BMEVIHIMA00 Hálózati technológiák integrációja

Számítógép-hálózatok

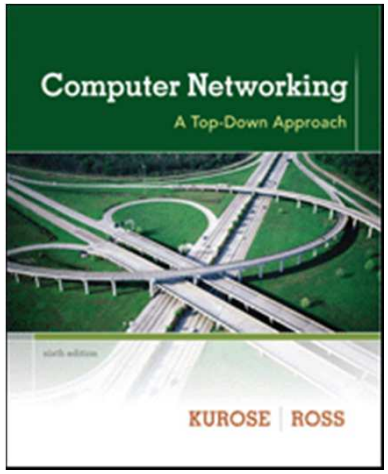
Áttekintő összefoglalás

Jakab Tivadar
jakab@hit.bme.hu

Budapest,
2020.05.18.

A számítógép-hálózatos alapok áttekintő összefoglalása

J. Kurose és K. Ross
Számítógép-hálózatok működése
című könyvének angol nyelvű oktatástámogató
anyagai alapján készült:
https://wps.pearsoned.com/ecs_kurose_compnetw_6/216/55463/14198700.cw/index.html



A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) in substantially unaltered form, that you mention their source (after all, we'd like people to use our book!)
- If you post any slides in substantially unaltered form on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

Computer Networking: A Top Down Approach 6th edition. Jim Kurose, Keith Ross Addison-Wesley, July 2007.

TCP/IP PROTOKOLL STACK

Réteg	Kommunikáló entitások (végpontok)	PDU	Főbb jellegzetességek	Példák
alkalmazási	alkalmazások	üzenet	kliens-szerver, peer-to-peer	HTTP
transzport	szoftver-folyamatok	szegmens	megbízható (adatvesztés nélküli, sorrendhelyes), nem megbízható, forgalomszabályzás, torlódáskezelés,	TCP, UDP
hálózati	hosztok (routerek közreműködésével)	datagram	címzés, útvonalválasztás, továbbítás	IP
adatkapcsolati	szomszédos L3 hálózatelemek (hosztok, routerek, L2 switchek közreműködésével)	keret	[Ethernet:] megbízhatatlan, összeköttetés nélküli szolgáltatás, kapcsolás, önálló tanulás	Ethernet
fizikai	szomszédos L2 hálózatelemek interfészei (L1 hálózatelemek közreműködésével)	bit	vezetékes, vezetéknélküli, dedikált vagy osztott média, kapacitás, hatótávolság	DF optika, WiFi

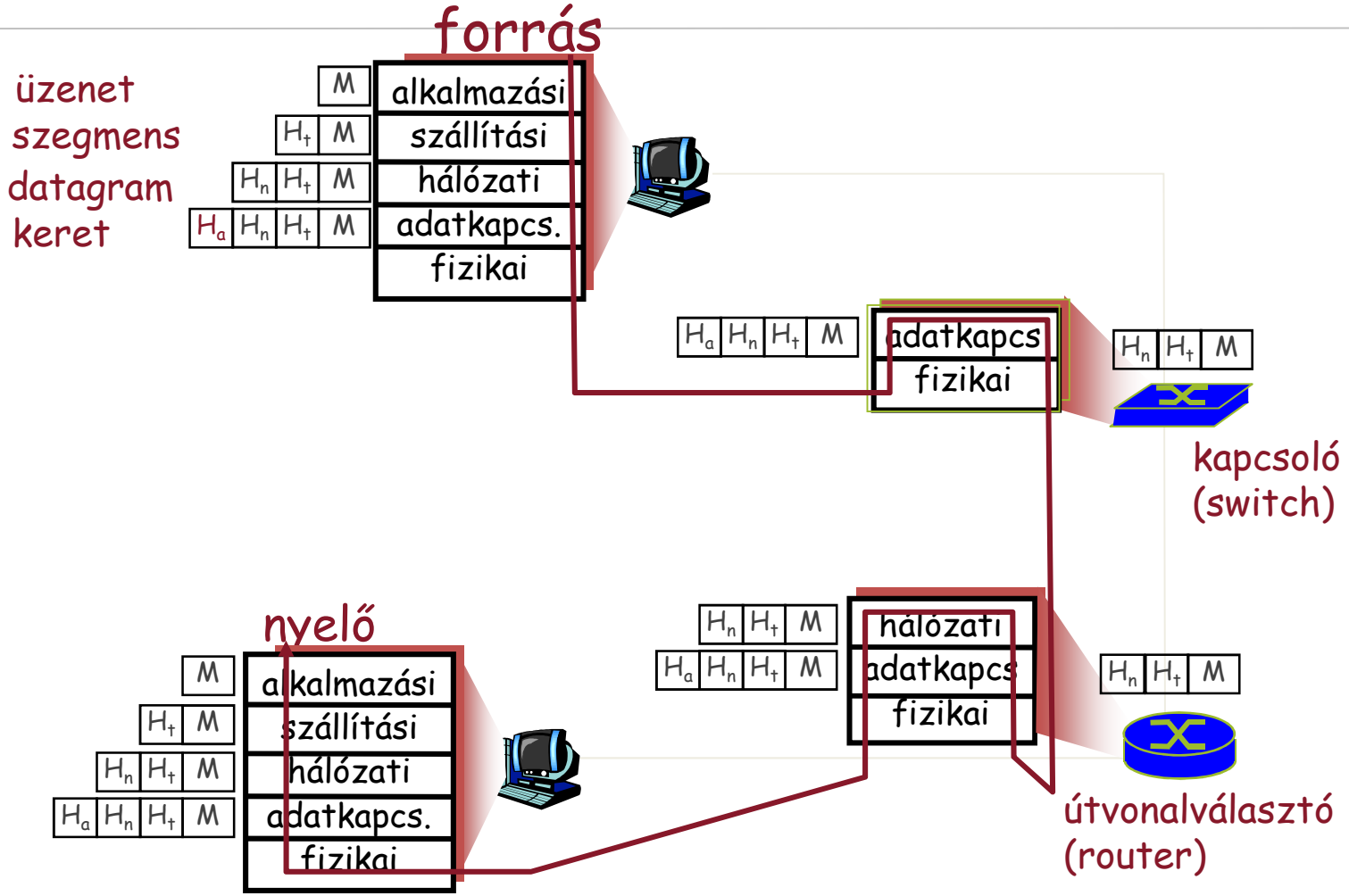
A **kommunikáló végpontok** az adott réteg PDU-jának hasznos tatalmára (adat) alapozottan (encapsulation) valósítanak meg felettes réteg funkciókat

A **közreműködő csomópontok** az adott réteg PDU-jának rétegspecifikus információira (pl. fejrész) alapozottan valósítanak meg adott rétegbeli funkciókat.

PDU – Protocol Data Unit

DF – Dark Fiber)sötét szálas optika, a fényvezető szálban egyet optikai csatornát szállít

BEÁGYAZÁS



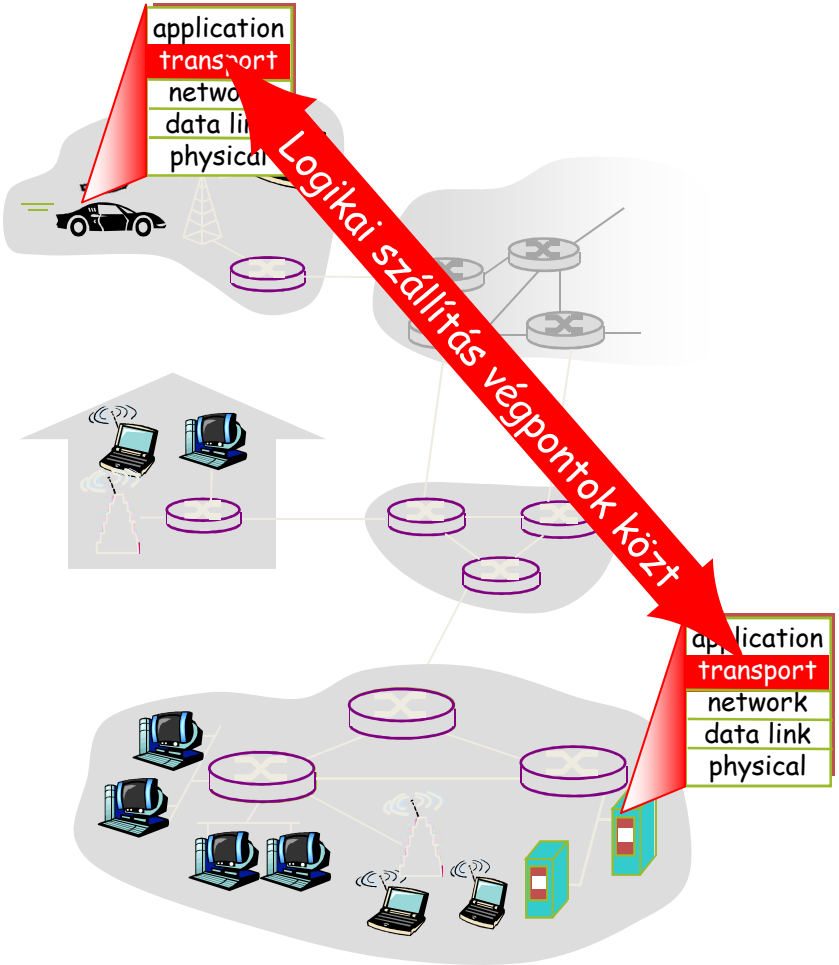
Beágyazás: rétegspecifikus információk (*header*) hozzáadása alapvető rétegfunkciók megvalósításához

Hasonló jellegű, de alapvetően más tartalmú célú és tartalmú fogalom: *alagutazás*: azonos rétegen (L3) belüli becsomagolás (pl. IPv4 IPv6-ban vagy fordítva), két hálózat (*network*) transzparens összekapcsolására

Néhány transzport réteg vonatkozás áttekintése:
Nyalábolás és nyalábbontás, UDP, TCP QUIC

SZÁLLÍTÁSI SZOLGÁLTATÁSOK ÉS PROTOKOLLOK

- A különböző hosztokon futó alkalmazások szoftver-folyamatai közti *logikai kommunikációt* biztosítják
- A szállítási protokollok a végponti rendszerek futnak
  - küldő oldal: az alkalmazásprotokoll üzeneteit szegmensekre darabolva adja át a hálózati rétegnek
  - fogadó oldal: összeállítja az eredeti üzenetet a szegmensekből, és átadja az alkalmazási rétegnek
- Nemcsak egyet szállítási protokoll áll az alkalmazások rendelkezésére
  - Internet: TCP és UDP (+QUIC)



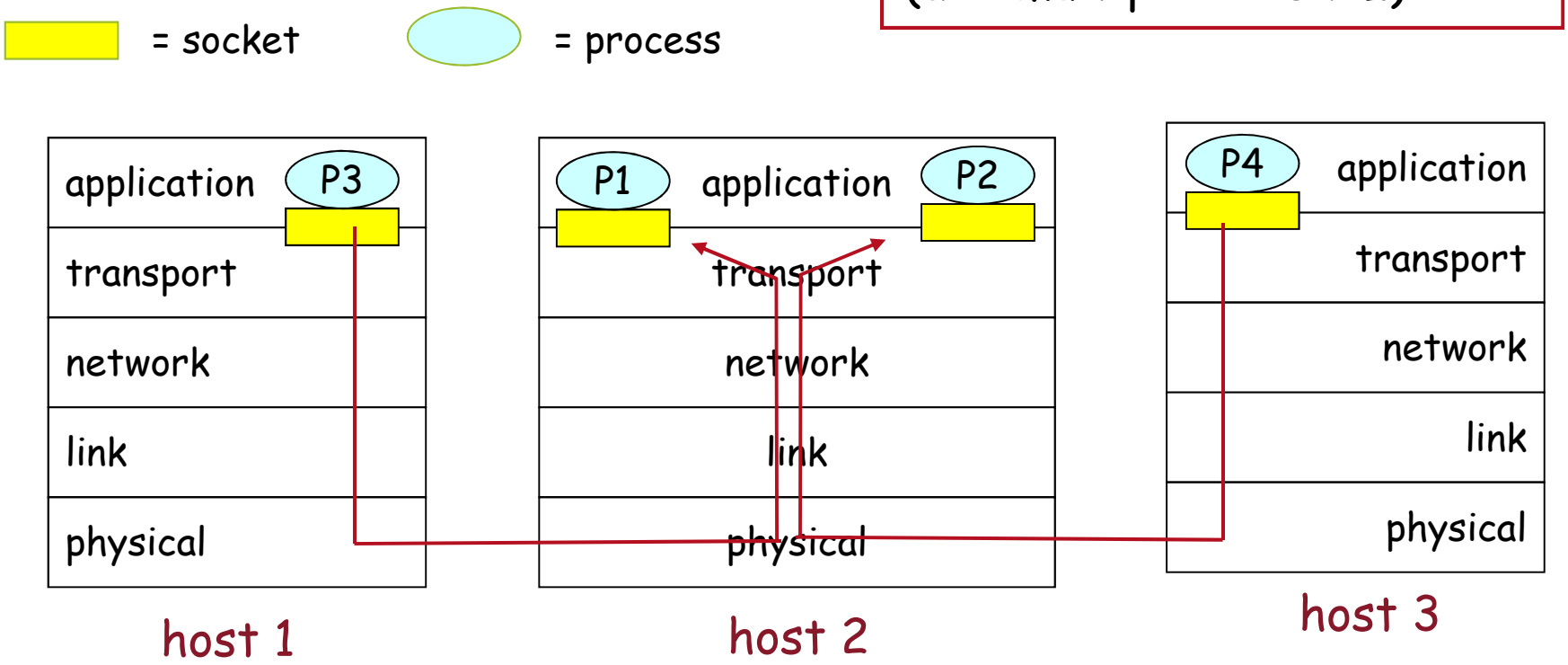
NYALÁBOLÁS/NYALÁBBONTÁS

Demultiplexlés a fogadó hosztnál:

a vett szegmensek továbbítása a megfelelő socketnek

Multiplexelés a küldő hosztnál:

különböző socketek adatainak összegyűjtése, becsomagolása, fejlécezése (a demultiplexeléshez)



HOGYAN MŰKÖDIK A DEMULTIPLEXELÉS

- a host az IP datagrammot
  - minden datagramnak van forrás és cél IP-címe,
  - minden egyes datagram pontosan 1 szállítási réteg szegmenst hordoz
  - minden szegmensnek van forrás és cél portszáma
- a host az IP-cím és a portszám alapján irányítja a megfelelő sockethez

a TCP/UDP szegmens szerkezete

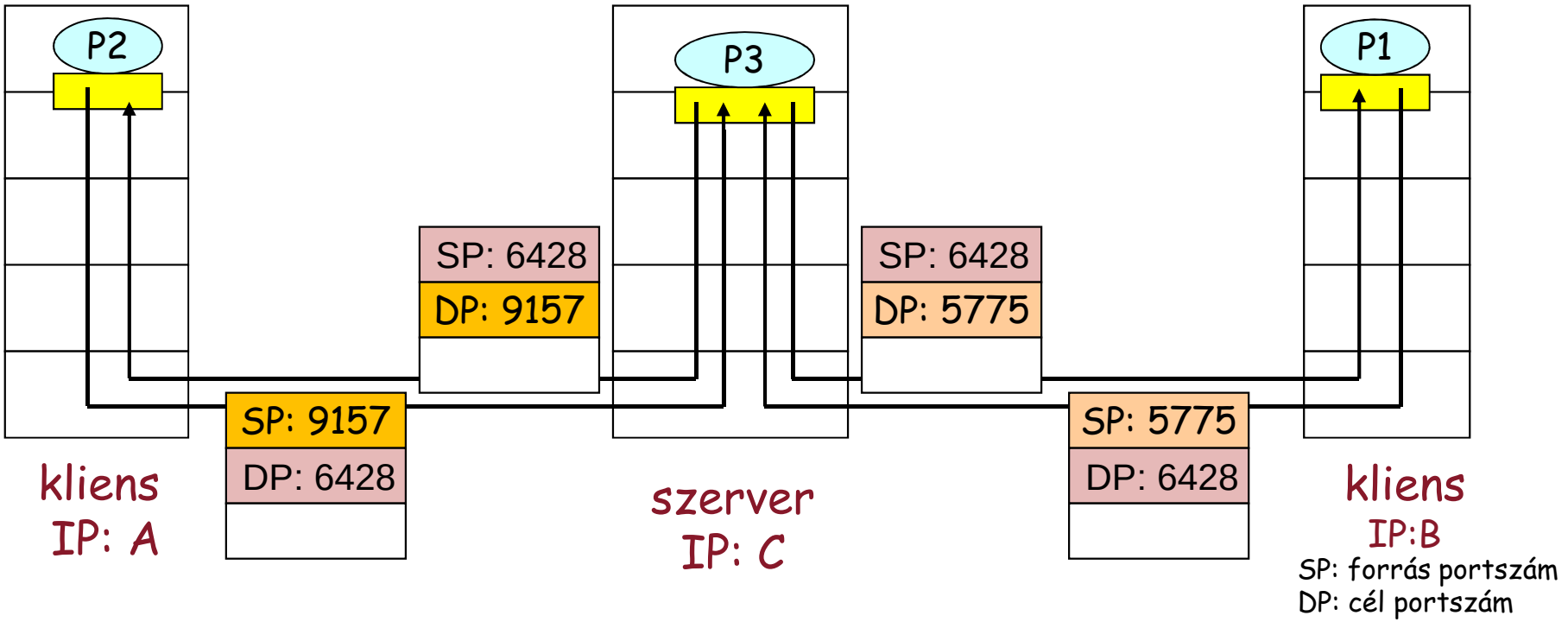
KAPCSOLATMENTES DEMULTIPLEXÁLÁS

- Sockets létrehozáskor portszám-hozzárendelés:
- UDP socketet egy értékpár azonosítja:

(cél IP cím, cél portszám)

- Amikor a host vesz egy UDP szegmenst:
  - megvizsgálja a szegmensben szereplő cél portszámot, és
  - az ennek megfelelő portszámú socketnek adja át a szegmenst
- A különböző forrás IP-című és/vagy forrás portszámot tartalmazó cél portszámuk alapján ugyanahhoz a sockethez kerülnek

KAPCSOLATMENTES DEMULTIPLEXÁLÁS (FOLYT.)



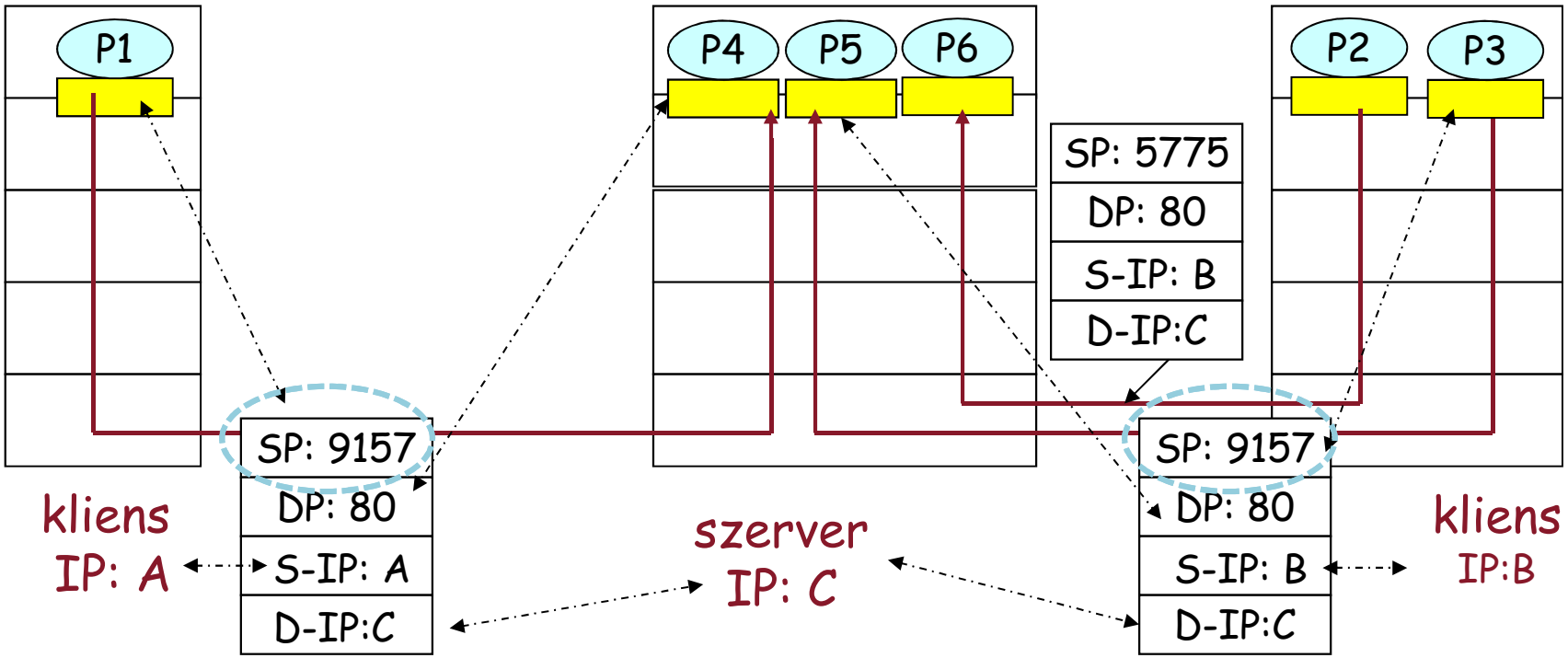
A forrás portszám SP adja meg a "válaszcímet"
(a szerver oldalon a vett SP, DP megcserélése a válaszban)

KAPCSOLAT ALAPÚ DEMULTIPLEXÁLÁS

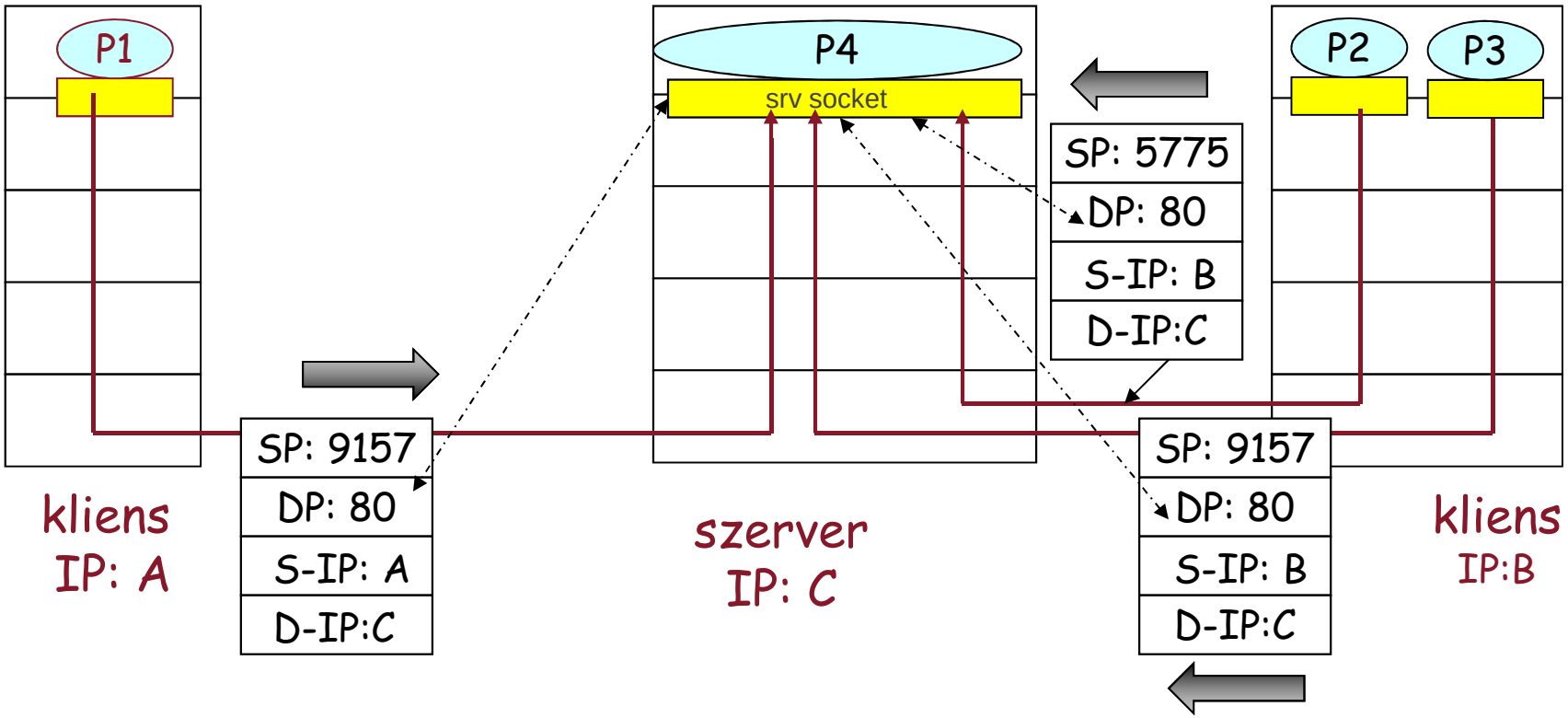
- A TCP socketet egy értéknégyes azonosítja:
  - forrás IP cím
  - forrás portszám
  - cél IP cím
  - cél portszám
- A vevő oldali host mind a négy értéket felhasználja a szegment megfelel sockethez továbbítására

- Egy szerver szerepű host egyszerre számos TCP socketet kezelhet:
  - minden egyes socketet saját értéknégyese azonosít
- Egy web szerver más-más socket keresztül kezeli az egyes éppen kapcsolódó klienseket
  - a nem perzisztens HTTP külön socketen keresztül kezel minden egyes kérést

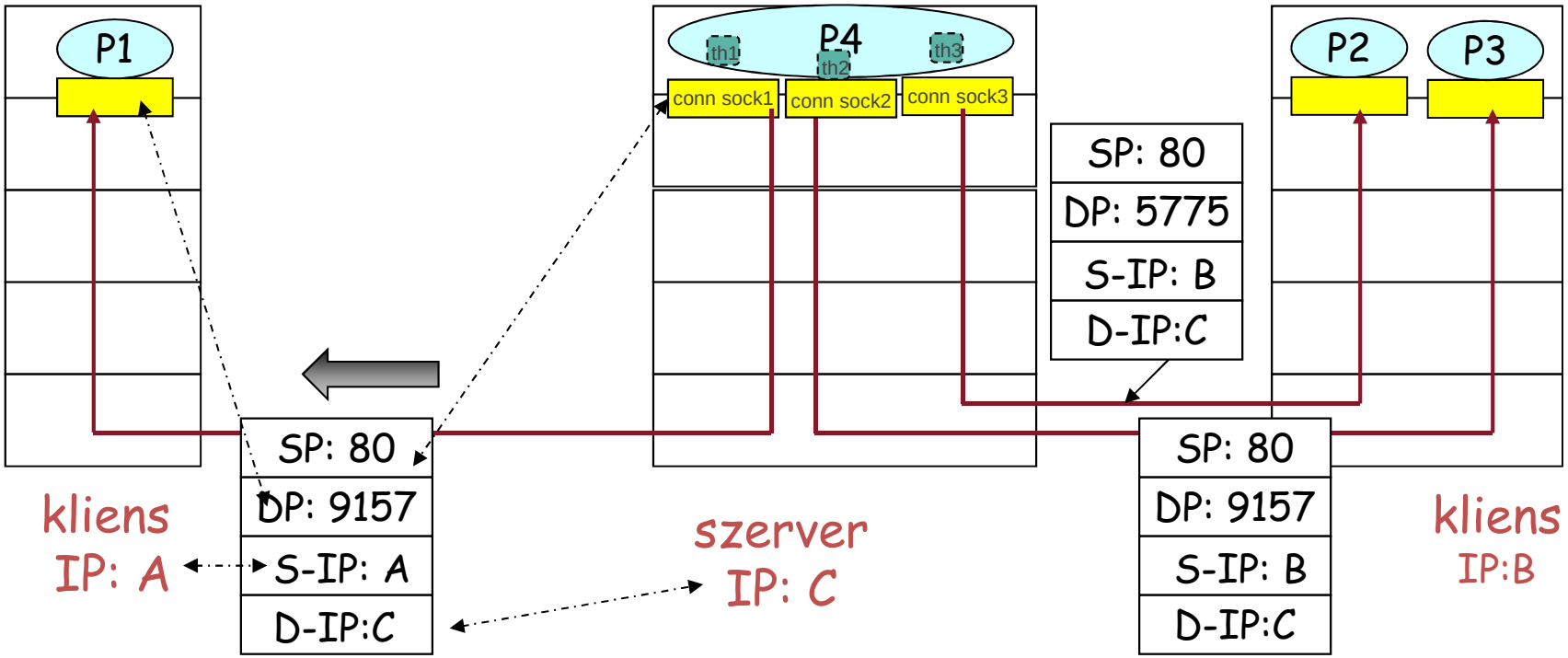
KAPCSOLAT ALAPÚ DEMULTIPLEXÁLÁS (FOLYT.)



KAPCSOLAT ALAPÚ DEMULTIPLEXÁLÁS: WEB SZERVER



KAPCSOLAT ALAPÚ DEMULTIPLEXÁLÁS: WEB SZERVER (FOLYT.)



UDP: USER DATAGRAM PROTOCOL [RFC 768]

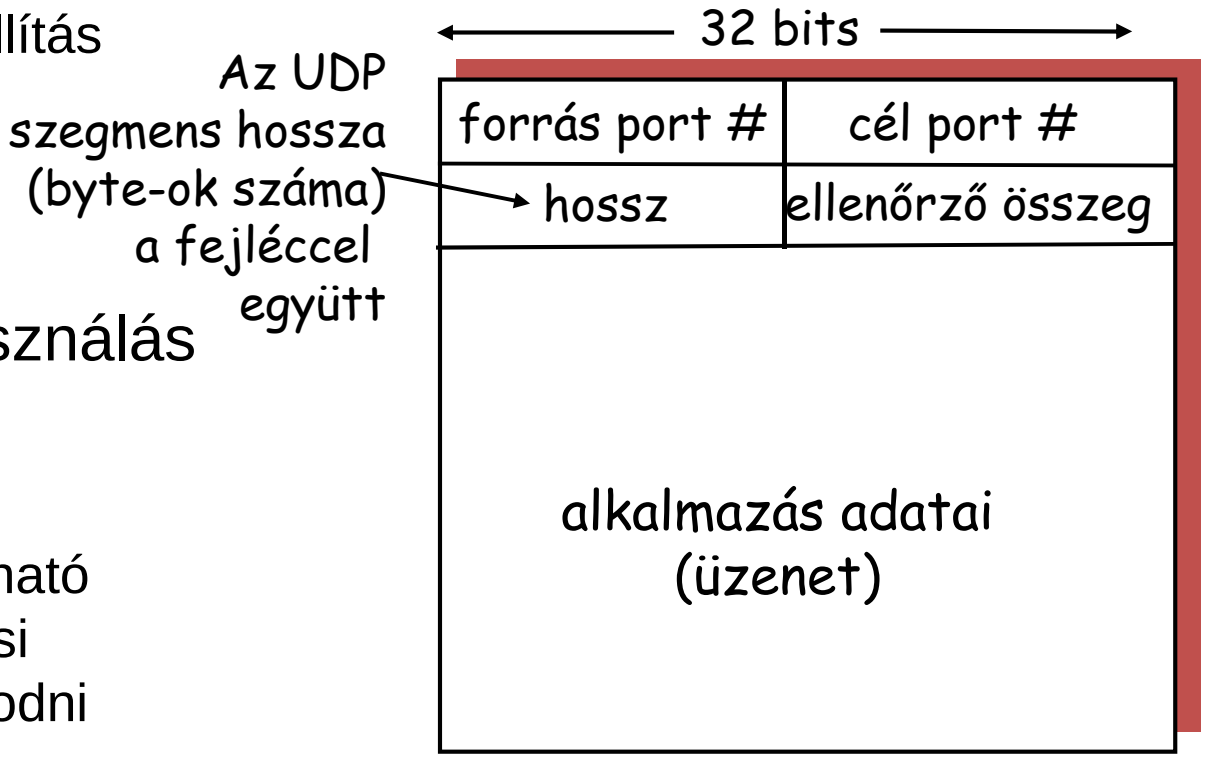
- “semmi fodor,” “lecsupaszított” Internet transzport protokoll
- “best effort” service, UDP segments may be:
  - lost
  - delivered out of order to app
- *összeköttetés nélküli*
  - nincs „kézfogás” az UDP küldő és fogadó oldala között
  - minden egyes UDP szegmenst kezelése a többitől független

Miért kell az UDP (is)?

- nem szükséges összeköttetés felépítés (ami növeli a késleltetést)
- egyszerű: nincs kapcsolatállapot-kezelés sem a küldő, sem a fogadó oldalon
- kis méretű szegmensfejléc
- nincs torlódáskezelés: az UDP a lehető leggyorsabban továbbítja az adatokat

UDP: BŐVEBBEN

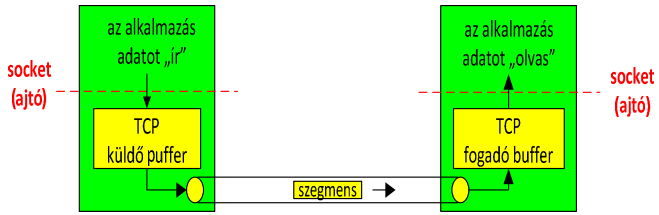
- Gyakori alkalmazása a multimédia folyam szállítás (streaming)
  - veszteségtűrő
  - rate sensitive
- további UDP felhasználás
  - DNS
  - SNMP
- Az UDP feletti megbízható átvitelről az alkalmazási rétegben kell gondoskodni
  - pl. alkalmazás specifikus hibakezelés



UDP szegmens formátuma

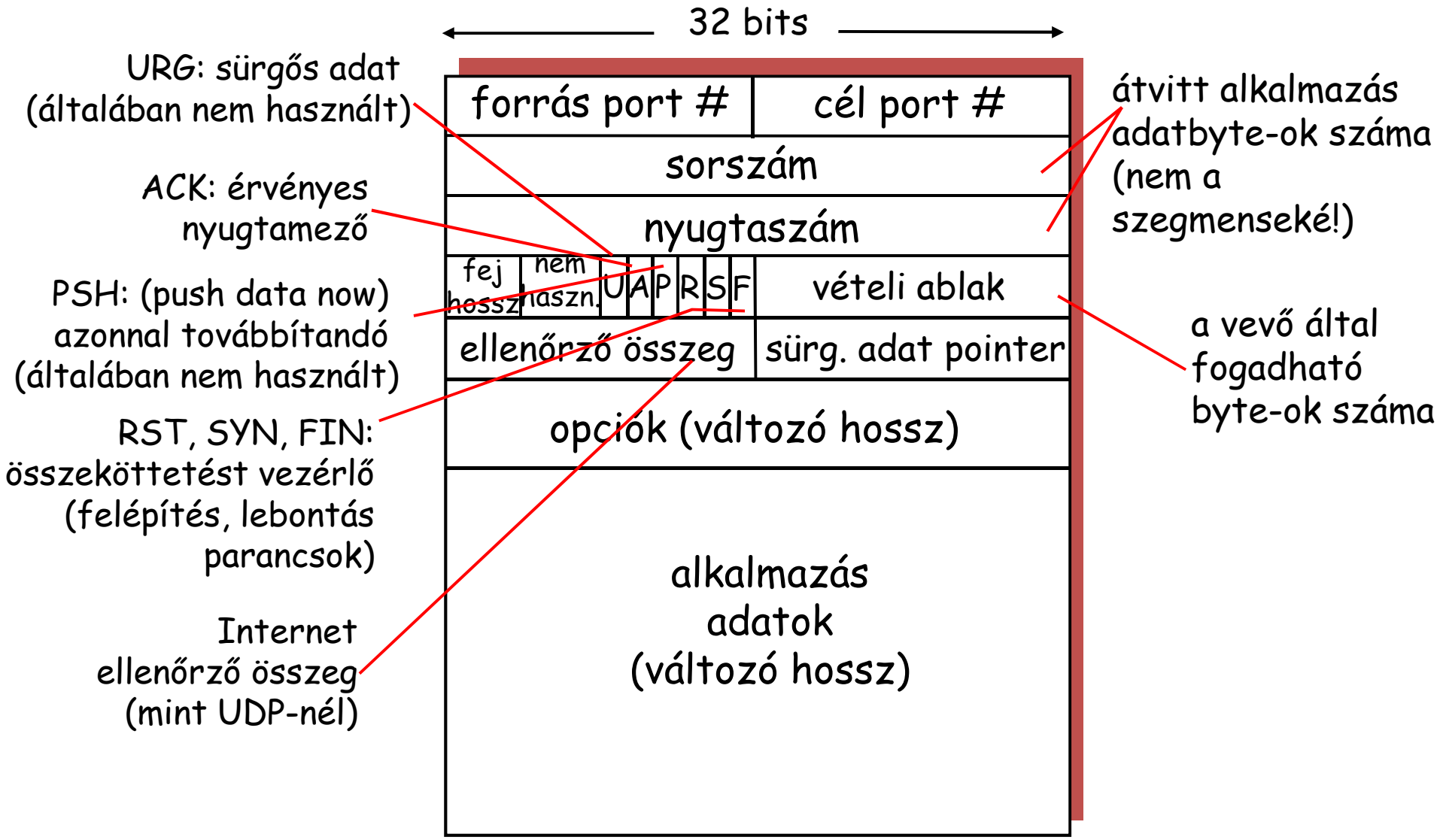
TCP: ÁTTEKINTÉS
RFCS: 793, 1122, 1323, 2018, 2581

- pont-pont elrendezés
  - egy küldő, egy fogadó
- megbízható, sorrendtartó byte folyam
- „csővezetékezett” (pipelined)
  - a TCP torlódáskezelés és forgalomvezérlés állítja az „ablakmértet”
- *küldő és fogadó puffer*



- full duplex adat:
  - kétirányú adatáramlás ugyanazon a összeköttetésen
  - MSS: maximum segment size
- összeköttetés alapú (connection-oriented)
  - kézfogás (vezérlő üzenetek cseréje), amit a küldő kezdeményez, vevőoldali állapot az adatcsere megkezdéséhez
- forgalomvezérlés
  - a küldő ne terhelje túl a fogadó (fogadó puffer!)
- torlódásvezérlés
  - fairness: a küldő visszaszabályoz, ha a hálózat túlterhelt

A TCP SZEGMENS SZERKEZETE



QUIC ALAPOK ÉS FŐBB ELEMEK

- A Google-nál kezdték fejleszteni, jelenleg Internet Draft
- Kapcsolat alapú, a TCP változatok előnyeit ötvözi
- **Quick UDP Internet Connections**
  - Megbízható adatátvitel UDP felett?
  - Egy fél réteggel feljebb (a szállítási és az alkalmazási rétegek között)
  - Egyelőre nem a TCP helyett, csak mellett
- A HTTP/2 és a HTTP/3 hatékony kiszolgálására
- Gyors kapcsolat-felépítés
- Hatékony újraküldés és torlódáskezelés
- Adatfolyamok (stream) multiplexálása
  - Egy adat nem tartja fel a többit
- Hiányzó adat helyreállítása

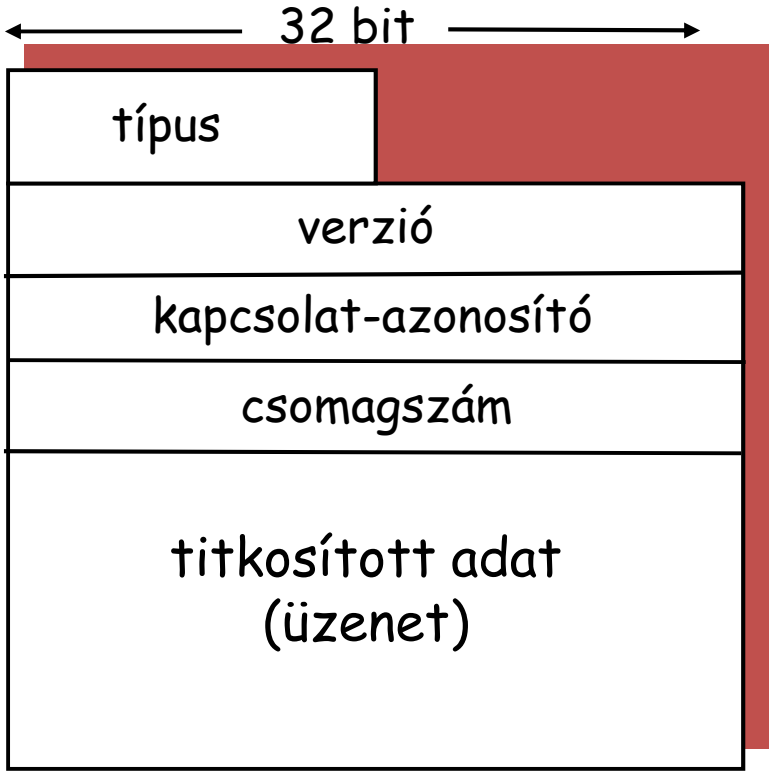
  Forward Error Correction

  Paritás ellenőrző adat több szegmensre

  Helyreállítás anélkül, hogy újraküldenénk
- Kapcsolatvégpontok migrálása
  - Internet értelemben mozoghatnak a végpontok
  - A kapcsolatnak egyedi azonosítója van
  - Nem a TCP-nél látott négyes információ, tehát akár változhat az IP cím, vagy a port száma
- Titkosítás beépítve
  - Az összes adat titkosítva megy át (TLS)

QUIC CSOMAGFORMÁTUM

- A QUIC csomag az UDP szegmensbe beágyazott adat
- Típus (flagek)
  - különböző célú csomagtípusokhoz
- Verzióra csak egyeztetéskor van szükség
- A kapcsolat-azonosító egyedi
  - a forrás és a nyelő oldalon is, biztosítja, hogy az alsóbb protokoll rétegek (UDP, IP és lejjebb) címzési változásai ne eredményezzék a csomagok rossz végponthoz továbbítását
- Egyedi csomagszám
  - monoton nő, lehet tudni, hogy melyiket küldték előbb
  - újraküldés esetén már más lesz
- Az adat különböző részekből állhat, pl.:
  - adatfolyamok adatai
  - nyugta



QUIC csomag egyszerűsített formátuma

Néhány áttekintő QUIC forrás:

- IETF 98 - QUIC Tutorial video: https://www.youtube.com/watch?v=lPSTcBITbvs , slide-ok: https://www.ietf.org/proceedings/98/slides/slides-98-edu-sessf-quic-tutorial-00.pdf
- M. Polese at al.: A Survey on Recent Advances in Transport Layer Protocols, IEEE Communications Surveys & Tutorials (Volume: 21 , Issue: 4 , Fourthquarter 2019), pp.3584-3608, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8786240
- Yong Ciu, et al.: Innovating Transport with QUIC: Design Approaches and Research Challenges, IEEE Internet Computing (Volume: 21 , Issue: 2 , Mar.-Apr. 2017), pp. 72-76, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7867726
- Version-Independent Properties of QUIC, IETF QUIC Workgroup
- https://quicwg.org/base-drafts/draft-ietf-quic-invariants.html
- IETF Draft https://datatracker.ietf.org/doc/draft-ietf-quic-transport/?include_text=1

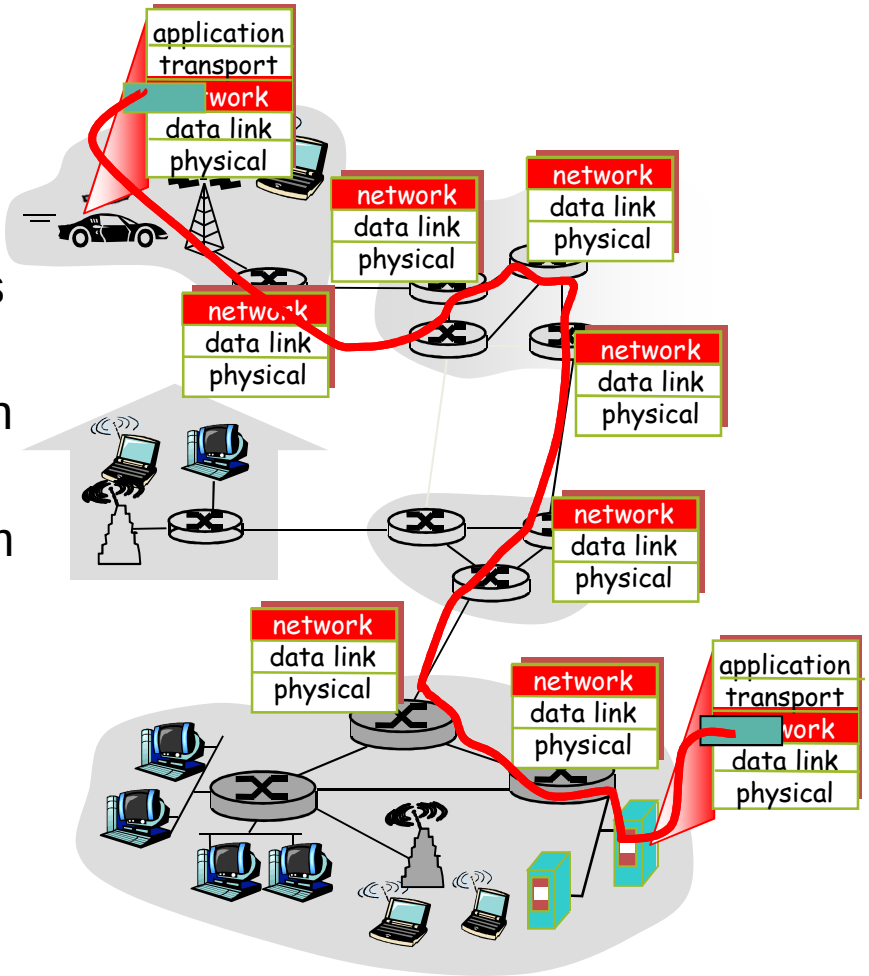
L4 ÖSSZEFOGLALÁS

- TCP/IP hosztok összekapcsolására
- TCP [AP, SA, DP, DA] azonosító négyes
- az IP cím a hálózati helyet határozza meg és a szoftver processz azonosításában is szerepel
- az IP cím - SA vagy DA - megváltozása a fennálló TCP kapcsolat megszakadásával jár
- QUIC – egyedi kapcsolatazonosító (az IP cím nem része a kapcsolat azonosításának), UDP trasznportot használ

Néhány hálózati réteg vonatkozás áttekintése:
IP címzés, útvonalválasztás, továbbítás, IGP, BGP

HÁLÓZATI RÉTEG

- transzport szegmens eljuttatása a küldő hoszttól a fogadó hosztnak
- a küldő oldalon a szegmensek datagramokba csomagolása (encapsulat)
- a fogadó oldalon a megérkezett szegmens átadása a transzport rétegnek
- hálózati réteg protokollok *minden* hosztban és routerben
- a router minden rajta áthaladó IP datagram fejlécét feldolgozza



A hálózati réteg és a transzportréteg szolgáltatásainak alapvető különbsége:

- hálózati réteg: két hoszt között (a közbülső routerek közreműködésével)
- *transzport réteg*: két – távoli hoszton futó - szoftverfolyamat (processes) kötözött

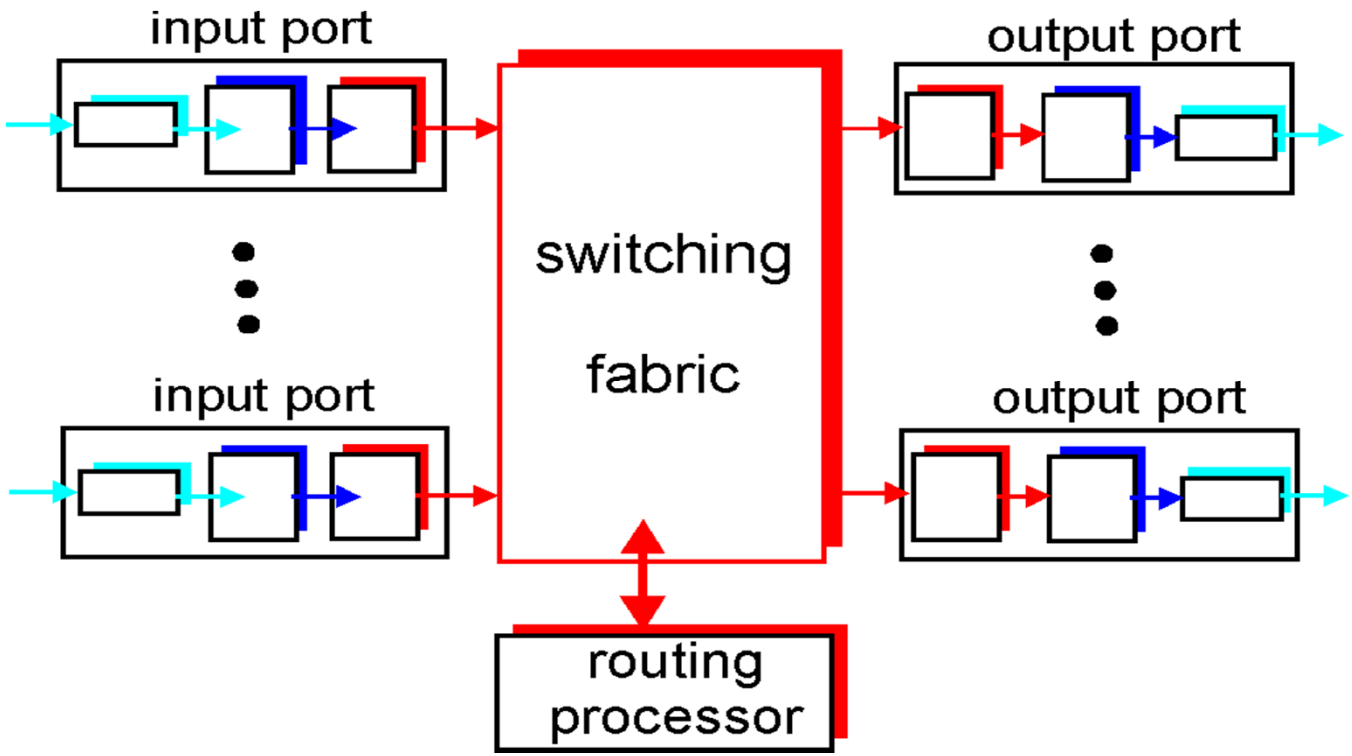
A HÁLÓZATI RÉTEG KÉT ALAPVETŐ FUNKCIÓJA

- *[csomag]továbbítás (forwarding):* csomag mozgatása a router bemenetéről a router megfelelő kimenetére
- *útvonalválasztás (routing):* a csomag útjának meghatározása a forrástól a nyelőig
  - *útvonalválasztó (routing) algoritmusok*

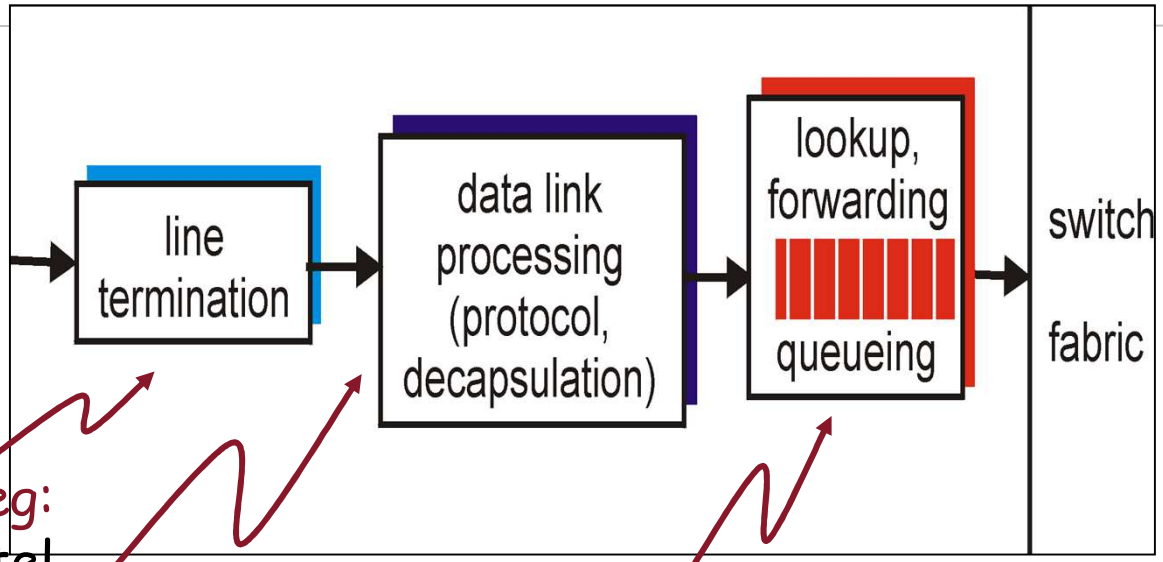
A ROUTER FELÉPÍTÉSE – ÁTTEKINTÉS

Két alapvető funkció:

- futtatja a routing algoritmusokat/protokollokat (RIP, OSPF, BGP)
- *továbbítja (forwarding)* a datagramokat a bejövő linkekről a megfelelő kimenő linkekre



BEJÖVŐ PORT FUNKCIÓK



Fizikai réteg:
bitszintű vétel

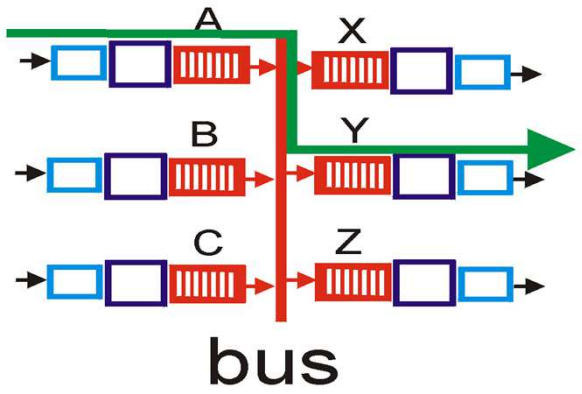
Adatkapcsolati réteg:
pl., Ethernet

Elosztott kapcsolás:

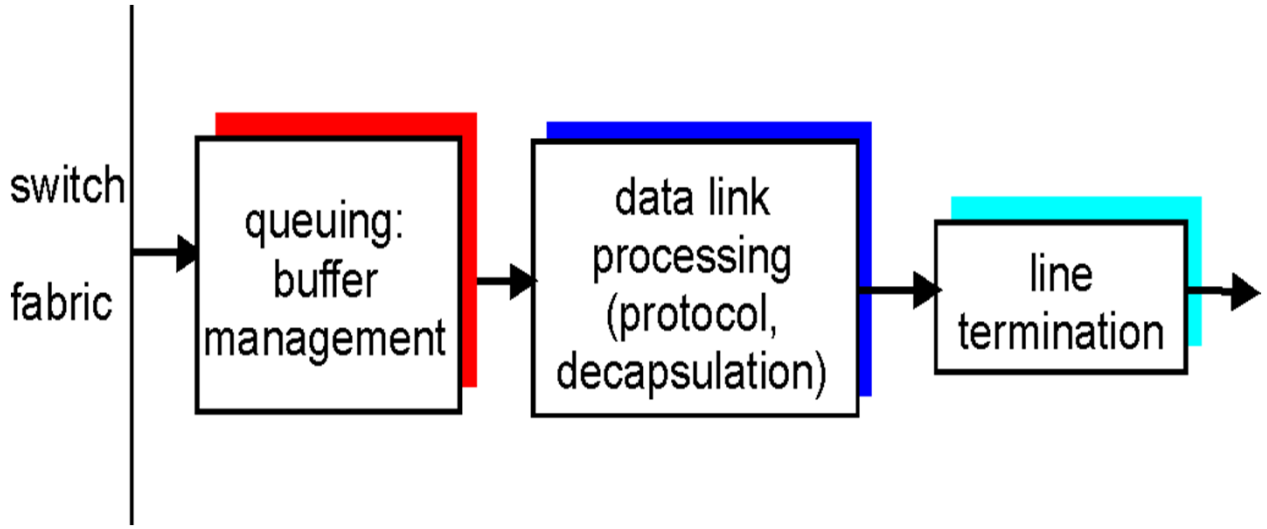
- az adott datagram célcíme alapján a kimenő port meghatározása a routing táblából az input port memódiájában
- cél: input port oldali teljes feldolgozás „drótsebességgel” (line speed)
- sorbanállás (queueing): ha a datagramok gyorsabban érkeznek, mint ahogyan a kapcsoló (switch fabric) továbbítani tudja őket

KAPCSOLÁS BUSZON

- Az input port memóriájából az output port memóriájában egy közös bus-on jut el a datagram
- a kapcsolási sebességet a busz sávszélesége korlátozza
- 32 Gbps bus, Cisco 5600: elegendő sebesség hozzáférési és vállalati routerekben (2007)

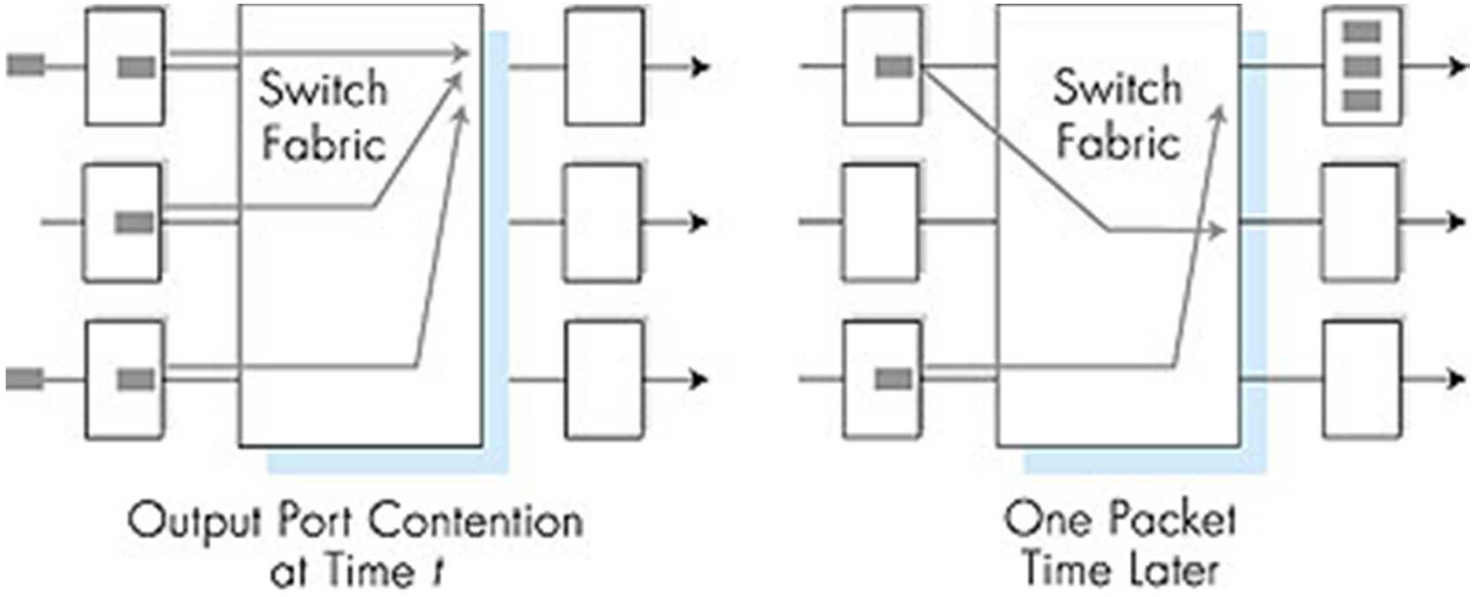


KIMENŐ PORTOK



- *Pufferelés:* akkor szüksége, ha a csomagok nagyobb intenzitással érkeznek, mint az átviteli sebesség
- *Ütemezési szabály:* az átvitelre kerülő datagram kiválasztása a sorban várakozók közül

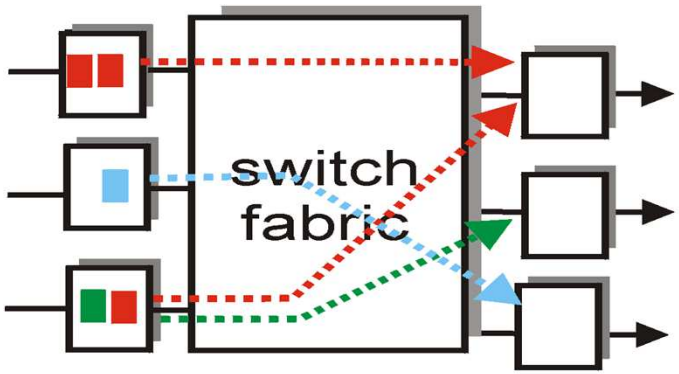
SORBANÁLLÁS A KIMENŐ PORTNÁL



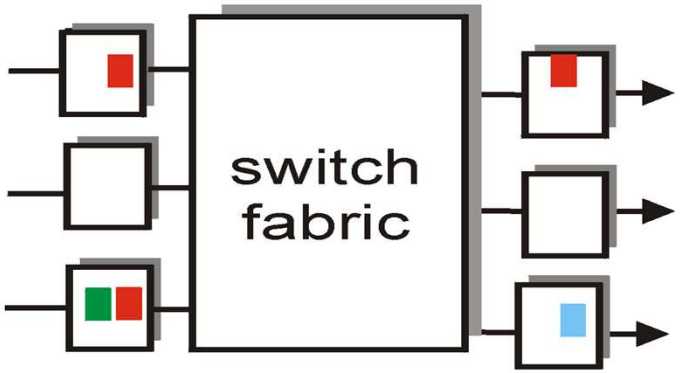
- pufferelés ha a csomagok a kapcsolón keresztül nagyobb intenzitással érkeznek, mint az átviteli sebesség
- *sorbanállási késleltetés*
- *csomagvesztés ha a kimenő puffer túlcsordul*

SORBANÁLLÁS A BEJÖVŐ PORTNÁL

- Ha a kapcsoló sebessége kisebb, mint a bejövő portok összesített sebessége, akkor sorok alakulnak ki a bejövő oldalon
- Soreleji blokkolás (Head-of-the-Line - HOL -blocking) : a sor elején várakozó datagram meggátolja a mögötte lévők továbbítását
- *sorbanállási késleltetés*
- *csomagvesztés ha a bejövő puffer túlcsordul*

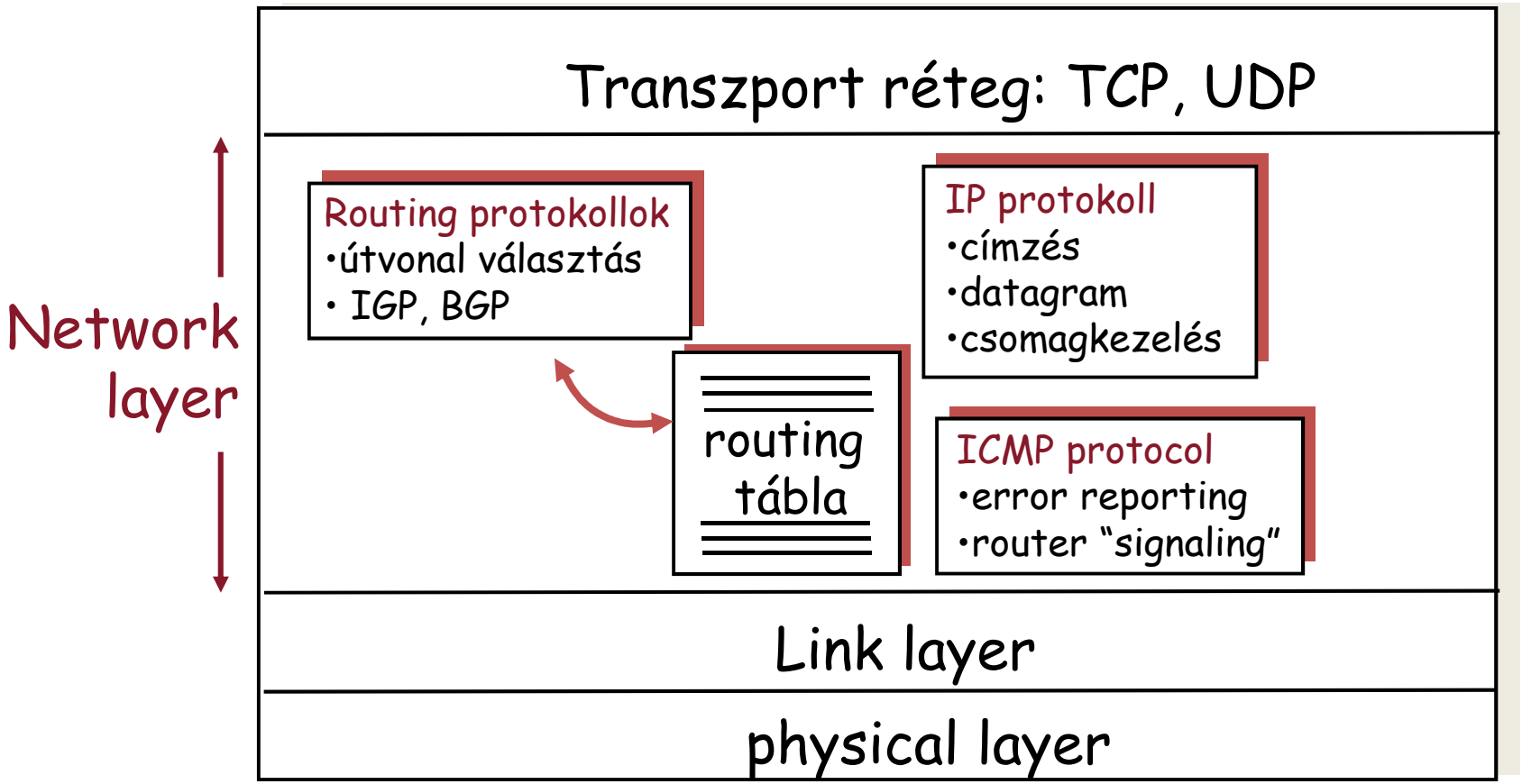


output port contention at time t - only one red packet can be transferred



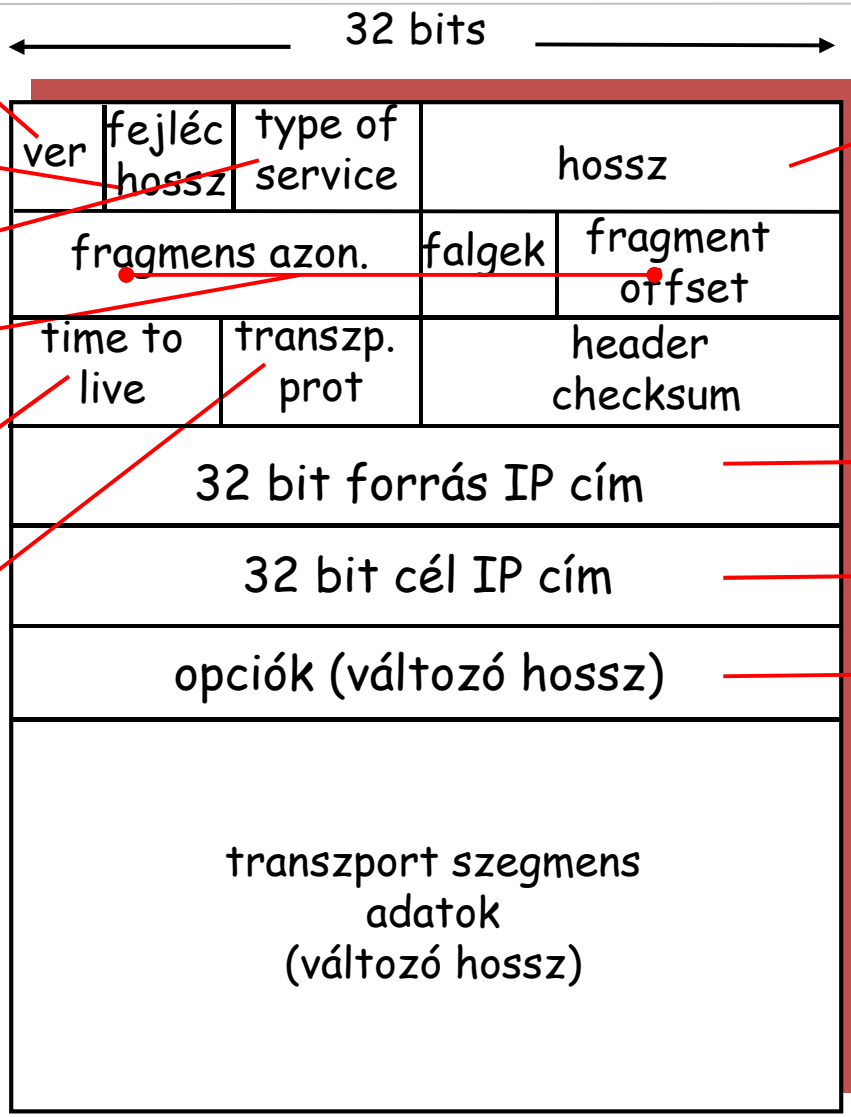
green packet experiences HOL blocking

Hoszt, router, rétegfunkciók



IPv4 DATAGRAM

- IP protokoll verziószám
- Fejléc hossza bájtban
- Információ a csomag kezelési besorolásáról (QoS-hez)
- Információk a darabolásról (fragmentációról)
- Hátralévő ugrások (hopok) maximális száma
  - minden router eggyel csökkenti
- Az adatokat küldő protokoll



- Teljes hossz (bájtban)
- Küldő címe
- Fogadó címe
- Opciók, például:
  - időbélyeg
  - érintendő
  - routerek listája

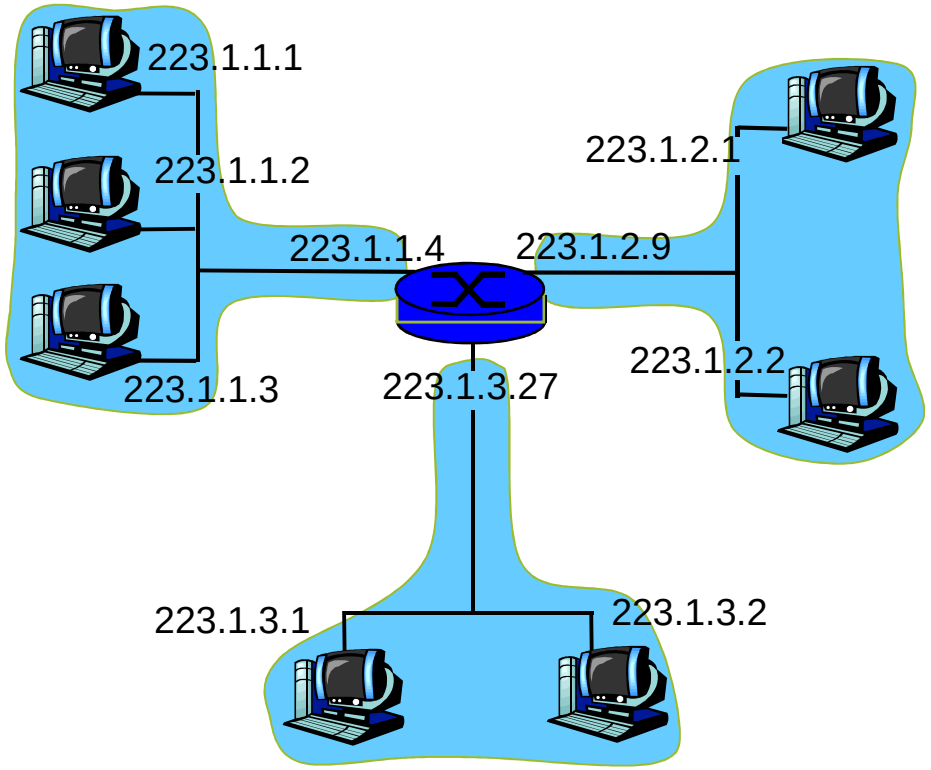
Mekkora az overhead TCP-vel?

- 20 bytes of TCP
- 20 bytes of IP
- = 40 bytes + app layer overhead

IP CÍM, HÁLÓZATOK

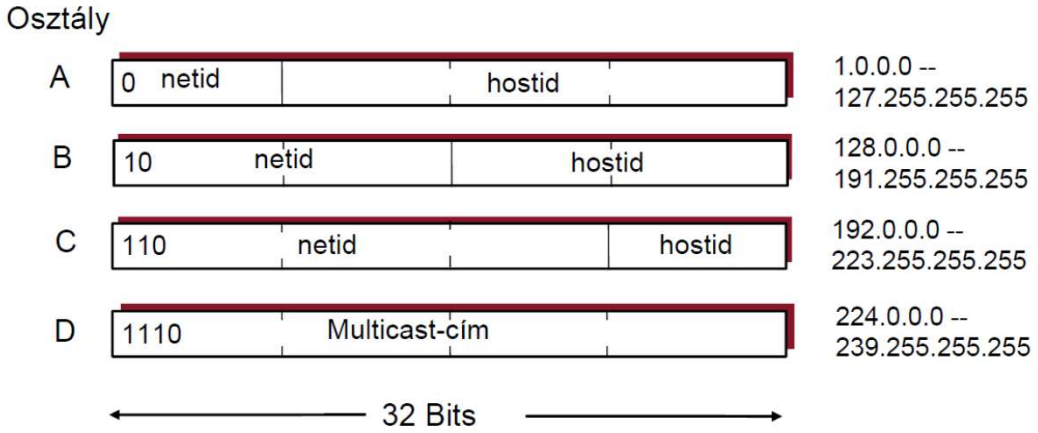
- Egy hoszt, vagy egy router egy interfészét azonosítja
- Interfész a rendszer és a link között
  - Általában egy hálózati kártya (NIC) valósítja meg a hosztban
  - A routereken portokhoz kapcsolódnak, de lehetnek „virtuálisak” is
  - Általában egy routernek több interfésze is van
  - Egy interfész – egy IPv4 cím
- Az IP cím két részből áll
  - **netid**: a felső bitek azonosítják a hálózatot
  - **hostid**: az alsó bitek azonosítják az interfészt a hálózaton belül
- A hálózatok értelmezése (network)
  - Azon az interfészek halmaza, amiknél a netid azonos
  - Az egy hálózatban lévő elemek
    - Szomszédosak (L3 szinten)
    - Úgy küldhetnek egymásnak, hogy nem kell keresztülmenni egy routeren sem
- Hálózati maszk
  - A hálózati részt maszkolja a címből
  - A felső bitjei egyesek a többiek nullások

- Három hálózat egy routerrel összekötve
  - Az első három oktet azonosít
- Hálózati maszk
  - 24 bites – 24 darab egyes
  - 255.255.255.0

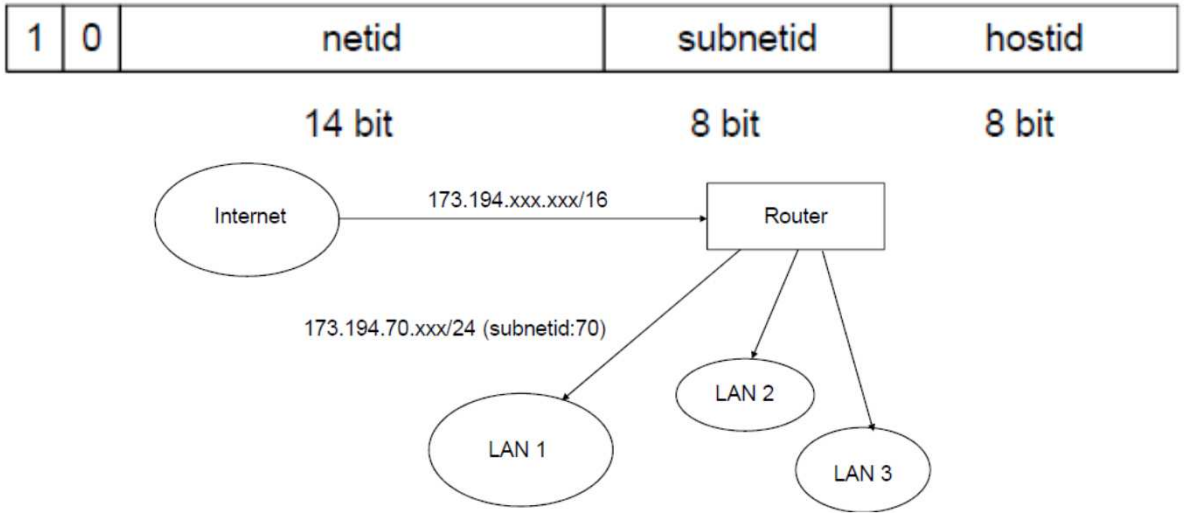


IPv4 CÍMOSZTÁLYOK

- Eredetileg az IPv4-ben osztályokra osztották a címeket
- Az osztály határozta meg a maszk hosszát
- Osztályalapú címzés (classful addressing)



- Az A és B osztályú hálózatok a gyakorlati felhasználhatóság szempontjából irreális méretűek
- CIDR: Classless InterDomain Routing: egy-egy hálózatot további alhálózatokra (subnet) lehet bontani subnetid-ket bevezetve, címformátum a.b.c.d/x, ahol x a hálózti (net+subnet) része a címnek
- Ez csak példa, a felosztás és az alhálózati azonosítók a hálózatot kezelő szervezet lokális döntései
- Egy hálózat felosztása kívülről nem kell, hogy látható legyen



SPECIÁLIS IPv4 CÍMTARTOMÁNYOK (RFC 3330)

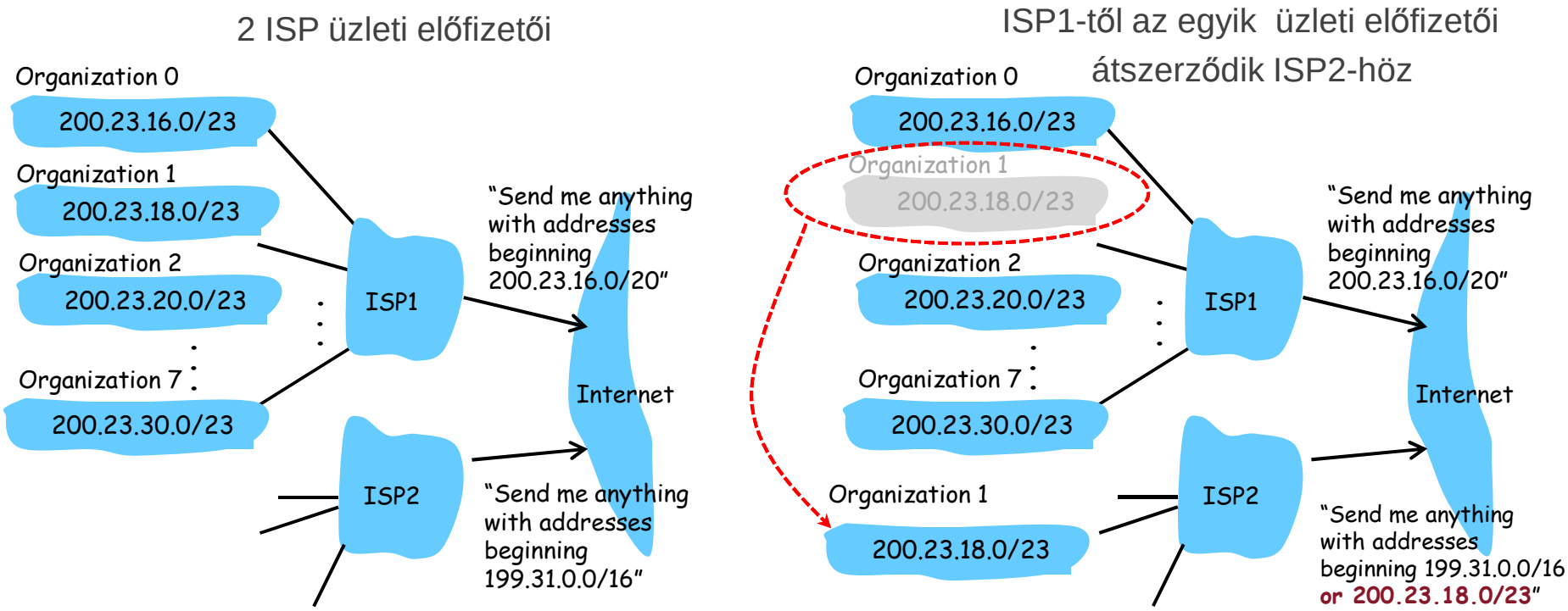
Address Block	Present Use	Reference
0.0.0.0/8	"This" Network	[RFC1700, page 4]
10.0.0.0/8	Private-Use Networks	[RFC1918]
14.0.0.0/8	Public-Data Networks	[RFC1700, page 181]
24.0.0.0/8	Cable Television Networks	--
39.0.0.0/8	Reserved but subject to allocation	[RFC1797]
127.0.0.0/8	Loopback	[RFC1700, page 5]
128.0.0.0/16	Reserved but subject to allocation	--
169.254.0.0/16	Link Local	--
172.16.0.0/12	Private-Use Networks	[RFC1918]
191.255.0.0/16	Reserved but subject to allocation	--
192.0.0.0/24	Reserved but subject to allocation	--
192.0.2.0/24	Test-Net	
192.88.99.0/24	6to4 Relay Anycast	[RFC3068]
192.168.0.0/16	Private-Use Networks	[RFC1918]
198.18.0.0/15	Network Interconnect Device Benchmark Testing	[RFC2544]
223.255.255.0/24	Reserved but subject to allocation	--
224.0.0.0/4	Multicast	[RFC3171]
240.0.0.0/4	Reserved for Future Use	[RFC1700, page 4]

IPv4 CÍM HONNAN?

- ISP: címblokkok, ICANN: *Internet Corporation for Assigned Names and Numbers* http://www.icann.org/
- Routerek (interfészek): konfigurálás
- Hosztok
  - statikus címkiosztás:
  - dinamikus címkiosztás (DHCP)
    - Célja: a hoszt a hálózathoz kapcsolódáskor dinamikusan tudjon címet szerezni („bérelni”)
    - A „bérleti idő” megújítható
    - A visszaadott címek újra kioszthatók
    - DHCP áttekintés:
      - hoszt broadcast üzenetben “DHCP discover”
      - DHCP szerver válasz “DHCP offer” msg
      - hoszt kéri az IP címet: “DHCP request” msg
      - DHCP szerver adja az IP címet: “DHCP ack” msg

HIERACHIKUS CÍMKIOSZTÁS: UTAK AGGREGÁLÁSA

A címek hierarchikus kiosztása a routing információk hatékony hirdetését teszi lehetővé

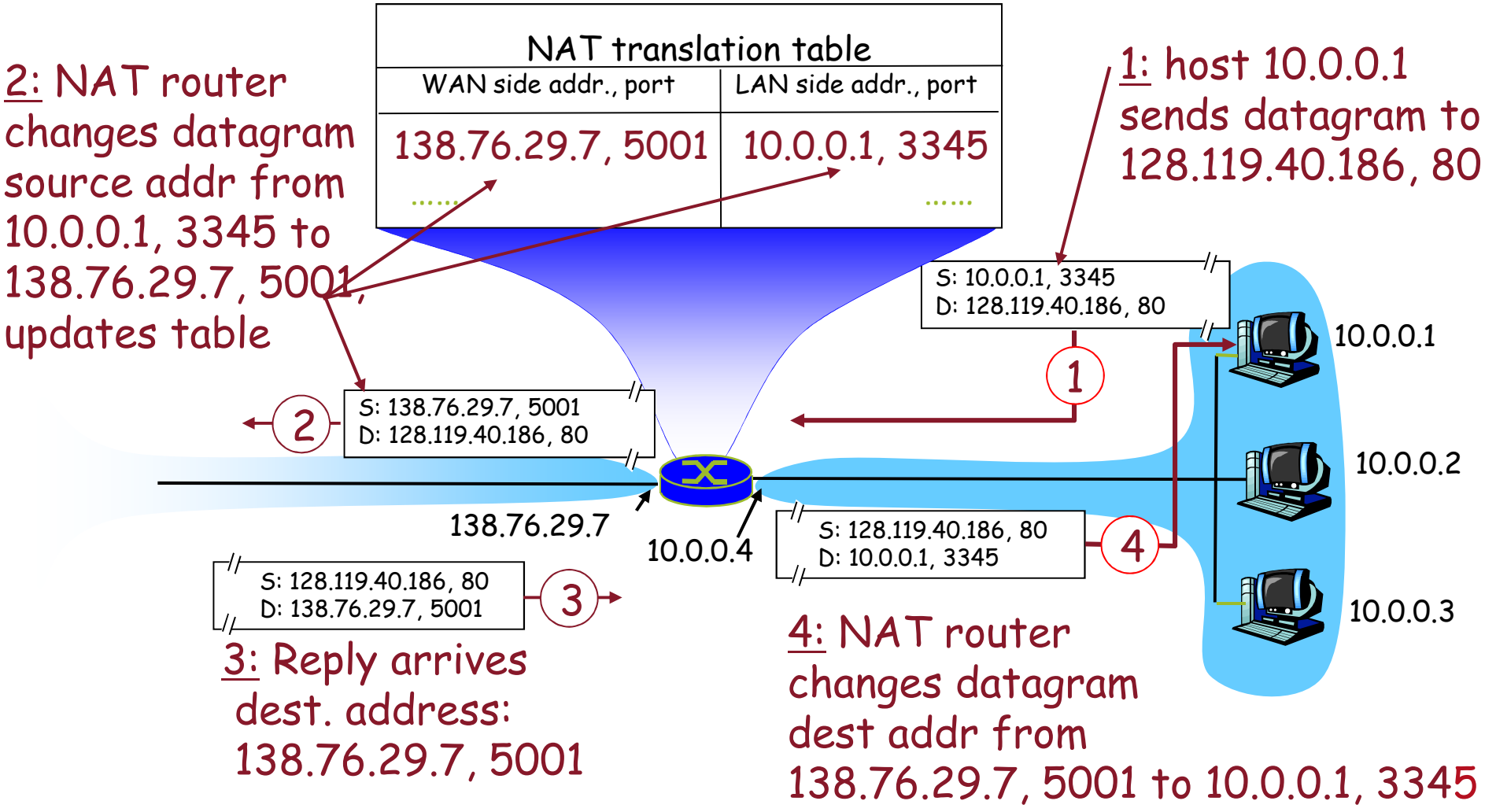


A leghosszabb illeszkedés (longest match) elvet kihasználva egy IP címtartományát megtartó szervezet hálózati „áthelyezése” is hatékonyan kezelhető (more specific prefix)

CÍMFORDÍTÁS : NETWORK ADDRESS TRANSLATION (NAT)

- Motivációk
  - Internet-kapcsolat megosztása (egy publikus cím mögött számos kapcsolódó hoszt)
- Megvalósítás (NAT router)
  - kimenő datagramokra lecseréli a (forráscím, forrásport) párt egy (NAT cím, választott port) párra, a (célcím, célport) változatlan marad
  - feljegyzi a címfordítási táblába a (forráscím, forrásport) - (NAT cím, választott port) összerendelést
  - Válaszként beérkező datagramokra címfordítási tábla bejegyzései alapján visszaállítja a célhoz tartozó (NAT cím, választott port) párost az eredeti (cím, port) párosra
  - 16 bites portszámok (elvileg 60 ezer egyidejű kapcsolat egyetlen publikus IP-címmel)
- Hálózaton belül privát cím
- Hálózaton kívül publikus cím (minden hálózaton belüli hosztra azonos, de a hosztok és kapcsolatok különböző portszámokkal megkülönböztetve)
- Következmények
  - ISP-váltáskor nem kell címkiosztást változtatni
  - megsérül a végpontok közti transzparencia
  - a helyi hálózatban lévő hosztok közvetlenül nem láthatók, címezhetők kívülről
  - az alkalmazások tervezésnél (pl. P2P alkalmazások, plug and play megoldások) figyelembe kel venni

HÁLÓZATI CÍMFORDÍTÁS - PÉLDA



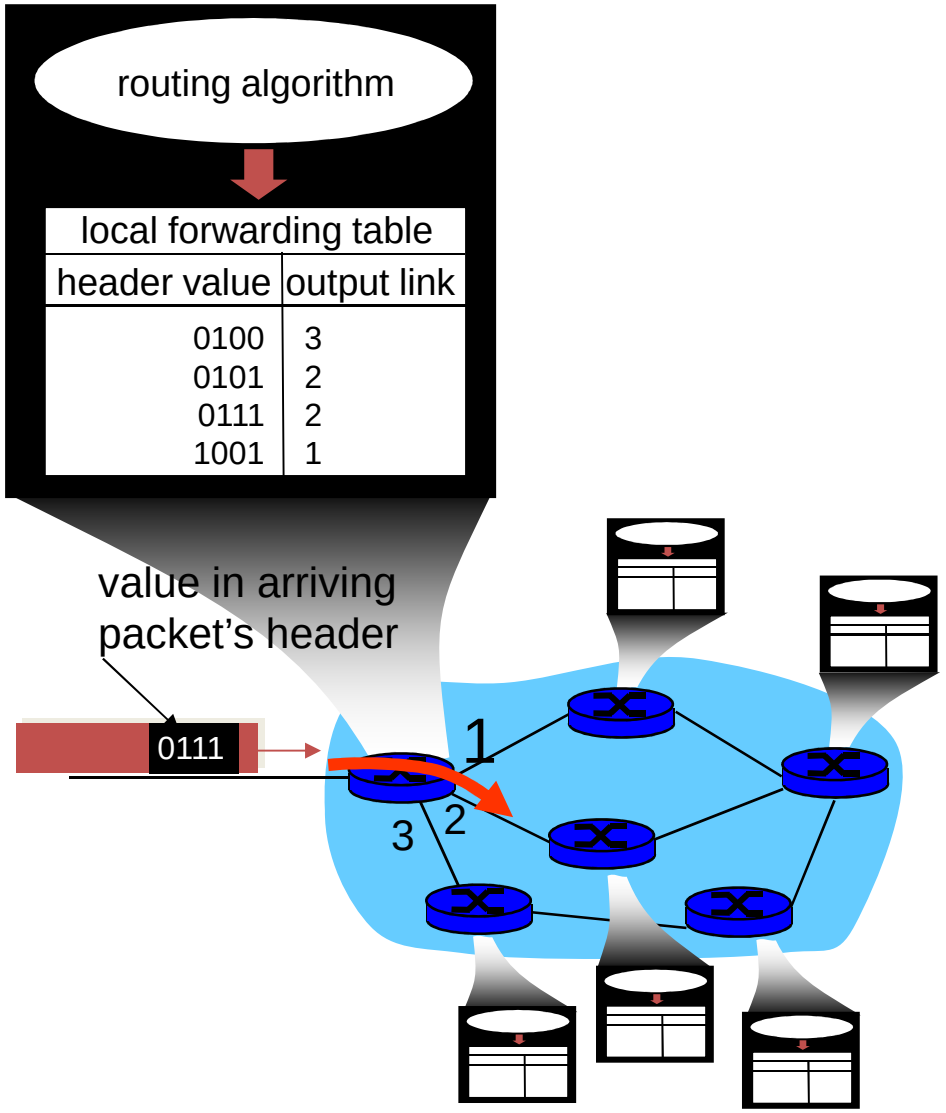
ÚTVONALVÁLASZTÁS ÉS TOVÁBBÍTÁS KAPCSOLATA

Útvonalválasztás (routing)

- a routing protokoll alapján a router
  - összegyűjti a különböző célcímek elérését meghatározó információkat
  - meghatározza a célcím preferált elérési útját
  - routing táblájába bejegyzi a célcím, kimenő interfész adatpárt

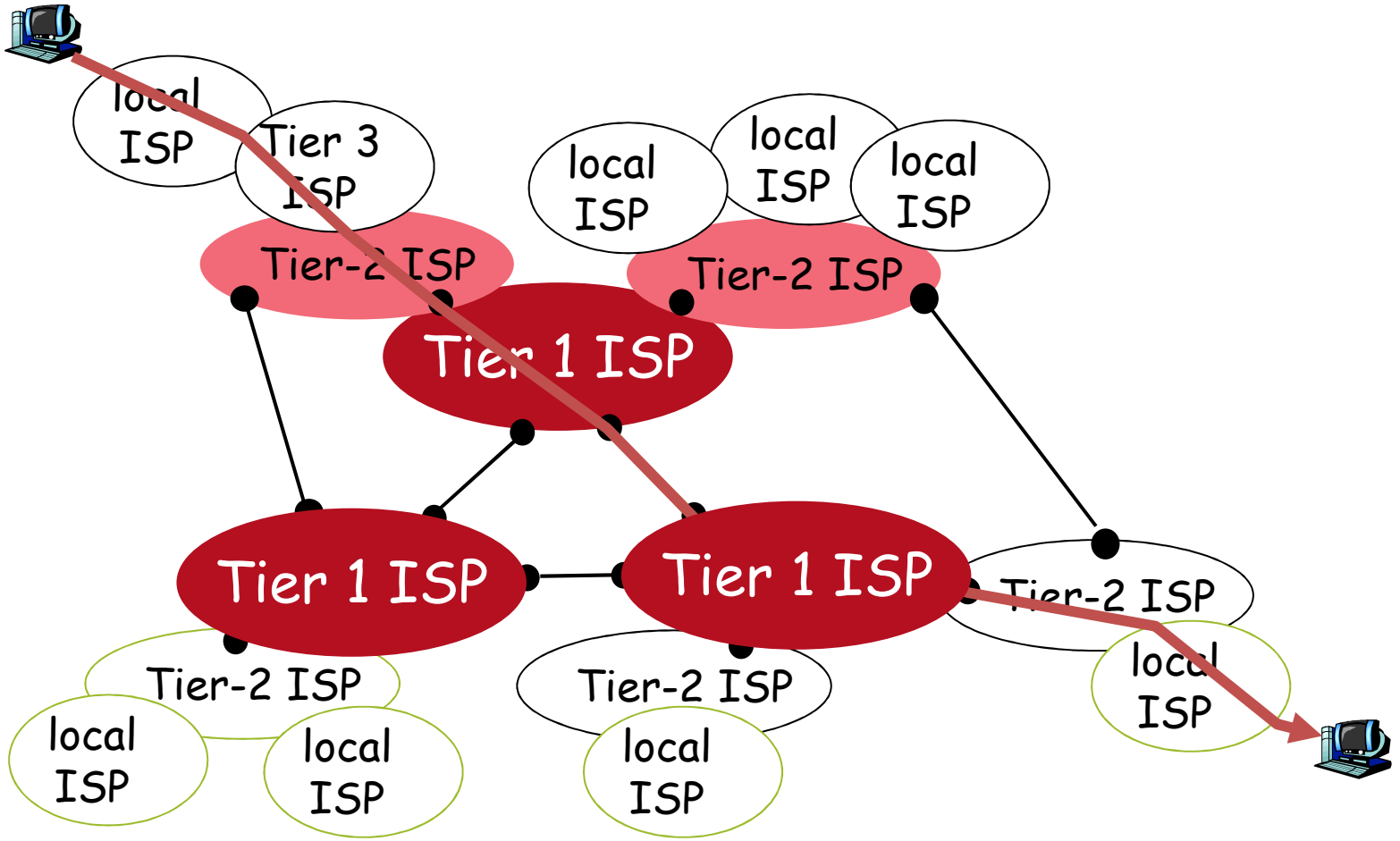
Datagram továbbítása (forwarding)

- a beérkező datagram célcíme alapján a router a megfelelő kimenő interfészre továbbítja a datagramot



AZ INTERNET STRUKTÚRÁJA: HÁLÓZATOK HÁLÓZATA

- Egy csomag számos hálózaton halad keresztül!

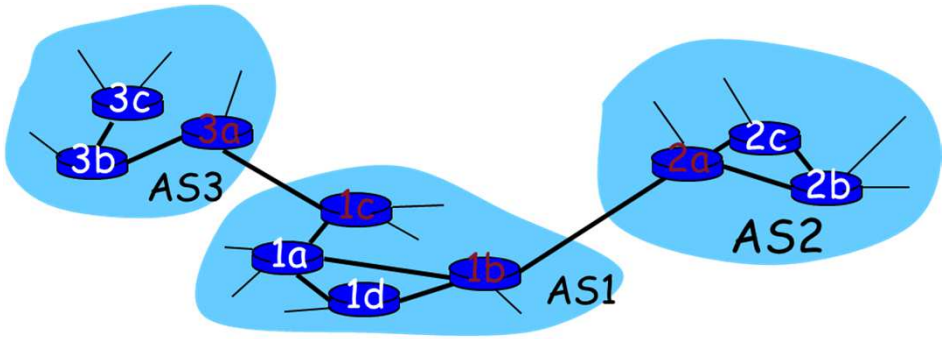


HIERARCHIKUS ÚTVONALVÁLASZTÁS

- routerek tartományokba rendezése, “autonomous systems” (AS)
- az azonos AS-bel lévő routerek ugyanazt a routing protokollt futtatják
  - “intra-AS” routing protokoll
  - a különböző AS-ekben lévő routerek különböző intra-AS routing routing protokollt futathatnak

Gateway router

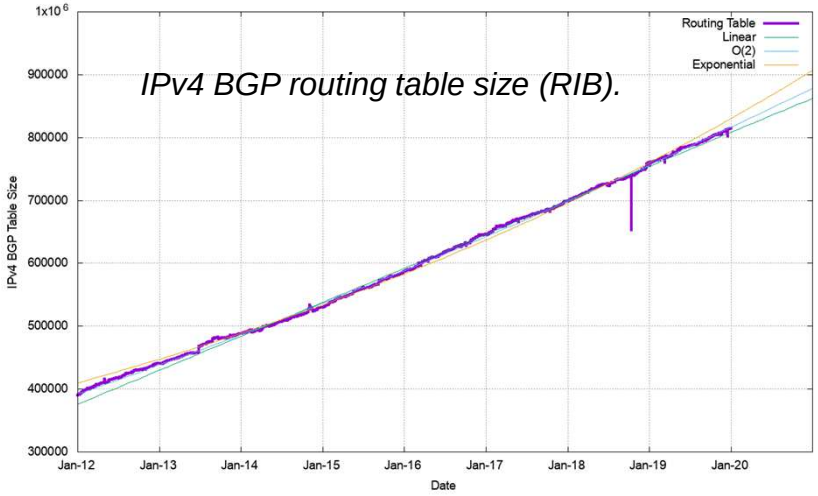
- közvetlenül kapcsolódik egy másik AS gateway routeréhez

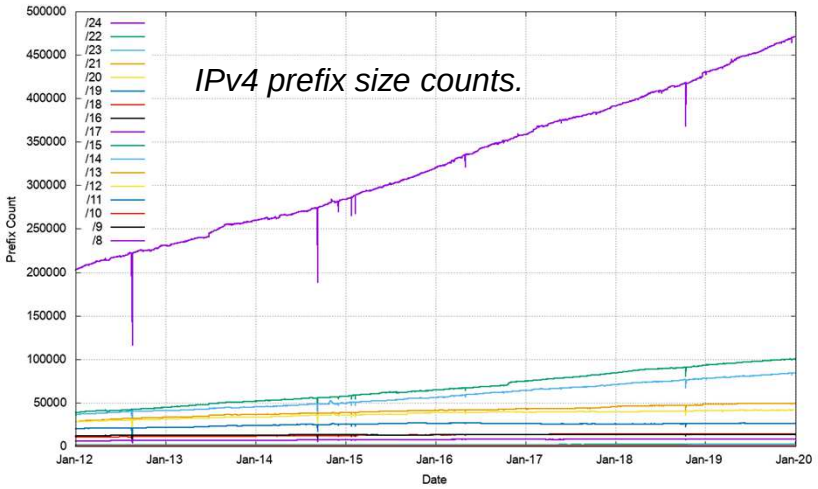


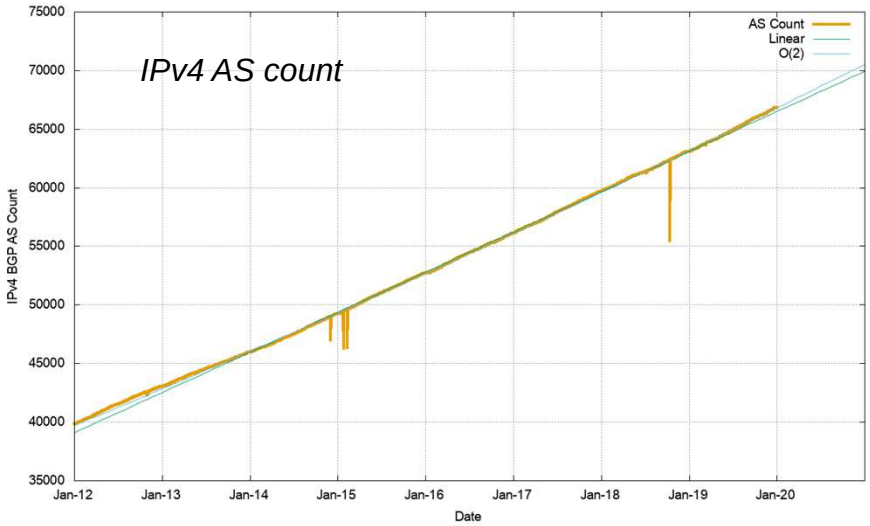
ÚTVONALVÁLASZTÁS, ROUTING PROTOKOLLOK

- Statikus útvonalválasztás: konfigurált utak, a változtatáshoz a konfigurációt kell módosítani (CLI)
- Dinamikus útvonalválasztás (állapotváltozások követése) automatikusan számolt utak, robusztus (bizonyos hibákkal szemben ellenálló), skálázható (hálózat mérete, célcímek száma)
- IGP
  - egy AS-ne belül – út egy router adott interfészéhez
  - távolságvektor (DV) alapú – a router lokális információk alapján építi fel a routing tábláját, vagy linkállapot (LS) alapú – a router globális az egész hálózatra kiterjedő információk alapján építi fel a routing tábláját
  - elosztott működés, egy router csak a datagram útjának következő szakaszáról dönt – a routing algortimus szerinti szomszédos routerhez továbbítja a datagarmot,
  - azonos hálózati kép és feldolgozás alapján lesz konzisztens (a lokális next hop döntések alapján célba ér a csomag), ha minden router azonos hálózati állapotot lát és azonos módon számol, akkor a next hop döntések sorozata a mindenki által számolt utat rakja össze
- BGP
  - AS-eken át – út egy távoli AS-hez (forrás és cél AS-en belül IGP)
  - „útvektor” alapú (PV)
  - elosztott működés, egy router csak a datagram útjának következő szakaszáról dönt – a routing algortimus szerinti szomszédos routerhez továbbítja a datagarmot

BGP IPv4 MÉRETSTATISZTIKÁK 2020



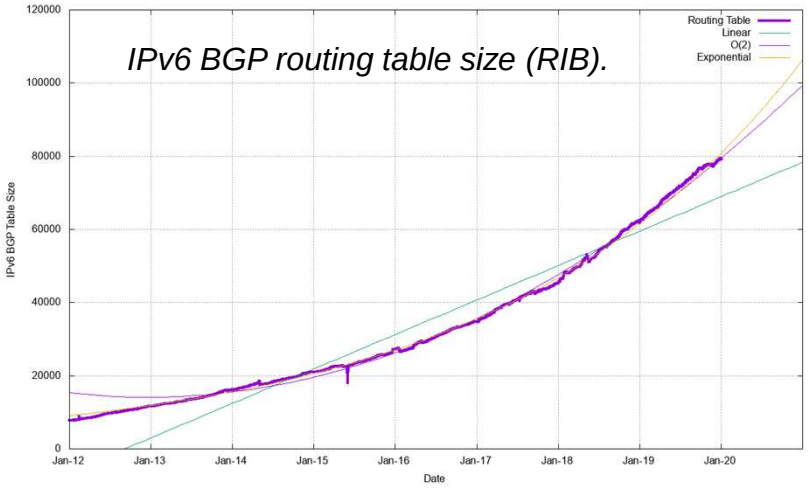


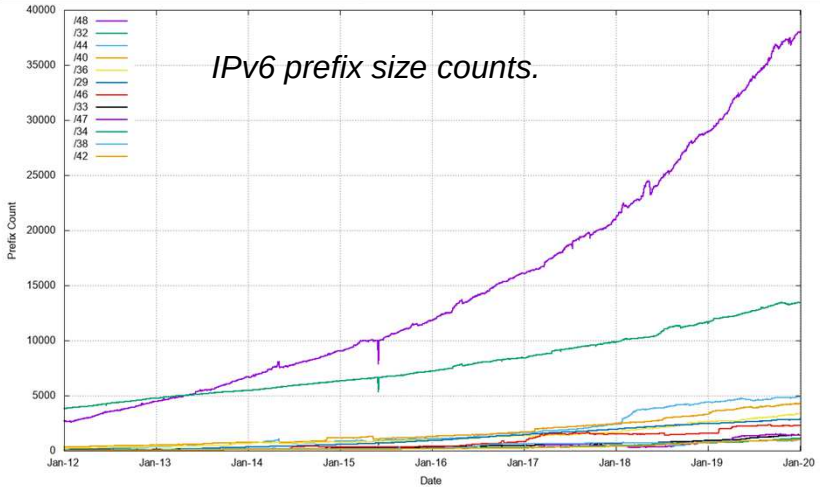


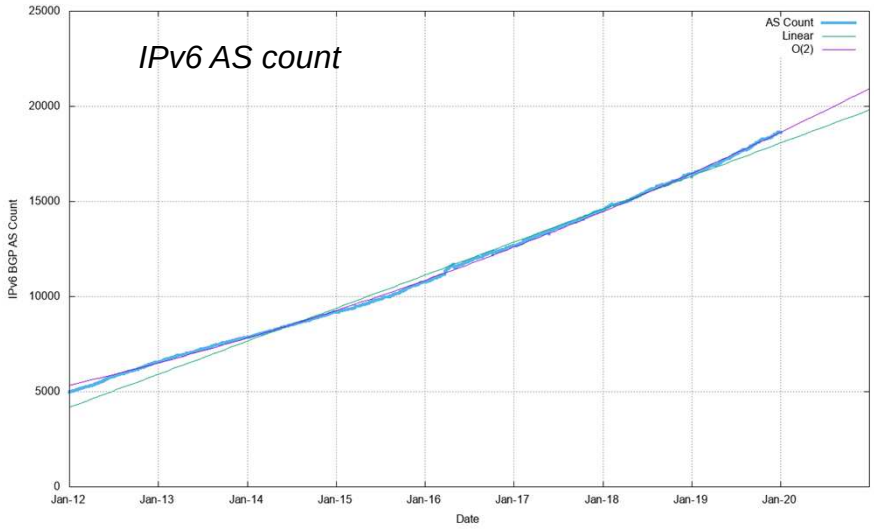
- IPv4 BGP RIB mérete: ~800 000
- IPv4 BGP prefixek száma:
  - /24 ~470 000
  - /22 ~100 000
  - /20 ~ 40 000
  - /16 < ~20 000
- IPv4 BGP AS-ek száma: ~67000

Forrás: https://blog.apnic.net/2020/01/14/bgp-in-2019-the-bgp-table/

BGP IPv6 MÉRETSTATISZTIKÁK 2020





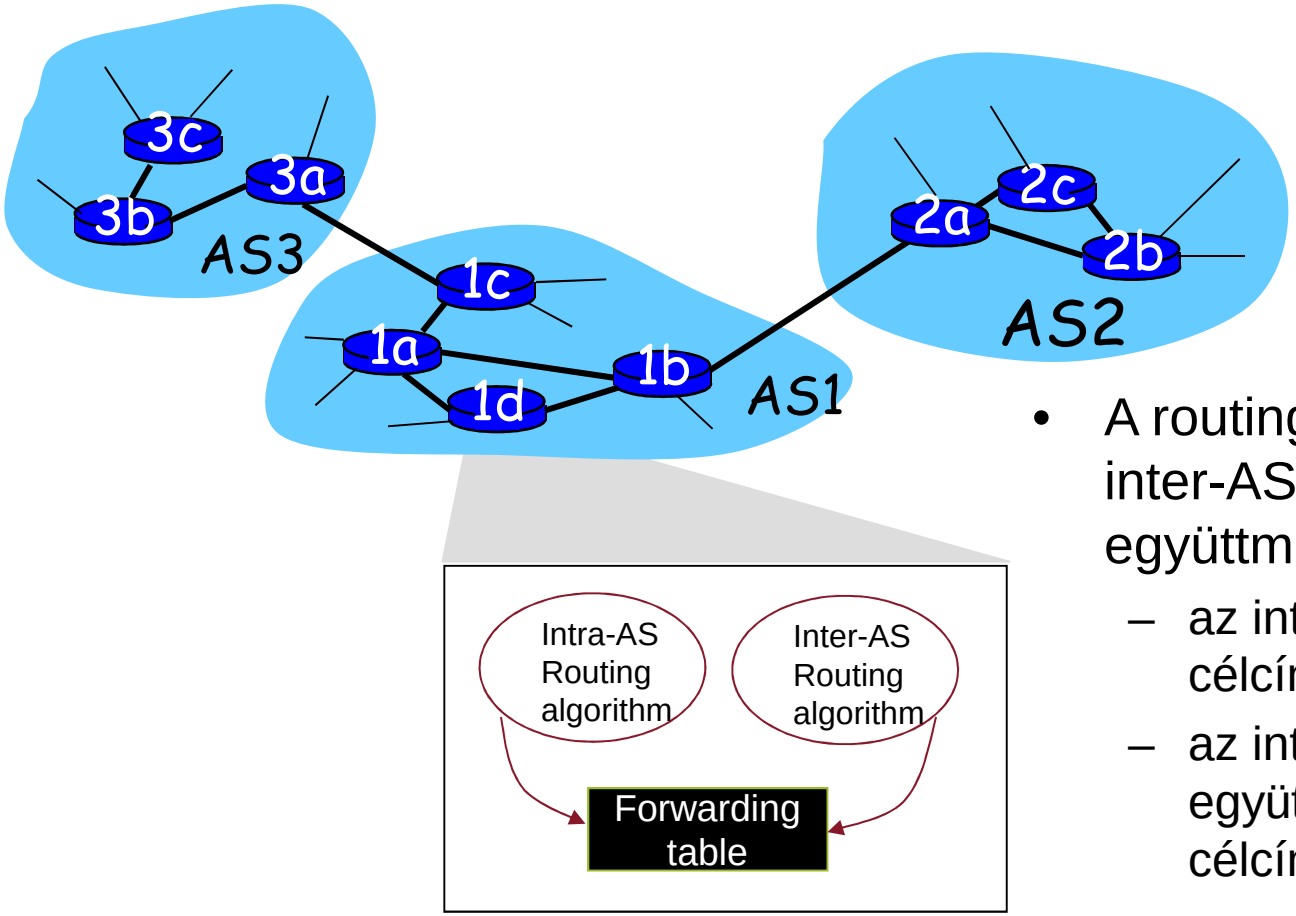


- IPv6 BGP RIB mérete: ~80 000
- IPv6 BGP prefixek száma:
  - /48 ~38 000
  - /32 ~14 000
- IPv4 BGP AS-ek száma: ~18000

(IPv6 elterjedtsége: a felhasználók ~25%-a)

Forrás: https://blog.apnic.net/2020/01/14/bgp-in-2019-the-bgp-table/

ÖSSZEKAPCSOLT AS-EK



- A routing táblát az intra- és inter-AS routing protokollok együttműködve állítja össze
  - az intra-AS az AS-en belüli célcímekre
  - az inter-AS és az intra-AS együtt az AS-en kívüli célcímekre

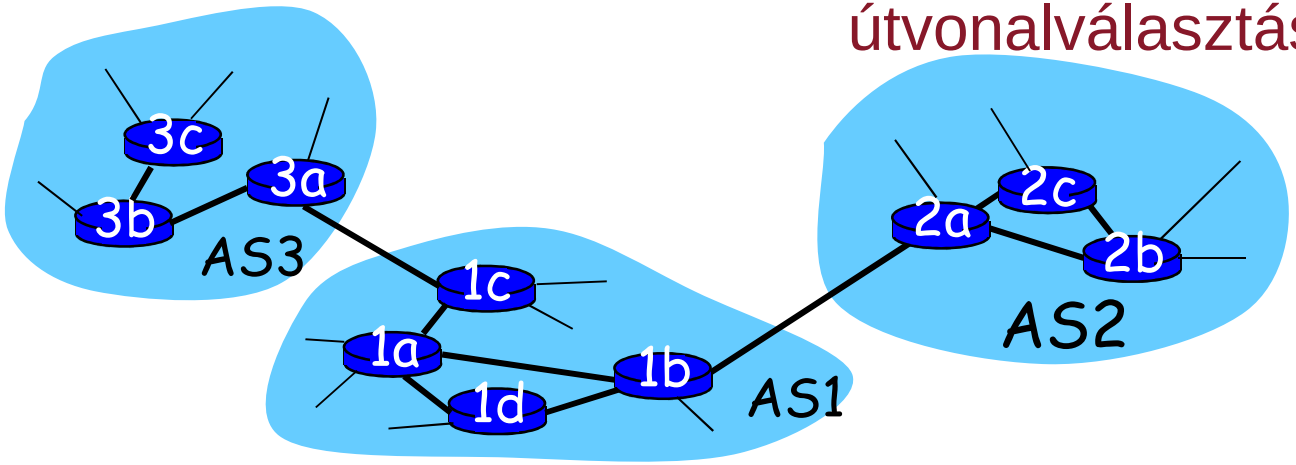
INTER-AS ÚTVONALVÁLASZTÁSI FELADATOK

- Tegyük fel AS1 1d routeréhez érkezik egy datagram AS1-en kívüli célcímmel:
  - A routernek valamelyik gateway-hez kell továbbítani a datagramot, de melyikhez?

AS1-nek :

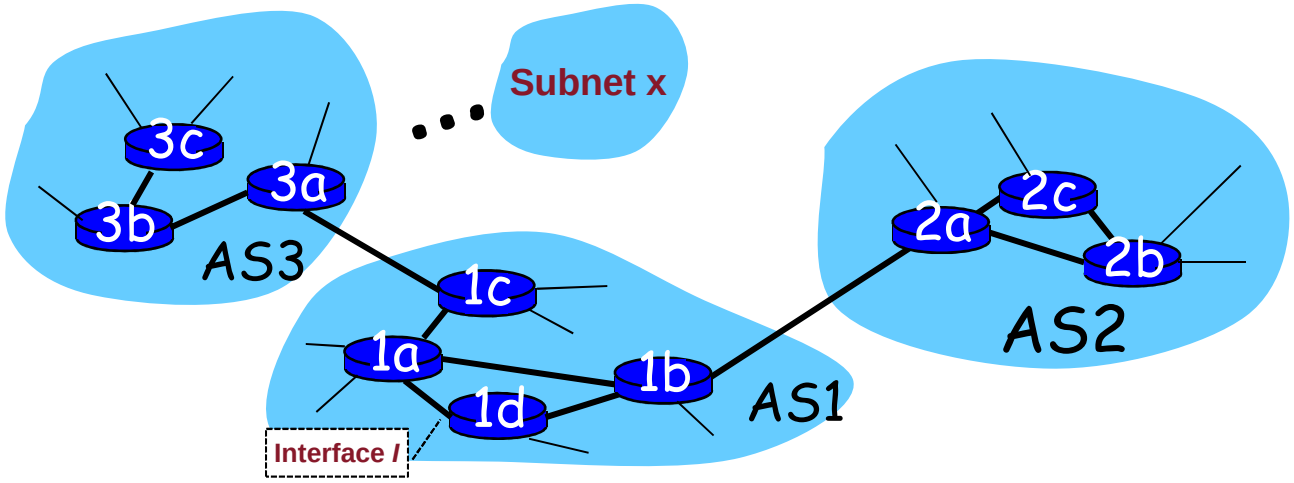
1. meg kell tudnia mely célcímek érhetők el AS2-n, és melyek AS3-n keresztül
2. el kell juttatnia ezt az információt minden AS1-ben lévő routerhez

Ezek az inter-AS útvonalválasztás feladatai!



PÉLDA: AZ 1D ROUTER ROUTING TÁBLÁJÁNAK EGY BEÁLLÍTÁSA

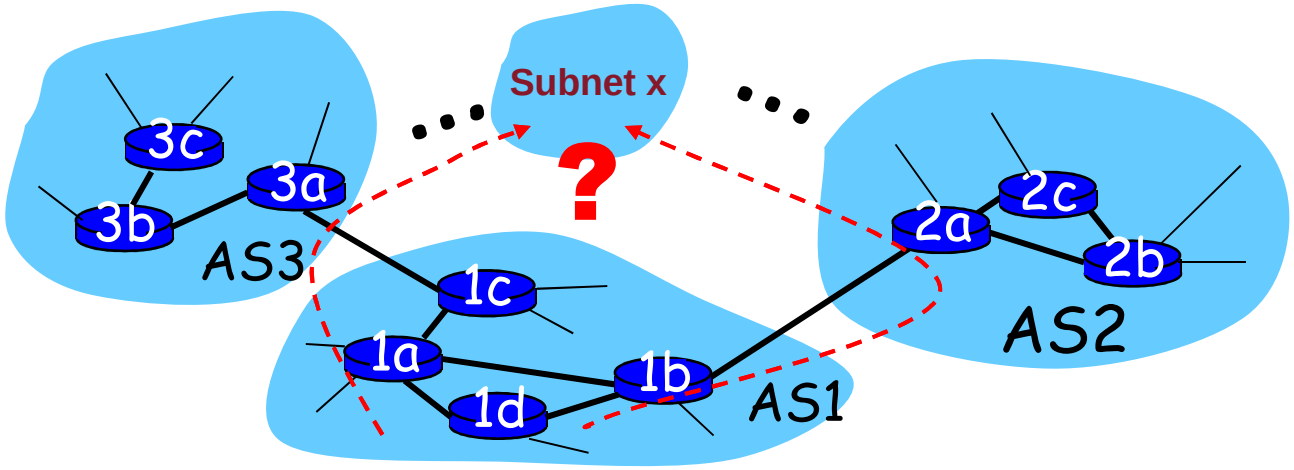
- AS1 megtudja (az inter-AS protokoll segítségével), hogy az *x* subnet az AS3-on (az 1c gateway-en) keresztül elérhető, az AS2-n keresztül nem.
- Az *x* subnet elérhetőségi információját az inter-AS protocol juttatja el AS1 minden routeréhez.
- Az 1d router az intra-AS protokoll segítségével meghatározza, hogy az *I* interfészén keresztül érhető el 1c a legrövidebb úton ,és
  - beállítja az ennek megfelelő routing tábla bejegyzését: *(x,I)*



PÉLDA: VÁLASZTÁS AS-EK KÖZÜL

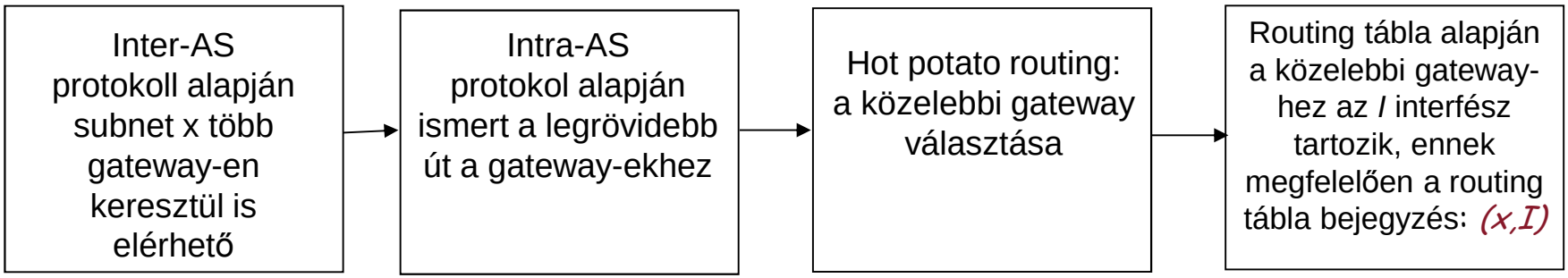
- AS1 megtudja (az inter-AS protokoll segítségével), hogy az *x* subnet az AS3-on (az 1c gateway-en) és AS2-n (az 1b gateway-en) keresztül is elérhető
- Routing táblájának beállításához az 1d routernek meg kell határoznia melyik gateway-en keresztül forgja továbbítani a datagramot az x subnet felé

Ez is az inter-AS útvonalválasztás feladata!



PÉLDA: VÁLASZTÁS NEXT HOP AS-EK KÖZÜL

- AS1 megtudja (az inter-AS protokoll segítségével), hogy az *x* subnet az AS3-on (az 1c gateway-en) és AS2-n (az 1b gateway-en) keresztül is elérhető
- Routing táblájának beállításához az 1d routernek meg kell határoznia melyik gateway-en keresztül fogja továbbítani a datagramot az x subnet felé
- **Hot potato routing**: datagram továbbítása a közelebbi gateway-hez (intra-AS útvonalválasztás alapján)



INTRA-AS ROUTING

- Más néven Interior Gateway Protocols (IGP)
- a legismertebb Intra-AS útvonalválasztó protokollok:
  - RIP: Routing Information Protocol
  - OSPF: Open Shortest Path First
  - IGRP: Interior Gateway Routing Protocol (Cisco tulajdonjog)

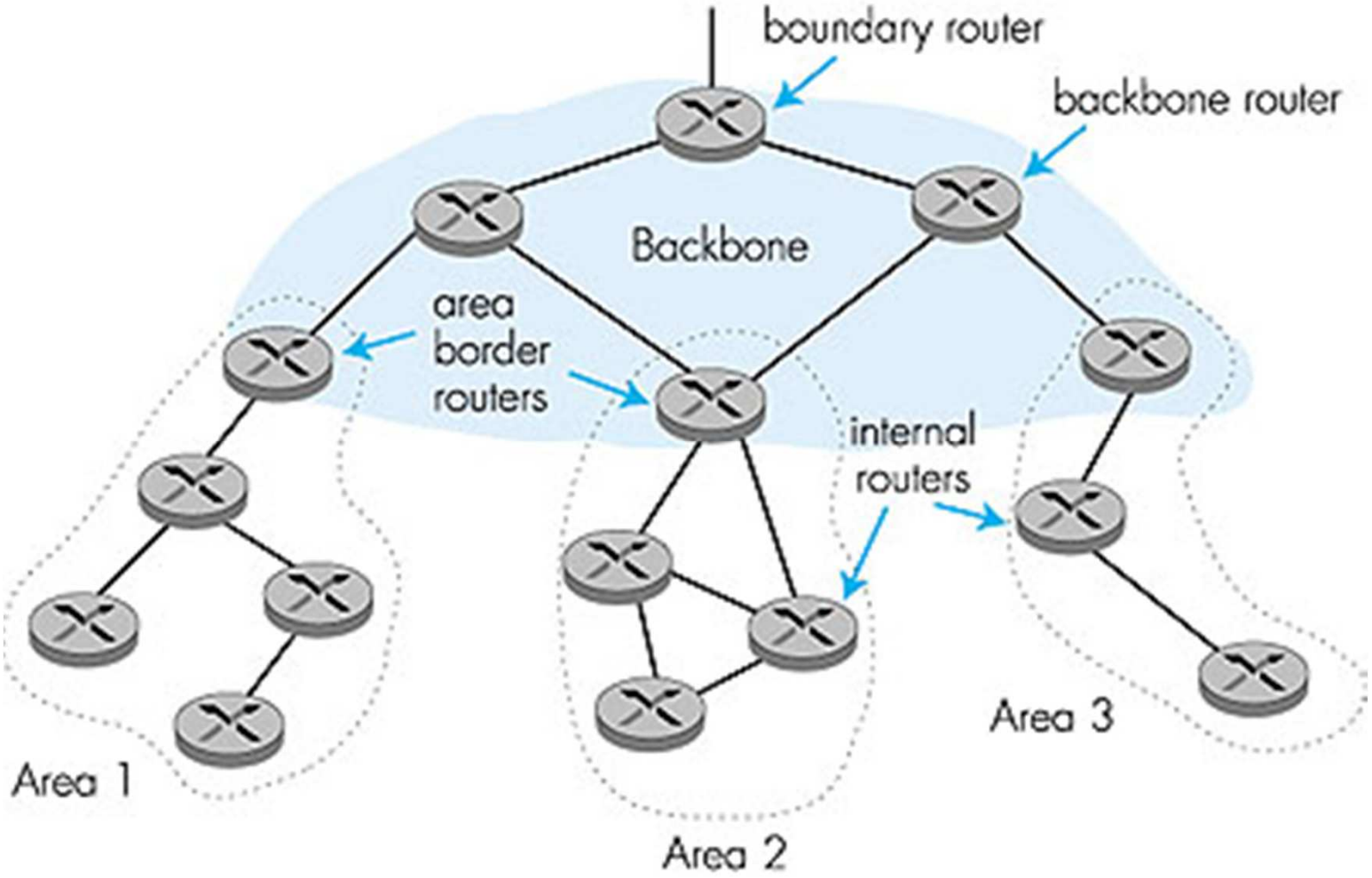
OSPF (OPEN SHORTEST PATH FIRST)

- „open”: nyitott, mindenki számára elérhető specifikáció
- linkállapot alapú
  - linkállapotokat hirdetése
  - ennek alapján hálózat topológiai képe minden routerben
  - Útszámítás Dijkstra-algoritmussal
- az OSPF hirdetmények egy bejegyzést tartalmaznak egy szomszédos routerre
- hirdetmények a **teljes** AS-re (elárasztással)
  - OSPF-üzenetek közvetlenülIP felett (a megbízható átvitel és az üzenetszórás alkalmazási szinten megvalósítva)

OSPF "ADVANCED" FEATURES (NOT IN RIP)

- **biztonság**: minden OSPF üzenet hitelesíthető (rossz szándékú behatolások megakadályozása)
- **több** azonos költségű **minimálút** (ECMP - Equal Cost Multi-Path) kezelése egy célcímre, így az oda menő forgalom megoszthető (a továbbító router feladata)
- Integrált uni- és **multicast** támogatás:
  - a Multicast OSPF (MOSPF) ugyanazt a topológiai adatbázist (aktuális hálózati állapot leírása) használja, mint az OSPF
- **hierarchikus** OSPF a nagyméretű hálózatokban a skálázhatóság javítására

HIERARCHIKUS OSPF



HIERARCHIKUS OSPF

- **kétszintű hierarchia**: helyi (local) és gerinc (backbone) area
- linkállapot hirdetmények elárasztással csak arean belül
  - Minden router részletesen ismeri az area topológiát, de a más areakban lévő célcímekre csak az irányokat (minimálutakat)
- ***area border routerek (ABR):*** összesítik a távolságokat az areajukban elérhető célcímekre, és ezt hirdetik más areak .ABR-jeinek
- ***backbone routerek:*** a kitüntetett gerinc area OSPF-jét futtaják.
- ***AS-határ (boundary) routerek:*** más AS-ek felé kapcsolódást biztosítanak

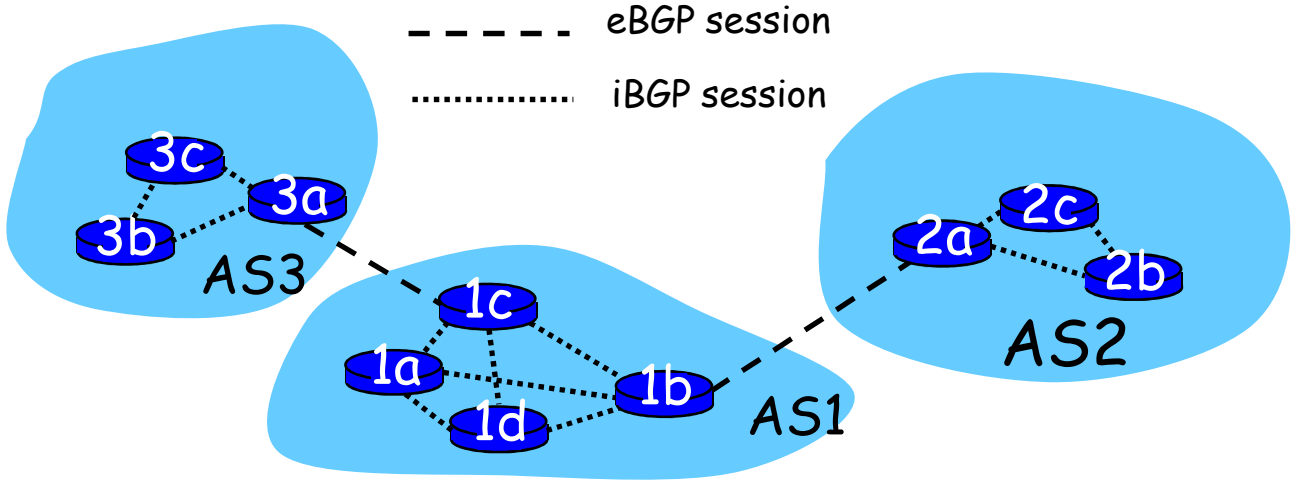
INTERNET INTER-AS ROUTING: BGP

- **BGP (Border Gateway Protocol):** a *de facto* szabvány
- a BGP biztosítja minden AS számára:
  1. A szomszédos AS-eken keresztül elérhető célcímekre vonatkozó információkat.
  2. Megosztja ezeket az elérhetőségi információat az AS összes routerével.
  3. Meghatározza a “jó” utakat a célcímekre az elérhetőségi információk és a forgalomirányítási politika (reachability information and policy) alapján.
- lehetővé tesz az alhálózatok számára, hogy az összes AS-nek hirdessék létezésüket : ***“itt vagyok”***

BGP ALAPOK

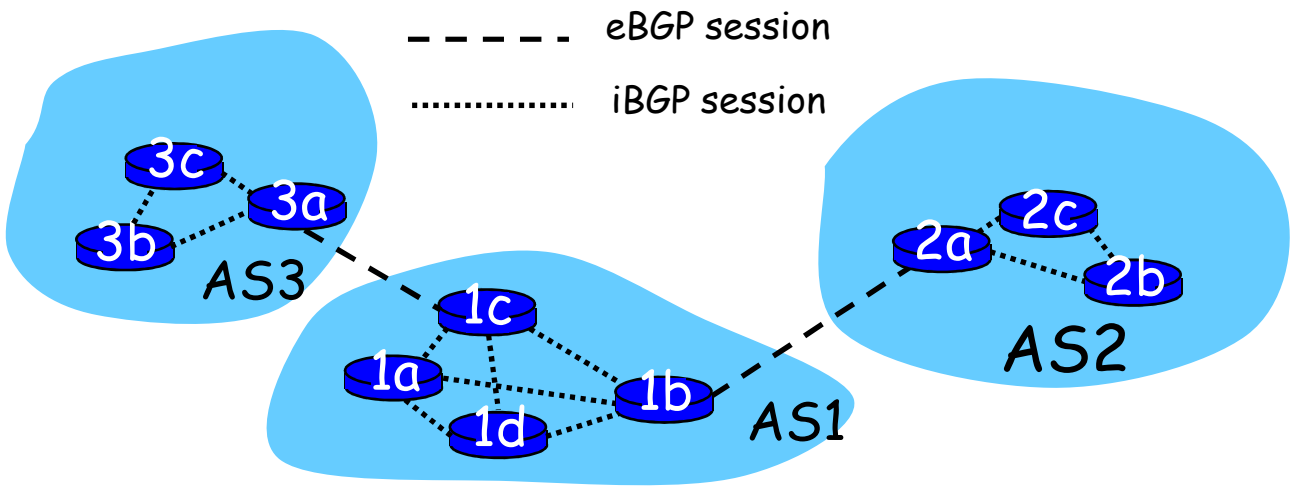
- Két router (BGP peers) routing információkat cserél részleges állandó (semi-permanent) TCP kapcsolatokon: **BGP session**
  - különöző AS-ekben lévő routerek között external: **eBGP**,
  - azonos AS-ben lévő routerek köztött internal: **iBGP**
  - a BGP session nem kell, hogy fizikai kapcsolatoknak feleljenek meg
- amikor az AS2 hirdet egy prefixet (nem célcímet, hanem egy alhálózat, vagy alhálózatok csoportjának címét) AS1-nek:
  - AS2 ***megígéri,*** hogy továbbítja a datagramokat az adott prefix felé
  - AS2 összevonhatja (aggregate) a prefixeket hirdetményeiben

(az összevonások során hierarchikus címzés kapcsán bemutatott példában - 40. slide - megismert *longest match*, *more specific prefix* megoldás ebben az esetben is alkalmazható)



ELÉRÉSI INFORMÁCIÓK TERJESZTÉSE

- A 3a és 1c között felépített eBGP sessionön AS3 elküldi az általa ismert és terjesztett prefix reachability információkat AS1-nek.
  - ennek alapján 1c az iBGP-t használva eljutatja az információkat minden routernek AS1-ben
  - 1b tovább tudja ezeket hirdetni AS2nek a 1b-2a eBGP sessionön
- Amikor a routerek új prefixekről értesülnek létrehozzák az ezekhez tartozó bejegyzéseket routing táblájukban.

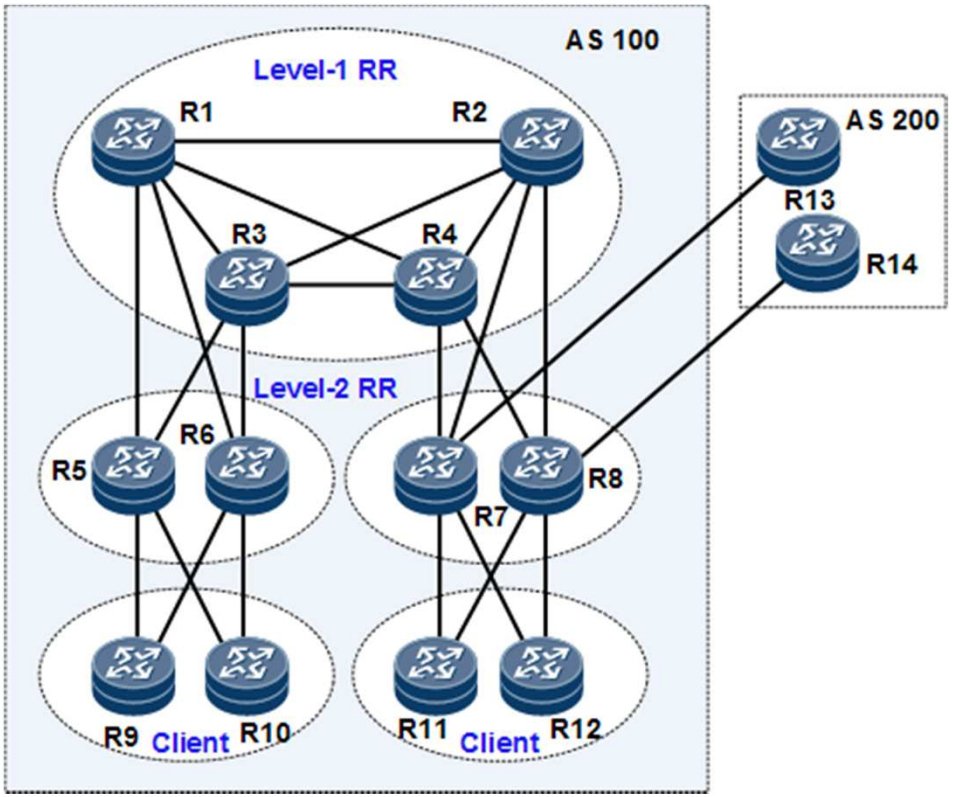


BGP ROUTE REFLECTOR

- Teljes szövevény iBGP sessionok skálázhatóságára új funkció (n peer esetén nx(n-1)/2 session kellene)
- BGP információk megosztása kitüntetett szerepű routerek (**route reflector** - RR) beiktatásával

Egy tipikus hálózati elrendezés hierarchikus RR-ekkel

- R1, R2, R3, és R4 Level-1 RR;
- R5, R6, R7, és R8 Level-2 RR és az Level 1 RR-ek kliense.
- a Level-1 RR-k teljes szövevénnyel összekapcsolva (semmilyen szinten nem kliensek).
- a Level-2 RR-ket a Level-1 RR-k klienseiként nem kell teljes szövevénnyel összekapcsolni
- R13 és R14 egy másik AS (AS 200) kapcsolódását illusztrálják



Forrás: https://support.huawei.com/enterprise/en/doc/EDOC1100055375/a2762e21/configuring-a-bgp-route-reflector

ÚTATTRIBUTUMOK ÉS BGP UTAK

- A hirdetett prefixhez BGP attribútumok társulnak
  - prefix + attributes = “route”
- két lényeges attribútum:
  - **AS-PATH**: tartalmazza, hogy a prefix hirdetése mely AS-eken keresztül érkezett: e.g, AS 67, AS 17
  - **NEXT-HOP**: megadja, hogy az adott AS-ben melyik a next hop router a nex hop AS felé
- Amikor egy gateway router BGP route advertisement-et kap, **import policy**ja alapján eldönti, hogy mit fogad el (mit hirdet tovább) és mit nem.

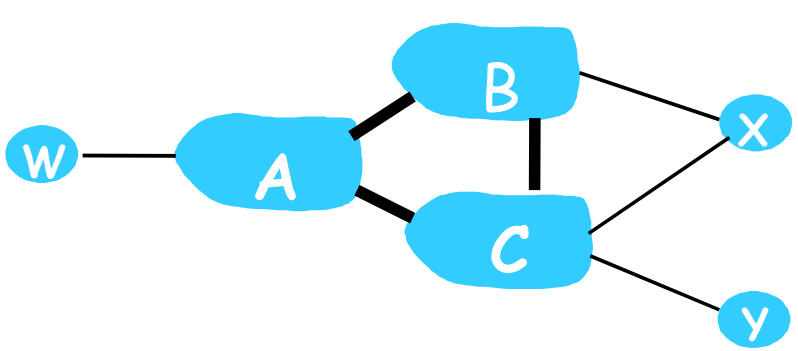
BGP ÚTVONALVÁLASZTÁS

- A BGP route advertisementek alapján egy router több utat is megtanulhat egy adott prefix felé, ezek közül kell egyet kiválasztania (a többit törölnie)
- törlési szekvencia:
  1. local preference value attribute: policy alapú döntések
  2. shortest AS-PATH
  3. closest NEXT-HOP router: hot potato routing
  4. további kritériumok

BGP ÜZENETEK

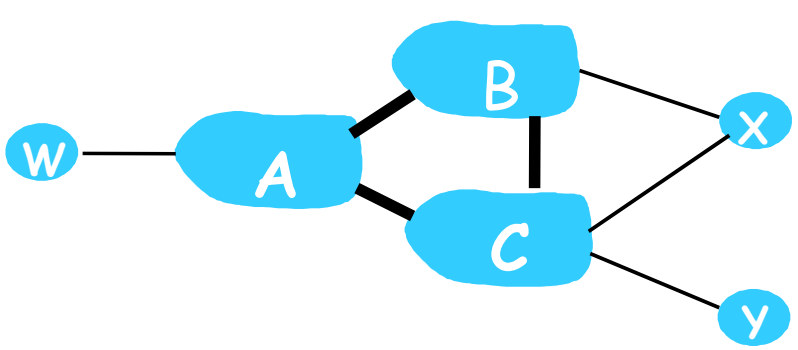
- BGP üzenetváltások TCP felett
- BGP üzenetek:
  - **OPEN**: megnyitja a TCP kapcsolatot és hitelesíti a küldőt
  - **UPDATE**: új út hirdetése, vagy korábban hirdetett visszavonása
  - **KEEPALIVE**: a kapcsolat fenntartása UPDATE-ek hiányában; vagy ACK az OPEN kérésre
  - **NOTIFICATION**: hibajelzés megelőző üzenetre; de a kapcsolat lezárására is használják

BGP ROUTING POLICY PÉLDA



- A,B, és C szolgáltatói hálózatok (fizetett szolgáltatásként továbbítják a forgalmat az ügyfélhálózatok és a külvilág között, mindháromnak van – az ábrán nem jelölt – kapcsolata világ felé)
- X,W, és Y (a szolgáltatók) ügyfélhálózatai (kizárólag a szolgáltatói hálózatokon kapcsolódnak a világhoz)
- X hálózat (pl. redundancia okokból) két szolgáltatói hálózathoz is csatlakozik (**dual-homed**):
  - X nem akar forgalmat továbbítani B-ből (X-ne át) C-be
  - .. ezért X nem fog B-nek utat hirdetni C felé

BGP ROUTING POLICY PÉLDA



- A hirdeti az A-W utat B-nek
- B hirdeti a B-A-W utat X-nek
- Szükséges B-nek hirdetnie a B-A-W utat C-nek?
  - Semmiképpen! B-nek származik bevétele a C-B-A-W úton továbbított forgalomból, mivel sem W sem S nem B ügyfele
  - B arra akarja kényszeríteni C-t, hogy W felé A-n keresztük küldjön forgalamt
  - B *kizárólag* saját ügyfelei forgalmát akarja továbbítani

MIÉRT SZÜKSÉGES KÜLÖN INTRA- ÉS INTER-AS ROUTING ?

Policy:

- Inter-AS: az elsődleges kérdés, hogy kinek a forgalma továbbítódik a hálózaton keresztül (tranzitforgalom)
- Intra-AS: az elsődleges kérdés, hogy hogy továbbítódik a forgalom a hálózatban (induló és végződő forgalom)

Méret:

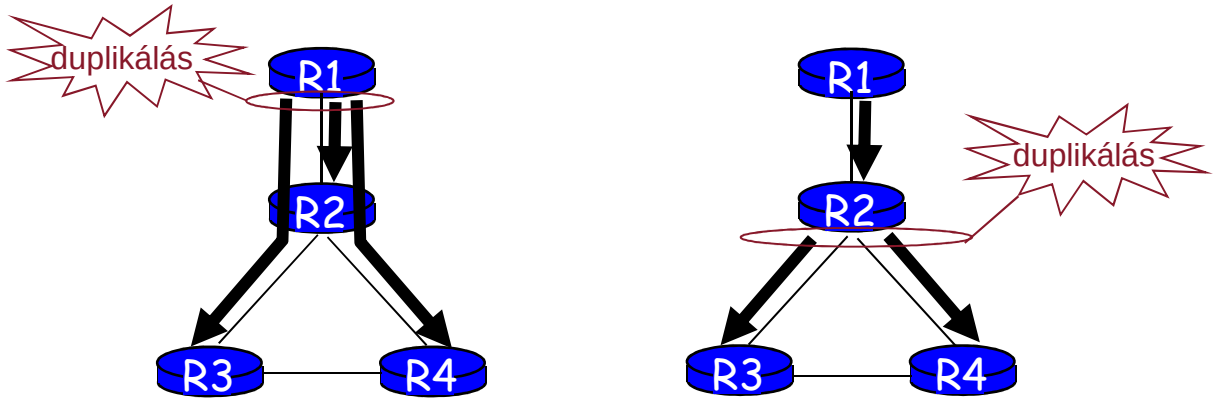
- a hierarchikus útvonalválasztás jobban skálázódik (kisebb routing táblák, kisebb jelzésforgalom)

Teljesítmény:

- Intra-AS: az erőforrások hatékony kihasználására fókuszál (pl. minimális utak)
- Inter-AS: a policy felülírhatja az erőforrás-hatékonyságot (kerüljük el ASx-et)

BROADCAST ROUTING

- csomagok eljuttatása a forrástól minden csomópontnak
- elvileg unicast küldésekkel is megvalósítható, de a csomagtöbbszörözés a forrásnál nem hatékony (ugyanaz a csomag több példányban, egymással párhuzamosan továbbítva



többszörözés a forrásnál

többszörözés a hálózatban

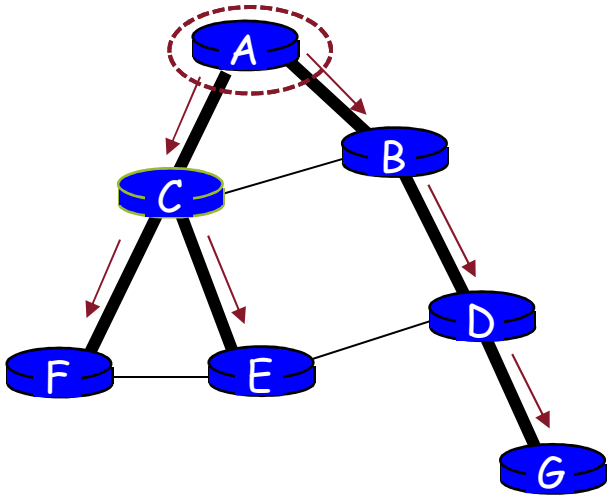
- többszörözés a forrásnál: hogyan tudja a forrás a nyelők címét meghatározni?

CSOMAGTÖBBSZÖRÖZÉS A HÁLÓZATBAN

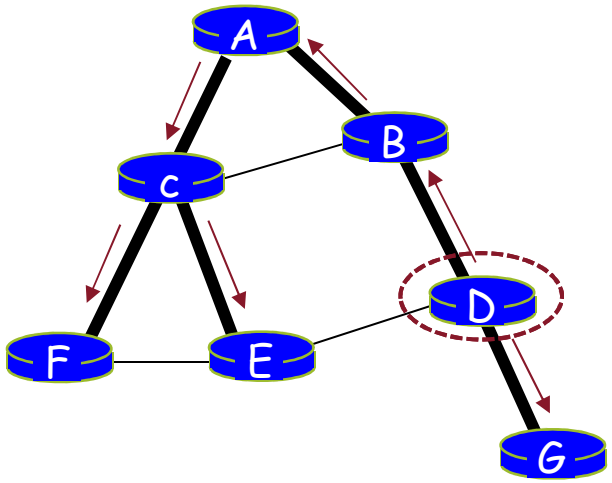
- Egyszerű elárasztás (flooding): amikor egy csomópont megkap egy broadcast csomagot, annak másolatát elküldi minden szomszédjának
  - problémák: hurkok & broadcast storm
- Ellenőrzött elárasztás: egy csomópont csak azokat a broadcast csomagot amelyek korábban még nem küldött
  - a csomópont nyilvántartja a már továbbküldött broadcast csomagokat, vagy
  - a reverse path forwarding (RPF) elvnek megfelelően: csak azokat a broadcast csomagokat küldi tovább, amelyek a forráshoz vezető minimálutja felől érkeztek
- Feszítő fa (spanning tree) alapú továbítás
  - Bármely két csomópont között csak egyetlen út, nincs redundáns csomag küldés

FESZÍTŐ FA

- első lépésben feszítő fa meghatározása
- A csomópontok a broadcast csomagok másolatait a f
  a mentén továbbítják



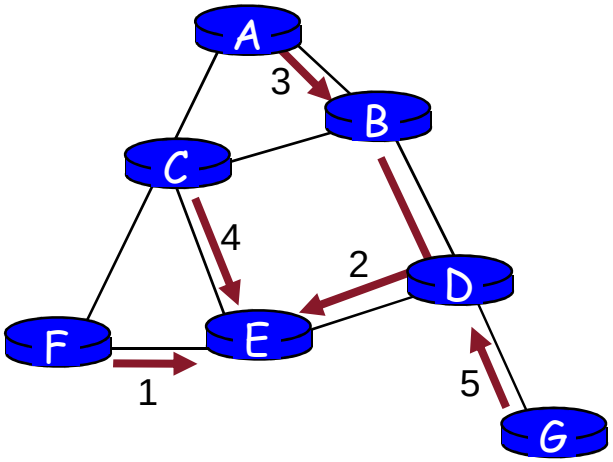
(a) A forrású broadcast egy feszítő fája



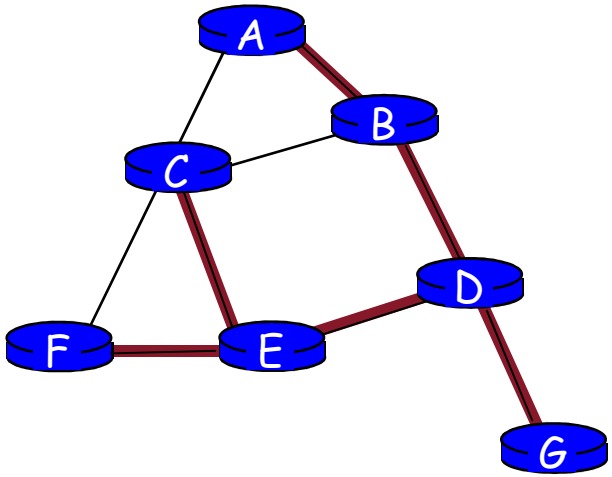
(b) D forrású broadcast egy feszítő fája

FESZÍTŐ FA LÉTREHOZÁSA

- Központi csomópont (root) kiválasztása
- Minden csomópont üzenetet küld a központi csomópontnak
  - az üzenet addig továbbítódik, míg el nem érkezik egy olyan csomóponthoz, ami már a fában van



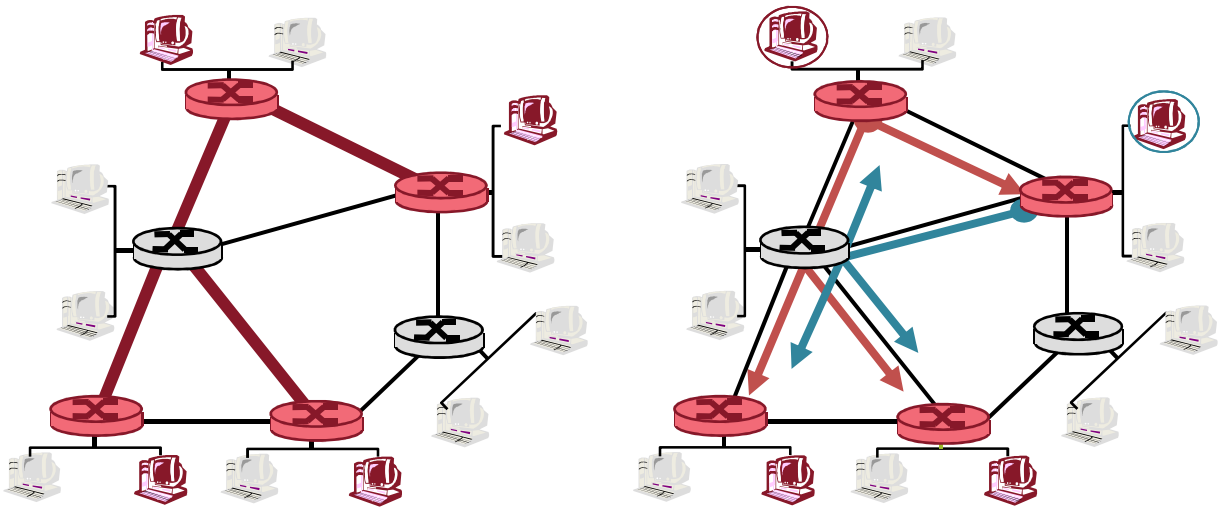
(a) A feszítő fa kialakításának lépései



(b) A kialakított feszítő fa

MULTICAST ROUTING: A MEGOLDANDÓ FELADAT

- A multicast csoport tagjai között több forrás is lehet
- ***Cél:*** fát (vagy fákat) találni ami(k) összeköti(k) a multicast csoport tagjait
  - *fa (tree):* csak egy út minden csoporttaghoz
  - *forrás alapú fa (source-based tree):* különböző fa minden küldőtől az összes csoporttaghoz
  - *osztott fa (shared tree):* ugyanazt a fát használja minden csoporttag



Shared tree

Source-based trees

L3 ÖSSZEFOGLALÁS

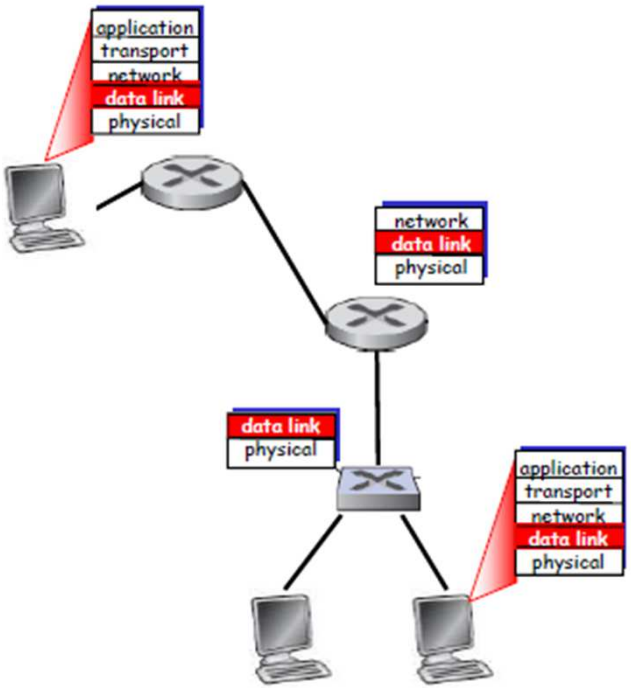
- címzés: hálózati cím és hálózaton belüli hoszt azonosítása (változó megosztással: VLSM)
- a címtartományok jobb kihasználhatóságához CIDR
- nem „vihető ki” az IP cím az alhálózatból
- másik alhálózatba (L3 subnet) átkerülő hosztnak másik (az adott alhálózatban lévő) IP cím kell

Néhány adatkapcsolati réteg vonatkozás áttekintése:

MAC-címek, kapcsolás, L3-L2 címfeloldás,

AZ ADATKAPCSOLATI RÉTEG ÉS SZOLGÁLTATÁSAI

- Cél: hálózati **datagram átvitele kétszomszédos**, hálózati funkciót megvalósító elem között
- A szomszédos elemek között egy **link** (adatkapcsolat) van
  - Vezetékes link
  - Vezetéknélküli link
  - LAN
- A link egyik végén a datagramok **keretekbe csomagolása**
- A link másik végén a megérkezett datagram kicsomagolása és átadása a hálózati rétegnek
- Az egyes linkeken eltérő protokoll lehet, eltérő szolgáltatásjellemzőkkel
  - Például IEEE802.11, GigabitEthernet
  - Eltérő sebesség
  - Eltérő biztonság
- Keretezés
  - Fej- és farokrész (**Header és Trailer**) illesztése az adathoz
- Hozzáférés az átviteli médiához
  - Mi legyen, ha több szomszéd egyszerre akar adni ugyanazon a linken?
- Címzés **fizikai cím** alapján
  - A cél-szomszéd azonosításához
  - Nem a logikai (IP) címről van szó
- Keretek megbízható átvitele
  - Pufferelés a végpontokon
  - **Bithibadetekció** (esetleges újraküldetés)
  - Bithibakorrekció
- Küldési irányok kezelése egy linken
  - Szimplex
  - Félduplex
  - Duplex (full-duplex)

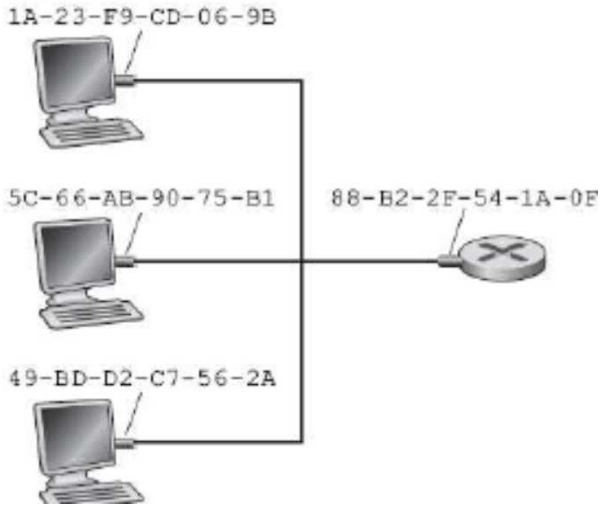


L2 ALRÉTEGK, FUNKCIÓK

- Logical Link Layer (**LLC**) alréteg
  - Az adat átvitelét szervezi
  - Multiplexáló funkció – a felsőbb rétegből érkező PDU-kra
  - Hibadetekció és hibajavítás
- Hibadetekció
  - **Redundáns bitek** a trailer-ben
  - Nem csak az adatra (datagram), hanem a fejrészre is vonatkozhat
  - Nem minden hiba észlelhető, mert nem csak egy bit lehet hibás
  - Például: paritásbit, transzport réteg ellenőrző összeg
- Hibajavítás
  - Nem csak észleljük, hogy hiba volt, hanem azt is tudjuk hol
  - Például: kétdimenziós paritás, ciklikus redundancia – CRC
- Media Access Control (**MAC**) alréteg

MAC CÍM ÉS HASZNÁLATA, KIOSZTÁSA

- Logikai cím – „egyedi” azonosítás az Interneten (globális)
  - A hálózati rétegben használt cím (IPv4, IPv6)
  - Cél a datagram továbbítása távoli hálózatba
  - Az alhálózat elhelyezkedése kikövetkeztethető
- Fizikai cím – egyedi **azonosítás az alhálózatban** (lokális)
  - Az adatkapcsolati rétegben használt cím (MAC cím)
  - Cél: egy keret továbbítása egy szomszédos elemhez, aminek van logikai címe (végpont, router interfész)
  - Nem fontos az alhálózat globális elhelyezkedése, mert csak azon belül használjuk
  - 48 bites azonosító
    - A hálózati adapter (kártya, port) ROM-jába égetve
    - Esetleg szoftverrel beállítható a használt érték
  - Olvasható formátum – hexaszámokkal leírt bájtok
    - Például: 01-23-45-67-89-ab vagy 01:23:45:67:89:ab
- Az adatkapcsolati réteget megvalósító technológiákban
  - Ethernet (IEEE 802.3)
  - WIFI (IEEE 802.11)
  - Bluetooth
  - Korábban Token Ring (IEEE 802.5), FDDI (IEEE 802.4 token bus), ATM
- Az (al)hálózaton, LAN-on belül egyedi címnek kell lennie
  - Szórási (broadcast) cím az L2-ben: FF-FF-FF-FF-FF-FF
  - Többesadás (multicast) címek: 01-00-05-xx-xx-xx
- A kiosztást az IEEE felügyeli
  - Az egyes gyártók a teljes címtér egy részét vásárolják meg
  - Az első három bájt: Organizationally Unique Identifier – OUI
- • MAC cím
  - **Nincs hierarchia** – hordozható
  - Egy hálózati kártya átvihető egy másik LAN-ba
- IP cím
  - Hierarchikus szervezés – nem hordozható
  - Egy végpont nem tehető át (egyszerűen) egy másik hálózatba az IP címével együtt, szükség van annak átírására



CÍMFELOLDÁS

- Milyen fizikai címre küldjük L2-ben az adott IP című DATAGRAMOT?
- Address Resolution Protocol (**ARP**)
- A hálózati elemek tárolják a feloldott címeket, a logikai cím – fizikai cím összerendelések, adott idő (pl. 20 perc) után törlődik egy bejegyzés

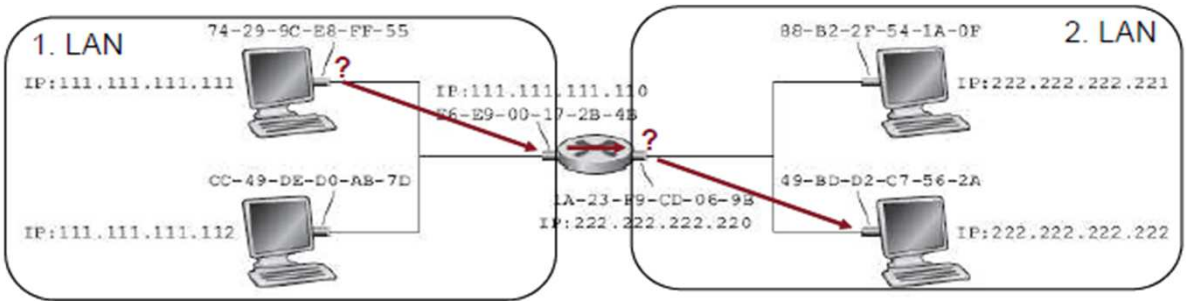
Az ARP működése

Az ARP automatikusan indul, nincs szükség kézi konfigurációra

1. Az A hoszt a B hosztnak küldene egy datagramot
   - B MAC címe nincs még benne az A hoszt arp táblájában
2. Az A elküld egy ARP-Query keretet a B IP címével
   - A broadcast MAC címre
   - A LAN összes hosztja és interfésze megkapja a keretet
3. B felismeri a saját IP címét és válaszol egy ARP-Replay kerettel
   - A válasz keretet A-nak címzi
   - A válasz tartalamazza B MAC címét
4. Az A felveszi a B IP címét feloldó bejegyzést az arp táblájába
5. Az A el tudja küldeni a datgramot B-nek
   - A most már ismert MAC címet használva a kerethez

Datagram küldése másik hálózatba

- A datagramot az alapértelmezett átjárón (default gateway) át kell küldenünk
  - Router interfész címének feloldása (az 1. LAN-ban) – ARP
  - Keret átküldése a routernek
  - Datagram kicsomagolása a keretből
- Továbbítás a routing tábla alapján
  - Célcím feloldása a megfelelő (a 2.) LAN-ban - ARP
  - Datagram becsomagolása
  - Keret átküldése a hosztnak



LAN-OK, SWITCH MŰKÖDÉSE

LAN-ok

- Szomszédos hálózatelemek
  - Logikailag szomszédos elemek halmaza
  - Vezetéknélküli esetben fizikailag is szomszédok
- Ütközés (collision) – a közegre (médiumra) kerülő keretek egymást zavarják
- Ismétlő (repaeter) funkció
  - Két kábel fizikai összekötése
  - Ma már inkább több kábelt összekötő eszközzel – hub
  - Minden keret megjelenik minden kábelen – logikailag egy közeg
- Kapcsoló (switch) funkció
  - Kezeli az adatkapcsolati rétegbeli PDU-kat (kereteket)
  - Szétdarabolja a LAN-t különálló közegekre
  - Csökkenti az ütközések valószínűségét

Switch működése

- Keretek feldolgozása
  - A kereteket nem neki, csak rajta keresztül küldik
  - A kapott keretet puffereli
  - A MAC cím alapján eldönti, hogy melyik irányba továbbítsa
- Ezzel csökken az ütközés esélye
- A továbbítás kicsit hasonlít a routingra, de
  - Csak a LAN-on belül megy
  - Sokkal egyszerűbb
  - Sokkal gyorsabb
- Transzparens funkció
  - A hosztok nem tudják, hogy vannak switchek a LAN-ban
- Automatikus tanulás – MAC learning
  - Nem kell külön konfigurálni
- Hatékonyság
  - Akár több keret is átmehet a hálózaton egyidőben, ütközés nélkül

SWITCH: MAC CÍMEK TANULÁSA

- A switch egy táblázatban tartja nyilván a MAC cím – port párokat
- Tanulás a switchhez érkező keretek forráscímei alapján
- Ha nincs a táblában a keresett cím, akkor minden irányba kiküldi, kivéve arra, amerről jött
- Adott idő után elfelejti (vagy törölhető)

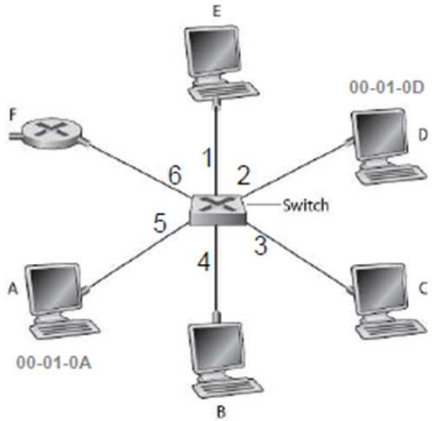
IP datagramot tartalmazó keret küldése A-ból D-be

- A cél MAC címe már ismert A-ban
- A kapcsoló címtáblája üres

Lépések

1. Keret küldése A-ból
2. Keret érkezik az 5-ös porton
3. Címtábla frissítése A MAC címével
4. Keret szétküldése az 1,2,3,4 és 6 portokon (floding)
5. Keret fogadása D-ben

MAC cím	Port
00-01-0A	5



D válaszol A-nak

- A kapcsoló címtáblájában csak A MAC címe szerepel

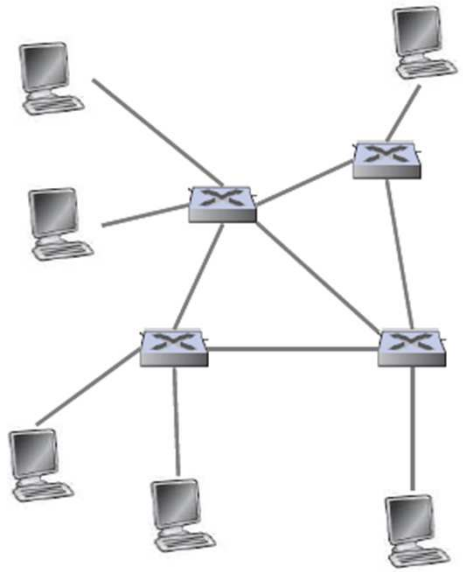
Lépések

1. Keret küldése D-ből
2. Keret érkezik a 2-es porton
3. Címtábla frissítése D MAC címével
4. Keret kiküldése az 5-ös porton (a kapcsoló előzőleg már megtanulta)
5. Keret fogadása A-ban

MAC cím	Port
00-01-0A	5
00-01-0D	2

TÖBB SWITCHBŐL ÁLLÓ LAN, REDUNDÁNS TOPOLÓGIA

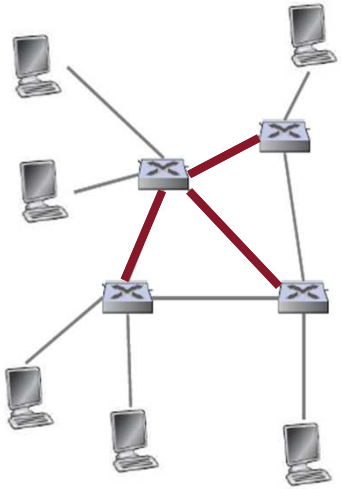
- Portok a switchben
  - Nagyszámú, de véges
- A LAN méretének növelése
  - Nagyobb switch – több port (egy határon túl nem skálázható)
  - Több switch kell
- Switch bemenetén nem csak egy hoszttól jöhetnek keretek
  - A MAC táblában több cím is lehet ugyanahhoz a porthoz rendelve

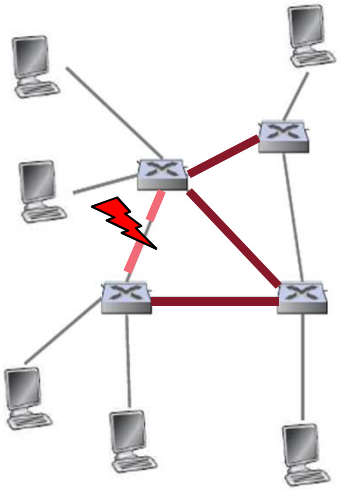


- Portok a switchben
  - Nagyszámú, de véges
- A LAN méretének növelése
  - Nagyobb switch – több port (egy határon túl nem skálázható)
  - Több switch kell
- Switch bemenetén nem csak egy hoszttól jöhetnek keretek
  - A MAC táblában több cím is lehet ugyanahhoz a porthoz rendelve
- Nagyobb LAN-okban sérülékenységet jelenthet, ha minden csak egyszeresen van összekötve
  - Fa szerkezetű gráf
  - Egy kábel hibája szétvághatja a hálózatot
- Redundancia
  - Többszörösen összekötött gráf
  - Hiba esetén is legyen alternatíva
- Hibamentes esetben
  - A szerkezetben lévő körök miatt továbbítási hurkok alakulhatnak ki (floding -> broadcast storm)
  - A switch a tanulás során felesleges irányokban is kiküldhet kereteket, nem egyértelmű, hogy merről (melyik portra) érkezik egy adott forrás MAC című keret a switchez

FESZÍTŐ FA

- A megoldás
  - Csak erre kiválasztott linkeken menjen forgalom
  - Feszítőfa képző protokoll – Spanning Tree Protocol (STP)
- Hiba esetén
  - Spanning Tree frissítése
  - Az eredetileg nem használt linkekkel egészítik ki a fát a leszakadt switch(ek) csatlakozásának helyreállításához
  - Továbbra is hurokmentes
- Új elem csatlakozása esetén változik a kép
  - Új switch
  - Switchek között új link
  - Spanning Tree frissítése
- Ha egy hoszt átkerül egy másik portra, akkor egy egyszerű broadcast keret kiküldésével a változás minden switchen azonnal érvényesíthető





L2 ÖSSZEFOGLALÁS

- XXX