INFORMÁCIÓS RENDSZEREK ÜZEMELTETÉSE

BME VIK TMIT

MÉRNÖK-INFORMATIKUS ALAPKÉPZÉS

INFORMÁCIÓS RENDSZEREK ÜZEMELTETÉSE

ADAMIS GUSZTÁV – TMIT

IE 345

ADAMIS@TMIT.BME.HU

3. ÜZEMELTETÉSI FELADATOK ÉS A HÁLÓZATI ISMERETEK

I. rész

Az üzemeltetési feladatok és a hálózati ismeretek összefüggései

IT hálózati elemek, hálózatba illesztés

(IP címek, címosztályok,

DHCP, ARP, RARP, NAT(P), DNS)

II. rész

Hálózati topológiák, VPN, demarkációs pontok, hálózati térképek

I. RÉSZ

KORÁBBAN TANULTAK ÁTTEKINTÉSE

KORÁBBAN TANULTAK ÁTTEKINTÉSE

- Korábbi tárgyakban tanultak
  – amik az IRÜ-ben is fontosak

- Persze, mindannyian tudjátok
  – biztos???

ISMÉTLÉS

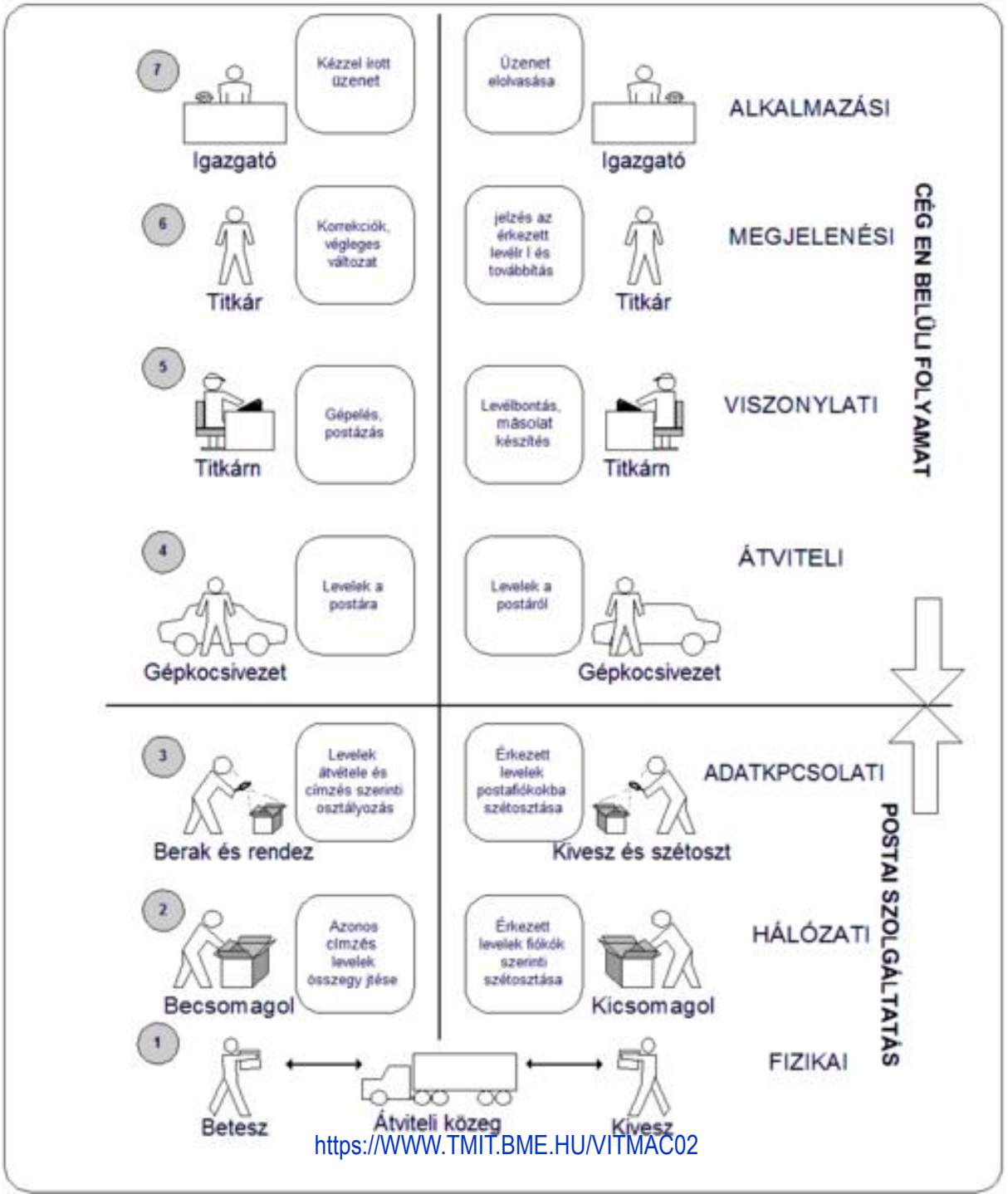
- Referencia modell, protokollok
- IP alapok
  - címek, címosztályok
  - DHCP
  - ARP/RARP
  - NA(P)T
  - DNS
  - ICMP

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


7
Kézzel írott üzenet
Igazgató
Üzenet elolvasása
Igazgató
ALKALMAZÁSI
6
Korrekciók, végleges változat
Titkár
jelzés az érkezett levélr l és továbbítás
Titkár
MEGJELENÉSI
5
Gépelés, postázás
Titkárn
Levélbontás, másolat készítés
Titkárn
VISZONYLATI
4
Levelek a postára
Gépkocsivezet
Levelek a postáról
Gépkocsivezet
ÁTVITELI
3
Levelek átvétele és címzés szerinti osztályozás
Berak és rendez
Érkezett levelek postafiókokba szétosztása
Kivesz és szétoszt
ADATKPCSOLATI
2
Azonos címzés levelek összegy jtése
Becsomagol
Érkezett levelek fiókok szerinti szétosztása
Kicsomagol
HÁLÓZATI
1
Betesz
Átviteli közeg
Kivesz
FIZIKAI
CÉG EN BELÜLI FOLYAMAT
POSTAI SZOLGÁLTATÁS

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)

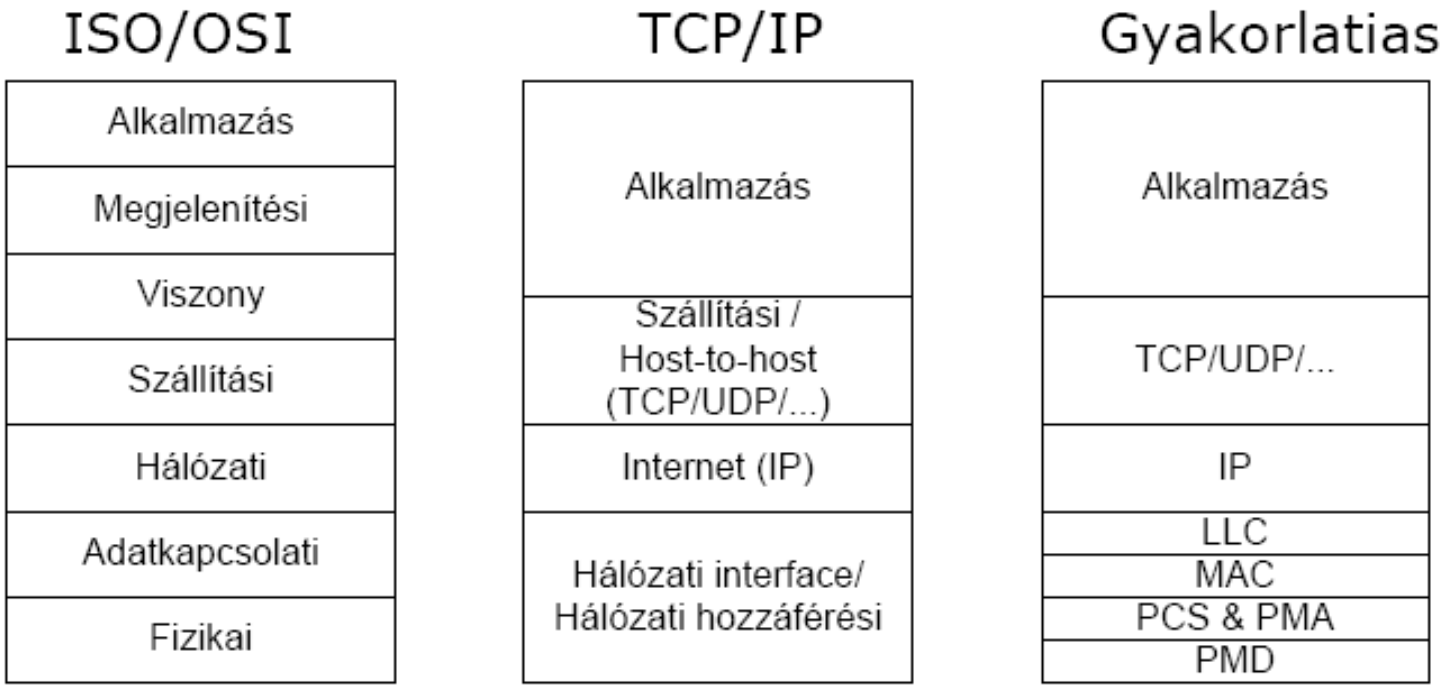
RÉTEG KARAKTERISZTIKÁK

- 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)

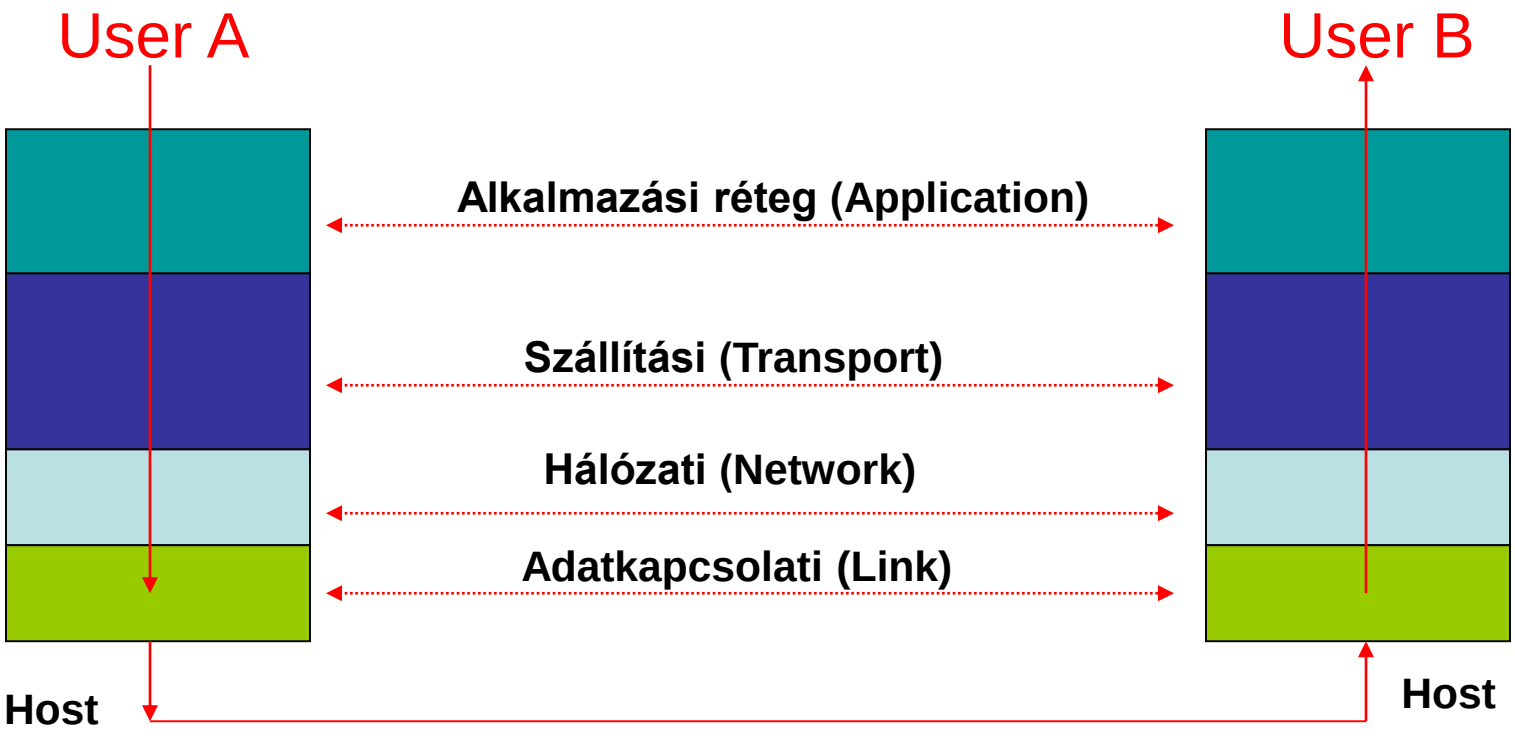
OSI – IP ARCHITEKTÚRA



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

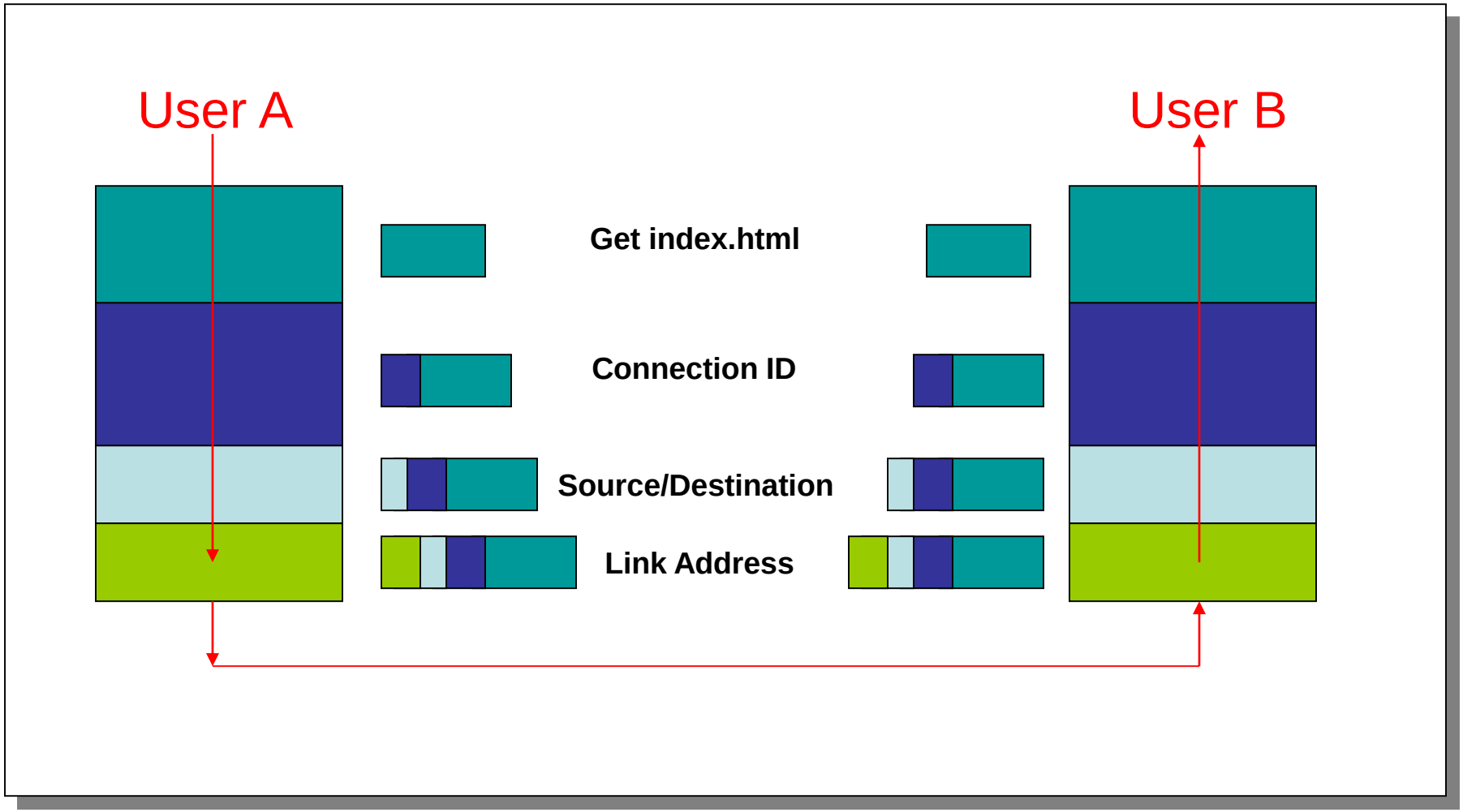
MAC: Medium Access Control
PCS: Physical Coding Sublayer
PMA: Physical Medium Attachment
PMD: Physical Medium Dependent

RÉTEGEZÉS



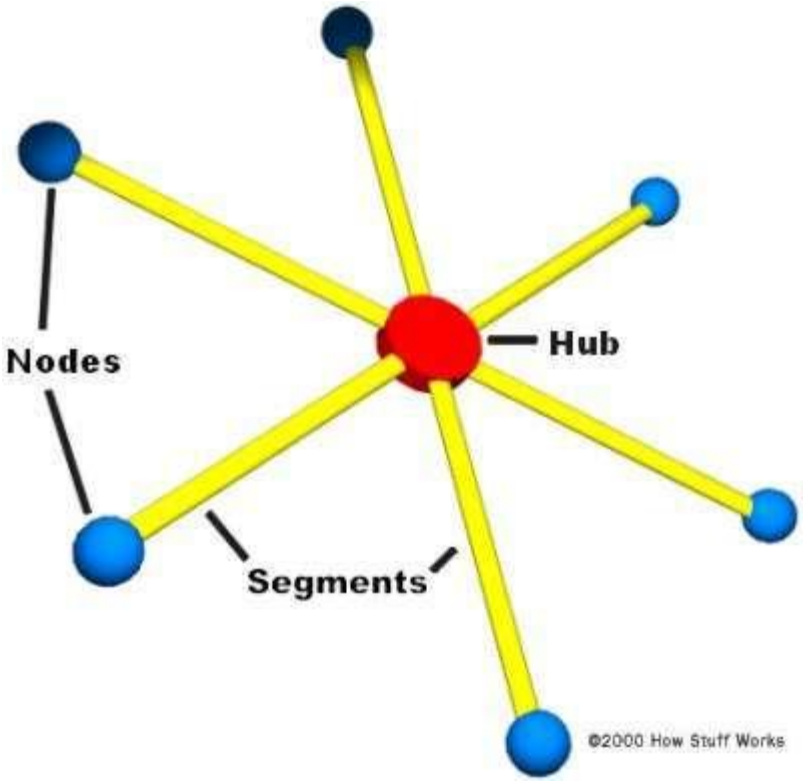
Rétegezés: bonyolult rendszerek egyszerűsítése céljából

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
    - 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???

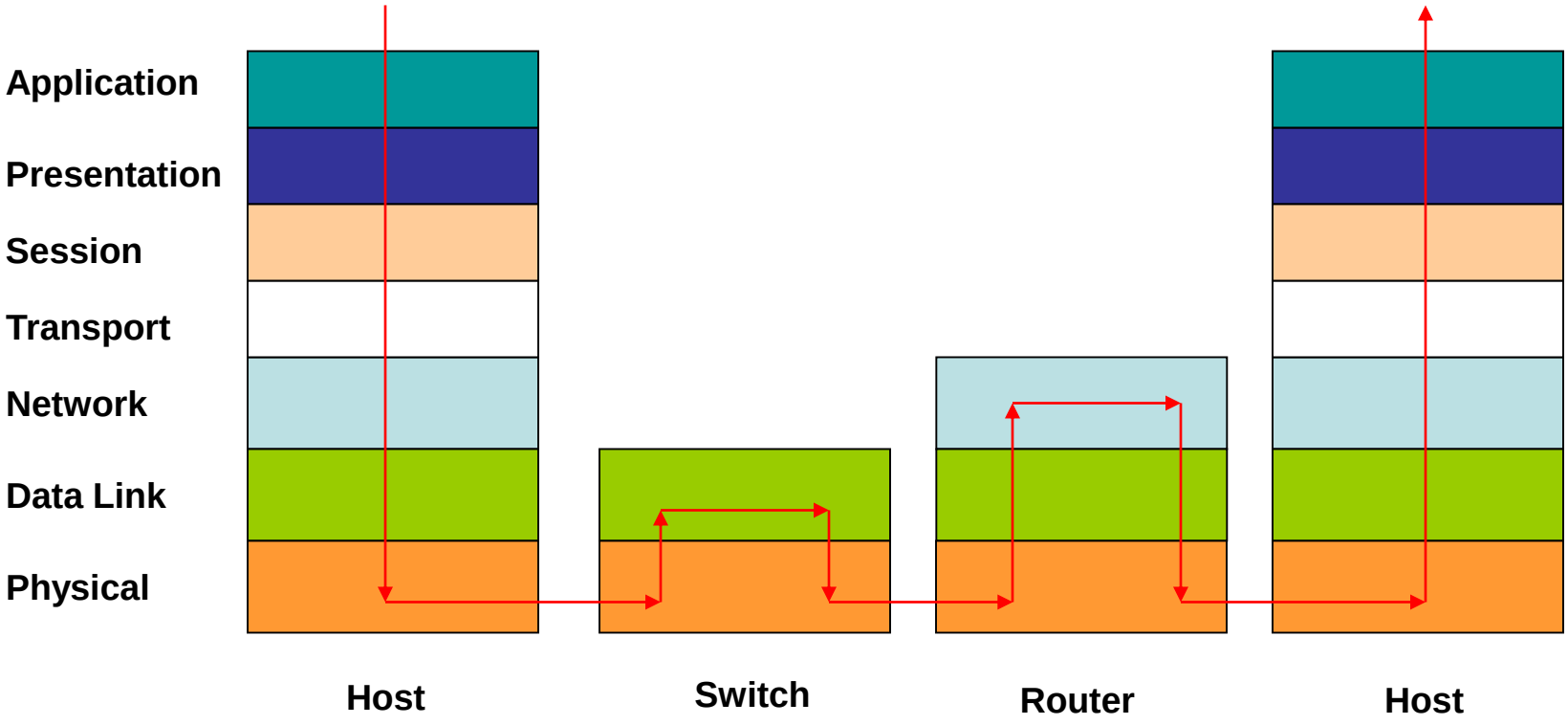
HUB, BRIDGE, ROUTER, SWITCH

- 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
      - VPN koncentrátor (Network Access Server)
    - 7. (alkalmazási) réteg
      - URL alapú terhelésmegosztás
      - alkalmazás szintű tranzakció kezelés

HÁLÓZATI ESZKÖZÖK HELYE A RÉTEGEKBEN



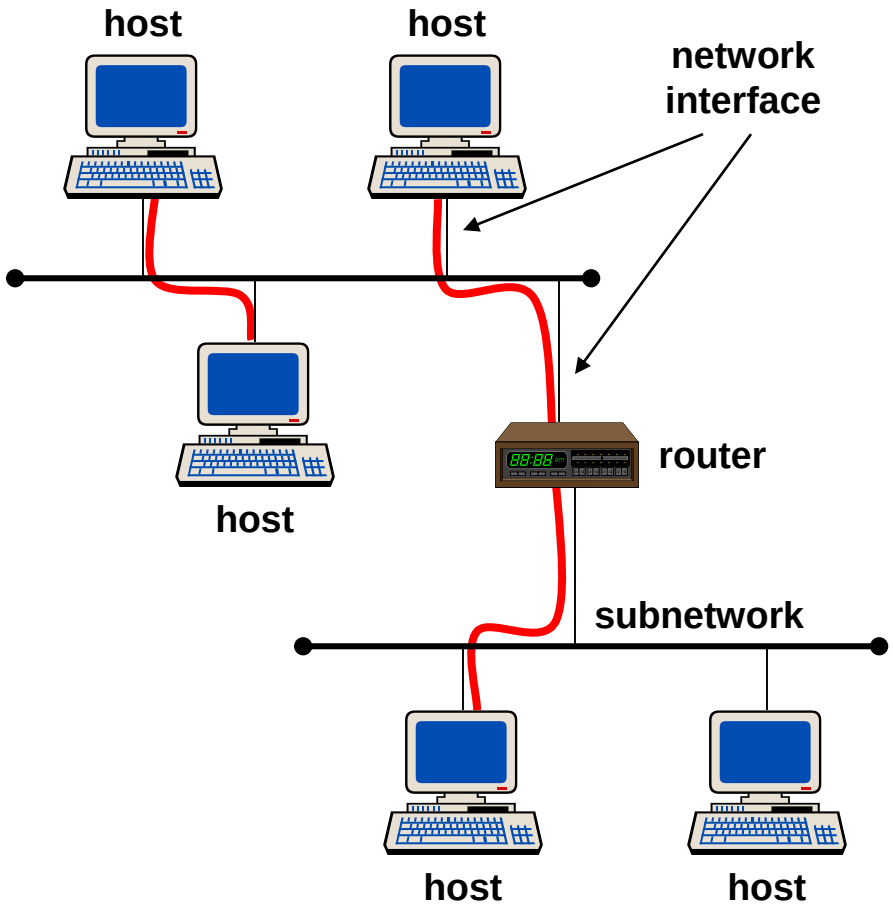
RÉTEGEZÉS

- 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

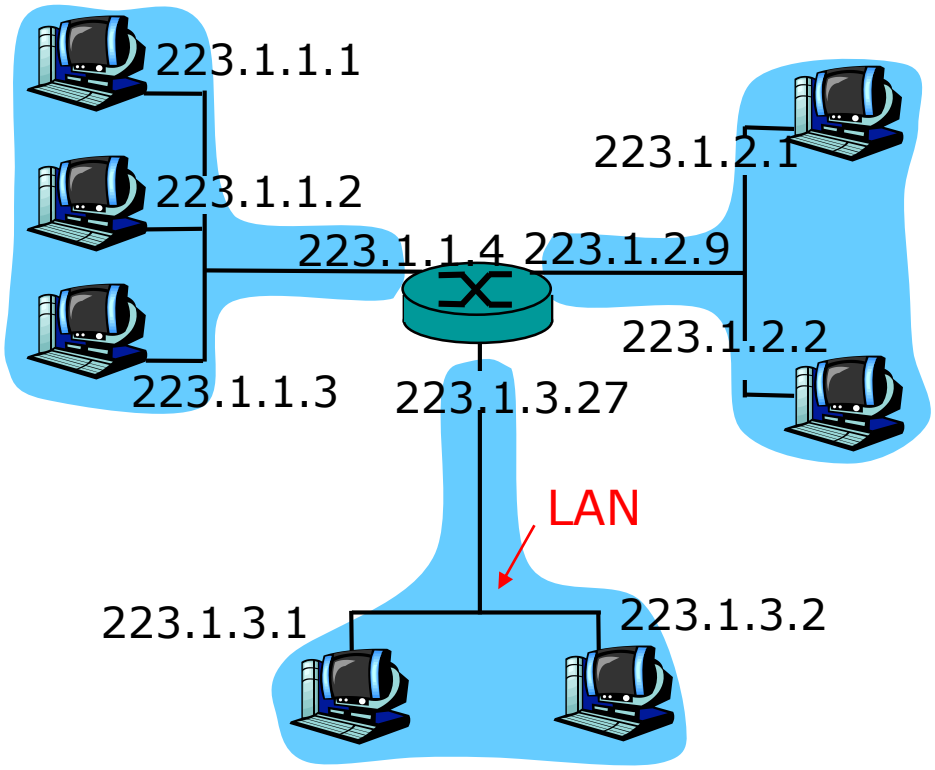
IP HÁLÓZATI ELEMEK



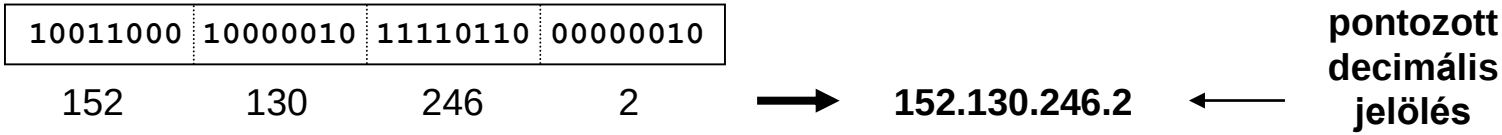
- **Hoszt (host)**: kommunikációs végpont
- **Alhálózat (subnetwork)**: fizikai hálózat, a hozzákapcsolt csomópontok közvetlenül tudnak kommunikálni
- **Útválasztó (router)**: közvetítő a külön alhálózaton található, kommunikáló hosztok között
- **Interfész (interface)**: csomópont kapcsolódási pontja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

IP CÍMEK

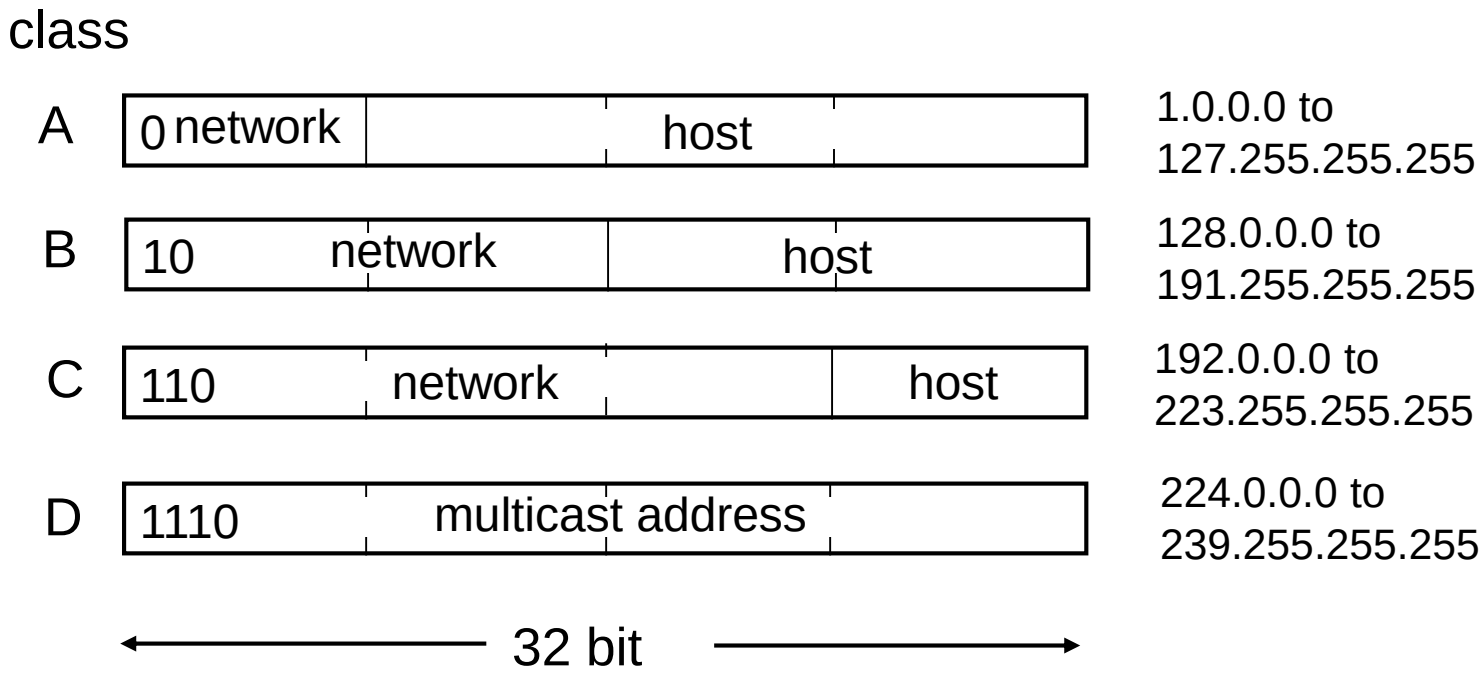
- IP cím:
  - hálózati cím (high order bits)
  - host cím (low order bits)
- *Hálózat?* (IP szempontból)
  - eszköz illesztő u.azzal a hálózati címrésszel
  - útválasztó nélküli összeköttetés ezen eszközök között



24 bites hálózati címek



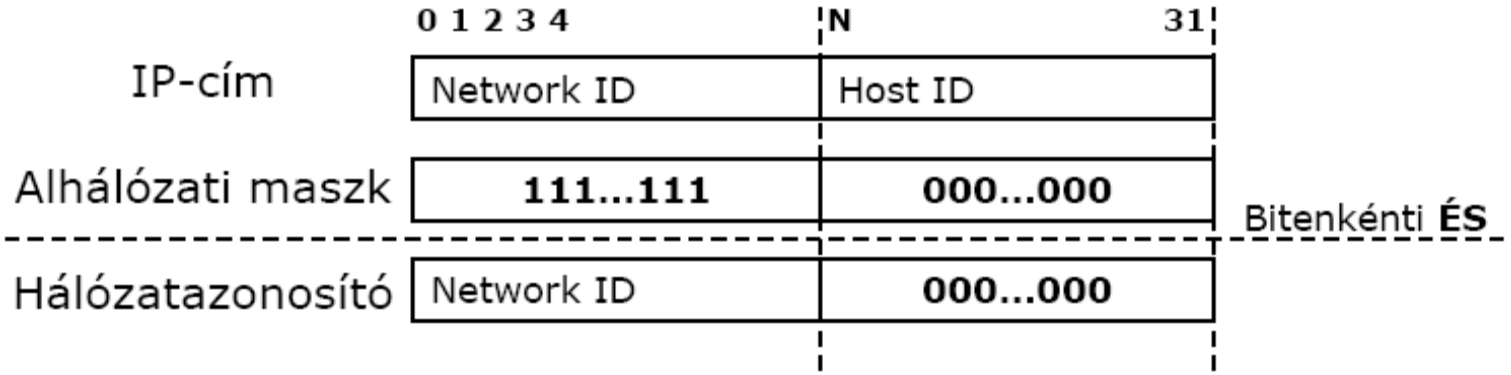
IP CÍMOSZTÁLYOK



- 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



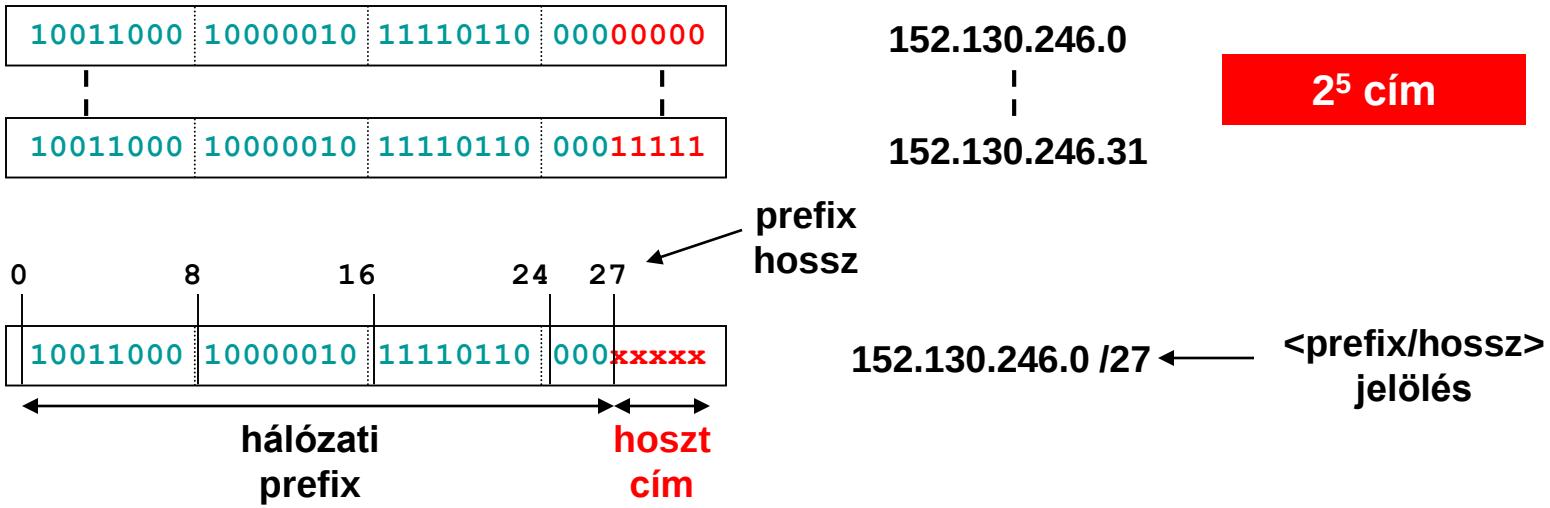
Alhálózati maszk (Netmask)

- 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



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 -> 32-28=4 bit host rész
  - 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

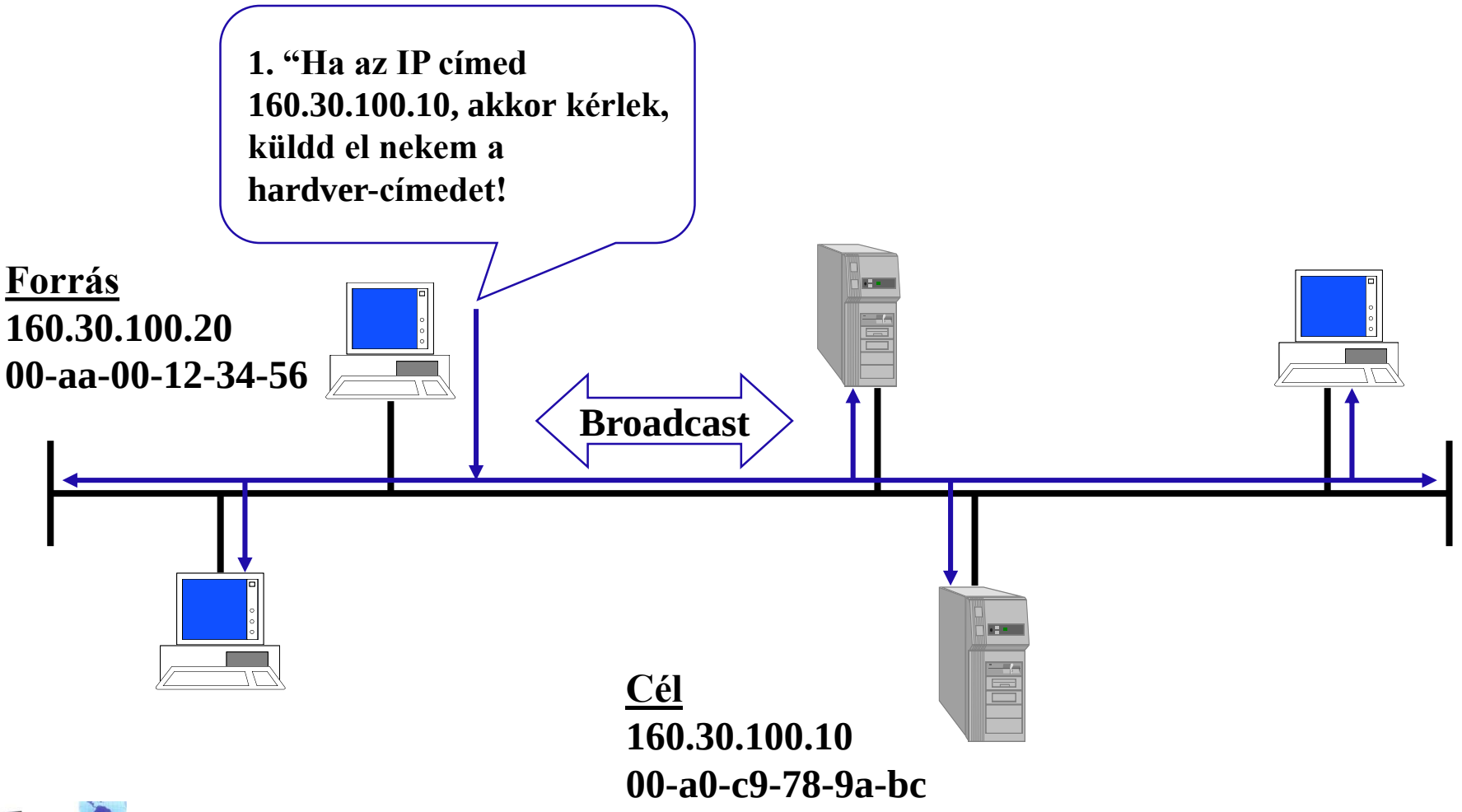
MAC cím

- 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

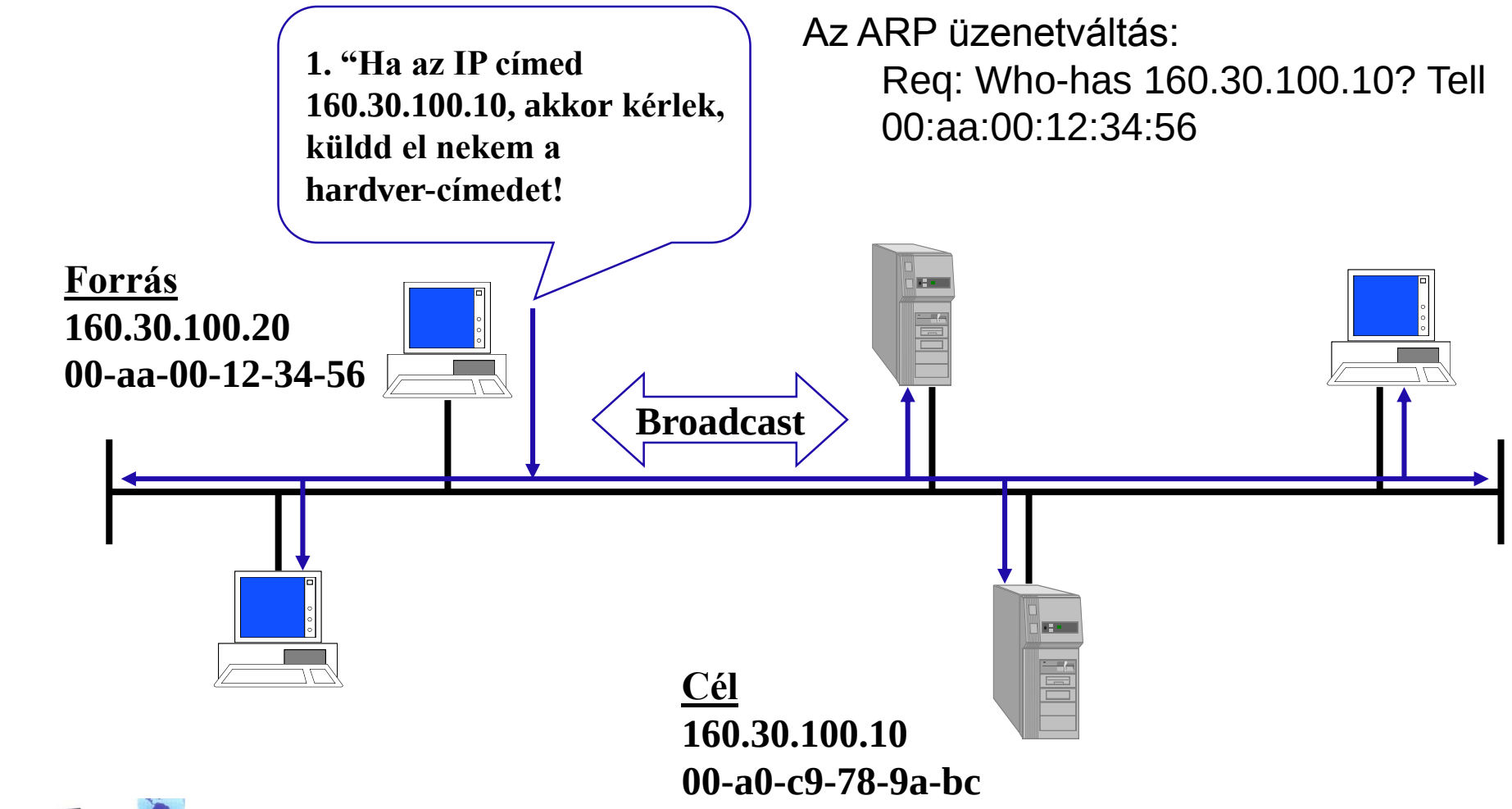
CÍMFELOLDÁSI PROTOKOLL
(ARP – *ADDRESS RESOLUTION PROTOCOL*)

- 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)

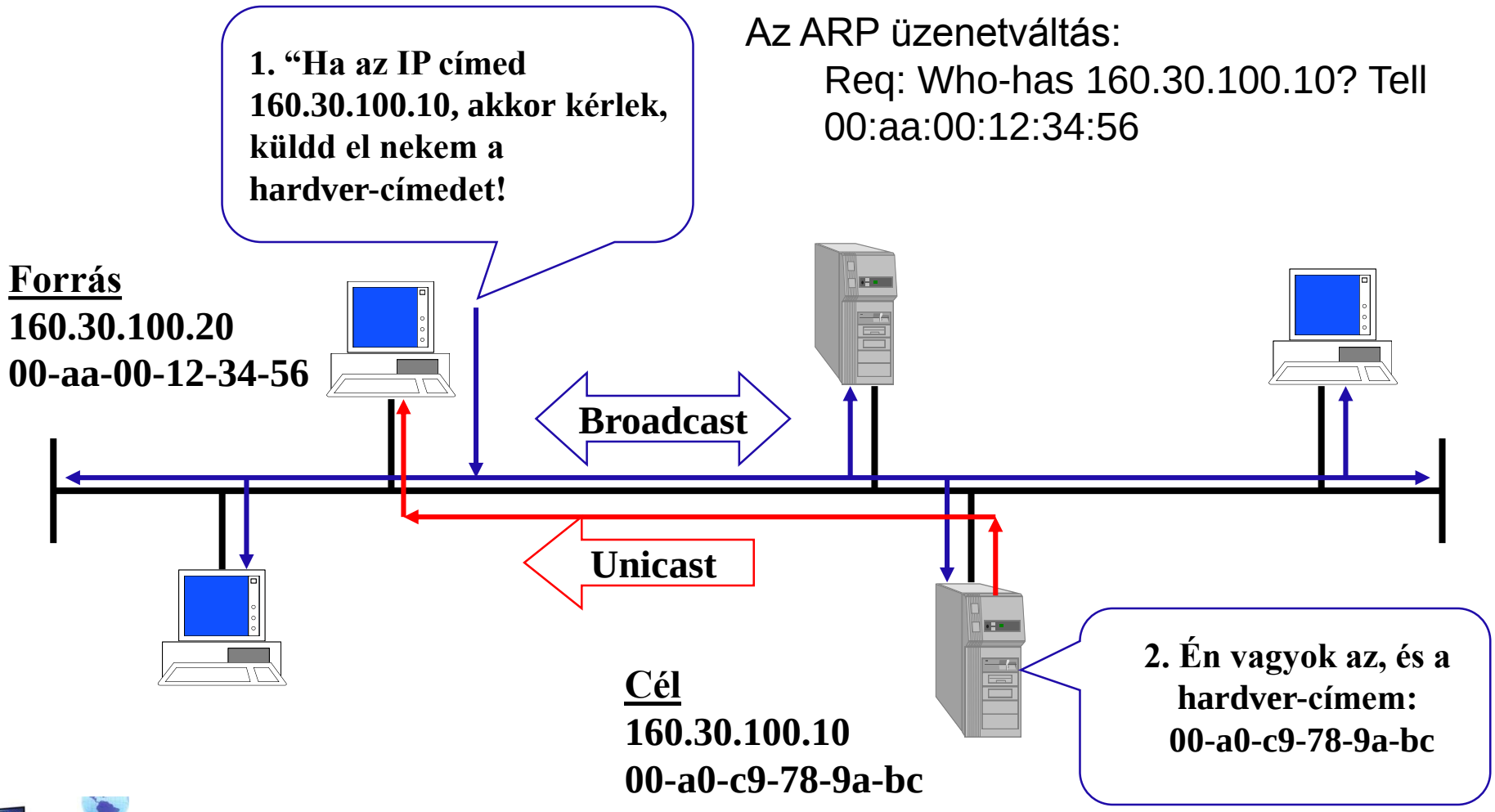
Címfeloldási Protokoll (ARP)



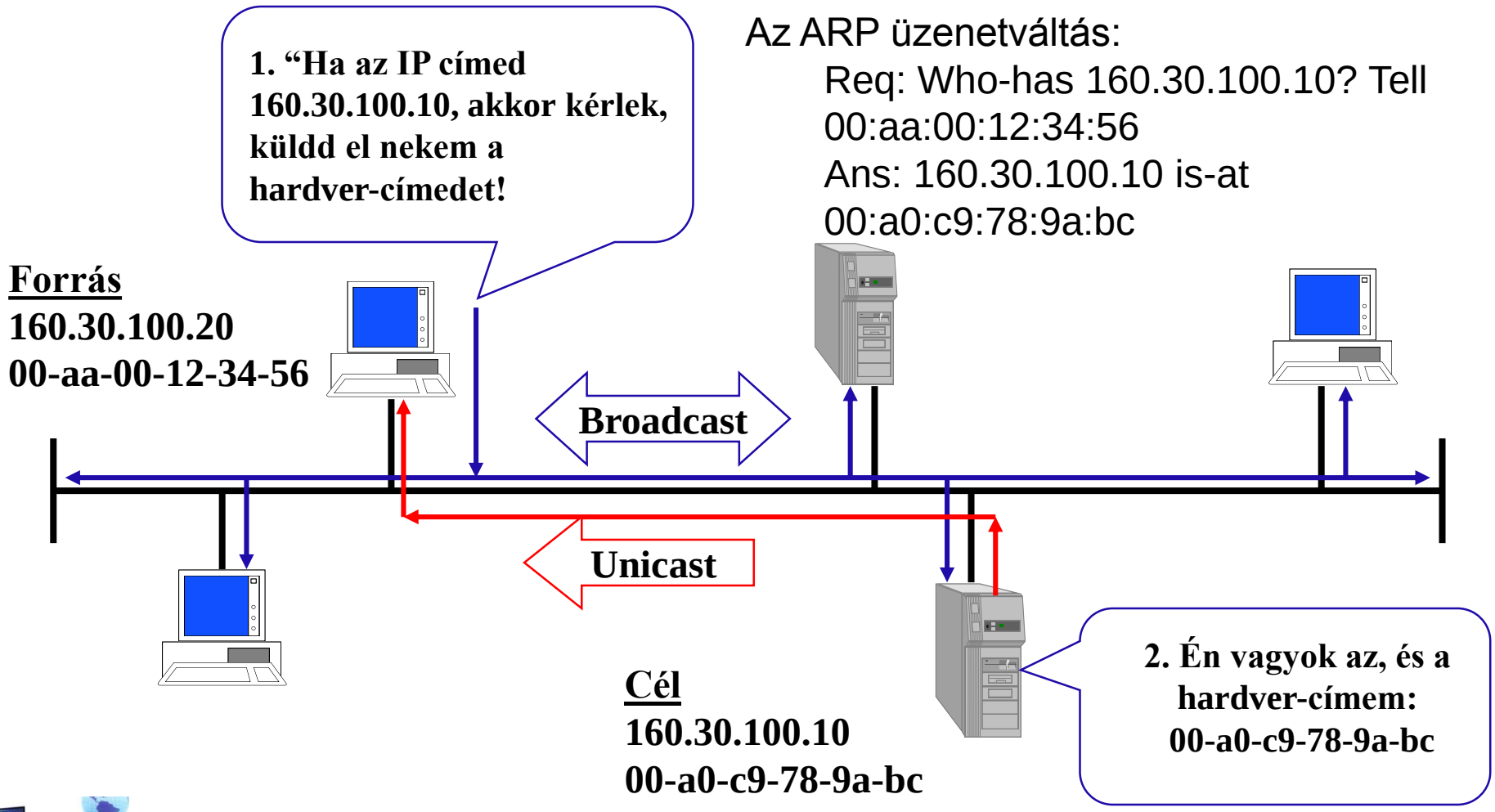
Címfeloldási Protokoll (ARP)



Címfeloldási Protokoll (ARP)



Címfeloldási Protokoll (ARP)

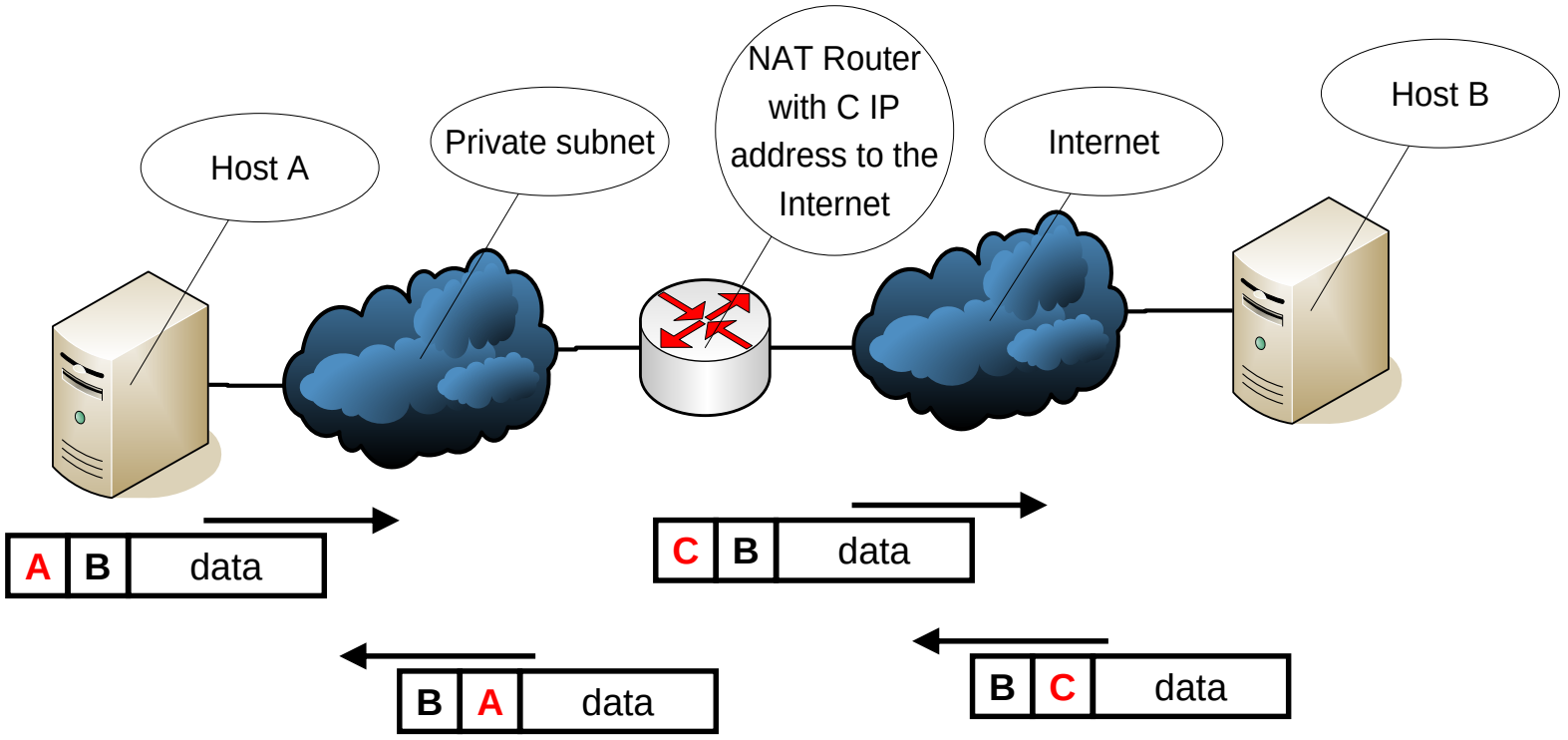


Fordított címfeloldási protokoll (RARP – Reverse Address Resolution Protocol)

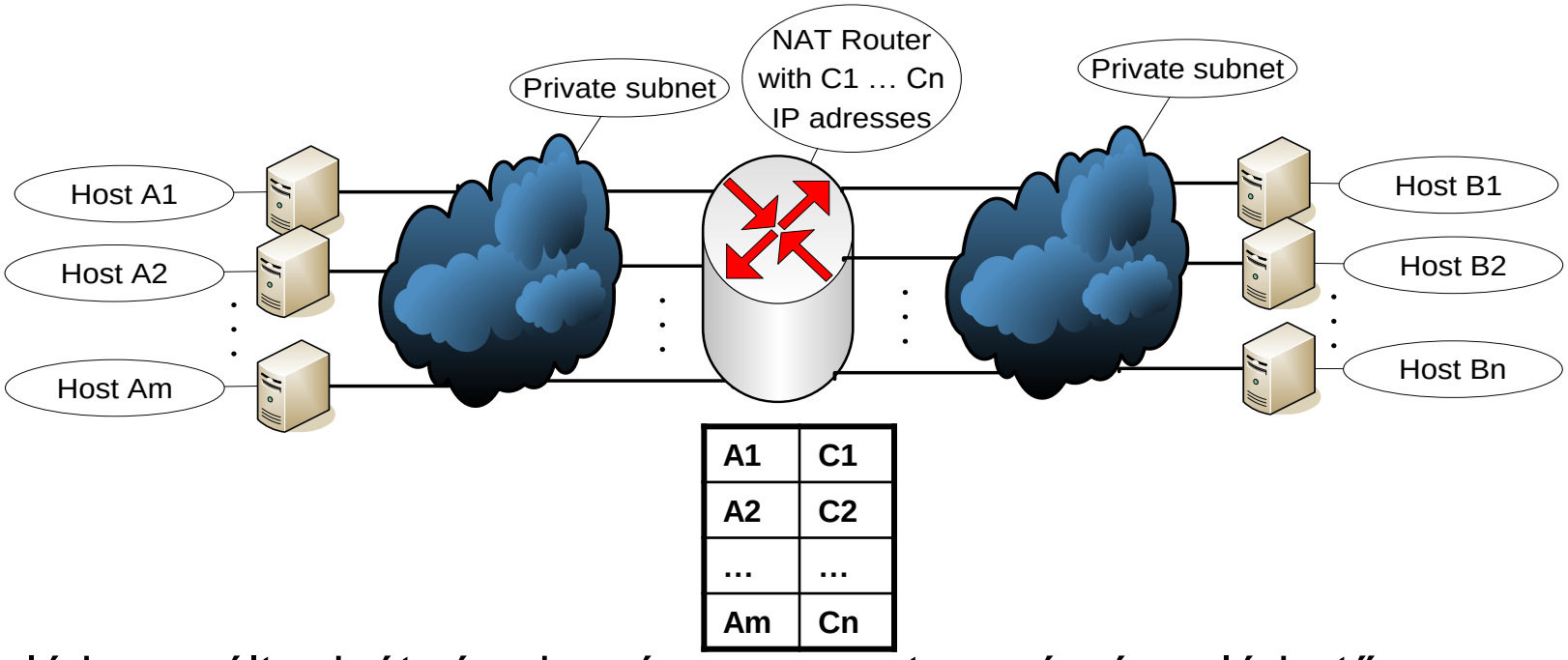
- A RARP hardver-címhez rendel IP címet
- A RARP lehetőséget teremt egy újonnan indult gépnek, hogy üzenetszórással kihirdesse Ethernet címét egy kérés formájában
  - „My 48-bit Ethernet address is 00-a0-c9-78-9a-bc.
    Does anyone know my IP address?”
- A RARP szerver észleli a kérést, és visszaküldi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



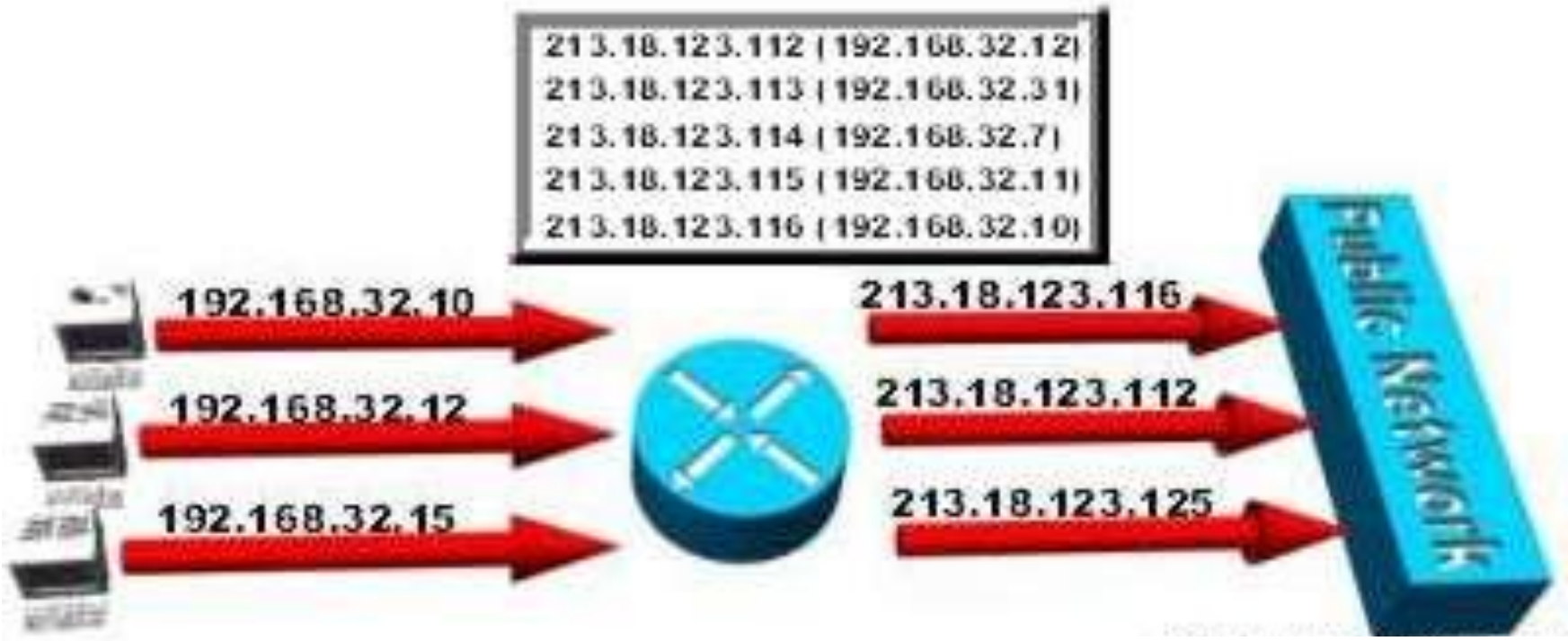
NAT – TÖBB HOSZTTAL (M=N)



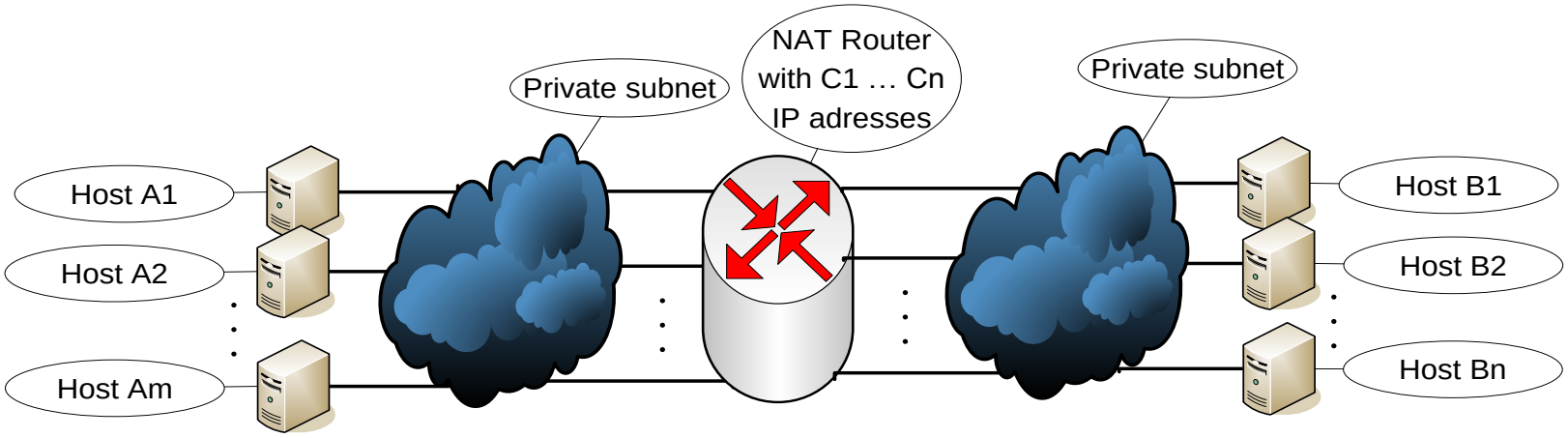
- Kifelé használt privát címek száma = a router számára elérhető publikus IP címek száma
- Hozzárendelés
  - statikus
  - dinamikus
    - biztonság növelésére

STATIKUS NAT PÉLDA

DINAMIKUS NAT PÉLDA



NAT – TÖBB HOSZTTAL (M>N)

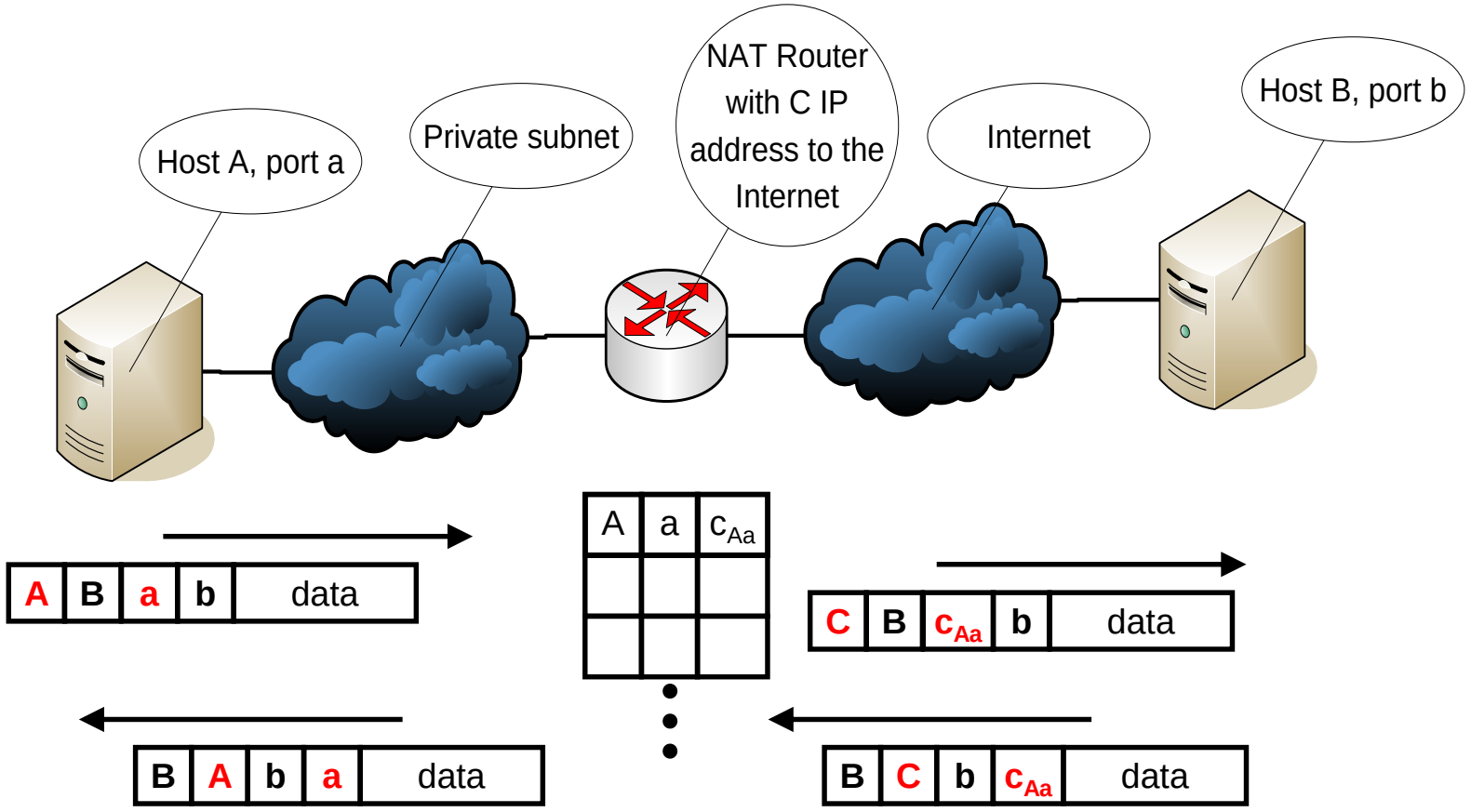


A1	C1
A2	C2
…	…
Am	Cn

- 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

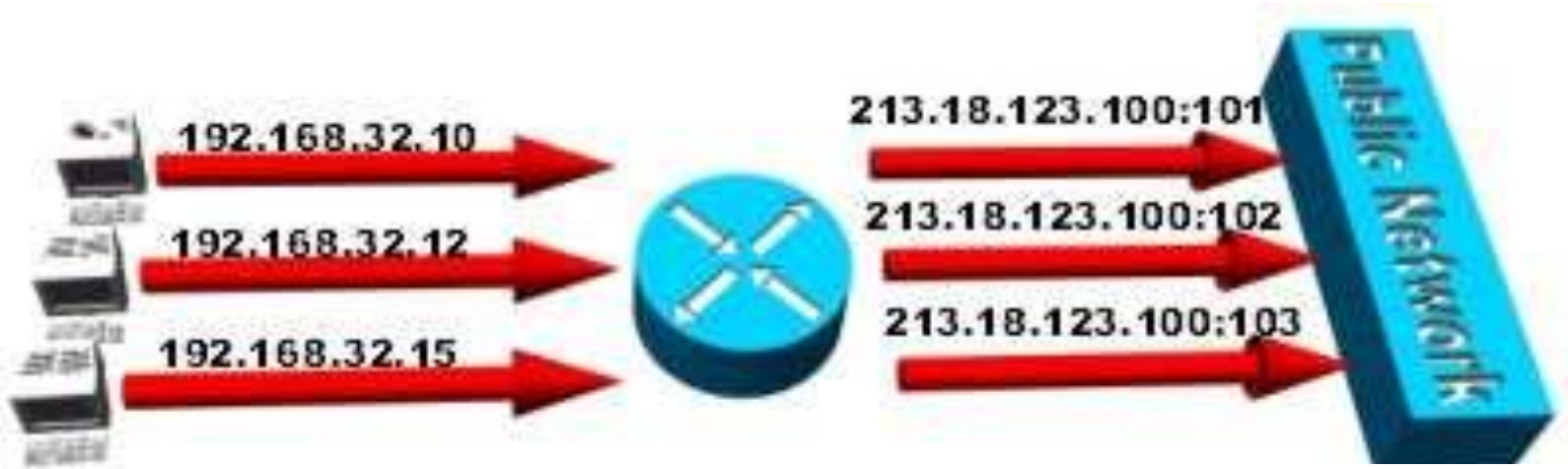
- Network Address Port Translation (NAPT)



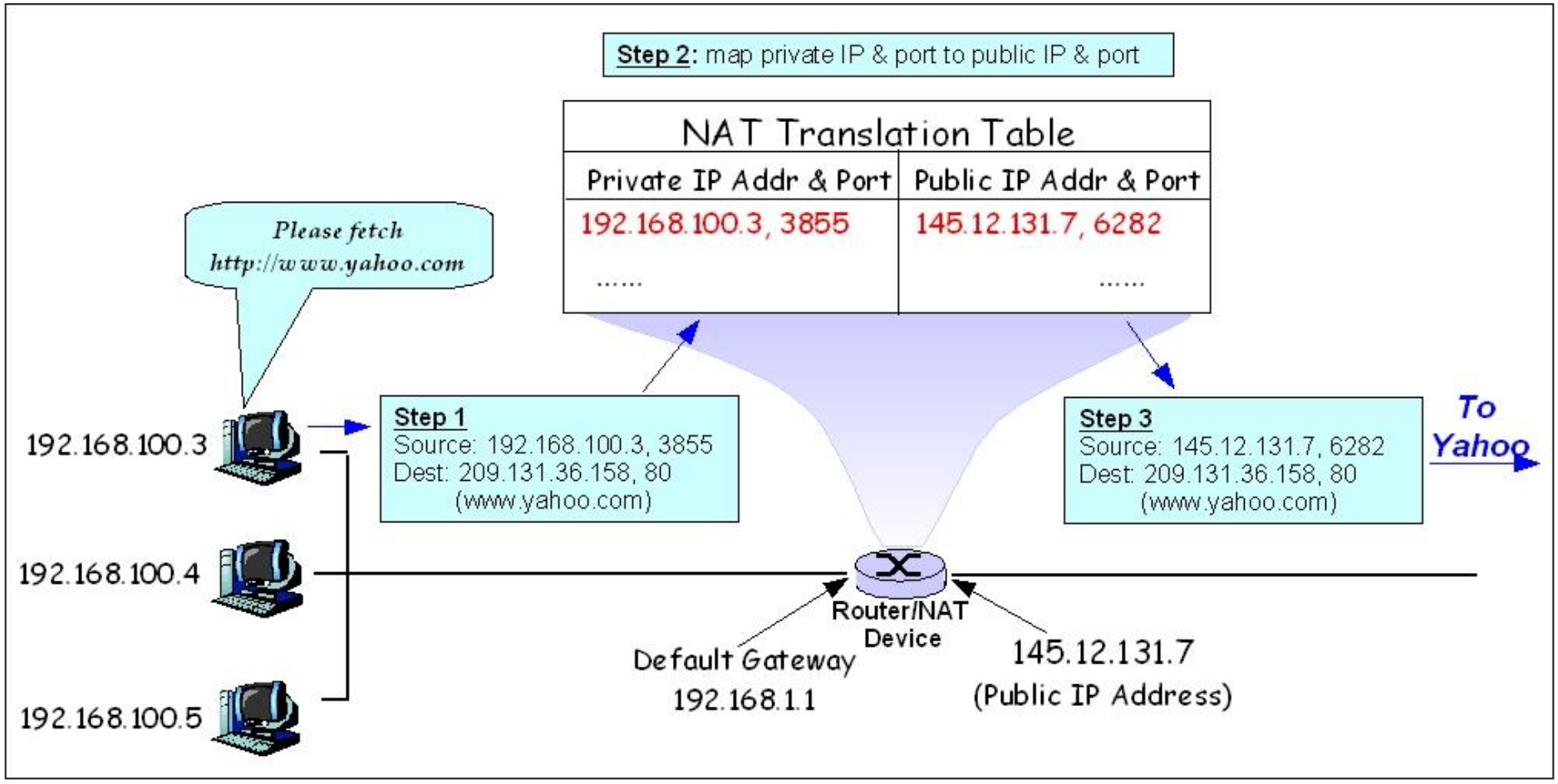
NAPT PÉLDA

Táblázat:

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

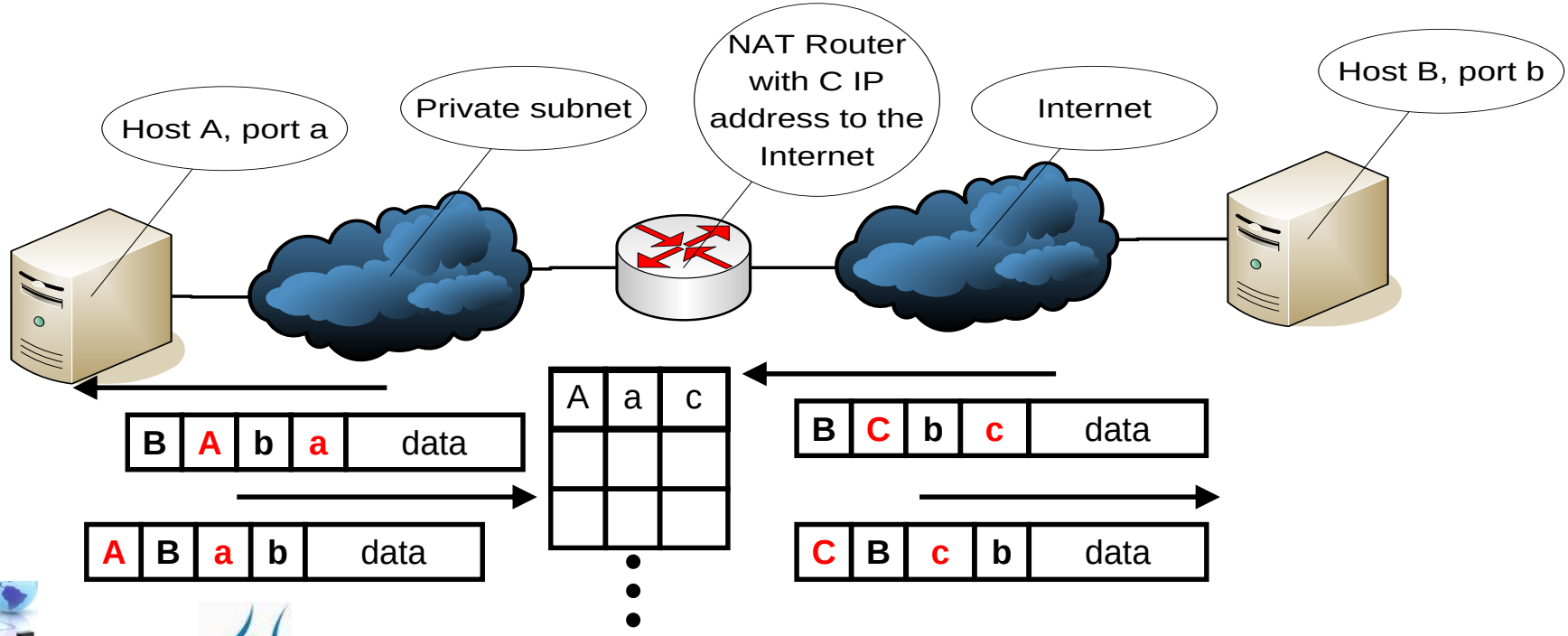


NAPT PÉLDA


Step 2: map private IP & port to public IP & port
NAT Translation Table
Private IP Addr & Port
Public IP Addr & Port
192.168.100.3, 3855
145.12.131.7, 6282
.....
.....
Please fetch
http://www.yahoo.com
192.168.100.3
192.168.100.4
192.168.100.5
Step 1
Source: 192.168.100.3, 3855
Dest: 209.131.36.158, 80
(www.yahoo.com)
Step 3
Source: 145.12.131.7, 6282
Dest: 209.131.36.158, 80
(www.yahoo.com)
To Yahoo
Router/NAT Device
Default Gateway
192.168.1.1
145.12.131.7
(Public IP Address)

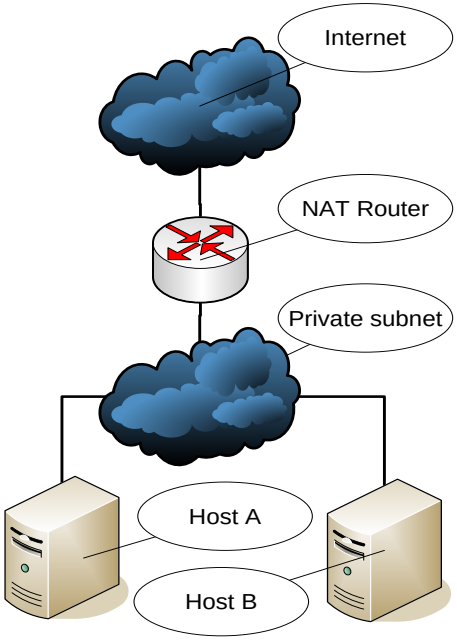
NAPT – VIRTUÁLIS SZERVER

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



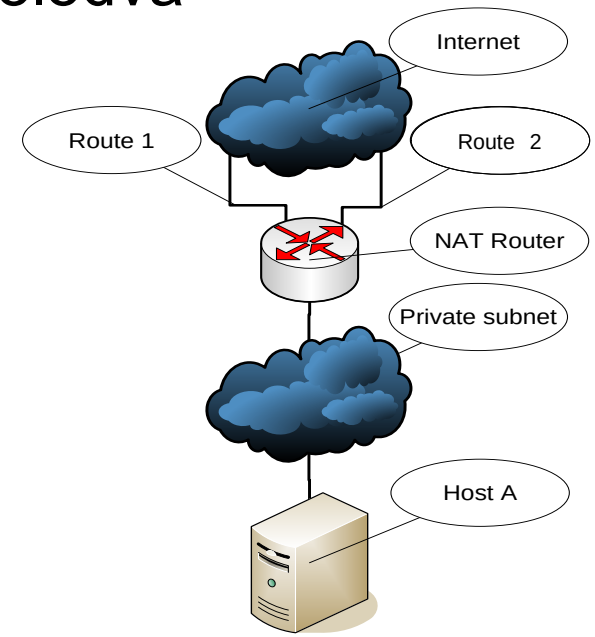
NA(P)T – OPTIMALIZÁCIÓK

- Több belső szerver
  - Terhelésmegosztás
  - Belső struktúra módosítható



NA(P)T – OPTIMALIZÁCIÓK

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

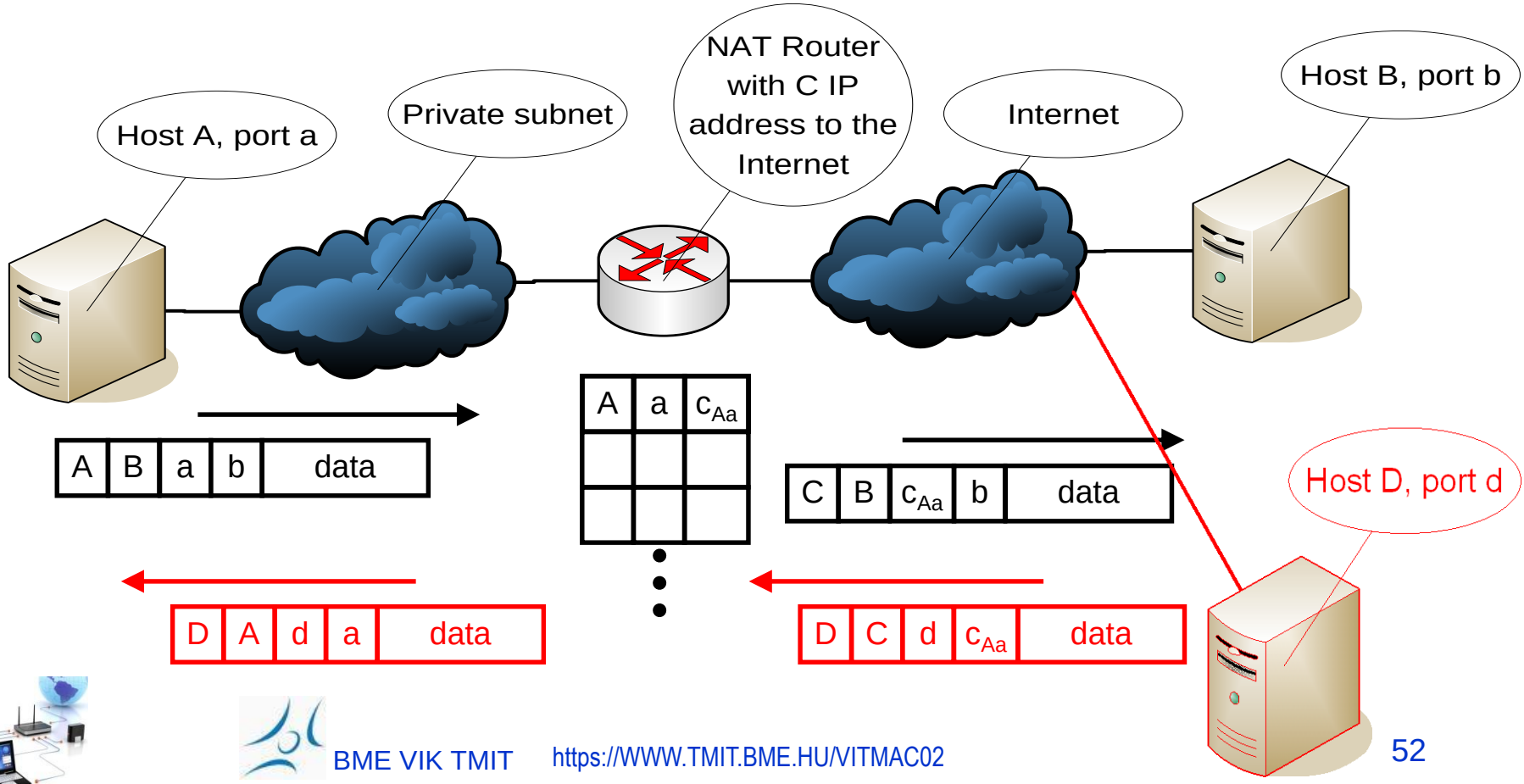


NA(P)T – TŰZFAL

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

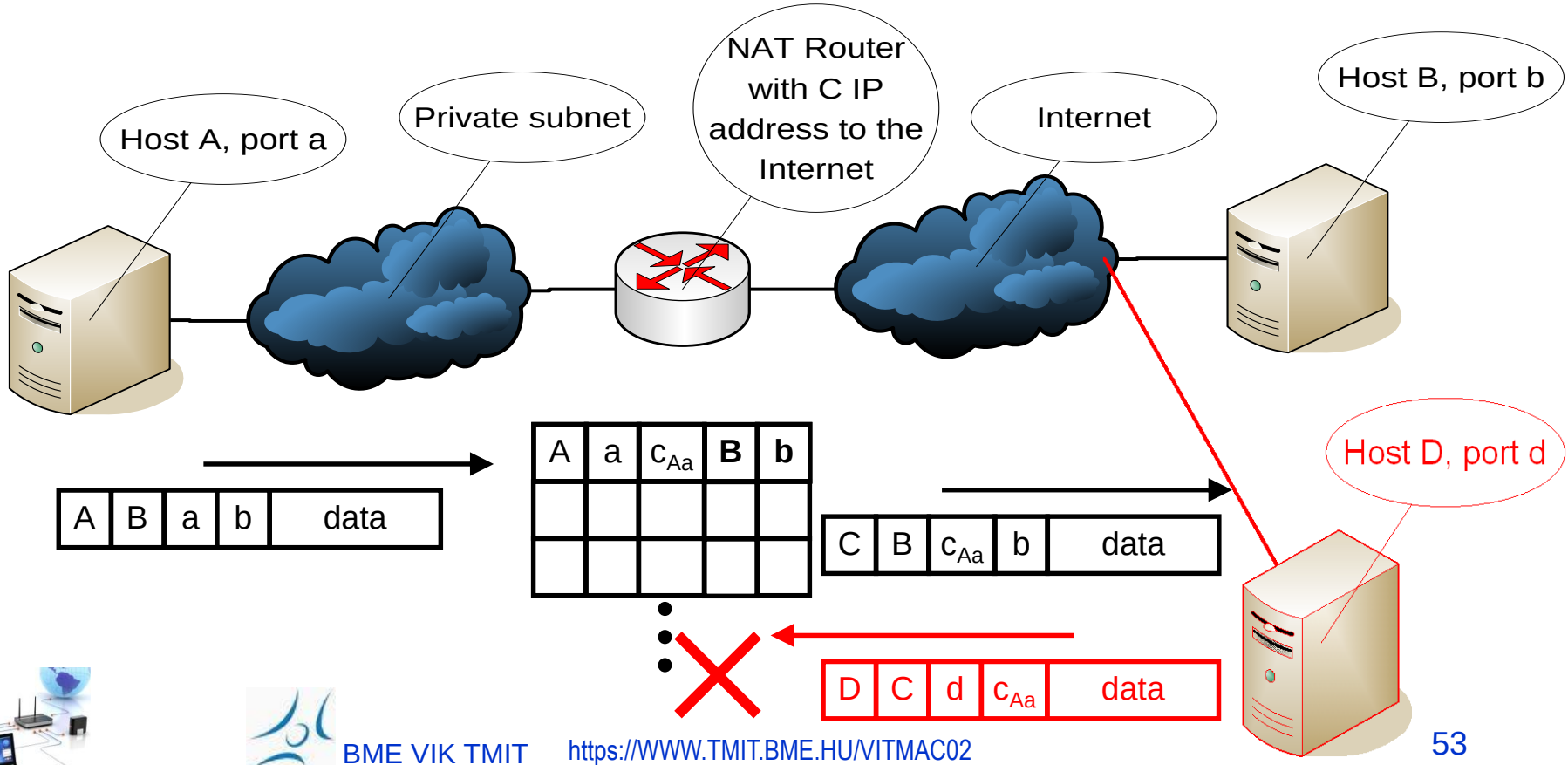
NAPT – BIZTONSÁG

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



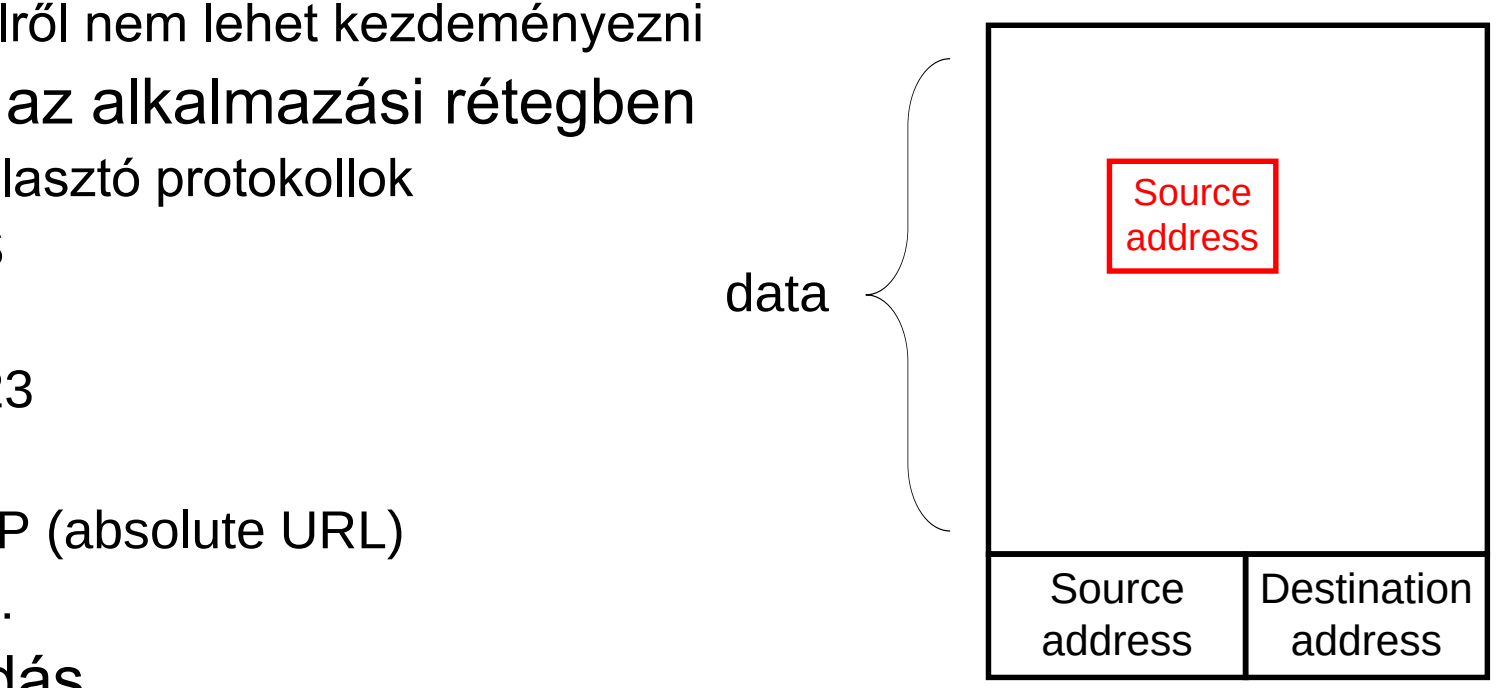
NAPT – BIZTONSÁGI KIEGÉSZÍTÉS

- Távoli IP címmel kiegészítve
- Egyszerű tűzfal megoldás

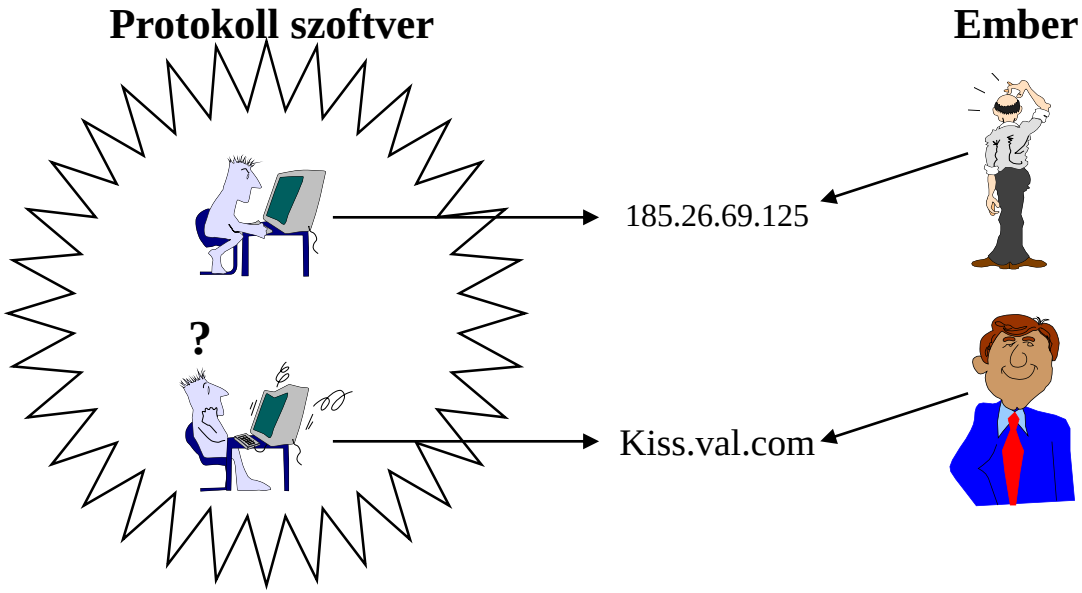


NA(P)T PROBLÉMÁK

- 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

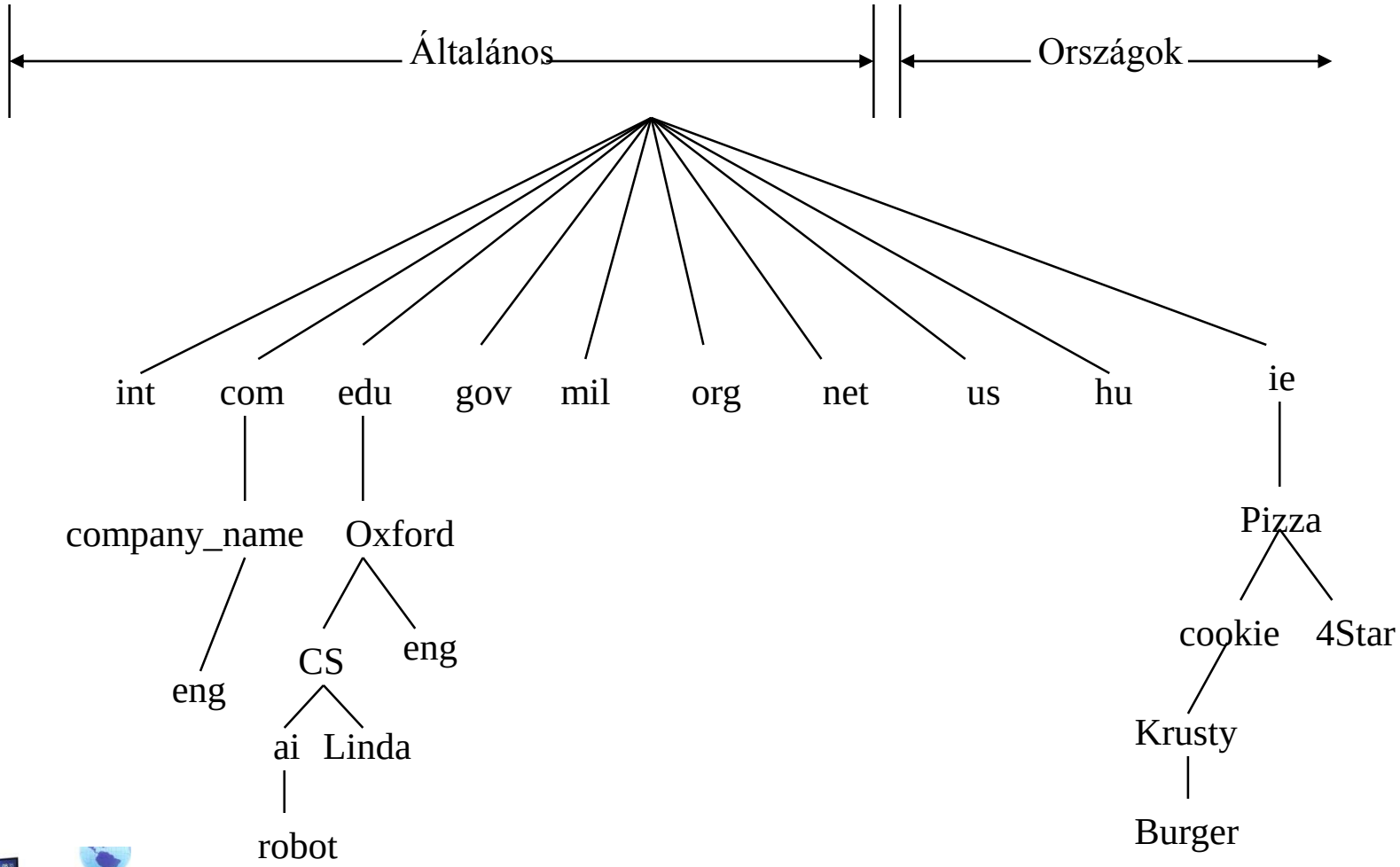
DNS NÉVTÉR

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

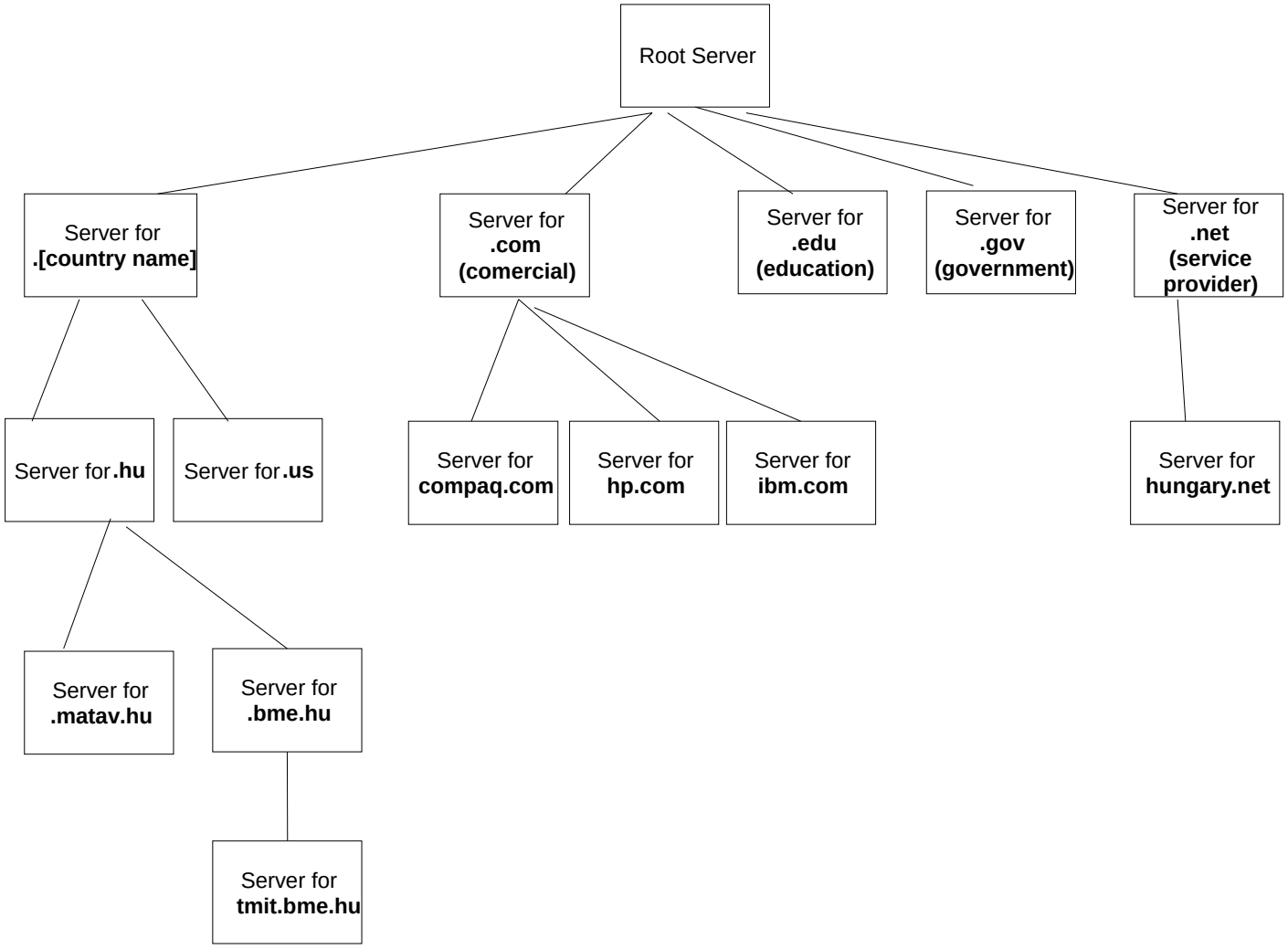
Domain	*Meghatározás*
.com	Kereskedelmi szervezetek
.edu	Oktatási intézmények
.gov	Kormányzati intézmények
.mil	Katonai csoportok
.net	Főbb hálózati szolgáltatók
.org	Szervezetek a fentieken kívül
.int	Nemzetközi szervezetek

- Országok
  - pl: .hu .us .fr .de

INTERNET DOMAIN NÉVTÉR

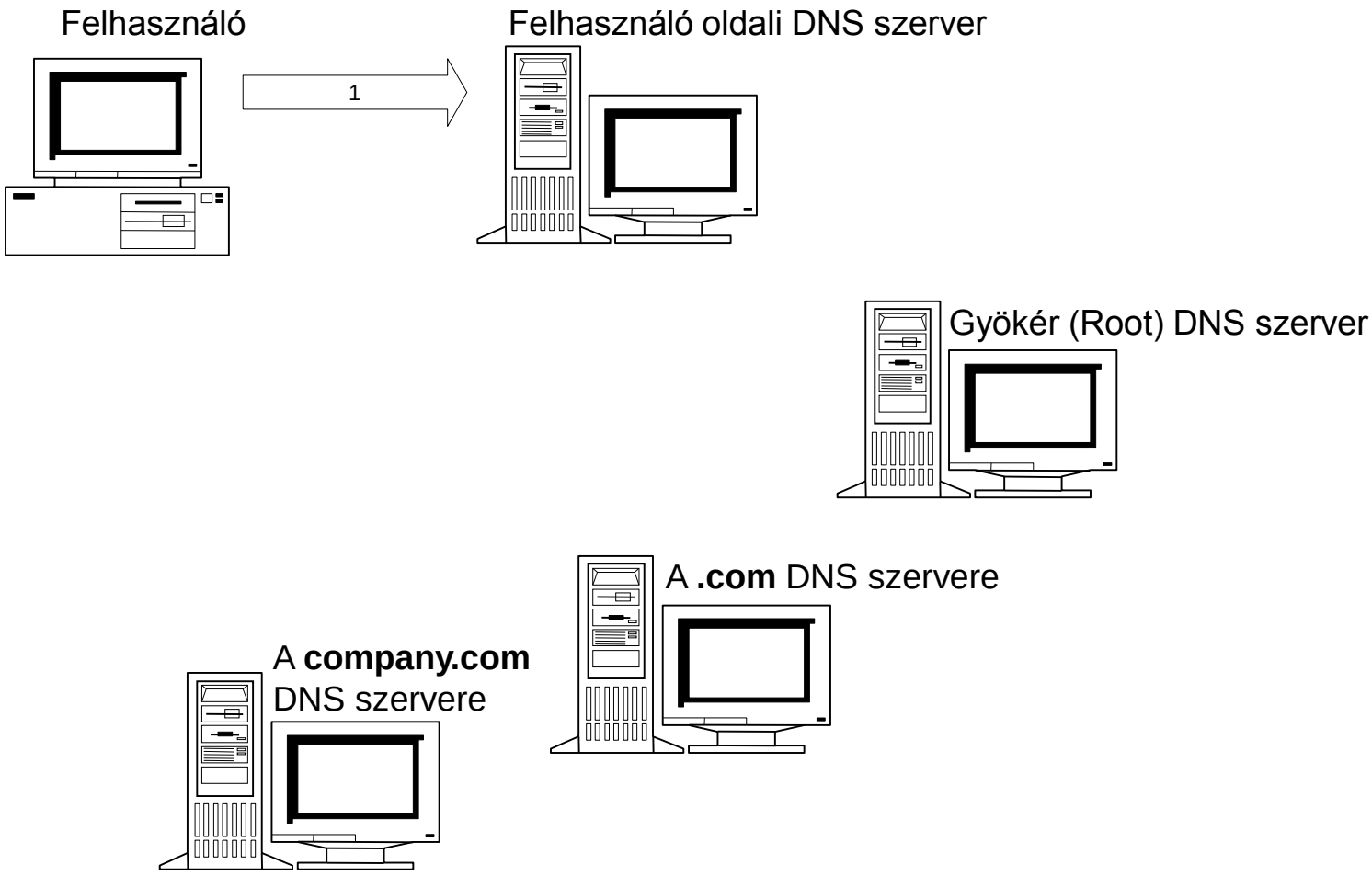


DOMAIN NÉV FELOLDÁSA



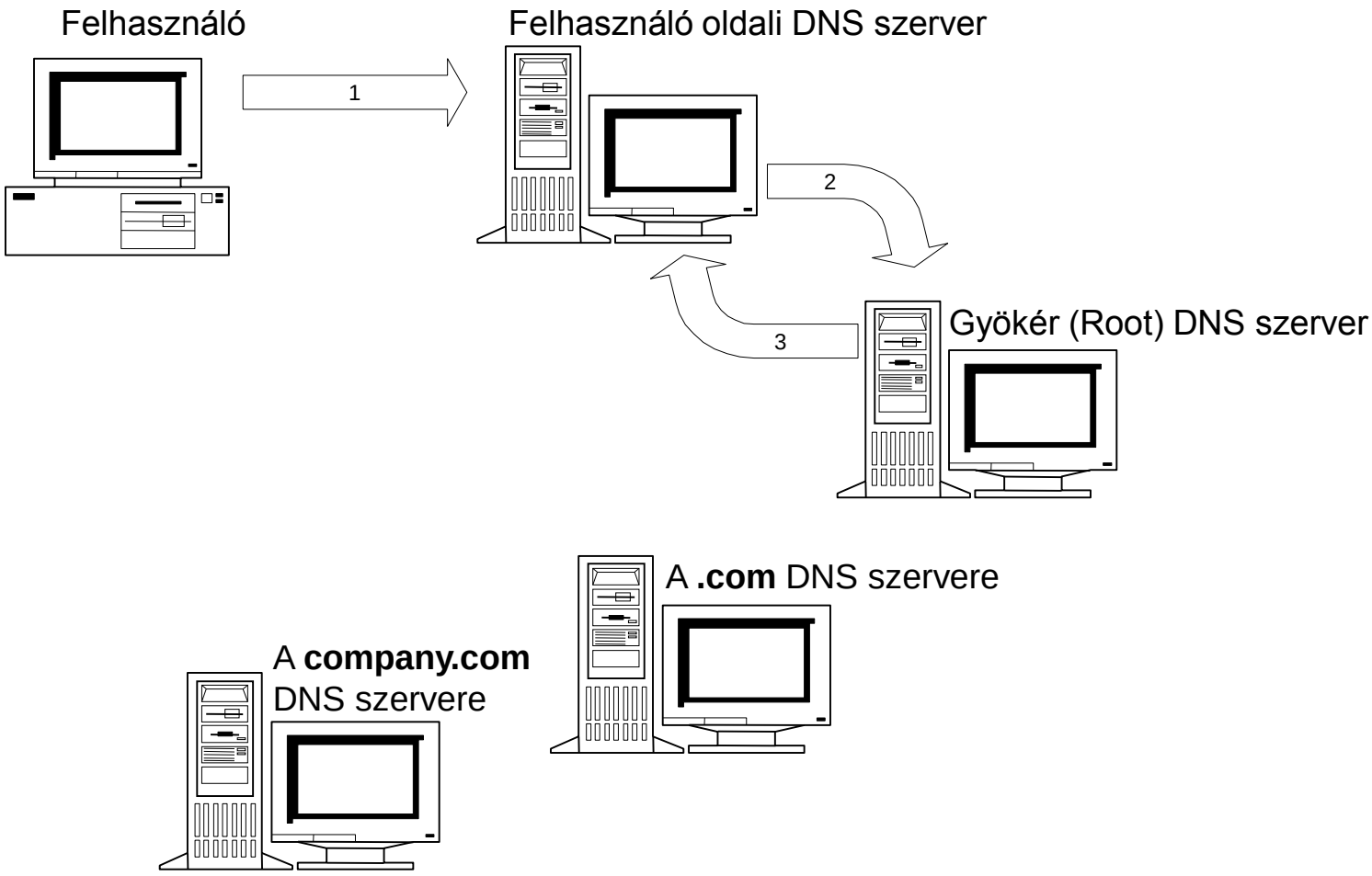
A DNS MŰKÖDÉSE

(A SOMEBODY.COMPANY.COM **DOMAIN NÉV FELOLDÁSÁNAK LÉPÉSEI**)



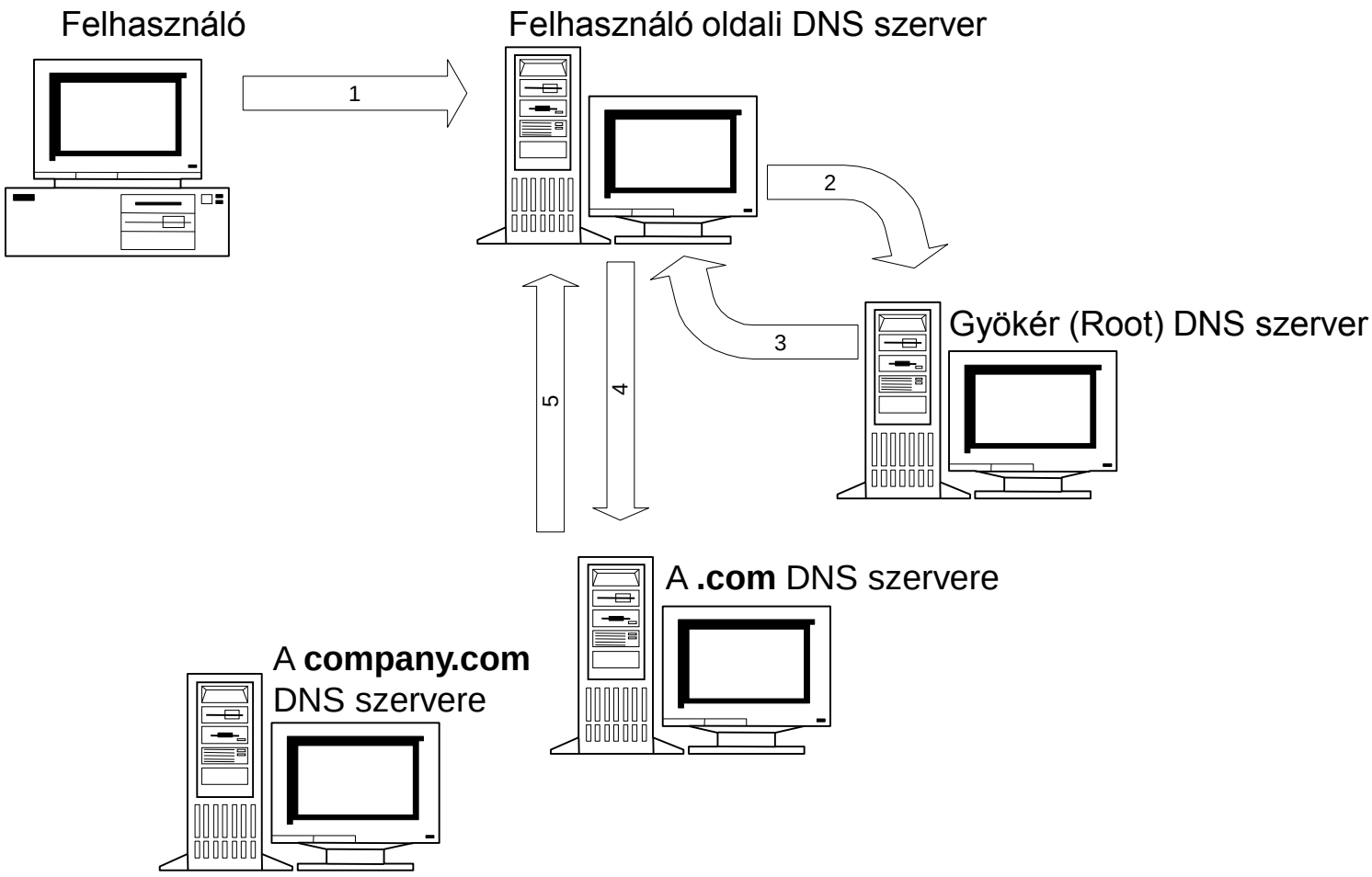
A DNS MŰKÖDÉSE

(A SOMEBODY.COMPANY.COM **DOMAIN NÉV FELOLDÁSÁNAK LÉPÉSEI**)



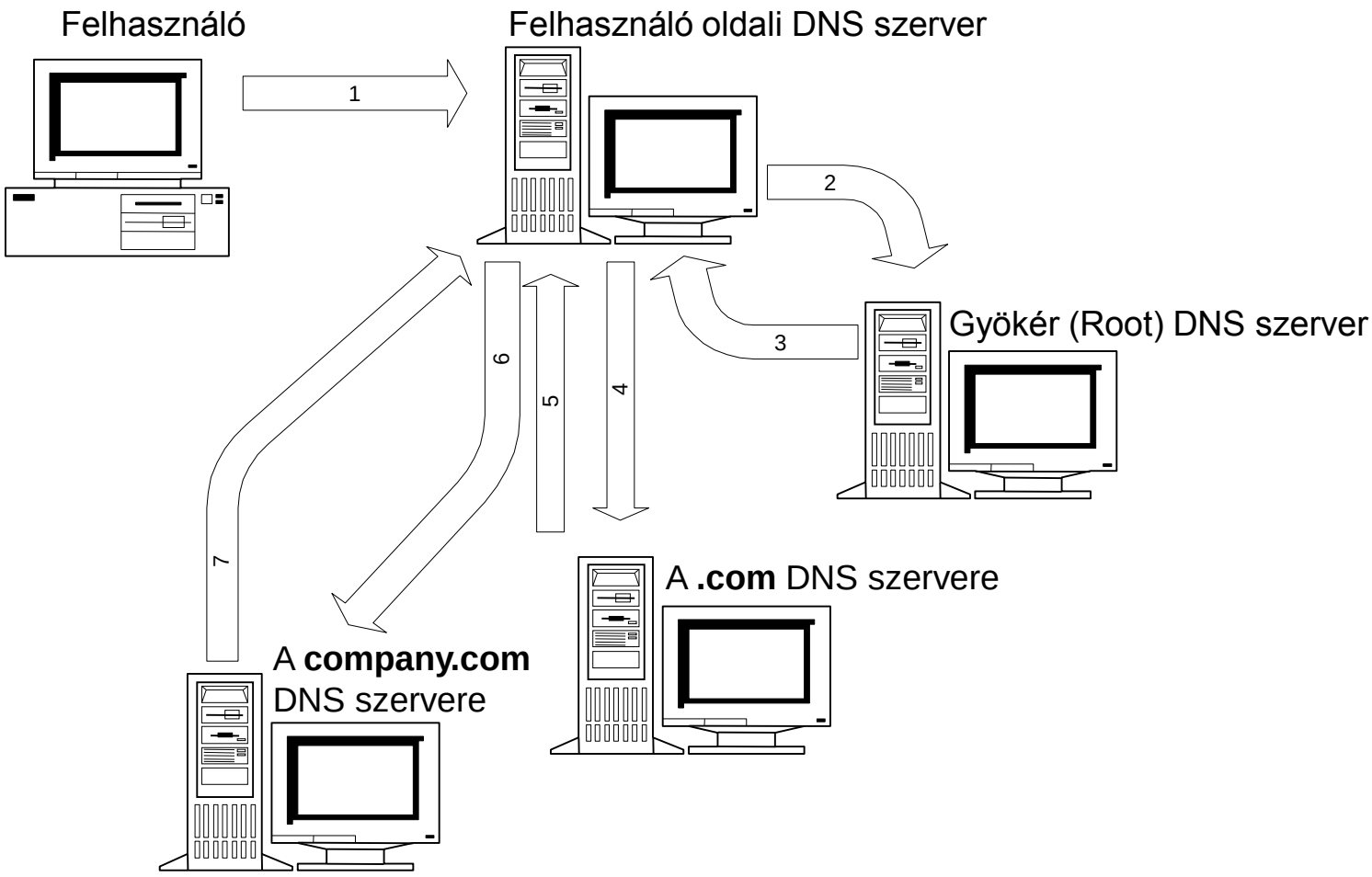
A DNS MŰKÖDÉSE

(A SOMEBODY.COMPANY.COM **DOMAIN NÉV FELOLDÁSÁNAK LÉPÉSEI**)



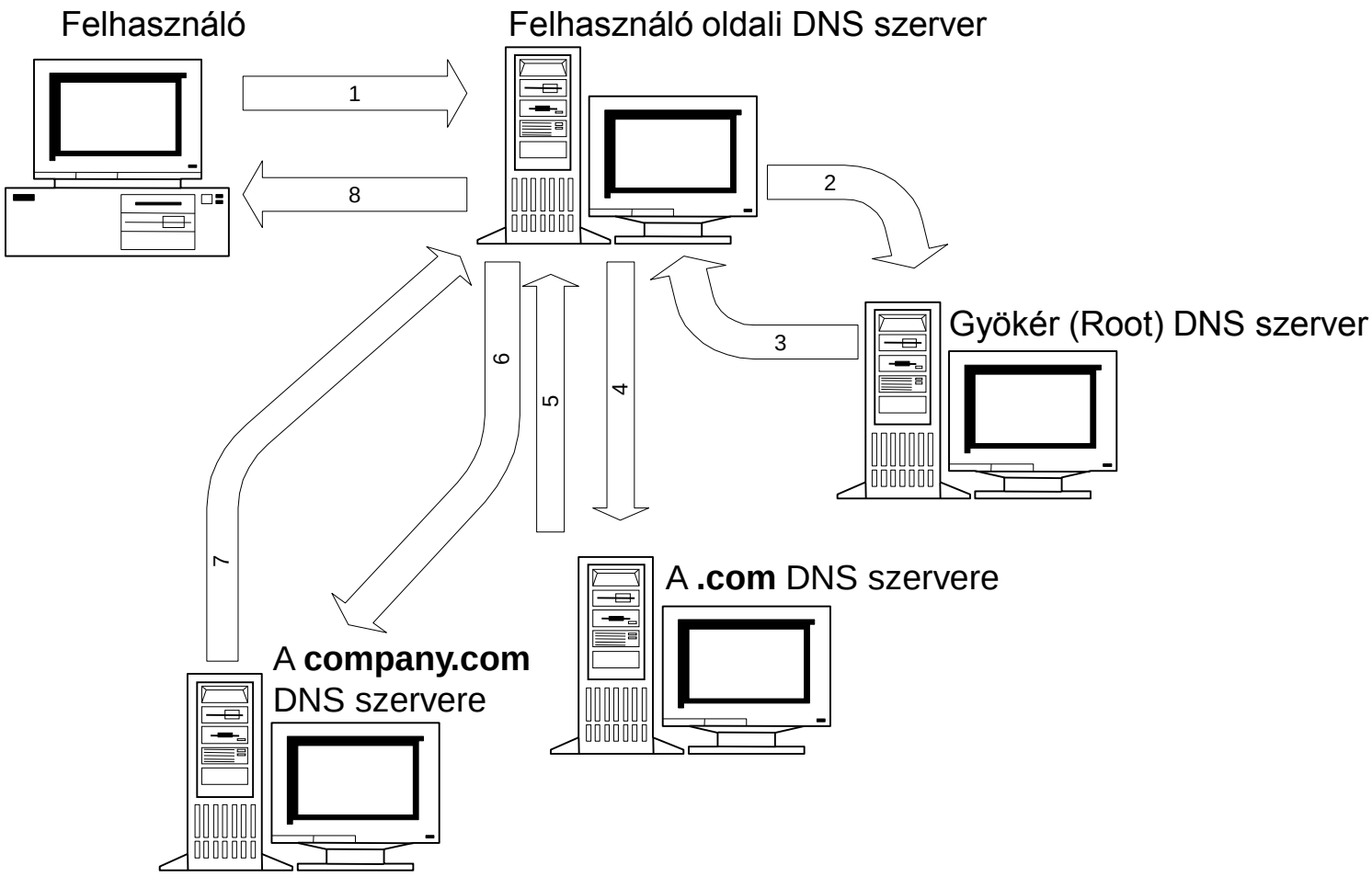
A DNS MŰKÖDÉSE

(A SOMEBODY.COMPANY.COM DOMAIN NÉV FELOLDÁSÁNAK LÉPÉSEI)



A DNS MŰKÖDÉSE

(A SOMEBODY.COMPANY.COM **DOMAIN NÉV FELOLDÁSÁNAK LÉPÉSEI**)



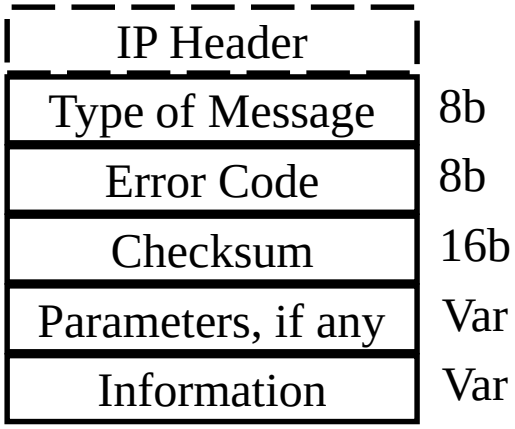
DNS GYORSÍTÓTÁR (DNS CACHING)

- 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



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

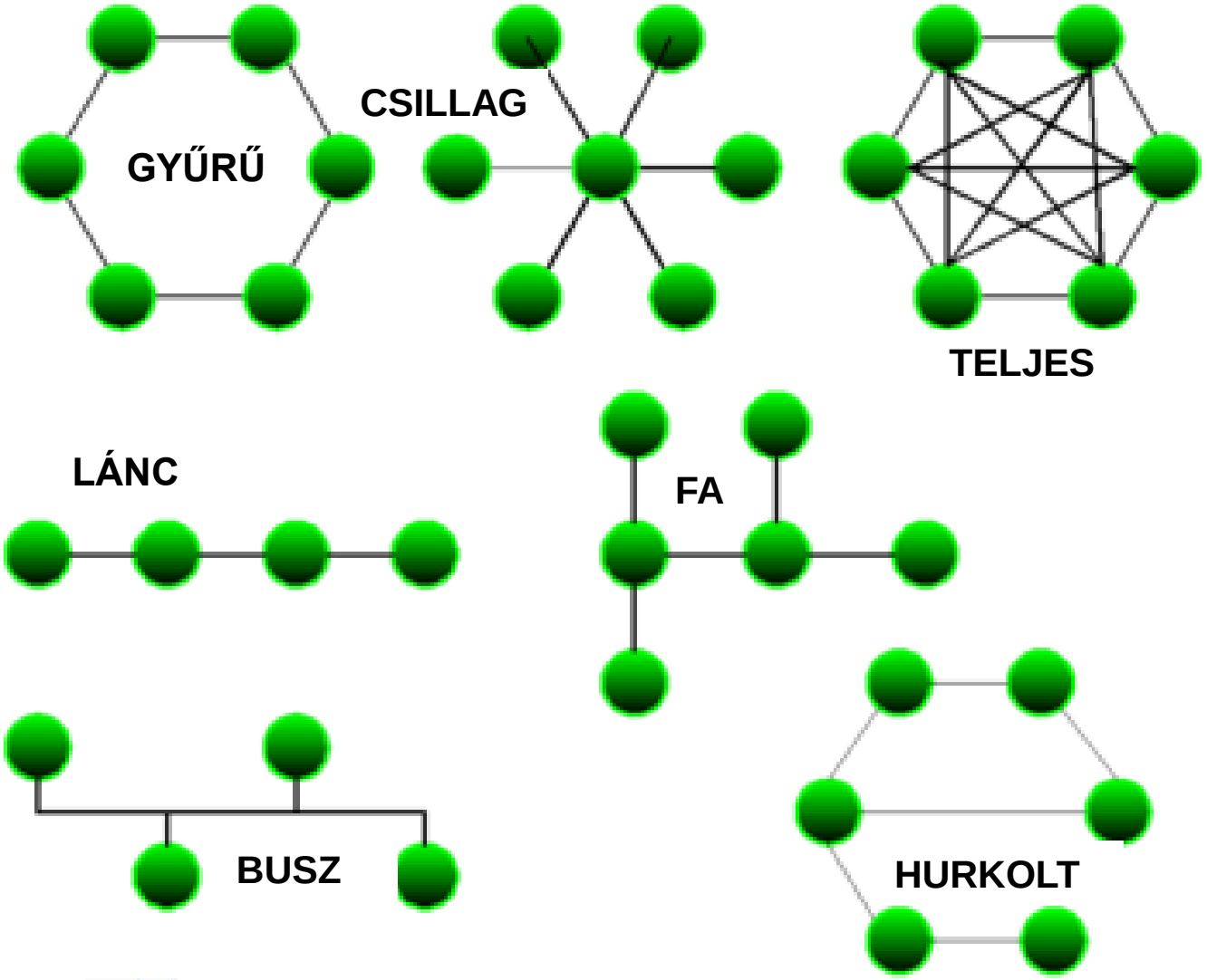
II. RÉSZ

HÁLÓZATOK
OTTHONI FELDOLGOZÁSRA

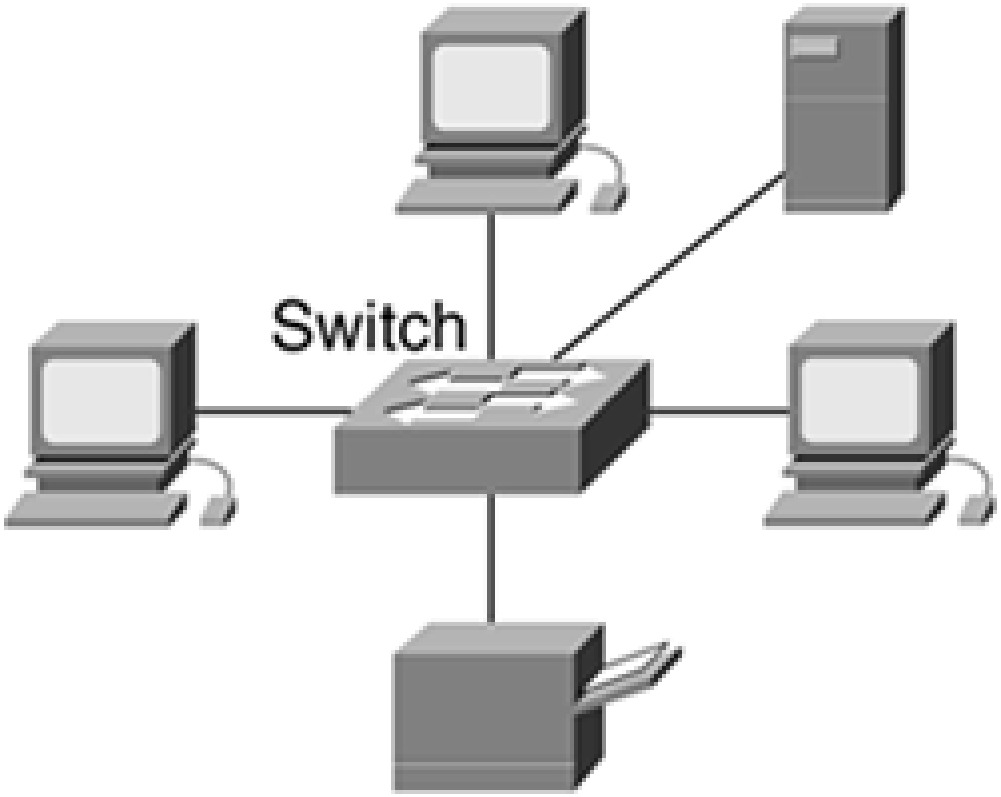
HÁLÓZATOK, HÁLÓZATOK ÜZEMELTETÉSE

- 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

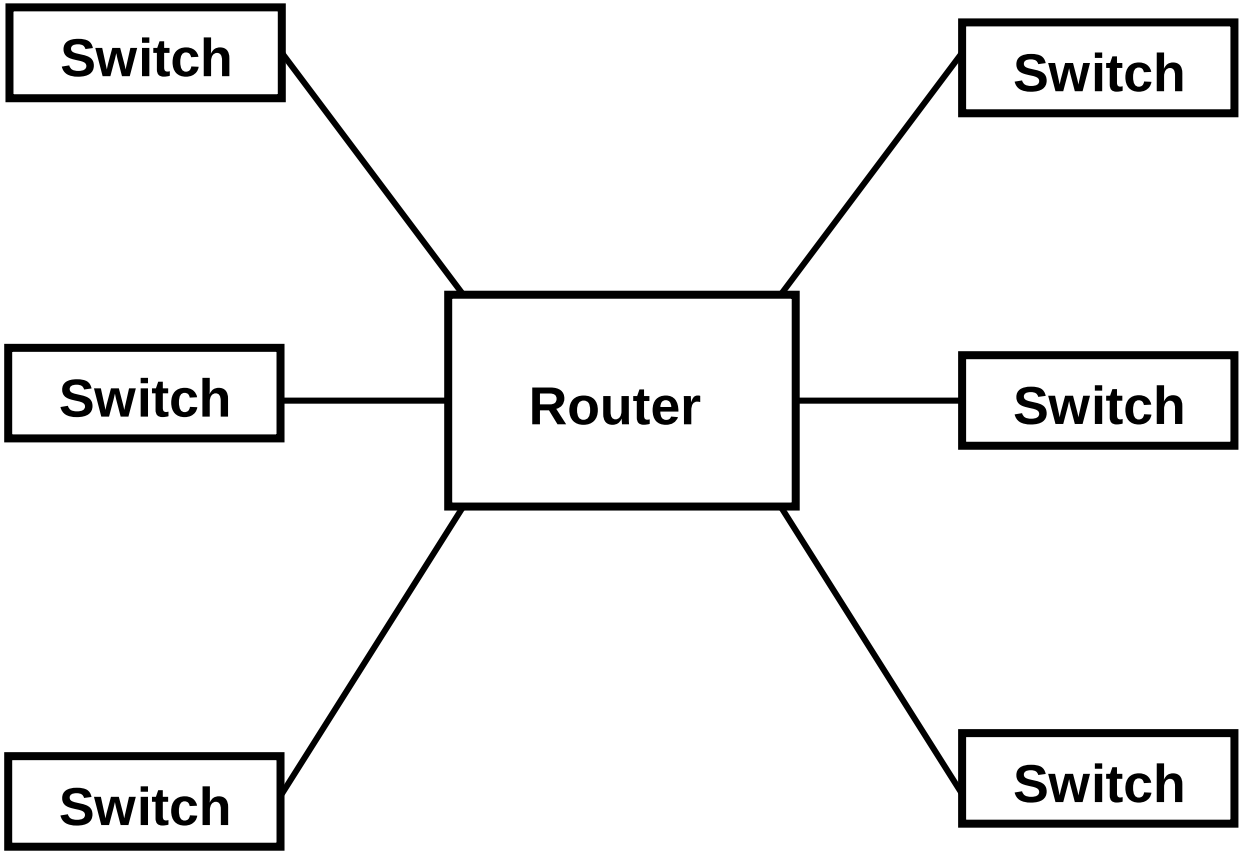
HÁLÓZATI TOPOLÓGIÁK



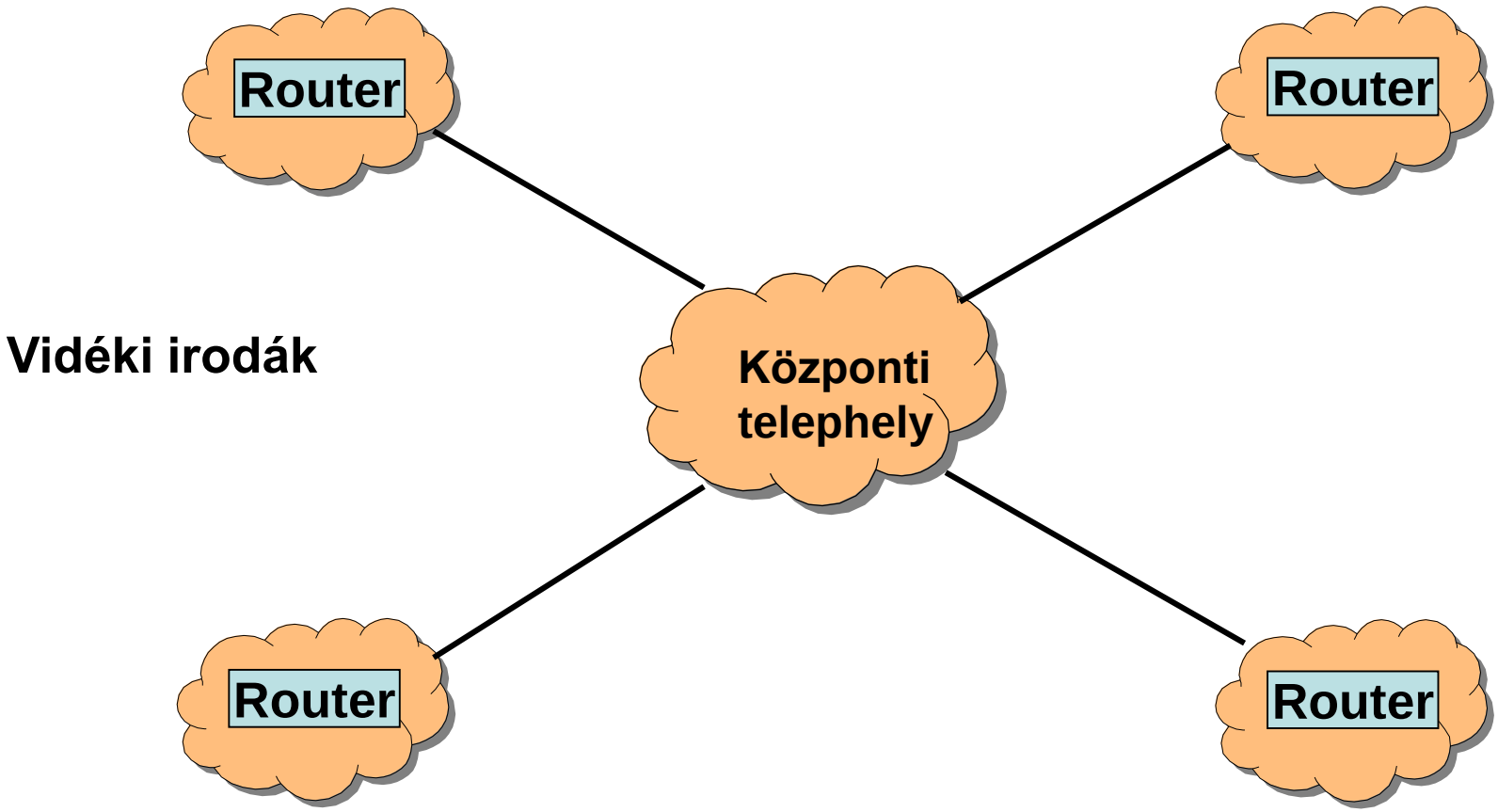
EGYSZERŰ CSILLAG LAN



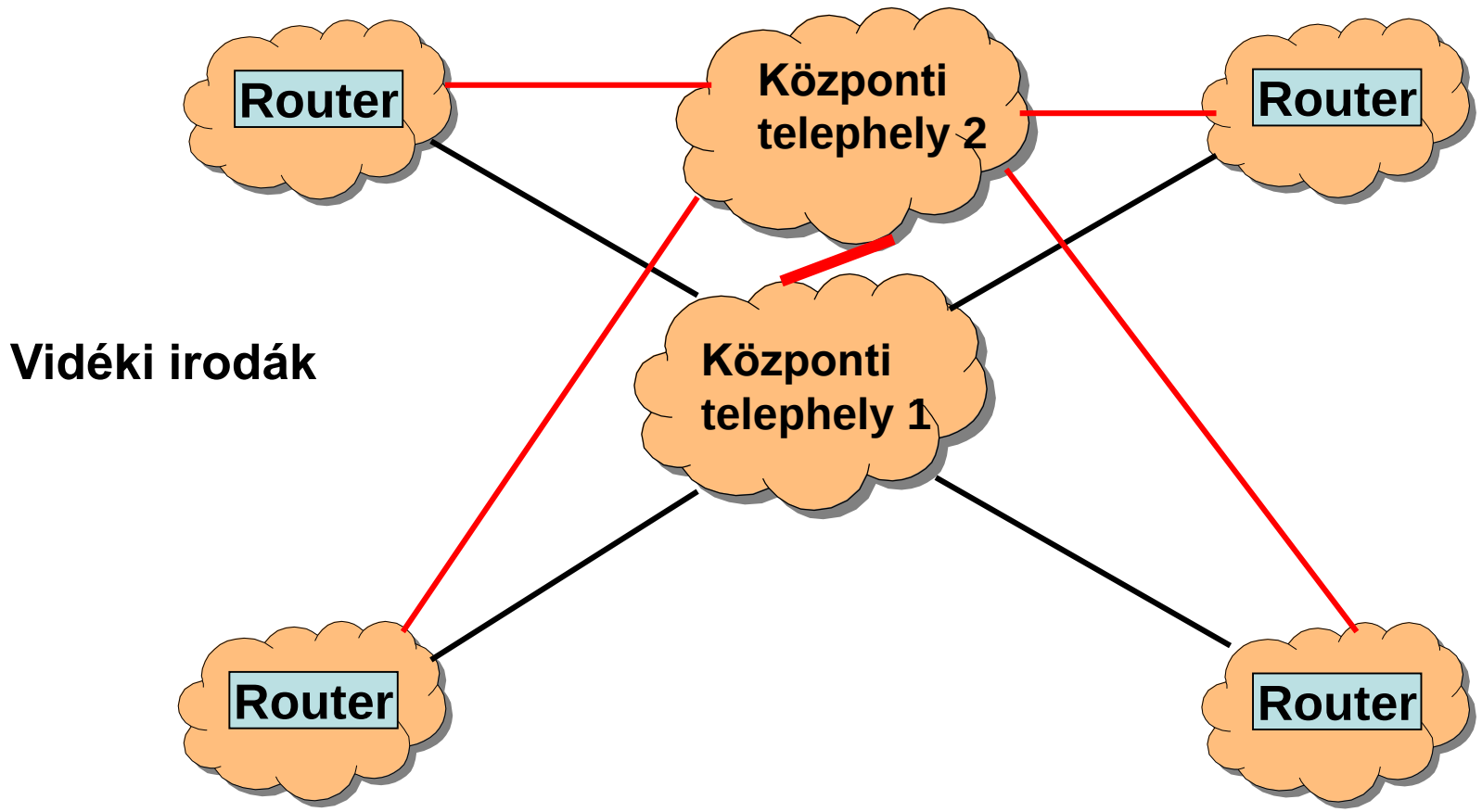
LAN, CAMPUS HÁLÓZAT - CSILLAG



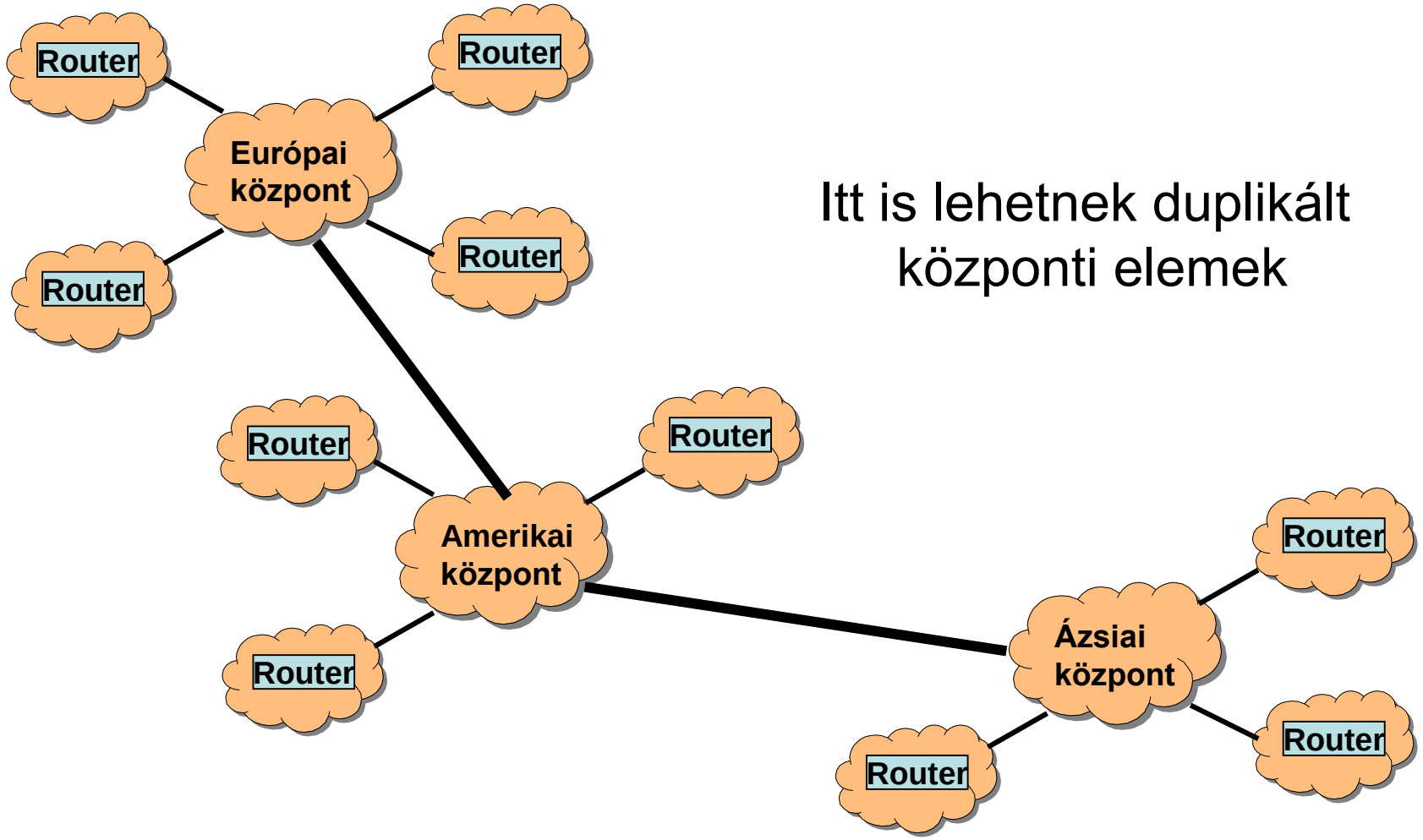
WAN – CSILLAG


Router
Router
Vidéki irodák
Központi telephely
Router
Router

WAN – CSILLAG – DUPLIKÁLT KÖZPONT



TÖBBSZÖRÖS CSILLAG (FA)

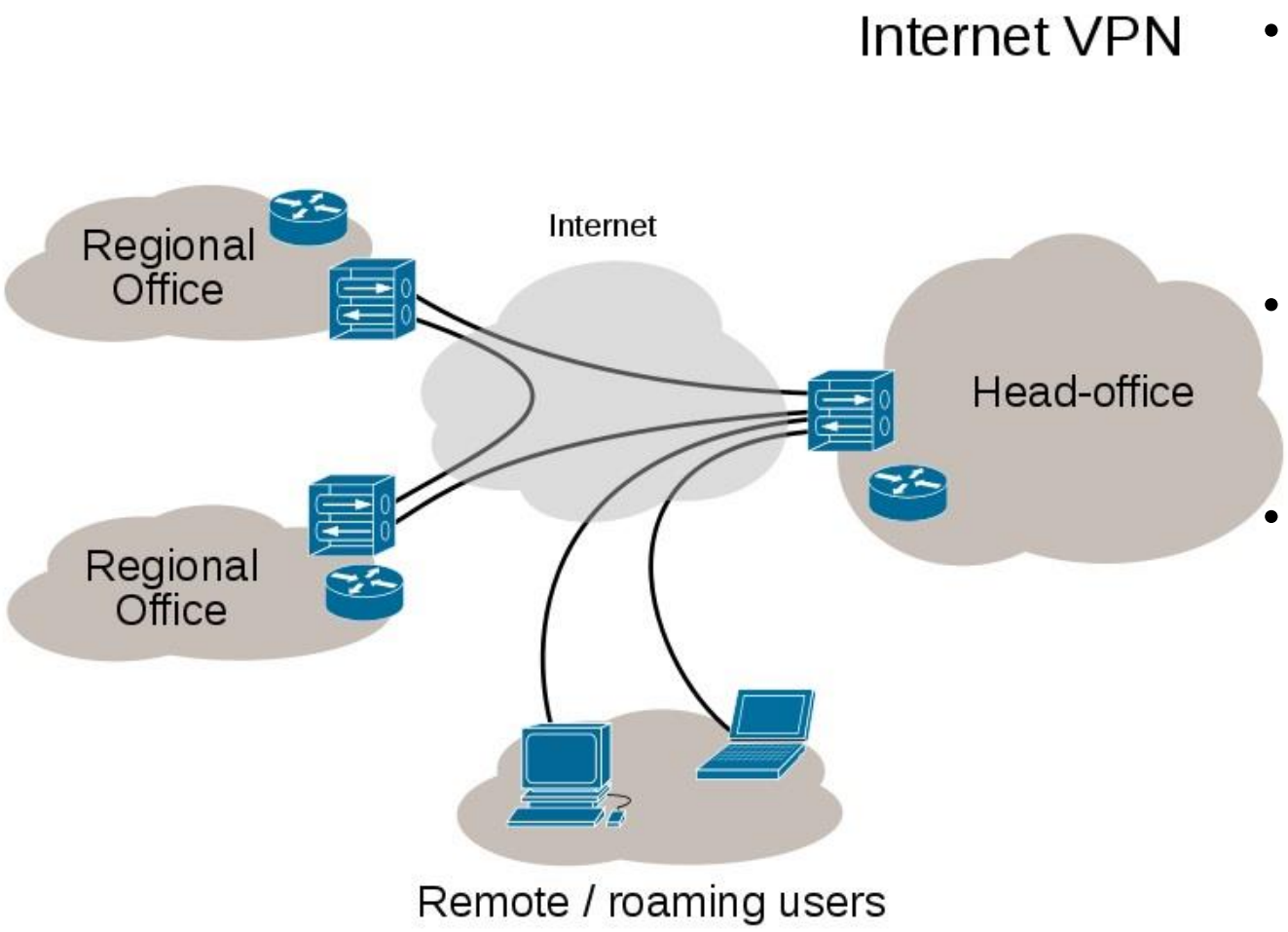


Itt is lehetnek duplikált központi elemek

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)

VIRTUÁLIS MAGÁNHÁLÓZATOK



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

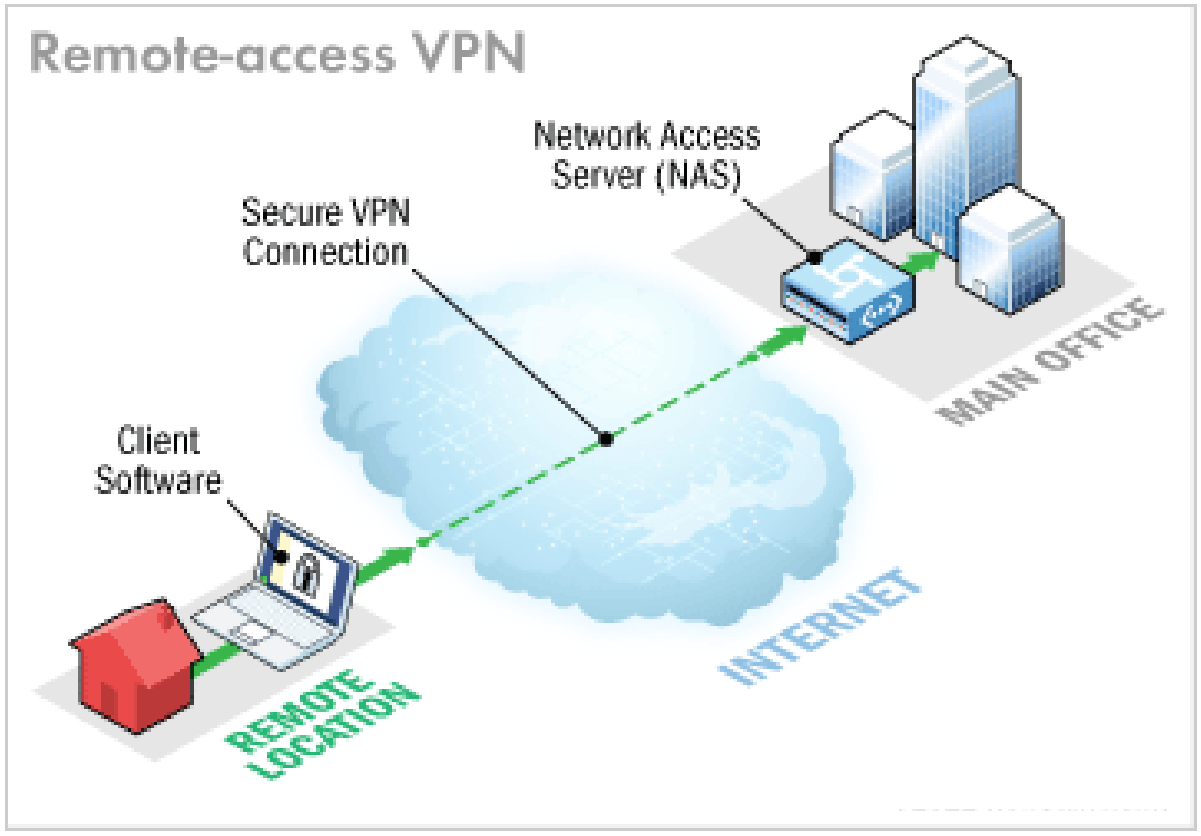
VPN ELŐNYÖK

- 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

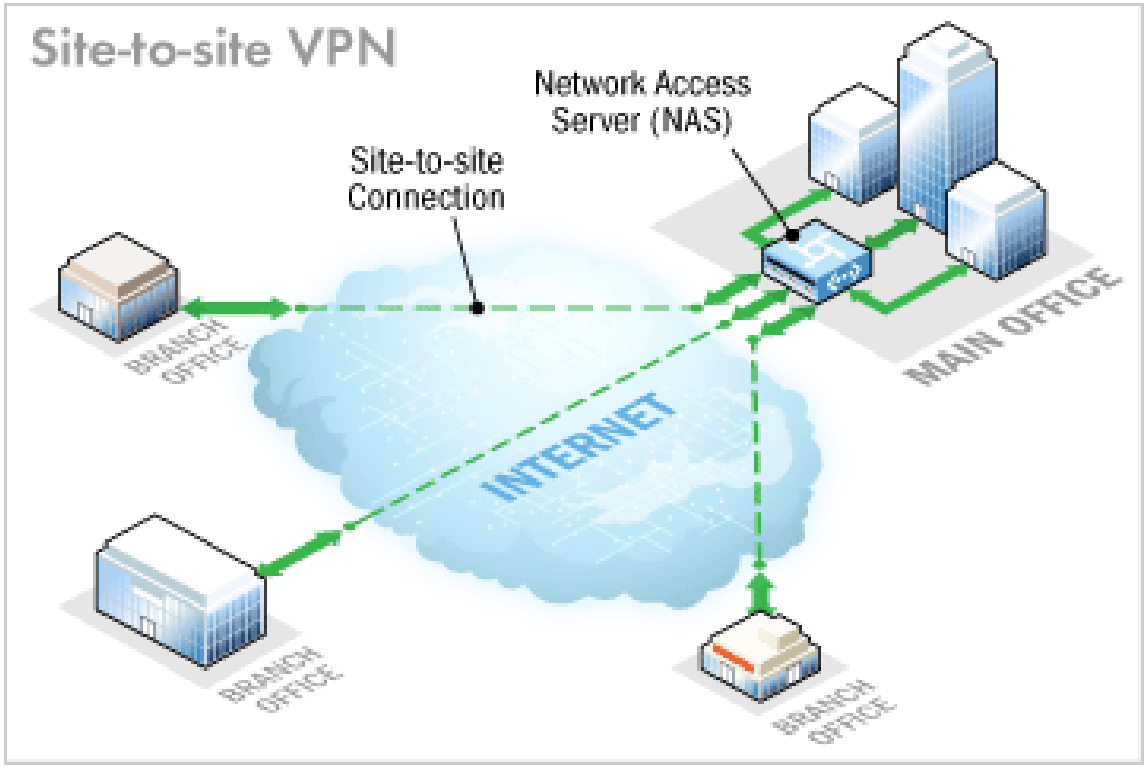
- Biztonság
  - VPN adatvédelem (titkosítás) a nyilvános hálózaton
    - Nem lehet lehallgatni
- Megbízhatóság
  - Munkavállalók/távoli irodák bármikor kapcsolódhatnak a VPN-hez
  - VPN minden használó számára ugyanazon paramétereket biztosítja – még a maximális egyidejű kapcsolat esetén is
- Skálázhatóság

REMOTE-ACCESS VPN



- Használókat köt be
  - Network Access Server (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, másnéven NAS – itt: Netwok Access Server

Network Access Server

- Tipikusan site-to-site VPN kialakításához:
  - Létrehozza és konfigurálja az alagutakat (logikai összeköttetéseket)
  - Használók autentikálása
  - Alagút/IP címek használókhoz rendelése
  - Adat titkosítás/visszafejtés
  - Vég-vég adattovábbítás
- VPN (alagutazásra képes) router
- Általában ma már tűzfallal integrálják

Network Access Server

- “Intelligens” VPN koncentrátor
  - VPN (alagutazásra képes) router
  - Létrehozza és konfigurálja az alagutakat (logikai összeköttetéseket) – remote-access VPN
  - Vég-vég adattovábbítás
  - Alagutazás (tunneling)
    - A használói adatokat becsomagolja egy keretbe
    - Vezérlő fejlécet ad hozzá
  - Titkosítás
    - IPSec
      - Site-to-site
    - SSL
      - Remote access

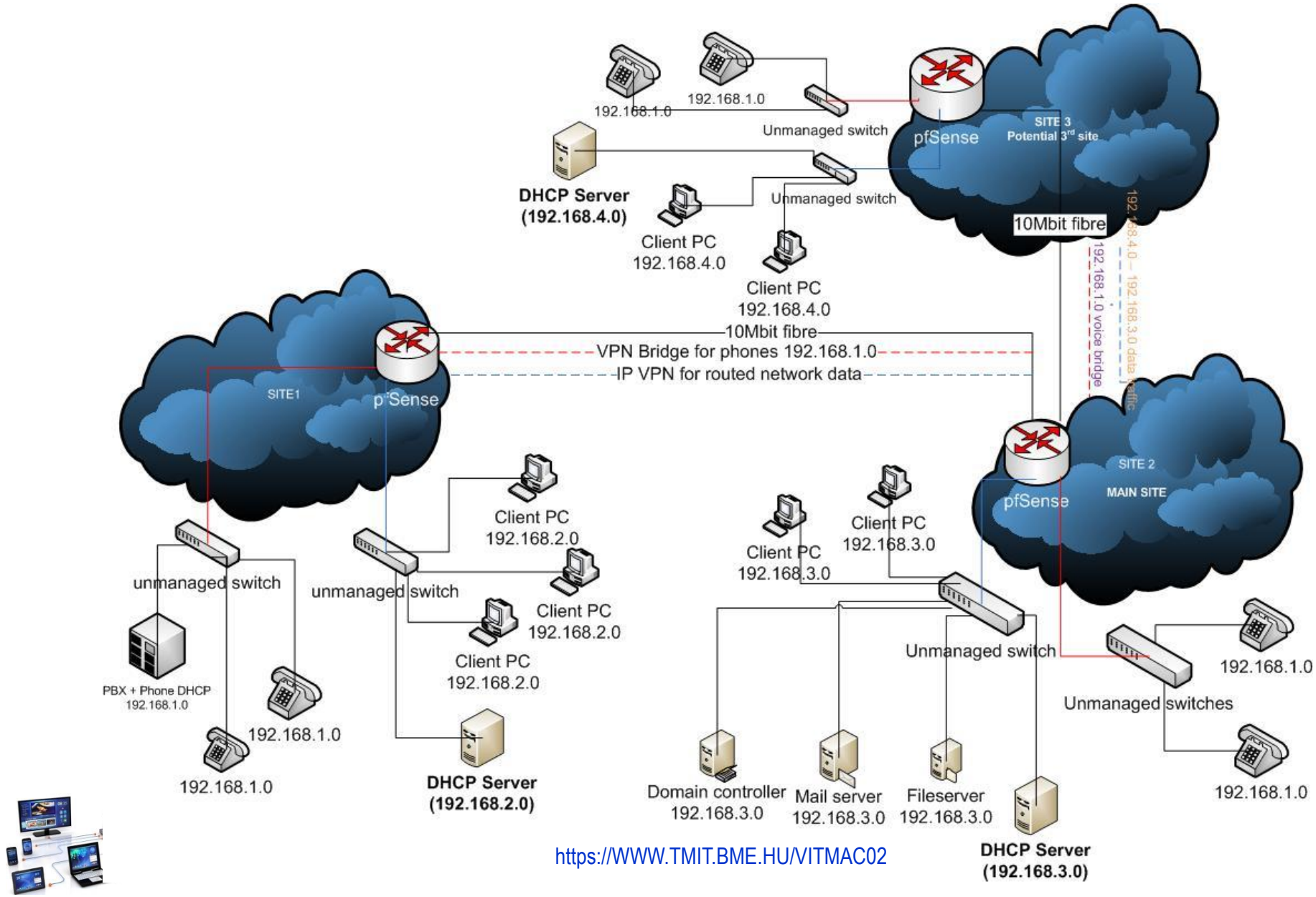
Network Access Server

- 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

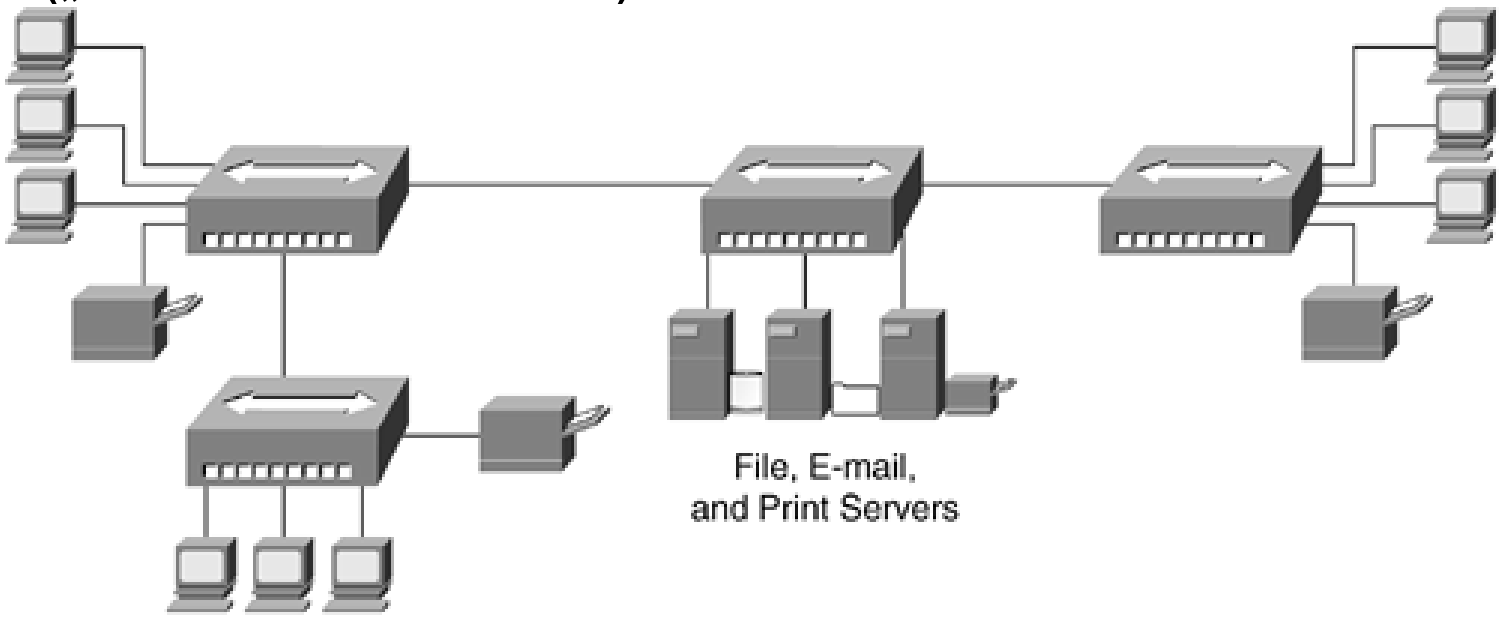
LOGIKAI HÁLÓZATI TÉRKÉP



https://WWW.TMIT.BME.HU/VITMAC02

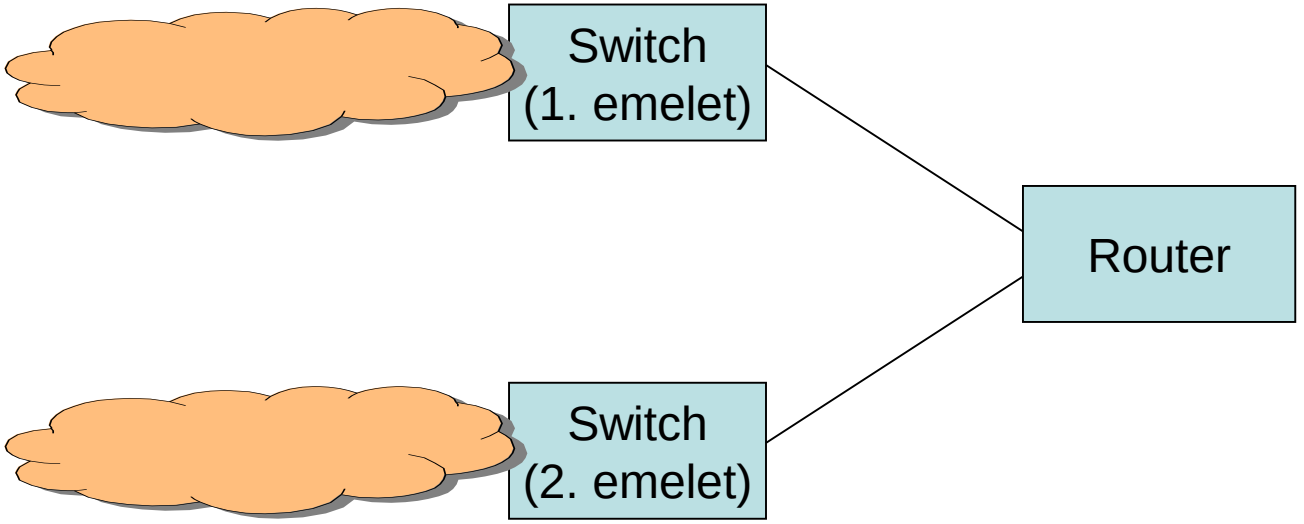
TIPIKUS LOGIKAI TOPOLÓGIÁK

- 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