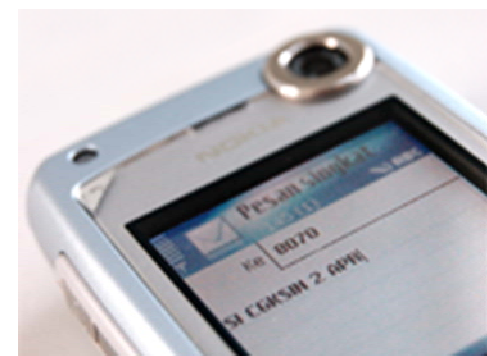
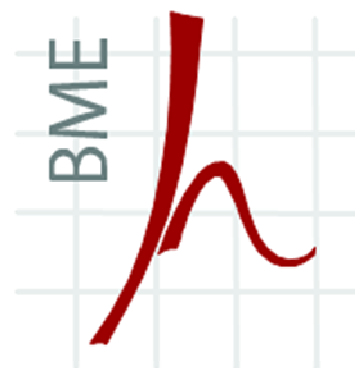
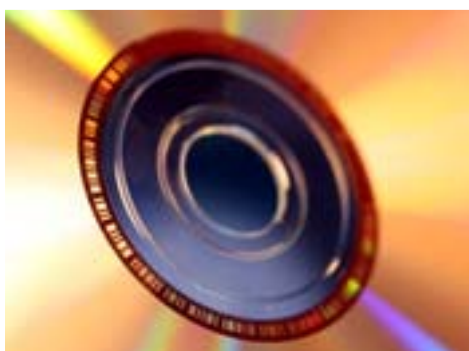




IP – Internet Protocol

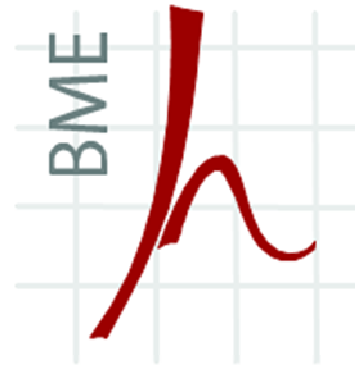
IP címzés, routing, IPv6, IP mobilitás

Dr. Simon Vilmos
adjunktus

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

2013.Április 4.

- Bevezetés
 - A TCP/IP protokollarchitektúra
 - Az IP feladata és jellemzői
- Címzés
- Az IP csomag szerkezete
- Routing
- IP segédprotokollok
- IPv6
- Mobil IP megoldások

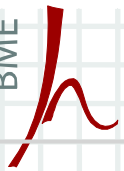


IP – Bevezetés

Az IP, mint hálózati protokoll

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!



TCP/IP architektúra és az ISO/OSI rétegmodell

ISO/OSI

Alkalmazás
Megjelenítési
Viszony
Szállítási
Hálózati
Adatkapcsolati
Fizikai

TCP/IP

Alkalmazás
Szállítási / Host-to-host (TCP/UDP/...)
Internet (IP)
Hálózati interface/ Hálózati hozzáférési

Gyakorlati

Alkalmazás
TCP/UDP/...
IP
LLC
MAC
PCS & PMA
PMD

IP: Internet Protocol

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

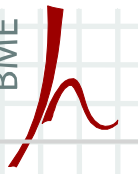
LLC: Logical Link Control

MAC: Medium Access Control

PCS: Physical Coding Sublayer

PMA: Physical Medium Attachment

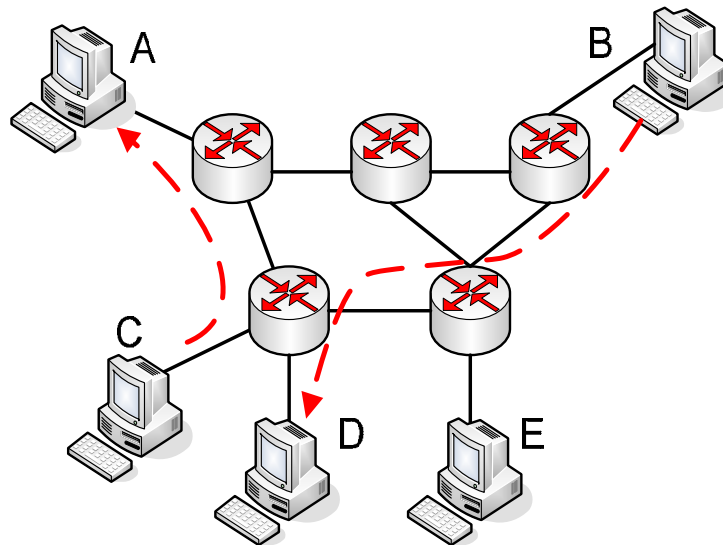
PMD: Physical Medium Dependent



ISO OSI vs. IETF

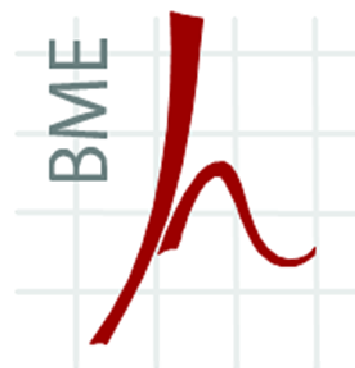
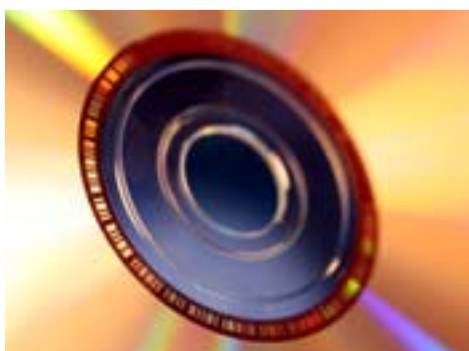
- OSI 7 rétegét a gyakorlatban nem szokták megvalósítani
- IETF szerint: Internet protokolljainak és architektúrájának fejlesztése továbbra sem lesz OSI alapú!
- Nálunk: 5 réteg, TCP/IP modell használata, de
 - interface réteg= adatkapcsolati réteg + fizikai réteg

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



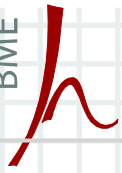
Az IP jellemzői

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



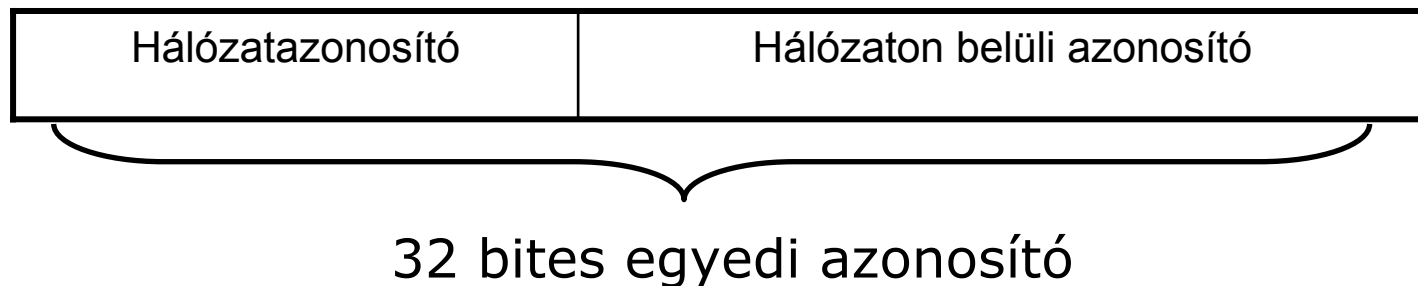
IP – Címzés

IP-címek és címosztályok



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



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

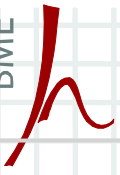
Osztály	Hálózatazonosító bitjeinek száma*	Hálózatok száma*	Hálózaton belüli címek száma*
A	8	126	16777214
B	16	16382	65534
C	24	2097150	254

- Az IP-címeket kezelő szervezet (IANA: Internet Assigned Numbers Authority) osztja ki
- Alatta 5 Regional Internet registry
 - A és B osztályú címet kaphatnak tipikusan:
 - Országok
 - Internet-szolgáltatók (ISP: Internet Service Provider)
 - Egyetemek

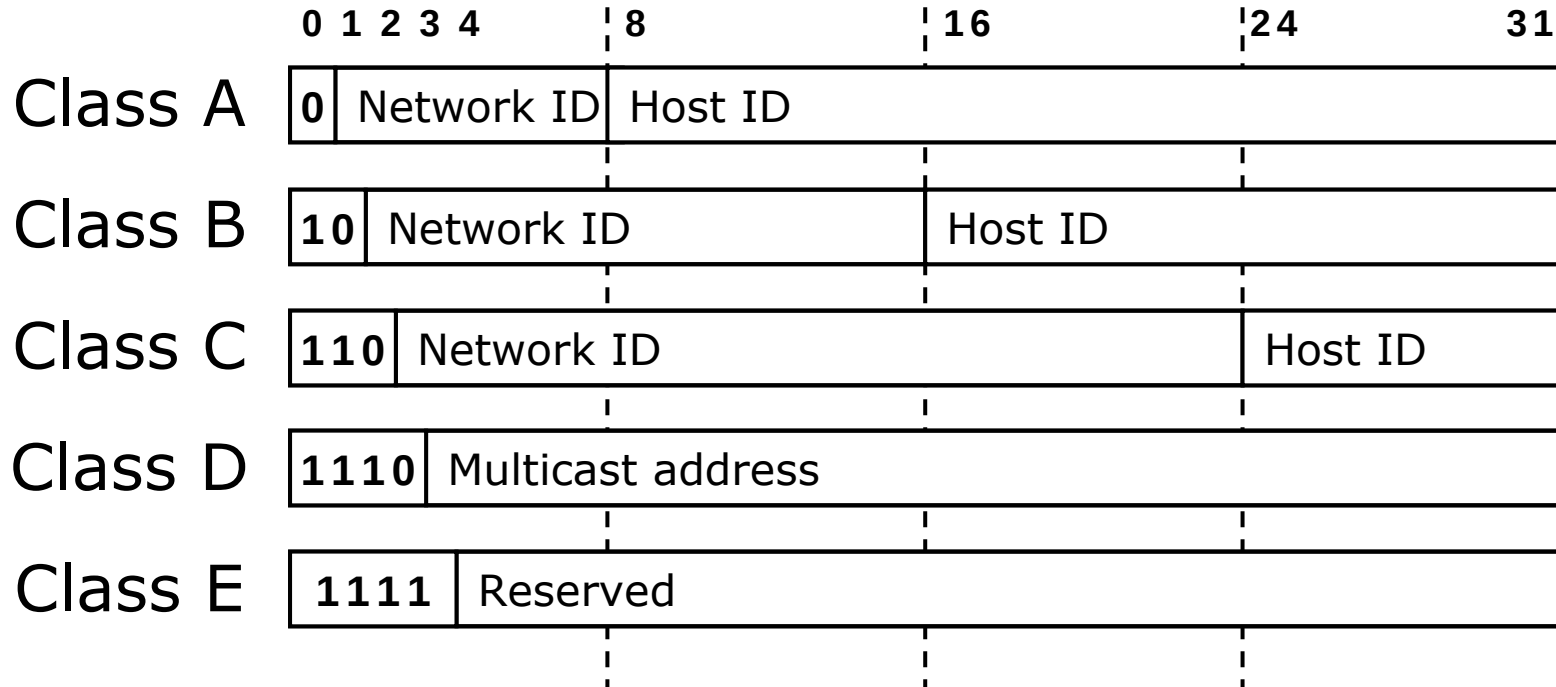
- A, B és C osztályú címek
 - Egyedi címzésre (unicast)

- D osztály
 - Többes címzésre (multicast) (később részletesen)
 - 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

- 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 cím
 - A helyi gépet azonosítja: localhost
 - Pl. vonaltesztelésre

Problémák a címosztályokkal

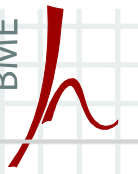
- Egyes nagy cégeknek, egyetemeknek *A* osztályú címek, amit nem használtak ki (16 millió cím)
 - *B* kicsi lett volna nekik
- Ugyanez középcégeknek: *C* túl kicsi, *B* túl nagy
- Gond a routing aggregációval
- Nem skálázható az osztályokon alapuló rendszer!

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)

Gondok privát címtartománnyal

- Késleltette az IPv6 bevezetését
- Megsérti a végpont-végpont konnektivitás elvét
 - Sőt egyes Internet protollokra nem is működik
- Privát hálózatok egyesítése: címduplikáció
 - Újracímezés
 - NAT közöttük
- Privát címek kiszivárgása az Internetre
 - Rosszul konfigurált privát hálózat
 - Komoly terhelés a névszervereknek
 - Blackhole anycast névszerverek
 - Határ routerek szűrik



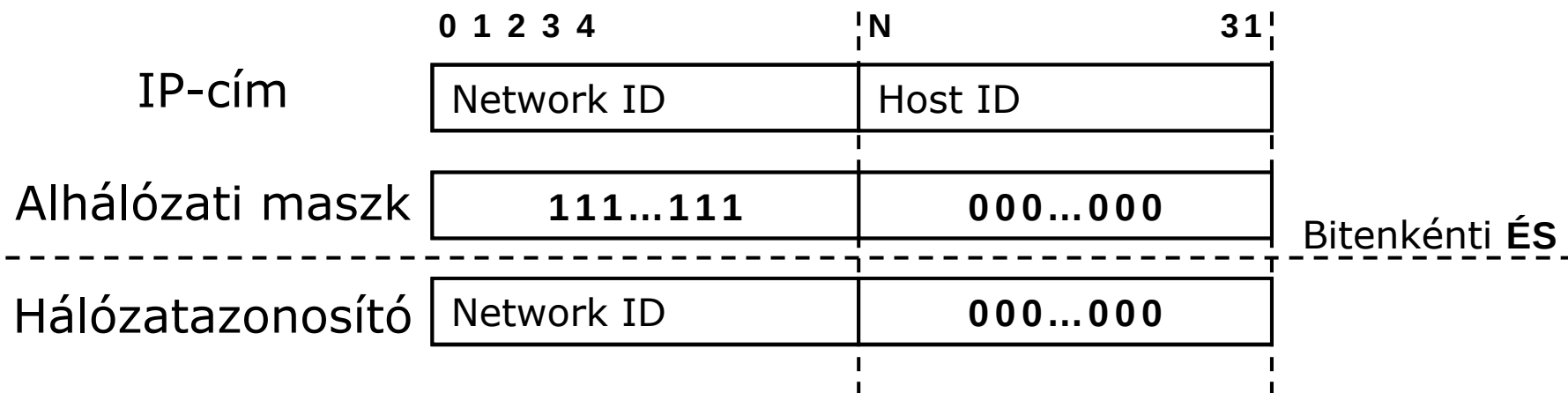
Példák: IP-címek

- Milyen IP-címek az alábbiak?
 - 152.66.115.35 (www.bme.hu)
 - Első bitjei: 10... $\Rightarrow$ B osztályú cím
 - Utolsó 16 bitje nem csupa 0 vagy 1 $\Rightarrow$ egyedi cím
 - 195.199.23.255
 - Első bitjei: 110... $\Rightarrow$ C osztályú cím
 - Utolsó 8 bitje csupa 1 $\Rightarrow$ broadcast cím
 - 10.97.15.255
 - Első bitje: 0... $\Rightarrow$ A osztályú cím
 - Utolsó 24 bitje nem csupa 0 vagy 1 $\Rightarrow$ egyedi cím
 - Privát címtartománybeli $\Rightarrow$ globálisan nem használható
- Mi legkisebb és legnagyobb C osztályú cím?
 - 11000000 00000000 00000000 00000000 $\Rightarrow$ 192.0.0.0
 - 11011111 11111111 11111111 11111111 $\Rightarrow$ 223.255.255.255

Címosztályok általánosítása

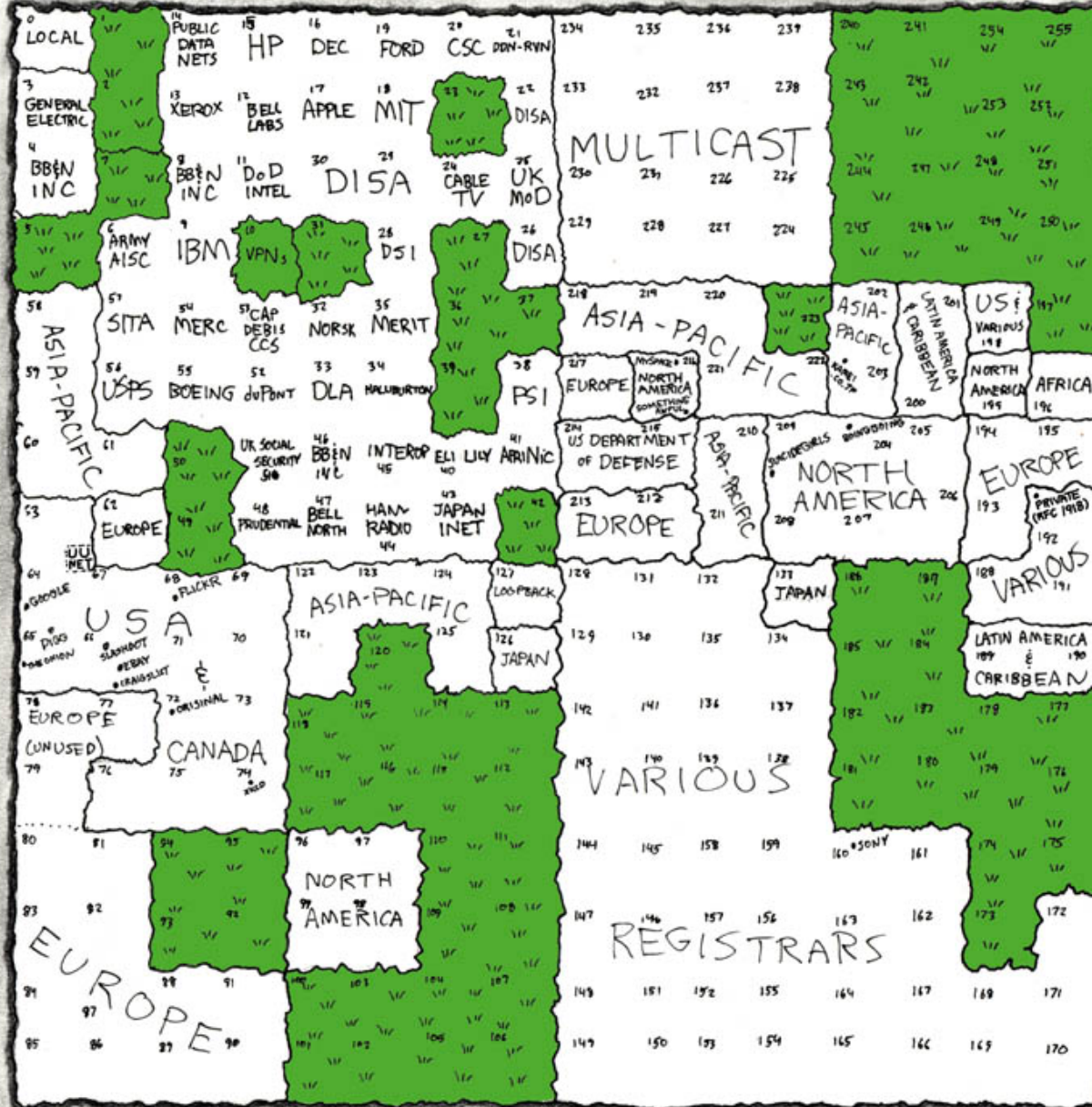
- Osztály alapú nem skálázható, plusz IPv4 címtartomány kimerülés
- **CIDR – Classless Inter-Domain Routing**
 - VLSM – Variable Length Subnet Mask
 - Osztályok eltörlése: a cím 32 bitje tetszőleges helyen lehet kettéosztva hálózat- és végponti azonosítóra
 - A címből nem lehet megállapítani, hol lett 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)



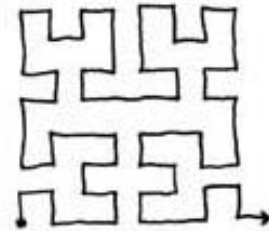
- Jelölés a hálózat egyértelmű azonosítására
 - <hálózat IP-címe> / <alhálózati maszk egyeseinek a száma>
 - Így pl. a BME hálózata: 152.66.0.0 /16
(alhálózati maszkja 255.255.0.0)
 - Hasonlóan:
 - A osztály: /8
 - B osztály: /16
 - C osztály: /24

MAP OF THE INTERNET



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.

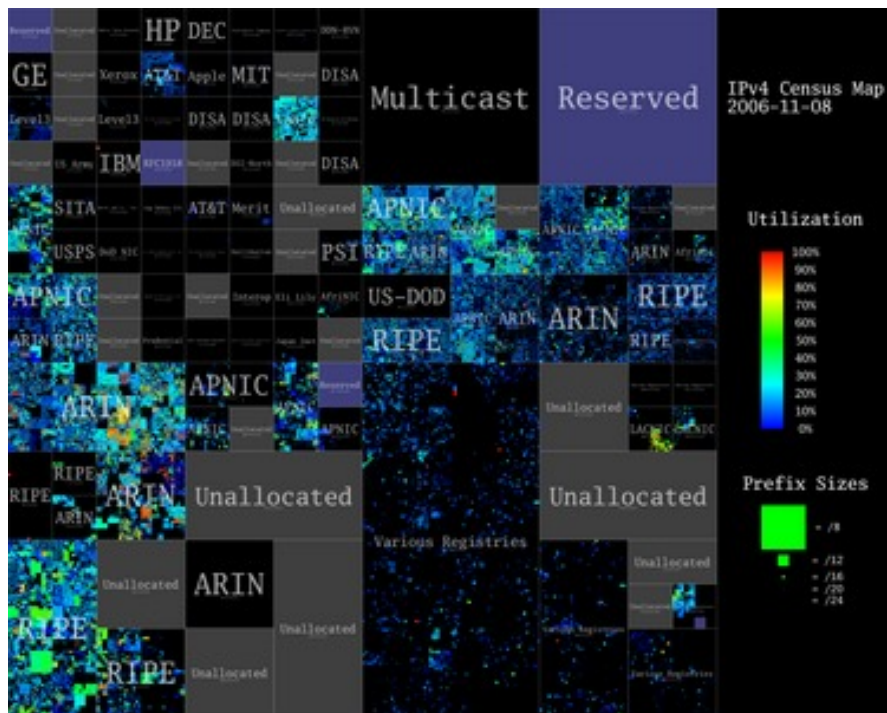
= UNALLOCATED
BLOCK



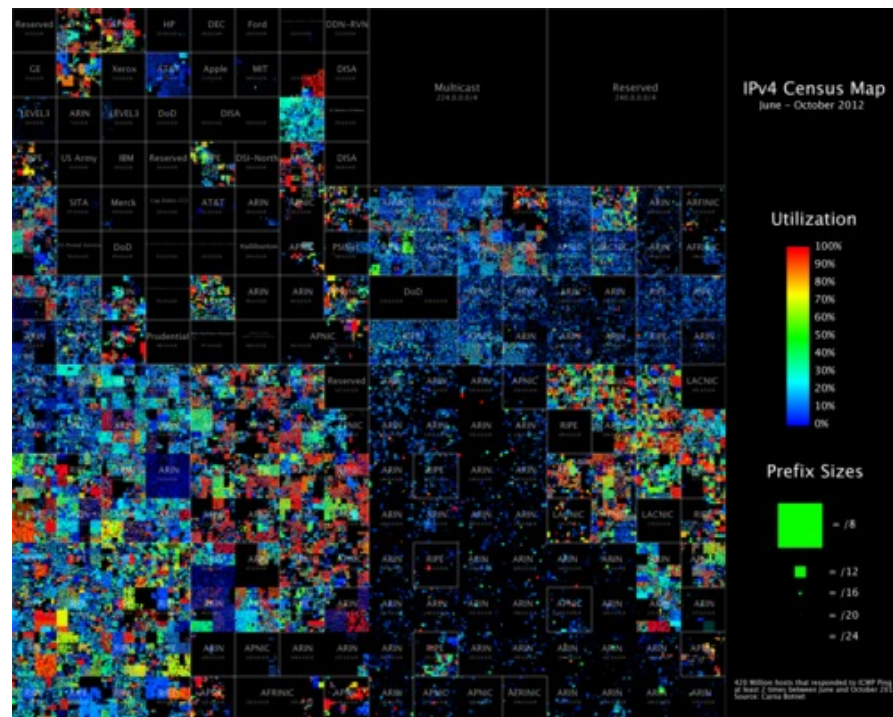
0	1	14	15	16	19	→
3	2	13	12	17	18	
4	7	8	11			
5	6	9	10			

IPv4 címtartomány kimerülése

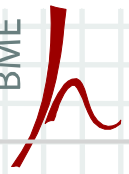
2006



2012

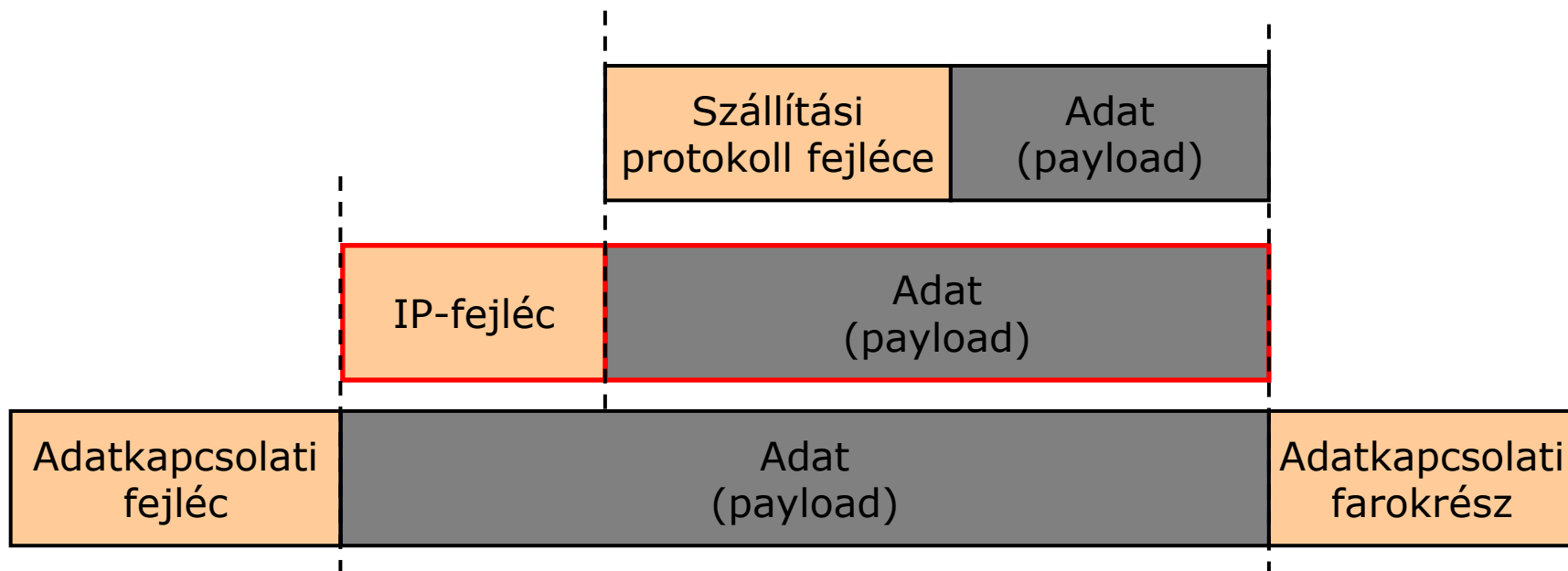


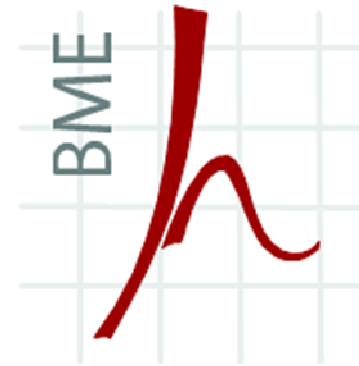
- Bevezetés
 - A TCP/IP protokollarchitektúra
 - Az IP feladata és jellemzői
- Címzés
- Az IP csomag szerkezete
- Routing
- IP segédprotokollok
- IPv6
- Mobil IP megoldások



Az IP-csomag szerkezete és „helye”

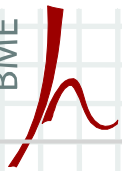
- Az IP-csomag két része:
 - IP-fejléc / fejrész (IP header)
 - Adat (payload)
- Az IP-csomag alsóbb rétegbeli protokoll adatrészébe ágyazódik be
- Az IP-csomag adatrészébe magasabb rétegbeli protokollüzenet (PDU) kerül



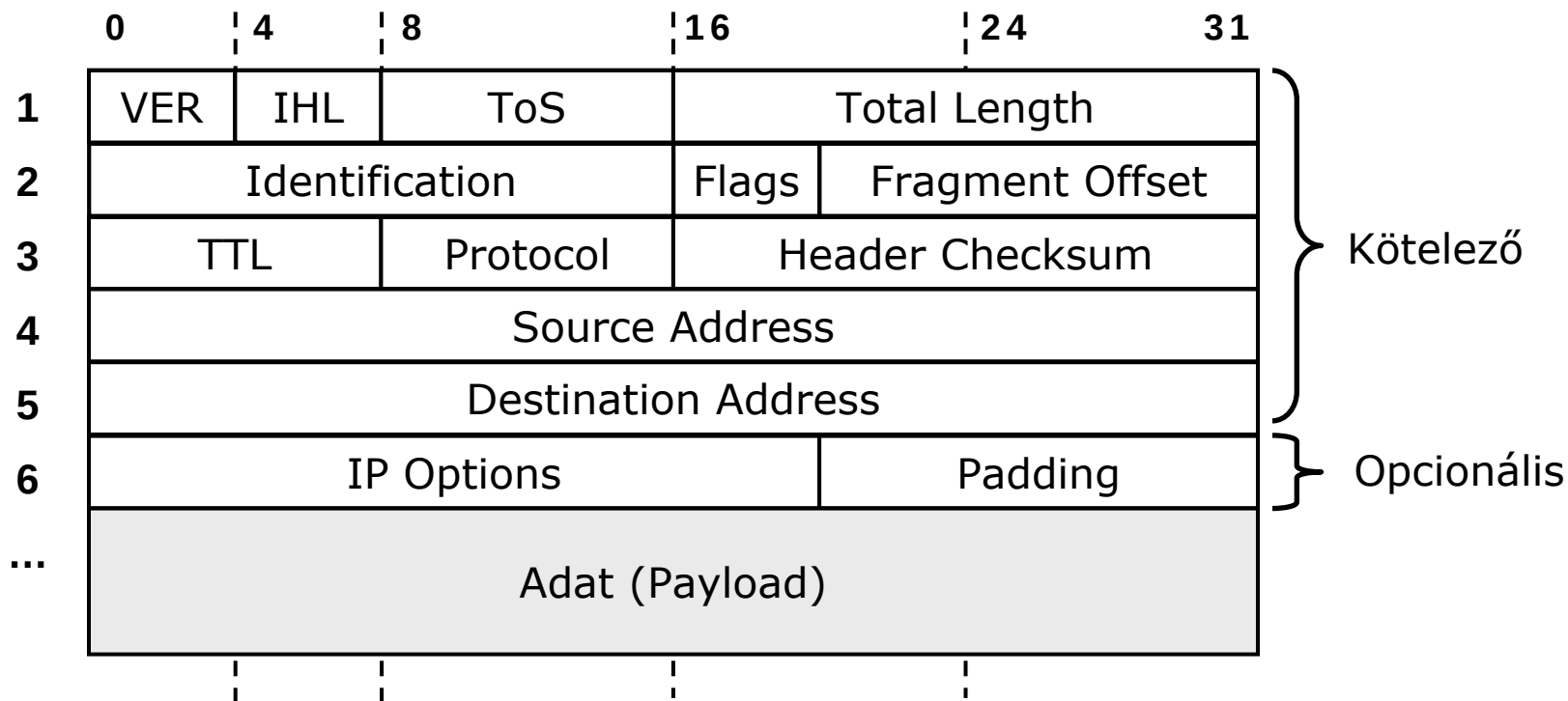


IP - Fejléc

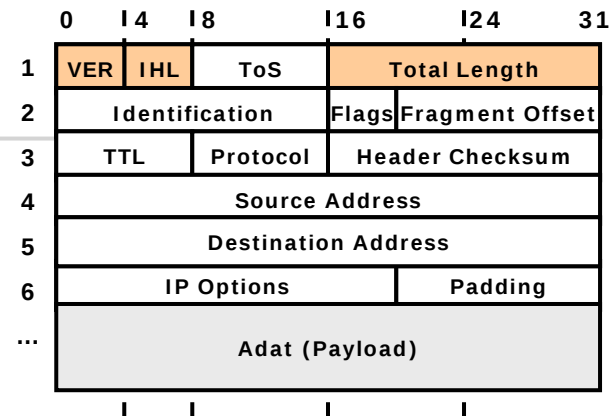
Az IP fejléc szerkezete



Az IP fejléc szerkezete



Az IP fejléc mezője I.



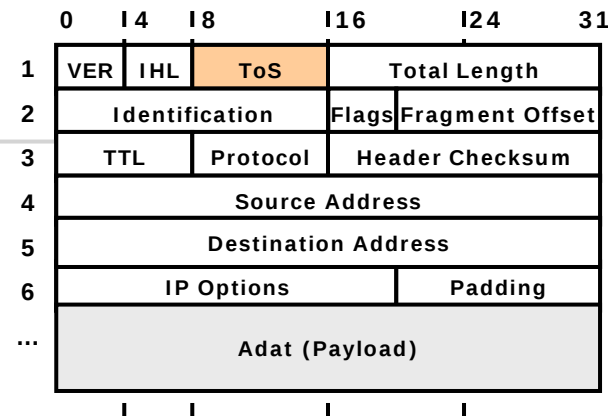
- VER – Version (4 bit)
 - Az Internet Protocol verziójának száma
 - Tipikus értéke: IPv4: 4, IPv6: 6
- IHL – Internet Header Length (4 bit)
 - Az IP fejléc mérete **32 bites szavakban**
 - Értéke:
 - Minimum: 5 (20 byte)
 - Maximum: $2^4-1=15$ (60 byte)
- Total Length (16 bit)
 - A teljes IP csomag 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.

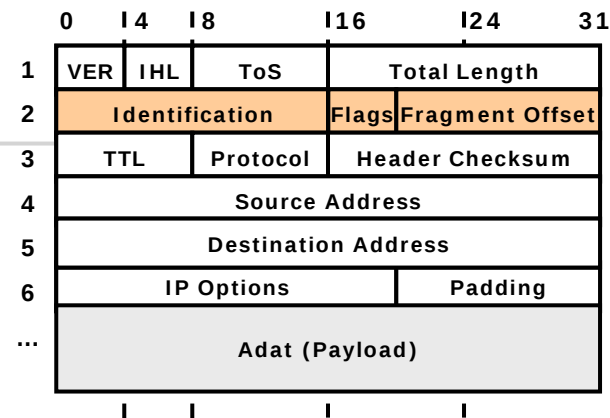
- ToS (Type of Service) (8 bit)
 - QoS osztályok, paraméterek jelzésére (RFC 791)

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
- Leggyakrabbi felhasználás:
 - DSCP – Differentiated Services Code Point (RFC 2474)- 6bit:
DiffServ (lesz róla szó később!)
 - ECN – Explicit Congestion Notification (RFC 3168)- 2bit

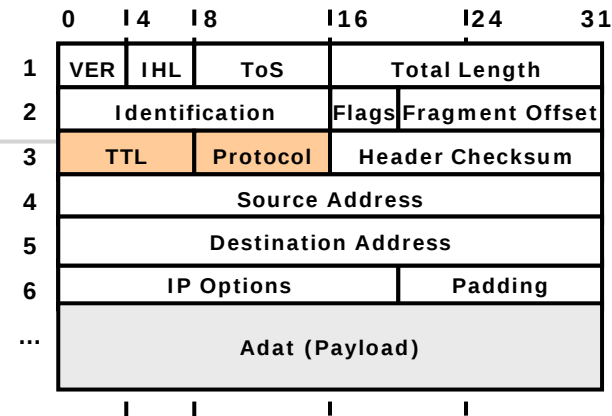


Az IP fejléc mezői III.



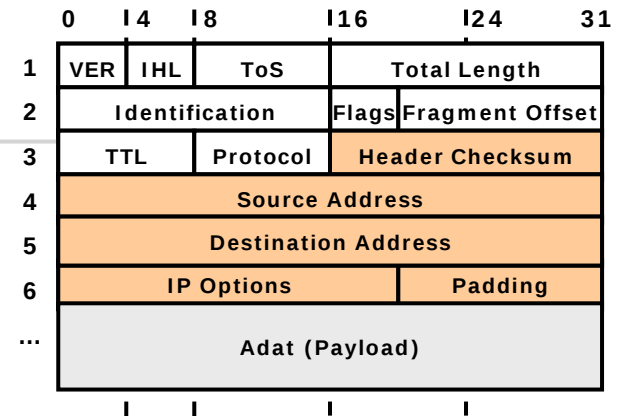
- **Identification (16 bit)**
 - Az IP-töredékek egyedi azonosítása
- **Flags (3 bit)**
 - 0: Fenntartott
 - 0-nak kell lennie
 - „Evil bit” (RFC 3514) (áprilisi tréfa 2003-ban)
 - 1: DF – Don’t Fragment
 - 1: ha tördelni kellene, el kell dobni
 - Ezt használják az MTU (Maximum Transmission Unit) Path 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)

Az IP fejléc mezői IV.

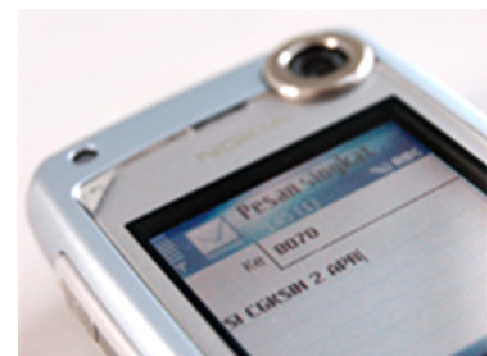
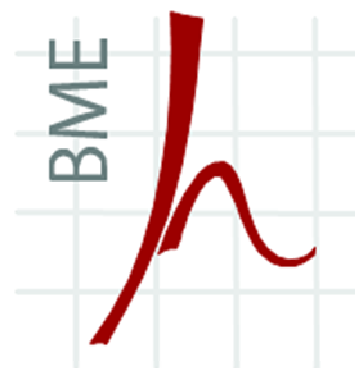
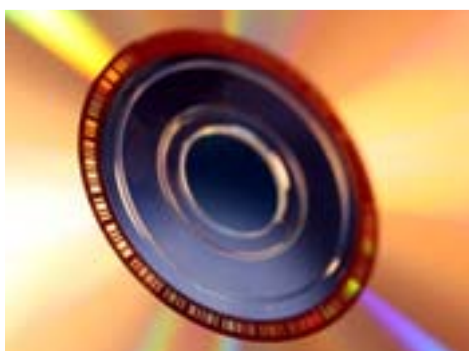


- **TTL – Time To Live (8 bit)**
 - Csomag élettartama
 - Eredetileg másodpercben
 - Gyakorlatban **hopszámban** mérve (hop count)
 - Minden továbbításnál csökkenteni kell ez értékét legalább 1-gyel
 - Ha a csökkentés után az értéke nem >0, akkor el kell dobni
- **Protocol (8 bit)**
 - Az adatrészben 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.



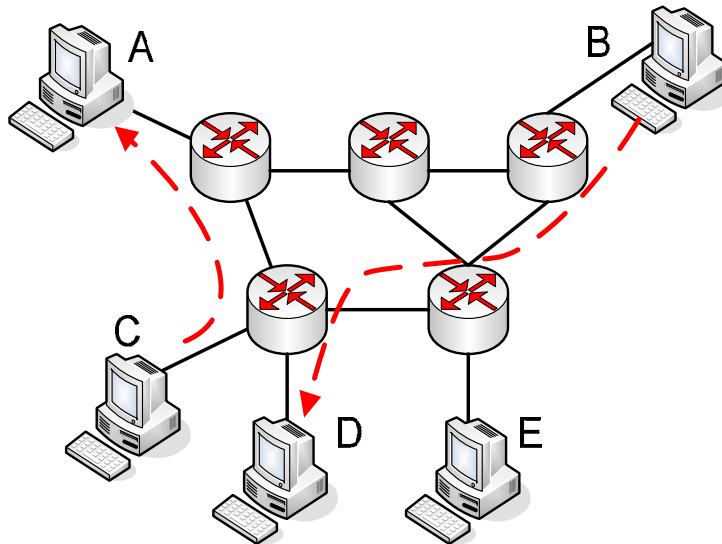
- **Header Checksum (16 bit)**
 - Az **IP fejléc** minden 16 bites szavának összegére számolt egyes komplementum
 - A csomag érkezésekor ellenőrizni kell a helyességét, és továbbítás esetén újra kell számítani
 - Új TTL minden lépésben, és fragmentáció is lehet
- **Source / Destination Address (2 x 32 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

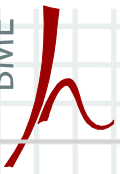


IP - Útvonalválasztás

Az IP routing működése

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

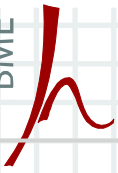




A csomagtovábbítás alapelve

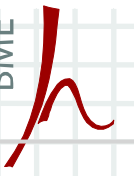
- Az IP jellemzői
 - Csomagkapcsolt
 - Összeköttetés-mentes (connectionless)
 - „Best effort” – nincs garancia
- **„Hot potato”-elv**
 - Minél gyorsabban továbbítsuk
 - Csak a következő csomópontot kell ismernünk (**hop-by-hop**)
 - Előnyei:
 - Kis erőforrásigény
 - Egyszerű, ezért gyorsan továbbítható
 - 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>

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

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 $\Rightarrow$ rosszul skálázódik
 - Általában bináris fával implementálják
 - $\Rightarrow$ n számú bejegyzésben lineáris keresés helyett csak a cím hosszában logaritmikus
- Keresés csak akkor, ha az nem saját cím

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
 - Átjáró: általában alkalmazás rétegbeli továbbító
 - Helyette inkább a router / útválasztó/ útvonalválasztó
- Nem feltétlenül van ilyen
 - Ha másra nem illeszkedik, akkor a célhálózat ismeretlen, így a csomagot eldobja
- 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!

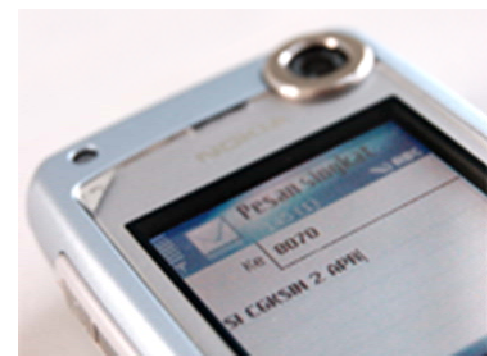
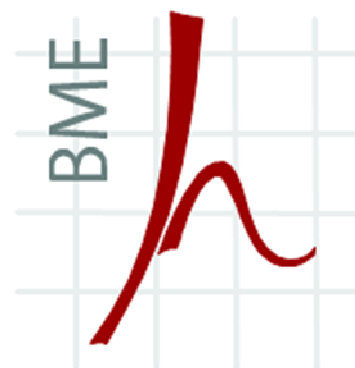
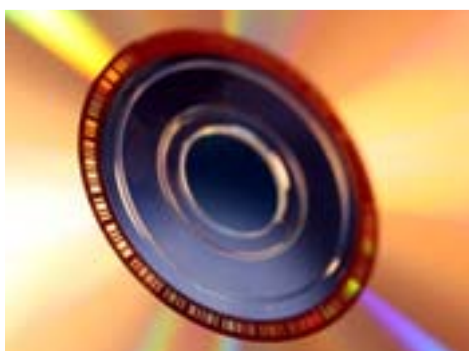
Megfelelő bejegyzés kiválasztva

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

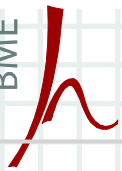
- Közvetlenül kapcsolódó (helyi) hálózat
 - A címzettnek közvetlenül küldeni
 - Ehhez a címzett **adatkapcsolati rétegbeli címére** van szükség
- Nem közvetlenül kapcsolódó (távoli hálózat)
 - Az útválasztónak kell küldeni
 - Az IP-címet tilos módosítani
 - Csak **adatkapcsolati rétegben** kell az útválasztónak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



IP – ARP/RARP

Kapcsolat az adatkapcsolati címek felé

- 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

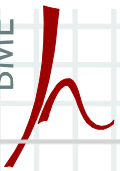
0 - 15 bits		16 - 31 bits
Hardware Type		Protocol Type
HLen (1 byte)	PLen (1 byte)	Operation
Sender HA (bytes 1 - 4)		
Sender HA (byte 5- 6)		Sender PA (byte 1 - 2)
Sender PA (byte 3 - 4)		Target HA (byte 1 -2)
Target HA (bytes 3 - 6)		
Target PA (bytes 1 - 4)		
RARP header structure		

- Hardware Type
 - Ethernet: 0x0001
- Protocol Type
 - IP: 0x8000
- HLen
 - Ethernet: 6 byte
 - TokenRing: 2 vagy 6 byte
 - FDDI: 2 vagy 6 byte
- PLen
 - IP: 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

- „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



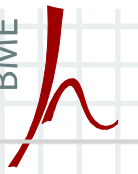
ARP egyéb alkalmazásai

■ 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

- 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)

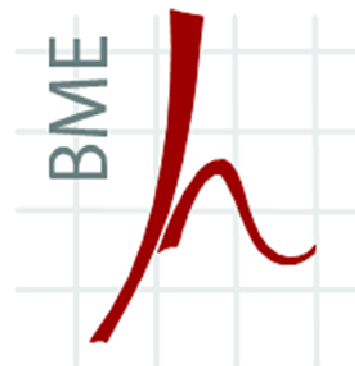


RARP – Reverse ARP

- Adatkapcsolati rétegbeli címből IP-címet
- Felhasználási terület
 - Hálózatmenedzsment
 - Permanens tár nélküli eszközök
 - Semmi ismeretük nincs a hálózatról
 - Hálózatról töltődik be az operációs rendszer
 - IP-cím nélküli kezdeti kommunikáció
- RARP kiszolgálók
 - RARP broadcast üzenetekre válaszolnak
- RARP helyett ma sokkal elterjedtebb megoldások
 - Bootstrap Protocol (BOOTP): hálózatról történő betöltésre
 - Dynamic Host Configuration Protocol (DHCP): IP-cím kérésére

Útválasztó tábla karbantartása

- Manuálisan
 - Minden hálózati operációs rendszer által támogatott
- Automatikusan
 - A tábla felépítéséhez szükséges információkat az útválasztók megosztják egymással
 - ⇒ útválasztó protokollok (routing protocols)



IP – Útvonalválasztó protokollok

Útvonalválasztó táblák építése automatikusan

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

- **Ad hoc** routing protokollok
 - Kis és gyorsan változó hálózatokra
 - Szenzor és egyéb vezeték nélküli hálózatokra

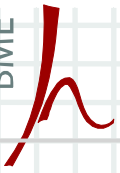
- **Interior Gateway Protocols (IGPs)**
 - Autonóm rendszereken (AS) belül
 - Kisebb hálózatokon

- **Exterior Gateway Protocols (EGPs)**
 - Autonóm rendszerek (AS) között
 - Az Internet routing protokollja

*

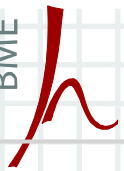
- Működési mód szerint
 - Proaktív
 - Folyamatosan karbantartott táblákkal
 - Reaktív
 - Igény szerinti célfelderítés
 - Hibrid
 - A fenti kettő együttes alkalmazása

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



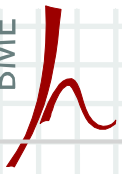
IGP routing: A „távolság-vektor” módszer

- A gyűjtött információ és a gyűjtés módja:
A csomópontok elmondják a **hálózatról alkotott elképzeléseiket** a **szomszédaiknak**
- Az „elképzelések”:
 - melyik csomópont milyen távol van
 - egy lista (vektor) melynek elemei
 - csomópont azonosító – távolság párok
- A távolság-vektorát közli mindegyik csomópont valamennyi szomszédjával



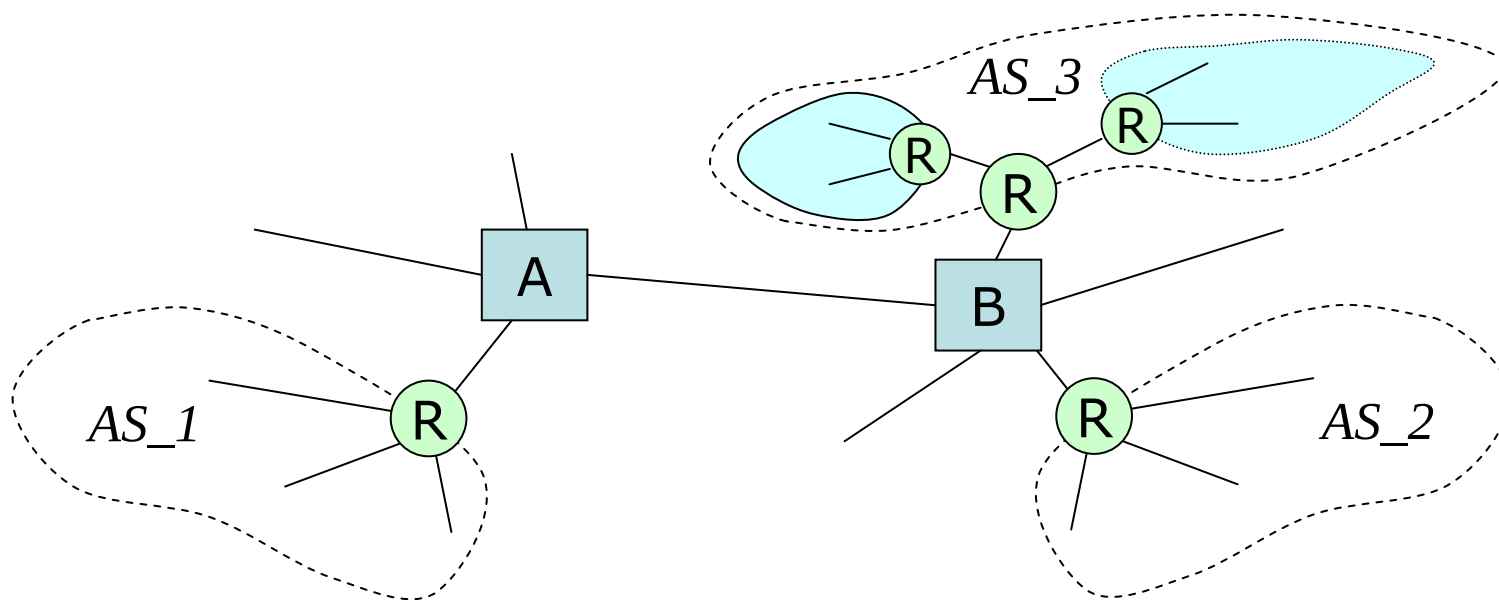
IGP routing: Az „összekötés-állapot” módszer

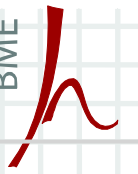
- A gyűjtött információ és a gyűjtés módja:
A csomópontok elmondják **mindenkinek** a **szomszédaikról** **nyert tapasztalataikat**
- A „tapasztalatok”:
 - a szomszédokhoz vezető linkek **aktuális állapota** (ez pontosan ismerhető)
- Az információ elküldése „mindenkinek” a korlátozott (felügyelt) *elárasztás*-sal:
 - elküldik a szomszédokhoz, akik továbbadják
 - **kivéve azon a linken, amelyen érkezett**



Autonóm rendszerek

- Egy autonóm rendszer a többi autonóm rendszer számára jelzi az általa képviselt csoporto(ka)t
- Az egész csoport egyetlen bejegyzés lesz az útvonal-táblában



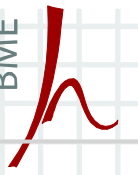


Interior Gateway Protocols (IGPs)

- 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)

- **RIP:** nem preferált
 - Lassan konvergál, nem skálázódik jól
 - Update: 30s
 - Hopszám limit korlátozza a hálózat méretét
 - Max 15
 - De könnyen konfigurálható
 - Metrika: hopszám
- **IGRP:** Cisco specifikus
 - Javította RIP hibáit
 - Max 255 hop
 - Többféle metrika figyelembe vétele
 - Már nem használják
- **EIGRP:** IGRP javítása (VLSM)
 - Gyorsabb konvergencia
 - Hurokmentes működés
 - 6 metrika kombinációja

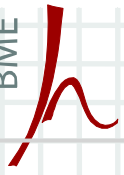
- Elterjedtebbek az összeköttetés-állapot módszerek
 - OSPF: nagy céges hálózatokban
 - Nagyon gyorsan konvergál
 - Többféle metrika
 - Hierarchikus: gerinc - routing tartományok, köztük határ routerek
 - IS-IS: nagy kiterjedésű ISP hálózatokban



OSPF vs. IS-IS

- OSPF (2-es verzió):
 - IPv4 forgalom irányítására tervezték: népszerűbb
 - több fejlesztés, alkalmazás
 - Át kellett specifikálni IPv6-ra (OSPFv3)

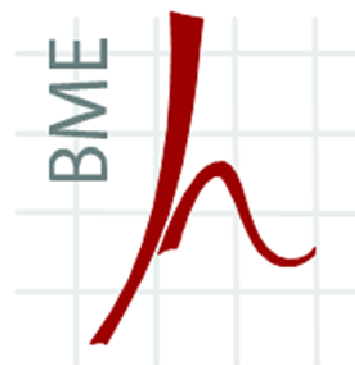
- IS-IS:
 - OSI fejlesztés, nem IP csomagokban
 - Nagyobb kiterjedésű hálózatokra (ISP)
 - Több routert támogat adott területen
 - Mivel nem IPv4 specifikus, könnyebb átállás IPv6-ra



Exterior Gateway Protocols (EGPs)

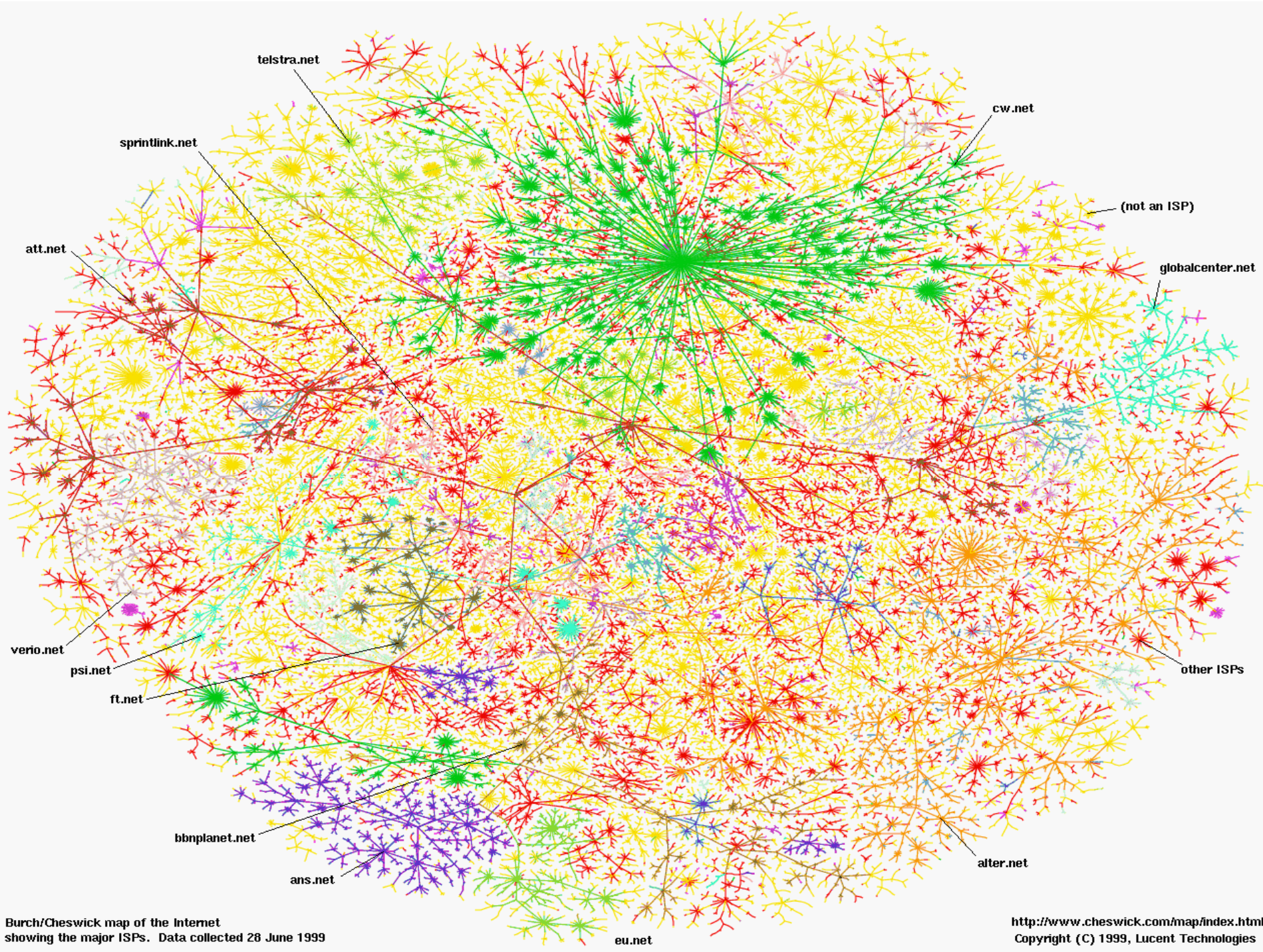
- Autonóm rendszerek (AS) között
- Példák:
 - EGP (Exterior Gateway Protocol)
 - Sokáig az Internet EGP-je, ma már nem használt
 - BGP (Border Gateway Protocol)
 - 1995-től használt EGP (BGPv4)
- Címaggregáció (supernet)
 - Gyorsabb keresés
 - Gyorsabb terjesztés

- **Path vector protocol (Útvonal-vektor protokoll)**
- Routing tábla bejegyzés:
 - Célhálózat
 - Következő router
 - **Útvonal a célhálózathoz**
- A **teljes útvonal** dinamikus nyilvántartása
 - AS határ routerek végzik: útvonal-vektor üzenetekkel (Path Vector Message) frissítés, hirdelve a többi AS elérhetőségét
 - **Útvonal-vektor üzenet:** **AS-ek sorozata a célhálózathoz**
 - Minden AS határ router fogadáskor megnézi megfelel-e a saját szabályainak
 - Ha igen, módosítja a routing tábláját és az útvonal-vektor üzenetet
 - Következő router: saját ID-je, illetve útvonal-vektorba AS száma

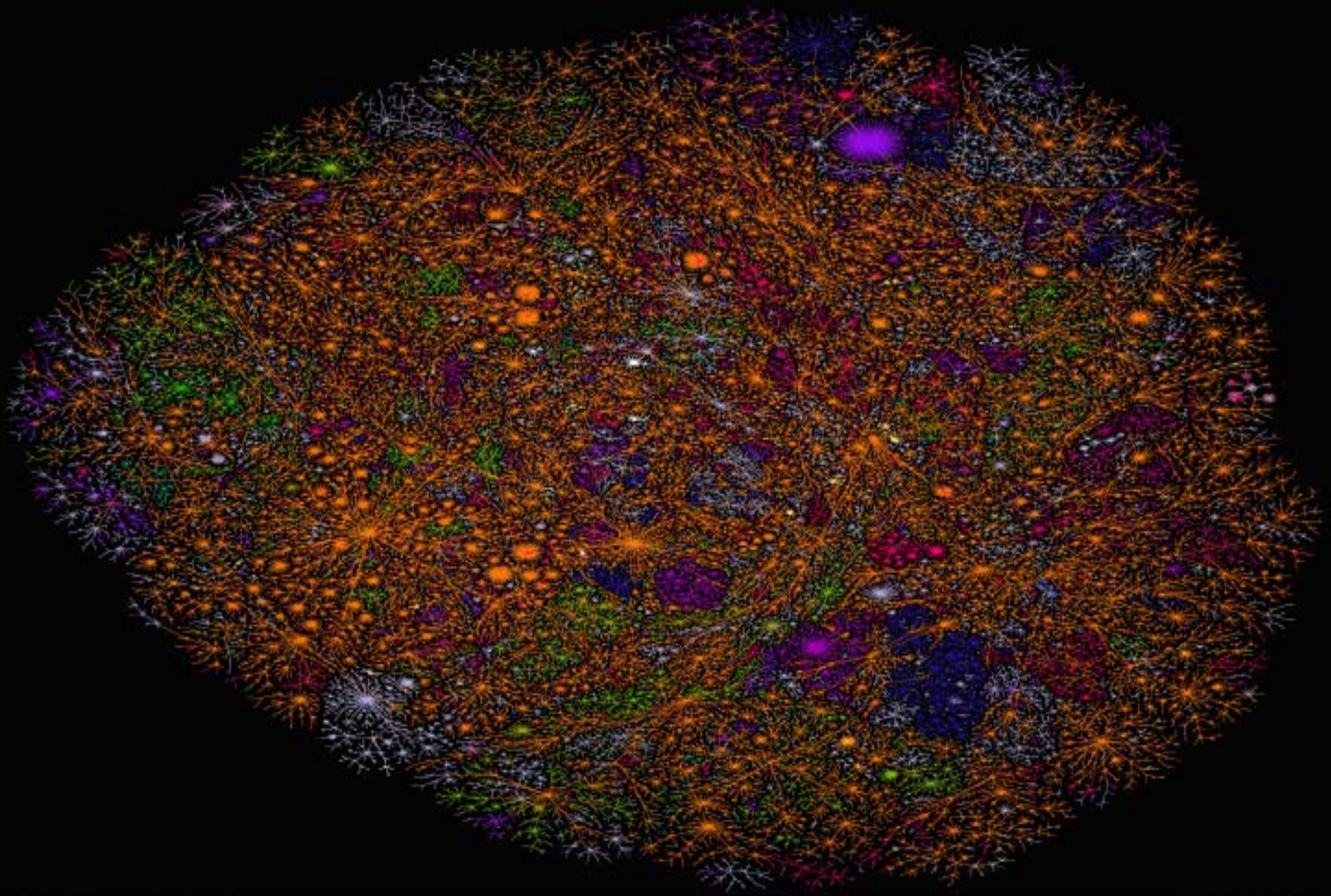


Hogyan néz ki az Internet?

Valóban decentralizált?



The Internet: 2002



Graph by the Rand and ISI Networks. Nodes by area flag and domain flag.

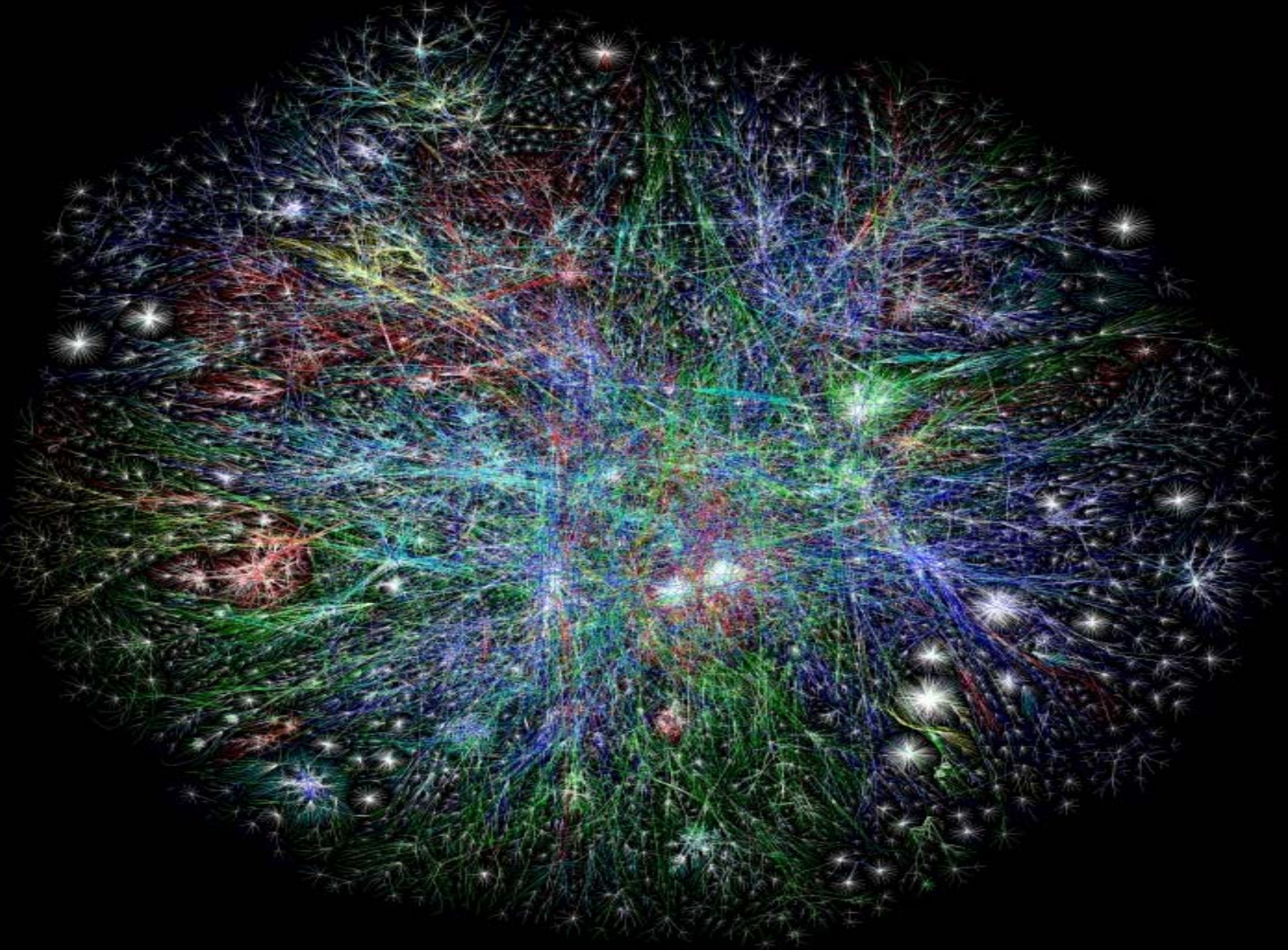
Copyright © 2002 LUMETA and Internet Map, Inc. 2002

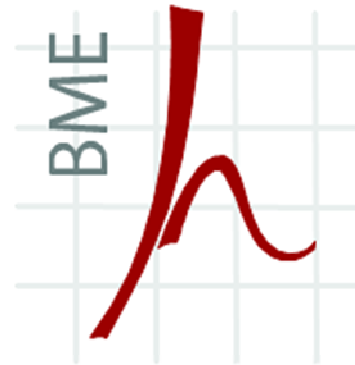
● North America
 ● Central America
 ● South America
 ● Africa
 ● South Africa
 ● Europe
 ● Germany
 ● France
 ● Netherlands
 ● United Kingdom
 ● Asia
 ● Japan
 ● Pacific Islands
 ● Australia
 ● New Zealand
 ● .mil
 ● .gov
 ● .com
 ● .edu
 ● .org
 ● .net
 ● other

The graph of the Internet was created by plotting the domain path structure as described in [1]. Nodes are colored by the 100,000 domains, listed in the global Internet register of North America Inc. and the corresponding routing system. The data was collected on January 1, 2002.

Published by
www.internetmap.com

Colors show the 100 top level Internet domains where network address numbers are registered. 100 countries are highlighted. (See legend in bottom right corner, requires map data a user select a. Clicked at a few examples in a "normal" windowing a map viewer.)





IP - Tördelés

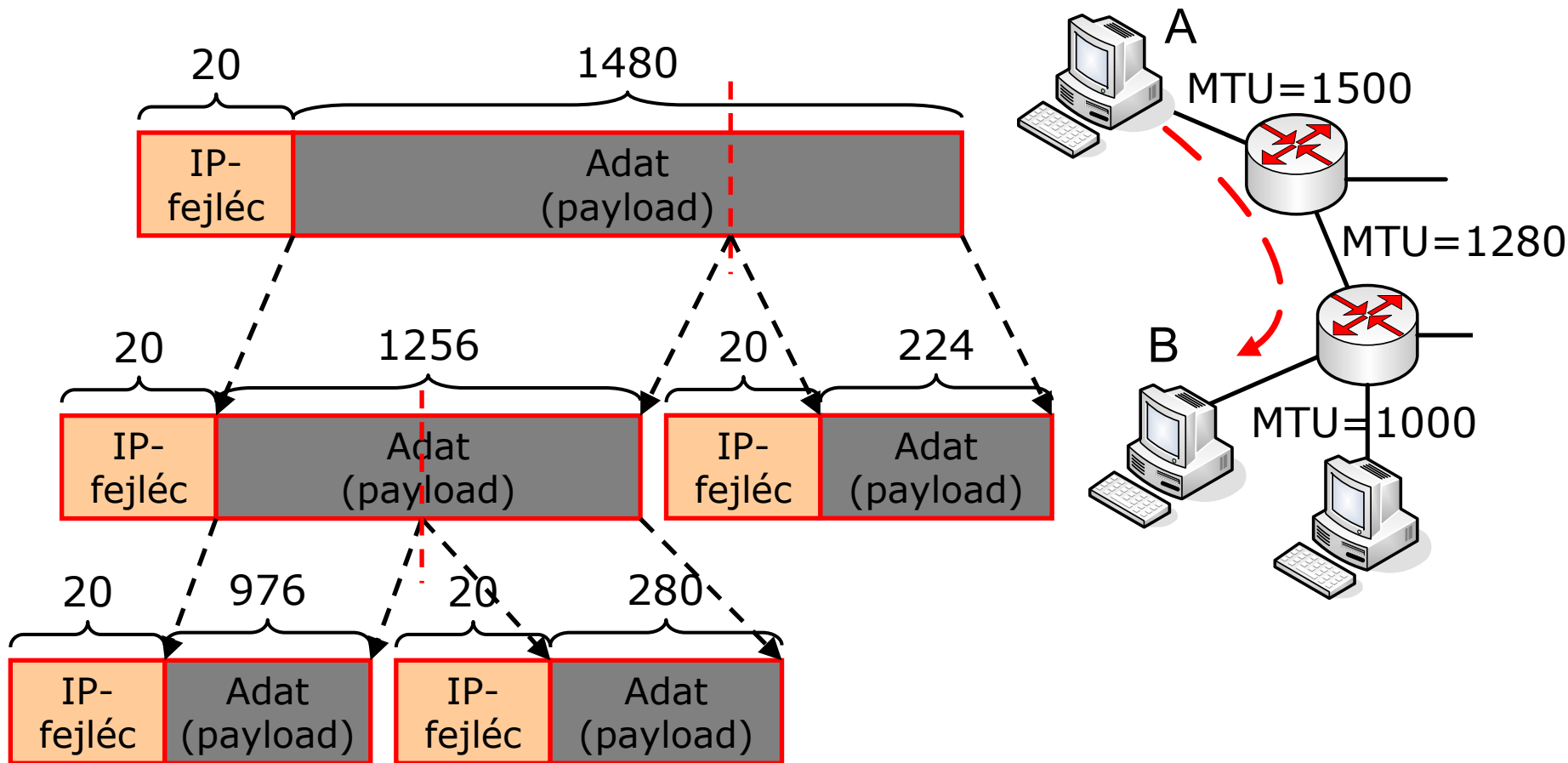
Darabolás és összeállítás

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 1500 byte
- Eltérő technológiák $\Rightarrow$ eltérő MTU-jú kapcsolatok $\Rightarrow$ tördelni kell

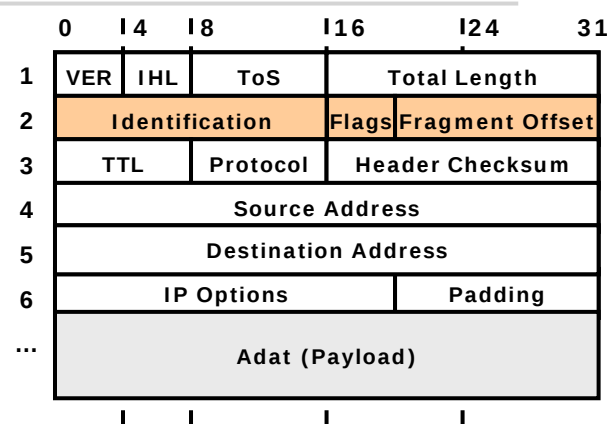
A tördelés menete

- Minden csomagnak kell fejléc (itt minimális fejléccel)!



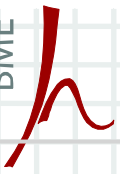
Tördeléssel kapcsolatos mezők az IP-fejlécben

- 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)



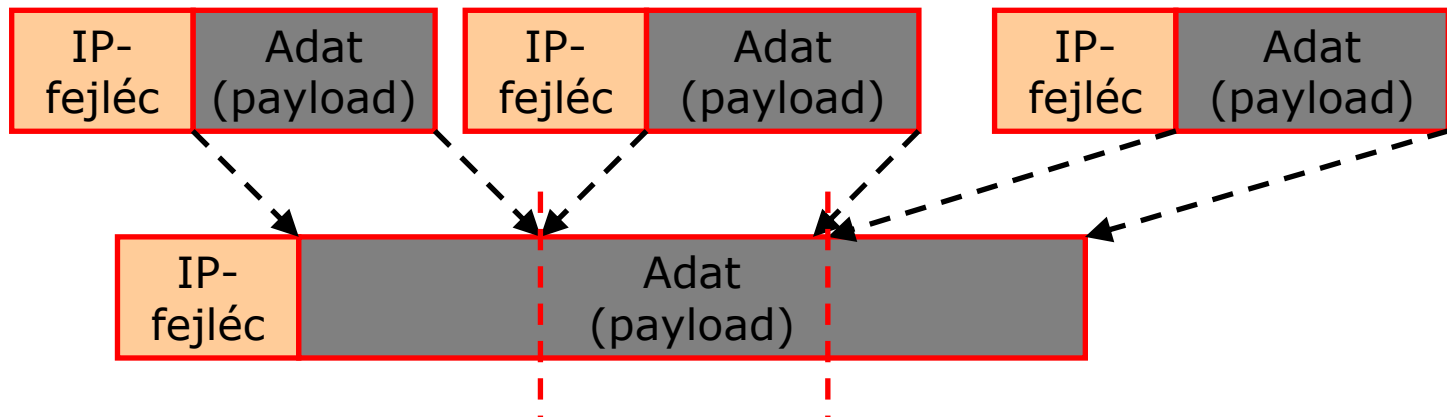
IP-fejléc változása tördelés közben

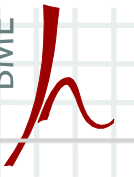
- Ha tördelés szükséges:
 - **Total Length** mezőt a töredék méretére állítani
 - Ha nem volt **Identification** mező érték, akkor generálni kell
 - Adat tördelése **8 bájtos egységekre**
 - A tördelésnek megfelelő **fragmentation offset**-et beállítani az új csomagokban
 - Minden csomagban az **MF bit**et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



A töredékek összeállítása

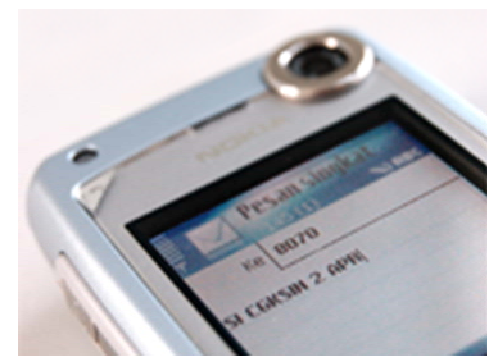
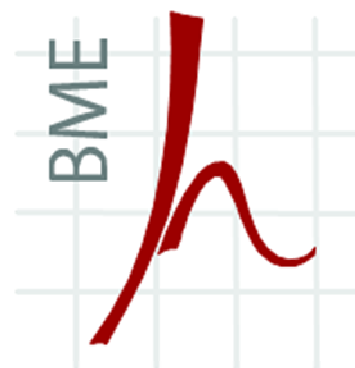
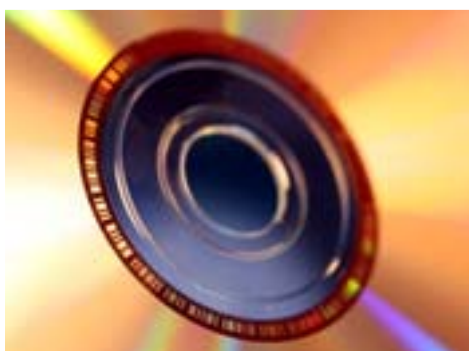
- Csak a címzett végezheti el
 - Kivéve pl. NAT
- Ha valamely darab nem érkezik meg, akkor **a többi is eldobja**
- Csak teljesen összeállított csomagokat továbbít a felsőbb réteg felé
- A „fragment offset”-ekből a töredék helye meghatározható





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

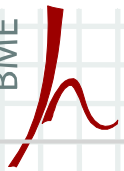
Az IP jelzés- és menedzsmentűzenetei

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

ICMP - Internet Control Message Protocol

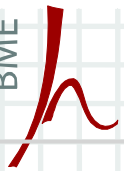
- Jelzés- és menedzsmentüzenetek
 - Visszajelzés a „best effort” hálózattól
- IP felett (0x01-es protokollazonosító)
- Üzenettípusok
 - Hibaüzenetek
 - Kérdések
 - Válaszok
- Gyakran használt ICMP üzenetek:
 - Echo request – Echo reply ⇒ **Ping (RTT)**
 - Echo request – Echo reply + TTL ⇒ **Traceroute**

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



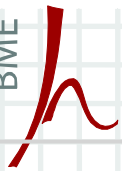
ICMP – Cél elérhetetlen

- 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

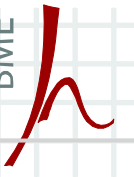
- Először TTL=1, majd TTL=2 ...
- Sorban eldobják a routerek és ICMP üzenetet küldenek róla (Time Exceeded)
- Megadja a csomópontok listáját, amelyeket érint a csomag a célig
- Nem mindig a realitást tükrözi a traceroute lista
- Alkalmazás:
 - Hibaelhárításra
 - Tűzfal felderítésre
 - Letöltésnél (mirror)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



További érdekes ICMP üzenetek

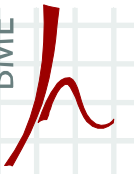
- **Source Quench**: felszólítás a küldőnek a forgalma visszafogására
- **Redirect**: felszólítás a küldőnek másik útvonal használatára
- **Address Mask Request**: host lekéri a router-től az alhálózati maszkot

- 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



Összefoglalás

- Bevezetés
 - A TCP/IP protokollarchitektúra
 - Az IP feladata és jellemzői
- IP címezés
 - 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
adjunktus

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