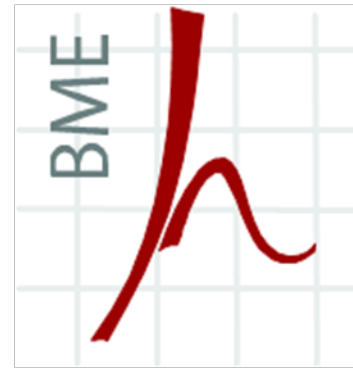




IP – Internet Protocol

IP címzés, routing, IPv6

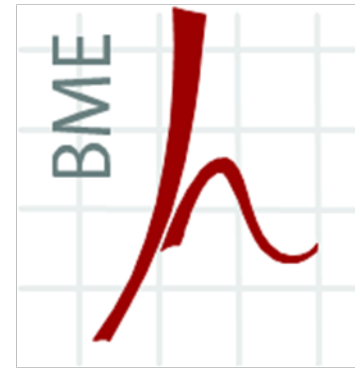
Dr. Simon Vilmos
docens

BME Hálózati Rendszerek és Szolgáltatások Tanszék

svilmos@hit.bme.hu

2017.október 11.

- Bevezetés
 - Az IP feladata és jellemzői
- Címzés
- Az IP csomag szerkezete
- Routing
- IP segédprotokollok
- IPv6



IP – Bevezetés

Az IP, mint hálózati protokoll

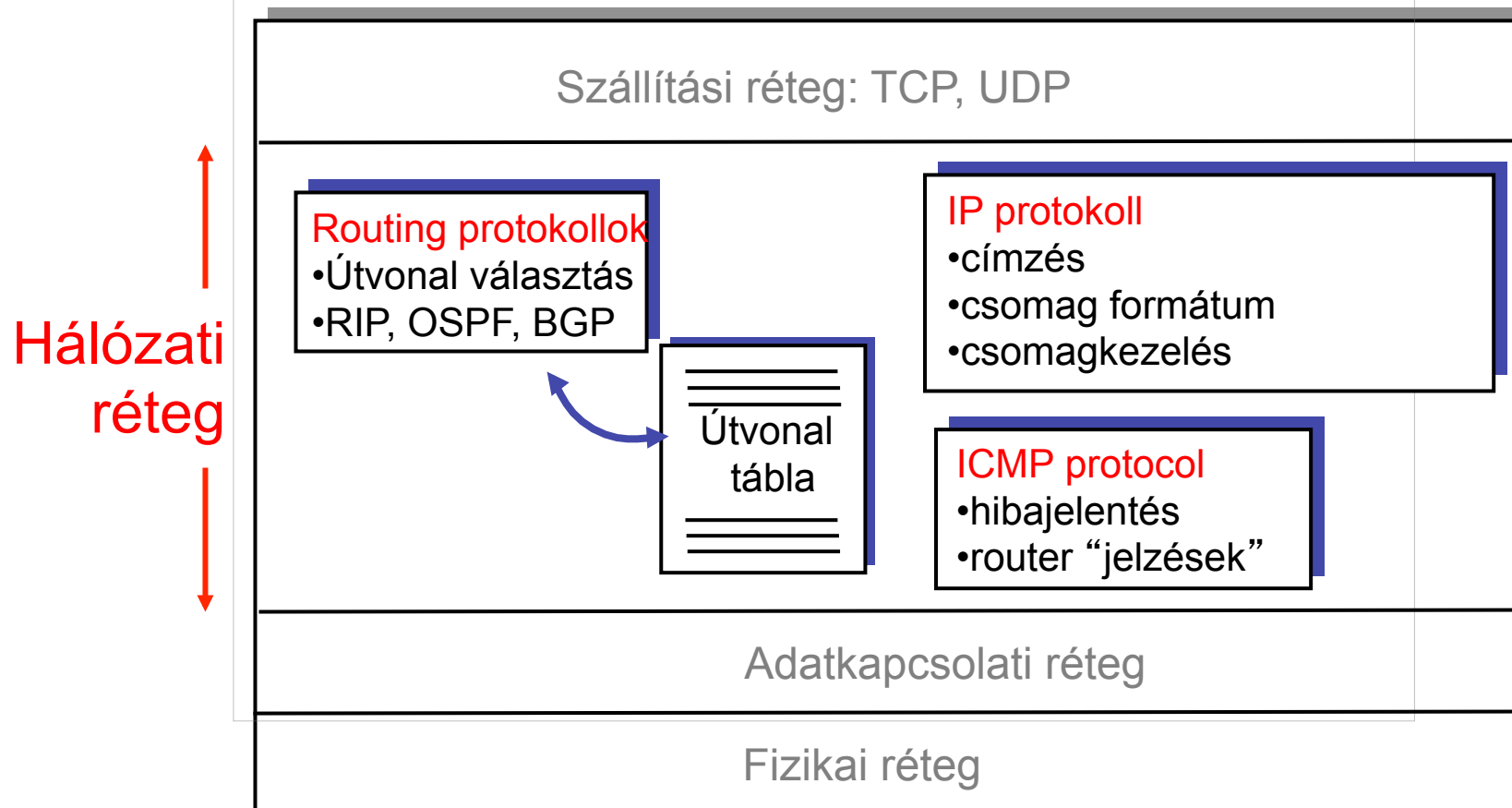
2017.október 11.

Az Internet és az IP rövid története

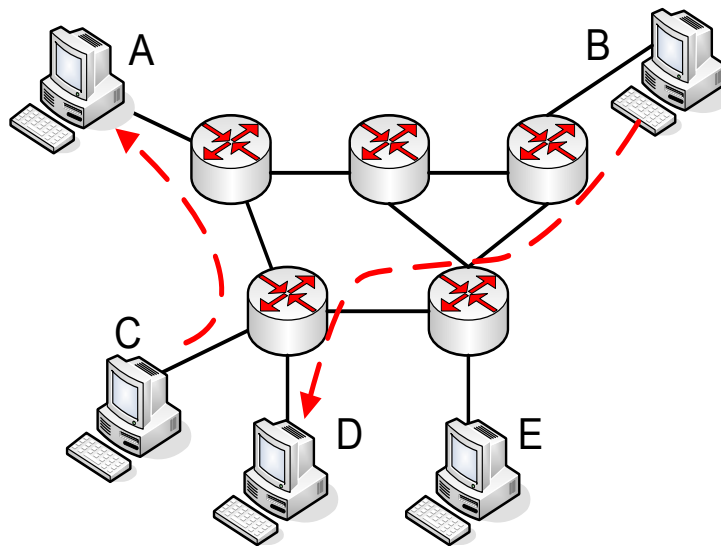
- 1969 – ARPANET, „az Internet őse”
- 1974 – Az IP és a TCP alap gondolata
 - Protokollarchitektúra az NCP kiváltására az ARPANET-en
 - „A Protocol for Packet Network Interconnection”
(Vinton G. Cerf, Robert E. Kahn)
 - Az „Internet” kifejezés megjelenése (Internet Protocol Suite)
- 1980 – IPv4 (Internet Protocol version 4)
 - Az első, széles körben használt IP és TCP verziók megalkotása
 - DoD (Department of Defense) által támogatott szabványok:
IP (RFC 760), TCP (RFC 761)
 - 1983. január 1: **Flag day**, NCP → TCP/IP
- Alapvetően ma is ezt használjuk!

Hálózati réteg feladatai

Csomópont, router hálózati rétegbeli feladatai:

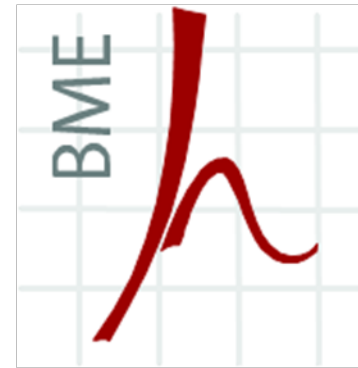


- Hálózati protokoll
 - Adattovábbítás a hálózat **végpontjai között**
- Két fő funkció
 - **Címzés (addressing) és útvonalválasztás (routing)**
 - Tördelés/fragmentálás (fragmentation)



Az IP jellemzői

- Csomagkapcsolt
 - Összeköttetés-mentes (connectionless)
 - „Best effort” – nincs garancia
 - A csomagokra igaz:
 - Elveszhetnek
 - Duplikálódhatnak
 - Sorrendjük megváltozhat
 - Meghibásodhatnak (nincs hibajavítás, hibaészlelés csak fejlécre)
 - Egyéb **NEM** nyújtott szolgáltatások:
 - Torlódáskezelés
 - Ütemezés
 - Titkosítás és hitelesítés
- } Datagram típusú



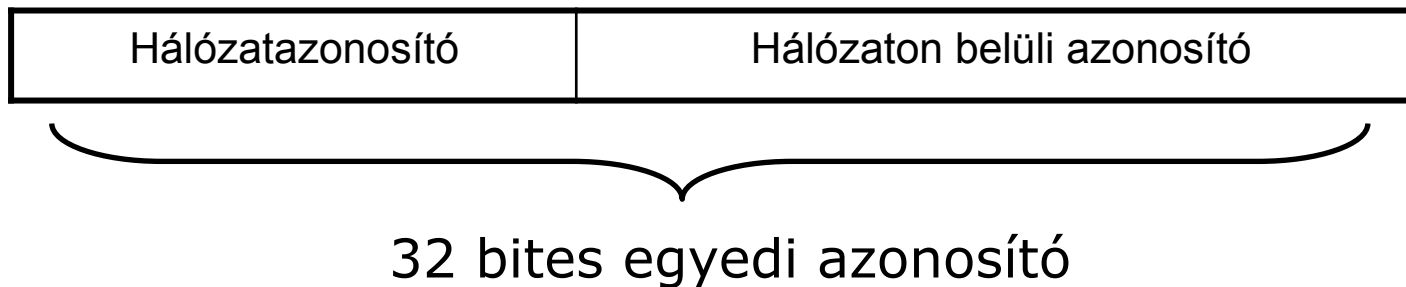
IP – Címzés

IP-címek és címosztályok

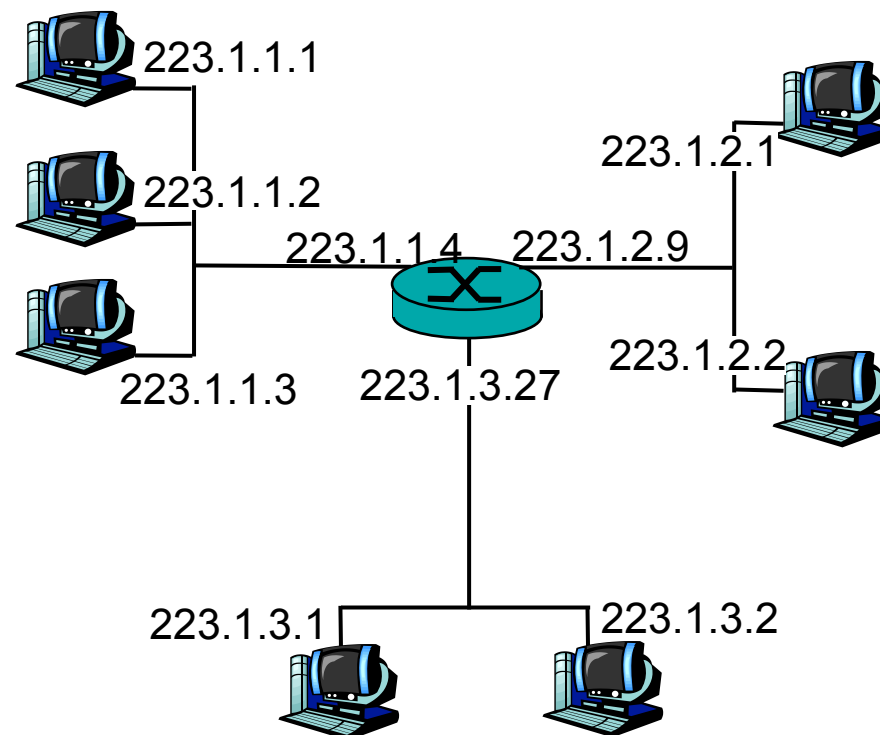
2017.október 11.

Az IPv4-cím felépítése

- 4 bájtos cím (32 bit)
 - $2^{32} \approx 4 \cdot 10^9 \Rightarrow$ kimerült!
- Jelölések
 - Bináris: 10110000 10010011 00111110 11100001
 - „Dotted decimal”: 176.147.62.225
- Cím = Hálózatazonosító + Egyedi azonosító

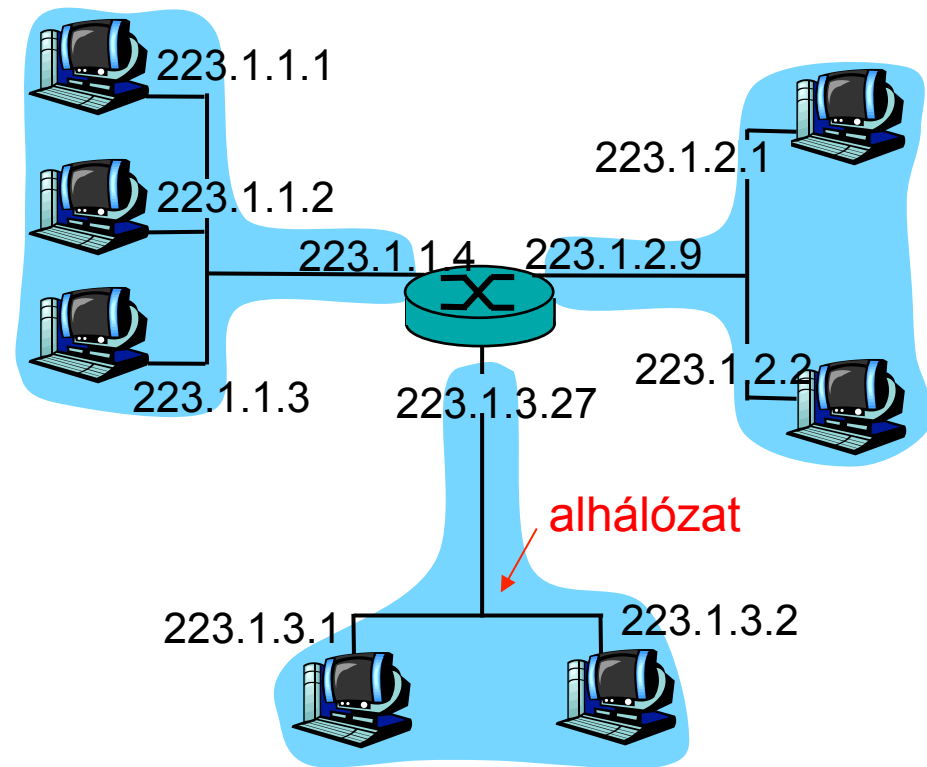


- **IP cím:** a végpont/router interfészét azonosítja
- **interfész:** kapcsolat a végpont/router és a fizikai link között
 - Router: jellemzően több interfész
 - Végpont: jellemzően egy interfész



$$223.1.1.1 = \underbrace{11011111}_{223} \underbrace{00000001}_1 \underbrace{00000001}_1 \underbrace{00000001}_1$$

- IP cím:
 - alhálózati rész
(magasabb helyiértékű bitek)
 - hoszt rész
(alacsonyabb)
- *Mi az alhálózat (subnet)?*
 - Olyan interfészek, amelyeknek megegyezik az IP címük alhálózati része
 - fizikailag eléri egymást, akár router nélkül is

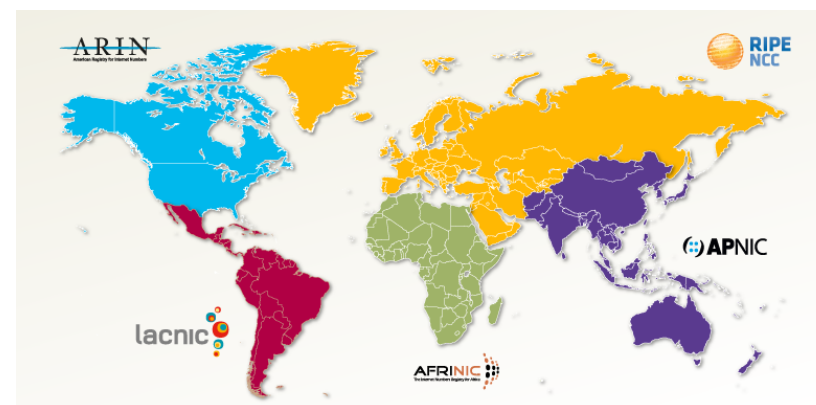


3 alhálózatból álló hálózat

- Eleinte első 8 bit hálózati, majd bevezették a címosztályokat (1981)
- Különböző méretű hálózatoknak más méretű IP-cím tartományok

Osztály	Hálózatazonosító bitjeinek száma*	Hálózatok száma*	Hálózaton belüli címek száma*
A	8	126	16777214
B	16	16382	65534
C	24	2097150	254

- Az IP-címeket kezelő szervezet, az **IANA**: Internet Assigned Numbers Authority osztja ki
- Alatta 5 Regional Internet registry
 - A és B osztályú címet kaphattak tipikusan:
 - országok, internet-szolgáltatók (ISP: Internet Service Provider), egyetemek

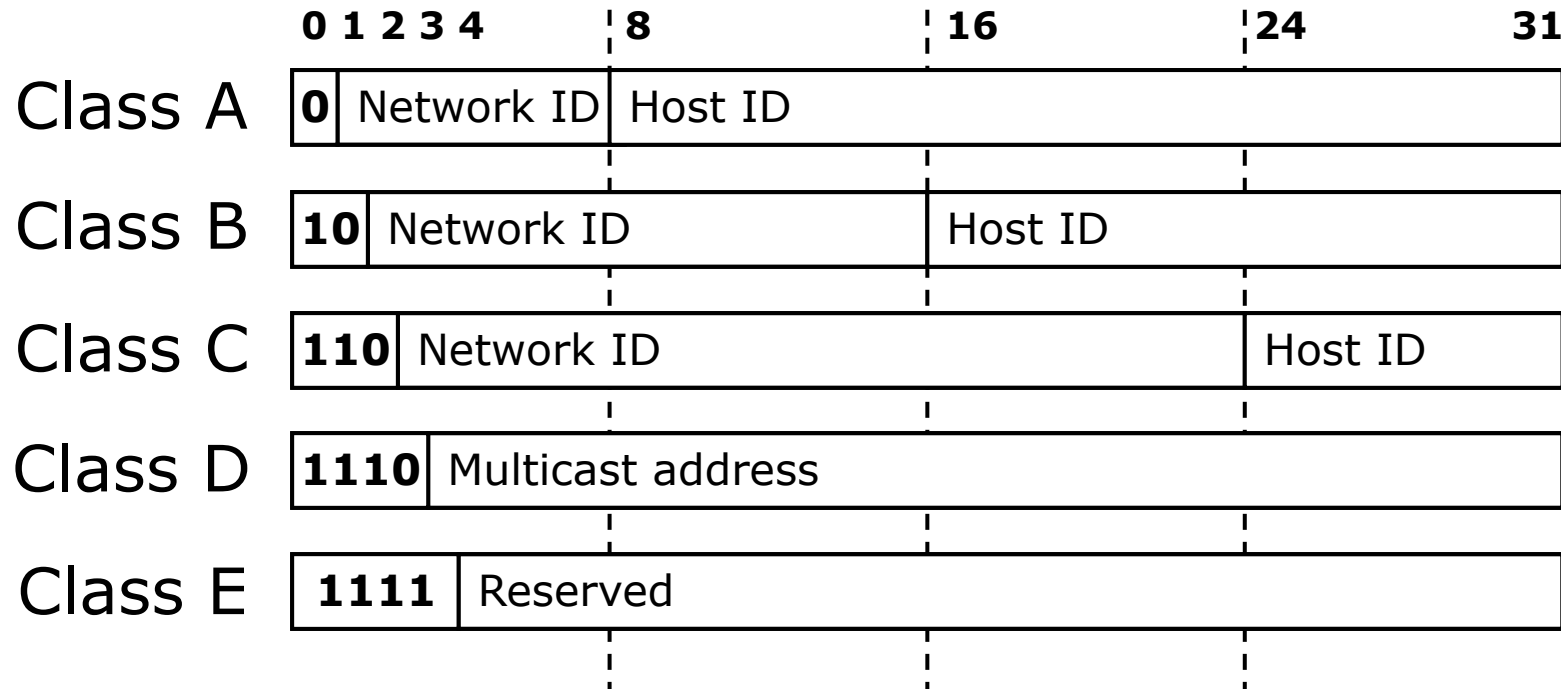


- A, B és C osztályú címek
 - Egyedi címzésre (unicast)

- D osztály
 - Többes címzésre (multicast)
 - Fenntartott címtartomány:
224.0.0.0-től 239.255.255.255-ig

- E osztály
 - Fenntartott osztály és címtartomány
240.0.0.0-től 255.255.255.255-ig

A címosztályok címkiosztása



- Osztályazonosító prefix
- Diszjunkt címtartományok

Speciális címek

- Host ID: csupa 0
 - Hálózat címe
 - Az adott hálózat eszközei opcionálisan kezelhetik
- Host ID: csupa 1
 - Broadcast cím
 - A hálózaton mindenkinek szól
- E kettő miatt csak $2^{N_{host}} - 2$ számú terminált lehet megcímezni
- 127.0.0.0 - 127.255.255.255
 - Loopback interfész
 - A helyi gépet azonosítja: localhost
 - Pl. vonaltesztelésre

Problémák a címosztályokkal

- Egyes nagy cégeknek, egyetemeknek *A* osztályú címek, amit nem használtak ki (16 millió cím)
 - *B* kicsi lett volna nekik
- Ugyanez középcégeknel: *C* túl kicsi, *B* túl nagy
- Gond a routing aggregációval
- Nem skálázható az osztályokon alapuló rendszer!

Címosztályok általánosítása

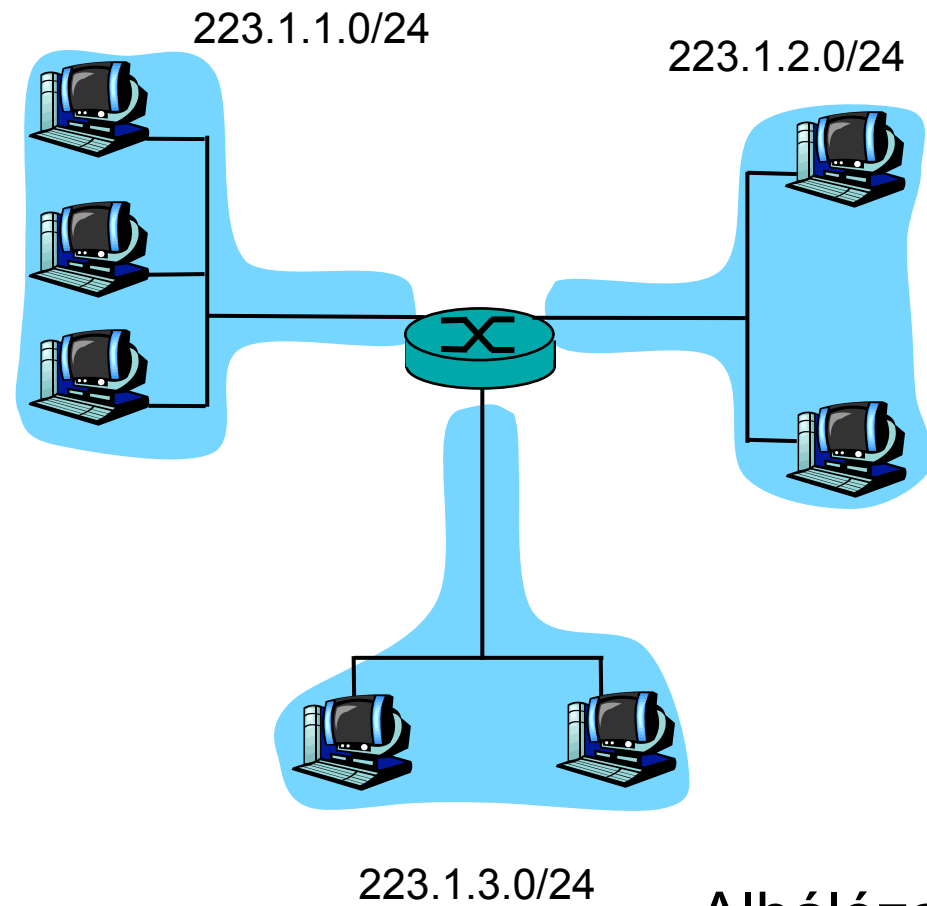
- Osztály alapú nem skálázható, plusz IPv4 címtartomány kimerülés
- **CIDR – Classless Inter-Domain Routing**
 - VLSM – Variable Length Subnet Mask
 - Osztályok eltörlése: a cím 32 bitje tetszőleges helyen lehet kettéosztva hálózat- és végponti azonosítóra
 - A címből nem lehet megállapítani, hol lett kettéosztva $\Rightarrow$ alhálózati maszk
- Subnetting
 - Alhálózatokra osztás vagy aggregálás
 - 1 db A osztályú $\Leftrightarrow$ 256 db B osztályú
 - 1 db B osztályú $\Leftrightarrow$ 256 db C osztályú
 - Már nem lehet a prefix alapján megállapítani

Alhálózati maszk (Subnet mask)

	0 1 2 3 4	N	31
IP-cím	Network ID	Host ID	
Alhálózati maszk	111...111	000...000	
Hálózatazonosító	Network ID	000...000	

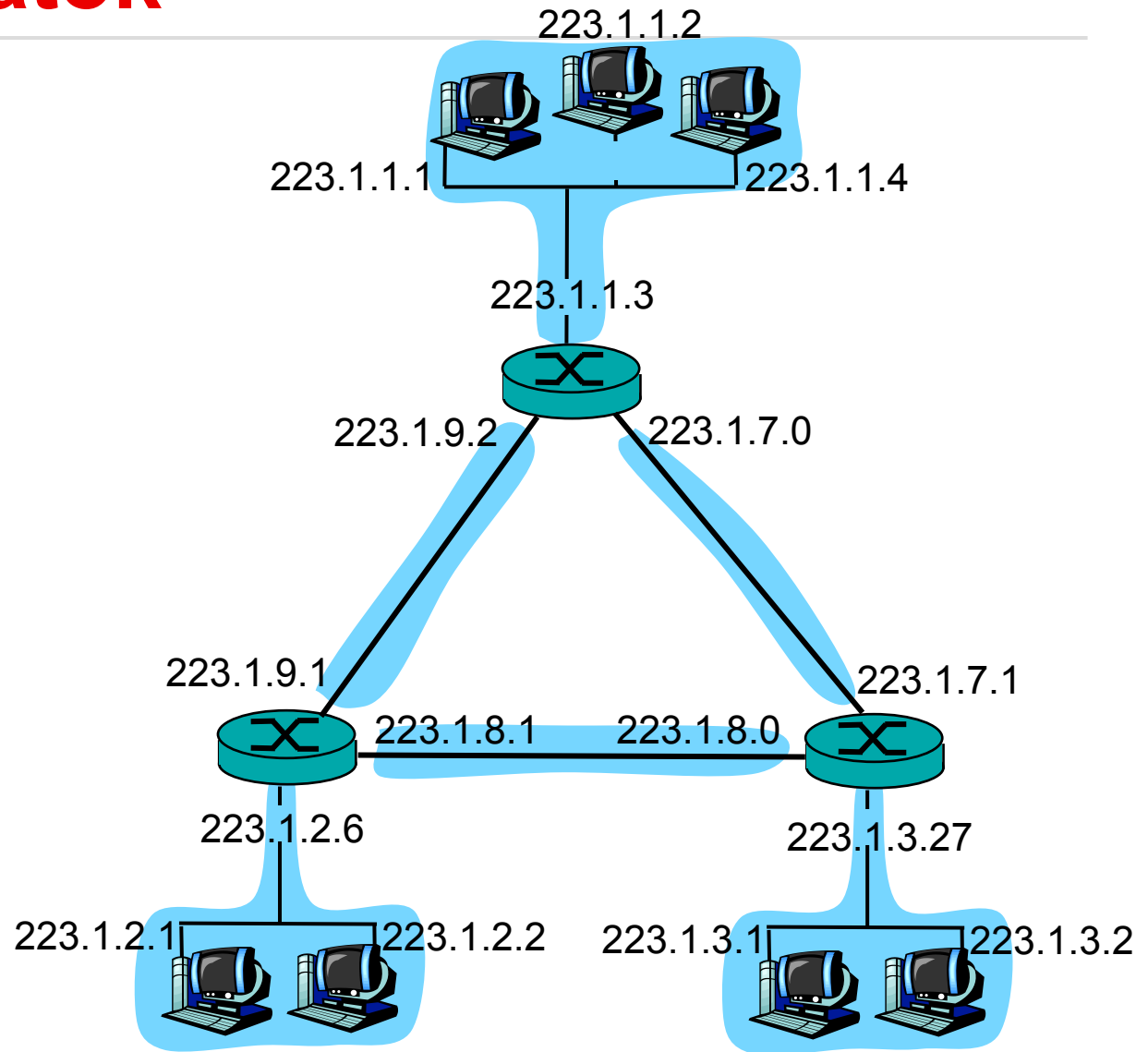
Bitenkénti **ÉS**

- Jelölés a hálózat egyértelmű azonosítására
 - <hálózat IP-címe> / <alhálózati maszk egyeseinek a száma>
 - Így pl. a BME hálózata: 152.66.0.0 /16
(alhálózati maszkja 255.255.0.0)
 - Hasonlóan:
 - A osztály: /8
 - B osztály: /16
 - C osztály: /24



Alhálózati maszk: /24

Hány legyen?

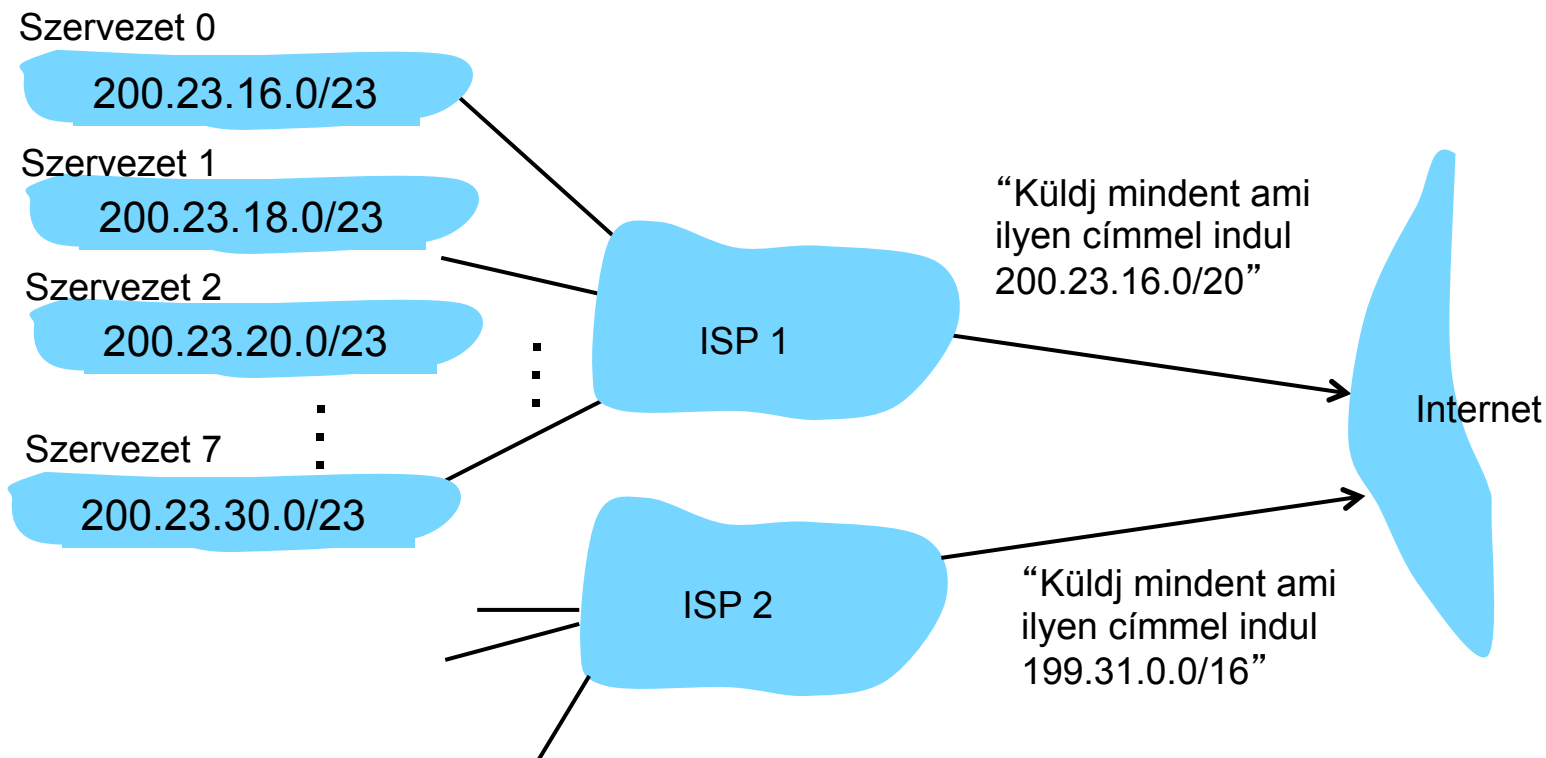


IP címek allokálása

ISP címtart.	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/20
Szervezet 0	<u>11001000</u>	<u>00010111</u>	<u>00010000</u>	00000000	200.23.16.0/23
Szervezet 1	<u>11001000</u>	<u>00010111</u>	<u>00010010</u>	00000000	200.23.18.0/23
Szervezet 2	<u>11001000</u>	<u>00010111</u>	<u>00010100</u>	00000000	200.23.20.0/23
...					
Szervezet 7	<u>11001000</u>	<u>00010111</u>	<u>00011110</u>	00000000	200.23.30.0/23

Hierarchikus címzés: útvonal aggregáció

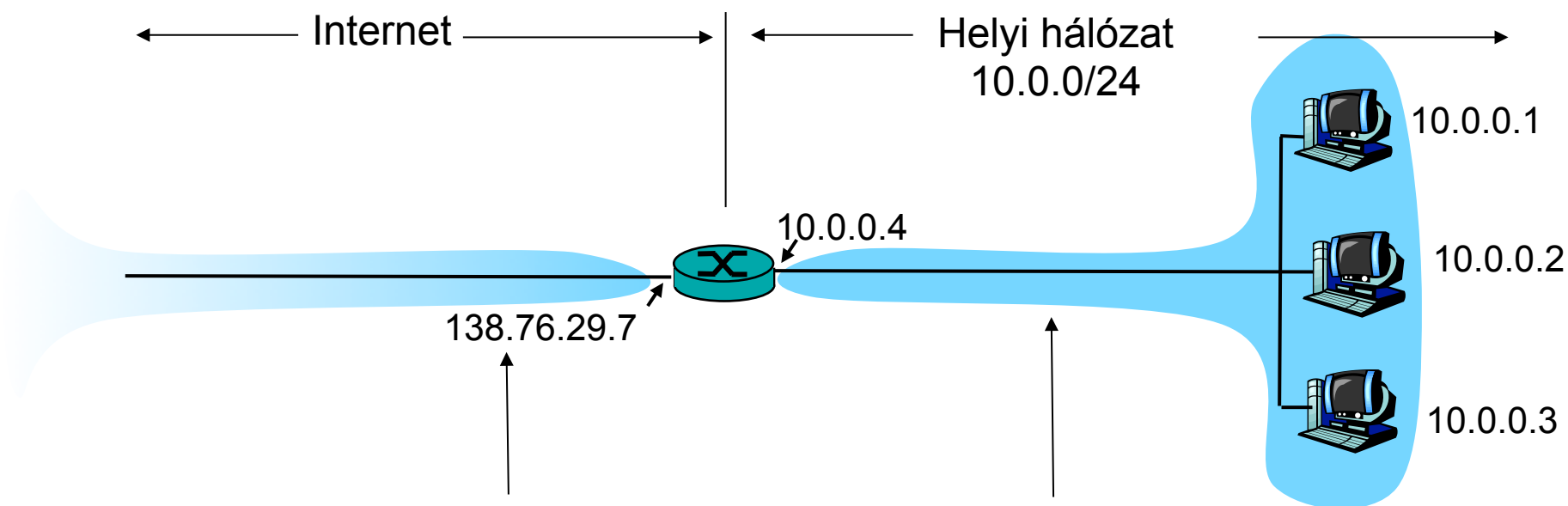
A hierarchikus címzés lehetővé teszi a routing információ hatékony hirdetését:



Privát címtartományok

- Első megoldás az IPv4 címtartomány kimerülésre
- Ötlet: pl. cégen belül nem kell globálisan egyedi IP cím ha nem kommunikál kifelé
- Nem kell hozzá RIR jóváhagyás
- Ha kifelé is szeretne: Network Address Translation (NAT)
- Privát IP-címtartományok (RFC 1918)
 - Csak helyi hálózaton (Interneten nem) érvényes címek
 - 10.0.0.0 – 10.255.255.255 (1 db A osztály)
 - 172.16.0.0 - 172.31.255.255 (16 db B osztály)
 - 192.168.0.0 - 192.168.255.255 (256 db C osztály)

NAT: Network Address Translation



Minden csomagnak, amely *elhagyja* a helyi hálózatot *egyforma* NAT IP forráscíme van: 138.76.29.7,

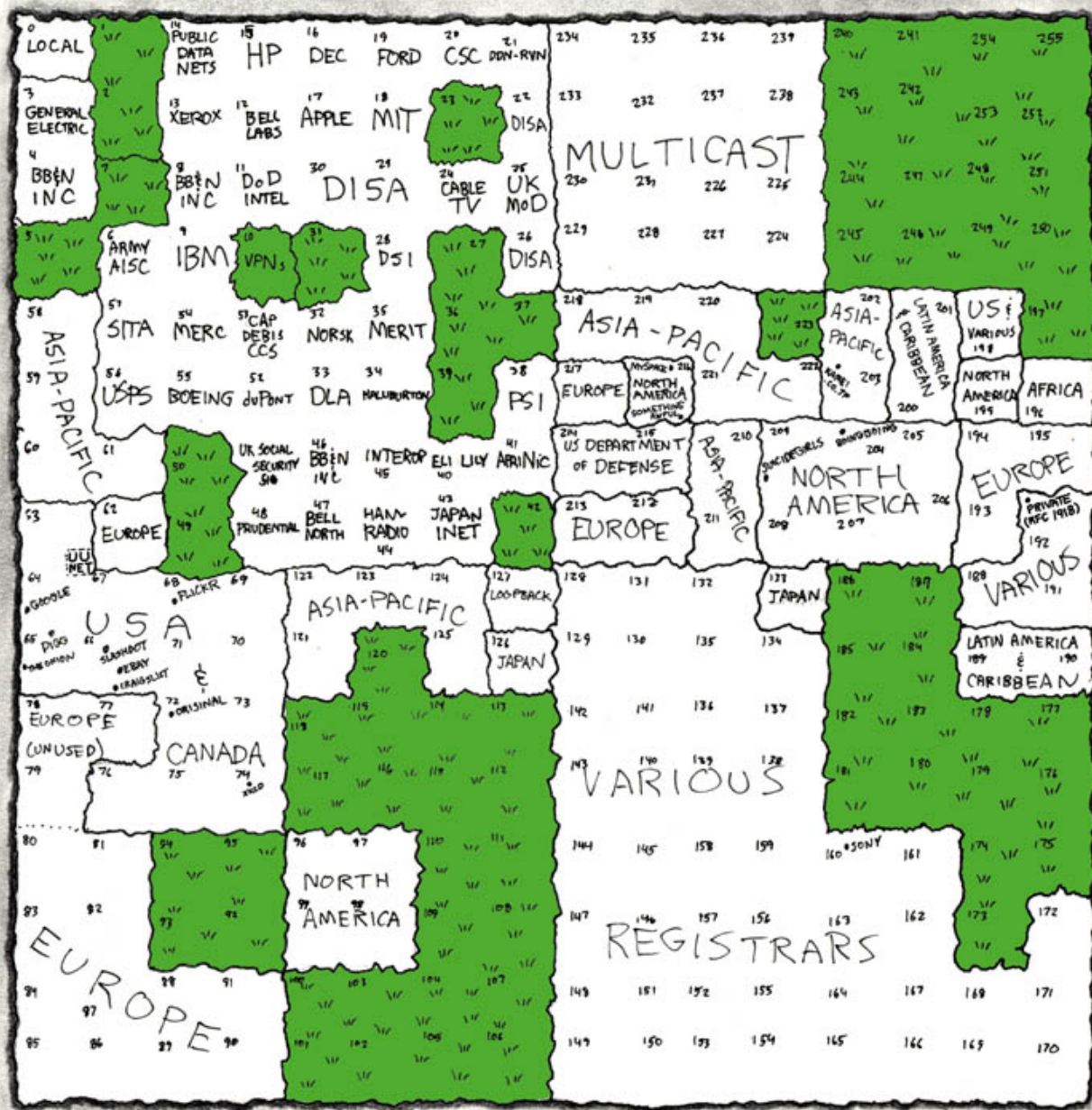
Helyi hálózaton belül 10.0.0/24 címeket használják forrás és célcímként is

Különböző port számok: szállítási rétegnél tárgyaljuk majd!

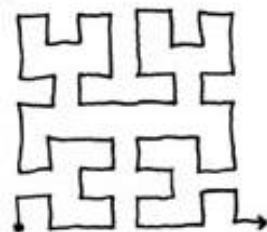
Gondok privát címtartománnyal

- Késleltette az IPv6 bevezetését
- Megsérti a végpont-végpont konnektivitás elvét
 - nehézség pl. P2P alkalmazásoknál: NAT traversal megoldások
- Routers elvileg csak a hálózati rétegig dolgozhatnak fel a csomagokat
- Privát hálózatok egyesítése: címduplikáció
 - Újracímzés
 - NAT közöttük
- Privát címek kiszivárgása az Internetre
 - Rosszul konfigurált privát hálózat
 - Határ routerek szűrik

THE IPv4 SPACE, 2006



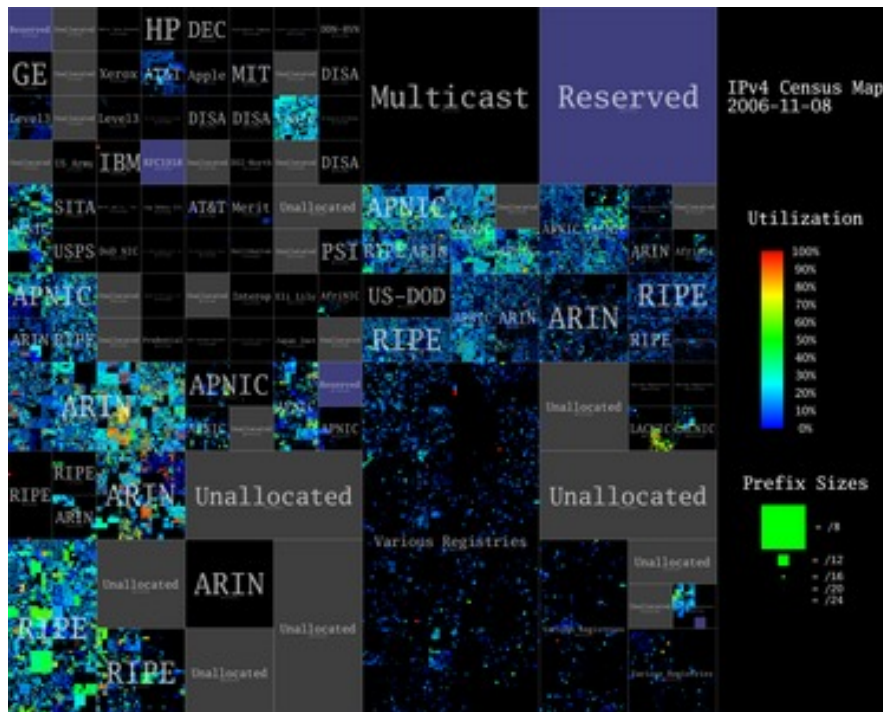
THIS CHART SHOWS THE IP ADDRESS SPACE ON A PLANE USING A FRACTAL MAPPING WHICH PRESERVES GROUPING -- ANY CONSECUTIVE STRING OF IP_s WILL TRANSLATE TO A SINGLE COMPACT, CONTIGUOUS REGION ON THE MAP. EACH OF THE 256 NUMBERED BLOCKS REPRESENTS ONE /8 SUBNET (CONTAINING ALL IP_s THAT START WITH THAT NUMBER). THE UPPER LEFT SECTION SHOWS THE BLOCKS SOLD DIRECTLY TO CORPORATIONS AND GOVERNMENTS IN THE 1990's BEFORE THE RIR_s TOOK OVER ALLOCATION.



0	1	4	5	16	19	→
3	2	13	12	17	18	
4	7	8	11			
5	6	9	10			

IPv4 címtartomány kimerülése

2006



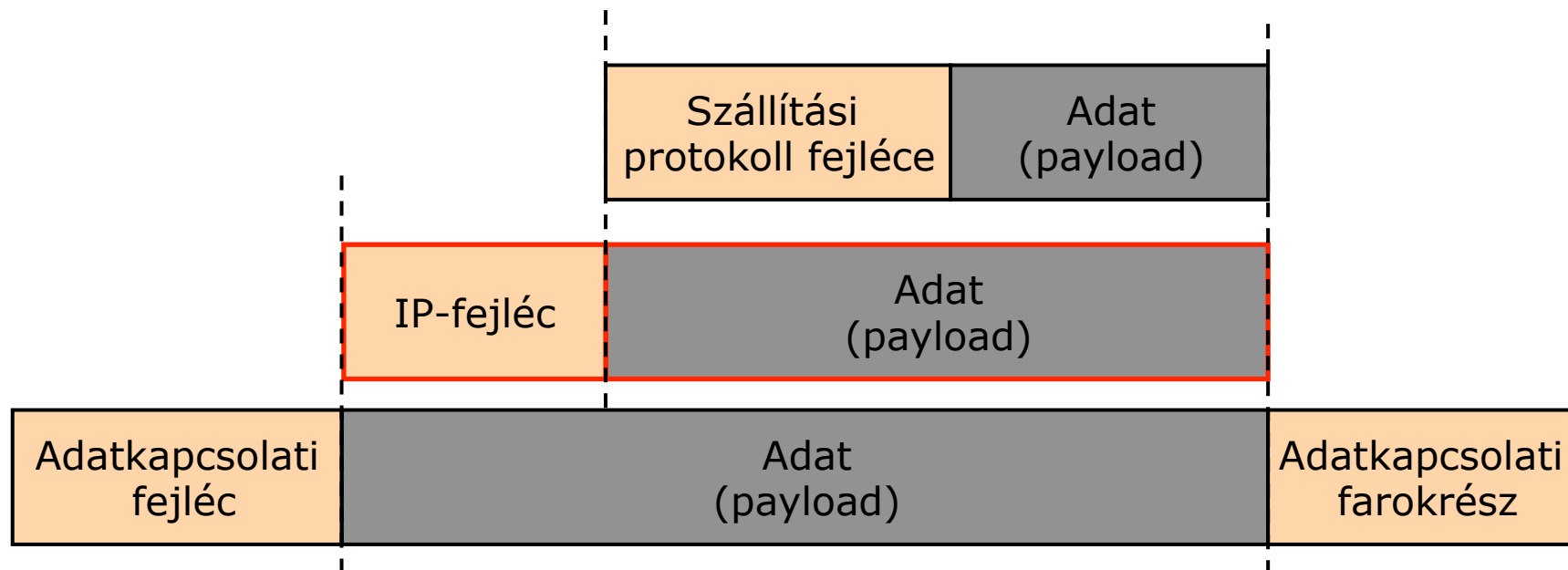
2012

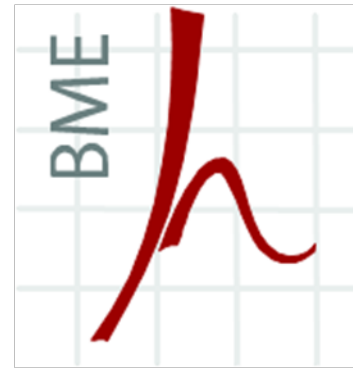


- Bevezetés
 - Az IP feladata és jellemzői
- Címzés
- Az IP csomag szerkezete
- Routing
- IP segédprotokollok
- IPv6

Az IP-csomag szerkezete és „helye”

- Az IP-csomag két része:
 - IP-fejléc / fejrész (IP header)
 - Adat (payload)
- Az IP-csomag alsóbb rétegbeli protokoll adatrészébe ágyazódik be
- Az IP-csomag adatrészébe magasabb rétegbeli protokollüzenet (PDU) kerül



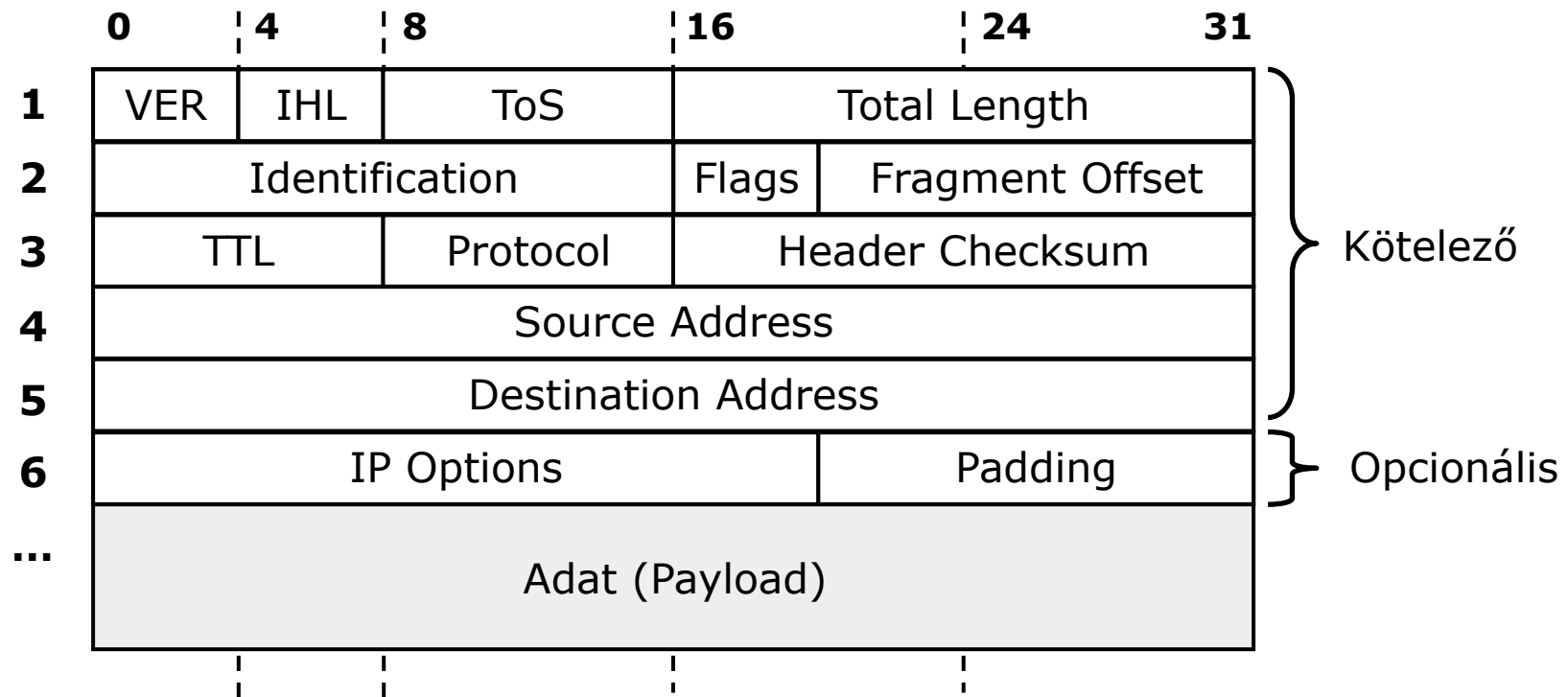


IP - Fejléc

Az IP fejléc szerkezete

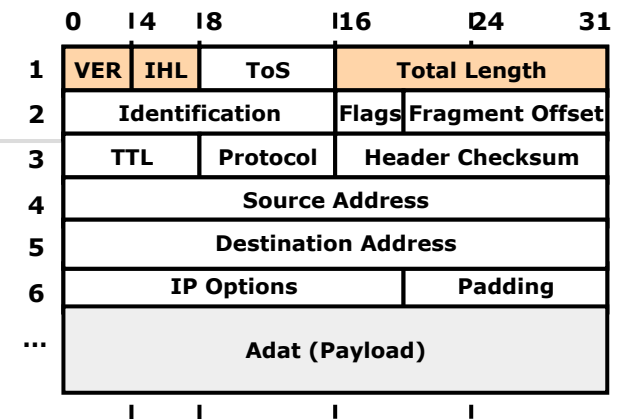
2017.október 18.

Az IP fejléc szerkezete



Az IP fejléc mezője I.

- VER – Version (4 bit)
 - Az Internet Protocol verziójának száma
 - Tipikus értéke: IPv4: 4, IPv6: 6
- IHL – Internet Header Length (4 bit)
 - Az IP fejléc mérete **32 bites szavakban**
 - Értéke:
 - Minimum: 5 (20 byte)
 - Maximum: $2^4-1=15$ (60 byte)
- Total Length (16 bit)
 - A teljes IP csomag mérete **bájtokban**
 - Értéke:
 - Minimum: 576 (IP-fejléc 20 + 512 adat + 44 IP-opciók és az alsóbb réteg fejlécei)
Ilyen méretű csomagot tördeletlenül kell továbbítani!
 - Maximum: $2^{16}-1=65535$ (max. 65515 bájt adat)

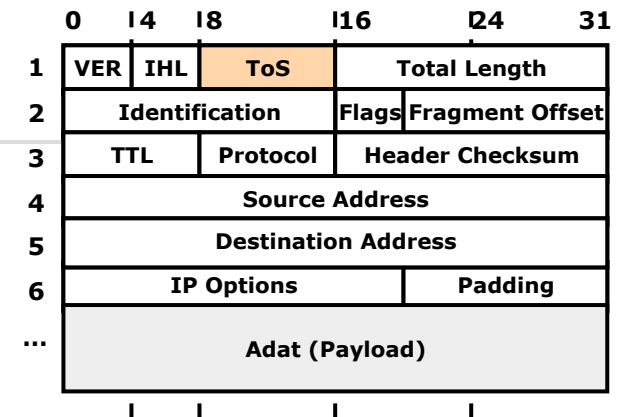


Az IP fejléc mezői II.

- ToS (Type of Service) (8 bit)
 - QoS osztályok, paraméterek jelzésére (RFC 791)

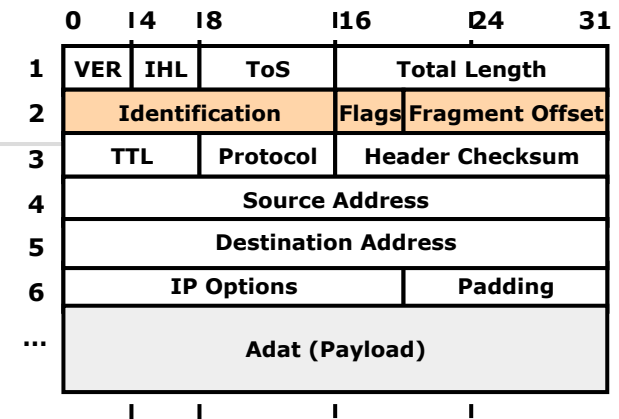
Bitek	Jelentés
0-2	Precedencia Példák: „network control” „priority” „routine”
3	Késleltetés (normal/low)
4	Throughput (normal/light)
5	Reliability (normal/high)
6-7	Fenntartott

- A legtöbb router nem támogatja, de jövőben várható (VoIP forgalom miatt)
- Leggyakrabbi felhasználás:
 - DSCP – Differentiated Services Code Point (RFC 2474)- 6bit:
DiffServ
 - ECN – Explicit Congestion Notification (RFC 3168)- 2bit

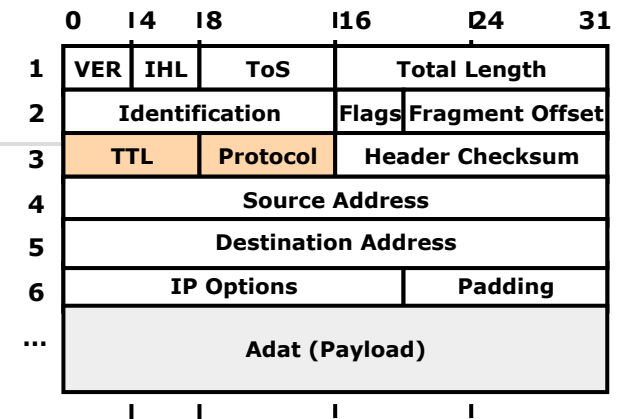


Az IP fejléc mezői III.

- **Identification (16 bit)**
 - Az IP-töredékek egyedi azonosítása
- **Flags (3 bit)**
 - 0: Fenntartott
 - 0-nak kell lennie
 - „Evil bit” (RFC 3514) (áprilisi tréfa 2003-ban)
 - 1: DF – Don’t Fragment
 - 1: ha tördelni kellene, el kell dobni
 - Ezt használja az MTU (Maximum Transmission Unit) Path Discovery néhány TCP verzióban és az IPv6-ban
 - 2: MF – More Fragment
 - 1: ha nem az utolsó töredék
 - 0: utolsó töredék vagy nem tördelt csomag
- **Fragment Offset (13 bit)**
 - Az eredeti csomagban lévő kezdőpozícióját adja meg e töredékben lévő adatnak **8 bájtos egységekben**
 - $(2^{13}-1) \times 8 = 65528 > 65515$ bájt (max. adat)
(így a maximális méretű csomag is tördelhető)

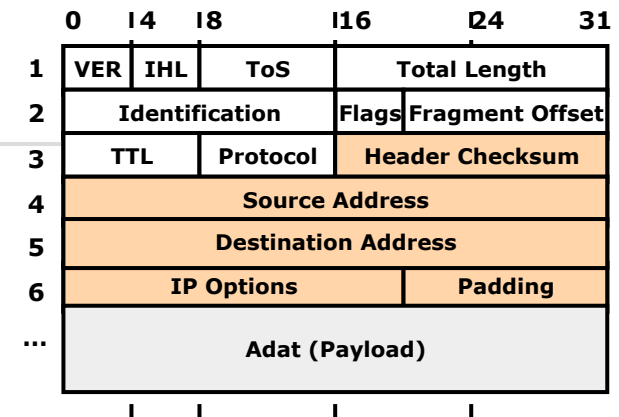


Az IP fejléc mezői IV.

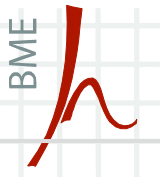


- **TTL – Time To Live (8 bit)**
 - Csomag élettartama
 - Eredetileg másodpercben
 - Gyakorlatban **hopszámban** mérve (hop count)
 - Minden továbbításnál csökkenteni kell ez értékét legalább 1-gyel
 - Ha a csökkentés után az értéke nem >0, akkor el kell dobni
- **Protocol (8 bit)**
 - Az adatrészben lévő protokoll azonosítója
 - Pl: (kezdeti lista az RFC 790-ben)
 - 1: Internet Control Message Protocol (ICMP)
 - 2: Internet Group Management Protocol (IGMP)
 - 6: Transmission Control Protocol (TCP)
 - 8: Exterior Gateway Protocol (EGP)
 - 17: User Datagram Protocol (UDP)
 - 89: Open Shortest Path First (OSPF)
 - 132: Stream Control Transmission Protocol (SCTP)
 - Az IANA felügyeli ezeket az azonosítókat

Az IP fejléc mezői V.



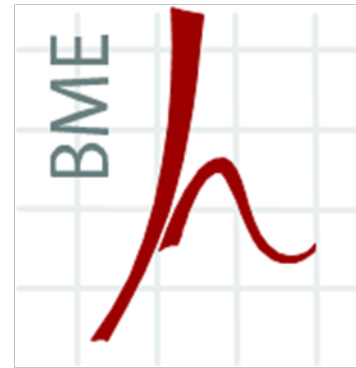
- **Header Checksum (16 bit)**
 - Az **IP fejléc** minden 16 bites szavának összegére számolt egyes komplement
 - A csomag érkezésekor ellenőrizni kell a helyességét, és továbbítás esetén újra kell számítani
 - Új TTL minden lépésben, és fragmentáció is lehet
- **Source / Destination Address (2 x 32 bit)**
 - Az IP-csomag feladójának és címzettjének az IP-címe
 - NAT miatt lehet nem a feladó tényleges címe
- **IP Options**
 - Ritkán használt opcionális része a fejlécnek
 - Segítségével például a csomag útjának lehet kijelölni
 - SSRR: Strict Source (Record) Route – pontos út kijelölése
 - LSSR vagy LSRR: Loose Source (Record) Route – kötelező útba ejtendő csomópontok kijelölése
 - Legtöbb router biztonsági okokból eldobja
- **Padding**
 - Az IP Options részt egészíti ki 4 bájt többszörösére



Példa ellenőrzőösszegre

- Túlcsordulást figyelembe kell venni
- Példa: két 16 bites integer összeadása

	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
	1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
carry bit	1	1	0	1	1	1	0	1	1	1	0	1	1	1	0	1
összeg	1	0	1	1	1	0	1	1	1	0	1	1	1	1	0	0
ellenőrzőösszeg	0	1	0	0	0	1	0	0	0	1	0	0	0	0	1	1

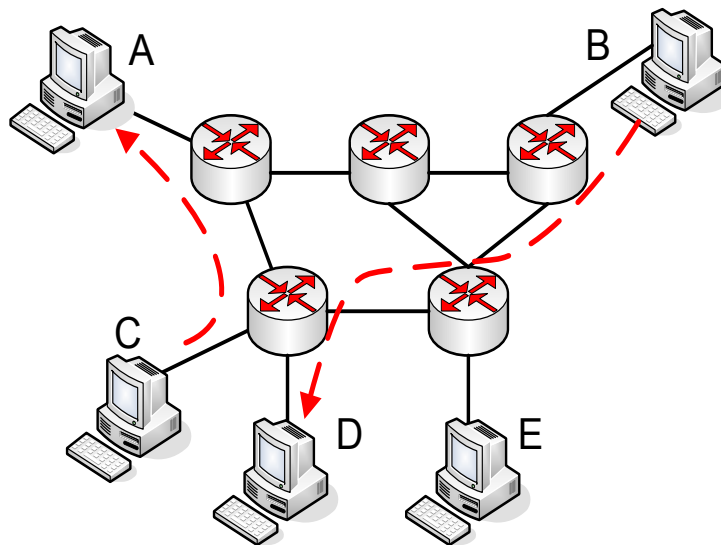


IP - Útvonalválasztás

Az IP routing működése

2017.október 18.

- Hálózati protokoll
 - Adattovábbítás a hálózat végpontjai között
- Két fő funkció
 - **Címzés (addressing) és útvonalválasztás (routing)**
 - Tördelés (fragmentation)



A csomagtovábbítás alapelve

- Az IP jellemzői
 - Csomagkapcsolt
 - Összeköttetés-mentes (connectionless)
 - „Best effort” – nincs garancia
- Minél gyorsabban továbbítsuk
- Csak a következő csomópontot kell ismernünk (**hop-by-hop**)
- Előnyei:
 - Kis erőforrásigény
 - Egyszerű, ezért gyorsan továbbítható
 - Gyors, ezért nem kell tárolnunk a csomagokat
 - » kis memóriaigény
 - „Kevés” ismeret a hálózatról
 - Datagram szolgáltatásra tökéletesen alkalmas
 - nem vállal garanciát, nincs szükség nyugtázásra és egyéb hibakezelésre ⇒ gyorsasága megmarad

} Datagram típusú

Továbbításhoz szükséges információk

- Kinek küldjük tovább?
 - Cél címe alapján $\Rightarrow$ csomag tartalmazza
 - Saját ismeret alapján $\Rightarrow$
útvonal-irányítási táblázat (routing table)
 - Hogyan küldjük tovább?
 - Mekkora egységekben?
 - Mekkora érkezik? $\Rightarrow$ csomag határozza meg
 - Mekkora továbbítható? $\Rightarrow$
a következő hálózat MTU-ja (Maximum Transmission Unit) határozza meg
 - Milyen QoS biztosításával?
 - „Best effort” – nincs garancia
 - Opcionális megoldás:
ToS mező felhasználásával egyéb protokollok és mechanizmusok
- Routing
(útválasztás,
útvonal-
irányítás)
- Tördelés
(fragmentation)
- QoS

Útválasztó tábla (Routing table)

- Szükséges információk
 - Hova tart?
 - Merre küldjük tovább?
 - Ki a következő csomópont?
 - Melyik interfészen kell továbbítani?

Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

Útválasztó tábla (Routing table)

Merre megy?		Merre küldjük?		
Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

- Táblázatban szereplő hálózatok közül melyikbe megy?
- Az ahhoz tartozó interfészre küldjük ki

Hálózat kiválasztása

	0 1 2 3 4	N	31	
Cél IP-cím	Network ID	Host ID		
n. bejegyzés alhálózati maszkja	111...111	000...000		

	?			Bitenkénti ÉS
n. bejegyzés hálózatazonosító	Network ID	000...000		

- A cél IP-cím akkor tartozik egy hálózatba, ha a hálózatazonosító résszel megegyezik

Keresés az útválasztó táblában

- Ha több hálózatra is illeszkedik: **leghosszabb egyezőséget** kell választani!
 - leghosszabb hálózati maszk
- Az útválasztó tábla összes bejegyzését végig kell nézni
 - ⇒ rosszul skálázódik
 - Általában bináris fával implementálják
 - ⇒ n számú bejegyzésben lineáris keresés helyett csak a cím hosszában logaritmikus

Alapértelmezett útvonal (Default route)

- Erre megy a csomag, ha nem ismeri a célhálózatot
- Minden címet tartalmazó hálózat
 - Ehhez a hálózati cím: 0.0.0.0/0
- Az alapértelmezett átjáró és elnevezése
 - A fenti bejegyzéshez tartozó következő csomópont IP-címe
 - **Alapértelmezett átjáró (default gateway, DG)** név nem szerencsés
 - Helyette inkább a router / útválasztó/ útvonalválasztó
- Végpontokon gyakran csak két bejegyzés szerepel:
 - Helyi hálózat (helyi végpont közvetlenül elérhető)
 - Alapértelmezett útvonal (minden más távoli hálózaton)

Metrikák szerepe az útválasztásban

- Metrika (mérték): Egy számérték, amely a hálózati utak közötti preferenciát adja meg
- Metrika alapja lehet például:
 - Elérhetőség
 - Terheltség
 - Késleltetés
- Metrika típusa
 - Statikus
 - Manuálisan megadott
 - Dinamikus
 - A link vagy a hálózat állapotától függően automatikusan változó
- A jobb metrikával rendelkező kapcsolaton küldjük ki a csomagot!

Megfelelő bejegyzés kiválasztva

Hálózat címe	Alhálózati maszk	Interfész	Közvetlenül kapcsolódó	Következő csomópont
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>
<IP-cím>	</N>	<azonosító>	<igen/nem>	<IP-cím>

- Mi a stratégia, ha
 - Közvetlenül (nincs következő csomópont!)
 vagy
 - nem közvetlenül kapcsolódik a hálózat?

Teendők helyi és távoli hálózat esetén

- Közvetlenül kapcsolódó (helyi) hálózat
 - A címzettnek közvetlenül küldeni
 - Ehhez a címzett **adatkapcsolati rétegbeli (MAC) címére** van szükség
- Nem közvetlenül kapcsolódó (távoli hálózat)
 - Az útválasztónak kell küldeni
 - A csomag IP-címét tilos módosítani
 - Csak **adatkapcsolati rétegben** kell az útválasztónak címezni
 - Ehhez szükség van az adatkapcsolati címére

Keret továbbítás MAC cím alapján

Közvetlenül kapcsolódó (helyi) hálózat esetén, nincs router:

Amikor a kapcsoló (switch) vesz egy keretet:

megnézi a kapcsolótáblát a MAC célcím alapján

if van bejegyzés az adott MAC célcímre

then{

if a cél azon a szegmensen van, ahonnan jött a keret

then eldobja a keretet

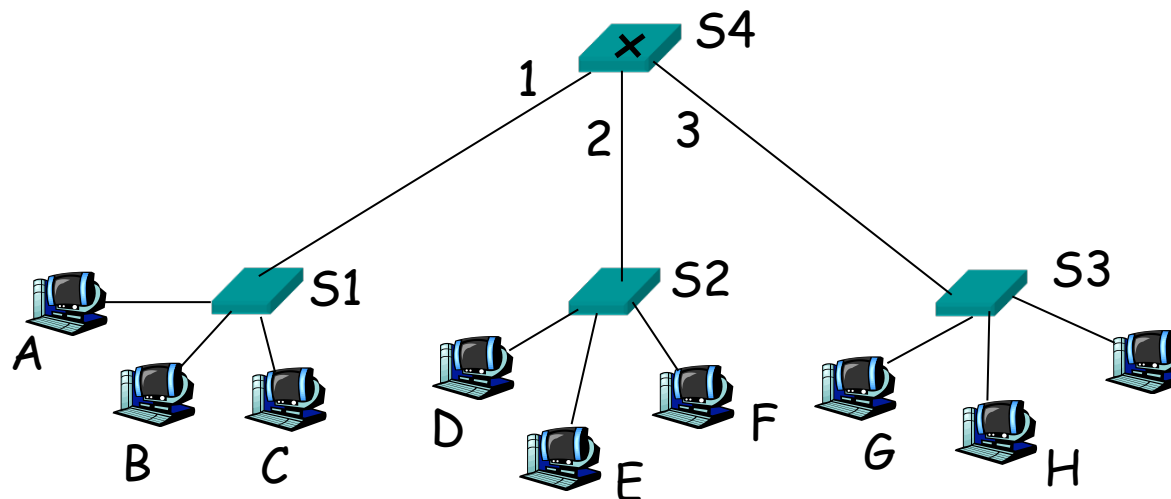
else továbbítja a megadott interfészre

}

else elárasztás

*továbbítás minden interfészre,
kivéve azt, amelyről érkezett*

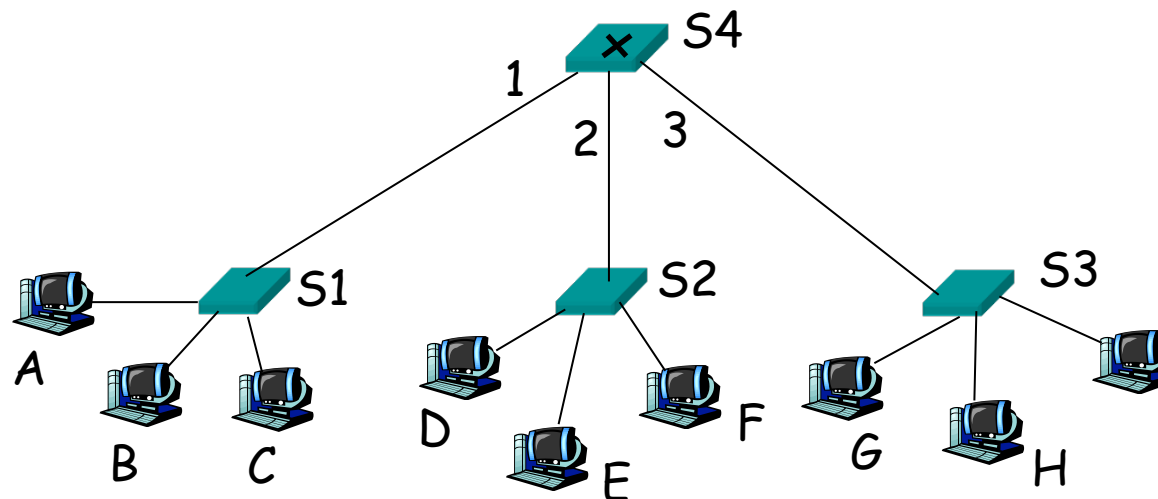
Példa alhálózaton belüli továbbításra



address	interface
A	1
B	1
E	2
G	3
I	

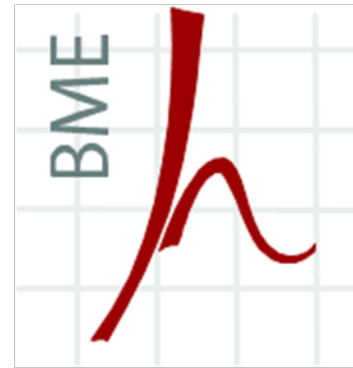
- A kapcsoló vesz egy **C-től D-nek** menő keretet
 - **bejegyzi a táblába**, hogy C az 1-es interfészen érhető el
 - mivel D nincs benne a táblában, továbbítja a keretet a 2 és 3 interfészre
- D veszi a keretet

Példa (folyt.)



address	interface
A	1
B	1
C	1
E	2
G	3
I	

- A kapcsoló veszi a keretet D-től
 - **bejegyzi a táblába**, hogy D a 2-es interfészen érhető el
 - mivel C benne van a táblában, továbbítja a keretet az 1-es interfészre (csak oda)
- C veszi a keretet



IP – ARP/RARP

Kapcsolat az adatkapcsolati címek felé

2017.október 18.

ARP – Address Resolution Protocol

- Ha ismerjük az IP-címet, és a hozzá tartozó adatkapcsolati rétegbeli címre van szükség
 - RFC826
- Szinte minden adatkapcsolati és hálózati réteget támogat
 - Token Ring, FDDI, ATM, IEEE802.3, IEEE802.11
- Működése:
 - **Broadcast** kérés: „Kinek az IP-címe a ...?”
 - Az IP-cím tulajdonosa válaszol
- Az ARP üzeneteket közvetlenül az adatkapcsolati réteg protokolljának küldjük (**Nem IP-csomag!**)

Az ARP fejléce

0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		
RARP header structure		

- Hardware Type
 - Ethernet: 0x0001
- Protocol Type
 - IP: 0x8000
- HLen
 - Ethernet: 6 byte
- PLen
 - IPv4: 4 byte
- Operation
 - ARP request = 1
 - ARP reply = 2
 - RARP request =3
 - RARP reply =4
- Sender Hardware Address
 - <MAC-cím>
- Sender Protocol Address
 - <IP-cím>
- Target Hardware Address
- Target Protocol Address

Névfeloldás ARP-vel

- „A” szeretné megtudni „B” MAC-címét
 - 1. „A” üzenete
 - Operation: **ARP Request** = 1
 - Sender HA: <A MAC-címe>
 - **Megegyezik a keret fejlécében** találhatóval
 - Sender PA: <A IP-címe>
 - Target HA: 00:00:00:00:00:00 (ismeretlen)
 - **A keret MAC címében FF:FF:FF:FF:FF:FF !!! (broadcast)**
 - Target PA: <B IP-címe>
 - 2. „B” válasza
 - Operation: ARP Reply = 2
 - Sender HA: <**B MAC-címe**>
 - Most már nem 00:00:00:00:00:00 (ismeretlen)
 - Megegyezik a keret fejlécében találhatóval
 - Sender PA: <B IP-címe>
 - Target HA: <A MAC-címe>
 - Target PA: <A IP-címe>

- Címpárok: Adatkapcsolati rétegbeli és IP-címek
- Két bejegyzéstípus
 - Statikus
 - Manuálisan felvitt bejegyzés
 - Dinamikus
 - ARP címfeloldás eredménye
 - **Gyorsítótár (cache)** funkció: ne kelljen mindig lekérdezni
 - Egy idő után elévül és törlődik

<i>HW-cím</i>	<i>IP-cím</i>	<i>típus</i>
<MAC-cím1>	<IP-cím1>	statikus
<MAC-cím2>	<IP-cím2>	dinamikus

ARP egyéb alkalmazásai

▪ ARP próba (probe)

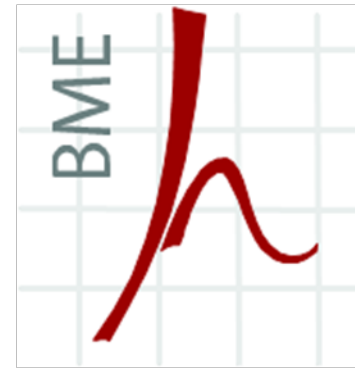
- Mielőtt használni kezdene egy IPv4 címet, **felderíti, hogy nem használja-e más**
- Broadcast ARP kérés, **küldő IP címe csupa nulla**, saját címét kérdezi le
- *IPv4 Address Conflict Detection* (RFC 5227)

▪ ARP hirdetmény (announcement)

- Ha változik MAC vagy IP címe, küld egy *gratuitous ARP* üzenetet, hogy mások tudják **frissíteni az ARP táblájukat**
- TPA=SPA és THA=0 (request) vagy TPA=SPA, THA=SHA (reply)
 - Pl. operációs rendszer betöltésnél ha változott a hálózati kártya
 - vagy terheléselosztásra (több hálókártyánál)

RARP – Reverse ARP

- Adatkapcsolati rétegbeli címből IP-címet: nem használatos már a RARP
- RARP kiszolgálók
 - RARP broadcast üzenetekre válaszolnak
- Nem használják már, helyette:
 - Bootstrap Protocol (BOOTP): hálózatról történő betöltésre
 - Dynamic Host Configuration Protocol (DHCP): IP-cím kérésére



IP – Útvonalválasztó protokollok

Útvonalválasztó táblák építése automatikusan

2017.október 25.

Útválasztó protokollok feladatai

- Útvonal-irányítási információk begyűjtése
- Hurokmentes útvonal-irányítás
- Újabb csomópontok és hálózatok csatlakoztatásának biztosítása
- Csomópontok és hálózatok leválasztásának kezelése

Útvonalválasztó protokollok funkcionális osztályozása

- **Ad hoc** routing protokollok
 - Kis és gyorsan változó hálózatokra
 - Szenzor és egyéb vezeték nélküli hálózatokra
- **Interior Gateway Protocols (IGPs)**
 - Autonóm rendszereken (AS) belül
 - Kisebb hálózatokon
- **Exterior Gateway Protocols (EGPs)**
 - Autonóm rendszerek (AS) között
 - Az Internet routing protokollja

Ad hoc routing protokollok osztályozása

- Működési mód szerint
 - Proaktív
 - Folyamatosan karbantartott táblákkal
 - Reaktív
 - Igény szerinti célfelderítés
 - Hibrid
 - A fenti kettő együttes alkalmazása

- Alkalmazási terület szerint
 - Hierarchikus
 - Földrajzi elhelyezkedés alapján
 - Multicast
 - Energiatakarékos

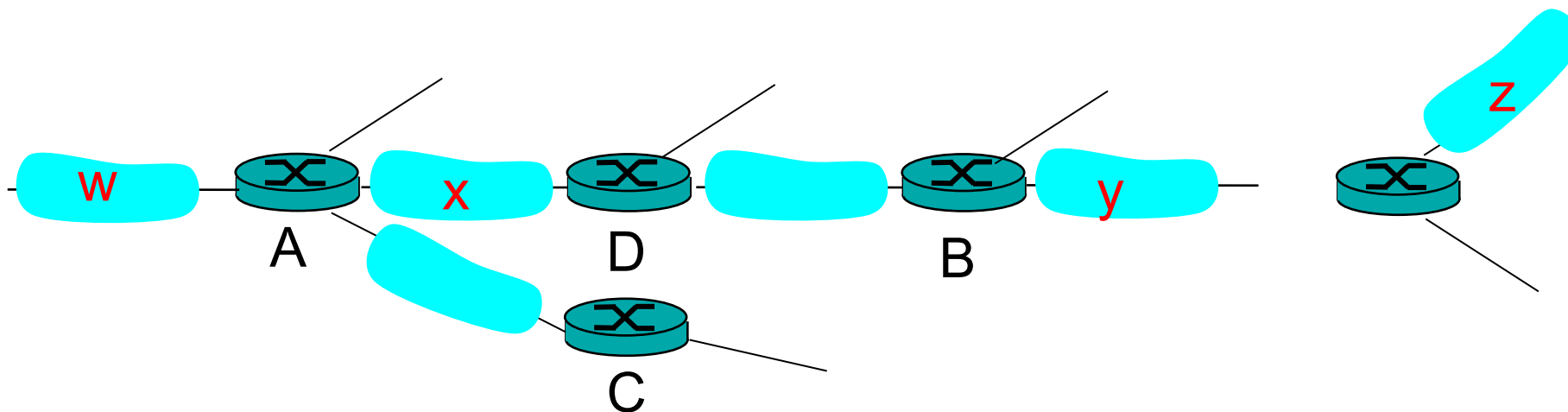
Interior Gateway Protocols (IGPs)

- Autonóm rendszereken (AS) belül
 - Távolság-vektor:
 - RIP (Routing Information Protocol)
 - IGRP (Interior Gateway Routing Protocol)
 - EIGRP (Enhanced Interior Gateway Routing Protocol)
 - Összekötés-állapot:
 - OSPF (Open Shortest Path First)
 - IS-IS (Intermediate System to Intermediate System)

Távolság-vektor protokollok: RIP

- Metrika: **hopszám**
- Lassan konvergál
 - RIP frissítés (advertisement): 30s-ként, max 25 alhálózatról az AS-en belül
 - 180s után törlődik a bejegyzés: advertisement szomszédoknak
 - soft state protokoll
- Nem skálázódik jól: **nincs hierarchia**
- **Hopszám limit** korlátozza a hálózat méretét
 - max 15
- Végtelenig számolás ellen: **split horizon + route poisoning + holddown timer**
- De könnyen konfigurálható

RIP: példa



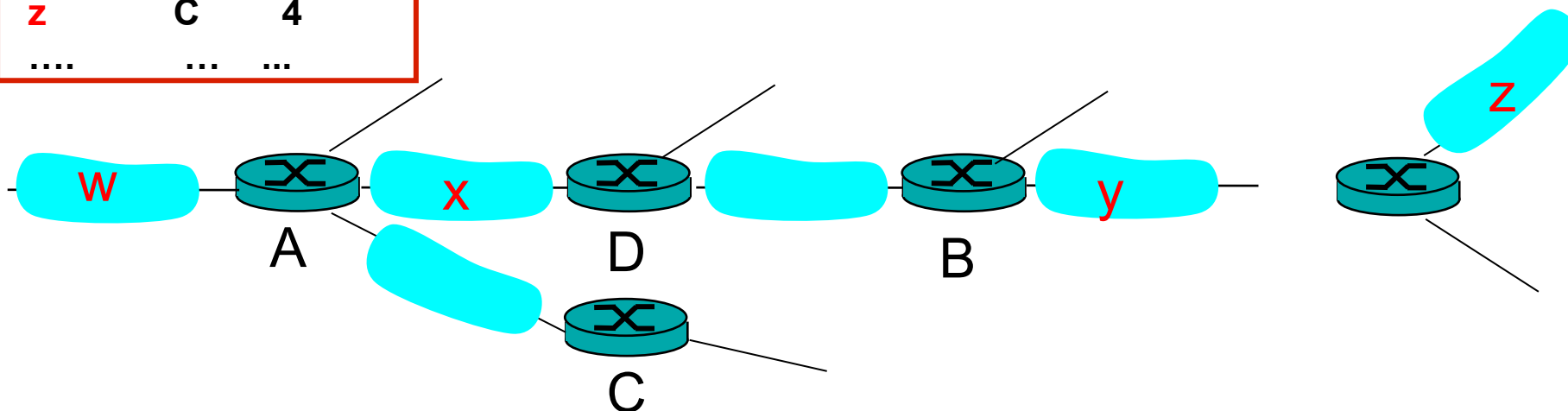
Célhálózat	Következő router	Hopszám a célig
w	A	2
y	B	2
z	B	7
x	--	1
....		

Útválasztó tábla D-ben

RIP: Példa

Cél	Köv.	Hopszám
w	-	1
x	-	1
z	C	4
....	...	...

Adv. A-tól D-nek



Célhálózat	Következő router	Hopszám a célig
w	A	2
y	B	2
z	B A	7 5
x	--	1
....		

Útválasztó tábla D-ben

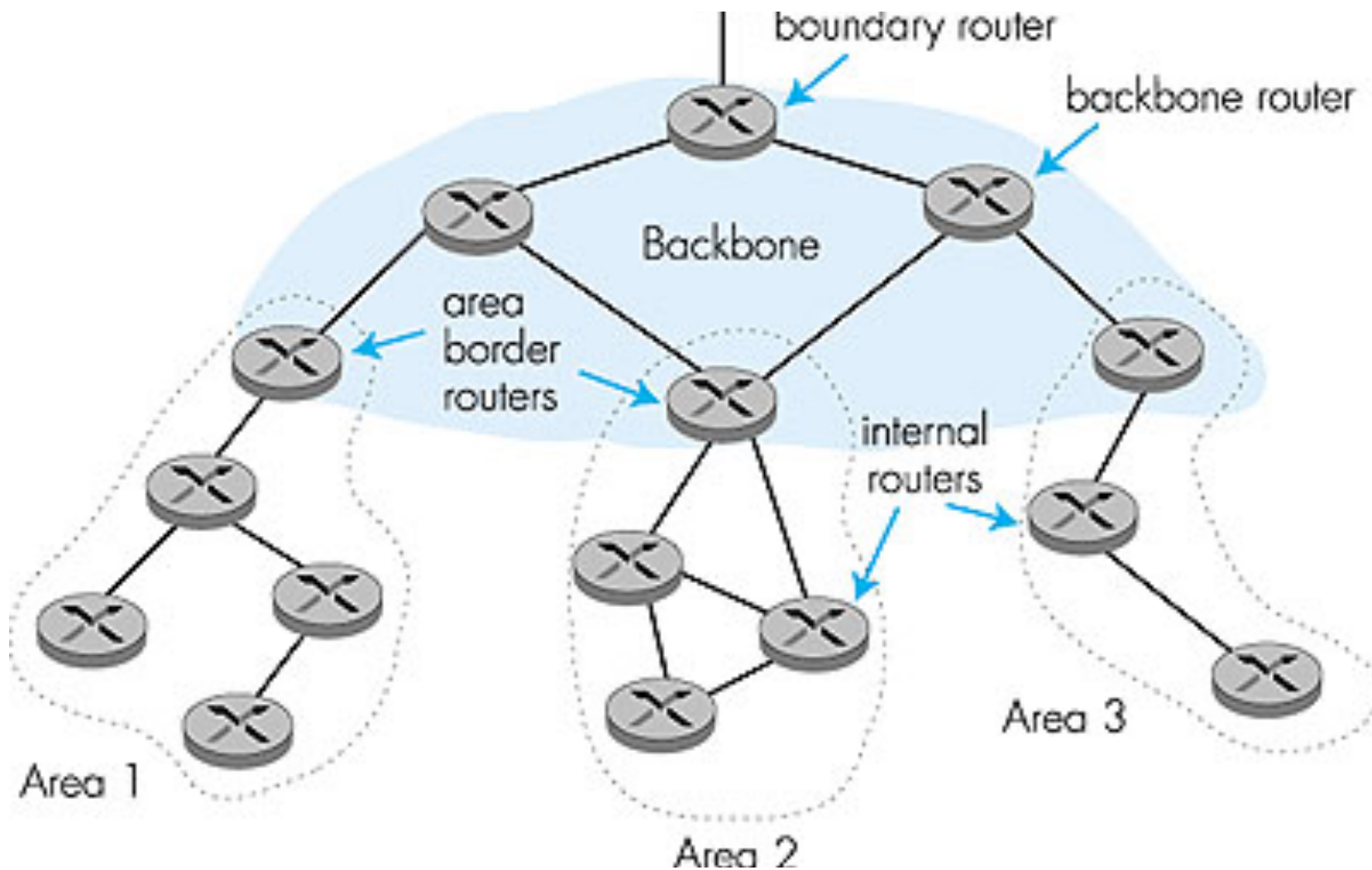
Távolság-vektor protokollok: EIGRP

- **IGRP:** Cisco specifikus
 - Javította RIP hibáit
 - Max 255 hop
 - **Többféle metrika** figyelembe vétele
 - Update: 90s
 - Már nem használják
- **EIGRP:** IGRP javítása - **Variable Length Subnet Mask** használata
 - Gyorsabb konvergencia
 - Hurokmentes működés
 - **5 metrika, de alapból csak 2 metrika kombinációja**
 - **minimális sávszélesség az útvonalon+útvonal késleltetése**

Összeköttetés-állapot protokollok: OSPF

- Link state database (LSDB) üzenetek **elárasztással**
 - ha változás van +periódikusan (30 percenként)
- Minden csomópontban **topológia térkép** (gráf)
- Ebből **legrövidebb útvonalú fa** Dijkstra algoritmussal, minden alhálózathoz
- **IP** üzenetekben (nincs UDP, mint pl. RIP-nél)
- Többféle metrika (admin állítja be)
- **Autentikált** OSPF üzenetek
- **Hierarchikus**: gerinc - routing tartományok, köztük határ routerek (AS-en belül)

Hierarchikus OSPF



OSPF vs. IS-IS

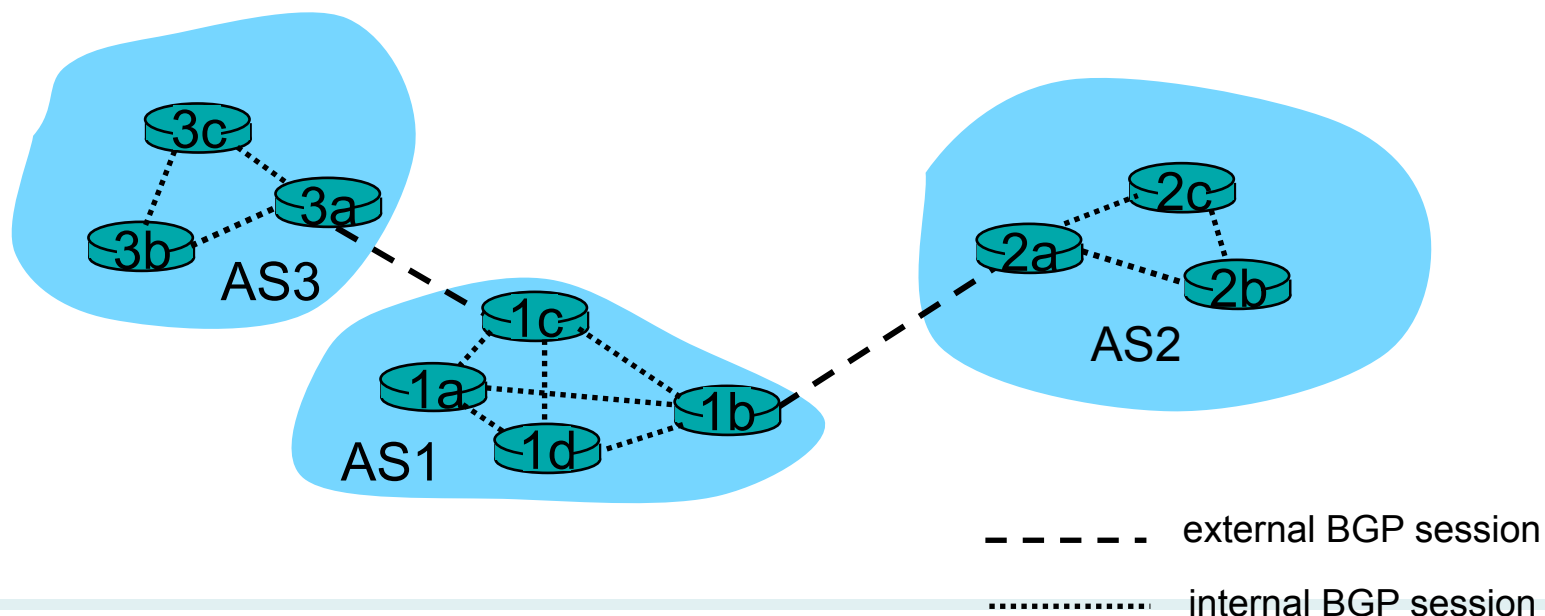
- OSPF (2-es verzió):
 - IPv4-re tervezték: népszerűbb
 - több fejlesztés, alkalmazás
 - Át kellett specifikálni IPv6-ra (OSPFv3)
 - Céges hálózatokban
- IS-IS:
 - OSI fejlesztés, nem IP csomagokban
 - Nagyobb kiterjedésű hálózatokra (ISP)
 - Több routert támogatott adott területen (már nem feltétlenül igaz ma)
 - Mivel nem IPv4 specifikus, könnyebb átállás IPv6-ra

Exterior Gateway Protocols (EGPs)

- Autonóm rendszerek (AS) között
- Példák:
 - EGP (Exterior Gateway Protocol)
 - Sokáig az Internet EGP-je, ma már nem használt
 - BGP (Border Gateway Protocol)
 - 1995-től használt EGP (BGPv4)
- Címaggregáció (supernet)
 - Kisebb routing táblák
 - Gyorsabb keresés
 - Gyorsabb terjesztés

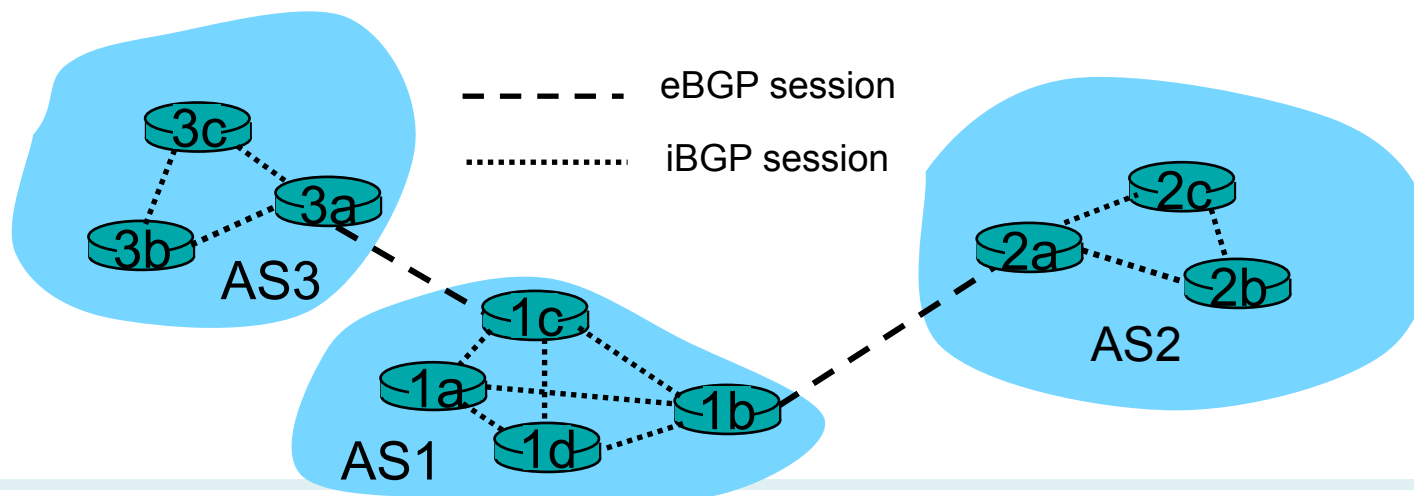
BGP alapok

- Routerek között (BGP peer-ek) TCP kapcsolatok: BGP session
- A hirdetett célpont: nem terminál, hanem **hálózati prefix** (CIDR-t használva)
- AS2 hálózati prefix-et hirdet AS1-nek: AS2 **megígéri**, hogy kézbesít minden a prefix-nek küldött csomagot
 - AS2 aggregálhatja a hálózati prefix-eket a hirdetésében



Az elérhetőségi infó terjesztése

- 3a és 1c közötti eBGP sessionön, AS3 prefix elérhetőségi infót küld AS1-nek.
 - 1c ezután iBGP-vel terjesztheti az új prefixet AS1 minden routerének
 - 1b újr hirdetheti az elérhetőségi infót AS2-nek 1b-2a eBGP sessionön
- Amikor a router új prefixet tanul, bejegyzi a routing táblájába

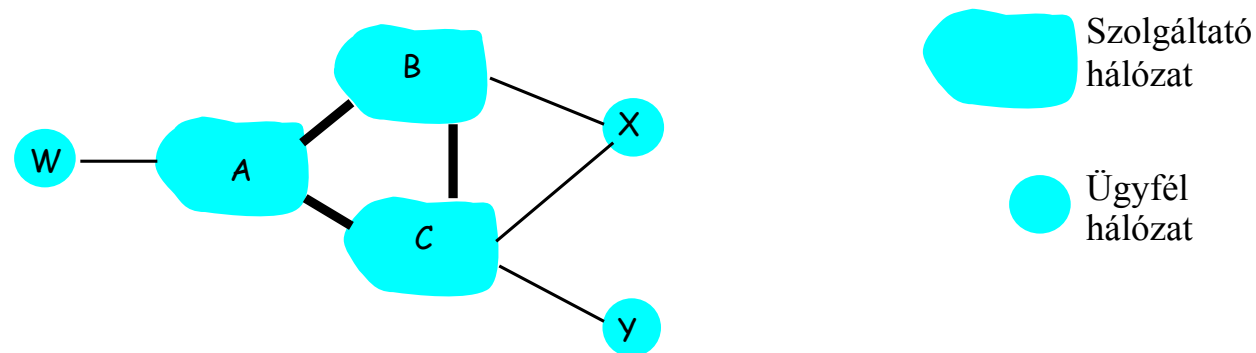


Útvonal attribútumok & BGP útvonalak

- prefix + attribútumok = útvonal (“route”) – *ezt hirdetik egymásnak*
- Két fontos attribútum:
 - **AS-PATH**: azon AS-ek sorozata, amelyeken áthaladt a prefix hirdetés: AS 67 AS 17
 - **NEXT-HOP**: a következő lépésbeli AS-hez vezető, AS-n belüli, router, tőle indul az AS-PATH
- Gateway router: **import policy** alapján dönti el, elfogadja-e az útvonalat.

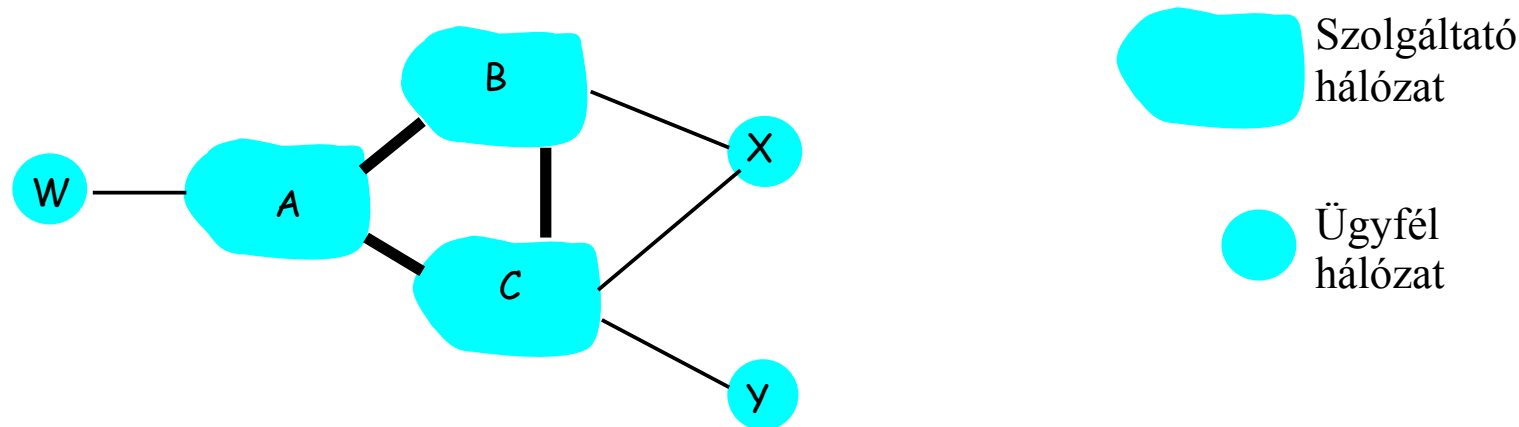
- Ha a router egynél több útvonalat kap egy prefix-hez: döntenie kell
- Döntési sorrend:
 1. Az útvonal helyi preferencia értéke: policy
 2. Legrövidebb AS-PATH
 3. Legközelebbi NEXT-HOP router: hot potato routing
 4. További szempontok

Példa: BGP policy (1)

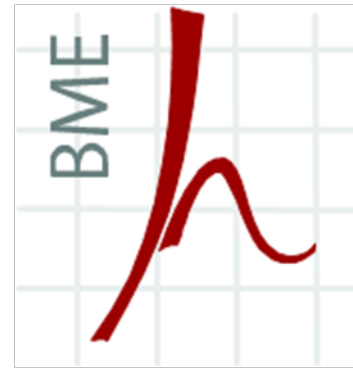


- A,B,C: szolgáltató hálózatok
- X,W,Y: ügyfél hálózatok
- Mind a 6 egy külön AS
- X: két szolgáltatóhoz csatlakozik
 - X nem akar forgalmat átvinni B-ből C-be saját magán keresztül
 - X nem hirdeti B-nek a C-hez vezető útvonalát

Példa: BGP policy (2)

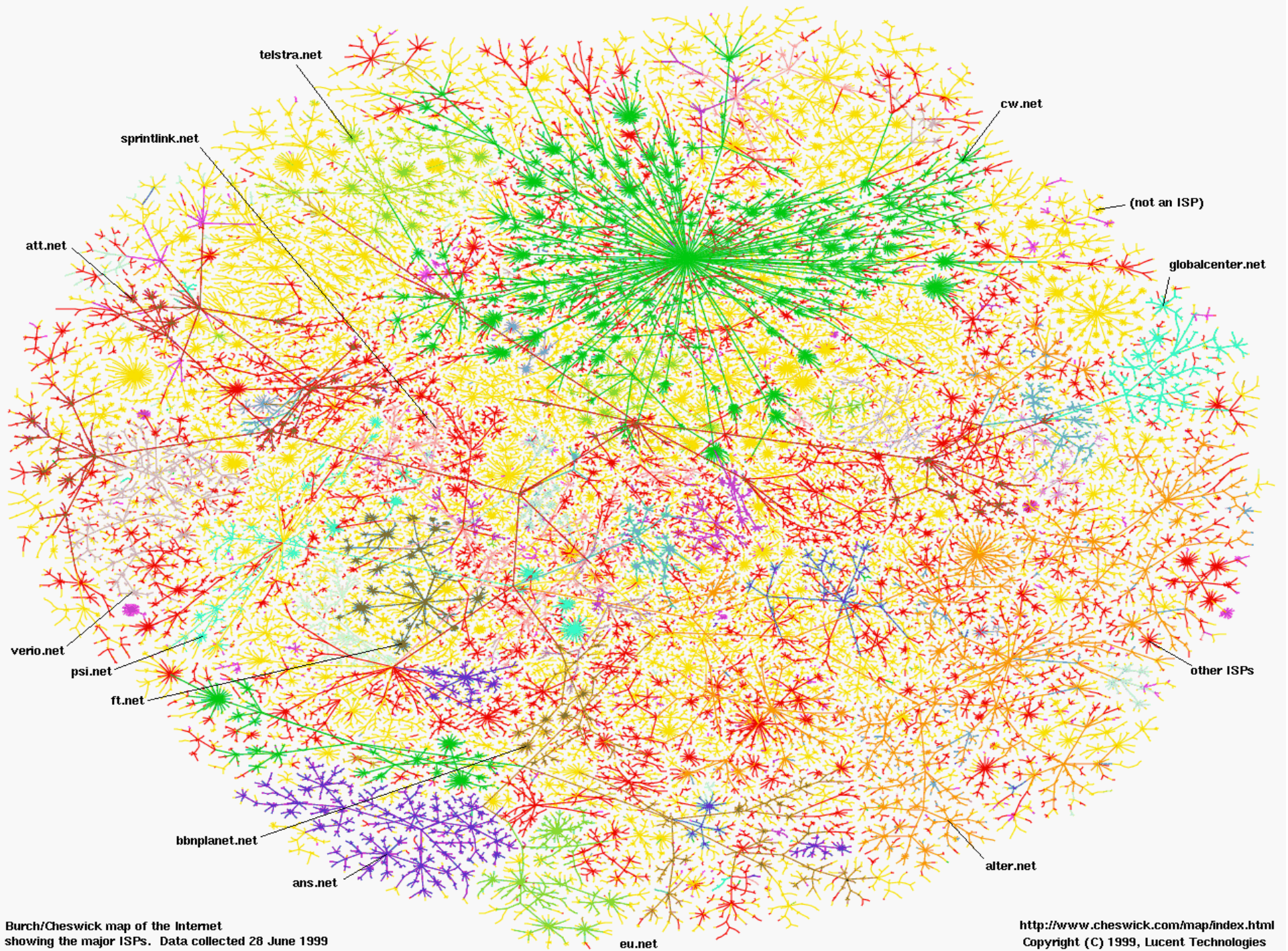


- ❑ A hirdeti B-nek az AW útvonalat
- ❑ B hirdeti X-nek a BAW útvonalat
- ❑ B hirdesse C-nek a BAW útvonalat?
 - Semmiképpen: B-nek nincs bevétele a CBAW-ből, mivel w és C nem B ügyfelei
 - B szeretné rákényszeríteni C-t, hogy A-n keresztül érje el w-t
 - B csak a saját ügyfeleit szolgálja ki



Hogyan néz ki az Internet?

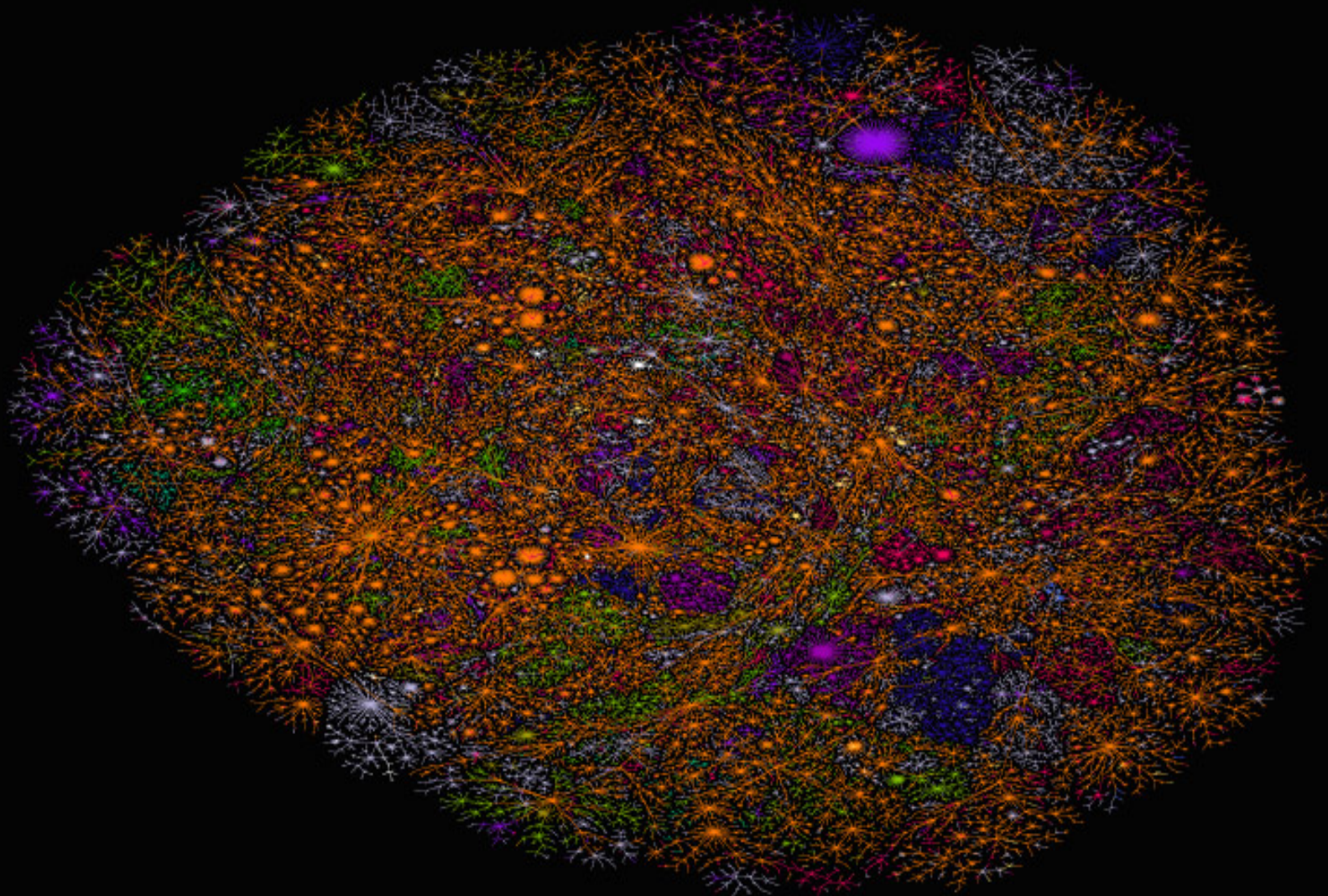
Valóban decentralizált?



Burch/Cheswick map of the Internet
showing the major ISPs. Data collected 28 June 1999

<http://www.cheswick.com/map/index.html>
Copyright (C) 1999, Lucent Technologies

The Internet: 2002



Graph by Irfan Ruth and 88 Others. Poster by Anne Rago and Gregory Rago.

Copyright © 2002 by COLUMBIA and Research Maps, Inc. 2002

North America Central America South America Africa South Africa Europe Germany France Netherlands United Kingdom Asia Japan Pacific Islands Australia New Zealand .mil .edu .gov .com .edu .org .net other

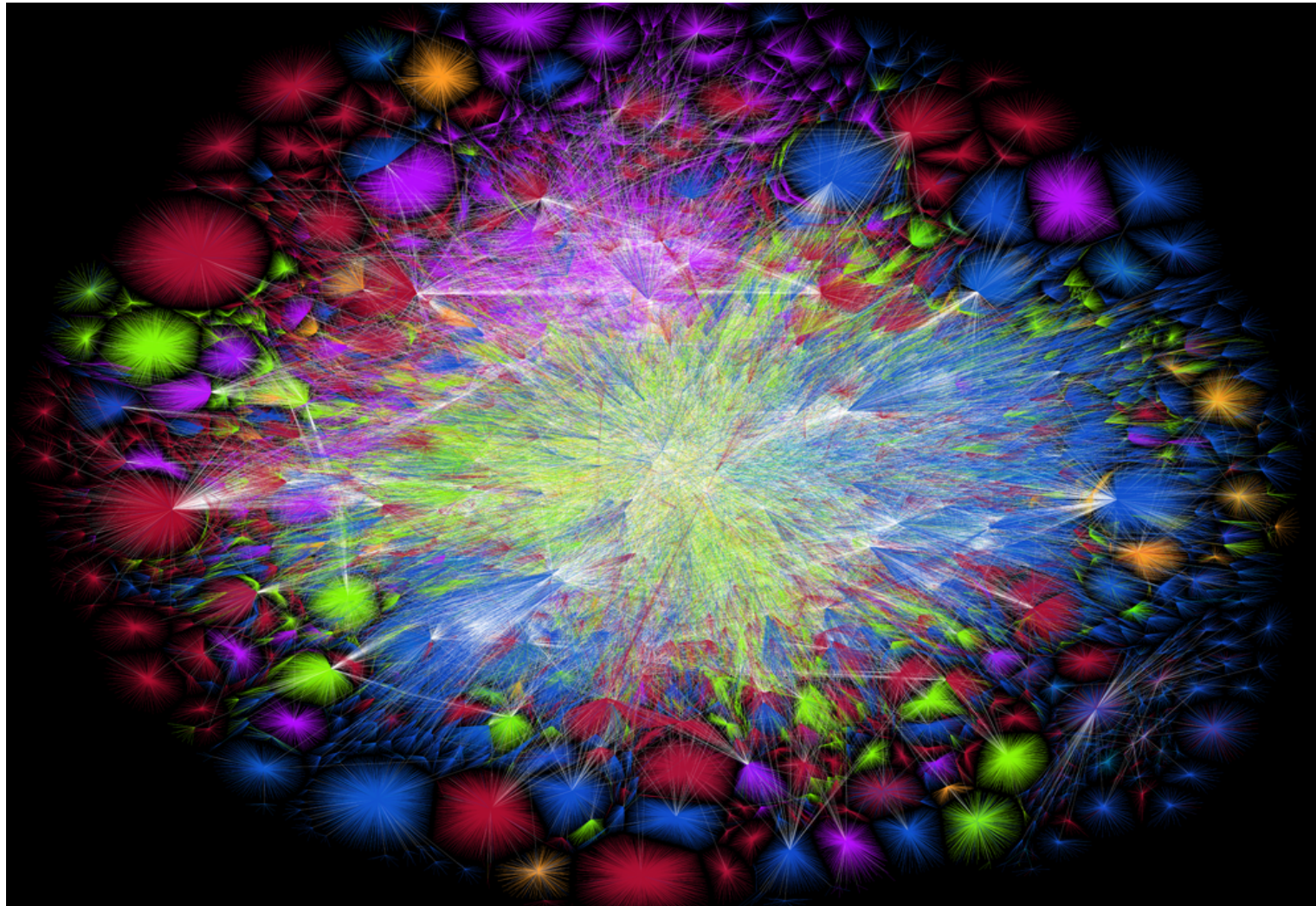
The graph of the Internet was created by plotting the shortest path between a centralized computer in Sumner, New Jersey and the 137,000 networks listed in the global Internet register of North America, Inc. and other authoritative routing sources. The data were collected on January 1, 2002.

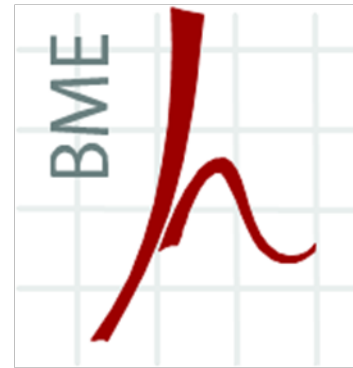
Published by
RESEARCH MAPS
www.researchmaps.com

Colors show the 100 top-level Internet domains where network switches (routers) are registered. 100 countries are included. Line length in routers; endpoints may show a router which is linked to a few computers or a "terminal" reflecting a large network.

Internet térkép 2015

Forrás: <http://www.opte.org/the-internet/>





IP - Tördelés

Darabolás és összeállítás

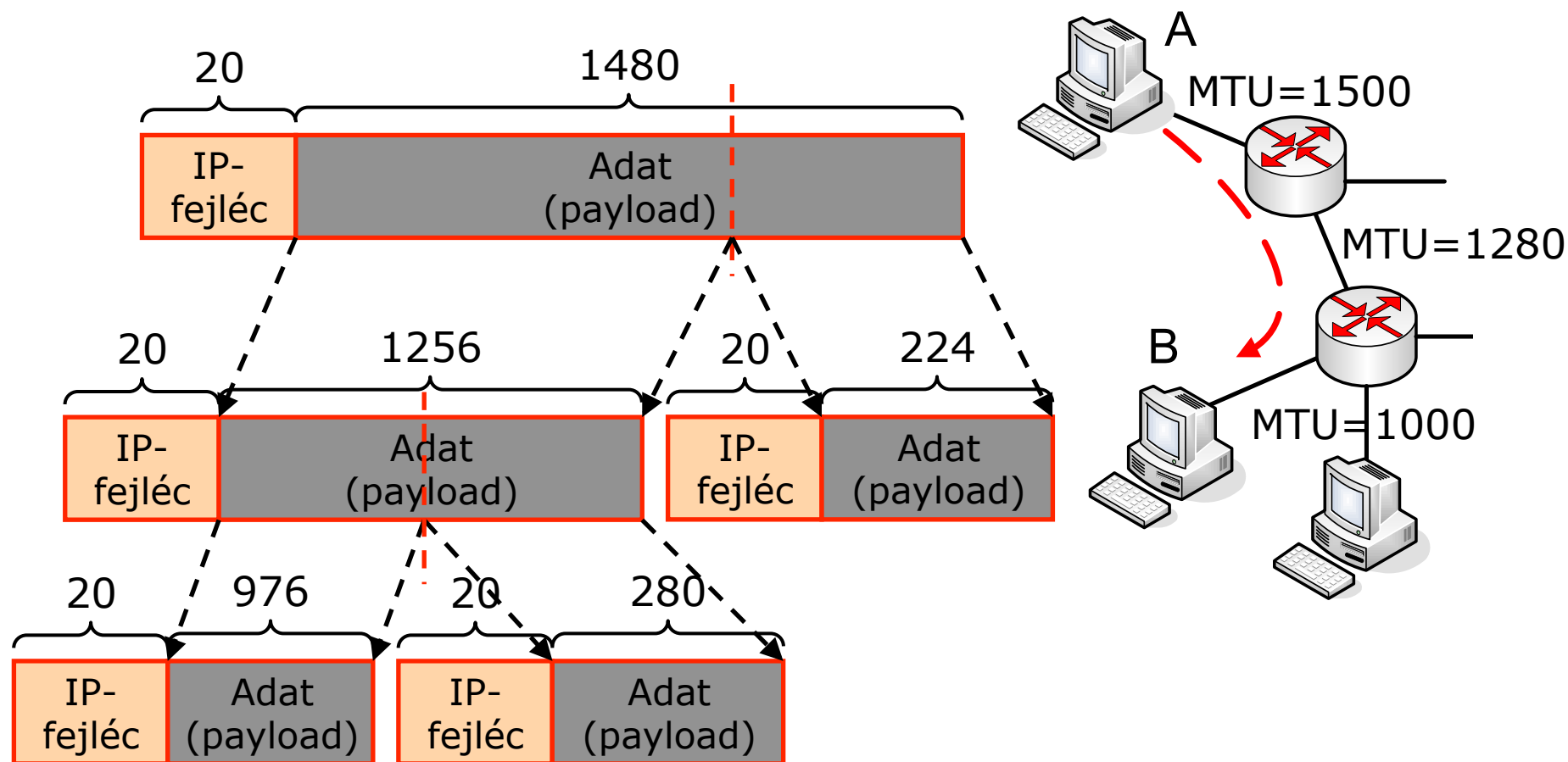
2017.október 25.

Tördelés szükségessége

- A hálózatok alsóbb rétegei meghatározzák a keret maximális méretét
 - Az adatkapcsolati réteg fej- és farokrészét leszámítva ez az **MTU (Maximum Transmission Unit)**
 - Ethernetnél pl. 1500 byte
- Eltérő technológiák $\Rightarrow$ eltérő MTU-jú kapcsolatok $\Rightarrow$ tördelni kell

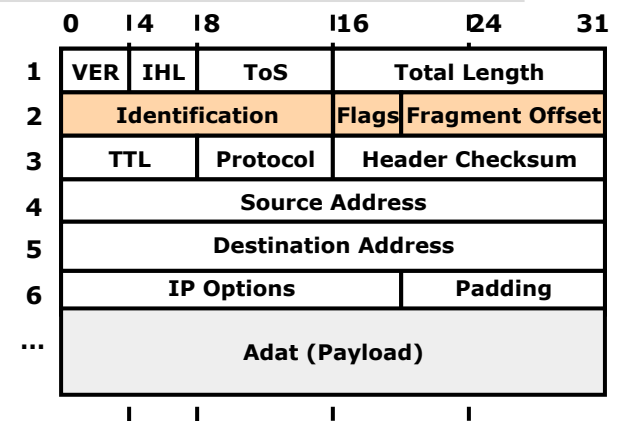
A tördelés menete

- Minden csomagnak kell fejléc (itt minimális fejléccel)!



Tördeléssel kapcsolatos mezők az IP-fejlécben

- Identification (16 bit)
 - Az IP-töredékek egyedi azonosítása
- Flags (3 bit)
 - 0: Fenntartott
 - 0-nak kell lennie
 - „Evil bit” (RFC 3514) (áprilisi tréfa 2003-ban)
 - 1: DF – Don't Fragment
 - 1: ha tördelni kellene, el kell dobni
 - Ezt használják az MTU (Maximum Transmission Unit) Path Discovery néhány TCP verzióban és az IPv6-ban
 - 2: MF – More Fragment
 - 1: ha nem az utolsó töredék
 - 0: utolsó töredék vagy nem tördelt csomag
- Fragment Offset (13 bit)
 - Az eredeti csomagban lévő kezdőpozícióját adja meg e töredékben lévő adatnak **8 bájtos egységekben**
 - $(2^{13}-1) \times 8 = 65528 > 65515$ bájt (max. adat)
(így a maximális méretű csomag is tördelhető)

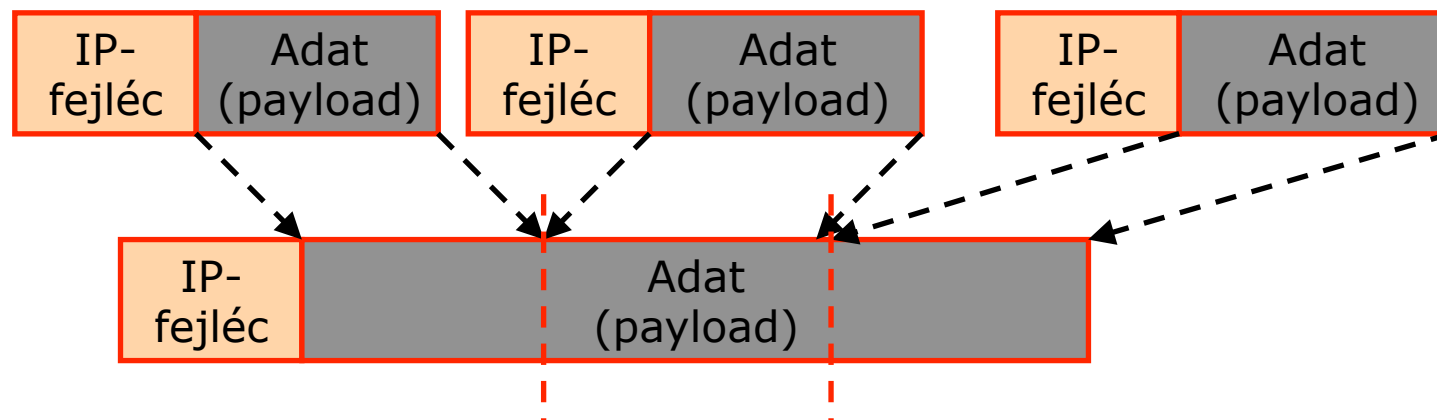


IP-fejléc változása tördelés közben

- Ha tördelés szükséges:
 - **Total Length** mezőt a töredék méretére állítani
 - Ha nem volt **Identification** mező érték, akkor generálni kell
 - Adat tördelése **8 bájtos egységekre**
 - A tördelésnek megfelelő **fragmentation offset**-et beállítani az új csomagokban
 - Minden csomagban az **MF bit**et 1-re kell állítani, kivéve annak a csomagnak az utolsó töredékénél
 - **Ellenőrző összeg** változása

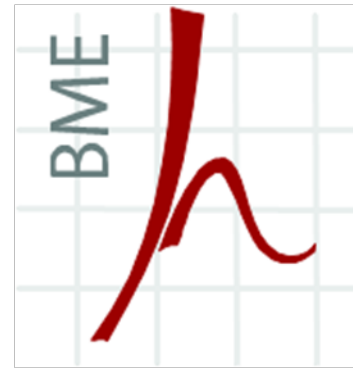
A töredékek összeállítása

- Csak a címzett végezheti el
 - Kivéve pl. NAT
- Ha valamely darab nem érkezik meg, akkor **a többi is eldobja**
- Csak teljesen összeállított csomagokat továbbít a felsőbb réteg felé
- A „fragment offset”-ekből a töredék helye meghatározható



A router feladatai

- Hibás-e a csomag (fejléce)?
- Nekem címezték-e?
- Ismerem-e a címzett hálózatát?
- A TTL érték csökkentés után >0 ?
- Kell-e tördelni? Lehet-e tördelni?
- Kell-e visszajelzést küldeni?



ICMP és IGMP

Az IP jelzés- és menedzsmentüzenetei

- *ICMP: Internet Control Message Protocol*
- *IGMP: Internet Group Management Protocol*

ICMP - Internet Control Message Protocol

- Jelzés- és menedzsmentüzenetek
 - Visszajelzés a „best effort” hálózattól
- IP felett (0x01-es protokollazonosító)
- Üzenettípusok
 - Hibaüzenetek
 - Kérdések
 - Válaszok
- Gyakran használt ICMP üzenetek:
 - Echo request – Echo reply ⇒ **Ping (RTT)**
 - Echo request – Echo reply + TTL ⇒ **Traceroute**

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

ICMP csomag és fejléce

- IP csomagba ágyazva, IPv4 fejléc után következik a fejléce (8 byte)
- Így best-effort szolgáltatás, de **különleges elbánást** kap a feldolgozásnál
 - Kötelező értesíteni a forrás címet, amely okozta a hibaüzenet generálását
- Fejléc:
 - **Típuson** belül **kód**, pl. típus: *címzett elérhetetlen*, ezen belül kód:
 - *címzett hálózat/host/protokoll/port elérhetetlen*
 - *tördelésre van szükség*
 - *letiltott hálózat/host*
 - **Ellenőrzőösszeg** egész ICMP üzenetre
 - **Hibaüzenetnél**: a hibás üzenet fejléce és adatmezőjéből az első 8 byte

ICMP – Cél elérhetetlen

- Gyakran előforduló üzenet:
„Destination unreachable” (ICMP Message Type: 0x03)

Hibakódok:

0 = net unreachable
1 = host unreachable
2 = protocol unreachable
3 = port unreachable
4 = fragmentation needed and DF set
5 = source route failed
6 = destination network unknown
7 = destination host unknown
8 = source host isolated
9 = communication with destination network administratively prohibited
10 = communication with destination host administratively prohibited
11 = network unreachable for type of service
12 = host unreachable for type of service

- Először TTL=1, majd TTL=2 ...
- Sorban eldobják a routerek és ICMP üzenetet küldenek róla
 - Time Exceeded
- Megadja a csomópontok listáját, amelyeket érint a csomag a célig
- Nem mindig a realitást tükrözi a traceroute lista
- Alkalmazás:
 - Hibaelhárításra
 - Tűzfal felderítésre
 - Letöltésnél (mirror)
 - Penetráció tesztelésre
- Hackerek is szeretik☺

További érdekes ICMP üzenetek

- **Source Quench:** felszólítás a küldőnek a forgalma visszafogására
 - pl. routernek betelik a buffere és visszaszól a forrásnak
- **Redirect:** felszólítás a küldőnek másik útvonal használatára
- **Address Mask Request:** host lekéri a routertől az alhálózati maszkot

IGMP – Internet Group Management Protocol

- IP-t futtató csomópont-csoportok kezelésére
 - Pl. online streaming video, játékok
 - IP csomagokban
- Főként **multicast csoportok** kezelése
 - Csoportok lekérdezése
 - Csoporthoz csatlakozás
- A TTL értéke általában 1
(csak a **helyi hálózaton** érvényes)
- Csak IPv4-hez, IPv6 máshogy oldja meg

- Bevezetés
 - Az IP feladata és jellemzői
- IP címzés
 - Címosztályok
 - Speciális címek
- Az IP fejrész szerkezete
- Routing protokollok
- Routingtáblák, subnet mask
- Továbbítás
- Címfeloldás: ARP, RARP
- MTU, tördelés
- Segédprotokollok: ICMP, IGMP

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Dr. Simon Vilmos

docens

BME Hálózati Rendszerek és Szolgáltatások Tanszék

svilmos@hit.bme.hu