Universidade de Aveiro
2007
Departamento de Electrónica, Telecomunicações e Informática

Nuno Gonçalo Martins Ferreira

Mobilidade Rápida Heterogénea em Arquitecturas de Redes de Próxima Geração

Universidade de Aveiro
2007
Departamento de Electrónica, Telecomunicações e Informática

Nuno Gonçalo Martins Ferreira

Mobilidade Rápida Heterogénea em Arquitecturas de Redes de Próxima Geração

Dissertação apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Engenharia de Computadores e Telemática, realizada sob a orientação científica do Professor Doutor Rui L. Aguiar, Docente do Departamento de Electrónica, Telecomunicações e Informática da Universidade de Aveiro

dedicatória

Para os meus pais que fizeram o maior esforço do mundo para que um dia eu fosse o que hoje sou.
Para as minhas irmãs.

o júri

presidente

Prof. Dr. José Carlos Neves
professor catedrático da Universidade de Aveiro

Prof. Dr. Rui Luís Andrade Aguiar
professor auxiliar da Universidade de Aveiro

Prof. Dr. Marília Pascoal Curado
professora auxiliar da Universidade de Coimbra

agradecimentos

Os sinceros agradecimentos a todos os membros dos Instituto de Telecomunicações pólo de Aveiro, em especial a todos os colegas e professores que me apoiarem durante o desenvolvimento do trabalho que deu origem a esta dissertação de mestrado.

palavras-chave

Mobilidade Rápida IPv6, Local-centric Mobility System (*LMS*), Mobilidade Localizada, Qualidade de Serviço (QoS), Desenvolvimento, Avaliação

resumo

Com o crescente aumento do impacto das redes móveis nas vidas dos cidadãos contemporâneos e a explícita necessidade de contacto com a Internet em qualquer lugar, torna-se fundamental encontrar alternativas e mecanismos viáveis que permitam dar resposta a estas necessidades. Assim, julga-se que a resposta passará naturalmente pela introdução do protocolo IP na estrutura lógica das redes de operador de forma a permitir que os terminais móveis possam aceder livremente a qualquer conteúdo e serviços em qualquer lugar e em qualquer momento. Contudo, o facto de integrar uma tecnologia protocolar IP numa rede móvel traz naturalmente sérios problemas visto que este nunca foi concebido para suportar mobilidade de endereçamento entre diferentes redes. Uma das actuais soluções mais proclamadas, e que é neste momento o "standard" para mobilidade IP, é o protocolo *Mobile IP*. Este protocolo, tanto na sua versão para IPv6 como para IPv4, suporta integralmente o conceito de mobilidade IP e permite que terminais móveis de próxima geração se possam movimentar livremente entre diferentes redes sem perderem as ligações existentes nesse momento. Contudo, o *Mobile IP* é um protocolo de compromisso, e como tal tem sérios impactos em alguns factores importantes tais como o tempo de handover, a perda de pacotes associada e o Jitter sofrido durante a transmissão dos mesmos. Assim, torna-se importante para os operadores de próxima geração encontrarem novas soluções que permitam suportar a mobilidade rápida de terminais móveis e também obter o menor impacto possível na sua estrutura de rede poupando recursos preciosos.

O trabalho realizado nesta dissertação consiste no estudo detalhado dos protocolos de mobilidade existentes actualmente, e como resultado desse estudo foi desenvolvido um novo conceito arquitectural e protocolar para ambientes de mobilidade rápida em redes móveis de próxima geração. O Local-centric Mobility System (*LMS*) surgiu como resposta a estes problemas e foi desenhado com base em conceitos de mobilidade rápida preditiva, micro-mobilidade, utilização de multicast para optimização do encaminhamento de pacotes, aplicação de segurança através de mecanismos criptográficos, serviços de controlo *AAAC* e por fim conceitos existentes nas redes celulares tais como o paging.

Como forma de comprovar cientificamente a exequibilidade deste novo conceito foi desenvolvido um protótipo completamente funcional onde se pôde testar o *LMS* em redes reais sobre condições diversas em ambiente de laboratório. Os resultados dos testes apresentados nesta dissertação comprovam a sua exequibilidade numa rede real mostrando que o *LMS* poderá ser um ponto inicial para novas descobertas no âmbito da integração da mobilidade IP. Por fim este estudo permitiu ainda a publicação de um artigo científico numa conferência internacional onde foi apresentado à comunidade.

keywords

Fast Mobility in IPv6, Local-centric Mobility System (*LMS*), Local Mobility, Quality of Service (QoS), Development, Evaluation

abstract

With the increasing impact of the mobile networks in the contemporaneous citizens and the current “Internet every where” phenomenon, it is fundamental to reach feasible mechanisms and solutions to handle this type of requirements. Thus, the research projects points the integration of *Internet Protocol* (IP) in the network operator structures as the possible solution for all of these needs. The integration of IP in the network operator structures will provide support of “Internet every where” and also other several services that, at now a days, does not exists. However, the integration of IP technology in the mobile operator networks will raise several problems since the *Internet Protocol* (IP) was not designed to support address mobility. The current standard solution for IP mobility is the *Mobile IP* protocol. This protocol allows the mobile terminals to move among the networks without breaking the network connections and established sessions. Nevertheless, the *Mobile IP* protocol implies blackout experiences and also some service disruption during the handoffs. These problems makes difficult to integrate the *Mobile IP* protocol in the next generation operator networks. Thus, new solutions for IP mobility in next generation networks are required in order to have seamless and fast handovers during the mobile terminal movements.

This master thesis consists in a deep study of current mobility protocols and, as result of this evaluation, a new mobility protocol and a next generation network architecture was architected, developed and evaluated. The developed mobility protocol, Local-centric Mobility System (*LMS*), was created in order solve the main mobility problems and also to have seamless integration with network operator agents such as *AAAC* (Access, Accounting, Authorization and Charging) servers. The *LMS* protocol supports Quality of Service (QoS), security based on cryptographic mechanism and also fast and seamless mobility. The *LMS* also supports paging and micro-mobility/local-mobility based on the cellular networks concepts.

In order to scientifically prove the feasibility of this novel approach, it was developed a complete functional prototype of Local-centric Mobility System (*LMS*) and it was tested in real conditions in real testbeds. The results of these tests prove that *LMS* could be able to support several mobile terminals under high mobility scenarios and also have seamless integration with network operator’s requirements. Finally this thesis also results in a scientific publication in an international conference where the *LMS* was presented to the scientific community.

Índice

Lista de Figuras

Lista de Tabelas

Acrónimos

2G	2nd Generation Mobile Networks
3G	3rd Generation Mobile Networks
4G	4G 4th Generation Mobile Networks
A4C	Authentication, Authorization, Accounting, Auditing and Charging
AAA	Authentication, Authorization and Accounting
AAAC	Authentication, Authorization, Accounting and Charging
ACK	Acknowledgement
AP	Access Point
AH	IP Authentication Header
AM	Aggregation Module
AN	Access Network
ANQoSB	Access Network QoS Broker
AP	Access Point
AR	Access Router
ARM	Advanced Router Mechanisms
BS	Base Station
BSC	Base Station Controllers
BU	Binding Update
CAN	Content Adaptation Node
CAR	Current Access Router
CARD	Candidate Access Router Discovery
CMS	Central Monitoring System
CN	Correspondent Node
CNQoSB	Core Network QoS Broker
CoA	Care of Address
COPS	Common Open Policy Service
CXT	Context Transfer
CXTP	Context Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name Service
DVB	Digital Video Broadcast
DVB-H	DVB Handhelds
DVB-S	DVB Satellite
DVB-T	DVB Terrestrial
ESP	Encapsulating Security Payload
EUI-64	IEEE Extended Unique Identifier for 64 bits
FBU	Fast Binding Update
FBack	Fast Binding Update Acknowledgement
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FHO	Fast Handover
FMIPv6	Fast Mobile IPv6

FNA	Fast Neighbor Advertisement
GUI	Graphical User Interface
HA	Home Agent
HAVAII	Handoff-Aware Wireless Internet Infrastructure
HIP	Host Identity Protocol
HI	Handover Initiate or Host ID
HIT	Host Identity Tag
HMIPv6	Hierarchical Mobile IPv6
HO	Handover
HoA	Home Address
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEEE	IEEE Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPng	Internet Protocol next gerenation
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPSec	Secure IP
L2	TCP/IP Model Layer 2
LAN	Local Area Network
LD	Local Domain
LM	Local Mobility
LMD	Local Mobility Domain
LMP	Local Mobility Protocol
LLA	Link Layer Address
MAC	Medium Access Control Address
MAG	Mobility Access Gateway
MAP	Mobility Anchor Point
MGEN	Multi Generator
MIP	Mobile IP
MIPv6	Mobile IPv6
MPLS	Multi Protocol Label Switching
MT	Mobile Terminal
MTRC	Mobile Terminal Remote Control
NAI	Network Access Identification
NAR	Next Access Router
nAR	New Access Router
NCoA	New CoA
OSI	Open System Interconnection
PAN	Personal Area Network
PAR	Previous Access Router
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PID	Personal Identification
PIM	Protocol Independent Multicast

PMIP	Proxy Mobile IP
PMIPv6	Proxy Mobile IPv6
QoS	Quality of Service
RtAdv	Router Advertisement
RtSol	Router Solicitation
SA	Security Association
SNR	Signal to Noise Ratio
SPI	SPI Security Parameter Index
SSID	Service Set Identifier
STA	Station
TAR	Target Access Router
TCP	Transmission Control Protocol
TD-CDMA	Time Division Code Division Multiple Access
TDM	Time Division Multiplexing
TLV	Type Length Value
UDP	User Datagram Protocol
VOD	Video on Demand
UMTS	Universal Mobile Telecommunication System
W-CDMA	Wideband Code Division Multiple Access
WLAN	Wireless Local Area Network

Capítulo I
Introdução

1.1 Motivação

As redes de próxima geração *(NGN – Next Generation Networks*) irão suportar grande parte dos terminais computacionais do futuro. Prevê-se que estas redes serão suportadas pelo protocolo de comunicações IP, mais concretamente pela sua versão 6 (seis), IPv6. Desta forma, tem vindo a mostrar-se extremamente interessante e importante o estudo da mobilidade em redes IP, em especial em redes IPv6. A mobilidade em redes IP ainda é palco de muita discussão, discórdia e ideias muito divergentes das quais vão nascendo dia após dia novos protocolos de extensão ou suporte à mobilidade IP. A dificuldade em encontrar um protocolo que responda eficazmente aos principais requisitos da mobilidade em redes de próxima geração transformou-se numa procura incansável que também enquadrou o trabalho descrito nesta dissertação de mestrado. Assim, procurou-se encontrar uma solução viável e exequível que integrasse um conjunto de funcionalidades vitais para as redes IP de próxima geração. De todos os requisitos poderá destacar-se a mobilidade rápida com *handovers* preditivos, micro-mobilidade ou mobilidade localizada, segurança e qualidade de serviço. Com o intuito de materializar esta solução, desenvolveu-se um novo protocolo, denominado *LMS – Local-centric Mobility System*, que pretende dar resposta a estes requisitos melhorando assim o estado actual da mobilidade IP em cenários de operador.

1.2 Redes Heterogéneas

A crescente proliferação de novas tecnologias de comunicação tem originado um ambiente de integração cada vez mais heterogéneo. O desenvolvimento de novos tipos de tecnologia de acesso ao meio em ambientes rádio, tais como *DVB (Digital Video Broadcasting)*, *UMTS (Universal Mobile Telecommunication System)* e *WIFI* torna cada vez mais possível a sua utilização em cenários de operador. Para que os utilizadores finais possam usufruir em pleno deste tipo de vantagens, os terminais de acesso terão obrigatoriamente que suportar múltiplas ligações e suporte para

diversos tipos de tecnologias de acesso. Este tipo de requisitos traduz-se no aumento da capacidade não só dos terminais mas também da estrutura da própria rede, implicando assim a necessidade de novas arquitectura e novos mecanismos protocolares que suportarão estas funcionalidades. Como tal, é imperativo que a redes de próxima geração empreguem mecanismos que suportem heterogeneidade de tecnologias de acesso permitindo que os utilizadores possam utilizar os seus terminais para receber a informação desejada da forma mais eficaz do ponto de vista económico e tecnológico. Por outro lado, a capacidade de utilização de novos processos de comunicação, por exemplo o *DVB*, permitirá aos operadores de telecomunicações explorarem novos nichos de mercado traduzindo-se assim num forte motivo para aplicação de recursos económicos e tecnológicos nos ambientes de comunicação heterogéneos.

Em suma, considerando o actual crescimento tecnológico e a tendência que os operadores de telecomunicações têm em explorar novos nichos de mercado, espera-se que as redes de próxima geração sejam tão heterogéneas quanto possível. Assim, considerando os requisitos apontados, torna-se indispensável que os protocolos de rede de próxima geração sejam tecnologicamente agnósticos permitindo assim uma maior margem de manobra e flexibilidade perante as circunstancias do futuro. O IPv6 surge neste contexto.

1.3 Internet Protocol versão 6 (IPv6)

As redes de próxima geração serão, muito provavelmente, suportadas pelo protocolo de rede Internet Protocol (IP) e comportarão um vasto leque de equipamentos que, por imposição dos próprios consumidores, estarão grande parte do seu tempo de vida ligados em constante comunicação na rede. Esta imposição, obrigará que o espaço de endereçamento IP seja igualmente grande por forma a suportar um tão elevado número de equipamentos na rede. O actual protocolo de rede IP, Internet Protocol versão 4 (IPv4) [3], contem um espaço de endereçamento de 32 (trinta e dois) bit o que lhe concede um total de 429,496,729,6 endereços que naturalmente não lhe permitirá cumprir este tipo de requisitos.

No início da década de 90 do século XX, alguns estudos apontavam que o espaço de endereçamento do IPv4 iria atingir o ponto de exaustão num futuro relativamente próximo. Desta forma, a necessidade de criar um novo protocolo sucessor do IPv4 surgiu impulsionado *pelo Internet Engineering Task Force* (IETF) e

originou a primeira definição para o Internet Protocol versão 6 (IPv6) [1] .O IPv6 é o sucessor do IPv4 e a sua maior vantagem relativamente IPv4 é o enorme espaço de endereçamento que este proporciona. O IPv6 estendeu o espaço de endereçamento de 32 (trinta e dois) bit para 128 (cento e vinte e oito) bit, o que representa efectivamente:

- 340,282,366,920,938,463,463,374,607,431,768,211,456 (endereços IP distintos)

Este enorme número de endereços disponíveis é ideal para suportar as redes de próxima geração que requerem um elevado número de terminais constantemente ligados na rede. Contudo, a arquitectura do IPv6 não se limitou a estender o espaço de endereçamento, também trouxe algumas inovações importantes que poderão tornar-se vitais para as redes do futuro. Uma das inovações agregadas ao desenho do IPv6 é a configuração automática dos terminais de rede. O processo de *Stateless Autoconfiguration* [4] permite que qualquer terminal de rede possa ser auto-configurado no momento em que se liga na mesma sem o uso de mecanismos activos tais como o *DHCPv6 (Dynamic Host Configuration Protocol)* [5].

De forma a aumentar a desempenho da rede, o desenho do IPv6 contemplou pacotes de tamanho muito elevado, denominados por *Jumbograms*. Ao contrário do IPv4 que apenas suporta 64KB de *payload* no IPv6 é possível transportar pacotes de tamanho bastante superior que podem atingir os 9000 KiB.

O suporte intrínseco para *Multicast* foi um ponto chave que garantirá um melhor suporte de aplicações multimédia nas redes de IPv6. Ao contrário do que aconteceu no IPv4, no IPv6 o suporte de *Multicast* é intrínseco e a estrutura hierárquica do endereçamento permite um melhor funcionamento do encaminhamento dos pacotes. A segurança das comunicações sobre o protocolo de rede IPv6 também foi assegurada desde o inicio do seu desenho. O *IPsec* tornou-se assim base do IPv6 garantindo confidencialidade, integridade, autenticação e não repudiação de todos os pacotes transmitidos. Para tal o *IPsec* serve-se dos protocolos *AH* [6] e *ESP* [7] para proporcionar garantias de segurança nos canais de comunicação entre os diferentes dispositivos de rede. Por fim, uma das maiores inovações do IPv6 foi a simplificação da mobilidade IP. Ao contrário do que acontecia anteriormente nos cenários IPv4, em cenários IPv6 não existem agentes estrangeiros (*Foreign Agents*) o que permite uma melhor optimização das rotas entre o terminal móvel (*Mobile Terminal - MT*) e o nós correspondente (*Correspondent Node – CN*). Estas inovações permitem que a mobilidade em IPv6 seja substancialmente mais robusta e eficaz que em redes IPv4.

Por todas as vantagens enumeradas anteriormente prevê-se que o IPv6 será o protocolo que sustentará as redes de próxima geração onde um largo espaço de endereçamento, segurança e suporte de mobilidade facilitarão o processo de integração em ambientes heterogéneos.

1.4 Mobilidade Rápida IPv6

Uma das grandes problemáticas das redes de comunicação do futuro é a relação entre o suporte de mobilidade e o número de utilizadores em movimento na rede em cada instante. Devido à rápida convergência entre os recursos tecnológicos e os serviços que potencialmente poderão ser prestados pelos operadores de telecomunicações, como por exemplo serviços multimédia, é crucial que a estrutura do sistema de comunicações permita uma adaptação constante às condições reais da rede em cada instante. O facto dos terminais serem recursos integrantes da rede e estarem potencialmente em movimento apresenta um enorme desafio, especialmente considerando que os serviços deverão ser sempre fornecidos com a qualidade de serviço acordada entre o operador e o cliente. Contudo, sempre que um terminal se move de um ponto de acesso para outro ponto de acesso, a rede tem que adaptar-se à nova posição do terminal reencaminhando os pacotes por diferentes troços de rede. Esta transição é tipicamente penosa e bastante complexa de conseguir em períodos reduzidos de tempo. Quando um terminal se move entre dois pontos de acesso distintos a falta de suavidade da transição em regra geral traduz-se num impacto directo na qualidade de serviço das comunicações activas no momento o que poderá romper com os contratos de serviço entre o utilizador e o operador de telecomunicações. No futuro, os utilizadores das redes de próxima geração poderão usufruir de serviços de tempo real tais como *VOD (Vídeo on Demand)* ou vídeo-telefonia, onde os requisitos de qualidade de serviço terão que ser obrigatoriamente respeitados para que o serviço de tempo real possa ser fornecido convenientemente. Desta forma, o processo de *handover* reactivo é completamente inaceitável pois o tempo de restabelecimento da ligação no novo ponto de acesso poderá levar várias centenas de milissegundos ou até mesmo segundos o que traduz-se numa degradação grave da qualidade de serviço prestada nesse momento.

A necessidade de fornecer transições entre pontos de acesso de forma suave, transparente e o com menor impacto possível nas ligações do utilizador torna-se um requisito crucial para o desenvolvimento das redes de próxima geração. A este processo atribui-se vulgarmente a designação *Seamless Handover* e este

tem-se tornado num ponto chave dos protocolos de mobilidade IP para redes do futuro. A tão desejada mobilidade suave e sem interrupções na comunicação dos terminais só pode ser conseguida através de mecanismos protocolares sofisticados que permitam tornar o processo de transição entre pontos de acesso praticamente indistinguível. Este tipo de procedimento é conseguido através de *handovers* preditivos onde o terminal notifica a rede do seu interesse em mudar de ponto de acesso. Desta forma, a rede torna-se capaz de se adaptar pró activamente ao novo cenário permitindo assim que a transição se faça da forma mais suave possível. Através do processo de *handover* preditivo poderá conseguir-se efectuar *smooth handovers* pois quando o terminal se move para o novo ponto de acesso toda a rede poderá já se encontrar preparada para o receber reduzindo assim o impacto da transição nas comunicações do terminal. Baseado nestas primitivas, espera-se que mobilidade rápida e suave seja umas das características base de qualquer protocolo de redes de próxima geração.

1.5 A Ideia Conceptual do Local-centric Mobility System

Pode-se entender como redes de próxima geração algo que ainda está muito pouco definido no sentido tecnológico visto que está em pleno crescimento até ao desenvolvimento desta dissertação. Como tal, e no âmbito deste cenário, o *LMS* (*Local-centric Mobility System)* vem tentar dar um contributo para a resolução de algumas das problemáticas apresentadas anteriormente, sendo que ele acrescenta também algumas discussões inovadoras ainda não totalmente implementadas por nenhum protocolo já existente. A ideologia do *LMS* foi de certa forma influenciada por outros projectos tais como o *Cellular IPv6* [10], *HAVAII (Handoff-Aware Wireless Internet Infrastructure)* [12] e também pelos requisitos apontados pelo grupo de trabalho *IEEE NetLMM* (*Network-based Localized Mobility Management)* [13].

O *LMS* pretende enquadrar-se no grupo dos protocolos de mobilidade local (*LMP*). O *LMS* é um sistema que tem como seu principal objectivo criar uma mobilidade localizada em micro-domínios permitindo desta forma diminuir os tempos de inoperatividade da rede durante as transições entre pontos de acesso do mesmo domínio local. No *LMS* pretendeu-se ainda que o sistema pudesse interagir com mecanismos de controlo de acesso, autorização, contabilidade e ainda facturação *(AAAC).* Por fim falta ainda acrescentar que pretendeu-se dar a este sistema, mecanismos

de segurança que permitissem protege-lo de ataques de intrusos essencialmente ataques ao bom funcionamento da rede de acesso e ataques de personificação de utilizadores fidedignos.

1.6 Objectivos

Os objectivos principais desta dissertação de mestrado é estudar, implementar e avaliar arquitecturas e protocolos de mobilidade rápida em redes heterogéneas de próxima geração. Assim, nesta dissertação são cumpridos os seguintes objectivos:

- Estudo e avaliação de alguns dos mais importantes protocolos de mobilidade existentes. (*Mobile IP, Fast Mobile IP*, *Proxy MIP*, *Cellular IP* e *HAVAII*)
- Enquadramento dos vários problemas apresentados pelos diferentes protocolos de mobilidade estudados no prisma de uma rede de operador.
- Projecção um modelo protocolar e de arquitectura para redes de próxima geração, centrados na visão de operador, que solucionem os problemas encontrados no estudos efectuados aos protocolos de mobilidade.
- Desenvolvimento de um protótipo funcional que demonstre as capacidades do modelo projectado.
- Estudo e avaliação das prestações do protótipo desenvolvido em ambiente de laboratório.

1.7 Publicações Científicas

Como resultado do trabalho realizado no âmbito desta dissertação de mestrado foi publicado o seguinte artigo científico que descreve o protocolo e a arquitectura em redes de próxima geração assim como apresenta os resultados obtidos através do protótipo desenvolvido.

- Nuno Gonçalo Ferreira, Rui L. Aguiar, Susana Sargento, “A novel Local-centric Mobility System (*LMS*)”, The International Conference on Information Networking 2007 (ICOIN 2007) - Janeiro de 2007

1.8 Organização desta Dissertação

Esta dissertação é organizada da seguinte forma:

Capítulo I. Descreve o âmbito desta dissertação e efectua uma resumida introdução à problemática da mobilidade IP que deu origem a este trabalho.

Capítulo II. Descreve o estado da arte referente aos protocolos de mobilidade existentes, as suas vantagens e as suas desvantagens. São apresentadas as características chave que motivaram o aparecimento do *LMS (Local-centric Mobility System)*.

Capítulo III. Descreve em detalhe o *LMS*. Neste capítulo são abordados detalhes como a arquitectura, mecanismos de mobilidade, protocolo de sinalização, segurança e *QoS (Quality of Service).*

Capítulo IV. Descreve como foi desenvolvido o protótipo e em que condições foi testado. Descreve ainda que testes foram efectuadas e quais os resultados que daí surgiram bem como a sua avaliação

Capítulo V. Apresenta a conclusão final sobre o trabalho realizado e indica quais as perspectivas para trabalhos futuros no mesmo âmbito.

Capítulo II
Mobilidade IP - Estado da arte

2.1 Introdução

Os requisitos das redes de próxima geração, especialmente originados pela era dos novos serviços multimédia, obrigará a uma forte evolução tanto ao nível tecnológico como ao nível dos protocolos que irão suportar as futuras redes. É de certa forma previsível que as redes de futuro serão suportas pelo protocolo de rede IP, muito provavelmente pela sua versão 6 (seis) o IPv6, e que os serviços fornecidos sobre ele obriguem um cumprimento estrito de uma panóplia de requisitos. O protocolo de rede IP assume que todos os terminais de rede detêm um endereço IP válido, único e topologicamente correcto na rede. Por conseguinte, todo o encaminhamento (*routing)* é efectuado partindo destes pressupostos e sem eles é impossível existir comunicação entre dois terminais localizados em redes IP diferentes. Quando dois terminais estão em comunicação em ambos existe uma máquina de estados que define as características do canal de comunicação. Em termos gerais um canal de comunicação é definido pelos endereços IP dos respectivos terminais, os portos de comunicação e o protocolo. Este conjunto de informação define inequivocamente um fluxo de dados na rede e permite que cada um dos terminais identifique o fluxo de dados na rede como sendo direccionado a eles. Contudo, no que diz respeito ao encaminhamento dos pacotes de dados nos troços de rede, a informação mais importante que o pacote transporta é o endereçamento IP de destino pois este indica a localização topológica do terminal de destino na rede. Desta forma os *Routers* (dispositivos de encaminhamento de pacotes na rede) podem identificar e calcular o melhor percurso para o fluxo de dados de forma a que este atinja o terminal de destino. Naturalmente, quando um terminal se move de uma rede IP para outra, o seu endereço IP deverá mudar para que fique topologicamente correcto com a sua nova posição na rede. Como tal, se durante o momento de transição topológica o terminal tiver um canal de comunicação activo com outro terminal, este canal será corrompido pela mudança de endereço IP. Corrompendo o canal de comunicação activo entre o terminal móvel (*MT*) e o terminal correspondente (*TC*) a comunicação falha entre ambos e torna-se imprescindível restabelecer a ligação. Este fenómeno é extremamente indesejável, especialmente se o cenário for uma rede de operador de próxima geração onde todos os dispositivos móveis comunicam sobre uma rede IP. Desta forma, sempre que um utilizador se movesse de uma área de cobertura para

outra, todas as suas comunicações teriam que ser restabelecidas o que é muito pouco viável para uma rede de próxima geração. Foi desta forma que a mobilidade IP se tornou num requisito chave para o desenvolvimento das redes de próxima geração. É assim natural que grande parte do foco das atenções dos grupos de investigação em todo o mundo esteja precisamente sobre a mobilidade IP e os processos de optimização da mesma. É compreensível que a forte aposta nesta investigação resulte em diversas modalidades de protocolos de mobilidade, bem como arquitecturas e mecanismos distintos, contudo de forma geral a mobilidade pode analisar-se em dois cenários distintos, que apesar de distintos deverão está sempre integrados. Desta forma a mobilidade em redes IP está organizada em protocolos de mobilidade global (*Global Mobility Protocol - GMP*) e protocolos de mobilidade local (*Local Mobility Protocol – LMP*). Com o desenvolvimento do *Mobile IPv6* o mecanismo de mobilidade, apresentado para as redes IPv4, foi reformulado e simplificado melhorando substancialmente a desempenho do mesmo. Contudo, a mobilidade global dada pelo *Mobile IP*, era ainda assim pouco eficiente no que diz respeito ao impacto nas comunicações existentes entre o terminal móvel e o terminal correspondente. Desta forma, era relativamente frequente sentir-se longas quebras na transmissão dos dados durante um *handover* entre pontos de acesso tornando assim a mobilidade IP em algo pouco interessante para comunicações de tempo real, como as aplicações multimédia. As longas quebras de comunicação davam-se devido ao tempo que o *Mobile IP* demorava a efectuar a actualização da posição do terminal móvel. Este processo de actualização denomina-se por *Binding Update (BU)* e acontece sempre que o terminal móvel se liga a num novo ponto de acesso. A actualização do agente de mobilidade da rede natural (*Home Agente – HA)* bem como, no caso de optimização, o tempo de actualização dos nós correspondentes (*Correspondent Node – CN),* implicava mudanças na maquina de estados de ambos bem como actualização de rotas. Este processo representava um tempo de inactividade substancialmente grande que por vezes poderia chegar à escala dos segundos e por isso tornava-se cada vez mais importante desenvolver novas soluções que não sofressem do mesmo problema. Como solução a este problema surgiu o conceito de micro-mobilidade ou mobilidade local. A mobilidade local, tal como o nome por si só já indica, representa o processo mobilidade de um terminal numa área concisa e tipicamente pequena, tal como por exemplo um campus universitário ou uma pequena cidade. Assim, sempre que o terminal se move neste espaço definido a mobilidade local deverá ser suficientemente rápida para não existir rompimento nas ligações e efectuando assim uma transição entre pontos de acesso rápida e suave. Por outro lado, sempre que o terminal se move dentro do domínio local, ou micro-domínio, a mobilidade local deve dar-se de forma transparente à mobilidade global. Desta forma o terminal poderá mover-se dentro do

domínio local sem necessitar de notificar os agentes de mobilidade global o que naturalmente traduz-se num melhoramento importante nos tempos de *handover.* Contudo, sempre que o terminal se move entre dois pontos de acesso que estão localizados em domínios locais distintos, ele terá obrigatoriamente que notificar o agente de mobilidade global (*HA*) por forma a actualizar a sua posição global. Hierarquizando desta forma o espaço de mobilidade tornou-se possível melhorar os tempos de *handover* dentro do domínio, diminuindo o impacto do *handover* na transmissão de dados e melhorando assim o suporte para aplicações de tempo real cujos requisitos são muito exigentes.

Uma outra proposta interessante que foi desenvolvida para diminuir os tempos de *handover* entre dois pontos acesso distintos foram os *handovers* preditivos para o *Mobile IP*, ou *Fast Handovers for Mobile IP* [15] . Este novo mecanismo trouxe a possibilidade de configurar e preparar a rede de destino ainda antes do terminal se mover para ela. Desta forma, quando o terminal efectua realmente o *handover* para o novo ponto de acesso toda a rede já está preparada para suportar os seus serviços e todas as configurações já foram efectuadas previamente permitindo assim que o terminal comece a transmitir mal obtenha capacidade física para o efeito. Em suma, existem duas formas proceder a uma *handover*: usando a técnica *Make-Before-Break* ou a técnica de *Break-Before-Make*, preparando a rede antes da transição ou não, respectivamente. Estas possibilidades depende directamente das capacidades intrínsecas da tecnologias em nível 2 (dois).

2.2 Mobilidade Layer 2 em 802.11

Com o crescente desenvolvimento da tecnologia rádio *IEEE802.11* e a sua forte afirmação perante operadores de telecomunicações que já começam a explorar os seus recursos, tem-se vindo a formalizar a ideia que as redes de próxima geração poderão possivelmente ser parcialmente suportadas por esta tecnologia. Pressupõe-se assim que as redes do futuro serão constituídas por micro células *IEEE802.11* [16] bem como possivelmente por células *UMTS* [16]. Desta forma, o tempo de *handover* de um terminal entre dois pontos de acesso à rede irá depender não só do protocolo de comunicação de camada 3 (L3) assim como dos mecanismos de camada 1 (L1) e camada 2 (L2). Por conseguinte, quando um terminal está associado a um ponto de acesso e pretende iniciar o *handover*, ele efectua um varrimento de todos os canais disponíveis por forma a mapear os pontos de acesso em seu redor nas devidas gamas de frequência. Assim, durante

esta fase de descoberta ele serve-se do *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) para aceder ao meio rádio partilhado. Seguidamente o terminal emite uma trama *Probe Request* para a rede na expectativa de receber uma resposta de um equipamento de rede de acesso, vulgarmente designado por *Access Point (AP).* Após emitir a trama, o terminal inicia um contador de tempo que lhe permitirá saber se o tempo de espera pela trama de resposta foi excedido, e nesse caso ele recomeça todo o procedimento seleccionando um novo canal rádio para a sua nova pesquisa. Em cada resposta recebida, *Probe Response*, o terminal mapeia o ponto de acesso no canal rádio correspondente. Este processo deve acontecer em todos os canais de rádio até que todos sejam completamente pesquisados e assim todo o mapeamento de pontos de acesso seja concluído. Este primeiro passo é muito importante pois permite ao terminal saber exactamente as características do ponto de acesso de destino assim como a sua localização no espectro de rádio. Contudo, por questões de optimização, muitas vezes o processo de pesquisa, vulgarmente designado por *Scanning* não é efectuado devido ao tempo que este necessita para ser completado. Como tal, as aplicações de controlo de *handover* informam o dispositivo de comunicação das características do ponto de acesso de destino bem como a sua localização no espectro rádio, ou seja o canal onde se encontra, aumentando consideravelmente a desempenho do *handover*.

O processo de re-autenticação e re-associação no novo ponto de acesso é iniciado logo após o terminal conhecer todas as características técnicas do mesmo. Desta forma, o terminal, vulgarmente designado por *Cliente Station* (STA), inicia o processo enviando uma trama *Authentication Request* para o ponto de acesso informando-o da sua identidade. O ponto de acesso recebe a trama de autenticação e verifica a sua validade fazendo um controlo de acesso à rede através da sua identidade. Após o processo de decisão interno o ponto de acesso, independentemente da sua decisão ser favorável ou não, envia uma trama *Authentication Response* ao terminal como resposta. Caso a resposta seja desfavorável o terminal não poderá associar-se a este ponto de acesso à rede, contudo caso seja favorável ele emite uma trama *Reassociation Request* indicando a sua vontade em re-associar-se a este dispositivo de acesso. Por fim, o processo termina quando o ponto de acesso envia uma trama de *Reassociation Response* indicando o veredicto final relativo ao processo de associação. Assim que se associa ao novo ponto de acesso, o mecanismo de controlo da camada 2 (L2) envia uma notificação de estado da ligação ao mecanismo de controlo da camada 3 (L3) dando assim por terminado o processo de *Layer 2 Handover* .

2.3 Mobile IPv6 - (MIPv6)

O *Mobile IPv6*, permite que um terminal se mova sem que os canais de comunicação estabelecidos entre ele e o terminal correspondente se quebrem. Este facto significa que o endereço natural (*Home Address*) nunca se modifica mesmo durante a mobilidade do terminal. No *Mobile IPv6* não existem agentes de mobilidade na rede estrangeira (FA - *Foreing Agents*) sendo que desta forma o *HA (Home Agent)* detém o papel principal no suporte da mobilidade.

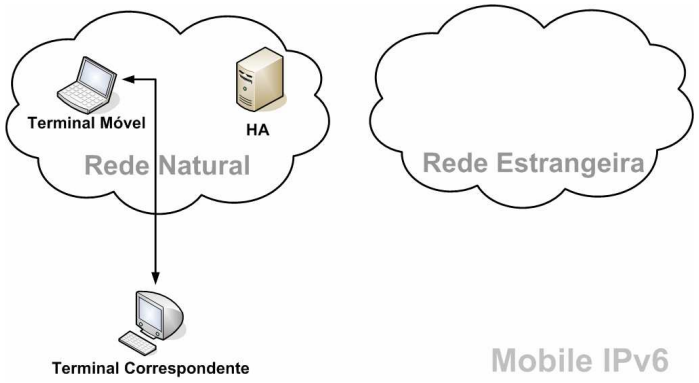


Figura 1 – Mobile IPv6, cenário inicial

A Figura 1 representa uma arquitectura típica de um cenário de mobilidade IP. Em qualquer rede IPv6 os *routers* enviam mensagens *Router Advertisement* para a rede indicando qual o prefixo de rede que deverá ser utilizado ali. Por conseguinte, quando o terminal se movimenta para a rede estrangeira ele recebe estas mensagens de *Router Advertisement* e apercebe-se que está numa nova rede IPv6 diferente da sua rede natural. Seguidamente, ele auto-configura um novo endereço IPv6 (CoA) através do prefixo de rede e da derivação EUI-64 do seu *MAC Address.* Após esta configuração o terminal envia uma mensagem de registo (*Binding Update*) para o *Home Agent* notificando-o do seu novo endereço IPv6 (CoA) e da sua posição topológica. Por sua vez o *Home Agent* regista a nova posição do terminal e envia-lhe uma mensagem de confirmação (*Binding Ack*) , tal como é descrito na Figura 2.

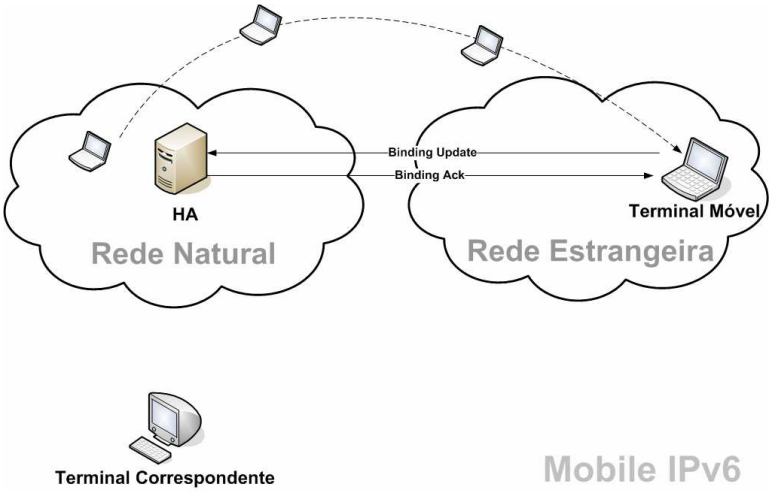


Figura 2 – Mobile IPv6, registo do terminal na rede estrangeira

Após o terminal se registar com sucesso no *Home Agent,* como pode ser observado na Figura 3*,* este inicia um túnel bi-direccional para o terminal que servirá para encaminhar os pacotes que cheguem à rede natural com o seu endereço como destino, sendo que o túnel termina exactamente no terminal móvel. Sempre que o terminal móvel pretende enviar pacotes para o terminal correspondente, este envia os mesmos através do túnel estabelecido com o *Home Agent*, que por sua vez irá retransmitir os pacotes para o terminal correspondente através de técnicas de encaminhamento clássicas.

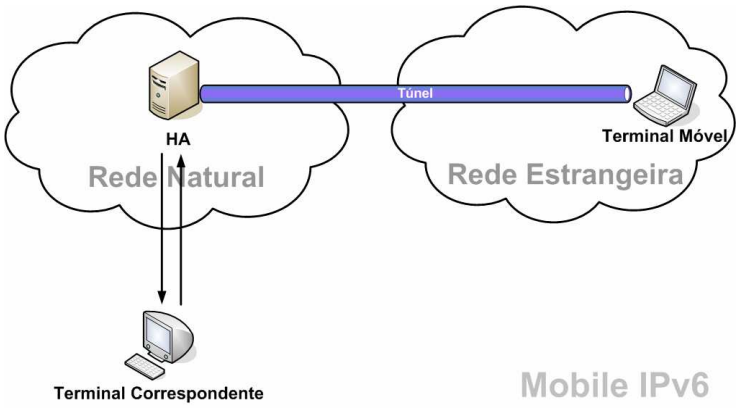


Figura 3 – Mobile IPv6, comunicação entre terminais

Do ponto de vista do terminal correspondente, a mobilidade acontece de forma completamente transparente sendo inclusive que este não necessita de ter suporte para mobilidade, apenas se pretender optimização de rotas. Opcionalmente o terminal móvel pode enviar uma mensagem de actualização (*Binding Update*) ao

terminal correspondente indicando assim o seu novo endereço topológico *CoA (Care-of-Address)*. (ver Figura 4)

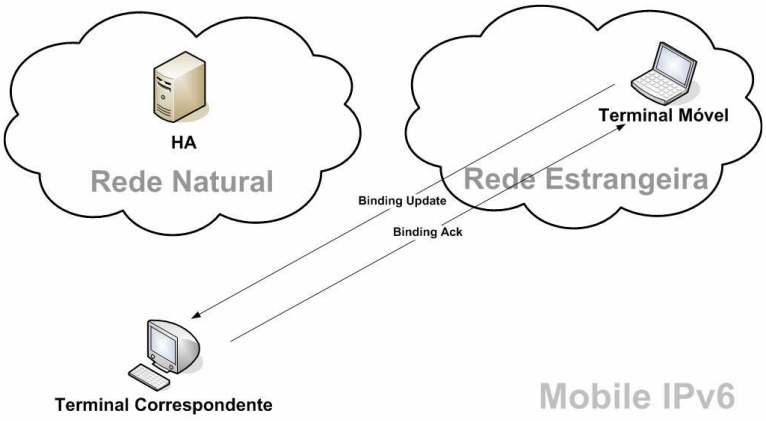


Figura 4 – Mobile IPv6, optimização de rotas com o terminal correspondente

Esta melhoria no protocolo permite optimizar as rotas de encaminhamento evitando que todo o tráfego passe pelo *Home Agent*, melhorando assim a desempenho e a escalabilidade dos mecanismos de mobilidade. Desta forma o terminal correspondente pode enviar os pacotes directamente para o terminal móvel através do seu *CoA (Care-of-Address)*. Contudo, para que a optimização seja possível, o terminal correspondente necessitará de ter suporte para mobilidade o que nem sempre é possível.

O *Mobile IPv6* é um protocolo robusto devido à sua simplicidade. Para alem disto, o *Mobile IPv6* serve-se de vantagens do intrínsecas IPv6 que no IPv4 não eram possíveis, tais como a segurança intrínseca do *IPsec* e a resolução nativa do problema das NATs que no IPv6 não existe. Assim as mensagens de registo do terminal móvel podem ser autenticadas usando *AH (Authentication Header)* [6]. Contudo, visto que no *Mobile IPv6* é possível optimizar as rotas efectuado um *Binding Update* ao terminal correspondente, isso implica um processo de registro entre o terminal móvel e o terminal correspondente. Dado, que o terminal correspondente é um equipamento que pode estar localizado em qualquer lugar na Internet, torna-se impossível criar qualquer relacionamento de segurança entre ambos sem algum mecanismo global de autenticação automática visto que o uso de *IPSec* é proibitivo neste cenário. Como solução a este problema de segurança foi proposto um novo mecanismo de autenticação descentralizado denominado por *Return Routability* (RR). Assim, quando o se pretende efectuar um processo de autenticação mutuo entre os terminais, o terminal móvel envia separadamente parte do material criptográfico para ambos os endereços do terminal móvel, o endereço natural e o endereço estrangeiro (*CoA*) . Através deste processo o terminal

correspondente é capaz de verificar se o terminal móvel pode ser alcançado através dos dois caminhos distintos. Visto que os pacotes enviados pelo *CoA (Care-of-Address)* são encaminhados directamente para o terminal móvel, e visto que os pacotes enviados pelo endereço natural são enviados pelo *Home Agent*, é possível garantir que o material criptográfico não é trocado todo pelo mesmo caminho de rede entre ambos os terminais. Desta forma é de certa forma garantido que apenas o terminal móvel fidedigno irá conseguir receber as duas partes do material criptográfico e refazer a chave final. Contudo, é importante realçar que o mecanismo de *RR (Return Routability)* não é totalmente seguro. Um atacante adequadamente localizado na rede poderia capturar ambas as mensagens enviadas pelo *CN* com a informação criptográfica antes de o caminho das mensagens se bifurcar. Isto permitiria que mensagens de *Binding Update* fossem forjadas pelo atacante comprometendo o mecanismo de mobilidade, como pode ser observado na Figura 5.

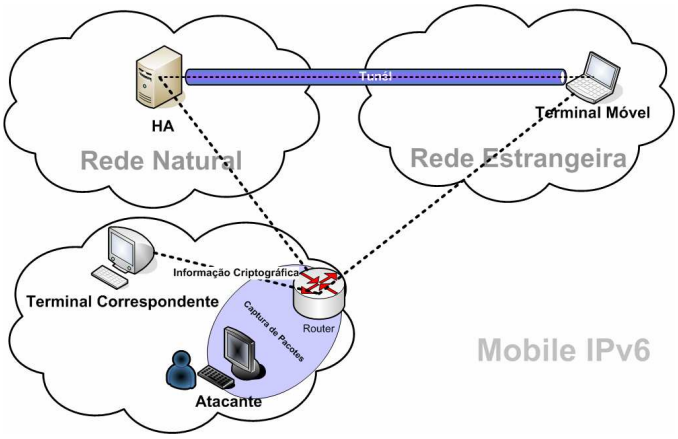


Figura 5 – Mobile IPv6, ataque ao mecanismo Return Routability (RR)

2.4 Fast Handovers for Mobile IPv6 - (FMIP)

Apesar de o *Mobile IP* ser o principal mecanismo de mobilidade em redes IP este não é muito eficiente no que diz respeito aos tempos de *handover* entre pontos de acesso. Quando um terminal móvel se move para um novo ponto de acesso este gasta algum tempo para configurar o novo endereço IP e no caso do IPv6 a executar o mecanismo *DAD (Duplicated Address Detection)*. Assim, existe um período de tempo onde o terminal fica inevitavelmente desligado da rede e consequentemente as suas ligações activas acabam por sofrer uma interrupção considerável. Este momento de interrupção tem um impacto negativo em todos os serviços de rede

activos nesse momento, especialmente perceptível nos serviços com requisitos de tempo real.

A criação do mecanismo de *Fast Handovers* [18] tornou-se assim imprescindível para a mobilidade em redes de próxima geração onde tipicamente existem serviços com requisitos de tempo real, tais como a voz sobre IP (*VOIP – Voice over IP*). Este mecanismo permite ao *Mobile IP* preparar e configurar todos os recursos de rede antes de o terminal móvel iniciar o processo de *handover*. Por conseguinte, quando o terminal chega à rede de destino todos os recursos estão devidamente configurados e disponíveis para ser utilizados. Desta forma os tempos de inactividade durante o handover tornaram-se bastante mais reduzidos que no cenário clássico de mobilidade IP com *Mobile IP*.

O problema do tempo de inactividade do terminal logo após a transição entre pontos de acesso acontece devido ao tempo que o terminal demora a detectar a nova rede bem como a configurar correctamente todos os seus interfaces. Mais ainda, a capacidade de comunicar ao nível da camada três do modelo OSI depende necessariamente do tempo que o protocolo de mobilidade demora para processar a actualização de posição topológica do terminal. Desta forma, o tempo estimado que um terminal está inactivo é o somatório do tempo de detecção da nova rede mais o tempo de configuração do novo endereço de rede mais o tempo de notificação do *Home Agent* e todos os terminais correspondentes.

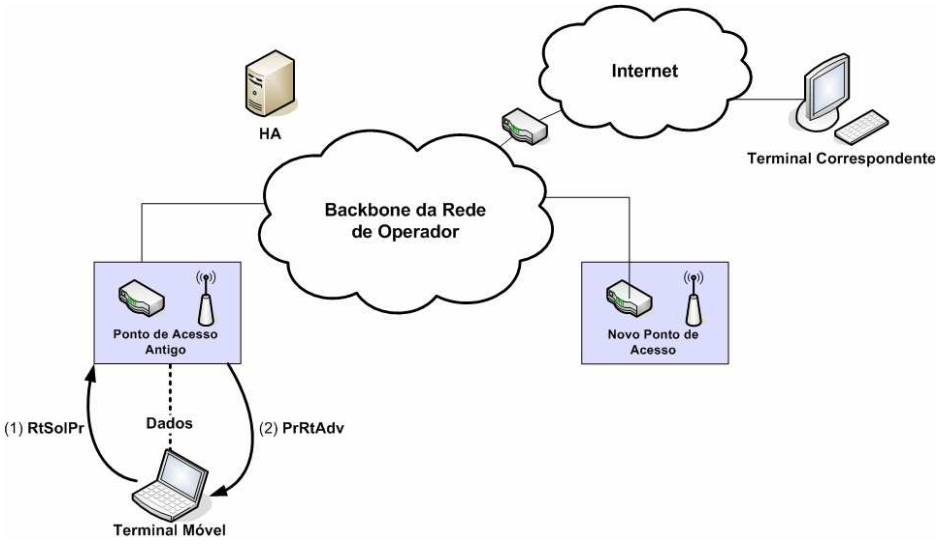


Figura 6 – Fast Mobile IPv6 (Parte I)

Quando um terminal pretende efectuar uma mudança de ponto de acesso este comunica com o ponto de acesso corrente de forma a adquirir informação sobre os pontos de acesso envolventes. Para

que isto seja possível, cada ponto de acesso tem que ter uma base de informação que especifica a configuração e o estado de cada um dos pontos de acesso em seu redor. Só desta forma é possível o terminal conseguir obter a informação sobre os pontos de acesso no meio envolvente através do ponto de acesso corrente. Como tal, sempre que um terminal pretende efectuar uma transição ele começa por requerer um conjunto de informação sobre todos os pontos de acesso em seu redor. (ver Figura 6)

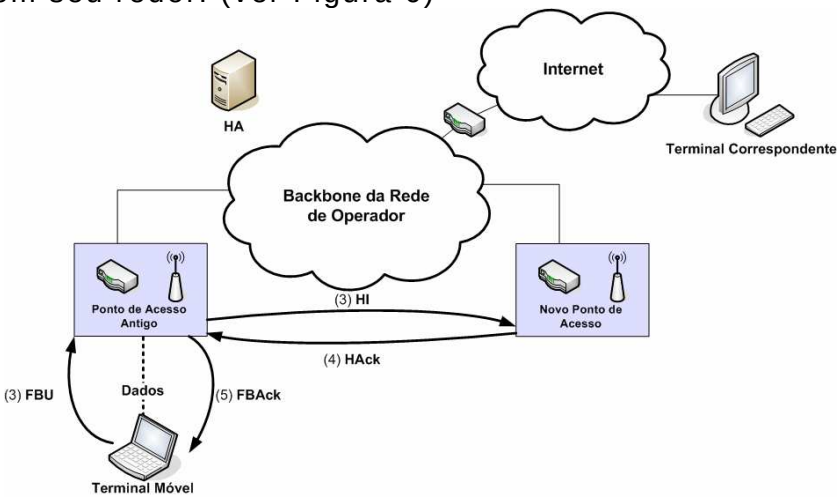


Figura 7 – Fast Mobile IPv6 (Parte II)

Esta informação é-lhe dada pelo seu ponto de acesso actual com base na sua tabela de informações sobre o espaço envolvente. Desta forma é possível que o terminal obtenha toda a informação que necessita para se configurar correctamente antes mesmo de se mover para a rede em questão. Visto que existe uma relação estreita entre o *router* do ponto de acesso de origem e o *router* do ponto de acesso de destino surgiu o conceito de *PAR* (*Previous Access Router)* para o *router* antigo e o conceito de *nAR (New Access Router)* para o *router* novo. Devido às novas funcionalidades apresentadas por esta extensão surgiram também novas mensagens protocolares de mobilidade. A mensagem *RtSolPr* (*Router Solicitation for Proxy)* é emitida pelo terminal sempre que este necessita de informação sobre os pontos de acesso em seu redor. Como resposta o *router* do seu ponto de acesso envia-lhe uma mensagem *PrRtAdv* (*Proxy Router Advertisement)* contendo toda a informação sobre todas as redes em seu redor. Após receber esta informação o terminal móvel envia uma mensagem para o seu ponto de acesso indicando que pretende efectuar um handover através da mensagem *FBU* (*Fast Binding Update).* Esta mensagem indica ao *router* do ponto de acesso actual para qual o ponto de acesso o terminal se pretende mover. Após a recepção desta mensagem o *router* do ponto de acesso antigo (*pAR*) envia uma mensagem *HI (Handover Initiate)* para o *router* do ponto de acesso novo (*nAR*) indicando que um terminal se irá mover para lá. Após receber a mensagem *Handover*

Initiate o *router* do ponto de acesso novo envia uma mensagem *HAck* (*Handover Acknowledgement)* para o *router* do ponto de acesso antigo (*pAR*) indicando que recebeu a notificação correctamente. Seguidamente o *router* do ponto de acesso antigo envia uma mensagem *FBAck* (*Fast Binding Acknowledgement)* para o terminal móvel e para o *router* novo. (ver Figura 7)

Depois desse momento o *router* antigo inicia um processo de duplicação de tráfego para o *router* novo. Este processo e vulgarmente designado por *Bicasting* e trata-se de uma replicação do fluxo de dados que vêm em direcção do *router* antigo para o *router* do ponto de acesso novo. Este mecanismo permite que o terminal se mova para o ponto de acesso novo e receba o tráfego que ainda está em transito para o ponto de acesso antigo evitando assim a perda de dados. Paralelamente, o terminal efectua a transição física para rede do novo ponto de acesso e envia uma mensagem *Fast Neighbor Advertisement* (*FNA*) para o ponto de acesso novo, tal como pode ser observado na Figura 8. Após este processo, o terminal móvel já é capaz de receber os dados que estão ainda em transito para o ponto de acesso antigo devido ao mecanismo de *Bicasting*. Por fim, o terminal móvel efectua o registo com o seu *Home Agent* normalmente, tal como já acontecia no *Mobile IPv6* clássico.

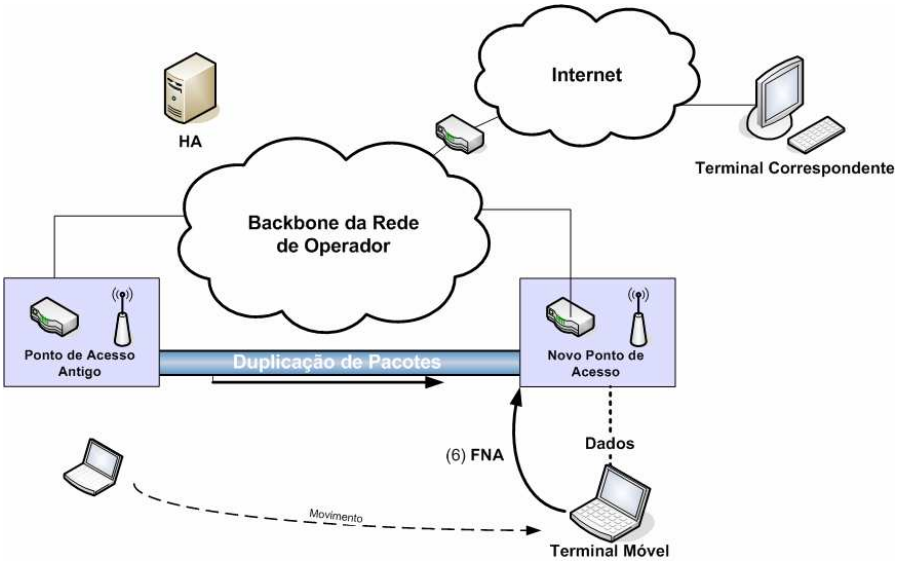


Figura 8 – Fast Mobile IPv6 (Parte III)

A figura Figura 9 mostra o diagrama de sequência respectivo ao processo de *handover* entre dois pontos de acesso distintos usando o mecanismo de *Fast Handovers* para o *Mobile IPv6.*

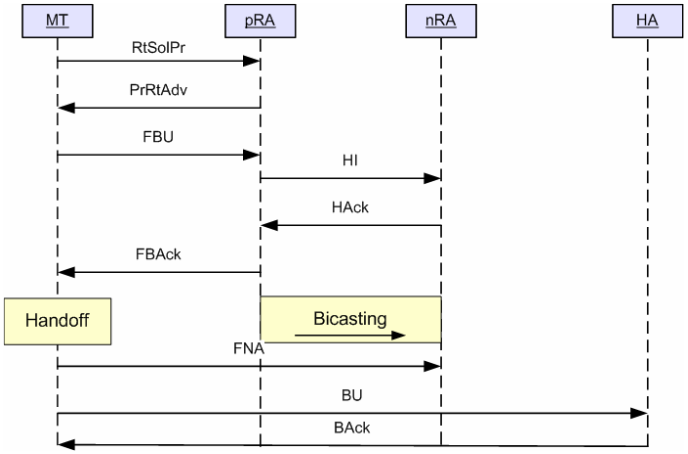


Figura 9 – Fast Mobile IPv6 (Diagrama de sequência)

2.5 Proxy Mobile IP - (PMIP)

O *Mobile IP* [8] ou o *FMIP*[18] exige que o terminal móvel suporte inteiramente na pilha protocolar as mensagens e mecanismos usados pelo protocolo de mobilidade. Este factor não é muito desejado nas redes heterogéneas dado que nem todos os terminais poderão ter suporte intrínseco para mobilidade. O *PMIP (Proxy Mobile IP)* [20], é um protocolo que estende o *Mobile IP* clássico de forma a permitir que o terminal móvel não necessite de suporte para mobilidade IP intrínseca. O *PMIP* é uma proposta protocolar feita no âmbito dos protocolos de mobilidade local incentivada pelo grupo *NetLMM* do *IETF*. No *PMIP* são usados agentes especiais que permitem negociar a mobilidade em nome do terminal móvel. A principal ideia do protocolo *PMIP* é permitir que tanto os terminais que suportam *Mobile IP* como os que não o suportam possam obter mobilidade IP nas redes *PMIP.*

Sempre que um terminal se move para um domínio *PMIP*, a rede proporciona-lhe o seu endereço natural, *Home Address*, de forma a que este possa sempre funcionar como se estivesse na sua rede natural, *Home Network*. Para que isto aconteça, a rede detém um conhecimento prévio de qual o endereço natural a ser indexado a cada terminal da rede. Este conhecimento é tipicamente obtido através de um processo de autenticação prévio feito pelo terminal. Desta forma, o terminal móvel por mais que se mova na rede julgará sempre que se encontra na sua rede natural, tornando assim a mobilidade completamente transparente para o mesmo. A Figura 10 mostra a arquitectura de um domínio *PMIP*.

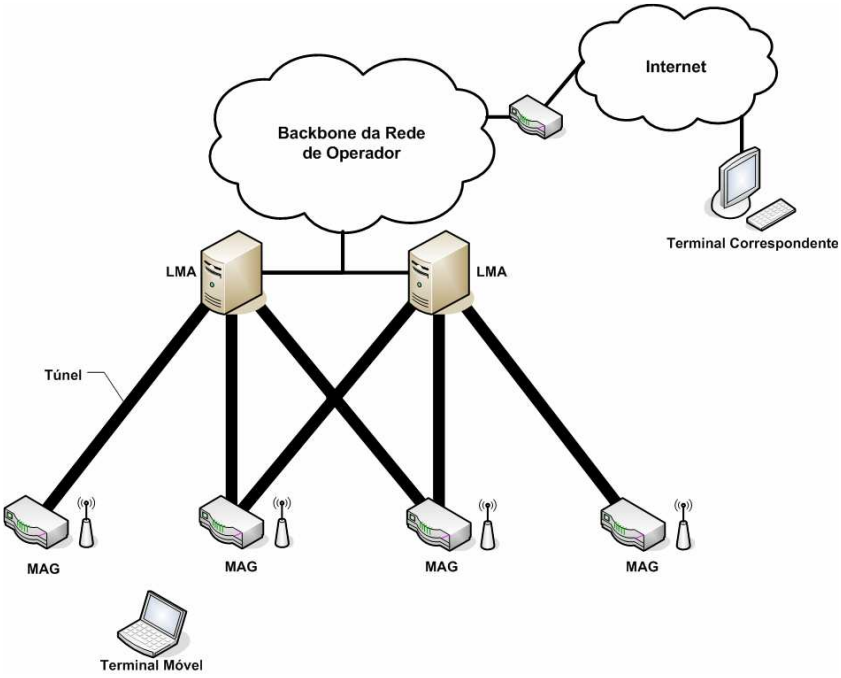


Figura 10 – Proxy MIP (PMIP), arquitectura da rede

Este novo conceito introduz um novo elemento funcional na rede, o agente de mobilidade *MAG (Mobility Access Gateway)*. Este agente de mobilidade esta localizado na rede de acesso e efectua a sinalização de mobilidade global em nome do terminal móvel. É este agente que permite que o terminal móvel se desassocie do conceito de mobilidade clássica e torne o mecanismo de negociação de mobilidade completamente transparente. Do ponto de vista do *LMA (Local Mobility Anchor)* o *MAG* é um elemento funcional que tem autorização para representar o terminal móvel no que diz respeito a toda a sinalização de mobilidade. O *LMA* é um agente de mobilidade do tipo *Home Agent* para o terminal móvel enquanto este permanece no domínio *PMIP*. Este agente de mobilidade tem como principal função garantir que o terminal móvel é alcançável tanto de dentro do domínio *PIMIP* como de fora do mesmo.

Quando o terminal móvel se liga na rede de acesso, ele associa-se ao *MAG* mais próximo. Após o processo de associação, o terminal móvel envia para a rede as suas credenciais de acesso de forma a ser identificado inequivocamente. O *MAG* efectua a autenticação do terminal na rede e através do servidor de *AAA (Authentication, Authorization, Accounting)* obtém o perfil do terminal, tal como pode ser observado na Figura 11.

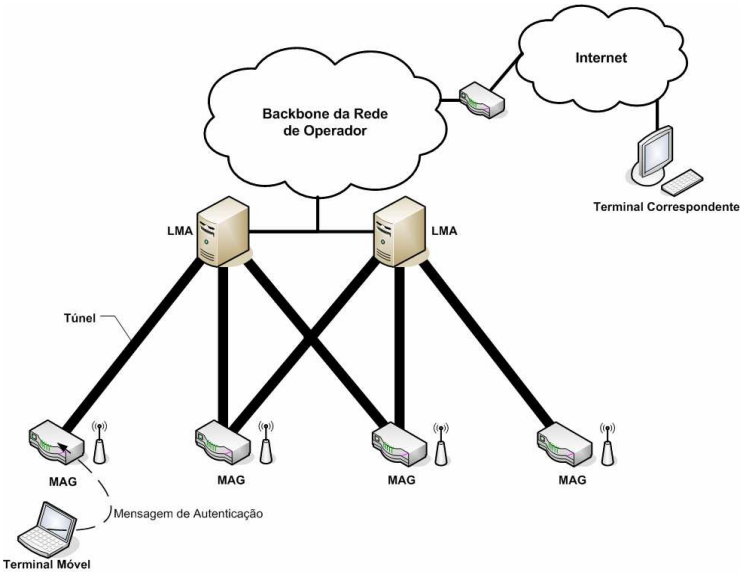


Figura 11 – Proxy MIP, Autenticação do terminal na rede

No perfil do terminal está toda a informação necessária para que o *MAG* possa emular a as características da rede natural do terminal e desta forma iludi-lo tornando o processo de mobilidade transparente. Para que o terminal julgue estar na presença da sua rede natural, o *MAG* inicia a transmissão periódica de mensagens de *RA* (*Router Advertisement)* indicando o prefixo de rede da sua rede natural. As mensagens de *RA* são mensagens emitidas pelos *routers* de acesso e permitem que os terminais se configurem com base na informação emitida no seu interior. Assim, o terminal móvel ao receber estas mensagens irá configurar-se da mesma forma como faria na sua rede natural, visto que o *MAG* a está a emular. A Figura 12 ilustra este processo.

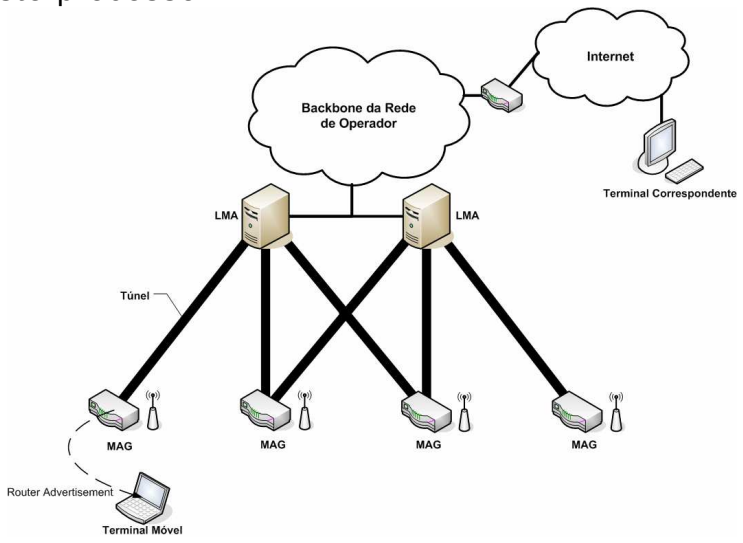


Figura 12 – Proxy MIP, emulação da rede natural do terminal móvel

Para notificar o *LMA* sobre a actual localização do terminal móvel, o *MAG* envia periodicamente mensagens especiais de mobilidade *PMIP* para o efeito. Estas mensagens, *PBU (Proxy Binding Update),* permitem que o *LMA* designado possa localizar e registar a posição topológica do terminal móvel para mais tarde poder encaminhar os pacotes até ele. O *LMA* logo após registar a posição topológica do terminal com sucesso envia para o *MAG* uma mensagem de *PBAck (Proxy Binding Ack)* notificando o sucesso do registo. Por fim, é estabelecido um túnel entre o *LMA* e o *MAG* que servirá para encaminhar os pacotes de dados com destino ao terminal móvel na rede *PMIP*. Na Figura 13 pode observar-se este mecanismo.

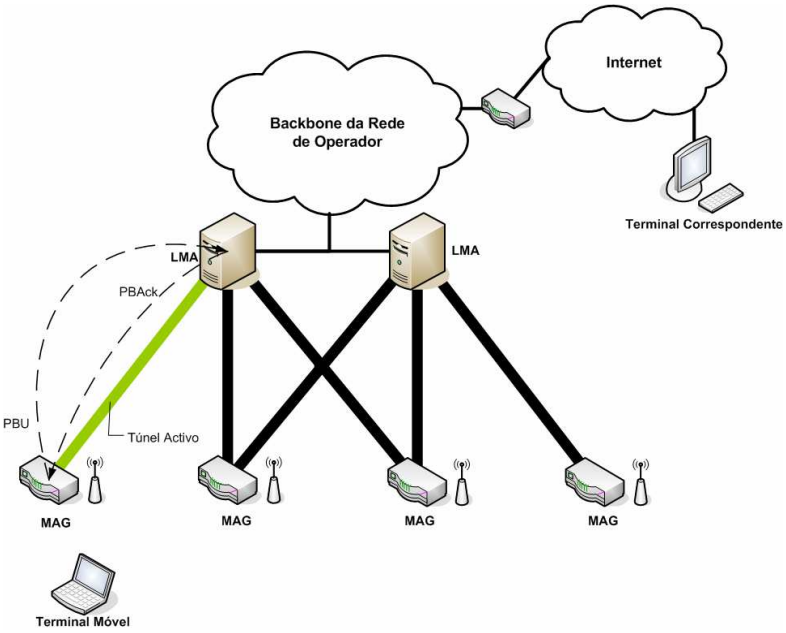


Figura 13 – Proxy MIP, processo de registo no LMA

Sempre que o terminal se move dentro do mesmo domínio *PMIP*, este não muda de *LMA.* Desta forma, o procedimento de *handover* é extremamente simples e subsequentemente eficaz. Quando o terminal móvel se move de um *MAG* para outro *MAG* dentro do mesmo domínio *PMIP*, o processo de associação faz com que o novo *MAG* efectue uma actualização da posição topológica do terminal móvel perante o *LMA.* Desta forma o *LMA* pode concluir que o terminal móvel se está a mover dentro do seu domínio e actualiza o túnel de encaminhamento de dados para o novo *MAG*. Visto que o novo *MAG* irá implicitamente emular a rede natural do terminal móvel, *Home Network*, o mesmo não se aperceberá do processo de *handover* ao nível da camada 3 (três) do modelo OSI *(Layer 3).* Desta forma, poderá concluir-se que os *handovers* dentro do mesmo domínio *PMIP* são geograficamente transparentes para a camada de rede do terminal móvel.

O *PMIP*, impõe alguns mecanismos de segurança na rede. Quando o terminal móvel se associa na rede, este tem que enviar a sua credencial de acesso que poderá ser comprovada perante um servidor de *AAA (Authentication, Authorization, Accounting)*. Por outro lado, sempre que o *LMA* e o *MAG* efectuarem transacções de informação, por exemplo para a troca de mensagens *Binding Proxy Update (PBU)*, a comunicação é efectuada segundo túneis *IPSec*. Os túneis *IPSec* são mecanismos criptográficos que recorrem a procedimentos de cifragem, autenticação de dados e verificação de corrupção dos dados durante a transmissão dos mesmos. Este tipo de mecanismos permite ao *PMIP* garantir um nível de fiabilidade e segurança razoáveis para ambientes de mobilidade rápida como os que se esperam para as redes de próxima geração.

2.6 Hierarchical Mobile IP - (HMIP)

O *Mobile IP* é um protocolo que trata a mobilidade do terminal de forma indiscriminada, esteja ele a mover-se entre dois pontos de acesso contíguos ou para um ponto de acesso no outro lado da rede. Este processo indiscriminado, tal como já foi explicado nas secções anteriores referentes ao *Mobile IP*, gera uma latência significativa nos momentos de *handover*. Apesar de esta latência poder ser minimizada através das extensões de mobilidade rápida, tais como o *FMIPv6*, o facto é que a mobilidade é sempre tratada da mesma forma independentemente do grau de mobilidade efectuada. Assim tornou-se importante dividir o espaço de mobilidade em dois tipos de domínio de movimentação, domínio de mobilidade global e domínios de mobilidade local.

Sempre que o terminal se move entre dois pontos de acesso distintos, ele necessita de actualizar a sua posição topológica e envia mensagens de *Binding Update* para o seu *Home Agent* bem como para todos os terminais correspondentes. Contudo, tal como já foi referido nas secções anteriores, este processo é extremamente penoso e indesejável, especialmente se acontecer em todas as transições do terminal. Assim, de forma a solucionar este problema foi proposto um esquema hierárquico de mobilidade designado por *Hierarchical Mobile IPv6* (*HMIPv6*) [19].

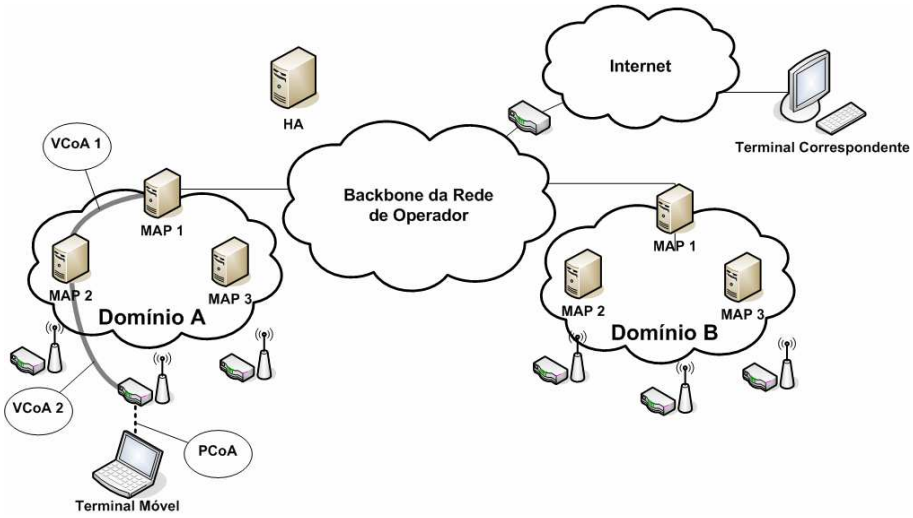


Figura 14 – Hierarchical Mobile IPv6 (Parte I)

A figura anterior (Figura 14) ilustra a arquitectura do hierárquica do *HMIP*. O protocolo *Hierarchical Mobile IP* distingue claramente dois tipos de mobilidade, a mobilidade local e a mobilidade global. Do ponto de vista da mobilidade local, os mecanismos de mobilidade executados são os pertencentes ao *HMIPv6*, do ponto de vista da mobilidade global, entre domínios locais, os mecanismos de mobilidade a executar são os do *Mobile IP*. Desta forma sempre que um terminal se move dentro de um domínio local, toda a sua movimentação é transparente para o *Home Agent* assim como para todos os terminais correspondentes. Por outro lado, quando o terminal se move de um domínio para outro domínio local, os mecanismos de mobilidade global são executados e tanto o *Home Agent* como os terminais correspondentes são notificados dessa movimentação através de mensagens de *Binding Update*.

A arquitectura da rede é hierarquizada por um novo tipo de agente de mobilidade designado como agente de ancoragem. Este novo agente denominado por *MAP (Mobility Anchor Point)* permite criar níveis de hierarquia dentro dos domínios tornando assim a mobilidade transparente para os nós externos, tais como *Home Agent.*

Quando um terminal entra num novo domínio local ele adquire um novo *PCoA (Phisical Care-of Address)*, por exemplo através de *Stateless Autoconfiguration* [4]. Este endereçamento tem que ser topologicamente correcto pois o terminal móvel usa-o como endereço de origem para todos os pacotes que envia. Após a configuração do endereço físico, o terminal envia um *Binding Update* e associa o PCoA com o *VCoA (Virtual Care-of Address)* do *MAP* mais perto da rede de acesso. Este processo continua até atingir o *MAP* do topo da hierarquia, criando assim um conjunto de associações que irão ser utilizadas para transmitir os pacotes ao longo do domínio até ao

terminal móvel. A figura seguinte mostra o processo de registo de um terminal móvel num novo domínio HMIPv6, que também acontece durante o mecanismo de *handover* entre diferentes domínios.

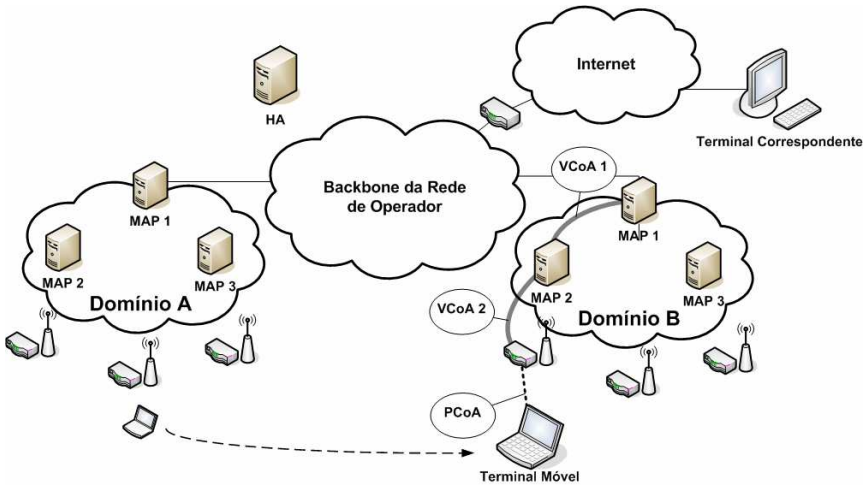


Figura 15 – Hierarchical Mobile IPv6 (Parte II)

Tal como a Figura 15 demonstra, sempre que o terminal se move para um novo domínio este mesmo processo é executado por forma a regista-lo nos *MAPs* existentes. Após o registo no novo domínio, o terminal móvel envia uma mensagem de *Binding Update* para o seu *Home Agent* e efectua a actualização da sua posição geográfica, ou seja indica em domínio onde se encontra. Este procedimento permite que os pacotes vindos do exterior do domínio possam ser correctamente encaminhados para o terminal. O diagrama seguinte da Figura 16 demonstra como um terminal móvel efectua o seu registo num novo domínio *HMIPv6.*

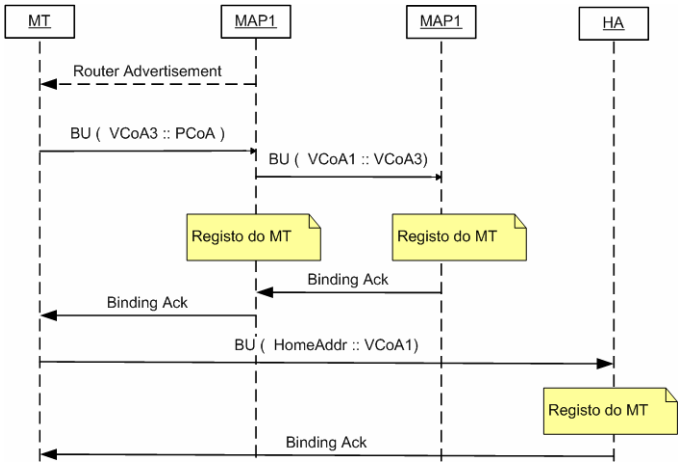


Figura 16 – Hierarchical Mobile IPv6, registo/handover num novo domínio

Sempre que o terminal se move dentro de um domínio local, este apenas actualiza o seu *VCoA* dentro do domínio o que torna processo de *handover* bastante mais rápido. Desta forma o seu endereço global mantém-se e a sua mobilidade é transparente para os terminais correspondentes e para o *Home Agent.* Mais ainda, através deste processo hierárquico de mobilidade o peso da sinalização na rede global também é significantemente reduzido. A Figura 17 ilustra este procedimento.

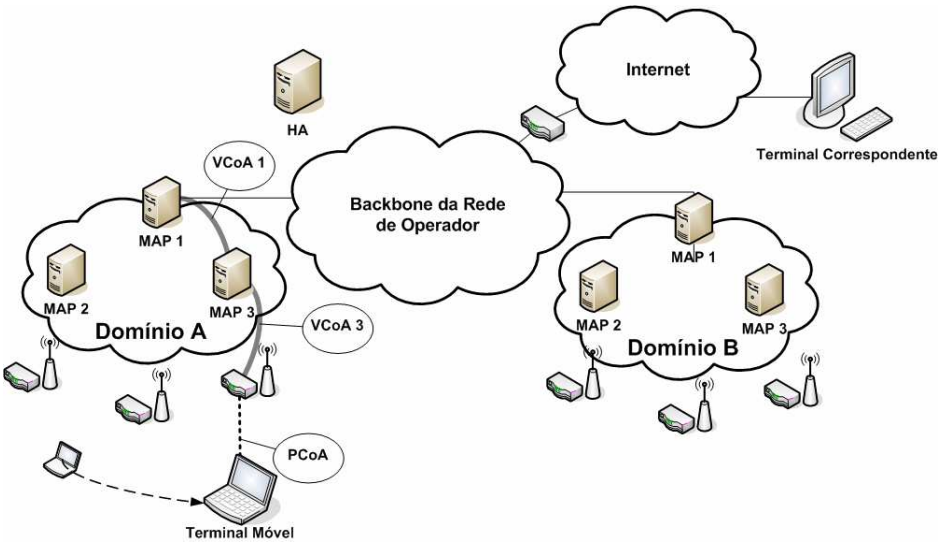


Figura 17 – Hierarchical Mobile IPv6, (Parte III)

O diagrama da Figura 18 mostra como é efectuada a sinalização entre os diferentes agentes de mobilidade durante um handover dentro do mesmo domínio HMIPv6.

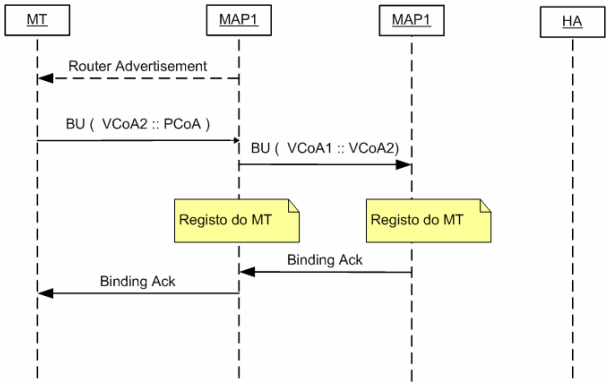


Figura 18 – Hierarchical Mobile IPv6, handover do mesmo domínio

O uso de um esquema hierárquico para suportar os mecanismos de mobilidade tem essencialmente duas vantagens quando o terminal se move dentro do domínio local: Primeiro,

melhora o tempo de *handover* consideravelmente e diminui consequentemente a perda de pacotes durante a transição. Segundo, reduz a quantidade de sinalização que atravessa toda a rede global para atingir o *Home Agent* visto que a sinalização apenas passa a existir dentro no domínio local. Acima de tudo o Hierarchical Mobile IP trouxe um novo conceito à mobilidade IP, dividindo a mobilidade em regiões de forma a minimizar o impacto dos *handovers* na rede e nas comunicações do terminal. Este conceito mostrou ser bastante importante e a prova disso mesmo é que ele encontra-se patente em protocolos mais recentes tais como os sugeridos pelo *IETF Work Group NetLMM.*

2.7 Cellular IP/IPv6 – (CIP / CIPv6)

Em traços gerais, poderá dizer-se que o protocolo IP nunca foi concebido para suportar mobilidade nativa e até ao momento o mecanismo padrão que lhe dá suporte é o Mobile IP [8]. Contudo, como já foi visto anteriormente o Mobile IP não é uma solução perfeita para as redes de próxima geração devido ás suas limitações de desempenho. Com base nas técnicas já utilizadas nas redes celulares desenvolveram-se novas técnicas que aplicados às redes IP aumentaram substancialmente a desempenho da mobilidade. Algumas dessas técnicas conduziram ao desenvolvimento do Cellular IPv4 [9] que mais tarde foi substituído pelo seu sucessor para IPv6, o Cellular IPv6 [10]. As redes Cellular IP, tanto para IPv4 como para IPv6, são constituídas por três novos tipos de agentes de mobilidade. O Cellular IP Gateway interliga a rede Cellular com outra rede não celular que tipicamente é a rede nuclear de operador com suporte para Mobile IP. O Cellular IP Gateway é também o agente controlador da rede celular e nele poderão ser colocados alguns mecanismos de qualidade de serviço (QoS) e autenticação, autorização, contabilidade e facturação (AAAC - Authentication, Authorization, Accounting and Charging). O Cellular IP Node é um nó interno da rede celular que permite a criação de uma estrutura topológica entre o Cellular IP Gateway e as diferentes Cellular IP Base Stations. Este agente é responsável por efectuar o encaminhamento dos pacotes ao longo da rede celular. Por fim, a Cellular IP Base Station interliga a rede celular com a rede de acesso e é através deste que o terminal móvel acede à rede Cellular IP. O Cellular IP implementa uma arquitectura topológica hierárquica em árvore onde o Cellular IP Gateway é a raiz principal e as Base Stations são as folhas da mesma. O tráfego é encaminhado ao longo dos Cellular IP Nodes que são os agentes internos da rede celular. A rede pode ser tão extensa quantos mais nós internos esta tiver,

suportando assim um maior número possível de folhas, ou seja Base *Stations*. A Figura 19 descreve o formato típico de uma rede *Cellular IP* bem como a organização entre todos os seus agentes de mobilidade.

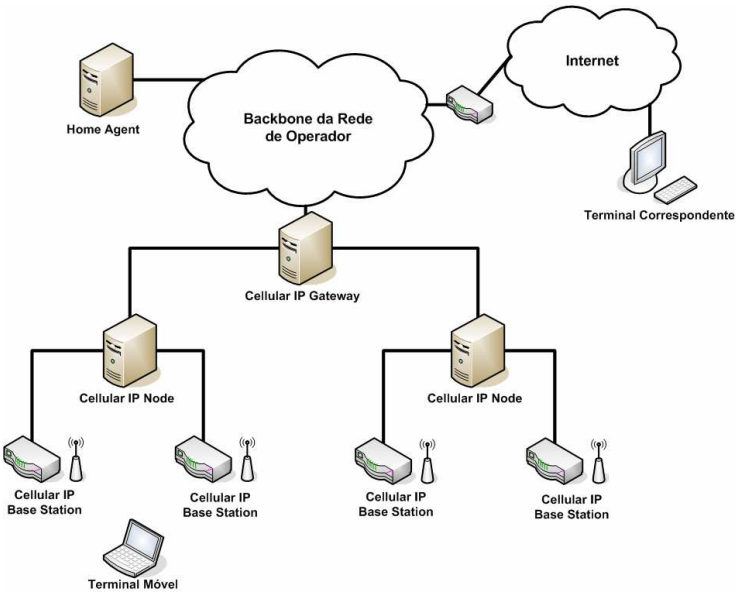


Figura 19 – Cellular IP, arquitectura geral da rede

As *Base Stations* da rede celular enviam periodicamente pacotes de sinalização para a rede designados por *Beacons*. Estes pacotes informam os terminais móveis das redondezas que se encontram numa área coberta por uma rede celular. Cada *Beacon* contem a informação necessária para que o terminal móvel se possa registar na rede celular e iniciar a sua ligação de dados. Quando um dado terminal móvel pretende iniciar uma ligação à rede *Cellular IP* este começa por escutar os *Beacons* enviados pelas *Base Stations* (Figura 20).

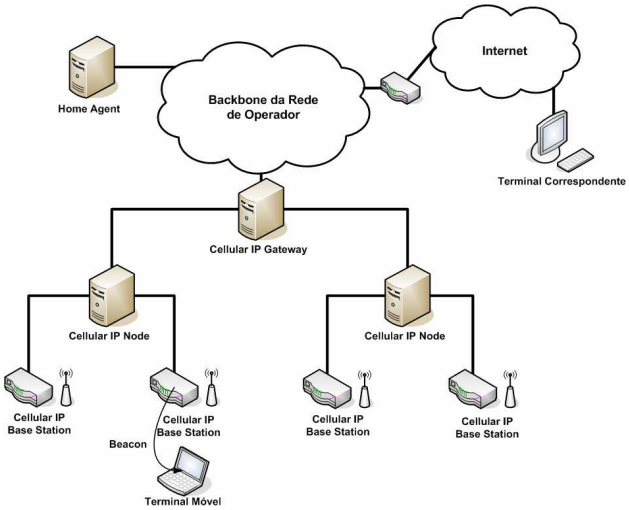


Figura 20 – Cellular IP, processo de registo (Parte I)

Por cada *Beacon* que recebe, o terminal processa os seus dados criando em tempo real uma tabela que descreve todas as *Base Stations* em seu redor. Com base nesta tabela o terminal efectua uma selecção da *Base Station* à qual se irá ligar.

Após a selecção da *Base Station* o terminal móvel inicia o processo de registo na rede *Cellular IP*. Para tal, envia um pacote *Registration Request* com destino ao *Cellular IP Gateway* da célula onde se ligou. No caso do *Cellular IPv6*, a segurança é um parâmetro obrigatório da sua arquitectura sendo assim necessário que o terminal se identifique através da sua chave de acesso à rede e o seu identificador pessoal único *NAI(Network Access Identification)*.
A Figura 21 demonstra este processo.

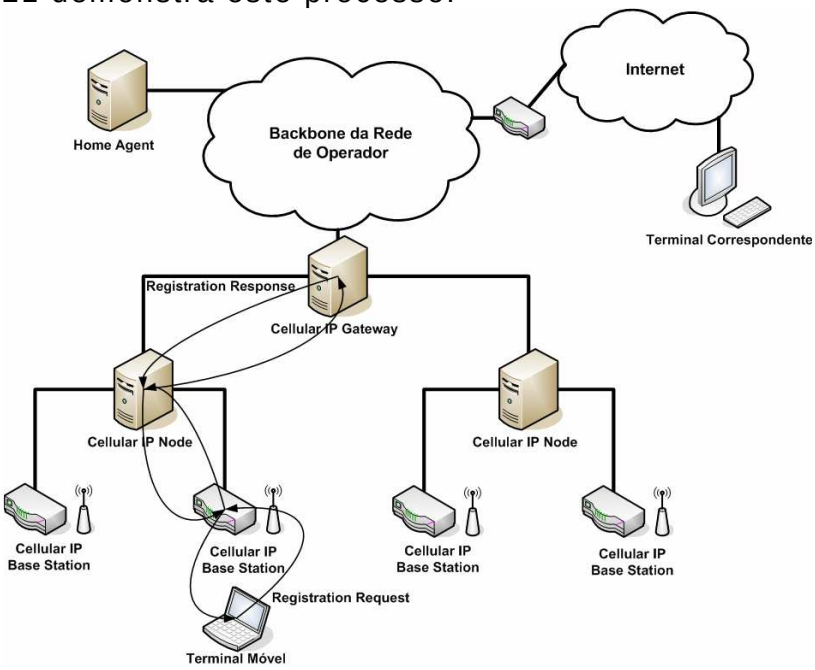


Figura 21 – Cellular IP, processo de registo (Parte II)

O *Cellular IP Gateway* após receber o pacote *Registration Request* proveniente do terminal móvel, efectua o registo do mesmo na célula e responde-lhe com uma mensagem de sucesso. No caso do *Cellular IPv6,* o *Cellular IP Gateway* acede primeiro ao servidor responsável pelo serviço de autenticação em rede (*AAAC - Authentication, Authorization, Accounting and Charging*) de forma a autenticar e validar a autorização de acesso na rede celular. No caso do terminal ser aceite na rede *Cellular IPv6* o *Gateway* da célula processa e envia uma chave de sessão (*PID – Personal IDentification*) que identifica inequivocamente o terminal nessa célula. O terminal serve-se desta chave (*PID*) para assinar todos os seus pacotes de sinalização, garantindo assim a sua autenticidade nessa célula.

No *Cellular IP* todos agentes têm *caches* que permitem localizar o terminal móvel dentro do espaço celular. As *caches* são listas internas que descrevem um conjunto de informação referente ao terminal e que permitem encaminhar os pacotes até ele. Opcionalmente, as *caches* podem também guardar informações referentes aos mecanismos de segurança da célula e identificação do terminal na rede. Cada agente do *Cellular IP* tem obrigatoriamente uma *Routing Cache* e opcionalmente uma *Paging Cache*.

Na redes *Cellular IP* o terminal móvel pode estar em dois estados distintos, activo *(active)* quando está a transmitir ou receber dados e dormente *(Idle)* quando está inactivo à algum tempo. Sempre que o terminal está no seu estado activo, a rede procura-o primariamente através da sua *Routing Cache* e de forma a encaminhar os pacotes de dados para a Base Station onde este se encontra nesse momento. Esta eficácia deve-se ao facto do terminal móvel estar constantemente a enviar pacotes de *Route Update* para a rede a uma taxa consideravelmente alta. Estes pacotes servem para actualizar as *Routing Caches* e quanto maior for a sua taxa de emissão maior a precisão com que a rede encaminha os pacotes para o terminal em cenários de mobilidade rápida. Contudo, o facto de todos os terminais activos estarem a emitir pacotes de sinalização a uma taxa significativamente alta origina um mau aproveitamento dos recursos da rede, especialmente de recursos rádio.

Quando o terminal móvel está sem emitir ou receber pacotes à algum tempo, o terminal passa automaticamente para um estado dormente *(Idle)*. Por conseguinte, sempre que este se encontra neste estado a rede localiza-o num conjunto de *Base Stations* (*Paging Area)* e não numa *Base Station* em especifico. Quando o terminal está num estado dormente *(Idle)*, o seu mecanismo de transmissão rádio é parcialmente desligado estando em baixa potência de emissão. Este apenas é ligado periodicamente para emitir pacotes de sinalização *Page Update*. Este pacotes são emitidos a uma taxa muito menor que os pacotes *Route Update* por forma a melhorar o aproveitamento energético do terminal. Por outro lado, o facto do terminal emitir pacotes *Page Update* a uma taxa mais baixa permite também efectuar um melhor aproveitamento dos recursos da rede, em especial dos recursos partilhados no meio rádio.

A *Routing Cache* serve para determinar qual o caminho que os pacotes de dados devem tomar na rede celular para que estes atinjam o terminal quando este se encontra no seu estado activo. Em traços gerais, cada elemento da *Routing Cache* contem a identificação do terminal na rede, o nome do interface de rede que permite atingi-lo e um campo que informa qual a data da ultima actualização desse elemento da *cache.* Caso a data de actualização tenha expirado então, o elemento é removido da tabela, garantindo

que nunca existem elementos residuais na mesma e aumentando assim a robustez do próprio mecanismo de encaminhamento. Quando os pacotes são encaminhados pela *Routing Cache* eles atingem o terminal com a máxima precisão pois são encaminhados especificamente para a *Base Station* onde este se encontra ancorado.

A *Paging Cache* serve para localizar o terminal numa *Paging Area* da célula sempre que este se encontra no estado *Idle.* As *Paging Areas* são conjuntos de *Base Stations* dentro da mesma célula. O encaminhamento baseado na informação das *Paging Caches* origina que os pacotes não sejam encaminhados com grande precisão devido ao facto de as *Paging Caches* definirem o destino num conjuntos de Base Stations e não uma *Base Station* em especifico. O terminal após ter-se registado correctamente na rede celular, começa por enviar pacotes *Page Update* para a rede identificando a *Paging Area* onde se encontra. Após iniciar uma transmissão de dados o terminal passa a enviar periodicamente pacotes *Route Update* indicando em que *Base Station* em especifico este se encontra.

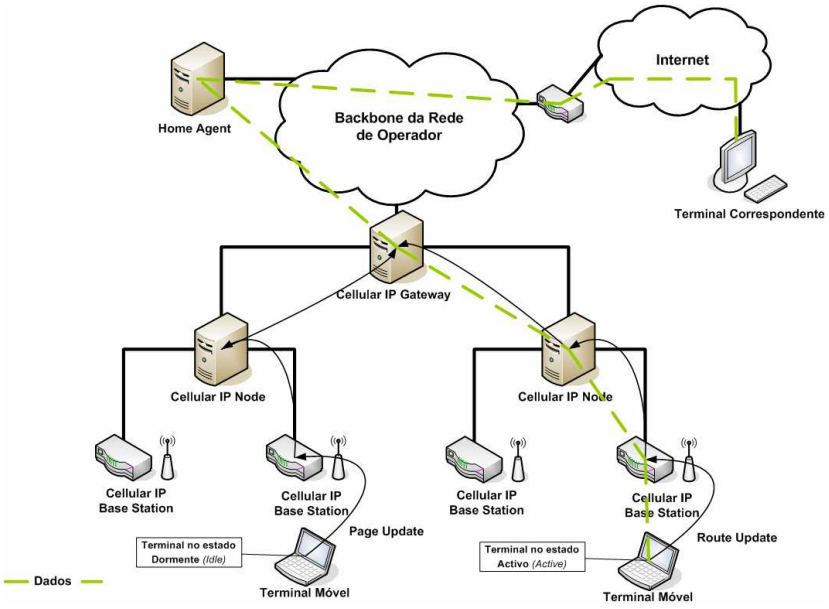


Figura 22 –Cellular IP, criação e manutenção de rotas na célula

No caso do *Cellular IPv6* todos os pacotes *Page Update* e *Route Update* são assinados pelo terminal usando o seu *PID*. Quando o terminal pretende enviar um determinado conjunto de pacotes de dados para a rede, este passa automaticamente do estado *dormente* para o estado *activo*. Sempre que o terminal passa para o estado *activo* ele envia pacotes *Route Update* para a rede.

Todos os pacotes *Router Update* assim como os pacotes de dados enviados pelo terminal vão refrescando a *Routing Cache* de cada um dos *Cellular IP Node* ao longo da célula, criando uma rota desde o *Cellular IP Gateway* até ele, tal como é ilustrado na Figura 22.

Quando um terminal correspondente pretende enviar pacotes de dados para o terminal móvel, estes chegam inicialmente ao *Gateway* da célula. O *Cellular IP Gateway* começa por verificar a existência do terminal na sua célula, consultando as suas *caches*. No caso de o terminal não existir na célula o *Gateway* descarta todos os pacotes endereçados a ele. No caso contrário, ele procura qual o melhor caminho para enviar o pacote até ao terminal com base na informação disponível na *Paging Cache* e na *Routing Cache*. Ao longo de toda a célula, até ao terminal móvel, todos os agentes da mesma efectuam o mesmo procedimento que o *Cellular IP Gateway* efectuou. Quando os pacotes são provenientes do exterior da célula as *caches* não são nem refrescadas nem actualizadas.

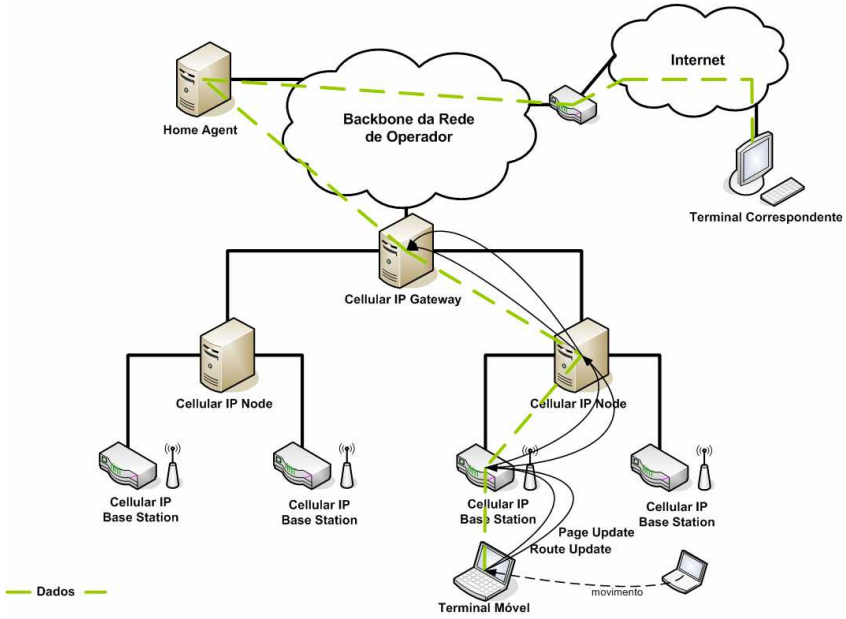


Figura 23 – Cellular IP, procedimento de handover

Nas redes *Cellular IP* o procedimento de handover não é explicito nem preditivo. Quando um terminal móvel pretende mudar de *Base Station* ele não sinaliza à priori a sua vontade permitindo assim que a rede se estruture e prepare para a sua transição. Pelo contrário, no *Cellular IP* todos os *handovers* são reactivos e desta forma a rede não tem nenhum mecanismo de preparação de recursos antes de o terminal se mover efectivamente para a *Base Station* de destino. A Figura 23 mostra como um cenário de *handover* é processado dentro de uma célula *Cellular IP.* Quando um terminal pretende efectuar um *handover* entre duas *Base Stations* pertencentes à mesma célula (ver Figura 23), ele efectua um

procedimento do tipo *Break-Before-Make*, ou seja, ele comuta de *Base Station* sem notificar a rede primeiro da sua vontade. Como tal, quando o terminal móvel efectua a ligação com a nova *Base Station*, ele envia uma mensagem de *Page Update* e uma mensagem de *Route Update* para a rede notificando-a da sua nova posição topológica. Estes dois pacotes ao percorrerem os diferentes nós da célula vão criando novos estados de encaminhamento em cada um deles até atingirem o *Cellular IP Gateway.* Através deste procedimento a célula adapta-se à nova posição topológica do terminal e os pacotes de dados já podem ser encaminhados correctamente para o mesmo. Por outro lado, quando um terminal se move entre células não é possível efectuar um *handover* suave. Desta forma, sempre que um terminal pretende fazer um *handover* entre células distintas ele tem de se registar na célula de destino de forma a que esta o aceite e comece a encaminhar pacotes de dados para ele. O processo é o mesmo descrito anteriormente para o registo do terminal na célula. A Figura 24 mostra um cenário de abandono da célula.

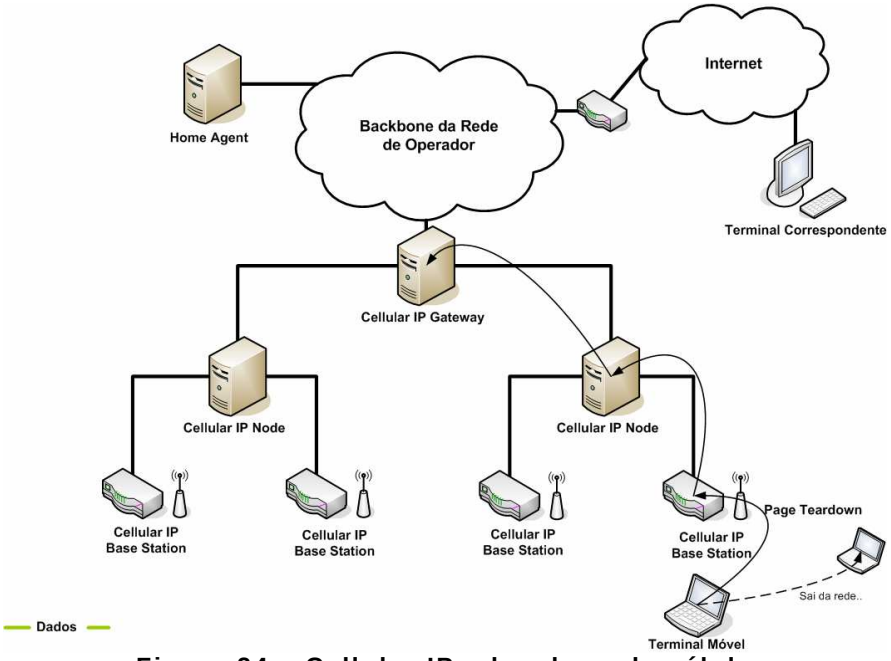


Figura 24 – Cellular IP, abandono da célula

Por fim, quando o terminal pretende deliberadamente abandonar a rede *Cellular IP*, este envia um pacote *Page Teardown,* tal como é ilustrado na Figura 24. Este pacote irá indicar a toda a célula que as rotas para este terminal devem ser eliminadas. Quando o terminal sai da rede inesperadamente e nenhum pacote é enviado a notificar o seu abandono, a rede destrói automaticamente as rotas para esse terminal após um período de tempo pré estipulado desde a ultima actualização das *Caches*.

2.8 Handoff-Aware Wireless Internet Infrastructure – (HAVAII)

Como já foi referido anteriormente o Mobile IP[8] é o protocolo clássico de mobilidade global, também designado por macro-mobilidade, nas redes de próxima geração. Contudo, o paradigma apresentado no modelo do *Mobile IP* necessita de ser substancialmente melhorado de forma a suportar ambientes de mobilidade local, também designados por ambientes de micro-mobilidade. O facto de o *Mobile IP* proporcionar *handovers* tipicamente lentos e fazer um grande uso de mensagens de controlo origina frequentemente problemas na recepção e transmissão de dados durante os mesmos. Outro problema acrescido é a dificuldade em suportar qualidade de serviço *(QoS)* em ambientes *Mobile IP*. O facto de o terminal mudar de endereçamento IP, *Care-of Address*, em cada *handover* efectuado dificulta o processo de manutenção das reservas de *QoS* e subsequentemente dificulta todo o processo de garantia de qualidade de serviço na rede. Desta forma a utilização do *Mobile IP* em redes de próxima geração poderá não ser suficiente para garantir um conjunto de requisitos que se esperam das redes do futuro. A Figura 25 descreve a arquitectura geral do HAVAII.

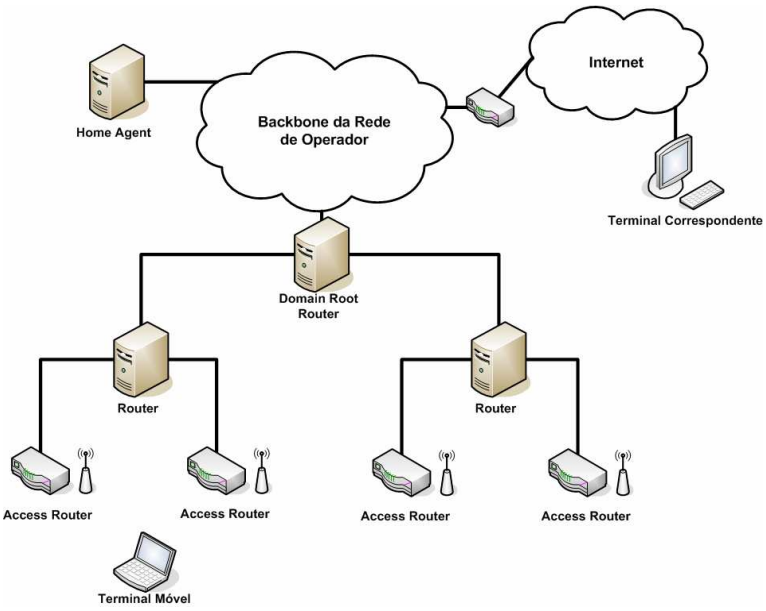


Figura 25 –HAVAII, arquitectura geral

Tal como no *Cellular IP* [9], o *HAVAII (Handoff-Aware Wireless Internet Infrastructure)* [12] baseia o seu mecanismo de mobilidade no facto de, probabilisticamente, o terminal se mover mais

frequentemente em determinadas áreas da rede, as quais são genericamente designadas por domínios locais ou micro-domínios. Consequentemente, protocolos como *HAVAII* [12] e o *Cellular IP* [9] criaram um novo processo de suporte à mobilidade em redes estruturadas o qual se designa por protocolo de mobilidade local ou micro-mobilidade. Nas redes *HAVAII* os terminais móveis mantêm o seu endereçamento IP durante os *handovers* dentro do mesmo micro-domínio. Desta forma, tal como já acontecia no *Cellular IP*, o *Home Agent* e os terminais correspondentes não são notificados da mobilidade do terminal móvel tornando assim a sua mobilidade transparente do ponto de vista do domínio global, ou seja da macro-mobilidade.

Apesar de no micro-domínio o protocolo de mobilidade ser o *HAVAII*, nesta arquitectura o mecanismo que dará suporte à mobilidade global continua a ser o *Mobile IP*. Esta conjunção da micro e macro mobilidade em domínios distintos na rede permitem aos protocolos como o *HAVAII* e *Cellular IP* minimizarem o impacto da mobilidade rápida nos recursos da rede assim como o distúrbio nas comunicações activas dos terminais. O *HAVAII* é um protocolo de micro-mobilidade hierarquizado que pode ser constituído por vários micro-domínios.

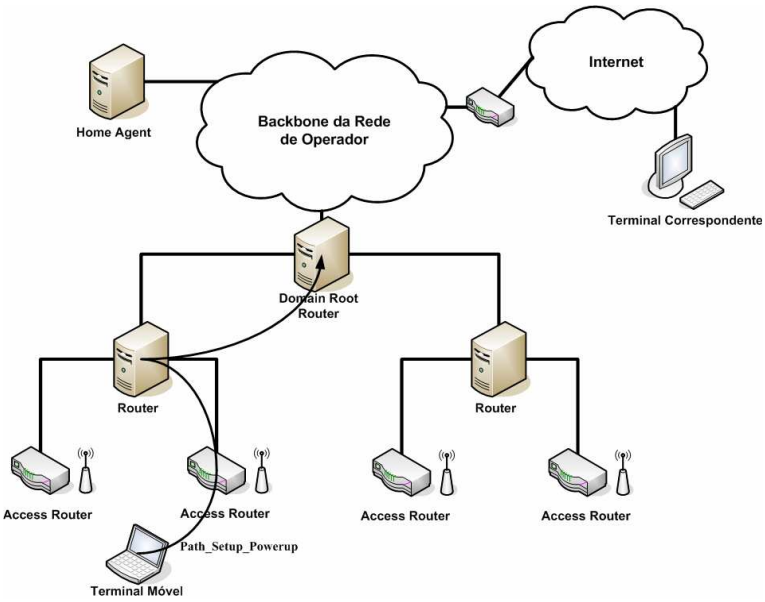


Figura 26 – HAVAII, registo na rede

Tal como no *Cellular IP* as rotas ao longo do micro-domínio são criadas através de pacotes de sinalização específicos que percorrem a rede desde o terminal móvel até ao *Domain Root Router*. Quando o terminal se liga na rede pela primeira vez, ele envia uma mensagem *path setup powerup message* indicando a sua presença e permitindo assim que a rede crie o encaminhamento desde o *Domain Root*

Router até ele. A Figura 26 descreve o processo de criação das primeiras rotas na rede do micro-domínio.

No *HAVAII*, tal como já acontecia anteriormente no *Cellular IP,* todos os *routers* do micro-domínio guardam as rotas para os terminais com base em *caches* do tipo *softstate.* As *caches softstate* são listas onde os elementos têm um prazo de validade. Dado que cada item da tabela tem um prazo de expiração, eles são auto-removidos pelo *router* a partir do momento que não forem refrescados periodicamente.

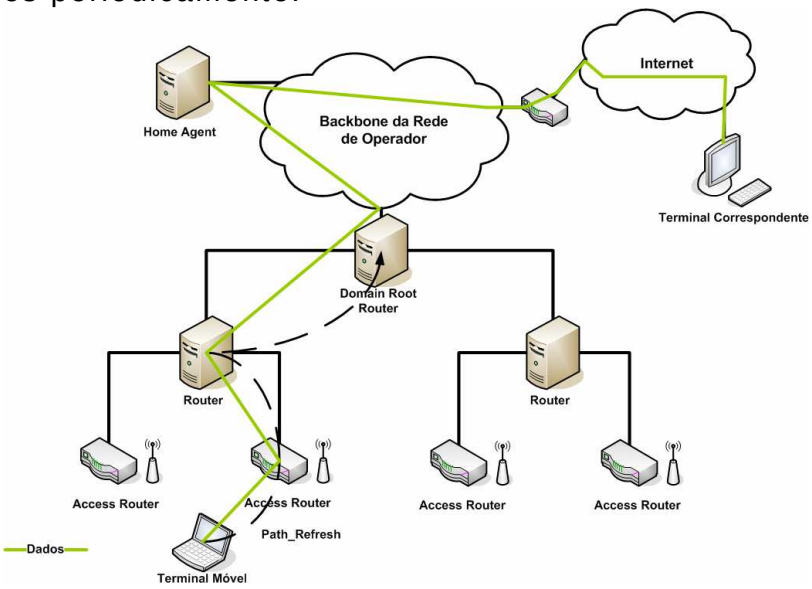


Figura 27 – HAVAII, refrescando as rotas na rede

A Figura 27 ilustra o processo de refrescamento de rotas no *HAVAII*. Este processo torna os protocolos de redes mais robustos e capazes de lidar com falhas de sinalização e inconsistências de rotas. Devido ao facto de todos os *routers* utilizarem *caches softstates* o terminal móvel, mesmo quando não está em movimento, tem que enviar periodicamente mensagens *path refresh messages* de forma a refrescar a sua entrada ao longo do Micro-Domínio. No *HAVAII* os *handovers* são efectuados segundo a política *Break-Before-Make*. Esta política, tal como já acontecia no *Cellular IP*, designa que os terminais efectuam sempre *handovers* reactivos. Como tal, quando um terminal móvel se move para um novo ponto de acesso, ele usa mensagens do tipo *path setup update messages* para actualizar a sua rota na rede. Estas mensagens só são enviadas depois de o terminal chegar ao *router* de destino. A Figura 28 descreve o procedimento de *handover* nas redes *HAVAII.*

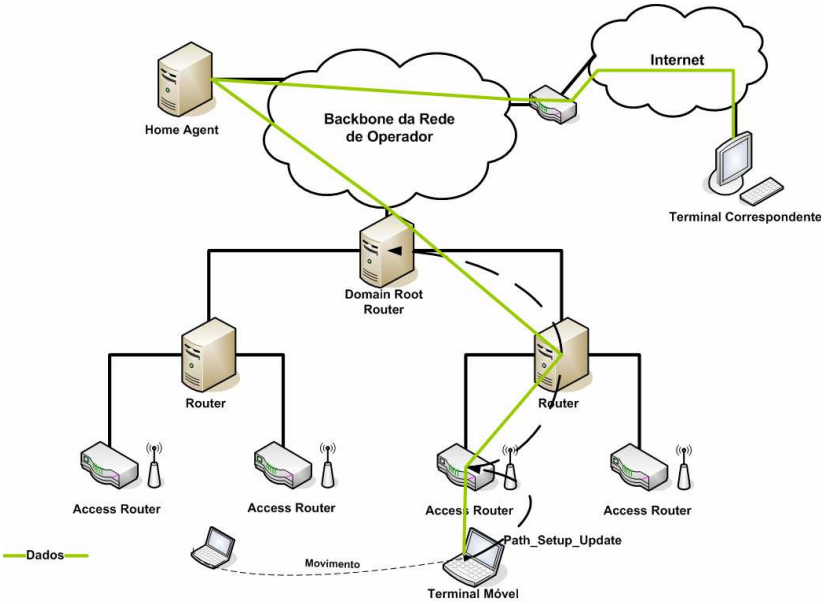


Figura 28 – HAVAII, procedimento de handover

Como pode verificado pela descrição efectuada anteriormente, o *HAVAII* é um protocolo muito semelhante ao *Cellular IP*. As grandes diferenças entre estes dois protocolos pretendem-se essencialmente no facto de o *HAVAII* não utilizar *Paging Areas*, visto ser uma propriedade das redes celulares, e oferecer o suporte nativo para qualidade de serviço (*QoS*). A qualidade de serviço é efectuada ao longo dos nós da árvore, através das mensagens *Path*, permitindo *QoS* por fluxo de dados mesmo em cenários de mobilidade. Por outro lado, o *Cellular IP* não garante reservas de qualidade de serviço na célula durante os cenários de mobilidade. Contudo, o *Cellular IP* efectua uma melhor utilização dos recursos de rede através dos processos de *paging* e de dualismo entre os estados activo ou dormente que o terminal pode oferecer. Por fim, pode-se concluir também que os mecanismos de suporte para mobilidade IP são em ambos muito semelhantes, efectuados através da propagação de mensagens especiais ao longo da rede do micro-domínio.

Capítulo III
Local-centric Mobility System (LMS)

3.1 Motivação

Os protocolos apresentados anteriormente demonstram ter alguns problemas, nomeadamente baixo desempenho durante os momentos de handover, inexistência de mobilidade local, demasiado overhead causado pela sinalização e pouca integração de serviços do ponto de vista das redes de operador. O facto de nenhum protocolo existente fornecer este tipo de características, motivou a arquitectura e posterior desenvolvimento do *LMS (Local-centric Mobility System)*. O *LMS* é um protocolo de redes de próxima geração que suporta mobilidade rápida em domínios locais, tem um baixo overhead causado pelo sinalização, integra suporte para *AAAC*, mecanismos de segurança e também conceitos de redes celulares tais como *Paging*. O desenvolvimento do *LMS* foi trabalho fundamental desta dissertação de mestrado.

3.2 Introdução

Existem várias soluções para proporcionar ambientes de mobilidade em redes IP contudo, tal como já foi abordado anteriormente, nenhuma das soluções é suficientemente eficaz em ambientes de operador. Em ambientes de operador onde as mobilidade dos terminais é constante torna-se obrigatório que os mecanismos de encaminhamento de pacotes suportem mobilidade rápida IP durante os momentos de *handover*. Por outro lado, neste tipo de redes é necessário maximizar a optimização dos recursos de rede tanto no núcleo da rede como na rede de acesso. Este tipo de considerações é de elevada relevância especialmente quando se pretende economizar recursos débito binário e espectro rádio nas redes de acesso. Quanto mais os terminais economizarem estes recursos, mas terminais poderão estar ligados nos mesmo pontos de acesso e por isso maior o sucesso do negócio do operador de telecomunicações. Assim, torna-se importante encontrar uma arquitectura e um protocolo que se aplique uniformemente a todos estes requisitos e que tome em atenção as necessidade base dos operadores de telecomunicações. No âmbito deste cenário, o *LMS* (*Local-centric Mobility System)* vem dar um contributo para a resolução das problemáticas apresentadas anteriormente, sendo

que ele acrescenta também algumas filosofias inovadoras ainda não totalmente implementadas por nenhum protocolo já existente.

O *LMS* é um sistema que tem como seu principal objectivo criar uma mobilidade localizada em micro-domínios permitindo desta forma diminuir os tempos de inoperatividade da rede durante os momentos de mobilidade do terminal. Pretendeu-se ainda que o sistema pudesse interagir com mecanismos frequentemente usados em ambientes de operador tais como, controlo de acesso, autorização, contabilidade e ainda facturação. Por fim falta ainda acrescentar que este sistema detém um conjunto de mecanismos de segurança que permitissem protege-lo de ataques de intrusos, essencialmente ataques ao bom funcionamento da rede de acesso e ataques de personificação de utilizadores fidedignos.

O *LMS* é um projecto que pretende criar um conjunto de funcionalidades que permita que as redes de próxima geração suportem terminais em ambientes de mobilidade rápida em redes IPv6. Este projecto desenvolveu-se após o estudo aprofundado e subsequente implementação de um protótipo do *Cellular IPv6* [10], que naturalmente lhe permitiu herdar um conjunto de características fundamentais das redes celulares IP. O *LMS* pretende enquadrar-se no grupo dos protocolos de mobilidade local (*Local Mobility Protocol – LMP)* sendo que parte dos seus fundamentos ideológicos foram fortemente influenciados pelos requisitos apontados pelo grupo *IETF NetLMM (Network-based Localized Mobility Management).*

3.3 Mobilidade LMS

O *LMS (Local-centric Mobility System)* é um sistema que implementa um protocolo próprio que proporciona um ambiente de mobilidade local em redes IPv6. Desta forma, este sistema possibilita que um terminal móvel possa comutar entre pontos de acesso sem infligir uma penalização na desempenho da sua ligação e nos recursos da rede de operador.

O *LMS* integra um protocolo de mobilidade local (Local Mobility Protocol - *LMP*). No *LMS* a rede é dividida em micro-domínios autónomos que gerem a sua rede de mobilidade independentemente do protocolo de mobilidade global utilizado. Desta forma, se for utilizado como protocolo de mobilidade global o *Mobile IPv6*, o terminal móvel apenas necessita de enviar um *Binding Update* quando muda de micro-domínio. Desta forma pode-se então dividir o processo de *handover* em dois tipos distintos:

- *Intra Micro-Domain Handover:* Transição entre Base Stations do mesmo domínio de mobilidade local

- *Inter Micro-Domain Handover:* Transição entre Base Stations de domínios de mobilidade local diferentes

A Figura 29 mostra a relação entre a *Mobilidade Global* e a *Mobilidade Local* em ambientes *LMS* (*Local-centric Mobility System)*.

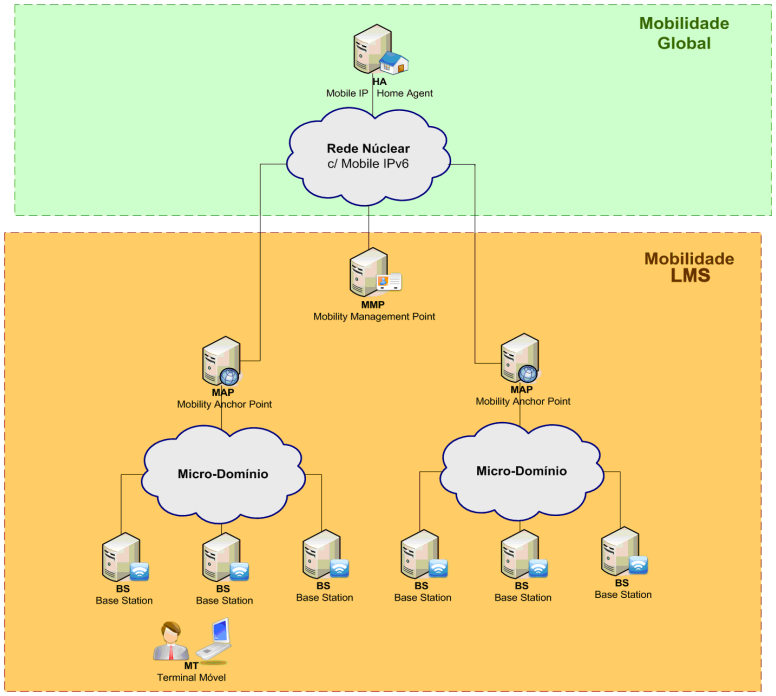


Figura 29 – LMS, mobilidade LMS e mobilidade global

3.4 Mobilidade Local em Micro Domínios

O *LMS* implementa um cenário explicitamente de mobilidade local. Neste conceito, todos os terminais móveis são inseridos em micro-domínios de mobilidade perante os quais devem efectuar todas as considerações de segurança relativas às políticas de segurança definidas pelo operador. Poderá compreender-se os micro-domínios como pequenas redes de acesso que aglomeram um conjunto bem definido de *Base Stations* que possibilitam por sua vez que o terminal móvel as use como ponto de acesso à rede.

Associado a cada micro-domínio está um domínio de rede IPv6. Desta forma, dentro do mesmo domínio todas as *Base Stations* do micro-domínio anunciam o mesmo prefixo de rede IPv6, permitindo assim que os terminais se movam dentro do domínio sem necessitarem de alterar o seu endereço IPv6 *(CoA – Care of Address)*. A este tipo de transição interna no micro-domínio designa-se por *Intra Micro-Domain Handover*, que será explicado na secção de *handovers*. Cada micro-domínio *LMS* tem uma chave secreta única que serve para derivar *PIDs (Personal IDentifiction)* para cada terminal móvel ancorado a ele. Estes *PIDs* servem para o terminal poder assinar todos os seus pacotes de controlo garantindo assim que não serão possíveis ataques de personificação.

A cada micro-domínio pode estar associado um nível de acesso distinto. Desta forma, poderá definir-se que um dado micro-domínio é restrito e que apenas determinados terminais móveis, devidamente especificados no servidor de *AAAC*, podem aceder ao mesmo. Esta flexibilidade permite estender o conceito de rede de operador a um nível mais avançado permitindo assim criar espaços de acesso reservados a determinados clientes da rede. No *LMS* pode-se então definir os micro-domínios em dois tipos diferentes: *Acesso Restrito* e *Acesso Total.* Devido à forma como os agentes da rede do micro-domínio comunicam, no *LMS* é possível criar espaços preenchidos por *Base Stations* pertencentes a micro-domínios diferentes, inclusive de categorias de acesso distintas. Desta forma, é possível misturar no mesmo conjunto, *Base Stations de Acesso Restrito* e *Base Stations de Acesso Total*, pertencentes a domínios de *Acesso Restrito* e domínios de *Acesso Total* respectivamente. Na Figura 30 pode-se ver um exemplo de um micro-domínio misto, onde as células mais escuras são espaços de *Acesso Restrito* e as mais claras são espaços de *Acesso Total.*

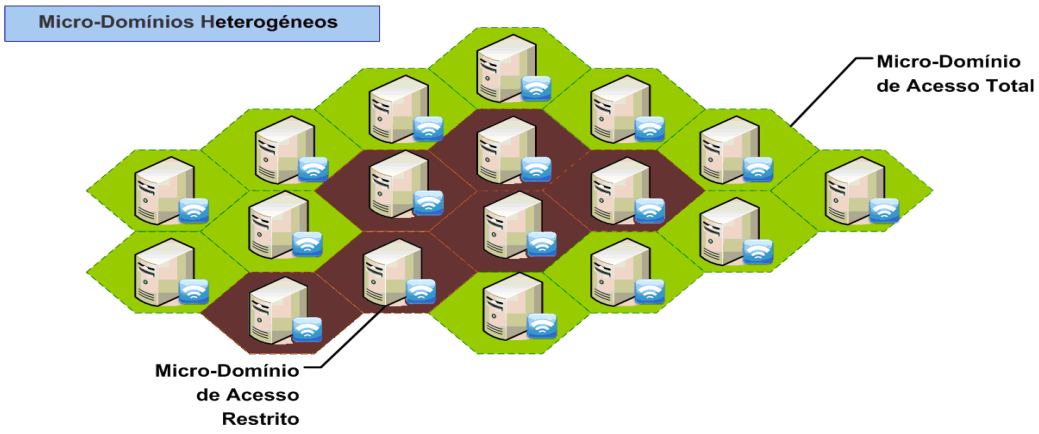


Figura 30 – LMS, representação de um cenário de Micro-Domínios heterogéneos

Um micro-domínio *LMS* é constituído por um *MAP – Mobility Anchor Point* e uma ou mais *Base Stations*. A relação entre estes agentes é hierárquica sendo que todas as *Base Stations* obedecem ás ordens do *MAP* do seu micro-domínio. O *MAP* é o responsável por todo o micro-domínio, e por essa razão é ele que controla o acesso à rede, contabiliza todo fluxo de dados e também é ele que negoceia os processos de *handover* requeridos pelos terminais móveis.

Como funcionalidade acrescida, o *MAP* tem ainda como sua responsabilidade configurar todas as *Base Stations* do seu micro-domínio. Este ponto será descrito com maior detalhe um pouco mais à frente na secção de auto-configuração da rede. Sempre que o *MAP* necessita de tomar uma decisão que não depende apenas do seu próprio domínio, mas sim da rede global de operador, ele questiona o *MMP (Mobility Management Point)* sobre qual a decisão a tomar perante a situação em que este se encontra. O *MAP* é também o responsável pela criação, gestão e controlo de todos os grupos Multicast usados para encaminhar os dados na rede nuclear do micro-domínio. Este ponto é também detalhado com maior pormenor um pouco mais a frente na secção *Multicast*. Por fim, falta ainda acrescentar, que o *MAP* é o responsável pela ligação de comunicação de dados entre o micro-domínio e a Internet. Ou seja, o *MAP* é responsável por encaminhar todos os pacotes do micro-domínio para a Internet e vice-versa, tendo sempre em consideração as politicas de acesso da rede. A Figura 31 ilustra a arquitectura de um micro-domínio *LMS*.

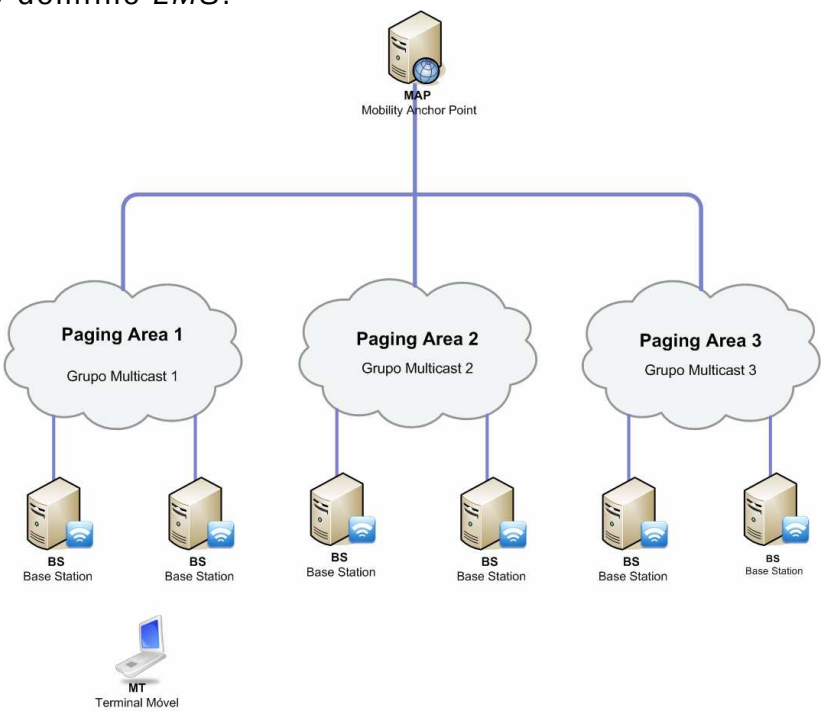


Figura 31 – LMS, Micro-Domínios

Poderá assim compreender-se um micro-domínio *Local-centric Mobility System* como uma rede autónoma constituída por dois tipos de agentes, *MAP* e Base Stations, onde devido ao tipo de hierarquização o *MAP* é o responsável total por todo o micro-domínio ao qual pertence.

3.5 Entidades da Arquitectura

O *Local Mobility System (LMS)* contempla 5 (cinco) agentes principais que definem a sua arquitectura.

MMP – Mobility Management Point

Este agente tem como principal objectivo efectuar a gestão sobre a mobilidade e *AAAC* da rede *LMS*. O *MMP* tem ainda a funcionalidade de um *Broker,* sendo assim um agente que pode negociar acções e enviar políticas com qualquer *Mobility Anchor Point (MAP)* de cada Micro-Domínio sempre que necessário. O *MMP* é ainda o responsável pela auto-configuração de todos os *MAP*s e todos os Micro-Domínios

MAP – Mobility Anchor Point

Este agente é responsável por toda a gestão do seu Micro-Domínio. O *MAP* funciona também como *gateway* dessa rede localizada e controla os fluxos de dados de todos os terminais móveis. O *MAP* é ainda o responsável pela auto-configuração de todas as *Base Stations*

BS - Base Station

Este agente é responsável por manter a interligação entre a rede do Micro-Domínio e os terminais móveis.

MT – Terminal Móvel

Este agente é responsável por efectuar toda a sinalização, e configuração necessária para que o terminal do utilizador móvel possa ser compatível com a rede *LMS*.

CDB – Base de Dados Central (Central Data Base)

Este agente é um sistema de gestão de base de dados onde são guardadas todas as informações referentes aos terminais assim como todas as informações referentes à configuração da rede de operador.

3.6 Gestão centralizada da rede

A rede promovida pelo *Local-centric Mobility System* é gerida de forma centralizada através de um mecanismo de configuração automática dos agentes. Desde o inicio da sua arquitectura deu-se elevada importância à necessidade de criar mecanismos que centralizem o poder de gestão da rede de forma a facilitar o processo de instalação e configuração dos agentes de mobilidade *LMS*. Num cenário de operador, o facto de a gestão dos dispositivos poder ser centralizada e a sua configuração ser automatizada permitirá um processo de integração mais simples e rápida resultando numa redução de custos para o operador. Desta forma, pretende-se que o instalador apenas necessite de ligar o dispositivo de mobilidade, por exemplo uma Base Station, na rede e que todo o processo de configuração seja feito automaticamente de uma forma simples e rápida.

Outro motivo importante foi a necessidade de centralizar o controlo de contabilidade, gestão de acessos e autorização dos diferentes micro-domínios. Este processo de centralização dos mecanismos de *AAAC* permite ao *LMS* adaptar-se melhor aos ambientes de operador em redes de próxima geração. Com base no *AAAC*, nos cenários *LMS* é possível criar zonas de *Acesso Restrito* e *Acesso Total*, tal como já foi abordado na secção anterior, permitindo criar células onde apenas determinados terminais pode aceder. Durante os momentos de *handover* Inter Micro-Domain, o *AAAC* é consultado para verificar se o terminal móvel pode mover-se para esse domínio.

No *LMS* o agente responsável pelos serviços de *AAAC* é o *MMP* (*Mobility Management Point)*. Este agente é responsável por um determinado conjunto de micro-domínios e gere todo o processo de autenticação, controlo de acesso, contabilidade e facturação. Os serviços de *AAAC* fazem parte integrante do *MMP* e as suas informações são guardadas numa base de dados relacional *SQL*. Por razões de integração com outros sistemas, o *MMP* pode ser integrado com um agente externo que providencie os serviços de *AAAC* tal como por exemplo um servidor *RADIUS*, delegando assim estas responsabilidades.

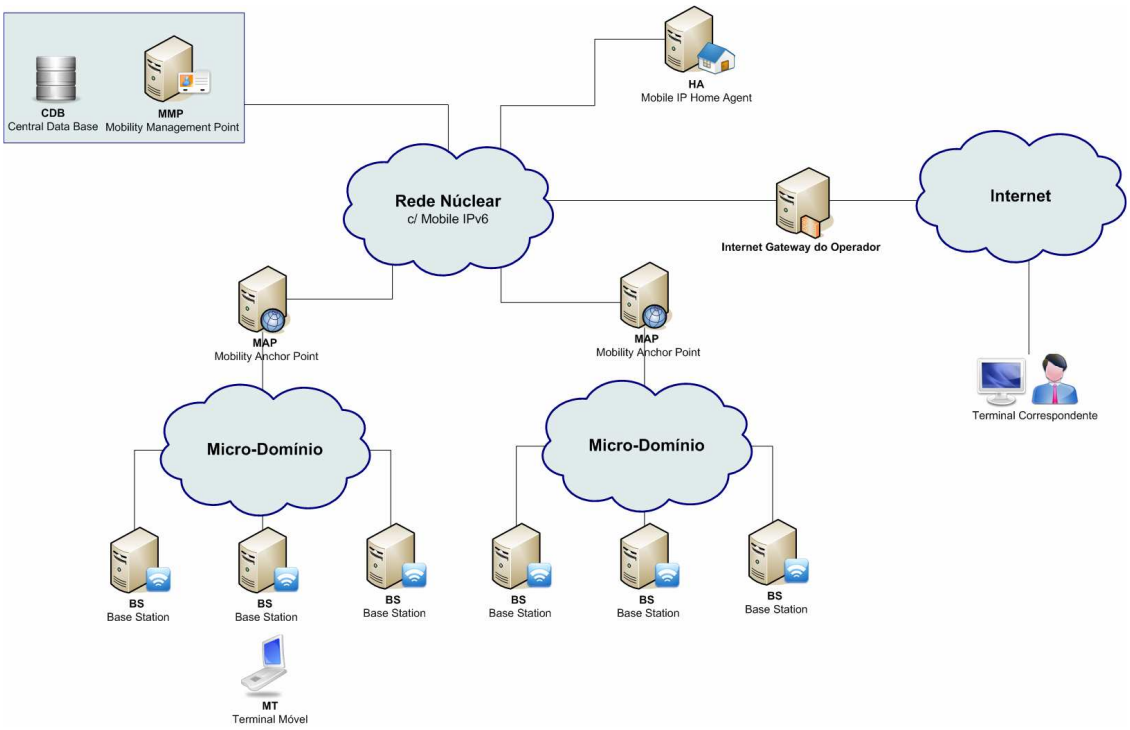


Figura 32 – LMS, arquitectura da rede

Por questões de escalabilidade, a base de dados relacional que suporta os serviços de *AAAC* e também as informações de auto-configuração dos agentes de mobilidade *LMS,* encontra-se autónoma do *MMP.* Isto traduz-se numa interacção do tipo cliente/servidor entre o *MMP* e o servidor da base de dados relacional. Visto que a base de dados detém mecanismos de acesso por exclusão mutua, é ainda possível que vários agentes *MMP* partilhem a mesma informação contida na base de dados relacional. Este tipo de arquitectura distribuída permite que o *LMS* possa ser integrado em ambientes de larga escala de forma simples e exequível. A Figura 32 ilustra a arquitectura global da rede incluindo os agentes de gestão de mobilidade e a base de dados central.

A Figura 32 ilustra uma arquitectura *LMS* de rede de operador gerida apenas por um único *MMP*. Alternativamente o *LMS* possibilita criar uma arquitectura de gestão balanceada entre diferentes pontes de gestão, dividindo as tarefas de decisão e negociação por diferentes agentes *MMP* ao longo da rede nuclear de operador. Este tipo solução é especialmente vantajosa em cenários onde existem vários micro-domínios com milhares de terminais móveis em constante movimento na rede resultando assim num constante número de pedidos de decisão e negociações por parte do *MMP*. Por conseguinte, nos cenários *LMS* é possível atribuir a responsabilidade de gestão de vários micro-domínios por diferentes *MMP* e desta forma balancear a carga de gestão dos mesmo. Este

balanceamento de carga torna a rede mais escalável e robusta permitindo que esta seja utilizável em cenários realistas em ambientes de produção. A Figura 33 mostra um possível cenário *LMS* onde a integração de vários *MMPs* pode criar um sistema de balanceamento de carga de gestão da rede de operador.

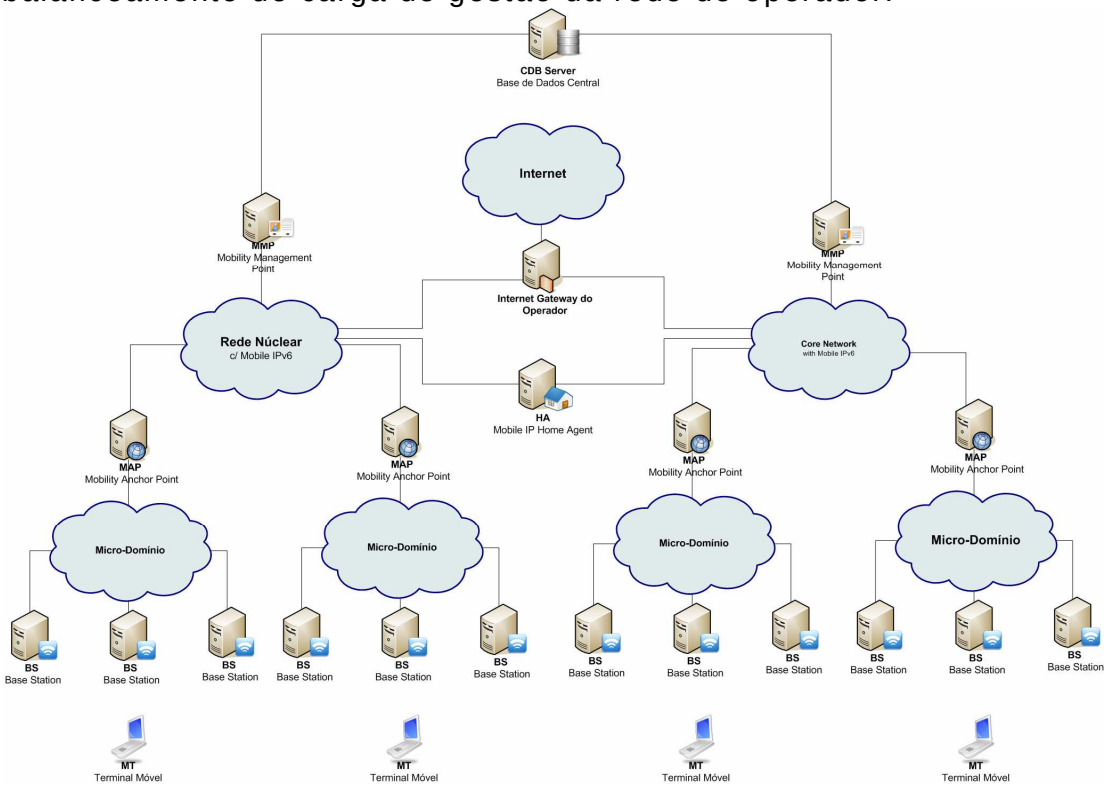


Figura 33 – LMS, cenário demonstrativo da escalabilidade do LMS

Como também pode ser observado na Figura 33, a cada *MMP* é associado um conjunto de micro-domínios dos quais este se torna responsável máximo. Neste caso, cada *MAP* de cada um dos micro-domínios comunica directamente com o seu *MMP* responsável sempre que necessita de tomar uma determinada decisão. Esta filosofia é muito semelhante à usada no Policy Base Management [22], onde o *MMP* se assemelha ao *PDP (Policy Decision Point)* e o *MAP* ao *PEP (Policy Enforcement Point).*

Com base na informação do *AAAC*, o *MMP* é responsável por decidir se um determinado terminal móvel pode ou não registar-se num determinado micro-domínio assim como se este pode ou não efectuar um determinado *handover*. O *MMP* é também o responsável por negociar o *handover* entre *MAPs* distintos *(Inter Micro-Domain Handover)*, mesmo que o *MAP* de destino não pertença ao conjunto dos *MAPs* dos quais ele é responsável.

Faz também parte das responsabilidades do *MMP*, registar toda a contabilidade dos terminais móveis ancorados a cada um dos *MAPs* dos quais ele é responsável. Este registo é efectuado através dos serviços de *AAAC* e a informação encontra-se sempre disponível ao acesso de qualquer *MMP* da rede. Assim, é possível que qualquer *MMP* verifique a relação *Facturação/Contabilidade* (*Charging / Accounting)* decidindo quando é que um dado terminal móvel deve ou não deixar de transmitir dados na rede porque, por exemplo, ultrapassou o seu limite de carregamento.

Por fim falta ainda referir que o *MMP* é o responsável também pelo registo dos *MAP*s na rede. Sempre que um *MAP* se liga na rede, este automaticamente inicia um processo de registo com o seu *MMP* responsável. Durante este processo de registo o *MMP* é também o responsável por informar o *MAP* de qual a configuração que ele deve adoptar para o seu micro-domínio, tais como prefixo de rede *(Network Prefix IPv6 Address)*, chave de rede (*Network Secret Key)*, entre outras configurações. Caso não sejam integrados outros agentes de gestão no sistema, com por exemplo um servidor *RADIUS*, a *Base de Dados Central* pode assumir o controlo total de toda a informação da rede. Desta forma todas as informações referentes aos serviços *AAAC* ficam automaticamente guardadas na *Base de Dados Central* permitindo que qualquer *MMP* da rede possa usufruir da mesma para efectuar as suas decisões.

Por outro lado, num cenário de inter operabilidade entre o *MMP* e outros agentes de gestão, tais como um servidor *RADIUS*, a *CDB (Base de Dados Central)* servirá exclusivamente para conter informação sobre os *MAPs* e os seus micro-domínios, servindo assim apenas como fonte de informação para a auto-configuração da rede.

3.7 Base de Dados Central (CDB)

A *CDB (Base de Dados Central)* é uma base de dados relacional que contem toda a informação referente ao sistema *Local-centric Mobility System*. Nela são guardadas informações referentes à configuração dos micro-domínios, configuração dos *MAPs* e configuração dos terminais móveis, Permissões de *Acesso, Autorização e também Contabilidade e Facturação (AAAC).* A *CDB* foi desenvolvida com o principal intuito de permitir guardar a informação referente a auto-configuração de toda a rede. Pretendia-se assim que através da *CDB* fosse possível ao operador guardar todos os dados referentes a cada micro-domínio e assim pudesse ,de uma forma centralizada, configurar toda a rede de operador.

Por forma a tornar o sistema mais flexível, a base de dados foi também desenhada para poder suportar o controlo de *Acessos, Autorização, Contabilidade e Facturação* (*AAAC*) dos terminais móveis. Alternativamente os serviços de *AAAC* podem estar num servidor externo, como por exemplo um *RADIUS*. Assim, por omissão, o sistema suporta todas estas funcionalidades descritas anteriormente directamente na *CDB*, sendo que o seu controlo é efectuado sempre por agentes *MMP*.

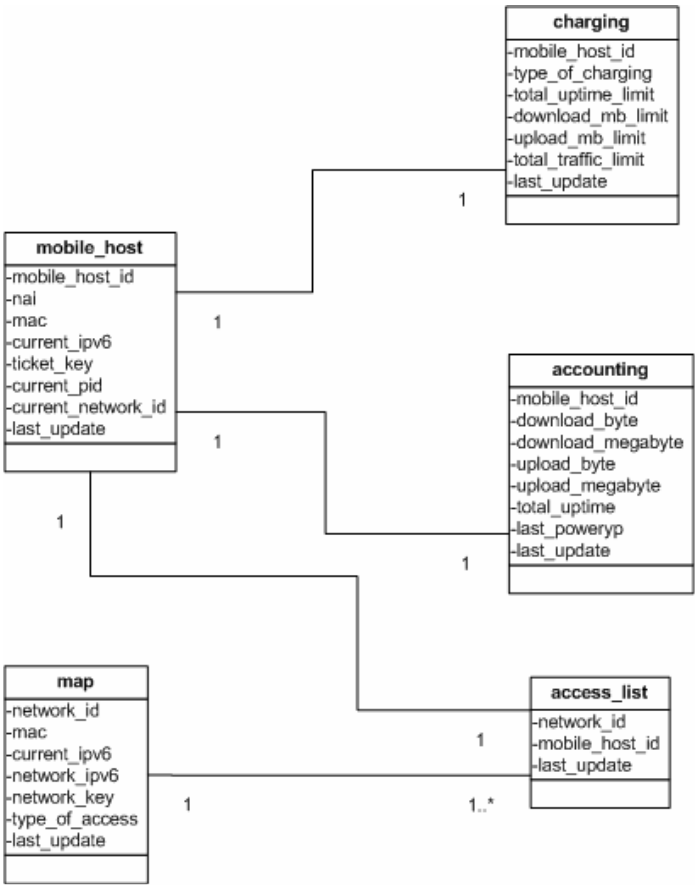


Figura 34 – LMS, diagrama de classes UML da estrutura da Base de Dados Central

A *CDB (Base de Dados Central)* usada no protótipo foi desenvolvida sobre um *SGBD (Sistema de Gestão de Base de Dados).* O *MMP* utiliza a tecnologia *SQL* para interagir com a base de dados e obter as informações que necessita para formalizar as decisões e politicas de rede. A Figura 34 demonstra o diagrama de classes *UML* que representa a estrutura da *CDB* do *Local-centric Mobility System*.

No protótipo do *LMS*, desenvolveu-se uma aplicação de interface com o utilizador (administrador da rede) que permite gerir toda a *CDB.* Esta aplicação permite registar novos terminais móveis na rede, registar *MAPs,* carregar (*Charging*) terminais móveis, consultar a contabilidade dos mesmos (*Accounting)* e gerir permissões de acesso (*Access)* aos diferentes micro-domínios.

Tal como se pode verificar, a opção de utilizar um sistema de gestão centralizado com múltiplos acessos à informação através dos diferentes *MMPs* possibilita uma flexibilidade, expansibilidade e simplicidade de utilização muito vantajosa para um sistema desta categoria, essencialmente ao nível das redes de operador.

3.8 Auto-Configuração da rede.

Desde do inicio da arquitectura deste sistema teve-se como forte convicção que algo muito importante para integração de uma rede de operador é a simplicidade de instalação de novos componentes/agentes na mesma pois só assim se poderá expandir a rede a baixo custo temporal e monetário. Desta forma optou-se pode desenvolver um mecanismo que permitisse a auto-configuração quase total de todo e qualquer componente/agente que fosse inserido na rede.

Como acréscimo, pretendia-se também que fosse possível inserir um novo componente na rede sem que fosse necessário reiniciar a mesma, ou seja, pretendia-se que o sistema permitisse a integração de novos componentes/agentes em tempo de execução (*runtime*) . Desta forma, resumindo, pretendia-se construir um sistema que, apesar de complexo, fosse extremamente fácil de expandir, onde todas as suas configurações pudessem ser alteradas a qualquer momento através de ordens dos *MMPs* sem que fosse necessário reiniciar total ou parcialmente a rede para o concretizar. Este tipo de mecanismo permite ainda aumentar a segurança e estabilidade dos agentes, visto que a configuração de cada um deles é dada sempre por agentes de confiança, as Base Stations confiam nos *MAPs* e os *MAPs* confiam nos *MMPs*. Assim é possível criar um sistema de configuração hierárquico, onde o *MMP* configura os *MAP*s e os *MAPs* configuram as *Base Stations*. Outra vantagem deste tipo de mecanismo é que desta forma é possível reduzir os erros humanos causados por más configurações que por vezes causam instabilidade na rede ou até a sua falha de execução. Como tal, este ponto mostrou-se bastante importante para o desenho e desenvolvimento do *LMS*.

O funcionamento da auto-configuração é baseado num mecanismo de sinalização suportado por *sockets TCP*. Todos os *MMPs* e todos os *MAPs* integram um servidor que pode suportar múltiplos pedidos de configuração em simultâneo. As *Base Stations* são os únicos agentes da rede que não integram nenhum servidor de configuração sendo apenas clientes. Todos os *MAPs* para além de um servidor de configuração de *Base Stations* também integram um cliente de configuração que comunica com o servidor integrado nos *MMPs,* e que permite aos *MAPs* configurarem-se segundo as ordens dos *MMPs*. Ao contrario dos *MAPs* e das *Base Stations,* o *MMP* é o único que não é configurado remotamente por nenhum agente não tendo assim nenhum cliente de auto-configuração integrado nele. A configuração do *MMP* é feita manualmente pelo administrador de rede.

a. Auto-Configuração do MAP

A configuração de um *MAP* começa quando este se liga na rede. Inicialmente o agente envia uma mensagem de *MAP Registration Request* para o seu *MMP* associado, contendo todas as informações referentes ao seu registo na *Base de Dados Central*. O *MMP*, ao receber o pedido de registo vai automaticamente tentar valida-lo, sendo que para isso ele questiona a *Base de Dados Central* por forma a obter todas as informações relativas a configuração deste *MAP*. Após ter efectuado esse pedido, o *MMP* constrói uma mensagem *Registration Response* e envia para o *MAP* com todas as informações necessárias para a sua auto-configuração: *network_ipv6, network_key* e *type_of_access*. O *MAP* após receber o *MAP Registration Response* já pode efectuar a sua auto-configuração e subsequentemente a configuração do seu micro-domínio.

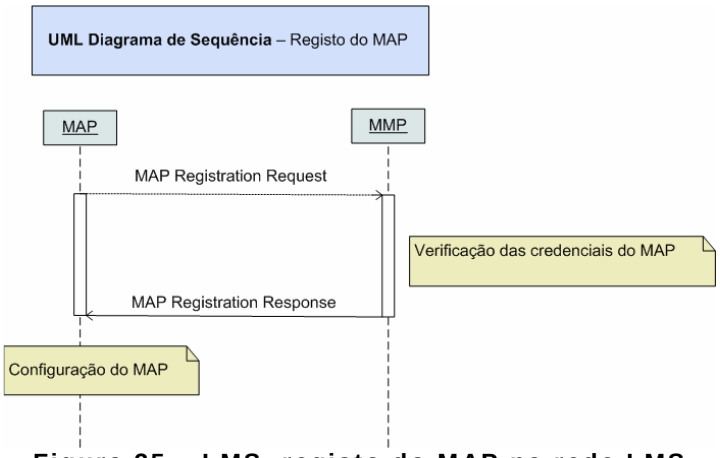


Figura 35 – LMS, registo do MAP na rede LMS

A Figura 35 mostra o processo de sinalização que é efectuado durante o registo do *MAP* no *MMP* durante o processo de auto-configuração.

Visto que a rede entre o *MAP* e o *MMP* pode ser potencialmente insegura, já que também da acesso a Internet, torna-se necessário contemplar algum tipo de mecanismo de segurança. Desta forma, as mensagens trocadas entre o *MAP* e o *MMP* são sempre assinadas pelo emissor. A assinatura é efectuado através de um processo de *digest* e depende de uma chave identificadora partilhada pela rede de operador que identifica inequivocamente que aquele agente pertence à mesma. A Figura 36 ilustra o diagrama de actividade do processo de registo do *MAP* na rede.

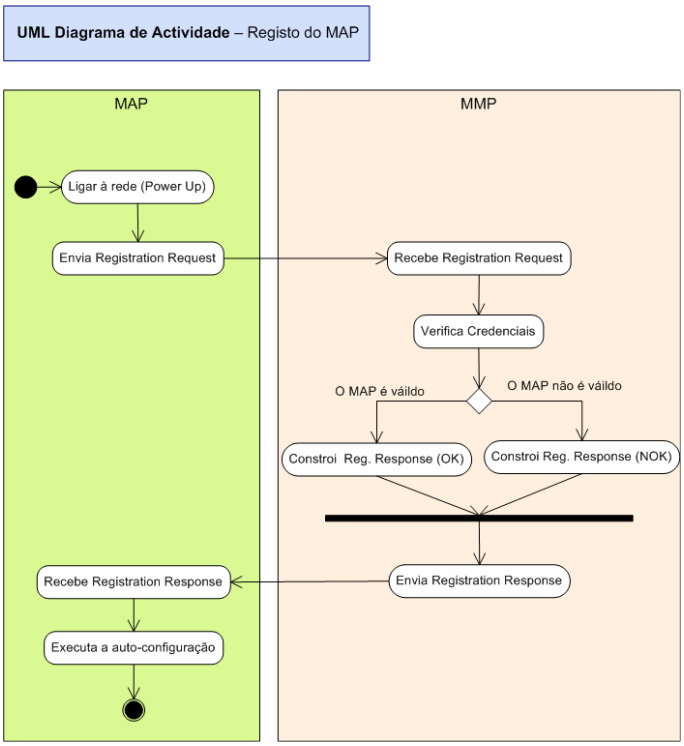


Figura 36 – LMS, diagrama do processo de registo do MAP

b. Auto-configuração da Base Station

Tal como o *MAP* a *Base Station* também tem um mecanismo de auto-configuração na rede que se inicia quando esta se liga na mesma. Inicialmente a *Base Station* envia uma *BS Registration Request* indicando que pretende efectuar um registo no micro-domínio. O *BS Registration Request* enviado pela Base Station contem a indicação da *Paging Area* onde esta pretende pertencer. Desta forma, o *MAP* ao receber o pedido de registo verifica se a *Paging Area* requerida já está a ser usada por mais alguma *Base Stations* do micro-domínio. No caso da *Paging Area* já estar activa, o *MAP* adiciona a Base Stations à *Multicast Group List* (cache interna) e envia um *BS Registration Response* indicando qual o IPv6 do grupo multicast e o porto usado para essa *Paging Area*. Caso a *Paging Area* ainda não exista, o *MAP* gera um endereço IPv6 para o novo grupo multicast e um porto para esta nova *Paging Area*, associando assim a nova *Paging Area* ao novo grupo multicast. Após isto, o *MAP* adiciona a *Base Station* à *Multicast Group List* e à *BS Cache* (cache interna) enviando seguidamente um *BS Registration Response* indicando qual o IPv6 do grupo e o porto para a *Paging Area* requerida. No *Registration Response*, em ambos os casos, também é indicado qual a chave da rede (*Network Key)* e o prefixo de rede (*Network IPv6 Prefix Address*).

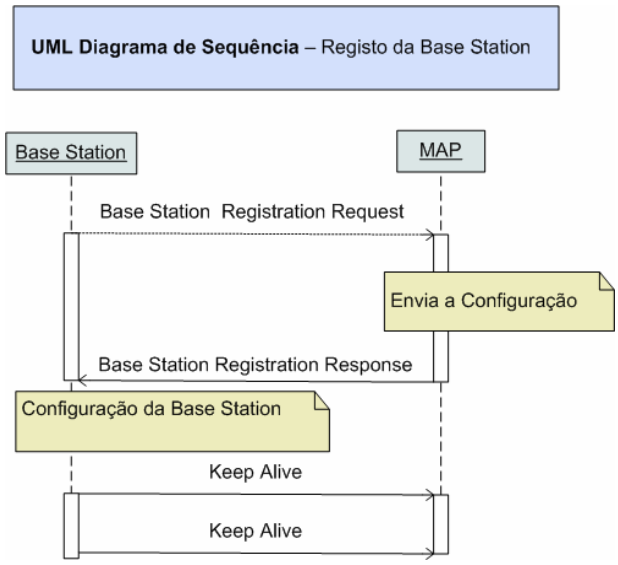


Figura 37 – LMS, registo da Base Station na rede

A *Base Station* após receber o *BS Registration Response* junta-se ao grupo multicast e configura o seu endereço IPv6 do interface de rede que comunica com os terminais móveis com base no prefixo de rede e no seu *Mac Address*. Por fim a Base Station necessita de periodicamente enviar uma mensagem de *Keep Alive* para o *MAP* por

forma a que ele a mantenha activamente relacionada com a *Paging Area* e consequentemente com o grupo multicast a onde ela pertence. Note-se que caso o tempo de refrescamento expire antes da chegada de um *Keep Alive*, o *MAP* procederá à remoção desta *Base Station* da *BS_Cache* e da *Paging Area* também. Todas as caches no *LMS* sofrem do efeito de *softstate* e têm que ser refrescadas periodicamente por razões de estabilidade e robustez. O mecanismo de registo pode ser observado na Figura 37.

Sempre que o *MAP* efectua a verificação dos tempos de refrescamento de todas as Base Stations este verifica também se cada uma das *Paging Areas* activas contêm pelo menos uma *Base Station* associada a ela. No caso de o *MAP* detectar que uma *Paging Area* activa não têm nenhuma *Base Station* associada a ela, então ele remove essa *Paging Area* e desassocia-se do grupo multicast correspondente.

A Figura 38 mostra o diagrama de actividade UML referente ao registo da Base Station no micro-domínio.

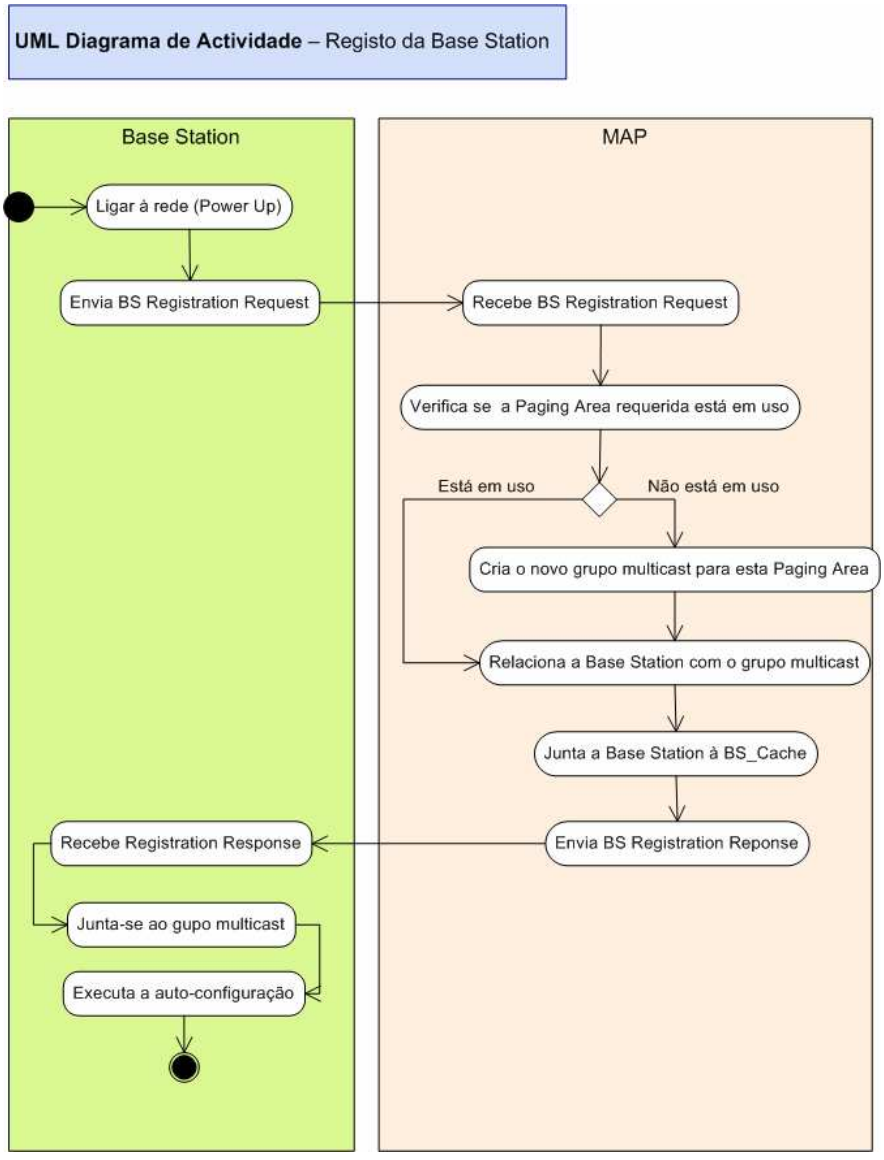


Figura 38 – LMS, diagrama de actividade UML do registo da Base Station na rede

c. Auto-Configuração do MMP

O *MMP – Mobility Management Point* não tem nenhum mecanismo de auto-configuração já que a sua configuração é extremamente simples e pode ser perfeitamente efectuada através de ficheiros de configuração.
Note-se que, em traços gerais, para configurar um *MMP* apenas é necessário indicar qual o caminho para o SGBD da *Base de Dados Central*.

d. Auto-Configuração do Terminal Móvel

O terminal móvel é totalmente auto-configurável pela rede *Local-centric Mobility System*. Quando o terminal se liga na rede, este começa por enviar uma mensagem *MH Registration Request* com as suas credenciais, indicando qual o seu *NAI – Network Access Identification*, o seu *Ticket Key* e qual o micro-domínio a onde pretende aceder.

O pacote referente à mensagem *MH Registration Request* é directamente injectado na rede, sendo que o terminal não necessita de ter um endereço IPv6 pré-configurado para o fazer. O pacote é posteriormente recebido pela *Base Station* mais próxima e é enviado directamente para o *MMP* através do *MAP*, sem qualquer tipo de verificação prévia. Note-se que nem a Base Station nem o *MAP* têm como verificar se o terminal móvel é fidedigno enquanto este não efectuar um registo no *MMP* e obtiver um *PID* para assinar todos os seus pacotes de controlo. Note-se também que nem o *MAP* nem a Base Station conseguem validar o *ticket_key* enviado pelo terminal móvel durante o registo pois só o *MMP* tem acesso a *Base de Dados Central* do sistema por razões de segurança.

O *MMP* após receber o pacote de registo reencaminhado pelo *MAP* e efectuar a verificação da sua autenticidade, verifica se o terminal pode aceder ao micro-domínio requerido. Nesta situação o *MMP* pode estar perante dois cenários distintos: o micro-domínio é do tipo *Acesso Total*; o micro-domínio é de *Acesso Restrito*.

No caso de o domínio pretendido ser de acesso total, o *MMP* pode automaticamente gerar um *PID* e um novo IPv6 para o terminal usar nesse micro-domínio. Seguidamente o *MMP* constrói a mensagem *MH Registration Response* e envia para o terminal móvel através do *MAP.* No caso do micro-domínio ser de *Acesso Restrito*, então o *MMP* irá verificar se o terminal consta na lista de terminais

com acesso a esse micro-domínio especifico. Caso o *MMP* verifique que o terminal pode aceder a esse micro-domínio, então gera um *PID* e um endereço IPv6 para o mesmo e envia um *MH Registration Response* através do *MAP*. O *MAP* recebe o *MH Registration Response* vindo do *MMP* e verifica se o terminal foi ou não aceite no seu micro-domínio. Se sim, então regista o terminal nas suas *caches* e envia um *Page Update* para toda a *Paging Area* registando o terminal em todas as Base Stations da mesma. Caso não tenha sido aceite pelo *MMP*, o *MAP* não efectua nenhuma operação. Em ambos os casos o *MAP* reencaminha *MH Registration Response* para o terminal através da *Base Station* por onde este enviou o *MH Registration Request*. Por fim, o terminal recebe a resposta ao seu pedido de registo e com base na resposta efectua a configuração dos interfaces de rede. No caso da resposta ter sido de acesso negado o terminal mostra uma mensagem de acesso negado e tenta ligar-se mais tarde. A Figura 39 descreve o diagrama de sequencia do registo do terminal na rede.

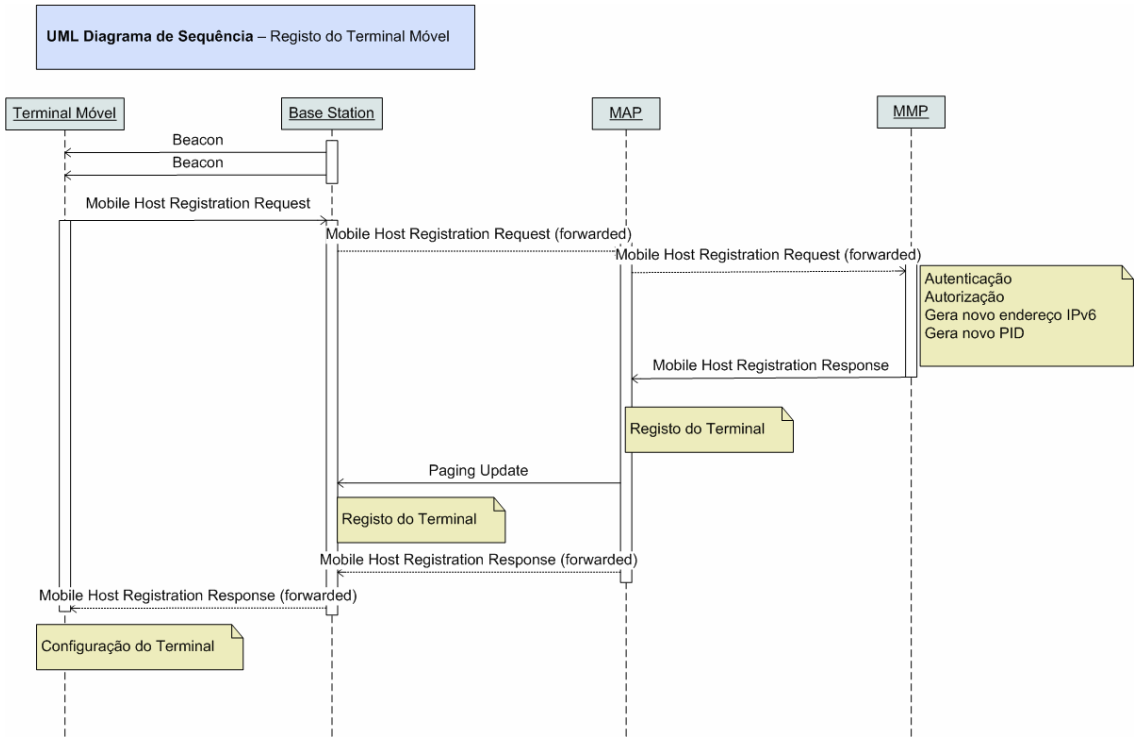


Figura 39 – LMS, diagrama de sequência UML referente ao registo do terminal na rede

A próxima figura (Figura 40) representa o diagrama de actividade do terminal móvel durante o registo na rede.

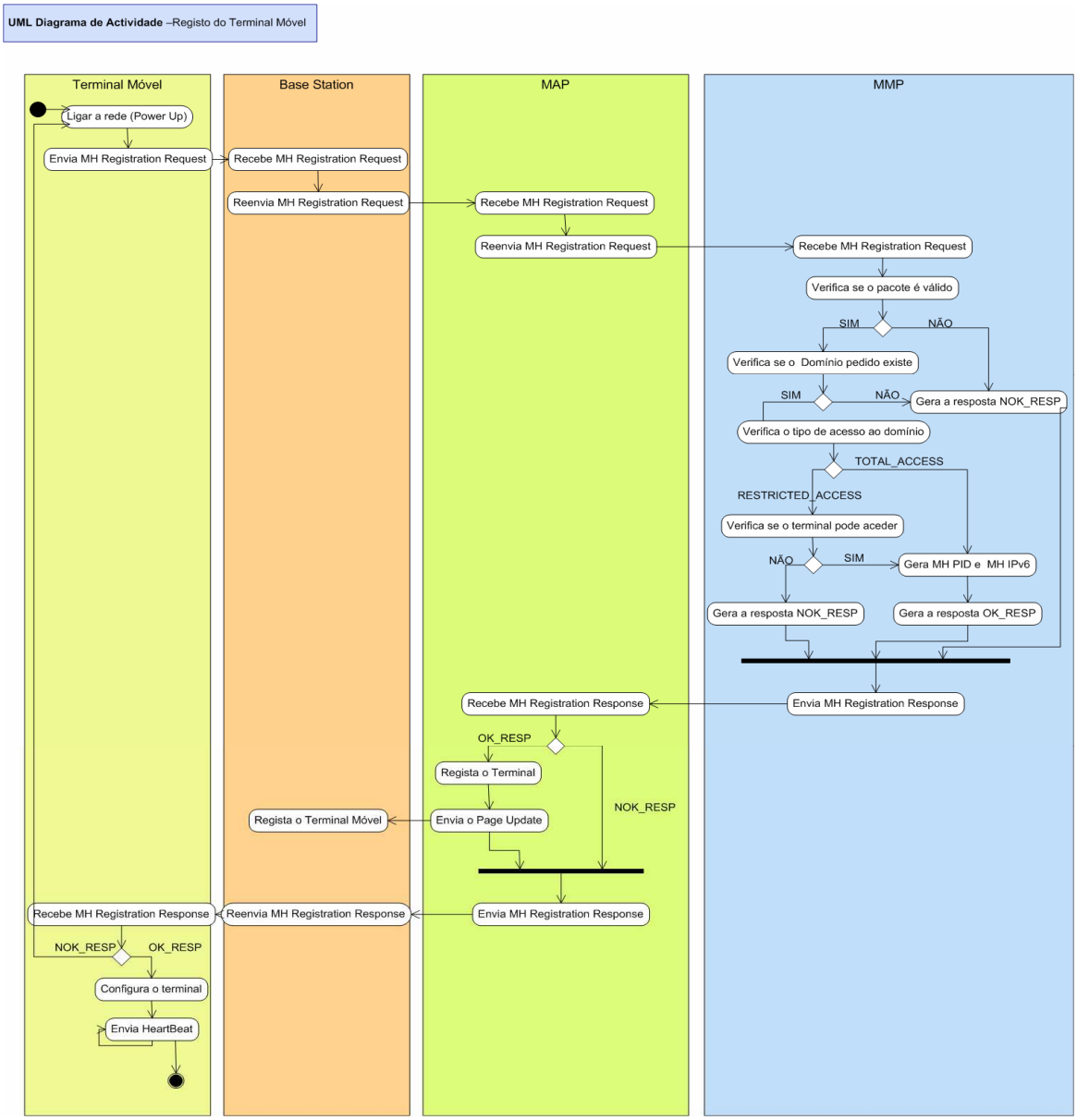


Figura 40 – LMS, diagrama de actividade UML referente ao registo do terminal na rede

3.9 Segurança

O *Local-centric Mobility System*, apesar de não ser embebido numa visão paranóica de segurança, foi arquitectado sobre a forte convicção de que a segurança do sistema é crucial para o seu sucesso. Segundo este prisma, optou-se por seguir o mesmo processo de *Cellular IPv6* aplicando assim autenticação a todos os pacotes de controlo e cifragem de todos os dados confidenciais. A autenticação e cifragem dos pacotes de dados, pode ser implementada através do uso de *IPsec* entre o terminal móvel e o terminal correspondente.

No prisma do *Local-centric Mobility System* apenas os agentes *MMP* têm conhecimento sobre a chave secreta do terminal móvel que está guardada na *Base de Dados Central*, diminuindo assim o número de agentes da rede a conhecerem a chave principal que é usada para autenticar o terminal na rede de operador e que poderia favorecer situações de personificação. De forma a garantir a confidencialidade da chave secreta do terminal, o *MMP* no acto de registo do terminal móvel ou no acto de negociação de um handover inter micro-domínio, gera um *PID* que servirá como chave de autenticação de todos os pacotes de controlo enviados pelo terminal nesse micro-domínio. O *MMP* gera um *PID* novo para cada micro-domínio onde o terminal se registe. O *PID* do terminal pode ser posteriormente recalculado por qualquer agente do micro-domínio de forma a comparar e validade todos os pacotes com autenticação.

O seguinte diagrama da Figura 41 representa a informação contida na mensagem de Registration Request enviada pelo terminal durante o processo de registo na rede.

Micro-Domain Network ID
NAI – Network Access Identification
Encrypted(md5(NAI+Ticket_Key) , KEY[Ticket_Key]);

Figura 41 – LMS, diagrama representativo do pacote MH Registration Request

Sempre que um terminal se liga na rede, ele necessita obrigatoriamente de se autenticar perante a mesma, enviando para isso uma mensagem de *Mobile Host Registration Request*. Neste caso, ele envia os seus dados e a sua chave de autenticação (*md5[NAI+Ticket_Key]*) cifrada com o seu *Ticket_Key* para a rede. Visto que nenhum agente da rede de acesso, *MAP e Base Stations* , conhecem o *Ticket_Key* do terminal logo não têm capacidade para decifrar este tipo de dados. Assim, o registo é redireccionado para

o *MMP* que irá decidir se o terminal pode ou não aceder aquele micro-domínio da rede. Para isso o *MMP* efectua todos passos necessários para se certificar de que o terminal é quem diz ser e que tem permissões para aceder ao micro-domínio que pretende. Para efectuar esta decisão, o *MMP* serve-se das informações contidas na *Base de Dados Central*. Caso o terminal possa aceder aquele micro-domínio, o *MMP* gera automaticamente um *PID* e um novo endereço IPv6 para o terminal usar naquele micro-domínio. Após ter decidido, o *MMP* constrói um *MH Registration Response* e envia a resposta para o terminal através do *MAP* do micro-domínio onde este se encontra. Caso a resposta seja positiva, o *MAP* cria um novo registo na rede para este terminal e anuncia a sua presença na rede para todas as *Base Stations* da *Paging Area* onde este se encontra. O *Paging Update* é enviado pelo grupo multicast associado à *Paging Area* em questão e cada uma das *Base Stations* ao receber essa informação insere o terminal na sua *Paging Cache*, permitindo assim que o terminal possa aceder a qualquer parte da mesma.

No *LMS* todos as mensagens de sinalização do protocolo são assinadas digitalmente através de mecanismos criptográficos. A construção da assinatura digital é efectuada com base numa função de criptográfica de *hash*. A função de *hash* utilizada no *LMS* é função criptográfica *MD5* [23] que gera uma *hash value* de *128 bit*. A Figura 42 ilustra o funcionamento básico do algoritmo usado na função *MD5* para quatro entradas (A,B,C,D) e quadro saídas (A,B,C,D).

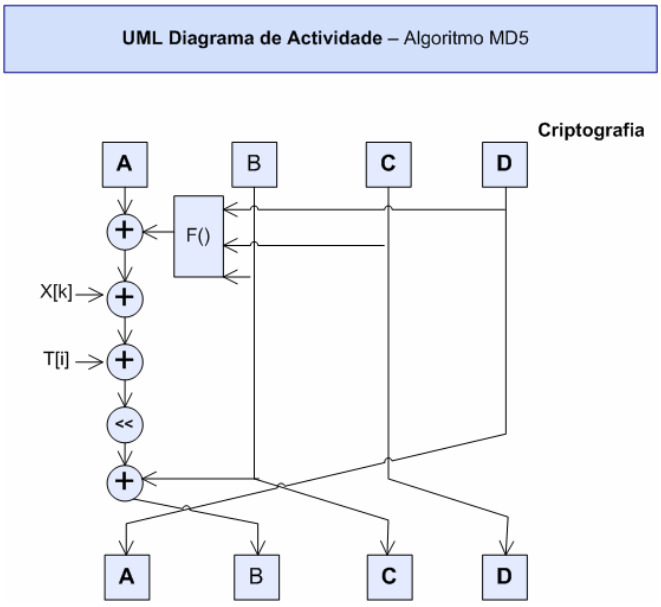


Figura 42 – LMS, funcionamento do algoritmo MD5

Tal como pode ser observado na Figura 42 figura anterior, o resultado final da função criptográfica é dado por uma soma

progressiva. As funções de *hash* são funções criptográficas unidireccionais progressivas de dispersão que modificam catastroficamente o seu resultado (*hash value*) caso a entrada da função mude 1bit que seja. O resultado da função (*hash value*) é sempre um valor único que representa a assinatura dos valores de entrada. Este tipo de funções criptográficas são comummente utilizadas nos mecanismos de segurança dos protocolos de comunicação de dados para verificar a integridade da mensagem enviada. O *LMS* utiliza este tipo de algoritmo criptográfico para garantir que as mensagens enviadas na rede não foram violadas durante a sua transmissão.

Este tipo de funções é também fortemente utilizada para assinar digitalmente conteúdos digitais. Visto que as funções de *hash* geram sempre valores criptográficos únicos, esta característica pode servir não só para garantir a integridade de uma dada mensagem mas também a sua autenticidade. Por conseguinte, através de funções de *hash* no *LMS* garante-se a integridade das mensagens, autenticidade das mesmas e não repudiação do seu conteúdo.

O *PID* é uma chave de *128bit* que serve para identificar o terminal móvel num dado micro-domínio. A figura seguinte ilustra o mecanismo usado pelo *MMP* para gerar o *PID* para o terminal móvel num dado micro-domínio.

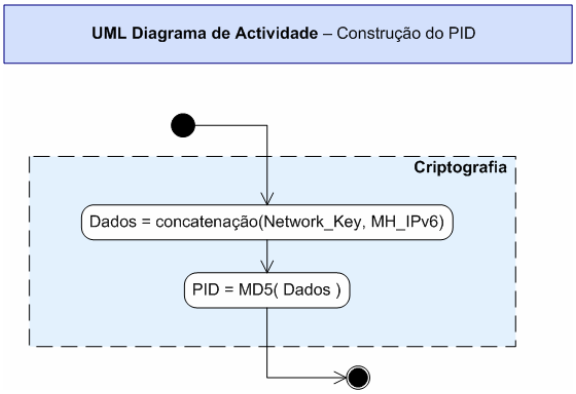


Figura 43 – LMS, diagrama de actividade UML usado na construção do PID do terminal móvel

A Figura 43 ilustra o mecanismo usado para a construção do *PID* do terminal móvel. Cada *PID* apenas é válido para um dado terminal num dado micro-domínio especifico. O terminal móvel serve-se desta chave de *128 bit* para assinar os seus pacotes de sinalização nessa rede garantindo assim a sua autenticidade. Cada micro-domínio detém uma chave criptográfica de *128 bit* única gerada no momento da sua criação na *Base de Dados Central*. Essa chave criptográfica identifica o micro-domínio inequivocamente na rede de operador e é conhecida por todos os seus agentes de mobilidade,

MAP e *Base Stations*. Como pode ser observado na figura anterior, o *MMP* gera o *PID* do terminal móvel com base na concatenação do *Network_Key* do micro-domínio com o endereço IPv6 do terminal móvel. Depois deste processo de concatenação o *MMP* utiliza uma função de *hash* para gerar uma chave de *128 bit* única apenas válida para aquele terminal móvel e para aquele domínio em especifico. A figura seguinte ilustra o mecanismo usado pelo terminal móvel para assinar digitalmente os pacotes de sinalização enviados para a rede.

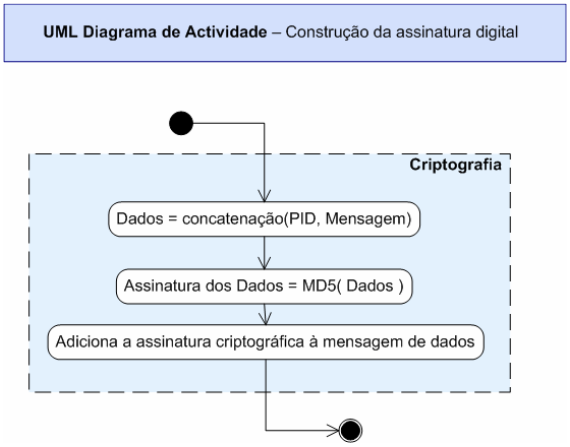


Figura 44 – LMS, construção da assinatura digital do terminal móvel

Como pode ser observado na Figura 44, o terminal utiliza o seu *PID (Personal Identifier)* para autenticar as mensagens que envia para a rede. O *PID* é uma chave de *128 bit* gerada pelo *MMP* apenas válida para o micro-domínio onde o terminal se encontra naquele momento. No *LMS* antes de utilizar a função de *hash*, o *PID* é acoplado à mensagem de dados por forma a criar um par (*Dados+NAI*) único, depois o par é percorrido pela função criptográfica de *hash* que gera um valor único para aquele par. A este valor único chama-se assinatura digital, que no caso do LMS tem *128 bit*. Esta assinatura é posteriormente acoplada no pacote de dados que será enviado para a rede. Quando este pacote de dados chega ao destino para ser verificado, o agente de mobilidade do micro-domínio efectua o mesmo procedimento de acoplação entre a mensagem de dados e o *PID* do terminal móvel.

No final o agente de mobilidade deverá obter o mesmo resultado (*hash value*) sendo assim garantido que a mensagem veio daquele terminal e que não foi corrompida durante a transmissão. Assim garante-se a autenticidade e integridade da mensagem. A Figura 45 ilustra o processo de criação da credencial usada no pacote de sinalização *MH Registration Request*

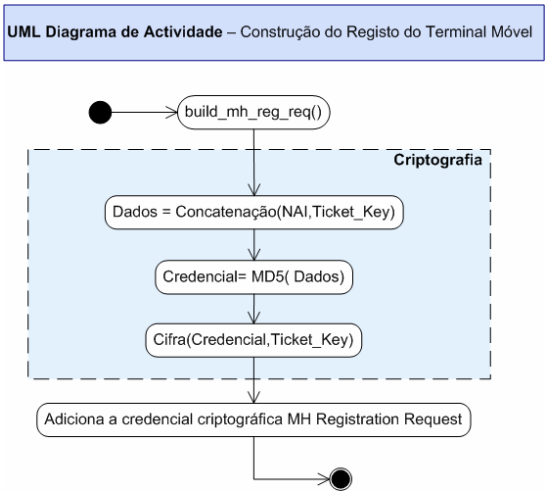


Figura 45 – LMS, criação das credenciais usadas no MH Registration Request

Na Figura 46 pode-se observar o mecanismo usado pelo *MMP* para verificar a assinatura do Mobile Host no pacote MH Registration Request.

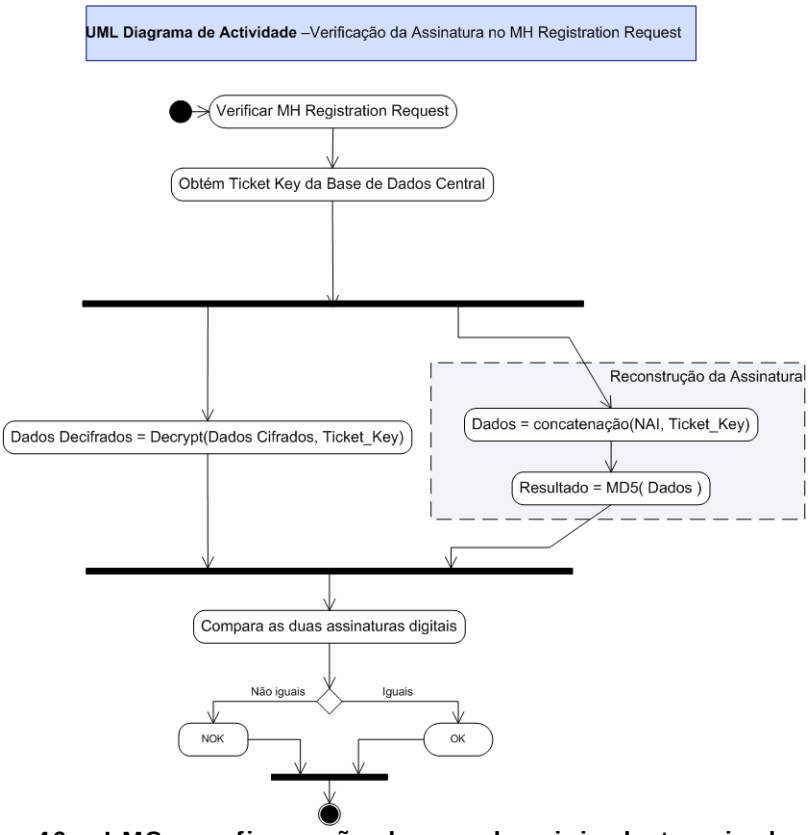


Figura 46 – LMS, configuração das credenciais do terminal móvel

Quando um terminal móvel se encontra registado na rede ele envia periodicamente mensagens do tipo *Heartbeat* para a rede anunciando a sua presença naquele micro-domínio. Estes pacotes contêm a identificação do terminal e permitem que a rede refresque as entradas nas *caches* referentes a este terminal. Como todas as *caches* do sistema são do tipo *softstate* elas expiram passado algum tempo sem serem refrescadas. Assim o terminal envia mensagens de *Heartbeat* (batimento cardíaco) de forma a sinalizar a sua presença e garantindo assim que as rotas até ele são mantidas em todos os agentes de mobilidade *LMS*. Estes pacotes são autenticados usando um cabeçalho *AH* [6] de *IPsec* de forma a que todo o micro-domínio tenha a garantia de que não se trata de um processo de personificação.

Também nos cenários de *handover* todos os *Handover Request* são autenticados com cabeçalho *AH*, sendo que no cenário de *Inter-Domain Handover* os dados que são enviados para o terminal poder aceder ao novo *micro-domínio* são cifrados usando o mesmo processo explicado nas figuras anteriores garantindo assim a confidencialidade e diminuindo assim o risco de um atacante poder roubar informações importantes que poderiam servir para criar uma situação de personificação na rede.

3.10 AAAC - Access, Authorization, Accounting and Charging

Tendo em consideração que este sistema foi projectado para um ambiente de operador, era importante conceber um mecanismo de proporcionasse o controlo de Acesso, Autorização, Contabilidade e Facturação (Figura 47).

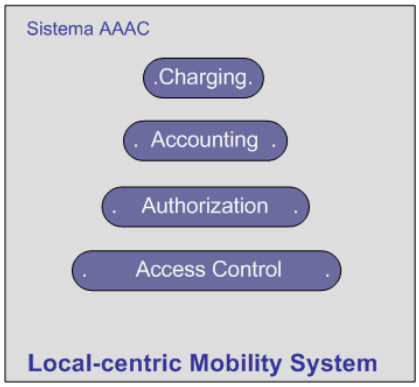


Figura 47 – LMS, sistema AAAC

A arquitectura do *LMS* é extremamente eficaz no que diz respeito ao controlo de fluxos de tráfego já que todo o tráfego de cada micro-domínio passa sempre pelo *MAP* do mesmo. Assim, aproveitando as vantagens da arquitectura, optou-se integrar no *LMS* um mecanismo de controlo de acesso, autorizações, contabilidade e facturação que é controlado pelo *MMPs* e executado pelos *MAPs* de cada micro-domínio.

Para concretizar as funcionalidades de *AAAC*, dividiu-se as acções em dois patamares cooperativos, um a funcionar no *MAP* e outro a funcionar no *MMP*. Desta forma, cabe ao *MAP* fazer o controlo da contabilidade (*Accounting*) referente ao seu micro-domínio e executar o controlo de fluxos segundo as regras do *MMP*.

Cada *MAP* é responsável por controlar todo o fluxo de dados do seu micro-domínio, e vai submetendo essa informação ao seu *MMP*. Desta forma, neste prisma, o *MMP* apenas tem que fundir os diferentes tipos de dados emitidos pelos vários *MAPs* na *Base de Dados Central*. Opcionalmente, o *MMP* pode aceder a estas informações através a um agente externo, por exemplo um servidor *RADIUS* .

Periodicamente o *MAP* envia toda informação referente à contabilidade do seu micro-domínio para o *MMP*. O *MMP* colecciona a informação da contabilidade de todos os *MAPs* da sua responsabilidade e cabe-lhe a tarefa de sincronizar toda essa

informação na *Base de Dados Central* ou enviar a mesma para um agente especifico para o efeito. Tendo em consideração que um dado terminal pode passar por vários micro-domínios distintos, o *MMP* tem que ser capaz de manter a sua contabilidade perfeitamente correcta com o volume de tráfego que esse terminal efectuou na sua totalidade, independentemente do micro-domínio onde isso se sucedeu.

O segundo patamar de acção cabe exclusivamente ao *MMP.* O *MMP* está encarregue de gerir todos os processos de Autenticação/Acesso e Autorização na rede. Desta forma, sempre que um *MAP* necessita de saber se um dado terminal pode ou não aceder a um dado recurso ele questiona o *MMP* de forma a saber qual deve ser a resposta adequada para esse terminal em específico. Cabe assim ao *MMP* gerir completamente todo o acesso à rede e as autorizações, pois só ele pode consultar a *Base de Dados Central* ou questionar um agente externo para obter as informações sobre as permissões do terminal.

Por fim falta referir a secção de Facturação (*Charging*), que é gerida por ambos os agentes *MAP* e *MMP*. Ao *MAP* cabe a responsabilidade de verificar se a contabilidade de um dado terminal ultrapassou ou não o seu limite de crédito. Por outro lado, cabe ao *MMP* colectar essa informação e informar todos os *MAPs* sobre o limite de crédito dos terminais da sua responsabilidade.

Poderá então compreender-se o *AAAC* como uma actividade cooperativa entre o *MAP* e o *MMP* contudo funcionando de uma forma perfeitamente integrada e única no *Local-centric Mobility System.* A Figura 48 mostra a relação entre as funcionalidades de Controlo de Acessos, Controlo de Autorizações, Contabilidade e Facturação nos dois agentes, *MAP* e *MMP* respectivamente:

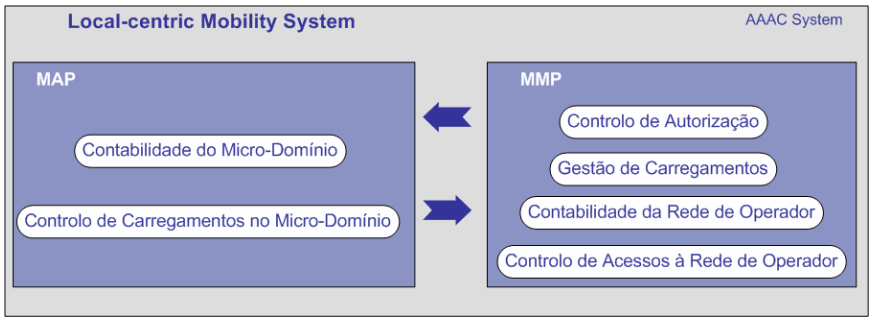


Figura 48 – LMS, serviços AAAC

3.11 Comunicação por multicast

A comunicação por multicast foi sem dúvida uma das grandes inovações do *Local-centric Mobility System.* Desde do inicio pretendia-se que o encaminhamento dos pacotes na rede do micro-domínio fosse flexível, dinâmica mas robusta o suficiente para ser integrada num ambiente de operador. Acrescido a isto pretendia-se também aplicar o conceito de paginação de terminais móveis em *Paging Areas* que permitiria enviar um dado pacote para um conjunto de *Base Stations* sem necessitar de replicação de pacotes de dados. Estas necessidades não podiam ser facilmente cobertas pelo *routing* IP unicast que se utiliza nas redes actuais. Por outro lado pretendia-se que o mecanismo de encaminhamento fosse o mais compatível possível com as infra-estruturas actuais. Desta forma optou-se por desenvolver um mecanismo de encaminhamento baseado em *routing multicast* e etiquetagem de pacotes. A Figura 49 representa a rede nuclear de um micro-domínio.

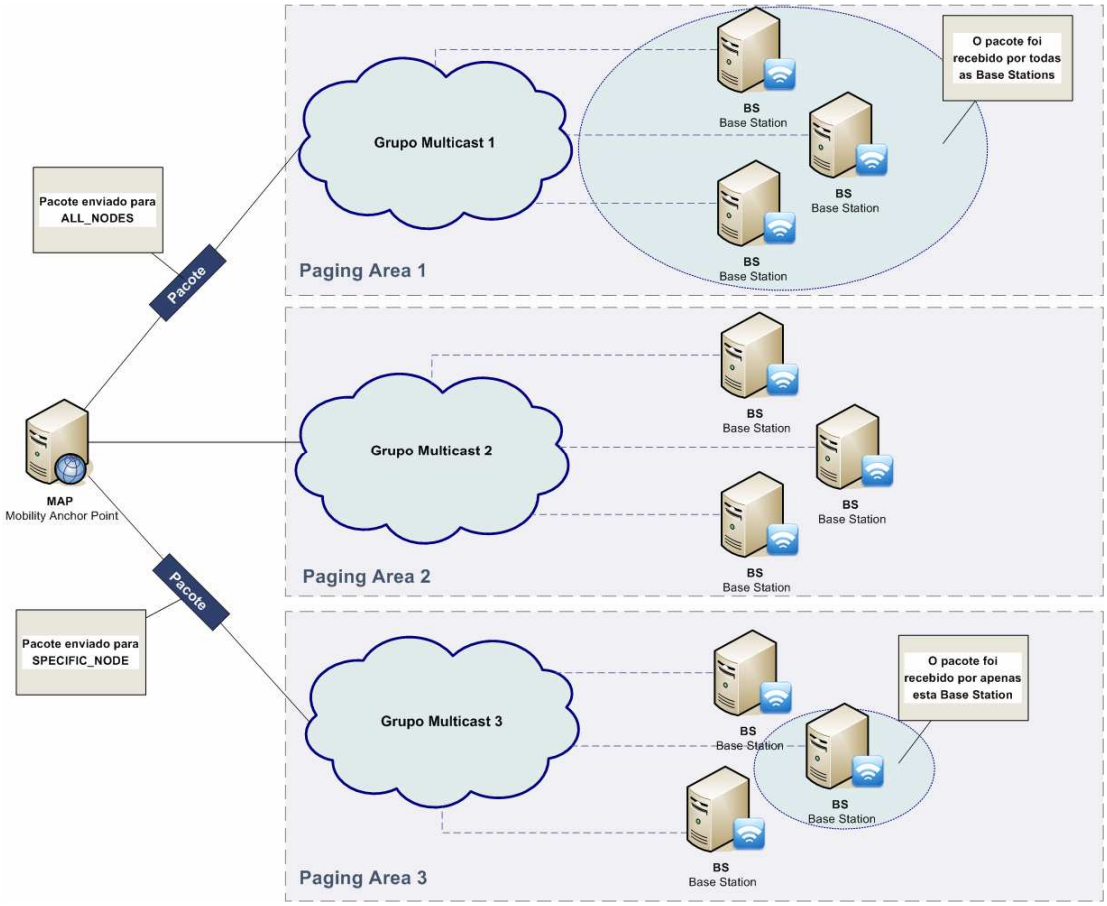


Figura 49 – LMS, ilustração do mecanismo de encaminhamento dentro do micro-domínio

Como pode observar-se na Figura 49, na *Paging Area 1* a emissão de um pacote do tipo *ALL_NODES* é recebido por todas as Base Stations dessa *Paging Area* sem ser necessário replicar os dados na rede. Na *Paging Area 3* poderá observar-se a emissão de um pacote do tipo *SPECIFIC_NODE* que é recebido apenas por uma Base Station especifica.

O encaminhamento de pacotes dentro da rede do micro-domínio é exclusivamente baseado em algoritmos de multicast. Desta forma consegue-se criar um mecanismo de comunicação entre qualquer elemento da rede assim como também é possível enviar a mesma informação para vários equipamentos (ou mesmo todos) sem replicar pacotes. Com este novo sistema é também possível organizar várias *Base Stations* em grupos (ou na terminologia das redes celulares, em *Paging Areas)* onde cada um é um grupo multicast.

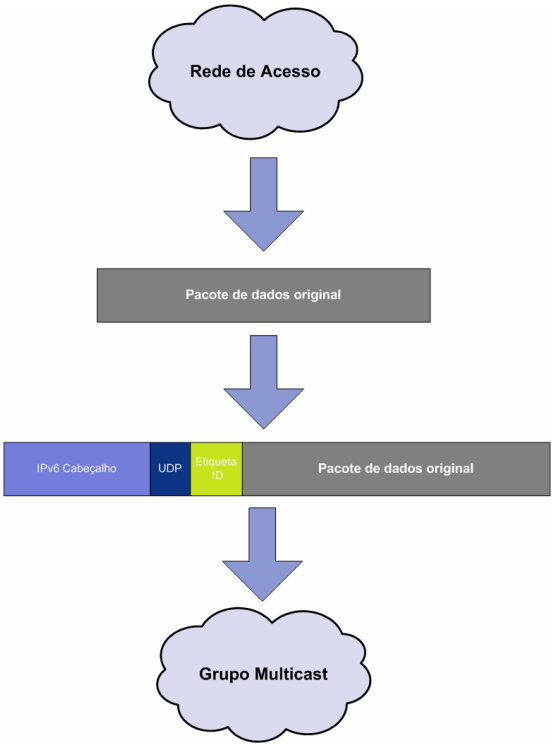


Figura 50 – LMS, processo de empacotamento para a rede multicast

O sistema de comunicação dentro da rede nuclear do micro-domínio funciona com base num mecanismo de identificação por etiquetas. Cada um dos agentes do Micro-Domínio é identificado por um *ID* pessoal que surge como uma etiqueta. Sempre que um pacote é emitido para a rede nuclear do micro-domínio o pacote é encapsulado sobre outro pacote IPv6 e é etiquetado com o *ID* do agente destinatário. Assim é garantido que o pacote apenas será interpretado pelo agente correcto, e todos os outros irão descarta-

lo no momento de recepção. De forma idêntica o pacote pode ser etiquetado de uma forma especial de maneira a que todos os agentes do micro-domínio o recebam e o processem. Estes dois procedimentos podem ser visualizados na figura anterior. Figura 50, mostra como os pacotes são capturados na rede de acesso e depois encapsulados e enviados para dentro da rede do micro-domínio. No cenário pode-se visualizar que o pacote de dados é capturado na rede de acesso e é reencaminhado pela rede multicast até ao seu destino.

Através deste mecanismo é possível ao *MAP* enviar ordens para um conjunto de *Base Stations* ou todas as Base Stations do seu micro-domínio aumentando drasticamente a desempenho da rede, essencialmente sob a forma de diminuição do tempo de propagação de informações e configurações referentes à rede.

Um bom exemplo das vantagens deste tipo de mecanismo de encaminhamento acontece durante os cenários *handovers*. Quando se dá um *handover* é possível que o terminal "julgue" que vai entrar numa determinada Base Station mas no entanto, devido ao tipo de movimento físico que ele está a efectuar, é possível que ele entre outra, no entanto ambas dentro da mesma *Paging Area*. Desta forma, sempre que um *handover* se dá é possível enviar o registo desse terminal para a *Paging Area* completa de forma a permitir que o terminal consiga comunicar em qualquer uma das *Base Stations* dessa *Paging Area*, mesmo que não seja a que ele requisitou inicialmente. Utilizando as técnicas tradicionais, *MAP* teria que fazer uma ligação a cada *Base Stations* e enviar o novo registo do terminal para cada um delas. Este processo levaria a um tempo total igual ao somatório do tempo da criação do canal e da transferência de dados para cada uma das *Base Stations*.

Este tipo de mecanismo de encaminhamento de pacotes na rede permite aumentar substancialmente a eficiência do uso dos recursos de rede bem como diminuir o tempo de notificação dos agentes de mobilidade *LMS*. Para melhor compreensão dos motivos pelos quais se desenvolveu este novo método, seguidamente irá apresentar-se alguns exemplos concretos de carácter prático numa rede de operador.

Exemplo 1

- Considere-se uma rede de um micro-domínio tem *n Base Stations* numa *Paging Area* e o *MAP* pretende enviar para todas elas um pacote que contem informação sobre um terminal que irá associar-se na rede.

- Usando multicast o tempo de transferência de informação entre *MAP* e as *Base Station* é *n* vezes menor do que usando métodos tradicionais, sendo *n* o número de *Base Stations* da *Paging Area*.

Exemplo 2

- Considere-se um terminal móvel em estado *Dormente (Idle)* mapeado numa dada *Paging Area* de um micro-domínio *LMS*. Considere-se ainda um terminal correspondente a iniciar uma sessão de transferência de um ficheiro para o terminal móvel. Devido ao facto de o terminal móvel estar em modo *Dormente* a rede não tem rotas directas para ele, apenas conhece a *Paging Area* onde este se encontra. Dado que a *Paging Area* é um conjunto de *Base Stations*, a rede terá que encaminhar os pacotes de dados para todas as Base Stations de forma a que o terminal receba os dados e passe para o estado *Activo (Active)*.

  - Considerando que o terminal passa ao estado *Activo* após o primeiro pacote de dados recebido, usando multicast o tráfego no *MAP* é *n* vezes menor do que usando métodos tradicionais, sendo *n* o número de *Base Stations* da *Paging Area*.

Como pode ser observado nos exemplos anteriores, este mecanismo baseado em encaminhamento multicast permite optimizar os recursos da rede de operador significativamente. É também possível verificar que utilizando este mecanismo é possível replicar dados na rede com um custo mínimo permitindo assim que a rede seja mais escalável diminuído o *overhead* nas ligações entre *MAP* e *Base Stations.*

b. Gestão dos grupos multicast

Os grupos multicast são gerados automaticamente pelo *MAP* sempre que uma *Base Station* requer uma *Paging Area* que ainda não está a ser usada. Este procedimento acontece sempre no momento de registo *da Base Station* no *MAP*. Quando a *Base Station* se liga e envia a mensagem *BS Registration Request* para o *MAP* este começa por verificar se a *Paging Area* requerida pela *Base Station* já está a ser usada.

No caso de já estar a ser usada, o *MAP* apenas precisa de adicionar a nova *Base Station* à *cache* interna e enviar o *Registration Response* com os dados necessários para que a *Base Station* se possa associar ao grupo multicast que define a *Paging Area* requerida. Tipicamente este dados são representados sobre a forma do endereço do grupo multicast e o porto de comunicações utilizado para o efeito.

No caso da *Paging Area* requerida pela Base Station ainda não estar a ser usada, então o *MAP* cria um novo grupo multicast para agregar todas as futuras Base Stations que pretenderem posicionar-se naquela *Paging Area*. Como tal, o *MAP* começa por gerar o novo endereço e porto para o grupo multicast. Após isso, a *Base Station* é adicionada à *cache* interna de forma a ficar mapeada naquele grupo. O *MAP* por fim, depois de efectuar todas as operações necessárias, constrói uma mensagem *BS Registration Response* e envia para a *Base Station* indicando todos os dados necessários para a sua configuração.

As *Base Stations* têm obrigatoriamente que enviar mensagens de *Keep-Alive* para o *MAP* de forma a refrescar a sua entrada na *BS Cache*. O *MAP* implementa um mecanismo de *softstates* em todas as suas *caches*, inclusive na *BS Cache*. Sempre que é detectado que uma *Base Station* não refresca a sua entrada com um *Keep-Alive* num período maior do que estipulado, então o *MAP* elimina essa Base Station de todas as *Caches* onde esta estiver registada. Consequentemente, o *MAP* verifica ainda se na *Paging Area* onde a Base Station estava associada existe alguma *Base Station* ainda activa. Caso o seja detectado que a *Paging Area* encontra-se vazia, o *MAP* elimina essa *Paging Area* e liberta todos os recursos utilizados para esta, incluindo o grupo multicast.

Desta forma, usando este mecanismo, consegue-se obter um sistema flexível que processa a criação e remoção de *Paging Areas* e subsequente gestão de grupos multicast de forma completamente automática e dinâmica. Assim é permitido ao administrador da rede remover e inserir *Base Stations* no sistema sem que seja necessário reiniciar todo o micro-domínio. Este mecanismo permite ainda aumentar a robustez do sistema visto que através deste garante-se que apenas os recursos necessários são utilizados. Sempre que os recursos de sistema deixam de ser necessários o mecanismo liberta-os aumentando a eficiência da rede. O facto de toda a gestão ser automatizada e completamente transparente para o administrador de rede, permite evitar a possibilidade de erros humanos assim como diminuir o tempo de integração de novos componentes na rede. Este tipo de factores aumenta a robustez da rede *LMS* assim como garante aos operadores o menor custo possível no processo de crescimento da rede. A

Figura 51 mostra como o *MAP* gere os grupos multicast assim como as *Paging Areas* no micro-domínio durante o registo de uma nova *Base Sation*.

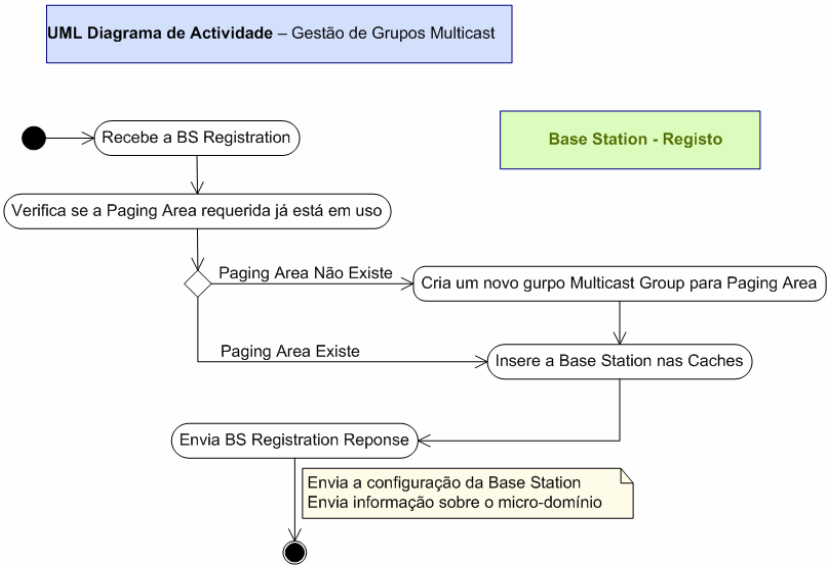


Figura 51 – LMS, processo de registo de uma nova Base Station

A Figura 52 ilustra como o *MAP* gere os grupos multicast assim como as *Paging Areas* no micro-domínio durante o processo de envelhecimento das *Base Stations*.

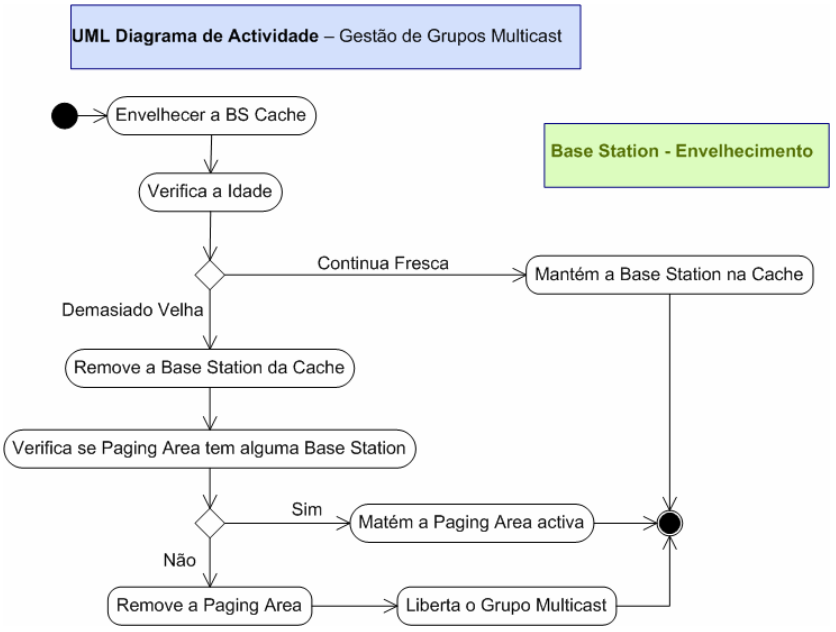


Figura 52 – LMS, envelhecimento (aging) das Base Stations

c. Paginação (*paging*) de terminais móveis

O *Local-centric Mobility System* implementa um processo o qual se designa por *Paginação* (*Paging*). A paginação de terminais permite criar dois estados distintos para cada terminal móvel em cada instante do tempo, o estado *Activo* e o estado *Dormente*. Tecnicamente, os agentes integram duas *caches* distintas, uma *Paging Cache* que contem a listagem de todos os terminais independentemente do seu estado (*Activo* ou *Dormente*) e uma *Routing Cache* que contem apenas os terminais em estado *Activo* na rede.

Cada agente da rede recorre à *Routing Cache* para encontrar um caminho para a Base Station onde o terminal activo se encontra naquele preciso momento. Por outro lado, os agentes da rede podem recorrer à *Paging Cache* para encontrar a *Paging Area* onde o terminal se encontra nesse momento. A implementação de duas *caches* permite aumentar a desempenho na rede visto que na *Routing Cache* apenas estão listados os terminais activos que tipicamente são em muito menor número do que a restante totalidade dos mesmos. Desta forma, as pesquisas de encaminhamento são extremamente optimizadas visto que o número de elementos da pesquisa é muito mais reduzido do que se fosse procurado na *Paging Cache* que contem a totalidade dos terminais.

A Figura 53 ilustra a relação entre uma *Paging Cache* e uma *Routing Cache* num agente de mobilidade *LMS.*

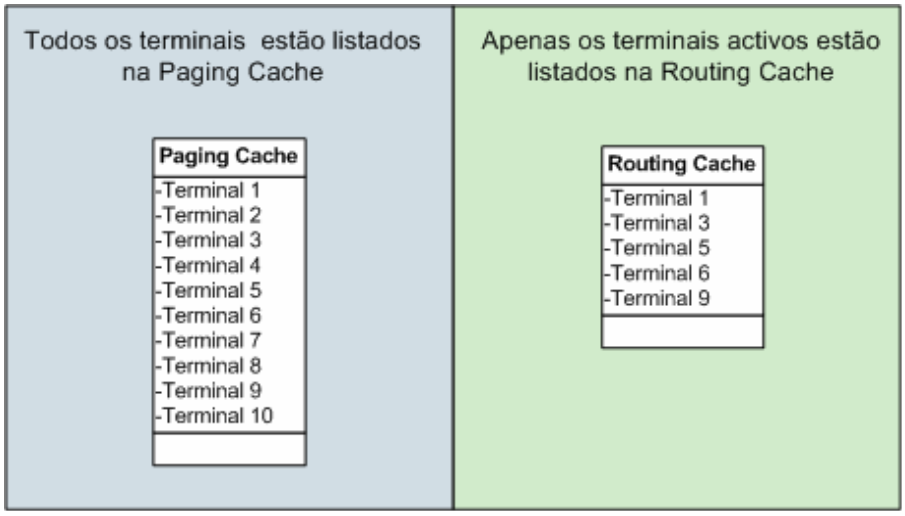


Figura 53 – LMS, relação entre a Paging Cache e a Routing Cache

Apesar da ideia de paginação ter surgido das redes celulares, no *LMS* a gestão das *caches* é completamente diferente da utilizada noutros protocolos, tais como o *Cellular IP.* No *LMS* tentou-se optimizar os recursos da rede, enviando menos pacotes de sinalização, tentando paralelamente corrigir algumas das falhas de segurança que o *Cellular IP* apresenta.

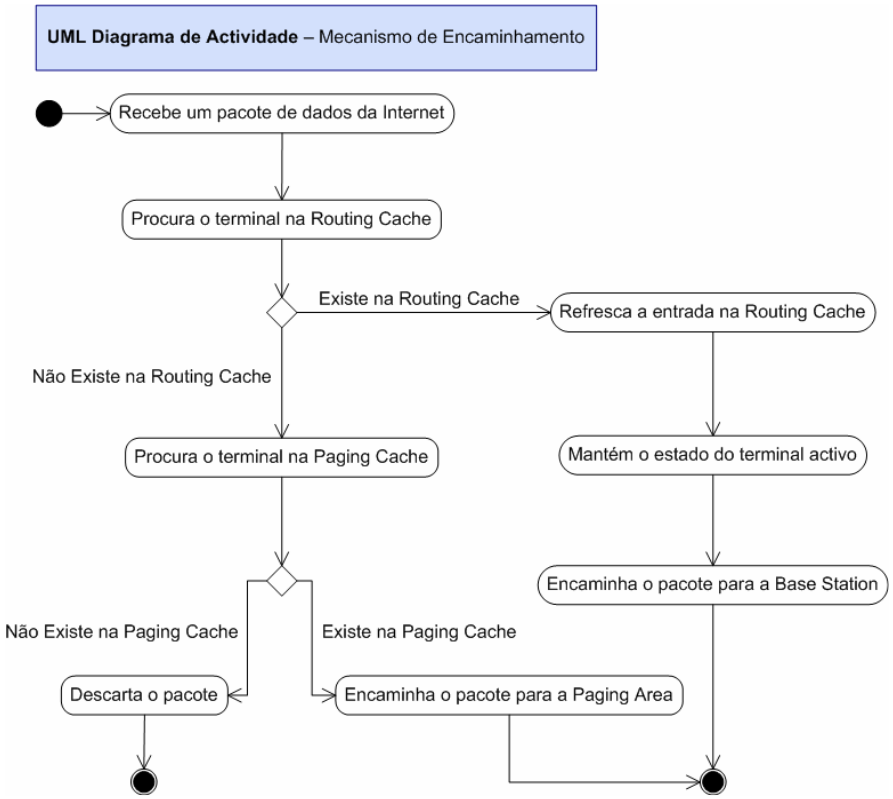


Figura 54 – LMS, mecanismo de encaminhamento do LMS

Este tipo de mecanismo permite que cada agente do sistema possa pesquisar uma rota para um terminal activo de uma forma muito mais eficaz e rápida aumentando assim drasticamente a desempenho do sistema. Apesar de algumas semelhanças com o *Cellular IP*, a gestão das caches no *LMS* funciona de forma muito distinta. No *LMS* a *Paging Cache* de cada agente apenas pode ser manipulada sobre as ordens de um agente hierarquicamente superior. Esta decisão proveio do facto de no *Cellular IP* a *Paging Cache* ser criada por um *Paging Update* enviados pelo terminal, o que tornava o sistema vulnerável a ataques de personificação. Teoricamente numa rede *Cellular IP* é possível um atacante capturar um pacote *Paging Update* e criar um sem fim de entradas em *Paging Caches* dos variados agentes da célula. Assim, para contrariar esta falha de segurança, no *LMS* optou-se por apenas criar as entradas nas *caches* do sistema apenas quando é recebido uma ordem de um

agente hierarquicamente superior. Segundo este raciocínio as *Base Stations* apenas criam entradas nas suas *Paging Caches* quando recebem um *Paging Update* do *MAP* e o *MAP* apenas cria uma entrada na sua *Paging Cache* quando recebe ordens do *MMP* para o fazer. Note-se que uma entrada na *Paging Cache* referente a um terminal indica que ele está registado naquele micro-domínio. Assim, caso este processo fosse subvertido por um atacante seria possível personificar um terminal não presente naquele micro-domínio num dado instante. Com este mecanismo, é possível garantir que um terminal apenas se encontra registado num micro-domínio segundo duas situações: por via de um registo fidedigno na rede, ou por via de um *Inter-Domain Handover Notify* enviado pelo *MMP*, que é um agente de confiança. Assim garante-se a impossibilidade que um atacante possa criar um registo falso num dado micro-domínio *LMS*.

A *Routing Cache* serve no *LMS* para destacar os terminais activos dos inactivos. Apesar do sentido ser o mesmo usado no *Cellular IP*, no *LMS* mais um vez o processo de gestão desta *cache* funciona de forma muito diferente. No *Cellular IP* o terminal necessita de enviar explicitamente para a rede várias mensagens de *Routing Update* a uma taxa elevada sempre que estava activo. Isto significava que o terminal satura a rede de acesso com pacotes de controlo que implica a perda de largura de banda disponível para os pacotes de dados. De forma a contrariar este ponto negativo do *Cellular IP,* no *LMS* o mecanismo de sinalização dos terminais moveis é diferente. No *LMS*, sempre que um agente verifica que um terminal envia um pacote de dados para a rede, automaticamente cria-lhe uma entrada na *Routing Cache* indicando qual o melhor caminho para o atingir. Sempre que este tipo de situação acontece, a rede passa o terminal para o estado activo de forma completamente automática e transparente. Caso o terminal receba pacotes vindos da Internet, mas este não se encontre ainda na *Routing Cache*, ou seja em estado activo, então os agentes da rede não podem precisar a sua localização. Desta forma a rede irá enviar os pacotes de dados directamente para a *Paging Area* completa. Assim é garantido que o terminal recebe sempre os pacotes de dados mesmo quando este não se encontra em estado activo e por isso não mapeado na *Routing Cache*. Note-se que mal o terminal envie um pacote de dados para o terminal correspondente, a rede pode automaticamente localizar a sua posição efectiva na rede e por isso ele é automaticamente introduzido na *Routing Cache* de todos os agentes, passando assim para o estado activo na rede. O terminal envia uma mensagem especial, *Hearbeat*, que indica a sua presença na rede. Esta mensagem permite refrescar todas as entradas das *Paging Caches*. Todos os *HeartBeats* são autenticados, garantido assim que não existe a possibilidade de um ataque de personificação. Note-se que o *Heartbeat* é extremamente necessário visto que todas as *caches* implementam *softstates* e neste caso, se o terminal não

refrescar periodicamente a sua entrada nas *Paging Caches* ele será automaticamente eliminado da rede por questões de segurança e desempenho dos agentes. A Figura 54 representa o diagrama de encaminhamento utilizado no *LMS.*

d. Mapeamento dos terminais em Paging Areas

A organização da rede nuclear dos micro-domínios em *Paging Areas*, permite ao *Local-centric Mobility System* mapear os diferentes terminais em grupos, dependendo da *Paging Area* onde estão associados. Desta forma é também possível agregar múltiplos terminais presentes na mesma *Paging Area* num só grupo multicast.

A paginação dos terminais em *Paging Areas* permite ao *MAP* de cada micro-domínio processar paralelamente o tráfego destinado a cada uma delas, já que em cada uma das *Paging Caches* estão apenas listados os terminais referentes à *Paging Area* em questão. Isto representa um aumento da eficiência computacional muito grande caso o *MAP* seja implementado com base de num sistema *multi-thread*. No protótipo do *LMS*, os *MAPs* foram desenvolvidos utilizando um sistema *multi-thread*, onde cada *thread* processa o tráfego referente a cada *Paging Area* forma independente.

Tal como se pode ver na Figura 55 que se segue o *MAP* processa o tráfego de cada *Paging Area* de forma completamente paralela. Assim é possível existir uma replicação de recursos permitindo ao agente retirar maior partido do processador e dos restantes recursos físicos do sistema computacional.

A Figura 55 mostra o sistema de processamento de pacotes do *MAP* num cenário de várias *Paging Areas*.

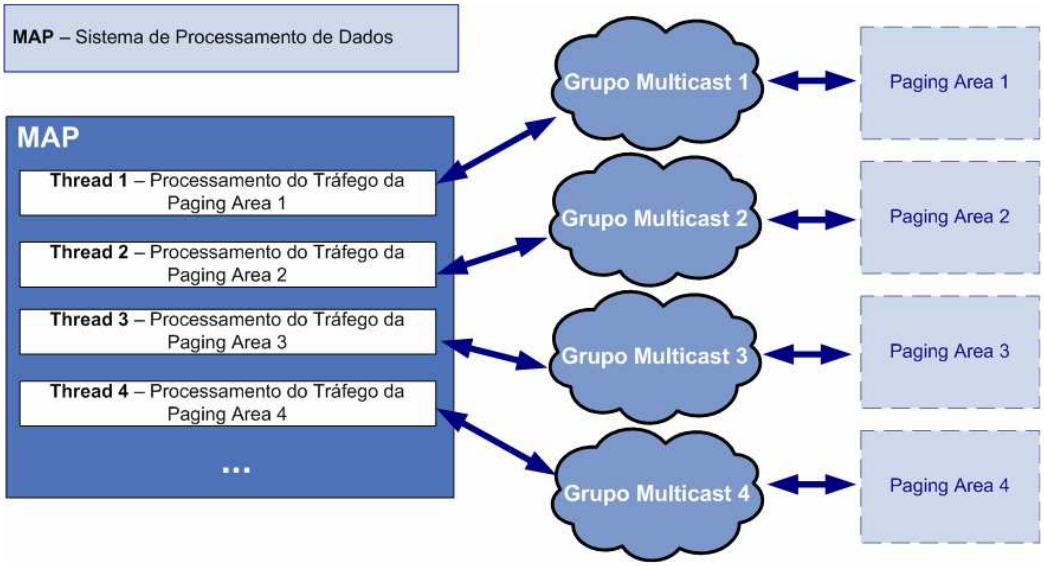


Figura 55 – LMS, sistema de processamentos de dados do MAP

3.12 Sinalização de Controlo

Segundo as considerações apresentadas pelo *workgroup NETLMM* [13] (*Network-based Localized Mobility Management*) um dos pontos importantes num sistema de *Mobilidade Local (LMP)* é a existência de pouco tráfego de controlo na rede de acesso. Este facto é justificado pelo razão de que numa rede partilhada a probabilidade de colisões de pacotes aumenta com o número de pacotes a ser emitido para a rede. De forma a não cometer este tipo de erro o *LMS* foi desenhado com o objectivo de necessitar do mínimo possível de pacotes de controlo na rede de acesso. Como tal, ao contrário de outros protocolos, no *LMS* apenas é necessário o terminal enviar um Heartbeat para a rede a uma taxa de emissão muito baixa. Desta forma consegue-se eliminar o efeito de desaproveitamento da rede diminuindo a necessidade de sinalização de controlo na mesma em situações normais.

De forma geral a sinalização de controlo que pode correr na rede de acesso é apresentada pela Tabela 1:

Tipo de Pacote	Motivo	Periodicidade
Heartbeat	Para sinalizar a presença do terminal móvel na rede	Periódico a uma taxa de emissão muito baixa. (Período de vários segundos)
Handover Request	Para sinalizar o pedido de Handover	Aperiódico.
Handover Response	Para sinalizar a resposta de Handover	Aperiódico
Registration Request	Para sinalizar o pedido de registo	Aperiódico
Registration Response	Para sinalizar a resposta de registo	Aperiódico

Tabela 1 – Mensagens de sinalização

3.13 Handover

No *Local-centric Mobility System* existem dois tipos de *Handover* possíveis, os *Inter-Domain Handovers* , que acontecem com transições de terminais entre micro-domínios distintos, e os *Intra Micro-Domain Handovers*, que surgem com as transições dos terminais dentro do mesmo micro-domínio. Os *Intra Micro-Domain Handovers* não necessitam de autorização especial do *MMP*, sendo que o *MAP* efectua todas as operações necessárias para o registo do terminal na nova *Paging Area* sem auxilio do *MMP*. Inversamente, quando se trata de *Inter Micro-Domain Handovers* torna-se imperativo a negociação do *Handover* entre o *MMP* e os dois *MAPs*, o antigo e o novo *MAP* respectivamente. Em ambos as situações o handover é sempre do tipo *Make-Before-Break*, o que indica que todos os recursos são reservados e garantidos antes do terminal se mover para o ponto de destino.

a. Intra Micro-Domain Handover

Quando um terminal pretende efectuar um *handover* dentro do mesmo micro-domínio, ele envia um *Handover Request* com um pedido de um *Intra Micro-Domain Handover* para o seu *MAP*. Visto que o terminal já se encontra registado neste micro-domínio, o *MAP* apenas tem que registar o terminal na nova *Paging Area* para onde ele se irá movimentar.

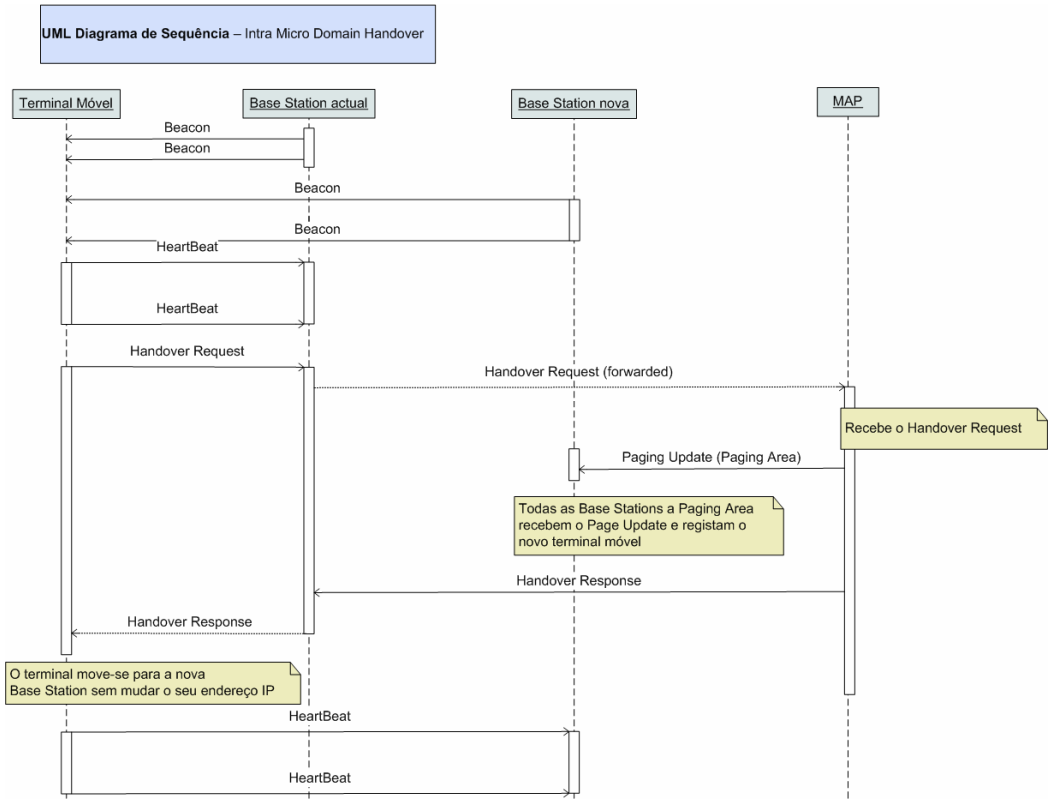


Figura 56 – LMS, Intra Micro-Domain Handover

O *MAP* envia para a nova *Paging Area* um *Paging Update* indicando todas as informações do terminal que irá chegar. As *Base Stations* da nova *Paging Area* ao receberem o *Paging Update* inserem os dados do terminal móvel nas suas *Paging Caches* criando assim um registo para o novo terminal em toda a *Paging Area*. Isto permite que o terminal ingresse em qualquer uma das *Base Stations* visto que tem um lugar reservado em todas elas. Contudo, como todas as *caches* implementam um sistema de *softstates*, e considerando que o terminal só irá indicar a sua presença numa das *Base Stations* dessa *Paging Area*, este acabará por ser eliminado de todas as outras já que a sua entrada nunca será refrescada e por isso o seu prazo de validade acabara por expirar. Como se pode

reparar este trata-se de um sistema perfeitamente adequado para ambientes de muita mobilidade e cujo registo de terminais na rede exija uma flexibilidade acrescida essencialmente durante as situações de *Handover*.

Quando o terminal recebe o *Handover Response*, este sabendo que se trata de um *Intra-Domain Handover*, não necessitará de reconfigurar o seu interface de rede nem terá de mudar de *PID*. Desta forma, *o Intra Micro-Domain Handover* efectua-se modificando apenas o *Default Gateway* do terminal móvel da *Base Station Velha* para a *Base Station Nova*. Este tipo de procedimento é extremamente rápido sendo que tipicamente demora muito poucos milissegundos.

Neste tipo de situação o sistema de *Mobilidade Global (GMP)* presente no terminal móvel não terá que efectuar um *Binding Update* ao *Home Agent* visto que o seu *Care-Of-Address IPv6* manteve-se. A mobilidade *LMS* Intra *Micro-Domínio* é completamente transparente para o mecanismo de *Mobilidade Global (GMP).* Neste tipo de *handover*, o terminal também não necessita de notificar o *MMP* da sua mudança visto que este manteve-se dentro do mesmo Micro-Domínio. Estes dois factores representam o ponto mais vantajoso dos *Protocolos de Mobilidade Local (LMP),* a redução de sinalização de controlo e o aumento de desempenho durante os *handovers* dentro do mesmo domínio de mobilidade local. A Figura 56 ilustra o diagrama de sequencia *UML* referente ao Intra Micro-Domain *Handover LMS*.

b. Inter Micro-Domain Handover

Os *Inter Micro-Domain Handover* são os *Handovers* mais complexos deste sistema. Este tipo de *Handover* exige não só o mesmo processo descrito anteriormente mas também exige a negociação do mesmo entre dois *MAPs* e o *MMP*. Neste cenário, quando o terminal pretende entrar num micro-domínio novo, ele envia para o seu *MAP* actual um pedido de *Handover Request* indicando que se trata de um *Inter Micro-Domain Handover*. O *MAP*, ao receber este pedido inicia o processo de negociação de *Handover* com o *MMP*.

O *MMP* ao receber *o Inter Micro-Domain Handover Request* procede à verificação de acesso do terminal no novo Micro-Domínio. Esta verificação pode ser efectuada questionando um agente externo *AAAC*, ou no caso da sua inexistência, questionando a *Base de Dados Central* do sistema. No caso de acesso permitido, o *MMP* gera um novo *IPv6 Care-Of-Address* e um novo *PID* para o terminal poder usar no novo micro-domínio. Antes de responder ao *MAP antigo*, o *MMP* envia um *Handover Notify* ao *MAP novo* indicando os dados referentes a este terminal móvel e pedindo um registo para ele nesse novo micro-domínio. O *MAP novo* irá verificar se a *Paging Area* requerida pelo terminal existe. Em caso de sucesso o *MAP novo* regista o terminal nas suas *caches* e envia um *Page Update* para a *Paging Area* requerida preparando assim todas as *Base Stations* da mesma para o receber. Tanto no caso da *Paging Area* existir como no caso de não existir o *MAP* novo responde sempre ao *MMP* notificando se o registo no novo domínio foi ou não bem sucedido.

O *MMP* espera por uma resposta do *MAP novo* referente ao registo do terminal no micro-domínio novo. Em caso de a resposta indicar sucesso do registo do terminal no novo micro-domínio, então o *MMP* gera um *Handover Response* com toda a informação necessária para o terminal se registar e envia o pacote para o *MAP antigo*. Em caso de a resposta do *MAP novo* ser negativa então o *MMP* gera um *Handover Response* indicando a negação do *Handover* e envia o pacote para o *MAP antigo*. O *MAP antigo* após receber o *Handover Response* do *MMP*, reencaminha-o para o terminal através do mesmo caminho por onde veio o *Handover Request*.

Quando o terminal recebe o *Handover Response*, fica apto para se poder reconfigurar para a nova rede. Nos *Inter Micro-Domain Handover*, o terminal necessita de mudar toda a sua configuração já que o micro-domínio é novo e por isso a configuração da rede é obrigatoriamente diferente do micro-domínio antigo. Assim o terminal muda o seu *PID*, efectua uma mudança de *IPv6* e *Default Gateway*. Após isto, é esperado que o Protocolo de *Mobilidade Global (GMP)* envie uma notificação ao *Home Agent*, no caso do *Mobile IPv6* um

Binding Update. No final deste processo todo, o terminal encontra-se de novo em comunicação e pode continuar todas as ligações que tinha anteriormente A Figura 57 descreve o processo de handover Inter Micro-Domínio bem sucedido.

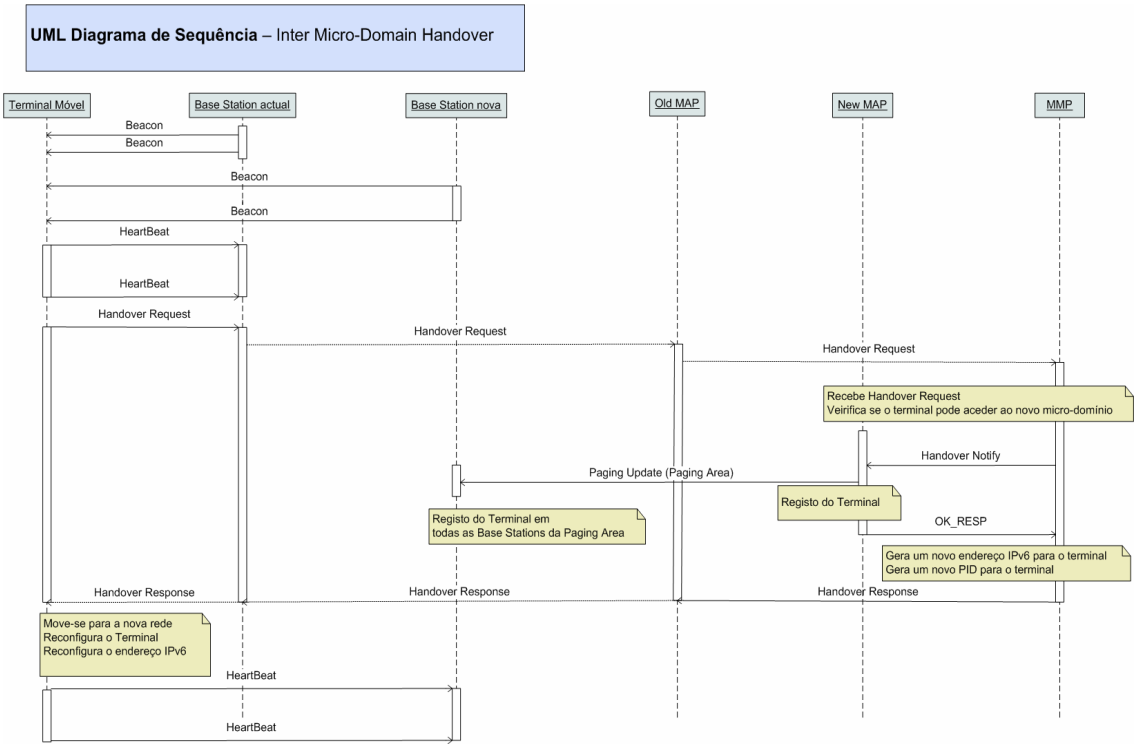


Figura 57 – LMS, processo de LMS Inter Micro Domain Handover

A Figura 58 descreve o processo de *handover* Inter Micro-Domínio com o acesso negado pelo novo *MAP* devido a recursos de rede inexistentes. Esta situação pode acontecer, por exemplo, devido ao terminal móvel pretender associar-se a uma *Paging Area* inexistente.

As figuras (Figura 58 e Figura 59) mostram o processo de handover com acesso negado pelo novo *MAP* e pelo *MMP* respectivamente. Quando o terminal obtém um acesso negado pelo novo *MAP* este deve-se ao facto de na rede de destino não existirem recursos suficientes para suportar o terminal lá. A falta de recursos pode ser de muitos tipos, mas essencialmente pode acontecer porque o número máximo de terminais na rede foi atingido ou porque o terminal móvel está a requerer um handover para uma *Paging Area* ou *Base Stations* inexistente.

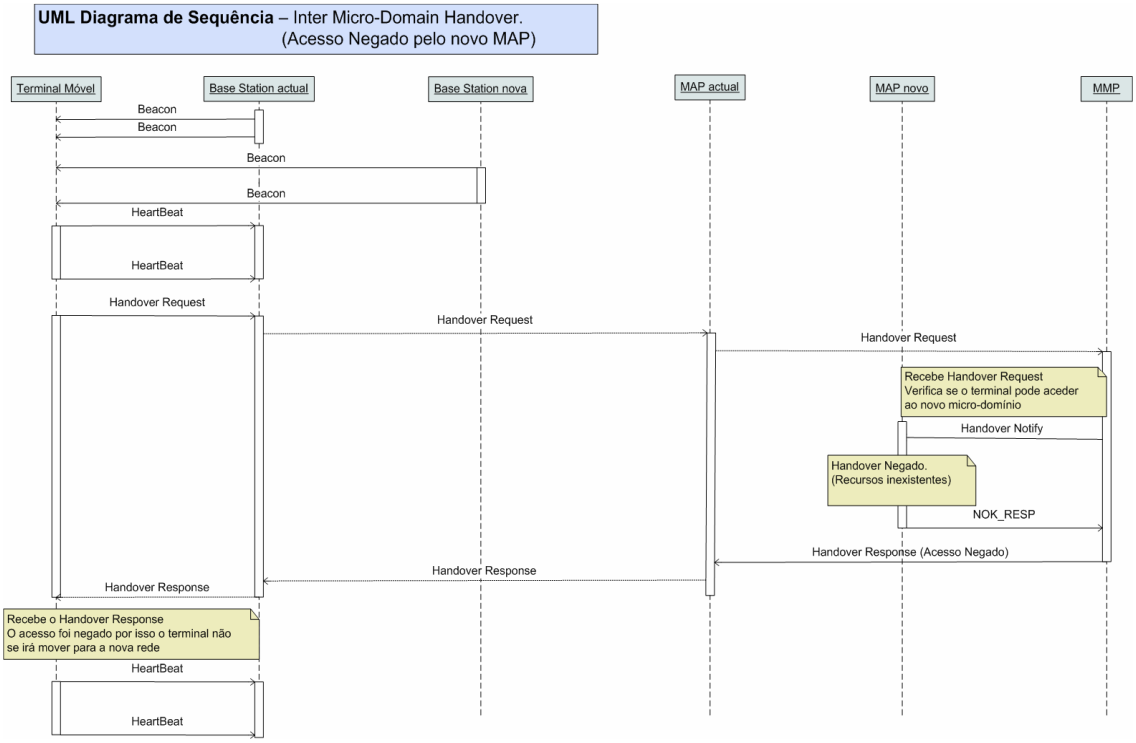


Figura 58 – LMS, Inter Micro-Domain Handover

Na Figura 59 o acesso é negado pelo *MMP* durante o processo de handover. Este facto deve-se tipicamente à tentativa de acesso a um micro-domínio do tipo *Acesso Restrito* com falta de regalias de acesso ao mesmo. Poderá também acontecer quando o terminal tenta aceder a um micro-domínio inexistente na rede de operador.

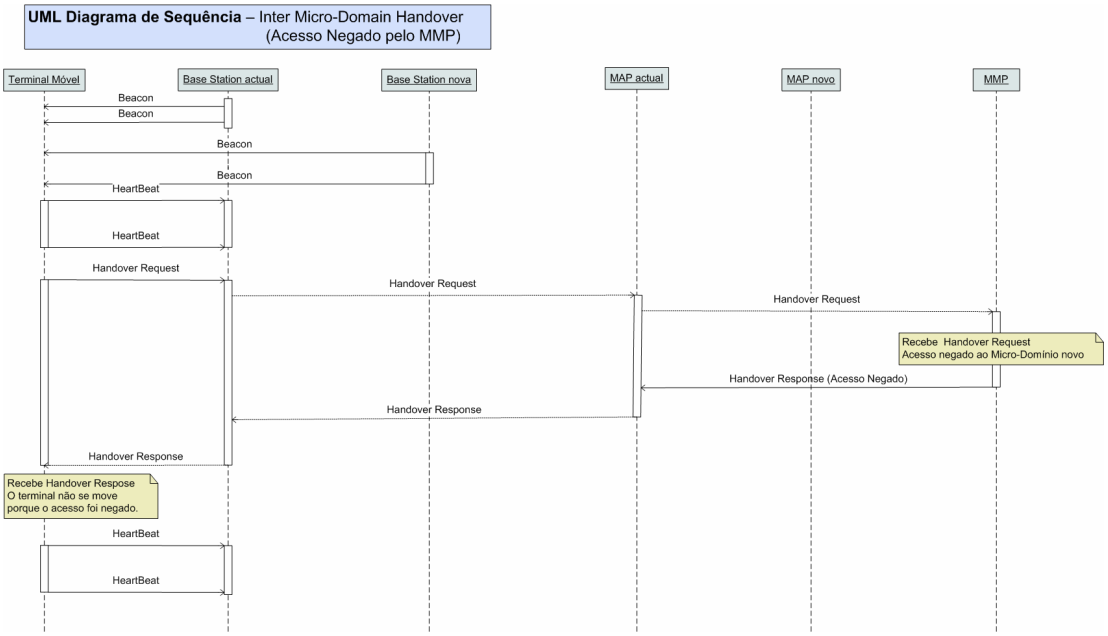


Figura 59 – LMS, Inter Micro-Domain Handover

Em ambos os casos ilustrados pelas figuras (Figura 58 e Figura 59) o *handover* é negado e o terminal não executa o procedimento de mudança de configuração. Neste caso o terminal mantém-se com o mesmo endereço IPv6, o mesmo *Gateway* e o mesmo *PID*.

3.14 Comunicação rádio

O *LMS* é um sistema preparado para actuar em redes de próxima geração onde os terminais serão obrigatoriamente móveis. O facto de serem móveis implica a utilização de mecanismos de comunicação rádio na rede de acesso ao micro-domínio. As redes de próxima geração deverão utilizar tecnologias heterogéneas de acesso ao meio. Espera-se assim encontrar diferentes tipos de tecnologias rádio tais como *UMTS* [25], *WIMAX* [26] e *WIFI* [24]. O protótipo do *LMS* serve-se da tecnologia *Ethernet* [27] para comunicar no núcleo da rede de operador e serve-se da tecnologia *WIFI* para comunicar na rede de acesso. Assim a as tecnologias base do *LMS* serão as representadas pela Figura 60.

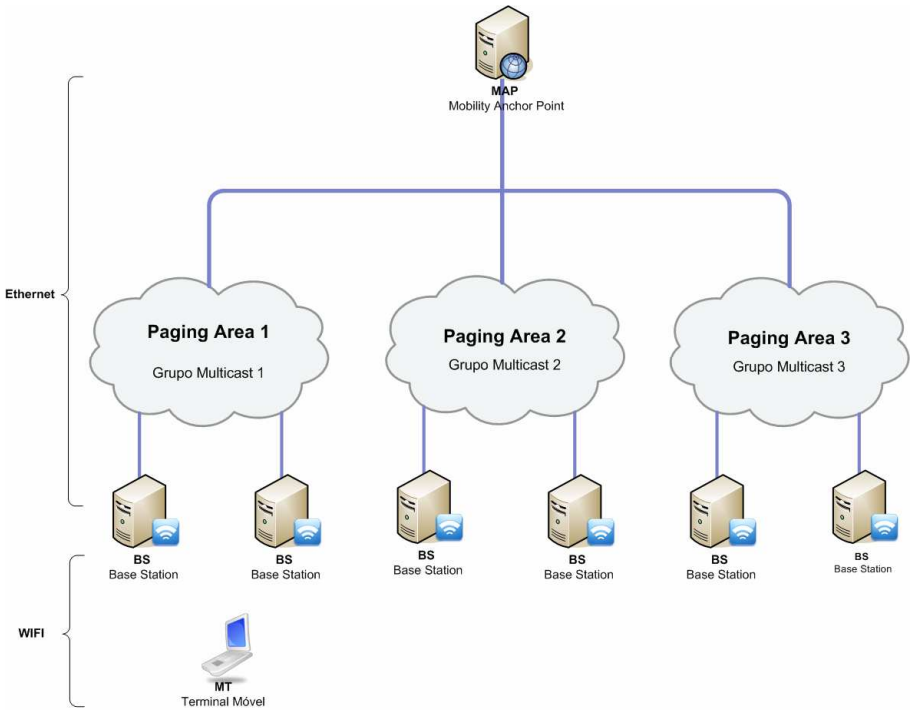


Figura 60 – LMS, tecnologias de comunicação usadas numa rede LMS

Tal como pode ser visualizado na Figura 60, no protótipo do *LMS* todos os agentes nucleares do micro-domínio comunicam através de ligações *Ethernet* e a comunicação entre o terminal móvel e as Base Stations é efectuada através de *WIFI* (IEEE802.11).Cada Base Station do micro-domínio tem um ponto de acesso *WIFI* o que permite que os terminais possam aceder de forma infra-estruturada à rede. Do ponto de vista do terminal a rede emite dois tipos diferentes de *beacons*, *IEEE802.11* e *LMS.* Os *beacons do tipo IEEE802.11* servem para o terminal identificar os pontos de acesso *IEEE802.11* a um nível físico. Estes *beacons* permitem ao terminal identificar quais as características da rede de acesso de forma a que este se possa associar a elas. Os *beacons LMS* servem para notificar o terminal das características da rede *LMS* tais como *NetworkID*, *Paging Area, Base Stations ID*, entre outros.

Quando o sistema *LMS* se inicia no terminal móvel ele começa por efectuar uma pesquisa na rede *IEEE802.11* de forma a mapear todas os pontos de acesso à sua volta. Essa pesquisa é efectuada através de uma varrimento das diferentes gamas de frequências rádio padronizadas no *IEEE802.11.* Ao efectuar esse varrimento o terminal mantém-se à escuta de pacotes do tipo *beacon IEEE802.11* e conforme vai recebendo nos diferentes canais rádio ele vai mapeando os pontos de acesso em seu redor. Após o mapeamento dos pontos de acesso *IEEE802.11* o terminal inicia outro processo de pesquisa tentando encontrar as *Base Stations LMS* em seu redor, através de um rastreamento de todos os canais onde foram mapeados pontos de acesso *IEEE802.11.* Por fim, o terminal tem um conhecimento sobre todos os pontos de acesso e *Base Stations* onde se pode associar para se ligar à rede e conhece também a qualidade de sinal rádio associado a cada um deles.

O terminal móvel *LMS* tem dois modos possíveis de funcionamento, modo automático e modo manual. Quando o terminal está em modo automático ele assume que a *Base Station* associada ao ponto de acesso com melhor sinal de rádio é o preferido pelo utilizador. Assim, após o processo de pesquisa, o terminal associa-se automaticamente ao ponto de acesso *IEEE802.11* com melhor relação sinal/ruído rádio e inicia o processo de registo na rede *LMS*. Por outro lado se o terminal estiver em modo manual este, após o processo de pesquisa inicial entra em modo de *booting.* Durante o modo de *booting* o terminal não está associado à rede e apenas vai fazendo pesquisas periódicas em seu redor para manter o mapeamento de todos os pontos de acesso e *Base Stations.* A Figura 61 demonstra como o mecanismo de detecção de redes e gestão de ligações funciona durante a sua execução em modo manual.

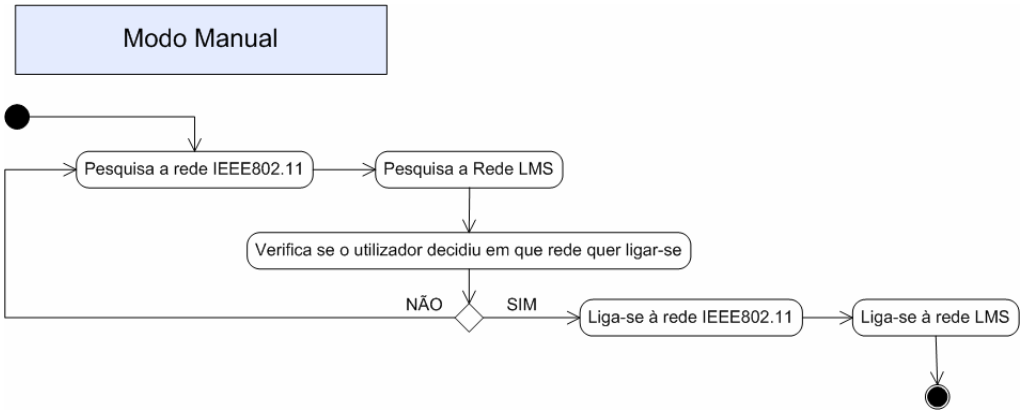


Figura 61 – LMS, mecanismo de gestão de ligações em modo manual

A Figura 62 demonstra como o mecanismo de detecção de redes e gestão de ligações funciona durante a sua execução em modo automático.

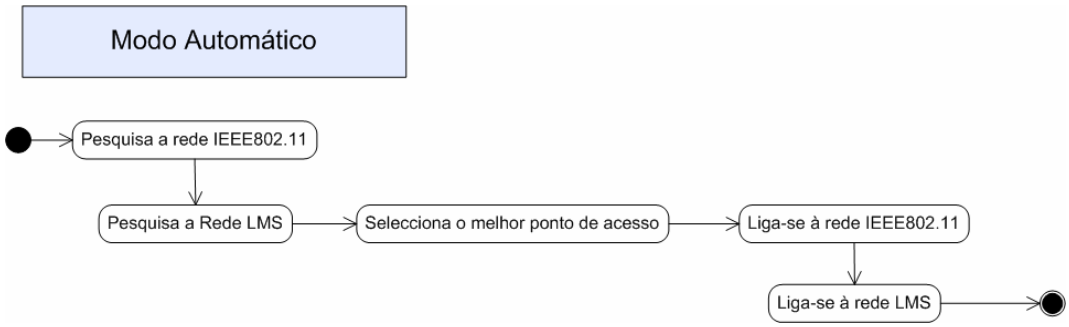


Figura 62 – LMS, mecanismo de gestão de ligações em modo Automático

A Figura 63 ilustra o processo completo que descreve o funcionamento básico do terminal quando este se encontra em modo de detecção manual das ligações à rede. Tal como pode ser observado pelo diagrama, o terminal fica à espera que o utilizador decida em que rede se pretende ligar. Após o utilizador tomar a sua decisão, o mecanismo de gestão de ligações efectua automaticamente a ligação com a rede pretendida.

Quando o terminal efectua uma pesquisa na rede *LMS* por novas *Base Stations* ele tem que percorrer todos os canais disponíveis e esperar por receber um *beacon* da rede *LMS.* Dado que os *beacons* da rede *LMS* normalmente são emitidos a uma taxa não muito elevada, para poupar recursos de rede, este tempo pode variar dos 100 (cem) milissegundos até 1 (um) segundo de espera. Neste caso, se por exemplo tivermos 6 (seis) pontos de acesso *IEEE802.11*

activos, o terminal poderia demorar até 6 (seis) segundos até conseguir efectuar o varrimento de todas as *Base Stations.*

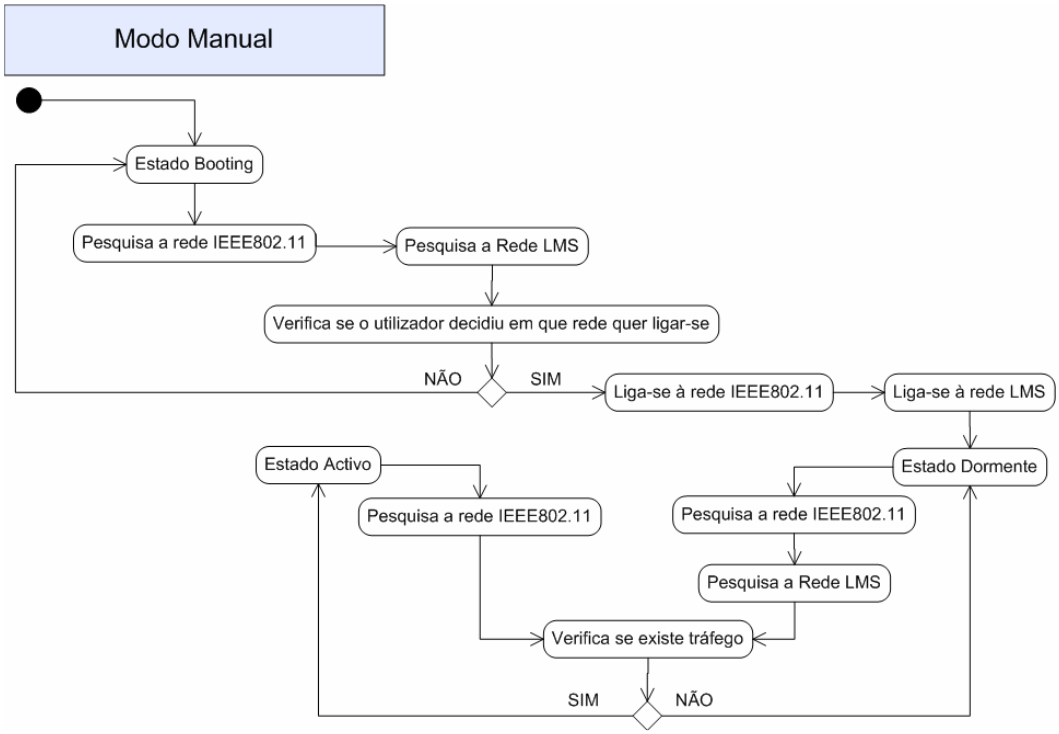


Figura 63 – LMS, diagrama que ilustra o funcionamento do terminal móvel

Para evitar este tipo de dificuldades, o terminal móvel apenas faz pesquisas completas quando se encontra em modo *Dormente* ou em modo de *Booting*. Como tal, apenas quando o terminal se encontra nestes estados é que ele executa um varrimento completo tanto dos pontos de acesso *IEEE802.11* como das *Base Stations*. Nestas situações, dado que o terminal não está a receber ou a enviar tráfego para a rede não existe problema em fazer este tipo de pesquisas dado que o impacto é probabilisticamente mínimo. Quando o terminal se encontra no estado *Activo* a enviar ou a receber pacotes de dados, o período entre pesquisas é substancialmente maior do que quando se encontra em modo *Dormente*. O período é maior dado que se pretende minimizar o impacto das pesquisas nas ligações activas do terminal. Por outro lado as pesquisas *IEEE802.11* não são tão penosas para as ligações activas como as pesquisas por Base Stations dado serem muito menos demoradas. Alem disso, algumas placas mais recentes já integram dois mecanismos de rádio separados, um para transferir dados e outro para efectuar as pesquisas, o que permite aos terminais fazerem pesquisas de rede em simultâneo com a transferência de dados.

Capítulo IV
Protótipo e Resultados

Tal como já foi descrito anteriormente, o *Local-centric Mobility System* é um sistema (arquitectura e protocolo) para redes de próxima geração com suporte de mobilidade rápida local em micro-domínios. De forma a testar o conceito de arquitectura e protocolar, desenvolveu-se um protótipo completamente funcional do *Local-centric Mobility System.* O protótipo respeitou integralmente todas as descrições efectuadas nos capítulos anteriores de forma a ser o mais realista possível em relação às considerações teóricas sobre o mesmo. A testbed foi desenvolvida com recurso a equipamento computacional padrão, computadores *x386* e equipamento de rede convencional, placas de rede *Ethernet* [27] e *WIFI (IEEE802.11)*[24]

O Software foi desenvolvido com base no sistema operação (SO) *GNU/Linux* [29][28] clássico e foi testado em duas distribuições diferentes, *Gentoo Linux* [30] e *Ubuntu* [31]. Em ambas as distribuições o sistema comportou-se da mesma forma pelo que poderá extrapolar-se que o *LMS* comportar-se-á de forma estável em qualquer distribuição *GNU/Linux,* tal como já era esperado. O sistema foi testado sobre a versão de *Kernel 2.6.17* [32] e não necessita de qualquer tipo de alteração ao mesmo para funcionar perfeitamente. O protótipo do *LMS* serve-se de ferramentas e bibliotecas de *User-Land* de forma a poder ser o mais genérico e portável possível. Desta forma, o *LMS* pode funcionar com qualquer tipo de *hardware* existente, desde que este seja suportado em *Linux*, e não tem qualquer tipo de dependências ou exigências especificas tanto de *hardware* como *software*. Assim, o *LMS* suporta todo o tipo de placas de rede *Ethernet* e *WIFI* sendo que os resultados finais de desempenho podem variar dependendo das implementações dos *drivers* das mesmas.

Todo o software pertencente ao sistema *LMS* foi desenvolvido em *ANSI C* [33] e é passível de ser compilado com *GCCv3.4* [34]. Foi desenvolvido um conjunto de bibliotecas próprias *LMS* que dão suporte ao protocolo de comunicação, sistema de gestão de *caches*, manipulação de associações de segurança entre agentes, manipulação de pacotes de dados, criação e gestão de pacotes de sinalização, comunicação com sistemas de gestão de bases de dados SQL, gestão de interfaces, gestão de recursos *wireless*, entre outros. Porem, o *LMS* serve-se de bibliotecas de sistema como base do seu funcionamento das quais se destacam a *libpcap* [35], *libssl* [36] e *libsqlite* [37] para um sistema de *SGBD SQL* embutido.

A *Testbed* foi implementada totalmente através de equipamento informático convencional, tais como computadores x386, placas de rede *Ethernet*, placas de rede *WIFI, Switchs* e *Routers IP*. O ambiente de testes foi efectuado sobre o protocolo de rede IPv6 tanto na rede de acesso como na rede nuclear do sistema visto que o *LMS* foi projectado para este protocolo de rede em especifico. Desta forma, todas as Base Stations enviam pacotes *Router Advertisement* para a rede de acesso de forma a garantir a estabilidade nas ligações de rede IPv6 entre os terminais e a rede de operador. Porem os endereços IPv6 são atribuídos dinamicamente pelo protocolo *LMS* no memento de registo com o *MMP* de forma a controlar e optimizar o processo de aquisição de endereços bem como permitir a configuração dos interfaces de rede antes mesmo de o terminal chegar à rede de destino. A Figura 64 ilustra o ambiente de testes usado para testar o sistema *LMS.*

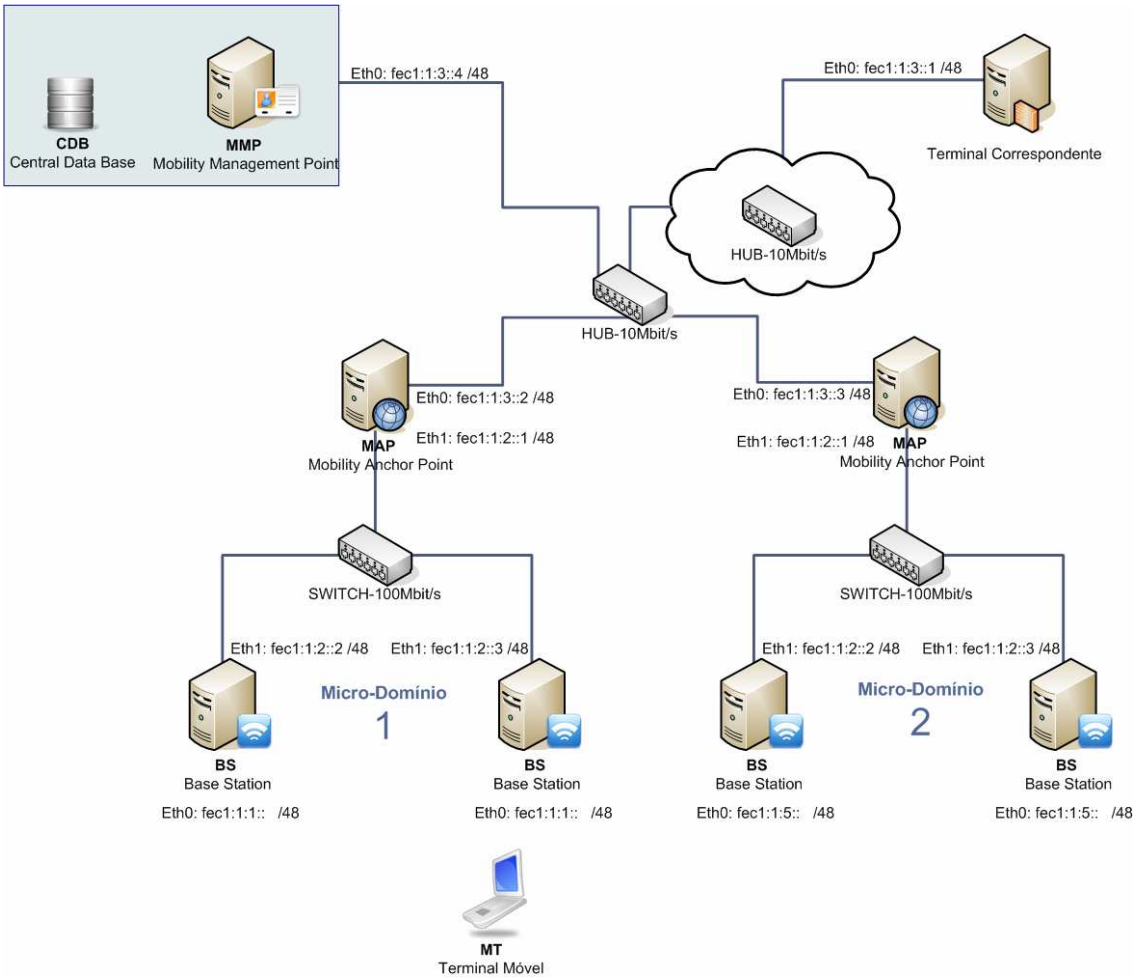


Figura 64 – LMS, ambiente de testes do LMS

Como pode ser visualizado na Figura 64, toda a rede de testes era suportada pelo protocolo IPv6. Os endereços de todos os agentes *LMS*, à excepção do *MMP* e os interfaces de rede dos *MAPs* que dão acesso a rede do *MMP*, são totalmente auto-configurados durante o processo de arranque da rede. Na figura pode-se visualizar todos os endereços usados durante a actividade do sistema em ambos os micro-domínios. Os endereços auto-configurados são guardados na base de dados central (*CDB*) e são enviados durante o processo de auto-configuração dos agentes através do *MMP*. O terminal móvel não tem endereçamento IPv6 dado que este depende do micro-domínio onde se liga e inicialmente ele não está ligado em nenhum dos existentes.

O debito binário disponibilizado pelos equipamentos de rede nuclear do ambiente de testes, *switchs* e *routers*, depende da zona da rede em questão. Dentro do micro-domínio, a rede de testes pode debitar 100Mbit/s sendo que na rede nuclear apenas pode debitar 10Mbit/s. Na rede de acesso, apenas é possível debitar 54Mbits/s, apesar de que sendo um meio partilhado sem fios, este valor nunca é conseguido na sua totalidade.

4.1 Características técnicas

Na Tabela 2 encontra-se as características técnicas dos equipamentos onde foram alojados os agentes de mobilidade *LMS.*

Entidade	Hardware
Terminal Móvel	**Memória:** 1024 MB **Cpu:** Pentium Core Duo – 1.6 GHz **Placa de Rede:** 54 Mbit/s – Ralink (Wifi)
Terminal Correspondente	**Memória:** 128 MB **Cpu:** Pentium III – 350 MHz **Placa de Rede:** 10 Mbit/s (Ethernet - Half Duplex)
Base Station	**Memória:** 512 MB **Cpu:** VIA – 1.2 GHz **Placa de Rede:** 54 Mbit/s – Atheros (Wifi)

Mobility Anchor Point (MAP)	**Memória:** 1024 MB **Cpu:** AMD Athlon XP 2600 – 1.9 GHz **Placa de Rede**: 10 Mbit/s (Ethernet - Full Duplex)
Mobility Management Point (MMP)	**Memória:** 1024 MB **Cpu:** AMD Athlon XP 2600 – 1.9 GHz **Placa de Rede**: 10 Mbit/s (Ethernet - Full Duplex)

Tabela 2 – Características técnicas do hardware usado na testbed

a. Debito Binário Teórico

Na Tabela 3 encontram-se os valores teóricos para cada troço da rede de testes apresentada anteriormente. Os valores teóricos são os valores estipulados como capacidade de débito binário dos diferentes equipamentos de rede por troço de rede.

Extremo A	Extremo B	Débito Binário Teórico
Terminal Móvel	Base Station	54 Mbit/s
Base Station	MAP	100Mbit/s
MAP	Terminal Correspondente	10Mbit/s

Tabela 3 – Débito binário teórico entre os diferentes extremos da rede

b. Debito Binário Real

A Tabela 4 mostra os valores encontrados através de testes com tráfego real em cada um dos troços da rede de testes apresentada anteriormente. Os valores foram medidos através de um software apropriado para o efeito. O Software de medição utilizado nos testes foi o IPerf [38] para um universo de 10 (dez) amostras.

Extremo A	Extremo B	Débito Binário Real (TCP)	Débito Binário Real (UDP)	Jitter (UDP)
Terminal Móvel	Base Station	19.12 Mbit/s (~0.34 Mbit/s)	24.87 Mbit/s (~1.73 Mbit/s)	1.760 ms (~0.45 ms)
Base Station	MAP	91.75 Mbit/s (~0.62Mbit/s)	95.51 Mbit/s (~1.98 Mbit/s)	0.021 ms (~0.01 ms)
MAP	Terminal Correspondente	7.18 Mbit/s (~0.17 Mbit/s)	8.76 Mbit/s (~0.45 Mbit/s)	0.644 ms (~0.11 ms)

Tabela 4 – Débito binário real entre os diferentes extremos da rede

4.2 Avaliação do Desempenho do Sistema

a. Intra Micro-Domain Handover

Um terminal móvel *LMS* pode efectuar dois tipos de *handover*, intra ou inter micro-domínio. Dependendo do tipo de *handover* o terminal tem que efectuar diferentes acções tanto internamente como de interacção com a rede. Esse conjunto de acções que o terminal tem que efectuar durante o *handover* vai representar o montante de tempo que o mesmo estará desligado da rede. Quando um terminal se move dentro do mesmo micro-domínio *LMS*, ele está a efectuar um *Intra Micro-Domain Handover*. Assim, o conjunto de acções que este tem que efectuar para concluir com sucesso o *handover* é:

- Sinalizar o *handover* com a rede
- Efectuar o *handoff* entre os dois pontos de acesso *IEEE802.11*
- Configurar o novo *Default Gateway* para a nova Base Station *LMS*.

As figuras seguintes ilustram o conjunto de procedimentos e o tempo necessário para os completar durante uma situação de handover intra micro-domínio com placas e *drivers* da *Ralink* para um fluxo de dados constante *UDP* [39] com um débito binário de 512KByte/s.

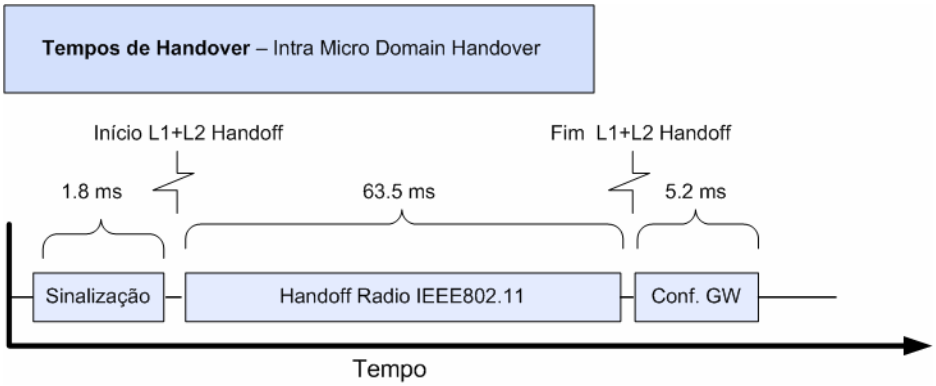


Figura 65 – LMS, Intra Micro-Domain Handover LMS

Como pode ser visualizado na Figura 65, quando o terminal pretende efectuar um *handover* dentro do mesmo micro-domínio ele tem que efectuar 3 (três) acções muito importantes. Em primeiro lugar o terminal sinaliza a sua vontade de efectuar o *handover* enviando uma mensagem de *Handover Request* para a rede de operador. A resposta demora cerca de 1.8 (1 ponto oito) milissegundos a ser processada, enviada e recebida pelo terminal móvel. Após saber a resposta, o terminal inicia o processo de *handoff* para o novo ponto de acesso à rede. Este processo não é dependente do sistema *LMS* visto que se trata exclusivamente de acções internas tanto do *Kernel Linux* como do *driver* da placa de rede sem fios *IEEE802.11.* Este tempo pode variar muito dependendo da placa de rede que se esteja a utilizar no terminal assim como da implementação do *driver* da mesma. Alguns testes efectuados paralelamente ao estudo do *LMS* demonstraram que o tempo de comutação entre dois pontos de acesso *IEEE802.11* pode variar entre os 40 (quarenta) milissegundos aos 2.5 segundos. Esta variação depende essencialmente da forma como *driver* da placa de rede *IEEE802.11* foi desenvolvido. Os testes mostraram que se o *driver* efectuar a comutação de canal de rádio e associar-se ao novo ponto de acesso sem notificar o *Kernel Linux* de que o interface de rede esteve em baixo (*down*) durante este processo de *handoff IEEE802.11* então o tempo de reassociação dura em média menos de 100 (cem) milissegundos. Este fenómeno foi encontrado durante a utilização dos *drivers* para as placas *Ralink*. Por outro lado, quando os *drivers* notificam o *Kernel Linux* de que o interface esteve em baixo (*down*) durante o processo de *handoff IEEE802.11* então o tempo pode ultrapassar o 2 (dois) segundos, como é o caso das placas *Intel Centrino IPW2200*. Testes efectuados com placas *Atheros* e respectivos drivers mostram que as mesmas comportam-se como as *Intel Centrino* sendo que o tempo de *handoff IEEE802.11* é inferior, contudo em todos os casos o tempo de *handover nunca* foi inferior a 1 (um) segundo. Por fim o terminal necessita de configurar

o *Default Gateway* o que demora em média 5.2 (cinco ponto dois) milissegundos. A Figura 66 ilustra o processo completo do *Intra Micro-Domain handover* numa rede *LMS* com placas e *drivers* da *Ralink*.

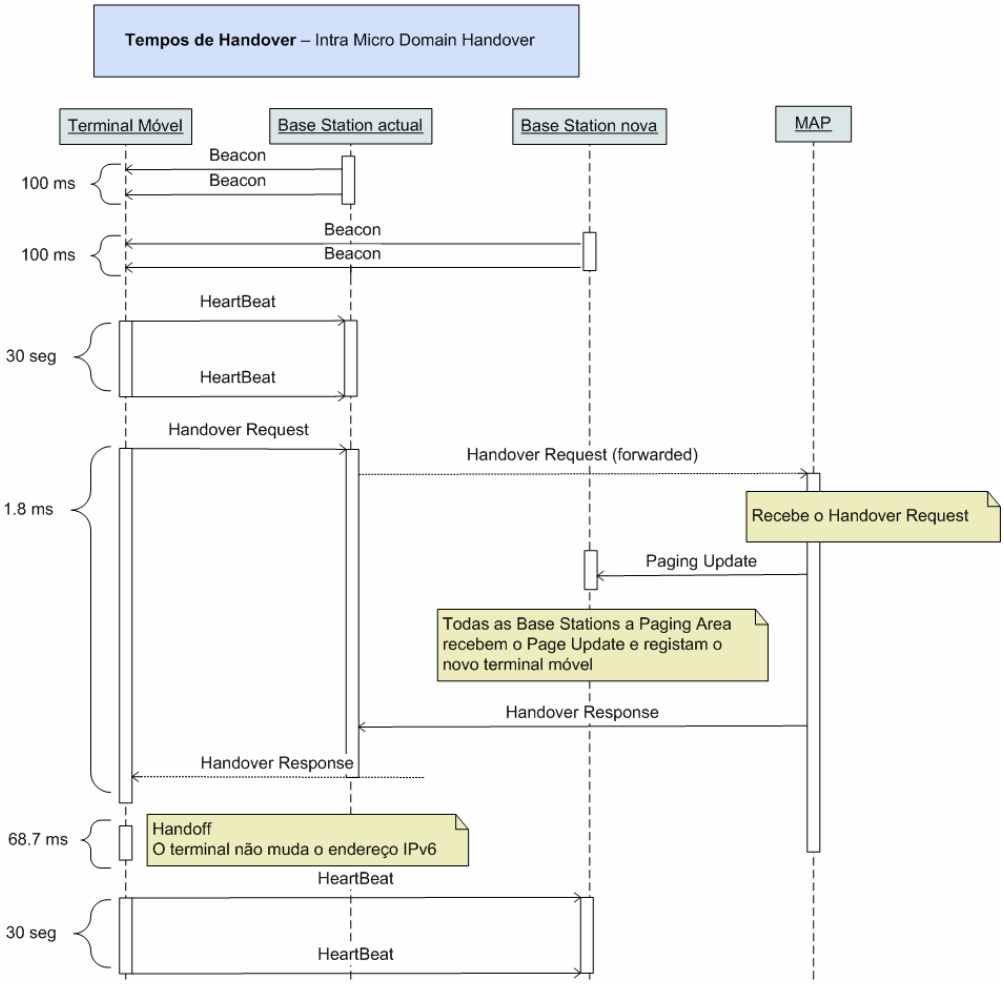


Figura 66 – LMS, procedimento e tempos do Intra Micro-Domain Handover na rede LMS

Como pode ser visualizado na Figura 66, os *handovers* dentro dos micro-domínios *LMS* são extremamente rápidos e exigem muito pouca sinalização na rede para serem conseguidos. O tempo de *blackout*, em que o terminal está desligado da rede, dá-se em menos 70 (setenta) milissegundos em média. O tempo de *blackout* é o somatório do tempo de comutação *IEEE802.11* e o tempo de configuração da camada de rede do terminal. No caso dos *Intra Micro-Domain handovers* o tempo de *blackout* é o somatório do tempo de *handoff IEEE802.11* e o tempo de configuração do *default gateway* do terminal. As tabelas seguintes ilustram os tempos para as diferentes tarefas executadas durante o handover.

	Sinalização	Handover 802.11	Configuração GW
Handover nº 1	*2*	*35*	*6*
Handover nº 2	*1*	*65*	*4*
Handover nº 3	*2*	*40*	*5*
Handover nº 4	*2*	*95*	*6*
Handover nº 5	*1*	*80*	*5*
Handover nº 6	*2*	*45*	*7*
Handover nº 7	*1*	*60*	*6*
Handover nº 8	*3*	*90*	*4*
Handover nº 9	*2*	*40*	*3*
Handover nº 10	*2*	*85*	*6*

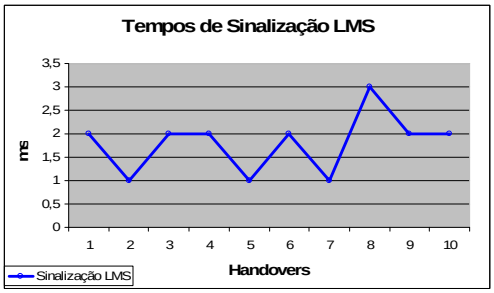
Tabela 5 – Tempos de Intra Micro-Domain handover. (ms)

A Tabela 5 representa os valores para o tempos de sinalização, tempo de handover *IEEE802.11* e configuração do *Default Gateway* durante um Inter Micro-Domain *handover*.

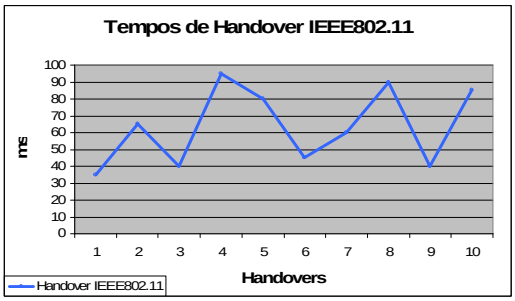
	Sinalização	Handover 802.11	Configuração GW
Média	*1.8*	*63.5*	*5.2*
Desvio Padrão	*0.63*	*22.88*	*1.15*

Tabela 6 – Média e desvio padrão para Intra Micro-Domain handover. (ms)

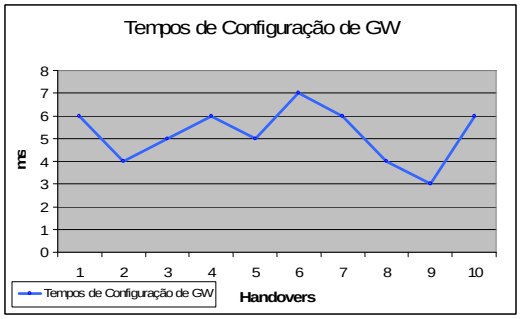
A Tabela 6 representa os valores para a média e desvio padrão para os tempos de sinalização, *handover IEEE802.11* e configuração do *Default Gateway* durante o Intra Micro-Domain handover.



(a)
tempo de sinalização



(b)
tempo de handover IEEE 802.11



(c)
tempo de configuração do default GW

Figura 67 – LMS, tempos de handover

As tabelas (Tabela 5 e Tabela 6), assim como as figuras (a), (b) e (c) (Figura 67) ilustram os tempos necessários para completar cada uma das tarefas durante o processo de *handover* ao longo de 10 (dez) *handovers*. Na figura (a) pode ser observado o tempo que o terminal demora a sinalizar o *handover* com a rede. Os pacotes de sinalização que transitam na rede têm um *RTT(Terminal Móvel, MAP)* e um tempo de processamento da decisão de handover que nos testes efectuados nunca ultrapassou os 3 (três) milissegundos e que em média ronda os 1.8 (um ponto oito) milissegundos. Pode ainda ser observado que a variação do tempo de resposta do *MAP* é de *630 (seiscentos e trinta)* micros segundos permitindo concluir que o tempo de sinalização é consideravelmente estável ao longo dos handovers. Na figura (b) pode ser observado o tempo que o terminal demora a concluir o *handover IEEE802.11*. Pode-se observar que nas condições de testes o terminal demora em média 63.5 (sessenta e três ponto cinco) milissegundos para concluir o *handover* nunca ultrapassando os 100 (cem) milissegundos. Dado o processo necessário para efectuar o handover *IEEE802.11* descrito nos capítulos anteriores, o tempo que o terminal demora a completar esta tarefa sofre flutuações na ordem dos 29 (vinte e nove) milissegundos ao longo dos diferentes *handovers* efectuados. Por fim, na figura (c) pode ser observado o tempo de configuração do *default gateway (GW)* ao longo dos diferentes *handovers*. O terminal móvel demora em média 5.2 (cinco ponto dois) milissegundos a completar a configurar do *default gateway (GW*). Em traços gerais pode-se concluir que o terminal tem um tempo de blackout, sem capacidade comunicação, inferior a 70 (setenta) milissegundos. Devido às flutuações no tempo de handover *IEEE802.11* este tempo poderá alcançar os 100 (cem) milissegundos nos piores casos. As próximas figuras ilustram o tráfego de rede recebido no terminal correspondente. Em todas as figuras o terminal móvel emitiu um fluxo de dados para terminal correspondente com um debito binário constante. No terminal correspondente foi efectuada uma captura do tráfego que posteriormente gerou os seguintes gráficos. A cada

20 segundos o terminal efectuou um *handover* entre duas *Base Stations* do mesmo Micro-Domínio alternadamente. O terminal móvel usava uma placa de rede *Ralink* nas condições gerais de funcionamento das rede de testes anteriormente descrita.

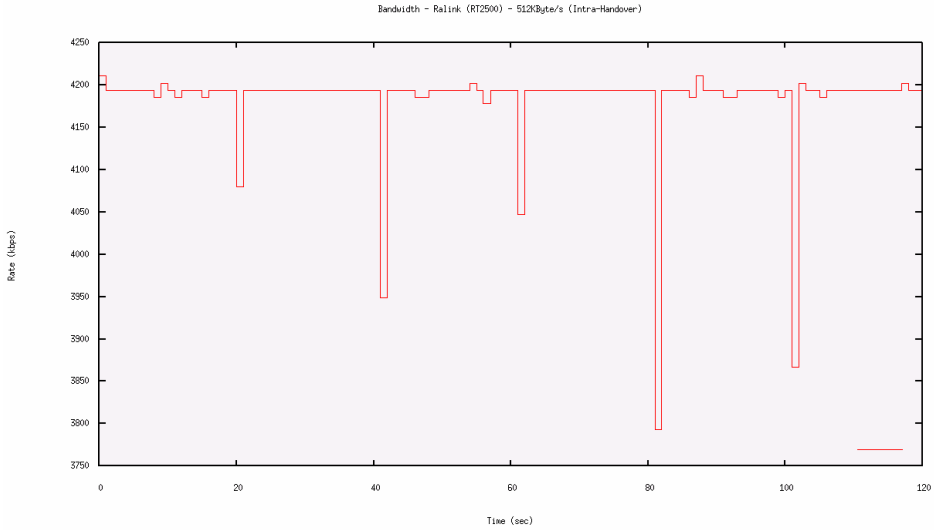


Figura 68 – LMS, Tráfego na rede durante Intra Mico-Domain Handovers com um fluxo de dados a 512KByte/s UDP

Como pode ser observado na Figura 68, o terminal móvel emitiu um fluxo de dados *UDP* [39] com um débito binário de 512KByte/s com destino ao terminal correspondente. Durante a emissão de tráfego o terminal efectuou *handovers* a cada 20 segundos. Pode ser observado na figura anterior que a transmissão foi atenuada durante os momentos de *handover* mostrando contudo que este foi bastante rápido. A próxima figura (Figura 69) mostra, para as mesmas condições, o *Jitter* obtido durante os momentos de *handover*.

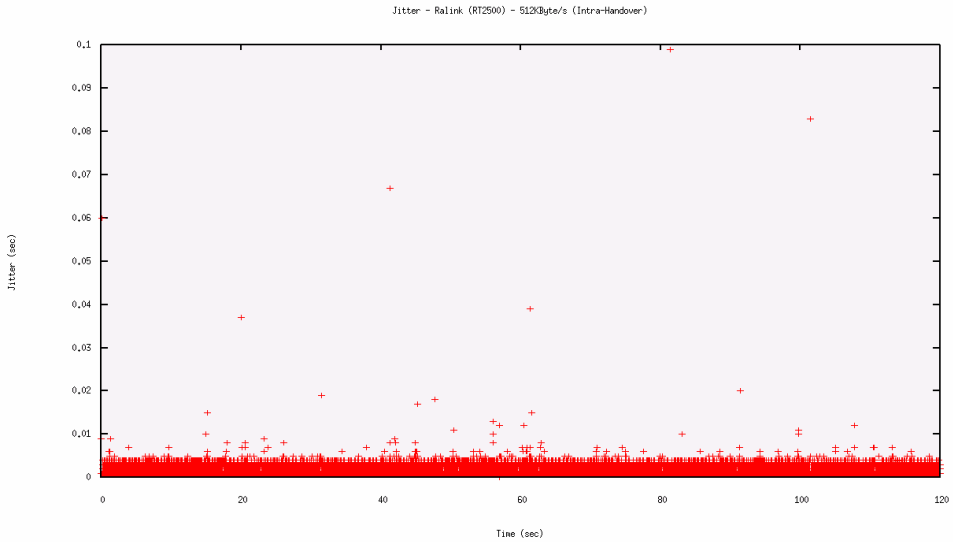


Figura 69 – LMS, Jitter dos dados durante Intra Micro-Domain Handovers com um fluxo de dados a 512KByte/s UDP

Neste cenário, poderá entender-se o *Jitter* como uma variação estatística do atraso na entrega de dados na rede do micro-domínio. Desta forma, poderá observar-se que nos momentos de *handover,* aos segundos {20,40,60,80,100}, destacam-se valores de *Jitter* entre os 40 (quarenta) e os 100 (cem) milissegundos. Dado a essência do conceito de *Jitter* pode-se observar que o tempo de *handover* é dado pelo *Jitter* nos instantes de tempo {20,40,60,80,100}. Assim, observa-se que o tempo de *handover* nunca ultrapassa os 100 (cem) milissegundos e que em média ronda os 70 (setenta) milissegundos de *blackout*.

A Figura 70 ilustra a perda de pacotes durante os momentos de handover nos instantes de tempo {20,40,60,80,100}. Como pode ser observado pela figura, a perda de pacotes é bastante baixa para os *handovers Intra Micro-Domain.* Para um fluxo de pacotes *UDP* com um débito binário de 512KByte/s, encontra-se uma percentagem de perda de pacotes inferior a 5% em média durante o handover. Os dados que se podem obter através desta figura mostram que o *LMS* pode suportar mobilidade rápida com atenuações muito ligeiras na transmissão de dados e por isso mostra-se capaz de suportar tráfego com requisitos de tempo real. Como tal, se um micro-domínio cobrir uma pequena cidade ou um campus grande, um terminal móvel poderá mover livremente dentro do micro-domínio sem que, por exemplo, a sua chamada de vídeo-telefonía seja gravemente afectada pelos *handovers* em causa.

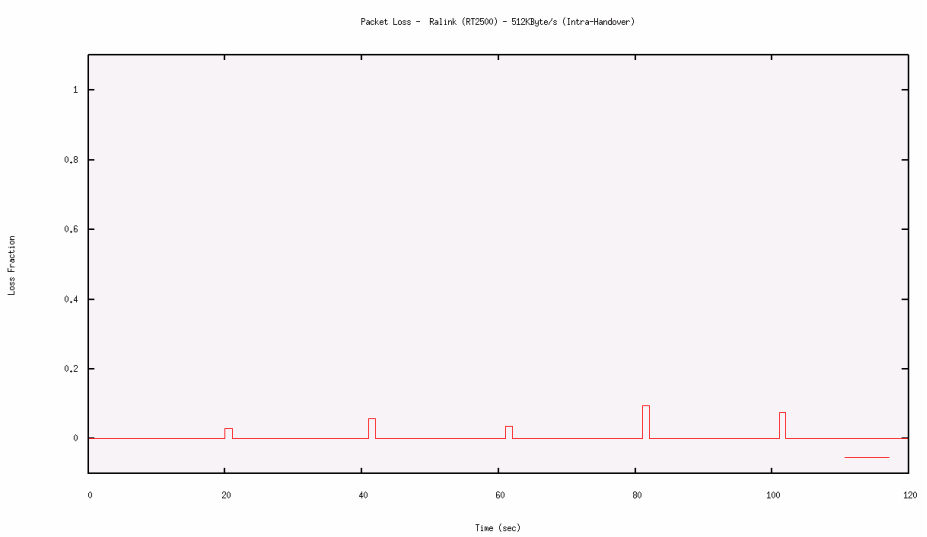


Figura 70 – LMS, perda de pacotes de dados durante Intra Micro-Domain Handover com um fluxo de dados a 512KByte/s UDP

Dado a forma como o *TCP* [40] opera durante uma sessão de dados, os *handovers* podem prejudicar gravemente a ligação, não só no preciso instante em que ocorrem, mas também nos tempos seguintes. Sempre que o terminal efectua um *handover* a pilha protocolar *TCP* detecta a interrupção na transmissão dos pacotes de dados e relaciona este facto com o congestionamento da rede. Por conseguinte, para a pilha protocolar *TCP,* quanto maior o tempo de *blackout* maior o congestionamento na rede. Após detectar o suposto congestionamento, a pilha protocolar *TCP* vai reduzindo o tamanho da janela de transmissão de forma a diminuir o tráfego emitido pelo terminal evitando aumentar o congestionamento geral da rede. Por esta razão, se o tempo de *handover* está intimamente ligado à qualidade da ligação após os momentos de *handover.* Assim, quanto menor o tempo de *handover* melhor a desempenho das sessões *TCP* durante e após os *handovers* serem executados. A Figura 71 mostra como os *handovers* afectam o tráfego *TCP* [40] durante a comunicação entre o terminal móvel e o terminal correspondente

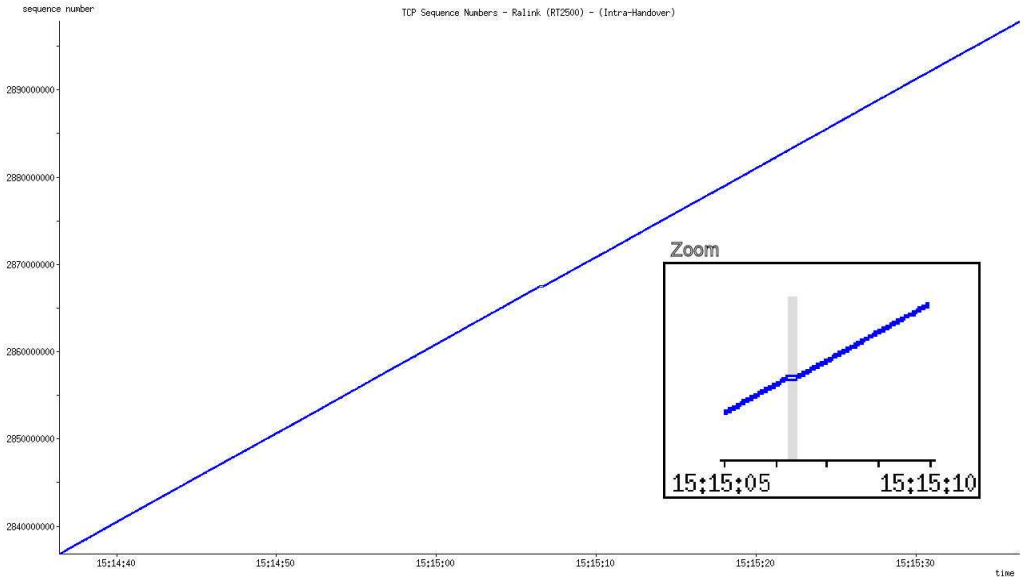


Figura 71 – LMS, impacto no número de sequencia TCP durante Intra Micro-Domain Handover

Na Figura 71 pode ser observado como um *handover* afecta uma sessão *TCP* estabelecida entre o terminal móvel e o terminal correspondente. O *handover* ocorre entre os instantes 15:15:05 e 15:15:10 durante a sessão estabelecida. Como pode ser observado, *handover* praticamente não afecta a transmissão de dados dado a sua rapidez e eficiência. Assim, o *LMS* cumpre os seus requisitos e mantém tempos de *handover* extremamente baixos com um custo mínimo de sinalização e com um impacto quase nulo nas ligações de dados estabelecidas entre o terminal móvel e o terminal correspondente. Em termos de tráfego *UDP* a figura seguinte

apresenta o débito binário do terminal durante os processos de handover.

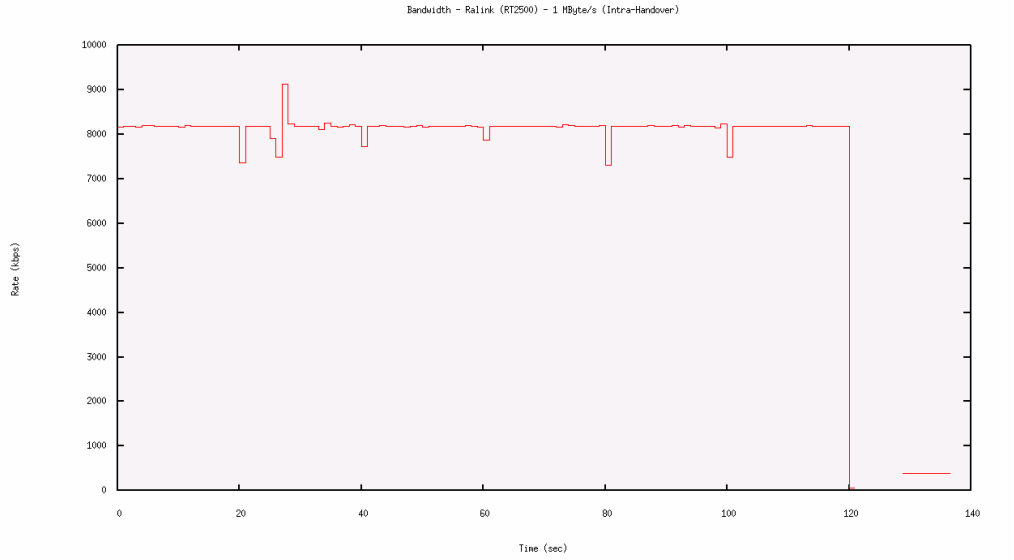


Figura 72 – LMS, tráfego na rede durante Intra Micro-Domain Handover com o fluxo de dados a 1MByte/s UDP

Como pode ser observado na Figura 72, o terminal móvel emitiu um fluxo de dados *UDP*[39] com um débito binário de 1MByte/s com destino ao terminal correspondente. Durante a emissão de tráfego o terminal efectuou *handovers* a cada 20 segundos. Pode ser observado na figura anterior que a transmissão foi atenuada durante os momentos de *handover* contudo este foi suficientemente rápido para nunca deixar o débito binário atingir o nível zero. Comparado com os valores para 512KByte/s, apesar da escala ser diferente para ambas, pode-se constatar que os resultados são igualmente bons em ambos os casos.

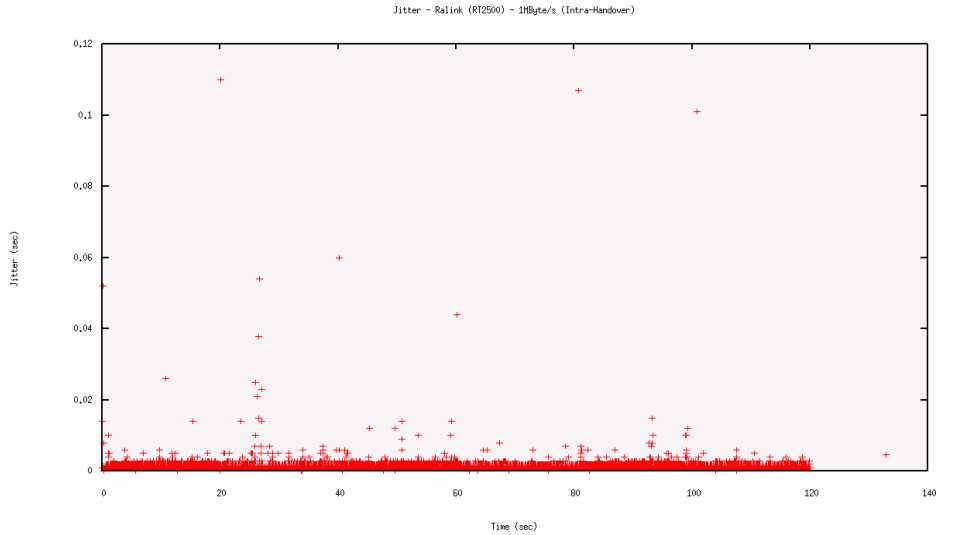


Figura 73 – LMS, Jitter na rede durante Intra Micro-Domain Handovers com um fluxo de dados a 1MByte/S UDP

A Figura 73, para as mesmas condições, o *Jitter* obtido durante os momentos de *handover*. Poderá observar-se que nos momentos de *handover,* aos segundos {20,40,60,80,100}, destacam-se valores de *Jitter* entre os 40 (quarenta) e os 110 (cento e dez) milissegundos. Comparado valores de *Jitter* obtidos para um fluxo de 512KByte/s pode-se observar que os valores são coerentes. Mesmo para fluxos de 1MByte/s o sistema mantém tempos de *blackout* substancialmente reduzidos o tendo assim um impacto bastante pequeno no tráfego de tempo real, tal como por exemplo tráfego multimédia.

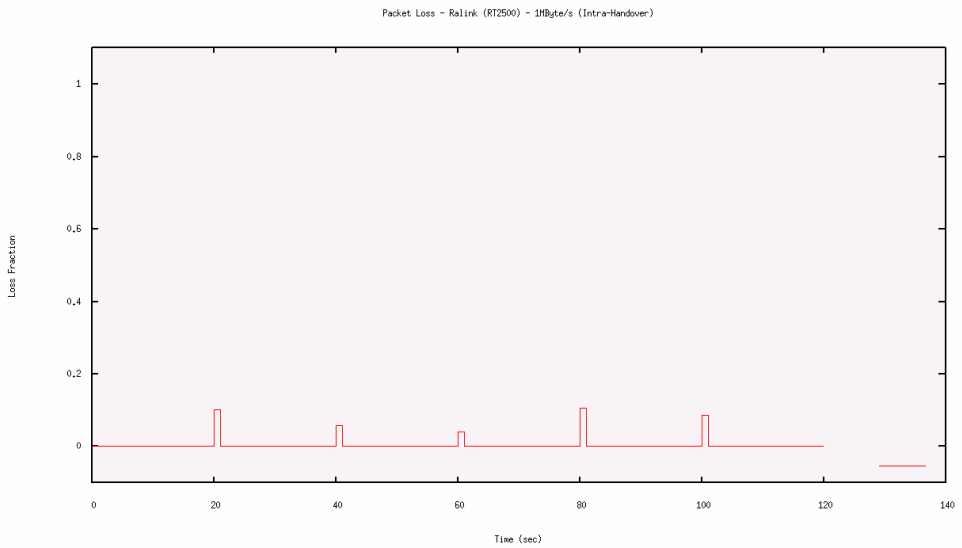


Figura 74 – LMS, perda de pacotes durante um Intra Micro-Domain Handover com um fluxo de 1 MByte/s UDP

.

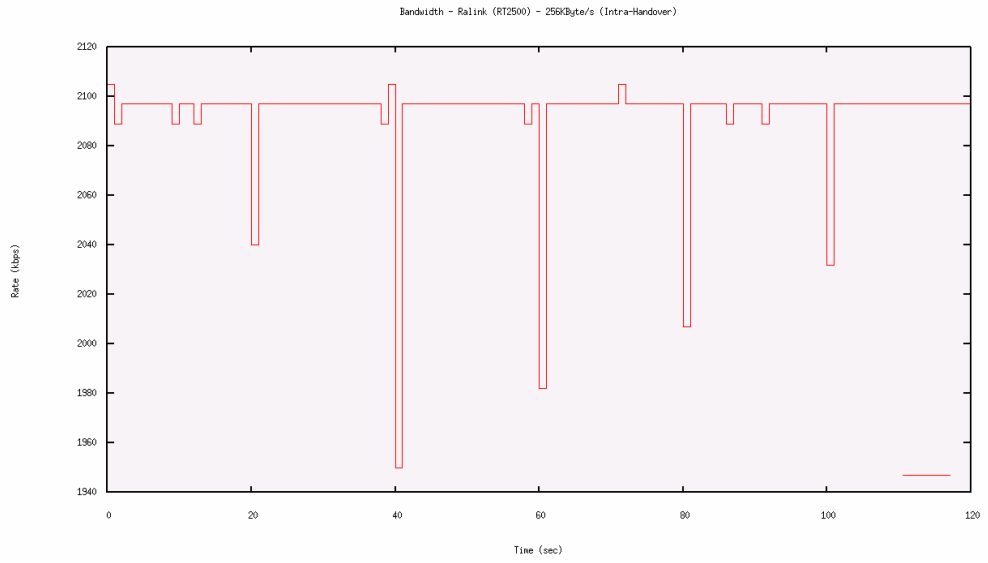


Figura 75 – LMS, tráfego na rede durante um Intra Micro-Domain Handover com um fluxo de dados 250KByte/s UDP

Na pode ser observado um fluxo de dados *UDP*[39] emitido pelo terminal móvel com um débito binário de 250KByte/s com destino ao terminal correspondente. Durante a emissão de tráfego o terminal efectuou *handovers* a cada 20 segundos. Pode ser observado na Figura 75 que a transmissão foi atenuada durante os momentos de *handover* contudo este foi bastante eficiente. Comparado com os valores para 512KByte/s e 1MByte/s, apesar da escala ser diferente para ambas, pode-se constatar que os resultados são igualmente bons em todos os casos.

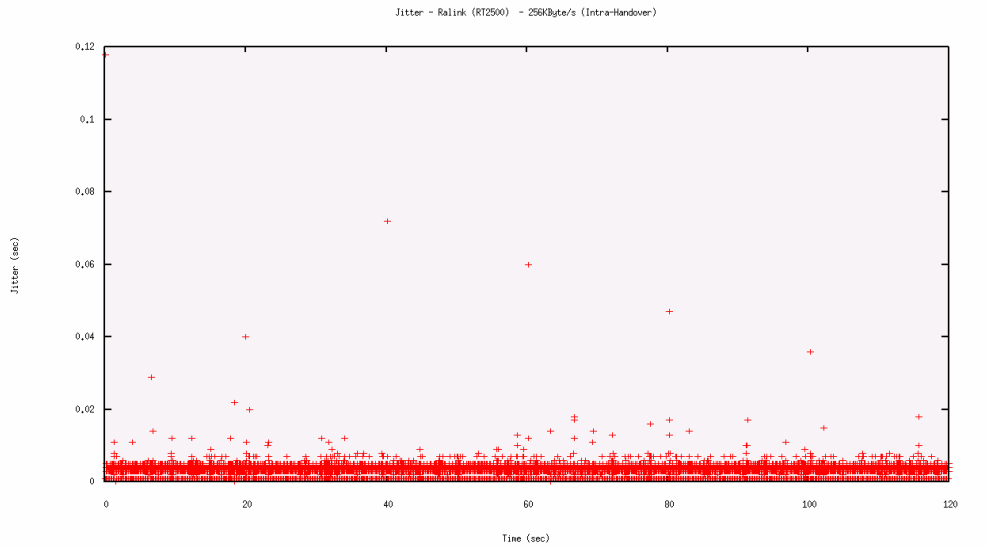


Figura 76 – LMS, Jitter na rede durante um Intra Micro-Domain Handover com fluxo de dados a 250 KByte/s UDP

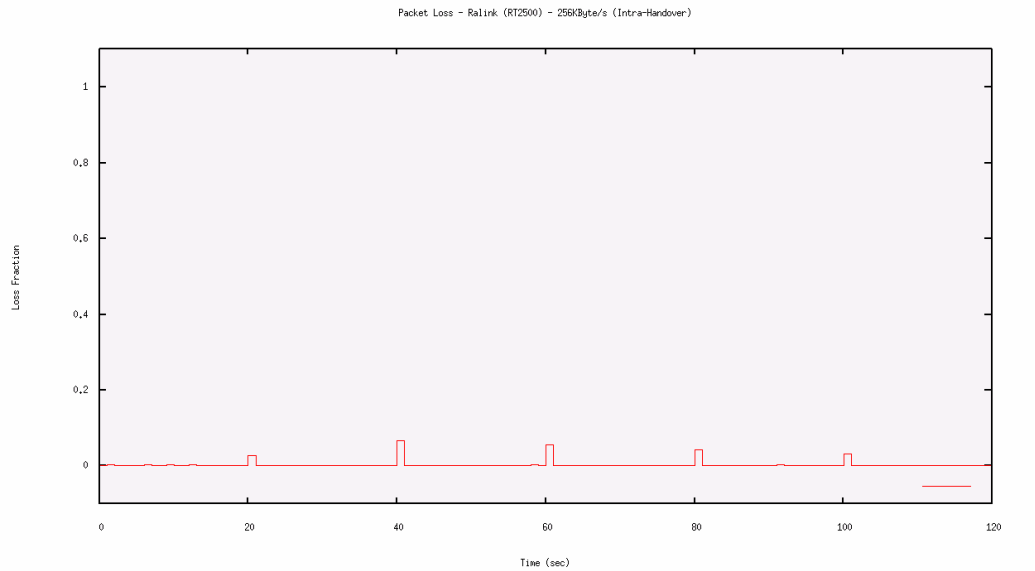


Figura 77 – LMS, perda de pacotes na rede durante um Intra Micro-Domain Handover com um fluxo de dados 250KByte/s UDP

.

Nas figuras (Figura 76 e Figura 77) pode ser observado o comportamento do sistema perante o Jitter e perda de pacotes na rede durante os momentos de *handover*. Na primeira figura pode ser observado o *Jitter* associado ao fluxo de dados entre o terminal móvel e o terminal correspondente. As variação dos valores durante os tempos de handover mostram ser ligeiramente menores do que as encontradas para 1MByte/s e 512KByte/s contudo mantendo-se coerente com as anteriores. A figura mostra um tempo de *blackout* nunca superior a 80 milissegundos o que, mais uma vez comprava que o *LMS* cumpre o seu papel como um protocolo de mobilidade rápida. Por fim, na segundo figura pode-se verificar a perda de pacotes associada a cada momento de handover. Como pode ser visualizado, a perda de pacotes é bastante reduzida nunca ultrapassando os 10% (dez por cento) de perdas de pacotes estando coerente com os restantes valores para os cenários de 512KByte/s e 1MByte/s.

As figuras (Figura 78 e Figura 79) ilustram o *Jitter* durante os *handovers* na rede. Neste caso, dado as características do *Jitter* pode-se também verificar o tempo de *blackout*, em que o terminal esteve sem capacidade de comunicação.

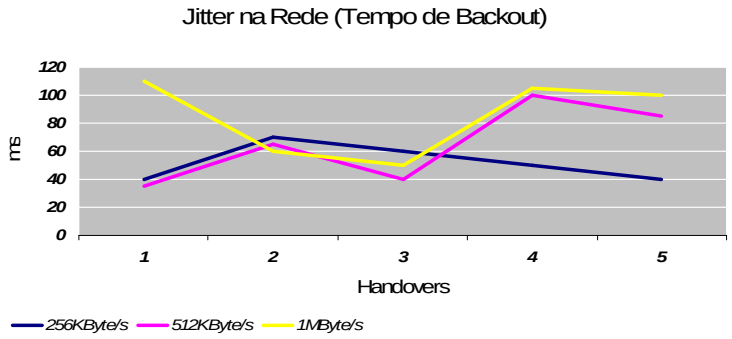


Figura 78 – LMS, Jitter na rede durante Intra Micro-Domain Handovers para fluxos de dados UDP com 256KByte/s, 512KByte/s e 1MByte/s

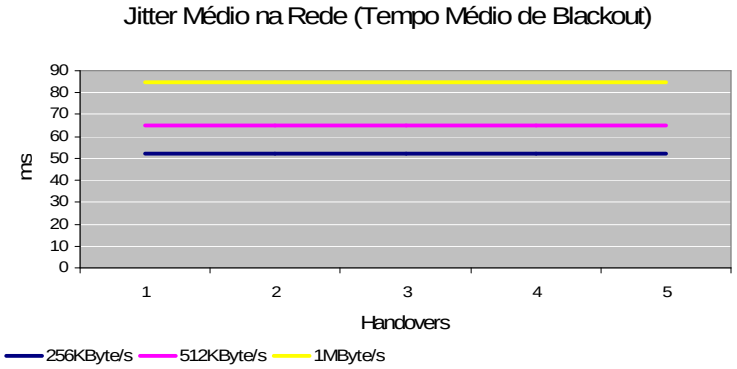


Figura 79 – LMS, Jitter médio na rede durante Intra Micro Domain Handovers para fluxos de dados UDP com 256KByte/s, 512KByte/s e 1MByte/s

As figuras (Figura 80 e Figura 81) ilustram a percentagem de perda de pacotes durante os *handovers* na rede.

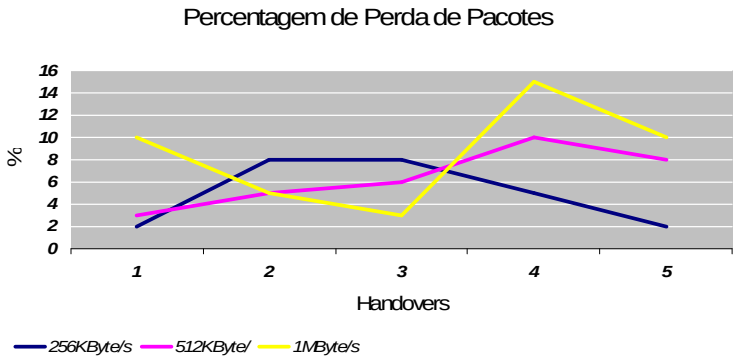


Figura 80 – LMS, percentagem de pacotes perdidos na rede durante Intra Micro-Domain Handovers para fluxos de dados UDP com 256KByte/s, 512KByte/s e 1MByte/s

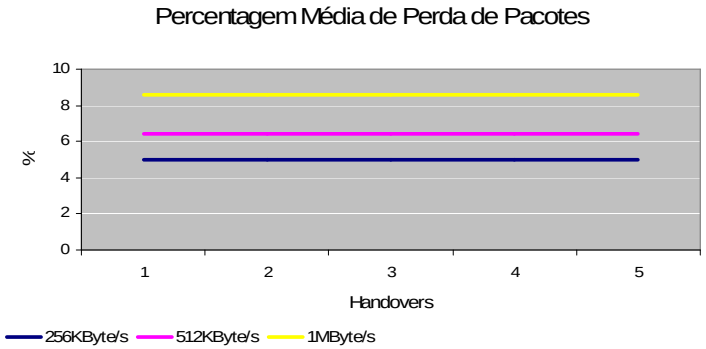


Figura 81 – LMS, percentagem média de pacotes perdidos numa rede durante Intra Micro-Domain Handovers para fluxos de dados UDP com 256KByte/s, 521KByte/s e 1MByte/s

b. Inter Micro-Domain Handovers

Quando o terminal se desloca entre dois micro-domínios diferentes ele executa um *Inter Micro-Domain handover*. Apesar de o *LMS* preparar os recursos no novo micro-domínio pró-activamente, este tipo de handovers é essencialmente de domínio global e da responsabilidade do protocolo de mobilidade global. Os *Inter Micro-Domain Handovers* são substancialmente diferentes dos *Intra Micro-Domain handovers* visto que os recursos de rede têm que ser reservados e preparados na rede do micro-domínio de destino. Essa preparação é efectuada através da negociação entre os *MAPs* e o *MMP* da rede de operador. Após a preparação dos recursos de rede, o terminal é notificado com uma resposta vinda do *MMP*

indicando se o *handover* foi aceite e qual a configuração que o terminal deve efectuar para se poder ligar no novo micro-domínio. Após este processo o terminal inicia o *handover* propriamente dito fazendo a comutação entre os diferentes pontos de acesso *IEEE802.11*. Posteriormente o terminal necessita de enviar outra mensagem de actualização para o terminal correspondente *(TC)* indicando o seu novo endereço IPv6 de forma a optimizar as rotas de encaminhamento IP existentes. Após este processo estar concluído o terminal encontra-se de novo ligado na rede podendo continuar a transmissão de pacotes sem qualquer problema. Opcionalmente, o terminal móvel pode proceder ao mecanismo de *Return-Routability*. A Figura 82 ilustra o processo de *handover* assim como os tempos necessários para completar cada uma das actividades executadas pelo terminal.

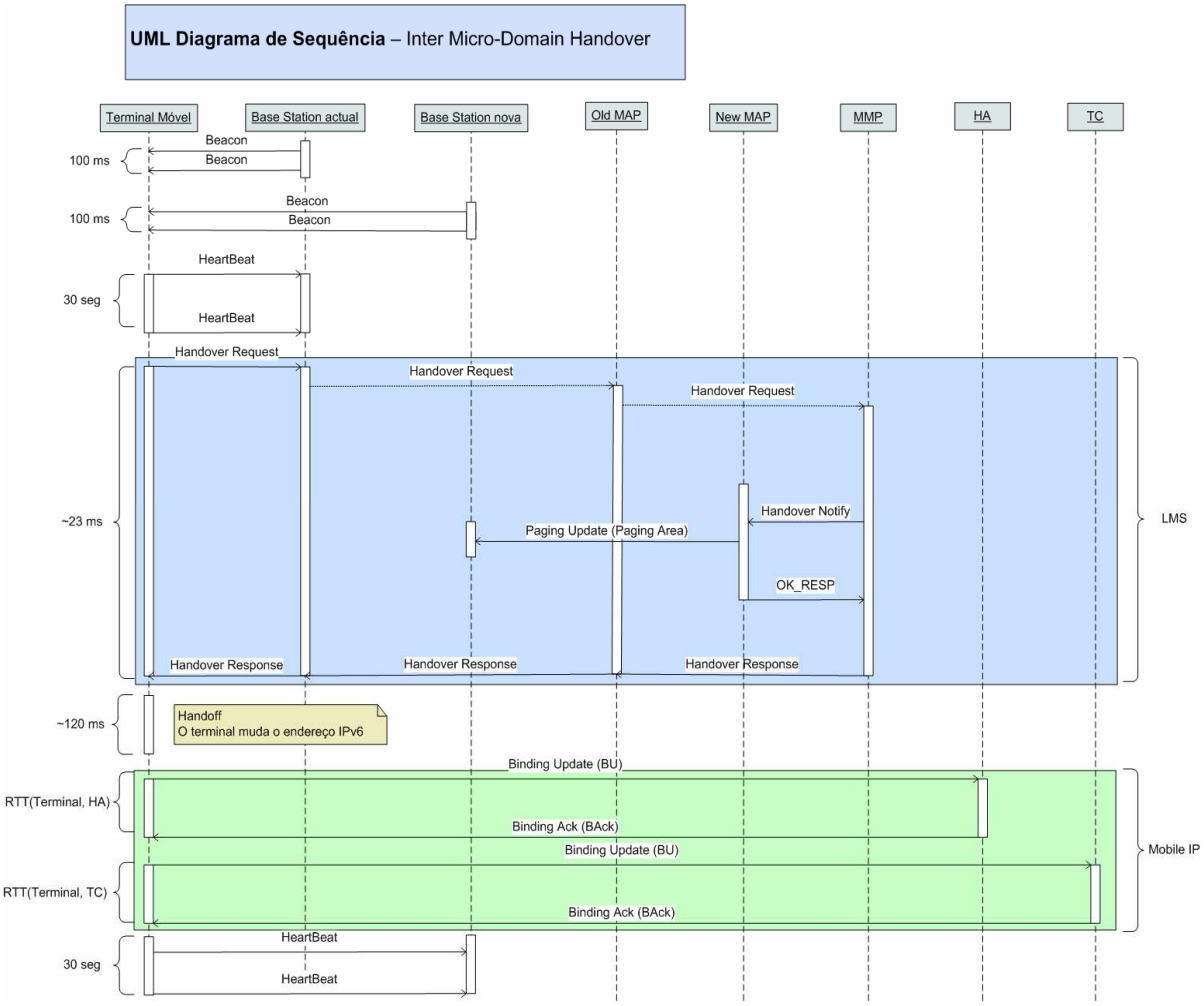


Figura 82 – LMS, Procedimento e tempos do Inter Micro-Domain Handover na rede LMS

Como pode ser observado pelo diagrama da Figura 82 os *Inter Micro-Domain Handovers* ocorrem em 2 fases distintas. Em primeiro lugar, o terminal sinaliza o *handover* com o micro-domínio corrente enviando uma mensagem de *Handover Request.* A rede processa o pedido e efectua a reserva de recursos no novo micro-domínio preparando-o para a chegada do terminal móvel. Após este processo, o terminal recebe uma resposta do sistema *LMS* informando-o se pode ou não associar-se no novo domínio e quais as configurações este deve tomar para o conseguir. Como tal, caso o terminal tenha tido autorização efectua o *handoff IEEE802.11* para o novo ponto de acesso e configura o seu interface de rede correctamente com base na informação obtida no *Handover Response.* Após este momento o *handover LMS* terminou e cabe ao protocolo de mobilidade global actualizar a localização geográfica do terminal no *Home Agente (HA)*. Por conseguinte, o protocolo de mobilidade global apercebe-se que entrou noutro domínio de rede, devido aos *Router Advertisements*, e envia uma mensagem de *Binding Update* para o *Home Agent*. O *Home Agent* actualiza a localização geográfica do terminal móvel e resposta com um *Binding Ack.* Opcionalmente, o terminal envia uma mensagem de *Binding Update* para o terminal correspondente, caso este tenha suporte de mobilidade, de forma a optimizar as rotas de encaminhamento de pacotes até ele. Após este processo, o mecanismo de handover é dado por completo e o terminal encontra-se novamente em comunicação com o terminal correspondente. A Figura 83 descreve a sequencia e duração das acções principais do terminal móvel.

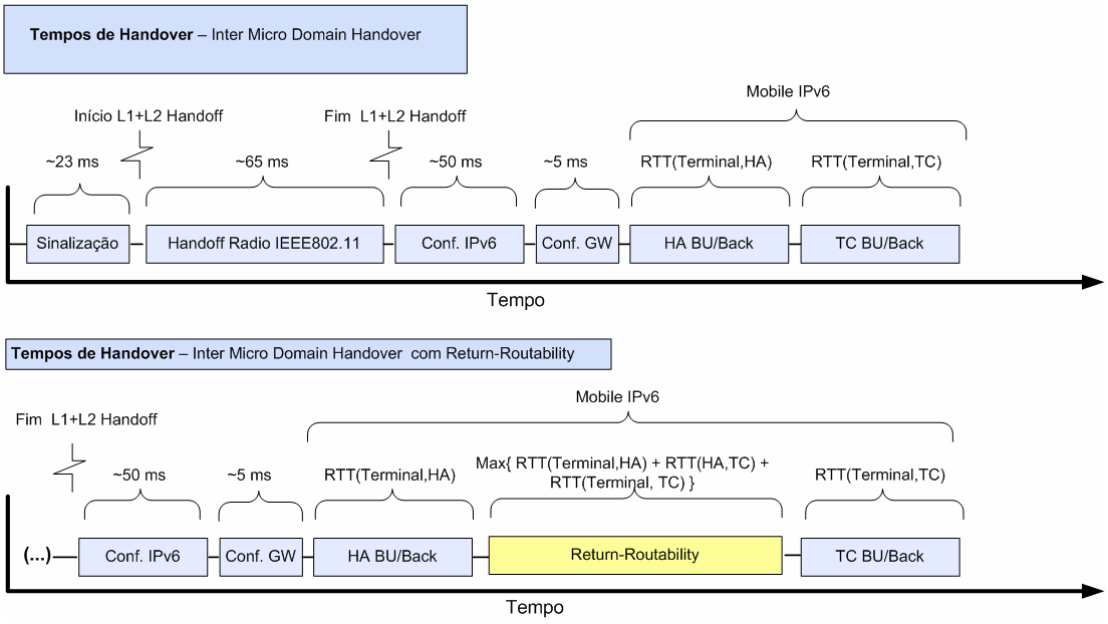


Figura 83 – LMS, Procedimento e tempos do Inter Micro-Domain Handover na rede LMS

Como pode ser verificado na Figura 83 o terminal, no caso geral, tem que executar 6 (seis) actividades importantes. Em primeiro, ele sinaliza o *handover,* ainda no seu micro-domínio, de forma a reservar os recursos no domínio de destino, demorando cerca de 23 (vinte e três) milissegundos a efectuar este procedimento. Após isto, o terminal inicia o processo de *handoff IEEE802.11* para o novo ponto de acesso demorando 65 (sessenta e cinco) milissegundos a ficar associado no mesmo. Após obter ligação ao nível da camada L1 e L2, o terminal configura o seu endereço IPv6 e *Default GW* com base na informação recebida no *Handover Response* emitido pelo *MMP* ainda no micro-domínio antigo, demorando cerca de 55 (cinquenta e cinco) milissegundos a terminar a sua configuração de rede. Após o terminal se associar ao novo ponto de acesso *IEEE802.11*, a pilha protocolar de mobilidade global detecta que o terminal se encontra num micro-domínio diferente dado que o prefixo de rede IPv6 anunciado nos *Router Advertisements* pelas Base Stations é diferente. Desta forma, o protocolo de mobilidade global inicia a actualização da informação da posição topológica do terminal ao *Home Agent* demorando um tempo *de Round Trip Time (RTT),* ou seja o tempo de uma mensagem percorrer a rede até ao *Home Agent* e voltar ao terminal móvel. Opcionalmente o terminal sinaliza a sua posição topológica ao terminal correspondente (*TC*) demorando um tempo *de Round Trip Time (RTT),* ou seja o tempo de uma mensagem percorrer a rede até ao terminal correspondente e voltar ao terminal móvel. Os tempos de *RTT* não são estáticos nem estimáveis facilmente pois dependem da distancia física e topológica a que o *Home Agent* e o terminal correspondente se encontram do terminal móvel. Tal como é mostrado na figura anterior, opcionalmente o terminal pode efectuar o procedimento de *Return-Routability* demorando o tempo máximo do somatório dos diferentes *RTT,* ou seja *Max{RTT(Terminal Móvel, Home Agent) + RTT(Home Agente, Terminal Correspondente) + RTT(Terminal Móvel, Terminal Correspondente)}.*

Após este processo estar completo, o terminal móvel encontra-se perfeitamente configurado e capaz de continuar a transmitir normalmente. Como tal, o mecanismo de *handover* entre os dois micro-domínios é dado por concluído após o *Binding Ack* do ultimo terminal correspondente a ser contactado pelo terminal móvel durante a actualização topológica. As tabelas (Tabela 7 e Tabela 8) ilustram os tempos necessários para cumprir cada tarefa a ser executada pelo terminal durante 10 handovers.

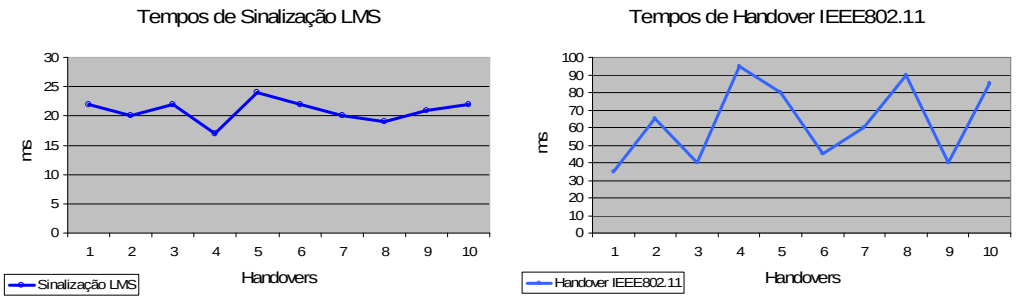
	Sinalização	Handover 802.11	Config. GW	Config. IPv6
Handover nº 1	*22*	*35*	*6*	*43*
Handover nº 2	*20*	*65*	*4*	*42*
Handover nº 3	*22*	*40*	*5*	*58*
Handover nº 4	*17*	*95*	*6*	*47*
Handover nº 5	*24*	*80*	*5*	*49*
Handover nº 6	*22*	*45*	*7*	*34*
Handover nº 7	*20*	*60*	*6*	*52*
Handover nº 8	*19*	*90*	*4*	*57*
Handover nº 9	*21*	*40*	*3*	*43*
Handover nº 10	*22*	*85*	*6*	*47*

Tabela 7 – Tempos de sinalização, handover IEEE 802.11 e configuração do default gateway durante um inter micro-domain handover. Resultados em milissegundos (ms)

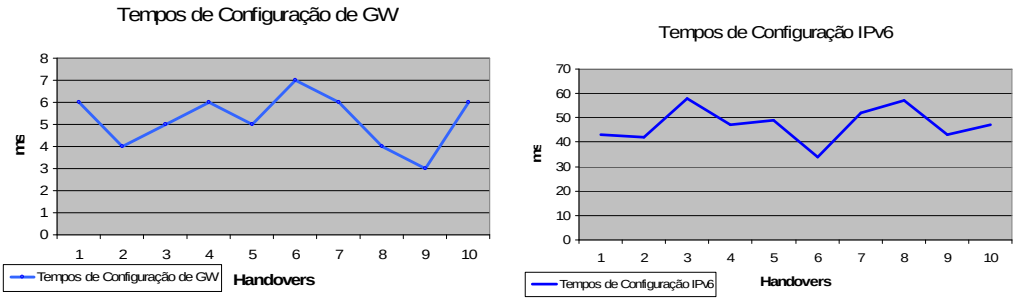
	Sinalização	Handover 802.11	Configuração GW	Configuração IPv6
Média	*20.9*	*63.5*	*5.2*	*47.2*
Desvio Padrão	*20.0*	*22.88*	*1.15*	*7.2*

Tabela 8 – Media e desvio padrão para os tempos de sinalização, handover IEEE 802.11 e configuração do default gateway durante o inter micro-domain handover (Resultados em milissegundos (ms))

Os gráficos (a), (b), (c) e (d) da Figura 84 ilustram a variação dos valores para o tempo de sinalização LMS, handover *IEEE802.11*, configuração do *Default GW*, e configuração do endereço *IPv6.*



(a) (b)



(c) (d)

Figura 84 – LMS, tempos de configuração e sinalização das entidades LMS

O *LMS* é um protocolo de mobilidade local e como tal não lhe cabe a responsabilidade de executar o mecanismo de mobilidade global. Assim, faz parte das competências do *LMS* gerir o momento de *handover* e preparar os recursos físicos no micro-domínio de destino, através de sinalização especifica *LMS.* O tempo de *blackout* é dado pela soma do tempo de *handover IEEE802.11*, tempo de configuração do *Default GW,* tempo de configuração do endereço *IPv6* e por fim o tempo de actualização do *Home Agent* e do nó correspondente dado pelo *Mobile IP*. Como pode ser observado pelos gráficos anteriores, o processo de *handover LMS* entre domínios é directamente dependente do tempo do sinalização do *Mobile IP*. O *LMS* sinaliza o *handover* entre micro-domínios de forma a garantir que o terminal móvel terá os recursos necessários para manter as suas ligações no micro-domínio de destino. Por conseguinte, quando o terminal móvel pretende iniciar um *handover* entre dois micro-domínios diferentes, ele envia uma mensagem de *Handover Request* para a rede. Esta mensagem é processada pelo *MMP* que irá verificar se é possível garantir os recursos de rede no micro-domínio de destino. Caso seja possível, os recursos são preparados e uma mensagem de retorno é enviado ao terminal. Como pode ser observado pelos gráficos anteriores, este tempo de sinalização é cerca de 21 (vinte e um) milissegundos. Após este passo, o terminal inicia o *handover IEEE 802.11* para o novo ponto de acesso, que demora cerca de 63.5 (sessenta e três ponto cinco) milissegundos a ser efectuado. Seguidamente o terminal configura o endereço *IPv6* e o *Default Gateway* que em soma demora 52.4 (cinquenta e dois ponto quatro) milissegundos a ser executado. Após estes procedimentos, o protocolo de mobilidade global inicia a notificação do *Home Agent* e do Terminal Correspondente. Após todas as tarefas anteriores serem correctamente executadas o terminal encontra-se de novo em comunicação com o terminal correspondente.

Capítulo V
Conclusões e Trabalho Futuro.

5.1 Conclusões

O futuro das telecomunicações passará obrigatoriamente pelo recurso à tecnologia IP para transportar os dados de um terminal para outro. A comunicação, tal como se conhece actualmente, efectua-se através de um mecanismo estruturado de encaminhamento de pacotes baseado numa hierarquia de endereçamento. Como tal, todos os terminais da rede têm necessariamente um endereço IP e servem-se dele para endereçar pacotes para a rede. O encaminhamento dos pacotes é efectuado com base na hierarquia de endereçamento topologicamente correcta dos diferentes terminais computacionais. Contudo, nas redes de próxima geração os terminais serão móveis e portanto o seu endereço IP mudará sempre que se moverem para uma nova rede. Assim, quando o terminal se move o seu endereço IP mudará para um novo topologicamente correcto com a rede de destino. Contudo, se o terminal estiver em comunicação com outros terminais na rede nesse momento, dado que o seu endereço mudou, todos lhe perderão o contacto e dessa forma as ligações activas passarão a inactivas nesse preciso instante. Este é o problema da mobilidade nas redes IP.

Como solução a esta problemática, várias soluções de mobilidade foram surgindo ao longos dos últimos anos, das quais se destaca com bastante particularidade o caso do *Mobile IP* [8]. Este protocolo permite que os terminais se movam livremente por diferentes redes IP sem nunca perder as ligações com os terminais correspondentes. Contudo, este mecanismo não é perfeito no que diz respeito ao uso eficiente dos recursos de rede assim como na rapidez de actualização de rotas. Portanto, quando um terminal se move entre dois pontos de acesso distintos, o tempo de *handover*, é normalmente grande quando se utiliza o *Mobile IP*, o que tem implicações graves no estado das ligações activas nesse momento.

Com vista a solucionar os novos problemas da mobilidade, e considerando as redes de próxima geração como principal alvo para estas tecnologias, nos últimos tempos surgiram novos protocolos de extensão a mobilidade. Com estes novos protocolos surgiram também novos conceitos de mobilidade, tais como a mobilidade hierárquica, micro-mobilidade e mobilidade local. Considerando que não existem soluções perfeitas, a busca interminável por um

protocolo mais adaptado à realidade dos operadores de telecomunicações das redes de próxima geração continua a ser um desafio constante para os investigadores da actualidade.

O *Local-centric Mobility System (LMS)* é um sistema de mobilidade local que vem dar resposta a alguns dos problemas encontrados nos outros protocolos de mobilidade já existentes. O *LMS* evita os longos tempos de *handover* bem como o uso ineficiente dos recursos de rede, tanto a rede nuclear como de acesso. Um terminal pode mover-se livremente por uma rede *LMS* de forma completamente transparente para o protocolo de mobilidade global, o que se traduz numa alta eficiência nos tempos de *handover*. O *LMS* introduz ainda alguns conceitos inovadores tais como o encaminhamento de dados comutados sobre multicast para ambientes que requerem alta eficiência tais como a rede dos micro-domínios de operador. O *LMS* é um sistema com detalhes interessantes que lhe proporcionam características únicas e que lhe permitem estar mais adaptado às necessidades típicas daquilo que se julga ser uma rede de operador de próxima geração. Destaca-se ainda a integração de servidos de contabilidade, facturação, controlo de acessos e autorizações *(AAAC)* directamente nos agentes de mobilidade *LMS*.

Esta tese de mestrado apresenta um novo conceito para um protocolo e arquitectura de mobilidade local desenvolvido e testado dentro do âmbito da mesma. Tanto o protocolo como a arquitectura proposta mostram-se ser bastante eficientes no que diz respeito à mobilidade rápida local, uso dos recursos de rede nuclear e de acesso, segurança, estabilidade, escalabilidade e integração com serviços de operador tais como *AAAC*. Dadas as suas qualidades, o *LMS* mostra-se ser um bom ponto de inicio para futuros protocolos que possam suportar as redes de próxima geração.

Conclui-se assim que o *LMS* propõe conceitos interessantes que podem ser reaproveitados para trabalhos futuros, mostrando mais uma vez que é possível obter melhores desempenhos servindo-se da mobilidade local. Nesta tese mostra-se ainda como é que é alguns conceitos das rede celulares podem trazer grandes vantagens para o panorama das redes de próxima geração IP.

5.2 Trabalho Futuro

Sendo o *Local-centric Mobility System* uma proposta ainda muito recente muitos dos seus aspectos poderão ainda ser melhorados e optimizados. Desta-se a possibilidade de desenvolver suporte para encaminhamento *multicast* com suporte de mobilidade de *multicast listeners* e *multicast sources.* Poderá ainda melhorar o mecanismo de integração dos Mobility Management Point (*MMP*) com mecanismos externos tais como servidores *A4C* ou *RADIUS*. Por fim, poderá ainda expandir-se as capacidades para suportar mecanismos integração de qualidade de serviço na rede dos micro-domínios. Estes deverão ser os pontos mais importantes a abranger num trabalho futuro.

Referências

[1] RFC2460, Internet Protocol, Version 6 (IPv6) Specification - S. Deering, Cisco, R. Hinden, Nokia, Dezembro de 1998.

[2] S. Ortiz Jr., Internet Telephony Jumps off the Wires – IEEE Comp. Vol 37 – Dezembro de 2004

[3] RFC721, Internet Protocol, - Protocol Specification - DARPA Internet Program

[4] RFC2462, IPv6 Stateless Address Autoconfiguration - S. Thomson, Bellcore, T. Narten, IBM, Dezembro de 1998

[5] RFC3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) - R. Droms, Ed., Cisco, J. Bound, Hewlett Packard, B. Volz, Ericsson, T. Lemon, Nominum, C. Perkins, Nokia Research Center, M. Carney, Sun Microsystems - Julho 2003

[6] RFC 2402, IP Authentication Header - S. Kent, BBN Corp, R. Atkinson, @Home Network - Novembro 1998

[7] RFC2406, IP Encapsulating Security Payload (ESP), S. Kent, BBN Corp, R. Atkinson, @Home Network - Novembro 1998

[8] Mobility Support in IPv6 - D. Johnson, C. Perkins, Work in Progress, <draft-ietf-mobileip-ipv6-12.txt> - Abril 2000

[9] Cellular IP - A. T. Campbell, J. Gomez, C-Y. Wan, S. Kim, Z. Turanyi, A. Valko, Work in Progress, <draft-ietf-mobileip-cellularip-00> - Janeiro de 2000

[10] Cellular IPv6 - Zach D. Shelby,VTT Electronics,Dionisios Gatzounas, Intracom,Andrew Campbell,Chieh-Yih Wan, Columbia University, < draft-shelby-seamoby-cellularipv6-00.txt> - Novembro 2000

[11] Cellular IP Desempenho - A. T. Campbell, J. Gomez, S. Kim, Z. Turanyi, A. Valko, C-Y Wan, Work in Progress, <draft-gomez- cellularip-desempenho-00> - Outubro 1999.

[12] Handoff-Aware Wireless Internet Infrastructure - IP micro-mobility support using HAWAII - R. Ramjee / T. La Porta, S. Thuel / K. Varadhan / L. Salgarelli, Lucent Bell Labs,< draft-ietf-mobileip-hawaii-01 > – Julho 2000

[13] Requirements and Gap Analysis for IP Local Mobility - J. Kempf, K. Leung, P. Roberts, K. Nishida, G. Giaretta, M. Liebsch < draft-ietf-netlmm-nohost-req-00 > - Fevereiro 2006

[14] RFC3344 - IP Mobility Support for IPv4 - C. Perkins, Ed., Nokia Research Center – Agosto 2002

[15] RFC4068 - Koodli, R., "Fast Handovers for Mobile IPv6", RFC 4068, Julho 2005

[16] IEEE 802.11 - Working Group, URL: http://www.ieee802.org/11/

[17] 3GPP (04) - Network architecture, 3GPP TS 23.002 V6.4.0, junho 2004.

[18] RFC 4068 - Fast Handover for Mobile IPv6, R. Koodli (ed), et al, IETF – Julho 2005.

[19] RFC4140 - Hierarchical mobile IPv6 mobility management (hmipv6), Hesham Soliman et al, IETF – Agosto de 2005

[20] Internet Draft Proxy Mobile IPv6 - S. Gundavelli, K. Leung, Cisco Systems, V. Devarapalli, Azaire Networks, K. Chowdhury, Starent Networks, B. Pati, Nokia - Março de 2007 - Data de Expiração: Setembro, 2007

[21] A novel Local-centric Mobility System (*LMS*) – Nuno Ferreira, Rui L. Aguiar, Susana Sargento – Janeiro de 2007

[22] RFC2748 - The COPS (Common Open Policy Service) Protocol - D. Durham, Ed., Intel, J. Boyle, Level 3, R. Cohen, Cisco, S. Herzog, IPHighway, R. Rajan, AT&T, A. Sastry, Cisco, Janeiro de 2000

[23] RFC1321 - The MD5 Message-Digest Algorithm - R. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc. – Abril de 1992

[24] IEEE802.11 – IEEE802.11 Workgroup – URL: http://www.ieee802.org/11/

[25] UMTSv7 - 3GPP Document. “25301.700 Radio interface protocol architecture version 7” – Abril de 2006.

[26] IEEE802.16 – IEEE802.16 Workgroup – URL: http://www.ieee802.org/16/

[27] IEEE802.3 – IEEE802.3 Workgroup – URL: http://www.ieee802.org/3/

[28] Linux – Linux Community -URL: http://www.linux.org/

[29] GNU - The GNU Operating System – URL: http://www.gnu.org/

[30] Gentoo Linux – URL: http://www.gentoo.org/

[31] Ubuntu – Debian Based GNU/Linux – URL: http://www.ubuntu.com/

[32] Linux Kernel – Linux Kernel – URL: http://www.kernel.org

[33] ANSI C – ANSI Organization - URL: http://www.ansi.org

[34] GCC – The GNU Compiler Collection - URL: http://gcc.gnu.org/

[35] Libpcap – The libpcap project-URL: http://sourceforge.net/projects/libpcap/

[36] LibSSL – The openssl project – URL: http://www.openssl.org/

[37] libSQLite – The SQLite project – UTL: http://www.sqlite.org/

[38] IPERF – A tool to measure the maximum TCP bandwidth between two points on the internet - URL: http://dast.nlanr.net/Projects/Iperf/

[39] RFC768 – UDP - User Datagram Protocol - J. Postel, ISI – Agosto de 1980

[40] RFC793 – TCP – Transmission Control Protocol – Darpa Internet Protocol – Setembro de 1981

[41] Scaling the Mobile Internet – Efficient and Scalable, End-to-End Mobility Support for Reative and Proactive Handoffs in IPv6 – IEEE Communications Magazine, vol 44 No 6 – Christian Vogt and Martina Zitterbart, Institute of Telematics, Universitat Karlsruhe (Germany) -Junho de 2006.

[42] GTK - Library to build graphical user interfaces (GUIs) originally for X Window – URL: www.GTK.org

[43] A performance comparison of Mobile IPv6,Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination – Volume 7, issue 4 - Xavier Pérez-Costa, Marc Toerrent-Moreno, Hannes Hartenstein – Outubro 2003

[44] A comparision of IP micro-mobility protocols. IEEE Wireless Communications, vol 9, pages 72-82, - A. Campbell, J. Gomez, S. Kim and C. Wan – Fevereiro 2002

[45] QoS-aware Mobility for Future Mobile Operators, IEEE Communications Magazine, vol 44 n.6 pp 92-102 – Rui L. Aguiar, et. al. - Junho 2006

[46] Fast Handovers for Hierarchical MIPv6 (F-HMIPv6), draft-jung-mobileip-fastho-hmipv6-01.txt, IETF – Jung H. et. al. - junho 2003

[47] A performance study of Fast Handover for Mobile IPv6 in proceedings of IEEE Local Computer Networks (LCN). – M. Torrent-Moreno, X. Pérez-Costa and S. Sallent-Ribes – Setembro 2003

[48] Handover Management for Mobile Nodes in IPv6 Networks, IEEE Wireless Communications Magazine – N. Montavont and T. Noel – Agosto 2002

[49] Analysis of a Local-area Wireless Netowork – ACM International Conference on Mobile Computing and Networking (MOBICOM) – D. Tang and M. Baker – 2000

[50] Comparision of IP Micro-Mobility protocols – IEEE Wireless Communications Magazine, vol. 9 - A. C. et. al. – Fevereiro 2002

Anexo Técnico

Detalhes sobre a aplicação desenvolvida

Screen Shots - Protótipo

Nesta secção apresentam-se algumas imagens relativas ao protótipo para GNU/Linux usadas para testar o *Local-centric Mobility System*. Os *daemons* que suportavam as funcionalidades de *Base Station, MAP e MMP* não têm nenhuma interacção com o utilizador apenas com o mecanismo de *log* do sistema. Por outro lado, o software que corre no terminal móvel poder ser controlado através de um mecanismo de *sockets*. Desta forma, é possível a um módulo externo ao *LMS*, controlar e obter estatísticas do estado do terminal e da rede em tempo real. Dado a abstracção que as *sockets* proporcionam, é possível controlar o terminal *LMS* através de um ambiente gráfico, por exemplo em *GTK* [42], ou através de um ambiente de consola de *Linux*.

Para este protótipo foi desenvolvida uma aplicação de controlo para ambiente de consola. Esta aplicação tem como principal objectivo ilustrar o estado actual da rede para o terminal em cada instante de tempo, ilustrar o estado interno do terminal e permitir que o utilizador possa escolher em que rede se ligar bem como iniciar *handovers*.

Figura 1 – Painel de controlo do terminal para ambiente de consola.

Como pode ser observado pela figura 1 o terminal tem um conhecimento geral do estado das redes *IEEE802.11* em seu redor. Para cada rede *IEEE802.11* o terminal tem ainda conhecimento em

qual delas existe uma *Base Stations LMS* associada. Através deste, o utilizador pode iniciar o processo de registo numa dada *Base Station* ou efectuar um *handover* para uma nova *Base Station*. Essas ordens são emitidas através do mecanismo de comunicação por *sockets* e a *daemon* do *LMS* no terminal recebe-as e executa.

A figura seguinte ilustra o processo do terminal a efectuar um *handover* dentro do mesmo domínio.

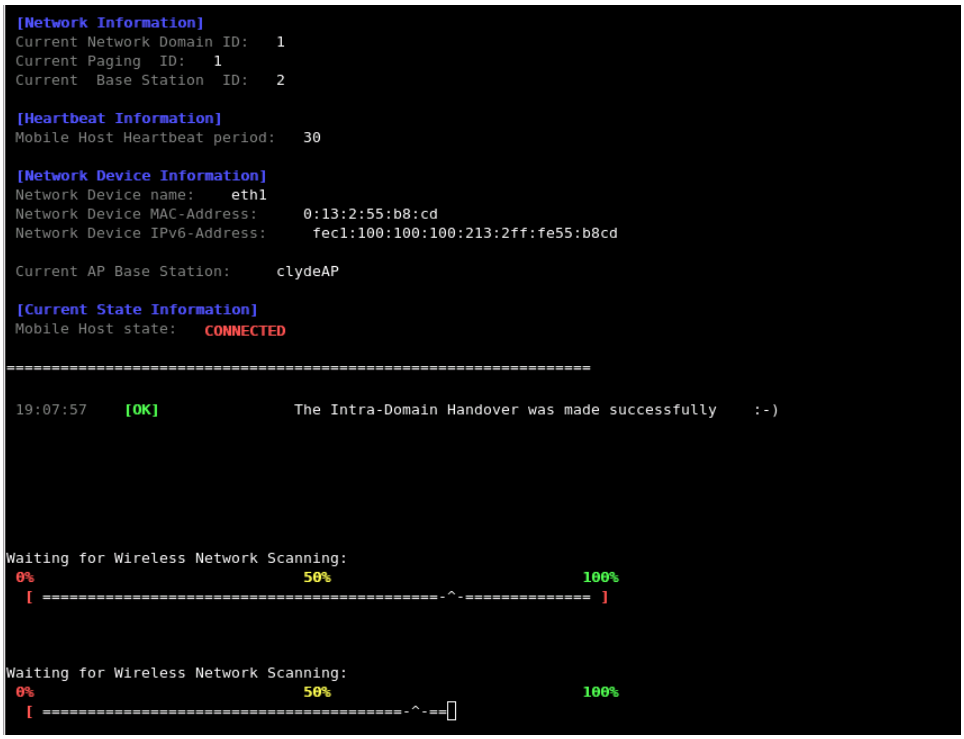


Figura 2 – Saída de texto da *daemon* de controlo LMS no terminal móvel

Na figura 2 pode-se observar o terminal a executar um Intra Micro Domain Handover. Após o handover ser efectuado, o terminal efectua pesquisas na rede (*scanning)* de forma a mapear todos os pontos de acesso à rede existentes nessa área . Com um período típico de 30 (trinta) segundos, o terminal envia para a rede uma mensagem de *Heartbeat* indicando a sua presença naquela *Base Stations.* Essas mensagens são sinalizadas na consola pelos caracteres "-^-" que indicam que o pacote de dados foi enviado com sucesso para a rede.

Após um registo numa nova rede ou um processo de *handover*, a *daemon LMS* imprime na consola a configuração actual do terminal para a nova rede. Neste caso, pode-se observar na figura que o terminal se encontra ligado na rede com o *ID=1*e na Base Station

número 2 (dois). Dado que o terminal não saiu do micro-domínio o seu endereço IPv6 não foi alterado durante o *handover* assim como o seu *PID (Personal IDentification),* apenas a *Base Station* mudou.

A figura seguinte ilustra a execução de um *Inter Micro-Domain Handover*.

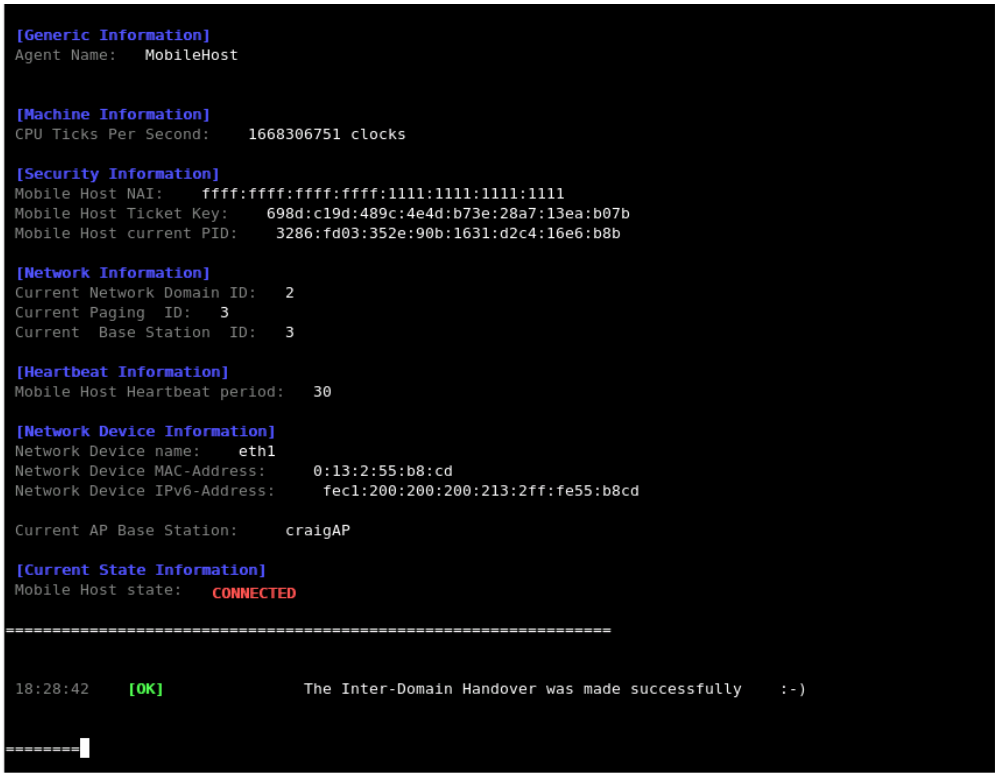


Figura 3 – Saída de texto da *deamon* de controlo LMS no terminal móvel

A figura 3 ilustra a execução de um *Inter Micro-Domain Handover*. Pode-se verificar que o terminal executou o *handover* com sucesso para a nova rede, pois o seu estado é ligado (“*connected”).* Pode ainda ser observado que o seu endereço IPv6 mudou, visto que o prefixo para a nova rede é diferente do antigo.

É ainda possível observar que o terminal antes estava associado ao ponto de acesso *ClydeAP* e agora está associado ao *CraigAP* e que mudou da *Base Station* número 2 (dois) para a número 3 (três).