IPv6

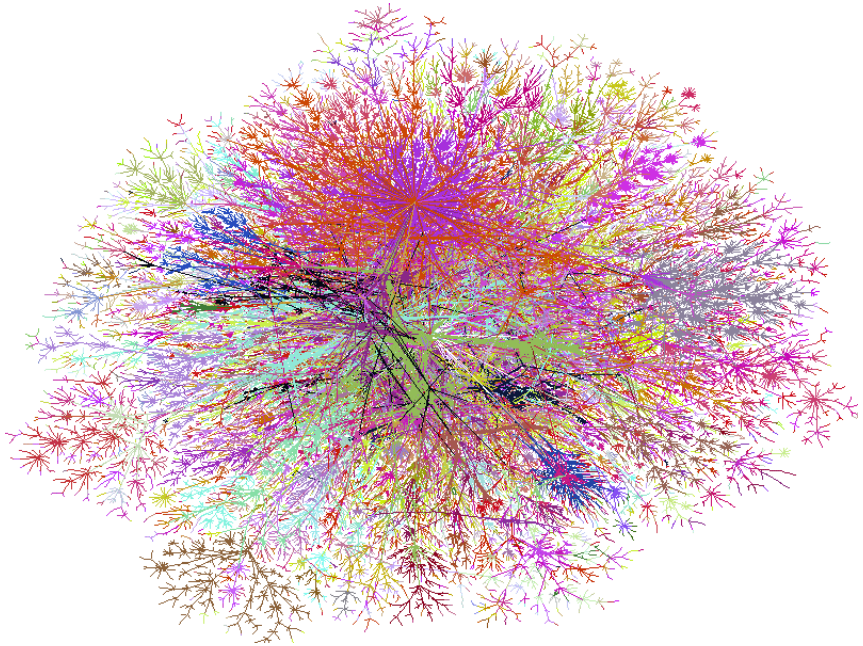
Médiakommunikációs hálózatok (VIHIM161)
Médiatechnológiák és -kommunikáció szakirány

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

2013. március 15.,
Budapest

Tartalom

- Bevezetés: miért kell az IPv4-et lecserélni?
- Az IPv6 általános jellemzői
- IPv6 címzés
- Az IPv6 datagramok felépítése
- Neighbor Discovery Protocol
- ICMPv6



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

BEVEZETÉS: MIÉRT KELL AZ IP 4-ES VERZIÓJÁT LECSERÉLNI?

Motiváció – problémák az IPv4-gyel

- 32 bites címtartomány kimerülése
- Erőforrás-igényes
  - Felesleges mezők vannak a fejrészben (pl. ellenőrző összeg)
  - Tördelésre lehet szükség a köztes csomópontokban
- Nem biztonságos
  - Nem támogatja a hitelesítést és a titkosítást
- Nehézkes konfigurálni
  - Automatikusan csak megfelelő infrastruktúrával
- Mobilitástámogatás csak külön protokollal

A címtartomány kimerülésének okai

- Egyre nagyobb az Internet elterjedtsége
- Fejlődő népes országok (Kína, India, Afrika)
- Egyre több eszköz
  - Mobiltelefonok
  - PDA-k
  - Szenzorok (intelligens otthon, biometrikus ~)
  - TV-készülékek, hűtők, mosógépek, …
- Pazarló címfelhasználás
- **Rövid (32 bites cím)**

Hol tartunk most?

- A központilag osztható IPv4 címtartomány kimerült
  - 2011. 01. 31-i igénylések után a (korábban megalkotott „végjáték” szabályok szerint) 2011. 02. 03-án az IANA ünnepélyesen kiosztotta az utolsó „/8” blokkokat a RIR-eknek
  - Az APNIC címtartománya 2011. 04. 15-én kimerült
  - A RIPE NCC címtartománya pedig 2012. 09. 14-én merült ki
  - Szigorúbb allokációs szabályok a RIR-ek legutolsó „/8” blokkjaira
- De hogyan sikerült idáig kihúzni?
  - Privát IP-címtartományok
  - Subnetting majd supernetting: CIDR (VLSM)
  - Címek visszaadása és újraosztása
  - DHCP
  - NAT – Network Address Translation
  - ISP-k IP-címgazdálkodása

AZ IPV6 ÁLTALÁNOS JELLEMZŐI

Az IPv6 koncepciója

- Megnövelt címtartomány, ami elég a belátható jövőben
- Egyszerűbb és rugalmasan bővíthető fejrészformátum
  - Alapfejrész: kevesebb funkció
  - Bővíthetőség opcionális funkciókkal
  - Gyorsabb feldolgozás a csomópontokban
- Erőforrás-allokáció támogatása
- Biztonságos kommunikáció támogatása
- Mobilitás támogatása
- Továbbfejlesztési lehetőség (nyitottság)

Az IPv6 „infrastruktúra” szolgáltatásai

- A hostok automatikus konfigurálása a Neighbor Discovery Protocol segítségével, ami tartalmazza:
  - Érvényes IPv6 cím előállítása (Stateless Address Autoconfiguration)
  - Átjáró kiválasztása (Router Discovery)
  - DNS szerver címének kiderítése
  - Duplikált cím észlelése (Duplicate Address Detection)
  - Link paramétereinek (pl. MTU) meghatározása (Parameter Discovery)
  - Címfeloldás
- Path MTU Discovery
  - Meghatározható a teljes úton az MTU, így nincs szükség tördelése (csak a feladónál)
- Beépített IPSec támogatás
  - Titkosítás és integritásvédelem a hálózati rétegben

A szolgáltatásokat nyújtó „eszközök”

- „Okos” routerek
  - Hálózati beállítások nyilvántartása és hirdetése a hostoknak
  - Hostok kérdéseinek megválaszolása
- Anycast címzés
  - Szolgáltatás elérésére
    - Pl.: „Valamely router mondja meg, hogy…”
- Multicast címzés
  - Azonos szolgáltatásokat nyújtó egységek egymás közötti kommunikációjához
    - Pl.: „Én már nem vagyok többé PIM-SM router”
- IPv6 Header Extension formában megvalósított opciók
  - Például az IPSec-hez
- ICMPv6
  - Például az NDP használja

IPv6 CÍMZÉS

IPv6 címek mérete és leírása

- 128 bit méretű címek
  - $2^{128} \approx 3{,}4 \cdot 10^{38}$ db ⇨ várhatóan igen sokáig elég lesz ☺
- 8 db 16 bites csoportban, hexadecimális számként írjuk le, a csoportokat kettősponttal („:”) elválasztva
  - FEDC:BA94:7654:3210:0123:4567:89AB:CDEF
- A csoportokban a vezető nullák elhagyhatók
  - FEDC:0094:0004:0000:000C:BA98:7654:3210 helyett írható:
  - FEDC:94:4:0:C:BA98:7654:3210
- A 16 bites, csak nullákat tartalmazó részek elhagyhatóak, ha egymás után vannak (maximum egy ilyen blokk hagyható el, mert csak így egyértelmű a dekódolás):
  - FEDC:0000:0000:0000:000C:BA98:0000:3210 helyett írható:
  - FEDC::C:BA98:0:3210

IPv6 címek leírása (folytatás)

- Egyes IPv6-os címek IPv4-ből származnak. Ekkor megengedett az IPv4 rész decimális írása:
  - 0:0:0:0:0:0:A00:1 helyett írható:
  - ::10.0.0.1
- Hálózati címek (prefixek) jelölése
  - Formátum: <prefix hexadecimálisan, esetleg rövidítve>::/n
  - ::/96
  - FEDB:ABCD:ABCD::/48
  - FEDB:ABCD:AB00::/40 -- *Megjegyzés: az utolsó olyan csoportot, ami nem csupa 0-t tartalmaz, mindig végig ki kell írni!*
- Hivatkozásként
  - http://[FEDC::C:BA98:0:3210]/index.html
  - http://[2001:738:2001:2012:221:70FF:FEC2:BA33]:8080/index.html
  - RFC 3986

Az IPv6 címzési architektúrája

- Az IPv6 címtartomány különféle célokra való felosztását *előtag*ok (prefix) segítségével lehet megadni.
- A következő főbb kategóriákat definiálták (RFC 4291):

Address type	Binary prefix	IPv6 notation
Unspecified	00...0 (128 bits)	::/128
Loopback	00...1 (128 bits)	::1/128
Multicast	11111111	FF00::/8
Link-Local unicast	1111111010	FE80::/10
Global Unicast	(everything else)	

A következő kategória is létezett, de érvénytelenítették:

Site-Local unicast	1111111011	FEC0::/10

Az IPv6 multicast címzése – 1

- Az IPv4-gyel ellentétben *broadcast nincs*.
- A multicast címek felépítése az alábbi:

bitek száma	8	4	4	112
mező neve	*prefix*	*flags*	*scope*	*group ID*

- Az egyes mezők jelentése:
  - prefix: a cím csoportcím voltát jelző előtag, értéke: FF
  - flags: ebben a mezőben jelzőbiteket definiáltak: 0, R, P, T
  - scope: a cím érvényességének a hatókörét fejezi ki (0-F)
  - group ID: az egyes csoportok azonosítására használható bitek

Az IPv6 multicast címzése – 2

- A *flags* mezőben található jelzőbitek értelmezése:
  - 0: fenntartott (reserved)
  - R: A csoporthoz tartozó randevú pont (Rendezvous Point) címe a csoportcímbe beágyazott-e (RFC 3956), 1: igen, 0: nem
  - P: A csoportcímet az azt létrehozó szervezet hálózatának előtagja (Prefix) alapján generálták-e (RFC 3306), 1: igen, 0: nem
  - T: A csoportcím dinamikus-e (Transient), 1: igen, 0: nem, azaz az IANA által kiosztott *well-known multicast address*.

    http://www.iana.org/assignments/ipv6-multicast-addresses/ipv6-multicast-addresses.xml

Az IPv6 multicast címzése – 3

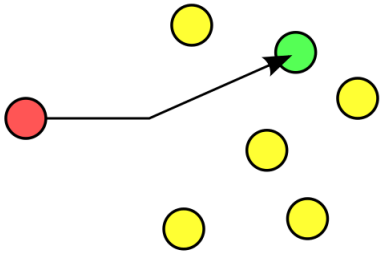
- A csoportcímek érvényességi körét kifejező 4 bites mező (scope) lehetséges értékei:
  - 0: Reserved – fenntartott
  - 1: Interface-local – multicast loopback átvitelére használható
  - 2: Link-Local – hatóköre a fizikai hálózat (üzenet)szórási tartománya (*broadcast domain*)
  - 4: Admin-Local – hatóköre a lehető legkisebb értelmes adminisztratív tartomány
  - 5: Site-Local – hatóköre egy fizikai telephely
  - 6-7: Unassigned – a hálózati adminisztrátorok definiálhatják
  - 8: Organization-Local – egy szervezet összes telephelyére kiterjed
  - 9-D: Unassigned – a hálózati adminisztrátorok definiálhatják
  - E: Global – globális
  - F: Reserved – fenntartott

Az IPv6 multicast címzése – 4

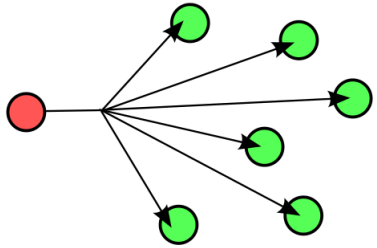
- Az IANA által kiosztott néhány általános célú csoport azonosító (group ID):
  - FF02::1 – link local all nodes – az összes eszköz az adott fizikai hálózaton (broadcast domainben)
  - FF02::2 – link local all routers – minden útválasztó a fenti körben
  - FF05::2 – site local all routers – a telephely összes útválasztója
- Vegyük észre, hogy az FF02::1 jelentése nem más, mint IPv4 esetén egy adott hálózatra vonatkozó broadcast cím!
  - Megjegyzés: IPv4-ben is van ilyen csoportcím: 224.0.0.1
- Vannak minden scope esetén érvényes csoport azonosítók is, például:
  - FF0x::C: SSDP – Az SSDP (Simple Service Discovery Protocol) által használt IPv6 csoportcím. (IPv4 alatt a 239.255.255.250 csoportcímre „szemetel” az SSDP.)

Az Anycast címzés – 1

- Ez NEM egy újabb IPv6 címtípus, mert:
  - IPv4-nél is alkalmazzák (nem IPv6 specifikus)
  - Unicast címeket használ (nem újabb típus)
- Címzési módszerek áttekintése
  - **Unicast**: A csomag pontosan egy általunk kiválasztott állomásnak szól.

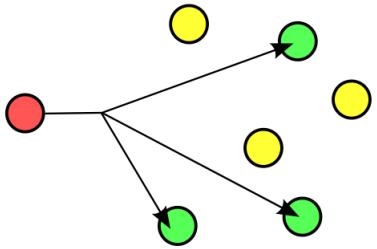


  - **Broadcast**: A csomag az adott hálózaton az összes állomásnak szól.

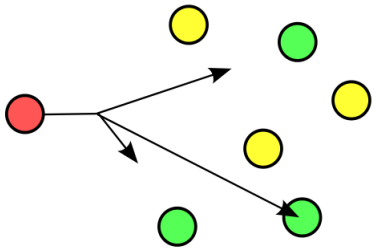


Az Anycast címzés – 2

- Címzési módszerek áttekintése (folytatás)
  - Multicast: A csomag egy csoport összes tagjának szól.



  - Anycast: A csomag egy csoport tagjai közül egynek szól, de nem a feladó, hanem a hálózat dönti el, hogy melyik legyen az. Tipikus választás, hogy legyen a küldőhöz legközelebb eső csoporttag.



Az Anycast címzés – 3

- Az Anycast címzés megvalósítása
  - Ugyanazt azt az IP-címtartományt (közönséges unicast címek!) több helyen is alkalmazzák és hirdetik az Interneten (BGP-vel).
  - Az IP datagramok a legközelebbi célhoz fognak megérkezni.
- Az Anycast címzés használata
  - DNS kiszolgálók esetén: ugyanolyan nevű (IP-című) legfelső szintű névkiszolgáló a világ több pontján is létezik. (A 13-ból 8 ilyen.)
    A kliensek a legközelebbit érik el.
  - Az *IPv4-ről IPv6-ra való átállás* (IPv6 transition) során használt 6to4 megoldás is ezt használja a legközelebbi 6to4 átjáró elérésére.
  - *Tartalomszolgáltató hálózat*ok (CDN: Content Delivery Network) is alkalmazzák abból a célból, hogy a kliens a legközelebbi szerverről tudja letölteni a médiatartalmat.

Speciális Unicast címek – 1

- Unique Local IPv6 Unicast Adresses (RFC 4193)
  - Segítségükkel érvényes globális unicast IPv6 prefix nélkül is lehet IPv6-ot használni.
  - Szerepükben hasonlítanak
    - az RFC 1918 szerinti privát IP-címekhez
    - és az érvénytelenített site-local unicast címekhez (de azok hibáit kiküszöbölve)
  - Felépítésük:

```
| 7 bits |1|  40 bits   |  16 bits  |          64 bits           |
+--------+-+------------+-----------+----------------------------+
| Prefix |L| Global ID  | Subnet ID |        Interface ID        |
+--------+-+------------+-----------+----------------------------+
```

    - Prefix: FC00::/7
    - L: kötelezően 0 értékű
    - Global ID: véletlenszerűen választott, igen jó eséllyel globálisan egyedi
    - Subnet ID: a használó osztja ki a hálózatainak
    - Interface ID: a hálózati interfész 64 bites azonosítója, lásd később

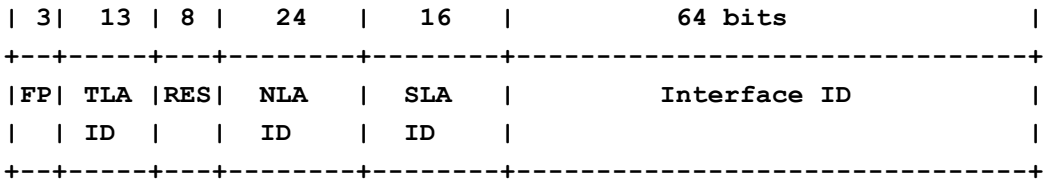
Speciális Unicast címek – 2

- Az *IPv4-ről IPv6-ra való átállás* (IPv6 transition) támogatására szánták az alábbi IPv6 címtípusokat azzal a céllal, hogy IPv6 hálózatokban IPv4 címeket reprezentáljanak:
  - IPv4 Compatible IPv6 Addresses (érvénytelenített!)
    - IPv6 hálózatokban az x.y.z.w IPv4 címet reprezentálta volna ::x.y.z.w (az elején 96 db 0 értékű bit volt)
  - IPv4-Mapped IPv6 Addresses (ez használható!)
    - IPv6 hálózatokban az x.y.z.w IPv4 címet reprezentálja ::ffff:x.y.z.w (az elején 80 db 0 értékű bit van)

Globális Unicast IPv6 címek – 1

- Bár jelenleg az IANA még csak a 2000::/3 tartományból delegált a RIR-eknek, ez elvileg semmiben sem különbözik a többi globális unicast IPv6 címtartománytól!
- A címek szerkezetét korábban RFC 2374 írta le „An IPv6 Aggregatable Global Unicast Address Format” címmel.
  - Erről annyit kell tudni, hogy *elavult* (obsolete), NEM HASZNÁJUK!
  - Az alábbi struktúrával támogatták volna meg az aggregálhatóságot:

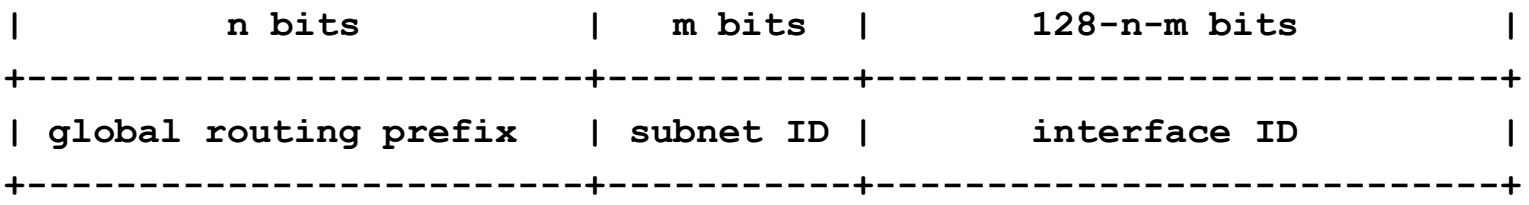
Ez csak egy érdekesség, már nem ezt használjuk!



- FP Format Prefix (001)
- TLA ID Top-Level Aggregation Identifier (régió)
- RES Reserved for future use
- NLA ID Next-Level Aggregation Identifier (szolgáltató)
- SLA ID Site-Level Aggregation Identifier (előfizető és alhálózat)
- INTERF. ID Interface Identifier

Globális Unicast IPv6 címek – 2

- RFC 3587: „IPv6 Global Unicast Address Format”
  - Általános felépítésük



  - global routing prefix
    - hierarchikus felépítésű
    - az aggregációról a RIR-ek és az ISP-k gondoskodnak
    - a site-ok az ISP-ktől kapják
  - subnet ID
    - hierarchikus felépítésű
    - az aggregációról a site-ok adminisztrátorai gondoskodnak
  - Interface ID
    - a hálózati interfészt azonosítja

Globális Unicast IPv6 címek – 3

- Az IPv6 címzési architektúráját definiáló RCF 4291 szerint a 0000/3 tartomány kivételével az Interface ID mérete 64 bit.
  - Így a felépítésük:

```
|         n bits           | 64-n bits |       64 bits              |
+--------------------------+-----------+----------------------------+
| global routing prefix    | subnet ID |       interface ID        |
+--------------------------+-----------+----------------------------+
```

- Ha a jelenleg használt 2000::/3 tartományban az egyes szervezetek a már *elavult RFC 3177* által ajánlott /48-as tartományokat kaptak, akkor a címeik felépítése a következő:

```
| 3 |     45 bits          |  16 bits  |       64 bits              |
+---+----------------------+-----------+----------------------------+
|001|global routing prefix| subnet ID |       interface ID         |
+---+----------------------+-----------+----------------------------+
```

- A BME tartománya: 2001:738:2001::/48

Címallokáció megfontolásai

- Az elavult (obsolete) RFC 3177 szerint a site-ok számára az alapértelmezett allokációs egység mérete a /48 volt.
- Az új irányelvet az RFC 6177 „IPv6 Address Assignment to End Sites” fogalmazza meg.
  - Kis felhasználóknál nem szükséges a pazarló /48 méret.
  - A /64 viszont nem elég, mert idővel több fizikai hálózatra lehet szükség.
  - Szempont a takarékosság is, de az is, hogy később sem legyen szükség NAT-ra (a site kapjon elegendő címet).
  - A reverse DNS feloldás szempontjából megfontolandó a 4 bites határra való illeszkedés.
  - Megemlíti az egyes RIR-ek gyakorlatát (/56-os méret), de alapelv, hogy nincs új alapértelmezett méret.
  - Bár a /128 bizonyos esetekben elfogadott, site esetén semmiképpen sem javasolt.

Az IPv6 címtér felosztása

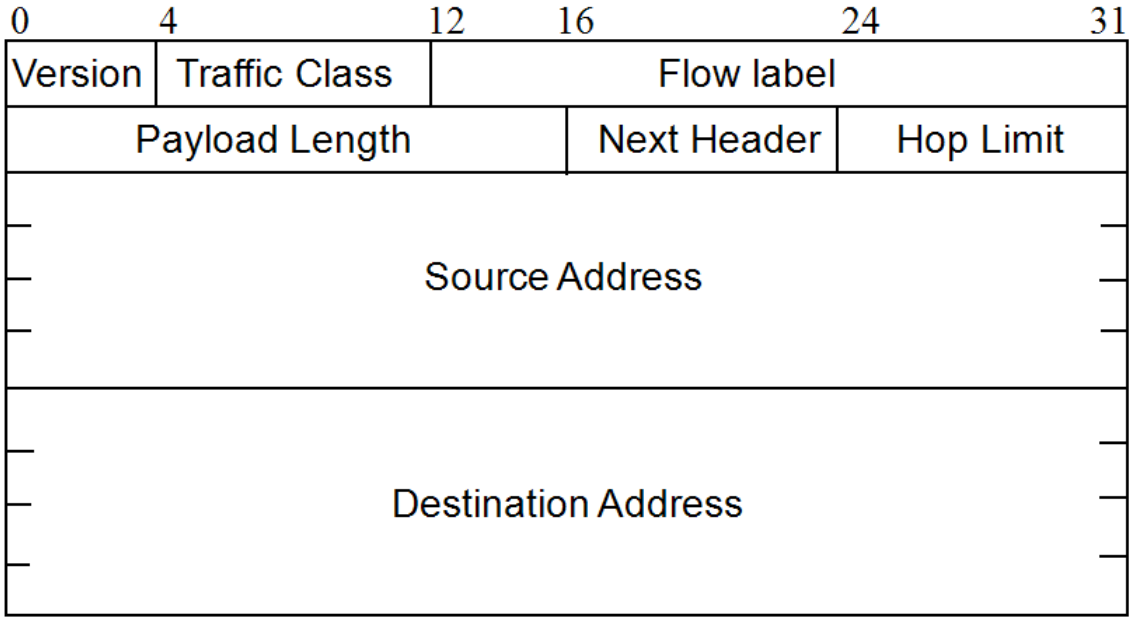
IPv6 Prefix	Allocation	Reference	Note
0000::/8	Reserved by IETF	[RFC4291]	[1][5][6]*
0100::/8	Reserved by IETF	[RFC4291]	
0200::/7	Reserved by IETF	[RFC4048]	[2] (korábban speciális célja volt)
0400::/6	Reserved by IETF	[RFC4291]	
0800::/5	Reserved by IETF	[RFC4291]	
1000::/4	Reserved by IETF	[RFC4291]	
2000::/3	Global Unicast	[RFC4291]	[3] (a többi is Global Unicast, de ebből oszt az IANA)
4000::/3	Reserved by IETF	[RFC4291]	
6000::/3	Reserved by IETF	[RFC4291]	
8000::/3	Reserved by IETF	[RFC4291]	
A000::/3	Reserved by IETF	[RFC4291]	
C000::/3	Reserved by IETF	[RFC4291]	
E000::/4	Reserved by IETF	[RFC4291]	
F000::/5	Reserved by IETF	[RFC4291]	
F800::/6	Reserved by IETF	[RFC4291]	
FC00::/7	Unique Local Unicast	[RFC4193]	
FE00::/9	Reserved by IETF	[RFC4291]	
FE80::/10	Link Local Unicast	[RFC4291]	
FEC0::/10	Reserved by IETF	[RFC3879]	[4] (korábban Site Local)
FF00::/8	Multicast	[RFC4291]	

* Számos speciális célút tartalmaz: ::/128, ::1/128, ::/96, ::ffff:/96, 64:ff9b::/96 (Well-Known Prefix, IPv4-Embedded IPv6)

Forrás: http://www.iana.org/assignments/ipv6-address-space/

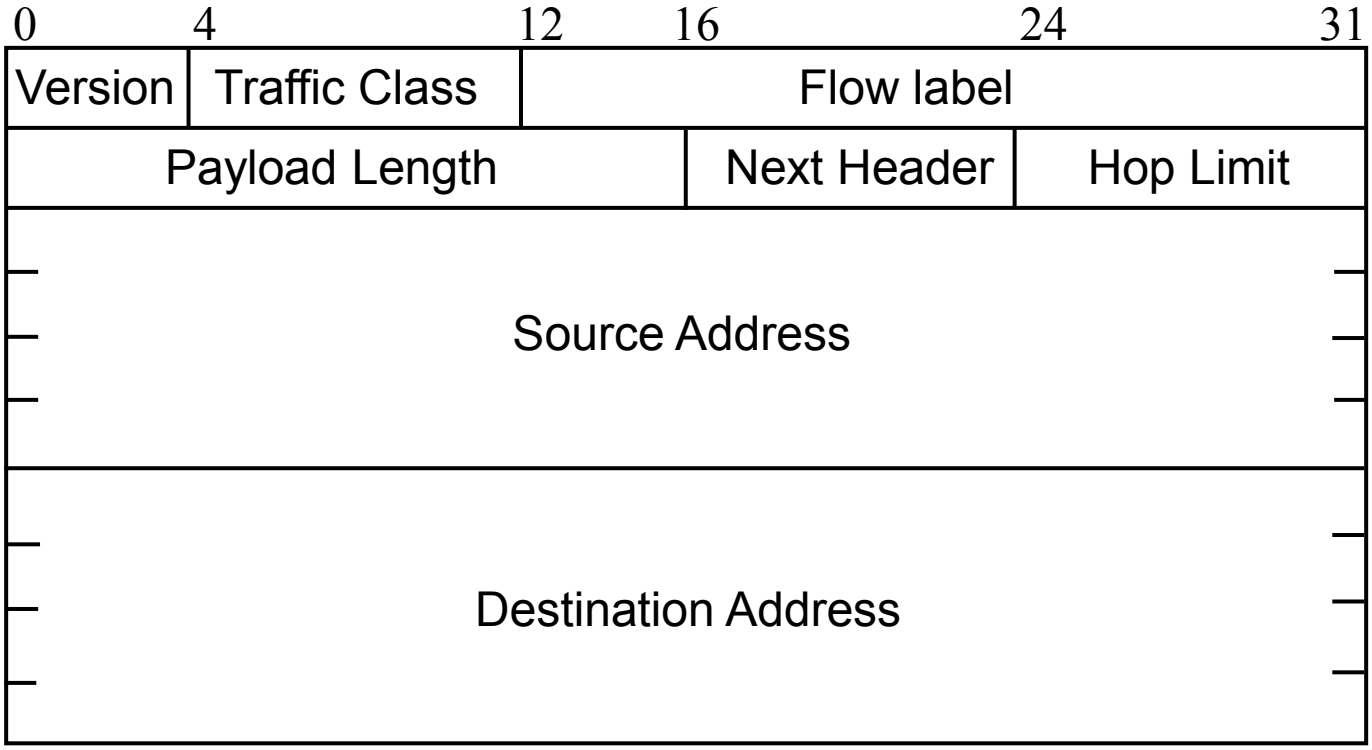
Szabványos dokumentációs prefix

- Dokumentációkban példákat szoktak használni
  - A példák címhasználatából adódó lehetséges problémák:
    - Zavar a fejekben
    - Ütközés működő rendszerekkel
- Lefoglaltak egy globális unicast prefixet kifejezetten dokumentációs célra: 2001:DB8::/32 (RFC 3849).
  - Ezt a prefixet soha senkinek sem fogják kiosztani és nem is routolják.
  - Ettől még nem számít lokális unicast prefixnek!
  - Ha egy példában ezt a prefixet használják, és valaki a példát szó szerint begépeli, az nem fog kárt okozni, mert a prefixet a valós életben soha semmire nem használjuk.
  - A prefixet helyi hálózatokban is kiszűrhetik; senki ne számítson rá, hogy működni fog, ha használni próbálná!
- Megjegyzés: IPv4-nél is vannak ilyenek, lásd: RFC 5737



IPv6 DATAGRAM FELÉPÍTÉSE

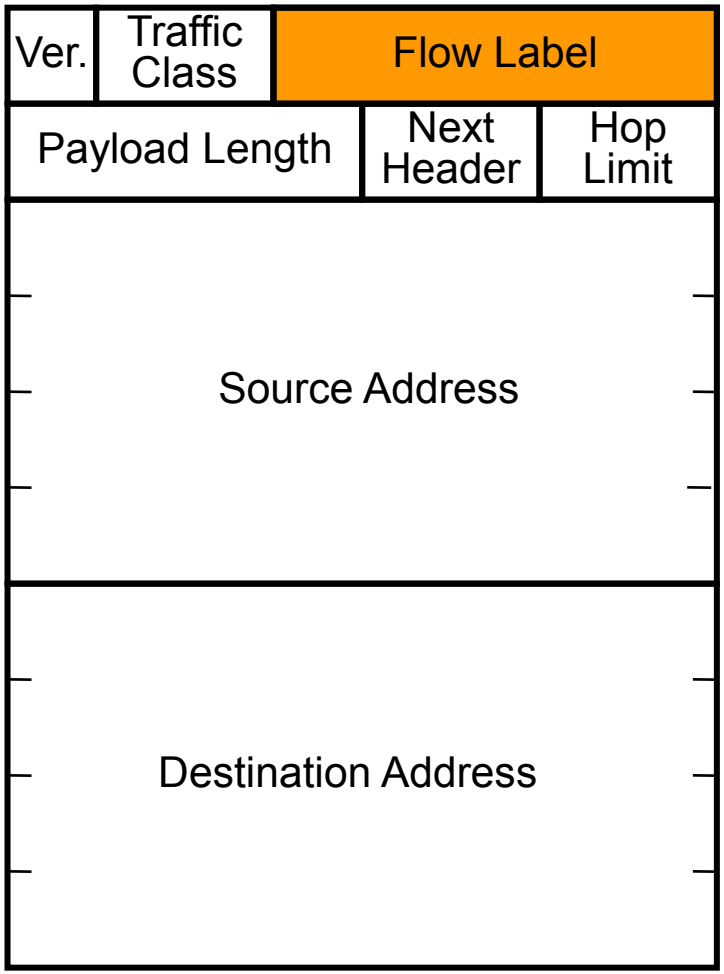
A kötelező IPv6 fejrész szerkezete

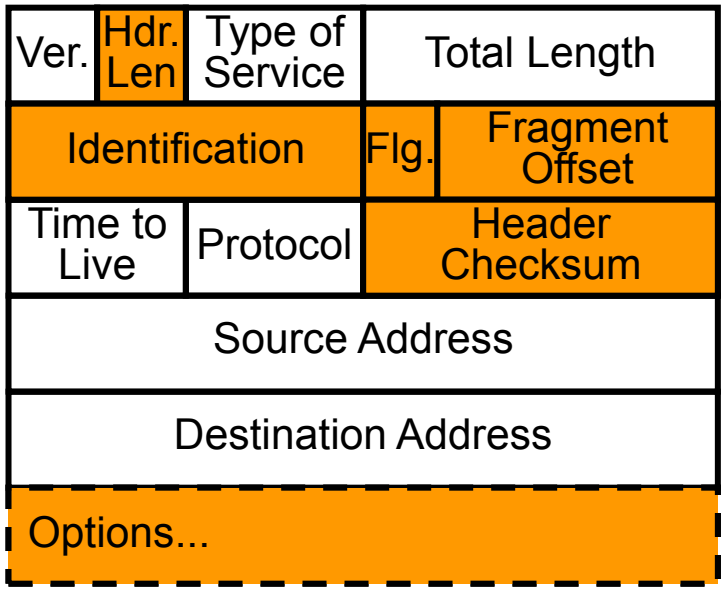


- A kötelező fejrészt változó számú opció követheti
- Majd az adatrész következik

Az IPv6 eredeti specifikációja: RFC 2460

IPv6 és IPv4 fejrészek összehasonlítása





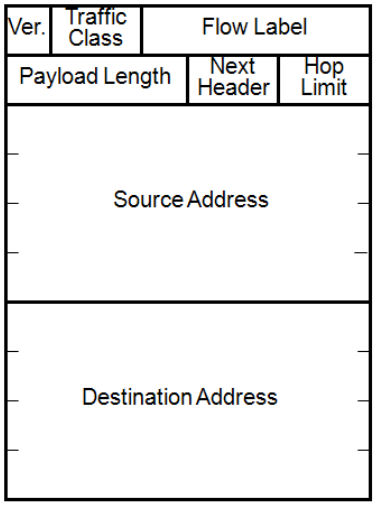
A kiemelt részek a másik verzióban nem találhatók meg.

Az IPv6 fejrésze alapesetben kétszer akkora, mint az IPv4-é.

Ami az IPv6 fejrészből kimaradt…

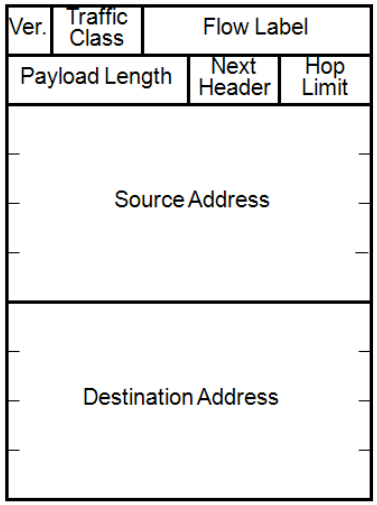
- Nem változik a (kötelező) fejrész mérete
  - Rögzített méret ⇨ nő a feldolgozási sebesség
  - Nem kell IHL mező ⇨ kisebb fejrész
  - De azért van lehetőség a fejrész kiterjesztésére (Next Header)
- Nincs ugrásonkénti tördelés
  - ⇨ nő a feldolgozási sebesség
  - Nem kell ehhez használt mező ⇨ kisebb fejrész
  - De MTU felderítés (Path MTU Discovery) kell!
- Nincs ellenőrzőösszeg (checksum)
  - Nem kell minden routernek ellenőriznie
    ⇨ nő a feldolgozási sebesség
  - Általában kevés a hiba (jó minőségű kapcsolatok link szinten)

Az IPv6 fejrész mezői – 1



- **Version** (4 bit)
  - IPv6 esetén a *verziószám* értéke: 6
  - De már link szinten megkülönböztethetők
    - EtherType értéke: IPv4: 0x0800; IPv6: 0x86DD
- **Traffic Class** (8 bit)
  - A *forgalmi osztály* lehetőséget nyújt QoS biztosítására, az IPv4 *Type of Service* mezőjével azonos módon
- **Flow Label** (20 bit)
  - A *folyam azonosító címke* kapcsolatok azonosítását szolgálja
    - Nem független datagrammok!
  - Az adatfolyamot a forrás- és célcím + a flow label együtt azonosítják
  - Virtuális összeköttetések biztosítása az adatfolyamok számára
  - QoS-t és igazságos adatsebesség-megosztást tesz lehetővé
  - Növekedési képesség probléma a folyam-alapú eljárásoknál

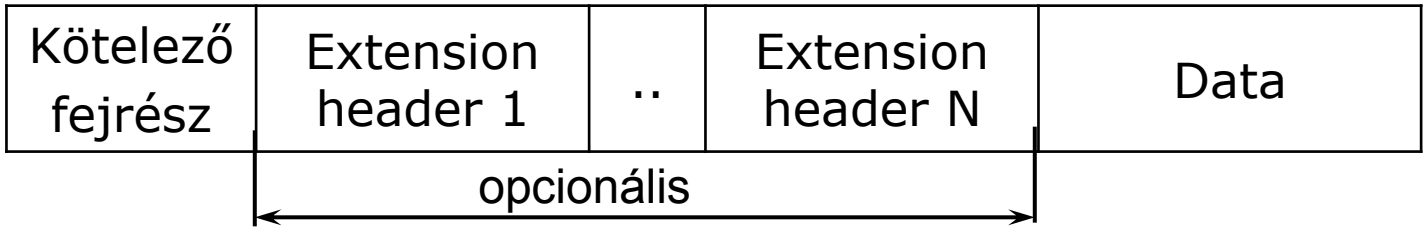
Az IPv6 fejrész mezői – 2



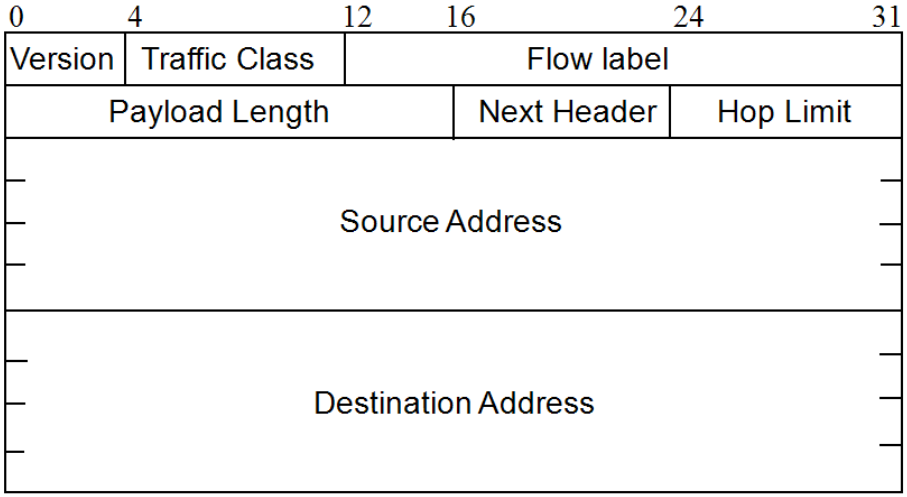
- **Payload Length** (16 bit)
  - Az *adatmező hossza* nem tartalmazza a fejrészt
  - Maximum 65535 lehet (de: jumbogram opció)
- **Next Header** (8 bit)
  - A következő fejrész kétféle lehet
    - A beágyazott PDU típusát adja meg (mint az IPv6 Protocol mezője)
    - Az IPv6 fejrész kiterjesztését jelentő „Extension header” típusát adja meg
- **Hop Limit** (8 bit)
  - Az *ugrás korlát*ot lényegében úgy használjuk, mint az IPv4 TTL-t (de nem másodpercben mérjük)
- **Source/Destination Address** (mindegyik 128 bit)
  - A *forrás-* és *célcím* a fejrész méretének jelentős részét teszi ki

Az IPv6 fejrész kiterjesztése

- Általános csomagformátum:

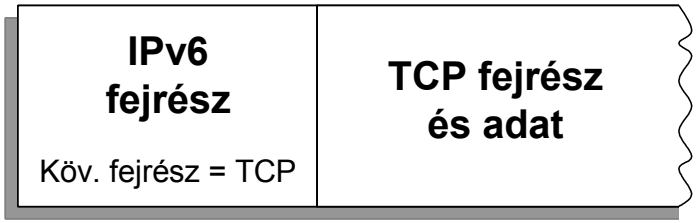


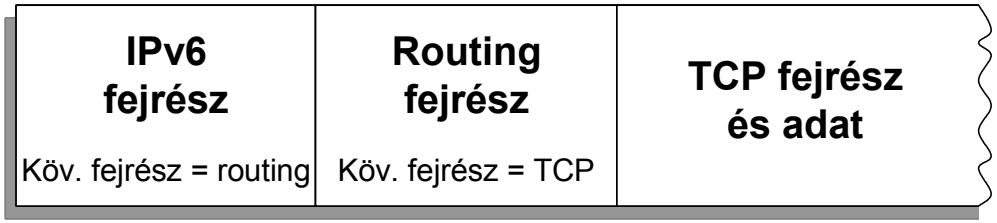
- Ahol a kötelező fejrész:

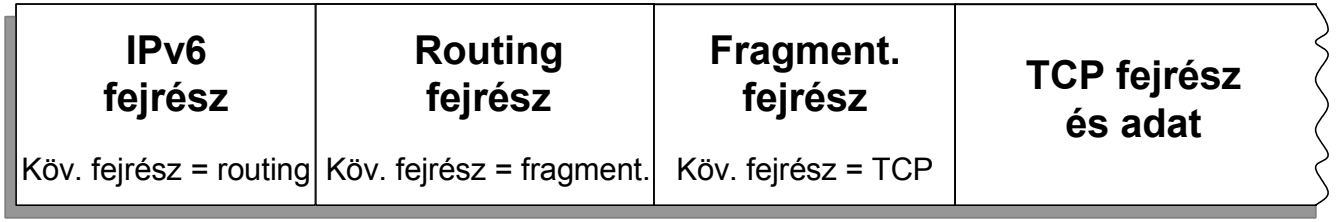


Példák IPv6 fejrészre

- Kiterjesztés nélkül, egy, illetve két kiterjesztéssel:







IPv6 „opciók” – Header Extensions – 1

Célja:

- A kötelező fejrész kiegészítése opcionális lehetőségekkel

Típusai:

- **Hop-by-Hop Options Header** (0)
  - Különféle információk, amelyeket minden csomópontnak meg kell vizsgálnia
  - Jumbogrammok támogatása (óriás-datagrammok)
  - QoS támogatása
- **Routing Header** (43)
  - Routerek felsorolása, amelyeket útba kell ejteni
  - Az IPv4 LSRR opciójához hasonló

IPv6 „opciók” – Header Extensions – 2

- **Fragment Header** (44)
  - Hasonló, mint v4-ben, de csak a forrás darabolhat
    - A tördelés bonyolultabb, mert az opciók egy részét (amit az útvonal mentén fel kell dolgozni) mindegyik töredékbe bele kell tenni, a többit pedig csak az elsőbe.
  - Ehhez kell a Path MTU Discovery
  - De feltételezik, hogy az MTU legalább 1280
- **Destination Options Header** (60)
  - Csak a célállomás vizsgálja
  - Egyelőre még nincs funkciója
- **Authentication Header** (AH) (51)
  - IPsec céljára
- **Encapsulation Security Playload Header** (ESP) (50)
  - IPsec céljára

IPsec az IPv6-ban

- Az IPsec (RFC 4301) az IPv6-ban két Extension Headert használ:
  - *Authentication Header (RFC 2402)*
    - Valóban a látszólagos feladó küldte-e?
    - Lett-e módosítva a csomag?
  - *Encapsulating Security Payload Header (RFC 2406)*
    - Titkosított a csomag további tartalma
- Korábban IPsec-re minden IPv6 csomópontnak képesnek kellett lennie, ez ma már csak ajánlott.
  - RFC 4294 (IPv6 Node Requirements) szerint az IPsec implementációja még minden IPv6-ra képes eszközben kötelező (MUST) volt.
  - Az RFC 4294 helyett kiadott RFC 6434 (obsoletes RFC 4294) követelményeiben ez ajánlottra (SHOULD) változott.
    - Ezt a létező egyéb megoldásokkal (pl. TLS, SSH) és azzal indokolja, hogy az IPsec nem feltétlenül az ideális megoldás minden esetben. (RFC 11. rész)

NEIGHBOR DISCOVERY PROTOCOL

Az NDP áttekintése

- Az NDP a TCP/IP referenciamodell internet rétegében működik
- Egy host működéséhez szükséges azonosítókat, paramétereket képes beszerezni, többek között képes:
  - Állapotmentes automatikus címkonfigurációra (SLAAC)
  - Routerek címének megállapítására
  - DNS szerverek címének megállapítására
  - Annak ellenőrzésére, hogy egy IPv6 címet már használnak-e (DAD)
  - Címfeloldásra (IPv6 címből MAC cím)
  - Az adott linken érvényes prefixek és MTU kiderítésére
- Működéséhez ICMPv6 protokoll üzeneteket használ
- Aktuális definíciója: RFC 4861

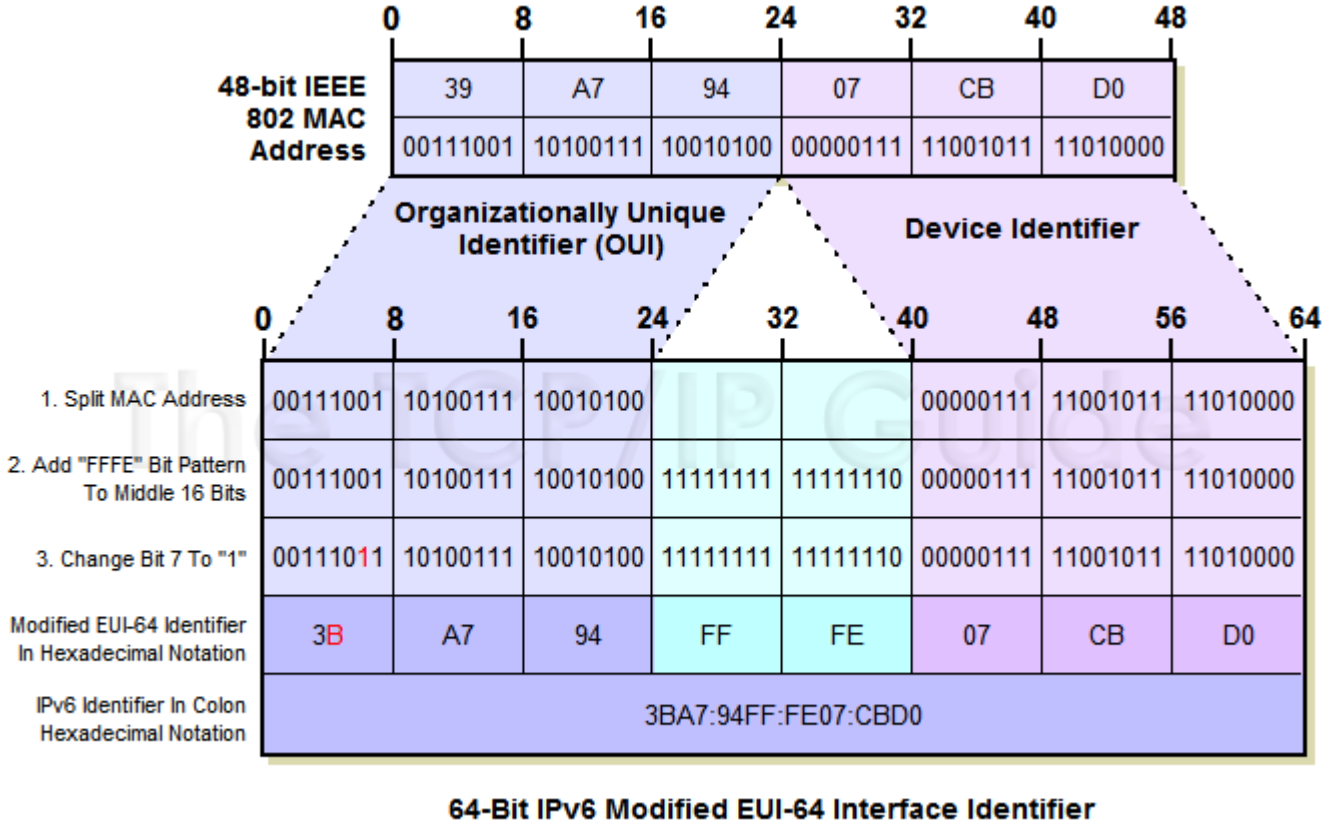
A módosított EUI-64 algoritmus – 1

- Célja a hálózati interfész 48 bites MAC címéből 64 bites azonosító létrehozása.
- Az algoritmus lépései:
  - A 48 bites címet középen kettévágva a két fél közé beszúrjuk az FFFE 16 bites értéket.
  - A MAC cím első bájtjának második legkisebb helyiértékű bitjét 1-re állítjuk.
    - Ez a MAC cím OUI (Organizationally Unique Identifier) részének U/L bitje, tehát azt jelezzük vele, hogy nem univerzálisan egyedi, hanem lokálisan adminisztrált címről van szó.
- Az algoritmus működését egy példával illusztráljuk
  - Az eredeti MAC cím: 00:21:70:C2:BA:33
  - Az első lépés eredménye: 00:21:70:FF:FE:C2:BA:33
  - A második lépés eredménye: 02:21:70:FF:FE:C2:BA:33
  - Az IPv6-nál használt alakban: 221:70FF:FEC2:BA33

A módosított EUI-64 algoritmus – 2

- Az algoritmus működését bit szinten illusztráló ábra

Forrás: http://www.tcpipguide.com/free/t_IPv6InterfaceIdentifiersandPhysicalAddressMapping-2.htm



64-Bit IPv6 Modified EUI-64 Interface Identifier

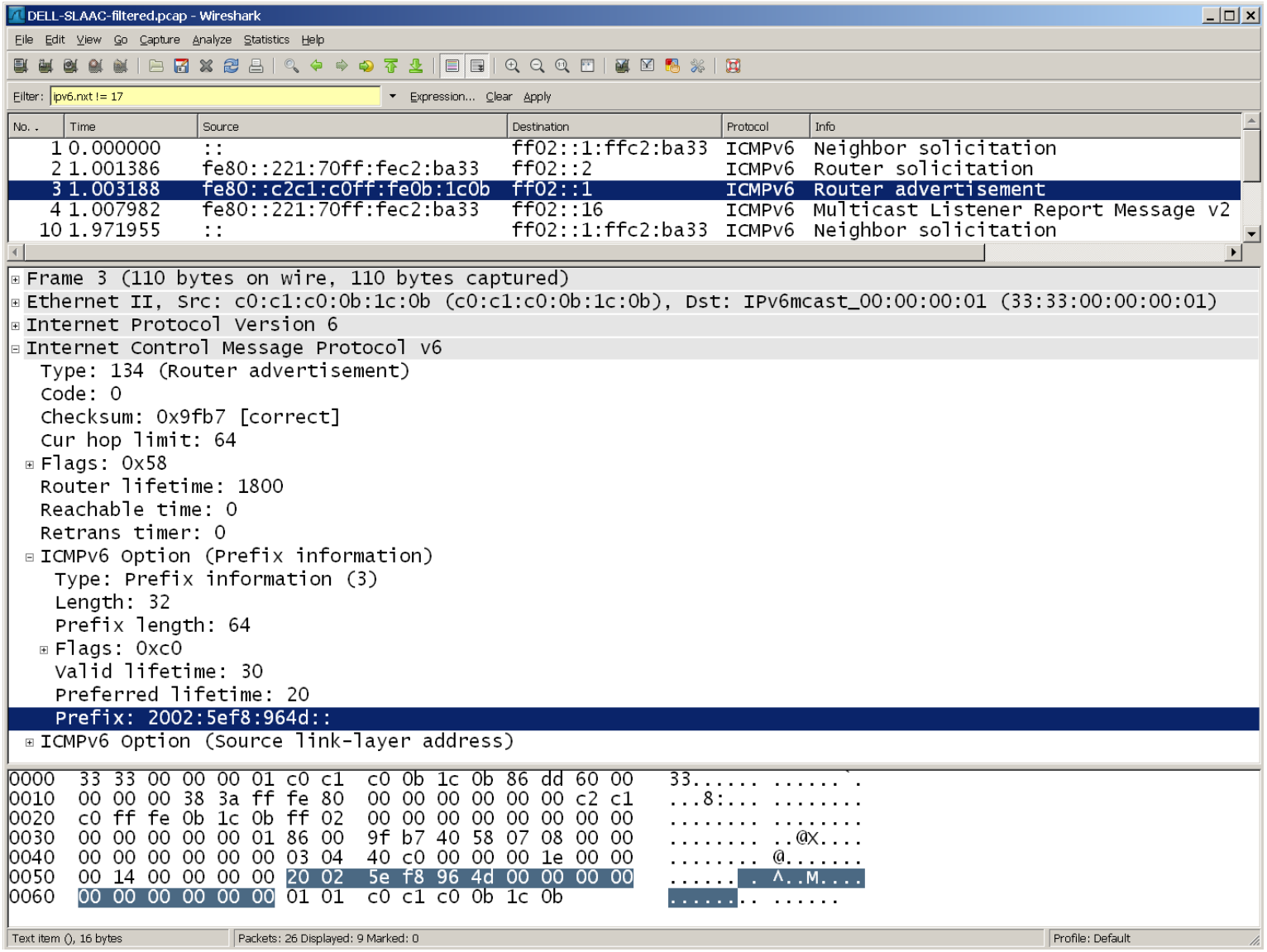
Állapotmentes autom. címkonf. – 1

- Az állapotmentes automatikus címkonfiguráció (Stateless Address Autoconfiguration) lépései:
  - Link-lokális cím generálása (FE80::/64 + módosított EUI-64)
  - Link-lokális cím ellenőrzése (ICMPv6 Neighbor Solicitation)
    - A küldő IP címe érvénytelen (::/128)
    - Mint IPv4-nél az ARP Probe üzenettel; ha nincs válasz: OK
  - Hálózati prefix kérése (ICMPv6 Router Solicitation)
  - Hálózati prefix információ vétele (ICMPv6 Router Advertisement)
  - Global Unicast cím előállítása (a kapott prefix + módosított EUI-64)
  - Global Unicast cím ellenőrzése (ICMPv6 Neighbor Solicitation)
- Az SLAAC biztonsági kockázattal jár
  - Hamis Router Advertisement üzenettel a kliens megtéveszthető
    - SLAAC Attack http://resources.infosecinstitute.com/slaac-attack/
    - RFC 6104: Rogue IPv6 Router Advertisement Problem Statement

Állapotmentes autom. címkonf. – 2

- Előre elkészített capture fájl alapján tanórán Wireshark segítségével vizsgáljuk az SLAAC folyamatát, otthoni elemzésre a capture fájl elérhető a tárgy anyagai között.
  - A nem kívánatos egyéb forgalom kiszűrése érdekében a capture fájl készítése az **`ip6`** capture filterrel történt.
  - A capture fájlba így is bekerültek a DNS szerver hiányában küldött *multicast DNS* üzenetek,ezeket az **`ipv6.nxt!=17`** display filterrel tudjuk megjelenítéskor kihagyni. (A 17 az UDP protokollt azonosítja.)
- Figyeljük meg:
  - Az üzenetek sorrendjét és ICMPv6 típusát!
  - Az ICMPv6 üzenetekben milyen IPv6 és MAC címek vannak?
  - Ellenőrizzük a módosított EUI-64 generálását!
  - Végül milyen prefixet kapott a kliens?

Állapotmentes autom. címkonf. – 3



Internet Control Message Protocol version 6

ICMPv6

- Az ICMP IPv6-os implementációja
- IPv6 felett utazik (next header=0x3A), de minden IPv6 implementáció kötelező része!
- Üzenettípusok
  - Hiba üzenetek
  - Információs üzenetek
- Aktuális dokumentáció: RFC 4443

ICMPv6 üzenetek felépítése

- Az ICMPv6 üzenetek formátuma egyedi
- Ami közös bennük, az az ICMPv6 fejrész első 32 bitjén található 3 adatmező:
  - Type (8 bit)
    - 0-127: hibaüzenetek
    - 128-255: információs üzenetek
  - Code (8 bit)
  - Checksum (16 bit)
- A további rész kiosztása függ az üzenet típusától

Fontosabb ICMPv6 üzenetek – 1

- **1 – Destination Unreachable** (cél nem elérhető)
  - Mint az azonos nevű ICMP üzenet
- **2 – Packet Too Big** (a csomag mérete túl nagy)
  - Az IPv6 útközben nem tördel. Ha egy csomag nem fér bele az MTU-ba, akkor a router eldobja, és visszajelzést küld.
- **3 – Time Exceeded** (időtúllépés)
  - Mint az azonos nevű ICMP üzenet
- **4 – Parameter Problem** (paraméter értelmezési hiba)
  - A hiba okát a Code mezőben jelzi:
    - 0: Hibás IPv6 fejrész mező
    - 1: Ismeretlen Next Header típus
    - 2: Ismeretlen IPv6 opció

Fontosabb ICMP üzenetek – 2

- **128 – Echo Request** (visszhang kérés)
  - Mint az azonos nevű ICMP üzenet
- **129 – Echo Reply** (visszhang válasz)
  - Mint az azonos nevű ICMP üzenet
- **133 – Router Solicitation** (router info kérése)
  - Az NDP része
- **134 – Router Advertisement** (router info adása)
  - Az NDP része, lehet kérésre válasz, de a routerek kérés nélkül is hirdetik.
  - A kéretlen hirdetés szándékosan nem pontosan periodikus.
- **135 – Neighbor Solicitation** (MAC-cím kérése)
  - Az NDP része, az ARP megfelelője (Request és Probe)
- **136 – Neighbor Advertisement** (MAC-cím hirdetése)
  - Lehet kérésre válasz, ekkor Solicited Neighbor Advertisement
  - Kérés nélkül is küldhető (pl. IP cím változásakor), ez Unsolicited N.A.

Fontosabb ICMP üzenetek – 3

Az alábbi üzenetekkel majd a multicast routing protokolloknál találkozunk:

- **130 – Multicast Listener Query** (csoporttagok lekérd.)
  - Multicast cím megadás nélkül: mely multicast csoportoknak vannak tagjai az adott hálózaton?
  - Multicast cím megadásával: a megadott című multicast csoportnak vannak-e tagjai az adott hálózaton?
- **131 – Multicast Listener Report** (csoporttagság jelzése)
  - A csoporttagok ezzel az üzenettel jelzik igényüket a multicast forgalomra.
- **132 – Multicast Listener Done** (mcast csoportból kilépés)
  - A csoporttagok ezzel az üzenettel jelzik, hogy már nem tartanak igényt az adott multicast csoport forgalmára.

Összefoglalás

- Bevezetés: miért kell az IPv4-et lecserélni?
- Az IPv6 általános jellemzői
- IPv6 címzés
- Az IPv6 datagramok felépítése
- Neighbor Discovery Protocol
- ICMPv6

Kérdések?

KÖSZÖNÖM A FIGYELMET!

Hálózati Rendszerek és Szolgáltatások Tanszék

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