MŰEGYETEM 1782

BME

# BEVEZETÉS AZ IPV6 ALAPÚ HÁLÓZATOK VILÁGÁBA


Bokor László
tudományos segédmunkatárs
BME Híradástechnikai Tanszék
bokorl@hit.bme.hu


2014. április 30.,
Budapest

# Kivonat

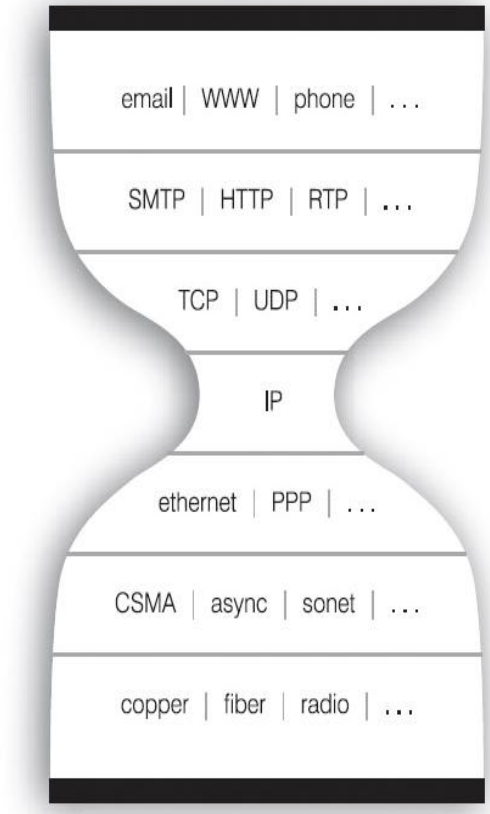
- Az Internet Protokollról dióhéjban
- Gondok az IPv4-gyel
- Ideiglenes megoldások
- A hosszú távú megoldás: IPv6
- Az IPv6 újdonságai
- Az IPv6 fejlécstruktúrája
- IPv6 címekről dióhéjban
- ICMPv6
- IPv6 és mobilitás
- Tanszéki R&D IPv6 témákban
- Összefoglalás

# Mi is az Internet?

- Nincs jó definíció
  - „kisebb–nagyobb hálózatok összekapcsolása”
  - „IP-lal működő hálózatok”
  - Hagyjuk meg a filozófusoknak
- Ami fontos: az Internet használatához IP kell
  - Internet Protokoll
  - Két verziója van: IPv4 és IPv6
    - Bár ma az előbbi az egyeduralkodó, a félév során az utóbbira fókuszálunk
    - ma IPv4, de rövidesen IPv6

# Az Internet Protokoll

- Úgy képzelhető el, mint a postaszolgálat
- Az IP (pont úgy, mint a Magyar Posta)
  - csomag alapú (csomagkapcsolt) protokoll
  - datagram jellegű, megbízhatatlan
  - cím alapján továbbítja a csomagokat
  - illetéktelenek is elolvashatják
- IP homokóra
  - Ma már szinte minden IP felett megy, a nem Internethez kapcsolódó szolgáltatások is
    - pl. Távközlési szolgáltatók beszéd- és faxforgalma




Forrás: http://www.w3.org/DesignIssues/diagrams/layers/IP-hourglass-zittrain.png

# Az IPv4 története néhány gondolatban

- Története:
  - 1969: Advanced Research Projects Agency Network (ARPANET)
  - 1974: Vinton G. Cerf és Robert E. Kahn, ARPANET új protokollstruktúra, NCP-t váltja le
  - 1979: Az IP 4-es verziójának dokumentációja
  - 1981: Internet Protocol szabvány, IETF RFC791
  - 1983: Teljesen kiszorítja az NCP-t
- A mai napig ezt a protokollstruktúrát használjuk (!)
- Idővel plusz protokollok csapódtak hozzá ahogy foltozgatták a hiányosságokat

# Gondok az IPv4-gyel


Forrás: http://www.gomonews.com/wp-content/uploads/2010/07/ipv4-ipv6-feature.jpg

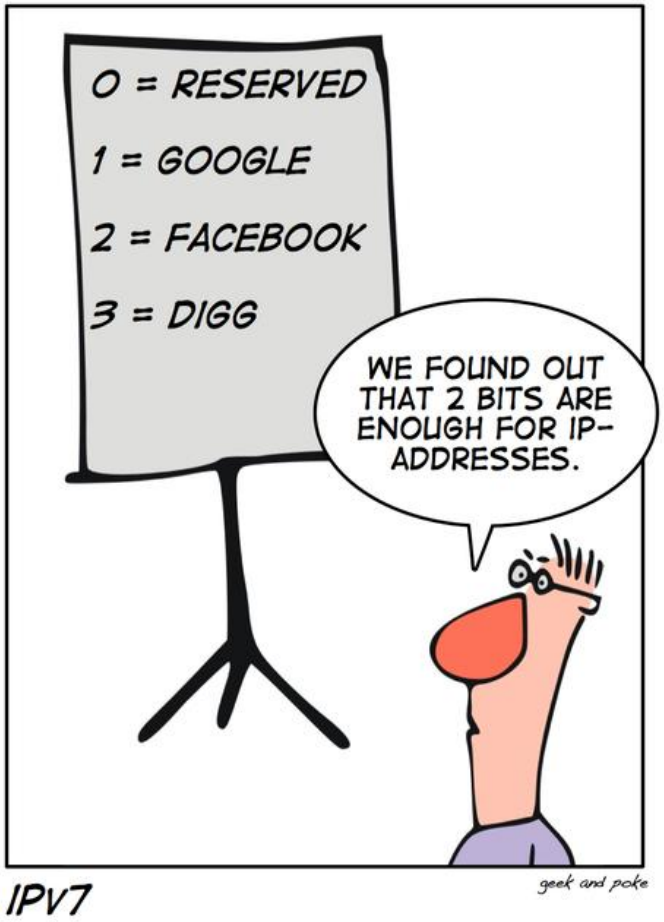
Vagy ahogy azt a RIPE 55 találkozón megénekelték:
http://www.youtube.com/watch?v=_y36fG2Oba0
(szöveg: https://apps.db.ripe.net/search/query.html?searchtext=POEM-RIPE55-SONG#resultsAnchor )

# Miért kell IPv6?

- IP – Internet Protocol: az információs társadalom egyik alapvető infrastruktúrájának fő protokollja
- Az IPv4 korlátozott
  - ~4,3 milliárd cím, 60% az USA-ban
  - egyre növekvő felhasználói populáció (pl. xDSL, mobil készülékek, játék konzolok, M2M, stb.)
  - **Kevés cím** (a NAT nem megoldás)
- Az IPv6 bevezetése nem egy lehetséges alternatíva
  - biztosan be fog következni előbb – utóbb (nagyjából most ☺)
- Tehát nincs más választás – nézzük az előnyeit:
  - Több IP cím
    - IPv4: $2^{32} = 4{,}29\ 10^{9}$ darab cím
    - IPv6: $2^{128} = 3{,}4\ 10^{38}$ darab cím
  - Auto-konfiguráció
  - Biztonság (end-to-end IPsec)
  - **Mobilitás (xMIPv6)**
  - Multicast
  - Egyszerűbb fejléc struktúra – hatékonyabb routing
  - Csökkenő fenntartási költségek – hosszútávon
- Az innováció, a hálózattechnikai fejlődés alapja!

# Híres kijelentések

- **“I think there is a world market for maybe five computers.”**
  - Thomas Watson, chairman of IBM, 1943
- **“640K ought to be enough for anybody.”**
  - Bill Gates, 1981
- **“32 bits should be enough address space for Internet.”**
  - Vint Cerf, 1977 (Honorary Chairman of IPv6 Forum 2000)




Forrás: http://geekandpoke.typepad.com/.shared/image.html?/photos/uncategorized/2007/05/17/ip1.jpg

# Címzés problémák

- Elfogynak a címek (ketyeg az óra)
- A nagyméretű site-ok több C osztályú blokkot igényelnek, ami miatt az  interdomain routing táblák gyorsabban nőnek, mint a router memóriája
- A felosztott címtér kezelése drága és összetett feladat (routerenként kell karban tartani)
- Az IPv4 nem jelzi a földrajzi távolságokat, pedig hasznos lenne az útvonalválasztásnál


Forrás: http://www.sum-it.com/?p=247


Forrás: http://media.bestofmicro.com/IPv4,A-R-255699-1.jpg

# Ideiglenes megoldások a címprobléma kezelésére

- CIDR – Classless Inter-Domain Routing
- NAT - Network Address Translator
- A használaton kívüli címek visszakérése
- Használaton kívüli A osztályú címek kiosztása
- A cím-birtoklás jelenlegi struktúrájának módosítása

# Classless Inter-Domain Routing

- A CIDR lényege, hogy szakít a címosztályok koncepciójával
- Helyette a hálózati prefix, hálózati maszk koncepcióját általánosítja.
  - Az Internet routerek nem az IP cím első három bitje alapján állapítják meg a határt a hálózati cím és az állomáscím között, hanem hálózati maszk alapján (amit cserébe tárolni kell)
  - A CIDR-t ismerő routing protokollok nem törődnek a címosztállyal, csak a maszkot figyelik
- Elemzők szerint, ha 1994/95-ben nem vezetik be a CIDR technológián alapuló címkiosztást, a routing táblák akkorára nőttek volna, hogy az Internet mára működésképtelen lenne
- A legtöbb router ma már ismeri ezt a technikát, és jelenleg az IANA (Internet Assigned Numbers Authority) is CIDR alapján osztja ki a címeket.

# NAT – Network Address Translator

- A NAT technika manapság az egyik legelterjedtebb módja az Internetre kapcsolódásnak
  - Alapötlete az RFC 1918
    - az Internetre nem kapcsolódó IP alapú hálózatok címkiosztására tesz ajánlást
    - Ezeknek a hálózatoknak nem kell globálisan egyedi címeket lefoglalni, elég, ha a lokálisan egyediek
- A NAT megoldást nyújt a címtérhiány ellen

# NAT – Network Address Translator

- Az IANA 3 különböző méretű címtartományt különített el erre a célra:
  - 10.0.0.0/8 (10.0.0.0—10.255.255.255)
  - 172.16.0.0/12 (172.16.0.0—172.31.255.255)
  - 192.168.0.0/16 (192.168.0.0—192.168.255.255)
  - Egy szervezet, mely nem kívánja hálózatát az Internetre kapcsolni, tetszőlegesen választhat ezen címekből
    - Így tehát nem kell az IANA-hoz fordulni IP-címekért
    - IANA vállalja, hogy ezen címek nem lesznek kiosztva

# A NAT működése

- A NAT-olni akaró szervezet kér tipikusan egy IP címet az Internet szolgáltatójától (ez lesz a NAT külső oldalán)
- A hálózaton levő állomásokat felcímkézi a fenti három címtartomány valamelyikéből vett címekkel (ez lesz a NAT belső oldalán)
- A NAT-oló modul
  - Dinamikusan helyettesíti a belső címeket a külsőkkel a kimenő csomagokban
  - A válaszcsomagokban visszaalakítja

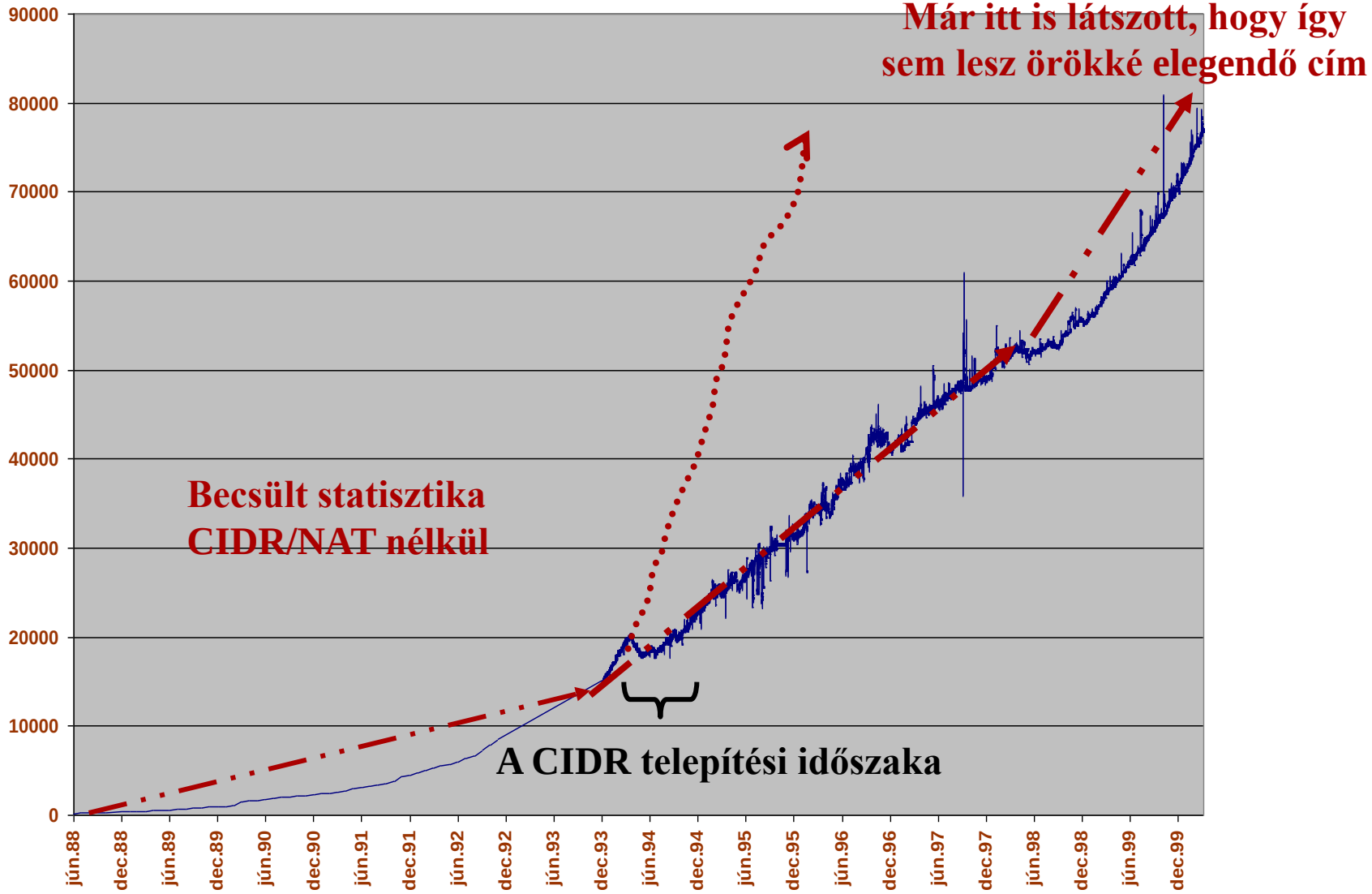
# NAT – előnyök és hátrányok

- Előnyei
  - csökkenti az Interneten szükséges címek számát
  - növeli a biztonságot (a belső hálózati struktúra láthatatlan a külvilág felé)
  - a hálózati címstruktúrát a szervezet akkor is megtarthatja, ha Internet szolgáltatót vált
- Hátrányai
  - kommunikációt csak belső végpont indíthat
    - NAT-olt szerverek üzemeltetése trükközést igényel
  - két NAT-os tartomány egyesítése nehéz lehet
  - megsérti a végpont-végpont kommunikációt!

# A CIDR és a NAT hatása

- Az osztályokra bontott címtér hátrányai hamar kiderültek
  - Nem volt meg benne a kellő granularitás lehetősége
  - Nem volt flexibilis
- Új megoldások:
  - Classless Inter Domain Routing (CIDR)
    - Finoman szabályozható címterek
    - Netmask bevezetése
  - Hálózati Címfordítás, Network Address Translation (NAT)
    - Magán hálózatoknak
    - Router mögé rekesztett címtartományok
    - Három címtartomány tetszőleges számban használható

# A CIDR és a NAT hatása



# A használaton kívüli címek visszakérése

- Az IANA javaslatokat tesz [RFC 1917]
  - azok a hálózatok, melyek biztonsági okokból sohasem kapcsolódnának az Internetre, szolgáltassák vissza a már lefoglalt IP címeiket
  - azok az ISP-k (Internet Service Provider) amelyek túl sok használaton kívüli hálózati előtagot birtokolnak, szolgáltassák vissza ezeket
- én pedig javaslom, hogy mindenki fizesse be nekem az összes pénzét
  - megkérdőjelezhető a sikeressége

# Használaton kívüli A és E osztályú címek kiosztása

- Az A címosztály egy részét egyéb célokra tartogatták
  - A 64.0.0.0/2 címtartományt nem osztották ki
  - Született egy ajánlás arra nézve, hogy ezt a címtartományt is ki lehessen osztani, hiszen a teljes IP címtartománynak jelentős részét teszi ki
- Az E osztályú címeknél
  - B és C osztályú címekként osztják ki
- Régi eszközökben nem triviális a megvalósítása

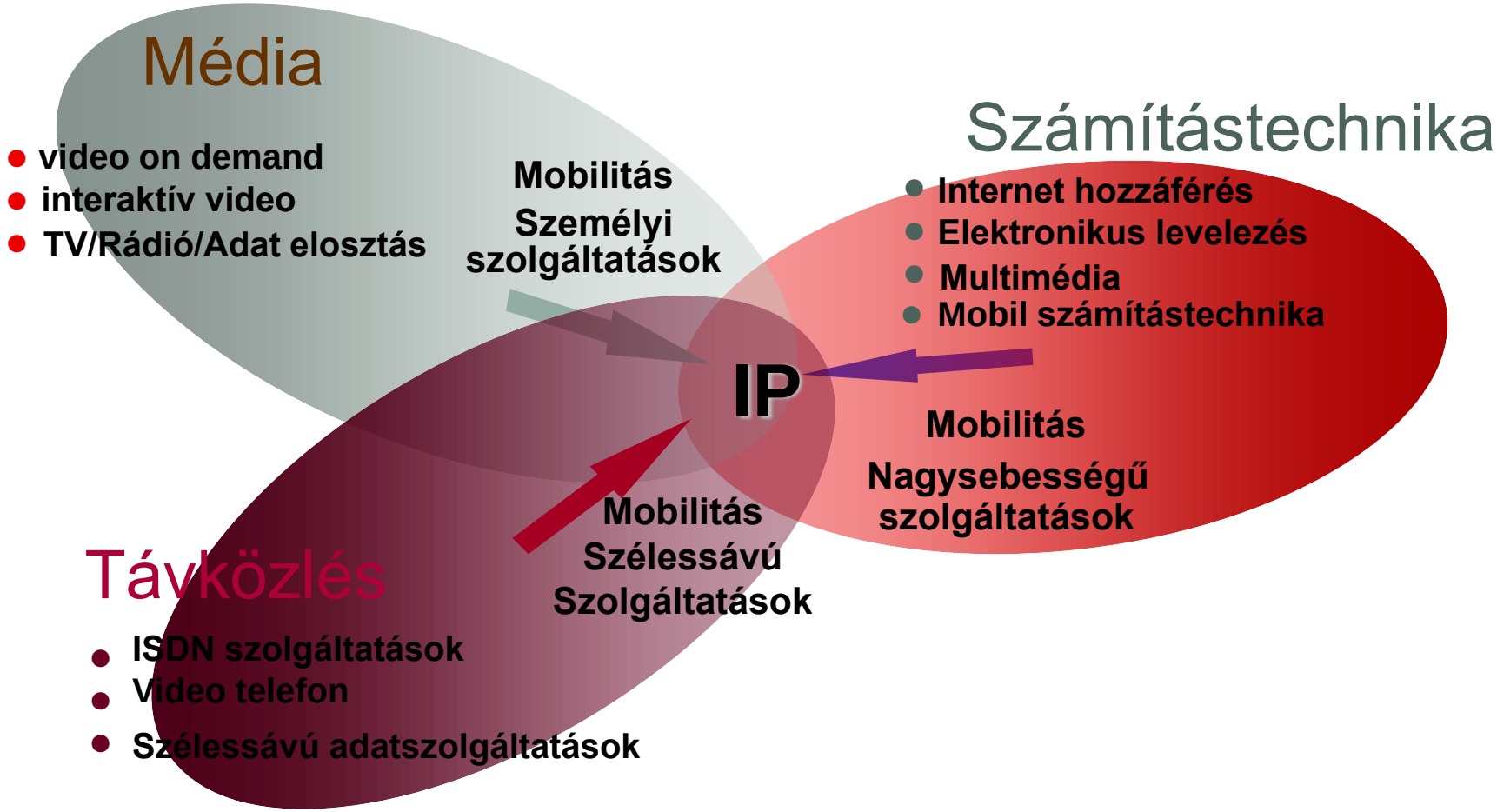
# A cím-birtoklás jelenlegi struktúrájának módosítása

- A címtér allokálás jelenleg
  - a szervezet kér egy címtartományt az IANA-tól
  - ha azt megkapja, addig birtokolhatja amíg az neki jól esik (vagy ameddig fizetni tud érte)
- IETF készített egy ajánlást, melynek lényege
  - a szervezet csak „kölcsön” kapja a címeket
  - egy idő után le kell mondania róla, és másikat kell igényelnie. Ezáltal bizonyos dinamizmussal ruháznánk fel a címek allokálását, a módszernek azonban több nagy hátránya is van.

# Cím-birtoklás: jelenlegi struktúra módosítása – hátrányok

- A CIDR technológia alapfeltétele: a címkiosztás tükrözze a hálózati topológiát
  - A folyamatos újra címzésekkel kaotikussá válik
  - egyre újabb és újabb elkerülő útvonalak beszúrása szükséges a routing táblákban
  - a dinamizmus árát a csomagok routolási hatékonyságának csökkenése jelentené
- A módszer az Internetes közösségek ellenérzését váltaná ki
  - IETF Procedures for Internet/Enterprise Renumbering (PIER) munkacsoport

# Aktuális trendek



# A címtartományok kimerülése

- Oka: Elégtelen méretezés több évtizeddel ezelőtt

- Súlyosbító körülmények:
  - Alacsony hatékonyságú címhasználat
  - Demográfiai tényezők
  - Állandó kapcsolatot biztosító hozzáférések
  - Mobil eszközök
  - Virtualizáció: több rendszer egy hardveren

- Enyhítő körülmények:
  - CIDR
  - NAT
  - Virtuális tárhelyek név alapján kihelyezve
  - RIR-ek szigorúbb kiosztási szabályai
  - Nagy, nem használt címterek visszavétele

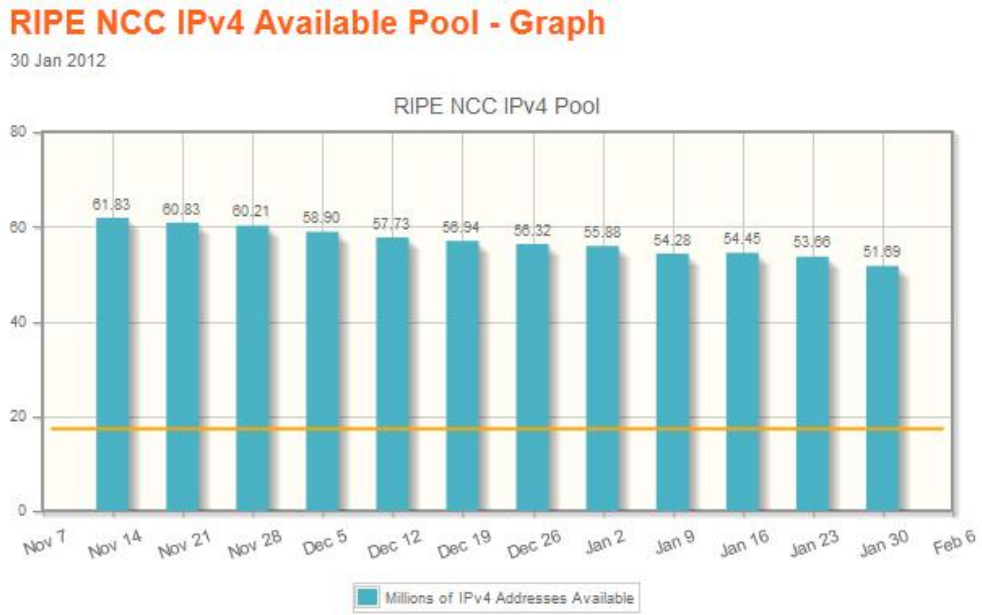
# A címtartományok kimerülése

- A takarékossági erőfeszítések ellenére:
  - 2011.02.01-én az IANA kioszt 2db /8-as hálózatot a meglévő 7-ből az APNIC-nak
  - „Vészhelyzeti” szabályozás lép életbe: az utolsó 5 /8-as tartományt elosztják az 5 RIR között
  - 2011.02.03-án ünnepélyes keretek között átadják az utolsó szabad tartományokat, ezzel az IPv4-es címtér KIMERÜL.


Forrás:
http://prensa.lacnic.net/news/en/6th-edition-february-2011

# A címtartományok kimerülése

- A RIR-eknél még találhatóak szabad címtartományok
- Ezek száma folyamatosan csökken
- Megjelenik a „RIR-shopping”: az egyes RIR-ek egymástól is vásárolnak címtereket
- Multinacionális cégek is „bespájzolnak”: Microsoft 13$/IP áron vásárolt tartományt 2011 márciusában




Forrás: http://www.ripe.net/internet-coordination/ipv4-exhaustion/ipv4-available-pool-graph

# Mi lesz így az Internettel?

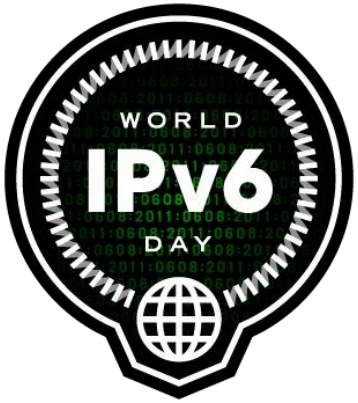
- „Don’t panic!” by Douglas Adams
- A probléma megoldásán már 1993-ban elkezdtek gondolkozni
- 1998-ra meg is született a szabványos megoldás:
  - Internet Protocol version 6
  - IETF RFC2460
- A kezdeti nagy remények után, részben a CIDR és NAT működése miatt az IPv6 háttérbe szorult
- A színfalak mögött azonban gőzerővel folyt a protokoll fejlesztése:
  - IPv6 protocol stack kifejlesztése, tesztelése
  - Jelentősebb projektek: KAME, Nautilus6, Tipster6 (magyar)
  - A Híradástechnikai Tanszék is kivette részét az IPv6 alapú technológiák fejlesztéséből, teszteléséből (Pl.: IST-PHOENIX, IST-ANEMONE, ICT-OPTIMIX, EUREKA-Celtic BOSS)

# Ráléptek a gázra: World IPv6 Day

- 2011.02.03-án, az IPv4-es címtér kimerülésekor elérkezett az IPv6 ideje
- Az új protokoll tesztelésére kijelöltek egy tesztnapot, 2011.06.08-át.
- Magyarországi idő szerint:
  2011.06.08 2:00 – 2011.06.09 2:00
- Mi is volt ez a nap?
  - „Egy globális szintű tesztrepülés az IPv6 szárnyán”, melyet az Internet Society (isoc.org) támogat
  - Ezen a napon a jelentősebb webes cégek és nagyobb ipari vállalatok beindították az IPv6-ot saját szolgáltatásaikon
  - Ezzel biztosítottak lehetőséget az IPv6-ra való zökkenőmentes átállásra

# Mire volt jó a World IPv6 Day?

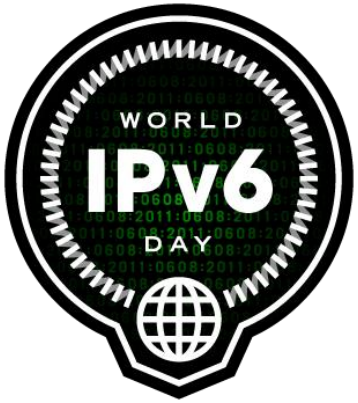
- Miért van szükség ilyen napokra?
  - A jövő hosszútávú megoldása az IPv6, így előbb vagy utóbb, de mindenkinek át kell rá térni
  - A nagyobb résztvevő vállalatok átlépésre sarkallják a versenytársakat is




- Hogyan motiválják ilyen akciók a technológia tesztelését és megváltoztatását?
  - Közös célt tűz ki az ISP-k, hardvergyártól, website üzemeltetők és operációs rendszer készítők elé
  - Együtt kell leküzdeniük az átállást
  - A World IPv6 Day napján: a globális skálázhatóság vizsgálata áll a központban

# Kik vettek részt ezen a napon?

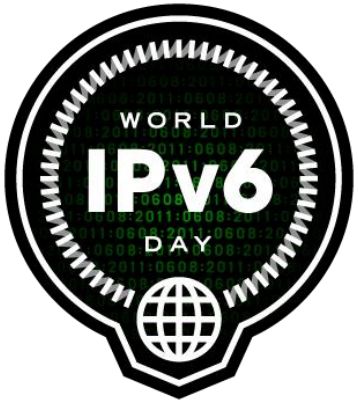
- Kik vettek részt az első globális IPv6 teszten?
  - Google
  - Youtube
  - Yahoo
  - Microsoft
  - Akamai
  - Cisco
  - W3C.org
  - Facebook
  - Stb.




- A teljes lista elérhető a http://www.worldipv6day.org/participants/index.html címen

# Mi hiányzik még az IPv6-os „boldogsághoz”?

- Mire van még szükség, hogy valóban mindenki használhassa az IPv6-ot?
  - Az ISP-knek IPv6-os elérhetőséget kell biztosítaniuk a felhasználóiknak
  - Webes szolgáltatóknak IPv6-on kell a szolgáltatásaikat nyújtaniuk
  - Az operációs rendszer készítőknek javítócsomagokat kell kiadniuk (kevés ilyen van szerencsére)
  - A Backbone hálózatok üzemeltetőinek is biztosítaniuk kell az IPv6-os kapcsolatot a peerjeiknek (Magyarországon IPv6 képes a Backbone nagyrésze)
  - A hardver és otthoni router, modem gyártóknak új firmware-t kell kiadniuk



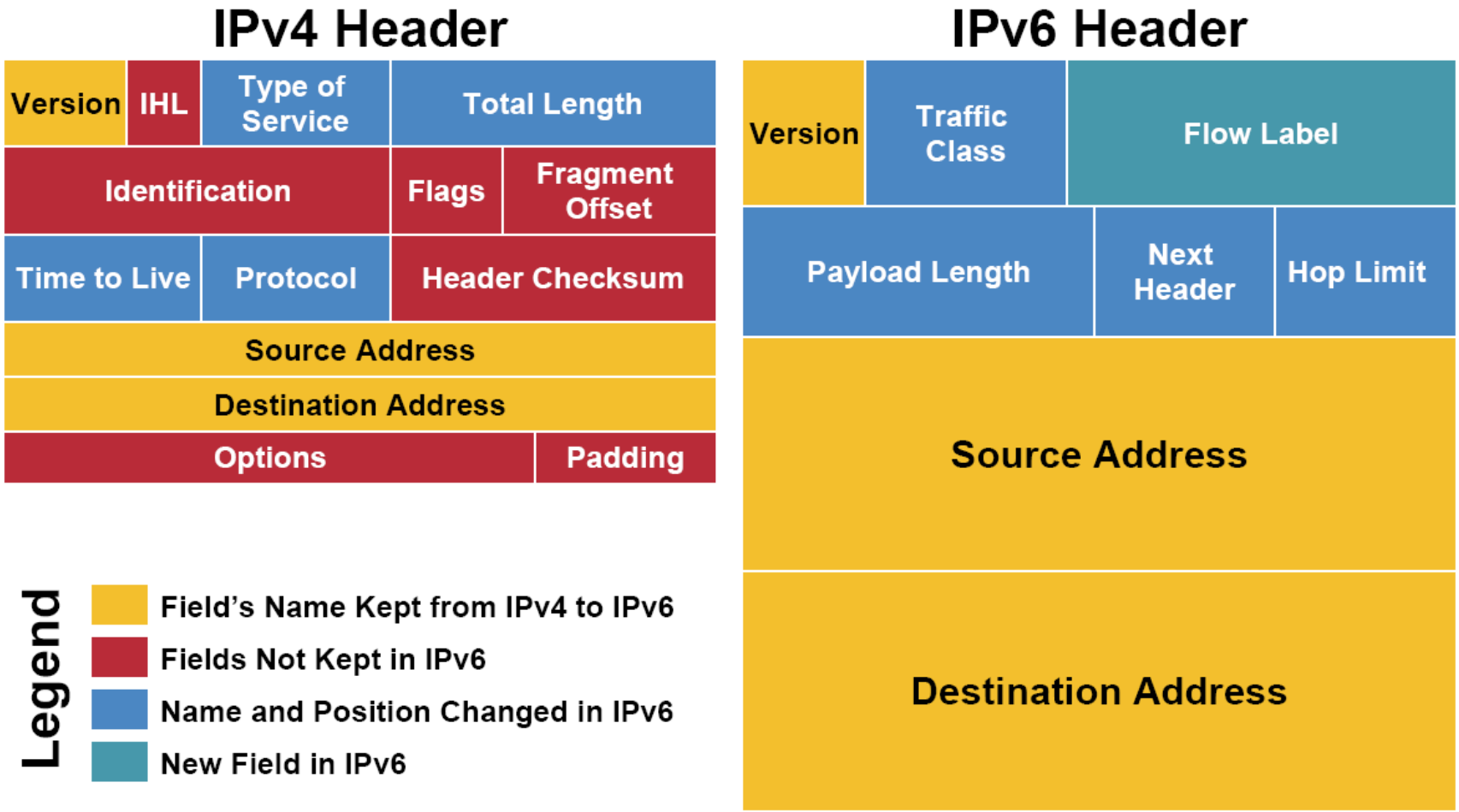
# Mire számíthatunk?

- A jövőben hosszabb tesztidőszakok jönnek
- A világ Internet felhasználói és szolgáltatói fokozatosan állhatnak át az IPv6-ra
- Az IPv4 és IPv6 együttélését körülbelül 20 évre becsülik
- Ezen időszak alatt a két protokoll közötti átjárást is meg kell oldani
- 2012-ben: World IPv6 Launch 2012 (Globális IPv6 Rajt 2012)
  - http://www.worldipv6launch.org/
  - http://test-ipv6.com/ipv6launch.html
  - 2012. június 6 !

# Az IPv6 újdonságai

- A legfontosabb: 128 bites címek, óriási címtér: Földünk minden $m^2$-re $6{,}5 \cdot 10^{23}$ cím (!)
- „Áramvonalasított” fejléc
- Opcionális kiegészítő fejlécek
- Beépített biztonsági rendszer
- Beépített mobilitás kezelés
- Autokonfiguráció
- Multicasting
- Anycasting
- Szomszéd felderítés
- Stb.

# IPv4 és IPv6 fejlécek összehasonlítása




Forrás: http://343networks.files.wordpress.com/2010/06/ipv4-ipv6-header.gif

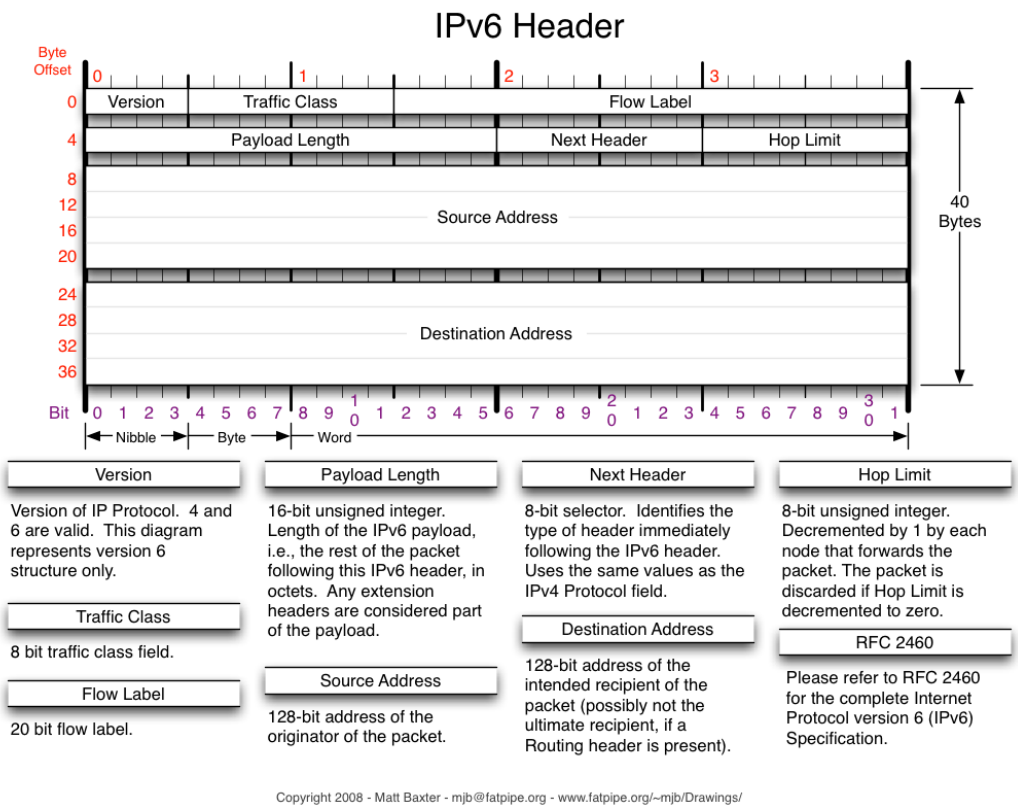
# Az IPv6-os fejléc – ami eltűnt

- Az alábbi IPv4-es mezők tűntek el
  - Fejléc hossz (IHL, fix 40 byte)
  - Azonosító, Flags, Fragment offset
  - Fejléc ellenőrzőösszeg
- A középső három a töredezés kezeléshez volt szükséges, ami az IPv6-ban nem létezik
- Ellenőrzőösszeg = lassúság

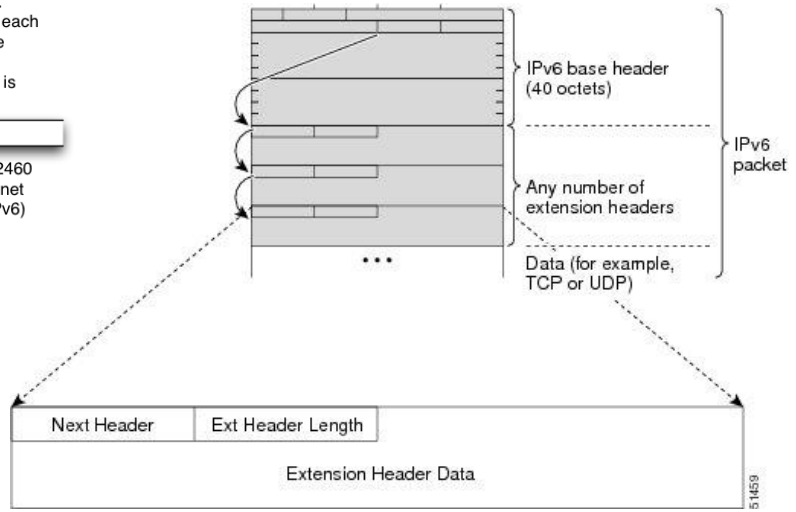
# Az IPv6-os fejléc – ami átalakult

- Type-of-Service => Traffic class (Forgalmi osztály)
  - prioritások kezelése
- Protocol Type => Next header
  - TCP, UDP, de kiegészítő fejlécek is, lásd később
- Time To Live (TTL) => Hop Limit
- Címzett és feladó címe (hosszabb)
- Új mező: Flow label (Folyam azonosító)
  - hatékonyabb csomagtovábbítás

# Az IPv6 fejléc




Forrás: http://www.siongboon.com/projects/2006-03-06_serial_communication/IP-Header-v6.png




Forrás: http://www.cisco.com/en/US/i/000001-100000/50001-55000/51001-51500/51459.jpg

# Az IPv6 kiegészítő fejlécei

- Ebben a sorrendben
  - Hop-by-Hop Options header (jumbogram)
  - Destination Options header (köztes célnál)
  - Routing header (routing type)
  - Fragment header
  - Authentication header
  - Encrypted Security Payload header
  - Destination Options header (végső célnál)
  - (Upper layer header)
- A “Next header” jelzi mi következik

# IPv6 címzés – néhány számadat

- IPv4 – 32 bit
  - $2^{32} = 4{,}29\ 10^9$ darab cím (elvileg)
    - már több, mint 6,5 milliárd ember a Földön
  - összesen 2 113 389 darab hálózat
- IPv6 – 128 bit
  - $2^{128} = 3{,}4\ 10^{38}$ darab cím (elvileg)
    - $6{,}65\ 10^{23}$ darab cím/$m^2$ a Föld felületén
  - $2^{45}$ darab /48-as hálózat (global unicast 001)
    - $3{,}5\ 10^{15}$ darab hálózat
    - mindegyikből további 65 535 /64-es alhálózat

# IPv6 cím típusok

- Címzett alapján
  - Unicast (egyes küldéses)
  - Multicast (többes küldéses)
  - Anycast
- Route-olhatóság alapján
  - globális (global)
  - nem globális (non-global)
    - link-local
    - egyedi lokális IPv6 cím (régen site-local)

# IPv6 cím

- 128 bit = 8 x 16 bit hexadecimális formában
  pl. 2001:0db8:0000:0000:0002:b3ff:fe1e:8329
- Egyszerűsítési lehetőségek
  - Bevezető nullák elhagyása
    2001:db8:0:0:2:b3ff:fe1e:8329
  - Dupla kettőspont: csupa nullák helyettesítésére
    2001:db8::2:b3ff:fe1e:8329
    Csak egyszer lehet!
- Prefixek jelölése: IPv6 cím/prefix alakban
  - 2001:db8:0:56::/64

# Nevezetes IPv6 címtartományok

- Kioszthető
  - 2000::/3 global unicast
  - FE80::/10 link-local unicast
  - FEC0::/10 korábbi site-local
    - már nem használatos
  - FC00::/7 lokális egyedi IPv6 címek
  - FF00::/8 multicast
- Speciális
  - :: unspecified address (mint 0.0.0.0 az IPv4-ben)
  - ::1 loopback

# Globális unicast címek

- Bináris 001-gyel kezdődnek (2000::/3)
- *n* bit a globális route-olhatósági prefix (pl. földrajzi pozíció alapján)
- 64-*n* bit alhálózati azonosító
- 64 bit interfész azonosító
- Pl.:
  - Hungarnet: 2001:738::/32
  - Műegyetem: 2001:738:2001::/48
  - pl. Híradástechnikai Tanszék: 2001:738:2001:4020::/64

# Lokális IPv6 címek

- Link-local: soha nem szabad route-olni
  - nem kell hozzá semmilyen beállítás
  - ad-hoc hálózatok, router nélküli hálózatok esetén ideális, vagy szomszéd felderítéshez
- Alakja: FE80::[64_bitnyi_Interface_ID]
  - Pl. ha az Ethernet kártya hardver címe 00:1A:6B:3A:9F:BC, akkor a link-local cím FE80::21A:6BFF:FE3A:9FBC lesz
- Módosított EUI-64 algoritmus:
  - Először a 48 bites MAC-címet 64 bites EUI-64-re konvertáljuk az FF:FE bitsorozat középre történő beillesztésével
  - Majd a hetedik legnagyobb helyiértékű bitet invertáljuk: 00->02 a fenti példában
- Egyedi lokális IPv6 címek:
  - azonosítás az FC00::/7 prefix-szel
  - [7_bit_prefix][1_bit_L_flag][40_bit_global_ID]:[16_bit_subnet_ID]:[64_bitnyi_Interface_ID]
    - L bit = 1 : helyi hozzárendelés egy pszeudo-random Global ID algoritmussal
    - L bit = 0 : központosított, nincs definiálva még a módszer

# Anycast címek

- A nagy terhelésű eszközökhöz találták ki
  - számítógépek egy csoportjából egyetlen (tipikusan a legközelebbi) állomást címzi
- Az unicast tartományból szabadon
- Subnet-router anycast
  - [n_bitnyi_subnet_prefix]:[128-n_bitnyi_0]
  - az első router fogja feldolgozni a linken
- Reserved subnet anycast cím
  - Az utolsó 7 biten, pl. 126 (7E): mobil IPv6 Home-Agent anycast

# Multicast címek

- FF[0RPT][4_bitnyi_scope][Csoport_ID]
  - 0RPT flagek (bitek)
    - R=0 Randevú pont nincs beágyazva
    - P=0 Multicast cím prefix infó nélkül
    - T=0 Jól ismert multicast cím (1: ideiglenes)
  - Scope példák
    - 1: Interface-local scope (~multicast loopback cím, nem hagyja el a csomópontot az ilyennel címzett csomag)
    - 2: Link-local scope (nem route-olható tovább)
    - 5: Site-local scope
    - E: Global scope

# Multicast cím példák

- Minden node
  - a küldővel azonos linken FF02::1
  - a küldővel azonos site-on FF05::1
- Minden router
  - a küldővel azonos linken FF02::2
  - a küldővel azonos site-on FF05::2
- Minden DHCP ügyfél FF02::1:2
- Minden DHCP szerver FF05::1:3
- Minden NTP szerver
  - a küldővel azonos site-on FF05::101
  - az Interneten FF0E::101

# Internet Control Message Protocol 6-os verzió (ICMPv6)

- Sokkal fejlettebb, mint az ICMPv4
  - Multicast management (IGMP helyett)
  - Neighbor Discovery (ARP, RARP helyett)
    - a szomszéd állomások, routerek, elérhető szomszédok és változó adatkapcsolati címek feltérképezésére
  - Echo request/echo reply (ping)
  - Packet too big (fragment fejlécek helyett)
- Két típusú üzenet
  - hiba
  - információs

# ICMPv6 hibaüzenetek

- Címzett elérhetetlen (destination unreachable)
  - ha az IP datagram nem továbbítható
    - Nincs route a célhoz, cím/port elérhetetlen, adminisztratíve tiltott
- Túl nagy csomag (Packet Too Big)
  - az MTU a köv. linken kisebb a csomagméretnél
- Lejárt az idő (Time Exceeded)
  - ha a hop számláló nullára csökkent
- Paraméter probléma (Parameter problem)
  - ha valamelyik paraméter nem értelmezhető

# ICMPv6 információs üzenetek

- Echo request / echo reply
- multicast felderítő üzenetek
  - router
  - listener
- router felderítés (router discovery)
- szomszéd felderítés (neighbor discovery)
- hálózat újraszámozás (router renumbering)
- mobilitás támogatáshoz kapcsolódó üzenetek
  - Részletesen lásd később

# ICMPv6: echo request és reply

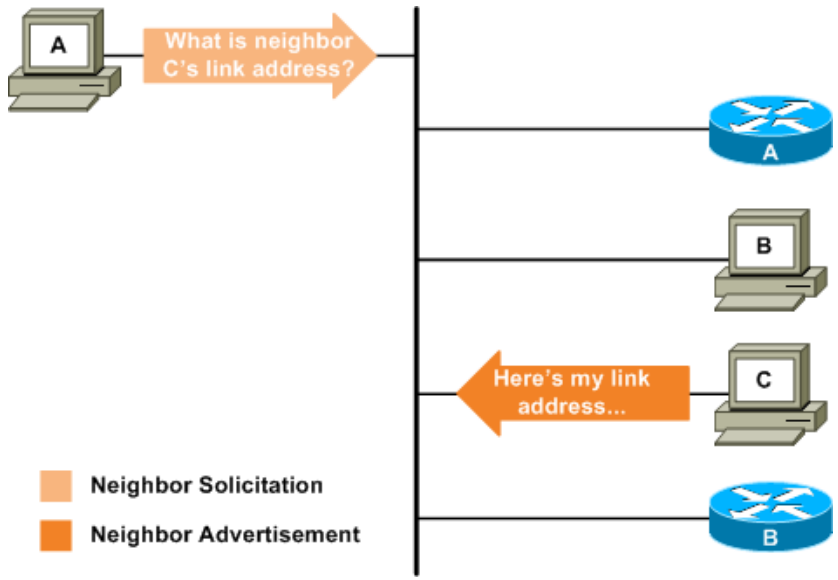
- Ugyanúgy, mint az ICMPv4-nél
- Az „echo request” üzenet adatát az „echo reply” üzenetbe kell másolni
- A ping6 alkalmazás is ezt használja

# ICMPv6: Neighbor Discovery

- Feladatai
  - Cím automatikus konfigurálása (állapotmentes autoconf.)
  - network prefix, router automatikus felderítése
  - duplikált IP cím érzékelés
  - MAC cím felderítés
  - Szomszédos routerek felderítése
  - A nem elérhető szomszédok azonosítása (NUD)
  - MAC cím váltások érzékelése
- Neighbor solicitation és router advertisement
  - MAC cím feloldás (IPv4-ben ARP volt)
  - A szomszédok elérhetőségének azonosítása
  - Duplikált IP címek azonosítása
- ICMP redirect
- Multicast Listener Discovery (MLD – RFC 3810)
- Multicast Router Discovery (MRD – RFC 4286)
- Inverse Neighbor Discovery (IND)
  - IPv4-ben ez volt a RARP
- Sebezhetőség, biztonság
  - SEcure ND (SEND)

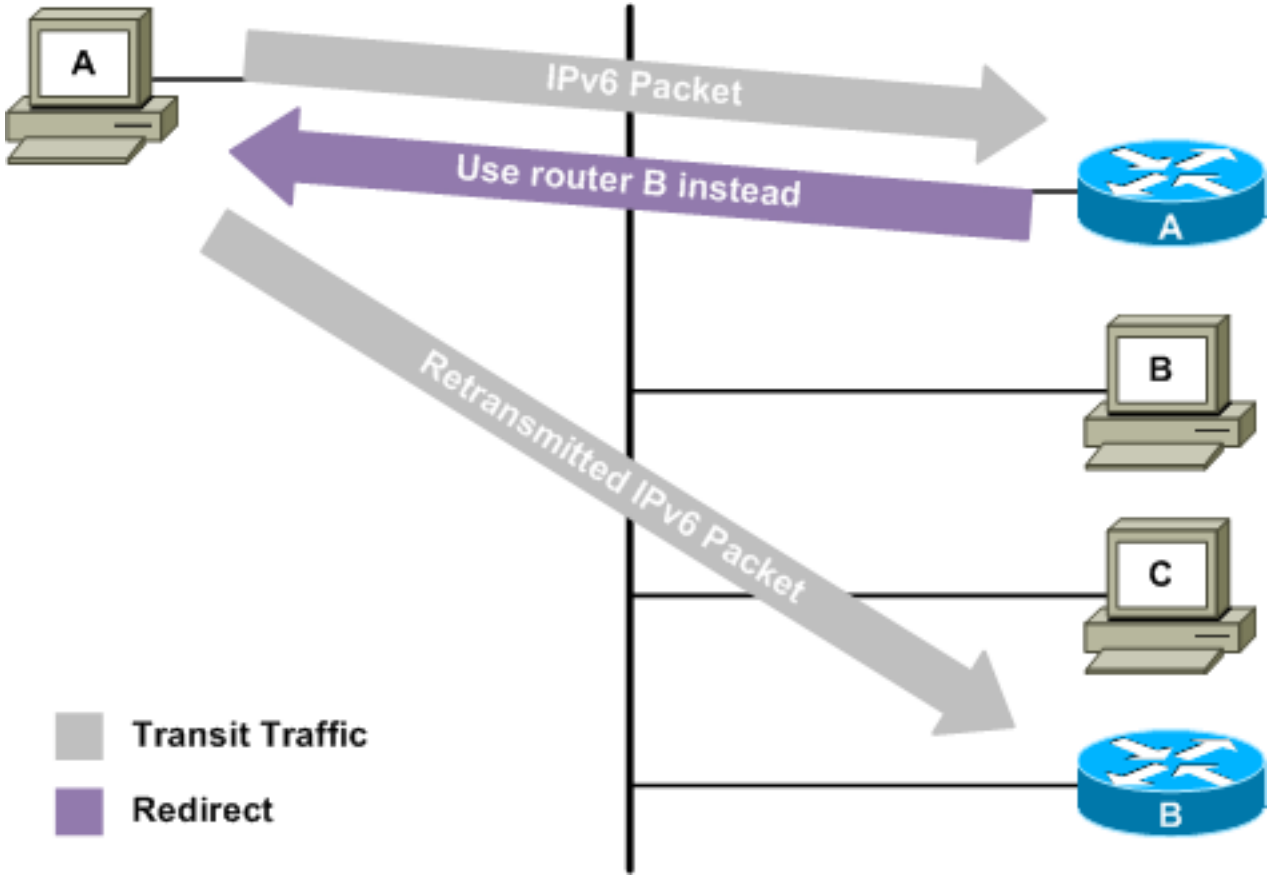
# ICMPv6 példa: Neighbor solicitation

- A neighbor solicitation üzenetben jön:
  - Típus: 135
  - Kód (code): nem használjuk
  - Checksum
  - Reserved
  - Célcím (target address): aminek a MAC címét fel akarjuk oldani
  - Options: pl. source link-layer address: a küldő MAC címe




Forrás: http://media.packetlife.net/media/blog/attachments/87/neighbor_solicitation.png

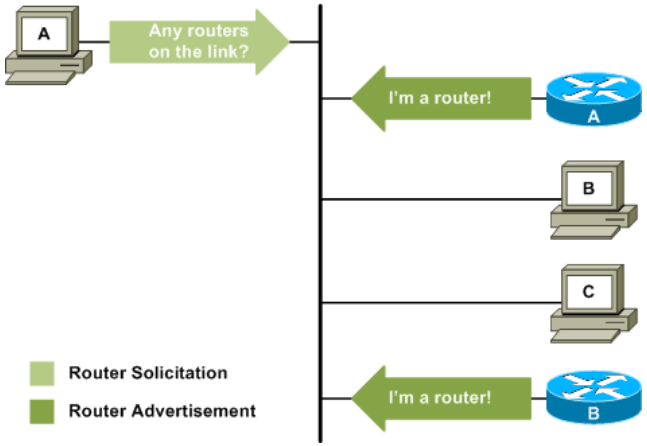
# ICMPv6 példa: Redirect




Forrás:
http://media.packetlife.net/media/blog/attachments/88/redirection.png

# ICMPv6: Router Discovery

- Két üzenet
  - Router advertisement (router információk)
  - Router solicitation (az előbbi kikényszerítése)
- Ami a router advertisement üzenetben jön:
  - Current Hop limit (hop limit ajánlás küldése a linken lévő node-ok számára)
  - Autoconfig flags
    - M: 0-SLAAC, 1-DHCPv6
    - O: 1-a címen és def. átjárón kívüli egyéb opciókra DHCPv6 használata
    - H: 1-Home link (Home Agent flag)
    - Prf (2 bit): Preferencia routerek között (RFC 4191)
  - Router lifetime
    - 0- nem default router
    - meddig elérhető a default router, s-ban
  - Reachable time
    - szomszédok vonatkozásában: elérhetőségi információ vétele után meddig tekintsük elérhetőnek az adott hostot
    - Neighbor Unreachability Detection használja
  - Retransmission timer
    - NS üzenetek újraadása közti idő ms-ben
    - A címfeloldás és a Neighbor Unreachability Detection használja
  - Options (forrás MAC cím, MTU, prefix infó)



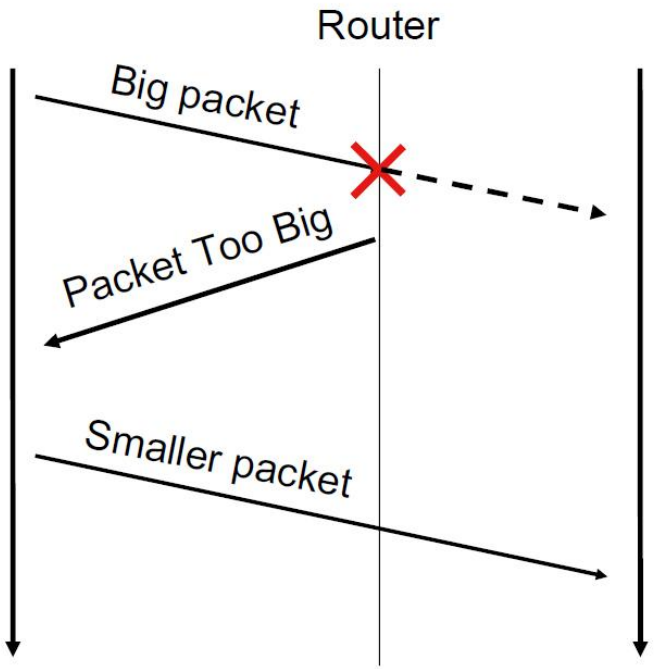

Forrás: http://media.packetlife.net/media/blog/attachments/86/router_solicitation.png

# ICMPv6: Autokonfiguráció

- Alapvető címkonfigurációs típusok:
  - Kézi
  - Stateless Address Autoconfiguration (SLAAC, RFC 4862)
    - Router Advertisement hirdeti a címet és az alapértelmezett átjárót
  - Stateless DHCPv6 (RFC 3736)
    - Router Advertisement hirdeti a címet és az alapértelmezett átjárót, de az O flag 1-ben van, így DHCPv6-tal csak DNS, NTP, stb. információt kap a csomópont
  - Stateful DHCPv6 (RFC 3315)
    - Router Advertisement-ben M flag=1, A flag=0 (autoconfig off). Ilyenkor címzés és minden egyéb információ DHCPv6-ból, DE alapértelmezett átjáró továbbra is Router Advertisement-ből
  - DHCPv6-PD (Prefix delegáció, RFC 3633)
    - Egész alhálózatok hozzárendelése routerekhez

# ICMPv6: Path MTU discovery

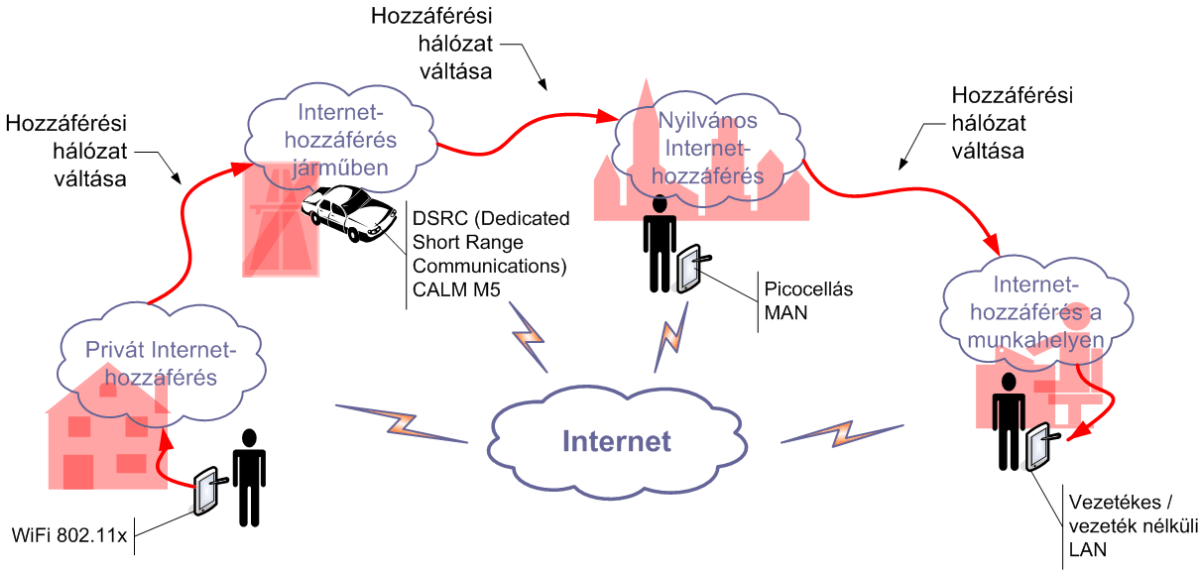
- Az IPv6-nál nincs fragmentálás
- Ha a csomag nagy (> MTU):
  - eldobja a router
  - küld egy ICMPv6 üzenetet a forrásnak (PTB)
    - A PTB tartalmazza a következő link MTU-ját
- Módszer:
  - küldjünk echo requestet a címre
  - kezdjünk nagy MTU-val, majd lépdeljünk lefelé
  - az új MTU-val próbálkozik
    - soha nem megy 1280 byte alá
  - GOTO eleje




Forrás: http://ripe60.ripe.net/presentations/Stasiewicz-Measurements_of_IPv6_Path_MTU_Discovery_Behaviour.pdf

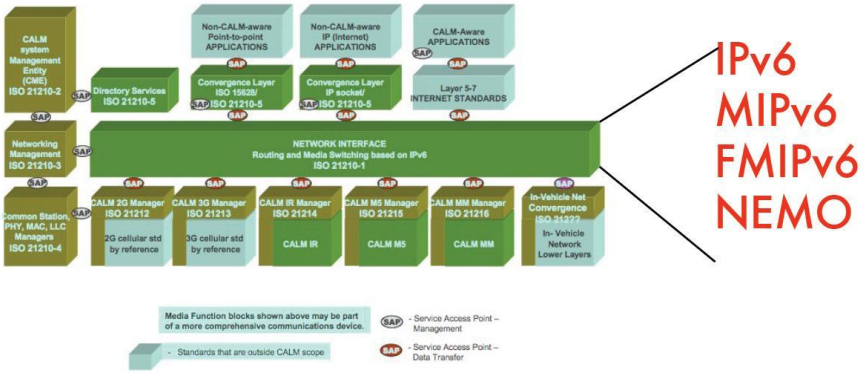
# Ubiquitous („mindenütt jelenlévő”) Internet

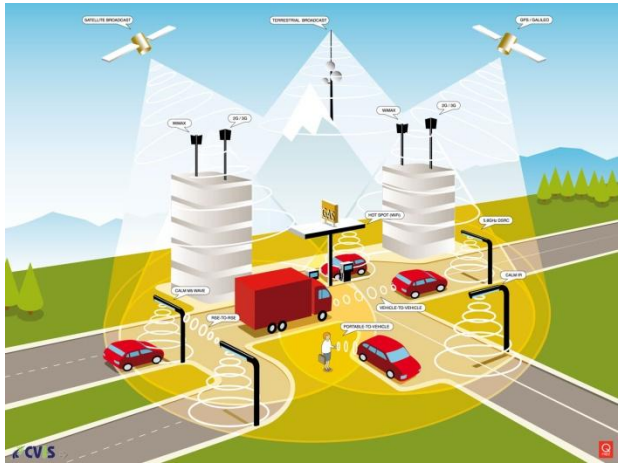
- Internet-hozzáférés mindig és mindenütt
  - háztartási eszközökben/berendezésekben
  - üzletekben, nyilvános helyiségekben (pl.: netcafé, utcai bútorok)
  - járművekben (pl.: gépkocsi, vonat)
  - embereken (pl.: PAN)
  - állatokon (pl.: nyomkövető megoldások)
- Kulcskérdések
  - átjárás különböző hozzáférési rendszerek között
  - az Internet protokolljainak mozgó környezetre való felkészítése: IP MOBILITÁS!



# Intelligent Transport Systems

- Az intelligens forgalom irányítás egyre növekvő kommunikációs igényeket mutat
  - Intelligent Transport Systems – ITS
  - v2v, v2i kommunikáció
  - A járművek számos hálózatot és eszközt hordozhatnak
  - Könnyíthetünk az eszközök fejlesztésén
- Nagyszámú és sokféle hozzáférési hálózat áll rendelkezésre
  - A CALM (Communications, Air-interface, Long and Medium range) szabványos architektúrája szintén IPv6 (és MIPv6, FMIPv6, NEMO stb.) hálózati rétegbeli protokollokra épít

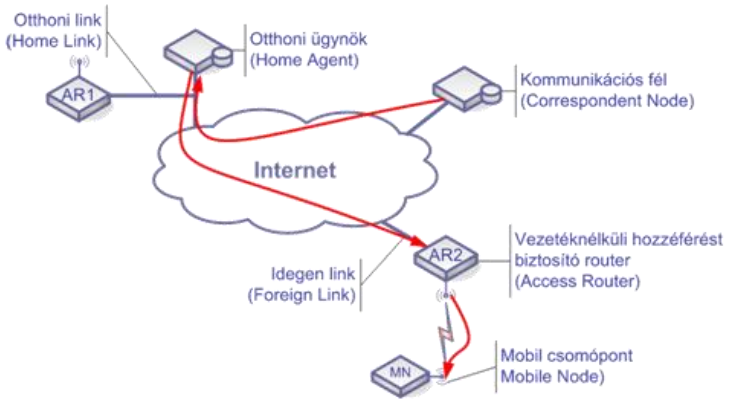


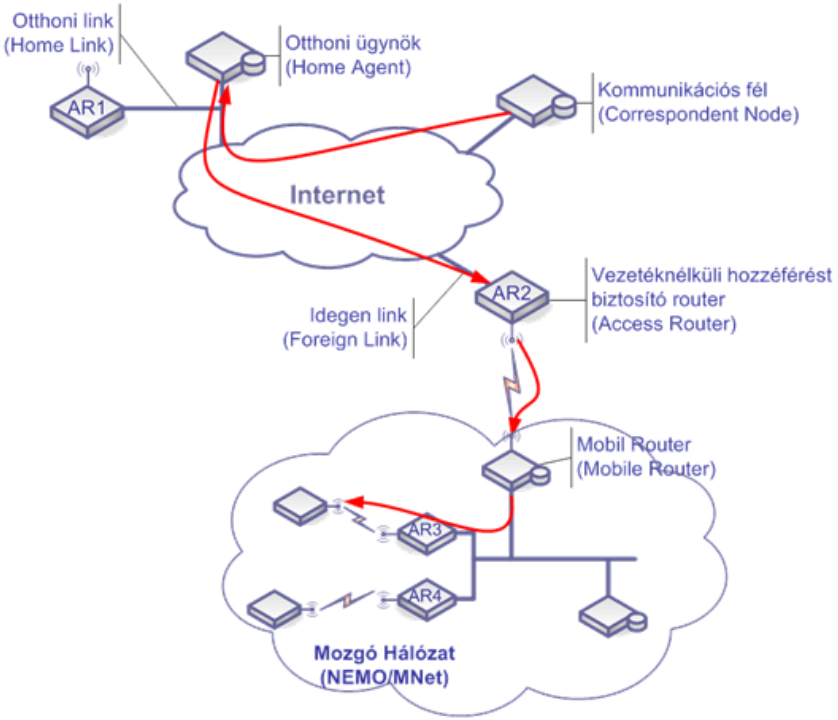
# Az IP alapú mobilitásról röviden

- IP csomópontok címzési követelményei
  - topológiailag helyes cím
  - minden interfészen olyan cím, ami az adott linken érvényes hálózati előtagnak (prefixnek) megfelelő
- IP szintű mobilitás
  - hálózati csatlakozási pont megváltozása = IP alhálózat megváltozása
  - IP alhálózat megváltozása = változások az útvonalirányításban
- Mindehhez a jelenlegi TCP/IP modellt adaptálni kell
  - eredetileg az Internetet fix csomópontok használatára tervezték
  - megsértették a rétegek függetlenségének elvét (az IP cím a hálózati és a szállítási rétegben is használatos)
  - az IP cím szemantikailag túlterhelt:
    - interfész azonosító szerep (Identifier)
    - topológiai helymeghatározó szerep (Locator)
  - az IP cím on-the-fly módosítása megszakítja a futó kapcsolatokat
  - az IP cím változatlanul hagyása alhálózat váltásnál a routing mechanizmusokban hibákat okoz
- Mobilitást támogató kiegészítésekre van szükség!

# Főbb mobilitási esetek



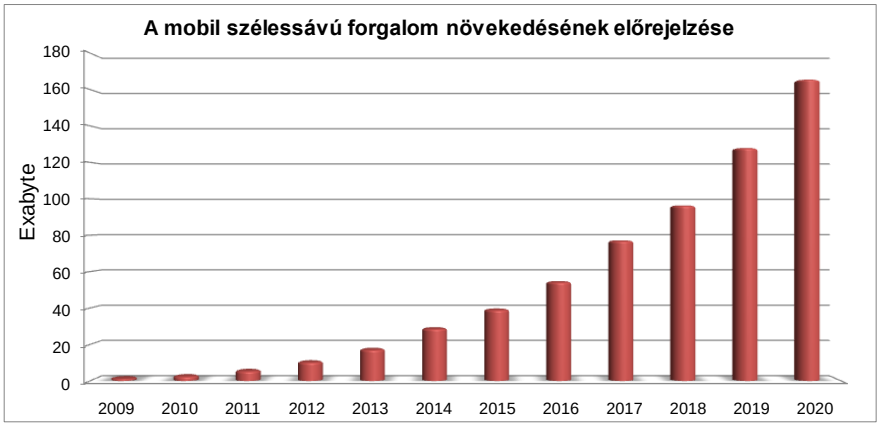

- Hoszt mobilitás:
  - egyetlen mobil terminál
  - alhálózat váltása esetén új, topológiailag helyes cím szerzése




- Hálózat mobilitás:
  - egész hálózat, egyetlen egységet alkotva mozog
  - Mobil útválasztó (Mobile Router) rejti el a hálózat belső jellemzőit a külvilág elől
  - A hálózat mozgásakor:
    - az MR változtat IP címet
    - a mozgó hálózat belsejében lévő csomópontok nem érzékelik a változást, nincs feladatuk ezzel kapcsolatban

# Miért használjunk IPv6-ot mobil hálózatokban?

- A mobil Internet-hozzáférés terjedése
  - sokszor a vezetékes hozzáférés helyett is!
- VoIP és adatszolgáltatások térnyerése
- Mobil végberendezések fejlődése
  - több interfész, nagyobb számítási kapacitás, játékkonzolok, stb.
- Új, speciális használati esetek megjelenése
  - M2M kommunikáció (Smart Grid, szenzorhálózatok)
  - ITS rendszerek

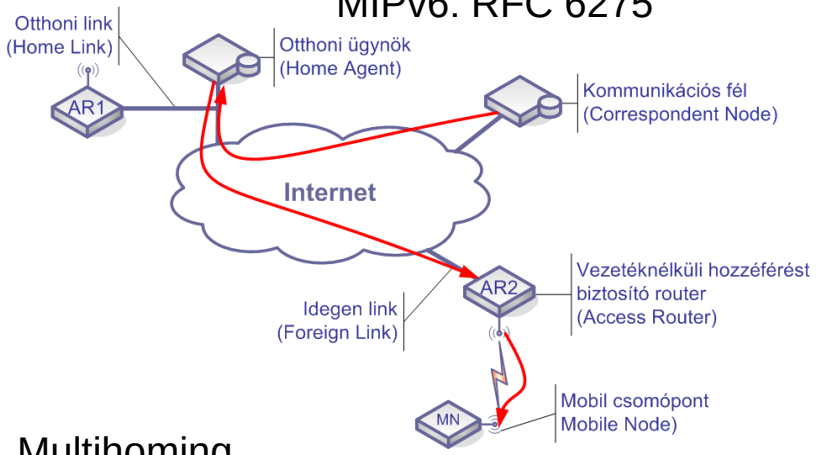



Cisco, NSN és Ericsson előrejelzések alapján

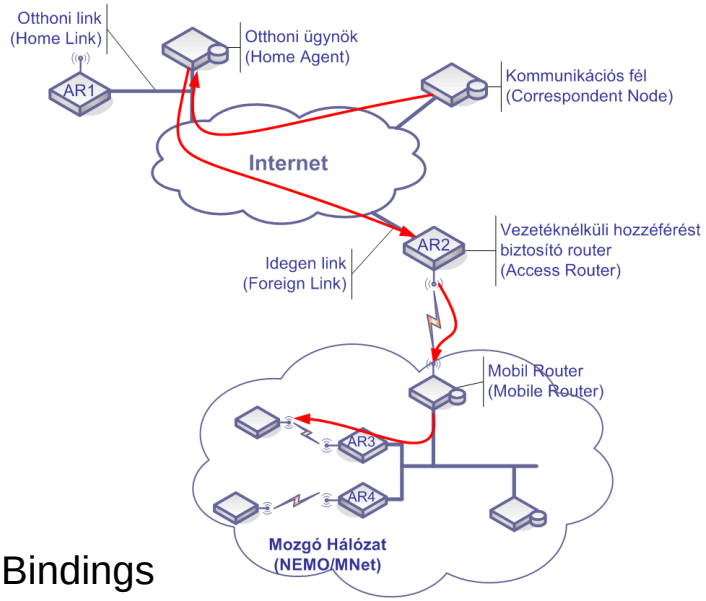
- IPv6 az előtérben, mert
  - több címre van szükség
  - végpont-végpont biztonságra van szükség
  - QoS-re van szükség
  - 3G és egyéb rendszerek közti mobilitás támogatására van szükség

# A Mobil IPv6 család alapvető tagjai

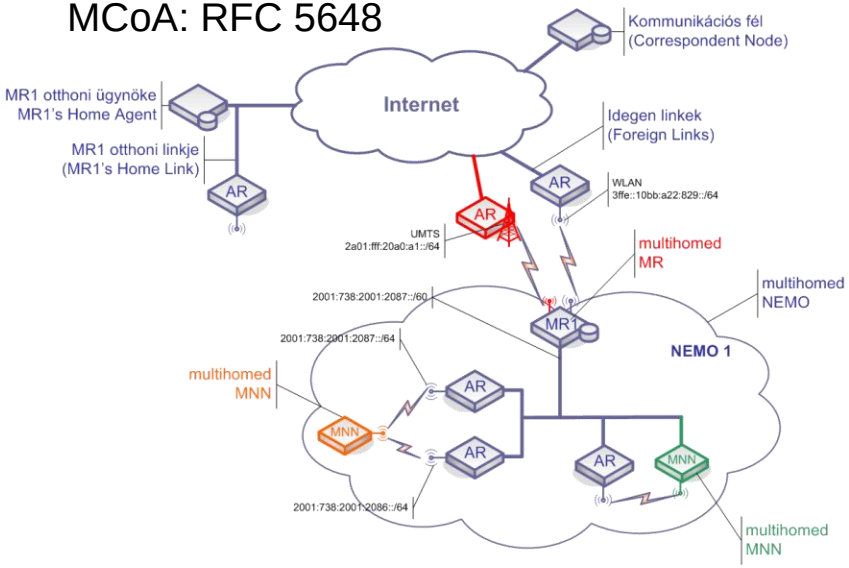
## Hoszt mobilitás
## MIPv6: RFC 6275



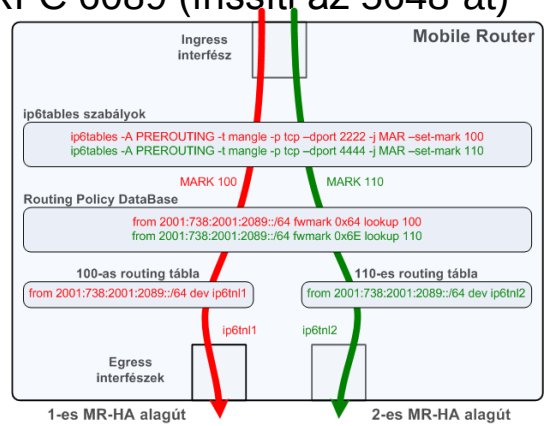

## Hálózat mobilitás
## NEMO BS: RFC 3963



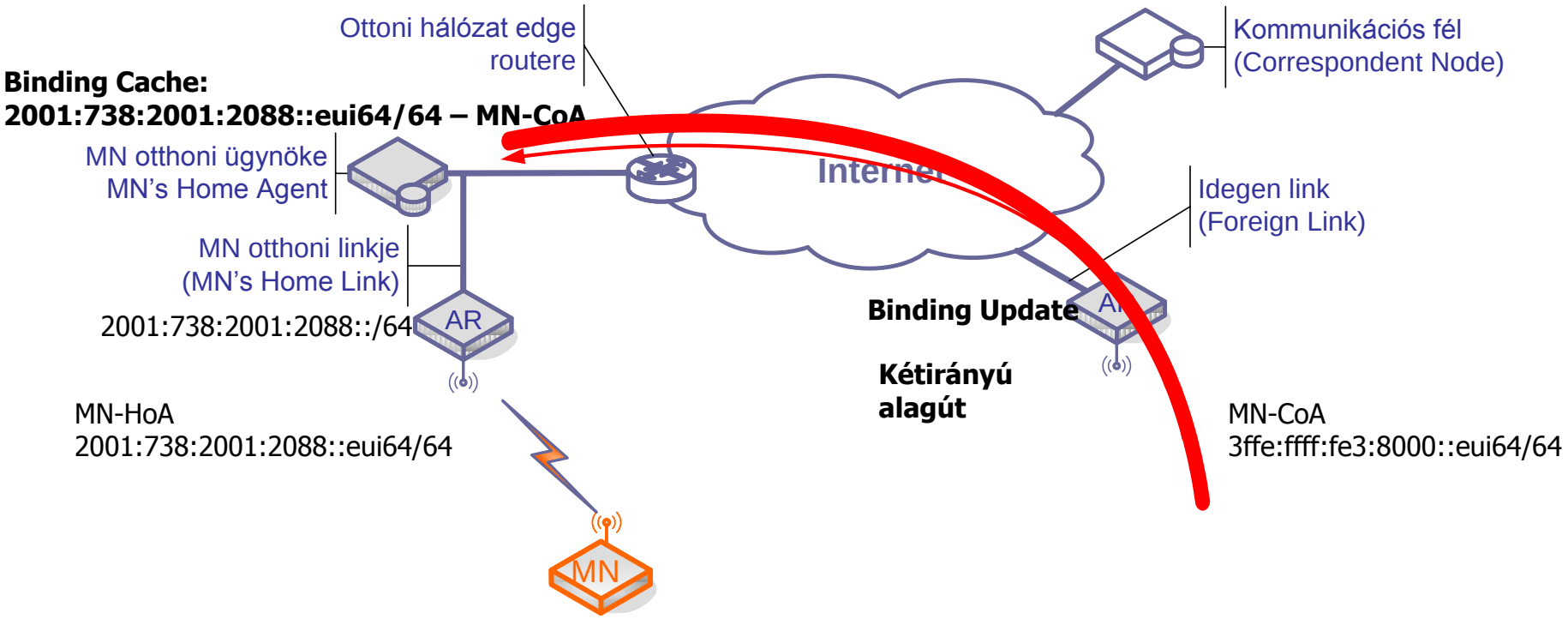

## Multihoming
## MCoA: RFC 5648




## Flow Bindings
## RFC 6089 (frissíti az 5648-at)



# Mobile IPv6



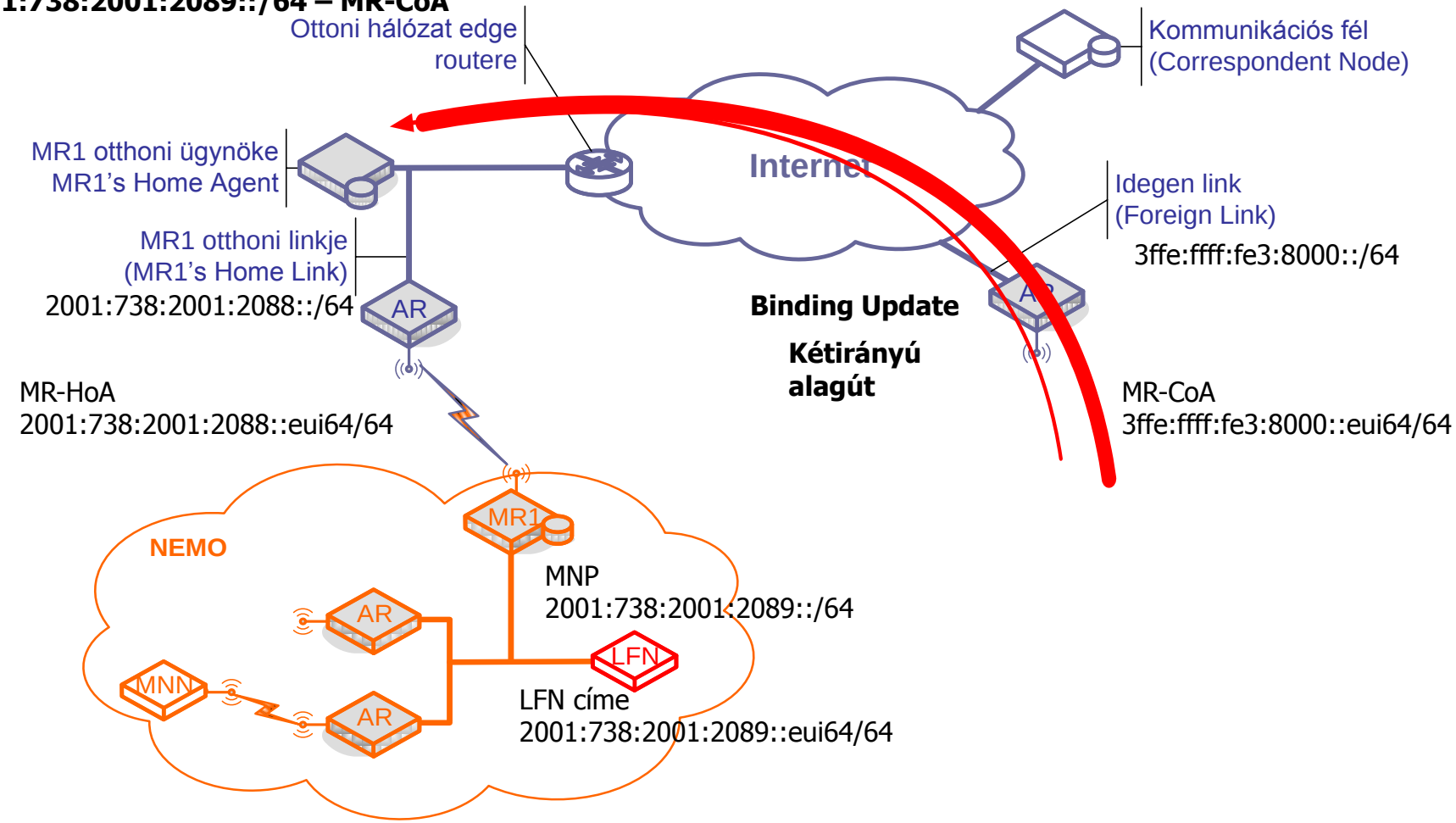

- Minden helyváltoztatást követően
  - A mobil terminál beregisztrálja a címét (helyét)
  - A kommunikációs fél az állandó címen (azonosítón) éri el a mobil terminált
  - Az otthoni ügynök (Home Agent) átirányítja a forgalmat

# A NEMO Basic Support protokoll működése

- Amíg a mozgó hálózat az otthoni hálózatában van, hagyományos útvonalválasztást alkalmazunk.
- Amint a hálózat megváltoztatja a helyét a topológiában
  - Beregisztrálja a helyét és hálózati prefixét az otthoni ügynökénél (Home Agent)
  - A Home Agent az összes ilyen prefixre érkező csomagot alagutazza (tunnelezi) a Mobil Router (MR) felé
- Minden új helyen
  - Új ideiglenes címet rendelünk a Mobil Router állandó címéhez (location <-> identity)
  - A mozgó hálózat többi csomópontjának a címe változatlan, számukra a mozgás transzparens!

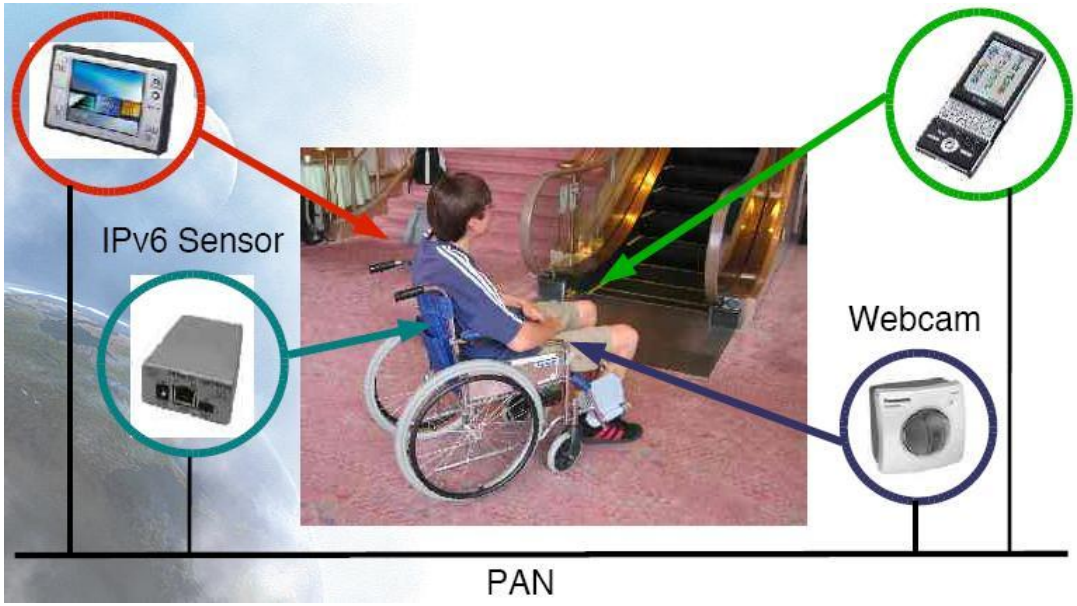
# A NEMO Basic Support protokoll működése

**Binding Cache:**
**2001:738:2001:2088::eui64/64 – MR-CoA**
**2001:738:2001:2089::/64 – MR-CoA**



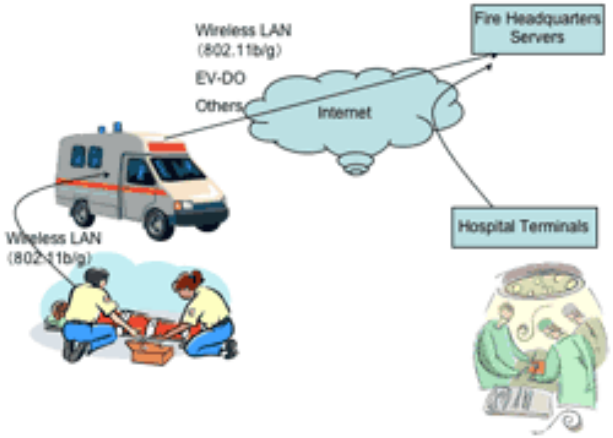
# A NEMO BS gyakorlati alkalmazásai, tesztrendszerek I.

- E-Wheelchair (Japán-Franciaország)
  - időskorúak, fogyatékkal élők egészségi állapotának monitorozása, felügyelete
  - távgyógyászat (kerekesszék érzékelői kapcsolatban a családdal/orvossal/kórházzal/ápolószemélyzettel)



# A NEMO BS gyakorlati alkalmazásai, tesztrendszerek II.

- Mobile ER Pilot Test (Japán)
  - viselhető eszközök a személyzeten (IP-telefon, laptop, GPS, szívverés-jelző)
  - mentőkocsi: 3G interfész
  - személyzet: WiFi
  - szolgáltatások:
    - interaktív és olcsó hang-kapcsolat
    - video/képek (multimédia) továbbítása a kórházba (pontosabb diagnózis, több ovos/vizsgálat, stb.)

# A NEMO BS gyakorlati alkalmazásai, tesztrendszerek III.

- ANEMONE (Advanced Next gEneration Mobile Open NEtwork - EU projekt)
- páneurópai teszthálózat IPv6 alapú mobilitási protokollok vizsgálatára

BME (Hungary)

CRES (Italy)

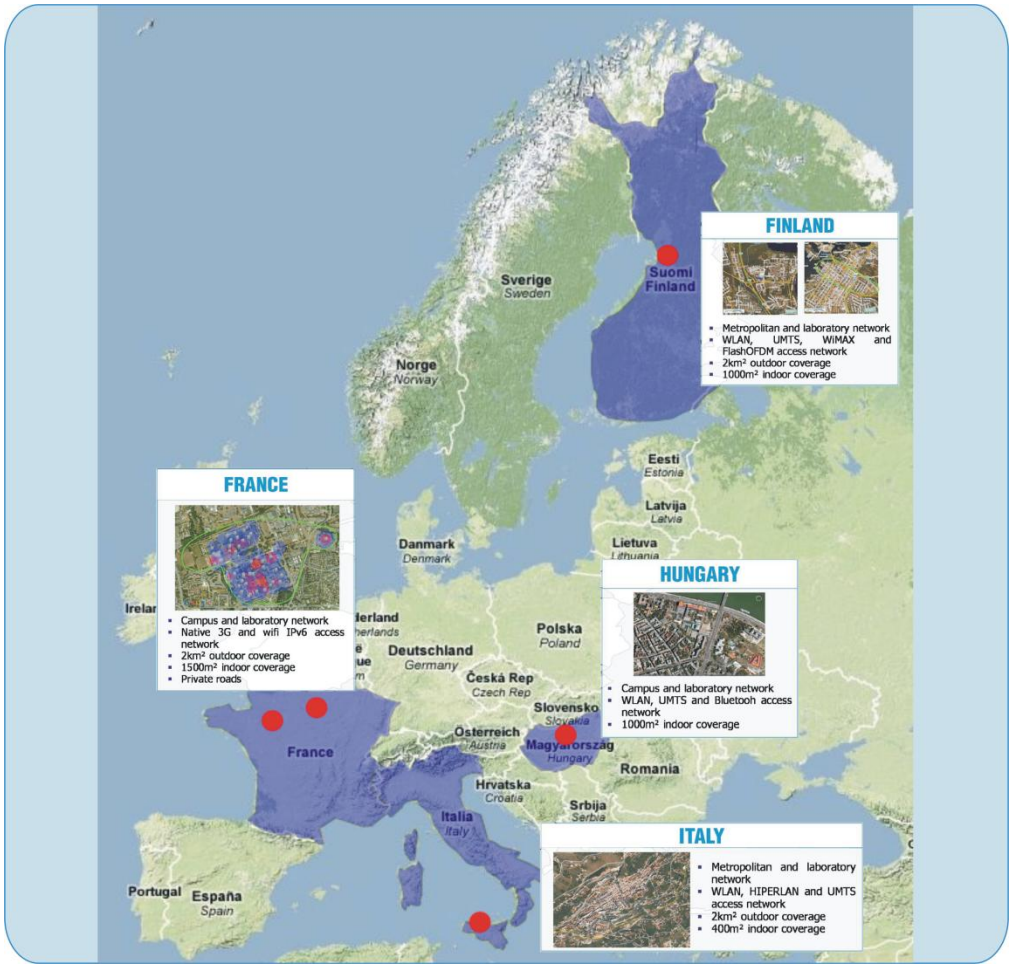
ENST-Bretagne (France)

INRIA (France)

SFR

Thales Comm. (France)

VTT (Finland)

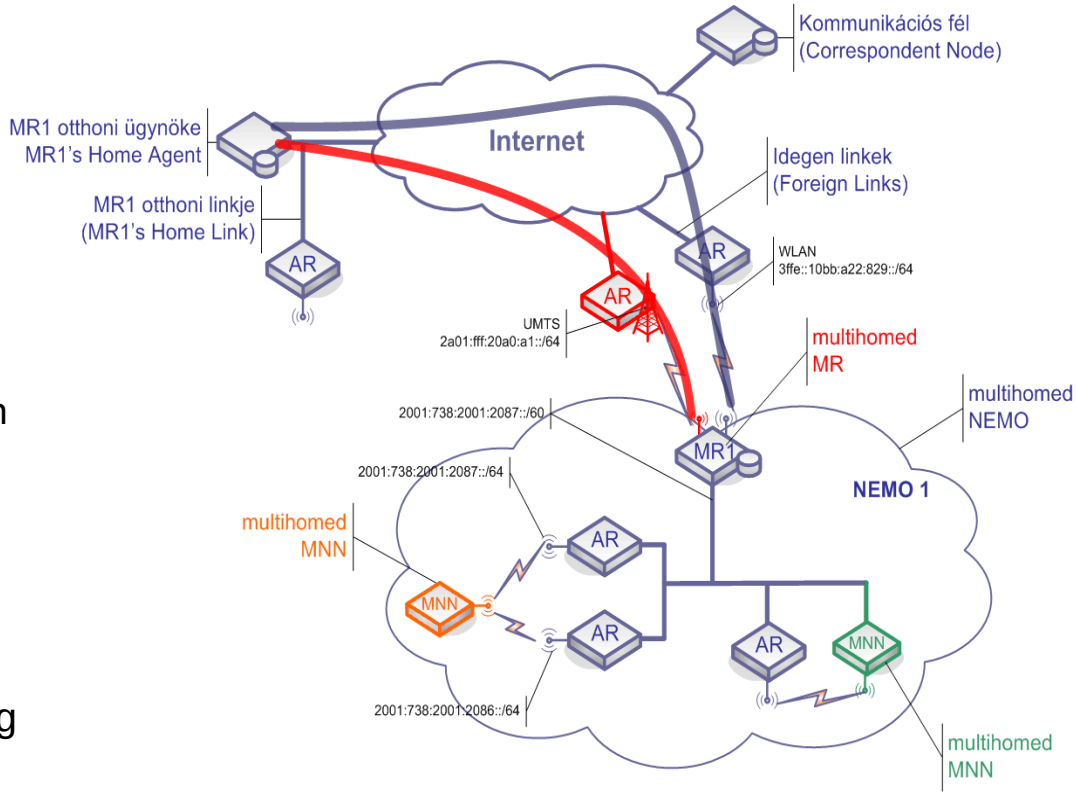


# Multihoming NEMO hálózatokban

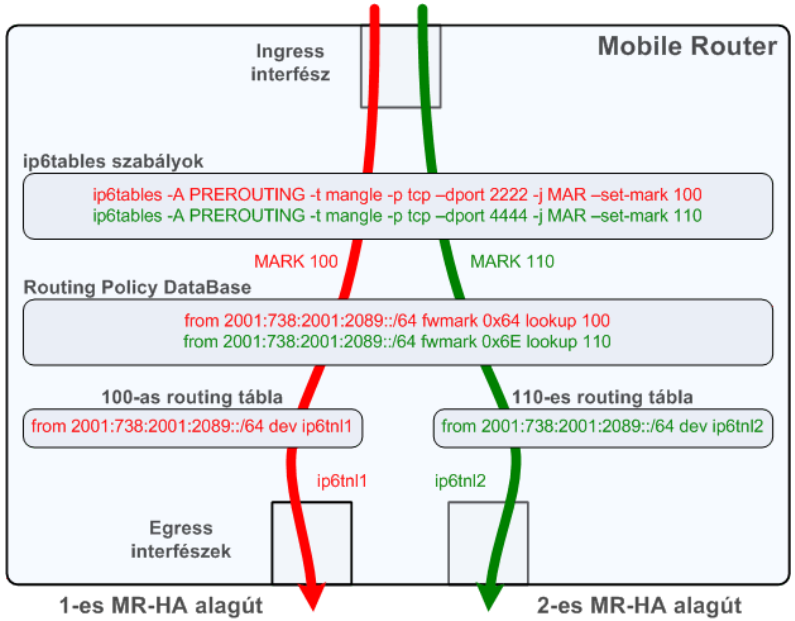
- Mozgó hálózatok „többotthonúságáról” akkor beszélünk, ha
  - az MR multihomed
  - több MR működik a NEMO-ban
- Alapvető célok és előnyök:
  - Állandó és „ubiquitous” hozzáférés
    - Hálózati lefedettség technológiákon átívelve történő növelése
  - Megbízhatóság, hibatűrés
    - Hálózati komponens multiplikálása
  - Kommunikációs folyamok átirányítása
    - A már kiépített folyam leállítása és ismételt felépítése nélkül!
  - Terhelés-megosztás
    - A hálózat terhelésének több útvonal segítségével történő elosztása
  - Terhelés-kiegyenlítés / folyamok szétosztása
    - Adott folyam több interfészen történő (együttes vagy szeparált) átvitele
  - Felhasználók választási lehetőségeinek bővítése
    - Felhasználói preferenciák alapján történő hozzáférés/hálózat kiválasztásának támogatása
  - Aggregált sávszélesség
    - Több interfész, több hozzáférés, több hálózat, nagyobb szávszélesség

# MCoA (Multiple Care-of Addresses Registration)

- A MR továbbra is egy otthoni címmel rendelkezik de a kötés kiegészül egy BID (Binding Unique Identifier) azonosítóval, amivel a kimenő interfész és ezáltal a kétirányú NEMO alagutak (az MN kötései) beazonosíthatók.
  - BID tartozhat interfészhez vagy ideiglenes címhez.
  - Erről az azonosítóról az MN a BU üzenetben értesíti a HA-t és a CN-eket, akik a BID-eket feljegyzik a Binding Cache-ükben
  - Az otthoni cím magát az MN-t azonosítja, míg a BID az ugyanazon MN által regisztrált egyes kötéseket különbözteti meg
  - Az ideiglenes IPv6-os címek megszerzése után az MN-ek legenerálják a CoA-khoz tartozó BID-eket, majd azokat eltárolják a Binding Update List-jükben
- A CoA-khoz tartozó BID-eket a Binding Unique Identifier al-opcióban helyezik el
- Sem a szabvány, sem az implementáció nem határozza meg, hogy mikor melyik interfészt kell használni a csomagtovábbításhoz!



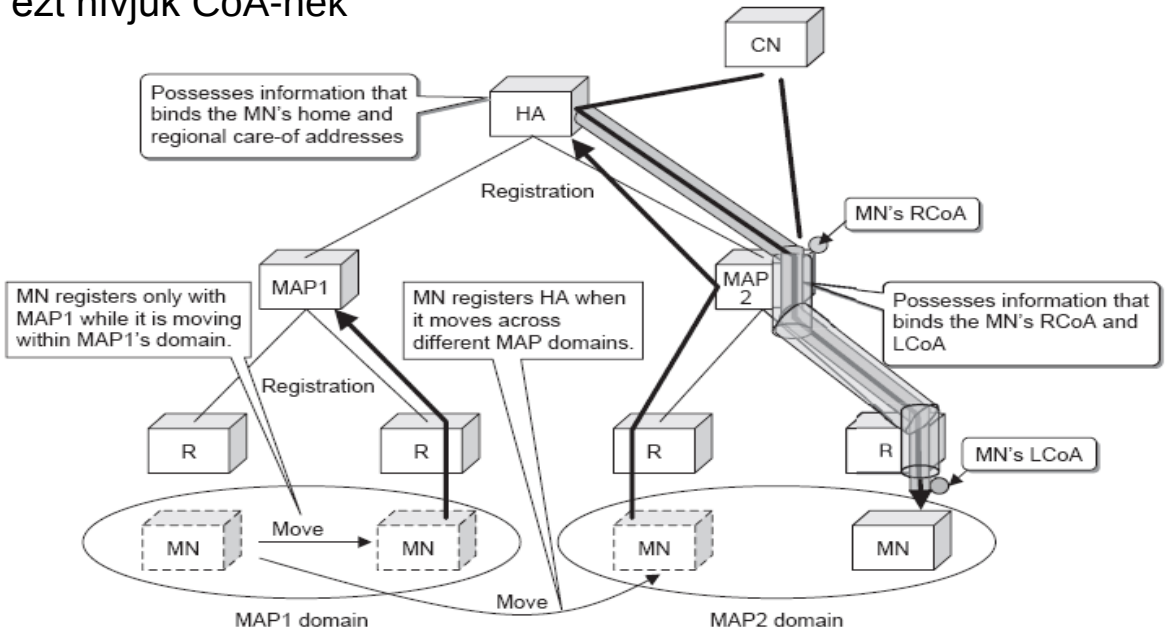
# Flow Bindings




- A Flow Binding mechanizmusai lehetővé teszik, hogy egy vagy több adatfolyamot kössünk a mobil adott ideiglenes címéhez és felkészítsük az otthoni ügynököt is a mobil felé irányuló csomagok adott címre történő irányítására.
- Linux rendszeren ez a policy alapú útvonalválasztás a netfilter keretrendszer csomagjelölő (MARK) képességinek segítségével valósítható meg
- A csomagok adott útvonalon való küldése érdekében a csomagokat az adott útvonalhoz tartozó interfész BID-jével jelöljük meg az útvonalirányítás előtt
- Az MCoA implementáció ezután már elvégzi a többit: az adott BID-del jelölt csomagokat az adott BID-hez tartozó útvonalirányítási szabályoknak megfelelően továbbítja.

# HMIPv6

- MAP (Mobility Anchor Point):
  - Mobile IPv6-ban nincs idegen ügynök (FA), azonban mégis szükség lenne egy olyan elemre, amely segíti a Mobile IP-vel lezajlódó cellaváltásokat, csökkentve az adott idegen domain-en kívülre irányuló jelzési forgalmat. Ezt a feladatot látja el az új hálózati elem, a MAP
  - Hierarchiába szervezhetők, ezáltal növelve a lokalitás kihasználását!
- RCoA (Regional CoA):
  - Ez az a cím amit akkor szerez a MN, ha egy MAP subnetjébe kerül
  - A címet autokonfigurációval állítja be helyi MAP hirdetések alapján
- LCoA (On-Link CoA):
  - Az éppen aktuális hely default routerének hirdetései alapján autokofigurációval beállított cím
  - MIPv6-ban ezt hívjuk CoA-nek

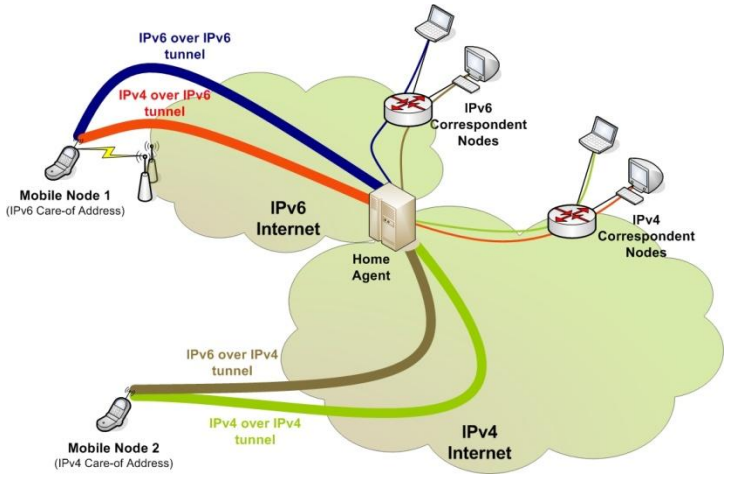


# FMIPv6

- Probléma a MIPv6-ban: lassú handoverek
  - IP-rétegű késleltetés (pl. Stateless Autoconf)
  - Binding Update késleltetés (hálózatba való bejelentkezés után)
- Az FMIPv6 ezeket próbálja lecsökkenti
- Az FMIPv6 szintén csak kiterjesztése a MIPv6 protokollnak
- Független az alatta lévő rétegektől
- Mi lenne ha előre tudnánk, hogy hová megyünk majd?
  - Lehetőség van rá, hogy előre megtudja a MN, hogy mely hálózatok vannak a közelében
  - Sőt arra is, hogy egy adott célhálózathoz előre generáljon magának egy CoA-t
- Használjuk ki az előbbi információkat!
  - Módosított BU üzenetekkel akkár már „távolról” is bejelentkezhet a MN az új hálózatba
  - Az új üzenetekkel funkciókat is összevonhatunk (Neigbour Advertisement és bejelentkezés az új hálózatba)

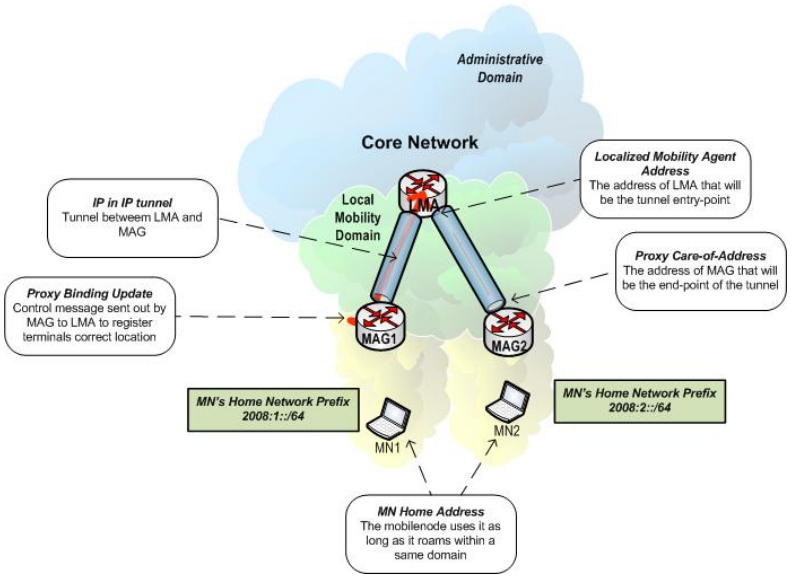
# Dual-Stack Mobile IPv6 (DSMIPv6)

- A DSMIPv6 a Mobile IPv6 (RFC6275) és a NEMO BS (RFC3963) protokollokon alapul
- 3GPP R8-ban jelent meg először: kliens alapú mobilitás-kezelés 3GPP és non-3GPP hozzáférések között
- Főbb jellemzők:
  - MIPv6 jelzések újrahasznosítása
  - Az MN IPv4-es HoA címet is szerezhet
  - A DSMIPv6 Home Agent és MN dual-stack
  - UDP beágyazás NAT-olt IPv4 hozzáféréshez
  - RO csak v6-os CN és v6-os MN között
- Előnyök:
  - Egyetlen, MIPv6 alapú protokol v4/v6 hálózatokra
  - Hozzáférés-független (routerek, stb. nem érintettek)
  - NAT és tűzfalak átjárása biztosított
  - RO lehetséges v6 vagy dual-stack hálózatokon
  - MCoA + Flow Bindings is használható: IFOM (3GPP R10)
- Hátrányok:
  - MN-HA alagutak okozta terhelés (fejléc tömörítés segíthet)
  - Kliens alapú, tehát a végberendezésnek aktívan támogatnia kell
  - NAT-olt IPv4 hálózatokon plusz jelzésterhelés (keep-alive + UDP)



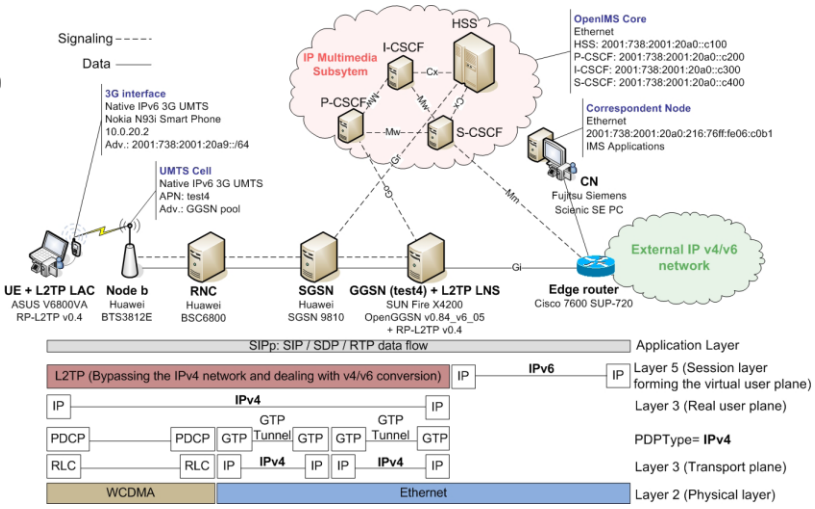
# Proxy Mobile IPv6 (PMIPv6)

- MIPv6/DSMIPv6 problémák:
  - sokszor túl nagy terhet jelent az MN-nek (akku, jelzés, rádiós interfész terhelés tekintetében)
  - az operátor nem szólhat bele a folyamatba
  - a gyártók vonakodtak a támogatástól, új utakat kerestek
- Alternatív módszer: PMIPv6
  - Cisco, WiMAX, 3GPP, Juniper, IETF, stb. támogatás
  - Nem kliens, hanem hálózat alapú mobilitás-kezlés!
  - Két új entitás:
    - LMA (a Home Agent a PMIP domain-ben + prefix alapú útválasztás)
    - MAG (emulálja az otthoni linket az MN-ek számára)
- Előnyök:
  - A kliens nem vesz részt a mobilitási jelzésekben
  - A kliensben nincs szükség szoftver upgrade-re
  - Nincs alagutazás miatti overhead a rádiós interfészen
  - Újrahasznosítja a MIPv6-ot
  - MN hagyományos IPv6 host-ként viselkedik
    (ND-vel vagy DHCPv6-tal címet szerez az új linken és kész)
- Hátrányok:
  - Csak a Per-MN prefix modell támogatott (a prefix követi az MN-t)



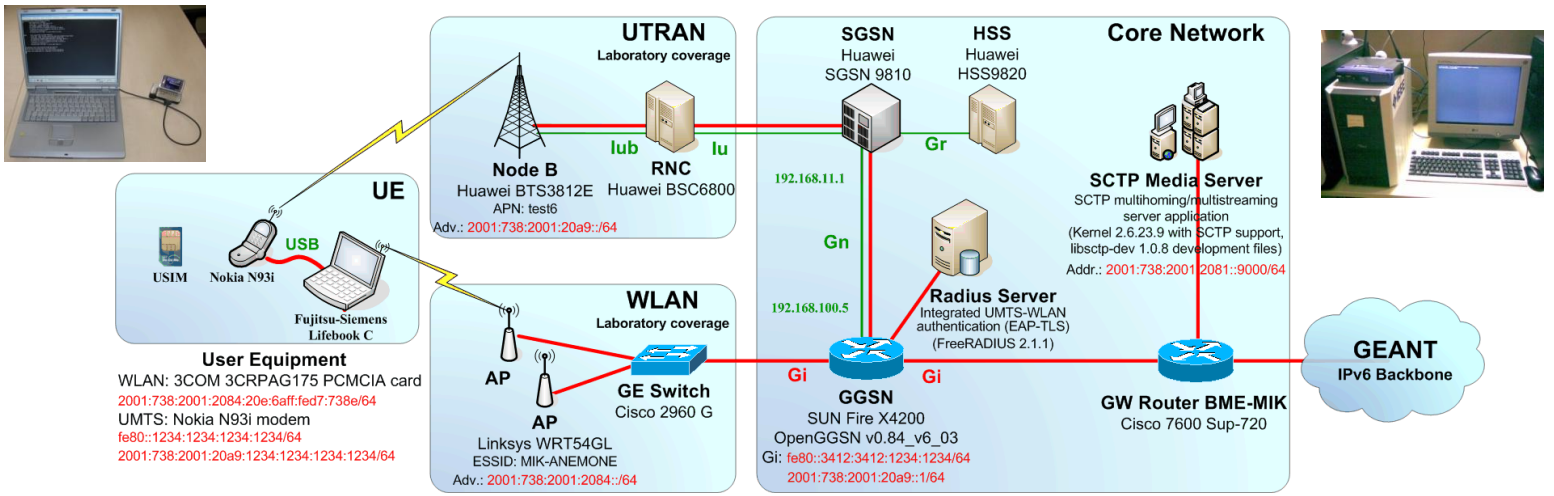
# IPv4-IPv6 áttérés/átjárás 3G hálózatokban

- Az IPv4 - IPv6 átállás problémái egyre égetőbbek (pl. az „all-IP 3G and beyond” multimédia rendszerekben is)
- IPv6 bevezetés három lépcsőfoka:
  - 1. IPv6 szigetek, IPv4-en húzott alagutakkal összekötve
  - 2. IPv6 széles körben elterjedt, de még nem egyeduralkodó (dual-stack eszközök dominálnak)
  - 3. IPv6 a domináns protokoll (már a dual-stack-re sincs szükség)
- IPv6 kapcsolat biztosítása 3G hálózatokban:
  - Natív IPv6 (dual-stack)
  - Alagutazás(pl. 6to4,Teredo,L2TP…)
  - Fordítás (pl. NAT-PT, TRT…)
- Kulcselemek (v4-v6 együttélés!):
  - Jelzés: SIP
  - DNS: A és AAAA bejegyzések
- Létrehoztunk egy 3G UMTS / IMS tesztrendszert, ahol
  - különböző PS szolgáltatásokat
  - **különböző átjárási módszereket vizsgálunk** IMS (IP Multimedia Subsystem) teljesítménymutatók segítségével



# IPv6 WLAN/3G multihoming SCTP segítségével

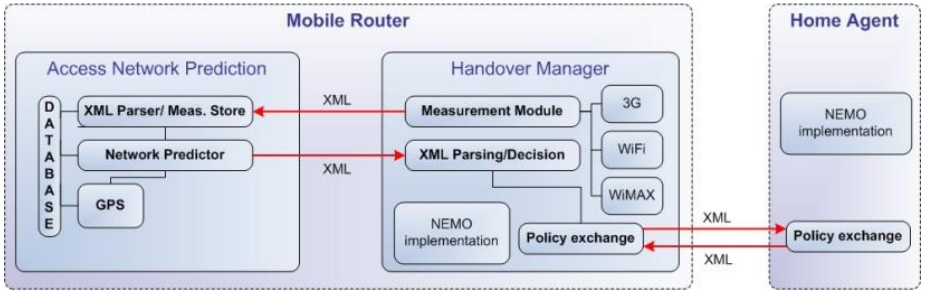
- Heterogén hozzáférés terjedése (WLAN, 2G, 3G, LTE, LTE-A, WiMAX, ZigBee, stb.)
- Több interfésszel felszerelt mobilok terjedése -> lehetőség a multihoming/multi-access megoldásokra!
- Napjainkban az IP-t tartják a legjobb megoldásnak a heterogén vezeték nélküli hozzáférési rendszerek integrálására
- IPv6 a jövő (már-már jelen), ez nem kétséges
- De az IPv6 egyedül nem képes valamennyi problémára tökéletes választ adni.
- Jó példa a multhoming: több, különböző rétegben működő megoldás él együtt jelenleg
  - Multiple Care-of Addresses (MCoA): 3. réteg
  - Host Identity Protocol (HIP): 3. és 4. rétegek között
  - **Stream Control Transmission Protocol (SCTP): 4. réteg**
  - Session Initiation Protocol (SIP): 7. réteg
- Létrehoztunk egy teszthálózatot, melyben az SCTP transzport protokoll IPv6 3G UMTS–WLAN környezetben mutatott teljesítményét jártuk körbe
- SCTP paraméter-optimalizálás: megfelelő beállításokkal az IPv6 multihoming (WLAN/UMTS) hálózatváltások okozta kiesés elhanyagolhatóvá válik!



# Hálózatváltások optimalizálása

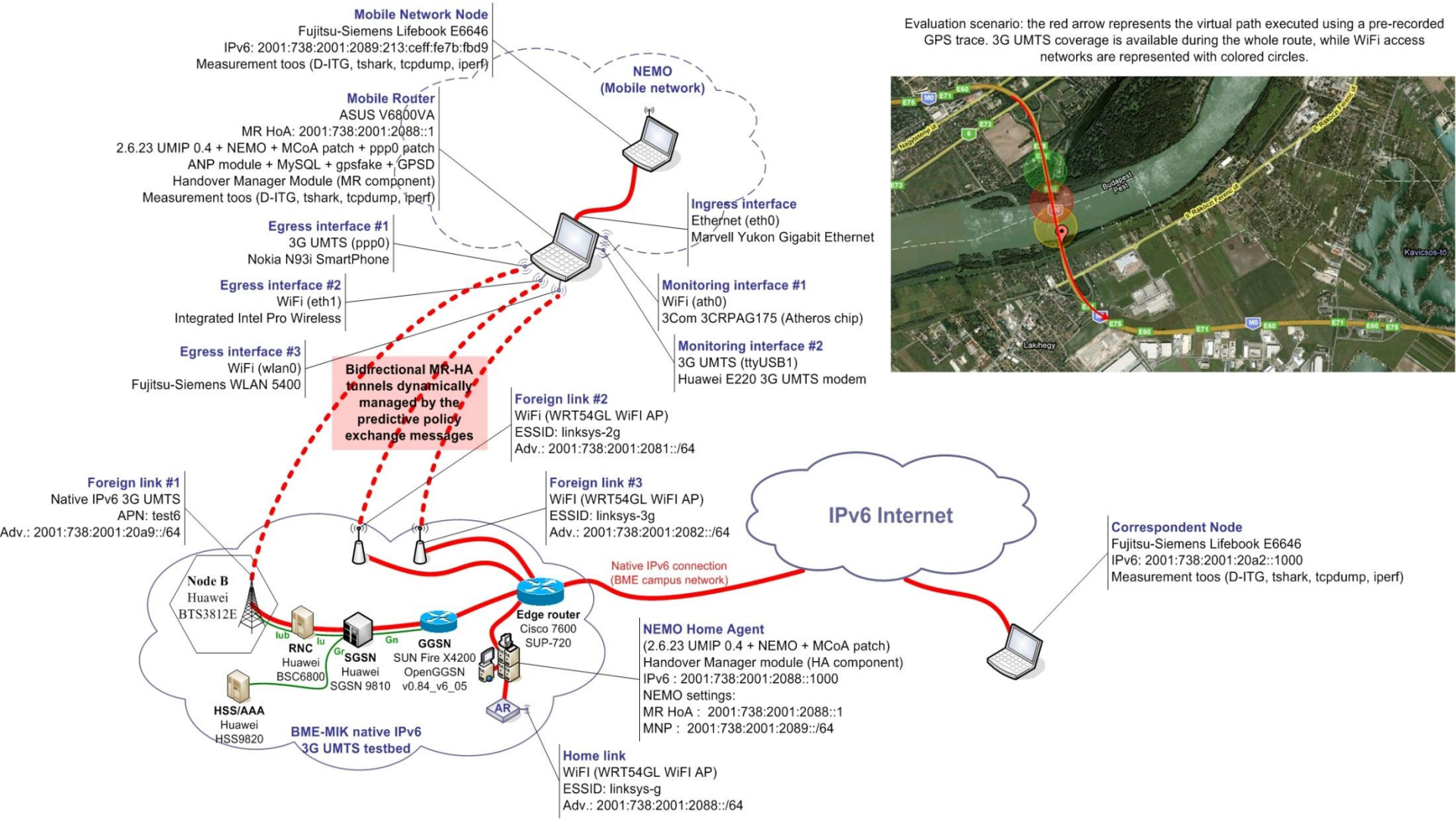
- A hálózatváltások során elvégzendő feladatok:
  - Új hozzáférési hálózatok keresése (scanning)
  - Hitelesítés, hozzáférés-menedzsment (authentication, authorizaton)
  - Csatlakozás (association)
  - IP címmel kapcsolatos műveletek
    - Új cím szerzése (acquiring Care-of Address)
    - Új cím ellenőrzése (Duplicate Address Detection)
    - Régi cím (és a hozzá tartozó routing bejegyzések) törlése (deletion of previous entries)
  - IP szintű mobilitáskezelés
    - Regisztráció az otthoni ügynöknél (registration to HA)
    - Regisztráció a kommunikációs partnereknél (registration to CNs)
- A mobilitás kezelése időigényes, ami a valós idejű (real-time) kommunikációt az okozott csomagvesztés, késleltetés miatt könnyen ellehetetlenítheti!

# GPS alapú prediktív mobilitás-kezelés




- Fókusz a NEMO-n:
  - Hosszú távon a NEMO lesz az elterjedt!
  - PAN, közlekedési eszközök mozgó hálózata, mozgó ad-hoc hálózatok, stb.
- Motiváció:
  - Tervezési probléma: IP cím szemantikailag túlterhelt (nem gondoltak a mobilitásra)
    - interfész azonosító szerep (identifier)
    - topológiai helymeghatározó szerep (locator)
  - Mozgó járművökön időben változhat a használt csatlakozási pont (pl.: a vonat nagy távolságokat szel át)
    - Ez sokszor a használt IP cím változásához (alhálózat váltáshoz) vezet
  - Az IP cím kommunikáció közbeni („on-the-fly”) módosítása megszakítja a futó kapcsolatokat
  - Eredmény: 3—5 másodperces késleltetés (= kapcsolatkiesési idő) a handoverek során
- Megoldás:
  - Meg kell jósolni a hálózatváltásokat és előre el kell végezni a műveleteket (pl. alagút kiépítés)
- A kötött útvonalon (1) közlekedő mozgó hálózatok esetében ha többször megyünk ugyanazon (2) az úton, akkor az előző utazások tapasztalatai (3) felhasználhatóak
  - (1) Pl. vonat, a villamos, a trolibusz
  - (2) Folyamatosan tudnunk kell, hogy hol vagyunk: GPS
  - (3) Hálózati mérésekre (L1/L2, L3) és azokat tároló adatbázisra van szükségünk

# GPS alapú prediktív mobilitás-kezelés (folyt.)




Evaluation scenario: the red arrow represents the virtual path executed using a pre-recorded GPS trace. 3G UMTS coverage is available during the whole route, while WiFi access networks are represented with colored circles.

# Összefoglalás

- Az IPv6 megérkezett
  - De hogy lép be a kapun?
  - v4-v6 átjárás és együttélés gyakorlati kérdései jelentősek!
- 1995 óta fejlesztett protokollcsalád, „rock-solid”
- Az IP alapú mobilitás-kezelés azonban még mindig vet fel kérdéseket:
  - Multihoming, multi-access, multi-path
  - NEMO és összetett struktúrái (egymásba ágyazott mozgó hálózatok!)
  - Speciális ID/Loc splitting (Host Identity Protocol)
  - Mindez pepitában: Distributed Mobility Management
    - A skálázhatóság miatt el kell hagyni a sub-optimális utakat és a user-plane anchor csomópontokat
    - Nem triviális! -> MEVICO (Mobile Networks Evolution for Individual Communications Experience) projekt

# Elérhetőség, ajánlott tárgyak

- Nevem: Bokor László
- Elérhetőségeim:
  - Személyes: I.E.419. vagy Z épület 3. emelet
  - Telefon: 3420 vagy 2048
  - E-mail: bokorl@hit.bme.hu

- Ajánlott tárgyak a témakörben való elmélyüléshez
  - VIHIAV96: Számítógép-hálózatok üzemeltetése I. („Cisco I.”)
    - https://www.vik.bme.hu/kepzes/targyak/VIHIAV96/
  - VIHIAV97: Számítógép-hálózatok üzemeltetése II. („Cisco II.”)
    - https://www.vik.bme.hu/kepzes/targyak/VIHIAV97/
  - VIHIAV07: IPv6 alapú számítógép-hálózatok
    - https://www.vik.bme.hu/kepzes/targyak/VIHIAV07/
  - VIHIAV16: Mobil IPv6 technológiák
    - https://www.vik.bme.hu/kepzes/targyak/VIHIAV16/
  - Önálló laboratóriumok

# Kérdések?

## KÖSZÖNÖM A FIGYELMET!

Híradástechnikai Tanszék

Bokor László
tudományos segédmunkatárs
BME Híradástechnikai Tanszék
bokorl@hit.bme.hu