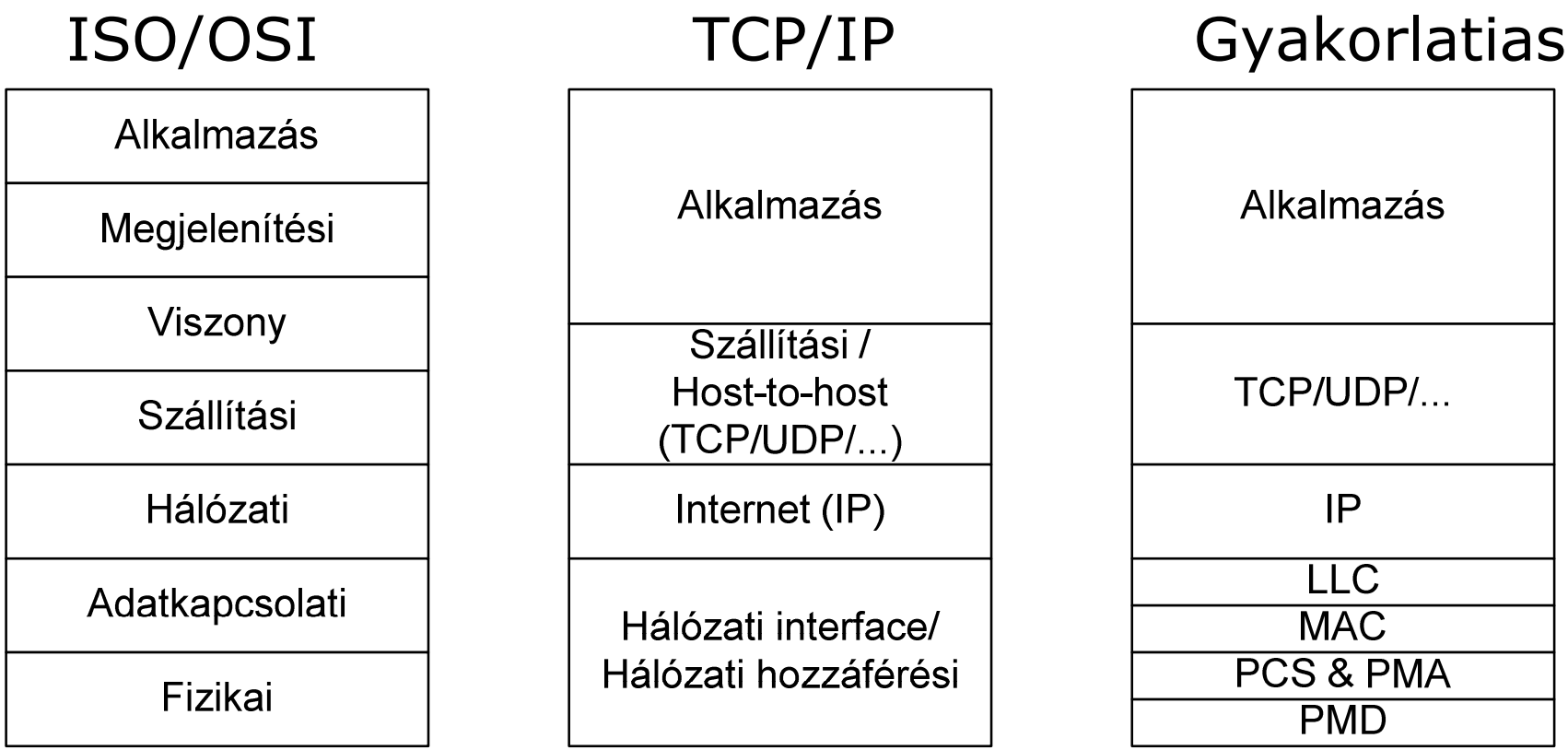
Hálózatbiztonság

TCP/IP architektúra és az ISO/OSI rétegmodell



IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

LLC: Logical Link Control

MAC: Medium Access Control

PCS: Physical Coding Sublayer

PMA: Physical Medium Attachment

PMD: Physical Medium Dependent

Hálózatbiztonság

az alkalmazásoknál

A hálózatbiztonság építőkövei

- AAA
  - Authentication: hitelesítés
    - Azonosítás (identification) és hitelesség
  - Authorization: jogosultság-hozzárendelés
    - A hitelesítés alapján az erőforrásokhoz való hozzáférés
  - Accounting: számlázás / fiókkezelés
- Algoritmusok
  - Titkosítás
  - Hitelesítés
  - Kulcscsere

Megoldások hitelesítésre

- Kerberos
  - Adott tartományon belül működik
  - Időbélyeget használ
- Public Key Infrastructure (PKI)
  - Nyilvános kulcsú titkosítás felhasználásával
  - Digitálisan aláírt tanúsítványokat kiállító szervezetek (CA: Certificate Authority)
    - Ők adhatnak ki tanusítványt
    - Mindegyik a felette lévőben bízik meg
    - Legfelsőbb szintű CA-ban meg kell bízni

Megoldások titkosításra

- Szimmetrikus kulcsú
  - DES
  - 3DES
  - AES
- Nyilvános kulcsú
  - RSA (PKI is ezt használja)
  - Elliptikus görbék

- Részletesebben: *Kódolástechnika* c. tárgy

Összetett megoldások

- IPSec
  - Hitelesítés, kulcscsere- és titkosítás-egyeztető és –megvalósító keretrendszer
  - Két fő típus
    - Authentication Header (AH): digitálisan aláírt IP-csomag beleértve az IP-fejlécet is
    - Encapsulated Security Payload (ESP): Titkosított tartalmú csomag
  - IPv6-ban kötelezően támogatott
- SSL
  - SSH, FTPS, HTTPS, SMTPS, POP3S, IMAP4S, …
- TLS

- Részletesebben: *Kódolástechnika* c. tárgy

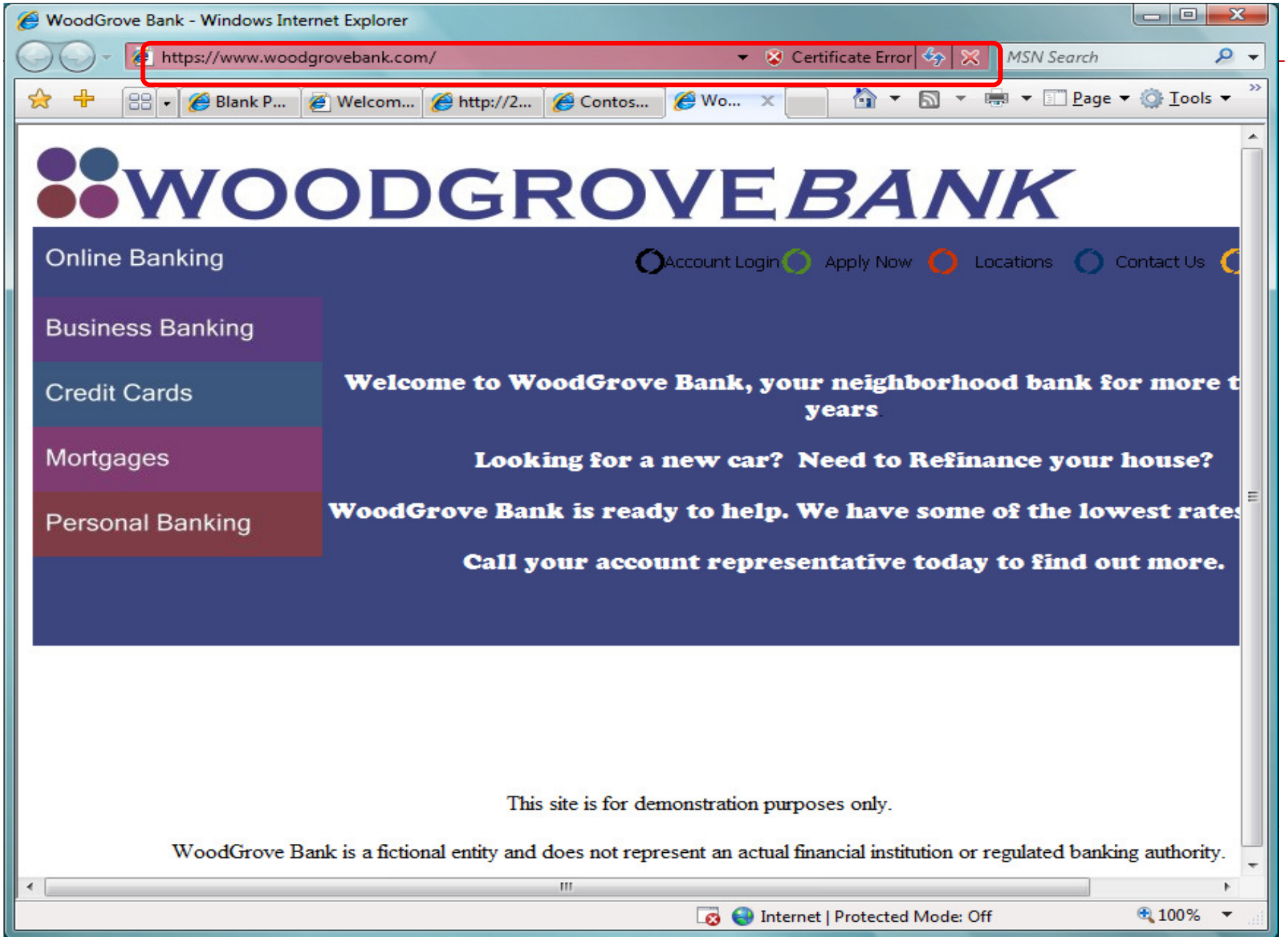
HTTP biztonság

- Hitelesítés
  - Névtelen hozzáférés (Anonymous)
  - Alapvető (Basic)
    - Base64 kódolás
  - Digest
    - Challenge/response alapú
  - Integrált (Integrated)
    - LANMan
    - NTLM
    - Kerberos
  - Tanúsítvány (Certificate)
  - Egyéb
- HTTPS
  - HTTP SSL-en (PKI:RSA; DES, 3DES)
  - TCP 443

A hálózatbiztonság eszközei

- Hálózati eszközök
  - Tűzfal (FW: FireWall)
  - Behatolás-észlelő rendszer (IDS: Intrusion Detection System)
  - Behatolás-megelőző rendszer (IPS: Intrusion Prevention System)
- Biztonságos alkalmazás (tervezés, implementálás, terjesztés,…)
- Biztonságosan üzemeltetett/használt alkalmazás (Social Engineering)

Adathalászat megelőzése

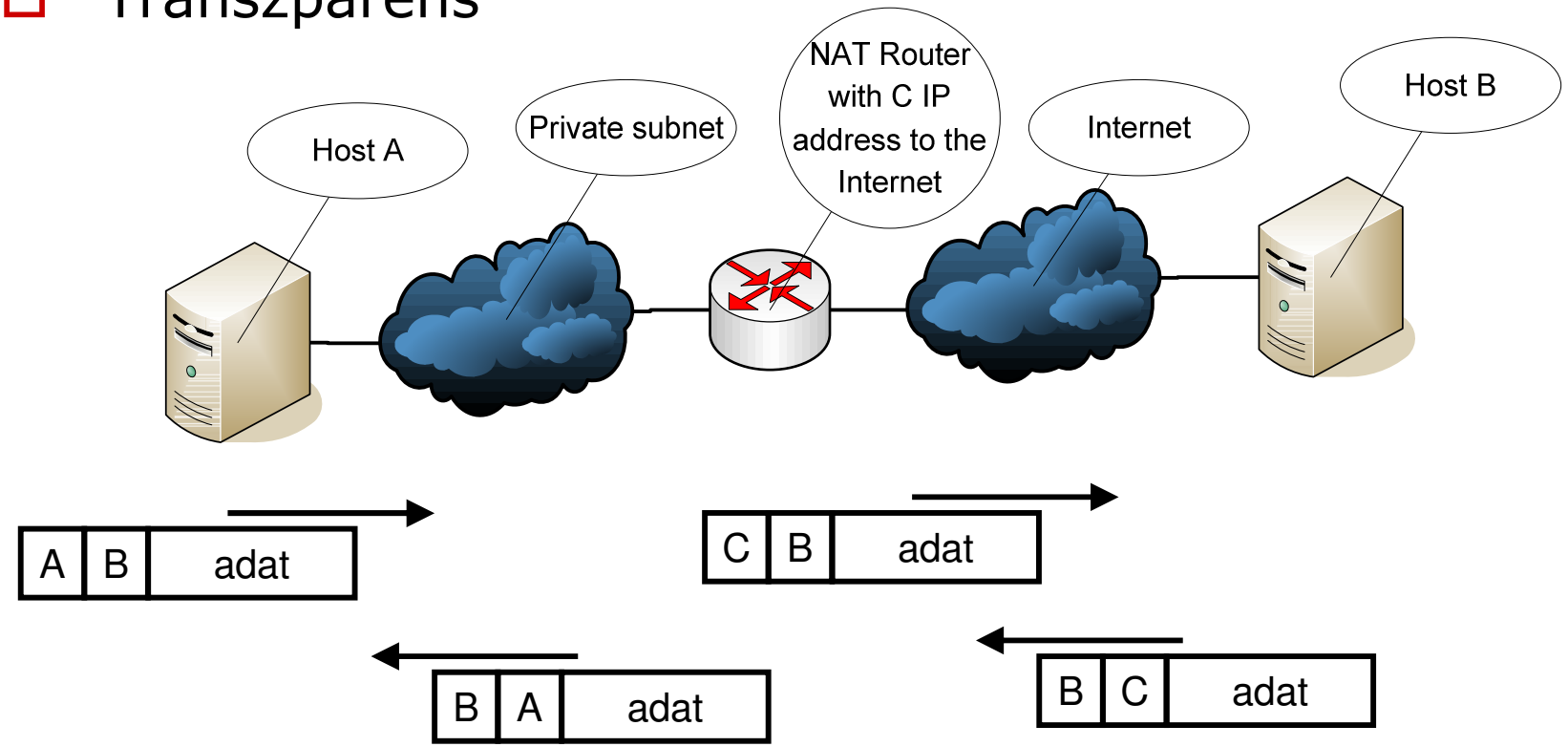


NAT – Network Address Translation

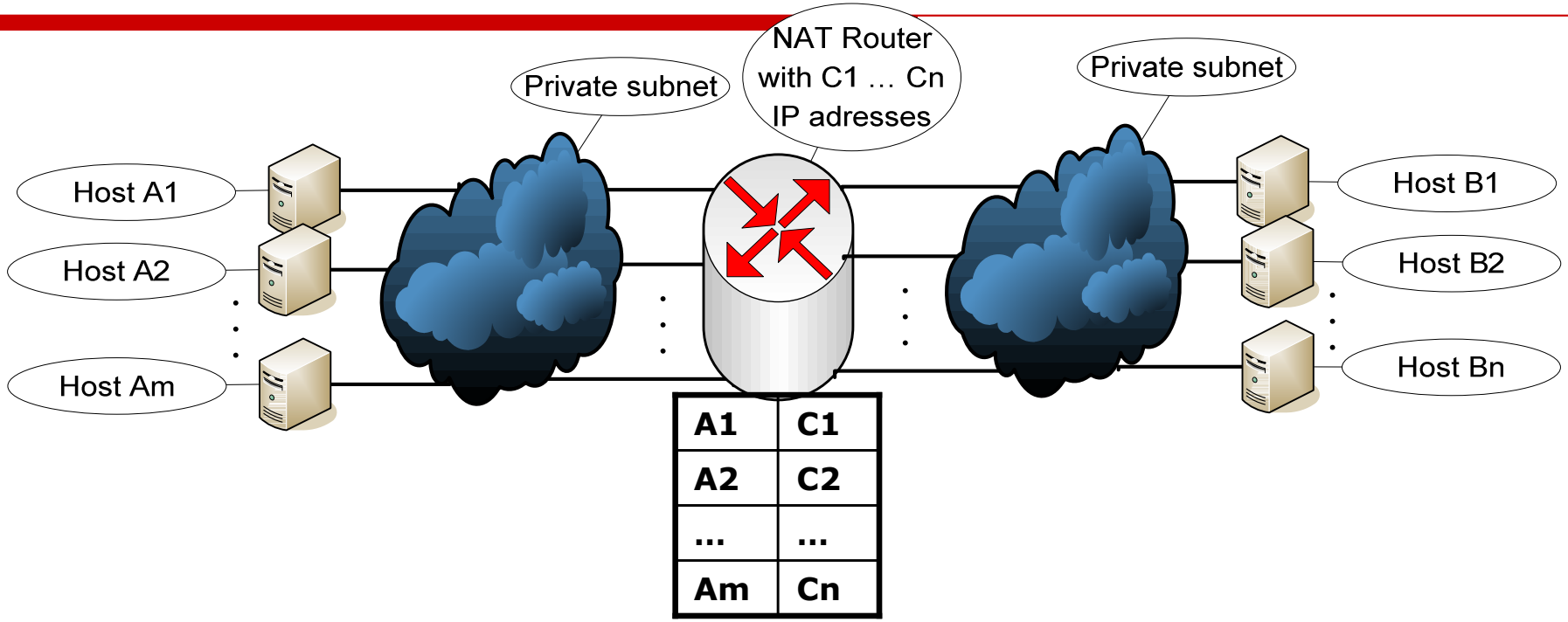
Hálózati címfordítás

NAT – Network Address Translation

- The IP Network Address Translator (RFC1631) (1994)
- A belső (magán-) hálózat és az Internet összekötésére
- Csak hálózati rétegbeli átalakítás - címcserével
- Transzparens

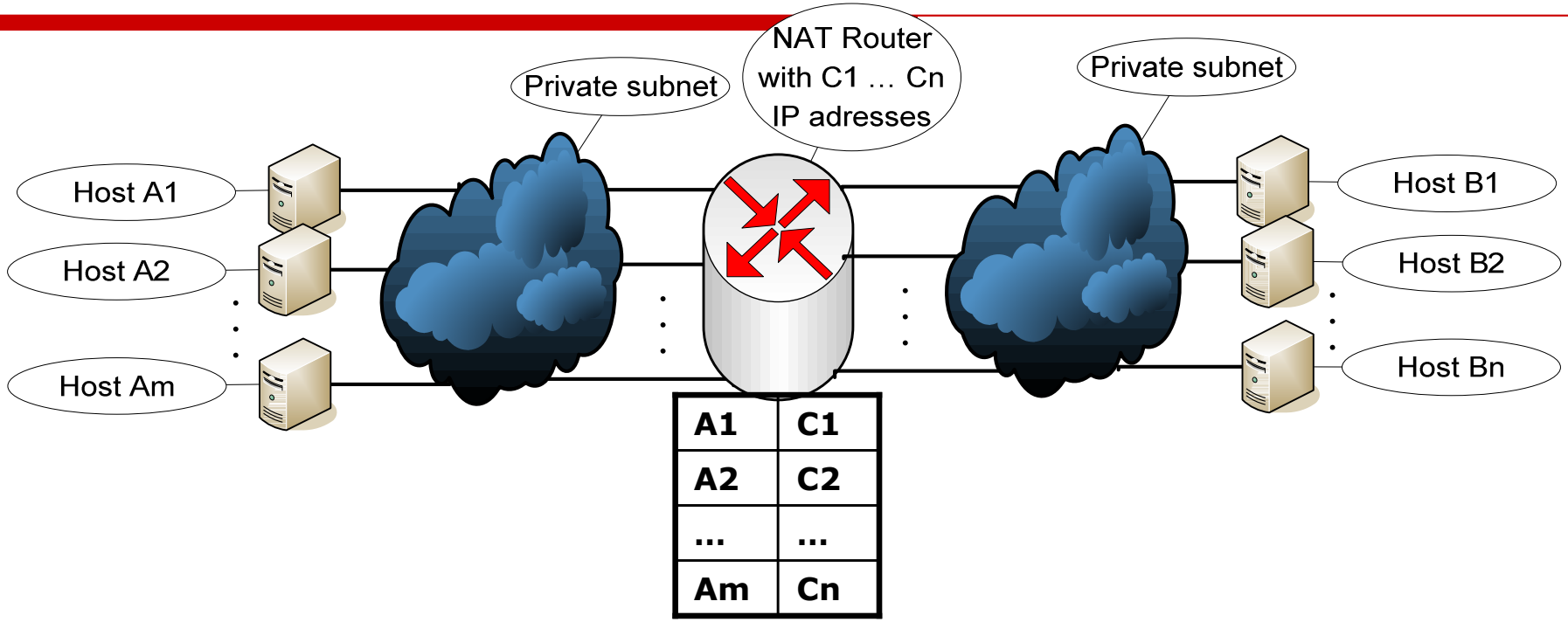


NAT router több IP-címmel (m=n)



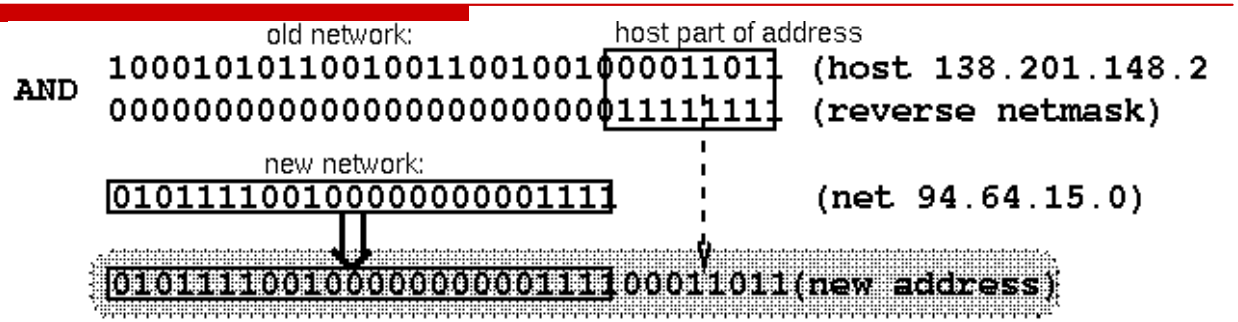
- A router rendelkezik megfelelő számú nyilvános címmel, hogy minden belső címhez hozzárendeljen egyet
- Külső-belső címösszerendelés
  - Statikus
  - Dinamikus – biztonsági szempontból előnyös

NAT router kevés IP-címmel (m>n)



- A router nem rendelkezik megfelelő számú nyilvános címmel, hogy minden belső címhez hozzárendeljen egyet
- Külső-belső címösszerendelési stratégiára van szükség

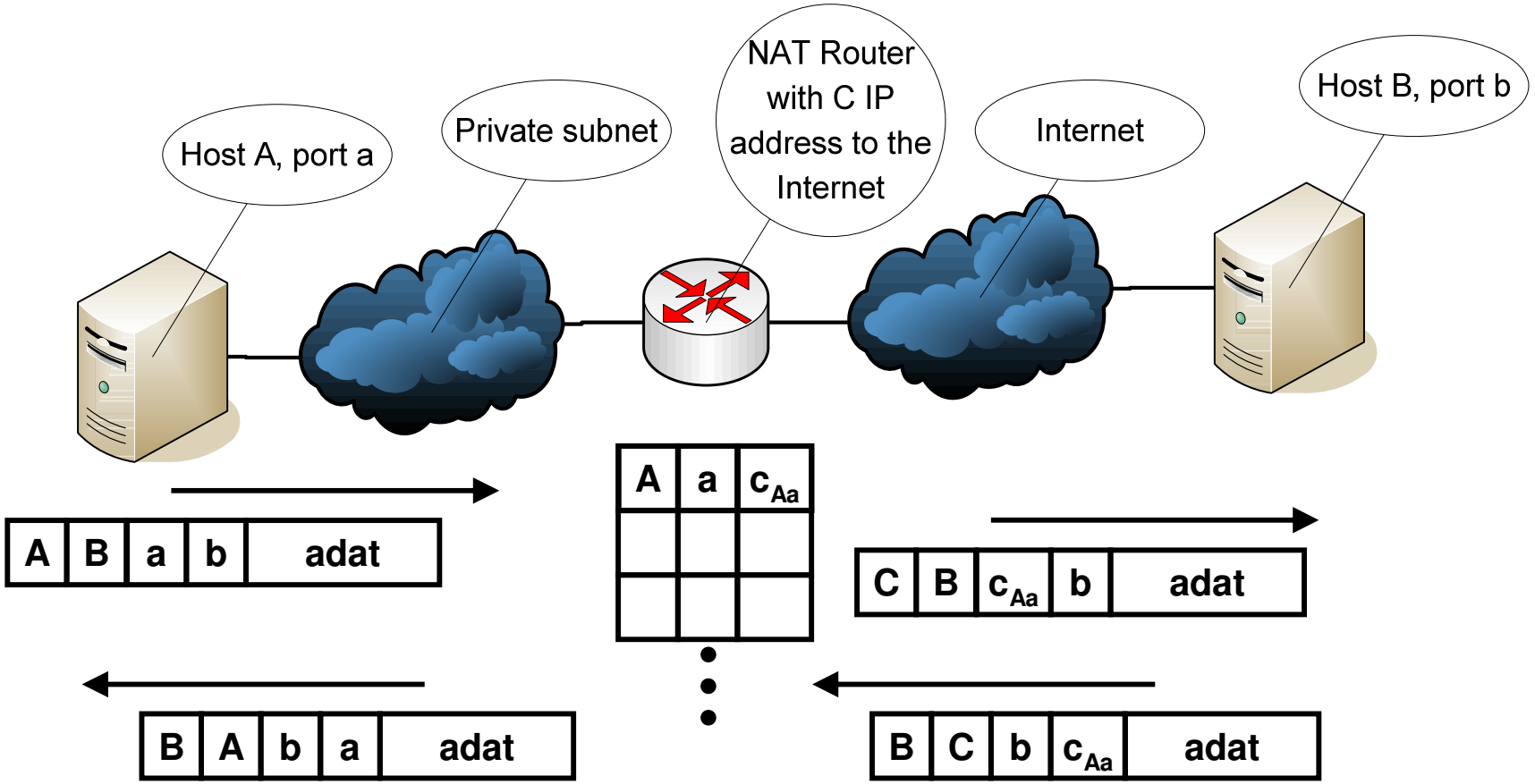
NAT – Cím-összerendelési stratégia



- Statikus
  - Probléma:
    - Több mint egy belső cím jut egy külsőre
    - Hogyan talál vissza a belső állomáshoz a vissza-irányú kommunikáció?
- Dinamikus
  - Használjuk a következő szabad IP-címet (C1 … Cn)
  - Probléma:
    - Nincs minden állomás számára elegendő IP-cím

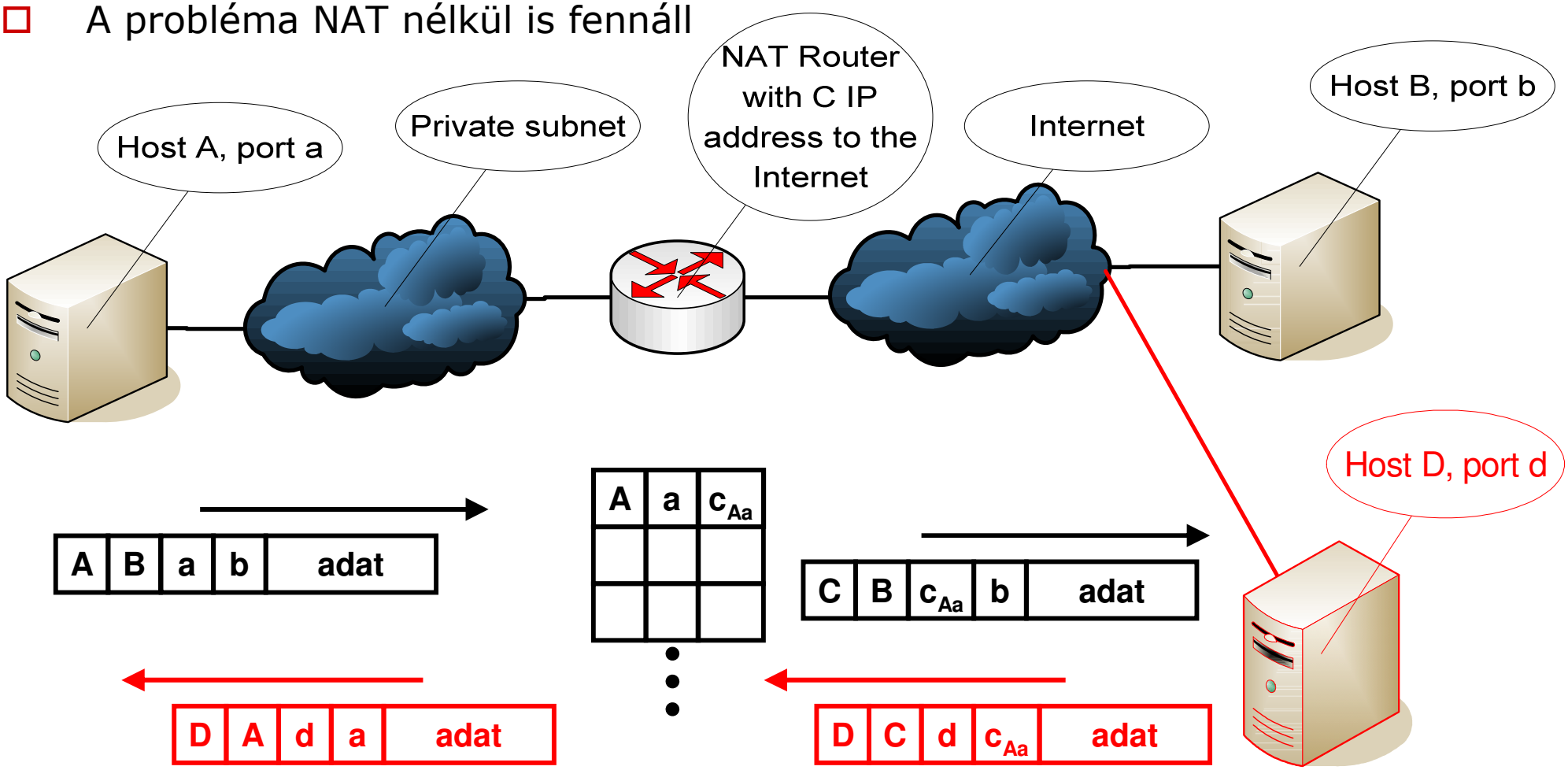
NAT – Hogyan működik valójában?

- Nem csak az IP-címeket, hanem a portokat is módosítjuk: Network Address Port Translation (NAPT)



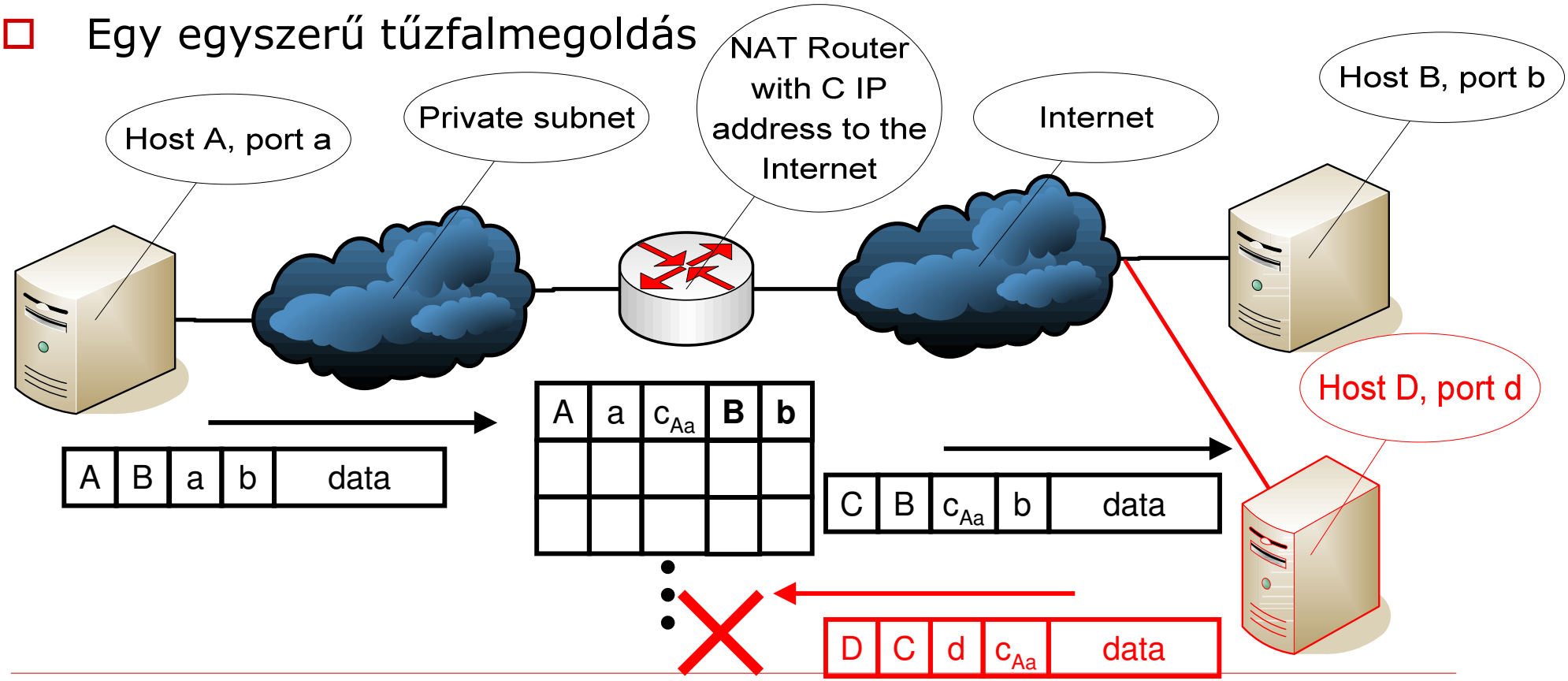
NAT – Biztonsági rés

- A NAT táblában a bejegyzések dinamikusan kerülnek hozzáadásra és törlésre
- Ha létezik c_{Aa} porthoz tartozó bejegyzés, és e portra bárki csomagot küld, akkor azt A állomás a portjára továbbítódik (port scan, Denial of Service)
- A probléma NAT nélkül is fennáll



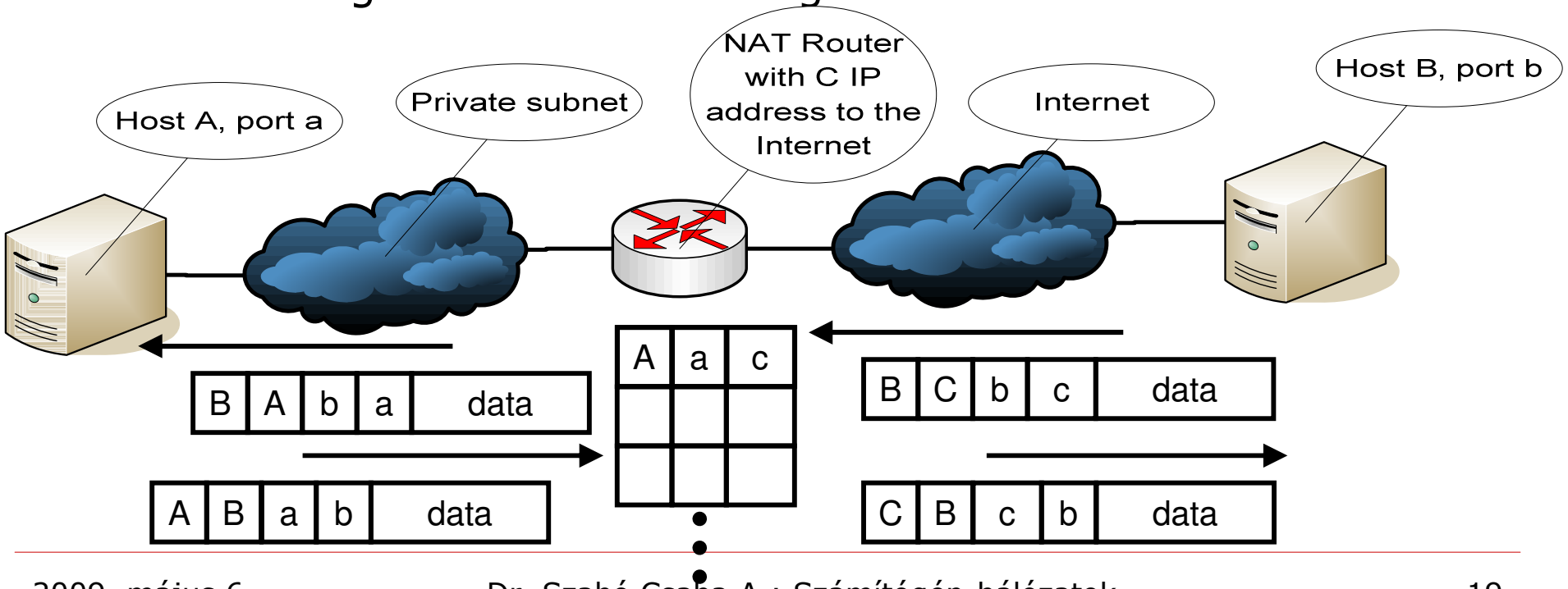
NAT – Biztonsági megoldás

- A NAT táblát bővíteni kell a külső fél IP és port címével
- A NAT router eldob minden más állomástól jövő csomagot
- Ezt a módszert *maszkolás*nak (*masquerade)* hívják
- Egy egyszerű tűzfalmegoldás



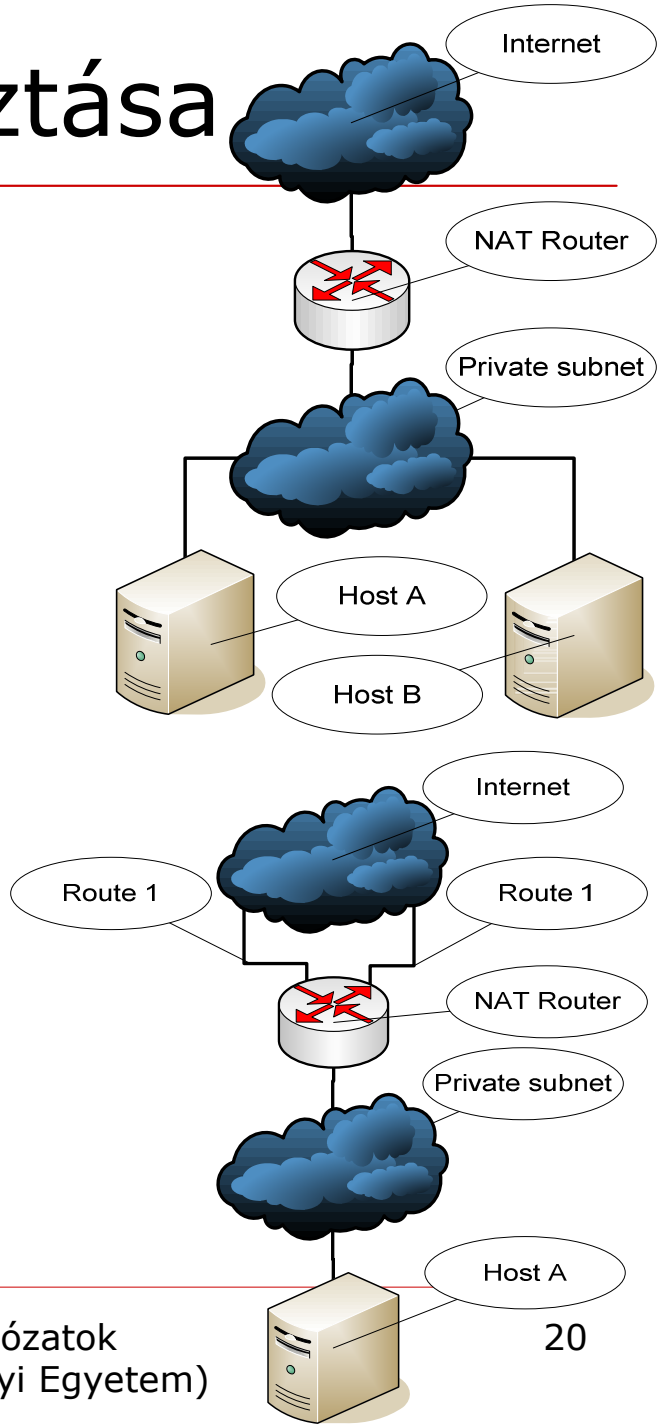
NAT – Virtual server

- Belső szerver közzététele statikus NAT tábla bejegyzéssel
- Úgy tűnik, mintha a szolgáltatás a NAT routeren lenne
- Két típus
  - Minden IP-forgalom továbbításra kerül
  - Csak az adott portra érkező forgalom kerül továbbításra
- A belső kiszolgálókat védi más forgalmaktól



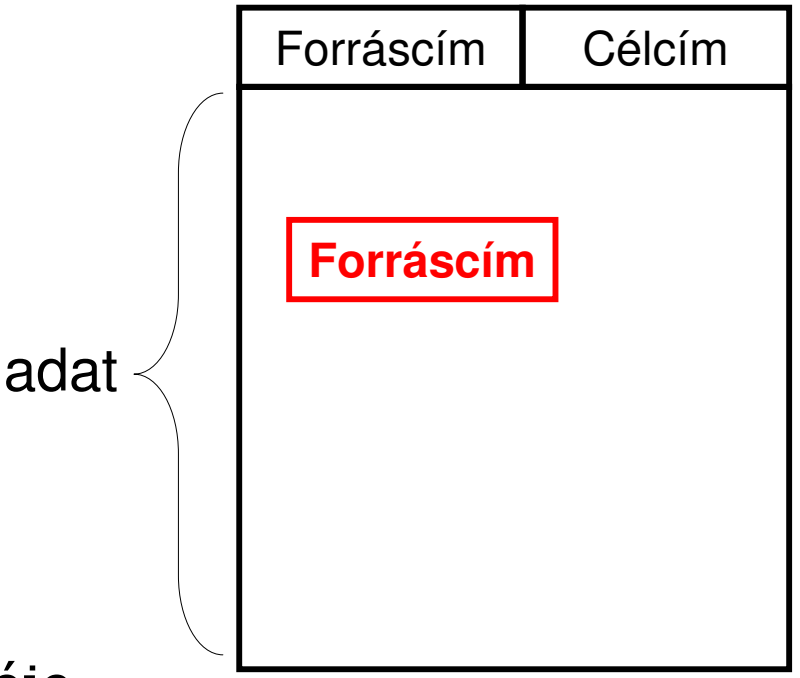
NAT – Erőforrások megosztása

- Több mint egy belső kiszolgáló
  - Terheléselosztás – a forgalom megosztása a belső szerverek között
  - Magas rendelkezésreállás – ha egy meghibásodik, a többi még kiszolgál
- Több mint egy külső interfész
  - Terheléselosztás – a több kapcsolaton
  - Magas rendelkezésreállás – ha egy kapcsolat meghibásodik, még mindig működhet



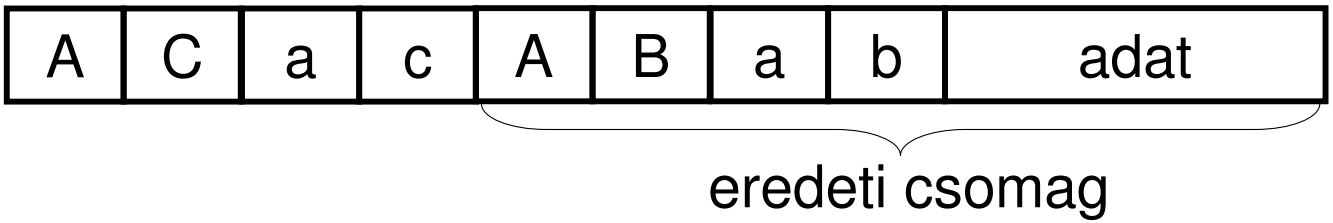
Problémák a NAT-tal

- Másodlagos kapcsolatok hibája
  - Pl. FTP (TCP 20/21: vezérlő-/adatcsatorna)
- IP-cím az alkalmazásrétegben ☹
  - Routing protokollok
  - DNS
  - FTP
  - H.323
  - SIP
  - HTTP (abszolút URL)
  - stb.
- Megoldás
  - Az alkalmazás-rétegbeli IP-cím cseréje
    - Az ISO OSI koncepció felrúgása ☹
  - Proxy alkalmazás a NAT routeren



NAT-problémák a biztonságos csatornákkal

- Nincs lehetőség a csatornák tartalmának, de általában még az IP-címek megváltoztatására sem ☹
  - IPSec (AH, ESP)
  - SSL/TLS (HTTPS, …)
- Megoldás
  - NAT-T (Traversal)
    - IETF RFC
    - Becsomagolás (encapsulation) és továbbítás az UDP 4500-as porton
    - A másik félnek is támogatnia lett a NAT-T-t a kicsomagoláshoz (decapsulation) és a becsomagolt válaszhoz



NAT összefoglalás

- Aggregálás egy multiplexelési szint elvesztésével (IP<->port)
- Beavatkozás a vég-vég kapcsolatba
- Körültekintéssel használható
  - Nem NATolható protokollok
  - Másodlagos kapcsolatok
  - Korlátozott tűzfalfunkció
- Kínában 3-4-szeres NATolás van