Budapesti Műszaki és Gazdaságtudományi Egyetem

Villamosmérnöki és Informatikai Kar

Hálózati Rendszerek és Szolgáltatások tanszék

Leiter Ákos

FOLYAM SZINTŰ ÉS OPERÁTOR-KÖZPONTÚ DINAMIKUS MOBILITÁS-KEZELÉS MEGVALÓSÍTÁSA PROXY MOBILE IP SEGÍTSÉGÉVEL

KONZULENS

Bokor László

BUDAPEST, 2014

Tartalomjegyzék

Kivonat

A folyamatosan növekvő adatforgalom új kihívások elé állítja a mobil távközlési hálózatokat. A problémák leküzdésére többféle terhelés-elosztási módszer született és van születőben. Ezzel párhuzamosan egyre nagyobb teret hódít az a szemlélet, hogy a különböző hozzáférési technikákat IP alapon átjárhatóvá kell tenni, bevonva a rendszerbe a non-3GPP (pl. Wi-Fi) eszközöket is, lehetőleg már IPv6 felett.

A fent vázolt probléma első megoldása, mely mind a két megközelítést alkalmazza, a Mobil IPv6 (MIPv6) megszületését hozta. Ezen technológia egy nagyon flexibilis, végfelhasználó központú módszert definiál, igényelve a mobil végberendezés aktív közreműködését a hálózat-kezelésben és hálózatváltásban is. A szolgáltató oldali elterjedéshez viszont egy operátor centrikus megközelítés szükséges. A Proxy Mobil IPv6 (PMIPv6) lett az a kiegészítés, mikor magát a hálózatok közötti váltást támogató funkciót a mobil terminál helyett a hálózatban, annak „szélén" működtetik. További előnye ennek a szemléletnek, hogy nem igényel semmilyen módosítást a végberendezés ahhoz, hogy IP szintű mobilitása akár 3GPP/non-3GPP viszonylatban is megoldott legyen.

A MIPv6 fejlődésével lehetővé vált, hogy egy adott mobil eszközből kiinduló folyamokat külön-külön is kezeljünk. A PMIPv6 szintén képes alkalmazni ezt a Flow Bindings-nak nevezett módszert. Ekkor a mobil terminálon is szükség van már szoftveres módosításokra, de a séma megoldja, hogy bizonyos folyamok csak bizonyos interfészen, csak bizonyos hálózat irányába kerüljenek továbbításra.

Nem minden folyam igényli, hogy a mobilitás-kezelésben is részt vegyen. Vannak alkalmazások, tipikusan a rövid idejű kapcsolatokkal operálók (online üzenetküldők, böngészés), melyeknél a hálózatváltás mobilitás-kezelés nélkül sem okoz romlást a szolgáltatás-minőségben: nem igénylik az előző hálózatban használt, korábbi IP címük továbbvitelét, így elhagyhatjuk a mobilitás-kezelést számukra. Ezzel csökkenthetjük a jelzésterhelést és optimális átviteli utakat hozhatunk létre az adott alkalmazások számára.

Ettől eltérően a hang/videó hívások és VPN alkalmazások felhasználói élménye úgy tartható a kívánt szinten, hogy számukra a hálózatváltások után is valamilyen formában, megmaradjon kapcsolatukban az előző, hálózat váltás előtti állapot. Egy videó konferencia megszakadása és

annak újraindítása jobban rontja a felhasználói élményt és a szolgáltatás minőségét, mint a mobilitás-kezelés esetleges negatív hatásai.

A dinamikus mobilitás-kezelés pontosan ezzel a területtel foglalkozik: útmutatást nyújt hálózatváltások esetén arra, hogy melyek azok a folyamok, amiket mobilitás-kezelésben kell részesíteni, és hogyan.

PMIPv6 esetén is lehet dinamikus mobilitás-kezelésről beszélni. Új hálózathoz érkezéskor (akár úgy, hogy a jelenlegi kapcsolat is él) érdemes megvizsgálni, hogy van-e olyan folyam, ami miatt inicializálni kell-e egy újabb mobilitás-kezelési folyamatot, vagy elég csak az új hálózaton kapott natív IP hozzáférést használni. Tipikus eset, mikor egy felhasználó a meglévő 3GPP hálózaton átmenő VoIP vagy video hívása nem terelődik át az újonnan hatósugárba kerülő Wi-Fi hálózatra és csak azok a folyamok fognak a terheléselosztás (offloading) végett átkerülni a non-3GPP hozzáférésre, amelyek nem igénylik az adott helyzetben a mobilitás-kezelést (pl. web-böngészés). Egy 3GPP mobil hálózatban szükséges egy dedikált eszköz, amely eldönti, hogy egyáltalán az adott folyamot mobilitás-kezelésben kell-e részesíteni vagy sem. Ezt a döntés hárulhat akár az MME-re vagy a PCRF-PCEF párosra is.

TDK dolgozatom ezen funkciók 3GPP rendszerekbe történő integrálására ad javaslatot, és valós implementációkkal végzett mérések segítségével keres válaszokat a vázolt problémákra az operátori hálózatokban bevezetés alatt álló PMIPv6 protokoll kiegészítésével.

Abstract

The continuous increase in mobile data traffic creates new challenges for mobile network operators. To solve this problem, many traffic offloading techniques have been created and continue to be created. In parallel, there is a trend to handle all the access techniques under the umbrella of IP, including non-3GPP networks (i.e. Wi-Fi), mainly with the help of IPv6.

Mobile IPv6 (MIPv6) was one of the first solutions which made possible to deploy the above-mentioned approaches. This technology is a very flexible, mobile-end-user-centric method, and demands active participation from the user's equipment to ensure network handling and network changes too. However, operators need a more network-centric way of working to deploy such services in a real provider environment. Proxy Mobile IPv6 (PMIPv6) was developed to satisfy this need. PMIPv6 moves the mobility-handling functions from the mobile node to the edge of the network. Another advantage of using PMIPv6 is that it does not call for any modifications in the network stack of the mobile end-terminal.

With the help of the evolving MIPv6, it started to be possible to separate and manage the IP flows one by one. PMIPv6 also adopted this method, called Flow Binding. This alteration requires software modifications in the network stack of the mobile node, but the flows are able to be forwarded to the proper interface and network.

However, not all the flows need to go through mobility handling procedures. There are applications which maintain short-lived connections (i.e., browsing, online messaging) where the network change does not cause problems in the quality of service and they do not require IP address preservation, so mobility handling can be omitted or ignored. With this approach the number of signal-related messages can be decreased and optimal transport routes can be established for each application. In spite of this, the Quality of Experience of voice calls, video calls and VPNs can be kept at a high level if network changes preserve the previous state (i.e., a globally available IP address with the help of appropriate mobility management mechanisms).

Dynamic mobility management schemes deal exactly with the above problem as they provide suggestions as to which flow needs to be handled by mobility management functions and how.

PMIPv6 could also implement this approach. When the user's equipment is connected to a network and then moves to a new one, the mobility management system could examine whether there are flows which require mobility management or whether native IP connection without additional mobility functions is enough. A typical use-case is when a user's current VoIP or video session through the 3GPP network is not forwarded to a newly-available Wi-Fi network due to offloading. Only those sessions will be newly initialized which do not require mobility handling (e.g., browsing).

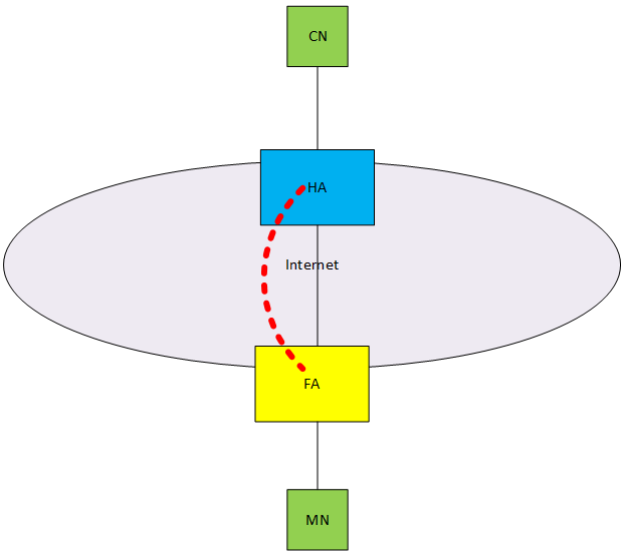
In a 3GPP core network there must be a functional entity for deciding whether a flow needs to be offloaded or needs to be handed over by the mobility management subsystem. This role can be applied in MMEs of PCRF-PCEF nodes.

In my TDK work I provide a scheme on how to integrate the above advanced dynamic mobility management methods into a 3GPP network, and analyze these open questions using real software implementations.

Bevezetés

A különböző hozzáférési technológiák közötti átjárhatóság biztosításának egyik legkézenfekvőbb módja, ha IP felett történik. A kutatások során ez az igény találkozott a mobilitás kezeléssel is, mely így már egyszerre képes megoldást adni e két problémára.

A Mobile IPv4[16] az IPv4 első olyan kiterjesztése, mely lehetővé teszi, hogy a hosztok a mozgásuktól és kapcsolódási pontjuktól függetlenül tudjanak kommunikálni egymással vagy akár nem mozgó elemekkel is.



1. ábra MIPv4

Az otthoni ügynökök (Home Agent, HA) és az idegen ügynökök (Foreign Agent, FA) meghirdetik szolgáltatásaikat, melyekről a mozgó csomópontok értesülhetnek. A mobil eszköz informálódik a hirdetésből, hogy hol tartózkodik. Ha otthon van, akkor mobilitást támogató kiterjesztések nélkül kommunikál, ha hazatért egy másik hálózatból, akkor végrehajt egy deregistration folyamatot a HA-nél.Ha új hálózatba került, akkor vagy Care of Address vagy Colocated Care of Address címet igényel, majd regisztrálja magát az otthoni ügynökénél.

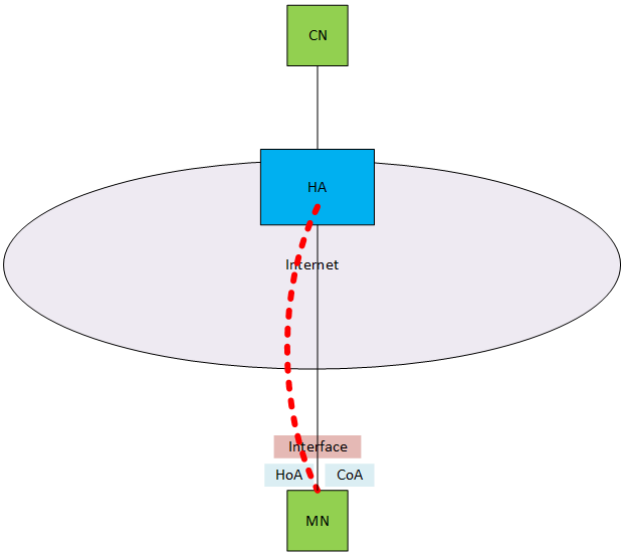
A mobil hoszt otthoni hálózatába küldött adatokat egy tunnel segítségével elküldi a nála bejegyzett címre. Fordított esetben alap IP forgalomirányítási megoldást lehet használni.

Mobile IPv6 (MIPv6)[1]

Az újgenerációs IP protokollhoz (IPv6) kifejlesztett mobilitás-kezelési séma, melyre megoldások egész sora épült (Mobile IPv6 protocoll family). Lényeges változás a Mobile IPv4-hez képest, hogy nincs idegen ügynök, a mobil eszköz magának szerzi be a címet. Ehhez nyújt segítséget az IPv6 autokonfigurációs (Auto Configuration) és a szomszédság feltérképező (Neighbor Discovery) metódusa.

A mobil eszköz rendelkezhet több ideiglenes címmel, ezek közül az elsődleges (Primary Care of Address) címet fogja a regisztráció során az otthoni ügynökének elküldeni. Ez a tulajdonsága megkönnyíti a hívásátadást, elérhető marad a MN akkor is, mikor új elsődleges címet regisztrál az otthoni ügynöknél. Nincs szükség a regisztrációnál és az összeköttetés-frissítésnél két különböző típusú üzenetre.

További újdonság, hogy az idegen hálózatban található MN az IPv6 csomag fejlécébe forrás címként a saját elsődleges ideiglenes IP címét is megadhatja. Ezzel a node-ok közötti kommunikáció során nincs szükség az otthoni ügynök használatára. Tipikusan csak a kommunikáció elején van szükség a HA használtára ebből következően.



2. ábra MIPv6

A Mobile IPv6 úgy oldja meg, hogy mindig elérhető legyen a hálózatban a mobil, hogy kihúz egy tunnelt a HA és a MN között, melynek végződéseinek a címei mindig ugyanazok lesznek.

Mozgás során az új CoA segítségével mindig újra felépíti a tunnelt. Mobil IPv6 esetén a következő kiterjesztésekről beszélhetünk:

- NEMO BS (RFC 3963): hálózatok mobilitásával foglalkozó szabvány.
- Fast Mobile IPv6 (RFC 4068): a második és a harmadik rétegbeli hálózatváltás gyorsítását oldja meg.
- Hierarchikus Mobil IPv6 (RFC 4140): bevezet egy új entitást (Mobile Anchor Point, MAP), annak érdekében, hogy a jelzésüzenetek késleltetéséből eredő szolgáltatás-kiesést ellensúlyozza és helyileg feldolgozza.
- Proxy Mobil IPv6 (RFC 5123): képes olyan mobil eszközök mobilitását kezelni, melyek nem rendelkeznek semmilyen mobilitás-kezelést lehetővé tévő kiterjesztéssel.
- Multiple Care of Addresses Registration (RFC 5648): megoldja, hogy a több CoA címet tarthassunk fent egy MN számára, így könnyítve meg a hálózatváltást és biztosítva redundanciát és több interfész együttes használatát.
- Flow Bindings (RFC 6089): olyan kiterjesztés, mely azzal foglalkozik, hogy egy vagy több adatfolyamot tudjon a készülék egy CoA cím mögé rendelni.

Proxy Mobile IPv6 (PMIPv6)

A protokollt alapkoncepciója szerint arra tervezték, hogy képest legyen egy maghálózattól és különböző hozzáférési technológiáktól (WiMAX, Wi-Fi, 3GPP) független mobil hálózatot létrehozni úgy, hogy közben a MN IP címe ne változzon.

A nevéből eredően a PMIPv6 képes olyan hosztok mobilitás kezelésére, melyek nem rendelkeznek a MIPv6 kiterjesztéssel („proxy-zza" számukra ezt a szolgáltatást). Ez nagy könnyebbséget jelent, hiszen a MIPv6 nincs széles körben elterjedve, viszont a mobilitással kapcsolatos igény nem csak mobiltelefonoknál, hanem sok egyéb eszköznél felvetődik. A PMIPv6 az egyetlen ilyen, hálózat-központú mobilitást kezelő protokoll, melyet az IETF szabványosított (2012). A hálózat-központúság azt jelenti, hogy ellentétben a Mobil IP-vel, itt kizárólag a hálózat feladata, hogy kezelje a mobil eszköz mozgását.

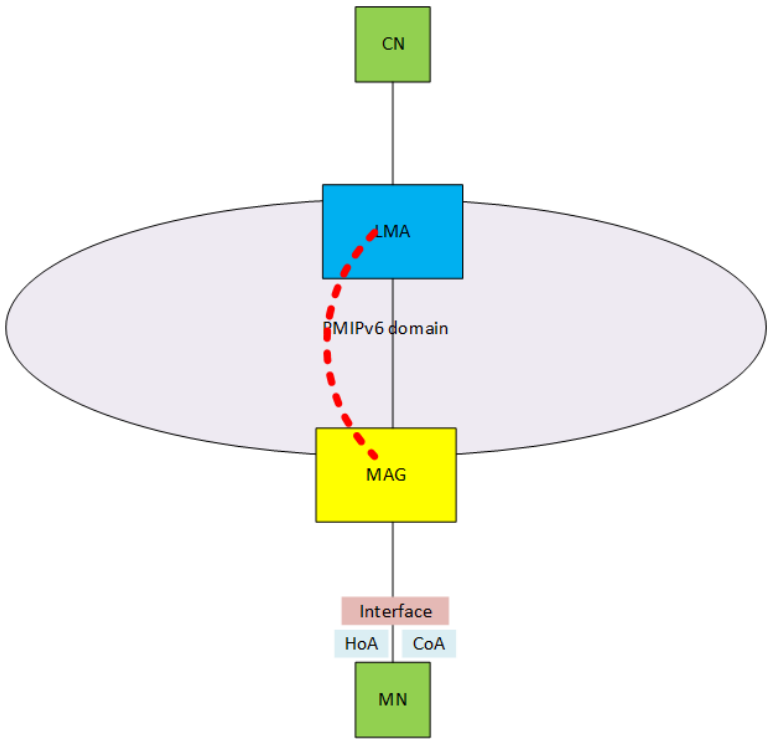
A PMIPv6 támogatja, hogy a szolgáltatók lokális mobilitás kezelést hajtsanak végre úgy, hogy közben nem az egyes mobil eszközökre bízzák ezt a feladatot, hanem hálózat szinten kezeljék.

A PMIPv6 főbb funkcionális elmei:

- Local Mobility Anchor (LMA)
- Mobile Access Gateway (MAG)

Az LMA tölti be a PMIPv6 architektúrában az otthoni ügynök szerepét. Az ő feladata a mobil eszköz címeinek a kezelése és felelős a MN folyamatos elérésének a biztosításáért. Több LMA is működhet a hálózatban.

A MAG szerepköre a mobilitás kezelésére terjed ki. Funkciói közé tartozik, hogy kezelje a mobil eszköz felkapcsolódását, illetve lekapcsolódását a különböző linkeken, tovább a regisztrációs folyamatot is ő indítja el. A mobilitással kapcsolatos jelzésüzeneteket ő generálja.



3. ábra PMIPv6

Különbség az Mobile IPv6-hoz képest, hogy a már korábban említett kétirányú alagutat itt nem az MN-ig húzza ki a HA (jelen esetben LMA), hanem csak a MAG eszközig.

Mikor egy mobil eszköz belép a Proxy Mobile IPv6 domain-be, és csatlakozik egy linkhez, a MAG az azonosítás után eldönti, hogy van-e joga adatokat forgalmazni abban a hálózatban az adott eszköznek. Tipikusan az MN-ID egyedi azonosító alapján történik az eszközök azonosítása. Ennek a mezőnek nincsen specifikálva a mibenléte, ezért gyakran a MAC cím alapján zajlik le a procedúra.

A MAG küld egy PBU üzenetet (Proxy Binding Update) az LMA számára. Itt van az egyik fő különbség a sima Mobil IPv6 és a PMIPv6 között: az előbbinél a BU üzenetet a mobil eszköz küldi, míg az utóbbinál a MAG. A PBU az alábbi főbb szegmenseket tartalmazza:

- Hozzáférési technológia
- Handoff indikátor
- Bejegyzés élettartama
- Flag, mellyen megjelöljük, hogy PBU-ról van szó, nem sima BU-ról.

A PBU elküldése után a MAG a Binding Update List (BUL)-ben készít egy bejegyzést a mobil eszközről. Szintén meg kell jegyezni, hogy a Mobil IPv6-ban ez az adat struktúrát a MN tartja karban, viszont a PMIPv6-ban már a MAG feladata ez. A BUL teszi lehetővé a MAG számára, hogy tudja melyik interfészén milyen mobil eszközök találhatóak.

Az LMA mikor megkapja a MAG-tól származó PBU üzenetet, akkor végez egy ellenőrzést rajta, hogy valóban érvényes-e. Ellenőrzi, hogy a Bindig Cache (BC) táblája tartalmazza-e már ezt a MN-ot. Ha ez a mobil eszköz először lépett be a PMIPv6 domain-be, akkor nem fog találni semmit, így készít egy új bejegyzést.

A BC-ben található egy jelzőbit (flag), mely megmutatja, hogy ez egy PMIPv6 és nem egy sima MIPv6 bejegyzés. Továbbá tartalmaz még információkat a MN-ról, az őt kiszolgáló MAG-ról és a mobil eszköz helyzetéről.

Miután megtörténtek a táblázatok frissítései, az LMA létrehoz egy IPv6 in IPv6 kétirányú alagutat a MAG felé. Végül az LMA küld egy Proxy Binding Acknowledgment (PBA) üzenetet a MAG számára. A PBA szintén tartalmaz egy flaget, mely jelzi, hogy Proxy Mobil környezetben értelmezendő.

Azt követően, hogy a fenti jelzésüzenetek lezajlottak, a MN küld egy Router Solicitation üzentet a hagyományos szomszédság feltérképezés részeként. A MAG-nak addig nem kell válaszolnia erre az üzenetre, amíg az LMA-ban végbe nem ment sikeresen a regisztráció.

Ezek után a mobil szerez magának IP címet valamilyen módon (IPv6 stateless autoconfiguration vagy DHCPv6).

Mobile IPv6 Flow Bindings [4]

A MIPv6 kifejlesztésével megjelent az az igény, hogy az egyes IP folyamokat különböző módon, különböző QoS osztályban, akár más interfészen továbbítsuk a célállomás felé.
A MIPv6 [1]DSMIPv6 [5] és a NEMO BS[4] segítségével egy MN (avagy NEMO esetében egy MR) a mobilitását BU üzenetekkel vezérli, mellyel megmondja, hogy egy adott CoA melyik HoA-hoz tartozzon. Az RFC 3775 (MIPv6) és az RFC 5555 (DSMIPv6) csak azt definiálja, hogy egy MN egy CoA-t kezel.

A MIPv6 Flow Bindings „Flow”-nak nevezi azoknak az IP csomagoknak a halmazát, melyek egy „Traffic Selector”-nak (TS) megfelelnek. A TS egy folyamnak fogja tekinti azokat a csomagokat, melyekre az alábbi attribútumok egyeznek („five tuple”):

- forrás IP cím
- cél IP cím
- transzport protokoll
- forrás port cím
- cél port cím
- (egyéb magasabb rétegbeli fejlécek egyezősége)

Ahhoz, hogy egy CoA-hoz több folyamot tudjunk allokálni, egy új ID-t kell bevezetni, melynek a neve Flow ID. Előnye ennek a megközelítésnek, hogy BU-ban is el lehet küldeni a flowID-t. Az IPv6 Mobility Headerben (MH) definiálták a Flow Identification Mobility Option nevű mezők halmazát, mely számos új attribútumot tartalmaznak a Flow Binding kezelésére:

- FID: a korábban említett Flow Binding ID
- FID-PRI: priorizálni lehet vele az átlapolódó flow-kat

Az alábbi táblázat szemlélteti egy lehetséges táblát MIPv6 MCoA Flow Binding esetben (rendezett listában) (1. táblázat, 2. táblázat):

FID-PRI	FID	Traffic Selector	BIDs	A/I
10	4	TCP	2	Active
30	2	srcAddr=IPy	4	Inactive
40	5	UDP	1,3	Active

1. táblázat MIPv6 MCoA Flow Binding BT

BID-PRI	BID	CoA
20	1	IP1
30	3	IP2
30	2	IP3

2. táblázat Flow table

Ezen listáknak megfelelően, minden TCP forgalom a BID2-re lesz továbbítva az IP3 címen keresztül. Mivel inaktív a második bejegyzés a FID táblában, ezért nem fogja befolyásolni a forgalmat. Továbbá a BID táblában sincs hozzá bejegyzés.
Bármilyen UDP forgalom, mely eddig nem lett kategorizálva, a harmadik bejegyzés szerint mind a BID1-en és mind a BID3-on ki lesz küldve. Végül azok a folyamok, melyek semmire nem illeszkednek, a legnagyobb BID szerint továbbítódnak.

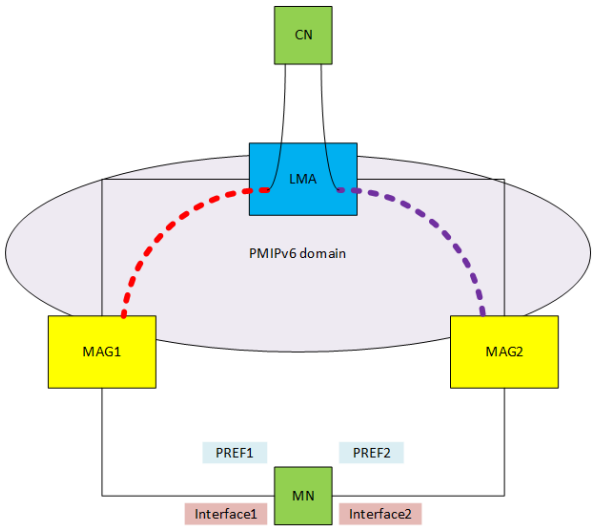
PMIPv6 Flow Bindings

A MIPv6 inkább felhasználói megközelítést tesz lehetővé, cserébe a felhasználóknak az IPv6 stackjüket képessé kell tenni a Mobility Header feldolgozására. Ezen segít a PMIPv6, mikor is már nem kell módosítani a meglévő implementációkat, hanem a hálózat fog gondoskodni (HA-LMA, MAG) segítségével a mobilitás kezelésről. Ez inkább egy szolgáltatói megközelítést tesz lehetővé. A szolgáltató maga vezérli, a saját hálózati eszközeivel a PBU, PBA üzeneteket, azok tartalmát, továbbá ő végzi el a működéshez szükséges alagutazást is.
A szolgáltatóknál is megvan az az igény, hogy különböző folyamokat, különböző módon kezelhessenek, egyfajta optimumra törekedjen a QoS, cellaterheltség és adatátviteli sebesség tekintetében. Mindezek mellett szeretnék minél jobban a saját kezükben tartani ezeknek a vezérlését.
A jelenlegi ipari alkalmazások egyelőre csak azt teszik lehetővé, hogy a felhasználó eldöntheti, hogy egy Wi-Fi vagy a mobilhálózat segítségével szeretne csatlakozni az Internetre. További fejlesztésként a szolgáltatónak fontos lehet az, hogy egy adott folyamot (pl. FTP letöltés) inkább a sávszélesség igényes, de kevésbé QoS érzékeny alkalmazásokhoz illeszkedő Wi-Fi hozzáférésen, míg egy telefonhívást (VoLTE) inkább a sokkal jobb QoS-t biztosító LTE hozzáférésen szolgáljon ki. A motiváció e mögött az, hogy a felhasználó alacsony prioritású kommunikációs kéréseit, ne egy drága és erőforrásokban relatíve korlátolt linken szolgáljuk ki.
Ennek a problémának a feloldására egyelőre nincsenek szabványok, csak RFC draftok, különböző cikkek állnak rendelkezésre.
A PMIPv6 Flow Binding[6] esetében sajnos nem teljesen igaz, hogy a felhasználói készülék mindenféle beavatkozása nélkül képes a folyamokat vezérelni. Ugyan a hálózat dönti el, hogy melyik interfészen milyen folyamot kell használni, ezt a döntést le kell juttatni a MN felé. Erre szolgál a Flow Policy Update (FPU) üzenet, mely egyfajta tűzfalszabályokat tartalmaz. Viszont

az FPU üzenet feldolgozására képesnek kell lennie az MN-nek. Emiatt némi módosítást végre kell hajtani az MN szoftverein, nem lesz számára teljesen transzparens a megoldás.

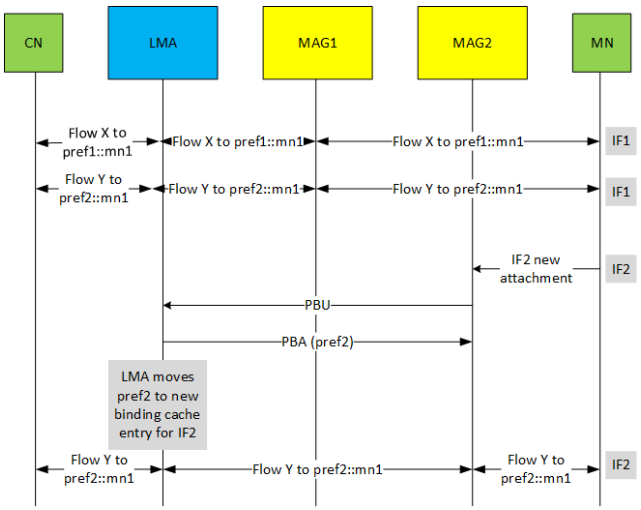
Különböző PMIPv6 Flow Mobility forgatókönyvet léteznek a protokoll alkalmazására. A fő különbségek, hogy a MN interfészei ugyanazon prefixeket használják-e vagy sem (4. ábra PMIPv6 Flow Mobility különböző prefixekkel)

- Új csatlakozás idején az MN ugyanazokat a prefixeket használja, melyeket már egy korábbi meglévő csatlakozása során használt. Ez nem az RFC 5213 szerinti alap PMIPv6 viselkedés.
- Új csatlakozás esetén más, teljesen új prefixeket igényel. Az RFC 5213 ezt definiálja
- Új csatlakozás esetén, az MN a prefixeit a már használatban lévőkből és újakból kapja. Ez a fenti kettő hibrid megoldása. Local policy-k segítségével hozza meg a döntést az LMA, hogy az eddig nem használt prefix kizárólagosan az adott kapcsolathoz rendelhető-e vagy sem.



4. ábra PMIPv6 Flow Mobility különböző prefixekkel

A Binding Cache-t (BC) az LMA-n ki kell terjeszteni ahhoz, hogy tudja kezelni az egy MN-ről származó több Proxy CoA regisztrációt, továbbá képessé kell tenni, hogy egy MN-hez tartozóan, ugyanazt a címet, több interfészen keresztül is kezelje. Az LMA emiatt egy MN-ra vonatkozóan akár több bejegyzést is nyilvántarthat a BC-ben. A Binding ID (BID) egy lokális azonosító, melyet csak az LMA használ, hogy képes legyen eldönteni, hogy hova kell továbbítani az adott folyamatot.



5. ábra PBU jelzésüzenetek Ha a prefixek különbözők, akkor IF1-hez miért tartozik pref1 és pref 2 is?

Példa, egy lehetséges BC táblára (3. táblázat):

BID-PRI	BID	MN-ID	ATT	HNP	Proxy-CoA
20	1	MN1	Wi-Fi	HNP1,HNP2	IP1 (MAG1)
30	2	MN1	3GPP	HNP1,HNP3	IP2 (MAG2)

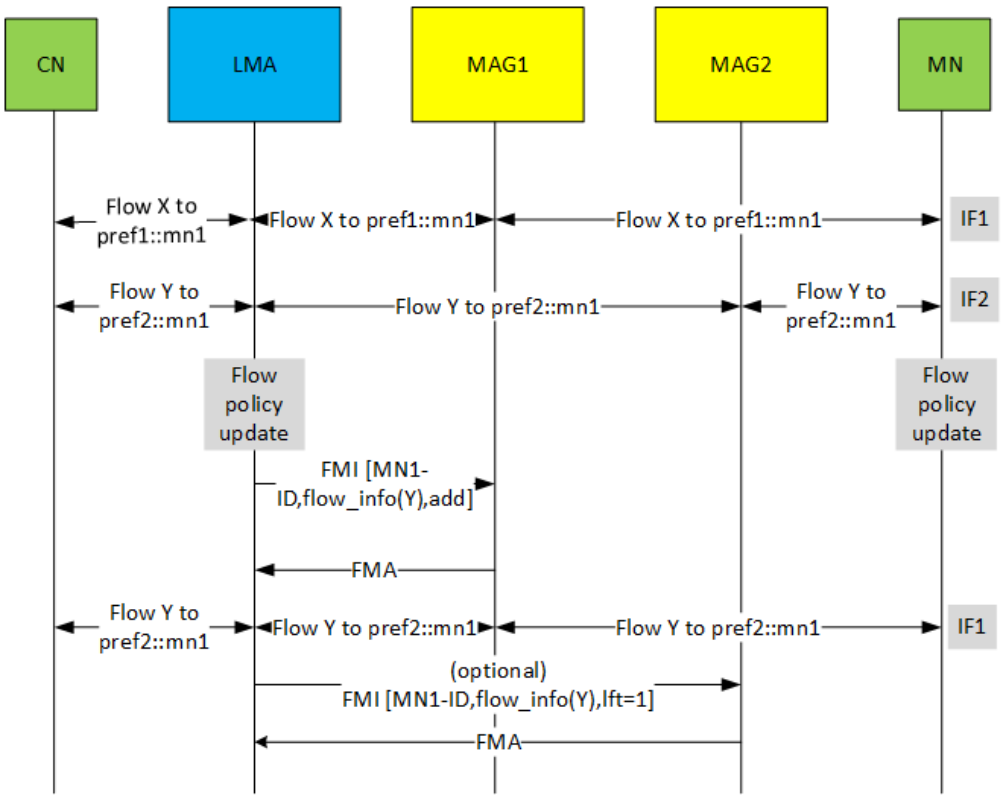
3. táblázat PMIPv6 Flow Bindings BC

A példában látszik, hogy ugyanaz az MN két MAG-on keresztül kapcsolódik egyszerre az LMA-hoz és továbbá ugyanazt az HNP-et használják mind a két különböző hozzáférési technológián.

A PMIPv6 Flow Mobility (is) bevezet egy újabb adatbázist is, mely magát a folyamokat tartja nyilván: Flow Mobility Cache (FMC) (4. táblázat).

FID-PRI	FID	TS	BIDs	Action	A/I
10	2	TCP	1	Forward	Active
20	4	UDP	1,2	Forward	Inactive

4. táblázat PMIPv6 Flow Mobility Cache



6. ábra FMI jelzés üzenetek itt nem pref1-re megy át az Flow Y az update után?

Folyamok és kapcsolatok kezelése 3GPP hálózatokban

Általános 3GPP LTE/EPC architekúra [26]

Főbb LTE hálózati elemek és feladataik:

MME (Mobility Management Entity):

- a vezérlő sík megvalósítója az EPC-ben
- mobilitás támogatás
- előfizető helyének lekérdezése, paging megfelelő helyre küldése
- útvonalválasztás az előfizető pozíciójának megfelelően
- minden egyéb vezérlési feladat: hordozó felépítése,
- autentikáció, titkosítási kulcsok cseréje, stb.

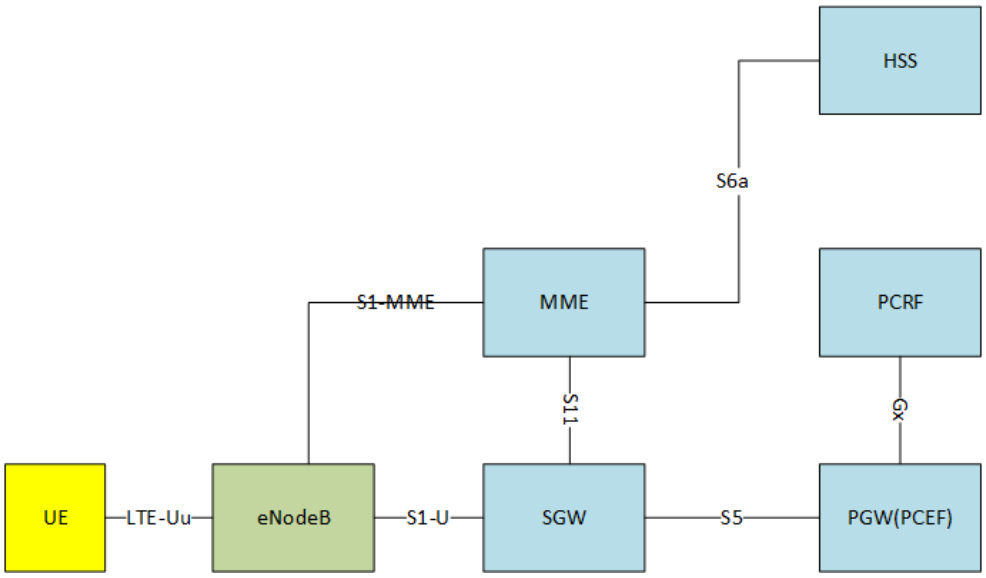
PGW (Packet Data Network Gateway):

- az interfész a külső csomagkapcsolt hálózatok felé: Internet, más szolgáltató hálózata, nem LTE hálózat
- egy kapcsolat alatt a külső hálózati forgalom egy PDN Gw berendezésen keresztül megy, akárhová mozog is az
- az előfizető felé az SGW-n keresztül az eNodeB-n át megy a forgalom
- a maghálózatban látszik a mobilitás
- minden cellaváltásnál új „alagútban” megy a forgalom az eNodeB felé/től
- ez nagy különbség a 3G-hez képest, ahol az RNC elfedte a lokális mobilitást (RNC-ig kellett az IP alagutat vezetni)

SGW (Serving Gateway):

- az előfizetői adatok továbbítója az EPC és az eNodeB között,az S1-U nagyban hasonlít a 3G Iu-PS-hez
- S1-U működése: tunnelt húz ki az eNodeB felé, a felhasználó csomagjainak továbbítására.

Az eNodeB az LTE képes bázisállomást jelöli. A HSS: a korábbi generációs HLR és AuC egységek aggregálása.



7. ábra Alap EPC architektura PCRF-fel kiegeszitve

MAPCON (Multi access PDN Connection)

A MAPCON [10] technika segítségével egy UE képes felépíteni több különböző PDN kapcsolatot, különböző hozzáférési hálózaton keresztül (LTE, Wi-Fi). Ehhez a két különböző PDN kapcsolathoz tarozó APN-ek függetlenek egymástól. Továbbá mind a felhasználónak, mind az operátornak lehetséges a forgalom elterelése (tehermentesítés). Így megengedett, hogy a hálózat fenntartson egy kapcsolatot a VoLTE/IMS kapcsolat számára a RAN-on keresztül és egyet az adatforgalmazásra valamilyen non-3GPP kapcsolaton keresztül.

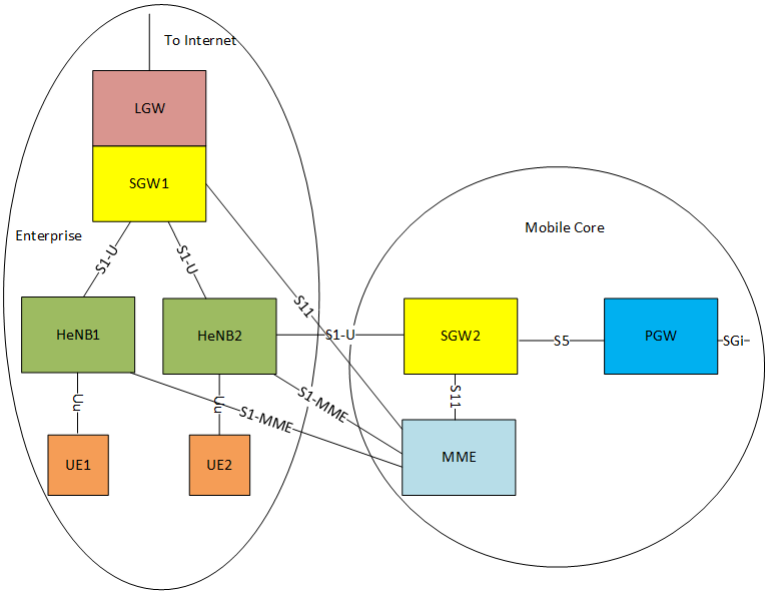
Selected IP Traffic Offload (SIPTO)

A SIPTO [7]célja, hogy már a hálózat hozzáférési részénél (RAN) vagy ahhoz minél közelebb képes legyen a forgalomtól tehermentesíteni a maghálózatot. Az MME vagy az SGSN megválaszthatja úgy a PGW-t vagy az SGW-t, hogy az fizikailag a lehető legközelebb legyen az UE-hez és a RAN-hoz. A SIPTO tipikusan alkalmas arra, hogy egy Home (e)NodeB-n keresztül tehermentesítse a hálózatot.

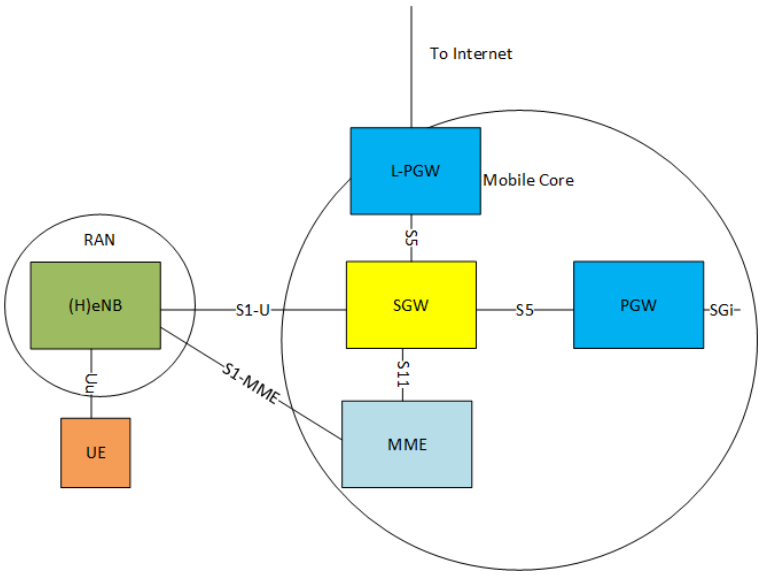
A Home (e)NodeB segítségével történő tehermentesítésre három forgatókönyv létezik:

- Mind a Home (e)NodeB alrendszert, mind a felhordó hálózatot ugyanaz a szolgáltató üzemelteti.
- Különböző szolgáltató üzemelteti a H(e)NodeB alrendszert és a felhordó hálózatot
- Az a pont, ahol a terheléselosztás megtörténik (L-PGW) egy privát tartományban van (pl. NAT)

Új PGW geográfiailag, de új IP cím is kell és ez meg tudja szakítani az IP folyamokat: IP szintű mobilitás-kezelésre van szükség.



8. ábra SIPTO@LN

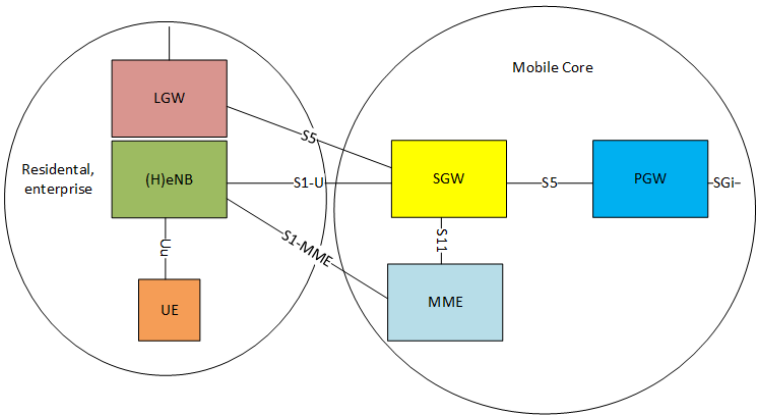


9. ábra SIPTO above RAN

Local IP access (LIPA)

A LIPA-t [13] alapvetően azért tervezték, hogy egy lokális 3GPP hozzáférési ponton (femtocella, picocella) tudjon elérhetőséget biztosítani a helyi hálózathoz (intranet). Tehát a mobil végberendezés képes elérni a lokális hálózati elemeket, egy alapvetően a mobilhálózat kiterjesztésére szolgáló eszközön úgy, hogy az adatfogalma nem terheli le a mobil maghálózatot.

LIPA-val lehetséges egyszerre, az az párhuzamosan elérni a mobilhálózat szolgáltatásit és a helyi hálózati eszközöket és szolgáltatásokat (külön számlázással is). Képes fenntartani a helyi hálózathoz köthető IP kapcsolatot, mialatt HeNB váltás történik. Növelhető a felhasználói élmény a mobilhálózat terhelésmentesítésével.



10. ábra LIPA

SIPTO és LIPA összehasonlítása [21](5. táblázat)

LGW elhelyezkedés	LGW együtt van az eNB-vel	LGW külön van az eNB-től	
Honnan Hova	LAN	Enterprise	RAN
Internet	SIPTO@LN	SIPTO@LN	SIPTO above RAN
LAN	LIPA	LIPA	

5. táblázat SIPTO és LIPA kapcsolata

Coordinated Selective IP Traffic Offload (CSIPTO)[14][15]

Ahogy a SIPTO is bemutatta, a PGW-t (LGW-t) egyre jobban a felhasználó közelébe igyekszik elhelyezni, közel a hálózat széléhez. Viszont egy PGW váltás IP cím változással is jár. Ez az IP cím változás nem ugyanolyan módon hat a különböző UE alkalmazásokra; emiatt megkülönböztetjük az alábbi típusúakat:

- Rövid életű folyamok: web böngészés, szöveges üzenetküldő szolgáltatások, melyeknél a legrosszabb esetben is csak frissíteni kell a weboldalt, vagy az üzenetküldő alkalmazások, amik nem feltétlen IP alapján találják meg a címzettet.
- Hosszú életű folyamok (valós idejű folyamok): telefonhívások, videokonferenciák. Ilyenkor a felhasználónak megszakad a kapcsolata a központ kiszolgálóval, újra be kell jelentkezni vagy tárcsáznia. A VPN kapcsolatok is megszűnnek.

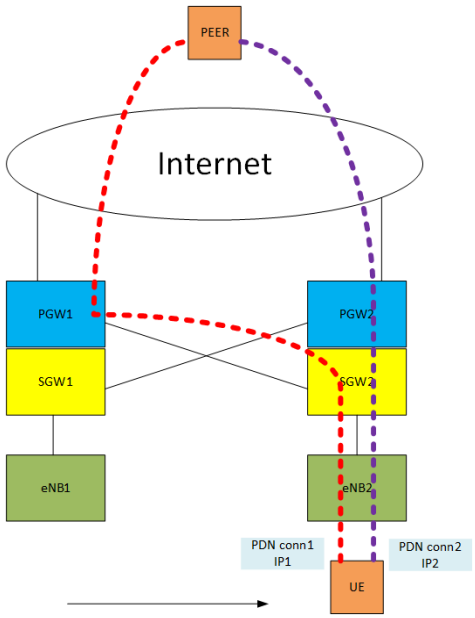
Tehát a fenti felvetések megkövetelik, hogy mi szerint optimalizáljuk a forgalmat:

- IP cím megőrzés
- adatfolyam útjának rövidítése

Három különböző esetet lehet megkülönböztetni a leírtak szerint.

Első eset

Miután megtörtént az SGW váltás, két PDN kapcsolatot fog a hálózat fenntartani.

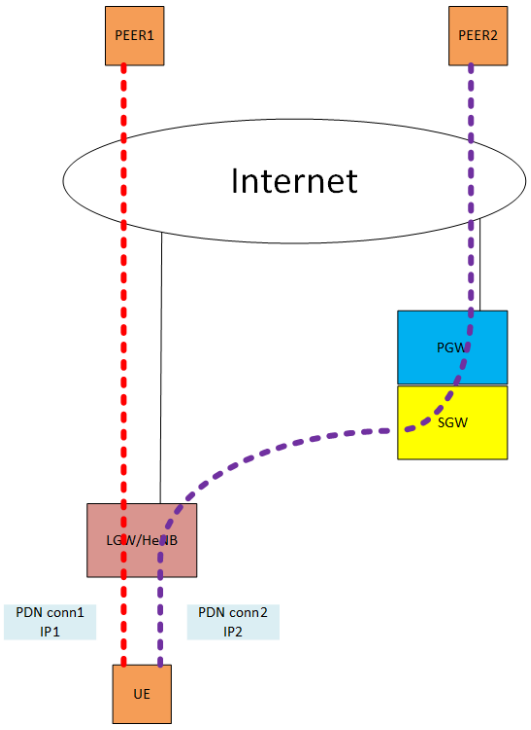


11. ábra Első eset

Az egyik PDN kapcsolat még a korábbi, de már szuboptimálissá vált PGW1-el tartja fent a kapcsolatot, hogy azok az alkalmazásokban, melyek igénylik az IP cím megőrzését, ne legyen kapcsolati probléma. A másik, immár az optimális útvonalon közlekedő csomagok számára. Amint megszűnik a kommunikáció a régi kapcsolaton, a hálózat el fogja bontani az.

Második eset

Már az elején alapvetően két PDN kapcsolat van felépítve. Az egyik, amelyiknél biztosított az IP cím megőrzése, a másik nem.

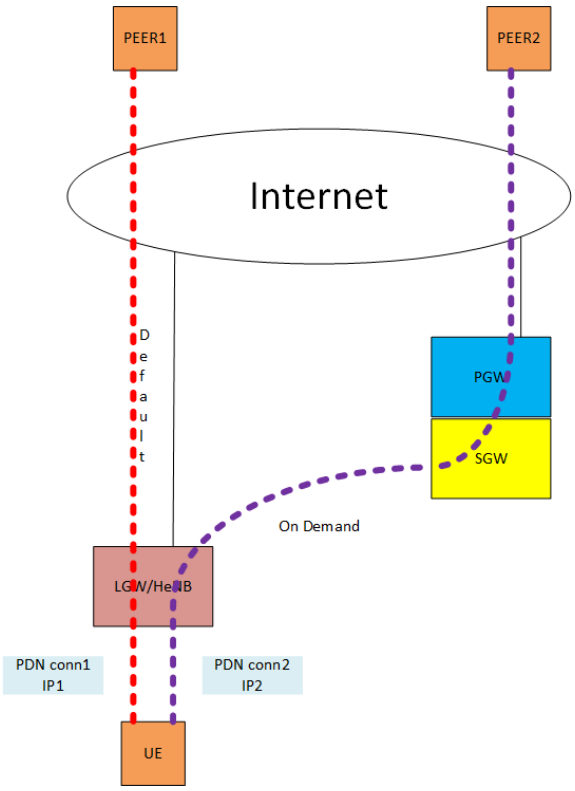


12. ábra Második eset

Új elemként bejön az LGW és HeNB páros, melyek segítségével terhelést lehet levenni a maghálózatról.

Harmadik eset

Az architektúra azonos a második esetben leírtakkal. Viszont ennél a megoldásnál alapértelmezetten csak az LGW-n átmenő PDN jön létre. A PGW-n átmenő PDN-t csak igény szerint hozza létre a rendszer, ha olyan IP folyam keletkezik, mely igényli az IP cím megőrzését.



13. ábra Harmadik eset

Elosztott és dinamikus mobilitás kezelés (Distributed and Dynamic Mobility Management, DMM)

Két féle módot tudunk megkülönböztetni:

- Részlegesen elosztott
- Teljesen elosztott

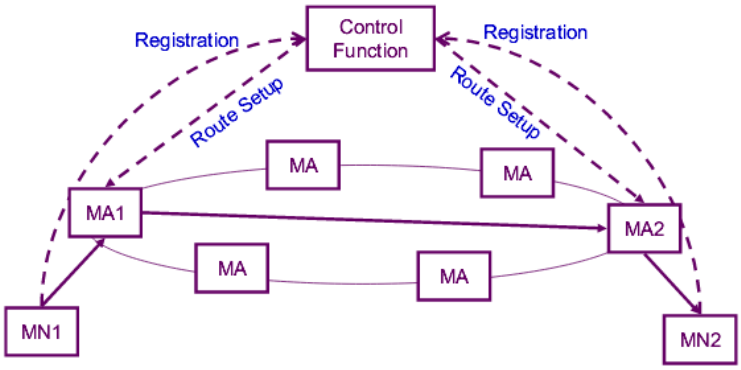
Részlegesen elosztott eset

A DMM-e alkalmazhatjuk részlegesen, azon tekintetben, hogy külön választjuk-e az adatsíkot és a vezérlősíkot.

Adatsík és vezérlősík szétválasztás

A hagyományos mobilitás-kezelési protokollok (MIP,PMIP) nem választják szét a egymástól a vezér és adatsíkot; minden jelzésüzenet és adatforgalom keresztülmegy a HA-n vagy LMA-n.

Az adatforgalom tipikusan nagyságrendekkel nagyobb, mint a jelzésüzenetek forgalma, tehát szétválasztva a két síkot hatékony forgalom elválasztás jöhet létre a különböző ágensek újra pozicionálása nélkül. Ez egyszerűsíteni tudja a különböző MA közötti kommunikációt.



14. ábra Közös vezérlősík, elosztott adatfolyam [17]

A routing funkciókat az MA-k látják el. Amikor egy MN egy másik MA-hoz kapcsolódik, a központi elem fogja értesíteni az előző és a jelenlegi MA-kat új hálózati beállításokról.

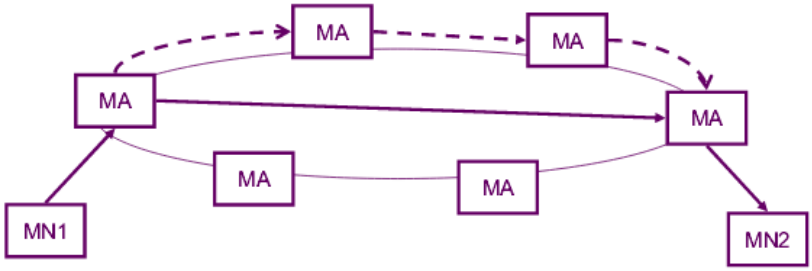
Teljesen elosztott megközelítés

Ennél a variációnál már az vezérlősíkot is elosztva kezeljük. Egy speciális mechanizmus szükséges annak érdekében, hogy képesek legyünk azonosítani az elemet, melyhez aktuális az adott MN kapcsolódva van. Egy lehetséges megoldás, hogy a HA-t minden hálózatba lemásoljuk és anycast-et használva irányítjuk a csomagot az MN-hez legközelebbi HA-hez.

Egy teljesen elosztott környezetben, a routing és az MA-k vezérlési funkciója az AR-re hárulhat. Ha egy MN csatlakozik egy MA-hoz és létrehoz egy IP kapcsolatot a CN-nel, akkor a fogalom az MA-n keresztül fog haladni. A handoverhez kapcsolódó vezérlési üzenetek a régi és az új MA között osztódnak meg. A régi MA az MN új helyére küldi a csomagokat, ami azt jelenti, hogy az adatsík is elosztott. Viszont a kontroll üzenetek célcímét meg kell találni.

P2P megközelítés

Először megkeresi, hogy kihez kapcsolódik aktuálisan az MN. Ehhez segítség lehet egy elosztott hash tábla (Distributed Hash Table, DHT) karbantartása. Bár, ahogy az MA-k száma növekszik, és ahogy egyre több hop kerül bele a táblába, már a keresési időt sem lehet figyelmen kívül hagyni.

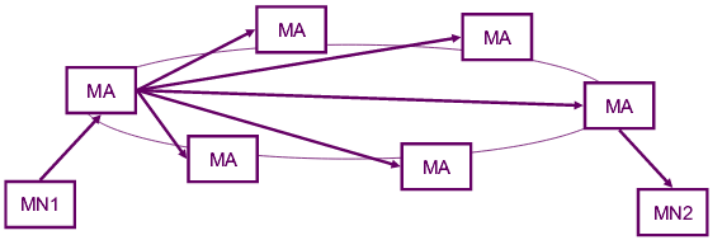


15. ábra P2P megközelítés [19]

Összességében, mikor az MN egy új hálózatba érkezik, a helyinformációkat frissíteni kell. Ezeket az információkat viszont el kell terjeszteni, ami többlet jelzésüzenetekkel jár, de ez nem befolyásolja az MN adatküldéseit.

Broadcast, multicast megközelítés

Minden csomagot minden MA (vagy MA csoportja) meg fog kapni, és az az MA fogja továbbítani a csomagot az MN-nek, akinél aktuálisan van.

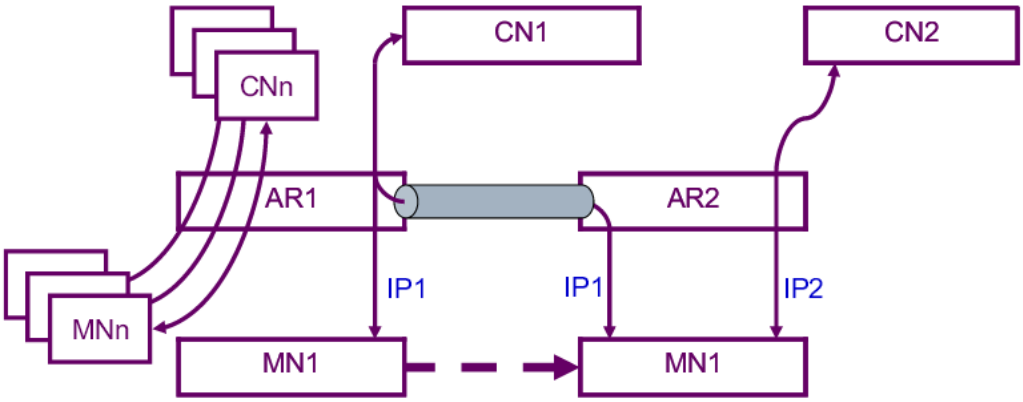


16. ábra Broadcast,multicast megközelítés [20]

Nem igényel MA keresési algoritmust és a nem igényel jelzés üzeneteket az MN mozgásával kapcsolatban. Viszont nem hatékony a hálózat terhelése szempontjából. Csak relative kis területeken érdemes használni.

Dinamikus mobilitás kezelés

A dinamikus mobilitás-kezelés célja, hogy csak akkor biztosítsunk mobilitást, amikor szükséges és csak azoknak az alkalmazásoknak, melyeknek szükséges is. Ezzel lehetséges csökkenteni a jelzésüzenetek számát, a hálózat terhelését. Hacsaknem egy mobil végberendezés valóban statikus IP-t használ, sok alkalmazásnak a handover után igazából nincs is szüksége mobilitás kezelése.



17. ábra DMM esetanulmány [18]

Az MN1 megkapja az IP1 címet a helyi routertől (AR1). Amikor az MN1 mozgása végett csatlakozik az AR2 hálózatához szintén kapni fog egy IP címet (IP2). Ezek után, azok IP folyamok, melyeket az IP1 címmel inicializált, tunnelezve lesznek az AR1 felé, viszont az aktuális hálózathoz tartozó folyamok, tehát, melyek az IP2 címet használják, azok normális routingban vesznek részt.

DMM PMIPv6 esetében [3]

A DMM célja, hogy túllépjünk a centralizált mobilitás-kezelés korlátain. Alapelve, hogy magát a mobilitás-kezelést (pl LMA) minél közelebb hozzuk a mobil végberendezéshez.

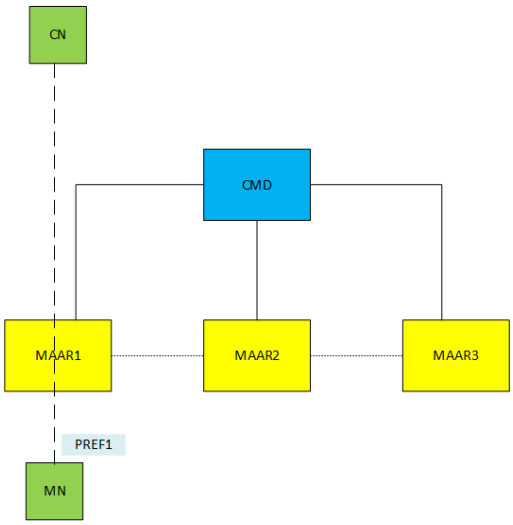
Két különböző elképzelés létezik az elosztottság bevezetésére:

- Részlegesen elosztott, mikor csak az adatsík van elosztottan megvalósítva
- Teljesen elosztott, mikor mind az adatsík, mind a vezérlősík is elosztott.

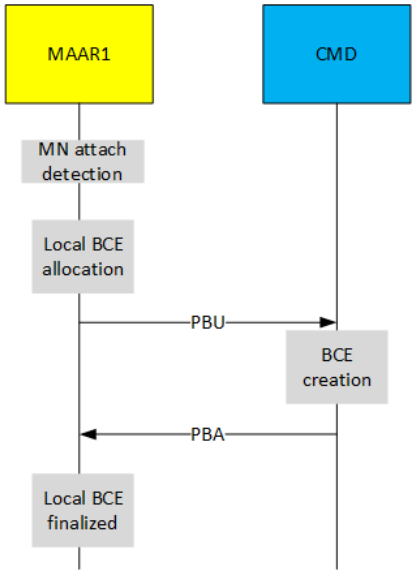
Részlegesen elosztott eset

Az LMA-t megfosztjuk az adattovábbítási feladattól és csak a gyakorlatilag Binding Cache (BC) kezelését végzi. Az így létrejövő elemet Central Mobility Datebase (CMD) kapja. Feladata továbbá a PBU és PBA üzenetek feldolgozása.

A MAG-t kiegészítjük az LMA funkcionalitásával: létrejön a Mobilty Anchor and Access Router (MAAR). A MAAR egy helyi BC-t is fenntart továbbá szintén feladata a PBU,PBA üzenetek kezelése. A MAAR tipikusan a hálózat szélén helyezkedik el, akár az alapértelmezett átjárón. Minden MAAR rendelkezik egyedi, MN-ek számára fenntartott prefixekkel és egy prefix csak egy MAAR-n jelenhet csak meg. Ha egy MAAR azt érzékeli, hogy egy MN csatlakozni akar vagy el akarja hagyni öt, akkor a CMD-hez fordul a helyzetinformációk frissítése végett (PBU és PBA üzenetekkel) .



18. ábra MN első csatlakozás, adatfolyam



19. ábra MN első csatlakozás folyamatábra

Teljesen elosztott megoldás

Az előbb ismertetett rendszer nem teljesen elosztottan viselkedik; a CMD még egy szerves központi elem. Viszont ezen megközelítésnek kezelnie kell a többi MAAR és az álaluk hirdetett prefixek ismeretlenségét. Különösen fontos ismerni egy MN P-MAAR listáját és a hozzájuk tartozó prefixeket.

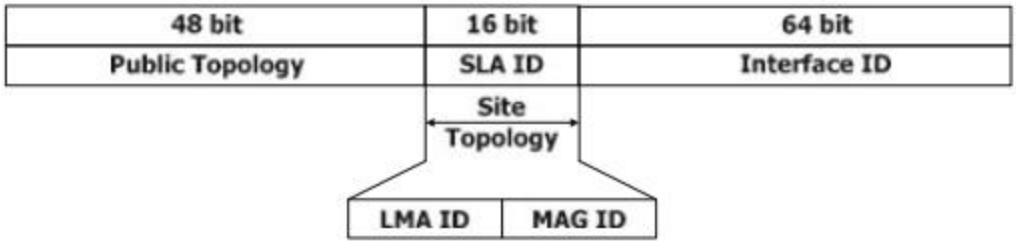
Az alábbi módok tudnak segíteni ezen:

- különböző második és harmadik rétegbeli technikákkal felderíteni, hogy mi lehet a következő MAAR
- Peer-to-peer rendszer bevezetése a MAAR-ok között
- MN ténylegesen elküldi a kívánt információkat az új MAAR-nak (pl ND)
- új protokoll kifejlesztése az MN és a MAAR között (pl 802,11)

Dinamikus megoldás[25]

Abban az esetben, ha csak akkor van mobilitás-kezelés, ha egy új MAG-hoz kerül az MN, akkor dinamikus mobilitás kezelésről beszélünk. A DM (dynamic mobility) képes csökkenteni az alagutazással kapcsolatos többlet terhelést azoknál az MN-knél akik ritkábban mozognak és az idejük nagy részét üresjáratban töltik. A centralizált PMIPv6 folyamatosan használ alagutazást, még akkor is, ha a MN már hosszú ideje nincs mozgásban. Az aktuális LMA-nak azonosítania kell azokat a csomagokat, melyeket a tunneleken keresztül kell elküldeni.

Minden LMA rendelkezik egy egyedi prefix halmazzal. Az aktuális LMA egyedi prefixeinek a halmazát elküldjük minden MAG-nak azért, hogy normál IP routing szerint küldjék el neki a MAG-k a csomagokat, melyek az adott perfixekről indulnak. Továbbá, hogy fenntartsanak egy olyan adatbázis, amiben minden LMA minden prefixe benne van, akik az azonos tartományban helyezkednek el velük. A MAG igy meg tudja találni, hogy ki a célállomáshoz tartozó H-LMA, aki felé a csomagokat kell irányítani.



20. ábra Prefix struktúra dinamikus PMIPv6 számára[24]

Be kell vezetni egy új azonositót (SLA ID), mely két részről áll: LMA ID és MAG ID. Ez az azonosító része lesz az IPv6os címeknek, melyeket a dinamikus mobilitás kezelésben használunk. Ahogy a MAG ID valójában egy LMA ID részhalmaza, emaitt a csomagot

alagutazás nélkül lehet elküldeni az MN-hez, hisz az ID-ban benne van, hogy ki az az LMA, aki vele egy tartományban van,

A DM hierarchikus prefixek halmazát használja, hogy kiderítse a célállomás helyzetét. Az MN több prefixet is igényelhet, ha új MAG-hoz érkezik. Feltételezzük, hogy az MN-nek van egy globális HoA-ja. Amikor az MN csatlakozik egy új MAG-hoz, egy új CoA-t fog használni az új kapcsolatokhoz. Ha az MN a korábbi MAG-ról egy új MAG-ra vándorol, akkor a meglévő kapcsolatai egy alagúton keresztül jutnak el hozzá. Az új kapcsolatok inicializálásakor normál IP routing szerint jár már el.

Architekturális kérdések PMIPv6 alapú dinamikus, folyam felbontású mobilitás kezelés kapcsán, 4G LTE/EPC hálózatokban

Dinamikus mobilitás kezelés alatt gyakorlatilag azt a folyamatot értjük, mely ténylegesen eldönti, hogy egy adott IP folyam igényli-e a mobilitás kezelést vagy sem. Az EPC hálózatban több olyan elem tálalható, mely elviekben képes lehet a folyamat futtatására és őt megfelelő információkkal való ellátására: ANDSF, MME, PCRF/PCEF.

Mobility Management Entity (MME)

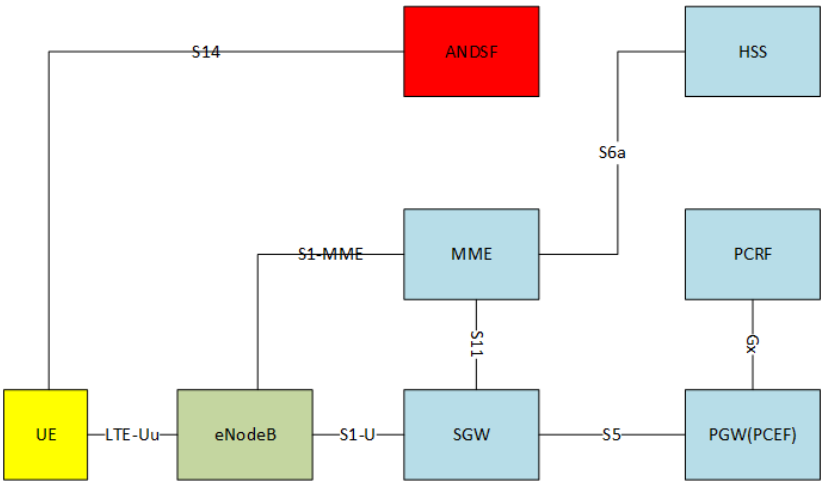
Az MME kezeli az EPC E-UTRAN hálózathoz és biztonsághoz (AAA) kapcsolódó jelzésüzeneteket. Feladatai közé tartozik még tovább az UE mozgásának követése és a paging alvó állapotban. A Non Access Stratum (NAS) végeztetési pontja egyben.

Policy and Charging rules Function / Policy and Charging Enforcement Function (PCRF/PCEF)

A PCRF feladatai közé tartozik az előfizetőkkel kapcsolatos szabályrendszerek nyilvántartása. Társa a PCEF, mely tipikusan a PGW egy része, ami kikényszeríti, végrehajtja ezeket a szabályokat. Képes a felhasználók egy csoportjára, de akár egy falhasználóra is szabályokat definiálni. Segítségével lehet a forgalmat „police”-olni vagy „shape”-elni, vagy bizonyos forgalmakat szűrni is akár. A dolgozat további fejezeteiben a PCRF-et egy egységként fogom kezelni, nem térek ki a belső, több entitásból álló felépítésére.

Access Network Discovery and Selection Function (ANDSF)

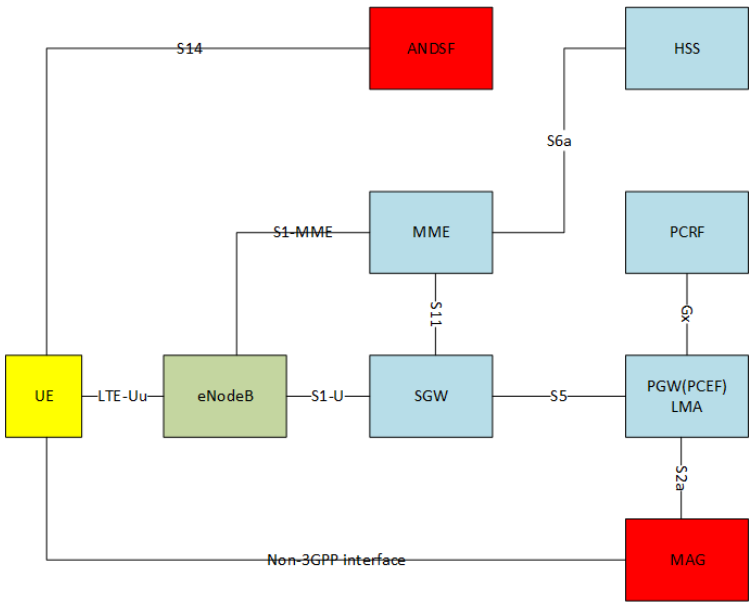
Új elemként került be a meglévő EPC hálózatba. Egy új interfészt definiál (S14) a mobil végberendezés és a hálózat közé. Az S14 interfészen, az OMA DM (Open Mobile Aliance – Device Management) protokoll segítségével képes direkt üzeneteket eljuttatni a mobil terminálhoz. Az ANDSF mind adat, mind vezérlősík elemeket tartalmaz, hogy segítsen az aktuális (mobil végberendezéshez közeli) hálózatok felderítésében, figyelembe vége a definiált operátor preferenciákat. Az aktuális rádiós adatokból (3GPP és non-3GPP hálózatokon is) képes eldönteni, hogy rádiós szempontból lehetséges-e a különböző hozzáférési technikák közötti hálózatváltás.



21. ábra ANDSF elemmel kiegészített architektúra

Architektúrajavaslat PMIPv6 alapú dinamikus, folyam szintű mobilitás-kezeléshez

A PMIPv6, mint protokoll az egyik megoldás a non-3GPP hálózatok EPC hálózatokhoz való kapcsolódására. Ehhez egy új interfész került definiálásra: S2a. Így már lehetővé válik több kapcsolat egyidejű fenntartása az EPC felé, a különböző hozzáférési technikákon keresztül.



22. ábra PMIPv6 az EPC-ben

A PGW-n minden forgalom keresztülmegy, függetlenül attól, hogy melyik hozzáférési technikán érkezett be. Ez megteremti a lehetőséget, hogy a PCRF segítségével bármilyen eredetű forgalomra szabályrendszereket tudjunk definiálni. Figyelembe véve a végcélt, hogy az IP

folyamokra külön-külön döntéssekkel hozott forgalomirányítást szeretnénk végrehajtani, az ezekhez kapcsoló szabályrendszert érdemes lehet a PCRF-ben tárolni. További előnye ennek a megoldásnak, hogy már alapvetően az egyes UE-kra érvényes forgalomkorlátozási beállítások is itt szerepelnek.

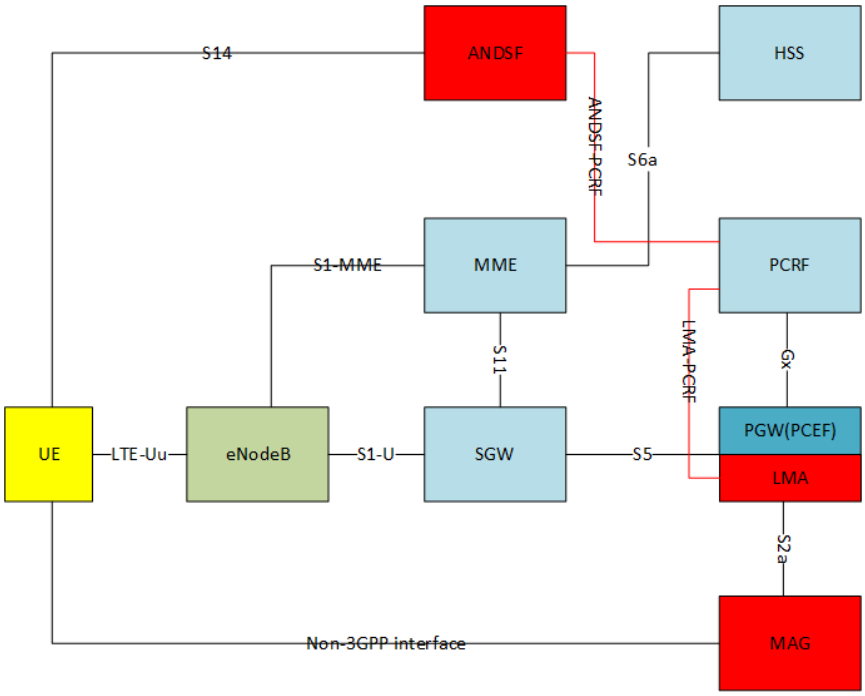
Dinamikus mobilitás-kezelés kapcsán a fő cél leginkább a 3GPP hálózat terhelésének a csökkentése, mintsem a lefedettség növelése, így azzal a feltételezéssel élek, hogy a 3GPP kapcsolat folyamatosan rendelkezésre áll, és csak a non-3GPP hálózatok megjelenésével / eltűnésével kapcsolatos problémákat vizsgálom meg. Ahogy a korábbi irodalmak is említik, a folyam alapú mobilitás kezeléshez már szükség van mobil végberendezési interakciókra. A PCRF-ben definiált szabályhalmazokat le kell juttatni a mobilhoz, melynek képesnek kell lennie ezeket alkalmaznia. Az alkalmazásnak a meglátásom szerint tűzfalszabályokat és a hozzá kapcsolódó policy routing (PBR, Policy Based Routing) szabályokat kell kezelnie, melyeket az S14-es interfészen ANDSF üzenetek formájában kaphat meg legegyszerűbben.

Linux kliens esetén ez azt jelenti, hogy Netfilter szabályokat fog az MN felvenni a Mangle nevű táblában. A Mangle tábla képes azonosítani az egyes forgalmakat, és különböző FWMARK (Forwarding Mark) értékeket rendel az egyes folyamokhoz. A jelölt csomagokat a megfelelő routing táblához lehet küldeni, ahol már az alapértelmezett útvonal a kapott szabályrendszer szerint lehet a 3GPP vagy a non-3GPP interfész. Így bármilyen forgalom, ami a kapott szabályrendszerekre illeszkedik, a megfelelő interfészen kerül továbbításra. A Netfilter keretrendszer alkalmazásának az előnye, hogy 5-tuple alapon, de akár a különböző forgalmi osztályok (ToS) szerint is lehet szabályokat alkotni.

Új, non-3GPP kapcsolat kialakítása során az LMA a kapott PBU alapján engedélyezést kérhet a PCRF-től, hogy az adott kérelmet elfogadja-e, vagy sem. Ezen kommunikációhoz viszont szükséges egy új interfész definiálása az LMA-PCRF viszonylatban. Ha a PCRF elfogadta a csatlakozási igényt, akkor a beállításokat le kell küldeni az UE-hez (UE-n futó alkalmazásnak).

Az LMA hatásköréből kikerül az a döntés, hogy egy adott PBU-ra válaszolhat-e. Minden döntés esetén a PCRF-hez fog fordulni. A PCRF lesz gyakorlatilag a hálózat alapú dinamikus mobilitás kezelés központja, a döntések meghozójaAz LMA-na nem tartja számon, hogy a különböző folyamaok, akár egy, ugyanazon MN-ról származnak. Így az LMA ezen része módositás nélkül alkalmazható az új architektúrában.

Mivel a PCRF az ANDSF-en keresztül éri el a mobil végberendezést, ezért definiálni kell egy ANDSF-PCRF interfészt is. A különböző authentikációs mechanizmusok megkönnyítése miatt érdemes egy PGW-HSS (AAA) interfészt is definiálni, de ezen interfész kifejtése nem része a dolgozatnak.

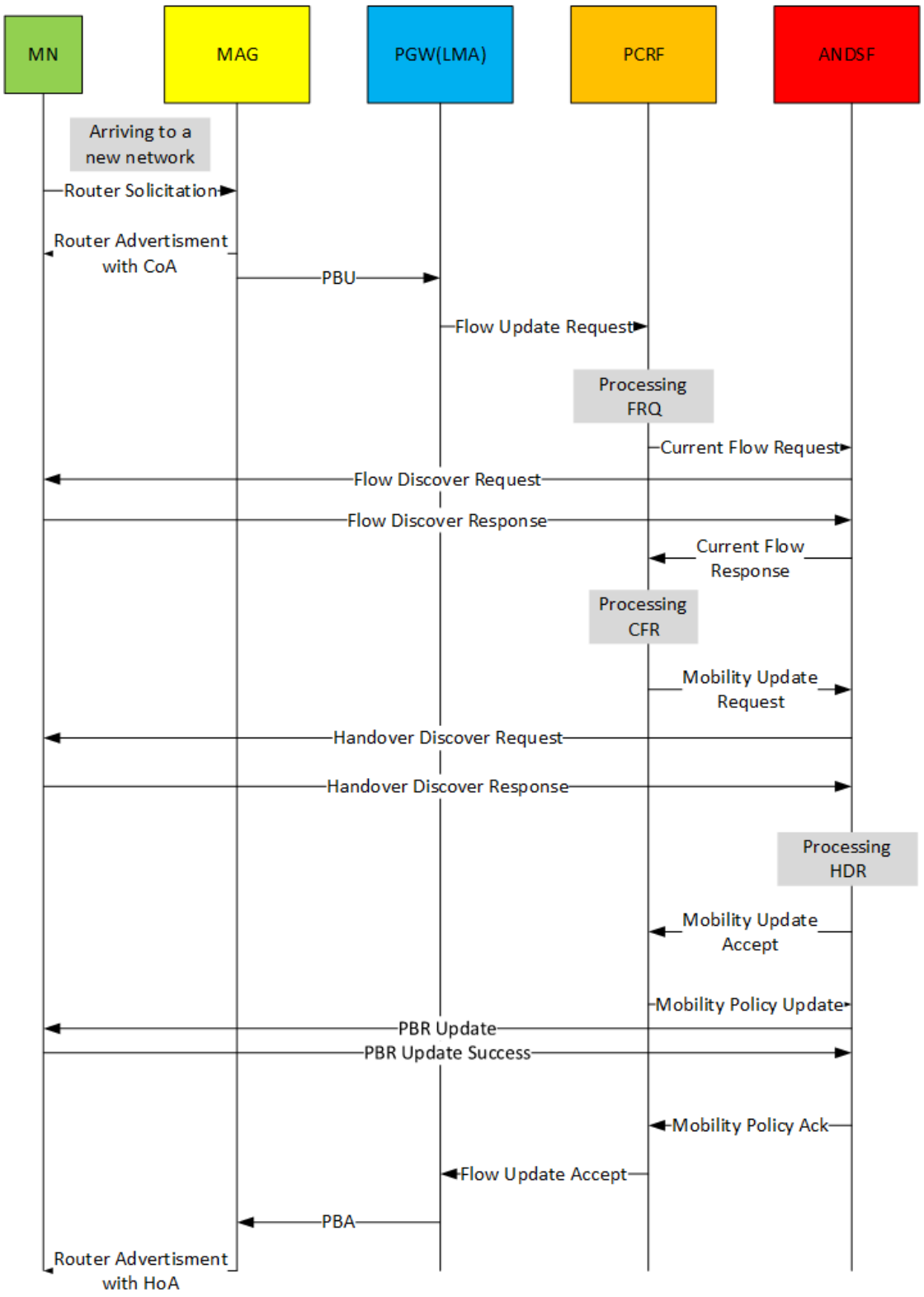


23. ábra Az új interfészekkel kiegészített, javasolt architektúra

Mobilitást igénylő folyam kezelése

Ha az MN egy (új) WLAN hálózathoz érkezik, akkor egy Router Solititation üzenetet fog kiküldeni a kapcsolódó interfészén. A kapcsolathoz tartozó MAG, ezt az üzenetet érzékelve az LMA irányába egy PBU üzenetet fog küldeni, párhuzamosan allokál egy Router Advertisment üzenettel egy IPv6 címet (CoA), az aktuális kapcsolatoz. Az LMA egy Flow Update Request üzenettel a PCRF felé fordul, hogy elfogadhatja-e PBU-t egy PBA-vel. A PCRF ellenőrzi a saját adatbázisában, hogy a MN számára egyáltalán engedélyezett-e WLAN interfész használata, és ha igen, akkor milyen megkötésekkel. A PCRF egy Current Flow Information Request üzenet segítségével megkérdezi az ANDSF-et, hogy milyen aktuális folyamok vannak az MN . Az ANDSF egy Flow Discover Request üzenettel az MN-hez fordul, hogy aktuálisan milyen kapcsolatokat tart fent. A Flow Discover Response üzenetben érkezik az információ, ahol fel van

sorolva minden IP folyam, legalább 5-tupple formában. Az ANDSF a PCRF-nek elküldi az MN folyamjait egy Current Flow Information Response üzenetben. Ha a PCRF úgy ítéli meg, hogy van olyan folyam, melyet át lehet terelni egy másik (vagy az újonnan hatósugárba került) interfészre, akkor a PCRF az ANDSF felé fordul egy Mobility Update Request üzenettel. A Mobility Update Request üzenet hatására az ANDSF felszólítja a MN-t egy Handover Discover Request üzenettel, hogy szolgáltasson adatokat az aktuális rádiós állapotokról. A MN erre, egy Handover Discover Response üzenettel válaszol. Az ANDSF feldolgozza a beérkező adatokat és eldönti, hogy lehetséges-e az új interfész használata rádiós szempontból [23]. Ha lehetséges, akkor egy Mobility Update Accept üzenettel válaszol a PCRF-nek. A PCRF majd elküldi az ANDSF-nek az új PBR beállításokat egy Mobility Policy Update üzenetben. Az ANDSF leküldi az új PBR beállításokat az MN számára a PBR Update üzenetben. Ha sikeres, akkor visszaküld egy PBR Update Success üzenetet. Erre küld egy nyugtát (Mobility Policy Ack) az ANDSF a PCRF-nek. Abban az esetben, ha nincs olyan folyam, melyet aktuálisan mobilitásban kellene részesíteni, akkor egy alapértelmezett, az operator által előre definiált PBR beállításokat fog elküldeni a PCRF a mobilnak. A PCRF válaszolni fog az LMA-nak, hogy engedje be az adott interfészt a hálózatba (Flow Update Accept üzenet). Az LMA válaszol a MAG-nak egy PBA üzenettel. A MAG egy Router Advertisement üzenettel leküldi az LMA által allokált, az interfészhez címet (Home Address).

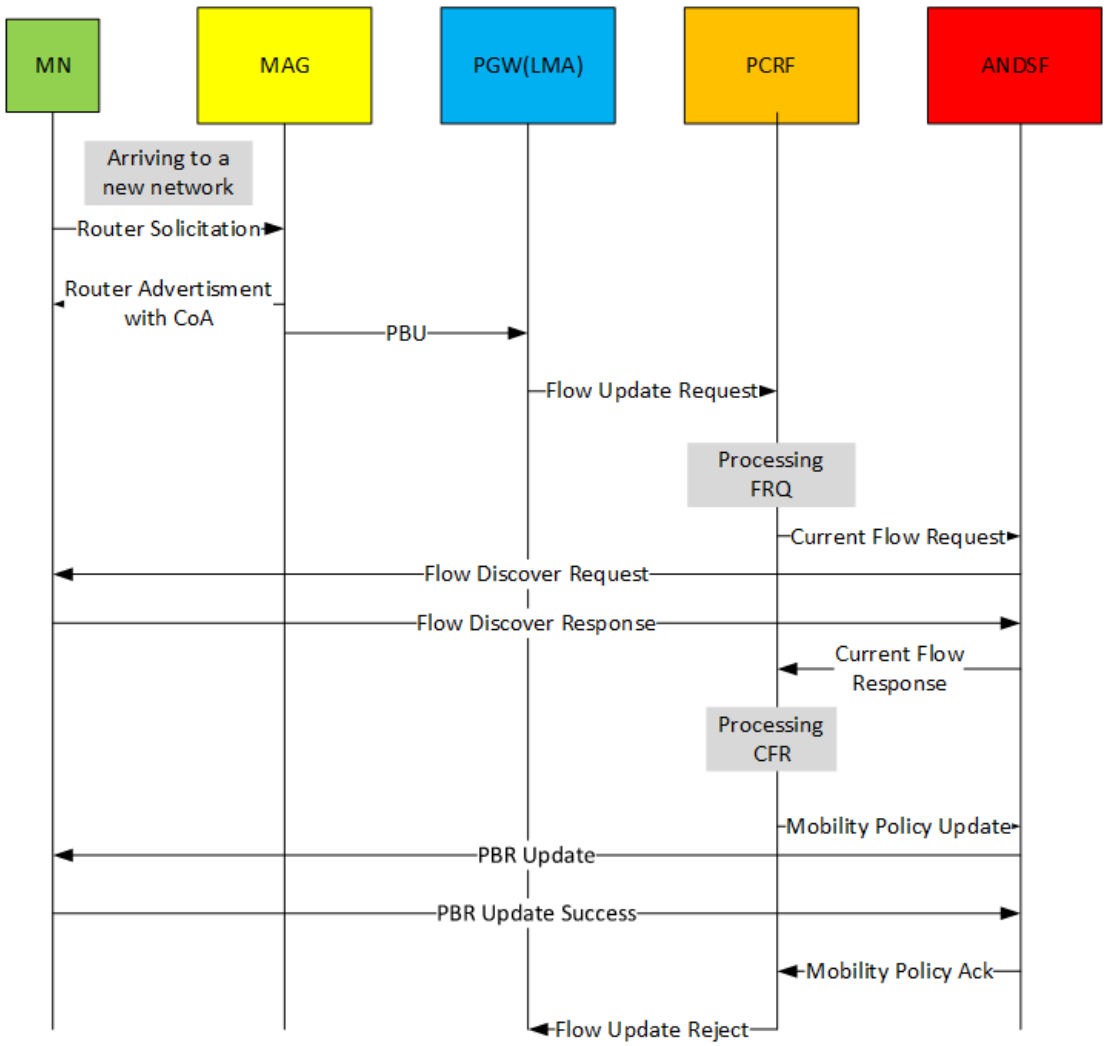


24. ábra Mobilitást igénylő folyam regisztrációja a javasolt sémában

Mobilitást nem igénylő folyam kezelése

Az MN az új hálózathoz való csatlakozást szintén egy Router Solicitation üzenettel kezdi. A MAG párhuzamosan kiküldi a PBU-t az LMA-nak és egy Router Advirtisment üzenetben egy IPv6-s címet allokál az MN-nak a köztük létrejövő hálózat használatára. Az LMA, amikor megkapja a PBU üzenetet a PCRF-hez fog fordulni egy Flow Update Request üzenettel. A PRCF ellenőrzi, hogy engedélyezett-e egyáltalán az új kapcsolat használata az MN számára, továbbá, esetleg milyen feltételekkel lehet használni. Ha engedélyezett, akkor az ANDSF-hez fordul egy Current Flow Information Request üzenettel, lekérdezve az aktuális MN folyamokat. (Ha nem engedélyezett, akkor már itt küldhet egy Flow Update Reject üzenetet.) Az ANDSF lekérdezi az aktuális folyamokat az MN-től, kiküldve egy Flow Discover Request üzenetet az MN-hez, mely Flow Discover Response üzenettel válaszol, tartalmazva az összes folyamot. Az ANDSF riportolja az eredményeket a PCRF-nek a Current Flow Information Response üzenetben, mely tartalmazza az összes folyamot. Ekkor, ha a PCRF úgy ítéli meg, hogy nincs szükség semmilyen folyam mobilitás-kezelésére, akkor nem fog válaszolni a PBU üzenetre. Így a MAG azt hiszi, hogy kvázi nem elérhető az LMA. Ennek hatására nem fog semmilyen intézkedést tenni a mobilitás kezelés végrehajtására és az MN-ről kiinduló folyamok a MAG routing táblája szerint lesznek továbbítva.

Viszont a PCRF el fog juttatni az MN-hez egy alapértelmezett PBR beállításokat tartalmazó üzenetsort, mely az alap, operator által definiált beállításokat tartalmazza. Ezt az ANDSF-nek küldött Mobility Policy Update üzenetbe teszi bele. Az ANDSF ezt a PBR Update üzenetén keresztül eljuttatja az MN-hez, mely egy PBR Update Success üzenettel válaszol, ha sikeres. Az ANDSF Mobility Policy Ack üzentet küld a PCRF-nek a sikeres PBR Update üzenetről. A PCRF Flow Update Reject üzenettel válaszol az LMA-nak, így ő nem fogja folytatni a megszokott PMIPv6 üzenetváltást.



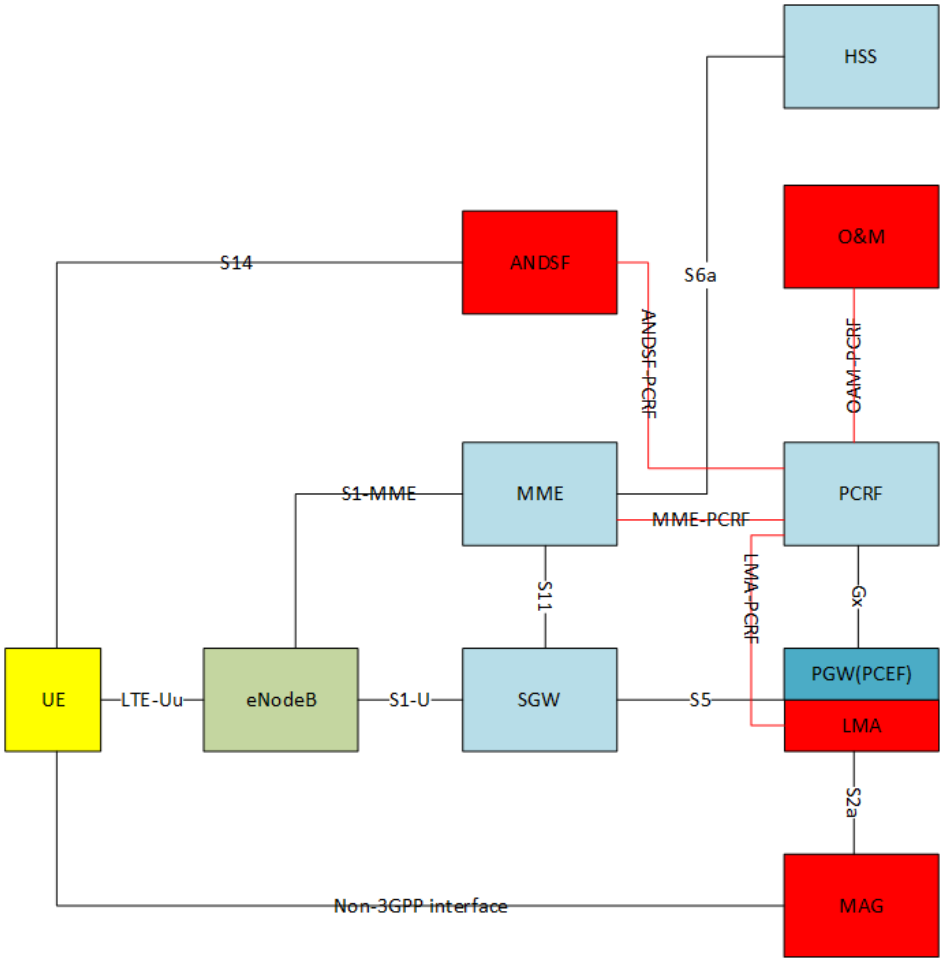
25. ábra Mobilitást nem igénylő folyam regisztrációja a javasolt sémában

Hálózat által inicializált mobilitás kezelés

A hálózat terheltségének folyamatos változása miatt szükséges lehet olyan eljárás definiálására, melynél a hálózat dönti el, a már (akár több interfésszel) csatlakozott MN folyamjainak elosztását (folyam alapú, hálózat központú offloading). Ilyen tipikus eset lehet, ha egy adott Tracking Area (TA) bázisállomásai vagy egy bizonyos bázisállomás (pl. sportesemény miatt) túlterheltté válik. A mobilhálózatok O&M rendszerei ezen mutatókat folyamatosan monitorozzák. A következőkben javasolni fogok egy lehetséges forgatókönyvet arra, ha a mobilhálózat valamely eleme, az eddigi megközelítésemet folytatva, a PCRF jelzést kap egy bázisállomás túlterheltségétől. Magát az O&M hálózatot (OSS/BSS) „fekete dobozként” kezelem, melyhez egy interfésszel csatlakozik a PCRF. Ezen az interfészen értesíti az O&M a

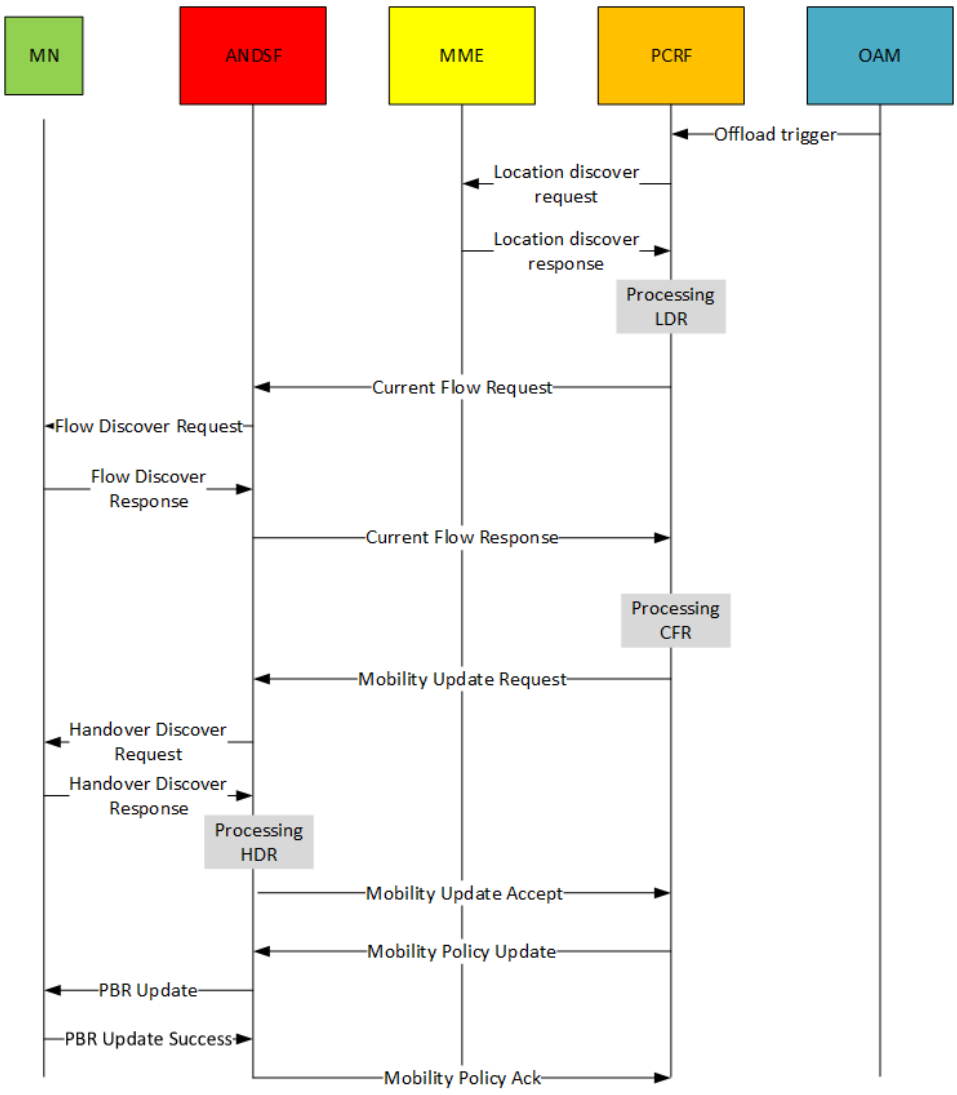
PCRF-et, ha egy TA bázisállomása túlterhelést jelez és azonnali beavatkozást vár a SAE részéről.

Ez az interakció jelen esetben egy átterhelési eljárást jelent, mikor megvizsgálja a PCRF, hogy mely UE-k, milyen folyamait lehet átterhelni a közeli WLAN hálózatra. A PCRF, mivel nem tárol lokációs adatokat, ezért az MME-hez fordul. Emiatt definiálni kell egy MME-PCRF interfészt. Az MME-vel szembeni új követelmény, hogy ezen az interfészen meg tudja válaszolni, hogy egy adott TA-hoz vagy eNodeB-hez milyen UE- kapcsolódnak és listaként elküldi ezt a PCRF-nek.



26. ábra OAM interfésszel kiegészített architektúrajavaslat

Az O&M hálózat felé nem küld nyugtát a PCRF az esetleges módosításokról, mert a terheléscsökkenésből számára nyilvánvaló lesz, hogy sikeres volt-e vagy sem. A UE-k folyamatos mozgása miatt, ha a PCRF-nek nem is sikerült átterheli megfelelő mennyiségű folyamot a WLAN hálózatokra, az újabb triggerek esetén is érdemes végrehajtani a procedúrát, hogy az esetleges újabb állapotokban már lehetséges-e.



27. ábra A javasolt hálózat által inicializált folyam-alapú mobilitás-kezelés

A PCRF az O&M hálózatból kapott értesítés után, mely tartalmaz egy bázisállomás azonosítót, egy Location Discover Request üzenetben fordul az MME-hez. Ebben az üzenetben kéri le, hogy egy adott eNodeB-hez aktuálisan milyen UE-k tartoznak. Az MME a Location Discover

Response üzenetben válaszol a MN-ek azonosítóival. A PCRF ezek után megvizsgálja, hogy van-e olyan UE, ami szerepel az adatbázisában, amik már korábban kapcsolódtak hozzá valamilyen non-3GPP hozzáférésen. Ha igen, akkor küld az ANDSF-nek egy Current Flow Information Request üzenetet, hogy az derítse ki, milyen folyamok vannak aktuálisan a MN-en. Current Flow Information Request üzenet ebben az esetben is hasznos lehet, hisz lehet, hogy vannak folyamok, melyek korábban nem voltak, de most érdemes lehet átterhelni. Ezek után az ANDSF felszólítja a mobil eszközt egy Flow Discover Request üzenetben az aktuális folyamjaira vonatkozó információk elküldésére. Erre a mobil egy Flow Discover Response üzenetben fog válaszolni. Az ANDSF a PCRF-nek ezt a listát elküldi a Current Flow Information Response üzenetben. A PCRF feldolgozza és eldönti, hogy van-e alkalmas folyam az aktuális állapotok szerint, amit érdemes lenne átterhelni. Ha igen, akkor egy Mobility Update Request üzenetet küld az ANDSF-nek, melynek hatására az ANDSF mérést kezdeményez a MN-n, egy Handover Discover Reqestben, hogy eldönthesse, hogy rádiós szempontból van-e valami akadálya [23]. Az MN egy Handover Discover Response üzenetben válaszol az ANDSF-nek, aki az üzenet feldolgozása után megállapítja, hogy lehetséges-e a handover. Ha igen, akkor Mobility Update Access üzenetet küld vissza a PCRF-nek. A PCRF ezek után kezdeményezi az új PBR beállítások lejuttatását a mobil végberendezéshez egy Mobility Policy Update üzenettel az ANDSF felé. A PRB beállításokat továbbküldi az ANDSF a mobil terminálhoz a PBR Update üzenet segítségével. Sikeresség esetén a MN válaszol egy PBR Update Success üzenettel az ANDSF-nek, aki az új PBR beállítások megtörténését a Mobility Policy Ack üzenetben tudatja a PCRF-fel.

Követelmények az alap PMIPv6 elemekkel szemben

MN szerepkörök

Az MN-nek az alábbi plusz funkciókra kell képesnek lennie, hogy részt vehessen a javasolt dinamikus folyam-alapú mobilitás kezelésben:

- S14 interfész implementálása
- Policy Based Routing
    - Új hálózat hatósugárba kerülése esetén nem használhatja addig az interfészt forgalom továbbítására, amíg erre nem kap engedélyt a hálózattól

LMA szerepkörök

Az LMA-nak azzal, hogy nem kell a külön a folyamkezeléssel törődnie, így csak a PCRF-LMA interfészen menő kommunikáció értelmezésére kell felkészíteni.

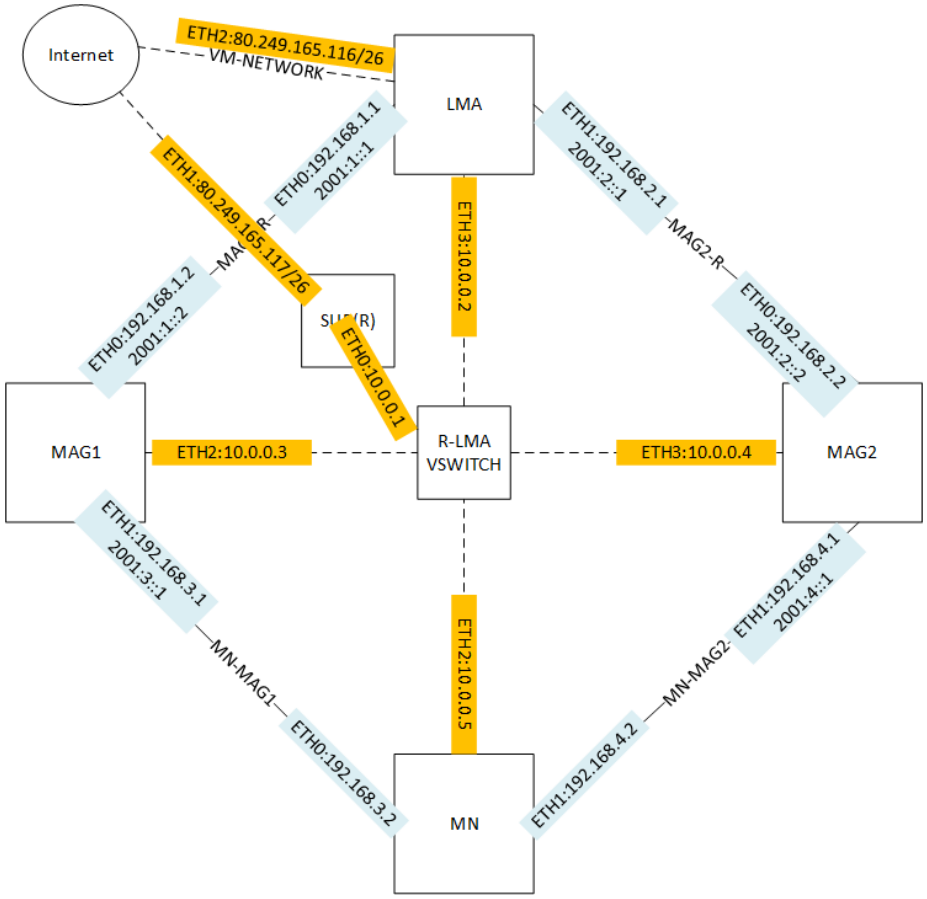
MAG szerepkörök

A MAG-t módosítás nélkül lehet használni az új architektúrában. Ami különbség lesz, hogy a MAG-n megnövekedhet a válasz nélküli PBU üzenetek száma, hisz ha egy folyamot nem kell mobilitás kezelésben részesíteni, akkor a MAG a kiküldött PBU-kra nem fog választ kapni. Így biztosítható a legkisebb architekturális beavatkozás.

Implementáció és mérési eredmények

A mérési tesztkörnyezet elkészítéséhez Vmware ESXi platformot használtam. Minden egyes virtuális gép egy mobilhálózati szerepkört tölt be, továbbá az LMA-n egy Radius szerver is fut. A Radius szerver segítségével MAC cím alapú authentikálás lehetséges a MN-k számára. Az egyes elemeket vSwitchel kötöttem össze. A hálózatban statikus routing van Policy Based Routinggal kiegészítve. A virtuális gépek Ubuntu 10.04 LTS rendszert futtatnak, 2.6-s Linux kernellel, melybe bele lettek fordítva a PMIPv6-tal kapcsolatos kernel modulok. A PBR-t az Iproute2 és a Netfilter modulok segítségével kezelem.

A PMIPv6 megvalósítását az Open Air Interface [22] nevű PMIPv6 implementációval valósítom meg.

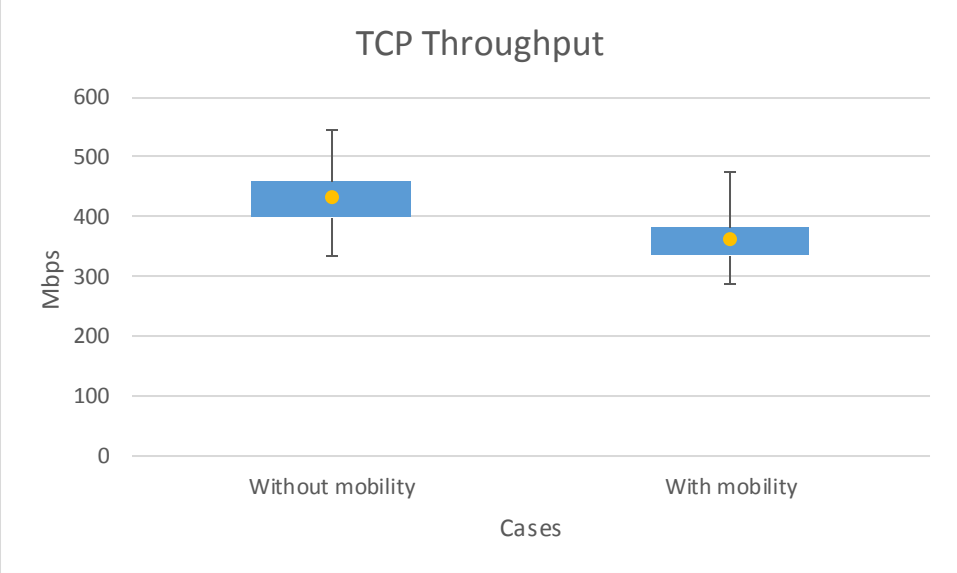


28. ábra A kialakított tesztkörnyezet

A tesztkörnyezet középpontjában egy olyan virtuális gép található, ami menedzsment szerepeket tölt be. Fő funkciója, hogy scriptjek segítségével [I.]lehet emulálni egy PBR beállításokat tartalmazó üzenet hatásait az S14-es logikai interfészen. Szintén ez a menedzsment csomópont vezérli az ESXi-nek közvetlenül kiadandó utasításokat (Perl script a hálózat átkonfigurálására, hálózatváltás létrehozására [II.]). A méréseket iPerf és D-ITG segítségével mértem, a scriptek megtalálhatók a függelékben.

A megvalósított tesztkörnyezet segítségével funkcionális és teljesítmény teszteket lehet végrehajtani, ha egy új hálózat hatókörébe érkezik az MN. Ilyenkor a két féle forgatókönyv szerinti viselkedés lehet vizsgálni: részesül-e mobilitás-kezelésben, illtetve, ha nem részesül egy adott hálózati folyam.

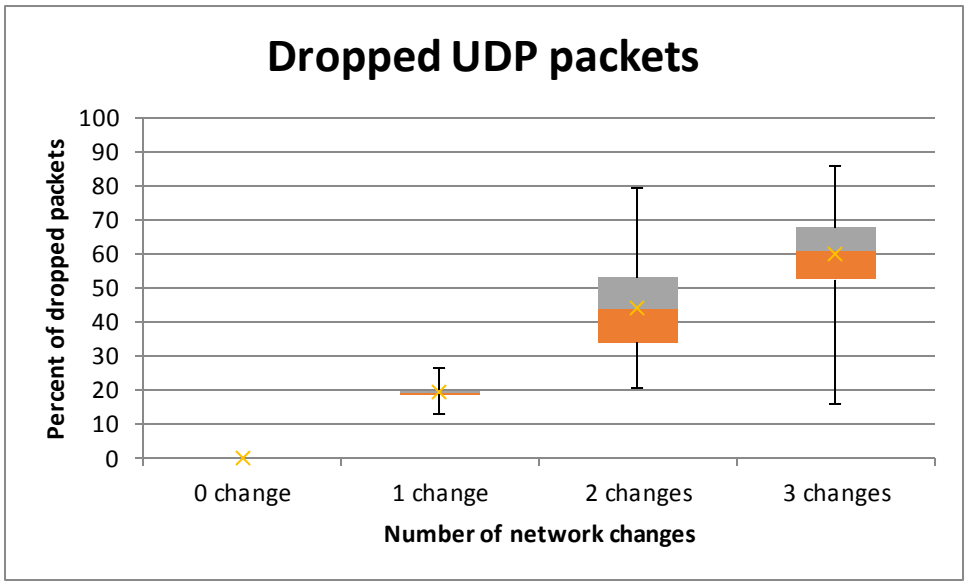
A TCP áteresztőképesség eredményeit az alábbi diagram szemlélteti (6. táblázat):



6. táblázat TCP áteresztőképesség

A különbségek abban rejlenek, hogy minden adatforgalmat alagutazásnak vetünk alá, így csökken az áteresztőképesség a megnövekedett késleltetés és jitter, valamint a jelentős alagutazási terhelés miatt.

UDP esetén azt vizsgáltam, ha egy folyamot (60 sec időtartamú) a hálózatváltások során mobilitás-kezelésben részesül, akkor hogyan változik a csomagvesztési arány (7. táblázat).



7. táblázat UDP csomagvesztési arány

A dinamikus mobilitás-kezelés további előnye, hogy a jelzésüzenetek száma csökkeni fog, hisz kevesebb PBU/PBA páros utazik a hálózatban, mind a csatlakozásnál, mind a lebontásnál. Továbbá az egyes elemekben csökken az alagutazás miatti többlet kapacitásigény, ha nem kell minden folyamhoz és/vagy MN-hoz alkalmazni a mobilitás-kezelési funkciókat.

Összefoglalás

A folyamatosan növekvő adatforgalom kezelésének egyik lehetséges módja a dinamikus (IP alapú) mobilitás-kezelés.

A PCRF-et tekintem központi elemnek, mely képes a dinamikus mobilitás kezeléssel kapcsolatos feladatok ellátására. A javaslataim között helyet kapnak új interfészek a 3GPP EPC hálózatban (MME-PCRF, PCRF-LMA, PCRF-OAM, PCRF-ANDSF). Ezeken az interfészeken több új üzenetet kellett bevezetni, ahhoz, hogy a PCRF az aktuális folyamokról egy teljes képet kaphasson, birtokában legyen a döntéseit megalapozó információknak.

A mérési eredményekből is látszik, hogy magának a mobilitás-kezelésnek is vannak korlátai, mégpedig a hálózatváltások növekvő gyakoriságának eredményeképpen. Meglátásom szerint az egyik javítási lehetőség az lenne, ha már az MN mozgásának becslése alapján előre ki lehetne számolni a lehetséges új kapcsolódási pontokat. Így már egy előre „elkészített" környezet várhatná a mobil eszközt (pl. már a tunnelek készen lennének).

További méréseket és elemzéseket igényelne, hogy melyek azok a folyamok, amiket mindenképpen mobilitás kezelésben kell részesíteni; ajánlásokat adni a speciális folyamok kezelésére: VoIP, videokonferencia. Fel lehetne mérni azokat a helyzeteket, mikor újonnan inicializált folyamokról beszélünk. Ezekben az esetekben döntési pont, hogy melyik interfészen indítsuk el. Kutatási terület lehetne ezen a téren különböző döntési algoritmusok keresése, melyek képesek eldönteni az egyes folyamokat merre küldje. Továbbá ezen algoritmusok, hogyan segíthetnének a hálózat tehermentesítésében.

A dinamikus és folyam-alapú mobilitás kezelés mindenképpen egy új irány a hálózatok evolúciójában, melyet az elosztott mobilitás kezeléssel kombinálva egy lehetséges jó választ adhatunk a jelenlegi adatforgalmi problémák megoldására.

Hivatkozások

[1]. D. Johnson,C. Perkins, J. Arkko: RFC 3775: Mobility Support in IPv6

[2]. S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil: RFC 5213: Proxy Mobile IPv6

[3]. CJ. Bernardos, A. de la Oliva,F. Giust: A PMIPv6-based solution for Distributed Mobility Management (draft-bernardos-dmm-pmip-03)

[4]. G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, K. Kuladinithi: RFC 5648: Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support

[5]. Mobile IPv6 Support for Dual Stack Hosts and Routers: RFC 5555: H. Soliman

[6]. CJ. Bernardos: Proxy Mobile IPv6 Extensions to Support Flow Mobility (draft-ietf-netext-pmipv6-flowmob-11)

[7]. RAJIV GUPTA, NUPUR RASTOGI: LTE ADVANCED – LIPA AND SIPTO

[8]. 3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 12) 3GPP TS 24.312 V12.6.1

[9]. MAPCON: http://blog.3g4g.co.uk/2011/01/mapcon-multi-access-pdn-connectivity.html

[10]. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network based IP flow mobility (Release 13) 3GPP TR 23.861 V1.9.1 (2014-07)

[11]. 3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 12) 3GPP TS 24.312 V12.6.1

[12]. H Anthony Chan,Hidetoshi Yokota,Jiang Xie, Pierrick Seite, Dapeng Liu: Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues

[13]. Mobile Traffic Offload "NEC's Cloud Centric Approach to Future Mobile Networks"

[14]. Alper Yegin: 3GPP CSIPTO prezentáció

[15]. 3GPP TR 22.828 V13.0.0 (2014-06) 3rd Generation Partnership Project;Technical Specification Group Services and System Aspects; Study on co-ordinated Packet data network GateWay (PGW) Change for Selected IP Traffic Offload (CSIPTO) (Release 13)

[16]. C. Perkins: RFC 3220: IP Mobility Support for IPv4

[17]. H Anthony Chan,Hidetoshi Yokota,Jiang Xie, Pierrick Seite, Dapeng Liu: Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues: Figure 12. Control/data plane separation scenario with signaling (dashed line) in a centralized control plane and data traffic (solidline) in a distributed data plane.

[18]. H Anthony Chan,Hidetoshi Yokota,Jiang Xie, Pierrick Seite, Dapeng Liu: Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues:Figure 13. A dynamic mobility management scenario: network sessions initiated after MN1 has moved to a new network uses the new IP address (IP2) which it acquires from the new network.

[19]. H Anthony Chan,Hidetoshi Yokota,Jiang Xie, Pierrick Seite, Dapeng Liu: Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues: Figure 14. P2P type of fully distributed mobility management with signaling traffic (dashed line) in a distributed control plane and data traffic (solid line) in a distributed data plane.

[20]. H Anthony Chan,Hidetoshi Yokota,Jiang Xie, Pierrick Seite, Dapeng Liu: Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues: Figure 15. Broadcast/Multicast type of fully distributed mobility management

[21]. SIPTO – LIPA Deployment: http://www.queryhome.com/26718/sipto-lipa-deployment-architecture

[22]. http://www.openairinterface.org/openairinterface-proxy-mobile-ipv6-oai-pmipv6

[23]. IEEE 802.21 MIH (Jee, Junghoon), IEEE802.21 WG Assistant Editor, IEEE802.21 MRPM SG Secretary, http://my.dreamwiz.com/junghoon, October 30, 2008

[24]. Youn-Hee Han, Doo-Soon Park, Weijia Jia, Sang-Soo Yeo: Ubiquitous Information Technologies and Applications: The proposed aggregatable global unicast address format in Dynamic Distributed PMIPv6

[25]. Youn-Hee Han, Doo-Soon Park, Weijia Jia, Sang-Soo Yeo: Ubiquitous Information Technologies and Applications:

[26]. Dr. Fazekas Péter: Mobil infokommunikációs rendszerek óravázlat 2012: http://www.mcl.hu/~fazek/mobil_infokom_oravazlat/15-18_eloadas_LTE_bevez%2bSAE%2bRIF.pdf

Ábrajegyzék

Röviditésjegyzék

AR: Access Router

BC: Binding Cache

BCE: Binding Cache entrty

CMD: Central Mobility Datebase

DMM: Distributed Mobility Management

HeNB: Home eNodeB

LMA: Local Mobility Ancor

MAAR: Mobilty Anchor and Access Router

MAG: Mobile Access Gateway

MME: Mobility Management Entity

MN: Mobile Node

MN-ID: Mobile Node ID

OAM: Operation and Management

PBA: Proxy Binding Acknolegment

PBU: Proxy Binding Update

PMIPv6: Proxy Mobile IPv6

P-MAAR: Previous MAAR

S-MAAR: Serving MAAR

TA: Tracking Area

Függelék

[I.] Példa egy PBR beállitásokat tartalmazó scriptre

```
#!/bin/bash
ip -6 route add default via fe80::250:56ff:fe8f:7b0b dev eth0 table link_udp
ip -6 route add default via fe80::250:56ff:fe8f:5b85 dev eth1 table link_tcp
ip6tables -A OUTPUT -t mangle -p udp -j MARK --set-mark 100
ip6tables -A OUTPUT -t mangle -p tcp -j MARK --set-mark 200
ip -6 rule add pri 20000 fwmark 100 table link_udp
ip -6 rule add pri 20001 fwmark 200 table link_tcp
```

[II.] Hálózatváltását segitó script:

```
#!/usr/bin/perl -w
Util::connect();
Util::disconnect();

my $network_name=
root@router:/home/router/vmwaretest# cat updateVMPortgroup.pl
#!/usr/bin/perl -w
##################################################################
# Author: William Lam
# Email: william2003[at]gmail[dot]com
# 06/06/2009
# http://www.engineering.ucsb.edu/~duonglt/vmware/
# Orignal code based off of: http://communities.vmware.com/message/840944#840944
##################################################################
use strict;
use warnings;
use VMware::VIRuntime;
use VMware::VILib;

my %opts = (
        'vmname' => {
        type => "=s",
        help => "The name of the virtual machine",
        required => 1,
        },
        'vnic' => {
        type => "=s",
        help => "vNIC Adapter # (e.g. 1,2,3,etc)",
        required => 1,
        },
        'portgroup' => {
        type => "=s",
        help => "Portgroup to add",
        required => 1,
        },
);
# validate options, and connect to the server
Opts::add_options(%opts);

# validate options, and connect to the server
Opts::parse();
Opts::validate();
Util::connect();

my $vnic_device;
my $vmname = Opts::get_option ('vmname');
my $vnic = Opts::get_option ('vnic');
my $portgroup = Opts::get_option ('portgroup');

my  $vm_view    =  Vim::find_entity_view  (view_type  =>  'VirtualMachine',  filter  =>{  'name'=>
$vmname});
```

```
if ($vm_view) {
        my $config_spec_operation = VirtualDeviceConfigSpecOperation->new('edit');
        my $devices = $vm_view->config->hardware->device;
        my $vnic_name = "Network adapter $vnic";

        foreach my $device (@$devices) {
                if ($device->deviceInfo->label eq $vnic_name){
                        $vnic_device=$device;
                }
        }
        if($vnic_device){
                $vnic_device->deviceInfo->summary($portgroup);
                $vnic_device->backing->deviceName($portgroup);
                my $vm_dev_spec = VirtualDeviceConfigSpec->new(device => $vnic_device,operation
=> $config_spec_operation);

                my $vmPortgroupChangespec = VirtualMachineConfigSpec->new(deviceChange => [
$vm_dev_spec ] );

                eval{
                        $vm_view->ReconfigVM(spec => $vmPortgroupChangespec);
                };
                if ($@) {
                        print "Reconfiguration of portgroup \"$portgroup\" failed.\n $@";
                }
                else {
                        $vm_view->update_view_data();
                        print "Reconfiguration of portgroup \"$portgroup\" successful for
\"$vmname\".\n";
                }
        } else {
                print "Unable to find $vnic_name\n";
        }
} else {
        Util::trace(0,"\nUnable to locate $vmname!\n");
        exit 0;
}

Util::disconnect();
```