



HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

HÁLÓZATOK ALAPJAI ÉS ÜZEMELTETÉSE

IP címek kiosztása, címfordítás
2023. április 14.

Mészáros András

BME Hálózati Rendszerek és Szolgáltatások Tanszék
meszarosa@hit.bme.hu



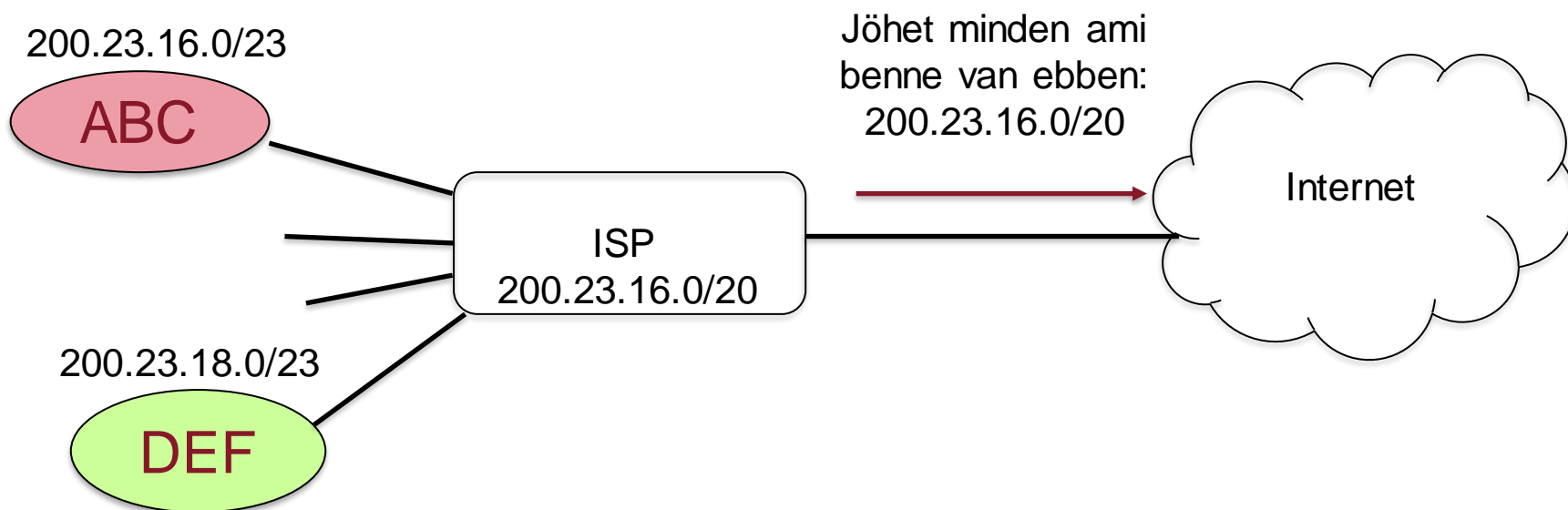
1. CIDR
2. Cím kiosztás, DHCP
3. Címfordítás
4. Datagram továbbítás

A fóliák elkészítéséhez felhasználtuk Jim Kurose és Keith Ross „Számítógép hálózatok működése” című könyvéhez készült fóliákat

- IPv4 címtartományok (hálózatok) kiosztása
 - Központi szolgáltató szervezetek döntenek (pl. IANA)
 - Osztályozási szabályokat figyelembe véve
 - Nehezen követhető, az egymást követő hálózatok tulajdonosainak semmi közük egymáshoz
- Problémák
 - Címek **pazarlása**
 - Óriási, kihasználatlan tartományok egyes cégeknek
 - Irányítási (routing) **táblák növekedése**
 - Nem lehet összefogni címeket
 - Minden hálózatot külön kell beletenni
 - A táblák frissítésének gyakorisága
 - Sok független hálózat
 - Sok változás
 - Sok frissítés

- CIDR: Classless InterDomain Routing
- Alapötlet
 - Az alhálózatokra osztás után a cím mellé a maszkot is kell tárolni
 - Nincs explicit határ a netid és a subnetid között
- Hálózatok kiosztása
 - Az IANA által kezelt összefüggő tartományok régió alapú szétosztása
 - Regional Internet Registries (RIR)
 - APNIC (Asia Pacific Network Information Centre) – Ázsia/Csendes Óceán
 - ARIN (American Registry for Internet Numbers) – Észak-Amerika, Afrika déli része
 - LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Latin-Amerika és a Karib-térség
 - RIPE NCC (Réseaux IP Européens) - Európa, Közel-kelet, Középázsia és Afrika északi része

- A regionális szervezetek összefüggő tartományokat tudnak adni az ISP-knek
- Az ISP-k összefüggő tartományokat tudnak adni a felhasználóiknak
- Irányítási táblákban összevonhatunk bejegyzéseket
 - Az alhálózatra bontás fordítottja

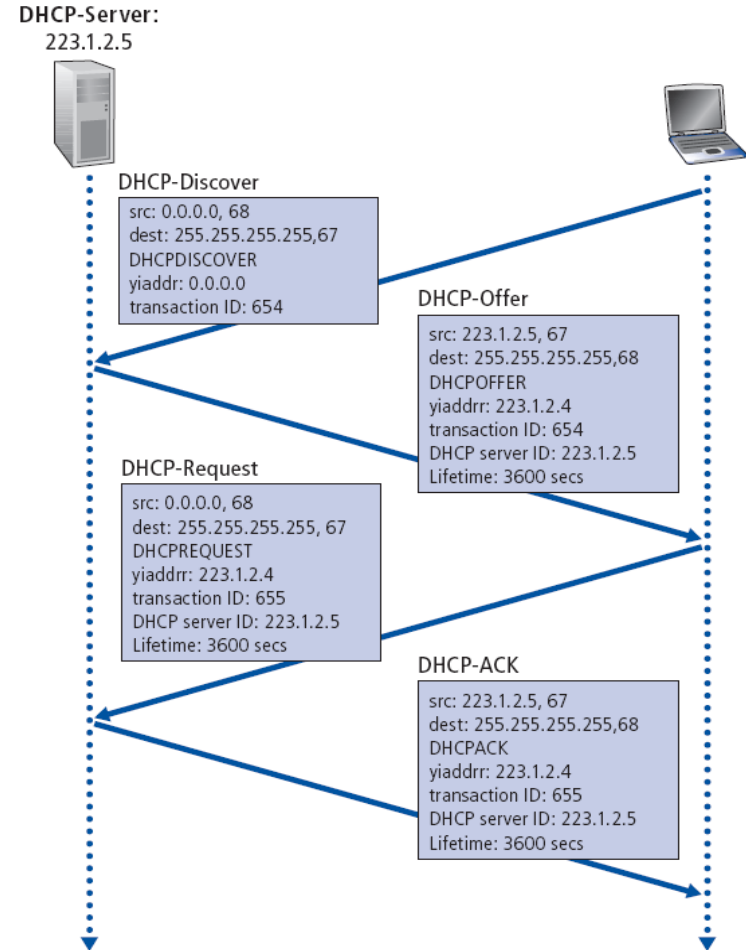


1. CIDR
2. Címkiosztás, DHCP
3. Címfordítás
4. Datagram továbbítás

- Kiindulás: megvannak az alhálózatok
- Következő lépés címek beállítása az interfészeken
- Manuális konfiguráció
 - IP cím
 - Maszk
- Automatikus konfiguráció
 - IPv4: DHCP - Dynamic Host Configuration Protocol
 - IPv6: a router képes automatikus címkonfigurációra (SLAAC – StateLess Address AutoConfiguration), vagy használhatja a DHCPv6-ot

- Routersen tipikusan ezt használjuk
- Szervereken tipikusan ezt használjuk
- Többféle hibát ejthetünk, például...
 - Hoszt interfészen beállított cím és maszk
 - 202.21.256.71, 255.255.250.0
 - Egy router két interfészen beállított címek és maszkok:
 - 203.55.22.57, 255.255.255.192
 - 203.55.22.24, 255.255.255.240
 - Két szomszédos hosztnál beállított címek és maszkok:
 - 204.88.54.15, 255.255.255.192
 - 204.88.54.72, 255.255.255.192
 - Router interfészen beállított cím és maszk
 - 205.66.87.48, 255.255.255.240
 - Router interfészen beállított cím és maszk
 - 206.44.76.95, 255.255.255.224

- Szerver-kliens alapú protokoll (alk. réteg)
 1. A hálózathoz csatlakoztatott hoszt címet kér: DHCP-Discover üzenetet küld
 - A teljes szórási címre (255.255.255.255)
 - A 67-es portra
 2. A DHCP szerver DHCP-Offer üzenettel válaszol és küld egy címet
 - A teljes szórási címre
 - A 68-as portra
 - Több szerver is lehet
 3. A hoszt elkéri a kapott címet DHCP-Request üzenetet küldve
 4. A DHCP szerver kiadja a címet a DHCP-Ack üzenettel



- A szerver nyilvántartja a kiadható és kiadott címeket
 - Különböző módokat használhat (pl. permanens, ideiglenes)
 - Meghosszabbíthatja a **kölcsönzést (lease)**
 - Újra kiadhatja a címet, miután lejár a kölcsönzés, vagy a kliens visszaadja
- További paraméterek
 - Alapértelmezett átjáró
 - DNS szerver

1. CIDR
2. Cím kiosztás, DHCP
3. Címfordítás
4. Datagram továbbítás

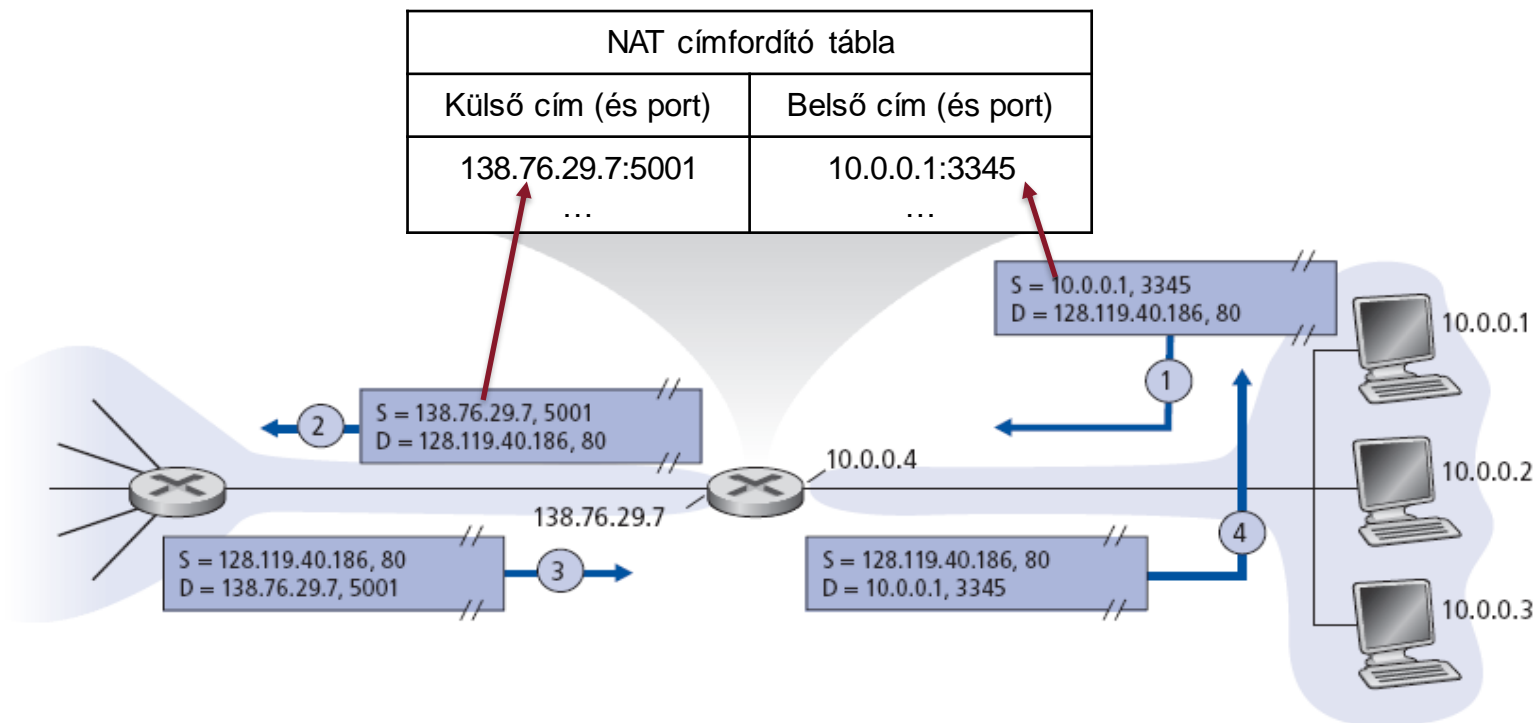
- **Motivációk**
 - Kifelé ugyanaz a cím látsszon, akkor is, ha belül változtatunk
 - Több hoszt lehessen ugyanazon a címen keresztül elérhető
 - Kevés az IPv4 cím
 - Privát címek a belső hálózatban
 - Egy hoszt belső (valódi) címe ne látsszon kifelé
- **Okok**
 - Csak egy címünk van, de több hosztunk
 - A hosztok címeit automatikusan osztottuk ki
 - ISP váltás miatt ne kelljen belül mindent átcímezni
 - Biztonság (minimális szint)

- **NAT - Network Address Translation**

- A belső cím csak belül egyértelmű
- Az Internethez hozzákapcsoló router **ki- és visszacseréli** a belső címet egy globálisan egyértelmű címre
- Szükség esetén a router a szállítási rétegbeli azonosítókön is változtat
- A router egy **címfordító (transzlációs) táblát** használ

- **A címfordítás beállítása**

- Statikusan – kézzel hozzárendeljük
 - Szükség esetén a portokat is átírjuk
- Dinamikusan – a router rendel hozzá egy poolból
 - Szükség esetén a portokat is átírja



- A LAN-t elhagyva **azonos forráscím** az összes csomagban (a példában 138.76.29.7)
- Megkülönböztetés a portszám alapján

- A LAN-ban a **valódi címeket** használjuk
- A példában ez a 10.0.0.0/24 privát tartomány

- **Megvalósítás a routerben**

- Külső és belső oldal azonosítása
- Az Internet felé kimenő datagramokban a küldő cím lecserélése
- Dinamikus esetben az aktuális címfordítás részleteinek megjegyzése
 - Belső IP cím és port
 - Külső IP cím és port
- Az Internet felől jövő datagramokban a célcím lecserélése

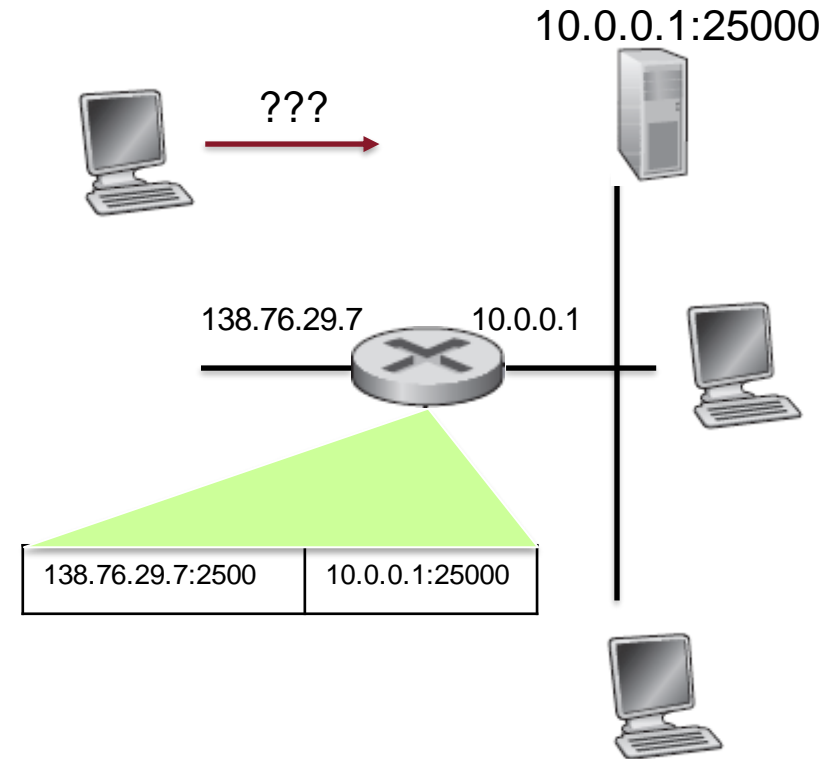
- **Megjegyzések**

- A 16 bites port azonosítók miatt sok hoszt lehet egy cím mögött
- Nem feltétlenül kell a portot is fordítani

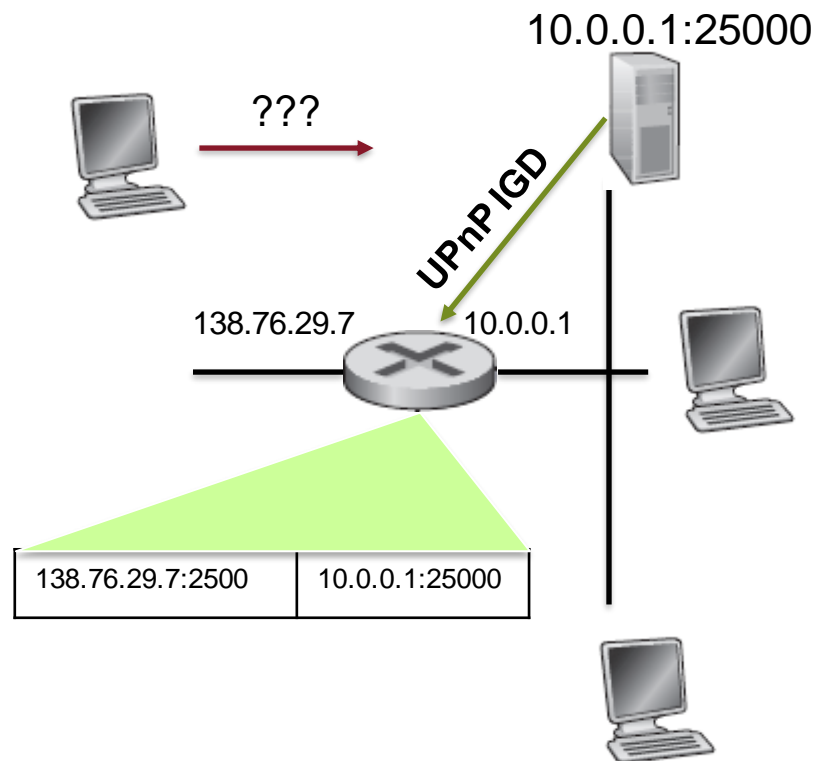
- **Ellentmondások**

- A router a hálózati rétegben dolgozik, nem kellene a portokhoz nyúlnia
- Sérül a végponttól-végpontig (end-to-end) küldött datagram elve
 - Figyelembe kell venni egy alkalmazás fejlesztésekor is

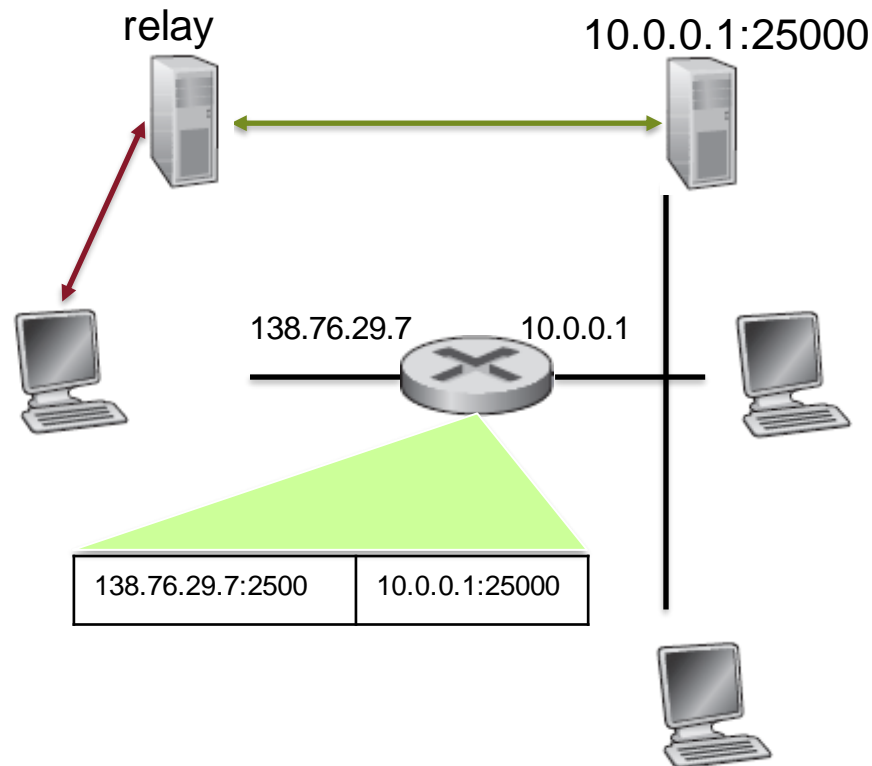
- NAT traversal
- Probléma
 - A kliens a 10.0.0.1 (valódi) címmel rendelkező serverhez akar kapcsolódni
 - Ez a cím privát cím, amit tipikusan nem lehet elérni az Internet felől (csak lokálisan alkalmazzuk)
 - A kifelé látszó egyetlen cím a 138.76.29.7
- 1. megoldás: statikus NAT
 - A server valódi port-cím páriját egy kívülről látható port-cím párra fordítjuk
 - Például a 138.76.29.7: 2500-ra érkező datagramok a 10.0.0.1:25000 felé mennek tovább



- 2. megoldás: statikus NAT – automatikus konfigurációval
 - A címfordító táblát beállíthatná a szerver is
 - Az Universal Plug and Play (UPnP) Internet Gateway Device (IGD) Protocol a NAT mögötti hosztoknak lehetővé teszi
 - A külső cím megismerését
 - A fordítási tábla megismerését
 - A fordítási tábla módosítását



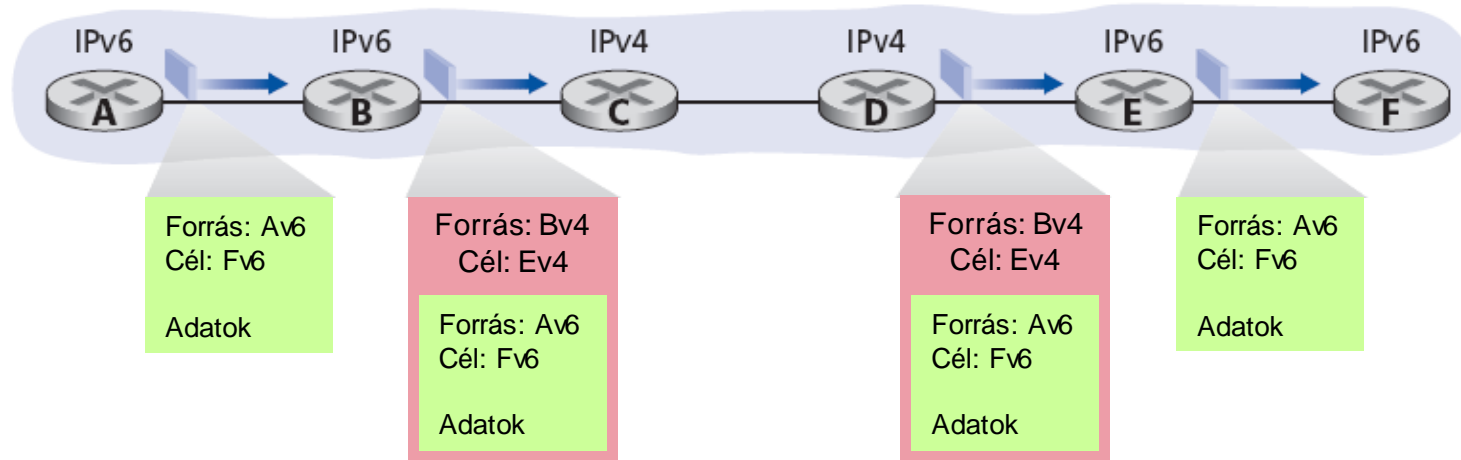
- 3. megoldás: köztes szerver használata – relay
 - A NAT mögött lévő szerver kapcsolódik a köztes szerverhez (relay)
 - A kliens a köztes szervert szólítja meg
 - A relay ismeri a valódi szerver nyilvános címét és portját
 - A relay továbbítja a kliens csomagjait a valódi szerver felé



- Large Scale NAT (LSN) megoldások
 - NAT az ISP hálózatán belül is
 - Így már két helyen is átalakítják az eredeti címet
- A NAT csak ideiglenesen megoldás az IPv4 kimerülésre, végső megoldás az IPv6
- Két külön világ, ami jelenleg párhuzamosan működik
- Sok routerben és hosztban mindkettő elérhető (dual stack)
- Hogyan lehet átjárni közöttük?
 - NAT64: IPv6 cím fordítása IPv4 címre (és vissza)
 - Alagutazás (tunneling): átbújtatás az IPv4 hálózatrészen



- **Megvalósítás**

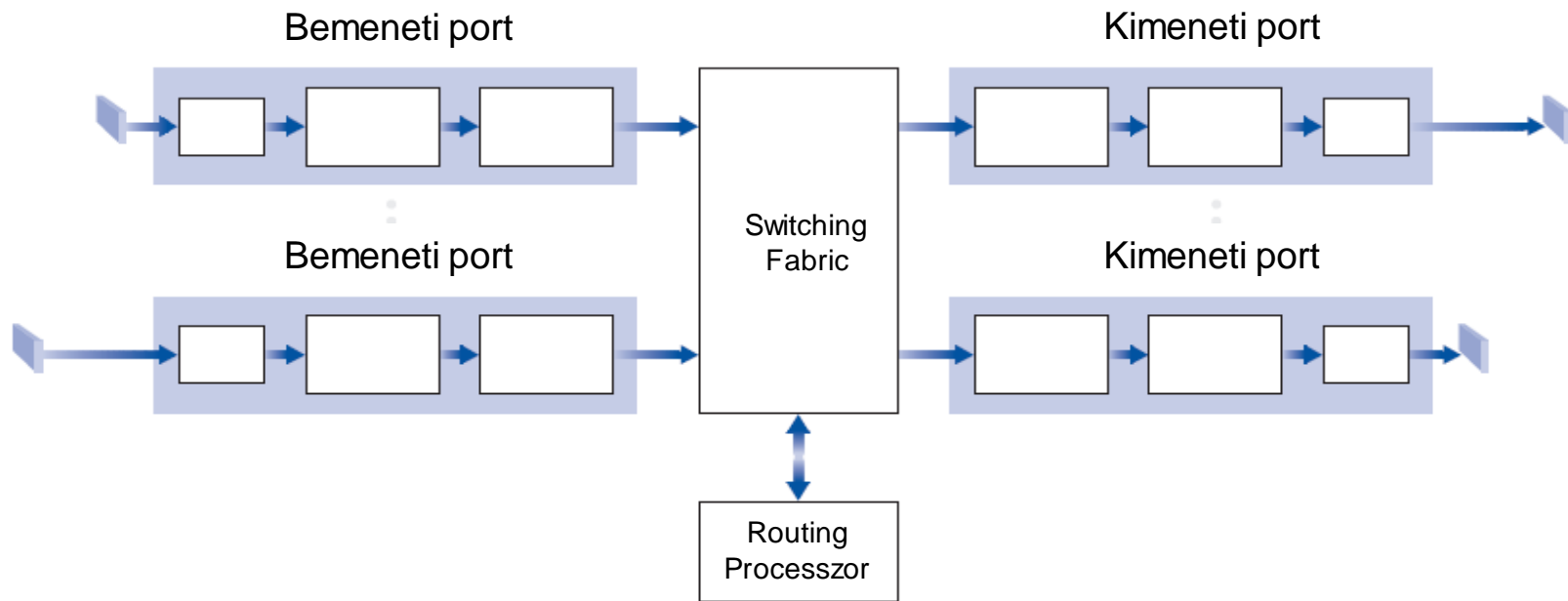


- Az IPv6 datagramot beletesszük egy IPv4 datagramba
- Átküldjük az alagúton
- A túloldalon kivesszük az IPv4-ből és továbbítjuk IPv6 datagramként

1. CIDR
2. Cím kiosztás, DHCP
3. Cím fordítás
4. Datagram továbbítás

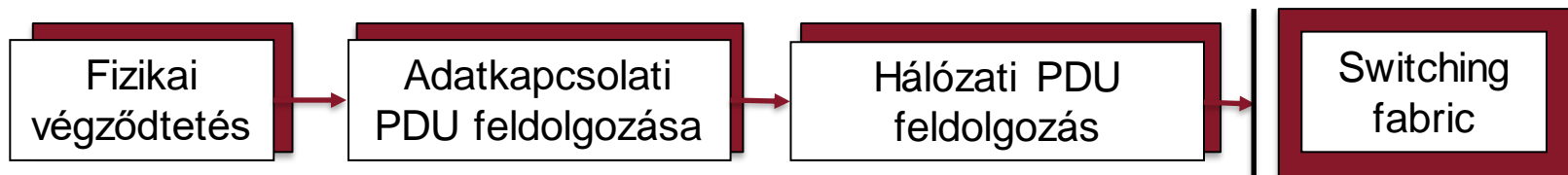
- Két fő funkció

- Útmeghatározó protokollok és algoritmusok futtatása
- Az egyik bemeneten beérkező csomag továbbítása egy kimenetre

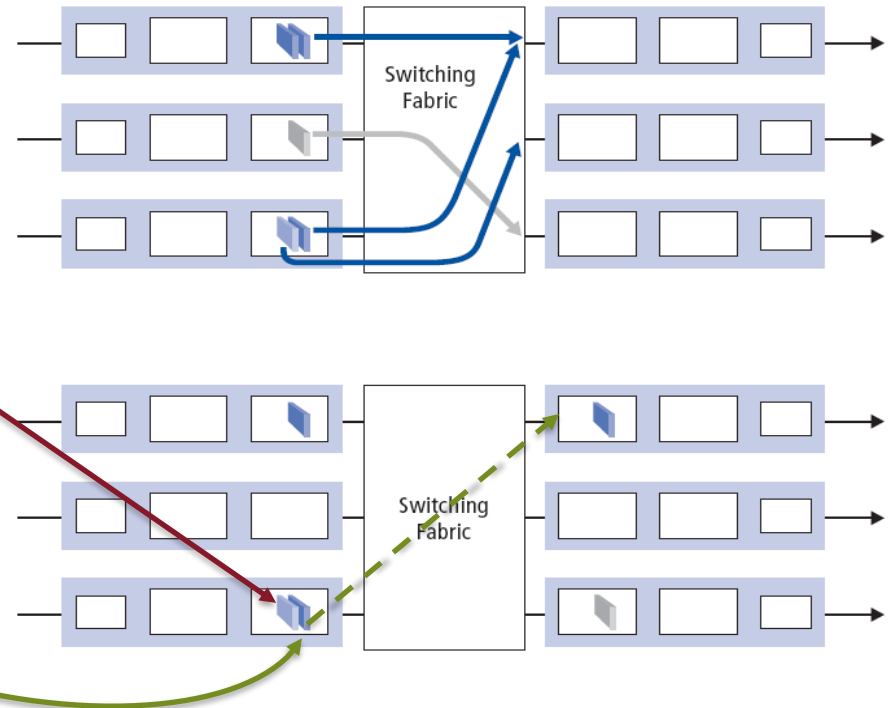


- Hogyan kerül a routerhez a datagram?
 - A hoszt a cím és a maszk alapján eldönti, hogy a cél vele egy hálózaton van-e
 - Ha igen, szomszédos hosztnak küld
 - Ha nem, akkor egy átjárón át az Internet felé
 - Alapértelmezett átjáró – **default gateway**
 - A hosztnál meg kell adni, hogy lehessen indítani a datagramot ebbe az irányba
 - Az első router hoszt felé eső interfésze
 - Egy hálózatban van a hoszttal
- A router a célcím alapján küldi tovább
 - Közvetlenül továbbítható egy hozzákapcsolt hálózatba
 - Távoli hálózat esetén az irányítási tábla bejegyzései alapján

- Fizikai réteg
 - Vezeték végződtes
 - Bitszintű vétel
- Adatkapcsolati réteg (pl. Ethernet)
 - Szomszédos hálózatelemtől kapott PDU
- Hálózati réteg
 - datagram fejléc feldolgozás, NAT
 - Továbbítási irány meghatározás az irányítási (routing) tábla alapján
 - Sorba állítás
- Sebesség cél
 - A feldolgozás sebessége legalább az adatok érkezési sebessége legyen
- Sorbanállás, ha a kapcsológép (switching fabric) nem elég gyors

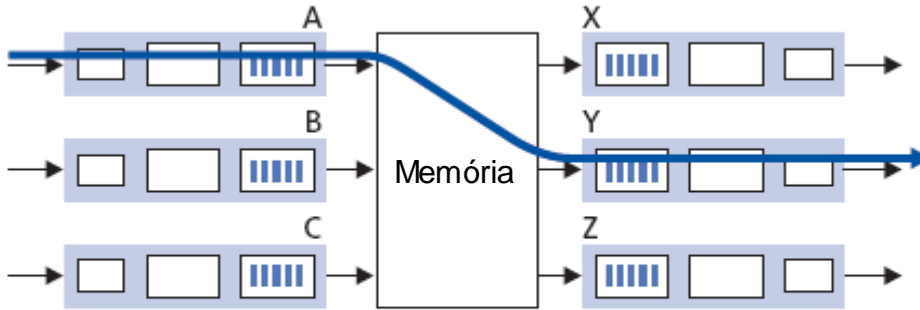


- Sorbanállás, pufferekés, ha a kapcsológép nem elég gyors az összes bemenethez képest
 - Késleltetés
 - Csomagvesztés
- Head Of Line (HOL) blokkolás
 - Lehetne továbbítani a datagramot, de feltartja egy másik
 - Ez a másik a kimenet foglaltsága miatt a kapcsológépre vár

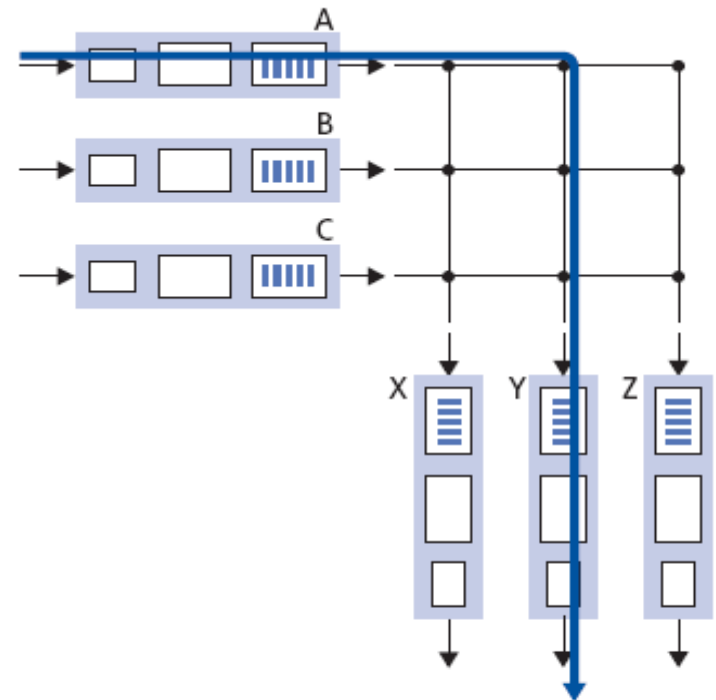


KAPCSOLÓGÉP ELRENDEZÉSEK

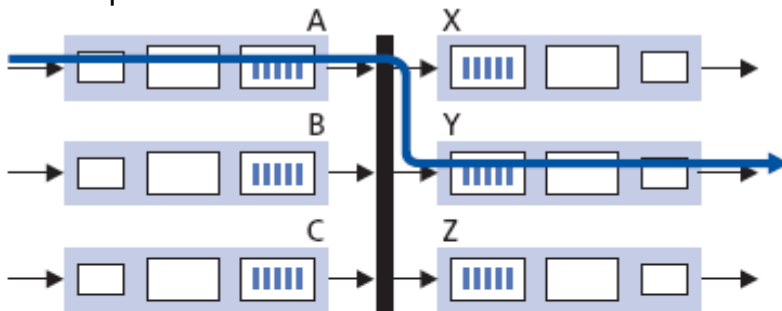
Memória-alapú



Keresztkapcsoló



Sín-alapú

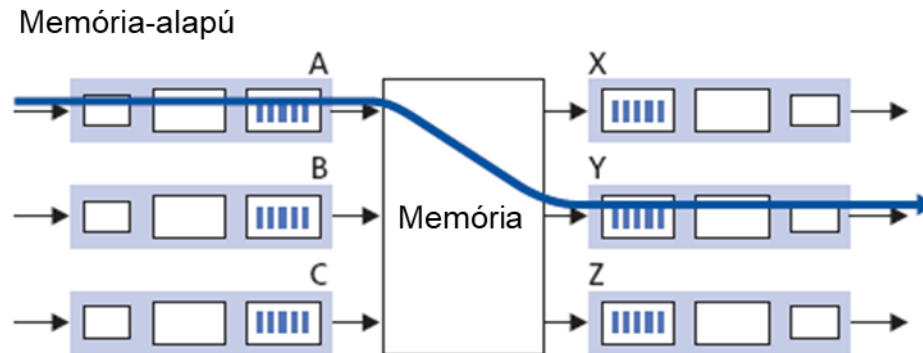


Bemeneti port

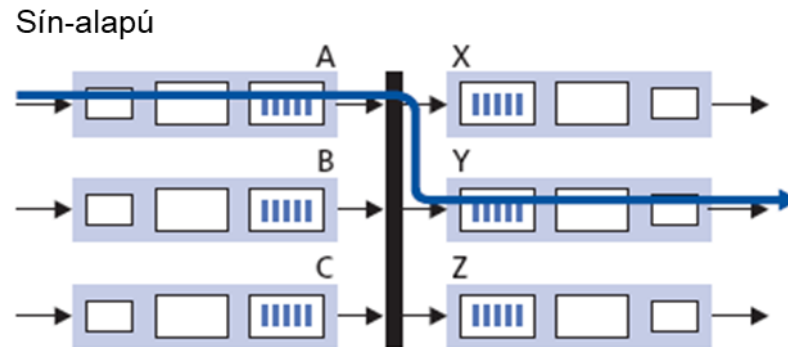


Kimeneti port

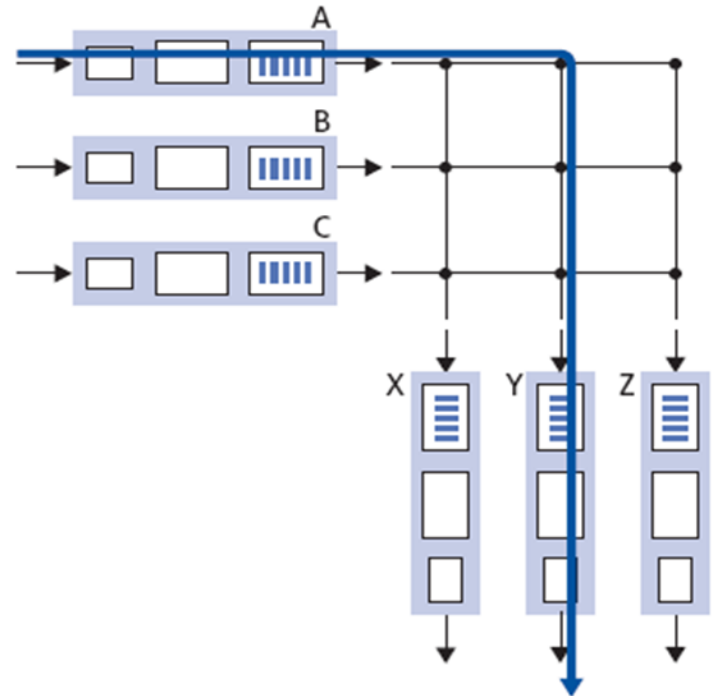
- Első generációs routerekben
- Hagyományos számítógépek a CPU felügyelete alatti kapcsolással
- Csomagok beírása a memóriába
- A kapcsolási sebességet a memóriaelérés sávszélessége határozza meg
 - datagramonként két memóriaelérés



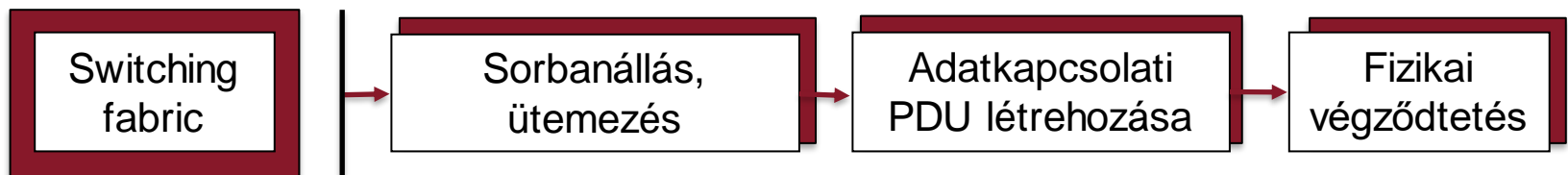
- A bemeneti port memóriájából a kimeneti port memóriájába egy közös sínen (bus) jut el a datagram
- A kapcsolási sebességet a sín sávszélessége korlátozza
- A teljesen osztott erőforrás szűkös lehet



- Crossbar kapcsolás
- A cél átlépni a sínek sávszélességéből adódó korlátokat
- Minden bemenet közvetlenül köthető minden kimenetre
 - Banyan hálózatok
 - Eredetileg többprocesszoros rendszerek processzorainak összekapcsolására
- Gyorsítás
 - a datagramok fix méretű cellákra tördelése
 - a cellák kapcsolása a kapcsolóban
- Akár több száz Gbps



- Sorbanállás, pufferezés, ha a kimenő link nem elég gyors
 - Késleltetés
 - Csomagvesztés
- Ütemezés
 - A következőként elküldendő datagram kiválasztása
- Adatkapcsolati réteg (pl. Ethernet)
 - Szomszédos hálózatelemnek küldendő PDU
- Fizikai réteg
 - Vezeték végződés
 - Bitszintű adás





HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

