Titre: Title:	Gestion de mobilité IP dans un réseau d'accès de nouvelle génération basée sur MPLS
Auteur: Author:	Jihad Hodroj
Date:	2004
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Hodroj, J. (2004). Gestion de mobilité IP dans un réseau d'accès de nouvelle génération basée sur MPLS [Master's thesis, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/7393/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/7393/
Directeurs de recherche: Advisors:	Samuel Pierre
Programme: Program:	Unspecified

UNIVERSITÉ DE MONTRÉAL

GESTION DE MOBILITÉ IP DANS UN RÉSEAU D'ACCÈS DE NOUVELLE GÉNÉRATION BASÉE SUR MPLS

JIHAD HODROJ
DÉPARTEMENT DE GÉNIE INFORMATIQUE
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
Novembre 2004

Your file Votre référence
ISBN: 0-494-01339-7
Our file Notre référence
ISBN: 0-494-01339-7

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

GESTION DE MOBILITÉ IP DANS UN RÉSEAU D'ACCÈS
DE NOUVELLE GÉNÉRATION BASÉE SUR MPLS

présenté par : HODROJ Jihad
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

M. FERNANDEZ José, Ph.D., président
M. PIERRE Samuel, Ph.D., membre et directeur de recherche
M. QUINTERO Alejandro, Doct., membre

DÉDICACE

À ma famille …

REMERCIEMENTS

Tout d'abord, je souhaite remercier mon directeur de recherche, monsieur Samuel Pierre, professeur au département de génie informatique, pour la qualité de son encadrement, ses suggestions, sa patience et son encouragement.

J'adresse ensuite mes sincères remerciements aux membres du LARIM (Laboratoire de Recherche en Réseautique et Informatique Mobile) de l'École Polytechnique de Montréal, pour les échanges constructifs que j'ai eus avec eux tout au cours de la réalisation de cette recherche. En particulier, je remercie Madame Betty Momplaisir pour la relecture des chapitres du mémoire et ses judicieux commentaires.

Finalement, je tiens à exprimer ma profonde gratitude à mes parents et à ma femme pour leur amour, support et encouragement continuel tout au long de ce travail.

RÉSUMÉ

Les réseaux d'accès mobiles de nouvelle génération (3G et plus) évoluent rapidement vers une définition de réseau entièrement IP (tout-IP). Ces réseaux, synonymes de services à valeur ajoutée, doivent offrir l'évolutivité requise pour satisfaire aux exigences du futur trafic IP en terme de nouveaux services multimédias et applications à temps réel, tout en assurant une gestion efficace de la mobilité des usagers. Outre la connectivité globale, les utilisateurs mobiles souhaitent obtenir des garanties de qualité de service (QdS) telles qu'une bande passante assurée au cours de leurs déplacements, un faible taux de pertes, un délai et une gigue minimale, afin de répondre aux exigences qualitatives spécifiques des nouveaux services visés. L'IETF a défini des standards que doit implanter un réseau IP pour supporter les architectures de qualité de service telles que IntServ, DiffServ et MPLS. L'architecture IntServ permet de faire des réservations par flot mais ne garantit pas le passage à l'échelle. Nous avons donc étudié les solutions évolutives pour offrir de la qualité de service dans l'Internet et en avons conclu qu'il était intéressant d'utiliser une architecture DiffServ.

Bien que l'architecture DiffServ offre une différenciation de services tout en ayant une bonne évolutivité, elle est conçue pour une architecture de QdS statique ou faiblement dynamique et, de plus, elle n'est pas adaptée aux environnements fortement mobiles. Ceci devient particulièrement contraignant dans les réseaux d'accès de nouvelle génération qui cherchent à offrir un débit élevé aux utilisateurs. En effet, l'augmentation de débit s'effectue en diminuant la taille des cellules et en montant en fréquences. Or, les handoffs deviennent plus fréquents, ce qui rend le protocole Mobile IP non évolutif du fait qu'un mobile doit signaler tous ses déplacements à son réseau mère. Nous avons donc étudié plusieurs protocoles de micro-mobilité, notamment HMIPv6 qui propose une solution complémentaire à Mobile IP basée sur une architecture hiérarchique, afin de masquer la mobilité au réseau mère lors d'un déplacement géographique réduit.

Cependant, la structure en arbre hiérarchique de ce modèle est statique, et le nœud de haut niveau dans la hiérarchie (appelé MAP) constitue un goulot d'étranglement. Un tel système, n'est évidemment pas très flexible.

D'autre part, plusieurs techniques de relève (*handover*) ont été proposées au sein de l'IETF qui constituent un apport au protocole Mobile IP, notamment le *fast handover* censé réduire le délai de déconnexion du *handover* de bas niveau. Cela nous a amené à proposer un cadre de travail (*framework*) intégrant les mécanismes de gestion de la micro-mobilité, notamment le protocole HMIPv6 combiné avec le mécanisme du *fast handover*, avec le protocole de signalisation RSVP-TE dans un réseau d'accès basé sur MPLS. L'idée principale est de remplacer les mécanismes de tunnelage dans HMIPv6 par des chemins MPLS (LSP). Dans ce contexte, nous proposons le modèle Q-HMIP qui vise à réduire la latence du handover en implémentant la technique du *fast handover*, à augmenter la robustesse et la flexibilité du système en distribuant la tâche assumée par le MAP sur tous les routeurs LSR du domaine, en appliquant le mécanisme de la modification dynamique des chemins LSP fourni par RSVP-TE, et finalement à garantir un service évolutif de la QdS aux usagers en mobilité en profitant de l'approche DiffServ sur MPLS.

ABSTRACT

Next generation mobile networks (3G and beyond) are all evolving towards network architectures relying entirely on IP (All-IP networks). Those networks, synonym of added value services, have to offer the required scalability in order to support future IP traffic, namely new multimedia services and real time applications, while providing an effective mobility management mechanism for mobile users. In addition to a global connectivity, mobile users would like to have quality of service guarantees such as, an assured bandwidth, a low rate of packet loss, a low delay and jitter in order to satisfy the specific qualitative demands of the envisioned services. IETF has defined standards that an IP network must implement to support QoS architectures such as IntServ, DiffServ and MPLS. IntServ architecture allows per flow reservations and has proved to be a non-scalable service.

While DiffServ provides a scalable differentiated service suitable for static/wired networks, it is not adapted for mobile environments. This becomes a serious restriction in next generation radio access networks in order to provide higher bandwidths for mobile users. Higher bandwidths require higher radio frequencies and smaller footprint of serving cells. Smaller cells mean more handoffs and increased signaling, rendering legacy mobility protocols, namely Mobile IP, non scalable where mobile users have to notify their home agents after each handoff. Hence, we have studied many micro-mobility protocols, namely Hierarchical Mobile IPv6 (HMIPv6) proposed as a complementary solution for mobile IP, which is based on a hierarchical architecture and tends to limit the handoff management at a local level. Unfortunately, the hierarchical architecture of HMIPv6 presents major drawbacks with respect to robustness and scalability. The paradox is that such structure is extremely vulnerable to a failure of the station at the higher level of the hierarchy (called MAP) and that this station is the most heavily loaded in the network constituting a system bottleneck.

On the other hand, many techniques have been proposed by the IETF in order to improve the handover management procedure, such as fast handover, which tends to reduce the handover latency. This lead us to propose a framework that integrates the micro-mobility management mecanisms, namely the protocol HMIPv6 combined with the fast handover technique, and the signaling protocol RSVP-TE in an MPLS based radio access network. The main idea is to replace the tunnels required by HMIPv6 with MPLS paths (LSP). In this context, we propose the Q-HMIP model which aims to reduce the handover latency by implementing the fast handover technique, to increase the robustness and flexibility of the system by distributing the load on the MAP node towards all the underneath LSR routers, through the application of the dynamic LSP modification mechanism integrated in the RSVP-TE signaling protocol, and finally to offer a guaranteed QoS for mobile users in a scalable fashion provided by DiffServ over MPLS approach.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

SIGLES ET ABRÉVIATIONS

AF	: Assured Forwarding
AP	: Access Point
AR	: Access Router
BA	: Binding Acknowledgement
BE	: Best effort
BG	: Border Gateway
BST	: Base Station
BU	: Binding Update
CN	: Correspondent Node
Codec	: Coder/Decoder
CR-LDP	: Constrained-Based Routing Label Distribution Protocol
DARPA	: Defense Advanced Research Projects Agency
DHCP	: Dynamic Host Configuration Protocol
DiffServ	: Differenciated Services
DoD	: Downstream on-demand
DSCP	: Differenciated Services Code point
EF	: Expedited Forwarding
EGW	: Edge Gateway
ER	: Explicit Routing
FEC	: Forwarding Equivalent Class
FIFO	: First In First Out
FTN	: FEC-to-NHLFE
HA	: Home Agent
HMIP	: Hierarchical Mobile Internet Protocol
IETF	: Internet Engineering Task Force
ILM	: Incoming Label Map

IntServ	: Integrated Services
IP	: Internet Protocol
IPPOA	: IP Wireless Point of Attachment
ITU	: International Telecommunication Union
Kbps	: Kilobits per second
LCOA	: Local Care-of-Address
LDP	: Label distribution Protocol
LER	: Label Edge Router
LFIB	: Label Forwarding Information Base
LSFSB	: Label State Fair Share Bandwidth
LSP	: Label Switched Path
LSR	: Label Switched Router
MA	: Mobility Agent
MAC	: Media Access Control
MAP	: Mobility Anchor Point
Mbps	: Megabits per second
MIP	: Mobile Internet Protocol
MN	: Mobile Node
MPLS	: Multi Protocol Label Switching
NHLFE	: Next Hop label Forwarding Entry
NS-2	: Network Simulator version 2
OSI	: Open System Interconnection
PCM	: Pulse Code Modulation
PHB	: Per-Hop Behavior
QoS	: Quality of Service
RAN	: Radio Access Network
RCOA	: Regional Care-of-Address
RFC	: Request For Comments
RSVP	: Ressource reSerVation Protocol

RWP	: Random Way Point
SLA	: Service Level Agreement
TCP	: Transmission Control Protocol
TE	: Traffic Engineering
TOS	: Type of Service
UD	: Unsolicited Downstream
UDP	: User Datagram Protocol
UMTS	: Universal Mobile Telecommunications System
VINT	: Virtual InterNetwork Testbed
VoIP	: Voice over Internet Protocol (IP)
VPN	: Virtual Private Network
WFQ	: Weighted Fair Queuing

CHAPITRE 1

INTRODUCTION

Les réseaux sans fil peuvent se classer généralement, selon la technologie d'accès, en deux catégories : les réseaux d'accès fixes sans fil (WLAN, Bluetooth, DECT, etc) et les réseaux d'accès mobiles ou cellulaires (GSM, GPRS, UMTS, etc). Les réseaux cellulaires comme GPRS se focalisent sur la meilleure gestion possible de la mobilité, c'est-à-dire les mécanismes permettant aux utilisateurs de pouvoir se déplacer sans rompre les communications en cours. En contrepartie, le débit offert est très limité, ce qui limite la portée de ces équipements cellulaires à la téléphonie. Actuellement, de nouvelles technologies 3G comme UMTS sont en train d'émerger, offrant un débit plus élevé (2 Mbit/s) permettant d'étendre les domaines des applications. D'autre part, les descriptions de tous les réseaux d'accès mobiles de nouvelle génération (3G et plus) présentent toutes une tendance vers ce qu'il est convenu d'appeler le Tout-IP (*All-IP*) : un réseau de transport en mode paquet, permettant la convergence des réseaux voix/données et fixe/mobile, et fonctionnant sous IP depuis la station mobile jusqu'à l'accès vers l'Internet. Ces réseaux permettront de fournir de nouveaux services multimédia à haut débit et simples d'usage incluant les données, la voix et la vidéo, indépendamment du réseau d'accès, et d'assurer une mobilité totale de terminaux, ce qui soulève un certain nombre de défis que ce mémoire abordera.

Dans ce premier chapitre, nous présentons d'abord quelques concepts et principes de base qui nous permettrons par la suite d'énoncer les éléments de la problématique. Ensuite, nous précisons nos objectifs de recherche, nos contributions et les principaux résultats escomptés, pour terminer avec le plan du mémoire.

1.1 Définitions et concepts de base

Les réseaux IP ont été mis en place initialement par l'interconnexion d'hôtes fixes, ayant chacun une adresse IP et reliés par un réseau filaire. L'objectif était d'offrir

une communication rapide à haut débit entre usagers distants. L'adresse IP d'une machine du réseau est son identificateur unique qui lui permet de communiquer avec d'autres machines. Pour que ces machines puissent coopérer, il a été nécessaire de définir un certain nombre de standards. L'architecture des machines de l'Internet repose sur une approche en couches, similaire au modèle OSI (Interconnexion des Systèmes Ouverts), reparti en 7 niveaux. On s'intéressera plus particulièrement aux couches liaison et réseau (couches 2 et 3 respectivement). La couche liaison gère l'accès au médium physique et certaines informations peuvent être très utiles dans la gestion de la mobilité dans IP. La couche réseau est actuellement implémentée par le protocole IP dans l'Internet.

Un réseau IP mobile est un réseau IP standard qui offre la mobilité aux usagers qui y sont connectés. La mobilité dans l'Internet a été introduite par l'IETF (Internet Engineering Task Force) qui s'est principalement penché sur la gestion des déplacements d'un ordinateur mobile sur l'Internet, c'est-à-dire du passage d'un réseau local à un autre réseau local. Ce travail a permis de définir un protocole appelé IP Mobile (Perkins et al., 2002; Johnson et al., 2004), qui existe en deux versions : la version 4 (utilisant le protocole sous-jacent IPv4) et la version 6 (utilisant le protocole sous-jacent IPv6). Cette dernière, offre plus de fonctionnalités tout en apportant des améliorations à la première. Le but de ce protocole était de permettre à un hôte mobile de poursuivre ses communications pendant un changement de point d'attache à l'Internet en fournissant à ce hôte une adresse temporaire (*Care-of-Address, CoA*) dans tout nouveau réseau visité. Selon ce protocole, on distingue deux types de réseaux suivant la position du nœud mobile. On appelle *réseau mère* ou *réseau principal* (HN) le réseau auquel est rattaché le nœud mobile administrativement. C'est le réseau dans lequel il est déclaré dans le DNS (*Domain Name System*) et sur lequel il obtient une adresse IP principale (HA). C'est l'adresse qui sera toujours utilisée par le hôte mobile et ses correspondants pour identifier les communications au niveau applicatif. D'un autre côté, on appelle *réseau visité* ou *réseau étranger* (FN) un réseau où le nœud mobile se trouve à un moment donné lors de ses déplacements. Lorsqu'un hôte mobile quitte son réseau

mère, IP Mobile utilise le «tunnelage» pour cacher l'adresse mère du nœud mobile aux routeurs situés entre le réseau mère et le nœud mobile. La fin du tunnel correspond à l'adresse temporaire du hôte mobile. Ce dernier devra indiquer cette adresse à son agent mère (et éventuellement à ses correspondants dans MIPv6) périodiquement pour qu'il puisse maintenir une correspondance entre l'adresse principale et une adresse temporaire. Les communications deviennent donc indépendantes de la localisation et l'hôte mobile doit toujours pouvoir continuer à utiliser son adresse IP principale.

Un modèle général des différents réseaux d'accès mobiles interconnectés et reliés à l'Internet est présenté à la Figure 1.1. On appelle un *domaine IP sans fil* un ensemble d'un ou de plusieurs réseaux d'accès sans fil (*Radio Access Networks,* RAN) placés sous une même autorité administrative. Du point de vue IP, les réseaux d'accès peuvent se considérer comme des *points d'attache IP sans fil* (IPPOA) connectés au réseau dorsal IP par des passerelles de frontière (*Border Gateways,* BG) vers l'Internet. Les réseaux d'accès sont organisés en se basant sur des technologies d'accès et/ou des régions géographiques différentes. De plus, chacun regroupe plusieurs stations de base (BST), appelés aussi *points d'accès* (AP), qui constituent l'interface entre les unités mobiles et le réseau. Un *hôte mobile* (MN) communique avec un ou plusieurs (pour la diversité) points d'accès, qui sont à leur tour connectés à des *routeurs d'accès* (AR) en utilisant un mode de transport choisi. Les routeurs d'accès gardent l'association (*mapping*) des points d'accès, c'est à dire les identités des APs et les interfaces physiques (canaux de communications), pour chacun de ses hôtes attachés.

Dans un RAN, la mobilité est gérée au niveau de la couche radio (*Access or Link-Layer Mobility*) de façon transparente. La couche supérieure (IP) verra donc le RAN comme une seule entité. Les stations du domaine dédiées à la gestion de la mobilité sont appelées *Agents de Mobilité* (*MA*). Dans un tel modèle, chaque MN est attachée à un réseau particulier dont il est «originaire», c'est son réseau mère, le réseau où l'abonnement a été pris par exemple. Dans le même ordre d'idée, nous appelons *réseau visité* (FN) tout autre domaine où le MN peut se connecter.

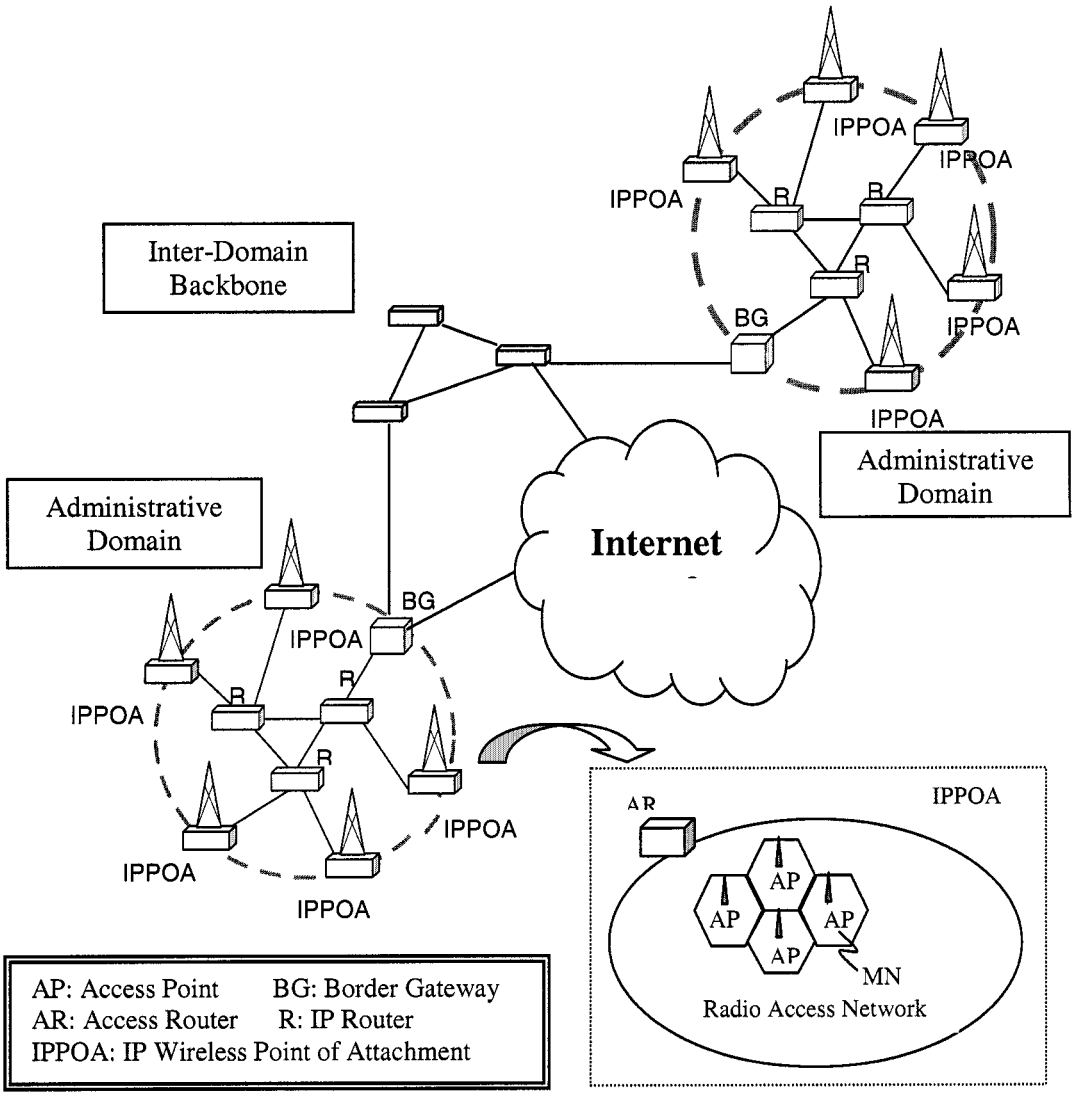

Figure 1.1 Modèle général d'un réseau d'accès mobile de nouvelle génération

1.2 Éléments de la problématique

On sépare généralement la gestion de la mobilité en deux parties distinctes : la macro-mobilité et la micro-mobilité. Formellement, la macro-mobilité concerne la gestion des déplacements des utilisateurs à grande échelle entre les différents domaines dont le nœud mobile a besoin d'acquérir une nouvelle adresse de routage IP. La micro-mobilité concerne la gestion des déplacements des utilisateurs à petite échelle à

l'intérieur d'un sous-réseau, d'un domaine administratif donné ou de plusieurs domaines dont l'adresse de routage IP du nœud mobile ne change pas. Cette division est aujourd'hui largement admise et les deux types de mobilité sont gérés indépendamment.

Le processus enclenché quand un mobile actif (en cours de communication) change son point d'attache à l'Internet est appelé la *relève* (*handoff* ou *handover)*. Ceci peut être vu aussi bien au niveau macro-mobilité (le MN change de domaine) qu'au niveau micro-mobilité (le MN change d'antenne ou de RAN).

La *latence de la relève* (*handoff latency*) est le laps de temps entre le dernier moment où le mobile peut recevoir et émettre des paquets IP à travers l'ancien routeur d'accès et le premier moment où il peut recevoir et émettre des paquets à travers le nouveau routeur d'accès. C'est donc le temps pendant lequel un nœud mobile ne peut ni recevoir, ni émettre un trafic IP. Par ailleurs, le processus de relève peut être amélioré soit en réduisant le nombre de paquets perdus, soit en diminuant la charge de la signalisation, soit encore en rendant le processus le plus rapide possible. On parlera alors de :

- ***Smooth handoff*** : une relève qui a pour but principal de minimiser la perte de paquets, sans condition sur le délai d'acheminement (*forwarding*) des paquets ;
- ***Fast handoff*** : une relève qui a pour but principal de minimiser le délai de déconnexion, sans conditions sur le nombre de paquets perdus ;
- ***Seamless handoff*** : la définition absolue est une relève où il n'y a pas de changement dans la capacité, la sécurité ou la qualité de service. En réalité, une dégradation est tout de même observée. La définition pratique est que les applications ou les utilisateurs ne remarquent pas ces dégradations.

La gestion de la relève est évidemment le point essentiel dans la gestion de la mobilité, un MN pouvant provoquer de nombreuses relèves durant une connexion. Cette gestion doit assurer la continuité de communication entre le MN et le réseau, en maintenant une qualité de service (QoS) acceptable.

Il a été démontré dans la littérature que IP Mobile résout le problème de la macro-mobilité. Il est moins bien adapté à la micro-mobilité, lorsque les unités mobiles effectuent des *handoffs* fréquents dans une même zone géographique. Tant que le déplacement du nœud ne se situe pas entre des points d'accès sur des sous-réseaux IP différents, des mécanismes de mobilité de niveau liaison (niveau 2 de la couche OSI) offrent probablement une convergence plus rapide et nécessitent bien moins d'*overhead* que IP Mobile. D'autre part, dans la version standard de IP Mobile, la nouvelle localisation d'un mobile est toujours signalée à son Home Agent. Ce dernier est ainsi averti de tous les déplacements des unités mobiles qu'il gère. Ces opérations génèrent un trafic important de signalisation (trafic de contrôle). Certaines optimisations ont été proposées au sein de l'IETF pour pallier cet inconvénient majeur mais aucune ne semble totalement satisfaisante pour gérer le trafic de bout en bout. De plus, les pertes de paquets pendant les relèves peuvent être importantes puisque la procédure d'enregistrement est longue, en particulier si le Home Agent se trouve à l'autre bout du monde. La durée d'une relève peut atteindre plusieurs secondes dans l'Internet actuel. D'autre part, les changements fréquents de CoA rendent difficile la fourniture de qualité de service avec IP Mobile.

Plusieurs solutions ont été proposées dans la littérature pour gérer la micro-mobilité (Campbell et al., 2002; Soliman et al, 2004). Toutes reposent sur le principe suivant: le réseau visité par un nœud mobile se charge des déplacements locaux; le Home Agent n'est donc pas prévenu de tous les changements de localisation du nœud mobile qu'il gère. De façon générale, ces propositions peuvent se classer en deux types (Campbell et al., 2002): modèles basés sur le routage (*routing-based schemes*) et modèles basés sur le tunnelage (*tunneling-based schemes*).

Les modèles basés sur le tunnelage sont généralement choisis pour réduire la latence du routage. Cependant, ils présentent un défaut important du point de vue de fiabilité et de flexibilité. En fait, la structure en arbre hiérarchique de ces modèles est statique, et il est extrêmement vulnérable aux pannes à un des stations de haut niveau dans la hiérarchie (*single point of failure*). Un tel système, proche d'un *bottleneck*, n'est

évidemment pas très flexible. Ce type d'architecture ne favorise pas non plus la robustesse du réseau. En effet, tout le système repose sur quelques machines dédiées assurant les fonctions principales, la défaillance de l'une d'entre elles est donc particulièrement difficile à récupérer. C'est beaucoup plus loin de la "philosophie" IP basée sur des structures étendues (*flat*) avec des algorithmes et des informations fortement distribués.

Les modèles basés sur le routage, quant à eux, bien qu'ils éliminent l'*overhead* du tunnelage, se prêtent moins bien à un déploiement graduel (*scaling*). En fait, pour chaque unité mobile, il faut répliquer les entrées de tables de renvoi (*forwarding tables*) dans tous les nœuds sur le chemin montant, contrairement aux quelques points sélectionnés dans le cas des modèles basés sur le tunnelage.

1.3 Objectifs de la recherche

L'objectif principal de ce mémoire est de proposer un nouveau modèle pour améliorer les procédures de gestion de la micro-mobilité dans un réseau d'accès mobile tout-IP. De manière plus spécifique, cette recherche vise à :

- proposer une architecture répartie des *agents de mobilité* en se basant sur le protocole MPLS pour supporter la micro-mobilité des usagers, de façon à augmenter la robustesse du réseau et la flexibilité du système;
- concevoir et implanter un ensemble de mécanismes et d'algorithmes basés sur l'architecture proposée pour gérer la mobilité des usagers d'une façon dynamique et en temps réel, tout en réduisant la *latence de la relève* et en fournissant une provision de qualité de service (QoS) assurée par les chemins MPLS;
- évaluer l'efficacité de cette architecture et la performance des algorithmes associés, en égard aux exigences de qualité de service, de robustesse de réseau et de flexibilité de système dans la gestion dynamique et en temps réel de la mobilité des usagers.

1.4 Plan du mémoire

Ce mémoire est organisé de la manière suivante. Le chapitre 2 présente les protocoles et architectures fondamentales impliquées dans ce mémoire, notamment MPLS et IP Mobile. Il examine également certaines propositions pour gérer la micro-mobilité afin d'améliorer la gestion de la mobilité présentée dans le protocole IP Mobile.

Le chapitre 3 introduit un nouveau modèle basé sur le protocole MPLS pour la gestion de la mobilité IP. Il présente l'architecture et les algorithmes de ce modèle ainsi qu'une analyse de performance de ces algorithmes.

Le chapitre 4 présente une analyse des résultats en comparant avec ceux fournis par des algorithmes existants. En guise de conclusion, le chapitre 5 résume les principaux résultats obtenus, fait état des limitations des travaux, pour finir avec une indication de recherches futures.

CHAPITRE 2

LA MOBILITÉ IP ET SES PRINCIPAUX ENJEUX

L'évolution des réseaux et services vers les "réseaux de nouvelle génération" ou NGN (*Next Generation Networks*) constitue une tendance majeure des télécoms, pour laquelle le marché montre un intérêt accru. Ces réseaux sont supposés être des plates-formes multiservices supportant des nouveaux services multimédias à haut débit incluant les données, la voix et la vidéo, en temps réel. L'évolution des réseaux mobiles visant à offrir cette multitude de services hybrides aux usagers mobiles n'a pas pu réussir sans l'introduction du support de la mobilité IP et de la qualité de service. Dans ce chapitre, nous présentons et analysons les solutions proposées dans la littérature pour gérer la mobilité IP. Tout d'abord, nous décrivons le protocole Mobile IP de l'IETF, qui est actuellement le protocole le plus largement utilisé dans l'Internet pour gérer la mobilité IP. Ensuite, nous exposons quelques méthodes proposées au sein de l'IETF pour améliorer ce protocole, notamment le *smooth-handover*, le *fast-handver* et le *Bi-directional Edge Tunnel Handover*. Par la suite, nous présentons quelques protocoles de micro-mobilité qui permettent de traiter les déplacements de mobiles à l'intérieur d'un même domaine. Enfin, nous introduisons quelques technologies et architectures impliquées dans cette recherche, notamment le protocole MPLS et l'architecture Diffserv de la Qualité de Service.

2.1 Le protocole Mobile IP

Le protocole Mobile IP existe en deux versions : Mobile IPv4 (utilisant le protocole sous-jacent IPv4) et Mobile IPv6 (utilisant le protocole sous-jacent IPv6).

2.1.1 Mobile IPv4

Mobile IPv4 (Perkins et al., 2002) est la technique la plus ancienne de gestion de la mobilité dans IP. Elle doit son succès à sa simplicité et sa flexibilité. Elle est à l'origine de plusieurs documents IETF.

Définitions

Tout d'abord, nous définissons les différentes entités qui composent le réseau IP mobile :

Nœud mobile (MN) : équipement IP qui change de point d'accès d'un réseau (ou sous-réseau) à un autre et implémente le protocole Mobile IP.

Agent mère (HA) : routeur d'accès sur le réseau de référence (réseau mère) d'un mobile, qui envoie les datagrammes dans un tunnel pour les remettre au mobile lorsqu'il visite un autre réseau. Le HA met à jour les informations concernant la localisation du mobile.

Agent visité (FA) : routeur d'accès sur un réseau visité par le nœud mobile, qui fournit des services de routage au mobile lorsqu'il est enregistré auprès de lui.

Agent de mobilité (MA) : agent mère ou agent visité.

Correspondant (CN) : machine (mobile ou non) qui communique avec un mobile.

Adresse temporaire (CoA) : cette adresse reflète le point d'accès courant du mobile lorsqu'il visite un autre réseau.

Point d'accès (AP) : équipement intermédiaire entre le réseau filaire et le nœud mobile qui offre la connexion aux nœuds mobiles qui lui sont rattachés. Un ou plusieurs points d'accès , appelé aussi stations de base (BS), sont connectés à un routeur d'accès.

Réseau d'accès radio (RAN) : le RAN regroupe plusieurs routeurs d'accès, connectés au réseau dorsal IP par des passerelles de frontière (*Edge Gateways, EGW*).

L'architecture de base de ces équipements est présentée à la Figure 2.1.

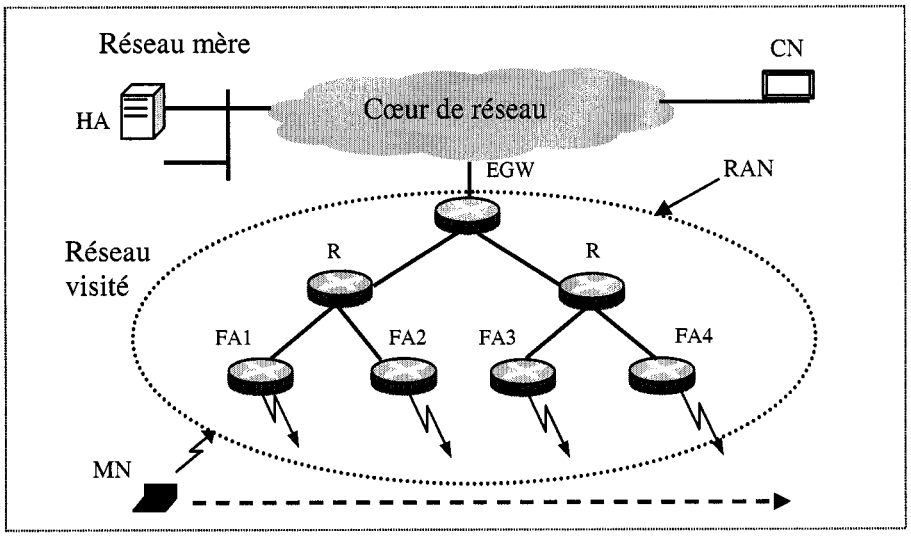

Figure 2.1 Architecture Mobile IPv4

Fonctionnement du protocole

Principe de base

Un nœud mobile se déplace de réseau en réseau et s'attache à des bases. Une base implémente des fonctionnalités de niveau 2 du modèle *OSI*. Elle assure une connectivité de niveau liaison de données et permet l'échange d'informations avec un mobile par un canal sans fil. Les agents de mobilité (agent mère et agent visité) maintiennent une liste des nœuds mobiles qu'ils gèrent. Cette liste est appelée *cache d'association*; elle associe l'adresse principale du mobile à son adresse temporaire. Le rôle principal de ces agents de mobilité est d'encapsuler, ou de décapsuler, les paquets en transit entre les correspondants et les nœuds mobiles en ajoutant ou en enlevant un en-tête d'adressage.

Adressage

Lorsqu'un mobile quitte son réseau mère, Mobile IPv4 utilise le "tunnelage" pour cacher l'adresse mère du mobile aux routeurs situés entre le réseau mère et le mobile. La fin du tunnel correspond à l'adresse temporaire (*CoA*) du mobile. Cette adresse temporaire doit être une adresse à laquelle les datagrammes peuvent être remis par des

mécanismes de routage IP classiques. À l'adresse temporaire, le datagramme d'origine est enlevé du tunnel et remis au nœud mobile. De façon générale, il existe deux types d'adresse temporaire:

i. Une "*Foreign Agent care-of address*" qui est une adresse temporaire fournie par un FA grâce aux messages *Agent Advertisement*. Dans ce cas, l'adresse temporaire est l'adresse IP du FA. C'est donc le FA qui est à l'extrémité du tunnel; lorsqu'il reçoit les datagrammes tunnelés, il les décapsule et remet le datagramme d'origine au mobile. Ce mode d'acquisition d'adresse temporaire est préférable, car il permet à de nombreux nœuds mobiles de partager une même adresse temporaire.

ii. Une "*co-located care-of address*" qui est une adresse IP locale, acquise par des moyens externes que le mobile associe à l'une de ses interfaces de réseau. Cette adresse peut être acquise dynamiquement par des mécanismes tels que DHCP (*Dynamic Host Configuration Protocol*), ou peut être possédée par le mobile comme adresse à utiliser dans certains réseaux visités. Lorsque le mobile utilise une "co-located care-of address", il se trouve lui-même à l'extrémité du tunnel et décapsule les datagrammes tunnelés jusqu'à lui. Ce mode permet à un mobile de fonctionner sans FA, mais il pose un problème au niveau de l'espace d'adressage d'IPv4.

Encapsulation IP dans IP

Le HA ne fait qu'encapsuler les paquets en ajoutant un nouvel en-tête IP devant l'en-tête du datagramme reçu (Perkins, 1996), comme le montre la Figure 2.2.

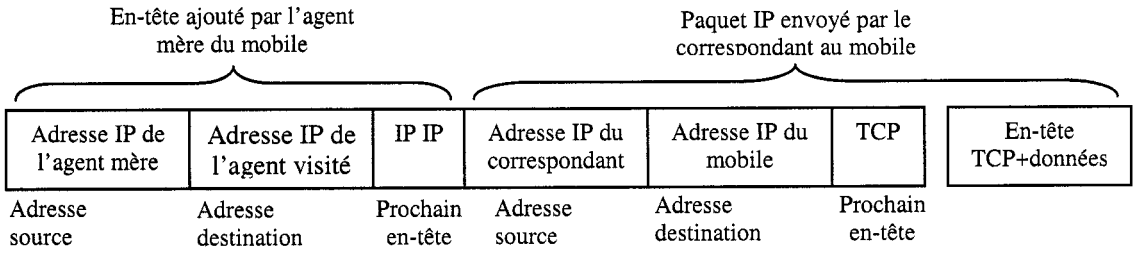

Figure 2.2 Encapsulation IP dans IP

Ainsi, les datagrammes sont facilement redirigés et routés dans l'Internet. L'adresse IP vers laquelle le Home Agent fait suivre les paquets destinés au mobile est la *care-of address*.

Découverte des agents de mobilité

Une caractéristique propre au mobile est de pouvoir se déplacer au cours d'une communication. Pour cela, un nœud mobile doit pouvoir détecter ses déplacements, c'est-à-dire détecter le changement de sous-réseau, ce qui nécessite l'obtention d'une nouvelle adresse temporaire. Le protocole de *Découverte des Agents* (Perkins et al., 2002) met en place un échange de messages permettant cette détection : les agents de mobilité envoient périodiquement des messages annonçant leur disponibilité sur le lien par l'émission de messages *Agent Advertisement* contenant l'information nécessaire pour l'identification du sous-réseau. Cette information peut être le préfixe réseau par exemple. Par ailleurs, un nœud mobile peut explicitement demander un tel message par l'émission d'un *Agent Solicitation* (cas où l'agent tombe en panne par exemple). Ces messages sont authentifiés et sont envoyés en *broadcast* ou *multicast*.

Enregistrement auprès de l'agent mère

Lorsque le nœud mobile détecte qu'il a changé de sous-réseau (à travers les messages explicités ci-dessus), il doit acquérir une nouvelle adresse temporaire et s'enregistrer auprès de son agent mère et de l'agent visité du réseau visité. L'acquisition de cette nouvelle adresse se fait grâce au protocole DHCP (Droms, 1997). Une fois que le nœud mobile a une adresse temporaire valide, il émet un message d'enregistrement (*Registration Request*) en indiquant la correspondance entre son adresse principale et son adresse temporaire et éventuellement d'autres options. Ce message passe par le FA qui le transmet au HA du mobile s'il accepte les requêtes du nœud mobile. L'agent mère doit acquitter le message *Registration Request* pour bien confirmer la réception et pour informer le nœud mobile de l'acceptation ou du refus de la requête par un message d'acquittement (*Registration Reply*). À la réception du message *Registration Request*,

aussi bien l'agent mère que l'agent visité mettent à jour leur cache d'association pour ce nœud mobile. Ensuite, tant que le nœud mobile reste dans le même sous-réseau étranger, il doit uniquement envoyer un *Registration Request* à intervalle régulier pour éviter que son entrée dans le cache d'association des agents de mobilité n'expire. Par contre, à chaque nouveau déplacement dans un autre sous-réseau étranger, il devra reprendre les mêmes opérations que celles décrites ci-dessus. Si le nœud mobile retourne dans son sous-réseau mère, il doit se dés-enregistrer auprès de son agent mère. Il envoie alors un message *De-Registration Request* jusqu'à ce qu'il reçoive le message d'acquittement *De-Regitration Reply* qui spécifie que l'agent mère a bien reçu le message et qu'il a supprimé l'entrée pour ce nœud mobile.

Communication

La communication entre un nœud mobile et un correspondant (CN) quelconque requiert plusieurs mécanismes des agents de mobilité. Comme un nœud correspondant d'un nœud mobile ne connaît que l'adresse principale du nœud mobile, les paquets à destination du nœud mobile sont toujours envoyés dans le sous-réseau mère du nœud mobile. Si le nœud mobile ne s'est pas déplacé, les paquets lui seront « livrés » de la même manière qu'un nœud fixe, c'est-à-dire sans opérations supplémentaires. Par contre, si le nœud mobile est dans un sous-réseau visité, son agent mère devra capturer tous les paquets destinés au nœud mobile et les lui transmettre à son adresse temporaire, grâce à son cache d'association. De l'autre côté, les paquets envoyés par le MN ont l'adresse du CN comme adresse destination et l'adresse principale du mobile comme adresse source. Ceci présente une entorse au modèle de l'Internet puisque l'adresse source des paquets envoyés par le nœud mobile ne correspond pas au préfixe du sous-réseau visité. Les paquets devront alors obligatoirement passer par l'agent visité pour éviter qu'ils ne soient détruits (Furguson et al., 2000). Par contre, une fois que les paquets ont été routés hors du sous-réseau visité, ils vont directement du nœud mobile au CN sans passer par le réseau mère.

La Figure 2.3 montre les messages échangés lors de la découverte et de l'enregistrement de CoA auprès de HA, aussi bien la communication de base entre le nœud mobile et un correspondant qui n'a pas l'adresse actuelle de MN dans sa cache.

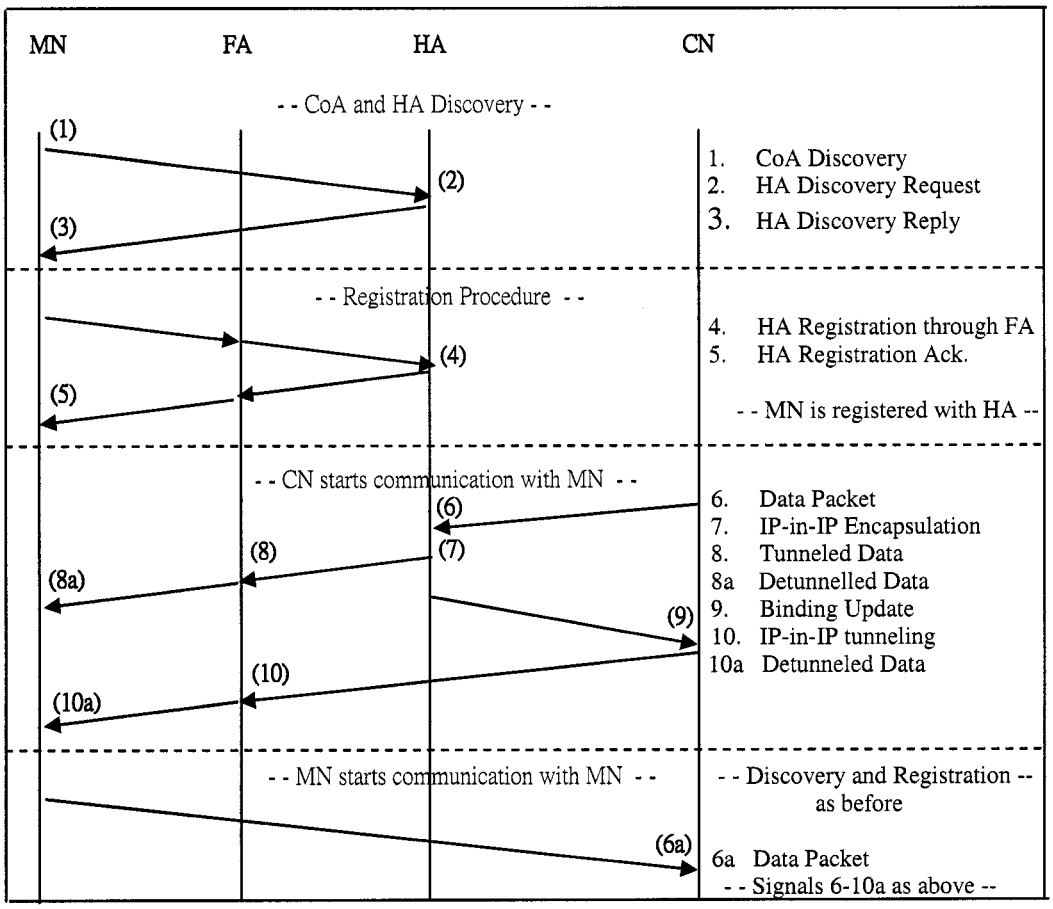

Figure 2.3 Messages de signalisation dans Mobile IPv4

Routage triangulaire

Du point de vue du routage, la principale faiblesse de Mobile IPv4 est le routage triangulaire, c'est à dire un routage via le Home Agent dans le sens correspondant vers le mobile. En effet, lorsqu'un mobile hors de son sous-réseau mère cherche à joindre une machine sur le même réseau visité, les paquets doivent néanmoins transiter par le sous-

réseau mère du mobile. Ce problème n'apparaît pas dans le sens mobile vers le correspondant, car Mobile IP définit un routage direct.

Routage optimisé

Afin d'obtenir un routage performant dans le sens correspondant vers le mobile, Perkins (2000) propose d'ajouter des mécanismes supplémentaires au Mobile IPv4 et de modifier la pile de protocoles TCP/IP. Dans cette proposition, seul le premier paquet envoyé à un mobile passe par son Home Agent ; après réception de ce paquet, le Home Agent indique au correspondant que la machine qu'il cherche à joindre est un mobile et fournit l'adresse à laquelle il peut être joint (son adresse temporaire).

2.1.2 Mobile IPv6

Mobile IPv6 (Johnson et al., 2004) est l'évolution logique de mobile IPv4. Il exploite les mécanismes avancés d'IPv6 pour introduire quelques améliorations par rapport à Mobile IPv4. Le mécanisme de configuration automatique des adresses d'IPv6 permet au mobile d'obtenir plus rapidement son adresse temporaire. L'architecture de base d'un réseau implémentant MIPv6 est présentée à la Figure 2.4.

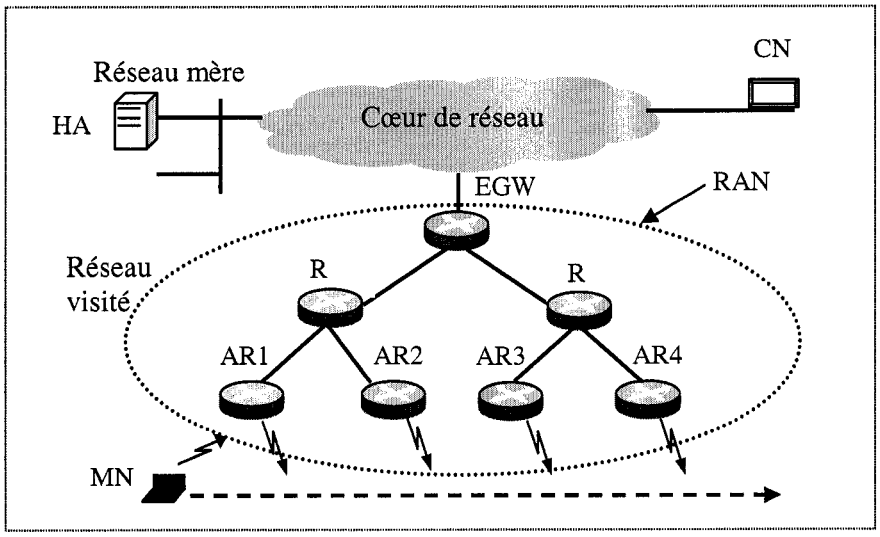

Figure 2.4 Architecture Mobile IPv6

Le protocole Mobile IPv6 partage avec Mobile IPv4 de nombreux points communs. Néanmoins, la version Mobile IPv6 est complètement intégrée dans IPv6, à la différence de Mobile IPv4 qui apparaît davantage comme une couche supplémentaire au-dessus de IPv4. Un espace d'adresses plus étendu est également disponible pour le mobile. Voici un résumé des différences entre les deux versions du protocole :

- Support de l'optimisation du routage : Mobile IPv6 intègre l'optimisation du routage (« Route Optimisation ») comme une fonctionnalité fondamentale à la différence de Mobile IPv4, qui en fait une extension optionnelle. L'optimisation du routage permet d'éliminer le routage triangulaire.
- Support intégré de la gestion des adresses d'origine (*Home Address*) et des adresses temporaires (*Care-of-Address*, *CoA*) de Mobile IP : lorsque le terminal mobile envoie des données, il intègre sa *Care-of-Address* dans le champ *Source Address* de l'en-tête du paquet IPv6. Cette adresse sera prise en compte dans le réseau pour le routage des paquets qui lui seront envoyés. En revanche, la *Home Address* doit être conservée du point de vue des applications (adresse unique), et celle-ci est placée dans le champ *Home Address* du paquet IPv6. Pour que ce mécanisme fonctionne et traite correctement la *Care-of-Address* et la *Home Address*, il requiert que l'ensemble des terminaux (mobiles ou fixes), routeurs et serveurs mis en jeu soient compatibles IPv6.
- L'utilisation directe de la *Care-of-Address* dans le champ *Source Address* de l'en-tête du paquet IPv6 évite l'opération d'encapsulation – ou de tunnellage – de Mobile IPv4. Les équipements distants envoient directement les paquets à la *Care-of-Address*.
- Il n'y a plus besoin de serveur *Foreign Agent* comme dans Mobile IPv4. Dans Mobile IPv6, le terminal mobile utilise directement les fonctionnalités IPv6 « *Neighbor Discovery* » et « *Address Autoconfiguration* ».

La Figure 2.5 montre les messages échangés pour les mêmes fonctions examinées dans la Figure 2.3. L'absence de l'agent visité et l'envoi des messages *Binding Update* par le mobile au CN, à la place de l'agent mère, montre la différence claire entre les deux cas. Une autre différence existe dans les mécanismes déjà décrits de découverte de *CoA* et l'enregistrement auprès de l'agent mère.

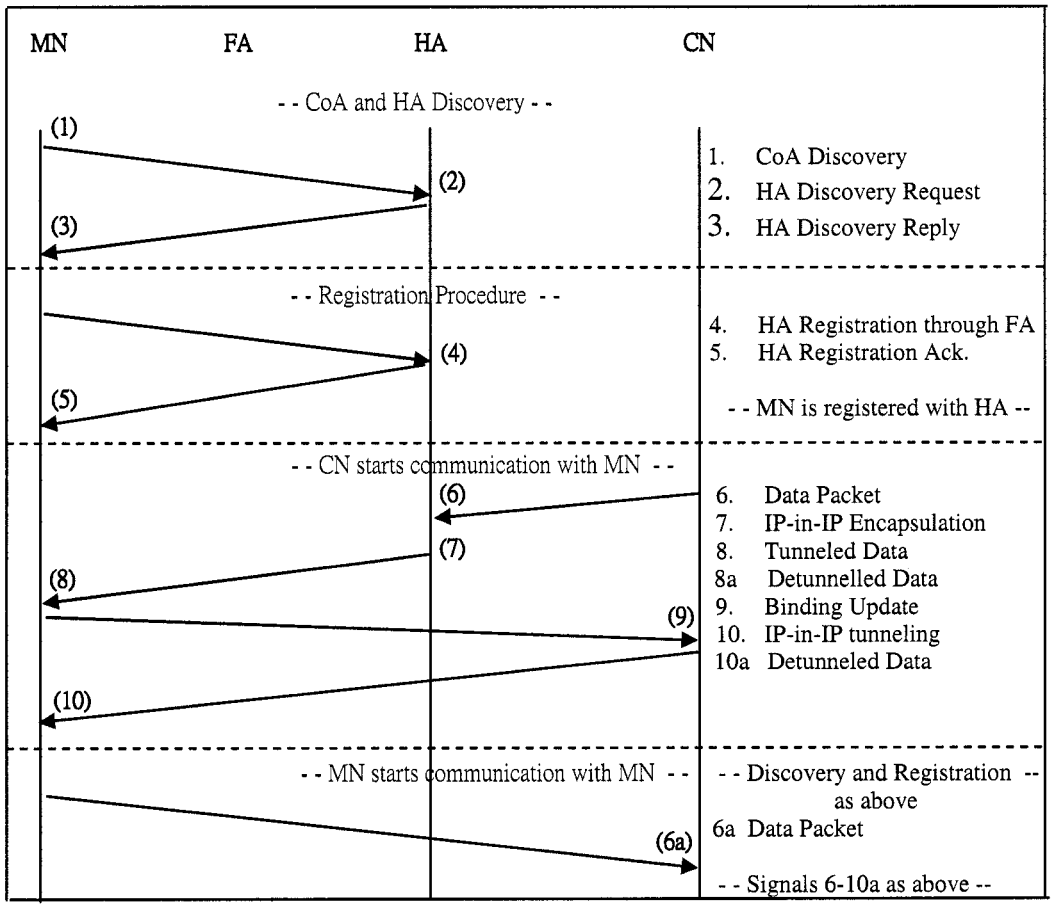

Figure 2.5 Messages de signalisation dans Mobile IPv6

2.2 Nouvelles techniques du *handover* IP

Plusieurs techniques ont été proposées au sein de l'IETF afin d'améliorer le processus du handover dans Mobile IP. Nous pouvons citer, entre autres, le *smooth-handover*, le *fast-handover* et le *Bi-directional Edge Tunnel Handover.*

2.2.1 Smooth-handover

Le *smooth-handover* (Koodli et al., 2000) est une technique censée réduire considérablement le nombre de pertes de paquets IP lors d'un handover. Pour réduire ces pertes, elle fait appel à un mécanisme de sauvegarde dans l'ancien routeur d'accès (RA). Ainsi, l'ancien RA effectue une copie de tous les paquets qu'il transmet au mobile avant, pendant et après la déconnexion. Bon nombre de paquets perdus en transmission ont été sauvegardés. Dès que le mobile obtient sa nouvelle connexion avec le nouveau RA et sa nouvelle adresse temporaire, le mobile dévoile au nouveau RA l'adresse du l'ancien RA. Le nouveau RA établit un tunnel IP avec l'ancien RA et lui indique la présence du mobile. À cet instant, l'ancien RA cesse de sauvegarder et de transmettre les paquets sur l'interface sans-fil à destination du mobile. Il transmet au mobile, et à travers le tunnel, tous les paquets précédemment sauvegardés. Le nouveau RA se chargera de relayer ces paquets vers le mobile. Les paquets dupliqués et sauvegardés lors de la déconnexion sont récupérés localement. Selon la technique de gestion du tampon, le mobile peut recevoir deux fois le même paquet. Il existe plusieurs techniques de sauvegarde afin d'optimiser les ressources de routeurs d'accès (Perkins et al., 1999).

2.2.2 Fast-handover

Le *fast-handover* (Koodli, 2004) étend MIPv6 et constitue un apport important aux protocoles de micro-mobilité. Son objectif principal est de réduire le délai de déconnexion du *handover* de bas niveau. Le principe est d'établir une nouvelle adresse temporaire avant de rompre la liaison du nœud mobile avec son ancien routeur d'accès, donc de réaliser le *handover* de niveau 3 avant que celui de niveau 2 n'ait terminé. Cela implique une anticipation sur le mouvement du mobile. Cette anticipation est faite par la remontée d'informations pertinentes de niveau 2, communément appelées *L2 triggers*.

Fonctionnement du protocole

Le protocole fonctionne en deux modes : handover initialisé par le mobile, et handover initialisé par le réseau. Dans le cas du handover contrôlé par le mobile, c'est le

mobile qui détecte qu'un handover va avoir lieu. Dans le cas du handover contrôlé par le réseau, une entité spécifique du réseau décide quand le mobile a besoin de se rattacher à un nouveau point d'accès.

La Figure 2.6 illustre le mode d'opération (cas du handover contrôlé par le mobile).

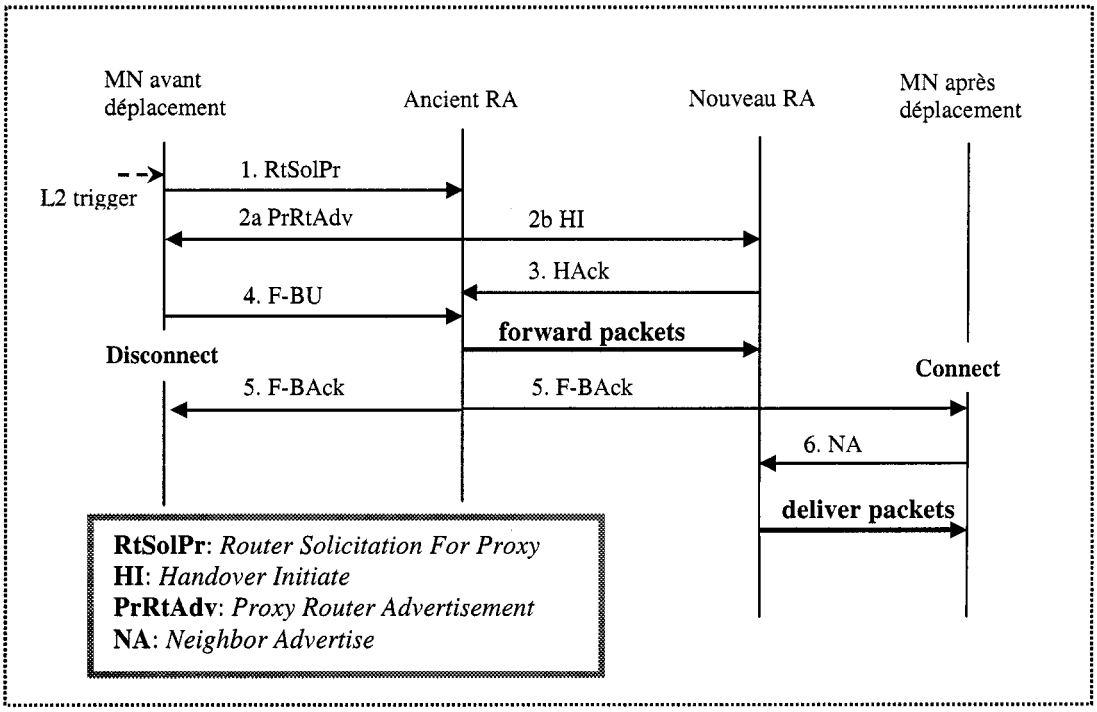

Figure 2.6 Mécanisme de *Fast-handover*

Nous considérons deux agents de mobilité: un ancien auquel le nœud mobile est attaché et un nouveau vers lequel le mobile se déplace. Ces agents de mobilité sont des agents visités (FA) dans le cas de MIPv4 et des routeurs d'accès (RA) dans le cas de MIPv6. L'opération s'effectuera de la manière suivante:

- Le MN envoie l'adresse du nouveau RA à l'ancien RA quand il détecte qu'un handover va avoir lieu, et ceci par l'intermédiaire d'un message appelé *Router Solicitation for Proxy* (*RtSolPr*);

- L'ancien RA retourne un message *Proxy Router Advertisement* (*PrRtAdv*) qui contient une nouvelle adresse temporaire (*nCoA*). Dans le même temps, l'ancien RA envoie une requête de validation d'adresse (*Handover Initiate*) au nouveau RA;
- Le nouveau RA retourne un acquittement de validation d'adresse par l'intermédiaire d'un message *Handover Acknowledgement* (*HAck*);
- Ensuite, le nœud mobile envoie un message *Fast Binding Update* (*F-BU*) à l'ancien routeur d'accès juste avant son déplacement pour lui indiquer son mouvement. Ce message déclenche le *forwarding* des paquets entre les routeurs d'accès, paquets que le nouveau RA met en *buffer*;
- L'ancien RA retourne un acquittement (*F-BAck*) à l'ancienne adresse temporaire du mobile (*oCoA*) et au nouveau RA, qui le fait suivre à la nouvelle adresse temporaire du mobile;
- Le MN averti le nouveau RA pour indiquer son arrivée par un message *Neighbor Advertise* (*NA*). C'est alors que le nouveau RA transmet les paquets mis en *buffer* au mobile

Contrairement au *smooth-handover*, les paquets ne sont pas sauvegardés lors du *handover*. Bien que ce protocole permette de rendre le *handover* plus rapide, des paquets peuvent être perdus . Pour résoudre ce problème, on peut utiliser le *bi-casting* vers les deux routeurs d'accès. Il est à noter que la charge due à la signalisation IP du *fast-handover* est importante.

2.2.3 Bi-directional Edge Tunnel Handover

BETH (*Bi-directional Edge Tunnel Handover*) (Kempf, 2001) est une extension du fast-handover, pour améliorer ses performances lors d'un handover rapide (mouvement extrême du mobile). BETH élimine la phase d'obtention de l'adresse temporaire et de son enregistrement. Quand un mouvement du mobile est détecté, les routeurs d'accès ont deux choix : soit ils appliquent le mécanisme du fast-handover et

entament le processus d'anticipation pour constituer la nouvelle adresse du mobile, soit ils décident de ne pas modifier l'adresse temporaire en cours, et d'utiliser cette adresse dans le nouveau réseau. Dans ce deuxième cas, un tunnel bidirectionnel est créé entre le nouveau RA et l'ancien RA. Le nouveau RA est averti que le mobile va établir une liaison, et qu'il est identifié par l'adresse définie par l'ancien RA. L'ancien RA intercepte tous les paquets destinés au mobile, et les dirige dans le tunnel. Le nouveau RA transmet directement ces paquets au mobile identifié par l'adresse temporaire initiale. Sachant que le mobile ne change pas d'adresse temporaire, tous les paquets qui lui sont destinés transiteront par l'ancien RA. De même, tous les paquets transmis par le mobile transiteront par l'ancien RA par l'intermédiaire du tunnel (contrairement au *fast-handover*, où les paquets sont transmis directement au correspondant). Ainsi, le déplacement du mobile est complètement transparent vis-à-vis du correspondant et de l'agent mère.

2.3 Protocoles de Micro-Mobilité

Le mécanisme de mobilité fourni par le protocole Mobile IP se révèle très inefficace pour des *handoffs* rapides et fréquents dans une même zone géographique, aussi appelé la *micro-mobilité*. Or, c'est précisément le cas d'un *handoff* entre deux points d'accès radio. Ces retards sont directement liés au temps d'aller-retour des messages d'enregistrement *(Binding Update, Binding Acknowledg*e), résultant :

- d'une surcharge de la signalisation;
- d'une perte de paquets assez élevée;
- d'une livraison retardée des données.

Dans la suite, nous allons présenter quelques solutions proposées dans la littérature pour améliorer les mécanismes du *handover* dans Mobile IP. Celui-ci gère la macro-mobilité alors que les nouveaux protocoles proposés ne s'occupent que de la micro-mobilité.

2.3.1 Mobile IPv6 Hiérarchique (HMIPv6)

Hierarchical Mobile IPv6 (Soliman et al., 2004) est une extension de Mobile IPv6. Son objectif principal est de minimiser le trafic de signalisation entre le nœud mobile et son agent mère. Comme les agents visités (FA) n'existent pas dans le contexte de MIPv6, le support de micro-mobilité nécessite l'introduction d'un nouveau type de nœud local qui agit comme un point d'ancrage pour assister les nœuds mobiles lors d'un handoff régional (dans un même domaine). Il s'agit de *Mobility Anchor Point* (*MAP*) qui est un routeur d'accès avec une adresse IP publique agissant comme un agent mère local pour les nœuds mobiles à l'intérieur d'un domaine particulier. Ainsi, le MAP reçoit tous les paquets destinés aux nœuds mobiles situés dans sa région (domaine) d'autorisation. La Figure 2.7 présente un réseau HMIPv6 typique.

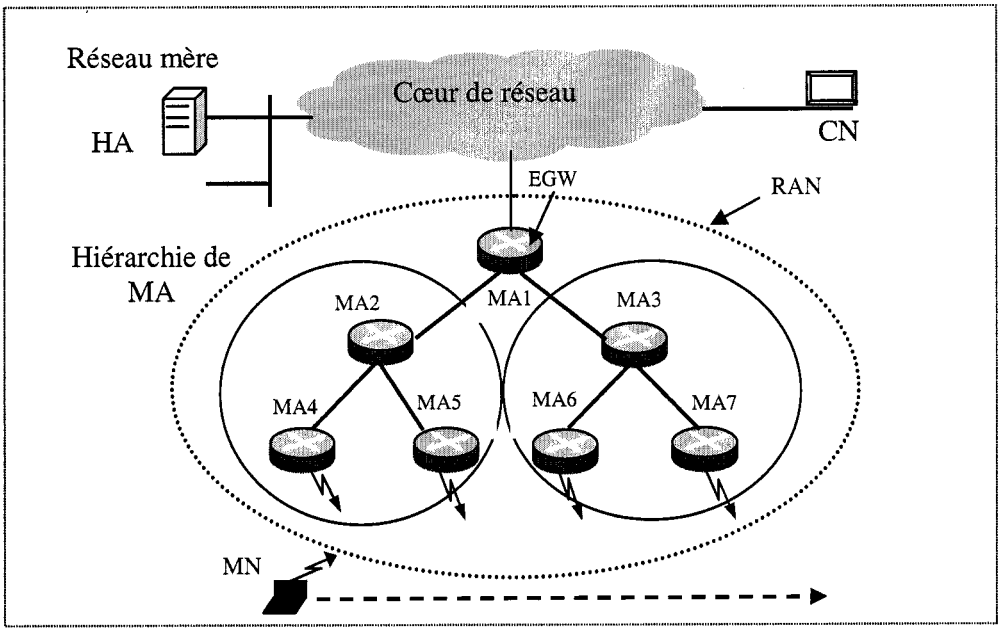

Figure 2.7 Architecture Mobile IPv6 Hiérarchique

L'architecture hiérarchique du réseau consiste à le découper en domaines, chaque domaine ayant son propre agent de mobilité (MA). Ce domaine à son tour est découpé en plusieurs régions ayant chacune son propre agent de mobilité. Ces agents sont

hiérarchiquement inférieurs à l'agent mobile du domaine. Une région peut à son tour être découpée en sous-régions. Généralement, un domaine est indépendant des sous-réseaux et sa taille est choisie par l'opérateur réseau.

Selon les spécifications, il y a deux modes d'opérations: le mode basique et le mode étendu. Or ce dernier s'adresse au cas des routeurs mobiles. Puisque nous ne nous intéressons pas à ce cas, nous allons présenter le mode basique seulement.

Mode d'opération basique

Lors de son arrivée dans un réseau visité, le MN découvre les adresses de différents MAPs existants et leurs distances respectives par des messages de type *Router Advertisment*. Ensuite, le MN établit deux *care-of-address* (*CoA*) : une adresse régionale (*RCoA*) basée sur le préfixe du MAP choisi (une adresse qui n'est pas topologiquement correcte) et qui reste active tant que le nœud mobile reste dans le même domaine administratif; l'autre adresse est locale (*LCoA*) et se base sur le préfixe du routeur d'accès sur le lien visité.

Ensuite, le nœud mobile s'enregistre auprès de son HA pour établir une association (*Binding*) entre son adresse principale et celle régionale (*RCoA*). Par la suite, le MN envoie un message de type *Binding Update* (*BU*) au MAP afin d'établir une association entre les adresses courantes de *RCoA* et *LCoA*. Ainsi, tous les paquets à destination de MN sont envoyés à l'adresse temporaire régionale en utilisant le champ *Routing Extension Header*. Le MAP reçoit ces paquets et les achemine dans un tunnel à l'adresse temporaire locale correspondante. Le MN établit aussi une association entre son adresse régionale et ses correspondants aux moyens de messages de type *BU*. Comme dans MIPv6, des messages *BU* sont envoyés périodiquement afin de garder à jour l'association entre l'adresse principale et le *RCoA*.

Une des options visant à optimiser la procédure de *Binding Update* consiste à encapsuler les messages HA *BU* à l'intérieur de MAP *BU* (Soliman et al., 2004). Les deux mêmes approches (séquentielle et encapsulée) sont proposées dans (Dommety et al., 2001). La Figure 2.8 illustre la différence entre les deux méthodes.

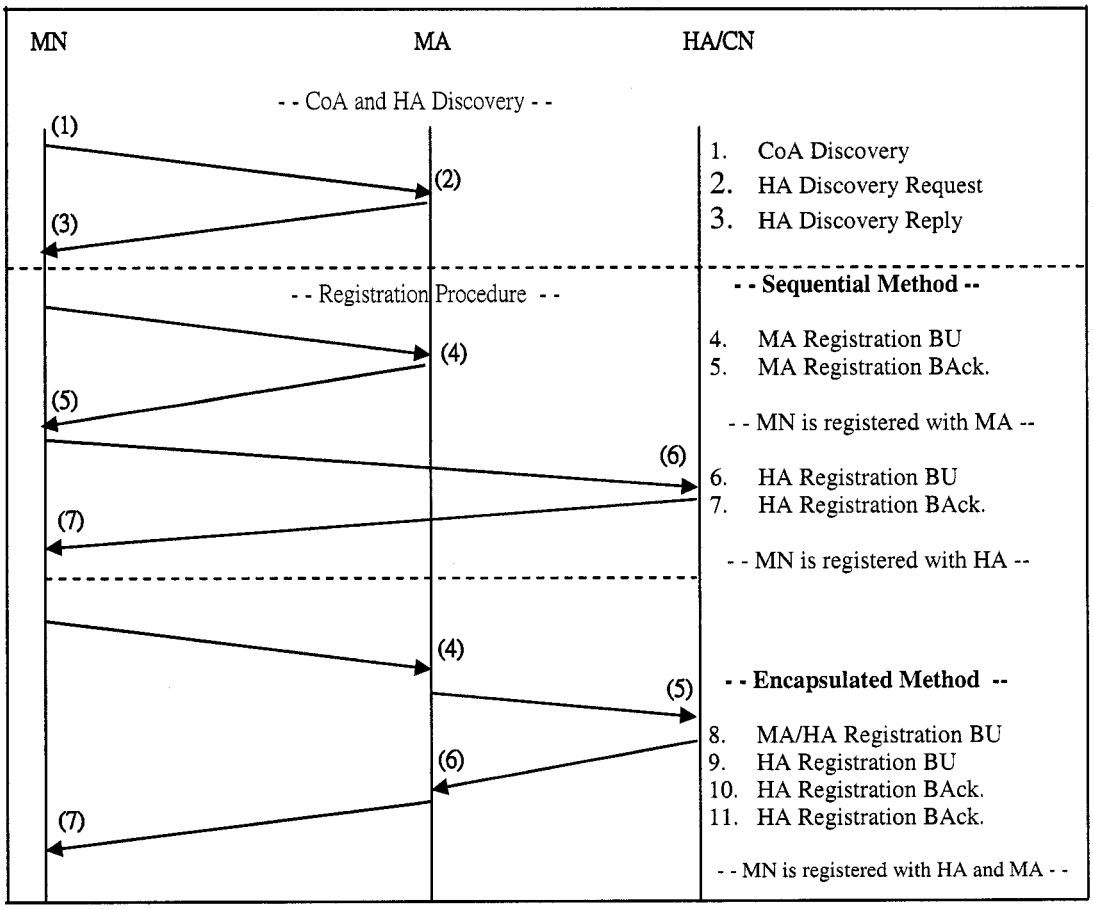

Figure 2.8 Options d'enregistrement dans Mobile IPv6 hiérarchique

2.3.2 Cellular IP

Cellular IP (Campbell et al., 2000), inspiré des systèmes cellulaires, est un protocole de micro-mobilité reposant sur le protocole Mobile IP pour la gestion de la mobilité entre domaines. Il ambitionne de remplacer Mobile IP dans le réseau d'accès. Un réseau *Cellular IP* est basé sur une architecture hiérarchique composée d'un routeur passerelle, des nœuds *cellular IP* (points d'accès) et des nœuds mobiles implémentant le protocole *Cellular IP*, comme l'illustre la Figure 2.9. Le routeur passerelle assure la liaison entre le réseau *Cellular IP* et le reste d'Internet. Il filtre, contrôle et propage les paquets en provenance et à destination du réseau. Les points d'accès sont connectés ensemble par un réseau filaire et ont une interface sans fil pour communiquer avec les nœuds mobiles.

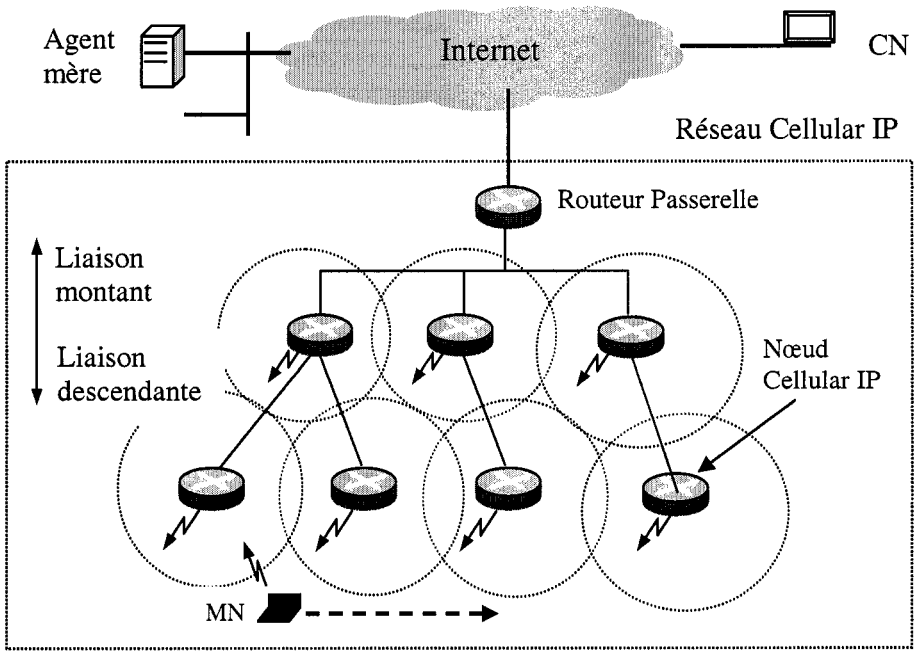

Figure 2.9 Réseau Cellular IP

La gestion de la localisation est très différente de celle utilisée par Mobile IP. L'adresse IP n'est plus utilisée pour localiser un équipement mais uniquement pour l'identifier. De ce fait, il n'est plus nécessaire de faire des encapsulations ou des conversions d'adresse. La localisation des nœuds mobiles est contenue dans deux différents caches dans les points d'accès. L'utilisation de deux caches permet de différencier le traitement des nœuds mobiles actifs de ceux inactifs. On dira qu'un hôte est actif quand il échange des paquets de données avec au moins un correspondant. Le *cache de pagination* est utilisé pour localiser les hôtes mobiles inactifs et le *cache de routage* pour la localisation des hôtes actifs. Ces caches gardent des associations entre l'adresse IP du nœud mobile et l'interface du point d'accès utilisé pour atteindre ce nœud. Ces associations sont construites par le chemin inverse des paquets envoyés par le nœud mobile (aussi bien les paquets de données que ceux de contrôle). Le routage se fait donc de saut en saut sur le plus court chemin. La localisation des nœuds mobiles inactifs est approximative : les points d'accès sont organisés en aires de pagination et cherchent uniquement à savoir dans quelle aire se situe le nœud mobile. Dans un réseau

Cellular IP donné, chaque aire de pagination a un identifiant unique annoncé par tous les points d'accès. Cependant, tous les points d'accès n'ont pas de cache de pagination.

Dans ce schéma, un nœud mobile n'a pas de point d'attache dédié, il utilise le meilleur à tout moment. Il n'y a donc pas d'authentification entre les points d'accès. Cependant, un contrôle est effectué lors de l'entrée des nœuds mobiles dans le réseau *Cellular IP*, et seuls les messages de contrôle peuvent créer des nouvelles entrées dans les caches pour assurer une sécurité.

Fonctionnement du protocole

Trois messages de contrôle sont nécessaires pour le fonctionnement du protocole: *Route-Update*, *Paging-Update* et *Paging-Teardown*. Le routeur passerelle envoie périodiquement des messages aux points d'accès pour leur indiquer leur port montant (*uplink port*), c'est-à-dire le port utilisé pour atteindre le routeur passerelle. Ceci indique qu'aucune configuration préalable n'est requise sur les points d'accès. Tous les autres ports des points d'accès sont des ports descendants. Les points d'accès envoient aussi des *beacons* contenant, entre autres, l'identificateur du réseau *Cellular IP*, l'adresse IP du routeur passerelle et un identifiant d'aire de pagination sur leur interface radio.

Quand un nœud mobile entre pour la première fois dans un réseau cellulaire IP, il envoie une authentification et des informations utilisateur dans un *Paging-Update* à destination du routeur passerelle. Si le routeur passerelle accepte la demande du nœud mobile, celui-ci doit faire un enregistrement mère. Dans le cas de MIPv4, l'adresse indiquée dans cet enregistrement est celle du routeur passerelle, alors que dans MIPv6, c'est une adresse temporaire locale (*CoA*) créée à partir de préfixe réseau. Comme on l'a dit précédemment, un nœud mobile peut se retrouver dans deux états. Lorsqu'il est inactif, il doit mettre à jour les caches de pagination à chacune de ses entrées dans une nouvelle aire de pagination ou juste avant que son entrée n'expire (cas où le nœud mobile ne s'est pas déplacé). Cette mise à jour est assurée par l'émission d'un *Paging-*

Update. Un *Paging-Update* détruit aussi les entrées dans les caches de routage. Un nœud mobile peut par ailleurs demander explicitement la destruction de son entrée dans un cache de pagination pour éviter tout conflit. La suppression explicite d'une entrée dans le cache de pagination est faite par l'envoi d'un *Paging-Teardown.*

Dans son état actif, un nœud mobile envoie des paquets de données, en reçoit ou fait les deux. Les paquets de données envoyés par le nœud mobile mettent à jour les caches de routage sans que le mobile n'ait besoin d'envoyer d'autres paquets de contrôle. Par contre, quand un nœud mobile ne fait que recevoir des données, il lui faut envoyer périodiquement un *Route-Update* pour éviter que son entrée dans les caches de routage n'expirent. Ceci dit, que le nœud mobile soit en émission ou en réception, il doit envoyer un *Route-Update* chaque fois qu'il change de point d'accès. Ce paquet crée une nouvelle entrée dans tous les nouveaux points d'accès sur le chemin allant du nœud mobile au routeur passerelle. Quand un flux de données arrive pour un nœud mobile inactif, le premier paquet est utilisé pour faire la pagination (pagination implicite). Le paquet est transmis suivant les informations contenues dans les caches de pagination. Si jamais un point d'accès reçoit un paquet pour un nœud mobile dont il n'a aucune entrée (pas de cache de pagination), il duplique le paquet sur tous ses ports descendants. Quand le nœud mobile reçoit ce premier paquet, il envoie un *Route-Update* pour créer une entrée dans les caches de routage et devient actif.

Gestion de la relève

La relève est gérée aux moyens de deux mécanismes spécifiques appelés : *hard handoff* et *semi-soft handoff*. Ce dernier permet de garantir que la perte de paquets due à la relève sera minimale. Ainsi, le changement de point d'accès, appelé *hard handoff*, est automatiquement géré par le protocole. Cependant, des paquets peuvent être perdus pendant le temps nécessaire pour que le *Route-Update* atteigne le point d'accès qui doit réaliser le changement de route. Quand un nœud mobile peut interagir simultanément avec deux points d'accès, il peut faire un *semi-soft handoff*. Quand un nœud mobile décide de se déplacer vers un nouveau point d'accès, il envoie un *Route-Update* avec un

flag spécifique à travers le nouveau point d'accès et retourne écouter l'ancien. Quand le *Route-Update* atteint le premier point d'accès qui doit modifier et non créer l'entrée pour le nœud mobile, une nouvelle entrée est créée sans remplacer l'ancienne. Les paquets de données sont alors envoyés à l'ancienne et à la nouvelle localisation du nœud mobile. Quand le nœud mobile décide par la suite de se rattacher au nouveau point d'accès, il envoie un *Route-Update* pour détruire l'entrée avec l'ancien point d'accès.

Pour les nœuds mobiles ne pouvant pas être connectés simultanément à deux points d'accès, une autre technique appelée *indirect semi-soft handoff* sera utilisée. Ainsi, quand le nœud mobile décide de changer de point d'accès, il envoie un *Route-Update* avec un flag 'I' à travers son ancien point d'accès avec l'adresse du nouveau point d'accès dans le champ de l'adresse destination. Ce paquet est transmis au routeur passerelle qui l'envoie au nouveau point d'accès. À la réception de ce paquet, le nouveau point d'accès envoie un *Route-Update* avec l'adresse du nœud mobile comme adresse source, et on se retrouve alors dans la même situation que dans le *semi-soft handoff.*

2.4 Le protocole MPLS

Le MPLS ou la commutation d'étiquette (Rosen et al., 2001) est un protocole proposé par l'IETF qui utilise un mécanisme de routage qui lui est propre, basé sur l'attribution d'une étiquette ("label", appelé aussi "tag" dans la littérature) à chaque paquet. Cela lui permet de router les paquets en optimisant les passages de la couche 2 à la couche 3 du modèle OSI et d'être indépendant du codage de celles-ci suivant les différentes technologies (ATM, Frame Relay, Ethernet, etc...).

L'objectif initial de MPLS était d'associer la puissance de la commutation de la couche 2 avec la flexibilité du routage de la couche 3. Schématiquement, on peut le représenter comme étant situé entre la couche 2 (liaison) et la couche 3 (réseau). Ainsi, l'utilisation des étiquettes permet de prendre des décisions de routage seulement basées sur la valeur de l'étiquette et de ne pas effectuer des calculs complexes de routage

portant sur l'adresse IP au niveau de la couche 3 du réseau. La Figure 2.10 présente l'emplacement du protocole MPLS dans le modèle OSI, aussi bien que la position et le contenu d'une étiquette MPLS.

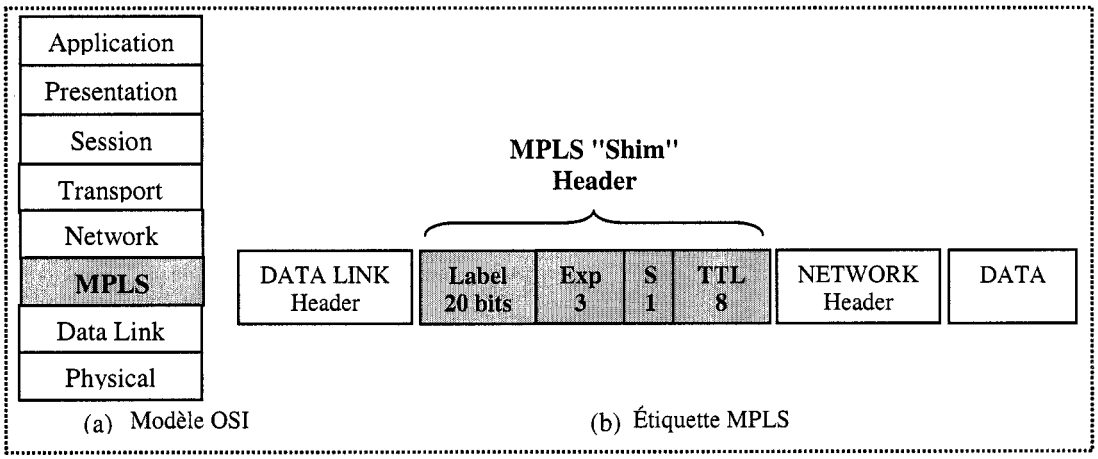

Figure 2.10 Emplacement du protocole MPLS dans le modèle OSI

Dans un réseau MPLS, les routeurs réalisant la commutation par étiquettes sont appelés LSR pour *Label Switch Routers*. Les routeurs situés à la périphérie du réseau (*Edge LSR ou LER*), qui possèdent à la fois des interfaces IP traditionnelles et des interfaces connectées au backbone MPLS, sont chargés d'imposer (*push*) ou de retirer (*pop*) les étiquettes des paquets IP qui les traversent. Les routeurs d'entrées, qui imposent les étiquettes, sont appelés *Ingress LSR*, tandis que les routeurs de sortie qui retirent les labels sont appelés *Egress LSR*, comme le montre la Figure 2.11.

À l'entrée du réseau MPLS, les paquets IP sont regroupés dans des classes FEC (*Forwarding Equivalent Classes*). Des paquets appartenant à une même FEC suivront le même chemin et auront la même méthode d'acheminement (*forwarding*). Typiquement, les FEC sont des préfixes IP appris par l'IGP (*Interior Gateway Protocol*) tournant sur la dorsale MPLS, mais peuvent aussi être définies par des informations de qualité de service ou de l'ingénierie de trafic (TE). À l'intérieur de la dorsale MPLS, les paquets sont transmis en échangeant des étiquettes (*label switching*), et aucune re-classification des paquets n'aura lieu par la suite. Chaque LSR affecte une étiquette locale qui sera

utilisée en entrée pour chacune de ses FEC, et la propage à ses nœuds voisins. Les LSR voisins sont appris grâce à l'IGP. L'ensemble des LSR utilisés pour une FEC, constituant un chemin à travers le réseau, est appelé *Label Switch Path* (LSP, Chemin à commutation de label). Il existe un chemin LSP pour chaque FEC et les LSP sont unidirectionnels. Les LSP sont établis en fonction du type de transmission des données (*control-driven*) ou après détection d'un certain type de données (*data-driven*). Les étiquettes, qui sont des identifiants spécifiques au protocole des couches basses, sont distribuées suivant un protocole de distribution d'étiquettes comme LDP (*Label Distribution Protocol*).

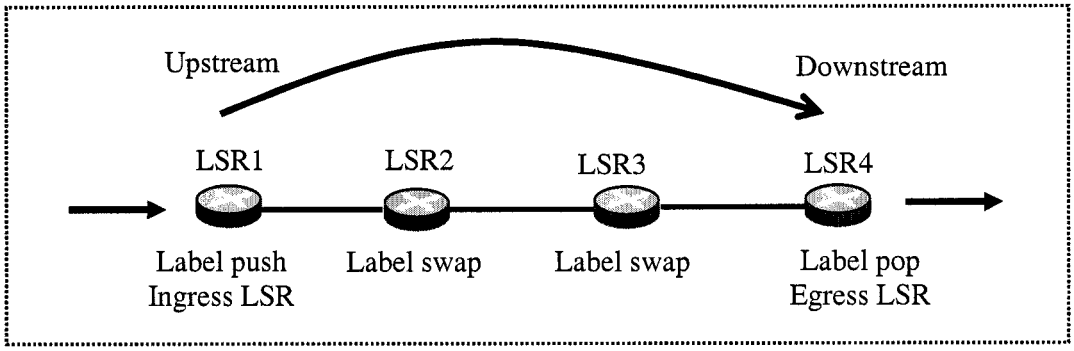

Figure 2.11 Composants d'un réseau MPLS

Dans l'architecture MPLS, la décision de lier une étiquette particulière L à une classe FEC particulière est prise par le LSR *downstream*. Le LSR *downstream* informe alors le LSR *upstream* du lien. La méthode de distribution des étiquettes est dite "downstream", car les liens label/FEC sont distribués dans la direction *downstream* vers *upstream*. Il en existe deux variantes : (a) *Downstream-on-demand* qui permet à un LSR de demander explicitement au prochain nœud d'une FEC, un label pour désigner cette FEC, (b) *Unsolicited downstream* qui permet aux LSR *downstream* de propager systématiquement toutes leurs étiquettes à leurs voisins, même s'ils ne l'ont pas explicitement demandé.

D'autre part, la technologie MPLS permet d'ajouter certaines fonctionnalités aux réseaux IP traditionnels notamment, l'ingénierie du trafic (TE) qui permet d'optimiser les ressources afin d'éviter les congestions dans le réseau ou encore amener de la redondance, et ceci par une répartition intelligente du trafic selon des critères tels que la destination du trafic, les paramètres de qualité de service, et bien d'autres. Présentement, il existe trois protocoles de signalisation dans MPLS : LDP, CR-LDP et RSVP-TE.

LDP, Label Distribution Protocol (Anderson et al., 2001), est un protocole de signalisation permettant d'apporter aux LSR les informations d'association des étiquettes (*label mapping*) dans un réseau MPLS. Il est utilisé pour associer des étiquettes à des classes FEC, ce qui crée des chemins LSP. Les sessions LDP sont établies entre deux éléments du réseau MPLS, qui ne sont pas nécessairement adjacents. Ce protocole ne supporte pas la réservation de ressources ni le routage explicite (*Explicit Routing*).

CR-LDP, Constrained-based Routing LDP (Jamoussi et al., 2002), est une extension du protocole LDP qui correspond à la notion de « routage basé sur les contraintes », ce qui permet de construire des chemins MPLS avec certaines contraintes de trafic ou de qualité de service. Ce protocole est dit *hard state* car la liaison est établie pendant toute la durée spécifiée du transfert jusqu'à ce qu'elle soit explicitement fermée.

RSVP_TE, *Ressource Reservation Protocol with Traffic Engineering* (Awduche et al., 2002), est une extension du protocole *RSVP* pour supporter des fonctionnalités de l'ingénierie de trafic et de gestion de qualité de service au sein d'un réseau MPLS. Ce protocole est dit *soft state* car la liaison n'est établie que pendant la durée spécifiée par des temporisateurs envoyés dans les messages de demande de réservation. Il faut alors rétablir la liaison une fois ce temps écoulé en recommençant la demande de réservation pour continuer à écouler le trafic.

Une description plus détaillée de protocoles RSVP et RSVP-TE est incluse en Annexe I. Les types et contenus de différentes tables MPLS sont présentés en Annexe II.

Ces annexes contiennent des informations utiles à une bonne compréhension du chapitre 3.

2.5 Qualité de Service – Services différenciés

L'objectif de la Qualité de Service (QdS) est de supporter des services de communications ayant des exigences qualitatives spécifiques. L'introduction de la QdS dans les réseaux mobiles est encore plus complexe, car leur topologie et leurs ressources évoluent dynamiquement. En fait, la QdS dans un réseau mobile est fortement liée aux mécanismes de *handover,* notamment le débit de transmission, la latence qui correspond au délai de transfert, la gigue et la perte de paquets. Principalement, il existe trois approches différentes pour fournir la qualité de service dans les réseaux IP : l'architecture à Intégration de Services (*IntServ*), l'architecture à Différenciation de Services (*DiffServ*) et DiffServ sur MPLS.

L'architecture *IntServ* (Braden et al., 1994) a été la première proposée. Bien qu'elle soit conçue pour fournir de la QdS de bout-en-bout, la réservation de ressources pour chaque flot entraîne de sérieux problèmes de passage à l'échelle (*Scalability*) dans les réseaux de cœur où le nombre de flots traités se compte en millions. Par conséquent, l'utilisation de l'architecture *IntServ* est limitée aux réseaux d'accès de petite taille où le nombre de flots qui utilisent des réservations est modeste.

L'architecture *DiffServ* (Blake et al., 1998) vise à fournir une solution de QdS globale résistant au facteur d'échelle. Les services sont offerts à des agrégats plutôt qu'à des flux particuliers. La différenciation de services est principalement réalisée grâce au champ *Differentiated Service* (DS ou DSCP : *Differentiated Services Code Point*) dans l'en-tête IP et au comportement associé (*Per-Hop Behavior* ou PHB). Cette architecture divise le réseau en domaines. Un domaine est un groupe de nœuds qui fonctionnent avec un ensemble commun de politiques d'allocation de service et de définitions de PHB. Un domaine DiffServ est constitué de deux types d'éléments fonctionnels: les éléments de bordure et les éléments de cœur du réseau. Les éléments de bordure sont responsables de la classification des paquets et du conditionnement du trafic en fonction des accords

de service (*Service Level Agreement* ou SLA) entre les domaines voisins. Les éléments de cœur du réseau ne sont responsables que du transit des paquets. L'IETF a été amené à définir deux nouveaux PHB pour l'architecture DiffServ : EF (*Expedited Forwarding*) (Jacobson et al., 1999) et AF (*Assured Forwarding*) (Heinanen et al., 1999).

Bien que DiffServ soit capable de fournir une solution de QdS globale résistant au facteur d'échelle, elle est conçue pour une architecture de QdS statique ou faiblement dynamique. Donc, elle n'est pas adaptée aux environnements fortement mobiles dans lesquelles les terminaux peuvent changer non seulement leurs points d'accès pendant une session de communication, mais encore leurs besoins en terme de QdS.

Le protocole MPLS, défini plus récemment, a été conçu pour répondre aux mêmes besoins adressés par DiffServ soit: fournir une solution de QdS qui résiste au facteur d'échelle. Pour le support de DiffServ dans MPLS, on trouve deux approches (Le Faucheur et al., 2002): (a) L-LSP: le choix du chemin est fait en fonction de la QdS du flux passant sur ce chemin, (b) E-LSP : le mode associé au champ expérimental (EXP) de trois bits de l'en-tête MPLS, qui permet de supporter jusqu'à 8 agrégats par un seul LSP. Ainsi, avec le protocole de signalisation RSVP-TE[1], il est possible de considérer des réservations dynamiques pour des LSP véhiculant un agrégat de flots plutôt que pour des micro flots séparés.

2.6 Panorama des propositions intégrant MPLS et Mobile IP

Dans cette section, nous aborderons les principaux travaux proposés dans la littérature qui intègrent le MPLS avec le protocole IP mobile. Le modèle proposé dans (Ren et al., 2001) est basé sur un des premiers draft proposé au sein de l'IETF qui porte sur le sujet. Après une description de base du fonctionnement du modèle dans un réseau

[1] Il n'est pas surprenant de trouver RSVP ici puisque RSVP lui aussi est lié à la construction de chemin, appelé *tunnel* dans le contexte RSVP, dans un modèle d'approche de la QdS IntServ. Insistons sur le fait que si RSVP est fait pour un réseau de routeurs IP, ici il s'agit de LSR, des équipements qui n'interviennent pas au niveau IP (qui n'utilise pas l'en-tête IP) pour la commutation MPLS. Des firmes, comme Cisco, traitent de «quantitatif» le RSVP IntServ et de « qualitatif » le RSVP DiffServ. RSVP-TE devient ainsi le protocole de signalisation utilisé dans un contexte par ailleurs DiffServ.

MPLS-MIPv4, une investigation en terme d'évolutivité (*Scalability*) est présentée. Plus spécifiquement, une évaluation du protocole en terme du délai de traitement dans le HA, le délai d'aller-retour ainsi que le débit (*throughput*) sur une connexion TCP est présentée. Les valeurs de ces métriques sont obtenues dans trois cas : MIPv4, MIPv4 sur MPLS dans une architecture *overlay* et MIPv4 sur MPLS dans une architecture intégrée. Les résultats montrent que la performance d'une architecture intégrée est toujours meilleure.

Une amélioration du modèle précédent est présentée dans (Um et al., 2001), qui utilise HMIPv4 comme protocole de mobilité et LDP comme protocole de signalisation dans MPLS. La contribution principale de ce travail est l'analyse de performance de trois différentes méthodes de routage. Un établissement complet d'une route, un établissement partiel et un routage *multicast* ont été comparés en prenant comme métriques le délai du *handover*, le délai d'interruption du service et les exigences du tampon (buffer requirements). Ce travail a conclu que le routage *multicast* est supérieur aux autres méthodes pour les deux premières métriques mais, il est inférieur en ce qui concerne les exigences du tampon et l'efficacité globale de la bande passante (*Overalay Bandwidth Efficiency*).

Une approche un peu différente est présentée dans (Kim et al., 2001), qui vise à fournir la QdS (DiffServ ou IntServ) au réseau d'accès sans-fil. Ce travail ne considère aucun protocole de mobilité particulier mais plutôt une architecture hiérarchique générale. Pour le service Diffserv, les auteurs proposent d'établir plusieurs chemins de redondance (backup) entre les routeurs d'accès et la passerelle de frontière (BG) dans un RAN. Ainsi, un chemin LSP pour chaque type de service (EF, AF et BE) est provisionné d'avance. Aussi, il y a un LSP dédié pour la signalisation entre le BG et chaque AR. Pour le service IntServ, juste les chemins de signalisation sont préétablis.

Une approche différente d'intégration du MPLS et des réseaux d'accès sans-fil est présentée dans (Chung et al., 2002). Ce travail propose le MPLS sans-fil (*Wireless* MPLS). Cette proposition est basée sur l'espérance que MPLS est capable de gérer la

communication entre un nœud mobile et une station de base sur la couche radio et de régler les erreurs sur les liens sans-fil. Ainsi, il propose des extensions aux protocoles LDP et RSVP-TE pour supporter un flux de bout-en-bout. Ces extensions incluent de nouveaux types d'en-têtes qui contiennent des champs de séquence et de CRC (*Cyclic Redundancy Check*) additionnels. Avec la supposition de base que MPLS opère sur la couche radio, nous pensons que ce travail se situe au-delà de notre recherche.

CHAPITRE 3

MODÈLE DE GESTION DE MOBILITÉ PROPOSÉ

L'objectif principal de ce mémoire est de proposer un nouveau modèle intégrant les mécanismes de gestion de la mobilité IP, notamment le protocole HMIPv6, avec le protocole de signalisation RSVP-TE, pour la gestion de mobilité dans un réseau d'accès mobile de nouvelle géneration. L'idée principale est de remplacer les mécanismes de tunnelage dans HMIPv6 par des chemins MPLS et de profiter de l'approche DiffServ sur MPLS dans la dorsale IP/MPLS/DiffServ de façon à répondre aux exigences des usagers en mobilité en terme de qualité de service, une exigence primordiale pour les nouveaux services multimédias et applications à temps réel.

3.1 Hypothèses de conception et spécifications

Le cadre d'intégration que nous proposons est basé sur les hypothèses suivantes:

- Les procédures de découverte et d'enregistrement de nœuds mobiles auprès de l'agent mère dans HMIPv6, comme décrit dans la section 2.2.1, sont inchangées;
- Tous les routeurs MPLS dans le RAN sont capables de modifier les chemins LSP en se basant sur le protocole RSVP-TE;
- Seuls les chemins MPLS point à point sont considérés;
- La communication entre les nœuds mobiles et les routeurs d'accès est basée sur le protocole IP et, par la suite, un nœud mobile ne contient aucune entité MPLS dans sa pile de protocoles (*protocol stack*);
- MPLS opère selon les modes suivants :
    - *Downstream-on-demand* : un routeur LSR demande explicitement au prochain nœud d'une classe FEC une étiquette pour désigner cette FEC;

- *Ordered LSP Control* : un routeur LSR ne lie une étiquette à une FEC que s'il s'agit du *routeur de sortie* (*egress LSR*) de cette FEC ou s'il a déjà reçu une étiquette référençant cette FEC;
- *Conservative Retention* : un routeur LSR ignore les associations d'étiquettes annoncées par les routeurs *downstream* si ces routeurs ne se trouvent pas (ou ne se trouvent plus) sur le prochain saut pour une FEC particulière. Ce mode d'opération permet au routeur LSR de retenir moins d'étiquettes.

- Pas d'agrégation d'étiquettes (*Label Aggregation*): l'agrégation est le fait de lier une seule étiquette à une union des FEC. Dans ce cas, l'union des FEC est aussi une FEC (dans un domaine particulier);
- Pas de fusion d'étiquettes (*Label Merging*) : Il y a une seule étiquette par un chemin LSP. Avec ce mode, deux paquets pour une même classe FEC qui arrivent avec des étiquettes différentes seront transmis avec des étiquettes de sortie différentes. Sinon, il est impossible de différencier entre les paquets transmis en se basant sur le champ source (interface ou étiquette d'entrée).

3.1.1 Méthodes d'établissement des chemins LSP

Généralement, il existe deux méthodes d'établissement d'un chemin LSP :

- *Data-driven LSP* – établit à la présence de données à transmettre seulement.
- *Control-driven LSP* – établit avant l'arrivée de données, en fonction d'informations fournies par un protocole de routage ou d'informations explicites d'une liste de connexion.

Normalement, la méthode *Data-driven* est utilisée avec le mode *Downstream on-Demand* (*DoD*) d'assignation et de distribution d'étiquettes, alors que la méthode *Control-driven* est utilisée avec le mode *Unsolicited Downstream* (*UD*). Dans notre cas, nous ne considérons pas le cas des LSP préétablis par avance, vu que nous voulons que la phase d'établissement des LSP soit contrôlée par les paramètres de qualité de service.

D'autre part, nous supposons qu'il n'y a pas d'agrégation ni de fusion d'étiquettes. En effet, l'association d'une étiquette à priori entre une pair source-destination n'est pas recommandée, étant donné que d'autres étiquettes seront requises plus tard.

3.1.2 Modification d'un chemin LSP

Il existe plusieurs mécanismes pour modifier ou pour rerouter un chemin LSP lors du changement de localisation d'un nœud mobile. Nous distinguons les mécanismes suivants :

- *LSP re-establishment* – un nouveau chemin LSP est établi vers/à partir de la nouvelle localisation du nœud mobile.
    - Avantages : simple.
    - Désavantages : les paquets en transit seront perdus.
- *LSP extension* – le chemin LSP est entendu à partir de l'ancien *routeur de sortie* (*egress LSR*) jusqu'au nouveau *routeur de sortie*.
    - Avantages : rapide, pas de perte de paquets.
    - Désavantages : chemin LSP plus long, augmentation probable de délai, besoin de mécanismes de détection des boucles.
- *LSP extension and modification* – dans un premier temps, le chemin est étendu ensuite, il sera modifié.
    - Combinaison de deux méthodes précédentes.
- *LSP multicast* – plusieurs chemins LSP sont créés vers toutes les localisations voisines du mobile.
    - Avantages : plus adapté aux mécanismes de *fast handoff* et *smooth handoff*.
    - Désavantages : besoin des LSPs point-multipoints, nécessite une connaissance extensive de la localisation, plus de difficulté à gérer les ressources.

- *LSP dynamic rerouting* – le chemin LSP est changé à partir du point le plus bas (le plus proche de MN) commun entre l'ancien et le nouveau chemin.
    - Une amélioration de la méthode *'LSP extension and modification'*.
    - Avantages : re-établissement complet de LSP non requis. Une partie du chemin LSP reste inchangée, ce qui engendre moins de signalisation.
    - Désavantages : plus de complexité.

Après l'analyse de différents mécanismes de reroutage d'un chemin LSP, on déduit que les deux mécanismes nommés *'LSP multicast'* et *'LSP dynamic rerouting'* sont les méthodes les plus efficaces. Donc, nous proposons l'utilisation de la deuxième méthode soit-le *'LSP dynamic rerouting'*, qui est possible avec le protocole RSVP-TE.

3.1.3 Support de la Qualité de Service DiffServ

Braun et al. (2000) ont fait une observation concernant l'architecture DiffServ dans un environnement IP mobile. Ils ont conclut que l'identification du flux basée sur les adresses IP et numéros de port source/destination n'est plus valide, puisque le changement de la localisation de nœuds en mobilité peut changer un ou plusieurs de ces paramètres. Une solution possible pour ce problème sera d'utiliser l'adresse mère de nœud mobile pour l'identification de flux. Dans HMIPv6, cela est possible en vérifiant le champ «*Home Address Destination Option* » dans l'en-tête IP de chaque paquet IP. Dans notre cas, nous traitons cette opération en nous basant sur MPLS. Nous avons déjà mentionné à la section 3.1 que l'agrégation et la fusion d'étiquettes ne sont pas permises dans notre approche. Ces deux hypothèses (avec la méthode L-LSP de séparer le trafic dans l'architecture DiffServ sur MPLS) permettent d'avoir un LSP différent pour chaque (*FEC-OA*) *pair*[2]. Ces trois critères établissent un traiteur (*handler*) unique des flux

[2] Le *OA* (*Ordered Aggregate*) est un ensemble d'agrégats *BA* (*Behavior Aggregates*), qui partagent une même contrainte, chaque paquet IP d'un *BA* étant sujet à un même comportement DiffServ (*PHB, Per-Hop Behavior*).

individuels. Ce traiteur est identifié comme l'objet « *LSP Tunnel session* » dans RSVP-TE.

3.2 Modèle de gestion de micro-mobilité Q-HMIP

Dans cette section, nous allons présenter notre modèle de gestion de la micro-mobilité nommé Q-HMIP. En premier lieu, nous présenterons le réseau de référence dans notre approche, pour entamer par la suite le fonctionnement du modèle ainsi que le mécanisme de micro-mobilité.

3.2.1 Réseau de référence

L'architecture de base d'un réseau d'accès radio (RAN) dans le cadre de cette recherche est présentée à la Figure 3.1.

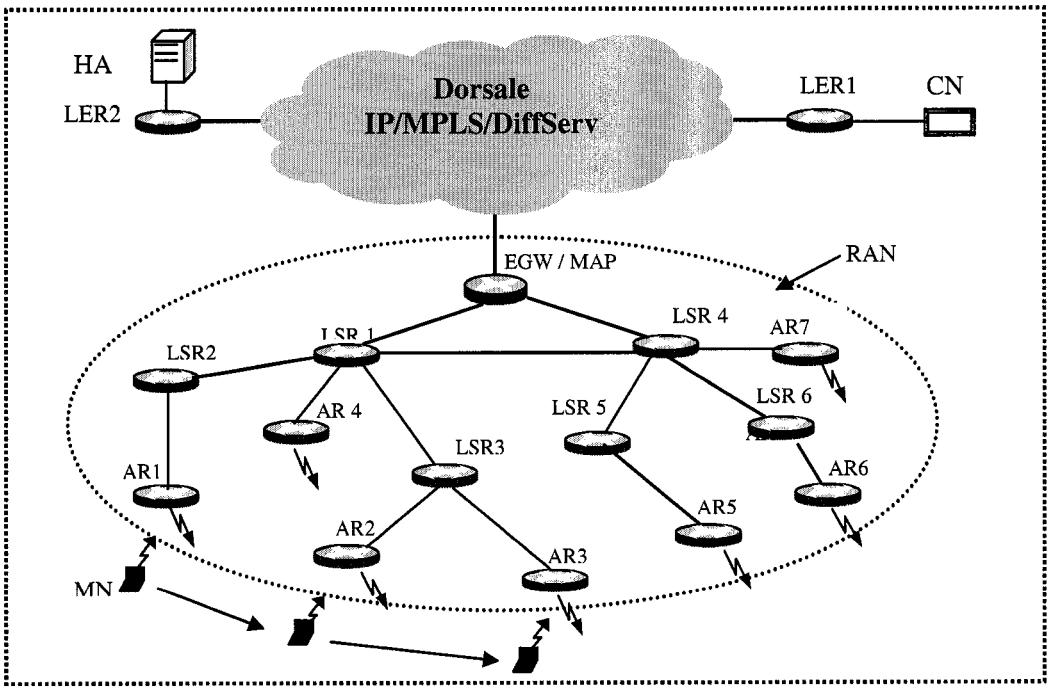

Figure 3.1 Réseau de référence

Le réseau est composé de plusieurs niveaux de routeurs LSR pour former ce qui est appelé un réseau *overlay*. Les composants de frontière sont les routeurs d'accès (AR), qui sont les premiers équipements IP vus par le nœud mobile. Un ou plusieurs points d'accès (AP), appelés aussi stations de base (BS), sont attachés (ou intégrés) à un routeur d'accès. Plusieurs ARs sont attachés à une (ou plusieurs) passerelle de frontière (EGW), qui est à son tour attachée à une dorsale IP/MPLS/DiffServ. Nous supposons que tous les routeurs d'accès dans le RAN sont des agents de mobilité (MA) et supportent les mécanismes de gestion de la mobilité dans HMIPv6. D'autre part, les ARs et le EGW (qui joue le rôle d'un MAP dans ce cas) sont interconnectés par des routeurs MPLS (LSR) afin de composer un réseau DiffServ.

3.2.2 Initialisation et établissement des chemins LSP

Dans notre cadre de travail (*framework*), les procédures d'enregistrement dans HMIPv6 sont utilisées pour l'établissement des chemins LSP avec les nœuds mobiles. Ainsi, au moment d'allumer son appareil, le nœud mobile détecte les signaux de balise (*beacon signals*) transmis par les stations de base voisines. Il choisit la station de base dont le signal transmis est le plus puissant, comme son point d'attache au réseau d'accès. De ce signal, le mobile sait s'il se trouve dans son réseau de référence (mère) ou dans un réseau visité. Dans le cas où il se trouve dans un réseau visité, le mobile acquiert alors deux nouvelles adresses IP temporaires. La première est l'adresse régionale (RCoA) valide au niveau du MAP, obtenue en concaténant l'identifiant de l'interface physique du mobile avec le préfixe réseau du MAP. La deuxième est l'adresse locale (LCoA), obtenue en concaténant l'identifiant de l'interface physique du mobile avec le préfixe réseau du routeur d'accès courant. Ensuite, le MN lance la procédure d'enregistrement des adresses LCoA et RCoA auprès du MAP et de son agent mère (voir section 2.3.1). Ces étapes, sont numérotées de 1 à 7 à la Figure 3.2. Les autres étapes illustrent la procédure initiale d'établissement d'un chemin LSP quand un correspondant initialise une communication vers un nœud mobile, comme nous allons le décrire dans la prochaine section.

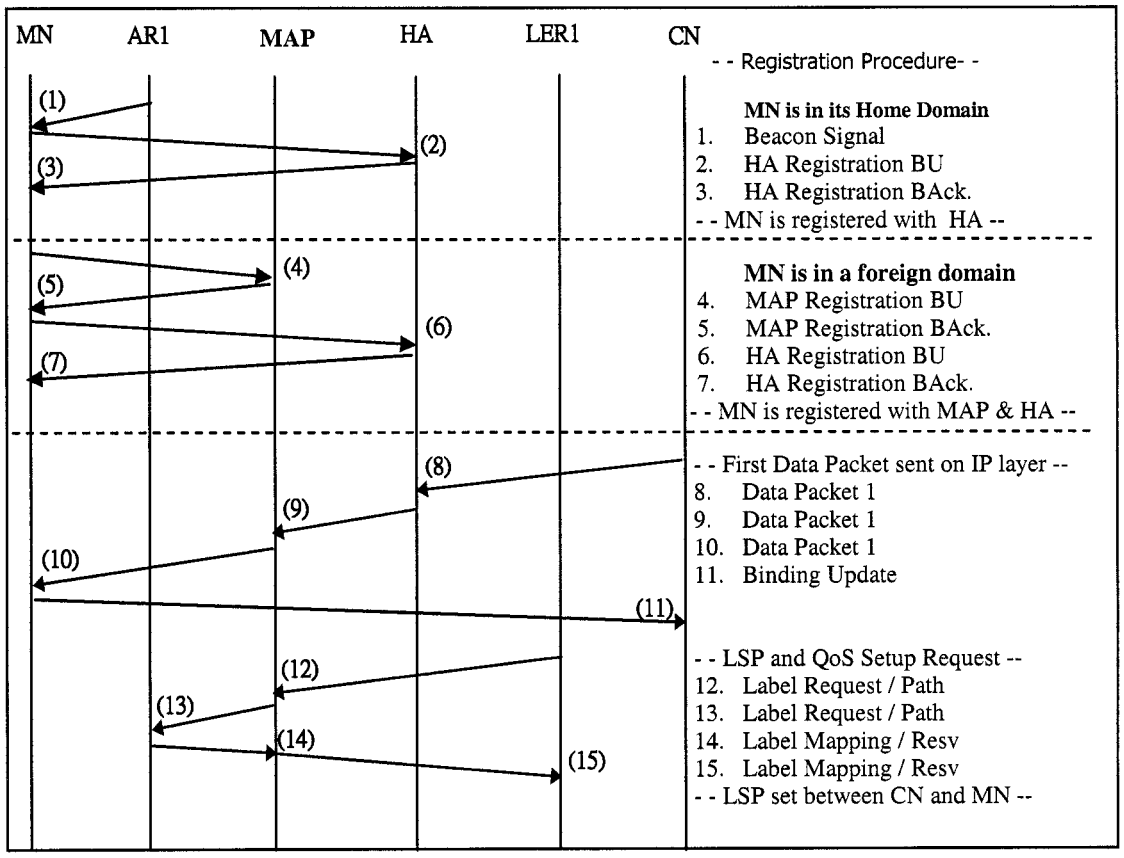

Figure 3.2 Initialisation et établissement des chemins LSP – CN vers MN

3.2.3 Communication initiée par le correspondant

Quand un correspondant (CN) initialise une communication vers le MN, il vérifie premièrement son cache d'association (*binding cache*) pour une entrée de l'adresse CoA de MN (enregistrée lors d'une session précédente). Dans le cas contraire, le MN envoie son premier paquet à l'adresse principale de MN. Si le routeur de périphérie de CN (LER1, à la Figure 3.1), n'a pas un LSP déjà établi vers le MN, il procède en acheminant ce paquet sur la couche IP comme décrit dans HMIPv6. L'agent mère (HA) intercepte ce paquet (étape 8 de la Figure 3.2) et vérifie son cache d'association pour une entrée de MN. Si le MN se trouve dans son réseau mère, le paquet sera acheminé directement vers lui. Sinon, le HA encapsule le paquet en ajoutant un nouvel en-tête IP devant l'en-tête du datagramme reçu en utilisant l'adresse RCoA de MN enregistrée dans sa cache comme adresse de destination. Ensuite, le MAP de la région où se trouve présentement le MN,

intercepte ce paquet et l'achemine vers le MN en utilisant l'adresse LCoA de MN enregistrée dans sa cache comme adresse de destination. À la réception d'un paquet tunnellé, le MN avise le CN de son adresse régionale *RCoA* par un message *Binding-Update* (BU), qui sera utilisé pour l'établissement d'un chemin LSP plus tard. Une autre variante consiste à envoyer un message de localisation (*Location Acquiring message*) par le correspondant à l'adresse principale de MN. Le HA intercepte ce message et retourne au CN l'adresse régionale RCoA de MN. Le CN utilise cette adresse pour envoyer les paquets qui suivent. Dépendamment de l'application que le CN roule et de ses paramètres de qualité de service, le routeur de périphérie LER1 établit un chemin LSP[3] vers celui de MN (AR1 dans ce cas), en envoyant un message PATH contenant l'objet LABEL_REQUEST à l'adresse RCoA de MN. Le MAP intercepte ce message et établit un chemin LSP avec le routeur AR1 en utilisant le protocole de signalisation RSVP-TE. Ainsi, le MAP envoie un message PATH au routeur *downstream* AR1 contenant, entre autres : (a) l'objet LABEL_REQUEST qui indique le type de données transporté et demande à ce qu'un LABEL soit associé à ce chemin, (b) l'objet EXPLICITE_ROUTE (ERO) qui contient la séquence de routeurs LSR à traverser jusqu'à AR1. Notons ici que l'adresse mère de MN avec les paramètres de QdS[4] sont utilisés comme FEC dans ce cadre afin d'établir des chemins LSP. Une fois le message PATH arrivé au routeur AR1, celui-ci renvoie un message RESV dans la direction montante (*upstream*) suivant le chemin pris par le message PATH avec l'objet LABEL. Chaque LSR intermédiaire met à jour cette valeur jusqu'à ce que le message RESV atteigne le MAP. C'est avec ce message que les réservations seront confirmées dans les routeurs. À partir de ce moment, le chemin LSP entre le MAP et le routeur AR1 est établi. Ensuite, le MAP envoie un message RESV contenant l'objet LABEL vers LER1. Finalement, un chemin LSP est établi entre le MAP et le routeur LER1.

---

[3] Le CN peut établir un ou plusieurs chemins LSP pour différents niveaux de qualité de service suivant le mode d'opération L-LSP.

[4] Les chemins LSP vers le MN sont établis seulement en fonction des accords de service (*Service Level Agreement* ou SLA) entre les domaines voisins et le MN. Même si nous ne les adressons pas dans ce travail, les considérations de sécurité constituent, à leur tour, un facteur que le HA ou d'autres nœuds doivent signaler avant de procéder.

Le Tableau 3.1 présente les entrées enregistrées dans les tables LFIB (*Label Forwording Information Base*) de différents routeurs impliqués dans l'établissement d'un chemin LSP entre CN et MN. Ces entrées sont les interfaces et les étiquettes d'entrée et de sortie de chaque routeur faisant partie du chemin LSP, le champ FEC et le champ *Timer* qui contient l'état du lien.

Tableau 3.1 Entrées des tables LFIB pour le LSP établi – CN vers MN

Node	Input I/F	Input Label	FEC	Output I/F	Output Label	Timer
LER1	--	--	FEC1	o-if-0	o-if-4	Tactive
GW/MAP	i-if-0	i-if-4	FEC1	o-if-0	o-if-3	Tactive
LSR1 (crossover)	i-if-0	i-if-3	FEC1	o-if-0	o-if-2	Tactive
LSR2	i-if-0	i-if-2	FEC1	o-if-0	o-if-1	Tactive
AR1	i-if-0	i-if-1	FEC1	--	--	Tactive

3.2.4 Communication initiée par le nœud mobile

Quand un nœud mobile veut communiquer avec un correspondant, il envoie ses paquets directement sur l'adresse IP de CN, sans passer par le HA. Au début de la communication, chaque paquet sera classifié à l'entrée du routeur d'entrée (*ingress*), AR1 dans ce cas, et il sera assigné à une classe FEC particulière suivant les paramètres de la qualité de service. Le routeur d'accès AR1 établit un (ou plusieurs) chemin LSP vers le routeur de frontière de CN (LER1) dans la direction montante avant d'envoyer les paquets. Ainsi, un LSP sera composé de routeurs {AR1, LSR2, LSR1, GW, --, LER1). À l'intérieur de la dorsale MPLS, les paquets sont commutés selon leur étiquette, et aucune re-classification des paquets n'aura lieu. Chaque LSR affecte une étiquette locale, qui sera utilisée comme entrée pour chacune de ses FEC et la propage à ses nœuds voisins.

3.2.5 Routage optimisé

Dans le cas ou le mobile se déplace dans un même domaine où se trouve le correspondant, le chemin LSP ne doit pas passer par le MAP afin de réduire le délai et de diminuer la charge sur le routeur EGW. Ainsi, quand le MN veut communiquer avec un CN, le premier paquet sera envoyé au CN en utilisant l'adresse RCoA de MN comme adresse source. Le MAP vérifie sa cache d'association pour une entrée de CN et le cas échéant, le MAP en déduit que le CN se trouve dans son domaine administratif et obtient son adresse locale LCoA. Ensuite, le MAP achemine le paquet vers le CN en utilisant l'adresse LCoA de CN comme adresse de destination. À la réception d'un paquet tunnelé par le MAP local, le CN envoie un message BU au MN contenant son adresse LCoA, qui sera utilisée par la suite dans l'établissement d'un LSP direct entre les deux nœuds. Comme déjà mentionné à la section 3.3.1, une autre variante consiste à envoyer un message de localisation (*Location Acquiring message*) par le MN au CN. À la réception d'un message dont le nœud d'origine et le nœud de destination se trouvent dans le même domaine administratif lui appartenant, le MAP intercepte ce message et retourne au MN l'adresse locale LCoA de CN. Le MN utilise cette adresse en vue d'établir un chemin LSP pour acheminer les paquets qui suivent.

Notons ici que, lors d'un déplacement, le MN avise le MAP et ses correspondants avec lesquels il est en communication de sa nouvelle adresse, afin de maintenir leurs caches d'association à jour.

3.3 Gestion de la relève dans Q-HMIP

Le déplacement de MN entre différents routeurs d'accès déclenche le processus de la relève décrit au le chapitre 1. Ainsi, nous distinguerons deux types de relève : une relève déclenchée lors d'un déplacement du mobile entre deux routeurs d'accès qui se trouvent dans un même RAN géré par un seul MAP, appelée *relève intra-RAN*, et une autre déclenchée lors d'un déplacement entre deux routeurs d'accès qui se trouvent dans deux RAN gérés par deux MAP différents, appelée *relève inter-RAN*.

3.3.1 Relève intra-RAN (micro-mobilité)

Notre approche pour la gestion de déplacement du mobile dans une même région est basée sur l'établissement d'un chemin LSP avec le nouveau routeur d'accès avant que le MN perde sa connexion avec l'ancien routeur d'accès. Nous adoptons le mécanisme d'anticipation du mouvement de MN présenté à la section 2.2.2.

La Figure 3.3 illustre le déplacement d'un nœud mobile (MN) récepteur de la zone desservie par le routeur d'accès AR1 vers celle desservie par le routeur AR2. Les messages de signalisation engendrés sont présentés à la Figure 3.4 et l'organigramme du mécanisme de la relève est présenté à la Figure 3.5.

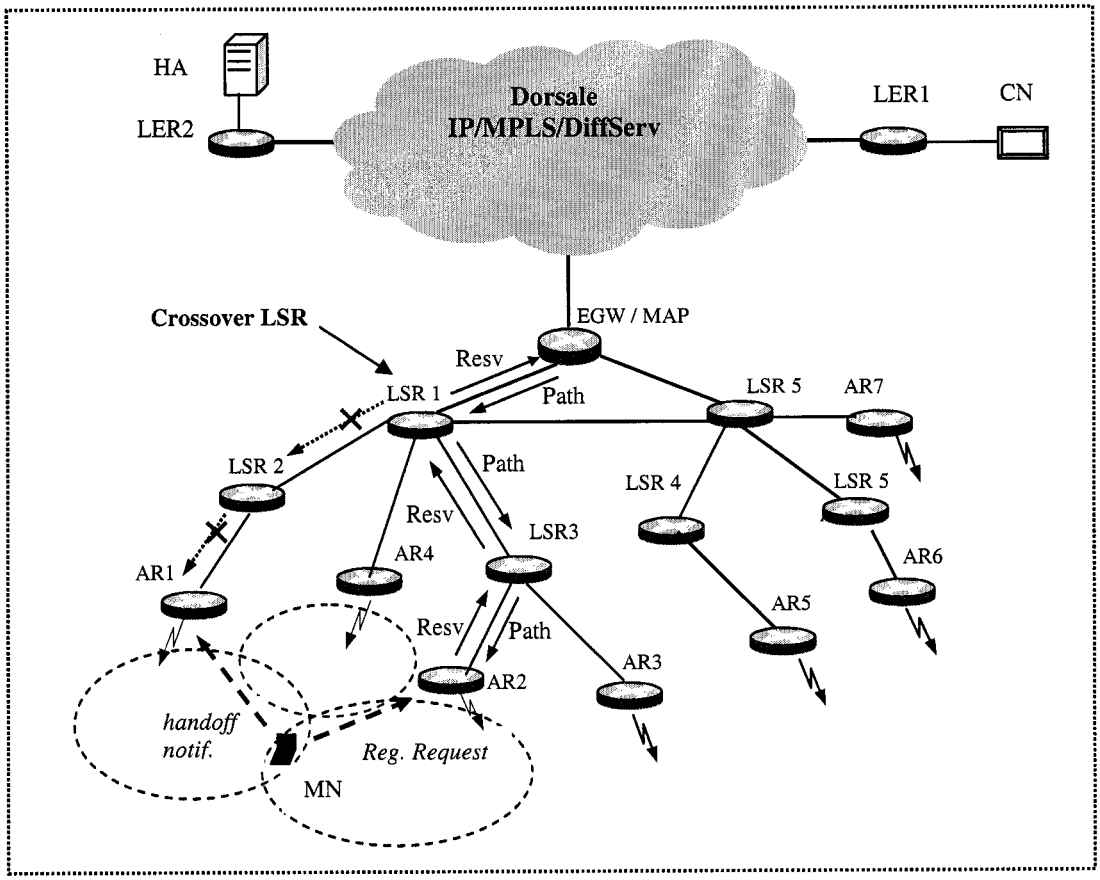

Figure 3.3 Relève intra-RAN

Selon cette approche, le MN contrôle en continu la qualité de la liaison radio avec son routeur d'accès courant, et ceci en mesurant l'intensité du signal reçu (S_{AR}). Aussi, il recueille les mesures de la qualité avec les routeurs d'accès voisins. Le MN analyse ces résultats et avise son routeur d'accès courant quand un handover va avoir lieu (par anticipation), au cas où l'intensité du signal reçu provenant du nouveau routeur d'accès dépasse un seuil prédéterminé appelé $S_{trigger}$, par un message *Handoff Notification* qui contient l'identité du prochain routeur d'accès.

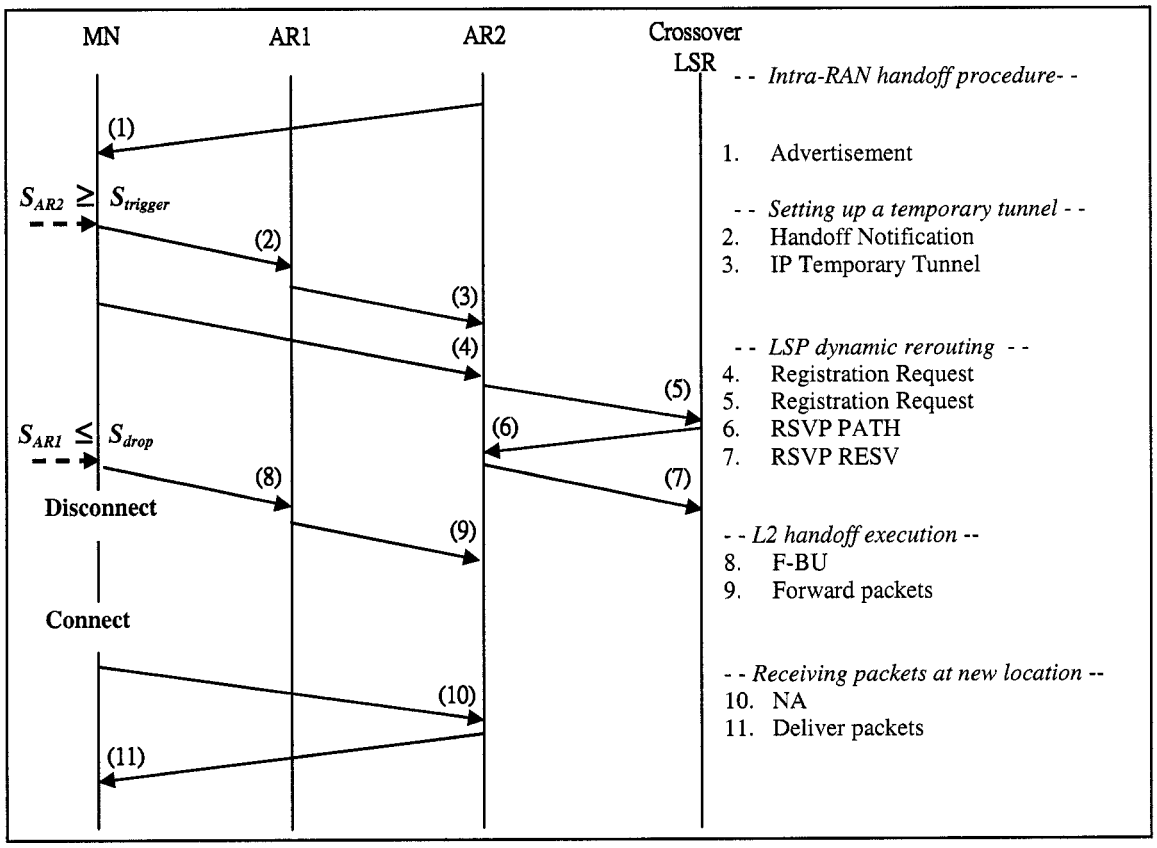

Figure 3.4 Messages de signalisation lors d'un handoff intra-domaine

Lorsque le routeur AR1 reçoit ce message, il établit un tunnel temporaire avec le nouveau routeur, AR2 dans ce cas, avec un intervalle de *timeout* Ta (si aucun paquet n'est transmis sur cette route pour une certaine période de temps, le tunnel sera annulé automatiquement). Cette route ne doit pas nécessairement être un chemin LSP associé

avec le chemin de CN vers le MN. Elle peut être une route IP traditionnelle, vu que les paquets provenant de CN sont déjà dépilés dans le routeur AR1 et ils sont prêts à être délivrés vers le MN.

Le MN, qui a encore un peu de temps avant de perdre sa connexion avec l'ancien routeur d'accès, procède de la façon suivante : 1) envoie un message d'enregistrement *Registration Request* vers le nouveau routeur d'accès AR2, qui l'achemine à son tour vers le MAP. Ce message contient la nouvelle adresse locale LCoA2 du mobile obtenue en concaténant l'identité de son interface physique avec le préfixe réseau du routeur AR2. 2) envoie un message *Fast-BindingUpdate* (*F-BU*) à l'ancien routeur d'accès juste avant son déplacement, lorsque l'intensité du signal provenant de celui-ci se dégrade sous un seuil prédéterminé appelé S_{drop} inférieur à $S_{trigger}$, pour lui indiquer son mouvement. Ce message déclenche l'acheminement des paquets vers le nouveau routeur d'accès.

À la réception du message *Registration Request*, chaque routeur intermédiaire vérifie sa table LFIB pour une entrée de MN, i.e. une entrée dont le champ FEC est associé à l'adresse mère de MN. Éventuellement, ce message atteint le routeur *upstream* LSR1, appelé *Crossover LSR* (au pire, il sera le MAP), qui contient une entrée pour le MN. Un *Crossover LSR* est défini comme le nœud bas le plus proche de MN et faisant l'intersection entre deux chemins LSP, le premier entre le MAP et l'ancien routeur d'accès AR1 et le deuxième entre le MAP et le nouveau routeur d'accès AR2. À la réception de ce message, le *crossover* LSR établit un nouveau chemin LSP vers le routeur AR2. Ensuite, il change sa table LFIB en reroutant l'ancien LSP dont le champ FEC est associé à l'adresse mère de MN en celui dont l'extrémité est le nouveau routeur AR2. Ensuite, le *crossover* LSR intercepte le prochain message PATH de mise à jour envoyé périodiquement par le MAP vers l'ancien routeur AR1, génère un message RESV qui contient le nouvel objet EXPLICIT_ROUTE OBJECT (ERO) identifiant le nouveau chemin LSP à partir de MAP vers le nouveau routeur d'accès AR2, et le retourne vers le MAP à la place de MN.

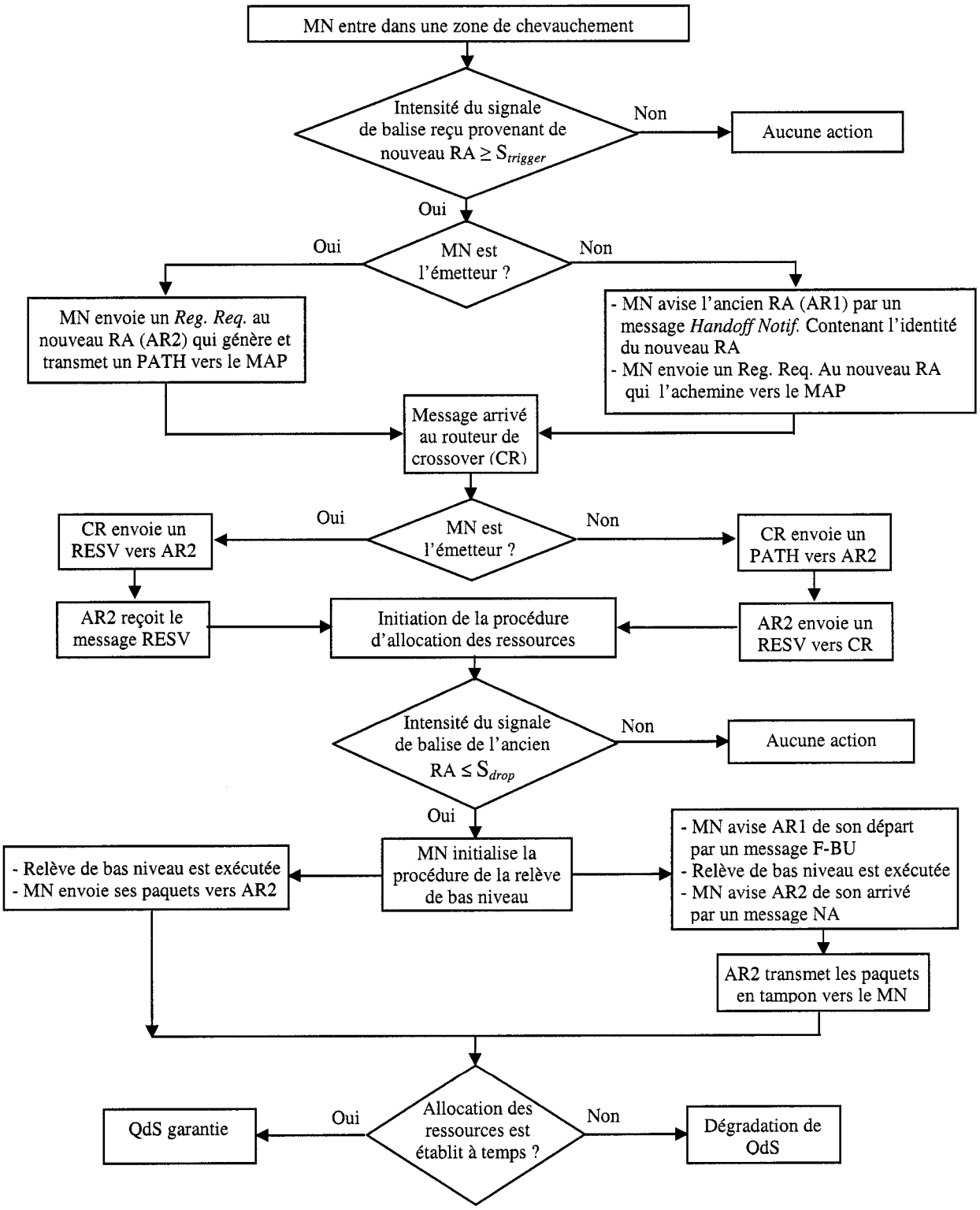

Figure 3.5 Organigramme de la procédure de la relève dans Q-HMIP

Par la suite, tous les messages PATH transmis périodiquement par le MAP, afin de mettre à jour les informations sur l'état de la session, contiennent le nouvel objet ERO et seront acheminés sur le nouveau chemin LSP vers le MN. En l'absence de messages de rafraîchissement d'état de lien, les nœuds qui se trouvent sur l'ancien LSP vers AR1 seront datés (*time-out*) et vont éventuellement enlever leurs entrées associées avec l'adresse mère de MN de leurs tables LFIB. Par la suite, tous les paquets qui suivent seront acheminés sur le nouveau chemin LSP.

Lors de son arrivée, le MN avertit le nouveau routeur AR2 par un message *Neighbor Advertise* (*NA*) pour indiquer sa présence. C'est alors que le routeur AR2 transmet les paquets mis en tampon et ceux provenant de CN vers le mobile. Le Tableau 3.2 présente les entrées enregistrées dans les tables LFIB de différents routeurs faisant partie du nouveau chemin LSP, ainsi que les entrées datées dans LSR2 et AR1.

Tableau 3.2 Entrées des tables LFIB après la relève

Node	Input I/F	Input Label	FEC	Output I/F	Output Label	Timer
LER1	--	--	FEC1	o-if-0	o-if-4	Tactive
GW/MAP	i-if-0	i-if-4	FEC1	o-if-0	o-if-3	Tactive
LSR1 (*crossover*)	i-if-0	i-if-3	FEC1	o-if-0	o-if-2	Tactive
LSR2	--	--	--	--	--	Tout
AR1	--	--	--	--	--	Tout
LSR3	i-if-0	i-if-2	FEC1	o-if-0	o-if-1	Tactive
AR2	i-if-0	i-if-1	FEC1	--	--	Tactive

3.3.2 Relève inter-RAN (macro-mobilité)

Lors d'un déplacement inter-RAN, le mobile obtient une nouvelle adresse régionale RCoA2 associée au MAP du nouveau réseau d'accès. Dans ce cas, le MN doit aviser son agent mère et ses correspondants avec lesquels il est en communication de sa

nouvelle adresse régionale, et ceci par des messages *Binding Update*. Aussi, il doit aviser l'ancien MAP de son déplacement, afin d'acheminer les paquets en transit vers sa nouvelle localisation. Dans le cas où les deux réseaux d'accès sont connectés à un domaine d'ingénierie de trafic, un changement de chemins LSP dans ce domaine va avoir lieu. Sinon, les paquets envoyés par le CN seront acheminés sur la couche IP avant d'établir un nouveau chemin LSP vers le MN, suivant les procédures déjà décrites à la section 3.2.2, si nécessaire.

La Figure 3.6 présente le nouveau chemin LSP entre le CN et le nouveau routeur d'accès lors d'un déplacement de RAN-1 vers RAN-2.

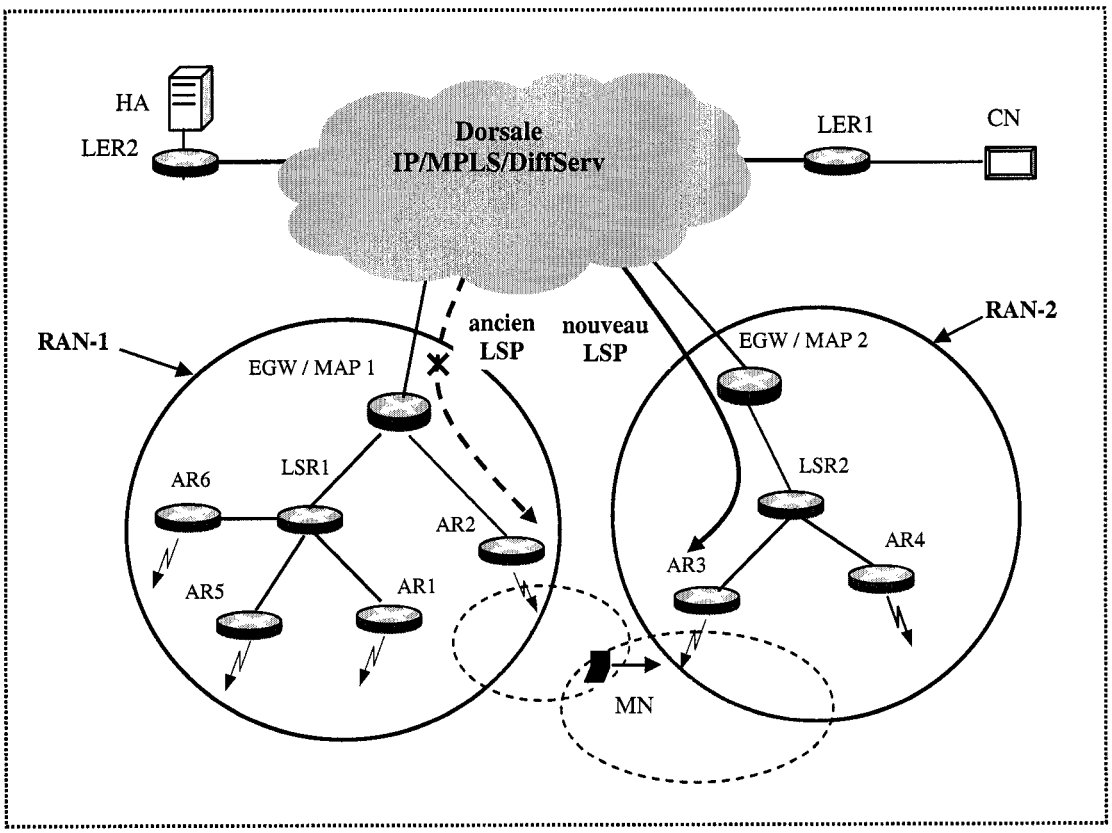

Figure 3.6 Relève inter-RAN

3.4 Analyse qualitative du modèle Q-HMIP

Dans ce qui suit, nous présentons une analyse qualitative de notre approche de gestion de la micro-mobilité, et nous la comparons avec d'autres propositions notamment, le protocole HMIPv6. Cette comparaison est basée sur différents critères dont la gestion du *handover*, le support de la qualité de service, l'évolutivité (*scalability*) et la fiabilité du système fournie par le support de l'ingénierie de trafic dans MPLS.

3.4.1 Analyse générale du handover

Dans cette section, nous analysons et comparons le mécanisme du handover présenté dans le modèle Q-HMIP avec d'autres mécanismes de gestion du *handover* IP, notamment ceux des protocoles MIPv6 et HMIPv6. Ces mécanismes peuvent être évalués selon différents critères, notamment :

- le délai de transfert: temps nécessaire pour qu'un mobile reçoive des paquets à sa nouvelle localisation;
- le nombre de paquets perdus pendant un *handover* ;
- la gigue: variation du délai de transfert des paquets.

Pour cette analyse, nous utiliserons le modèle de réseau simplifié présenté à la Figure 3.7.

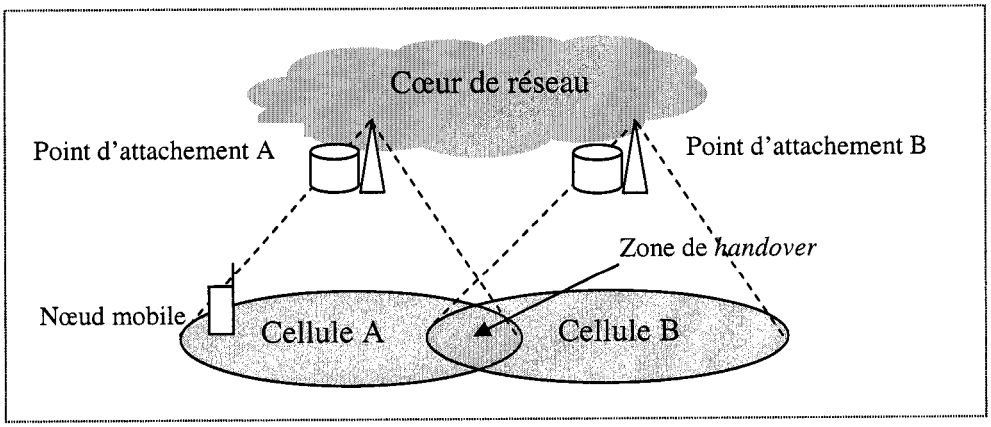

Figure 3.7 Interaction entre un terminal mobile et le cœur de réseau

Ainsi, un terminal mobile est connecté à un point d'attachement A relié à un réseau filaire. La portée du point d'attachement est symbolisée par la cellule A. Afin de simplifier notre analyse, nous supposerons qu'une cellule IP n'est constituée que d'une cellule de bas niveau, que le point d'attachement de bas niveau et le routeur d'accès constituent une seule entité.

Le déplacement du terminal mobile entraîne la déconnexion du point d'attachement A, et la connexion au point B, produisant ce qu'on appelle la relève (*handover*). Le délai Δ du handover de bas niveau est susceptible de provoquer des pertes de paquets et d'influencer les délais de transmission des autres paquets. Durant cette période, aucun paquet ne peut être transmis vers ou depuis le terminal mobile.

Le délai D de déconnexion IP du terminal mobile désigne le temps d'indisponibilité du mobile au niveau IP provoqué par le *handover*. Cette indisponibilité débute au moment précis où le mobile perd sa connectivité avec son ancien routeur d'accès, jusqu'au moment où il est capable d'envoyer et de recevoir les paquets IP à travers son nouveau routeur d'accès. La quantité de paquets IP perdus, provoqués par le handover IP, est proportionnelle au délai D. Ce délai est composé de deux grandes périodes τ et Δ, comme l'illustre la Figure 3.8. La période τ correspond au délai nécessaire de configuration des paramètres IP du mobile. L'enregistrement d'une adresse IP est un exemple typique de cette configuration.

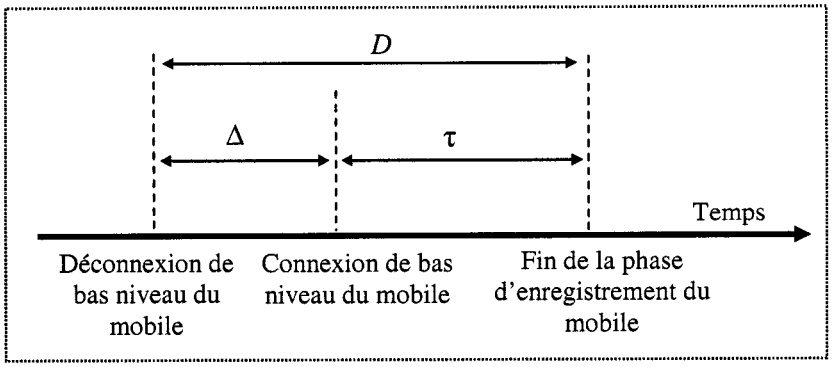

Figure 3.8 Délai *D* de déconnexion IP du mobile

Cas de MIPv6

La Figure 3.9 montre un diagramme temporel des événements intervenant lors d'un *handover* IP pour Mobile IPv6. Dans ce diagramme, Δ représente le délai du *handover* de bas niveau, Φ_{MIPv6} est le délai nécessaire au mobile pour obtenir une nouvelle adresse temporaire, Ω_{MIPv6} est le délai nécessaire pour la phase d'enregistrement de cette adresse auprès de l'agent mère. La somme de Φ_{MIPv6} et de Ω_{MIPv6} est la valeur τ définie précédemment.

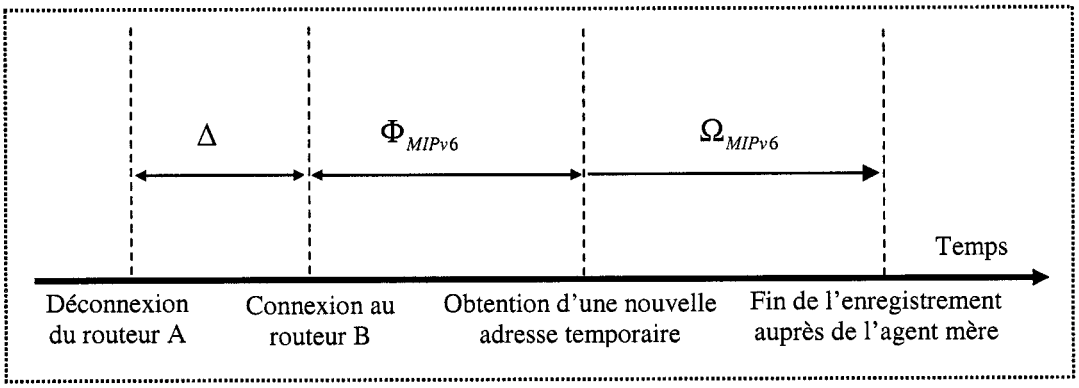

Figure 3.9 Diagramme temporel du *handover* pour Mobile IPv6

Le délai global de déconnexion du mobile est :

$$D_{\text{MIP6}} = \Delta + \Phi_{MIP6} + \Omega_{MIP6} \tag{3.1}$$

Le nombre de paquets perdus N_{MIP6} lors du *handover* est :

$$N_{MIP6} = R.D_{\text{MIP6}} = R.(\Delta + \Phi_{MIP6} + \Omega_{MIP6}) \tag{3.2}$$

où R désigne le débit moyen de transmission entre le correspondant et le mobile.

Dans MIPv6, le mobile enregistre sa nouvelle adresse temporaire auprès de son agent mère, mais aussi directement auprès de l'ensemble de ses correspondants. Ainsi, le délai de transfert de paquets après le handover devient :

$$T_{MIP6} = T_{CB} + T_{radio} \tag{3.3}$$

où T_{CB} désigne le délai de transfert entre le correspondant et le routeur B.

La gigue induite par le handover sera :

$$J_{MIP6} = |T_{CA} - T_{CB}| + J_{radio} \tag{3.4}$$

où T_{CA} désigne le délai de transfert entre l'agent mère et le routeur d'accès A.

Cas de Mobile IPv6 Hiérarchique

Comme nous l'avons déjà décrit, HMIPv6 est basé sur l'introduction d'une architecture hiérarchique d'agents de mobilité dans le réseau. Chaque mouvement du mobile au sein d'une région entraîne un enregistrement local de l'adresse temporaire auprès de l'agent de mobilité local. L'agent de mobilité étant vraisemblablement plus proche que le correspondant, nous déduisons que le délai d'enregistrement Ω_{HMIP} est inférieur à celui de Mobile IP v6.

Ainsi,

$$\Omega_{HMIP} < \Omega_{MIP6} \tag{3.5}$$

Le délai nécessaire pour l'obtention d'une nouvelle adresse temporaire étant identique à mobile IPv6, le délai de déconnexion sera :

$$D_{HMIP} = \Delta + \Phi_{MIP6} + \Omega_{HMIP} \tag{3.6}$$

Le nombre de paquets perdus pendant le handover devient :

$$N_{HMIP} = R.D_{HMIP} = R.(\Delta + \Phi_{MIP6} + \Omega_{HMIP}) \tag{3.7}$$

De (3.2), (3.5) et (3.7), nous déduisons que :

$$N_{HMIP} < N_{MIP6}$$

Cependant, l'introduction des agents de mobilité MA_i et des tunnels successifs augmente le délai de transfert des paquets IP :

$$T_{HMIP} = T_{CN,MA1} + \sum T_{MAi,MAi+1} + T_{MAn,B} + T_{radio} \tag{3.8}$$

avec :

$T_{MAi,MAi+1}$: le délai de transfert entre les agents de mobilité MA_i et MA_{i+1}

$T_{CN,MA1}$: le délai entre le correspondant et l'agent MA_1

$T_{MAn,B}$: le délai entre l'agent de mobilité MA_n et le routeur B

Or,

$$T_{CN,MA1} + \sum T_{MAi,MAi+1} + T_{MAn,B} \geq T_{CB}$$

Nous déduisons que :

$$T_{HMIP} > T_{MIP6}$$

La gigue induite par le *handover* sera :

$$J_{HMIP} = | T_{MAn,A} - T_{MAn,B} | + J_{radio} \tag{3.9}$$

où $T_{MAn,A}$ désigne le délai de transfert entre l'agent MA_n et le routeur d'accès A.

Les agents de mobilité étant proches des routeurs d'accès, et si A et B appartiennent à un même domaine de gestion, il est fortement probable que la gigue de Mobile IPv6 hiérarchique soit inférieure à celle de Mobile IPv6. Si A et B n'appartiennent pas au même domaine de gestion, il n'y a pas de comparaison possible. Cependant, si l'on suppose que la gigue est prépondérante, la gigue globale de mobile IP hiérarchique, de mobile IPv4 et de mobile IPv6 serait similaire :

$$J_{HMIP} \cong J_{MIP6} \cong J_{radio}$$

Cas de Q-HMIP

Comme on l'a déjà décrit, le mécanisme d'anticipation du mouvement du mobile permet de réduire le délai Φ_{Q-HMIP} nécessaire à l'obtention d'une nouvelle adresse temporaire. Le délai d'enregistrement étant identique à celui de HMIPv6, le délai de déconnexion devient :

$$D_{Q-HMIP} = \Delta + \Phi_{Q-HMIP} + \Omega_{HMIP} \tag{3.10}$$

avec $\Phi_{Q-HMIP} < \Phi_{HMIP}$

Ainsi, après la déconnexion, tous les paquets reçus par le routeur A et destinés au mobile seront transmis au routeur B par l'intermédiaire du tunnel. Si le temps de déconnexion de bas niveau est inférieur au délai de traversée du tunnel, tous les paquets redirigés par le routeur A arriveront au mobile après sa liaison avec le routeur B. À cette condition, aucun paquet n'est perdu. Dans le cas contraire, un certain nombre de paquets arriveront au routeur B avant l'établissement de la nouvelle connexion et seront perdus. Dans tous les cas, le nombre de paquet perdus a la propriété suivante :

$$N_{Q-HMIP} < R.\Delta \tag{3.11}$$

Puisque le routeur de *crossover* est un nœud intermédiaire entre la passerelle de frontière (EGW) et le routeur d'accès courant, l'acheminement du message d'enregistrement *Registration Request* requiert moins de temps pour atteindre le routeur de *crossover* que le MAP.

La gigue induite par le *handover* dans Q-HMIP est similaire à celle dans HMIPv6 :

$$J_{Q-HMIP} = |T_{MAn,A} - T_{MAn,B}| + J_{radio}$$

Cependant, l'agent MA_n dans notre approche n'est que le routeur de *crossover*, et par la suite la gigue induite par le *handover* sera :

$$J_{Q-HMIP} = |T_{MAcrover,A} - T_{MAcrover,B}| + J_{radio} \tag{3.12}$$

Le routeur de *crossover* étant plus proche des routeurs d'accès A et B que le MAP, il est fortement probable que la gigue dans Q-HMIP serait inférieure à celle de Mobile IPv6 hiérarchique. Ainsi,

$$J_{Q-HMIP} < J_{HMIP}$$

Dans le cas où le routeur de *crossover* est le EGW, la gigue sera équivalente à celle de HMIPv6.

Le Tableau 3.3 présente un récapitulatif des performances de *handover* basées sur IP.

Tableau 3.3 Récapitulatif des performances de *handover* basées sur IP

	Performances de *handover*	Comparaison
Mobile IPv6	$D_{MIP6} = \Delta + \Phi_{MIP6} + \Omega_{MIP6}$ $N_{MIP6} = R.D_{MIP6}$ $T_{MIP6} = T_{CB} + T_{radio}$ $J_{MIP6} = \lvert T_{CA} - T_{CB} \rvert + J_{radio}$	
Mobile IPv6 Hiérarchique	$D_{HMIP} = \Delta + \Phi_{MIP6} + \Omega_{HMIP}$ $N_{HMIP} = R.D_{HMIP}$ $T_{HMIP} = T_{CN,MA1} + \sum T_{MAi,MAi+1} + T_{MAn,B} + T_{radio}$ $J_{HMIP} = \lvert T_{MAn,A} - T_{MAn,B} \rvert + J_{radio}$	$D_{HMIP} < D_{MIP6}$ $N_{HMIP} < N_{MIP6}$ $T_{HMIP} > T_{MIP6}$ $J_{HMIP} \cong J_{MIP6}$ (Intra-RAN)
Q-HMIP	$D_{Q-HMIP} = \Delta + \Phi_{Q-HMIP} + \Omega_{HMIP}$ $N_{Q-HMIP} < R.\Delta$ $T_{Q-HMIP} = T_{CN,MA1} + \sum T_{MAi,MAi+1} + T_{MAn,B} + T_{radio}$ $J_{Q-HMIP} = \lvert T_{MAcrover,A} - T_{MAcrover,B} \rvert + J_{radio}$	$N_{Q-HMIP} < N_{MIP6}$ $T_{Q-HMIP} = T_{HMIP}$ $J_{Q-HMIP} < J_{HMIP}$ $(MA_n = MA_{crover})$

3.4.2 Qualité de Service

Comme on l'a signalé précédemment, l'architecture DiffServ dans un réseau IP est capable de fournir une solution de QdS globale résistant au facteur d'échelle. Cependant, elle est conçue pour une architecture de QdS statique ou faiblement

dynamique. Donc, elle n'est pas adaptée aux environnements fortement mobiles dans lesquels les terminaux peuvent changer non seulement leur points d'accès pendant une session de communication, mais encore leurs besoins en terme de QdS.

Le protocole MPLS introduit la notion de *jonction de trafic* (*trafic trunk*) qui n'est autre qu'une agrégation de flux de trafic d'une même classe, flux qui sont placés dans un même chemin LSP. Ceci permet aux différents types de flux de recevoir des acheminements et des traitements distincts qui tiennent compte de différents niveaux de QdS. Ainsi, l'intégration de mécanismes de mobilité IP avec le protocole de signalisation RSVP-TE dans un réseau IP/MPLS/DiffServ a montré qu'il est possible d'établir des réservations dynamiques pour des chemins à commutation d'étiquettes LSP véhiculant un agrégat de flots plutôt que pour des micro flots séparés. Ceci permet en conséquence de fournir la QdS minimale pour des nouveaux services multimédias et applications en temps réel.

3.4.3 Évolutivité

Un des avantages du modèle Q-HMIP est la possibilité de rérouter le trafic d'un chemin LSP à un autre de façon dynamique, permettant ainsi d'améliorer l'évolutivité du réseau d'accès en augmentant la robustesse et la flexibilité du système. En effet, dans HMIPv6, le MAP qui est la machine assumant les fonctions de passerelle est également la plus chargée du réseau. Le MAP doit traiter *tous* les messages de mise à jour et maintenir une entrée pour *tous* les mobiles présents dans le réseau. Un tel système, proche d'un *bottleneck*, n'est évidemment pas très flexible. Dans le modèle Q-HMIP, cette tâche est distribuée sur tous les routeurs LSR du domaine, ce qui augmente par conséquent la robustesse du système.

3.4.4 Ingénierie de trafic

L'ingénierie de trafic consiste à définir les meilleurs chemins possibles pour des flux identifiés. Généralement, la plupart des gros réseaux IP, en particulier ceux des

opérateurs, disposent de liens de secours en cas de panne. Toutefois, il est assez difficile d'obtenir une répartition du trafic sur ces liens qui ne sont traditionnellement pas utilisés, car n'étant pas sélectionnés comme chemins optimaux par l'IGP. Avec la technologie MPLS, l'ingénierie de trafic assure un meilleur emploi des liaisons, puisqu'elle permet l'établissement des tunnels LSP à travers le réseau MPLS, indépendamment de l'IGP, ce qui assure l'efficacité et la fiabilité du fonctionnement du réseau et en même temps une utilisation optimale des ressources disponibles.

CHAPITRE 4

ÉVALUATION DE PERFORMANCE DU MODÈLE PROPOSÉ

Afin d'évaluer les performances du modèle Q-HMIP proposé pour la gestion de la micro-mobilité, un environnement de simulation basé sur le simulateur NS-2 a été conçu. Ainsi, nous commençons par une brève introduction du simulateur NS-2. Ensuite, nous exposons les principes de conception et l'architecture interne du modèle Q-HMIP implémenté. Nous présentons par la suite l'implémentation des indices de performance les plus pertinents qui serviront à produire les différents résultats de simulation sous forme de statistiques. Nous exposons ensuite les résultats des scénarii simulés accompagnés d'interprétations détaillées.

4.1 Choix du simulateur réseau NS-2 et modules utilisés

Dans le chapitre précédent, nous avons présenté une analyse qualitative générale du mécanisme de handover dans le modèle proposé, basée sur une étude analytique simple. Cependant, cette analyse ne peut pas fournir une quantification réaliste du gain de performance. Pour sa part, la simulation est une méthode fiable pour étudier un système donné avec une grande précision, car on peut prendre en compte concrètement les détails du système réel autant que l'on veut. Ainsi, la simulation est l'approche la plus adaptée à notre étude de performance. Pour cela, nous avons besoin d'un simulateur qui supporte le modèle proposé, notamment la signalisation et la transmission de messages de contrôle, et qui fournit une granularité au niveau du paquet. Ce niveau de granularité est requis afin de mesurer certaines statistiques, notamment la perte de paquets, le délai et la gigue, avec un minimum de certitude. En se basant sur les préalables précédents, nous avons choisi d'utiliser un simulateur à événements discrets. Notre choix s'est porté sur le simulateur NS-2 (The Network Simulator) [NS-2], qui a été développé au Laboratoire National de Lawrence Berkeley (*LBNL*) et qui fait

maintenant partie du projet *VINT* (*Virtual InterNetwork Testbed*) [VINT], dirigé par l'Université de Californie du sud (*USC*) et financé par le *DARPA* en collaboration avec *Xerox PARC*, *LBNL* et *UCB* (*University of California, Berkeley*).

L'architecture réseau de NS-2 est fortement basée sur le modèle des couches OSI. Il est développé en C++ et en Otcl (MIT Object Tcl, extension to Tcl/Tk for object-oriented programming). Le package inclut une hiérarchie de classes compilée d'objets écrits en C++ et une hiérarchie de classes interprétée d'objets écrits en OTcl. Ces deux hiérarchies sont étroitement liées; quand l'utilisateur crée un nouvel objet par l'interpréteur OTcl, un objet correspondant appelé objet reflet est aussi créé dans la hiérarchie compilée. On dit que ces objets sont des « objets fendus ». Bien entendu, les objets peuvent être accédés aussi bien en OTcl qu'en C++ grâce à la mise en place de procédures d'appel entre Otcl et C++. Le langage OTcl est un langage interprété qui ne demande pas de compilation. Il est principalement utilisé pour concaténer des objets, accéder aux objets à partir de l'interpréteur et configurer des simulations (début et arrêt des évènements, perte réseau, rassemblement de statistiques). D'un autre côté, C++ est utilisé pour créer les classes de base et pour traiter un grand nombre de données (tel que calcul des tables de routage, mouvement des mobiles, et bien d'autres.). NS-2 est bien adapté pour simuler la circulation de paquets dans des réseaux commutés. Il est principalement utilisé pour tester des algorithmes de gestion de files d'attente, des contrôles de congestion, des protocoles de transport, le *multicast* et la mobilité. Il est modulaire et gratuit.

Dans le cadre de notre travail, l'architecture du modèle Q-HMIP est modélisée en totalité en englobant un certain nombre de modules fournis avec le simulateur NS-2 :

- *Module HMIPv6 with Fast Handover* [Hsieh] developé par Robert Hsieh, est une extension de l'implémentation de Mobile IP dans NS. Cette dernière a été conçue à l'origine par les chercheurs de l'université Carnegie Mellon de Pittsburgh (CMU) en vue de simuler des réseaux ad hoc, ensuite elle a été modifiée pour supporter l'implémentation de Sun Microsystem de Mobile IP (Perkins et al., 1996). Comme

l'objectif était de simuler des réseaux entièrement mobiles, il a fallu mettre en place des protocoles de routage. Actuellement, il y a quatre protocoles de routage mis en œuvre dans NS-2 : DSDV (*Destination Sequenced Distance Vector Protocol*), DSR (*Dynamic Source Routing Protocol*), TORA (*Temporally-Ordered Routing Algorithm routing protocol*) et AODV (*Ad-hoc On-Demand Distance Vector Protocol*). Une autre amélioration de cette implémentation a été apportée par l'introduction de l'agent NOAH (*Non-Ad-Hoc Routing*) implémentée par Jörg Widmer du laboratoire AT&T ACIRI à Berkeley [Widmer]. NOAH est un agent de routage sans fil qui supporte uniquement la communication entre les points d'accès et les nœuds mobiles (en contraste avec les agents de routage DSDV, DSR, ..), dont le routage multi-sauts entre les nœuds mobiles n'est pas désiré. La Figure 4.1 montre la structure du nœud MAP de l'implémentation du protocole HMIPv6 dans NS. Une description plus détaillée de ses composants sera abordée plus loin (section 4.2) lors de la description du modèle Q-HMIP.

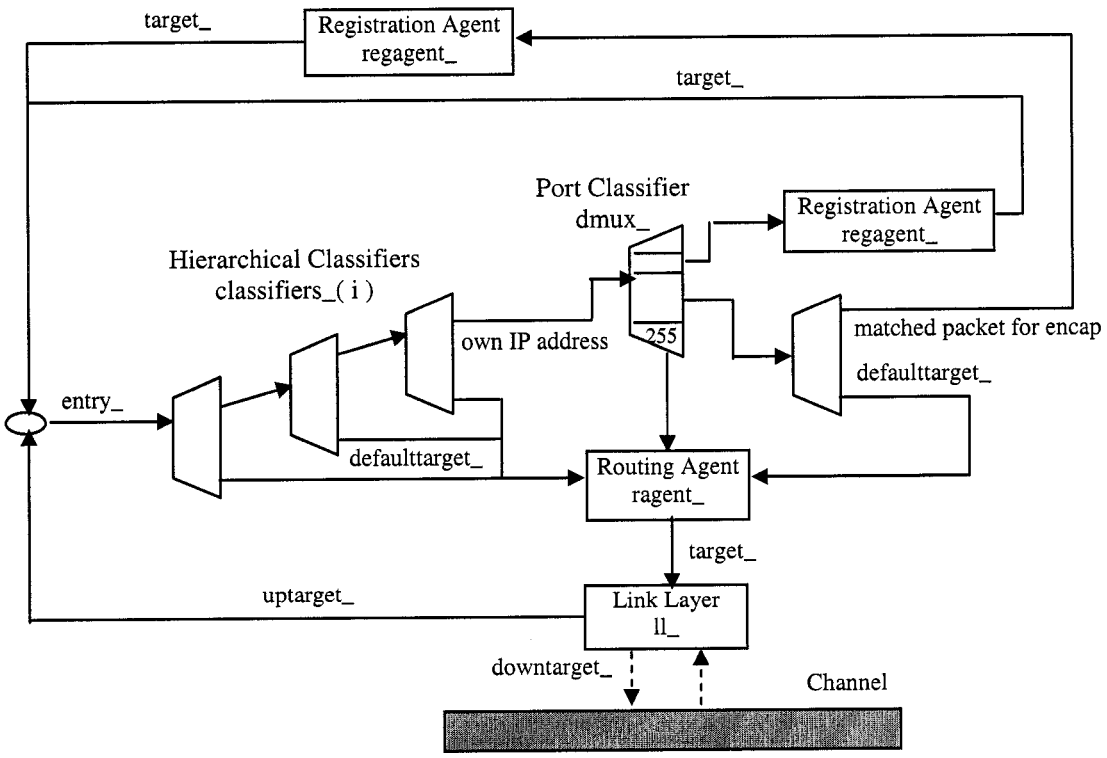

Figure 4.1 Structure du nœud MAP dans l'implémentation NS de HMIPv6

- *Module MPLS Network Simulator* [MNS], développé par Gaeil Ahn, est l'implémentation du protocole MPLS dans NS. Pour le support de DiffServ, une des extensions disponibles dans NS [Murphy] a été intégrée dans MNS. La Figure 4.2 présente l'architecture et les différentes composantes d'un nœud MPLS dans NS-2.

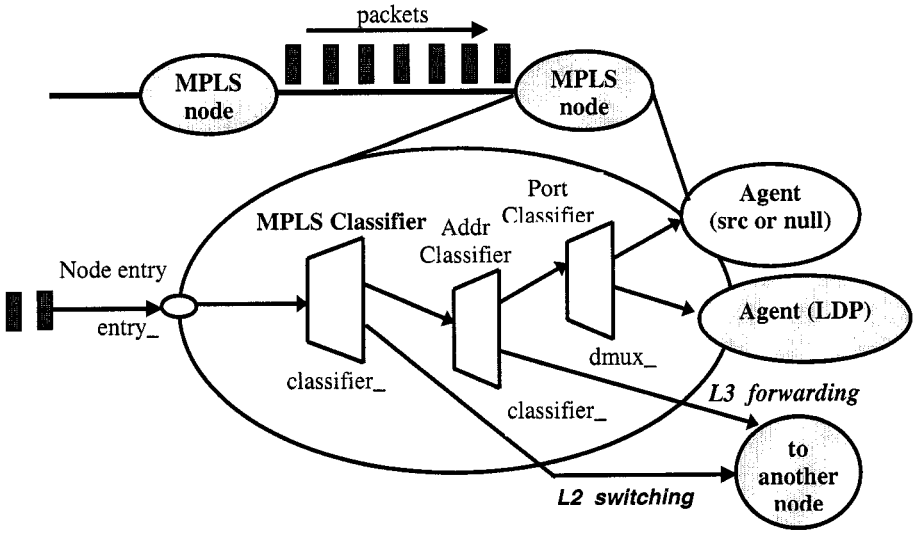

Figure 4.2 Architecture du nœud MPLS dans MNS

Essentiellement, un nœud est composé des agents et des classificateurs. Le rôle d'un agent est de générer et réceptionner des paquets suivant un protocole de transport (TCP, UDP, RTP...). Le classificateur est la partie du nœud qui traite chaque segment des paquets reçus. Il en existe donc plusieurs, chacun étant spécifique au champ examiné. Ainsi, lors de la réception d'un paquet, un nœud MPLS fonctionne de la façon suivante :

- *MPLS Classifier* vérifie si le paquet reçu est associé à une étiquette ou non. Si une étiquette est présente, le paquet sera commuté selon son étiquette (*L2 Label switching*) par le *MPLS Classifier* vers le prochain nœud. Si le paquet reçu ne contient aucune étiquette mais son chemin LSP est déjà signalé, une étiquette lui sera assignée; ensuite le paquet sera commuté selon son étiquette comme auparavant. Sinon, le *MPLS Classifier* achemine le paquet vers le classificateur d'adresse;

- *Addr Classifier* achemine le paquet vers sa destination sur la couche IP (*L3 forwarding*);
- Si le prochain saut du paquet est le nœud MPLS lui-même, le paquet sera envoyé vers le *Port Classifier*, qui l'achemine vers l'agent correspondant.

Pour le routage des paquets étiquetés, trois tables sont définies dans MNS :

- *Partial Forwarding Table* (PFT) – qui contient une partie des entrées de la table d'acheminement notamment, les entrées FEC, PHB et LIBptr;
- *Label Information Base* (LIB) – qui contient des informations pour l'établissement des chemins LSP;
- *Explicite Routing Information Base* (ERB) - qui contient des informations pour l'établissement des chemins LSP explicite, tels que l'identificateur du LSP (LSPID) et l'identificateur du service (ServiceID).

La structure des tables MPLS tel qu'implémentées dans MNS et l'interaction entre celles-ci est présentée à la Figure 4.3.

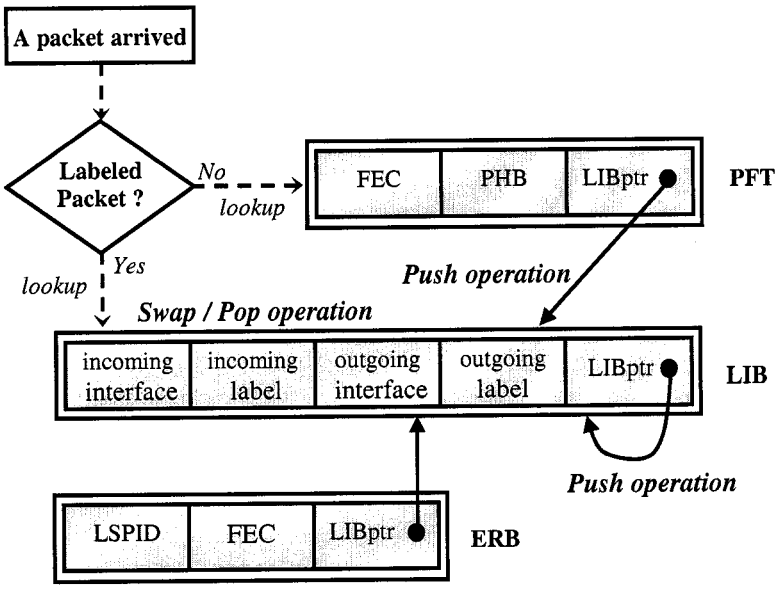

Figure 4.3 Structure de tables MPLS dans MNS

- *Module RSVP-TE*, développé par René Böringer [Böringer], est utilisé principalement comme un protocole de signalisation pour l'implémentation existante du protocole MPLS (MNS). La Figure 4.4 illustre les interfaces implémentées de l'agent RSVP-TE (en gras) et ajoutées au modèle MNS :

- *Protocole de routage* – maintient une table de routage utilisée pour déterminer le saut suivant à prendre pour joindre une certaine destination;
- *Service Classifier* – conçu pour le support de plusieurs types de trafic. Ainsi, lors de la réception d'un paquet, le *service classifier* consulte la table *ERB* pour vérifier le champ *ServiceID* associé au paquet afin de l'enfiler dans une des files d'attente selon le mécanisme d'ordonnancement WRR (*Weighted Round Robin*), appelé aussi CBQ (*Class-based Queing*), déjà existant dans NS-2;

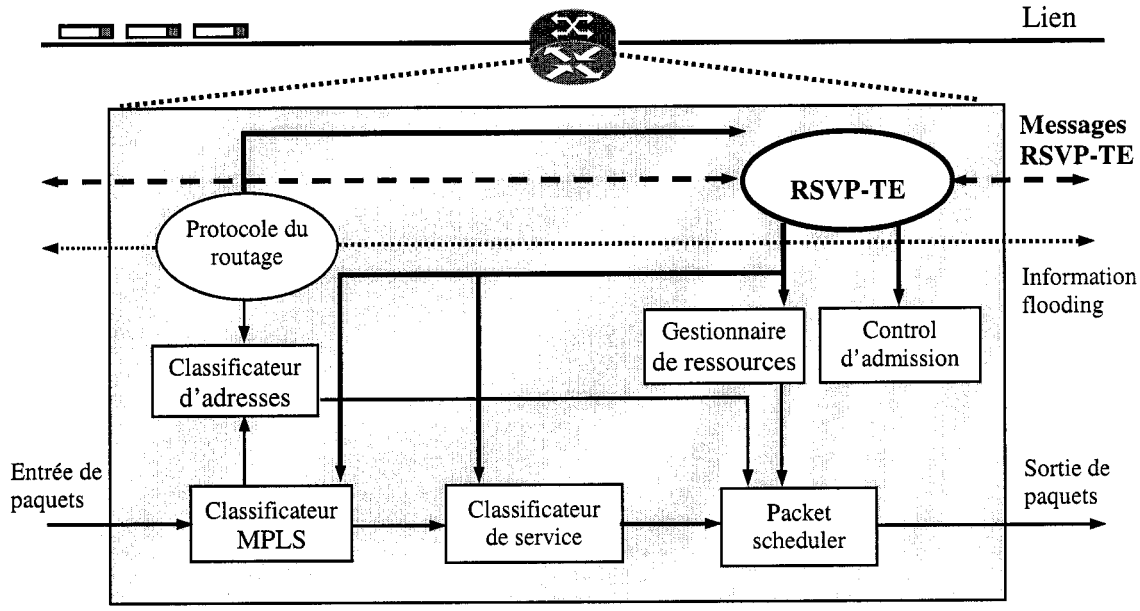

Figure 4.4 Modules MNS et interfaces RSVP-TE ajoutées

- *Packet Schedular*[5] – implémenté au niveau des liens et qui gère un ou plusieurs files;

[5] Dans les réseaux réels, le *packet scheduler* est implémenté au niveau des nœuds et non pas des liens, cas de MNS.

- *Admission Control* – vérifie s'il y a suffisamment de ressources disponibles pour assurer la QdS demandée à partir d'informations récoltées par RSVP-TE;
- *Ressource Manager* – crée et efface des files sur demande et gère aussi les tables d'informations des ressources.

Le mécanisme WRR prend en considération les classes et le partage de la bande passante disponible sur chaque lien, ce qui lui permet d'allouer différentes bandes passantes selon les exigences de chaque classe du trafic. Ainsi, le modèle CBQ dans MNS permet la création de trois niveaux de classes nommés BT pour *Best Effort Traffic Service*, RT pour *Real Time Traffic Service* et ST pour *Signalling Traffic Service*, comme illustré à la Figure 4.5. À son tour, la classe BT peut se diviser en *high priority BT* (HBT) et *simple BT* (SBT).

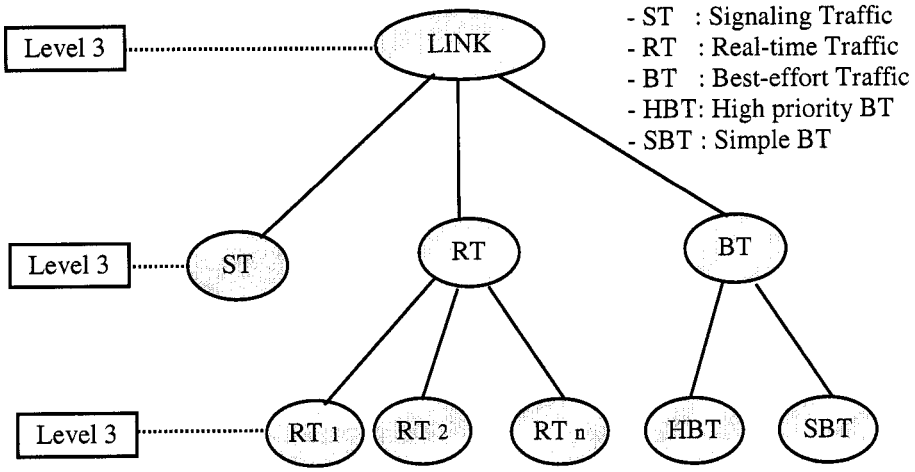

Figure 4.5 Mécanisme d'ordonnancement CBQ/ERR

À l'origine, le module RSVP-TE est basé sur l'extension RSVP/ns développée par Marc Greis [Greis], qui est l'implémentation du protocole RSVP dans NS. Cependant, il a fallu changer ou ajouter plusieurs messages et objets à l'extension RSVP/ns pour que le module RSVP-TE soit conforme au standard défini par Awduche et al. (2002). En fait, à l'opposé de RSVP qui est un protocole de signalisation de bout-

en-bout entre une paire d'hôtes et qui réserve des ressources pour des flux singuliers, RSVP-TE signale entre différents routeurs MPLS et réserve des ressources pour des LSP véhiculant un agrégat de flots plutôt que pour des micro flots séparés. Aussi, le concept de réservation dans RSVP/ns est basé sur le service IntServ qui implémente des algorithmes de contrôle d'admission et le mécanisme d'ordonnancement de partage pondéré équitable WFQ (ou WF^2Q). Le module RSVP-TE, à son tour, remplace le mécanisme WFQ par celui de CBQ.

Un aperçu de tous les objets implémentés dans RSVP-TE est présenté au Tableau 4.1.

Tableau 4.1 Objets RSVP/RSVP-TE implémentés

objet	RSVP	implémenté (RSVP/ns)	RSVP-TE	changé/ implémenté
SESSION	*x*	*x*	*x*	*x*
RSVP HOP	*x*	*x*	*x*	o
TIME VALUES	*x*	*x*	*x*	o
ERROR SPEC	*x*	*x*	*x*	o
STYLE	*x*	*x*	*x*	o
FLOW SPEC	*x*	*x*	*x*	o
FILTER SPEC	*x*	*x*	*x*	*x*
SENDER TEMPLATE	*x*	*x*	*x*	*x*
SENDER TSPEC	*x*	*x*	*x*	o
RESV CONFIRM	*x*	*x*	*x*	o
LABEL	o	n	*x*	*x*
LABEL REQUEST	o	n	*x*	*x*
EXPLICIT ROUTE	o	n	*x*	*x*
RECORD ROUTE	o	n	*x*	*x*
SESSION ATTRIBUTE	o	n	*x*	*x*
HELLO REQUEST	*x*	n	*x*	n
HELLO ACK	*x*	n	*x*	n

La première colonne définit si un objet est considéré ou non par le standard RSVP ou par une de ses extensions (*x* – défini dans le standard, *o* – non défini). C'est le cas de messages *HELLO* à titre d'exemple. La seconde colonne compare le standard avec l'implémentation de RSVP dans NS (*x* – est implémenté, *n* – non défini). Les

troisième et quatrième colonnes présentent la comparaison entre le standard RSVP-TE et son implémentation dans NS (cas de RSVP-TE implémenté : *x* – ajouté ou l'ancien objet a été modifié, *o* – pas de changement, *n* – non implémenté).

4.2 Implémentation du modèle Q-HMIP

Le module MPLS dans NS supporte l'adressage plat seulement. L'adressage hiérarchique est utilisé présentement dans les réseaux IP afin de créer des domaines administratifs distincts, un préalable nécessaire pour la simulation du module HMIPv6. Pour cela, il a fallu modifier le module MPLS dans ce travail, en ajoutant une hiérarchie des classificateurs d'adresse (*Address Classifiers*). D'autre part, afin de supporter la gestion de la micro-mobilté telle que décrite à la section 3.2.6, un nouveau module nommé *MMAgent* a été conçu et ajouté à chaque nœud MPLS. Les agents de mobilité *MAPAgent* et *MIPBSAgent* déjà implémentés et existants dans les nœuds EGW et BS sont modifiés à leur tour, pour qu'il puissent communiquer avec l'agent *MMAgent*. La Figure 4.5 montre les différents composants de la nouvelle structure d'une station de base (BS) dans le modèle Q-HMIP, qui est un nœud hybride entre un nœud hiérarchique et un nœud mobile:

- *module MIPBSAgent* contient un agent d'enregistrement (*regagent_*) qui envoie les "beacons", effectue l'encapsulation et la décapsulation des paquets et répond aux messages de sollicitation envoyés par les nœuds mobiles;
- *module MMAgent* est implémenté dans tous les nœuds MPLS. Ces agents communiquent directement entre eux et avec les agents *MAPAgent* et *MIPBSAgent*. Dans chaque nœud MPLS, l'agent *MMAgent* communique avec le *MPLS Classifier* pour accéder aux tables PFT/LIB;
- *module NOAH* est l'agent de routage sans fil par défaut. Il achemine les paquets transmis par le classificateur MPLS et destinés aux nœuds mobiles vers l'objet *LinkLayer* (LL);

- *objet LinkLayer* appelle le module ARP (*Address Resolution Protocol*) pour obtenir l'adresse MAC de nœuds de destination. Ensuite, il met les paquets dans la file d'attente Ifq;

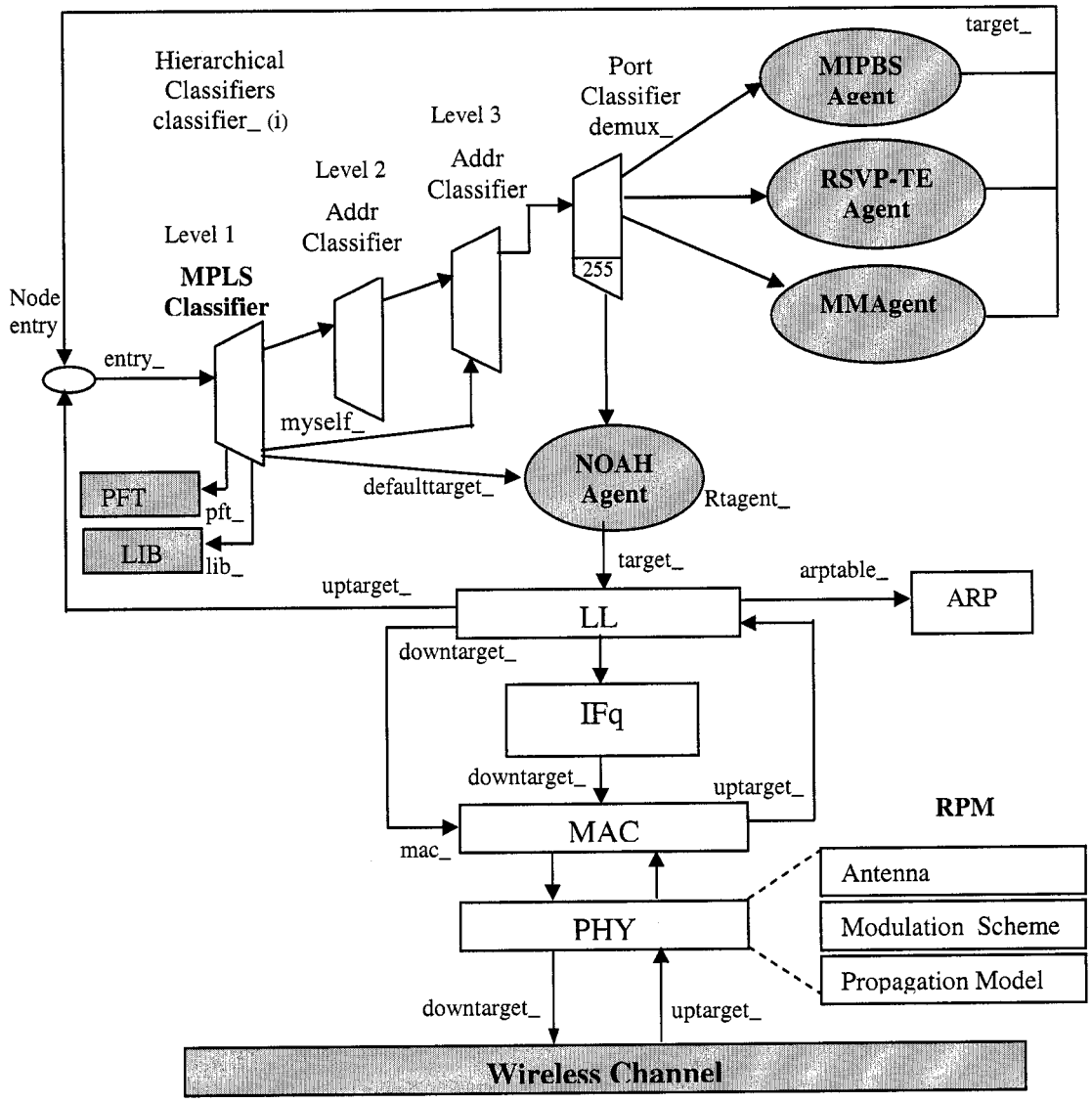

Figure 4.6 Structure d'une station de base (BS) dans Q-HMIP

- *module ARP* traite les demandes de l'objet *LinkLayer* en utilisant une table de correspondance entre l'adresse IP et l'adresse MAC. Il se sert d'un tampon pour mettre les paquets pour lesquels il ne connaît pas de correspondance. Dans ce cas, il

envoie un message *ARP-REQUEST* à tout le réseau. Le nœud visé répond par un message *ARP-REPLY* qui contient son adresse MAC. Par la suite, le module ARP envoie le paquet dans son cache à la couche MAC;

- *couche MAC* implémente uniquement la norme IEEE 802.11 pour les nœuds mobiles. Elle transmet les paquets stockés dans la file d'attente vers la couche physique selon un protocole d'accès au médium (CSMA,..). Au niveau de la couche physique, l'objet *Channel* simule le médium partagé et supporte des mécanismes d'accès au médium des objets MAC, afin de transmettre les paquets vers tous les nœuds qui lui sont attachés;
- *hiérarchie des classificateurs* supporte l'adressage hiérarchique. L'adressage hiérarchique dans NS fonctionne de la manière suivante : il est composé de trois niveaux et noté ainsi : x.x.x. Le premier chiffre indique le domaine, le deuxième indique le cluster et le dernier est l'identifiant du nœud;
- *module de propagation radio* (*RPM*) implémente le modèle de propagation radio CMU: l'atténuation espace-Friss ($1/r^2$) pour les courtes distances et *Two Ray Ground* ($1/r^4$) pour les grandes distances.

4.3 Plan d'expérience

Dans ce qui suit, nous allons présenter le plan d'expérience que nous avons suivi pour construire les différents scénarii de simulation. Les scénarii choisis ont été conçus de façon assez large pour fournir des résultats proches de la réalité, et en même temps assez petite pour qu'il soit supporté par le simulateur NS-2. La topologie du modèle réseau commune à tous les scénarii est présentée à la Figure 4.7.

La topologie est composée d'un agent mère (HA) et d'un correspondant (CN) connectés à une dorsale IP/MPLS via un routeur de frontière (LER). La dorsale est symbolisée par un lien avec un délai (ld) relativement grand, par rapport aux autres liens dans la topologie, pour refléter la distance entre les domaines de macro et micro-mobilité. La dorsale est connectée à un réseau d'accès composé d'un routeur de frontière

(EGW), qui joue le rôle du MAP dans ce cas, de trois routeurs MPLS (LSR1, LSR2 et LSR3) et de quatre routeurs d'accès (AR1, AR2, AR3 et AR4) représentant les points d'accès radio au réseau.

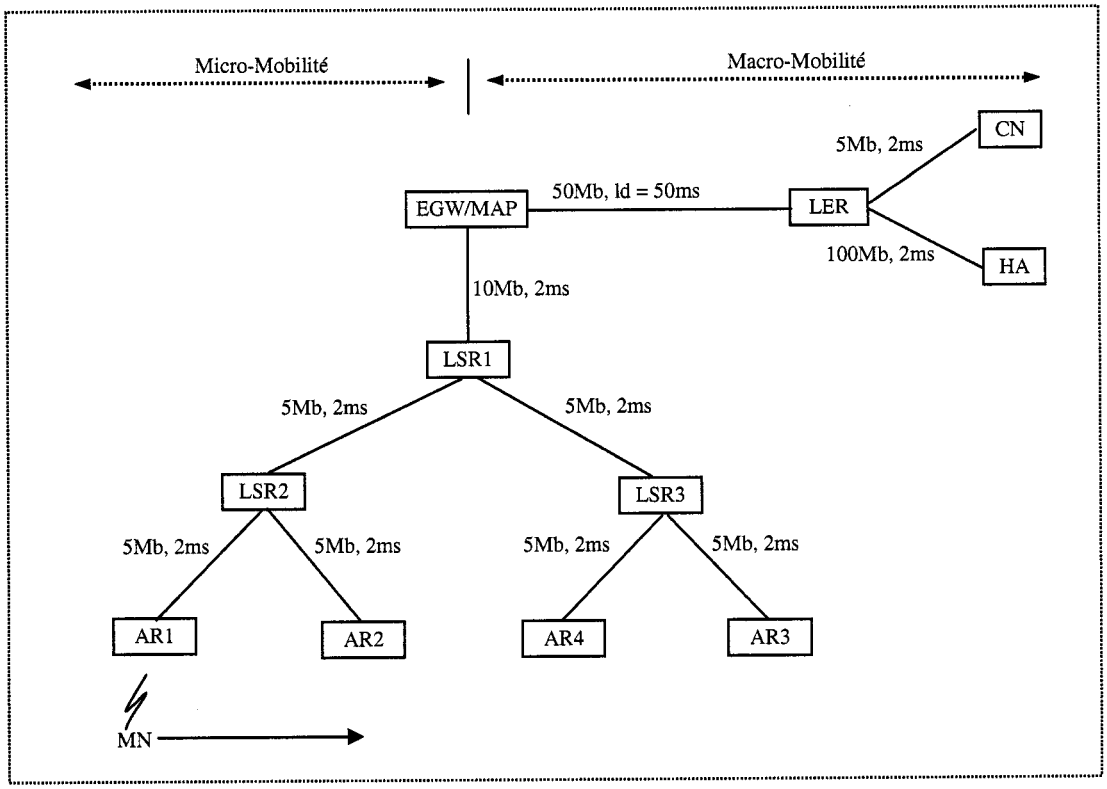

Figure 4.7 Topologie de modèle réseau commune à tous les scénarii

La Figure 4.8 présente l'emplacement des routeurs d'accès et leur couverture radio. L'espace est considéré comme étant une grille dont les frontières (valeurs de x abscisse et y ordonnée) sont déterminées par la portée radio et l'emplacement des routeurs d'accès dans la topologie.

Les hypothèses et scénarii que nous avons fixées pour l'ensemble des expériences sont les suivants :

- Le réseau d'accès est basé sur la norme IEEE 802.11 comme technologie d'accès au médium sans-fil avec un débit de transmission sans-fil de 2 Mbits/s;

- Les routeurs d'accès sont placés de façon à fournir une couverture radio de 700×700 mètres carrés, dont la portée de chacun est de 250 m;

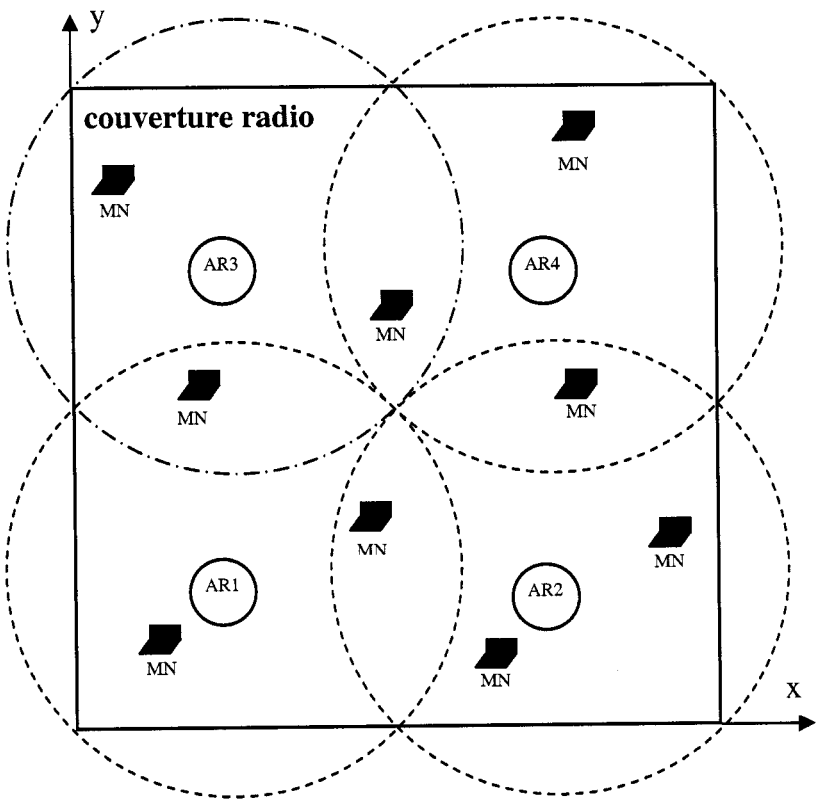

Figure 4.8 Couverture radio des routeurs d'accès

- Les mobiles sont uniformément distribués dans la couverture radio au commencement des simulations et communiquent entre eux uniquement par l'intermédiaire des routeurs d'accès (à l'opposé des réseaux Ad Hoc dont les mobiles peuvent communiquer directement sans passer par un point d'accès);
- Du point de vue mobilité IP, le réseau d'accès constitue un seul domaine de micro-mobilité. Les quatre routeurs d'accès représentent quatre sous-réseaux IP distincts. Les mobiles appartiennent au domaine de mobilité dont le HA agit comme agent de référence (mère), et s'attachent au MAP qui joue le rôle d'un agent mère local dans ce cas.

Afin de simuler des cas réels dont un nœud mobile reçoit des paquets à partir d'une file d'attente partagée, et dont un nœud mobile émetteur se trouve en compétition avec d'autres mobiles émetteurs pour accéder au médium sans-fil, nous considérons dans tous nos scénarii des mobiles qui communiquent entre eux parmi lesquels la moitié sont des émetteurs et l'autre moitié sont des récepteurs. Les mobiles se déplacent aléatoirement dans la zone de couverture radio selon le modèle de mobilité RWP (*random waypoint mobility model*) (Bettstetter et al., 2004). Ce modèle a été utilisé principalement dans des simulations de réseaux Ad Hoc dans NS-2, mais nous trouvons qu'il est bien adapté pour notre simulation aussi..

D'autre part, notre étude de performance se focalise sur un nœud mobile MN récepteur qui est en communication avec un correspondant CN émetteur, étant donné que le but de cette étude est d'examiner la dégradation de la QdS due à la mobilité. Nous justifions cela par le fait que les nœuds mobiles récepteurs sont les nœuds les plus affectés par la dégradation de la QdS. En fait, ces nœuds partagent la même file d'attente au niveau de routeur d'accès avec lequel ils sont rattachés, alors que les nœuds émetteurs (mobile ou non) ne le sont pas. Ainsi, nous examinons les statistiques sur les indices de performance recollés par un nœud mobile singulier et affecté par d'autres nœuds en mobilité.

4.3.1 Scénarii de mobilité

Les scénarii que nous avons étudiés se basent sur la façon dont le nœud mobile se déplace et ils se divisent principalement en deux parties:

Mouvement linéaire

Le mobile observé suit un trajet bien déterminé au début de la simulation alors que les autres mobiles se déplacent aléatoirement, selon le modèle RWP déjà mentionné, avec des vitesses qui varient entre 1 m/sec et 10 m/sec. Durant toute la période de la simulation, les nœuds mobiles exécutent des mises à jour de routage pour changer de destination et de vitesse de telle sorte, qu'ils se déplacent uniquement à l'intérieur de la

couverture radio. Dans ce scénario, le mobile observé choisit le prochain routeur d'accès détecté dans les zones de chevauchement en se basant sur une sélection intelligente implémentée par l'algorithme de priorité fourni par l'agent NOAH. Ainsi, le mobile vérifie l'identité et la priorité de chaque routeur d'accès transmis par les signaux de balise (*beacon signals*), et choisit celui dont la priorité est supérieure. Ceci nous permet de bien contrôler la mobilité et par la suite le nombre de handovers exécuté par le nœud observé, alors que l'interférence engendrée par les autres mobiles est réelle en raison de leur mobilité aléatoire.

Mouvement en ping-pong

Le mobile observé fait des déplacements rapides en aller-retour (*ping-pong*) dans la zone de chevauchement radio entre deux routeurs d'accès voisins (AR1 et AR3). Ainsi, le mobile se déplace à partir d'un point d'origine au début de la simulation vers un point de destination bien déterminé. Lors de l'exécution du premier handoff, le mobile renverse sa direction à toutes les deux secondes afin d'exécuter plusieurs handoffs avant de reprendre son chemin vers sa destination initiale, comme le montre la Figure 4.9.

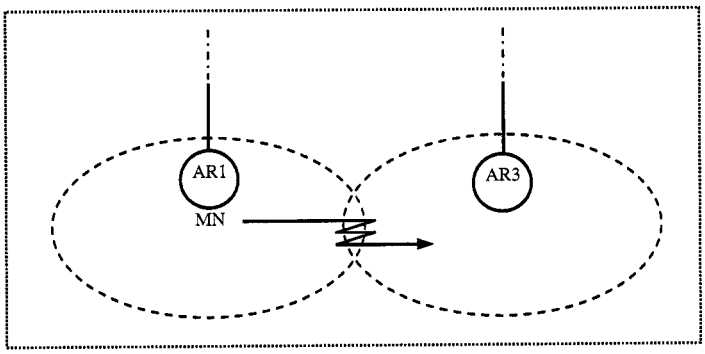

Figure 4.9 Mouvement en *ping-pong*

Dans ce scénario, le mobile choisit le prochain routeur d'accès détecté en se basant sur le niveau de signal reçu seulement (pas de priorité comme le cas précédent).

4.3.2 Sources de trafic

TCP (*Transmission Control Protocole*) et UDP (*User Datagram Protocol*) sont les protocoles de transport les plus utilisés sur IP. TCP est un protocole complexe qui dispose d'un contrôle de flux et de congestion, afin d'utiliser au mieux les ressources du réseau et des terminaux. À l'opposé, UDP ne possède aucun contrôle sur la congestion ni sur la vitesse de transmission. Comme première source de trafic, nous avons utilisé une source FTP (File Transfer Protocol) en continu afin d'étudier l'impact de la mobilité sur le mécanisme de contrôle sur la congestion dans TCP. Une deuxième source de trafic est celle de la voix. En fait, la voix sur IP (VoIP) est une des applications prévues pour être fournies dans les réseaux mobiles de nouvelle génération. Le modèle générique d'une source de trafic de voix a été paramétré pour générer un trafic conforme à celui issu d'un codec PCM tel fourni dans (Chuah et al., 2000). La modélisation de la source de voix est basée sur une chaîne de Markov à temps continu et à deux états discrets: l'état ON ou l'état « *talkspurt* », qui correspond à la période d'activité vocale, et l'état OFF qui correspond à la période de silence. Le temps de maintien de chacun des deux états suit une loi exponentielle de moyenne $1/\lambda = 1.004$ s pour l'état ON et $1/\mu = 1.587$ s pour l'état OFF. Tel que défini par la recommandation ITU-T pour un trafic conversationnel (ITU-T, 1993), ce modèle considère un temps moyen de « *talkspurt* » de 38.57% et un temps moyen de silence de 61.47%. Ainsi, on considère une source de voix avec un taux de 88kbps[6] pour la période ON et de 0 kbps pour la période OFF, avec la détection et la suppression de périodes de silence.

4.4 Statistiques sur les indices de performance

Tout d'abord, nous allons définir les indices de performance que nous avons jugés les plus critiques et la façon dont les statistiques associés vont être calculées :

- *La latence de la relève*

---

[6] Supposons un taux de codage de 8KHz pour un codec PCM de 8 bits/trame, avec une trame de 20ms par paquet. Avec un en-tête RTP, UDP et Ipv6 de 12, 8 et 40 octets respectivement, la longueur d'un paquet de voix sera de 220 octets. La bande passante requise sera de $(220 \times 8)/20 \times 10^{-3}$=88kbps.

Cet indice caractérise l'impact de la relève sur les sessions en cours et constitue une bonne indication des performances de la relève. De façon générale, la latence de la relève est définie comme la différence entre le moment où le nœud mobile reçoit le dernier paquet à travers l'ancien point d'accès et le moment où il reçoit le premier paquet à travers le nouveau point d'accès. Dans notre cas, nous aimerions étudier l'impact de la relève sur une session TCP entre un nœud correspondant émetteur et un nœud mobile récepteur. Dans ce contexte, nous allons définir cet indice comme le temps écoulé entre le moment où le premier paquet TCP retransmis par l'application source est reçu par le nœud mobile par l'intermédiaire du nouveau routeur d'accès et le dernier moment où ce paquet a été transmis.

- *Le débit*

Cet indice de performance est évalué pour une session TCP entre un correspondant émetteur et un mobile récepteur qui se déplace à des vitesses différentes. En fait, le délai de déconnexion a un impact direct sur une session TCP. Pendant cette période, tous les paquets TCP et les acquittements envoyés ou provenant du mobile sont perdus. Ceci a deux conséquences directes sur les performances de TCP :

- Si le temporisateur de retransmission expire ou si l'émetteur reçoit plusieurs acquittements dupliqués, TCP conclut que le réseau est en état de congestion. Le débit d'émission sera réduit à tort;
- Une longue période de déconnexion implique plusieurs réductions successives du débit de la connexion, et la diminution de la réactivité de TCP.

- *Le délai de bout-en-bout*

Les applications en temps réel (voix sur IP par exemple) sont sensibles au retard dans la livraison des paquets. Dans ce contexte, nous allons étudier l'impact de la différentiation du trafic sur le délai de bout-en-bout pour un flux de voix sur IP bien déterminé. Cette statistique représente le délai écoulé entre la date de création d'un paquet par l'application source et la date de son arrivée à l'application cible.

- *La gigue*

De façon similaire au délai, les statistiques de la gigue sont récoltées à la réception de chaque nouveau paquet et se calculent comme la valeur absolue de la différence entre les délais encourus par deux paquets successifs.

- *Le coût de signalisation*

Les statistiques sur cet indice sont limitées au médium sans-fil et se calculent comme le nombre de messages de signalisation envoyés et reçus par le nœud mobile. Nous avons calculé ce coût pour différents taux de handoff (nombre de handoffs par minute).

Une table récapitulative de différents scénarii et statistiques récoltées est présentée au Tableau 4.2.

Tableau 4.2 Configuration des différents scénarii et statistiques récoltées

Scénario	**Mouvement Linéaire**		**Mouvement en ping-pong**
Source de trafic	FTP	Voix	FTP
Protocole de transmission	TCP	UDP	TCP
Comportement TCP	X		X
Latence	X		
Débit	X		
Délai de bout-en-bout		X	
Gigue		X	
Coût de signalisation			X

4.5 Résultats et interprétation

4.5.1 Impact de la relève sur le comportement TCP

Dans ce qui suit, nous allons présenter l'impact du handoff sur le comportement TCP dans le modèle Q-HMIP, en déduisant par la suite la valeur de la latence *D*. La Figure 4.10 expose les numéros de séquence des paquets de données arrivés et des acquittements observés par MN pendant le handoff lors d'un déplacement linéaire. Elle présente en ordonnée les numéros de séquence TCP côté client (paquets de données et acquittements) et en abscisse, le temps en secondes. Avant que le handoff ne soit initialisé, l'expéditeur TCP au niveau du CN utilise une fenêtre d'émission maximale de 20 paquets, ce qui se remarque par la différence des numéros de séquence entre les

paquets de données et les acquittements, comme le montre la Figure 4.11. D'après la Figure 4.10, le handoff de bas niveau (*L2 handoff*) est initialisé par le nœud mobile à 100.97 secondes dans la simulation. Quelques paquets consécutifs sont perdus comme indiqué par les acquittements manquants consécutifs. Grâce au mécanisme du tunnelage de *fast handover*, les paquets reçus par l'ancien routeur d'accès et destinés au mobile seront tunnelés vers le nouveau routeur d'accès (en utilisant le message *NA* envoyé par le MN vers l'ancien routeur d'accès) qui les achemine vers le MN juste à la fin du handoff de bas niveau, comme le montre l'étiquette *a*. Ces paquets sont cependant reçus dans le mauvais ordre et impliquent la duplication des acquittements par le récepteur. Cette duplication est indiquée par la ligne horizontale des numéros de séquence des acquittements (étiquette *b*). Les acquittements dupliqués informent l'émetteur TCP des pertes et causent la retransmission des paquets perdus, comme indiqué par l'étiquette *e* à la Figure 4.11. Ceci est interprété par l'émetteur comme une congestion qui cause la réduction du taux de transmission.

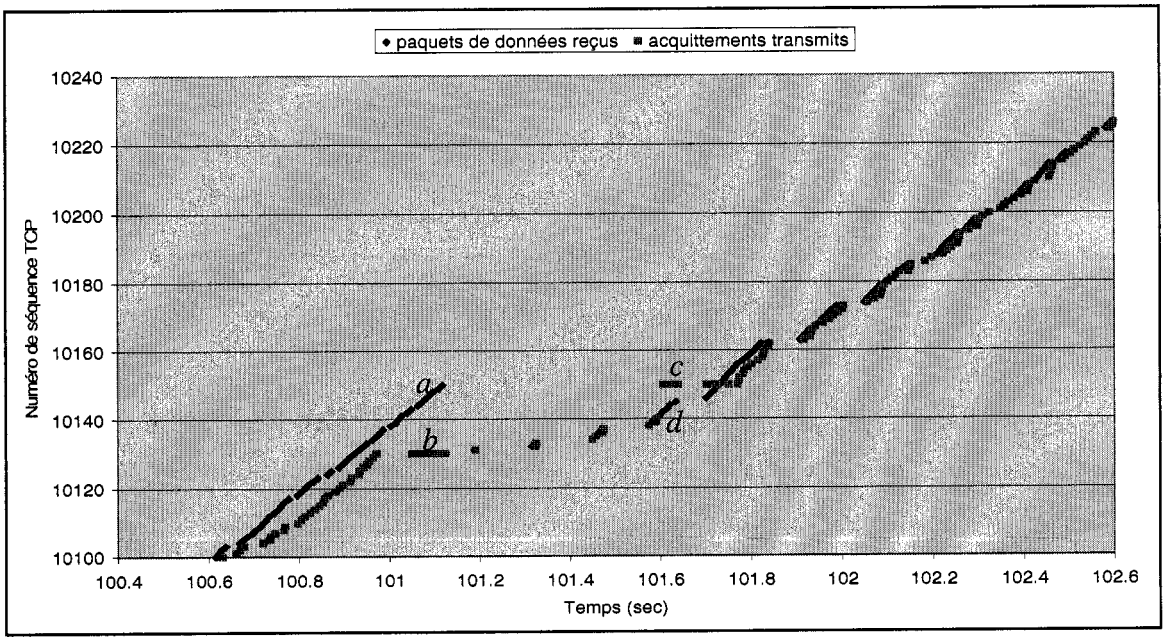

Figure 4.10 Comportement TCP du handoff vu par MN (récepteur)

Le contrôle du flux TCP dans NS-2 permet l'augmentation ou la réduction progressive de la fenêtre d'émission selon les erreurs produites. Si jamais une perte ou une congestion est observée, l'émetteur réduit immédiatement la fenêtre. Le premier paquet retransmis arrive environ 220 ms après le handoff de bas niveau (à 101.19 secondes). Le processus d'ajustement de la fenêtre de transmission continue jusqu'à ce que tous les paquets 'perdus' soient reçus par le mobile. En raison des acquittements accumulés, la fenêtre au nœud mobile s'ouvre brusquement, ce qui est indiqué par l'étiquette *f*. Cependant, les paquets déjà envoyés par l'émetteur (étiquette *g*) continuent à arriver au mobile (étiquette *d*).

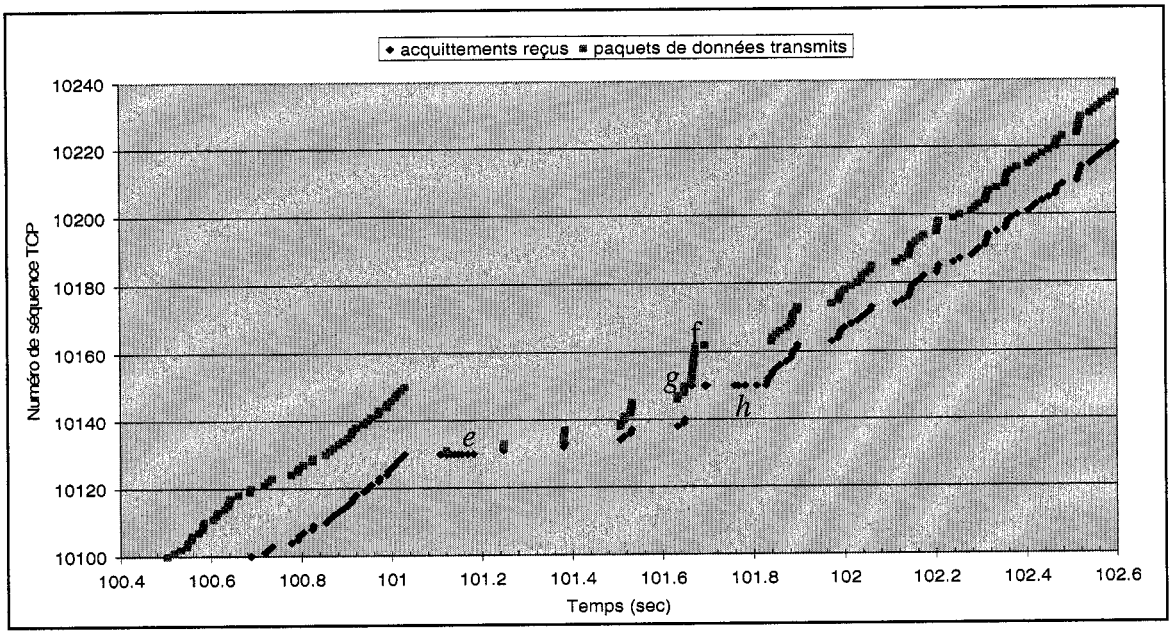

Figure 4.11 Comportement TCP du handoff vu par CN (émetteur)

Ces paquets seront éventuellement acquittés par le mobile avec le même numéro de séquence (étiquette *c*). Ces acquittements arrivent au CN (étiquette *h*) et ils seront ignorés vu que leurs numéros de séquence sont déjà acquittés. Par la suite, la communication retourne à la normale et le taux TCP maximum est à nouveau atteint à 101.77 secondes. La valeur de la latence *D* est 278 ms (220 ms + 58 ms de délai dans le réseau filaire).

Comparaison du comportement TCP entre Q-HMIP et HMIPv6

La Figure 4.12 présente la comparaison du comportement TCP observé par un nœud mobile récepteur suivant les modèles HMIPv6 et Q-HMIP. Le scénario étudié est celui d'un déplacement linéaire tel que présenté à la section précédente. Comme dans le cas précédent, nous déduisons que la valeur D de la latence du handoff pour le modèle HMIPv6 est environ 328 msec.

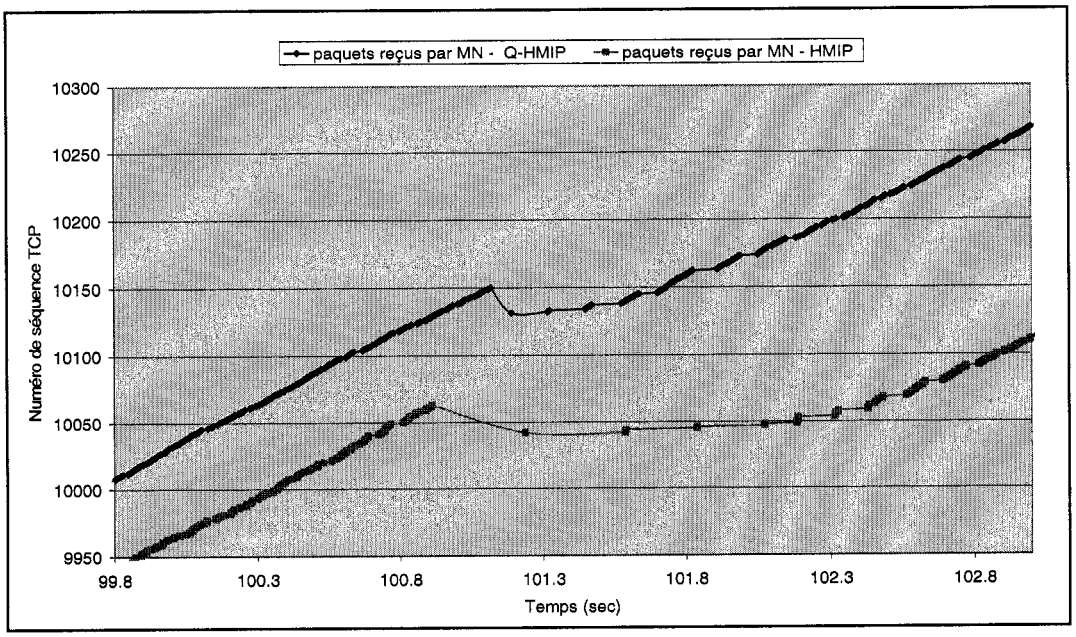

Figure 4.12 Comportement TCP – mouvement linéaire

La Figure 4.13 présente la comparaison du comportement TCP vu par le mobile suivant le scénario de ping-pong.

Ainsi, en se déplaçant vers le routeur d'accès AR3, le mobile renverse sa direction à t = 32 s (temps de simulation) et retourne vers le routeur d'accès AR1. Par la suite, il renverse sa direction à toutes les 2 secondes pour se diriger finalement vers AR3 à partir de t = 38 s. Ces résultats montrent que le modèle Q-HMIP est moins affecté par un mouvement en ping-pong que le modèle HMIPv6.

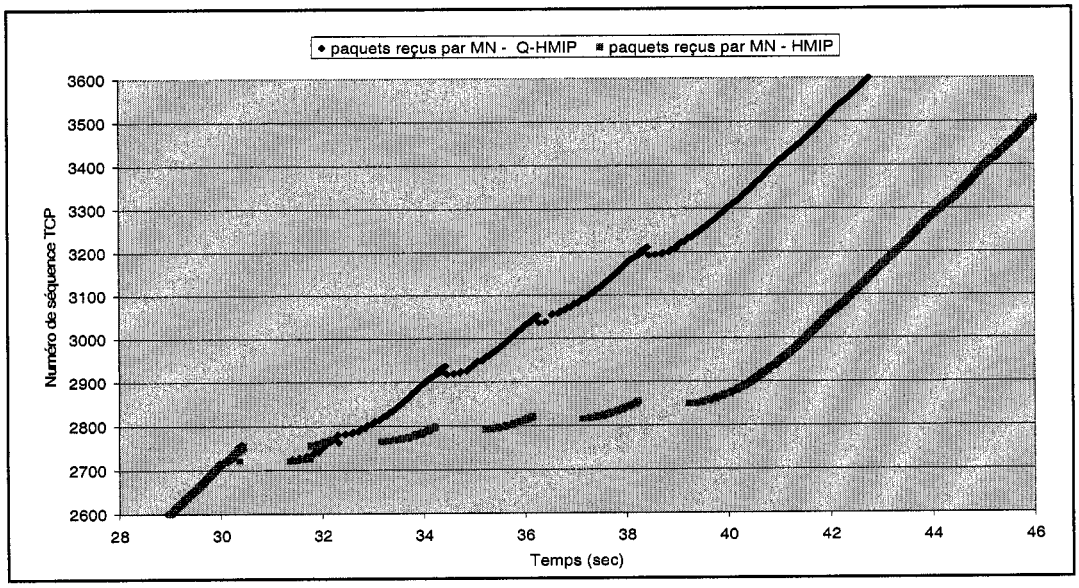

Figure 4.13 Comportement TCP – mouvement en ping-pong

4.5.2 Impact de la vitesse du mobile sur le débit

Dans cette section, nous analysons l'effet de la vitesse du mobile sur le débit TCP reçu. Ainsi, le mobile se déplace à des vitesses différentes allant de 1 m/s jusqu'à 45 m/sec pour une simulation de 300 secondes.

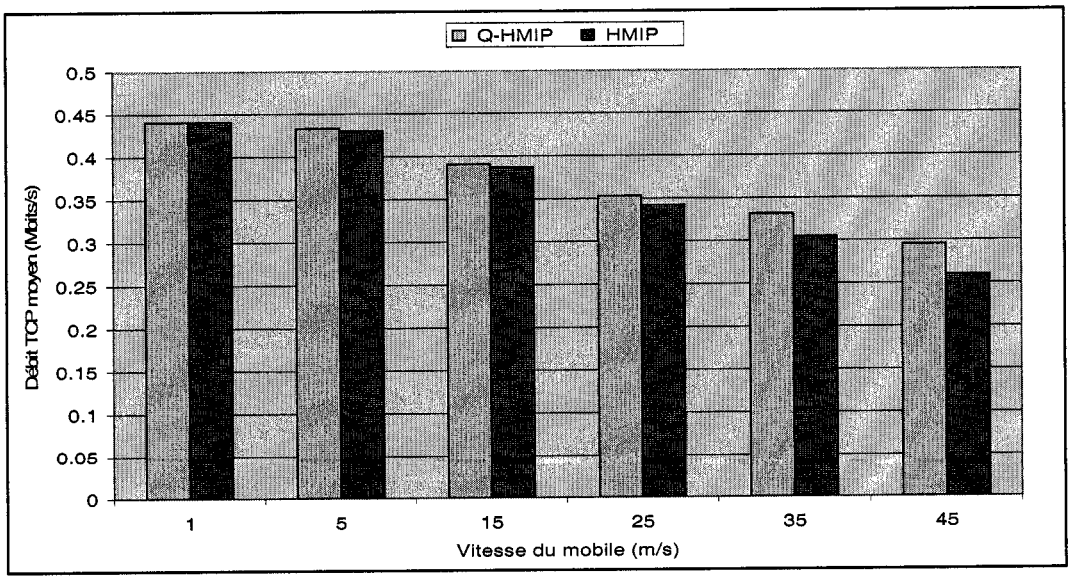

Figure 4.14 Variation du débit TCP reçu avec la vitesse du mobile

Nous remarquons que le débit TCP reçu diminue avec l'augmentation de la vitesse. Ceci s'explique par le fait que plus la vitesse augmente, plus vite le MN traverse la zone de chevauchement radio entre deux points d'accès voisins, et par la suite le MN aura moins de temps pour déclencher le processus du handover (le laps de temps entre le moment où le MN détecte le *beacon* de nouveau routeur d'accès et le moment où il quitte la cellule radio de l'ancien routeur d'accès). Ce qui implique une latence de relève plus élevée et par la suite, le contrôle du flux TCP au niveau du nœud CN interprète cela comme une congestion et éventuellement, il réduit le débit d'émission.

4.5.3 Impact de la différenciation du trafic sur le délai et la gigue

Dans cette section, nous allons examiner l'impact de la différenciation de flux de trafic selon leurs exigences en terme de qualité de service, tel que fourni par le modèle CBQ, sur les indices de performance notamment le débit, le délai de bout-en-bout et la gigue. Ainsi, chaque type de trafic sera routé dans un chemin MPLS différent selon ses critères en terme de qualité de service. Deux sources de trafic CBR (*constant bit rate*) src1 et src2 avec un débit constant de 250 kbits/s, et une troisième de voix src3 avec un taux maximal de 88 kbits/s sont attachées au correspondant CN (voir Figure 4.6). Les bandes passante (BP) sur les liens entre les routeurs d'accès AR1 et AR2 avec LSR1 ont été diminuées pour une valeur maximale de 500 kbits/s chacune. Les sources src1 et src2 sont actives pour toute la durée de la simulation (80 secondes) alors que src3 est active pour une période de 40 secondes seulement (entre t = 20 s jusqu'à t = 60 s, temps de simulation). Pendant cette période, la bande passante requise est plus grande que celle allouée aux liens entre les routeurs d'accès AR1 et AR2 avec LSR1.

Nous avons comparé deux scénarii : 1) les trois flux de trafic sont traités selon *le service au mieux* (*best effort service*). On appelle ce scénario BE-HMIP. 2) les sources src1 et src2 sont classifiées comme des sources SBT et HBT respectivement et partagent le même LSP entre le MAP et MN, alors que src3 est classifié comme une source RT et transite dans un LSP séparé. Ce scénario est noté par Q-HMIP. Les Figures 4.15 et 4.16

présentent le débit reçu par le nœud mobile de trois sources de trafic dans le cas de BE-HMIP et Q-HMIP respectivement.

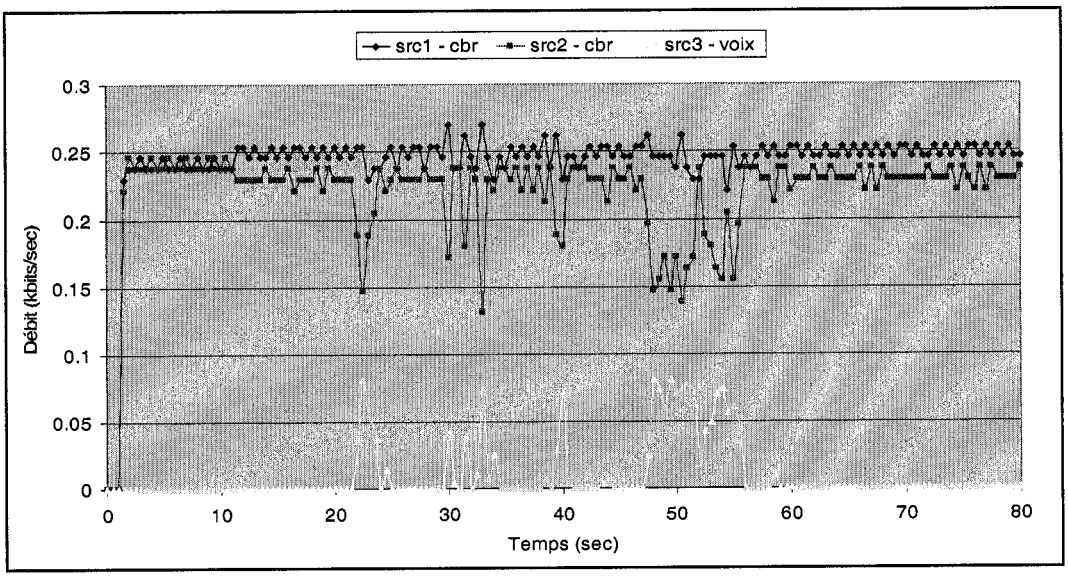

Figure 4.15 Débit reçu par MN – cas de BE-HMIP

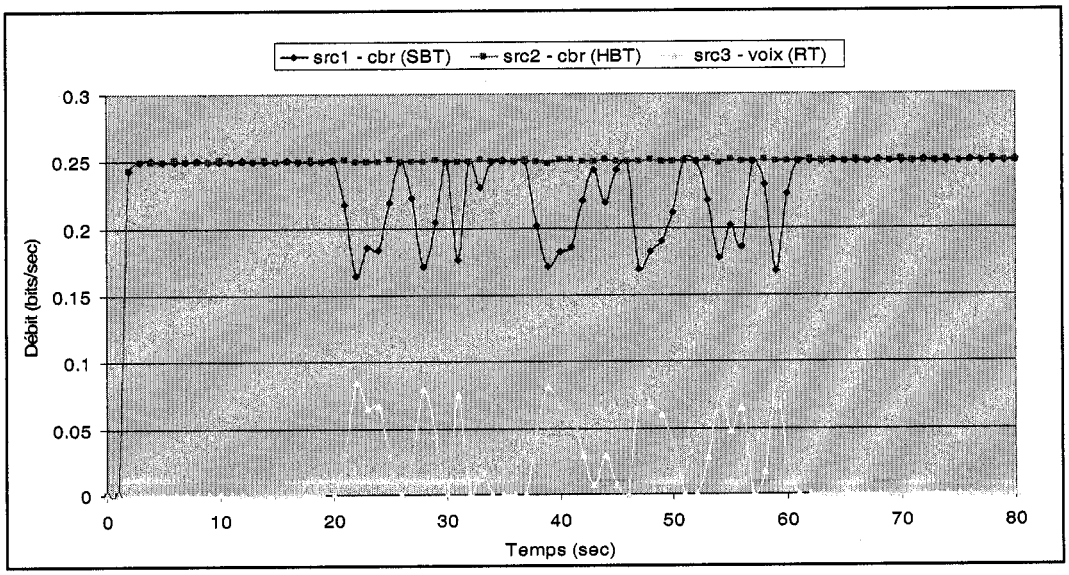

Figure 4.16 Débit reçu par MN – cas de Q-HMIP

Dans le cas de Q-HMIP, nous remarquons que la source prioritaire de la voix a obtenu la bande passante requise alors que les sources SBT et HBT ont obtenu le restant de la BP, ou HBT a été servi mieux que SBT.

L'impact de la séparation de flux de trafic dans des LSP différents sur le délai de bout-en-bout d'un flux de voix est présenté aux Figures 4.17 et 4.18.

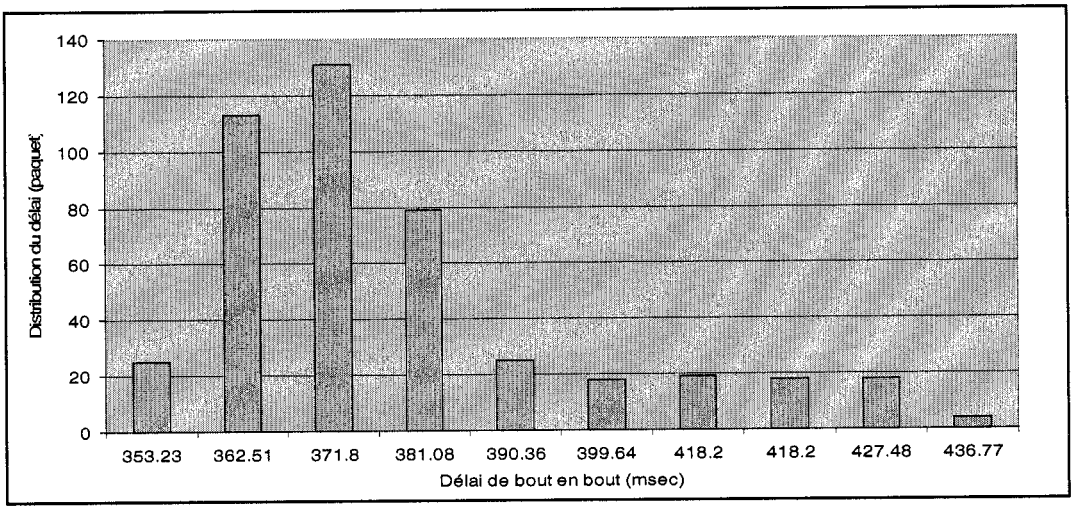

Figure 4.17 Distribution du délai de la voix – cas de BE-HMIP

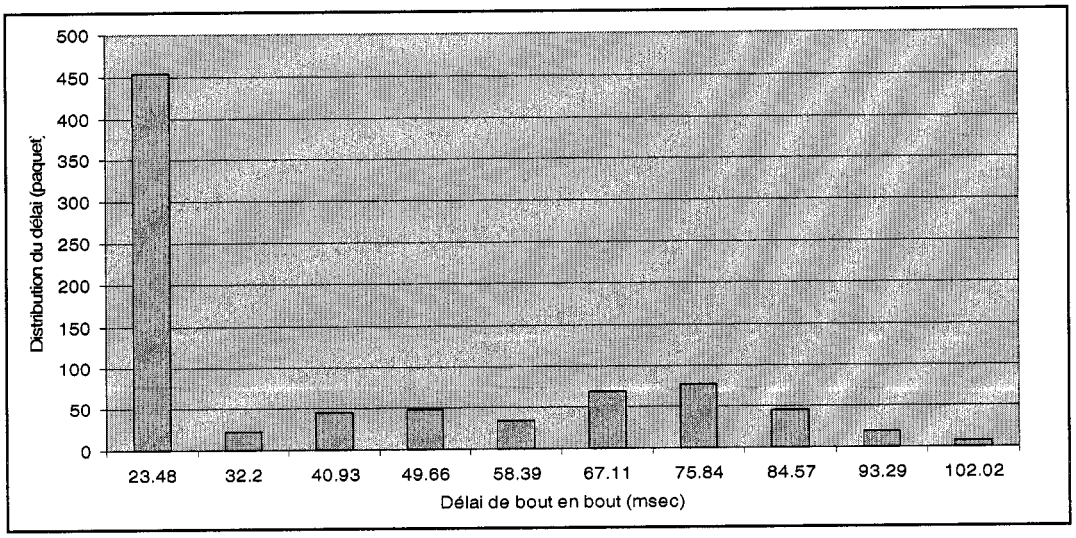

Figure 4.18 Distribution du délai de la voix – cas de Q-HMIP

Ces figures présentent en ordonnée la distribution du délai (nombre de paquets ayant subi un délai particulier) et en abscisse le délai en msec. Nous remarquons que la séparation du flux de voix dans le cas de Q-HMIP a diminué le délai de bout-en-bout avec une valeur maximale de 102.02 msec (< 150 msec).

De même que pour les statistiques de délai, les statistiques récoltées sur la gigue sont présentées aux Figures 4.19 et 4.20.

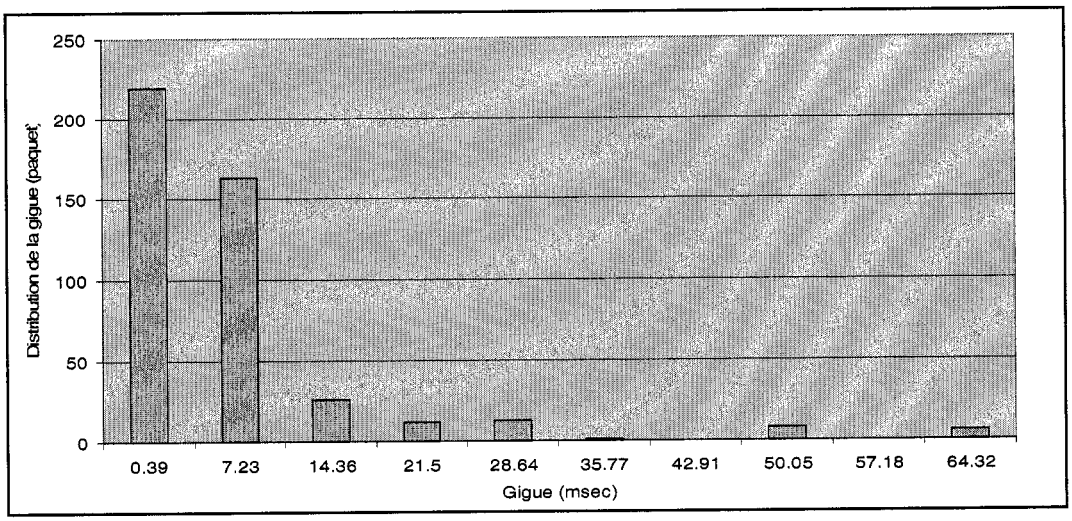

Figure 4.19 Distribution de la gigue– cas de HMIP

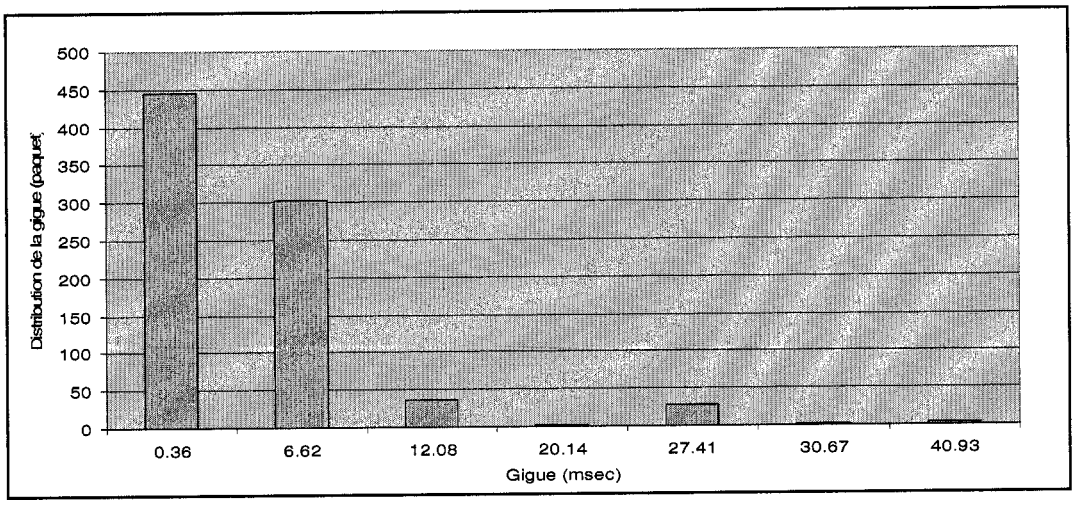

Figure 4.20 Distribution de la gigue– cas de Q-HMIP

Ces statistiques montrent que le modèle Q-HMIP engendre moins de gigue pour une source de trafic sensible aux variations de délai de bout-en-bout, telle que la voix, par rapport à celui de HMIPv6 avec le service au mieux.

4.5.4 Impact du taux de handoff sur le coût de signalisation

Dans ce qui suit, nous allons comparer le coût de signalisation pour différents taux de handoffs suivant le protocole HMIPv6 et celui du modèle proposé. Ainsi, un nœud mobile se déplace en aller-retour entre les deux routeurs d'accès AR1 et AR2 avec une vitesse qui varie entre 1 et 10 m/sec. Au début de chaque exécution, le mobile est placé de manière à produire un taux de handoffs de 0 à 8 handoffs par minute. La durée de chaque simulation est de 65 secondes, dont la source de trafic connecté au CN débute à t = 5 sec, temps de simulation. Bien que le modèle proposé soit mieux adapté pour le mécanisme du handover, il génère plus de signalisation comme prévu, comme le montre la Figure 4.21

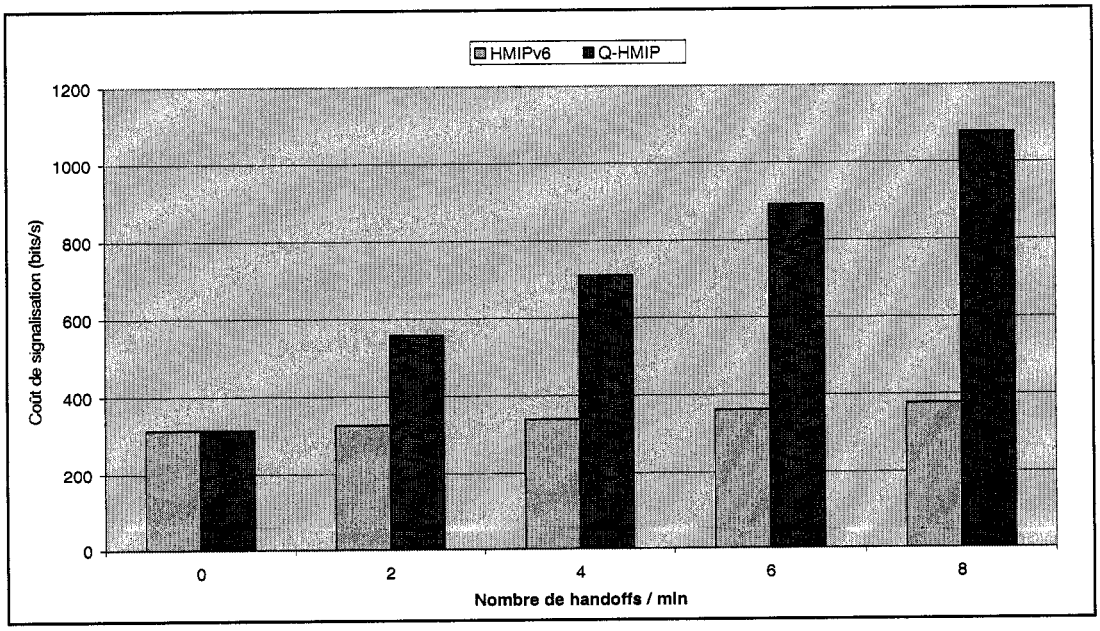

Figure 4.21 Variation du coût de signalisation avec le taux de handoff

CHAPITRE 5

CONCLUSION

En raison de l'énorme succès de la technologie IP dans les réseaux fixes, on admet aujourd'hui que le protocole IP fournira le moyen d'unifier des environnements de plus en plus hétérogènes omniprésents et mobiles tendant vers ce qu'il est convenu d'appeler les réseaux de nouvelle génération (NGN). Ces réseaux visent, entre autres, non seulement à fournir de nouveaux services multimédias à haut débit et des applications à temps réel, mais encore à assurer une mobilité totale de terminaux. Ce mémoire s'est concentré principalement sur l'étude des problèmes liés à la mobilité des usagers dans un réseau d'accès de nouvelle génération, et a examiné l'impact de celle-ci sur la continuité de qualité de service lors des déplacements d'usagers à petite échelle (micro-mobilité).

5.1 Synthèse des travaux et principales contributions

Dans ce mémoire, nous avons proposé un certain nombre de mécanismes visant à améliorer les procédures de gestion de la mobilité d'usagers, tout en fournissant une garantie de qualité de service de bout-en-bout. Tout d'abord, nous avons présenté la mobilité IP et les aspects essentiels qui la caractérisent, ainsi que l'architecture générale des réseaux mobiles de nouvelle génération. Puis, nous avons analysé les protocoles proposés au sein de l'IETF pour la gestion de la mobilité IP ainsi que les méthodes proposées pour améliorer ces protocoles, en considérant leur efficacité et leur performance.

En partant de ces analyses, nous avons proposé un cadre de travail intégrant plusieurs mécanismes de gestion de la mobilité IP, notamment ceux du protocole HMIPv6 et du *Fast Handover*, avec le protocole de signalisation RSVP-TE dans un réseau d'accès IP/MPLS/DiffServ. L'idée principale est de remplacer les mécanismes de

tunnelage dans HMIPv6 par des chemins MPLS et de profiter de l'approche DiffServ sur MPLS de façon à répondre aux exigences des usagers mobiles en terme de qualité de service. Dans ce contexte, nous avons proposé le modèle Q-HMIP qui vise, entre autres, à: réduire la latence du handover et ceci en implémentant la technique du fast handover, de façon à établir un chemin LSP avec le nouveau routeur d'accès avant que le mobile perde sa connexion avec l'ancien routeur d'accès; augmenter la robustesse et la flexibilité du système en distribuant la tâche assumée par le MAP vers tous les routeurs LSR du domaine, et ceci en appliquant le mécanisme de la modification dynamique des chemins LSP possible avec RSVP-TE; et finalement garantir un service évolutif de QdS aux usagers en mobilité et ceci en profitant de l'approche DiffServ sur MPLS. De plus, nous avons étudié la performance de ce modèle par rapport au modèle HMIPv6 en réalisant plusieurs simulations avec le simulateur réseau NS-2.

Nous avons considéré différents scénarii de mobilité notamment, un déplacement linéaire avec des vitesses allant de 1 m/sec jusqu'à 45 m/s et un déplacement en ping-pong, en prenant en considération des cas réels où le mobile observé se trouve en compétition avec d'autres mobiles, qui se déplacent aléatoirement selon le modèle RWP, pour accéder au médium sans-fil. Les simulations que nous avons implémentées nous ont amené à plusieurs conclusions sur l'impact de la relève sur le comportement d'une session TCP, l'impact de la vitesse du mobile observé sur le débit reçu d'une source de trafic FTP, l'impact de la différenciation de trafic sur le délai de bout-en-bout et également sur la gigue d'une source de trafic de voix, et finalement l'impact du taux de handoff sur le coût de signalisation au niveau de la couche radio.

Les résultats de simulations ont montré que le modèle Q-HMIP est mieux adapté pour des handoffs répétitifs avec une latence de 278 msec comparée avec celle de HMIPv6 de 328 msec. D'autre part, le débit moyen reçu par le mobile est plus élevé dans le cas de Q-HMIP comparé avec celui de HMIP, et ceci grâce au mécanisme du tunnelage entre le nouveau et l'ancien routeur d'accès pendant la relève. Un des grands avantages du modèle proposé est la possibilité d'offrir une garantie de bande passante aux usagers pendant leurs déplacements, afin de répondre aux exigences qualitatives

spécifiques des applications à temps réel, et ceci par l'établissement de différents chemins LSP pour acheminer différents types de trafic selon leurs exigences en terme de qualité de service. Ainsi, les résultats de simulations ont montré que le modèle Q-HMIP est mieux adapté aux applications sensibles au délai de bout-en-bout et à la gigue, comme la voix sur IP. Bien que le modèle proposé soit mieux adapté au mécanisme du handover, il génère plus de messages de signalisation que celui de HMIPv6.

5.2 Limitations des travaux

Comme dans toute activité de recherche accomplie, dans le travail présenté il y a toujours une place à l'amélioration. En fait, les simulations implémentées se basent sur une architecture simplifiée du réseau de référence. Il faudrait, par exemple, étudier l'influence du handover sur les performances en terme de temps pour l'établissement de la QdS dans une architecture réelle. D'autre part, les réseaux tout-IP sont supposés supporter un nombre important de services de toutes sortes, notamment de nouveaux services multimédias à haut débit. Étant donné les limitations de sources de trafic disponibles dans NS-2, nous n'avons retenu qu'une partie de nouveaux services visés, notamment un codec de base de la voix. Il faudrait également étudier les performances du modèle Q-HMIP pour d'autres types de sources de trafic telles que la vidéo. Par ailleurs, ce travail n'a pas considéré l'aspect de l'ingénierie de trafic en établissant un nouveau chemin MPLS lors d'un handoff. Il faudrait, par exemple, étudier le cas où le nouveau réseau d'accès n'a pas assez des ressources disponibles pour établir un nouveau chemin LSP avec les mêmes paramètres de qualité de service que l'ancien LSP. Afin d'empêcher qu'une demande d'établissement d'un nouveau LSP ne soit refusé, le mobile pourrait accepter une dégradation de la QdS vers sa nouvelle localisation. Ainsi, le mobile devrait être capable de négocier les paramètres de la QdS au début d'une session de communication avec un correspondant, et d'ajuster ou adapter ces valeurs pour tout changement futur de conditions de réseau.

5.3 Recommandations pour des travaux futurs

Il convient de mentionner, malgré toutes les recherches effectuées et les méthodes proposées, que le problème de gestion de la mobilité IP demeure encore un problème ouvert et d'actualité. Nos travaux se sont focalisés sur l'étude du réseau d'accès dans son support d'une QdS homogène, soit DiffServ sur MPLS. Il serait intéressant d'explorer des solutions fonctionnant dans des réseaux d'accès utilisant des paradigmes de QdS hétérogènes. Par exemple, un mobile pourrait effectuer un handoff entre deux routeurs d'accès l'un appartenant à un domaine IntServ et l'autre à un domaine DiffServ. Il serait également intéressant d'étudier l'aspect de la sécurité dans MIPv6 et son intégration dans le cadre de ce travail, afin d'examiner son impact sur l'établissement et la gestion des chemins MPLS.

Dans ce mémoire, nous avons adopté le mécanisme nommé "*LSP dynamic rerouting*" fourni par RSVP-TE pour modifier ou rerouter un chemin LSP lors du changement de localisation d'un nœud mobile. Une autre direction de recherche future pourrait consister à étudier l'approche d'établissement des chemins MPLS point à multipoints proposée dans une extension de RSVP-TE (Aggarwal et al., 2004).

BIBLIOGRAPHIE

Articles de revues et de conférences, RFCs

[Aggarwal et al., 2004] R. Aggarwal, D. Papadimitriou et S. Yasukawa, "Extensions to RSVP-TE for Point to Multipoint TE LSPs," Internet draft, draft-raggarwa-mpls-rsvp-te-p2mp-00.txt, Work in progress, July 2004.

[Anderson et al., 2001] L. Anderson, P. Doolan, N. Feldman, A. Fredette, et B. Thomas, "LDP Specification," Request for Comment 3036, Internet Engineering Task Force, January 2001.

[Awduche et al., 2001] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan et G. Swallow, "RSVP-TE : Extensions to RSVP for LSP Tunnels," Request for Comment 3209, Internet Engineering Task Force, December 2001.

[Bettstetter et al., 2004] C. Bettstetter, H.Hartenstein et X. Perez-Costa., "Stochastic Properties of the Random Waypoint Mobility Model", *Wireless Networks*, vol. 10, pp. 555–567, September 2004.

[Blake et al., 1998] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, et W. Weiss, "RFC2475: An Architecture for Differentiated Services", December 1998.

[Braden et al., 1994] R. Braden, D. Clark et S. Shenker, "Integrated Services in the Internet Architecture: an Overview," Request for Comment 1633, Internet Engineering Task Force, June 1994.

[Braden et al., 1997] B. Braden, L. Zhang, S. Berson, S. Herzog et S. Jamin, "Ressource ReSerVation Protocol (RSVP), Version I Functional Specification" Request for Comment 2205, Internet Engineering Task Force, September 1997.

[Braun et al., 2000] T. Braun, C. Castelluccia, G. Stattenberger et I. Aad, "An Analysis of the DiffServ Approach in Mobile Environments," *In Proceedings of 1st W orkshop on IP QoS for Wireless and Mobile Networks (IWQiM)* 1999, April 2000.

[Campbell et al., 2000] A. T. Campbell, J. Gomez, S. Kim, A. G. Valkó, C-Y. Wan et Z. Turányi, "Cellular IP", Internet draft, draft-ietf-mobileip-cellularip-01.txt, January 2000.

[Campbell et al., 2002] A. T. Campbell, J. Gomez, S. Kim, Z. R. Turanyi, C-Y. Wan et A. G. Valko, "Comparison of IP Micro-Mobility Protocols", *IEEE Wireless Communications Magazine*, vol. 9, no. 1, pp. 72-82, February 2002

[Chuah et al., 2000] C. N. Chuah, L. Subramanian, R. H. Katz et A. D. Joseph, "QoS Provisioning Using a Clearing House Architecture," in the *Proc of the IEEE International Workshop on Quality of Service (IWQoS)*, Pittsburgh, PA, pp. 115-124, June 2000.

[Chung et al., 2002] J-M Chung, K. Srinivasan., et M. A. Subieta., "wireless Multiprotocol Label switching," Internet draft, draft-chung-mpls-wmpls-00.txt, Mars 2002.

[Dommety et al., 2001] G. Dommety, M. Subarrao, K. Leung et R. Patil "Local Mobility Agents in IPv6," Internet draft, draft-dommety-mobileip-lma-ipv6-03.txt, July 2001.

[Droms, 1997] R. Droms, "Dynamic Host Configuration Protocol", Request For Comment 2131, Internet Engineering Task Force, Mars 1997.

[Furguson et al., 2000] P. Furguson, D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", Request for Comment 2827, Internet Engineering Task Force, May 2000.

[Heinanen et al., 1999] J. Heinanen, F. Baker, W. Weiss et J. Wroclawski, "Assured Forwarding PHB group", Request for Comment 2597, Internet Engineering Task Force, 1999.

[ITU-T, 1993] ITU-T Recommendation p.59, "Artificial conversational speech", 1993.

[Jacobson et al., 1999] V. Jacobson, K. Nichols et K. Poduri, "An Expedited Forwarding PHBgroup", Request for Comment 2598, Internet Engineering Task Force, 1999.

[Jamoussi et al., 2002] B. Jamoussi, L. Andersson, R. Callon, R. Dantu, L. Wu, P. Doolan, T. Worster, N. Feldman, A. Fredette, M. Girish, E. Gray, J. Heinanen, T. Kilty et A. Malis, "Constraint-Based LSP Setup using LDP", Request for Comment 3212, Internet Engineering Task Force, January 2002.

[Johnson et al., 2004] D. Johnson, C. Perkins et J. Arkko, "Mobility support in IPv6", Request for Comment 3775, Internet Engineering Task Force, June 2004

[Katz, 1997] D. Katz, "IP router alert option", Request for Comment 2113, Internet Engineering Task Force, 1997.

[Kempf, 2001] J. Kempf, "Bi-directional Edge Tunnel Handover for IPv6", Internet draft, draft-kempf-beth-ipv6-03.txt, Avril 2002.

[Kim et al., 2001] H. Kim, K-S D. Wong, Chen et C. L. Lau, "Mobility-aware MPLS in IP-based Wireless Access Networks Integration of Mobile IP," *In Proceedings of IEEE Global Telecommunications Conference, 2001(GLOBECOM '01)*, vol. 6, pp.3444-3448.

[Koodli et al., 2000] R. Koodli et C. Perkins, "A Framework for Smooth Handovers with Mobile IPv6", IETF, draft-koodli-mobileip-smoothv6-00.txt, July 2000.

[Koodli, 2004] R. Koodli, "Fast Handovers for Mobile IPv6", draft-ietf-mipshop-fast-mipv6-02.txt, work in progress, July 2004.

[Le Faucheur et al., 2002] F. Le Faucheur, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval et J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Service", Request for Comment 3270, Internet Engineering Task Force, May 2002.

[Perkins, 1996] C. Perkins, "IP Encapsulation within IP", Request for Comment 2003, Internet Engineering Task Force, October1996.

[Perkins, 2000] C. Perkins, "Route Optimization in Mobile IP", draft-ietf-mobileip-optim-12, Avril 2002.

[Perkins et al., 1996] C. Perkins, "IP Mobility Support", Request for Comment 2002, Internet Engineering Task Force, October 1996.

[Perkins et al., 1999] C. Perkins et K. Y. Wang, "Optimized Smooth Handoffs in Mobile IP", *Proceedings of the fourth IEEE Symposium on Computers and Communications*, pp. 340-346, July 1999.

[Perkins et al., 2002] C. Perkins, "IP Mobility Support for IPv4", Request for Comment 3220, Internet Engineering Task Force, January 2002.

[Ramjee et al., 1999] R. ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S. Y. Wang et T. La Porta, "HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area Wireless Networks," *IEEE/ACM Transactions on Networking*, vol. 10, no. 3, pp. 396-410, June 2002.

[Ren et al., 2001] Z. Ren, C-K Tham, C-C Foo et C-C Ko, "Integration of Mobile IP and Multiprotocol Label switching," *In Proceedings of IEEE International Conference on Communications (ICC) 2001*, pp. 2123-2127, June 2001.

[Rosen et al., 2001] E. Rosen, A. Viswanathan et R. Callon, "RFC3031: Multiprotocol Label Switching Architecture", January 2001.

[Soliman et al., 2004] H. Soliman, C. Catelluccia, K. El Malki et L. Bellier, "Hierarchical MIPv6 Mobility Management," Internet draft, draft-ietf-mipshop-hmipv6-02.txt, work in progress, June 2004.

[Um et al., 2001] T. W. Um et J. K. Choi, "A Study on Path Re-routing Algorithms at the MPLS-based Hierarchical Mobile IP Network," *In Proceedings of Region 10 International Conference on Electrical Ans Electronic Technology (TENCON) 2001*, pp. 691-697, Aug. 2001.

Outils logiciels et pages Web de référence

[NS-2] "The Network Simulator ns-2", http://www.isi.edu/nsnam/ns

[Hsieh] Hsieh, R. the NS implementation of HMIPV6 with Fast Handover, http://mobqos.ee.unsw.edu.au/~robert/research.php

[Widmer] Widmer, J. Extensions to the ns Network simulator, http://icapeople.epfl.ch/widmer/MobileIP/ns-extension

[VINT] Virtual InterNetwork Testbed, http://www.isi.edu/nsnam/vint/index.html

[MNS] "MPLS Network Simulator", http://flower.ce.cnu.ac.kr/~fog1/mns

[Murphy] Murphy, S. "The ns/MPLS/DiffServ patch," Dublin City University, Ireland, 2000.

[Böringer] Böringer R. RSVP-TE Enhacement for ns2, http://www-ihs.theoinf.tu-ilmenau.de/mitarbeiter/boeringer/rsvp_te_ns2.html

[Greis] Greis, M. RSVP/ns, http://www.isi.edu/nsnam/ns/ns-contributed.html

ANNEXE I

Protocoles de Signalisation

I.1 RSVP (Ressource reSerVation Protocol)

Le protocole de signalisation RSVP (Braden et al., 1997) est un mécanisme dynamique conçu pour effectuer des réservations de ressources explicites dans une architecture de qualité de service (QdS) Intserv. RSVP est utilisé uniquement pour la communication des paramètres de QdS. Il ne comprend pas l'information qu'il transporte dans les requêtes de QdS. RSVP est initié par une application au début d'une session de communication. Une session est identifiée par l'adresse IP de destination, le type de protocole de la couche de transport et le numéro de port de destination. Chaque paquet RSVP contient les détails sur la session à laquelle il appartient. L'affectation des ressources demandées par l'intermédiaire de RSVP pour un flot donné est indépendante de RSVP; elle dépend d'IntServ. Une fois que les ressources demandées par RSVP sont réservées, elles sont utilisées pour ce flot de données. RSVP établit et maintient un état logiciel entre les nœuds constituant le chemin réservé. Par opposition à la réservation d'un chemin statique, cet état logiciel est caractérisé par des messages de rafraîchissement envoyés périodiquement le long du chemin pour maintenir l'état. RSVP fournit aussi une QdS dynamique, tenant compte des modifications de ressources; celles-ci peuvent être dues au destinataire, à l'émetteur ou encore à de nouveaux membres dans un groupe multicast.

Messages RSVP

Le protocole RSVP définit sept types de messages, les principaux étant les messages PATH et RESV. Ces deux messages assurent le fonctionnement de base de RSVP. Les autres messages RSVP, présentés dans le Tableau I.1, sont utilisés soit pour fournir des informations sur l'état des réservations, soit pour annuler explicitement les réservations le long d'un chemin d'une session de communication. Tous les messages

RSVP sont envoyés sur le réseau comme des datagrammes IP avec le numéro de protocole 46, et PATH, PATH Tear et RESV Conf doivent être envoyés avec l'option d'alerte de routeur activée [Katz, 1997].

Tableau I.1 Messages RSVP

Messages RSVP		
PATH	PATH Tear	
RESV	RESV Tear	
PATH Err	RESV Con	
RESV Err		
Ces messages incluent un ou plusieurs des objets suivants:		
SESSION	FILTER_SPEC	ADSPEC
ERROR SPEC	SENDER_TEMPLATE	POLICY_DATA
SCOPE	SENDER_TSPEC	RESV_CONFIRM
STYLE	INTEGRITY	TIME_VALUES
FLOWSPEC	RSVP_HOP	

Fonctionnement de base

Le message PATH est envoyé par la source qui initie la session de communication et envoie ses exigences au destinataire. Le message PATH contient le champ SENDER_TSPEC (spécification du trafic de l'émetteur), utilisé par la source pour spécifier les caractéristiques de trafic de ses flots de données. Tous les éléments de réseau par lesquels transite le message PATH, ainsi que le destinataire lui-même, mettent en place une information d'état sur la session décrite dans PATH. ADSPEC est un autre champ du message PATH; ce champ optionnel fournit une indication d'état sur le réseau.

Après réception du message PATH, le destinataire RSVP utilise le chemin inverse pour générer une requête RESV qui spécifie la QdS souhaitée. En dehors des informations concernant le style de réservation souhaité par le récepteur (champ Filter),

le message RESV contient deux champs, FLOWSPEC et FILTER_SPEC, qui constituent la description du flux.

FLOWSPEC définit les exigences pour le flot de données, c'est à dire :

- le type de service demandé (garanti ou à contrôle de charge) ;
- les paramètres du service pour invoquer la QdS (RSPEC) ;
- les paramètres du flot demandant ce service (TSPEC).

RSPEC n'est présent dans la description du flot que si le service demandé est le service garanti. Le champ FILTER_SPEC fixe les paramètres adéquats pour la classification des paquets.

Chaque nœud RSVP, à la réception du RESV, réalise le contrôle d'admission, réserve les ressources appropriées et renvoie la requête au nœud en amont. Ce processus se répète jusqu'à la source. L'émetteur RSVP peut alors envoyer les données. En cas d'échec de la réservation, un message d'erreur est envoyé. Notons qu'à l'inverse des messages PATH qui sont envoyés à l'adresse de la session (unicast ou multicast), les messages RESV sont envoyés à une adresse unicast.

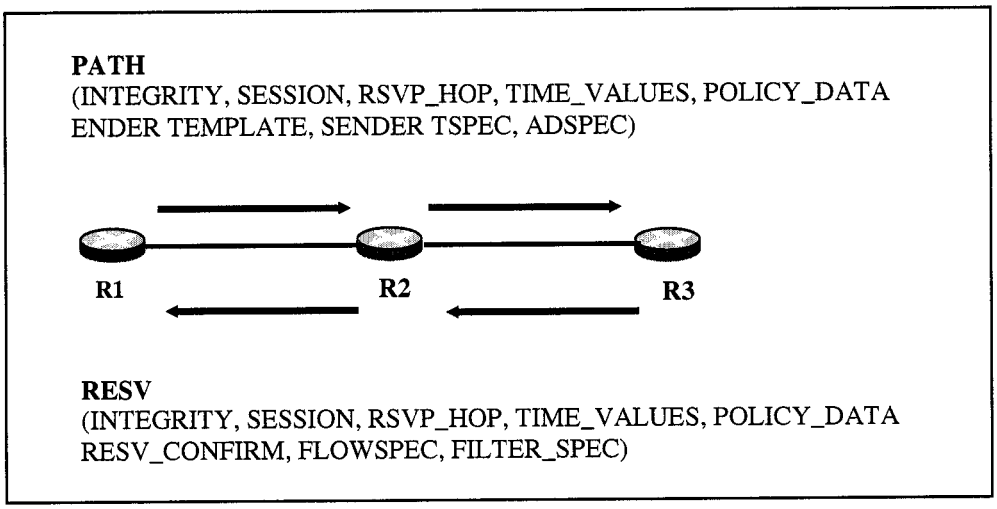

Figure I.1 Session RSVP

La Figure I.1 présente les messages échangés afin d'établir une session RSVP entre un routeur source R1 et un autre destinataire R3.

L'état des réservations RSVP est dit *soft state* et doit être mis à jour régulièrement. Les messages PATH et RESV sont retransmis périodiquement, ce qui permet de mettre à jour les informations sur l'état de la session. Cette technique évite d'allouer inutilement des ressources à une session terminée; elle permet également de s'adapter à des changements de configuration du réseau, comme une modification du routage.

I.2 RSVP-TE (Resource ReserVation Protocol with Traffic Engineering)

Le protocole RSVP-TE est une extension du protocole RSVP pour l'établissement des tunnels LSP et qui supporte des fonctionnalités de gestion de QdS au sein d'un réseau MPLS. À l'origine, ce protocole était prévu pour réclamer la bande passante (BP) requise et des conditions de trafic sur un certain chemin, et le lien n'était établi que si la bande passante nécessaire était disponible. RSVP-TE est un protocole dit «soft state», c'est à dire qu'il établit une session dans chacun des nœuds du chemin d'un LSP. Un mécanisme de rafraîchissement par des messages (PATH, RESV) permet de maintenir ces sessions. Donc, RSVP-TE est considéré aussi comme un protocole de signalisation et de distribution d'étiquettes dans l'architecture MPLS.

RSVP-TE utilise la mode *Downstream-on-demand* pour la distribution d'étiquettes et l'établissement des LSP. Il supporte la création des chemins LSP explicites avec ou sans réservation. Il permet de rediriger le trafic (*rerouting*) sans provoquer une coupure pour l'utilisateur, ce mécanisme est appelé aussi « *make-before-break* ». L'identification et l'association des tunnels LSP est possible grâce aux objets SESSION, SENDER et FILTER_SPEC du protocole RSVP. Il permet également la préemption et la détection des boucles.

Nouveaux objets et messages

Cinq nouveaux objets ont été ajoutés au protocole RSVP, comme le montre le Tableau I.2 :

Tableau I.2 Nouveaux objets RSVP

Nom de l'objet	Appliqué dans les messages RSVP
LABEL_REQUEST	PATH
LABEL	RESV
EXPLICIT_ROUTE	PATH
RECORD_ROUTE	PATH, RESV
SESSION_ATTRIBUTE	PATH

Création d'un chemin LSP explicite

La Figure I.2 montre l'établissement d'un chemin LSP explicite entre les LSR A et LSR E en passant par LSR B et LSR C. Pour créer le LSP, le routeur ingress (LSR A) envoie un message PATH avec le nouvel objet session «LSP_TUNNEL», contenant :

- L'objet LABEL_REQUEST qui indique le type de data transporté et demande à ce qu'un LABEL soit associé à ce chemin;
- L'objet EXPLICIT_ROUTE (ERO) qui permet à l'émetteur de déterminer la route explicite pour le LSP demandé. Chaque LSR intermédiaire (LSR B et LSR C) ajoute son adresse IP. Si un LSR est incapable de joindre le LSP demandé, il retourne un message PATH Err;
- L'objet SESSION_ATTRIBUTE qui permet d'avoir une authentification et un diagnostic. Des informations de contrôle telles que les priorités, les ressources, et les protections locales sont données (préemption);
- L'objet TSPEC qui définit le type de trafic.

L'objet RECORD_ROUTE (RRO) enregistre les étiquettes empruntées par un LSP et par la suite, permet à l'émetteur de connaître la route prise par le LSP (détection de

boucles). Il pourra, avec cet objet, être notifié des changements de routes dans le réseau.

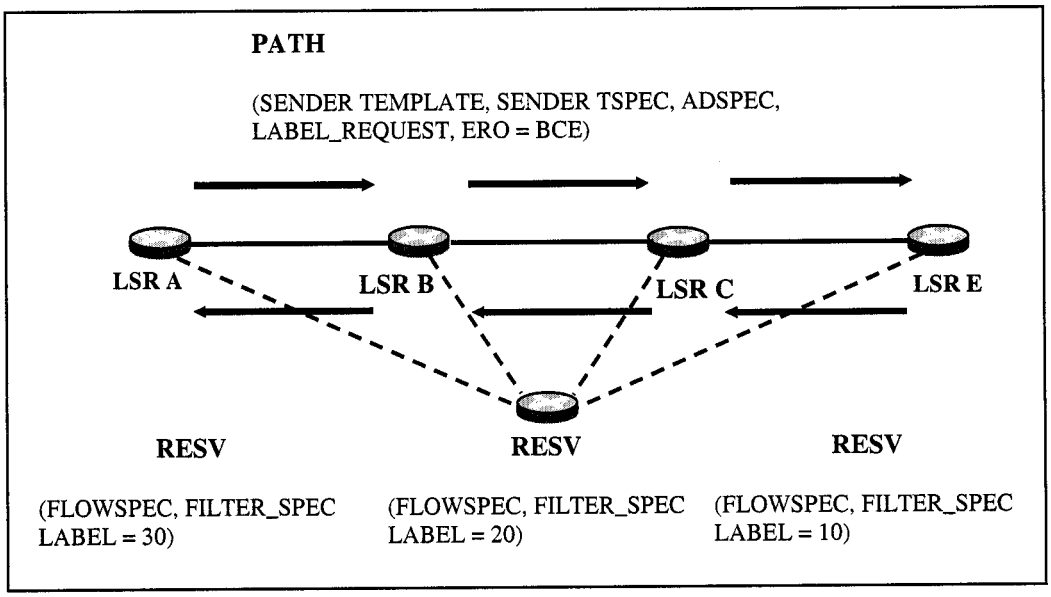

Figure I.2 Création d'un LSP avec RSVP-TE

Une fois le message PATH arrivé au routeur egress (LSR E), celui-ci renvoie un message RESV suivant le chemin pris par le message PATH avec l'objet LABEL, car on a un LABEL_REQUEST dans le message PATH. Chaque LSR intermédiaire met à jour cette valeur jusqu'à que le message RESV atteigne le routeur ingress (LSR A). C'est avec ce message que les réservations seront confirmées dans les routeurs.

Type de réservation

Chaque LSP doit être établi avec un type de réservation. Ce type est défini par le routeur egress. Il existe 3 types :

FF (Fixed Filter)

Ce style crée une réservation distincte pour chaque émetteur qui ne pourra pas être partagée, ce qui permet d'isoler les trafics entre eux. La quantité totale de

réservation de BP sur un lien partagé pour des sessions utilisant ce style est la somme des réservations individuelles. Chaque émetteur a ses propres réservations, ce qui correspond à un LABEL unique pour chacun. On peut donc dire qu'un LSP est un LSP point à point. Chaque LSP a sa propre identification et a sa propre réservation de bande passante (BP).

SE (Shared Explicit)

Avec ce style, plusieurs émetteurs peuvent partager le même LSP. On a là un LSP multipoint-à-point. Une seule valeur de session étant attribuée, on aura, du coté du récepteur une réserve de BP qui sera moins que ce qui est demandé, et du coté de l'émetteur on aura plus que ce qui est demandé.

WF (Wildcard Filter)

Ce style crée une simple réservation sur un lien qui est partagé par une liste explicite d'émetteurs. Chaque émetteur étant explicitement listé dans un message RESV, différentes étiquettes peuvent être allouées, ce qui permet d'avoir des LSP séparés. Chacun des LSPs a sa propre identification mais ils se partagent entre eux la même réservation de BP sur le lien.

ANNEXE II

Les Tables MPLS

Le protocole MPLS sauvegarde les informations associées aux étiquettes dans trois éléments :

i. ***Next Hop Label Forwarding Entry*** **(*NHLFE*)** - est une table utilisée pour le routage des paquets étiquetés. Elle contient les informations suivantes :

1. Le prochain saut du paquet.
2. L'opération à effectuer sur l'étiquette du paquet. Il s'agit de l'une des opérations suivantes :
   - remplacer l'étiquette du haut de la pile avec une nouvelle étiquette spécifiée ;
   - retirer l'étiquette de la pile ;
   - remplacer l'étiquette du haut de la pile avec une nouvelle étiquette spécifiée, puis ajouter une ou plusieurs nouvelle étiquettes spécifiées dans la pile label.

Entry #	Next Hop	Operation	Next Label
		Swap	
		Pop	
		Swap and Push	

La table peut aussi contenir :

a- l'encapsulation des données de liaison à utiliser lors de la transmission du paquet;

b- la manière d'encoder la pile label lors de la transmission du paquet;

c- toute autre information nécessaire pour disposer correctement du paquet.

ii. ***Incoming Label Map (ILM)*** – cette table met en relation un jeu de NHLFE pour chaque étiquette entrant. Elle est utilisée pour router les paquets qui arrivent en tant que paquets étiquetés

Incoming Label	NHLFE

iii. ***FEC-to-NHLFE Map (FTN)*** – cette table fait le lien entre chaque FEC et un jeu de NHLFE. Elle est utilisée pour router les paquets qui arrivent sans étiquette mais qui doivent être étiquetés avant d'être redirigés.

FEC	NHLFE

Ces éléments ne sont pas forcés de se trouver dans des tables séparées. En fait, la relation entre ces éléments dépend de l'implémentation actuelle du protocole de façon à utiliser les informations associées de manière optimale. Une des façons les plus courantes consiste à ajouter l'information des étiquettes dans la table ILM à celle de NHLFE, comme illustré ci-dessous.

Entry #	Input I/F	Input Label	Operation	Next Hop / Out I/F	Out Label

La table résultante est référée quelquefois par *Label Forwording Information Base* (LFIB).