Estudo do IPv6 móvel em Linux

Tiago Sousa, Edmundo Monteiro, Fernando Boavida

tsousa@student.dei.uc.pt, {boavida, edmundo}@dei.uc.pt

Laboratório de Comunicações e Telemática

CISUC/DEI – Universidade de Coimbra

Pólo II, Pinhal de Marrocos, 3030-290 Coimbra

http://lct.dei.uc.pt

Resumo

Nos dias de hoje, o conceito de mobilidade é cada vez mais pertinente, devido, em grande parte, ao aumento do número de portáteis e de PDA's, sendo por isso de antever um uso massificado desta tecnologia dentro em breve.

Neste artigo serão discutidos os aspectos mais relevantes da mobilidade em IPv6 e será descrita uma a implementação e configuração de uma *Testbed* de uma rede experimental *wireless* implementada sob o protocolo IPv6 .

Palavras Chave

Mobilidade, IPv6, *Roaming*, *Handover*

1- Introdução

Existem três formas distintas de mobilidade na Internet: dispositivos portáteis, que são transportados e ligados em diferentes pontos de rede e em redes diferentes; computadores móveis que permanecem ligados durante os seus movimentos; e redes móveis.

A maneira mais simples de oferecer mobilidade consiste em utilizar protocolos que permitam ao computador móvel obter um endereço temporário, que descreva a sua localização numa rede remota. O facto dos endereços serem temporários implica que a ligação não poderá ser mantida quando o mesmo computador mudar de ponto de ligação à rede, sendo a mobilidade oferecida bastante restringida. Neste tipo de configurações a segurança também é posta em causa, uma vez que existe pouca diferença entre um computador local e um que use uma configuração dinâmica nessa rede.

Este tipo de abordagem da mobilidade não deixa de ser estática, isto é, ainda não se torna possível a um computador transitar entre diferentes redes sem que perca as suas ligações.

A vertente *wireless* da mobilidade desempenha aqui um papel importante, uma vez que possibilita a mobilidade no sentido mais lato da palavra.

Daqui advém um conceito importante na mobilidade, o conceito de **célula**, que não é mais que uma área limitada onde é partilhada a mesma frequência de rádio, emitida pelos *Acess Points* pertencentes á rede daquela célula. Em cada célula existirá um

computador ligado à Internet e capaz de conduzir os pacotes IP entre o canal de rádio e a Internet.

A transição de célula para célula é designada de ***roaming*** e o objectivo principal da tecnologia IP móvel é que essa transição se possa fazer sem que o computador móvel perca as suas ligações, i.e., será mantido o endereço IP do computador independentemente da sua localização, de maneira a que as suas ligações TCP, que são identificadas por um par endereço-porta, possam ser mantidas.

O objectivo deste artigo é estudar a mobilidade em IPv6. Será feita uma abordagem teórica aos principais conceitos que suportam a mobilidade em IPv6 a que se seguirá a descrição do ambiente de testes desenvolvido e os testes de *benchmarking* aplicados com vista a determinar o *handover*, e outras características relevantes, da rede.

2- Mobilidade em IPv6

Os efeitos das limitações do número de endereços disponibilizados pelo IPv4, foram atenuados, durante algum tempo, pelos NAT (Network Address Translation) e por *gateways* de aplicação entre as intranets e a Internet. Esta solução introduz algumas barreiras, por exemplo não permite peer-to-peer, invalida os protocolos que assentem em endereços globais e únicos (ex. IPSec) e consequentemente não resolve o nosso problema da limitação da gama de endereços. Talvez este tenha sido o primeiro factor a levar ao desenvolvimento de uma evolução do IPv4, o IPv6, apesar de não ser a evolução mais importante.

2.1- Protocolo IPv6

O protocolo IPv6 eliminou a restrição do número de endereços, bem como introduziu alguns melhoramentos dos quais se destacam: endereços hierárquicos – fáceis de encaminhar; capacidades de segurança embutidas no próprio protocolo (IPSec); Plug-n-Play – configuração automática dos endereços (Stateless, Stateful, Parameter discovery); possibilidade de Multicast, Anycast e QoS. Como era de prever a estrutura de um pacote IPv6 é bastante diferente. A figura abaixo ilustra a estrutura de um pacote IPv6.

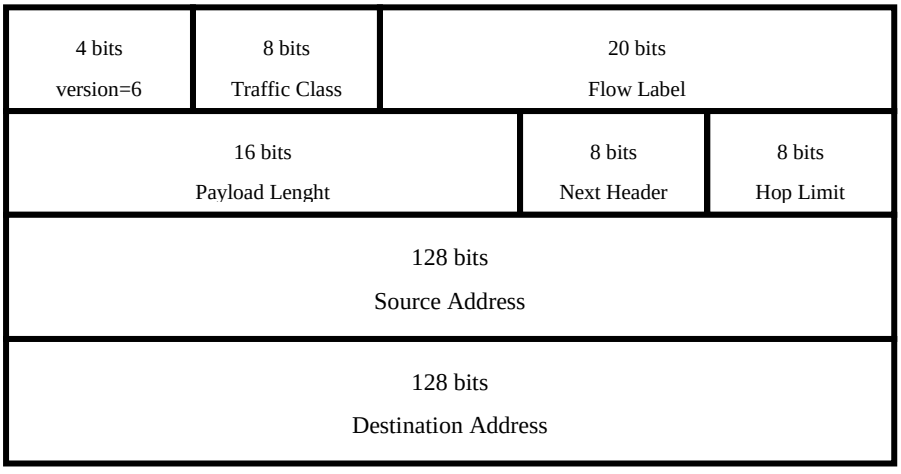


Fig.1 – Pacote IPv6

Podemos detectar as seguintes modificações em relação a um pacote IPv4:

- O cabeçalho IP passou a ser de tamanho fixo. Os campos opcionais são *daysy-chained*.

- Espaço de endereçamento passou para 16 bytes.

- Checksum eliminado

- Alguns campos mudaram de nome: - Time to live -> Hop Limit; - Protocol -> Next Header; - Type of Service -> Traffic Class

Os vários tipos de extensão, existentes no protocolo IPv6, têm como objectivo mover os campos de comprimento variável presentes nas *header* dos pacotes IPv4, para o próprio pacote IPv6. Desta maneira o tamanho de uma *header* de um pacote IPv6 é totalmente previsível e podem ser adicionadas novas extensões facilmente. Cada extensão é identificada pelo campo *Next Header*. Cada pacote IPv6 pode ter zero, uma ou mais extensões. A figura seguinte mostra 3 tipos de extensões existentes, as restantes estão relacionadas com a segurança, nomeadamente com o protocolo *IPSec*.

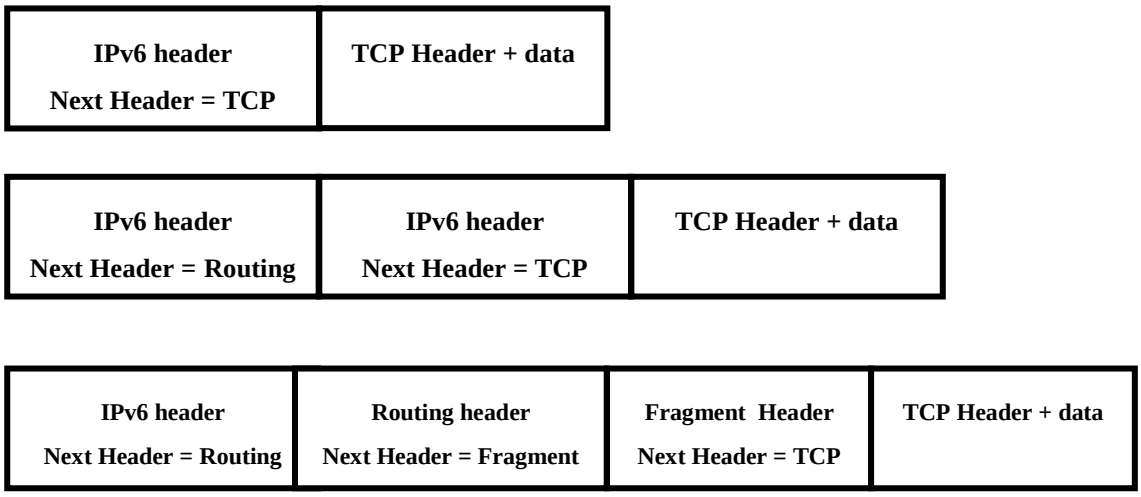


Fig. 2 – Extensões ao cabeçalho dos pacotes IPv6

Vão ser estas extensões ao cabeçalho do pacote IPv6 que vão possibilitar a mobilidade, na medida em que vão transportar vários tipos de informação que permitirá aos nós em causa, principalmente ao nó móvel, comunicar a sua posição.

2.2 - IPv6 Móvel

Como já foi dito, a principal dificuldade em oferecer mobilidade é o facto de ter que manter as ligações activas de um nó enquanto este se move, isto é, muda de pontos de ligação à rede. O problema advém dos mecanismos/protocolos de *routing* que são usados actualmente e que partem do princípio que todos os nós têm sempre o mesmo ponto de ligação à rede. Adicionalmente o endereço IP de cada nó identifica a "linha" onde se está ligado, o que faz com que uma mudança de ponto de ligação à rede implique a obtenção e consequente reconfiguração do novo endereço IP obtido. De modo a suportar a mobilidade foi desenvolvido um protocolo chamado IP móvel. Existem 2 variações, o IPv4 móvel, que foi visto atrás e o IPv6 que trataremos agora.

No IPv6 cada nó é identificado pelo seu endereço estático, na sua rede local, em vez de o ser pelo seu ponto de ligação à rede. De cada vez que o nó está fora da sua rede local envia a sua nova "localização" ao seu agente local, presente na sua rede local, fazendo com que este conheça a sua posição em todos os momentos. O agente local, por sua vez, intercepta os pacotes endereçados ao nó móvel e envia-lhos, via *tunneling*. Este é o mecanismo básico de comunicação da tecnologia IP móvel baseada no protocolo IPv6. Para suportar e possibilitar esta solução, a tecnologia IPv6 móvel cria um COA de cada vez que o nó muda de ponto de ligação. Este COA pode ser obtido através da recepção de *router advertisements* (stateless address auto-configuration) ou pode ser obtido via servidor DHCP (stateful address auto-configuration).

2.2.1- Processo de Discovery

Assumindo que cada nó móvel não sabe o endereço IP do seu agente local, a tecnologia IPv6 móvel fornece um mecanismo que permite a este "descobrir" dinamicamente o endereço do seu HA, através do qual pode registar o seu COA enquanto estiver numa rede remota.

O processo de obtenção é o que se descreve: o nó móvel envia um *Binding Update* para o endereço *unicast* do seu agente local. Este descarta o pacote e devolve uma resposta (Binding Acknowledgement) com uma lista de todos os possíveis *routers* que se podem comportar como agentes locais do nó móvel. Esta lista é mantida por todos os agentes locais e actualizada devido aos *advertisements* feitos periódicamente. Desta maneira o nó móvel consegue obter periodicamente o endereço do agente local que mais lhe convém.

Através dos *router advertisements*, referidos atrás, cada nó móvel consegue extrair o prefixo do endereço do ponto da rede remota onde se liga. Este nó conseguirá, devido aos mecanismos de auto-configuração de endereços do IPv6, obter um endereço nessa rede, o COA. Este facto faz com que não seja necessária a presença de um agente na rede remota que forneça o mesmo COA para todos os nós que cobre.

Podemos, então, concluir que os mecanismos de *neighbor discovery* do IPv6 permitem que um nó móvel descubra qual o seu agente local e que consiga extrair, para si, um endereço, o COA, na rede onde se encontra. O passo seguinte será registar o COA obtido junto do seu agente local.

2.2.2- Processo de Binding

O registo do COA por parte de um nó móvel, é feito no IPv6 recorrendo a um campo opcional do cabeçalho dos pacotes IPv6, a opção *Destination*, que transporta informação adicional que será examinada unicamente pelo nó destino. Foram definidas 4 opções novas, correspondentes a 4 tipos de acções possíveis de registo: Binding Update, Binding Acknowledgement, Binding Request e o Home Address.

> **Binding Update –** Esta opção é usada pelo nó móvel para informar o seu agente local ou o nó correspondente acerca do seu novo COA. Cada pacote que inclua esta opção deve incluir igualmente uma *header* AH ou ESP.
>
> **Binding Acknowledgement –** Esta opção é usada para confirmar a recepção de um Binding Update por parte do agente local. Cada pacote que inclua esta opção deve incluir igualmente uma *header* AH ou ESP.

Binding Request – Esta opção é usada por qualquer nó para pedir que outro nó lhe envie um Binding Update com o seu COA actual.

Home Address – Esta opção é usada num pacote enviado por um MN para informar o receptor do pacote acerca do *home address* do próprio MN.

Existem, principalmente, 3 estruturas conceptuais que suportam a acção de registo:

Binding cache – Todos os nós IPv6 tem uma cache que aloja os *Bindings* de outros nós. Veremos como funciona na secção da optimização do routing.

Binding Update List – Esta lista também está presente em todos os nós IPv6 e armazena informação acerca dos *Binding Updates* enviados pelo próprio nó e cujo período de vida ainda não tenha expirado.

Home Agents List - Esta lista está presente em todos os routers que servem como agente local e contém informação sobre todos os HA´s presentes numa dada rede. Esta informação é recolhida através dos *router advertisements* que são enviados por todos os agentes locais.

2.3- Processo de comunicação entre um nó correspondente e um nó móvel

- O nó correspondente envia um pacote para o *home address* do nó móvel.

- O agente local usando os mecanismos de *neighbor discovery*, intercepta o pacote, reescreve o cabeçalho inserindo uma *routing header* que redirecciona o pacote para o COA do nó móvel.

- O nó móvel recebe o pacote através do seu COA, processa-o e envia a resposta.

- No *source address* do pacote resposta é posto o COA do nó móvel. O *home address* é inserido como opção destino. Se houver uma associação de segurança disponível (entre os dois extremos), o nó móvel insere uma AH ou ESP e insere igualmente a opção de *Binding Update*. O pacote é enviado ao nó correspondente.

- O nó correspondente ao receber a resposta usa o campo de *home address* do pacote recebido e verifica que este provém do nó móvel. Usando a opção de *Binding Update* do pacote recebido, valida o COA do nó móvel e o próximo pacote que lhe é enviado conterá uma *routing header* que especificará o *routing* através do COA, incluirá uma *header* AH ou ESP e finalmente incluirá um *Binding Acknowledgement*.

Cada agente local intercepta todos os pacotes dirigidos ao nó móvel. Para isso é usado o mecanismo de *Neighbor Discovery***.** Se o nó móvel pretender enviar um pacote para outro nó qualquer, fá-lo-á directamente para o destino. O nó móvel colocará COA no campo *source address* e inclui na opção destino o seu *home address*. Devido ao carácter estático do *home address* (em contraste com o COA), permite que o nó correspondente use com transparência este endereço em camadas superiores.

Se o nó móvel comunicar com o nó correspondente enquanto estiver fora da sua rede local, os pacotes são encaminhados do nó correspondente para o agente local, e deste para o nó móvel que responderá, novamente, para o nó correspondente. Este tipo de situação chama-se *routing* triângular. Para evitar o routing triângular, cada nó móvel

pode enviar *Binding Updates* para todos os nós correspondentes. Isto permite a estes colocarem na sua cache o COA do nó móvel e enviar-lhe os pacotes directamente.

Qualquer nó IPv6 antes de iniciar a comunicação, com o envio do primeiro pacote, verifica a sua *Binding Cache* à procura de uma entrada com o endereço destino pretendido. Se essa entrada existir, o pacote será enviado para o nó respectivo usando uma *routing header*, em vez da encapsulação. O caminho especificado pela *routing header* tem duas "fases", a primeira é o COA e a segunda é o *home address* do nó móvel. Isto resulta no envio do pacote directamente para o COA do nó móvel. Este recebe o pacote e redirecciona-o para a próxima "fase" especificada pela *routing header*, como esta é composta pelo *home address* do nó móvel, o pacote já não sai deste nó.

Se a *Binding Cache* não tiver nenhuma entrada o pacote é enviado directamente.

3- Ambiente experimental

O ambiente de testes descrito a seguir foi desenvolvido para testar a mobilidade em IPv6 e para medir algumas características da rede quando nó móvel comunica com o nó correspondente, por exemplo, as perdas e atrasos na entrega dos pacotes. Nesta comunicação o nó móvel transitará entre duas redes distintas, por forma a existir *handover*. As características do *handover* existente também serão estudadas.

3.1- Ambiente de testes

A arquitectura da rede implementada é mostrada na figura seguinte.

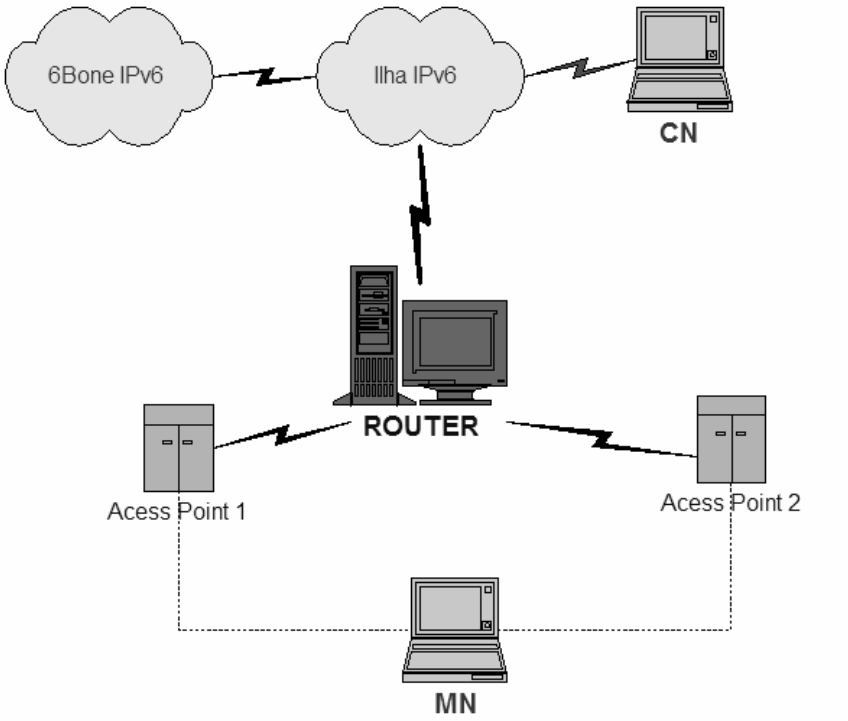


Fig. 4 – Rede de teste

Pode-se ver que ela é constituída por um portátil, que serve de nó móvel (MN), e que transita entre os dois AP's existentes, pertencentes a redes com *ESSID's* diferentes, para possibilitar o estudo do *handover*. Estes estão ligados a duas interfaces diferentes no Router, que tem 3 , estando a outra ligada á ilha IPv6 existente no LCT.

Todos os testes serão efectuados tendo como base a comunicação entre o nó móvel e o nó correspondente.

É de realçar que os AP's utilizados utilizam a frequência dos 2.4 GHZ e permitem taxas de transmissão de 11Mbps. A tecnologia wireless que serve de suporte é a 802.11b.

Hardware e Software utilizado

O principal hardware utilizado na rede é mostrado na tabela abaixo.

HARDWARE	**CARACTERÍSTICAS**
Portátil (MN)	Pentium IV 2.4 GHz, 512 Mb RAM
AP_1	3Com AirConnect -11 Mbps
AP_2	Cisco Aironet – Serie 1100 – 11Mbps
Router	Pentium Celerom 1.7 Ghz, 512 Mhz
Placa wireless	3Com AirConnect 11Mbps – Modelo**:** 3CRWE737A-E1
CN	Pentium MMX 266 MHz, 98 Mb RAM

Tabela 1- Principal hardware utilizado na rede de testes

Quanto ao software utilizado destaca-se o sistema operativo Linux, distribuição Mandrake 9.0, que utiliza a versão do kernel 2.4.19. Este sistema operativo serve de suporte nos três nós principais da rede. Será feito um upgrade para o kernel 2.4.20 para estar de acordo com a versão mais recente do MIPL.

Será implementado o MIPL6 versão 0.9.5.1-v2.4.20.

Para utilizar e configurar a placa PCMCIA no nó móvel foi instalado o pacote pcmcia-cs-3.1.3.

No caso do router foi instalado o *daemon* radvd-0.7.2, que tem como objectivo enviar *router advertisements* para as duas redes cobertas pelos dois *Acess Points*, de modo a que o nó móvel quando se encontrar numa dessas redes possa auto-configurar a parte dinâmica do seu endereço de acordo com o prefixo enviado nesses *advertisements*.

3.2- Configuração

Em termos de configuração, tanto no router como no nó móvel foram feitos upgrades ao kernel original do Mandrake 9.0, o 2.4.19, para a versão mais recente, a 2.4.20. Antes de ser feito o upgrade ao kernel, foi instalado o suporte IPv6, quer no Router, quer no nó móvel.

Como já foi dito é necessário efectuar o upgrade do kernel para a versão 2.4.20, para ser compatível como a versão mais recente do MIPv6. Este *upgrade* tem de obedecer ás especificidades requeridas pelo cenário em questão, i.e., a escolha dos módulos a instalar terá de integrar, fundamentalmente, as opções relacionadas com o protocolo IPv6 e com o MIPv6. As opções escolhidas para o nó móvel e para o router são muito semelhantes, sendo a diferença o facto de um actuar como HA e outro como MN.

Depois de configurados, quer a nova versão do kernel quer o suporte para o MIPv6, os próximos passos são a configuração das placas de rede do router, os seus endereços IPv6, configurar o endereço do MN, instalar e configurar os dois AP's disponíveis e instalar e configurar os módulos PCMCIA no MN.

3.3- Configuração do endereçamento IPv6

A atribuição dos endereços IPv6 ás 3 placas do *router*, uma que liga á ilha IPv6 do LCT, a interface externa da rede, e as restantes duas que ligam aos dois AP's, é feita herdando parte dos endereços atribuídos ao DEI e á ilha IPv6 do LCT, respectivamente. Assim, a figura seguinte mostra os endereços dos nós mais importantes.

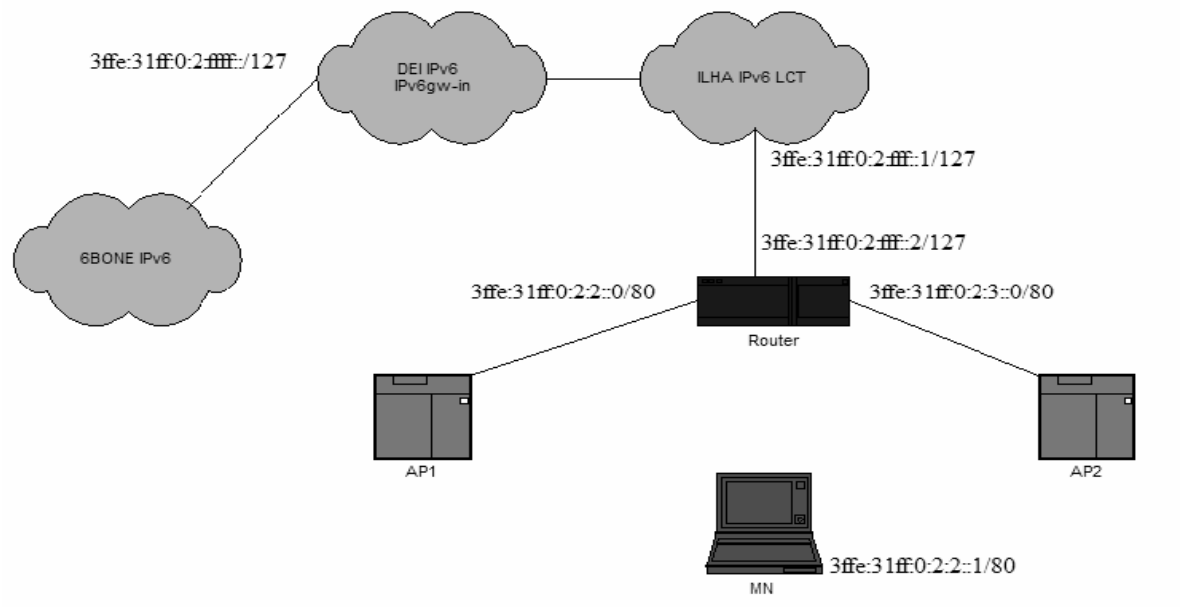


Fig.5 – Endereçamento IPv6 dos principais nós da rede

3.4 – Outras etapas da configuração da mobilidade

Existem duas etapas fundamentais na configuração da mobilidade, a instalação e configuração do *daemon* radvd no router e a configuração do MIPv6 quer no router quer no portátil. A primeira é feita através do ficheiro de configuração radvd.conf, no qual se

deve incluir os prefixos das *interfaces* para onde se pretender enviar os *advertisements*. A segunda etapa consiste em configurar, quer no agente local quer no nó móvel, o mipv6 através do seu ficheiro de configuração, */etc/sysconfig/network-mip6.conf*. Aqui explicita-se o papel de cada nó, agente local ou nó móvel.

Depois da configuração no Router, do MIPv6 e do radvd e no nó móvel, do MIPv6, basta executar os *daemons* respectivos para que a rede esteja apta a suportar a mobilidade.

4- Experimentação

Como foi dito anteriormente, os testes aqui efectuados têm por objectivo medir características da rede tais como as perdas e os atrasos na entrega de pacotes e o *handover* existente na aquisição de um novo endereço, *handover* ao nível da camada 3 da OSI.

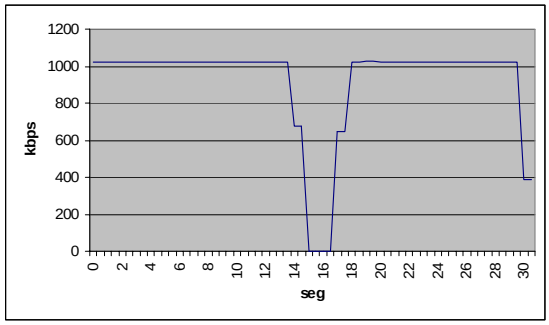
As ferramentas usadas para medir tais características foram, principalmente, o MGEN e o *trpr*. Com a primeira ferramenta é possível gerar tráfego para portas especificas e monitorizar o tráfego que se recebeu em portas específicas. Possibilita, igualmente, elaborar *logs*, quer daquilo que se enviou quer do que se recebeu. O *trpr* permite, a partir dos ficheiros gerados pelo MGEN, extrair características como a taxa de transmissão, as perdas de pacotes e a latência, entre outras, existentes no fluxo de dados correspondente.

Os testes efectuados consistirão em gerar tráfego a diferentes débitos, provocar uma situação de *handover* no nó móvel e medir as características da rede mediante os diversos cenários. O fluxo de dados é enviado do nó móvel para o nó correspondente.

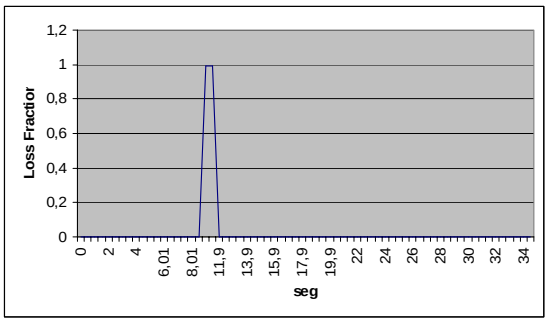
Os gráficos mostrados a seguir reproduzem os resultados obtidos.

Handover a 512 kbps

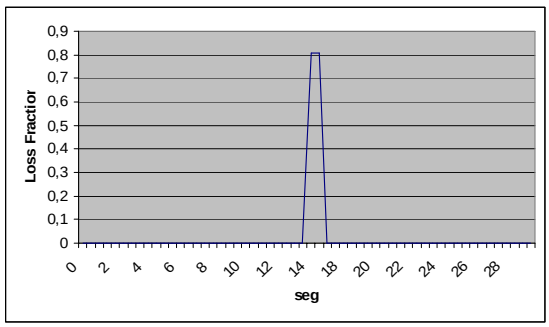
Handover a 1 Mbps



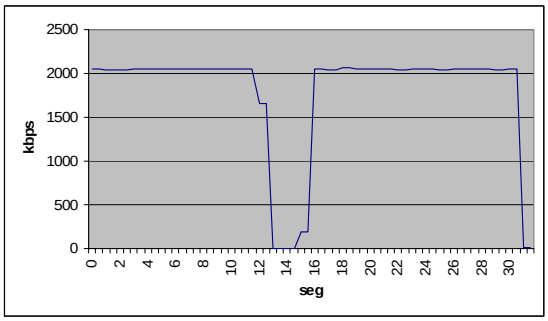
% da perca de pacotes a 512 kbps



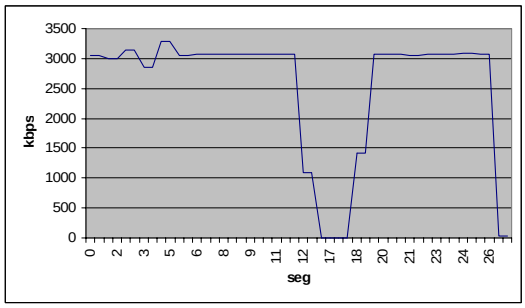
% da perca de pacotes a 1 Mbps



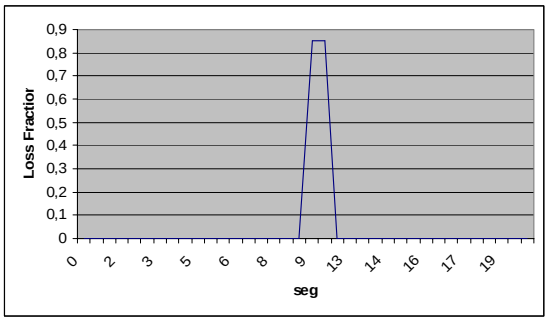
Handover a 2 Mbps



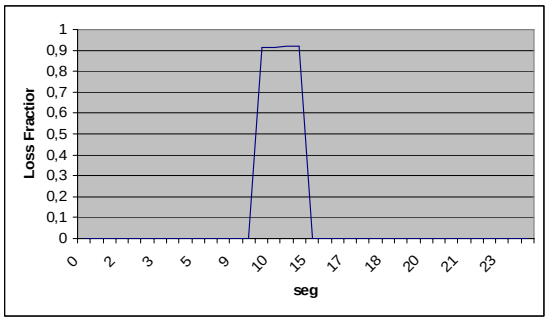
Handover a 3 Mbps



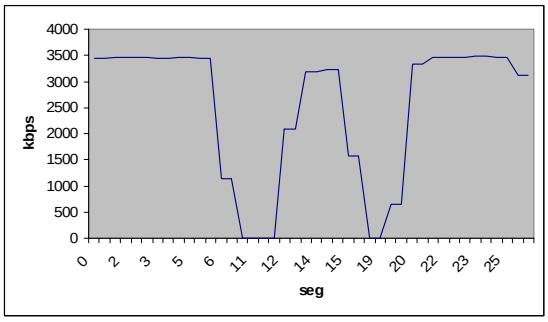
% da perca de pacotes a 2 Mbps



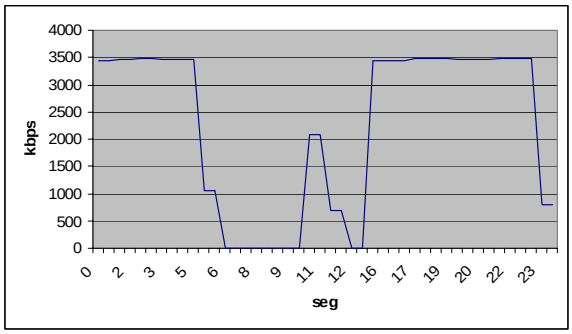
% da perca de pacotes a 3 Mbps



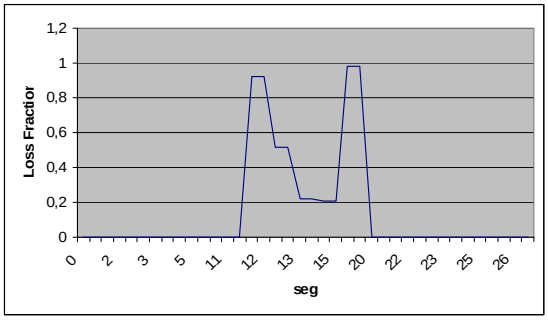
2 handover a 4 Mbps



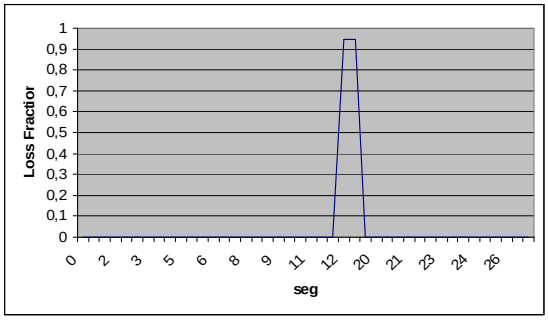
2 handover a 6 Mbps



% da perca de pacotes a 4 Mbps com 2 handover



% da perca de pacotes a 6 Mbps com 1 handover



A partir da análise dos gráficos anteriores podem-se retirar várias conclusões, entre as quais se destacam, o débito máximo suportado pela rede (Troughput) ronda os 3.5 Mbps, não existe *handover* que não envolva a perca de pacotes, e regra geral pelo que pudemos experimentar cada *handover* tem uma duração de aproximadamente 3 segundos.

5- Conclusão e trabalho futuro

Podemos concluir, que apesar dos melhoramentos introduzidos pelo protocolo IPv6, no que se refere á mobilidade, ainda existem algumas questões que precisam de refinamentos, de entre as quais se destacam os problemas de *handover* e de *routing*. Por esta razão os trabalhos a serem desenvolvidos no futuro centrar-se-ão nestas duas áreas. Existem várias formas de melhorar quer o *handover* quer o *routing*, uma delas é a hierarquização da rede. Esta pode ser umas das próximas etapas. No estado de desenvolvimento em que se encontra a tecnologia IP móvel, sobretudo a sua vertente IPv6, podemos considerar pertinente efectuar uma comparação entre as várias implementações existentes na Europa e a desenvolvida no nosso laboratório.

6- Bibliografia

Gast, M., (2002, April). 802.11 Wireless Networks: The Definitive Guide. Available at:

http://www.oreilly.com/catalog/802dot11/chapter/ch15.html#56622.

Bieringer, P. (2002). Linux+IPv6-HOWTO. Available at: http://linux-howto.ipv6.telepac.pt/.

Brabson, R. (2002). Coming to a network near you: IPv6. Available at: www.share.org/proceedings/sh98/data/S3406.PDF.

Kato, T., Takechi, R., Ono, H. (2001). A study on mobile IPv6 based mobility management architecture. Available at: www.gta.ufrj.br/~ascher/artigos/ MIPv6mobilitymanagementarchitecture.pdf.

Fritsche, W., Heissenhuber, F. (2001). Mobility support for the next generation Internet. Available at: www.ipv6forum.com/navbar/papers/ MobileIPv6_Whitepaper.pdf.

Chown, T., Kirstein, P., Edwards, C. (2001). Project Deliverable 7 Report: IPv6 wireless LANs and mobile IPv6. Available at: http://www.ipv6.ac.uk/bermuda2/.

Chaparro, D., Rodríguez, R. (2002). Testbed for MIND project on IPv6. Available at: gsyc.escet.urjc.es/Mobiquo/Mind/documentacion/ MontajeMaquetaIPv6_en/.

Vuopionperä R., (2001). Specification and Architecture of the Network Available IPv6 communications, gateways and components. Available at: www.6winit.org/docs/.

Hedenfalk, M., (2002). Access Control in an Operator Neutral Public Access Network Available at: www.e.kth.se/~e97_mhe/thesis/

Escudero, A., Pehrson, B., Pelletta, E., Vatn, J., Wiatr, P., (2001). Wireless access in the Kista – IP University. Available at: www.it.kth.se/~aep/licentiate/PB-lanman2001.pdf

Bjonnes, L., Bryhni, H., Evang, J.M., Gjessing, S., (1999). Wireless Experimental Metropolitan Area Network Using IPv6 in Norway (WEMAN). Available at: www.computer.org/proceedings/hicss/ 0001/00018/00018031abs.htm

Perkins, C., (1996).RFC 2002. Available at: www.ietf.org/rfc/rfc2002.txt

Perkins, C., (1996).RFC 2003. Available at: www.ietf.org/rfc/rfc2003.txt

Johnson, D., Perkins, C., Arkko, J., (2003). draft-ietf-mobileip-ipv6-20.txt. Available at: http://www.eecs.wsu.edu/~rgriswol/Drafts-RFCs/draft-ietf-mobileip-ipv6-21.txt