

Információs rendszerek üzemeltetése

Adamis Gusztáv – TMIT

IE 345

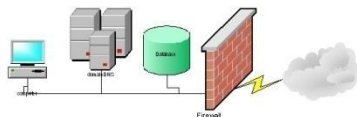
adamis@tmit.bme.hu

I. rész

Korábban tanultak áttekintése

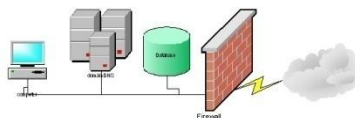


BME VIK TMIT



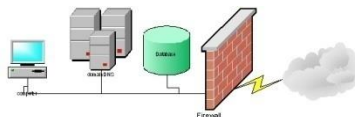
Korábban tanultak áttekintése

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



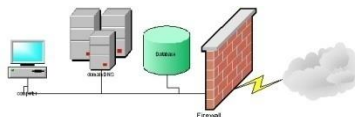
Ismétlés

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



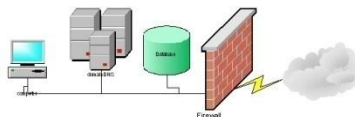
Ismétlés

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



OSI referencia modell

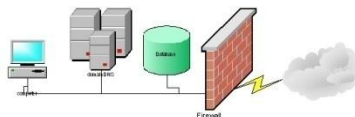
- Hét réteg
 - számítógépek kommunikációjához szükséges hálózati protokollok feladatait határozza meg
 - fő cél: együttműködés különböző gyártók termékei között
- Minden réteg CSAK az alatta levő réteg szolgáltatásaira támaszkodik és a felette levő réteg számára nyújt szolgáltatást
 - protokoll verem (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	CSOMAGOK	Logikai címezés (pl. IP címek) és azon alapuló irányítás, útvonalválasztás (routerek)
2	Adat-kapcsolati Data Link	KERETEK	Interfész (MAC) szintű címezés, 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

ISO/OSI

Alkalmazás
Megjelenítési
Viszony
Szállítási
Hálózati
Adatkapcsolati
Fizikai

TCP/IP

Alkalmazás
Szállítási / Host-to-host (TCP/UDP/...)
Internet (IP)
Hálózati interface/ Hálózati hozzáférési

Gyakorlatias

Alkalmazás
TCP/UDP/...
IP
LLC
MAC
PCS & PMA
PMD

IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

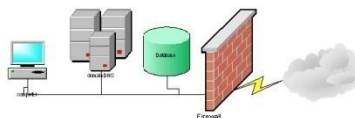
LLC: Logical Link Control

MAC: Medium Access Control

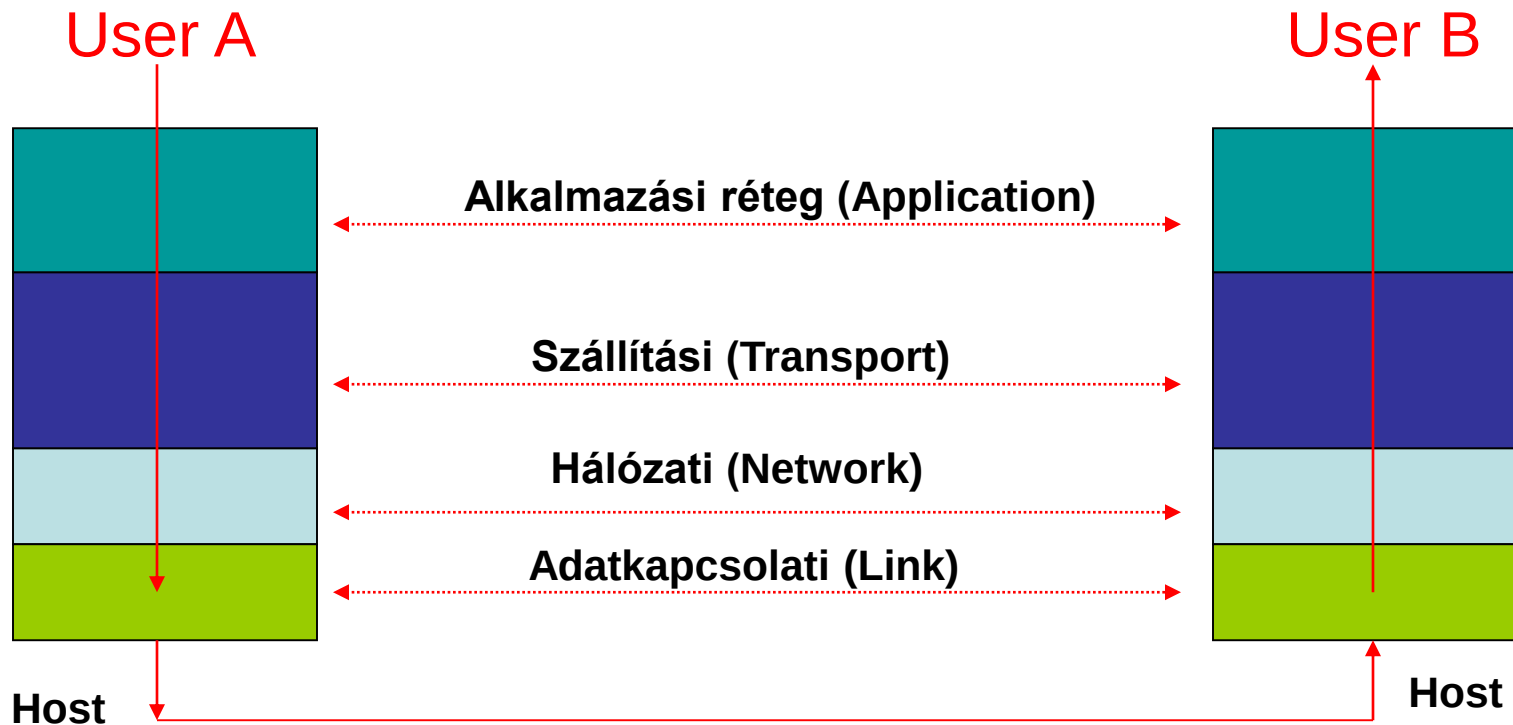
PCS: Physical Coding Sublayer

PMA: Physical Medium Attachment

PMD: Physical Medium Dependent

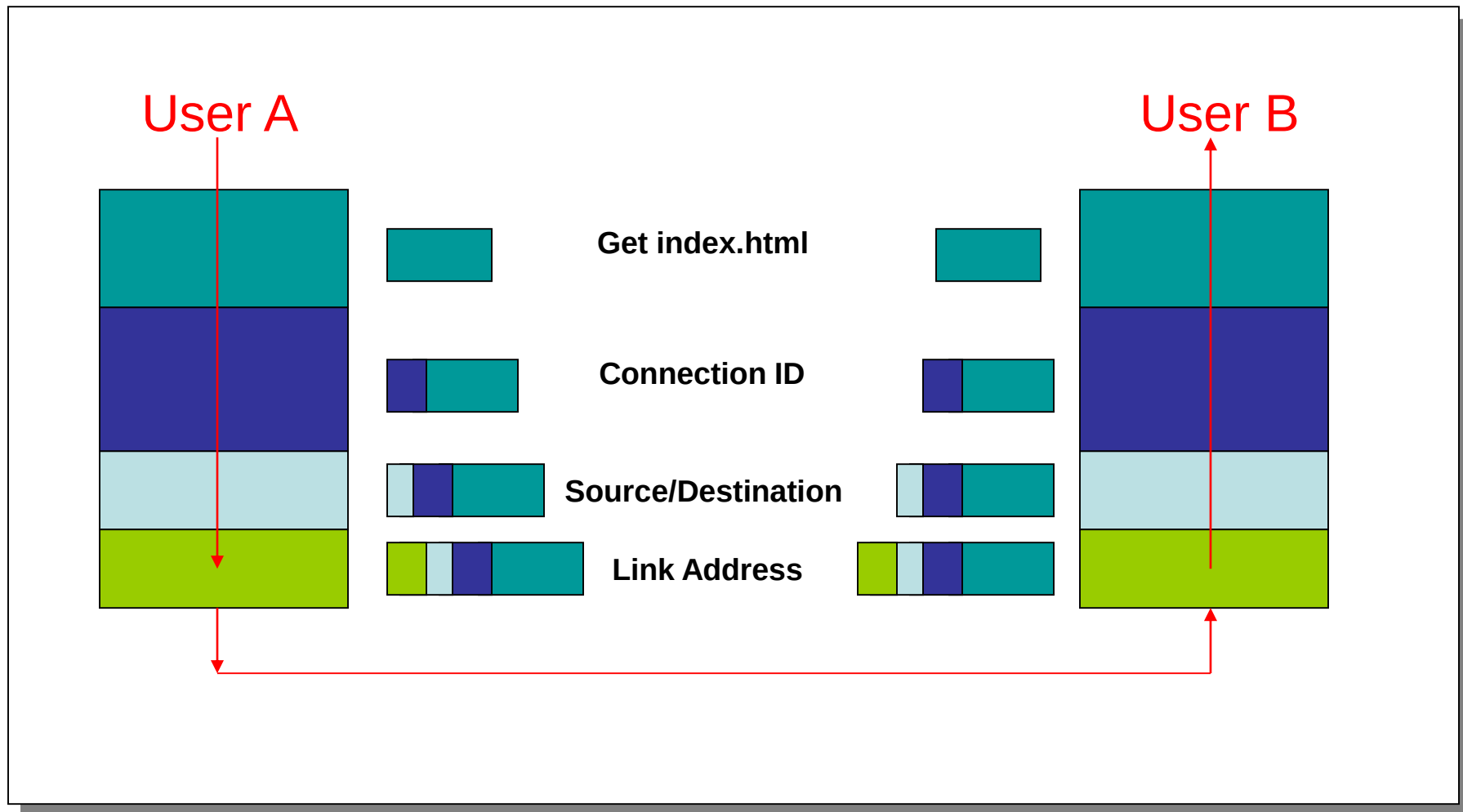


Rétegezés



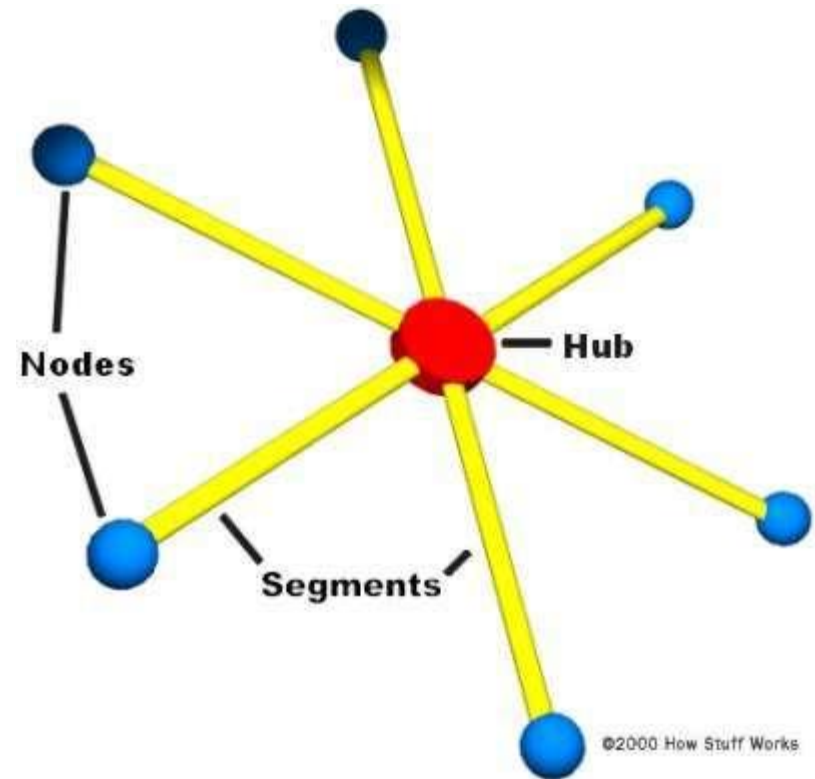
Rétegezés: bonyolult rendszerek egyszerűsítése céljából

Rétegek: egymásba ágyazás



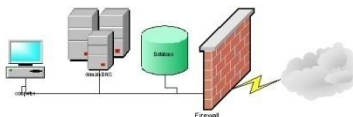
Hub, bridge, router, switch

- Hub
 - 1. (fizikai) réteg
 - Broadcast eszköz
 - bejövő jel az összes többi portra, nincs jelfeldolgozás (gyors)
 - Hubbal rendelkező Ethernet hálózat
 - Megosztott medium
 - > ütközés detektálás
 - > ütközés feloldás (idő!)
 - > osztott sávszélesség
 - > half duplex



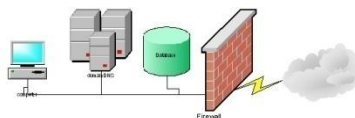
Hub, bridge, router, switch

- Bridge (híd)
 - 2. (adatkapcsolati) réteg
 - Keretanalízis, MAC (fizikai) cím alapú irányítás
 - Nincs ütközés, de lassabb a feldolgozás
 - Dedikált belső összeköttetések
 - Mivel nincs üzenetszórás, több kapcsolat lehet egyszerre
 - > Dedikált (teljes) sávszélesség
 - Transzparens (adaptív hidak)
 - Forrás által irányított- De mikor jobb a hub???



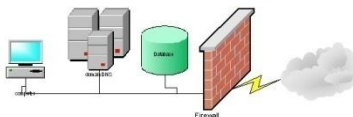
Hub, bridge, router, switch

- Router (útválasztó)
 - 3. (hálózati) réteg
 - IP (!!) cím alapú irányítás
 - Két vagy több IP alhálózatot köt össze
 - Tkp. speciális célú nagyszámítógép

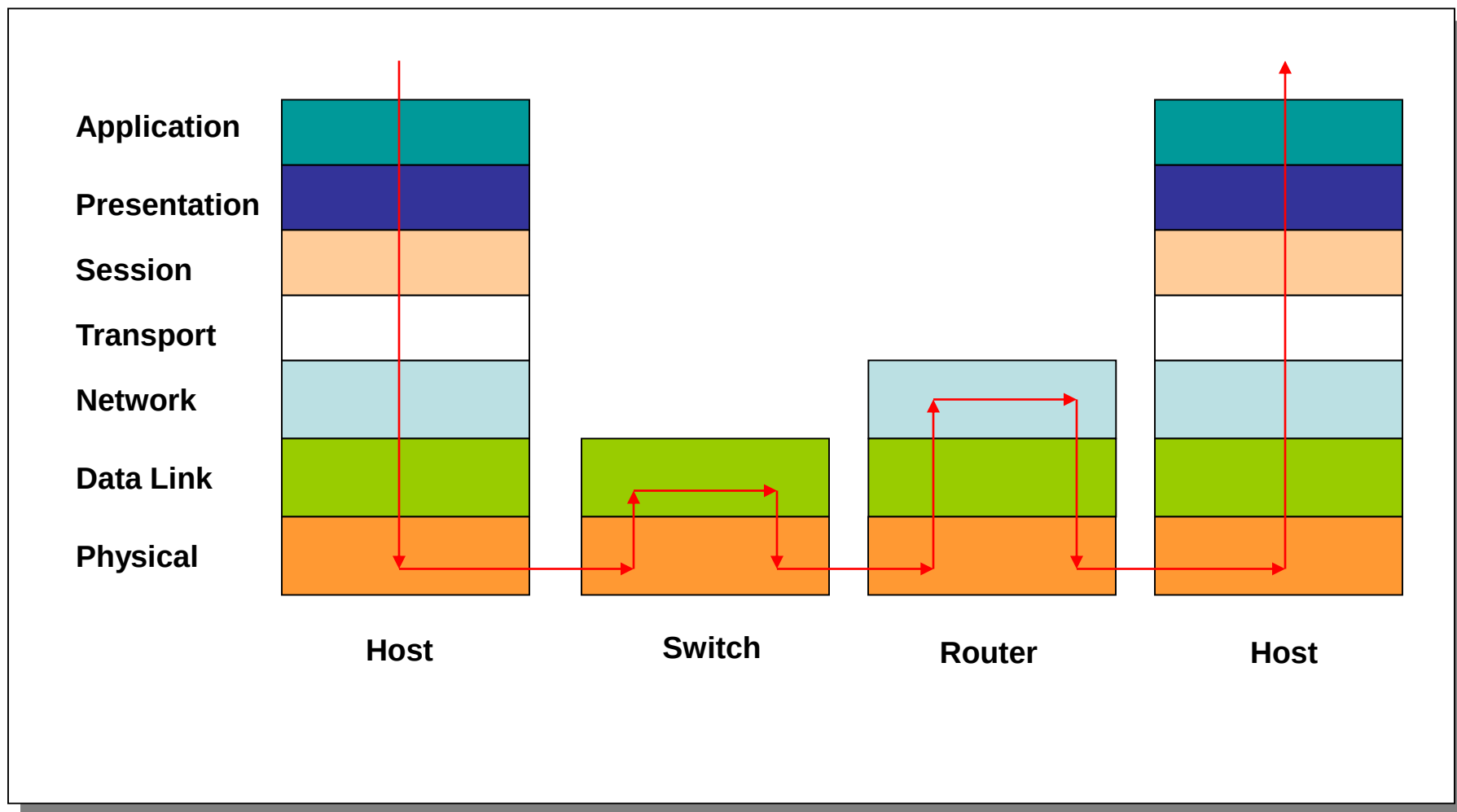


Hub, bridge, router, switch

- 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

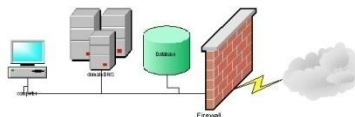


Hálózati eszközök helye a rétegekben



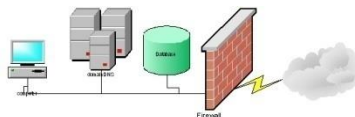
Rétegezés

- 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 rovasára mehet

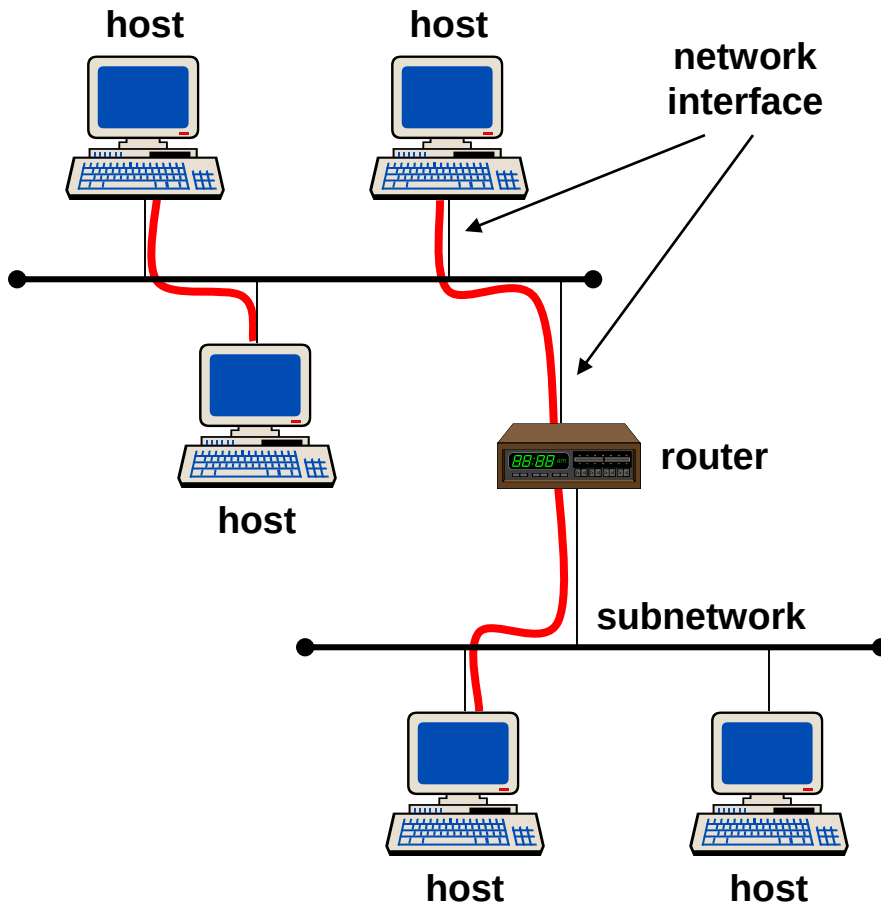


Ismétlés

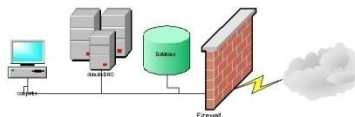
- Referencia modell, protokollok
- **IP alapok**
 - Címek, címosztályok
 - DHCP
 - ARP/RARP
 - NA(P)T
 - DNS
 - ICMP



IP hálózati elemek

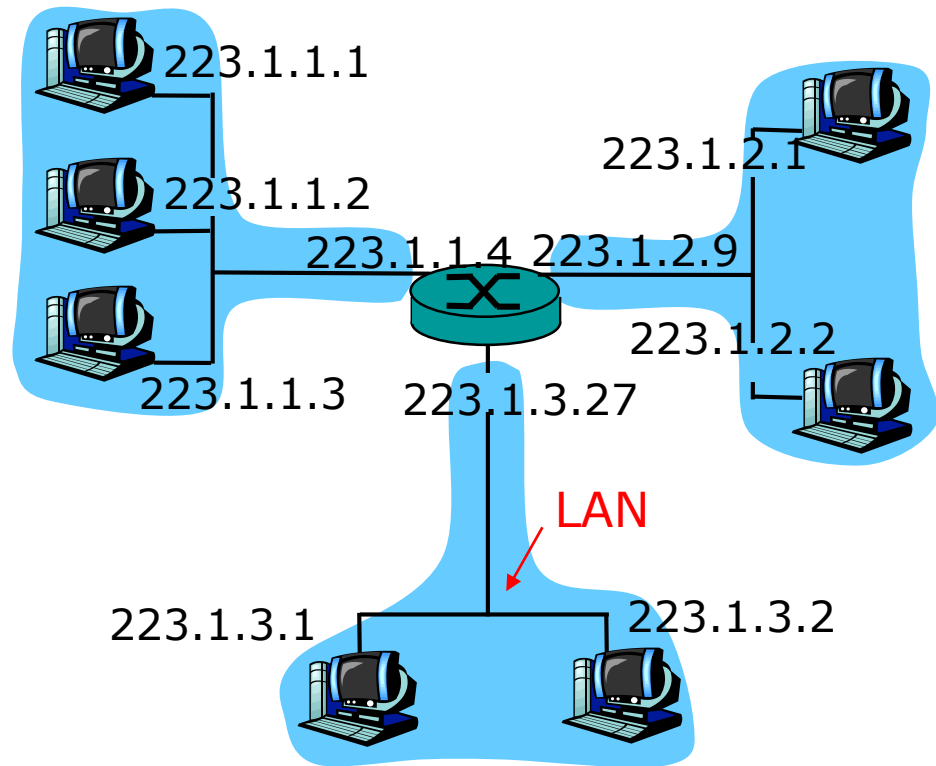


- **Hoszt (host):**
kommunikációs végpont
- **Alhálózat (subnetwork):**
fizikai hálózat, a hozzákapcsolt csomópontok közvetlenül tudnak kommunikálni
- **Útválasztó (router):**
közvetítő a külön alhálózaton található, kommunikáló hosztok között
- **Interfész (interface):**
csomópont kapcsolódási pontja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

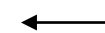


24 bites hálózati címek

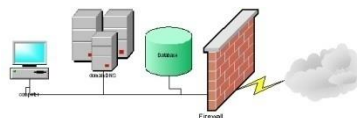
10011000	10000010	11110110	00000010
152	130	246	2



152.130.246.2



pontozott
decimális
jelölés



IP címosztályok

class

A	0 network	host	1.0.0.0 to 127.255.255.255
B	10 network	host	128.0.0.0 to 191.255.255.255
C	110 network	host	192.0.0.0 to 223.255.255.255
D	1110 multicast address		224.0.0.0 to 239.255.255.255

← 32 bit →

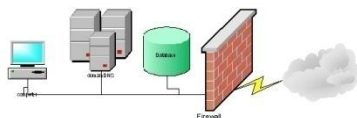
- Elvileg 2^{32} (~4,3 milliárd) cím, de gyakorlatilag csak ~3,3 milliárd
- Nem elég flexibilis – túlságosan fogyasztja az IP címeket ☹
- CIDR: Classless Inter-Domain Routing

Alhálózati maszk (Netmask)

- Az alhálózatok méretét a netmask adja
- A netmask annyi 1-essel kezdődik, ahány bites a címben a hálózati rész

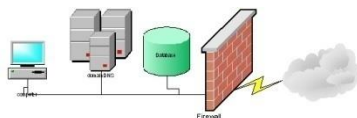
	0 1 2 3 4	N	31	
IP-cím	Network ID	Host ID		
Alhálózati maszk	111...111	000...000		
Hálózatazonosító	Network ID	000...000		

Bitenkénti **ÉS**



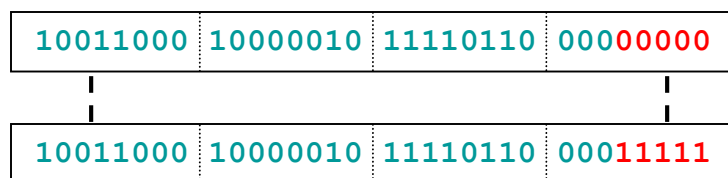
Alhálózati maszk (Netmask)

- 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
- Ha a hálózati cím nemcsak 8,16, 24 bites lehet -> a netmask meghatározhatja a hosszát -> a hálózat méretét



Variable Length Subnet Mask

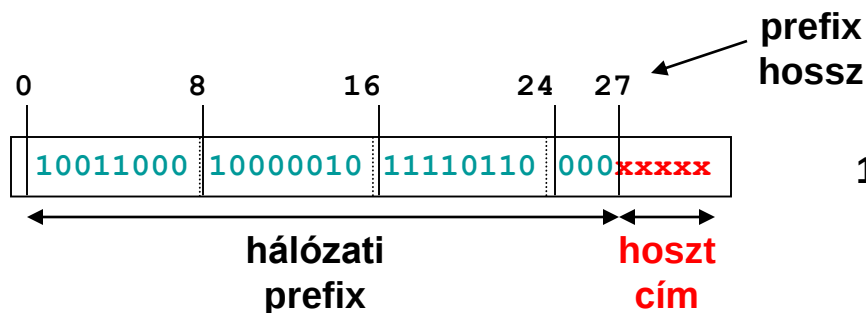
Alhálózatokhoz összefüggő IP címblokkokat rendelünk



152.130.246.0

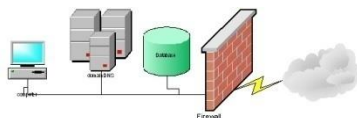
152.130.246.31

2⁵ cím



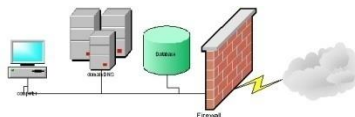
152.130.246.0 /27

<prefix/hossz>
jelölés



Speciális IP címek

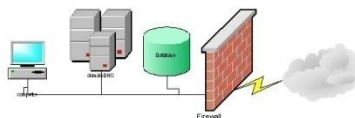
- Host ID csupa 0: a hálózat címe
 - Hálózati cím: 152.66.244.**0**
 - Nem rendelhető hosthoz
- Host ID csupa 1: broadcast cím
 - Broadcast – Üzenetszórás
 - Az alhálózat utolsó címe: pl. 152.66.244.**255**
 - A szabvány engedi a 255.255.255.255 használatát
 - Az alhálózat minden gépének szól
- 127.0.0.0-127.255.255.255: loop-back network (a gép saját magának kézbesíti)
 - **127.0.0.1: helyi gép saját címe**



Private IP címek

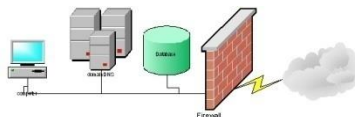
Méret	Tartomány	Prefix	Osztályok szerinti leírás	Legnagyobb CIDR blokk
24 bites blokk	10.0.0.0-10.255.255.255	/8	1 db A osztályú blokk	10.0.0.0/8
20 bites blokk	172.16.0.0-172.31.255.255	/12	16 db folytonos B osztályú blokk	172.16.0.0/12
16 bites blokk	192.168.0.0-192.168.255.255	/16	256 db folytonos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

Private címek nem routolhatók (non-routable)



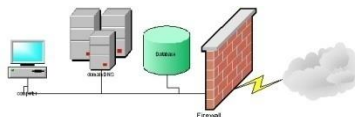
Példa

- 152.130.246.128/28
 - Hány IP címet tartalmaz?
 - Max. hány gépet tartalmaz?
 - Mi a broadcast cím?
- Netmask 28 bites $\rightarrow 32-28=4$ bit host rész
 - $2^4=16$ IP cím
 - $16-2=14$ gépcím (hálózati + broadcast cím!)
 - Ebből 1 cím a router
 - 1000**1111** $\rightarrow 128+15=143 \rightarrow$
152.130.246.143



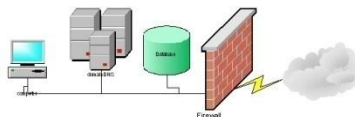
DHCP

- 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

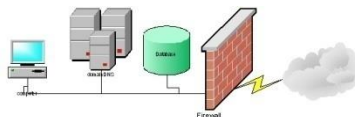
- Media Access Control (Extended Unique Identifier)
 - EUI-48 ill. MAC-48: 48 bites,
 - EUI-64: 64 bites cím
 - 12 hexa formában: **00-09-6B-26-ED-37**
 - Gyártók adják a kártyáknak (**IEEE alapján**)
 - OUI: Organizational Unique Identifier
 - 2^{48} kombináció (281 ezer milliárd)
 - Ethernet
 - Bluetooth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

1. “Ha az IP címed
160.30.100.10, akkor kérlek,
küldd el nekem a
hardver-címedet!”

Forrás

160.30.100.20

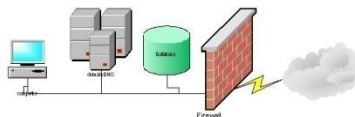
00-aa-00-12-34-56

Broadcast

Cél

160.30.100.10

00-a0-c9-78-9a-bc



Címfeloldási Protokoll (ARP)

1. “Ha az IP címed
160.30.100.10, akkor kérlek,
küldd el nekem a
hardver-címedet!”

Az ARP üzenetváltás:

Req: Who-has 160.30.100.10? Tell
00:aa:00:12:34:56

Forrás

160.30.100.20

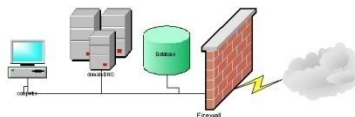
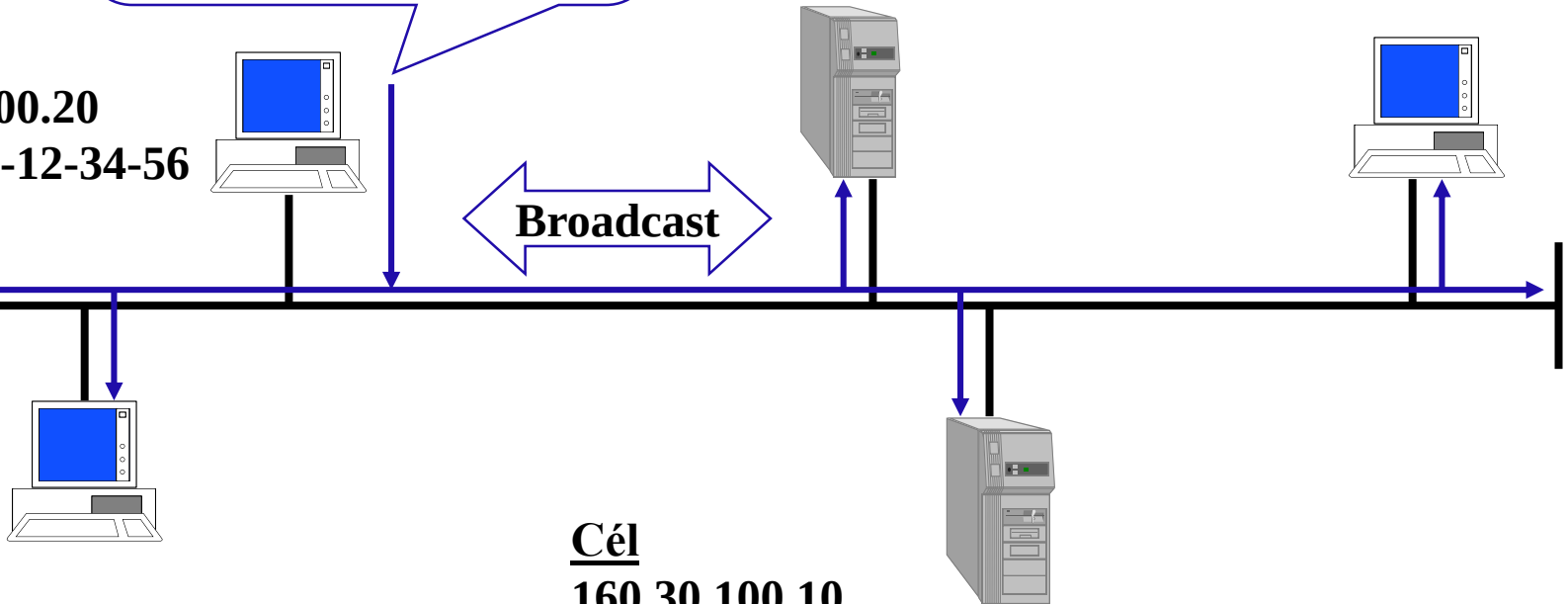
00-aa-00-12-34-56

Broadcast

Cél

160.30.100.10

00-a0-c9-78-9a-bc



Címfeloldási Protokoll (ARP)

1. “Ha az IP címed
160.30.100.10, akkor kérlek,
küldd el nekem a
hardver-címedet!”

Az ARP üzenetváltás:

Req: Who-has 160.30.100.10? Tell
00:aa:00:12:34:56

Forrás

160.30.100.20

00-aa-00-12-34-56

Broadcast

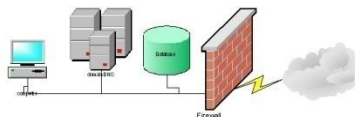
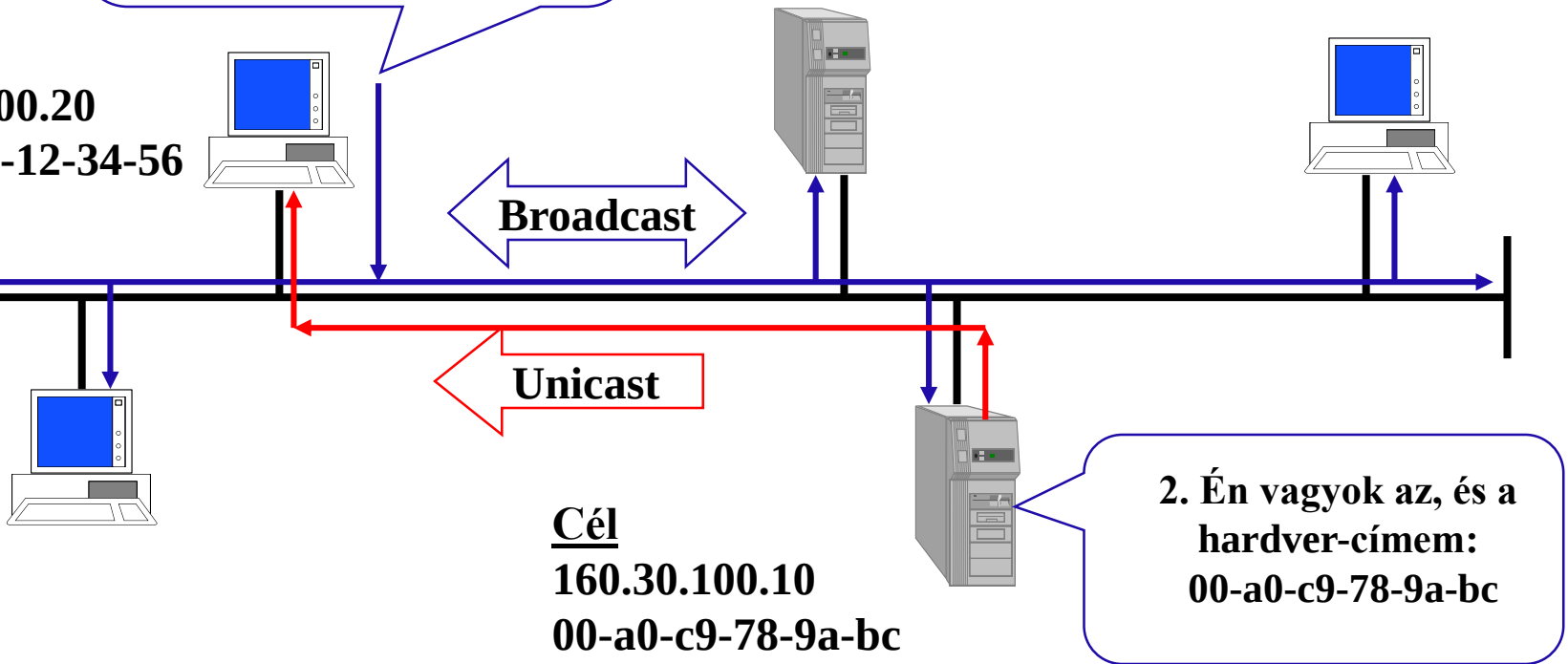
Unicast

Cél

160.30.100.10

00-a0-c9-78-9a-bc

2. Én vagyok az, és a
hardver-címem:
00-a0-c9-78-9a-bc



Címfeloldási Protokoll (ARP)

1. “Ha az IP címed
160.30.100.10, akkor kérlek,
küldd el nekem a
hardver-címedet!”

Az ARP üzenetváltás:

Req: Who-has 160.30.100.10? Tell

00:aa:00:12:34:56

Ans: 160.30.100.10 is-at

00:a0:c9:78:9a:bc

Forrás

160.30.100.20

00-aa-00-12-34-56

Broadcast

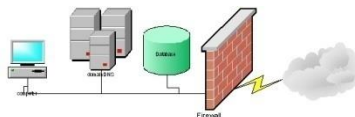
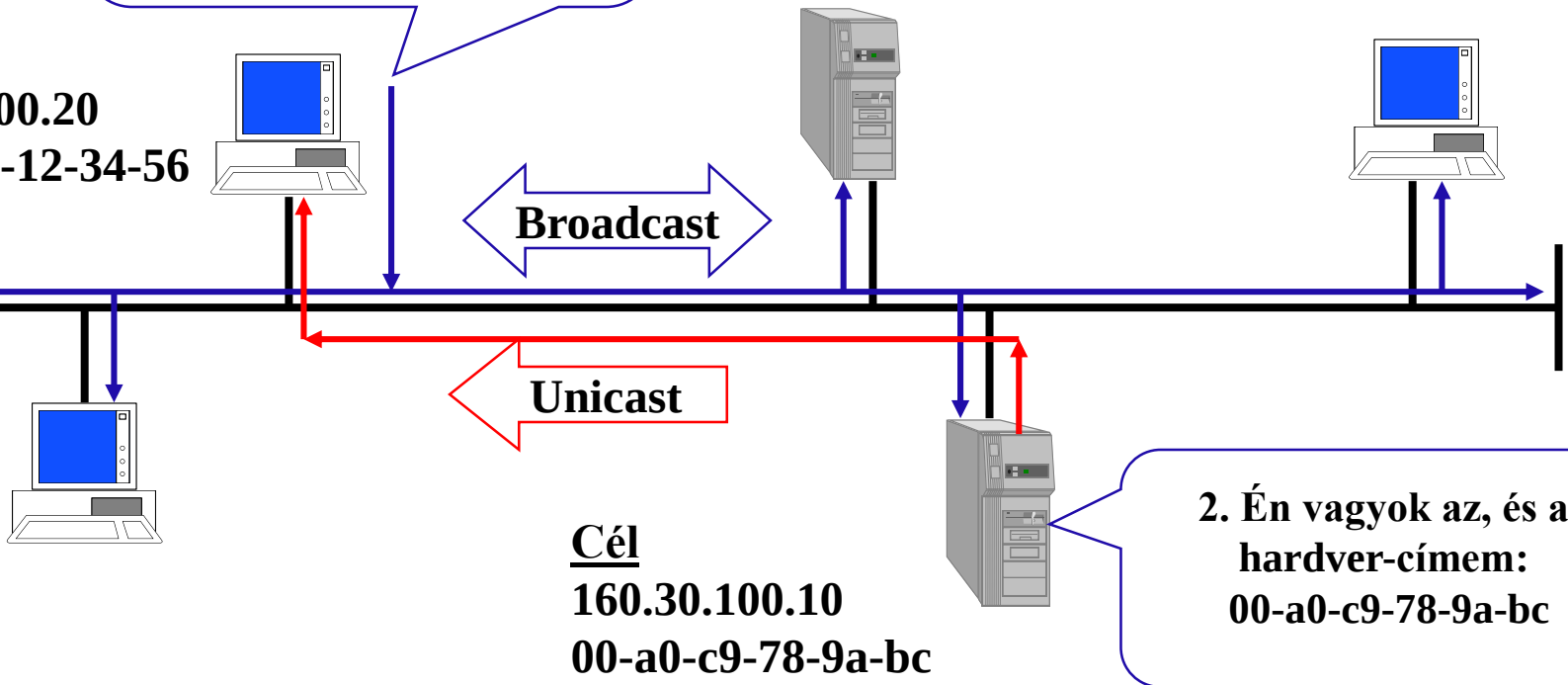
Unicast

Cél

160.30.100.10

00-a0-c9-78-9a-bc

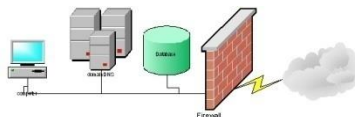
2. Én vagyok az, és a
hardver-címem:
00-a0-c9-78-9a-bc



Fordított címfeloldási protokoll

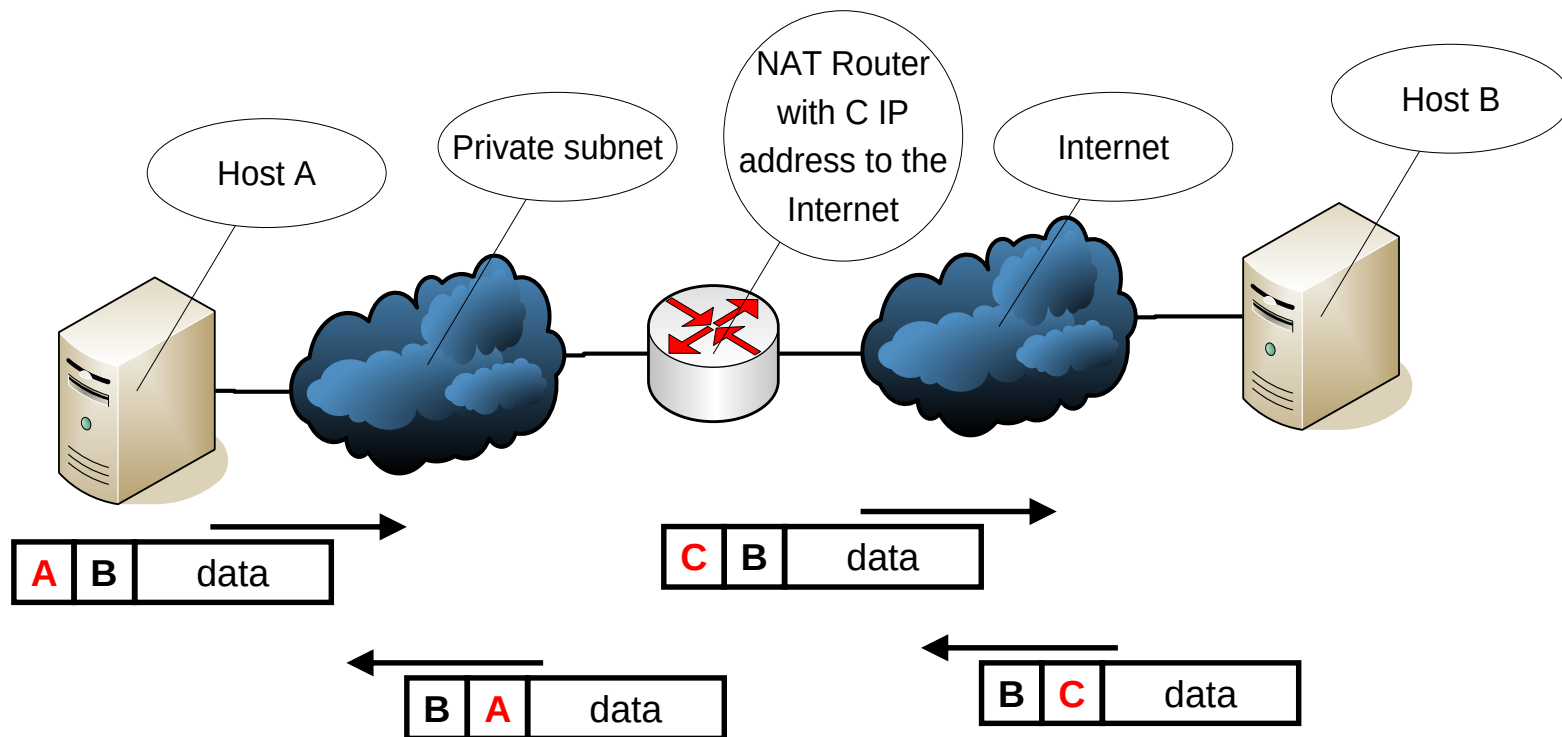
(RARP – Reverse Address Resolution Protocol)

- 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
 - DHCP
 - For ‘stupid’ devices, e.g. printer

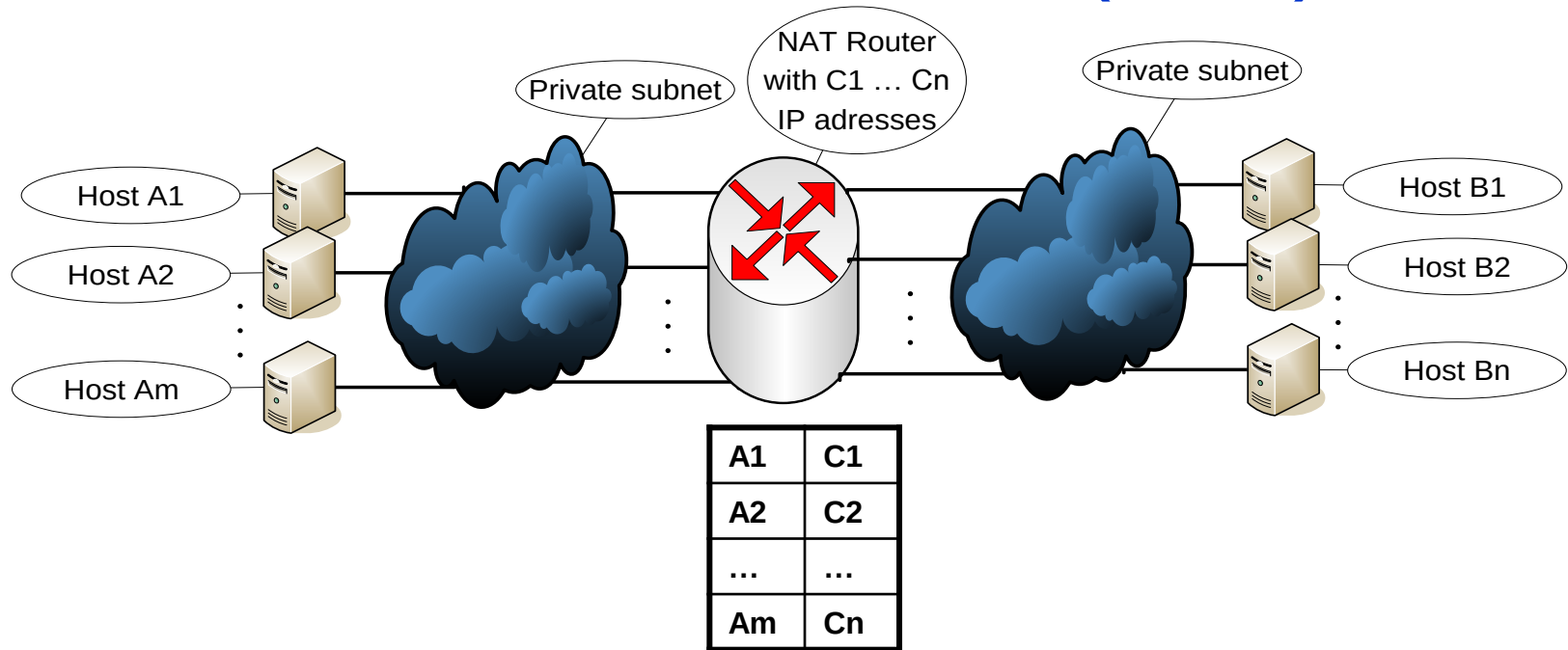


NAT

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

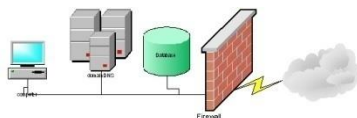
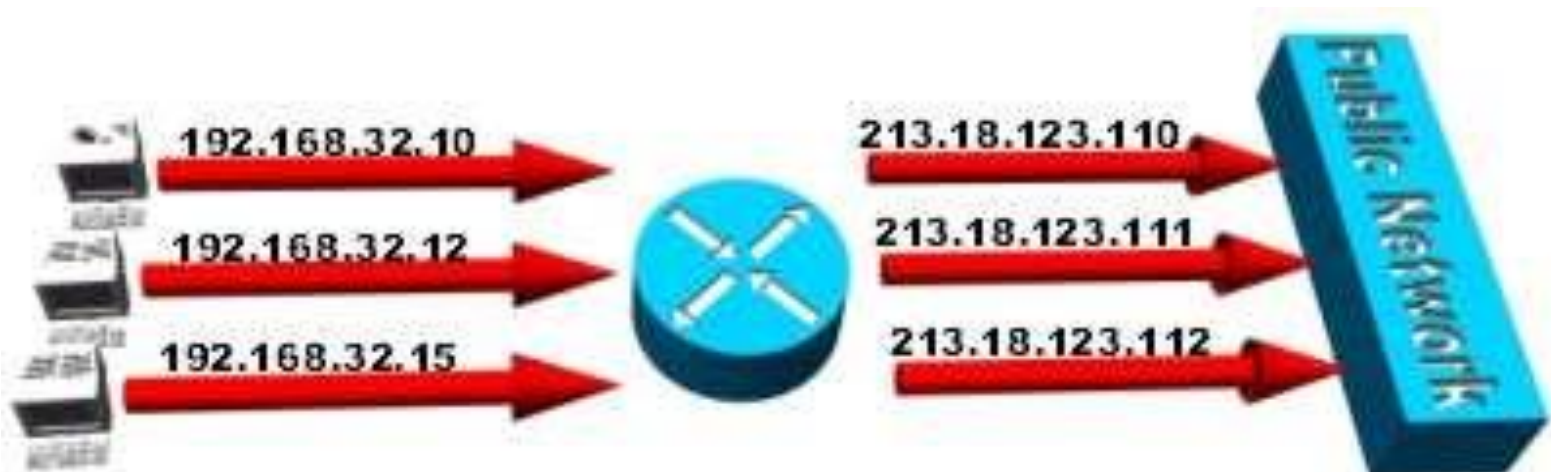


NAT – több hoszttal ($m=n$)

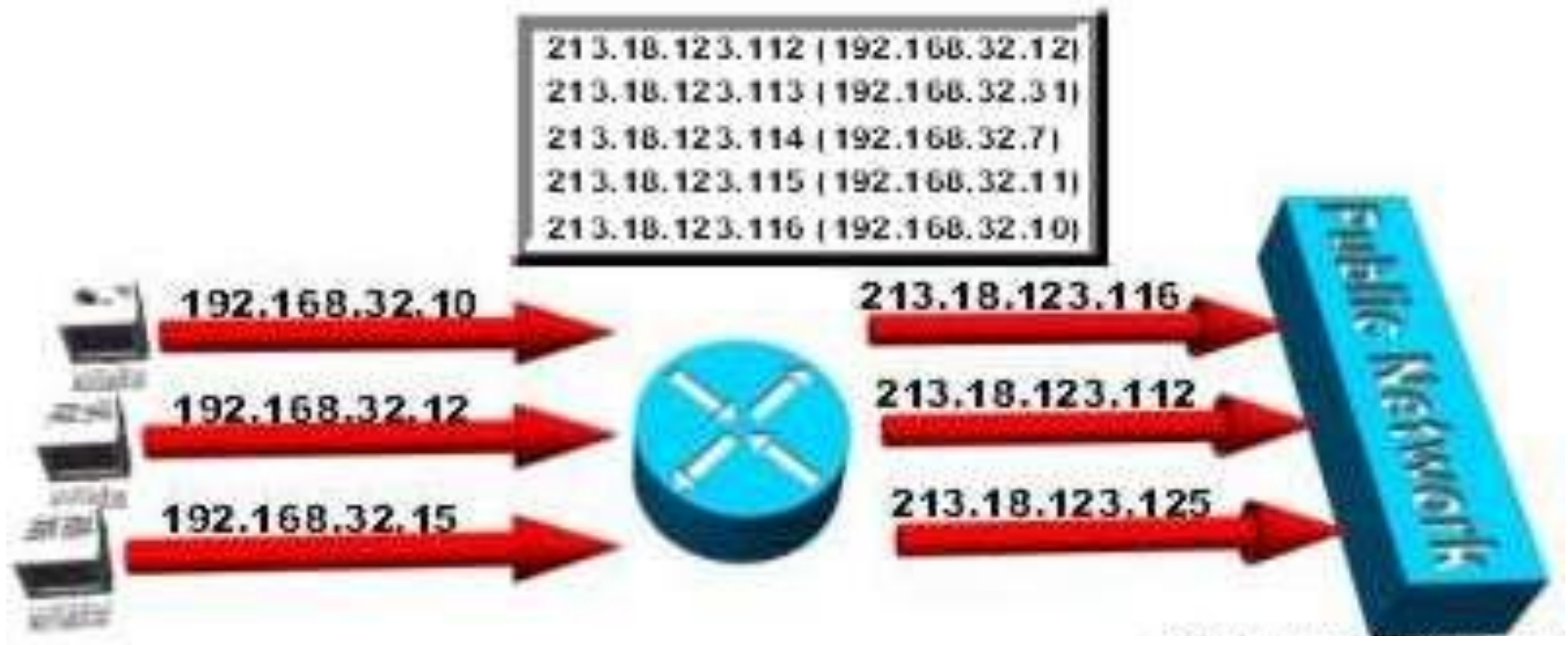


- Kifelé használt privát címek száma = a router számára elérhető publikus IP címek száma
- Hozzárendelés
 - statikus
 - dinamikus
 - biztonság növelésére

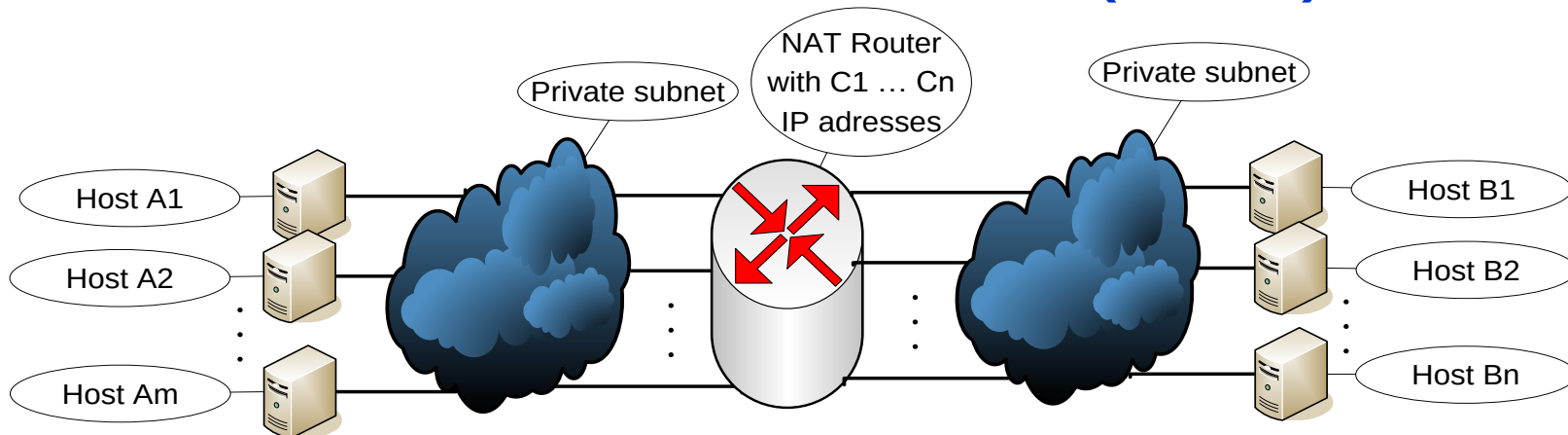
Statikus NAT példa



Dinamikus NAT példa



NAT – több hoszttal ($m > n$)

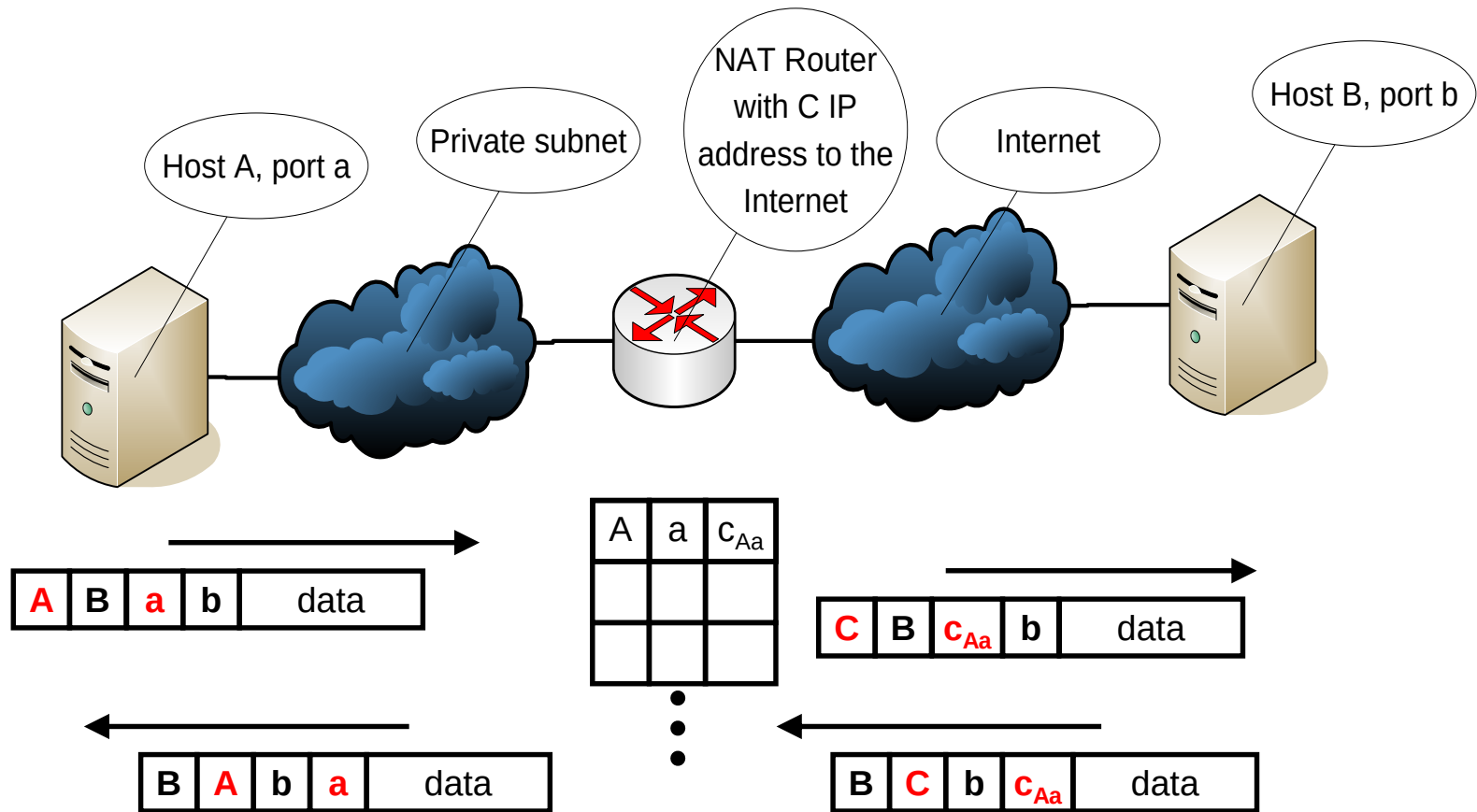


A1	C1
A2	C2
...	...
Am	Cn

- Hozzárendelési stratégia kell
 - ha nincs elég ($m > n$)???
 - Tipikusan: $n = 1$ (szerver szolgáltatás)
 - 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

NAT + port transzláció

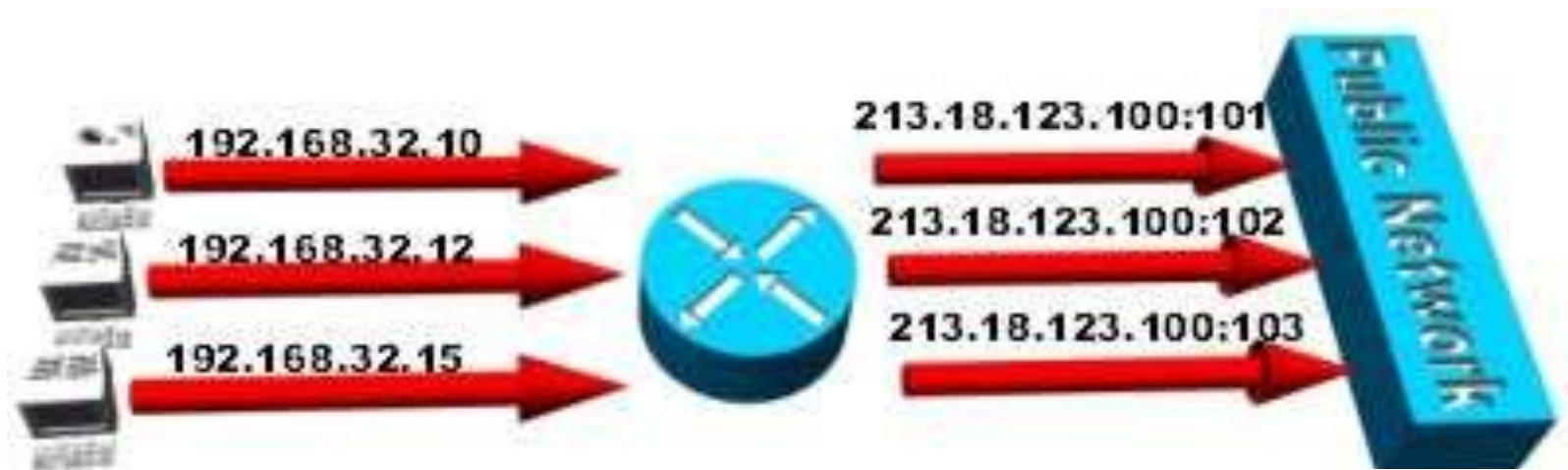
- Network Address Port Translation (NAPT)



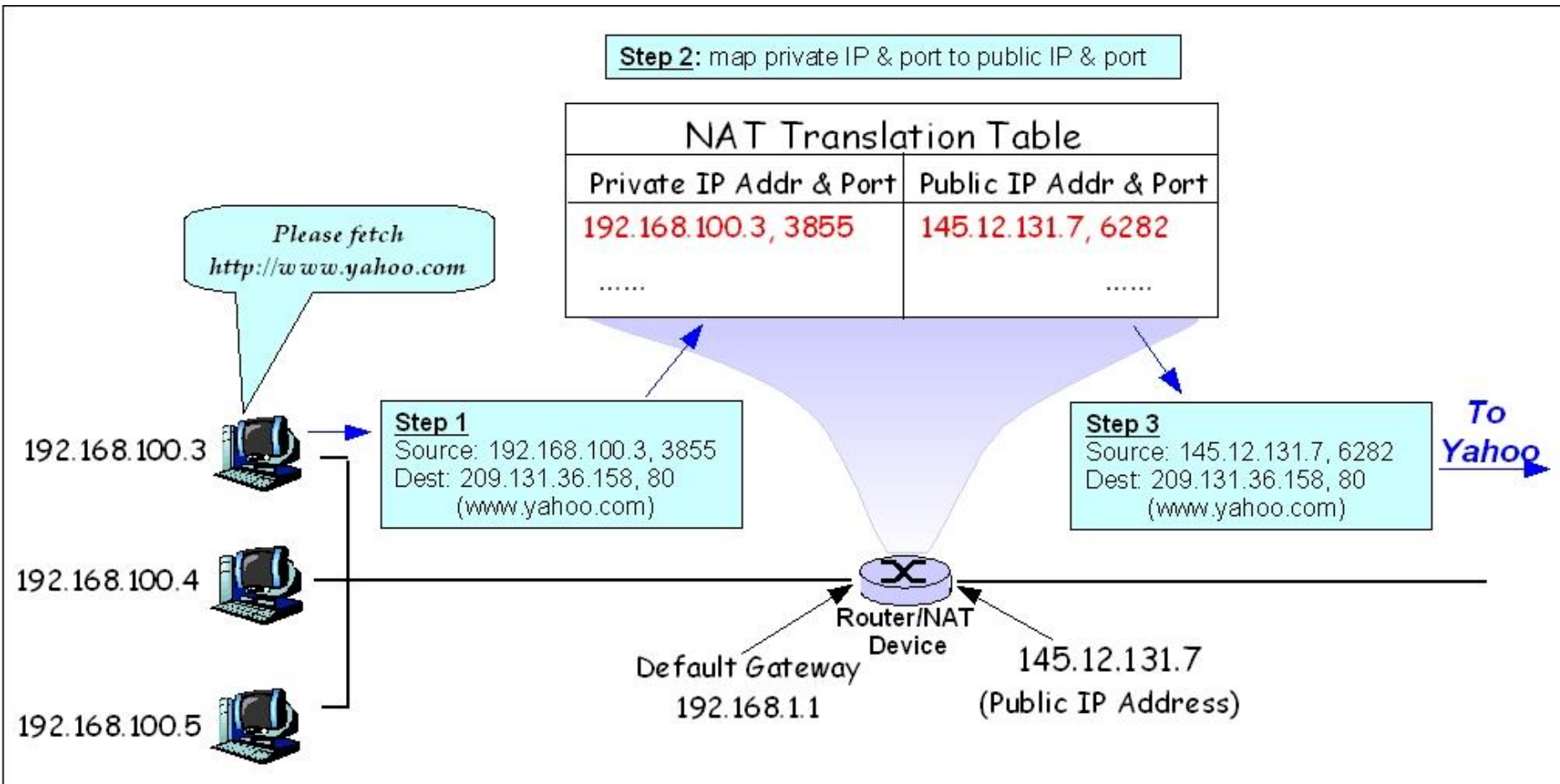
NAPT példa

Táblázat:

- DRAM (Dynamic RAM)
- 4MB ~26000 kapcsolat

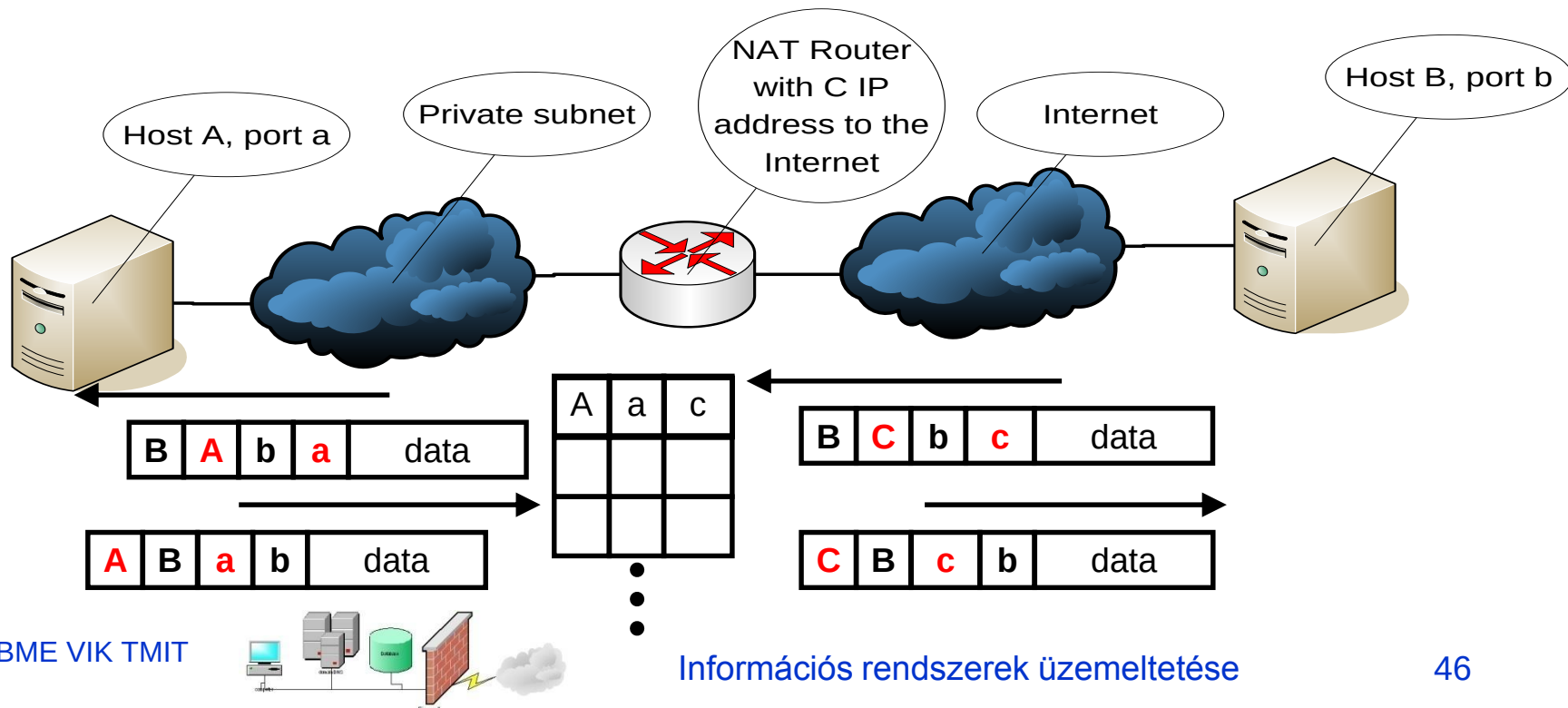


NAPT példa



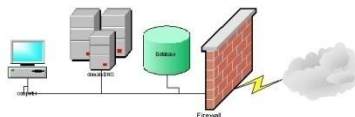
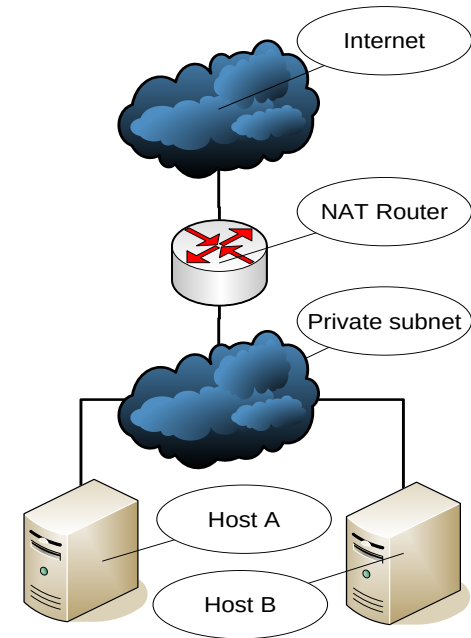
NAPT – virtuális szerver

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



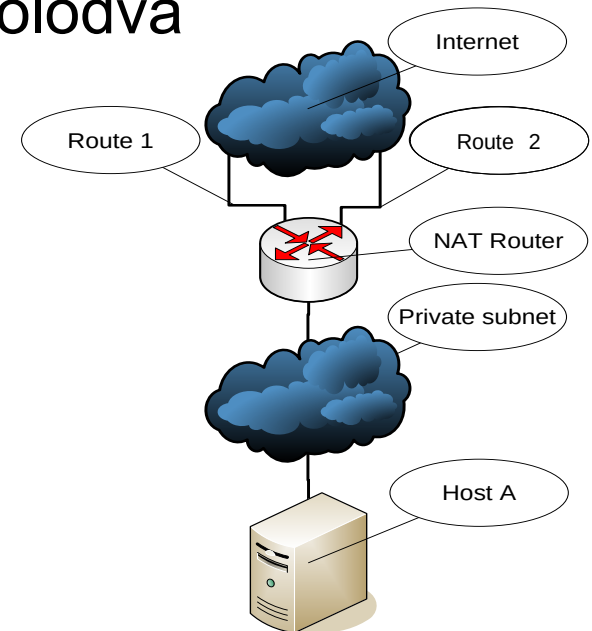
NA(P)T – optimalizációk

- Több belső szerver
 - Terhelésmegosztás
 - Belső struktúra módosítható



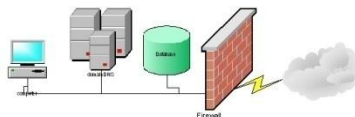
NA(P)T – optimalizációk

- Több külső interfész
 - Rendelkezésre állás
 - Multi-homing
 - Tipikusan több ISP-hez kapcsolódva



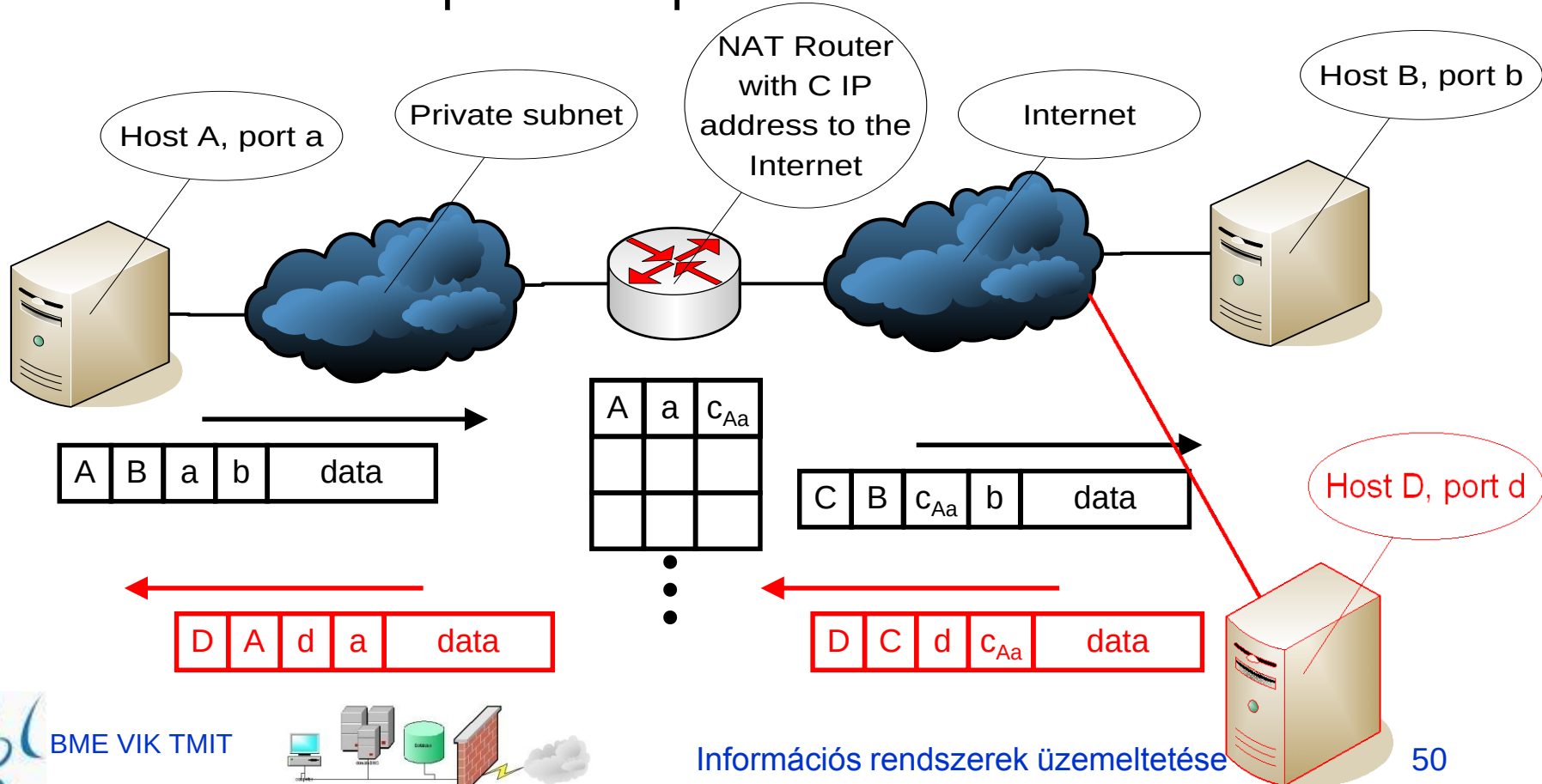
NA(P)T – tűzfal

- Külső kapcsolatokat tilt
 - Csak belülről indított kapcsolatokra enged választ
- DE: inbound mapping
 - Bizonyos eszközökről (IP címekről) “beenged”
 - Pl. otthonról dolgozás
 - Előre konfigurálni kell
- NAPT $\neq$ proxy szerver
 - NA(P)T transzparens a szerverek számára



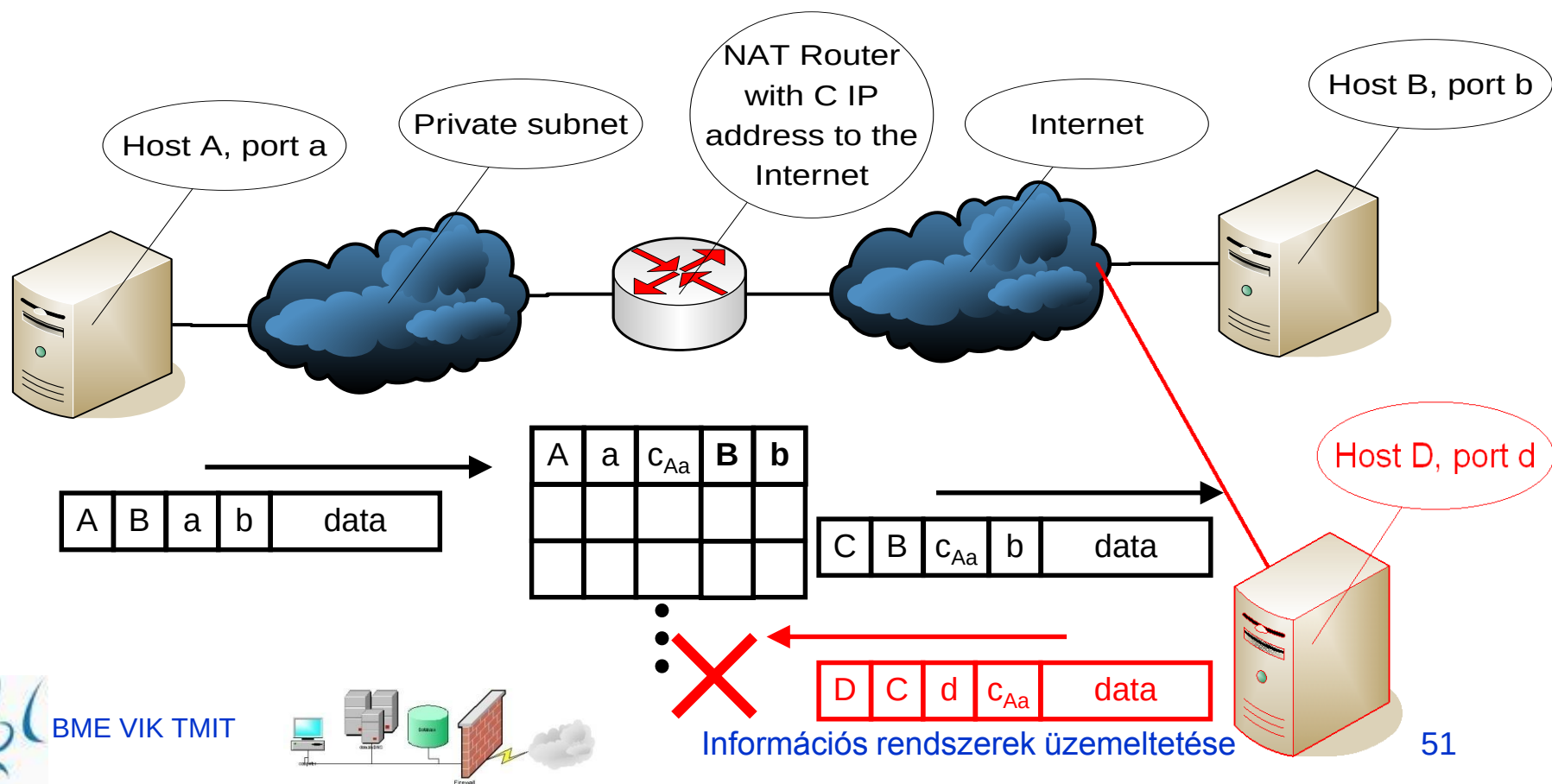
NAPT – biztonság

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



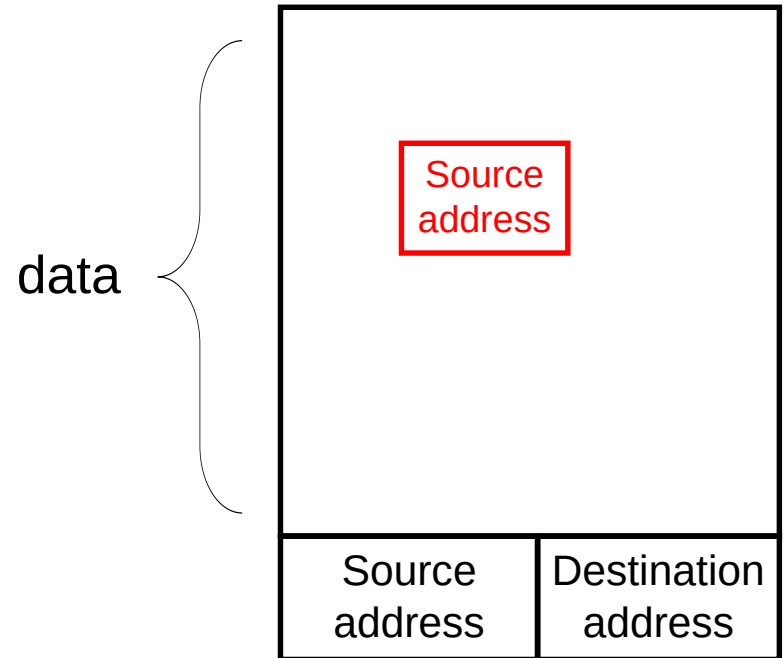
NAPT – biztonsági kiegészítés

- Távoli IP címmel kiegészítve
- Egyszerű tűzfal megoldás

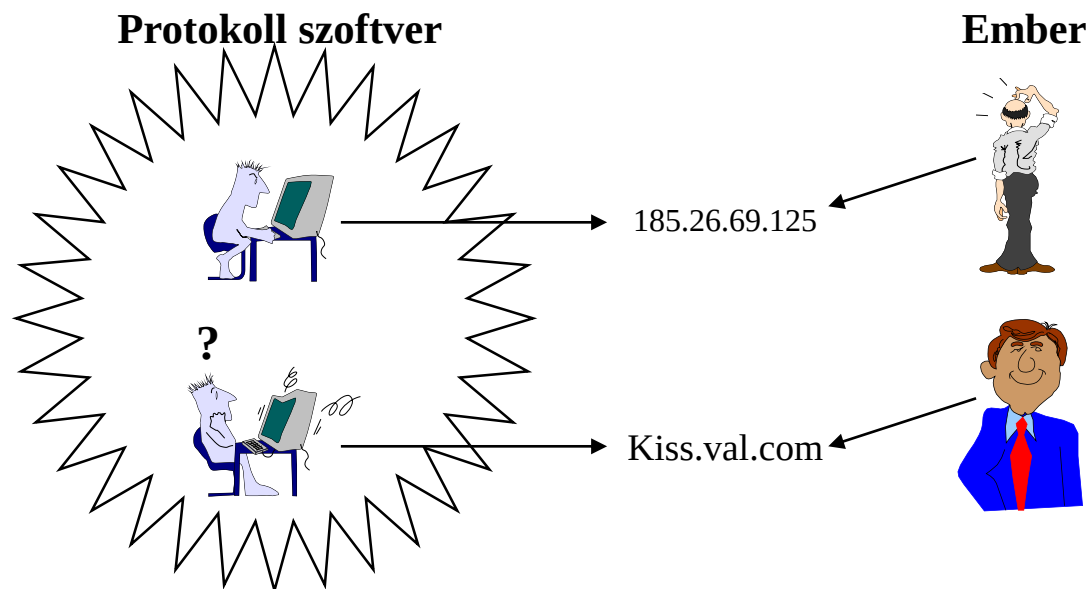


NA(P)T problémák

- 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



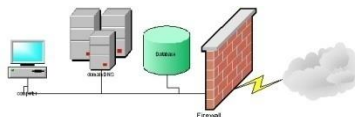
Domain Name System (DNS)



- 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

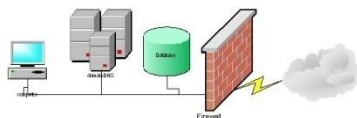


DNS névtér

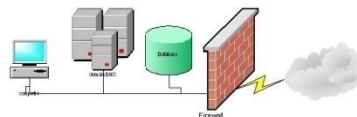
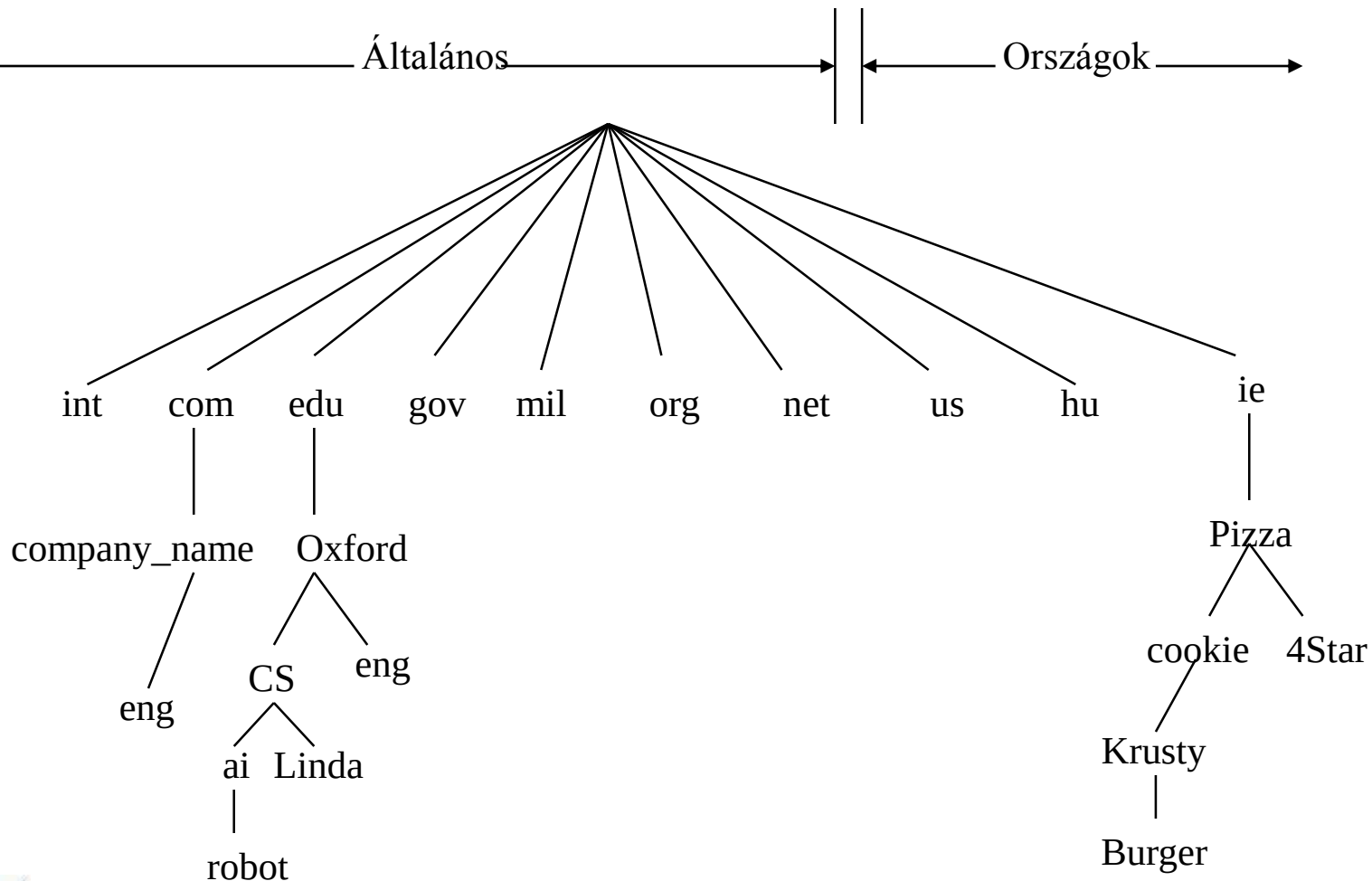
- Általános csoportok:
 - (Nagyrészüket csak az USA-ban lehet regisztrálni, de a .com pl. szabadon regisztrálható)

<i>Domain</i>	<i>Meghatározás</i>
.com	Kereskedelmi szervezetek
.edu	Oktatási intézmények
.gov	Kormányzati intézmények
.mil	Katonai csoportok
.net	Főbb hálózati szolgáltatók
.org	Szervezetek a fentiekén kívül
.int	Nemzetközi szervezetek

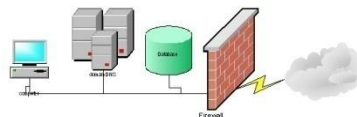
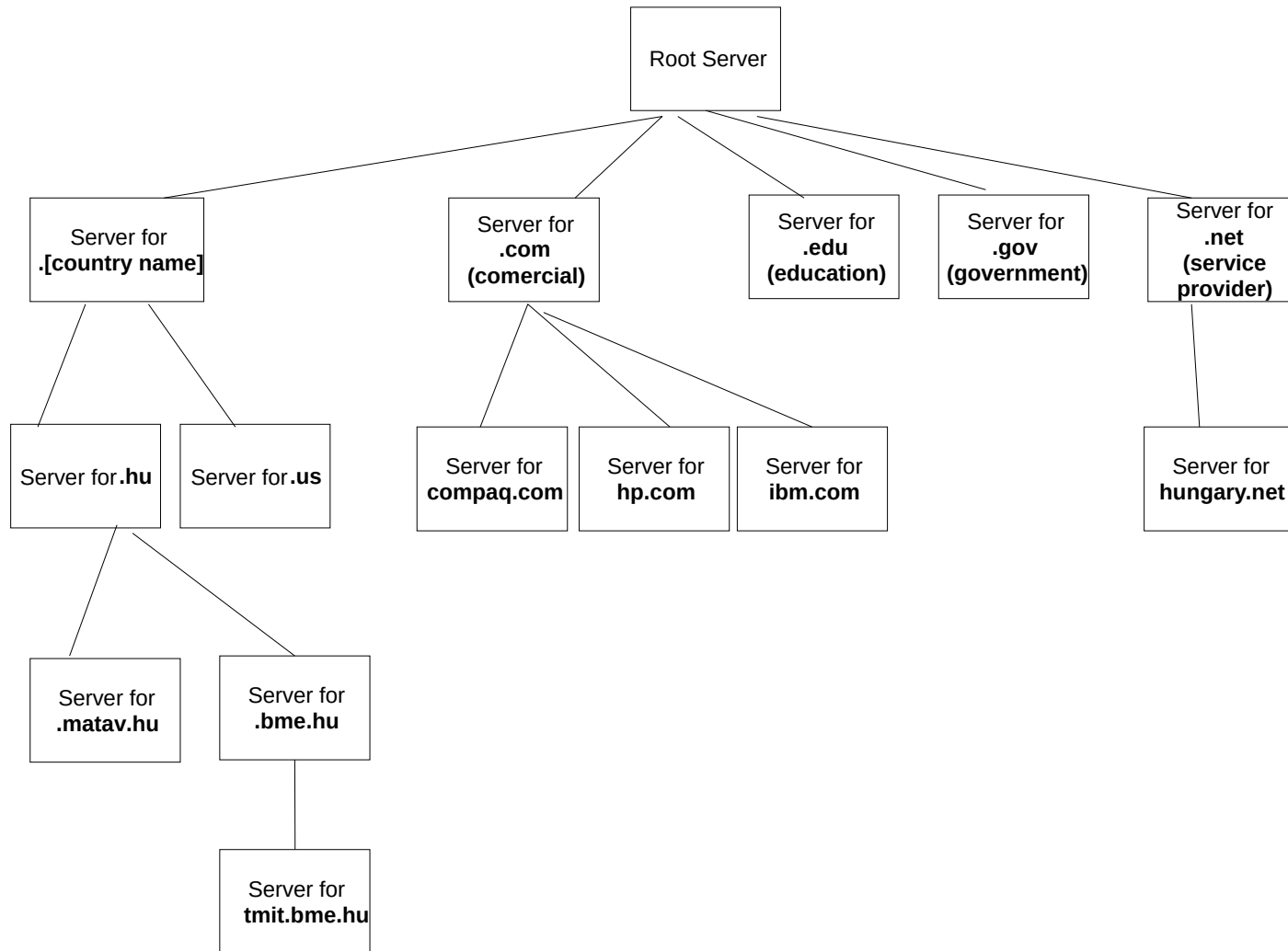
- Országok
 - pl: .hu .us .fr .de



Internet domain névtér

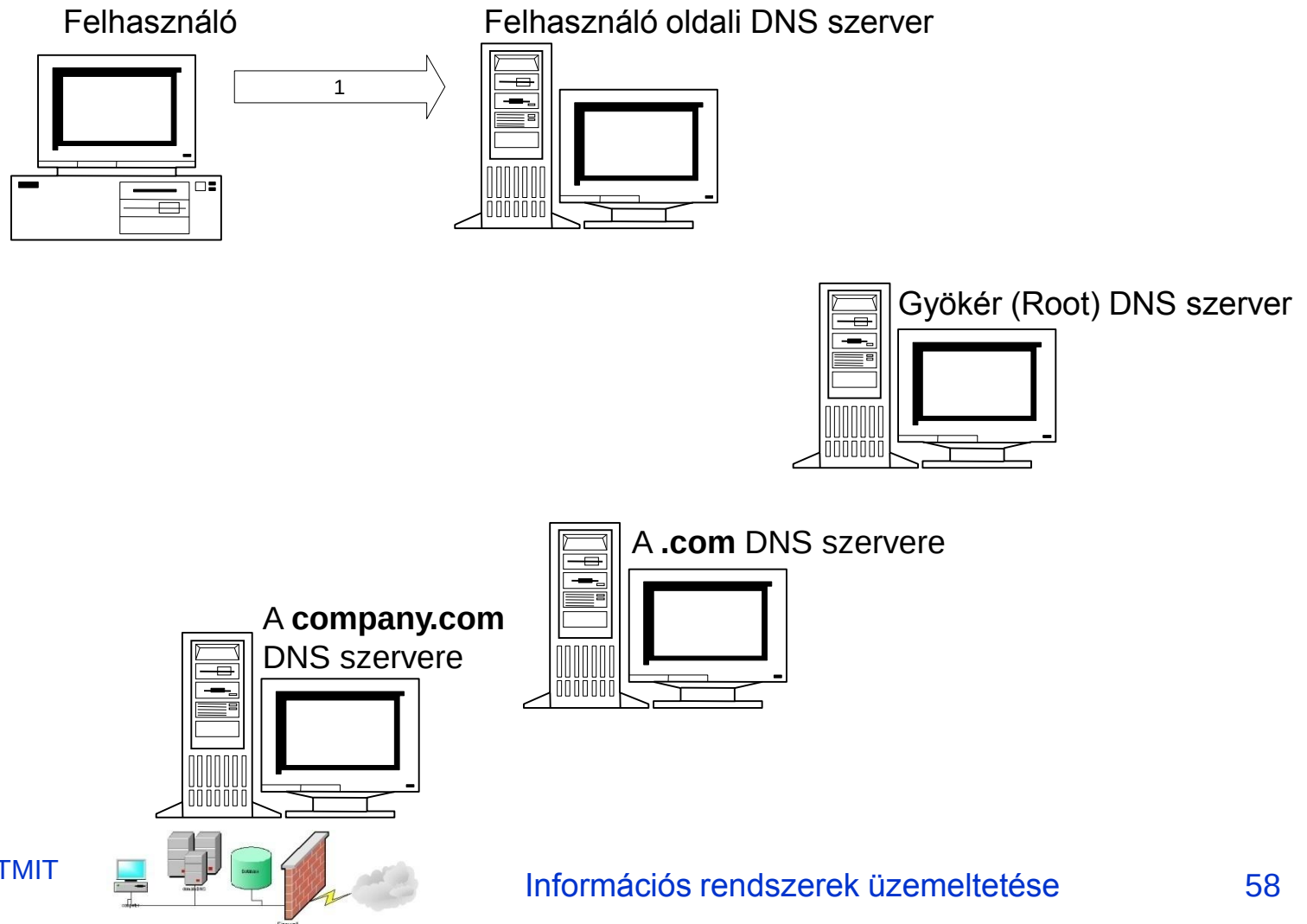


Domain név feloldása



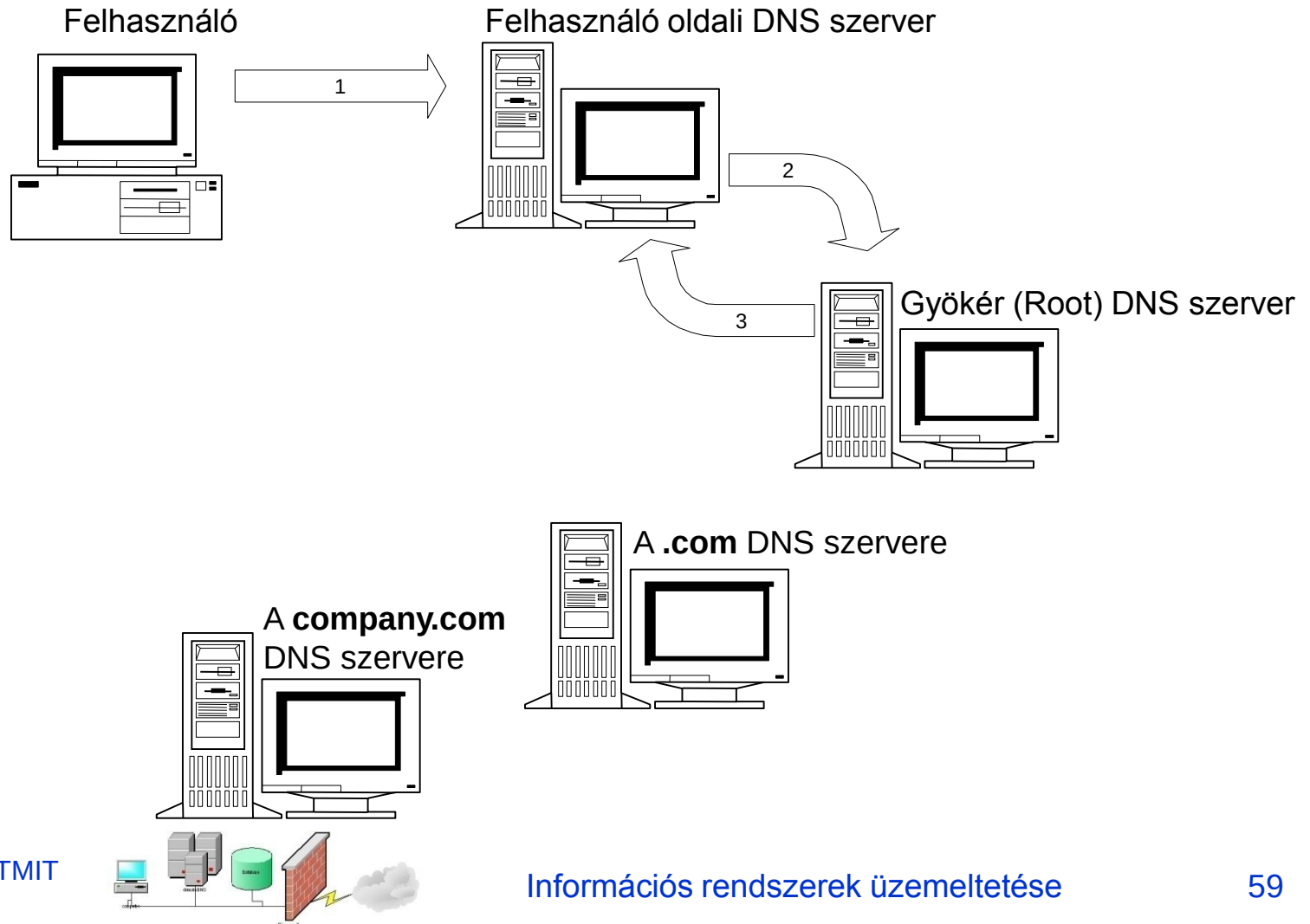
A DNS működése

(A somebody.company.com domain név feloldásának lépései)



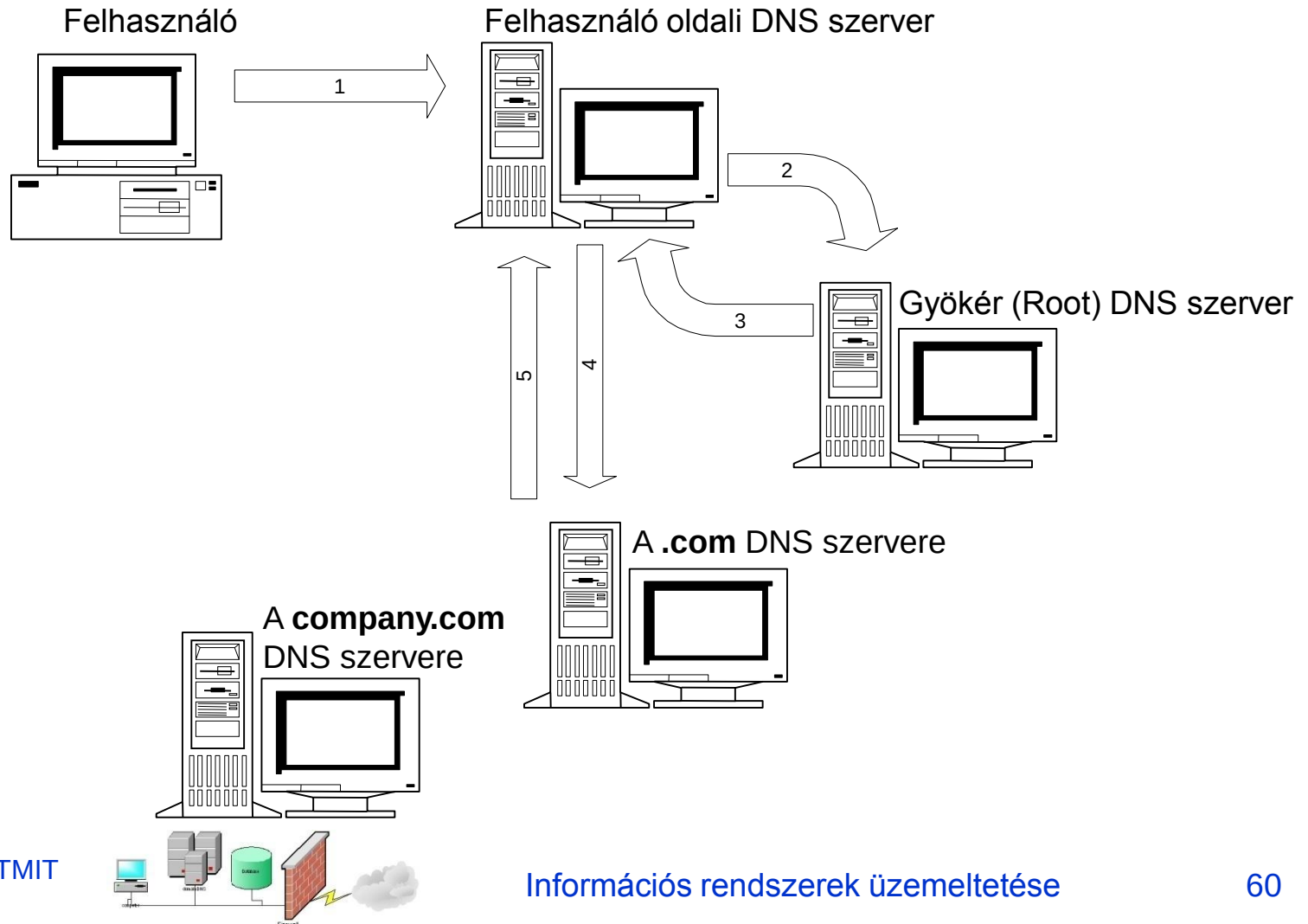
A DNS működése

(A somebody.company.com domain név feloldásának lépései)



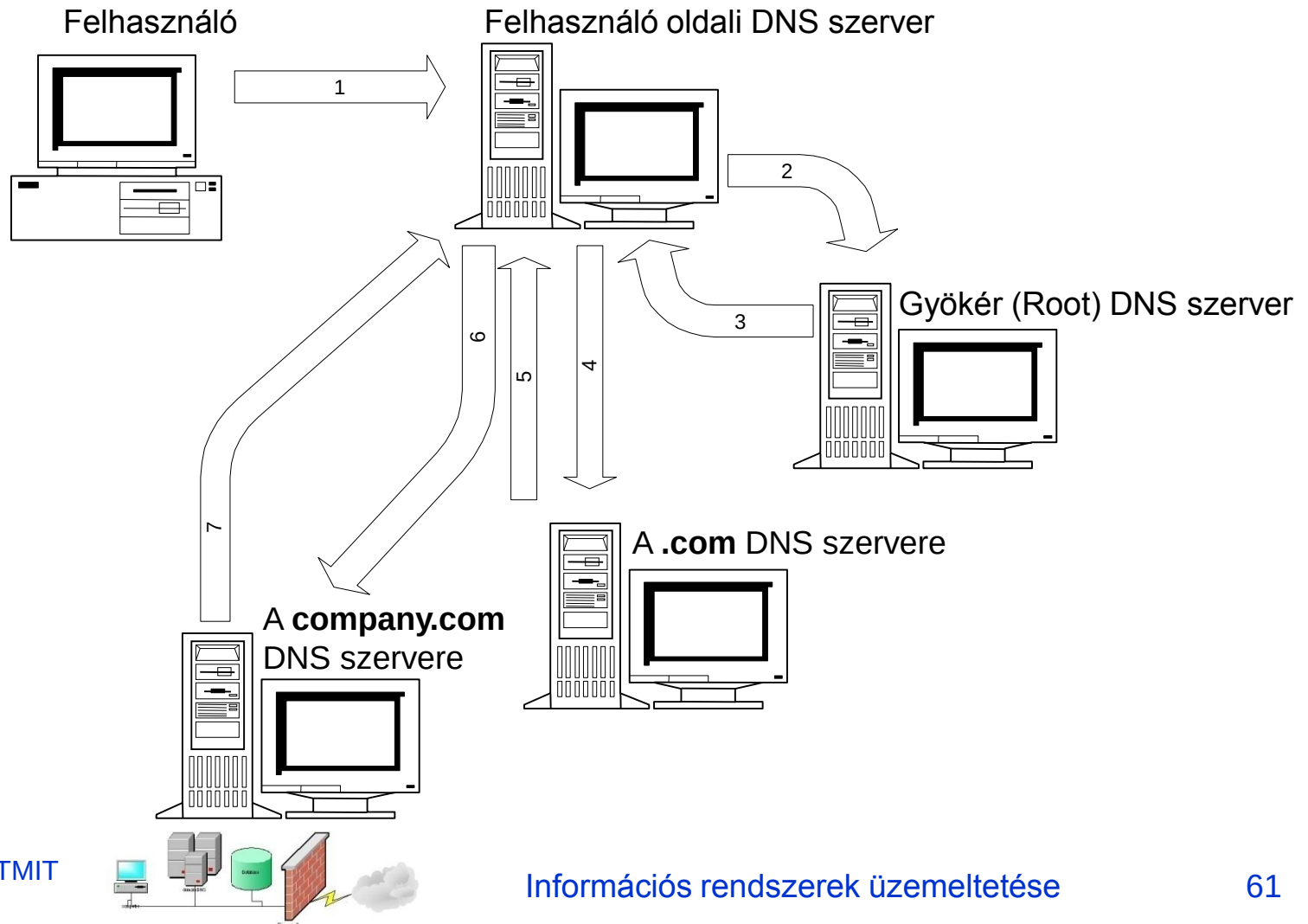
A DNS működése

(A somebody.company.com domain név feloldásának lépései)



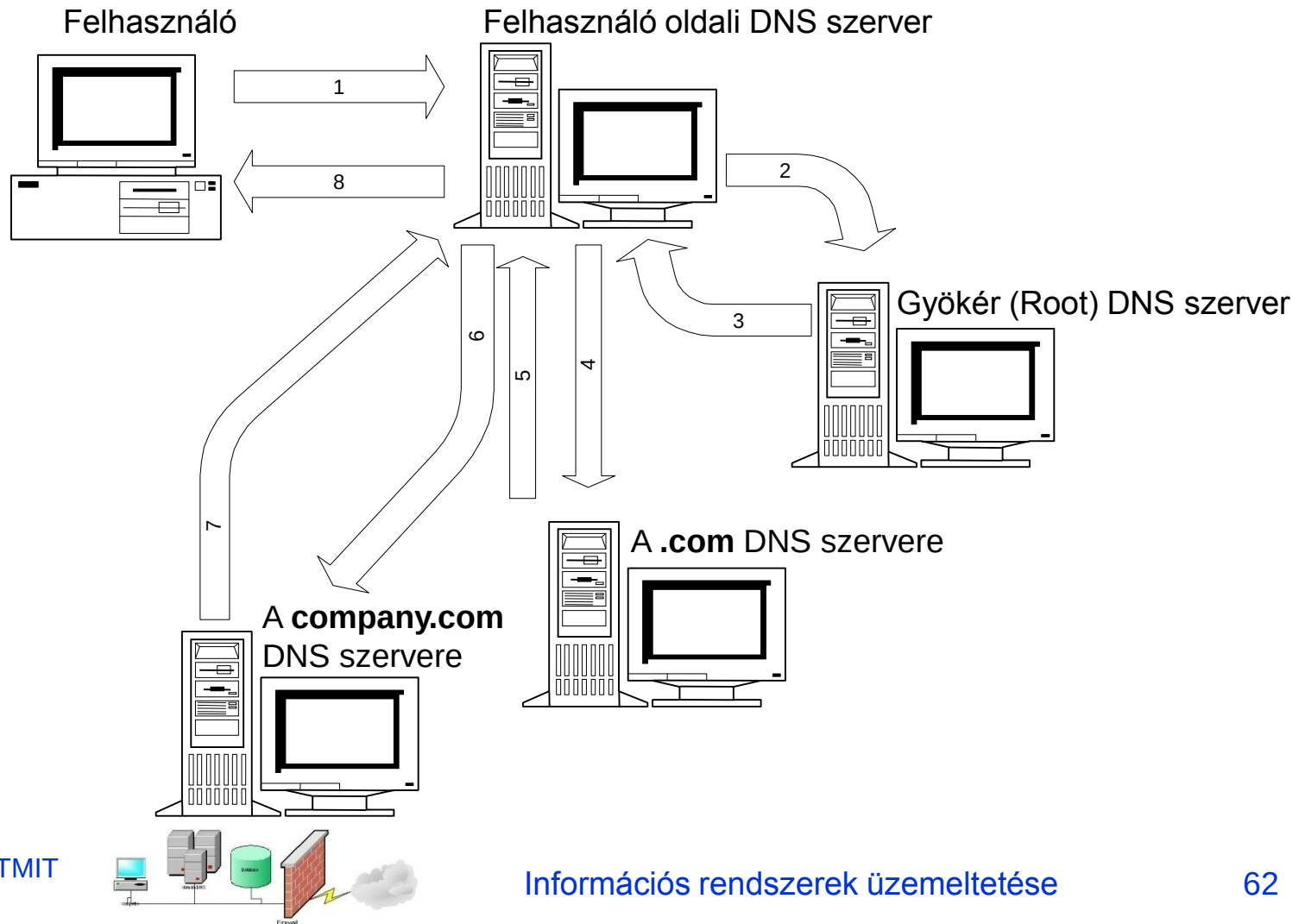
A DNS működése

(A somebody.company.com domain név feloldásának lépései)



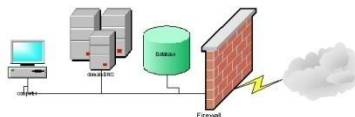
A DNS működése

(A somebody.company.com domain név feloldásának lépései)



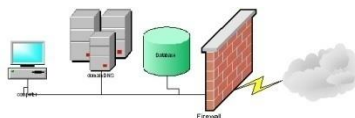
DNS Gyorsítótár (DNS Caching)

- 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)

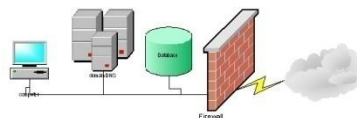
- Hibajelentésekre és IP szintű kontroll üzenetek továbbítására
- Direkt IP csomagokban
- Leggyakrabban használt debuggoló eszköz
 - Ping, traceroute



Üzenetformátum és -típusok

IP Header	
Type of Message	8b
Error Code	8b
Checksum	16b
Parameters, if any	Var
Information	Var

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

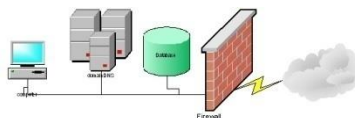
Reply from 152.66.246.10: bytes=32 time=27ms TTL=250

Ping statistics for 152.66.246.10:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

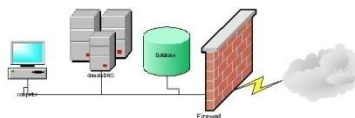
Approximate round trip times in milli-seconds:

Minimum = 23ms, Maximum = 114ms, Average = 47ms



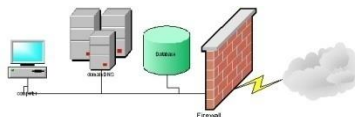
IP beállítások

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



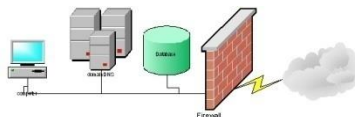
II. rész

Hálózatok

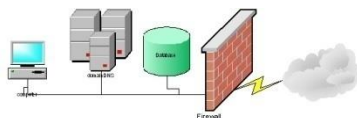
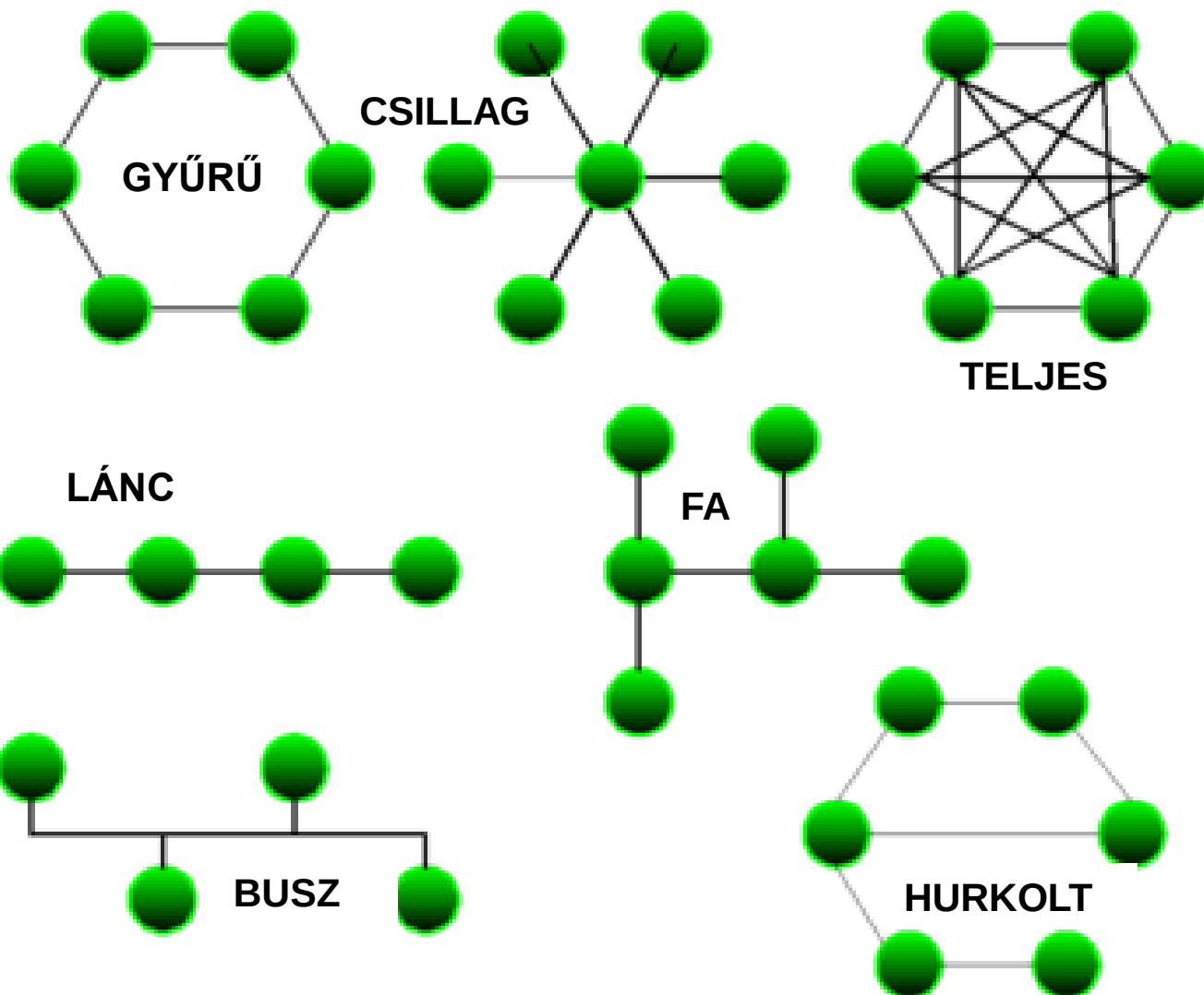


Hálózatok, hálózatok üzemeltetése

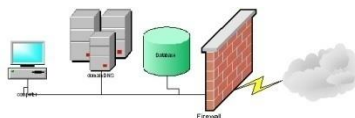
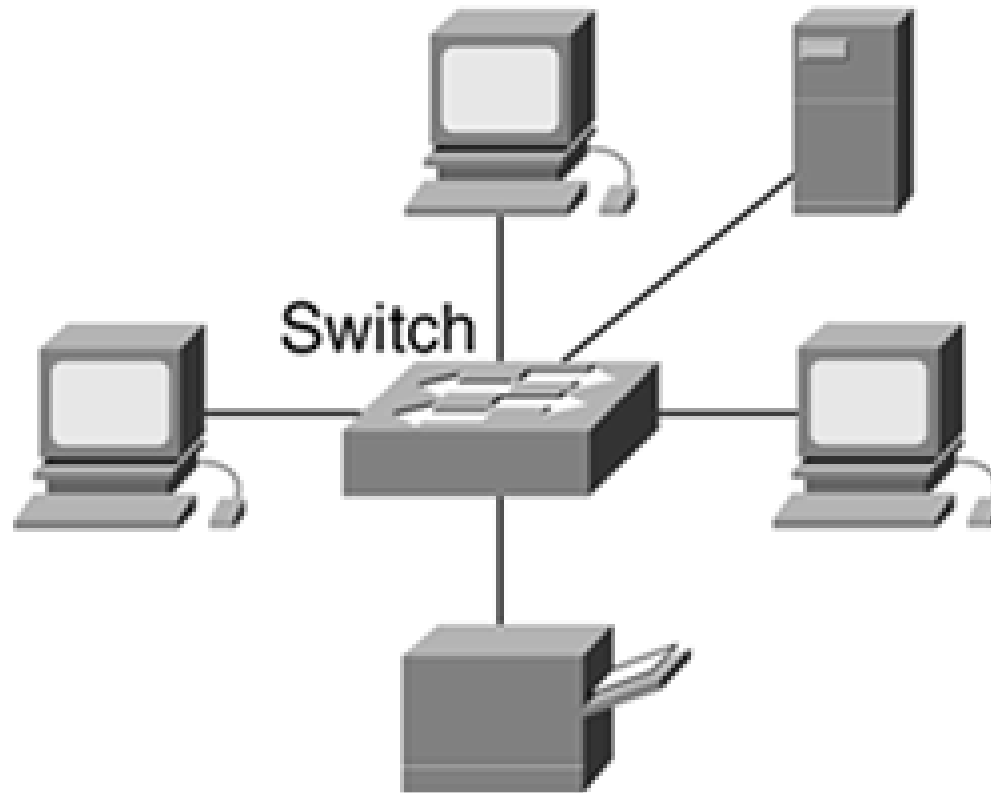
- Ez a tantárgy épít
 - Számítógép-hálózatok
 - Távközlő hálózatok tantárgyak ismereteire
- Ebben a fejezetben olyan hálózati témákat érintünk csak, amelyek az üzemeltetési feladatok megértéséhez fontosak
 - Hálózati topológiák
 - Fizikai és logikai hálózati térképek
 - Demarkációs pontok



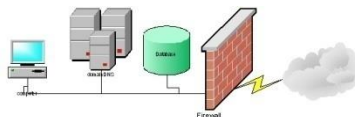
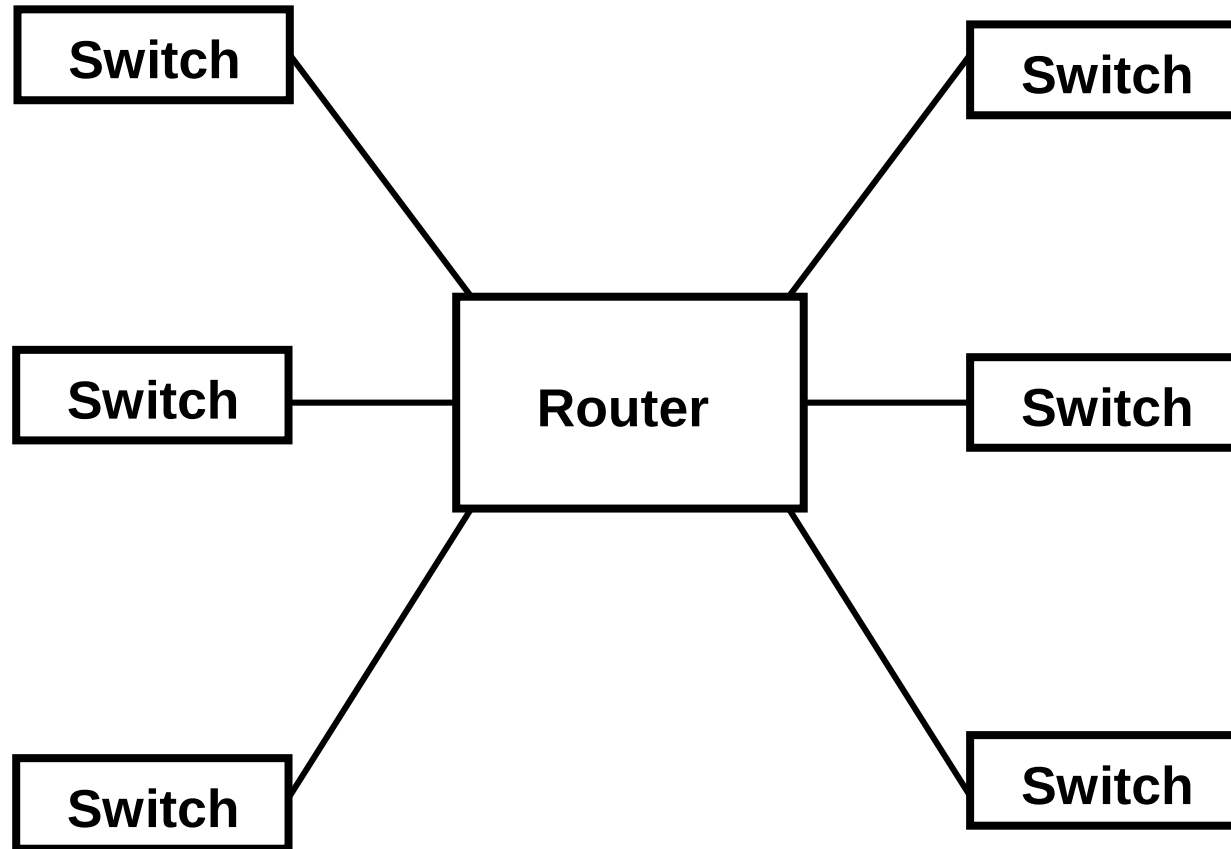
Hálózati topológiák



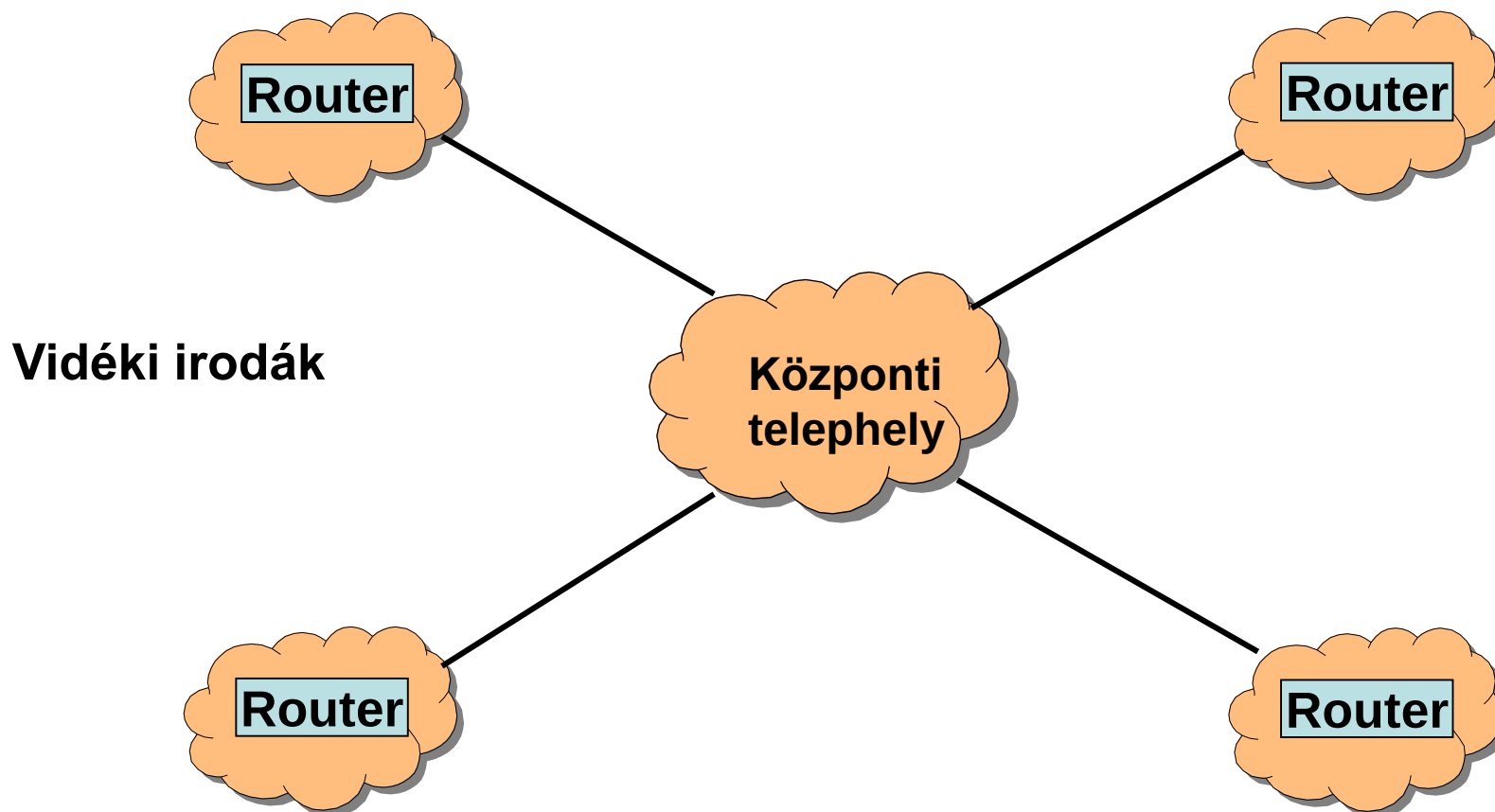
Egyszerű csillag LAN



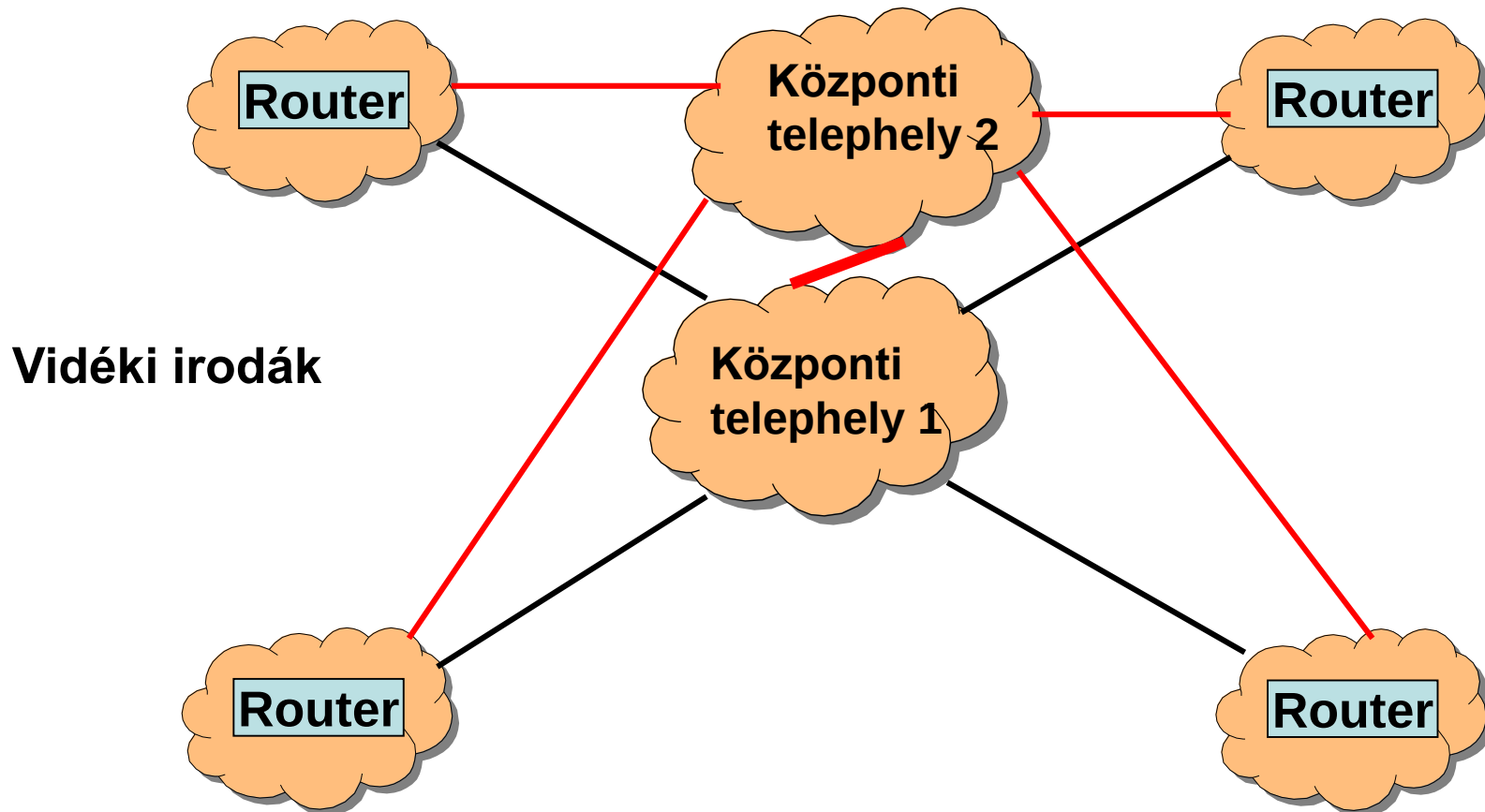
LAN, Campus hálózat - csillag



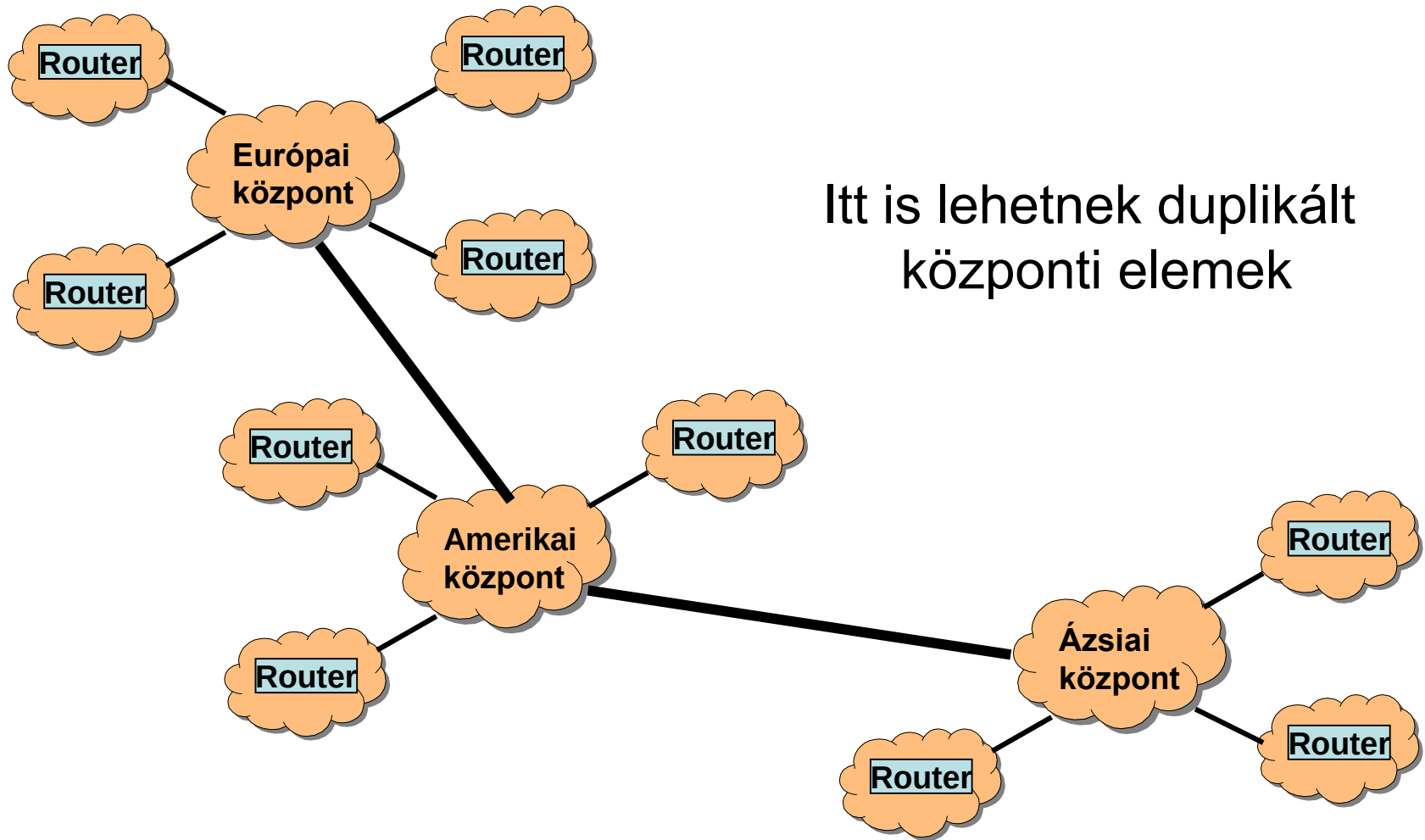
WAN – csillag



WAN – csillag – duplikált központ

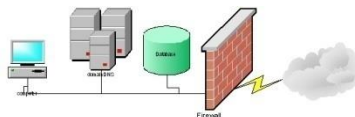


Többszörös csillag (fa)

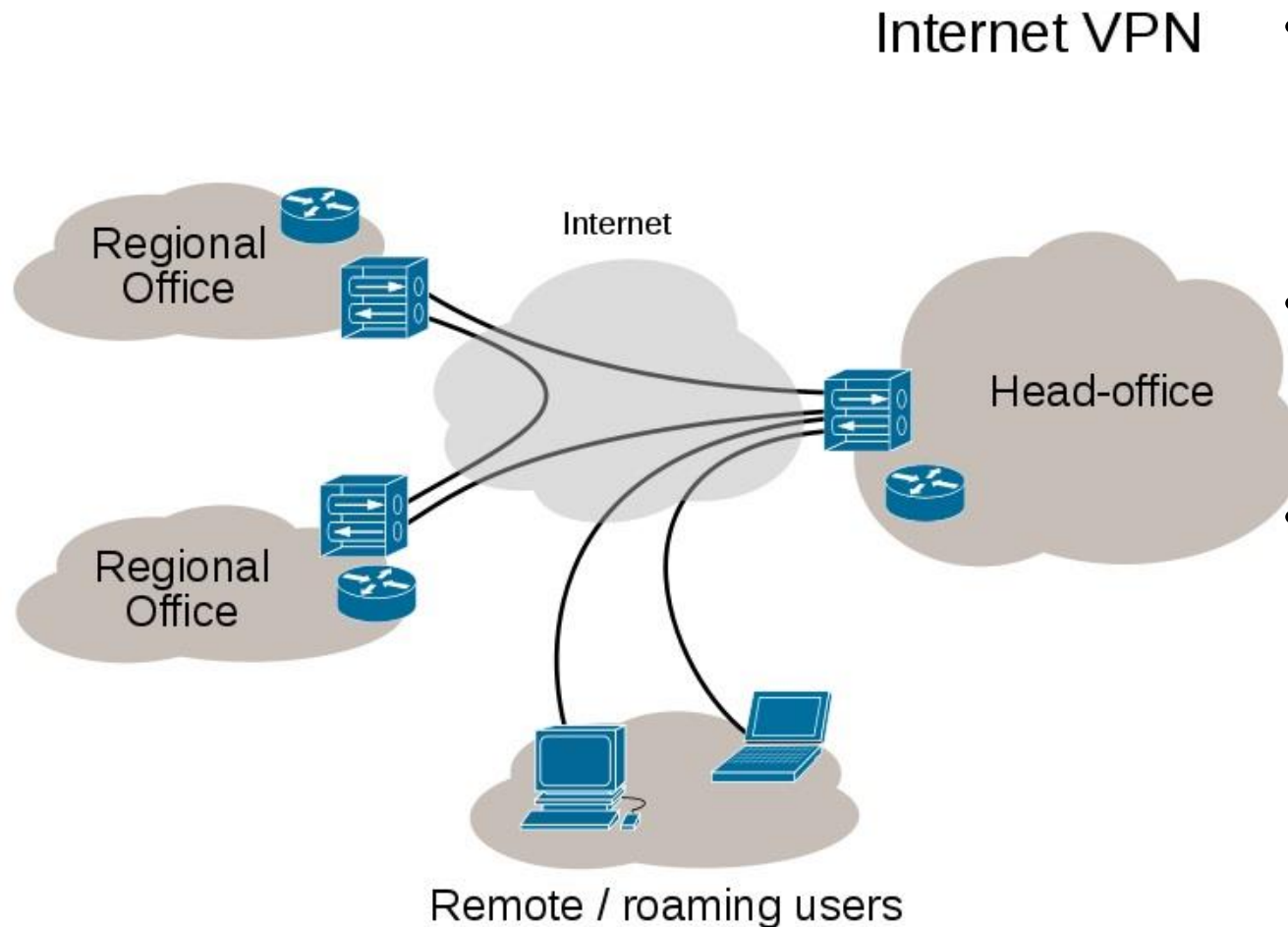


Decentralizált hálózatok

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



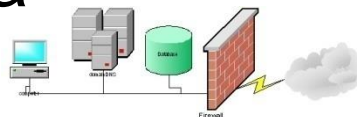
Virtuális magánhálózatok



- Adattovábbítás Interneten
 - Nem biztonságos
- Bérelt vonal (Leased line)
 - Drága
- Virtuális magánhálózatok (Virtual Private Network - VPN)
 - Titkosítás
 - Alagutazás (tunneling)

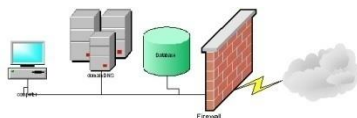
VPN előnyök

- Kapcsolatok különböző földrajzi helyek között – bérelt vonal nélkül
- Megnövelt biztonság
- Flexibilitás – távoli irodák-munkavállalók használhatják az intranetet
 - Interneten keresztül
 - De mintha közvetlenül csatlakoznának hozzá
- Idő- és pénzmegtakarítás
 - Nem kell utazni
- Megnövelt produktivitás távoli munkavállalók számára



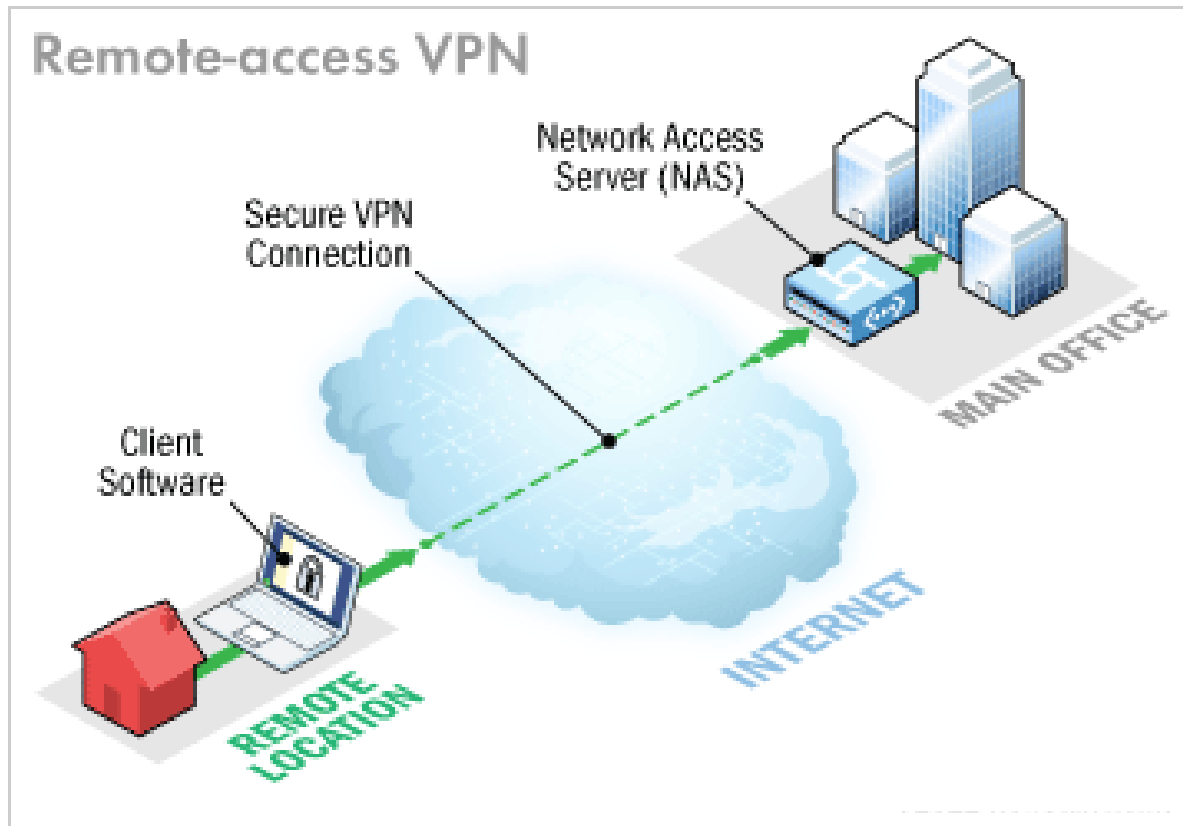
VPN szolgáltatások

- Biztonság
 - VPN adatvédelem (titkosítás) a nyilvános hálózaton
 - Nem lehet lehallgatni
- Megbízhatóság
 - Munkavállalók/távoli irodák bármikor kapcsolódhatnak a VPN-hez
 - VPN minden használó számára ugyanazon paramétereket biztosítja – még a maximális egyidejű kapcsolat esetén is
- Skálázhatóság

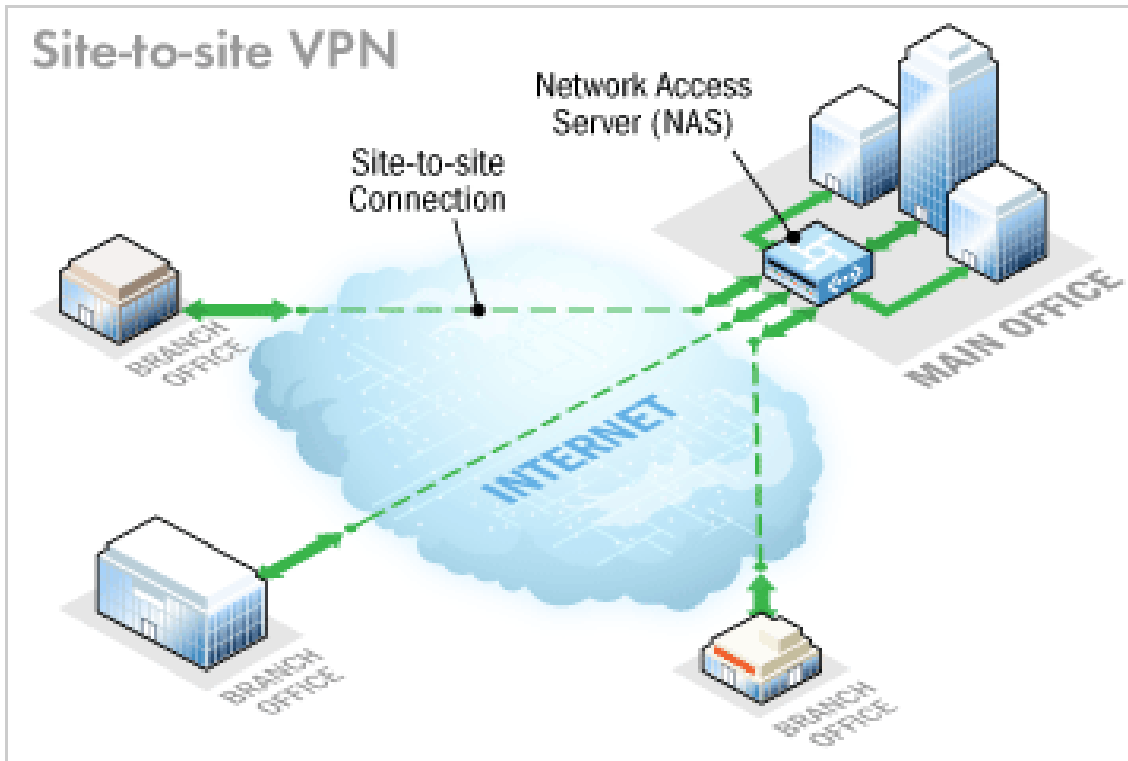


Remote-Access VPN

- Használókat köt be
 - Network Access Server (NAS) (Media Gateway, Remote-Access Server)
 - Kliens oldali szoftver



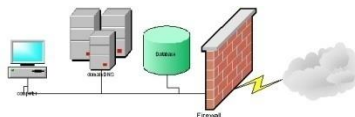
Site-to-site VPN



- Fix helyek között
 - Intranet-alapú
 - Extranet-alapú
- Nem kell kliens oldali szoftver
- VPN Koncentrátorok
 - (NAS)

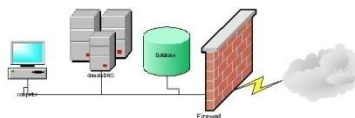
VPN koncentrátor

- Network Access Server
 - VPN (alagutazásra képes) router
 - Létrehozza és konfigurálja az alagutakat (logikai összeköttetések) – remote-access VPN
 - Vég-vég adattovábbítás
 - Alagutazás (tunneling)
 - A használói adatokat becsomagolja egy keretbe
 - Vezérlő fejléccet ad hozzá
 - Titkosítás
 - IPSec
 - Site-to-site
 - SSL
 - Remote access



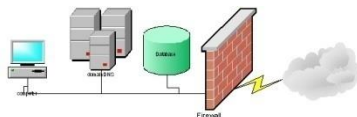
VPN koncentrátor

- Tűzfal
 - Milyen típusú forgalom mehet az Internetről a LAN-ra, milyen TCP és UDP portokon
- AAA Szerver
 - Ellenőrzi, ki vagy (authentication)
 - Meghatározza, mihez férhetsz hozzá a kapcsolaton keresztül (authorization)
 - Nyomon követi, mit csinálsz, míg be vagy jelentkezve (accounting)

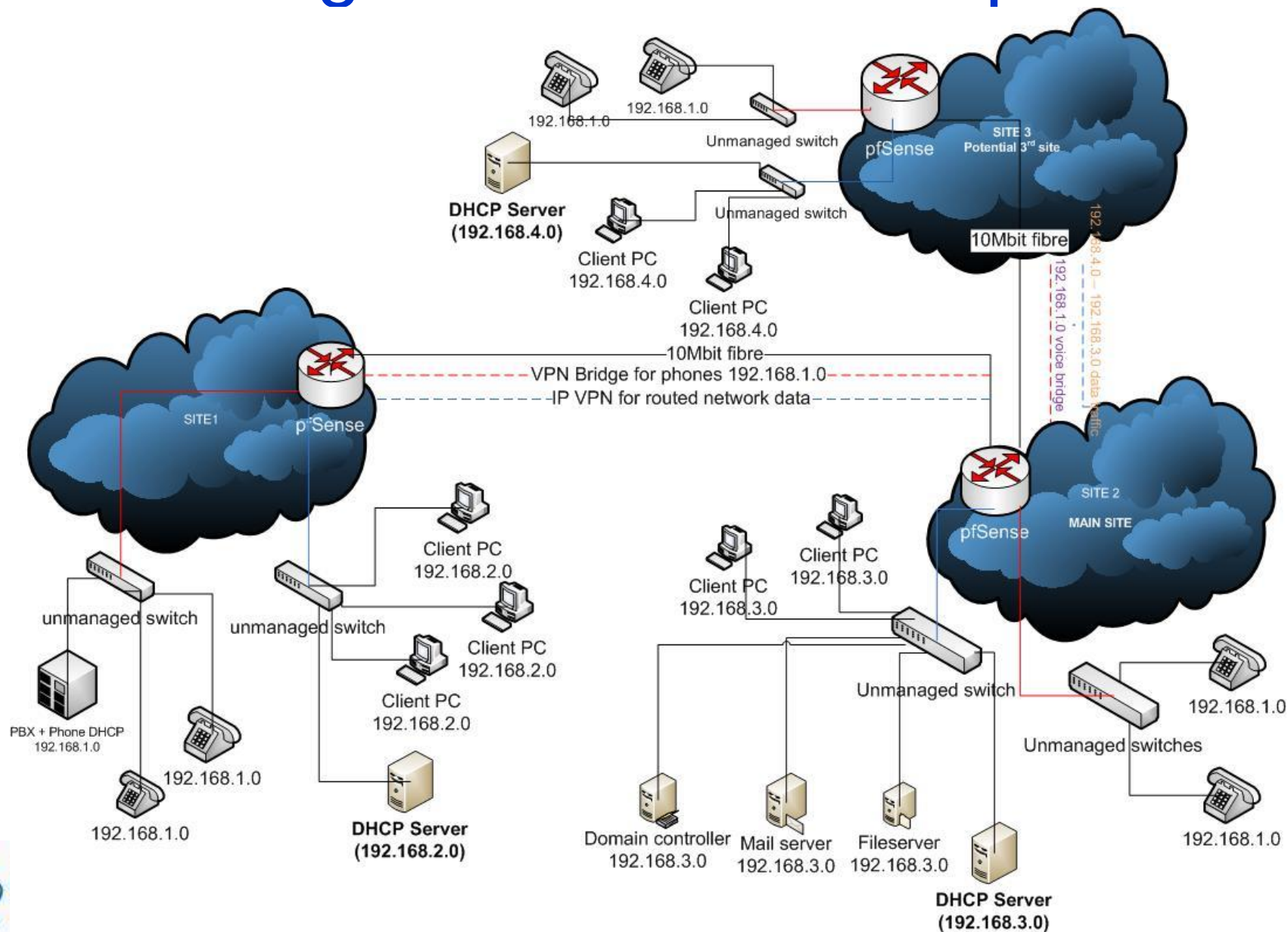


Fizikai és logikai hálózati térképek

- 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

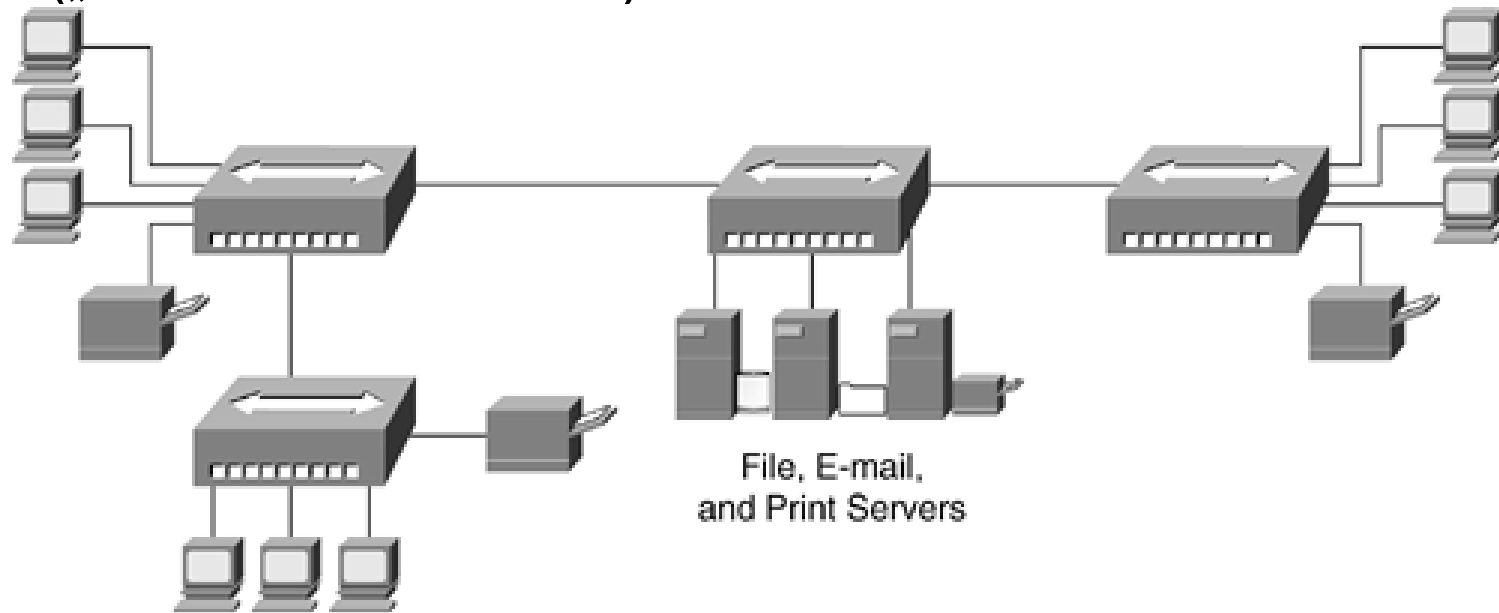


Logikai hálózati térkép



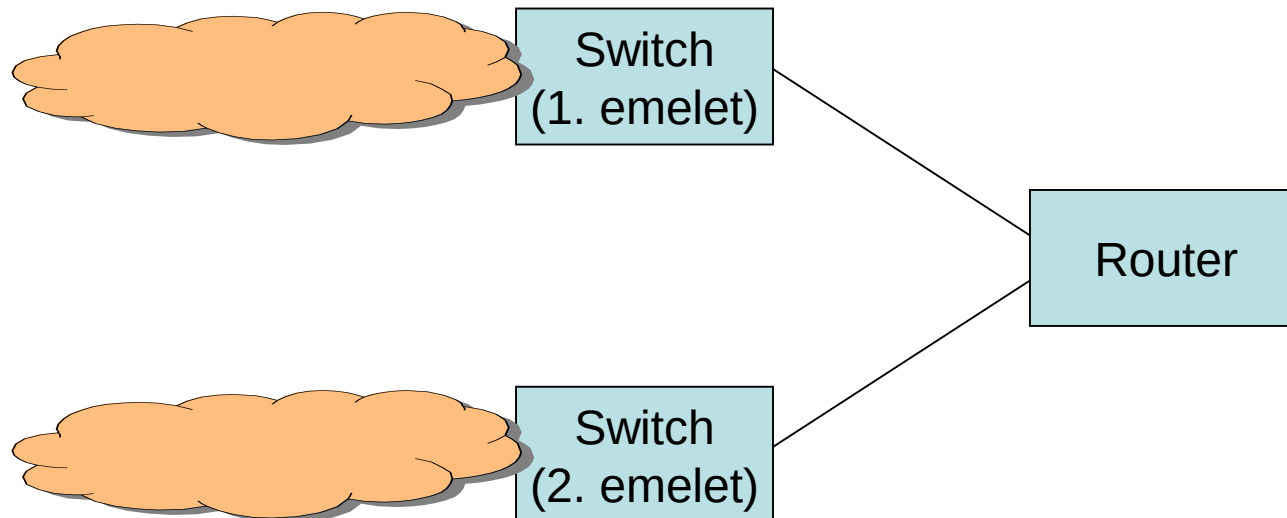
Tipikus logikai topológiák

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



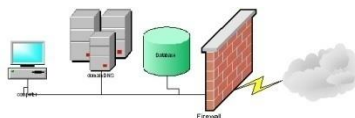
Tipikus logikai topológiák

- 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

