Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão de Leiria

Engenharia Informática e Comunicações

IPv6@ESTG-Leiria

Testes de Mobilidade IPv6

Tiago Mira Amado

Leiria

Fevereiro de 2006

Projecto:

"IPv6@ESTG-Leiria – Testes de Mobilidade IPv6"

Âmbito:

Relatório final da disciplina de Projecto II, da Licenciatura em Engenharia Informática e Comunicações, ano lectivo 2005/2006, desenvolvido no âmbito do projecto *"IPv6@ESTG-Leiria"*. O projecto foi realizado entre Outubro de 2005 e Fevereiro de 2006 nas instalações do Departamento de Engenharia Informática (DEI) da ESTG de Leiria.

Instituição:

Instituto Politécnico de Leiria (IPL)

Escola Superior de Tecnologia e Gestão de Leiria (ESTG)

Curso:

Licenciatura em Engenharia Informática e Comunicações

Autor:

Tiago Mira Amado nº10449 - eic10449@student.estg.ipleiria.pt

Orientador:

Professor Mário Antunes - mario.antunes@estg.ipleiria.pt

Agradecimentos:

Fundação para a Computação Científica Nacional (FCCN), Centro de Informática (CI) da ESTG e equipa do projecto e-U do IPL.

Data:

O projecto foi realizado entre 3 de Outubro de 2005 e 24 de Fevereiro de 2006.

Leiria

Fevereiro de 2006

Agradecimentos

Em primeiro lugar os agradecimentos são endereçados à minha família pelo apoio que me deram não só durante este período difícil de desenvolvimento deste projecto, mas ao longo de todo o percurso que me permitiu chegar onde cheguei, e pelo apoio que sei que vou sempre continuar a receber deles.

Ao Professor Mário Antunes, o meu orientador, agradeço a exigência, rigor e competência colocados em cima da mesa de reuniões desde o início, os reparos, sugestões, comentários e melhoramentos que me foram sendo apresentados, as condições proporcionadas para a execução do projecto e, sobretudo, a liberdade que senti para desenvolver e criar.

Dirijo também agradecimentos a todos os meus amigos pelo apoio e ajuda que me deram neste período.

É com orgulho que digo que sou aluno da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, pelas excelentes condições que tem e proporciona aos seus alunos.

É ainda com mais orgulho que digo ser do curso de Engenharia Informática e Comunicações, pela qualidade do curso em si e também pela qualidade dos seus alunos, não só como profissionais mas também como pessoas.

Aos meus colegas do último ano do curso, Hugo Oliveira e Rui Bernardo, obrigado pelo apoio nesta fase final.

Aos professores das disciplinas do 5º ano obrigado pelo incentivo. Obrigado também ao Director de Curso, o Professor Luís Távora, pelo excelente trabalho que vem a fazer à frente da direcção do curso.

Ao David Serafim e Vítor Santos, antecessores no Projecto IPv6@ESTG-Leiria, agradeço a base de trabalho que deixaram e a ajuda que deram com o IPv6.

Ao Rui Silva, o “Linux Expert”, agradeço a ajuda com o Linux.

Aos membros do projecto e-U no IPL, Leandro Romano, Luís Frazão, Professor Vítor Távora, Rui Silva e Bruno Duarte agradeço a disponibilidade em fornecer informações sobre o e-U.

Ao Centro de Informática da ESTG, mais concretamente ao Engenheiro Carlos Canudo, obrigado pelos esclarecimentos sobre a rede da ESTG.

Queria agradecer à FCCN, nomeadamente ao Carlos Friaças e Mónica Rodrigues, pela ajuda nos testes que envolveram a FCCN.

Por último agradeço a todos aqueles com quem troquei emails para esclarecimento de dúvidas.

”The day will arrive, hastened by Mobile IP,

when no person will ever feel ’lost’ or out of touch.(…)”

”Mobile IP” de Charles E. Perkins

“Chegará o dia em que nenhuma pessoa poderá sentir-se “perdida” ou incontactável devido à chegada da Mobilidade IP.(…)”

Resumo

A RFC 3775 (“Mobility Support in IPv6”) especifica o protocolo Mobile IPv6 (MIPv6) que permite aos utilizadores mudarem a sua localização na Internet IPv6 mantendo-se contactáveis. É definido um novo cabeçalho de mobilidade, novas mensagens de mobilidade, novas mensagens ICMPv6, novas e actualizadas opções para fornecer suporte de funções e processos de mobilidade. São especificadas três entidades: o Mobile Node (MN), o Home Agent (HA) e o Correspondent Node (CN). É definido o processo de troca de mensagens entre estas três entidades, quando o MN se move da rede origem para outras redes, e quando regressa à sua rede origem.

Neste projecto foi realizado um estudo da mobilidade em IPv6, centrado no protocolo MIPv6, embora focando também outras tecnologias associadas à mobilidade, nomeadamente protocolos de micromobilidade, macromobilidade e de mobilidade de rede. Para efeitos de comparação e compreensão da evolução foi também abordado o comportamento destas tecnologias em IPv4.

Apresentam-se os últimos avanços realizados neste domínio pelo grupo “mip6” do IETF. Descreve-se ainda o estado actual das implementações nos mais importantes sistemas operativos (Windows, IOS, Linux, xBSD).

Com base nos estudos e pesquisas foram configurados diversos cenários de teste usando diferentes sistemas operativos e topologias. Inicialmente usou-se uma infra-estrutura *wired* que permitiu configurar e testar as implementações. Posteriormente usou-se um cenário heterogéneo que inclui uma infra-estrutura *wireless* de modo a avaliar o desempenho do MIPv6 ao nível do *handover*. Sobre os cenários construídos no âmbito deste projecto são apresentadas as configurações, os resultados obtidos e as principais conclusões.

A ESTG possui uma rede piloto IPv6 com ligação à Internet por intermédio da FCCN (Fundação para a Computação Científica Nacional), o actual ISP. Por outro lado, a FCCN disponibiliza duas plataformas (em Lisboa e no Porto) com conectividade ao *Backbone* da rede, permitindo assim realizar testes entre Sistemas Autónomos (SAs) distintos, testando o funcionamento e o desempenho do protocolo MIPv6 entre redes distintas na Internet.

Aproveitando o facto do Instituto Politécnico de Leiria pertencer à rede e-U, e atendendo ao trabalho desenvolvido pela ESTG no âmbito do projecto “IPv6@ESTG”, apresenta-se uma possível solução para permitir o uso de Mobilidade IPv6 na rede e-U.

Palavras-chave:

- ✓ IPv6@ESTG-Leiria
- ✓ IPv6
- ✓ MIPv6, MIPv4, MIP
- ✓ Mobilidade, *Mobility*, *Mobile*
- ✓ e-U, FCCN
- ✓ *Wireless*, WLAN, “redes sem fios”, Wi-Fi
- ✓ *Roaming*
- ✓ *Handover*, *Handoff*
- ✓ microMobilidade, MacroMobilidade

Lista de abreviaturas e siglas

ANACOM – Autoridade Nacional de Comunicações

AP – Access Point

CIDR - Classless Inter-Domain Routing

DA – Destination address

DAD - Duplicate Address Detection

DHCP - Dynamic Host Configuration Protocol

DHCPv4 – Dynamic Host Configuration Protocol for IPv4

DHCPv6 - Dynamic Host Configuration Protocol for IPv6

DiffServ - Differentiated Services

DNS - Domain Name System

DoS - Denial of Service

ESTGL – Escola Superior de Tecnologia e Gestão de Leiria

ETSI - European Telecommunications Standards Institute

e-U – Universidade Electrónica

FCCN - Fundação para a Computação Científica Nacional

GPRS - General Packet Radio Service

GSM - Global System for Mobile Communications

HA – Home Agent

HoA – Home Address

IANA - Internet Assigned Numbers Authority

ICMP - Internet Control Message Protocol

IEEE - Institute of Electrical and Electronics Engineers

IETF - Internet Engineering Task Force

IP – Internet Protocol

IPL – Instituto Politécnico de Leiria

IPSec - Internet Protocol Security

IPv4 – Versão 4 do IP

IPv6 – Versão 6 do IP

IPv6@ESTG-Leiria – Projecto da ESTGL que visa promover a implementação do IPv6

ISP - Internet Service Provider

ITU - International Telecommunication Union

ITU-R - ITU – Radiocommunication Standardization Sector

ITU-T - ITU – Telecommunication Standardization Sector

LAN - Local Area Network

MAC - Medium Access Control

MAN - Metropolitan Area Network

MN - Mobile Node

MIP – Mobile Internet Protocolo (Mobilidade IP)

MIPv4 – Versão MIP para a versão 4 do IP, ou seja, MIP para IPv4

MIPv6 - Versão MIP para a versão 6 do IP, ou seja, MIP para IPv6

MTU - Maximum Transmission Unit

NAT - Network Address Translator

OSI - Open System Interconnection

RF - Radio Frequency

SA - Source Address

WLAN - Wireless Local Area Network

Índice

Lista de Figuras

Lista de Tabelas

1. Introdução

O transporte dos dados na Internet é assegurado pelo protocolo IP (versão 4). Embora a sua utilização se tenha inicialmente revelado adequada, tornou-se necessário implementar medidas de ajuste à evolução da Internet e ao seu crescimento exponencial. Por exemplo, o NAT, o VLSM e o sub-endereçamento surgiram para minimizar o desperdício de endereços. Também o CIDR se revelou indispensável no encurtamento das tabelas de encaminhamento e consequente melhoria de processamento pelos *routers*. O aparecimento de novos paradigmas de comunicação assentes na mobilidade efectiva mostrou também inadequação do protocolo IPv4 e necessidade de mudança.

O objectivo da versão 6 do protocolo IP (IPv6), desenvolvido pelo IETF, consiste em resolver algumas inadaptações do IPv4 face ao cenário actual da Internet. Destacam-se como pontos fortes a estrutura e dimensão do espaço de endereçamento, a auto-configuração dos terminais, a simplificação do processamento nos *routers* e os cuidados relacionados com a segurança, QoS e a mobilidade. O IPv6 encontra-se actualmente numa fase madura de desenvolvimento, como o comprovam as implementações estáveis na maioria das plataformas de sistemas operativos. Também os principais serviços da Internet se encontram implementados em ambas as versões.[43]

É fornecida alguma mobilidade pelos protocolos das camadas Física e de Ligação de dados. Por exemplo, o IEEE 802.11 (Ethernet sem fios). Contudo, a mobilidade, neste caso, existe apenas no âmbito local (*Wireless LAN*), sendo impossível que um terminal móvel se desloque entre redes diferentes, conservando, portanto, a sua configuração de rede inalterada durante a movimentação.

A atribuição dinâmica de endereços por DHCP também poderá ser vista como um mecanismo de mobilidade, uma vez que permite a mudança de redes. No entanto, inerente a esta mudança está sempre uma quebra de ligação.

A mobilidade IP (MIP), por outro lado, possibilita que um terminal móvel se desloque entre diferentes redes sem que as ligações ou sessões em curso sejam interrompidas, e permitindo que outras novas sejam estabelecidas. A mobilidade IP evita que as ligações, cuja parametrização contém o endereço IP do terminal móvel local, sejam quebradas no evento de uma movimentação, de uma forma transparente para as camadas superiores.

A mobilidade IP constitui a melhor forma de interligar redes de diferentes tecnologias. Por exemplo, redes *wireless* (IEEE 802.11, GPRS, *HiperLan*, etc) e as tradicionais redes com fios.

A Mobilidade IPv6 (MIPv6) consiste em adições realizadas ao protocolo IPv6 para se conseguir o "*always-on*", independentemente da movimentação e localização. Além de todos os benefícios

inerentes à comunicação sobre IPv6 (nomeadamente melhor desempenho, QoS e segurança), dos benefícios da mobilidade (tais como conforto, flexibilidade, transparência, mobilidade global), o MIPv6 possui várias diferenças sobre o seu antecessor o MIPv4, como sejam, optimização de rotas, segurança, independência e transparência para as redes visitadas, entre muitas outras melhorias.

A adopção do MIPv6 está dependente da transição do protocolo IP. Os custos inerentes a esta mudança irão depender de vários factores. Será necessário novo software, hardware, formação dos responsáveis pela rede de informação, tempo para mudança de equipamentos e serviços, com as respectivas configurações. A transição poderá ainda afectar outros sectores que dependem do sistema informático.

O tempo de adaptação ao novo protocolo por parte dos gestores das redes poderá ser visto como uma dificuldade a superar. Porém, é sabido que este protocolo tem mais facilidades de gestão que o seu antecessor, existindo serviços e novos métodos de gestão que terão de ser aprendidos.

Em relação à mobilidade que por vezes é associada a um decréscimo de segurança das redes, tal não se verifica com o MIPv6, em que a rede mantêm o mesmo nível da segurança.

O MIPv6 foi concebido para garantir mobilidade ao IPv6, tirando partido de todas as vantagens deste novo protocolo, tendo como base o seu antecessor o MIPv4, procurando corrigir ou optimizar as falhas e limitações deste.

1.1 Aplicações e Enquadramento

Imagine-se um mundo móvel, com uma lista extensa de dispositivos móveis ou não, mas todos a necessitar de um endereço unívoco, desde computadores portáteis, PDAs, telemóveis, electrodomésticos, automóveis, sensores inteligentes, dispositivos bio-electrónicos, robôs, ou até alguns dispositivos que ainda nem sequer existem. Com o número limite de endereços associado ao protocolo actual a aproximar-se do fim, dia após dia, a necessidade de um novo protocolo emerge.

Esta utopia de interligação de múltiplos dispositivos numa rede global vai um dia deixar de o ser, tornando-se um hábito dos nossos dias. Um novo paradigma de computação está cada vez mais a emergir, o conceito de computação ubíqua (*ubiquitous computing*). Este conceito é inverso ao da realidade virtual. Nesta são os humanos que entram no mundo computacional, mas no caso da computação ubíqua é o computador que entra no nosso mundo, adquire os nossos hábitos, faz parte da nossa vida mais rotineira [43].

Não será difícil imaginar um futuro em que cada pessoa possui dezenas, centenas por vezes milhares de dispositivos a necessitarem de ligação permanente à Internet independentemente da sua localização.

O IPv6 com o seu vasto espaço de endereçamento, características como a auto-configuração dos terminais e a simplificação do processamento nos routers, e ainda o suporte nativo para segurança, QoS e mobilidade, assumirá um papel preponderante nessa evolução.

1.2 Motivações

O futuro é cada vez mais digital e completamente dependente das comunicações, onde as comunicações sem fios assumirão um papel indispensável, permitindo a qualquer pessoa satisfazer as suas necessidades de comunicação e aceder a conteúdos em qualquer altura e em qualquer lugar onde quer que se encontre com o máximo conforto, o mínimo de esforço, de forma confiável e robusta e com total segurança. Para cumprir este objectivo, os esforços deverão convergir no sentido de garantir compatibilidade entre diferentes tecnologias. O IPv6 surgiu com o intuito de permitir no futuro todas as tecnologias e dispositivos serem IP, tendo o MIPv6 sido criado com o intuito de ser uma solução de mobilidade escalável a nível mundial.

As comunidades académicas são reconhecidas pelos contributos que dão nos processos de evolução para as novas tecnologias, encontrando-se muitas das vezes ligadas ao desenvolvimento destas, estando na linha da frente da implementação, seguindo-se a mobilização das restantes entidades, como sejam as entidades governamentais, empresas, operadores de telecomunicações, sistema de ensino, utilizadores individuais e os demais utilizadores da Internet.

O IPv6 já não é uma incógnita, mas sim uma certeza e uma realidade. O MIPv6 assumirá um papel preponderante nessa realidade.

1.3 Objectivos

O tema central do projecto é a Mobilidade IPv6. Os principais objectivos definidos inicialmente englobam o enquadramento do tema, o estudo dos conceitos associados à mobilidade em redes IPv4 e apresentadas as diferenças relativamente ao IPv6. O estudo realizado foi suportado na configuração de cenários em ambientes móveis.

O plano de trabalho inicialmente proposto englobou as seguintes fases:

- estudar o conceito de mobilidade em IPv4 e IPv6;
- apresentar o estado da arte neste domínio, nomeadamente os últimos avanços realizados pelo IETF, através do seu grupo “mip6”
- identificar as principais acções a tomar na implementação do IPv6 numa rede móvel, nomeadamente ao nível dos clientes e serviços (DNS, HTTP, Proxy)

- configurar um ambiente de testes heterogéneo, incluindo obrigatoriamente uma infraestrutura *wireless*
- efectuar testes conclusivos sobre a configuração e o uso da tecnologia IPv6 em ambientes móveis
- apresentar um relatório técnico sobre o estado da arte, o trabalho desenvolvido e as conclusões aos resultados obtidos

A segurança em mobilidade, apesar da sua extrema importância, não faz parte dos objectivos e âmbito deste projecto. No entanto, ao longo do texto efectua-se o enquadramento necessário nalguns capítulos, sem o aprofundamento devido.

Um outro objectivo que se tomou em consideração e que inicialmente não estava previsto, foi o de apresentar uma solução para a configuração da mobilidade na rede e-U, usando exclusivamente o protocolo IPv6. Ou seja, configurar o MIPv6 na rede e-U.

Além do relatório de projectos, foram ainda realizados os seguintes contributos: guião sobre o uso da Moblidade IPv6 em Linux e a submissão de um artigo à Conferência Ibérica de Sistemas e Tecnologias de Informação (CISTI) [108], actualmente em revisão.

1.4 Estrutura do relatório

Além deste capítulo introdutório, no qual é apresentado um enquadramento contextual, o relatório tem a seguinte estrutura:

2. IPv6

   Será abordado o IPv6 e algumas das suas características principais. Pretende-se apenas realizar um breve enquadramento, partindo-se do pressuposto que o leitor possui alguns conhecimentos em IPv6.

3. Mobilidade

   Serão apresentadas as definições e características de mobilidade, e será explicada a necessidade da Mobilidade IP, o seu funcionamento básico e outros protocolos associados.

4. MIPv6 - Mobilidade IPv6

   Este capítulo foca a Mobilidade em IPv6, o seu funcionamento e características, e os protocolos associados.

5. Normalização e implementações MIPv6

   É apresentado um apanhado geral do estado actual da arte, nomeadamente os últimos avanços realizados pelo grupo “mip6” na normalização da mobilidade, quais as implementações

práticas do protocolo e qual o seu estado de desenvolvimento nos principais sistemas operativos.

6. Arquitectura de testes

   Este capitulo descreve os equipamentos e software usados, assim como os cenários de testes configurados (Testbeds) justificando as arquitecturas configuradas, os objectivos e a necessidade da sua utilização.

7. Testes e resultados

   Com base nos cenários descritos no capítulo anterior, descrevem-se os resultados obtidos e as conclusões mais importantes.

8. Testes com a rede da FCCN

   De modo a estudar o desempenho do MIPv6 entre diferentes sistemas autónomos recorreu-se à plataforma de testes IPv6 disponibilizada pela FCCN. Uma vez que já existe uma ligação em IPv6 nativa entre a ESTG e a FCCN, apresentam-se as principais ações a desenvolver no sentido de testar a mobilidade entre domínios separados fisicamente por uma distância considerável.

9. Implementação de MIPv6 no e-U.

   O projecto e-U (universidade electrónica), lançado pelo governo Português é pioneiro a nível mundial. Consiste em criar uma rede *WiFi* integrada nas instituições de ensino superior nacionais. Tornou-se num *Case Study* para os países ditos mais evoluídos e para as principais empresas mundiais como a cisco, Microsoft ou a Intel (ver anexo B). Este capítulo pretende mostrar como se poderia enquadrar o MIPv6 nesta rede apresentando-se um estudo dos requisitos necessários.

10. Trabalho futuro

    Neste capítulo são apresentadas algumas propostas de trabalho futuro no âmbito da Mobilidade IPv6.

11. Conclusões

    O relatório termina com as conclusões ao trabalho realizado, referências bibliográficas e anexos.

2. IPv6

O IPv6 [10] é a "próxima geração" do protocolo IP, desenhado pelo IETF para substituir o actual IPv4.

Trata-se de um novo protocolo da camada de rede que abrange diversos aspectos relacionados com diferentes ramos das tecnologias de rede. Além do endereçamento, que é directamente afectado, encaminhamento, qualidade de serviço, mobilidade, segurança e mesmo serviços e protocolos, são alguns dos temas que vêem alguns dos seus conceitos modificados. Sendo assim, além de um novo protocolo da camada de rede, irá existir uma reacção em cadeia para todo um conjunto de outros protocolos, aplicações, sistemas operativos, sistemas e serviços. A reacção terá sempre como objectivo a melhoria da tecnologia. Outro objectivo não menos importante é garantir facilidades a todo um processo de administração de redes, assegurando também o melhor desempenho da rede em questão.

O nascimento do IPv6 deve-se a motivos que constituem factos inegáveis, protagonizados principalmente pelo crescimento da Internet e inclusão da mesma em diversos meios, de modo a facilitar qualquer forma de acesso à mesma.[43]

2.1 Características

O protocolo IPv6 tem muitos outros benefícios além da maior quantidade de endereços proporcionados devido ao seu tamanho de 128 bits. Um dos benefícios é a simplificação da Internet, que poderá deixar de ser uma InterNAT[1], ou seja, uma Internet repleta de tradutores (NAT - *Network Address Translation*) de endereços privados para endereços globais. A solução do NAT é muito utilizada e útil actualmente, porém traz inúmeros problemas, por exemplo, a incompatibilidade com aplicações ponto-a-ponto.

Ao longo do tempo foram sendo criadas sucessivas "adendas ao IPV4". Foram vários os protocolos e implementações criadas para IPv4, que funcionando como complemento ou em conjunto com este protocolo, permitiram corrigir ou "remendar" alguns dos seus problemas, que foram surgindo com o crescimento das redes (NAT, CIDR, VLSM, sub-endereçamento). Estes permitiram que o IPv4 se mantivesse "vivo", e conseguisse aguentar-se até hoje e por mais algum tempo como o principal protocolo da Internet. No entanto todas essas soluções são consideradas soluções de curto prazo.

[1] InterNAT – Termo usado por diversos autores referindo-se ironicamente ao uso de NAT encadeado (em cascata).

O IPv6 foi criado para substituir o IPv4, corrigindo as falhas e limitações deste, com o objectivo de ser, não uma, mas, a solução de longo prazo.

Alguns dos benefícios associadas ao IPv6 sobre o seu antecessor podem definir-se sucintamente como:

- maior capacidade de endereços.

  O limite teórico de endereços IPv4 é de 4 mil milhões (4.294.967.296 – 2^{32}), mas na prática apenas cerca de 250 milhões podem ser alocados por utilizadores.

  $3{,}4 \times 10^{38}$ (340.282.366.920.938.463.463.374.607.431.768.211.456 – 2^{128}) é o número teórico de endereços associado ao IPv6. $6{,}7 \times 10^{23}$ (665.570.793.348.666.943.898.599) é aproximadamente o número de endereços possíveis de atribuir por metro quadrado do Planeta Terra.

- auto-configurável (permite o Plug and Play).

  Existem duas formas de autoconfiguração *stateless* e *statefull*. A primeira é através dos prefixos anunciados pelo *Router* do *link*, e a segunda através do servidor de DHCPv6.

- mais preocupações de segurança na sua concepção, logo mais seguro (inclusão do IPsec).

  Os mecanismos de NAT desaparecem, e cada máquina possui um endereço unívoco, logo as comunicações serão ponto-a-ponto, permitindo o uso de IPSec.

- concebido a pensar no QoS, logo melhor suporte de QoS (distinção de fluxos).

  Aumento do campo *Traffic class* e criação do campo *Flow label* no cabeçalho IPv6.

- pensado de raiz em função da mobilidade, logo melhor performance na mobilidade.

  A forma como foi pensado o mecanismo de extensões IPv6 permite o uso de mobilidade numa rede de forma transparente e independente de todas as outras.

- privilegia o modelo ponto-a-ponto (condenando o NAT à extinção).

  Cada máquina possui um endereço unívoco, com o qual comunica directamente com outras.

- globalmente mais eficiente (corrige os erros e limitações do IPv4, optimizando-o). Exemplos:
  - Simplificação do formato do cabeçalho (apesar do aumento de 20 para 40 bytes, ou seja, para o dobro do tamanho do cabeçalho IPv4 sem opções), tamanho fixo, possibilidade de utilizar cabeçalhos opcionais encandeados,
  - Sem operações de *checksum* na camada de rede,
  - Optimização do processo de fragmentação de pacotes, usa o *path MTU discovery* em vez da segmentação *hop-by-hop*,
  - Não há *broadcasts* (uso do *multicast* e *anycast*)

Em toda esta lista, está sempre presente no horizonte do IPv6, a facilidade e simplicidade de qualquer tipo de configuração necessária. Assim sendo, tanto gestores como utilizadores vulgares, têm as suas tarefas facilitadas.

2.2 A transição

Devido à já vasta implementação do IPv4 nas redes mundiais e ao seu enraizamento, torna-se impossível migrar para ipv6 da mesma forma que sucedeu a 1 de Janeiro de 1983, quando o IPv4 se tornou no principal protocolo da Internet. Assim sendo, apesar de todas as vantagens, esta transição prevê-se lenta e faseada. A figura seguinte mostra o mapa da topologia do *Backbone* da Internet (só IPv4) em Abril de 2005, concebido a partir de duas semanas de análise do tráfego IPv4.

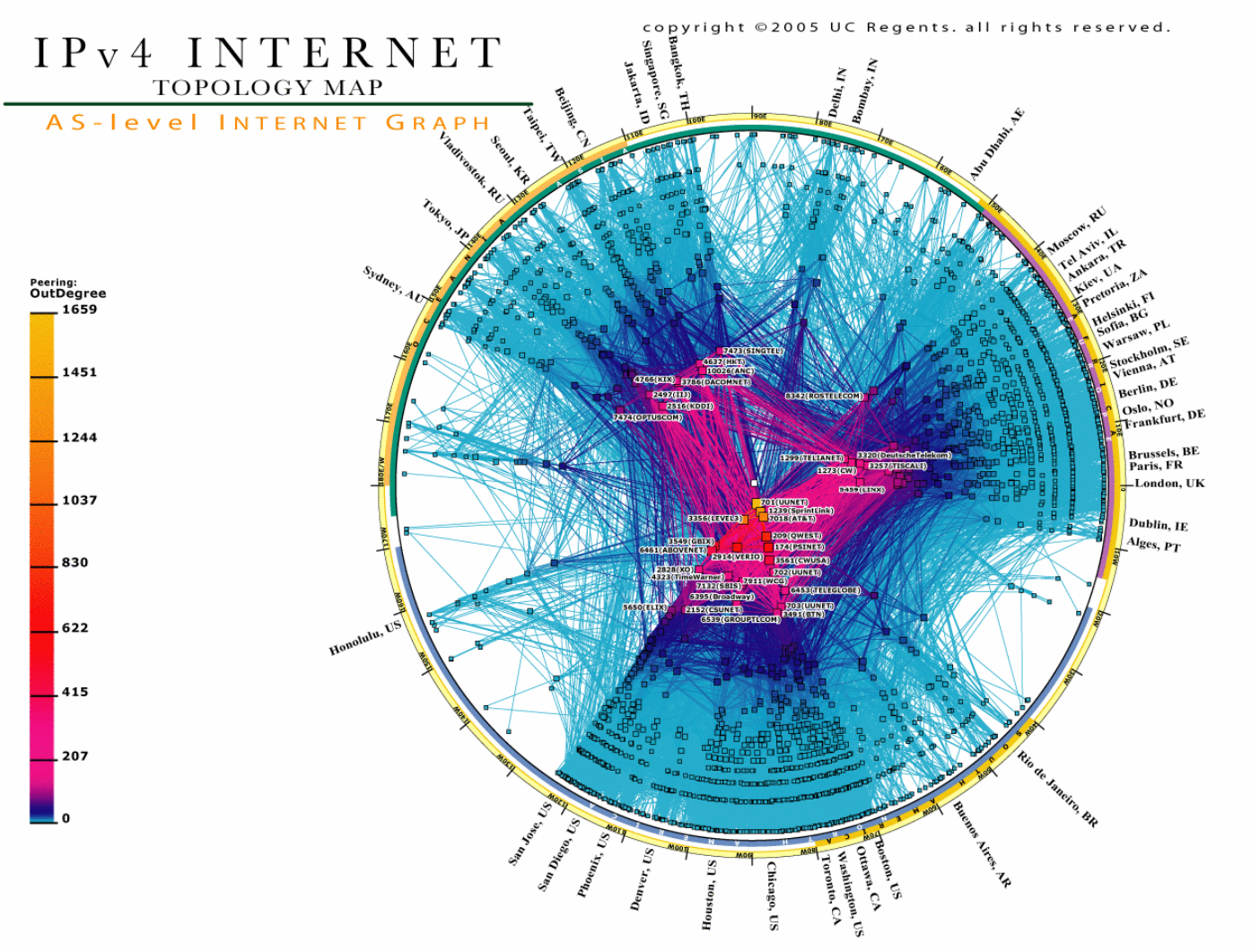


figura 1 - Mapa da topologia da Internet IPv4 (retirado em: http://www.caida.org).

A figura 2 apresenta a mesma representação da topologia mas para o *Backbone* da Internet em IPv6, e a figura 3 apresenta uma comparação relativa de ambas. Pretende-se mostrar o maior desenvolvimento do IPv4, mas um já considerável *Backbone* IPv6.

As maiores dificuldades da adopção do IPv6 prendem-se precisamente com a fase de transição do protocolo. Os custos e o tempo inerentes a esta mudança irão depender de vários factores. Será necessário novo software, hardware, formação dos responsáveis pela rede de informação, tempo para mudança de equipamentos e respectivas configurações, e além disto esta transição poderá ainda afectar outros sectores que depedem do sistema informático. O tempo de adaptação ao novo protocolo por parte dos gestores das redes poderá ser visto como uma dificuldade, porém o IPv6 tem mais facilidades de gestão que o seu antecessor. Relativamente à Internet, enquanto todas as instituições não migrarem, ou adoptarem mecanismos de transição, poderão existir limitações de acesso à informação. A figura 2mostra o mapa da topologia do *Backbone* IPv6 da Internet IPv6 em Março de 2005. A escala de cores mostra o número de ligações entre os servidores, mas note-se que a gama de valores é diferente da apresentada na figura 1.

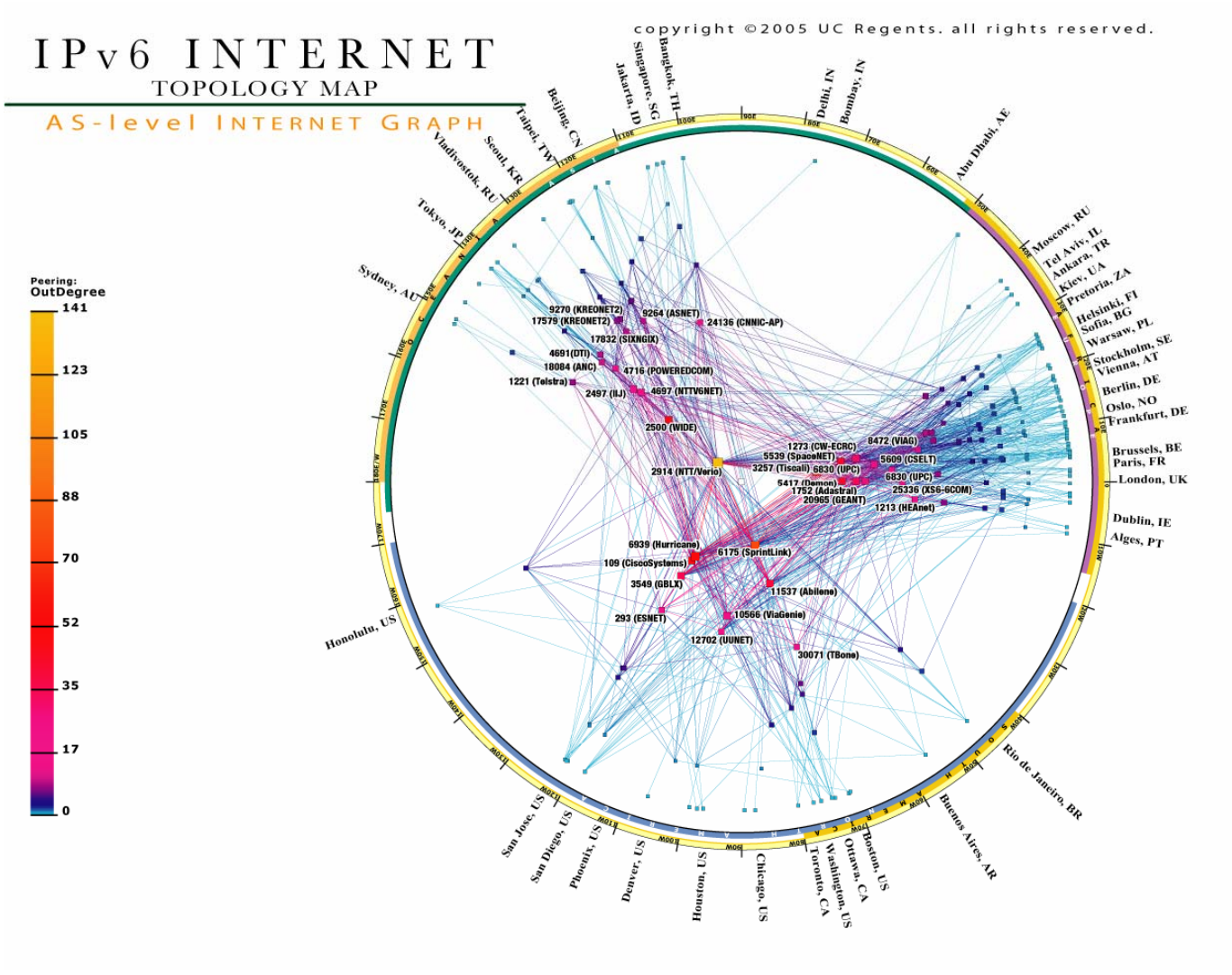


figura 2 - Mapa da topologia da Internet IPv6 (retirado em: http://www.caida.org).

Analisando os mapas das topologias IPv4 realizados anteriormente, pode-se verificar que a actual topologia IPv6, não difere muito da topologia IPv4 existente em Janeiro de 2000. Segundo esta

análise, caso o IPv6 venha a ter um crescimento semelhante ao do IPv4 nos últimos 5 anos, então daqui a 5 anos existirá um *Backbone* IPv6 igual ao actual IPv4.

Sendo a transição a maior dificuldade na adopção deste protocolo, têm sido concebidos inúmeros mecanismos de transição para permitir primeiramente, que a mudança seja possível, e permitir atenuar as consequências negativas inerentes ao período do processo de transição.

Alguns métodos de transição para IPv6 são:

- DNS – através da introdução de um novo Resource Record (AAAA);
- Pilha dupla (*Dual-Stack*) – permite aos terminais terem configurado em simultâneo duas stacks IP;
- Túneis: IPv6 sobre IPv4 – o tráfego IPv6 é encapsulado em pacotes IPv4.

O actual tráfego IPV6 existente não compensa às operadoras os investimentos para implementar IPv6 no core, e está longe de ser um investimento viável e rentável. Por isso todos os esforços se concentram em soluções que permitam a convivência dos dois protocolos mantendo as infra-estruturas existentes. Numa fase mais avançada as soluções a ser criadas serão para permitir a convivência de ambos os protocolos, mas permitindo usar o IPv4 sobre as novas infra-estruturas criadas para o IPv6.

A figura seguinte permite fazer uma análise comparativa da topologia (não do tráfego) da Internet IPv6 e IPv4. As escalas são as apresentadas na figura 1 e figura 2.

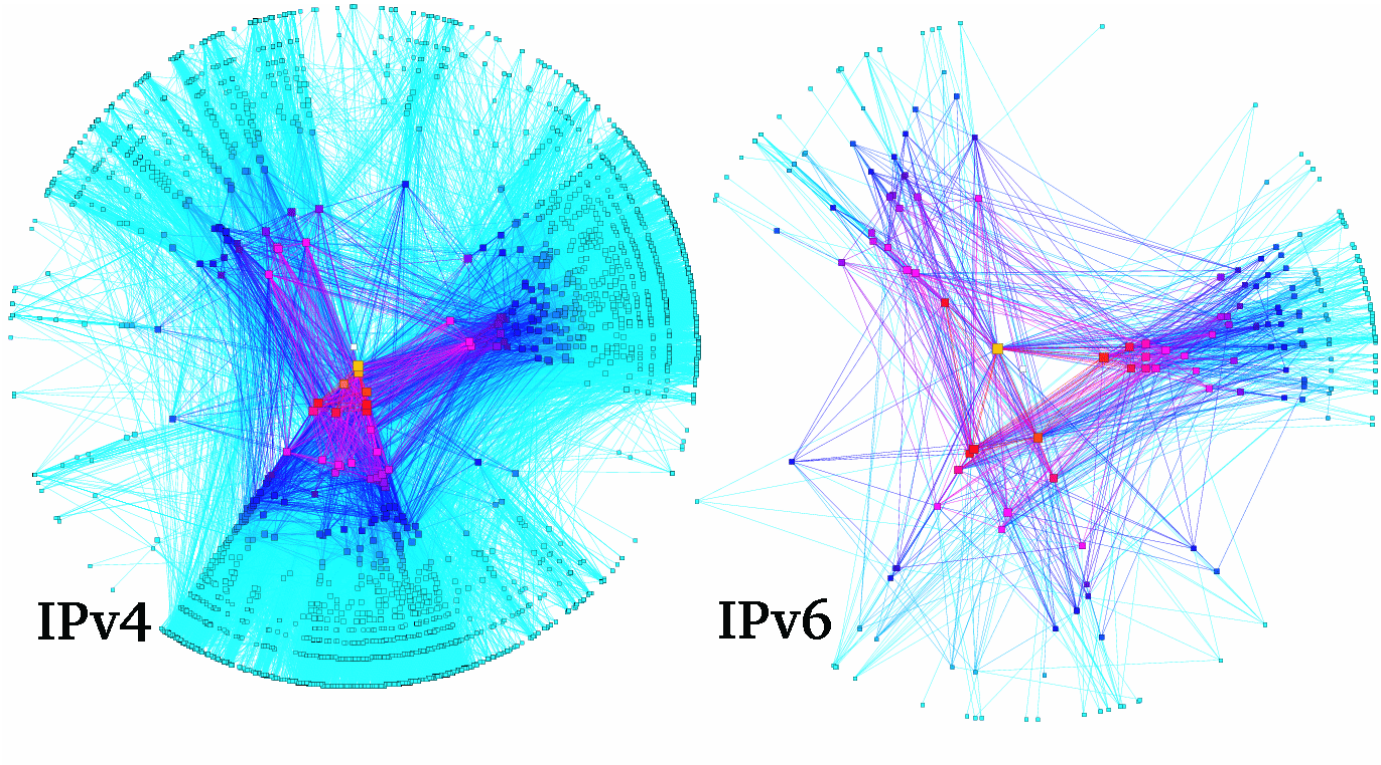


figura 3 - Comparação da topologia do *Backbone* IPv4 e IPv6 (retirado em: http://www.caida.org/).

Irónico porém, é que a transição do IPv6, o protocolo que veio para substituir o IPv4 e todos os seus "remendos" (soluções de curto prazo), tenha de ser implementada à custa de mais "remendos".

Gradualmente o IPv4 e os protocolos a ele associados, bem como todos os mecanismos de transição criados, irão começar a desaparecer, tornando-se a Internet numa rede IPv6 bem mais simples, segura e completa do que é hoje.

2.3 Contributos

O desenvolvimento do IPv6, tal como qualquer outra tecnologia que se pretende afirmar, teve vários pontos essenciais, uns mais do que os outros, mas todos eles devem ser lembrados. Fala-se tanto no futuro do IPv6, que por vezes até se esquece o seu passado de igual importância. As especificações do IPv6 do IETF, nomeadamente as RFCs 1883 [8] e 2460 [10], são o maior passo na normalização do IPv6. O projecto 6Bone é o maior passo na igualmente importante parte prática deste novo protocolo. Depois disso seguem-se inúmeros projectos que conjugam de certa forma, a parte teórica, prática e principalmente a convergência dos esforços entre os diversos países.

Diversas entidades deram, e continuam a dar o seu contributo. De seguida são enumeradas algumas das mais importantes:

- IETF [54]
- 6Bone [55]
- IPv6 Forum [49]
- 6Net [57]
- Euro6IX [58]
- DoD (Departamento de Defesa dos Estados Unidos [60]
- "*Tasks Force*" de vários países

Em Portugal, a Task Force IPv6 [46] está sob a gestão da FCCN [45] e tem como objectivos a promoção, o desenvolvimento e a evolução do IPv6.

Também por todo o mundo, as comunidades académicas dão um importante contributo rumo à mudança.

2.4 Projecto IPv6@ESTG-Leiria

As comunidades académicas dão um importante e valioso contributo para a evolução das novas tecnologias, apresentando estudos, sugestões, testes e resultados. Na ESTGL, em 2005 o projecto IPv6@ESTG-Leiria [44], cujo objectivo constitui em construir uma rede piloto IPv6 com acesso

nativo ao exterior (através da FCCN) e incentivar o estudo e utilização do protocolo IPv6 e de outros protocolos e aplicações relacionados.

O primeiro projecto realizado, "IPv6@ESTG-Leiria - Instalação de uma rede piloto", consistiu, tal como o nome sugere, na instalação com configuração e testes de uma rede piloto IPv6 heterogénea com diversos servidores indispensáveis (DHCPv6, DNS, HTTP), e no estabelecimento de uma ligação em IPv6 nativa à FCCN, o actual ISP da ESTG.

A figura 4 mostra a ligação IPv6 entre a ESTGL e o seu ISP, a FCCN.

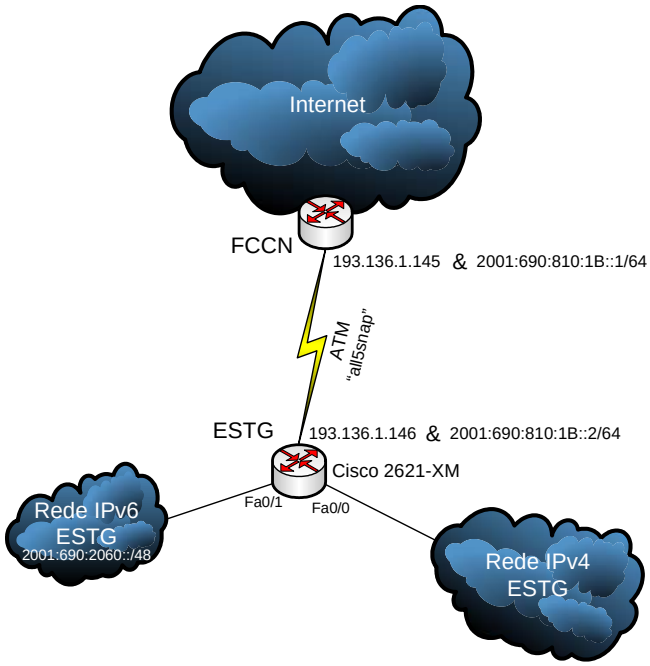


figura 4 - Cenário da ligação da ESTG à Internet, com IPv4 e IPv6 (retirado de [43]).

A figura 5 representa um esquema da topologia de rede configurada na rede piloto IPv6.

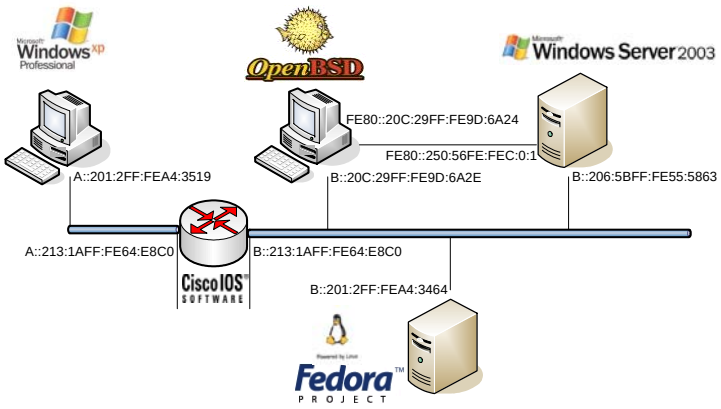


figura 5 - Representação da rede heterogénea configurada (retirado de [43]).

A figura 5 representa a rede heterogénea configurada, onde é possível verificar a existência de máquinas com diversos sistemas operativos onde foram configurados diversos serviços.

Após a instalação da rede piloto IPv6 no âmbito do projecto referido em [43], foi possível executar um conjunto de outros projectos. Actualmente o projecto IPv6@ESTG-Leiria[2] conta com mais quatro projectos a decorrer em simultâneo, destacando-se os seguintes:

- Mobilidade IPv6
- Vídeo-difusão sobre *multicast* IPv6
- VoIP em IPv6
- QoS na Vídeo-difusão sobre IPv6

Além destes projectos está previsto a curto prazo a realização de outros. A informação actualizada poderá ser encontrada no sítio oficial em www.ipv6.estg.ipleiria.pt.

[2] Sítio do projecto IPv6@ESTG-Leiria: http://www.ipv6.estg.ipleiria.pt

3. Mobilidade

Neste capítulo pretende-se enquadrar o conceito de mobilidade, permitir uma melhor compreensão e assimilação da Mobilidade IP (MIP), enumerando definições, necessidades e limitações da mobilidade.

Depois de no capítulo anterior ter sido realizado um breve enquadramento ao IPv6, este capitulo comtempla um enquadramento à mobilidade. No capítulo seguinte descreve-se a mobilidade IPv6, o seu funcionamento, implementações e estado da arte. Ainda neste capítulo será abordada a Mobilidade IPv4, uma vez que os princípios de funcionamento mantêm-se da versão IPv4 para a IPv6.

3.1 Introdução

Actualmente quando se fala em mobilidade a primeira associação que é realizada é com a telefonia móvel, a mais predominante e vulgar nas sociedades actuais, com inúmeros serviços disponibilizados. A figura 6 ilustra o cenário actual da integração de serviços por parte das operadoras de telecomunicações.

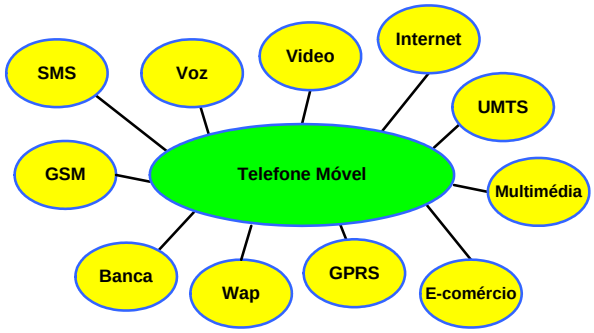


figura 6 - Integração de serviços por parte das operadoras de telecomunicações

O conceito de mobilidade é também associado às WLANs (*Wireless LANs*). No entanto esta restringe-à camada 2 do modelo OSI (ligação), impossibilitando a transição de rede ou subrede sem que haja quebra de ligação. O DHCP pode ser encarado como mecanismo de mobilidade, visto que permite que um dispositivo transite de uma rede para outra, atribuindo dinamicamente um endereço ao dispositivo, claro que implicando quebra de ligação. Em IPv6, a configuração também poderá ser realizada automaticamente pelo terminal móvel com base nas mensagens recebidas no link onde o nó se ligou.

A Mobilidade IP (MIP), protocolo da camada de rede, surgiu para contornar este problema, tendo como objetivo permitir a mudança de rede de segmento de rede de uma forma transparente para as camadas superiores, permitindo assim mobilidade entre diferentes redes e diferentes tecnologias,

sejam elas *wireless* (IEEE 802.11, HiperLan, …) ou as tradicionais redes com fio. Contudo neste caso, embora independente das tecnologias inferiores, existe dependência da interface física. A figura seguinte representa o modelo OSI e mostra alguns protocolos das camadas 2, 3 e 4.

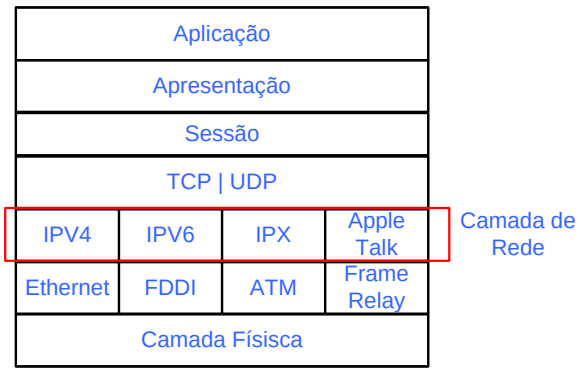


figura 7 - Modelo OSI.

Com o protocolo IPv6, prevê-se que no futuro todos os dispositivos móveis possuam pelo menos um endereço único e possam comunicar entre si com ligações ponto a ponto. Na telefonia móvel surgirá a 4G que será a geração IP, em que cada dispositivo possuirá um endereço IP (na realidade poderão ser mais do que 1 como será visto mais à frente) permitindo comunicar com os dispositivos das tradicionais redes IP que, entretanto também irão migrar gradualmente para IPv6.

A figura seguinte representa a integração de diferentes tecnologias por intermédio do IPv4.

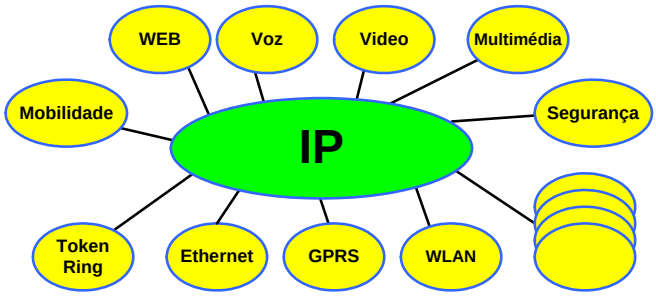


figura 8 - Interligação de diferentes tecnologias através do IPv4

A figura 9 mostra a integração de serviços e tecnologias por parte do IPv6. De salientar o facto de a segurança e a mobilidade se encontrarem integradas no protocolo IP.

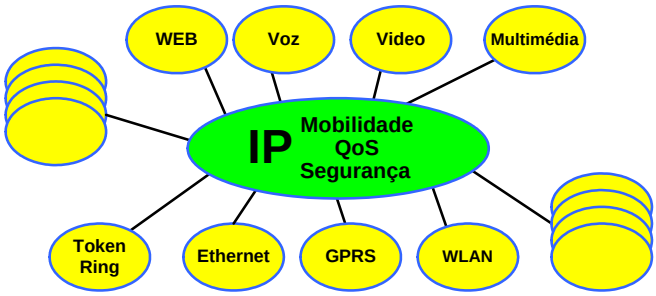


figura 9 - Integração de serviços e tecnologias por parte do IPv6

No entanto ainda é necessário muito trabalho de normalização, desenvolvimento de dispositivos e aplicações para que a evolução siga esse rumo.

Assim, alguns objectivos dos protocolos de mobilidade são os enumerados de seguida:

- fornecer um serviço transparente para as camadas de transporte e superiores, mantendo a ligação quando o ponto de ligação à rede é alterado;
- independência em relação às camadas inferiores à camada de rede (garantindo assim compatibilidade entre tecnologias), ou seja, não depende dos protocolos da camada de física e de ligação.
- segurança, eficiência, escalabilidade;
- sistema de sinalização leve permitindo um sistema escalável na Internet.

3.2 Conceitos de Mobilidade

Apresentam-se de seguida alguns conceitos de mobilidade em redes. Outros poderão ser encontrados no dicionário técnico presente no A neste relatório.

3.2.1 *Handover* ou *Handoff*

Handover ou *handoff* consiste na mudança de ponto de acesso de um terminal à rede. Inerente a esta mudança poderá estar a mudança de rede ou subrede, de tecnologia de acesso, de protocolo de rede e/ou de domínio administrativo.

O *handover* pode ser classificado em função do seu comportamento,ou seja, dependendo da sua rapidez, transparência para o utilizador final e se implica quebra da ligação ou se, pelo contrário, permite uma mobilidade efectiva/permanente à rede.

3.2.2 Roaming

Roaming não é mais do que o conceito de mobilidade. Consiste na capacidade de um terminal se deslocar entre diferentes redes (que formam uma rede global) mantendo a sua conectividade à rede global.

3.2.3 Conectividade passiva

O conceito é o mesmo que o dos sistemas celulares. A conectividade passiva permite que os terminais móveis não necessitem de ligação permanente à rede, diminuindo o consumo de recursos desta, podendo inclusivé adoptar mecanismos de gestão dos seus próprios recursos (nomeadamente

energéticos). No entanto, o terminal móvel precisa estar sempre pronto para ter acesso à rede ou ser contactado. Para isso, utiliza-se a noção dos sistemas celulares de divisão em áreas de *paging*.

3.2.4 Paging

Um domínio é sub-dividido em áreas de *paging*. Enquanto um terminal móvel (MN) se move dentro de uma área de *paging*, não necessita de enviar informações de actualização. Apenas envia essa informação quando houver uma mudança entre áreas de *paging*. Para isso, existe um outro tipo de tabela para auxiliar na operação de busca, ou *paging*, chamada de *paging cache*. Esse tipo de tabela é mantido apenas em alguns nós (reponsáveis por uma área de paging) da rede. O terminal móvel envia periodicamente pacotes de *paging-update*, que possuem informações diferentes dos pacotes de *route-update*, de forma a serem reconhecidos pelos nós responsáveis por manter as tabelas de *paging (paging cache).*

Desta forma, dois tipos de tabela são mantidos na rede, uma para os terminais em estado activo, presente em todos os nós e actualizadas por pacotes de *route-update* e outra para os inactivos, mantida em apenas alguns nós da rede. A primeira serve para localizar o terminal de estação para estação sem a necessidade de procurar o móvel. No caso de terminais no estado inactivo, são usadas as tabelas de paging para encontrá-los quando necessário.

O *paging-cache* possui um tempo de vida, denominado *paging-timeout*, que é maior do que o período do *routing-cache*. Os "mapeamentos" *paging-caches* são actualizados por qualquer pacote enviado por um MN, mas os *paging-updates* não actualizam a *routing-cache*.

3.3 Âmbito da Mobilidade

Actualmente podem-se definir vários tipos de mobilidade existentes na Internet. Pode definir-se a mobilidade pessoal e a mobilidade de terminal. A primeira é caracterizada por permitir ao utilizador a troca do dispositivo para aceder à rede e ainda assim continuar a ter acesso aos recursos e serviços oferecidos por tal rede. Um exemplo desse tipo de mobilidade acontece com os sistemas celulares GSM (*Global System Mobile*) através dos módulos SIM (*Subscriber Identity Modules*). Os sistemas GSM também permitem a mobilidade de terminal, que consiste no facto de um dispositivo de acesso à rede se poder deslocar, mudando de ponto de acesso a esta mesma rede mantendo a ligação. O presente trabalho foca as redes IP que são um exemplo de mobilidade de terminal.

Define-se também dois outros conceitos de mobilidade: microMobilidade (mM) e MacroMobilidade (MM).

MacroMobilidade define a mobilidade entre domínios administrativos (DAs) ou Sistemas Autónomos (SAs) distintos. Um DA é um domínio sobre uma mesma administração ou gestão. Um SA possui uma estrutura interna que é independente de tudo o que está para além do seu domínio.

MicroMobilidade é a mobilidade existente dentro de um mesmo domínio administrativo (DA), isto é, dentro de uma organização, entre pontos de acesso WLAN. Engloba também os casos em que num DA existem diferentes redes ou subredes. Assim, a mM poderá implicar a mudança entre diferentes tecnologias, e a mudança de enderenço IP, dependendo do protocolo de microMobilidade utilizado.

Como já referido, o conceito de mobilidade existe nas WLANs. No entanto esta restringe-se à rede ou subrede em que o terminal se encontra, e à tecnologia da camada de ligação usada(camada 2 do modelo OSI), impossibilitando a transição de (sub)rede sem que haja quebra de ligação, visto que a mudança de (sub)rede implica a mudança de configuração que, por sua vez, implica interrupção da sessão.

De notar que em várias bibliografias são encontradas diferentes definições para os mesmos conceitos. Exemplo disso são os conceitos de microMobilidade e macroMobilidade, cuja definição varia de bibliografia para bibliografia. Optou-se por seguir a definição que foi a apresentada anteriormente, e que será usada ao longo deste relatório, não por se considerar a mais correcta, mas porque é a mais comum nas diversas bibliografias.

3.4 A necessidade da Mobilidade IP

O protocolo IP encaminha pacotes de um ponto de origem a um ponto de destino através de *routers*, que recebem pacotes por interfaces de entrada e os encaminham para interfaces de saída, de acordo com tabelas de encaminhamento. Estas tipicamente, mantêm a informação do *next-hop* para cada endereço IP destino, de acordo com o número de rede ao qual o endereço IP está associado. Analisando agora uma aplicação de rede, esta contém no seu código a abertura de um *socket*, que é a associação de um endereço de origem (camada de rede) e um porto (camada de transporte) de origem, com um endereço de destino e porto de destino através de um protocolo (por exemplo: 192.168.232.72, 10001, 192.168.232.76, 100002, TCP). Isto garante que a camada 3 do modelo envia os dados da aplicação correctamente quando os pacotes chegam à máquina de destino.

Supondo que um dispositivo móvel inicia, por exemplo, uma transação FTP e, no meio da transmissão, o nó móvel muda de rede. Para manter a ligação FTP na camada de transporte, é preciso manter o mesmo endereço IP. Mudando o endereço IP, a ligação é desfeita.

Por outro lado, a entrega de pacotes para o ponto de ligação corrente do nó móvel depende do seu endereço IP. Quando o nó móvel muda de rede, recebe um novo endereço IP e isto significa que haverá uma mudança no encaminhamento dos pacotes enviados a este.

Resumindo, a solução da mudança do endereço IP da máquina móvel não é viável, pois os endereços a atribuir estão dependentes da localização do terminal, tornando a localização do terminal difícil, e a constante actualização de DNS seria impensável. Além disto haveria quebra de ligações TCP, não permitindo o "*always-on*" e causando problemas de segurança.

Outra possível solução para a mobilidade é a alteração das rotas para as máquinas móveis. No entanto, isto implica a mudança de tabelas de encaminhamento dos routers, tornando-se uma solução não compatível (não escalável) com mudanças frequentes de posição e número elevado de terminais móveis, para além dos acrescidos problemas de segurança.

3.5 MacroMobilidade (MM)

A MacroMobilidade já foi definida anteriormente, como sendo a mobilidade entre sistemas administrativos diferentes. Este tipo de mobilidade é pouco frequente, o que resulta em handoffs pouco frequentes, e consequentemente numa baixa mobilidade.

São exemplos de protocolos de gestão de macromobilidade as duas versões do MIP, MIPv6 [19], MIPv4 [17] e o Session Initiation Protocol (SIP) [16]. Outras propostas têm surgido, provenientes de projectos de investigação, no entanto estas não serão focadas.

3.5.1 MIPv6

A mobilidade em IPv6 será abordada no próximo capítulo, com incidência óbvia no protocolo MIPv6 [19], mas onde também serão focados os protocolos de mM na sua versão para IPv6. Será realizado um enquadramento histórico, descrito o funcionamento deste protocolo, e dos mecanismos associados, e será também realizada alusão ao seu antecessor o MIPv4 para efeitos de comparação, estudo e compreensão da evolução. Serão ainda abordadas questões relacionadas com a segurança.

3.5.2 MIPv4

A RFC 2002 [9], actualizada pelas RFCs 3220 [15] e mais recentemente pela RFC 3344 [17], define a mobilidade IPv4 (MIPv4). Este protocolo foi projectado para resolver o problema da mobilidade, permitindo que um nó móvel tenha dois endereços IP, denominados *Home Address* (HoA) e *Care-of Address* (CoA). O HoA é estático e referenciado, por exemplo, para identificar ligações da camada de transporte (por exemplo, TCP). O CoA muda a cada novo ponto de ligação e pode ser visto como endereço de significado topológico do nó móvel. O CoA indica o novo ponto de ligação do nó móvel.

A solução MIPv4 considera 4 elementos no seu processo, são eles o *Home Agent* (HA - router na rede de origem do nó móvel), o *Foreign Agent* (FA - router na rede, que não a de origem, onde o nó móvel

está ligado), o teminal móvel (MN); o terminal correspondente (CN). Ao mudar de rede o MN adquire um CoA com o FA e registrá-lo com o HA (*binding*).

A figura seguinte apresenta as entidades intervenientes da arquitetura MIP.

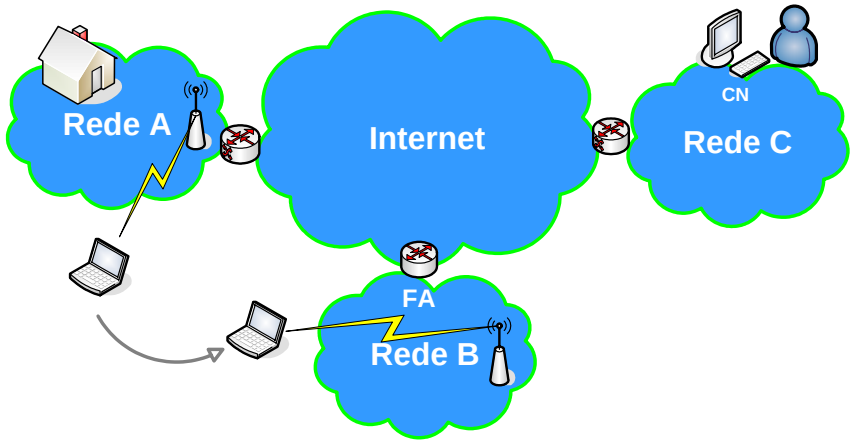


figura 10 - Arquitectura Mobile IP

A operação do protocolo MIP pode ser brevemente descrita pelos seguintes passos:

- Os agentes de mobilidade (HA e FA) anunciam as suas presenças através de mensagens chamadas "*Agent Advertisement*";
- Estas mensagens podem, opcionalmente, ser solicitadas por nós móveis, através de mensagens chamadas "*Agent Solicitation*";
- Um nó móvel recebe estes anúncios enviados pelos agentes de mobilidade e determina se está na sua rede ou numa outra rede (rede visitada),
- Se o nó móvel detecta que está na sua rede original, ele opera sem o serviço de mobilidade. Se ele acaba de voltar à sua rede, ele retira o registro (*binding*) realizado anteriormente com o seu HA, através de uma troca de mensagens "*Registration Request*" e "*Registration Reply*" com o agente;
- Quando um nó móvel detecta que se moveu para uma rede “estrangeira”, ele obtém um CoA naquela rede. O CoA pode ser alocado pelo FA ou por outro mecanismo, como DHCP, por exemplo;
- Quando o nó móvel está a operar fora da sua rede, ele precisa registar o seu CoA com o seu HA (*binding*). Isso é realizado através da troca de mensagens *Registration Request* e *Registration Reply*;
- Os pacotes enviados para o endereço de origem do nó móvel (HoA), por um nó correspondente (CN), são interceptados e enviados por tunel pelo HA para o CoA, recebidos na saída do túnel e, finalmente, entregues ao nó móvel;

- Os pacotes enviados pelo nó móvel são, geralmente, entregues ao destino usando mecanismos de encaminhamento padrão, não passando necessariamente pelo HA,
- Os pacotes enviados para o CoA do nó móvel usam também os mecanismos de encaminhamento padrão.

Percebe-se, com a descrição acima, que o funcionamento do MIP gera um "encaminhamento triangular", ou seja, um nó correspondente, conhecendo apenas o HoA do nó móvel, enviará os pacotes para a rede original do nó móvel. Porém, como o nó móvel se moveu, o HA intercepta os pacotes e encaminha-os, através de um túnel, para o nó móvel no seu CoA, ou seja, envia o pacote para a rede em que o nó móvel está momentaneamente. Este facto é um dos problemas do MIP, já que todos os pacotes serão enviados por túnel para o nó móvel noutra rede, o que gera sobrecarga de processamento no HA, além deste ser um ponto de falha único na rede. O MIPv6 soluciona este problema através de optimização de rota e será visto mais tarde. O IPv4 também tem optimização de rotas, no entanto existem restrições:

- O CN precisa de uma pilha IP melhorada
- A gestão de chaves é problemática (não existe protocolo de troca de chaves, sendo esta realizada manualmente)
- Considerações de segurança
- Chaves partilhadas ou infra-estrutura PKI
- Solução pouco escalável

Outras soluções para optimização de rota no MIPv4 também foram propostas mas, actualmente, este item não é de interesse do IETF.

A figura seguinte ilustra o encaminhamento de pacotes para um nó móvel fora de sua rede.

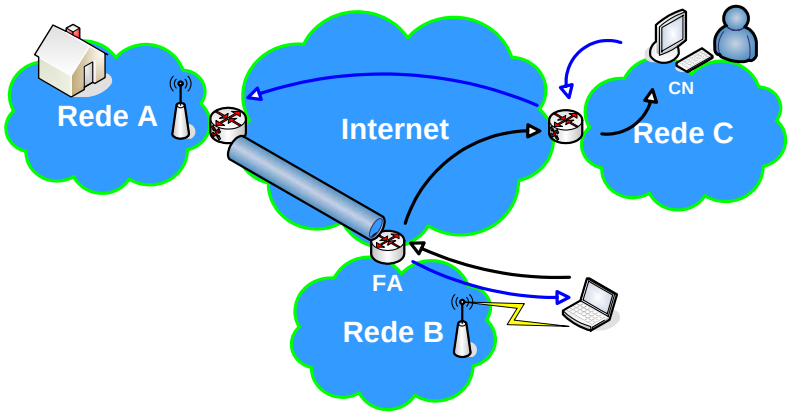


figura 11 - Operação de IPv4 móvel

O *Agent Discovery* é um método pelo qual um nó móvel determina se está correntemente ligado à sua rede ou a uma rede visitada, além de possibilitar a detecção de movimento de uma rede para outra.

Quando ligado a uma rede estrangeira, o método possibilita a determinação do CoA atribuído por cada FA sobre a rede.

Quando um nó móvel detecta um movimento, deve-se registar na nova rede visitada com um CoA adequado, e quando ele detecta que regressou à sua rede de origem, deve remover o registo de que estava fora de sua rede com o HA.

Quando o nó móvel não se encontra na rede original deve:

- requisitar serviços de encaminhamento quando em visita a outra rede;
- informar o seu CoA corrente ao HA;
- renovar o registro quando expira;
- remover o registro quando retornar à sua rede de origem.

È através do mecanismo de registo (*Registration*), que o nó móvel comunica a sua informação corrente de acessibilidade ao HA.

As mensagens de registo trocam informações entre um nó móvel, um FA (opcional) e o HA. O *Registration* cria ou modifica uma ligação de mobilidade (*binding*) no HA, associando o HoA do nó móvel com seu CoA por um tempo especificado (lifetime).

3.5.3 SIP

O *Session Initiation Protocol* (SIP) difere dos outros porque é um protocolo de MM da camada de aplicação (L7), definido na RFC 3261 [16]. É um protocolo de gestão de mobilidade, desenvolvido pelo IETF, capaz de fornecer mobilidade pessoal e mobilidade de terminal.

Para o funcionamento do SIP é necessária a presença de agentes de utilizador (User Agent - UA) nos dispositivos do utilizador. Os utilizadores do SIP devem ser identificados através de SIP URLs, que lembram o formato de endereço de e-mail, e que têm o formato SIP: **utilizador@domínio**, onde domínio é o domínio original do utilizador.

Em cada domínio há um servidor de registo SIP, que possui um endereço IP estático e é facilmente acessível por servidores DNS. Esse servidor SIP intercepta as mensagens de registo e actualiza a informação de localização do dispositivo. A mensagem de registo possui o SIP URL, o endereço IP actual, o número do porto e o protocolo de transporte que é utilizado pelo dispositivo. São possíveis outros campos adicionais na mensagem de registo, como o tempo de validade do pedido do registo, que por omissão é uma hora. O servidor de registo autentica o utilizador e cria o “mapeamento” entre o URL SIP e o endereço de rede no banco de dados de localização.

Através do SIP URL e de um servidor de proxy ou de redireccionamento, o utilizador pode ser contactado independente da sua localização actual e do endereço IP utilizado.

O servidor *proxy* é o responsável pelo “mapeamento” da URL para o endereço IP actual utilizando o servidor de registo. Após o mapeamento, o *proxy* encaminha a mensagem recebida para o endereço IP obtido. O servidor de redireccionamento é menos frequente na arquitectura SIP e tem função similar ao servidor de DNS. Através dele, um utilizador A pode solicitar a localização de um utilizador B e receber uma lista de endereços. Após isso, o utilizador A realiza toda comunicação directamente com o utilizador B.

3.5.4 Aspectos de segurança no MIPv4

Apesar da segurança não ser objecto de estudo neste projecto, dada a sua importância no contexto actual, era inevitável fazer-se referência a esta, ainda que de forma breve. Este é um tema muito extenso, por isso nesta secção será restrito apenas às questões mais importantes da segurança na mobilidade IP.

A mobilidade IP pode trazer sérios problemas à segurança, caso não seja implementada de uma forma adequada. A autenticação do nó móvel é imprescindível. Imagine-se o cenário em que alguém mal intencionado faz, remotamente, um registo num HA de uma rede local. Poderia então manipular as regras da *firewall* e explorar vulnerabilidades dentro da rede interna. Além disto, diversos tipos de ataques poderiam ser facilmente implementados. É importante, portanto, que uma solução para MIP mantenha a segurança do protocolo IP original.

Um requisito básico para o funcionamento seguro do MIPv4 é que o mesmo ofereça mecanismos para autenticar o processo de registo ("*binding update*") dos nós móveis, enquanto remotos. O HA deve ser capaz de autenticar um nó móvel da rede e oferecer serviços de mobilidade. A RFC 3344 [17] especifica mecanismos para que esta autenticação seja realizada em mensagens de registo provenientes de nós móveis. Além de autenticar o registo de nós móveis junto ao seu respectivo *Home Agent*, a especificação permite que os mesmos mecanismos sejam adoptados para a implementação de autenticação entre o nó móvel e um FA, e entre um FA e um HA.

O mecanismo utilizado para autenticação usa uma chave secreta partilhada entre as partes envolvidas. Para componentes dentro de um mesmo domínio administrativo, como HA e MN, é simples de configurar manualmente (um protocolo de distribuição automática de chaves pode ser usado, mas a especificação não cita nenhum em especial) esta chave secreta em cada um dos nós da rede. Todavia, entre nós em diferentes domínios administrativos, é impossível estabelecer um relacionamento de segurança prévio entre os participantes. Isto oferece problemas para a implementação de autenticação envolvendo o FA, uma vez que o mesmo pode estar nos mais remotos lugares.

Por não oferecer nenhum mecanismo de segurança nativo, o IPv4 tem que recorrer a outras soluções para garantir confidencialidade e integridade dos dados trocados, principalmente entre os nós locais.

Várias propostas existem para uma implementação usando IPSec, mas nenhuma solução foi padronizada ainda pelo IETF.

No MIPv4, o HA faz uso do protocolo ARP após o processo de registo de um determinado MN. O HA implementa a funcionalidade de Proxy ARP para responder requisições ARP pelos MN e, desta forma, é capaz de atrair para si todo o tráfego destinado aos MNs registados, enquanto estes últimos estiverem remotos. Além disto, ele usa o *Gratuitous* ARP para actualizar a ARP cache de todos os nós na rede. Isto evita que nós com o endereço MAC de um nó móvel tentem enviar pacotes para o mesmo directamente, enquanto ele estiver numa outra rede. Vários ataques podem ser implementados usando as conhecidas e bastante exploradas fragilidades do protocolo ARP.

O MIPv4 pode oferecer problemas para *firewalls* e routers. Isto acontece porque o MN transmite pacotes para os CNs usando como endereço de origem, nos pacotes, o seu próprio HoA. Como uma protecção anti-spoofing, muitos routers e *firewalls* implementam a chamada "*ingress filtering*". Isto significa que estes softwares e/ou hardwares verificam se o endereço de origem dos pacotes pertence à rede na qual ele está situado. Se tais pacotes usam endereços estranhos à rede, eles devem ser descartados e "logados" como uma tentativa de realizar IP *Spoofing*. Portanto, a comunicação entre o MN e o CN pode ser comprometida, uma vez que os pacotes, provenientes do MN e destinados ao CN, seriam descartados.

Pelo mesmo motivo, o MIPv4 também pode ter problemas em redes, onde o NAT seja usado. A solução para estes problemas é usar "*Reverse Tunneling*", onde todos os pacotes destinados ao CN seriam encapsulados e transmitidos, usando o CoA, via HA. Contudo, tal solução acarreta um *overhead* e um significativo impacto no processo de encaminhamento dos pacotes, para além do já existente devido ao encaminhamento triangular.

3.5.5 Problemas do MIP

O MIP foi idealizado para ambientes com utilizadores de baixa mobilidade, ou seja, baixo número de *handoffs*. Para ambientes de alta mobilidade (*handoffs* frequentes), apresenta alguma inadaptação e ineficiência, devido à frequente necessidade do MN realizar o registo no seu *Home Agent* (HA) sempre que mudar de rede. Isto implica longos atrasos no processo de registo e grande carga de sinalização na Internet, principalmente quando o terminal móvel (MN) estiver distante do seu HA. Com a intenção de possibilitar *handoffs* rápidos e suaves, algo não possível através do MIP, foram idealizados os protocolos de microMobilidade (mM), que são soluções adequadas para áreas geográficas restritas, denominadas de Domínio Administrativo (DA).

Através desses protocolos, o processo de actualização do registo (*binding*) é realizado por uma entidade responsável no domínio administrativo, denominado de *gateway*, não necessitando de actualizar o HA.

Na figura 12 são ilustrados alguns movimentos possíveis dentro de Domínios Administrativos (DAs) e entre DAs. Os movimentos representados por 0, 1 e 3 correspondem à microMobilidade, e os movimentos 2 só são possiveis com recurso à MacroMobilidade (por exemplo com o MIP).

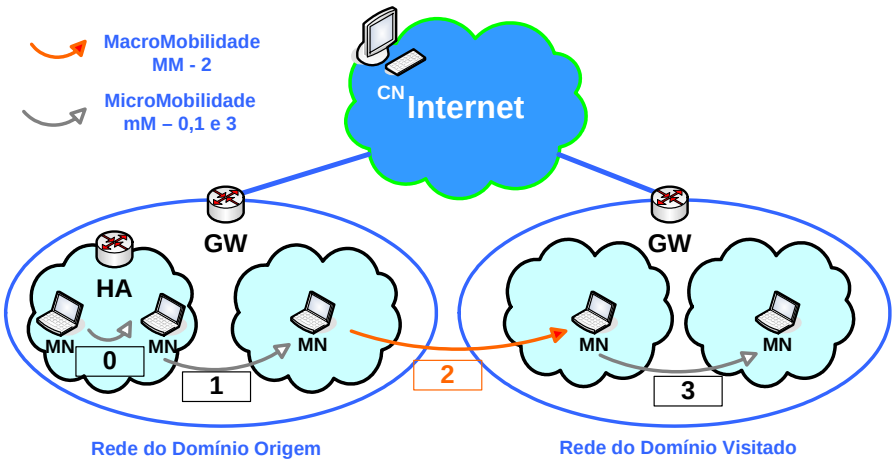


figura 12 - Movimentos de microMobilidade e MacroMobilidade.

Apesar das vantagens dos protocolos de microMobilidade, a gestão de mobilidade entre áreas de mM é realizado através do protocolo MIP, que recai nos problemas já citados anteriormente, mas devido à sua menor frequência, não será tão crítico.

Resumindo, os problemas associados à mM são:

- Tempo de detecção do movimento
- Tempo de configuração do endereço da nova rede visitada
- Tempo de actualização da nova localização (*biding update*)
- Pacotes enviados para CoA antigo são perdidos
- Mudança frequente implica muita sinalização

3.6 MicroMobilidade

A microMobilidade (mM) consiste em *handoffs* dentro de um mesmo sistema administrativo. Este tipo de mobilidade poderá ser muito frequente, o que resulta em *handoffs* críticos e frequentes, ou seja, existe uma alta mobilidade.

Para os casos em que não existe mudança de rede ou subrede, os protocolos da camada de ligação conseguem fazer os *handovers*, e neste caso são os mais indicados pois são mais rápidos e eficazes, apresentando um nível de desenvolvimento bastante avançado, existindo diversas soluções bastante completas, maduras e estáveis.

Sempre que existe mudança de rede ou subrede, terá de ser usado um protocolo da camada de rede. Uma solução eficaz consiste no uso de protocolos de microMobilidade dentro de um DA,tendo MIP a interligar os DAS.

Para resolver a questão da mM surgiram vários protocolos:

- CIP – *Celullar* IP,
- HAWAII,
- TIMIP - Terminal Independent Mobility for IP

Existem ainda as extensões do MIPv6 para suporte de microMobilidade:

- HMIP – Hierarchical Mobile IP,
- FMIP – FastHandover for MIP

Estes protocolos procuram resolver os problemas da mM com transições mais rápidas, maior eficiência, podendo substituir mobilidade na camada de ligação, com vantagens de uma solução "*all-IP*". Apresentam uma estrutura de domínio hierárquica e um desempenho de mobilidade rápido. Porém estão limitados ao domínio administrativo, necessitando dos protocolos de MM para mobilidade global.

Os protocolos de mM oferecem suporte de mobilidade para as transições mais frequentes e que implicam rapidez: Movimentos do tipo 1 e 3 (ver figura 12), e adicionalmente do tipo 0 (estes podem ser realizados ao nível 2).

Todas as propostas, com excepção do *FastHandover*, têm em comum o facto de haver um *gateway* principal na rede para gestão da mobilidade dos terminais móveis visitantes, estrutura de domínio hierárquica. O MN, autentica-se na 1ª vez que chega à rede visitada, efectuando o registo no HA. Uma vez autenticado, o MN tem sua localização mapeada por tabelas ao longo da rede, de forma a ser sempre alcançável a partir do *gateway* comum. As informações de localização serão actualizadas pelos nós intermédios, formando uma nova rota até ao MN. O *Gateway* será responsável pela gestão da mobilidade do MN dentro do DA, não sendo necessário mais registos no HA, devido a movimentações dentro do DA.

3.6.1 CIP – Cellular IP

O *Cellular* IP (CIP) encontra-se definido no *draft* com o mesmo nome [28], proposto pela Columbia University e pela Ericsson baseado no paradigma IP, herdando os princípios dos sistemas celulares para gestão de mobilidade: conectividade passiva, *paging* e controlo rápido de *handoff*.

Com este protocolo a rede de acesso é conectada à Internet através de um *gateway* principal comum a todos os nós, como mencionado na secção 3.6. Os MN visitantes comunicam com a rede através dos

APs. Periodicamente, o *gateway* envia um sinal de *broadcast* para toda a rede de acesso. Os nós intermédios registam de onde receberam o sinal para que possam enviar, por aquela rota, pacotes endereçados ao *gateway*. Os APs periodicamente emitem sinais (*beacons*) que permitem aos terminais móveis identificar a rede mais próxima deles. Os pacotes são transmitidos a esse AP e daí até o *gateway* comum. Cada nó mantém uma tabela de rotas (*routing-cache*) e os pacotes transmitidos actualizam uma entrada da tabela da seguinte forma: ao passar por um nó, a tabela é actualizada indicando de qual vizinho o pacote veio e qual a sua origem. Isso forma uma cadeia que é utilizada quando os pacotes vêm em sentido contrário (*downlink*). Os pacotes são encaminhados de acordo com as tabelas mantidas em cada nó até ao MN. Pacotes de controlo são enviados periodicamente pelo terminal móvel para evitar que o mapeamento seja removido por expiração do tempo das entradas na tabela. Se não tiverem pacotes para transmitir, os terminais móveis enviam apenas pacotes de *route update*, para manter as suas entradas nas tabelas.

Em "http://www.comet.columbia.edu/cellularip/overview.htm" encontra-se disponível o código fonte da implementação e manuais (porem já não é actualizado há bastante tempo).

3.6.2 HAWAII

O *Handoff-Aware Wireless Access Internet Infrastrucuture* (HAWAII), é definido no draft "*IP micro-mobility support using HAWAII*" [29], também usado no draft "*Paging support for IP mobility using HAWAII*" [30], ambos os drafts expirados.

Cada domínio é estruturado de acordo com uma hierarquia de nós, com um "router raiz"(*gateway*) no topo da rede. Dentro desse domínio, mesmo mudando o ponto de acesso, o MN consegue comunicar porque todos os pacotes que o têm como destino são enviados ao *gateway*. A partir daí, encontram o MN através de rotas dinamicamente estabelecidas. Em cada sub-rede visitada, o CoA é utilizado como endereço do MN, sendo actualizados os nós da rede de modo a manterem rotas para esse endereço, além das rotas do encaminhamento tradicional.

3.6.3 TIMIP - Terminal Independent Mobility for IP

O TIMIP, definido no *draft* "*Terminal Independent Mobile IP* (TIMIP)" [31], tem a curiosidade de ser um *draft* elaborado por portugueses membros do INESC.

Neste o MN precisa registar alguns dados com o *gateway*. Esses dados incluem endereços IP e MAC, além de informação de autenticação. Os dados são então enviados para todos os pontos de acesso. Ao se ligar, o MN fornece o endereço MAC ao ponto de acesso, que actualiza sua tabela com uma entrada para a localização do MN, e envia uma mensagem de *Routing Update* para um outro nó mais próximo do *gateway* de acesso à Internet. O procedimento é repetido e as tabelas com o caminho para o MN são actualizadas pelos nós até ao *gateway*.

3.6.4 HMIP – Hierarchical Mobile IP

O "*Hierarchical Mobile IP"* (HMIP) [36] propõe uma nova entidade, chamada *Gateway Foreign Agent* (GFA). Ao visitar uma rede que possua esta arquitectura, o terminal móvel regista-se apenas uma vez com o HA, através do GFA, cujo endereço será o *Care-of Address*. Na hierarquia inferior, poderão ser visitadas outras redes, mas os novos registos serão realizados apenas com o GFA. Assim, para o HA, enquanto o terminal permanecer na área de microMobilidade, o CoA é o endereço do GFA, evitando registos frequentes com a rede de origem.

3.6.5 FastHandover para MIP

O FMIP, especificado no *draft* "*Mobile IPv4 Fast Handovers*"[32], reduz a perda de pacotes fornecendo conectividade IP rápida assim que uma nova ligação é estabelecida. Isto é realizado fixando o encaminhamento durante o processo de configuração e de *binding update*, permitindo assim que os pacotes entregues ao CoA sejam encaminhados para o novo.

Em adição, o FMIP fornece suporte para pré-configuração da informação da ligação (tal como o prefixo de subrede) na nova subrede, enquanto o MN ainda se encontra conectado à subrede "anterior". Isto reduz a quantidade de tempo de pré-configuração da ligação

3.6.6 Low Latency *Handovers* para MIP

O mecanismo de "*Low Latency Handovers*" [37] consiste em extensões ao MIP, que permite optimizações de detecção, utilizando mecanismos dependentes da tecnologia, com recurso a primitivas genéricas:

- *PRE-Registration* – Modelo predictivo, antes do *handover* acontecer (semelhante ao *CIP Semi-Soft Handover*)
- *POST-Registration* – Modelo reactivo, imediatamente depois do *handover* acontecer (semelhante ao *TIMIP Handover*)

Usa também optimizações de registo:

Redirecção temporária do tráfego desde o FA anterior para o novo FA (semelhante ao HAWAII *Forwarding Handover*).

3.7 WiMax

O WiMAX (Worldwide Interoperability for Microwave Access) [103]é a norma IEEE 802.16 [102] que define uma tecnologia *wireless* para fornecer conectividade em banda larga ao nível de uma MAN

(Metropolitan Area Network). Os sistemas baseados no WiMAX podem ser usados para transmitir sinais até 30 milhas. Esta é uma tecnologia que apresenta uma solução capaz de fornecer mobilidade ao nível de uma MAN, suportando diferentes tecnologias, nomeadamente ATM, IPv4, IPv6, Ethernet, e VLANs.

3.8 O futuro 4G, a geração IP

Espera-se que num futuro próximo exista o conceito de "*Always best concected*", em que qualquer dispositivo se liga á rede através do serviço que lhe confere uma melhor ligação, independentemente das características de transmissão.

A evolução das gerações das comunicações móveis seria então a seguinte:

- 1ª - Comunicações móveis analógicas
- 2ª - GSM (circuitos digitais), GPRS (pacotes)
- 3ª - UMTS (maior banda, pacotes, QoS)
- 4ª - *Always Best Connected*

A 4ª geração das comunicações móveis ainda está em investigação, sendo por isso uma incógnita.

De uma forma simplista, existem duas aproximações em estudo: uma evolutiva, a partir das soluções celulares (GSM+GPRS/UMTS), com interesses por parte do ETSI, 3GPP, fabricantes de telecomunicações; a outra baseada em IP, usando IPv6, apoiada pelo IETF e fabricantes de equipamento IP.

Porém, a idealização de que no futuro todos os dispositivos, sejam eles móveis ou fixos, possam comunicar entre si, pode passar pela coexistência de diversas tecnologias, todas elas com mecanismos que permitam a interoperabilidade entre si. A figura figura 13representa a interoperabilidade de várias tecnologias, integrando num único terminal suporte para acesso a diferentes redes de diferentes tecnologias, integrando na *interface* de acesso ao meio o respectivo suporte para acesso a estas.

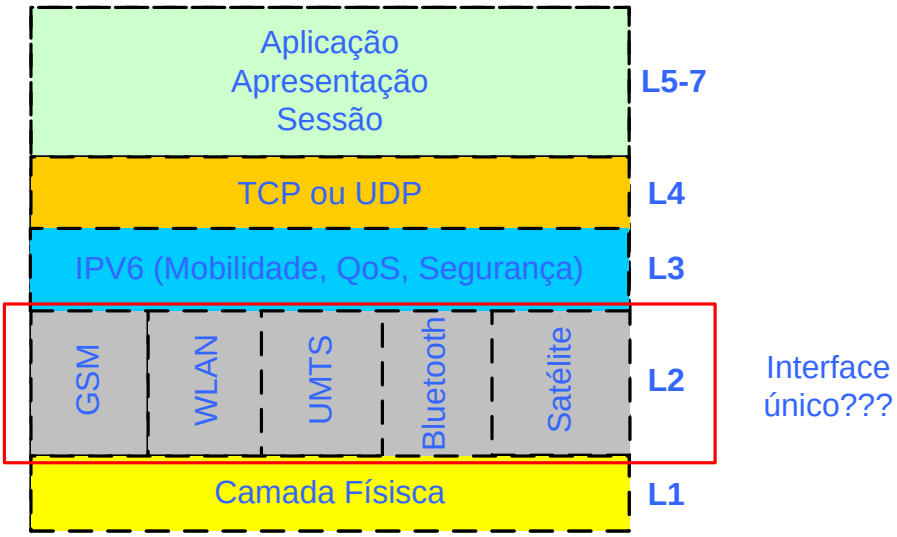


figura 13 - Possível arquitectura de um terminal.

Supondo que no futuro existisse o conceito de *Body Area Network* [104], onde as funcionalidades do terminal se encontrassem embutidas no vestuário, corpo, óculos, relógio, (…). Neste caso o utilizador transportaria uma rede, em vez de um terminal, e esta comunicaria com as redes ambiente.

Algumas previsões podem parecer irrealistas, mas tomando em consideração algumas previsões realizadas no passado, constata-se que poderão até ser um pouco conservadoras.

Muitos são os que preferem reservar-se quando se fala no futuro das tecnologias de informação, talvez com medo de errar. Limitam-se a fazer discursos vagos, e usando como termo de comparação a evolução realizadas nos últimos anos. Falam que muitos dos produtos e serviços do futuro ainda não existem e estão para ser inventados à medida em que evoluímos.

3.9 Conclusão

As tecnologias de WLAN permitem apenas *handoffs* ao nível da camada de acesso, ou seja, entre pontos de acesso da mesma rede. Qualquer outro movimento terá de ser ao nível da camada de rede.

Os mecanismos de DHCP não permitem a mobilidade efectiva do terminal, visto que, apesar de permitem que um dispositivo transite de uma rede para outra, atribuindo dinamicamente um endereço ao dispositivo, implicam no entanto a quebra de ligação. Além disso, se para além de um terminal querer aceder à Internet, também quiser ser acedido, mudando constantemente o IP, torna-se um processo difícil.

A MacroMobilidade (MM) foi definida como a mobilidade existente entre domínios administrativos (DAs), e a MicroMobilidade (mM) como a mobilidade existente dentro de um mesmo domínio administrativo (DA).

O protocolo MIP prevê-se o único capaz de fornecer mobilidade à escala planetária. No entanto existem algumas limitações ao nível do seu desempenho quando existe mudança frequente de rede por causa dos atrasos provocados com a detecção de movimento, tempo de configuração do endereço e actualização da nova localização. Também a perda de pacotes enviados para o antigo CoA e a elevada sinalização existente se tornam críticos quando a distância à rede original é elevada, e os percursos por onde é enviada a sinalização têm pouca largura de banda ou se encontram congestionados.

Os protocolos de mM oferecem mecanismos eficientes de mobilidade não global, com transições rápidas, maior eficiência, limitados apenas a domínios administrativos. Porém, para suportar a mobilidade global entre DAs, a mM é integrada com o MIP.

Sempre que possível a micro mobilidade poderá ser realizada mais eficientemente ao da ligação, no entanto, os protocolos de microMobilidade podem substituir a mobilidade no nível 2, com vantagens de uma solução "*all-IP*". Por exemplo, a segurança será mais eficaz ao nível da camada de rede do que ao nível da ligação.

A maioria dos estudos de microMobilidade IPv4 nunca passaram de *drafts* (os que lá chegaram), e a maioria já há muito que deixou de ser objecto de estudo e interesse, e por isso encontram-se obsoletos. Todos os esforços parecem agora concentrar-se em encontrar soluções em IPv6:

- Primeiro têm a vida facilitada porque com IPv6 é muito mais simples

A complexidade das redes e do encaminhamento é reduzida em muito com o IPv6. Veja-se o caso da segurança entre outros problemas do IPv4 que desaparecem ou são simplificados com o IPv6.

- Segundo porque já se compreendeu que o ipv6 é inevitável e é mesmo uma realidade

Todos os principais sistemas operativos já possuem suporte nativo, existem esforços em desenvolver aplicações complementares para a migração, mecanismos de transição, (…).

- Terceiro a mobilidade em IPv4 neste momento não faz muito sentido, e provavelmente nunca terá sucesso, isto se chegar a ser implementada em larga escala

É impensável partir para um projecto de mobilidade à escala mundial com a escassez de endereços IP, isto porque a mobilidade necessita de ligações ponto a ponto, de modo a garantir performance, fiabilidade e segurança. Este objectivo pressupões a existência de endereços IP públicos em número suficiente.

Além disso, a Mobilidade IP ainda não está muito implementada, e vai demorar até se tornar uma necessidade e ganhar popularidade, e provavelmente nessa altura já o IPv6 assumiu o papel de principal protocolo da Internet.

4. MIPv6 - Mobilidade IPv6

Este capítulo aborada o MIPv6, contudo dado que este descende do MIPv4, e possui um comportamento muito idêntico a este, terá de realizada obrigatoriamente referência ao seu antecessor e ao seu funcionamento para efeitos de comparação

Assim neste capitulo serão descritos os marcos históricos do MIPv6 desde o seu nascimento até ao dia de hoje, posteriormente será descrito o MIPv4 e o seu funcionamento, que servirá para ajudar a descrever o funcionamento MIPv6 no sub-capítulo seguinte, bem como para estabelecer a comparação entre ambos. Serão ainda enumerados e descritos diversos mecanismos e comportamentos associados ao MIPv6, bem como outros protocolos de mobilidade IPv6.

Antes de apresentar a conclusão deste capítulo será realizada referência à segurança do MIP, onde a descrição de questões do MIPv4 servirá de termo de comparação com o MIPv6, permitindo assim perceber a evolução deste, e verificar quais as novidades introduzidas em relação ao seu antecessor.

4.1 História do MIPv6

Neste ponto são apresentados alguns dos principais marcos do MIPv6:

- Janeiro 1996: primeiro *draft* do MIPv6 [26]com 20 páginas.
- Julho 2003: IESG aprova os *drafts* do MIPv6.
  - draft 24 do *Mobility Support in IPv6* [24] com 171 Páginas
  - draft 6 do “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents” [27] com 48 Páginas.
- Junho de 2004: RFC 3775 “Mobility Support in IPv6” [19].
- Junho de 2004: RFC 3776 “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents” [20]
- Fevereiro de 2006: versão final do MIPv6 2.0 para Linux com suporte para todas as funcionalidades das RFC’s 3775 e 3776.

No futuro aguarda-se pela sua inclusão no *kernel* do Linux e de toda a família Unix. Espera-se que os próximos lançamentos dos principais sistemas operativos (Windows, IOS, ...) venham com suporte de MIPv6 incluído. Entretanto outros protocolos relacionados com a mobilidade serão desenvolvidos e permitirão complementar o funcionamento do MIPv6, tais como os protocolos de microMobilidade e

de mobilidade de redes. A segurança associada a estes protocolos também é objecto de estudo constante.

4.2 Introdução ao MIPv6

Sem suporte especifico para mobilidade IPv6 (MIPv6), os pacotes destinados para um nó móvel (PC ou *Router*), não estarão aptos a alcançar esse nó enquanto este se encontrar fora do seu troço de ligação original (o *link* original do nó móvel e cujo prefixo de subrede é igual ao do seu Home Address (HoA)). Tal acontece porque o encaminhamento é baseado no prefixo de subrede existente no campo do endereço IP de destino do pacote. De modo a manter a comunicação, mesmo que ocorra movimento, o nó móvel poderá mudar o seu IP cada vez que se move para um novo *link*, mas, neste caso, o nó móvel não poderá manter o transporte e as ligações das camadas superiores quando muda de localização. O suporte de mobilidade em IPv6 é particularmente importante, uma vez que os computadores móveis irão constituir uma maioria, ou pelo menos uma fracção significativa da população da Internet durante o tempo de vida do IPv6.

4.3 Definição do MIPv6

Cada nó móvel é sempre identificado pelo seu HoA, independentemente do seu ponto de ligação à Internet. Enquanto situado longe da sua rede original (*home network*), o nó móvel tem também atribuído um Care-of-Address (CoA), que fornece informação da sua localização. Os pacotes IPv6 enviados para o HoA do nó, são reenviados de forma transparente, pelo Home Agent (HA), para o CoA. O protocolo permite que os nós IPv6 armazenem o registo da ligação entre um HoA e um CoA de um nó móvel, podendo assim enviar pacotes destinados a esse nó móvel directamente para o seu CoA.

4.4 Operação do MIPv6

O protocolo IPv6 apresenta características que o tornam primordial no desenvolvimento de soluções de mobilidade, sejam elas para ambientes UMTS, GPRS ou WLANs. Algumas dessas características são o seu vasto espaço de endereçamento, autoconfiguração e suporte integrado de mobilidade.

No entanto, a integração de IPv6 actualmente, implica o uso não só de soluções “IPv6-only”, mas também a utilização de mecanismos de transição (túneis automáticos ou manuais), e de mecanismos de tradução (conversão de tráfego IPv6 em IPv4), de modo a desenvolver cenários operacionais IPv6, integrando mobilidade entre diferentes tecnologias (3G/UMTS, GPRS, WLANs), e soluções operacionais de integração de serviços

O Mobile IPv6 tem um funcionamento semelhante ao MIP, permitindo que um terminal móvel (MN) se mova entre diferentes redes sem quebrar a ligação. Isto significa que o endereço original (Home Address - HoA) nunca se modifica. O nó móvel pode estar em qualquer lugar sendo os pacotes encaminhados correctamente para ele através de mecanismos apropriados. O movimento é, desta forma, transparente para as camadas superiores.

O HoA é constituído por um prefixo válido no *link* da sua rede original (*home network*). É através deste endereço que um nó correspondente ou outro nó qualquer comunica com o nó móvel, independentemente de onde este estiver. Quando o nó móvel muda de rede, mantém o HoA e recebe outro endereço, o CoA, constituído por um prefixo válido numa rede visitada. Este endereço é conseguido de forma *statefull*, (através servidor de endereços DHCPv6) ou *stateless* (autoconfigurado com base nos prefixos anunciados pela rede visitada). Desta forma, o MN terá um HoA e um ou mais CoA enquanto se move entre redes.

Para que seja possível saber onde o nó móvel se encontra, deve ser realizada uma associação entre os endereços HoA e CoA (*binding*). Esta associação do CoA é realizada pelo nó móvel, no HA. Esta associação é realizada através de um *binding registration*, onde o MN envia mensagens de *Binding Update* (BU) para o HA, que responde com uma mensagem *Binding Acknowledgement* (BAck).

Os nós correspondentes (CNs) no MIPv6 possuem capacidade para a optimização de rotas, ou seja, eles podem armazenar *bindings* entre HoA e CoA de nós móveis. Sendo assim, um nó móvel pode fornecer informações sobre sua localização para CNs, através do *correspondent binding procedure*. Neste procedimento é realizado um mecanismo de autorização de estabelecimento de *binding*, chamado de *return routability procedure*.

A figura 14 mostra um cenário de mobilidade IPv6 típico com os elementos básicos.

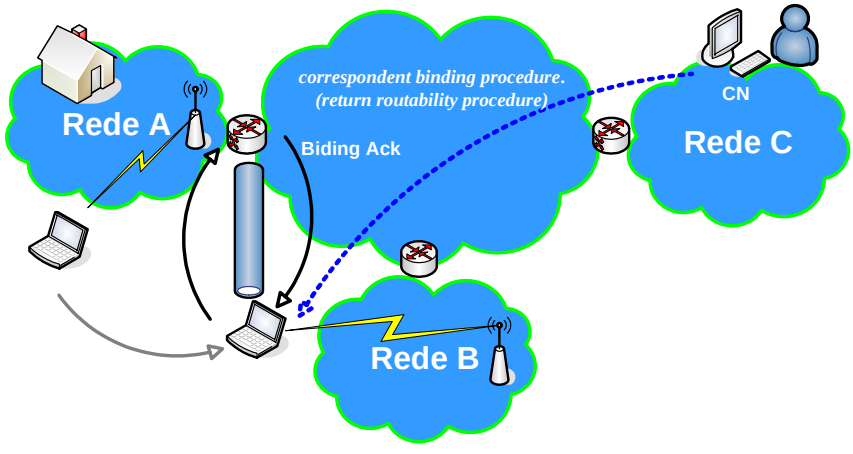


figura 14 - Visão geral do MIPv6

Conforme se ilustra na figura 14, o *Foreign Agent* (FA), presente no MIPv4 não existe, e a comunicação entre o MN e o CN pode ocorrer de dois modos distintos:

- Através do Home Agent: não requer que o CN tenha suporte ao MIPv6 e que o MN se tenha registrado com o CN. È usado um túnel bidireccional estabelecido préviamente entre o HA e o MN. Os pacotes são encaminhados normalmente do CN para o HA e do HA são enviados por túnel para o MN. Depois, o MN responde para o HA pelo túnel que, por sua vez, responde para o CN. Cada pacote interceptado é enviado por túnel para o CoA do MN (este é o modo de funcionamento no MIPv4);
- Optimização de rota: neste caso o CN deve ter suporte de MIPv6 ("inteligência" para realizar o *binding*) e o MN deve-se registar com o CN. Neste caso, o CN, antes de enviar o pacote, procura na *cache* uma associação entre o HoA e o CoA do MN, que permita o encaminhamento directo para o CoA do nó móvel. Desta forma elimina-se congestionamento na rede origem e no HA.

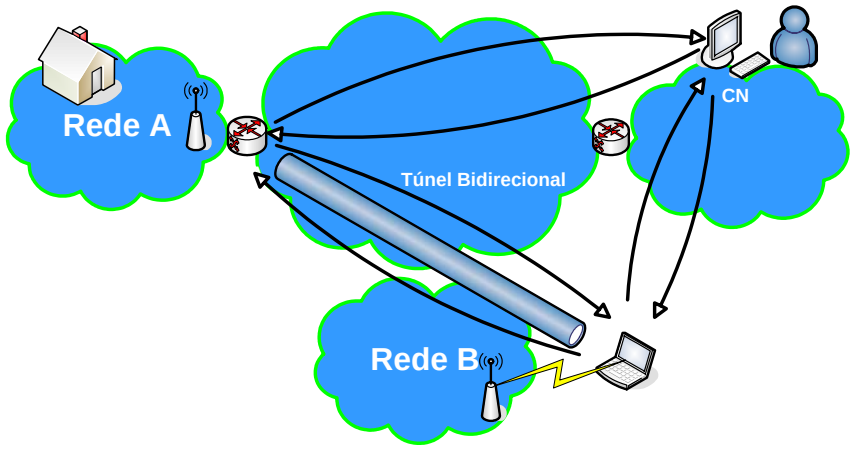


figura 15 - Modos de comunicação entre MN e CN

O MIPv6 apresenta significativas vantagens face ao seu homólogo IPv4. Contudo, o MIPv6 apenas foi (originalmente) preparado para resolver os problemas de MacroMobilidade, uma vez que introduz ainda demasiado *overhead* em ambientes de mobilidade rápida (mM). Em cenários onde o nó móvel muda frequentemente de ponto de acesso à rede, este problema é particularmente relevante. A utilização de ambientes de mM onde é necessário lidar com requisitos de QoS (por exemplo em aplicações de tempo-real) levou ao aparecimento de várias propostas para acelerar os procedimentos associados à mudança de ponto de ligação à rede, característicos dos protocolos MIP.

4.5 Serviços de rede com MIPv6

O MIPv6 actua exclusivamente na camada de rede, e é totalmente transparente para os protocolos das camadas superiores e independente das camadas inferiores. Existem em especificação algumas

extensões que serão dependentes do protocolo das camadas inferiores, nomeadamente o *draft* "Mobile IPv6 Fast *Handovers* for 802.11 Networks" [33].

Também ao nível dos serviços, o funcionamento dos serviços ditos normais das redes de comunicações (DNS, DHCP, Proxy,...), não são directamente afectados pelo MIPv6. Em termos de configurações tudo se mantêm, uma vez que o MIPv6 é transparente para estes.

A mobilidade de um terminal é transparente para todos os terminais da sua rede com excepção do HA. É igualmente transparente para toda a rede visitada e para os nós correspondentes (CNs), porém neste ultimo caso existe a possível perda de performance.

Para numa rede ser disponibilizado o serviço de mobilidade aos seus terminais, basta que estes suportem o serviço e que haja um ou mais HAs, dependendo da rede em questão e/ou do numero de utilizadores. Os HAs poderão ser ou não máquinas dedicadas, porém não deverá ser o *gateway* para não haver sobrecarga de processamento deste. Além disso, há que pensar nas questões da segurança, na hora de escolher a máquina e a sua localização, uma vez que o HA contém informação sensível e poderá ser uma porta de entrada para a rede.

4.6 Configuração Stateless e Statefull

Existem duas possíveis formas de um terminal obter um endereço: usando um mecanismo *stateless* [12] (sem estado, as máquinas configuram o seu endereço com base no prefixo recebido nas mensagens RouterAdvertisements (RAs) e asseguram que é único), *statefull* (por DHCPv6). Também poderão ser usados os processos de autoconfiguração ou a configuração manual do endereço.

Apesar de serem mecanismos necessários ao funcionamento do MIPv6, o funcionamento destes processos é independente do MIPv6, ou seja, o processo é igual para máquinas que não usam MIPv6.

4.7 Configuração dos Router Advertisements

Quando os terminais móveis são configurados para configuração de endereço via *stateless* existem algumas configurações a realizar nos routers que enviam Router Advertisements (RAs), nas redes origem e visitadas. Algumas destas configurações são apontadas de seguida:

- Redução dos valores máximo e mínimo do período de envio de RAs;

  Quanto menor for o intervalo de envio dos RAs maior é a probabilidade de o MN detectar o movimento mais rapidamente e realizar o processo de mobilidade.

- O HA deverá enviar RA com a flag HomeAgentFlag e Info activas;

  A primeira flag é para indicar no RA que ele é um Home Agent, e a segunda é para incluir a *Home Agent Information Option* especificada pelo MIPv6.

- Deverá ser enviado o endereço do HA e não apenas o prefixo de rede.

No seu processo de configuração o MIPv6 requer o endereço da interface e não apenas o prefixo de rede.

Existem outras configurações que poderão ser realizadas, em função da rede ou do que se pretende na rede, quer para o seu correcto funcionamento, quer para optimizar o processo de mobilidade.

Home Agent	Router na rede visitada

interface eth0
{
AdvSendAdvert on;
AdvIntervalOpt on;
MinRtrAdvInterval 0.05;
MaxRtrAdvInterval 1.5;
AdvHomeAgentFlag on;
 	
HomeAgentLifetime 10000;
HomeAgentPreference 20;
AdvHomeAgentInfo on;
 	
prefix 2000:a::/64
{
AdvOnLink on;
AdvAutonomous on;
AdvRouterAddr on;
AdvPreferredLifetime 500;
AdvValidLifetime 600;
};
};
	interface eth1
	{
	AdvSendAdvert on;
	AdvIntervalOpt on;
	
	MinRtrAdvInterval 3;
	MaxRtrAdvInterval 4;
	
	AdvHomeAgentFlag off;
	
	prefix 2000:c::/64
	{
	AdvOnLink on;
	AdvAutonomous on;
	AdvRouterAddr on;
	};
	
	};

tabela 1 - Exemplo de uma possível configuração dos RAs em Linux.

A tabela 1 apresenta o exemplo de um ficheiro de configuração dos RAs num Home Agent e numa outra máquina de uma rede visitada. Como já referido existem muitas outras variáveis de configurações que poderão ser usadas para melhorar o desempenho dos processos da rede.

4.8 Configuração do MIPv6

A configuração do MIPv6, bem como dos endereços e RAs, será objecto de estudo em capítulos futuros. Pode-se adiantar no entanto que dependendo do sistema operativo, existirá maior ou menor flexibilidade de configuração. Por exemplo, em Windows ou IOS, as configurações serão limitadas ao essencial enquanto que em Linux ou Unix, será possível um maior leque de opções.

Existem opções de configuração comuns para os diversos agentes do MIPv6 (CN, HA e MN), bem como opções distintas específicas do papel desempenhado. De notar que um terminal apenas poderá acumular uma das funções do MIPv6, CN ou HA ou MN, e nunca acumular estas funções.

A tabela 2 apresenta um exemplo de configuração para os ficheiros num CN, HA e MN.

MN	HA	CN

NodeConfig MN;
 	
DoRouteOptimizationCN enabled;
 	
Interface "eth1";
 	
UseMnHaIPsec disabled;
 	
SendMobPfxSols enabled;
 	
DoRouteOptimizationMN enabled;
 	
MnHomeLink "eth1" {
HomeAddress 2000:a::20/64;
HomeAgentAddress 2000:a::10;
 	
}
	NodeConfig HA;
	
	DebugLevel 10;
	
	DoRouteOptimizationCN enabled;
	
	Interface "eth0";
	
	UseMnHaIPsec disabled;
		NodeConfig CN;
		
		DebugLevel 10;
		
		DoRouteOptimizationCN enabled;

tabela 2 - Exemplo de uma possível configuração dos ficheiros MIPv6 para Linux.

As configurações apresentadas são apenas um exemplo. Existem outras variáveis de configuração que poderão ser usadas para optimizar o processo de mobilidade.

4.9 Micromobilidade IPv6

O MIPv6 só recentemente se tornou standard, através da RFC 3775 [19], não existindo por esse motivo muitas implementações. Por o MIPv6 ainda ser muito recente e por ser uma prioridade, não existem muitos desenvolvimentos maduros e estáveis na área de microMobilidade (mM) em IPv6. No entanto a mM será extremamente importante, não só pelo registo no HA, como já acontecia em IPv4, mas agora assume uma importância acrescida no *return routability procedure* (registos nos CNs).

De seguida serão apresentados os seguintes protocolos de mM:

- CIPv6 – Cellular IPv6 [34],
- HAWAII [29],
- TIMIP - Terminal Independent Mobility for IP [31],

Extensões do MIPv6 para suporte de mM:

- HMIPv6 – Hierarchical Mobile IPv6 [23],
- FastHandovers MIPv6 [22],
- Mobile IPv6 Fast *Handovers* for 802.11 Networks [33].

4.9.1 CIPv6

O CIPv6 encontra-se definido no *draft* "Cellular IPv6" [34]. Este protocolo fornece mobilidade e suporte de *handoff* para terminais de frequência elevada de movimentos. È indicado para uso a nível local, por exemplo um campus ou uma área metropolitana. Pode interagir com o MIPv6 para suporte de mobilidade global (WAN *mobility*), possibilitando a mobilidade entre domínios CIPv6. É um processo complementar mas transparente par o mipv6.

O seu funcionamento assenta nos princípios do CIPv4 descrito no capítulo anterior.

Em http://cipv6.intranet.gr [83] encontra-se disponível o código fonte e documentação da implementação, não actualizados há bastante tempo e por isso tendencialmente obsoletos.

4.9.2 HAWAII

Os *drafts* do "*Handoff-Aware Wireless Access Internet Infrastrucuture"* (HAWAII) [29], foram concebidos para o Mobile IP na sua versão 4, mas uma vez que este protocolo pretende fornecer uma solução de mM transparente para o MIP, seria facilmente adaptável ao MIPv6. Os seus princípios de funcionamento, mesmo na sua versão MIPv4, poderão ser aproveitados em favorecimento do MIPv6.

4.9.3 TIMIP

Tal como o HAWAII [29], o TIMIP [31] também se encontra apenas definido na perspectiva de uso em complemento ao MIPv4.

4.9.4 HMIPv6

O "*Hierarchical Mobile IPv6 Mobility Management"* (HMIPv6) definido no RFC 4110 [23], ainda em fase experimental, consiste num conjunto de extensões ao MIPv6 e ao IPv6 *Neighbor Discovery* para permitir reduzir a quantidade de sinalização entre o MN e os seus CNs e com o seu HA. A gestão de mobilidade hierárquica realizada pelo HMIPv6 também é usada para aumentar o desempenho em termos de velocidade de *handover*. O funcionamento também assenta os seus princípios no HMIPv4 apresentado no capítulo anterior.

4.9.5 FMIPv6 – FastHandover Mobility IPv6

O FMIPv6 encontra-se definido na RFC 4068 "Fast *Handovers* for Mobile IPv6" [22], e consiste num conjunto de extensões ao MIPv6.

Durante o *handover* do MIPv6 existe um período em que o terminal fica incontactável, devido aos atrasos da mudança de *link* e procedimentos associados ao MIPv6 (detecção de movimento, configuração do CoA e *binding update*). O FMIPv6 pretende reduzir o tempo associado aos atrasos devido aos procedimentos do MIPv6. Porem não resolve o problema de comutação do *link*.

4.9.6 Mobile IPv6 Fast *Handovers* for 802.11 Networks

O "Mobile IPv6 Fast *Handovers* for 802.11 Networks" (FMIPv6802.11) [33] consiste em extensões ao MIPv6 e pretende fornecer uma solução de mM, certamente mais eficaz que as duas anteriores, mas com a desvantagem de estar dependente da tecnologia L2 que terá de ser 802.11. No entanto atendendo ao facto da grande popularidade das redes 802.11, e visto ser a tecnologia wireless L2 predominante, justificasse plenamente a especificação destas novas extensões.

4.9.7 Nemo –Network Mobility

As redes da próxima geração baseiam-se num novo paradigma "*all-IP*", em que existe uma total integração de tecnologias ao redor do protocolo IP. Neste contexto, a interligação das redes fixas com redes "auto-ad-hoc" assume uma particular importância. Este tipo de redes tem diversos cenários de aplicação, que vão desde os transportes, até à saúde, passando pelo simples entretenimento. Um dos problemas complexos que se coloca nestes domínios é a forma como se processa a comunicação entre a rede móvel e a rede fixa

O Grupo de Trabalho "nemo" (Network Mobility) [85], do IETF, especifica no RFC 3963 "Network Mobility (NEMO) Basic Support Protocol" [21], cujo estado actual é "Standards Track", uma proposta para mobilidade de redes, baseado num conjunto de extensões ao MIPv6. A RFC 3963 [21] descreve o protocolo de suporte básico de mobilidade de redes (NEMO), que permite a ligação de redes móveis a diferentes pontos da Internet.

O protocolo é uma extensão ao MIPv6, e permite a continuação das sessões para cada nó da rede móvel, enquanto esta (a rede) se move. Também permite que cada nó da rede móvel se mantenha contactável enquanto se move na rede. Ou seja, a rede move-se, e os terminais nessa rede também se movem, mantendo-se permanentemente contactáveis.

O *router* móvel, que liga a rede à Internet, corre o protocolo de suporte básico Nemo, assim como o seu *Home Agent*. O protocolo é concebido de modo à mobilidade de rede ser transparente para os nós dentro da rede.

Para dar um exemplo da aplicabilidade desta tecnologia, supondo que no futuro cada carro, autocarro, avião, (...), possui uma rede de dados. Essa rede move-se constantemente, bem como os terminais associados a essa rede. Com o MIPv6 e o nemo é possível estarem sempre alcançaveis.

4.9.8 Segurança no MIPv6

Vários dos problemas existentes no MIPv4 simplesmente não existem em MIPv6. A mobilidade em IPv6 não oferece problemas para a "*ingress filtering*", implementada em *firewalls* e *routers*. Tal acontece porque um MN usa sempre o seu *CoA*, obtido por autoconfiguração *stateful* ou *stateless*, na comunicação com nós correspondentes. O NAT, que é basicamente um mecanismo usado para amortizar os efeitos do limitado espaço de endereçamento em IPv4, não é mais necessário em redes IPv6. Portanto, problemas com NAT são exclusivos da versão actual do protocolo IP. Confidencialidade e integridade de dados podem ser implementadas usando o protocolo IPSec, imperativo no IPv6. Além disto, o IPv6 básico tenta resolver outros problemas de segurança existentes em IPv4, sendo mais adequado para a actual realidade encontrada na Internet.

No MIPv6, o HA faz uso do protocolo *Neighbor Discovery* (ND), implementado por mensagens ICMPv6, para fazer o mapeamento entre os endereços MAC e endereços IPv6, abolindo a necessidade do ARP, usado no IPv4 para essa função.

É possível implementar, segundo uma especificação própria, um esquema de autenticação para mensagens do protocolo, usando IPSec e chaves secretas manualmente configuradas. Em contrapartida, isto vai de encontro a uma das principais vantagens do IPv6 em relação ao IPv4: a existência de mecanismos de autoconfiguração, onde nenhuma intervenção do administrador é necessária para configurar os nós na rede.

Quanto à adopção de esquemas de autenticação, para tornar mais seguro o processo de *binding update*, o protocolo IPSec nativo no IPv6 pode ser usado sem problemas. Para as mensagens de registo no HA, a autenticação pode ser realizada usando o protocolo AH do IPSec, desde que seja possível ter um relacionamento prévio de segurança entre o MN e o HA. Isto significa que, por exemplo, uma chave secreta pode ser previamente configurada por um administrador da rede. Entretanto, o MIPv6 inclui um processo de registo entre o MN e o CN. O CN é um nó que pode estar localizado em qualquer lugar na Internet, sendo impossível criar qualquer relacionamento de segurança entre estas partes, sem um mecanismo global de autenticação automática. O uso de IPSec não pode ser usado neste caso, tendo sido criado um mecanismo designado de "*Return Routability Procedure*". O *Return Routability Procedure* (RRP) envia paralelamente mensagens para ambos os endereços de um MN: *home address* e *care-of address*. Desta forma, o CN é capaz de verificar que o MN pode ser alcançado por dois caminhos distintos. Os pacotes enviados para o *care-of address* seguem directamente para o MN no seu novo ponto de ligação. Já os pacotes enviados para o *home address*, são encaminhados para a sua rede origem e, daí, são transmitidos pelo HA para o MN, através de túnel. Estas duas mensagens também transferem *cookies* distintos, por ambos os caminhos. No nó móvel, uma função calcula um valor usando esses *cookies* e transmite a saída na mensagem de BU para o nó correspondente. O CN, supondo que apenas o MN é capaz de obter os dois *cookies* distintos das mensagens anteriormente

enviadas, recalcula o valor e verifica o resultado contra a saída calculada no nó móvel. Se os valores forem iguais, o MN é autenticado.

Interessa ressaltar que o RRP não é totalmente seguro. Um atacante, adequadamente localizado, pode capturar ambas as mensagens enviadas pelo CN com as informações secretas, e realizar o mesmo cálculo que o MN. Isto permitiria que mensagens de BU forjadas fossem criadas. Porém, se um atacante pode capturar tais mensagens, ele também pode implementar ataques similares contra o protocolo IPv6 sem mobilidade, através da sua privilegiada posição na rede. Logo, o RRP e o MIPv6 não introduzem riscos adicionais ao protocolo IPv6.

4.10 Conclusão

O MIPv6 apresenta melhorias significativas em relação ao MIPv4, a maioria das quais derivadas do uso do protocolo IPv6. Muitos dos problemas do IPv4 deixam de existir no IPv6, e isso é benéfico para todos os outros protocolos em IPv6. Em termos funcionais a optimização de rotas e a inexistência do FA são a maior diferença no MIPv6.

Em termos de mM (grupo de trabalho “mipshop”), os vários protocolos propostos (CIP, HAWAII e TIMIP) não foram muito bem aceites e por isso não chegaram sequer a ser normalizados. Dos três referidos, o CIP foi o único a ser especificado sob a forma de *draft* para IPv6. Uma das razões da não afirmação destes poderá ser a sua dependência em relação a mecanismos dos protocolos de ligação, no caso do CIP e HAWAII. O TIMIP não tinha esta restrição mas também não teve muito sucesso. A razão mais lógica é o facto de os grupos de trabalho perceberem que, usando estes protocolos, estariam a recorrer a dois meios para um mesmo fim, ou seja, usar o MIPv6 com um destes protocolos para se ter mobilidade com *handovers* suaves.

No entanto todo o trabalho aplicado nestes protocolos não foi em vão, uma vez que, usando os princípios de funcionamento destes, foi possível evoluir no sentido de desenvolver extensões ao protocolo MIPv6, de modo a obter os mesmos fins com o mesmo protocolo. O HMIPv6 e o FMIPv6 surgiram com o intuito de optimizar o processo do MIPv6 associado aos *handovers* em ambientes de mM. Com estas extensões a solução completa de mobilidade global concentra-se num único protocolo, o MIPv6.

NEMO é o nome do grupo de trabalho e do protocolo definido na RFC3963. Ambos são relativamente recentes, mas apesar de apenas existir uma RFC neste grupo de trabalho, existem já 9 *drafts* em especificação, o que mostra o desenvolvimento recente nas especificações. Trata-se de mais um conjunto de extensões ao MIPv6, ou seja, um complemento e acrescento de funcionalidade ao MIPv6.

Em termos de segurança o MIPv6 não introduz vulnerabilidades significativas ao IPv6, mas esta é agora um dos focos de principal interesse nas especificações. O grupo de trabalho do IETF “mip6”

encontra-se actualmente a desenvolver protocolos que pretendem fornecer capacidades de gestão e segurança ao MIPv6.

Conforme o IPv6 integra as versões dos principais sistemas operativos (e.g. Windows, IOS, Linux, UNIX,…) no futuro também o MIPv6 virá. Então, num futuro IPv6 a mobilidade será transparente para os utilizadores. Com todas as extensões que foram desenvolvidas e estão ainda a ser desenvolvidas, o MIPv6 será uma solução de mobilidade completa, segura e fiável.

5. Normalização e implementações MIPv6

Neste capítulo é apresentado o estado da arte no domínio da mobilidade, nomeadamente os últimos avanços realizados pelo IETF, através dos seus grupos de trabalho.

Posteriormente são apresentadas algumas implementações desenvolvidas para suporte de mobilidade em IPv6 e para as várias extensões que começam a surgir.

5.1 Normalização

O IETF possui actualmente vários grupos de trabalho [80] em diferentes áreas. Na área da Internet, que é a que interessa para este trabalho encontram-se alguns grupos que trabalham mais especificamente com a mobilidade. Destes pode-se destacar o “mip4” (mobilidade em ipv4), o “mip6” (mobilidade em ipv6), o “nemo” (mobilidade de redes ipv6) e o “mipshop” (optimização de *handoffs* e sinalização na mobilidade ipv6).

Pela análise dos grupos apresentados, pode-se constatar que em termos de mobilidade existe maior interesse no IPv6. Algumas razões que poderão ser apontadas, é o facto de ser mais fácil implementar mobilidade em ipv6, é mais fácil implementar segurança na mobilidade, entre outras vantagens do IPv6.

Quem desenvolve estes trabalhos de especificação também percebe facilmente que ainda existem muitas especificações e implementações a fazer. Ou seja, vai demorar algum tempo até que estas estabilizem e atinjam um nível aceitável para se avançar para o mercado, e atingir um elevado nível de adesão. Este período de tempo poderá ser suficiente para que o IPv6 se imponha ao IPv4, e aí todos os trabalhos de especificação seriam quase despropositados. A ideia de fazer um projecto de mobilidade à escala mundial com o IPv4, dadas as suas limitações, a escassez de endereços, a falta de segurança, entre outros factores, prevê-se uma tarefa difícil.

Quanto ao MIPv6, mais concretamente, os esforços do grupo “mip6” concentram-se agora em especificar optimizações do modelo e implementação de segurança e mecanismos de gestão.

Os grupos “mipshop” e “nemo” implementam extensões ao mipv6 para fornecer optimização de *handoffs* e mobilidade de rede respectivamente.

5.2 Implementações MIPv6

Quanto a implementações práticas, existem inúmeras relacionadas com a mobilidade, quer seja IPv4 ou IPv6. Neste secção são enunciadas apenas algumas relacionadas com o MIPv6 em função do sistema operativo para o qual foram concebidas.

5.2.1 Windows

Quando colocada a questão se o protocolo IPv6 para o Windows suporta MIPv6, existem várias respostas que se podem encontrar na *web*. Alguns indicam nesse sentido, outras são contraditórias e outras defendem que apenas existe suporte para a funcionalidade de *Correspondent Node* (CN).

Ao verificar as configurações do IPv6 (na linha de comando ”ipv6 install”, “interface ipv6”), verificamos que já existe suporte de mobilidade (“show mobility”). Contudo apenas é possível configurar a funcionalidade de CN, e segundo o especificado no já obsoleto *draft* 13 do MIPv6 [25].

Segundo informação disponibilizada no sítio oficial da Microsoft, o grupo de pesquisa (Microsoft Research), já desenvolveu uma aplicação com suporte da totalidade das funcionalidades do MIPv6. A aplicação esteve em tempos disponível ao público para testes (Mobile IPv6 Technology Preview), mas já não está mais disponível. A Microsoft pondera disponibilizar uma versão para o novo Windows Vista.

5.2.2 IOS

A partir da versão 12.3(14)T, o IOS da Cisco passou a incluir suporte de mobilidade IPv6 mas apenas para a funcionalidade de Home Agent. Assim, não existe por enquanto suporte da funcionalidade de MN. Além disso, o uso de IPSec para proteger as comunicações entre o MN, HA e CNs, especificado no RFC 3776 também ainda não foi implementado.

5.2.3 Linux

No que diz respeito a implementações de MIPv6 em Linux (MIPL), a Universidade de Lancaster no Reino Unido desenvolveu a primeira implementação, já obsoleta, desenvolvida para o Kernel 2.1.90, de acordo com o especificado no draft 5 do IETF de Mobilidade em IPv6 (o actual RFC 3775).

Outra implementação do MIPL, é a “Helsinki University of Technology's MIPL Project”, desenvolvida pelo grupo de trabalho GO-Core, actualizada periodicamente. O último *kernel* suportado é o 2.6.11 (ultima actualização do software em 31-10-2005).

A partir da versão 2.0 do MIPL o desenvolvimento foi em co-operação com o USAGI/WIDE Project [87][88]. Em colaboração desenvolveram extensões para a pilha IPv6 do Linux de modo a suportar MIPv6, com o objectivo de ver estas extensões aceitas na linha principal do *kernel*.

Em http://www.mobile-ipv6.org/, encontra-se disponível o *patch* e as user space tools, bem como documentação, *links*, e uma Mailing List bastante solicitada, com o respectivo arquivo.

Este grupo de trabalho desenvolveu também uma implementação da Plataforma NEMO para Linux (NEPL) em co-operação com o Nautilus6/WIDE Project [77] [88].

5.2.4 Unix - BSD

SHISA [86] é uma implementação de MIPv6 e NEMO em BSD. O SHISA resultou da junção de dois projectos distintos, o KAMEMIP [89] desenvolvido pelo KAME [78], e o SFCMIP [91] desenvolvido pelo projecto InternetCAR [92]. Suporta as funcionalidades de *Mobile Node*, *Home Agent* e *Correspondent Node*, bem como várias extensões tais como as do *NEMO Basic Support* e *Multiple Care-of-Address Registration*.

5.3 Implementações de extensões do MIPv6

Existem já especificadas várias extensões ao protocolo MIPv6, algumas das quais já implementadas, normalmente em Linux e/ou BSD.

5.3.1 NEMO

O NEMO mencionado anteriormente, tem implementações em Linux e BSD. Mais informação pode ser encontrada em http://www.nautilus6.org/.

5.3.2 HMIPv6

Em http://www.ctie.monash.edu.au/ipv6/, existe uma implementação pública de HMIPv6 para Linux, disponível para testes. Em http://www.tkn.tu-berlin.de/research/hmip/, é possível encontrar outra implementação do HMIPv6 mais antiga.

5.3.3 FMIPv6

A página oficial do FMIPv6 para Linux, http://www.fmipv6.org/, é uma página bastante completa e actualizada. É possível encontrar desde o código fonte até à documentação da *testebed*.

Em http://software.nautilus6.org/TARZAN/, está disponível a implementação de FMIPv6 para BSD.

5.3.4 Outros

O sítio http://www.nautilus6.org/implementation/index.php, contém outras implementações de extensões ao protocolo MIPv6 para Linux e BSD.

5.4 Conclusões

São muitas as implementações existentes relacionadas com a mobilidade. Há várias preocupações actuais nesta área, não só ao nível da especificação como também da implementação. Verifica-se que existem muitos grupos de trabalho, envolvidos em diversos projectos e cooperando entre si para o desenvolvimento das especificações do IETF, com o objectivo de fornecer suporte de MIPv6 para os diversos sistemas operativos. Linux e BSD são o alvo preferencial das equipas de desenvolvimento, por serem os mais populares e existirem no domínio *open source*.

6. Arquitectura de testes

De modo a testar a mobilidade IPv6 foi necessário criar vários cenários de teste com diverso equipamento e software. Neste capítulo é enumerado e descrito o hardware usado, o software (sistemas operativos e programas), e os cenários de teste.

6.1 Cenário Geral

Os cenários configurados para testar o MIPv6 assentam todos numa estrutura semelhante, em que existe um HA e um MN. Este último desloca-se entre a sua rede e uma ou várias outras redes. Existe também um ou vários CNs, que comunicam com o MN. Aqueles podem ou não ser configurados com MIPv6, variando apenas o suporte ou não, respectivamente, de optimização de rotas.

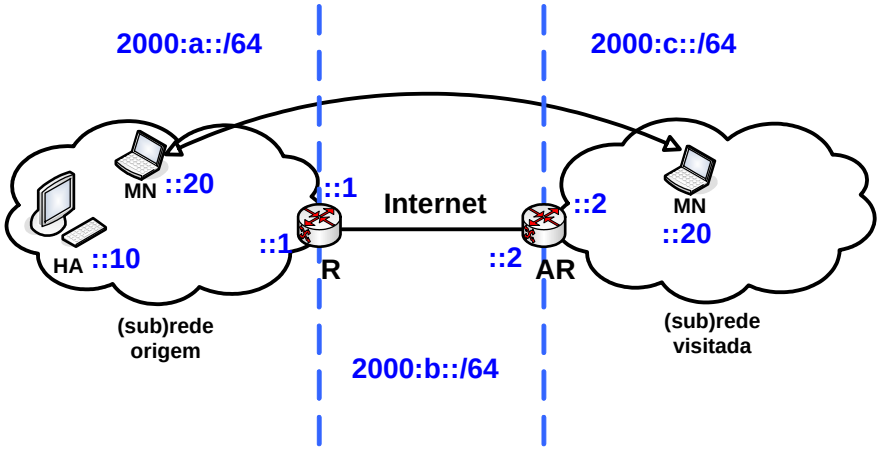


figura 16 - Cenário base dos testes de mipv6.

De referir que a mobilidade IPv6 não implica necessariamente um ambiente wireless. No entanto, usando um cenário com fios, para efectuar a mudança de rede terá de ser através da mudança física do cabo de rede, o que implica quebra da ligação e perda de alguns pacotes. Ainda assim esta topologia permite testar o processo de mobilidade na plenitude.

6.2 Hardware

Esta secção enumera os vários equipamentos usados nos diversos cenários de teste que foram usados, mencionando algumas das características mais importantes, bem como justificações de uso.

Assim o hardware usado foi o seguinte:

- PCs (Intel(R) Pentium(R) 4, CPU 3.00GHz, 496MB de RAM)

- Hubs Cisco 1538M
- Routers Cisco 2600 Series (Cisco 2620XM e Cisco2621XM).
- Access Points Cisco 1200 Series
- Placa PCI Cisco (AIR-PCI352)

6.2.1 PCs

Os PCs usados (Intel(R) Pentium(R) 4, CPU 3.00GHz, 496MB de RAM) foram configurados com os sistemas operativos Windows XP SP2, e o sistema operativo Linux Fedora Core 3. As configurações realizadas e o software instalado serão posteriormente descritos.

6.2.2 Hubs

Os *Hubs* Cisco usados não precisaram de nenhuma configuração em especial.

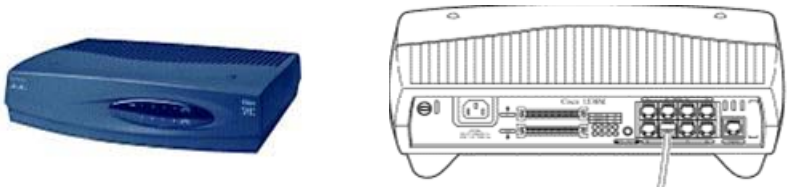


figura 17 - Hubs Cisco 1538M.

6.2.3 Routers Cisco

Os *routers* usados nos vários testes foram os "Cisco 2600 Series", mais concretamente, "Cisco 2620XM" e "Cisco 2621XM".

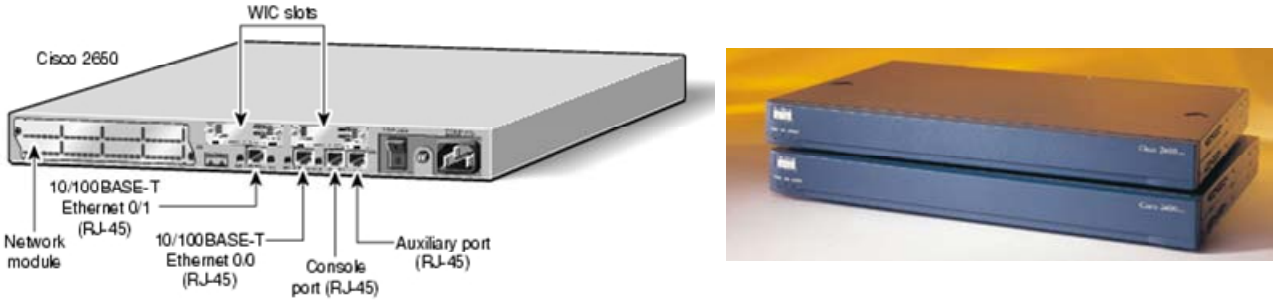


figura 18 - *Router* Cisco 2620XM.

As características mais relevantes são 32Mbytes de flash e 128Mbytes de memória, com a versão do IOS 12.4(5) com suporte para mobilidade IPv6. As configurações realizadas no IOS são descritas posteriormente.

6.2.4 Access Points Cisco

Os APs Cisco da série 1200 podem ser usados para clientes 802.11a(5GHz) e 802.11b/g(2.4GHz). Para isso, possuem módulos de rádio distintos. O módulo 2.4GHz é integrado, e possui duas antenas amovíveis. O módulo de 5GHz, não é integrado e não vem de origem com o AP, sendo adquirido independentemente com antena integrada.

As configurações destes equipamentos serão mencionadas posteriormente quando se justificar.

figura 19 - *Access Points* Cisco 1200 Series.

6.2.5 Placa PCI Cisco

Após instalar a placa no PC é necessário instalar os *drivers* no S.O. de modo a poder funcionar. No FC3 (Linux) é detectado no *boot* o novo *hardaware*, e basta apenas seleccionar a opção de instalar os drivers, e a placa fica operacional. Para o Windows XP têm de se instalar os *drivers* que vêm no CD fornecido na compra da placa.

figura 20 - Placa PCI Cisco (AIR-PCI352).

6.3 Software

Neste ponto é descrito com mais detalhe o suporte de Mobilidade IPv6 para os três sistemas operativos usados neste projecto, mais concretamente o IOS da Cisco (proprietário), o Windows XP SP2 da Microsoft (proprietário) e o Fedora Core 3 da distribuição Linux, variante do Unix (*Open Source*).

6.3.1 IOS Cisco

A Cisco detém mais de 80% do mercado mundial das redes, por isso é óbvio que nos testes se utilize equipamentos Cisco e o seu sistema operativo, o IOS.

A versão original do IOS existente nos *routers* Cisco (12.3(13)), não suportava a funcionalidade de mobilidade IPv6, pelo que teve de ser realizado uma actualização a esta. A tabela seguinte mostra as versões mínimas requeridas para suporte de mobilidade IPv6.

Feature	*Minimum Required Cisco IOS Release by Release Train*
Mobile IPv6 home agent	12.3(14)T, 12.4, 12.4(2)T
IPv6 ACL enhancements	12.4(2)T

tabela 3 - Versões mínimas de IOS com suporte para Mobilidade IPv6.

A versão do IOS foi escolhida em função dos seus requisitos mínimos de memória e flash, que não poderiam exceder os 32Mbytes de flash e 128Mbytes de memória dos *routers* existentes no laboratório.

6.3.1.1 Restrições

A versão 12.4(5), à data da realização dos cenários, era a versão de IOS mais recente e ainda não suportava IPSec para a mobilidade IPv6. Será então necessário aguardar por futuras versões do IOS para que haja inclusão desta funcionalidade descrita na RFC 3776.

Outra das restrições é que apenas existe suporte para as funcionalidades de HA e CN. Não se justifica muito por enquanto ter um *router* a fazer de MN. No futuro poderá fazer sentido um *router* com funcionalidades de MN, por exemplo, com a inclusão do conceito de *Network Mobility* (NEMO), cujos princípios de funcionamento assentam em extensões ao MIPv6, em que o *router* será uma unidade móvel.

Quanto ao processo de optimização de rotas, esse sim já é suportado.

Notas:

- A RFC 3776, (“Using IPSec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”) [20], ainda não é suportado pelas publicações actuais do IOS.
- A implementação de mobilidade IPv6 no IOS da Cisco apenas possui suporte para as funcionalidades de *Home Agent* (HA) e *Correspondent Node* (CN).

6.3.1.2 Configuração do mipv6

A configuração de mobilidade ipv6 no IOS é simples e resume-se a um comando na interface:

```
Router(config-if)# ipv6 mobile home-agent
```

De referir, que como é óbvio, é necessário activar também no *router* IPv6.

Outros comandos relativos ao funcionamento do mipv6,poderão ser usados, nomeadamente para as funções de:

- Activar o mipv6 no *router*
- Configurar a informação de *binding* para o mipv6
- Filtrar os cabeçalhos do protocolo mipv6 e respectivas opções
- Controlar as mensagens “ICMP Unreachable”
- Optimizar o mipv6 nas *interfaces*
- Monitorizar e gerir o mipv6 nos *routers*

6.3.2 Microsoft Windows XP SP2

O Windows é o sistema operativo mais usado em todo o mundo, por isso é óbvio que teve de ser ponderada a sua utilização nos testes. Foi usado o Windows XP SP2 Professional.

Foi necessário pesquisar se o protocolo IPv6 para Windows possui suporte para Mocilidade IPv6. Algumas informações contraditórias foram encontradas. Algumas indicavam que o Windows fornece suporte para a funcionalidade de Correspondent Node (CN), segundo o especificado no já obsoleto draft 13 com o titulo de "Mobility Support in IPv6" (a actual RFC 3775) [25]. No entanto sem suporte para das funcionalidades de Home Agent e Mobile Node. Por defeito a funcionalidade de CN está desactivada e os “*bindings updates*” requerem o uso de IPsec Authentication Header (AH) para autenticação. Para activar a funcionalidade de CN usa-se o commando “netsh interface ipv6 set mobility correspondentnode=enabled”.

Outras informações indicam que o grupo de pesquisa da Microsoft desenvolveu uma aplicação com suporte das funcionalidades de HA, MN e CN.

De facto ambas as informações estão correctas, uma vez que a aplicação desenvolvida não se encontra disponivel actualmente para o Windows XP. A Microsoft considera disponibilizar uma versão para uso no novo Windows Vista, após este ser oficialmente lançado.

6.3.2.1 Restrições

Como referido no ponto anterior, as versões correntes do Windows apenas possuem suporte para as funções de Correspondente Node (CN). Não é então possível configurar um MN ou um HA. Esteve disponível uma aplicação, para experimentação da tecnologia mipv6, que fornecia capacidade de suporte para todas as funcionalidades do MIPv6. Esta aplicação não se encontra mais disponível, e aguarda-se pela saída do novo Windows Vista, após a qual poderá ser lançada uma nova versão para este sistema operativo.

6.3.2.2 Configuração do mipv6

A configuração da mobilidade no Windows é através da linha de comando (Iniciar>Executar>cmd), na net shell (comando “netsh”), no contexto interface ipv6 (comando “interface ipv6”).

Para visualizar as opções de mobilidade configuradas, antes de avançar com qualquer configuração, é usado o comando “show mobility”.

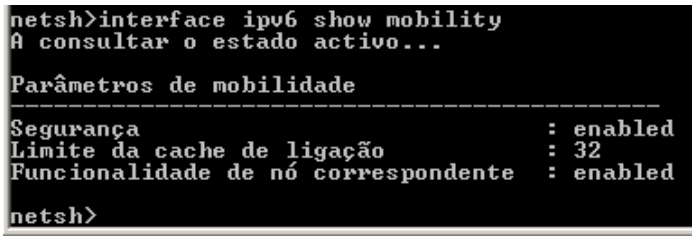


figura 21 - *Output* do comando “show mobility”.

Para alterar as configurações é necessário saber as opções disponíveis. Para isso usa-se o comando “set mobility ?”:

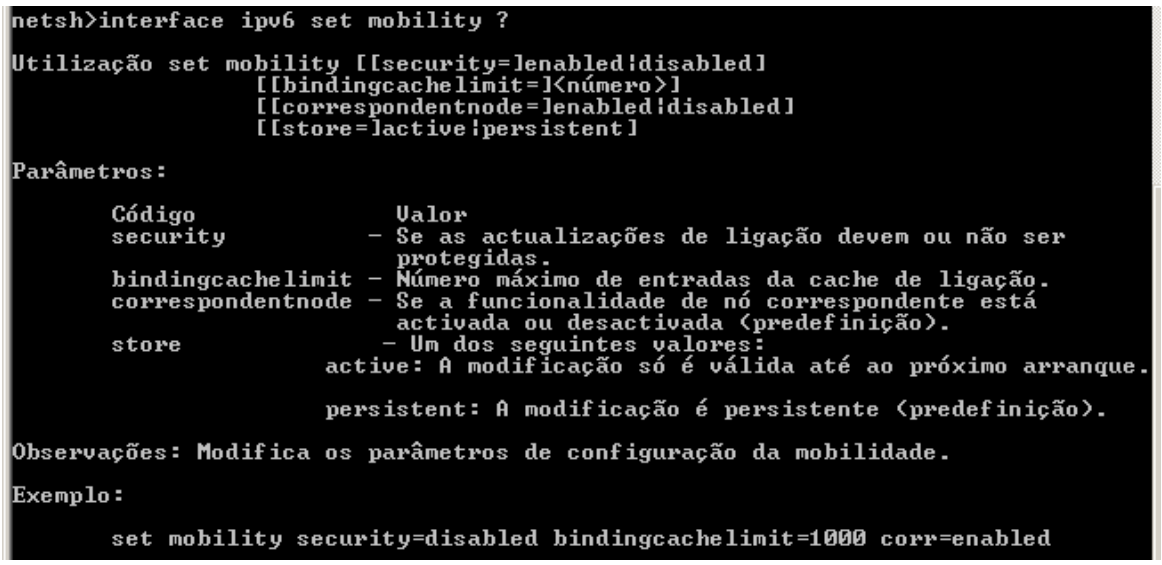


figura 22 - *Output* do comando "set mobility ?".

A configuração usada nos cenários deste projecto foi a seguinte:

set mobility bindingcachelimit=1000 correspondentnode=enabled store=persistent

O parametro bindingcachelimit estabelece o numero máximo de registo que permite guarder num determinado momento. O parametro correspondentnode activa ou desactiva a funcionalidade de CN. O parametro store define o modo de como as configurações do comando são guardadas.

6.3.3 Linux – Fedora Core 3

Actualmente existem mais de 70 variantes de Unix. Alguns exemplos são o LINUX, BSD, SunOS,(…). A vantagem de ter um elevado número de variantes é o poder de escolha, mas por outro lado os problemas de compatibilidade entre elas são uma grande desvantagem.

Existem imensas distribuições de Linux. Algumas das mais conhecidas são o RedHat/Fedora, Debian, Suse, Slackware, Mandrake, Knoppix, Kanotix, Gentoo, (…).

Na maioria dos casos, quando se implementa uma *testebed* opta-se pela variante e distribuição com que se está mais familiarizado. Foi o que aconteceu neste caso (também porque existia uma implementação mipv6 para Linux) em que se optou pela variante Linux na sua distribuição Fedora Core, que evoluiu do antigo Red Hat.

Existem duas implementações de Mobilidade IPv6 para Linux (MIPL) disponíveis.

A Universidade de Lancaster no Reino Unido tem a mais antiga (http://www.cs-ipv6.lancs.ac.uk/MobileIP/). A última implementação foi desenvolvida para o Kernel 2.1.90, de acordo com o especificado no draft 5 do IETF de "*Mobilidade em IPv6*" (a actual RFC 3775 [19]). No entanto a última actualização é de 1998, sendo por isso uma solução a não considerar.

A outra implementação é a da “Helsinki University of Technology's MIPL Project”, que é actualizada periodicamente. O último *kernel* suportado é o 2.6.11 (ultima actualização do software em 09-02-2006).

Como é óbvio, a implementação escolhida para a *testbed*, foi a disponibilizada pela universidade de Helsínquia. Para além de existir já uma familiarização com Linux, derivada da sua grande popularidade, a existência desta implementação também contribui para a sua escolha.

A popularidade foi também o motivo de escolha da distribuição Fedora Core, mas porquê a escolha da sua versão 3 quando a mais recente é a 4?

Contrariamente ao que sucede com o IPv6, o MIPv6 ainda não vem de base no *Kernel*. Então, enquanto se aguarda pela sua inclusão definitiva, que se pensa estar para uma próxima versão, tem de se recorrer à aplicação de um *patch*. No sítio oficial do MIPL [68], encontra-se disponível a aplicação e o *patch* mais recentes, este último para o *kernel* 2.6.11.

O FC4 trás de origem o *kernel* “kernel-2.6.11-1.1369_FC4”, pelo que houve uma tentativa de aplicar o *patch* a este *kernel*, que no fundo é a versão 2.6.11, mas esta mostrou que teria de ser usada a versão “original”. Então após aplicar o *patch* ao *kernel*, e ter sido realizada a respectiva configuração, houve problemas no processo de compilação. Em ultima instância mudou-se a distribuição FC4 para a FC3, e simplesmente os problemas não existiram. Este foi o motivo do uso da distribuição FC3.

A implementação MIPL suporta na integra as funcionalidades definidas no RFC 3775 (MIPv6), incluindo o uso de IPSec no MIPv6 definido no RFC 3776.

Em anexo existe um tutorial que explica detalhadamente o processo de configuração e teste de mobilidade IPv6 em Linux. Neste HOWTO passo-a-passo, estão descritos processos, resumidamente:

- Aplicação do *patch* ao *kernel*,
- Configuração e compilação do *kernel*,
- Instalação da aplicação e configuração dos ficheiros associados,
- Instalação, configuração e testes.

6.3.4 BSD

As variantes BSD do Unix são outras das variantes de maior sucesso. O projecto SHISA apresenta implementações de Mobile IPv6/NEMO para as variantes BSD.

Quanto a restrições e configurações, não são mencionadas aqui, uma vez que neste trabalho esta implementação não foi usada. No entanto segundo as informações disponíveis, esta implementação suporta a funcionalidade completa do MIPv6 e ainda de várias extensões como o suporte básico do “NEMO” e “Support and Multiple Care-of Address Registration”.

6.4 Cenários

Neste Ponto são apresentados e descritos os cenários configurados para testar a mobilidade. Será também dada uma justificação do seu uso e será dada explicado o que se pretende testar e como.

6.4.1 Cenário 1

O primeiro cenário usado consistiu em 4 máquinas Linux e dois hubs, numa topologia inteiramente com fios.

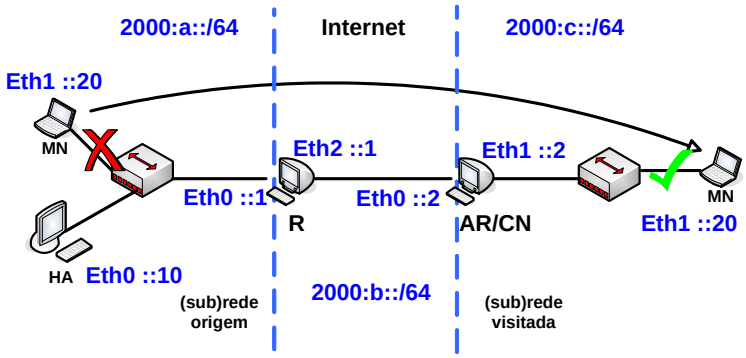


figura 23 - Cenário 1 – 4 máquinas Lina e dois cubas.

Foram configuradas três redes, a rede origem, a rede visitada e outra que pretende simular a Internet. Foram configurados três elementos do MIPv6: o MN, o HA e o CN.

As máquinas HA, AR/CN e R são configuradas com encaminhamento activo. Além disso as duas primeiras também foram configuradas para enviar RAs de modo ao MN conseguir detectar quando se move entre as redes.

Para testar a mobilidade, basta desligar o cabo do MN do interface do Hub da rede origem e ligar no Hub da rede visitada. Para testar o regresso a caso é o processo inverso. Assim, enquanto o MN está na rede origem, toda a comunicação IPv6 funciona normalmente e todas as máquina devem conseguir aceder umas às outras. Por exemplo, pode ser testada a conectividade usando o comando ping6.

Quando o MN se move para a outra rede o HA e o AR/CN devem conseguir fazer a optimização de rota, se esta foi configurada. A máquina R tambem vai comunicar com o MN mas sem MIPv6 configurado, para verificar que neste caso a comunicação é realizada por intermédio do HA.

Após o regresso à rede origem tudo volta a funcionar normalmente.

6.4.2 Cenário 2

No segundo cenário usado, manteve-se o MN mas substituíram-se as outras máquinas Linux por *routers* Cisco. Além disso também se acrescentou um CN configurado numa máquina Windows XP

SP2. Este cenário, apresentado na figura 24, teve como objectivo testar a interoperabilidade entre diferentes implementações do MIPv6.

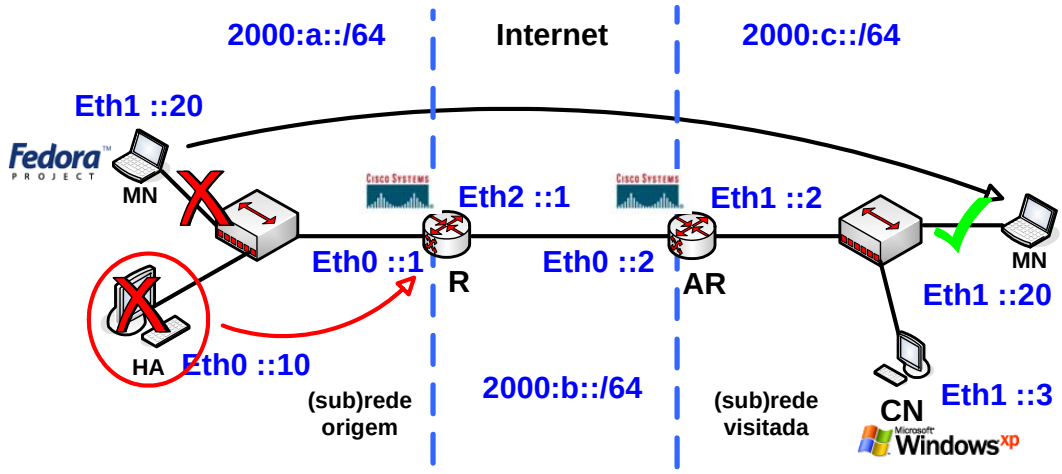


figura 24 - Cenário 2 – máquinas Linux e cisco.

Em Windows apenas é possível configurar a funcionalidade de CN, e uma vez que o IOS da Cisco não suporta as funcionalidades de MN, não houve outra hipótese senão usar o MN configurado em Linux.

Outra das restrições do IOS da Cisco é o facto de não suportar IPSec tal como definido na RFC 3776, logo não foi usado IPsec.

6.4.3 Cenário 3

No terceiro cenário (ver figura 25) adoptou-se a mesma estrutura do cenário 1, no entanto foram colocados dois APs em cada *Hub*, e no MN configurou-se a interface *wireless*, desactivando-se a *ethernet*, para deste modo a comunicação entre o MN e os restantes elementos da rede ser realizada via *wireless*, possibilitando o teste dos "*handovers* suaves".

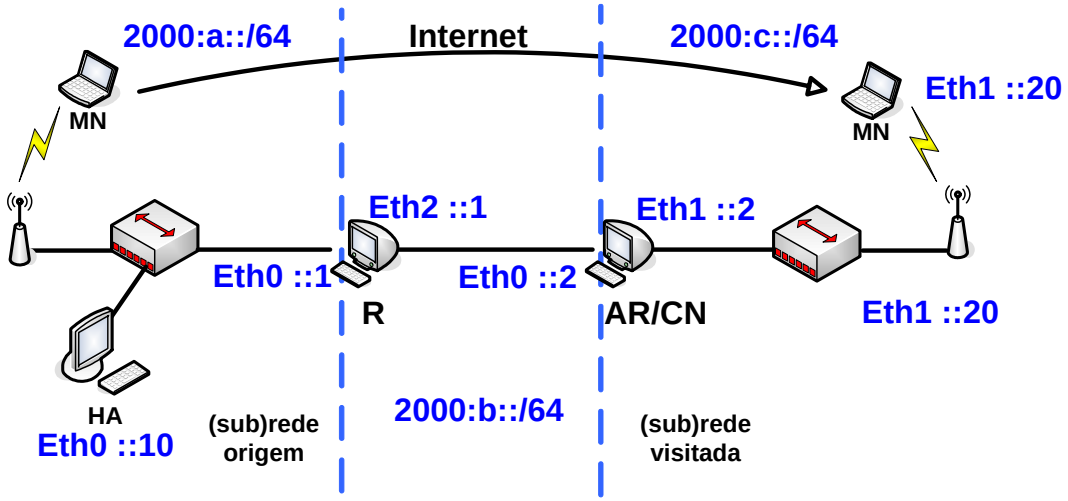


figura 25 - Cenário 2 – máquinas Linux e cisco.

6.5 Aplicações para testar o MIPv6

Várias soluções têm sido apresentadas para testar a mobilidade.

Em http://www.bullopensource.org/mipv6/index.php existe uma aplicação recente, concebida para efeitos de teste do MIPv6. Encontra-se também documentado um plano de testes e procedimentos. A ferramenta usada também se encontra descrita, assim como alguns dos *bugs* detectados na implementação do MIPL. Por fim também são disponibilizados os resultados obtidos nos testes.

Em http://www.cavone.com/mipv6-analyzer/ existe uma aplicação *web* para analizar *Logs* gerados pelo funcionamento do MIPv6 concebida em Itália. A aplicação já não é recente e poderá estar desactualizada.

Aplicações de conversação em tempo real também poderão ser usadas para efeitos de teste. O MN inicia uma chamada de voz e vídeo, e depois move-se entre as redes para verificar a mobilidade. O GnomeMeeting é uma possível aplicação para este efeito com a vantagem que mostra estatísticas da comunicação.

Outro possível teste é usando aplicações que geram tráfego e medem os parâmetros da comunicação, tais como o MGEN e o TRPR.

Outras métodos de verificar a operação da mobilidade são os já existentes no sistema operativo, tais como *ping traceroute*, visualização da tabela de encaminhamento (routing table) e estado das interfaces.

6.5.1 MIPv6 Tester

Em http://www.bullopensource.org/mipv6/tester.php, encontra-se disponível uma aplicação para testar o MIPv6, o MIPv6 Tester. Encontra-se uma versão desenvolvida em Python/PyGTK e outra escrita em C/libcurses

Esta ferramenta é usada para facilmente testar as características da mobilidade. O seu funcionamento consiste em abrir uma ligação bidireccional TCP e duas UDP unidireccionais, entre dois pontos na rede designados de servidor e cliente e servidor (apesar de ambos serem cliente e servidor desempenham apenas uma dessa funções num dado instante). A ferramenta testa a conectividade entre os pontos e regista o tempo de falha (*downtime*) de cada ligação.

A figura seguinte mostra um *screenshot* da janela principal da aplicação e da janela de configuração, para a versão em Python.

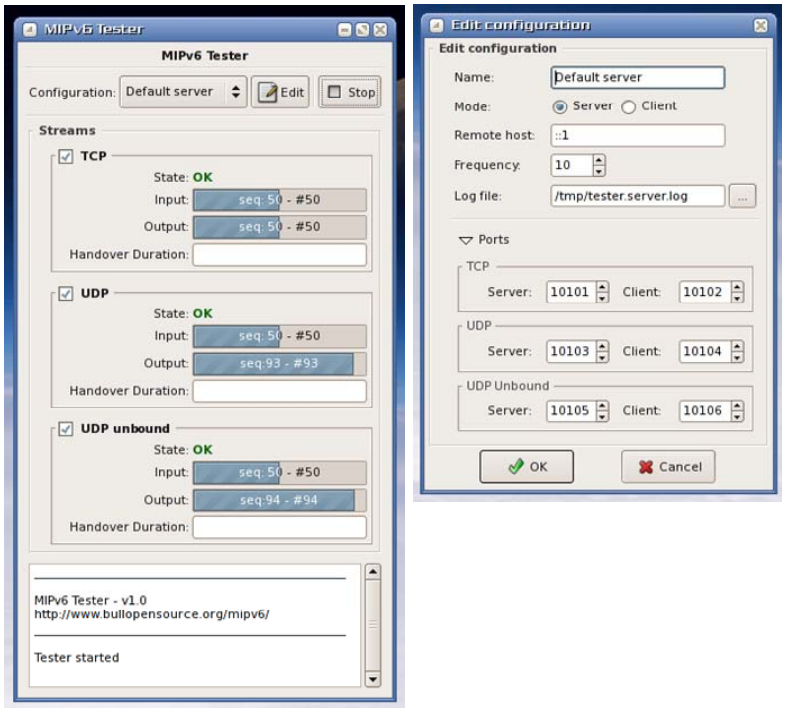


figura 26 - MIPv6 Tester – Interfaces principal e de configuração.

A aplicação depois de terminar gera um ficheiro de *logs* para análise.

6.6 Medição de tráfego

A engenharia de tráfego é usada para optimizar a utilização dos recursos de rede para as exigências do tráfego. Em resumo, consiste em colocar o tráfego onde existe capacidade, ou então, estabelece a capacidade onde o tráfego precisa dela. O tráfego pode ser medido em fluxos, interfaces, *links*, nós, pares de nós e caminhos (túnel ou circuito entre emissor e receptor).

As entidades de medida são o volume de tráfego, tempos médios, largura de banda disponível, *throughput*, atrasos, variações do atraso, pacotes perdidos, utilização dos recursos, entre outras.

Em medições muito extensas são necessários dispositivos de armazenamento de dados, aplicações de processamento destes dados e aplicações para gerar estatísticas e relatórios. Quando se pretende medir um pequeno cenário em laboratório, a própria máquina de medição armazena e processa os dados. É necessário apenas uma aplicação que, usada nessa máquina, consiga processar os dados e gerar os resultados.

6.6.1 Medição das comunicações com MIPv6

Uma vez que serão usados cenários de testes, as medições terão de ser activas. Ou seja, terão de ser estabelecidas ligações e/ou fluxos em que são injectados pacotes para teste da rede. No caso das medições em ambientes reais poderiam ser realizadas apenas medições passivas, analisando apenas o

tráfego gerado pelos utilizadores comuns, não havendo qualquer tráfego gerado para as medições.O volume de tráfego (bits, bytes ou pacotes) é a quantidade de tráfego medido um período de tempo.

As medições de tráfego servem para caracterizar o tráfego e planear a capacidade da rede. Permitem identificar padrões de tráfego, determinar distribuições de tráfego ao nível dos fluxos, interfaces, *links*, nós, pares de nós e *paths*. Permite observar e prever a evolução do tráfego permitindo dimensionar a rede correctamente.

Associado ao MIPv6, tal como a muitos outros protocolos, torna-se útil uma vez que o MIPv6 introduz *overhead* adicional em algumas comunicações, bem como tráfego extra de sinalização.

6.6.2 Ferramentas para medição do tráfego

Existem diversas aplicações para medir e analisar tráfego. O Rude e o Crude (disponíveis em http://rude.sourceforge.net) são ferramentas com esse propósito. O Rude é um pequeno e fléxivel programa que gera tráfego UDP em tempo-real para a rede, e o Crude poderá recolher esse tráfego noutro ponto da rede permitindo a sua análise. Actualmente estes programas apenas suportam medições de tráfego UDP.

O Mgen (Multi-Generator)(http://tang.itd.nrl.navy.mil/5522/mgen/mgen4.html) é um *sotware Open Source* com capacidade de avaliar o desempenho em redes IP com medições de tráfego UDP/IP. O suporte para TCP está actualmente a ser desenvolvido. O TRPR é uma aplicação que permite analisar os dados gerados pelo Mgen.

O Chariot (http://netiq.com) é uma ferramenta mais robusta e com mais capacidades que permite desenvolver tarefas de medição e análise de tráfego. Esta aplicação requer no entanto licença.

Existem instituições que se dedicam á analise do tráfego da Internet. A Caida (http://www.caida.org) recolhe, monitoriza, analiza e visualiza diversas formas de tráfego na Internet.

6.7 Network Simulator

Durante as pesquisas de implementações de teste no Network Simulator [97] para MIPv6 apenas uma foi encontrada, e já algo desactualizada em http://www.inrialpes.fr/planete/pub/mobiwan/.

A aplicação, designada de MobiWan [98], é de 2002, anterior à RFC MIPv6 (2004), por isso baseado nos *drafts* existentes na altura.

O Network Simulator é ideal para simular cenários virtuais com muitas máquinas e com diferentes e complexas topologias, algo muito difícil e no mínimo complicado de fazer com terminais físicos.

7. Testes e resultados

Nos capítulos anteriores já foi descrito o funcionamento geral do MIPv6, e foram apresentados os cenários de teste. Neste capítulo são apresentados os resultados com base nos cenários configurados. De modo a permitir uma melhor compreensão e analise, será feito um resumo do especificado na RFC 3775 [19], devidamente acompanhado pelos resultados de modo a comprovar que a implementação segue o que está especificado. A ordem de conteúdos é a apresentada segundo na especificação do MIPv6, ou seja, a RFC 3775.

7.1 Vista geral do MIPv6

Nesta secção são apresentados alguns dados do funcionamento geral do MIPv6.

7.1.1 Novo protocolo IPv6

O “Mobile IPv6” define um novo protocolo, usando o cabeçalho da mobilidade. Este cabeçalho é usado para transportar as seguintes mensagens:

- Home Test Init(HoTI), Home Test(HoT), Care-of Test Init(CoTI), Care-of Test(CoT)

Usadas para o “Return Routability Procedure” (RRP) do MN para o CN, assegurando autorização dos Binding Updates (BUs) seguintes.

- Binding Update (BU), Binding Acknowledgement (BAck)

  O BU é usado para notificar o HA ou o CN do seu registo. O BAck é a resposta.

- Binding Refresh Request

  Refresca os registos expirados ou prestes a expirar.

- Binding Error

  Indica um erro no processo de mobilidade.

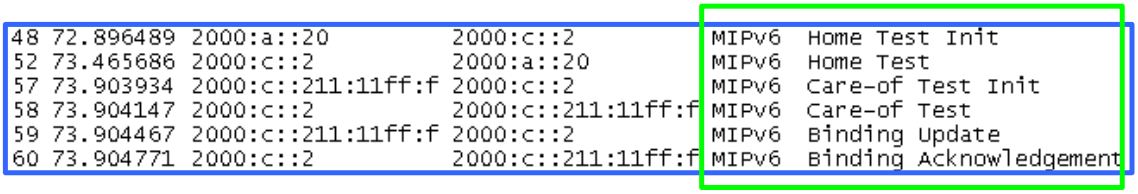


figura 27 - Captura de mensagens MIPv6 .

7.1.2 Nova opção de destino IPv6

O MIPv6 define uma nova opção IPv6 designada “Home Address Destination Option”.

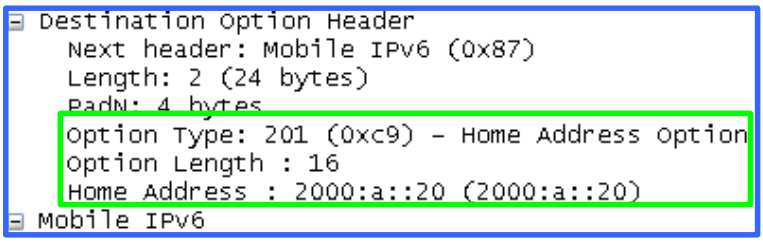


figura 28 - Novo “Destination Option Header” definido pelo MIPv6.

Este pacote apenas é processado pela máquina destino.

7.1.3 Novas mensagens ICMPv6

O MIPv6 introduz 4 novas mensagens ICMP, duas para o uso na descoberta dinâmica do endereço do HA, e duas para renumeração e configurações de mobilidade:

- Home Agent Address Discovery Request,
- Home Agent Address Discovery
- Mobile Prefix Solicitation,
- Mobile Prefix Advertisement.

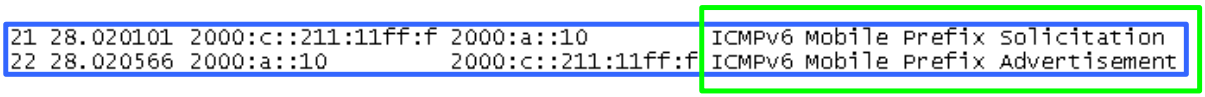


figura 29 - Exemplo de duas das quatro novas mensagens ICMPv6.

7.1.4 Estrutura de dados

O MIPv6 é descrito nos termos das seguintes estruturas de dados:

- Binding Cache – A *cache* de *bindings* mantida pelos HAs e CNs. A *cache* contém entradas "correspondent registration" e entradas "home registration".
- Binding Update List – Lista mantida por cada MN, que contem uma entrada por cada registo ou tentativa de registo. Registos com CNs e Has (correspondent e home registrations) estão incluídos na lista. As entradas são apagadas quando o tempo de vida expira.

- Home Agents List – Os HAs precisam de saber se existem outros HAs no mesmo *link*, e para isso usam esta lista. Esta lista é útil para informar os MNs durante a descoberta dinâmica de HAs.

7.1.5 Endereçamento Site-Local

Na altura da especificação do MIPv6 era possível o uso de endereços *site-local* se não fosse necessário o acesso à Internet. No entanto o uso destes era desaconselhado, uma vez que era possível que as redes origem e visitada fossem configuradas com os mesmos endereços, entre outros problemas.

Por outro lado, este tipo de endereços já não é usado no IPv6.

No entanto estes endereços *site-local* já desapareceram e por isso não podem ser usados.

7.2 Funcionamento geral da segurança no MIPv6

O MIPv6 fornece diversos mecanismos de segurança. Isso implica a protecção dos BUs enviados para os HAs e para os CNs, a protecção da descoberta do prefixo e dos mecanismos usados pelo MIPv6 para transportar informação. Os BUs são protegidos pelo uso dos cabeçalhos de extensão IPSec, ou pelo uso da "Binding Authorization Data option". Esta opção emprega uma *binding management key*, Kbm, que pode ser estabelecida através do *return routability procedure*. O mecanismo de descoberta do prefixo também é protegido pelo uso dos cabeçalhos de extensão IPSec. Os mecanismos relacionados com o transporte de pacotes como o *Home Address Destination option* e R*outing Header type* 2, foram especificados de modo a restringir o seu uso em ataques.

O MIPv6 especifica uma série de condições para que seja possível o registo de um MN perante um HA (Binding Updates to Home Agents) enquanto se move por diferentes redes.

São também especificadas várias condições necessárias ao processo de registo perante um CN (Binding Updates to Correspondent Nodes). A protecção dos BUs enviados para os CNs não necessita de configuração de associações de segurança ou da existência de uma infra-estrutura de autenticação entre ambos. Em vez disso é usado o *return routability procedure* para garantir que é o realmente o MN correcto que enviou a mensagem.

7.3 Novo protocolo IPv6, tipos de mensagens, e opção de destino

Já foi referido anteriormente que o MIPv6 define um novo protocolo IPv6, um novo cabeçalho de mobilidade, novas mensagens, novas opções de destino e novas mensagens ICMPv6.

Só para relembrar, a figura seguinte representa o cabeçalho IPv6 e os seus campos.

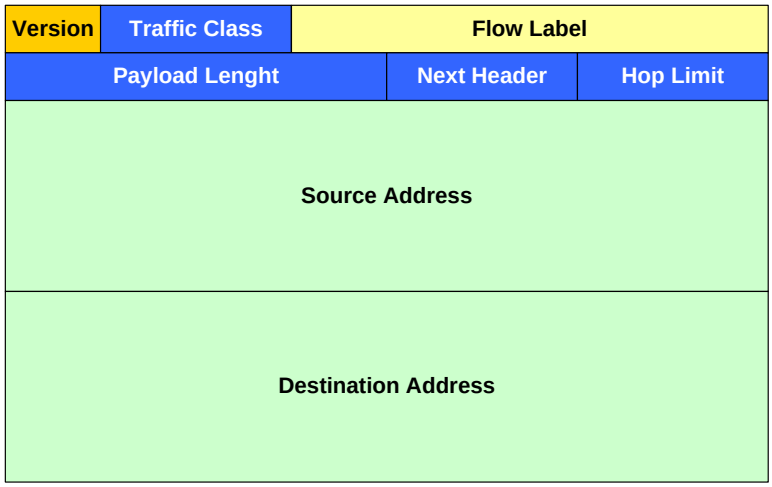


figura 30 - Cabeçalho IPv6.

O campo *Next Header* é usado pelo mecanismo de extensões para identificar qual o cabeçalho no pacote IPv6 que se segue. No MIPv6 o cabeçalho de extensão seguinte pode ser o cabeçalho de Mobilidade, identificado pelo valor *Next Header* 135, o *Destination Option* (Home Address Option), identificado pelo valor *Next Header* 60, ou o *Routing Header Type* 2, identificado pelo valor *Next Header* 43.

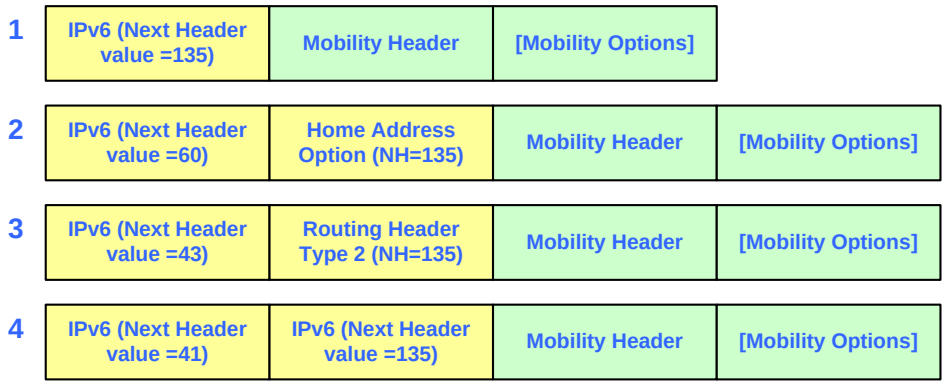


figura 31 - Diferentes possíveis sequências de cabeçalhos IPv6 na Mobilidade.

O quarto exemplo apresentado consiste no encapsulamento do cabeçalho IPv6 com outro. Este mecanismo é usado por exemplo para estabelecer o túnel entre MN e HA.

O MIPv6 define também novas mensagens ICMP para descoberta do *Home Agent* e Solicitação de prefixo, conforme referido na secção 7.1.3.

7.3.1 Cabeçalho de Mobilidade

O cabeçalho de mobilidade é um cabeçalho de extensão usado pelos MNs, CNs e Has em todas as mensagens relacionadas com a criação ou manutenção de registos.

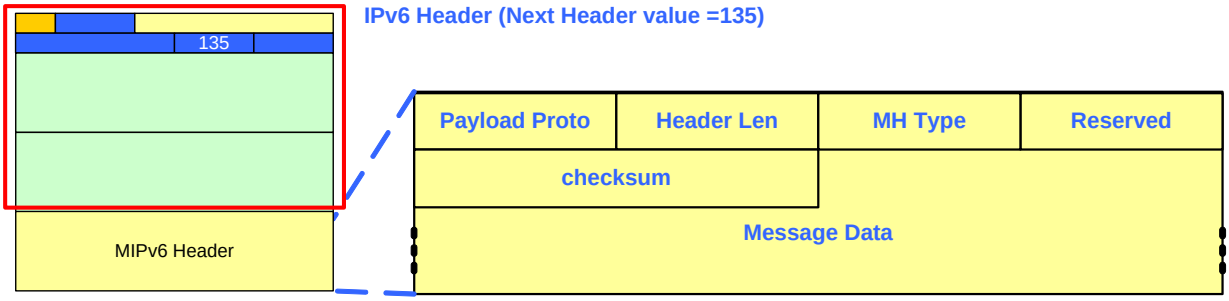


figura 32 - Cabeçalho de Mobilidade IPv6

Existem vários tipos de mensagens que são enviadas através do cabeçalho de mobilidade. A figura seguinte ilustra a título de exemplo o formato de um *Binding Update*.

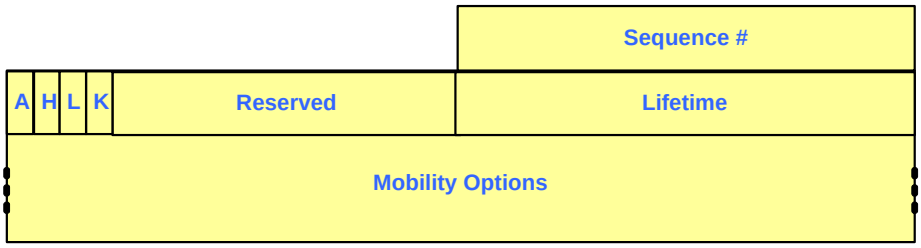


figura 33 - Formato da mensagem *Binding Update*.

As opções, por sua vez, possuem uma estrutura semelhante à da figura seguinte.

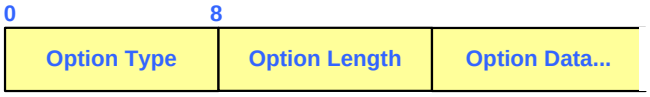


figura 34 - Formato das opções de mobilidade.

7.3.2 Home Address Option

A *Home Address option* é transportada pelo cabeçalho de extensão *Destination Option.* É usada num pacote enviado pelo MN enquanto for a da sua rede origem para informar o receptor do seu *Home Address*.

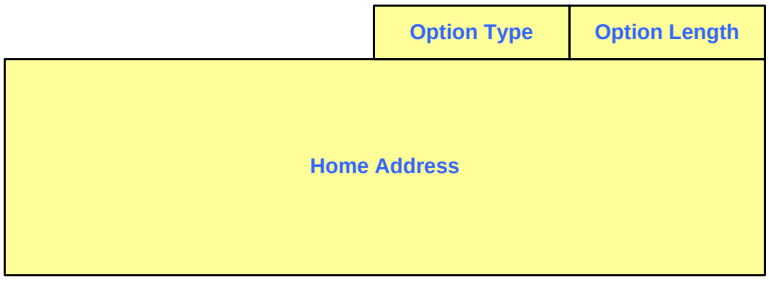


figura 35 - Formato do cabeçalho *Home Address Option*.

7.3.3 Router Header type 2

O MIPv6 define uma nova variante de um cabeçalho de encaminhamento, o *Routing Header Type 2*, para permitir que um pacote seja enviado directamente de um CN para o CoA do MN. O CoA é inserido no campo do endereço destino no cabeçalho IPv6. Assim que o pacote chega ao CoA, o MN recupera o seu endereço original do pacote, e este é usado como endereço final de destino para o pacote.

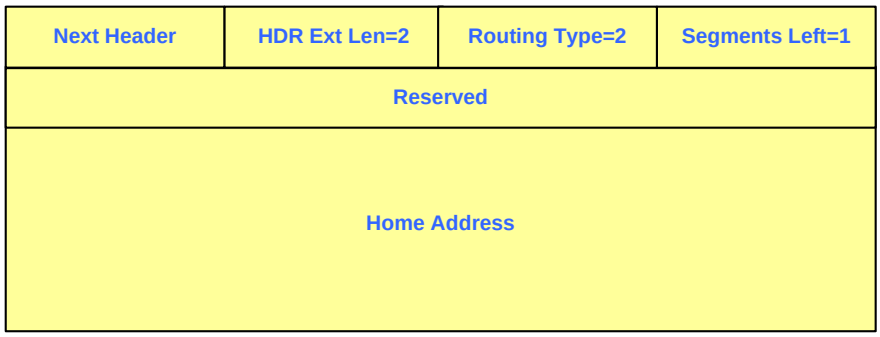


figura 36 - Formato do cabeçalho *Routing Header type 2*.

Este novo cabeçalho de encaminhamento usa um tipo diferente de encaminhamento do definido para o "IPv6 normal", possibilitando que as *firewalls* apliquem diferentes regras para este.

7.4 Modificações ao IPv6 Neighbor Discovery

A mobilidade requer algumas mudanças a mecanismos já existentes.

O MIPv6 "modifica" o formato da mensagem *Router Advertisement* adicionando um *flag bit* para indicar que o router que envia a mensagem está a servir de *Home Agent* naquele *link*.

O MIPv6 modifica o formato do *Prefix Information Option*, pois requer o conhecimento de um endereço global ao construir a sua lista de *Home Agents* através do mecanismo de descoberta de HAs. Contudo, o *Neighbor Discovery* só envia o endereço *link-local*. O MIPv6 permite que seja enviado o endereço global mudando uma *flag bit* no formato do *Prefix Information option* para uso no *Router Advertisement*.

O MIPv6 define um novo *Advertisement Interval option*, usado nas mensagens RA para anunciar o intervalo no qual são enviados RAs não solicitados para o endereço *multicast*.

O MIPv6 define um novo *Home Agent Information option*, usado nos RAs enviados pelo *Home Agent* para fornecer informação específica para este *router* funcionar como HA.

No MIPv6 também são definidas alterações ao envio de RAs, nomeadamente aos seus valores mínimos. O protocolo *Neighbor Discovery* especifica um intervalo mínimo de 3 segundos entre mensagens não solicitadas. Este intervalo é limitado pelas variáveis "MinRtrAdvInterval" e

"MaxRtrAdvInterval", respectivamente para o valor mínimo e máximo do intervalo. Os novos valores definidos para estas variáveis foram:

- MinRtrAdvInterval 0.03 segundos
- MaxRtrAdvInterval 0.07 segundos

7.5 Funcionamento do MN, HA e CN

Para testar o funcionamento do MIPv6, nomeadamente das suas entidades recorreu-se a cenários de teste. O primeiro cenário configurado para testar a mobilidade, já descrito no capítulo anterior, consistiu em 4 máquinas Linux e dois *hubs* interligados entre si via cabo. Note-se que o princípio da mobilidade IP é o mesmo para redes com e sem fios.

Foram configuradas três redes: a rede origem, a rede que pretende simular a Internet e a rede visitada, referenciadas respectivamente como rede A, B e C, para uma melhor identificação. As letras usadas são as presentes no prefixo do endereço da respectiva rede.

Foram também configurados três elementos do MIPv6, o MN, o HA e o CN.

A figura seguinte ilustra o cenário configurado.

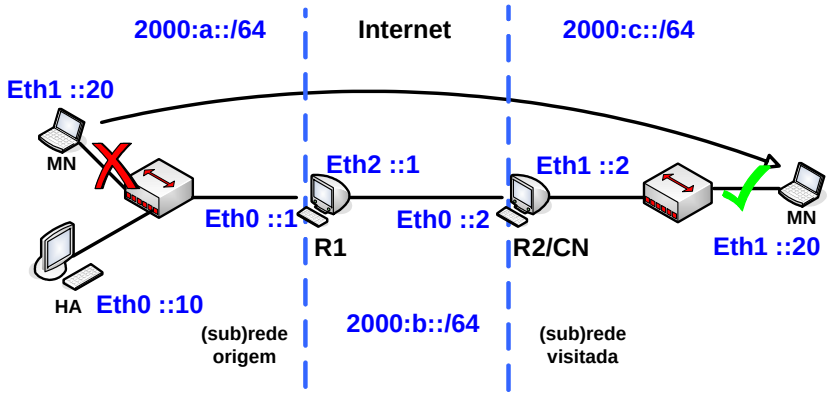


figura 37 - Cenário *wired* configurado para testar o MIPv6.

As máquinas HA, AR/CN e R são configuradas com encaminhamento (*forwarding*) activo. Além disso as duas primeiras também foram configuradas para enviar RAs de modo a que o MN consiga detectar quando se move entre as redes.

7.5.1 Configuração

A configuração deste cenário básico é bastante complexa, e por isso, foi concebido um *HowTo* para o efeito, existente no Anexo D. Apresentam-se todos os passos necessários para a configuração deste cenário, bem como os ficheiros de configuração das máquinas, alguns testes e resultados, *trobleshooting* e *faqs*.

7.5.2 Terminal na rede origem

Inicialmente foi possível constatar que estando o MN na sua rede origem, todo o encaminhamento funciona normalmente sem recurso ao MIPv6. Não existe sequer troca de pacotes MIPv6 entre nenhumas entidades. A única alteração visível é a existência de uma interface túnel gerada no MN.

Aqui a implicação do MIPv6 é que tanto o R como o AR estão constantemente a enviar RAs para as suas redes internas, mas como estes também são usados por outros protocolos, poder-se-á dizer que o MIPv6 implicará apenas o seu envio com maior frequência, por exemplo em vez de 3 segundos, será 0.05 segundos.

Além disso, quando é iniciado o mip6d no MN, também é possível verificar o envio de mensagens (*router solicitations*) *multicast*.

```
[root@localhost ~]# tcpdump -i eth1 -vv ip6 or proto ipv6
(...)
10:32:53.274337 :: > ff02::2: [icmp6 sum ok] icmp6: router solicitation
(len 8, hlim 255)
10:32:53.320868   fe80::230:4fff:fe0a:49a0   >   ff02::1:   icmp6:   router
advertisement(chlim=64,   pref=medium,   router_ltime=9,   reachable_time=0,
retrans_time=0)[ndp opt] (len 64, hlim 255)
10:32:53.322753 :: > ff02::16: HBH (rtalert: 0x0000) (padn)icmp6: type-#143
[hlim 1] (len 56)
10:32:53.467738 :: > ff02::1:ff59:e99: [icmp6 sum ok] icmp6: neighbor sol:
who has 2000:c::211:11ff:fe59:e99 (len 24, hlim 255)
```

figura 38 - Resultado do comando tcpdump.

O MN envia estas mensagens para solicitar os Router Advertisements, através dos quais sabe em que rede está, detectando assim os *handovers* posibilitando-lhe o *roaming*.

Exceptuando o envio destas mensagens, enquanto o MN está na rede origem toda a comunicação IPv6 funciona normalmente e todas as máquinas conseguem comunicar umas com as outras.

7.5.3 Mudança para outra rede

Para testar a mobilidade neste cenário desligou-se o cabo do MN da interface do Hub da rede origem e ligou-se no Hub da rede visitada.

O MN muda assim para outra rede, e uma vez que está a enviar "router solicitation" (multicast), o AR responde com o seu prefixo. O MN procede então à sua autoconfiguração, criando um novo endereço IPv6 a partir do prefixo recebido e do seu próprio MAC. O comando “ifconfig eth0” permite ver a o novo endereço.

```
[root@localhost ~]# ifconfig eth0
eth1      Link encap:Ethernet  HWaddr 00:11:11:59:0E:99
          inet6 addr: 2000:c::211:11ff:fe59:e99/64 Scope:Global❶
          inet6 addr: 2000:a::211:11ff:fe59:e99/64 Scope:Global❷
          inet6 addr: fe80::211:11ff:fe59:e99/64 Scope:Link❸
          inet6 addr: 2000:a::20/64 Scope:Global❹
```

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:924 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:93984 (91.7 KiB)  TX bytes:8770 (8.5 KiB)
          Base address:0xbc00 Memory:ff8e0000-ff900000
```

❶O novo Care of Address, gerado combinando o MAC com o prefixo do AR.
❷O endereço supérfluo da rede origem.
❸O endereço link local gerado no boot
❹O Home Address

figura 39 - Configuração da interface de rede do MN após mudança de rede.

Quase ao mesmo tempo, o MN irá enviar o BU para o HA. Na janela *tcpdump* é possível ver vários pacotes enviados para o HA. O *ethereal* também pode ser usado para verificar o envio de mensagens quando existe movimento, como por exemplo os BUs enviados para o HA após configurar o CoA.

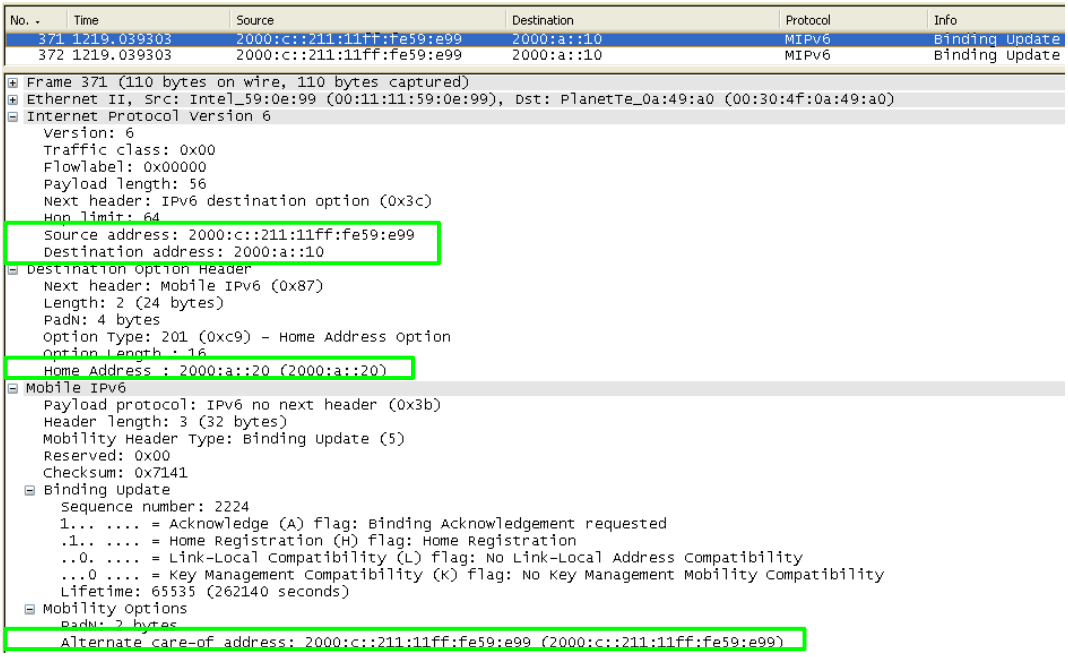


figura 40 - BU enviado para o HA

É possível verificar que a mensagem tem origem no CoA do MN com destino ao HA. No *Destination Option Header* podemos verificar a indicação do *Home Address*.

No cabeçalho *Mobility options* segue a indicação do CoA, que é igual ao *source address* do cabeçalho IPv6.

Na sequência do movimento foi enviado mais do que 1 pacote. Isto justifica-se pelo facto de o MN ter configurado mais do que um endereço da rede origem. Porém, esta situação não está especificado e não devia acontecer, uma vez que só 1 desses 2 endereços é que é o HoA, e só será criado um túnel entre o MN e HA com base neste endereço.

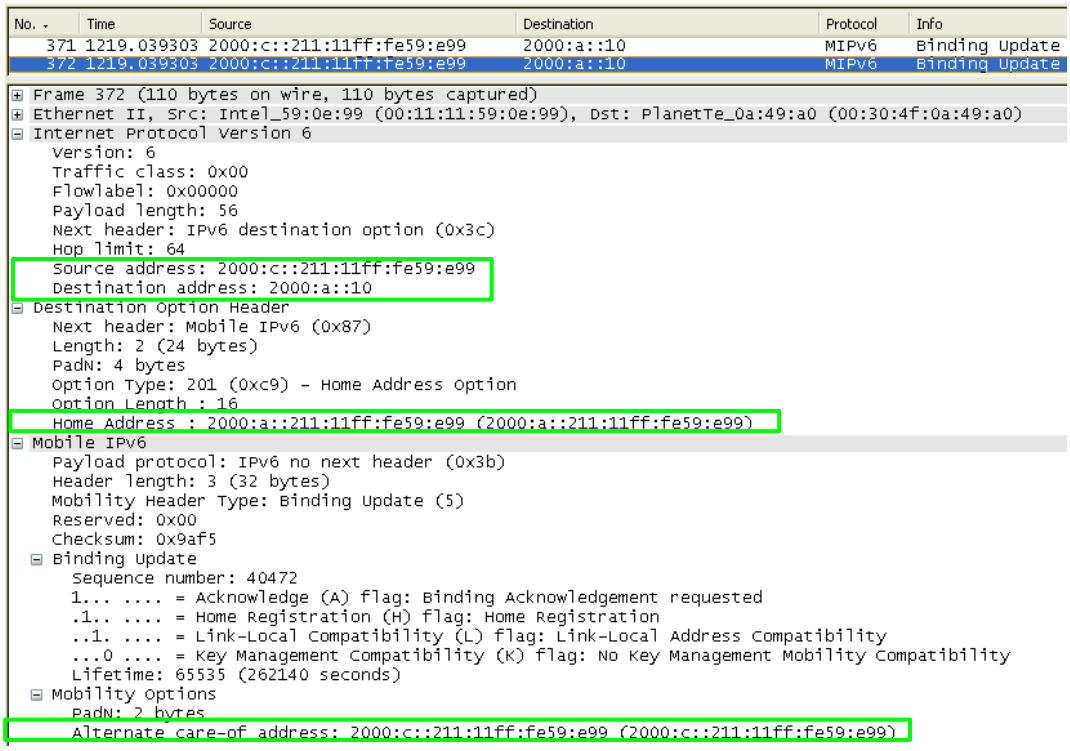


figura 41 - *Binding update* enviado para o HA

Depois do envio do *Binding Update* é recebido um *Binding Acknowledgement* (BAck) para confirmar a recepção do BU. A mensagem Back é apresentada na figura 42.

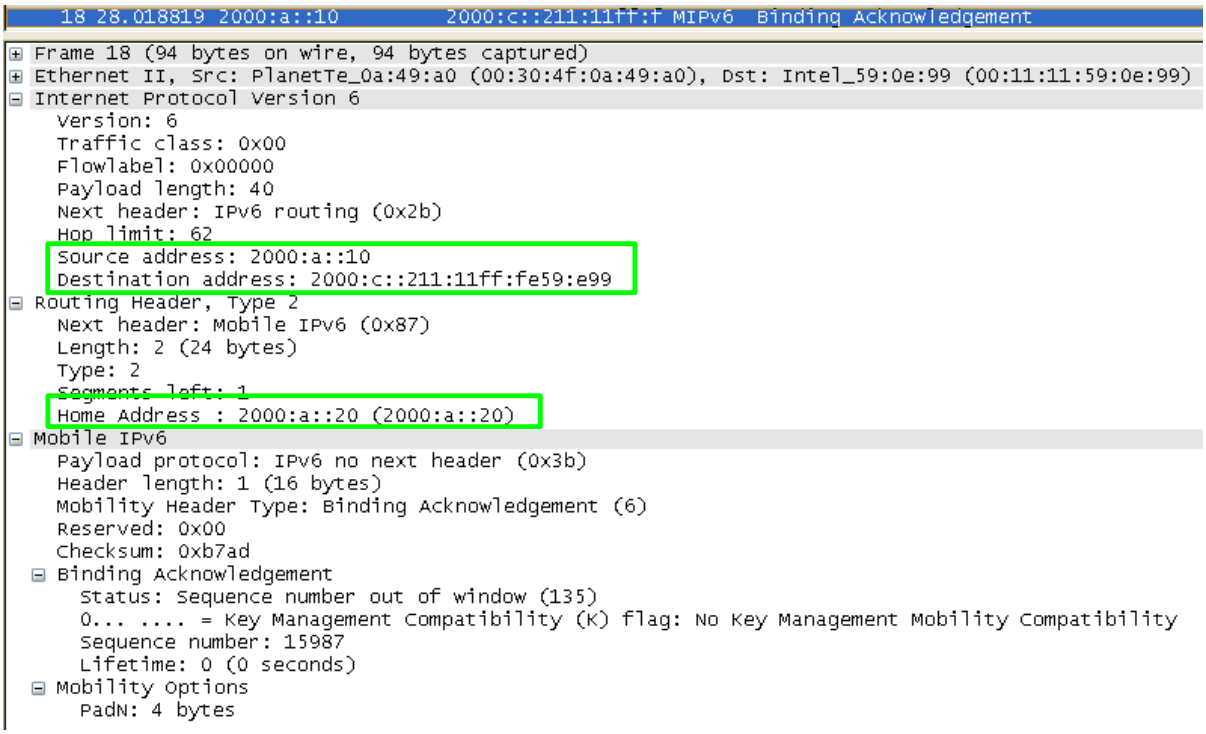


figura 42 - *Binding Acknowledgement* enviado do HA para o MN

Quando o MN se move para a outra rede, o AR/CN deve conseguir fazer a optimização de rota se esta foi configurada. A máquina R também vai comunicar com o MN mas sem MIPv6 configurado, para

verificar que neste caso a comunicação é feita por intermédio do HA. Para verificar como se processa a comunicação sem optimização de rotas, configurou-se a máquina AR/CN sem esta funcionalidade e usou-se o utilitário traceroute6. O resultado foi o apresentado na figura seguinte:

```
[root@localhost ~]# traceroute6 2000:c::2
traceroute to 2000:c::2 (2000:c::2) from 2000:a::211:11ff:fe59:e99, 30 hops
max, 16 byte packets
 1  * * *
 2  2000:a::1 (2000:a::1)  745.556 ms  0.684 ms  0.598 ms
 3  2000:c::2 (2000:c::2)  1.607 ms  0.743 ms  0.732 ms
[root@localhost ~]#
```

figura 43 - Resultado do comando traceroute executado no MN na rede C.

O resultado do comando não é o mais elucidativo, uma vez que o utilitário traceroute apresenta alguns problemas com o uso de túneis. No entanto, na figura seguinte está ilustrado o processo associado ao comando.

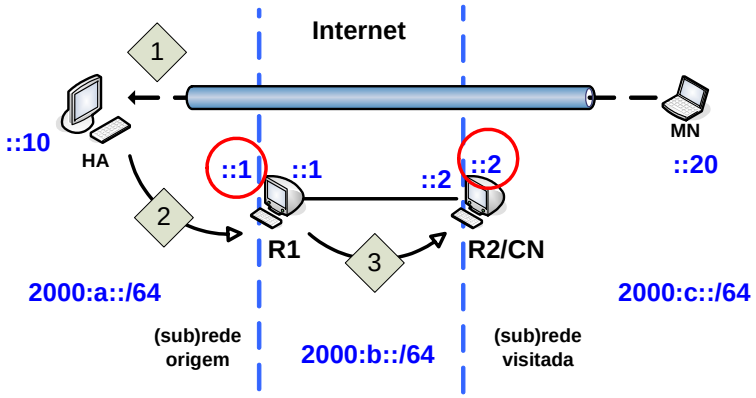


figura 44 - Descrição do processo associado ao traceroute6.

Os losângulos da figura anterior identificam os saltos existentes na comunicação entre o MN e o R2. Os círculos identificam os endereços devolvidos pelo comando nos saltos 2 e 3.

Para testar então como funciona o mecanismo de optimização de rotas entre o MN e o CN, foi configurada esta funcionalidade no R2 e repetiram-se os testes. Estes são apresentados na secção seguinte.

7.5.4 Correspondent Binding Procedure/Return Routability Procedure

O "*Correspondent Binding Procedure*" (CBP) é o mecanismo que o MN usa para efectuar um registo perante um CN. Este processo envolve um mecanismo de autenticação entre os extremos da comunicação designado de "*Return Routability Procedure*" (RRP). O RRP é um processo que permite autenticação mútua entre um MN e um CN de modo ao MN efectuar o registo no CN que permite a optimização de rota entre ambos.

Este mecanismo consite em enviar duas mensagens com duas diferentes chaves geradas por dois caminhos distintos. Uma é enviada directamente usando o CoA, enquanto que a outra é enviada

através do HA usando o HoA. O CN responde ao MN com outras duas mensagens enviadas pelos percursos inversos e levando as chaves recebidas. A figura seguinte ilustras o processo do RRP.

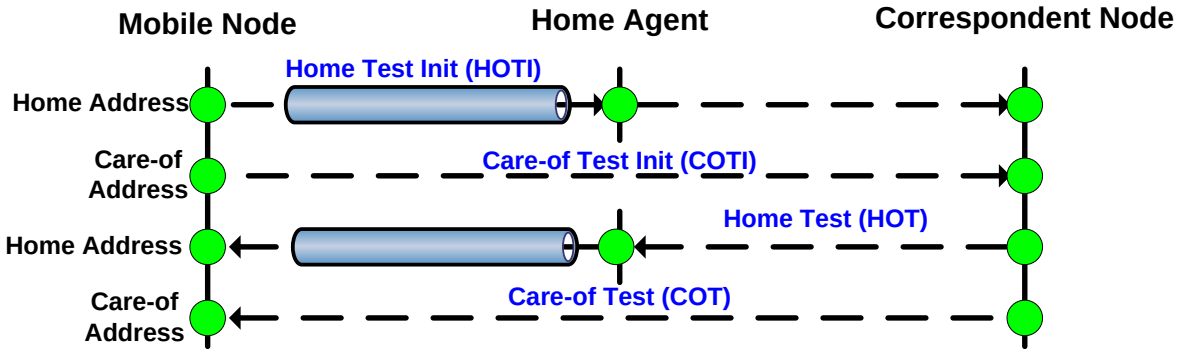


figura 45 - Diagrama de fluxo do Return Routability Procedure.

É possível verificar a troca de menagens entre o MN e o CN, primeiro via túnel usando o seu HoA, e depois directamente usando o seu CoA. Este mecanismo garante segurança ao processo do MIPv6, pois mesmo que um terminal localizado estrategicamente na rede, consiga capturar ambas as mensagens, essa posição privilegiada permitir-lhe-á fazer outro tipo de ataques muito mais facilmente do que com recurso ao registo falso no HA. Depois deste processo é então realizado o registo através do envio de um BU pelo MN usando já o percurso directo. O seguinte diagrama de fluxo corresponde a uma captura de pacotes MIPv6 no MN após a mudança de rede.

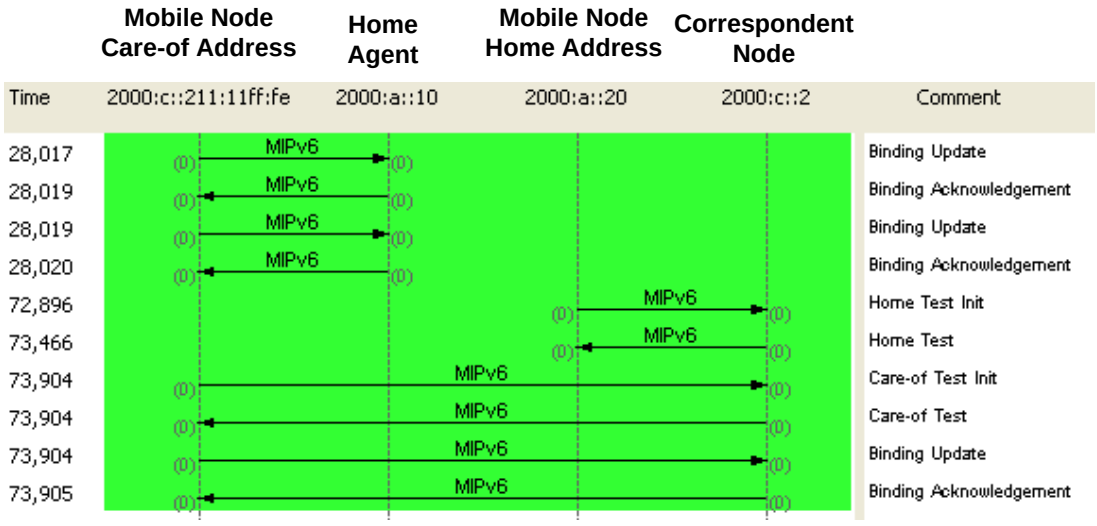


figura 46 - Diagrama de fluxo de troca de mensagens entre o MN e o HA/CN

Neste diagrama, as primeiras quatro mensagens correspondem ao *Binding Procedure* (registo realizado no HA), e as quatro seguintes correspondem ao RRP. As duas últimas completam o CBP, após o qual a comunicação entre MN e CN passa a ser directa.

A imagem seguinte mostra a mensagem *Home Test Init* (HoTI) enviada do MN para o CN através do HA por túnel.

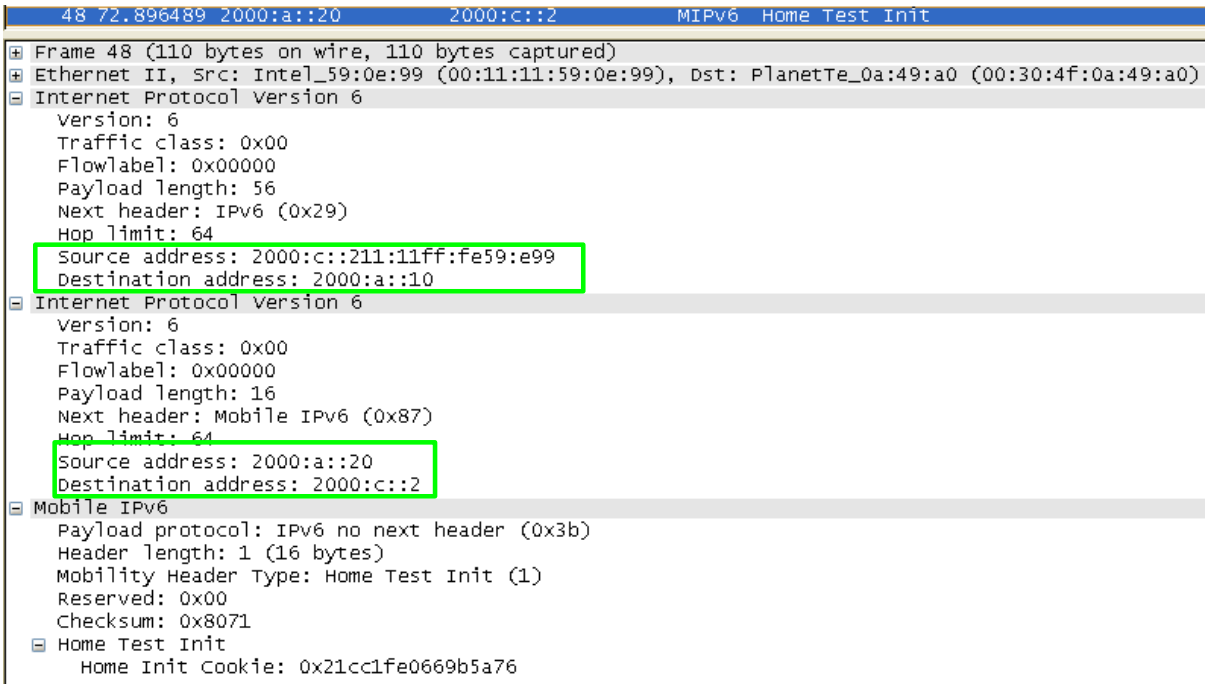


figura 47 - Mensagem *Home Test Init* (HoTI) enviada do MN para o CN através do HA.

A imagem seguinte mostra a resposta do CN à mensagem HoTI recebida. A *Home Test* (HoT) é enviada do CN para o MN usando o percurso inverso da HoTI, ou seja, através do HA.

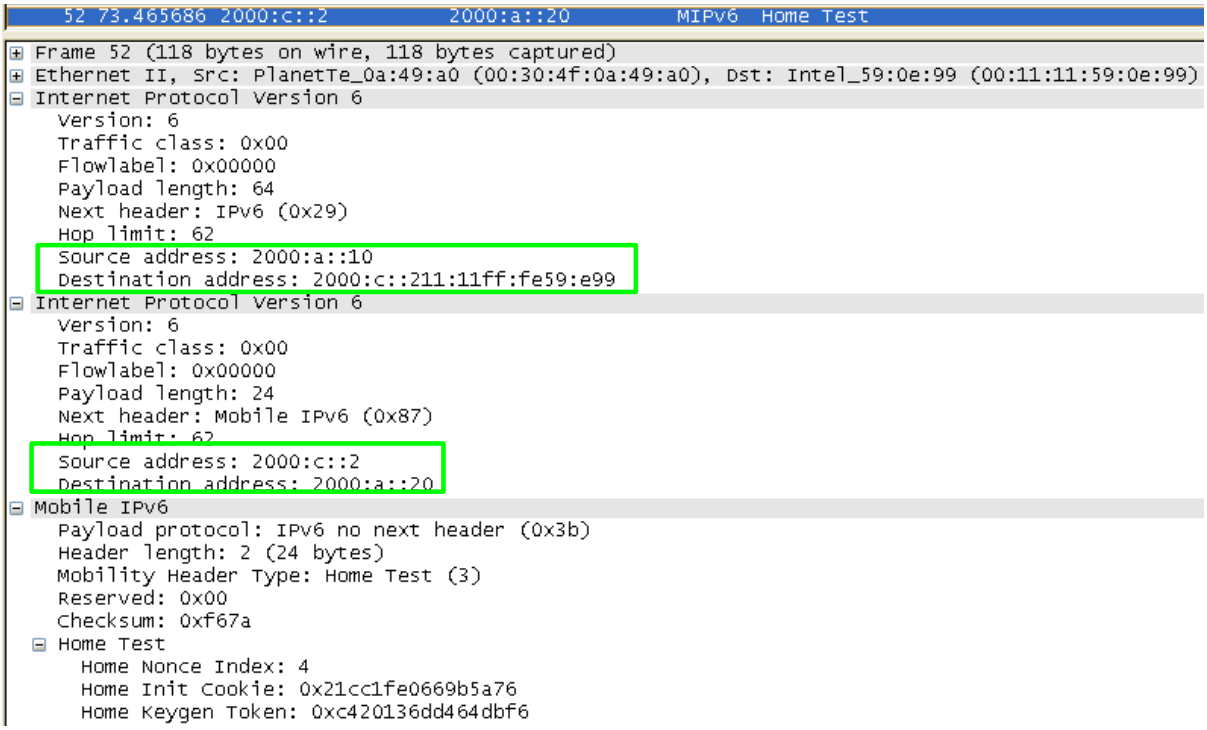


figura 48 - Mensagem *Home Test* (HoT) enviada do CN para o MN através do HA.

A imagem seguinte a mensagem *Care-of Test Init* (CoTI) enviada do MN directamente para o CN fazendo uso do seu CoA.

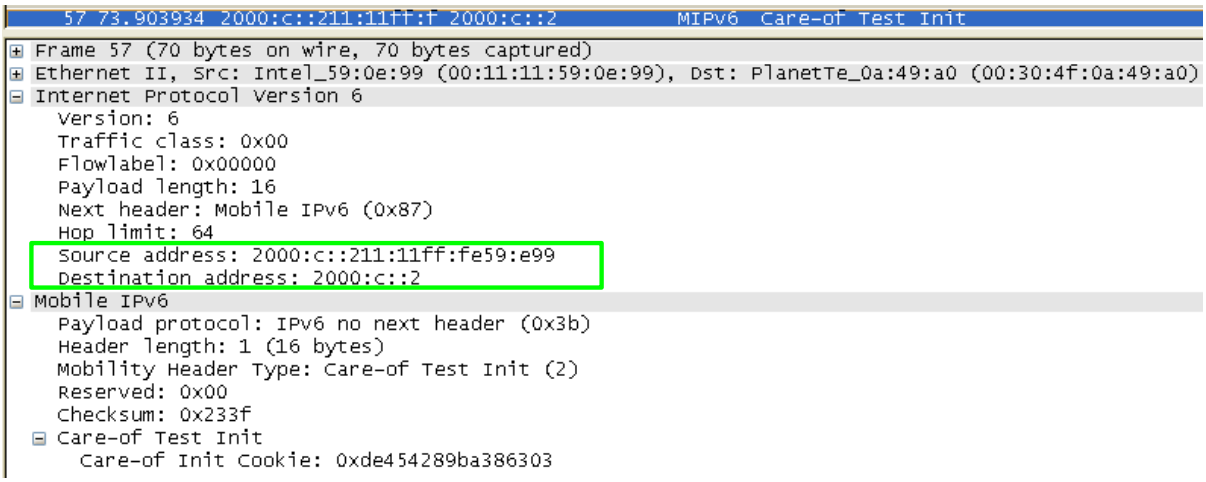


figura 49 - Mensagem *Care-of Test Init* (CoTI) enviada do MN directamente para o CN.

A resposta do CN á mensagem CoTI recebida é uma mensagem *Care-of Test* (CoT) enviada directamente para o CoA do MN.

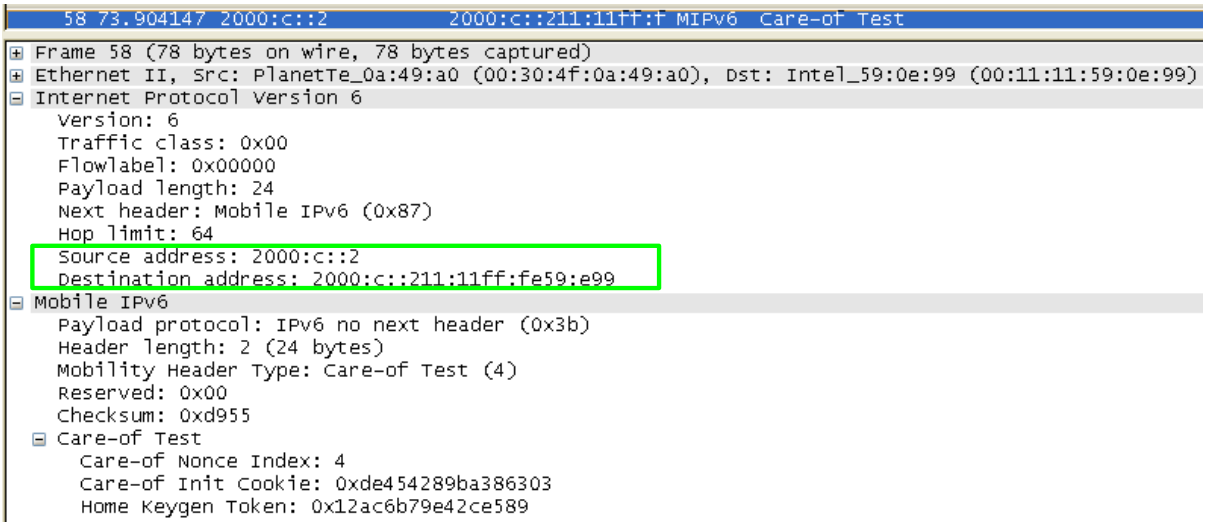
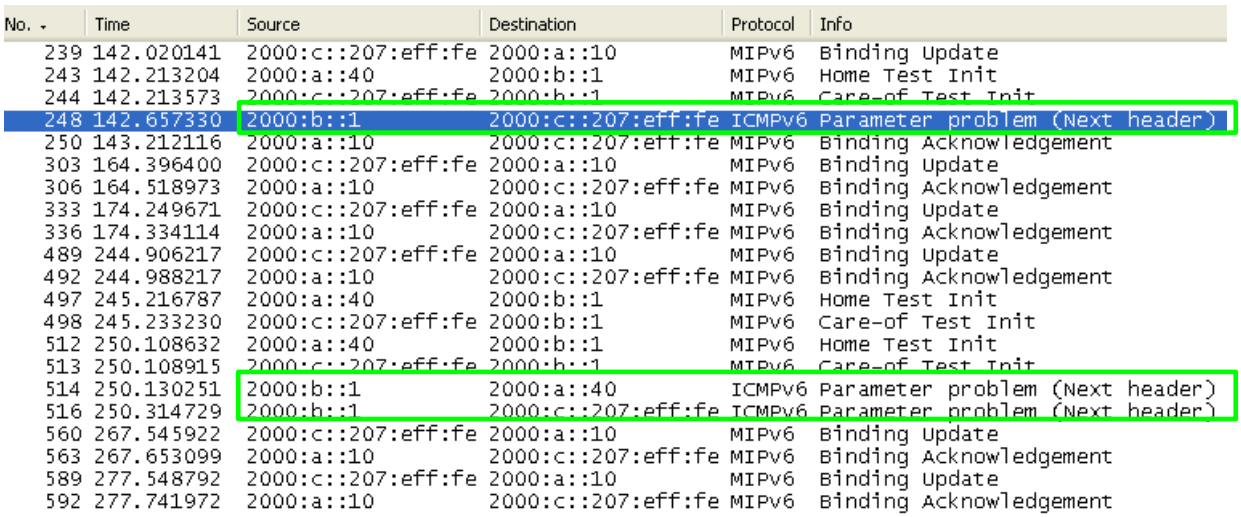


figura 50 - Mensagem *Care-of Test* (CoT) enviada em resposta à CoTI.

Após isto é garantida a autenticação mútua entre MN e CN, e é então efectuado o registo através do envio de um BU do MN directamente para o CN, e recepção do respectivo BAck. Este processo e as mensagens são iguais ás do registo realizado no HA.

Este é o processo realizado quando a máquina com a qual o MN tenta fazer o registo possui suporte da funcionalidade de CN. No entanto a máquina poderá não ter suporte dessa funcionalidade, e aí o registo não é realizado. Ao tentar comunicar com uma nova máquina, enquanto ausente da rede origem, o MN tenta imediatamente estabelecer um registo nessa nova máquina através do RRP enviando as mensagens de CoTI e HoTI. Ao receber estas mensagens, a máquina como não as conhece, responde com mensagens de parameter problem, conforme se ilustra na figura seguinte.

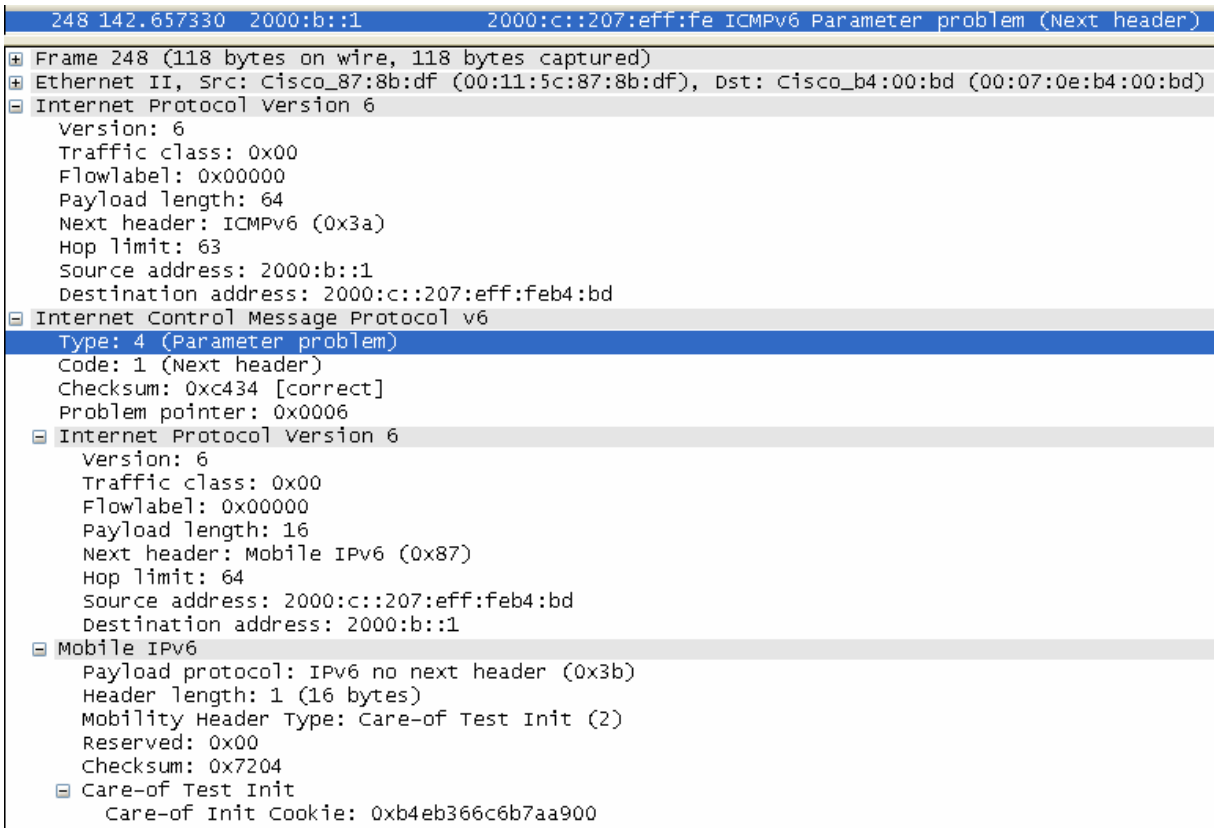


No.	Time	Source	Destination	Protocol	Info
239	142.020141	2000:c::207:eff:fe	2000:a::10	MIPv6	Binding Update
243	142.213204	2000:a::40	2000:b::1	MIPv6	Home Test Init
244	142.213573	2000:c::207:eff:fe	2000:b::1	MIPv6	Care-of Test Init
248	142.657330	2000:b::1	2000:c::207:eff:fe	ICMPv6	Parameter problem (Next header)
250	143.212116	2000:a::10	2000:c::207:eff:fe	MIPv6	Binding Acknowledgement
303	164.396400	2000:c::207:eff:fe	2000:a::10	MIPv6	Binding Update
306	164.518973	2000:a::10	2000:c::207:eff:fe	MIPv6	Binding Acknowledgement
333	174.249671	2000:c::207:eff:fe	2000:a::10	MIPv6	Binding Update
336	174.334114	2000:a::10	2000:c::207:eff:fe	MIPv6	Binding Acknowledgement
489	244.906217	2000:c::207:eff:fe	2000:a::10	MIPv6	Binding Update
492	244.988217	2000:a::10	2000:c::207:eff:fe	MIPv6	Binding Acknowledgement
497	245.216787	2000:a::40	2000:b::1	MIPv6	Home Test Init
498	245.233230	2000:c::207:eff:fe	2000:b::1	MIPv6	Care-of Test Init
512	250.108632	2000:a::40	2000:b::1	MIPv6	Home Test Init
513	250.108915	2000:c::207:eff:fe	2000:b::1	MIPv6	Care-of Test Init
514	250.130251	2000:b::1	2000:a::40	ICMPv6	Parameter problem (Next header)
516	250.314729	2000:b::1	2000:c::207:eff:fe	ICMPv6	Parameter problem (Next header)
560	267.545922	2000:c::207:eff:fe	2000:a::10	MIPv6	Binding Update
563	267.653099	2000:a::10	2000:c::207:eff:fe	MIPv6	Binding Acknowledgement
589	277.548792	2000:c::207:eff:fe	2000:a::10	MIPv6	Binding Update
592	277.741972	2000:a::10	2000:c::207:eff:fe	MIPv6	Binding Acknowledgement

figura 51 - Falha do processo RRP.

Na primeira tentativa de realizar o RRP apenas recebe uma mensagem de resposta à CoTI, e por isso tenta realizar o registo outra vez, enviando novamente a CoTI e a HoTI. Recebe então duas mensagens de Parameter Problem, e então fica a saber que aquele terminal não é um CN e comunica com ele através do túnel estabelecido com o HA.

A figura seguinte mostra o conteudo da mensagem Parameter Problem recebida no MN.



```
248 142.657330  2000:b::1          2000:c::207:eff:fe ICMPv6 Parameter problem (Next header)

⊞ Frame 248 (118 bytes on wire, 118 bytes captured)
⊞ Ethernet II, Src: Cisco_87:8b:df (00:11:5c:87:8b:df), Dst: Cisco_b4:00:bd (00:07:0e:b4:00:bd)
⊟ Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 64
    Next header: ICMPv6 (0x3a)
    Hop limit: 63
    Source address: 2000:b::1
    Destination address: 2000:c::207:eff:feb4:bd
⊟ Internet Control Message Protocol v6
    Type: 4 (Parameter problem)
    Code: 1 (Next header)
    Checksum: 0xc434 [correct]
    Problem pointer: 0x0006
  ⊟ Internet Protocol Version 6
      Version: 6
      Traffic class: 0x00
      Flowlabel: 0x00000
      Payload length: 16
      Next header: Mobile IPv6 (0x87)
      Hop limit: 64
      Source address: 2000:c::207:eff:feb4:bd
      Destination address: 2000:b::1
  ⊟ Mobile IPv6
      Payload protocol: IPv6 no next header (0x3b)
      Header length: 1 (16 bytes)
      Mobility Header Type: Care-of Test Init (2)
      Reserved: 0x00
      Checksum: 0x7204
    ⊟ Care-of Test Init
        Care-of Init Cookie: 0xb4eb366c6b7aa900
```

figura 52 - Mensagem Parameter Problem.

7.5.5 Regresso à rede origem

O terminal móvel ao permanecer muito tempo numa rede visitada terá, de tempos a tempos, de refrescar os registos, umas vez que estes possuem um determinado tempo de vida. Este tempo poderá ser configurado.

Ao mover-se entre redes todos os processos de registos e actualizações de registos se repetem, inclusivé quando o MN se move para a sua rede origem. Neste caso, ao detectar que voltou à rede origem, o MN envia BUs para o HA e CNs para estes saberem da sua nova localização, e ao analisarem o pacote verificam que o MN se encontra na sua rede origem e então é desfeito o registo de mobilidade e toda a comunicação IPv6 se processa normalmente a partir desse momento sem recurso aos mecanismos de mobilidade.

7.6 Interoperabilidade do MIPv6 em Linux, IOS e Windows

No segundo cenário de teste configurado, tomou-se como base o cenário funcional anterior, manteve-se o MN mas substituíram-se as outras máquinas Linux por *routers* Cisco. Além disso, também se acrescentou um CN configurado numa máquina Windows. O HA foi configurado na máquina R1. Este cenário teve como objectivo testar a interoperabilidade entre diferentes implementações do MIPv6.

Em Windows apenas é possível configurar a funcionalidade de CN (baseada no draft 12 do MIPv6), e uma vez que o IOS da Cisco não suporta as funcionalidades de MN, não houve outra hipótese senão usar o MN configurado em Linux. Outra das restrições do IOS da Cisco é o facto de não suportar IPSec tal como definido na RFC 3776, logo não foi usado IPsec.

A figura seguinte ilustra o cenário configurado.

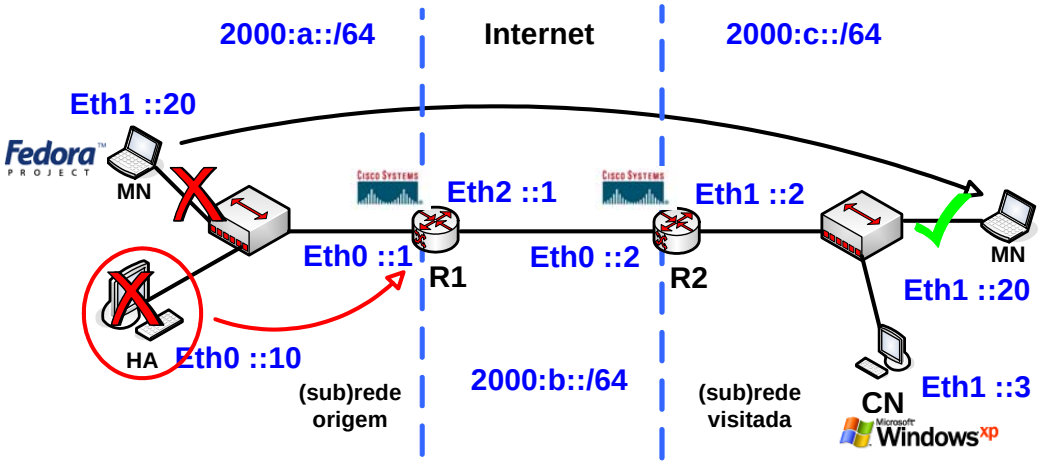


figura 53 - Cenário 2 – máquinas linux e cisco.

Os *routers* Cisco foram configurados para enviar *Router Advertisements* na rede origem e rede destino, para deste modo o MN detectar quando se move de rede, e o *router* na rede origem também

foi configurado como HA. A máquina Windows foi configurada como CN para comunicar com o MN (máquina Linux).

O MN detecta a mudança de rede, consegue configurar o CoA e alterar a sua rota por omissão. No entanto, as mensagens MIPv6 não são reencaminhadas pelo router Cisco. Deste modo o MN não consegue fazer o registo (*Binding Update*) no *Home Agent* nem nos CNs. Mesmo estando um CN na mesma rede que o MN o registo envolve obrigatoriamente o sucesso do *return routability procedure.* Neste, a troca de mensagens além de se processar directamente também é feita através do HA. Estando este inacessível, o MN é incapaz de se registar seja onde for.

Este cenário não foi bem sucedido devido essencialmente ao fraco suporte de mobilidade e de interoperabilidade existente nos sistemas operativos envolvidos. Além das limitações do Windows e IOS já mencionadas, refira-se também que a implementação MIPL ainda não é a versão final e por isso é provável que existam ainda *bugs* por resolver.

A imagem seguinte é um exemplo de como as implementações ainda estão imaturas.

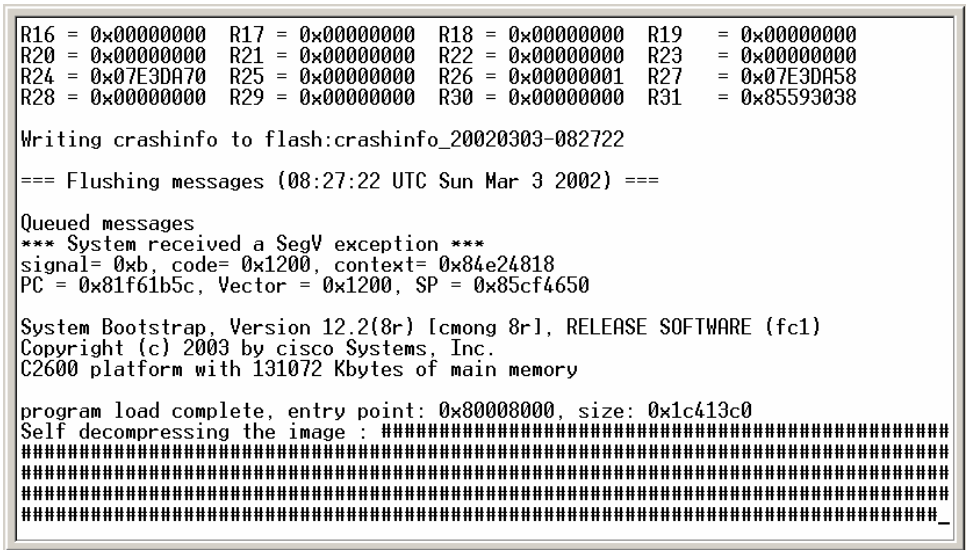


figura 54 - Erro do IOS ocorrido no cenário de Mobilidade IPv6.

O erro do IOS apresentado na figura 54 foi motivado pelas mensagens de mobilidade recebidas, provenientes do terminal móvel Linux.

7.7 Desempenho do Handover no MIPv6

O terceiro cenário configurado para testar a mobilidade, já descrito no capítulo anterior, foi elaborado a partir do primeiro, com a única diferença que a comunicação com o MN é *wireless*.

Assim mantiveram-se as 4 máquinas Linux e os dois *hubs*, acrescentando-se um AP ligado a cada *hub*, e colocou-se uma placa PCI no MN.

As redes configuradas e os endereços usados foram os mesmos do primeiro cenário.

A figura seguinte ilustra o cenário configurado.

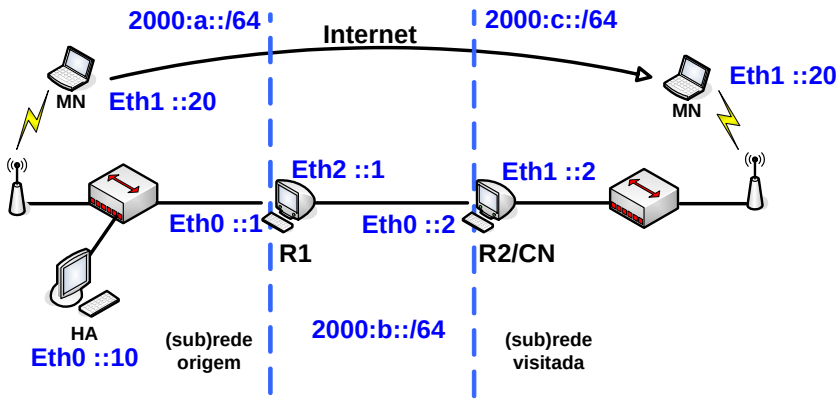


figura 55 - Cenário *wireless* configurado para testar o MIPv6.

As máquinas HA, R2/CN e R1 são configuradas com encaminhamento activo. Além disso as duas primeiras também foram configuradas para enviar RAs de modo a que o MN consiga detectar quando se move entre as redes.

O objectivo deste cenário era testar o desempenho do *handover* do MIPv6, mas alguns problemas surgiram que não conseguiram ser resolvidos em tempo útil. E por isso não foi possível testar este cenário. Os problemas encontrados estavam relacionados com os APs Cisco, mais concretamente com o facto de estes não reencaminharem os pacotes recebidos com destino a um endereço *layer* 2 *multicast*. Assim, os *Routers Advertisements* recebidos na sua interface *FastEthernet* e os *Routers Solicitations* recebidos na interface *wireless* não são reencaminhados, e com isso o MN não consegue detectar a mobilidade e consequentemente não consegue formar o CoA. Resumindo, não era possível detectar o movimento e efectuar o processo da mobilidade, logo a ligação perdia-se.

De modo a contornar este problema construiu-se um cenário semelhante mas no qual todas as máquinas possuem placas *wireless* e comunicam entre si em modo *had-hoc*. Instalou-se então placas PCI em todas as máquinas e configurou-se redes *ad-Hoc* com diferentes identificadores (essid).

A representação do cenário é apresentada na figura seguinte.

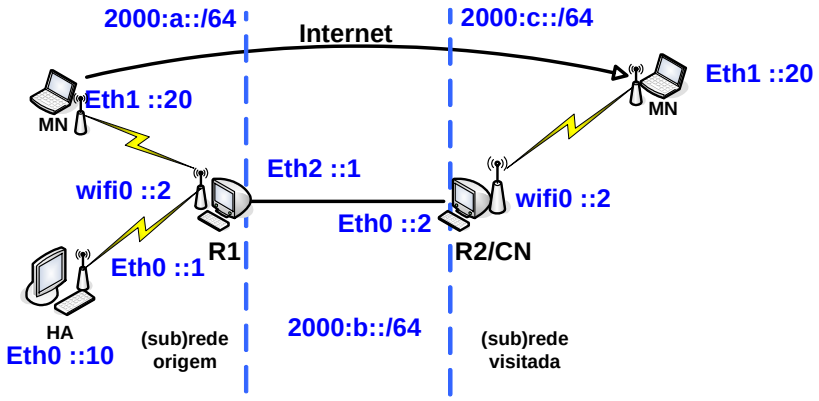


figura 56 - Cenário *ad-hoc* configurado para testar o MIPv6.

A configuração deste cenário é apresentada no tutorial presente no Anexo D.

Depois de se obter conectividade IPv6 entre todas as máquinas, e de se configurar o MIPv6 foi possível avançar com os testes. Utilizando os utilitários *ping*, *traceroute* e *ethereal* foi possível verificar a operação do MIPv6. No entanto, para verificar e analisar o *handover* enquanto o MN anda continuamente em *roaming* com sucessivas mudanças de rede, torna-se útil uma ferramenta como o "MIPv6 Tester".

7.7.1 MIPv6-Tester

O MIPv6 Tester[3] é uma aplicação *open source* concebida para testar a Mobilidade IPv6.

O seu funcionamento consiste em definir um cliente e um servidor que comunicam ponto-a-ponto, criando uma ligação TCP e duas UDP entre eles. Para além do modo (cliente ou servidor), do endereço remoto, também poderá ser configurado o número de pacotes enviados por segundo em cada ligação. Esta aplicação é bastante simples, e possui apenas duas janelas, uma para configuração e outra para os resultados. A figura seguinte mostra um *screenshot* das janelas da aplicação:

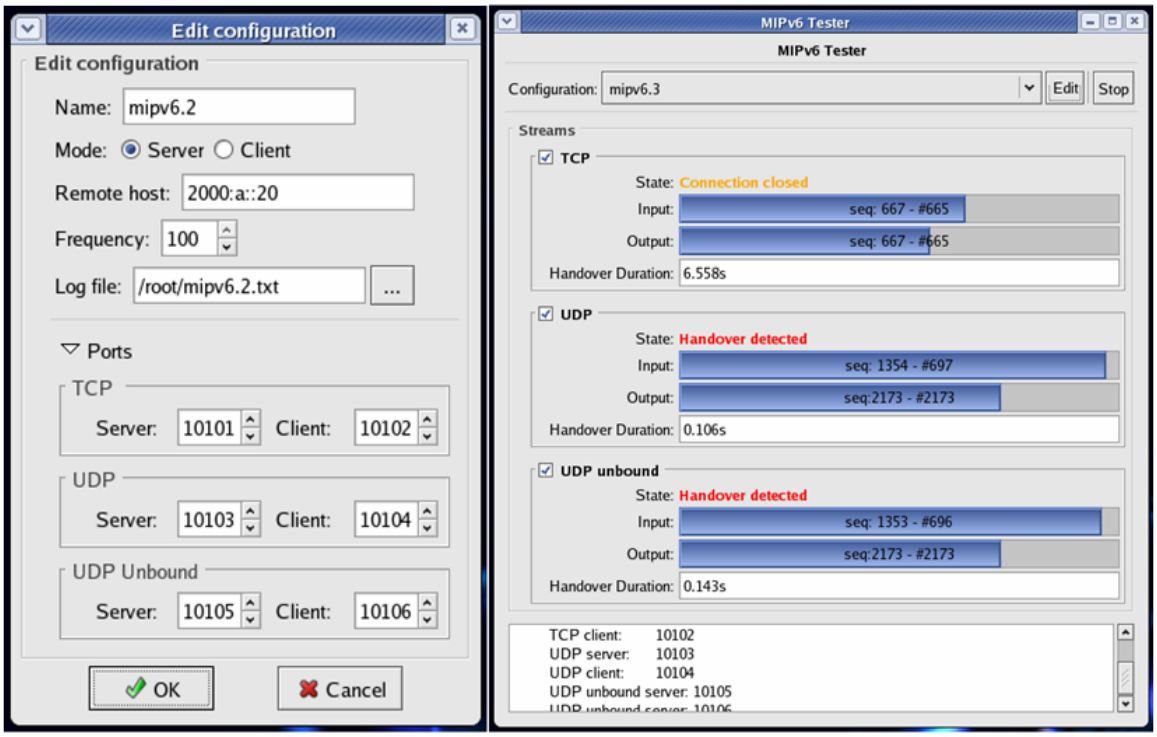


figura 57 - *ScreenShot* das duas janelas da aplicação MIPv6 Tester.

A janela de configuração permite definir o nome do perfil de configuração, o modo

É a partir dos RAs recebidos, e da informação neles contida que o MN gera o seu Care-of Address. A periodicidade destes RAs irá influenciar a performance do *handover*. Este também está dependente da largura de banda e do estado de congestão da rede.

[3] Aplicação disponível em: http://www.bullopensource.org/mipv6/index.php

7.7.2 Análise dos resultados

O intervalo de tempo para envio de *Router Advertisements* (RAs) não solicitados por máquinas Linux encontra-se especificado nas variavéis presentes no ficheiro de configuração "/etc/radvd.conf". Os parâmetros *MinRtrAdvInterval MaxRtrAdvInterval* definem esse intervalo. As especificações iniciais definiram que os valores mínimos para estas variáveis seriam 3 e 4 segundos respectivamente. Assim o intervalo mínimo de envio de RAs é {3;4}segundos. Contudo a RFC 3775 altera os valores mínimos destes valores para 0.03 e 0.07 segundos respectivamente, podendo existir assim um intervalo mínimo de envio de RAs de {0.03;0.07}. No entanto, o *deamon* RADVD (responsável pelo envio de RAs), presente na instalação Fedora Core 3 usada nos testes, apenas aceita apenas valores mínimos de 0.05 e 1.5, estabelecendo um intervalo mínimo de {0.05;1.5}.

Posto isto, configurou-se um intervalo de envio de RAs de {0.05;1.5} na rede origem. Na rede visitada configurou-se um intervalo de {3;4}. Pretende-se assim representar um cenário em que um utilizador possui suporte de mobilidade na sua rede origem, e desloca-se para uma rede visitada sem suporte de mobilidade, mas na qual até existem RAs a serem enviados com o intervalo mínimo {3;4} (frequência máxima considerando os valores sem suporte para mobilidade).

A figura 58 ilustra o deslocamento do MN entre as redes e mostra os valores dos intervalos de envio de RAs configurados.

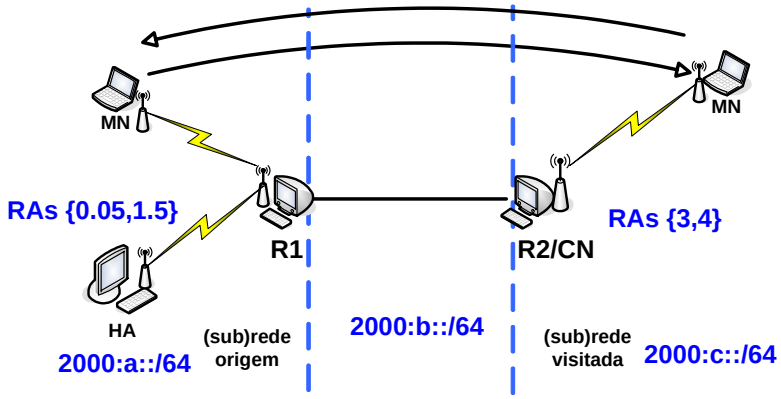


figura 58 - Deslocação do terminal móvel entre as redes

Outro factor relevante que deve ser mencionado, é que as ligações *wireless* (*ad-hoc*) configuradas, usam placas PCI com suporte da norma 802.11b a 11Mbps. Assim o débito teórico destas é de 11/8=1,375Mbytes. As ligações por fio são *fastethernet* (100Mbps) com débito teórico de 12,5Mbytes.

Para iniciar os testes instalou-se o MIPv6 Tester nas máquinas MN e R1. Configurou-se as ligações e a frequência de envio de pacotes. Após iniciar os testes, verificaram-se alguns problemas, aparentemente por falta de sincronismo da aplicação ou devido ao excesso de tráfego, causando perda de pacotes. Os sintomas eram a existência constante de *handovers*, mesmo sem o MN se encontrar em roaming. Este facto pode ser observado na figura 59.

figura 59 - Imagem do funcionamento do MIPv6 Tester.

Iniciou-se então uma captura para analisar os pacotes enviados pela aplicação. A figura 60 seguinte mostra um pacote de um dos fluxos UDP.

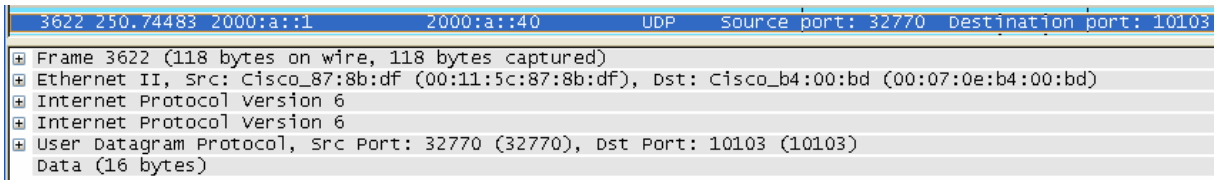


figura 60 - Pacote UDP gerado pelo MIPv6 Tester.

Estavam a ser usadas 3 ligações bidirrecionais (uma TCP com pacotes de 126bytes, duas UDP com pacotes de 118 bytes e 78 bytes) e aplicação estavam configurada para enviar pacotes com uma frequência de 100 por segundo. Assim havia 6 fluxos a gerar 100 pacotes/segundo de, em média, 110bytes, o que perfaz um total de 66000 bytes/segundo (66Kbytes). Este valor é em muito inferior ao débito teórico das ligações wireless.

Experimentou-se então usar apenas uma ligação bidireccional UDP a gerar 5 pacotes de 118bytes/segundo. Assim, havia 2 fluxos de 590bytes, dando uma total de 1180bytes. Este valor é mais de mil (1000) vezes inferior ao débito teórico da ligação, sendo possível observar a não existência de perdas de pacotes.

Com o *MIPv6 Tester* configurado no MN como servidor, e no R1 como cliente, e com a ligação bidireccional de 5 pacotes/segundo activa, realizaram-se 10 movimentos com o MN, alternadamente da rede origem para a visitada e vice-versa, conforme se ilustra na figura.

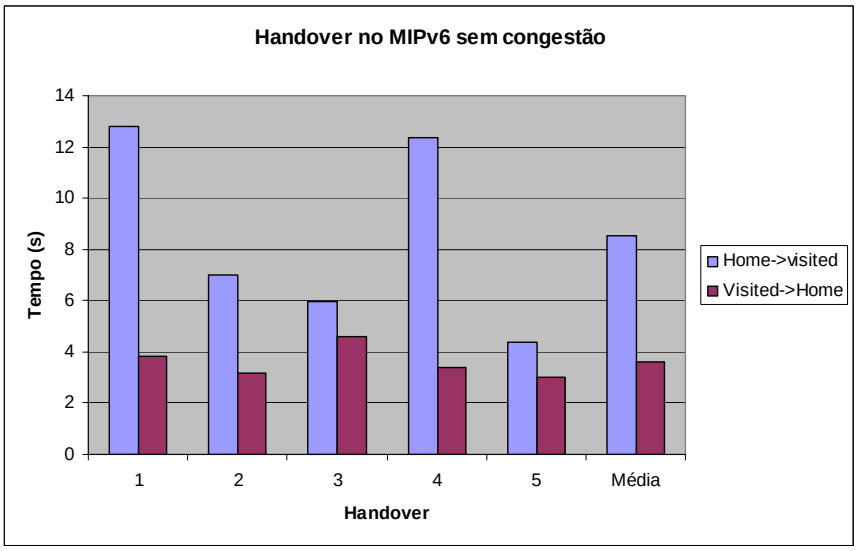


figura 61 - Tempo dos *handovers* do MN durante o roaming.

A primeira conclusão que se pode tirar é que os *handovers* são bastante longos, o que será crítico numa comunicação em tempo real. Outra conclusão é que os *handovers* no sentido da rede origem são bastante mais rápidos.

A tabela seguinte mostra o tempo de duração dos *handovers* do teste anterior.

Handover	Home->visited	Visited->Home
1	12,817	3,806
2	6,985	3,199
3	5,987	4,59
4	12,373	3,406
5	4,366	2,99
Média	8,5056	3,5982

tabela 4 - Registo dos tempos dos *handovers*.

Experimentou-se fazer novamente os testes mas aumentando a frequência de pacotes/segundo para 10. Foi possível verificar que existia já perdas de pacotes durante o processo de comunicação normal. Apesar de teoricamente a largura de banda ocupada ser 2fluxos*10pacotes/s*118bytes/s=2360bytes/s, o que é muito inferior à largura de banda teórica de 1,375Mbytes dos *links wireless*, existia congestão. Uma possível explicação poderá ser o facto de existirem na proximidade vários equipamentos a operar na mesma banda de frequência (2.4Ghz), nomeadamente AP´s da rede e-U e portáteis. As duas redes *ah-hoc* foram configurados em dois canais diferentes da banda dos 2.4Ghz, existindo AP´s a operar nos mesmos canais das células *ad-hoc* configuradas.

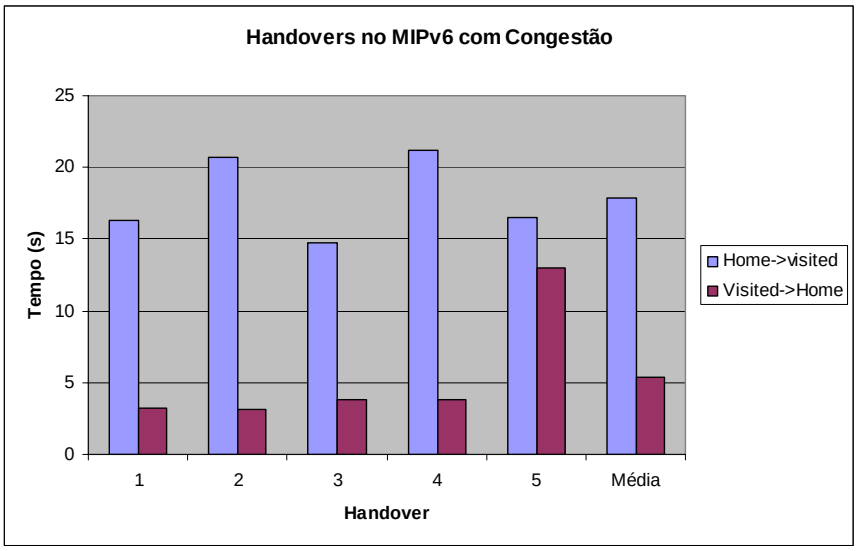


figura 62 - *Handovers* do MN durante o roaming com a ligação UDP a 10pacotes/s.

A tabela seguinte contém o registo dos tempos de *handover* dos testes anteriores

Handover	Home->visited	Visited->Home
1	16,336	3,191
2	20,72	3,096
3	14,747	3,798
4	21,227	3,825
5	16,465	13,025
Média	17,899	5,387

tabela 5 - Registo dos tempos dos *handovers*.

É possível verificar que o tempo de *handover* aumentou significativamente em relação ao 1ºteste, principalmente nos *handovers* do sentido da rede visitada. A explicação para a maior duração destes poderá dever-se ao tempo de envio de RAs configurado na rede visitada. Recorde-se que na rede origem foi configurado o intevalo mínimo possivel {0.05s;1.5s}, recorrendo ás configurações de mobilidade, e na rede visitada foi configurado um intervalo de {3s;4s}. Deste modo, configurou-se a máquina R2 na rede visitada para enviar RAs com o intervalo de {0.05s;1.5s} e voltou-se a repetir os testes anteriores.

7.7.3 Testes com o intervalo mínimo de envio de RAs

Após ambas as redes A e C estarem a enviar RAs com o intervalo mínimo possível, voltou-se a configurar a configurar o cenário tal como nos testes anteriores. O MIPv6 Tester configurado no MN como servidor, e no R1 como cliente. Com a ligação UDP bidireccional de 5 pacotes/segundo activa, iniciou-se o roaming do MN com 30 movimentos, alternadamente da rede origem para a visitada e vice-versa, conforme se ilustra na figura.

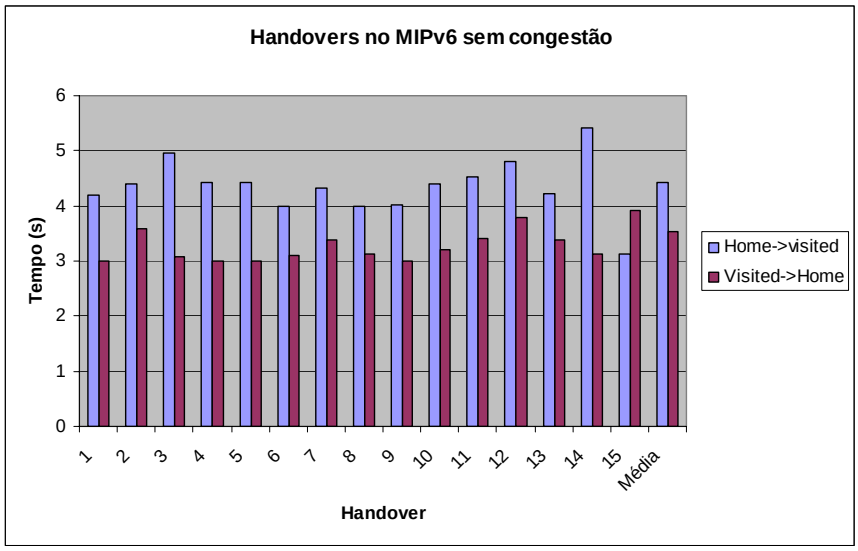


figura 63 - *Handovers* do MN com duas ligações UDP a 5pacotes/s.

A partir da análise da figura, é possível verificar que os *handovers* no sentido da rede visitada continuam mais longos. No entanto, verifica-se que o *handover* no sentido da rede visitada baixou em relação ao 1ºteste realizado.Verifica-se que o intervalo de *handover* ronda os 3 e 5 segundos, o que numa comunicação em tempo real ainda é significativamente crítico se estes se sucederem diversas vezes.

A tabela 6 mostra os valores dos tempos de *handover*.

Handover	Home->visited	Visited->Home
1	4,196	2,992
2	4,405	3,596
3	4,968	3,07
4	4,435	3,01
5	4,417	2,997
6	4,004	3,099
7	4,334	3,393
8	4	3,117
9	4,019	2,993
10	4,405	3,197
11	4,518	3,411
12	4,805	3,796
13	4,23	3,385
14	5,404	3,136
15	3,136	3,926
Média	4,351733	3,274533

tabela 6 - Registo dos tempos dos *handovers*.

Posteriormente analisou-se os dados estatísticos da captura feita durante os testes anteriores.

Pela figura seguinte é possível verificar que a média de bytes/segundo é ligeiramente superior ao débito teórico de 1180bytes calculado anteriormente.

Traffic	Captured
Packets	12498
Bytes	1183748
Between first and last packet	1029,513 sec
Avg. packets/sec	12,140
Avg. packet size	94,000 bytes
Avg. MBit/sec	0,009
Avg. bytes/sec	1149,814

figura 64 - Dados estatísticos da captura de pacotes do MIPv6 Tester no MN.

O facto de este valor ser superior deve-se à existência de mensagens de sinalização a serem constantemente enviadas na rede, nomeadamente Router Advertisements, Router Solicitations, Neighbor Solicitations e Neighbor Advertisements.

O gráfico seguinte mostra o tráfego das ligações do MN durante o seu roaming.

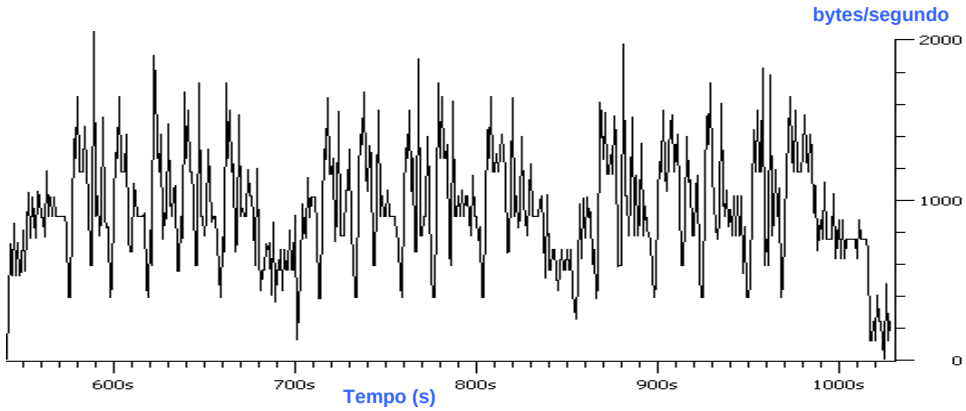


figura 65 - Gráfico do tráfego de rede existente no MN durante o roaming.

O gráfico mostra que o débito médio ronda sensivelmente os 1000bytes/segundo, tal como mencionado anteriormente.

Analisou-se a troca de mensagens dos vários protocolos ao longo da comunicação que registou os 30 *handovers*. A figura seguinte mosta estes dados estatísticos capturados no MN.

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100,00%	12498	1183748	0,009	0	0	0,000
Ethernet	100,00%	12498	1183748	0,009	0	0	0,000
Internet Protocol Version 6	99,83%	12477	1181963	0,009	0	0	0,000
User Datagram Protocol	51,49%	6435	498095	0,004	0	0	0,000
Data	51,49%	6435	498095	0,004	6435	498095	0,004
Internet Control Message Protocol v6	14,90%	1862	198770	0,002	1862	198770	0,002
	2,53%	316	31856	0,000	0	0	0,000
ICMPv6 Internet Control Message Protocol v6	1,32%	165	16366	0,000	165	16366	0,000
Mobile IPv6	1,21%	151	15490	0,000	151	15490	0,000
IPv6 Internet Protocol Version 6	30,53%	3816	449514	0,003	0	0	0,000
User Datagram Protocol	30,22%	3777	443189	0,003	0	0	0,000
Data	30,22%	3777	443189	0,003	3777	443189	0,003
Mobile IPv6	0,02%	2	220	0,000	2	220	0,000
Internet Control Message Protocol v6	0,30%	37	6105	0,000	37	6105	0,000
Mobile IPv6	0,38%	48	3728	0,000	48	3728	0,000
Logical-Link Control	0,17%	21	1785	0,000	0	0	0,000
Internet Protocol Version 6	0,17%	21	1785	0,000	0	0	0,000
User Datagram Protocol	0,17%	21	1785	0,000	0	0	0,000
Data	0,17%	21	1785	0,000	21	1785	0,000

figura 66 - Dados estatísticos durante a comunicação *e handovers* do MIPv6.

É possível observar que a percentagem de mensagens MIPv6 enviadas, quer como mensagens ICMPv6 quer em mensagens IPv6, é relativamente baixa.

A ferramenta ethereal permite ainda vizualizar informação relativa aos pacotes enviados em função dos endereços IPv6 e portos, conforme se ilustra na figura seguinte.

UDP Conversations

Address A	Port A	Address B	Port B	Packets	Bytes	Packets A->B	Bytes A->B	Packets A<-B	Bytes A<-B
2000:a::1	32772	2000:a::40	10103	631	64944	631	64944	0	0
2000:a::1	32771	2000:a::40	10103	1209	111579	1209	111579	0	0
2000:a::1	32770	2000:a::40	10103	4314	395211	4314	395211	0	0
2000:a::40	51811	2000:b::1	10104	310	23762	310	23762	0	0
2000:a::40	53512	2000:b::1	10104	565	53087	565	53087	0	0
2000:a::40	51812	2000:b::1	10104	568	50331	568	50331	0	0
2000:a::40	52704	2000:b::1	10104	577	51497	577	51497	0	0
2000:a::40	46728	2000:b::1	10104	991	90138	991	90138	0	0
2000:a::40	48912	2000:b::1	10104	1068	102520	1068	102520	0	0

figura 67 - Fluxos existentes no MN durante os testes realizados.

Importa referir que os endereços 2000:a::1 e 2000:b::1 pertencem ambos à máquina R1, encontrando-se atribuidos a duas interfaces distintas.

Analisou-se também a captura de tráfego realizada no túnel do MN e obteve-se o gráfico apresentado na figura 68.

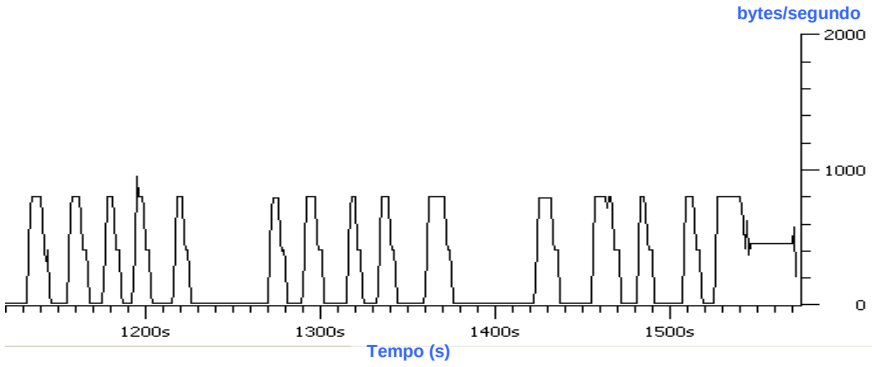


figura 68 - Captura de tráfego no túnel do MN.

Neste é notória a existência dos 30 *handovers*. O túnel só é activado quando o MN se move para a rede visitada, e assim que regressa à rede origem, este é desactivado. Cada "pico" corresponde a dois *handovers*, um que activa o túnel, e o outro que desactiva.

A análise do tráfego ilustrada na figura seguinte permite observar que a percentagem de tráfego do MIPv6 no túnel também é relativamente baixa.

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
⊟ Frame	100,00%	5663	450642	0,002	0	0	0,000
⊟ Linux cooked-mode capture	100,00%	5663	450642	0,002	0	0	0,000
⊟ Internet Protocol Version 6	100,00%	5663	450642	0,002	0	0	0,000
⊟ User Datagram Protocol	99,28%	5622	445655	0,002	0	0	0,000
Data	99,28%	5622	445655	0,002	5622	445655	0,002
Mobile IPv6	0,07%	4	288	0,000	4	288	0,000
Internet Control Message Protocol v6	0,65%	37	4699	0,000	37	4699	0,000

figura 69 - Análise do tráfego do túnel no MN associado aos protocolos.

As poucas mensagens MIPv6 existentes correspondem à tentativa do MN efectuar o binding no R1 (*return routability procedure*), que é o router com o qual está a comunicar. No entanto como este não tem configurada a funcionalidade de CN não aceita o binding, devolvendo mensagens de *parameter problem* como resposta às mensagens MIPv6 recebidas.

Experimentou-se fazer novamente os testes mas aumentando a frequência de pacotes/segundo para 10. A figura seguinte apresenta o resultado de 30 *handovers* realizados alternadamente no sentido da rede visitada e rede origem.

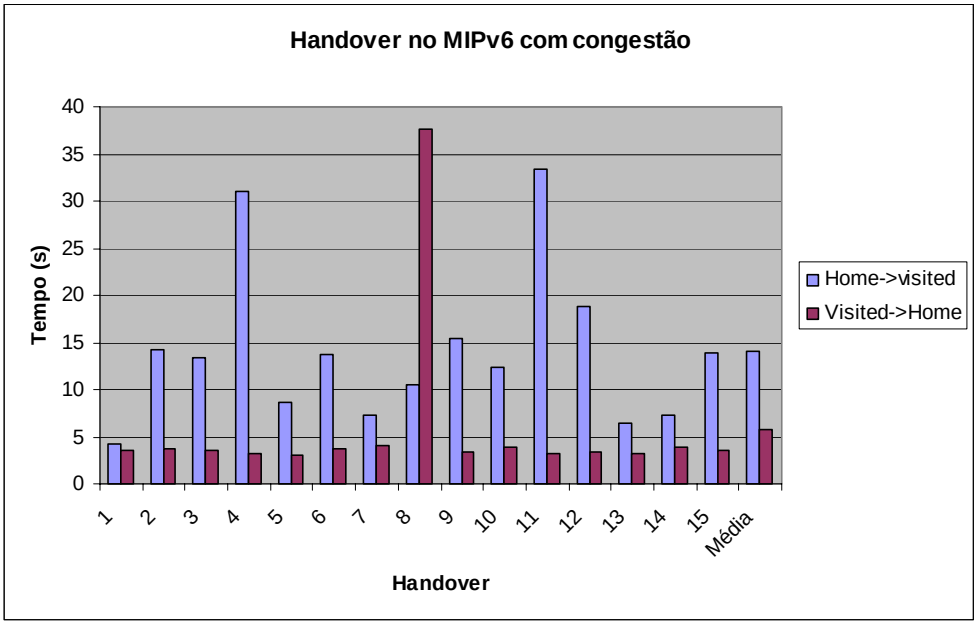


figura 70 - *Handovers* do MIPv6 realizados com alguma congestão.

É possível verificar que o tempo dos *handovers* subiu ligeiramente para o caso dos *handovers* no sentido da rede origem, e subiu substâncialmente para o caso dos no sentido da rede visitada. No teste anterior o intervalo do *handover* ía de 3 a 4 segundos, e neste caso vai de 4 a 38. A média era de

3,5segundos para os *handovers* no sentido da rede origem, e 4,5 no sentido da rede visitada, subindo agora para 5,5 e 14 segundos respectivamente.

Na tabela seguinte são apresentados os tempos associados aos *handovers* anteriores.

Handover	Home->visited	Visited->Home
1	4,194	3,603
2	14,191	3,697
3	13,358	3,597
4	31,067	3,193
5	8,604	3,118
6	13,72	3,796
7	7,303	4,013
8	10,444	37,579
9	15,5	3,426
10	12,429	3,82
11	33,405	3,297
12	18,81	3,423
13	6,507	3,271
14	7,22	3,914
15	13,92	3,62
Média	14,0448	5,824467

tabela 7 - Registo do tempo dos *handovers*.

O gráfico seguinte corresponde ao tráfego capturado no MN ao longo dos testes que envolveram o *roaming* entre as redes.

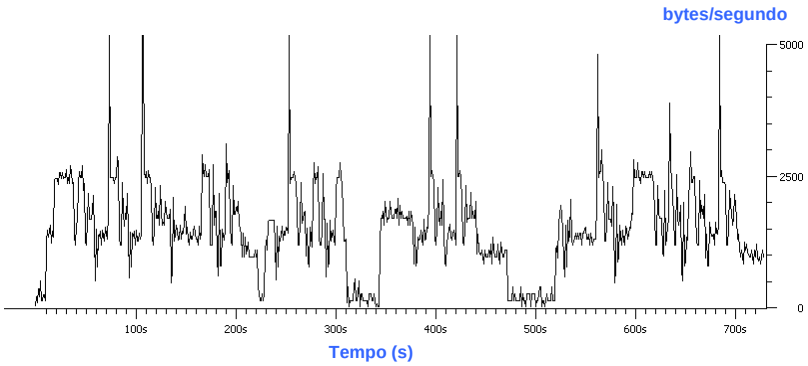


figura 71 - Tráfego capturado no MN ao longo destes testes

O gráfico seguinte corresponde ao tráfego capturado no túnel do MN.

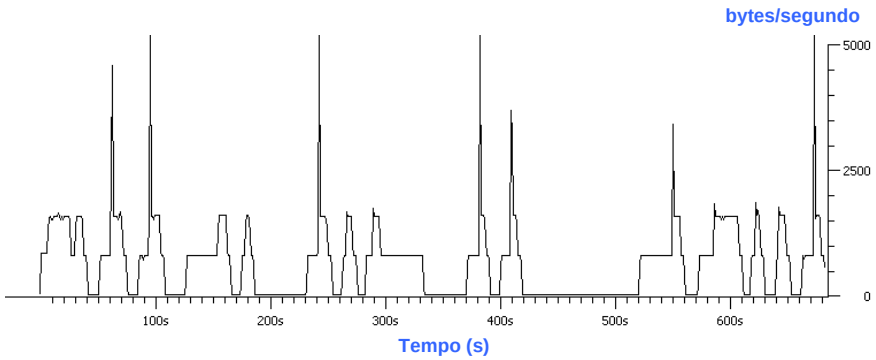


figura 72 - Tráfego capturado no túnel ao longo destes testes.

Após este teste, pretendeu-se verificar como evolui o tempo de *handover* com a congestão. Para isso aumentou-se a frequência de envio de pacotes para 20 e obteu-se o resultado apresentado na figura seguinte.

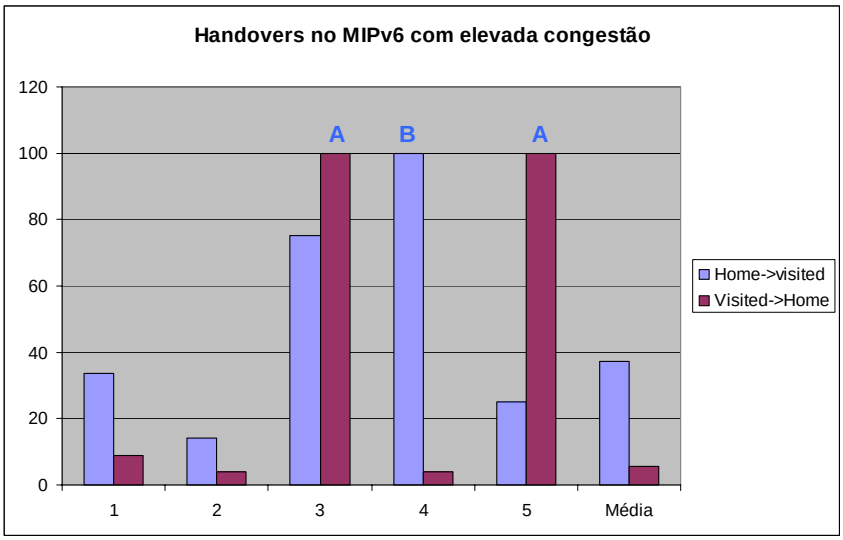


figura 73 - *Handovers* no MIPv6 com duas ligações UDP a enviar 20 pacotes/s.

Os *handovers* identificados na figura 73 por "A" nunca chegaram a ocorrer (excederam o tempo de 250segundos). O *handover* identificado por B também não chegou a ocorrer. Uma vez que o anterior não existiu, então o registo no HA e o túnel não foram desfeitos, e assim que o MN voltou à rede visitada, continuou a comunicar sem estabelecer novo registo. No caso dos valores médios apresentados, estes três "*handovers*"(tentativas de *handover*) não foram considerados, como se pode observar na tabela 8 .

Handover	Home->visited	Visited->Home
1	33,79	8,89
2	14,294	4,045
3	75,229	---
4	---	3,841
5	25,089	---
Média	37,1005	5,592

tabela 8 - Registo do tempo dos *handovers*.

Experimentou-se aumentar ainda mais o tráfego da ligação bidireccional UDP para 100 pacotes/s. Este é o valor máximo permitido pelo MIPv6 Tester, sendo que o mínimo é de 1 pacote/s. Para aumentar ainda mais o tráfego poder-se-ia usar as outras duas ligações bidireccionais disponíveis (UDP e TCP), mas foi usada apenas a ligação UDP. A figura seguinte mostra o teste referente a 10 *handovers*.

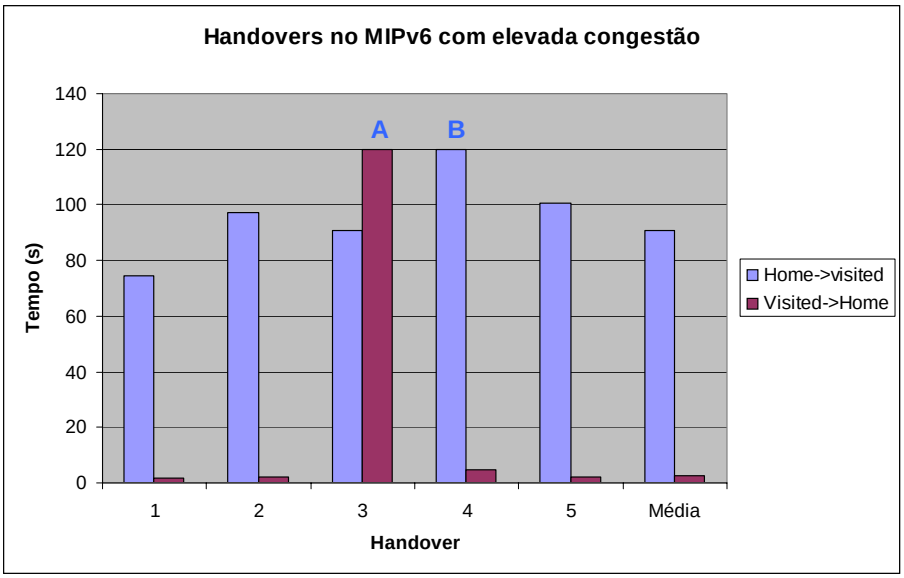


figura 74 - *Handovers* no MIPv6 com duas ligações UDP a enviar 100 pacotes/s.

Nos *handovers* identificados por "A" e "B" sucedeu o mesmo que no teste anterior, e estes não chegaram efectivamente a acontecer. Um dado curioso é que o *handover* no sentido da rede origem baixou para um valor médio abaixo dos três segundos. Aparentemente a ligação *wireless* existente na rede origem (célula *ad-hoc* com um único canal de frequência) poderá não estar a ser tão afectada pelas interferências externas dos APs a operar na mesma frequência como a ligação da rede visitada.

A tabela seguinte contém os valores do tempo de *handover* deste teste.

Handover	Home->visited	Visited->Home
1	74,305	1,669
2	97,021	2,336
3	90,656	---
4	---	4,886
5	100,4	2,056
Média	90,5955	2,73675

tabela 9 - Registo do tempo dos *handovers*.

Estes foram os testes realizados referentes ao cenário *wireless* configurado. Muitos outros poderiam ser feitos, no entanto os apresentados permitem já retirar bastantes conclusões.

7.8 Conclusões

Estes testes vieram comprovar a necessidade dos protocolos de microMobilidade já mencionados anteriormente. Sendo que o *handover* é mais crítico no sentido da rede origem, o HMIPv6 poderia ser usado para reduzir a sinalização existente entre o MN, o HA e o CN. O FMIPv6 seria usado para reduzir o tempo de *handover*. A utilização destes protocolos é apresentada como proposta de trabalho futuro no capitulo 10. Propõem-se a implementação e configuração de mecanismos de micromobilidade num cenário já configurado com MIPv6. Tendo como base os testes e resultados apresentados nesta secção, poderá ser feito um estudo comparativo, de modo a perceber as vantagens do uso destes protocolos.

Também foi possível verificar que num estado de congestão da rede, os *handovers* demoram mais tempo. Estes estão assim dependentes da largura de banda e do estado de congestão da rede.

A frequência de envio dos *Routers Advertisements* também é um factor que influência a detecção de movimento e por isso influência o *handover*. É a partir dos RAs recebidos, e da informação neles contida que o MN gera o seu CoA. A periodicidade destes RAs irá influenciar o desempenho do *handover*.

8. Testes com a rede da FCCN

De modo a permitir realizar testes entre distintos Sistemas Autónomos (SAs) recorreu-se à plataforma de testes disponibilizada pela FCCN. Pretendia-se testar o funcionamento e o desempenho do MIPv6 através de redes distintas na Internet.

No contexto de projectos IPv6 em curso, a FCCN disponibiliza duas plataformas de testes - uma em Lisboa e outra no Porto - com conectividade ao *Backbone* da RCTS.

Trabalhos científicos, no âmbito de teses, projectos de investigação ou realização de projectos de cadeiras curriculares, que possam beneficiar da disponibilidade da infra-estrutura de experimentação, poderão então candidatar-se à sua utilização. O acesso distribuído (a ambas as plataformas) também será possível, se necessário.

Não foi possível resolver em tempo útil alguns problemas de modo a permitir realizar testes exaustivos de mobilidade. No entanto, documenta-se o trabalho de configuração do cenário para testes futuros.

8.1 Cenário existente

A ESTG encontra-se ligada à Internet por intermédio da FCCN. Neste momento, para além da ligação IPv4, já se encontra configurada uma ligação IPv6 nativa. Assim na ESTG é já possível ter um domínio IPv4 e outro IPv6, ambos com acesso à Internet.

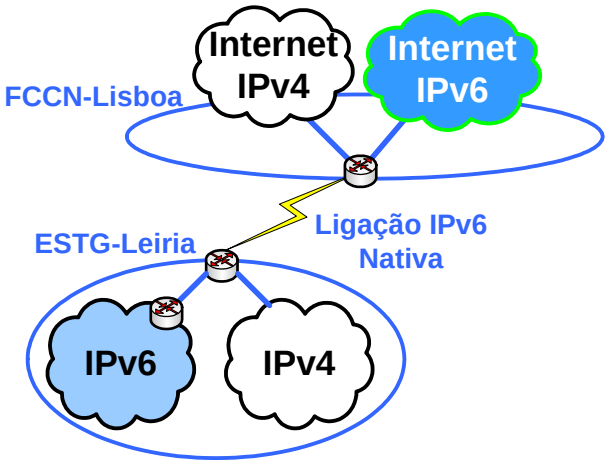


figura 75 - Ligação IPv6 nativa da ESTG para a FCCN.

A ESTG tem atribuída a gama de endereços IPv6 2001:690:2060::/48.

Inicialmente antes de existir a ligação IPv6 nativa, o *router* de acesso, um Cisco 2600, tinha apenas uma interface *Ethernet* que servia toda a rede. A ligação à FCCN era realizada através de uma interface ATM com um PVC com encapsulamento "aal5mux ip".

De modo a estabelecer a ligação IPv6 nativa entre a FCCN e a ESTG, foi instalado um *router* Cisco 2621-XM com suporte IPv6 e duas interfaces *FastEthernet*, de forma a se poder separar internamente o tráfego IPv4 e IPv6. Uma das interfaces *FastEthernet* ficou para a rede IPv4 e outra para a rede IPv6 pura. Para se poder ter tráfego IPv6 puro na ligação ATM existente foi necessário alterar o encapsulamento do PVC de "aal5mux ip" para "all5snap" (comando "encapsulation all5snap") nos dois lados da ligação. Na interface ATM do *router* da ESTG foi necessário configurar, para além do endereço IPv4 193.136.1.146, o endereço IPv6 2001:690:810:14::2/64 (comando "ipv6 address 2001:690:810:14::2/64"); na interface ATM do lado da FCCN foi configurado o endereço 2001:690:810:14::1/64.

Na figura seguinte é apresentado o cenário da ligação da ESTG à Internet, com IPv4 e IPv6.

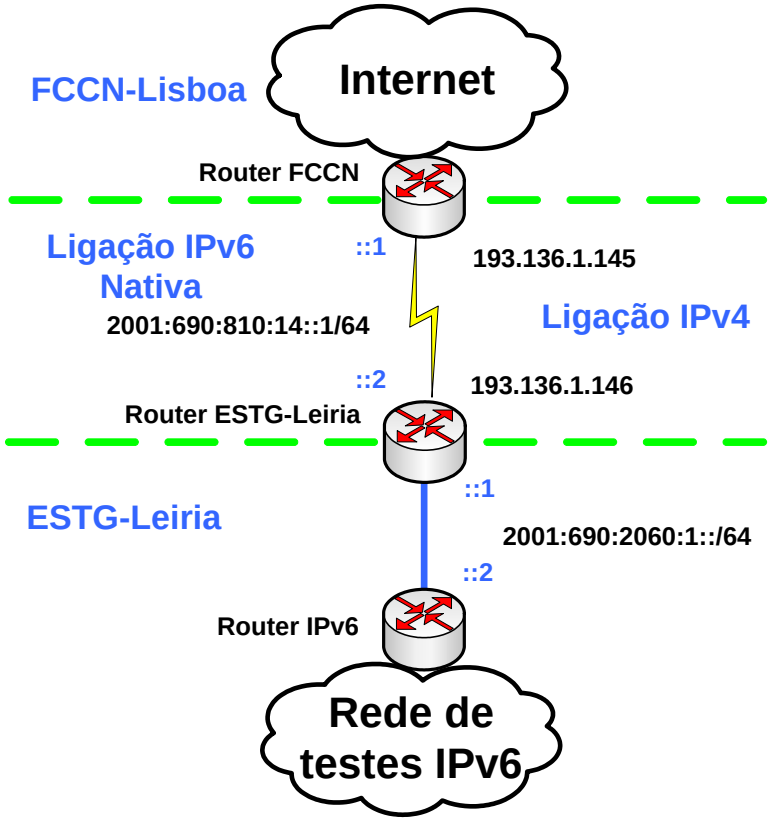


figura 76 - Ligação entre a FCCN e a ESTG

Como se pode observar pela figura anterior, também foi estabelecida uma ligação entre o *router* que faz de *gateway* na ESTG e um *router* instalado no Laboratório de Comunicações Avançadas (LCA), de modo a permitir realizar testes diversos com a ligação nativa IPv6.

8.2 Cenário configurado para testes MIPv6

De modo a permitir a realização de testes de Mobilidade IPv6, partiu-se do cenário anterior e configuraram-se mais algumas máquinas.

Na interface *FastEthernet* do *router* IPv6 do LCA com o endereço 2001:690: 2060:2::1/64, ligou-se um *switch* de modo a permitir ligar várias máquinas de teste, evitando alterar as configurações do *router* IPv6 principal que liga ao *gateway*.

Nas interfaces e*thernet* que ligam ao *switch* serão configurados endereços da rede 2001:690:2060:2::/64, sendo os endereços configurados segundo o modelo 2001:690:2060:2::Fx/64, sendo 'x' o número da interface *FastEthernet* do *switch* à qual se liga o *router*, F1, F2... F10.

A partir dos *routers* que se ligam ao *switch* poderão ser usadas quaisquer redes do prefixo base (2001:690:2060::/48), sendo apenas necessário configurar no *router* principal rotas para essas redes. De modo a haver uniformidade no uso dessas redes, convencionou-se o uso de redes segundo o prefixo 2001:690:2060:FF::/52, variando os 8bits seguintes ao FF (2 dígitos hexadecimais), ou seja, FFxx, do género FF01, FF02, (…) FFEF.

A figura seguinte ilustra o cenário de testes MIPv6 configurado.

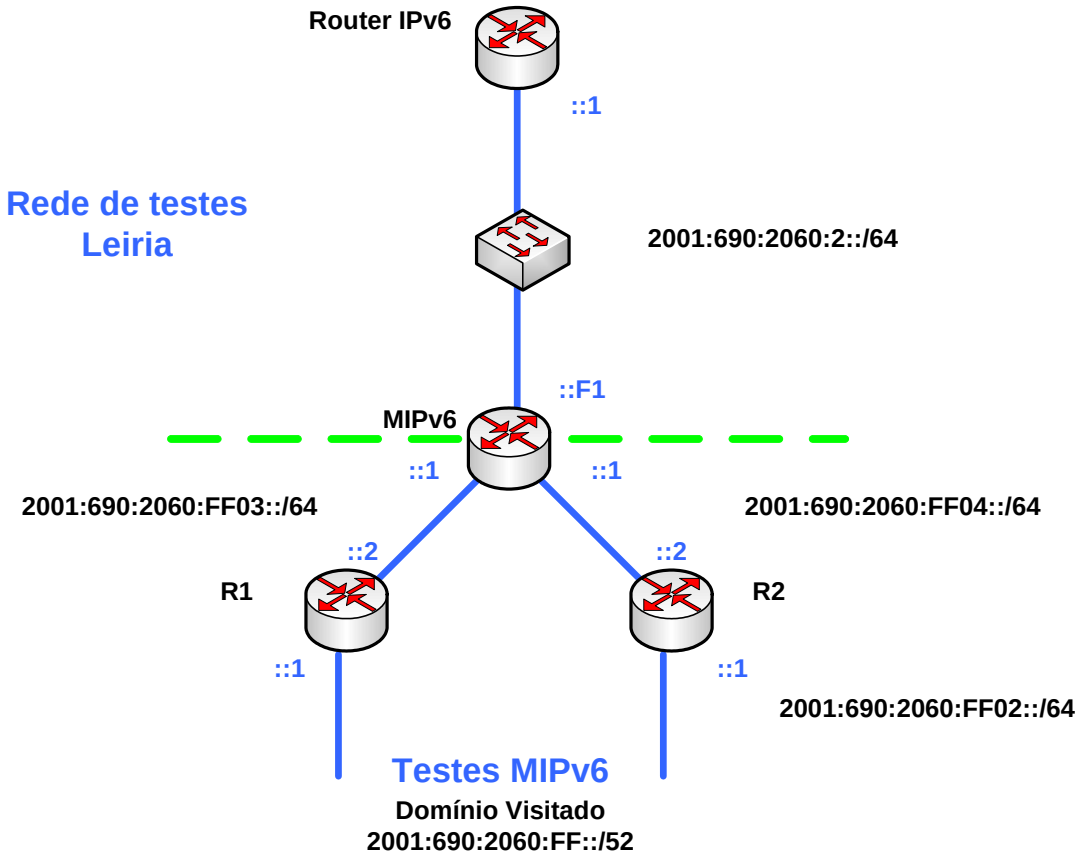


figura 77 - Rede de testes MIPv6.

De referir que neste cenário, a ESTG irá fazer de domínio visitado em relação ao terminal móvel usado nos testes.

A rede IPv6 da ESTG também possui um servidor DNS para resolução de nomes IPv6, mas neste cenário IPv6 não foi necessário o seu uso, mas em todo o caso bastava fazer as configurações necessárias no servidor existente no laboratório junto ao *router* IPv6.

Do lado da FCCN foi configurado um *router* que se encontra ligado ao mesmo segmento *ethernet* do *router* que liga a ESTG/IPL. Na rede de testes da FCCN os *routers* correm o protocolo de encaminhamento OSPF3 (incluindo o *router* de testes MIPv6) e por isso não são precisas configurações de rotas adicionais.

A figura seguinte ilustra o cenário configurado na FCCN.

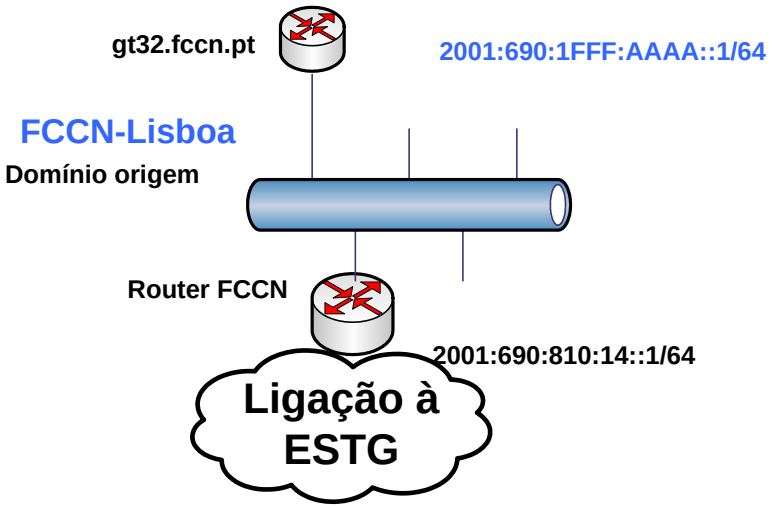


figura 78 - Cenário de teste MIPv6 configurado na FCCN

O rede da FCCN foi configurada como sendo a rede origem do terminal Móvel, e o *router* gt32 foi configurado como sendo o servidor agente de mobilidade (*Home Agent*).

Assim, a rede em Lisboa na FCCN será a rede origem, e a rede em Leiria na ESTG será o domínio visitado, onde serão realizados os testes. De modo a dar a ordem de grandeza das distâncias entre as duas redes, poder-se-á dizer que entre Lisboa e Leiria são cerca de 150km. Assim, uma comunicação bidireccional, por exemplo, um teste de conectividade com pedido e resposta, implica uma comunicação de 300kms, com o pedido e a resposta a fazerem o mesmo percurso mas em sentido inverso, causando assim algum *delay*.

O cenário final completo ficou semelhante ao representado na figura 78.

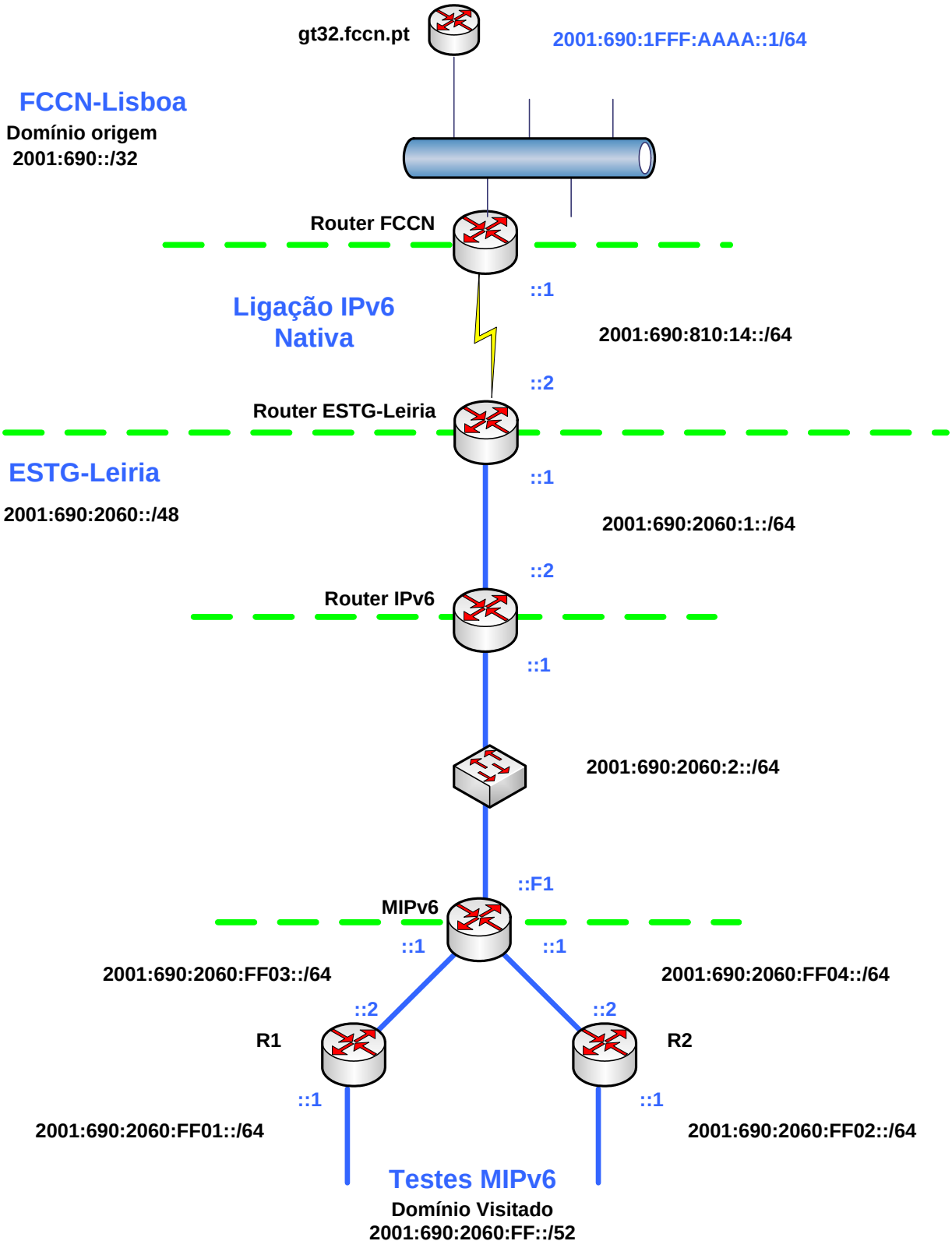


figura 79 - Cenário final de testes MIPv6 completo.

De modo a simplificar o esquema anterior pode-se suprimir a ligação IPv6 já existente, ou seja, o cenário que já se encontrava configurado, conforme se ilustra na figura 79.

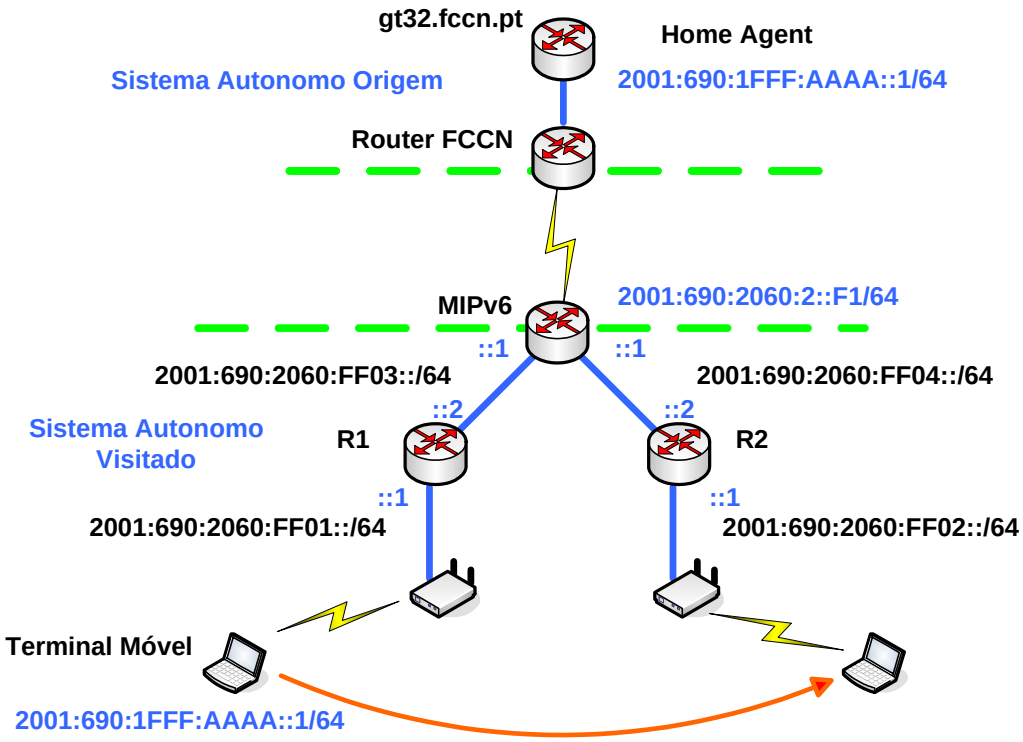


figura 80 - Esquema de testes MIPv6 configurado.

O cenário construído permite realizar diversos testes envolvendo a mobilidade.

Um deles é o teste de *performance* do *handover* durante uma comunicação. Estabelece-se um ou vários fluxos com diferentes débitos, e durante estes experimenta-se fazer o *handover* sucessivas vezes e observar o comportamento. O *handover* encontra-se muito dependente das configurações do terminal móvel, *Home Agent* e da frequência dos *Router Advertisements* nos *link* visitados.

Outro teste consiste em estudar a performance introduzida com a optimização de rotas. Usando uma máquina a fazer de CN na rede visitada em Leria, primeiro sem suporte de optimização de rotas, implicando que todos os pacotes tenham de ir de Leiria até ao HA em Lisboa, e depois com optimização de rotas existindo comunicação directa entre CN e MN.

8.3 Equipamento Usado

Na rede da FCCN apenas dois *routers* interessam para este cenário, o *gateway* que liga à ESTG e o *router Home Agent* MIPv6, o gt32.

O gt32, que é o que está relacionado com os testes MIPv6, é um Cisco 7200 Software (C7200-ADVIPSERVICESK9-M), com versão do IOS 12.4(4)T1.

Do lado da rede da ESTG, para além dos dois *routers* Cisco 2621XM que fazem de "*gateway*" e "*Router* IPv6", foram usados mais 1 *Switch* Cisco, e 3 *routers* Cisco 2600 (C2600-ADVENTERPRISEK9-M), com a versão da imagem do IOS 12.4(5).

Foram também usados dois AP´s “Cisco séries 1200” e placas PCI “Aironet” com suporte da norma 802.11b a 11 Mbps.

Por ultimo foi usado um PC com sistema operativo Fedora Core 3 e outro com sistema operativo Windows XP.

8.4 Configurações

Nesta secção apresenta-se apenas as configurações relativas ao cenário de Mobilidade IPv6.

8.4.1 Configuração do router na rede da FCCN

Foram configurados os seguintes comandos no *router* de testes (*Home Agent*):

```
hostname HomeAgent
ipv6 unicast-routing
interface FastEthernet0/0
  ipv6 enable
  no shutdown
  ipv6 address 2001:690:1FFF:AAAA::1/64
  ipv6 mobile home-agent
```

O endereço configurado na interface do *router*, atribuído da gama da rede ipv6 da FCCN é o 2001:690:1FFF:AAAA::1/64

NA FCCN não foi configurada nenhuma rota para a ESTG, uma vez que o *router* de testes está a correr OSPF3, encontrando-se ligado ao mesmo segmento *ethernet* do *router* que liga à ESTG/IPL. Assim o *router* já tinha “conhecimento” da rede 2001:690:2060::/48, que é a gama de endereços atribuída à ESTG.

Em todo o caso, a rota a configurar para a ESTG seria algo do género:

```
ipv6 route 2001:690:2060::/48 GATEWAY
```

em que GATEWAY representa o endereço IPv6 do *router* de acesso à ESTG.

Este *router* servirá então para actuar como *Home Agent* na rede origem do terminal móvel, no qual seria realizado o registo (*binding update*) do MN. Servirá também para informar os CNs da localização do MN, ou para redirreccionar o tráfego das comunicações entre ele e máquinas sem suporte de MIPv6.

De modo a ser possível visualizar as estatísticas dos registos de mobilidade foi facultado o acesso para gestão remota ao *router* gt32.

```
Router#
Router#telnet 2001:690:1fff:aaaa::1
Trying 2001:690:1FFF:AAAA::1 ... Open

---                LISBOA - ROUTER 32                ---
---  ------------------------------------------------  ---
---        UNAUTHORISED ACCESS IS PROHIBITED          ---
---  Entradas nao autorizadas sao punidas por lei     ---
---            (lei 109/91 de 17 Agosto)             ---


User Access Verification

Username:
Password:

% Authentication failed

Username:
Password:

gt32>
gt32>exit

[Connection to 2001:690:1fff:aaaa::1 closed by foreign host]
Router#
```

figura 81 - Acesso para gestão remota ao *router* gt32.

A figura anterior mostra o acesso realizado após a configuração do cenário, através de uma sessão *telnet*.

8.5 Configurações do cenário de teste na ESTG

No cenário de testes no laboratório da ESTG teve de ser implementada conectividade IPv6 entre os *routers*, as máquinas e a rede da FCCN.

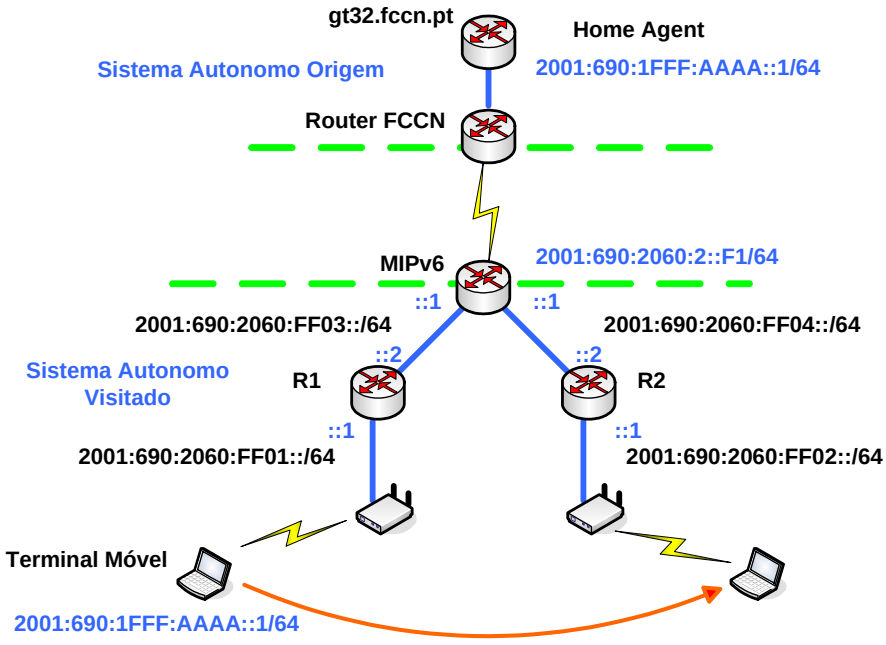


figura 82 - Esquema de testes MIPv6 configurado.

Foram configuradas duas redes distintas de modo a permitir estudar a mudança de rede pelo terminal móvel. Os *access points* foram configurados com autenticação aberta e com diferentes identificadores (ESSIDS).

O MN configurado foi uma máquina Linux, cujas configurações são apresentadas no tutorial no Anexo D, sendo a máquina XP usada para comunicar com o MN. Primeiro foi configurada para comunicar apenas em IPv6, e depois foi configurada com suporte da funcionalidade de CN do MIPv6.

Os primeiros teste realizados foram os de conectividade IPv6, uma vez que para os testes de Mobilidade IPv6 seria necessário ter um cenário completamente funcional. Usando o utilitário *ping*, verificou-se a conectividade entre extremos, nomeadamente entre o gt32 e os *routers* R1 e R2.

Primeiro testou-se a partir de Leiria no *router* R1:

```
Router#ping 2001:690:1fff:aaaa::1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:690:1FFF:AAAA::1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/150/168 ms
Router#
```

figura 83 - Teste de conectividade entre os *routers* R1 e R2 e o *router* gt32.

Depois testou-se a conectividade a partir de Lisboa no *router* gt32:

```
gt32>ping 2001:690:2060:ff04::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:690:2060:FF04::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/65/104 ms
gt32>
gt32>ping 2001:690:2060:ff03::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:690:2060:FF03::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/41/44 ms
gt32>
```

figura 84 - Teste de conectividade entre o *router* gt32 e os *routers* R1 e R2.

Uma primeira conclusão que se pode obter imediatamente a partir destes testes é que o *round-trip time* é mais elevado no sentido Leiria – Lisboa. Este deverá ser um factor a ter em conta nos testes MIPv6.

Depois do cenário configurado em IPv6 totalmente funcional, poder-se-á partir para os testes de performance da Mobilidade IPv6.

8.6 Teste e Resultados

Como já referido anteriormente, não foi possível em tempo útil resolver o problema que impediu a realização de testes exaustivos e conclusivos, nomeadamente a rejeição dos pacotes MIPv6 (gerados pelo terminal móvel Linux) por parte dos *routers* Cisco.

O cenário foi construído e configurado, apresentando-se totalmente funcional em termos de comunicação IPv6. O problema ocorrido dever-se-á a problemas com alguma das implementações usada, nomeadamente a MIPL e a do IOS. Relembre-se que a versão do MIPL usada não foi a final, apresentado ainda alguns erros e instabilidade (a versão final saiu dias antes da conclusão deste projecto). A implementação em IOS do MIPv6 também não apresenta a totalidade das funcionalidades do MIPv6 e é possível que ainda apresente problemas devido à sua imaturidade.

Uma vez mais, o objectivo destes testes será estudar de que forma o *handover* MIPv6 é afectado com a distância em relação à rede origem, e a performance introduzida na comunicação com o processo de optimização de rotas entre os MNs e os CNs. Num trabalho futuro no âmbito da mobilidade IPv6 poderá ser intensificada a realização de testes exaustivos usando o cenário apresentado (caso a FCCN ainda disponibilize as plataformas de testes). Entretanto deverão sair novas versões do MIPL actualizadas e corrigidas bem como novas versões do IOS com a totalidade das funcionalidades do MIPv6. Nessa altura poderão então ser realizados testes conclusivos. Poder-se-á usar também implementações de outros sistemas operativos, comprovar a sua funcionalidade e interoperabilidade. O teste de desempenho da mobilidade das diversas implementações também poderá ser apresentado.

9. Implementação de MIPv6 no e-U

O projecto e-U[4] (universidade electrónica) foi um projecto lançado pelo governo, pioneiro e inédito a nível mundial. Consiste numa rede *WiFi* integrada em todas as instituições de ensino superior nacionais. Tornou-se num *Case Study* para os países mais evoluídos e para as principais empresas mundiais como a Cisco, Microsoft ou a Intel.

Uma vez que o IPLeiria possui uma infra-estrutura e-U implementada em todos os *campus* das suas instituições, efectuou-se o estudo sobre a viabilidade de realização de testes de Mobilidade IPv6 na rede e-U. A realização de testes de mobilidade entre os seus *campus* ou diferentes edifícios com diferentes redes ou subredes configurados seria objectivo final. Não tendo sido possível em tempo útil, os testes terão início após a conclusão deste projecto, com vista a testar e implementar o MIPv6 na rede e-U.

9.1 Estudo da infra-estrutura de rede

Sendo a ESTG e o *campus* do Edifício Sede IPLeiria (será usado apenas IPL para simplificar), os dois pontos mais importantes ao nível da rede e-U, uma vez que é nestes que residem as principais estruturas, serviços, servidores, e gestores, procurou-se aplicar os testes entre estes dois *campus*. A figura seguinte mostra a localização destes dois campos na periferia da cidade de Leiria.

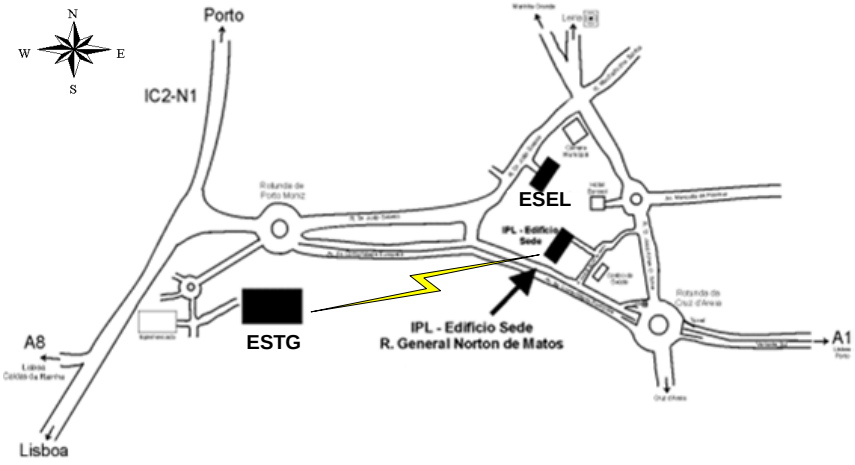


figura 85 - Localização do campus do central do IPL, da ESTG e da ESEL.

Toda a infra-estrutura central da rede se encontra na ESTG. Os elementos do projecto e-U no IPLeiria fazem parte da Incubadora de Empresas localizada no IPL.

[4] Sítio do projecto e-U: http://www.e-u.pt

A realização dos testes de Mobilidade implica a colaboração de elementos responsáveis pelas redes nas duas infra-estruturas. Numa primeira abordagem procurou-se com o auxílio dos membros do projecto e-U no IPL fazer o levantamento dos requisitos.

Primeiro procurou-se conhecer a natureza da ligação entre os dois *campus* e a estrutura básica da rede.

Depois de conhecer a infra-estrutura e definir alguns dos requisitos básicos para os testes, através de testes em laboratório, realizou-se uma reunião com os elementos do projecto e-U de modo a conhecer outros requisitos do cenário real, fazer um levantamento da estrutura mais especifica da rede, das configurações e dos serviços usados bem como os sistemas operativos e aplicações usados.

Do lado da ESTG, a reunião com o elemento do Centro de Informática (CI) responsável da rede permitiu conhecer em pormenor o estado actual da estrutura da rede do *campus* da ESTG, os equipamentos usados e as ligações existentes. Também se ficou a conhecer o que deveria ser realizado para se configurar a ligação em IPv6 nativa para o IPL.

A figura seguinte representa de uma forma genérica a rede de todo o Instituto.

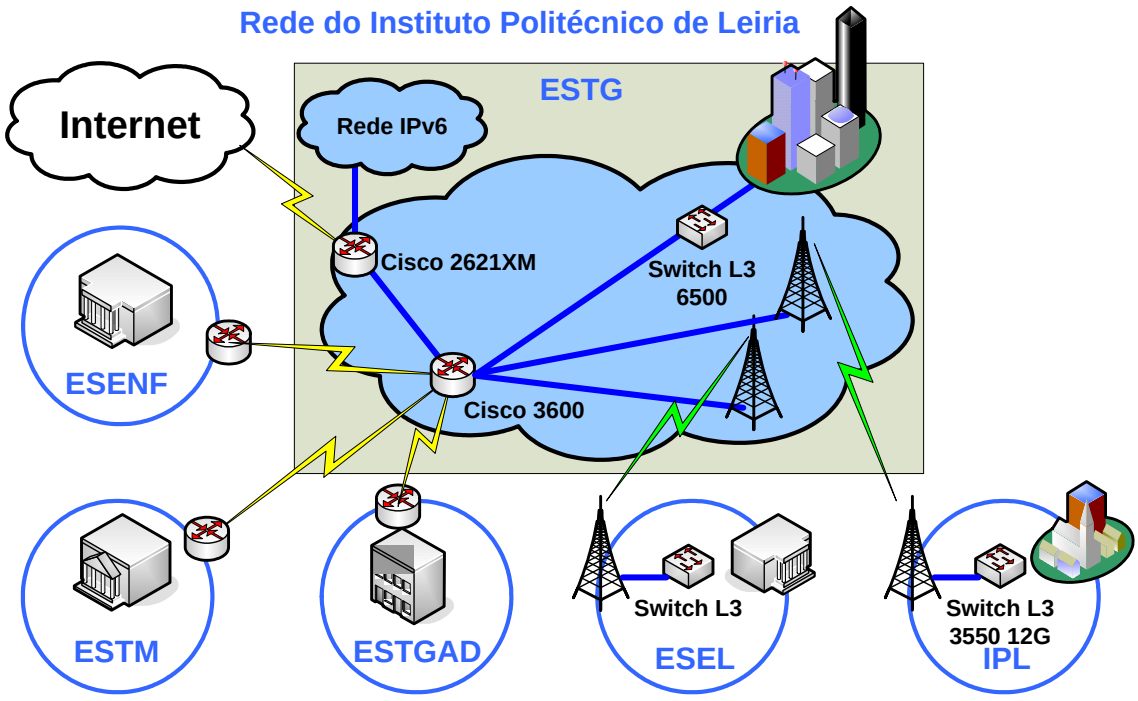


figura 86 - Rede do instituto politécnico de Leiria.

Pode-se então observar que todas as instituições (incluindo o IPL) se ligam à ESTG por intermédio de um *router* Cisco 3600. No *campus* do IPL, o extremo da ligação *wireless* termina num *Switch Layer* 3 Cisco 3550. Existe na ESTG um Switch Layer 3 Cisco 6500 que interliga toda a rede interna da ESTG. O *gateway* da rede é um Cisco 2621-XM. Este já possui uma ligação em IPv6 nativa para o exterior e uma ligação numa *FastEthernet* para a rede piloto IPv6 interna.

O objectivo será estender a rede IPv6 de testes da ESTG até ao *campus* da sede do IPL.

A figura resume a estrutura da rede e o percurso do IPL até à Internet e à rede IPv6.

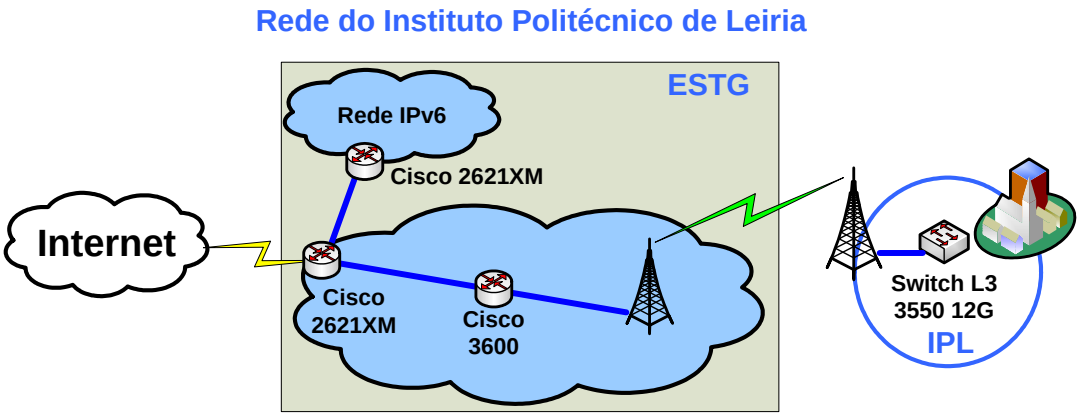


figura 87 - Ligação do IPL à Internet e à rede IPv6 nativa

Pela figura pode-se constatar que para estender a rede IPv6 até à sede do IPL, terá de se configurar o *router* Cisco 3600 e o *switch layer* 3550 com suporte IPv6 e MIPv6. O *gateway* já está configurado para encaminhar o tráfego entre a FCCN e a rede IPv6 interna, e por isso teria de se acrescentar rotas para encaminhar o tráfego para a rede do IPL.

9.2 Testes de Mobilidade

Antes de avançar para os testes de mobilidade foram definidos os cenários de teste que se pretendiam realizar, e em função destes foi realizado um levantamento das dos requisitos e limitações existentes.

A figura seguinte mostra alguns dos testes possíveis em MIPv6. Existem dois Sistemas Autónomos (SAs), cada um com várias subredes, nos quais poderão existir *handovers* entre subredes do SA origem, entre os SAs e entre subredes do SA visitado.

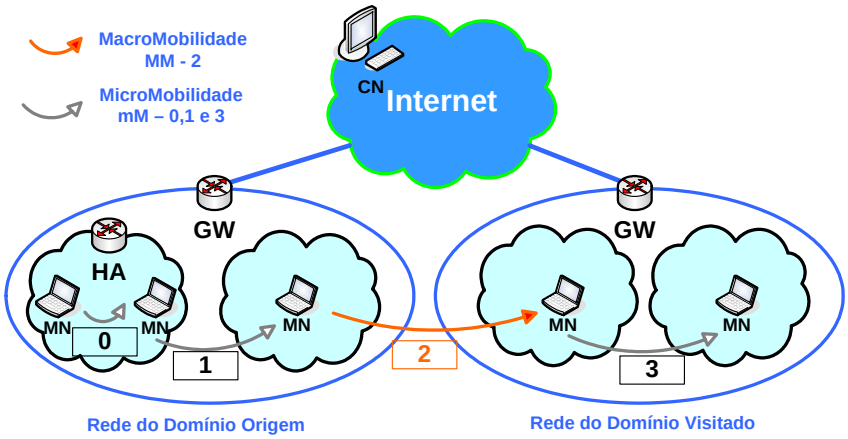


figura 88 - Teste de Mobilidade IPv6

Os *handovers* identificados na figura com 0 não envolvem MIPv6, são realizados ao nível dos protocolos das camadas inferiores. Os testes 1 serão realizados no domínio origem e os testes 2 seriam a transição entre o domínio origem e o visitado. Os testes 3 seriam realizados no domínio visitado.

Este cenário poderia ser facilmente reproduzido em laboratório e já anteriormente o foi tal como se encontra documentado no capitulo 7. No entanto seria interessante reproduzi-los num cenário real, nomeadamente para os testes 2 e 3. Considerando a ESTG e o IPL como dois diferentes domínios, não seria viável fazer os testes 2 uma vez que a separação física entre os dois *campus* não permite uma transição suave, mas poderiam ser realizados os testes 3. Assim poderiam ser consideradas duas alternativas:

- Configurar a rede origem na ESTG e fazer os testes no IPL.
- Configurar a rede origem no IPL e fazer os testes na ESTG.

Apesar de a ESTGL e o IPL serem domínios administrativos diferentes, pertencerem ao mesmo Sistema Autónomo (SA), no entanto para efeitos de teste podem ser vistos como SAs diferentes, pois isso é transparente para o MIPv6. Teríamos assim o seguinte cenário:

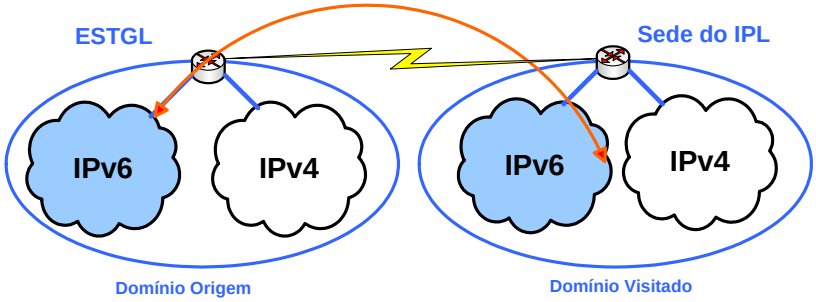


figura 89 - Configuração da ligação da ESTGL com a Sede do IPL em IPv6 nativo.

Uma vez configurada a ligação IPv6 entre os domínios poderia avançar-se para os testes de Mobilidade. Seria interessante estudar a performance do *handover* em movimentos do tipo 3, e calcular a necessidade de implementar protocolos de microMobilidade, nomeadamente o FMIPv6 e o HMIPv6.

Para ser possível realizar os testes, vários requisitos são necessários. O principal seria estabelecer uma ligação entre a sede do IPL e a rede IPv6 da ESTG. Esta ligação iria passar pelos *routers gateway* e central da ESTG e ainda pelo *Switch* L3 do IPL. O primeiro já tem suporte para IPv6, no entanto no *router* central, um cisco 3600, e no *Switch* L3, um Cisco 3550, teria de ser actualizado o IOS para um com suporte IPv6. Não é necessário suporte MIPv6, mas se tiver, permite mais flexibilidade nos testes.

Após isto seria possível introduzir as configurações para estabelecer uma ligação em IPv6 nativo entre a ESTG e o IPL, mais concretamente entre a rede piloto IPv6 existente na ESTG e a sede do IPL. Deste modo o IPL fica também com acesso à Internet IPv6.

Uma vez que a maioria dos testes são realizados na rede visitada, configura-se a rede origem na sede do IPL de modo a realiza os testes na ESTG.

Na rede origem apenas é necessário configurar uma máquina como *Home Agent*. Este, para os testes, poderia ser no *gateway* do domínio (*switch* L3), mas por uma questão de performance numa implementação futura seria mais aconselhável o uso de um servidor de mobilidade dedicado.

Assim, usando o *switch* como HA, após configurar o encaminhamento IPv6 terá de se activar e configurar o MIPv6 numa das interfaces. Os comandos são os seguintes:

```
R(config)# ipv6 enable
R(config)# ipv6 unicast-routing
R(config)# interface fast-ethernet 0
R(config-if)#ipv6 address IPv6ADDRESS/PREFIXLENGTH
R(config-if)#ipv6 mobile home-agent
R(config-if)#no shut
R(config-if)#ipv6 enable
```

Na ESTG, configurada como domínio visitado, irão ser reproduzidas as configurações dos APs do e-U em APs de teste, e irão ser recriados os serviços existentes (DHCP, Autenticação, DNS) de modo a ter um cenário mais aproximado possível do real.

Para realizar os testes, basta existir diferentes identificadores de rede (ESSID) nos APs, e realizar automaticamente a mudança de ESSID forçando o terminal a mudar de AP associado e consequentemente mudar de rede.

Existem algumas limitações na implementação deste cenário que devem ser tidas em conta.

Uma delas é o facto do IOS da Cisco não suporta protecção das mensagens de sinalização MIPv6 com IPSec definido na RFC 3776. Outra é o facto de o Windows, o sistema operativo mais usado, ainda não possuir a funcionalidade de Mobile Node (MN). O servidor de DNS para IPv6 já está implementado na rede piloto IPv6, mas deveria ser configurado um servidor de DHCPv6. Os mecanismos de autenticação teriam de ser estudados, e terá de ser arranjado um mecanismo que permita conciliar os clientes IPv6 e IPv4. Também mecanismos como VPN's terão de ser tidos em conta.

9.3 Conclusões

Neste capítulo foi realizado um estudo com o objectivo de se implementar MIPv6 na rede e-U. Antes de avançar para os testes existiam já alguns requisitos e restrições conhecidas, mas foi preciso conhecer e compreender o que existe actualmente, nomeadamente a nível da topologia da rede *wired* e *wireless*, equipamentos existentes, serviços e configurações.

A ligação entre a ESTG e o IPLeiria consiste numa ligação *wireless* dedicada de 6 Mbps com dois equipamentos Cisco nos extremos, um *Switch* L3 3550 na sede do IPL e um *router* 3600 na ESTG. O switch L3 no IPLeiria possui uma versão de IOS sem suporte para IPv6 e MIPv6. O *router* 3600 da ESTG, por seu lado também possui uma versão sem suporte de IPv6 ou MIPv6. Deste modo teria de ser realizado uma actualização do IOS a ambos para configurar a ligação IPv6 nativa entre a ESTG e o IPL, sendo necessário configurar dual-stack (IPv4+IPv6) em ambos.

A existência de *firewalls* também teria de ser tida em conta, uma vez que teriam de ser configuradas de modo a deixar passar o tráfego associado à mobilidade.

Em termos de serviços, foram identificados quatro serviços principais que existem na rede e-U, e que teriam de ser disponibilizados em IPv6, nomeadamente DNS, DHCP, Proxy e Autenticação Radius. O DNS e o DHCP poderiam ser excluídos para efeitos de teste. O primeiro porque os endereços usados são conhecidos (evitando o uso de DHCP), e o segundo porque nos testes seria usada a auto-configuração IPv6 e/ou configuração estática também para garantir que não seria necessário o DNS. O Proxy também poderia ser excluído. Em termos da autenticação Radius, a sua exclusão iria comprometer os testes, uma vez que este é um requisito essencial para acesso à rede. Teria então de se pensar numa solução para autenticação IPv6 com o cliente Linux usado nos testes.

Muitos outros detalhes foram identificados, bem como vários requisitos e restrições. A informação obtida permitiu avançar para um estudo mais preciso da viabilidade de avançar com os testes. Tendo em consideração as informações fornecidas (*show version* dos APs, do *switch* L3, do *router* Cisco 3600 e exemplo de configuração dos APs), pretendia-se antes de se avançar para o campo, realizar alguns testes preliminares usando topologias, equipamentos, serviços e configurações apropriados.

10. Propostas de futuros trabalhos

No seguimento do trabalho apresentado seguem algumas propostas de trabalho futuro, que não foram realizadas ora por falta de tempo ou porque não faziam parte do âmbito do projecto.

10.1 Mobilidade de rede (Nemo)

As redes da próxima geração baseiam-se num novo paradigma "*all IP*", em que existe uma total integração de tecnologias em redor do protocolo IP. Neste contexto, a interligação das redes fixas com redes "auto-ad-hoc" assume uma particular importância. Este tipo de redes tem diversos cenários de aplicação, e muitos mais terão num futuro próximo.

O Grupo de Trabalho NEMO (*Network Mobility*) do IETF trabalha actualmente na especificação de soluções de Mobilidade de rede, tendo inclusive já definido a RFC 3963 que especifica o seu funcionamento básico (*Network Mobility* (NEMO) *Basic Support Protocol*). A mobilidade de rede consiste num conjunto de extensões ao protocolo de Mobilidade IPv6 (MIPv6), e por isso o estudo desta tecnologia implica o conhecimento necessário do funcionamento da tecnologia MIPv6.

Existem implementadas em Linux e BSD aplicações em IPv6 que pretendem fornecer capacidade de mobilidade de rede aos terminais segundo especificado pelo IETF. Desconhece-se porém o estado de maturação e estabilidade destas, uma vez que se encontram em constante desenvolvimento.

A implementação NEMO para Linux pode ser obtida no sitio oficial, que é o mesmo do MIPv6, em www.mobile-ipv6.org [68], e para BSD pode ser obtida no sitio oficial em http://www.mobileip.jp/ [86]. Outras implementações poderão ser obtidas no sitio http://www.nautilus6.org/ [77].

Usando uma ou várias implementações do protocolo NEMO poderão ser configurados cenários para testar o funcionamento deste protocolo, quais os requisitos e restrições, como se comporta com *handovers* frequentes entre outros factores.

10.2 Suporte de Micro-Mobilidade em Redes IPv6

No âmbito das redes sem fios, suportadas em tecnologia IP, o problema da mobilidade coloca-se a dois níveis. Ao nível da MacroMobilidade (MM), com transições entre domínios administrativos diferentes, para as quais o tempo de *handover* não é o factor mais relevante; microMobilidade (mM), que está associada a transiçõe que ocorram dentro do mesmo domínio, sendo o tempo de *handover* um factor crítico.

O Mobile IP (MIP) é o standard para MM, sendo suportado quer em redes IPv4, quer em redes IPv6. Para mM existem diversas propostas no IETF: como *Cellular IP* (CIP), o *HAWAIII* e o *Terminal Independent Mobile IP* (TIMIP). Estas baseiam-se na existência de redes com características muito específicas, nomeadamente a nível de topologia e a nível de equipamentos terminais, que dificilmente se enquadram numa realidade organizacional. Para que o suporte de mM seja viável dentro duma rede corporativa é necessário encontrar soluções que suportem topologias de rede genéricas. Esse foi um dos factores que levou a que não tivessem seguimento e por isso surgiram normas baseadas em extensões ao MIPv6 como o HMIPv6 e o FMIPv6. Embora estas últimas se baseiem em mecanismos existentes nas primeiras, tiveram mais sucesso porque consistem em extensões do MIPv6, o que significa que fazem parte da mesma solução genérica de mobilidade, enquanto que com as outras seria necessário ter dois ou mais protocolos para garantir a solução completa de mobilidade.

Estudar o funcionamento dos novos protocolos de mM baseados em extensões do MIPv6, verificar quais os seus requisitos e restrições, e avaliar de que modo melhora as comunicações ao nível do *handover* é o que se propões. Poderá ser realizado um estudo comparativo entre *handovers* em MIPv6 com e sem suporte de mM.

10.3 Mecanismos de transição associados à Mobilidade IPv6

A transição do protocolo IPv4 para o protocolo IPv6 será realizada de forma gradual e existem disponíveis mecanismos de transição que resolvem o problema de conectividade básica entre terminais IPv4 e terminais IPv6. Por outro lado, existem implementações de mobilidade IPv4 e de mobilidade IPv6. No entanto, existem questões em aberto quando por exemplo se pretende que um terminal IPv6 tenha simultaneamente mobilidade e capacidade de comunicar com um terminal IPv4.

Deverá ser realizado um estudo de integração de sistemas e serviços associados ao mecanismo de mobilidade, e quais os mecanismos e aplicações disponíveis para o efeito. Deverá ser realizado um estudo não só de soluções "*IPv6 only*", mas também de soluções de transição (túneis automáticos e manuais), soluções de tradução (mecanismos de conversão IPv6 em IPv4) e integração de serviços,

11. Conclusões

Muitos dos problemas do IPv4 deixam de existir no IPv6, e todos os protocolos em IPv6 aproveitam as vantagens do novo protocolo IP. Nomeadamente, o MIPv6 apresenta melhorias significativas em relação ao MIPv4, mais concretamente ao nível do encaminhamento e segurança. Em termos funcionais, a optimização de rotas e a inexistência do Agente de Mobilidade na rede visitada (FA) são a maior diferença no MIPv6.

Este estudo permitiu concluir que a tecnologia ainda se encontra muito imatura, uma vez que as implementações existentes ainda não possuem todas as funcionalidades especificadas pelo protocolo ou então apresentam ainda erros ou são difíceis de configurar. Além disso ainda se encontram em especificação outras funcionalidades que pretendem fornecer novas capacidades ao protocolo, nomeadamente maior segurança e mecanismos de gestão.

O *handover* associado ao MIPv6 é um factor crítico, uma vez que tem uma ordem de grandeza de segundos, o que justifica a necessidade dos protocolos de micromobilidade. Estes poderão reduzir a sinalização associada ás movimentações entre redes e optimizar o mecanismo de *handover*, reduzindo o tempo de transição, e resolvendo os problemas de pacotes enviados para o endereço antigo após a mudança.

Em termos de micromobilidade (grupo de trabalho mipshop), os vários protocolos propostos (CIP, HAWAII e TIMIP) não tiveram desenvolvimento e por isso não chegaram a RFCs. O HMIPv6 e o FMIPv6 são um conjunto de extensões ao MIPv6, especificadas em RFC, que surgiram com o intuito de optimizar o processo associado aos *handovers* em ambientes de micromobilidade. A mobilidade de rede, NEMO, definida pelo grupo de trabalho com o mesmo nome, também consiste num conjunto de extensões ao MIPv6. Com estas extensões a solução completa de mobilidade global concentra-se num único protocolo, o MIPv6.

Em termos de segurança o MIPv6 não introduz vulnerabilidades significativas ao encaminhamento IPv6, mas esta é agora um dos focos de principal interesse nas especificações.

Apesar dos muitos problemas para instalar e configurar o MIPL, e de ainda existirem alguns problemas no seu funcionamento e na interoperabilidade com outras implementações, devido á sua imaturidade, é possível verificar que esta é uma tecnologia com bastante potencialidade para um futuro assente em mobilidade de dispositivos.

Tal como o IPv6 já vem de origem nas versões dos principais sistemas operativos (Windows, IOS, Linux, UNIX) no futuro também o MIPv6 virá. A Microsoft, por exemplo, anunciou que possui uma

aplicação com todas as funcionalidades do MIPv6 e pondera disponibilizar uma aplicação para o novo Windows Vista. Em Linux e BSD, continuam os esforços para acompanhar as especificações do IETF, e melhorar as implementações já existentes que ainda continuam em desenvolvimento na fase de experimentação e estabilização.

Num futuro IPv6 a mobilidade será transparente para os utilizadores. Com todas as extensões que foram desenvolvidas e estão ainda a ser desenvolvidas, o MIPv6 será uma solução de mobilidade completa, segura e fiável.

Os testes realizados foram satisfatórios, embora a interoperabilidade entre as implementações dos Sistemas Operativos seja fraca. Este facto é bastante compreensível uma vez que a tecnologia é bastante recente, e revela por isso alguma imaturidade. No entanto os desenvolvimentos emergentes irão permitir resolver todos os problemas desta tecnologia, tornando-a mais madura e estável. Actualmente ainda existe muito pouco documentação nesta área, e a que existe por vezes encontra-se já desactualizada, tal é o ritmo de evolução tecnologia.

A implementação MIPv6 para Linux permitiu verificar o funcionamento do protocolo segundo a especificação. A configuração do cenário wireless permitiu fazer um estudo do desempenho do *handover*. Pretendia-se complementar este estudo com testes usando a rede piloto IPv6 da ESTG e a plataforma de testes disponibilizada pela FCCN. Estando as duas instituições separadas fisicamente, era previsto realizar testes para avaliar o desempenho do MIPv6 com a distância. O cenário foi configurado totalmente funcional, porém problemas de interoperabilidade das aplicações MIPv6, que não se conseguiram resolver em tempo útil, impediram a realização de testes exaustivos.

Tirando partido da existência de uma rede piloto IPv6 na ESTG, e aproveitando o facto de existir uma infra-estrutura da rede e-U em todos os campus do IPL, foi desenvolvido um estudo para estudar a viabilidade de implementar MIPv6 na rede e-U. Foi realizado um levantamento da topologia da rede existente, dos protocolos, serviços e sistemas existentes. Foram identificadas restrições e requisitos. Apesar de não ter sido possivél avançar com testes mais concretos e específicos, estes terão lugar após a conclusão deste projecto.No fundo este projecto permitiu ganhar conhecimento e sensibilidade na matéria, à qual se pretende dar seguimento avançado para os testes de Mobilidade IPv6 na rede e-U.

Referências bibliográficas

Livros:

[1] Soliman, Hesham; Mobile IPv6 – Mobility in a Wireless Internet. Addison Wesley, 2005

[2] Perkins, C. E.. Mobile IP: Design Principles and Practices. Editora Prentice Hall, 1998.

[3] HAGEN, S. – IPv6 Essentials, O'Reilly, ISBN 0596001258, 2002.

[4] DAVIES, J. – Understandig IPv6, Microsoft Press, ISBN 0735612455, 2002.

[5] MALONE, D.; MURPHY, N. R. – IPv6 Network Administration, O'Reilly, ISBN 0596009348, 2005.

RFCs:

[6] RFC 1826 - R. Atkinson. IETF, RFC 1826 - IP Authentication Header, 1995.

[7] RFC 1827 – R. Atkinson. IETF, RFC 1827 - IP Encapsulating Security Payload header (ESP), 1995.

[8] RFC 1883 – S. Deering, R. Hinden. IETF, RFC 1883 - Internet Protocol, Version 6 (IPv6)Specification, 1995.

[9] RFC 2002 - C. Perkins. IETF, RFC 2002 – IP Mobility Support, 1996.

[10] RFC 2460 - Deering S., Hinden R.. IETF, RFC 2460 - Internet Protocol, Version 6 (IPv6) Specification, 1998.

[11] RFC 2461 - T. Narten, E. Nordmark, W. Simpson. IETF, RFC 2461 - Neighbor Discovery for IP Version 6 (IPv6), 1998.

[12] RFC 2462 - Thomson S., Narten, T.. IETF, RFC 2462 - IPv6 Stateless Address Autoconfiguration, 1998.

[13] RFC 2463 - A. Conta, S. Deering. IETF, RFC 2463 - Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6)Specification

[14] RFC 2471 – R. Hinden, R. Fink, J. Postel. IETF, RFC 2471 - IPv6 Testing Address Allocation, 1998.

[15] RFC 3220 – C. Perkins. IETF, RFC 3220 - IP Mobility Support for IPv4, 2002.

[16] RFC 3261 – J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, IETF, RFC 3261 – SIP: Session Initiation Protocol, 2002.

[17] RFC 3344 – Perkins, C.. IETF, RFC 3344 - IP Mobility Support for IPv4, 2002.

[18] RFC 3513 - R. Hinden, S. Deering. IETF, RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture, 2003.

[19] RFC 3775 - Johnson D.; Perkins C.; Arkko J.; RFC 3775 (Standards Track) – Mobility Support in IPv6; Junho de 2004.

[20] RFC 3776 - Arkko, J., Devarapalli, V., Dupont, F.. IETF, RFC 3776 - Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, 2004.

[21] RFC 3963 - V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert. IETF, RFC 3963 - Network Mobility (NEMO) Basic Support Protocol, 2005.

[22] RFC 4068 - Koodli, R.. IETF, RFC 4068 - Fast *Handovers* for Mobile IPv6(FMIPv6), 2005.

[23] RFC 4110 - Soliman, H., Castelluccia, C., El Malki, K., Bellier, L.. IETF, RFC 4140 - Hierarchical Mobile IPv6 Mobility Management (HMIPv6), 2005.

Drafts:

[24] MIPv6 draft 24 - Mobility Support in IPv6: draft-ietf-mobileip-ipv6-24.

[25] MIPv6 draft 12 - Mobility Support in IPv6: draft-ietf-mobileip-ipv6-12.

[26] MIPv6 draft 0 - Mobility Support in IPv6: draft-ietf-mobileip-ipv6-0.

[27] Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents: draft-ietf-mobileip-mipv6-ha-ipsec-06.

[28] CIP – Cellular IP: draft-ietf-mobileip-cellularip-00.

[29] HAWAII - Handoff-Aware Wireless Access Internet Infrastrucuture: IP micro-mobility support using HAWAII: draft-ietf-mobileip-hawaii-01.

[30] Paging support for IP mobility using HAWAII: draft-ietf-mobileip-paging-hawaii-00.

[31] TIMIP - *Terminal Independent Mobile IP* (TIMIP): draft-estrela-timip-01.

[32] FMIP - *Mobile IPv4 Fast Handovers*: draft-koodli-mip4-fmipv4-00.

[33] FMIP802.11 - Mobile IPv6 Fast *Handovers* for 802.11 Networks: draft-ietf-mipshop-80211fh-04).

[34] CIPv6 - Cellular IPv6: draft-shelby-seamoby-cellularipv6-00.

[35] FMIPv6N802.11 - Mobile IPv6 Fast *Handovers* for 802.11 Networks: draft-ietf-mipshop-80211fh-04.

[36] HMIP - Hierarchical Mobile IPv4/v6 and Fast Handoffs:draft-elmalki-soliman-hmipv4v6-00

[37] LLhMIP - Low Latency Handoffs in Mobile IPv4. K. El Malki: draft-ietf-mobileip-lowlatency-handoffs-v4-11.

Normas:

[38] Institute of Electrical and Electronics Engineers Website, http://www.ieee.org, 2005. (Norma 802.11, Norma 802.11b, Norma 802.11g e Whitepaper IEEE 802.11g)

HOWTO:

[39] Linux Mobile IPv6 HOWTO - Lars Strand

[40] Linux IPv6 HOWTO (en) - Peter Bieringer

[41] NEPL (NEMO Platform for Linux) HOWTO - Romain KUNTZ http://www.nautilus6.org/doc/tc-nepl-howto-20060209-KuntzR/nepl-howto.html

Documentos:

[42] Amado, Tiago M.; Crespo, Lúcio M. B. - Planeamento e testes de desempenho de uma rede WLAN (802.11g) em comunicações multimédia; Relatório final da disciplina de Projecto I (1º ciclo), do curso de Engenharia Informática e Comunicações; ESTG Leiria, Setembro de 2004.

[43] Serafim, David L. S.; Santos, Vítor A. C. d.; IPv6@ESTG-Leiria - Instalação de uma Rede Piloto; Relatório final da cadeira de Projecto I, do curso de Licenciatura em Engenharia Informática e Comunicações; ESTG Leiria, Julho de 2005.http://www.ipv6.estg.ipleiria.pt/

Sítios Web (visitados entre Outubro de 2005 e Janeiro de 2006):

[44] IPv6@ESTG-Leiria, http://www.ipv6.estg.ipleiria.pt/.

[45] FCCN, http://www.fccn.pt.

[46] Task Force Portuguesa de IPv6, http://www.ipv6-tf.com.pt/.

[47] The IPv6 Portal, http://www.ipv6tf.org/.

[48] IPv6 Forum, http://www.ipv6forum.com/.

[49] IPv6 Forum: Global Forum Events, http://www.ipv6forum.org.uk/navbar/events/global.htm.

[50] IPv6 Ready Logo Program, http://www.ipv6ready.org/.

[51] IPv6 Ready Logo Phase-1, http://www.ipv6ready.org/logo_db/approved_list.php.

[52] IPv6 Ready Logo Phase-2, http://www.ipv6ready.org/logo_db/approved_list_p2.php.

[53] IPv6 Information Page, http://www.ipv6.org/.

[54] The Internet Engineering Task Force, http://www.ietf.org/.

[55] 6Bone Home Page, http://www.6Bone.net/.

[56] IST IPv6 Cluster, http://www.ist-ipv6.org/.

[57] 6NET, http://www.6net.org/.

[58] Euro6IX, http://www.euro6ix.org/.

[59] IANA, http://www.iana.org/.

[60] DoD – Departamento de defesa dos Estados Unidos, http://ipv6.disa.mil/.

[61] Cisco Website, http://www.cisco.com.

[62] Universidade Electrónica (e-U), http://www.e-u.pt.

[63] Biblioteca Online (B-on), http://www.b-on.pt.

[64] Redes Móveis, http://www.rnp.br/newsgen/0301/mip.html.

[65] Ethereal, http://www.ethereal.com/download.html.

[66] ITU-R, http://www.itu.int/ITU-R.

[67] MIPv6 for BSD,: http://www.mobileip.jp/.

[68] MIPv6 for Linux (MIPL), http://www.mobile-ipv6.org/6.

[69] Mipv6 Tester (2006), www.bullopensource.org/mipv6/tester.php.

[70] Cisco - Implementing Mobile IPv6: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/products_configuration_guide_chapter09186a00804160bf.html

[71] Microsoft IPv6 technologies (1): http://www.microsoft.com/windowsserver2003/technologies/ipv6/default.mspx

[72] Microsoft Mobile IPv6: http://research.microsoft.com/mobileipv6/

[73] Microsoft IPv6 technologies (2): http://www.microsoft.com/technet/community/columns/cableguy/cg0904.mspx

[74] Microsoft IPv6 technologies (3): http://www.microsoft.com/downloads/details.aspx?familyid=42BF4711-27AF-4C4C-8300-7BCF900DE5C3&displaylang=en

[75] Microsoft IPv6 technologies (4): http://www.microsoft.com/downloads/details.aspx?FamilyID=f85dd3f2-802b-4ea3-8148-6cde835c8921&displaylang=en

[76] Nautilus6 ,http://www.nautilus6.org/

[77] Implementações do projecto Nautilus6, http://www.nautilus6.org/implementation/index.php, Janeiro de 2006.

[78] Kame, http://www.kame.net/.

[79] IEEE 802.11 (2006) - The Working Group for WLAN Standards. http://www.ieee802.org/11/.

[80] IETF, Active IETF Working Groups - Internet Área (2006). http://www.ietf.org/html.charters/wg-dir.html#Internet%20Area

[81] IETF, Active IETF Working Groups - Mobility for IPv6 (mip6) (2005). Grupo de trabalho do IETF em mobilidade IPv6: http://www.ietf.org/html.charters/mip6-charter.html

[82] CIP - http://www.comet.columbia.edu/cellularip/overview.htm

[83] CIPv6 - http://cipv6.intranet.gr

[84] FMIPv6 - http://www.fmipv6.org/

[85] nemo - http://www.ietf.org/html.charters/nemo-charter.html

[86] SHISA - http://www.mobileip.jp/

[87] USAGI – http://www.linux-ipv6.org/.

[88] Wide - http://www.wide.ad.jp/

[89] KAMEMIP – http://www.kame.net/

[90] KAME – http://www.kame.net/

[91] SFCMIP – http://www.wakikawa.net/Research/contents/mip6.html

[92] InternetCAR – http://www.wakikawa.net/Research/contents/mip6.html.

[93] HMIPv6 - http://www.ctie.monash.edu.au/ipv6/,

[94] HMIPv6 - http://www.tkn.tu-berlin.de/research/hmip/,

[95] FMIPv6 for BSD - http://software.nautilus6.org/TARZAN/,

[96] Projectos MIPv6 - http://www.nautilus6.org/implementation/index.php,

[97] Network Simulator, http://www.isi.edu/nsnam/ns/

[98] Mobiwan - http://www.inrialpes.fr/planete/pub/mobiwan/.

[99] TAHI Project, http://www.tahi.org/.

[100] The Linux Kernel Archives, http://www.kernel.org/.

[101] IPv6 on Fedora Core mini-HOWTO, http://linux.yyz.us/ipv6-fc2-howto.html.

[102] IEEE web site for 802.16: http://grouper.ieee.org/groups/802/16/.

[103] WiMAX Forum - http://www.wimaxforum.org/home/

[104] Body Area Network: http://www.ban.fraunhofer.de/index_e.html.

Artigos:

[105] Serafim, D., Santos, V., Antunes, M., Veiga, N., (2005). *IPv6@ESTG-Leiria - Instalação de uma Rede Piloto*. 3.ª Conferência de Engenharias, Engenharia'2005 - Desenvolvimento e Inovação; Universidade da Beira Interior, Covilhã.

Outros:

[106] http://www.fccn.pt/files/documents/D4.01v1.PDF

[107] Fundamentals of wireless LANs v1.1 - Curriculum “Wireless”, da Academia Cisco.

[108] Conferência Ibérica de Sistemas e Tecnologias de Informação. 21 a 23 de Junho de 2006, Esposende Portugal. http://www.est.ipca.pt/cisti/

Anexos

A - Dicionário técnico

Aqui será apresentado um dicionário técnico com alguns dos termos técnicos usados ao longo do presente relatório.

A.1 Mobilidade

MN - Mobile Node (estação móvel). Máquina móvel que muda de ponto de ligação, mantendo o endereço IP.

HA - Home Agent (Agente na rede origem) Sistema (router) na rede origem do MN que regista a localização do MN. Usa um túnel para enviar datagramas IP para o COA

FA - Foreign Agent (Agente na rede visitada). Sistema (router) na rede visitada pelo MN. Entrega pacotes recebidos pelo túnel ao MN.

CoA - Care-of Address, endereço IP da extremidade do túnel na rede visitada. Localiza o MN.

HoA – Home Address, endereço

CN - Correspondent Node é a Máquina que comunica com o MN.

MacroMobilidade - Mobilidade entre domínios administrativos (DA).

microMobilidade - Mobilidade dentro de um Domínio Administrativo (DA).

Roaming – capacidade de deslocar entre diferentes pontos de acesso e diferentes redes.

Handover ou **Handoff**– processo de transição de ponto de acesso e de rede.

Seamless *handover* – *Handover* suave.

A.2 Redes de dados e sistemas distribuídos

Link MTU – A taxa de transmissão máxima de um link

Path MTU – O menor valor do MTU de todos os links que prefazem o caminho de origem até ao destino (para IPv6 o minimo Link MTU é de 1280 octetos, 68 octetos para IPv4. Nos Links com MTU < 1280, deve utilizar-se fragmentação e reagrupamento dos pacotes).

Socket – Mecanismo de comunicação entre processos sejam eles do mesmo sistema (comunicação local) ou de diferentes sistemas (comunicação remota). È um canal de comunicação bidireccional entre dois ou mais processos. Encaixa-se no nível 4 do modelo OSI da ISO (Camada de transporte). Uma

ligação Socket é plenamente descrita através de 5 parametros: Protocolo, Endereço Local, Porto Local, Endereço remoto, Porto Remoto (Exemplo: TCP, 192.168.234.21, 4500, 192.168.234.7, 23).

Multiplicidade de portos – 1 endereço IP apresenta vários portos (2^16 = 65536, o porto é representado por um inteiro de 16 bits). Deste modo é possível a multiplexagem, ou seja, uma dada máquina pode manter várias ligações em simultâneo com outras máquinas.

Testes benchmarking - Processo contínuo de avaliação e comparação do nível de desempenho, que visa atingir uma melhoria de performance.

A.3 Segurança

Disponibilidade – capacidade de garantir a disponibilidade dos recursos mesmo na sequência de ataques ou falhas.

Confidencialidade – capacidade de limitar o acesso à informação apenas às entidades (pessoas, processos, máquinas…) autorizadas.

Integridade – capacidade de garantir a detecção da alteração da informação transportada ou armazenada.

Serviços derivados da confidencialidade e da integridade:

- **Autenticação** – capacidade de garantir que uma entidade é quem afirma ser
- **Controlo de Acesso** – capacidade de impedir o acesso não autorizado a um recurso, ou a sua utilização além dos limites autorizados
- **Não Repudiação** – capacidade de impedir que uma entidade envolvida numa transacção negue a sua participação no evento (total ou parcialmente).

B - Projecto e-U

Certamente qualquer universitário ou qualquer pessoa que trabalhe no ramo das comunicações sabe o que é ou já ouviu falar no e-U[5].

Basicamente o projecto e-U é um projecto a nível nacional que consiste em implementar uma rede sem fios em todas as Instituições de Ensino Superior em Portugal, universidades e politécnicos. Será então possível a transmissão de dados em banda larga, disponibilizar e ter acesso a aulas, artigos, trabalhos, resultados das avaliações, serviços, internet e muito mais.

e-U *Campus Virtual* é uma iniciativa lançada pelo Governo, no âmbito do Plano de Acção para a Sociedade da Informação. A e-U envolve serviços, conteúdos, aplicações e rede de comunicações móveis para estudantes e professores do Ensino Superior, que pretende incentivar e facilitar a produção, acesso e partilha de conhecimentos. Outra iniciativa do governo é a b-on[6], Biblioteca do Conhecimento On-line, que pretende criar uma biblioteca digital, disponibilizando e facilitando o acesso a conteúdos bibliográficos actualizados. Reúne as principais editoras de revistas científicas internacionais de modo a oferecer um conjunto vasto de artigos científicos disponíveis on-line.

O e-U está a ser desenvolvido tendo como base uma convergência de esforços entre diversos tipos de entidades que trabalham em conjunto para o desenvolvimento e sucesso desta iniciativa. São estas, Instituições Financeiras, Fabricantes de *Hardware*, Fabricantes de *Software*, Operadores de Telecomunicações, ISPs (*Internet Service Provider*), e outros parceiros genéricos que quiseram dar o seu contributo e aderiram a este projecto nacional.

Assim, com um PC (*Personal Computer*) portátil e a partir de qualquer ponto do *campus* universitário, é possível professores e alunos acederem a serviços e conteúdos académicos, constantemente acessíveis. É por tudo isto e muito mais que a iniciativa da e-U é uma experiência inovadora a nível mundial e está a ser apresentada como exemplo europeu da utilização do conceito de mobilidade nos meios académicos. Portugal é o primeiro país a criar, nesta escala, uma rede integrada Wi-Fi em todo o ensino superior. Embora sendo um país pequeno, esta iniciativa é enorme e inédita no mundo. Algumas das maiores e mais conceituadas empresas a nível mundial como a Intel, Cisco ou Microsoft estão a apresentar mundialmente o *case study* português.

A Fundação para a Computação Cientifica Nacional (FCCN), entidade responsável pela gestão e operação da actual rede académica, encontra-se a desenvolver um projecto que visa interligar por meio

[5] Sítio do e-U - http://www.e-u.pt
[6] Sítio do b-on - http://www.b-on.pt

de Fibra Óptica as cidades de Lisboa, Coimbra, Aveiro, Porto e Braga. No âmbito da Iniciativa Nacional para a Banda Larga promovida pela Unidade de Missão Inovação e Conhecimento (UMIC), também parte integrante do Plano de Acção para a Sociedade da Informação.

Esta iniciativa pioneira na história da rede académica nacional, é uma aposta inequívoca na Inovação e no Conhecimento. Vai ser criado um sistema que proporcionará rapidez e qualidade no acesso à internet, que são fundamentais para o ensino e para a investigação. Em questões de velocidade de acesso, este investimento irá fazer com que Portugal se eleve ao nível das grandes potências mundiais.

Esta infra-estrutura servirá de complemento às iniciativas e-U e b-on. Em conjunto, estes projectos irão dotar as instituições de Investigação e Desenvolvimento e de Ensino Superior dos meios mais avançados para desenvolver a sua actividade, que assume extrema importância para o desenvolvimento do País.

Com o aumento de largura de banda que será possível através da ligação em fibra óptica, os investigadores nacionais poderão também desfrutar da rede GÉANT, a rede de investigação e de ensino europeia, uma infra-estrutura financiada pela União Europeia.

C - Configuração da consola minicom

A consola *minicom* basicamente permite fazer o mesmo em Linux que o *hyperterminal* no Windows. Podemos então usar a consola *minicom* para configuração do IOS nos *routers* cisco usando uma máquina Linux. Existem outras aplicações disponíveis para o efeito:

- Minicom – o mais popular;
- Kermit – como programa de comunicação é mais poderoso que a minicom;
- Seyon – programa de comunicação X-Based.

Outras menos conhecidas:

- ecu – programa de comunicação;
- pcomm – procomm;
- xc - xcomm communication package.

Para realizar as configurações usando a minicom, utiliza-se um cabo de consola (invertido) para comunicar com a porta de consola do router, hub switch, AP ou router. Depois configura-se a consola diditando na linha de comandos “Minicom –s”.

Os parâmetros a utilizar são os seguintes (serial port setup):

- /dev/ttyS0 (S0 para a Com1, S1 para Com2 e assim sucessivamente)
- 9600bps 8N1
- Sem controlo de fluxo (hardware e software)

Antes de sair da configuração deve-se guardar as configurações (save setup as dfl).

Para obter ajuda usa-se a combinação de teclas “ctrl+a” seguido de “z”.

Para sair da consola usa-se “ctrl+a” seguido de “x”.

D - MIPL Howto

Este anexo apresenta o guião de configuração e utilização da aplicação de Mobilidade IPv6 para Linux (MIPL).

MIPL HOWTO (pt)

Manual de instalação e configuração da aplicação de Mobilidade IPv6 para Linux - versão Portuguesa

Versão: mipv6-2.0-rc3_v1

22 de Janeiro de 2006

1. Introdução

Este documento descreve o software e os procedimentos para configurar e usar mobilidade IPv6 em linux (MIPL).

A RFC 3775, "Mobility support in IPv6", definida pelo IETF, esclarece o que é, e o porquê da mobilidade IPv6.

O site www.mobile-ipv6.org, é o site oficial da mobilidade IPv6 para Linux (MIPL), gerido e mantido por um grupo de trabalho da Universidade de Helsínquia na Finlândia, responsáveis pela implementação prática do draft "Mobility Support in IPv6" nº24, levando à sua evolução para a RFC 3775. Neste site encontra-se disponível o software MIPL, juntamente com alguma informação, documentação e links úteis. Encontra-se também um bom MIPL HOWTO (Mobile IPv6 for linux (en) by Lars Strand), embora que já desactualizado e algo incompleto, no qual se baseia este documento.

1.1. O que é a Mobilidade IPv6?

"(…)Cada nó móvel é sempre identificado pelo seu home address (HoA), independentemente do seu ponto de ligação à Internet. Enquanto situado longe da sua rede original (home network), o nó móvel tem também atribuído um care-of-address (CoA), que fornece informação da sua localização. Os pacotes IPv6 enviados para o HoA do nó, são reenviados de forma transparente, pelo Home Agent (HA), para o CoA. O protocolo permite que os nós IPv6 armazenem o registo da ligação entre um HoA e um CoA de um nó móvel, podendo assim enviar pacotes destinados a esse nó móvel directamente para o seu CoA.(…)"

RFC 3775 "Mobility Support in IPv6", Abstract, pag. 0.

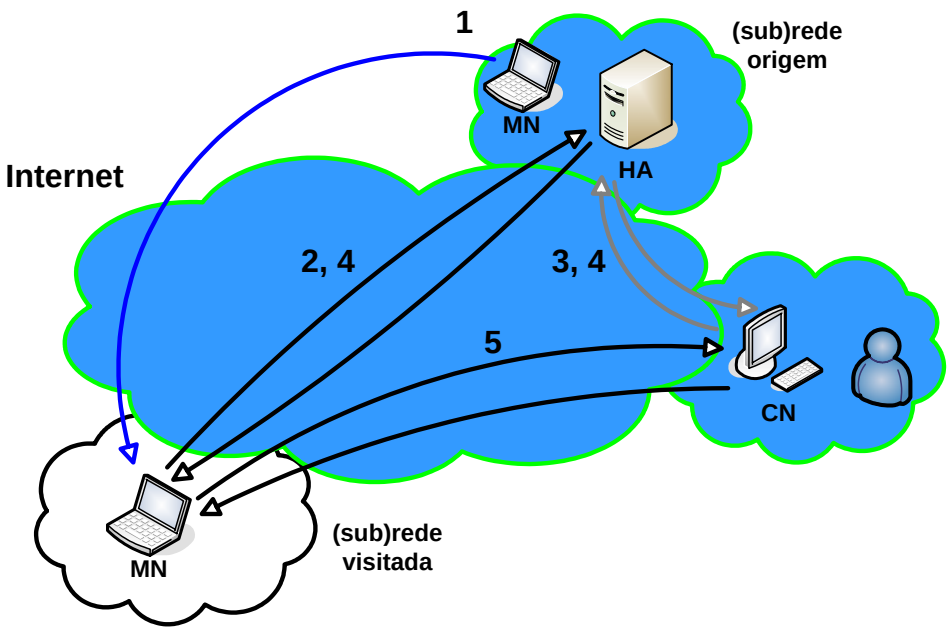
1.2. Porquê Mobilidade IPv6?

"(...)Sem suporte especifico para mobilidade IPv6 (MIPv6), os pacotes destinados para um nó móvel (PC ou Router), não estarão aptos a alcançar esse nó enquanto este se encontrar fora do seu troço de ligação original (o home link original do nó móvel e cujo prefixo de subrede é igual ao do seu HoA), uma vez que o encaminhamento é baseado no prefixo de subrede existente no campo do endereço IP de destino do pacote. De modo a manter a comunicação, mesmo que ocorra movimento, o nó móvel poderá mudar o seu IP cada vez que se move para um novo link, mas, neste caso, o nó móvel não poderá manter o transporte e as ligações das camadas superiores quando muda de localização. O suporte de mobilidade em IPv6 é particularmente importante, uma vez que os computadores móveis irão constituir uma maioria, ou pelo menos uma fracção significativa da população da Internet durante o tempo de vida do IPv6.(…)"

RFC 3775 "Mobility Support in IPv6", Introduction, pág. 5 e 6.

1.3. Como funciona?

Neste ponto estão explicados os passos básicos do funcionamento de MIPv6.



Mobilidade IPv6

1. O nó móvel (MN) desloca-se para uma rede diferente, e recebe um novo care-of-address (CoA).
2. O MN regista o seu movimento (binding update (BU)) no Home Agent (HA)(o novo CoA é associado ao Home Address(HoA) no HA). O HA envia um binding acknowledgement(BA) para o MN.
3. Um nó, designado de Correspondent Node (CN), quer comunicar com o MN, usando o seu HoA. O HA intercepta os pacotes destinados ao MN.
4. O HA envia por túnel todos os pacotes destinados ao MN usando o seu CoA.
5. O MN responde para o CN usando o seu CoA (fazendo um registo no CN caso este suporte MIPv6), comunicando directamente com este (optimização de Rota), ou pode enviar por túnel todos os pacotes para o HA, sendo este responsável por os enviar para o CN.

Ver figura “Mobilidade IPv6” no topo.

Para mais detalhes, ler a RFC 3775, "Mobility Support in IPv6".

2. IPv6

O IP versão 6 (IPv6) [RFC - 2460] é a nova versão do protocolo da Internet (IP), designado como o sucessor do IP versão 4 (IPv4) [RFC 0791]. As mudanças mais significativas do IPv4 para o IPv6 são as enumeradas de seguida:

- Expansão das capacidades de endereçamento
- Simplificação do formato do cabeçalho
- Melhoramento do suporte de extensões e opções
- Capacidade de fluxo por labels
- Capacidades de autenticação e privacidade

Deverá haver conhecimento básico do processo de auto-configuração IPv6 stateless, para compreender como funciona a mobilidade IPv6 (MIPv6), especificado em "IPv6 Stateless Address Autoconfiguration" no *[RFC2462]*.

Para mais informações genéricas do IPv6, poderá ser consultada a página do IETF's IPv6 Working Group.

3. Mobilidade IPv6 para Linux

Existem duas implementações de Mobilidade IPv6 para Linux disponíveis.

A Universidade de Lancaster no Reino Unido tem a mais antiga (http://www.cs-ipv6.lancs.ac.uk/MobileIP/). A última implementação foi desenvolvida para o Kernel 2.1.90, de acordo com o especificado no draft 5 do IETF de Mobilidade em IPv6 (o actual RFC 3775). No entanto o código e o sítio web não são actualizados desde 1998, por isso esta solução é considerada obsoleta.

A outra implementação, é a "Helsinki University of Technology's MIPL Project", que é actualizada periodicamente. O último kernel suportado é o 2.6.11 (ultima actualização do software em 31-10-2005). No site http://www.mobile-ipv6.org/, encontra-se disponível o patch e as user space tools, bem como documentação, links, e uma Mailing List bastante solicitada, com o respectivo arquivo.

Como é óbvio, a implementação escolhida para a Test bed, foi a disponibilizada pela universidade de Helsínquia.

3.1. Aplicar o patch ao kernel

Enquanto se aguarda pela inclusão da Mobilidade IPv6 no kernel do Linux, tal como já sucede com o IPv6, há que recorrer à aplicação de um Patch ao Kernel. A implementação modifica a pilha IPv6 do Kernel, por isso é necessária a sua recompilação. De seguida é apresentado este processo detalhado.

Nota! Este processo permite instalar o suporte para as funcionalidades de HA, MN e CN. Apesar de não ser possível manter mais do que uma funcionalidade em simultâneo, o modo escolhido irá depender das configurações posteriores.

Notas e considerações antes de começar a implementação:
A distribuição usada para implementar a Test Bem foi a Fedora Core 3 (FC3).
A distribuição Fedora mais recente é o Fedora Core 4 (FC4), e inicialmente foi esta distribuição que começou por ser usada, no entanto alguns problemas levaram a abdicar desta em função da FC3. Os motivos desta opção em detrimento da primeira são enunciados de seguida.
No FC4, o kernel usado é o kernel-2.6.11-1.1369_FC4 (na linha de comando: rpm –q kernel). Este deriva do 2.6.11 ao qual foram aplicadas algumas modificações (patchs) exclusivamente para a sua inclusão na distribuição, no entanto a sua versão não deixa de ser a 2.6.11. Por isso houve uma tentativa de aplicar o patch neste kernel, que se revelou infrutífera. Ocorreram falhas (failed hunks) que permitiram concluir que teria de ser usada a versão 2.6.11 "pura".
Após o download desta, aplicar o patch foi fácil e não ocorreram problemas, no entanto o processo de recompilação revelou-se uma tarefa complicada, nomeadamente a recompilar os módulos (Make Modules), cujo processo não foi possível completar devido a uns erros ocorridos.
Após várias tentativas falhadas, pensou-se que o problema seria devido ao facto de o kernel ser igual ao usado na distribuição, e de alguma forma estaria a ocorrer um conflito no processo recompilação.
Optou-se então por usar a distribuição do FC3, que traz de origem o kernel-2.6.9-1.667. Nesta não existiu nenhum problemas nem a aplicar o Patch ao kernel 2.6.11, nem no processo de

recompilação deste. Como a máquina usada era bastante rápida o processo completo de recompilação também o foi.

De seguida são apresentados os passos necessários para implementar suporte de MIPv6 numa máquina Linux.

1. Fazer download da ultima versão do código fonte do MIPv6 para Linux e respectivo Patch no sítio http://www.mobile-ipv6.org/. A ultima versão disponível à data deste documento (sítio actualizado em 31-10-2005) é a *mipv6-2.0-rc3*, sendo o respectivo patch o mipv6-2.0-rc3-linux-2.6.11.patch, tal como indicado no nome, para o kernel 2.6.11.

```
# cd /usr/local/src
# wget http://www.mobile-ipv6.org/software/download/mipv6-2.0-
rc3.tar.gz
# wget http://www.mobile-ipv6.org/software/download/mipv6-2.0-rc3-
linux-2.6.11.patch.gz
# tar zxfv mipv6-2.0-rc3.tar.gz
# tar zxfv mipv6-2.0-rc3-linux-2.6.11.patch.gz
```

2. Fazer download e descompactar a versão do kernel correspondente no sítio oficial, ftp.kernel.org, ou no mirror mais próximo.

```
# cd /usr/src
# wget ftp://ftp.kernel.org/pub/linux/kernel/v2.6/linux-2.6.11.tar.bz2
# tar jxvf linux-2.6.11.tar.bz2
# cd linux-2.6.11
```

3. Antes de aplicar o patch, podemos ver a configuração existente através de um qualquer make *config, e.g., make menuconfig.

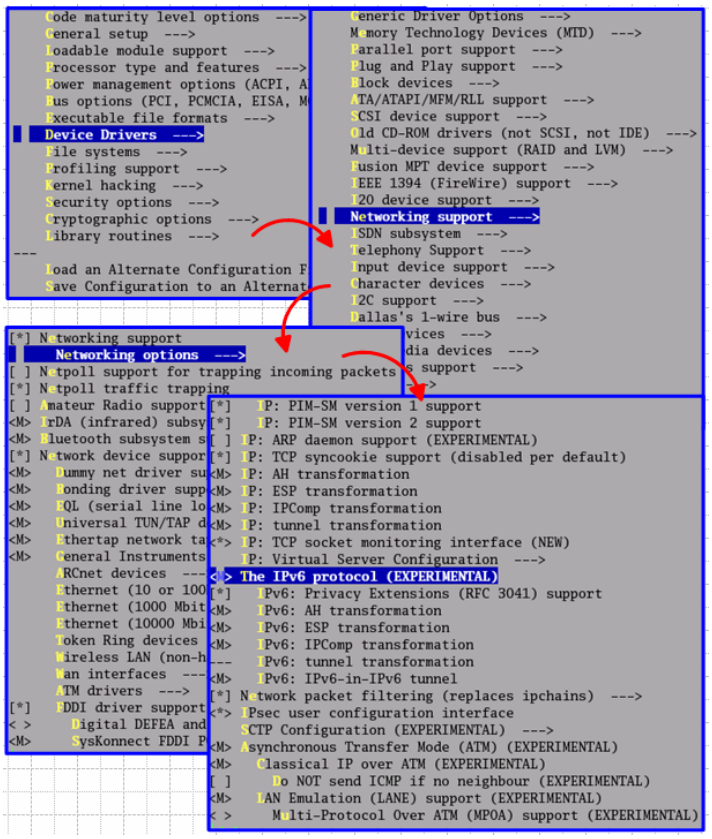
```
# make menuconfig
```

No menu de configuração:

```
Device Drivers --->
    Networking support --->
        Networking options --->
```

Neste menu poderá ser visto as opções de suporte IPv6, e a inexistência de opções de MIPv6. Antes de avançar deverá sair do menu de configuração e fazer o make clean.

```
# make clean
```



Configurações disponíveis antes de aplicar o patch.

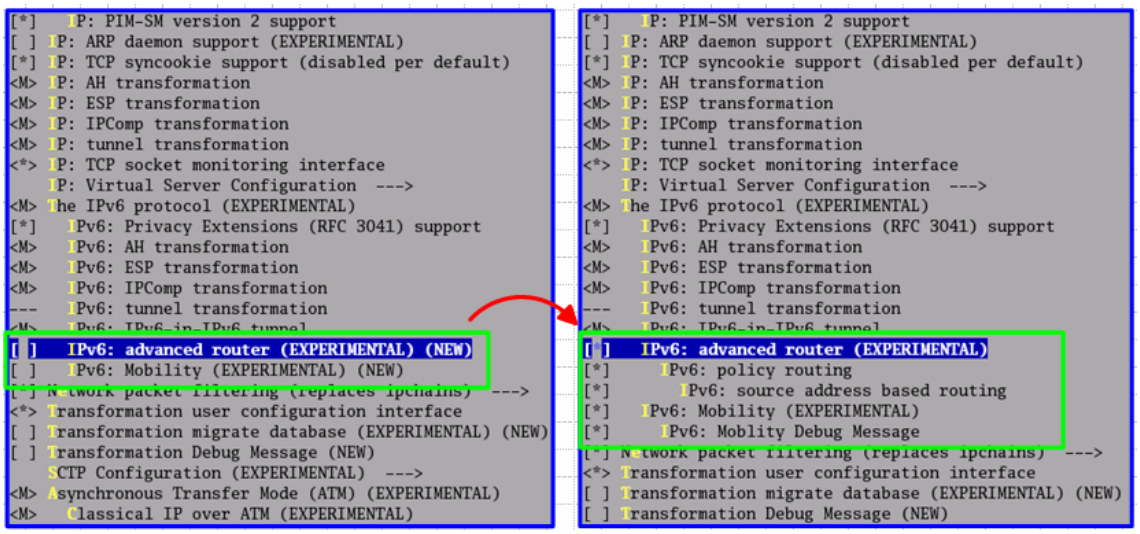
4. Verificar se o Patch pode ser aplicado correctamente:

```
# patch -p1 --dry-run < /usr/local/src/mipv6-2.0-rc3-linux-2.6.11.patch
```

5. A opção --dry-run, verifica se o Patch será aplicado correctamente. Se ocorrerem erros (failed hunks) algo está incorrecto e o processo não poderá continuar, devendo ser revistos os passos anteriores. Se tudo correr bem então há que aplicar efectivamente o Patch:

```
# patch -p1 < /usr/local/src/mipv6-2.0-rc3-linux-2.6.11.patch
```

6. Agora a árvore do kernel está pronta para a configuração. Como referido anteriormente, as opções de MIPv6 estão em “Device Drivers > Networking support > Networking options”. È possível verificar que novas opções apareceram, nomeadamente opções de MIPv6. A figura seguinte mostra essas mesmas opções.



Configurações após aplicar o patch.

O “M” significa Módulo, e o “*” é embutido no kernel.

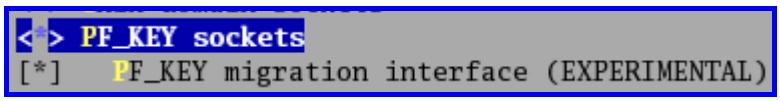
7. Para ter a certeza de que todas as opções estão correctamente seleccionadas, poderá ser usado o script **`chkconf_kernel.sh (indicando o kernel a verificar)`**, que é um pequeno script shell que vem junto com as userspace tools mipv6 .

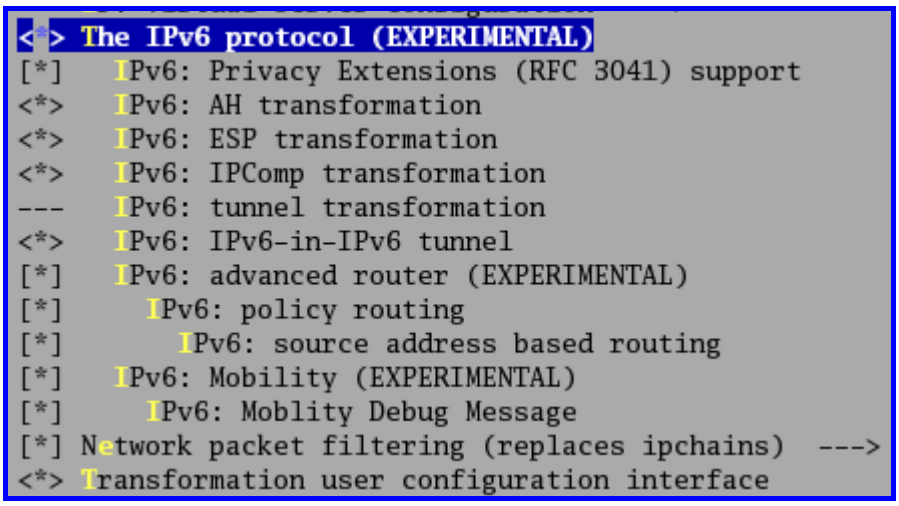
```
# cd /usr/local/src/mipv6-2.0-rc3
# ./chkconf_kernel.sh /usr/src/linux-2.6.11
```

O output do script deverá ser semelhante ao apresentado de seguida:

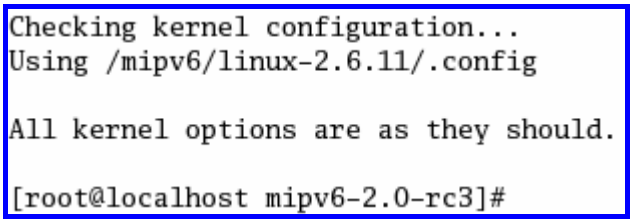
```
Checking kernel configuration...
Using /mipv6/linux-2.6.11/.config
 Warning: CONFIG_IPV6 should be set to y (m)
 Warning: CONFIG_IPV6_TUNNEL should be set to y (m)
 Warning: CONFIG_INET6_ESP should be set to y (m)
 Warning: CONFIG_NET_KEY should be set to y (m)
 Warning: CONFIG_NET_KEY_MIGRATE should be set to y (not supported)

Above 5 options may conflict with MIPL.
If you are not sure, use the recommended setting.

[root@localhost mipv6-2.0-rc3]# _
```

Deverá ser editado mais uma vez o menu de configuração, seleccionando as seguintes opções com “*:”





Após gravar estas alterações, o output do script deverá ser o seguinte:



Caso não seja, deverá ser revista a configuração, alterando-a em conformidade com o resultado do output.

8. Neste ponto, o kernel estará pronto a ser compilado e instalado.

   Dica: Para distinguir facilmente este kernel de outros, poderá ser alterada a variável "EXTRAVERSION" no **`/usr/src/linux/Makefile`** para por exemplo "FC3-k2.6.11-MIPv6-2.0-rc3".

```
# cd /usr/src/linux-2.6.11
# make clean
# make dep
# make bzImage
# make modules
# make modules_install
# make install
```

9. Se tudo correu bem, óptimo!! Poderá então editar o /boot/grub/grub.conf e fazer o reboot. Se durante algum dos passos ocorreu algum erro, então será mais complicado…os passos anteriores deverão ser revistos com cuidado.

Ler o Linux Kernel HOWTO para instruções detalhadas em como aplicar o patch, compilar e instalar o novo kernel.

3.2. Userspace tools

As userspace tools mip6d (em versões anteriores o mip6d não existia, existindo sim o mipdiag), os ficheiros de configuração e os init scripts devem ser instalados para obter as funcionalidades da mobilidade IPv6.

```
# cd /usr/local/src/mipv6-2.0-rc3
# CPPFLAGS='-isystem /usr/src/linux-2.6.11/include' ./configure
# make && make install
```

De notar que para executar o ./configure tem de ser dada a localização do novo kernel.

3.3. MIPv6 device node

O módulo MIPv6 necessita de uma nova entrada de nó no dispositivo. Usar o comando:

```
# mknod /dev/mipv6_dev c 0xf9 0
```

3.4. Arranque automático no boot

1. *Fedora core 3:*

   No HOWTO original está descrito um método para iniciar o MIPv6 automaticamente no boot, mas uma vez que existem configurações a fazer antes de iniciar o deamon, o arranque automático no boot será realizado de outra maneira.

   Será criado um script com todas as configurações a fazer. A título de exemplo, poderá ser chamado de mipv6_ConfFile, e poderá ficar na directoria /mipv6.

   Então poderá ser adicionado ao ficheiro /etc/rc.local a seguinte linha de código:

   ```
   cd /mipv6; ./mipv6_ConfFile
   ```

   O script rc.local é executado no boot após todos os scripts de configurações terem sido executados.

2. *Outras distribuições:*

   Não foram testadas outras distribuições para além do fedora core 3. No HowTo original, são apresentados comandos para o Debian e para o Slackware, no entanto não é possível dizer que estes estão desactualizados. No entanto tal como no caso apresentado para o FC3, existem configurações a fazer, pelo que pode ser usado um método igual ao apresentado.

   De referir ainda que a partir da versão 2 do MIPL, para iniciar o mipv6 já não usa o mobile-ip6, mas sim o deamon mip6d.

4. Test bed

Neste momento deverá existir um kernel MIPL funcional com um patch correctamente aplicado, userlevel tools instaladas e activação automática no arranque. Se alguma coisa correu mal, deverá verificar as secções anteriores com atenção.

4.1. Testcase

Os endereços usados no MIPL HowTo são site-local. No entanto, estes endereços já não existem. Quem faz a gestão dos endereços IPv6 é a IANA (Internet Assigned Numbers Authority), e em http://www.iana.org/assignments/ipv6-address-space é possível verificar como estão alocados actualmente. A tabela seguinte mostra os prefixos que se encontram alocados. À data deste documento todos os outros se encontravam reservados.

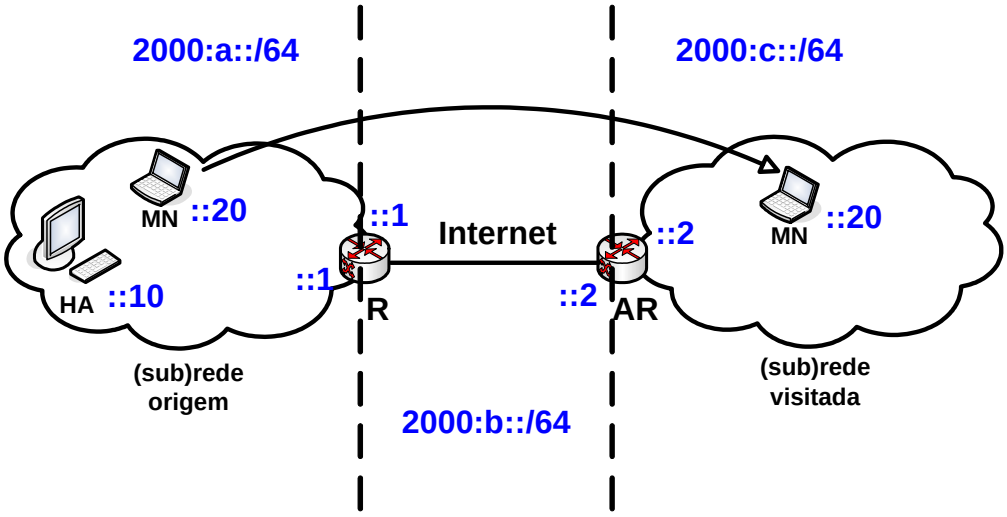
Prefixo IPv6	Alocação	Referência
2000::/3	Global Unicast	[RFC3513]
FC00::/7	Unique Local Unicast	[RFC4193]
FE80::/10	Link Local Unicast	[RFC3513]
FF00::/8	Multicast	[RFC3513]

Alocação de endereços pela IANA [last updated 05 October 2005].

Os endereços a usar nesta test-bed serão do tipo Global. Os Unique Local Unicast também não estão pensados para serem encaminhados na Internet global, ficando limitados a uma área mais restrita tal como um site. Os multicast, como é óbvio também não podem ser usados.

O cenário de teste consiste em 4 nós:

1. *HA - Home Agent:* O HA está localizado na rede origem com o endereço 2000:a::10.
2. *MN - Mobile Node:* Quando o MN está na rede origem, tem o endereço 2000:a::211:11ff:fe59:e99. Quando se move para uma rede destino, gera automaticamente um novo care-of-address, e.g., se for para a rede 2000:c::/64 irá ficar com o CoA 2000:c::211:11ff:fe59:e99.
3. *R - Router:* Este é o router que interliga a rede origem com a Internet. Tem uma interface na rede origem com o endereço 2000:a::1, e a outra interface para o exterior com o endereço 2000:b::1.
4. *AR - Access Router:* O link entre o AR e o R é a suposta Internet, bastando para o caso de teste usar um cabo cruzado. O AR tem duas interfaces, uma que liga à “Internet” com o endereço 2000:b::2, e a outra na rede destino com o endereço 2000:c::2.



Mobile IPv6 testbed.

4.2. Configuração Passo-a-Passo

Para o cenário anterior, foi usado apenas um cabo cruzado para simular a Internet, e foi usado um hub em cada rede, sendo necessário apenas mudar o cabo do terminal móvel de um hub para o outro para testar a mobilidade. No HowTo original foram usadas interfaces wireless nas redes origem e visitada, mas o princípio de funcionamento é o mesmo.

4.2.1. Configurar uma rede IPv6 funcional

Antes de começar a testar a mobilidade IPv6, é necessário configurar a rede com encaminhamento totalmente funcional. Todos os nós deverão estar acessíveis (para tal poderá testar-se com o utilitário ping). Se por exemplo, o AR não conseguir alcançar o HA, então não haverá troca de mensagens MIPv6.

Será dada uma breve instrução dos comandos necessários para configurar a rede com IPv6. Para mais informações sobre configurações IPv6, poderá ser consultado o HowTo de Peter Bieringer's, Linux IPv6 HOWTO. Para configurar as interfaces serão usados os seguintes comandos:

```
#/sbin/ip link set dev <interface> {up|down}
#/sbin/ifconfig <interface> {up|down}

#/sbin/ip -6 addr add <ipv6_address>/<prefixlength> dev <interface>
#/sbin/ifconfig <interface> inet6 add <ipv6_address>/<prefixlength>
```

Para configurar as rotas:

```
#ip -6 route flush all
#ip -6 route add <ipv6_address>/<prefixlength> via <gateway>
#route -A inet6 add <ipv6_address>/<prefixlength> gw <gateway>
```

1. *R:* O router da rede origem tem duas interfaces, uma para a “Internet e outra para a rede origem. Deve, por isso, ter activo o encaminhamento (forwarding).

```
#Interface eth0
ip link set dev eth0 down
ip link set dev eth0 up
ip -6 addr add 2000:a::1/64 dev eth0

#Interface eth1
/sbin/ifconfig eth1 down

#Interface eth2
/sbin/ifconfig eth2 down
/sbin/ifconfig eth2 up
/sbin/ip -6 addr add 2000:b::1/64 dev eth2

#Activate IPv6 forwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

#Configuring Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:b::2
```

2. *AR:* O router de acesso (na rede visitada), também tem duas interfaces, uma para a Internet, e a outra para a sua rede. Também neste o encaminhamento deve estar activo.

```
#interface eth0
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
/sbin/ip -6 addr add 2000:b::2/64 dev eth0

#interface eth1 - realtek
ip link set dev eth1 down
ip link set dev eth1 up
/sbin/ip -6 addr add 2000:c::2/64 dev eth1

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:b::1
```

3. *HA:* O Home Agent tem uma interface. Deverá ter o forwarding activo, porque ele usa encaminhamento normal para reenviar os pacotes capturados na interface física para a interface túnel virtual.

```
#interface eth0 - Intel
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
/sbin/ip -6 addr add 2000:a::10/64 dev eth0

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
```

```
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:a::1
```

4. *MN:* O nó móvel possui apenas uma interface de rede. O encaminhamento deve ser desligado, mas deverá aceitar auto configuração e router advertisements.

```
#interface eth1 - Intel
#/sbin/ifconfig eth1 down
/sbin/ifconfig eth1 up
/sbin/ip -6 addr add 2000:a::20/64 dev eth1


#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=0
/sbin/sysctl -w net.ipv6.conf.all.autoconf=1
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=1
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=1


#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:a::1
```

É preferível o uso do sysctl a mudar as variáveis do proc (echo "0" > /proc/sys/net/ipv6/conf/eth0/), pois o sysctl muda os parâmetros do kernel em runtime.

Se no cenário forem usados APs nas redes origem e visitada, os terminais deverão usar o seguinte comando de modo a garantir conectividade com estes:

```
iwconfig eth0 mode managed essid <ESSID> enc off
```

A encriptação é desligada para efeitos de teste. Outras configurações no terminal poderão ser necessárias em função das configurações do AP, ver “man iwconfig”.

Se no cenário forem usados placas de rede unicamente, então deverá ser usado:

```
iwconfig eth0 mode ad-hoc essid <ESSID> enc off
```

Nota: Neste momento, com os endereços IPv6 e rotas estáticas configurados, deverá existir conectividade entre todos os nós. Poderá ser usado o ping6 para verificar esta condição.

4.2.2. Configuração da Mobilidade IPv6

A ultima configuração é a do ficheiro mip6d.conf. Se não for dito nada ao mip6d, ele procura o ficheiro de configuração em “/usr/local/etc/mip6d.conf”, pode no entanto ficar noutra localização, indicando ao mip6d qual “mip6d -c <dir>/<fileName>. Este ficheiro não é criado no momento da instalação, portanto terá de ser criado manualmente. Na pasta extra das userspace tools encontram-se 3 exemplos de configuração do CN, HA e MN. Estes ficheiros também se encontram em anexo neste HOWTO.

Para auxiliar a tarefa de configuração poderão ser consultadas as páginas do manual electrónico:

- Man mipv6
- Man mip6d
- Man mip6d.conf

1. CN: O CN poderá ser o AR, e deverá ter no ficheiro de configuração os seguintes parâmetros.

```
# This is an example of mip6d Correspondent Node configuration file

NodeConfig CN;

## If set to > 0, will not detach from tty
DebugLevel 0;

## Support route optimization with MNs
DoRouteOptimizationCN enabled;
```

2. *HA:* O ficheiro de configuração do HA deverá ter os seguintes parâmetros.

```
 # This is an example of mip6d Mobile Node configuration file

#Common Options
#####################################################################

#Set the mode witch the daemon will run
NodeConfig HA;

## Support route optimization with other MNs
DoRouteOptimizationCN enabled;

#Options Specific to Home Agent and Mobile Node
#####################################################################

#Specifies the interface and options. If no options "Interface "eth0""
Interface "eth0";

#We won't use IPSec
UseMnHaIPsec disabled;

#Home Agent Specific Options
#####################################################################

#END
```

3. *MN:* O ficheiro de configuração do MN deverá ter os seguintes parâmetros.

```
 # This is an example of mip6d Mobile Node configuration file

#Common Options
#####################################################################

#Set the mode witch the daemon will run
NodeConfig MN;

## Support route optimization with other MNs
DoRouteOptimizationCN enabled;
```

```
#Options to Home Agent e Mobile Node
#################################################################

#Specifies the interface and options. If no options "Interface "eth0""
Interface "eth1";

#
UseMnHaIPsec disabled;

#Mobile Node Specific Options
#################################################################

#
SendMobPfxSols enabled;

## Use route optimization with CNs
DoRouteOptimizationMN enabled;

#
UseCnBuAck enabled; #Default disabled;


MnHomeLink "eth1" {

      HomeAddress 2000:a::20/64;

      HomeAgentAddress 2000:a::10; #Default ::

}
#END
#################################################################
```

4. De seguida inicie o mip6d no CN, HA e MN (a linha de código poderá ser adicionada aos scripts apresentados no ponto 4.2.1.):

```
mip6d -c /usr/local/etc/mip6d.conf
```

5. Para ver o output do debug na consola, usar a opção –d com um valor de 1 a 10 (0 não mostra nada, maior que 1 bloqueia a consola. Não é erro! É suposto acontecer! Depois são mostradas mensagens de debug na sequência de eventos):

```
mip6d –d<num> #num={0;10}
```

Após iniciar o mip6d, é possível verificar que no MN foi criado um túnel virtual (no HA o túnel só é criado quando o MN muda de rede e faz o binding update).

```
[root@localhost ~]# ifconfig
eth1      Link encap:Ethernet  HWaddr 00:11:11:59:0E:99
          inet6 addr: 2000:a::20/64 Scope:Global
          inet6 addr: fe80::211:11ff:fe59:e99/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:130 errors:0 dropped:0 overruns:0 frame:0
          TX packets:19 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15224 (14.8 KiB)  TX bytes:1730 (1.6 KiB)
          Base address:0xbc00 Memory:ff8e0000-ff900000
```

```
ip6tnl1   Link encap:UNSPEC  HWaddr 20-00-00-0A-00-00-00-00-00-00-00-00-00-00-00-00 ❶
          inet6 addr: fe80::211:11ff:fe59:e99/64 Scope:Link
          UP POINTOPOINT RUNNING NOARP  MTU:1460  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3649 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3649 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4554342 (4.3 MiB)  TX bytes:4554342 (4.3 MiB)
```

❶ Túnel criado pelo mip6d no MN.

4.2.3. Configurar radvd no AR

Quando o MN se move para uma nova rede, ele faz uma configuração link local (através dos pacotes Neighbor discover e neighbor advertisement), e avança para a próxima fase se tudo correr bem. A [RFC2462] (IPv6 Stateless Address Autoconfiguration) descreve a próxima fase:

"(…)A próxima fase da auto-configuração, envolve a obtenção de um Router Advertisement ou determinar que nenhum router está presente. Se houver routers, eles enviam um Router Advertisement que especifica que tipo de auto-configuração o nó deve fazer. Se não houver routers, então deve ser invocada a auto-configuração statefull.(…)"

"(…)Os Routers enviam RAs periodicamente, mas o atraso entre sucessivos RAs é geralmente mais longo do que um nó em auto-configuração pretende esperar. Para obter um RA rapidamente um nó envia um ou mais Router Solicitations para o grupo multicast all-routers.(…)." --- pág. 8

Nesta testebed será usada configuração Stateless usando o RADVD para gerar RAs.

Ler a [RFC2462] para mais detalhes sobre a configuração Stateless (IPv6 Stateless Address Autoconfiguration).

Para configurar o RADVD na interface do AR, deverá ser editado primeiro o ficheiro /etc/radvd.conf. Um exemplo dessa configuração é apresentada de seguida:

```
# cat /etc/radvd.conf
interface eth1
{
      AdvSendAdvert on;
      AdvIntervalOpt on;

# These settings cause advertisements to be sent every 3-10 seconds.
      MinRtrAdvInterval 1;
```

```
      MaxRtrAdvInterval 3;

      AdvHomeAgentFlag off;

      prefix 2000:c::/64
      {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
      };
};
```

Após editado o ficheiro, pode-se iniciar o serviço:

```
# /etc/init.d/radvd start
```

Após iniciar o deamon radvd, poderá ser usado o ethereal para visualizar se as mensagens estão a ser enviadas periodicamente, ou então recorrer ao comando **radvdump**:

```
[root@localhost ~]# radvdump
Router advertisement from fe80::230:4fff:fe0a:49a0 (hoplimit 255)
Received by interface eth1
        # Note: {Min,Max}RtrAdvInterval cannot be obtained with radvdump
        AdvCurHopLimit: 64
        AdvManagedFlag: off
        AdvOtherConfigFlag: off
        AdvHomeAgentFlag: off
        AdvReachableTime: 0
        AdvRetransTimer: 0
        Prefix 2000:c::/64
                AdvValidLifetime: 2592000
                AdvPreferredLifetime: 604800
                AdvOnLink: on
                AdvAutonomous: on
                AdvRouterAddr: on
        AdvSourceLLAddress: 00 30 4F 0A 49 A0
        AdvIntervalOpt:
                AdvInterval: 10
```

Nota! Quando é usado o radvd no HA e é activada a auto configuração no MN, então a interface deste irá configurar um endereço por auto configuração (que será supérfluo) para além do endereço estático.

4.2.4. Configurar radvd no HA

Para permitir que o MN saiba quando regressa à rede origem, deverá existir nesta uma entidade que envia RAs, que neste caso será o HA. Deverá então ser activado o RADVD no HA, mas não sem antes editar o ficheiro /etc/radvd.conf.

```
interface eth0
{
      AdvSendAdvert on;
      AdvIntervalOpt on;

# These settings cause advertisements to be sent every 1-3 seconds.

      MinRtrAdvInterval 1;
      MaxRtrAdvInterval 3;
```

```
      AdvHomeAgentFlag on;

HomeAgentLifetime 10000;
HomeAgentPreference 20;
AdvHomeAgentInfo on;

      prefix 2000:a::/64
      {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
            AdvPreferredLifetime 500;
            AdvValidLifetime 600;
      };
};
```

Uma vez mais o ethereal ou o **`radvdump`** no HA para verificar o envio dos RAs.

```
    # radvdump
    Router advertisement from fe80::202:2dff:fe54:d11e (hoplimit 255)
    Received by interface eth0
        # Note: {Min,Max}RtrAdvInterval cannot be obtained with radvdump
        AdvCurHopLimit: 64
        AdvManagedFlag: off
        AdvOtherConfigFlag: off
        AdvHomeAgentFlag: on
        AdvReachableTime: 0
        AdvRetransTimer: 0
        Prefix fec0:106:2700::2/64
                AdvValidLifetime: 12000
                AdvPreferredLifetime: 10000
                AdvOnLink: on
                AdvAutonomous: on
                AdvRouterAddr: on
        AdvSourceLLAddress: 00 02 2D 54 D1 1E
        AdvHomeAgentInfo:
                HomeAgentPreference: 20
        HomeAgentLifetime: 1000
```

Após a configuração dos RAs no HA, poderá ser vista a alteração provocada no MN.

```
[root@localhost ~]# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:11:11:59:0E:99
          inet6 addr: 2000:a::211:11ff:fe59:e99/64 Scope:Global❶
          inet6 addr: fe80::211:11ff:fe59:e99/64 Scope:Link❷
          inet6 addr: 2000:a::20/64 Scope:Global❸
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:924 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:93984 (91.7 KiB)  TX bytes:8770 (8.5 KiB)
     Base address:0xbc00 Memory:ff8e0000-ff900000
```

❶

O endereço supérfluo auto configurado. Uma vez que no MN a auto configuração foi activada e o HA envia RAs, o MN gera um novo endereço combinando o prefixo do HA e o seu próprio endereço MAC

❷ O endereço link-local address gerado no boot.

❸ O endereço IPv6 configurado estaticamente.

4.3. Configurar a interface do MN para definir o endereço estático

A interface poderá estar configurada para obter o endereço automaticamente via rede. Isso irá interferir com os testes, por isso tem de se mudar a configuração:

- Aceder ao menu de configuração das interfaces:

Menu>Network Device Control>Configure

- Seleccionar a interface de saída do MN e editar a sua configuração

Interface eth0>edit

- Seleccionar a opção:

Statically Set Ip Addresses>Ok

4.4. Desligar interfaces que não são usadas

Para prevenir resultados indesejados, aconselha-se a desligar todas as interfaces que não são usadas no cenário. Por exemplo, se o MN tiver duas interfaces de rede, então deverá ser desligado o que não é usado.

5. Testes

5.1. Teste primário

Após realizadas todas as configurações mostradas anteriormente é necessário realizar alguns testes para confirmar o funcionamento do mipv6. Se forem usados cenários wireless (com APs e placas wireless), devem ser configurados ESSIDs diferentes na rede origem e rede visitada.

Quando é iniciado o mip6d no MN, é possível verificar o envio de mensagens (router solicitations) multicast.

```
[root@localhost ~]# tcpdump -i eth1 -vv ip6 or proto ipv6
(...)
10:32:53.274337 :: > ff02::2: [icmp6 sum ok] icmp6: router solicitation
(len 8, hlim 255)
10:32:53.320868 fe80::230:4fff:fe0a:49a0 > ff02::1: icmp6: router
advertisement(chlim=64, pref=medium, router_ltime=9, reachable_time=0,
retrans_time=0)[ndp opt] (len 64, hlim 255)
10:32:53.322753 :: > ff02::16: HBH (rtalert: 0x0000) (padn)icmp6: type-#143
[hlim 1] (len 56)
10:32:53.467738 :: > ff02::1:ff59:e99: [icmp6 sum ok] icmp6: neighbor sol:
who has 2000:c::211:11ff:fe59:e99 (len 24, hlim 255)
```

5.2. Detecção de movimento

A detecção genérica de movimento usa mensagens “Neighbor Unreachability Detection” para detectar quando é que o default router não está bi-direccionalmente alcançável, o que neste caso força o nó a descobrir um novo default router (geralmente num novo link).

Para verificar o que acontece, poderá ser usado o Ethereal para ver a troca de mensagens, e alguns comandos em diferentes janelas de consola, como por exemplo:

```
# watch ifconfig eth0
# watch route -A inet6
# tcpdump -i eth0 -vv ip6 or proto ipv6
```

Para se mover para uma nova rede, no caso do cenário com cabo, basta simplesmente mudar o cabo de um hub para outro. No caso do cenário wireless, pode ser desligado o AP da rede origem e ligado o da rede destino (processo não aconselhável) ou então pode ser indicado por comando ao MN para se ligar à outra rede

```
# iwconfig eth0 essid visitnet
```

O MN muda assim para outra rede, e uma vez que está a enviar "router solicitation" (multicast), o AR responde com o seu prefixo. O MN procede então à sua autoconfiguração, criando um novo endereço IPv6 a partir do prefixo recebido e do seu próprio MAC. O comando “ifconfig eth0” permite ver a o novo endereço.

```
[root@localhost ~]# ifconfig eth0
eth1      Link encap:Ethernet  HWaddr 00:11:11:59:0E:99
          inet6 addr: 2000:c::211:11ff:fe59:e99/64 Scope:Global❶
```

```
          inet6 addr: 2000:a::211:11ff:fe59:e99/64 Scope:Global❷
          inet6 addr: fe80::211:11ff:fe59:e99/64 Scope:Link❸
          inet6 addr: 2000:a::20/64 Scope:Global❹
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:924 errors:0 dropped:0 overruns:0 frame:0
          TX packets:77 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:93984 (91.7 KiB)  TX bytes:8770 (8.5 KiB)
          Base address:0xbc00 Memory:ff8e0000-ff900000
```

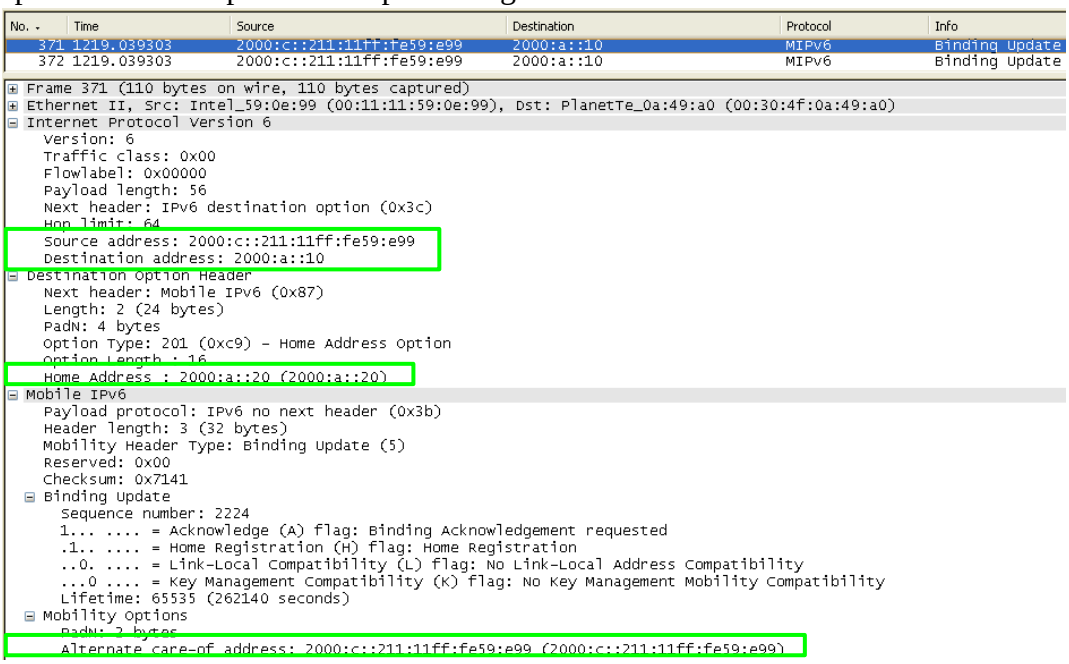
❶ O novo Care of Address, gerado combinando o MAC com o prefixo do AR.

❷ O endereço supérfluo da rede origem.

❸ O endereço link local gerado no boot

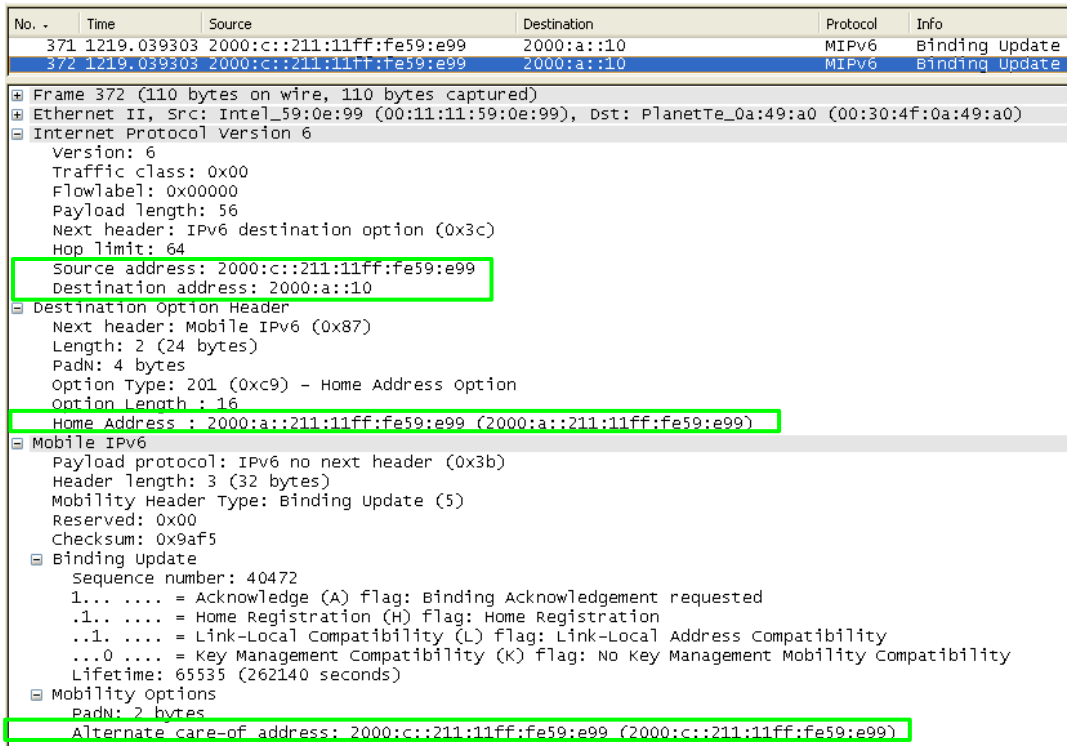
❹ O Home Address

Quase ao mesmo tempo, o MN irá enviar o binding update para o HA. Na janela tcpdump é possível ver vários pacotes enviados para o HA. O ethereal também pode ser usado para verificar o envio de mensagens quando existe movimento, como por exemplo os bindings updates enviados para o HA após configurar o CoA.



Binding update enviado para o HA

È possível verificar que a mensagem tem origem no CoA do MN com destino ao HA. No Destination Option Header podemos verificar a indicação do Home Address.
No cabeçalho Mobility options segue a indicação do CoA, que é igual ao source address do cabeçalho IPv6.
Na sequência do movimento foi enviado mais do que 1 pacote. Isto justifica-se pelo facto de o MN ter configurado mais do que um endereço da rede origem, porem isto não está especificado na RFC e não devia acontecer, uma vez que só 1 desses 2 endereços é que é o HoA, e só será criado um túnel entre o MN e HA com base neste endereço.



Binding update enviado para o HA

5.3. ping6

O comando ping6 pode ser usado para testar a conectividade antes durante e após o *handover*. O ideal será antes do *handover* colocar o MN a pingar a uma máquina, por exemplo a interface 1 do AR, e colocar esta máquina a pingar ao MN. Recorde-se que neste cenário a máquina AR foi configurada para funcionar também como CN. Esta configuração não é necessária para haver conectividade, mas sim para o processo de optimização de rotas. O uso do traceroute6 é desaconselhado.

No caso do cenário wired, haverá sempre perda de pacotes, dependendo da rapidez da mudança do cabo. No caso do cenário sem fios é suposto não haver perda de pacotes.

Ping do MN para o AR durante o *handover*:

```
[root@localhost ~]# ping6 2000:c::2
PING 2000:c::2(2000:c::2) 56 data bytes
64 bytes from 2000:c::2: icmp_seq=0 ttl=63 time=0.347 ms
64 bytes from 2000:c::2: icmp_seq=1 ttl=63 time=0.372 ms
ping: sendmsg: Invalid argument
ping: sendmsg: Invalid argument
From 2000:a::20 icmp_seq=7 Destination unreachable: Address unreachable
64 bytes from 2000:c::2: icmp_seq=8 ttl=62 time=0.584 ms
64 bytes from 2000:c::2: icmp_seq=9 ttl=62 time=0.612 ms
```

O Ping do AR para o MN também pode ser usado durante o *handover* para verificar que o MN está alcançável antes e depois. O ethereal pode ser usado para verificar que existe optimização de rotas entre o MN e o AR/CN (o host AR do cenário foi configurado anteriormente como CN).

Fazendo o ping do host R para o MN, uma vez que aquele não foi configurado como MN, é possível verificar que a comunicação é realizada através do HA em ambos os sentidos.

Outro comando que pode ser usado para verificar o percurso dos pacotes é o traceroute6, mas nos testes com mipv6 os resultados deste comando são muito inconsistentes devido ao uso de túneis, e por isso se desaconselha o seu uso.

5.4. Tabela de encaminhamento IP do Kernel

Algo interessante no MIPv6 é que ele muda a sua default route para o túnel que criou do MN para o HA:

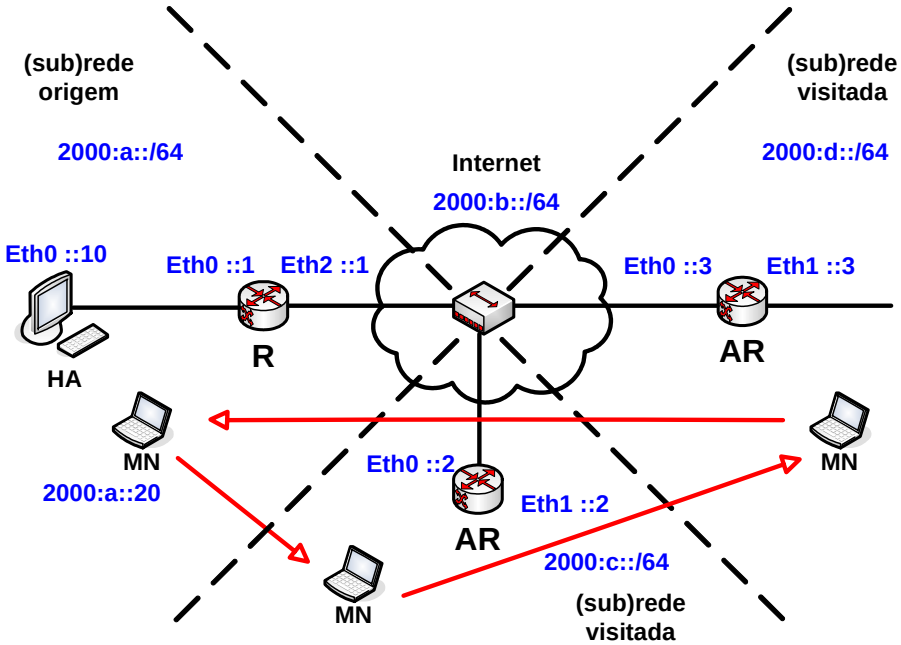
```
# route -A inet6
Kernel IPv6 routing table
Destination      Next Hop       Flags Metric Ref    Use Iface
::/0             ::             UD    64     0        0 ip6tnl1
```

Caso não mude, uma rota poderá ser adicionada manualmente:

```
# ip route ::/0 via dev ip6tnl
```

5.5. Mover-se através de várias redes

Mover-se ao longo de várias redes visitadas não é muito diferente do que viajar através de uma. Há que ter em conta é que por cada rede visitada será criado um novo endereço por auto configuração.



O MN a mover-se por várias redes..

1. O MN visita uma rede, auto configura um CoA e faz um binding update no HA.
2. O MN move-se de uma rede visitada para outra e faz novo BU no HA.
3. O MN regressa à rede origem

O AR na rede D está configurado exactamente como o da rede C, excepto que está configurado noutra rede. No caso do uso de cenários com APs, terá de se configurar outro ESSID no AP desta rede diferente dos outros, ou no caso de se usarem interfaces wireless nos terminais terá de se atribuir um ESSID ao AR da rede D:

```
# iwconfig eth0 essid <ESSID da rede D>
```

5.6. Regresso à rede origem

Para fazer o regresso à rede origem, no caso do cenário wired basta ligar o cabo do MN ao hub da rede origem, e no caso do cenário wireless basta mudar o ESSID ao qual o MN está associado:

```
# iwconfig eth0 essid <ESSID da rede origem>
```

Como o HA envia periodicamente mensagens radvd com o bit HA activo (AdvHomeAgentFlag enable), o MN irá detectar que regressou à rede origem.

Poderá verificar-se que o MN se registou correctamente analisando a informação da binding cache do HA, que deverá estar vazia. Isto poderá ser realizado através do output do Debug do HA.

5.7. Teste em comunicações - smooth *handover*

Para verificar a funcionalidade do MIPv6 numa comunicação real, poderá ser usado o GnomeMeeting (ver figura abaixo). Este programa permite estabelecer uma comunicação de voz e vídeo extremo-a-extremo.

Após instalar e configurar o programa em duas máquinas, poderá ser iniciada uma comunicação, e durante esta poderão ser realizadas algumas mudanças de rede de modo a ver *handovers* suaves, mas só para o caso de um cenário wireless como é óbvio. A versão do GnomeMeeting terá de ter suporte de IPv6.

Imagem do uso do gnomeMeeting para testar o roaming entre as redes wireless.

5.7. Outros Testes

Outros testes poderão ser realizados usando aplicações para gerar tráfego e medir os parâmetros da comunicação, tais como o MGEN e o TRPR.

6. FAQ

Esta FAQ foi construída com base na existente no HowTo original, foi actualizada, e foram acrescentados novos tópicos com base na mailing list oficial do MIPv6 e em diversas pesquisas realizadas no âmbito deste trabalho.

1. *Q: Porque é que é necessário criar a entrada `/dev/mipv6_dev`?*

   A: O ficheiro dev serve, principalmente, para que a ferramenta mipv6 possa fazer modificações aos parâmetros do kernel, usando chamadas ioctl através do ficheiro do dispositivo. O mknod cria um ficheiro de dispositivo especial com parâmetros reconhecíveis pelo mipv6.

2. *Q: O MIPL suporta IPSec?*

   A: A partir da versão 2.6 do MIPL, que foi implementado suporte para IPSec de raiz. A *[RFC 3776] define este processo.*

3. *Q: Como se pode controlar os parâmetros de mobilidade tais como o uso de IPSec na comunicação ou o uso ou não de optimização de rotas?*

   DoRouteOptimizationMN enabled;
   UseMnHaIPsec enabled;
   (…) Ver man mip6d.conf

4. *Q: Será que diferentes redes wireless podem ter diferentes chaves WEP?*

   A: Sim, mas terá de ser mudado aquando da mudança para a nova rede, uma vez que o MIPv6 do MIPL não consegue realizar este processo automaticamente.

5. *Q: Se o MN viajar ao longo de várias LANs, regressando depois a casa, a interface irá guardar todos os endereços IPv6 auto configurados de todas as redes que visitou? Haverá uma maneira de remover estes endereços?*

   A: Os endereços têm um tempo de vida definido nos router advertisements, findo o qual são eliminados. Também poderão ser eliminados manualmente:

   ```
   # ifconfig eth0 inet6 del <ipv6-address>/<prefix-length>
   ```

6. *Q: A máquina B tem duas interfaces com duas sub redes diferentes atribuídas. Quando a máquina A pinga a máquina B, esta não responde. A máquina A sabe onde a máquina B está!*

   A: A máquina B poderá não saber onde está a máquina/rede B. Deverá ser adicionada uma rota:

   ```
   # ip route add 2000:a::1/64 via 2000:c::2
   ```

   ou

   ```
   # route -A inet6 add 2000:a::1/64 gw 2000:c::2 dev eth0
   ```

7. *Q: Como se configura um default gateway em IPv6?*

   A: Usando a tradicional rota:

   ```
   # route -A inet6 add default gw <ipv6-host>
   ```

   Ou o commando ip:

   ```
   # ip -6 route add ::/0 via <ipv6-host>
   ```

8. *Q: Porque é que o terminal envia um endereço multicast em vez do anycast, quando envia o router solicitation?*

   A: Porque quer uma resposta de todos os routers, não de qualquer um. A ideia é receber todos os parâmetros e escolher o melhor default router.

9. *Q: Porque é que o MN por vezes não consegue detectar o movimento?*

   A: Ele pensa que o seu router anterior ainda está alcançável. Isto resulta de tempos de vida elevados dos router advertisements. Estes valores poderão ser manipulados, editando o ficheiro /etc/radvd.conf (nos routers que enviam os RA, e.g. no caso do cenário serão os routers AR e HA), alterando os valores mínimos e máximos dos intervalos de envio destes. Consultar man radvd.conf para mais informação.

10. *Q: Posso usar endereços do tipo a::/64 de modo a simplificar e poupar tempo nos testes?*

    A: Não, não deverão ser usados. Apesar de ser possível configurar as interfaces com estes endereços, não será possível configurar o gateway. Os comandos :

    ```
    # route -A inet6 add default gw <ipv6-host>

    # ip -6 route add ::/0 via <ipv6-host>
    ```

    não suportam este tipo de endereços, apenas os começados pelos prefixos alocados pela IANA (http://www.iana.org/assignments/ipv6-address-space), nomeadamente endereços globais 2000::/3.

11. *Q: Posso usar endereços site-local, com prefixo fec0::64?*

    A:. Os endereços FEC0::/10 foram anteriormente definidos como Site-local, no entanto esta definição foi destituída em Setembro de 2004 pela RFC 3879.

12. *Q:* O libnetlink é distribuído com o MIPL*?*

    A: Uma versão modificada do libnetlink é distribuída com o MIPL. Esta versão não inclui todas as funcionalidades da package da libnetlink, apenas as necessárias para o funcionamento do MIPL.

13. Existem algumas implementações disponíveis para testar ou ver o modo de operação do MIPv6?

A: Na mailing List vêm referenciados algumas aplicações desenvolvidas para o efeito

http://www.bullopensource.org/mipv6/index.php

http://www.cavone.com/mipv6-analyzer/

14. *Q:* No debug aparece o erro “DoD failed” quando existe o *handover*, e a mobilidade não funciona!

    A: O MIPL usado vai no 3º pré-lançamento antes de sair a versão final, portanto poderão existir alguns erros, falhas ou alguns processos a melhorar. Mudando o HoA na interface do MN e no ficheiro mip6d.conf é o suficiente para voltar a testar a mobilidade

15. Existem implementações publicas do RFC 4068 "Fast *Handovers* for Mobile IPv6" e/ou RFC 4140 "Hierarchical Mobile IPv6 Mobility Management HMIPv6)".

    A: Ver os sítios:
    http://www.ctie.monash.edu.au/ipv6/
    http://www.tkn.tu-berlin.de/research/hmip/

7. Recursos

1. Mobile IPv6 for Linux http://www.mobile-ipv6.org/
2. Linux Mobile IPv6 HowTo http://www.tldp.org/HOWTO/Mobile-IPv6-HOWTO/
3. Mobile IPv6 Working Group (IETF) http://www.ietf.org/html.charters/mip6-charter.html
4. IPv6 Working Group (IETF) http://www.ietf.org/html.charters/ipv6-charter.html
5. RFC 3775 Mobility for IPv6 http://www.ietf.org/rfc/rfc3775.txt?number=3775
6. RFC 3776 Using IPSec to Protect MIPv6 Signaling Between MN and HA http://www.ietf.org/rfc/rfc3775.txt?number=3775
7. RFC 2460 Internet Protocol, Version 6 (IPv6) Specification http://www.ietf.org/rfc/rfc2460.txt
8. RFC2461 Neighbor Discovery for IP Version 6 (IPv6) http://www.ietf.org/rfc/rfc2461.txt
9. RFC2462 IPv6 Stateless Address Autoconfiguration http://www.ietf.org/rfc/rfc2462.txt
10. Peter Bieringer's Linux IPv6 HOWTO (en) http://ldp.linux.no/HOWTO/Linux+IPv6-HOWTO/
11. Current Status of IPv6 Support for Networking Applications http://www.deepspace6.net/docs/ipv6_status_page_apps.html
12. MIPL MailingList Archives http://www.mobile-ipv6.org/pipermail/mipl/
13. Endereçamento IPv6 http://www.iana.org/assignments/ipv6-address-space

E - Configurações dos cenários de teste

De seguida são apresentadas as diversas configurações realizados nos vários cenários de teste..

E.1 Cenário 1 – topologia com fios com máquinas Linux

Script de configuração dos endereços nas interfaces do MN

```
#!/bin/bash
#Mobile Node Configuration

#interface eth1 - intel
/sbin/ifconfig eth1 down
/sbin/ifconfig eth1 up
/sbin/ip -6 addr add 2000:a::20/64 dev eth1
#/sbin/ip -6 addr add 2000:a::211:11ff:fe59:e99/64 dev eth1

#Show configurations
ifconfig
```

Script de configuração das rotas e MIPv6 do MN

```
#!/bin/bash
#Mobile Node Configuration

clear

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=0
/sbin/sysctl -w net.ipv6.conf.all.autoconf=1
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=1
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=1

#
echo "0" > /proc/sys/net/ipv6/conf/eth1/forwarding
echo "1" > /proc/sys/net/ipv6/conf/eth1/autoconf
echo "1" > /proc/sys/net/ipv6/conf/eth1/accept_ra
echo "1" > /proc/sys/net/ipv6/conf/eth1/accept_redirects

#Routes
ip -6 route flush all
#ip -6 route add ::/0 via 2000:a::1
route -A inet6 add ::/0 gw 2000:a::1

#Show configurations
ip -6 route show
route -A inet6 -n

#test configurations
echo "###############Ping to Next hop"
ping6 -c 2 2000:a::1 #Next hop
echo "###############Ping to foreign network"
ping6 -c 2 2000:c::2 #Foreign network

#
mip6d start
```

```
#mip6d -c /usr/local/etc/mip6d.conf
#mip6d stop
```

Ficheiro de configuração do mip6d no MN.

```
# mip6d Mobile Node configuration file
#/usr/local/etc/mip6d.conf

#Common Options
#################################################################

#Set the mode witch the daemon will run
NodeConfig MN; #

## Support route optimization with other MNs
DoRouteOptimizationCN enabled;


#Options to Home Agent e Mobile Node
#################################################################

#Specifies the interface and options. If no options "Interface "eth0""
Interface "eth1";

#
UseMnHaIPsec disabled;


#Mobile Node Specific Options
#################################################################
#
SendMobPfxSols enabled;

## Use route optimization with CNs
DoRouteOptimizationMN enabled;

#
UseCnBuAck enabled; #Default disabled;

#
MnHomeLink "eth1" {
      HomeAddress 2000:a::20/64;
      HomeAgentAddress 2000:a::10; #Default ::
}
#################################################################
```

Script de configuração dos endereços nas interfaces do HA

```
#!/bin/bash

#Home Agent configuration

#interface eth0 - intel
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
/sbin/ip -6 addr add 2000:a::10/64 dev eth0

#Show configurations

ifconfig
```

Script de configuração das rotas e MIPv6 do HA

```
#!/bin/bash

clear

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

#
echo "1" > /proc/sys/net/ipv6/conf/eth0/forwarding
echo "0" > /proc/sys/net/ipv6/conf/eth0/autoconf
echo "0" > /proc/sys/net/ipv6/conf/eth0/accept_ra
echo "0" > /proc/sys/net/ipv6/conf/eth0/accept_redirects

#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:a::1
route -A inet6 add ::/0 gw 2000:a::1

#Show configurations
ip -6 route show
route -A inet6 -n

#test configurations

echo "###############Ping to Next hop"
ping6 -c 2 2000:a::1 #Next hop

echo "###############Ping to foreign network"
ping6 -c 2 2000:c::2 #Foreign network

#
mip6d -c /usr/local/etc/mip6d.conf
mip6d start

#(Des)Activate router advertisements
#radvd stop
radvd start

#chkconfig --list | grep radvd
#chkconfig --level 234 radvd off
#service radvd stop
```

Ficheiro de configuração do mip6d no HA.

```
# This is an example of mip6d Mobile Node configuration file



#Common Options
#################################################################

#Set the mode witch the daemon will run
NodeConfig HA; #

## Support route optimization with other MNs
DoRouteOptimizationCN enabled; #Default enabled
```

```
#Options to Home Agent e Mobile Node
#################################################################

#Specifies the interface and options. If no options "Interface "eth0""
Interface "eth0";

#
UseMnHaIPsec disabled;


#Home Agent Specific Options
#################################################################


#END
#################################################################
```

Ficheiro de configuração do radvd no HA.

```
interface eth0
{
      AdvSendAdvert on;
      AdvIntervalOpt off;

#
# These settings cause advertisements to be sent every 3-10 seconds.  This
# range is good for 6to4 with a dynamic IPv4 address, but can be greatly
# increased when not using 6to4 prefixes.
#

      MinRtrAdvInterval 1;
      MaxRtrAdvInterval 3;

      AdvHomeAgentFlag on;

HomeAgentLifetime 10000;
HomeAgentPreference 20;
AdvHomeAgentInfo on;

#
# example of a standard prefix
#
      prefix 2000:a::/64
      {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
            AdvPreferredLifetime 500;
            AdvValidLifetime 600;
      };
};
```

Script de configuração dos endereços nas interfaces do R1

```
#!/bin/bash

#Sources
#http://ldp.linux.no/HOWTO/Linux+IPv6-HOWTO/
#http://www.tldp.org/HOWTO/Mobile-IPv6-HOWTO/

clear

#Interface eth0 - 3COM
ip link set dev eth0 down
ip link set dev eth0 up
ip -6 addr add 2000:a::1/64 dev eth0


#Interface eth1 - Intel (used for internet, not for the scenario)
/sbin/ifconfig eth1 down


#Interface eth2 - Realtek
/sbin/ifconfig eth2 down
/sbin/ifconfig eth2 up
/sbin/ip -6 addr add 2000:b::1/64 dev eth2


#Show configurations
ifconfig
```

Script de configuração das rotas do R1

```
#!/bin/bash

#Sources
#http://ldp.linux.no/HOWTO/Linux+IPv6-HOWTO/
#http://www.tldp.org/HOWTO/Mobile-IPv6-HOWTO/


#Routes
ip -6 route flush
ip -6 route add ::/0 via 2000:a::1 #Works!!
#route -A inet6 add ::/0 gw 2000:a::1 #Works!!


#Used for MIPv6 scenario
echo "0" > /proc/sys/net/ipv6/conf/eth1/forwarding
echo "1" > /proc/sys/net/ipv6/conf/eth1/autoconf
echo "1" > /proc/sys/net/ipv6/conf/eth1/accept_ra
echo "1" > /proc/sys/net/ipv6/conf/eth1/accept_redirects

/sbin/sysctl -w net.ipv6.conf.all.forwarding=0
/sbin/sysctl -w net.ipv6.conf.all.autoconf=1
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=1
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=1


#mip6d stop
#mip6d -c /usr/local/etc/mip6d.conf
#mip6d start

#Show configurations
ifconfig
```

```
ip -6 route show
route -A inet6 -n


#Test configurations
echo "##########Ping to Next hop"
ping6 -c 2 2000:a::1 #Next hop

echo "##########Ping to Foreign network"
ping6 -c 2 2000:c::3 #Foreign net
```

Script de configuração dos endereços nas interfaces do R2

```
#!/bin/bash

#Access Route (AR) address configuration

clear

#/sbin/ip link set dev <interface> {up|down}
#/sbin/ifconfig <interface> {up|down}

#/sbin/ip -6 addr add <ipv6_address>/<prefixlength> dev <interface>
#/sbin/ifconfig <interface> inet6 add <ipv6_address>/<prefixlength>


#interface eth0 - intel - using ifconfig
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
/sbin/ip -6 addr add 2000:b::2/64 dev eth0

#interface eth1 - realtek - using ip
ip link set dev eth1 down
ip link set dev eth1 up
/sbin/ip -6 addr add 2000:c::2/64 dev eth1


#Show configurations - Comment to disable output
ifconfig
```

Script de configuração das rotas e MIPv6 do R2

```
#!/bin/bash

#Access Route (AR) ROUTE configuration

clear

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

/sbin/sysctl -w net.ipv6.conf.eth1.forwarding=1
/sbin/sysctl -w net.ipv6.conf.eth1.autoconf=0
/sbin/sysctl -w net.ipv6.conf.eth1.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.eth1.accept_redirects=0

/sbin/sysctl -w net.ipv6.conf.eth0.forwarding=1
/sbin/sysctl -w net.ipv6.conf.eth0.autoconf=0
```

```
/sbin/sysctl -w net.ipv6.conf.eth0.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.eth0.accept_redirects=0

#
#echo "1" > /proc/sys/net/ipv6/conf/eth0/forwarding
#echo "0" > /proc/sys/net/ipv6/conf/eth0/autoconf
#echo "0" > /proc/sys/net/ipv6/conf/eth0/accept_ra
#echo "0" > /proc/sys/net/ipv6/conf/eth0/accept_redirects


#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:b::1
route -A inet6 add ::/0 gw 2000:b::1


#Show configurations - Comment for disable output
ip -6 route show
route -A inet6 -n


#test configurations - Comment for disable output

echo "###############Ping to Next hop"
ping6 -c 2 2000:b::1 #Next hop

echo "###############Ping to foreign network"
ping6 -c 2 2000:a::1 #Foreign network


#Enable Mobile IPv6 mode
mip6d -c /usr/local/etc/mip6d.conf
mip6d start


#Before this step you should configure /etc/radvd.conf ->for AR
#(Des)Activate router advertisements
#radvd stop
#service radvd stop
radvd start
#service radvd restart

#chkconfig --level 0123456 radvd off
#chkconfig --list | grep radvd
#service radvd restart
```

Ficheiro de configuração do mip6d no R2 (CN).

```
# This is an example of mip6d Correspondent Node configuration file

NodeConfig CN;

## If set to > 0, will not detach from tty
DebugLevel 0; #DebugLevel 10;

## Support route optimization with MNs
DoRouteOptimizationCN enabled; #DoRouteOptimizationCN enabled;
```

Ficheiro de configuração do radvd no R2.

```
interface eth1
```

```
{
      AdvSendAdvert on;
      AdvIntervalOpt on;

#
# These settings cause advertisements to be sent every 3-10 seconds.  This
# range is good for 6to4 with a dynamic IPv4 address, but can be greatly
# increased when not using 6to4 prefixes.
#

      MinRtrAdvInterval 3;
      MaxRtrAdvInterval 10;

#
# Disable Mobile IPv6 support
#
      AdvHomeAgentFlag off;

#
# example of a standard prefix
#
      prefix 2000:c::/64
      {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
      };

#
# example of a 6to4 prefix
#
# Note that the first 48 bits are specified here as zeros.  These will be
# replaced with the appropriate 6to4 address when radvd starts or is
# reconfigured. Be sure that the SLA ID (1234 in this case) is specified
# here!
#
      #prefix 0:0:0:1234::/64
      #{
      #     AdvOnLink on;
      #     AdvAutonomous on;
      #     AdvRouterAddr off;

#
# This setting causes radvd to replace the first 48 bits of the prefix
# with the 6to4 address generated from the specified interface.  For
example,
# if the address of ppp0 is 192.0.2.25 when radvd configures itself, this
# prefix will be advertised as 2002:C000:0219:1234::/64.
#
# If ppp0 is not available at configuration time, this prefix will not be
# advertised, but other prefixes listed in the configuration will be
# advertised as usual.
#
# When using the Base6to4Interface option, make sure radvd receives a
# SIGHUP every time the ppp0 interface goes up, down, or is assigned a
# new IPv4 address.  The SIGHUP will cause radvd to recognize that the
# ppp0 interface has changed and will adjust the advertisements
# accordingly.
#

      #     Base6to4Interface ppp0;
```

```
#
# If the IP address of ppp0 is assigned dynamically, be sure to set the
# lifetimes for this prefix to be small.  Otherwise, hosts on your network
# may continue to use a prefix that no longer corresponds to the address
# on ppp0!
#
      #     AdvPreferredLifetime 120;
      #     AdvValidLifetime 300;
      #};

};
```

E.2 Cenário 2 – topologia com fios com máquinas Linux, IOS e XP

Configuração da máquina Linux (MN)

A configuração da máquina MN manteve-se igual à do cenário 1.

Configuração da máquina Windows XP SP2

```
#Iniciar -> Executar -> cmd
Ipv6 install
netsh
interface ipv6 set mobility bindingcachelimit=1000
correspondentnode=enabled store=persistent
#interface ipv6 show mobility
#interface ipv6 set mobility ?
```

Configuração da máquina R1

```
enable
conf t
hostname R1

ipv6 unicast-routing

interface FastEthernet0/0
 ipv6 enable
 no shutdown
 ipv6 address 2000:a::1/64
 ipv6 rip mipv6l enable
 ipv6 mobile home-agent
 no ipv6 nd suppress-ra
 ipv6 nd ra-interval 3


interface Serial0/0
 shutdown

interface Serial0/0
 ipv6 enable
 clock rate 56000
 no shutdown
 ipv6 address 2000:b::1/64 anycast
 ipv6 rip mipv6l enable
 ipv6 mobile home-agent
```

```
ipv6 router rip mipv6l
copy run start

exit
exit
```

Configuração da máquina R2

```
enable
conf t
hostname R2

ipv6 unicast-routing


interface FastEthernet0/0
 ipv6 enable
 no shutdown
 ipv6 address 2000:c::2/64 anycast
 ipv6 rip mipv6l enable
 ipv6 mobile home-agent
 no ipv6 nd suppress-ra
 ipv6 nd ra-interval 3


interface Serial0/0
 ipv6 enable
 clock rate 56000
 no shutdown
 ipv6 address 2000:b::2/64 anycast
 ipv6 rip mipv6l enable
 ipv6 mobile home-agent


ipv6 router rip mipv6l
copy run start

exit
exit
```

Comandos de debug e estatisticas do MIPv6 no IOS

```
debug ipv6 mobile binding-cache
debug ipv6 mobile forwarding
debug ipv6 mobile home-agent
debug ipv6 mobile registrations


sh ipv6 mobile binding
sh ipv6 mobile  globals
sh ipv6 mobile  home-agents
sh ipv6 mobile traffic
```

E.3 Cenário 3 – topologia sem fios com máquinas Linux

Script de configuração dos endereços nas interfaces do MN

```
#!/bin/bash
#Mobile Node (MN) address configuration

clear
/etc/init.d/network restart

#realtek - eth0
ip link set dev eth0 down

#realtek - eth1
ip link set dev eth1 down

#intel - eth2
ip link set dev eth2 down

#interface eth0 - aironet
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
/sbin/ip -6 addr add 2000:a::20/64 dev eth0

iwconfig eth0 mode ad-hoc essid homenet enc off
#iwconfig eth0 mode ad-hoc essid visitnet enc off

#Show configurations - Comment to disable output
ifconfig
```

Script de configuração das rotas e MIPv6 do MN

```
#!/bin/bash
#Mobile Node (MN) ROUTE configuration

clear

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=0
/sbin/sysctl -w net.ipv6.conf.all.autoconf=1
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=1
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=1

echo "0" > /proc/sys/net/ipv6/conf/eth0/forwarding
echo "1" > /proc/sys/net/ipv6/conf/eth0/autoconf
echo "1" > /proc/sys/net/ipv6/conf/eth0/accept_ra
echo "1" > /proc/sys/net/ipv6/conf/eth0/accept_redirects


#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:a::1

#Show configurations - Comment for disable output
ip -6 route show
route -A inet6 -n

#test configurations - Comment for disable output
echo "###############Ping to Next hop"
ping6 -c 2 2000:a::1 #Next hop
```

```
echo "##############Ping to foreign network"
ping6 -c 2 2000:c::2 #Foreign network


#Enable Mobile IPv6 mode
mip6d -c /usr/local/etc/mip6d.conf
#mip6d start
```

Ficheiro de configuração do mip6d no MN.

```
# This is an example of mip6d Mobile Node configuration file

##########################################
NodeConfig MN;

## If set to > 0, will not detach from tty
#DebugLevel 1;

## Support route optimization with other MNs
DoRouteOptimizationCN disabled;
##########################################

##########################################
Interface "eth1";
#{
#     MnIfPreference 10;
#}

UseMnHaIPsec disabled;
##########################################

##########################################
SendMobPfxSols disabled;

## Use route optimization with CNs
DoRouteOptimizationMN disabled;

UseCnBuAck disabled;

MnHomeLink "eth1" {
      HomeAgentAddress 2000:a::10;
      HomeAddress 2000:a::20/64;
}
##########################################
```

Script de configuração dos endereços nas interfaces do HA

```
#!/bin/bash
#Home Agent configuration

clear
/etc/init.d/network restart

#interface eth0 - intel
/sbin/ifconfig eth0 down

#interface eth1 - Aironet Cisco
/sbin/ifconfig eth1 down
/sbin/ifconfig eth1 up
/sbin/ip -6 addr add 2000:a::10/64 dev eth1
```

```
iwconfig eth1 mode ad-hoc essid homenet enc off

#Show configurations
ifconfig
```

Script de configuração das rotas e MIPv6 do HA

```
#!/bin/bash

clear

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

#
echo "1" > /proc/sys/net/ipv6/conf/eth0/forwarding
echo "0" > /proc/sys/net/ipv6/conf/eth0/autoconf
echo "0" > /proc/sys/net/ipv6/conf/eth0/accept_ra
echo "0" > /proc/sys/net/ipv6/conf/eth0/accept_redirects

#Routes
ip -6 route flush all
ip -6 route add ::/0 via 2000:a::1
#route -A inet6 add ::/0 gw 2000:a::1

#Show configurations
ip -6 route show
route -A inet6 -n

#test configurations

echo "###############Ping to Next hop"
ping6 -c 2 2000:a::1 #Next hop

echo "###############Ping to foreign network"
ping6 -c 2 2000:c::2 #Foreign network

#(Des)Activate router advertisements
#radvd stop
radvd start

#
mip6d -c /usr/local/etc/mip6d.conf
#mip6d start
```

Ficheiro de configuração do mip6d no HA.

```
# This is an example of mip6d Home Agent configuration file

#Common Options
#####################################################################

#Set the mode witch the daemon will run
NodeConfig HA; #

#DebugLevel 10;
```

```
## Support route optimization with other MNs
DoRouteOptimizationCN enabled; #Default enabled


#Options to Home Agent e Mobile Node
#################################################################

#Specifies the interface and options. If no options "Interface "eth0""
Interface "eth1";

#
UseMnHaIPsec disabled;


#Home Agent Specific Options
#################################################################
#################################################################
```

Ficheiro de configuração do radvd no HA.

```
interface eth1
{
      #envia RAs periodicamente
      AdvSendAdvert on;
      MaxRtrAdvInterval 1.5;
      MinRtrAdvInterval 0.05;

      #AdvDefaultLifetime 3 * MaxRtrAdvInterval = 9
      AdvHomeAgentFlag on;
      AdvHomeAgentInfo on;
      HomeAgentLifetime 10000;#AdvDefaultLifetime = 9
      HomeAgentPreference 20;#default 0
      AdvIntervalOpt on;
#
      prefix 2000:a::/64
      {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr on;
            #AdvPreferredLifetime 500;
            #AdvValidLifetime 600;
      };

};
```

Script de configuração dos endereços nas interfaces do R1

```
#!/bin/bash

clear
/etc/init.d/network restart

#Interface eth0 - Aironet wireless PC480
ip link set dev eth0 down
ip link set dev eth0 up
ip -6 addr add 2000:a::1/64 dev eth0

iwconfig eth0 mode ad-hoc essid homenet enc off

#Interface eth1 - Realtek
ip link set dev eth1 down
```

```
ip link set dev eth1 up
ip -6 addr add 2000:b::1/64 dev eth1

#Interface eth2 - 3COM
ip link set dev eth2 down

#Interface eth3 - Intel (used for internet, not for the scenario)
/sbin/ifconfig eth3 down
ip link set dev eth3 down

#Show configurations
ifconfig
```

Script de configuração das rotas e MIPv6 do R1

```
#!/bin/bash

#Routes
ip -6 route flush
ip -6 route add 2000:a::/64 via 2000:a::1
ip -6 route add ::/0 via 2000:b::2

#Used for MIPv6 scenario
echo "1" > /proc/sys/net/ipv6/conf/eth1/forwarding
echo "0" > /proc/sys/net/ipv6/conf/eth1/autoconf
echo "0" > /proc/sys/net/ipv6/conf/eth1/accept_ra
echo "0" > /proc/sys/net/ipv6/conf/eth1/accept_redirects

/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0

#Show configurations
ifconfig
ip -6 route show
route -A inet6 -n

#Test configurations
echo "##########Ping to Next hop"
ping6 -c 2 2000:b::2 #Next hop

echo "##########Ping to Foreign network"
ping6 -c 2 2000:c::2 #Foreign net
```

Script de configuração dos endereços nas interfaces do R2

```
#!/bin/bash

#CN Configuration

clear
/etc/init.d/network restart

#interface eth0 - wireless
/sbin/ifconfig eth0 down
/sbin/ifconfig eth0 up
/sbin/ip -6 addr add 2000:c::2/64 dev eth0
```

```
iwconfig eth0 mode ad-hoc essid visitnet enc off

#interface eth1 - intel
/sbin/ifconfig eth1 down
/sbin/ifconfig eth1 up
/sbin/ip -6 addr add 2000:b::2/64 dev eth1

#Show configurations
ifconfig
```

Script de configuração das rotas e MIPv6 do R2

```
#!/bin/bash
#R2 Configuration

clear

#Activate IPForwarding
/sbin/sysctl -w net.ipv6.conf.all.forwarding=1
/sbin/sysctl -w net.ipv6.conf.all.autoconf=0
/sbin/sysctl -w net.ipv6.conf.all.accept_ra=0
/sbin/sysctl -w net.ipv6.conf.all.accept_redirects=0


#
echo "1" > /proc/sys/net/ipv6/conf/eth1/forwarding
echo "0" > /proc/sys/net/ipv6/conf/eth1/autoconf
echo "0" > /proc/sys/net/ipv6/conf/eth1/accept_ra
echo "0" > /proc/sys/net/ipv6/conf/eth1/accept_redirects

#Routes
ip -6 route flush all
ip -6 route add 2000:c::/64 via 2000:c::2
ip -6 route add ::/0 via 2000:b::1


#Show configurations
#ip -6 route show
route -A inet6 -n

#test configurations

echo "###############Ping to Next hop"
ping6 -c 2 2000:b::2 #Next hop

echo "###############Ping to foreign network"
ping6 -c 2 2000:a::10 #Foreign network

#
radvd start

#mip6d -c /usr/local/etc/mip6d.conf
#mip6d restart
#mip6d stop
```

Ficheiro de configuração do radvd no R2.

```
interface eth0
{
      AdvSendAdvert on;
```

```
      MinRtrAdvInterval 3;

      MaxRtrAdvInterval 4;

#
# Disable Mobile IPv6 support
#
      AdvHomeAgentFlag off;

#
# example of a standard prefix
#
      prefix 2000:c::/64
      {
            AdvOnLink on;
            AdvAutonomous on;
            AdvRouterAddr off;
      };

};
```

Comandos para o roaming do MN

```
#mudar para a rede visitada
iwconfig eth0 mode ad-hoc essid visitnet enc off
iwconfig eth0 essid visitnet

#mudar para a rede origem
iwconfig eth0 mode ad-hoc essid homenet enc off
iwconfig eth0 essid homenet
```

Comandos para configurar os APs

```
ap>
ap>enable
Password: Cisco
ap#
ap#conf t
ap(config)#interface dot11Radio 0
ap(config-if)#ssid homenet
ap(config-if-ssid)#authentication open
ap(config-if-ssid)#exit
```

E.4 Cenário 4 – testes com a FCCN

Configuração do MN

A configuração do MN é semelhante à apresentada no cenário 1.

Acesso ao router da FCCN

```
telnet 2001:690:1fff:aaaa::1
```

Configuração do router da FCCN

```
############################
gt32
############################


enable
conf t
hostname gt32_virtual


ipv6 unicast-routing


interface FastEthernet0/0
 ipv6 enable
 no shutdown
 ipv6 address 2001:690:1fff:aaaa::1/64
 ipv6 mobile home-agent
 no ipv6 nd suppress-ra
 ipv6 nd ra-interval 3

exit
exit
```

Configuração do router da r2

```
############################
r2
############################

enable
conf t
hostname r2


ipv6 unicast-routing


interface FastEthernet0/0
 ipv6 address 2001:690:2060:FF02::1/64
 ipv6 enable
 no shut
 #ipv6 mobile home-agent
 no ipv6 nd suppress-ra
 ipv6 nd ra-interval 3



interface Serial0/0
 ipv6 address 2001:690:2060:FF04::2/64
 ipv6 enable
 clock rate 56000
 no shut

exit

ipv6 route ::/0 2001:690:2060:ff04::1
```

```
copy run start
#
```

Configuração do router da r1

```
############################
r1
############################

enable
conf t
hostname r1


ipv6 unicast-routing


interface FastEthernet0/0
 ipv6 address 2001:690:2060:FF01::1/64
 ipv6 enable
 no shut
 #ipv6 mobile home-agent
 no ipv6 nd suppress-ra
 ipv6 nd ra-interval 3



interface Serial0/0
 ipv6 address 2001:690:2060:FF03::2/64
 ipv6 enable
 clock rate 56000
 no shut


ipv6 route ::/0 20001:690:2060:ff03::1

copy run start

#
```

Configuração do router da r1

```
############################
mipv6
############################


enable
conf t
hostname mipv6


ipv6 unicast-routing



interface FastEthernet0/0
 ipv6 address 2001:690:2060:2::F1/64
 ipv6 enable
```

```
 no shut



interface Serial0/0
 ipv6 address 2001:690:2060:FF03::1/64
 clock rate 56000
 ipv6 enable
 no shut



interface Serial0/1
 ipv6 address 2001:690:2060:FF04::1/64
 ipv6 enable
 clock rate 56000
 no shut



ipv6 route 2001:690:2060:FF01::/64 2001:690:2060:FF03::2
ipv6 route 2001:690:2060:FF02::/64 2001:690:2060:FF04::2
ipv6 route ::/0 2001:690:2060:2::1

copy run start
```

E.5 Cenário 5 – Testes de MIPv6 na rede e-U

Show version do Switch L3 da rede do IPL

```
sh version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I5Q3L2-M), Version 12.1(20)EA1, RELEASE
SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 04-Feb-04 23:28 by yenanh
Image text-base: 0x00003000, data-base: 0x00827298

ROM: Bootstrap program is C3550 boot loader

SW_3550_S041_B04 uptime is 6 weeks, 2 days, 22 hours, 10 minutes
System returned to ROM by power-on
System image file is "flash:c3550-i5q3l2-mz.121-20.EA1.bin"

cisco WS-C3550-12G (PowerPC) processor (revision A0) with 65526K/8192K
bytes of memory.
Processor board ID FAA0608T03X
Last reset from warm-reset
Bridging software.
Running Layer2/3 Switching Image

Ethernet-controller 1 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 2 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 3 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 4 has 1 Gigabit Ethernet/IEEE 802.3 interface
```

```
Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 7 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 8 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 9 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 10 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 11 has 1 Gigabit Ethernet/IEEE 802.3 interface

Ethernet-controller 12 has 1 Gigabit Ethernet/IEEE 802.3 interface

12 Gigabit Ethernet/IEEE 802.3 interface(s)

The password-recovery mechanism is enabled.
384K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:05:31:3C:58:00
Motherboard assembly number: 73-5526-04
Power supply part number: 34-0967-01
Motherboard serial number: FAA06081EIM
Power supply serial number: LIT0603016A
Model revision number: A0
Model number: WS-C3550-12G
System serial number: FAA0608T03X
Configuration register is 0x10F

SW_3550_S041_B04#
```

Show version do router Cisco 3600 da rede da ESTG

```
Cisco Internetwork Operating System Software

IOS (tm) 3600 Software (C3660-IS-M), Version 12.2(2)T,  RELEASE SOFTWARE
(fc1)

TAC Support: http://www.cisco.com/cgi-bin/ibld/view.pl?i=support

Copyright (c) 1986-2001 by cisco Systems, Inc.

Compiled Sat 02-Jun-01 12:12 by ccai

Image text-base: 0x600089C0, data-base: 0x61360000



ROM: System Bootstrap, Version 12.0(6r)T, RELEASE SOFTWARE (fc1)

ROM: 3600 Software (C3660-IS-M), Version 12.2(2)T,  RELEASE SOFTWARE (fc1)



Riplei uptime is 2 weeks, 4 days, 58 minutes

System returned to ROM by reload at 17:04:44 UTC Thu Dec 29 2005

System restarted at 17:05:32 UTC Thu Dec 29 2005
```

```
System image file is "flash:c3660-is-mz.122-2.T.bin"



cisco 3660 (R527x) processor (revision C0) with 111616K/19456K bytes of
memory.

Processor board ID JAC0544A1RA

R527x CPU at 225Mhz, Implementation 40, Rev 10.0, 2048KB L2 Cache

Channelized E1, Version 1.0.

Bridging software.

X.25 software, Version 3.0.0.

SuperLAT software (copyright 1990 by Meridian Technology Corp).

Primary Rate ISDN software, Version 1.1.




3660 Chassis type: ENTERPRISE

4 Ethernet/IEEE 802.3 interface(s)

3 FastEthernet/IEEE 802.3 interface(s)

4 Serial network interface(s)

2 Channelized E1/PRI port(s)

DRAM configuration is 64 bits wide with parity disabled.

125K bytes of non-volatile configuration memory.

16384K bytes of processor board System flash (Read/Write)
```

Show version dos APs do IPL e da ESTG

```
AP3.006-P0-A2.193#sh version
Cisco Internetwork Operating System Software
IOS (tm) C1100 Software (C1100-K9W7-M), Version 12.2(15)XR2, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Fri 17-Sep-04 13:29 by kellythw
Image text-base: 0x00003000, data-base: 0x005E8494

ROM: Bootstrap program is C1100 boot loader
BOOTLDR: C1100 Boot Loader (C1100-BOOT-M) Version 12.2(8)JA, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)

AP3.006-P0-A2.193 uptime is 5 weeks, 2 days, 23 hours, 36 minutes
System returned to ROM by power-on
System restarted at 12:28:25 UTC Tue Nov 15 2005
System image file is "flash:/c1100-k9w7-mx.122-15.XR2/c1100-k9w7-mx.122-
15.XR2"
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found
at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco AIR-AP1121G-E-K9     (PowerPCElvis) processor (revision A0) with
14326K/2048K bytes of memory.
Processor board ID FOC08280TEK
PowerPCElvis CPU at 197Mhz, revision number 0x0950
Last reset from power-on
Bridging software.
1 FastEthernet/IEEE 802.3 interface(s)
1 802.11 Radio(s)

32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: 00:11:92:9D:BA:3A
Part Number                          : 73-7886-07
PCA Assembly Number                  : 800-21481-07
PCA Revision Number                  : A0
PCB Serial Number                    : FOC08280TEK
Top Assembly Part Number             : 800-22053-04
Top Assembly Serial Number           : FHK0830V1C5
Top Revision Number                  : A0
Product/Model Number                 : AIR-AP1121G-E-K9

Configuration register is 0xF

AP3.006-P0-A2.193#
```

Outras configurações

Os ficheiros com o resultado do show run dos Routers, Switchs e APs, bem como os ficheiros com as configurações a realizar na rede não são aqui publicados por motivos de segurança, uma vez que estará acessível via web.

F - Artigo

Este anexo apresenta o artigo submetido à Conferência Ibérica de Sistemas e Tecnologias de Informação (CISTI - http://www.est.ipca.pt/cisti/) a realizar de 21 a 23 de Junho de 2006 em Esposende, Portugal.

IPv6@ESTG-Leiria

www.ipv6.estg.ipleiria.pt