Számítógép-hálózatok
A gyakorlatban elterjedt hálózati architektúrák

2025/2026. tanév, I. félév

Dr. Kovács Szilveszter

E-mail: szilveszter.kovacs@uni-miskolc.hu

www.iit.uni-miskolc.hu/~szkovacs

Informatika Intézet 107/a.

Tel: (46) 565-111 / 21-07

A hálózati architektúra

- **Rétegek és protokollok halmaza**
- **Elegendő információ az implementációhoz**
- **Nem része sem a részletes implementáció, sem az interfészek specifikációja**
  (ezek a konkrét implementáció során tervezői döntések).

Mai főbb témák

- **Protcol stack-**ek, más néven **protokoll hierarchiák,** illetve **protokollszövetek. Pl:**
  - **TCP/IP: Internet – világháló!** (Ez és csak ez!)
  - **IPX/SPX: Novell NetWare.**
  - **NetBEUI/NetBIOS: Microsoft**
    (NetBEUI: NetBIOS Extended User Interface – nem routeolható (nincs hálócím) – csak kis LAN-ok (MS))
  - **BanyanVines, DecNet stb.**

  } **LAN**

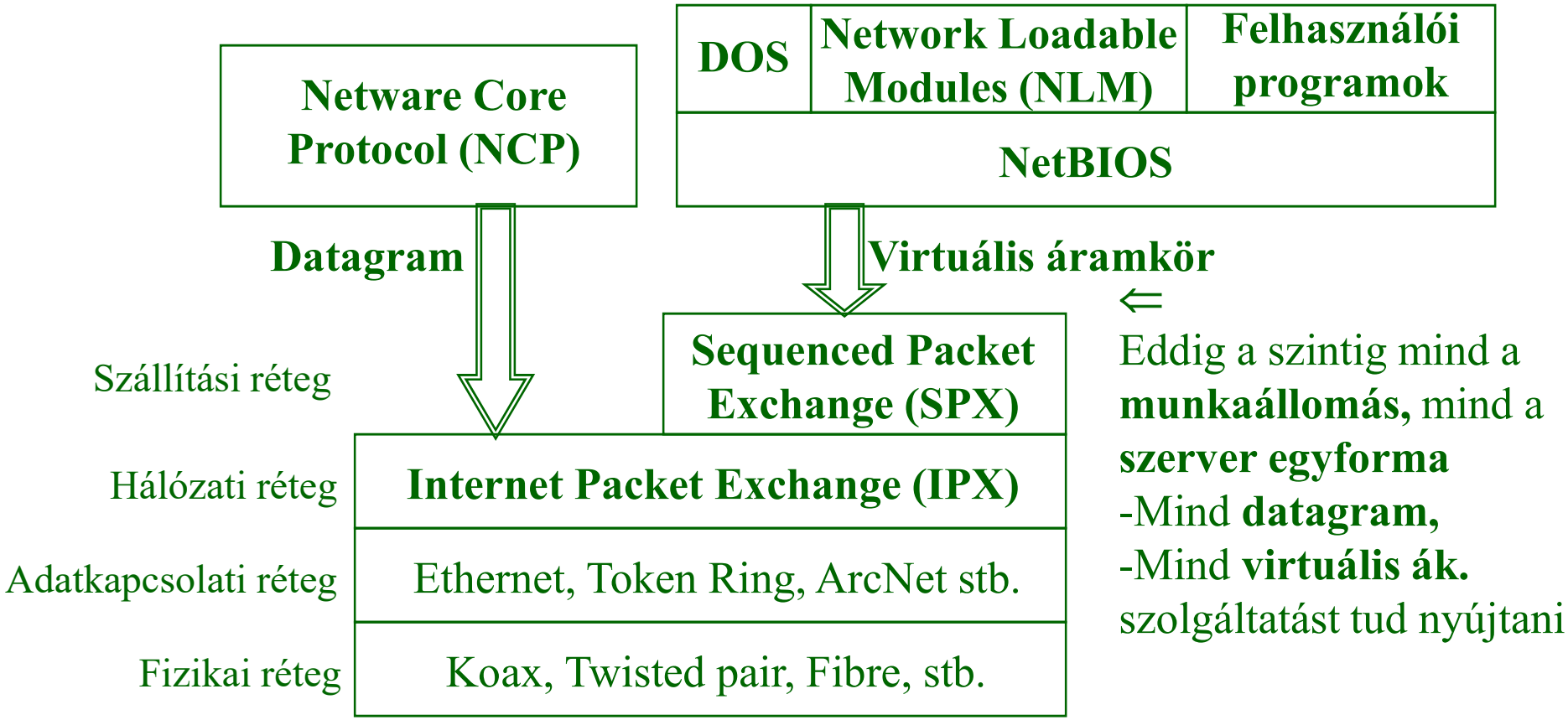
- **Bővebben:**
  - **Novell Netware (IPX/SPX)**
  - **Internet (TCP/IP)**

Novell Netware: IPX/SPX protocol stack

- Eredetileg csak erőforrás megosztás, mint
  - File-rendszer és
  - nyomtató.
- A hálózat
  - szerver(ek)ből és
    - dedikált vagy nem dedikált (az ő erőforrásait osztják meg)
  - munkaállomásokból áll.
- De! Kommunikációs szempontból egyenrangúak (egyformák)
- A „Network Operation System”, vagy „hálózati operációs rendszer” – Novell elnevezés

Novell Netware: IPX/SPX protocol stack

- **Az IPX/SPX az XNS-en alapszik** (Xerox Network System)

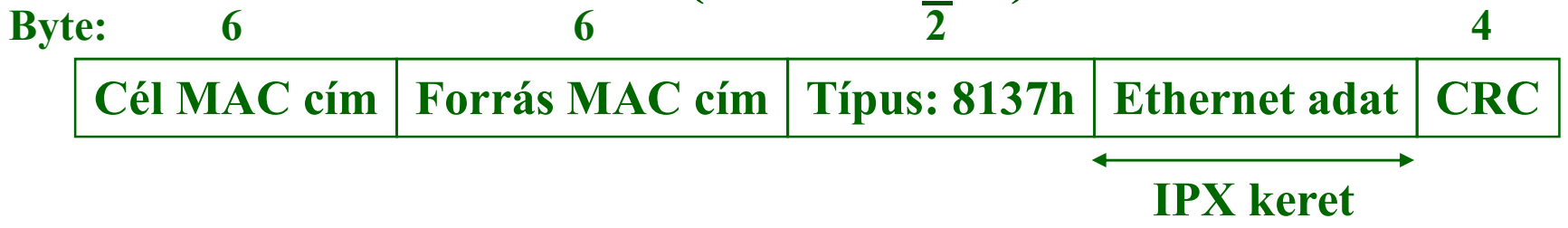


⇐

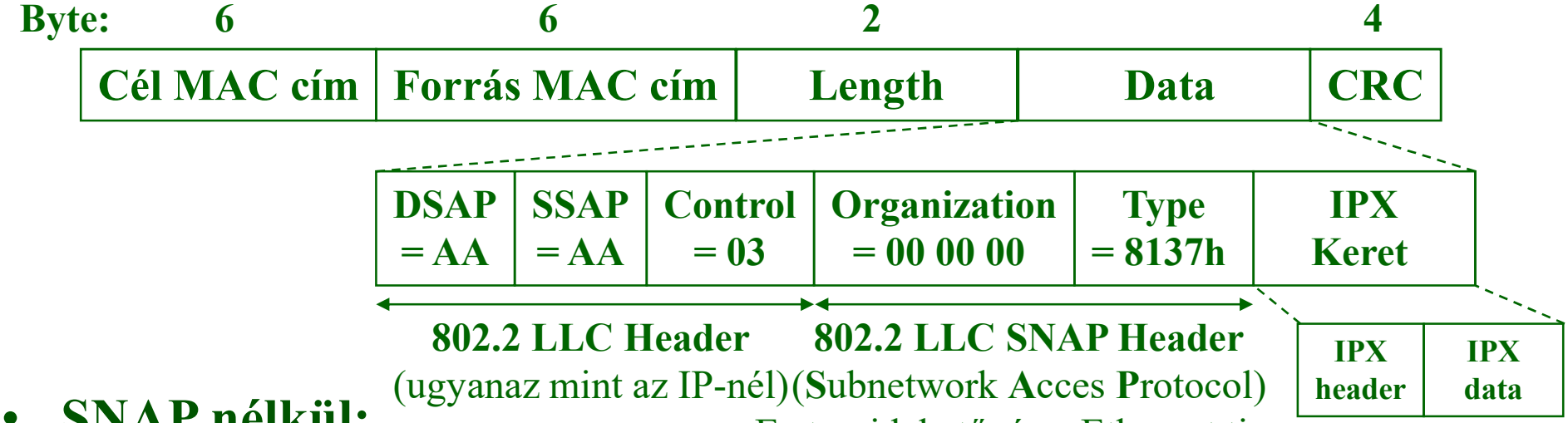
Eddig a szintig mind a **munkaállomás,** mind a **szerver egyforma**
-Mind **datagram,**
-Mind **virtuális ák.**
szolgáltatást tud nyújtani

IPX keretformátum

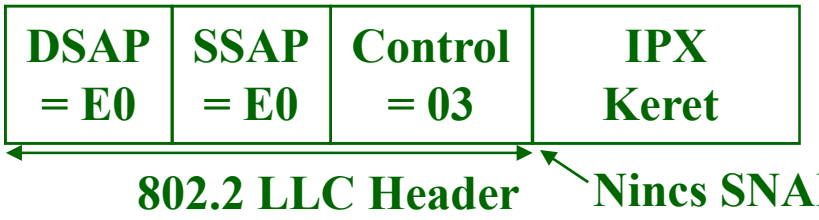
- **IPX enkapszuláció** (encapsulation) **az adatkapcsolati rétegben**
- **Ethernet keretformátum (Ethernet_II) esetén:**



- **802.3 keretformátum (802.2 LLC + SNAP) esetén:**

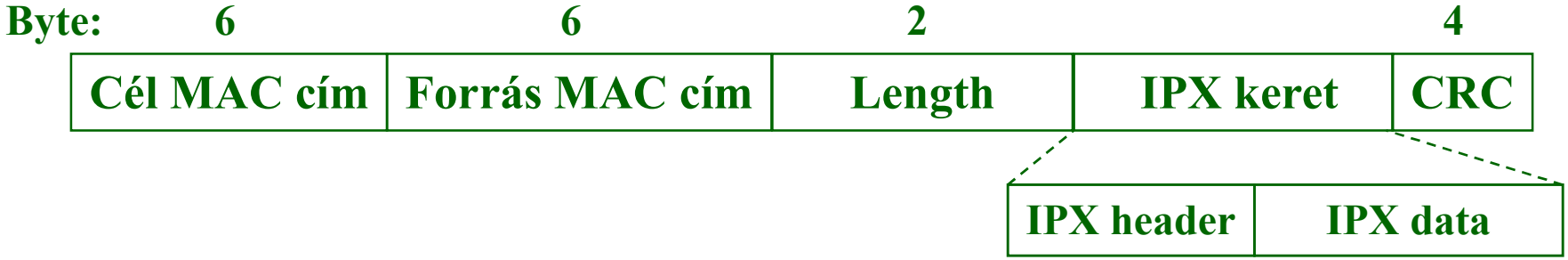


- **SNAP nélkül:**



IPX keretformátum

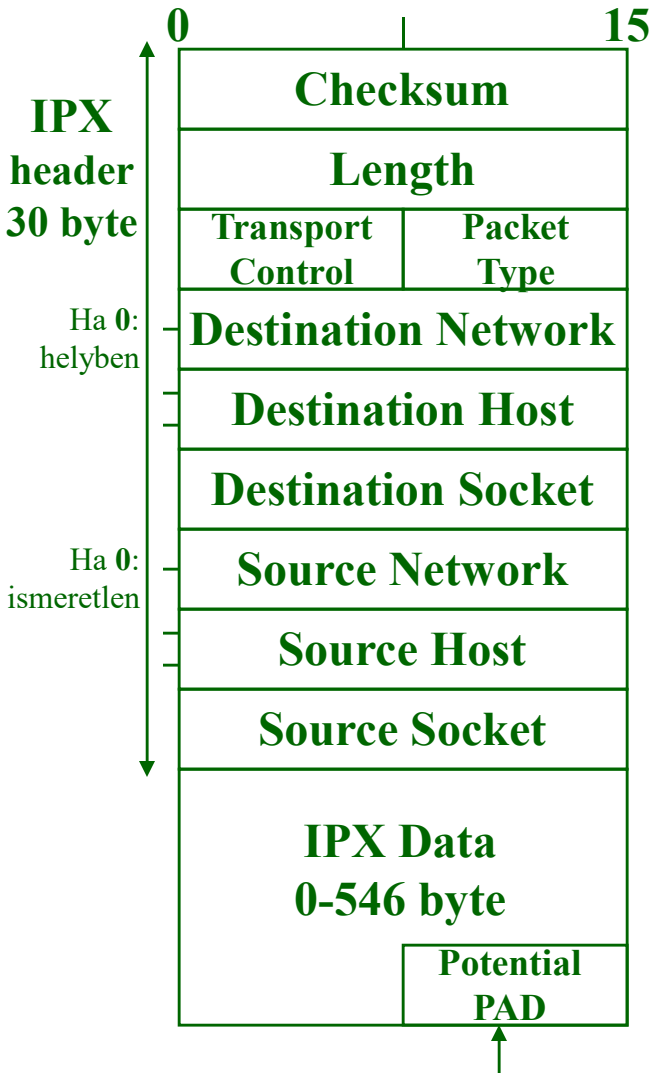
- **IPX enkapszuláció** (encapsulation) **az adatkapcsolati rétegben**
- **802.3 keretformátum (802.2 LLC nélkül) esetén:**



- **Hátrány: Nincs jelölve a tipusa!**
  ⇒ Csak akkor lehet így, ha csak IPX van a hálózaton.

IPX keretformátum

IPX keret:



Párosra egészíti ki a byte számot (de nincs benne a hosszban).

IPX címformátum Pl:

&00000025 %080002001216 !5

Network Number **Host Number** **Socket Number**

Network Number: 32 bit (4byte)

- Egyedi hálózat azonosító (route-olható).
- Nem támogatja a hierarchikus címzést (tipikusan LAN)

Host Number: 48 bit (6byte) – MAC cím

Socket Number: 16 bit – szolgálat elérési pont

Pl: **1:** Routing Information, **2:** Echo, **3:** Router Error
0451: Netware File Server, **0452:** Netware SAP
0453: Netware RIP (Routing Information Protocol), **stb.**

Transport Control: 0000xxxx – 4bit hop counter

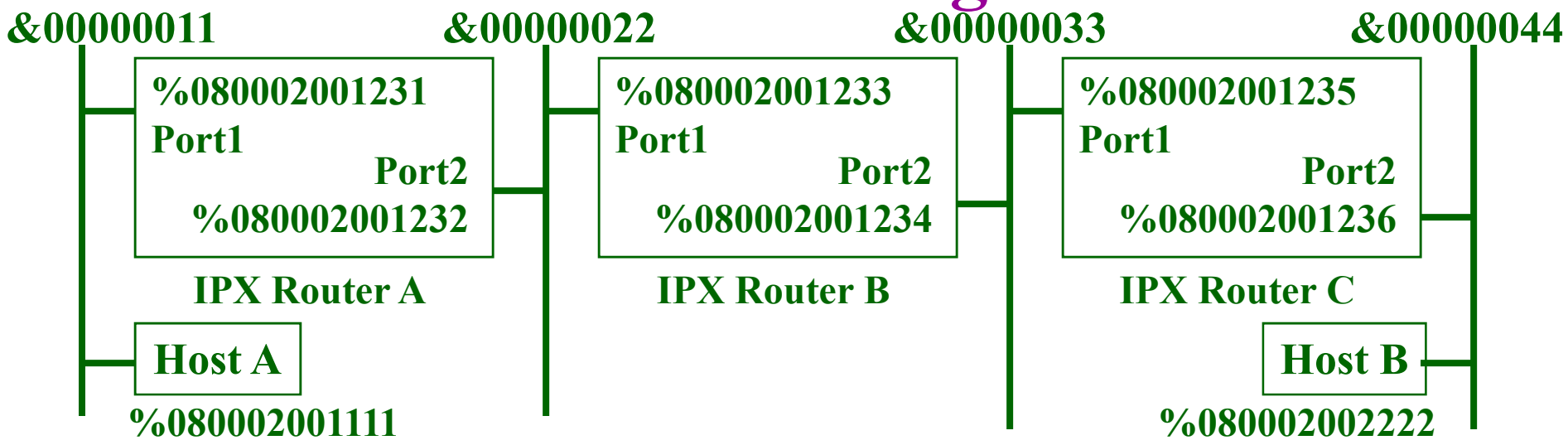
Packet Type: az adatok tipusát határozza meg

Pl: **0:** Unknown, **1:** Routing Information packet **2:** Echo packet,
3: Error packet, **4:** Packet Exchange, **5:** Sequence Packet Protocol

IPX routing

- **A router-eket itt „bridge”-nek hívják**
- **Valamennyi táblázat, amely tartalmazza valamennyi hálózat elérési irányát.**
- **Beállításuk vagy kézzel (statikus routing), vagy (és) elosztott dinamikus módon:**
  IPX RIP: IPX Routing Information Protocol
  (A szomszédok táblát cserélnek.)

IPX routing



IPX Frame:

(A→B)

DNet	DHost	DSock	SNet	SHost	SSock	IPX
&44	%080002002222	!451	&11	%080002001111	!B9	DATA

Datalink Frame (Ethernet): **Router A-nak küldi Host A**

Dest MAC	Source MAC	Type:	Ethernet Data:	CRC
%080002001231	%080002001111	8137h	IPX Frame	

Datalink Frame (Ethernet): **Router B-nek küldi Router A**

Dest MAC	Source MAC	Type:	Ethernet Data:	CRC
%080002001233	%080002001232	8137h	IPX Frame	

Nem (alig, csak a hop counter, checksum) változik! Majdnem ugyanazt az IPX keretet adják tovább.

Internet: TCP/IP protocol stack

- Hierarchikus címzés is lehetséges
- Világméretű hálózat alakítható ki belőle
- Újabb elnevezések:
  - Internet: „külső” hálózat (WAN)
  - Intranet: „belső” hálózat (LAN)
- Általános hálózati kommunikációs szolgálatok készletét biztosítja
- A szolgálatok szabványosítottak, és ma már szinte valamennyi OS-re implementálták
- ARPANET 1969-1990 (1983 MILNET kiválik)
- 1978- Magyarország ARPANET elérés

Internet Technical Bodies (technikai testületek)

- **ISOC - Internet Society. (1992-)**
  Professzionális közösség az Internet kutatási és oktatási felhasználásának támogatására.
- **IAB - Internet Architecture Board.**
  Az ISOC alá tartozó technikai koordinációs testület.
- **IETF - Internet Engineering Task Force.**
  Meglévő protokollok és specifikációk standardizálása.
  Évente háromszor, munkacsoportokban (working groups) ülésezik.
- **IRTF - Internet Research Task Force.**
  Kutatás orientált csoport.

Internet adminisztráció

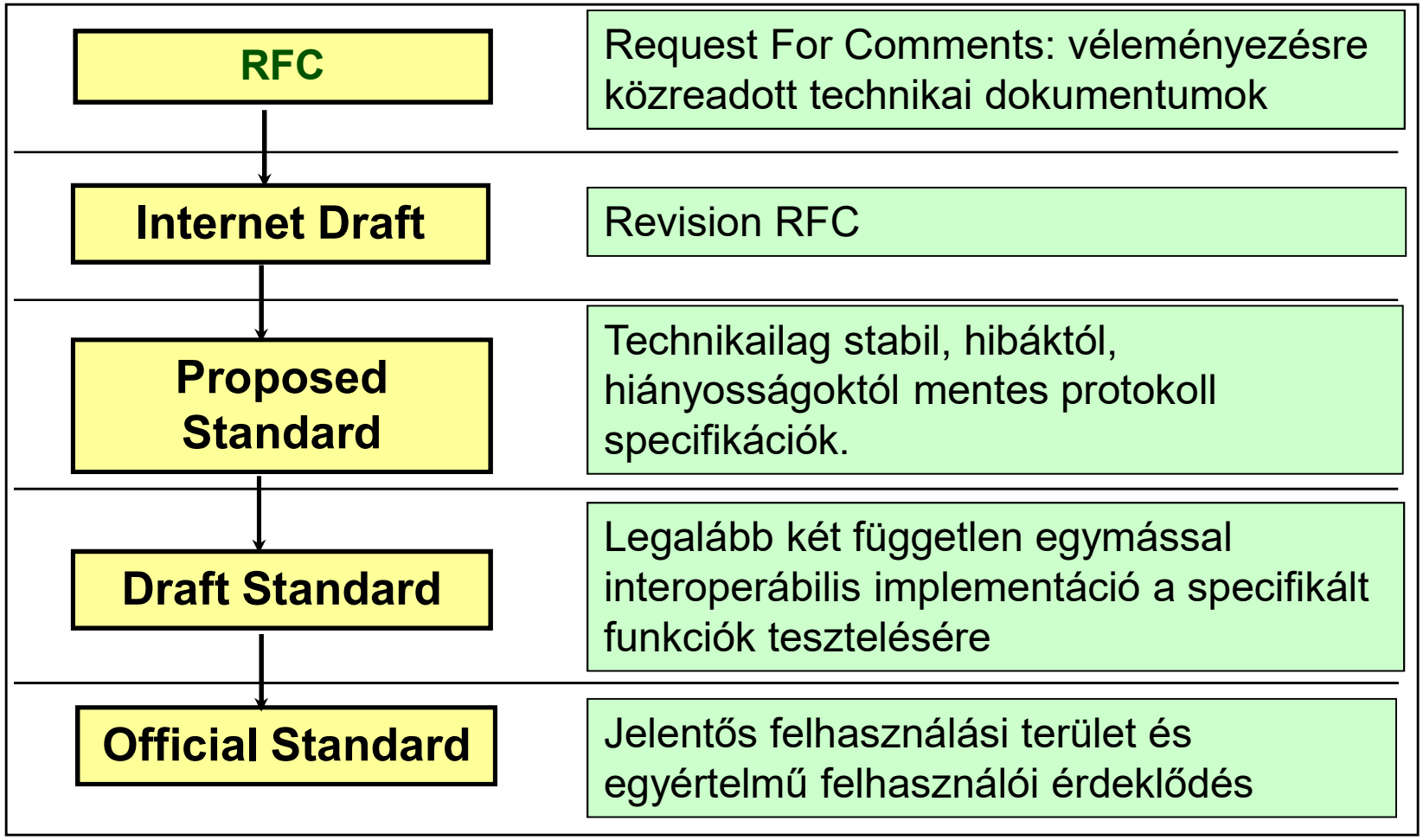
- **USA:**
  - **DDN (Defense Data Network) – az Internetért felelős kormányszervezet**
  - **NOC (Network Operations Center) – kommunikációs linkekért felel**
  - **DDN NIC (Network Information Center)**
    - **TCP/IP protokollal összefüggő anyagok gyűjtése és terjesztése**

IANA Internet Assigned Numbers Authority

  - **Az egész világon egyedi hálózati címek, Domain nevek és szolgálat azonosítók kiosztása**

- **Regionális szervezetei (Regional Inrenet Registries):**
- **RIPE NCC (www.ripe.net) Réseaux IP Européens Network Coordination Centre – Európa, Közel-Kelet, Észak-Afrika**
- **ARIN (www.arin.net) American Registry for Internet Numbers**
- **APNIC (www.apnic.net) Asian Pacific Network Information Centre**

IAB szabványosítási folyamat



Protocol Status Levels

- **Valamennyi TCP/IP protokoll az alábbi öt állapot valamelyikében van:**
  - **Required – szükséges**
  - **Recommended – ajánlott**
  - **Elective – választható**
  - **Limited use – részlegesen használható**
  - **Not recommended – nem ajánlott**

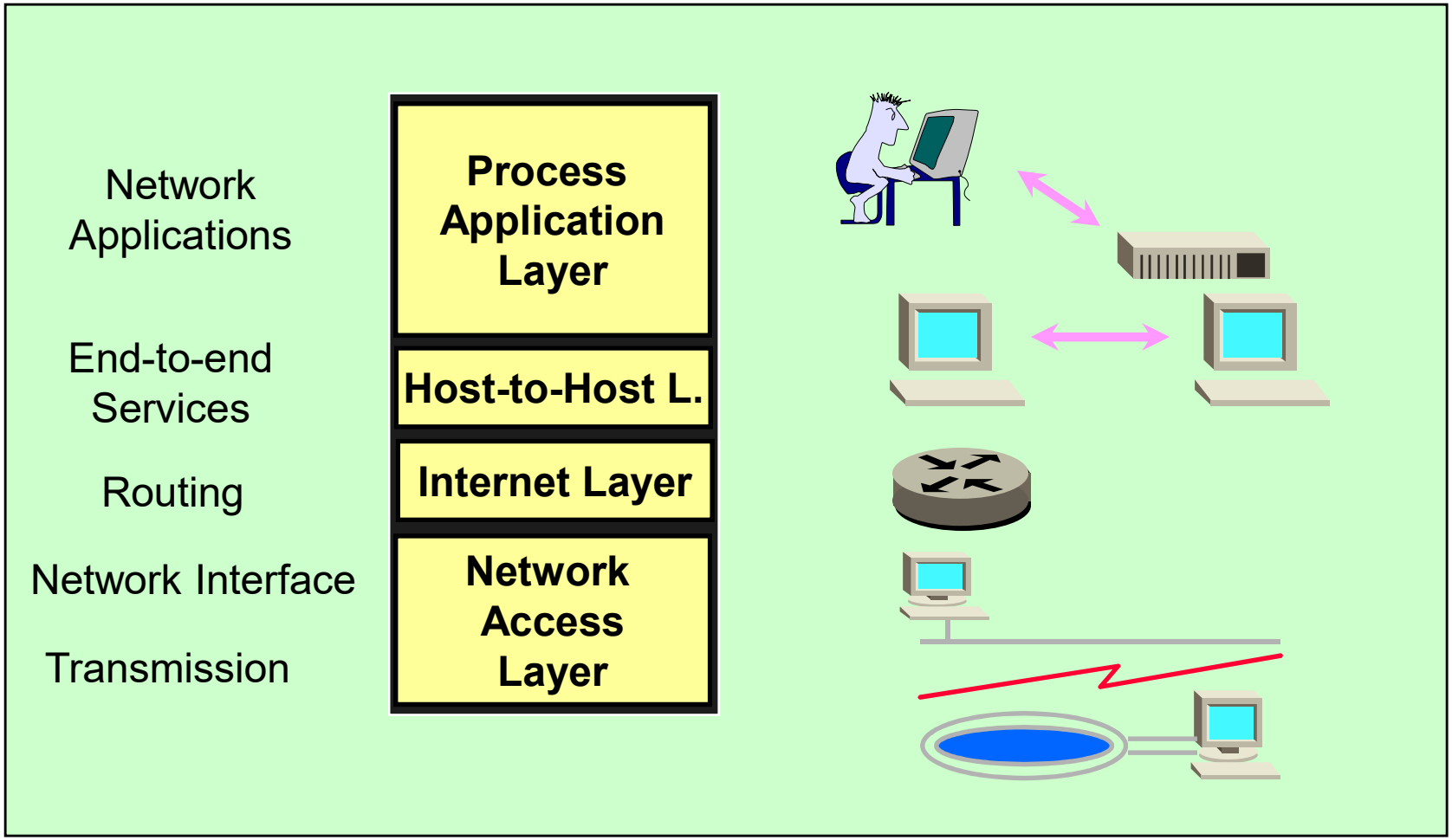
Internet dokumentumok

- **RFC**
  - **RFC XXXX – több mint 2500 létezik belőle**
  - **A frissített RFC-k új RFC számmal jelennek meg**
  - **Nem mindegyik RFC ír le protokollokat és nem mindegyiket használják**
  - **ftp://ds.internic.net**
- **STD (STandDard)**
  - **hivatalos Internet standard**
- **FYI (For Your Information)**
  - **RFC-k, amik nem protokoll leírást tartalmaznak**

RFC dokumentum fejléc minták

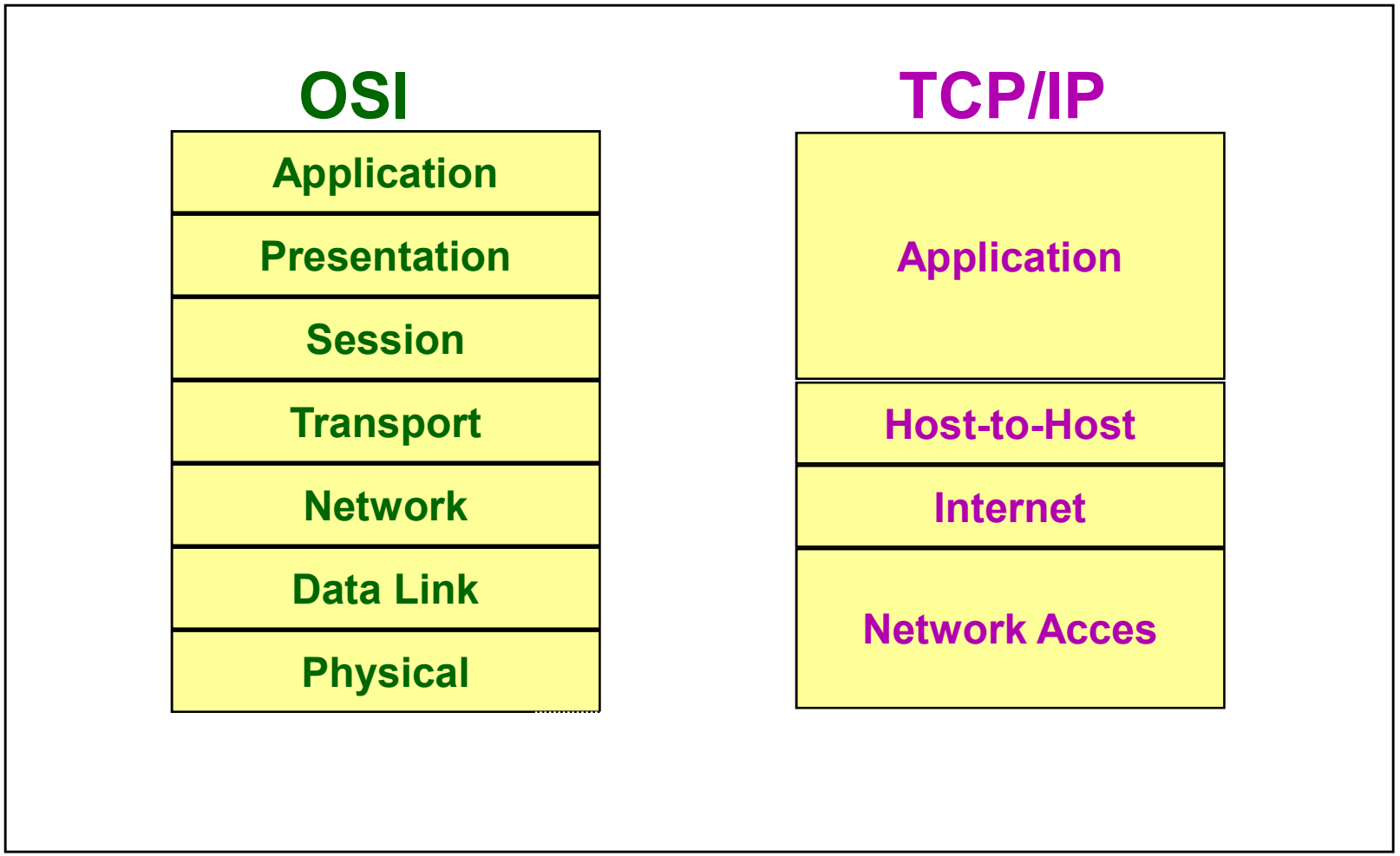
- **RFC**
  - **2030 I D. Mills, "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", 10/30/1996. (Pages=18) (Format=.txt) (Obsoletes RFC1769)**
  - **1879 I B. Manning, "Class A Subnet Experiment Results and Recommendations", 01/15/1996. (Pages=6) (Format=.txt)**
- **FYI**
  - **0023 Guide to Network Resource Tool. EARN Staff. March 1994. (Format:TXT=235112 bytes) (Also RFC1580)**
  - **0028 Netiquette Guidelines. S. Hambridge. October 1995. (Format: TXT=46185 bytes) (Also RFC1855)**

Az Internet hivatkozási modell (DoD)

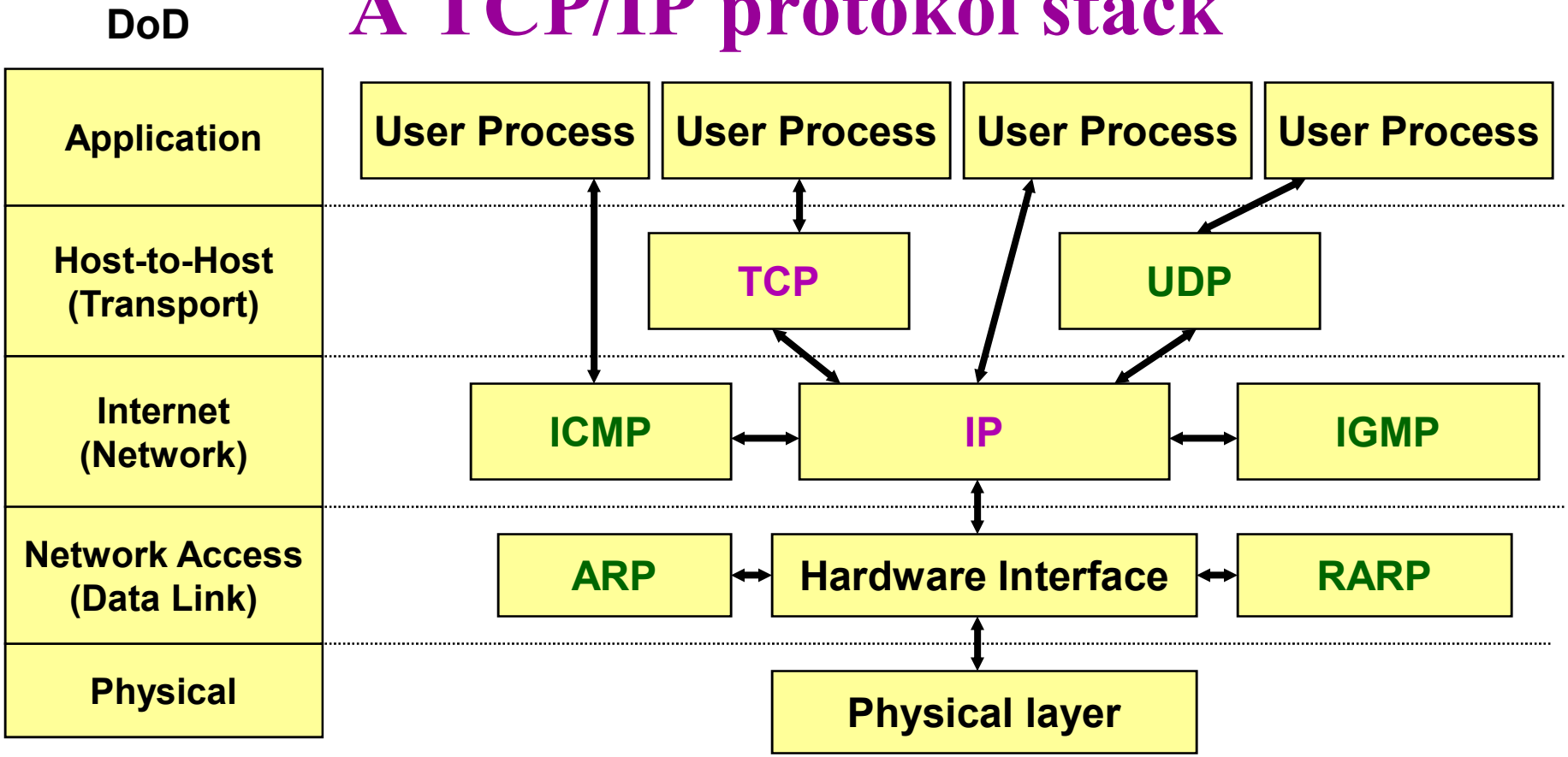


Az ISO/OSI és a DoD modellek

DoD (Department of Defense)



A TCP/IP protokol stack



Szállítási réteg:

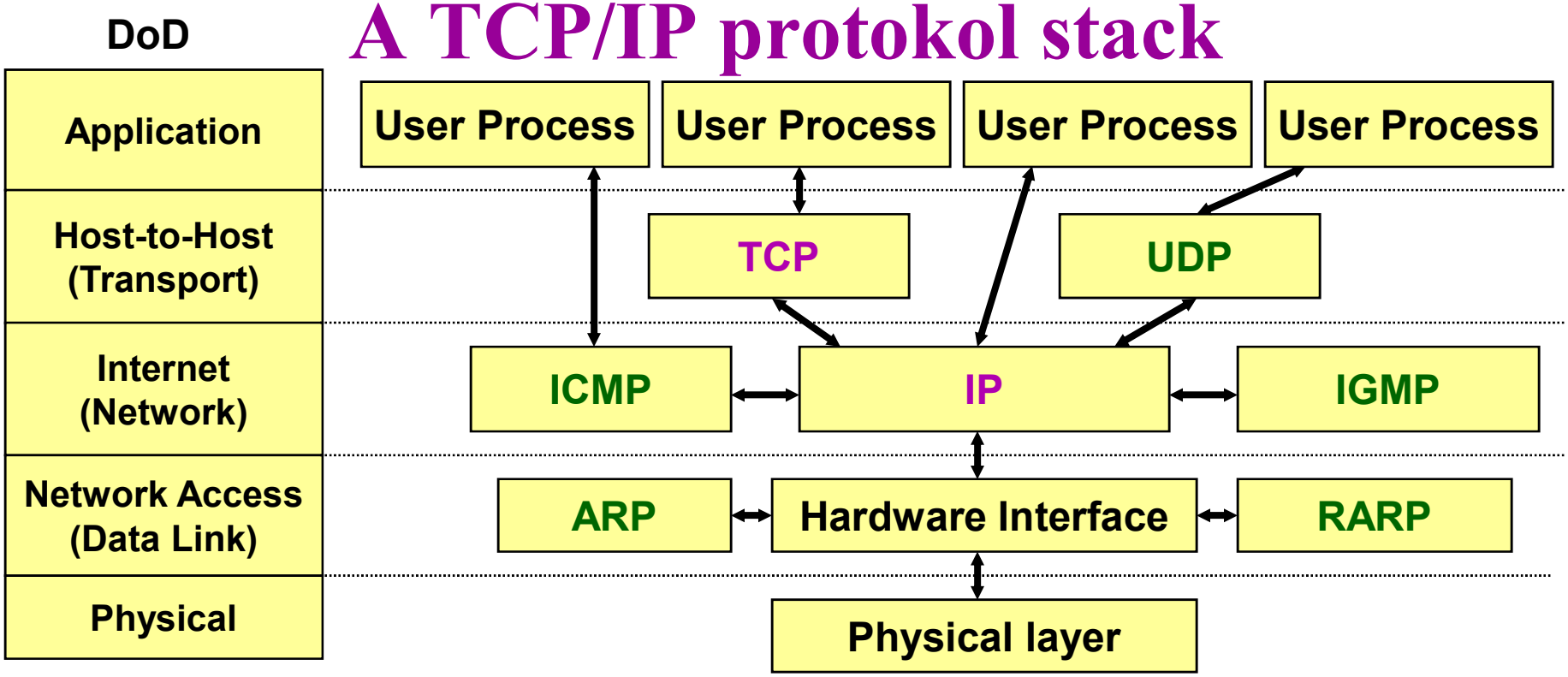
TCP: Transmission Control Protocol (Telnet, Rlogin, FTP, SMTP)

→ megbízható adattovábbítás (összeköttetés alapú szolgálat)

UDP: User Datagram Protocol (TFTP, SNMP, DNS (TCP is))

→ összeköttetés-mentes datagram szolgálat

A TCP/IP protokol stack



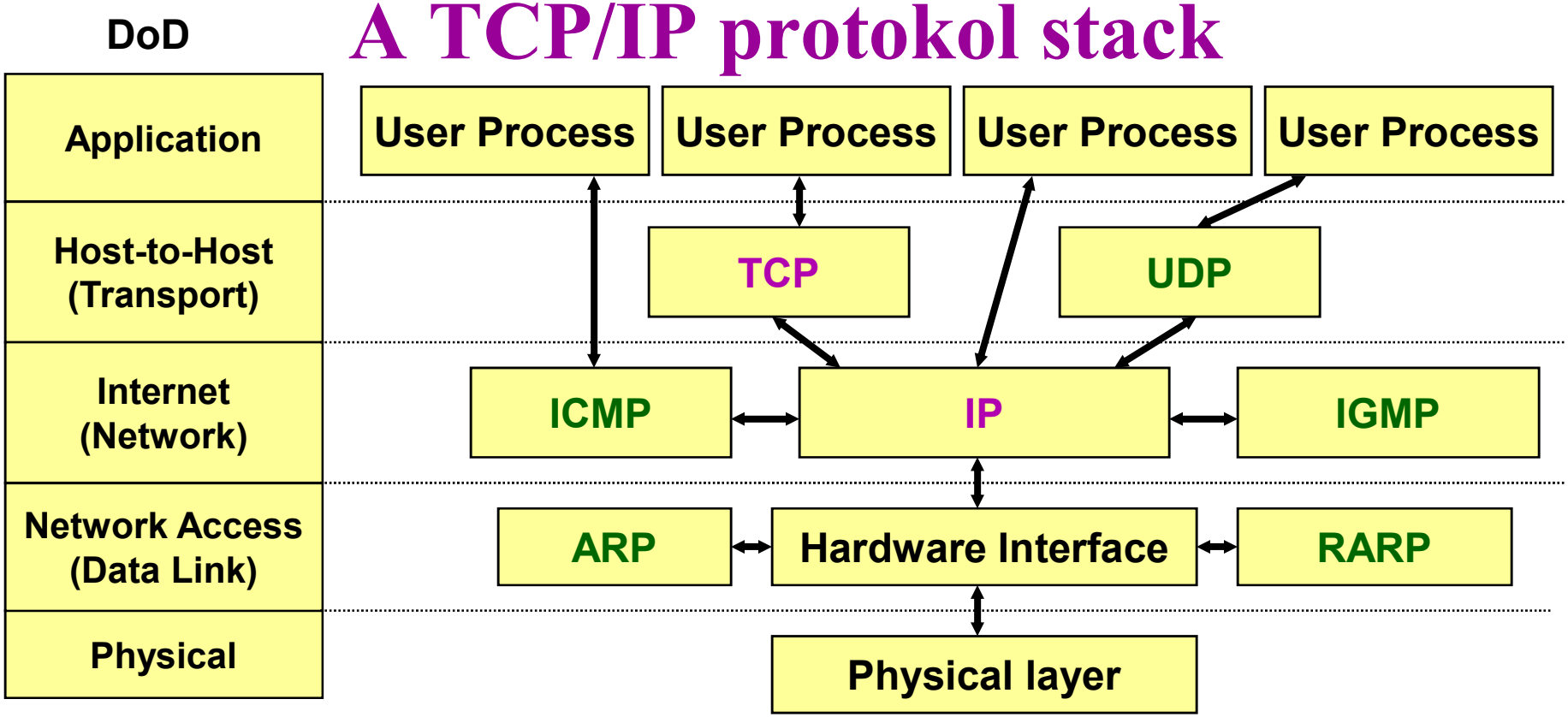
Hálózati réteg:

IP: Internet Protocol → összeköttetés-mentes datagram szolgálat változó méretű csomagokra → Best effort delivery (a telhető legjobb): változó késleltetés, hiba, adatvesztés
→ kapcsolódhat hozzá alkalmazói program közvetlenül, de ritka

ICMP: Internet Control Message Protocol → a hálózati réteggel kapcsolatos üzenetek (pl. Router csomageldobás esetén visszaüzen)
→ lehet közvetlen alkalmazói program kapcsolat (pl. ping –echo request/reply)

IGMP: Internet Group Management protocol
→ multicasting (többes címzés)-el kapcsolatos üzenetek

A TCP/IP protokol stack



Adatkapcsolati réteg:

Hardware interface: megbízható csatorna kialakítása

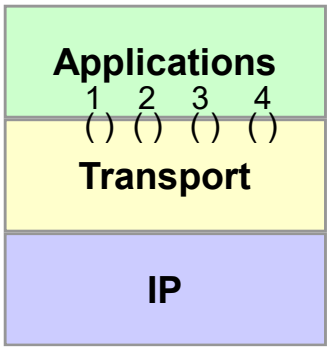
→ keretképzés, hibavédelem, adatfolyam vezérlés, kapcsolat menedzsment

ARP: Address Resolution Protocol

RARP: Reverse Address Resolution Protocol (gond: L2, leváltja a BOOTP, DHCP: UDP)

→ Ethernet Broadcast → MAC címek ↔ IP címek közötti kétirányú megfeleltetés

A TCP és UDP SAP azonosítás



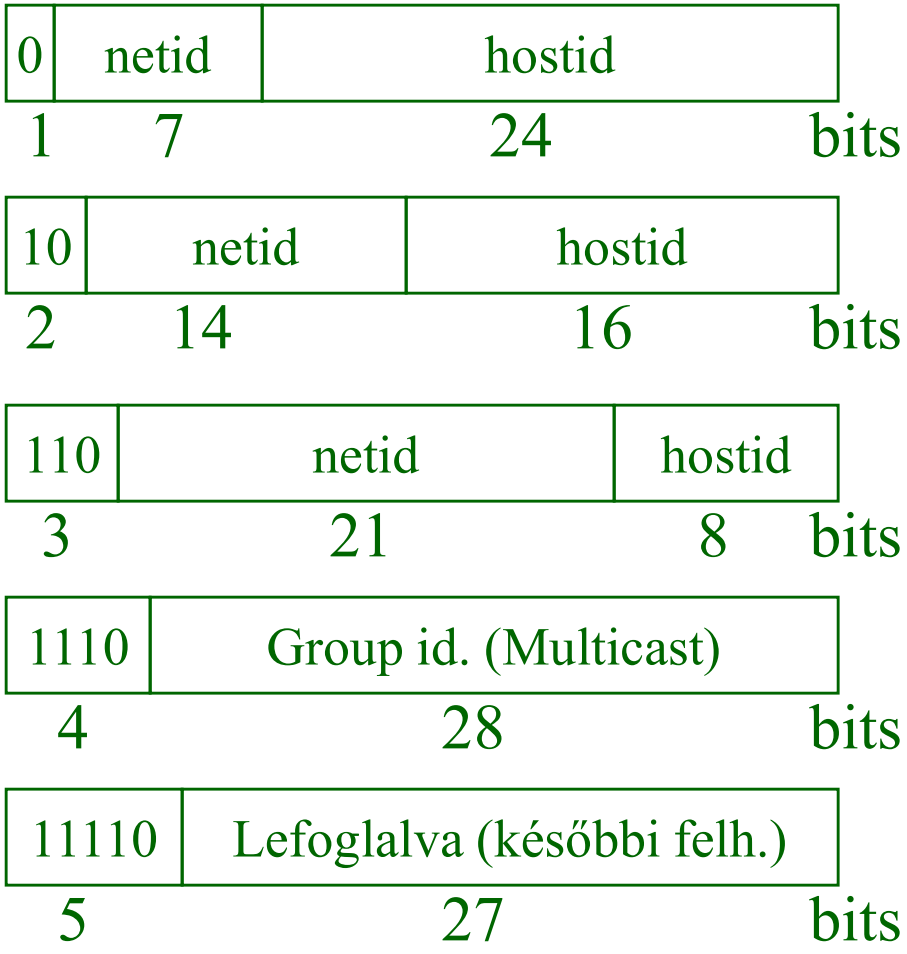
- **A szolgáltatott alkalmazásokat 16 bites portszámokkal azonosítják**
  (SAP Service Access Point)
  - **0 --not used**
  - **1-255 --Reserved ports for well-known services (IANA)**
  - **256-1023 --Other reserved ports**
  - **1024-65535 --user-defined server ports**
- **Unix stores general used port in /etc/services**
  Pl:
  - **telnet TCP: 23; ftp TCP: 20(data), 21(control); tftp UDP: 69;**
  - **http: 80; smtp: 25; stb.**

Internet címek

- **32 bit, 4 byte**
- **Pontok közötti decimális alak**
  (Dotted decimal notation - egészen jól olvasható)
  164.107.134.5
  10100100.01101011.10000110.00000101 (bin)
  A4:6B:86:05 (hexa)
- **Max címszám: 2^{32} = 4 milliárd csomópont**
- **Class A Networks = 15 millió csomópont**
- **Class B Networks = 64K csomópont**
- **Class C Networks = 254 csomópont.**

IP címosztályok

- **Hierarchia: hálózat cím + hoszt cím (netid+hostid)**
- **Class A**
  0.0.0.0 - 127.255.255.255
- **Class B**
  128.0.0.0 - 191.255.255.255
- **Class C**
  192.0.0.0 - 223.255.255.255
- **Class D** (többes címzés)
  224.0.0.0 - 239.255.255.255
- **Class E**
  240.0.0.0 - 247.255.255.255



multicast: többes címzés ⇒
az üzenet a multicast csoport minden tagjának szól (broadast → mindenkinek szól)

IP címtér

Osztály	Oszt.+hálózati bitek száma	Hálózatok száma	Gép bitek száma	Gépek száma	Címmező foglalás
A	1 + 7	$2^7 - 2 = 126$	24	$2^{24} - 2 = 16777214$	49,21%
B	2 + 14	$2^{14} = 16384$	16	$2^{16} - 2 = 65534$	24,99%
C	3 + 21	$2^{21} = 2097152$	8	$2^8 - 2 = 254$	12,40%
D Multicast	4 + 28	$2^{28} = 268435456$	-	-	6,25%
E Fenntartva	4	-	32 - 4	$2^{28} - 1 = 268435455$	6,25%

Speciális címek és jelentésük

- **Nem minden cím osztható ki állomáscímnek**

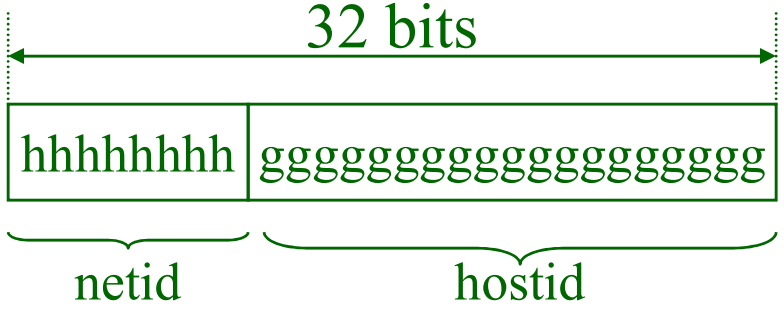
Hálózat bitek	Gép bitek	Jelentés
..0..	..0..	Ideiglenes forrás cím, amíg nem tanulja meg a gép a címét. Nem szabad célcímként használni. Default route: 0.0.0.0
..1..	..1..	Broadcast, mindenki ezen a helyi fizikai hálózaton. MAC broadcast keretben kell küldeni.
x	..0..	Ez a logikai hálózat. Korábban logikai broadcast.
x	..1..	Directed broadcast, mindenki ezen a távoli hálózaton. Távolról MAC unicast keretben kell
127.0.0	x	Loopback, a helyi TCP/IP stack pszeudó címe a hoszton belül. A hálózaton nem fordulhat elő.
224.0.0.2	-	Multicast, az összes router ezen a hálózaton van.

Klasszikus címzés összefoglaló

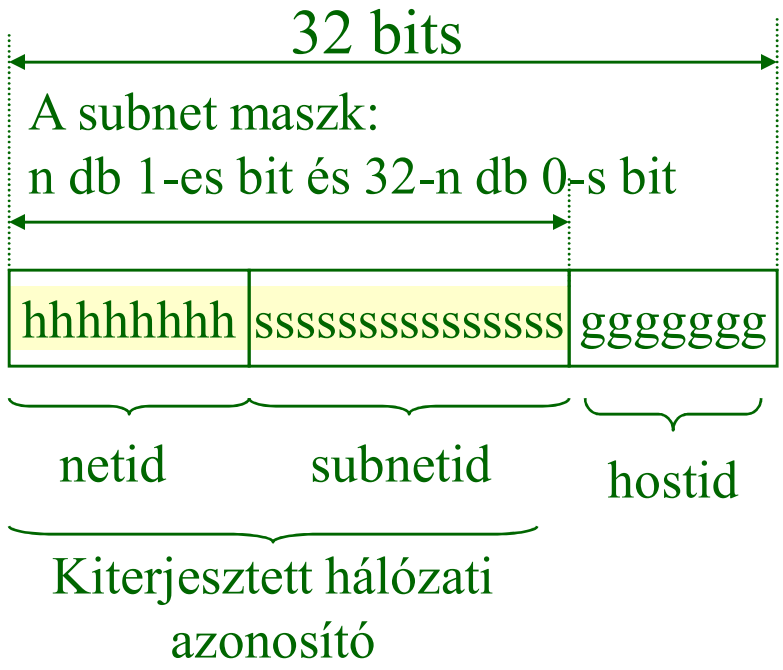
- A cím egyértelműen két részre bontható
  - az első bitek megmondják, hol a határ
  - ugyanakkor merev bit-határok
  - broadcast cím egyértelműen számítható (a host id. csupa 1-es)
- Igény a címzési hierarchia bővítésére
  - Intézményi hálózatok fejlődése
  - a pazarló A és B osztályok elfogytak
  - pont-pont kapcsolatokra teljes C osztály

Alhálózat (subnet) bevezetése

- **Az eredeti felosztás**



- **A subnet maszkkal a**
  - **hálózat bitjeit jelöljük**



Alhálózat címzések

- A (sub)net maszk (RFC 950)
- A kiterjesztett hálózati azonosító hosszabb lehet, mint a címosztály hálózati azonosítója!
- C osztályú címnél a default maszk: 255.255.255.0
- A prefix jelölés:
  - 193.6.5.0/24
    - 193.6.5.0
    - 255.255.255.0

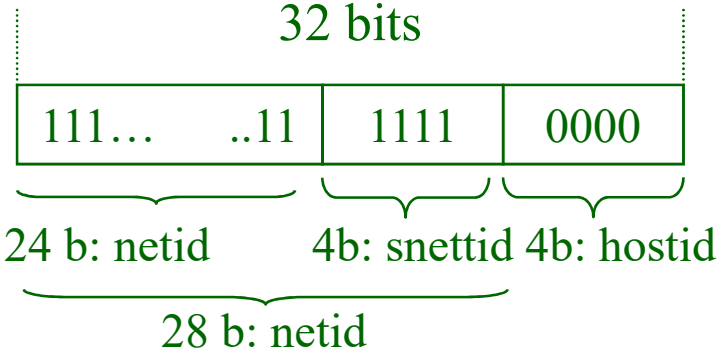
Osztály	Prefix	Netmask
A	/8	255.0.0.0
B	/16	255.255.0.0
C	/24	255.255.255.0

A subnetting eredménye

- **A címező jobb kihasználása**
  - **pont-pont kapcsolatok 2 biten elférnek**
  - **több LAN befér egy IP hálózatba**
- **A cím nem tartalmazza a hálózat-azonosítót**
  - **A maszkot is jól kell konfigurálni**
    - **a broadcast cím nem található ki az IP címből**
  - **A maszkot is kell továbbítani (plussz 4 byte az útvonal-választási információkban)**
  - **De az útvonalválasztás egyszerűsödhet** (pl. hálózatok összefogása „szupernetting”)

A címfeldolgozás

- Pl 193.6.5.1 IP címből a
  - /24 (255.255.255.0) maszk és az and logikai művelet leválasztja a hálózati címet
  - a /24 maszk negáltjának és az and logikai művelet leválasztja a gép címet
- Ha a szubnet maszk hosszabb
  - Pl. /28: 255.255.255.240, akkor
    - 28 bits: net
    - 4 bits: host



- Ha rövidebb, mint a címosztályé: „supernetting”
  - több hagyományos osztály összefogása
  - Pl. 16 C összefogása: /20: 255.255.240.0

Alhálózat címkiosztási példa

- **Adott 193.6.5.0/24; és bontsuk öt egyforma méretű alhálózatra!**
  - **$2^2 < 5 < 2^3 \rightarrow$ 3 subnet bit kell $\rightarrow$ /27 a prefixes (255.255.255.224) jelölés $\rightarrow$ valójában 8 alhálózatra osztunk**

Bitminta	Címtartomány	Megjegyzés
11000001|00000110|00000101|000xxxxx	193.6.5.0/27	Subnet 0/All zeros *
11000001|00000110|00000101|001xxxxx	193.6.5.32/27	Subnet 1
11000001|00000110|00000101|010xxxxx	193.6.5.64/27	Subnet 2
11000001|00000110|00000101|011xxxxx	193.6.5.96/27	Subnet 3
11000001|00000110|00000101|100xxxxx	193.6.5.128/27	Subnet 4
11000001|00000110|00000101|101xxxxx	193.6.5.160/27	Subnet 5
11000001|00000110|00000101|110xxxxx	193.6.5.192/27	Subnet 6
11000001|00000110|00000101|111xxxxx	193.6.5.224/27	Subnet 7/All ones *

*** Ezeket régen nem volt szab használni!**

Alhálózat címkiosztási példa /2

- **A Subnet 4-et osszuk ki …**
  - **Csak 30 gépet tudunk azonosítani, mert**
  - **egyet elvisz a subnet azonosító,**
  - **egyet pedig a subnet broadcast cím ...**

Bitminta	IP cím	Megjegyzés
11000001|00000110|00000101|10000000	193.6.5.128	Subnet azonosító
11000001|00000110|00000101|10000001	193.6.5.129	Gép 1
11000001|00000110|00000101|10000010	193.6.5.130	Gép 2
11000001|00000110|00000101|10000011	193.6.5.131	Gép 3
…	…	…
11000001|00000110|00000101|10011101	193.6.5.157	Gép 29
11000001|00000110|00000101|10011110	193.6.5.158	Gép 30
11000001|00000110|00000101|10011111	193.6.5.159	Subnet broadcast

Változó alhálózat méretek

- **Variable Length Subnet Mask (VLSM) (RFC 1009)**
  - **Különböző alhálózatok létrehozása**
    - **hatékonyabb címfelhasználás**
  - **A routing-nak támogatnia kell (RIP-1 nem jó!)**
    - **a kiterjesztett prefixet (subnet maszkot) is át kell adni (terjeszteni kell)**
    - **Minden router a leghosszabb prefix egyezése elvén továbbítsa a csomagokat**
    - **Az aggregációhoz a címkiosztásnak követnie kell a topológiai feltételeket**
  - **A többszintű hierarchia előnye**
    - **alhálózatokat tovább tudunk bontani**
    - **az aggregáció miatt ez kívülről nem látszik**

Maszk (bin)	Maszk (dec)
10000000	.128
11000000	.192
11100000	.224
11110000	.240
11111000	.248
11111100	.252
11111110	.254

Longest prefix match

- **Tegyük fel, a 2.28.137.130 címre kell a csomagot továbbítani, az alábbi router tábla esetén: Forgatókönyv:**
  - **Kigyűjteni az összes bejegyzést, ahol cél IP és maszk a prefixet adja**
  - **Ezekből kiválasztani azt, amelyiknek a leghosszabb a maszkja. Legrosszabb esetben 0.0.0.0, azaz a default route a választás**

Route prefix	Interface	Next-hop	Target IP mask	
0.0.0.0./0	Serial 0	1.1.1.1	0.0.0.0	☺
2.28.0.0/16	Serial 1	2.2.1.1	2.28.0.0.	☺
2.28.137.0/24	Serial 2	2.3.1.1	2.28.137.0	☺
2.28.137.128/25	Ethernet 0	2.3.1.4	2.28.137.128	☺ ☺
3.10.0.0/16	Serial 1	2.2.1.1	2.28.0.0.	
3.10.11.0/24	Serial 2	2.3.1.1	2.28.137.0	

Az osztály nélküli címzés

- **Classless Inter-Domain Routing (CIDR) (RFC 1517-1520)**
  - **A maszk rövidebb is lehet, mint a hálózat-azonosító (superneting)**
    pl:**193.6.0.0-193.6.15.0** 16db **C osztály**
    → 255.255.240.0 (/20) → 193.6.0.0 /20
  - **Több hagyományos A,B,C osztály összefogása**
  - **laza bithatárok: /4 … /30**
  - **szükségtelenné válik az osztályok használata**
  - **a routing nem az első bitek szerint dönt**
  - **a címtér sokkal jobban kihasználható**
- **A CIDR együtt élhet a klasszikus routinggal, de**
  - **a régebbi eszközök nem mindig kezelik**

A VLSM és a CIDR

- **Mindkettő támogatja egy A, B, C hálózaton**
  - **flexibilis alhálózat-rendszer kialakítását**
  - **belsejének elrejtését (aggregáció)**
- **A CIDR azonban lehetővé teszi**
  - **több bitszomszédos hálózatok összefogását** (supernetting)
    - **és ezen belül tetszőleges hierarchia kialakítását**
  - **több szomszédos A, B, C hálózat összevont útvonal-választási bejegyzését**

Címfoglalási szabályok

- **A globális Interneten minden IP cím egyedi**
  - **a globális IP címeket engedélyeztetni kell** (IANA, EU: RIPE)
- **Internettől elszigetelt magánhálózaton**
  - **tetszőleges kiosztást készíthetünk, de így a**
  - **későbbi esetleges csatlakozás gondot okozhat.**
  - **Lokális címtartományok (IANA) (RFC 1918)**
    - **10.0.0.0./8**
    - **172.16.0.0./12**
    - **192.168.0.0./16**

Magánhálózat csatlakoztatása az Internetre

- **Ha bejegyzett címtartományokat használtunk,**
  - **nincs gond.**
- **A lokális címtartományú magánhálózatot tűzfallal leválasztjuk (se ki, se be)**
  - **nincs gond, de nem használható az Internet közvetlenül**
- **Lokális címtartományú magánhálózatról bejegyzett címtartományra kívánunk áttérni**
  - **átszámozás (elég költséges),**
  - **címfordítás NAT (Network Address Translation) (RFC 1631) lehetséges.**

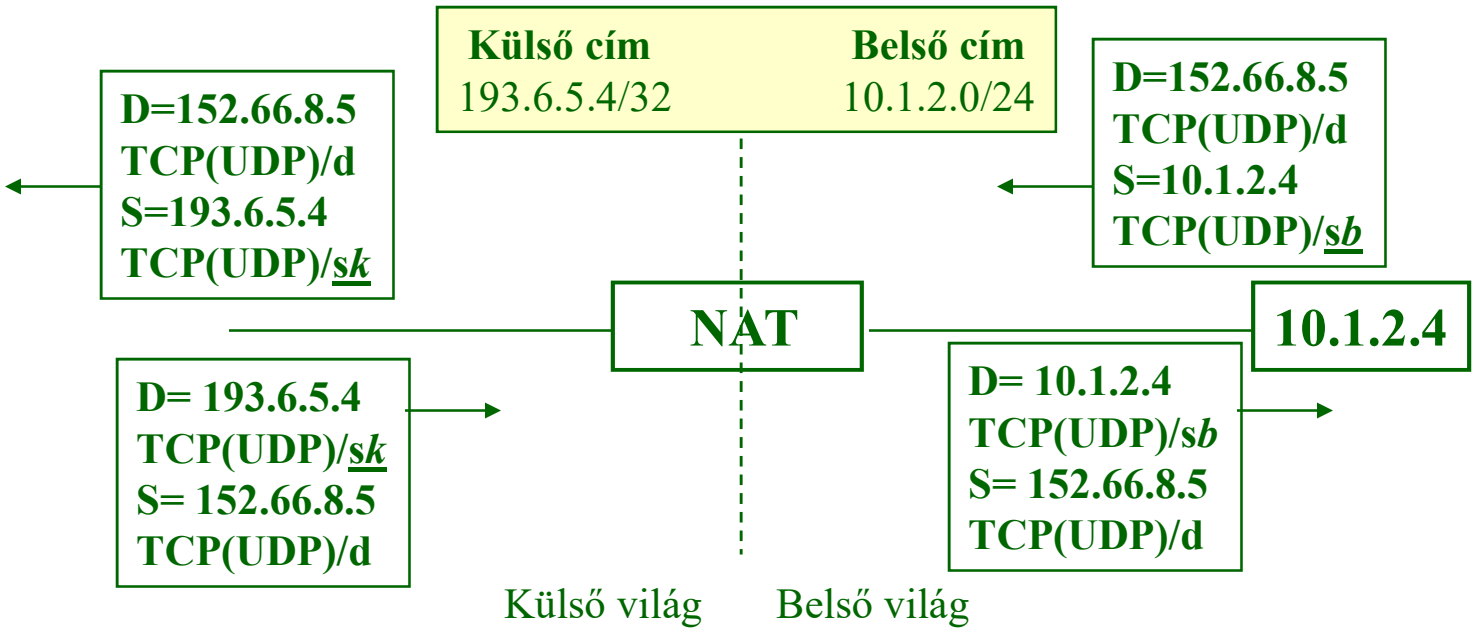
Címfordítás, NAT (IP masquerade)

- **A belső és a külső IP címek összerendelése**
  - **Címfordítási táblázat (ötlet ua. Protokoll – több port):**

Külső IP cím(ek)
Protokoll (TCP, UDP)
Külső Port

⇔

Belső IP cím(ek)
Protokoll (TCP, UDP)
Belső Port



Címfordítás, NAT

Egyetlen külső cím esetén:

- **Kicseréli a belső forrás címet a külső címre**
- **Megnézi, hogy az eredeti forrás port szabad-e a külső oldalon.**
- **Ha szabad, akkor azt választja.**
- **Ha foglalt, akkor a szabad (választható) portok közül választ egyet.**
- **Ha nincs szabad port, akkor eldobja a csomagot.**
- **Bejegyzi egy táblázatba a fordítást a visszafelé jövő, illetve a további csomagok érdekében.**

Több külső cím esetén:

- **Ha nincs szabad port, akkor veszi a következő külső címet és azon keres szabad portot.**
  (Ugyanúgy mint egy cím esetén.)

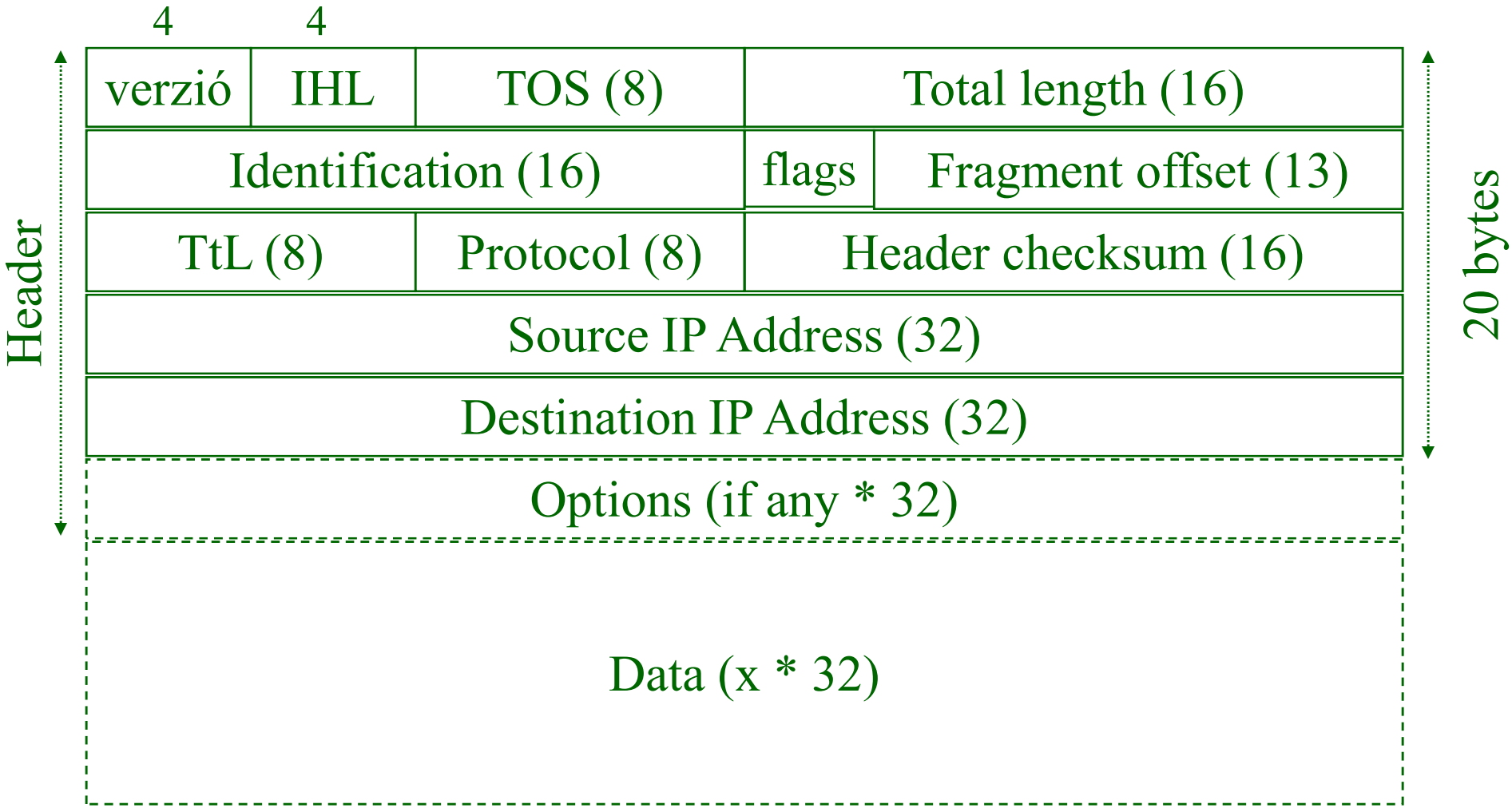
Címfordítás, NAT

- **A NAT transzparens mindazon protokollokra melyek**
  - **nem használnak IP címeket a csomag belsejében,**
  - **nem használnak előre megbeszélt, vagy magasabb szinten egyeztetett címet.**
- **A NAT amennyiben felismeri (és ismeri) a magasabb szintű protokollokat, úgy a csomag belsejében is elvégezheti a címváltoztatást.**
  Pl:
  - **FTP** (a behívó kliens mondja meg a szervernek, hogy hova hívjon vissza a szerver – aktív FTP, (passzívnál a behívó hív újra)).
  - **embedded IP Addresses in DNS "A and PTR" records.**
    NAT will translate the address(es) which appear in DNS responses to name lookups (A queries) and inverse lookups (PTR queries).

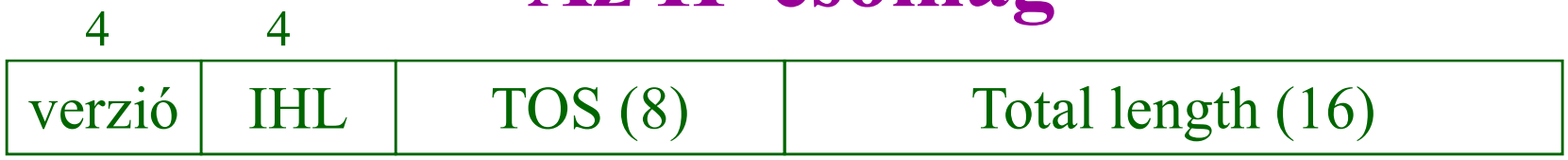
IPv4 címzés fejlődése

- **Klasszikus címosztályok: 1981**
  - **a címzési rendszer alapelvei**
- **Alhálózatok: 1985**
  - **kétszintű hierarchia**
- **Változó méretű alhálózatok: 1987**
  - **többszintű hierarchia, aggregáció**
- **Osztálymentes címzés: 1993**
  - **tetszőleges hálózatméret, hálózatok közti aggregáció**
- **Címfordítás: 1994**
  - **a címtér többszörös lefedése**

Az IP csomag


4
4
verzió
IHL
TOS (8)
Total length (16)
Identification (16)
flags
Fragment offset (13)
TtL (8)
Protocol (8)
Header checksum (16)
Source IP Address (32)
Destination IP Address (32)
Options (if any * 32)
Data (x * 32)
Header
20 bytes

Az IP csomag



- **Verzió: 4 (IPv4)**
- **IHL: Header length** (a header hossza az opciókkal együtt)
  32 bites szavakban 4 bit ⇒ a header max 60 byte hosszú lehet
- **TOS: Type of Services, csak 3+4 bitet használ:**
  - **3 bit a prioritásra (7 a magas, 0 az alacsony) + 4 bit:**
  - **D bit: Minimize delay (Pl. telnet)**
  - **T: Maximize throughput (Pl. Ftp data)**
  - **R: Maximize reability (pl SNMP)**
  - **Minimize monetary cost**

  egyszerre csak egy bit lehet 1

  (Nem minden implementáció használja (pl. OSPF dönthet ez alapján))
- **Total length: az IP datagram teljes mérete bájtokban**
  16 bit ⇒ IP datagram max. 65535 byte

Az IP csomag

Identification (16)	Flags	Fragment offset (13)

- **Identification: a datagram egyedi azonosítója, amit a küldő hoszt állít be (pl fregmentáció esetén azonosítja az egyes darabokat)**
- **Flags (3 bit):**
  - **1 bit nem használt**
  - **1 bit (DF): "don't fragment" bit: ha 1, a csomag nem fregmentálható.**
    - **Ha mégis kellene: ICMP error**

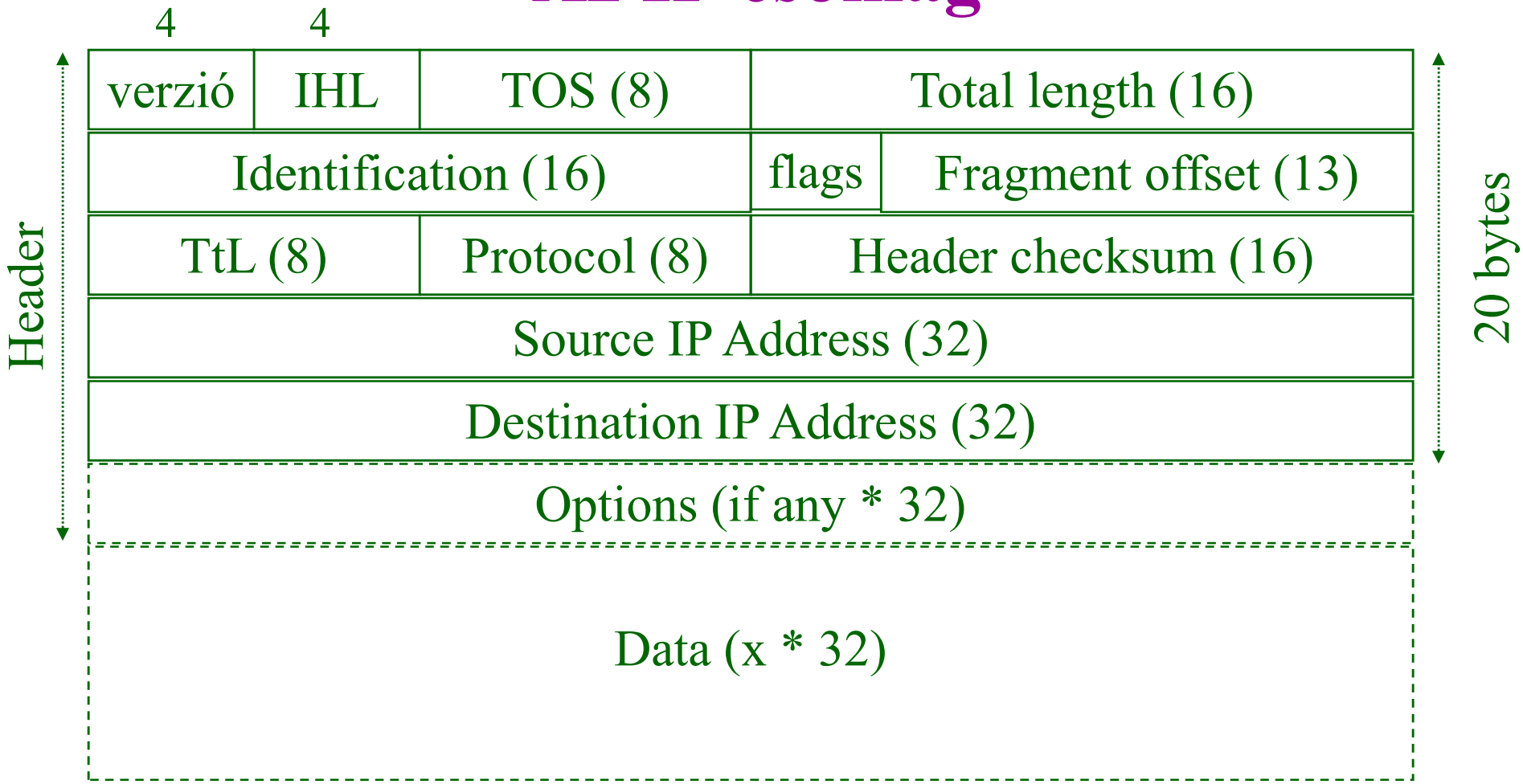
    "fragmantation needed but don't fragment bit is set"
  - **1 bit (MF): fregmentálás esetén 1, ha van még további darab; 0, ha ez az utolsó**
- **Fragment offset (13 bit): fregmentáció esetén a data melyik része (milyen az eltolás 8 byte-okban számolva). Az első darab esetén = 0. Az összes darab hossza csak 8 egész többszöröse byte lehet (kivéve az utolsó darabot).**

Az IP csomag

TTL (8)	Protocol (8)	Header checksum (16)

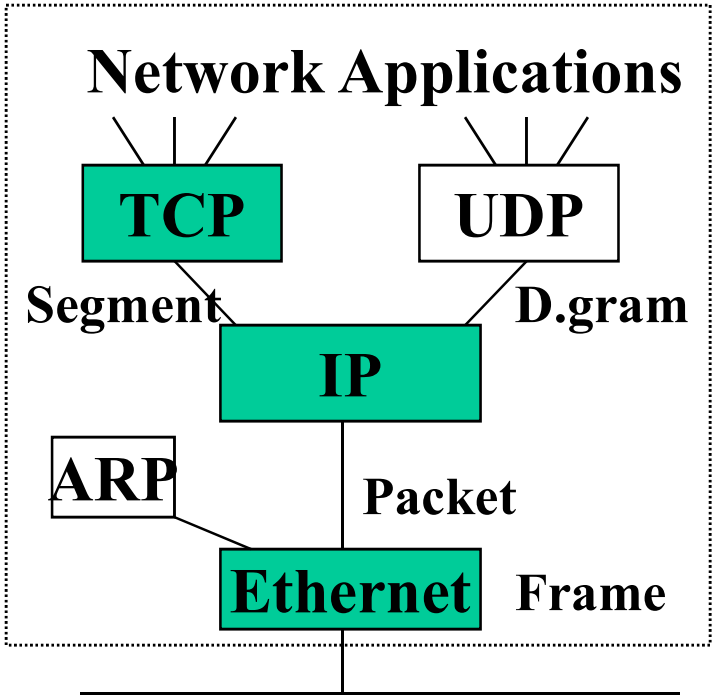
- **Time to Live (TTL, 8 bit):**
  - **Minden ugrás esetén a router annyival csökkenti, ahány sec-ot állt nála (de legalább 1-gyel).**
  - **Régebben 32 v. 64, manapság 128 kezdeti értékkel**
  - **Ha eléri a 0-át,**
    - **a router eldobja és**
    - **ICMP "time exceeded" error a feladónak.**
- **Protocol: az IP csomagot előállító protokollt (pl TCP, UDP, ICMP, IGMP) azonosítja**
- **Header cheksum: az IP fejrészre vonatkozó 1 komplemens 16 bites összeg. Mivel a TTL változik, mindig újraszámítandó (Hop). Hiba esetén eldobják a csomagot.**
  (A vevő az egészre számol 1 komplemens összeget → ha jó, csupa 1)

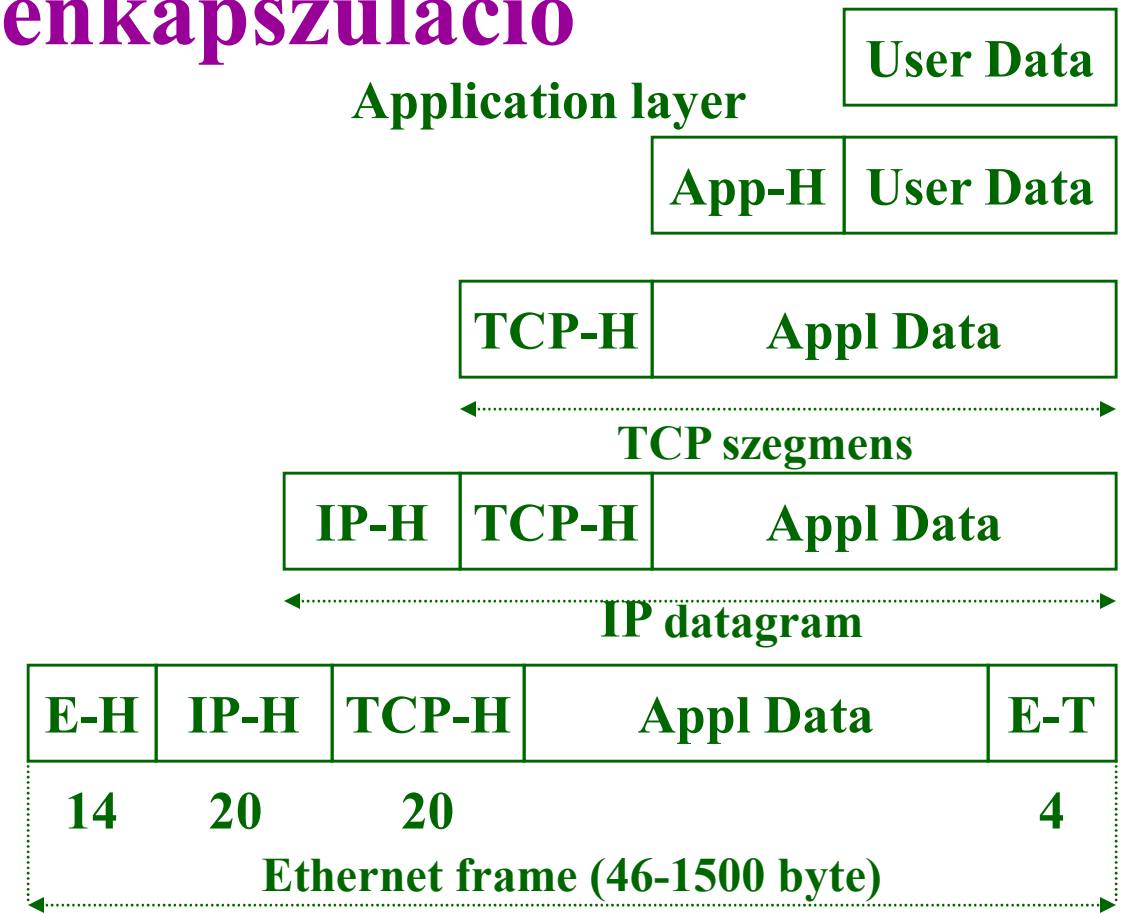
Az IP csomag



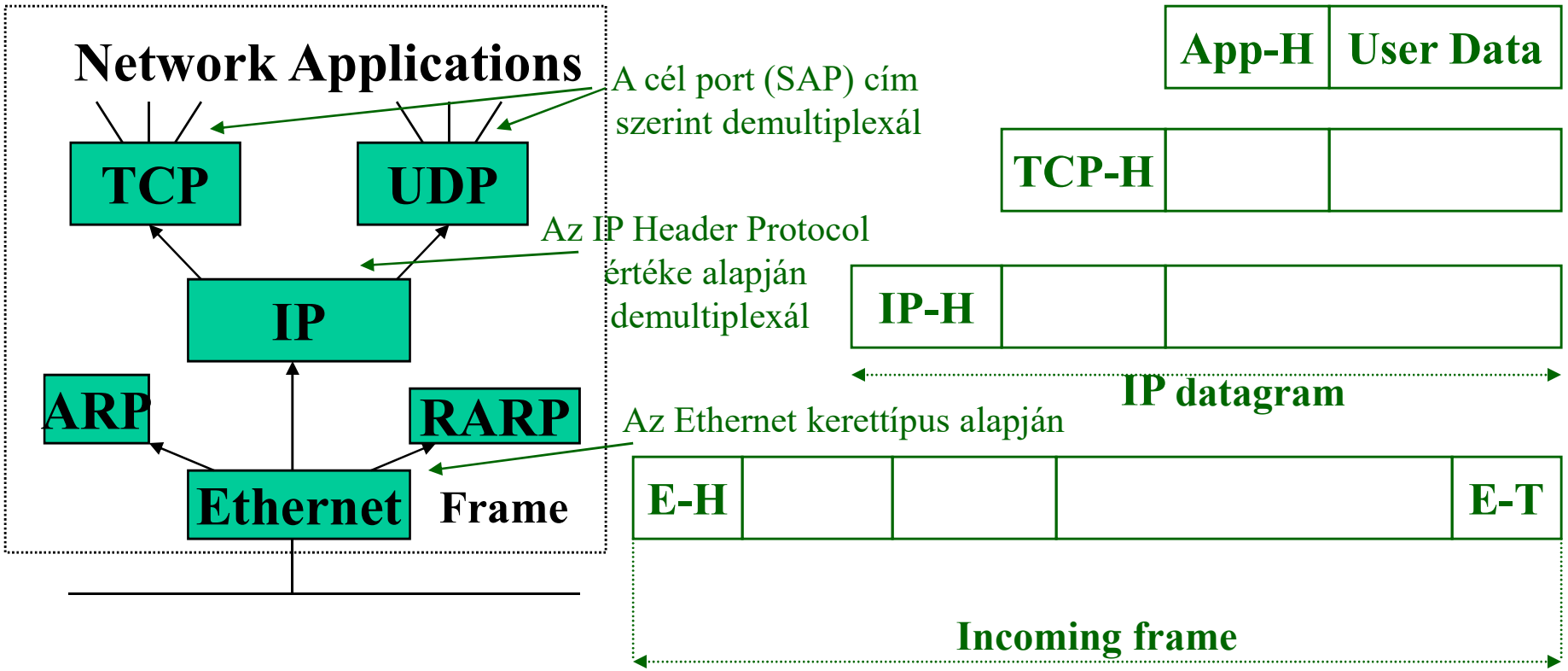
- **SA, DA (IP címek)**
- **Opciók és adatok**

Az enkapszuláció





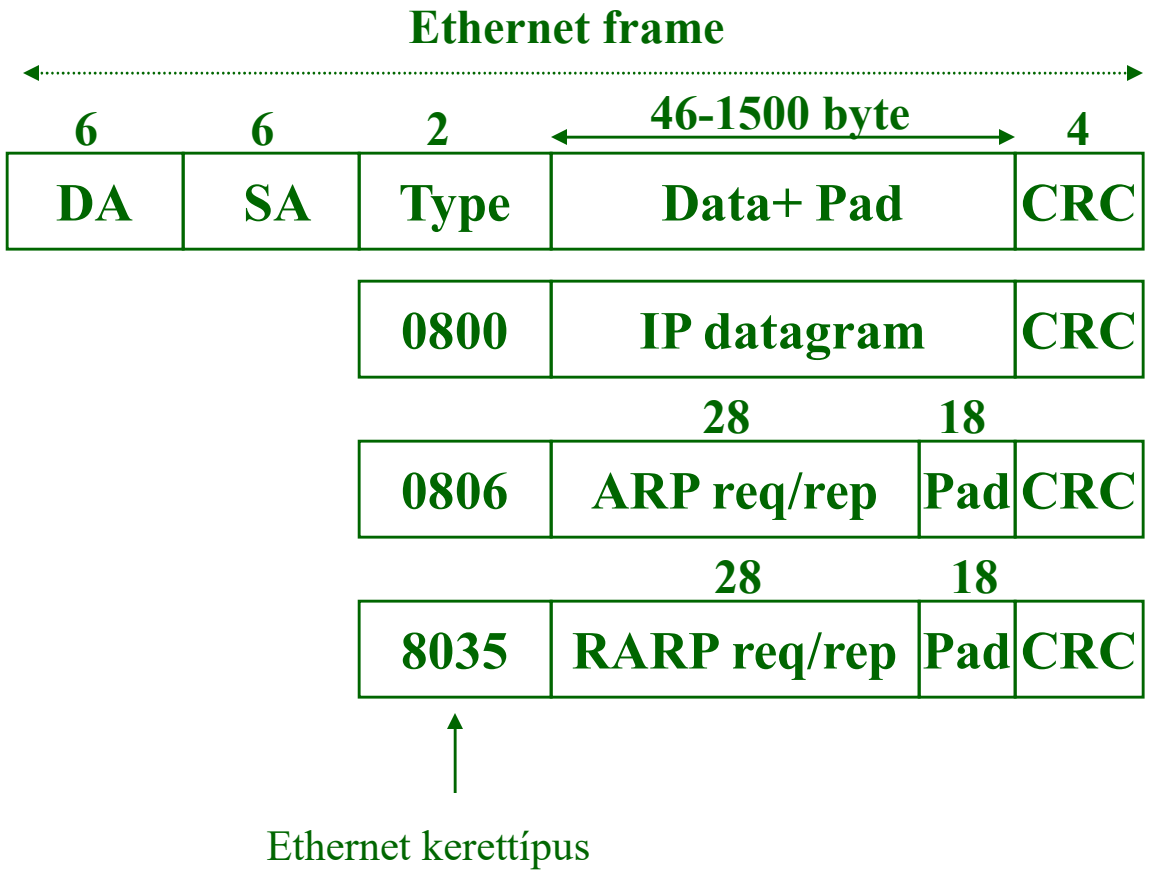
A visszaállítás (demultiplexálás)



A TCP SAP, UDP SAP azonosítás: 16 bites port szám alapján (port number)

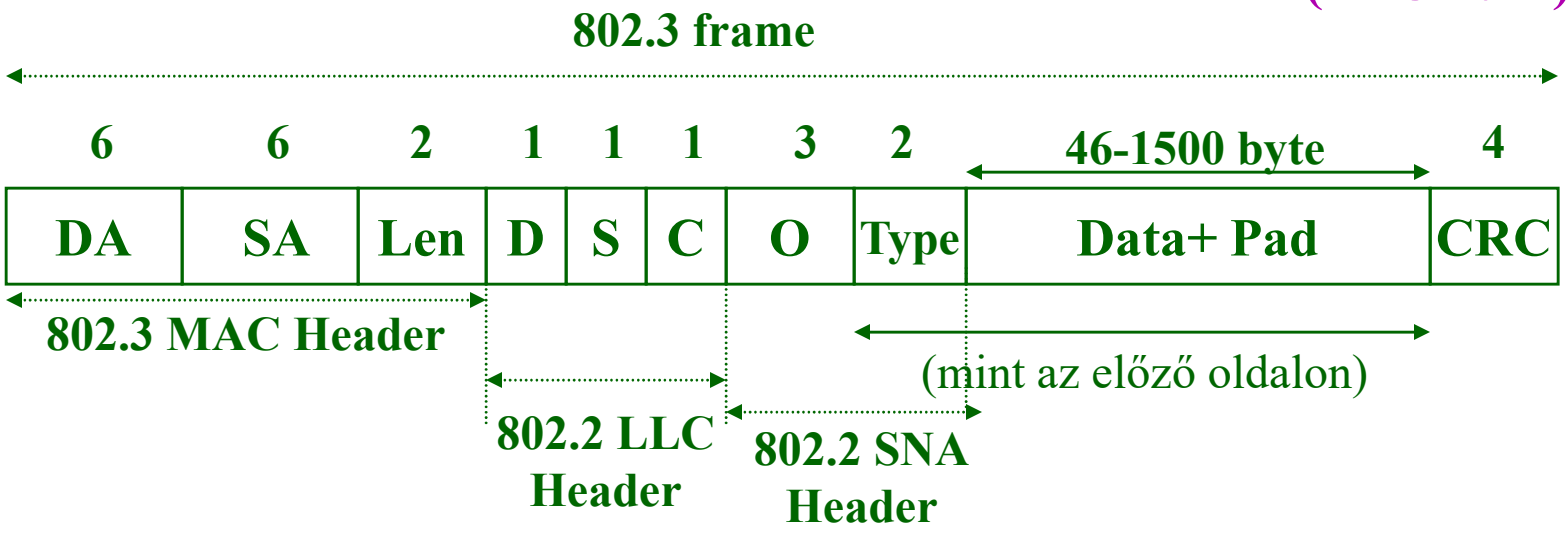
Link Layer: Ethernet enkapszuláció

(RFC 894)



Link Layer: 802.3 enkapszuláció

(RFC 1042)



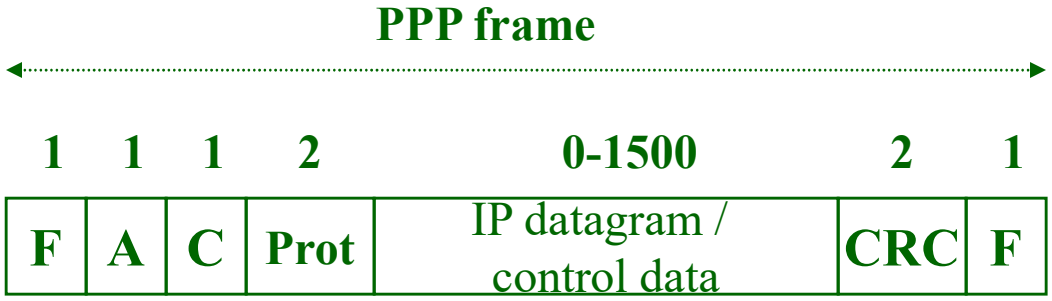
D: Destination SAP (AA)
S: Source SAP (AA)
C: Control (vezérlés) (03)

} **LLC: Logical Link Control Header**

O: Organisation Code (00)
Type: Lásd Ethernet

} **SNA: Sub Network Access Protocol Headre**

Link Layer: PPP enkapszuláció



F: Flag

szinkron:7E (bitbeszúrás: 01111110)

aszinkron: 7E, de karakter orientált

transzparens: adatok között

7E: 0x7D=escape: 0x7E→7D,5E;

adatok közt 0x7D→7D,5D;

20h-nál kisebb →7D,20H+d

A: Address (FF)

C: Control (03)

Prot: 0021: IP datagram

C021: Link Control Data

8021: Network Control Data

Nincs ARP ← ez pont-pont kapcsolat !

IP soros vonalon (nem csak IP)

Point to Point Protocol

- aszinkron, 8 bites adatok,
- szinkron, bit orientált.

A protokoll lehet:

LCP (Link Control P) (RFC 1548):

Data link kapcsolat létrehozása, tesztje, konfigurációja

NCP (Network Cont. Prot.) (RFC 1332):

különböző hálózati protokollok (pl. IPX) átvitele PPP-n

Az ARP (RFC 826)

- **Feladat: host vagy router IP címének leképzése MAC címmé (1982)**
- **Fogalmak, alapok:**
  - **IP cím: hálózat + host cím, a subnet maszk segít a szétválasztásban**
  - **Default router: egy hálózathoz tartozó router és annak IP címe**
  - **Helyi kommunikáció: egy hálózaton belüli**
    - **Ua a hálózati cím (ua a subnet-mask)**
  - **Távoli kommunikáció: hálózaton kívüli**
    - **más a hálózati cím**

Az ARP (RFC 826)

- **Fogalmak:**
  - **Címzési szabályok:**
    - **minden hosztnak (legalább egy) egyedi IP címe van**
    - **az egy hálózaton lévőknek közös a hálózati címe (netid) és a szubnet maszkja**
  - **A hálózat itt azonos a „Broadcast Domain”-nel!**
    - **A hálózat azon része, melyről „Local Broadcast Packet” használatával információt nyerhetek**
      - **ismétlők, hidak továbbítják a Local Broadcast Packet-et,**
      - **routerek nem!**
  - **A szegmensen belül helyi kommunikáció, „Direct Delivery” (közvetlen kézbesítés) van.**

Az ARP (RFC 826)

- **A MAC címek nyerhetők:**
  - **Local Broadcast ARP_REQUEST küldése után a válaszokból ARP_REPLY** (amiket azonnal cache-elni lehet)
  - **Majd a későbbiekben a cache-ből (IP - MAC párok)**
- **A továbbiakhoz tegyük fel, hogy megvan a cél IP címe (Pl. DNS-ből)**

Az RARP (RFC 903)

- **Saját IP cím lekérdezése (pl. boot) a saját MAC cím alapján (gond: L2 protokoll, leváltja a Bootp)**
  - **RARP_REQUEST Broadcast-al**
  - **A szerver táblázat alapján válaszol RARP_REPLY**
  - **Elavult, felváltotta a DHCP**

További protokollok

- **Boot Protocol (RFC 1542)**
  - MAC és IP cím statikus összerendelése
  - Kliens-szerver-relay_agent konfiguráció
  - UDP csomagokban request-reply
- **Dynamic Host Configuration Protocol (RFC 1541)**
  - MAC és IP cím dinamikus összerendelése,
  - címtartományok kijelölhetők,
  - címhasználat időben korlátozódhat,
  - kérheti a korábbi címét,
  - hasznos erőforrások (pl. DNS) jelezhető,
  - BOOTP-vel felülről kompatibilis.

Az IP csomagok továbbítása

- **Megvizsgálja a cél IP címet, az „helyi”, vagy „távoli”**
  - **A saját subnet maszkkal leválasztja a hálózati címrészt, és összeveti a sajátjával: ha egyezik: helyi, ha nem: távoli.**
- **Ha helyi, akkor (Direct Delivery)**
  - **Nézi a cache-ében, van-e hozzá MAC cím. Igen: a MAC szinten elküldi a címzettnek.**
  - **Nincs: Local Broadcast (ARP) kezdeményezéssel választ kér, és így megkapja a cél MAC címet. Mindjárt cache-eli, és MAC szinten elküldi a címzettnek.**

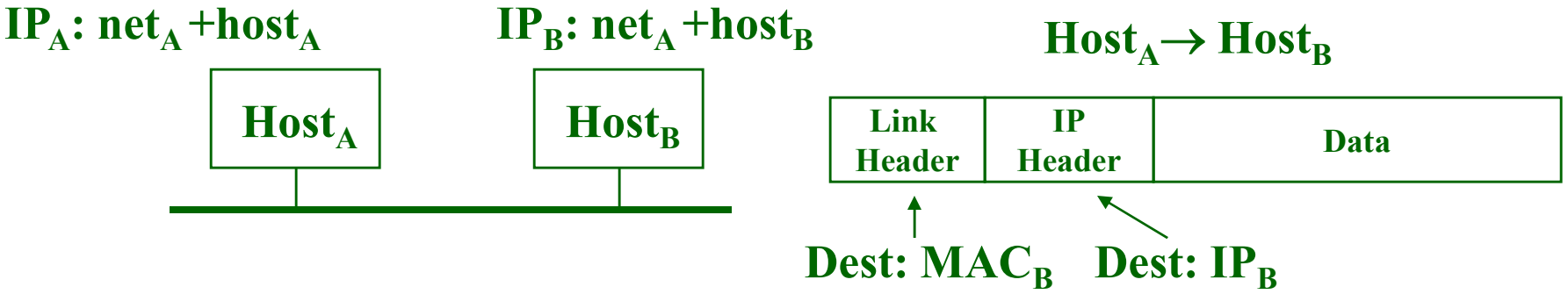
Az IP csomagok továbbítása

Ha a cél cím „távoli”, akkor (Indirect Delivery)

- **Nézi saját forgalomirányító tábláját (route table), van-e speciális út a célhoz, ha van,**
  - **keresi a cache-ében, ismeri-e az úthoz rendelt router MAC címét. Igen: MAC elküldi annak.**
  - **Nincs: Local Broadcast (ARP) kezdeményezéssel választ kér, és így megkapja a router MAC címet. Mindjárt cache-eli, és MAC szinten elküldi neki**
- **Ha nincs speciális út (esetleg nincs is forgalomirányító tábla) – a default router-nek küldi:**
  - **Nézi a cache-ében, van-e a default router-hez MAC cím. Igen: MAC elküldi annak.**
  - **Nincs: Local Broadcast (ARP) kezdeményezéssel választ kér, és így megkapja a default router MAC címet. Mindjárt cache-eli, és MAC szinten elküldi.**

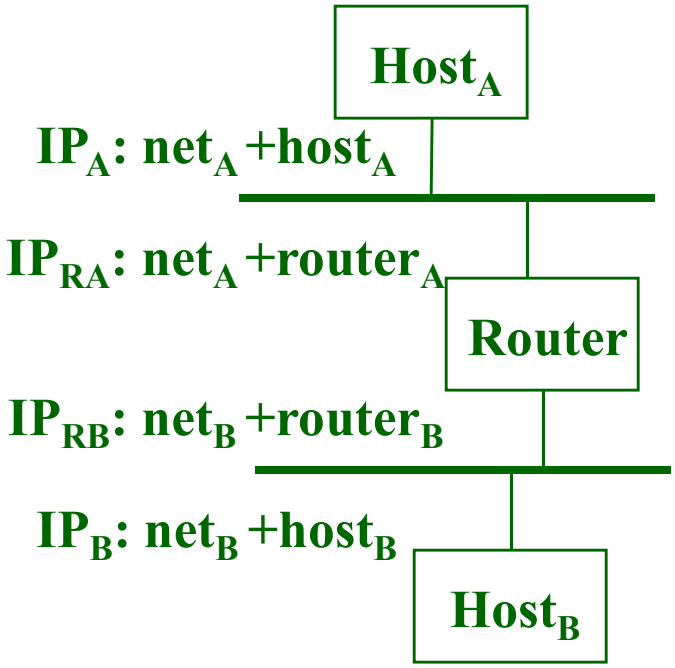
Az IP csomagok továbbítása

- **Két host közös hálózaton (netid), közös adatkapcsolati réteg**

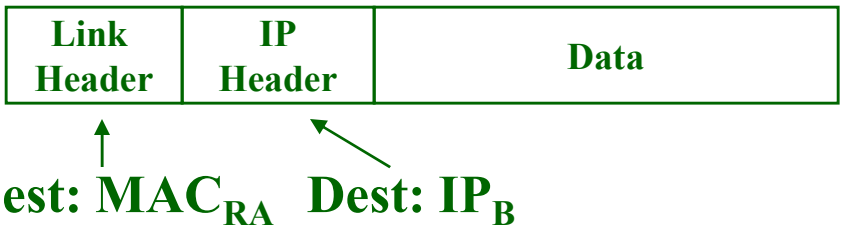


Az IP csomagok továbbítása

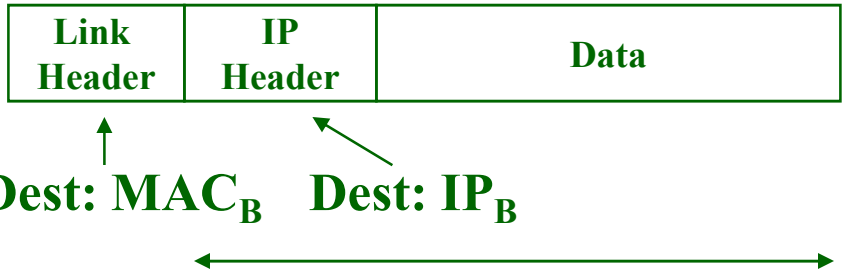
- **Két host különböző hálózaton**



1: Host$_A$ → Router$_A$



2: Router$_B$ → Host$_B$



Az IP csomag nem (alig (TTL+checksum)) változik, csak a Link Layer Header más.

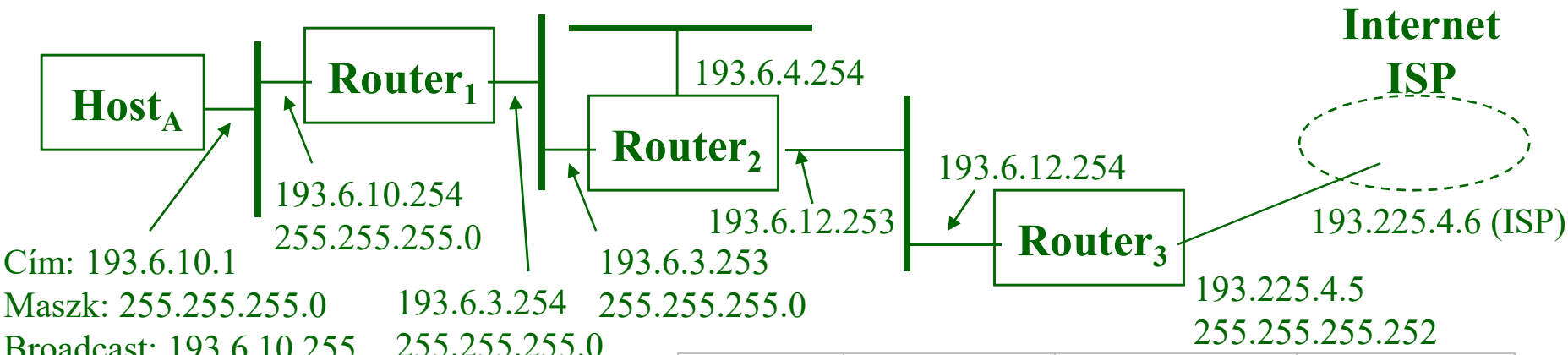
Az IP routing

- **Az útvonalválasztó az eredeti datagram-on a következőket változtatja meg:**
  - **Dekrementálja a Time-to-Live mezőt (amiből eldönthető, hány sec-ig, vagy ugrásig maradhat meg a datagram).**
  - **Újraszámítja a checksum-ot.**

IP routing tábla

- **Egy router a routing tábláját nézi végig, hogy melyik portjára (melyik interfészére) küldje a datagramot.**
  - **A keresési kulcs a cél IP hálózati címe.**
  - **A kereséshez kell a szubnet maszk is.**
- **A csomagtovábbítás**
  - **a leghosszabb illeszkedő prefix (longest prefix match),**
  - **hop-by-hop (azaz minden router maga dönt),**
  - **nem megfelelő router választása esetén (a router ugyanazon interfészén visszaküldi a csomagot) ICMP Redirect a küldőnek.**

Routerek konfigurációja



A gateway (router) címe mindig olyan, amit a saját hálóján közvetlenül elér.

Ez a statikus kitöltési módja a routing tábláknak (static routing)

Router1	net id	mask	gateway
IP Route	193.6.12.0	255.255.255.0	193.6.3.253
	193.6.4.0	255.255.255.0	193.6.3.253
Default	0.0.0.0	0.0.0.0	193.6.3.253
Router2	net id	mask	gateway
IP Route	193.6.10.0	255.255.255.0	193.6.3.254
Default	0.0.0.0	0.0.0.0	193.6.12.254
Router3	net id	mask	gateway
IP Route	193.6.3.0	255.255.255.0	193.6.12.253
	193.6.4.0	255.255.255.0	193.6.12.253
	193.6.10.0	255.255.255.0	193.6.12.253
Default	0.0.0.0	0.0.0.0	193.225.4.6

Az ICMP

- **Internet Control Message Protocol**
  - **Az alapvetően a hálózati réteggel kapcsolatos üzenetek továbbítására**
- **Az ICMP enkapszuláció**
- **ICMP message**

Type (8)	Code (8)	Checksum (16)
Content (type és code függő tartalom)		

Checksum: a teljes ICMP üzenet ellenőrzése

- **Típusok:**
  - **hibaüzenetek,**
  - **információk,**
  - **diagnosztikai üzenetek.**

ICMP példák

Type	Code	Üzenet (RFC792)
0	0	echo reply (ping)
3		Destination unreachable
	0	Network unreachable
	1	Host unreachable
	3	Port unreachable
	4	Fregmentation is needed but don't fragment bit set
4	0	Source quench: fojtócsomag (flow control)
5		Redirect
	0	Redirect for network
	1	Redirect for host
8	0	echo request (ping)
11		Time exceed
	0	Time to live = 0 during transmit (traceroute)
	1	Time to live = 0 during reassembly

stb.

ICMP

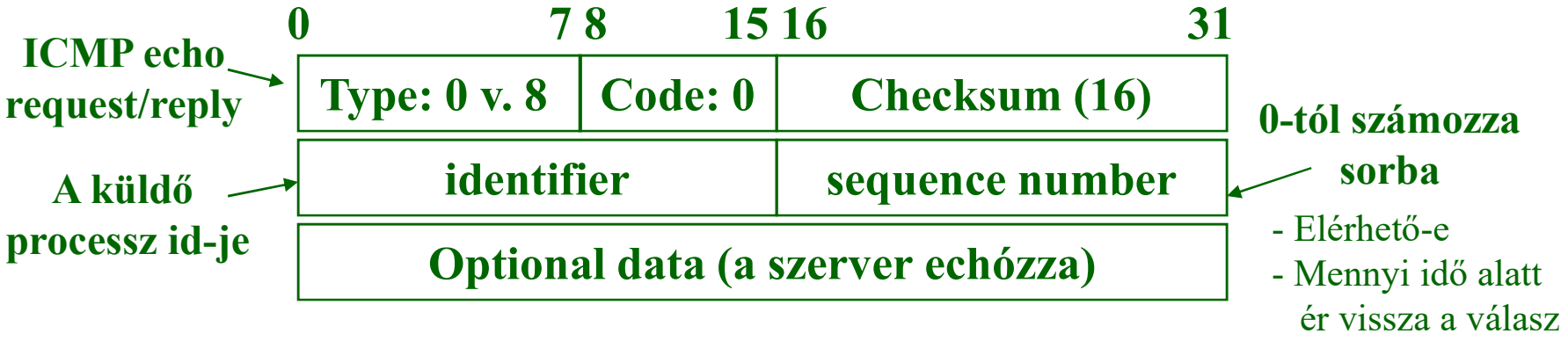
- **Az ICMP hibaüzenetek mindig tartalmazzák annak az IP datagram-nak a fejrészét (20 byte) és első 8 bájtját, ami a hibát okozta.**
- **Így a fogadó ICMP modul meghatározhatja a protokollt és a user processzt, amihez a hiba tartozik.**

IP hálózatok vizsgálata

- A vizsgálatok szükségessége
  - Hálózat beüzemelése, tesztelése
    - a végpontok látják-e egymást? (connectivity)
    - a csomagszűrés jól van-e beállítva?
  - Üzemelő hálózat teljesítményének fokozása
    - hatékony a működés (perfomance)
    - torlódások vannak-e?
    - Erőforrások kihasználtsága?
- Van néhány egyszerű alkalmazás
  - ping: az elérhetőség ellenőrzésére
  - traceroute: állomás elérési útvonalának vizsgálata

A ping

- **Állomás elérhetőségének ellenőrzésére**
  - **ping kliens:**
    aki kezdeményez egy ICMP echo request-tel;
  - **ping szerver: aki válaszol egy ICMP echo reply-vel.**
  - **A csomagok sorszámot és időbélyeget kapnak**
    - **csomagvesztés detektálható,**
    - **duplikáció detektálható,**
    - **sorrendcsere detektálható,**
    - **késletetési viszonyok változása (torlódás) detektálható.**



A traceroute

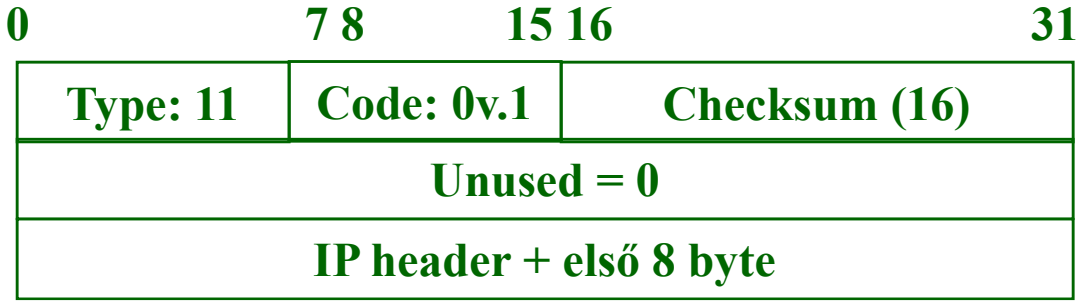
- **Állomás elérési útvonalának vizsgálata**

  Ötlet:

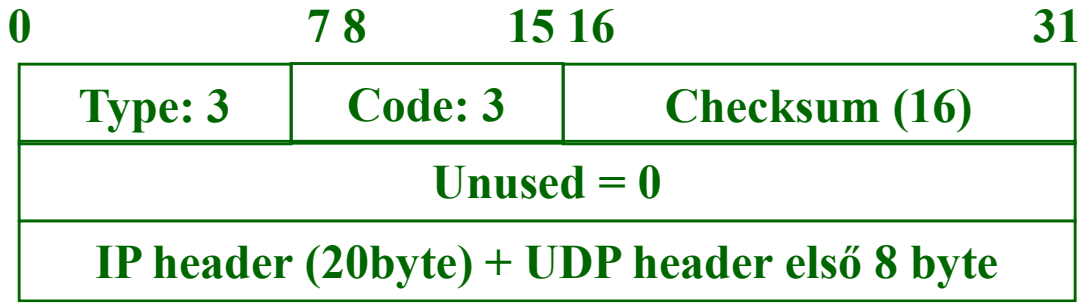
  - **Ha router TTL = 1 vagy 0 IP datagramot kap, azt nem továbbítja, hanem ICMP time exceed üzenetet küld.**
  - **Ha a router IP datagramot továbbít, a TTL értéket annyival csökkenti, ahány sec-ig nála volt a csomag, de legalább 1-el → gyak. a router 1 sec.-nél rövidebb ideig tart egy csomagot, így a TLL olyan mint egy ugrásszámláló**
  - **Küldjünk csomagokat rendre TTL=1,2,3 … értékekkel olyan UDP portra, amihez nem tartozik szerver alkalmazás (pl. 30000 feletti portszám)**
    - **A soron következő első, második stb. router eldobja és ICMP üzenetet küld a saját címével mint feladóval → megtudható a köztes routere-ek címe;**
    - **Amikor eljut a célállomásra → ICMP port unreachable üzenet jön vissza (a célállomás címével), ebből tudható, hogy elérte a célállomást.**

A traceroute

- **ICMP time exceeded:**

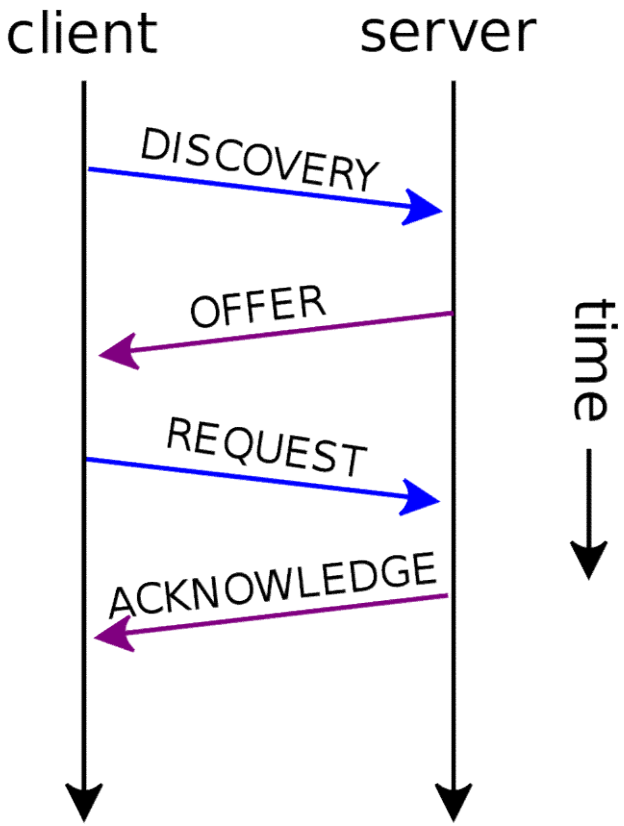


- **ICMP UDP port unreachable:**



Dynamic Host Configuration Protocol

- **DHCP (RFC 1541, RFC 2131)**
  - **RARP, gond az L2 protokoll implementálása**
  - **UDP 67 server, UDP 68 client**
  - **DHCP Relay Agent**



DHCP Discovery

Octet 0	Octet 1	Octet 2	Octet 3
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID (Transaction Identifier)			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x8000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0x00000000			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s, or overflow space for additional options; BOOTP legacy.			
Magic cookie			
0x63825363			
DHCP options			
53: 1 (DHCP Discover)			
50: 192.168.1.100 requested			
•55 (Parameter Request List): 1 (Request Subnet Mask), •3 (Router), •15 (Domain Name), •6 (Domain Name Server)			

IP: source=0.0.0.0; destination=255.255.255.255

UDP: source port=68; destination port=67

OP: Operation Code, 0x01 request, 0x02 reply

HTYPE: Hardwer type, 0x01 Ethernet

HLEN: Hardware Address Length (0x06 MAC)

HOPS: client:0, a Relay Agent használja

SECS: Seconds, not always used, number of seconds elapsed since a client began an attempt to acquire or renew a lease

XID: Transaction Identifier , client azonosítja vele az üzenetet

FLAGS: Broadcast flag – client nem tudja az IP címét

en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DHCP Offer

IP: source=192.168.1.1; destination=255.255.255.255

UDP: source port=67; destination port=68

Octet 0	Octet 1	Octet 2	Octet 3
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00

XID

0x3903F326

SECS	**FLAGS**
0x0000	0x0000

CIADDR (Client IP address)

0x00000000

YIADDR (Your IP address)

0xC0A80164 (192.168.1.100)

SIADDR (Server IP address)

0xC0A80101 (192.168.1.1)

GIADDR (Gateway IP address)

0x00000000

CHADDR (Client hardware address)

0x00053C04

0x8D590000

0x00000000

0x00000000

192 octets of 0s; BOOTP legacy.

Magic cookie

0x63825363

DHCP options

53: 2 (DHCP Offer)

1 (subnet mask): 255.255.255.0

3 (Router): 192.168.1.1

51 (IP address lease time): 86400s (1 day)

54 (DHCP server): 192.168.1.1

•6 (DNS servers): 9.7.10.15,

•9.7.10.16,

•9.7.10.18

en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DHCP Request

Octet 0	Octet 1	Octet 2	Octet 3
OP	**HTYPE**	**HLEN**	**HOPS**
0x01	0x01	0x06	0x00
XID			
0x3903F326			
SECS		**FLAGS**	
0x0000		0x0000	
CIADDR (Client IP address)			
0x00000000			
YIADDR (Your IP address)			
0x00000000			
SIADDR (Server IP address)			
0xC0A80101 (192.168.1.1)			
GIADDR (Gateway IP address)			
0x00000000			
CHADDR (Client hardware address)			
0x00053C04			
0x8D590000			
0x00000000			
0x00000000			
192 octets of 0s; BOOTP legacy.			
Magic cookie			
0x63825363			
DHCP options			
53: 3 (DHCP Request)			
50: 192.168.1.100 requested			
54 (DHCP server): 192.168.1.1			

IP: source=0.0.0.0 destination=255.255.255.255;
UDP: source port=68; destination port=67

en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

DHCP Acknowledgement

IP: source=192.168.1.1; destination=255.255.255.255

UDP: source port=67; destination port=68

Octet 0	Octet 1	Octet 2	Octet 3
OP	**HTYPE**	**HLEN**	**HOPS**
0x02	0x01	0x06	0x00

XID

0x3903F326

SECS	FLAGS
0x0000	0x0000

CIADDR (Client IP address)

0x00000000

YIADDR (Your IP address)

0xC0A80164

SIADDR (Server IP address)

0xC0A80101 (192.168.1.1)

GIADDR (Gateway IP address switched by relay)

0x00000000

CHADDR (Client hardware address)

0x00053C04

0x8D590000

0x00000000

0x00000000

192 octets of 0s. BOOTP legacy

Magic cookie

0x63825363

DHCP options

53: 5 (DHCP ACK) or 6 (DHCP NAK)

1 (subnet mask): 255.255.255.0

3 (Router): 192.168.1.1

51 (IP address lease time): 86400s (1 day)

54 (DHCP server: 192.168.1.1

•6 (DNS servers): 9.7.10.15,

•9.7.10.16,

•9.7.10.18

en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol

Routing Algoritmusok és Protokollok

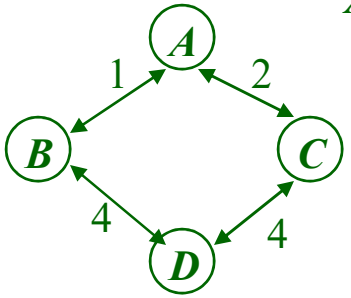
- **A routing protokollok határozzák meg az utak számításának módját, és a router-ek közötti üzenetcserét (routing update).**
- **Vector Distance Algorithm** (shortest path using hops): **Eleinte mindegyik router csak a kapcsolódó hálózatokat ismeri, majd más routerekkel táblát cserélve és frissítve saját tábláját megismeri a többi hálózatot.**
- **Shortest Path First Algorithm:**
  Mindegyik routernél ott a teljes hálózat térképe az egyes utak árával. Az „ár” függhet a hop számtól, sebességtől stb.

Vector Distance Algorithm (Bellman-Ford)

- A routing tábla távolság oszlopot is tartalmaz.
- Distance = number of hops = number of gateways to traverse
- Mindegyik router megküldi a tábláit azokra a hálózatokra, melyek kapcsolódnak hozzá.
  Azok a routerek, melyek megkapják ezen táblákat, módosítják azok metrikáit és felhasználják értékeit, ha:
  - még nem ismernek olyan utat
  - Vagy az így kapott út jobb, mint amit eddig ismertek.
- A routerek periodikusan, vagy a változások esetén küldik el tábláikat.
- A lassabb hálózatok magasabb hop számmal jelölhetőek.

Vector Distance Algorithm
(Bellman-Ford 1957, 1962)

A-t vizsgáljuk, aki *B*-től és *C*-től kap táblákat:



B táblája	
A	A:1
C	A:3
D	D:4

C táblája	
A	A:2
B	A:3
D	D:4

A "módosítja" a kapott táblákat a küldő távolságával: +1 +2

Módosított	
B	B:1
C	B:4
D	B:5

Módosított	
C	C:2
B	C:5
D	C:6

A kiválasztja a legjobbakat:

A a legjobbakból új táblát készít:

A táblája	
B	B:1
C	C:2
D	B:5

Bellman-Ford algoritmus: count-to-infinity

A végtelenig számolás problémája (count-to-infinity):

- **A jó hír (*A* megjavult) gyorsan,**
- **a rossz hír (*A* elromlott) lassan terjed**
  (a terjedés sebessége a ∞ ábrázolásától függ pl. 16)
  - **A probléma oka, hogy egy csomópont nem tudja eldönteni, hogy rajta van-e egy másik csomópont által javasolt úton.**

A megjavult →

A	*B*	*C*	*D*	*E*	
0	∞	∞	∞	∞	Kezdet
0	1	∞	∞	∞	1 csere
0	1	2	∞	∞	2 csere
0	1	2	3	∞	3 csere
0	1	2	3	4	4 csere

A elromlott →

A	*B*	*C*	*D*	*E*	
x	1	2	3	4	Kezdet
x	3	2	3	4	1 csere
x	3	4	3	4	2 csere
x	5	4	5	4	3 csere
x	5	6	5	6	4 csere
x	7	6	7	6	5 csere
.....					
x	∞	∞	∞	∞	

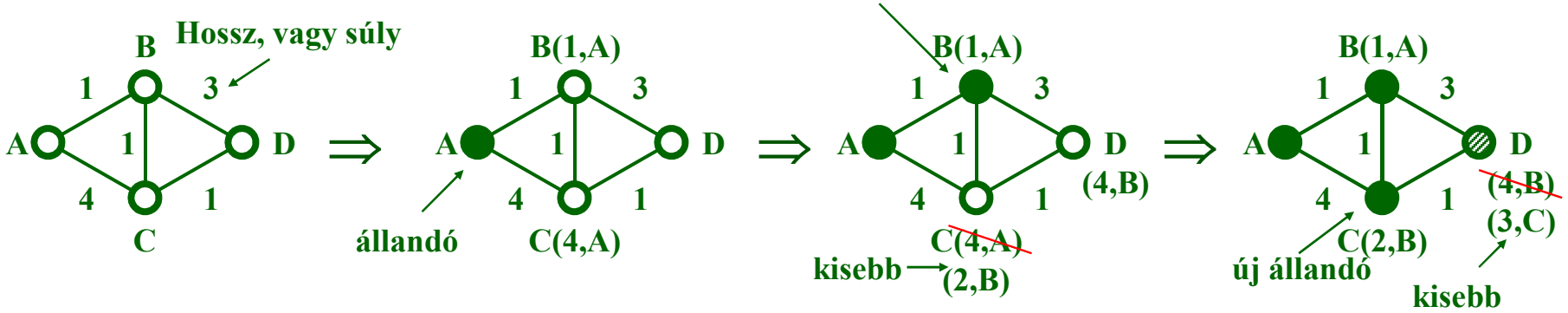
Shortest Path First (Link Status)

- **Mindegyik router-nél ott a teljes hálózat térképe az egyes utak árával.**
- **Mindegyik routert periodikusan üzenetet küld a linkjeinek tesztelésére (*link status*).**
  Ha érkezik rá válasz – a link él (up)
  Ha nem, akkor bejelöli a táblájába, hogy a link nem elérhető (down).
- **Minden változás esetén gráfelméleti módszerekkel újraszámolja az utakat (link).**
- **Gyakori a legrövidebb út algoritmus (*shortest path, forward search*) alkalmazása.**

Shortest Path First (Dijkstra 1959)

- **Legrövidebb út algoritmus:**
  - **Állandóvá tesszük a kiindulási állomást → (1)**
  - **(1) Ideiglenesen felcímkézzük a szomszédos állomásokat – az úthosszal és az állandó állomás címével**
  - **A legrövidebb úthossz címkéjűt állandóvá tesszük → (1)**

Pl: A→D legrövidebb út



A cél állandó lett → kész

Routerek „hierarchiája”

- **Core Gateway routerek:**
  az INOC (Internet Network Operation Center) **által kontrollált routerek:**
  - **az egész Internetre vonatkozó ismereteik vannak (nincs default router fogalmuk),**
  - **backbone hálózatokat formálnak.**

Autonom rendszerek (AS)

- **Autonom System (AS) csoportosítási egység:**
  - **olyan hálózatok és routerek csoportja, amit egy szervezet üzemeltet, vagy**
  - **olyan hálózatok és routerek csoportja, amik azonos routing politikát folytatnak.**
- **Az AS-ek INOC** (Internet Network Operation Center) **által kiadott AS számmal rendelkeznek.**
- **Az AS-eket Exterior Gateway (EG) –ek kötik össze**
- **Az AS-ek hirdetik saját hálózataik elérhetőségét más AS-eknek**
- **Az AS-en belül nem kell feltétlen az egész Internet címtartományt ismerni (default router/út)**
- **AS-en belüli lokális forgalom, topológiai változás nem látszik kifelé**

Exterior Gateway Protocol (EGP)

- EGP az a protokoll, amivel az Exterior Gateway-ek hirdetik elérhetőségi információikat szomszédaiknak és a Core Gateway-eknek
- Mindegyik gateway a saját hálózatából gyűjt információt és EGP-vel hirdeti szomszédainak.
- Az EGP-nek 3 fő funkciója van:
  - Támogatja az új szomszédok fogadását.
  - Teszteli az EGP szomszádait (Hello Protocol).
  - Rendszeresen hálózat elérhetőségi információkat cserélnek EGP szomszédaikkal (routing update).

Interior Gateway Protocols (IGP)

- **Az IGP az AS-en belül használt routing protokoll (eltérhet az EGP-től).**
- **Routing Information Protocol (RIP), (Vector Distance Algorithm) az egyik legelterjedtebb IGP.**
- **Open Shortest Path First Protocol (OSPF): Open standard uses the SPF algorithm.**

Internet felépítés: IGP-EGP

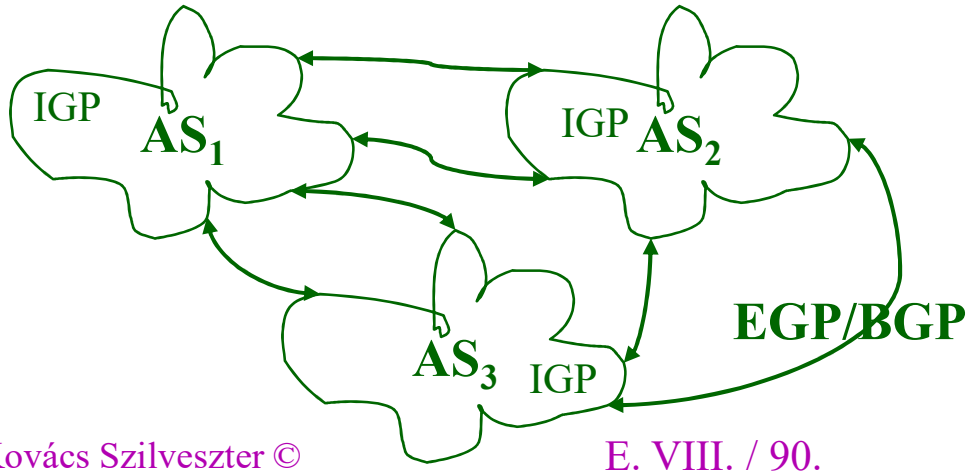
- **AS-en belüli Intra-Domain (Interior Gateway Protocol, IGP)**
  - **Lehet RIP/OSFP a méretektől, elvárásoktól függően**
- **AS-ek közötti Inter-Domain Exterior Gateway Protocol (EGP), vagy Border Gatway Protocol (BGP)**
  - **Alap: egy default út ki az AS-ből egy nagy ISP-hez, (Gateway router fogalom)**
  - **Újabb a BGP (Border Gatway Protocol)**
    - **Hálózat elérhetőségi információkat cserél → melyik AS milyen teljes útvonalon érhető el**
    - **Célja az AS-en átmenő forgalom minimalizálása**
    - **Képes kezelni**
      - **multi homed AS-t (több helyre szétosztott AS),**
      - **üzleti/politikai szabályrendszereket.**

Exterior Gateway Protocol

- **EGP, RFC 904**
  - **AS-ek között útvonalválasztás, elérhetőségi információk alapján**
  - **Régi, kifejlesztésekor még hierarchikus volt az Internet.**
  - **Alapvetően vector-distance protokoll**
  - **Nem véd a hurokképződés ellen, nincsenek védelmi mechanizmusai**

Border Gateway Protocol

- **Egy AS szempontjából a forgalom lehet**
  - **helyi (local traffic), az illető AS-ből indul, vagy abba érkezik**
  - **átmenő (transit traffic)**
- **BGP célja ⇒ az átmenő forgalom minimalizálása**
  - **Lehetővé teszi a szabályalapú (policy based) routolást ⇒ az AS adminisztrátorok meghatározzák, hogy több lehetséges út esetén melyiket válassza**
  - **A BGP (mint a RIP) távolságokat továbbít a szomszédainak, de a teljes utat (AS-ek sorozata) is megadja az egyes cél AS-ekhez**



Border Gateway Protocol

- **BGP, RFC 1771**
- **Az EGP hiányosságait küszöböli ki**
- **CIDR** (Classless Inter-Domain Routing) **támogatás (hatékony cím aggregáció)**
- **Konfigurálni kell a BGP szomszédokat, nincs „szomszéd felfedezés”**
- **TCP fölött fut (179-es port), megbízható kapcsolatorientált transzportot feltételez**
- **Nincs periodikus újraküldés, minden hallott útvonalat megjegyeznek a routerek.**
- **A hurokmentesség ellen path vektor módszert használ (célig vezető AS-ek listája)**

EBGP - IBGP

- **Exterior BGP**
  - **AS-ek között**
- **Interior BGP**
  - **AS-en belüli kapcsolatokra (pl. ha nem túl nagy, nem érdemes az OSPF-et használni, de nem felel meg a RIP)**

Interior Gateway Protocols (IGP)

ICMP redirect (ICMP átirányítás):

- **Valójában nem IGP, de itt érdemes megemlíteni**
- **Ha a router a kapott csomagot ugyanazon a hálón küldi tovább, mint amin kapta egy másik routernek**
  ⇒ ICMP redirect üzenet közvetlenül a feladónak azzal a címmel, akinek küldenie kellett volna helyette
- **Támadási lehetőséget biztosíthat:**
  Hamis redirect: „Man in the middle" hack

A RIP és RIP2

- **Routing Information Protocol**
  - **az UDP-re épül, az 520-as porton.**
- **A szomszédok táblákat cserélnek**
  - **Konfigurálni kell, hogy ki kinek küldjön, kitől fogadjon**
- **A hálócímek (netid) mellet metrika (metric) a táblában (a netid hány ugrással érhető el)**
  - **A csatlakozó interfészeken állítani lehet az értékét (a többi ezt küldi szét, illetve ennyivel növeli az azon irányból kapottakat)**
- **Metrika korlát (max. 16):**
  - **metric = 16 → nem elérhető**
- **A RIP a subneteket (maszkokat) nem hirdeti**
- **a RIP2 (RIP Version 2) a subneteket is hirdeti.**

Open Shortest Path First (Link Status)

- **OSPF (közvetlenül az IP-re épül)**
- **Nem távolságokat gyűjt, hanem a szomszédai elérhetőségét vizsgálja (Link State Protocol)**
- **Képes több utat kezelni** (pl. Az IP **T**ype **o**f **S**ervice alapján)
- **Az utakhoz súlyokat lehet rendelni** (pl. ToS)
- **Az azonos súlyúak között képes terhelésmegosztásra**
- **Hirdeti a subnet maszkot is**
- **Minden (gateway) router periodikusan küld egy üzenetet, tesztelve a link státust**
  - **az üzenet routing információkat nem tartalmaz.**
  - **Ha van válasz: a link él, a térképben ez jelezhető.**
  - **Ha nincs válasz: a link nem él.**

OSPF komponensek

- Szomszédok felfedezése (Hello)
- Designated Router (DR), tartalék (BDR) választás
- Szomszédsági viszony (adjacencies) kialakítása
- Adatbázis szinkronizáció (DS)
- Él állapot terjesztés (LSA flooding)
- Routing tábla számítás

- OSPF csomagok (fejrészében típus)
  - Hello
  - Database Description
  - Link-State Request/Reply/Ack

OSPF AB szinkronizáció (DS)

- **Kérés-válasz alapon**
  - **Link-State (LS) fejléceket cserélnek, és**
  - **ami hiányzik, lekérik LS Request-tel**
- **Link-State-Advertisment (terjesztés is, flooding-al)**
  - **minden szomszédnak továbbadom, kivéve ahonnan jött, és Ack-ra várok**
  - **Ha megkapta, nyugtázza, vagy újabb saját LS-t küld (ez is egyfajta „nyugta”)**
  - **Ez „fa mentén terjedő, egyszer átlapolódó körbe-küldős elv”**
- **Minden LSA „öregszik”**

OSPF Hello

- A linkek állapotának folyamatos figyelésére
- Broadcast linken Designated Router választás

Szomszédsági viszony

- A szomszédaival, hangolja össze az adatbázisát, annak küldi az LSA-kat
  - A pont-pont link másik vége a szomszéd.
  - A broadcast linken a DR (designated router) a szomszéd.

Dinamikus

- **Észreveszi, ha egy link megszakad**
  - **az adatkapcsolati réteg jelzi a router alkalmazásnak (néhány sec), vagy**
  - **a Hello csomagok elmaradnak (40 sec).**
- **És egyből terjeszti a router az új topológiai állapotot.**

Irodalom

- **RFC 1058 Routing Information Protocol**
- **RFC 1723 RIP Version 2**
- **RFC 2328 OSPF Version 2**
- **RFC 1771 BGP-4**
- **J. T. Moy: OSPF: Anatomy of an Internet Routing Protocol Addison-Wesley, 1998**
- **EIGRP: www.cisco.com/warp/public/457/7.html**
- **IBM Redbooks: www.redbook.ibm.com/abstracts/gg243376.html**