IPv6 protokoll

Varga Tibi 2021

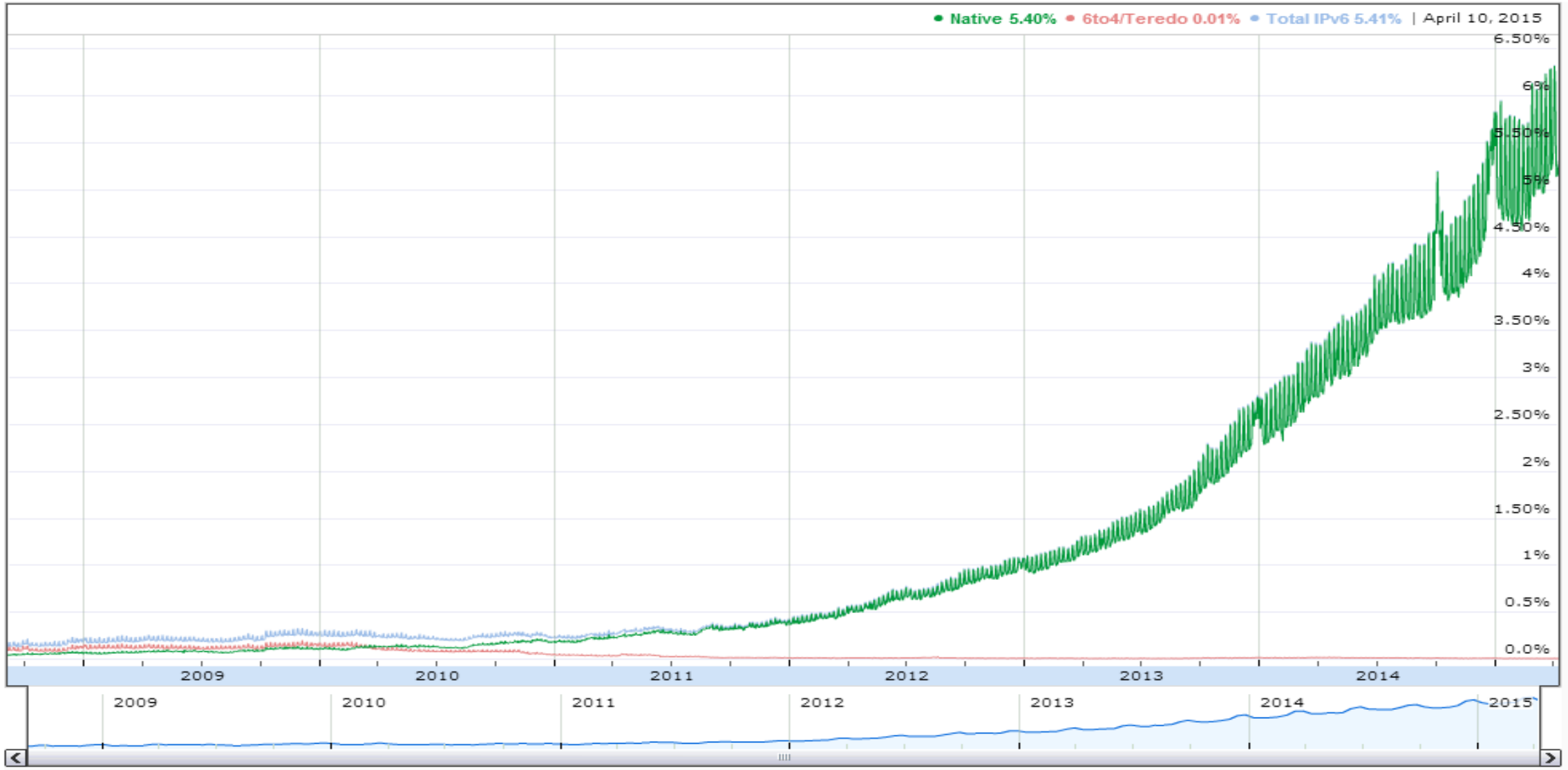
IPv6 – Megoldás a címhiányra

- Már 1990-ben elkezdték kidolgozni az IPv6-t 1998 óta szabvány
- 128 bit hosszú - 3.4×10^{38} (34 sextillió) cím
- Ma már minden piacon kapható eszköz támogatja, dual-stack megoldások, növekvő IPv6 elérhető tartalom
- Számos kompatibilitási szcenáriót dolgoztak ki hozzá
- Jelenleg mégis alig 5.4% az IPv6 részesedése
- Helyette: másodlagos IPv4 piac

Miért nem terjed el, ha technikailag minden szempontból jobb, mint a régi?

IPv6 forgalom aránya

Online statisztikák a Google vagy az IANA oldalán (kb. 9 havonta duplázódik?



Elvárások az IPv6-al szemben

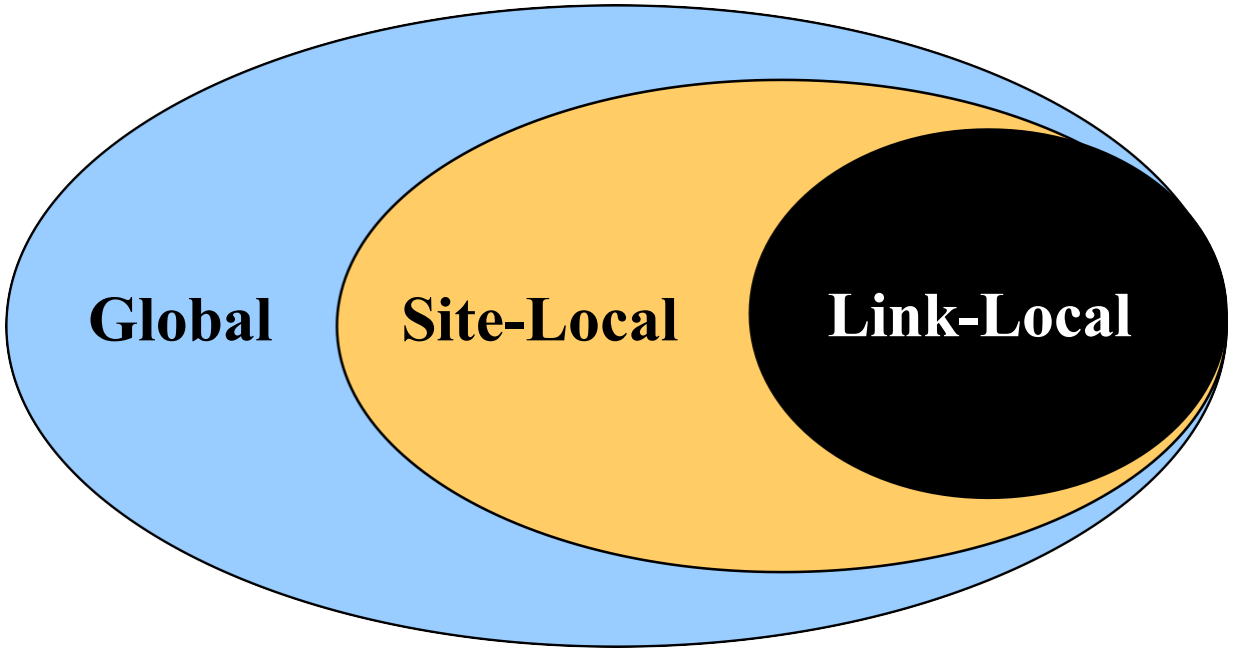
- Nagyobb címtartomány
- Hierarchikus címkiosztás (útválasztás támogatása)
- QoS architektúrák támogatása
- Mobilitás támogatása
- Végpontok közötti biztonságos adatátvitel támogatása
- Egyszerű hálózatmenedzsment
- Automatikus konfiguráció (pl. címkonfiguráció)!
- Többes küldés (multicast) támogatás

Az IPv6 címzési rendszere

- Az IPv6 címtér rendkívül nagy
  - 2^{128} = 340.282.366.920.938.463.463.374.607.431.768.211.456
  - 67 milliárd milliárd cím a Föld területének minden cm^2-ére
  - 10^{30} cím a Föld minden lakosának
  - címek kijelölése és útvonalválasztása hierarchia kialakítását teszi szükségessé
- Az IPv6 cím típusát a cím kezdő bitjei szabják meg
  - a prefix hossza változó - Format Prefix (FP) – de a hostcím jellemzően 64 bitnél nem rövidebb, általában pontosan ennyi!

Az IPv6 címzési rendszere

- Egy interfésznek több címe is lehet, hatásköre lehet:
  - Link Local
  - Site Local
  - Global



Az IPv6 címzési rendszere

- Három típus:
  - Unicast címek
    - egyedi interfészt azonosítanak
  - Multicast címek
    - interfészek egy csoportját azonosítják, a csomagot ezek mindegyikéhez eljuttatják
    - Helyettesítik a broadcast címeket is
  - Anycast címek
    - interfészek egy csoportját azonosítják, a csomagot ezek egyikéhez juttatják el.

Néhány előre definiált multicast cím

Address	Scope	Meaning
FF01::1	Node-Local	All Nodes
FF02::1	Link-Local	All Nodes
FF01::2	Node-Local	All Routers
FF02::2	Link-Local	All Routers
FF05::2	Site-Local	All Routers
FF02::1:FFXX:XXXX	Link-Local	Solicited-Node

- Pl. a ’02’ a 9-12 bit pozícióban azt jelenti, hogy állandó és link-scope címről van szó
- További részletek: http://www.iana.org/assignments/ipv6-multicastaddresses

IPv6 címek – összefoglalás

Address Type	Binary Prefix	IPv6 Notation
Unspecified	00…0 (128 bits)	::/128
Loopback	00…1 (128 bits)	::1/128
Multicast	1111 1111	FF00::/8
Link-Local Unicast	1111 1110 10	FE80::/10
ULA	1111 110	FC00::/7
Global Unicast	(everything else)	
IPv4-mapped	0..0:1111 1111:1111 1111:IPv4	::FFFF:IPv4/128
Site-Local Unicast (deprecated)	1111 1110 11	FEC0::/10
IPv4-compatible (deprecated)	00…0 (96 bits)	::IPv4/128

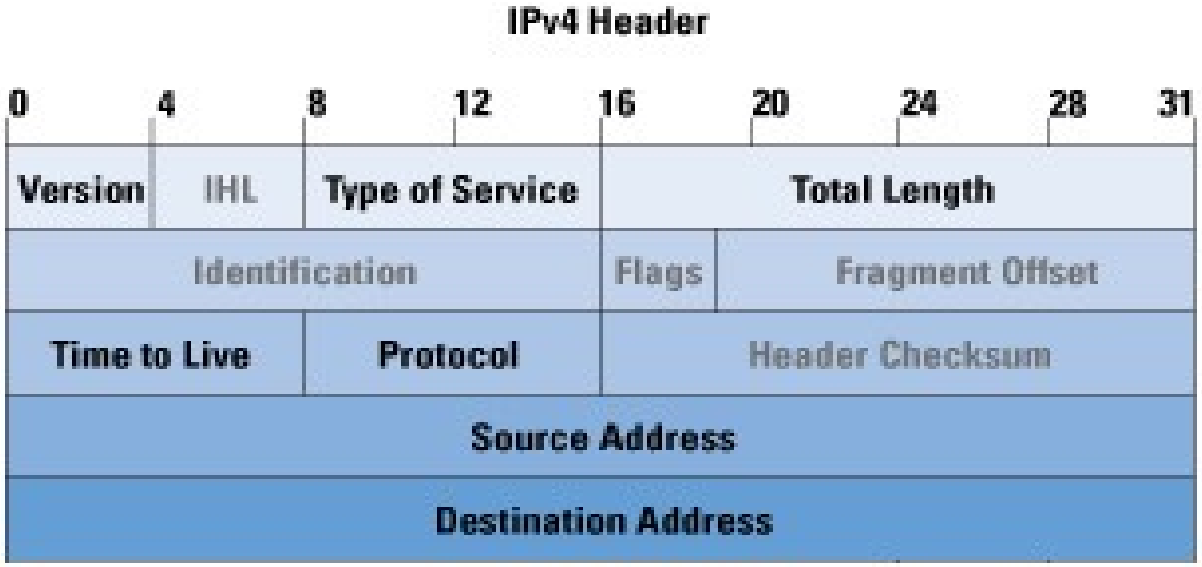
Global Unicast hozzárendelés a 2000::/3-t (001 prefixet) használja

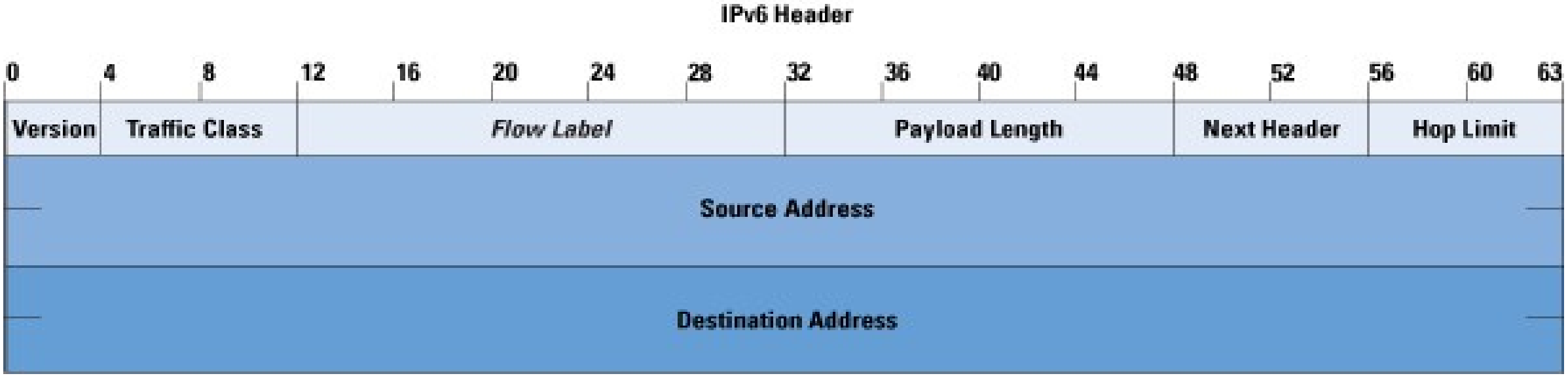
Anycast címek az unicast prefixekből kerülnek foglalásra

Több IPv6 cím per interfész

- A szabályok szerint tehát egy interfésznek számos címe kell legyen alapból (de routereknek pl. még több):
  - link-local cím
  - legalább egy globális unicast és (esetleg több) anycast címek
  - loopback cím
  - all-node multicast cím
  - solicited-node multicast cím az összes unicast és anycast címre
  - más multicast címek
- Preferencia szabályok, hogy mely címeket használja:
  - azonos scope-val rendelkező forrás-cél párok preferáltak
  - legkisebb használható scope célcím használata
  - lehetőleg legyen a cím aktuálisan valid (pl. kivont címet ne!)
  - leghosszabb közös prefixü forrás-cél címpár használata
  - és még elég sok ilyen szabály…(legfontosabbak is kb.10-15 db.)

Az IPv6 alap fejléc formátum (vs. IPv4)





IPv4 fejléc

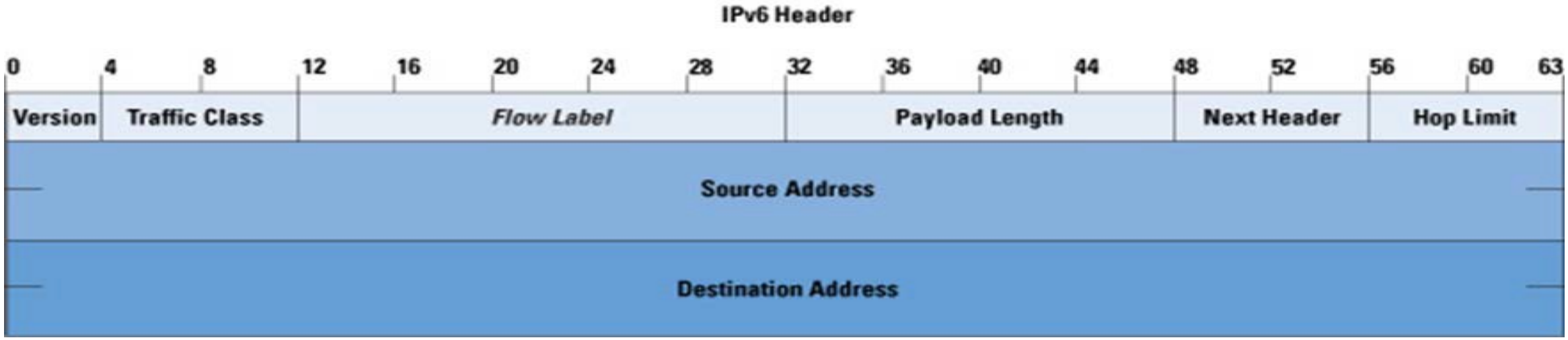
IPv4 Header Format

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

- IHL – IP header length
  - Változó hosszúságú lehet, a fejléc végén levő opciók miatt
- Identification
  - Fragment (darab) azonosítója
- Flags
  - DF – Don’t Fragment
  - MF – More Fragments
- Fragment Offset
  - Mennyivel van elcsúsztatva a darab
- Header checksum
  - Minden útválasztó újraszámolja, mivel a TTL mező változik

IPv6 alap fejléc

- **Version** – verzió (4 bit): IP verziószáma
- **Class** - prioritás osztály (8 bit)
  - csomag prioritását definiálja
  - ToS (Type of Service) mező az IPv4-ben
    - A prioritás jelentése különbözik két forgalmi típus esetén: torlódásvezérelt
      - A csomagok kiszolgálása a prioritás szerint :nem-torlódásvezérelt (valós idejű forgalom).
      - Torlódás esetén a csomagok eldobása a prioritás szerint

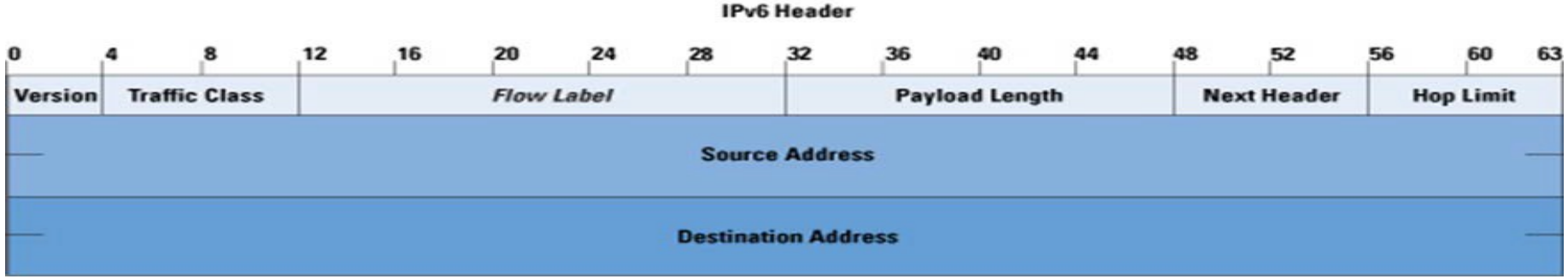


IPv6 alap fejléc

- **Folyam címke (Flow Label) -** Speciális QoS követelményű adatfolyamhoz rendelhető - 20 bit hosszú
  - Kulcsként használható az útvonalválasztók tárolójában a feldolgozási idő csökkentésére:

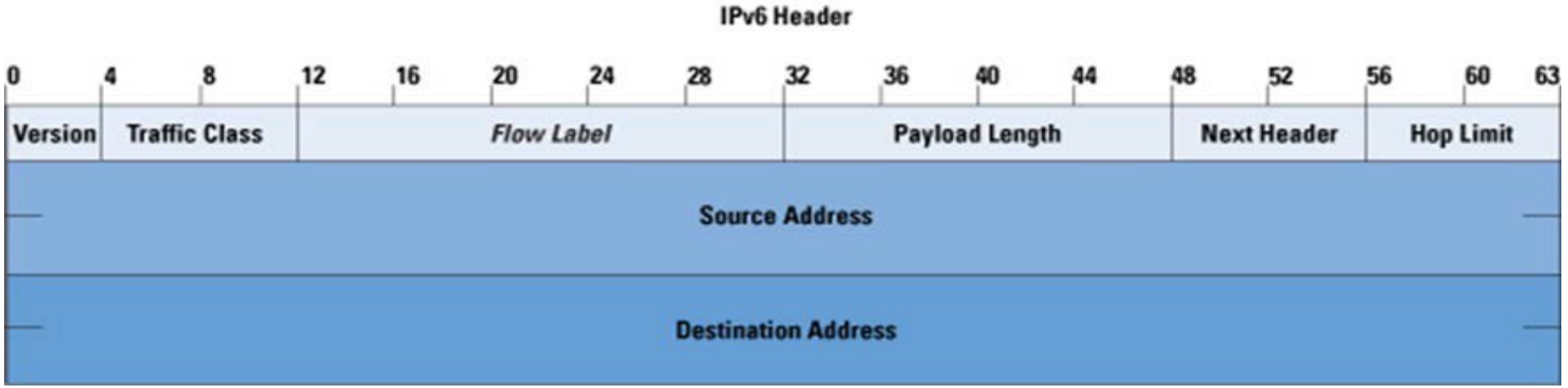
    Egy csomag először érkezik az útvonalválasztóhoz

    - Elmenti a folyam címkéjét a tárolójában
    - Ha ezután ugyanilyen folyam címkéjű csomag érkezik nincs szükség az útvonalválasztó táblában való keresésre, azonnal továbbítható a csomag a folyam címke alapján.
    - Valós idejű forgalomnál, ha több lehetséges útvonal van, a folyam csomagjait ugyanazon az útvonalon tartja, így nem kell újrarendezni a csomagokat



IPv6 alap fejléc

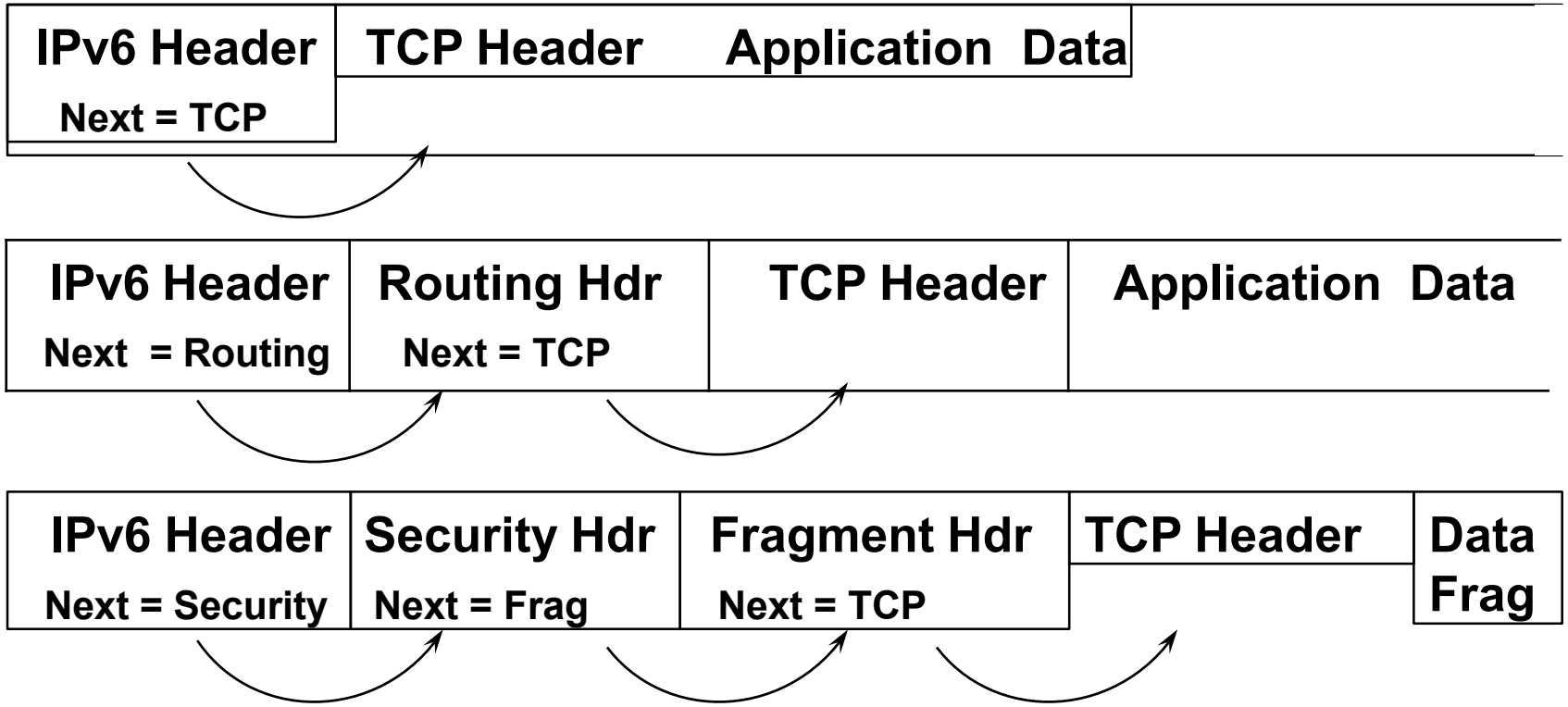
- **Payload Length** (16 bit) - hasznos információ hossza, byte-ban
- **Next-Header** - következő fejléc (8 bit) - azonosítja az alap IP fejlécet közvetlenül követő fejlécet
  - Ez lehet kiegészítő fejléc vagy egy felső rétegbeli protokoll
- **Hop Limit** - ugrás szám (8 bit) - Megadja, hogy a csomag milyen messzire utazik
  - megegyezik az IPv4 Time To Live (TTL) mezőjével
- **Source Address** - forrás cím (128 bit)- a csomag eredeti küldőjének címe
- **Destination Address** - cél cím (128 bit) - a csomag szándékolt vevőjének a címe
  - nem biztos, hogy az utolsó vevő címe, ha opcionális Routing Header-t is tartalmaz a csomag



IPv6 kiegészítő fejlécek

- IP csomag - 40 byte hosszú alap fejléccel kezdődik
- A közbenső hálózatra vonatkozó extra információhoz kiegészítő fejlécek - **Extension Headers**
- Legtöbb kiegészítő fejlécet az útvonalon található útvonalválasztók nem vizsgálják és nem dolgozzák fel, csak a célállomás.
- A kiegészítő fejlécek mindegyike saját egyedi értékkel rendelkezik a next header mező számára
  - így több kiegészítő fejlécet is használhat egyszerre
  - az utolsó kiegészítő fejléc next header mezője azonosítja a felsőbb réteg protokollt
  - A fejléc tetszőleges hosszúságú lehet

IPv6 kiegészítő fejlécek



IPv6 kiegészítő fejlécek

Az ajánlott fejlécsorrend:

- IPv6 Header
- Hop-by-hop Options Header (type = 0)
- Destination Options Header (1)
- Routing Header (type = 43)
- Fragment Header (type = 44)
- Authentication Header (type = 51)
- Encapsulating Security Payload (ESP) (type = 50)
- Destination Options Header (2) (type = 60)
- Upper Layer Header (pl. TCP vagy UDP)

IPv6 kiegészítő fejlécek

- Hop-by-hop Options Header- A csomag útvonalán található gépek számára tartalmaz IP opciókat
  - Az útvonal minden útvonalválasztójának meg kell vizsgálnia és fel kell dolgoznia a Hop-by-hop Header-t
  - **Router Alert opció riasztja a tranzit útvonalválasztókat**
    - Ha a csomag olyan információkat tartalmaz, melyeket egy közbeeső routernek fel kell dolgoznia különben nem próbálja meg értelmezni a csomagot, csak továbbküldi
- Routing Header - Normál esetben az IP csomag forrása a hálózatra bízza a csomag eljuttatását a célhoz
  - Lehetőség van forrás oldali útvonal megadására az útválasztók címeivel
    - A teljes lista a Routing Header-ben (pl. A, B, C, D)
    - A célcím mindig a következő útválasztó címe, kivéve az utolsó útválasztót
    - A célcímet minden útválasztó átírja továbbítás előtt

IPv6 kiegészítő fejlécek

- **Fragment Header**
  - IPv4 – tördelés és visszaállítás automatikusan, ha explicit módon nem tiltják
  - IPv6 - alapértelmezésben a csomagokat nem tördelik
- **Authentication Header -** Garantálja, hogy a kapott csomag hiteles
    - nem változtatták meg az út során
    - megadott küldőtől érkezett
- **Destination Option Header -** A cél opció a cél számára tartalmaz IP opciókat
  - Source routing esetén a közbeeső csomópontoknak is

IPSEC

- Az IPSec protokoll a TCP/IP architektúra **hálózati rétegének** szabványosított biztonsági protokollja.
- Ez azt jelenti, hogy az IP és minden fölötte található protokoll (TCP, UDP, ICMP, stb.) számára védelmet biztosít.

- Két alprotokollja van, az **AH (Authentication Header)** és az **ESP (Encapsulated Security Payload).**
- Az AH és az ESP protokollok kombinálhatók az IP csomagok teljeskörű védelme érdekében.

- Az IPSec protokollhoz tartoznak még az ISAKMP (Internet Security Association and Key Management Protocol) és az IKE (Internet Key Exchange) protokollok. Mindkettő kulcscserével kapcsolatos feladatokat lát el.

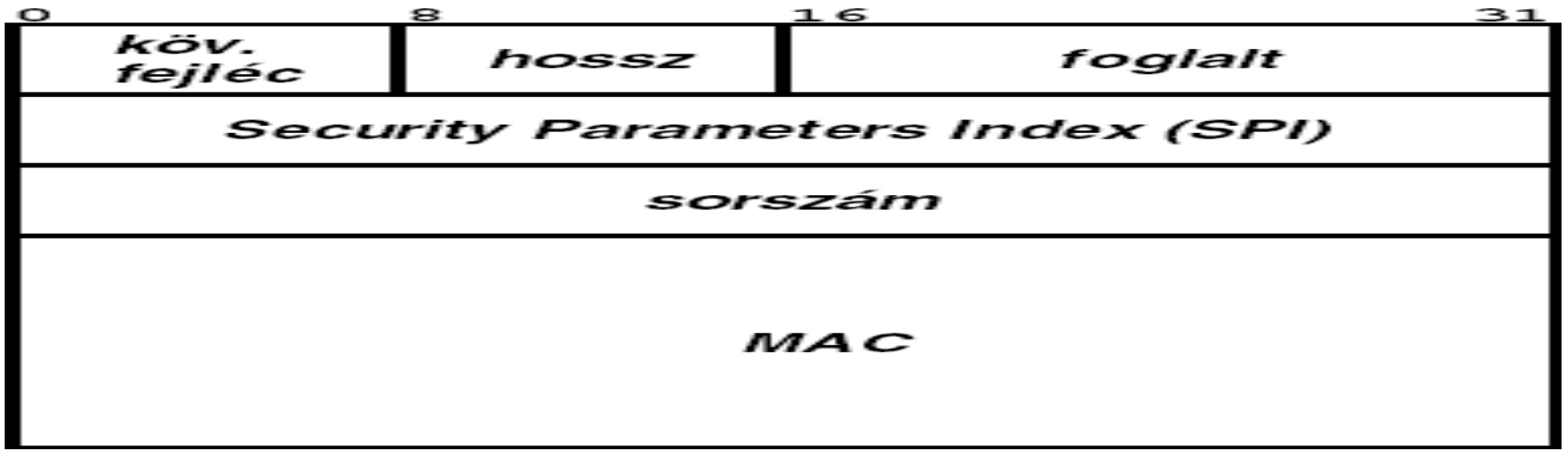
AH protokoll

Az AH protokoll

- integritásvédelmet,
- eredethitelesítést
- visszajátszás elleni védelmet

biztosít az IP csomagok számára.

AH fejléc



Az **integritásvédelmet és az eredethitelesítést** úgy éri el, hogy az IP fejléc és az azt követő felsőbb szintű protokoll fejléce közé beszúr egy AH fejlécet, mely egy, a teljes IP csomagra számolt üzenethitelesítő kódot tartalmaz.

A **visszajátszások detektálásának** érdekében, az IP csomagokat sorszámozza.

ESP protokoll

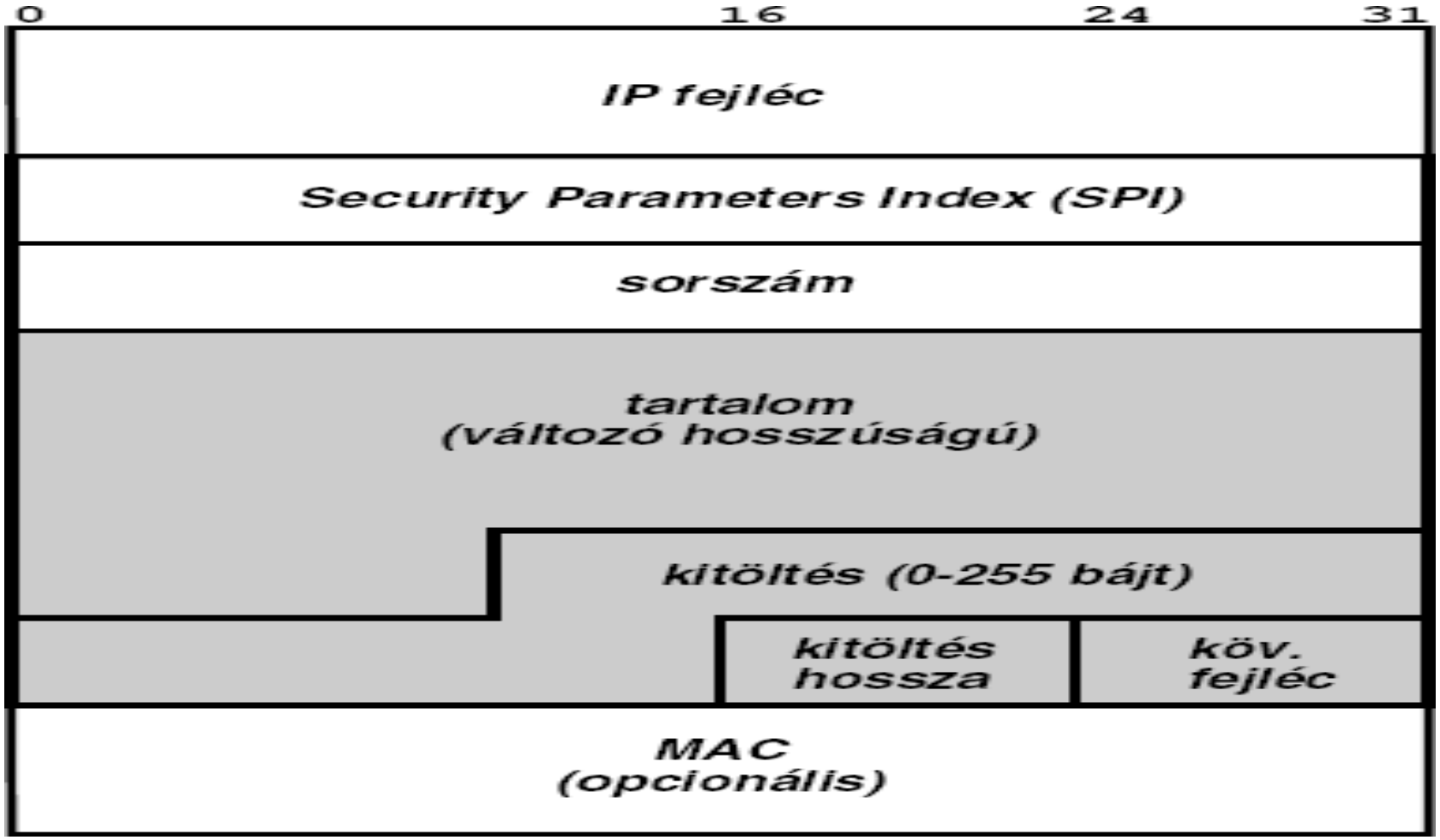
Az ESP protokoll feladata az

- IP csomag tartalmának rejtése,
- a tartalom integritásának védelme (opcionális)

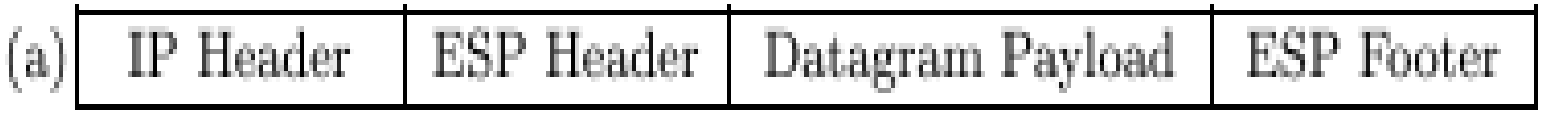
Az előbbit az IP csomag tartalmának rejtjelezésével oldja meg a protokoll, az utóbbit pedig úgy, hogy az ESP fejlécre és a csomag tartalmára számít MAC kódot és azt a csomaghoz csatolja.

Az AH-val ellentétben az ESP MAC nem védi az IP fejléc mezőit.

ESP-vel védett csomag felépítése



IPSEC üzemmódok



Mind az AH, mind az ESP protokollt két üzemmódban lehet használni. Ezeket **szállítási (transport)** és **alagút (tunnel)** módoknak nevezzük.
Szállítási módban (a) az AH vagy az ESP fejléc a csomag eredeti IP fejléce és a felsőbb szintű protokoll (például TCP, UDP) fejléce közé kerül.
Alagút módban (b) azonban az eredeti IP csomagot teljes egészében beágyazzuk egy másik IP csomagba (IP tunneling), és az AH vagy az ESP fejléc az új, és az eredeti IP fejléc közé kerül.

Alkalmazás

Az alagút móddal létrehozhatunk **virtuális magánhálózatokat** (Virtual Private Network , VPN), ahol két, tűzfallal védett belső hálózatot az interneten keresztül, IPSec-et használva biztonságosan összekötünk.