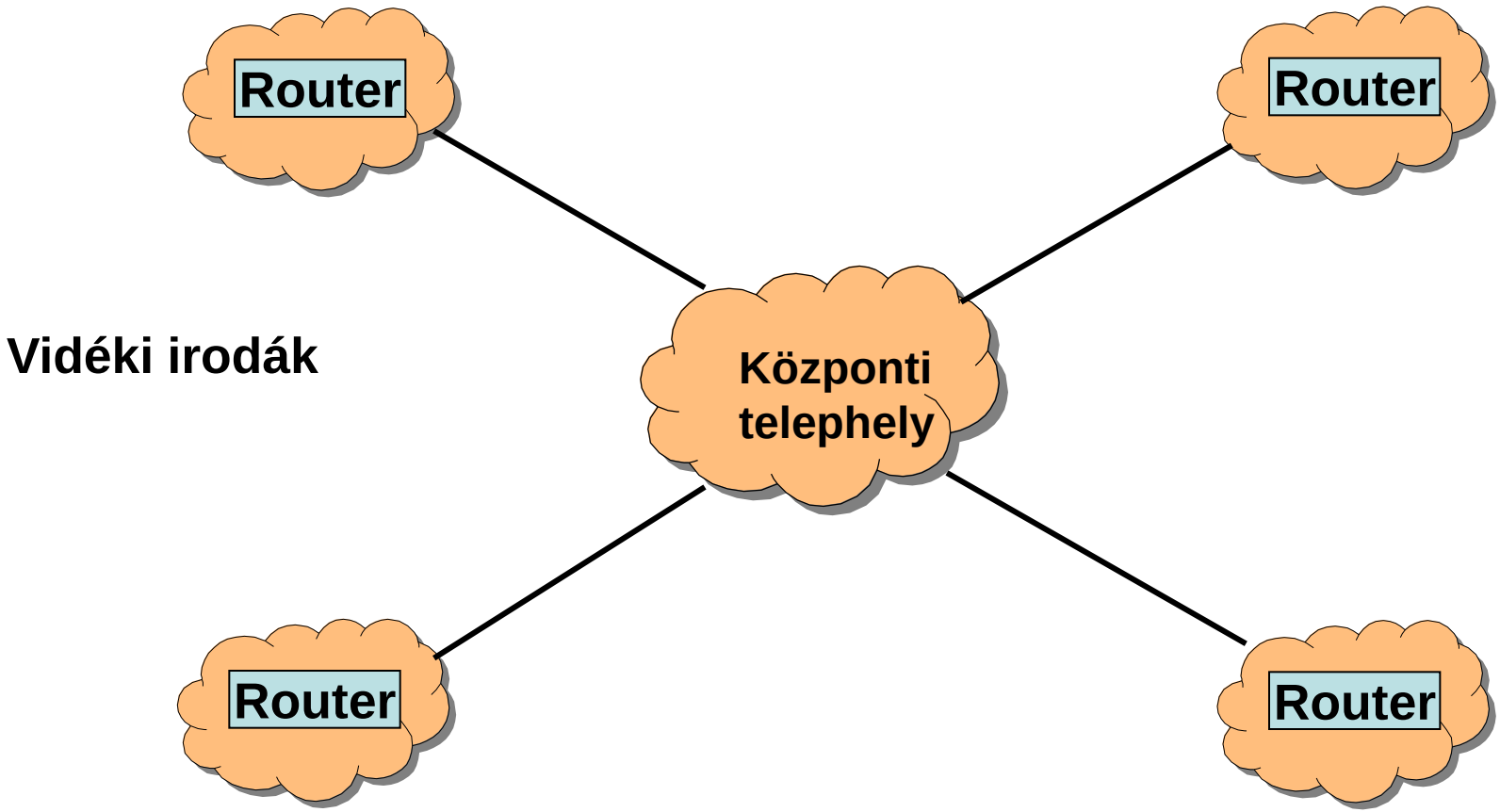
Egyszerű csillag LAN



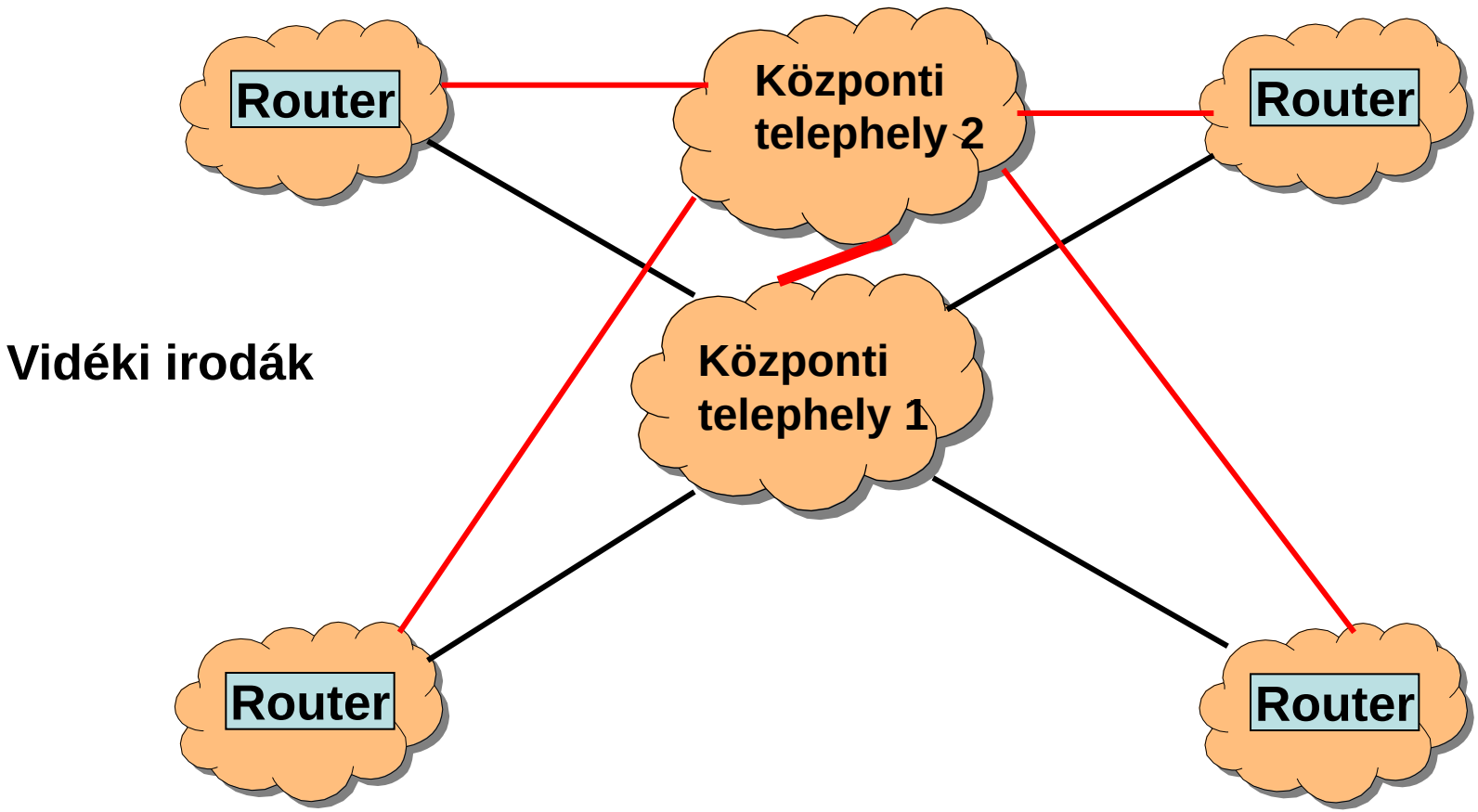
LAN, Campus hálózat - csillag



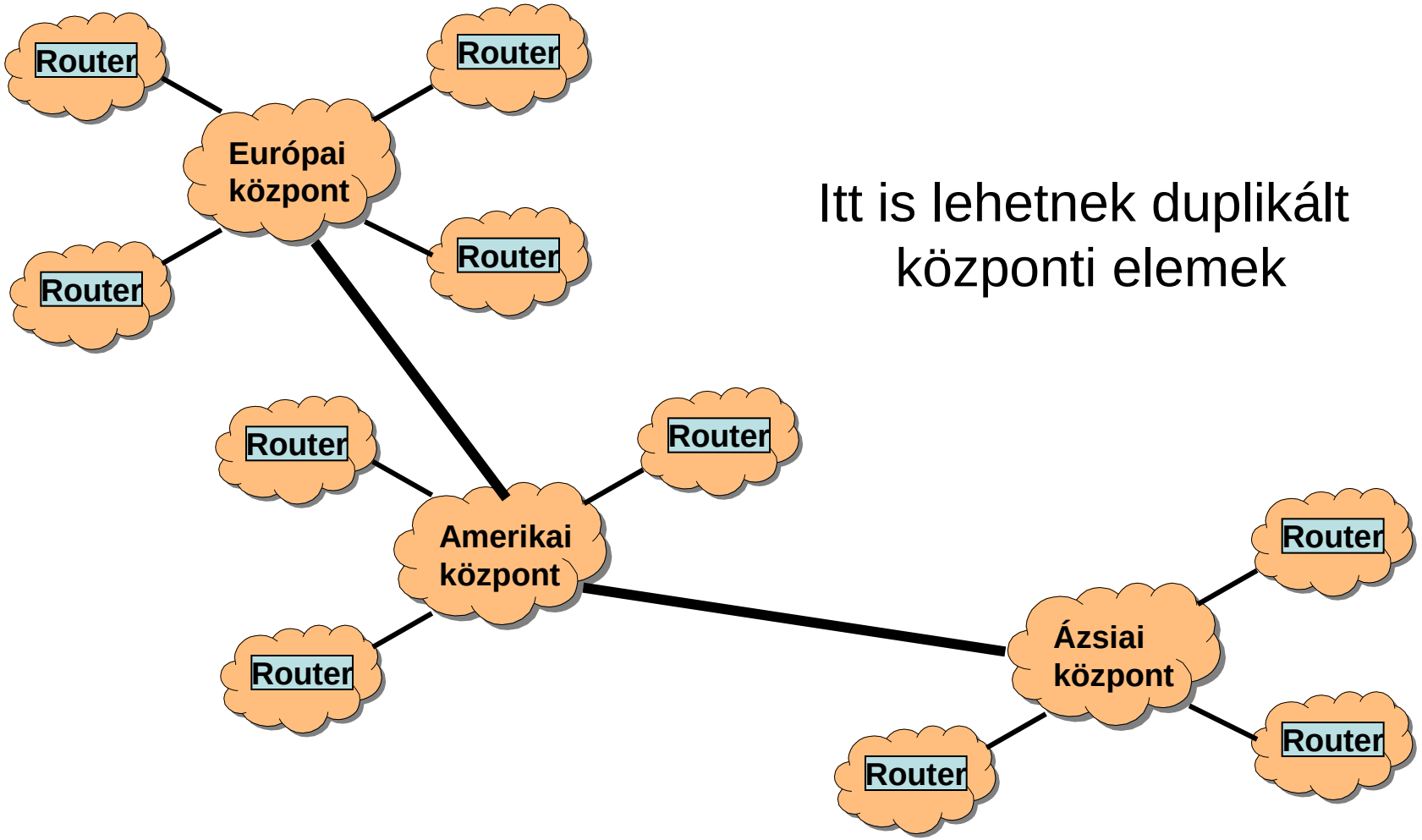
WAN – csillag


Router
Router
Vidéki irodák
Központi telephely
Router
Router

WAN – csillag – duplikált központ



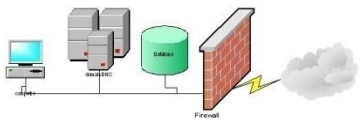
Többszörös csillag (fa)



Itt is lehetnek duplikált központi elemek

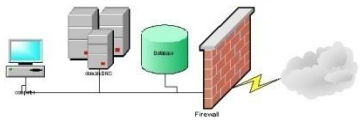
Decentralizált hálózatok

- Lánc
  - hiba: két szigetre esik szét
- Gyűrű
  - hiba esetén lánccá válik
- Hurkolt
  - (bizonyos) csomópontok között két (több) kapcsolat van
- Teljes (full mesh)
  - mindenki mindenkivel
  - megbízható, de drága (n*(n-1)/2 ÖK)

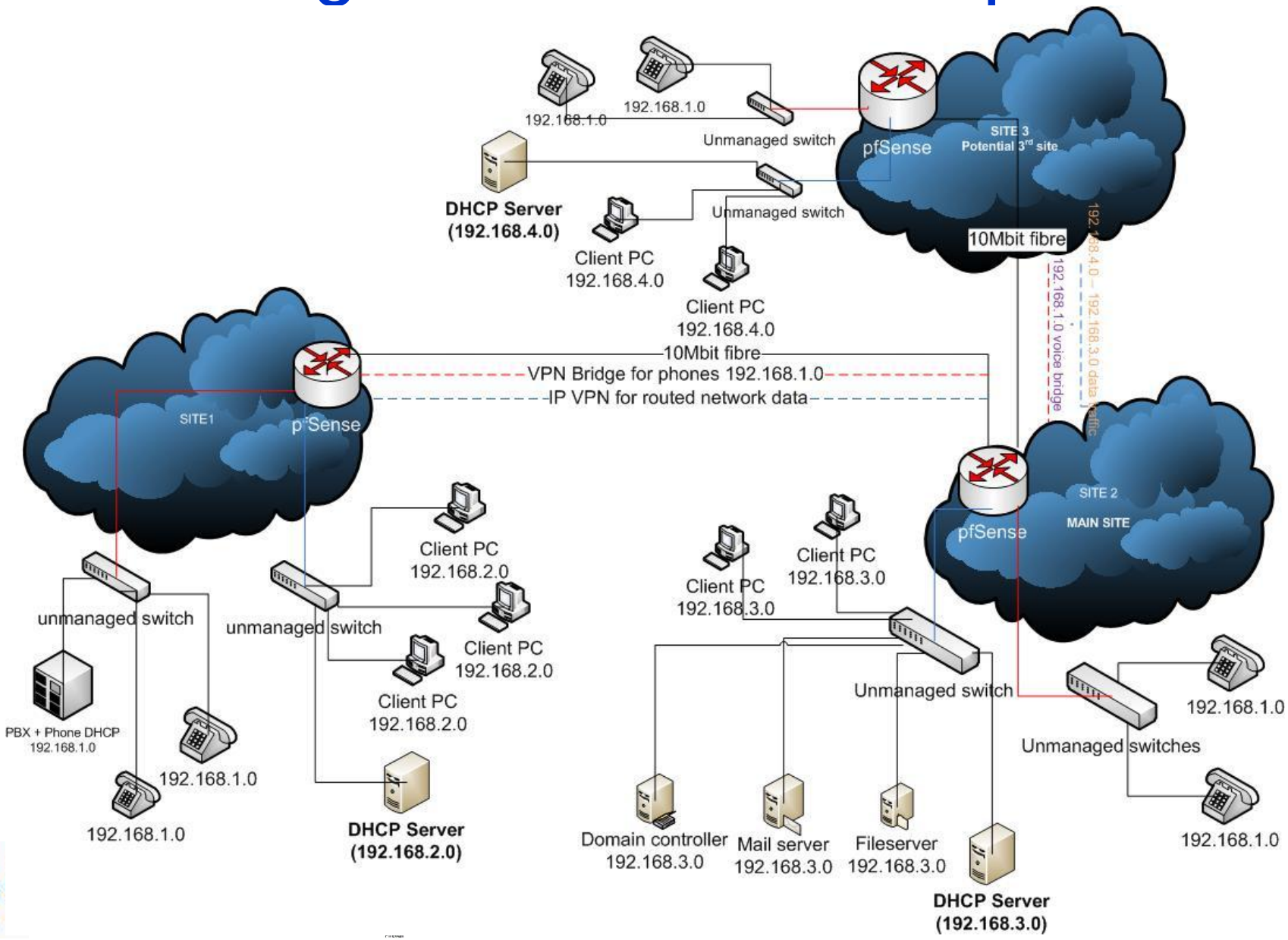


Fizikai és logikai hálózati térképek

- Fizikai:
  - kábelek útvonala, típusa, végződésük pontos helye
  - redundancia – (ha van): helyettesítő szakaszok pontos azonosítása
- Logikai:
  - logikai topológia: hálózatszámok, nevek, sebességek
  - használt protokollok
  - adminisztratív domének (ha több van)
- Címkézés (labeling) fontossága
- Mind a logikai, mind a fizikai térképeknek fel kell tüntetniük a hálózat határait is,
  - a külső hálózatokhoz való fizikai és logikai csatlakozásokat is.

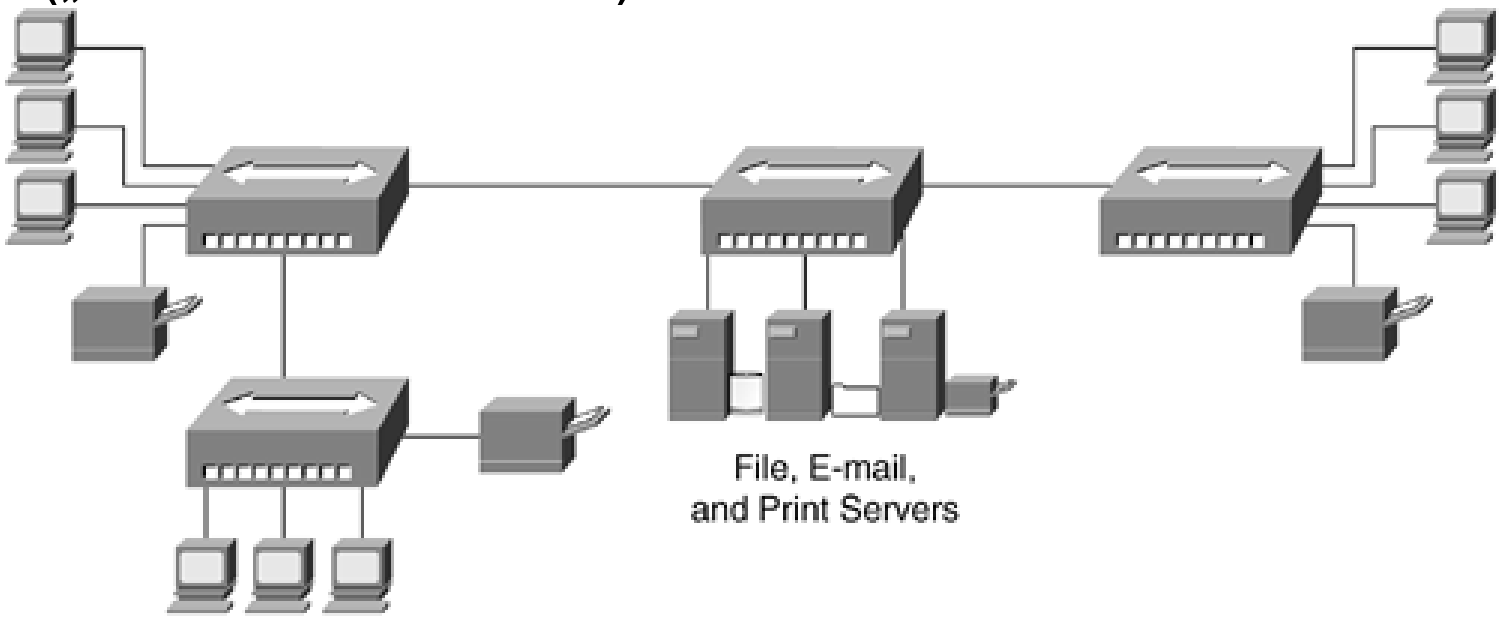


Logikai hálózati térkép



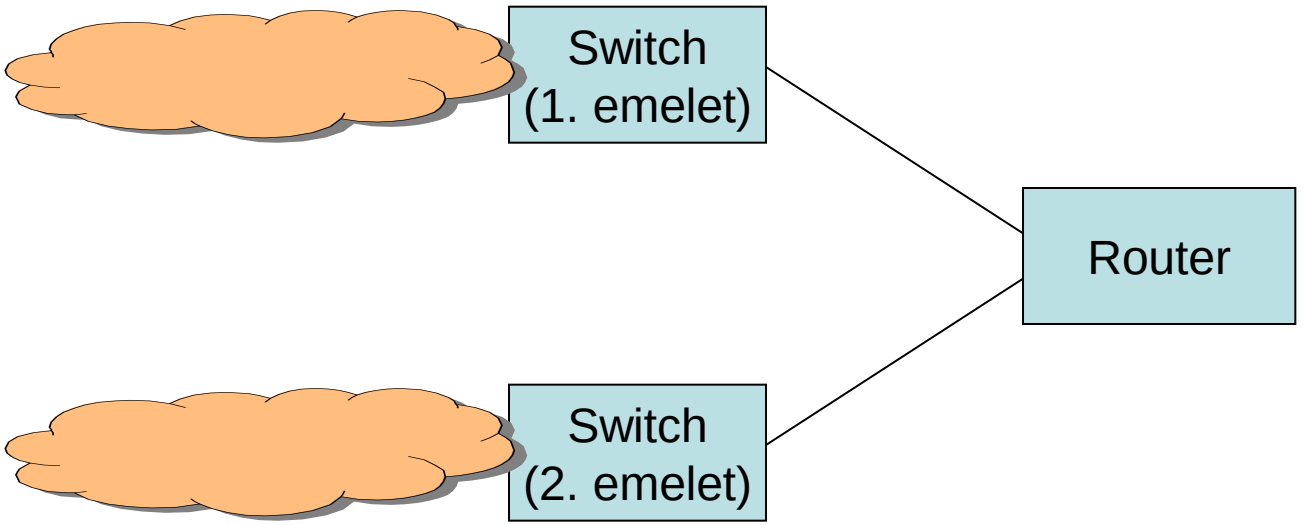
Tipikus logikai topológiák

- Flat topology
  - csak a kijáraton 3. rétegbeli entitás (router)
  - minden gép u.abban az IP címtartományban („broadcast domain”)



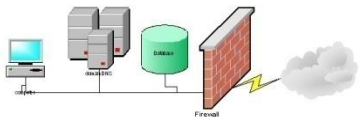
Tipikus logikai topológiák

- Location-based topology
  - pl. emeletenként egy-egy alháló (saját IP címtartomány)



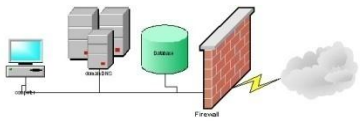
Tipikus logikai topológiák

- Functional-group based topology
  - fizikai elhelyezkedéstől függetlenül logikai csoportok szerint (eladók, mérnökök, menedzsment, marketing) flat network
  - szolgáltatások (nyomtatás, fájl-, névszerver, autentikáció) tipikusan csoportonként
  - 3. rétegbeli eszközök kapcsolják a központi hálózathoz



Demarkációs pont

- Definíció:
  - demarkációs pont a vállalati hálózat és egy kommunális szolgáltató (telefon, hálózati szolgáltató) közötti határpont
  - a demarkációs pontig a szolgáltató
  - onnan a vállalat a felelős
- Célszerű a demarkációs pontokat megfelelően feliratozni

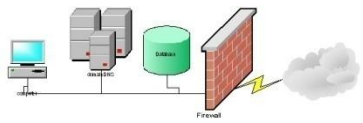


Információs rendszerek üzemeltetése

V. fejezet
Adattárolás, tároló rendszerek, tároló hálózatok

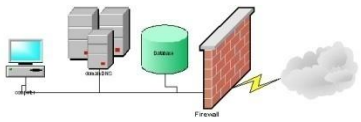
BME VIK TMIT

Mérnök-informatikus alapképzés



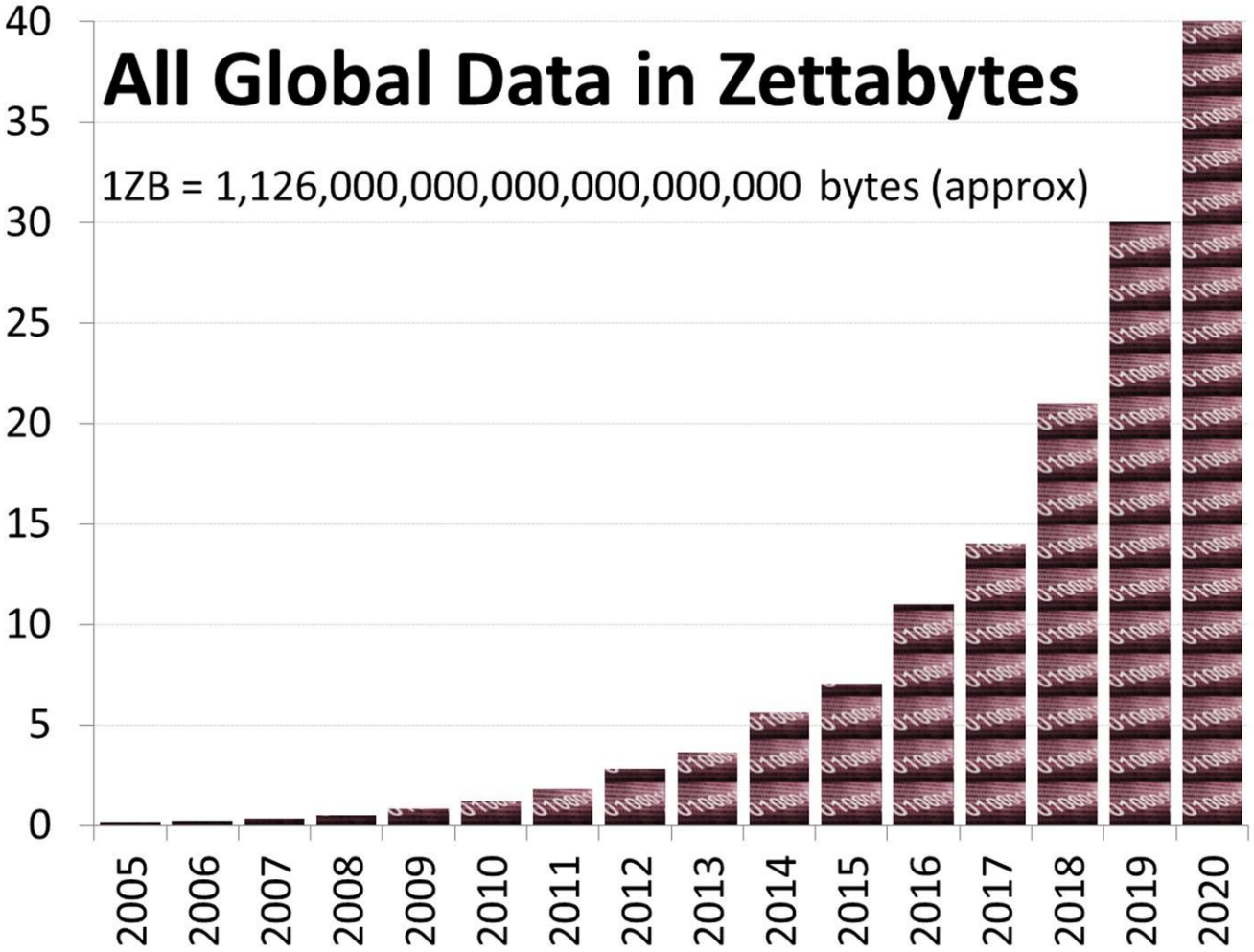
Adattárolók, adattárolás

- Adatok típusai
- Adattároló eszközök
- Diszkek megbízhatósága (RAID)
- Tárolórendszerek (DAS, SAN, NAS, IP SAN) és átviteli technológiák
- Adatmásolási eljárások (Volume/Flash copy)
- Virtualizáció
- Adattároló hálózatok menedzsmentje



Data Generated

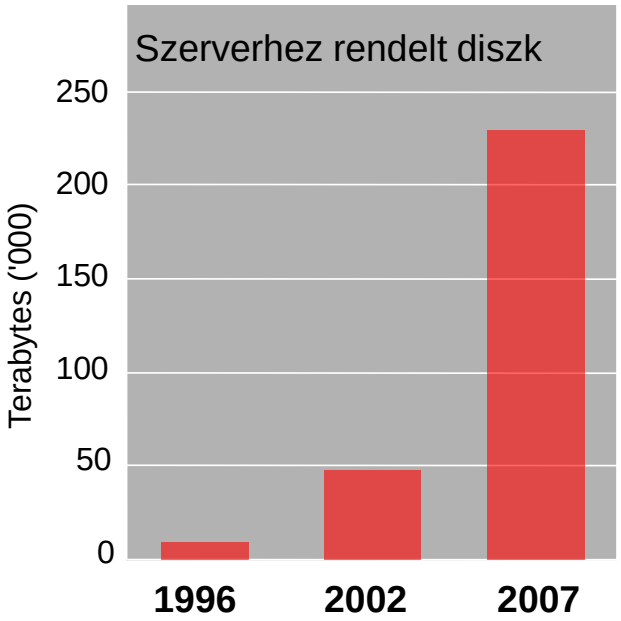
- Zetta = 10^{21}
- Az elmúlt két évben kb. 10x annyi adat született, mint addig összesen

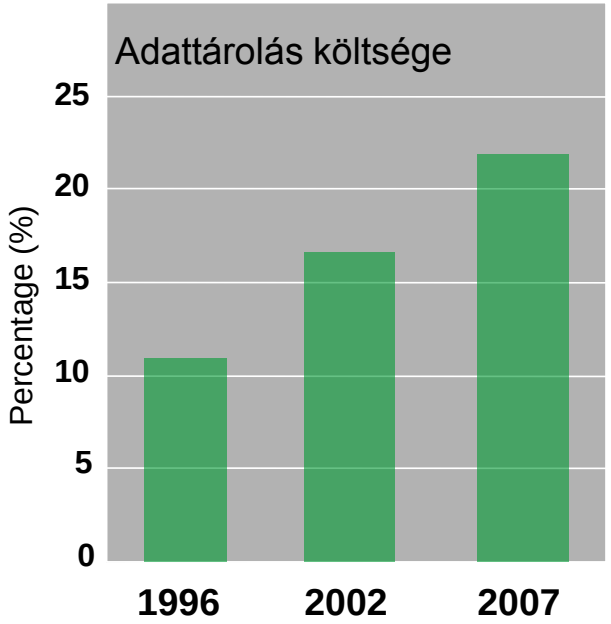


Tárkapacitás, költség

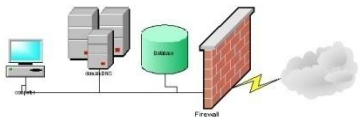
Több adat önmagában nem jelent több információt – de több költséget biztosan!

Diszk kapacitás

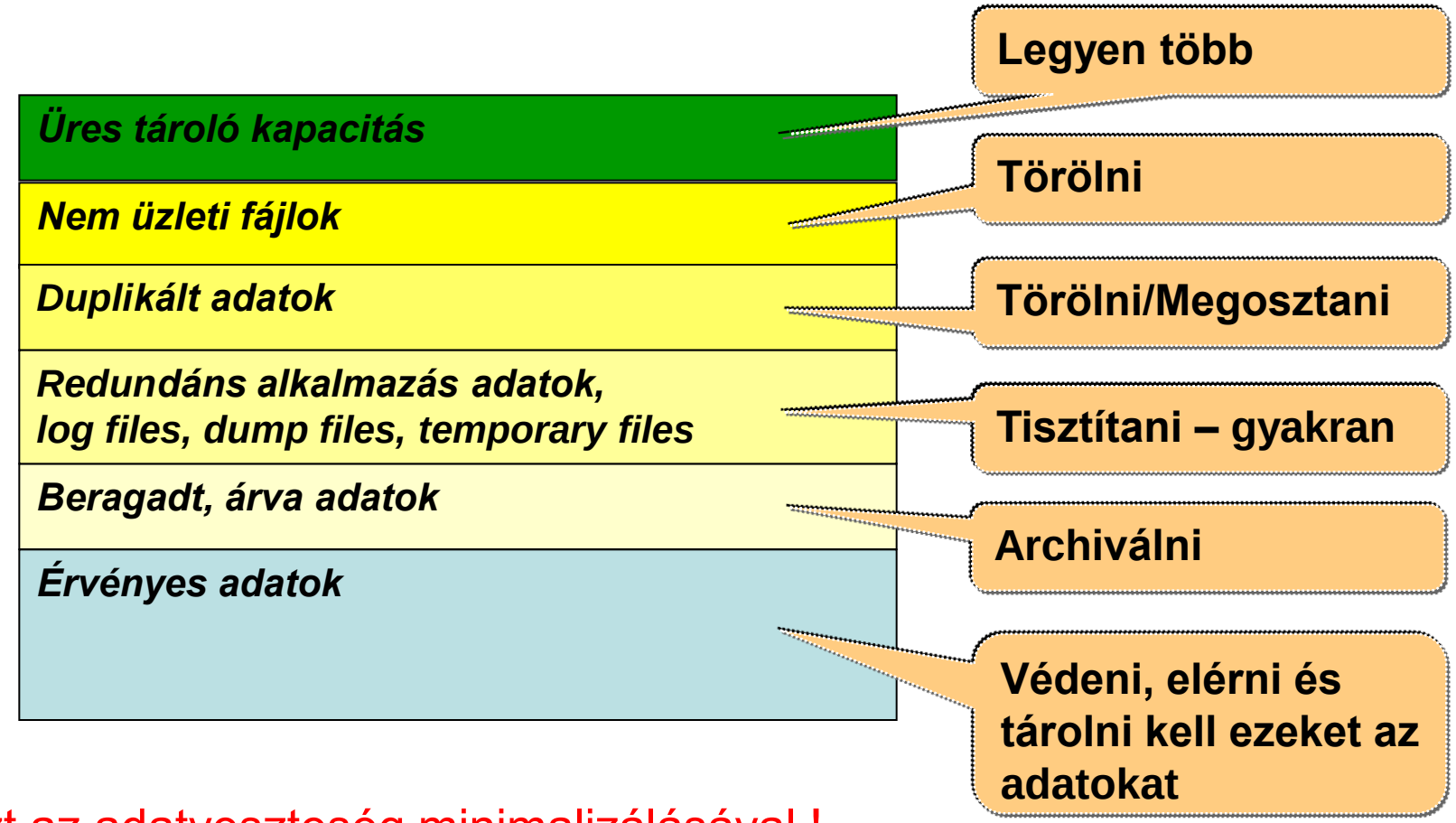




Forrás: International Technology Group, Sept 2003
* hardware, software, storage networking, personnel, backup operations, recovery, security

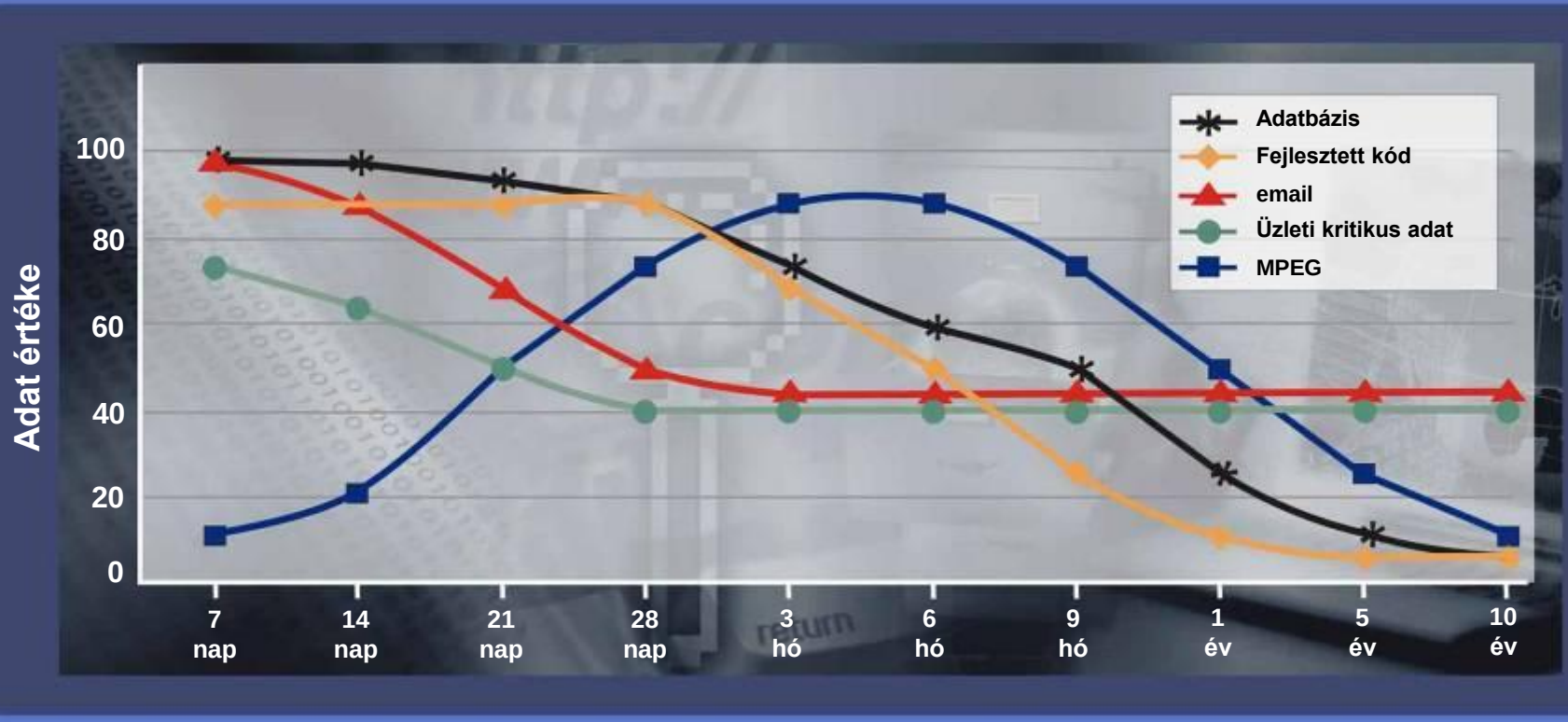


Adatok típusai



Mindezt az adatveszteség minimalizálásával !

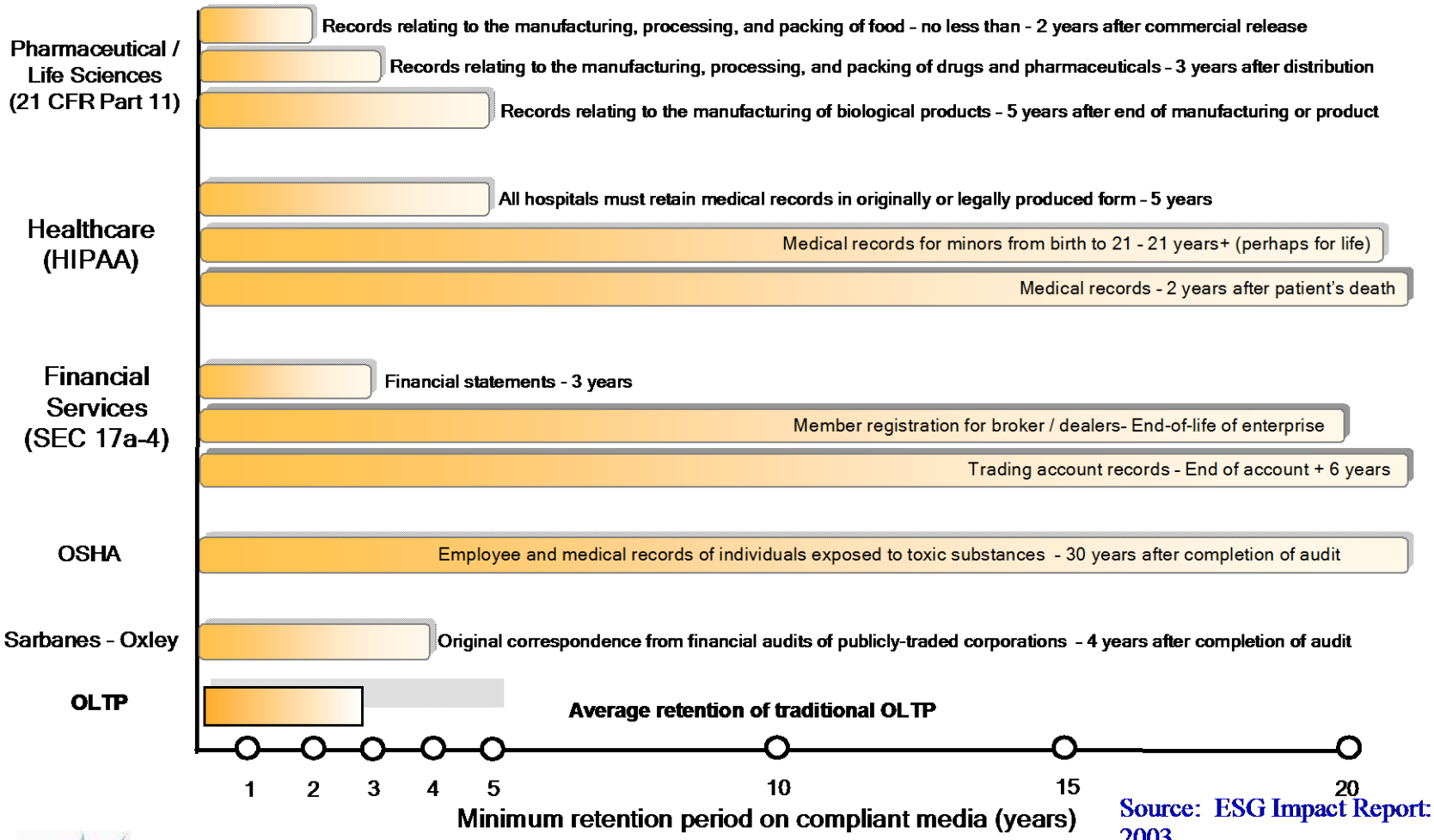
Az adat értéke annak minőségétől függően időben változó



Source of graph: Enterprise Storage Group

Az információ üzleti értéke szerint kell az IT befektetéseket végezni

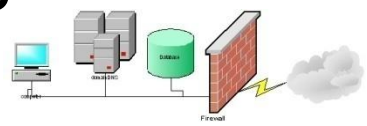
Kötelező adatmegőrzési időkre vonatkozó törvényi előírások



Source: ESG Impact Report: Compliance, May 2003

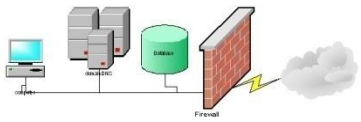
Adatfolyamok

Strukturált adatfolyam	**Strukturálatlan adatfolyam**
Forrása és célja ismert	Nem ismert
Server-to-Server	Client-to-client, Client-to-Server
Üzleti eszközök	Személyes eszközök
Speciális alkalmazások	E-mail, Web
Erős biztonság	Gyenge biztonság
Privát hálózatok	Publikus hálózatok
Tervezhető	Nehezen tervezhető, statisztika
Adatbázis adatok	Fájlszerverek
Monitorozható és ez alapján tervezhető	**Inkább házirendekkel szabályozható**



Adatgazdálkodás

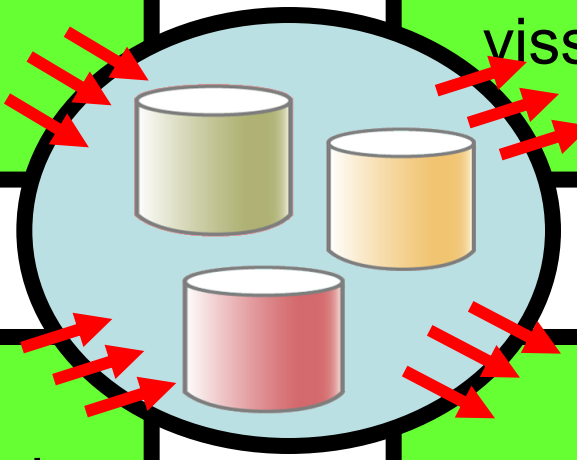
- IT infrastruktúra és menedzsmentjének egyszerűsítése, automatizálása
  - Cél: alacsonyabb élettartam-költség (TCO, *Total Cost of Ownership*), magasabb megtérülés (ROI, *Return on Investment*)
- Üzletfolytonosság, biztonság, adat-sérthetetlenség biztosítása
  - Cél: az üzlet folyamatosságának biztosítása
- Hatékony információ élettartam-menedzsment
  - Cél: az információt az értékének megfelelő tárterületen kell tárolni, az adat-megőrzési kötelezettségeket is figyelembe véve



Információ és adat életciklus, adattípusok

Az információ rögzítése és a megfelelő adatformátumba kódolása

Az adatformátum értelmezése az eredeti információ visszanyerése céljából



Index és meta-adatok készítése az adatok kereséséhez, katalogizálásához

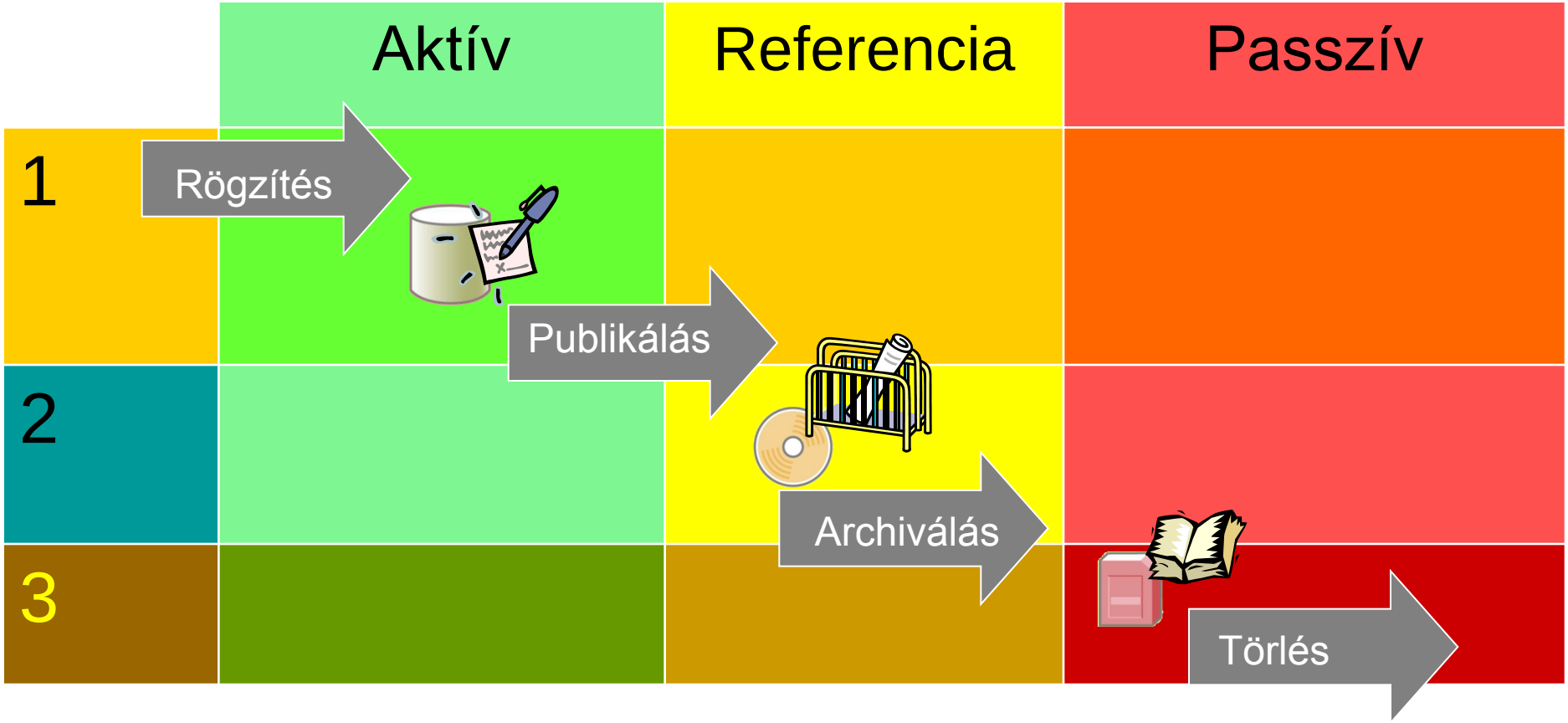
Adatbányászat – nagy mennyiségű adat logikai, statisztikai feldolgozása

Az egyes adatok iránti igény változó

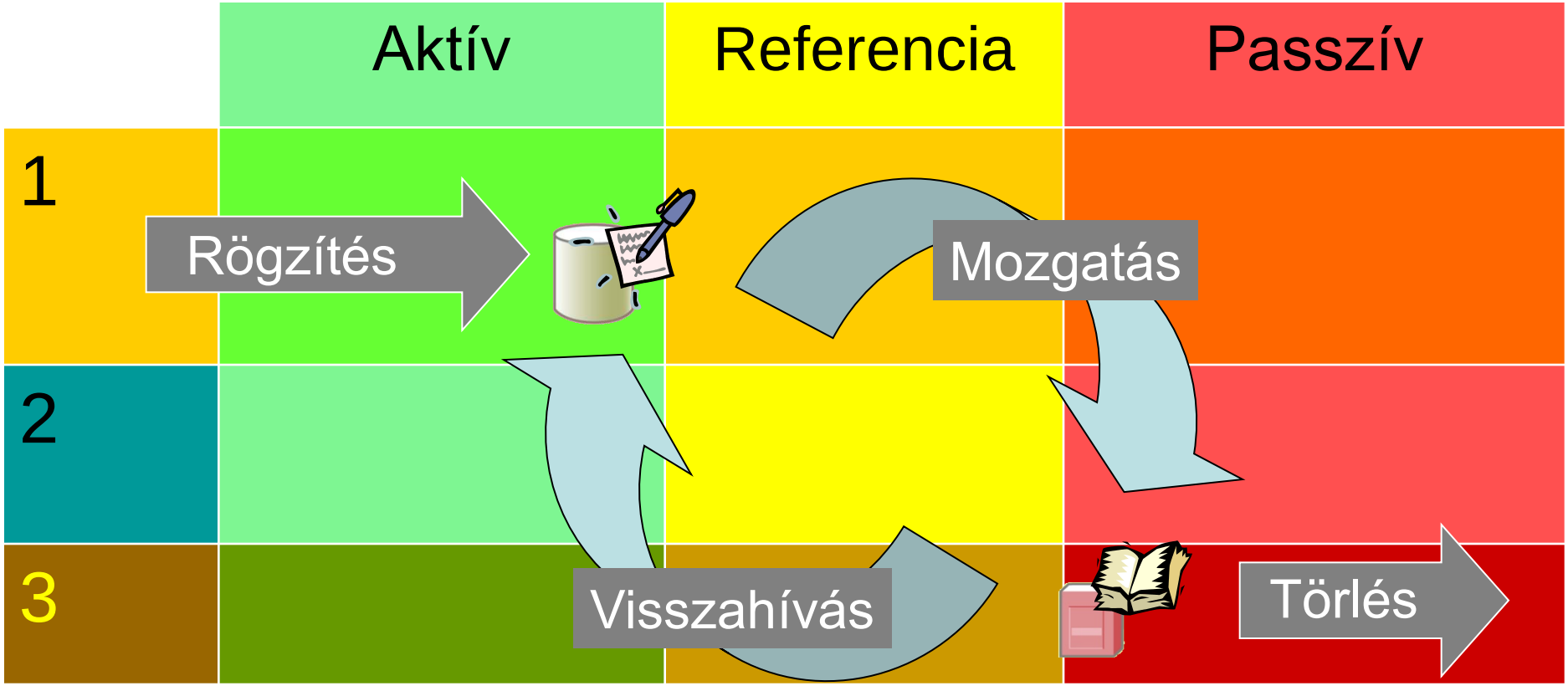
Aktív	Referencia	Passzív
Alkalmazás DB Online Transaction Processing (OLTP) Dokumentum kezelés Software fejlesztés	Riportok Tranzakciós jelentések Publikált dokumentumok, Web oldalak, email üzenetek Audio/Video felvételek	Archívumok Mentések Szkennelt képek Biztonsági videó állományok

Rögzítés → Publikálás → Archiválás → Törlés

Optimális adattárolási technológia: választás az adat értékének megfelelően



Hierarchikus tároló menedzsment (HSM) (Hierarchical Storage Management)



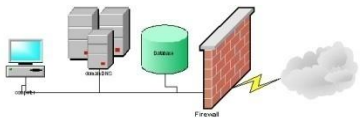
HSM paraméterei: adat mérete, típusa és az utolsó olvasás időpontja

Adattároló eszközök

	Előny	Probléma
Diszk 	• „Azonnali” adat elérés • Közvetlen írás/olvasás (R/W)	• Diszk csere • Tápellátás, hűtés • Élettartam 3-4 év! • Mozgó alkatrészek
Flash memó-ria 	• Nincsenek mozgó alakatrészek • Viszonylag gyors	• Kis kapacitás • (Még) drága
Optikai 	•Másodlagos tároló – automata könyvtárak • WORM (*Write Once Read Many*)	• Nem igazán tartott lépést a diszk és szalag fejlődéssel, SOHO eszköz (*Small Office Home Office*)
Szalagos 	•10-20x olcsóbb, mint a diszkes tároló • 30 éves adatmegőrzési idő	• Nem azonnali elérés • Soros írás/olvasás

Diszkek megbízhatósága

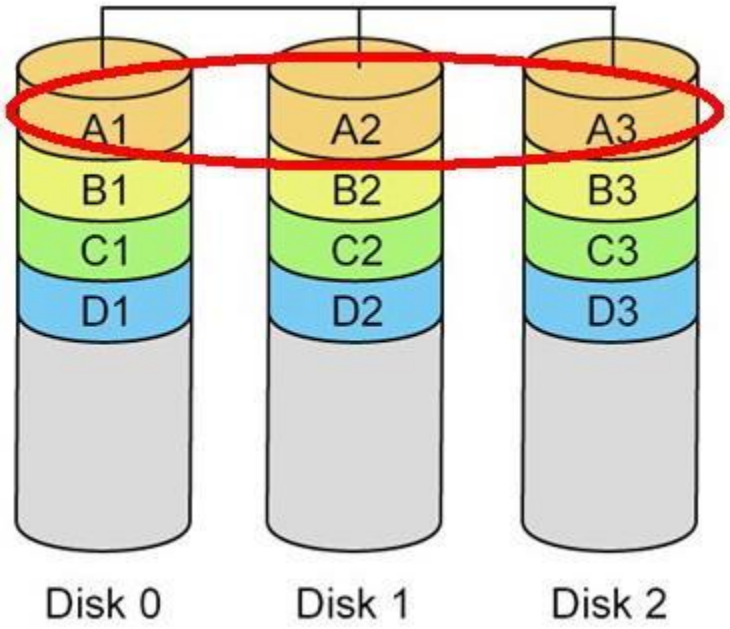
- A szervereken tárolt adatok ne sérüljenek meg
- Eredetileg egyetlen nagy, nagymegbízhatóságú diszk
  - SLED: Single Large Expensive Drive
  - Drága…
  - MTBF (Mean Time Between Failure)
    - Kb. 750 000 óra (kb. 85 év)
    - De egy nagy(??) tárolótömb 1000 diszkkel
    - MTBF: 750 000 óra / 1000 = kb. 1 hónap



RAID Redundant Array of Independent (Inexpensive) Disks

- 1987 California, Berkeley Egyetem
- RAID 0, 1-5, 6

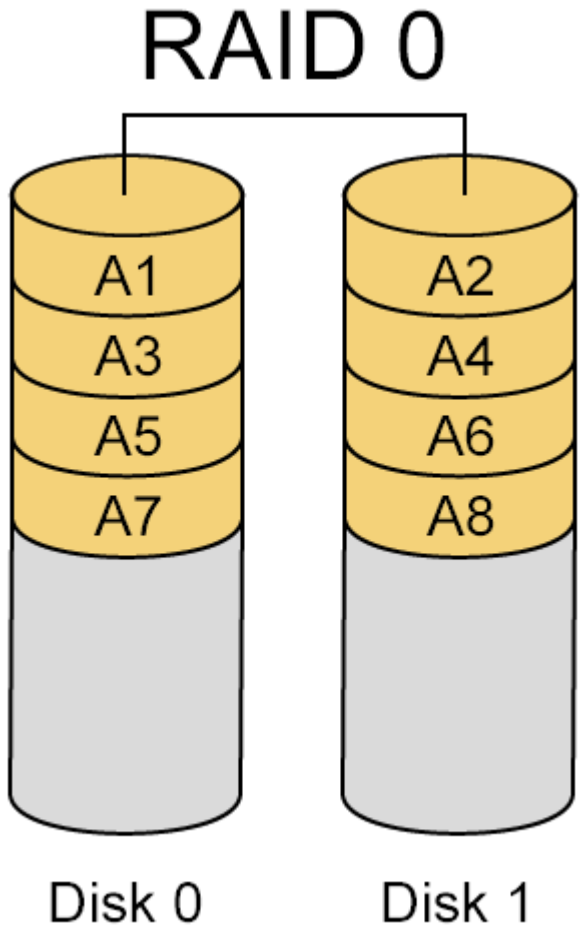
- Lemezek sávokra (stripes) osztása



RAID 0 - striping

- Nem biztonság növelési cél
- Kapacitásnövelés
- Sebességnövelés

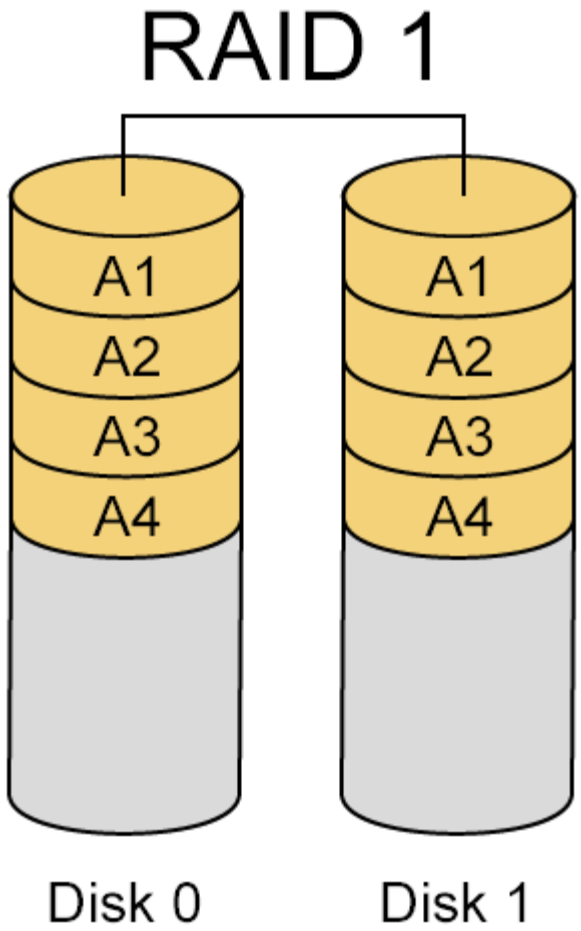
  (párhuzamos írás/olvasás)



RAID 1 – diszk tükrözés (mirroring)

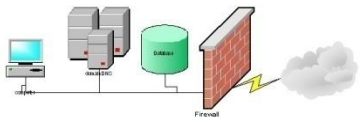
- Diszk duplikálás
- Nagy megbízhatóság
- Nagy (2x) méretnövekedés

- Lehet közel ekkora biztonság, kisebb veszteséggel?



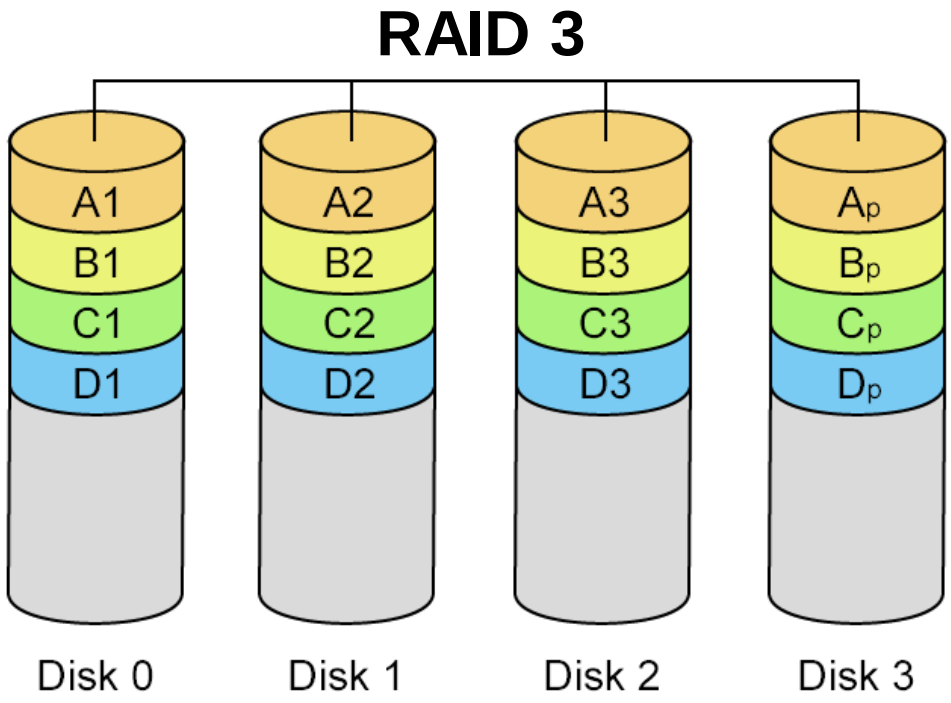
RAID 2 – hibajavító kód

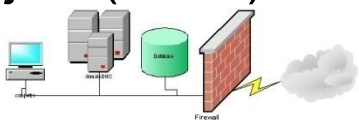
- Sávokra bontás
- Egyes meghajtókon hibajavító kódokat (ECC – Error Correcting Code) tárolnak
  - Képes a diszkhiba detektálására, javítására
- Ma már nem használják, mert ma már a meghajtókon belül képeznek hibajavító kódokat



RAID 3 – paritásdiszk

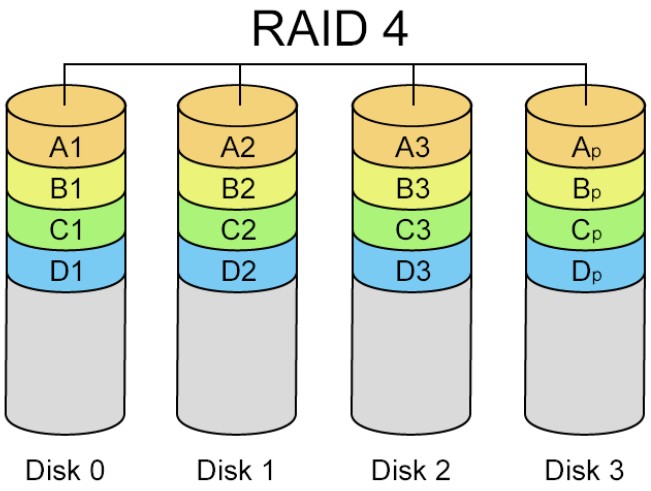
- +1 diszk: paritás (XOR)
- Egy meghajtó kiesése: a többiből XOR művelettel helyreállítható – idő, lelassul
- Diszkhibát nem érzékel
- Tipikus: 2+1, 5+1,
  8+1, 14+1
- Paritásdiszk korlátoz
- Kis sávok, mindig egész stripe művelet (Adatdiszkek egyszerre érhetők el)
  - Single user
  - Nagy fájlok (video)





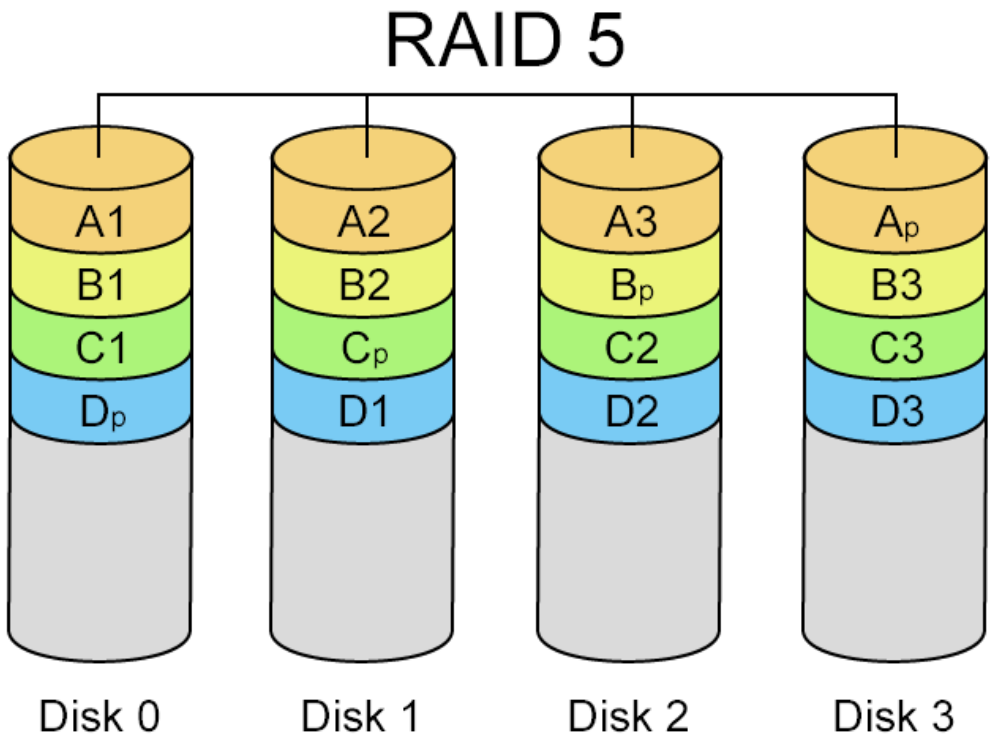
RAID 4

- Hasonló a RAID 3-hoz, de nagyméretű sávok
- Közvetlenül bármelyik diszkhez hozzáférhetünk
  - Párhuzamos kiszolgálást lehetővé tesz
  - Paritásdiszk nagyon korlátoz!
- Nem használják a gyakorlatban



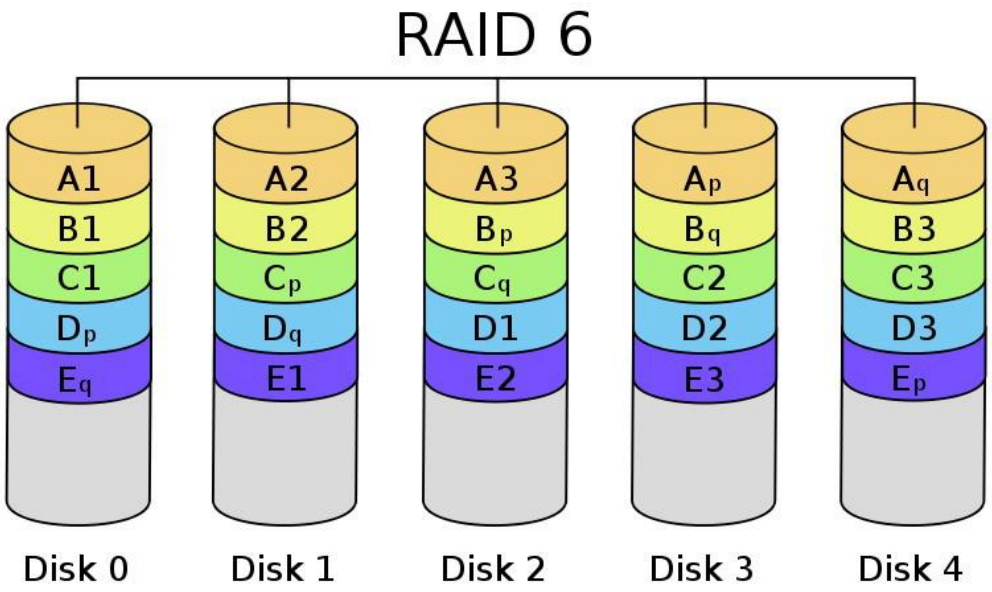
RAID 5 – elosztott paritás

- Paritás egyenletesen szétosztva
- Kiküszöböli a paritásmeghajtó okozta szűk keresztmetszetet
- Közvetlenül elérhetők a diszkek
- Változtatható sávméret

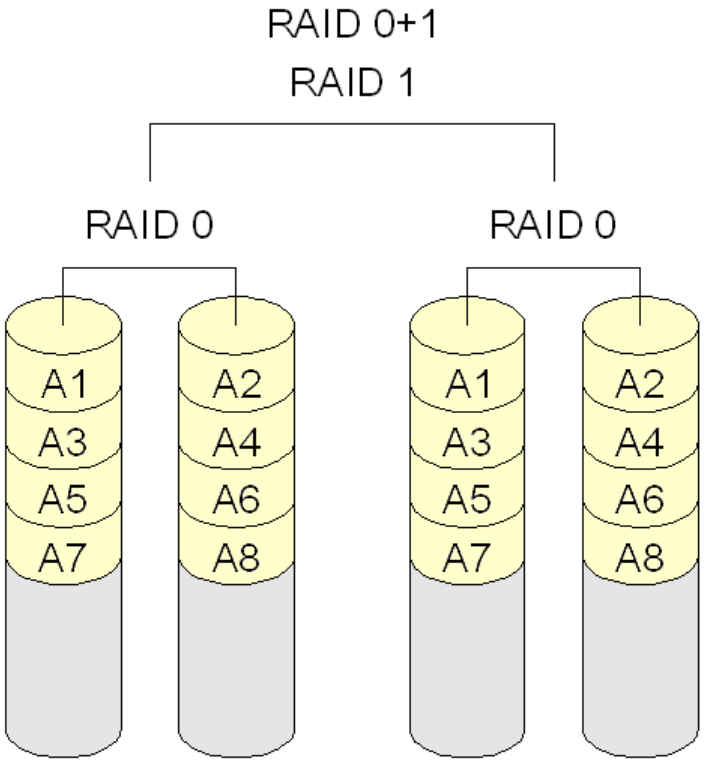


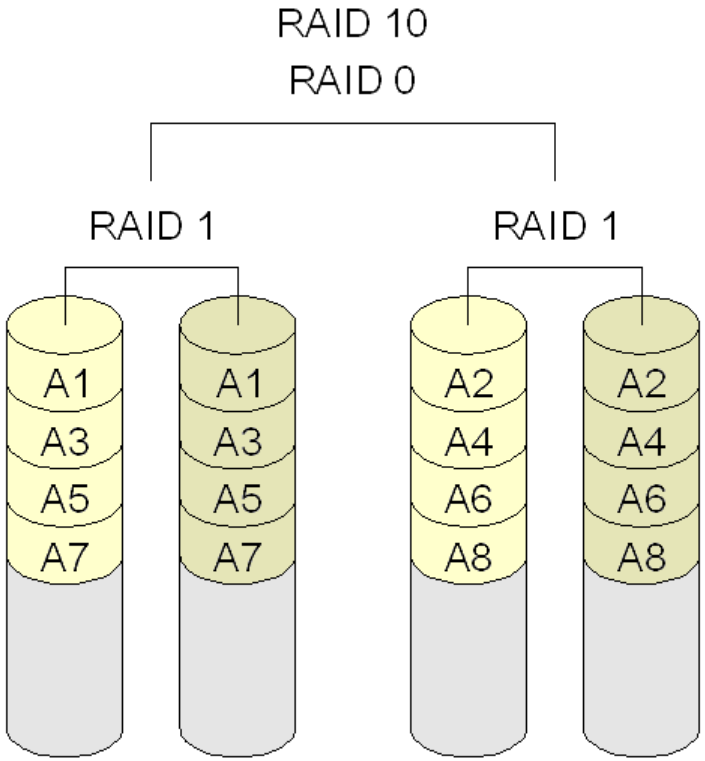
RAID 6 – kettős paritás

- Sor (XOR – P) és oszlop (Reed-Solomon kód – Q) paritás
  - kettős hiba ellen is véd – de lassú
- Diszkek között szétosztva



RAID 01, RAID 10

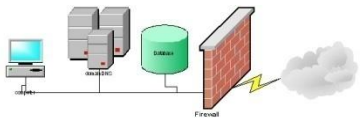




Egyformák?

Hiba: egész stripe – nincs tükrözés (!!) csak a felén nincs tükrözés

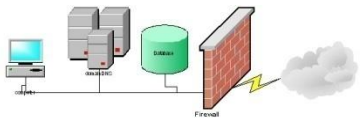
Helyreállítás: egész stripe(!!) csak a rossz diszk



RAID

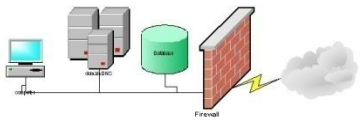
- Gyakorlatban 0,1, 5 elterjedt

- RAID csak a FIZIKAI diszk hibák ellen véd!
  - Logikai hibák ellen: mentés!



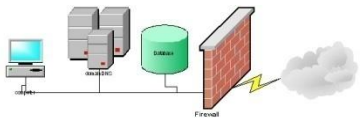
Tároló rendszerek

- DAS – Direct-Attached Storage
- SAN – Storage Area Network
- NAS – Network-Attached Storage
- IP SAN (iSCSI)



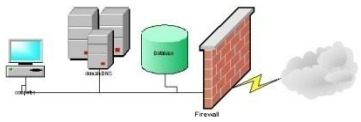
DAS – Direct-Attached Storage

- A tároló közvetlenül a szerverhez csatlakozik
  - Blokkszintű hozzáférés
  - Főképp kis rendszereknél
- Két alaptípus
  - Belső (Internal DAS)
  - Külső (External DAS)



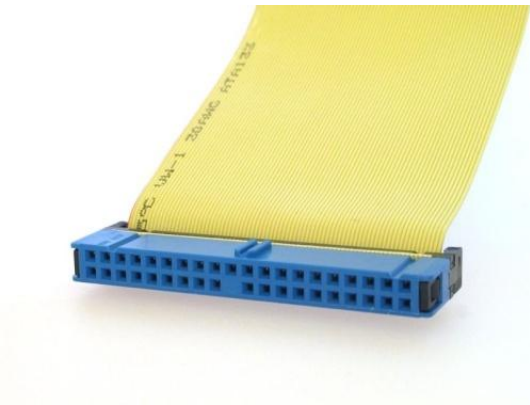
Internal DAS

- A tároló közvetlenül a szerverhez kapcsolódik belső soros vagy párhuzamos buszon keresztül
  - Távolság korlátozott
  - Általában a buszhoz csak korlátozott darabszámú eszköz csatlakoztatható
    - (P)ATA vagy SATA csatlakozó
  - Nagy helyet foglal a szerveren belül
    - Nehezebb karbantartás



(P)ATA

- Párhuzamos elérésű HDD interfész
- PATA – Parallel Advanced Technology Attachment
  - UDMA – Ultra Direct Memory Access
  - *IDE – Integrated Device Electronics*
  - EIDE – Enhanced IDE
- 40 & 80 eres kábel
  - 40 eres: UDMA max. 33 MB/s
  - 80 eres: UDMA 66, 100, 133 MB/s
  - nagy helyigény => fejlesztés megállt (~2004)

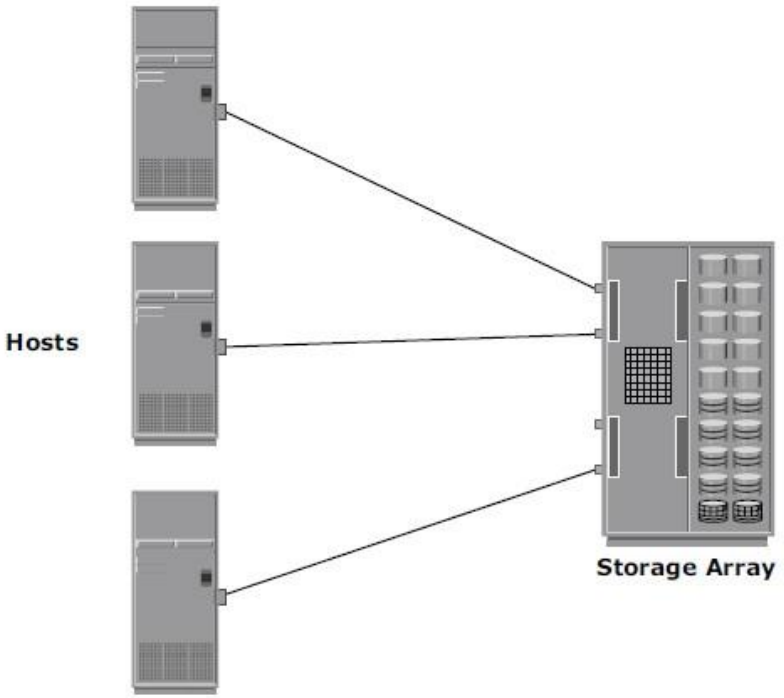


SATA

- Serial Advanced Technology Attachment (SATA)
- Pont-pont összeköttetést teremt a SATA host adapter és a SATA eszköz között
  - Új csatlakozó felület
  - Nagyobb átviteli sebesség
    - (P)ATA max. 133 MB/s
    - SATA 1,5 Gbit/s (150 MB/s)
    - SATA 2.0: 3 Gbit/s (300 MB/s)
  - A csatlakozó kábel 4 eres, maximális hossza 1 m

External DAS

- A szerver közvetlenül kapcsolódik egy külső tárhoz
  - Nagyobb távolság
  - Általában nem (annyira) korlátozott a csatlakoztatható eszközök száma
  - SCSI (vagy FC) csatlakozás

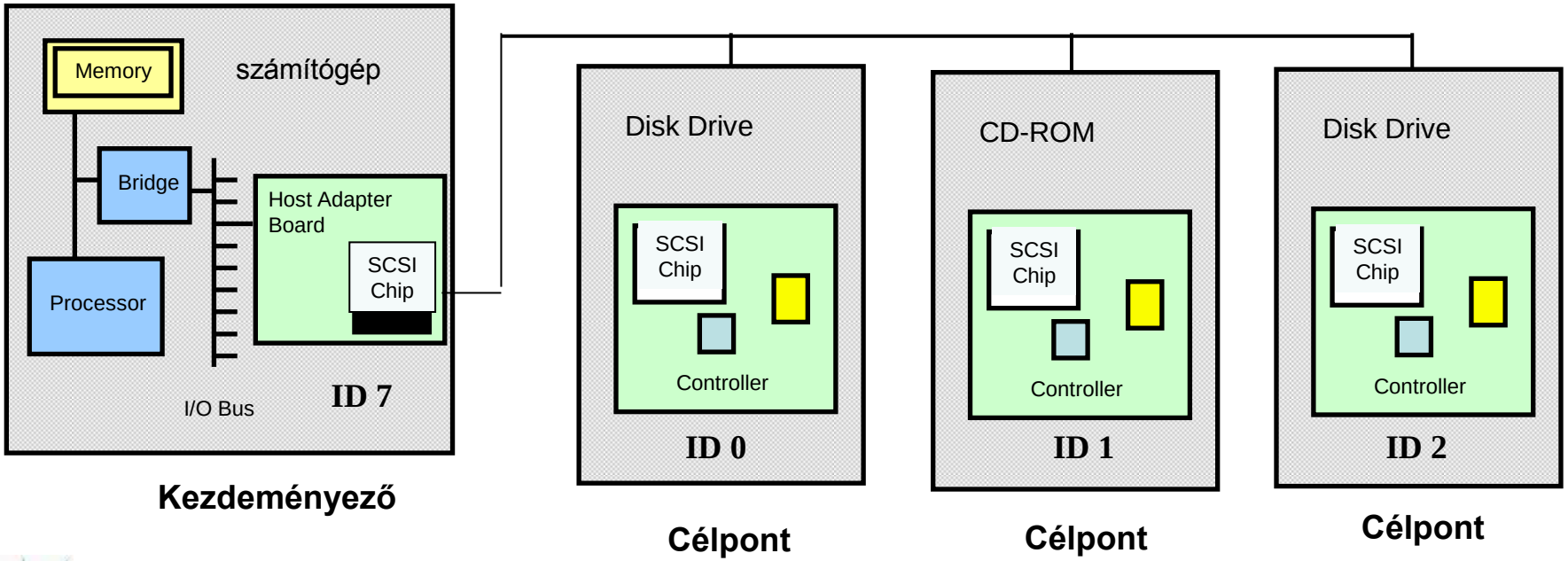


SCSI interfész

- SCSI
  - Small Computer System Interface (SCSI)
  - Szabványos I/O busz
  - Nagy teljesítményű interfész
- Eszközök
  - Disk Drives
  - Tape Drives
  - Removable Media Drives
  - CD-ROM, CD-R/CD-RW Drives
  - Optical Memory Drives
  - Nyomtatók

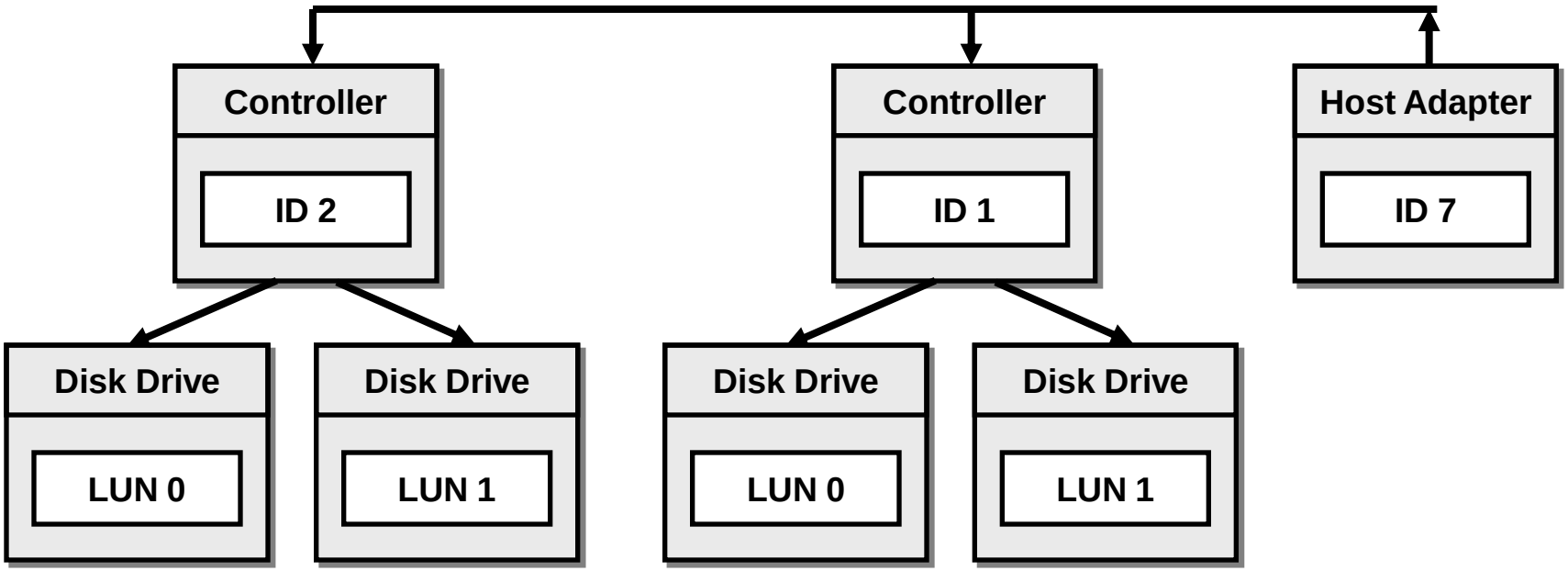
SCSI topológia

- Összes eszköz egy közös buszon osztozik
- Az eszközök egyedi azonosítóval rendelkeznek
- Csoportosításuk szerepük alapján történik
  - A kezdeményező általában számítógép
  - A célpont tipikusan merevlemez, CD-ROM

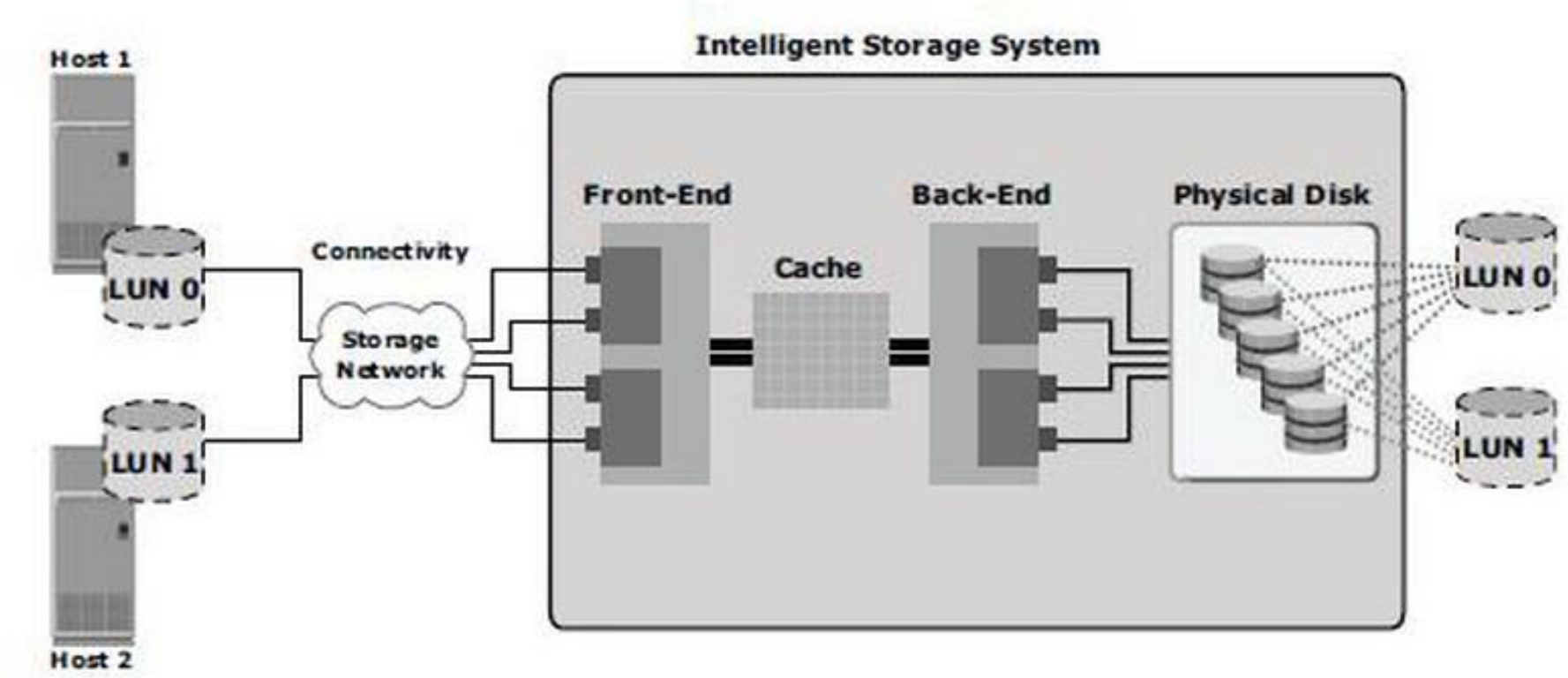


Logical Unit Number (LUN)

- NEM (!!!) szám – egy tárolócsoport
- LUN egy SCSI részcsoport címzési mód
  - Különböző fizikai eszközökön elhelyezett területek logikailag egy egységnek látszanak



LUN


Host 1
LUN 0
LUN 1
Host 2
Connectivity
Storage Network
Intelligent Storage System
Front-End
Cache
Back-End
Physical Disk
LUN 0
LUN 1

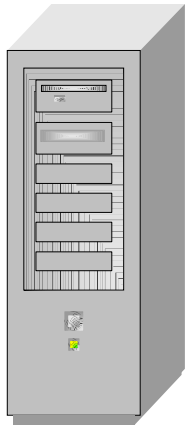
SAS - Serial Attached SCSI

- Serial Attached SCSI (SAS)
  - A párhuzamos (parallel) SCSI adapter továbbfejlesztése
  - Adatátviteli sebesség 320-1200 MB/sec
  - Full duplex, magasabb megbízhatóság
  - Több drive címezhető egyetlen kontroller portról

Direct-Attached Storage (DAS)

Előnyök
- Jobb, mint ha az adatokat a kliens tárolná
- Korlátozott redundanciát tud nyújtani
- Kis költség
- Egyszerű

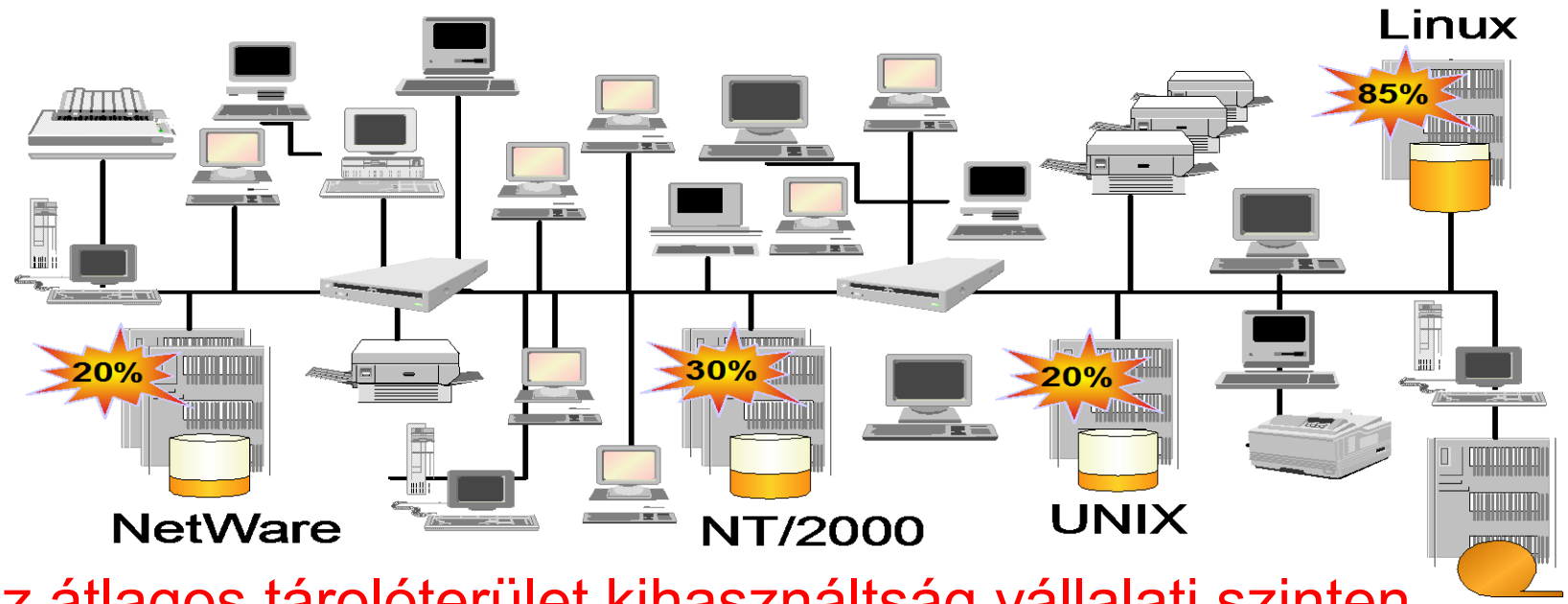
Hátrányok
- Nehézkes menedzsment
- Backup költséges
- Elpocsékolt tárolóterület
- Nehézkes az adatmegosztás
- Nem (jól) skálázható
- Korlátozott darabszámú eszköz csatlakoztatható
- Kis teljesítmény, korlátozott sávszélesség



DAS Device

Dedikált tároló eszközök

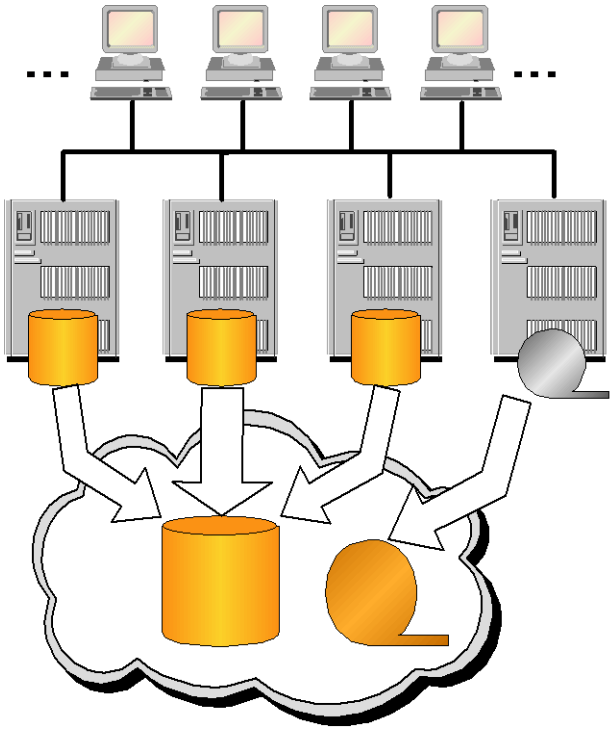
- Elosztott szerverek és tárolók – információ szigetek, különálló menedzsment alatt
- Nem hatékony az erőforrások (technikai és emberi) használata, magasak fajlagos költségek



Az átlagos tárolóterület kihasználtság vállalati szinten tipikusan 40-60%.

Konszolidált tároló eszközök

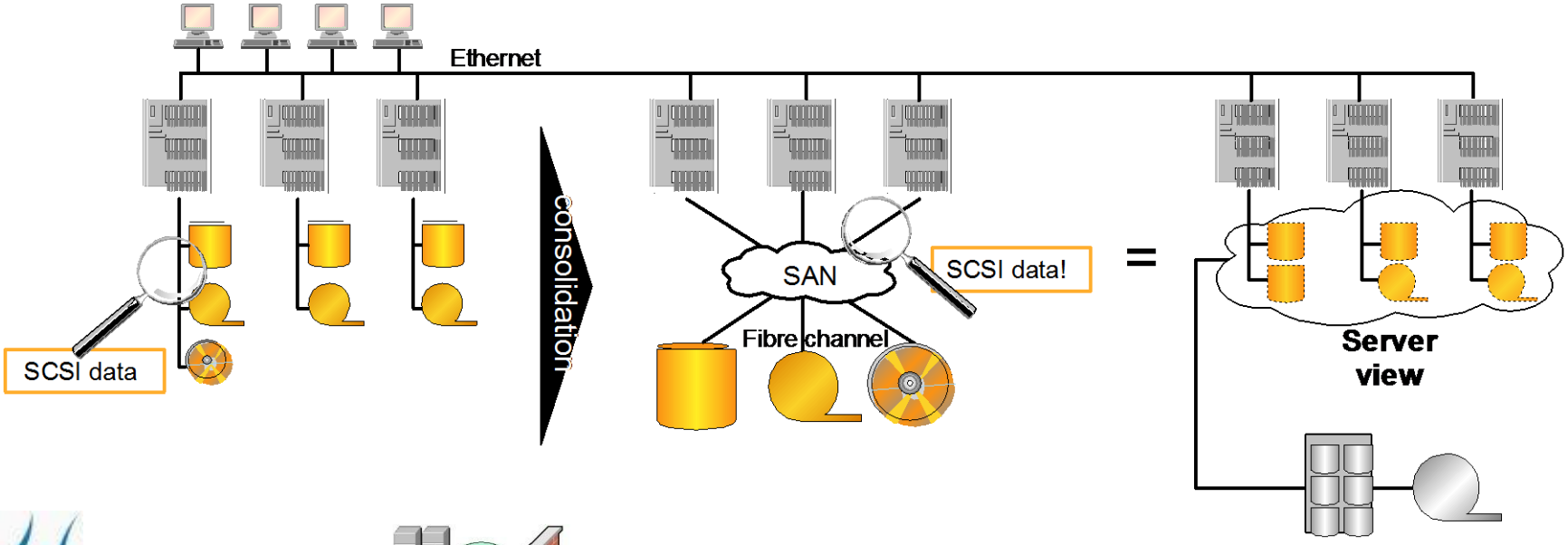
- Konszolidált eszközök, menedzsment, adat
- Kevésbé komplex, alacsonyabb fajlagos költségek
- Nagy rendelkezésre állású, skálázható, katasztrófa tűrő rendszerek alakíthatóak ki



A konszolidált (consolidated) tárhasználat hálózati architektúrában valósítható meg

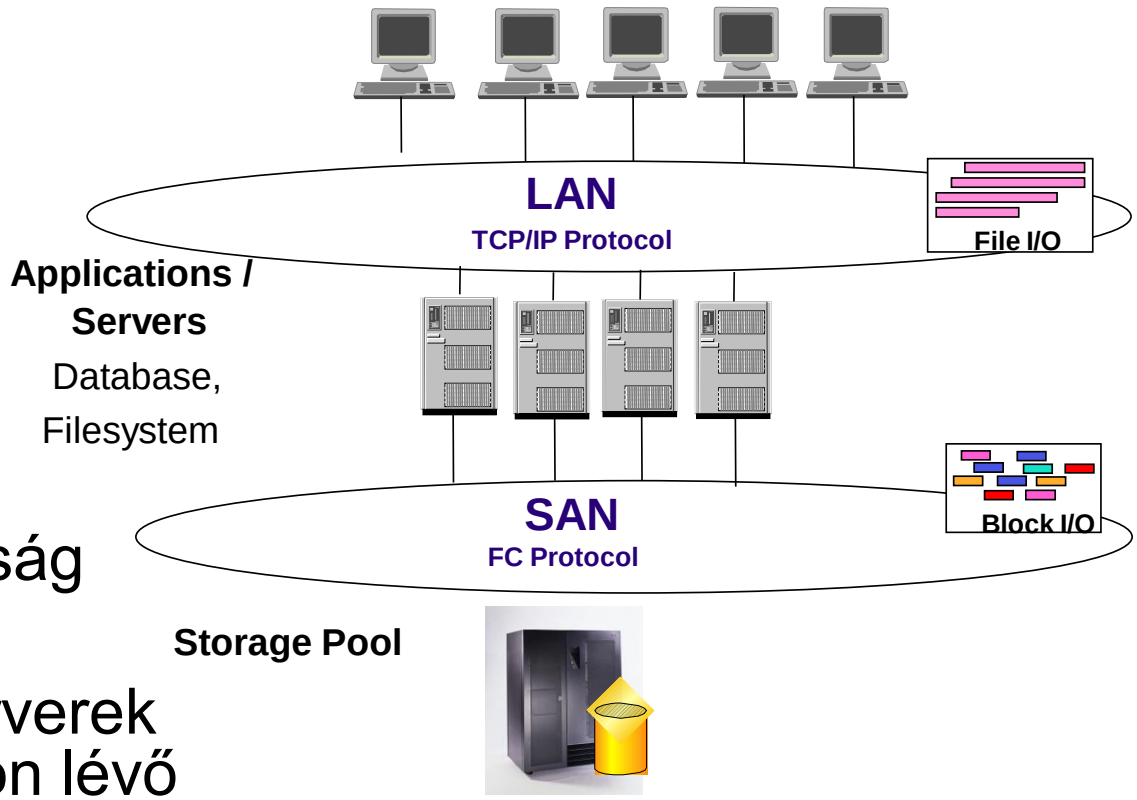
SAN - Storage Area Network

- Adattároló hálózat, adatforgalomra dedikált hálózat
- A tároló eszközök az egyes szerverektől fizikailag elválnak, több szerver képes ugyanazt az eszközt elérni
- Nem változik az adatkezelési protokoll, a szerverek dedikált, saját tárat látnak



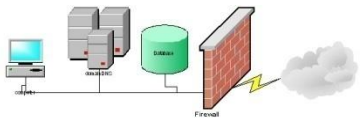
A SAN hálózatok előnyei

- **Erőforrások**
  - Az erőforrások kihasználtsága nő
  - Skálázhatóság
  - Magasabb szintű rendszerfunkciók valósíthatók meg (replikáció)
- **Menedzsment**
  - Nagyobb hatékonyság
- **Információ elérés**
  - Az alkalmazás szerverek bármely, a hálózaton lévő adatot bármikor elérhetnek



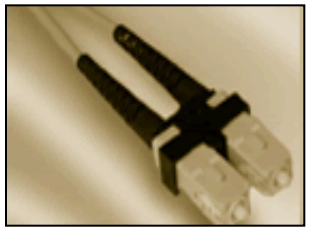
Átviteli technológia: Fibre Channel

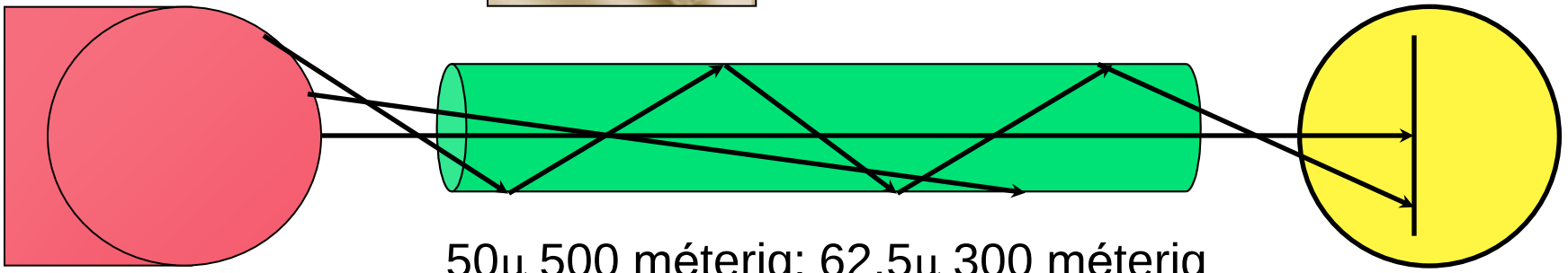
- Skálázható
  - Nagyszámú eszköz
  - Nagy távolság
  - Átviteli megoldás számos protokollhoz
    - SCSI-3 (=> diszkek ugyanúgy érhetők el, mint ha helyiek lennének !!)
    - IP, ATM, …
- Kapcsolt hálózati topológia
  - Megosztott eszközökkel, sávszélességgel kapcsolatos problémák elkerülése
- Sokféle eszköz, sebesség
  - Különböző típusú rézdrót, üvegszál
  - 2, 4, 8, 16 Gb/s sebesség



Üvegszál

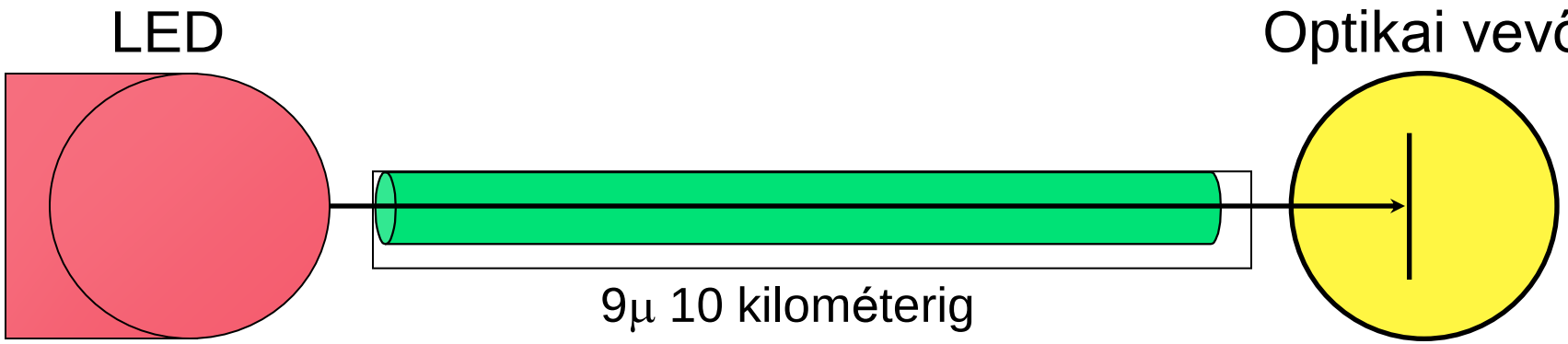
- Multimode
  LED





50μ 500 méterig; 62,5μ 300 méterig

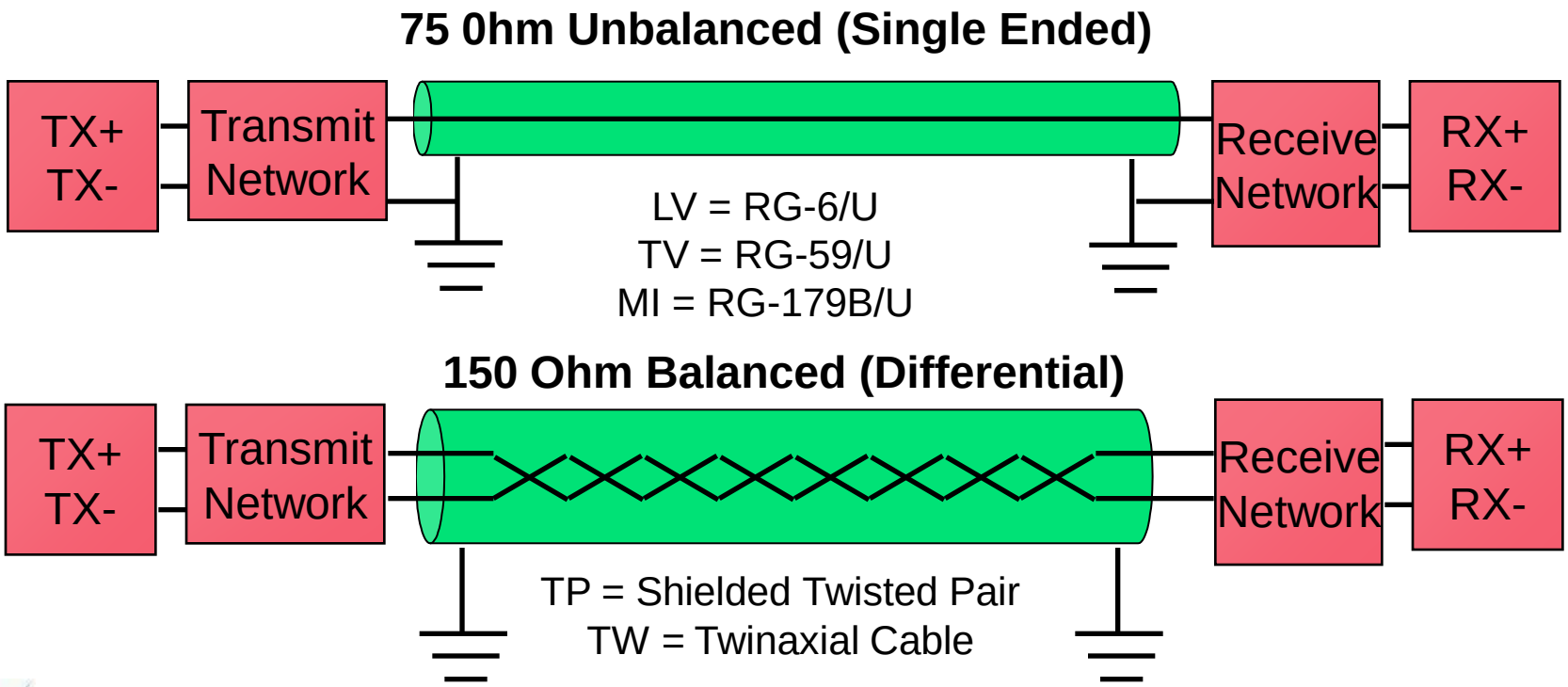
- Single mode
  LED



9μ 10 kilométerig

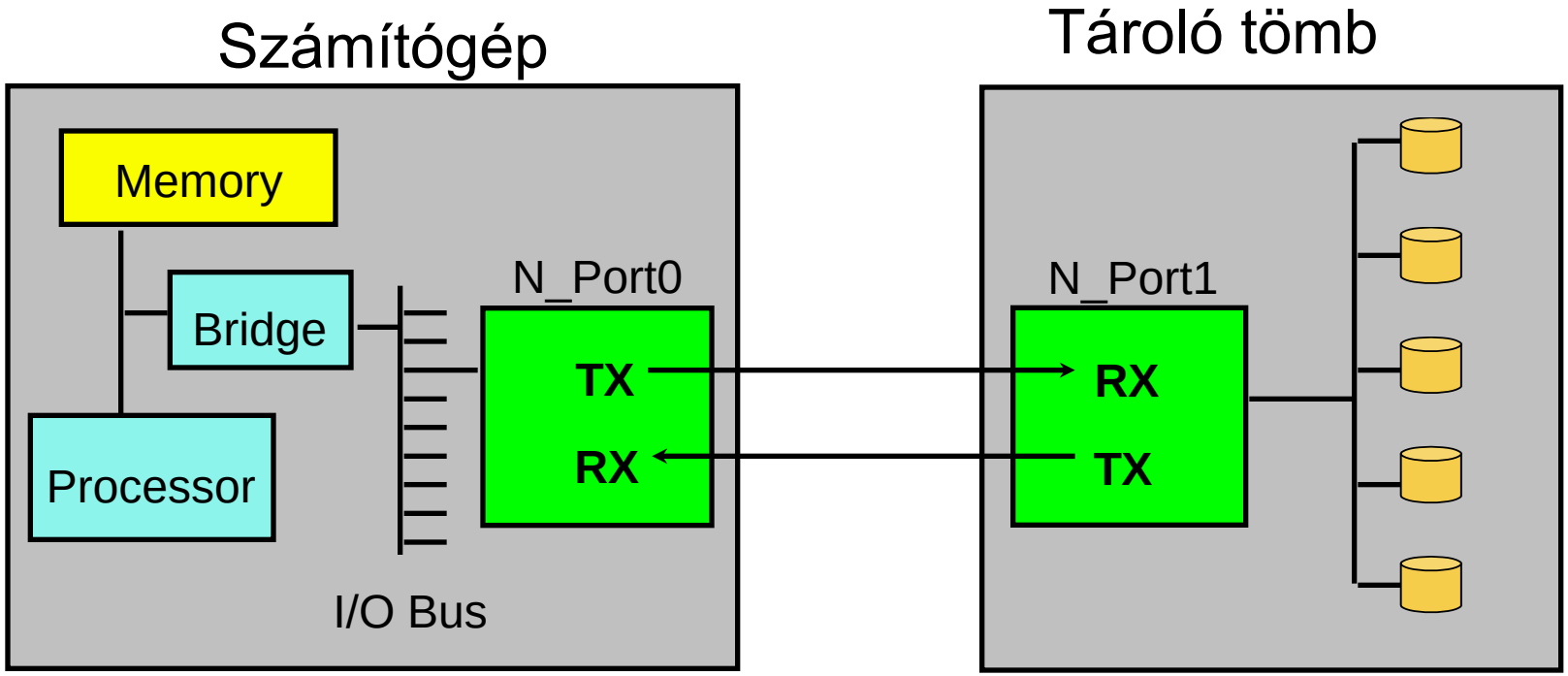
Rézvezeték

- Főleg Back-end
- Max. 30 méter
  - Jobb jel-zaj viszony, mint az üvegszálon



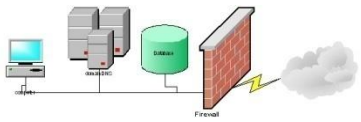
Pont-pont

- DAS
  - SCSI: max. 320 MB/s
  - FC: max. 1600 MB/s

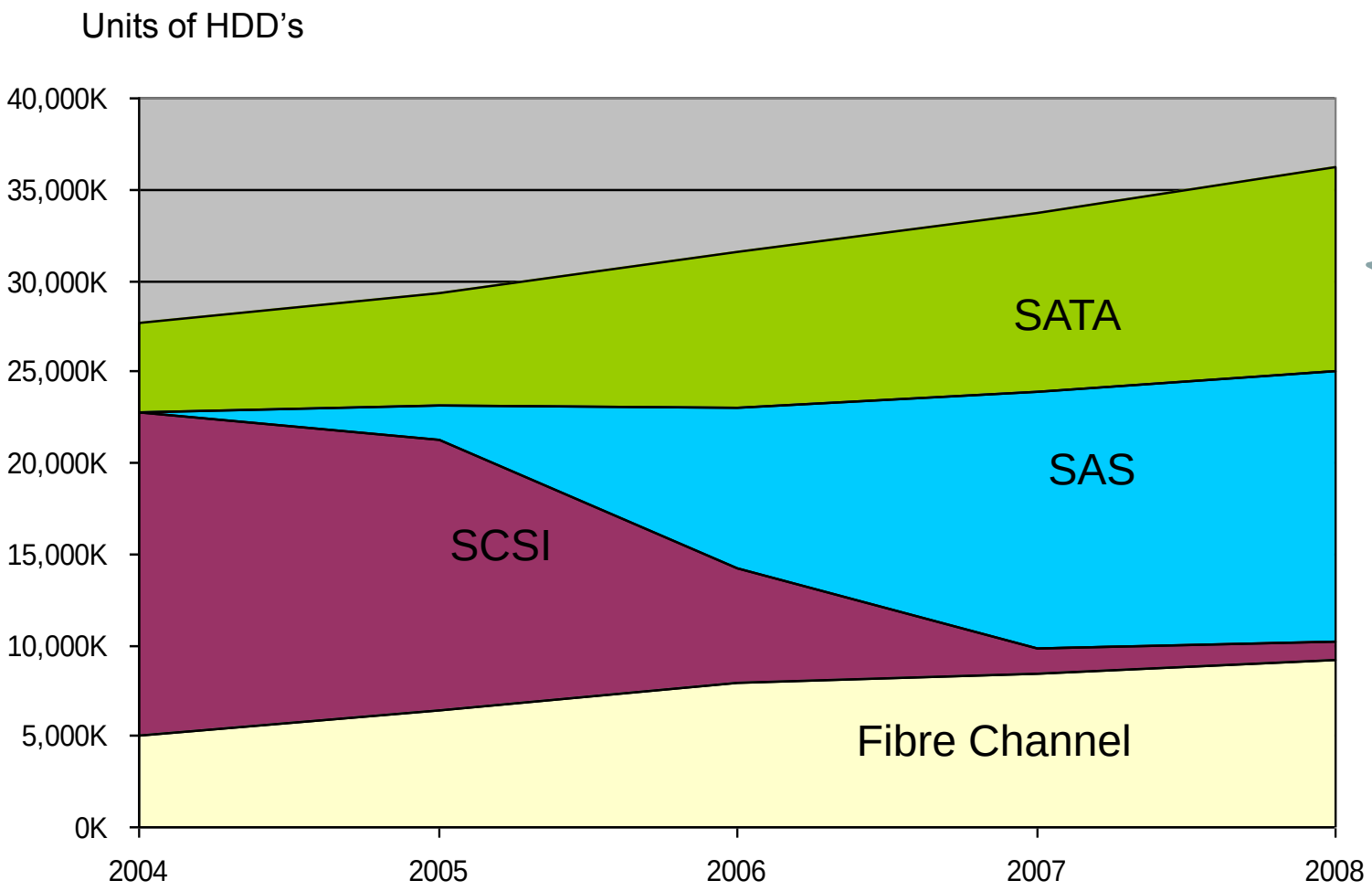


HDD Technológiák összehasonlítása

	SATA 2.0		SAS		Fibre Channel
Teljesítmény	Half-duplex	≠	Full-duplex with Link Aggregation	=	Full Duplex
	3 Gb/s		6 Gb/s	=	16 Gb/s
Interfész	1 m internal cable	≠	> 6 m internal and external cables		15 m external cable (Copper)
	Multipliers 15 HDD max	≠	Expanders >128 devices	=	127 devices (FC-AL) 16 Million (Fabric)
Kialakítás	Single-port HDDs	≠	Dual-port HDDs	=	Dual-port HDDs
	Single-host	≠	Multi-initiator	=	Multi-initiator
Driver sw.	Software transparent with Parallel ATA	≠	Software transparent with Parallel SCSI	=	Software transparent with Parallel SCSI

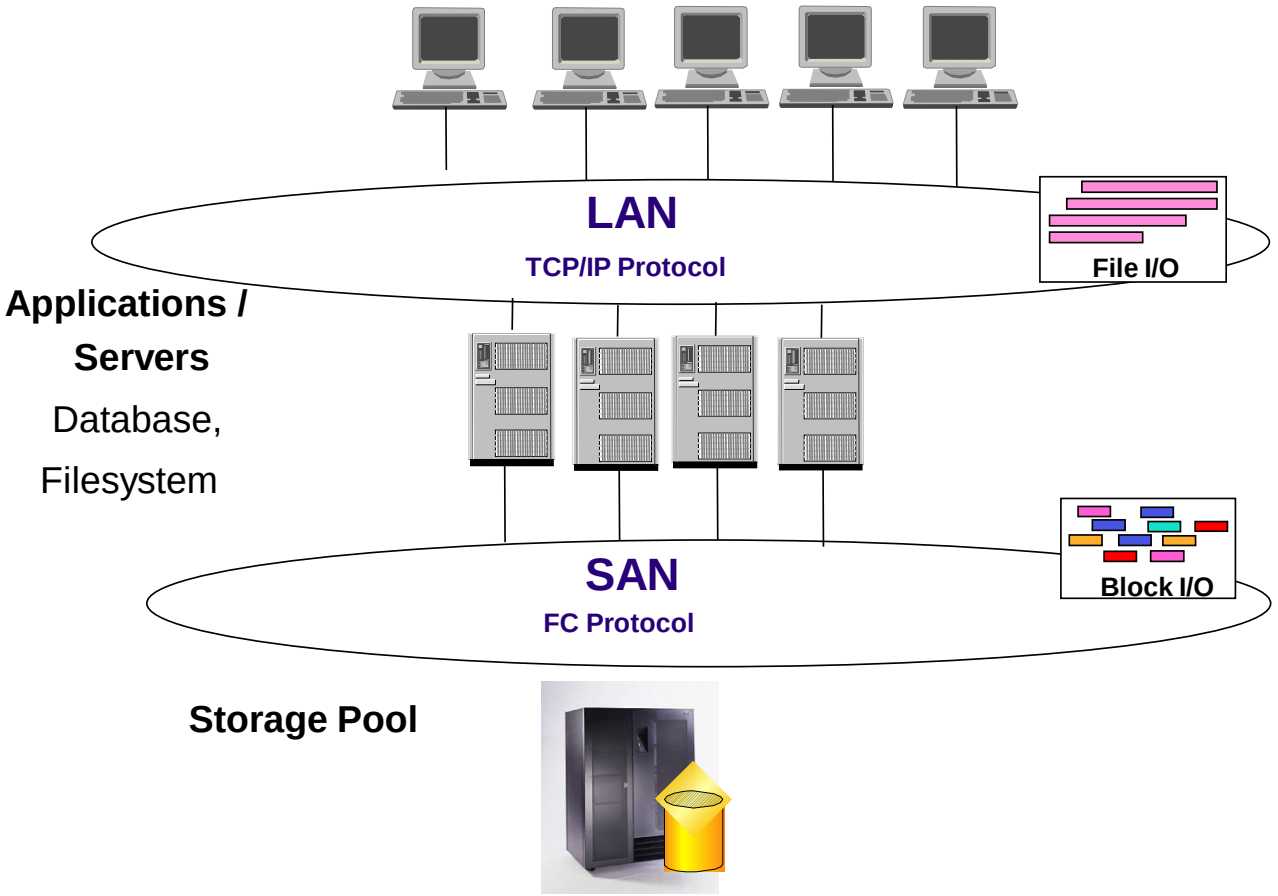


A nagyvállalati diszk tárolási technológiák



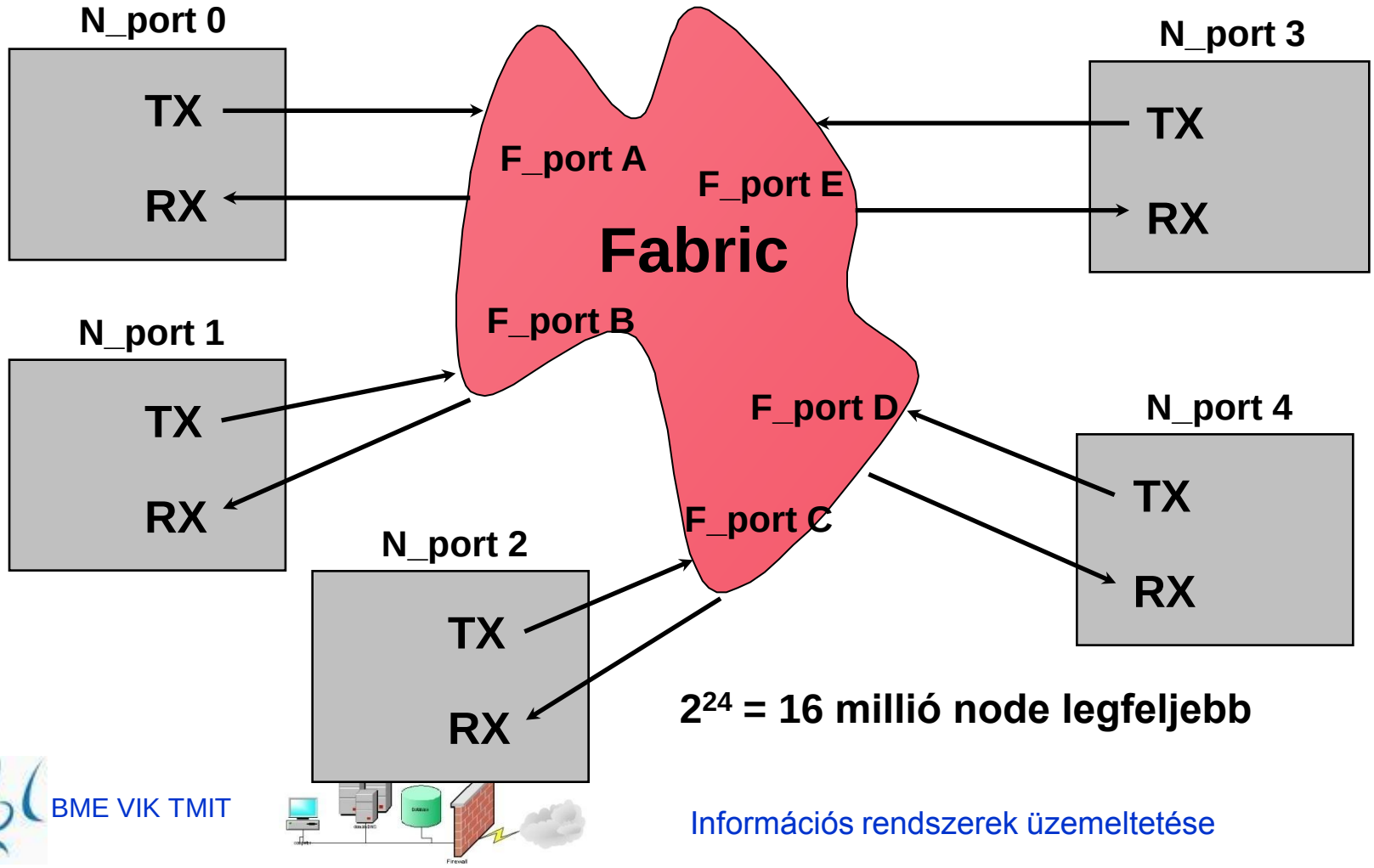
Flash

Vissza: SAN hálózatok

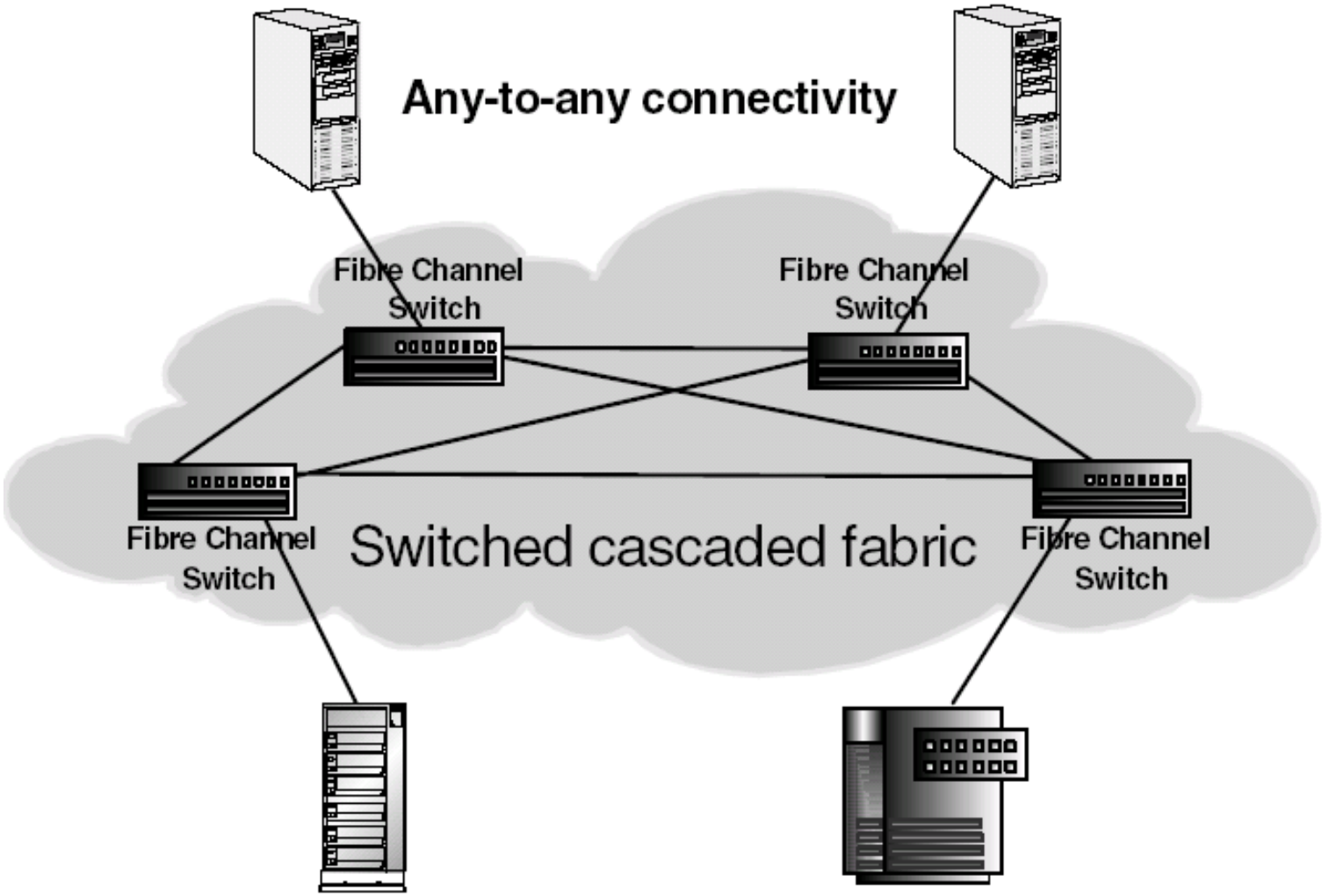


Kapcsolt hálózat

- Vannak más elrendezések is, de ma ált. ezt használják

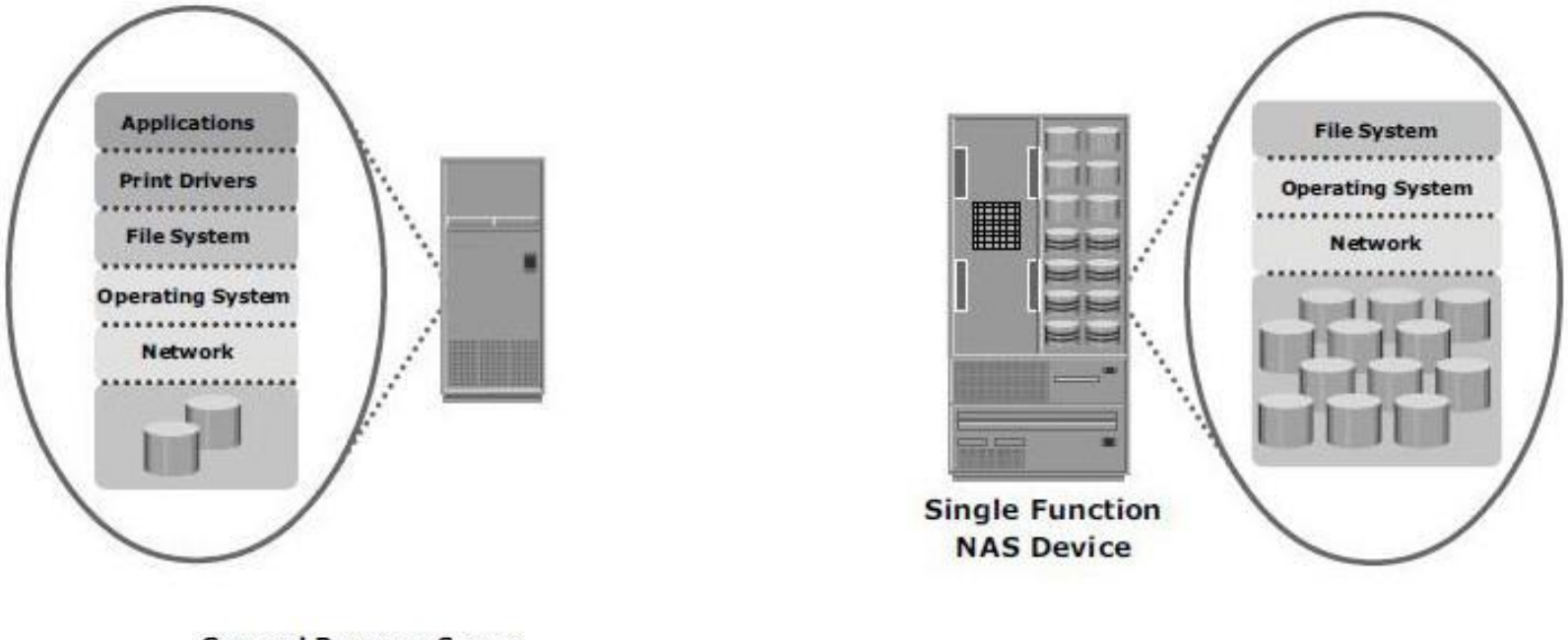


Kapcsolt hálózat



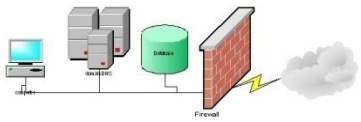
NAS – Network-Attached Storage

- Olyan tároló, amely IP hálózathoz csatlakozik
  - Dedikált célú fájlszerver
    - I/O műveletekre optimalizált op. rendszerrel



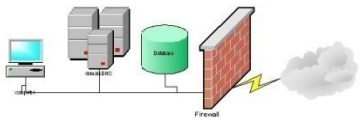
NAS

- IP (LAN, WAN) kapcsolat, belső SCSI struktúra
- Belső RAID - hibatűrés
- Fájlszintű elérés (Blokk elérés nem támogatott)
- Könnyen telepíthető
- Skálázás eszközön belül
- Performancia korlátok (LAN sávszélesség, protokoll overhead)



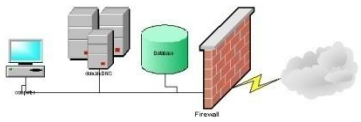
NAS protokollok

- NFS (Network File System) – UNIX
  - UDP feletti, fájlműveletekre specializált protokoll
- CIFS (Common Internet File System)
  - Operációsrendszer-független
    - Szerver
    - Kliens
  - TCP/IP feletti
- FTP (File Transfer Protocol)



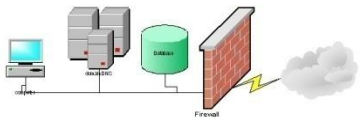
IP SAN (iSCSI)

- SAN: blokkszintű hozzáférés, FC hálózat
- NAS: fájlszintű hozzáférés, IP hálózat
- IP SAN: blokkszintű hozzáférés, IP hálózat
  - iSCSI (Internet Small Computer System Interface)
  - FCIP (Fibre Channel over IP)



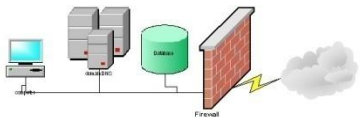
Diszkrendszeren belüli adatmásolási eljárások

- Nagymennyiségű adat másolását kell elvégezni
- Blokkszintű másolati példányokat készítünk
- Diszkrendszeren belüli nagysebességű, firmware támogatott másolási eljárások
- A felhasználó szempontjából teljes másolati kötegek – *volume copies* – jönnek létre



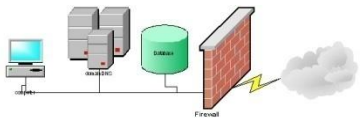
Volume Copy - Clone

- Egy adott tároló eszközön belül firmware eszközökkel megvalósított másolati technológia
- Valódi duplikátum kötet jön létre
- Teljes másolat: back-up, analitika, adatbányászat, stb. célra is alkalmazható
- Alkalmas alkalmazások más karakterisztikájú diszkekre történő migrálásához



Volume Copy - Clone

- Az adat-konzisztenciát biztosítani kell, az alkalmazások állapotának figyelembe vétele, I/O műveletek leállítása szükséges a másolat készítésekor
- A másolás a terjedelemtől függően időigényes, az alkalmazások addig állnak
- Alternatíva: Split mirror, tükrözött állományok közötti kapcsolat felbontása után az állományok külön kezelése. Az alkalmazások futása folyamatos, de külön idő, amíg az újabb szinkronizáció létrehozható

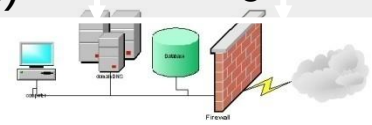


FlashCopy (Snapshot)

- Ha egy blokkot módosítunk, nem írjuk felül az eredetit, hanem máshová tesszük
- FlashCopy tábla, mely nyilvántartja az egyes fájlok blokkjait
  - „Pillanatfelvétel”
  - Tetszőleges időpontbeli állapot helyreállítható
- COW: Copy On Write
- A futó alkalmazást csak egy pillanatra kell leállítani, hogy koherens legyen
- Nem alkalmas back-up célra, mivel nem keletkezik valódi másolt állomány!

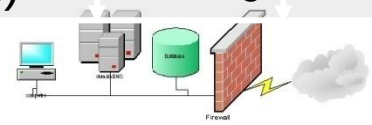
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
	B0		B8	B0		B8
	B1	B1		B1	B1	
	B2		B9	B2		B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8			8	8	8
Delta (flashcopy inkrementum)	0			Látszólagos Volume A		



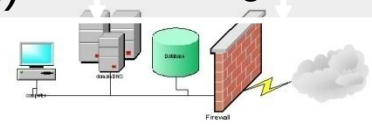
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0		B8
	B1	B1		B1	B1	
	B2		B9	B2		B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8			8	8	8
Delta (flashcopy inkrementum)	0			Látszólagos Volume A		



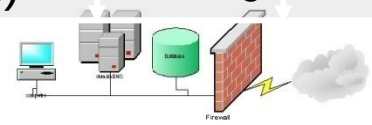
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
	B1	B1		B1	B1	
	B2		B9	B2		B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8			8	8	8
Delta (flashcopy inkrementum)	0			Látszólagos Volume A		



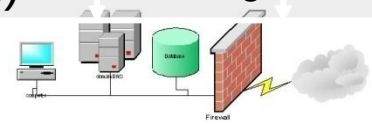
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
	B1	B1		B1	B1	
Írás t2	B2	**B2>B9**	B9	B2		B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8			8	8	8
Delta (flashcopy inkrementum)	0			Látszólagos Volume A		



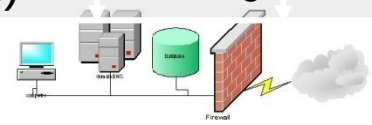
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
	B1	B1		B1	B1	
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8			8	8	8
Delta (flashcopy inkrementum)	0			Látszólagos Volume A		



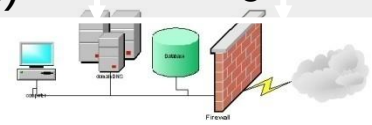
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
	B1	B1		B1	B1	
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10		8	8	8
Delta (flashcopy inkrementum)	0			Látszólagos Volume A		



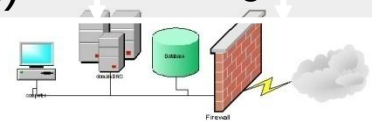
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
	B1	B1		B1	B1	
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10		8	8	8
Delta (flashcopy inkrementum)	0	2		Látszólagos Volume A		



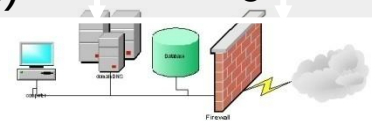
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
	B1	B1		B1	B1	
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10		8	8	8
Delta (flashcopy inkrementum)	0	2		Látszólagos Volume A	B	



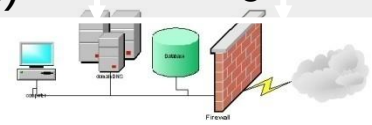
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
Írás t3	B1	B1	**B1>B10**	B1	B1	
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10		8	8	8
Delta (flashcopy inkrementum)	0	2		Látszólagos Volume A	B	



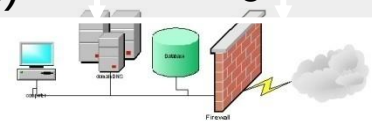
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
Írás t3	B1	B1	**B1>B10**	B1	B1	**B10**
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10		8	8	8
Delta (flashcopy inkrementum)	0	2		Látszólagos Volume A	B	



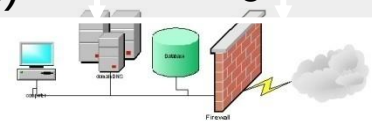
FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
Írás t3	B1	B1	**B1>B10**	B1	B1	**B10**
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10	11	8	8	8
Delta (flashcopy inkrementum)	0	2	3	Látszólagos Volume A	B	



FlashCopy - blokkok

Blokktábla				Flashcopy tábla		
Időpontok	**T1**	**T2**	**T3**	**F1**	**F2**	**F3**
Írás t2	B0	**B0>B8**	B8	B0	**B8**	B8
Írás t3	B1	B1	**B1>B10**	B1	B1	**B10**
Írás t2	B2	**B2>B9**	B9	B2	**B9**	B9
	B3	B3	B3	B3	B3	B3
	B4	B4	B4	B4	B4	B4
	B5	B5	B5	B5	B5	B5
	B6	B6	B6	B6	B6	B6
	B7	B7	B7	B7	B7	B7
Összes blokkszám	8	10	11	8	8	8
Delta (flashcopy inkrementum)	0	2	3	Látszólagos Volume A	B	C



SAN vagy NAS összefoglalás 1.

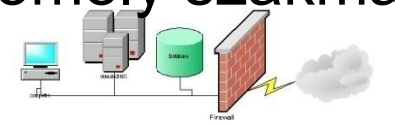
SAN (Storage Area Network)

Központosított, nagy teljesítményű, adattárolásra dedikált hálózat, amely

- Összeköti a szervereket, tároló eszközöket,
- Hálózati elemeket és kapcsoló eszközöket, valamint támogató szoftver megoldásokat tartalmaz

Előnyei:

- Skálázható, bővíthető
- Nagy adatátviteli sebesség (4 -10 Gb/s)
- Központilag felügyelhető, támogatja a hierarchikus tároló technológia kialakítását, de komplex, heterogén hálózat esetén komoly szakmai feladat a megfelelő üzemeltetés



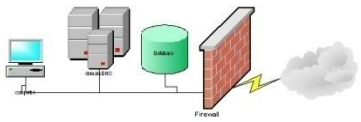
SAN vagy NAS összefoglalás 2.

NAS (Network Attached Storage)

A hálózatra csatlakoztatott adattároló eszköz, amely támogatja a adatmegosztást kliensek és szerverek között.

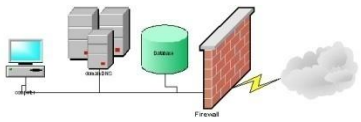
Előnyei:

- Skálázható, bővíthető, de az adatátviteli sebesség korlátozott (LAN)
- Könnyen telepíthető, üzemeltethető eszköz
- Főleg kisebb környezetek esetén alkalmazható



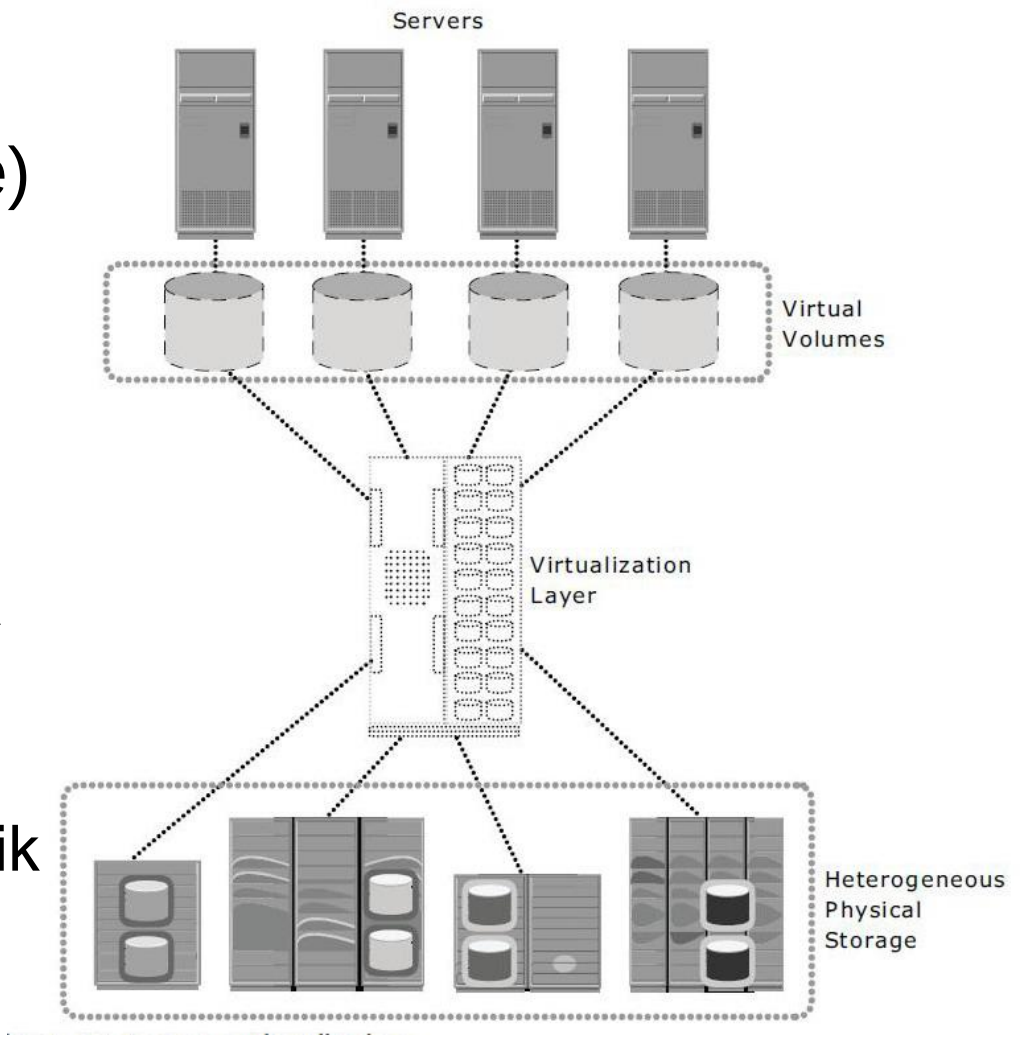
Tárterület virtualizáció

- A virtualizáció olyan technológia, amely lehetővé teszi, hogy bizonyos erőforrások más erőforrásoknak tűnjenek, lehetőleg kedvezőbb tulajdonságokkal
- A virtualizáció jellemzően elfedi a háttér-rendszer komplexitását, és új, hatékonyabb funkciókat biztosít a háttér-rendszer szolgáltatására építve
- A virtualizáció a rendszer különböző rétegeiben valósítható meg



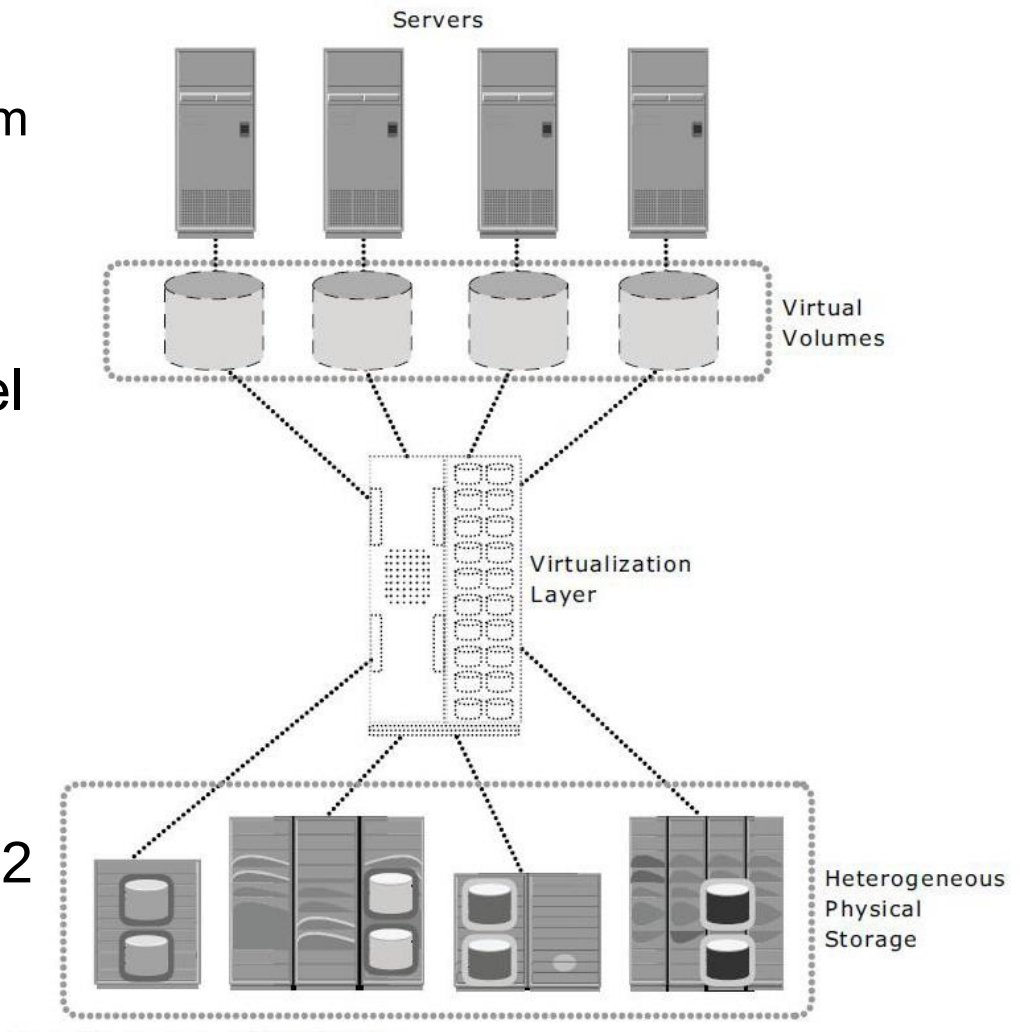
Tároló virtualizáció

- A virtualizáló motor (Virtual Engine or Virtualization Appliance) elfedi a diszkek különbözőségét
  - „fordít” a két formátum között
  - diszkek megoszthatók
    - nő a kihasználás
  - diszkek cseréje, módosítása nem látszik a szerver számára



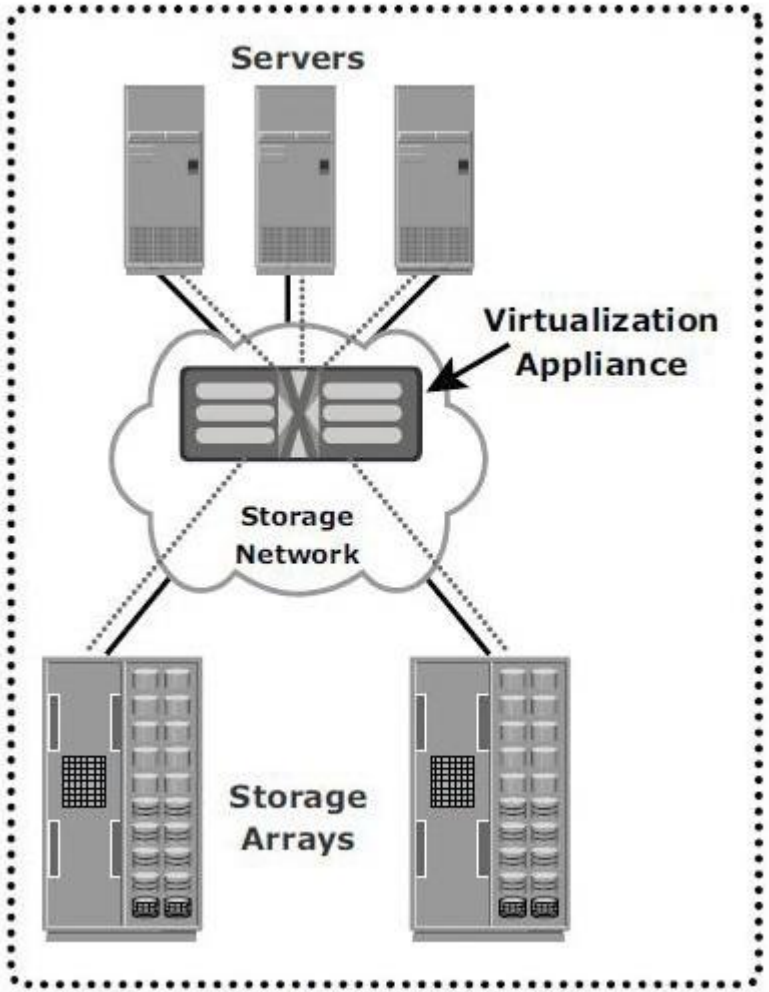
Virtualizáló motor működése

- Meta-data
  - tkp. egy összerendelési táblázat a logikai – fizikai cím között
- Szerver: LUN=1, LBA=32
  - LBA Logical Block Address
- VM: táblázatból, ez megfelel a fizikai LUN=4, LBA=0 címnek
- Elkéri az adatot a fizikai diszktől
- A megkapott adatot úgy továbbítja a szervernek, mintha az a LUN=1, LBA=32 címről érkezett volna



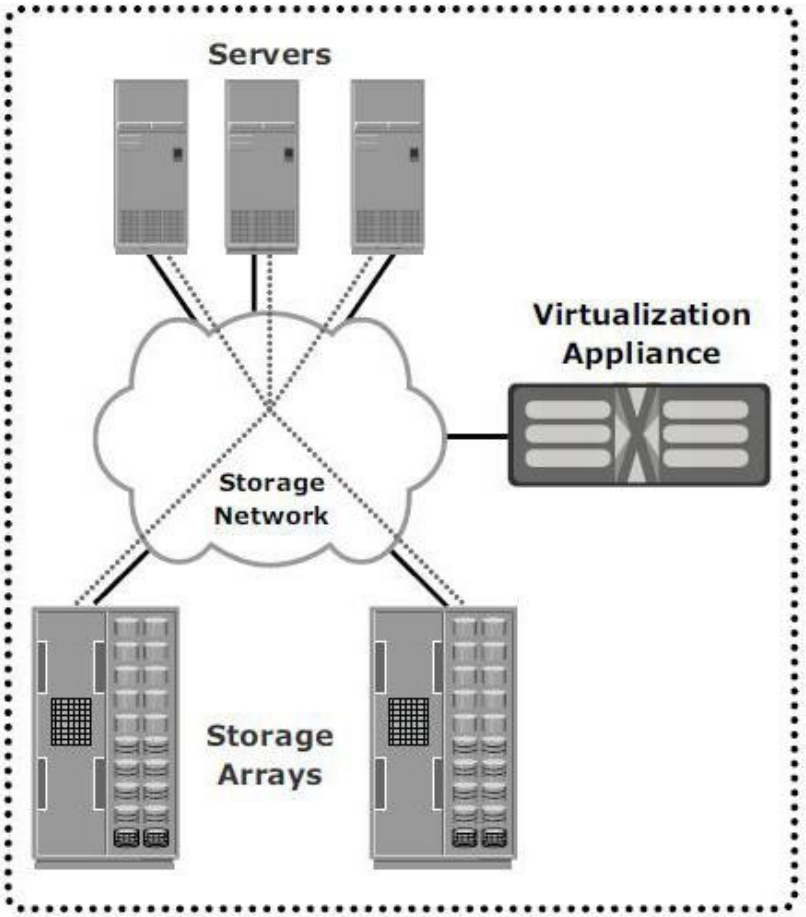
Virtualizáció konfiguráció – in-band

- Virtualizáló motor az adatútban
  - nincs szükség külön szoftverre a szerveren
  - de lassabb, mert az adat átmegy a VM-en



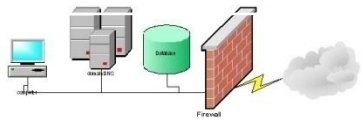
Virtualizáció konfiguráció – out-of-band

- A vezérlés és az adatút elválik
  - a szerveren külön szoftver kell:
    - először lekérdezi az adat fizikai helyét a VM-től
    - majd közvetlenül eléri az adatot
  - gyorsabb az adatátvitel, mert nincs az adatútban semmi



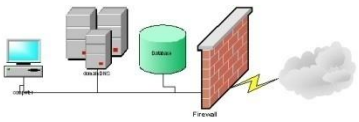
Blokkszintű virtualizáció

Ezek az erőforrások …	ilyennek tűnnek …
• LUN (különböző gyártók, különböző típusai)	• Virtuális LUN-ok, amelyek úgy tűnnek, mintha egy gyártó egy típusa lennének
• Tipikusan fix méretű	• A mérete dinamikusan csökkenthető és növelhető
• Különböző szállítói felületek konfiguráció, és copy szolgáltatások	• Központi menedzsment, egységes felületek és szolgáltatások
• Nehéz a migráció az új technológiákra	• Migráció az alkalmazások zavarása nélkül



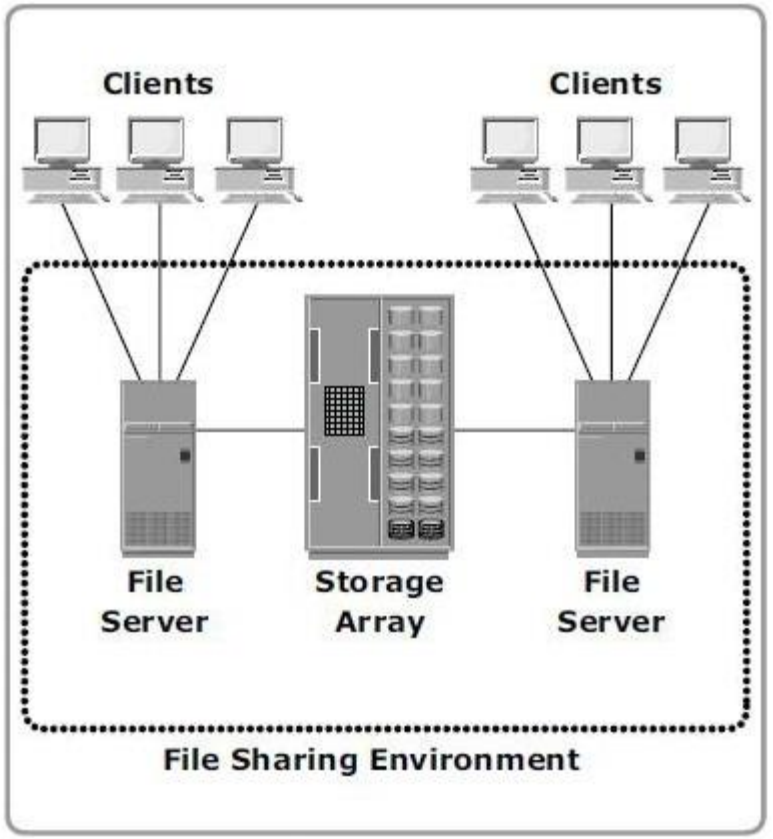
Virtualizáció szintjei

- Blokkszintű virtualizáció
  - eddig erről volt szó
  - a *szerver* egy adott *adatblokk*hoz akar hozzáférni
  - aminek ismeri a (logikai) címét
- Fájlszintű virtualizáció
  - egy *kliens*/host egy *fájlt* szeretne elérni egy adott fájlszerveren
  - tudnia kell, hogy melyiken



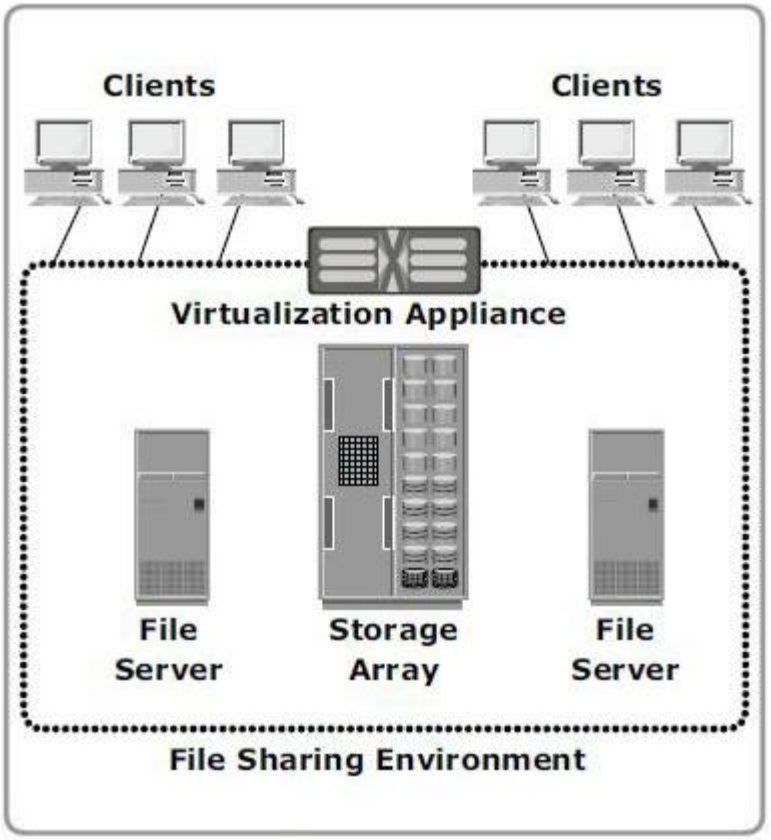
Fájlszintű virtualizáció

- Fájlszintű virtualizáció nélkül
  - egy kliens/host egy fájlt szeretne elérni egy adott fájlszerveren
  - tudnia kell, hogy melyiken
  - lehet, hogy az egyik szerver tele, a másik üres
  - fájl mozgatás érinti a klienst is

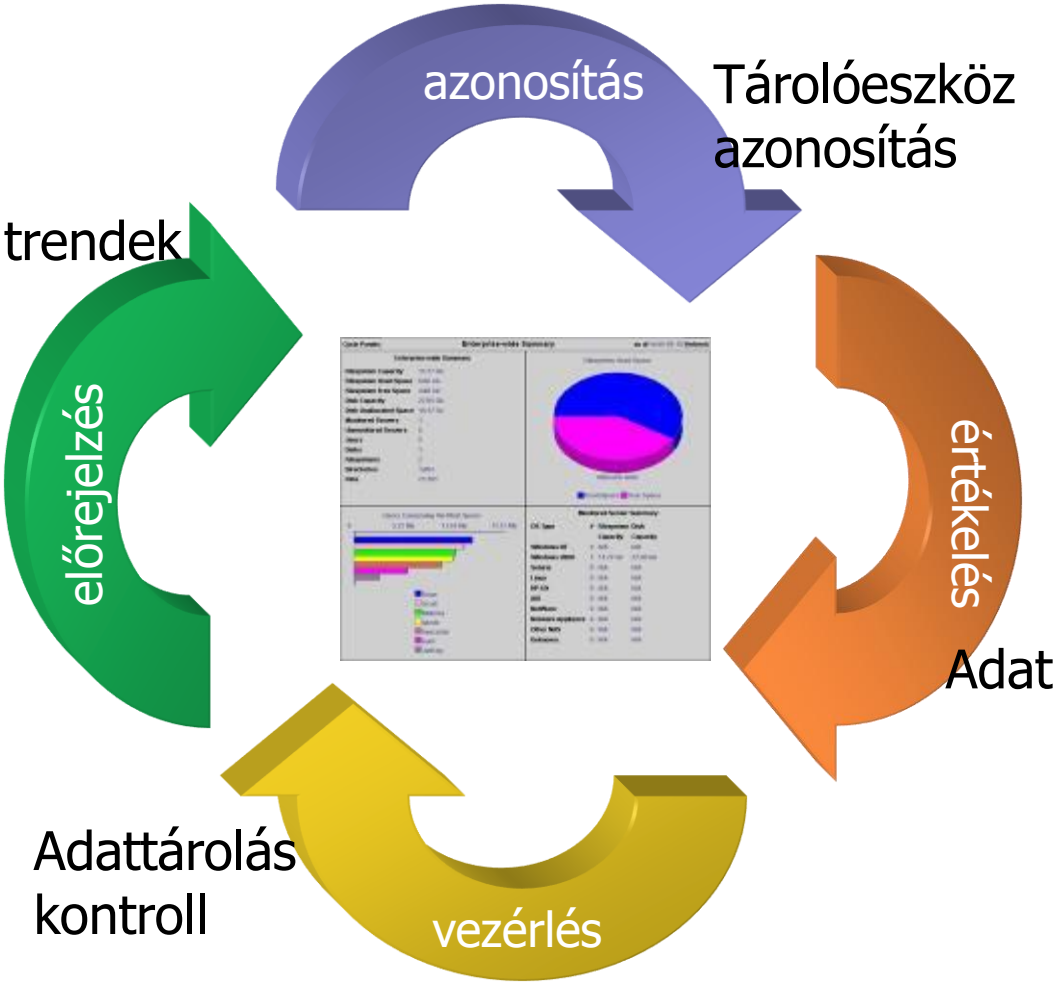


Fájlszintű virtualizáció

- Virtualizált fájlszerver
  - a kliensnek nem kell tudni, melyik fizikai szerveren van a fájl
  - egyszerűbb
    - terhelésmegosztás
    - fájlmozgatás
    - bővítés
- Cloud computing

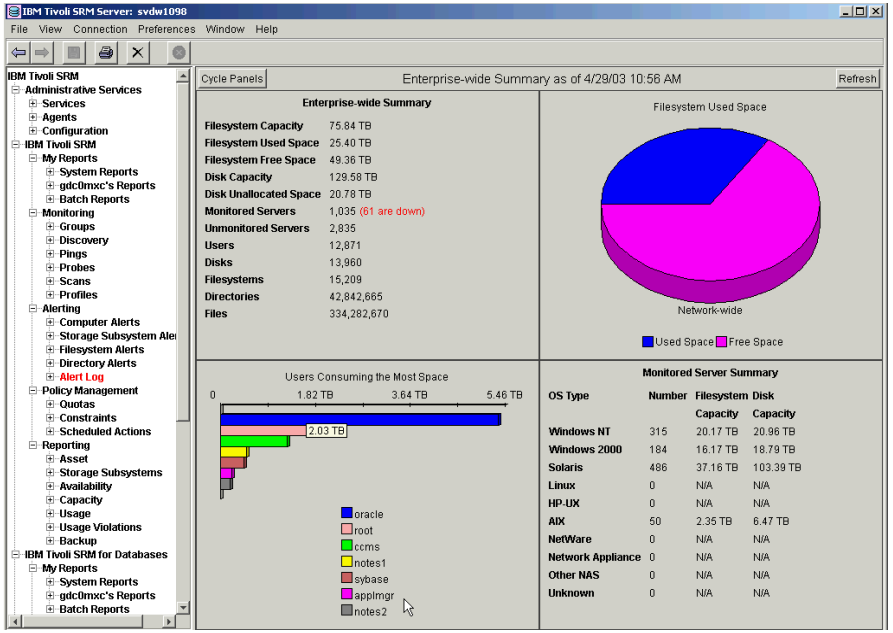


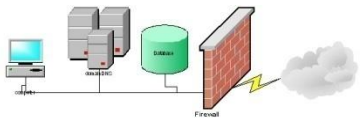
A tároló erőforrás menedzsment főbb lépései (Storage Resource Management)



SRM megoldás (1)

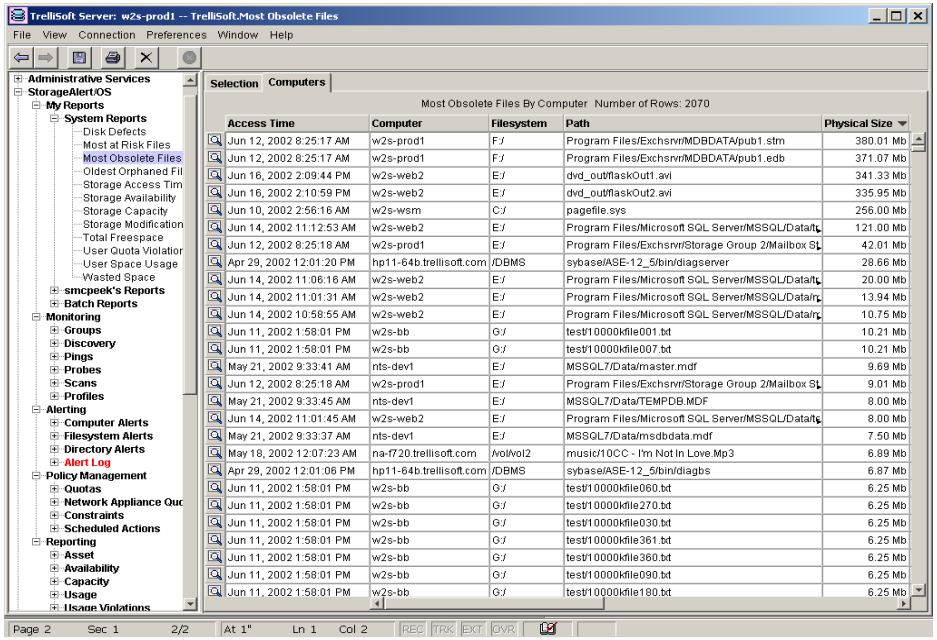
- Azonosítás
  - Eszközleltár
  - Lefoglalt területek
  - Mi az aktuális kapacitás kihasználás
  - Van-e kritikus fájlrendszer?
  - Allokált, de nem használt területek

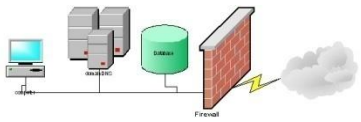




SRM megoldás (2)

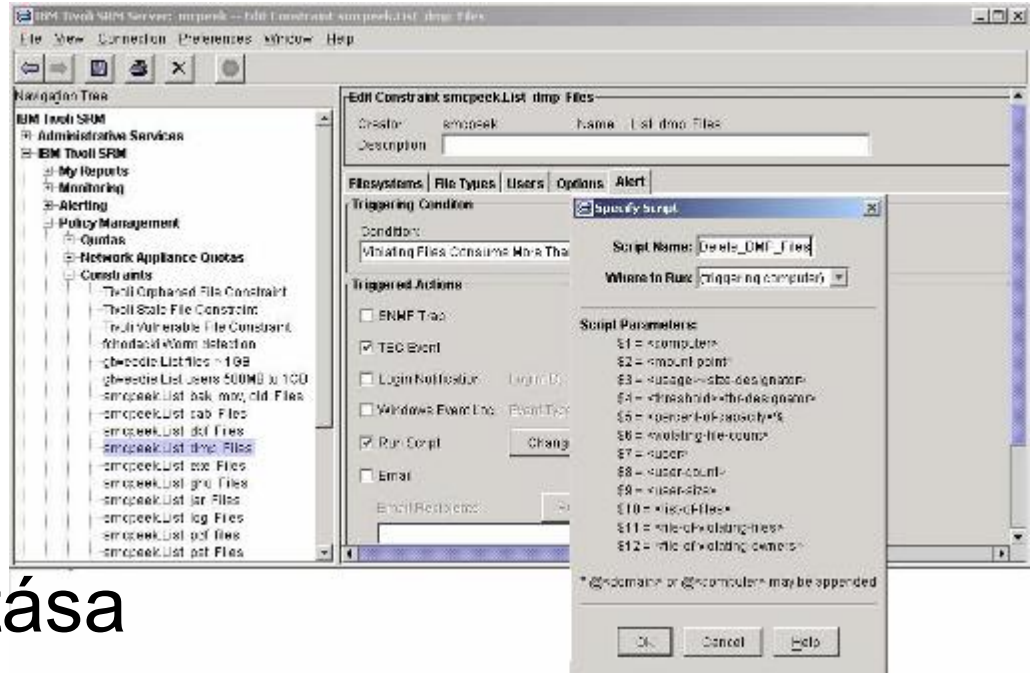
- Értékelés (adat osztályozás)
  - Fájl és könyvtár szintű analízis
  - Feleslegesen foglalt tárterületek azonosítása
  - Árva, régi, nem használt, duplikált állományok azonosítása





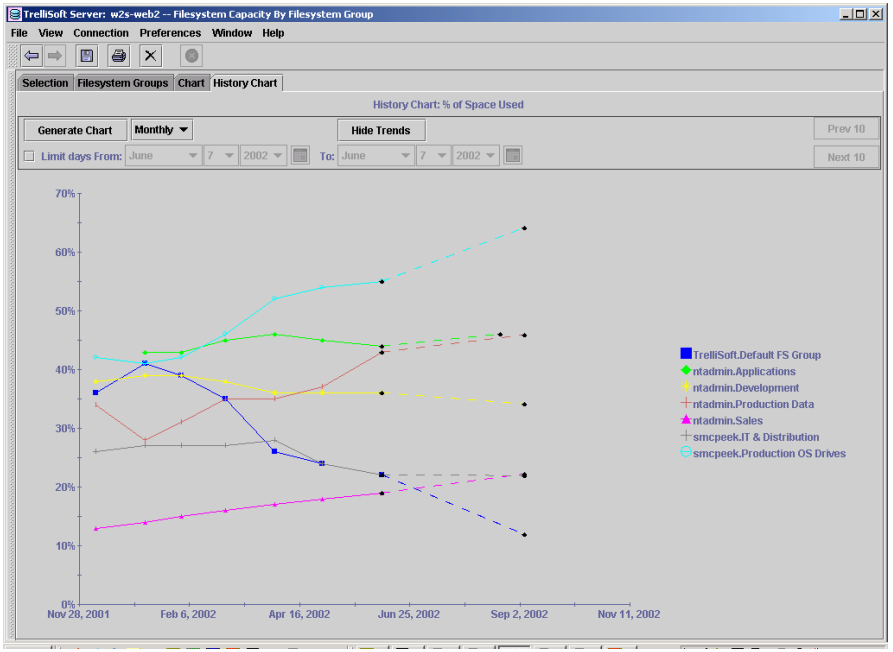
SRM megoldás (3)

- Vezérlés
  - Központi riasztási rendszer
  - Kvótakezelés
  - Automatikus válaszakciók indítása
  - A menedzsment funkciók automatizálhatóak



SRM megoldás (4)

- Előrejelzés
  - Leggyorsabban növekvő felhasználók, fájlrendszerek, adatbázis táblák.
  - Trendek azonosítása, és előrejelzés

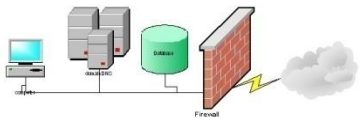


Információs rendszerek üzemeltetése

VI. fejezet
Mentés és helyreállítás (Backup and Restore)

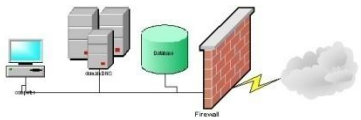
BME VIK TMIT

Mérnök-informatikus alapképzés



Mentés és helyreállítás

- Mentés / archiválás definíció
- Mentés
  - Szalagos eszközök
  - Mentőrendszerek
  - Mentési módszerek
    - Teljes, inkrementális, differenciális, progresszív
- Archiválás
  - Archiválási követelmények
- Mentés megtervezése vállalati szinten
  - Példa
- Helyreállítással kapcsolatos kérdések



Mentés és archiválás

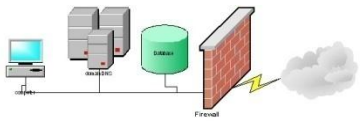
"You caught a virus from your computer and we had to erase your brain. I hope you kept a back-up copy."

Mentés és archiválás

A mentés / archiválás célja: a helyreállíthatóság biztosítása, adatvesztések elkerülése (minimalizálása) **másolati** adatpéldányok készítésével

Mentés célja: üzletfolytonosság biztosítása

- Törlés: a felhasználó véletlenül / szándékosan! törölt
- Meghibásodás: egy tároló eszköz / rendszer elromlott

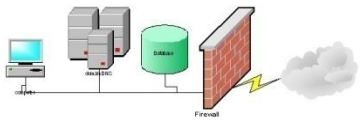


Mentés és archiválás

Archiválás célja: referencia időpontnak megfelelő adattartalom megőrzése

- Üzleti, jogi, törvényi okok miatt az adatokról meghatározott időnként archiválást kell végezni, adat visszakeresési, bizonyítási, referencia stb. célból
- Nem használt adatokat a produktív rendszerekből el kell távoltani: üzemeltetési igény
- Szintje: fizikai (file, image) vagy logikai (alkalmazás)

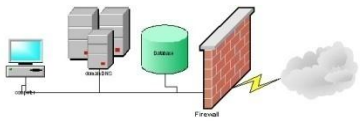
Jellemzően közös alaptechnológia végzi a mentési / archiválási feladatokat – ezért össze is keverik a kifejezéseket, hibásan!



A helyreállíthatóság szükségességének 3 fő oka

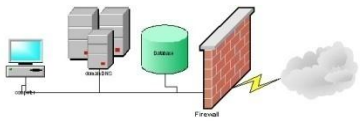
- Véletlen fájl törlés
- Diszk meghibásodás

- Archiválás



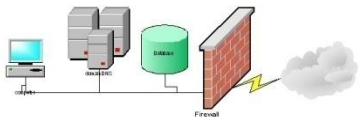
Véletlen fájl törlés

- Felhasználói igény: gyors visszaállítás
- Tipikus irodai környezet:
  - Max. 1 nappal előző állapot állítható helyre
  - Max. 1 napig tart a helyreállítás
  - Új SW-k: felhasználók maguk képesek a visszaállításra
    - DE: csak ha a szalag még a mentőegységben van!
    - Ha nem: várni a rendszergazdára, míg előkeresi…



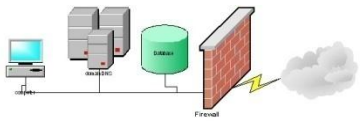
Automatikus mentőrendszerek előnyei

- Rendszergazda
  - Nem „zargatják” folyton helyreállítási kérelmekkel
- Használók
  - Gyorsabb helyreállítás
  - Munkastílus változik
  - Diszk kihasználtság nő
  - Automatikusan készül – „nem lesz elfelejtve”
  - Áttekinthetőbb könyvtárak
  - Nem csak törlésnél, fájl módosításkor is hasznosak



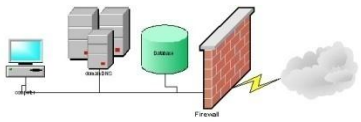
Diszk hiba

- Diszk hiba
  - Diszk hardver hiba
  - Egyéb hardver / szoftver hiba, amely a teljes diszktartalom elvesztését okozza
- Két fő következmény
  - adatvesztés
  - szolgáltatás kimaradás
- Lassú, tipikusan több gigabájtnyi adat helyreállítása
  - Többlépéses helyreállítás
    - Legutolsó teljes mentés
    - Azt követő inkrementális/differenciális mentések



Archiválás

- Célja
- Hasonló a teljes mentéshez, négy fő eltéréssel
  - MINDIG teljes mentés
  - Eltérően kezelendőek az archív szalagok a „normál” mentésekétől – duplikálás
  - Más („külső telephely”) helyszínen való tárolás
  - „Hosszú életű”, ezért nem csak a szalagokat, hanem
    - Azokat az eszközöket is tárolni kell, amivel a másolat készül
    - Azokat a tool-okat is tárolni kell, amivel az adat elérhető



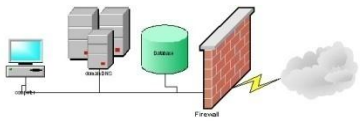
Miért kell még szalag?

Előnyök:

- Olcsó fajlagos tárolási kapacitás
- Az adathordozók kivehetőek, nincs állandó mechanikai igénybevétel
- Hosszú megőrzési idő – akár 30 év
- A tárolt adatok egyszerűen törölhetők

Hátrány:

- Az adatok sorosan érhetők el
- Hosszabb befűzési idő szalagok között
- A média sérülékenyebb

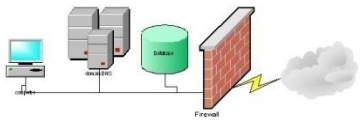


Linear Tape-Open (LTO) szabvány

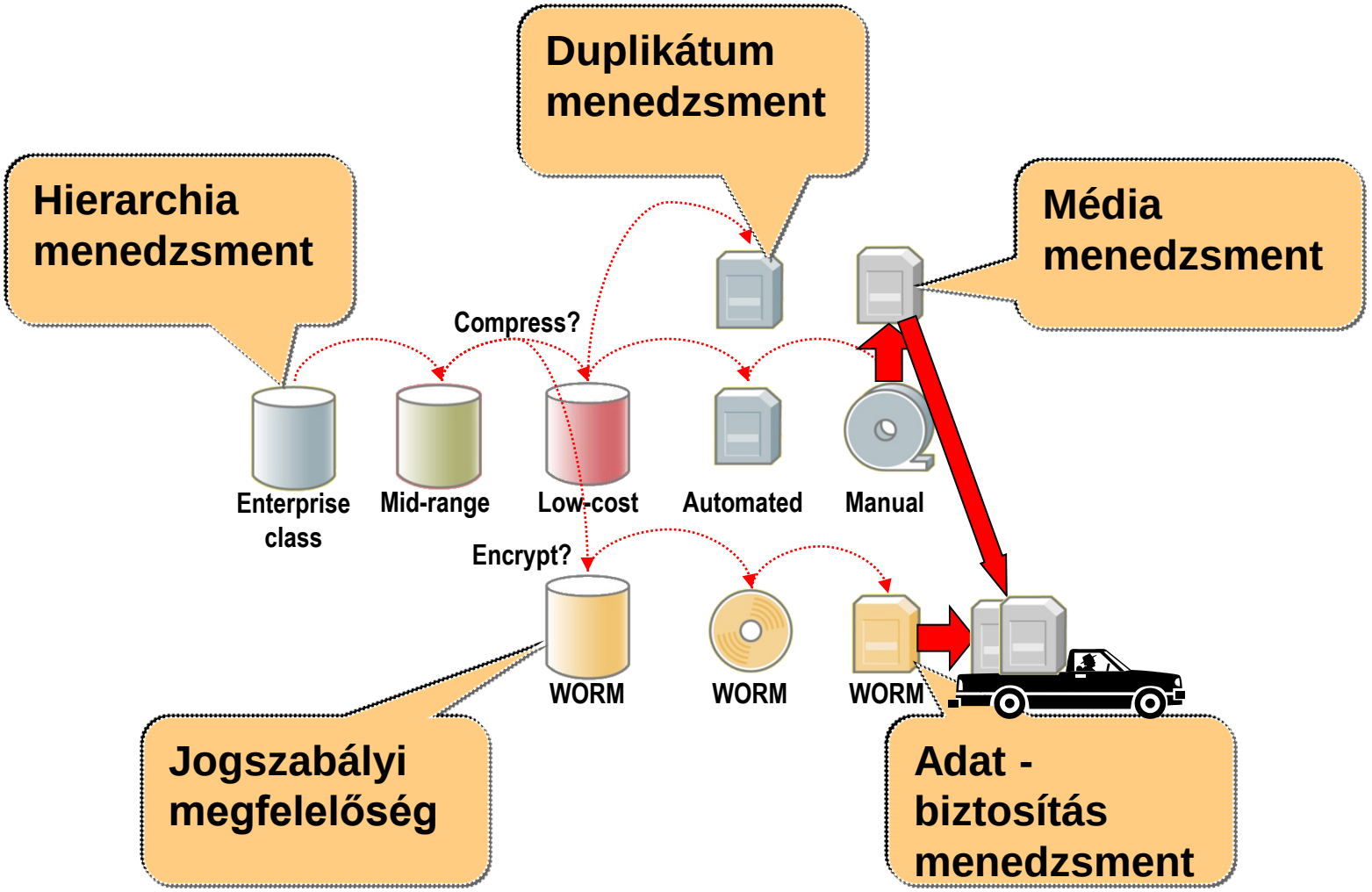
- Szalagformátum *(Tape Format Standard)*: IBM, HP és Certance (Seagate) konzorcium
  - Nyílt rendszerű szabvány technológia
  - 4. generációs termék
  - Lefelé kompatibilitás
- Megjelenése óta (2000) széles körű ipari elfogadottság, a vezető szalagtechnológia
  - 2000: 100 GB
  - 2012: 2,5 TB (v6)

LTO jellemzők

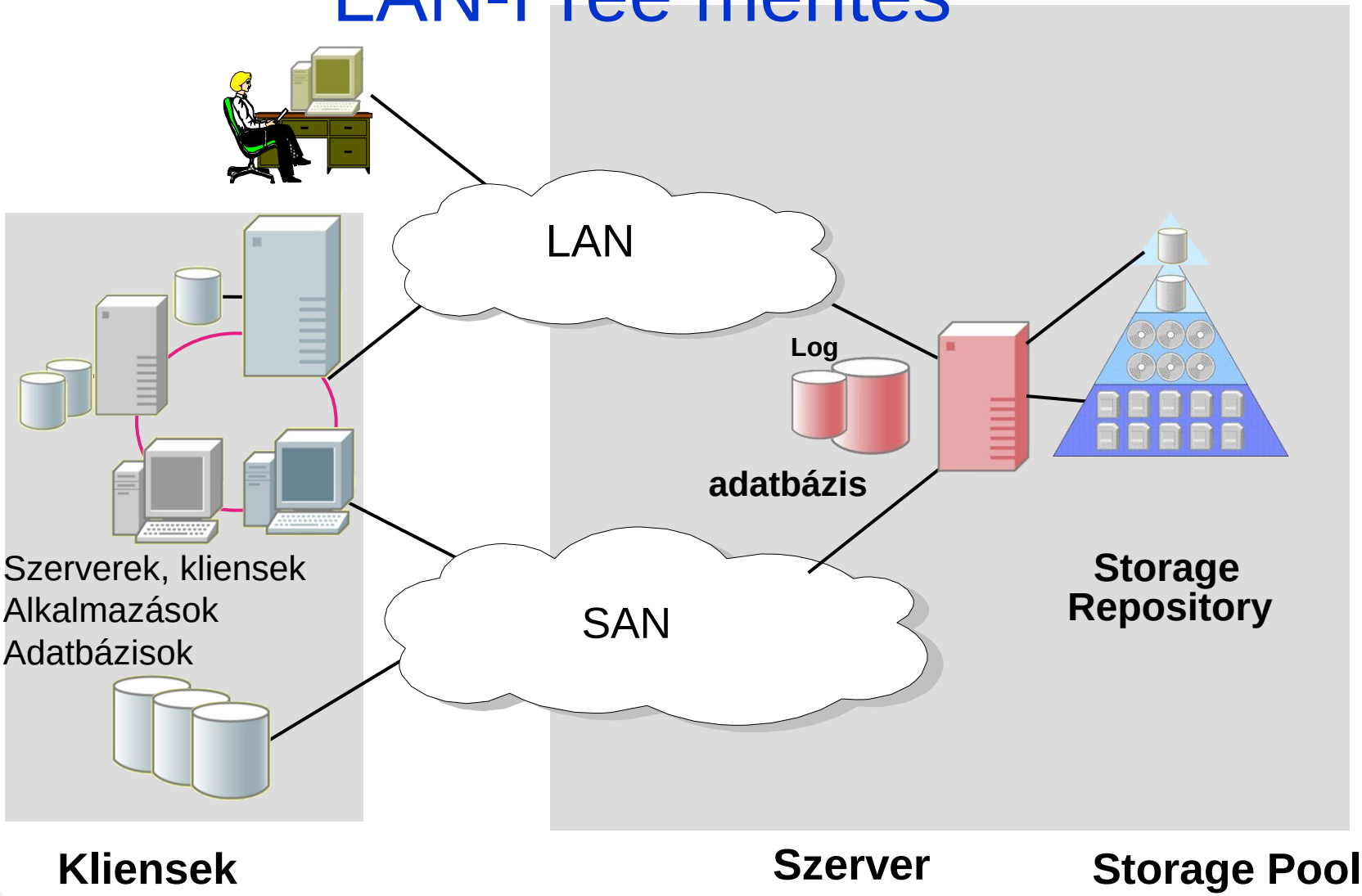
Type	Year	Capacity	Entire-tape reads/ writes	Approximate years of life assuming one tape filled...	
				per *month*	per *week*
LTO-1	2000	100 GB	200	17	4
LTO-2	2003	200 GB	250	21	5
LTO-3	2005	400 GB	364	30	7
LTO-4	2007	800 GB	200	17	4
LTO-5	2010	1500 GB	200	17	4
LTO-6	2012/13	2500 GB	—	—	—



Egy korszerű mentőrendszer követelményei



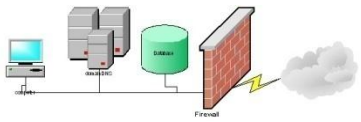
Mentőrendszer architektúra – LAN-Free mentés



LAN-Free mentés és visszaállítás

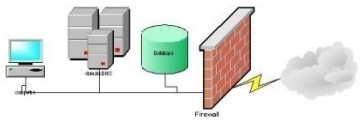
- LAN-Free kliens adatátvitel
  - A szerver menedzseli a belső tárterületet
  - A kliens mozgatja az adatokat diszkről szalagra vagy a SAN-on lévő diszkre
  - Meta-adatok LAN hálózaton mozognak.
  - A LAN-t nem terheli a mentési adatforgalom

- LAN-Free előnyök
  - Minimalizálja a LAN túlterhelés veszélyét
    - Csökkenti a LAN forgalmat
    - Rugalmasabb lesz a mentési ablak időzítése
  - Ütemezett és házirend alapú működés, a megosztott SAN erőforrások terhelésének optimalizálására



Mentési módszerek

- Teljes mentés (Full backup)
- Inkrementális mentés (Incremental backup)
- Differenciális mentés (Differential backup)
- Progresszív mentés (Progressive Backup Methodology)

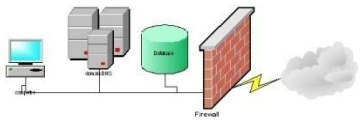


Teljes mentés

- Minden nap a teljes diszktartalmat mentjük
  - Nagy adatmennyiség
  - Lassú
  - Rossz szalagkihasználtság
    - Ugyanaz sokszor mentésre kerül, akkor is, ha nem változik

  DE:

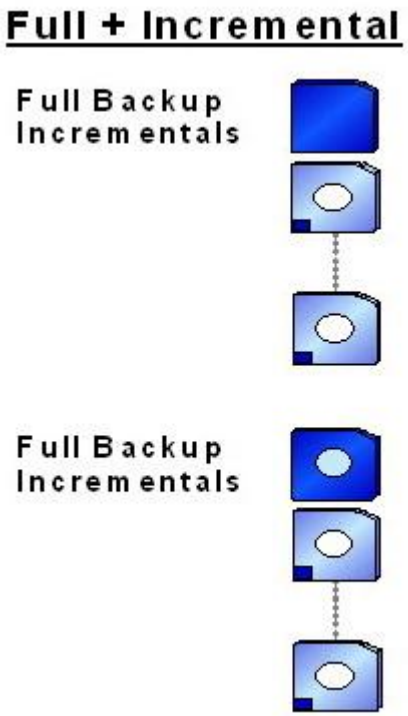
  - Egy szalagról helyreállítható



Inkrementális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző mentés óta történt változások
  - Kis adatmennyiség

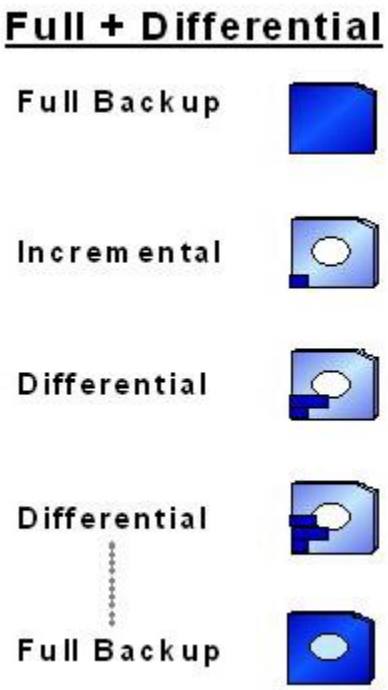
  DE:
  - Hosszú visszaállítási idő
  - Rossz szalagkihasználtság



Differenciális mentés

- Ciklus első napján teljes mentés
- Utána minden nap csak az előző teljes mentés óta történt változások
  - Nagyobb, egyre növekvő napi adatmennyiség

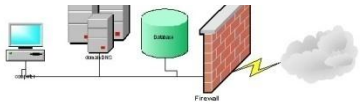
  DE:
  - Rövidebb visszaállítási idő (max. 2 szalag)
  - Több szalag



Inkrementális / Differenciális mentés problémája

Day 1	Day 2	Day 3	Day 4	Day 5
File A	File A renamed to File F	File F	File F	File F deleted
File B	File B deleted			
File C	File C renamed to File G	File G	File G	File G
File D	File D moved to new location	File D (new location)	File D deleted	
File E	File E	File E	File E	File E

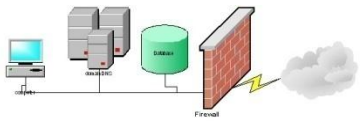
Files from Day 1 FULL backup		Files from Day 3 INCREMENTAL / DIFFERENTIAL backup		Hard Drive after a restore to Day 3
File A		File F		File A – **wrong** File F
File B	+		=	File B – **wrong**
File C		File G		File C – **wrong** File G
File D		File D (new location)		File D – **wrong** File D (new location)
File E				File E



Progresszív mentési stratégia

- Teljes mentés csak egyszer
- Utána csak inkrementális mentés
- De mellette az adott napi fájlstruktúrát is mentjük
  - Kicsivel(!) több mentés, mint az inkrementálisnál
- Így helyreállításkor visszakereshető, hogy egy fájlnak melyik az aktuális állapota
  - Jelentős időnyereség
    - Többször módosított
    - Törölt fájlok

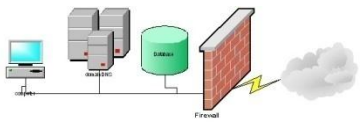
  helyreállításakor



Progresszív mentés előnye

Day 1	Day 2	Day 3	Day 4	Day 5
File A	File A renamed to File F	File F	File F	File F deleted
File B	File B deleted			
File C	File C renamed to File G	File G	File G	File G
File D	File D moved to new location	File D (new location)	File D deleted	
File E	File E	File E	File E	File E

Required files from Day 1 FULL backup		Required files from Day 2 & Day 3 INCREMENTAL backups		Hard Drive after a restore to Day 3
	+	File F	=	File F
		File G		File G
		File D (new location)		File D (new location)
File E				File E

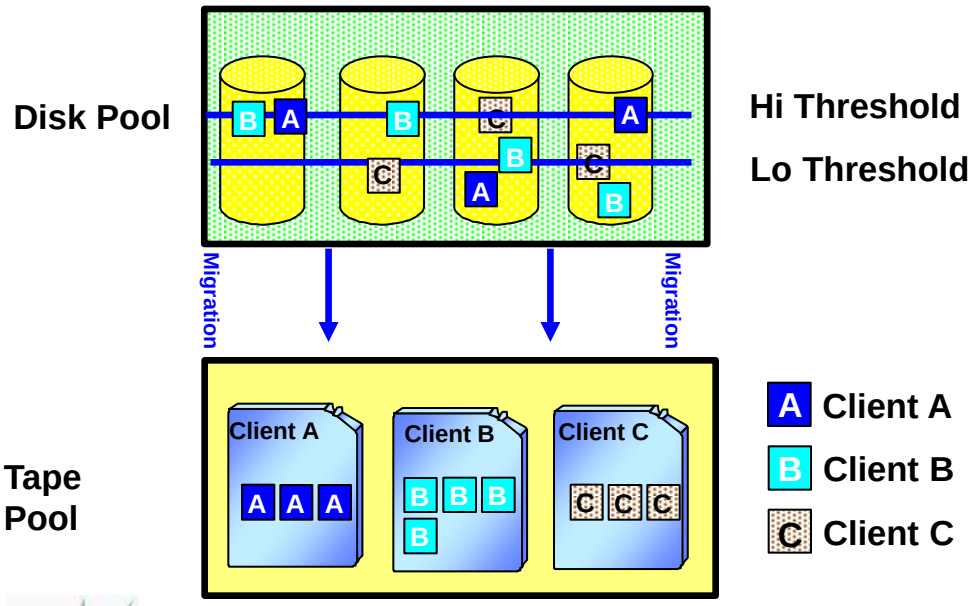


Kollokáció és szalagvisszanyerés

Kollokáció (Collocation)

Az egy klienshez vagy klienscsoporthoz tartozó adatokat egy szalagra vagy szalagcsoportra másolja

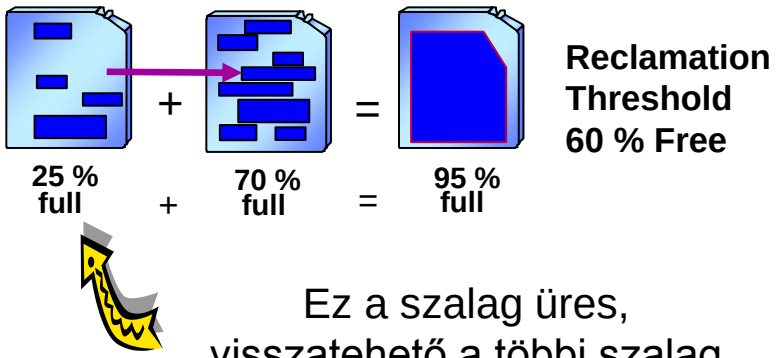
Csökkenti az adott visszaállítás során a szalagbefűzéseket és rövidebb visszaállítási idő biztosítható



Szalagvisszanyerés (Tape Reclamation)

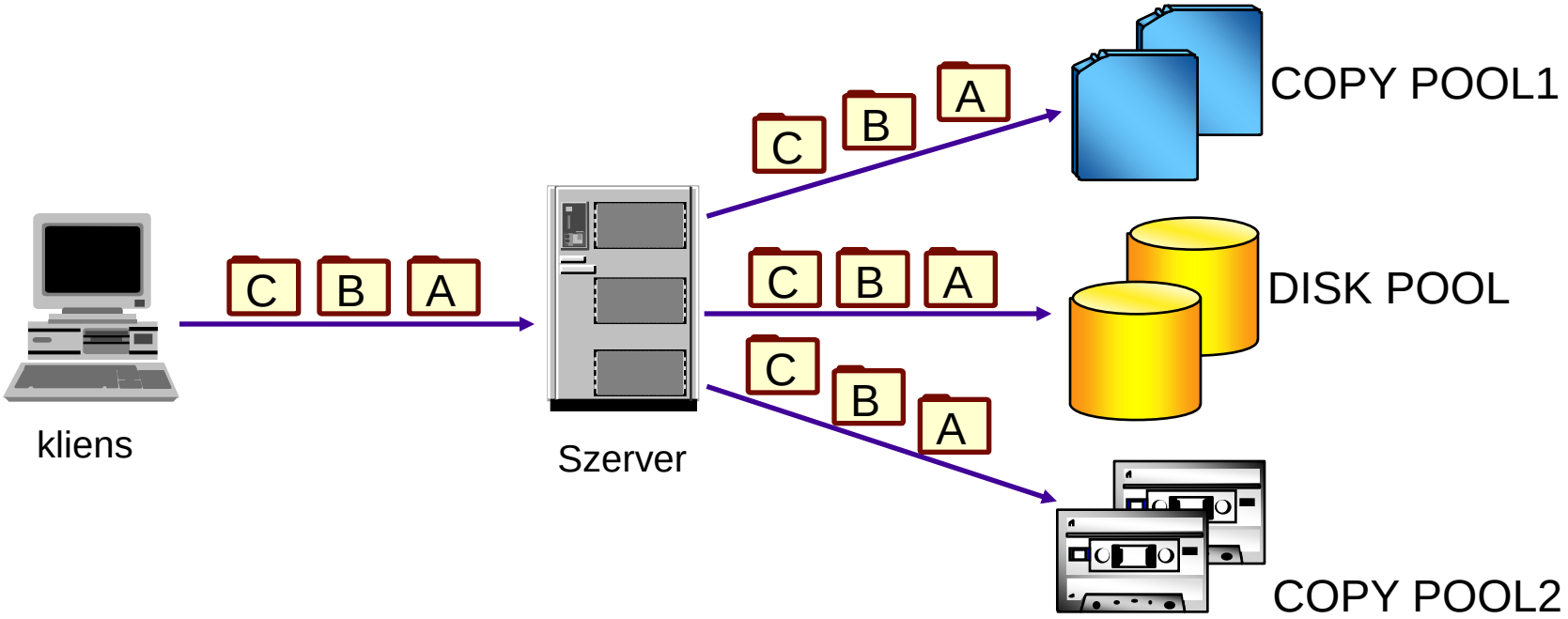
A felhasználó által definiálható küszöbérték elérésekor az érvényes adatokat egy új szalagra másolja át

Ez a másolás időzíthető, kontrollálható



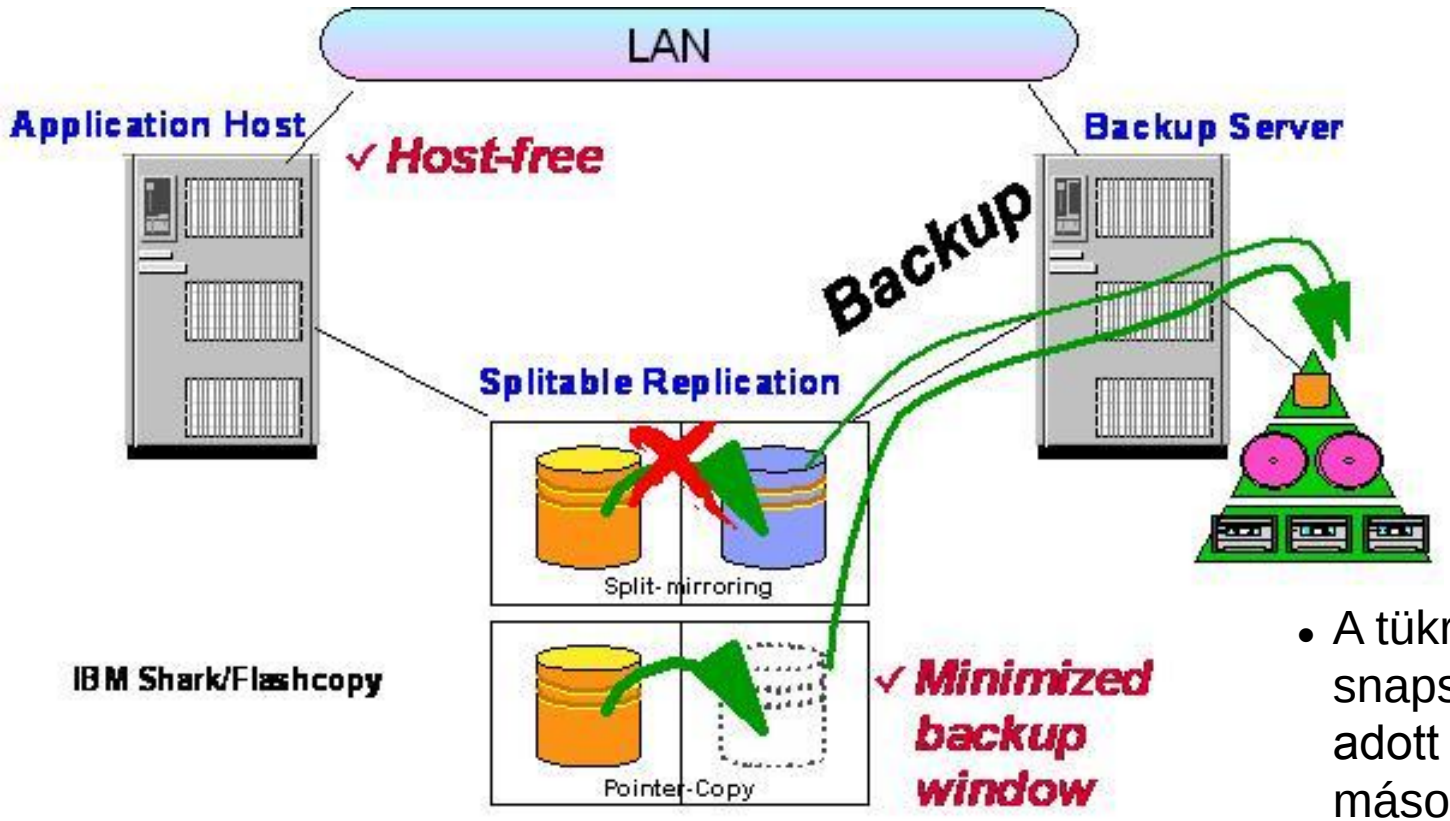
Ez a szalag üres, visszatehető a többi szalag közé, újra hasznosítva

Párhuzamos mentés



- Több copy storage pool definiálható és ezekbe szimultán történik az írás
- A cél storage pool-ok eltérő típusúak lehetnek (szalag, diszk)
- Katasztrófatűrő rendszerek kialakításánál előnyös

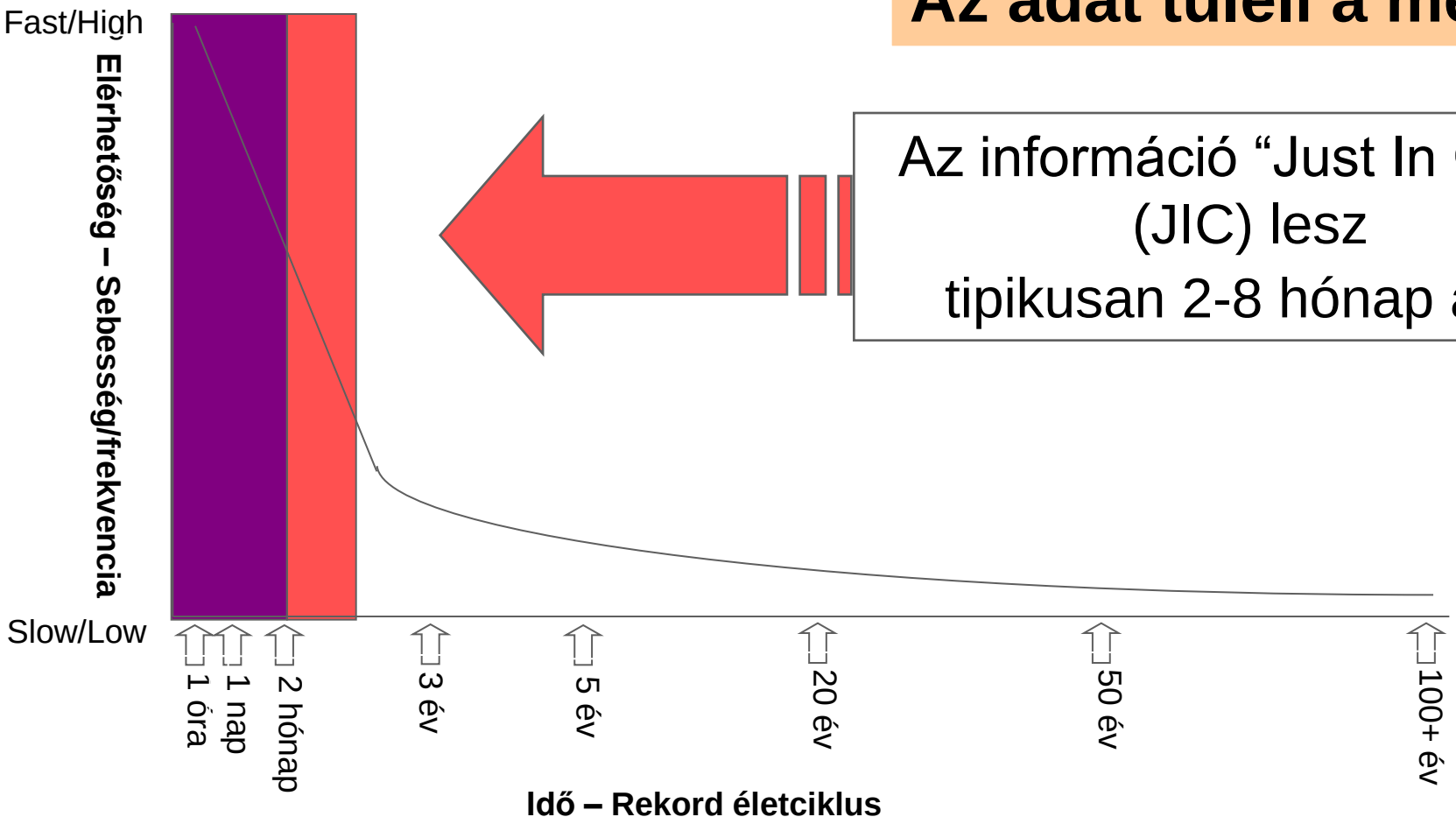
Zero down-time mentés



- A tükrözött kötet vagy snapshot tartalmazza az adott időpillanatbeli másolatot
- A mentés az így készült másolatról készül.
- Nincs szükség az alkalmazás jelentősebb leállítására

Archiválás – A JIC információ születése

Az adat túléli a médiát!

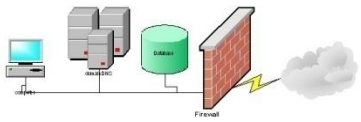


Source: Cohasset Associates, Inc.

Speciális archiválási követelmények

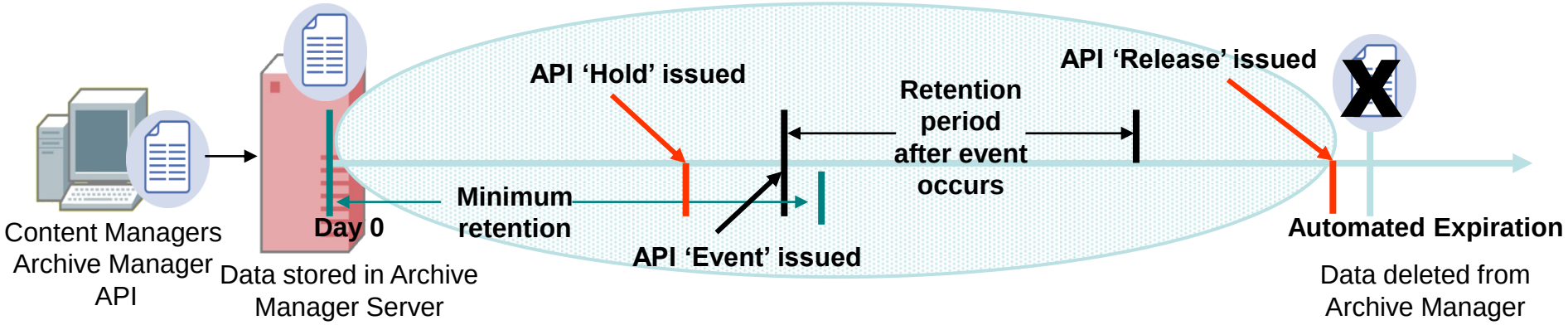
Célja az előírásoknak megfelelő adatmegőrzési kötelezettség illetve adatmegsemmisítés biztosítása

- Adat-menedzsmentet végez megőrzési és adatlejárati eljárásokon keresztül
  - Védi az adatokat a beállított megőrzési idő előtti törlés ellen
  - De törli a megőrzési idő lejártakor



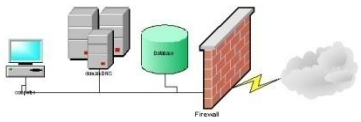
Speciális archiválási követelmények

Gazdag archiválási funkcionalitás
- –Előre definiált megőrzési idő
  - Az objektumokat egy előre meghatározott ideig – pl. 3. évig – meg kell őrizni
- –Esemény alapú megőrzés
  - A megőrzési időszak egy eseménytől függ – pl. életbiztosításnál a biztosított halála után 70 évig,
- –Törlés tiltás, engedélyezés
  - Bizonyos állományok esetében a törlés felfüggesztve – pl. egy bírósági eljárás végéig.



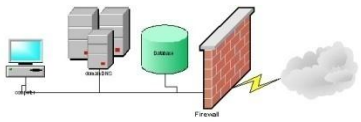
A mentést meg kell tervezni

- Nem elég, hogy „kezdjük éjfélkor”
  - Több mentés típus!
  - Ne legyen ugyanaz a *mentési ablak* (backup window)
  - A mentés mindig a rendszer teljesítménycsökkenését okozza
  - Mindig csúcsidőn kívül végezzük
    - Mikor van csúcsidő?
  - Mentés outsourcing probléma



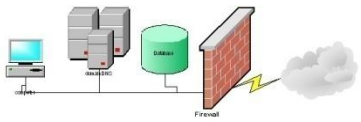
Mentés tervezésének menete

- Vállalati stratégia (Corporate Guidelines)
- Szolgáltatási szint meghatározása (SLA)
- Mentési politika (Backup and Restore Policy)
- Mentési ütemterv (Backup Schedule)



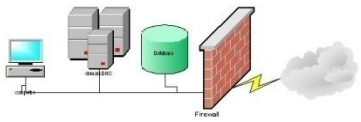
Vállalati mentési stratégia

- Egész szervezetre vonatkozik
- Jogi minimumokat, mentési célokat, szempontokat, mentendő adatok típusát határozza meg
- Nem foglalkozik a mentés megvalósításának részleteivel



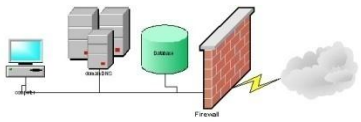
Mentési terv - igényfelmérés

- Különböző mentések – különböző célszemélyek: igényfelmérés
  - jogi osztály
  - rendszerüzemeltetés
  - gazdasági osztály
- Nagyobb cégeknél többfordulós, sokszor csak kompromisszum
- Kisebb cégeknél sokszor nincs stratégia, de ilyenkor is célszerű
  - igényfelmérés
  - különböző célú mentések szeparálása
  - egymástól elkülönült végrehajtása



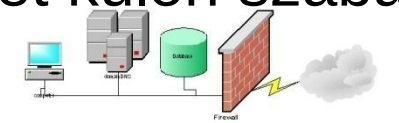
SLA meghatározása

- Ez tartalmazza, hogy az adott telephely(ek)en, mik az elvárt és biztosítandó szolgáltatási szintek
- Tipikusan a használókkal egyeztetve készül
- Egy SLA készítésekor meg kell határozni pl.:
  - a mentések típusát
  - az elvárt helyreállítási időket az egyes típusokra
  - a mentések gyakoriságát (milyen mentés milyen gyakran legyen)
  - az adatok megőrzésének idejét
  - a mentési ablako(ka)t a különböző típusú mentésekhez.



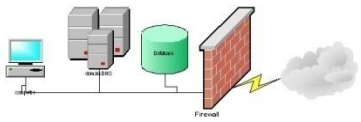
SLA példa

- A használók az utolsó 6 hónap bármelyik fájljának 1 munkanapos pontossággal való visszaállítását kérhetik.
- A használók az utolsó 6 hónap – 3 év bármelyik fájljának 1 hónapos pontossággal való visszaállítását kérhetik.
- A diszkhibák max. 4 órán belül helyreállítandók, 2 napnál nem régebbi adatokkal.
- Az archiválandó adatok negyedévente generált teljes mentések, amelyeket „örökké” meg kell őrizni.
- A kritikus adatokat olyan rendszereken tároljuk, amelyek a használók számára elérhető módon megtartják a reggel 7 és este 7 között óránként készített pillanatfelvételeket, + az éjfélkor készült pillanatfelvételeket 1 hétig.
- Az adatbázisokra és a pénzügyi rendszerekre vonatkozóan szigorúbb követelmények állhatnak fent, amelyeket külön szabályozunk.



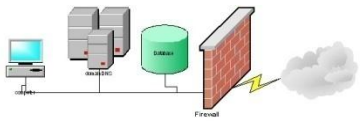
Mentési politika

- Ha az SLA elkészült,meg kell határozni azt a politikát, amellyel teljesíthetők az SLA-ban rejlő követelmények
- Ez tipikusan eléggé magától értetődik
- Az előző példa SLA esetén:
  - napi mentés
  - az SLA-ban meghatározott tárolási idők
  - annak az eldöntése, hogy legalább hány naponta legyen teljes mentés (a többi differenciális/inkrementális)



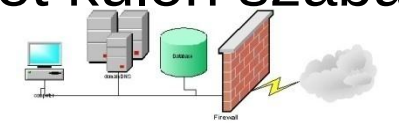
A mentési ütemterv (Backup Schedule)

- Az SLA és a mentési politika általános és ritkán változik
- Az ütemterv konkrétan leírja, hogy mikor milyen hoszt melyik partícióját kell menteni
- Sokszor a mentési ütemtervet nem írják le külön, hanem a mentő szoftver konfigurációjában rögzítik



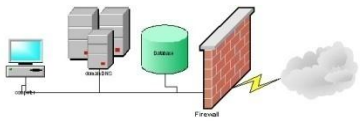
SLA példa – újra

- A használók az utolsó 6 hónap bármelyik fájljának 1 munkanapos pontossággal való visszaállítását kérhetik.
- A használók az utolsó 6 hónap – 3 év bármelyik fájljának 1 hónapos pontossággal való visszaállítását kérhetik.
- A diszk hibák max. 4 órán belül helyreállítandók, 2 napnál nem régebbi adatokkal.
- Az archiválandó adatok negyedévente generált teljes mentések, amelyeket „örökké” meg kell őrizni.
- A kritikus adatokat olyan rendszereken tároljuk, amelyek a használók számára elérhető módon megtartják a reggel 7 és este 7 között óránként készített pillanatfelvételeket, + az éjfélkor készült pillanatfelvételeket 1 hétig.
- Az adatbázisokra és a pénzügyi rendszerekre vonatkozóan szigorúbb követelmények állhatnak fent, amelyeket külön szabályozunk.



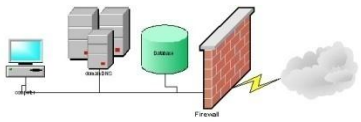
Mentési ütemterv készítése

- A pillanatfelvételeket a szerver maga készíti és kezeli, erre nem kell külön tervet készíteni
- Egy munkanap a mentés legkisebb felbontása (granularity)
- A diszk helyreállítás két nap pontossággal van előírva, nem elég csak munkanapokon menteni
- A teljes mentés (full backup) lényegesen tovább tart, mint az inkrementális/differenciális, ezért azt célszerű úgy tervezni, hogy kezdődjön péntek éjjel, és tart, amíg tart
- A többi napokon csak inkrementális/differenciális mentést végzünk



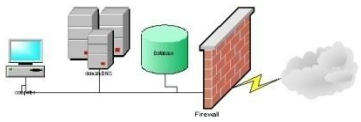
Mentési ütemterv készítése

- A mai mentőrendszerekben
  - általában elég csak azt megadni, hogy mely partíciókat kell menteni,
  - a pontos ütemtervet a szoftver elkészíti
  - a mentést elvégzi és pl. e-mailben értesítést küld, ha szalagot kell cserélni
  - de sokszor “kézzel” kell megadni, hogy a teljes mentések mikor történjenek
- A példánkban a minimális felbontás 1 hónap. Mikor legyen teljes mentés?
- Pl. minden hétvégén elmentjük a rendszerünk egy negyedét - gyors, de
  - minél ritkábban végzünk teljes mentést, a köztük készített differenciális mentések mérete annál jobban megnő !!!
  - célszerűbb teljes mentést gyakrabban végezni !!!



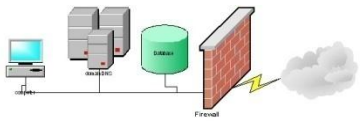
Mentési ütemterv példa 1.

- Egy partíció mérete 4GB
- Teljes mentést 4 hetente (28 nap) végzünk
- Tegyük fel, hogy a differenciális mentés mérete 5%-kal nő naponta
  - Az első nap a teljes mentés: 4GB
  - A második nap: 200MB
  - A harmadik nap: 400MB, stb.
  - A 10. nap: 2 GB
  - A 11. nap. 2,2GB,
  - Ez a két nap önmagában több, mint egy teljes mentés igénye!!!
  - Ez azt jeleni, hogy a 11. napon már érdemesebb újra egy teljes mentést végeznünk



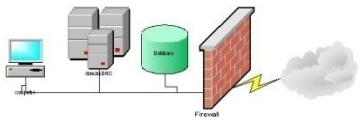
Mentési ütemterv példa 1.

– Ha táblázatban/grafikonon összefoglaljuk, hogy mennyit kell mentenünk 7, 14, 21, 28, 35 napos teljes mentési ciklusokkal, ebből kiderül, hogy az optimális a 7 napos ciklus (kb. 30% a napi teljes mentés szalagigényéhez képest), utána jön a 14 napos ciklus (kb. 40%), majd a többi, közel egyforma (60% körüli “teljesítménnyel”). Ebből az látszik, hogy bár csak havi teljes mentés van előírva, hatékonyabb a heti (kétheti, ill. e két érték közötti, praktikus megfontolásból a heti az optimális).



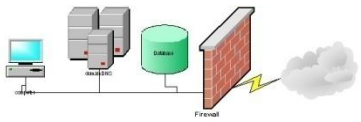
Mentési ütemterv példa 2.

- Az előző példa nem tipikus
- „80/20 szabály”: a hozzáférések 80%-a az adatok 20%-ának az ismételt elérésére irányul
- Tegyük fel: naponta az adatok 20%-át érik el, és ennek felét (10%) módosítják
- Első differenciális mentés: a partíció 10%-a
- Ez naponta csak 1%-kal nő (10% 10%-a)



Mentési ütemterv példa 2.

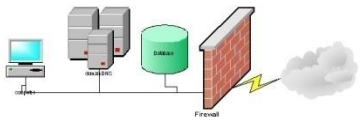
- Ezeket megint táblázatban/grafikonon ábrázolva, így a 14 napos teljes mentési ciklus az optimális (kb. 37%-os hatékonysággal), ezt követi a 21 napos (39%), majd a 28 ill. 7 napos (41%, ill. 42%).



Mentési ütemterv

- Optimális teljes mentési ciklusidő nagyban függ a tényleges használattól
- Induljunk 14 naptól + „finomhangolás”

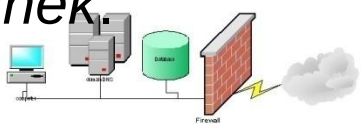
- Egyéb szempontok is figyelembe veendők
  - Hétvégén érdemesebb,
    - ha nagy a mentendő terület
    - ha nagy a hálózat/szerverek munkanap éjjeli leterheltsége



Mentési politika ismertetése

- A használókkal ismertetnünk kell a mentési politika lényegét és azt, hogy hogyan kérhetik egy fájl helyreállítását.
- Különösen fontos arról a tájékoztatás, bizonyos gépeken mentés nincs!

- "*A mentéseket csak azokon az adatokon végzünk, amelyeket a hálózati könyvtárakban tárolnak (Z: meghajtó a PC-n, ill. /home könyvtár UNIX alatt). A mentéseket minden éjjel éjfél és reggel 8 óra között végezzük.* ***Soha nem végzünk mentést a PC lokális C: meghajtóján****. Ha egy fájl helyreállítására van szükség, forduljon a következő URL-hez további információért vagy küldjön egy e-mail-t ide, a szerver nevével, a fájl komplett elérési útvonalával, és hogy milyen időponttól kell a helyreállítás. Hozzáférési problémák kezelése, egyszerű fájl helyreállítások 24 órán belül megtörténnek.*"



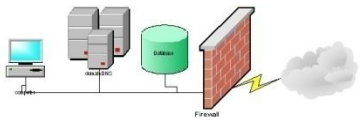
Az eddig gyakorlat szerint az anyo minden este szinkronizálódott egy melegtartalék gépre. Ez hardver kiesés esetén nyújt segítséget max. 1 napos adatvesztés mellett.

A ritkán, de olyankor annál hangsúlyosabban, felmerülő igény miatt gyártottam egy backup szervert az anyo-s tartalmak egy kicsit nagyobb időintervallumot felölelő megőrzésére. Óvatos becsléssel kb 3-4 havi adat őrizhető meg visszamenőleg. A szerver egy felújított darab, 417 GB-os tárterülettel.
A mentés három részből áll. Minden esetben hó elején van egy teljes mentés, majd az azt követő 4 alkalommal csak az ehhez viszonyított különbségek mentődnek.

1. Levelezés : minden felhasználó "Maildir" könyvtára. Azoknak, akik mailbox-ot használnak a "Mail" és "/var/mail/usernév".
(* Ez az IMAP-ot használók esetében jelenti a levelezés mentését. A POP3-at használók a saját gépükön tárolnak minden levelet.
Azt saját hatáskörben kell mentegessék.)
FULL: minden hó első napja
INKREMENTÁLIS: 7,14,21,27

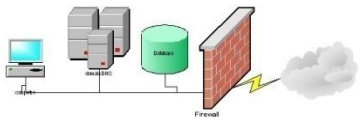
2. A projects könyvtárak: Ez egyelőre a munkaügy, titkárság és staff
FULL: minden hó második napja
INKREMENTÁLIS: 8,15,22,28

3. A /home/usernév/data tartalma. Sajnos a teljes home kötet túl sok, mentésre nem indokolt, install és egyéb nagy terjedelmű anyagot tartalmaz.
De, hogy mégis legyen lehetőség egyes fontos tartalmak mentésére, a home köteten belül a "data" nevű alkönyvtár minden felhasználó esetében mentésre kerül. Kérek mindenkit, aki ezt igénybe kívánja venni, hogy figyeljen az ide helyezendő anyagok jellegére. Erősen le lehet csökkenteni a megtartható mentések számát, ha ide install anyagok, képek, filmek, sok képet tartalmazó PPT prezentációk kerülnek.
FULL: minden hó harmadik napja
INKREMENTÁLIS: 9,16,23,29



Példa méretezés

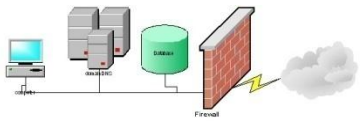
- Egy szerverkörnyezetben **2TB** adatmennyiséget kell menteni.
- Inkrementális mentést használunk.
- A változás mértéke kb. 10%/nap
  - a. Határozza meg, hogy hetes mentési ciklus, és napi mentések esetén mekkora adatmennyiséget kell menteni az első 4 hétben
- Teljes mentés: 2 TB
- Inkrementum: 2TB * 10% = 0,2 TB (naponta)
- Egy hét: 2TB + 6*0,2 TB = 3,2 TB
- Négy hét: 4 * 3,2 TB = 12,8 TB



Példa folyt.

b. Mekkora lesz a szükséges mentési időablak az egyes napokon, ha egy mentőeszköz effektív írási teljesítménye 100 GB/h?

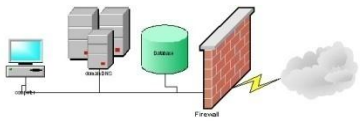
- Vasárnap (teljes mentés)
  - 2 TB / 100 GB/h = 20 (!!) óra
- Hétköznap:
  - 0,2 TB / 100 GB/h = 2 óra



Példa folyt.

c. Hány mentőeszköz szükséges, hogy a mentési ablak 8 óránál ne legyen több?

- Legrosszabb: vasárnap: 20 óra
- 3 mentőeszköz kell



Példa folyt.

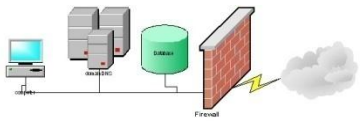
d. Hány szalag szükséges a mentéshez, ha feltételezzük hogy minden mentés új szalagra kerül, és egy szalag maximális kapacitása 500 GB?

Vasárnap: 2 TB / 500 GB = 4 szalag

Hétköznap: 0,2 TB (= 200 GB) = 1 szalag

Összesen: 4+ 6*1 = 10 szalag / hét

40 szalag / 4 hét



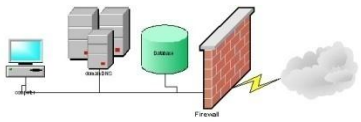
Példa folyt.

e. Egy adott időpont visszaállításához maximum hány szalag visszatöltésére van szükség?

Legrosszabb: szombat

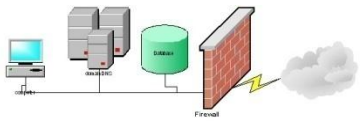
Visszaállítás: 1 full + 6 inkrementum

4 + 6*1 = 10 szalag kell



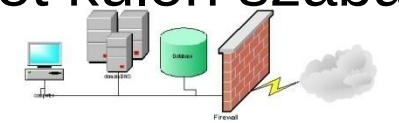
Fogyóeszköz tervezés

- A mentési politika és időzítés befolyásolja azt is, hogy mennyi fogyóeszközt kell használnunk



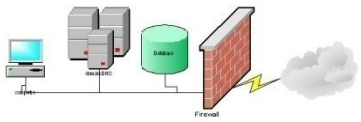
SLA példa – újra

- A használók az utolsó 6 hónap bármelyik fájljának 1 munkanapos pontossággal való visszaállítását kérhetik.
- A használók az utolsó 6 hónap – 3 év bármelyik fájljának 1 hónapos pontossággal való visszaállítását kérhetik.
- A diszk hibák max. 4 órán belül helyreállítandók, 2 napnál nem régebbi adatokkal.
- Az archiválandó adatok negyedévente generált teljes mentések, amelyeket „örökké” meg kell őrizni.
- A kritikus adatokat olyan rendszereken tároljuk, amelyek a használók számára elérhető módon megtartják a reggel 7 és este 7 között óránként készített pillanatfelvételeket, + az éjfélkor készült pillanatfelvételeket 1 hétig.
- Az adatbázisokra és a pénzügyi rendszerekre vonatkozóan szigorúbb követelmények állhatnak fent, amelyeket külön szabályozunk.



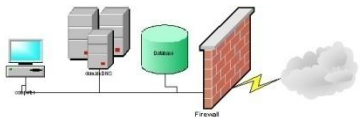
Fogyóeszköz tervezés

- *Példa:*
  - Politikánkból kiindulva:
    - az inkrementális mentéseket tartalmazó szalagokat 6 hónap után használhatjuk újra
    - a teljes mentést tartalmazókat (az archiválandó kivételével) 3 év után használhatjuk újra
    - negyedéves archiválás



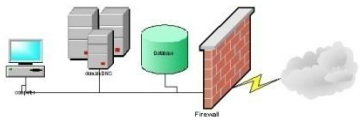
Idő és kapacitás tervezés

- A mentés és helyreállítás időben korlátozott
- DE az SLA-ban megadott időn belül meg kell történnie
- A szolgáltatás a mentés alatt szünetelhet
- A mentés idejét a következő tényezők befolyásolják:
  - a diszk olvasási sebessége
  - a mentési szalag írási sebessége
  - a sávszélesség
  - a diszk és a mentőszalag közötti hálózat késleltetési ideje



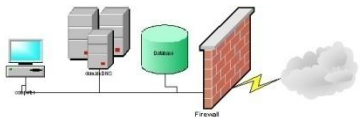
A helyreállítás

- Lassú...
- A szalagok írási és olvasási sebessége sokszor erősen eltér + megtalálási idő!!
  - Sokszor önmagában több, mint egy partíció helyreállítása
- A helyreállítás sebességét döntően a fájlrendszerek írási sebessége korlátozza!!
- A mentés meggyorsítására alkalmazott trükkök (pl. inkrementális mentés) lassítják a helyreállítást
- Hardver korlátok
  - Ha az írással azonos sebességgel jön az adat...
- Gyorsítás: sokszor külön mentőhálózat



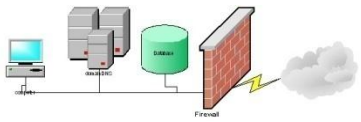
Helyreállítás: biztonsági kérdések

- Van-e joga valakinek az adott fájl helyreállítását kérni (és a fájlt használni)? – kérés validálása!
- A fájl hozzáférési jogosultságok és tulajdonjogok változnak-e a helyreállítás során?
- A kért adatot az eredeti helyen – az eredeti hozzáférési jogokkal – állítjuk helyre (tudjuk helyreállítani) vagy máshol esetlegesen más jogokkal?
- Felülír-e ez meglévő adatokat?



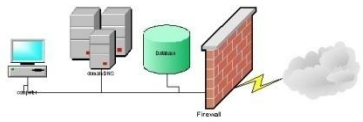
Személyzeti kérdések

- A helyreállítást több ember is tudja elvégezni, ne csak az, aki tervezte a rendszert
- Dokumentálás:
  - on-line,
  - papíron a helyreállító egység közelében
- A dokumentáció és a betanítás legyen arányos azzal, hogy milyen gyakran kell helyreállítást végezni
- Különösen fontos: mit kell tenni akkor, ha a helyreállító egységet vezérlő gép hal meg
- A dokumentumoknak tartalmaznia kell
  - a szállítók kapcsolattartóinak elérhetőségét,
  - a műveletet elvégezni képes/jogosult személyek telefonszámát,
  - a szükséges jelszavakat



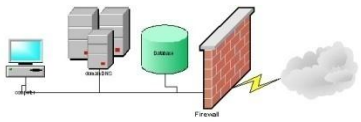
Centralizáció

- A centralizációval tipikusan kétféle költséget lehet jelentősen csökkenteni:
  - a berendezésekét (drágák, mert nagypontosságú, nagysebességű mechanikát igényelnek és nagy megbízhatóságot, kis hibavalószínűséget).
  - a szalagcseréét (költséges, mert munkaigényes)
- Elosztott mentés hátrányai
  - Minden gép mellé mentőegység – hiba – 2db!
  - Kazettacsere hosszadalmas
- Hálózati mentő rendszerek
- Jukebox-ok
- Szalag meghajtó (tape drive) törés - tartalék



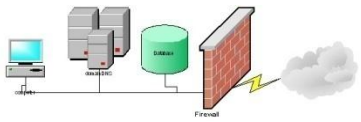
Szalag nyilvántartás

- A mentés nyilvántartás nélkül nem ér semmit
- A tartalomjegyzéket RAID-del védeni
- Automatikus nyilvántartás
  - Nincs – minden szalagon olvasni időben visszafelé
  - Partíció szintű
  - Fájl szintű – gyors, de nagy
  - Kompromisszum a kettő között
- Nyilvántartás (automatikus) helyreállítása
- Nyilvántartás, hogy egy szalag hányszor használt
- Mi van, ha úgy kell helyreállítani, ha a helyreállító rendszer rossz?
  - a szalagon magán legalább minimális tartalom info



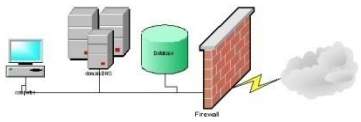
„Tűzriadók” – Fire drills

- Csak akkor tudjuk meg, hogy valójában mennyire jó egy mentő rendszer, ha helyreállítást végzünk vele – gyakorlat kell
- Véletlenszerűen kiválasztott fájl helyreállítása
- Diszk helyreállítása
  - Ritkább – kijövünk a gyakorlatból
  - Nagy adatmennyiség – mindenhol elég a kapacitás?
  - Monitorozás (diszk, szalag, hálózat) – ha gond van
  - Ha nincs elég hely – új szerver beállításakor



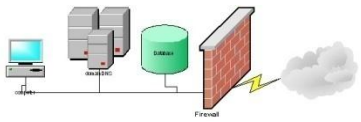
Külső telephelyen való tárolás

- Biztonságos tárolás szükségessége
  - Zárható szekrény
  - Más telephely
    - Duplikálás
    - Csak az előző mentést tároljuk ott
- Raktárszolgálat – SA hazaviszi
- Több telephellyel rendelkező cég
  - Helyben mentés – szalag csere
  - Kis kihasználtságú hálózati összeköttetés – mentés a „másik” helyen a hálózaton keresztül



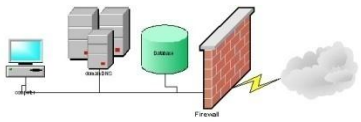
Adatbázisok problémája

- Az adatbázis tipikusan átlátszó a mentőrendszer számára, az az egész adatbázist egy egységként (fájlként) kezeli.
- Baj akkor van, ha az adatbázis mentés közben módosul, mert egy adat megváltoztatása például több, fizikailag máshol lévő indexbejegyzés módosítását is igényli.
- Mivel ezek távol vannak egymástól, mentés során inkonzisztencia alakulhat ki.
- Ezért adatbázist csak annak kikapcsolt állapotában szabad menteni, ami sokszor nem engedhető meg.
- RAID rendszerek (duplikált diszk) alkalmazása.
- Mentés idejére a két diszket szétválasztják.
- Különösen kritikus esetekben három diszken dolgozik az adatbázis-kezelő, így mentés alatt is marad duplikátum.



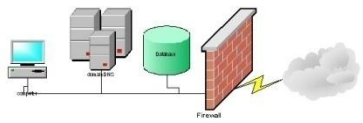
Technológiai változások

- Diszk és szalag technológia fejlődése nem egyenletes
  - Diszk: közel lineáris (1-1,5 évente duplikálódik)
  - Szalag: nagyobb ugrások
    - Szalagos egységek drágák – ne kelljen cserélni ***ezeket*** gyakran
- Technológia váltáskor a régi szalagos egységből is el kell tenni 1 (2) darabot!
- Egyenlőtlen fejlődés – a mentés módját is változtatja



Mentés és helyreállítás - Összefoglalás

- Mentés / archiválás
- Mentés típusai
  - Teljes, inkrementális, differenciális, progresszív
- Mentés megtervezése
  - Vállalati stratégia, SLA, Mentési politika, Mentési ütemterv, Idő- és kapacitástervezés, Fogyóeszköz tervezés, Mentési politika ismertetése
- Helyreállítással kapcsolatos kérdések
  - Biztonság, Személyzet, Centralizáció, Nyilvántartás, Gyakorlás, Külső tárolás, Adatbázisok, Technológiai fejlődés hatásai

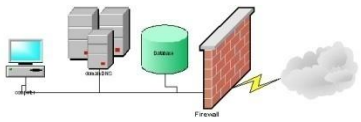


Információs rendszerek üzemeltetése

Felhő IT (Cloud Computing)

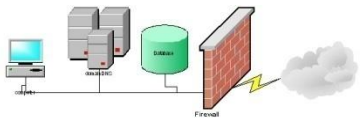
BME VIK TMIT

Mérnök-informatikus alapképzés

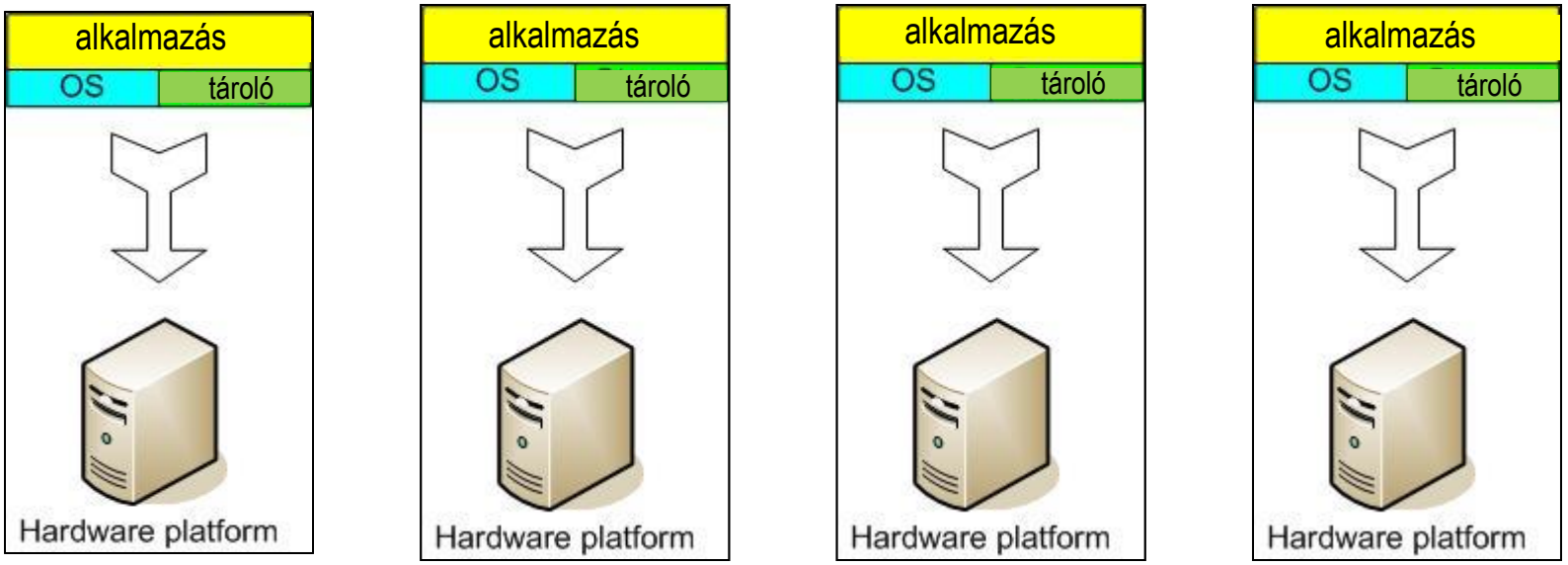


Virtualizáció és felhő IT (Cloud Computing)

- Virtualizáció:
  az a képesség, hogy egy fizikai rendszeren több(féle) operációs rendszer futtatható (és megosztják a rendelkezésre álló erőforrásokat)
- Felhő IT:
  Szolgáltatások kívánság szerint, az erőforrások le/felskálázásával



Nézzünk egy példát: hagyományos szerver koncepció



webszerver

Windows

IIS

alkalmazás-szerver

Linux

DB szerver

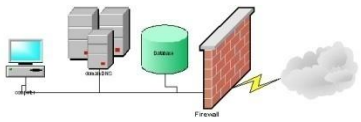
Linux

MySQL

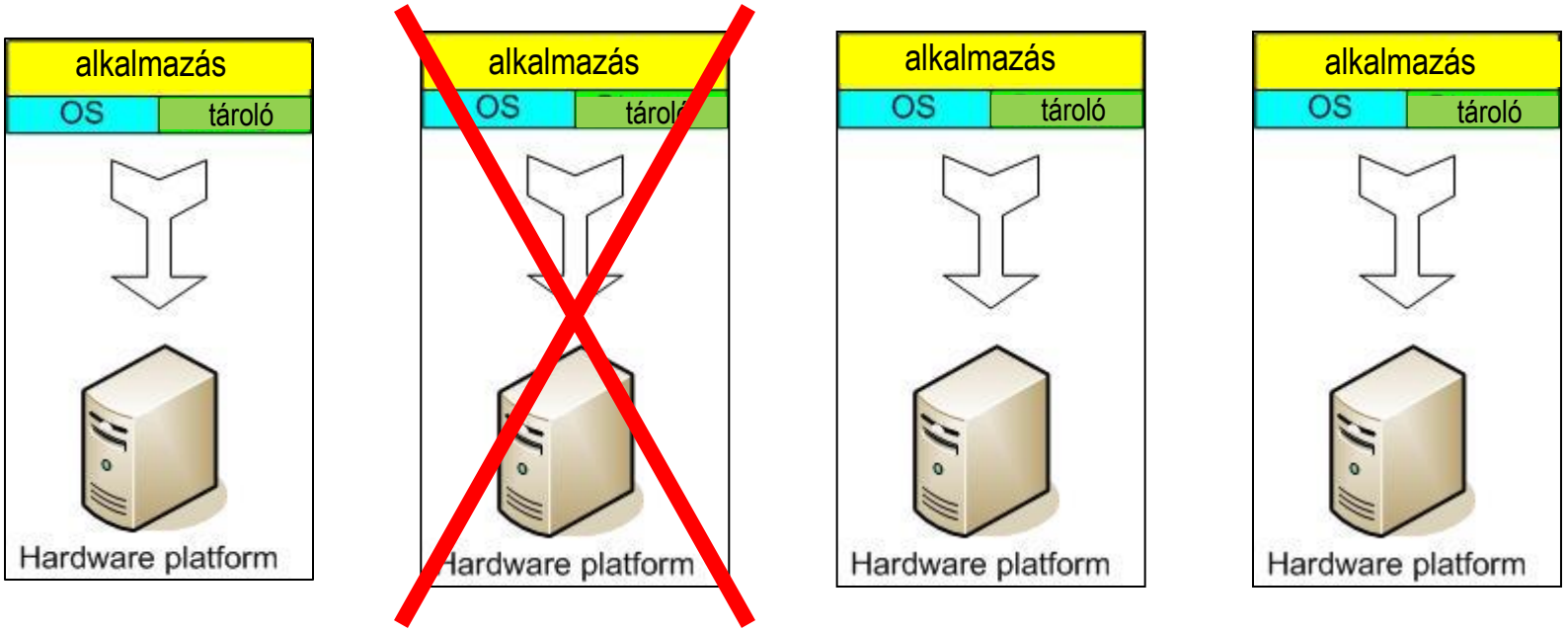
e-mail

Windows

Exchange



... ha valamelyik elromlik:



webszerver	az alkalmazás	DB szerver	e-mail
Windows	szerver leáll	Linux	Windows
IIS		MySQL	Exchange

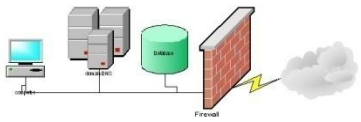
A hagyományos szerver koncepcióban

a rendszergazda a szervert tipikusan olyan egységnek fogja fel, amiben benne van a hardver, az op. rendszer, a tároló és az alkalmazások

a szerverekre gyakran szolgáltatásaik szerint hivatkoznak (levelező, adatbázis, fájl szerver, stb.)

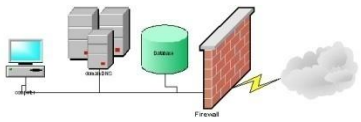
az egység hibája esetén a szolgáltatás leáll

hibatűrő megoldásokkal a leállás esélye csökkenhető (persze ennek is vannak korlátai).

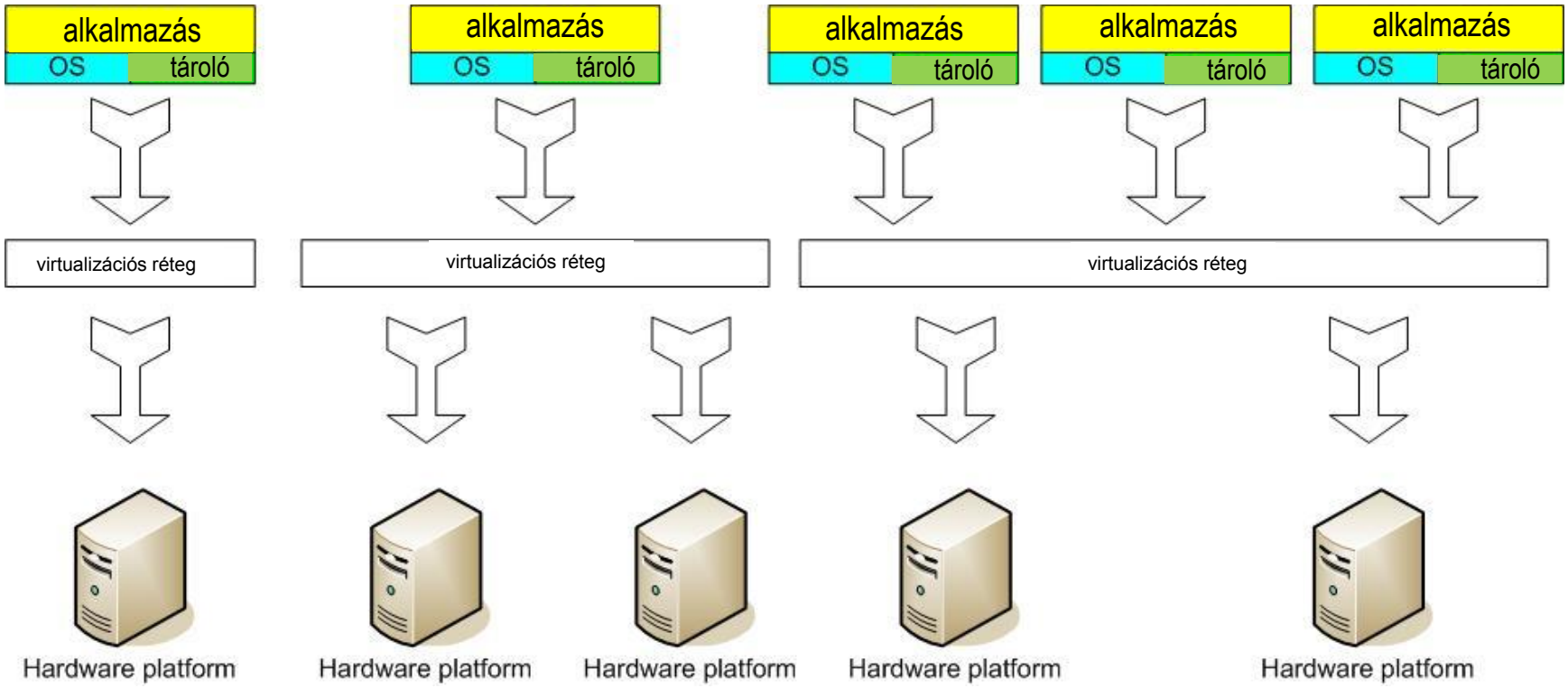


A hagyományos szerver koncepció

- előnyei
  - könnyű tervezni
  - könnyű megvalósítani
  - könnyű menteni (backup)
  - virtuálisan bármely alkalmazás/szolgáltatás futtatható ilyen telepítésben
- hátrányai
  - viszonylag drága felállítani és karbantartani a hardvert
  - nem nagyon skálázható
  - nehéz másolni (replicate) a konfigurációt
  - redundanciát viszonylag nehét implementálni
  - hardver üzemszünet miatt sebezhető
  - a processzor kihasználtsága gyakran alacsony



Virtuális szerver koncepció



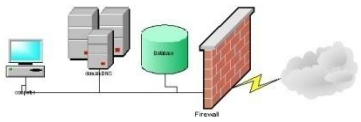
Virtuális gép réteg a felhasználói („vendég”) op. rendszer és a hardver között

A virtuális szerver koncepció

logikailag elválasztja a szerver szoftvert a hardvertől

- a szerver szoftverbe beleérthetjük az op. rendszert, az alkalmazásokat és a tárolást is

- Egy virtuális szervert egy vagy több host is megvalósíthat és fordítva: egy host több virtuális szervert is magába foglalhat.
- A virtuális kiszolgálókat (is) funkció szerint szokás hivatkozni (levelező, adatbázis, fájl szerver, stb.).



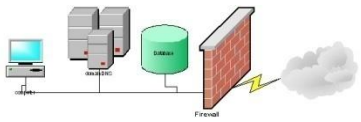
A virtuális szerver

szolgáltatásai (jó tervezéssel) nem szünetelhetnek egy host kiesésével (ezzel pl. a karbantartás és a hardver upgrade is leállítás nélkül elvégezhető)

könnyen skálázható (szükség szerint allokálható erőforrás)

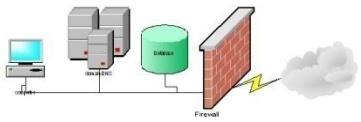
szerver mintákkal (templates) többszörözhető

hostról hostra könnyen telepíthető



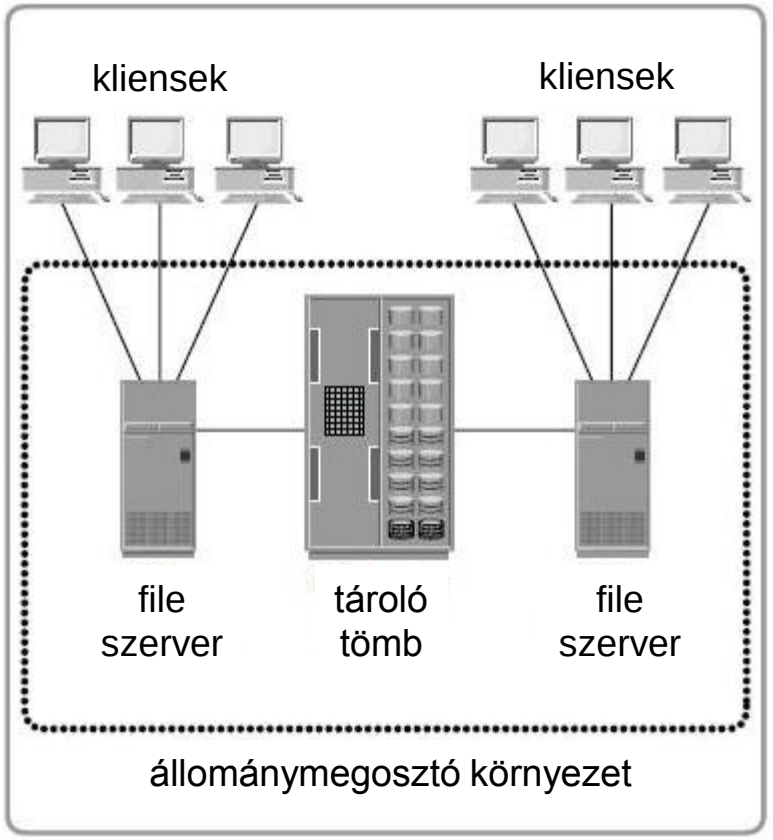
A virtuális szerver koncepció

- előnyei
  - közös erőforrás gazdálkodás (Resource pooling)
  - redundancia
  - magas rendelkezésre állás
  - új szerver gyors telepítése
  - leállás nélkül átkonfigurálható
  - fizikai erőforrások optimalizálása gazdaságos
- hátrányai
  - bonyolultabb tervezés
  - drágább konfiguráció, mint a hagyományos (ugyanúgy meg kell a hardvert, az OS-t, az alkalmazásokat + az absztrakciós réteget is)



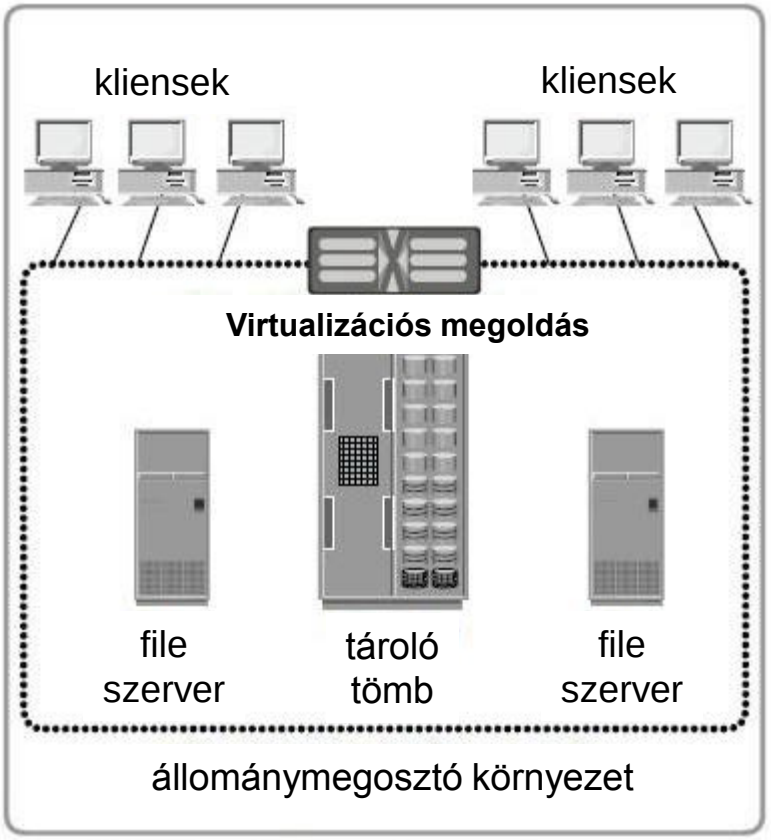
Fájlszintű virtualizáció

- Fájlszintű virtualizáció nélkül
  - egy kliens/host egy fájlt szeretne elérni egy adott fájlszerveren
  - tudnia kell, hogy melyiken
  - lehet, hogy az egyik szerver tele, a másik üres
  - fájl mozgatás érinti a klienst is



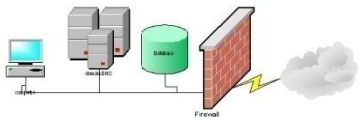
Fájlszintű virtualizáció

- Virtualizált fájlszerver
  - a kliensnek nem kell tudni, melyik fizikai szerveren van a fájl
  - egyszerűbb
    - terhelésmegosztás
    - fájlmozgatás
    - bővítés
- Cloud computing



A virtualizáció következő lépése a felhő IT

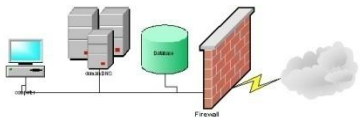
- Nem kell saját hardverrel rendelkezned.
- Bérelheted a „felhőből”.
- Nyilvános, privát, vagy hibrid felhő IT.



A felhő IT (Cloud Computing)

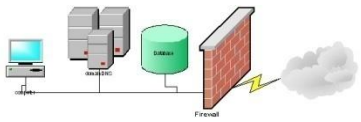
felhasználás alapján fizetett IT erőforrás igénybe vételi modell.

Hálózati hozzáférés egy megosztott IT erőforrás készlethez (pl., szerverek, tárolók, alkalmazások, szolgáltatások), amit (a szükséges verzióban) gyorsan lehet biztosítani, kevés szolgáltatói interakcióval.



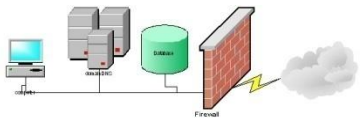
Amit a felhasználó igényel:

- teljesítmény
- skálázhatóság
- rendelkezésre állás
- biztonság
- erőforrások igény szerint
- költséghatékonyság
- azt fizessem, amit használok
- fix költség változó költséggé fordítása



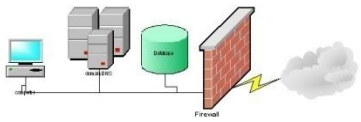
Az elterjedés legfontosabb feltételei

	Mit értünk alatta?
Univerzális hozzáférés	A felhő IT szolgáltatásai legyenek mindenütt igénybe vehetők (ubiquitous) – munkaállomásról, mobil eszközről, telefonról, céleszközről
Skálázható szolgáltatások	Fel/leskálázás, az ezt vezérlő infrastruktúrával. Üzletvezérelt erőforrás-allokálás: a tőke és a működési költségek alapján fogják megítélni, hogy mi/mennyi szükséges.
Új alkalmazás-szolgáltatási modellek	Párhuzamos és folytonos szolgáltatások is lehetnek.



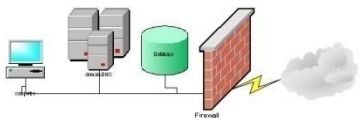
Alapelvek

- Internet protokollokkal elérhető bármely számítógépről.
- Mindig elérhető és az igényekhez igazítható.
- Felhasználás szerint fizetett (pay per use).
  (lesz más is? – pl. reklámérték szerinti?)
- Vezérlő/ellenőrző interfészek.
- „Önkiszolgáló”



National Institute of Standards and Technology (NIST) definíció:

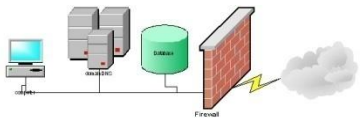
"pay-per-use” (fizesd-amit-használsz) modell létező, kényelmes és igény-szerinti hálózati hozzáférés engedélyezésére konfigurálható IT erőforrások (hálózatok, szerverek, tárolók, alkalmazások és szolgáltatások) megosztott készletéhez, amelyek könnyen létesíthetők és változtathatók minimális menedzsment erőfeszítéssel vagy szolgáltatói interakcióval.”

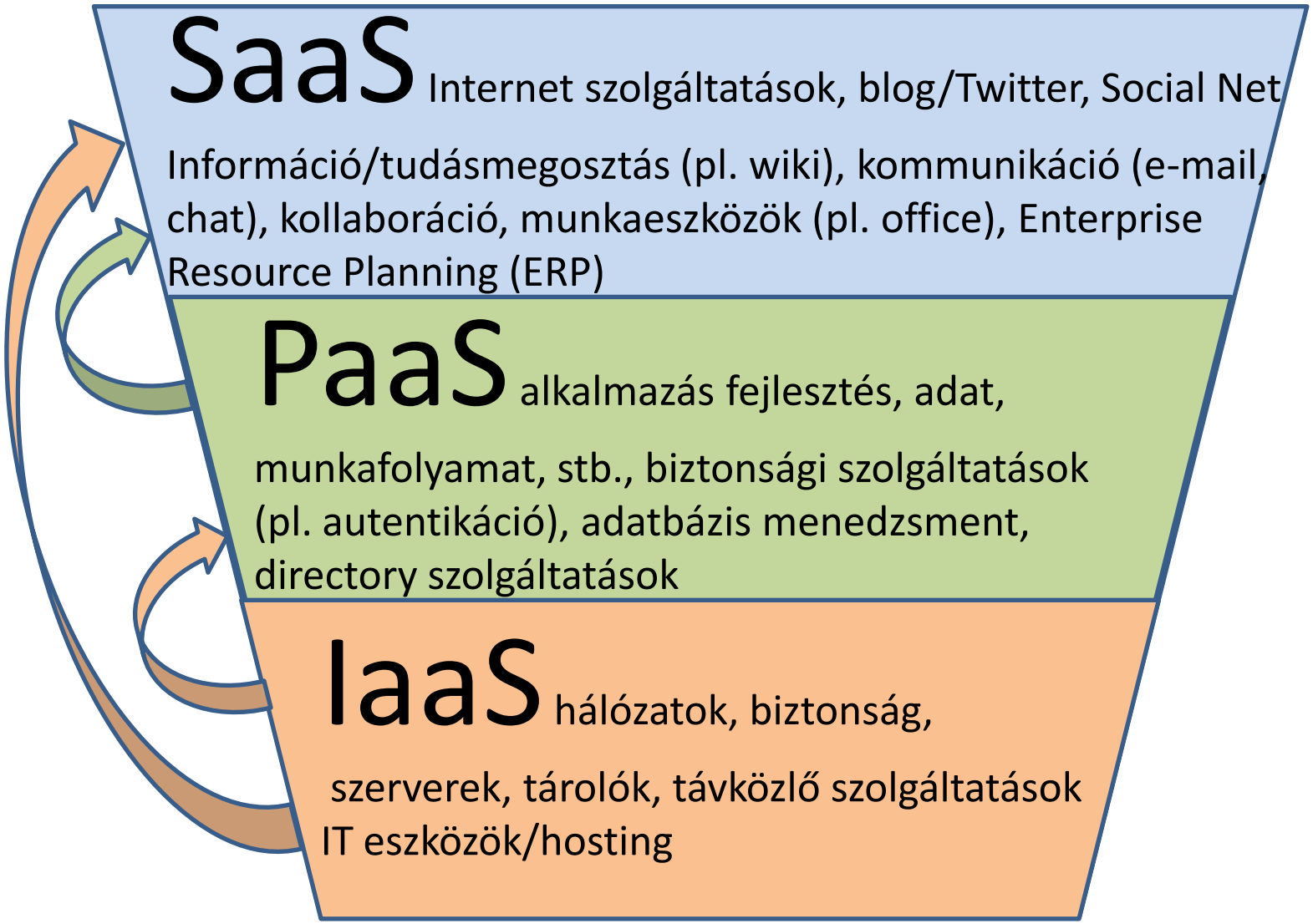


SaaS (Software as a Service): szoftver szolgáltatási modell, amiben a felhasználó alkalmazás licencet kap, igény-szerinti (on demand) szolgáltatásként

PaaS (Platform as a service): IT platform & megoldási csomag szolgáltatásként

IaaS (Infrastructure as a Service): IT infrastruktúra, mint szolgáltatás (tipikusan platform virtualizációs környezet)

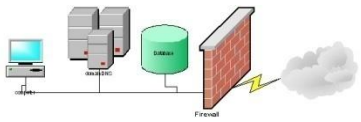



SaaS Internet szolgáltatások, blog/Twitter, Social Net
Információ/tudásmegosztás (pl. wiki), kommunikáció (e-mail, chat), kollaboráció, munkaeszközök (pl. office), Enterprise Resource Planning (ERP)
PaaS alkalmazás fejlesztés, adat,
munkafolyamat, stb., biztonsági szolgáltatások (pl. autentikáció), adatbázis menedzsment, directory szolgáltatások
IaaS hálózatok, biztonság,
szerverek, tárolók, távközlő szolgáltatások
IT eszközök/hosting

SaaS (Software as a Service): szoftver szolgáltatási modell, amiben a felhasználó alkalmazás licencet kap, igény-szerinti (on demand) szolgáltatásként

PaaS (Platform as a service): IT platform & megoldási csomag szolgáltatásként

IaaS (Infrastructure as a Service): IT infrastruktúra, mint szolgáltatás (tipikusan platform virtualizációs környezet)

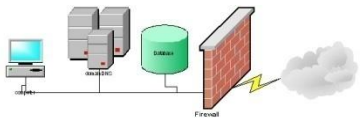


… *akármi*-as-a service

Vigyázat: a világ tobzódik az XaaS – ben !

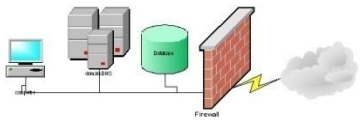
- Storage-as-a-service
- Database-as-a-service
- Information-as-a-service
- Process-as-a-service
- Application-as-a-service
- Platform-as-a-service
- Integration-as-a-service
- Security-as-a-service
- Management/Governance-as-a-service
- Testing-as-a-service
- Infrastructure-as-a-service

Az IRÜ tantárgyban visszafogjuk magunkat ebben …



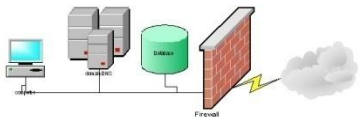
Típusai

- Nyilvános felhő (Public Cloud)
  - az IT infrastruktúrát egy szolgáltató a saját telephelyein működteti. Az ügyfél nem tudja, nem befolyásolja, hogy hol. Az infrastruktúrán tetszőleges ügyfelek osztoznak.
- Magánfelhő (Private Cloud)
- Hibrid felhő (Hybrid Cloud)



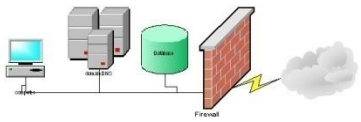
Típusai

- Nyilvános felhő (Public Cloud)
- Magánfelhő (Private Cloud)
  - dedikált IT infrastruktúra egy bizonyos szervezet számára, nem osztozik mással *(… lehet, hogy ez nem is igazi felhő IT ???)*; drágább, biztonságosabb, mint a nyilvános felhő IT
  - *on-premise* (az adott szervezet telephelyén) vagy *externally hosted* (egy felhőből dedikálva)
- Hibrid felhő (Hybrid Cloud)



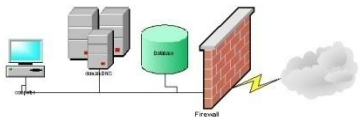
Típusai

- Nyilvános felhő (Public Cloud)
- Magánfelhő (Private Cloud)
- Hibrid felhő (Hybrid Cloud)
  - pl. (1) kritikus alkalmazások magánfelhőben, mások nyilvános felhőben;
    pl. (2) normál IT üzem a szervezet saját infrastruktúráján, különleges/csúcs terheléshez pótlólagos erőforrás nyilvános felhőből



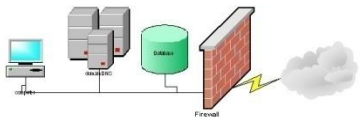
Szolgáltatási példák

Software-as-a service	- Internet alkalmazási webhelyek - csoportmunka - Office	Flickr, Gmail, Myspace, Cisco Webex, IBM Bluehouse
App-components-as-a-service	- API alkalmazás integrációhoz - webes szoftverek, amik kombinációival új szolgáltatások hozhatók létre (ld. Mashup)	Google Calendar API Yahoo! maps API Salesforce.com's AppExchange Amazon Flexible Payment Services zembly
Platform-as-a-service	- fejlesztési platform (as a service) - Message Queue - Blob / object data stores	Google App Engine, BigTable MS SQL Server Data Services Engine Yard Salesforce.com's Force.com
Infrastructure-as-a-service	- virtuális szerverek - logikai diszkek - VLAN hálózatok - rendszer menedzsment	Akamai, Amazon EC2, Cohesive FT, Mosso, Nirvanix Storage Delivery Networks
Fizikai infrastruktúra	- menedzselt hosting - nem menedzselt hosting - kolokáció - ISP	GoDaddy Rackspace Savvis



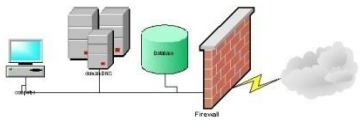
Migráció a felhőbe?

- Miért?
  - költségtakarékosság
  - energiatakarékosság
  - „zöld IT”
  - nagyobb fürgeség a szoftver piacon
  - biztonsági megfontolások



Migráció a felhőbe?

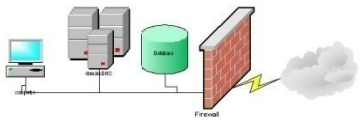
- Hogyan?
  - áttelepülés nyilvános felhő IT-be
  - magánfelhő létrehozása
    - adatközpont migrálása magánfelhővé
    - új magánfelhő IT
  - hibrid migráció
    - fontos: az adat- és alkalmazás-hordozhatóság megoldása



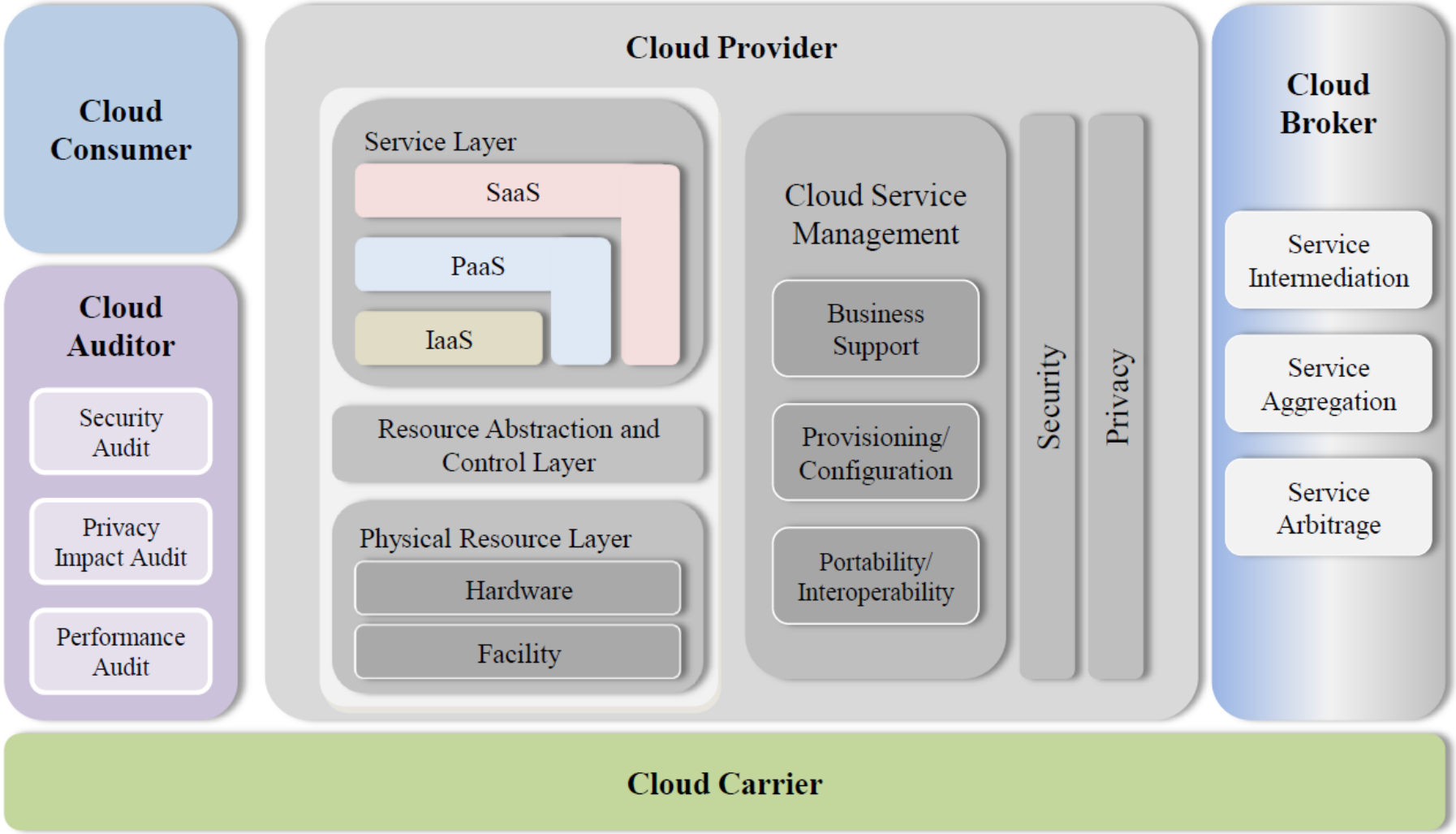
A felhő IT-k együttműködtethetősége szabványosítást kíván.

- adat- és alkalmazás-hordozhatóság
- felhő IT-k integrálhatósága

De: a túlspecifikáltság megölné az innovációt.



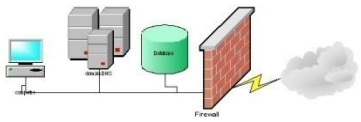
Elvi referencia modell



Szabványosítási törekvések

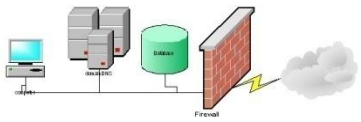
- **UCI**: Unified Cloud Interface by Cloud Computing Interoperability Forum (CCIF).
  - http://groups.google.com/group/unifiedcloud
- **OCCI**: The Open Cloud Computing Interface by Open Grid Forum (OGF).
  - http://www.occi-wg.org

- Cloud Standards Wiki (cloud-standards.org)



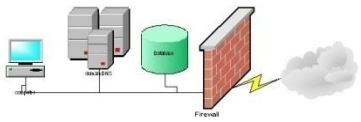
továbbá …

- ITU-T Focus Group on Cloud Computing
- OGF (Open Grid Forum)
- Cloud Computing Interoperability Forum
- NIST (National Institute of Standards and Technology)
- ETSI (European Telecommunications Standards Institute)
- OASIS (Organization for the Advancement of Structured Information Standards)
- DMTF (Distributed Management Task Force)



UCI

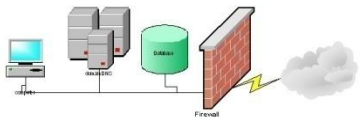
- Az egységes felhő interfész (unified cloud interface = UCI) más néven „felhő bróker” egy szemantikus specifikációból és egy ontológiából áll (Semantic Cloud Abstraction). Az ontológia tartalmazza az aktuális modell leírását, a specifikáció definiálja a más modellekkel való integrálás részleteit.
  http://groups.google.com/group/unifiedcloud



OCCI

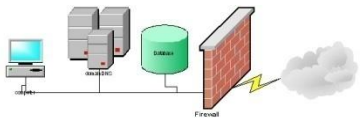
OCCI = Open Cloud Computing Interface

- Az Open Grid Forum fejleszt egy specifikáció-készletet.
  Lényegében: protokoll és API különböző felhő IT menedzsment feladatokhoz.
  Eredetileg egy távoli (remote) menedzsment *„API for IaaS model based Services”* volt a cél (különböző felhő IT infrastruktúrákban közös feladatokhoz: szolgáltatás bevezetése, skálázása, monitorozása). Ebből egy rugalmas API nőtt ki: integráció, hordozhatóság, interoperabilitás céljaira (bővíthető).



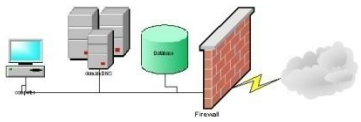
OCCI specifikáció

- kapcsolat
  - Single OCCI REST end point over HTTP(S).
- autentikáció
  - SSL/TLS, NTLM, Kerberos
- reprezentáció
  - OCCI deszkriptor formátum (alkalmazás/occi+xml)
  - nyílt virtualizációs formátum (alkalmazás/ovf+xml)
  - nyílt virtualizációs archívum (alkalmazás/x-ova)
  - konzol (VNC)



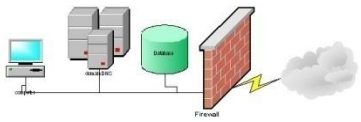
OCCI specifikáció

- Deszkriptorok
  - feldolgozó (Compute)
  - hálózat (Network)
  - tároló (Storage)
- Azonosítók
  - URI-val hivatkozott erőforrások



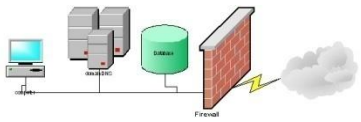
OCCI műveletek

- Create
  - POST
- Retrieve
  - GET
- Update
  - GET and PUT
- Delete
  - DELETE
- Requests
  - Trigger State Changes via POST



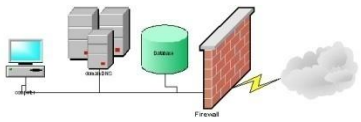
OCCI: OpenNebula

- nyílt forrású ipari standard adatközpont virtualizációhoz
- virtualizációs menedzsment eszköz
- http://opennebula.org/



Nebula implementációs alapelvek

- Nyílt és nyilvános API-k
- Nyílt (open-source) platformok, app-ok és adatok
- Nyílt forráskódok és dokumentációk
- Referencia platformok



Néhány megfontolás …

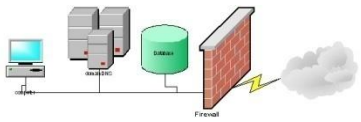
… pay-per-use alapú hozzáférés az Internet „*végtelen*” erőforrásaihoz
… az Internet NEM VÉGTELEN ERŐFORRÁS

… a felhő infrastruktúra ad keretet az alkalmazásokhoz való skálázható, megbízható, igény szerinti hozzáféréshez …
… mindennek ára van: ez új infrastruktúra réteget jelent

… a felhő szolgáltatások „láthatatlan” hátteret (backend) adnak a legtöbb mobil alkalmazáshoz is …
… mégis van néhány nagy elkülönült platform

… nagyfokú rugalmasság ez energiafogyasztásban …
… csak „nagyban” értelmes

… történeti gyökerek
… keresőmotor, e-mail, közösségi háló; állománytárolók (Flicker, Dropbox, stb.) – eddig sem érdekelt, hol kapnak erőforrást



Nyilvános és magánfelhő együttműködése

OpenStack Compute

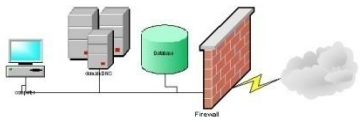
OpenStack Object Storage

OpenStack Image Service

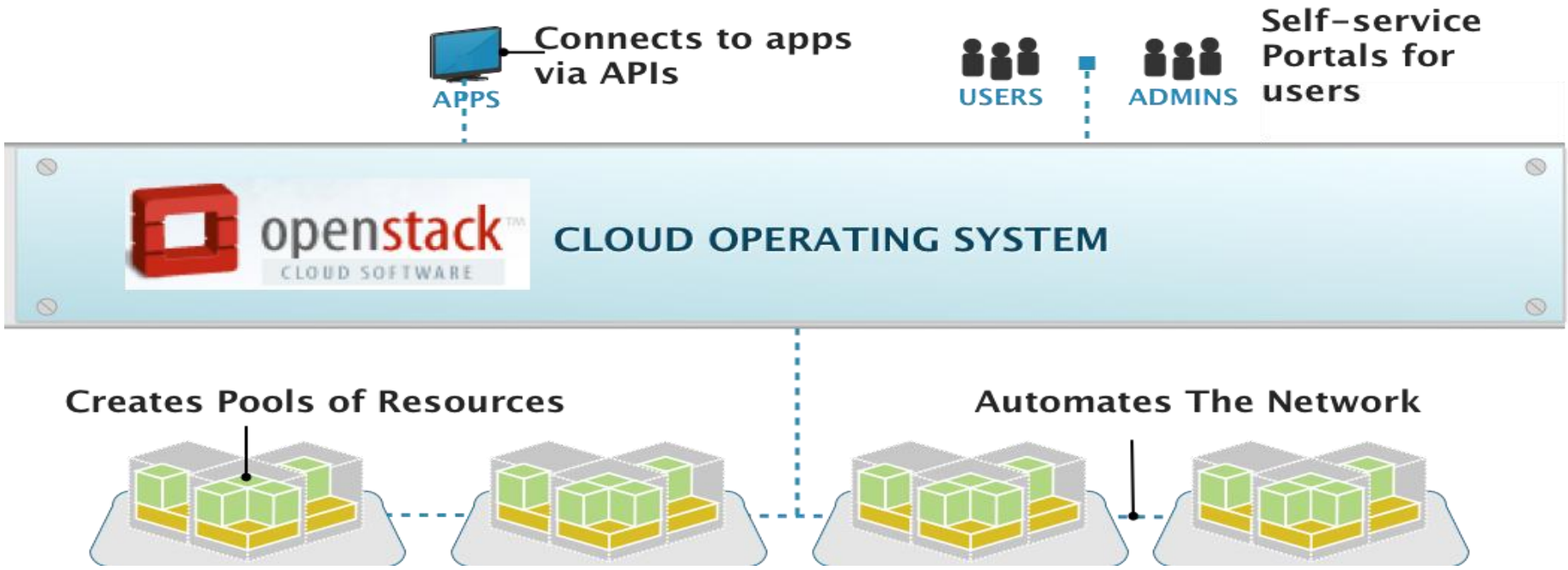
openstack™
CLOUD SOFTWARE

OpenStack elemek

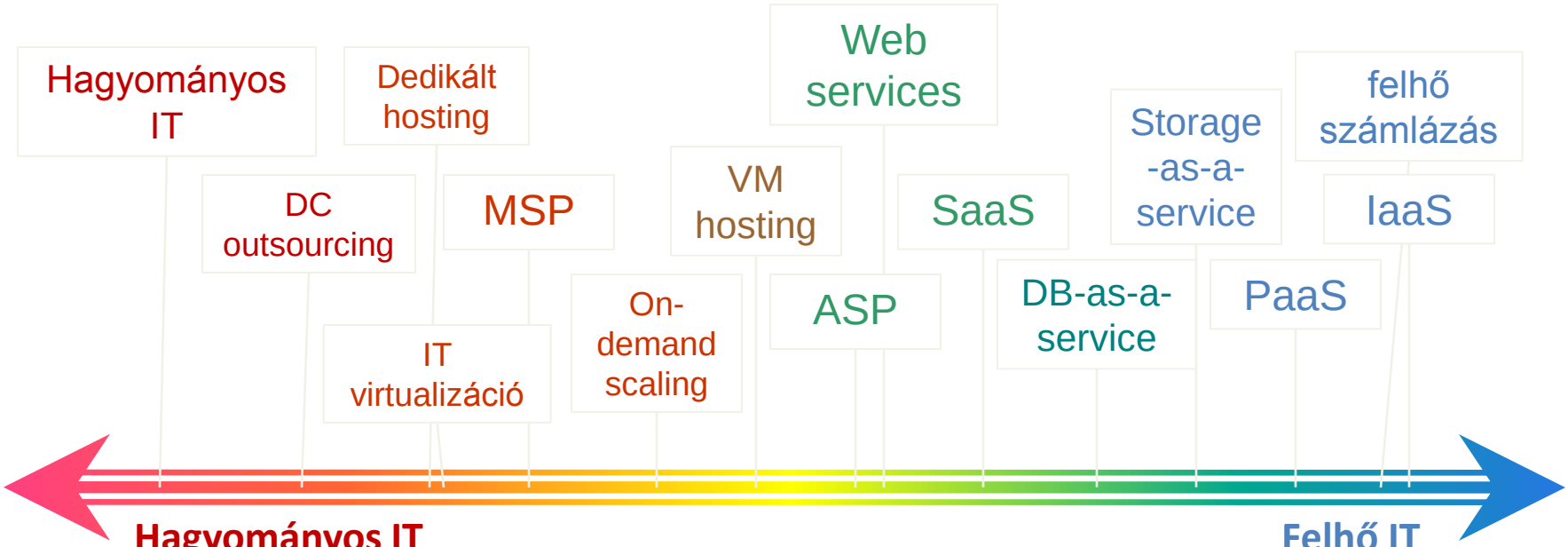
- Dashboard
- Identity Management
- Networking
- Load balancers
- Database
- Queueing



Menedzsment réteg: automatizálás és felügyelet



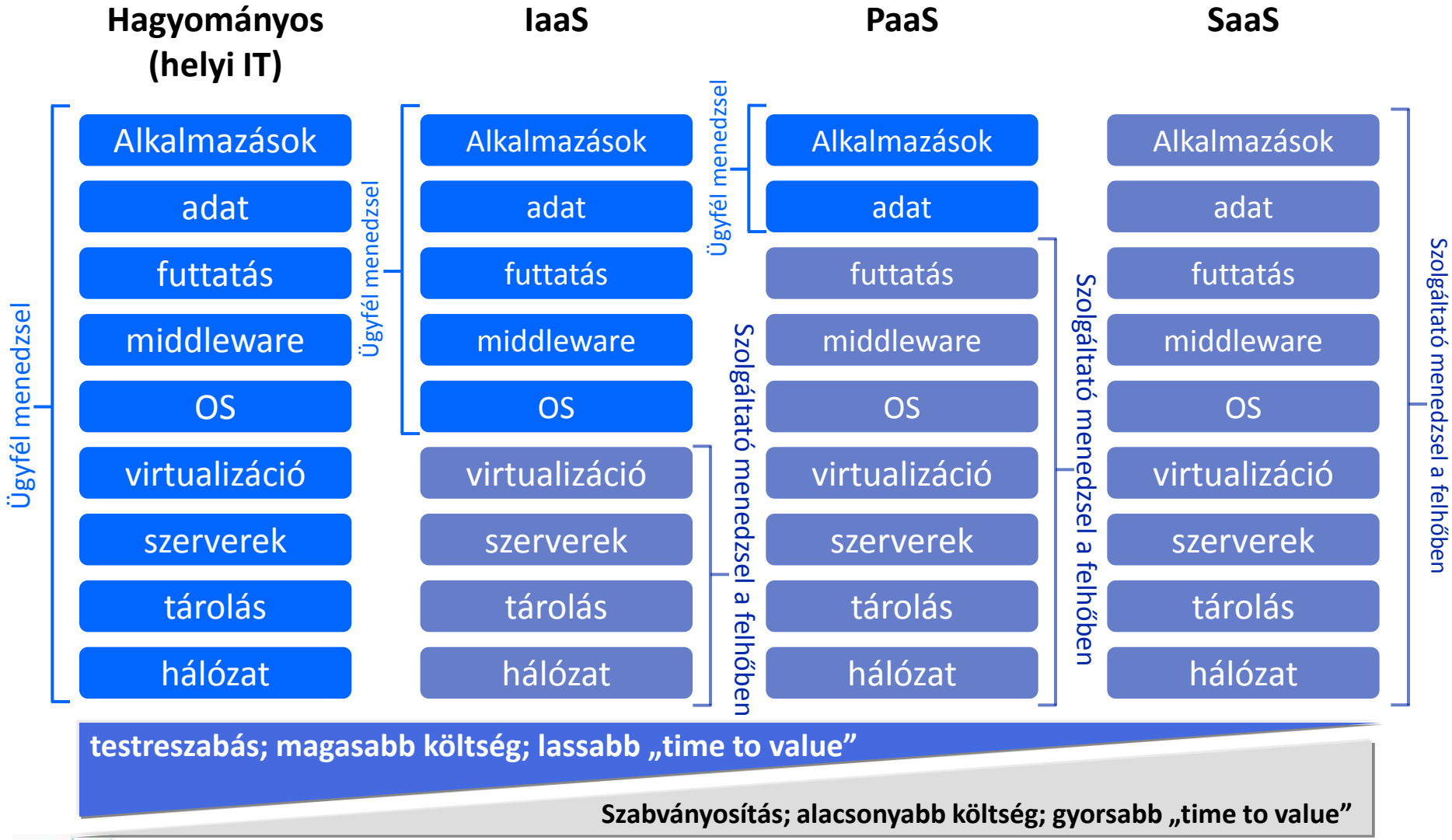
Nem megy minden a felhőbe



Hagyományos IT
- fix költség/feltételek
- változó bevezetés
- egyetlen felhasználó
- több „kézivezérlés”
- testreszabhatóság

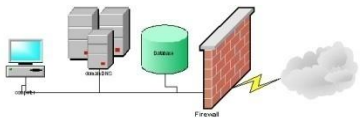
Felhő IT
- változó költség/feltételek
- standard bevezetés
- „társbérlet”
- nagyon automatizált
- korlátozott testreszabhatóság

Az üzleti igényből kell kiindulni



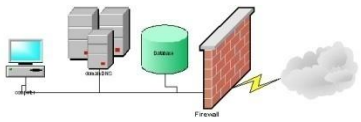
A felhő IT biztonsági előnyei

- Egységes biztonsági politika.
- Automatizált biztonsági eljárások és műszaki megoldások.
- A felhő homogenitása egyszerűbbé teszi az ellenőrzést és az auditálást.
- Redundancia, mentés/helyreállítás.



A felhő IT biztonsági előnyei

- Dedikált biztonsági szakértelem.
- Technológiai naprakészség.
- Nagy(obb) befektetés a biztonsági infrastruktúrába.
- Hibatűrés és megbízhatóság tervezése.
- Valós idejű támadás-észlelés.
- Kapcsolódás biztonsági kezdeményezésekhez.

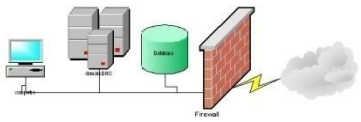


A felhő IT biztonsági kockázatai

Felhő IT = komoly erőforrás koncentráció

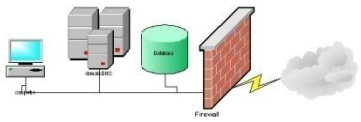
== komoly kockázat-koncentráció

- egy átfogó hiba következményei kiterjedtebbek lehetnek
- az ügyfelek koncentrációja egyúttal veszélyeztetettség-koncentrációt is jelent



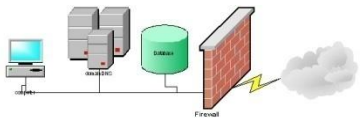
Általában: elosztott rendszerekben nem elegendő csak a jelszó/tanúsítvány autentikáció + az adatátvitel bizalmasságának megőrzése.

- Pl. egy felhő IT specifikus támadás *„csendes”* lehet, nem feltétlenül hagy nyomot az adott node operációs rendszerében.



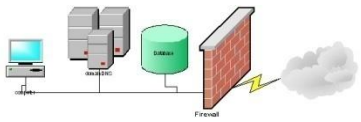
Nem lesz nagy baj, ha …

- a felhő szolgáltató biztonsági politikája legalább olyan erős, mint az ügyfél elvárása,
- a felhő szolgáltató szakemberei jók, felelősségteljesek,
- a web-service interfészek nem hoznak be túl sok sebezhetőséget,
- …



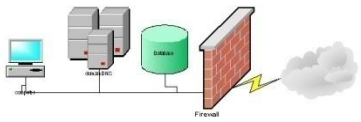
Lehetséges problémák

- tipikus:
  - az ellenőrzés elvesztése
  - bizalomhiány (mechanizmus !)
  - sok bérlő-társ
- A fentiek a nyilvános felhő IT-re vonatkoznak.



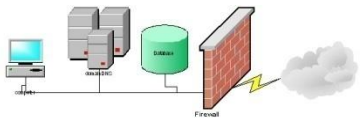
Az ellenőrzés elvesztése

- A felhasználó a szolgáltatóra bízza
  - adatbiztonság, privacy, erőforrás-elérhetőség, monitoring és javítás/helyreállítás
- Az ügyfél elveszítheti az ellenőrzést
  - adatai, alkalmazásai, erőforrásai felett, amelyek (fizikailag) a szolgáltatónál vannak
  - a felhasználók (személy)azonosítása felett
  - a felhasználói hozzáférési szabályok érvényesítése felett



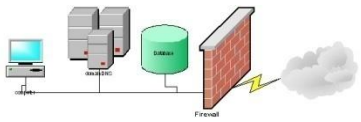
Intézkedések ellenőrzés megtartásához

- monitoring
- különböző felhők használata
- hozzáférés menedzsment



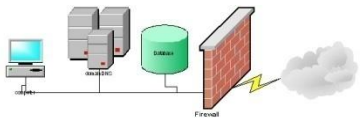
Monitoring

- Az ügyfél-igény pontos azonosítása
  - Mi a teendő egy bizonyos hiba esetén?
  - Visszaállítási mechanizmus (mi a szolgáltató és mi az ügyfél dolga ?)
- Alkalmazás-specifikus run-time monitoring és menedzsment eszköz
  - Az ügyfél is kaphat hozzáférést az eszközhöz
  - Szolgáltató/ügyfél: eltérő nézetek
  - Az ügyfél is beavatkozhat?
    RAdAC (Risk-adaptable Access Control); VM remote portolás másik fizikai host-ra, jog és lehetőség másik felhőbe átmozgatni az alkalmazást



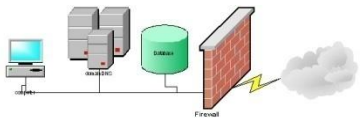
Hozzáférés-szabályozás (Access Control)

- Különböző szintek (pl. hozzáférés a felhőhöz, szerverhez, szolgáltatáshoz, adatbázishoz: közvetlenül/ web services, VM-hez, VM objektumhoz
- Ügyfél-menedzselt hozzáférés
- Autentikáció: végső soron a szolgáltató biztosítja



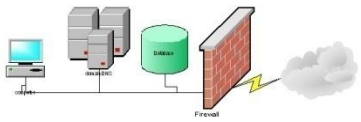
Bizalomhiány

- Definiálni kell a kockázatokat és a bizalmi kérdéseket
  - Különböző érdekei vannak a szolgáltatónak és az ügyfélnek!
  - Ne csak akkor merüljön föl, ha már megtörtént a baj.
- Menedzsment sémák
  - Egyensúlyozni a bizalom és a kockázat között



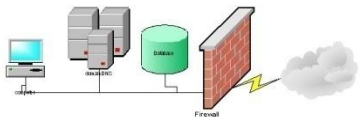
A sok bérlő-társ kérdése

- Konfliktusok lehetősége a bérlők érdekkülönbözőségei miatt
  - minden lehetséges esetre jó együttműködési szabály-rendszer nincs,
  - ha valaki nem „fair” játékos, mit lehet kezdeni vele?
- Egyáltalán: az ügyfelek elválasztásának kérdése is része a felhő üzemeltetési politikának.
  - erős/gyenge elválasztás
  - VPC: az erőforrások azért végesek és megosztottak



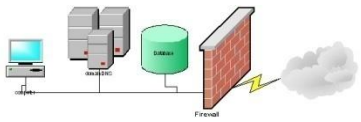
Policy Language

- Standard SLA nyelvezet
  - Géppel értelmezhető (feldolgozható),
  - Kombinálható/összehasonlítható leíró blokkok
  - “a VM-ek elválasztása szükséges”, “a VM-ek fizikai elválasztása szükséges”, stb.
  - Validációs eszköz: az üzemeltetési politika az SLA-ban a létrehozó szándékait tükrözi-e?

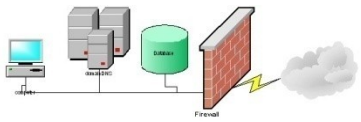


A bizalomvesztés elkerülése: tanúsítványok

- Tanúsítvány (Certification):
  - elismert, független, ellenőrizhető leírása a biztonsági kérdéseknek és a biztosításnak
- Kockázatértékelés
  - third party
  - biztosítási konstrukció alapja is lehet

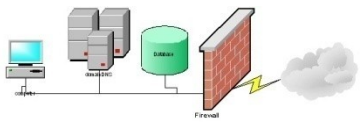


Információs rendszerek üzemeltetése



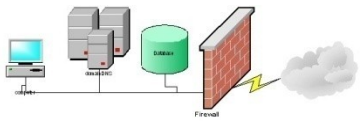
III. rész

Szerverek



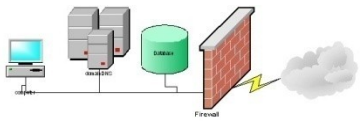
Szerverek

- Termékcsaládok
- Megbízhatóság
- Adatközpontok
- Szerviz szerződések
- Szerver frissítések
- Redundancia



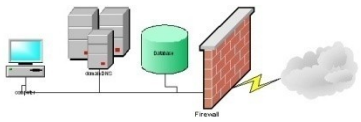
Szerverek - definíció

- A ***kiszolgáló*** vagy ***szerver*** (az angol ***server*** szóból) az informatikában olyan (általában nagyteljesítményű) számítógépet, ill. szoftvert jelent, amely
  - más számítógépek számára a rajta tárolt vagy előállított **adatok** felhasználását,
  - a kiszolgáló hardver **erőforrás**ainak (például nyomtató, háttértárolók, processzor) kihasználását, illetve
  - más **szolgáltatás**ok elérését teszi lehetővé.



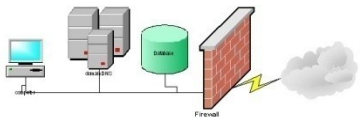
Tipikus termékcsaládok

- Egy számítógép-gyártónak tipikusan három termékcsaládja van:
  - otthoni (home),
  - üzleti (business),
  - szerver (server)



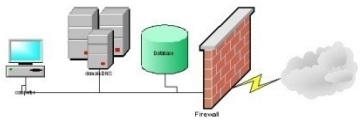
Otthoni termékcsalád

- Az otthoni család jellemzői:
  - legolcsóbb induló ár
  - drága bővítés, kiegészítők
  - a jellemzőit általános terminusokban adják meg
  - gyakran változtatják a beszállítókat, így nincs „két ugyanolyan”
  - sok „játéklehetőség”, nagyfelbontású grafika, audió



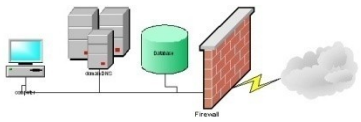
Üzleti termékcsalád

- Az üzleti család jellemzői
  - a teljes „életköltség” minimalizálása (drágább induló ár, de hosszabb élettartam)
  - ritkább változások: drága a cégek számára
    - a sok pótalkatrész raktározása,
    - a változatok oktatása a kereskedők számára



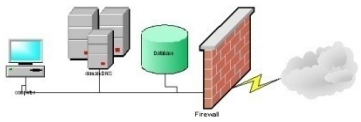
Szerver termékcsalád

- A szerver család jellemzői
  - más architektúra, mint az asztali gépeknél („hosszabb életű” legyen: szabad kapacitás, bővíthetőség)
  - teljesítményhez viszonyított minimális költség
  - könnyen szervizelhető, robosztusabb kivitel, a javítási idő kicsi legyen
  - csatlakozó/kezelőszervek elhelyezésénél a könnyű szervizelhetőséget és nem a helytakarékosságot tekintik elsődlegesnek
  - a megbízhatóság kulcskérdés



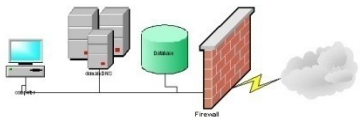
Szerverek hardver jellemzői

- Több belső hely kártyák, CPU-k, meghajtók stb. számára
- Nagyobb CPU teljesítmény: több CPU vagy egy nagyon gyors CPU
- Nagyteljesítményű I/O: a szerverek általában több I/O műveletet végeznek, mint a kliensek (I/O ~ #kliens)
  - nagysebességű I/O alrendszer,
  - nagysebességű belső buszok,
  - nagysebességű hálózati interfészek,
  - RAID technika
- Több upgrade opció
- Rack-re szerelhető kivitel
- Nincsenek oldalsó csatlakozók



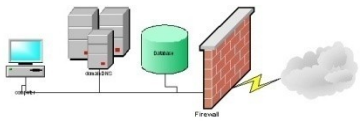
Szerver berendezések

- Egy ***szerver berendezés*** (Server Appliance) egy olyan eszköz, amely egy kitüntetett feladat ellátására jó. Például:
  - Fájl szerver
  - Web szerver
  - E-mail szerver
  - DNS szerver



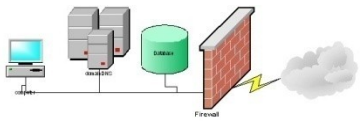
Homogén / heterogén rendszerek

- A szerverek lehetnek
  - homogének (egy gyártótól való/ azonos családból való)
  - heterogének (több, különböző gyártótól/gyártmánycsaládból).
- A homogén rendszerek előnyei:
  - egyszerűbb fenntartás
  - egyszerűbb oktatás
  - egyszerűbb pótalkatrész raktározás (csak egy kell mindenből)
  - könnyebb javítás
- A heterogén rendszerek előnyei:
  - nem “ragadunk be”, ha a szállítóval valami történik
  - minden feladathoz a legjobb berendezést választhatjuk
  - a gyártók közti versenyeztetés miatt olcsóbb beszerzési költség



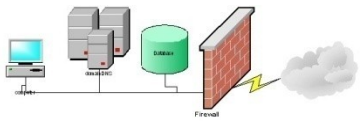
Szerverek megbízhatósága

- Több használó függ tőlük – megbízhatóság kulcskérdés
- Javítási idő kicsi legyen
- Más architektúra, „hosszabb életű”
- Legyen szabad kapacitása
- Szervereknél – a desktopokkal szemben:
  - más elhelyezkedés (data center)
  - karbantartási szerződés
  - diszk mentés
  - más operációs rendszer konfiguráció



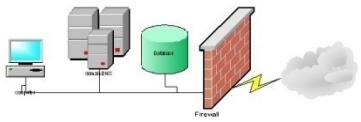
Szerverek elhelyezése

- Védeni kell őket
  - elemi kár
  - elektromos zavarok
  - emberi károkozás ellen
- Védett helyre telepítés elengedhetetlen
  - védett táp (UPS – Uninterruptible Power Supply)
  - hőmérséklet- és páraszabályozás (HVAC - heating, ventilating and air conditioning)
  - tűzbiztosság
  - fizikai védelem (sérülés, illetéktelen hozzáférés ellen)



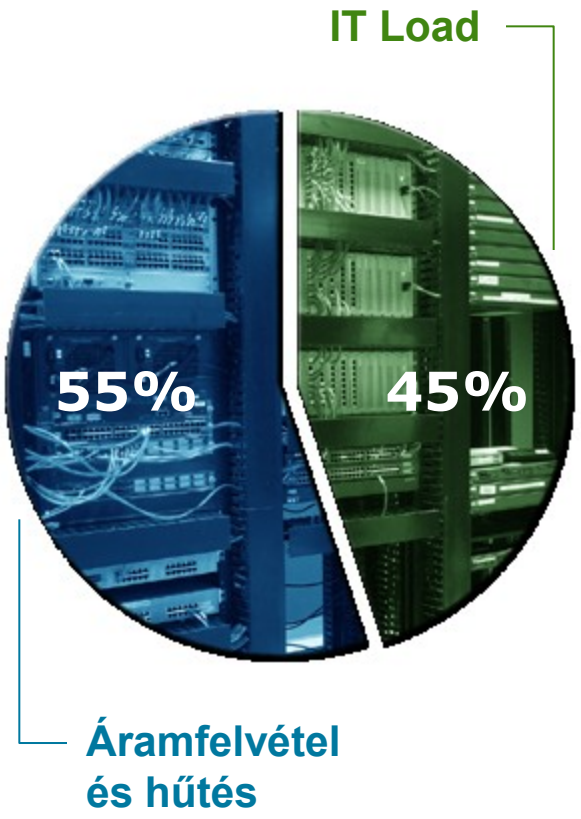
Hogy is néz ki egy tipikus adatközpont energia ellátása?

- Szerintetek az energia hány %-a fordítódik hasznos processzor teljesítményre?



Hogy is néz ki egy tipikus adatközpont energia ellátása?

Data Centre

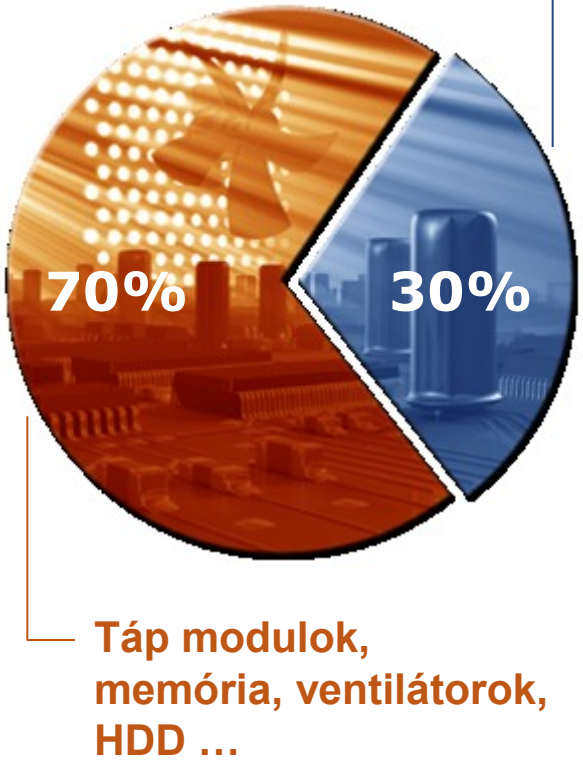


Data source: *Creating Energy-Efficient Data Centres, , U.S. Department of Energy , Data Centre Facilities and Engineering Conference, May 18, 2007*

Hogy is néz ki egy tipikus adatközpont energia ellátása?

Data Centre

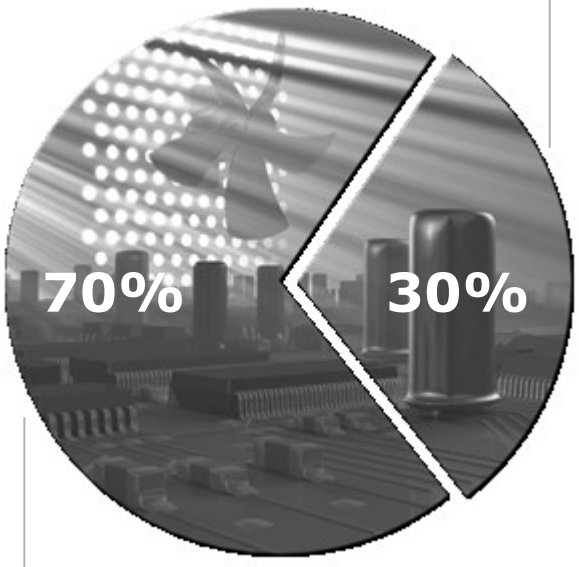
Server hardware



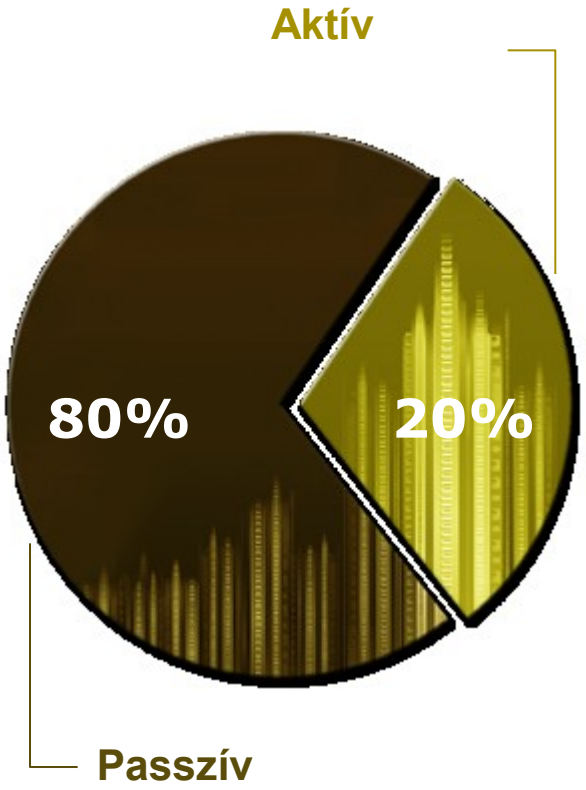
Hogy is néz ki egy tipikus adatközpont energia ellátása?

Data Centre

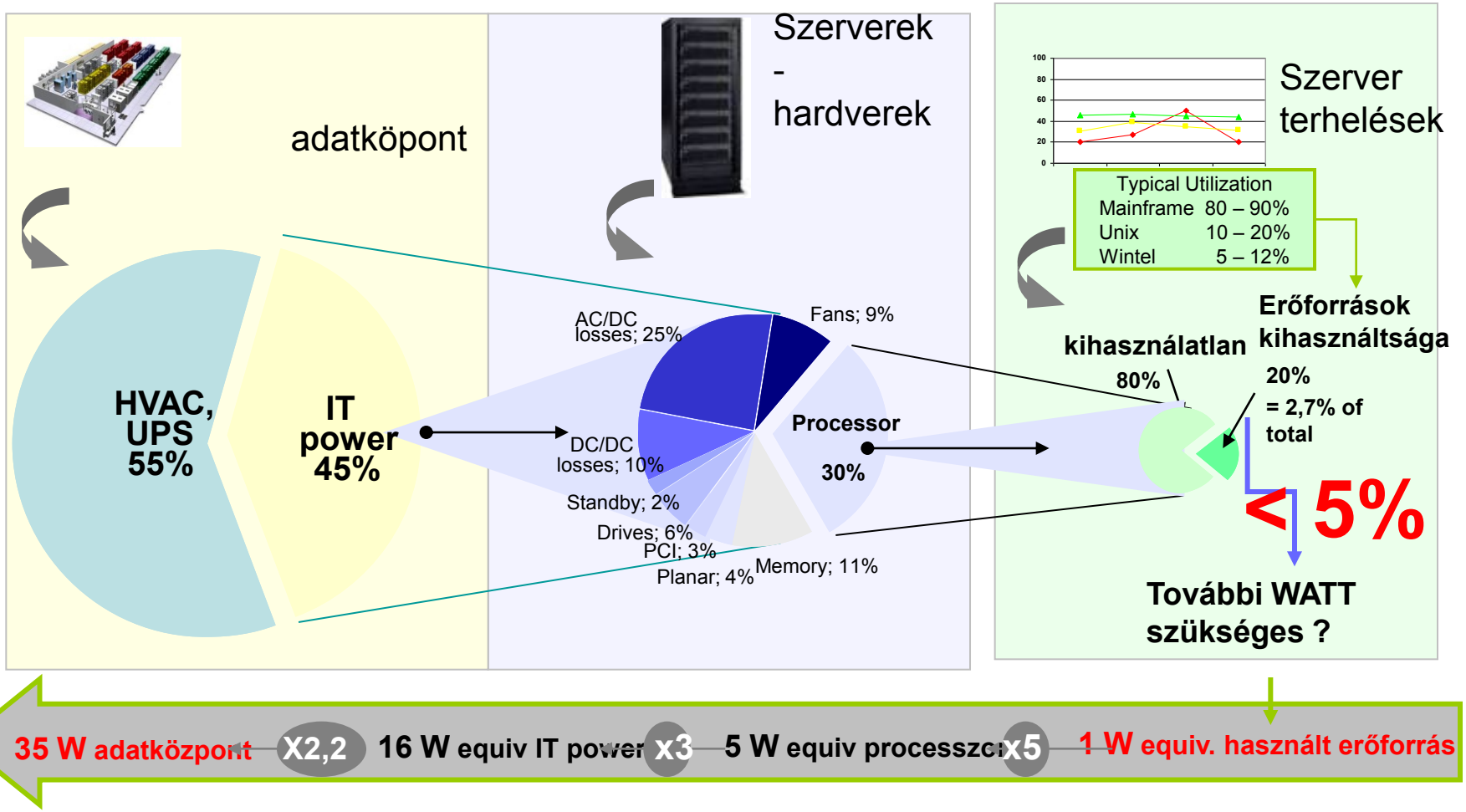
Server hardware



Server loads



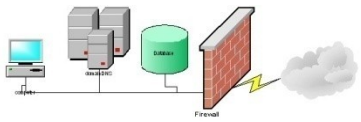
Valós kép az adatközpontok felhasználásáról – hol fogynak a WATT-ok?



Adatközpontok (Data Center)

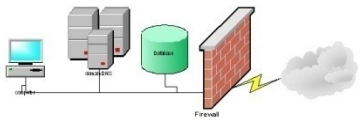
- Saját telephely
- Adatközpontok, szerver hotelek
- Szerver szolgáltatás

- Kihelyezés (Outsourcing)
  - Előnyök
    - gazdaságosabb, speciális szakértelem
  - Hátrányok
    - kiszolgáltatottság



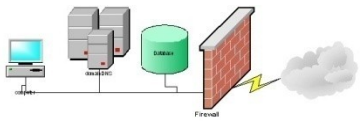
Szerverek végleges elhelyezése

- Operációs rendszer és egyéb szoftverek telepítése ELŐTT a végleges helyükre beállítani
- Ellenkezőleg:
  - akkor bizonyos ideig még a laborban marad a gép, ahol nincs UPS, légkondicionálás stb., ami önmagában zavart, szolgáltatás-kiesést okozhat,
  - nincs megfelelő biztonság, ha már ott van a gép a laborban, „próba” rendszereket telepítünk rá (akár különben jogosulatlan használók is)
  - amikor aztán a végleges helyére visszük, ez alatt az idő alatt BIZTOS, hogy szolgáltatás-kiesés van!



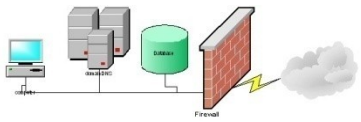
Szerviz (maintenance) szerződések

- Szerver vásárlásakor gondolnunk kell a szervizelésre is
- Többféle lehetőség közül lehet általában választani:
  - 4 órás,
  - 12 órás,
  - 1 napos szerviz,
  - csak tartalék alkatrész biztosítása, amit felhasználás után pótolnak



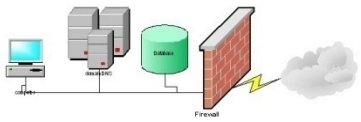
Szerviz szerződések - példák

- Kicsit/közepesen kritikus host:1-2 napos szerviz, vagy egyáltalán semmi
- Azonos szerverek nagy csoportja: ált. elegendő a tartalék alkatrész
- Vezérelt modellválasztás: Az a cél, hogy mindig csak két típus legyen
- Kritikus szerver: túl drága lehet komplett készletet tartani, ezért csak a kritikus elemekből tároljunk + 1 napnál rövidebb kiszállási idejű szerviz
- Azonos gyártó sokfajta modellje:
  - nagyon nagyszámú szerver esetén állandó technikus
  - közepes méret esetén regionális raktárból telefonhívásra szerelő küldés is
- Nagyon kritikus host: állandó technikus + duplikált gép (nem technikai jellegű cégek esetén ez adhatja a legnagyobb biztonságot)



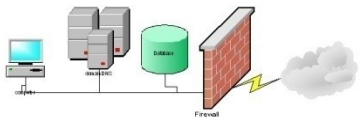
Pótalkatrészek helyi tárolása – Szerviz szerződés

- Kompromisszum kell a pótalkatrészek helyi tárolása (1) és a szerviz szerződés (2) között
  - (1) Drága lehet kis cégek számára,
  - (2) Általában (táv)diagnosztikai szolgáltatásokat is magában foglal.
- Ált. legjobb, ha a hibás alkatrészt azonnal kicseréljük és utána vizsgáljuk.



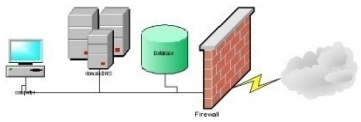
Szerviz szerződések megkötése

- Sokszor baj esetén derül ki, hogy egy gépre nincs érvényes szerviz szerződés. Ennek elkerülésére:
  - jó leltározó/nyilvántartó program
  - ha a beszerzést intéző személy egyben a szervizszerződések kötéséért is felelős
  - garancia ideje alatt is élő szerviz szerződés, csak a garancia idejére 0 Ft-os díjjal



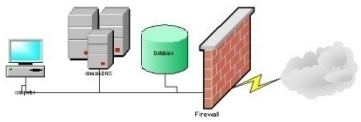
Adatmentések (Data Backup)

- Elmélet:
  - A klienseken tárolt adatokat nem mentjük. Ezért célszerű, ha a használók adataikat a szerveren tárolják – annak tartalmát ugyanis mentjük. Így nincs is szükség a helyi adatok mentésére.
- De:
  - különösen Windows alapú rendszereknél egy csomó személyes beállítás, konfigurációs fájl, utólag letöltött program helyben tárolódik. (Megoldható, hogy kijelentkezéskor a beállításokat a szerverre mentsük, de ez nem teszi feleslegessé a helyi tárolást!)



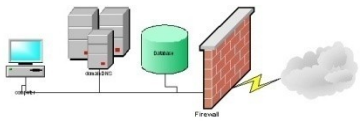
Adatmentések (Data Backup)

- A szervereken tárolt adatokról biztonsági másolatokat készítünk
  - hiba esetén helyre lehessen állítani az adatokat (egy nem túl régi állapotnak megfelelően)
  - archiválási célokra
- Ezekről a kérdésekről később részletesen, egy külön fejezet keretében beszélünk majd



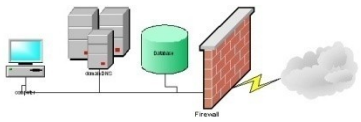
A szerverek és a kliensek operációs rendszere

- Különbözők
  - Pl. web szerver esetén a kliens és a szerver operációs rendszere teljesen eltérő lehet, csak a kommunikációs protokollt kell mindkettőnek tudnia futtatni.
- Azonosak (teljesen vagy más beállításokkal)
  - Unix CPU szerver / Unix desktop környezetben a szerver/kliens operációs rendszere azonos kell legyen, csak különböző beállításokkal.



Külön adminisztrációs hálózat

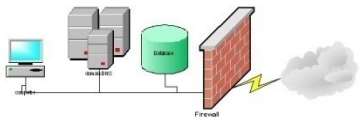
- Célszerű speciális, adminisztrációs hálózatot fenntartani mentésekre és monitorozásra.
- A mentések nagy mennyiségű adat átvitelét igénylik (jelentősen) csökkentve a használói sávszélességet.
- A külön adminisztratív hálózat egyszerűbb és így hibatűrőbb elemekből épülhet fel
- Független a külső hálózat esetleges hibájától!
  - monitorozás esetén nem ad a hálózati hiba miatt rossz mérési eredményt
  - hálózati hiba esetén is van lehetőség a gépekhez való hozzáférésre



Távoli kezelői hozzáférés

(Remote Administration Access)

- Régen: minden szerverhez külön billentyű + monitor
- Ma: konzol szerver
- Előny:
  - Helynyereség
  - Beavatkozások egy (távoli) helyről végezhetők
- Távolról vezérelhető tápegységek



Szerver frissítések (Server Upgrades)

A feladat:

Adott kiinduló helyzet:

– Működő szolgáltatásokat biztosító szerver

– Frissítő csomagok(ok)

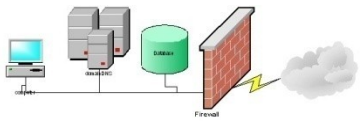
- valamely szolgáltatás(ok)hoz, vagy
- az operációs rendszerhez

Elvárt végeredmény:

– A kívánt szoftverfrissítések

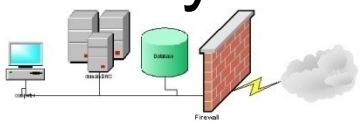
- felkerülnek a szerverre és
- aktiválódnak ott;

– A szerver elérhető, minden szolgáltatás megfelelően működik



A megoldáshoz vezető út

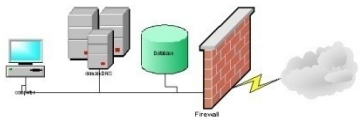
1. Feladatlista-készítés
2. (új) szoftvercsomagok kompatibilitása az (új) OS-sel…?
3. Ellenőrző teszt minden szolgáltatáshoz
4. Visszakozz-terv készítés
5. Karbantartási időszak
6. A frissítés hirdetése a felhasználók között
7. Ellenőrző tesztek futtatása
8. **Frissítés elvégzése**
9. … Ha nem sikerül: visszakozz
10. Az eredményt tudatjuk a felhasználókkal



1. A feladatlista elkészítése

A kérdések:

- Milyen szolgáltatásokról van szó?
- Kik a felhasználók?
- Milyen szoftvercsomagok az érintettek?



A feladatlista (folyt.)

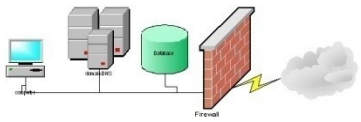
Mi a feladatlista (checklist)?

Funkcionálisan:

- terv / forgatókönyv / leírás
- mit nem akarunk elfelejteni megtenni

Fizikailag:

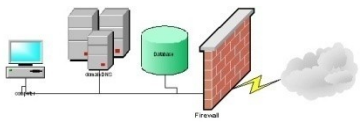
- fehér papír
- négyzetrácsos papír
- vonalas papír
- Weboldal
- Excel tábla
- stb…



Egy ***egyszerű*** feladatlista (példa)

CVW Server and Document Server (3.0 to 3.2)

- Shut down the CVW Server and Document Server
- Retain a backup copy of the CVW Server dir by moving a copy to /opt/CVWserver.old
- Create a new CVW Server directory (/opt/CVWserver)
- If the directory path to the doc-store has changed, correct the paths in the doc-store/index.db file
- Install the new CVW Document Server in /opt/CVWserver
- Modify the cvwds.boot startup script with custom settings and copy to /etc/init.d/cvwds, then link to /etc/rc3.d/S99cvwds
- If upgrading from 3.0, upgrade the CVW database using the updater program and copy the resulting DB file to /opt/CVWserver
- Modify the cvw.boot startup script with custom settings and copy to /etc/init.d/cvw, then link to /etc/rc3.d/S99cvw
- Set file permissions
- Test CVW Server operation with telnet
- If upgrading from 3.1, apply the 31to32_patch.txt file to your DB using the Tk client
- Test CVW Document Server operation with web browser
- Archive /opt/CVWserver.old



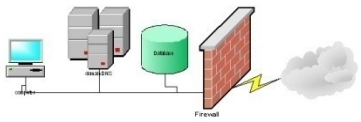
A feladatlista (folyt.)

Ki olvassa el valóban az érintettek közül?

- Alig valaki…

Emiatt proaktívan végig kell vezetni őket:

- Megfelelőnek tartják?
- Kérdésekkel felszínre hozni az igazi részleteket.
- Ettől máris meg fog változni a megfelelőség…

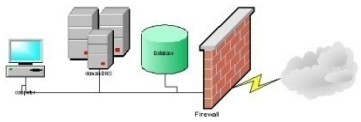


A feladatlista (folyt.)

Mi van a gépen?

- Rejtett függőségek feltárása
  - Szoftvercsomagok közötti függőségek
  - Érintett felhasználói csoportok
  - Más eszközök / szerverek függősége
  - Szoftvercsomagok amelyek nem jelennek meg a függőség-listán (**feleslegesek!**)
- A függőségek dokumentálása

  -> feladatlista tökéletesítése



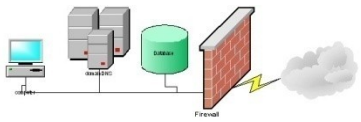
2. A SW kompatibilitás ellenőrzése

Információszerzés:

- Terméktámogatói honlap
- Kapcsolatfelvétel a gyártókkal
  - aktív kérdések
- Korábbi tapasztalatok (másoké is)
  - pl. Internetes fórumok

Információk ellenőrzése tesztgépen:

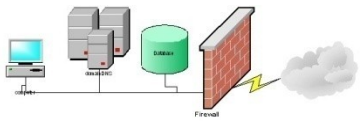
- Kevés felhasználós, nem-kritikus alkalmazásnál: kihagyható
- Kritikus, sok felhasználót érintő szolgáltatásnál: létfontosságú



SW kompatibilitás ellenőrzése (folyt.)

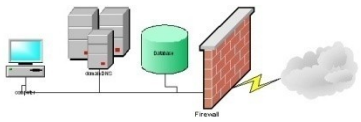
- Ha a SW-t az új OS nem támogatja:
  - Olyan változatra frissítünk, amit még/már támogat az új és a régi OS is
- Ha a SW-t csak az új OS támogatja:
  - Csak az új OS-sel lehet tesztelni (tesztgép !!)
- Ha a SW-t az új OS végképp nem támogatja:
  - a felhasználókat győzzük meg: nem kell a SW,

  vagy…
  - el kell tekinteni az OS frissítéstől



3. Ellenőrző tesztek

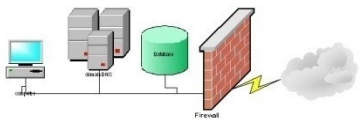
- Minden szolgáltatást teszteljünk az új OS-sel
- Automatikus tesztek (szkriptek)
  - Szolgáltatás elindítása
  - Szolgáltatás működése (ellenőrző pontok)
  - Teszteredmények naplózása (OK / NOK)
- Manuális tesztek
  - Szúrópróbaszerűen az auto-tesztek mellett
  - GUI-t csak manuálisan lehet tesztelni
- Regressziós teszt
  - Ugyanolyan kimenetet ad-e az új rendszer, mint a régi adott?
  - Apró eltéréseket (verziószám, dátum) el lehet/kell fogadni



4. A visszakozz-terv

- Ha nagyon nem a tervek szerint haladunk
  - Az eredeti állapot visszaállítandó
  - A visszaállás sikerét is tesztelni kell
- A visszaállítást is meg kell tervezni előre
  - Teendők listája
  - Elvégzéshez szükséges idő
- Frissítésre szánt idő=

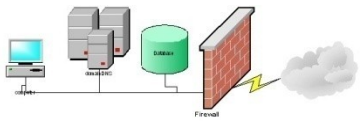
  Karbantartási idő – visszakozz-idő – sikerességi teszt
- A visszaállítás forrása
  - Kis- és középméretű rendszer: klónozás
  - Nagy rendszer: *inkrementális (/ differenciális) backup*



5. A karbantartási időszak

- Mikor legyen?
  - A felhasználóknak nem jó, ha munka közben van leállás karbantartás miatt
  - A rendszergazda nem akar mindig éjjel/hétvégén dolgozni
  - Ha karbantartás alatt gond van, a termék-supportot is el kell tudni érni

…*kompromisszum*…



Karbantartási időszak (folyt.)

- Meddig tartson?

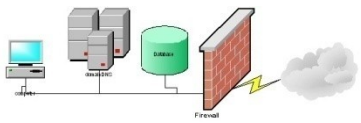
Karbantartási idő =

(Frissítési idő +

Teszt idő +

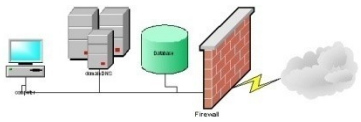
Visszakozz-idő +

Visszakozz-teszt idő) * [2..3]



Példa

- Háromfős IT csapatával egy rendszert üzemeltet, amelyben 4 szerver és 30 desktop gép van. A vezetés rossz pénzügyi politikája miatt a rendszer nem redundáns.
  - Három kilences rendelkezésre állást feltételezve, éves átlagban (egy év 31 536 000 másodpercből áll) mennyi ideig megengedhető, hogy ne működjön a rendszer?
  - Tervezetlen leállás nincs a rendszerben. Ez esetben mekkora a negyedéves szerver-karbantartási ablak?
  - A legkomplexebb szerveren a frissítési idő 20 perc. A régi rendszer visszaállítása 15 percet vesz igénybe. A rendszer akármilyen állapotban történő tesztelésére 10 perc kell.
    - Mennyi időt tervez ennek a szervernek a karbantartására?
    - Ha látszik, hogy nem sikerül a frissítés, mikor kezdi a visszakozzt?

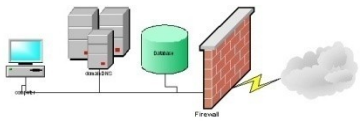


Megoldás 1.

- Három kilences rendelkezésre állást feltételezve, éves átlagban (egy év 31 536 000 másodpercből áll) mennyi ideig megengedhető, hogy ne működjön a rendszer?

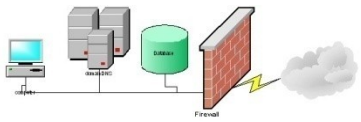
- Három kilences rendelkezésre állás = az idő 99,9%-ában jó, 100% - 99,9%-ában (0,001) rossz.

- 31 536 000 * 0,001 = 31 536 másodperc (~ 8 és ¾ óra)



Megoldás 2.

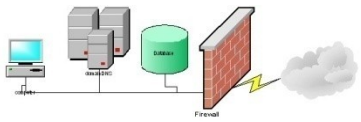
- Tervezetlen leállás nincs a rendszerben. Ez esetben mekkora a negyedéves szerver-karbantartási ablak?
- Nincs tervezetlen leállás -> az előző pontban kiszámolt a *tervezett* leállás (karbantartás) egy évben
- Negyedéves: 31 536 / 4 = 7884 másodperc
  (~ 2 óra 11 perc)



Megoldás 3.

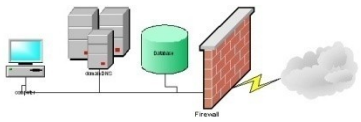
- A legkomplexebb szerveren a frissítési idő 20 perc. A régi rendszer visszaállítása 15 percet vesz igénybe. A rendszer akármilyen állapotban történő tesztelésére 10 perc kell.
  - Mennyi időt tervez ennek a szervernek a karbantartására?

- 20 perc update + 10 perc teszt + 15 perc visszakozz + 10 perc teszt = 55 perc - szorozva 2..3 közötti számmal, a biztonság kedvéért.
- De maximum a karbantartási ablak (2 óra 11 perc)!



Megoldás 4.

- A legkomplexebb szerveren a frissítési idő 20 perc. A régi rendszer visszaállítása 15 percet vesz igénybe. A rendszer akármilyen állapotban történő tesztelésére 10 perc kell.
  - Ha látszik, hogy nem sikerül a frissítés, mikor kezdi a visszakozzt?
  - A karbantartási ablak vége előtt 15 perc (visszakozz) + 10 perc (teszt) = 25 perccel

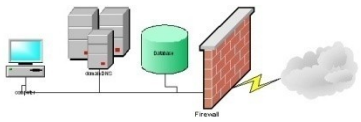


6. A frissítés / karbantartás hirdetése

- ***Figyelemkeltő módon***

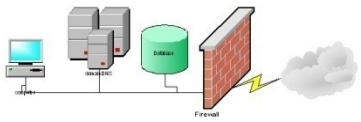
- Formálisan (vegyék komolyan)

- Választandó „média”
  - az adott helyen megszokott, elfogadott
  - pl. célratörő kör-email



7. A tesztek végrehajtása

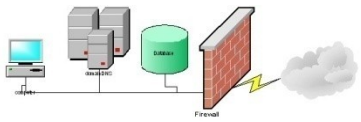
- A karbantartás elkezdése előtti utolsó lépés
- A működő rendszeren elvégezzük az előírt teszteket
- Javítjuk a tesztek hibáit



8. A frissítések elvégzése

- Maga Az Éles Feladat

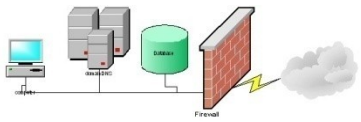
- Felügyelet mellett végezzük
  - A tapasztalatok könnyebben megoszthatók
  - Elakadás esetén könnyebb a továbblépés



9. A frissítések tesztelése

- A korábban megtervezett teszteket az új rendszeren is végrehajtjuk

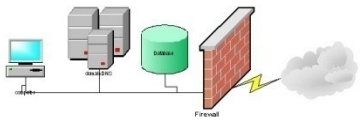
- A további lépések a tesztek kimenetelétől függnek
  - minden OK
  - apró módosítások kellenek
  - visszakozz



10. Ha minden borul: visszakozz

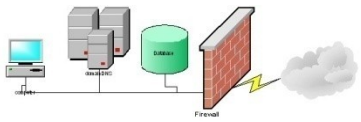
- Nézzük az órát
- Ha elérkezik az idő, nincs mese, el kell kezdeni a visszakozz-terv végrehajtását
- Lehet, hogy nem kell teljes visszakozz
  - Felhasználókkal konzultálva kiderülhet:

    adott szolgáltatás időszakos/végleges elérhetetlensége mégsem tragédia



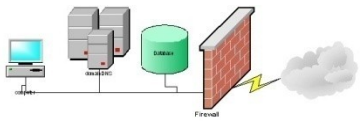
11. A karbantartás eredményének kihirdetése

- Hirdetni kell, hogy
  - az eddig elérhetetlen szolgáltatások újra működnek
  - mi az, ami változott
  - ha valamit mégsem találnak rendben, jelezzék
    - milyen módszerrel?!



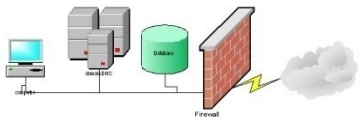
További tippek/trükkök

- Több szolgáltatás hozzáadása/leszedése ugyanabban az időszakban
- Friss install
- A tesztek újrahasznosítása
- Változáslista
- A begyakorlás fontossága
- Minimális változtatások az alaprendszeren



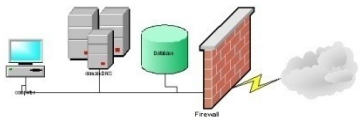
Több szolgáltatás frissítése egy időben

- Komplikált; de ha szükség van rá: tegyük
- Szolgáltatások hozzáadása:
  - a korábban említett problémák
  - Megoldás:
    - Feladatlista
    - Kompatibilitás-kezelés
    - Tesztek, tesztek, tesztek
    - Visszakozz-terv



Több szolgáltatás levétele egy időben

- Amire figyeljünk:
  - Minden használó ki legyen lépve
  - Ha nem használnak valamit, lehet, hogy nincs is rá szükség:
    - Eltávolítás előtt adott ideig (pl. 1 hónap) deaktiváljuk
  - A deaktivált szolgáltatást egy idő után el kell távolítani (ne feledjük…)

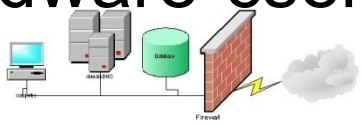


Friss install

– Egy friss install *lehet*, hogy
  » jobb,
  » gyorsabb,
  » biztonságosabb,
  mint a frissítés.

Megoldások:

- Kis luxus: Klónozás
- Nagy luxus: Teljesen új rendszeren végezzük (és hardware-cserebere!)

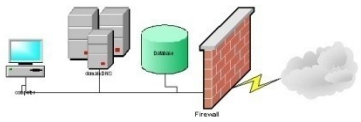


A tesztek újrahasznosítása

Azért sem érdemes a kézi tesztelgetésnél maradni, mert

- Egy jól megírt tesztsorozat
  - máskor is segít,
  - máshol is segít

… pl: a szolgáltatás-monitorozásban

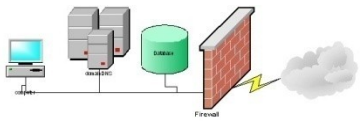


Változáslista

- Minden változást, frissítést

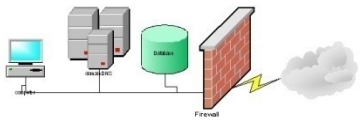
  dokumentálni kell

Jó, ha a változáslista az érintett gépen is elérhető.



Gyakorlás, gyakorlás, gyakorlás

- Minél jobban rákészülünk, annál jobban sikerül az éles módosítás
- Egy jó gyakorlás során … akár egy új rendszer is előállhat
- Az érdekelt felek együtt végiggondolják a tennivalókat
  - Ezalatt nagyon sok minden tisztázódik

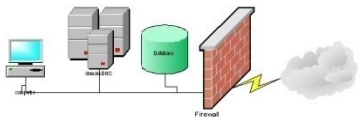


Minimális változtatások az alaprendszeren

- Kezeljük külön
  - A rendszer-partíciót
  - Az alkalmazás-partícióktól

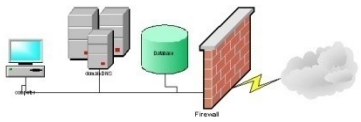
Ha ez nem lehetséges, akkor legyen jól áttekinthető a könyvtárszerkezet:

megkönnyíti a fenntartást/karbantartást



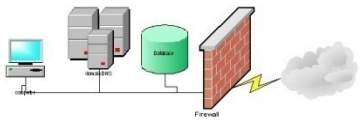
Redundancia biztosítása

- Diszk tárolási redundancia (RAID)
- Redundancia a komponensekre
- Redundáns tápellátás
- Melegtartalék komponensek



Teljes és n+1 redundancia
(Full and n+1 Redundancy)

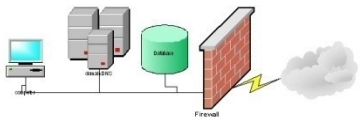
- n+1 redundancia: ha EGY komponens meghibásodik, az egész rendszer még működőképes marad.
- Teljes redundancia: mindenből kettő van + egy hibadetektáló algoritmus (vagy ember), aki szükség esetén átkapcsol.
  - Egyik komponens működik, és ha az meghibásodik, átkapcsolnak a másikra manuálisan vagy automatikusan
  - Terhelésmegosztás. Mindkét elem kb. fele terheléssel dolgozik, de mindkettőnek van annyi szabad kapacitása, hogy szükség esetén a teljes forgalmat átvegye.
- n>2 esetén az n+1 redundancia olcsóbb a teljesnél.
- Gyakran nem az egész rendszer, hanem csak bizonyos részei n+1 redundánsak



Redundáns tápellátás

(Redundant Power Supply)

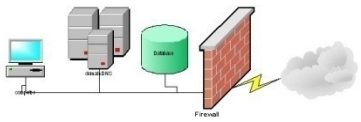
- Tápellátás: a második leggyakrabban meghibásodó elem
- n+1 redundancia
- Minden tápnak saját kábele kell legyen
  - Rossz csatlakoztatás problémája
  - Áthelyezhető leállítás nélkül
  - Megbízhatóság növelése – minden kábel más áramforrásról



Melegtartalék komponensek

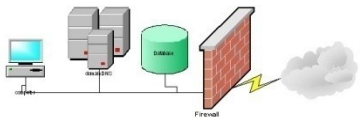
(Hot-swap Components)

- Általában: komponens eltávolításakor, cseréjekor le kell állítani a rendszert
- Melegtartalék: a rendszer ilyenkor is működőképes marad – de sokszor a csere „ráér” a tervezett karbantartásig
  - dupla hiba (risk of double failure)
- Igazi előny: meghibásodáskor
  - RAID
  - n+1+1 redundancia



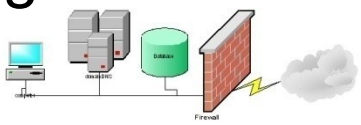
Melegtartalék - problémák

- Mely részek ilyenek és melyek nem?
- Mennyi ideig tart az átkapcsolás és eközben mi sérülhet?
- Mennyi ideig és hogyan (esetleg csökkentett teljesítménnyel?) üzemelhet a rendszer
- Sokszor melegtartalékosnak hirdetnek egy rendszert, de esetleges bővítése reset-et kíván...
- Azaz a melegtartalék nem szünteti meg mindig a leállást, az csak csökkenti annak kockázatát!

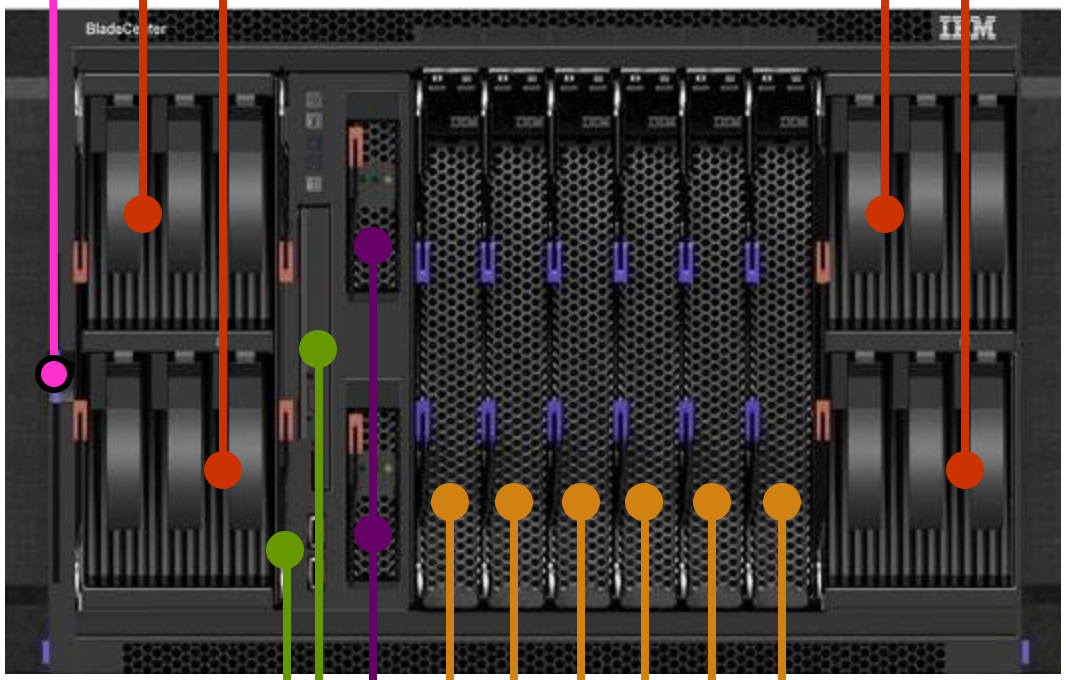


Példa redundanciára

- Megbízhatóság
  - Redundáns diszk (RAID)
  - Redundáns tápegységek
  - Redundáns hűtés
  - Minden I/O kapcsolat redundáns
  - Megkettőzött kapcsolómodulok
  - Redundáns buszok, diszk csatlakozók
  - Megkettőzött menedzsment modulok
- Rendelkezésre állás
  - Menedzsment modul figyeli a komponenseket
  - Kiterjedt Predictive Failure Analysis
  - Hibalogok



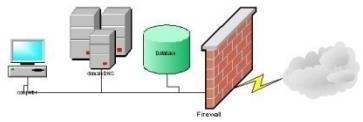
Szerver előlap



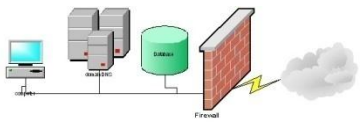
Szerver hátlap

Szerverek - összefoglalás

- Termékcsaládok
- Megbízhatóság
- Adatközpontok
- Szerviz szerződések
- Szerver frissítések
- Redundancia

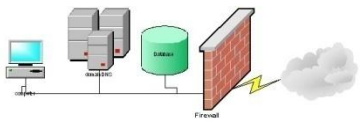


Információs rendszerek üzemeltetése



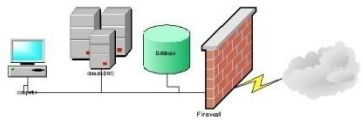
IV. rész

Személyes gépek



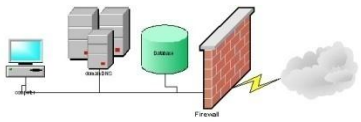
Személyes gépek

- Típusok
- Példa: operációs rendszer telepítése
- Desktop management
  - feladatai részletesen



Asztali / személyi számítógép

- Asztali gép (desktop)
- Személyi számítógép (PC)
- Újabb megoldások
  - Dokkoló (noteszgép – laptop)
  - Digitális személyi asszisztens (PDA)
  - Okostelefon (smartphone)
- ***Személyi végberendezés***, személyes gépek

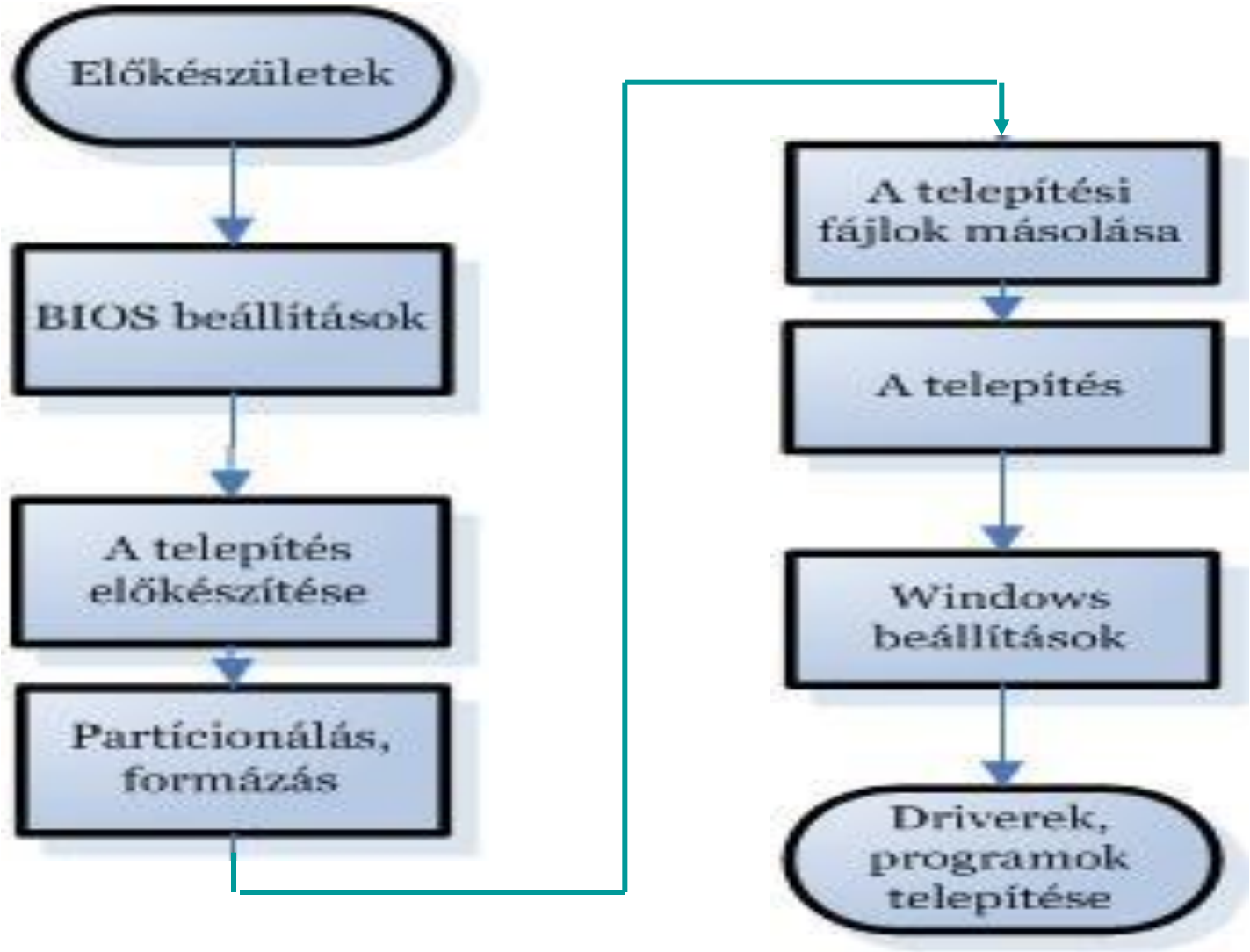


PDA

Első PDA (AT&T EO440) 1993

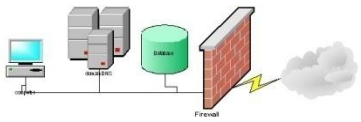
Okostelefon - Smartphone

Operációs rendszer telepítése - áttekintés



Személyes gépek telepítése nagyvállalati környezetben

- Képzeljük el az előző folyamatot alkalmanként több tucat – több száz gépen
  - lassú
  - sok hibaforrás
- Ráadásul:
  - különböző felhasználói csoportok
  - különböző programok
  - különböző ***felhasználói profilok***
- Automatizálni kell…

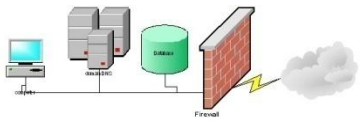


Személyes gépek – operációs rendszer

- Sokszor: előre telepített operációs rendszer
  - Problémaforrás: nem tudhatjuk *pontosan* mi is van telepítve…
  - ált. nem egyszerre vásároljuk, hanem folyamatosan
  - hirtelen cserére szoruló gép
  - szervezet bővülése/átalakítása miatti vásárlás

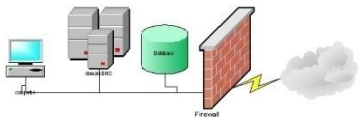
- Nem homogén a gép ill. operációs rendszer állomány – problémaforrás!

- De nem biztos, hogy elérhető a homogenitás „házi” telepítéssel sem ☹



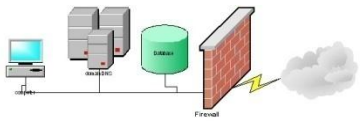
Menedzselés - automatizálás

- A rendszerszoftver későbbi menedzselését is automatizálni célszerű
  - Hálózatba illesztés
    - IP cím, protokollok, jogosultságok
  - Szolgáltatások elérése
    - nyomtatás, levelezés, Internet elérés, stb.
  - Egyéb feladatok
    - postafiók kezelés; vírus, spam, kémprogram elleni védelem; távoli tárhely elérés

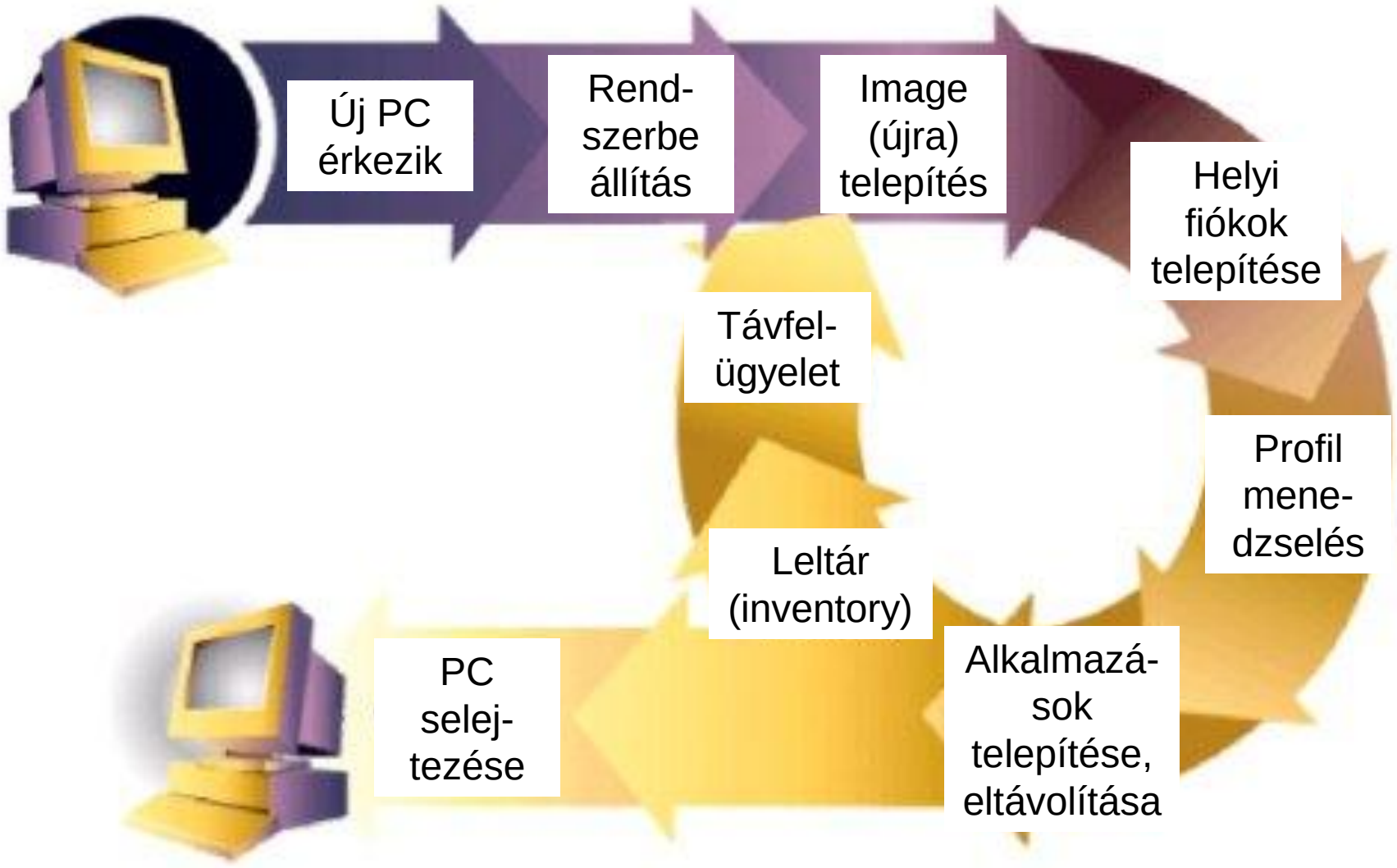


Menedzselési feladatok

- A személyes gépek menedzselése tehát többféle feladatot ölel fel:
  - operációs rendszer és az alkalmazások telepítését, frissítését,
  - ezek mentését és/vagy archiválását,
  - az adott szervezetben egységes („belső szabvány szerinti”) felhasználói felület kialakítását
  - gépek leltározását.
- Minél kevesebb emberi munkával, minél inkább automatizált módon végezzük el.
  - gazdaságosabb
  - csökkenti az emberi hibából vagy mulasztásból származó károkat.
- A személyes gépek menedzselése: ***Desktop Management***.

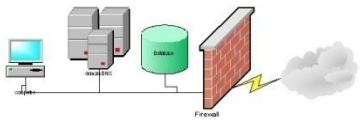


PC életciklus, menedzselési feladatok



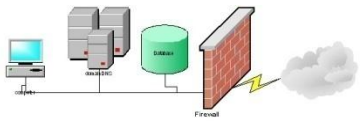
Desktop management szolgáltatások

- Rendszerkép (system image) készítés, automatikus géptelepítés
- Személyre szabott szoftver telepítés, alkalmazás felügyelet, szoftverhasználat mérése
- Különböző irányelvek menedzselése (policy management)
- Távoli felügyelet
- Teljes körű szoftver és hardver leltár (inventory)



Desktop management szolgáltatások

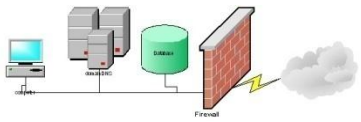
- ***Rendszerkép (system image) készítés, automatikus géptelepítés***
- Személyre szabott szoftver telepítés, alkalmazás felügyelet, szoftverhasználat mérése
- Különböző irányelvek menedzselése (policy management)
- Távoli felügyelet
- Teljes körű szoftver és hardver leltár (inventory)



Rendszerkép-készítés, automatikus géptelepítés

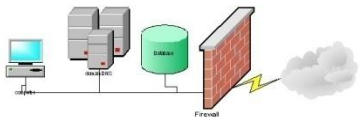
- Rendszertelepítés
  - image-file (rendszerkép)
  - mintatelepítés utáni disztribúciója

- Összerendelések az „Alkalmazás”-objektumok és a munkaállomások között
  - A frissítéseket egyetlen helyen kell elvégezni, a címtár „Alkalmazás”-objektumában
  - Az „Alkalmazás”-objektum használói azonnal a friss változatot használhatják



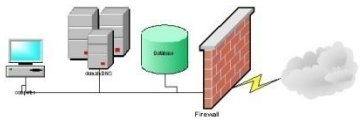
Rendszerkép-készítés, automatikus géptelepítés

- „Wake On LAN”-funkcionalitás támogatása
- Az alkalmazások automatikus továbbítása
  - akár egyszerre több felhasználó számára
  - személyre szabottan
  - feltétel alapú (pl. elfér-e...)
  - rendszerképek továbbítása rendszerindítás előtti szolgáltatással
  - automatizált online alkalmazás-telepítési funkció
    - közben dolgozhatunk a gépen
  - Réteges elektronikus terjesztési ügynökprogramok
    - egy központi pontból több telephely több szerverére
    - onnan a helyi gépekre



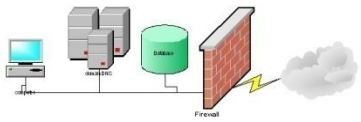
Desktop management szolgáltatások

- Rendszerkép (system image) készítés, automatikus géptelepítés
- ***Személyre szabott szoftver telepítés, alkalmazás felügyelet, szoftverhasználat mérése***
- Különböző irányelvek menedzselése (policy management)
- Távoli felügyelet
- Teljes körű szoftver és hardver leltár (inventory)



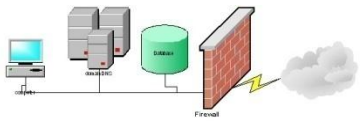
Személyre szabott szoftver telepítés

- A személyre szabható adatok körébe például az alábbiak tartoznak:
  - Mely alkalmazásokhoz fér hozzá a felhasználó
  - Hogyan néz ki az felhasználó asztala (háttér, képernyővédő stb.)
  - Mit állíthat be a felhasználó
  - Ki férhet hozzá távolról az egyes PC-khez és milyen jogosultságokkal
  - Mely nyomtatókat használhatják a felhasználók
  - Hová fordulhat az illető, ha gondja van a gépével



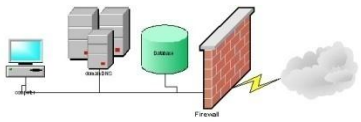
Alkalmazás-felügyeleti funkciók

- A központi adatbázisban tárolt rendszerképek segítségével „öngyógyító”-vá tehetők az alkalmazások:
  - a véletlenül letörölt vagy megsérült alkalmazásfájlok, az elrontott regisztrációs beállítások automatikusan kijavításra kerülnek
- A munkaállomás-hozzárendelési funkcióval szabályozható, honnan férhetnek hozzá a felhasználók az alkalmazásokhoz
- Alkalmazás-eltávolítási funkció



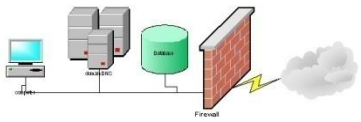
Szoftverhasználat mérése

- A szoftver mérési funkcióval automatizálható a szétosztott alkalmazások ellenőrzése és mérése
  - Pl. ha a maximális licencszámot túllépné a rendszer, beállítható például, hogy további felhasználó ne indíthassa el az alkalmazást
- Jelentések készítése: alkalmazások szétosztásról és használatáról



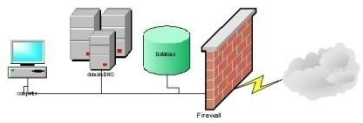
Desktop management szolgáltatások

- Rendszerkép (system image) készítés, automatikus géptelepítés
- Személyre szabott szoftver telepítés, alkalmazás felügyelet, szoftverhasználat mérése
- ***Különböző irányelvek menedzselése (policy management)***
- Távoli felügyelet
- Teljes körű szoftver és hardver leltár (inventory)



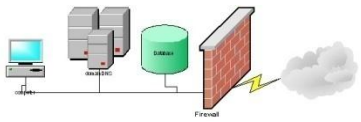
Irányelv alapú munkaállomás-felügyelet

- Irányelvek
  - vállalati szinten meghatározzák, hogy egy használó/használói csoport milyen lehetőségekkel rendelkezzen
    - mit konfigurálhat
    - mit telepíthet
    - milyen szoftvereket futtathat
    - asztali beállítások
    - milyen hálózati erőforrásokhoz férhet hozzá
  - személyhez, nem géphez kötött
  - központi adatbázisban tárolt – módosítás esetén automatikusan eljuttatja az összes géphez



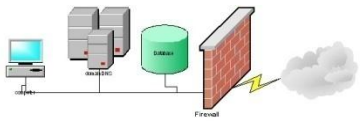
Desktop management szolgáltatások

- Rendszerkép (system image) készítés, automatikus géptelepítés
- Személyre szabott szoftver telepítés, alkalmazás felügyelet, szoftverhasználat mérése
- Különböző irányelvek menedzselése (policy management)
- ***Távoli felügyelet***
- Teljes körű szoftver és hardver leltár (inventory)



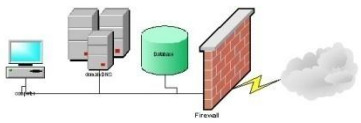
Távoli felügyelet

- Megelőzhetők, elháríthatók a hibák
  - nem kell a használóknak műszaki kérdésekre felelniük
  - help request megnyomása – e-mail a rendszergazdáknak a hiba leírásával
- Távolról irányíthatóak a gépek
  - amennyiben joga van rá!
- Bárhonnan (Interneten keresztül) kapcsolódhat



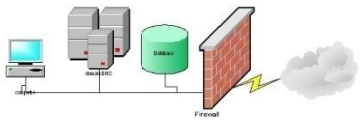
Távoli felügyelet funkciói

- Távoli fájlátvitel, távoli programvégrehajtás és távoli diagnosztika
- Billentyűzet és egér lezárása, képernyő elsötétítése távoli vezérlési alatt
- „Wake on LAN”
- A hozzáférési jogok megállapíthatók
  - felhasználónként,
  - osztályonként, telephelyenként,
  - munkaállomásonként
  - korlátozások állíthatók be egyes rendszergazdák számára is



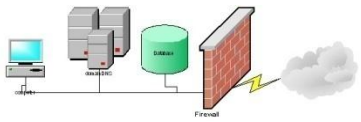
Desktop management szolgáltatások

- Rendszerkép (system image) készítés, automatikus géptelepítés
- Személyre szabott szoftver telepítés, alkalmazás felügyelet, szoftverhasználat mérése
- Különböző irányelvek menedzselése (policy management)
- Távoli felügyelet
- ***Teljes körű szoftver és hardver leltár (inventory)***



Munkaállomás leltár

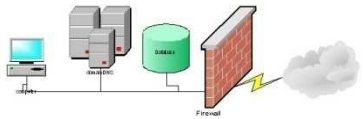
- Hardver leltár
- Szoftver leltár
  - „beépített” lista
  - bővíthető
  - beállítások is
- SQL adatbázisban tárolt adatok
- Előre elkészített ill. „saját” jelentések készíthetők
  - frissítések
  - licenszek lejárta
  - állományok, programok elérési útja (eltávolítás!)



Információs rendszerek üzemeltetése

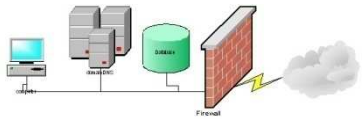
Adatbázis-menedzsment

Erős Levente (eros@db.bme.hu)
BME VIK TMIT
Mérnök-informatikus alapképzés



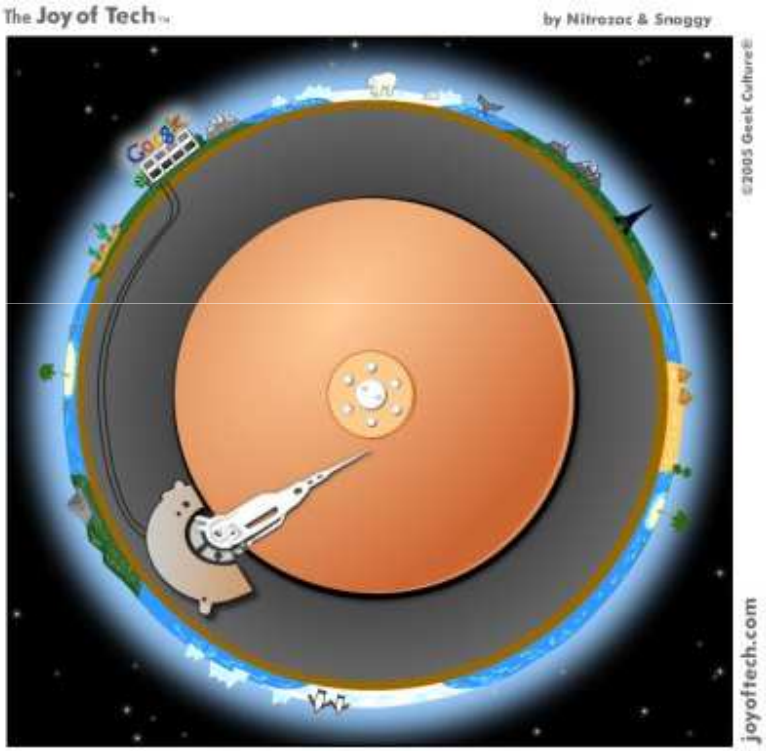
Tartalom

- 1. Tárolás (Storage)
- 2. Mentés (Backup)
  - Oracle
- 3. Visszaállítás (Recovery)



1. Tárolás

- Alapprobléma
  - Nagy táblák tárolása
  - (Hálózat több pontján hozzáférő felhasználók számára)
- Kívánalmak
  - Nagy teljesítmény
  - Alacsony költségek
- Megoldás
  - Különböző tárolóeszközök használata
  - Partícionált tárolás (táblatöredékek tárolása)
  - (Partíciók szétszórása a hálózaton)



Where Google gets all that Gmail hard drive space.

1.1. Különböző tárolóeszközök

- Költségoptimalizálás
  - Kevésbé fontos adatokat lassabb, olcsóbb eszközön tároljuk

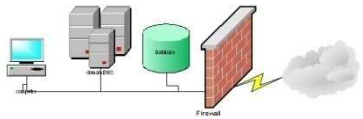
- Memória, SSD, merevlemez, mágnesszalag

S E B E S S É G

K Ö L T S É G H A T É K O N Y S Á G

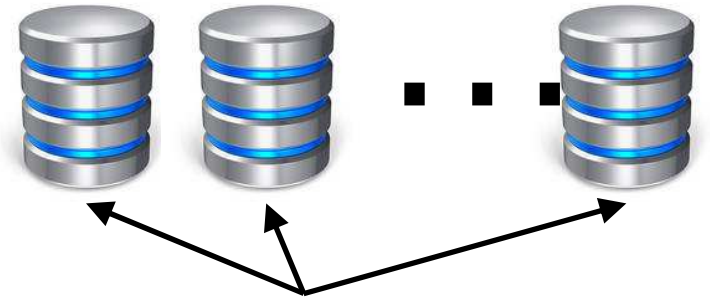
1.1. Különböző tárolóeszközök

- MAID
  - Massive Array of Idle Disks
  - Szalag vetélytársa
  - Működése
    - Több száz – több ezer lemez
    - Csak aktív lemezek forognak
  - Előnyök
    - Alacsony fogyasztás
    - Költség/TB kazettáét közelíti
  - Hátrányok
    - Alacsony throughput
    - Nagy késleltetés a lemezek felpörgetésekor



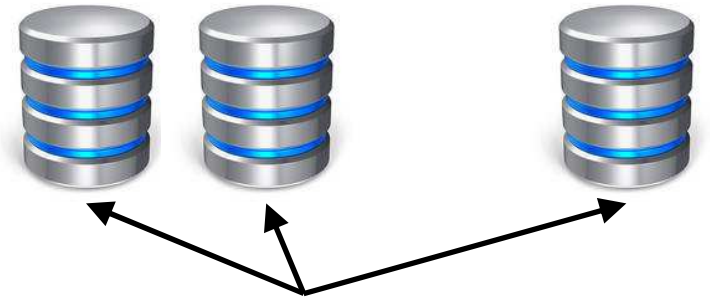
1.2. Partícionált tárolás

- Részrelációk tárolása teljes reláció helyett
- Partícionálás módjai
  - Vertikális felosztás (attribútumok mentén)
  - Horizontális felosztás (rekordok mentén)
- Szempontok
  - Lekérdezés végrehajtásakor minél kevesebb töredék használata
  - Hálózat terhelésének minimalizálása
  - Fontosság szerinti partícionálás – különböző tárolóeszközökre
    - Horizontális felosztás esetén
- Alapelv
  - Felhasználó egységes adatbázist lát



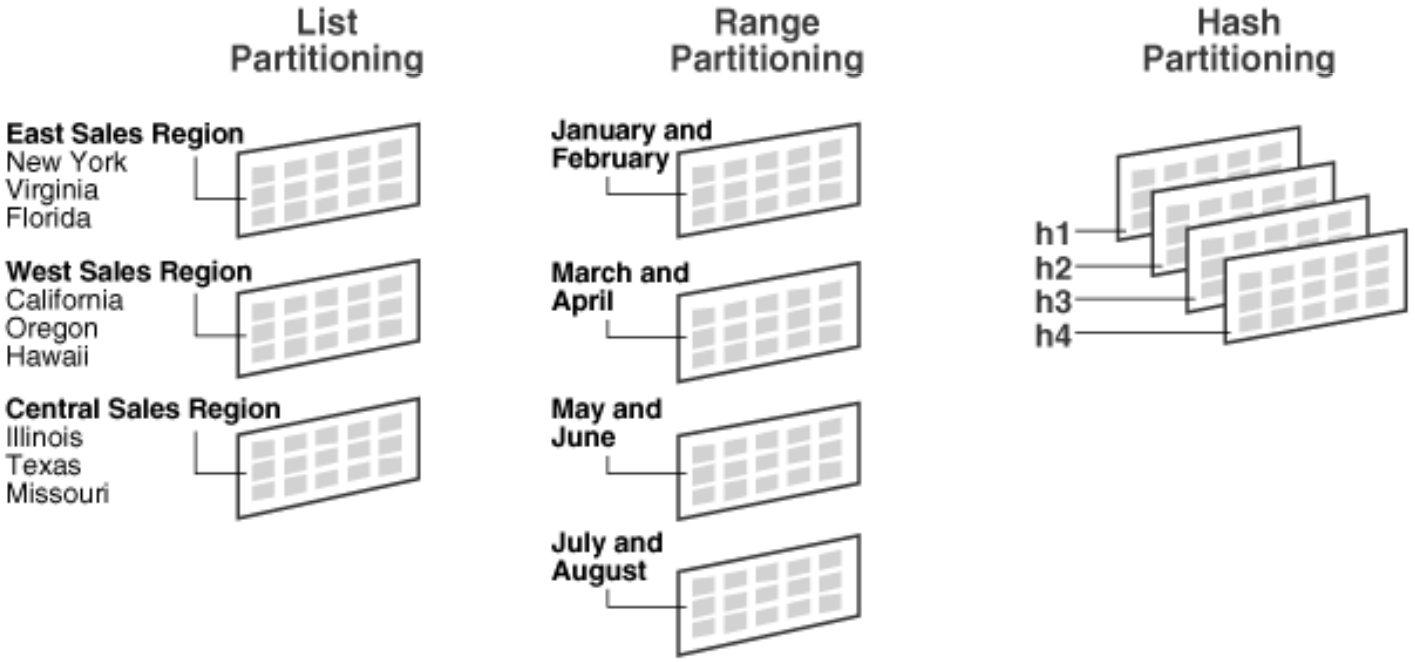
1.2. Partícionált tárolás

- Előnyök
  - Menedzsment
    - Indexelés, backup, recovery partíciószinten
    - Gyorsabb
  - Műveletek teljesítménye
    - Párhuzamosítás
    - Lekérdezés szűkítése partíciókra – jelentős nyereség (ld. később)
  - Hálózathoz alkalmazkodó tárolás
    - Hálózati terhelés minimalizálása
  - Partícióra szabható tárolás
    - Különböző adattároló hardware különböző adatokhoz
    - Különböző indexek különböző partíciókra
  - Magasabb rendelkezésreállás



1.2. Partícionált tárolás

- Megvalósítás (Horizontális felosztás)
  - Lista alapján
  - Tartományok alapján
  - Hash alapján

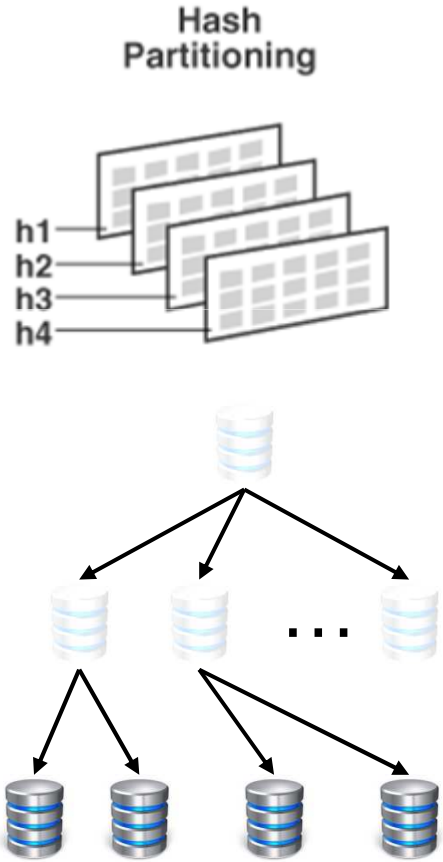


1.2. Partícionált tárolás

- Partíciós kulcs alapján
  - Ennek értéke mentén partícionálunk
- Fajtái
  - Lista alapú partícionálás
    - Diszkrét értékkészlet
    - Minden partícióra külön megadjuk az oda tartozó értékek halmazát
    - Pl. Telephelyek szerint
  - Tartomány alapú partícionálás
    - Alsó és felső korlátokat adunk az egyes partíciókban tárolt értékekre
    - Pl. Dátum szerint

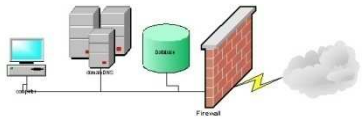
1.2. Partícionált tárolás

- Partíciós kulcs alapján
  - Ennek értéke mentén partícionálunk
- Fajtái
  - Hash alapú partícionálás
    - Hash függvény adja meg a kulcshoz tartozó rekord célpartícióját
    - Hasznos, ha nem tudjuk előre az egyes tartományok méretét, és így nagy eltérés lenne a méretükben
      - Jó hash egyenletesen szór
    - Pl. Ügyfélazonosító szerint
  - Hibrid partícionálás
    - Fentiek vegyítése több szinten
    - Pl. Először lista szerint kirendeltségek alapján, majd idő szerint



1.2. Partícionált tárolás

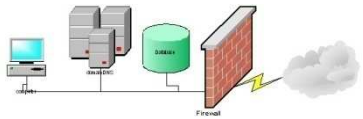
- Egyéb partícionálási módszerek
  - Intervallum alapú partícionálás
    - Tartomány alapú partícionálás egyszerűsítve
    - Nem kell kézzel létrehozni előre a partíciókat, azok automatikusan jönnek létre
    - Azt adjuk meg, mi szerint hoznánk létre kézzel (pl. minden hónapra)
  - Virtuális oszlop alapján történő partícionálás
    - Az attribútumokon megadott függvény értéke szerint
  - Származtatott partícionálás
    - Külső kulcs alapján, pl. Autó(tulajnév, rendszám) táblát cím szerint partícionáljuk Személy(tulajnév, cím, tel) cím szerinti partícionálásának megfelelően



1.2. Partícionált tárolás

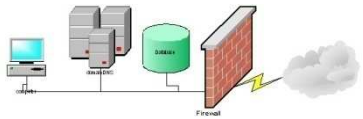
- Lekérdezések partícionált táblákon
  - Teljes relációk
    - Személy(<u>szemszám</u>, név, cím, telefonszám)
    - Jármű(<u>rendszám</u>, <u>szemszám</u>, típus)
  - Töredékek
    - $\text{Személy}_1 = \sigma_{\text{szemszám}<20000000000}\text{Személy}$
    - $\text{Személy}_2 = \sigma_{\text{szemszám}\geq 20000000000}\text{Személy}$
    - $\text{Jármű}_1 = \sigma_{\text{szemszám}<30000000000}\text{Jármű}$
    - $\text{Jármű}_2 = \sigma_{\text{szemszám}\geq 30000000000}\text{Jármű}$

    felosztási szabály
  - Teljes reláció a töredékek uniója



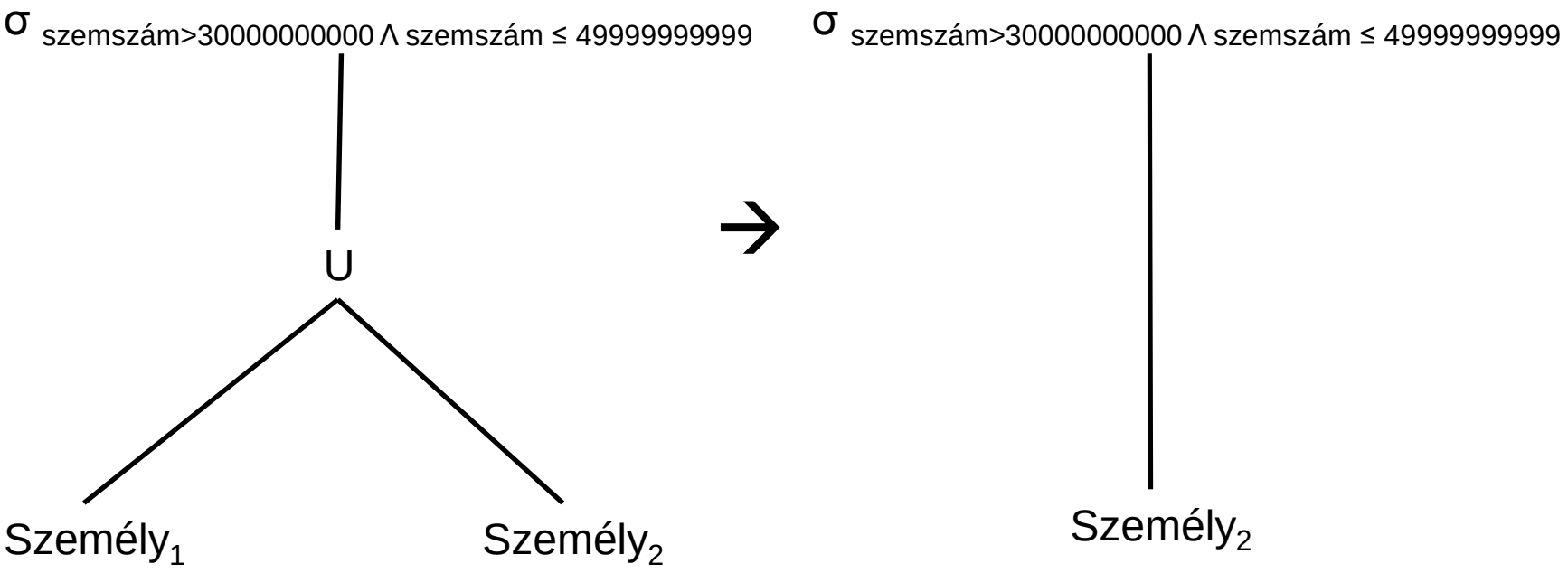
1.2. Partícionált tárolás

- Lekérdezés egyszerűsítése szelekció esetén
  - Szelekciós feltétel ellentmond a felosztási szabálynak → üres eredmény adott töredékből
  - Példa lekérdezés
    - $\sigma_{\text{szemszám}>30000000000 \wedge \text{szemszám} \leq 49999999999}$ Személy
  - Töredékekre átfogalmazva
    - $\sigma_{\text{szemszám}>30000000000 \wedge \text{szemszám} \leq 49999999999}$ ($\text{Személy}_1 \cup \text{Személy}_2$)
  - Személy_1 felosztási szabálya ellentmond a szelekciós feltételnek
  - Egyszerűsített lekérdezés
    - $\sigma_{\text{szemszám}>30000000000 \wedge \text{szemszám} \leq 49999999999}$ Személy_2



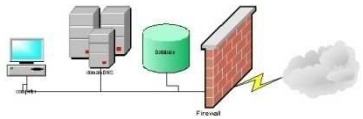
1.2. Partícionált tárolás

- Egyszerűsítés szelekció esetén lekérdezési fával



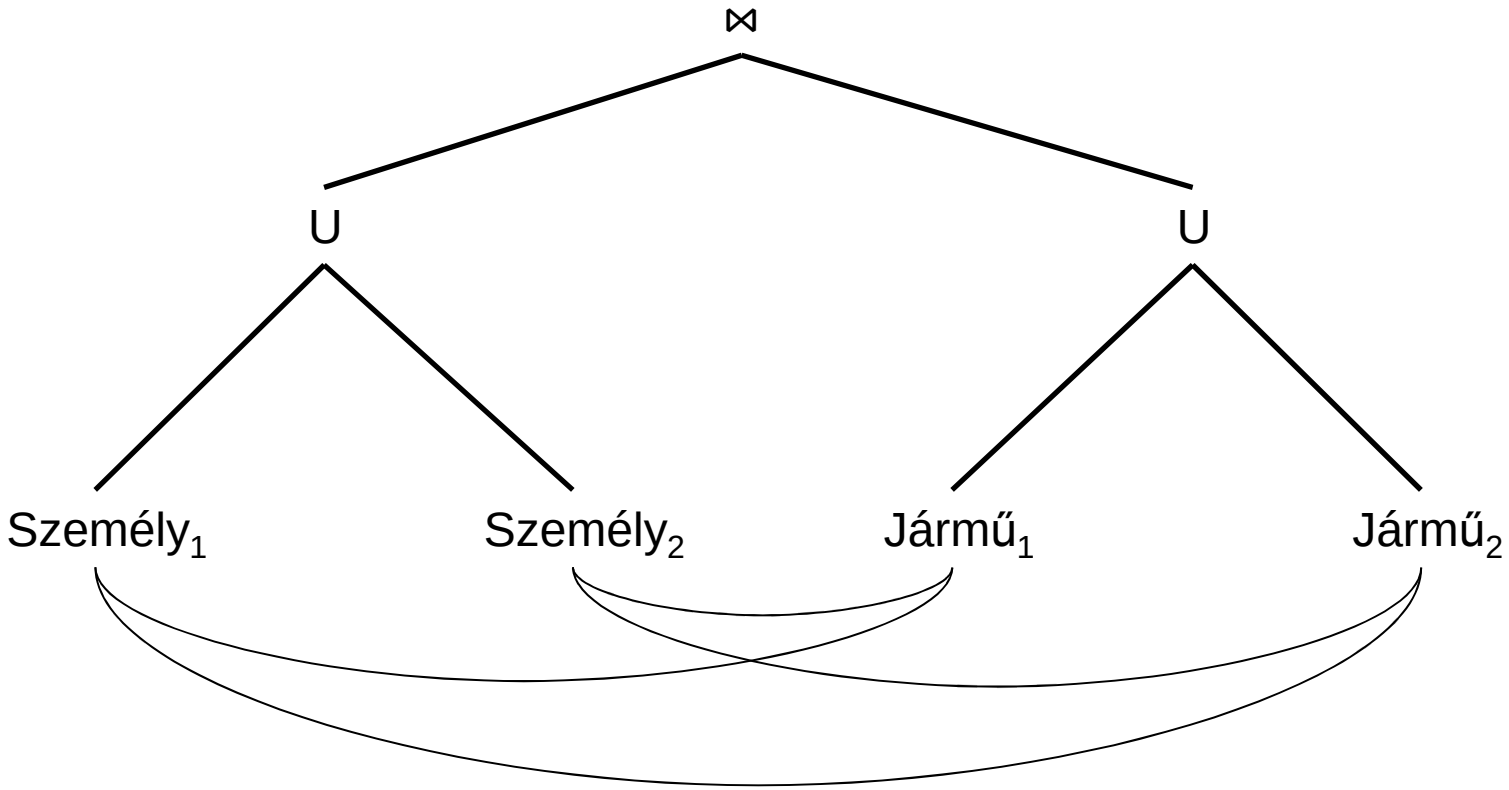
1.2. Partícionált tárolás

- Lekérdezés egyszerűsítése illesztés esetén
  - Feltétele: Illesztett relációk a join-attribútum szerint fragmentáltak
    - A join-attribútumra (is) vonatkozik a felosztási feltétel
  - Példa lekérdezés:
    - Személy ⋈ Jármű
  - Töredékekre átfogalmazva
    - $(\text{Személy}_1 \cup \text{Személy}_2) \bowtie (\text{Jármű}_1 \cup \text{Jármű}_2)$
  - Illesztés süllyesztése
    - $((\text{Személy}_1 \cup \text{Személy}_2) \bowtie \text{Jármű}_1) \cup ((\text{Személy}_1 \cup \text{Személy}_2) \bowtie \text{Jármű}_2)$
    - $(\text{Személy}_1 \bowtie \text{Jármű}_1) \cup (\text{Személy}_1 \bowtie \text{Jármű}_2) \cup (\text{Személy}_2 \bowtie \text{Jármű}_1) \cup (\text{Személy}_2 \bowtie \text{Jármű}_2)$
  - Személy_1 és Jármű_2 felosztási feltételei ellentmondanak egymásnak
    - $(\text{Személy}_1 \bowtie \text{Jármű}_1) \cup \cancel{(\text{Személy}_1 \bowtie \text{Jármű}_2)} \cup (\text{Személy}_2 \bowtie \text{Jármű}_1) \cup (\text{Személy}_2 \bowtie \text{Jármű}_2)$
    - **$(\text{Személy}_1 \bowtie \text{Jármű}_1) \cup (\text{Személy}_2 \bowtie \text{Jármű}_1) \cup (\text{Személy}_2 \bowtie \text{Jármű}_2)$**



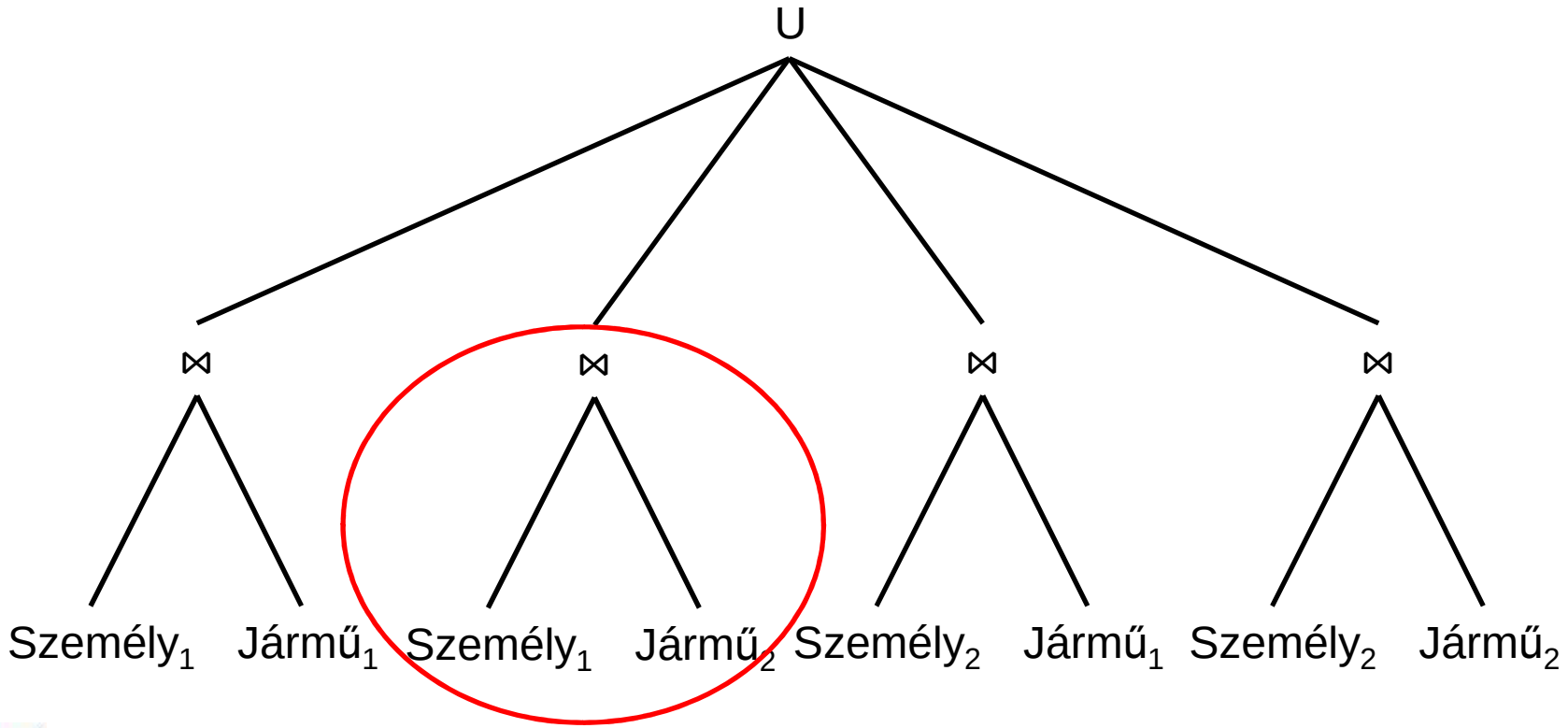
1.2 Partícionált tárolás

- Egyszerűsítés illesztés esetén lekérdezési fával



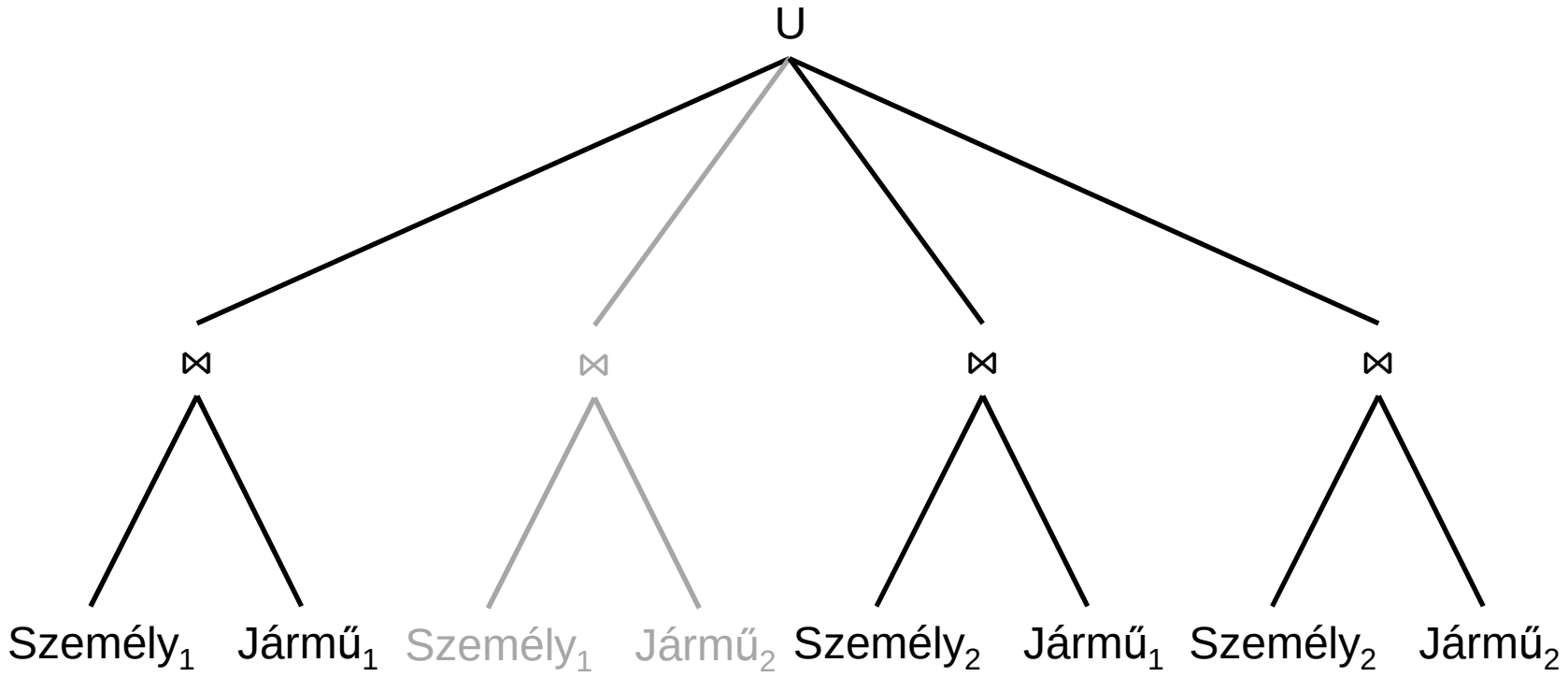
1.2 Partícionált tárolás

- Egyszerűsítés illesztés esetén lekérdezési fával
  - Illesztés süllyesztése



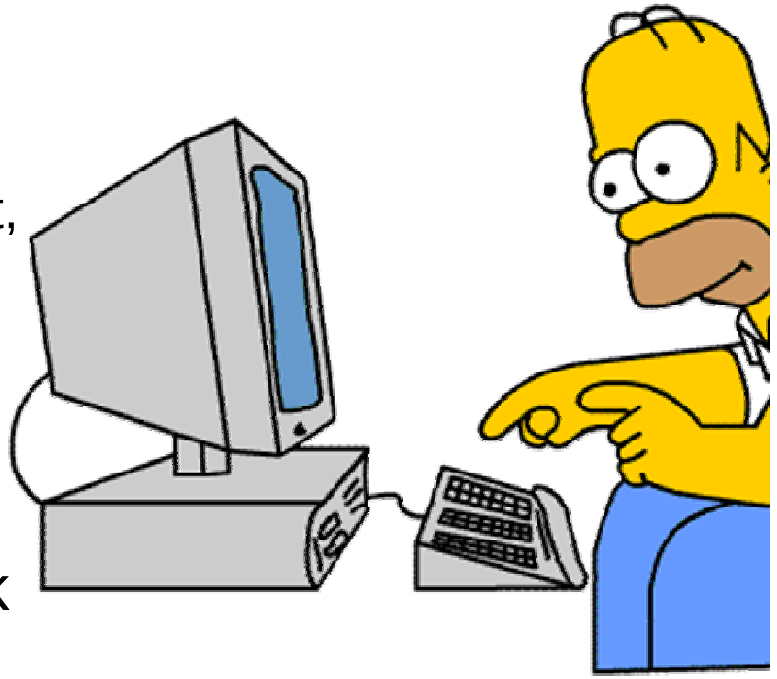
1.2 Partícionált tárolás

- Egyszerűsítés illesztés esetén lekérdezési fával
  - Redukció



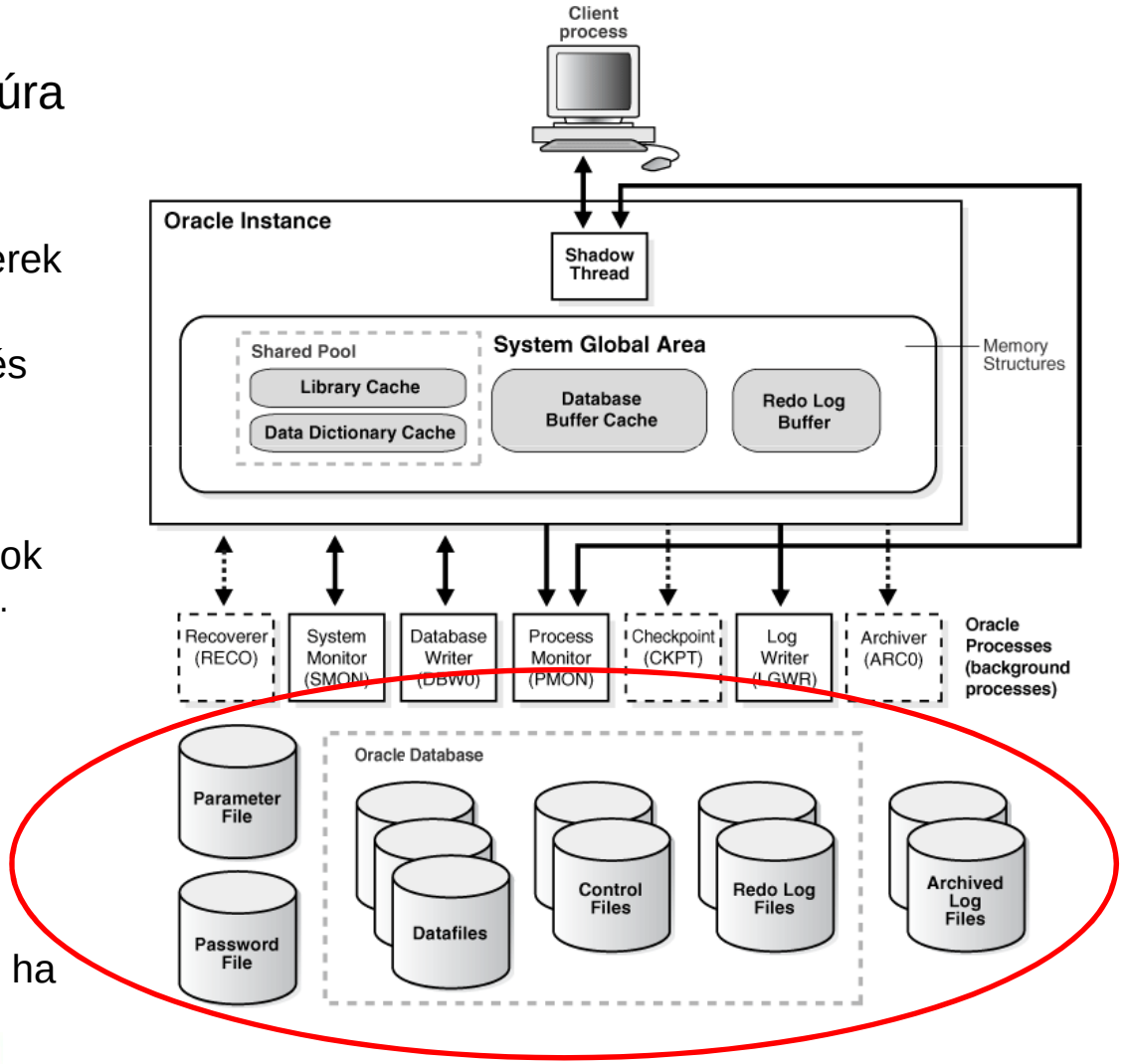
2. Adatbázisok mentése

- Miért készítsünk biztonsági mentést?
  - Hardverhibák
    - Lemezhiba
      - Ritka – fizikai szintű védelem – pl. RAID
  - Szoftverhibák, bug-ok
    - OS/DBMS/Alkalmazás
  - Adatbázispéldány hibája
    - Bug, túlterhelés, kihúzzuk a dugót, inkonzisztens állapotban történő leállítás
  - Felhasználói hibák
    - Pl. Tábla eldobása
    - Leggyakoribb
  - Adatbázis-adminisztrátori hibák



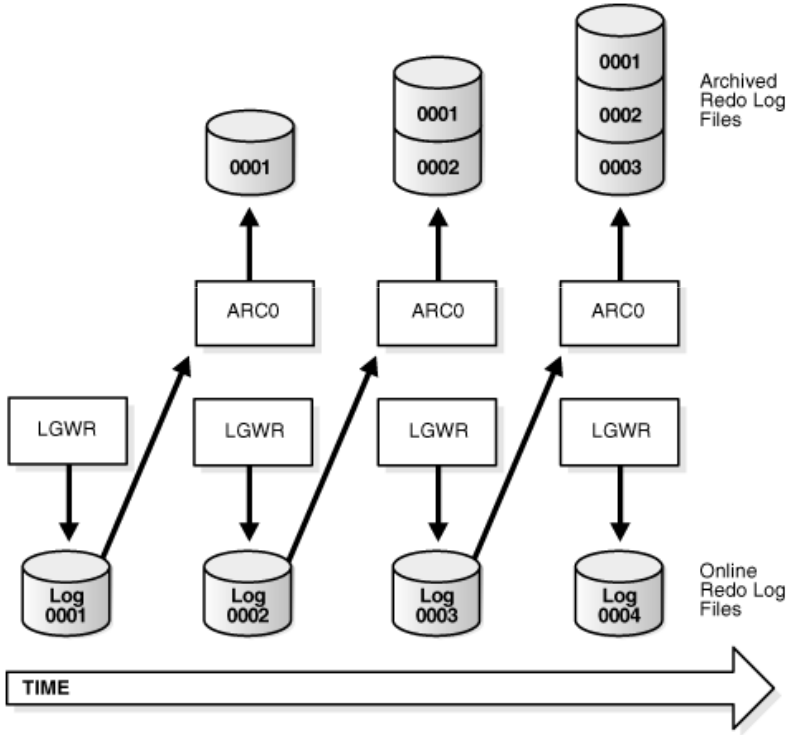
2. Adatbázisok mentése

- Kitérő – Oracle-architektúra
- Adatbázisfájlok
  - Paraméterfájlok
    - Adatbázis-paraméterek
  - Vezérlőfájl(ok)
    - Adatbázis állapota és fizikai struktúrája
  - Adatfájlok
    - Táblaterek
    - Adatbázis-objektumok
      - Tábla, nézet, stb.
  - Redo napló fájljai
    - 2 vagy több, redo-bejegyzéseket tartalmazó fájl
    - *Undo információ*
  - Archivált naplók
    - Naplók alapesetben felülíródnak, kivéve, ha archiváljuk őket



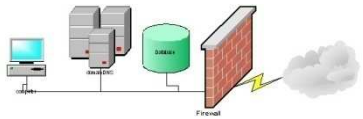
2. Adatbázisok mentése

- Kitérő – Archivelog mód
  - Alapértelmezett mód: Noarchivelog
    - Redo naplók kezelése ciklikus
    - Régi bejegyzéseket felülírják az újak
  - Archivelog mód
    - Felülírás előtt archiválás
  - Előny
    - Visszaállíthatóság tetszőleges időpontba az adatbázis-mentéstől kezdve, naplóbejegyzések alapján haladva
    - Vasárnapi mentés, pénteki összeomlás esetén:
      - Archivelog mód – pénteki állapot
      - Noarchivelog mód – vasárnapi állapot
    - Nyitott mentések lehetővé tétele
  - Hátrány
    - Overhead



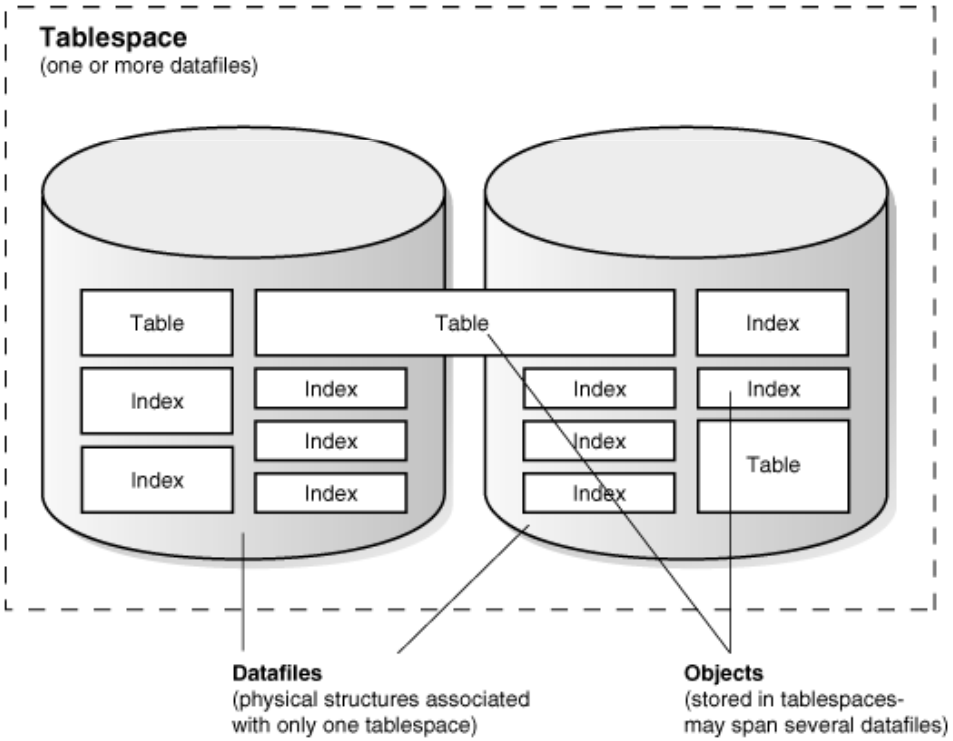
2. Adatbázisok mentése

- Mentések típusai
  - Fizikai mentés
    - Összes fenti hiba ellen véd
  - Logikai mentés
    - Emberi hibák, adatbázis-alkalmazások hibái ellen véd
  - Nyitott adatbázis mentése
    - Adatbázis üzemelése közben
    - Hot backup
  - Zárt adatbázis mentése
    - Adatbázis leállításával
    - Cold backup
- Cél: konzisztens állapot visszaállíthatósága



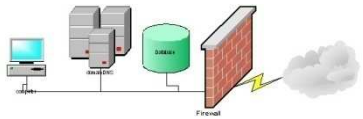
2.1. Fizikai mentés

- Adatbázis-fájlok mentése
- Oracle Recovery Manager (RMAN) alkalmazással
- Mit ment a fizikai mentés?
  - Adatfájlokat
  - Táblatereket
  - Teljes adatbázist
  - Vezérlőfájlokat
  - Paraméterfájlokat
  - Archivált naplókat



2.1. Fizikai mentés

- Lehetőség van
  - Zárt adatbázis mentésére
    - Adatbázist le kell állítani a mentés idejére
    - „Cold backup”
  - Nyitott adatbázis mentésére
    - Adatbázis működik mentés közben
    - „Hot backup”
- Lehet
  - Konzisztens
  - Inkonzisztens

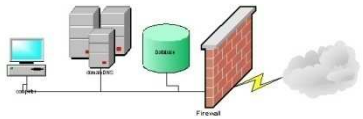


2.1.1. Zárt adatbázis mentése

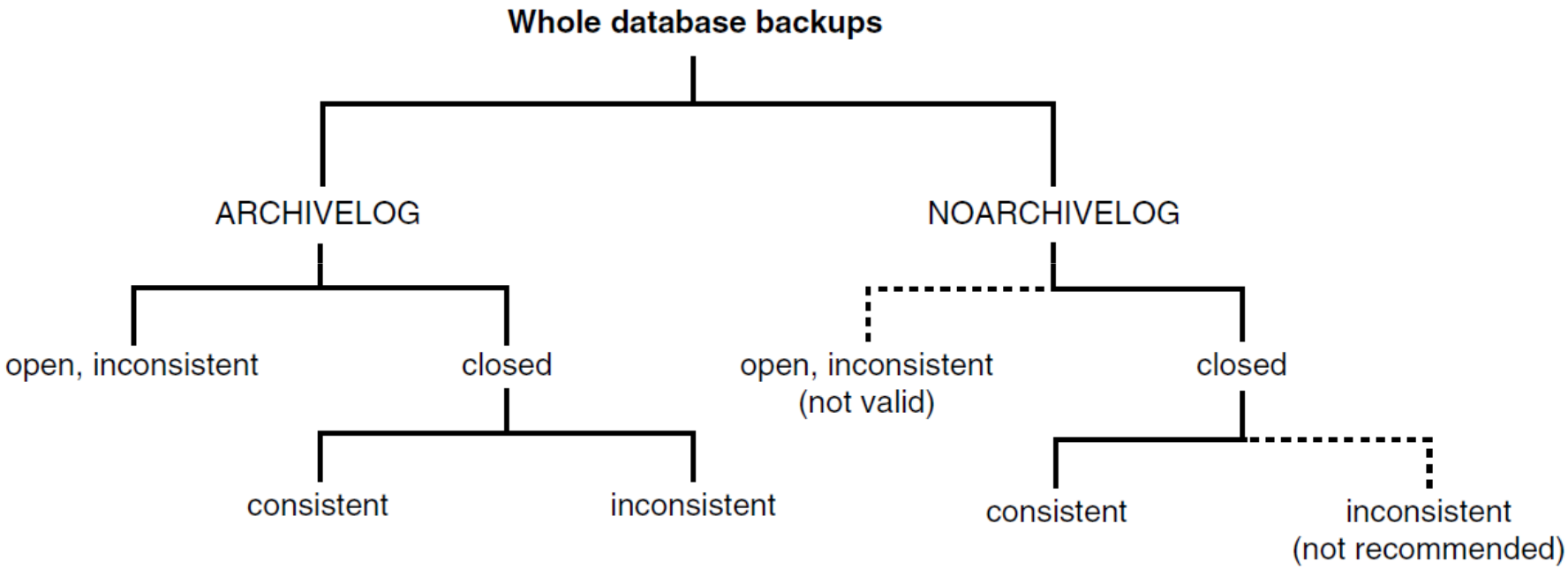
- Működése
  - Adatbázis leállítása
  - Adatbázis-fájlok fizikai szintű mentése
  - Adatbázis elindítása
- Konzisztens vagy inkonzisztens?
  - Ha szabályosan állt le az adatbázis, konzisztens
  - Ha szabálytalanul, lehet, hogy inkonzisztens
    - → NOARCHIVELOG mód ellenjavallt
- Előnyök
  - Szabályos leállás esetén konzisztens állapotot tükröz
  - Gyors visszaállítás
    - Fizikai szintű másolás
- Hátrány
  - Adatbázist le kell állítani, mentés idejére használhatatlan
- Egyetlen lehetőség NOARCHIVELOG módban

2.1.2. Nyitott adatbázis mentése

- Működése
  - Adatbázisfájlok mentése használat közben
- Garantáltan inkonzisztens
  - ARCHIVELOG mód követelmény
  - Naplók szükségesek a konzisztens visszaállításhoz
- Előnyök
  - Mentés közben hozzáférhető az adatbázis
- Hátrányok
  - Hosszabb ideig tart a zárt mentésnél
  - Hosszabb a visszaállítás
- 24 órás üzemelés esetén szükséges
- Mentés után
  - Archiválatlan naplók archiválása
  - Archivált naplók és vezérlőfájl(ok) mentése
  - Cél: Konzisztencia visszaállíthatósága a mentés végéig

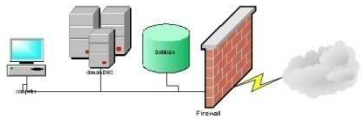


2.1. Fizikai mentés



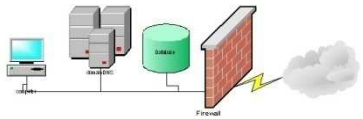
2.1 Fizikai mentés

- Fizikai mentés lehet továbbá
  - Teljes
    - RMAN alapértelmezett
    - Valamennyi elmentendő fájl valamennyi blokkjának mentése
  - Többszintű
    (Oracle terminológia szerint *inkrementális*)
    - Az elmentendő fájlok előző mentés óta változott blokkjainak mentése



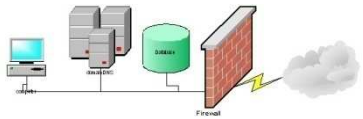
2.1 Fizikai mentés

- Többszintű mentés
  - 0. szintű mentés
    - Következő 1.szintű mentések alapjául szolgál
    - Fizikailag teljes mentés, de mégsem az
      - Adatfájlok valamennyi használt adatblokkjának mentése
      - Teljes mentés nem része inkrementális mentési sorozatnak, függetlenül végezhető
  - 1. szintű mentés
    - Típusai
      - Inkrementális mentés (Oracle terminológiájában *differenciális* mentés)
      - Differenciális mentés (Oracle terminológiájában *kumulatív* mentés)



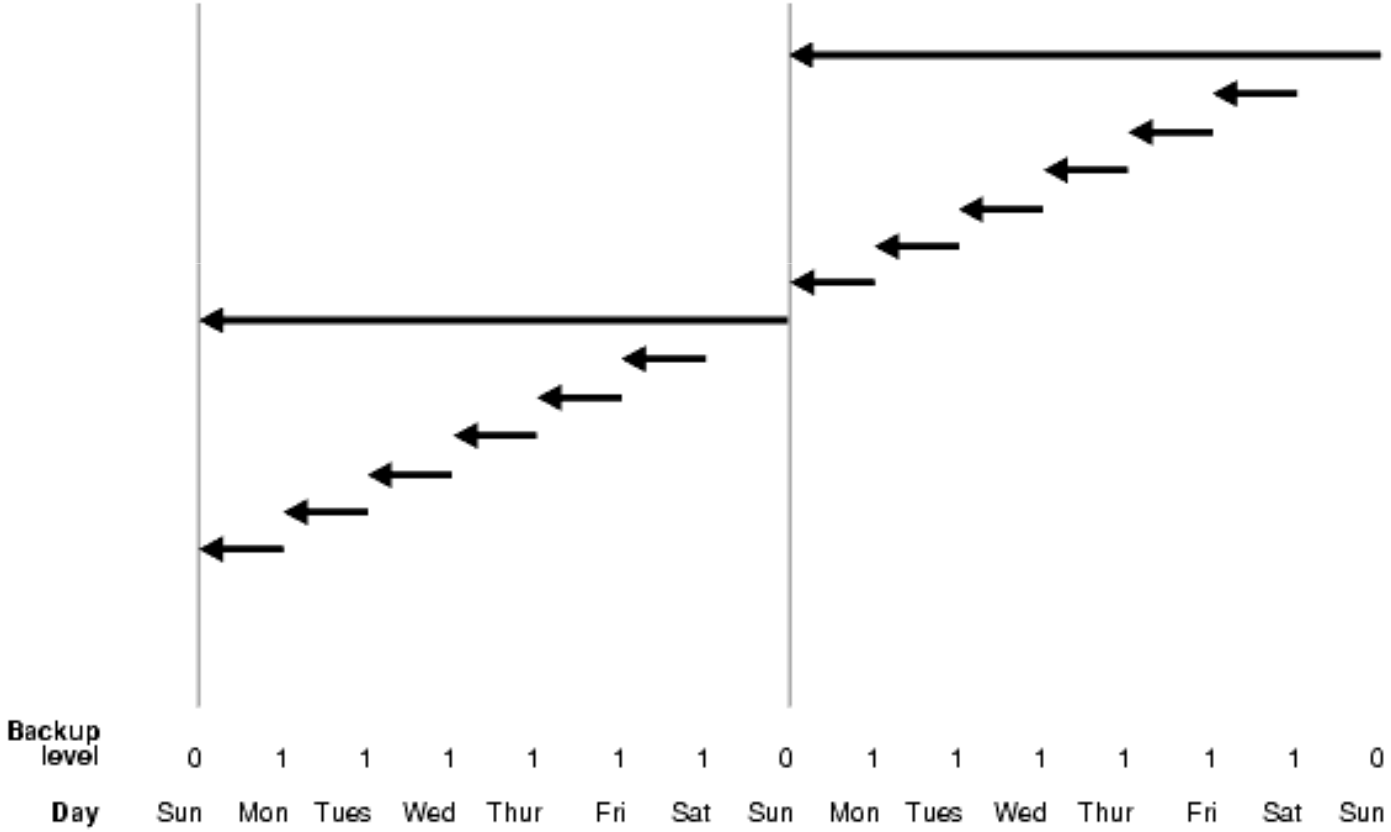
2.1 Fizikai mentés

- Inkrementális 1. szintű mentés
  - Alapértelmezett
  - Legutóbbi 0. vagy 1. szintű mentéshez képest változott blokkokat menti
    - Legutóbbi 1. szintű inkrementális vagy differenciális mentés megkeresése
      - Ehhez képest változott blokkok mentése.
    - Ha a legközelebbi mentés 0. szintű, akkor az ahhoz képest változott blokkokat mentjük el.
- Differenciális1. szintű mentés
  - Legutóbbi 0. szintű mentés óta változott blokkok mentése



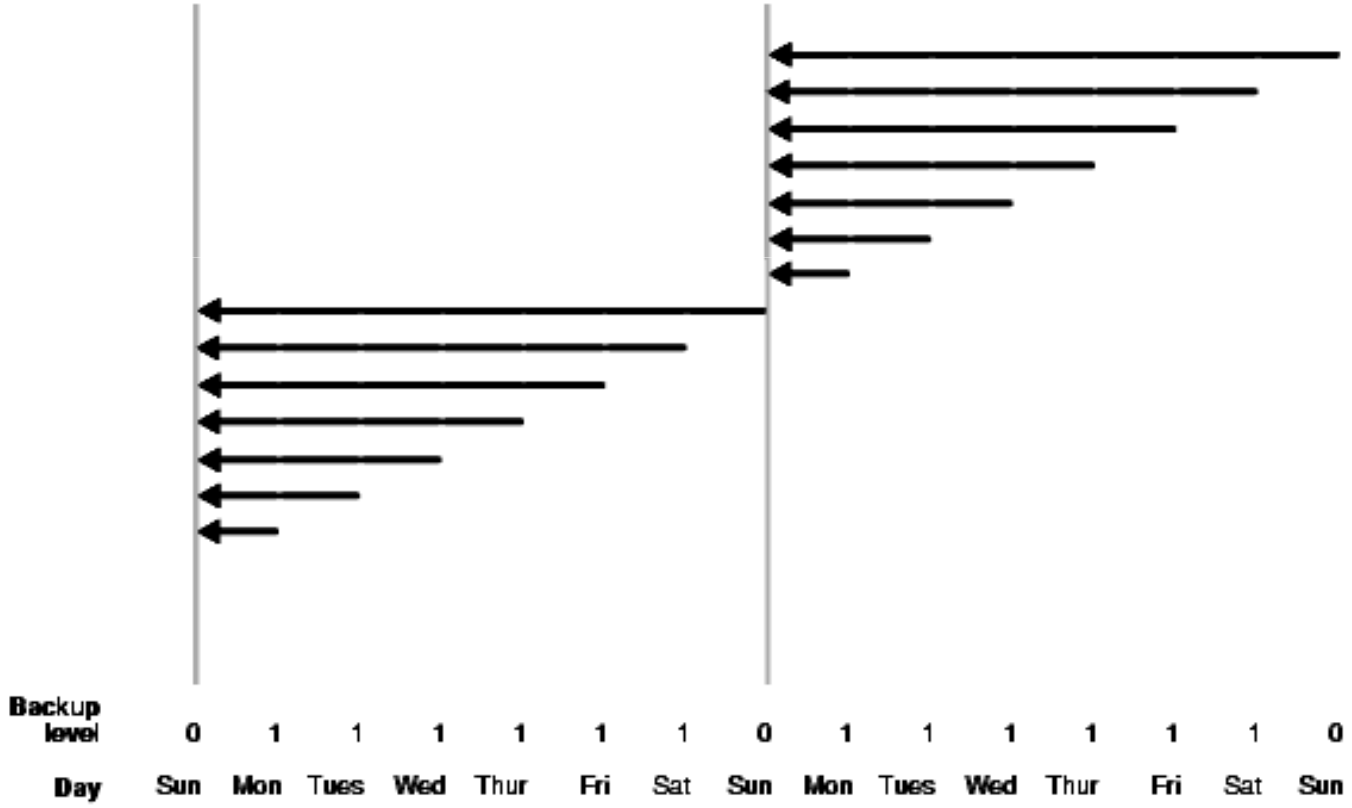
2.1 Fizikai mentés

- Példa inkrementális mentésre



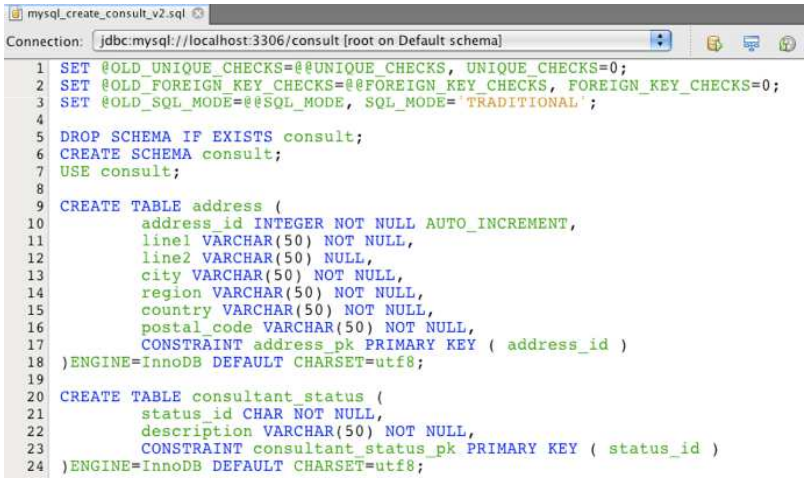
2.1 Fizikai mentés

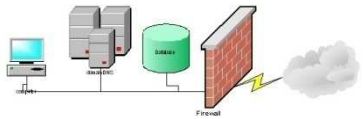
- Példa differenciális mentésre



2.2. Logikai mentés

- Logikai adatbázis (egy részének) mentése, függetlenül az őt tároló állományoktól
- Lehetséges:
  - Adatbázis-objektum mentése (pl. tábla, tárolt eljárás)
    - Táblaeldobás ellen remekül véd
  - Adatbázisséma mentése
  - Teljes adatbázis mentése
- Oracle Data Pump
  - Logikai objektumokból dump állomány generálása
  - Dump-ból SQL-szkript lesz, ez végzi a visszaállítást (ezért logikai)
- Konzisztens kép mentése
  - Mentés kezdete utáni módosítások nem látszanak



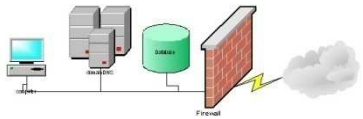


2.2. Logikai mentés

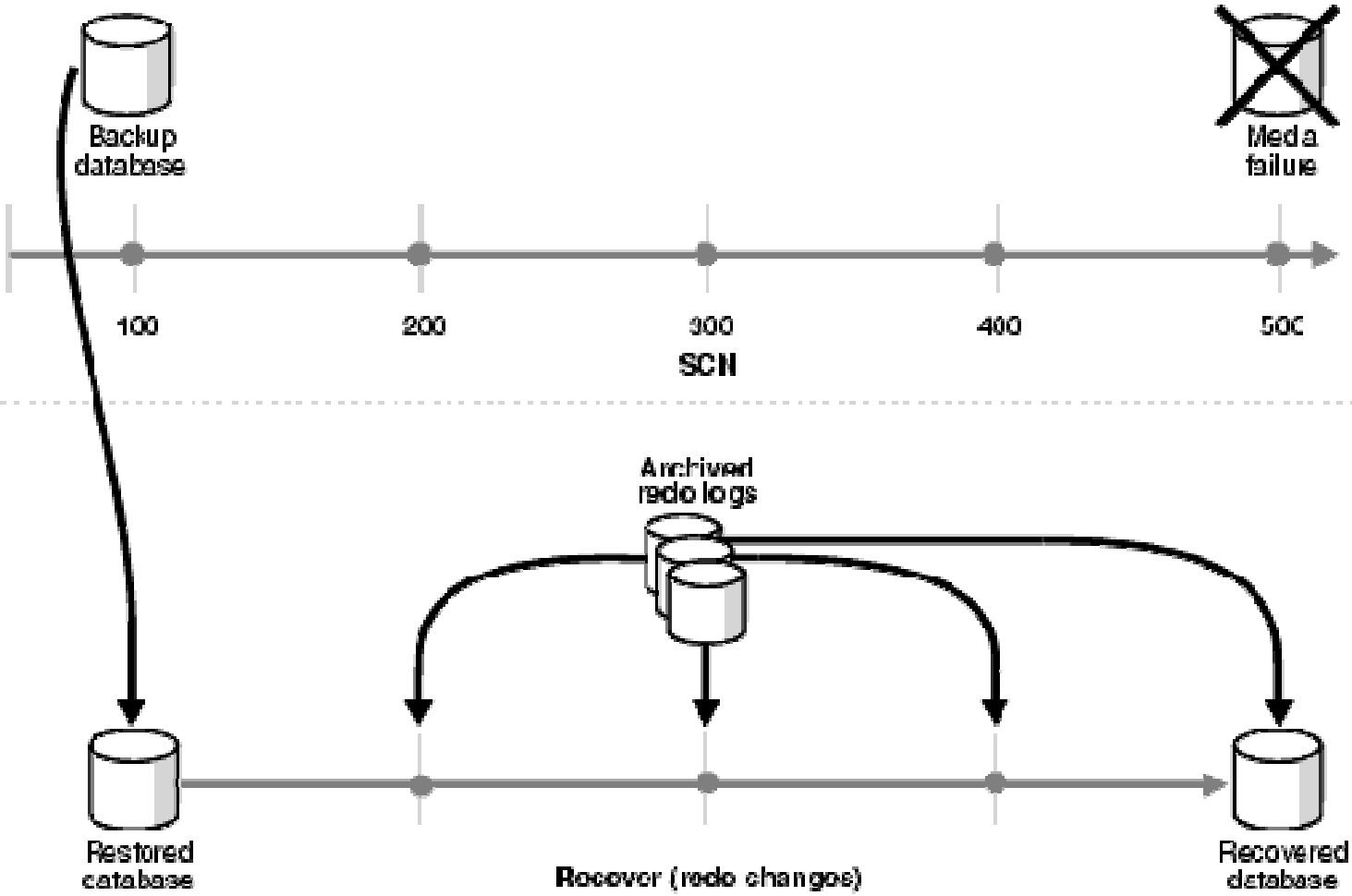
- Előnyök
  - Hordozható
  - Kiválaszthatók a visszaállítandó elemek
- Hátránya
  - Lassú

3. Visszaállítás (Recovery)

- Lépések logikai mentés esetén
  - Import (gyakorlatilag SQL szkript futtatása)
- **Lépések fizikai mentés esetén**
  - Adatfájlok visszaállítása a mentés helyéről (Restoration)
  - Mentés óta történt változások érvényesítése az adatfájlokon (Recovery)
    - Inkonzisztens mentés esetén kötelező
    - Adott SCN-ig
      - SCN – System Change Number, minden commit-nál nő eggyel
      - Általában a legutolsó SCN-it
  - Visszaállítás forrása
    - Adatfájlok
      - A backup-ot tároló tárról
    - Mentés óta történt változások
      - Napló
      - Archivált naplók

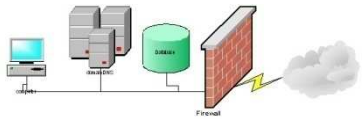


3. Visszaállítás (Recovery)



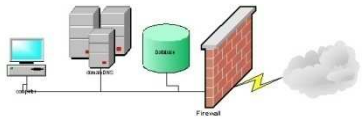
3. Visszaállítás (Recovery)

- Fajtái
  - Teljes
    - Legutolsó olyan időpontba történő visszaállítás, amely csak committált tranzakciók futását tükrözi
    - Legutóbbi SCN
    - Valamennyi committált tranzakció hatása érvényre jut
  - Nem teljes
    - Tetszőleges korábbi SCN-ig committált tranzakciók futását tükröző állapot
    - Pl. Felhasználói hiba, táblaeldobás esetén a tábla eldobását megelőző SCN-be



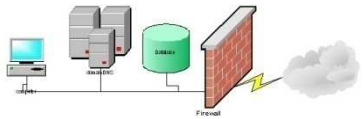
Összefoglaló

- Különböző tárolóeszközök
- Partícionált tárolás (horizontális)
  - Partícionálás lehetőségei
  - Lekérdezés-feldolgozás
- Mentés
  - Motivációk
  - Oracle lehetőségei, architektúrája, Archivelog mód
  - Mentések típusai
    - Fizikai/Logikai
    - Nyitott/Zárt
    - Konzisztens/Inkonzisztens
    - Teljes/Több szintű
- Visszaállítás
  - Lépései
  - Fajtái
    - Teljes/Nem teljes



Források

- M. Tamer Özsu, Patrick Valduriez – Principles of distributed database systems, Prentice Hall International, 1999.
- http://gavinsoorma.com/wp-content/uploads/2009/06/ausoug_partitioning.ppt
- http://en.wikipedia.org/wiki/Backup#Live_data
- http://docs.oracle.com/cd/B28359_01/backup.111/b28270/rcmcncpt.htm#BGBFHAGF
- www.radford.edu/~cshing/340/lectures/orabackup.ppt
- http://hep-proj-database.web.cern.ch/hep-proj-database/workshop-July2001/backrecov.ppt
- http://docs.oracle.com/cd/B19306_01/server.102/b14220.pdf
- http://docs.oracle.com/cd/B19306_01/backup.102/b14192/bkup003.htm#i1006297
- http://docs.oracle.com/cd/B19306_01/backup.102/b14192/bkup003.htm#i1023104
- http://docs.oracle.com/cd/B28359_01/backup.111/b28270/rcmcncpt.htm#BRADV89501
- http://www.clt.astate.edu/kfish/CIT4403/Slides/CIT4403-Chpt15.ppt
- http://www.stanford.edu/dept/itss/docs/oracle/10g/server.101/b10735/intro.htm
- http://oracleonline.info/consistent_backup.html

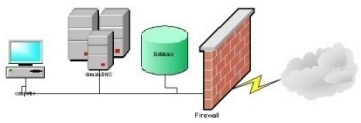


Linux Rendszerek adminisztrációja

- áttekintés és példák -

Varga Pál

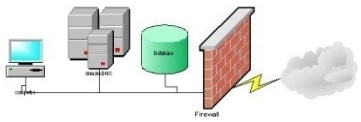
pvarga@tmit.bme.hu



Áttekintés

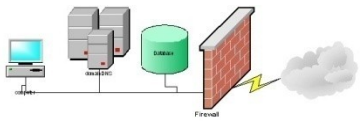
- Linux kernel általános felépítése
- File System
- Alapvető műveletek

- Shell
- Scripting
- Általános ismeretek a laborgyakorlatokhoz
- Rendszer-konfiguráció
- LAPD

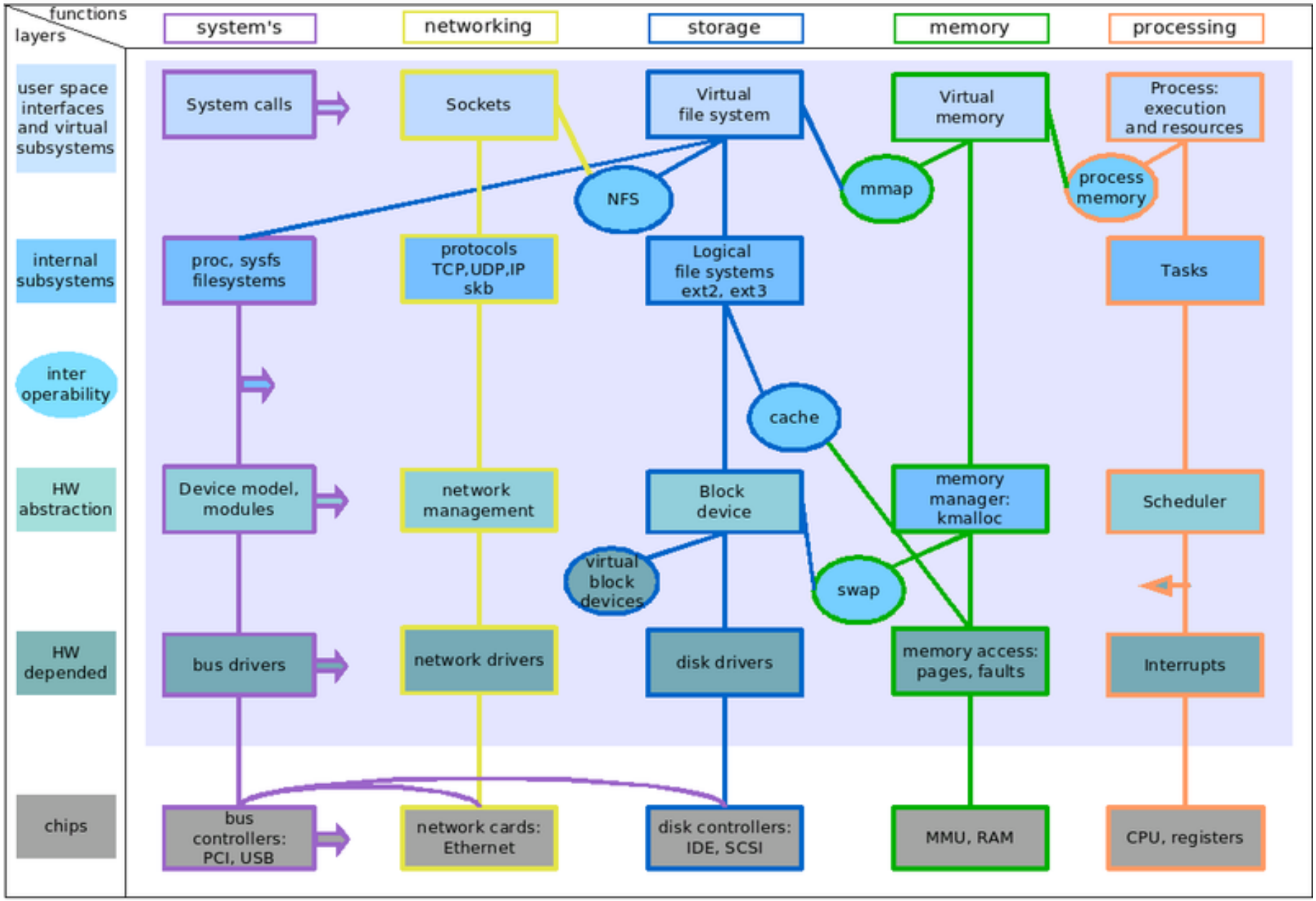


LINUX RENDSZEREK ADMINISZTRÁCIÓJA

I. Kernel
II. File System
III. Alapvető műveletek



Simplified Linux kernel diagram in form of a matrix map



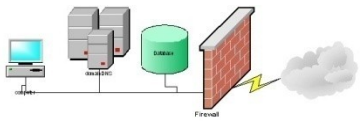
File System

- „device” vagy „partition” ami file-ok tárolására van formázva
- Sok formátum – a felhasználó előtt ugyanolyan megjelenés: könyvtárszerkezetben
- /proc/filesystems - pl. ext2 ext3 vfat NFS ntfs

- A hozzáféréshez *mount*-olni kell – így könyvtárként látszik/elérhető

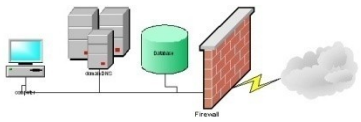
  mount -t vfat /dev/hda1 /windows/cdrive

- mount / umount /eject



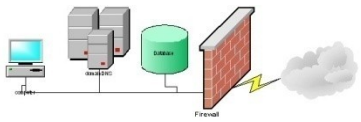
File System (cont)

- Applikáció is
  - Az adathozzáférés vezérlésére
  - A könyvtárak kezelésére és hozzáféréséhez
  - Más applikációk is használják a szolgáltatásait
    - állományokat és könyvtárakat készít
    - megnyit és módosít létezőket
    - törlés
    - hozzáférés-szabályozás



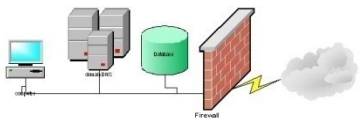
Néhány főbb alkönyvtár

/bin	common programs, shared by admins, users
/boot	startup files and kernel. Also GRUB data
/dev	references to all hardware as special files
/etc	important system configuration files. Sort of like Control Panel
/home	containes home directories for most users
/initrd	information contained for booting.. Don't mess with it!
/lib	library files, common files needed by many programs
/lost+found	files that were recovered after a system failure
/mnt	mount point for all external devices
/net	mount point for remote filesystems
/opt	extra third party software
/proc	info about system resources, man proc
/root	home dir. for the the admin
/tmp	temporary space
/usr	program, libraries, docs for most user programs
/var	other temporary files, such as logs, downloaded files, mail queue



Alapvető műveletek

- cd könyvtárak közötti navigációhoz
- mkdir könyvtár létrehozása
- rmdir könyvtár törlése
- ls könyvtár tartalma
- echo $PATH végrehajtható parancsok helyei
  pl.: /usr/local/bin/:/usr/bin:/bin/
- export környezeti változó beállítása
  pl. PATH=$PATH:/new/directory/path
- man help a parancsok használatához
- history eddig használt parancsok listája
- & parancs után írva: fusson a háttérben *ls & -> [1] 23142*
- fg futó job visszahozása előtérbe *fg 23142*

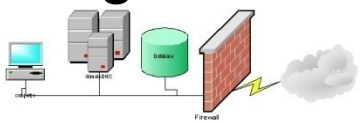


Szöveges manipuláció

- cat teljes file szövegének összeállítása (kiírás)
- tac utolsó sor legelöl (hasznos pl. log file esetén)
- head a file kezdő sorai (default:10)
- tail a file záró sorai (default:10)
- more szöveg kiírása oldalanként a terminálra
- less szöveg kiírása: a felhasználó mászkálhat benne

regxp – regular expressions

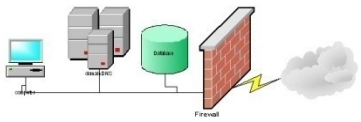
- grep szövegben keresés szabályok szerint
- (g)awk szövegben keresés/manipuláció
- sed szöveg egyszeri futás alatti szerkesztése
- vi klasszik szövegszerkesztő
- emacs legendás szövegszerkesztő



Accounting

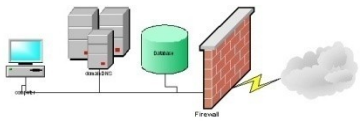
- Multiuser operációs rendszer
- Account:
  - felhasználónév azonosítja,
  - jelszó védi
- Password file:

  username:password:uid:gid:gecos:homedir:shell
- Kétféle account:
  - Root
  - User



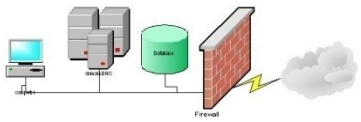
Accounting (cont)

- su — root átvált az adott userre/ré
- adduser — felhasználó hozzáadása
- passwd — jelszó megváltoztatása
- userdel — felhasználó törlése
- /etc/passwd — elem törlése



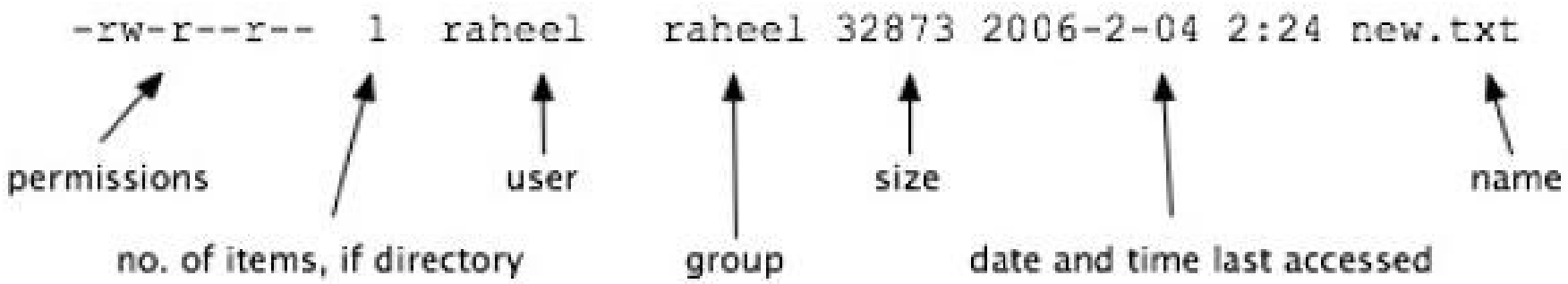
Authorization: ownership & access

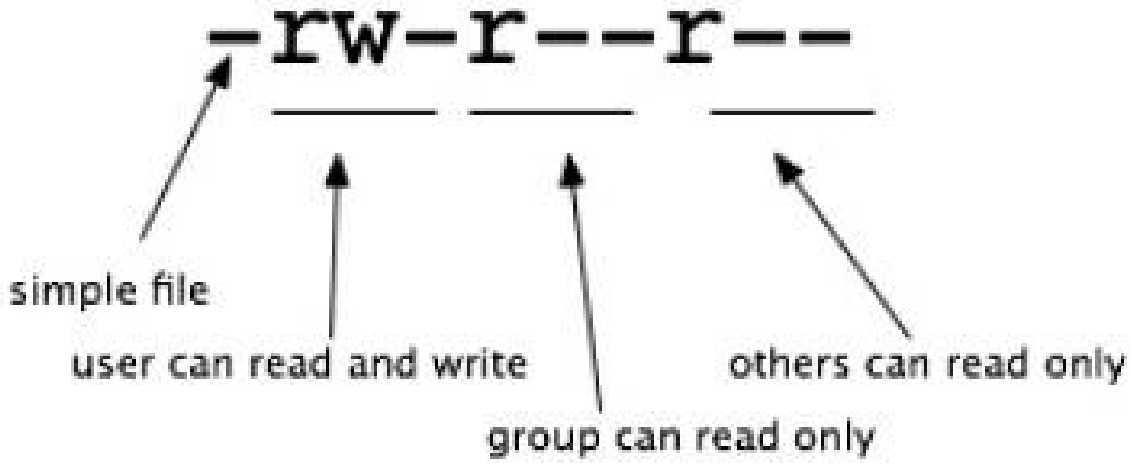
- Hozzáférés
  - Multi-user környezet!
  - Felhasználók nem férnek hozzá egymás file-jaihoz
  - Speciális file-okhoz csak a root fér hozzá
- Csoportok – groups
  - a felhasználók több csoporthoz tartozhatnak
  - könnyebb/rugalmasabb hozzáférés-kezelés
- Hozzáférés: felhasználók / csoportok / egyéb

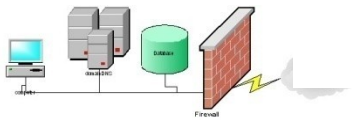


Hozzáférés - példa

- ls – l - parancs példa kimenete





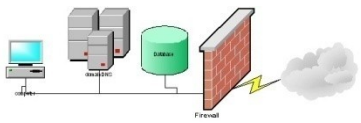


Ownership változtatás

- Ownership (birtoklás) változtatás: chown
  chown username file_or_dir

- Csoport-birtoklás változtatás: chgrp
  chgrp groupname file_or_dir

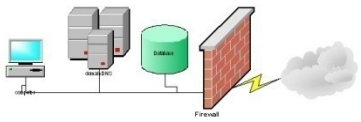
- Kombinált csoport és felhasználónév:
  chgrp name.name file_or_dir



Hozzáférés változtatás

- *chmod* parancs

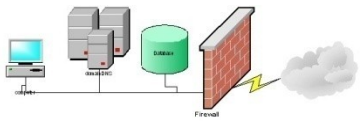
- *r, w, x: read, write, execute*
- *Root: megváltoztathatja bármely file/directory hozzáférés-szabályait*
- *A root mellett csak a birtokos (user) tudja változtatni*



SCRIPTING IN A (NUT)SHELL

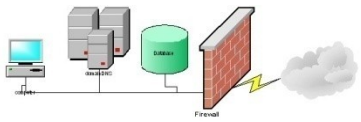
Bash

Ajánlott gyakorlatok:
http://linuxconfig.org/Bash_scripting_Tutorial



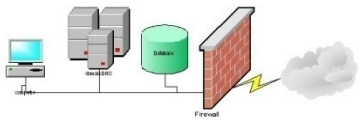
bash - „Bourne-again shell”

- a shell mindig elérhető (sh, bash, ksh,..)
- rendszergazdai script-ek: shell-ben
- összetettebb script-nyelvek (pl.)
  - Perl
  - Python
  - Ruby
- a script (v. interpreter-)nyelvek jellegzetességei
  - programkódja akár soronként is értelmezhető
  - minden futási időben értékelődik ki
  - string paramétert is képes értelmezni parancsként
  - típustalan változókezelés



processzek kommunikációs csatornái

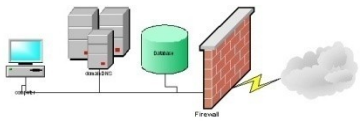
- Standard I/O, minden programnak
  - 0 – STDIN
  - 1 – STDOUT
  - 2 – STDERR
- Átirányítás
  - `tail file` #file→STDOUT
  - `tail file 2>&1` #STDERR→STDOUT
  - `tail file.o > file.n` #file.o→STDOUT→file.n
  - `tail file.o 2> file.n` #file.o→STDOUT, STDERR→file.n
  - grep ‘From’ < /etc/mail/laboruser #grep input: /etc/mail/laboruser



Csövezés: pipes

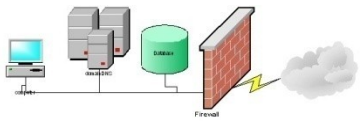
- `cat /etc/mail/laboruser | grep 'From'`
  `#cat STDOUT-ját a grep STDIN-be`
- `cat /etc/passwd | grep ‘:x:’ | sort`
  `#cat STDUT-ját a grep-en átszűrve a sort-ba`

- Láncolás pro és kontra:
  - Formázatlan bináris adatátadás!
  - Gyors, de strukturált adatot nem kezel
  - Strukturált adatot szöveges formába kell alakítani (valamilyen módon), majd a fogadó oldalon sorokra, majd azon belül mezőkre bontva feldolgozni
  - Erre használható programok: cut, awk, sed



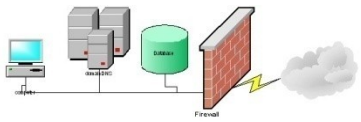
bash: változók és nevek

- A változónevekre nincs külön jelölés
  - etcdir='/etc' # de ne legyenek space-ek a = körül!! (command)
- $-előtét, ha a változó értékét hivatkozzuk
  - echo $etcdir
- Egyéb szövegtől elválasztható {} jelekkel:
  - echo ”Saved ${rev}th version of file”



bash: tömbök

```
ARRAYVAR=(ERTEK1 Ertek2 "Ertek3");        #értékadás #felsorolással
OTHERARRAY[5]= "Ertek4";        #értékadás konkrét indexre, ritka tömb

echo "elemszam: ${#ARRAYVAR[@]} ";
echo "elso elem $ARRAYVAR";

   #for ciklus az összes elemre, figyeljünk a ;-k helyére!
   #ritka tömbnél így nem működik!
for ((i=0;i<${#ARRAYVAR[@]};i++));
do
   echo "${ARRAYVAR[$i]}";
done;
```

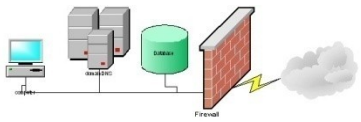



Az 'aposztrófok'

(legyen: mysport=chess)

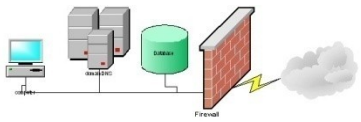
- A dupla-idézőjel kifejtő funkciójú
  - echo ”I play ${mysport}.” # I play chess.
- a szimpla nem fejti ki a változót
  - echo 'I play ${mysport}.' # I play ${mysport}.
- a `backtickek`
  - közé írt parancssor standard outputját a shell végrehajtja és behelyettesíti
  - echo ”There are `-wc –l < /etc/passwd` lines in the passwd file.”

    # There are 28 lines in the passwd file.



Speciális változók, paraméterek

- Bemenő paraméterek
  - `$1, $2` … - bemenő paraméterek
  - `$#` - paraméterek száma
  - `$@` - paraméterek tömbje
- Előző parancs
  - `$?` – legutóbbi futtatott parancs visszatérési értéke
  - `$!` – legutóbbi háttérben indított folyamat PID-je
  - `$$` - éppen futó shell PID-je
- Mezőelválasztó karakter
  - `$IFS` – ennek az értéke alapján automatikusan darabolja a stringeket külön paraméterekké
  - Alapból az IFS értéke minden whitespace `” ” ”\n” ”\t”`



Néhány általános szűrő

- cut - sorokat mezőnként szétválasztja
- sort - sorbarakja a sorokat

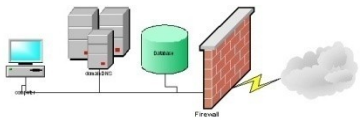
  -f : case sensitive sort

  -k : key column for sorting

  -n : fields are integer numbers

  -r : reverse sort order

  -u: otput unique records only
- unique - az egyedi sorokat írja ki
- wc - word count (-l, -w, -c vajon mi…)
- tee - kétfelé küldi a bemenetét



bash scripting

((a helloworld file tartalma:))

```
#!/bin/bash
echo ”Hello, world!”
```

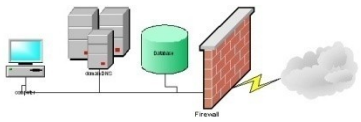
((beírjuk a shell-be:))

chmod +x helloworld

./helloworld

((kiírja a shell:))

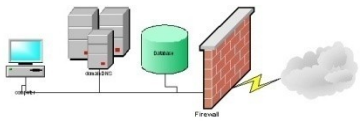
Hello, world!



Elágazások

```
#!/bin/bash
if [ "foo" = "foo" ];
then
    echo expression evaluated as true
else
    echo expression evaluated as false
fi
```

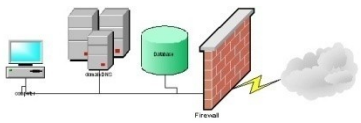
http://tldp.org/HOWTO/Bash-Prog-Intro-HOWTO.html



Ciklusok

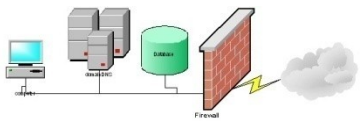
```
#!/bin/bash
for i in $( ls ); do
    echo item: $i
done
```

```
#!/bin/bash
COUNTER=0
while [ $COUNTER -lt 10 ]; do
    echo The counter is $COUNTER
    let COUNTER=COUNTER+1
done
```

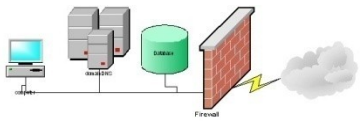



bash scripting hozzáállás: egy hasznos módszer

1. Fejlődjön a script lépésről lépésre, mint egy **pipeline**, végig a **command line**-ban
2. Mindent küldjünk a STDOUT-ra, hogy lássuk, minden rendben megy-e
3. A lépéseknél használjuk a shell command history-t és így szerkesszük tovább a parancsokat
4. Mindaddig, míg a kimenet nem tökéletes, lehet finomítani, semmi undo-ra nincs szükség
5. Amint megfelelő a kimenet, hajtsuk végre a konkrét parancsokat, így ellenőrízve, hogy tényleg rendben
6. Használjuk az **fc**-t a munka befejezésekor, letisztázásra, mentésre



ÁLTALÁNOS LABORISMERETEK

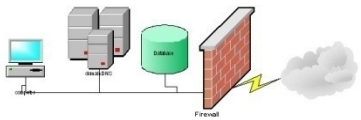


Általános laborismeretek

- VMWARE - Váltás a gazdagépre: **Ctrl+Alt**

- A feladatok mellett: hint
  - Milyen parancsot használjunk:
    man it!
    Google it!
  - Parancsok opciói/kapcsolói/szintaxisa: helyben kitalálandó!

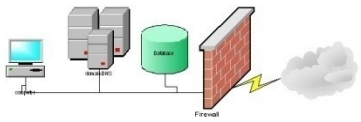
- Hasznos felkészülés
  - Alap Linux a HSZK-ban / otthon
  - SQL ismétlés otthon… (help)



Labor bemelegítés

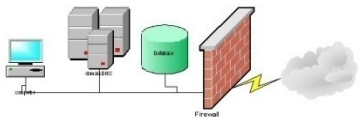
- Körbenézés: **mc**

- Hálózati kapcsolatok: **netstat**
  - Kapcsolók..!
- Tűzfalszabályok: **iptables**
  - Kapcsolók..!



Labor: felhasználókezelés

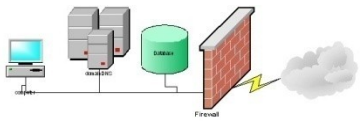
- visudo – rendszergazda jogokhoz
- felhasználói jogok:
  - /etc/passwd
- file-hozzáférés
  - chmod
  - chown
  - chgrp



MySQL

- help ☺

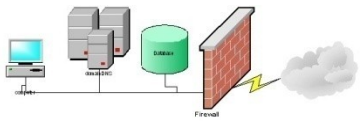
- describe
- show
- show grants
- select
- insert



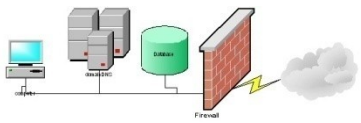
Címtár / LDAP

- http://tldp.org/HOWTO/LDAP-HOWTO/

- ldapsearch
- ldapadd
- ldappasswd

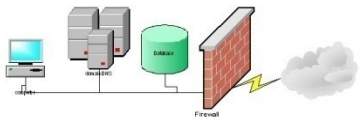


SCRIPTING BEST PRACTICES

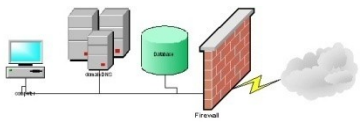


Mitől lesz még jobb a script?

- Ha rosszul használják: usage v. –help hint!
- A bemeneti változókat ellenőrzi (sanity check)
- Használ visszatérési értéket: 0 – siker; egyékként más
- Változók, rutinok elnevezése következetes;
  - nem hosszú, és szeparált (_) nevek
- Felismerhető a stílus projekten v. csapaton belül
- Comment-block-kal kezdődik, alapadatok itt vannak (név, utolsó módosítás, milyen bővítményt használ, stb.)
- Comment for programmers, not dummies
- Figyelmes futtatás: bash –x ; perl –w …



IT Szolgáltatások

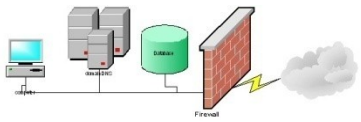


IT Szolgáltatások

Általános kívánalmak

&

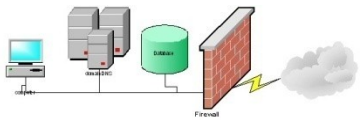
alapelvek



IT Szolgáltatások - áttekintés

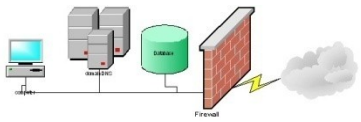
- A vállalaton belül az IT feladatok több szinten jelentkeznek
- Példa: *egy* vállalat, *egy* IT csoport
- IT szolgáltatások
  - Megtervezése
  - Beüzemelése
  - Fejlesztése
    - Megbízhatóság!
    - Skálázhatóság!
  - Felügyelete (*Monitorozás*!)
  - Karbantartása
  - ...Támogatása...

„Ha egy >>szolgáltatás<< nincs monitorozva,
akkor az még nem Szolgáltatás.”



IT szolgáltatások – áttekintés ‘2

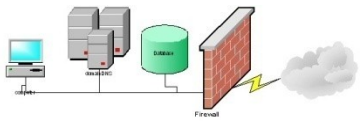
- A vállalati környezetet keresztülfonják...
- Alapszolgáltatások (kritikus és látható)
  - Hálózati kapcsolódás
  - DNS
  - **Email**
  - Authentikáció
  - **Távoli elérés**
  - **Nyomtatás**
- További szolgáltatások
  - Fejlesztői eszközök
  - Licensz-kezelés
  - Megosztott tárterületek
  - Megosztott naptár
  - Backup szolgáltatások,....stb.



Alapkérdések

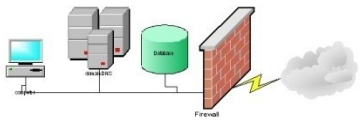
- Megbízhatóság
- Felhasználói kívánalmak
- Szerver minőségű gépek, szerverterem
- Szerverek alaptulajdonságai
  - egyszerűség
  - jelentős védelem (security)
- Szolgáltatások függősége
  - pl: vállalati ügymenet - email - DNS – hálózat
  - pl2.: authentikációs szolgáltatástól
- Hozzáférés a szervergépekhez: csak „SA”

Ha alapszolgáltatás leáll, a tőle függő is érintett!



Alapkérdések „alap”-kezelése

- A jól karbantartható szolgáltatás legyen
  - Egyszerű
  - Kevés függőséget tartalmazó
  - „Szabványos” hadveren
  - „Szabványos” szoftverekkel
  - Szabványosított konfigurációkkal
  - Dokumentált, egy „szabványosított” helyen
  - Független a gazdagép hardverétől
    - Használjunk *szolgáltatásneveket* a klienseken!

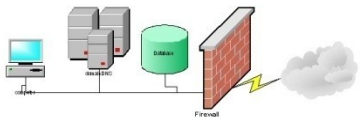


Felhasználói kívánalmak

- Nekik építjük a szolgáltatásokat: legyen nekik tetsző!
- Derítsük ki az elvárásaikat – racionális határokon belül valósítsuk is meg.
- Definiáljuk és hirdessük a

  szolgáltatás szintjét (SLA)

  – ezzel elkerülhetők a félreértések
- Tisztázzuk a felhasználókkal, hogy melyik *SLA* miért és mennyire limitált



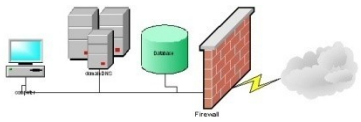
Működ(tet)ési kívánalmak

- **Vastag (fat) kliens**
  - Az applikáció főleg a felhasználói gépen fut
- **Vékony (thin) kliens**
  - Az applikáció jelentős része szerver(ek)en fut

Mindkettőnél számos működtetési /karbantartási nehézséggel találkozhatunk!

- **Frissítési módszer (upgrade path)**

- Mennyire
  - támaszkodik a **hálózatra**?
  - terheli a **hálózatot**?

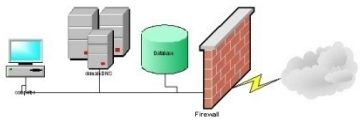


Nyílt - vs. – Saját komponensek

- Ha lehet, használjunk
  - Standard
  - Nyílt
  - Alaposan és bizonyítottan tesztelt

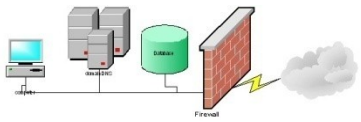
  komponenseket
- *Protokoll*
  - ez maga a kommunikációs forma leírása (lehet szabványosított)
  - „bővített protokoll” – ez rossz jel: eltér a szabványtól
- *Protokoll-megvalósítás*
  - ez egy termék (része), a szabványtól *vszg.* ***eltér***
  - *két protokoll-megvalósítás ritkán „érti meg egymást” tökéletesen*
- *Protokoll-átalakító (gateway)*
  - *Néha szükséges, de alapvetően kerülendő (SPF)*

Single Point of Failure



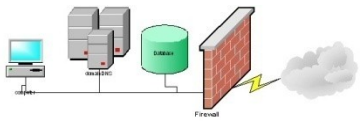
Egyszerűség

- Tervezzünk/építsünk egyszerű dolgokat
- Szorítkozzunk az alapfunkcióra
  - kevés (be?- / át!-) állítási lehetőséggel
- A rendszer növekedtével úgyis komplex lesz



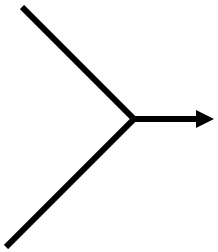
Megbízhatóság

- *Egyszerűség*...!
- Redundancia
  - Redundáns hardver; hatékony kihasználás
    - Pl: egy gép két tápegységgel – külön áramforrásra
    - ...külön telephelyeken!
- A nem-redundáns szolgáltatás-elemek
  - Legyenek nagyon összefogottak
    - Kisebb függőség, kevesebb SPF
    - Azonos tápellátás
    - Azonos hálózati elemek/kiszolgálók
- Kisebb-nagyobb kimaradások
  - Soft outage / hard outage



Centralizáció és Szabvány-megoldások

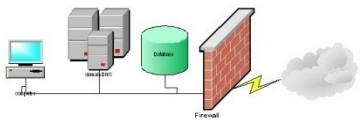
- Karbantarthatóság, követhetőség, ár szempontjából megfontolandó:
  - Eszközök (tools)
  - Alkalmazások
  - Szolgáltatások



Centralizáció

- Földrajzi vagy szervezeti határokat nem fontos átlépni

  (több centrális pont lehet)



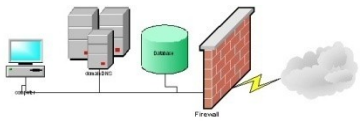
Teljesítmény

- „Működik”... és elég gyors-e?

  - Megbízható
  - Funkcionálisan megfelelő
  - Kellemes a GUI
  - ...

- Az elvárások fokozódnak, amint a hálózatok, grafika, processzor,... Gyorsul
- Rossz kapacitásterv – rossz *első élmény*
  - Szerver választáskor:
    - Lemezkapacitás?
    - Memória?
    - Processzor?

→ Szolgáltatás igényeihez

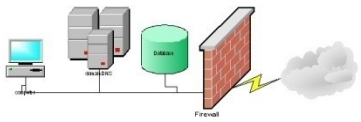


Szolgáltatás-felügyelet

...Monitoring...!

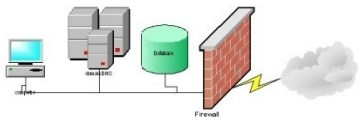
lásd pl.

- Fault Mgmt,
- Performance Mgmt

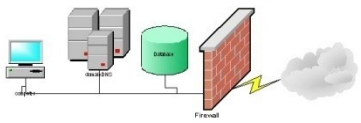


Túl a...

- Extra odafigyelés -> extra eredmények
  - Szolgáltatás beüzemeléskor
    - Teljes dokumentáció elérhető
    - Oktatás
    - A kisegítő és támogató személyzet felkészült
  - Dedikált gépek szolgáltatásonként
  - Teljes redundancia
    - A szolgáltatás egészét át tudja venni egy másik szerver(csoport)



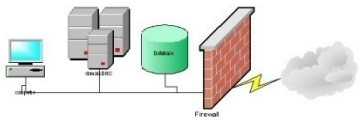
E-mail szolgáltatás



Nem kapta meg az e-mailt?!

- Egész vállalatok *nyugszanak* *megbízható* e-mail szolgáltatáson

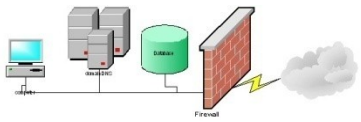
- Emellett...
  - Skálázható
  - Egyszerű, világosan áttekinthető
  - Általános és egységes
  - Automatizált
  - Biztonságos
  - Archivált
  - Ha változik, az jól kommunikáltan zajlik



Az e-mail küldés lépései

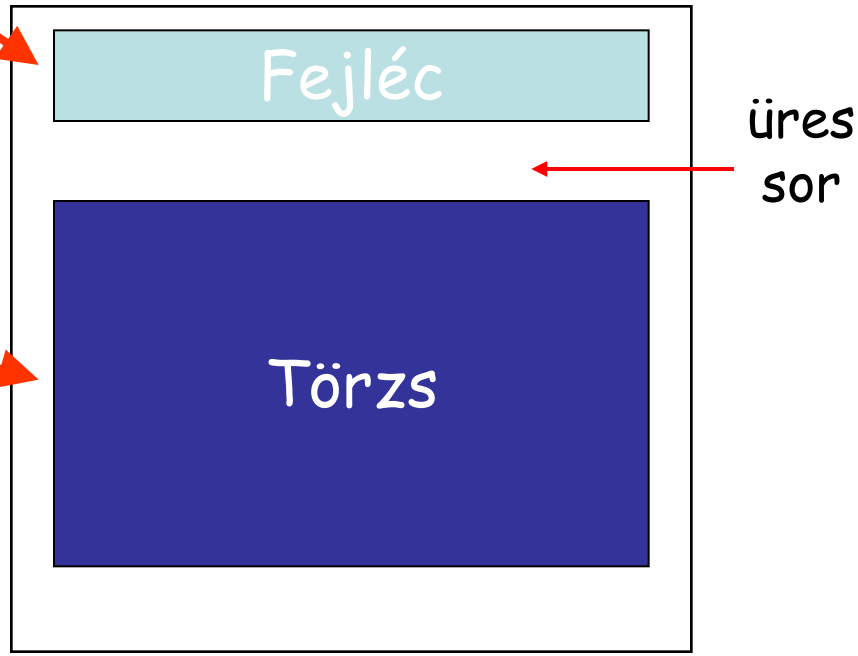
Különböztessük meg:

- Üzenettovábbítás
  - Ahogyan az e-mail szerverről szerverre jut
- Kézbesítés
  - Amikor az email a fogadó mailbox-ába kerül
- Üzenet-listák feloldása
  - Amikor a listacímre küldött levél megsokszorozódik és így kerül továbbításra



E-Mail üzenetformátum (RFC 822)

- Az üzenet két részből áll
  - Fejléc (header), kódolás: 7-bit U.S. ASCII text
  - Törzs (body), szintén 7-bit U.S. ASCII text
- Fejléc (header)
  - “type: value” alakú sorok
  - “To: iru.bme@gmail.com”
  - “Subject: Meresek”
- Törzs (body)
  - A szöveges üzenet
  - Nincs különösebb struktúrája

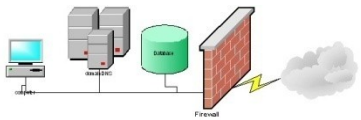


Megszorítás: Nem-szöveges adat küldése...

- E-mail törzs 7-bit U.S. ASCII
  - És ha valaki nem *angol* **szöveget** szeretne küldeni?
  - ...bináris állományok (pl. Képek, .exe-k) ?
- Megoldás: konvertáljunk... nem-ASCII -> ASCII
  - Base64 kódolás: minden 3 byte-ot alakítsunk 4 nyomtatható U.S.-ASCII karakterré
  - Uuencode (Unix-to-Unix Encoding) elterjedt

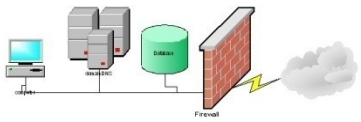
```
begin 644 cat.txt
#0V%T
`
end
```

  - Korlát: a file-név az egyetlen „tipp” az adat típushoz...



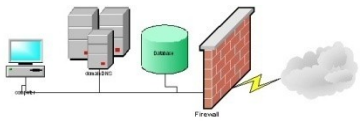
Megszorítás: Több adategység küldése

- A felhasználók gyakran akarnak több(féle) adatot küldeni egy üzenetben
  - Több kép, powerpoint file, vagy e-mail üzenet
  - Mégis, az e-mail törzse egyetlen adattömeg
- Példa: e-mail digest
  - Több e-mail üzenetet egy nagy üzenetbe csomagolhatunk
  - Nagy volumenű e-mail listákon gyakran használják
- Több megoldás született a részek szétválasztására
  - Pl. „közismert” elválasztó-sztring a részek között
  - Mégis, jó lenne egy szabványos módszer...

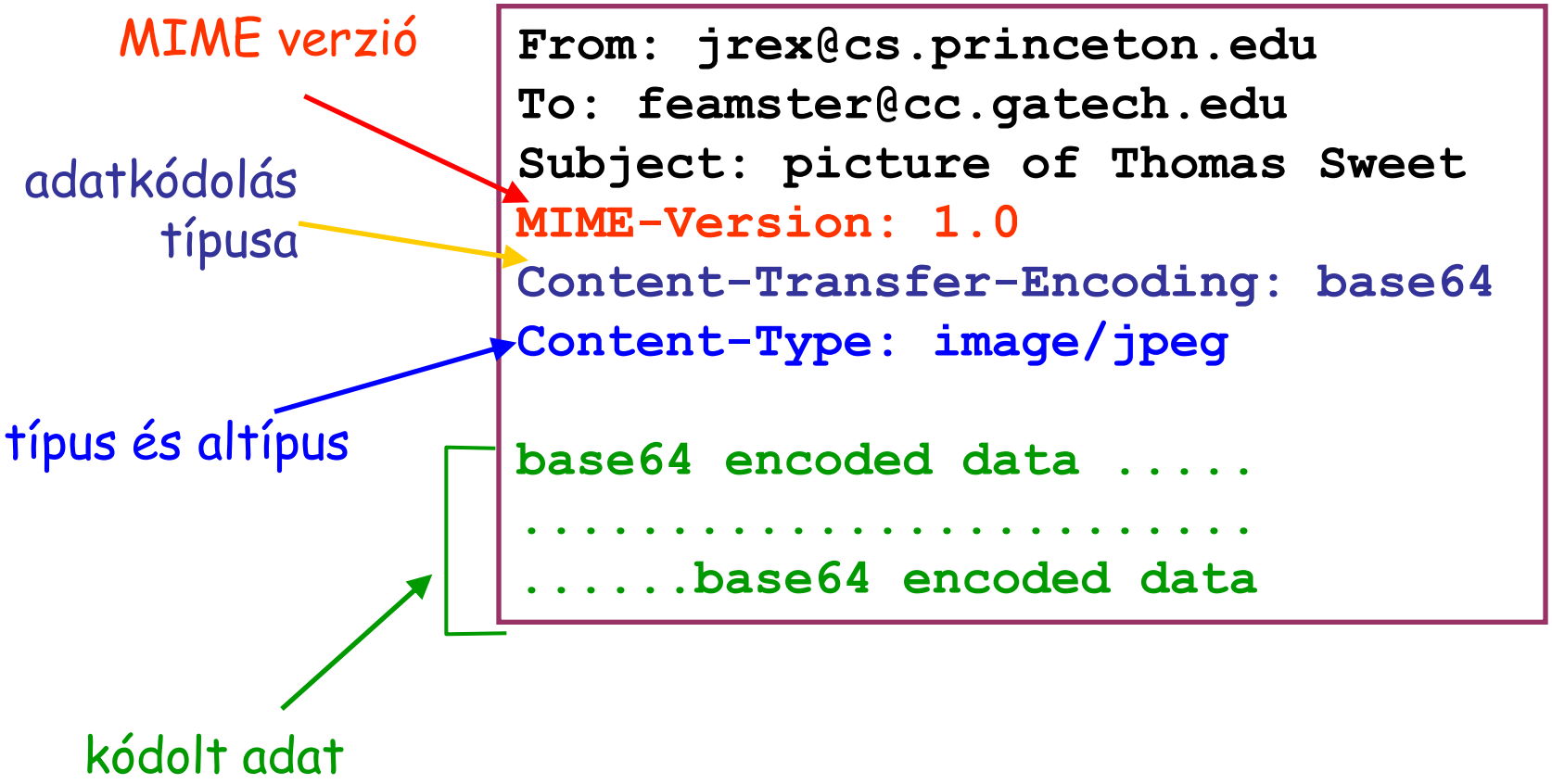


Multipurpose Internet Mail Extensions

- Hozzáadott fejlécek a törzs leírására
  - MIME-Version: melyik MIME verziót használja
  - Content-Type: milyen adattípus van a törzsben
  - Content-Transfer-Encoding: hogyan kódolt az adat
- Tartalom-típusok és altípusok definíciói
  - Pl. image – altípus: gif, jpeg
  - Pl. text – altípus: plain, html, és richtext
  - Pl. application – altípus: postscript és msword
  - Pl. multipart – több adattípust tartalmazó üzenet
- Hogyan kódolja az adatot ASCII formátumban?
  - Base64 kódolással, mint: uuencode/uudecode

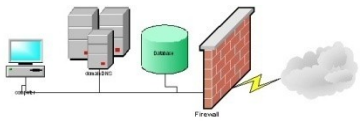


Példa: E-Mail üzenet MIME-olva

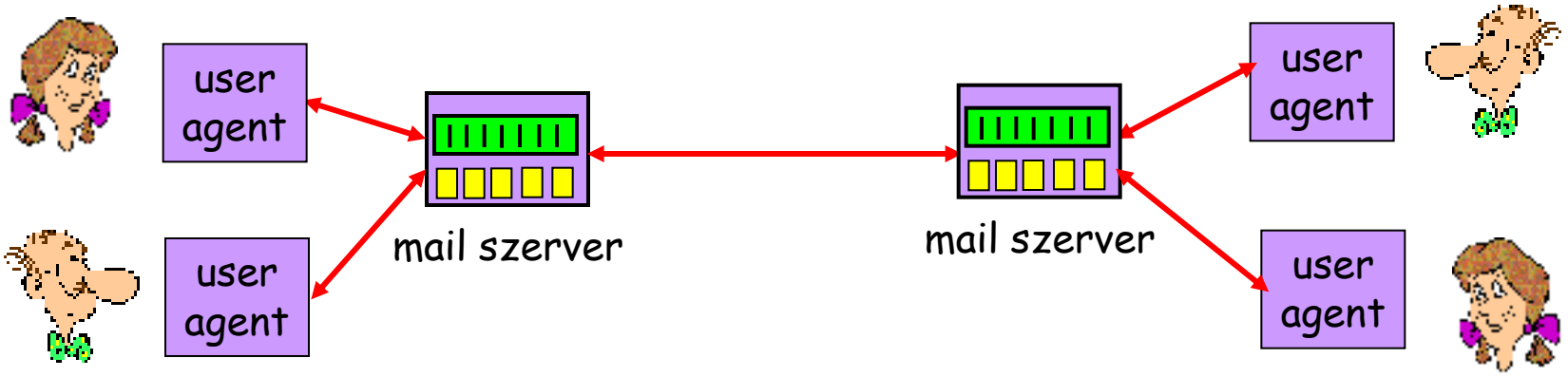


E-Mail címek

- Az e-mail cím komponensei
  - Helyi mailbox (pl. pvarga vagy john.smith)
  - Domain név (pl. tmit.bme.hu)
- A domain név nem feltétlenül a mail szerveré
  - A mail szervernek lehet hosszabb/titkosított neve
    - Pl. tmit.bme.hu vs. mail.tmit.bme.hu
  - Több szerver is lefedheti (hibatűrés)
    - pl. cnn.com vs. atlmail3.turner.com és nycmail2.turner.com
- A domain-hez tartozó mail szerver azonosítása
  - DNS kérés, MX rekordokért (Mail eXchange)
    - Pl.: nslookup -q=mx tmit.bme.hu
  - Aztán hagyományos DNS kérés az IP címért



Mail Szerverek és User Agent-ek



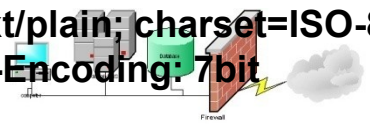
- Mail szerverek
  - Mindig bekapcsolva és mindig hozzáférhetően
  - e-mail „szállítása” más szerverektől / szerverekhez
- User agents
  - Néha bekapcsolva és néha elérhetően
  - A felhasználó felé különféle interfészekkel

SMTP
Store-and-Forward Protocol

- Az üzeneteket szerverek sorozata szállítja
  - A szerverek a bejövő üzeneteket sorokban tárolják
  - … és amikor alkalom adódik, továbbítja a következőnek (next hop)
- Ha a következő nem elérhető
  - A szerver tárolja az üzenetet; később újra próbálkozik
- Minden „hop” beírja az azonosítóját az üzenetbe
  - A “Received” fejléc így sokat segít a hibák keresésekor

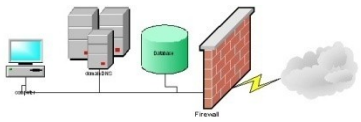
Példa, **Received** Header-rel

Return-Path: <casado@cs.stanford.edu>
Received: from ribavirin.CS.Princeton.EDU (ribavirin.CS.Princeton.EDU [128.112.136.44])
by newark.CS.Princeton.EDU (8.12.11/8.12.11) with SMTP id k04M5R7Y023164
for <jrex@newark.CS.Princeton.EDU>; Wed, 4 Jan 2006 17:05:37 -0500 (EST)
Received: from bluebox.CS.Princeton.EDU ([128.112.136.38])
by ribavirin.CS.Princeton.EDU (SMSSMTP 4.1.0.19) with SMTP id M20060104170536079 46
for <jrex@newark.CS.Princeton.EDU>; Wed, 04 Jan 2006 17:05:36 -0500
Received: from smtp-roam.Stanford.EDU (smtp-roam.Stanford.EDU [171.64.10.152])
by bluebox.CS.Princeton.EDU (8.12.11/8.12.11) with ESMTP id k04M5XNQ005204
for <jrex@cs.princeton.edu>; Wed, 4 Jan 2006 17:05:35 -0500 (EST)
Received: from [192.168.1.101] (adsl-69-107-78-147.dsl.pltn13.pacbell.net [69.107.78.147])
(authenticated bits=0)
by smtp-roam.Stanford.EDU (8.12.11/8.12.11) with ESMTP id k04M5W92018875
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT);
Wed, 4 Jan 2006 14:05:32 -0800
Message-ID: <43BC46AF.3030306@cs.stanford.edu>
Date: Wed, 04 Jan 2006 14:05:35 -0800
From: Martin Casado <casado@cs.stanford.edu>
User-Agent: Mozilla Thunderbird 1.0 (Windows/20041206)
MIME-Version: 1.0
To: jrex@CS.Princeton.EDU
CC: Martin Casado <casado@cs.stanford.edu>
Subject: Using VNS in Class
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 7bit



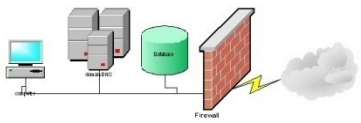
Többszörös Szerver-átadás (hops)

- Tipikusan legalább két mail szerver
  - Küldő és fogadó-oldal
- Lehet több is
  - Külön szerverek a kulcsfunkciókra
    - Spam szűrés
    - Vírus scan
  - Üzenet-átirányító szerverek
    - pvarga@tmit.bme.hu -> pvarga@alpha.tmit.bme.hu
  - Elektronikus üzenet („mailing”) listák
    - Az üzenet a listaszerverhez továbbítódik
    - … és onnan a lista kibomlik -> minden listatag felé

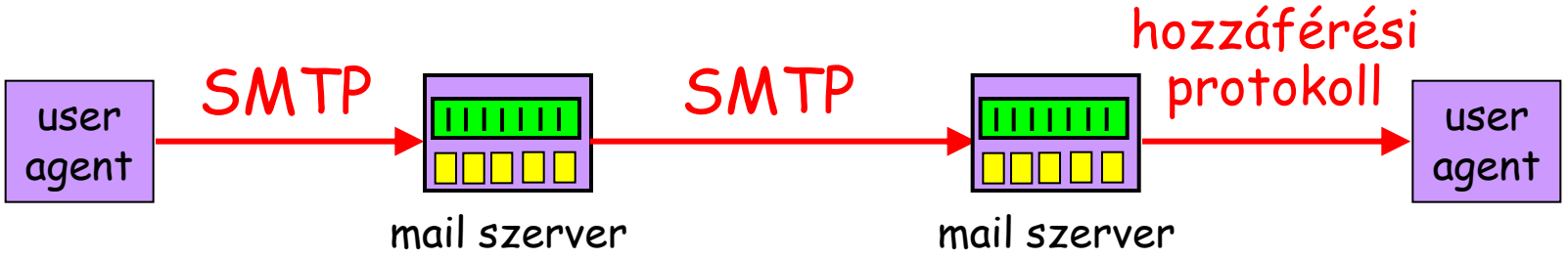


Elektronikus üzenet-listák

- Felhasználói csoportok egy cím alatt elérhetőek
- Üzenetrobbanás
  - Egyetlen e-mail-ből sok-sok elküldött üzenet lesz
  - Fogadónként egy üzenetmásolat
- Visszapattanó üzenetek kezelése
  - Számos oka lehet a visszapattanásnak
  - Pl. fogadó mailbox nem létezik; erőforrások korlátosak,...
- E-mail digest-ek
  - Az üzenet-lista leveleinek elküldése *egy*ben
  - Az üzeneteket elválasztó karaktersorok határolják
  - … vagy multiple/digest formában küldődnek el



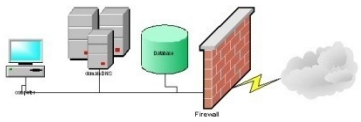
Simple Mail Transfer Protocol



- Kliens-szerver protokoll
  - A *Kliens* a küldő mail szerver
  - A *Szerver* a fogadó mail szerver
- Megbízható adattovábbítás
  - TCP fölött halad (on port 25)
- „Push” protokoll
  - A küldő szerver benyomja a file-t a fogadó szerverbe
  - … ahelyett, hogy kivárná, amíg a fogadó elkéri

Simple Mail Transfer Protocol (folyt.)

- Command/response
  - Command: ASCII text
  - Response: 3-digites státusz-kód és szöveg
- Szinkron
  - A küldő vár a „command”-ra választ (response)
  - … mielőtt kiküldi az új „command”-ot
- A továbbítás három fázisa
  - Handshaking (üdvözlet)
  - Üzenettovábbítás
  - Lezárás



Eset:
Anna üzenetet küld Bélának

1) Anna az UA-t használja, hogy üzenetet írjon ide: **beela@nagyceg.com**

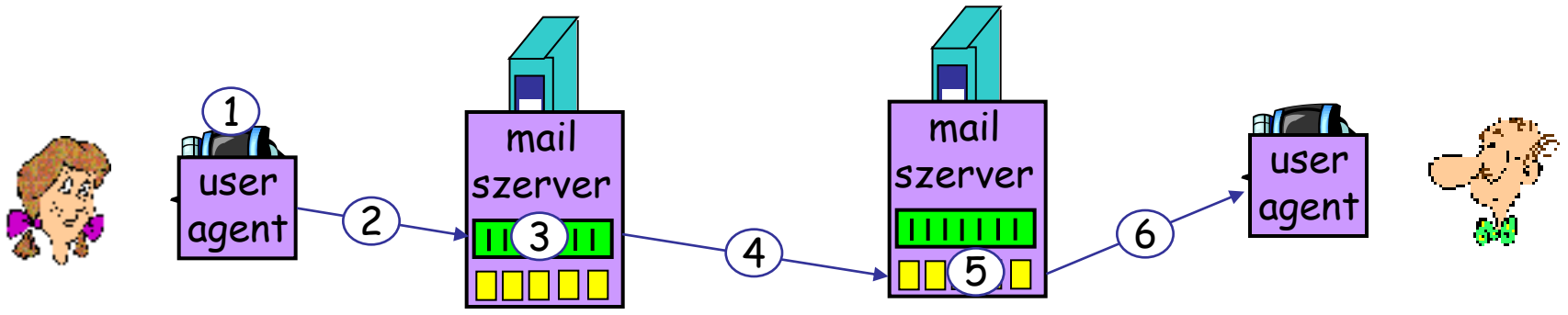
2) Anna UA-je üzenetet küld a mail szerverének; az üzenet bekerül egy sorba

3) A kliens oldali SMTP egy TCP kapcsolatot nyit Béla mail szerverével

4) Az SMTP kliens átküldi Anna üzenetét a TCP kapcsolaton

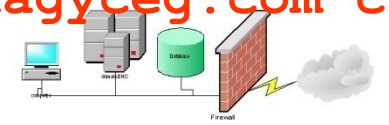
5) Béla mail szervere berakja az üzenetet Béla postaládájába (mailbox)

6) Béla aktiválja az UA-ját az üzenet elolvasásához



Példa SMTP üzenetváltásra

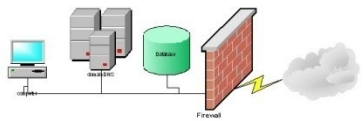
```
S: 220 nagyceg.com
C: HELO segitokez.hu
S: 250  Hello segitokez.hu, pleased to meet you
C: MAIL FROM: <anna@segitokez.hu>
S: 250 anna@segitokez.hu... Sender ok
C: RCPT TO: <beela@nagyceg.com>
S: 250 beela@nagyceg.com ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Dear Beela,
C: Thank you for the flowers!
C: Anna
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 nagyceg.com closing connection
```



E-Mail lekérése a Szervertől

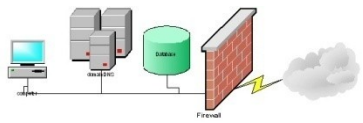
- A szerver mailbox-onként tárolja a bejövő leveleket
  - Az üzenet “To” mezője alapján válogatja szét
- A felhasználónak le kell kérni (retrieve) az e-mailt
  - Aszinkron módon a küldési időhöz képest
  - ...úgy, hogy megnézhesse és válaszolhasson
  - ...úgy, hogy rendszerezhesse és tárolja az üzeneteket

- Bezzeg a régi szép időkben…
  - A felhasználó belépett a gépre, ahová az üzenet továbbítódott
  - A felhasználók a munkahelyi gépükön nézték a mail-t



A PC-k hatása az E-Mail lekérési módszerekre

- Külön gép személyes használatra
  - A felhasználók nem akarnak belépni távoli gépekre
- Erőforrás-korlátok
  - A legtöbb PC-nek nincs elég erőforrása, hogy teljes e-mail szerverként működjön
- Időszakos kapcsolódás/elérhetőség
  - A PC-k ritkásan kacsolódnak a hálózatra
  - ...az Internet-kapcsolat jellege, valamint a PC be/kikapcs miatt
  - A szervernek túl sokat kellene feleslegesen próbálkoznia
- És lőn: Post Office Protocol (POP)

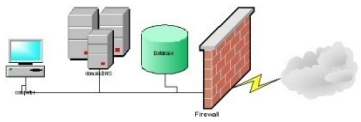


Post Office Protocol (POP)

- POP célok
  - Időszakosan kapcsolódó felhasználók igényeihez alkalmazkodik
  - Tegye lehetővé az e-mail-jeik leszedését amikor kapcsolódnak
  - … és megnézhesse/manipulálhassa őket, amikor nincs csatlakozva

- Tipikus user-agent interakció a POP szerverrel
  - Kapcsolódás a szerverhez
  - Minden e-mail leszedése (Retrieve)
  - Az üzenetek „Új”-ként való tárolása a PCn
    - Letörölhesse az üzeneteket a szerverről
  - Kapcsolat lezárása a szerverrel

- Az UA még SMTP-t használ az üzenetküldéshez



POP3 Protokoll

Authorizációs fázis

- Kliens „command”:
  - **`user:`** felhasználónév
  - **`pass:`** password
- Szerver „response”
  - **`+OK`**
  - **`-ERR`**

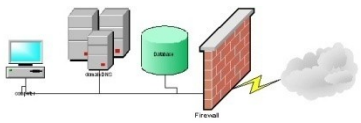
```
S: +OK POP3 server ready
C: user beela
S: +OK
C: pass nagyfonokvagyok
S: +OK user successfully logged on
```

Tranzakciós fázis,

kliens:

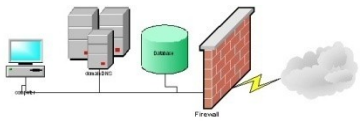
- **`list:`** számozva listázza az üzeneteket
- **`retr:`** a szám alapján leszedi őket
- **`dele:`** delete (törlés)
- **`quit`**

```
C: list
S: 1 498
S: 2 912
S: .
C: retr 1
S: <message 1 contents>
S: .
C: dele 1
C: retr 2
S: <message 1 contents>
S: .
C: dele 2
C: quit
S: +OK POP3 server signing off
```



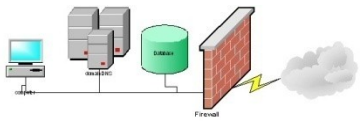
A POP korlátai

- Nem könnyen kezel többszörös mailbox-okat
  - A felhasználó bejövő e-mailjeinek egy helyre rakására tervezve
- Nem az üzenetek szerveren tárolására tervezték
  - ...hanem az üzenetek kliensre való letöltésére
- A mailboxhoz a többszörös kliens-hozzáférés nehéz
  - Egyre fontosabb, mivel a felhasználónak van otthoni, munkahelyi PC-je, laptopja, cyber café-beli, barátnál levő gépe, stb.
- Nagy hálózati sávszélességet igényel
  - Minden üzenetet átvisz, gyakran sokkal elolvasásuk előtt (...és lehet, hogy sosem lesznek elolvasva...)



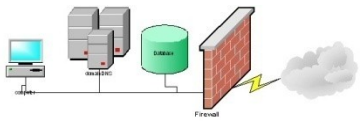
Interactive Mail Access Protocol (IMAP)

- „Connected” és „Disconnected” módok támogatása
  - A felhasználók igény szerint tölthetik le az üzenetet
- Egyszerre több kliens is csatlakozhat a mailboxra
  - Detektálja a más kliensek által a mailbox-on történt változtatásokat
  - A Szerver figyeli és tárolja az üzenet állapotát (pl. olvasatlan, olvasott, megválaszolt)
- Hozzáférés az üzenetek MIME részeihez & részleges letöltés
  - A kliensek darabonként is leszedhetik a MIME részeket
  - Pl. Az üzenet szöveges részét – a csatolmány letöltése nélkül



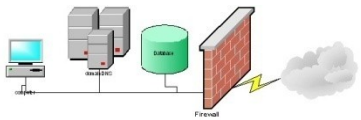
Interactive Mail Access Protocol (IMAP) folyt.

- Többszörös mailbox-ok a szerveren
  - A kliens tud létrehozni, átnevezni, és törölni mailboxot
  - A kliens tud egyik folderből másikba áthelyezni üzenetet
- Szerver-oldali keresések
  - Az üzenet letöltése előtt a szerveren lehet keresést indítani rá



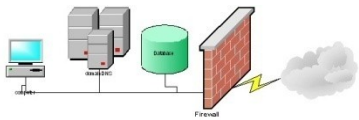
Webes E-Mail

- User agent: hagyományos Web browser
  - A felhasználó HTTP-n kommunikál a szerverrel
  - Pl.: Gmail, Yahoo mail, Hotmail, freemail,...
- E-mail olvasás
  - A Weboldalak a folderek tartalmát jelenítik meg
  - … és lehetővé teszik az üzenetek megnézését, letöltést
  - “GET” kérés a különféle Weboldalak megjelenítéséhez
- E-mail küldés
  - A szöveget egy „form”-ba írjuk, majd „submit” a szervernek
  - “POST” kérés és adatfeltöltés a szerverhez
  - A Szerver SMTP-vel küldi az üzenetet más szerverhez
- Könnyű az anonymous e-mail (pl. spam) küldése



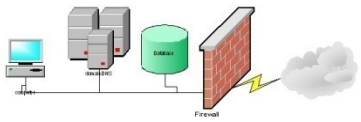
Az IT-crowd e-mailt szolgáltat a Vállalatnak

- Tudod, hogyan kell, Morris?!
- *Tudom; standard protokollok, meg biztonság..*
- És még ezek is:



Privacy Policy

- A hely e-mail policy-jével mindenki legyen tisztában (...és fogadja el...)
- Előfordulhat, hogy diagnosztikai okokból az SA turkál a levelek között
- Előfordulhat, hogy nem csak diag.....
- A vezetőség dönthet úgy, hogy privát levelek küldését céges címről *nem támogatja*
- Akárhogyan is,... Az SA-nak meg kell valósítani a privacy policy-t

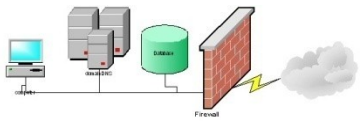


Namespace-ek

- Az e-mail cím a vállalat namespace-ének egyik legláthatóbb része
  - Fontos, hogy rendesen működjön
- Ugyanaz legyen a belső és a külső e-mail cím
- Legyen standard címformátum
  - Pl. first.last

    john.smith: nem biztos, hogy jó/egyedi
  - Pl. Rövidítés vagy azonosító

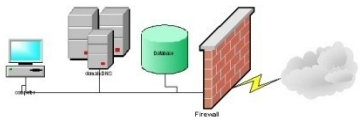
    jsmith, pvarga, lkovacs, lakovacs



Megbízhatóság

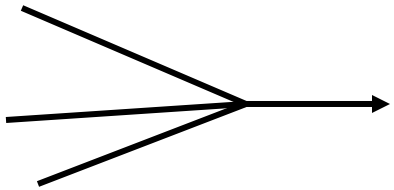
- Az e-mail alapeszköz. Mindig Jól Működjön.
- A rossz e-mail rendszer sokba kerül.
  - Elveszett levél.... Üzleti pánik

- Melegtartalék az egész rendszerről
  - Ha nem lehetséges („drága”):
- Készenléti terv, begyakorolt lépések a hibából való helyreállásra



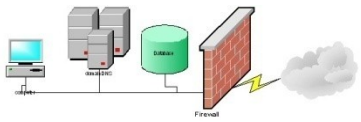
Egyszerűség

- Korlátozzuk a szükséges gépek számát
- Ne használjunk desktop PC-ket (csak az UA)
- Kis telephely:
  - üzenettovábbítás
  - kézbesítés
  - listakezelés



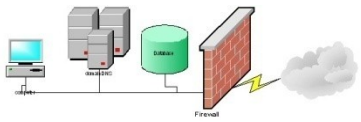
egy gépen

- Nagy telephely:
  - ezek külön gépeken / gép-csoportokon
  - a desktop gépek és nem-email szerverek SMTP portja legyen letilva
- Kerüljük a protokoll- vagy formátum-gateway-ek használatát



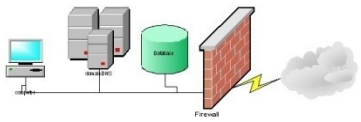
Automatizáltság

- Az e-mail account létrehozása legyen az általános account-készítési folyamat része
- ...az eltávolítás is hasonlóképpen
- A búcsúzó kollegák e-mailjeit nem forwardoljuk; listákról töröljük
  - Érzékeny információ kerülhet rossz helyre
  - ...inkább jelezzük automatikusan, hogy „vége”
- Accountok másolása szerverek között
- Listák adminisztációja (létrehozás, törlés, módosítás) – a felhasználók, s nem az SA részére



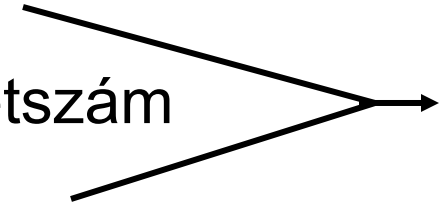
Monitorozás

- Minden, az e-mail küldésben részt vevő gépet figyeljünk
- Hálózat: **ping** (ICMP **echo** üzenetet küld)
- Tárterület (disk out of space...)
- TCP 25-ös port elérhető?
- Kézbesítéshez használt protokollok üzeneteit jól kezeli?
- Visszapattanó üzenetek – *diagnosztikai info*
- Naplóállományok (pl. üzenet-mennyiségek, előrejelzéshez)

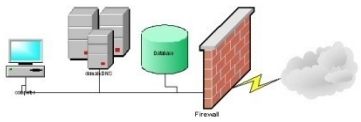


Skálázhatóság

- Növekvő felhasználói bázisnak
- Nagy adatforgalmat kell kezelni
  - Üzenetméret
  - Felhaszn.kénti üzenetszám
  - Felhasználók száma

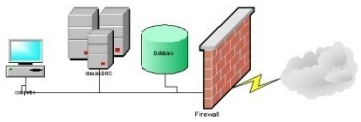


- Forgalmi börsztök kezelése
- Óriási, akkumulálódó adattömeg tárolása
- Mail spool használata segít
- Üzenetméret korlátozás is segít (időszakosan)



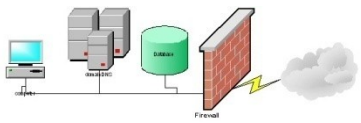
Security

- Az e-mail rendszer gépei alapvetően támadásnak vannak kitéve (extranet, Internet)
- Wormok, vírusok, biztonsági rések,... jajj.
  - Tartalomszűrés!
  - Privacy Policy
  - Detektáló alkalmazások – frissítés
- Ellenőrzés a szervereken ÉS a felhasználói gépeken is
- A tűzfallal együtt: vállalati biztonsági stratégia



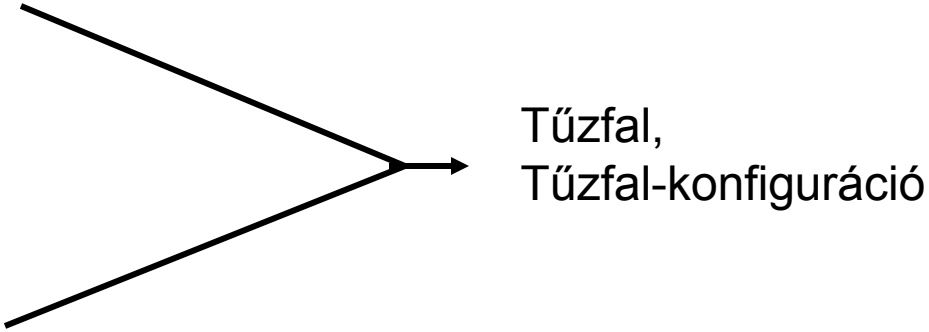
Remote Access Service

Távoli hozzáférés



Vállalati Internet-hozzáférés

- Biztonság
- Biztonság
- Biztonság

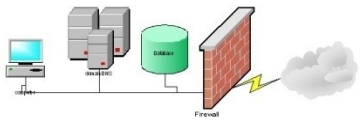


- Internet-hozzáférési szabályzat
  - Adott területek TELJES tiltása
  - Magán-internetezés visszaszorítása
- Sávszélesség-korlát (*addikció*)
- Munkatársak bejelentkezése távolról

Egy példa: „Remote Desktop”

- Windows alapú (MS Win XP óta elérhető)
- A teljes távoli képernyő látható, egér+bill vezérlés
- A (távoli gép) Windows jelszavával lehet belépni

  → legyen nagyon összetett!!

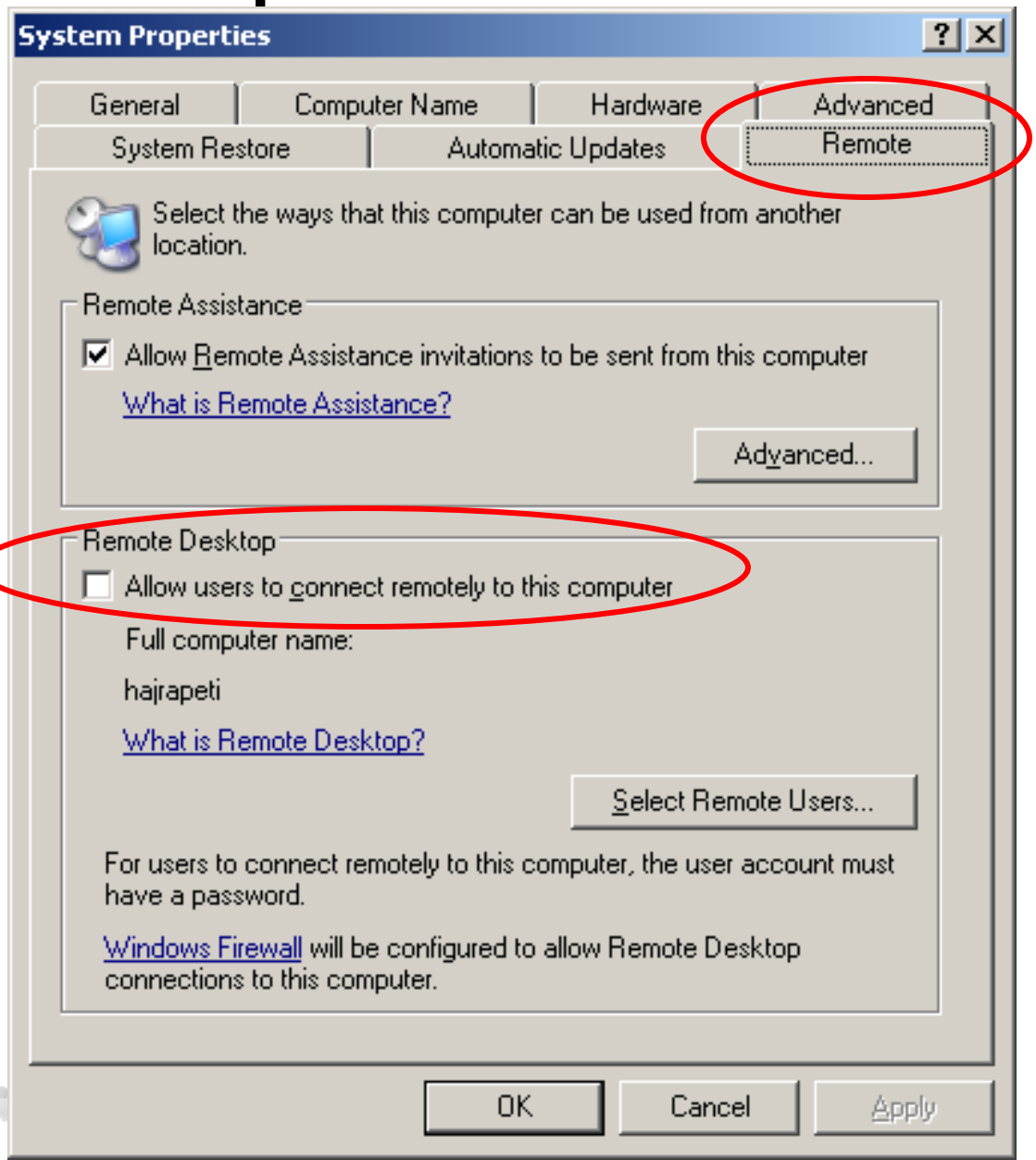


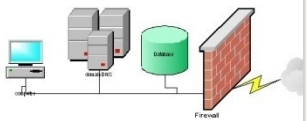
Remote Desktop beállítás - 1

- Távoli gép:

  Komplex jelszó!

- My Computer – ”jobb click”
  - Properties, Remote fül

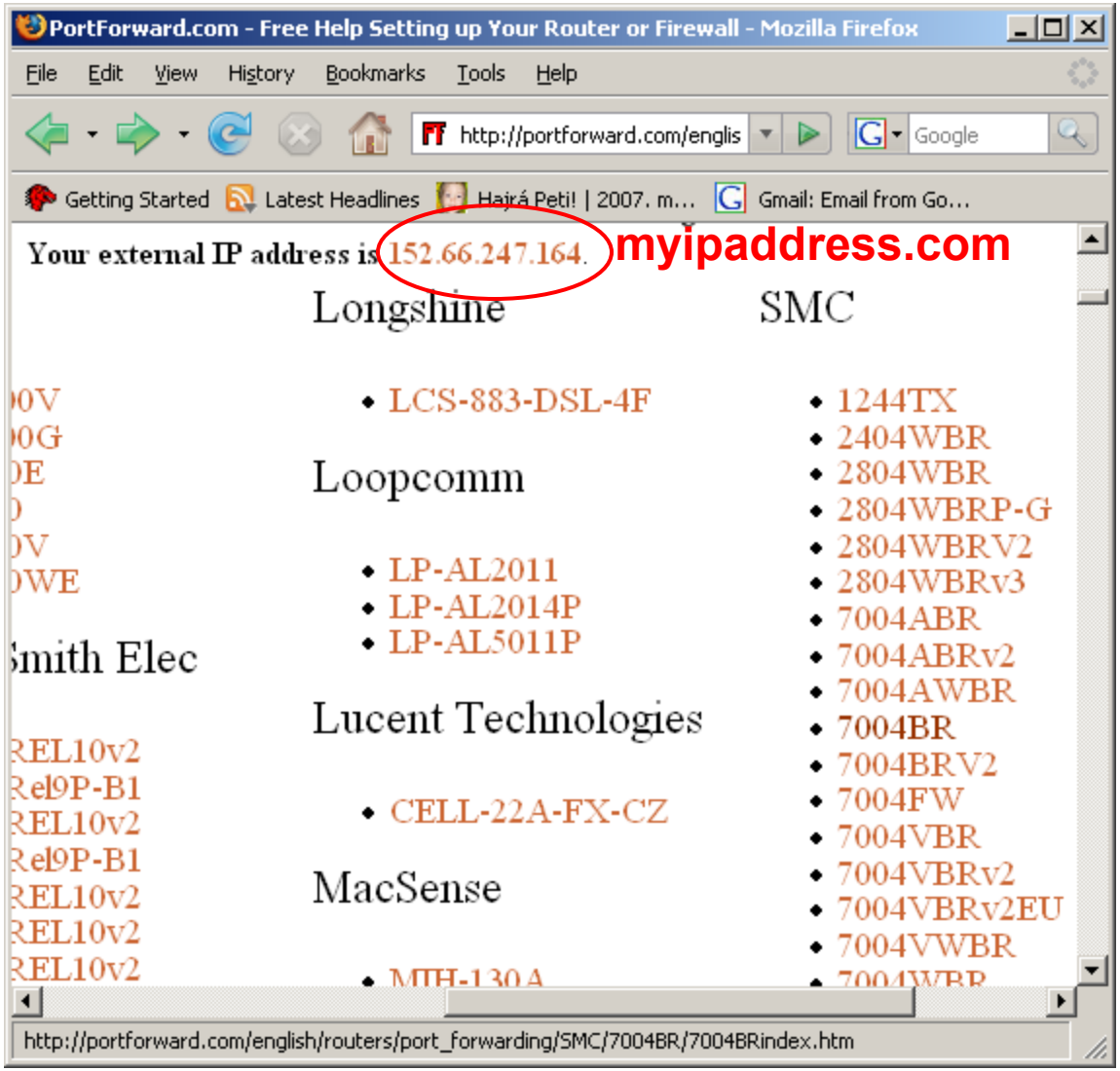




Remote Desktop beállítás - 2

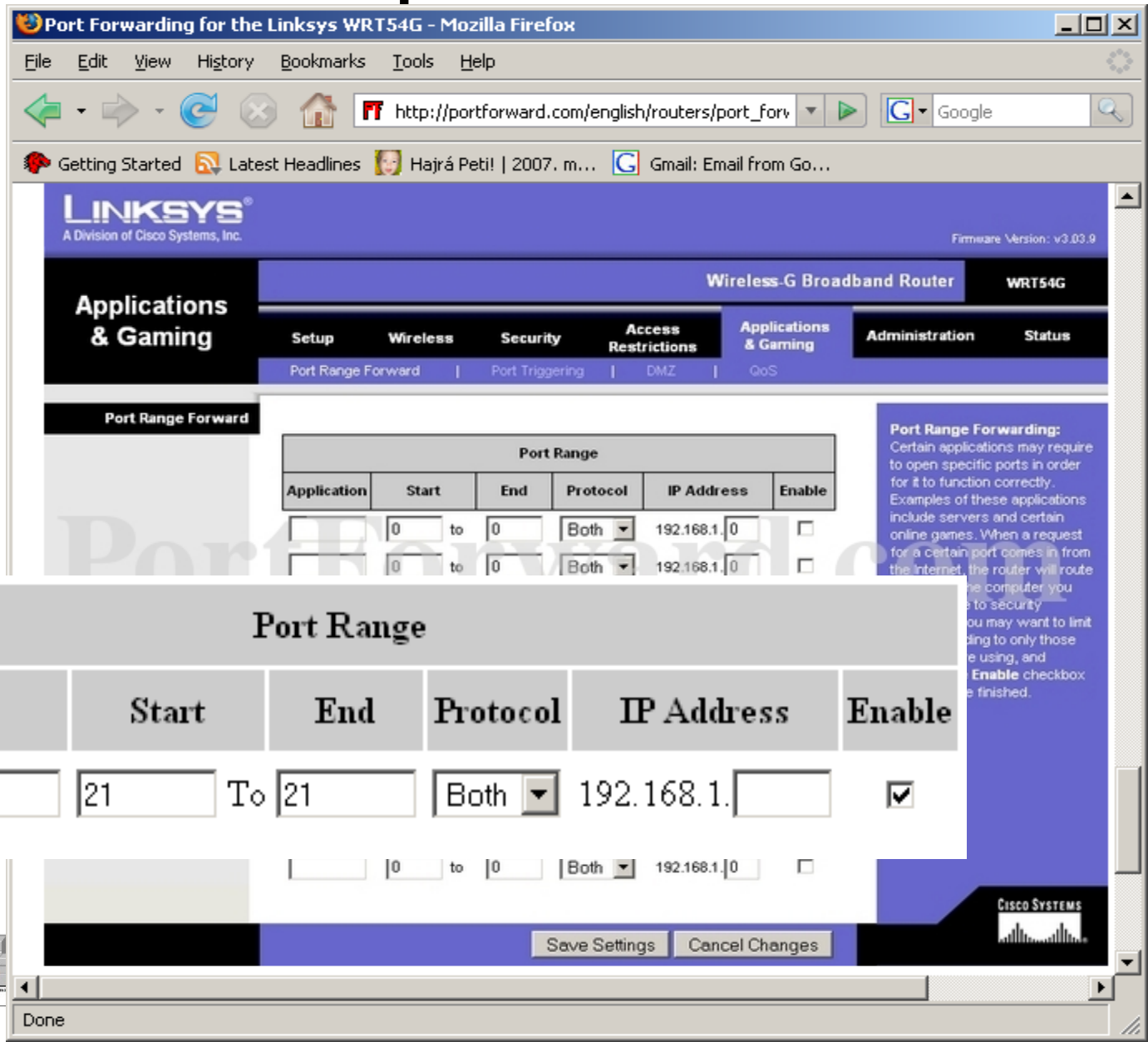
- Router:
  Komplex jelszó!
  (10-16 karakter)

- Port forwarding beállítás
  (router -> „távoli gép”)
  - Gyártónként változik
  - Jó kiindulás:
  http://portforward.com/



Remote Desktop beállítás - 3

- Router:
  - Applikáció
  - Portlista
  - *Engedély*

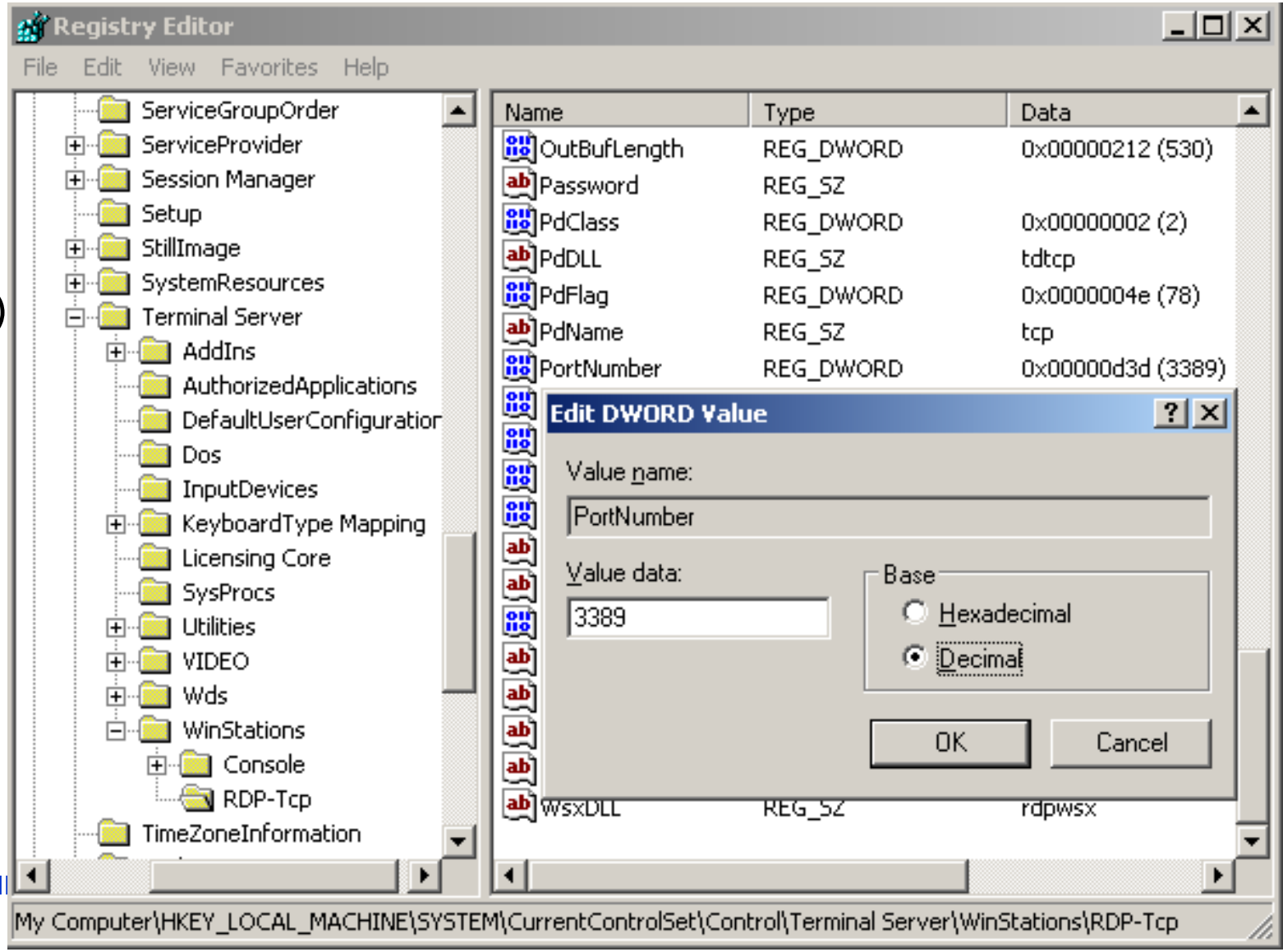


Remote Desktop beállítás - 4

Növelt biztonság:

RDP port változtatás

(eredeti: 3389)

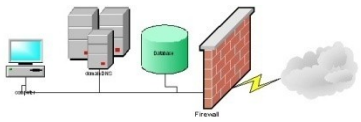


Tűzfal-lyukasztás

- A külső alkalmazások eléréséhez (pl. Remote Desktop) a
  - vállalti tűzfal(**ak**)on
  - a helyi gép tűzfalán

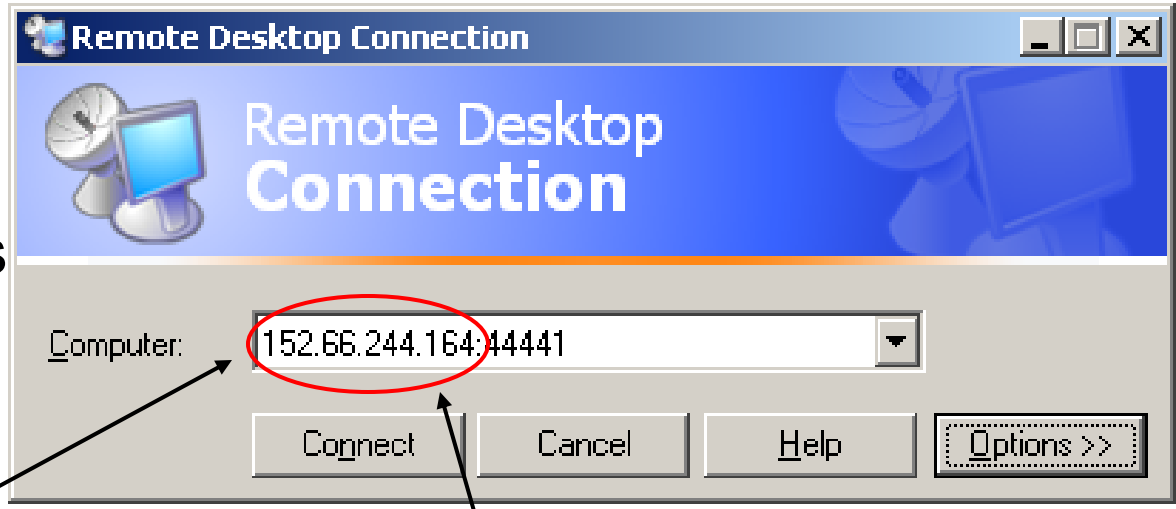
az alkalmazás protokolljához rendelt portot átjárhatóvá kell tenni

- Ez jobb helyeken hosszas engedélyezési folyamat



Remote Desktop - belépés

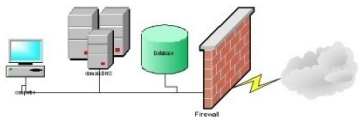
- Programs
  - Accessories
    - Communications
      - Remote Desktop Connection
- IP cím : port
- Felhasználónév / jelszó



A távoli gépünk IP-címe (amit megtudtunk pl. a www.myipaddress.com -ról)

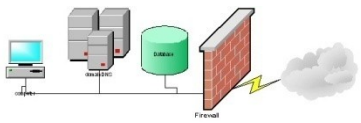
VNC – Virtual Network Computing

- „Bármilyen OS alatti gép” felületének megjelenítése bármilyen másik gépen
- Két komponensű:
  - VNC szerver: a megjelenítendő gépen fut
    - (pl. távoli szerver)
  - VNC kliens: a megjelenítő gép
    - (pl. IT-s kollega laptopja)
    - ***vncviewer*** alkalmazás – vagy
    - Web-Browseren futó Java alkalmazás
- Példánkban: Linux szerver, WinXP kliens



VNC – Szerver oldal (pl. Linux)

- http://www.realvnc.com/
- Install
  - Ha '**vnc**' a home
    - vnc/bin – bináris állományok (include binary search path..)
    - vnc/classes – további osztályok
    - **$vncClasses** legyen a **$HOME/vnc/classes**
      - $vncClasses = ((-d "/home/pvarga/VNC/classes") && "/home/pvarga/VNC/classes");
- Futtatás: 'vncserver :n'
    - n: session number
    - használt port: 5800+n
- Végeztem: 'vncserver –kill :n'



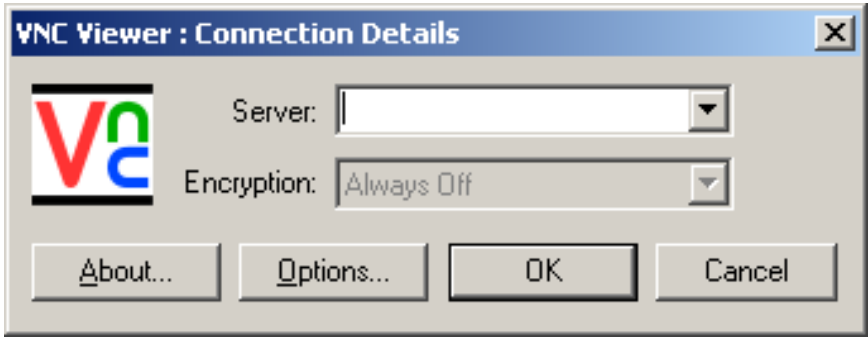
VNC – Kliens oldal (pl. WinXP)

- ‘vncviewer a.b.c.d:port’
  - a.b.c.d – a szervergép IP-címe
  - port: 5800+n

  Vagy:

  ‘szerver:session’

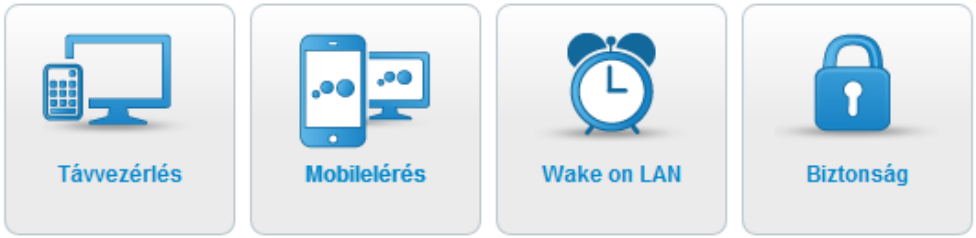
  Vagy:



- Web-browser, Java alkalmazás
  - http://szerver:port/
  - pl.: http://foszerver.ceg.hu/5801/

„Modern” megoldások

- LogMeIn

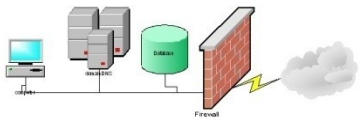


- TeamViewer

- Join.Me
- Mikogo

Távoli bejelentkezés (RAS)

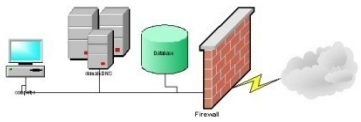
- Hozzáférésre jogosultak beléphetnek a vállalati hálózatba
  - otthonról,
  - külső telephelyről,
  - a világ bármely pontjáról
- Felhasználói igények
  - „csak ránézni az e-mailre”
  - teljes értékű munkavégzés, bármikor
- Alapos tervezést igényel



Szolgáltatási szint

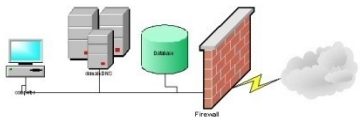
- Tisztázni kell a felhasználókkal
  - a lehetőségeket
  - a szabályokat (policy), beleértve a biztonságot
  - a felelősségeket
  - a fizetési konstrukciót (ki miért fizet)
- Amennyire lehet, adjuk ki a RAS-szolgáltatásának feladatát (outsource)

- A Biztonsági feladatokat NEM adjuk ki...
  - Authentication (username/password)
  - Authorization (jogosultságkezelés)
  - hálózat-védelem



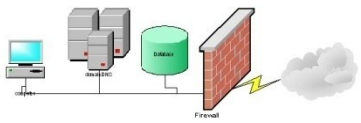
Követelmények (RAS)

- MINDENKINEK legyen távoli hozzáférése ami egyszerű, olcsó, kényelmes
  - Ha nincs: épít magának... *Nem biztonságos*
- Rövid idejű belépés: kis sávszélesség-igény
- Hosszabb munka (pl. otthon)
  - Kimaradások hátráltatják
  - Nagy sávszélesség-igény
  - Más költségmodell
  - Adatkódolás (felh.nevek/jelszavak)
- Más cégtől bejelentkezve
  - A két vállalat szokásait (policy) össze kell hangolni
  - Nem alkalmas az „always-on” hozzáállás
  - Tűzfal**ak** lyukasztása
  - Alkalmazások által használt protokollok (-> port)



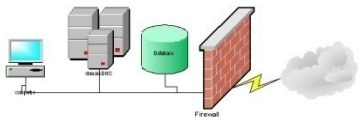
Nyomtatás

...nagy tételben...

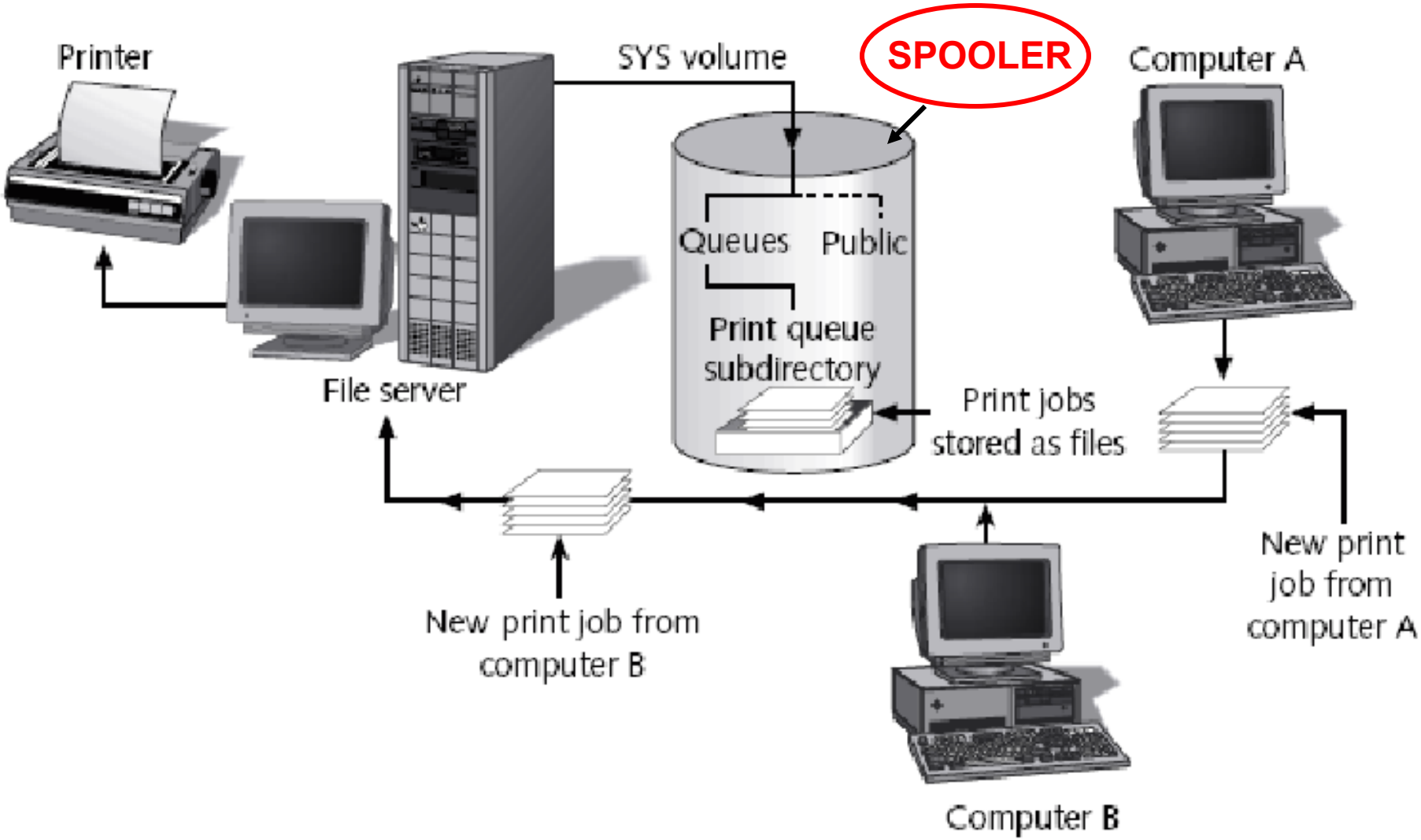


A Nyomtatás alapszolgáltatás

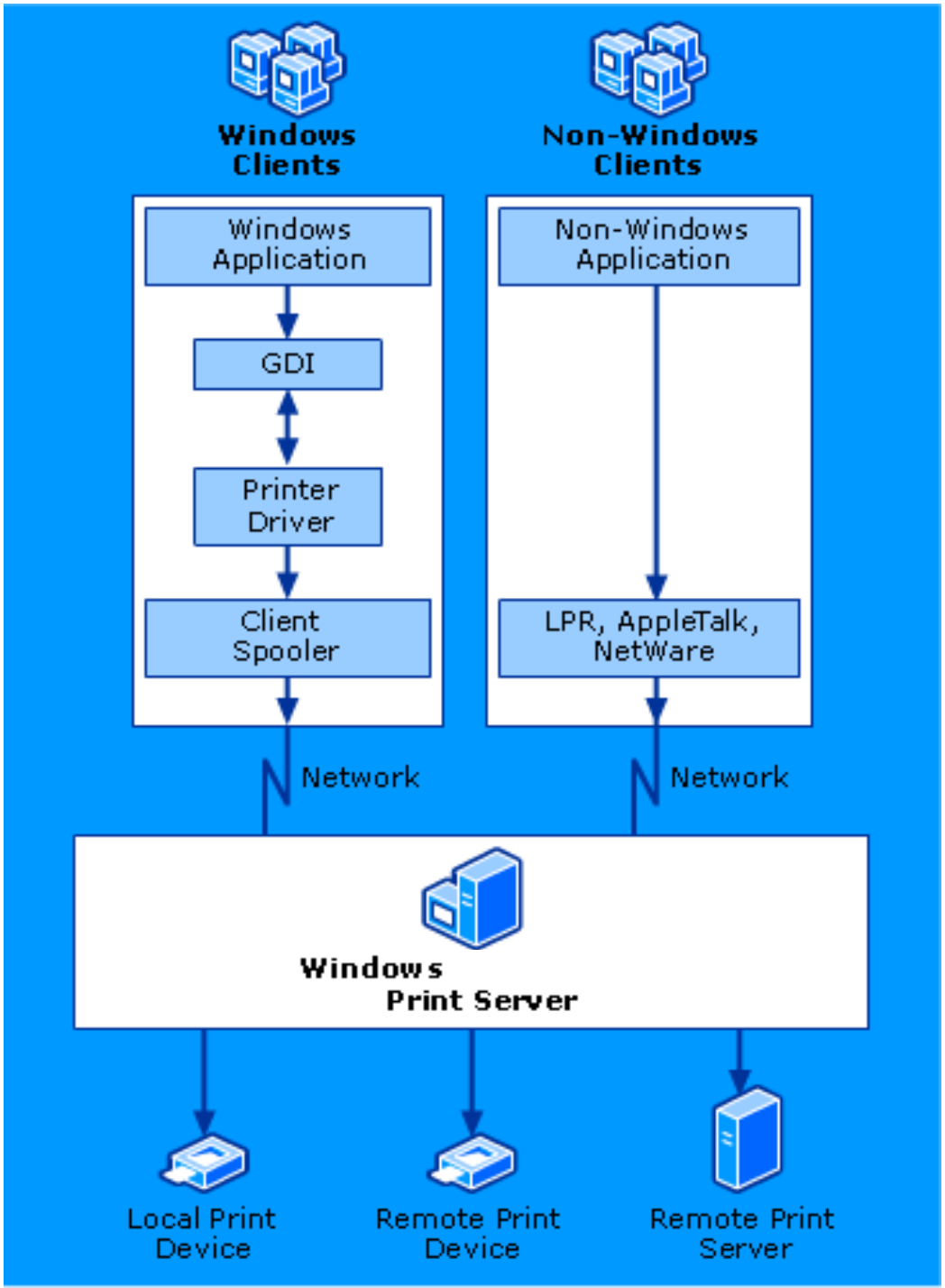
- A felhasználóknak szüksége van rá
  - v.ö. Papírmentes iroda
  - aláírás: tintával
  - átolvasás/javítás
  - A nyomtatás a 2. legkritikusabb szolgáltatás (az e-mail után!)
- Vezérelvek
- Mire legyen képes a print-szerver
- Környezettudatos printerhasználat

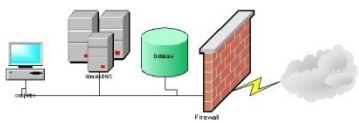


Hálózati nyomtatás - Novell

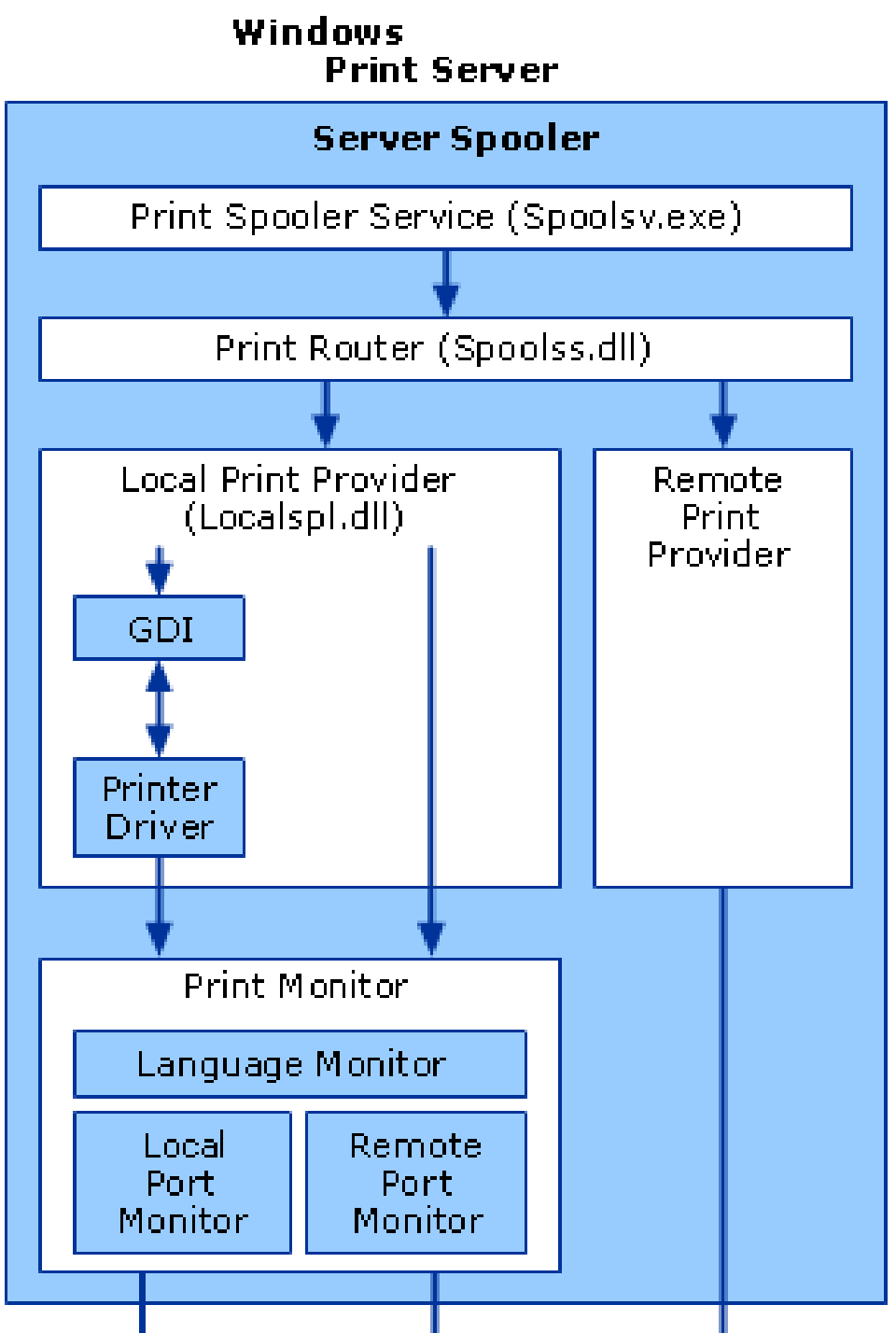


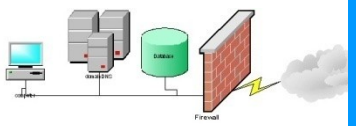
Nyomtatás: Windows





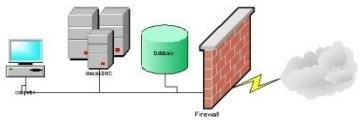
A Windows Print Szervere





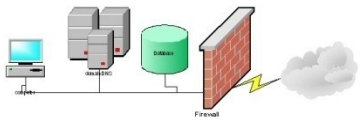
Hálózati nyomtatás - protokollok

- **Klienstől a szerverhez:**
  - **SMB** – Server Message Block (port 137-139)
  - **LPR (LPD)** - Line Printer Remote (-Daemon) Protocol (port 721-731, >1023) (szabvány: RFC 1179)
  - **IPP** – Internetwork Printing Protocol /(HTTP, 80)
  - ...
- **Szervertől a nyomtatóig:**
  - LPR
  - IPP
  - TCP app. socket (port 9100), RAW
  - ...



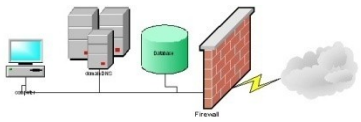
Hálózati nyomtatás - formátumok

- RAW – „nyers”, a nyomtató által emészthető formátum
  - **PCL** – Printer Command Language (HP)
  - **PostScript**
- EMF – Enhanced Metafile
    - Windows: GDI konvertálja át RAW-ba
- ANSI Text
- Egyéb formátumok
  - GDI vagy Printer Driver konvertálja az adott nyomtató által emészthetővé



Centralizáció

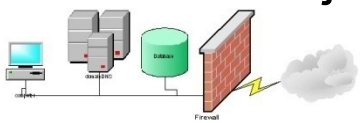
- Végletek:
  - Saját nyomtatót mindenkinek!
  - Bármely munkahelyről bármely nyomtatóra..!
- Különféle feladatokra más-más követelmények:
  - Gyors
  - Jó minőségű (felbontás)
  - Színes
  - ezek kombinációi…
- Sok nyomtató sokba kerül!!
- Megoldás:
  - Központi nyomtatók is
  - Egyes embereknek saját nyomtató is



Nyomtatási architektúra

- Mennyi embernek ...?
- Ki üti meg a mércét a saját nyomtatóhoz?
- Hogyan rendeződnek hálózatba a nyomtatók?
- Mennyi *„printer spool”*? (központi nyomtatási puffer)

- Ki fizet a...?
  - Vásárlásért
  - Karbantartásért
  - Utánpótlásért (papír, toner)
    - költséghely figyelmeztetése
    - szakember cserélje a tonert

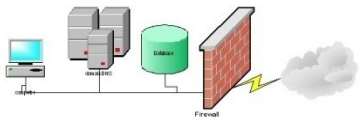


Nyomtatási standardok

Ha a rendszergazda standard nyomtatással tervez, később kevesebb dolga lesz

- Postscript vagy PCL
- Mikor kell duplex-egység?
- Támogatott protokollok
- Nyomtató kapcsolódásai (USB, Eth, p.port)

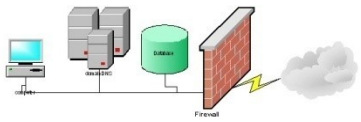
- Lista: Jelenleg támogatott nyomtatók / driverek



Hozzáférés elvei

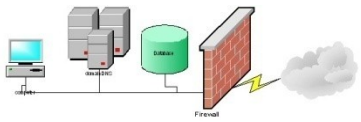
- Ki mihez férhet hozzá
- Ki adja ehhez a jogokat
- Ki melyik sorból mit lőhet ki?
  - Cancel WAR

- Névadás
  - Típus (pl. duplex, color, high...)
  - Fizikai hely azonosítás



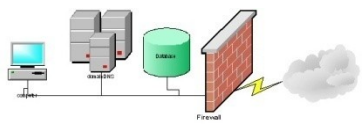
Ki mit ér el...?

- peer2peer (a felhasználók direktben bármelyik nyomtatóra spool-ozhatnak)
- Központi elosztás
  - nagy központi spool
  - intelligens döntésekre van lehetőség
  - „Single point of failure!”
- Csoportonkénti spool
- Többszörösen redundáns spool-ok



Dokumentáció

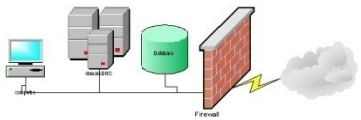
- Hogyan kell nyomtatni?
  - milyen menü
  - milyen nyomógomb
  - hol duplaklikk
- Fel kell sorolni a nyomtatókat
  - képességeikkel, helyükkel, szabályaikkal
- Feliratozzuk a nyomtatót
  - legyen rajta a neve,
  - ha tálcákra külön lehet nyomtatni, akkor azokon is legyen rajta a tálca/sor neve!



Monitorozás

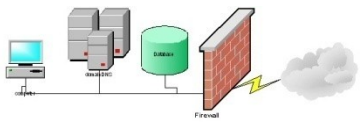
- Spooling: a nyomtató jelzi, ha baja van (pl. SNMP)
  - tele a sora
  - tele a diszkje
  - túl van terhelve (CPU), stb.

- Printing: Maga a nyomtatási környezet rendben van-e, hogyan állunk tartalékokkal
  - toner
  - papír
  - papír a polcokon
  - beragadás van-e



További tippek

- Automatikus fail-over és terhelésmegosztó eljárások
  - hogyan detektáljuk, ha gond van
  - hogyan kapcsolunk át?
- Dedikált nyomtató-karbantartó személy (külsős akár)
  - Daraboljuk apróra (Shredding)
  - biztonság…
- Printer Abuse
  - “You can’t solve social problems using technology”
  - fizetés oldalanként (akár jelképes is…)
  - Top 10 nyomtató személyek publikálása

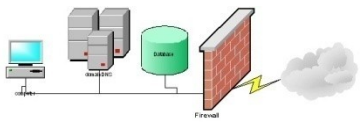


Telecommunications Management Network (TMN)

- áttekintés és példák -

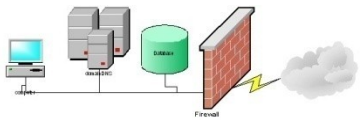
Varga Pál

pvarga@tmit.bme.hu



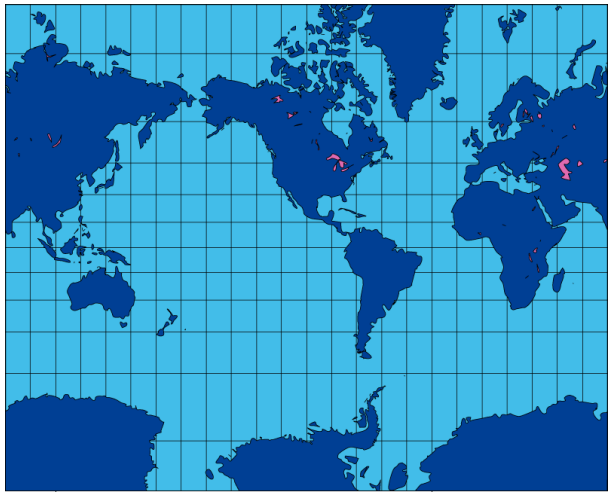
Áttekintés

- Röviden a hálózati szolgáltatások minőségéről
  - Elvárások a hálózati szolgáltatásokkal szemben
  - QoS, SLA és SLS
  - Végpontok közötti szolgáltatásminőség, elégedettség, QoE
- TMN – Az első szabványosított távközlés-menedzsment keretrendszer
  - FCAPS
- Hálózatfelügyeleti módszerek
  - A forgalom monitorozása
  - Szolgáltatás-szintű elemzés
  - Hibamenedzsment

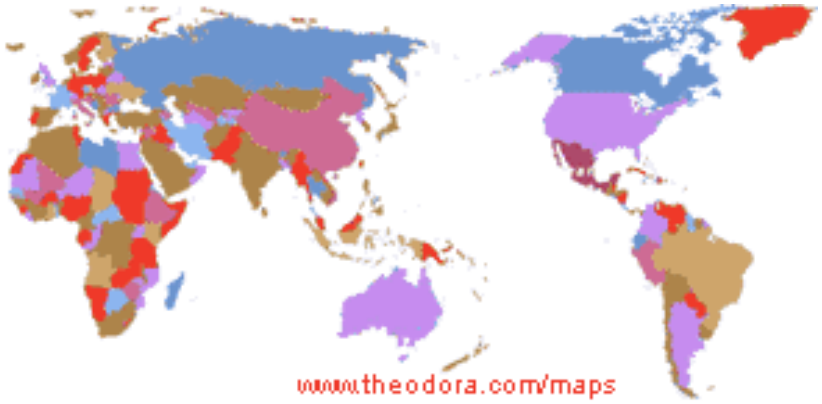


Alapprobléma: Lokális és globális nézőpont

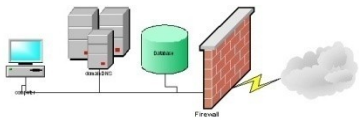
A világ Európából,



Amerikából,



… és Ausztráliából nézve

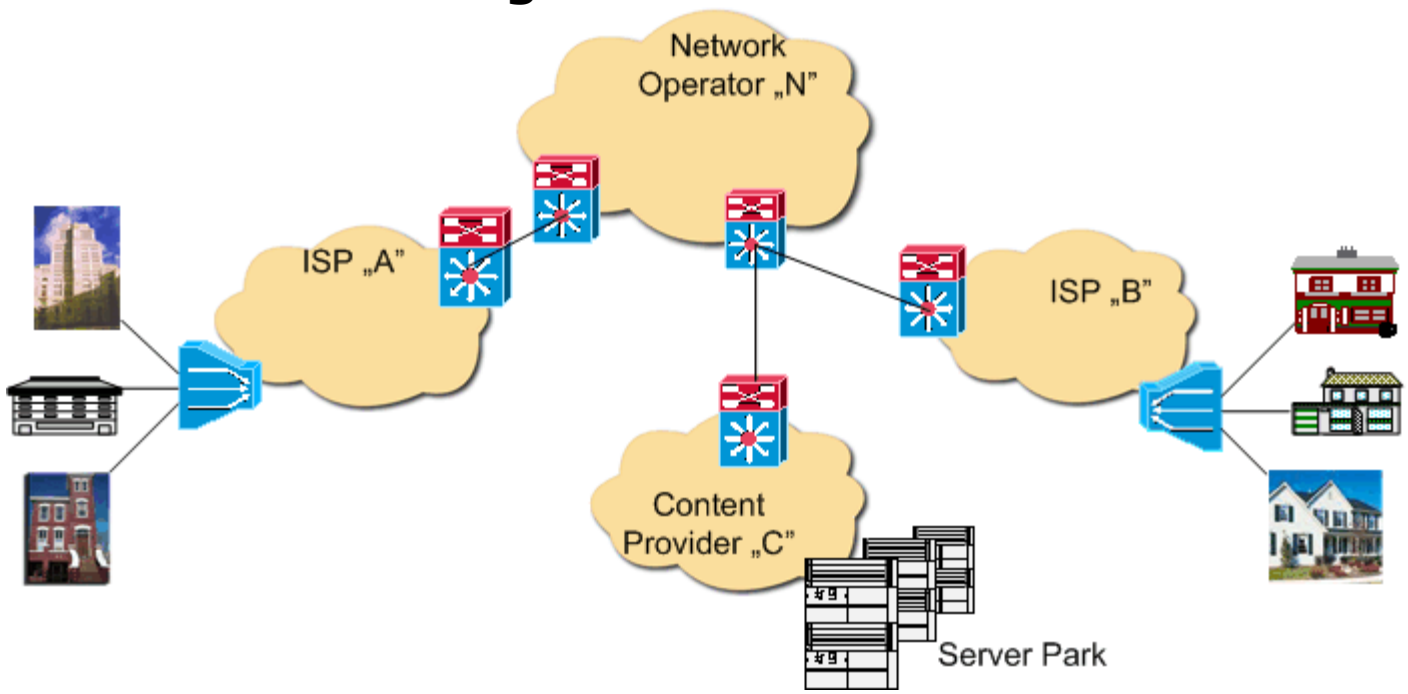


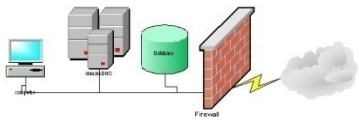
A hálózati szolgáltatások globális, „end-to-end” nézete

A felhasználó akkor elégedett a szolgáltatással, ha

- ☑ kéréseit **kiszolgálják**,
- ☑ a szolgáltatás **minősége** is kielégítő,
- ☑ az időszakos problémák hamar **megoldódnak**.

A felhasználó szemszögéből mellékes, hogy milyen szolgáltatókon keresztül teljesül a kérése.

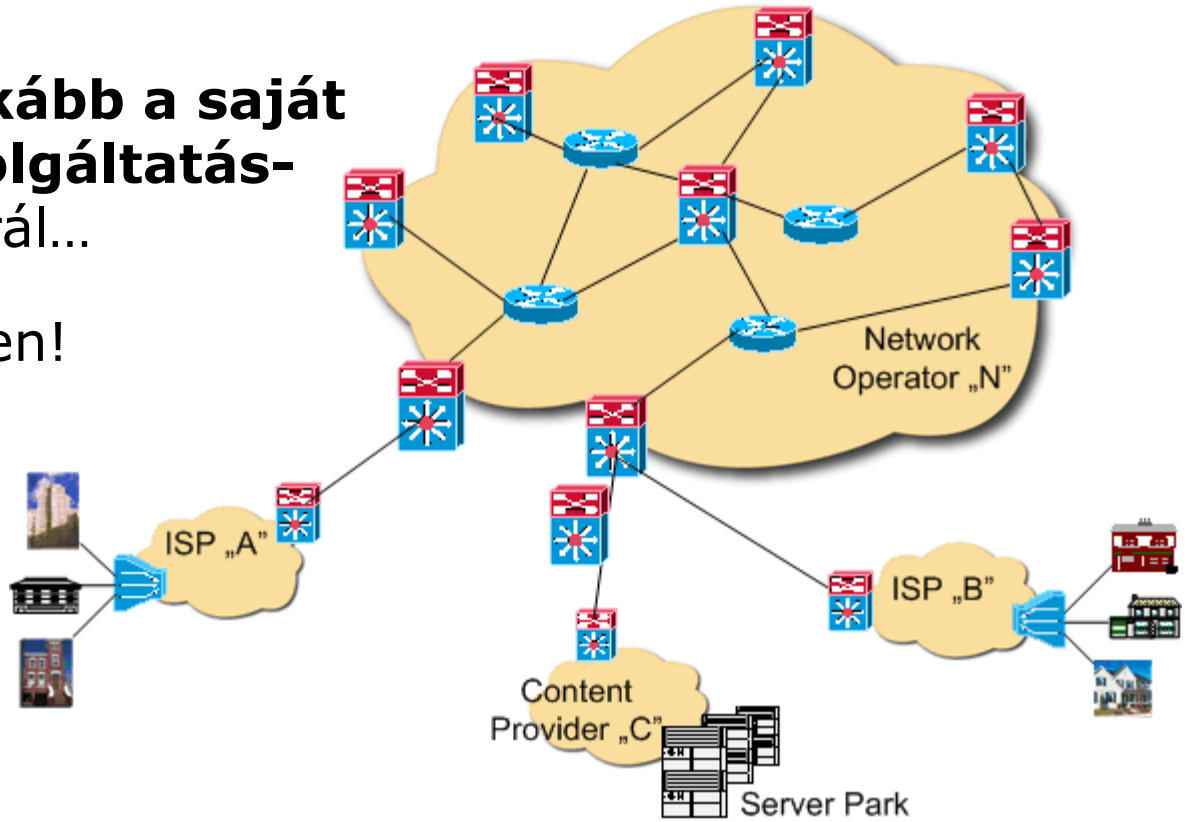




A hálózati szolgáltató képe a világról - 1

A szolgáltató **leginkább a saját** hálózatán belüli **szolgáltatás-**minőségre koncentrál…

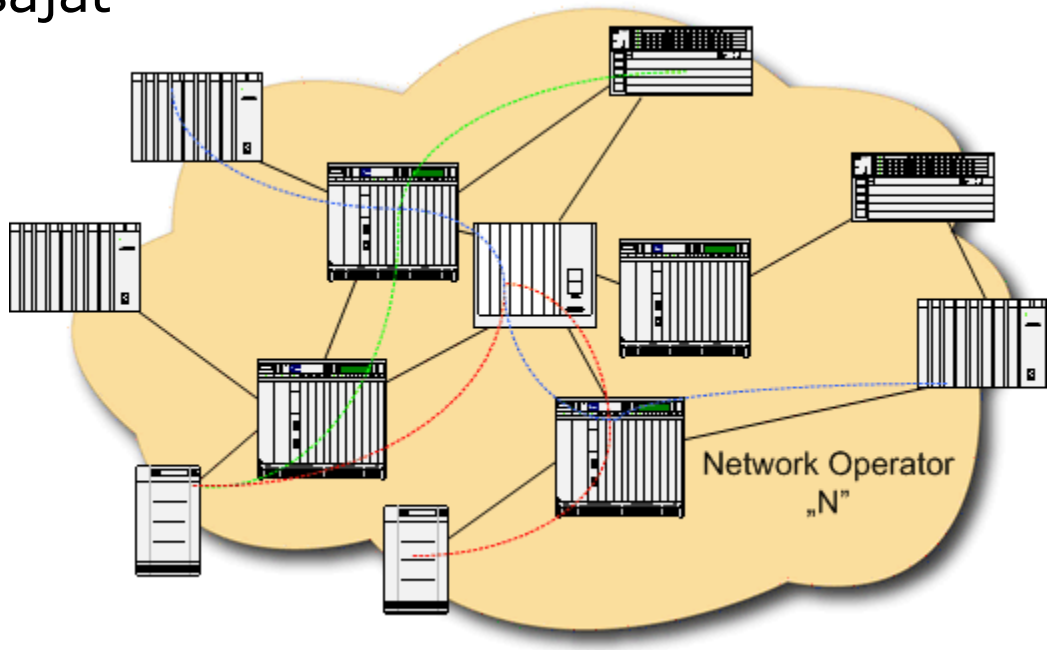
…szerencsés esetben!



A hálózati szolgáltató képe a világról - 2

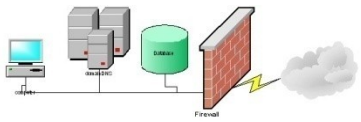
…kevésbé szerencsés esetben azonban…

A szolgáltató **kizárólag** a saját hálózatán belüli **hálózat-**minőségre koncentrál



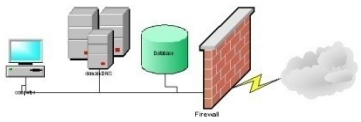
Quality of Service

- Tipikus mércék
  - …Rendelkezésre állás…
  - Áteresztőképesség (throughput)
  - Késleltetés
  - Késleltetés-ingadozás (jitter)
  - Csomagvesztés



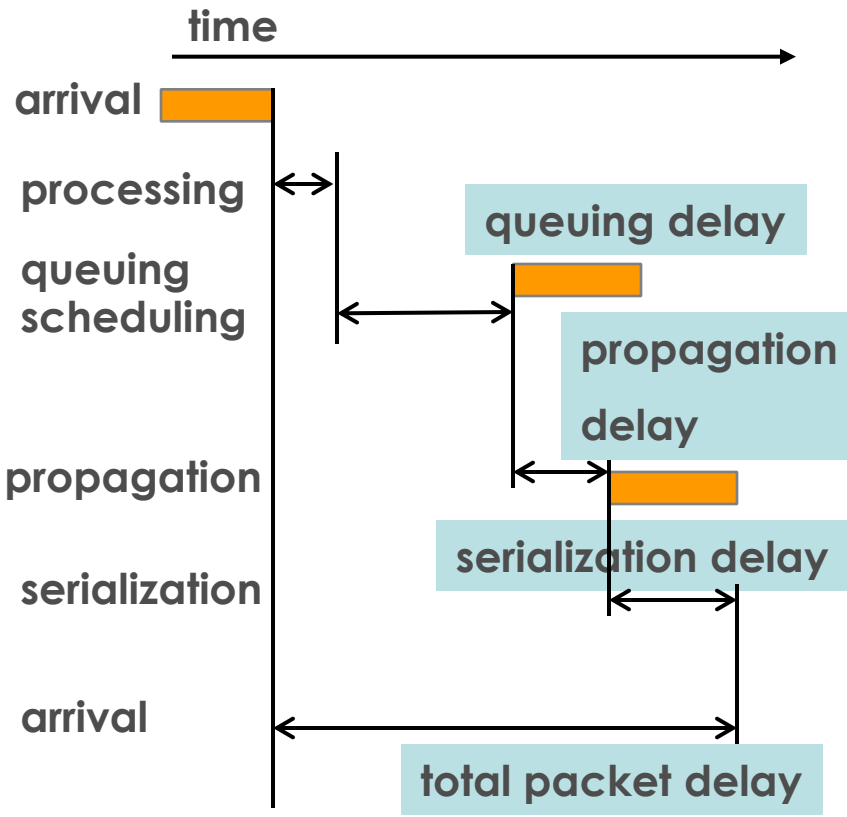
Rendelkezésre állás

- Szolgáltatás rendelkezésre állását befolyásoló tényezők
  - Hálózati rendelkezésre állás
    - *Fizikai szintű, adatkapcsolati szintű*, etc…
    - Erőforrások
  - Szolgáltatói tényező
    - Rendszer hiba

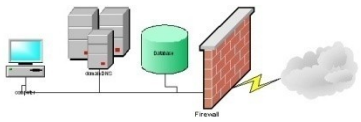


Késleltetés

- Feldolgozási késleltetés (processing)
  - A csomagok feldolgozása és felkészítése az újraküldésre
- Sorbanállási késleltetés (queuing delay)
  - Csomagok sorbanállási ideje (a terhelés és az alkalmazott ütemezési eljárás határozza meg)
- Terjedési késletetés (propagation)
  - Adatok kapcsolaton való terjedés ideje
- Továbbítási késleltetés (transmission, serialization delay)
  - A teljes csomag megérkezésének ideje (az első és utolsó bitnek beérkezése között eltelt idő)



teljes csomag késleltetés = (feldolgozási idő) + sorbanállási idő + (terjedési idő) + továbbítási idő

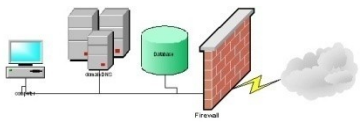


A jitter

- Több értelmezése is van, ezekben a közös: a jitter a késleltetés ingadozása
- Mértéke:
  - Szórás (átlagtól való átlagos letérés)
  - A kis valószínűségű, de nagyobb késleltetéseket is beleszámítja (pl. p>0,001) – jitter–buffer méretezés
- Hasznossága „itt”: a *csomagközti idők* jittere az interaktív hang/video átvitelnél érdekes
  - Nagy jitter: nagy szünet a lejátszandó keretek között; kiürülhet a buffer

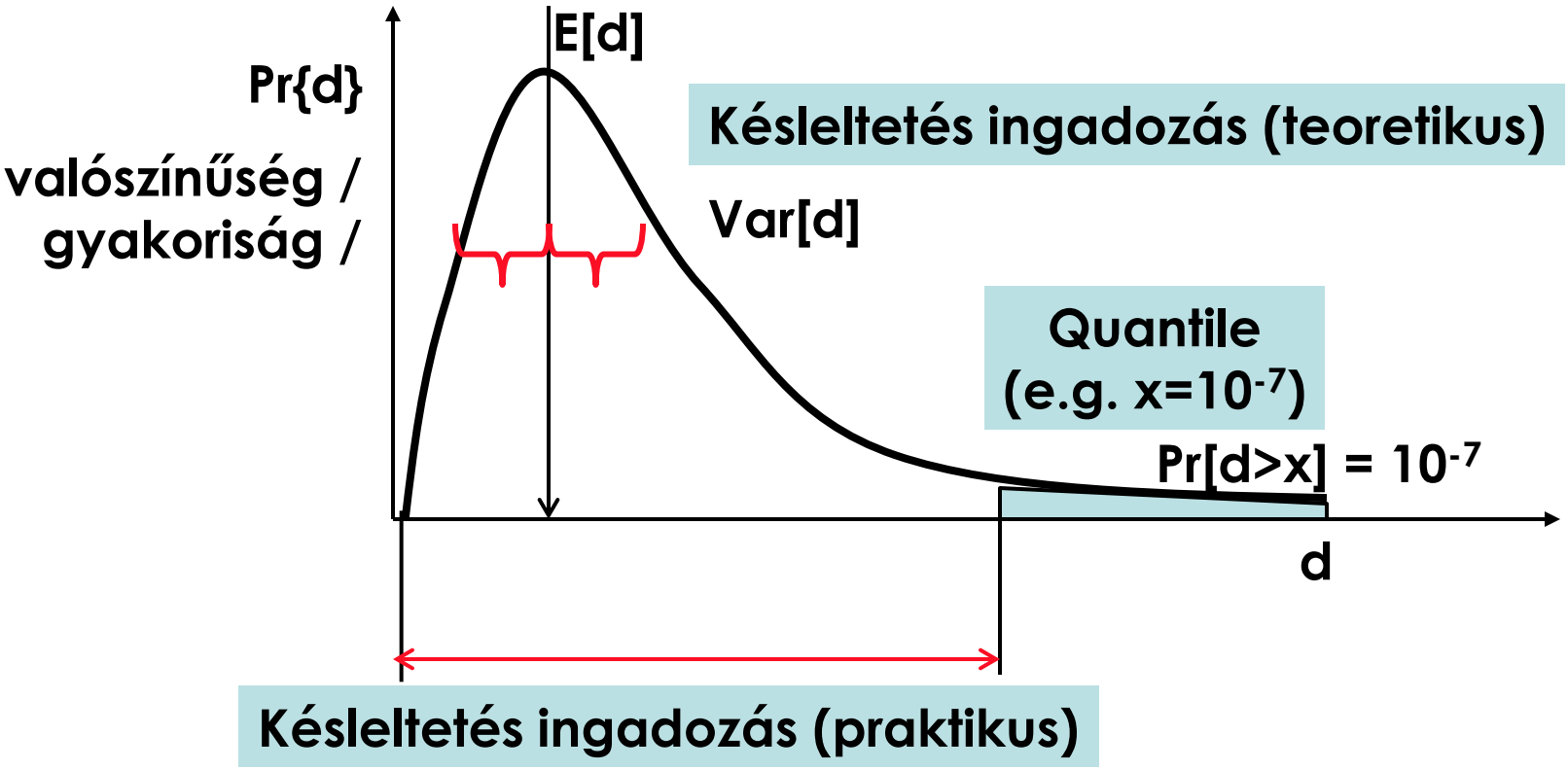
| | | | | | | | | - csomagok közötti idő közel állandó: kis jitter

| | | ||| | | - börsztös forgalom: NAGY jitter



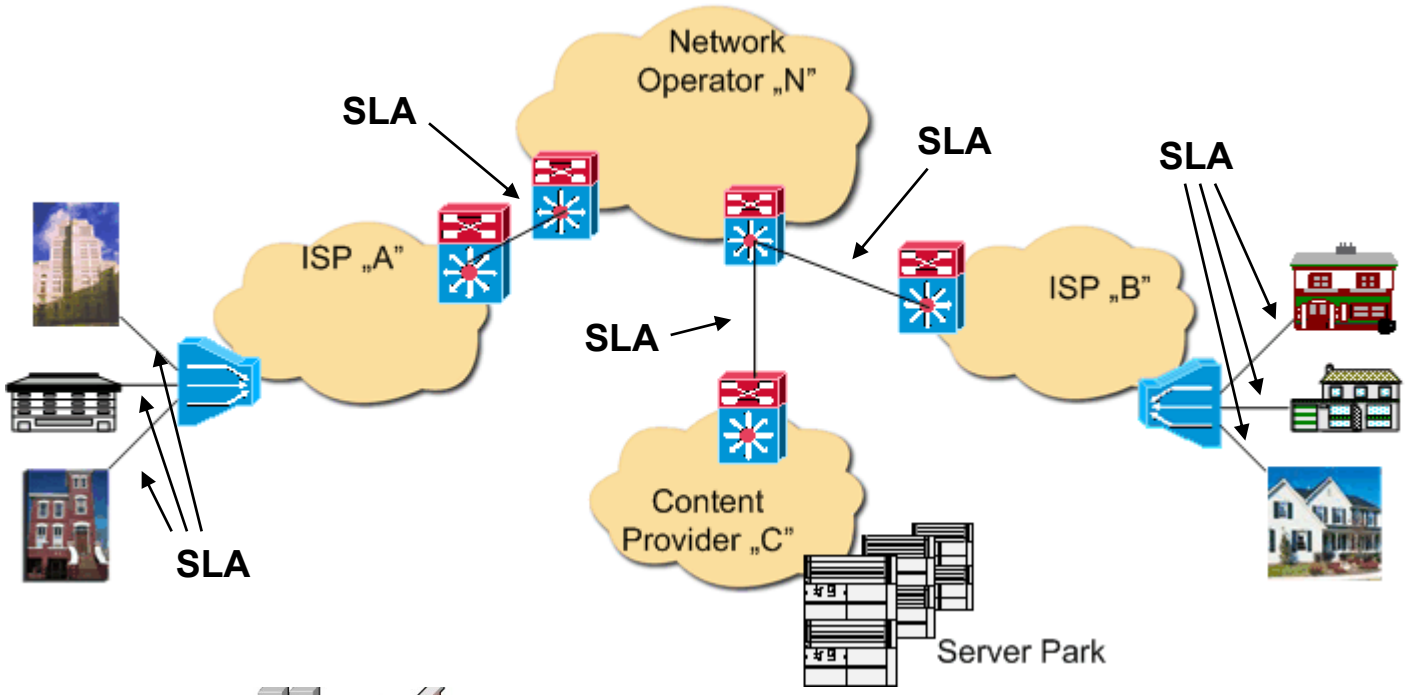
Jitter – késleltetési ingadozás

PDF, sűrűségfüggvény



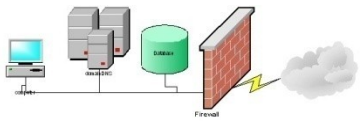
Megegyezés a szolgáltatási szintről -SLA

- SLA: Service Level Agreement
  - Ez maga a szerződés
    - a szolgáltatók/hálózat-operátorok között
    - a hozzáférési hálózatot biztosító szolgáltató és az előfizető között



Megegyezés a szolgáltatási szintről -SLS

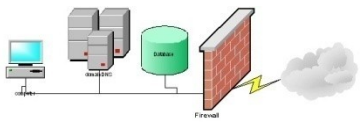
- …az SLA „műszaki melléklete” az
- SLS: Service Level Specification
  - A szolgáltatás „minőségét” leíró műszaki…
    - áteresztőképesség - [kbps]
    - (késleltetés)
    - (jitter)
    - (vesztési arány)
  - … és nem-műszaki…
    - rendelkezésre állás
    - probléma-megoldási időintervallumok
  - …paraméterek és küszöbértékeik.



Quality of Experience - QoE

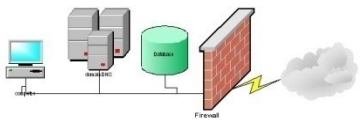
- A felhasználó a hálózati szolgáltatásokat a hálózati adottságok „észrevétele nélkül” szeretné használni.
- A hálózati szolgáltatásokkal kapcsolatos elégedettsége (QoE) szubjektív küszöbértékektől függ

- A QoE mércék típusai:
  - szolgáltatás elérhetősége
    - az alaphozzáférés működik-e
    - az alkalmazás elérhető-e, és ad-e (egyszer csak) választ
  - a szolgáltatás minősége
    - … lásd „elvárások a szolgáltatásokkal szemben”
    - szolgáltatásonként eltérő küszöbértékek az „end-to-end” QoS-re
  - a felmerülő problémák megoldásának időtartama és minősége



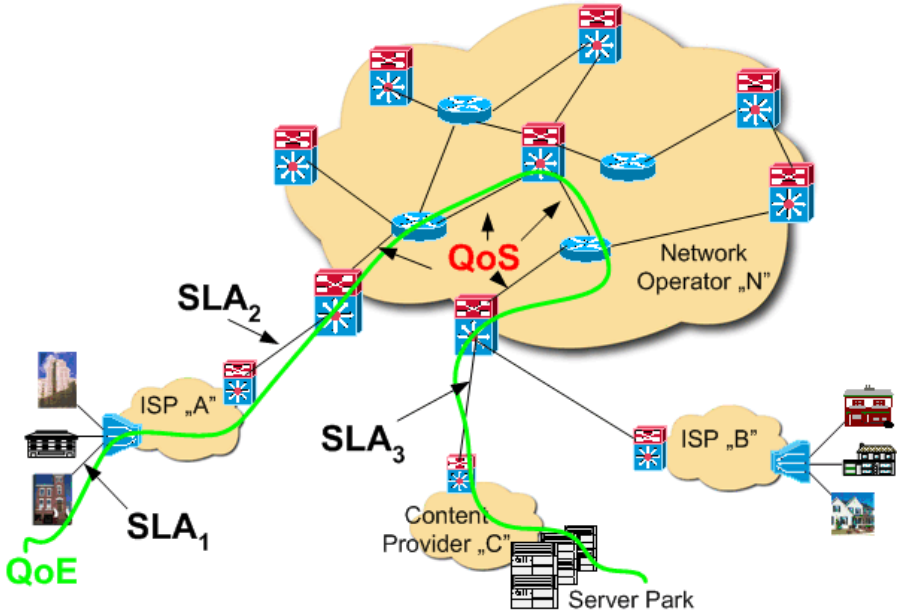
Elvárások a szolgáltatásokkal szemben

Elvárások ➤ **Szolgáltatás ➘**	Sáv-szélesség	Késleltetés	Adat-vesztés	Egyéb
Interaktív beszéd és video (konf.)	**B: kicsi** **V: NAGY**	**Minimális**	**Best Effort**	**Alacsony jitter**
Off-line streaming audio és video	**A: kicsi** **V: NAGY**	**Best Effort**	**Best Effort**	**Alacsony jitter**
Kliens-szerver lekérdezések	**kicsi**	**Alacsony**	**Alacsony**	
Letöltések	**NAGY**	**Alacsony**	**Best Effort**	
Potenciálisan rosszindulatú forg.	**kontrolált**	**Best Effort**	**Best Effort**	**Izoláció javasolt**
Hálózati játékok	**Változó**	**Minimális**	**Minimális**	
Egyéb (E-mail, …)	**Kicsi**	**Best Effort**	**Best Effort**	

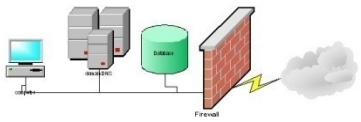


QoE – SLA – QoS

…Van-e a „mai” valóságban kapcsolat közöttük?

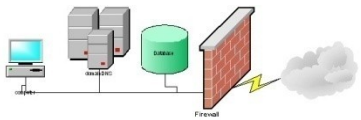


- Ha nincs, akkor „Szolgáltatás-szintű menedzsment” tekintetében nem hagyatkozhatunk a hálózatra
- Kell egy folyamatosan és megbízhatóan működő **felügyeleti rendszer**!



Hálózatfelügyeleti módszerek

- A TMN filozófia
  - Logikai modell:
    - Business-, Service-, Network-, Element-, Network-element-szintek
- A forgalom monitorozása – szintek és módszerek
- Szolgáltatás-szintű elemzés
- Hibamenedzsment
  - Hibajel (event)
  - Hibajegy (alarm)
  - Hibajel-feldolgozás
  - Hibaok-keresés



TMN – Telecommunications Management Network

„A TMN segítségével a szolgáltatók menedzselhetik a különböző

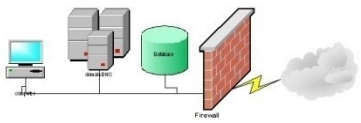
- operációs rendszereken
- hálózati elemeken
- hálózattípusokon

átívelő kapcsolatokat és kommunikációt.”

A TMN (ITU-T M.3010)

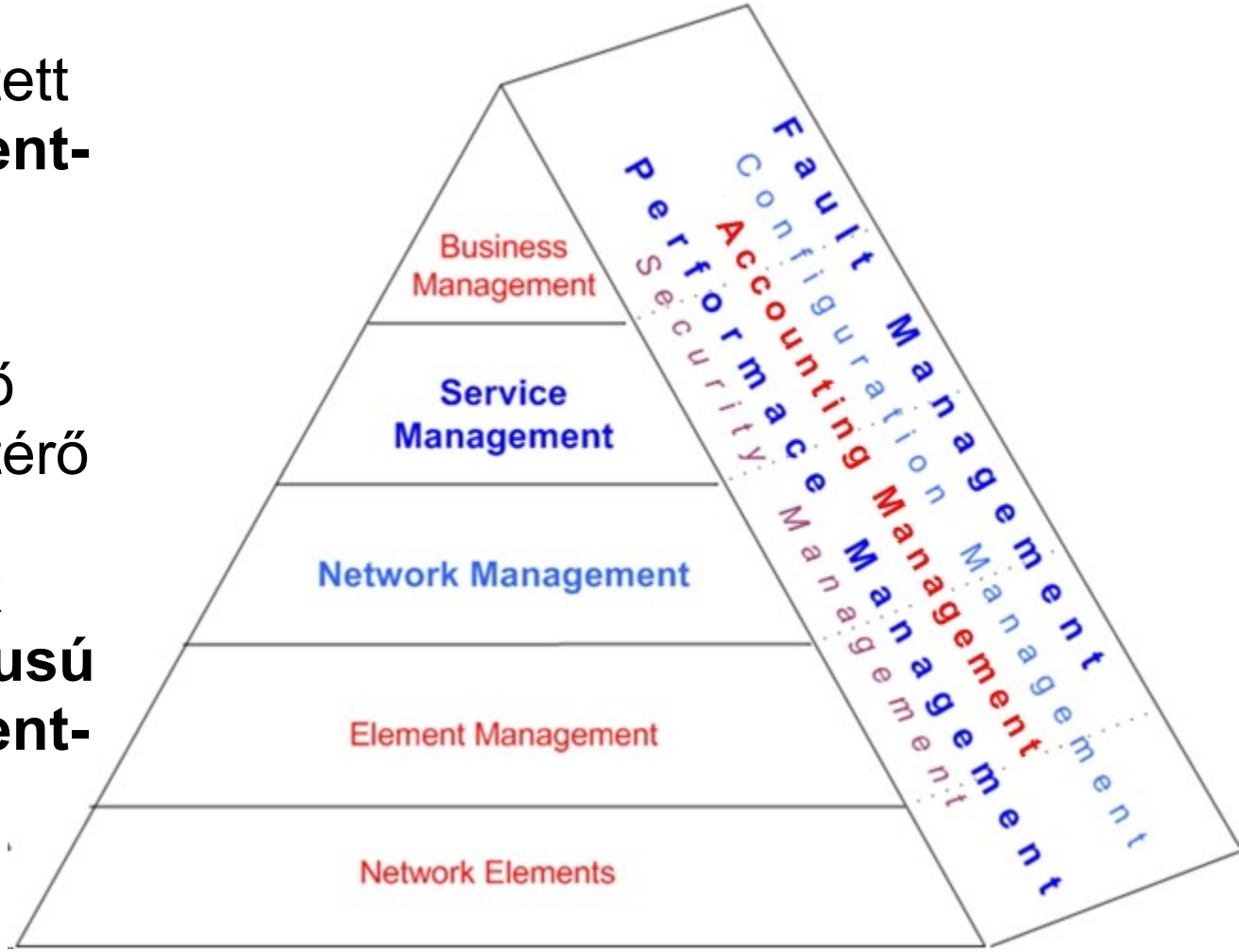
- funkcionális modellt
- **logikai modellt**
- szabványos interfészeket kínál

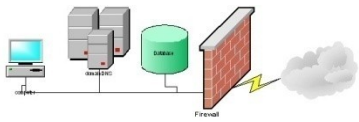
a hálózatmenedzsment során felmerülő problémák megoldására.



A TMN logikai modell

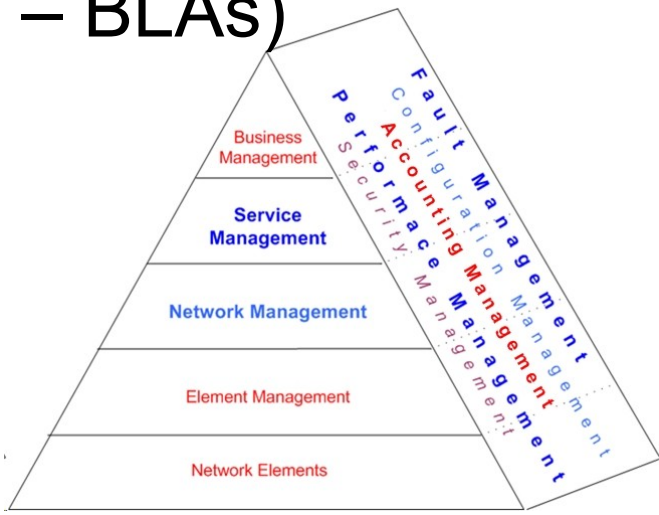
- Jól elkülönített **menedzsment-szintek**
- A különböző szinteken eltérő mértékben jelentkeznek **hasonló típusú menedzsment-feladatok**

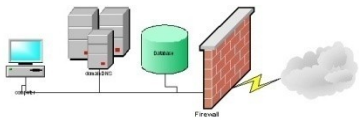




TMN – Business Management

- Magas szintű tervezés
- Pénzügyi tervek és ellenőrzés
- **Célok definiálása**
- Döntéshozás
- Üzlet-szintű egyezmények
  (Business Level Agreements – BLAs)

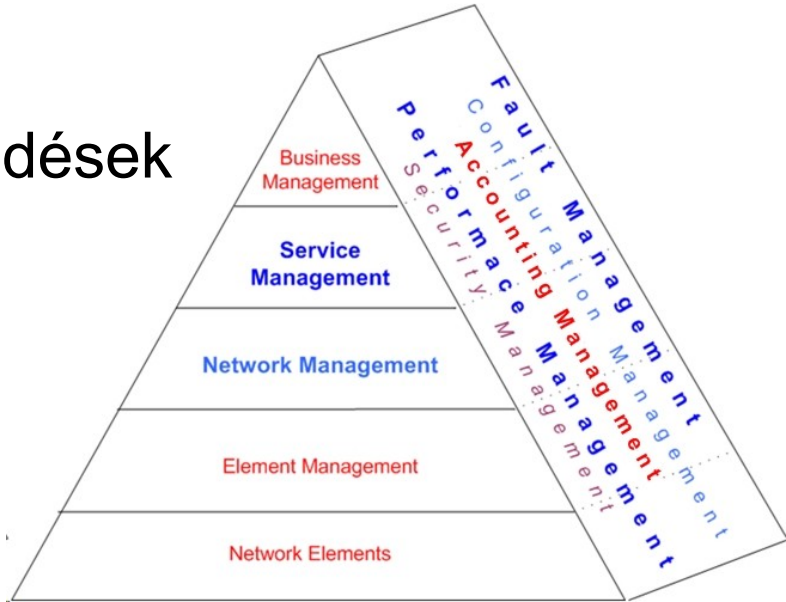


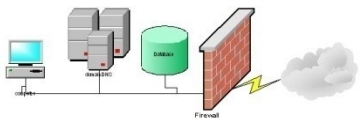


TMN – Service Management

- Alapvetően ide tartozik a felhasználóval való kapcsolattartás:
  - szolgáltatás beindítása és módosítása
  - számlázási feladatok
  - szolgáltatásminőség felügyelete és biztosítása (PM)
  - hibamenedzsment (FM)
- A hálózati szintű információk felhasználása
  - a felhasználóval és
  - a többi szolgáltatóval

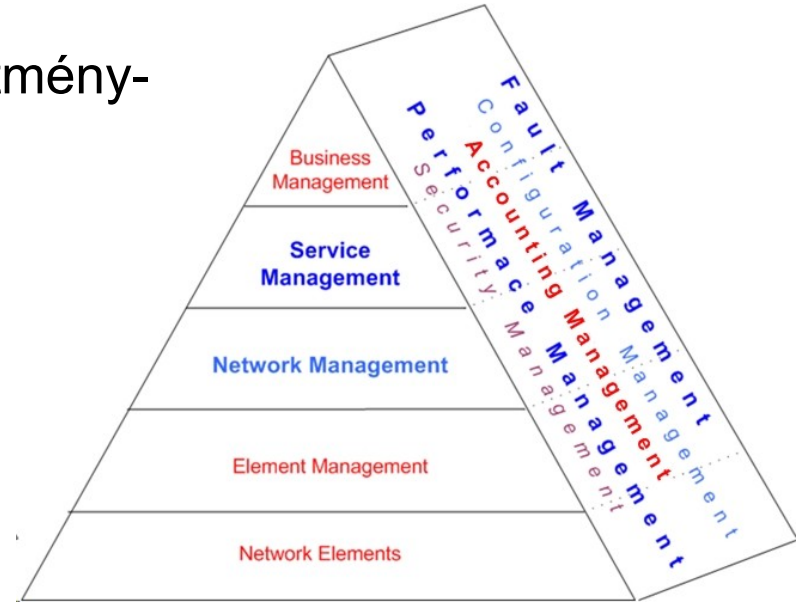
kialakított szolgáltatás-szintű szerződések (SLAs) biztosítása érdekében.

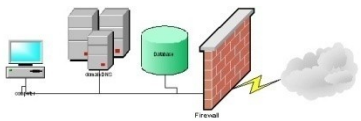




TMN – Network Management

- A hálózat, mint elkülöníthető funkcionális egység felügyeletére és vezérlésére vonatkozó feladatok
  - az egyes hálózati elemek (ilyen minőségű) menedzsmentje
  - a hálózati szegmensek menedzsmentje
- A hálózati elemektől érkező információk felhasználása
  - a hálózati szintű hiba- és teljesítmény-menedzsment során
  - a szolgáltatás szintű feladatok elvégzésének előkészítésére

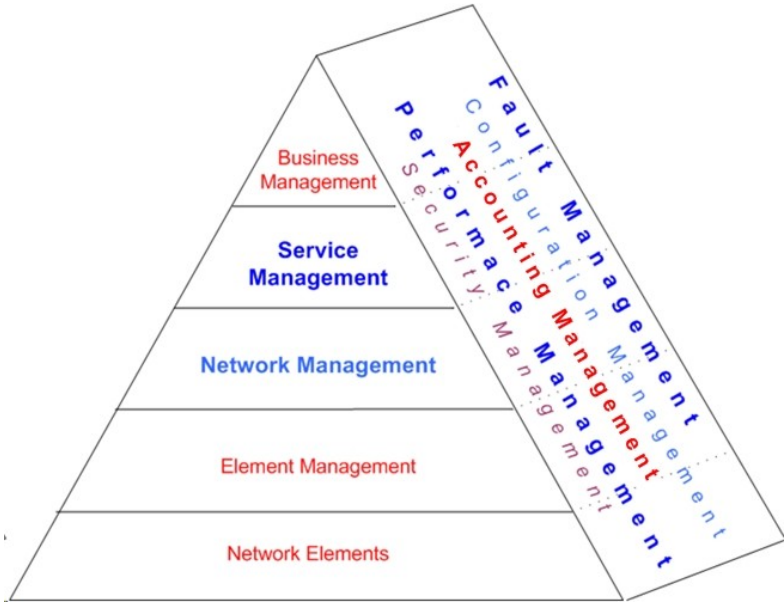


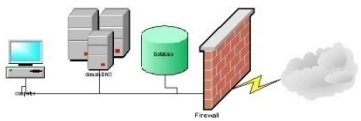


TMN – Element Management

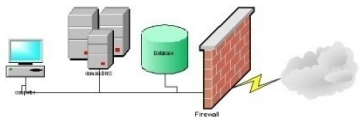
– Az egyes hálózati elemek, mint önálló, sok funkcionalitással rendelkező gépek felügyeletére és vezérlésére vonatkozó feladatok

– Tipikusan a rendszergazda felelős ezekért

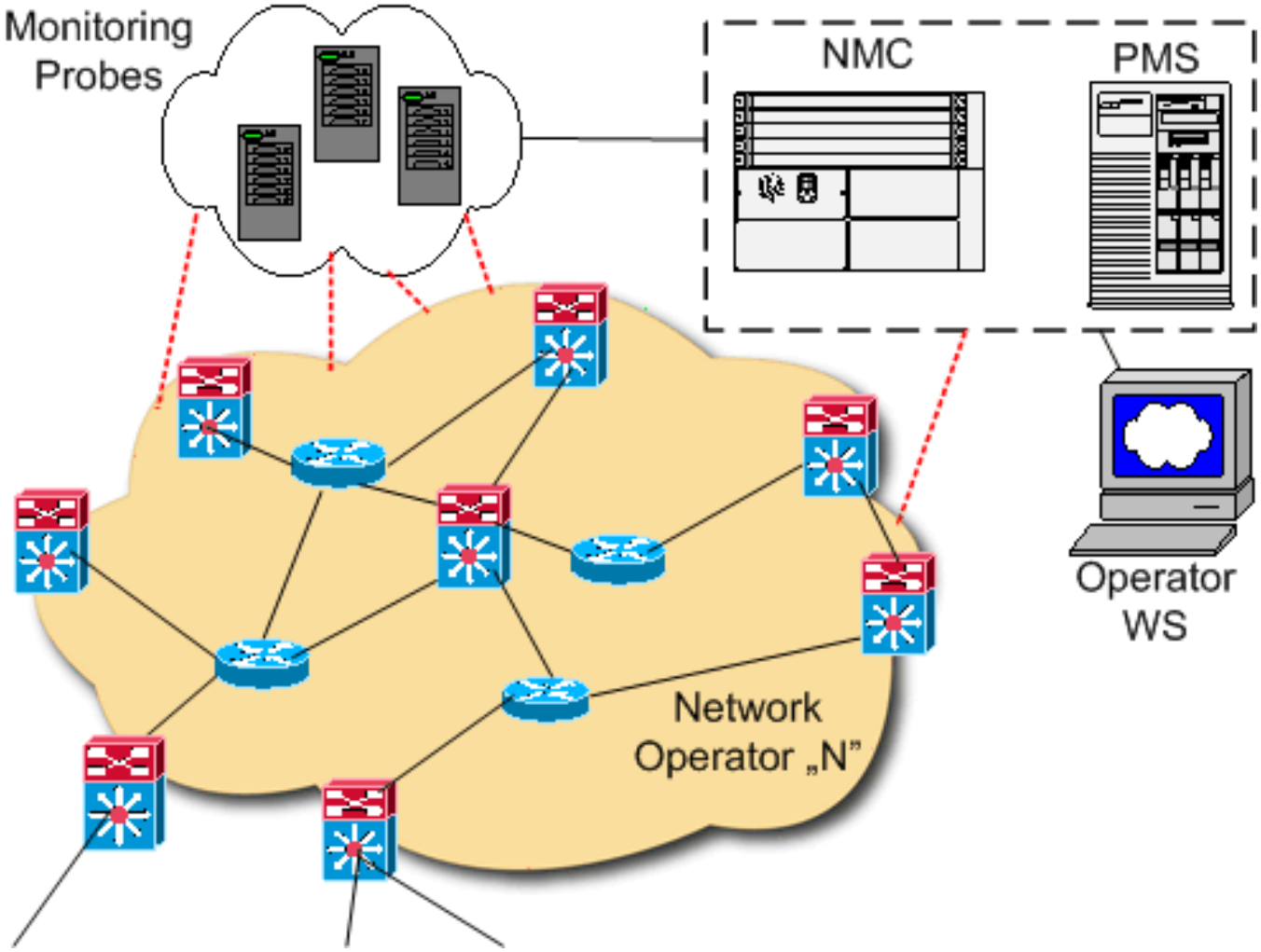




TMN FCAPS



TMN FCAPS – a felügyelő hálózat



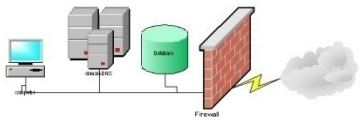
TMN – FCAPS - Fault Management

Az FM felelős azért, hogy a szolgáltatások mindig elérhetőek legyenek.

- Hibaesetek detekciója
- Hibaesetek jelzése az operátor felé
- Hibafeldolgozás
- Hibaok feltárása
- Hiba javítása

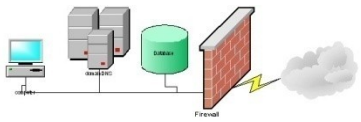
- Az ezekkel kapcsolatos események
  - nyomonkövetése és
  - naplózása.

A hibamenedzsment folyamatról részletesebben – később.



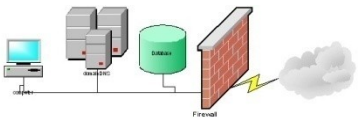
TMN – FCAPS - Fault Management -2

- A rendszerelemektől származó információ lehet Push és Pull jellegű.
  - Mindkettőre van példa az SNMP keretein belül:
    - Push: SNMP trap
    - Pull: SNMP Get, Getnext, Getbulk…



TMN – FCAPS - Configuration M’gmnt

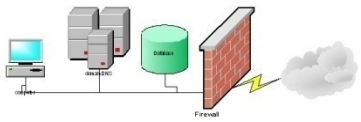
- Mindazokat a funkciókat lefedi, amelyek
  - a (hálózati) elemek felépítésének azonosításával,
  - az építőelemek részleteinek változásával foglalkoznak.
- Ide tartozik
  - Erőforrás-kihasználás
  - Hálózatfenntartás
  - Backup and Restore adatbázis kezelés
  - Topológia-felderítés és nyilvántartás
  - Változás-menedzsment
  - Eszköz- és raktár-adatbázis (Inventory)



TMN – FCAPS - Accounting M’gmnt

- *Használati statisztikák gyűjtése és feldolgozása.
  - *- Eszköz- és egyedi erőforrás használat (CPU, mem,…)
  - * - Hálózat-használat
  - * - Szolgáltatás-használat, stb.

– Felhasználói adatok kezelése
  - Számlázás
  - Kvóta-kezelés

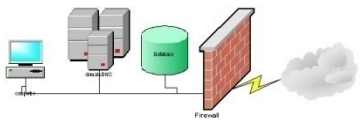


TMN – FCAPS - Performance M’gmnt -1

- Általánosan feladatai közé tartozik
  - teljesítményre jellemző mércék (QoS vs. KPI vs. KQI) gyűjtése,
  - értékelése és
  - a küszöbértékek túllépésének jelzése;
  - a hálózat illetve a rendszer szűkös erőforrásainak lokalizálása,
  - a szűk keresztmetszetek hatásának minimalizálása.

- Üzemeltetési „intelligencia” felhasználása:

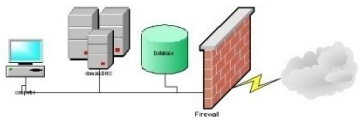
  milyen típusú szűk keresztmetszetek hogyan eliminálhatóak? (Action Plan…)



TMN – FCAPS - Performance M’gmnt -2

- Mindennapi rendszergazdai feladatok:
  - Teljesítmény-adatgyűjtés
    - Passzív
    - Aktív

    - Egyszerű számlált statisztikák
    - Korrelált, származtatott statisztikák
  - Teljesítmény-riport
    - generálás,
    - gyűjtés,
    - archiválás.
  - Teljesítmény adat-elemzés
  - Küszöbértékek karbantartása, túllépés figyelés
  - Problémák jelzése (hasonlóan az FM-hez)



TMN – FCAPS - Security M'gmnt -1

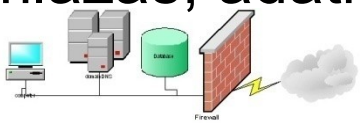
- Feladata a nem jogos (unauthorized, vagy „véletlen") hálózat vagy rendszer-erőforrás használatának minimalizálása.

- AAA:
- - Authentikáció

  (username/password)
- - Authorizáció

  (adott felhasználó hozzáférési/változtatási jogosultságának kezelése) ITU-T M.3010
- - Accounting

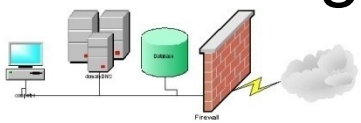
  (számlázás, adatnyilvátartás)



TMN – FCAPS - Security M'gmnt -2

Feladatai:

- Authentikációs rendszer kezelése, karbantartása
- Authorizációs rendszer
  - A szelektív erőforrás-hozzáférés kezelése
  - Felhasználói hozzáférés-kezelés
  - Hozzáférési naplók karbantartása, feldolgozása
- Biztonsági események jelzése
  (event/alarm reporting)
- Biztonsági frissítések kezelése
  (mint a configuration mgmt-ben)
- Biztonsági audit lefolytatása, a kiadódó módosítások elvégzésének ellenőrzése

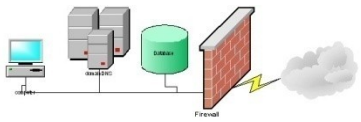


TMN

feladatkörök szintenként

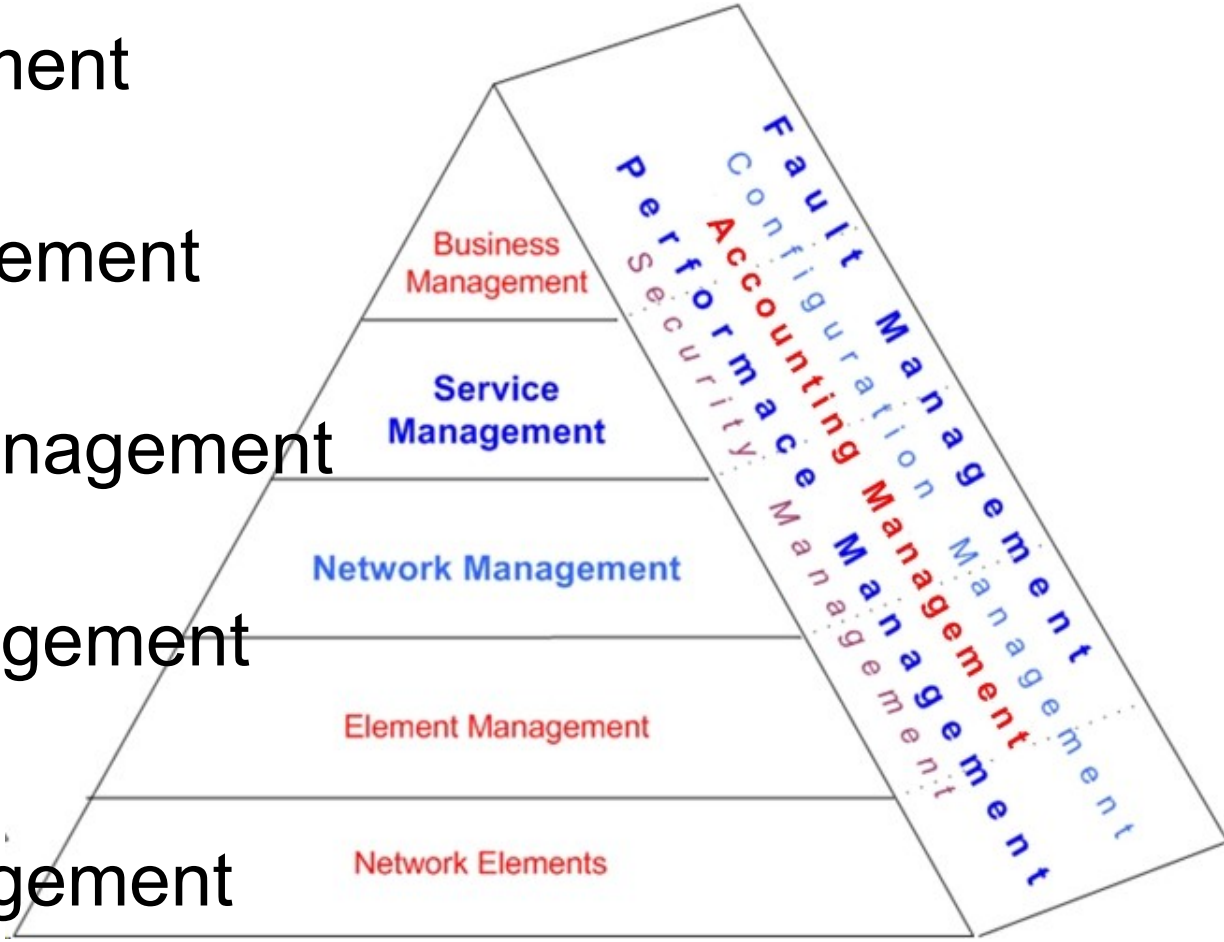
-- Példa az előadáson: --

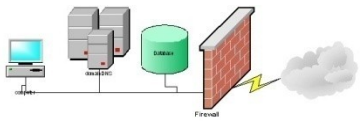
körzeti IPTV szolgáltatás



Business Management

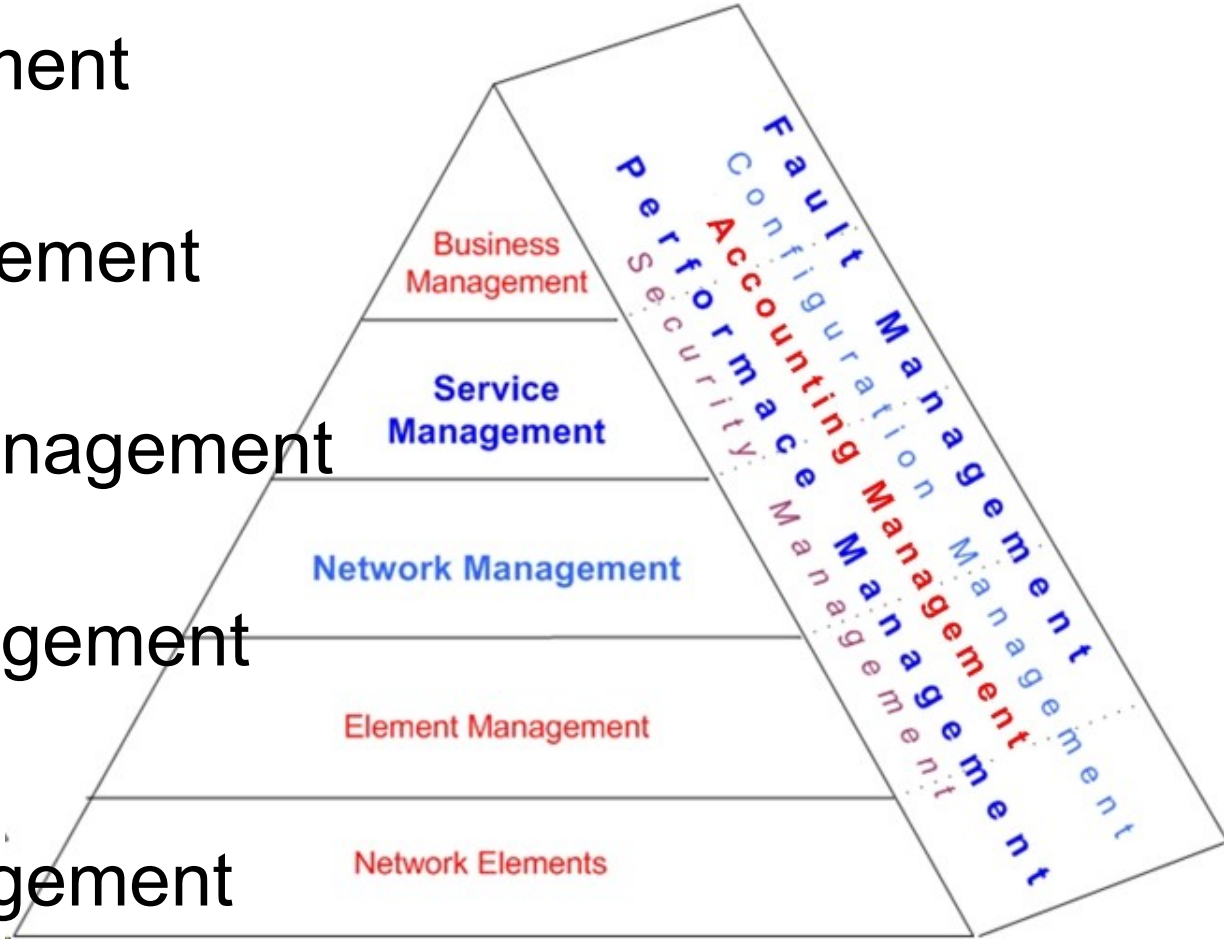
- Fault Management
- Config. Management
- Accounting Management
- Perform. Management
- Security Management

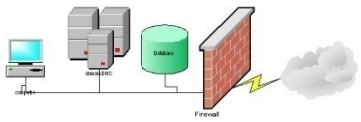




Service Management

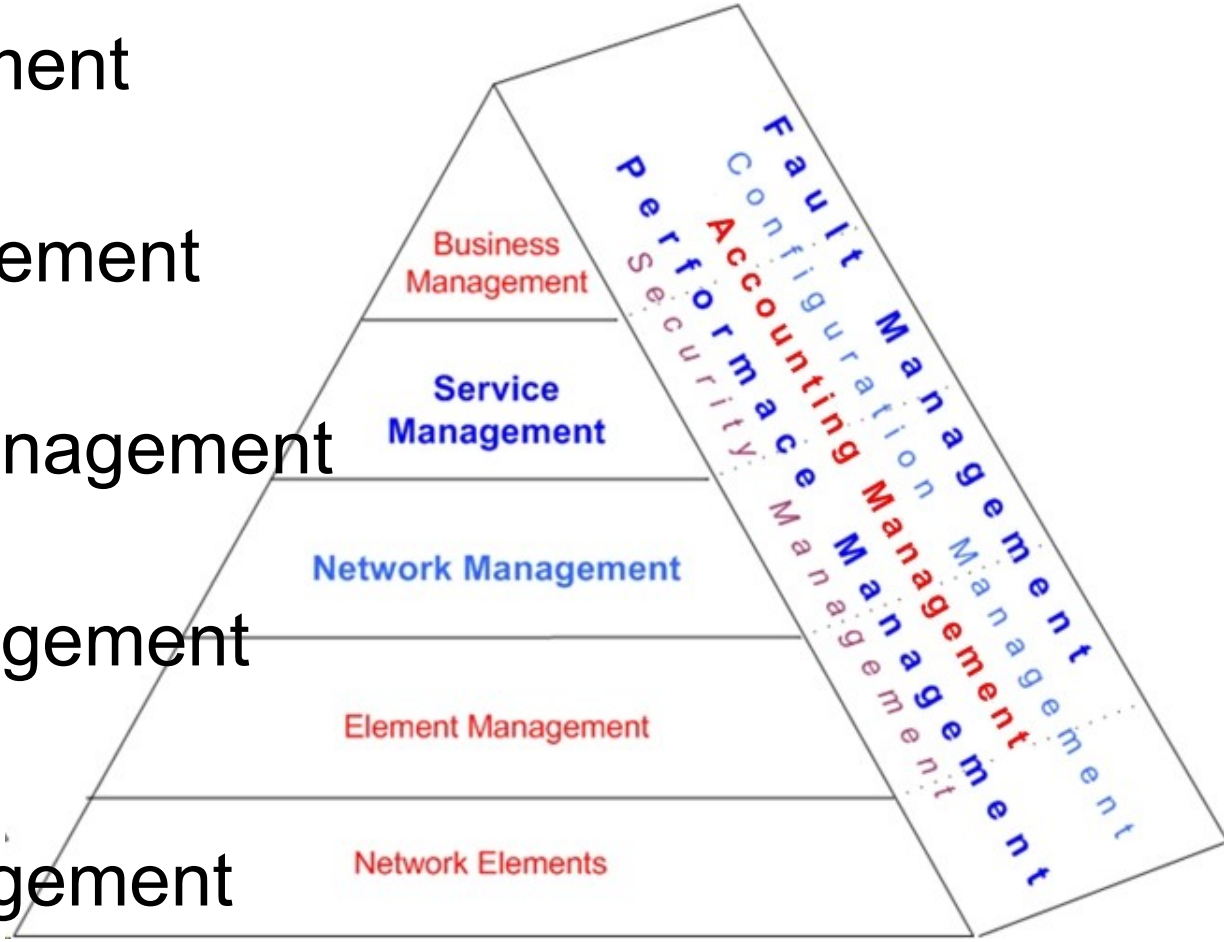
- Fault Management
- Config. Management
- Accounting Management
- Perform. Management
- Security Management

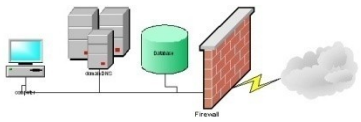




Network Management

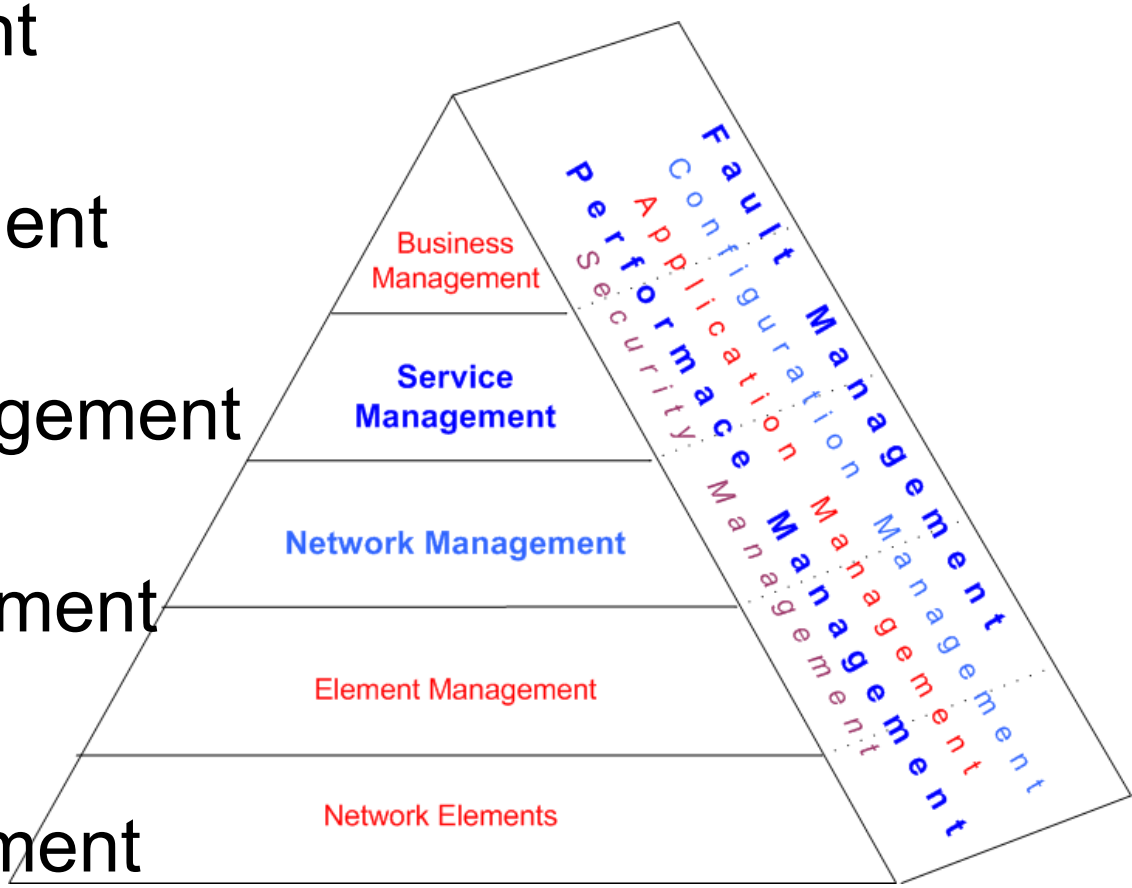
- Fault Management
- Config. Management
- Accounting Management
- Perform. Management
- Security Management

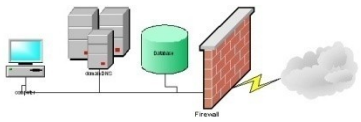




Element Management

- Fault Management
- Config. Management
- Accounting Management
- Perform. Management
- Security Management





TMN – FCAPS

Részletesebb kitérő a

Network Management

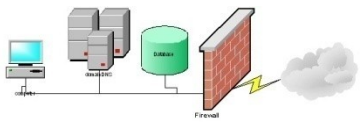
feladatok felé:

Performance Management

-> Forgalom monitorozás

Fault Management

-> Hibamenedzsment



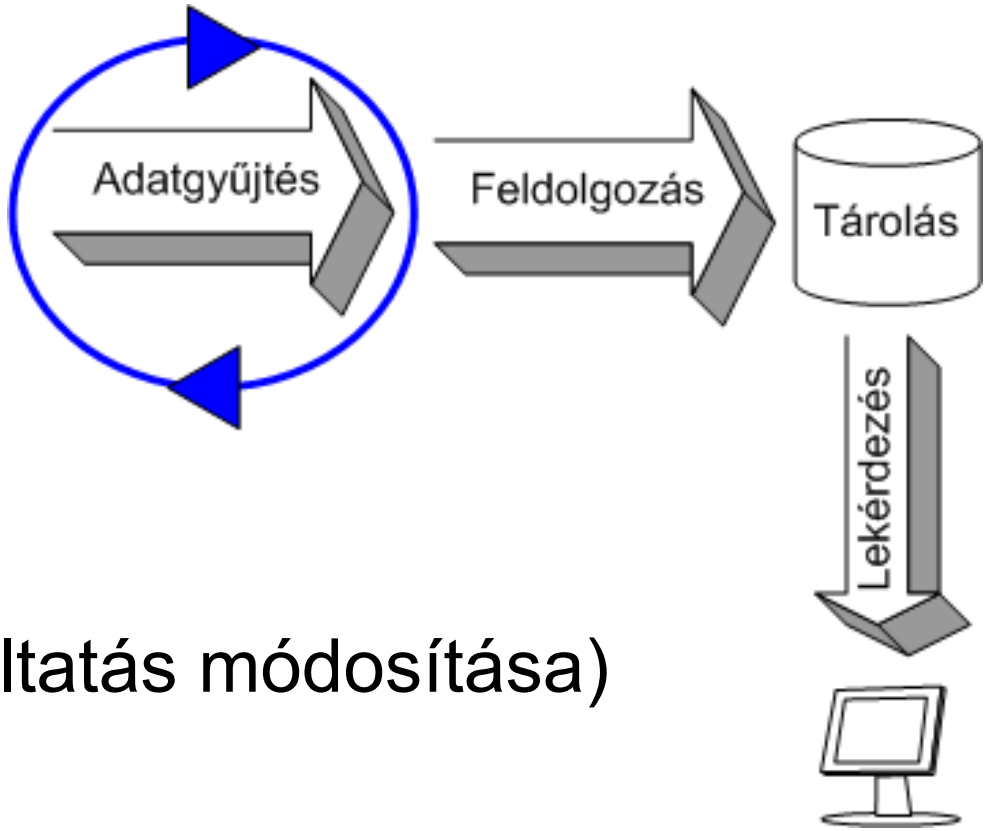
A forgalom monitorozása

Mely feladatoknál használjuk?

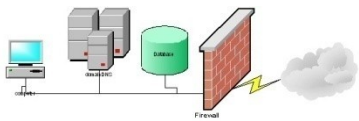
- ❑ Hálózattervezés
- ❑ Hálózati optimalizálás
- ❑ Hálózatfelügyelet

Mit értünk alatta?

- ❑ Monitorozó berendezések csatlakoztatása
- ❑ **Adatgyűjtés**
- ❑ **Adatfeldolgozás**
- ❑ Értékelés

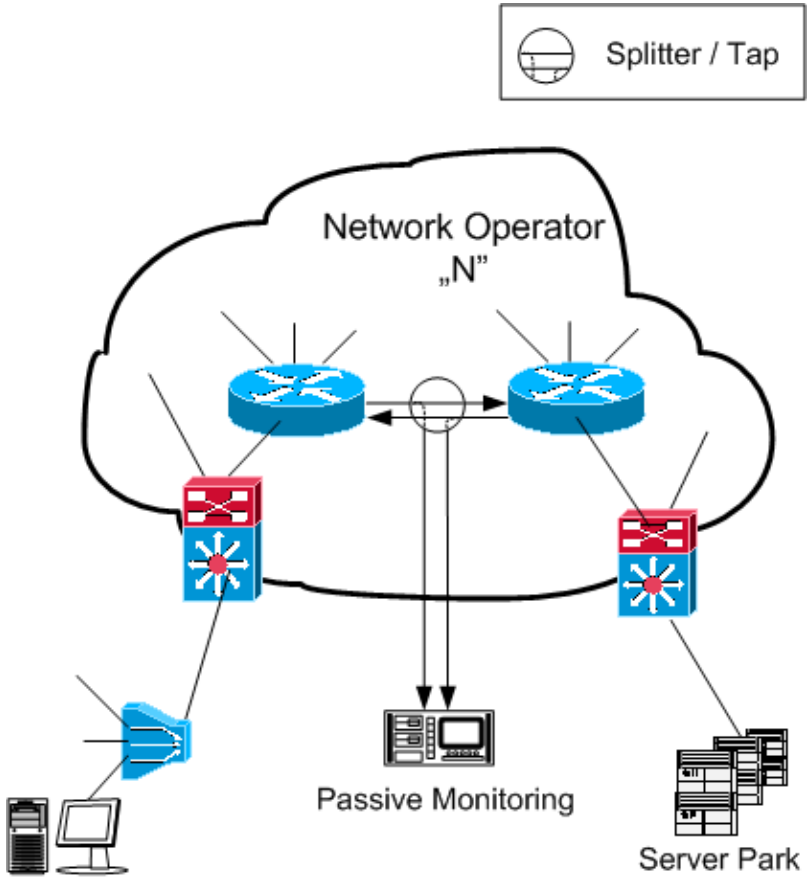


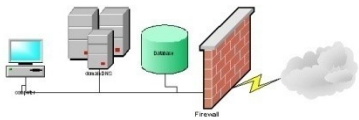
(a hálózat/szolgáltatás módosítása)



A forgalom monitorozása - Módszerek

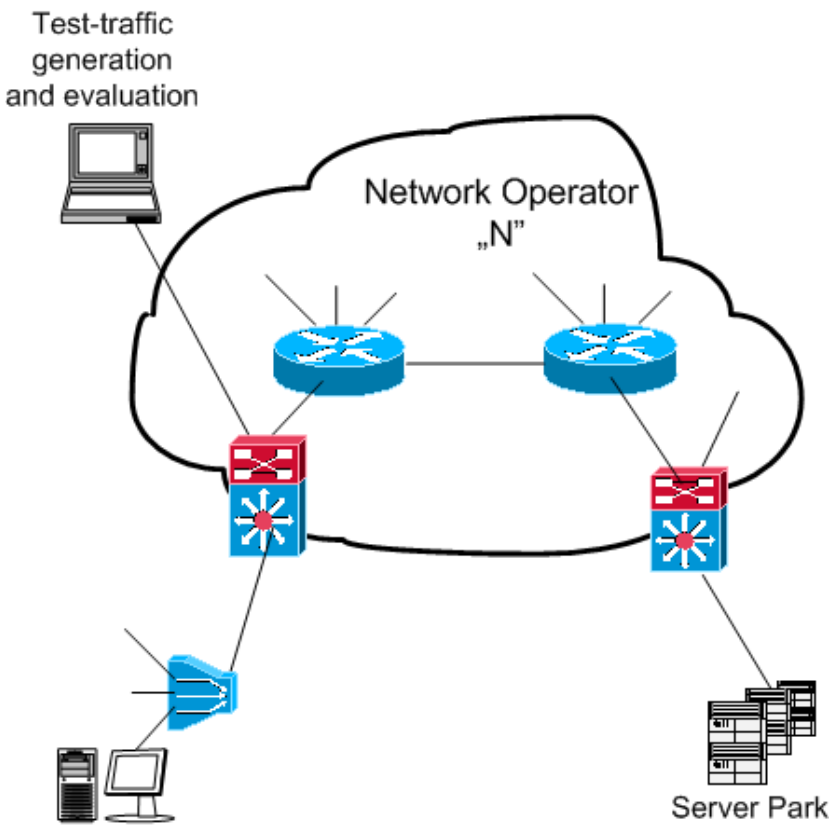
- Passzív monitorozás
  - a hálózati forgalom figyelése, „non-intrusive”
  - zavartalan, tiszta képet ad, a teljes időskálán
  - egyetlen kapcsolat („link”) vizsgálata leszűkíti az elemzés terét
  - több (…az összes…) link vizsgálata sokszor nem lehetséges, vagy az adatfeldolgozás túl bonyolult

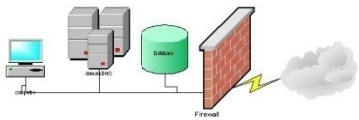




A forgalom monitorozása - Módszerek

- Aktív monitorozás
  - próbaforgalom beiktatása és a „hatás” vizsgálata
  - a meserséges forgalom torzíthatja a vizsgálatokat
  - végpontok közötti vizsgálatra is kézenfekvően egyszerű
  - nem folytonos, csak mintavételezés-típusú eredményeket szolgáltat

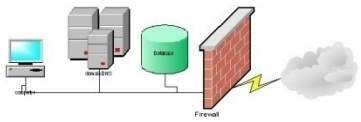




Adatgyűjtés

Milyen típusú adatokat gyűjtünk és dolgozunk fel?

- „Nyers” forgalmi adatok - bitszintű adatok, csomagfejlécek
  - egyszerű, számított statisztikák (hálózati szint)
  - tranzakciós rekordok (szolgáltatás szint)
  - tranzakciós statisztikák
- Topológiai adatok
- Naplóállományok

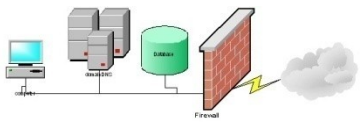


Forgalmi adatok feldolgozása

- Egyszerű, számított statisztikák
  - Csomagszintű statisztikák
    - beérkezési idő eloszlás jellemzői
    - csomagméret eloszlás jellemzői
    - börsztösségi jellemzők

Mire használhatók???

  - Alkalmazás-szintű statisztikák
    - alkalmazások eloszlása (pl. port szerint)
      - felhasznált sávszélesség alapján
      - csomagszám alapján
    - csomagvesztési arány



Forgalmi adatok feldolgozása - 2

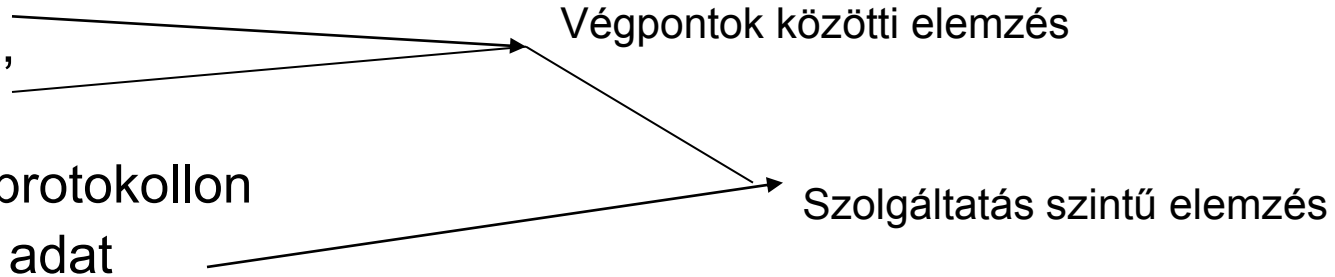
- Tranzakciós (folyam-szintű) rekordok

  Egy tranzakció azonosítása:

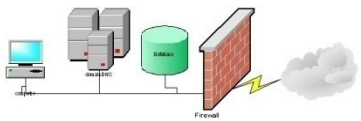
  - 5-tuple: forrás IP, cél IP, forrás Port, cél Port, IP protokoll (TCP vagy UDP)
  - 3-tuple: forrás IP, cél IP, IP protokoll
  - N-tuple…

A rekord tartalma:

- mikor,
- honnan,
- hová,
- milyen protokollon
- mennyi adat
- ...„hogyan”



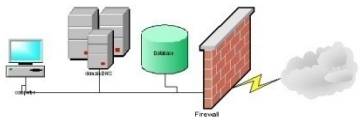
haladt



Forgalmi adatok feldolgozása - 3

- Tranzakciós statisztikák
  - Átvitt adatmennyiség elephants - mice
  - Időbeli terjedelem tortoise - dragonfly
  - Tranzakció börsztössége (jitter) porcupine - cheetah
  - Csomagvesztési arány
  - Forgalmi irányok, „diszperzió”
  - (számlázáshoz használható információk)

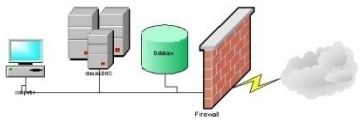
… alkalmazásonként eltérő küszöbértékekkel és számítási módszerekkel



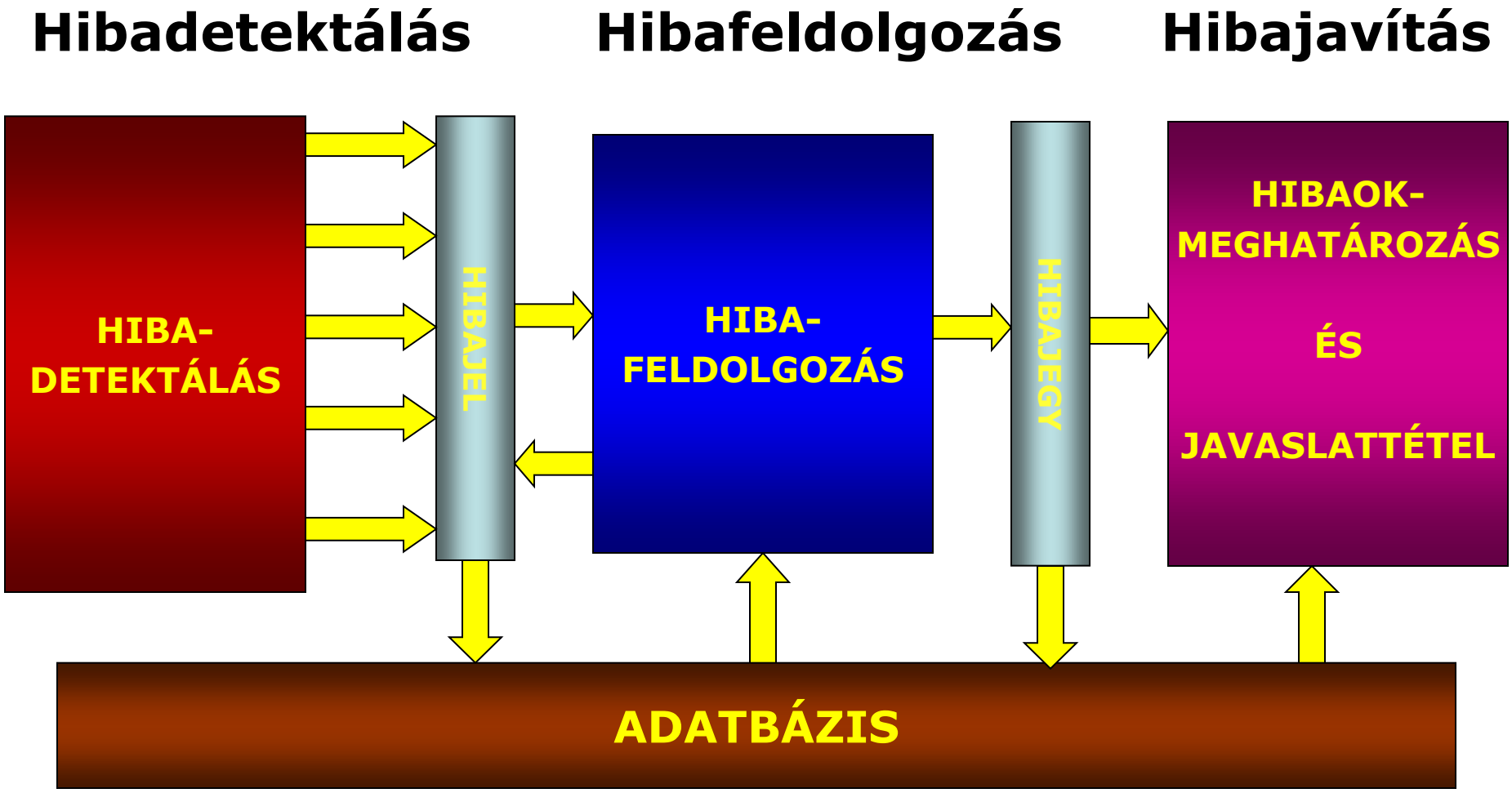
Hibamenedzsment

- A hibamenedzselés folyamata
- A folyamat elemei
- Elvi módszerek
- Megvalósítási lehetőségek

- Alkalmazási példák



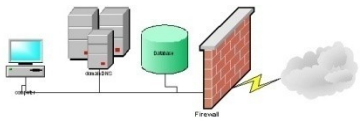
A hibamenedzsment folyamat



Hibajel – Hibajegy

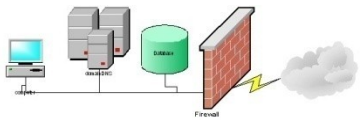
Alapvető különbségek!

- **Hibajel** (EVENT, esemény, naplóbejegyzés)
- **Hibajegy** (ALARM, megszüntetendő hiba jelzése)



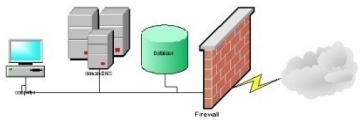
A hibamenedzselés folyamata

- **Hibadetektálás**
  - Feladata: kifejezetten a szolgáltatást hátrányosan érintő hibajelenségek minél hamarabbi észrevétele és a hibamenedzsment rendszer értesítése
  - Eredménye: **Hibajelek** halmaza
- **Hibajelfeldolgozás**
  - Feladata: a detektált hibajelekből történő hibajegy-generálás folyamatának szabályozása
  - Eredménye: **Hibajegyek** halmaza
- **Hibaok-meghatározás és hibajavítás**
  - Feladata: a keletkezett hibajegyekben megfogalmazott hibajelenség(ek) okainak felderítése
  - Eredménye: Javaslattétel ezek kijavítására



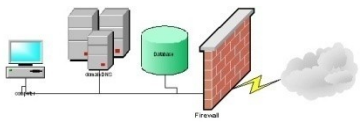
Hibadetektálás

- A hálózatban használt ***hibadetektáló elemek*** használata, szolgáltatás-specifikus hibaüzenetek kiszűrése (pl. Syslog, QoS monitor (próbahívó))
- A tranzakciókról ***információt gyűjtő elemek*** használata, adatvizsgálat (pl. AAA rekordok)
- ***Aktív monitorozó elem*** használata
- ***Felhasználók által jelzett hibák*** gyűjtése
- A különböző hibajel-forrásokból gyűjtött hibajelek *egységes kezelése* (egységes hibajel-formátum) és *továbbítása* a hibajelfeldolgozó alrendszer felé



Hibajelfeldolgozás

- Szűrés
  - A beérkezett hibajelekre különböző **szűrőszabályok** definiálhatóak és ezek alapján szabályozható a hibajegy-generálás
- Korrelálás
  - A beérkezett hibajelekből **korrelációs szabályok** alapján új, összetettebb hibajelek generálhatóak, melyek a szabályokban megfogalmazott hibajel-összefüggések alapján pontosabb információt adnak a hibajegy-generáláshoz
- Trendanalízis
  - A beérkezett hibajelek hosszabb távú elemzése alapján, **trendszabályok** definiálásával olyan folyamatokból generálható hibajel, melyek feltételezhetően az adott szolgáltatást sérteni fogják amennyiben a folyamat trendje nem változik

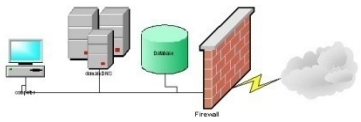


Hibajelfeldolgozás - 2

– Szűrés

- A beérkezett hibajelekre különböző **szűrőszabályok** definiálhatóak és ezek alapján szabályozható a hibajegy-generálás

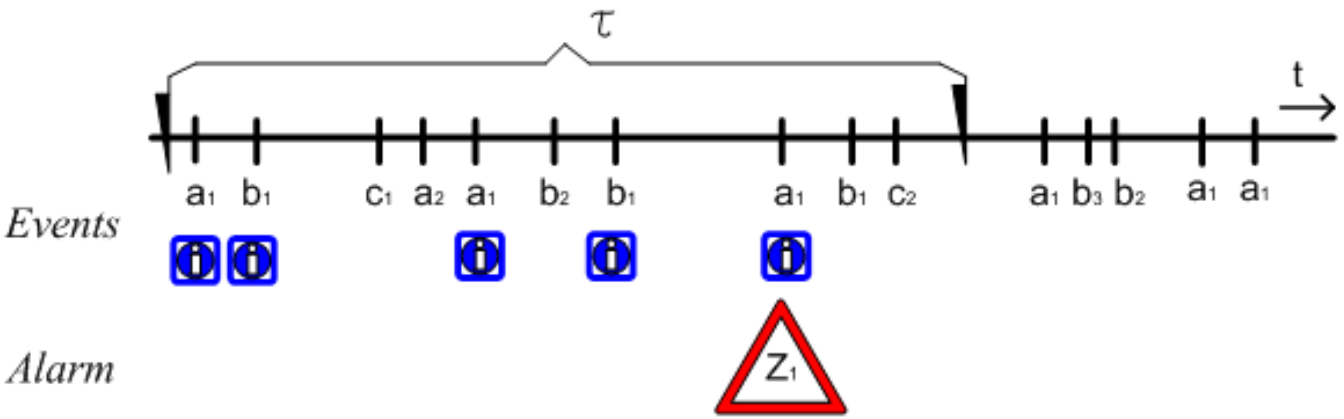
- Számláló (Counter)
- Elnyomó (Suppress)
- Redundancia-gátló (Redundancy)
- Domináns elnyomó (Dominance)



Hibajelfeldolgozás - 3

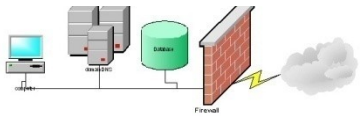
❑ Korrelálás

Correlation rule: *if* during $t<\tau$ events $(\alpha_1 a_1 | \alpha_2 a_2 | \alpha_3 a_3)$ & $(\beta_1 b_1)$ arrive
then: report alarm Z_1



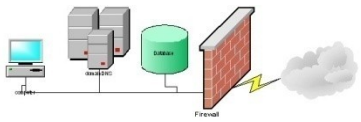
where

a,b,c,... z	- event types
1,2,3	- priority of the event/alarm
$\alpha,\beta,\gamma,\ldots\omega$	- counter thresholds
A,B,C,...Z	- ALARMS



Hibaok-meghatározás és hibajavítás

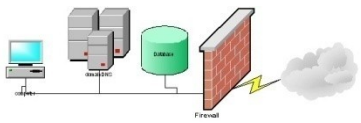
- Hibaok-meghatározás
  - Egyszerű, korreláció-alapú
  - Algoritmikus…
- Hibajavítás
  - Passzív hibajavítás, a talált hibaok(ok) elhárítására a rendszer javaslatot tesz
  - Maga a hibaelhárítás tevékenysége a hálózatfelügyeletre hárul



Hibaok-analízis

Esemény-korrelációs és hiba-lokalizációs módszerek

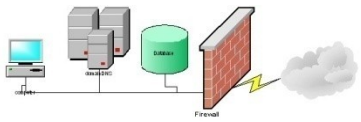
- Alarm vektor
- Szabály alapú
- Eset alapú (case-based)
- Modell alapú
- Fuzzy
- Neurális hálózatok
- Oksági hálózatok
- Szavazás
- Adatvezérelt modell



Alarm vektor

- Kétdimenziós tömbben
  - a lehetséges (logolt) események,
  - a lehetséges korrelációval kialakuló hibakódok
- Adott méretű időablakot vizsgálva a beérkezett alarmokat 1-el, a többit 0-val jelölve egy hosszú kódszót kapunk.
- Javasolt alarm az lesz, amelynek a legkisebb a Hamming-távolsága ehhez a kódszóhoz képest.

- Nagyon gyors, hatékony módszer
- De eléggé rugalmatlan…

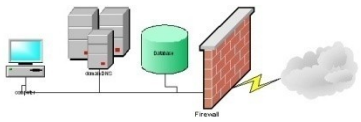


Alarm vektor - példa

	link nem elérhető	útvonal nem elérhető	"interface down"	eszköz nem válaszol	magas vesztés	magas jitter	…	…
Link x hibás	1	1	0	1	0	0	…	…
Link x túlterhelt	0	1	0	0	1	1	…	…
"interface misconfig"	1	1	1	1	0	0	…	…
xy hardware hiba	0	1	0	1	1	0	…	…
xy irány túlterhelt	0	0	0	0	0	1	…	…
…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…

t1 és t2 időpillanatok között:

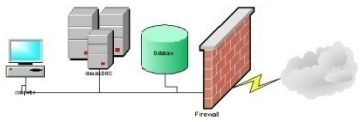
1	**1**	**1**	**0**	**0**	**0**	…	…



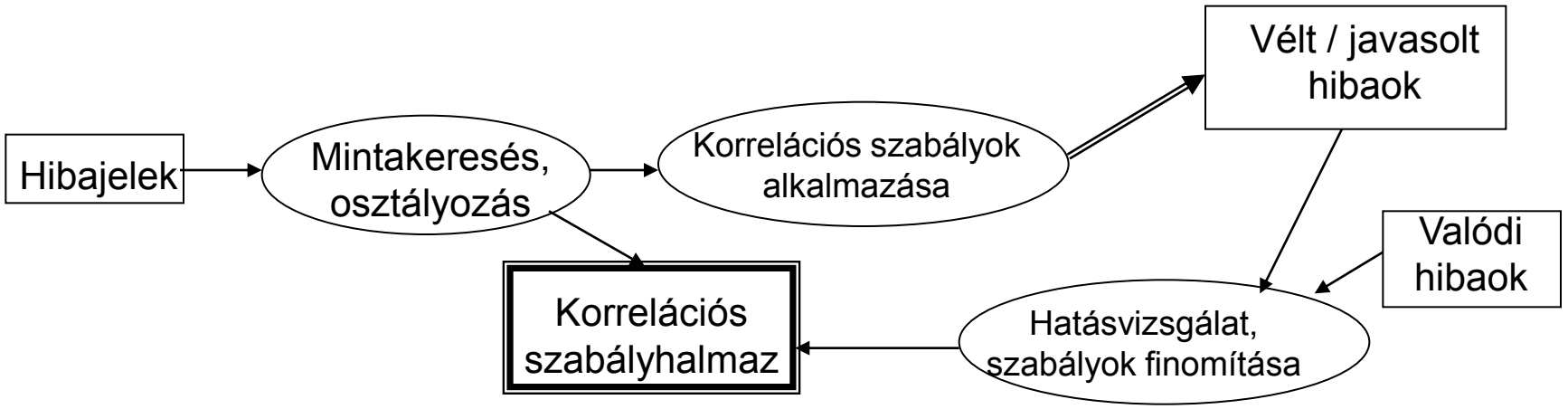
Szabály alapú esemény-korreláció

- Alapja egy tudásbázis, ami leírja, hogy
  - milyen esetekben
  - milyen **összetett** alarmmal kell **helyettesíteni** a
  - beérkező **elemi** hibajeleket.
- A tudásbázisban a szabályok tipikusan a Bool-algebrára jellemző relációként jelennek meg
- Ha a reláció értéke igaz, akkor végrehajtódik a szabályhoz rendelt művelet (pl. összetett alarm generálása)
- A módszer
  - egyszerű,
  - a szabályok rugalmasan változtathatók, és
  - a szabályok kiértékelése is gyorsan kivitelezhető.

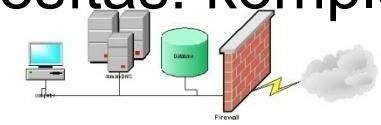
- {2; a104 || a302;Host=<Korrelátor IP címe>; Kind=6; Prio=2; Code=602; Parameter="HIVASOK RENDELLENESEN VEGZODNEK"}



Eset alapú (case-based) korreláció

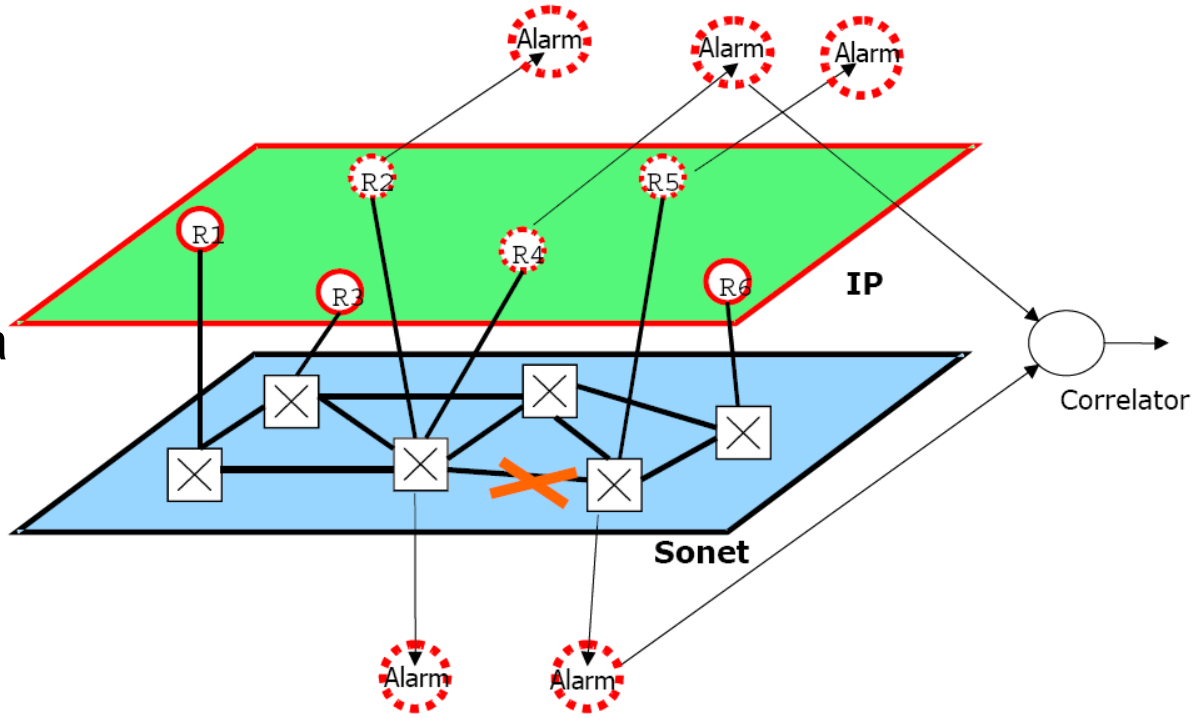


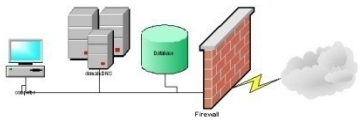
- Meglévő hálózati adatok feldolgozása
  - mintakeresés, osztályozás
- Korrelációs szabályok kialakítása
- Korrelációs szabályok alkalmazása
- A döntések visszacsatolása
- Szabályok finomítása (machine learning)
- Megvalósítás: komplex



Modell alapú

- A hálózati topológiát egy rugalmas modell írja le
- A korrelációs szabályok hierarchikusak
- Rugalmasan kötődnek a topológiához (sablon)
- A szabályrendszer a topológia változása után automatikusan generálható. Bonyolult, de nagyon rugalmas megoldás.

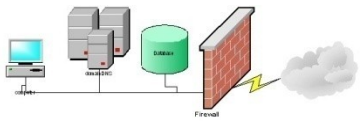




Fuzzy

- Fontos emlékeznünk rá, hogy az egyes hibaokokról való **passzív** hibakorrelációs döntés **bizonytalan**.

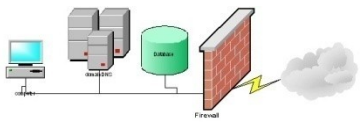
- A hálózatot és az alarmokat Fuzzy halmazokkal leírva is lehet alarm-korrelációs rendszereket készíteni.
- Bonyolult, bár (bizonyára) gyors megoldás.



Oksági hálózat, Bayes hálózat

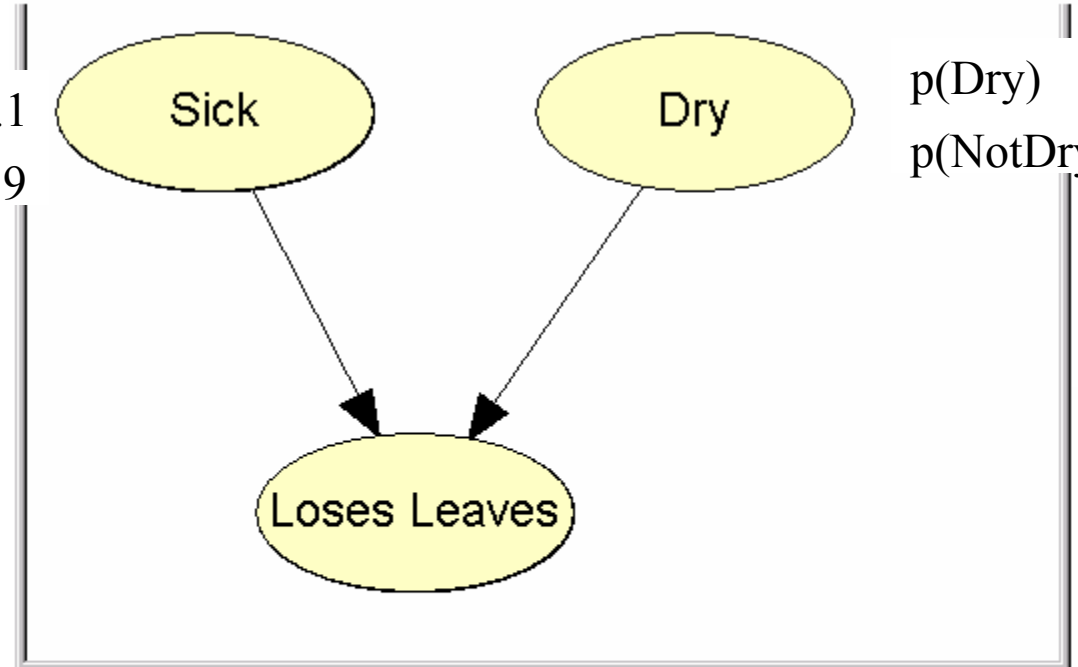
- Oksági hálózat
  - Hibalehetőségek
  - Megfigyelések
  - Hiba-okok

- Bayes-hálózat
  - az oksági hálózat éleihez valószínűségek vannak rendelve
  - a bizonytalanság leírásán van a hangsúly
  - a hálózat csomópontjaihoz rendelt állapotoktól (normál,hibás,…) függően **különböző valószínűséggel** jutunk a következő szintű hibalehetőség-csoporthoz
  - az élekhez tartozó valószínűségek megfelelően jó megválasztásával a legvalószínűbb korrelált hibajegy jelezhető
  - az élek valószínűségei a valódi eredmények visszacsatolásával változtathatóak (machine learning)



Egy egyszerű Bayes-hálózat

p(Sick) = 0.1
p(NotSick)=0.9



p(Dry) = 0.1
p(NotDry) =0.9

Dry	Dry		NotDry	
Sick	Sick	NotSick	Sick	NotSick
LosesLvs	0.95	0.85	0.9	0.02
NotLosesLvs	0.05	0.15	0.1	0.98

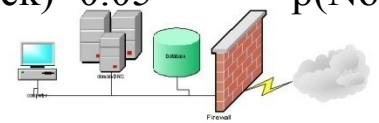
Mitől hullanak a levelek?

p(LosesLvs |Dry,Sick)=0.95
p(NotLosesLvs|Dry,Sick)=0.05

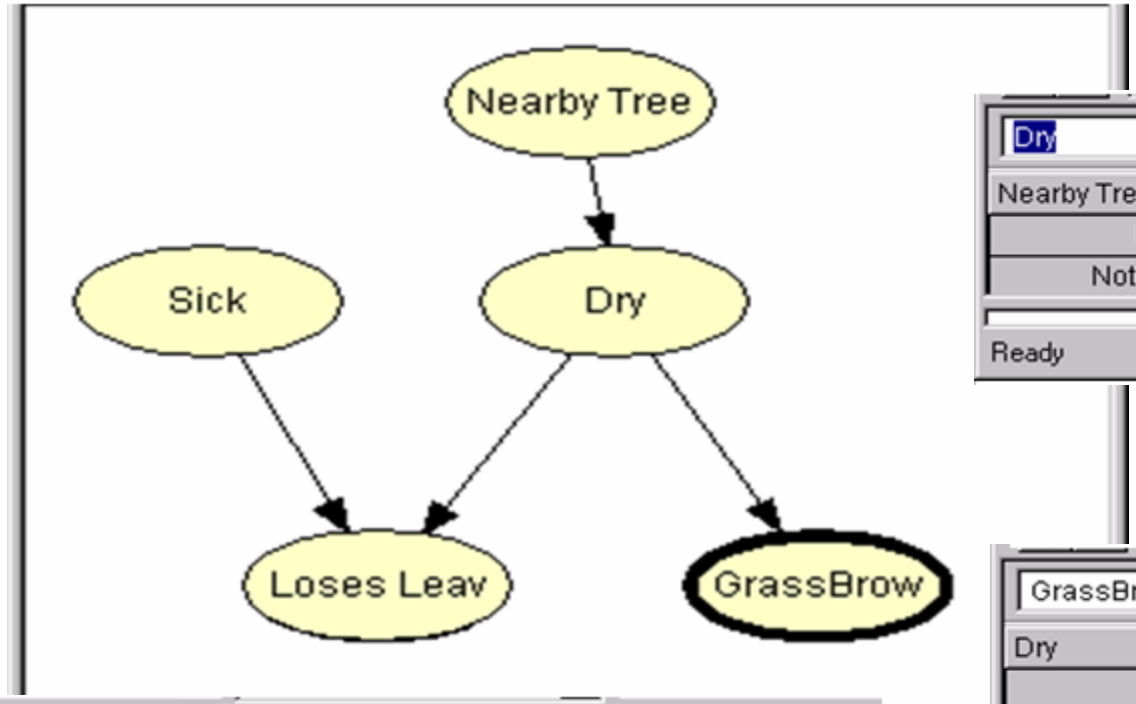
p(Losesvs |Dry, NotSick)=0.85
p(NotLosesLvs|Dry, NotSick)=0.15

etc.

Forrás:
A Simple Bayesian Network,
Alan Rector,
The University of Manchester



Bayes hálózat – több összefüggéssel



Dry | Labelled

Nearby Tree	yes	no
Dry	0.7	0.1
NotDry	0.3	0.9

Ready

GrassBrown | Labelled

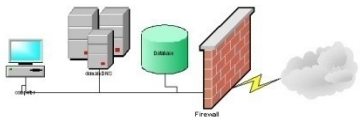
Dry	Dry	NotDry
yes	0.9	0.1
no	0.1	0.9

Node Type

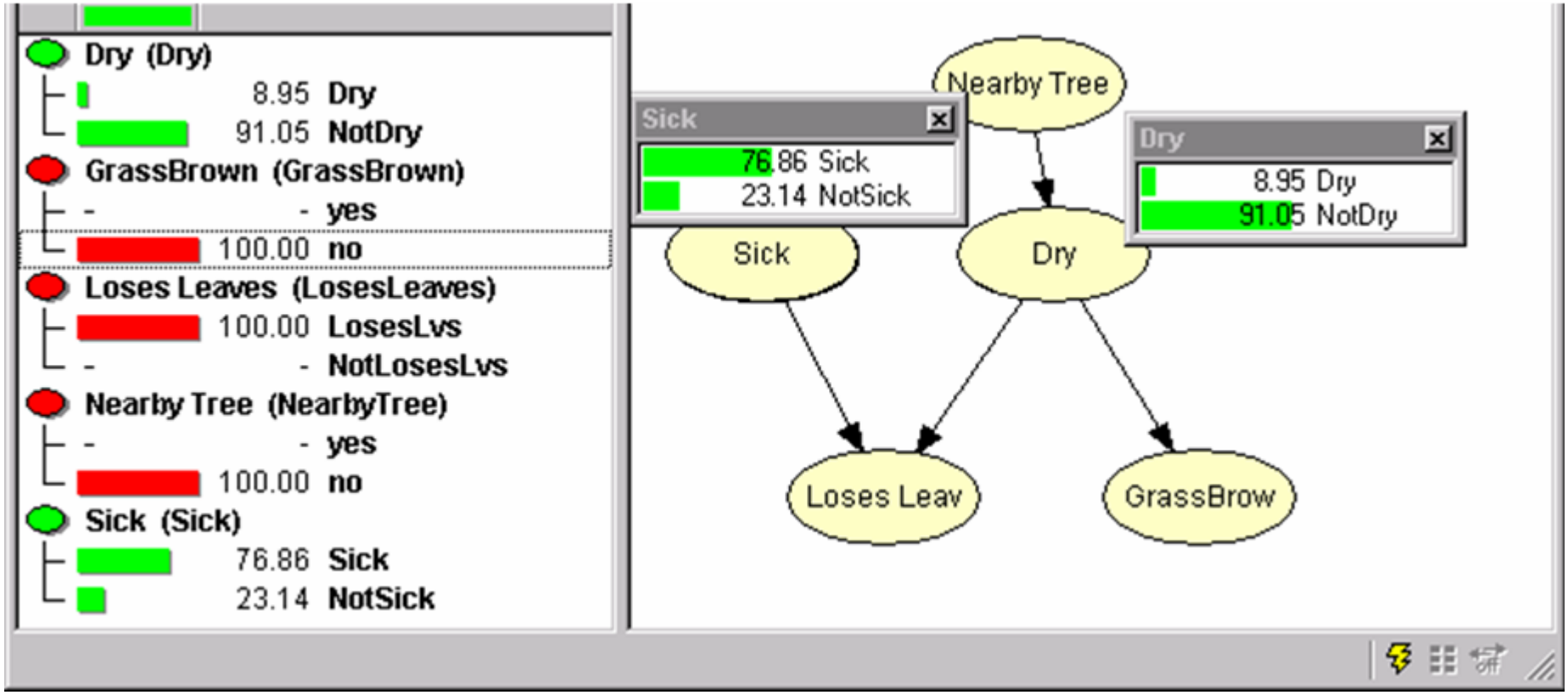
Ready

Dry	Dry		NotDry	
Sick	Sick	NotSick	Sick	NotSick
LosesLvs	0.95	0.85	0.9	0.02
NotLosesLvs	0.05	0.15	0.1	0.98

Forrás:
A Simple Bayesian Network,
Alan Rector,
The University of Manchester

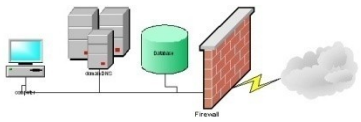


Bayes hálózat kiértékelés - 1

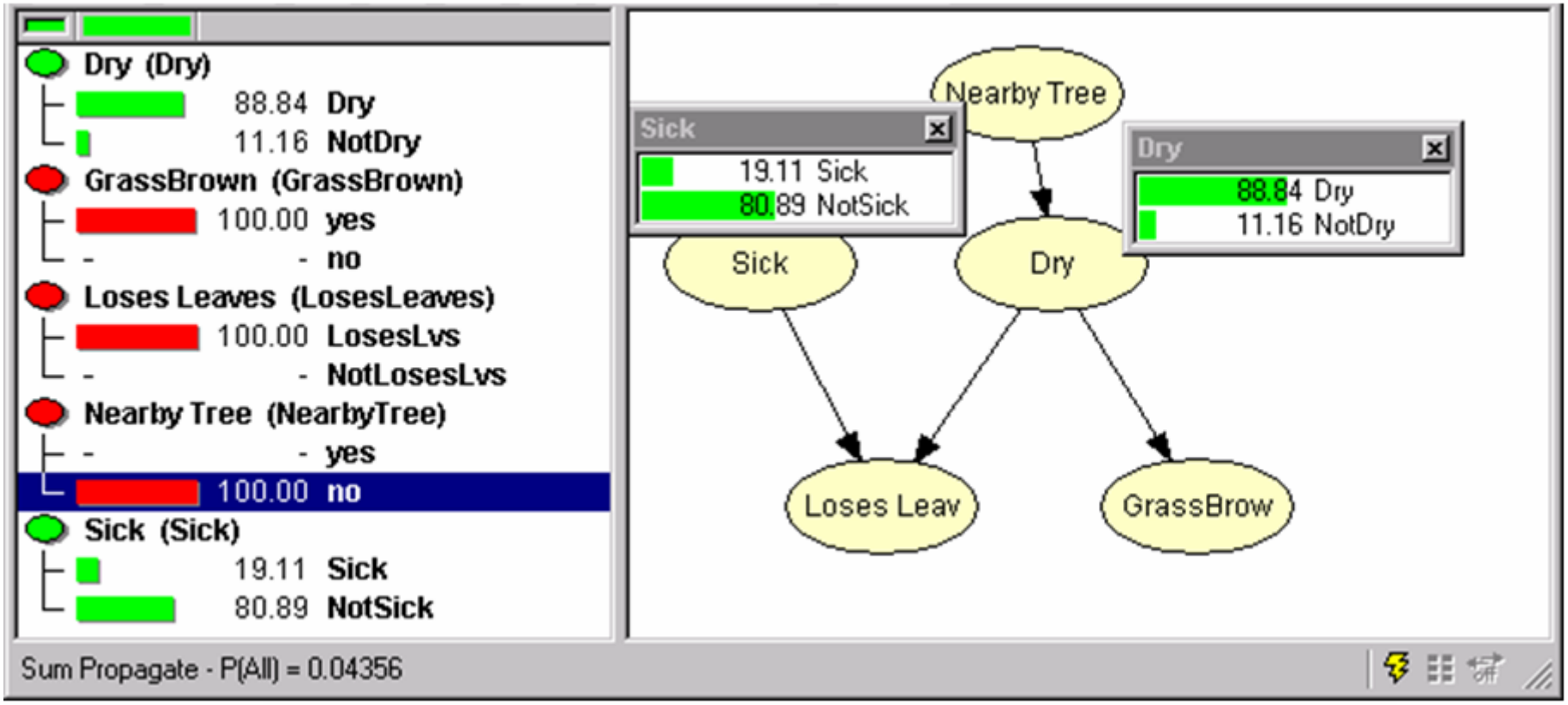


A bizonyítékok (levélhullás, nincs környező barna fű) betegségre utalnak

Forrás:
A Simple Bayesian Network,
Alan Rector,
The University of Manchester

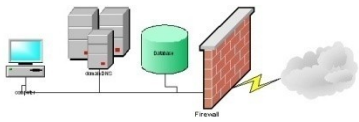


Bayes hálózat kiértékelés - 2



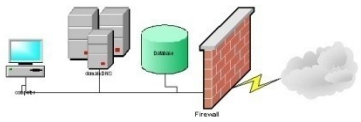
A levélhullás és a környező barna fű akkor is kiszáradásra utal, ha nincs a közelben nagy fa…

Forrás:
A Simple Bayesian Network,
Alan Rector,
The University of Manchester



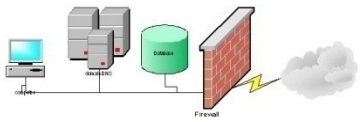
Szavazás

- Központi döntés helyett elosztottan
- Minden döntésképes csomópont megbecsüli, hogy a hozzá eljutott információk szerint milyen hibák korrelálhatóak, majd ezt egy dedikált csomópont kiértékeli.
- Ha a csomópontok jelentősen különböző funkcionalitással rendelkeznek, a módszer használhatósága csökken.



Neurális hálózat

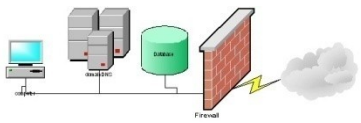
- Az esemény-korrelációra nehezen ráhúzható tanulási folyamat
- Bonyolult, sok állapotú hálózat
- …emiatt ezen a területen nincs használható implementáció



Adatvezérelt modell

A hálózati hibákat feltáró szakemberek módszereit követi

- A **hibajegy paramétereiből** indul ki
- A lehetséges (tipikus) hibaokok után kutatva **aktív ellenőrzések** kezdeményezése
- Ha egy ellenőrzéshez előállnak a **kiindulási adatok**, azt el is indítja
- Az ellenőrzések **eredmény**étől függően újabb adatok beszerzése, újabb ellenőrzések…
- A tesztek végrehajtása **párhuzamosan** zajlik



Adatvezérelt modell – a Petri hálók

- Az adatvezérelt számítási architektúra legismertebb leírási módja a Petri háló.
- Alapelemei:

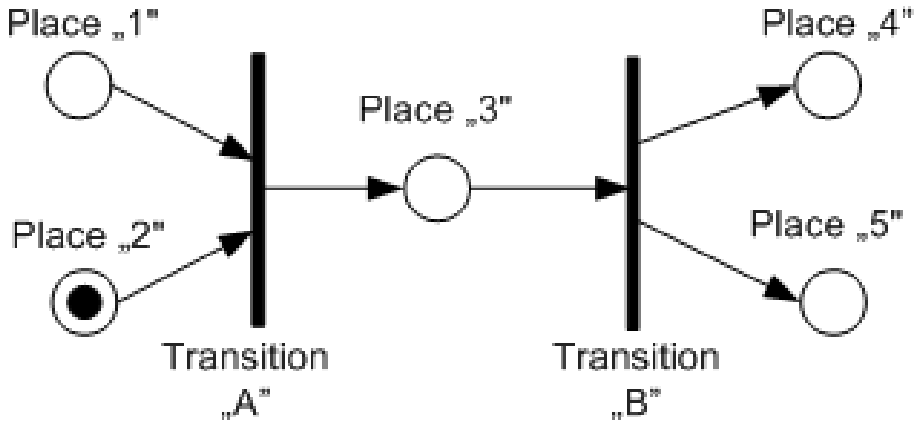
❑ Átmenetek (transitions)

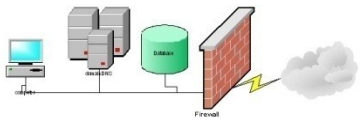
❑ Helyek (places)

❑ Zsetonok (token)

A Petri háló kiindulási helyzetében néhány „hely” tartalmaz zsetonokat.

Ezek olyan adatok, amelyek a kiinduláskor is rendelkezésre állnak.



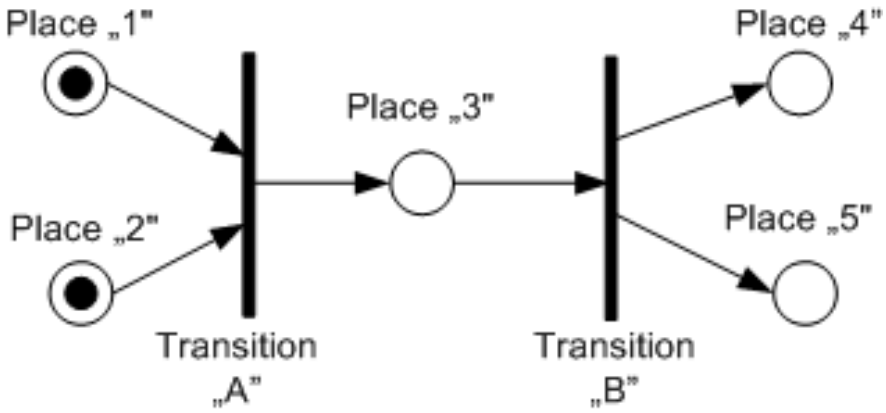


Adatvezérelt modell – a Petri hálók (2)

- Egy „átmenet” akkor „tüzel”, ha minden bemeneti helyén van „zseton”.

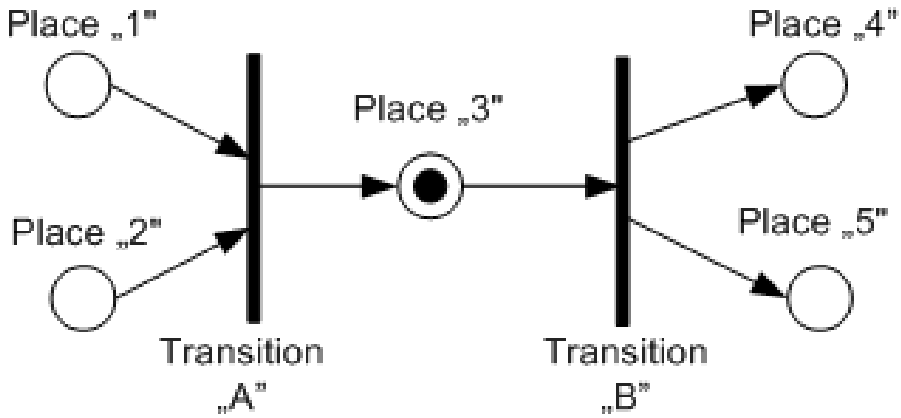
- A „**tüzelés**” hatására
  - ❑ az összes bemeneti helyről eltűnik a zseton
  - ❑ az összes kimeneti helyén zseton jelenik meg

(nem a zsetonok „vándorolnak”, azok csak jelzik, hogy mely helyeken áll rendelkezésre adat)

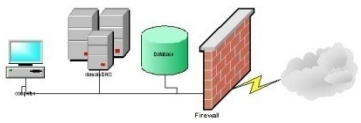


Adatvezérelt modell – a Petri hálók (3)

- … az „A” jelű átmenet tüzelése után előálló helyzet:

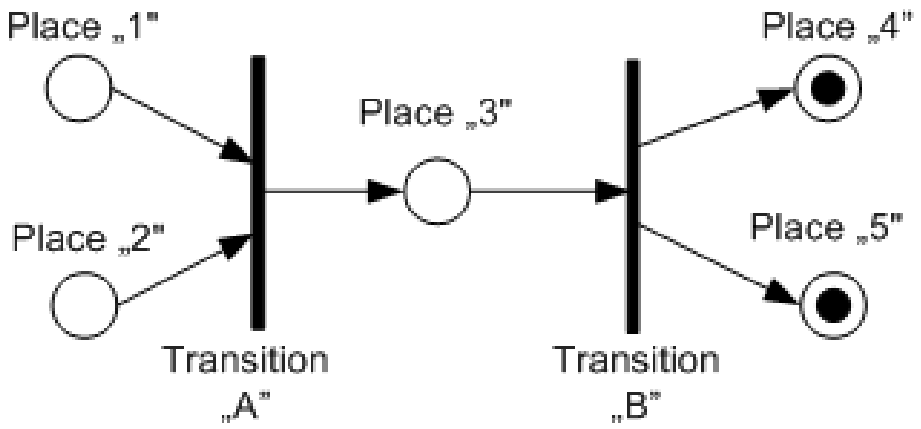


- Ha az „átmenetek” elemi függvényeket, **hibakereső ellenőrzéseket** testesítenek meg, akkor az ezekből kialakított Petri hálóval szimulálható a szakemberek által elvégzett **ellenőrzés-sorozat**.

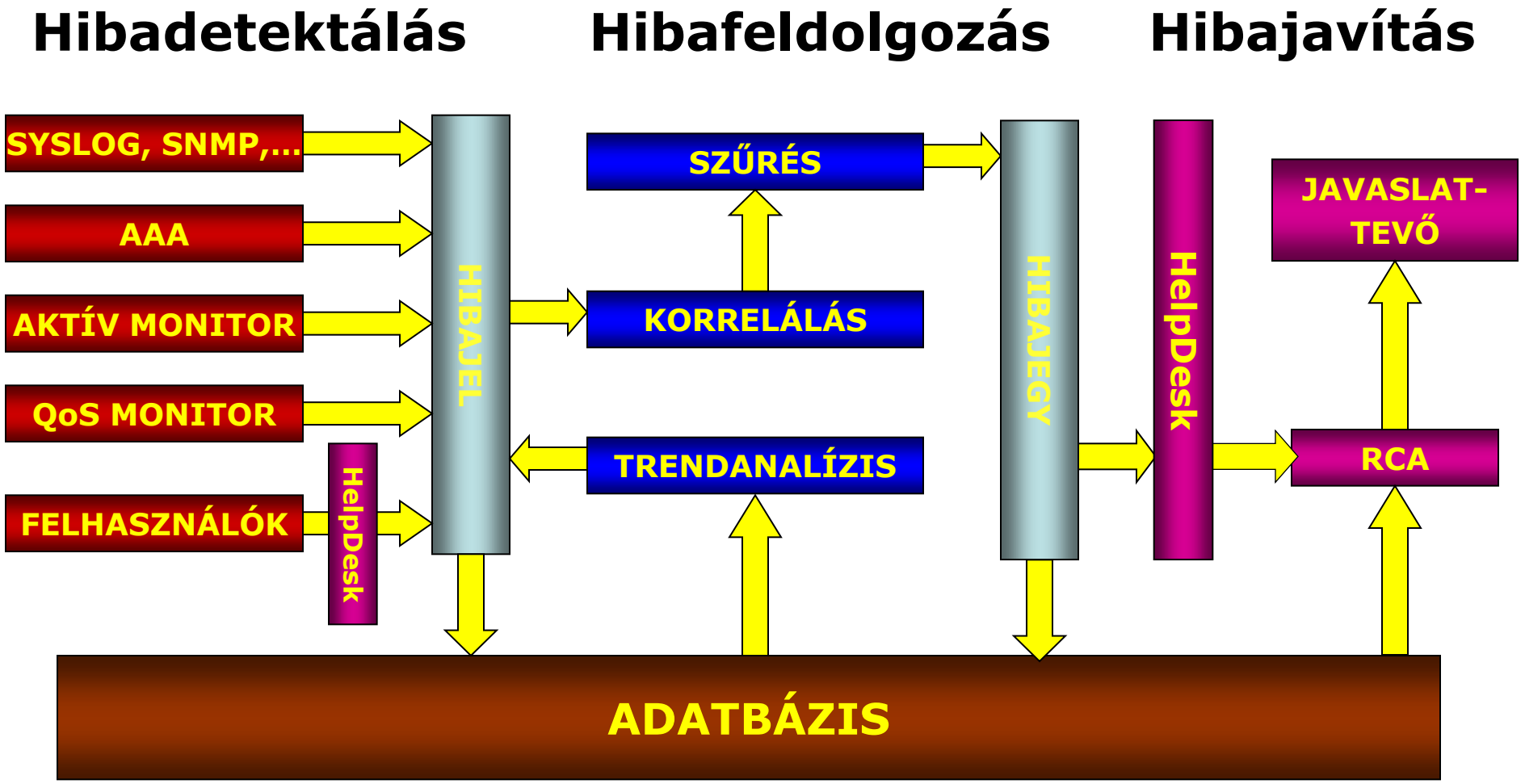


Adatvezérelt modell – a Petri hálók (3)

- … a „B” jelű átmenet tüzelése után előálló helyzet:
- a Petri háló végállapota



Esettanulmány: VoIP szolgáltatás



Az üzemeltetés információbiztonsági kérdései

BME VIK TMIT

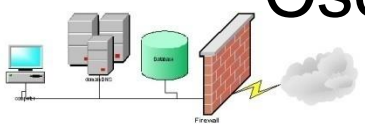
Mérnök-informatikus BSc szak

dr. Jankó Árpád, CISA, CRISC, CISSP

T-Systems Magyarország Zrt.

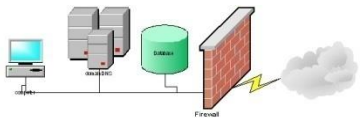
Információbiztonsági Tanácsadás

Csoportvezető



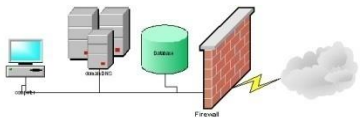
Tartalom

- Miért kell megvédeni az információt?
- Mi az információbiztonság?
- Szabályozási rendszer
- Üzemeltetés biztonsága
- Fizikai biztonság
- Internet, cloud, email biztonság
- Infrastruktúra biztonsága
- Incidenskezelés
- Tipikus problémák



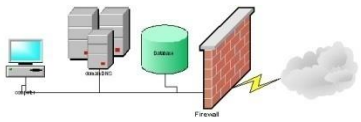
Miért vagyunk célpontok?

- Adatok nagy része elektronikus formában létezik
- Ezek egy része bizalmas, mások számára is értékkel bír
  - Anyagi, személyes, politikai célok
- IT eszközöktől erős függés (tárolás, alkalmazások, kommunikáció, stb.)
- A világ „nem barátságos”



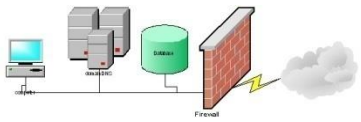
Kitől/mitől kell félni?

- Természeti események
- Hw/sw eszköz meghibásodás
- Emberi tényező
  - Hackerek
  - Szervezett alvilág
  - Konkurencia
  - Belső munkatársak
  - Titkosszolgálatok
  - Véletlen hiba



Milyen eseményektől kell félni?

- Személyazonosság ellopása, és azzal visszaélés
- Adatok integritása sérül
- Adatok vagy eszközök ellopása
- Adatok vagy eszközök elvesztése
- Illetéktelen hozzáférés
- IT szolgáltatások elérhetetlensége
- Kémkedés
- Rongálás
- Social Engineering
- Kiberháború



Oroszország kiberháborút indított Észtország ellen

KITEKINTŐ
2007. május 19., szombat

Címkék: észtország oroszország történelem

Megosztás: Tetszik Tweet 0 +1 0

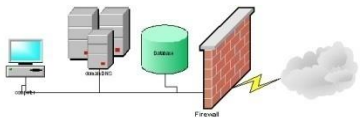
Jaak Aaviksoo, észt védelmi miniszter, azzal vádolja az orosz kormányt, hogy nagyszabású kiberhadjáratot indított országa weblapjai ellen, amely Észtország biztonságát is veszélyeztetheti.

2010.12.15. 15:45

A Stuxnet 2 évvel vetette vissza Irán atomprogramját

Egy vezető német számítástechnikai szakember szerint a vírus olyan hatékony volt, mint egy katonai rajtaütés.

Twitter Facebook Tumblr Startlap -A +A



Adathalászok támadják a CIB Bank ügyfeleit

Index
2010. január 4., hétfő 10:30

Hétfő reggel indult az adathalász akció, amiben a CIB Bank ügyfeleitől próbálnak jelszavakat kicsalni internetes csalók. A hamis levél és weboldal egészen ügyes, de előbbit a magyartalan nyelvezet buktatja le, utóbbit pedig a Firefox máris tiltólistára tette.

Olvasóink, és az érintett bank is jelezte, hogy adathalász inváziót indult hétfő reggel a CIB Bank ügyfelei ellen. Az adathalász levelet nemcsak a bank ügyfelei kapták meg, így azt valószínűleg nem egy belső címlistát megszerezve küldték ki az internetes csalók, hanem egy nagyobb, a feketepiacon beszerezhető címadatbázist használtak, bízva abban, hogy a szórásba olyanok is bekerülnek, akiknek valóban a CIB-nél van számlájuk.

A levél a szokásos adathalász trükköt alkalmazza: a bank nevében arra figyelmezteti a felhasználót, hogy zárolták a számláját, mert valaki többször megpróbált hozzáférni hamis adatokkal, és arra kérik a címzettet, hogy a valódi adatait megadva lépjen be a bank online rendszerébe, hogy feloldja a zárolást. A megadott link azonban nem a bank weboldalára visz, hanem egy arra megszólalásig hasonló oldalra, ami a jerseycitymuseum.org (minden bizonnyal feltört) szerverén helyezkedik el, és az ott megadott adatok és jelszavak egyenesen a csalókhoz kerülnek.

NEWS CHINA

Home | UK | Africa | Asia | Europe | Latin America | Mid-East | US & Canada | Business | Health | Sci/Environ

Asia Business | China | India

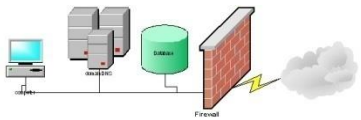
19 February 2013 Last updated at 19:57 GMT

China military unit 'behind prolific hacking'

The BBC's John Sudworth was detained while filming the reported hub of the hacking operation

A secretive branch of China's military is probably one of the world's "most prolific cyber espionage groups", a US cyber security firm has said.

Related Stories



NÉPSZABADSÁG ONLINE

éjszakai min: 0 °C

Belföld | Külföld | Gazdaság | Kultúra | Vélemény | Sport | Tud/Tech | N

Gigantikus adatlopás a Pepsi honlapjáról

Egy hackerportál információi szerint egy török hackercsapat feltörte a Pepsi magyar honlapján lévő promóciós oldalt, ahonnan mintegy ötvenezer felhasználó személyes adatait, jelszavait lopták el és publikálták az interneten – adta hírül az Origo.

NOL | 2012. október 13. | 4 komment

TJX data breach: At 45.6M card numbers, it's the biggest ever

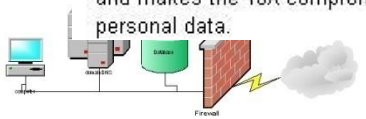
It eclipses the compromise in June 2005 at CardSystems Solutions

By Jaikumar Vijayan
March 29, 2007 12:00 PM ET

Comments (3) Recommended (187) Digg Twitter Share/Email

Computerworld - After more than two months of refusing to reveal the size and scope of its data breach, TJX Companies Inc. is finally offering more details about the extent of the compromise.

In filings with the U.S. Securities and Exchange Commission yesterday, the company said 45.6 million credit and debit card numbers were stolen from one of its systems over a period of more than 18 months by an unknown number of intruders. That number eclipses the 40 million records compromised in the mid-2005 breach at CardSystems Solutions and makes the TJX compromise the worst ever involving the loss of personal data.



Home > News > Clinton White House data on missing National Archives drive

Clinton White House data on missing National Archives drive

Angela Moscaritolo May 20, 2009

PRINT EMAIL REPRINT PERMISSIONS FONT SIZE: A | A | A BOOKMI

Updated Wednesday, May 20, 2009 at 5:37 p.m. EST

The National Archives and Records Administration (NARA) has lost an external hard drive that contained copies of sensitive data belonging to the Clinton administration, the agency confirmed Wednesday.

RELATED ARTICLES

- Octomom's hospital f
- UC Berkeley suffers l
- LexisNexis admits to major data breach
- Data leakage prevent

T-Mobile lost disk containing data on 17 million customers

By Peter Sayer, IDG News Service\Paris Bureau, IDG
Published: October 6, 2008

Deutsche Telekom's German mobile phone subsidiary T-Mobile lost a disk containing personal information about 17 million of its customers in early 2006, the company said Saturday.

SIGN RECO
TWIT
SIGN E-MAI THIS

Forrás: http://datalossdb.org

Az adatvédelmi biztos is vizsgálja a veszprémi adatvesztést

VÁMOSI GERGŐ 2008. 12. 11., 16:15 Utolsó módosítás: 2008. 12. 12., 17:10

Ez a cikk 304 napja frissült utoljára. A benne szereplő információk a megjelenés idején pontosak voltak, de mára elavultak lehetnek.

ESZKÖZÖK:

Már az adatvédelmi biztos is vizsgálatot indított a veszprémi Pannon Egyetemen történt adatvesztés ügyében, amely miatt az év egyik legnagyobb ilyen botránya robbant ki. Az egyetem szerint már nem biztos, hogy rendszerbetörés miatt történt az eset, és a rendszergazda felelősségét is vizsgálják.

NYITÓ | HÍREK | KÖZÖSSÉG | PROGRAMOK | ISTEN HOZTA! | KIKAPCS | SZÉPEK SZÉPE | APRÓ

Szeged | Hódmezővásárhely | Makó | Szentes | Csongrád | Kecskemét | **Belföld** | Külföld | Gazdaság |

Itt vagyok: Nyitólap > Belföld - Magyarország hírei > Már vizsgálódik a rendőrség a veszprémi adatvesztés ügyében

Már vizsgálódik a rendőrség a veszprémi adatvesztés ügyében

FÜGGETLEN HÍRÜGYNÖKSÉG

2008.12.09. 15:57

Hozzászólok!

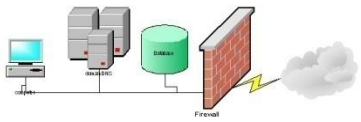
Értékelem a cikket!

A+ A–

Már vizsgálja a rendőrség, hogy történt-e bűncselekmény annak kapcsán, hogy több ezer veszprémi egyetemista személyes adata hónapokon keresztül elérhető volt egy internetes oldalról - mondta el Váradi Piroska, a Veszprém Megyei Rendőr-főkapitányság szóvivője.

Milyen hatása lehet?

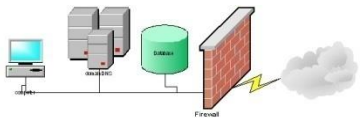
- Az üzleti folyamatok megszakadása
  - Szolgáltatás, gyártás
- Titkos adatokat megszerzi a konkurencia
- Személyes adatokkal visszaélés
- Bankszámlákhoz hozzáférés
- Jogi következmények (szerződések, törvények megsértése)
- Jó hírnév sérülése
- Üzleti előnyök elvesztése
- Közművek elérhetetlensége (SCADA)



Információbiztonság

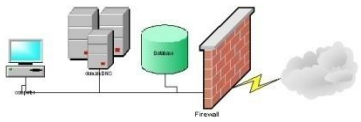
- Az információ értékes
- Az információ sokféle formában jelenhet meg:
  - papíron, **elektronikusan**
  - képekben, hangban, dokumentumban

- Az információvédelem: az információ bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítása



Információbiztonság

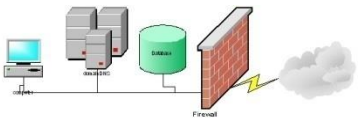
- **Bizalmasság:** annak biztosítása, hogy az információ csak az arra felhatalmazottak számára elérhető.
- **Sértetlenség** (integritás): az információk és a feldolgozási módszerek teljességének és pontosságának megőrzése.
- **Rendelkezésre állás:** annak biztosítása, hogy a felhatalmazott felhasználók hozzáférjenek az információkhoz.



Információbiztonság

- Biztonság =
  - Bizalmasság (Confidentiality) +
  - Sértetlenség (Integrity) +
  - Rendelkezésre állás (Availability)

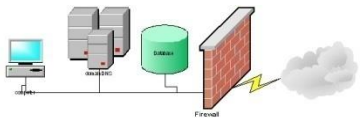
- Az információvédelem nem más, mint az információval kapcsolatos biztonsági kockázatok folyamatos menedzselése



Információbiztonság

- Kockázatok csökkentése intézkedések alkalmazásával

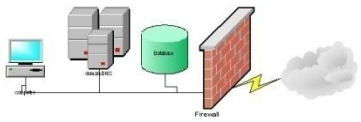
- Intézkedések – kontrollok
  - Adminisztratív
  - Logikai
  - Fizikai
- Ezen belüli kategóriák
  - Megelőző (preventive)
  - Feltáró (detective)



Megfelelés

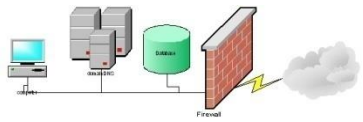
- Törvényi szabályozás, szabványok, legjobb gyakorlatok

- Kötelező érvényűek
  - Pénzügyi iparági törvények
  - PSZÁF ajánlások
  - Adatvédelmi törvény
  - PCI DSS

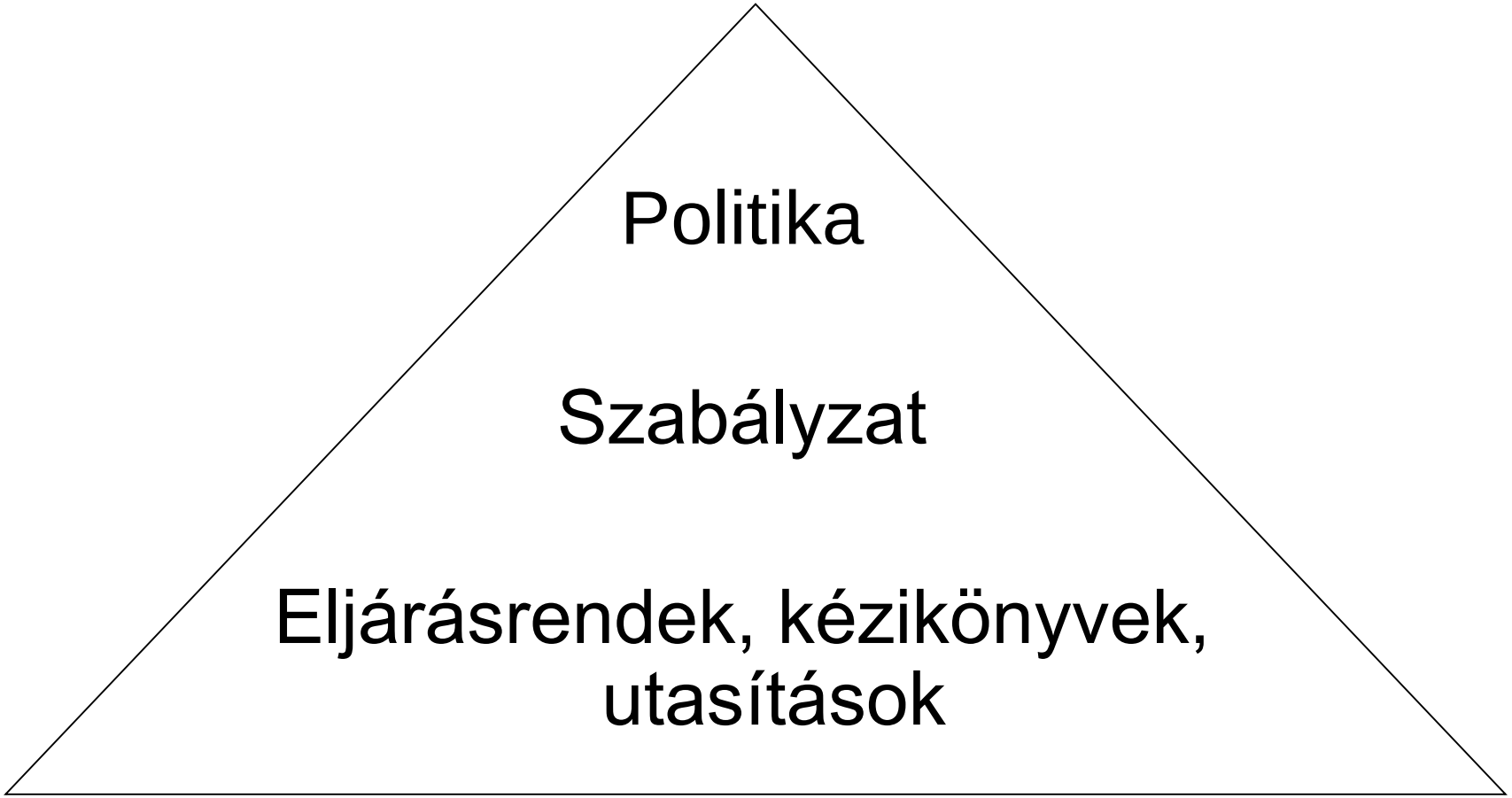


Megfelelés

- Nem kötelező érvényűek
  - ISO17799/ISO27002 – Az információbiztonság irányítási gyakorlatának kézikönyve
  - ISO27001 – Információbiztonság irányítási rendszerei: Követelmények
  - Cobit v4 – Control Objectives for Information and Related Technology



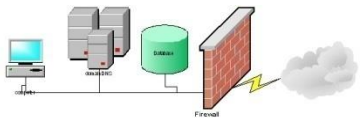
Szabályozás



Szabályozás

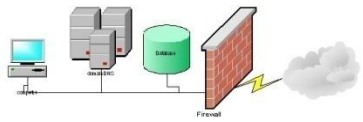
- Információbiztonsági Politika
  - Általános irányelvek, felelősségi körök
  - A legfelső vezetés biztonsági elkötelezettsége
  - Hosszú távra készül
  - Legfelső szintű vezetői jóváhagyást igényel

- Információbiztonsági Szabályzat
  - IBP-nek megfelelő intézkedések
  - Középtávra készül
  - Legfelső szintű vezetői jóváhagyást igényel



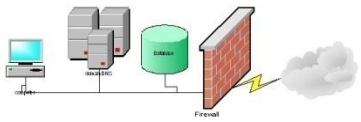
Szabályozás

- Eljárások, utasítások
  - Technikai, technológiai irányultságú intézkedések
  - Folyamatok
  - Rövidtávra készülnek
  - Informatikai vezetői jóváhagyást igényelnek
  - Pl. mentési rend, incidenskezelési folyamat, vírusvédelmi eljárás, stb.

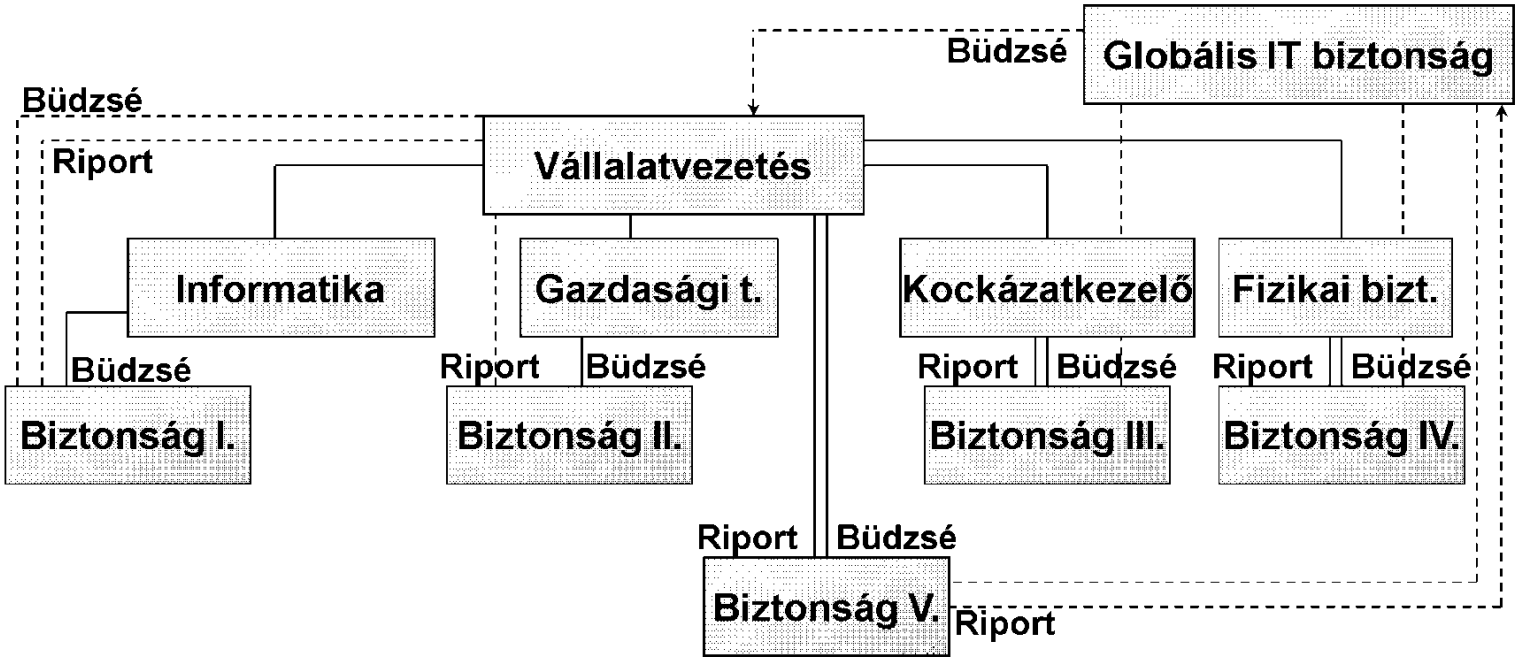


Információbiztonsági szerepek

- Információbiztonsági vezető
  - Információbiztonsági keretrendszer kidolgozása és működtetése
  - Információbiztonsági stratégiai tervezés
  - Információbiztonsági operatív feladatok felügyelete
  - Törvényeknek, szabványoknak való megfelelés biztosítása

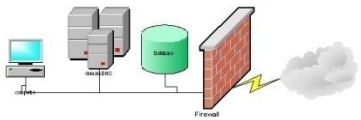


Biztonsági szervezet szerepe, mérete és helye a **mai** magyar vállalatoknál



Információbiztonsági szerepek

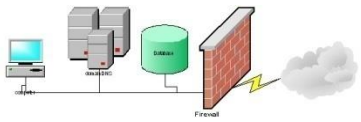
- Információgazda, -kezelő, -használó
  - Egy adott információ, információs rendszer vonatkozásában értendő
- Információ gazda
  - Adat-, rendszer-, alkalmazás- és hálózatgazda
  - Általában üzletági vezetők
  - Teljes felelőséggel tartoznak a hozzájuk rendelt információ és információs rendszerek biztonságáért



Információbiztonsági szerepek

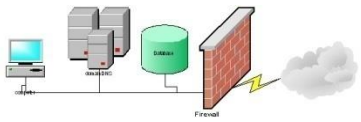
- Információkezelő
  - Az információgazdák a napi feladatokat az információkezelőknek delegálják
  - Rendszer-, hálózatadminisztrátorok, ügyfélszolgálat (help desk)

- Információ-felhasználó
  - Bárki aki az információt napi munkája során használja
  - Belső munkatársak és külső felek



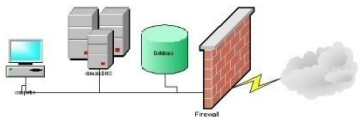
Információbiztonsági szerepek

- Belső ellenőrzés
  - Az információbiztonság független „minőségbiztosítója”



Üzemeltetés biztonsága

- Tipikus üzemeltetési biztonsági feladatok
  - Védelem rosszindulatú kódok ellen
  - Adatmentés és -megőrzés
  - Naplózás
  - Biztonsági frissítések
  - Adathordozók kezelése
  - Logikai hozzáférések kezelése
  - Kriptológiai megoldások



Védelem rosszindulatú kódok ellen

- Virus, féreg, kémprogram, rootkit, bot, mobil kódok, stb.
  - Ezek kombinációja
- Botnetek
  - Bredolab 30M (3,6 milliárd spam /nap)
  - Mariposa 12M

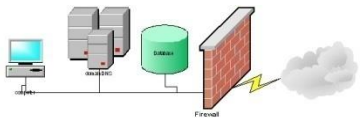
Lekapcsolták a világ egyik legnagyobb zombihálózatát

Index
2010. március 3., szerda 15:31 | Frissítve: 2010. március 3.

A spanyol rendőrség nemzetközi szakértők segítségével elkapta a világ egyik legnagyobb zombihálózatának, a 12,7 millió vírusfertőzött számítógépet tartalmazó Mariposa botnetnek az üzemeltetőit.

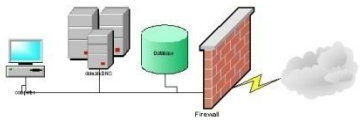
A fertőzött gépek a világ 190 országában voltak szétszórva, a Fortune magazin top1000-es listájából (a világ legnagyobb forgalmú cégeit összegző éves összeállítás) több mint 500-nál volt fertőzött gép, és a világ legnagyobb bankjai közül is több mint 40-nél találtak olyan gépet, ami a használója tudta nélkül a zombihálózatnak dolgozott.

A Mariposa botnet 2008 decemberében tűnt fel a neten, és 2009 tavaszán kezdtek el nyomozni utána a biztonságtechnikai szakértők. A zombigépeket megfertőző vírust borzasztó egyszerű módszerrel, MSN-en és más üzenetküldő programokon át terjesztették, a fertőzött gépek tulajdonosai nevében linkeket küldözgetve azok ismerőseinek. A linkre kattintva a beígért izgalmas képek és hírek helyett a vírust töltötte le az áldozat a gépére, majd zombiként maga is nekiállt tovább terjeszteni azt. A hálózat szakértők szerint technikailag jóval kifinomultabb, és nagyobb volt, mint a kínaiak Google-támadásához használt botnet, vagy a tavaly világméretű pánikot keltett Conficker zombihálózat.



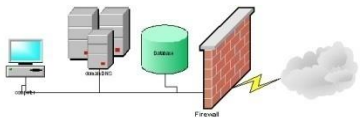
Védelem rosszindulatú kódok ellen

- Virusvédelmi szoftver
  - Központilag menedzselt
  - Rendszeresen frissített virusminta-adatbázis és viruskereső motor (lehetőleg automatikusan)
  - Felhasználók ne tudják hatástalanítani
  - Email gateway



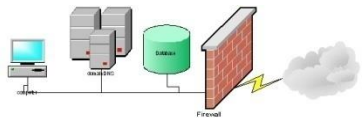
Védelem rosszindulatú kódok ellen

- Virusvédelmi folyamatok
  - Vírusmegelőzés
    - Rendszeres szkennelés
    - Könyvtár megosztások tiltása
    - Cserélhető adathordozók kezelése
    - Mobil kódok korlátozása
    - Oktatás
  - Vírusmentesítés
    - Dokumentált folyamat szerint
    - Izolálás, helyreállítás, tesztelés



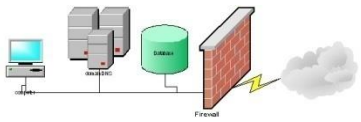
Adatmentés és adatmegőrzés

- Az adatokat kritikussági szintjüknek megfelelően rendszeresen menteni kell
  - Elfogadható adatvesztési ablak definiálása
  - Alkalmazott mentési technika kiválasztása ennek megfelelően
- Adatgazdák felelőssége
- Rendszeres tesztelés
- Telephelyen kívüli tárolás



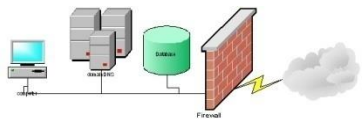
Adatmentés és adatmegőrzés

- Mentés fajtái
  - Teljes mentés
    - Minden adat
  - Differenciális mentés
    - A teljes mentés óta változott adatok
  - Inkrementális mentés
    - Az utolsó teljes, differenciális vagy inkrementális mentés óta megváltozott adatok
- Időszak
  - Napi, heti, havi, stb.



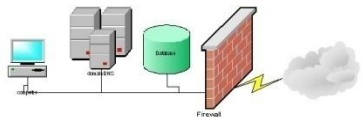
Adatmentés és adatmegőrzés

- Törvényi előírások és üzleti érdekek szerint
  - Pl. naplóállomány, változáskezelési jegyzőkönyvek, emailek, könyvelési adatok
- Adatgazdák felelősége
- Technológiai háttér figyelembevétele
- Titkosítási kulcsok megőrzése
- Megőrzési idő után az adatok szakszerű megsemmisítése



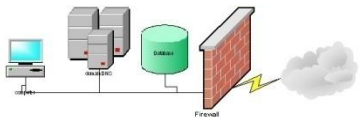
Naplózás

- Mit gyűjtsünk?
  - Minden olyan adatot, amely biztonsági események észleléséénél, kiderítésénél fontos lehet
  - Bizalmas adatok (pl. jelszó) nem tárolhatóak a naplóállományokban
  - Rendszerek kritikussági szintjének figyelembe vétele
  - Naplóállományok mérete



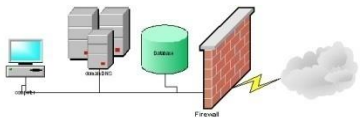
Naplózás

- Milyen attribútumokat naplózunk?
  - Esemény típusa
  - Dátum
  - Felhasználó azonosító
  - IP cím
  - Sikerült vagy sem
- Korreláció
  - Komplex támadások azonosítása
  - Költséges célszoftverek



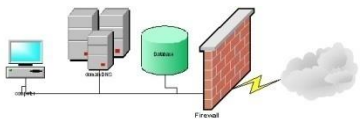
Naplózás

- Monitorozás, riasztás
  - Rendszeres monitorozás
  - Automatizált <> Kézi
  - Valós idejű riasztás
- Integritás védelem
  - Ne helyben tároljuk
  - CD/DVD, csak olvasható állományok
  - Hozzáférés védelem
  - Munkakörök elválasztása
- Megőrzés
  - On-line, off-line



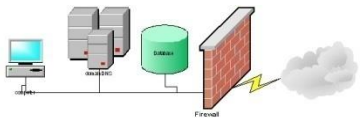
Biztonsági frissítések

- Frissítés
  - Funkcionális vagy biztonsági
- A szoftverek biztonsági réseket tartalmaznak
- Megoldás: rendszeres biztonsági frissítés
- Kritikus a frissítés gyorsasága
  - a sebezhetőség felfedezése és az exploit megjelenése közötti idő drasztikusan lecsökkent
  - Zero-day attack
- Kritikus, nem kritikus patch
- Változáskezelési folyamattal összhangban



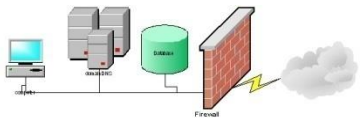
Biztonsági frissítések

- Manuális vagy automatizált
- Patch menedzsment folyamat
  - Új patchek monitorozása
    - Hiteles forrásból
  - Kritikussági szint alapján kockázatelemzés
  - Kockázatcsökkentés
    - Patch alkalmazása
    - Kompenzáló intézkedés



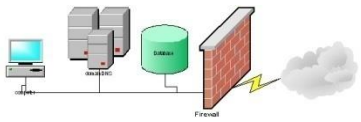
Biztonsági frissítések

- Patch menedzsment folyamat (folyt)
  - Tesztelés
    - Funkcionalitás
    - Biztonság
    - Visszaalakítási terv
  - Éles rendszeren alkalmazás
  - Ellenőrzés (verifikáció)



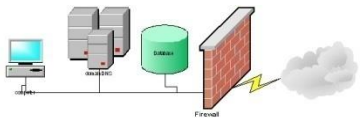
Adathordozók kezelése

- Probléma
  - adatszivárgás
- Cserélhető/hordozható adathordozók kezelése
  - USB eszközök
  - CD/DVD
- Titkosítás
  - Bizalmas adatok tárolása



Adathordozók kezelése

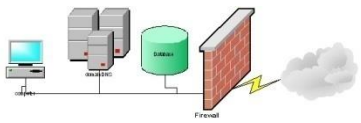
- Biztonságos megsemmisítés
  - DVD/CD
  - Háttértároló
- Adathordozók biztonságos elhelyezése, kezelése
- Adathordozók biztonságos szállítása



Logikai hozzáférés kezelés

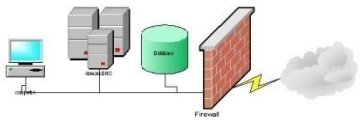
- Azonosítás, hitelesítés authorizáció

- Azonosítás
  - Ki?
  - pl. felhasználói név, telefon szám, név
  - Egyedi azonosítók
    - Számonkérhetőség
  - Nem változik egy felhasználó esetén
  - Elnevezési konvenciók



Logikai hozzáférés kezelés

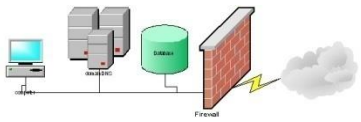
- Hitelesítés (authentikáció)
  - Tényleg ő?
  - Azonosítás az alábbi faktorok alapján
    - Amit a felhasználó tud
    - Amivel a felhasználó rendelkezik
    - A felhasználó fizikai tulajdonsága
  - Alap authentikáció <-> Erős authentikáció
  - A védendő információval és a kockázattal arányos módszer alkalmazása



Logikai hozzáférés kezelés

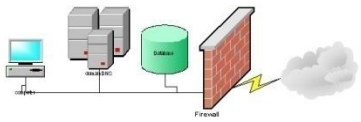
- Authorizáció
  - Mit csinálhat?
  - Hozzáférési jogosultságok
  - Normál <-> privilegizált
  - Speciális segédprogamok használata

- Központi authentikációs és authorizációs technológiák
  - RADIUS
  - TACACS



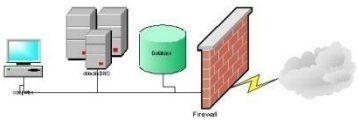
Logikai hozzáférés kezelés

- Alapelvek
  - Need-to-know
    - A felhasználó csak annyi információt tudhat, ami feltétlenül szükséges a munkája ellátásához.
  - Minimális jogosultság (least privilege)
    - A felhasználó a legszűkebb körű jogosultsággal rendelkezhet, amely elegendő a munkavégzéséhez
  - Feladatok elhatárolása (separation of duties)
    - Egy személy nem lehet felelős egy tranzakciólánc több lépéséért (pl. végrehajtás és ellenőrzés)



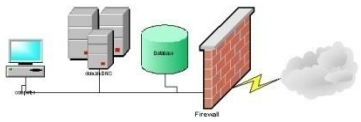
Logikai hozzáférés kezelés - Jelszókezelés

- Alapértelmezett jelszó
- Ideiglenes jelszó
- Egyszer használatos jelszó
- Jelszó öregedés
- Nem tárolható, továbbítható titkosítatlanul
- Erős jelszavak használata
- Probléma, ha
  - túl komplex a jelszó
  - túl gyakran kell változtatni
- 3 próbálkozás után felhasználó kizárása



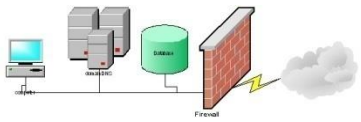
Logikai hozzáférés kezelés - Jogosultság menedzsment

- Egyedi felhasználói azonosítók
- Információgazda rendel jogosultságokat
- HR osztállyal együttműködve
- Felhasználói azonosítók rendszeres felülvizsgálata
  - Redundáns és inaktív azonosítók letiltása
- Kilépéskor azonnali tiltás, jogosultságok felfüggesztése



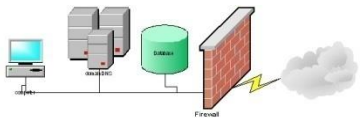
Logikai hozzáférés kezelés – Távoli elérés

- A telephelyen kívülről vállalati erőforrások elérése
  - Megemelt kockázat
  - Felhasználói munkavégzés, távadminisztráció
  - Közvetlen vagy közvetett elérés
  - VPN (IPSec, SSL)



Kriptológiai megoldások

- Bizalmasság biztosítása
  - Titkosítás
  - Tárolás, továbbítás
  - L3 (IPSec), L4 (SSL), L7 (SSH, SFTP)
- Integritás biztosítása
  - Hash függvények (md5, SHA-1, SHA-2)
  - Ellenőrző összegek (CRC)
- Feladó azonosítása, letagadhatatlanság
  - Digitális aláírás

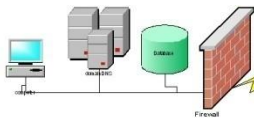


Kriptológiai megoldások

- Erős algoritmusok és kulcsok alkalmazása

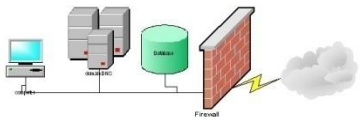
Year	Symmetric Key Size in Bits				
	Hacker	Small Org.	Medium Org.	Large Org.	Intelligence
1996	50	55	60	70	75
2005	56	61	66	76	81
2015	63	68	73	83	88
2020	66	71	76	86	91
2030	73	78	83	93	98

RSA/DLOG Key	Equivalent Symmetric Key Size
512	50
768	62
1024	73
1536	89
2048	103



Fizikai biztonság

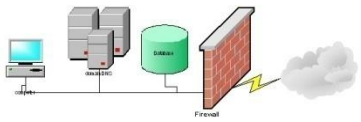
- Fizikai biztonsági zónák, beléptetés
  - Beléptető rendszer, őr, lakat, korlátok, zárható szekrények, kamera, riasztó, stb.
  - Látogatókontrol
- Környezeti hatások elleni védelem
  - Tűz, víz, földrengés
- Áram, légkondicionálás
  - UPS, generátorok, redundáns tápellátás



Fizikai biztonság

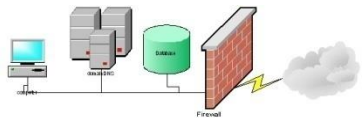
- Sugárzás elleni védelem
  - Titokszobák, NATO helyiségek, stb.
  - Tempest

- Berendezések védelme, karbantartás
- Eszközök telephelyről/re történő kivitele/bevitele



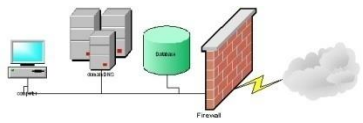
Internet biztonság

- Internet, Intranet, Extranet
- Belső IT infrastruktúrát meg kell védeni a nyilvános hálózati szegmenstől
- Határvédelem
  - Tűzfalak, IDS/IPS
- Külső kapcsolatok elérése csak engedélyezett kapcsolatokon keresztül
  - Modemek (3G is) és WIFI eszközök használata



Internet biztonság

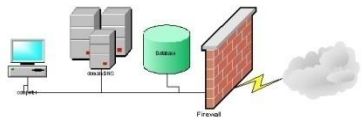
- Kommunikáció
  - Protokollok
    - HTTPS, SSL, SSH, SFTP,SNMPv3
    - FTP, Telnet, SNMPv1, NFS
  - VPN
- Architektúra
  - Dedikált server a DMZ-ben
  - Funkciók szétválasztása -> 2 vagy 3 szintű architektúra
- Szolgáltatások biztonsága



Cloud biztonság

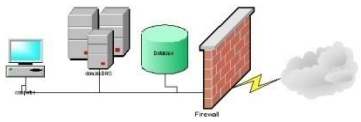
- A Cloud Computing (CC) számos üzleti előnnyel jár
  - Opex vs Capex, fizetés igény szerint, agilitás, gyors bevezethetőség, új üzleti lehetőség, stb.
- DE adatok kikerülnek a szervezet ellenőrzése alól.

- Hagyományos és új kockázatok



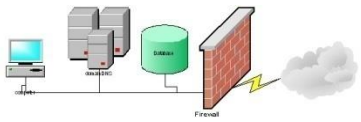
Cloud biztonság

- Cloud specifikus kockázatok (pl.)
  - Adatok fizikai helye
  - Megfelelőségi kényszer
  - Közös bérlők (osztott infrastruktúra)
  - Korlátozott monitoring
  - Korlátozott auditálási lehetőség
  - Szolgáltató váltás nehézsége
  - Támadások vonzó célpontja az aggregáció miatt



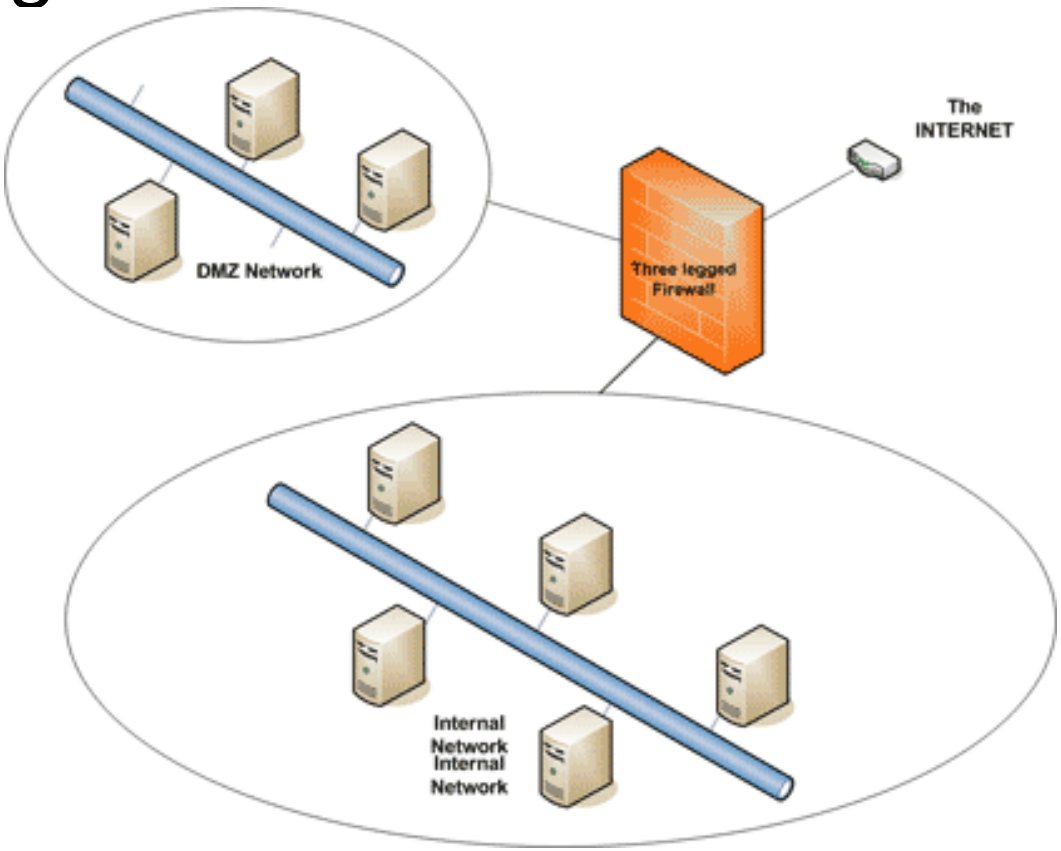
Email biztonság

- Biztonság nem volt szempont az email kidolgozásánál
- Egyike a legrégebben használt internetes protokolloknak: smtp, pop
- Sebezhető levelező rendszerek (MTA)
  - sendmail, qmail
- Hasonló gondok IM esetén is
- További gondok
  - Spam, hitelesség, bizalmasság, sértetlenség biztosítása (phishing, whaling), adatszivárgás, rosszindulatú programok



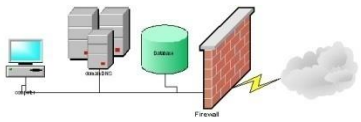
Infrastruktúra biztonság - Hálózatbiztonság

- Biztonsági zónák kialakítása



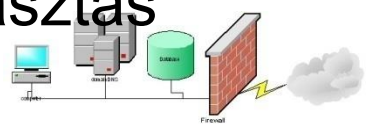
Infrastruktúra biztonság – Hálózatbiztonság

- Tűzfalak
  - Biztonsági zónák közötti forgalom ellenőrzése
    - Internet, DMZ, belső hálózat
  - Layer 3 – Layer 7
  - Típusai
    - Csomagszűrő
    - Stateful inspection
    - Proxy
      - alkalmazás-szintű, összeköttetés-szintű
  - Default policy



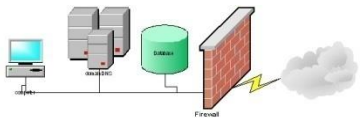
Infrastruktúra biztonság – Hálózatbiztonság

- IDS/IPS - Behatolás-észlelő és megakadályozó rendszerek
  - Internet kilépési pontoknál
  - Működés szerint
    - Minta-alapú (signature-based)
    - Anomáliadetektorok
    - Honeypot
  - Leglényegesebb funkciók
    - Aggregálás
    - Korrelálás
    - Riasztás



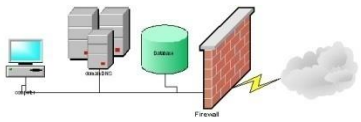
Infrastruktúra biztonság

- Egyéb infrastruktúra biztonsági eszközök
  - NAC (Network Access Control)
  - Webtartalomszűrő
  - Email tartalomszűrő
  - Spam szűrő
  - VPN gateway
  - DLP (Data Loss Prevention) eszköz



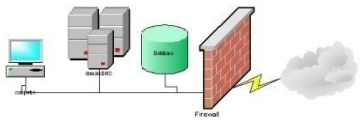
Infrastr. biztonság – Szerverek és munkaállomások biztonsága

- Dedikált szerverek
- Távoli adminisztráció csak titkosított kapcsolatokon keresztül
- Titkosítatlan protokollok letiltása (pl. FTP, SNMPv1)
- Gyártó alapbeállításainak megváltoztatása
- USB portok kontrolálása
- Naplógyűjtés, monitorozás, riasztás
- Szoftver telepítési szabályok



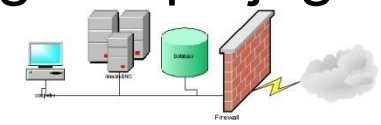
Infrastr. biztonság – Szerverek és munkaállomások biztonsága

- Fizikai elhelyezkedés
- Patch menedzsment
- Mentés
- Antivírus program alkalmazása
- Személyes tűzfalak alkalmazása
- Eszközök biztonságos megsemmisítése
- Incidenskezelés és katasztrófa-elhárítás
- Rendszeres audit



Incidenskezelés

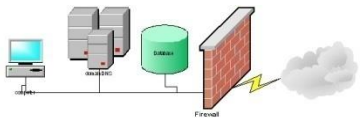
- Incidens
  - Minden olyan esemény, amely negatívan befolyásolja az információ és információs rendszerek biztonságát
  - Pl. DoS, vírusfertőzés, jogosulatlan hozzáférés, stb.
  - Hatókör
    - Csak informatikai incidensek (természeti katasztrófa nem)
    - Fizikai: pl. lopás
    - Logikai: pl. jogosulatlan hozzáférés



Incidenskezelés

- Az incidensek bekövetkezése még a legjobb intézkedések (kontrollok) alkalmazása esetén sem küszöbölhető ki

- Incidenskezelés
  - Incidensek észlelésének, analizálásának, helyreállításának a szervezett folyamata
  - Károk minimalizálása és további károk elkerülése a cél

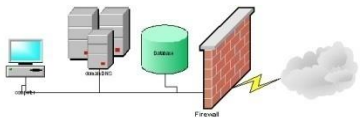


Incidenskezelés

- Az Incidenskezelés legfontosabb előnyei
  - Strukturált megközelítés
  - Gyors és hatékony helyreállítás
  - Korábbi incidenseknél nyert tapasztalatok felhasználása
- Folyamat

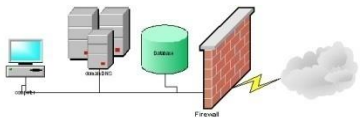
Információbiztonsági Incidens Elhárító Csapat (CSIRT)

- Feladata
  - Kivizsgálni hogyan történt az incidens, milyen kárt okozott
  - A kiváltó okok kiderítése
  - Sérült rendszerek/szolgáltatások visszaállítása
  - A nem sérült kritikus rendszerek működőképességének megóvása
  - Adatok gyors visszatöltése
  - Hasonló incidens újbóli bekövetkezésének megakadályozása



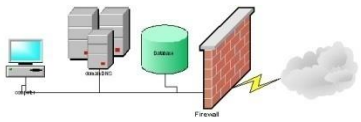
Információbiztonsági Incidens Elhárító Csapat (CSIRT)

- Feladata (folyt.)
  - Negatív visszhang elkerülése (megfelelő kommunikáció alkalmazása
- Felépítése
  - Centralizált ⇔ Elosztott
  - Állandó ⇔ Ad Hoc



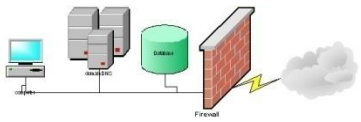
Információbiztonsági Incidens Elhárító Csapat (CSIRT)

- Összetétel (belső és külső munkatársak)
  - Információbiztonsági Incidens Elhárító Csapat vezető
  - Ügyfélszolgálati (service desk) munkatárs
  - Jogi osztály munkatársa
  - Felső vezető
  - Rendszer és hálózati adminisztrátor
  - Vállalati kommunikáció (PR) munkatársa
  - HR munkatárs
  - Épületbiztonsági munkatárs



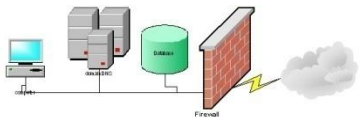
Eszkaláció

- Definició
  - Ha az incidens nem oldható meg egy előre rögzített időn belül, akkor több szakértelem vagy hatáskör bevonása szükséges



Eszkaláció

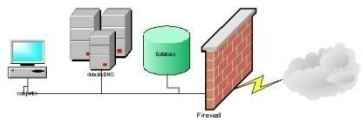
- Eszkaláció fajtái
  - Funkcionális eszkaláció
    - Nagyobb gyakorlattal rendelkező, képzettebb egyén bevonása
    - Pl. Ügyfélszolgálat -> IT szakember -> Szoftver vagy hardver szállító/gyártó
  - Hierarchikus eszkaláció
    - A vállalati szervezetben egy magasabb szintű pozíció bevonása
    - Pl. Ügyfélszolgálat -> CSIRT Vezető -> Informatikai vezető



Kommunikációs szabályok

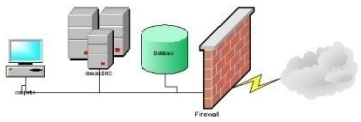
- Az incidenssel kapcsolatban külső és belső felek tájékoztatása. pl. media, rendőrség, ügyfelek, beszállítók, stb.
- Nem megfelelő információ kommunikálása nagyobb kárt okozhat, mint az incidens maga

- Ellenőrzött kommunikáció szükséges (ki, mit, mikor, hogyan)
- Személyes adatok
- „Whistler blower”



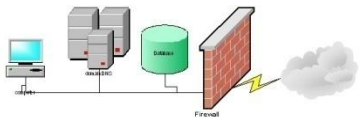
Bizonyítékgyűjtés és -kezelés

- Cél
  - Megoldani az incidenst
  - Bíróság által elfogadható bizonyíték létrehozása
- Chain of custody
  - A bizonyíték gyűjtésének, elemzésének, szállításának, megóvásának a története
  - Biztosítja a bizonyíték integritását



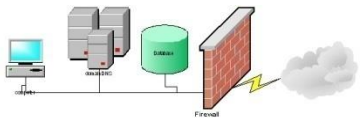
Bizonyítékgyűjtés és -kezelés

- Részletes napló vezetése
  - Időbélyeg
  - A bizonyíték azonosítása (sorszám, IP vagy MAC cím, stb.)
  - Hogyan történt a bizonyíték gyűjtése
  - A személyek nevei, akik gyűjtötték és kezelték a bizonyítékot
  - A helyszín, ahol a bizonyítékot tárolták



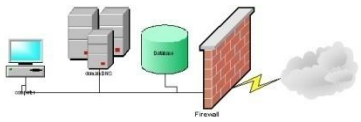
Bizonyítékgyűjtés és -kezelés

- Bizonyítékgyűjtés
  - A nem permanens adatok megőrzése (pl. RAM memória tartalma)
  - Teljes disk image készítése
  - Minden bizonyítékot aláírni és dátummal ellátni
  - Kettesével dolgozni (tanú, tévedés mérséklése)
  - Forensics eszközök használata
  - A bizonyíték felelősének megnevezése



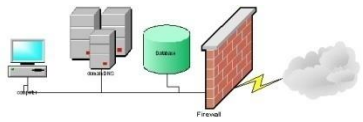
Bizonyítékgyűjtés és -kezelés

- Bizonyítékkezelés
  - Forensics eszközök használata a bizonyíték elemzése során
  - A bizonyíték bizalmasságának és sértetlenségének biztosítása
  - A bizonyíték megőrzése a tárgyalás lezárásáig
  - A hozzáférés szigorú kontrolálása



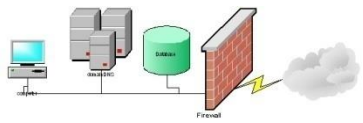
Példa – Rosszindulatú kódok

- Előkészület
  - A rosszindulatú kódokkal kapcsolatos felhasználó ismeretek bővítése
  - Host-based IDS
  - Antivirus, antispyware programok telepítése



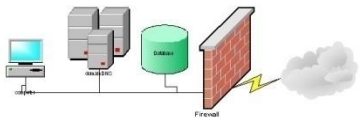
Példa – Rosszindulatú kódok

- Detektálás és analízis
  - Antivírus program riasztása
  - A küldött vagy fogadott emailek számának szembetűnő megváltozása
  - Szokatlan objektumok a képernyőn
  - Programok futása lelassul
  - Rendszer leállás, elszállás
  - Hálózati forgalom jelentős növekedése
  - Ismeretlen folyamatok futása, stb.



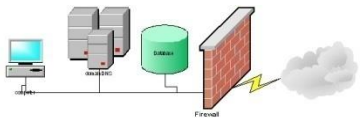
Példa – Rosszindulatú kódok

- Behatárolás
  - A vírusfertőzés másik rendszerre történő átterjedésének megakadályozása
    - A fertőzött rendszer elkülönítése
    - Az emailek blokkolása
    - Szerverek leállítása
    - A belső hálózat leválasztása az Internetről
  - Bizonyítékok gyűjtése, megőrzése, biztonságos tárolása és dokumentálása



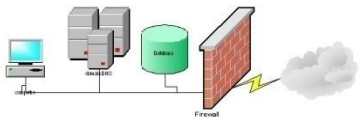
Példa – Rosszindulatú kódok

- Kiirtás
  - Fertőzött állományok megtisztítása, karanténba zárása, törlése, vagy tiszta forrásból pótlása
    - Az antivirus program végzi
    - Adminisztrátor korábbi mentésből állítja helyre
    - A rendszer teljes újratelepítése
  - Más rendszerek hasonló sebezhetőségének megszüntetése



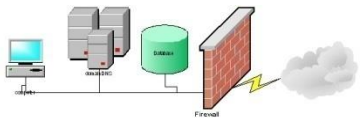
Példa – Rosszindulatú kódok

- Helyreállítás
  - A normál működés helyreállítása
  - A rendszer működésének és a hálózatnak további monitorozása



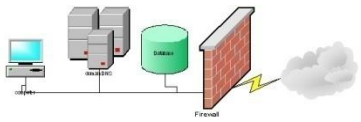
További tipikus problémák

- Vezetői támogatás hiánya
  - Forráshiány
  - Biztonság <-> Használhatóság
  - Hamis illúzió
- Nem kockázatarányos megközelítés
- Belső szabályozás hiánya
  - Szankcionálás hiánya
  - Nem determinisztikus működés
  - Nem léteznek folyamatok



További tipikus problémák

- Felhasználók biztonságtudatossága alacsony
- Szervezetek éretlenek
  - Törvényi kikényszerítés
- Új típusú fenyegetések megjelenése
  - Mobil eszközök, cloud computing, web2
- Elhanyagolt területek
  - Ipari rendszerek, közművek



Köszönöm a figyelmet

Janko.Arpad@pp.t-systems.hu