Számítógépes Hálózatok

10. Előadás: Hálózati réteg 3

Based on slides from **Zoltán Ács ELTE** and D. Choffnes Northeastern U., Philippa Gill from StonyBrook University , Revised Spring 2016 by S. Laki

IPv6

Fogyó IPv4 címek

- Probléma: az IPv4 címtartomány túl kicsi
  - 2^{32} = 4,294,967,296 lehetséges cím
  - Ez kevesebb mint egy emberenként
- A világ egy részén már nincs kiosztható IP blokk
  - IANA az utolsó /8 blokkot 2011-ben osztotta ki

Régió	Regional Internet Registry (RIR)	Utolsó IP blokk kiosztása
Asia/Pacific	APNIC	April 19, 2011
Europe/Middle East	RIPE	September 14, 2012
North America	ARIN	13 Jan 2015 (Projected)
South America	LACNIC	13 Jan 2015 (Projected)
Africa	AFRINIC	17 Jan 2022(Projected)

IPv6

- IPv6, 1998(!)-ban mutatták be
  - 128 bites címek
  - 4.8 * 10^{28} cím/ember
- Cím formátum
  - 16 bites értékek 8 csoportba sorolva (‘:’-tal elválasztva)
  - Minden csoport elején szereplő nulla sorozatok elhagyhatók
  - Csupa nulla csoportok elhagyhatók , ekkor ‘::’

2001:0db8:0000:0000:0000:ff00:0042:8329

2001:db8:0:0:0:ff00:42:8329

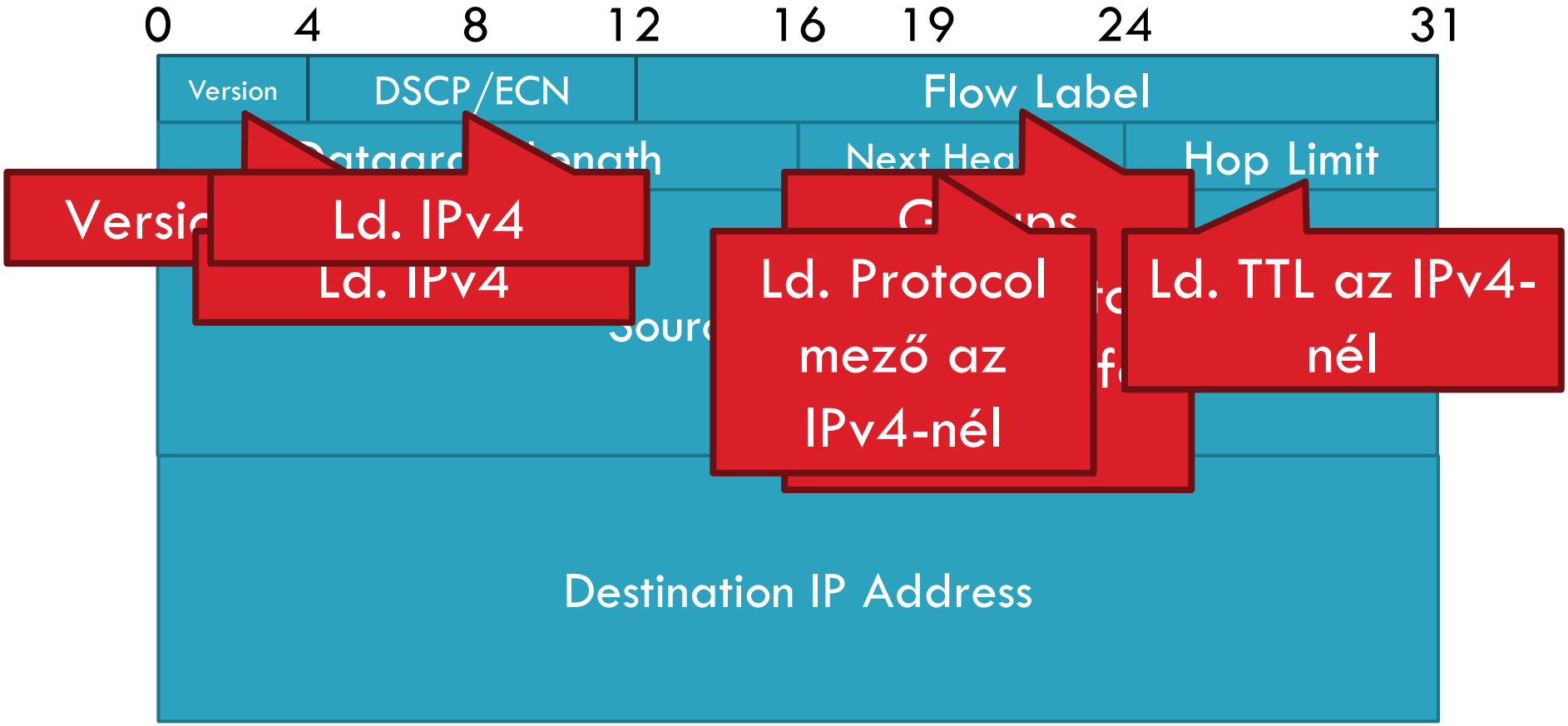
2001:db8::ff00:42:8329

IPv6

- Ki tudja a localhost IPv4 címét?
  - 127.0.0.1
- Mi ez az IPv6 esetén?
  - ::1

IPv6 Fejléc

- Az IPv4-nél látott kétszerese (320 bit vs. 160 bit)



Különbségek az IPv4-hez képest

- Számos mező hiányzik az IPv6 fejlécből
  - Fejléc hossza – beépült a Next Header mezőbe
  - Checksum – nem igazán használták már korábban se…
  - Identifier, Flags, Offset
    - IPv6 routerek nem támogatják a fragmentációt
    - Az állomások MTU felderítést alkalmaznak
- Az Internet felhasználás súlypontjainak megváltozása
  - Napjaink hálózatai sokkal homogénebbek, mint azt kezdetben gondolták
  - Azonban a routing költsége és bonyolultsága domináns

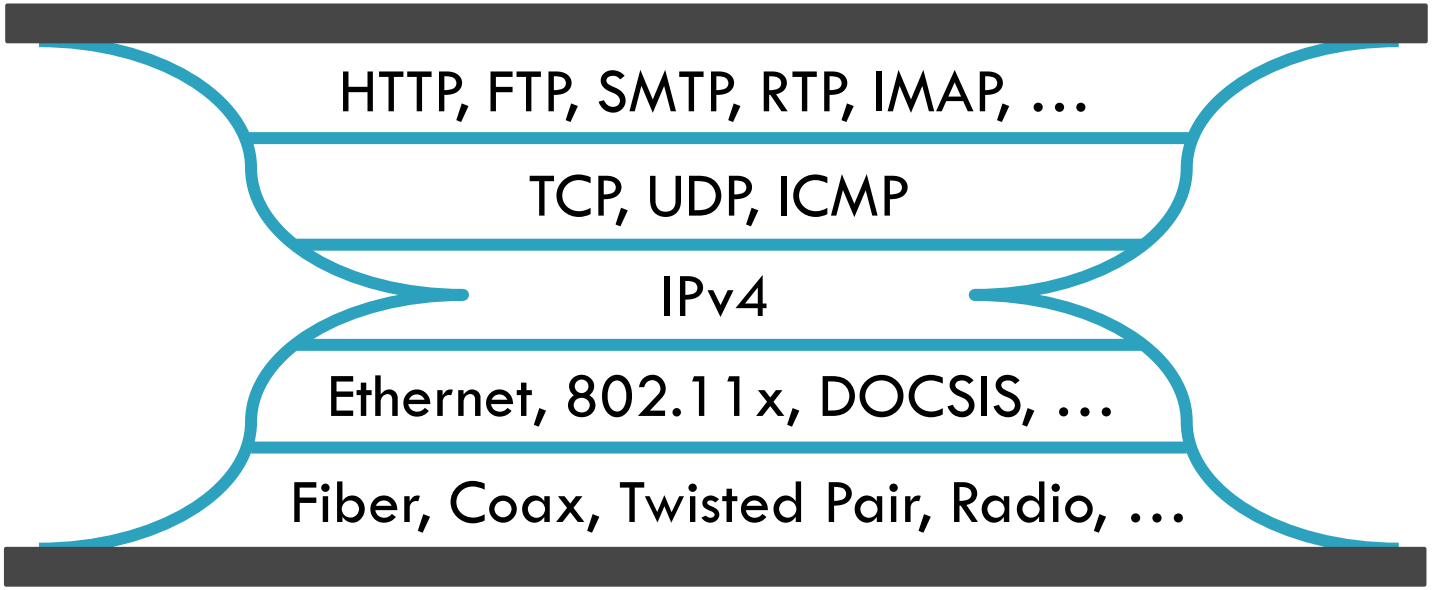
Teljesítmény növekmény

- Nincsenek ellenőrizendő kontrollösszegek (checksum)
- Nem szükséges a fragmentáció kezelése a routerekben
- Egyszerű routing tábla szerkezet
  - A cím tér nagy
  - Nincs szükség CIDR-re (de aggregáció szükséges)
  - A szabványos alhálózat méret 2^{64} cím
- Egyszerű auto-konfiguráció
  - Neighbor Discovery Protocol

További IPv6 lehetőségek

- Forrás Routing
  - Az állomás meghatározhatja azt az útvonalat, amelyen a csomagjait továbbítani szeretné
- Mobil IP
  - Az állomások magukkal vihetik az IP címüket más hálózatokba
  - Forrás routing használata a csomagok irányításához
- Privacy kiterjesztések
  - Véletlenszerűen generált állomás azonosítók
  - Megnehezíti egy IP egy adott állomáshoz való kapcsolását
- Jumbograms
  - 4Gb-es datagramok küldése

Bevezetési nehézségek



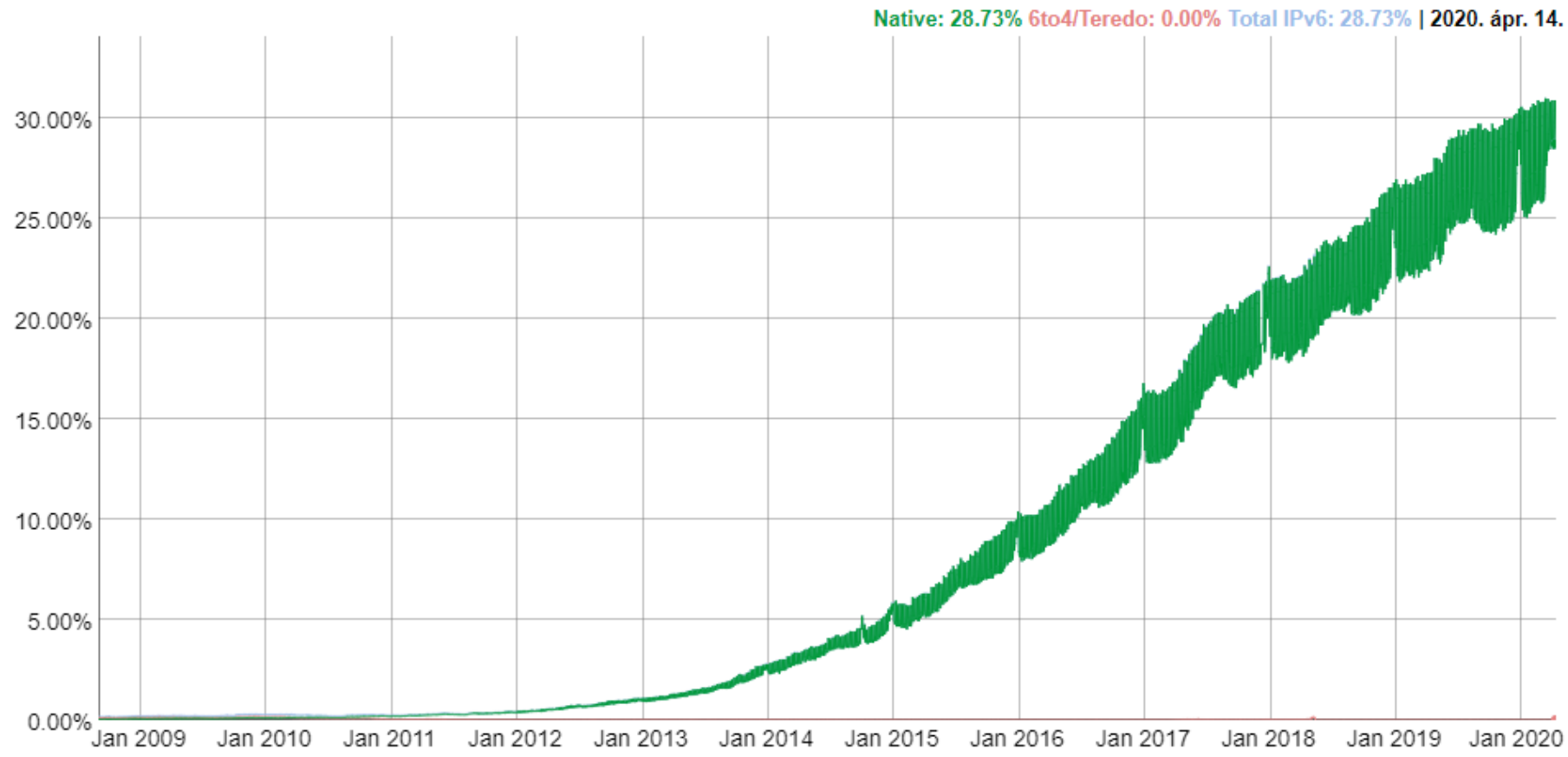
- IPv6 bevezetése a teljes Internet frissítését jelentené
  - Minden router, minden hoszt
  - ICMPv6, DHCPv6, DNSv6
- 2013: 0.94%-a a Google forgalmának volt IPv6 feletti
- 2015: ez 2.5%

https://www.google.com/intl/en/ipv6/statistics.html

IPv6 Adoption

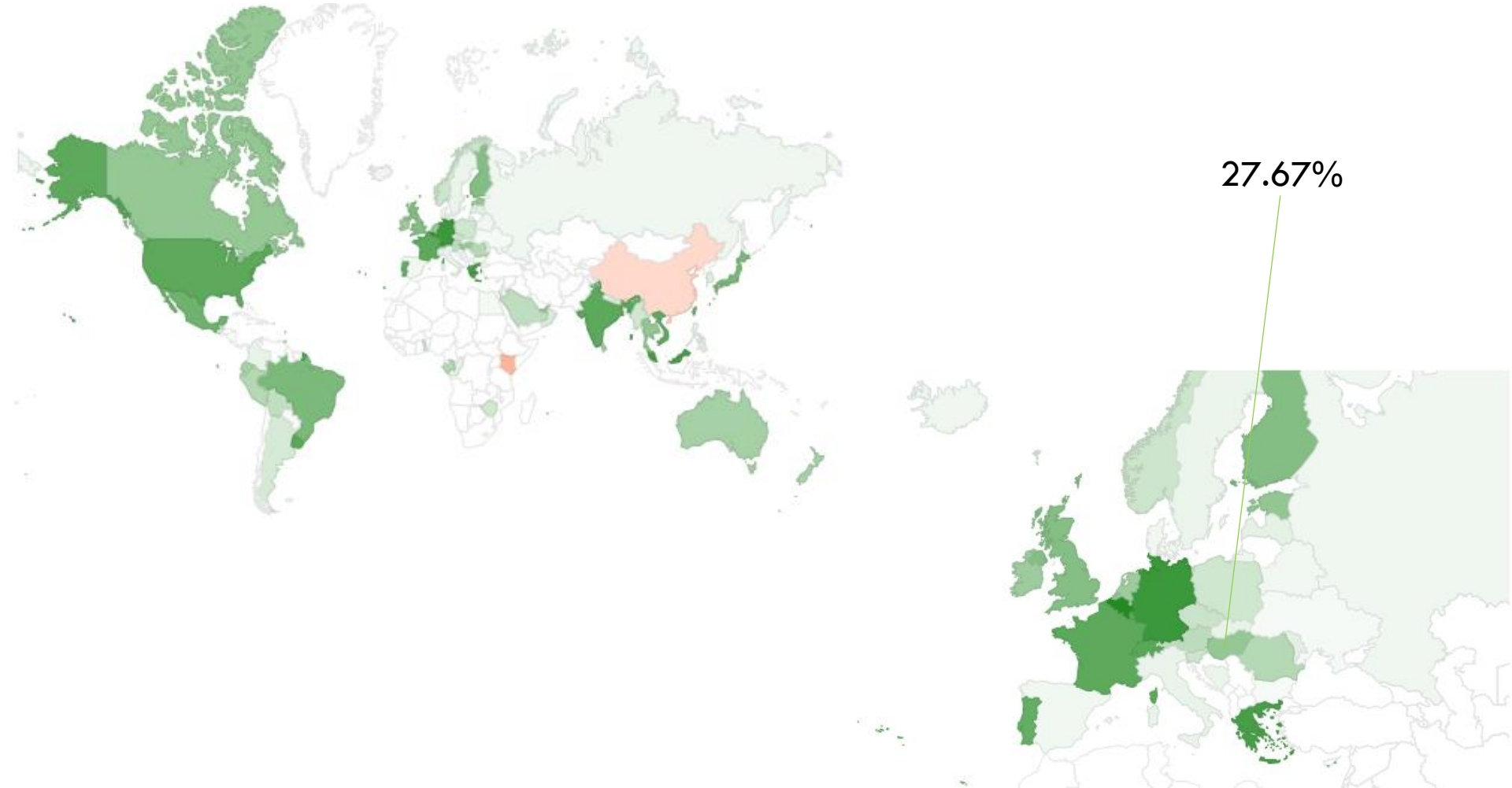
IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



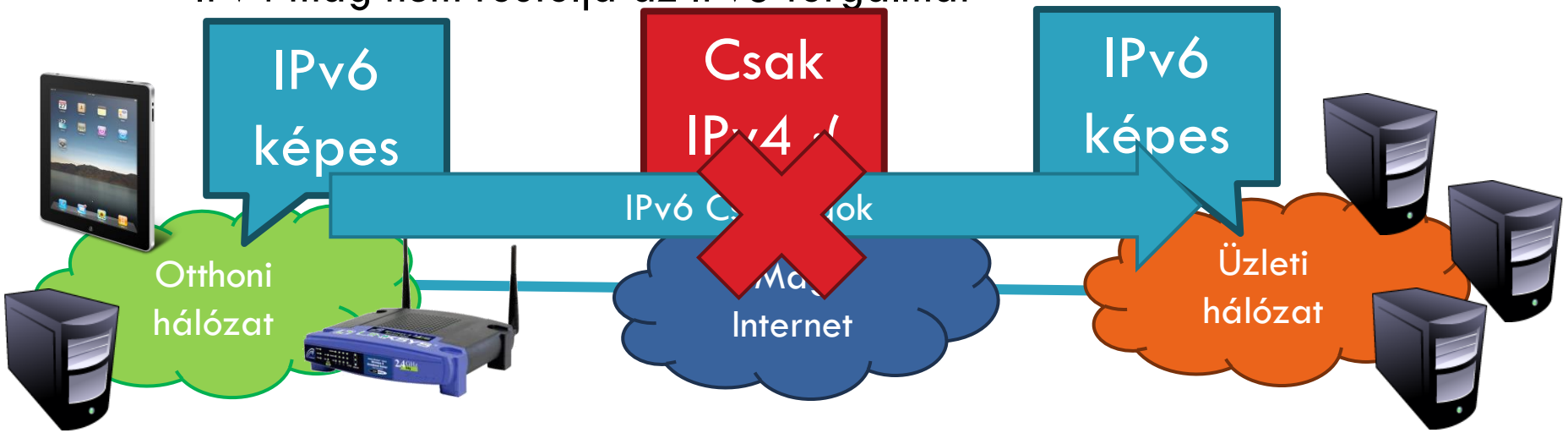
https://www.google.com/intl/en/ipv6/statistics.html

IPv6 Adoption



Átmenet IPv6-ra

- Hogyan történhet az átmenet IPv4-ről IPv6-ra?
  - Napjainkban a legtöbb végpont a hálózat széleken támogatja az IPv6-ot
    - Windows/OSX/iOS/Android mind tartalmaz IPv6 támogatást
    - Az itteni vezetéknélküli access point-ok is valószínűleg IPv6 képesek
  - Az Internet magja a probléma
    - IPv4 mag nem routolja az IPv6 forgalmat



Átmeneti megoldások

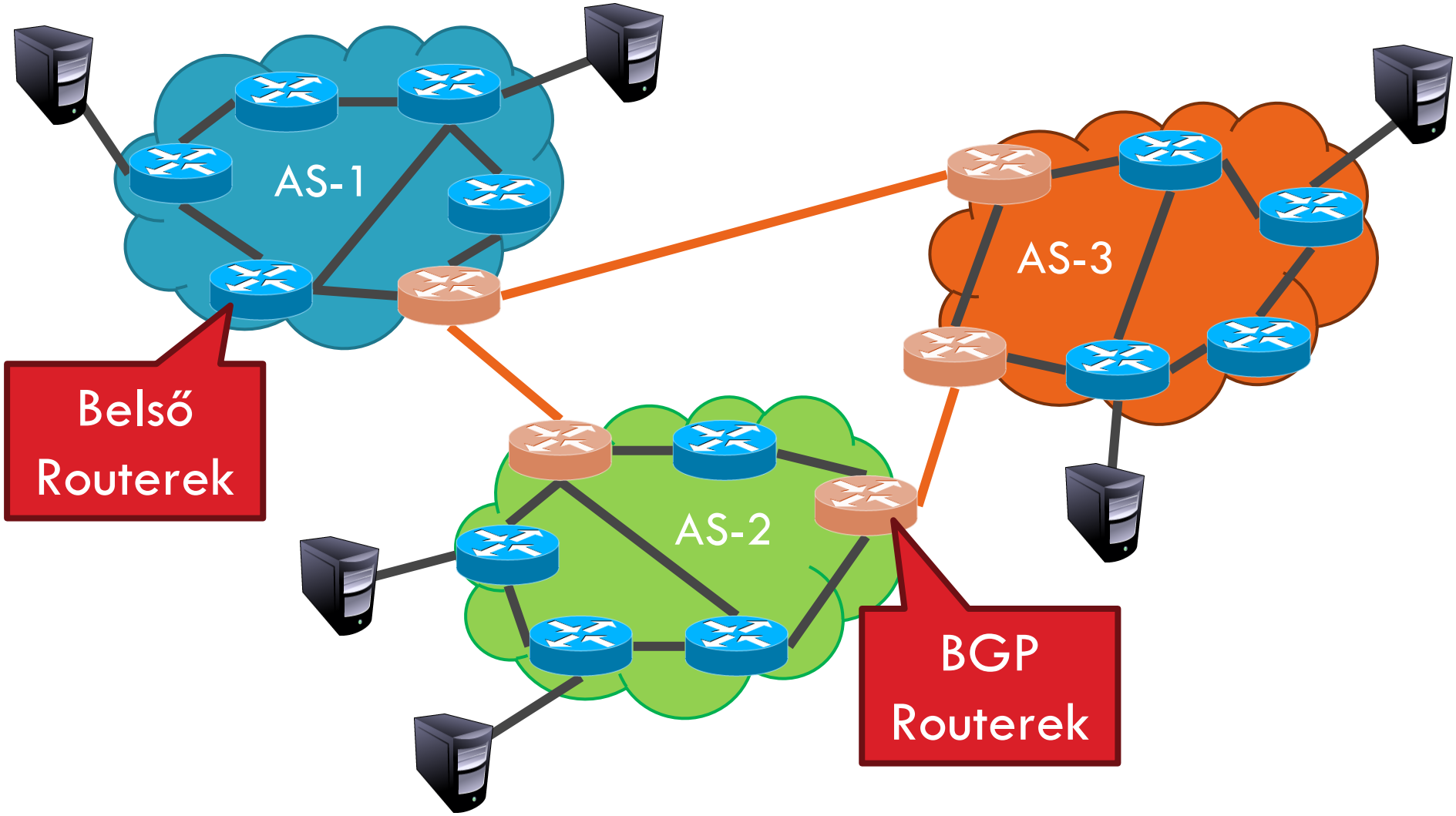
- Azaz hogyan routoljunk IPv6 forgalmaz IPv4 hálózat felett?
- Megoldás
  - Használjunk tunneleket az IPv6 csomagok becsomagolására és IPv4 hálózaton való továbbítására
  - Számos különböző implementáció
    - 6to4
    - IPv6 Rapid Deployment (6rd)
    - Teredo
    - …

Routing 2. felvonás

Újra: Internet forgalom irányítás

- Az Internet egy két szintű hierarchiába van szervezve
- Első szint – autonóm rendszerek (AS-ek)
  - AS – egy adminisztratív tartomány alatti hálózat
  - Pl.: ELTE, Comcast, AT&T, Verizon, Sprint, ...
- AS-en belül ún. intra-domain routing protokollokat használunk
  - Distance Vector, pl.: Routing Information Protocol (RIP)
  - Link State, pl.: Open Shortest Path First (OSPF)
- AS-ek között ún. inter-domain routing protokollokat
  - Border Gateway Routing (BGP)
  - Napjainkban: BGP-4

AS példa



Miért van szükség AS-ekre?

- A routing algoritmusok **nem elég hatékonyak** ahhoz, hogy a teljes Internet topológián működjenek
- Különböző szervezetek **más-más politika** mentén akarnak forgalom irányítást (policy)
- Lehetőség, hogy a szervezetek **elrejtsék a belső hálózatuk szerkezetét**
- Lehetőség, hogy a szervezetek **eldöntsék,** hogy mely más szervezeteken keresztül forgalmazzanak

- Egyszerűbb az útvonalak számítása
- Nagyobb rugalmasság
- Nagyobb autonómia/függetlenség

AS számok

- Minden AS-t egy AS szám (ASN) azonosít
  - 16 bites érték (a legújabb protokollok már 32 bites azonosítókat is támogatnak)
  - 64512 – 65535 más célra foglalt
- Jelenleg kb. 40000 AS szám létezik
  - AT&T: 5074, 6341, 7018, …
  - Sprint: 1239, 1240, 6211, 6242, …
  - ELTE: 2012
  - Google 15169, 36561 (formerly YT), + others
  - Facebook 32934
  - Észak-amerkiai AS-ek → ftp://ftp.arin.net/info/asn.txt

Inter-Domain Routing

- A globális összeköttetéshez szükséges!!!
  - Azaz minden AS-nek **ugyanazt** a protokollt kell használnia
  - Szemben az intra-domain routing-gal
- Milyen követelmények vannak?
  - Skálázódás
  - Rugalmas útvonal választás
    - Költség
    - Forgalom irányítás egy hiba kikerülésére
- Milyen protokollt válasszunk?
  - link state vagy distance vector?
  - Válasz: A BGP egy path vector (útvonal vektor) protokoll

Border Gateway Protocol

ÁLTALÁNOS

AS-ek közötti *(exterior gateway protocol)*.

Eltérő célok vannak forgalomirányítási szempontból, mint az AS-eken belüli protokollnál.

Politikai szempontok szerepet játszathatnak a forgalomirányítási döntésben.

NÉHÁNY PÉLDA FORGALOMIRÁNYÍTÁSI KORLÁTOZÁSRA

- Ne legyen átmenő forgalom bizonyos AS-eken keresztül.
- Csak akkor haladjunk át Albánián, ha nincs más út a célhoz.
- Az IBM-nél kezdődő illetve végződő forgalom ne menjen át a Microsoft-on.

- A politikai jellegű szabályokat kézzel konfigurálják a BGP-routeren.
- A BGP router szempontjából a világ AS-ekből és a közöttük átmenő vonalakból áll.

DEFINÍCIÓ

- Két AS összekötött, ha van köztük a BGP-router-eiket összekötő él.

Border Gateway Protocol

Hálózatok csoportosítása az átmenő forgalom szempontjából

1. **Csonka hálózatok**, amelyeknek csak egyetlen összeköttetésük van a BGP gráffal.
2. **Többszörösen bekötött hálózatok**, amelyeket használhatna az átmenő forgalom, de ezek ezt megtagadják.
3. **Tranzit hálózatok**, amelyek némi megkötéssel, illetve általában fizetség ellenében, készek kezelni harmadik fél csomagjait.

Jellemzők

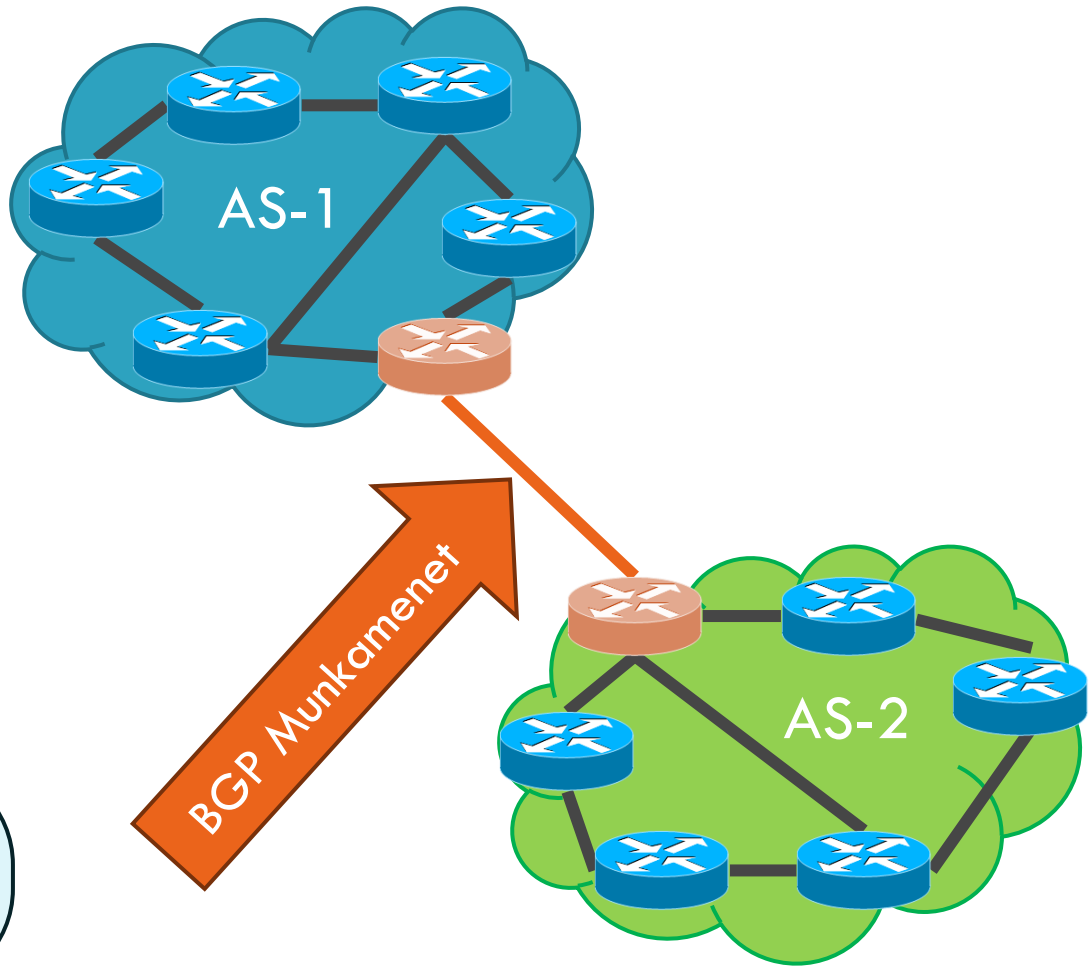
- A BGP router-ek páronként TCP-összeköttetést létrehozva kommunikálnak egymással.
- A BGP alapvetően távolságvektor protokoll, viszont a router nyomon követi a használt útvonalat, és az útvonalat mondja meg a szomszédjainak.

BGP egyszerűsített működése

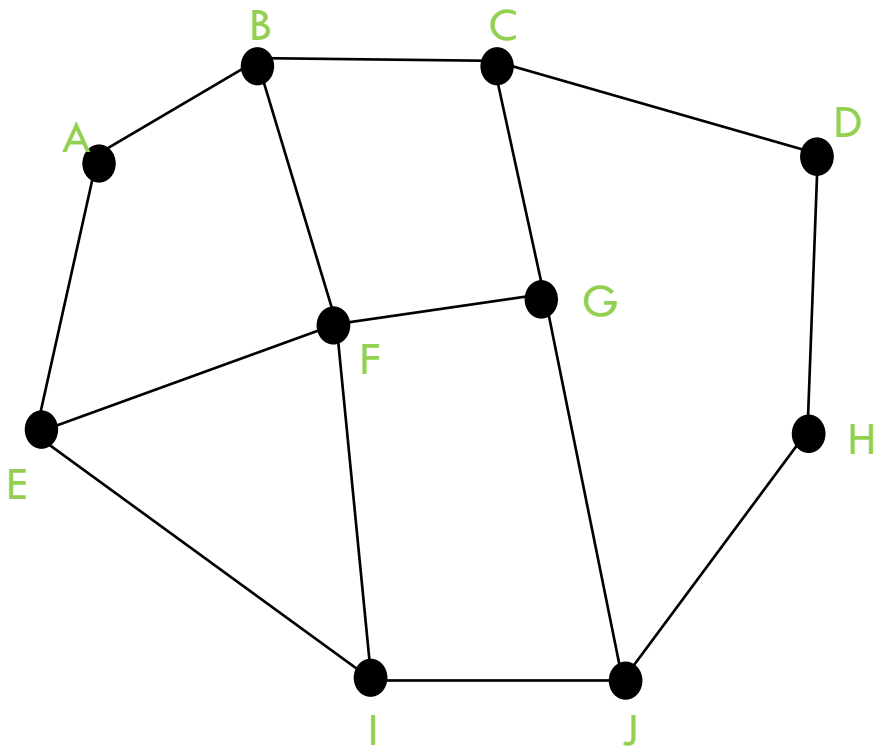
Munkamenet létrehozása a TCP 179-es portján

Aktív útvonalak kicserélése

Folyamatos frissítések cseréje



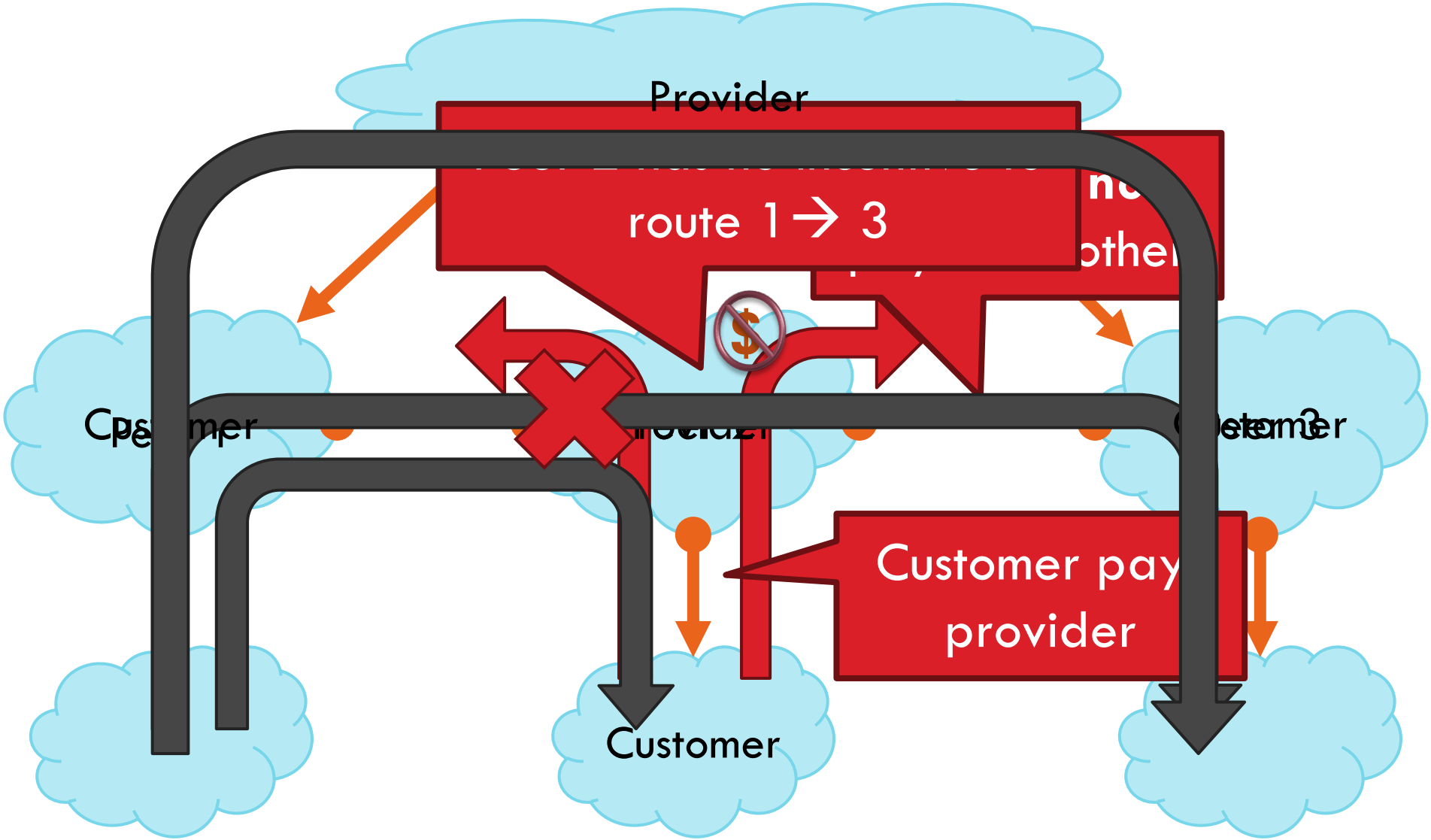
Border Gateway Protocol



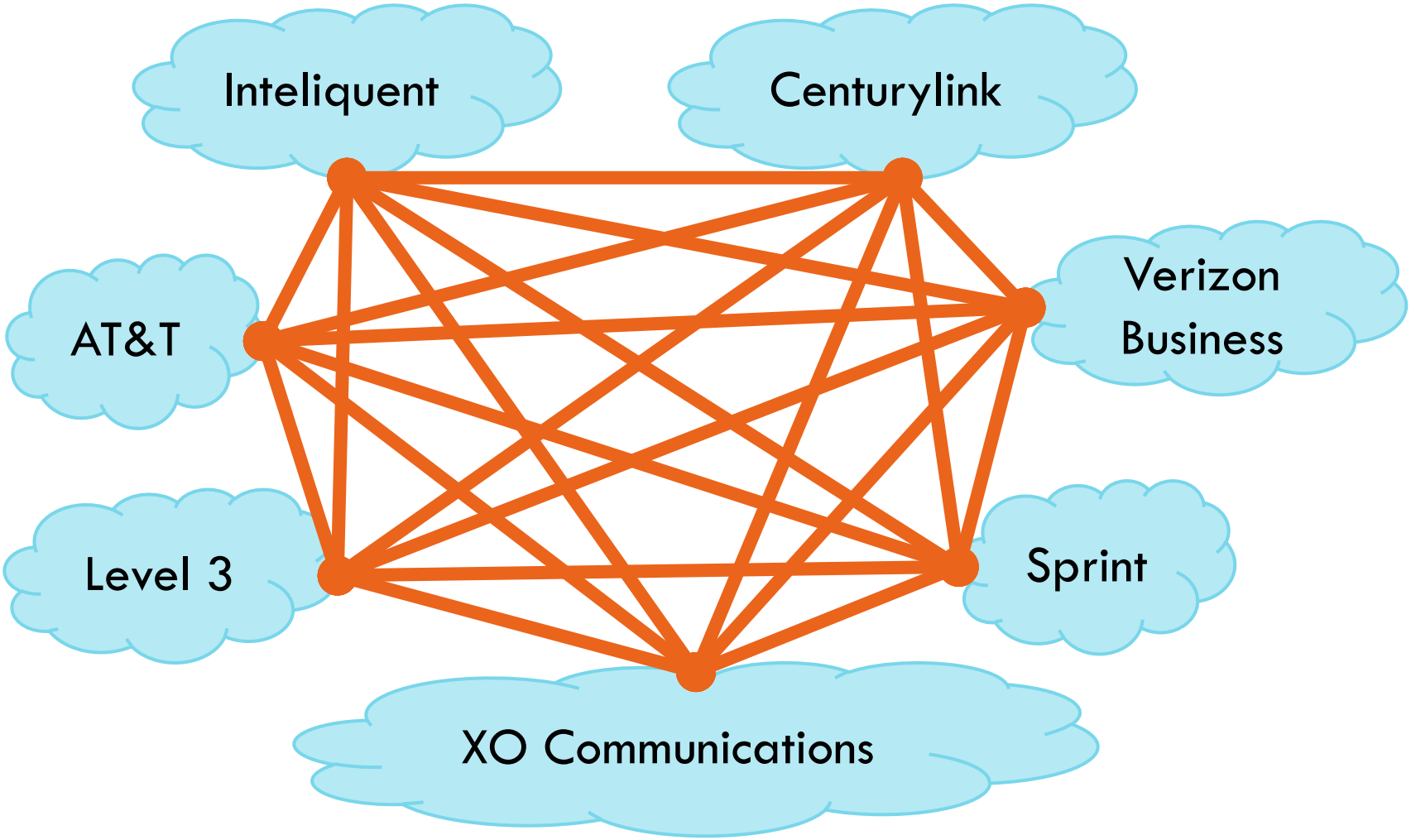
A *F* által a szomszédjaitól kapott *D*-re vonatkozó információ az alábbi:

B-től: „Én a *BCD*-t használom”
G-től: „Én a *GCD*-t használom”
I-től: „Én a *IFGCD*-t használom”
E-től: „Én a *EFGCD*-t használom”

BGP kapcsolatok



Tier-1 ISP Peering



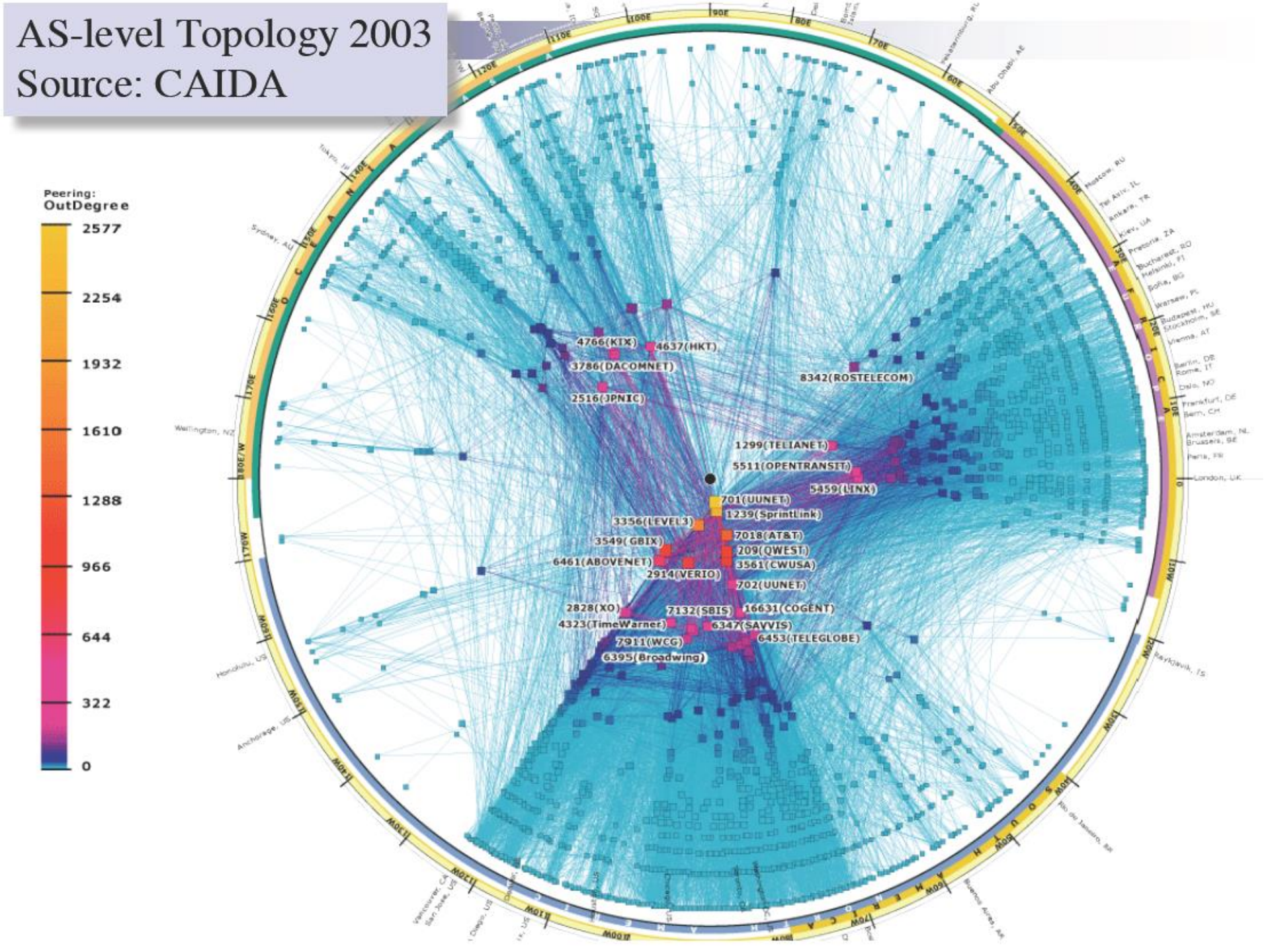
Tier-1 ISP Peering

Azaz egy tier 1 hálózat üzemelteltése nem is olyan egyszerű…

Csak annyi dolgod van, hogy minden tier 1 hálózat üzemeltetőt rávegyél, hogy legyen a peer-ed!

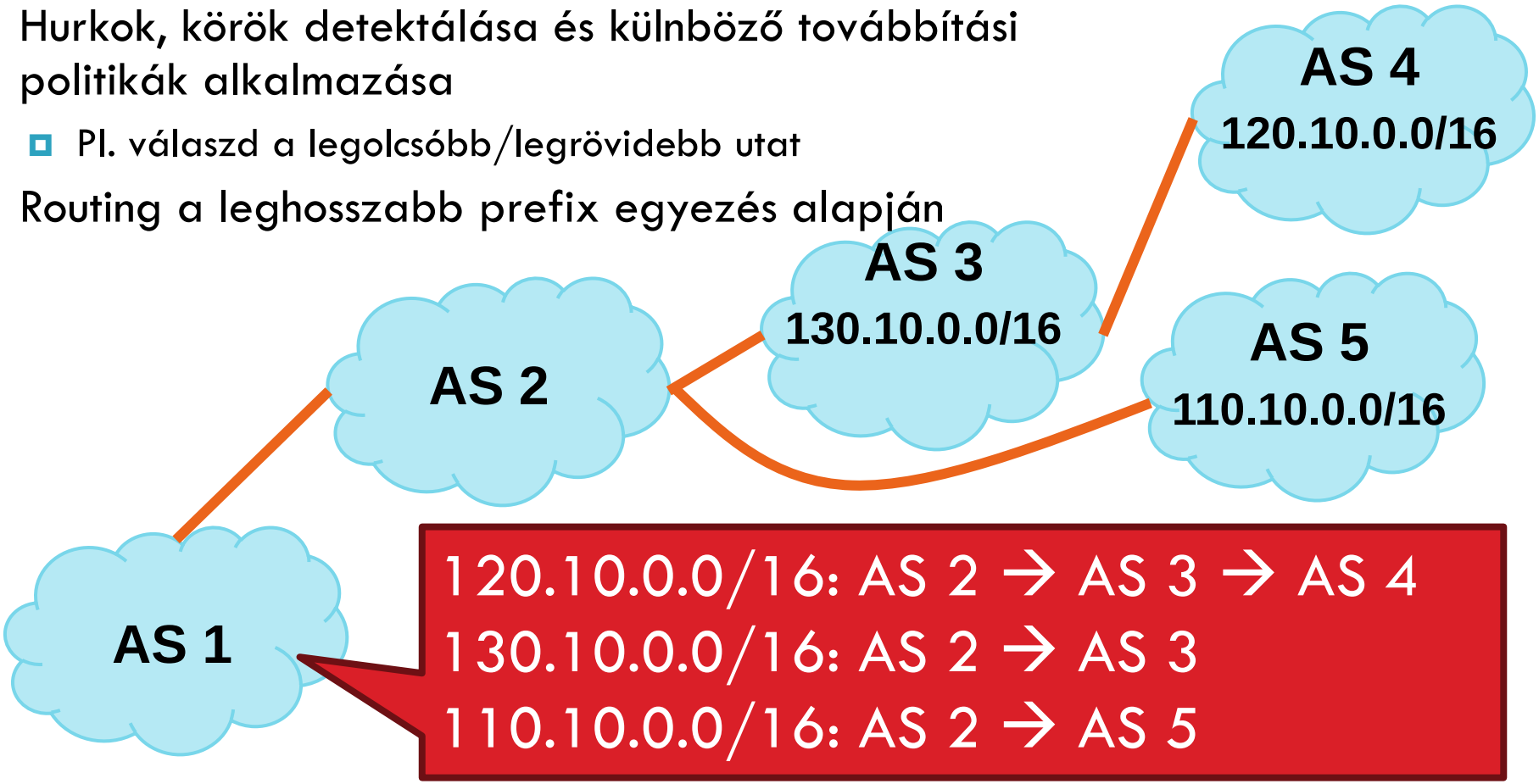
(nem túl könnyű ☺)

AS-level Topology 2003
Source: CAIDA



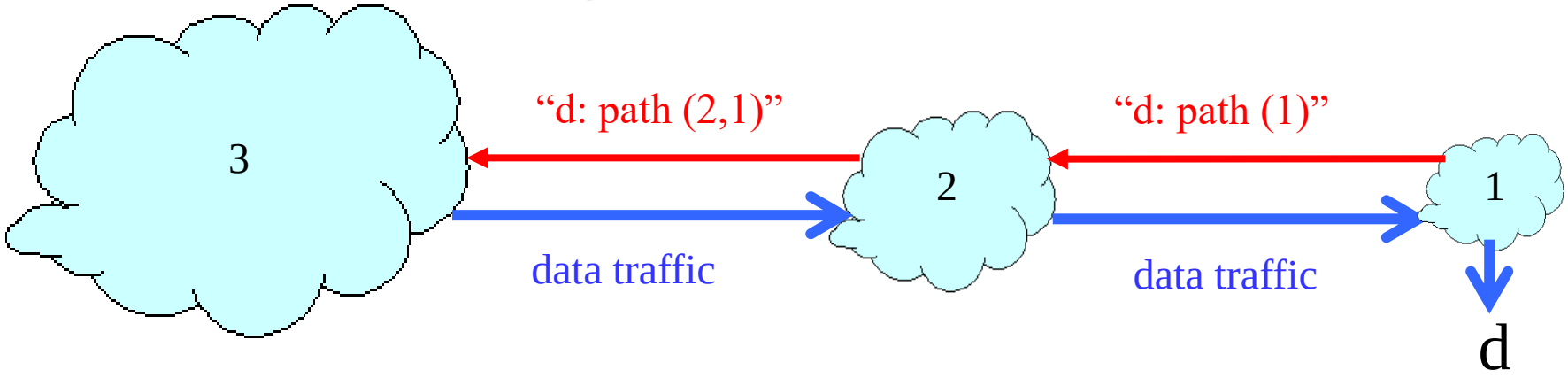
Útvonalvektor protokoll
Path Vector Protocol

- AS-útvonal: AS-ek sorozata melyeken áthalad az útvonal
  - Hasonló a távolságvektorhoz, de további információt is tartalmaz
- Hurkok, körök detektálása és különböző továbbítási politikák alkalmazása
  - Pl. válaszd a legolcsóbb/legrövidebb utat
- Routing a leghosszabb prefix egyezés alapján



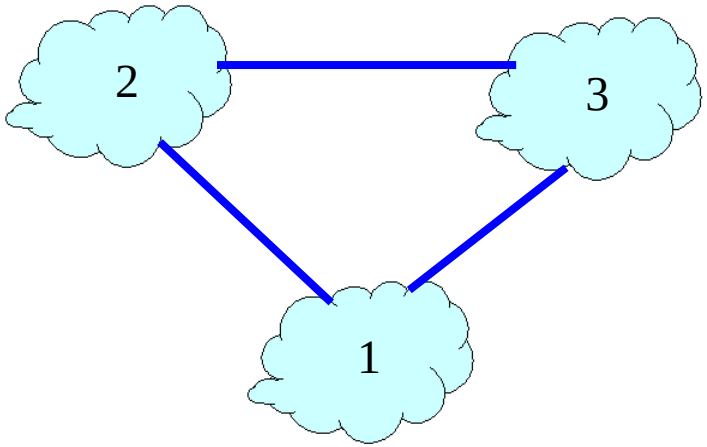
Útvonalvektor protokoll
Path Vector Protocol

- A távolságvektor protokoll kiterjesztése
  - Rugalmas továbbítási politikák
  - Megoldja a végtelenig számolás problémáját
  - Útvonalvektor: Célállomás, következő ugrás (nh), AS útvonal
- Ötlet: a teljes útvonalat meghirdeti
  - Távolságvektor: távolság metrika küldése célállomásonként
  - Útvonalvektor: a teljes útvonal küldése célállomásonként

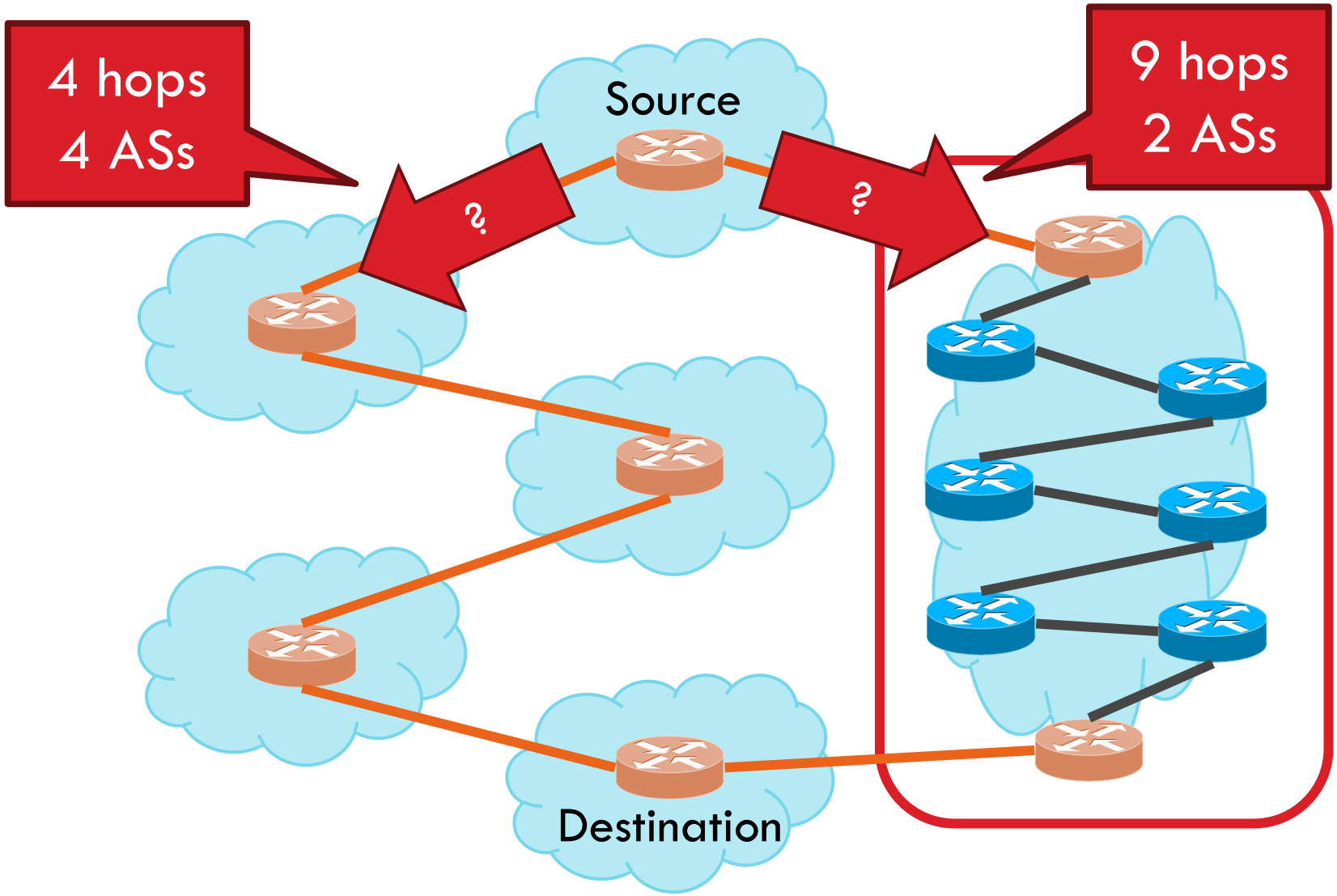


Rugalmas forgalomirányítás

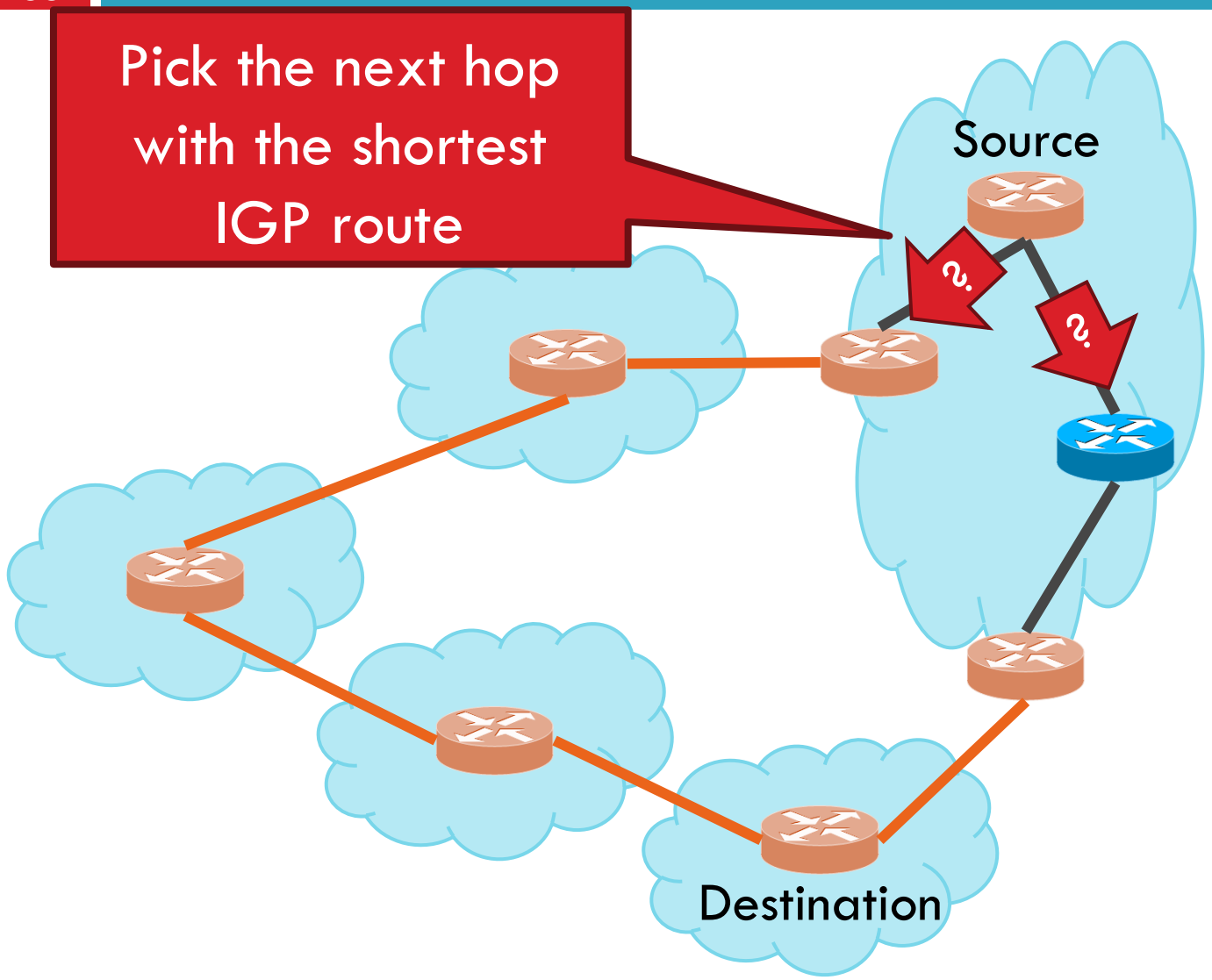
- Minden állomás hely/saját útválasztási politikát alkalmaz
  - Útvonal kiválasztás: Melyik útvonalat használjuk?
  - Útvonal export: Melyik útvonalat hirdessük meg?
- Példák
  - A 2. állomás által preferált útvonal: “2, 3, 1” (nem a “2, 1”)
  - Az 1. állomás nem hagyja, hogy a 3. állomás értesüljön az “1, 2” útvonalról



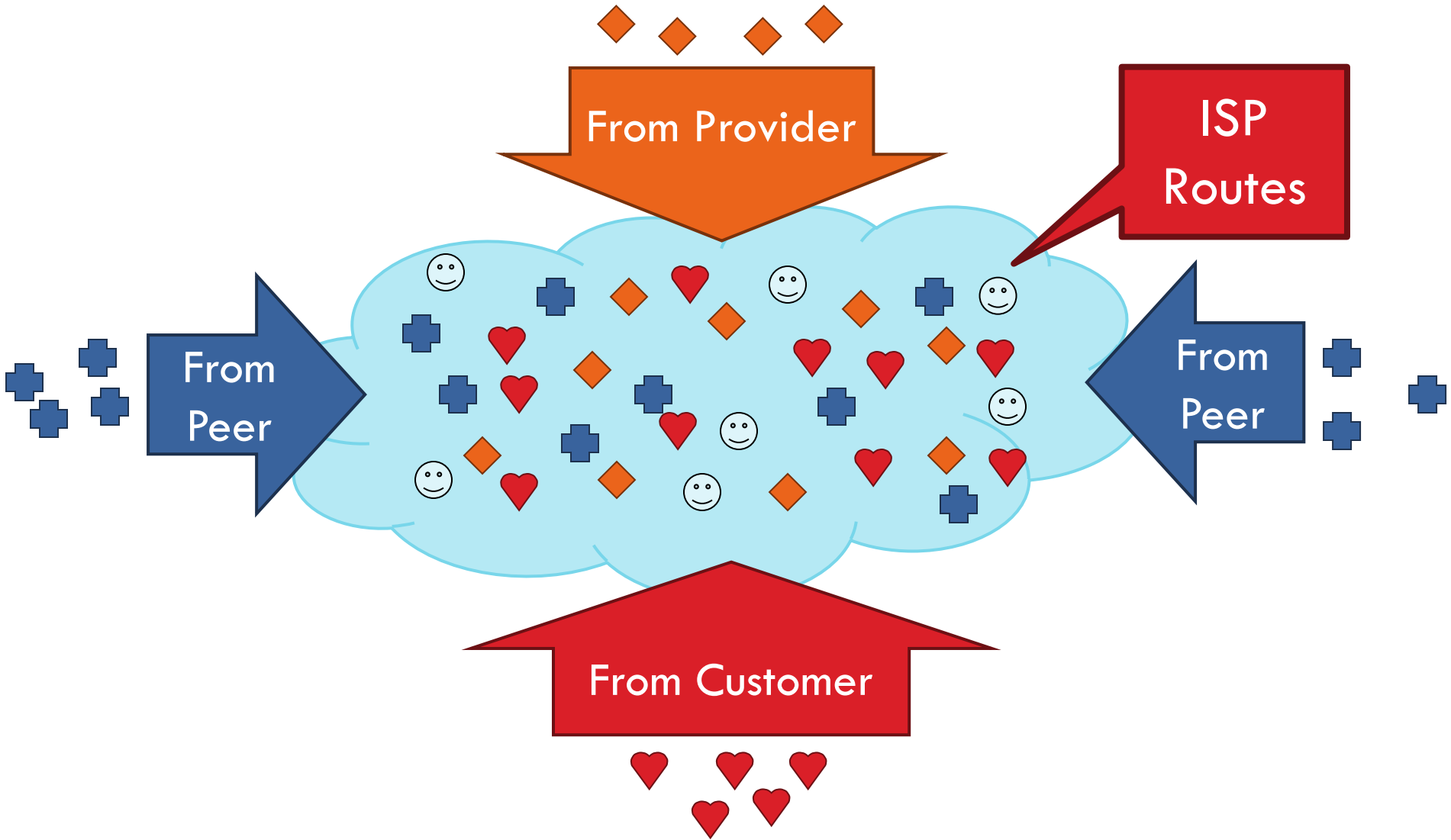
Shortest AS Path != Shortest Path



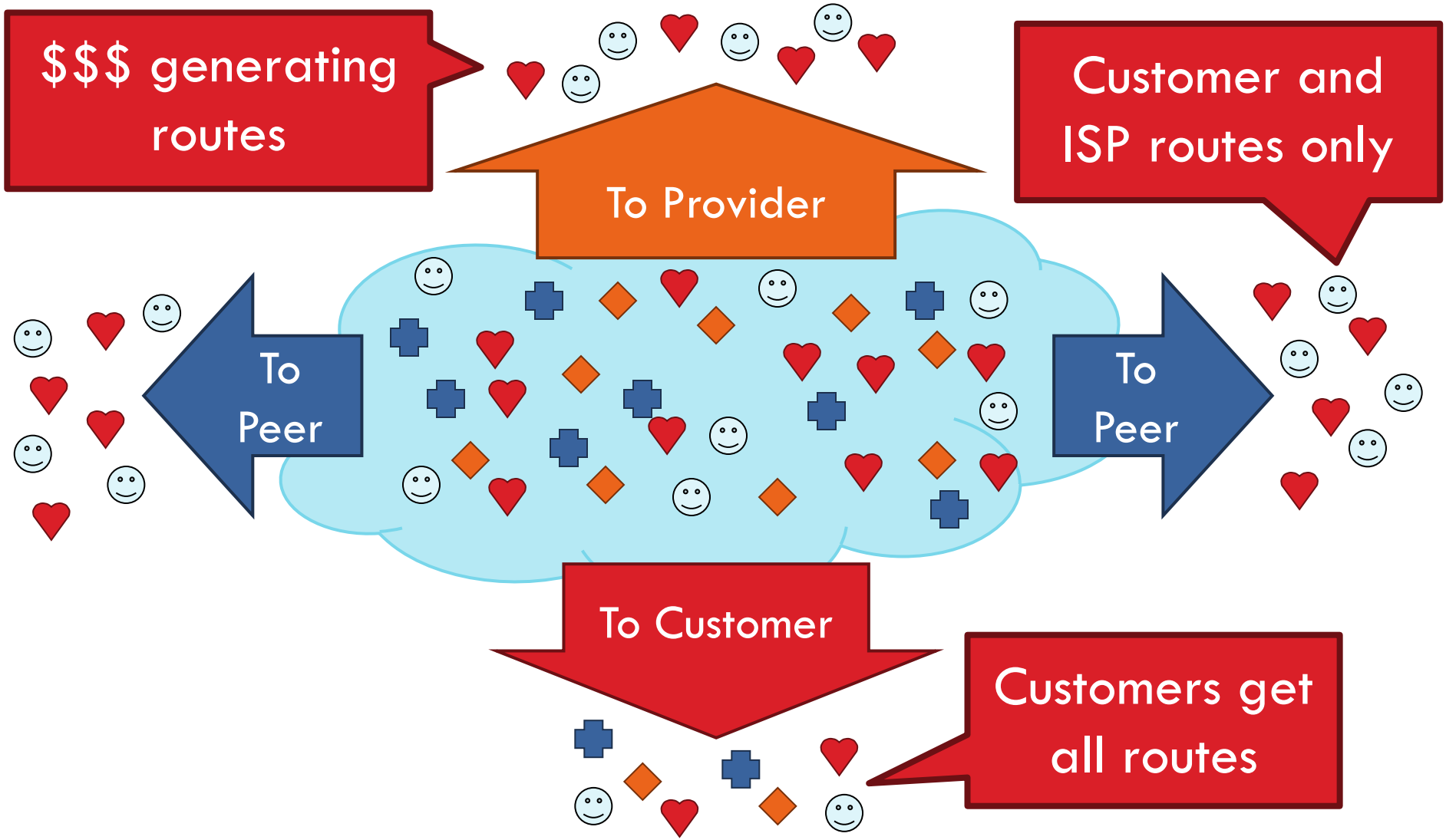
Hot Potato Routing



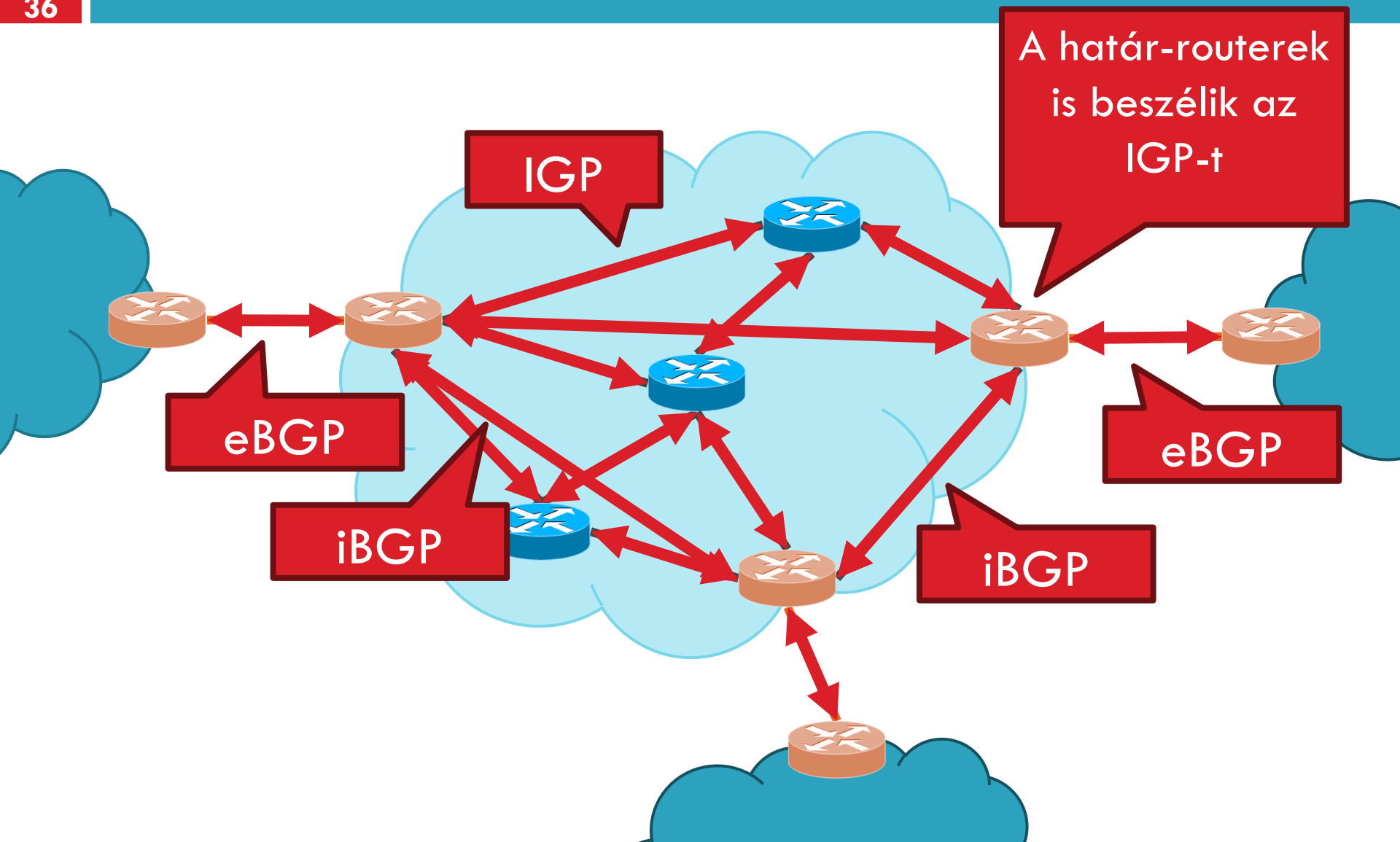
Importing Routes



Exporting Routes



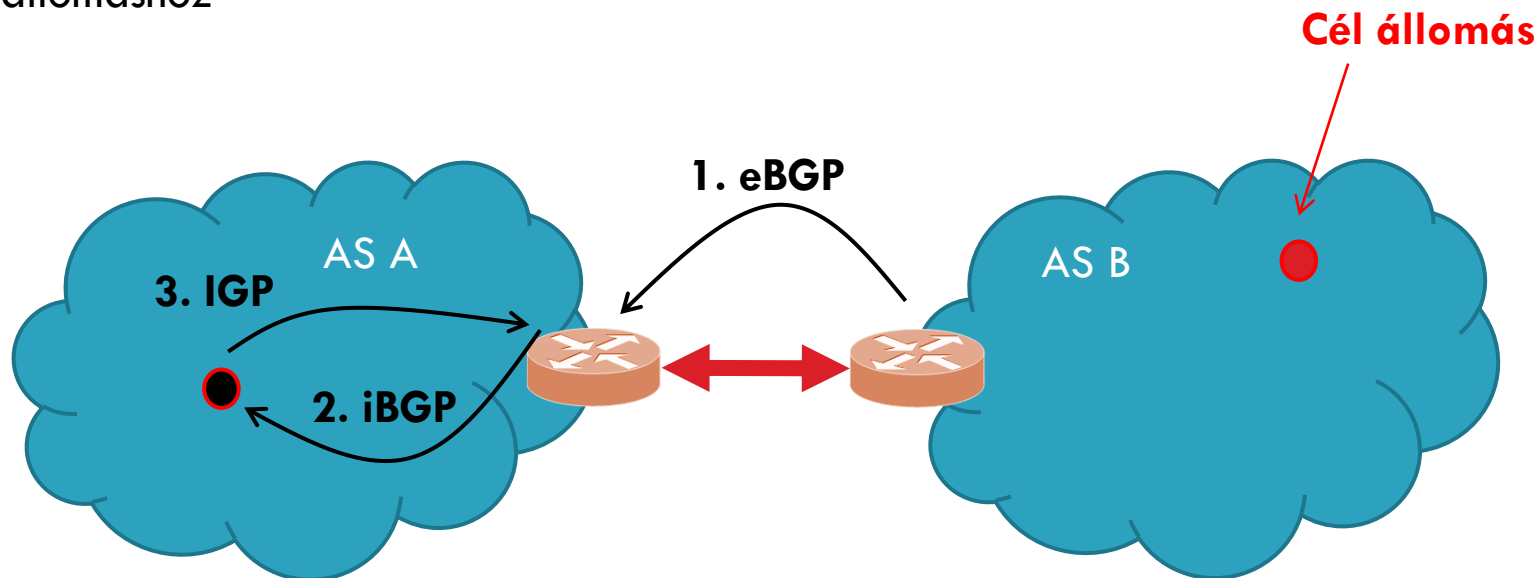
BGP



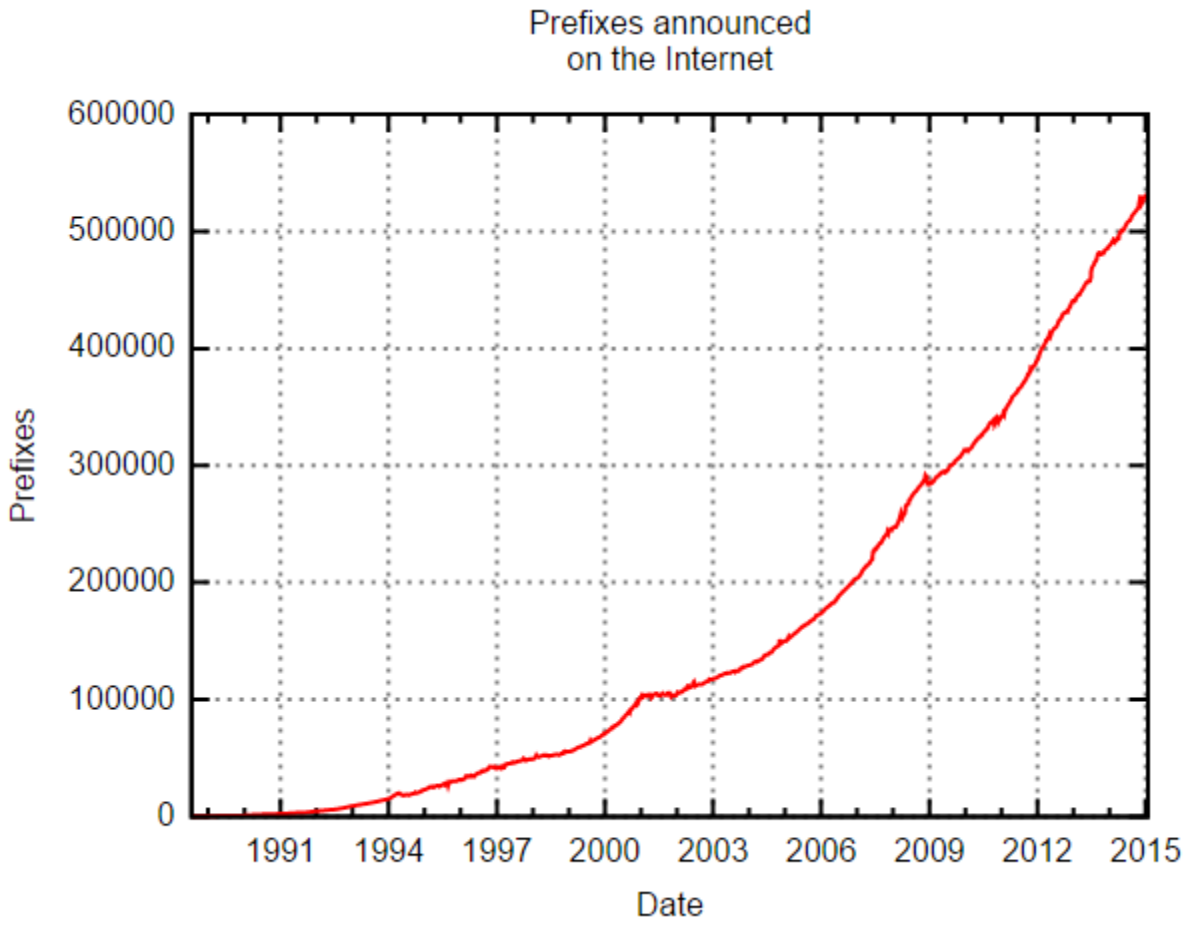
IGB – iBGP – eBGP

- eBGP: Routing információk cseréje autonóm rendszerek között
- IGP: útválasztás egy AS-en belül belső célállomáshoz
- iBGP: útválasztás egy AS-en belül egy külső célállomáshoz

- 1. eBGP – A megismeri az útvonal a célhoz, ehhez eBGP-t használunk
- 2. iBGP – A-ban levő router megtanulja a célhoz vezető utat az iBGP segítségével (a köv. ugrás a határ router)
- 3. IGP – IGP segítségével eljuttatja a csomagot az A határrouteréig



Forrás: wikipedia



További protokollok

Internet Control Message Protocol

FELADATA

- Váratlan események jelentése

HASZNÁLAT

- Többféle *ICMP*-üzenetet definiáltak:
  - Elérhetetlen cél;
  - Időtúllépés;
  - Paraméter probléma;
  - Forráslefojtás;
  - Visszhang kérés;
  - Visszhang válasz;
  - ...

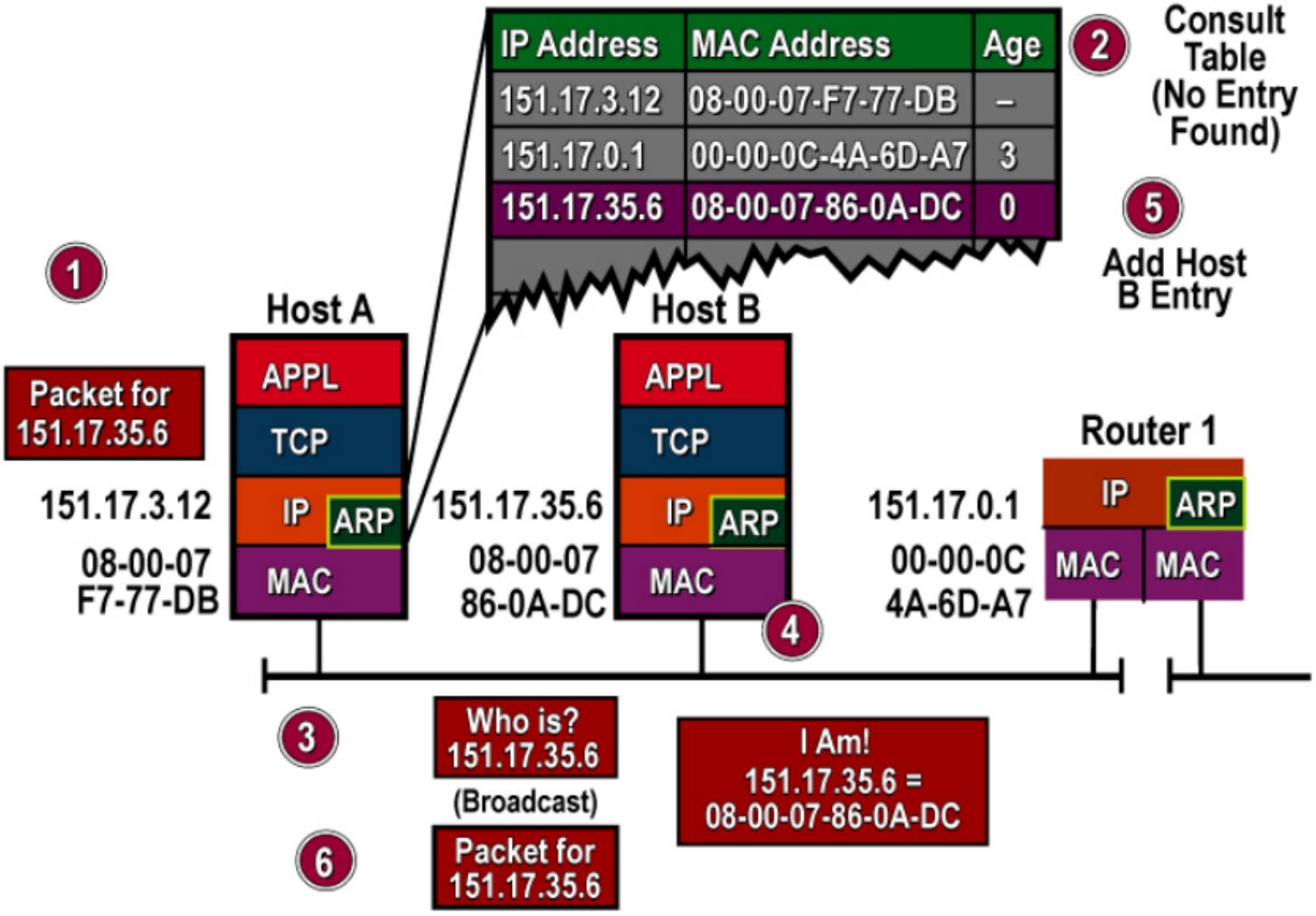
Internet Control Message Protocol

- *Elérhetetlen cél* esetén a csomag kézbesítése sikertelen volt.
  - **Esemény lehetséges oka:** Egy nem darabolható csomag továbbításának útvonalán egy „kis csomagos hálózat” van.
- *Időtúllépés* esetén az IP csomag élettartam mezője elérte a 0-át.
  - **Esemény lehetséges oka:** Torlódás miatt hurok alakult ki vagy a számláló értéke túl alacsony volt.
- *Paraméter probléma* esetén a fejrészben érvénytelen mezőt észleltünk.
  - **Esemény lehetséges oka:** Egy az útvonalon szereplő router vagy a hoszt IP szoftverének hibáját jelezheti.

Internet Control Message Protocol

- Forráslefojtás esetén lefojtó csomagot küldünk.
  - **Esemény hatása:** A fogadó állomásnak a forgalmazását lassítania kellett.
- Visszhang kérés esetén egy hálózati állomás jelenlétét lehet ellenőrizni.
  - **Esemény hatása:** A fogadónak vissza kell küldeni egy visszhang választ.
- Átirányítás esetén a csomag rosszul irányítottságát jelzik.
  - **Esemény kiváltó oka:** Router észleli, hogy a csomag nem az optimális útvonall.

Address Resolution Protocol



Address Resolution Protocol

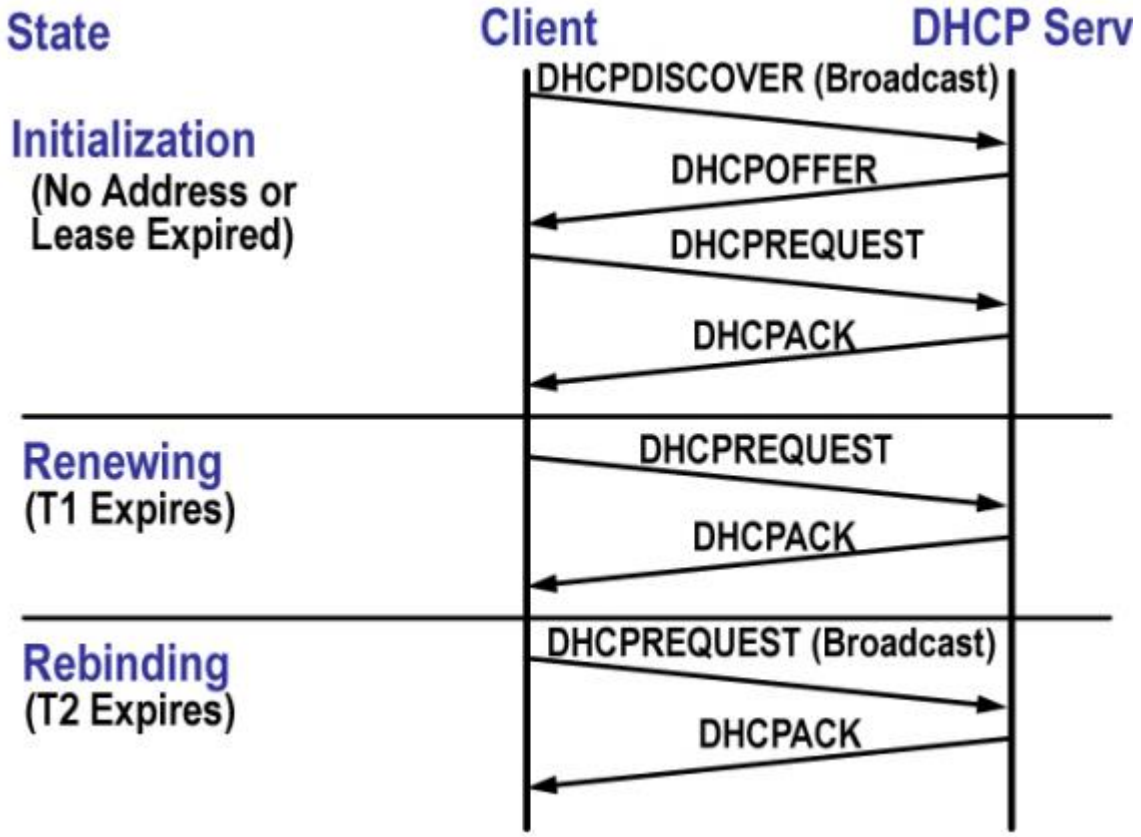
FELADATA

- Az IP cím megfeleltetése egy fizikai címnek.

HOZZÁRENDELÉS

- Adatszóró csomag kiküldése az *Ethernet*re „Ki-é a 192.60.34.12-es IP-cím?” kérdéssel az alhálózaton, és mindenegyes hoszt ellenőrzi, hogy övé-e a kérdéses IP-cím. Ha egyezik az IP a hoszt saját IP-jével, akkor a saját *Ethernet* címével válaszol. Erre szolgál az ARP.
- Opcionális javítási lehetőségek:
  - a fizikai cím IP hozzárendelések tárolása (*cache használata*);
  - Leképezések megváltoztathatósága (*időhatály bevezetése*);
- Mi történik távoli hálózaton lévő hoszt esetén?
  - A router is válaszoljon az ARP-re a hoszt alhálózatán. (*proxy ARP*)
  - Alapértelmezett Ethernet-cím használata az összes távoli forgalomhoz

DHCP: DYNAMIC HOST CONFIGURATION PROTOCOL



DHCP

- Lényegében ez már az **Alkalmazási réteg**
  - de logikailag ide tartozik

- Segítségével a hosztok automatikusan juthatnak hozzá a kommunikációjukhoz szükséges hálózati azonosítókhoz:
  - IP cím, hálózati maszk, alapértelmezett átjáró, stb.

- Eredetileg az RFC 1531 a BOOTP kiterjesztéseként definiálta. Újabb RFC-k: 1541, 2131 (aktuális)

DHCP lehetőségei

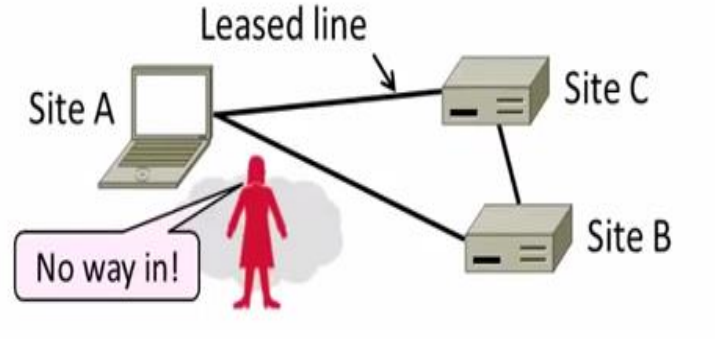
- IP címek osztása MAC cím alapján DHCP szerverrel
  - Szükség esetén (a DHCP szerveren előre beállított módon) egyes kliensek számára azok MAC céméhez fix IP cím rendelhető
- IP címek osztása dinamikusan
  - A DHCP szerveren beállított tartományból „érkezési sorrendben” kapják a kliensek az IP címeket
  - Elegendő annyi IP cím, ahány gép egyidejűleg működik
- Az IP címeken kívül további szükséges hálózati paraméterek is kioszthatók
  - Hálózati maszk
  - Alapértelmezett átjáró
  - Névkiszolgáló
  - Domain név
  - Hálózati rendszerbetöltéshez szerver és fájlnév

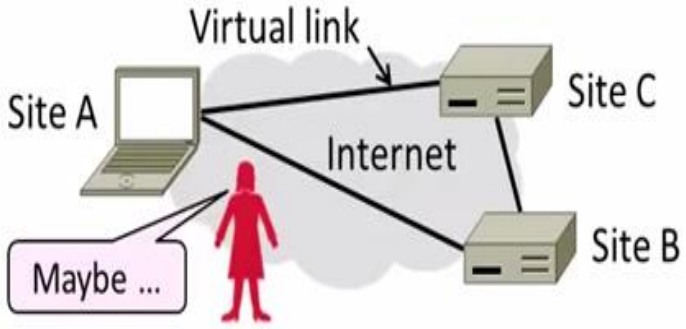
DHCP – Címek bérlése

- A DHCP szerver a klienseknek az IP-címeket bizonyos bérleti időtartamra (lease time) adja „bérbe”
  - Az időtartam hosszánál a szerver figyelembe veszi a kliens esetleges ilyen irányú kérését
  - Az időtartam hosszát a szerver beállításai korlátozzák
- A bérleti időtartam lejárta előtt a bérlet meghosszabbítható
- Az IP-cím explicit módon vissza is adható

Virtuális magánhálózatok alapok

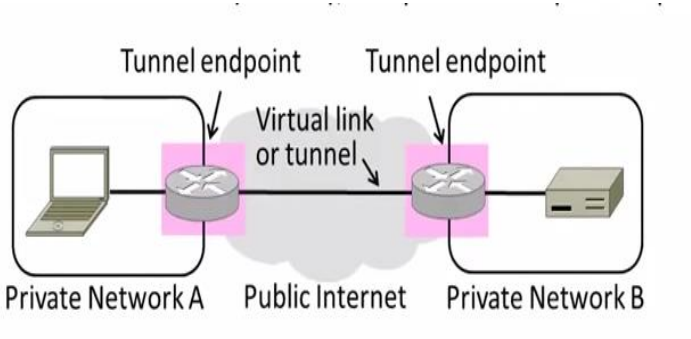
- **Fő jellemzői**
  - Mint közeli hálózat fut az interneten keresztül.
  - IPSEC-et használ az üzenetek titkosítására.
- Azaz informálisan megfogalmazva fizikailag távol lévő hosztok egy közös logikai egységet alkotnak.
  - Például távollévő telephelyek rendszerei.
- **Alapelv**
  - Bérelt vonalak helyett használjuk a publikusan hozzáférhető Internet-et.
  - Így az Internettől **logikailag** elkülöníthető hálózatot kapunk. Ezek a virtuális magánhálózatok avagy VPN-ek.
  - A célok közé kell felvenni a külső támadó kizárását.

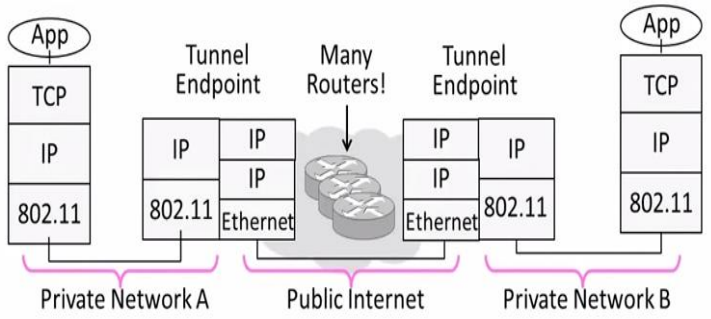




Virtuális magánhálózatok alapok

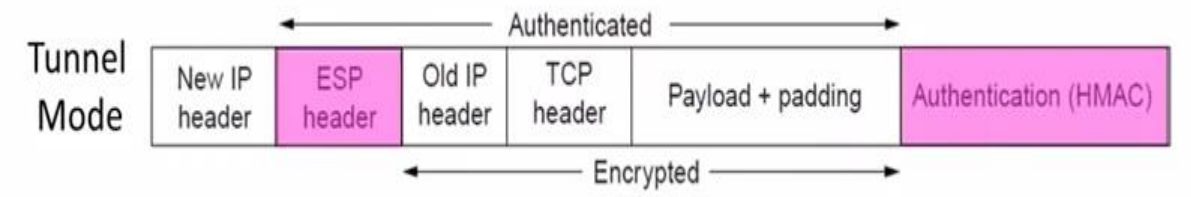
- A virtuális linkeket alagutak képzésével valósítjuk meg.
- **ALAGÚTAK**
  - Egy magánhálózaton belül a hosztok egymásnak normál módon küldhetnek üzenetet.
  - Virtuális linken a végpontok beágyazzák a csomagokat.
    - IP az IP-be mechanizmus.
- Az alagutak képzése önmagában kevés a védelemhez. Mik a hiányosságok?
  - Bizalmasság, authentikáció
  - Egy támadó olvashat, küldhet üzeneteket.
  - *Válasz:* Kriptográfia használata.





Virtuális magánhálózatok alapok

- **IPSEC**
  - Hosszú távú célja az IP réteg biztonságossá tétele. (bizalmasság, autentikáció)
  - <u>Műveletei:</u>
    - Hoszt párok kommunikációjához kulcsokat állít be.
    - A kommunikáció kapcsolatorientáltabbá tétele.
    - Fejlécek és láblécek hozzáadása az IP csomagok védelme érdekében.
  - Több módot is támogat, amelyek közül az egyik az **alagút mód**.



Szállítói réteg

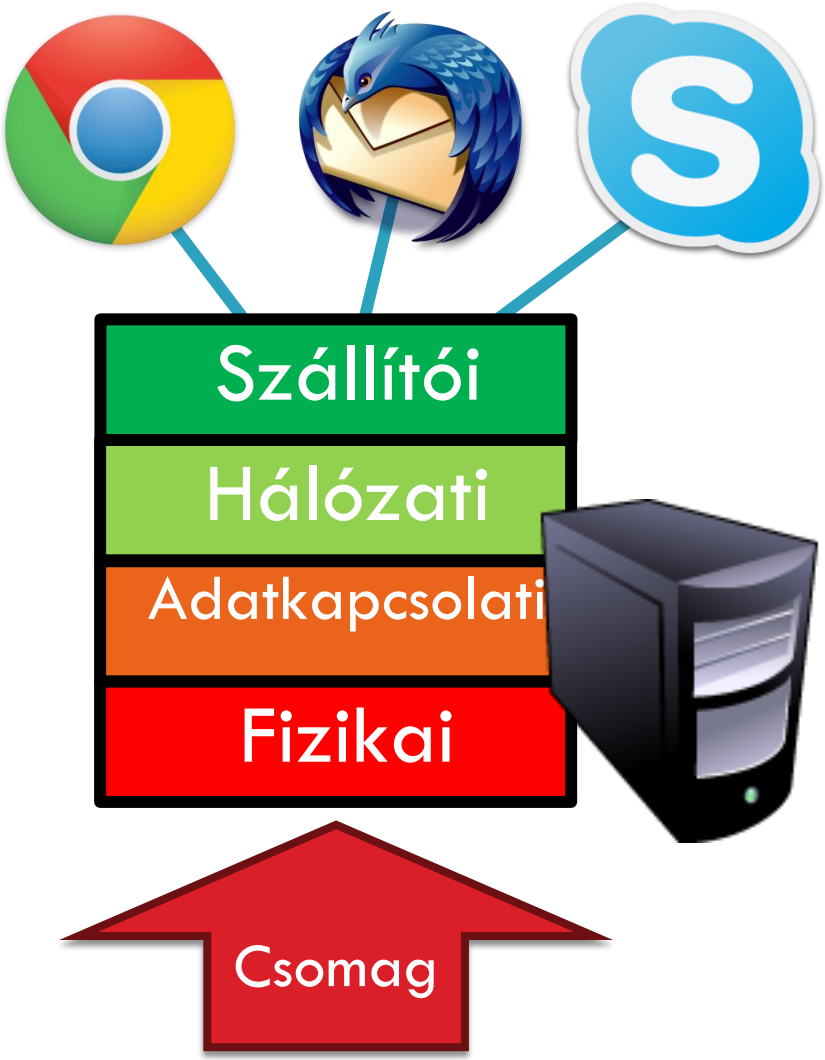
- Feladat:
  - Adatfolyamok demultiplexálása
- További lehetséges feladatok:
  - Hosszú élettartamú kapcsolatok
  - Megbízható, sorrendhelyes csomag leszállítás
  - Hiba detektálás
  - Folyam és torlódás vezérlés
- Kihívások:
  - Torlódások detektálása és kezelése
  - Fairség és csatorna kihasználás közötti egyensúly

Kivonat

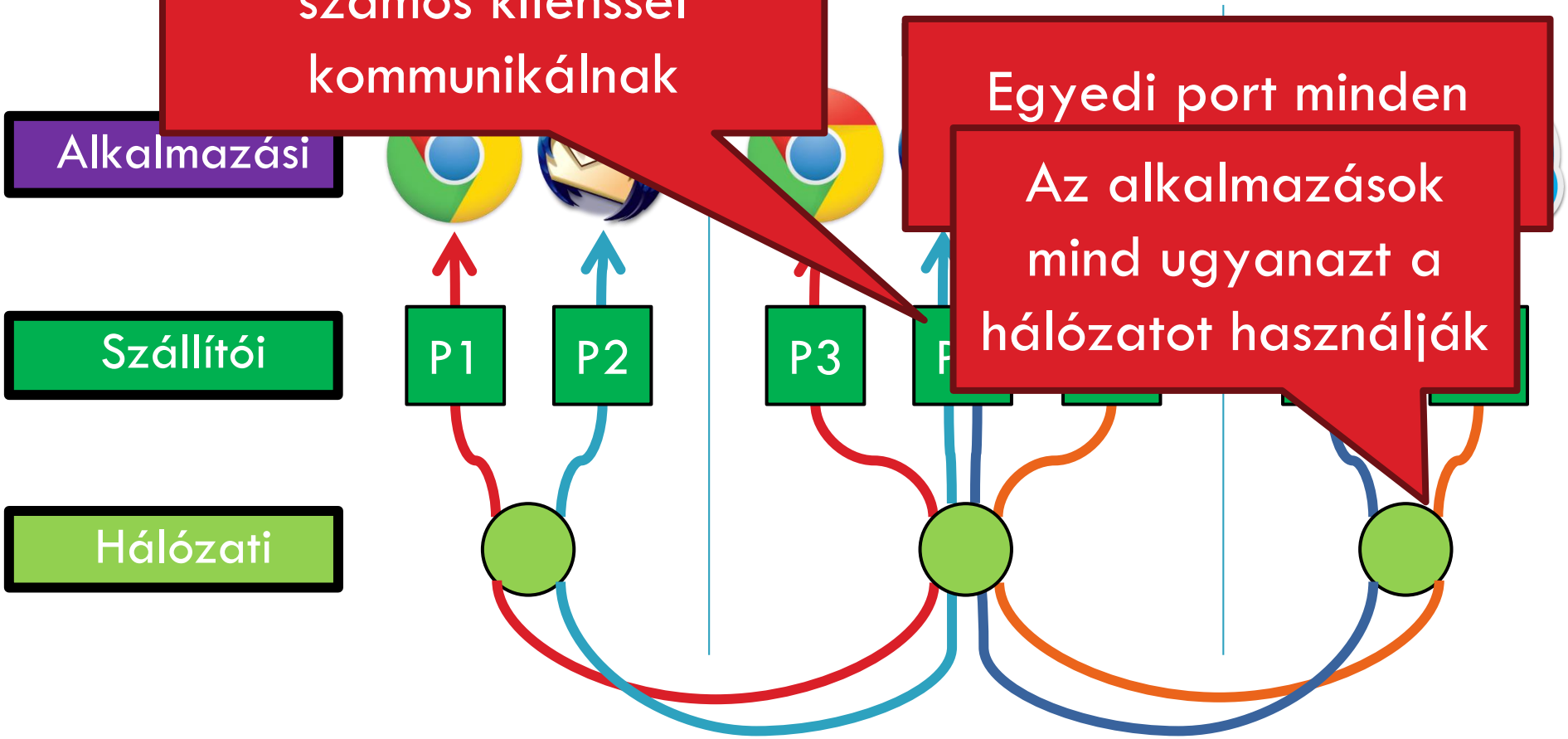
- UDP
- TCP
- Torlódás vezérlés
- TCP evolúciója
- A TCP problémái

Multiplexálás

- Datagram hálózat
  - Nincs áramkör kapcsolás
  - Nincs kapcsolat
- A kliensek számos alkalmazást futtathatnak egyidőben
  - Kinek szállítsuk le a csomagot?
- IP fejléc “protokoll” mezője
  - 8 bit = 256 konkurens folyam
  - Ez nem elég…
- Demultiplexálás megoldása a szállítói réteg feladata



Forgalom demultiplexálása



Végpontok azonosítása: <*src_ip, src_port, dest_ip, dest_port, proto*>

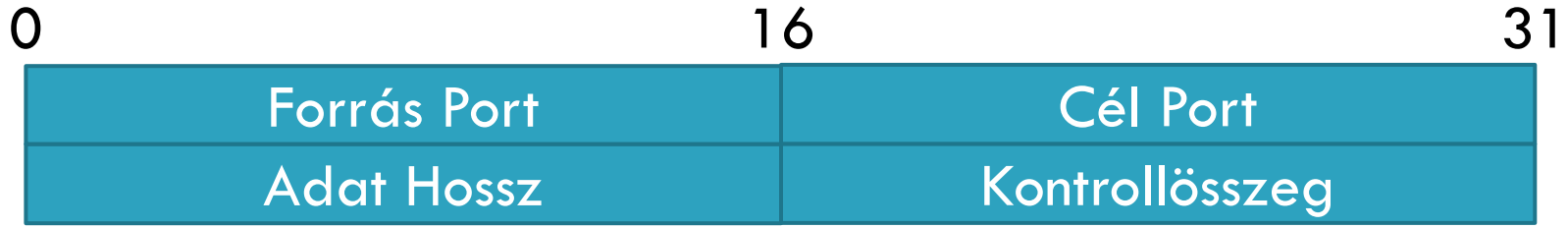
ahol src_ip, dst_ip a forrás és cél IP cím,

src_port, dest_port forrás és cél port, proto pedig UDP vagy TCP.

Réteg modellek

- A legalacsonyabb szintű végpont-végpont protokoll
  - A szállítói réteg fejlécei csak a forrás és cél végpontok olvassák
  - A routerek számára a szállítói réteg fejléce csak szállítandó adat (payload)

User Datagram Protocol (UDP)



- 8 bájtos UDP fejléc
- Egyszerű, kapcsolatnélküli átvitel
  - C socketek: SOCK_DGRAM
- Port számok teszik lehetővé a demultiplexálást
  - 16 bit = 65535 lehetséges port
  - 0 port nem engedélyezett
- Kontrollösszeg hiba detektáláshoz
  - Hibás csomagok felismerése
  - Nem detektálja az elveszett, duplikátum és helytelen sorrendben beérkező csomagokat (UDP esetén nincs ezekre garancia)

UDP felhasználások

- A TCP után vezették be
  - Miért?
- Nem minden alkalmazásnak megfelelő a TCP
- UDP felett egyedi protokollok valósíthatók meg
  - Megbízhatóság? Helyes sorrend?
  - Folyam vezérlés? Torlódás vezérlés?
- Példák
  - RTMP, real-time média streamelés (pl. hang, video)
  - Facebook datacenter protocol

Köszönöm a figyelmet!