# IPv4

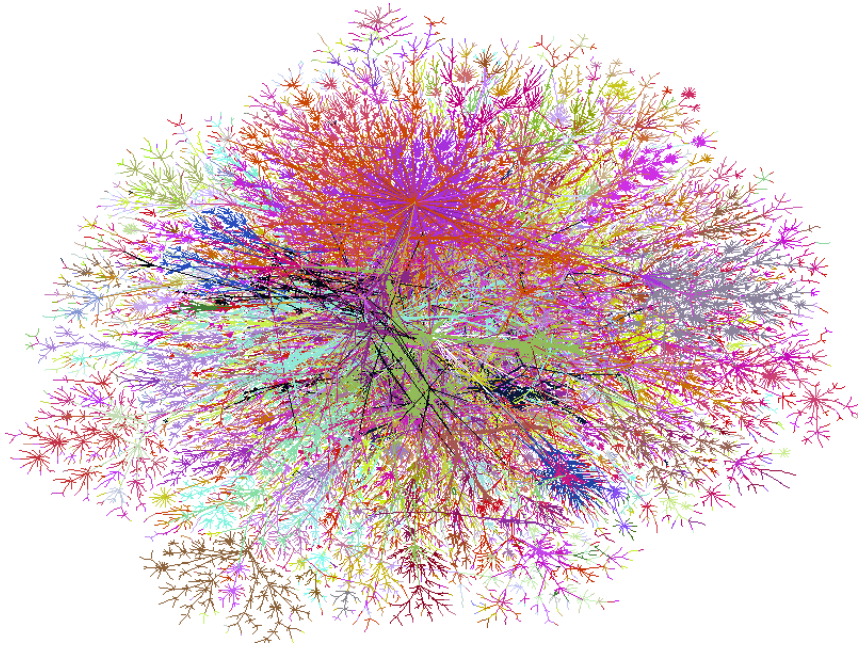
*Médiakommunikációs hálózatok (VIHIM161)*
*2013. évi fóliái alapján készült*

Dr. Lencse Gábor
tudományos főmunkatárs
BME Hálózati Rendszerek és Szolgáltatások Tanszék
lencse@hit.bme.hu

2023. február 28.,
Győr

# Tartalom

- Bevezetés: az IP általános jellemzői
- IP címzés
  - Osztály alapú címzés
  - Osztály nélküli címzés
  - IP címek kiosztása
- Az IP datagramok felépítése
- Csomagtovábbítás
- Datagramok tördelése
- ICMP



http://cheswick.com/ches/map/gallery/wired.gif

# BEVEZETÉS: AZ IP ÁLTALÁNOS JELLEMZŐI

# Az IP helye

| | |
|---|---|
| Alkalmazási | (7. Application) |
| Megjelenítési | (6. Presentation) |
| Viszonylati | (5. Session) |
| Szállítási | (4. Transport) |
| Hálózati | (3. Network) |
| Adatkapcsolati | (2. Data Link) |
| Fizikai | (1. Physical) |

**ISO OSI**

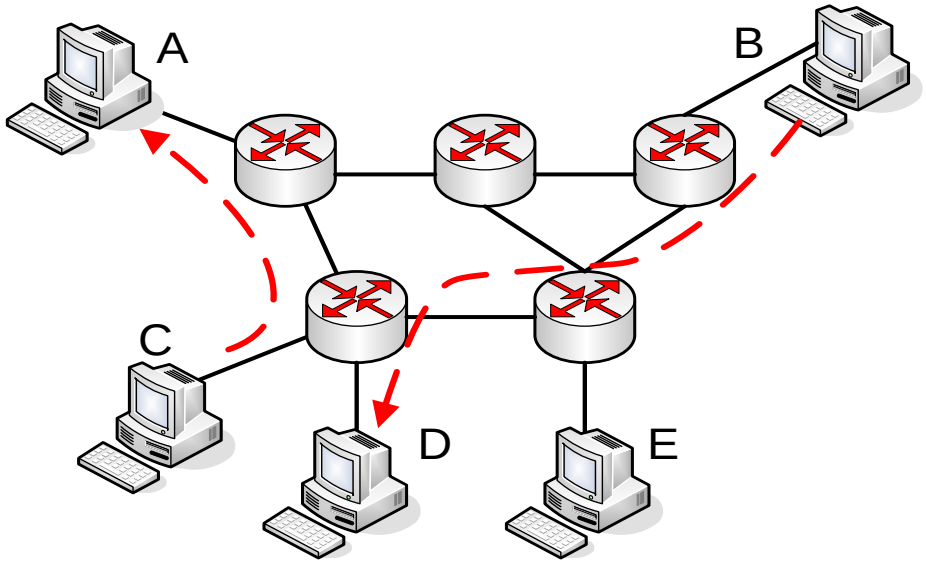
| | |
|---|---|
| Alkalmazási | (Application) |
| Szállítási | (Transport) |
| Hálózati | (Internet) |
| Hordozó-hálózat | (Link) |

**TCP/IP**

- Ahol az IP alatti hordozóhálózat:
  - akár nagykiterjedésű, akár helyi hálózatok két szomszédos csomópontja közötti adatátvitelt biztosítja
  - tartalmazhat hibadetektálási/hibajavítási funkciókat, de az IP erre a funkcióra nem épít, nélküle is működőképes

# Az IP feladata

- Hálózati protokoll által nyújtott szolgáltatás
  - Adattovábbítás a hálózat végpontjai között
- Legfontosabb funkciói
  - Címzés (addressing)
  - Csomagtovábbítás (packet forwarding)
    - az út(vonal)választási (routing) információ alapján
  - Tördelés (fragmentation)



# Az IP jellemzői

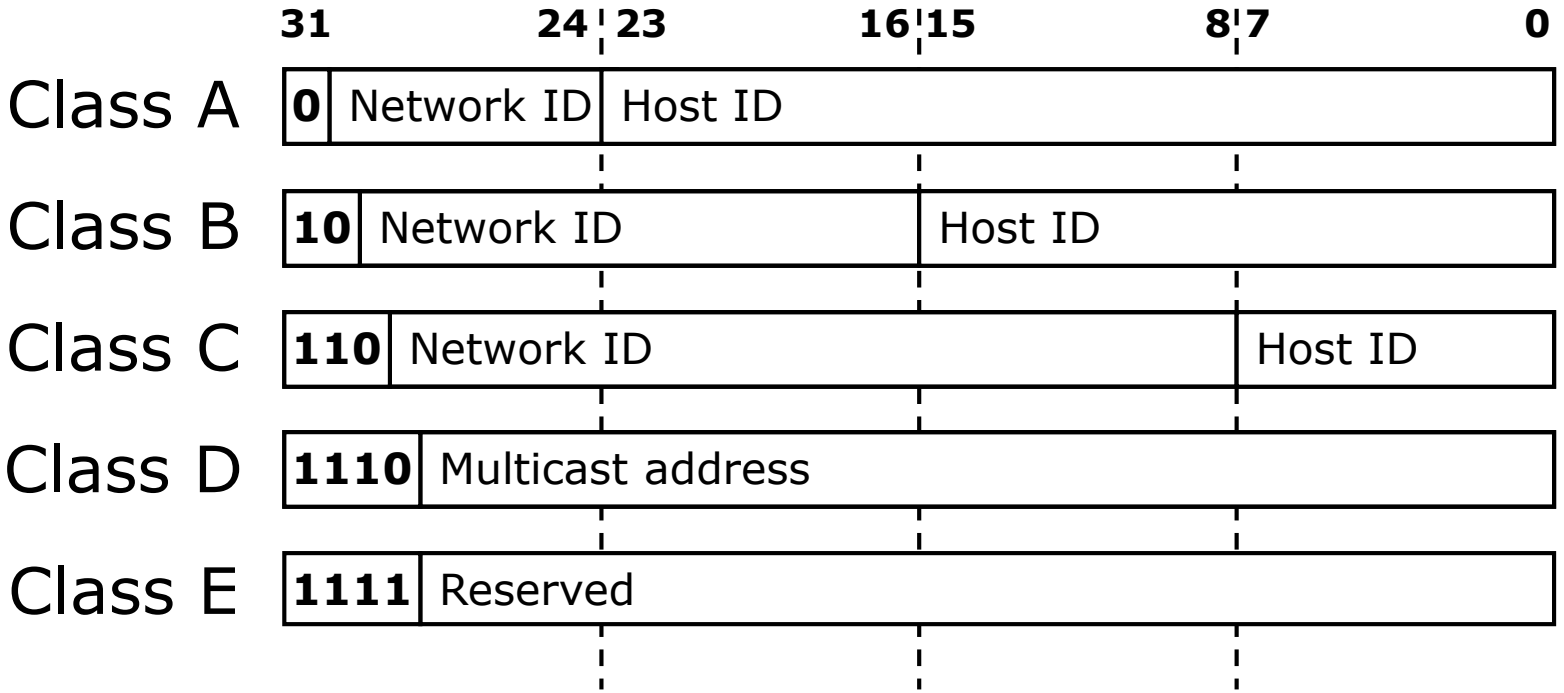
- Az IP jellemzői
  - Csomagkapcsolt
  - Összeköttetés-mentes (connectionless)

  } Datagram típusú

  - „Best effort” – nincs garancia
    - A csomagok:
      - Elveszhetnek
      - Duplikálódhatnak
      - Sorrendjük megváltozhat
      - Meghibásodhatnak (nincs hibaészlelés és -javítás)
  - Egyéb NEM nyújtott szolgáltatások:
    - Torlódáskezelés
    - Ütemezés
    - Titkosítás és hitelesítés

# Kitérő: RFC-k

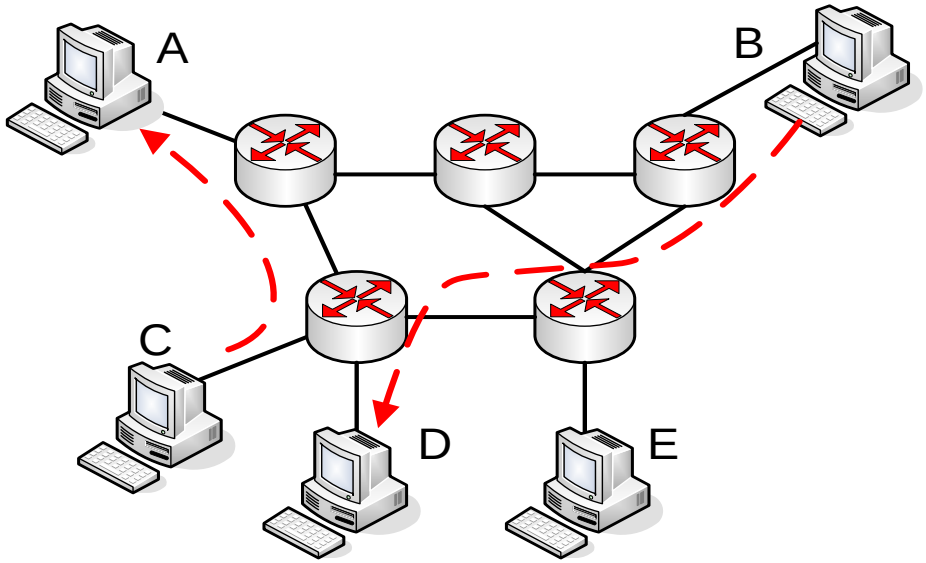
- RFC: Request For Comments
  - Hálózati protokollok, alkalmazások leírásának elsődleges forrásai
  - IETF: Internet Engineering Task Force fogadja el
  - elfogadásuk hosszú folyamat eredménye
  - először: Internet Draft, például:
    - https://datatracker.ietf.org/doc/html/draft-ietf-v6ops-transition-comparison-01
  - Évente 3 IETF meeting, ezeken Working Group-okban vitatják meg
    - Valamint a munkacsoport levelező listáján
    - WGLC: Working Group Last Call
  - Standard Track:
    - Régi: Proposed Standard --> Draft Standard --> Standard
    - Új: Proposed Standard --> Internet Standard (RFC 6140)
    - Ha elavul: Historical (feltüntetik, hogy: obsolated by …)
    - HTML forrásban érdemes nézni, ott megvan, ha: obsolated, updated
  - Van még: Informational, Experimental


31
24
23
16
15
8
7
0
Class A
0
Network ID
Host ID
Class B
10
Network ID
Host ID
Class C
110
Network ID
Host ID
Class D
1110
Multicast address
Class E
1111
Reserved

# IP CÍMZÉS

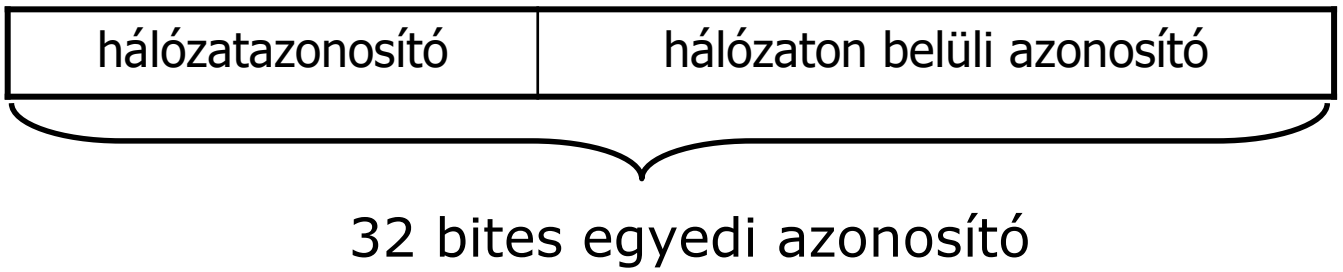
# Az IP feladata (ismétlés)

- Hálózati protokoll által nyújtott szolgáltatás
  - Adattovábbítás a hálózat végpontjai között
- Legfontosabb funkciói
  - **Címzés (addressing)**
  - Csomagtovábbítás (packet forwarding)
    - az út(vonal)választási (routing) információ alapján
  - Tördelés (fragmentation)



# Az IP-cím felépítése

- 4 bájtos cím (32 bit)
  - $2^{32} \approx 4 \cdot 10^9$ ⇨ kb. 1/2 IP-cím/fő (a föld lakossága kb. 8 milliard fő)
- Jelölések
  - Bináris: 10110000 10010011 00111110 11100001
  - Kanonikus formátum (Dotted decimal): 176.147.62.225
- Hierarchikus címzés eredetileg két szinten
  - Cím = hálózatazonosító + hálózaton belüli azonosító



# Címosztályok

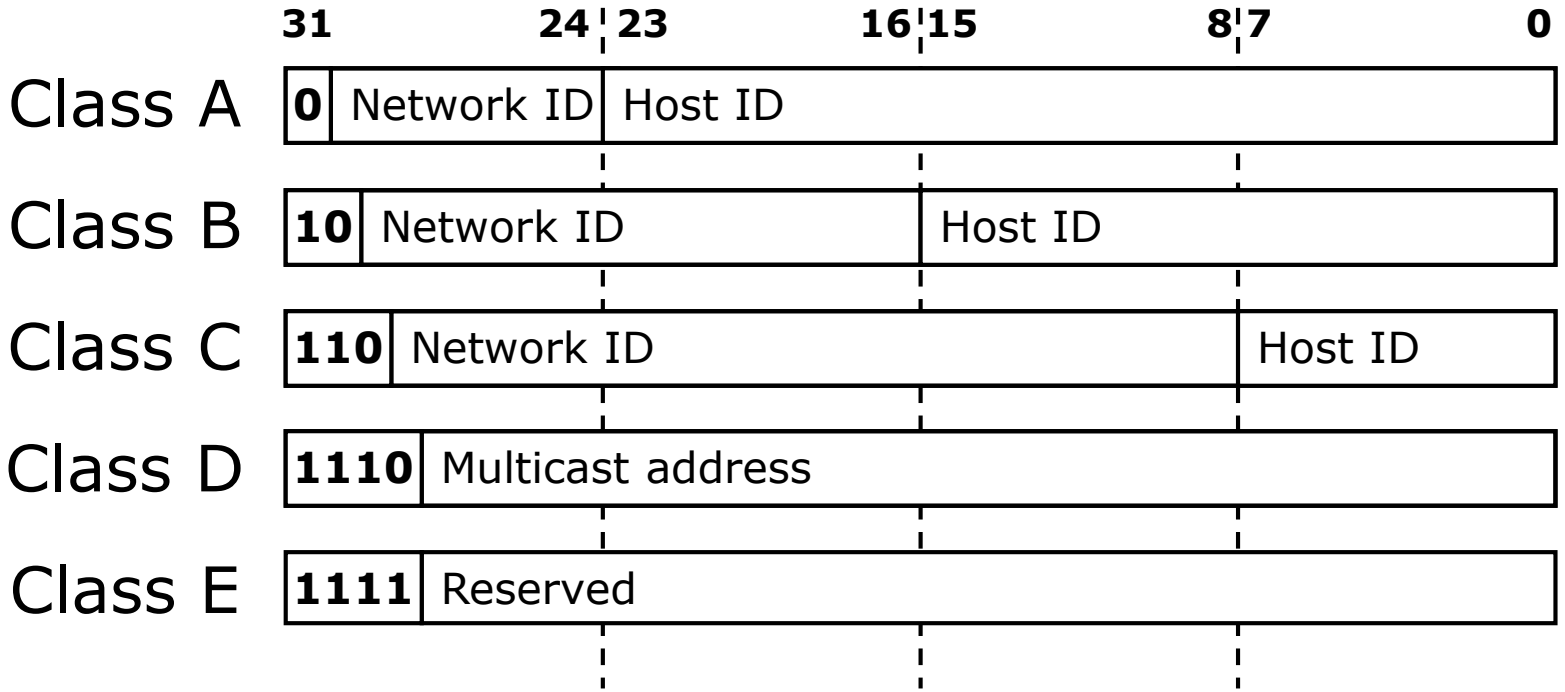
- Az osztály alapú címzés (classful addressing) részben csak történeti jelentőségű!
- Alapötlet: különböző méretű hálózatoknak más méretű IP cím tartomány

| Osztály | Hálózatazonosító bitjeinek száma* | Hálózatok száma* | Hálózaton belüli címek száma* |
|---|---|---|---|
| A | 8 | $2^7-2=126$ | $2^{24}-2=16777214$ |
| B | 16 | $2^{14}-2=16382$ | $2^{16}-2=65534$ |
| C | 24 | $2^{21}-2=2097150$ | $2^8-2=254$ |

- * elméleti értékek
  - A hálózatazonosító bitjeinek a számából lejön az osztályjelölő prefix
  - a hálózatok számánál már a prefix okozta csökkenés is le van számolva, valamint az első és az utolsó hálózat is (ami helytelen!)
  - a hálózaton belüli címeknél az első és az utolsó cím nem használható címzésre (lásd később)

# A címosztályok jelölése és címkiosztása

- Osztályazonosító prefixek
- Diszjunkt címtartományok



# Az egyes osztályok felhasználása

- A, B és C osztályú címek
  - Egyedi címzésre (unicast)
- D osztály
  - Többes címzésre (multicast) (később részletesen)
  - Címtartomány: 224.0.0.0-tól 239.255.255.255-ig
- E osztály
  - Fenntartott osztály és címtartomány 240.0.0.0-tól 255.255.255.255-ig

# Speciális címek

- Host ID: csupa 0
  - Hálózat címe
  - Az adott hálózat eszközei (elvileg) opcionálisan kezelhetik
- Host ID: csupa 1
  - Broadcast cím
  - Az adott hálózaton mindenkinek szól
- 127.0.0.0 - 127.255.255.255
  - Loopback cím
  - A helyi gépet azonosítja
  - Bármelyik használható, a 127.0.0.1 a szokásos

*(folytatjuk)*

# Speciális címek

*(folytatás)*

- 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)
- Link lokális IP-címtartomány (RFC 3927)
  - 169.254.0.0 – 169.254.255.255 (1 db B osztály)
  - Útválasztók NEM továbbítják
  - De az automatikus címkonfigurációhoz használható tartomány csak: 169.254.1.0 – 169.254.254.255, használat előtt ARP Probe kötelező

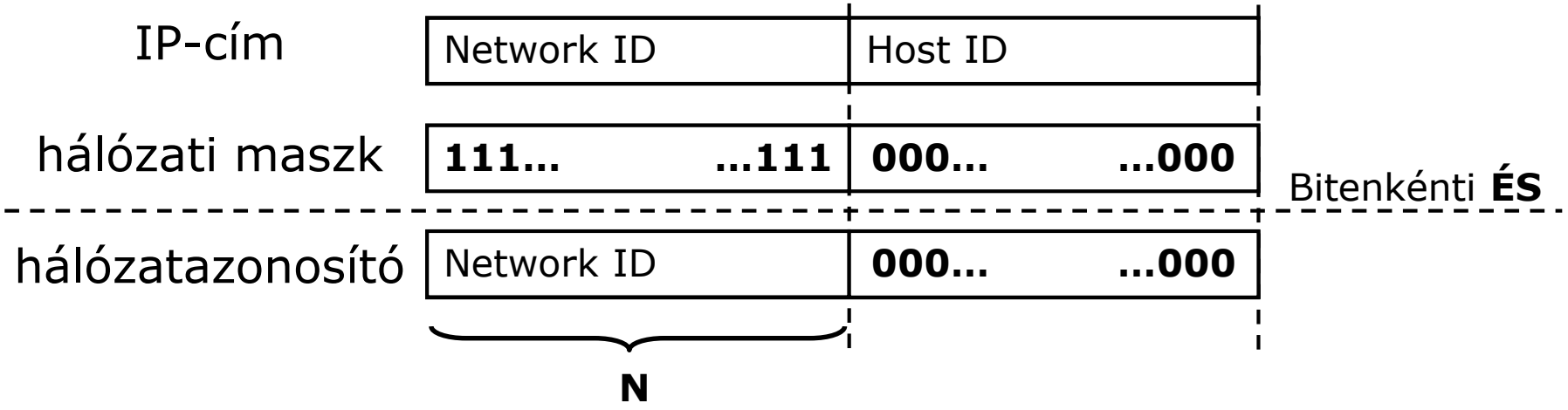
*További speciális célra lefoglalt tartományok: RFC 6890*

# Osztálymentes címzés szükségessége

- Problémák
  1. Az osztály alapú címzés nem igazodik a fizikai hálózatstruktúrához
     - Egy nagy hálózat kisebb fizikai hálózatokból épül fel.
       ⇨ Az A, B osztályú hálózatokat kisebb hálózatokra KELL bontani.
  2. A címzésben a két hierarchia szint túl kevés
     - Az útválasztási (routing) táblázatok mérete drasztikusan nőtt
       ⇨ aggregációval megoldható a több hierarchia szint bevezetése.
- Megoldás: osztálymentes címzés (classless addressing) és CIDR (Classless Inter-Domain Routing) 1517-20 RFC-k
  - Nem az IP cím első néhány bitjéből, hanem egy maszk alapján állapítjuk meg, hogy hol a határ az IP cím két része közt.
  - VLSM – Variable Length Subnet Mask
    A cím 32 bitje tetszőleges helyen lehet kettéosztva hálózat- és végponti azonosítóra

# Osztálymentes címzés megvalósítása

- A hálózati maszk használata



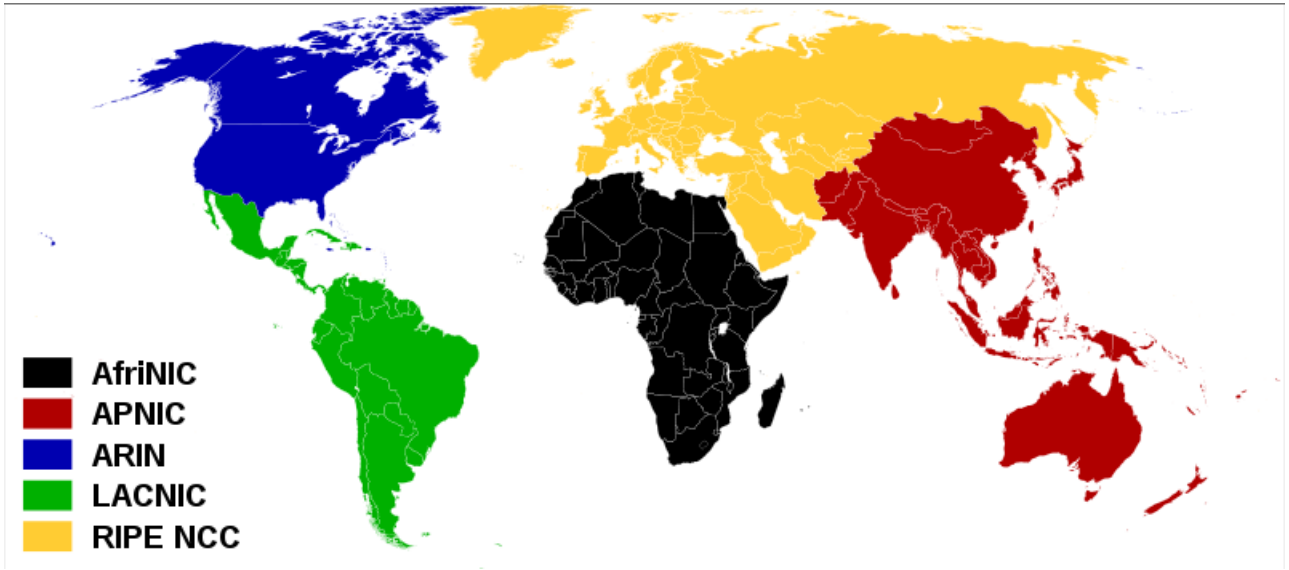

- Jelölés a hálózat egyértelmű azonosítására
  - <hálózat IP-címe> / <alhálózati maszk egyeseinek a száma>
  - Így pl. a BME hálózata: 152.66.0.0 /16 (hálózati maszkja 255.255.0.0)
  - Hasonlóan:
    - A osztály: /8
    - B osztály: /16
    - C osztály: /24

# Az IP címzés történeti fejlődése

- A fejlődés fő lépései:
  - kb. 1980 Classful Addressing (RFC 790)
  - kb. 1985 Subnetting (RFC 950)
  - kb. 1993 Classless Addressing (RFCs 1517-1520)
- A fejlődés „melléktermékе”:
  - Visszamaradt kifejezések ma is élnek
    - pl. „alhálózati maszk” (subnet mask) kifejezés használata; helyesebben „hálózati maszk” (netmask), hiszen a CIDR-ben a supernetting is benne van!
  - Visszamaradt szabályok élnek a köztudatban
    - pl. első és utolsó subnet (csupa 0 és csupa 1) nem osztható ki (RFC 950), pedig ez már régen nincs így, lásd RFC 1878

# Az IP-címek kiosztása

- Az IP-címeket az IANA (Internet Assigned Numbers Authority) osztja ki (pontosabban: osztotta ki) az 5 RIR (Regional Internet Registry) számára „/8” blokkonként
- A RIR-ek kisebb blokkonként osztják tovább internet szolgáltatóknak, oktatási intézményeknek, nagy cégeknek, stb.



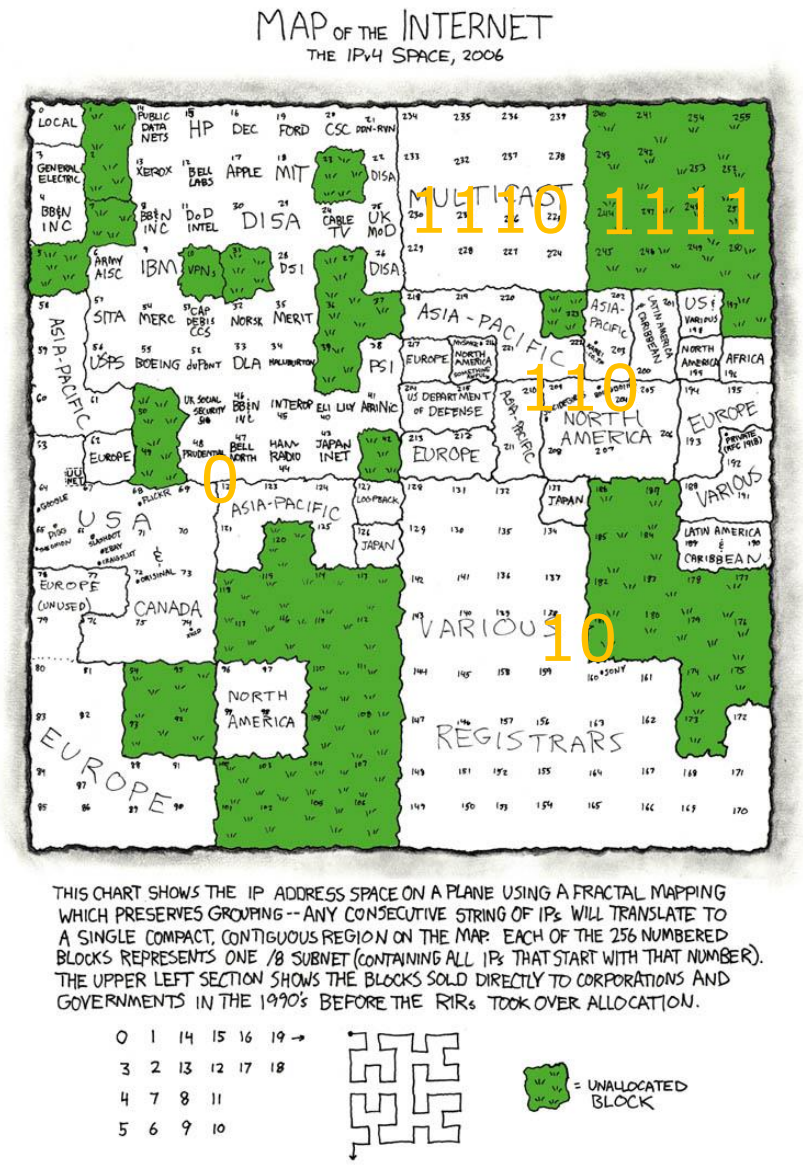

A kép forrása: http://en.wikipedia.org/wiki/File:Regional_Internet_Registries_world_map.svg

# A kiosztott IPv4 címek – 2006

- 2006-os állapot fraktálos ábrázolása

  A kép forrása: http://xkcd.com/195/

- Figyeljük meg:
  - kezdeti „/8” blokkok nagy cégeknek (főleg az első negyedben)
  - A „C” osztálynál látható a regionális elv érvényesülése
  - A „D” osztály a multicastnak van lefoglalva
  - Az „E” osztály fenntartott
    - Ezt végül „sikerült elveszteni”



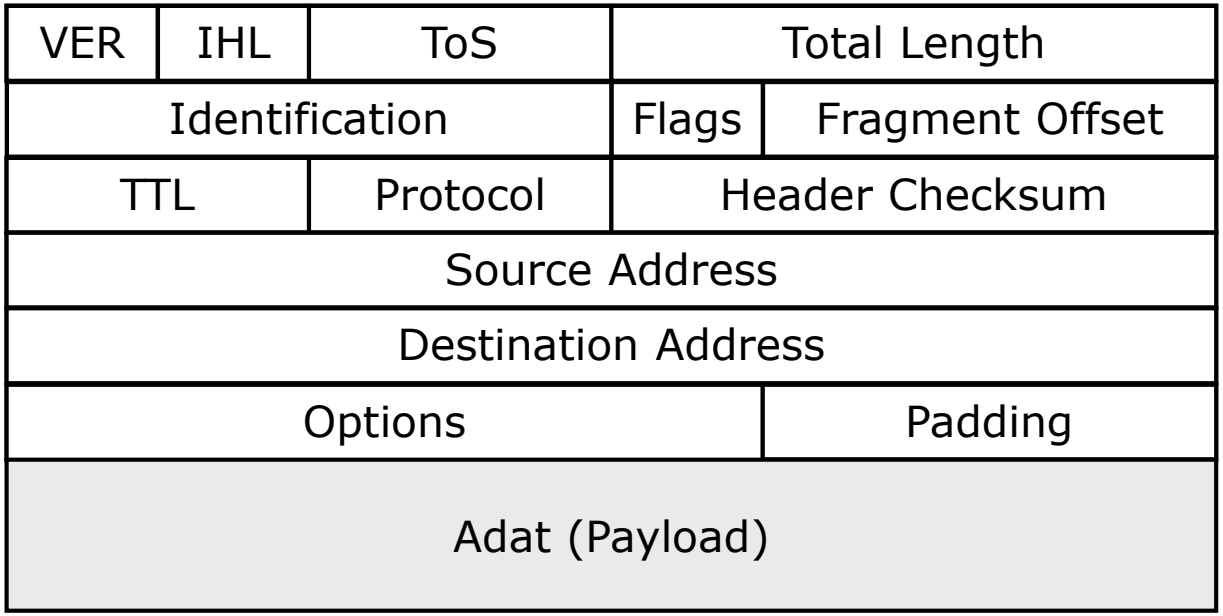
# Az IPv4 címek elfogyásának állása

- Különböző módszerekkel sikerült jelentősen kitolni az IPv4 címtartományának kimerülését
  - osztálymentes címzés
  - privát IP címek + NAT (RFC 1631) használata
  - a kezdetben kiosztott túlságosan nagy címtartományok visszaadása
- Az IANA központi készletének kimerülése
  - 2011. 01. 31-i APNIC igénylés alapján, a borítékolt terv szerint
  - 2011. 02. 03-án kiosztotta az utolsó „/8” blokkokat a RIR-eknek
  - RIR-ek tartományának kimerülése: https://ipv4.potaroo.net
    - APNIC: 2011. 04. 19.; RIPE NCC: 2012. 09. 14.; LACNIC: 2014. 06. 10.
    - ARIN: 2015. 09. 24.; AfriNIC: 2. fázisban van: https://afrinic.net/exhaustion

    ⇨ Szigorúbb allokációs szabályok a legutolsó „/8” blokkjukra!

  ⇨ Az IPv6 bevezetése tovább nem halogatható!

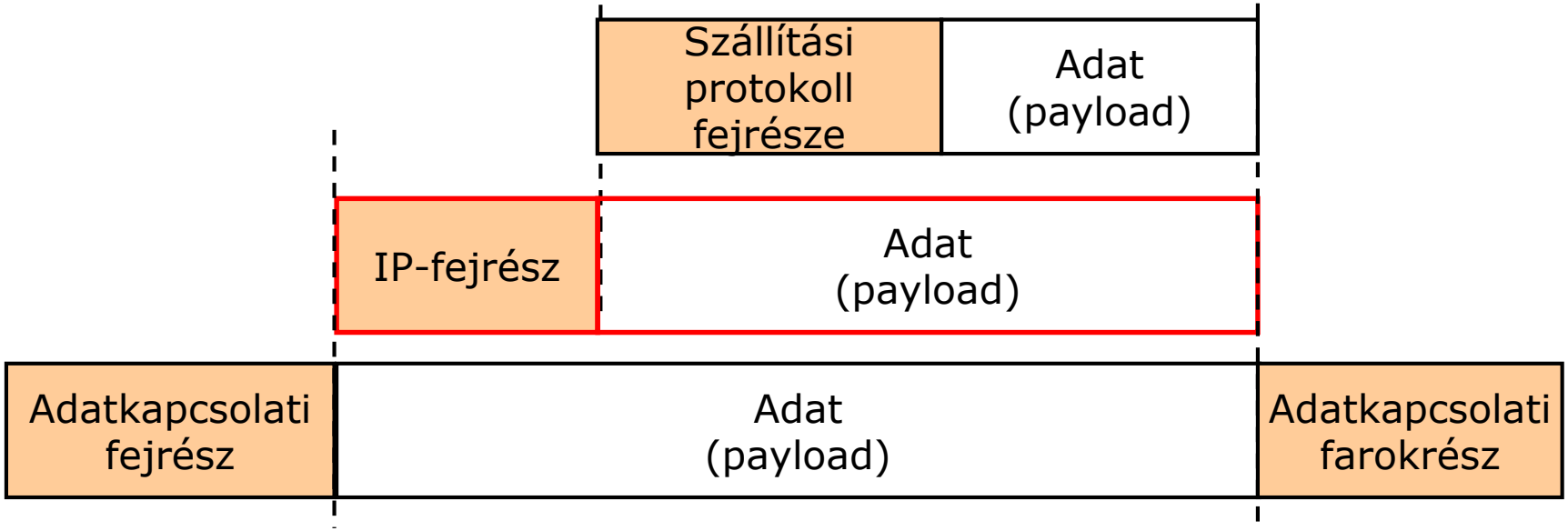
  ⇨ Az IPv6, valamint a két rendszer együttélésének oktatása kulcsfontosságú!



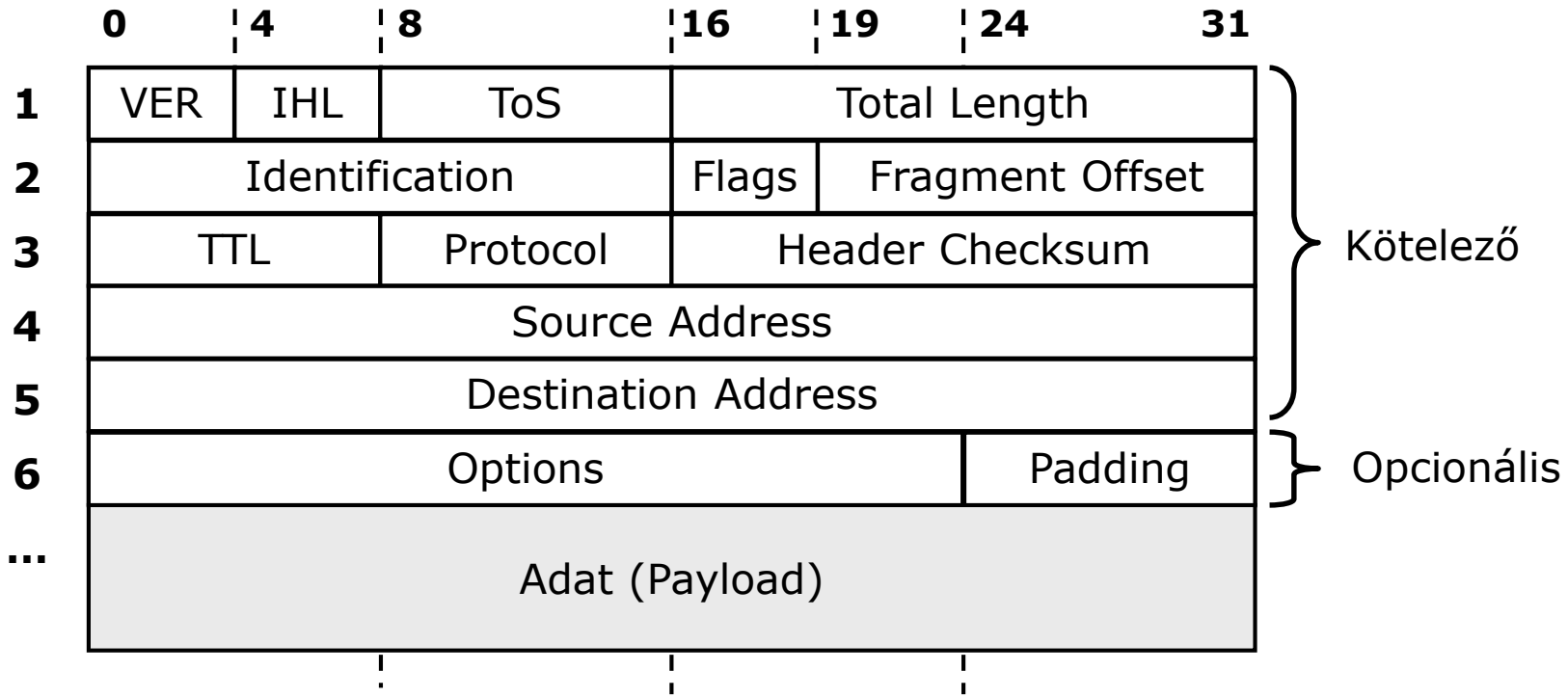

# IP DATAGRAM FELÉPÍTÉSE

# Az IP-csomag szerkezete és „helye”

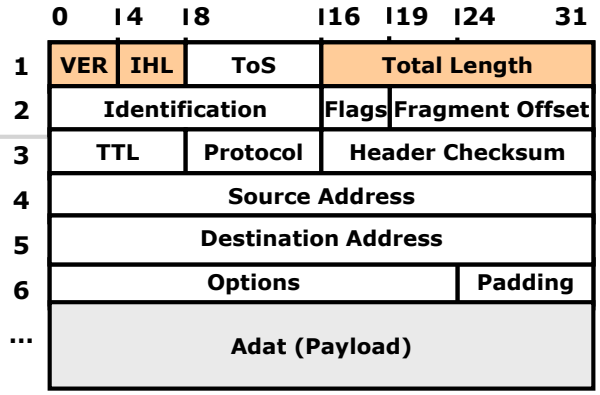
- Az IP-csomag két része:
  - IP-fejrész (fejléc) (IP header)
  - Adat (payload)
- Az IP-csomag alsóbb rétegbeli protokoll adatrészébe ágyazódik be
- Az IP-csomag adatrészébe magasabb rétegbeli protokollüzenet (PDU) kerül



# Az IP fejrész szerkezete

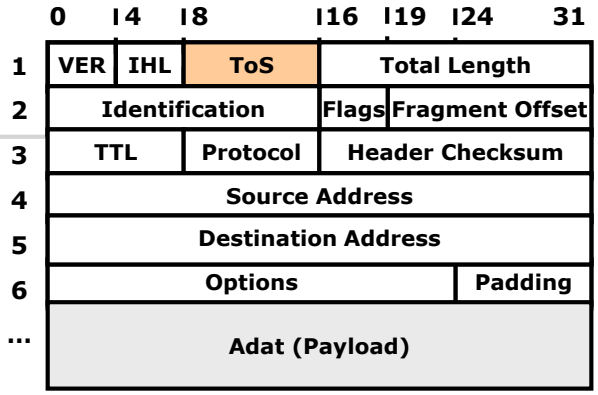


# Az IP fejrész mezői I.




- **VER – Version** (4 bit)
  - Az Internet Protocol verziójának száma
  - Tipikus értéke: IPv4: 4, IPv6: 6
- **IHL – Internet Header Length** (4 bit)
  - Az IP fejrész 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 (in octets)**
  - Értéke:
    - **Minimum támogatandó**: 576 bájt
      (512 adat + 20 IP fejrész + 44 IP-opciók és a felsőbb rétegek fejrészei)
      Ilyen méretű csomagot tördeletlenül kell tudni továbbítani a linken
    - Maximum: $2^{16}$-1=65535 (max. 65515 bájt adat)

# Az IP fejrész mezői II.



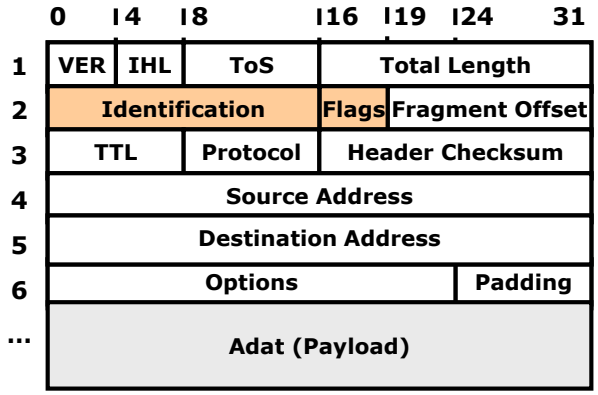

- **ToS (Type of Service)** (8 bit)
  - QoS osztályok, paraméterek jelzésére (az eredeti RFC 791 szerint)

| Bitek | Jelentés |
|---|---|
| 0-2 | Precedence<br>Példák:<br>„network control”<br>„priority”<br>„routine” |
| 3 | Delay (0: normal, 1: low) |
| 4 | Throughput (0: normal, 1: high) |
| 5 | Reliability (0: normal, 1: high) |
| 6-7 | Fenntartott |

A 3 bitből max. 2db lehet 1-es

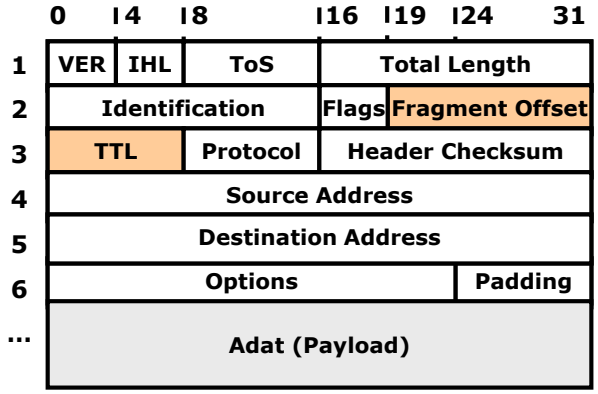
  - A legtöbb router nem támogatja
  - Helyette a leggyakrabb felhasználás:
    - 0-5 bit: DSCP – Differentiated Services Code Point (RFC 2474)
    - 6-7 bit: ECN – Explicit Congestion Notification (RFC 3168)

# Az IP fejrész mezői III.



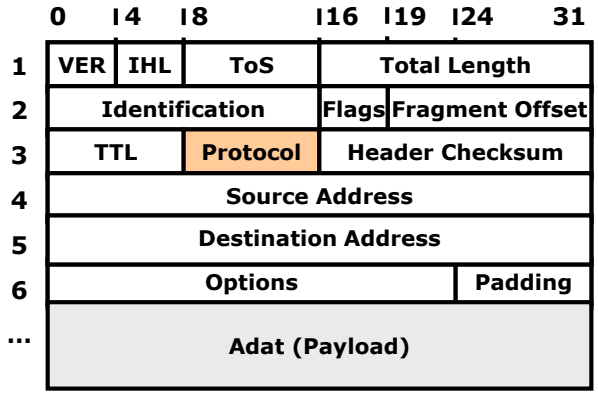

- **Identification** (16 bit)
  - Az IP-töredékek egyedi azonosítása
- **Flags** (3 bit)
  - 0: Fenntartott
    - 0-nak kell lennie
    - „Evil bit” (RFC 3514) (áprilisi tréfa 2003-ban)
  - 1: DF – Don’t Fragment
    - 1: TILOS tördelni; ha tördelni kellene, el kell dobni
    - Ezt használják a Path MTU (Maximum Transmission Unit) Discovery céljára néhány TCP verzióban
  - 2: MF – More Fragments
    - 1: ha nem az utolsó töredék
    - 0: utolsó töredék vagy nem tördelt csomag

# Az IP fejrész mezői IV.



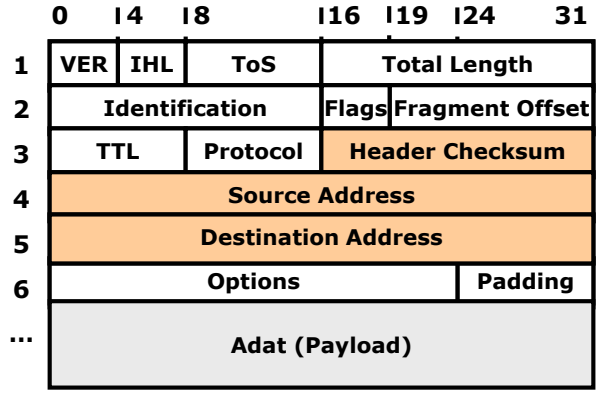

- **Fragment Offset** (13 bit)
  - Az ebben a töredékben lévő adatnak az eredeti csomagban lévő kezdő pozícióját adja meg **8 bájtos egységekben**
  - $(2^{13}-1)x8=65528 > 65515$ bájt (max. adat)
    ⇨ maximális méretű csomag is tördelhető
- **TTL – Time To Live** (8 bit)
  - Csomag élettartama
  - Eredetileg másodpercben
  - Gyakorlatban hopszámban mérve (hop count)
    - Minden továbbításnál csökkenteni kell ez értékét legalább 1-gyel
    - Ha a csökkentés után az értéke 0 (vagy negatív), akkor el kell dobni

# Az IP fejrész mezői V.



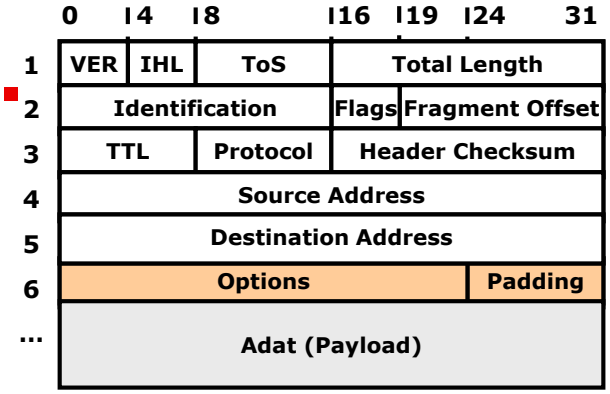

- **Protocol** (8 bit)
  - Az adatrészben lévő protokoll azonosítója
  - A kezdeti lista az RFC 790-ben volt
  - Az IANA felügyeli ezeket az azonosítókat
  - Az aktuális lista elérhető: http://www.iana.org/assignments/protocol-numbers/
  - Példák:
    - 1: Internet Control Message Protocol (ICMP)
    - 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 IP fejrész mezői VI.

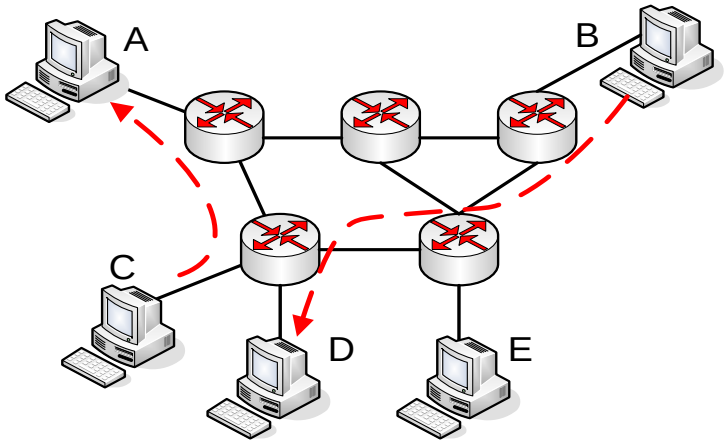



- **Header Checksum** (16 bit)
  - Az IP fejrész minden 16 bites szavát egyes komplemens összeadással összegezzük és az eredmény egyes komplemensét vesszük (a számításnál ez a mező csupa 0)
    Előnye: a módszer érzéketlen a számítást végző aritmetika alvég/felvég fajtájára (endianness)
    Így kell kiszámolni: http://mathforum.org/library/drmath/view/54379.html
  - A csomag érkezésekor ellenőrizni kell a helyességét, és továbbítás esetén újra kell számítani (a TTL változása miatt)
- **Source Address** (32 bit)
  - Az IP-csomag feladójának az IP-címe
- **Destination Address** (32 bit)
  - Az IP-csomag címzettjének az IP-címe

# Az IP fejrész mezői VII.



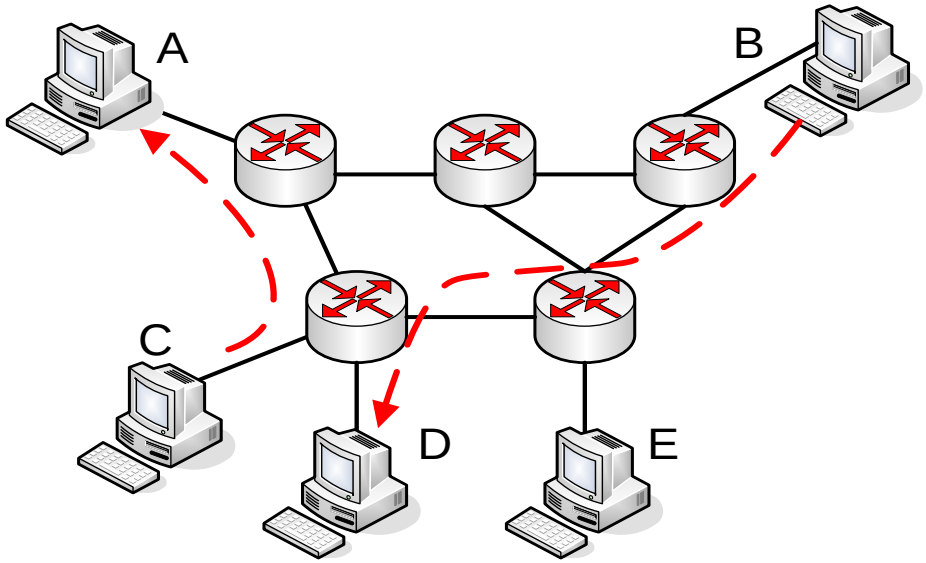

- **IP Options**
  - A fejrésznek ritkán használt része
  - Segítségével például a csomag útját lehet kijelölni:
    - SSRR: Strict Source and Record Route – pontos út kijelölése
    - LSRR: Loose Source and Record Route – kötelező útba ejtendő csomópontok kijelölése
    - Használható például hálózati működés tesztelésére – és támadásokra is!
    - Legtöbb router biztonsági megfontolásból eldobja
- **Padding**
  - Az IP Options részt egészíti ki 4 bájt többszörösére
  - Kitöltésre 0 értékű bájtokat kell használni




# CSOMAGTOVÁBBÍTÁS

# Az IP feladata (ismétlés)

- Hálózati protokoll által nyújtott szolgáltatás
  - Adattovábbítás a hálózat végpontjai között
- Legfontosabb funkciói
  - Címzés (addressing)
  - **Csomagtovábbítás (packet forwarding)**
    - az út(vonal)választási (routing) információ alapján
  - Tördelés (fragmentation)



# A csomagtovábbítás alapelve

- Az IP jellemzői
  - Csomagkapcsolt
  - Összeköttetés-mentes (connectionless)
  - „Best effort” – nincs garancia

  } Datagram típusú

- „Hot potato”-elv
  - Minél gyorsabban továbbítsuk
  - Csak a következő csomópontot kell ismernünk (hop-by-hop)
  - Előnyei:
    - Kis erőforrásigény
      - Egyszerű, ezért gyors működésű
      - Gyors, ezért nem kell (sokáig) tárolnunk a csomagokat (kis memóriaigény)
    - „Kevés” ismeret kell a hálózatról
    - Datagram szolgáltatásra tökéletesen alkalmas
      nem vállal garanciát, ezért nincs szükség nyugtázásra és egyéb hibakezelésre ⇨ gyorsasága megmarad

# A továbbításhoz szükséges információk

- Kinek küldjük tovább?
  - Cél címe alapján ⇨ csomag tartalmazza
  - Saját ismeret alapján ⇨ útválasztási táblázat (routing table)

Útválasztás (routing)

- Hogyan küldjük tovább?
  - Mekkora egységekben?
    - Mekkora érkezik? ⇨ csomag határozza meg
    - Mekkora továbbítható? ⇨ a következő hálózat MTU-ja (Maximum Transmission Unit) határozza meg

Tördelés (fragmentation)

  - Milyen QoS biztosításával?
    - „Best effort” – nincs garancia
    - Opcionális megoldás: ToS mező felhasználásával egyéb protokollok és mechanizmusok

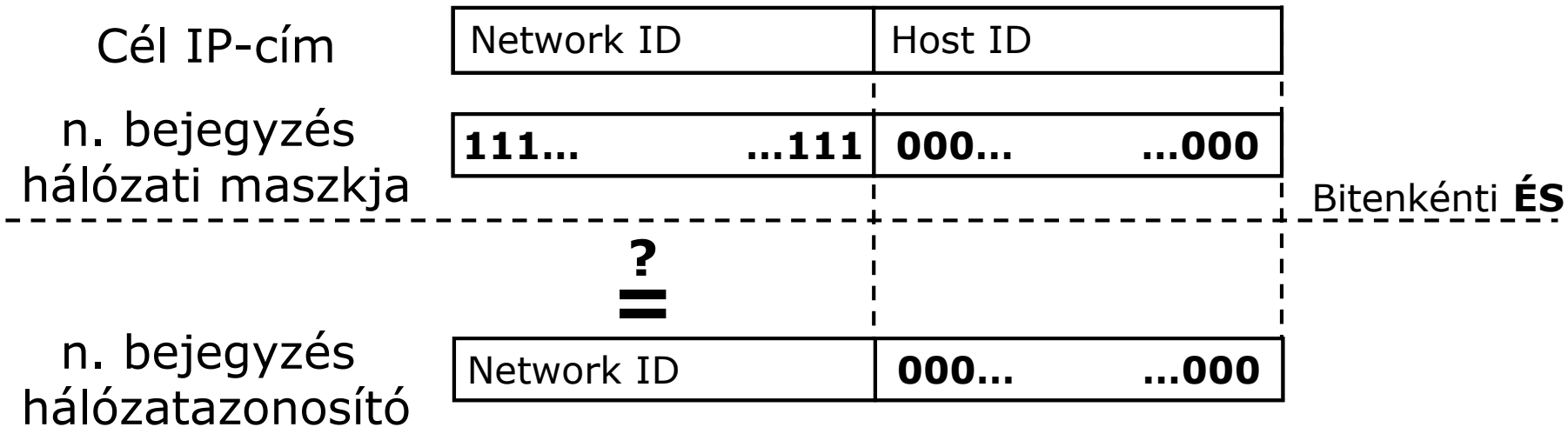
QoS (szolgáltatás-minőség)

# Útválasztó tábla (Routing table)

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

| *Hova tart?* | | *Merre küldjük tovább?* | | |
|---|---|---|---|---|
| Hálózat címe | Hálózati maszk | Következő csomópont | Interfész | Közvetlenül kapcsolódó |
| <IP-cím> | </N> | <IP-cím> | <azonosító> | <igen/nem> |
| <IP-cím> | </N> | <IP-cím> | <azonosító> | <igen/nem> |
| <IP-cím> | </N> | <IP-cím> | <azonosító> | <igen/nem> |

# Hálózat kiválasztása




- A cél IP-cím akkor tartozik a táblázat n. sorában leírt hálózatba, ha a cél IP-cím és az n. sorban található hálózati maszk bitenkénti ÉS műveletének eredménye az n. sorban található hálózatazonosítóval megegyezik.

# Keresés az útválasztó táblában

- Ha a cél IP-cím több hálózatra is illeszkedik, akkor legspecifikusabb illeszkedés alapján kell továbbítani:
  ⇨ ez az, ahol a leghosszabb a hálózati maszk
  - A problémának komoly irodalma van, akit mélyebben érdekel, Logest Prefix Math Algorithm néven érdemes keresni.
- Az útválasztó tábla összes bejegyzését végig kell nézni
  ⇨ akadályozza a „növekedést”
  - Általában bináris fával implementálják
    ⇨ így a bejegyzések számában lineáris keresés helyett a lépésszám csak a prefix hosszával arányos
  - Gerinchálózatban hardveres megoldás
- Keresés csak akkor, ha az nem saját  cím

# Alapértelmezett útvonal (Default route)

- Erre megy a csomag, ha nem ismert a célhálózat
- Ez is megadható egy megfelelő bejegyzéssel
  - Minden címet tartalmazó hálózat: **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: router / útválasztó / útvonalválasztó
- Nem feltétlenül van ilyen
  - Ha egyik bejegyzésre sem illeszkedik, akkor a célhálózat ismeretlen, így a csomagot eldobja
- Végpontokon gyakran csak két bejegyzés szerepel:
  - Helyi hálózat (a helyi végpontok közvetlenül elérhetők)
  - Alapértelmezett útvonal (minden más távoli hálózat)

# Metrika szerepe az útválasztásban

- Metrika (mérték): 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 értékkel rendelkező kapcsolaton küldjük ki a csomagot!

# Teendők helyi és távoli hálózat esetén

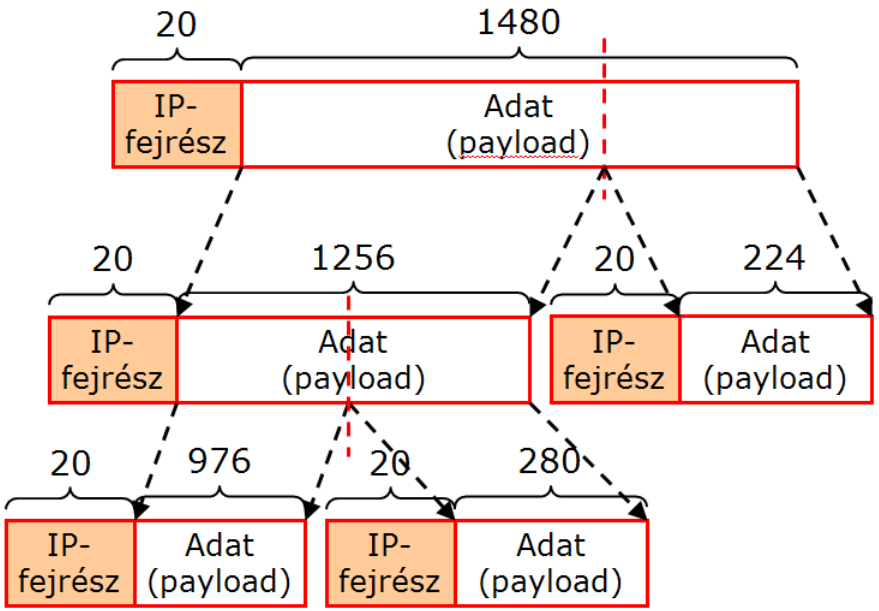
- Közvetlenül kapcsolódó (helyi) hálózat
  - A címzettnek közvetlenül küldeni
    - ⇨ Ehhez a címzett adatkapcsolati rétegbeli címére van szükség
- Nem közvetlenül kapcsolódó (távoli hálózat)
  - A megtalált „következő csomópont” útválasztónak kell küldeni
    - Az IP-címet tilos módosítani
    - Csak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

*Megoldandó feladat:*

*Velünk szomszédos állomás (csomópont vagy végpont) adatkapcsolati rétegbeli címét kideríteni annak IP címe alapján*

*Megoldás:*

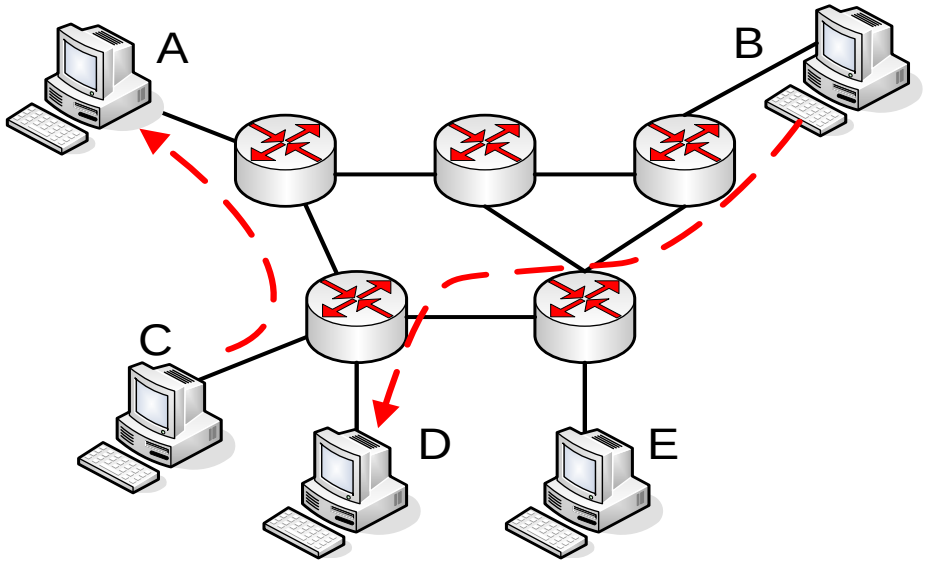
*ARP (Address Resolution Protocol)*




# IP DATAGRAMOK TÖRDELÉSE

# Az IP feladata (ismétlés)

- Hálózati protokoll által nyújtott szolgáltatás
  - Adattovábbítás a hálózat végpontjai között
- Legfontosabb funkciói
  - Címzés (addressing)
  - Csomagtovábbítás (packet forwarding)
    - az út(vonal)választási (routing) információ alapján
  - **Tördelés (fragmentation)**



# Tördelés szükségessége

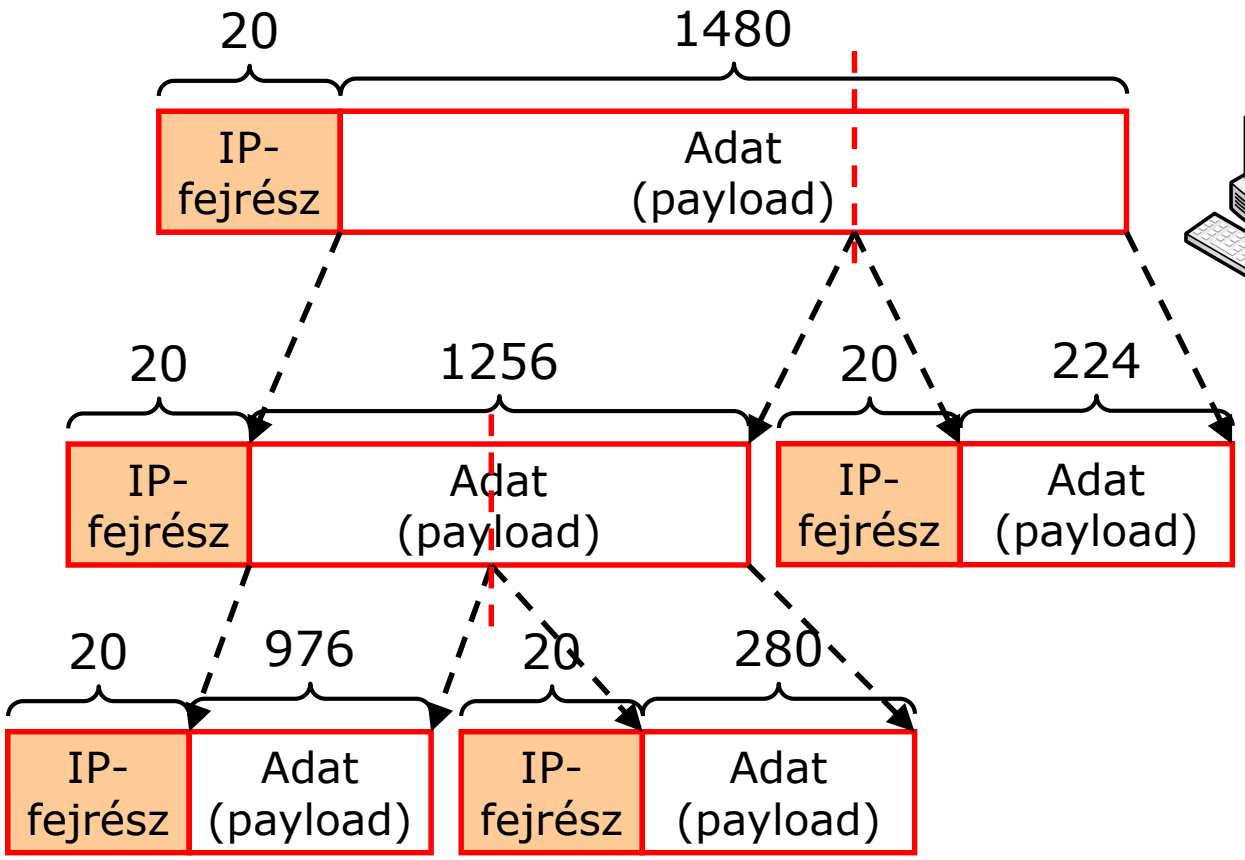
- Hálózatok alsóbb rétegei meghatározzák a keret maximális hosszát (PDU). Ebből az adatkapcsolati réteg fej- és farokrészét leszámítva kapjuk az SDU-t, amit itt MTU-nak nevezünk (Maximum Transmission Unit)
  (Ethernetnél 1500 byte)
- Eltérő technológiák ⇨ eltérő MTU-jú kapcsolatok ⇨ tördelésre lehet szükség!

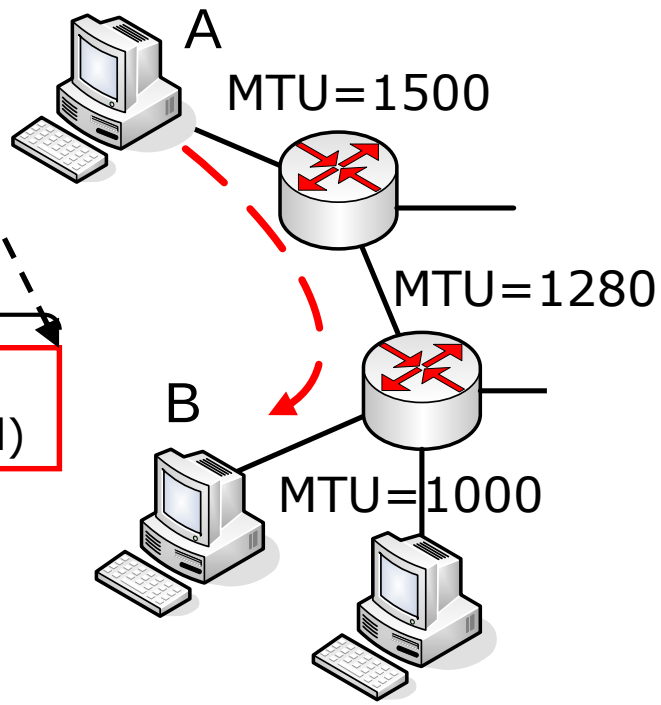
*Megjegyzés:*

*Van más lehetőség is: Előre ki lehet deríteni, hogy mi az az MTU, amit az adott útvonal során minden csomópont támogat. Lásd: Path MTU Discovery (RFC 1191)*

# A tördelés elvi megoldása példával

- A fejrészt minden csomag megkapja
- Tördelni csak 8 többszörösénél lehet



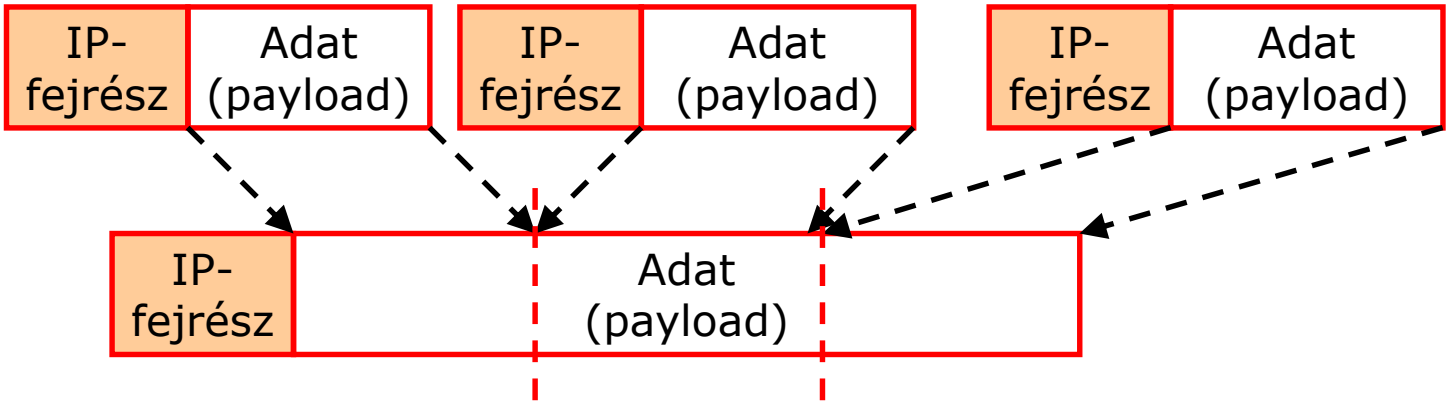



# A tördelés kivitelezése

- Ha tördelés szükséges
  - DF bit vizsgálata
    - 1 érték esetén tördelni tilos, a csomagot el kell dobni
    - 0 érték esetén a tördelés végrehajtható
  - Ha nem volt 0-tól különböző „Identification” mező érték, akkor generálni kell
  - Adat mező tördelése 8 bájtos határon, megfelelő méretű darabokra
  - Az IP fejrész mezőit bemásolni a töredékek fejrészébe
  - A tördelésnek megfelelő „Fragmentation Offset”-et beállítani a töredékekben
  - Minden csomagban az MF bitet 1-re kell állítani, kivéve annak a csomagnak az utolsó töredékét, amelyben az MF nincs beállítva

# A töredékek összeállítása

- Csak a címzett végezheti el
- Ha valamely darab nem érkezik meg, akkor a többit is eldobja
- Az IP réteg csak teljesen összeállított csomagokat továbbít a felsőbb réteg felé
- A „fragment offset”-ekből a töredék helye meghatározható



# A router feladatai (összefoglalás)

- Hibás-e a csomag (fejrésze)?
- Nekem címezték-e?
- Ismerem-e a címzett hálózatát?
  - Közvetlen kézbesítés a címzettnek
  - Átadás a következő útválasztónak
  - Eldobás
- A TTL érték csökkentés után >0?
- Kell-e tördelni? Lehet-e tördelni?
- Kell-e visszajelzést küldeni?
  ⇨ *visszajelzés küldéséhez: ICMP*

| 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 |

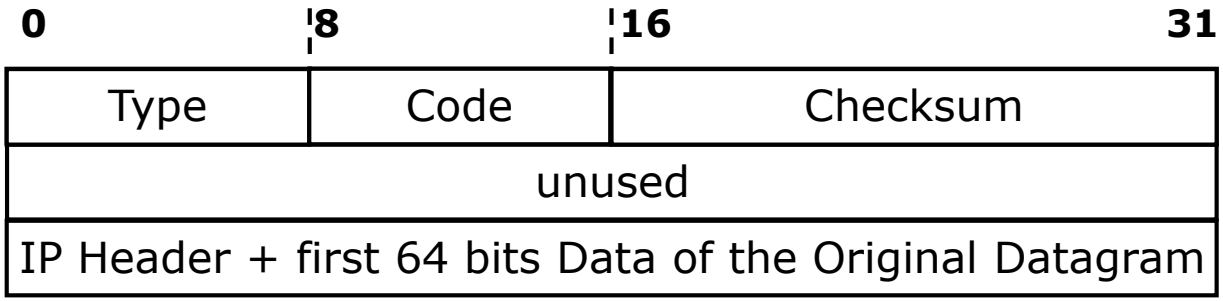
# Internet Control Message Protocol

# Internet Control Message Protocol

- Jelzés- és menedzsmentüzenetek
  - Visszajelzés a „best effort” hálózattól
- IP felett utazik (0x01-es protokollazonosító), de minden IP implementáció kötelező része!
- Üzenettípusok
  - Hiba üzenetek
  - Kérdések
  - Válaszok

# ICMP üzenetek felépítése

- Az ICMP üzenetek formátuma egyedi
- Ami közös bennük, az az ICMP fejrész első 32 bitjén található 3 adatmező
- A további rész kiosztása függ az üzenet típusától
- Példa: *Destination Unreachable* üzenet




- Hibaüzeneteknél tipikus, hogy az üzenet 64. bitjétől a hibaüzenetet kiváltó datagram fejrésze és első 64 bit adata szerepel

# Fontosabb ICMP üzenetek I.

- **Destination Unreachable** (cél nem elérhető)
  - A datagram célja valamiért nem elérhető.
  - Az okáról a Code mező értéke ad felvilágosítást
    - 0 = net unreachable
    - 1 = host unreachable
    - 2 = protocol unreachable
    - 3 = port unreachable
    - 4 = fragmentation needed and DF set
    - 5 = source route failed.
- **Time Exceeded** (időtúllépés)
  - Ha egy datagram TTL-je lejár (0-ra csökken), akkor az az útválasztó, ahol éppen a datagram tartózkodik, köteles (MUST) a datagramot eldobni.
  - Az eldobásról értesítést küldhet (MAY) a forrásnak time exceeded üzenettel
  - Ha a célállomás hiányzó szegmensek miatt nem tud összerakni egy tördelt datagramot, akkor eldobja azt, és szintén time exceeded üzenetet küldhet (MAY) a forrásnak.

# Fontosabb ICMP üzenetek II.

- **Redirect** (átirányítás)
  - Egy útválasztó megadhat a forrásnak a tőle kapott datagram *célja* felé egy rövidebb útvonalat eredményező másik útválasztót. A Code mező fejezi ki, hogy mit értünk „cél” alatt:
    - 0 = Redirect datagrams for the Network
    - 1 = Redirect datagrams for the Host
    - 2 = Redirect datagrams for the Type of Service and Network
    - 3 = Redirect datagrams for the Type of Service and Host.
  - De az eredeti datagramot az útválasztó ettől még továbbítja!
- **Echo** Request (visszhang kérés)
  - Az üzenet forrása arra kéri a címzettet, hogy küldje vissza az üzenetet
  - Az üzenet tartalmaz egy 16 bites azonosítót és egy 16 bites sorszámot
  - Opcionálisan további adatmező szerepelhet
- **Echo Reply** (visszhang válasz)
  - A visszhang kérés üzenet címzettje ezzel az üzenettel válaszol
  - Mezőit az eredeti üzenetből tölti fel (kivétel természetesen a Type mező)

# Fontosabb ICMP üzenetek III.

- **Timestamp Request** (időbélyeg kérés)
  - Az üzenet mezői tartalmazzák a visszhang kérés üzenettípus kötelező mezőit, valamint még a következő 32 bites mezőket
    - Originate Timestamp
    - Receive Timestamp
    - Transmit Timestamp
  - Az időbélyegek az éjfél óta eltelt időt tartalmazzák ezredmásodpercben mérve, UTC szerint
  - Az üzenet küldője csak az első időbélyeg mezőt tölti ki, méghozzá közvetlenül az üzenet elküldése előtt
- **Timestamp Reply** (időbélyeg válasz)
  - Az időbélyeg kérés üzenet címzettje ezzel az üzenettel válaszol
  - Kitölti a másik két időbélyeg mezőt is (rögtön érkezéskor, illetve közvetlenül a visszaküldés előtt)

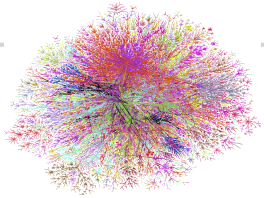
# ICMP a felhasználó számára I.

- A **`ping`** parancs
  - Egy vagy több *visszhang kérés* ICMP üzenetet küld a felhasználó által megjelölt másik gépre.
  - A címzett pedig *visszhang válasz* ICMP üzenetet küld annak a gépnek, ahonnan a kérés érkezett.
  - A felhasználó ilyen módon tesztelheti, hogy egy másik gép elérhető-e a hálózaton keresztül.
  - A ping parancs célszerűen kiírja a visszaérkező üzenetből a TTL értékét, így azt is megtudhatjuk, hogy milyen távol van a vizsgált gép (útválasztók számában mérve).
  - A ping parancs ezenkívül mérni szokta a *visszhang kérés* küldése és a vele azonos sorszámú *visszhang válasz* megérkezése között eltelt időt, így megtudhatjuk a teljes oda-vissza út idejét (RTT, *round-trip time*).

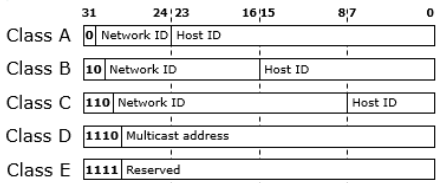
# ICMP a felhasználó számára II.

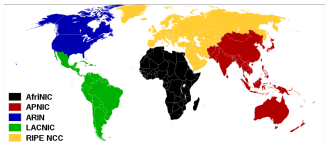
- A **`traceroute`** parancs
  - Egy távoli géphez vezető útvonal során érintett útválasztók válaszidejét deríti ki.
    - Ehhez többféle trükkös módszert is használhat, például egy elterjedt megoldás, hogy a vizsgált eszköz (router) *33434-es UDP portjára* küld egy UDP csomagot.
      - A beállított TTL-t 1-ről növeli.
      - Amíg a TTL túl kicsi, addig *time exceeded* üzenetet kap vissza valamelyik közbenső routertől.
      - Amikor pedig már elég nagy, akkor *port unreachable* üzenet érkezik (feltéve, hogy a 33434-es porton nem figyel alkalmazás, ha mégis, akkor a felhasználó választhat más portot).
    - Alternatívaként a felhasználó azt is megadhatja, hogy UDP datagram helyett ICMP *echo* üzenetet küldjön.
    - Megjegyzés: Windows 7 alatt a *tracert* parancs ICMP *echo* üzenetet küld.

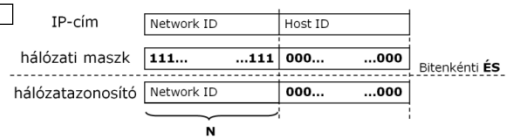
# Összefoglalás



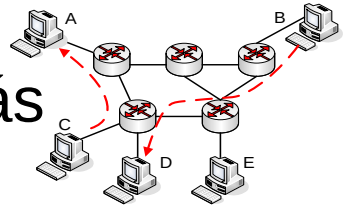
- Az IP általános jellemzői
- IP címzés
  - Osztály alapú címzés
  - Osztály nélküli címzés
  - IP címek kiosztása
- Az IP datagramok felépítése
- Csomagtovábbítás
- Datagramok tördelése
- ICMP
  - `ping, traceroute`

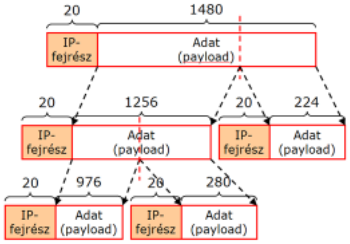



| VER | IHL | ToS | Total Length |
|---|---|---|---|
| Identification | | Flags | Fragment Offset |
| TTL | Protocol | Header Checksum | |
| Source Address | | | |
| Destination Address | | | |
| Options | | | Padding |
| Adat (Payload) | | | |




| 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 |

# Kérdések?

## KÖSZÖNÖM A FIGYELMET!

Hálózati Rendszerek és Szolgáltatások Tanszék

Dr. Lencse Gábor
tudományos főmunkatárs
BME Hálózati Rendszerek és Szolgáltatások Tanszék
lencse@hit.bme.hu