Titre: Title:	Support des applications multimédia dans les réseaux de prochaine génération
Auteur: Author:	Georges Abou-Khalil
Date:	2013
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Abou-Khalil, G. (2013). Support des applications multimédia dans les réseaux de prochaine génération [Thèse de doctorat, École Polytechnique de Montréal]. PolyPublie. https://publications.polymtl.ca/1150/

UNIVERSITÉ DE MONTRÉAL

SUPPORT DES APPLICATIONS MULTIMÉDIA DANS LES RÉSEAUX DE PROCHAINE GÉNÉRATION

GEORGES ABOU-KHALIL
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

THÈSE PRÉSENTÉE EN VUE DE L'OBTENTION
DU DIPLÔME DE PHILOSOPHIÆ DOCTOR
(GÉNIE INFORMATIQUE)
JUIN 2013

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Cette thèse intitulée :

SUPPORT DES APPLICATIONS MULTIMÉDIA DANS LES RÉSEAUX DE PROCHAINE GÉNÉRATION

présentée par : ABOU-KHALIL Georges
en vue de l'obtention du diplôme de : Philosophiæ Doctor
a été dûment acceptée par le jury d'examen constitué de :

Mme BELLAÏCHE Martine, Ph.D., présidente
M. PIERRE Samuel, Ph.D., membre et directeur de recherche
M. CHAMBERLAND Steven, Ph.D., membre et codirecteur de recherche
M. QUINTERO Alejandro, Doct., membre
M. AJIB Wessam, Ph.D., membre

À ma future épouse Joëlle,
pour son amour inconditionnel.

À mes parents,
pour leur soutien permanent.

REMERCIEMENTS

J'aimerais, premièrement, remercier mon directeur de recherche, Prof. Samuel Pierre, ainsi que mon co-directeur de recherche, Prof. Steven Chamberland, pour leur support tout au long de mon parcours, tant au niveau technique, qu'au niveau financier.

J'aimerais également remercier le Fonds Québécois de la Recherche sur la Nature et les Technologies (FQRNT), ainsi que Ericsson Research Canada, pour m'avoir accordé la chance d'obtenir une bourse industrielle. Je remercie notamment Denis Monette, Laurent Marchand et Suresh Krishnan, qui m'ont guidé tout au long de mon séjour à l'industrie.

Finalement, je tiens à remercier tous mes collègues, aussi bien anciens qu'actuels, du LAboratoire de recherche en Réseautique et Informatique Mobile (LARIM). Nous avons passé de très bons moments ensemble et je ne retiens que de merveilleux souvenirs pendant mon séjour au LARIM. Une mention spéciale va à Angelo Rossi et Stéphane Ouellette, pour leur apport et collaboration au niveau technique, ainsi qu'à Valérie Justafort pour m'avoir corrigé les épreuves écrites.

RÉSUMÉ

Les applications multimédia sont devenues tellement populaires que certaines d'entre elles sont utilisées quotidiennement par les usagers. Cette popularité peut être attribuée à plusieurs facteurs, tels que la diversification du contenu et des services offerts, l'accès en tout temps grâce à la mobilité et à la nomadicité, ainsi qu'aux avancées au niveau des architectures et des protocoles utilisés, afin de supporter les requis plus exigeants de ces applications. Par exemple, ce qui était jadis un simple appel téléphonique, se transforme désormais en une vidéoconférence, permettant à un nombre dynamique d'usagers d'y participer. Un autre exemple d'application multimédia, qui connait également un essor fulgurant, est IP Tele-Vision (IPTV), soit la technologie permettant la transmission de la télévision, en direct et sur demande, sur des réseaux IP. On retrouve également sa version mobile, soit Mobile IP TeleVision (MobileTV).

Du côté des opérateurs, le focus est mis sur le déploiement des réseaux de prochaine génération. Les opérateurs sans-fil se tournent vers les technologies cellulaires de quatrième génération, telles que 3GPP Long Term Evolution (LTE), alors que ceux qui offrent les services filaires regardent plutôt vers les réseaux basés sur la fibre optique, tels que Fiber to the Home (FTTH). Ces réseaux promettent d'augmenter le débit offert, ainsi que de réduire la latence, soit deux critères importants pour le déploiement des applications multimédia à grande échelle. Malgré ces avancées technologiques, il existe encore plusieurs obstacles au bon fonctionnement des applications multimédia. Dans cette optique, cette thèse se penche sur trois problématiques importantes dans les réseaux de prochaine génération, chacune faisant l'objet d'un article scientifique.

Les deux premiers volets s'attardent sur la convergence des réseaux fixes et mobiles, ou Fixed-Mobile Convergence (FMC). Cette convergence vient brouiller la distinction entre les réseaux mobiles et les réseaux fixes. Entre autre, elle permet à un usager d'avoir accès à ses services, autant sur le réseau cellulaire (LTE, par exemple) que sur un réseau local (Wireless Fidelity (WiFi), par exemple). Pour s'y faire, l'usager est généralement muni d'un terminal pouvant se connecter sur les deux réseaux. La première problématique soulevée dans cette thèse est au niveau de la prise de décision de la relève. En effet, les deux protocoles de mobilité les plus populaires, soit Mobile IP (MIP) et Proxy Mobile IP (PMIP), adoptent deux approches diamétralement opposées. Avec le premier protocole, ce sont l'usager et son terminal qui prennent entièrement en charge la relève. Même si cette approche permet la FMC, les opérateurs préfèrent plutôt garder le contrôle sur la prise de décision, afin de pouvoir optimiser leur réseau. En effet, avec MIP, beaucoup de messages de signalisation

sont envoyés, ce qui gaspille des ressources réseaux, surtout au niveau de l'accès radio, la partie la plus précieuse du réseau. De plus, en ne sollicitant pas le réseau, le terminal ne prend pas nécessairement les meilleures décisions. Il peut donc basculer vers un réseau qui est plus chargé et qui ne garantit pas nécessairement ses exigences au niveau de la qualité de service. De ce fait, le protocole PMIP a été proposé. Son approche est exactement à l'opposé de celle de MIP, soit la mobilité qui est entièrement gérée par le réseau. De ce fait, la mobilité est masquée au niveau du terminal, qui pense toujours se trouver dans son réseau mère. Grâce à l'ajout de nouveaux nœuds dans le réseau, qui gèrent la mobilité à la place du terminal, on élimine la signalisation sur l'accès radio. De plus, les informations supplémentaires que le réseau détient lui permettront de prendre une meilleure décision. Par contre, le problème avec ce protocole est que, sans l'intervention du terminal, il lui est impossible de détecter toutes les situations de relèves. Dans plusieurs cas, le réseau fixe de l'opérateur est masqué par un réseau interne, par exemple un réseau WiFi, et la détection de ce réseau n'est possible que grâce à l'intervention du terminal. Ainsi, PMIP n'est pas un protocole qui se prête bien au déploiement de FMC.

Le premier article, qui s'intitule « *Client-Based Network-Assisted Mobile IPv6* », s'attaque donc à ce problème, en proposant un nouveau protocole, basé sur Mobile IP v6 (MIPv6), et qui introduit l'implication du réseau. Le résultat obtenu est un protocole hybride qui combine les avantages de MIPv6 et de Proxy Mobile IP v6 (PMIPv6). Pour s'y faire, deux étapes ont été nécessaires. La première consiste en une refonte du protocole MIPv6 qui, dans son état actuel, était difficile à modifier, à cause de ses spécifications qui sont lourdes. Le résultat de cette étape est un protocole beaucoup plus léger et offrant uniquement les fonctionnalités de base. Les autres fonctionnalités, telles que les mécanismes de sécurité, ont été séparées dans des modules. En deuxième lieu, un nouveau module a été proposé, qui introduit un nouveau nœud dans le réseau, capable de gérer la mobilité du terminal. Ainsi, la collaboration entre le terminal et ce nœud permet de réduire les messages de signalisation et d'optimiser les décisions au niveau des relèves, tout en offrant le support pour FMC.

La deuxième problématique, sur laquelle la thèse porte, se trouve au niveau de la transparence de la relève entre les deux réseaux. On parle d'une relève qui est transparente si cette dernière n'engendre aucune interruption des services de l'usager. Par exemple, un appel en cours, qui est démarré sur le réseau cellulaire, ne doit pas être interrompu lorsque la connexion bascule sur le réseau local, et vice-versa. Les applications visées, par notre travail, sont les applications multimédia en temps réél, notamment IPTV et MobileTV (en mode télévision en direct). Ces applications emploient des protocoles de multidiffusion permettant l'envoi optimisé de données à partir d'une ou de plusieurs sources vers plusieurs destinataires, avec un nombre minimal de paquets. Le problème avec ces applications est que, lorsqu'une

relève verticale survient (dans le cadre de FMC par exemple), la connexion est rompue et doit être réétablie. Ceci est dû au fait que le terminal change son adresse IP, ce qui le force à rejoindre ses services à partir de la nouvelle adresse. Cette déconnexion résulte en une perte de paquets, se traduisant par une interruption de l'application de l'usager.

Le second article, qui s'intitule « *Seamless handover for multicast Mobile IPv6 traffic* », propose une solution à ce problème. Cette solution consiste en l'ajout d'un nouveau nœud, dans le réseau, dont le rôle est de mettre en tampon les paquets perdus, lors de la relève du terminal. Ainsi, lorsque ce dernier recouvre sa connectivité, il est en mesure de récupérer ces paquets auprès de ce nœud. L'application de l'usager se déroule alors sans interruption.

La troisième problématique abordée dans cette thèse porte sur la planification des réseaux d'accès, afin de supporter les requis des applications multimédia au niveau du débit. Pour que la FMC soit réussie, il faut que le réseau local puisse supporter les débits nécessaires de l'application. Le réseau WiFi interne n'étant généralement pas un problème, la limitation se trouve plutôt au niveau de l'accès filaire. Afin d'augmenter les débits offerts, les opérateurs ont introduit la fibre optique dans leurs réseaux, complémentant ainsi les méthodes traditionnelles, tels les paires de cuivre torsadées et le câble coaxial. Ainsi, de nouvelles technologies optiques hybrides ont été proposées.

Dans un contexte où une infrastructure est déjà existante, le choix d'une technologie hybride est très attrayant, car l'opérateur peut rentabiliser son investissement précédent, minimisant ainsi le coût de la mise à jour. Par contre, dans un environnement vierge, il n'existe pas d'infrastructure à réutiliser. Le consensus, dans un tel scénario, est que la meilleure technologie à déployer est celle qui n'emploie que des liens en fibre optique, car elle offre les meilleurs débits ainsi que la plus grande flexibilité au niveau de l'évolutivité. La différence, au niveau du coût, devient moins grande et n'est plus nécessairement le critère principal au niveau du choix de la technologie à déployer.

Une des difficultés, qui compliquent la planification, est que ces réseaux sont souvent déployés par les opérateurs, en phases. La planification doit être alors dynamique et prendre en considération la nature évolutive de la demande des clients. Le troisième article, qui s'intitule « *Dynamic Greenfield Fiber to the Home Planning* », propose donc une modélisation dynamique du problème de planification des réseaux d'accès en fibre optique. Le résultat est un modèle mathématique linéaire, en nombres entiers, qui prend en entrée des paramètres, tels que les demandes des clients, et qui produit la planification minimisant le coût total du réseau et ce, sur plusieurs phases. Les résultats numériques obtenus en simulant notre modèle montrent sa supériorité par rapport aux méthodes séquentielles existantes.

ABSTRACT

Multimedia applications have been gaining momentum and are finding their way into everyday life. Their popularity can be attributed to several factors, such as the diversification of content and services, ubiquitous access thanks to the mobility and nomadicity, as well as advances in architectures and protocols used to support their most demanding requirements. For example, what was once a simple phone call has morphed nowadays into a videoconference, allowing a dynamic number of users to participate. Another example of a multimedia application that gained popularity is IP TeleVision (IPTV), which is the technology that allows the transmission of live and on demand television, on IP networks. There also exists a mobile version, called Mobile IP TeleVision (MobileTV).

From the operators' point of view, the focus is put on the deployment of next generation networks. Wireless operators are therefore deploying fourth generation cellular technologies, such as 3GPP Long Term Evolution (LTE), while those offering wired connectivity are looking into fiber optical based networks, such as Fiber to the Home (FTTH). These new networks increase the rate offered, as well as reduce latency, which are two important criteria for the deployment of large-scale multimedia applications. However, despite these advances, there still exist several obstacles hindering the proper operation of multimedia applications. This thesis therefore focuses on three important issues in next generation networks, each of these subjects leading to a scientific article.

The first two works deal with the issues of the Fixed-Mobile Convergence (FMC). This convergence is blurring the distinction between mobile and fixed networks. Among other things, it allows a user to have access to its services, both on the cellular network (LTE, for example) as well as on a local network (Wireless Fidelity (WiFi), for example). This is usually accomplished by equipping the user with a device with that can connect to both networks. The first issue raised in this thesis is about the decision of when to execute a handover. The two most popular mobility protocols, Mobile IP (MIP) and Proxy Mobile IP (PMIP), approach this problem with diametrically opposed views. With the first protocol, the decision is made by the user and his device. Although this approach allows for FMC, operators would much rather have complete control over the decision-making, in order to optimize their network. Indeed, with MIP, many signaling messages are sent, wasting valuable network resources, especially at the radio access, which is the most precious part of the network. Furthermore, by not involving the network, the decision taken by the device will not be necessarily optimal. It might request to switch to a more overloaded network, that cannot meet its demands of Quality of Service (QoS). For these reasons, the PMIP protocol

was proposed. Its approach is the opposite of that of MIP, the mobility being managed entirely by the network. By doing so, the device is actually shielded from any aspect of the mobility, and is fooled into thinking that it's always in its home network. This is possible by introducing new nodes in the networks that act on its behalf, which eliminates all signaling on the radio link. In addition, since the network is usually better suited to make the right decision, because of the additional information it holds, the mobility is optimized. However, the big issue that arises is that, without the intervention of the terminal, it is impossible to detect all the handover possibilities. In many cases, the operator's fixed network is hidden by an internal network, usually a WiFi network, and the detection of the network is only possible with the help of the terminal. Thus, PMIP is not a protocol that is well suited to deploy FMC.

The first article, entitled "*Client-Based Network-Assisted Mobile IPv6*", therefore addresses this problem by proposing a new protocol based on Mobile IP v6 (MIPv6), in which we introduce the involvement of the network. The result is a hybrid protocol that draws upon the strength of MIPv6 and Proxy Mobile IP v6 (PMIPv6). To accomplish this, two steps were required. The first consisted of a complete overhaul of the MIPv6 protocol, as in its current state, it was near impossible to make any modifications, because of the complexity and heaviness of its specifications. The result is a much more lightweight protocol which provides only basic functionality. Other features, such as security mechanisms, were separated into modules. In the second step, we proposed a new module, which introduces a new node in the network that can handle the terminal mobility. Thus, the collaboration of the terminal and the new node reduces the signaling messages and optimizes the decisions for handing over, while still offering support for FMC.

The second issue that this thesis tackles is the seamlessness of a handover between two networks. A handover is deemed seamless if it does not cause any disruption to the user's services. For example, a call that is in progress on the cellular network should not be interrupted when the connection switches to a local network, and the same goes for the other way around. The applications targeted by our work are multimedia applications operating in real-time , such as IPTV and MobileTV (in live television mode). These applications employ multicast protocols that are optimized for the transmission of data from one or more sources to multiple receivers, while using the minimum number of packets required. The problem, however, with these applications is that when a vertical handover occurs (in the case of FMC, for example), the connection is lost and must be re-established. This is because the terminal changes its IP address, which forces it to rejoin the services from the new address. This disconnection results in a packet loss, which entails an interruption of the user application.

The second article, entitled "*Seamless handover for multicast Mobile IPv6 traffic*", pro-

poses a solution to this problem. This is accomplished by introducing a new node in the network, whose role is to buffer the lost packets while the handover is occurring. Thus, when the device reconnects, it is able to recover these packets. The user application is therefore able to proceed without interruption.

The third issue addressed in this thesis focuses on the planning of access networks, to support the high bandwidth required by multimedia applications. For the FMC to be successful, it is necessary that the local network supports the bandwidth requirements. The internal WiFi network is generally not an issue, the limitation rather lies in the wired network. To increase the offered rates, operators have started introducing fiber optic links in their networks, complementing the traditional links, such as twisted pair copper and coaxial cable. Thus, new hybrid optical technologies have been proposed.

In a context where an infrastructure already exists, the choice of a hybrid technology is very attractive, because the operator can leverage its previous investment and minimize the cost of the upgrade. However, in a new environment, there is no infrastructure to reuse. Therefore, the consensus in such a scenario is that the best technology to deploy is the one that only uses fiber optic links, as it offers the best rates and the greatest scalability. The cost difference is smaller and therefore no longer the main criterion for selecting the technology to deploy.

One of the difficulties of network planning is that these networks are often deployed by operators in phases. Therefore, the planning must be dynamic and take into account the changing nature of customer demands. The third article, entitled "*Dynamic Greenfield Fiber to the Home Planning*", proposes a dynamic model for the network planning problem of fiber optic networks. The result is a linear integer mathematical model, which takes input parameters, such as customer demands, and produces a planning that minimizes the total cost of the network, over all of the phases. The numerical results obtained when simulating our solution show its superiority compared to existing sequential methods.

TABLE DES MATIÈRES

DÉDICACE iii

REMERCIEMENTS iv

RÉSUMÉ v

ABSTRACT viii

TABLE DES MATIÈRES xi

LISTE DES TABLEAUX xv

LISTE DES FIGURES xvi

LISTE DES SIGLES ET ABRÉVIATIONS xviii

CHAPITRE 1 INTRODUCTION 1
1.1 Définitions et concepts de base 2
1.1.1 Mobilité 2
1.1.2 Applications multimédia 4
1.1.3 Réseaux de prochaine génération 5
1.1.4 Multidiffusion 6
1.1.5 Qualité de l'expérience 8
1.2 Éléments de la problématique 8
1.3 Objectifs de recherche 11
1.4 Plan de la thèse 11

CHAPITRE 2 PLANIFICATION DES RÉSEAUX D'ACCÈS À HAUT DÉBIT, PROTOCOLES DE MOBILITÉ ET DE MULTIDIFFUSION 13
2.1 Technologies des réseaux d'accès à haut débit 13
2.1.1 Technologies d'accès des réseaux filaires 13
2.1.2 Technologies d'accès des réseaux sans-fil 20
2.2 Planification des réseaux d'accès filaires 24
2.2.1 Problématique 24
2.2.2 Approches de résolution 25

2.2.3 Réseaux d'accès à haut débits . . . 27
2.2.4 Planification dynamique . . . 27
2.3 Protocoles de mobilité . . . 28
2.3.1 MIPv6 . . . 28
2.3.2 PMIPv6 . . . 30
2.3.3 Comparaison des protocoles de mobilité . . . 31
2.4 La multidiffusion . . . 31
2.4.1 Protocoles de multidiffusion dans IP . . . 32
2.4.2 Problématique de la multidiffusion dans un environnement mobile . . . 33

CHAPITRE 3 DÉMARCHES DE L'ENSEMBLE DU TRAVAIL DE RECHERCHE . 37

CHAPITRE 4 CLIENT-BASED NETWORK-ASSISTED MOBILE IP version 6 (IPv6) 40
4.1 Introduction . . . 40
4.2 State Of The Art Of Mobile IP Protocols Suite . . . 41
4.2.1 Introduction . . . 41
4.2.2 Mobile IPv6 . . . 42
4.2.3 Proxy Mobile IPv6 . . . 44
4.3 Proposed Solution . . . 45
4.3.1 Overview of Our Solution . . . 46
4.3.2 Base Module . . . 46
4.3.3 Security Interface . . . 47
4.3.4 Modules . . . 48
4.3.5 Profiles . . . 49
4.3.6 Mobile Node Proxy . . . 50
4.4 Comparison Between Our Solution, MIPv6 and PMIPv6 . . . 52
4.4.1 Our solution vs MIPv6 . . . 52
4.4.2 Our solution vs PMIPv6 . . . 54
4.5 Conclusion . . . 54

CHAPITRE 5 SEAMLESS HANDOVER FOR MULTICAST MOBILE IPV6 TRAFFIC . . . 56
5.1 Introduction . . . 56
5.2 Related works . . . 58
5.2.1 Mobile IPv6 defined multicast solutions . . . 58
5.2.2 Other multicast solutions for MIPv6 . . . 60
5.2.3 Multicast solutions for MIPv6 variants . . . 60

5.2.4 Large scale multicast support . . . 61
5.3 Proposed solution . . . 61
5.3.1 Assumptions . . . 61
5.3.2 Overview of the proposed solution . . . 61
5.3.3 Modifications to Mobile IPv6 . . . 63
5.3.4 Reactive mode . . . 64
5.3.5 Buffer sizes . . . 65
5.3.6 Security . . . 66
5.3.7 Example scenario . . . 66
5.4 Simulation model and results . . . 67
5.4.1 Overview . . . 67
5.5 Conclusion and future works . . . 70

CHAPITRE 6 DYNAMIC GREENFIELD FIBER TO THE HOME PLANNING . . 73
6.1 Introduction . . . 73
6.2 Overview of broadband access network technologies . . . 75
6.2.1 Digital Subscriber Line (xDSL) . . . 75
6.2.2 Fiber to the Node (FTTN) Networks . . . 75
6.2.3 Fiber to the Home (FTTH) Networks . . . 76
6.2.4 Fiber to the Building (FTTB) Networks . . . 76
6.3 Related works . . . 77
6.3.1 Access network design . . . 77
6.3.2 Copper-based broadband access networks . . . 78
6.3.3 Passive Optical Network (PON) broadband access networks . . . 78
6.3.4 Dynamic access network planning . . . 79
6.4 Problem statement and optimization model . . . 80
6.4.1 Problem statement . . . 80
6.4.2 Example scenario . . . 80
6.4.3 Optimization model . . . 81
6.5 Solution and numerical results . . . 88
6.6 Conclusion . . . 90

CHAPITRE 7 DISCUSSION GÉNÉRALE . . . 94
7.1 Mobilité et multidiffusion . . . 94
7.2 Planification des réseaux d'accès filaires . . . 95

CHAPITRE 8 CONCLUSION ET RECOMMANDATIONS 97
8.1 Contributions de la thèse 97
8.2 Limitations de la thèse 98
8.3 Travaux futurs 99

RÉFÉRENCES 100

LISTE DES TABLEAUX

Tableau 2.1	Technologies xDSL	15
Tableau 2.2	Débit typique pour ADSL2+	16
Tableau 2.3	Standards WiFi (IEEE 802.11)	22
Tableau 2.4	Performance de WiMAX	24
Table 4.1	Comparison betweens protocols	54
Table 5.1	MIPv6 existing multicast solutions	59
Table 5.2	Initial buffer state	68
Table 5.3	Buffer state after handover	68
Table 5.4	Buffer state after first Multicast Buffer Send (MBSend)	68
Table 5.5	Buffer state after rejoiging multicast group	68
Table 5.6	Buffer state after recovery	68
Table 6.1	Overview of xDSL technologies	75
Table 6.2	Parameters and costs for the simulations	89
Table 6.3	Cost of links for Scenario 1 (clients 1 to 5)	90
Table 6.4	Cost of links for Scenario 1 (clients 6 to 10)	91
Table 6.5	Simulation results	93

LISTE DES FIGURES

Figure 1.1 Relève horizontale vs relève verticale . . . 3
Figure 1.2 Architecture de IPTV . . . 5
Figure 1.3 Exemple de multidiffusion . . . 7
Figure 1.4 Scénario de mobilité . . . 9
Figure 2.1 Différentes configurations de réseau . . . 14
Figure 2.2 Architecture d'un réseau xDSL . . . 15
Figure 2.3 Architecture d'un réseau FTTH (AON ou PON) . . . 17
Figure 2.4 Architecture d'un réseau FTTN . . . 18
Figure 2.5 Architecture d'un réseau FTTB . . . 19
Figure 2.6 Architecture d'un réseau HFC . . . 20
Figure 2.7 Architecture d'un réseau BPL . . . 21
Figure 2.8 Architecture d'un réseau LTE . . . 22
Figure 2.9 Arbre de recouvrement minimal avec capacité . . . 26
Figure 2.10 Protocoles de mobilité . . . 36
Figure 4.1 Overview of MIPv6 . . . 42
Figure 4.2 Overview of PMIPv6 . . . 45
Figure 4.3 MIPv6-compatible profile . . . 51
Figure 4.4 Route Optimization (RO) process . . . 53
Figure 4.5 RO process when handover occurs . . . 53
Figure 4.6 Bandwidth savings vs MIPv6 . . . 55
Figure 5.1 Multicast example . . . 59
Figure 5.2 Sequence diagram (proactive mode) . . . 62
Figure 5.3 Sequence diagram (reactive mode) . . . 66
Figure 5.4 MIPv6 handover scenario . . . 68
Figure 5.5 IP packets received with standard MIPv6 handover . . . 69
Figure 5.6 MIPv6 handover scenario with proposed solution . . . 70
Figure 5.7 IP packets received with proposed solution . . . 71
Figure 5.8 Undersized MBA buffer . . . 71
Figure 5.9 Buffer size vs packet loss . . . 71
Figure 6.1 Broadband access network technologies . . . 77
Figure 6.2 Example scenario . . . 81
Figure 6.3 Optimal solution . . . 82
Figure 6.4 Solution using sequential method . . . 83

Figure 6.5 Solution using backtrack method 84
Figure 6.6 Scenario 1 90
Figure 6.7 Optimal solution of Scenario 1 91
Figure 6.8 Solution of Scenario 1 using sequential method 92
Figure 6.9 Solution of Scenario 1 using backtrack method 92
Figure 6.10 Comparison of obtained costs for 16 scenarios 93

LISTE DES SIGLES ET ABRÉVIATIONS

2G	2nd Generation
3G	3rd Generation
3GPP	3rd Generation Partnership Project
4G	4th Generation
ADSL	Asymmetric digital subscriber line
ADSL2+	Asymmetric digital subscriber line 2+
AMPL	A Mathematical Programming Language
AMT	Automatic Multicast Tunneling
AON	Active Optical Network
AS	Autonomous System
ASM	Any Source Multicast
BA	Binding Acknowledgment
BE	Binding Error
BGP	Border Gateway Protocol
BPL	Broadband Power Lines
BU	Binding Update
CATV	Cable Television
CDMA	Code-Division Multiple Access
CIDR	Classless Inter-Domain Routing
CO	Central Office
CoA	Care-of-Address
CMST	Capacitated Minimum Spanning Tree
CN	Correspondant Node
DBA	Delegated Binding Acknowledgment (BA)
DBS	Direct Broadcast Satellite
DBU	Delegated Binding Update (BU)
DHAAD	Dynamic Home Agent Address Discovery

DHCP	Dynamic Host Configuration Protocol
DOCSIS	Data Over Cable Service Interface Specification
DSLAM	Digital Subscriber Line Access Multiplexer
DSMIPv6	Dual Stack MIPv6
EDGE	Enhanced Data rates for GSM Evolution
EPC	Evolved Packet Core
EPON	Ethernet Passive Optical Network
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
FDM	Frequency Division Multiplexing
FDMA	Frequency-Division Multiple Access
F-HMIPv6	Fast Handover for Hierarchical MIPv6
FMC	Fixed-Mobile Convergence
FMIPv6	Fast Handovers for Mobile IPv6
FQRNT	Fonds Québécois de la Recherche sur la Nature et les Technologies
FTTB	Fiber to the Building
FTTC	Fiber to the Curb
FTTH	Fiber to the Home
FTTN	Fiber to the Node
FR	Foreign Router
GbE	Gigabit Ethernet
GPON	Gigabit PON
GPRS	General Packet Radio Service
GSM	Global System for Mobile communications
GTP	GPRS Tunneling Protocol
HA	Home Agent
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure
HFC	Hybrid Fiber-Coaxial
HMIP	Hierarchical MIP
HMIPv6	Hierarchical MIPv6

HoA	Home Address
HR	Home Router
HSPA	High Speed Packet Access
HSPA+	Enhanced HSPA
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGMPv1	Internet Group Management Protocol v1
IGMPv2	Internet Group Management Protocol v2
IGMPv3	Internet Group Management Protocol v3
IKE	Internet Key Exchange
IKEv2	Internet Key Exchange (IKE) version 2
ILP	Integer Linear Programming
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
IPSec	IP Security
IPTV	IP TeleVision
ITU-T	International Telecommunication Union-Telecommunication
L2	Data-Link Layer
L3	Network Layer
L7	Application Layer
LARIM	LAboratoire de recherche en Réseautique et Informatique Mobile
LMA	Local Mobility Anchor
LMDS	Local Multipoint Distribution Service
LoS	Line of Sight
LP	Linear Programming
LTE	3GPP Long Term Evolution
MA	Multicast Agent
MAG	Mobile Access Gateway

MAP	Mobility Anchor Point
MBA	Multicast Buffering Agent
MBStart	Multicast Buffer Start
MBSend	Multicast Buffer Send
MBStop	Multicast Buffer Stop
MBAck	Multicast Buffer Ack
MBError	Multicast Buffer Error
MCMST	Multicenter Capacitated Minimum Spanning Tree
MDU	Multiple Dwelling Units
MIP	Mobile IP
MIPv4	Mobile IP v4
MIPv6	Mobile IP v6
MLD	Multicast Listener Discovery
MLDv1	Multicast Listener Discovery v1
MLDv2	Multicast Listener Discovery v2
MMDS	Multichannel Multipoint Distribution Service
MN	Mobile Node
MobileTV	Mobile IP TeleVision
MS	Multicast Source
MST	Minimum Spanning Tree
NGN	Next-Generation Network
NGA	Next-Generation Access
nMAG	new Mobile Access Gateway (MAG)
OLT	Optical Line Terminal
OMIPv6	Optimizing MIPv6
ONT	Optical Network Terminal
ONU	Optical Network Unit
OPNET	Optimized Network Engineering Tool
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First

PBA	Proxy BA
PBU	Proxy BU
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast (PIM) Dense Mode
PIM-SM	PIM Sparse Mode
PIM-SSM	PIM Source-Specific Multicast
PMIP	Proxy Mobile IP
PMIPv6	Proxy Mobile IP v6
PON	Passive Optical Network
PRA	Proxying Request Acknowledgment
PRI	Proxying Request Initiation
PSTN	Public Switched Telephone Network
QoS	Quality of Service
QoE	Quality of Experience
RA	Router Advertisement
RAN	Radio Access Network
RF	Radio Frequency
RIP	Routing Information Protocol
RO	Route Optimization
RP	Rendez-vous Point
RTP	Real-time Transport Protocol
SA	Security Association
SDO	Standards Developing Organization
SDSL	Symmetric Speed Digital Subscriber Line
SMA	Simultaneous Multi-Access
SSM	Source-Specific Multicast
TDM	Time-Divison Multiplexing
TDMA	Time-Division Multiple Access
UMTS	Universal Mobile Telecommunications System
UTRAN	Universal Terrestrial Radio Access Network

VDSL	Very High Speed Digital Subscriber Line
VoD	Video on-Demand
VoIP	Voice over IP
W-CDMA	Wideband Code-Division Multiple Access
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
xDSL	Digital Subscriber Line

CHAPITRE 1

INTRODUCTION

Les applications multimédia ont connu un essor phénoménal, ces dernières années, et leur usage ne cesse de croitre auprès des usagers. Leur popularité est due, d'une part, à la grande diversité du contenu et des services offerts et, d'autre part, à l'amalgame de dispositifs sur lesquels elles sont disponibles (allant des petits écrans d'appareils mobiles aux grands écrans haute définition). Ce sont les résultats d'avancées technologiques au niveau des réseaux qui ont permis d'offrir ces services à une plus grande échelle, car il faut pouvoir satisfaire certains requis, tels que le grand débit nécessaire. Pour cette raison, l'explosion de ces applications a un impact majeur sur les réseaux des fournisseurs. Les défis se situent autant au niveau de l'architecture de ces réseaux, qu'au niveau des protocoles utilisés pour déployer ces services. Ainsi, si la planification n'est pas à point, l'expérience des usagers en souffrira, se traduisant généralement par une baisse de revenus.

Cette thèse a donc pour objectif de s'attaquer à plusieurs lacunes des réseaux de prochaine génération, dans le but d'assurer un support adéquat aux applications multimédia. Deux volets portent sur la mobilité des nœuds, plus précisément sur les relèves. Les protocoles de mobilités les plus populaires sont Mobile IP (MIP) et Proxy Mobile IP (PMIP). Avec le premier, c'est le mobile qui gère entièrement les relèves. Ceci ne permet pas d'optimiser ce processus, car le réseau n'est pas sollicité. Le second, quant à lui, effectue la gestion de la mobilité entièrement par le réseau. Le problème qui survient alors est que certaines relèves ne sont pas possibles, sans la collaboration du nœud mobile. Notre premier travail propose donc un nouveau protocole de mobilité, basé sur Mobile IP v6 (MIPv6), qui permet de balancer la gestion de la mobilité entre le nœud mobile et le réseau. Le résultat obtenu est ainsi un protocole hybride.

Un autre problème qui survient lors d'une relève est que, lorsque cette dernière entraîne un changement d'adresses Internet Protocol (IP), les applications multimédia en temps réel sont perturbées, dû à la déconnexion qui engendre des paquets perdus. À cause de leur mode de transmission en multidiffusion, et de par leur nature temps réel, il n'est pas possible de récupérer ces paquets perdus. Ainsi, la fluidité de l'expérience de l'usager en souffre. Notre second travail s'attaque donc à ce problème, en proposant l'ajout d'un nouveau nœud dans le réseau et en modifiant le protocole de mobilité, afin de permettre à ce nœud de mettre en mémoire-tampon les paquets perdus lors de la relève. Ainsi, lorsque le nœud mobile aura terminé d'effectuer sa relève, et donc aura réétabli sa connectivité, il pourra récupérer les

paquets perdus auprès de ce nœud.

Le troisième volet, quand à lui, s'attaque plutôt aux architectures des réseaux d'accès filaires. Une des problématiques posées par les applications multimédia se trouve au niveau du débit requis, et les réseaux d'accès sont généralement perçus comme le goulot d'étranglement dans la chaîne de connectivité d'un client. Il existe plusieurs technologies possibles pour déployer un réseau d'accès dans les réseaux de prochaine génération. Par contre, le consensus, pour la planification d'un réseau d'accès dans un environnement sans infrastructure existante, est que la meilleure solution est le déploiement de la fibre optique de bout en bout. Elle offre le meilleur débit possible et il s'agit de l'option la plus évolutive. Par contre, elle requiert un plus gros investissement que ses alternatives. De plus, avec la nature dynamique et évolutive des réseaux et des demandes des clients, il devient primordial d'effectuer les bons choix dans toutes les phases d'installation, afin d'optimiser le réseau dans son ensemble. Notre objectif est donc de proposer une planification évolutive des réseaux d'accès en fibre optique, dans un environnement sans infrastructure existante.

Ce chapitre d'introduction commence par présenter certaines définitions et concepts de base, qui serviront d'ancrage à la compréhension des sujets abordés. Ensuite, les différents objectifs de recherche sont énoncés. Enfin, le plan de la thèse va clore ce chapitre.

1.1 Définitions et concepts de base

Cette section présente au lecteur les définitions et concepts de base, qui seront utiles lors de la présentation des travaux existants, ainsi que de ceux proposés.

1.1.1 Mobilité

La mobilité est un concept assez vaste et, de ce fait, on distingue deux types de mobilité, soit la mobilité du terminal et la mobilité personnelle. Lorsque le mot mobilité est mentionné tout court, on réfère généralement à la mobilité au niveau du terminal. Elle permet à un usager de pouvoir se déplacer dans un réseau, sans interruption de ses services. L'emphase est alors mise sur l'équipement de l'usager, qui doit posséder une interface radio, lui permettant de se déplacer entre plusieurs points d'accès. Ce déplacement, entre deux points d'accès, est appelé une relève.

La mobilité personnelle, quant à elle, met l'emphase sur l'abonné qui, peu importe son emplacement dans le réseau, doit pouvoir s'identifier afin de retrouver ses services personnels. Appelé également le nomadisme, ce mécanisme n'implique donc pas de relève au niveau du terminal et ne requiert pas d'interface radio au niveau des équipements impliqués. L'usager doit, par contre, pouvoir être identifiable, en utilisant, par exemple, une carte d'accès et un

code personnel.

La mobilité peut être implémentée à plusieurs niveaux dans le modèle Open Systems Interconnection (OSI) : à la couche liaison (Data-Link Layer (L2)), à la couche IP (Network Layer (L3)) ou encore à la couche application (Application Layer (L7)). Dans le cas où la mobilité est gérée entièrement par la couche liaison, on parle alors de micro-mobilité. Dans ce cas, l'adresse IP du mobile reste inchangée et la mobilité n'est pas apparente au niveau des applications, car les connexions en cours ne sont généralement pas perturbées. Par contre, si le mobile doit changer d'adresse, la couche IP est nécessairement également impliquée. Dans ce cas-ci, on parle plutôt de macro-mobilité, et les connexions en cours vont être interrompues. Lorsqu'elle est implémentée à la couche application, c'est à l'application de gérer la relève. La gestion devient donc dépendante du type de l'application, car elles ne sont pas toutes affectées de la même manière par une relève.

Finalement, on distingue deux types de relèves, soit les relèves horizontales et les relèves verticales. Les relèves horizontales se produisent lorsqu'un nœud mobile se déplace entre deux points d'accès de même technologie. Si ce déplacement s'effectue plutôt entre deux point d'accès de différentes technologies, on parle alors d'une relève verticale. Les relèves verticales engendrent généralement davantage de signalisation et prennent plus de temps à s'effectuer. Une relève est considérée transparente lorsque les services de l'usager ne sont pas perturbés ou interrompus pendant son exécution. La figure 1.1 illustre la différence entre les deux types de relèves.

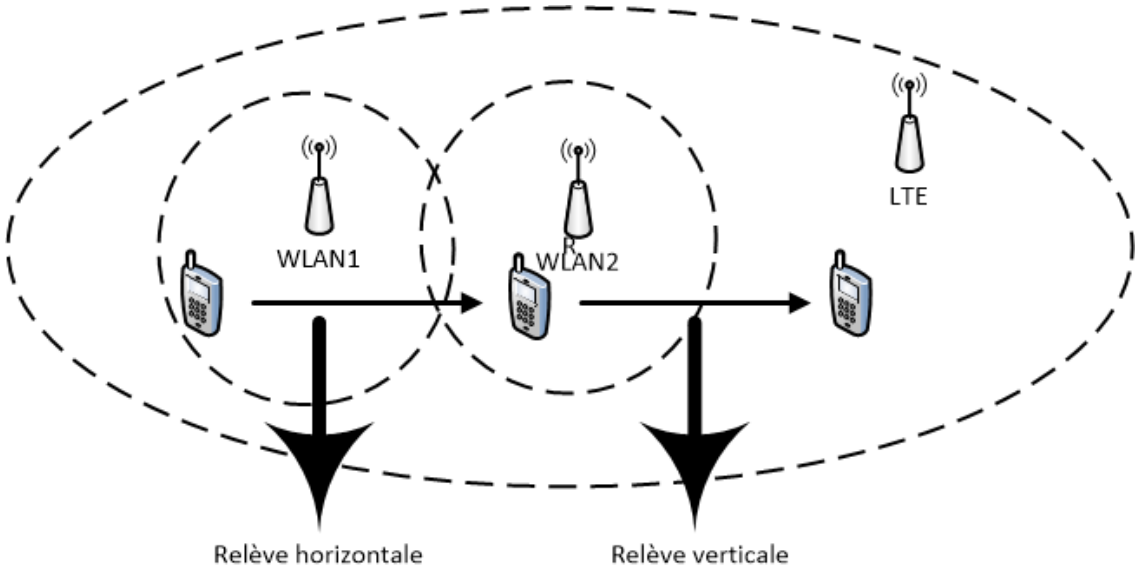


Figure 1.1 Relève horizontale vs relève verticale

1.1.2 Applications multimédia

Comme nous l'avons énoncé auparavant, les applications multimédia ont gagné énormément en popularité auprès des usagers. Il existe plusieurs types d'applications multimédia, chacune avec ses propres caractéristiques, mais également ses propres défis au niveau de son déploiement. On peut regrouper les applications multimédia en deux familles, soit les applications en temps réel et les applications sur demande.

Les applications multimédia en temps réel sont celles où le contenu est produit (par une ou plusieurs sources) et consommé (généralement par plusieurs clients) dans un intervalle de temps très court. Les deux applications multimédia en temps réel les plus populaires sont la télévision en direct et la vidéoconférence. La première est celle où des sources, généralement fixes et connues d'avance, diffusent un flôt multimédia en temps réel. Les clients abonnés à ces sources vont recevoir les données quelques instants après leur diffusion. La vidéoconférence se distingue de la télévision en directe par le fait que les usagers jouent à la fois le rôle de sources et de clients. Ceci complique davantage l'implémentation, vu que les sources ne sont plus connues d'avance, mais sont désormais dynamiques. Il faut donc prévoir un mécanisme pour constamment mettre à jour la liste de ces sources. De plus, les requis aux niveau de la latence sont beaucoup plus strictes, à cause de la nature interactive de ces applications. Ce requis est moins stricte pour la télévision en direct, car l'expérience de l'usager n'est pas affectée si celui-ci perçoit l'information avec un certain délai. Ceci permet donc l'implémentation de techniques de mise en mémoire-tampon (« buffering ») au niveau du nœud, ce qui a pour but d'amortir et d'éliminer la gigue. On peut donc distinguer ces applications comme étant des applications quasi-temps réel.

Les applications multimédia en temps réel sont donc des applications où une même donnée est envoyée vers plusieurs clients à la fois. Leur nature se marie parfaitement à la multidiffusion, concept qui sera présenté plus tard dans ce chapitre. Cela permet de réduire énormément le débit requis pour l'envoi, surtout autour de la source. Par contre, la multidiffusion présente ses propres défis qui peuvent dégrader l'expérience de l'usager.

L'autre famille d'applications multimédia est celle qui offre le contenu sur demande, telle que la vidéo sur demande ou Video on-Demand (VoD). Ces applications permettent aux usagers d'accéder à des services et à des contenus à leur guise, donc généralement à n'importe quel moment désiré. Contrairement aux applications en temps réel, chaque usager reçoit un flôt différent, qui correspond au contenu demandé, à un instant donné. Ainsi, la multidiffusion est rarement utilisée pour ce genre d'applications. Afin d'optimiser leur réseau, les fournisseurs vont plutôt se pencher vers des serveurs de cache placés proches des clients. Ceci permet donc de raccourcir le lien entre les clients et la source du contenu, réduisant ainsi les délais et les ressources utilisées. Ces serveurs vont généralement héberger les contenus les plus populaires,

qui représentent généralement la majorité de la demande des clients.

Une des technologies multimédia qui devient populaire est IP TeleVision (IPTV), permettant d'offrir à la fois la télévision en direct et la télévision sur demande. Il s'agit de la technologie permettant de diffuser la télévision sur un réseau utilisant le protocole IP. Les méthodes traditionnelles étant la diffusion terrestre, la câblo-diffusion et la diffusion par satellite, IPTV se distingue en offrant plusieurs avantages très attrayants, tant aux opérateurs, qu'aux usagers. D'une part, elle permet une réduction des coûts grâce à sa meilleure efficacité de gestion du débit et aux possibilités d'offres groupées avec les services de voix, d'Internet et de téléphone. D'autre part, elle offre une meilleure interactivité grâce à sa nature bi-directionnelle, permettant d'offrir des services plus avancés, tels que des guides interactifs. De plus, elle offre de meilleurs mécanismes de chiffrement et de protection des données, un aspect qui est très important pour les gestionnaires de contenus. La figure 1.2 présente l'architecture d'un réseau capable d'offrir des services IPTV.

On note également le protocole Mobile IP TeleVision (MobileTV), qui permet aux usagers d'avoir accès à IPTV et ce, peu importe leur emplacement, en prenant en considération la nomadicité et la mobilité.

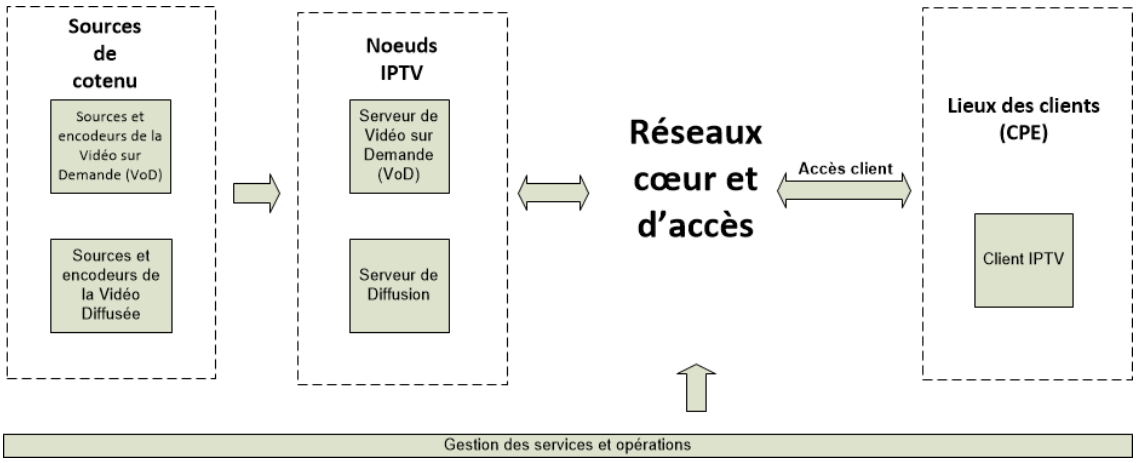


Figure 1.2 Architecture de IPTV

1.1.3 Réseaux de prochaine génération

Les réseaux de prochaine génération, ou Next-Generation Network (NGN), désignent un ensemble de changements architecturaux, tant au niveau des réseaux dorsaux, qu'au niveau des réseaux d'accès, et dont l'objectif principal est que le réseau transporte tout type d'informations et de services (voix, vidéo, données, etc...) par commutation de paquets, similaire au fonctionnement sur Internet. Ils utilisent donc le protocole IP pour le transport.

La définition des NGNs qui est donnée par International Telecommunication Union-Telecommunication (ITU-T) est la suivante : « *A Next-Generation Network (NGN) is a packet-based network able to provide services including Telecommunication Services and able to make use of multiple broadband, Quality of Service (QoS)-enabled transport technologies and in which service-related functions are independent from underlying transport-related technologies. It offers unrestricted access by users to different service providers. It supports generalized mobility which will allow consistent and ubiquitous provision of services to users.* »

Les NGNs permettent une séparation entre la partie transport du réseau et les services qui y sont offerts. Cette séparation permet à un fournisseur de déployer de nouveaux services sans devoir apporter de modification à la partie transport. Dans les réseaux dorsaux traditionnels, plusieurs réseaux de transport existaient pour différents services. Le changement implique donc une migration vers un seul réseau de transport dorsal, basé sur IP et Ethernet. Plus précisément, ceci implique la migration du service de voix, traditionnellement effectuée en commutation de circuits (Public Switched Telephone Network (PSTN)), vers un service sur IP, soit Voice over IP (VoIP). De plus, d'autres services patrimoniaux (« legacy »), tels que X.25 et frame relay, sont migrés vers des services entièrement en IP.

Les réseaux d'accès doivent également migrer vers des réseaux d'accès de prochaine génération, appelés Next-Generation Access (NGA). L'objectif des NGA est d'offrir aux clients des accès à haut débit afin de pouvoir profiter des capacités supérieures offertes par les réseaux dorsaux des NGNs. Dans les réseaux filaires, ceci est possible en déployant de la fibre optique, qui peut ensuite être complémentée par des liens traditionnels, tels que les réseaux Digital Subscriber Line (xDSL) ou câbles coaxiaux. Ces différentes technologies filaires seront présentées, en détail, au prochain chapitre.

Des réseaux d'accès sans-fil, ou Radio Access Network (RAN), de prochaine génération ont également été proposés, les deux plus populaires étant 3GPP Long Term Evolution (LTE) et Worldwide Interoperability for Microwave Access (WiMAX). Ces deux technologies permettent aux opérateurs d'offrir des accès sans-fil avec de plus hauts débits et de meilleures latences que ceux offerts par les technologies qu'elles remplacent. Elles seront également présentées, plus en détail, au prochain chapitre.

1.1.4 Multidiffusion

Dans un réseau IP, trois méthodes de transmission sont possibles. La première, soit l'envoi individuel ou unicast, permet la transmission de données d'une source vers un seul client. Elle est donc de type point à point ; il s'agit de la méthode de transmission la plus utilisée dans les réseaux traditionnels. La deuxième, soit la diffusion générale ou broadcast, permet l'envoi de données d'une source vers tous les clients dans un domaine de diffusion (généralement appar-

tenant à un même sous-réseau donné). Il s'agit donc d'une liaison de type point à multipoint. La troisième est la multidiffusion, appelée également diffusion groupée ou multicast.

La multidiffusion est le mécanisme par lequel un nœud peut transmettre à un ensemble précis de destinaires, tout en minimisant le nombre requis de paquets envoyés. En effet, la source n'a besoin d'envoyer qu'un seul paquet et ce sont les nœuds intermédiaires qui sont en charge de dupliquer ce paquet, lorsque nécessaire. Ceci réduit considérablement le nombre de paquets dans le réseau comparativement à l'envoi individuel, surtout autour de la source.

Afin d'illustrer le fonctionnement de la multidiffusion, prenons l'exemple présenté à la figure 1.3. Si l'on désire acheminer un paquet de la source vers les destinations (clients hachurés), en multidiffusion, il suffit que la source envoie un seul paquet. Ce paquet sera ensuite dupliqué par le routeur 1, en envoyant une copie vers chacun des routeurs 2 et 3. Ensuite, le routeur 2 va acheminer deux copies de ce paquet vers les deux destinations qu'il dessert. Le routeur 3, lui, doit également envoyer deux fois ce paquet, soit vers une destination qu'il dessert et vers le routeur 4. Finalement, le routeur 4 achemine une copie vers chacune des deux destinations qu'il dessert. Au total, en utilisant la multidiffusion, il y a eu 9 paquets transmis. Si le mode de transmission avait été l'envoie individuel, ce nombre serait 17. Dans notre cas, on observe donc un gain de 47%.

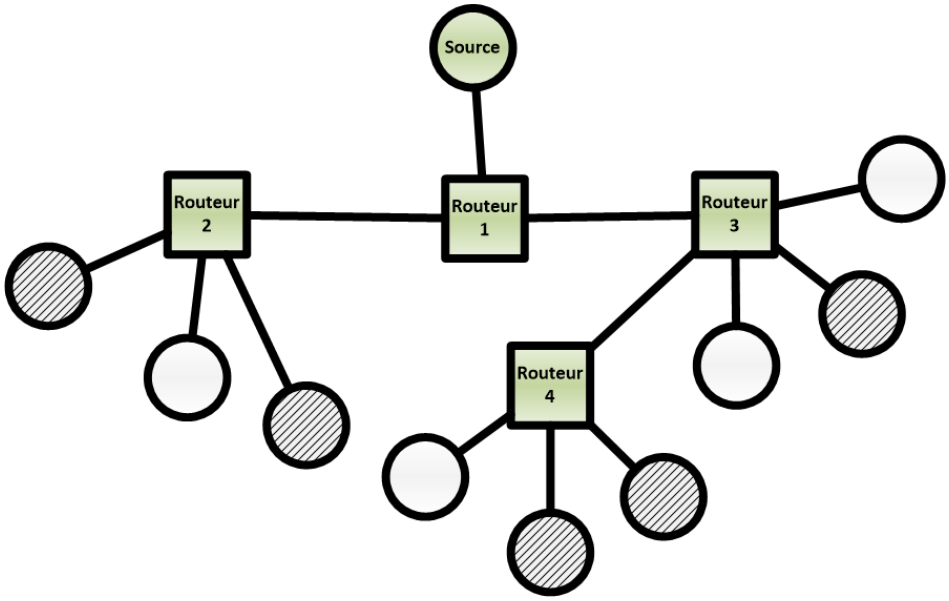


Figure 1.3 Exemple de multidiffusion

Afin de permettre la multidiffusion dans un réseau IP, l'opérateur doit déployer des protocoles qui permettent aux clients de se souscrire à des groupes de multidiffusion et qui permettent aux nœuds intermédiaires de bien relayer l'information. Il existe des protocoles

pour les réseaux IP version 4 (IPv4) ainsi que leurs équivalents pour les rseaux IP version 6 (IPv6). Ceux-ci seront présentés au prochain chapitre.

Finalement, on note que, contrairement à IPv4, IPv6 n'implémente pas directement la diffusion générale. En effet, pour avoir un résultat similaire, la source doit transmettre, par multidiffusion, vers une adresse de destination spécifique (« all-hosts »). Cette modification, apportée à IP, permet aux interfaces d'ignorer les transmissions qu'elles ne désirent pas recevoir. En IPv4, les interfaces doivent absolument traiter tous les paquets qui sont envoyés par diffusion générale. Il s'agit donc d'une optimisation apportée au protocole IPv6.

1.1.5 Qualité de l'expérience

La qualité de l'expérience, ou Quality of Experience (QoE) est une mesure subjective de l'expérience de l'usager par rapport à un service qu'il reçoit. Son objectif est donc d'établir des métriques, afin de mesurer les facteurs qui influencent la qualité perçue par l'usager. Par exemple, si on prend IPTV comme application, une mesure serait le délai perçu lors d'un changement de chaîne (« zappage »). Évidemment, plus ce délai est petit, meilleure est l'expérience perçue. La difficulté, par contre, se trouve au niveau de la subjectivité de la mesure, car un délai, qui peut être considéré acceptable par une personne, ne le serait pas nécessairement par une autre. La QoE implique donc une évaluation humaine des attentes, sensations, perceptions, cognitions et satisfaction vis-à-vis d'un service donné (ur Rehman Laghari *et al.*, 2011).

Une autre famille de mesures, liée à la QoE, est la qualité de service ou QoS. Cette dernière établit des mesures qui sont objectives, pour évaluer le service offert. Ces mesures sont généralement au niveau de la performance du réseau, plutôt qu'au niveau de la perception de l'usager. Celles-ci incluent, par exemple, le débit offert, la latence ou encore la gigue. Il est donc plus facile d'établir des requis au niveau des métriques de la QoS et de les faire respecter. Par contre, ceci ne donne aucune garantie au niveau de la QoE. On peut se retrouver dans des scénarios où toutes les métriques de QoS sont satisfaites mais que la QoE reportée par un usager est inacceptable. L'inverse peut également survenir, où la QoE de l'usager est satisfaisante, sans pour autant respecter une ou plusieurs métriques de QoS.

1.2 Éléments de la problématique

L'explosion des applications multimédia amène de nouvelles problématiques aux fournisseurs, tant au niveau de la planification de leurs réseaux, qu'au niveau des protocoles utilisés. De plus, avec la mobilité qui est de plus en plus prédominante, les usagers s'attendent à avoir accès à leurs services en tout temps, à tout lieu et ce, avec plus ou moins la même qualité

d'expérience.

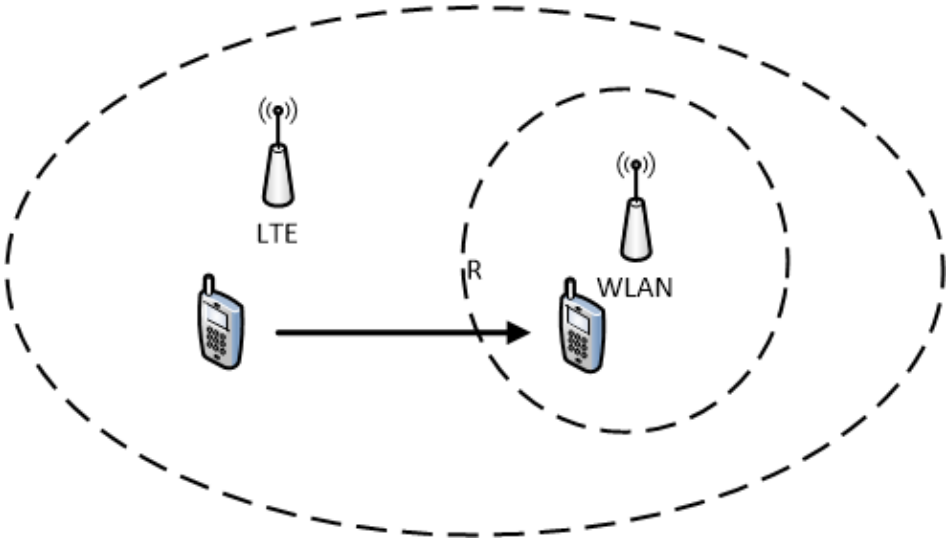


Figure 1.4 Scénario de mobilité

Prenons le scénario illustré à la Figure 1.4. L'usager dispose d'un appareil mobile possédant deux antennes, une qui peut s'associer à un réseau LTE et l'autre à un réseau Wireless Fidelity (WiFi). Supposons maintenant que l'usager soit souscrit à un service IPTV et reçoit donc le flôt de données sur son appareil mobile. À l'instant 1, il est connecté au réseau LTE. Ensuite, lors de son déplacement, l'usager entre dans la portée d'un réseau WiFi, à son domicile. À cet instant, un choix doit être fait. Est-ce que l'usager reste connecté au réseau LTE ou bien est-ce qu'il bascule sur le réseau WiFi ? Cette décision peut être motivée par un aspect financier. En effet, si on se place du côté de l'usager, si son abonnement LTE est à un prix fixe, il n'a aucun incitatif de faire le changement, si ses exigences de QoS sont déjà respectées. Par contre, si son abonnement est facturé à l'utilisation, il a grand intérêt à minimiser les transferts de donnéées sur son interface LTE et il devrait alors basculer vers WiFi dès que possible. Du point de vue du fournisseur, les motivations sont bien évidemment l'inverse. Si l'abonnement est à un taux fixe, celui-ci a tout intérêt que son client utilise le moins souvent les fréquences réservées à LTE, car celles-ci sont précieuses et dispendieuses.

D'un point de vue technologique, le problème se trouve au niveau de quelle entité doit gérer cette relève, ce qui dépend du protocole de mobilité utilisé. S'il s'agit d'un protocole de mobilité où la gestion des relèves est effectuée au niveau du nœud mobile, tel que MIPv6, l'usager a le contrôle complet des relèves. Ceci n'implique donc pas le réseau, ce qui rend les fournisseurs réticents à déployer de tels protocoles. Ils veulent garder le contrôle sur l'accès à leur réseau, afin de pouvoir optimiser son utilisation. Pour cette raison, des protocoles de mobilité, où la gestion de la mobilité est effectuée par le réseau, ont été proposés, tels que

Proxy Mobile IP v6 (PMIPv6). L'avantage est évidemment que les fournisseurs gardent le contrôle complet, car c'est le réseau qui effectue toutes les relèves. La mobilité est alors masquée à l'usager, et son terminal garde toujours l'adresse de son réseau-mère. Par contre, si on considère toujours notre scénario, le problème avec un tel protocole est que, sans l'implication du nœud mobile, il est impossible au réseau LTE de détecter la présence du réseau WiFi et d'effectuer la relève. En effet, les relèves horizontales sont facilement gérées, car les points d'accès, étant de même technologie, impliquent la même interface et sont également sous le contrôle du même fournisseur. Quand il s'agit plutôt de relèves verticales, comme dans notre scénario, celles-ci ne sont pas possibles à gérer par le réseau, car il s'agit de deux technologies différentes. Même si le fournisseur LTE et le fournisseur de la connexion à domicile sont la même entité, le réseau WiFi est un réseau interne qui ne transmettra pas l'information nécessaire afin de pouvoir détecter la possibilité de la relève. Dans un tel scénario, l'implication du nœud mobile est donc nécessaire afin de pouvoir effectuer la relève.

Un autre problème survient lorsque la relève est effectuée, et celui-ci est dû au fait que l'adresse IP du nœud mobile change. En effet, un changement d'adresse implique une terminaison de toutes les connexions en cours. Pour la multidiffusion, il faut donc que le mobile s'abonne de nouveau à l'arbre, avec sa nouvelle adresse IP. Ainsi, pendant le temps requis au nœud mobile pour rejoindre l'arbre, des paquets sont perdus, se traduisant par une interruption de l'expérience de l'usager. Dans le cas d'un service sur demande, cette interruption, quoique désagréable, n'entraîne pas nécessairement une perte de paquets, car l'application peut toujours récupérer l'information perdue. Par contre, pour les applications en temps réel, ces paquets perdus ne sont pas recouvrables, car l'information est multidiffusée en temps réel et il est impossible de redemander les paquets perdus. Dans le cas d'une vidéo par exemple, ceci se traduit par une perte de trames.

Finalement, un prérequis pour que la relève soit efficace dans notre scénario est de s'assurer que la connexion à domicile puisse supporter le haut débit requis par l'application multimédia. Le réseau WiFi interne ne pose généralement pas de problème. Avec les protocoles 802.11n et 802.11ac, les débits offerts sont généralement supérieurs à ceux de la connexion à Internet. C'est donc cette dernière qui représente le goulot d'étranglement. Il devient alors important que le réseau, notamment le réseau d'accès, puisse supporter les hauts débits requis par ces applications. Bien que plusieurs technologies d'accès existent, celle qui est considérée comme étant la meilleure est celle qui ne contient que des liens de types optique, de bout en bout, soit Fiber to the Home (FTTH).

À partir de notre scénario, nous avons recensé trois problèmes qui peuvent perturber autant l'expérience de l'usager que la bonne gestion du fournisseur. Ainsi, les éléments de la problématique peuvent se résumer aux trois questions suivantes, qui mèneront vers les

objectifs de recherche, chacun faisant l'objet d'un des articles présentés dans cette thèse :

- Comment gérer les relèves verticales afin de s'assurer que les ressources du réseau, surtout au niveau de l'accès, soient utilisées de manière optimale ?
- Comment assurer une expérience sans interruption pour un usager mobile, lorsque ce dernier reçoit un service multimédia en temps réel et qu'une macro-mobilité survient ?
- Comment s'assurer que le réseau d'accès puisse supporter les applications multimédia, qui sont reputées être gourmandes au niveau du débit requis ?

1.3 Objectifs de recherche

L'objectif de cette thèse est de proposer des améliorations aux réseaux de prochaine génération, afin de mieux supporter les applications multimédia, autant au niveau de l'architecture des réseaux qu'au niveau des protocoles déployés. Plus spécifiquement, cette thèse vise à :

1. proposer une refonte du protocole MIPv6 en séparant les fonctionalités de base des autres fonctionalités, telle la sécurité, ce qui amènera à un module de base et des modules d'extension ;
2. proposer une interface de sécurité entre le module de base et les modules de sécurité, ce qui permettra de créer plusieurs modules de sécurité basés sur différents protocoles ;
3. concevoir un module qui s'intègre au protocole simplifié et qui ajoute un nouveau nœud dans le réseau capable de gérer la mobilité du mobile, tout en prenant en considération l'état du mobile (système hybride) ;
4. proposer un nouveau nœud à MIPv6 permettant d'assurer une relève transparente pour les applications multimédia en temps réel lors d'un changement d'adresse suite à une relève ;
5. proposer une planification des réseaux d'accès filaires optiques satisfaisant la demande dynamique des clients, dans un environnement complètement nouveau (« greenfield »).

1.4 Plan de la thèse

Après avoir introduit les concepts et notions de base dans ce chapitre, le chapitre 2 présentera, en détail, les architectures des réseaux de prochaine génération et les protcoles assurant la transmission des applications multimédia et ceux de la gestion de la mobilité. De plus, les travaux scientifiques les plus pertinents seront présentés, tant au niveau de la planification des réseaux, qu'au niveau des protocoles énoncés. Dans le chapitre 3, nous décrirons les démarches de l'ensemble du travail de recherche.

Le chapitre 4 présente le texte intégral d'un article publié intitulé « *Client-Based Network-Assisted Mobile IPv6* ». Cet article propose une refonte complète du protocole MIPv6, en y retirant toutes les fonctionalités qui ne sont pas essentielles (la sécurité par exemple). Ensuite, on y propose le concept de modules et de profils, pour étendre les fonctionalités de base, de manière structurée. Finalement, on y propose un module qui ajoute la gestion de la mobilité par le réseau, permettant ainsi la collaboration entre le nœud mobile et un nœud du réseau, pour optimiser les relèves.

Le chapitre 5 présente le texte intégral d'un article intitulé « *Seamless handover for multicast Mobile IPv6 traffic* ». Dans ce dernier, on y propose une amélioration au niveau de la multidiffusion pour le protocole MIPv6. Cette amélioration permet aux usagers mobiles d'avoir une expérience sans interruption, lorsqu'ils reçoivent un service multimédia en temps réel et qu'une macro-mobilité survient. Le fonctionnement repose sur l'ajout d'un nouveau nœud qui effectue la mise en mémoire-tampon des paquets lors de la relève et qui les renvoie, au nœud, une fois que ce dernier réétablit sa connectivité au réseau.

Le chapitre 6 présente le texte intégral d'un article intitulé « *Dynamic Greenfield Fiber to the Home Planning* ». Celui-ci propose une planification des réseaux d'accès en fibres optiques de bout en bout. Cette planification est destinée aux déploiements sans infrastructures existantes et prend en compte la nature dynamique et évolutive du réseau. Le résultat est un modèle mathématique en nombres entiers, qui sera utilisé pour résoudre différents scénarios générés aléatoirement. Les résultats sont alors comparés à ceux obtenus avec les méthodes séquentielles existantes.

Une discussion générale, en regard des aspects méthodologiques et des résultats obtenus au cours de cette recherche et en lien avec la revue de littérature, est présentée au chapitre 7. Finalement, le chapitre 8 conclut la thèse en effectuant la synthèse de tous les travaux effectués et en exposant leurs limitations et les travaux futurs potentiels.

CHAPITRE 2

PLANIFICATION DES RÉSEAUX D'ACCÈS À HAUT DÉBIT, PROTOCOLES DE MOBILITÉ ET DE MULTIDIFFUSION

Ce chapitre présente, d'une part, une revue des différentes technologies d'accès des réseaux à haut débit de prochaine génération, incluant les travaux les plus pertinents portant sur la planification de ces réseaux. Dans un second temps, les protocoles de mobilité et les protocoles de multidiffusion les plus populaires, y sont présentés, suivis d'une revue des principaux travaux retrouvés dans la littérature, portant sur la problématique de la multidiffusion dans un environnement mobile.

2.1 Technologies des réseaux d'accès à haut débit

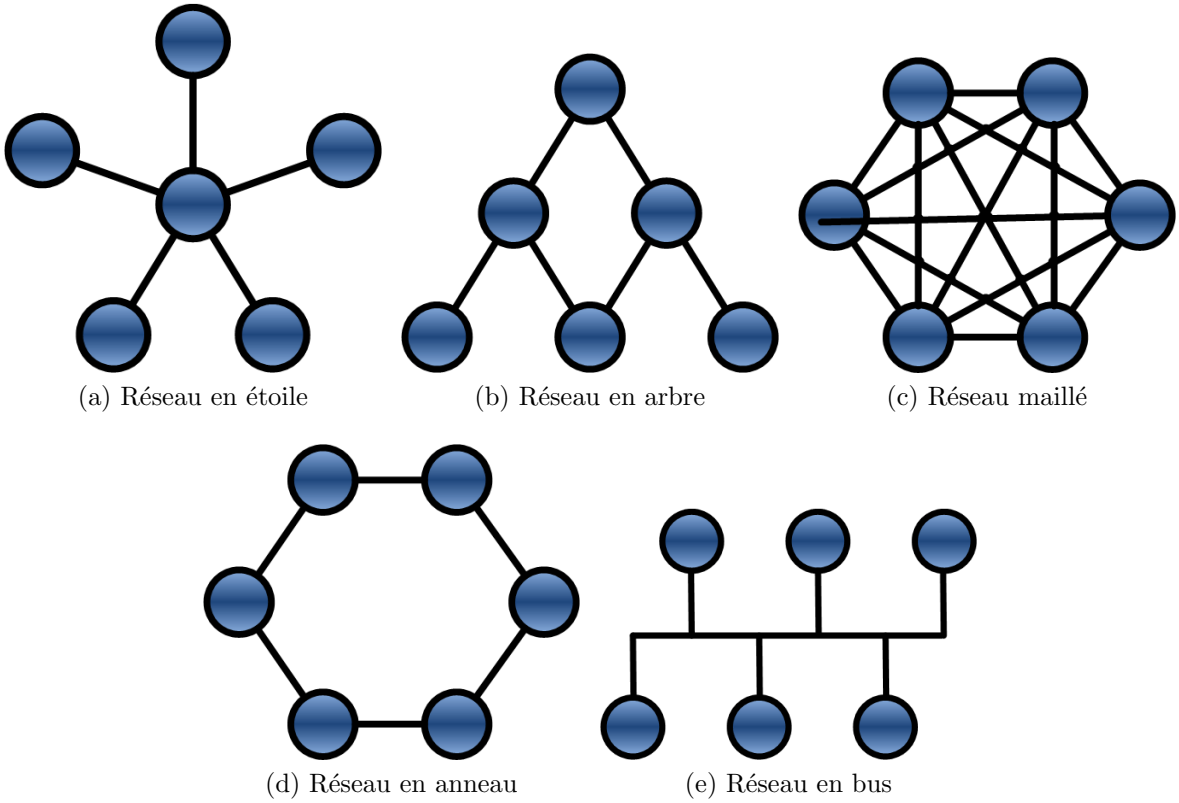
Les réseaux d'accès à haut débit peuvent être regroupés en deux familles, soient les réseaux filaires et les réseaux sans-fil. La première famille englobe toutes les technologies dont la connectivité est assurée par un lien physique, câblé, entre le client et le fournisseur. Différentes configurations sont possibles pour les réseaux filaires, soient les réseaux en étoile (2.1a), les réseaux en arbre (2.1b), les réseaux maillés (2.1c), les réseaux en anneau (2.1d) et les réseaux en bus (2.1e). La deuxième famille, quant à elle, regroupe toutes les technologies employant des fréquences radio (Radio Frequency (RF)) ou des faisceaux hertziens (« microwave ») pour assurer la connectivité.

2.1.1 Technologies d'accès des réseaux filaires

Traditionnellement, les réseaux d'accès filaires les plus populaires étaient au nombre de deux, soient les réseaux basés sur les paires de fils de cuivre torsadées et les réseaux basés sur les câbles coaxiaux. Cependant, afin de supporter de plus hauts débits, la fibre optique a été introduite dans les réseaux d'accès, ce qui a abouti à de nouvelles technologies. Les prochaines sous-sections feront la revue des différents types de ces réseaux.

Les réseaux xDSL

xDSL est la technologie qui permet la transmission de données grâce aux infrastructures téléphoniques existantes (paires de cuivre torsadées). Traditionnellement, les paires de cuivre ne servaient qu'à transporter la voix, le débit étant limité à 3,4 kHz. Cependant, le débit



(a) Réseau en étoile (b) Réseau en arbre (c) Réseau maillé

(d) Réseau en anneau (e) Réseau en bus

Figure 2.1 Différentes configurations de réseau

possible est beaucoup plus grand, dans les Megahertz (cette capacité est inutilisée pour le service téléphonique de base). En allouant une plage de fréquences différente pour les données, il est donc possible d'offrir un service à haut débit et ce, sans interférer avec le service téléphonique existant. Il existe plusieurs variantes de xDSL, la plupart étant de nature asymétrique (débit plus grand en aval qu'en amont). Le Tableau 2.1 présente les principales caractéristiques des technologies xDSL les plus populaires, soit Asymmetric digital subscriber line (ADSL) (ITU-T, 1999b), Symmetric Speed Digital Subscriber Line (SDSL) (ITU-T, 2003), Asymmetric digital subscriber line 2+ (ADSL2+) (ITU-T, 1999a) et Very High Speed Digital Subscriber Line (VDSL) (ITU-T, 2004).

Dans un réseau xDSL, chaque client possède un lien point-à-point entre son modem et un Digital Subscriber Line Access Multiplexer (DSLAM), qui est en charge d'effectuer l'agrégation des trafics, via multiplexage, des différents clients qui y sont reliés. Le trafic obtenu est ensuite acheminé vers le réseau fédérateur de l'opérateur. Le DSLAM opère au niveau de la couche 2 du modèle OSI (L2), similaire à un commutateur de réseaux. La Figure 2.2 présente l'architecture typique d'un réseau xDSL.

L'avantage des réseaux xDSL est le fait de pouvoir réutiliser une infrastructure déjà existante, ce qui a été une motivation majeure pour son déploiement. Leur désavantage majeur

est qu'ils sont très sensibles aux distances. En effet, plus le client est loin, moins le débit offert est grand. Ceci est dû au fait que les paires de câbles ont une grande atténuation pour les hautes fréquences. D'autres facteurs, tels que l'interférence ou la qualité du réseautage domestique, peuvent également avoir un impact négatif sur le débit offert. Le Tableau 2.2 présente l'influence de la distance du client sur le débit offert avec la technologie ADSL2+.

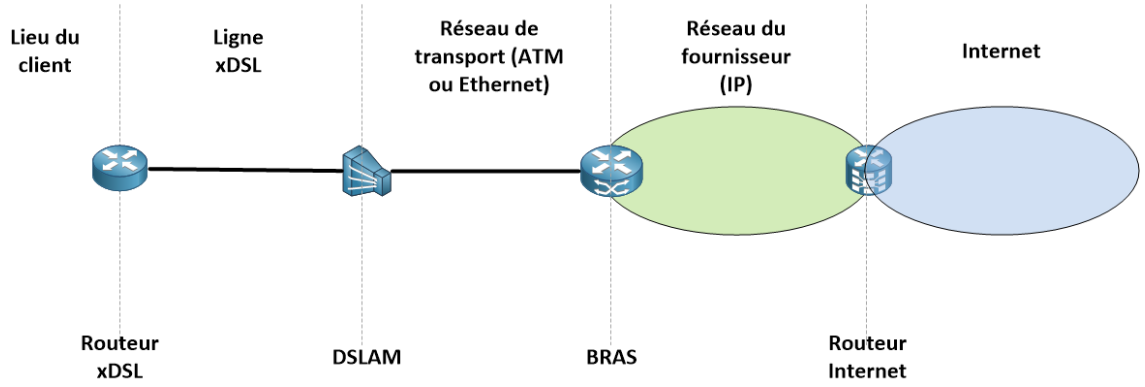


Figure 2.2 Architecture d'un réseau xDSL

Les réseaux FTTH

Les réseaux FTTH offre une connectivité tout en fibre, du Central Office (CO) jusqu'aux lieux des clients. Le déploiement le plus courant consiste en quelques liens en fibre optique, partant du CO, et qui sont ensuite divisés, pour être distribués à chaque client. Deux technologies existent, soit les réseaux Active Optical Network (AON) et les réseaux Passive Optical Network (PON), la différence se trouvant au niveau de la manière de diviser la fibre optique. Dans un réseau AON, ce sont des noeuds actifs qui sont utilisés pour effectuer cette division. Le signal optique est converti, en premier lieu, vers un signal électrique, pour ensuite être converti, à nouveau, vers un signal optique. Ces noeuds peuvent être soit des commutateurs, soit des routeurs, et effectuent une commutation de paquets au niveau 2 ou au niveau 3 (le routage au niveau 3 s'effectue généralement au niveau du CO). Un exemple de technologie

Tableau 2.1 Technologies xDSL

Technologie	Débit maximal en aval	Débit maximal en amont	Distance maximale
ADSL	640 Kbps	12 Mbps (0.3km)	5.4 km (1.5 Mbps)
SDSL	3 Mbps	3 Mbps	2.7 km (2 Mbps)
ADSL 2+	1 Mbps	26 Mbps (0.3km)	3.6 km (4 Mbps)
VDSL	16 Mbps	52 Mbps (0.3km)	1.3 km (13 Mbps)

Tableau 2.2 Débit typique pour ADSL2+

Vitesse	Distance
25 Mbit/s	300 m
24 Mbit/s	600 m
23 Mbit/s	900 m
22 Mbit/s	1.2 km
21 Mbit/s	1.5 km
19 Mbit/s	1.8 km
16 Mbit/s	2.1 km
8 Mbit/s	3 km
1.5 Mbit/s	4.5 km
800 kbit/s	5.2 km

basée sur AON est « active ethernet », qui emploie des commutateurs optiques Ethernet pour distribuer le signal, formant ainsi un large réseau commuté Ethernet entre les clients et le CO.

Les réseaux PON, quant à eux, emploient des noeuds passifs pour distribuer le signal. Il s'agit de séparateurs de faisceaux qui divisent le signal optique sans le convertir et qui n'ont pas besoin d'être alimentés. Les deux technologies PON les plus populaires sont Gigabit PON (GPON) (Hood (2012)) et Ethernet Passive Optical Network (EPON) (Beck (2005)). Elles permettent le transfert de données sur une seule fibre, qui est ensuite séparée en plusieurs fibres, se terminant chez les clients. La transmission des données, vers les clients, s'effectue en mode diffusion générale (« broadcast »). Tous les clients reçoivent alors le même signal et c'est grâce à des techniques d'adressage que chaque client peut identifier ses propres données. Souvent, le chiffrement est également utilisé afin d'éviter les écoutes non-autorisées. Pour les données allant des clients au CO, Time-Divison Multiplexing (TDM) est utilisé afin d'éviter les collisions au niveau de la fibre partagée.

La figure 2.3 illustre un exemple d'un réseau de type FTTH, la différence entre AON et PON se trouvant au niveau du type du nœud.

Les réseaux Fiber to the Node (FTTN)

Les réseaux FTTN sont des réseaux hybrides, où la fibre optique est utilisée du CO jusqu'à un noeud situé à proximité des clients. La terminaison des liens est ensuite assurée par des paires torsadées de câbles en cuivre, qui se terminent dans un modem xDSL. Les noeuds destinés aux FTTN sont responsables de la conversion optique à électrique et sont installés dans des cabinets. Ces derniers doivent être alimentés et doivent endurer des conditions

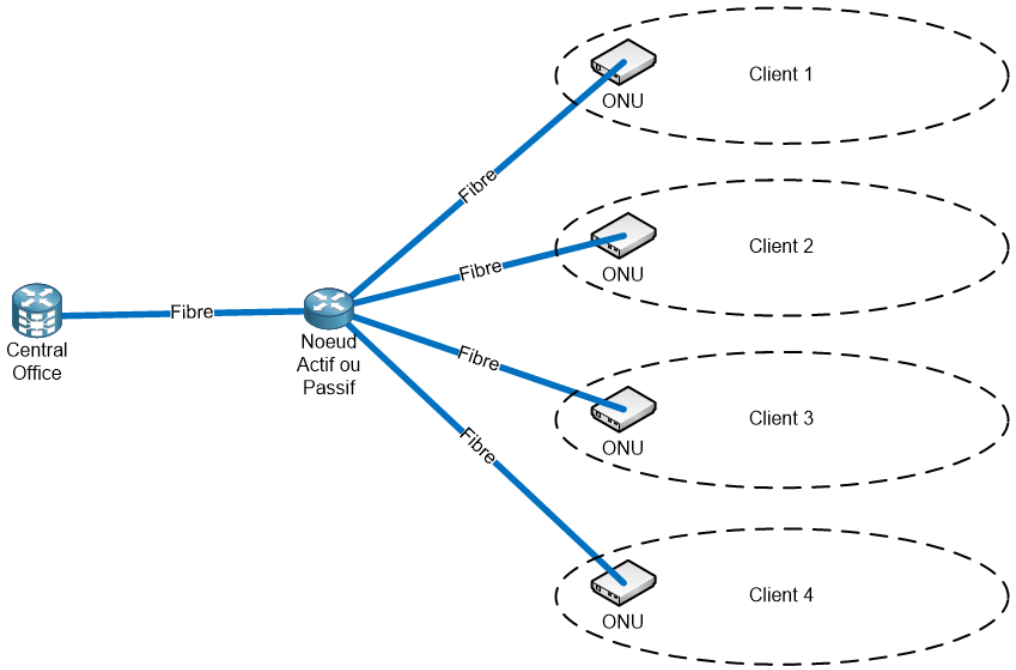


Figure 2.3 Architecture d'un réseau FTTH (AON ou PON)

extrêmes, telles que les hautes et basses températures et la foudre. Similaire aux réseaux xDSL, le débit offert par un réseau FTTN dépend fortement de la longueur des câbles de cuivre (donc de la distance entre le client et le noeud). Afin d'atteindre un haut débit, il est généralement requis que cette distance soit limitée à 300 mètres, ce qui permet l'utilisation de VDSL. On désigne parfois ce type de réseau comme étant un réseau de type Fiber to the Curb (FTTC), afin de mettre l'emphase sur le fait que le cabinet est installé très proche des clients.

La figure 2.4 illustre un exemple d'un réseau de type FTTN.

Les réseaux Fiber to the Building (FTTB)

Les réseaux FTTB sont un autre type de réseau hybride. Ils peuvent être vus comme un hybride entre les réseaux PON et les réseaux FTTN. Dans un tel réseau, la fibre se termine dans un noeud qui est placé chez le client. Ensuite, c'est un réseau distinct qui termine la connexion. Ce réseau peut être de n'importe quelle nature, autre qu'optique, par exemple un réseau xDSL ou Gigabit Ethernet (GbE). Étant hébergé chez le client, le cabinet n'a pas besoin d'être aussi résistant que dans un réseau FTTN, puisqu'il se trouve dans un emplacement où les conditions sont contrôlées. L'utilisation primaire d'un réseau FTTB est pour servir une unité résidentielle multiple (Multiple Dwelling Units (MDU)).

La figure 2.5 illustre un exemple d'un réseau de type FTTB.

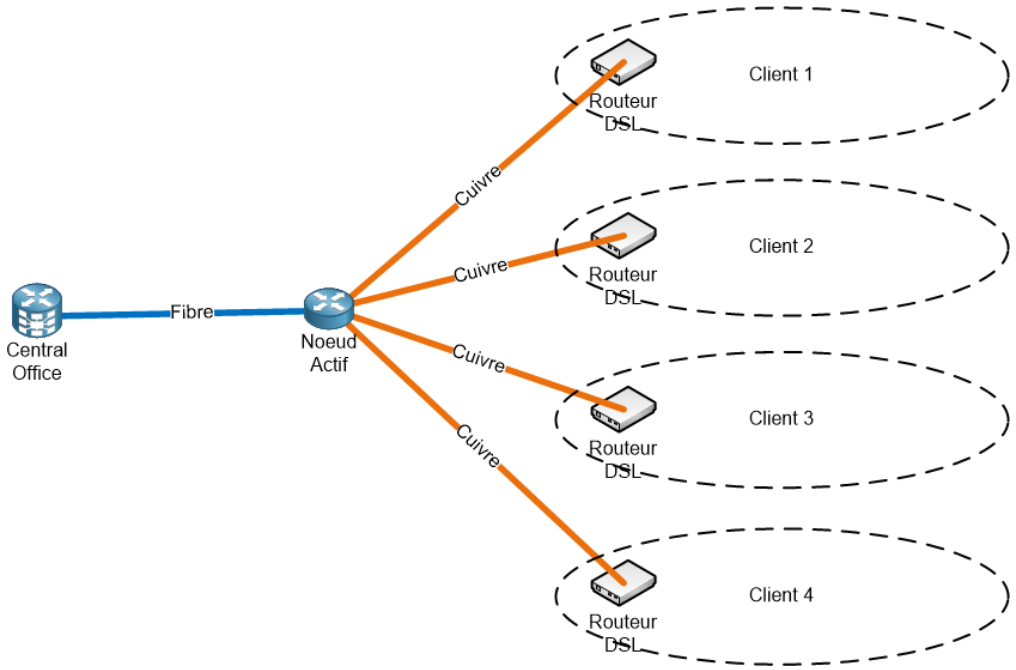


Figure 2.4 Architecture d'un réseau FTTN

Les réseaux câblés et Hybrid Fiber-Coaxial (HFC)

Les réseaux de câbles coaxiaux, ou Cable Television (CATV), sont un autre type de réseau permettant la transmission de données à haut débit. Ils utilisent les infrastructures de câbles coaxiaux existantes. Similaires aux réseaux FTTN, les réseaux HFC, sont des réseaux hybrides, où la première partie de la connectivité est assurée grâce à une fibre optique allant jusqu'à un noeud. Ce noeud est responsable de la conversion optique-électrique et à partir duquel on retrouve un réseau CATV, qui termine la connectivité. Cette partie dessert typiquement une population de 500 clients, en utilisant une configuration de type « tree-and-branch ». Les réseaux HFC ont remplacé la quasi-totalité des réseaux CATV traditionnels.

Les réseaux HFC permettent aux opérateurs d'offrir plusieurs services, tels que la télévision analogue, la télévision numérique (définitions standard et haute), la vidéo sur demande, la téléphonie et Internet. Les services sont acheminés par RF (5 Mhz à 1000 Mhz) et Frequency Division Multiplexing (FDM) est utilisé pour la différenciation entre les différentes données. Le standard le plus populaire, pour déployer des réseaux HFC, est Data Over Cable Service Interface Specification (DOCSIS). La dernière version de ce protocole, soit 3.0, permet à un fournisseur d'offrir des débits très intéressants, pouvant dépasser les 200 Mbps en aval.

La figure 2.6 illustre un exemple d'un réseau de type HFC.

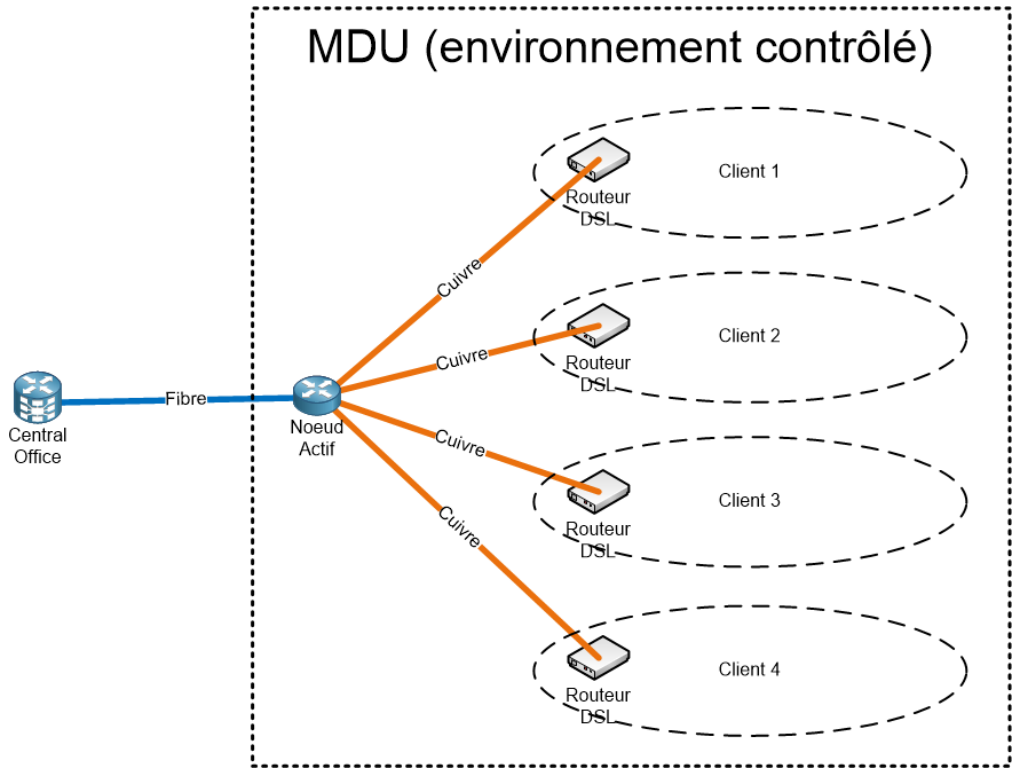


Figure 2.5 Architecture d'un réseau FTTB

Les réseaux Broadband Power Lines (BPL)

Les réseaux BPL permettent la transmission de données à haut débit, à travers le réseau électrique déjà existant, ce qui leur permet donc de desservir tous les clients qui s'y rattachent. La transmission est assurée par un signal à bas voltage, qui est envoyé sur de hautes fréquences ; ces dernières sont choisies de manière à minimiser les interférences possibles avec le signal électrique déjà existant. Les débits atteints par les premiers essais n'étaient pas très élevés (2 à 3 Mbps), mais des avancées technologiques promettent de biens meilleurs débits (jusqu'à 200 Mbps).

Cependant, les réseaux BPL n'ont pas eu de succès au niveau du déploiement à cause de plusieurs facteurs. D'abord, des contraintes technologiques limitent la portée du signal à environ 1 km (il est cependant possible d'étendre cette portée en augmentant le voltage utilisé). De plus, l'investissement requis pour le déploiement, afin d'offrir un service fiable et à haut débit, est élevé. Finalement, le signal est souvent confronté à des problèmes d'interférences (les transmissions radio amateur par exemple) et d'atténuation de signal. Pour toutes ces raisons, il est très peu probable que cette technologie soit déployée à grande échelle.

La figure 2.7 illustre un exemple d'un réseau de type BPL.

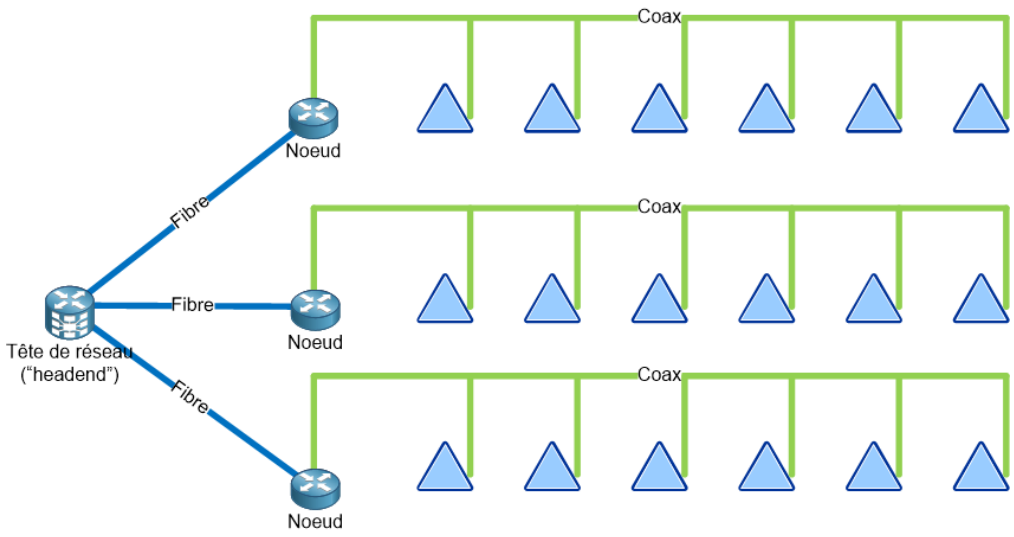


Figure 2.6 Architecture d'un réseau HFC

2.1.2 Technologies d'accès des réseaux sans-fil

Les technologies sans-fil sont celles qui acheminent l'information grâce à des signaux employant des fréquences RF ou des faisceaux hertziens, en utilisant l'air comme médium de transmission. Elles peuvent être regroupées en deux familles, dépendamment de si elles requièrent la visibilité directe (Line of Sight (LoS)) ou non. Même s'il est possible de les utiliser dans le réseau dorsal, les réseaux sans-fil sont employés presqu'exclusivement dans les réseaux d'accès.

Dans cette sous-section, nous effectuerons la revue des principales technologies d'accès sans-fil, soit 3GPP Long Term Evolution , Wireless Fidelity et Worldwide Interoperability for Microwave Access. Nous terminerons par un survol des autres technologies existantes.

Les réseaux LTE

LTE est un standard de communication sans-fil pour réseaux cellulaires, défini par 3rd Generation Partnership Project (3GPP). Ce consortium inclut un ensemble de manufacturiers et d'opérateurs à travers le monde et est responsable de produire les spécifications des technologies cellulaires les plus populaires à travers le monde, comptant environ 6 milliards d'abonnés. Plus précisément, on y retrouve :

– les technologies de deuxième génération, ou 2nd Generation. Celles-ci incluent Global System for Mobile communications (GSM) qui utilise Time-Division Multiple Access (TDMA) et Frequency-Division Multiple Access (FDMA) pour offrir le service de voix et de données jusqu'à 8 Kbps. Ensuite, General Packet Radio Service (GPRS) et Enhanced

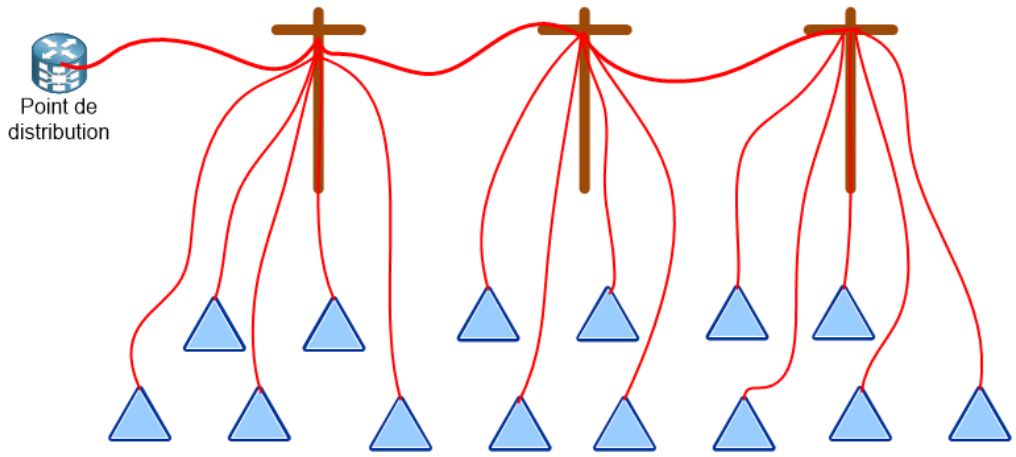


Figure 2.7 Architecture d'un réseau BPL

Data rates for GSM Evolution (EDGE) ont été ajoutées, permettant d'atteindre des débits de 144 Kbps et 236 Kbps, respectivement ;

– les technologies de troisième génération, ou 3rd Generation. Celles-ci incluent Universal Mobile Telecommunications System (UMTS) qui utilise Code-Division Multiple Access (CDMA) pour offrir des débits jusqu'à 384 Kbps, ainsi que High Speed Packet Access (HSPA) et Enhanced HSPA (HSPA+) qui permettent d'augmenter le débit offert jusqu'à 42 Mbps ;
– les technologies de quatrième génération, ou 4th Generation. Celles-ci incluent un nouveau réseau coeur basé entièrement sur IP, soit le Evolved Packet Core (EPC). On y retrouve également une nouvelle technologie radio, LTE qui vient s'ajouter aux technologies GSM et Wideband Code-Division Multiple Access (W-CDMA) et sur laquelle est basé un nouveau réseau d'accès radio appelé Evolved Universal Terrestrial Radio Access Network (E-UTRAN). Finalement, la combinaison du EPC et du E-UTRAN est connue sous le nom de Evolved Packet System (EPS).

La figure 2.8 présente l'architecture d'un réseau de type LTE.

Les réseaux WiFi

WiFi est une techonlogie d'accès sans-fil très populaire, permettant l'échange de données à haut débit dans un réseau informatique. Il existe plusieurs versions de cette technologie, incluant 802.11b, 802.11g, 802.11a, 802.11n et 802.11ac, qui sont toutes définies par « Wi-Fi Alliance ». La transmission est effectuée sur des spectres de fréquences qui ne sont pas régulés, soit 2,4 Ghz et 5,8 Ghz. Ces fréquences permettent une bonne pénétration du signal, ce qui réduit la puissance requise pour l'envoi tout en maintenant une portée d'environ 30

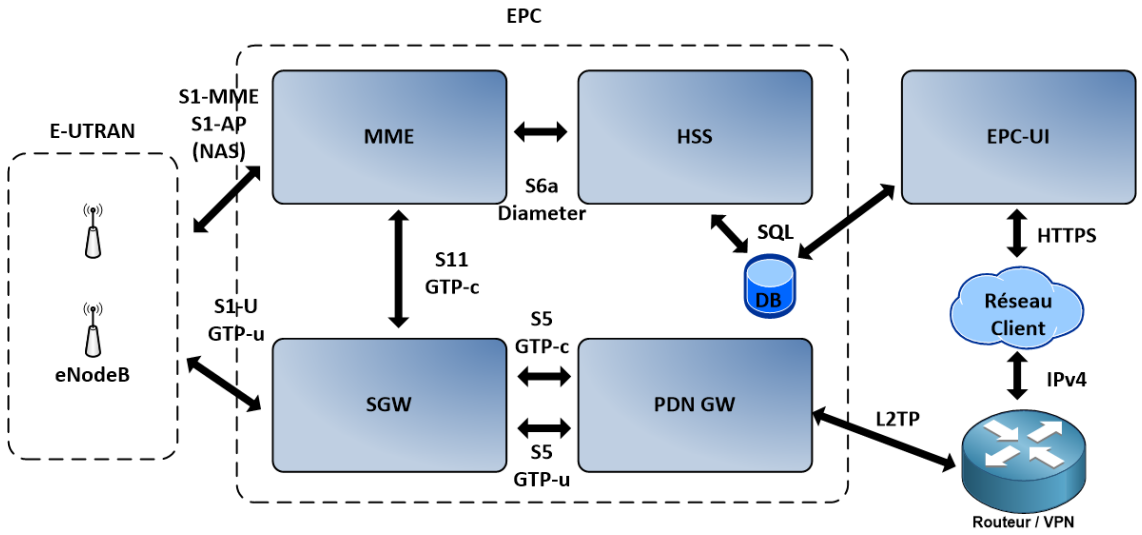


Figure 2.8 Architecture d'un réseau LTE

mètres à l'intérieur et 450 mètres à l'extérieur.

Les réseaux WiFi sont généralement destinés à des réseaux privés dans les résidences ou en entreprise. Ils ne sont pas destinés à des déploiements à grande échelle, même si de tels déploiements ont déjà été tentés (à Amsterdam, par exemple). Le tableau 2.3 présente les caractéristiques des différents standards WiFi.

Les réseaux WiMAX

WiMAX est une technologie d'accès sans-fil permettant un déploiement à grande échelle et donc une couverture bien plus grande que WiFi. Elle est basée sur le standard Institute of Electrical and Electronics Engineers (IEEE) 802.16 et est définie par « WiMAX Forum »,

Tableau 2.3 Standards WiFi (IEEE 802.11)

Année	Standard	Fréq. (Ghz)	Bande pass. (Mhz)	Modulation	Technologies d'antenne avancées	Débit maximal
1997	802.11	2.4	20	DSSS,FHSS	-	2 Mbps
1999	802.11b	2.4	20	DSSS	-	11 Mbps
1999	802.11a	5	20	OFDM	-	54 Mbps
2003	802.11g	2.4	20	DSSS,OFDM	-	54 Mbps
2009	802.11n	2.4,5	20,40	OFDM	MIMO	600 Mbps
2012	802.11ad	60	2160	SC,OFDM	Formation de faisceau	6.76 Gbps
2014	802.11ac	5	40,80,160	OFDM	MIMO,MU-MIMO	6.93 Gbps

qui décrit la technologie comme étant « *A standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL* ».

Il existe deux modes pour WiMAX, soit le mode qui requiert LoS et celui qui ne le requiert pas. Le premier mode permet d'obtenir une meilleure portée et donc d'avoir une meilleure couverture, mais son déploiement est plus difficile. Ainsi, lorsqu'il s'agit de couvrir une région dense, c'est le mode sans LoS qui est utilisé, même si la portée est bien inférieure. De plus, il existe d'autres paramètres qui influencent la portée du signal ainsi que le débit offert. Par exemple, le déploiement peut être fait par l'usager lui même (similaire à WiFi) et donc destiné pour un usage domestique, ou encore il peut être déployé par un fournisseur pour un usager extérieur. De plus, il existe deux classes d'installation des réseaux WiMAX, soit l'installation standard et l'installation haut de gamme. Une station de base de type standard implémente le protocole WiMAX de base, et sa puissance d'émission RF est plus faible, contrairement aux stations de base qui implémentent le protocole haut de gamme. Le Tableau 2.4 résume la performance de WiMAX au niveau de la portée et du débit offert, dans les différentes configurations possibles.

Autres technologies sans-fil

La technologie sans-fil la plus ancienne est celle qui emploie des liaisons par faisceaux hertziens (« microwave »). Les liens sont de type LoS et la portée est de 5 km. Ils sont faciles à déployer, par contre, les débits offerts sont faibles (155 Mbps), ce qui inhibe leur utilisation lorsqu'on a besoin de déployer des liens à haute capacité.

Multichannel Multipoint Distribution Service (MMDS) est une autre technologie utilisant des liaisons par faisceaux hertziens et de type LoS. Son avantage est qu'elle est de type point à multipoint. Ainsi, une station émettrice peut distribuer le signal vers plusieurs destinations en même temps (dans un angle de 60° à 90°). Ceci réduit le coût, par lien, du réseau. Un exemple d'application, qui emploie MMDS, est la télévision et cette technologie a été proposée comme alternative au câble coaxial, surtout dans les endroits éloignés ou difficiles à rejoindre. La portée est relativement grande et peut atteindre les 100 km si la surface est plate.

Similaire à MMDS, les réseaux basés sur Local Multipoint Distribution Service (LMDS) emploie une transmission de type point à multipoint. Par contre, les fréquences utilisées sont supérieures, ce qui permet un plus grand débit, au détriment de la portée. Ainsi, il s'agit d'une solution qui est plutôt déployée de manière locale.

Une autre technologie sans-fil est Direct Broadcast Satellite (DBS). Elle est utilisée principalement pour la diffusion de la télévision numérique, à l'aide de satellites géostationnaires. Ces derniers reçoivent l'information à partir d'une station sur terre et la relaient aux usagers en couvrant une certaine région. Leur plus gros désavantage se trouve au niveau de la latence,

Tableau 2.4 Performance de WiMAX

Type	Portée	Débit max. en aval	Débit max. en amont	Débit max. en aval à la frontière de la cellule	Débit max. en amont à la frontière de la cellule
Standard LoS	10 à 16 km	8 à 11,3 Mbps	8 à 11,3 Mbps	2,8 à 11,3 Mbps	2,8 à 11,3 Mbps
Standard non-LoS	1 à 2 Mbps	8 à 11,3 Mbps	8 à 11,3 Mbps	2,8 à 11,3 Mbps	2,8 à 11,3 Mbps
Haut de gamme LoS	30 à 50 Mbps	8 à 11,3 Mbps	8 à 11,3 Mbps	2,8 à 11,3 Mbps	2,8 à 11,3 Mbps
Haut de gamme non-LoS	4 à 9 Mbps	8 à 11,3 Mbps	8 à 11,3 Mbps	2,8 à 11,3 Mbps	0,175 à 0,7 Mbps

qui est autour de 250 ms, à cause de la distance des satellites (22,300 km).

2.2 Planification des réseaux d'accès filaires

Dans cette section, nous faisons la revue des travaux les plus pertinents dans la littérature, qui portent sur la planification des réseaux d'accès filaires, sujet qui est traité au chapitre 6. La planification des réseaux sans-fil ne sera pas abordée dans cette thèse. Nous débuterons par un rappel de la problématique, suivi d'une revue des topologies et travaux les plus pertinents. Ensuite, nous verrons les travaux plus récents et nous terminerons par une revue des travaux traitant de l'aspect dynamique des réseaux.

2.2.1 Problématique

Un réseau moderne est typiquement composé de deux parties, soit le réseau fédérateur et le réseau d'accès. La planification est un processus important qui doit pouvoir équilibrer l'investissement requis par rapport à la qualité de service offerte aux clients. Idéalement, la planification doit être effectuée sur l'ensemble du réseau, car les parties sont interdépendantes. Par exemple, le nombre de clients desservis à un endroit en particulier du réseau a une influence sur les capacités du réseau fédérateur qui les prend en charge. Cependant, les planifications sont généralement effectuées séparément, afin de réduire la complexité.

Les réseaux d'accès forment donc la partie qui relie les utilisateurs au réseau de l'opérateur. Désignés parfois par l'expression « derniers kilomètres » (« last mile »), les réseaux d'accès peuvent représenter jusqu'à 90 % de l'investissement total de l'opérateur (Pujolle, 2011).

Au niveau du réseau d'accès, plusieurs décisions doivent être prises :

– Quelles topologies déployer dans les réseaux d'accès ?

– Comment interconnecter les clients entre eux et au réseau ?
– Quels types de noeuds à déployer ?
– Où placer les noeuds ?

Il s'agit donc d'un problème complexe à résoudre et dont l'objectif est de trouver une topologie optimale, qui minimise le coût total de la planification, en sélectionnant l'emplacement et en dimensionnant les noeuds et liens. Les auteurs dans Gouveia et Lopes (1997) le décomposent en 4 sous-problèmes, soit :

– la recherche du nombre optimal de noeuds ;
– la recherche de l'emplacement optimal de noeuds ;
– la recherche de l'assignation optimale des clients aux noeuds ;
– la recherche de l'interconnexion optimale entre les clients et les noeuds.

Généralement, ces sous-problèmes sont résolus de manière séparée et séquentielle, donc une approche itérative. Le résultat obtenu par la résolution d'un sous-problème est fourni en entrée au prochain. La planification est donc simplifiée ainsi. Par contre, ceci ne garantit pas une résolution globale qui est optimale.

2.2.2 Approches de résolution

Le problème de la planification des réseaux d'accès n'est certainement pas nouveau. Une revue complète des travaux effectués peut être trouvée à Balakrishnan *et al.* (1991), Gavish (1991) et, plus récemment, Klincewicz (1998). Nous effectuerons un survol des topologies les plus utilisées, ainsi que des travaux qui les emploient.

Arbres de recouvrement minimal avec capacités

Les arbres de recouvrement, ou Minimum Spanning Tree (MST), sont des structures qui sont typiquement utilisées dans les réseaux d'accès. Le problème consiste à trouver un arbre de recouvrement à coût minimal qui lie un ensemble de noeuds, à un noeud central. De plus, la capacité limitée des liens et des noeuds donnent lieu à l'utilisation plutôt d'arbres de recouvrement avec capacités, ou Capacitated Minimum Spanning Tree (CMST). Ce problème ajoute des contraintes afin de respecter les capacités maximales des liens et noeuds. CMST et ses variantes ont été démontrés être des problèmes NP-difficile (Camerini *et al.* (1980), Camerini *et al.* (1983) et Papadimitriou (1978)). Le problème de CMST peut être formulé en tant que problème à nombres entiers binaires ou en tant que problème de multiples flôts de demande (« multi-commodity flow problem ») (Gavish, 1991). Un exemple de CMST est présenté à la Figure 2.9.

Certaines approches de résolution exacte ont été proposées, incluant des méthodes de

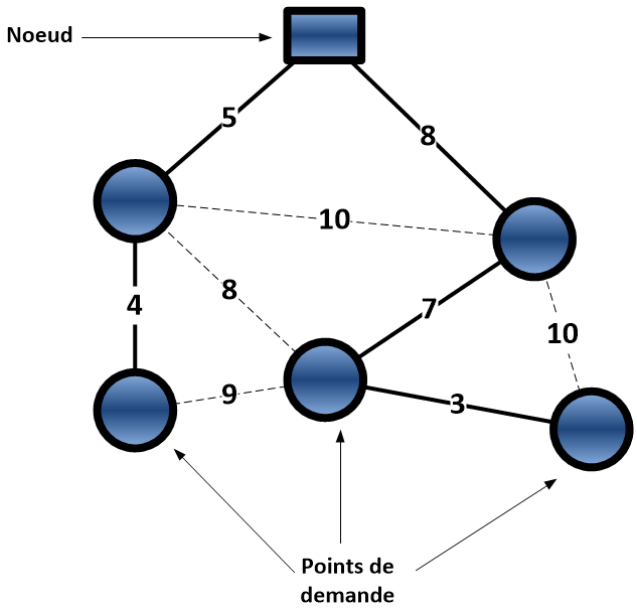


Figure 2.9 Arbre de recouvrement minimal avec capacité

« branch and bound », la décomposition de Benders (Gavish (1982)), la relaxation Lagrangienne (Gavish (1983)) et la relaxation Lagrangienne augmentée (Gavish (1985) et Kershenbaum *et al.* (1980)). La nature difficile du problème limite les solutions exactes à de petits jeux de données. Ainsi, pour attaquer des problèmes de plus grandes envergures, des méthodes heuristiques doivent être employées pour approximer le problème. Celles-ci incluent le recuit simulé (Lukic, 1999), la recherche de voisinage avec tabous (Girard *et al.*, 2001) ainsi que les algorithmes génétiques (Routen, 1994).

Arbres de recouvrement minimal avec capacités et plusieurs centres

Le problème d'arbres de recouvrement minimal avec capacités et plusieurs centres, ou Multicenter Capacitated Minimum Spanning Tree (MCMST), se distingue du problème de CMST en permettant l'existance de plusieurs nœuds. Ainsi, un client peut être connecté à n'importe lequel de ces nœuds.

La planification des réseaux d'accès est formulée comme un problème utilisant une topologie MCMST à Girard *et al.* (2001). Une heuristique de recherche de voisinage avec mouvements tabous est également proposée afin d'approximer le problème. Cette topologie est également employée par Carpenter *et al.* (2001) afin de modéliser des réseaux FTTC. Du côté des réseaux HFC, Gupta et Pirkul (2000) propose une heuristique basée sur la relaxation lagrangienne afin de minimiser le coût du réseau. Finalement, Soni *et al.* (2004) présente une variante de cette topologie où chaque client est relié à un multiplexeur et chaque multiplexeur

est relié à deux commutateurs, assurant ainsi une meilleure fiabilité du réseau. Les résultats qu'il obtiennent sont grâce à des heuristique basées sur le recuit simulé.

2.2.3 Réseaux d'accès à haut débits

Les travaux de recherche plus récents traitent plutôt des réseaux d'accès à haut débits. Par exemple, Carpenter *et al.* (1996), Mazur (1999) et Carpenter *et al.* (2001) se sont concentrés sur la planification des réseaux hybrides FTTN et HFC. Du côté des réseaux en fibre optique, les auteurs de Li et Shen (2008) se sont attaqués au problème de la planification des réseaux PON. Ils l'ont décomposé en deux sous-problèmes, soit l'affectation des clients aux noeuds et l'emplacement et dimensionnement optimaux de ces noeuds. Ils proposent ainsi deux heuristiques pour approximer le problème, la seconde étant basée sur le travail effectué dans Cooper (1963). Leurs résultats montrent une amélioration de 50 à 70%, lorsque comparés aux méthodes existantes.

Un autre travail portant sur la planification des réseaux PON est présenté à Lee *et al.* (2006). Le problème est modélisé en tant que modèle de programmation en nombres entiers mixtes. Les résultats sont obtenus grâce à la technique de génération de colonnes. Ils sont ensuite comparés à une borne inférieure obtenue en relâchant certaines contraintes. Les résultats obtenus étaient cependant jusqu'à 81% plus grands. Un autre travail, présenté à Kim *et al.* (2011), a réduit cette marge, en effectuant une relâche de la fonction-objectif, combinée à une heuristique de recherche locale.

Les auteurs de Jaumard et Chowdhury (2012) s'attaquent également au problème de la planification des réseaux PON, en le divisant en trois phases. Premièrement, des hiérarchies potentielles d'équipements sont générées. Lors de la seconde phase, un modèle mathématique de génération de colonnes est utilisé afin de choisir le type et l'emplacement de l'équipement de commutation, pour chaque hiérarchie, de manière à réduire le coût de la topologie des équipements, tout en accomodant tout le trafic demandé. La dernière phase choisit la meilleure hiérarchie parmi toutes celles générées et dimensionnées.

2.2.4 Planification dynamique

La plupart des travaux de planification des réseaux supposent que la planification est effectuée en une seule et unique phase. Certains travaux proposent, par contre, d'introduire plusieurs phases dans la planification, pour représenter l'aspect évolutif des réseaux. Par exemple, les auteurs dans Shulman (1991) ont formulé le problème en tant que problème d'optimisation combinatoire, en considérant plusieurs types de nœuds, afin de trouver la combinaison optimale de nœuds à chaque site. La résolution a été effectuée grâce à une relâche

lagrangienne, et les résultats obtenus étaient à 3% de la borne inférieure dans la plupart des scénarios. D'autres travaux incorporant l'aspect dynamique des réseaux sont présentés à Dias *et al.* (2007) et Zhao *et al.* (2010). Le premier considère la possibilité d'étendre et de réduire la capacité maximale disponible à chacun des sites, durant les différentes phases de la planification. Le deuxième, quant à lui, propose un modèle de migration complet et généralisé vers les réseaux FTTH.

2.3 Protocoles de mobilité

Le protocole IPv6, dans sa version standard, n'offre pas de mécanismes de gestion de mobilité. En effet, un noeud possède une adresse IP et cette adresse est utilisée pour identifier le réseau auquel il appartient. Ainsi, lorsqu'un noeud correspondant lui envoie des paquets, ces derniers seront aiguillés au bon réseau, grâce justement à cette adresse IP. Les problèmes surviennent, alors, lorsque le noeud décide de migrer d'un réseau vers un autre. En effet, si son adresse IP reste inchangée, le noeud ne sera plus rejoignable, car cette adresse n'est pas topologiquement valide dans le nouveau réseau ; le protocole de routage ne pourra pas aiguiller correctement les paquets. Le noeud se voit forcé à changer d'adresse, pour en obtenir une qui est valide dans le nouveau réseau. Le problème qui survient, alors, est que toutes les connexions, qui sont en cours, sont interrompues.

La gestion de la mobilité devient donc un élément essentiel lorsqu'on veut permettre la mobilité dans un réseau. Elle permet à un noeud mobile de préserver son adresse IP lors de sa mobilité, tout en restant rejoignable. Pour s'y faire, il faut instaurer la gestion de l'emplacement du noeud et la gestion de ses relèves. La première s'occupe de garder la position du Mobile Node (MN) en tout temps, le gardant ainsi rejoignable. La deuxième, quant à elle, s'occupe de maintenir les connexions existantes lors des relèves (donc lorsque le MN change de réseaux). Les prochaines sections présentent les protocoles de mobilité les plus populaires.

2.3.1 MIPv6

Défini comme un protocole de communications standard dans Internet Engineering Task Force (IETF), MIPv6 permet aux noeuds mobiles de migrer d'un réseau vers un autre, tout en maintenant la même adresse IP. Il est destiné aux réseaux IPv6 et succède à Mobile IP v4 (MIPv4) qui, lui, opère sur un réseau IPv4. Pour s'y faire, lorsqu'un noeud se retrouve dans un réseau qui n'est pas le sien, il se voit attribuer une adresse IP valide pour ce réseau. Cette adresse, appelée Care-of-Address (CoA), peut être attribuée par n'importe quel mécanisme (Dynamic Host Configuration Protocol (DHCP), par exemple). Une fois qu'il reçoit cette

adresse, le noeud doit s'enregistrer auprès d'un noeud, appelé Home Agent (HA), qui se trouve dans son réseau-mère. Cette étape, appelée le Binding Update (BU), permet au noeud d'associer sa nouvelle adresse à son adresse qu'il possède dans son réseau-mère (Home Address (HoA)). Ainsi, pour le rejoindre, les noeuds correspondants continuent à utiliser la HoA du noeud. C'est le HA qui s'occupe alors d'intercepter ces paquets et de les encapsuler dans un tunnel vers le MN. MIPv6 définit également un mécanisme, appelé Route Optimization (RO), qui permet au MN de communiquer son adresse CoA au Correspondant Node (CN), permettant ainsi une communication directe entre les deux noeuds, sans avoir recours au tunnel du HA. La figure 2.10a illustre le fonctionnement de MIPv6.

Plusieurs problèmes font en sorte que le déploiement de MIPv6 est faible. Premièrement, le déploiement de MIPv6 est contingent à celui de IPv6, qui n'est pas encore déployé à grande échelle et ce, malgré sa standardisation, il y a de celà plus d'une dizaine d'années. Le protocole Dual Stack MIPv6 (DSMIPv6) peut minimiser ce problème en permettant le déploiement sur IPv4. De plus, les spécifications de MIPv6 requièrent l'utilisation de IP Security (IPSec) et de Internet Key Exchange (IKE) pour le chiffrement de la signalisation entre le MN et le HA. Par contre, l'interface entre MIPv6 et IPSec n'est pas bien définie, ce qui complique l'implémentation et augmente le coût d'implantation. Un autre problème est que MIPv6 requiert que le MN envoie des messages de signalisation après chaque relève. De plus, il doit rafraichir périodiquement l'association avec le HA. Tous ces paquets envoyés par le MN contiennent un entête IPv6 de 40 octets, ce qui représente un grand surdébit sur le lien radio, qui est généralement la partie la plus chère.

Un autre problème est que la majorité des opérateurs voudraient être en contrôle de la gestion de la mobilité, ce qui n'est pas possible avec MIPv6, car la gestion est entièrement effectuée par le MN. Ceci limite certaines options, telles que le multi-accès vers des liens moins coûteux ou moins congestionnés. De plus, certains noeuds dans le réseau peuvent détenir des informations pertinentes quant aux conditions dynamiques, celles-ci ne pouvant être présentement utilisées pour gérer les relèves.

Plusieurs extensions à MIPv6 on été proposées afin d'améliorer les performances et ajouter de nouvelles fonctionnalités. Les deux plus populaires sont FMIPv6 et HMIPv6.

FMIPv6

Un problème avec MIPv6 est que, durant la relève, le MN se retrouve sans connexion pendant une période de temps. Il lui est donc impossible d'envoyer ou de revecoir des packets lors de ce délai. Ceci a évidemment un effet néfaste sur certains trafics, tels que les trafics en temps réél. L'objectif de FMIPv6 est donc de permettre au MN d'envoyer et de recevoir des paquets dès que le lien physique avec le nouveau point d'accès est établi, sans devoir attendre

la mise à jour avec le HA. Ceci est possible grâce à une anticipation de la relève par le MN, qui va alors avertir le nouveau routeur d'accès. Ainsi, lorsque la relève est effectuée, les mises à jour auront déjà été effectuées. La figure 2.10b illustre le fonctionnement de FMIPv6.

HMIPv6

HMIPv6 propose d'améliorer MIPv6 en réduisant le nombre de messages de signalisation requis et en améliorant la vitesse de la relève. Le protocole propose de séparer la mobilité globale, qui sera toujours gérée par MIPv6, de la mobilité locale, qui sera désormais gérée par HMIPv6.

Pour s'y faire, un nouveau noeud, le Mobility Anchor Point (MAP), est introduit et sert d'entité locale pour aider les noeuds mobiles à effectuer leurs relèves. Ce noeud va être situé généralement dans le réseau visité. Ainsi, pour les relèves lors d'une mobilité locale, le noeud n'a plus besoin de communiquer avec son HA, la mise à jour s'effectuant désormais avec le MAP. La figure 2.10c illustre le fonctionnement de MIPv6.

2.3.2 PMIPv6

PMIPv6 est un autre protocole standard de gestion de mobilité à IETF. Son objectif est le même que MIPv6, par contre son approche est différente. Contrairement à MIPv6, où la mobilité est gérée par le MN, la mobilité est entièrement gérée par le réseau dans PMIPv6. Ainsi, aucune modification n'est nécessaire au niveau du MN pour déployer PMIPv6. De plus, l'élimination des messages de signalisation au niveau de l'interface radio réduit la congestion et minimise l'impact au niveau de l'utilisation énergétique du MN.

Pour s'y faire, PMIPv6 introduit deux nouveaux noeuds, soit le Local Mobility Anchor (LMA) et le Mobile Access Gateway (MAG). Le premier est l'équivalent du HA de MIPv6, dans un environnement PMIPv6. Le MAG, quant à lui, s'occupe de gérer la mobilité à la place du MN, en détectant ses mouvements d'un lien d'accès vers un autre. C'est alors que le MAG envoie des Proxy BU (PBU) au LMA. Ceci est effectué sans aucune connaissance, ni collaboration, du MN. Le MAG est également responsable de simuler la présence du réseau-mère du MN, en lui envoyant des messages de Router Advertisement (RA), contenant les préfixes du réseau-mère. Ainsi, au niveau du MN, aucune mobilité n'est apparente. La figure 2.10d illustre le fonctionnement de PMIPv6.

Malgré les avantages nombreux de PMIPv6, certains problèmes inhibent son déploiement, comme par exemple le support pour accès multiples qui est quasiment inexistant, les problèmes niveau des relèves entre différentes technologies, ainsi que le manque de support au niveau du Simultaneous Multi-Access (SMA). De plus, son déploiement introduit une grande

complexité au niveau du réseau.

2.3.3 Comparaison des protocoles de mobilité

Plusieurs études ont porté sur l'évaluation de la performance des différents protocoles de mobilité existants, parmi lesquelles, on recense principalement le travail de Makaya et Pierre (2008). Dans cet article, les auteurs ont proposé des cadres d'analyse afin de comparer, en détail, la performance de MIPv6, HMIPv6, FMIPv6 et Fast Handover for Hierarchical MIPv6 (F-HMIPv6), en utilisant plusieurs métriques, telles que le coût de la surcharge de la signalisation, le coût d'acheminement des paquets, la latence des relèves et le nombre de paquets perdus. Les résultats numériques ont permis de conclure quant à l'effet de chacun de ces paramètres sur les protocoles, permettant ainsi à un opérateur d'effectuer des choix judicieux en fonction du réseau à déployer. Par exemple, ils ont trouvé que F-HMIPv6 améliore la latence au niveau des relèves et minimise les pertes de paquets par rapport aux autres protocoles, au détriment de la signalisation ainsi que de l'espace mémoire tampon requis, qui sont augmentés.

2.4 La multidiffusion

Telle que mentionnée dans le chapitre précédent, la multidiffusion permet la transimission de type point à multipoint. Le fonctionnement de la multidiffusion repose sur le concept de groupes (appelés également canaux). Ces derniers sont formés par la combinaison de l'adresse IP de la source ainsi que l'adresse IP du groupe auquel les données sont acheminées. Contrairement aux autres méthodes de transmission, les adresses des groupes de multidiffusion n'ont pas de signification ou de limite géographique, ce qui permet à n'importe quelle machine de pouvoir joindre n'importe quel groupe et ce, peu importe l'emplacement des noeuds (tant qu'un lien peut être établi).

Les adresses de multidiffusion sont définies, en IPv4, par les adresses débutant par les bits 1110. Ceci inclut donc toutes les adresses entre 224.0.0.0 et 239.255.255.255 (le prefix Classless Inter-Domain Routing (CIDR) est donc 224.0.0.0/4). Certaines de ces adresses sont réservées, telles que spécifié dans Cotton *et al.* (2010). En IPv6, le préfixe est ff00 : :/8. Différentes plages de ce préfixe sont réservées à différentes portées, similaire à la transmission individuelle.

Lorsqu'un client désire rejoindre un groupe de multidiffusion, deux choix sont possibles. Il peut, soit recevoir les données de toutes les sources dans le groupe, soit préciser uniquement une seule source à recevoir. Dans le premier cas, il suffit de connaitre l'adresse IP du groupe. Cette méthode est appelée Any Source Multicast (ASM). Généralement, pour chaque groupe,

il existe un nœud, appelé Rendez-vous Point (RP), vers lequel les sources envoient les données, qui sont ensuite acheminées vers les noeuds souscrits à ce groupe. Dans le deuxième cas, le client doit connaitre, en plus de l'adresse IP du groupe, celle de la source en question. Cette méthode est appelée Source-Specific Multicast (SSM). Puisque l'adresse de la source est connue d'avance, il n'est pas nécessaire d'avoir un RP pour le bon fonctionnement.

SSM est généralement vue comme une meilleure méthode que ASM. Ses avantages sont les suivants :

- une allocation d'adresses plus simple : l'adresse d'un groupe SSM est locale à la source, ce qui simplifie son allocation (aucun besoin d'un mécanisme ou d'un protocole pour une allocation globale) ;
- plus sécuritaire : les attaques de type déni de service sont moins efficaces, car les sources sont connues d'avance ;
- routage inter-domaine plus simple : il n'est pas nécessaire de découvrir les sources, ou de synchroniser leurs adresses entre différents domaines.

Par contre, SSM présente également les faiblesses suivantes :

- les noeuds doivent connaitre l'adresse de la source qu'ils désirent recevoir. Si plusieurs sources existent dans un même groupe, et surtout si ces sources varient, ceci complique la procédure ; l'implémentation d'autres mécanismes de découverte des adresses peut s'avérer nécessaire ;
- tous les protocoles de multidiffusion supportent ASM, mais ne supportent pas nécessairement SSM, ce qui peut ralentir le déploiement de SSM. La prochaine sous-section présente ces protocoles en détail.

Dans un scénario où une seule source, ou encore un petit nombre de sources existe et ne change pas, SSM est la méthode à priviligier. Ce genre d'applications incluent par exemple la diffusion de l'audio et la vidéo, (IPTV par exemple). Par contre, il existera encore des applications pour lesquelles SSM n'est pas adéquat. Un exemple est la vidéoconférence, où chaque noeud est à la fois client et source, et le nombre de noeuds peut varier rapidement.

2.4.1 Protocoles de multidiffusion dans IP

Il existe plusieurs protocoles permettant d'assurer le support de la multidiffusion dans un réseau IP. On peut les regrouper en deux groupes, soient les protocoles qui s'occupent d'établir les abonnements des hôtes aux différents groupes, ainsi que les protocoles de routage qui assurent la création et le maintien des routes.

Le protocole le plus populaire pour établir les abonnements est Internet Group Management Protocol (IGMP), pour les réseaux IPv4, et Multicast Listener Discovery (MLD), pour les réseaux IPv6. Il existe trois versions de IGMP, soit Internet Group Management Pro-

tocol v1 (IGMPv1), Internet Group Management Protocol v2 (IGMPv2) et Internet Group Management Protocol v3 (IGMPv3) et deux versions de MLD, Multicast Listener Discovery v1 (MLDv1) et Multicast Listener Discovery v2 (MLDv2), qui sont basées sur IGMPv2 et IGMPv3, respectivement.

Pour les protocoles de routage entre les routeurs supportant la diffusion groupée, on distingue les protocoles intra-domaines, des protocoles inter-domaines. Les protocoles intra-domaines permettent la découverte des sources et la création et le maintien des arbres de distribution à l'intérieur d'un Autonomous System (AS). Le protocole le plus populaire est Protocol Independent Multicast (PIM). Celui-ci n'offre aucun mécanisme de découverte de topologie, mais va plutôt utiliser l'information mise disponible par les autres protocoles de routage tels que Routing Information Protocol (RIP), Open Shortest Path First (OSPF) et Border Gateway Protocol (BGP).

On retrouve quatre différentes implémentations de PIM, avec chacune ses propres spécificités. La première, PIM Sparse Mode (PIM-SM) (Fenner *et al.*, 2006), bâtit de manière explicite les arbres, par groupe, avec comme racine le RP. Optionnellement, les liens les plus courts sont bâtis par source. Son avantage est qu'elle est évolutive pour les déploiements à grande échelle, où la densité des clients inscrits est faible. La deuxième variante, PIM Dense Mode (PIM-DM) (Adams *et al.*, 2005), bâtit les arbres implicitement, en inondant le réseau avec du trafic de multidiffusion, et en éliminant les branches où aucun client n'est présent. Son avantage est dans la simplicité de son implémentation et fonctionne bien pour de petits réseaux où la densité des clients inscrits est grande. Par contre, à cause de l'inondation, elle n'est pas évolutive. PIM bidirectionnel (Handley *et al.*, 2007) est semblable à PIM-SM car les arbres sont également bâtis de manière explicite, mais en utilisant des liens bidirectionnels. Les arbres obtenus ne sont jamais les plus courts et donc les délais peuvent être plus grands. Par contre, elle est évolutive car aucun état sur la source n'a besoin d'être gardé. Finalement, PIM Source-Specific Multicast (PIM-SSM) (Bhattacharyya, 2003) bâtit des arbres avec une seule racine, pour le mode SSM de la multidiffusion.

2.4.2 Problématique de la multidiffusion dans un environnement mobile

Lorsque déployée dans environnement mobile, la multidiffusion présente plusieurs problèmes. Ceux-ci peuvent être regroupés en deux, soient les problèmes liés aux sources mobiles et ceux liés aux clients mobiles. Le premier groupe traite des problèmes qui surviennent lorsque la source, qui diffuse l'information, change d'adresse IP. Le deuxième, quant à lui, traite des problèmes qui surviennent lorsqu'un client change d'adresse IP pendant qu'il reçoit l'information.

Problèmes reliés à la mobilité de la source

Une source de multidiffusion opère sans connaissance des noeuds qui reçoivent son flôt. Lorsqu'elle envoie un paquet, elle n'a pas de mécanisme pour s'assurer qu'il a bel et bien été enovoyé aux clients. De ce fait, si une relève survient, la source peut perdre la connectivité avec les noeuds récepteurs, sans le réaliser. Elle doit donc offrir une transparence d'adresse, ce qui s'avère une tâche difficile. La mobilité de la source n'est pas traitée dans cette thèse, car nous supposons que la source est un noeud fixe (notre application cible étant IPTV, cette supposition est généralement valide).

Problèmes reliés à la mobilité du client

Lorsqu'un MN change d'adresse IP suite à une relève, il doit pouvoir recevoir les paquets des groupes auxquels il est souscrit, en temps réel. Dépendamment des conditions du réseau, cette relève peut s'avérer complexe. Dans le cas le plus simple, s'il existe déjà des membres de ces groupes dans le nouveau réseau, les paquets sont déjà acheminés dans ce réseau et donc le MN pourra rejoindre le groupe très rapidement. Par contre, si ce n'est pas le cas, il faut établir une nouvelle branche de l'arbre de distribution, et cette opération peut s'avérer longue. Dans le pire cas, le nouveau réseau ne supporte pas nativement la multidiffusion. Dans ce cas, il faut rejoindre l'arbre grâce à de l'encapsulation dans un tunnel vers un autre réseau qui supporte nativement la multidiffusion.

On retrouve donc les problématiques suivantes :

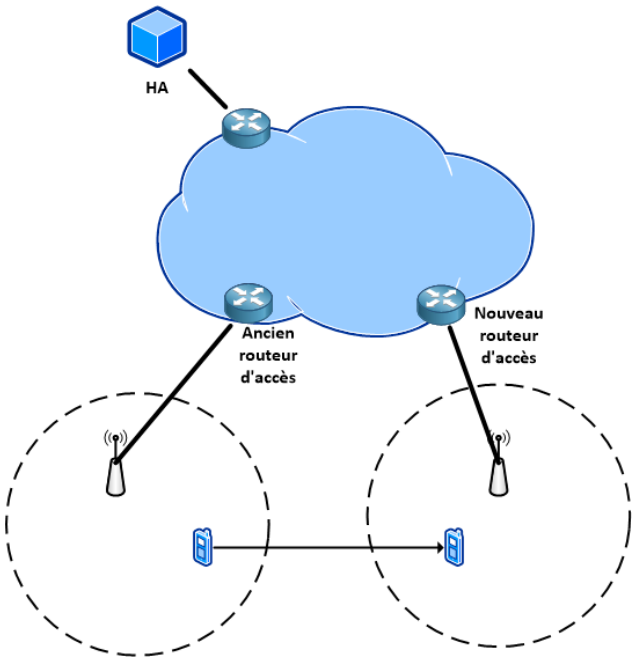
- Il faut assurer le support pour la multidiffusion dans les réseaux visiteurs et ce, même si ces derniers ne la supportent pas nativement ;
- Minimiser le délai de relève de la multidiffusion afin d'offrir une transition rapide et transparente (important pour les services en temps-réel). Ceci dépend évidemment du temps de relève des couches 2 (L2) et 3 (L3), car la relève de la multidiffusion ne peut démarrer avant que la nouvelle connexion IPv6 n'ait été établie ;
- Minimiser, voire même éliminer, les pertes de paquets lors des relèves. De plus, il faut pouvoir gérer le fait que les paquets peuvent potentiellement arriver en désordre ;
- Dans un environnement mobile, il y a toujours un souci de minimiser la signalisation sur l'interface radio, afin de réduire la consommation d'énergie du noeud mobile.

Le protocole MIPv6 propose deux approches simples à ce problème. La première solution consiste en l'encapsulation des paquets de multidiffusion dans un tunnel unicast. Les paquets sont donc reçus par le HA, qui les achemine ensuite au MN à travers le tunnel. Cette approche fonctionne en tout temps, car elle ne requiert pas que le réseau supporte la multidiffusion. Par contre, elle souffre du problème d'évolutivité, car la nature de la multidiffusion est perdue.

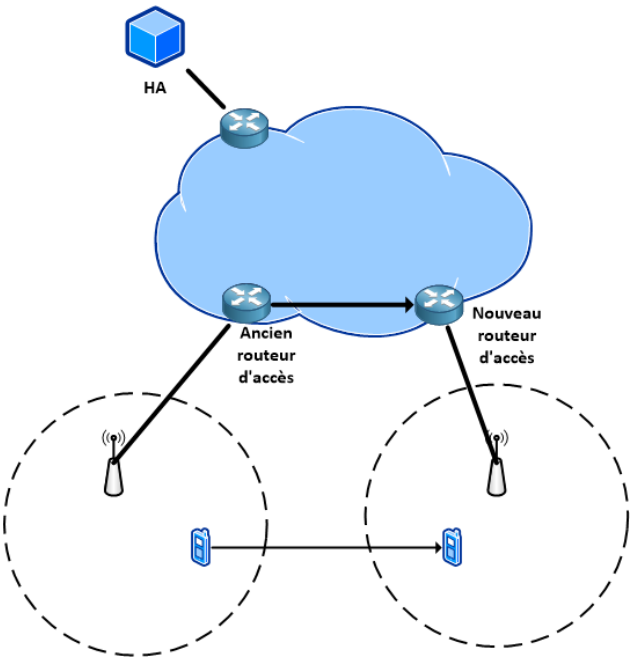
L'autre solution proposée est d'utiliser la multidiffusion de manière native, avec l'adresse CoA. Cette approche est plus optimale, car elle ne gaspille pas de ressources. Par contre, elle requiert un support natif de la multidiffusion dans les réseaux visités. De plus, à chaque fois que le noeud mobile change d'adresse, il doit réétablir sa connectivité à l'arbre de multidiffusion, ce qui peut être un processus relativement long.

D'autres solutions, plus complexes, ont été proposées. Certaines, comme par exemple Hong-Ke Zhang (2007), dépendent de l'existence d'un noeud, appelé Multicast Agent (MA), qui garde en mémoire le contexte du noeud mobile dans le réseau. Il joue ainsi le rôle de proxy, lorsque le noeud mobile effectue une relève. D'autres solutions proposent un hybride des approches de base du protocole MIPv6. Elles essayent donc d'équilibrer les avantages de chacune de ces approches tout en minimisant leurs inconvénients. Par exemple, Garyfalos et Almeroth (2005b) propose une architecture de recouvrement (« overlay ») qui permet de déployer la multidiffusion plus rapidement et de manière moins complexe. Cette approche, qui utilise un réseau de recouvrement, a suscité plusieurs autres travaux, tels que Waehlisch et Schmidt (2007), Buford (2008a) et Waehlisch (2013).

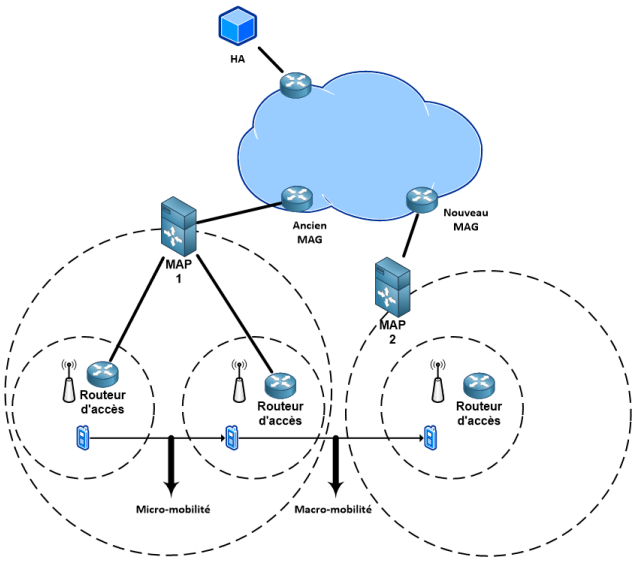
Il existe également des travaux ont qui été proposés pour les variantes de MIPv6. Par exemple, du côté de FMIPv6, les auteurs de Kyungjoo Suh et Park (2004) proposent une modification au protocole afin de minimiser la latence requise afin de rejoindre un arbre de multidiffusion, ainsi que le nombre de paquets perdus, par un noeud, lors d'un changement d'adresse. La solution proposée est de permettre au noeud mobile d'anticiper la relève et d'envoyer au nouveau point d'accès la liste des groupes de multidiffusion auxquels il est souscrit. Ainsi, lorsque le noeud effectuera sa relève, ces groupes seront déjà reçus dans le nouveau réseau, ce qui réduit considérablement le temps de reconnexion. Du côté de HMIPv6, on retrouve le travail présenté à Thomas C. Schmidt (2005). Celui-ci propose des modifications mineures à HMIPv6, MIPv6 et MLDv2 afin d'obtenir des relèves transparentes, en profitant de l'aspect architectural de HMIPv6. Une solution qui offre également une relève transparente, pour PMIPv6, est proposée à Gohar *et al.* (2010). Deux modes sont proposés, soit le mode intra-LMA et le mode inter-LMA.



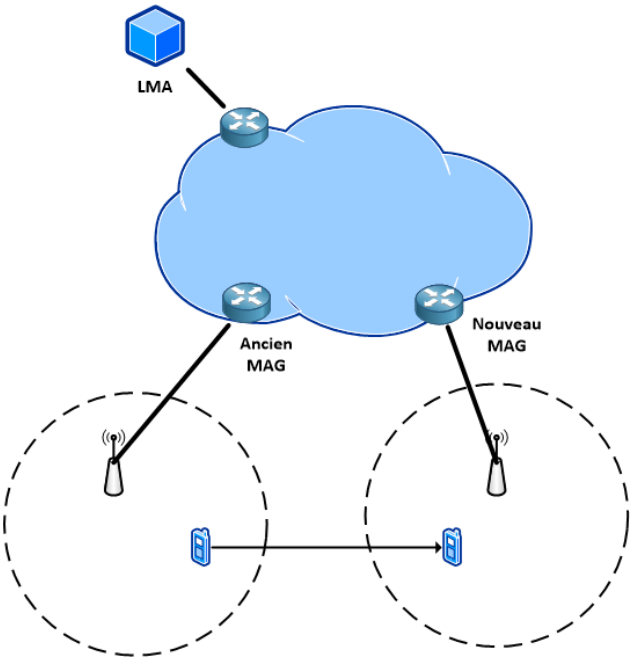
(a) MIPv6



(b) FMIPv6



(c) HMIPv6



(d) PMIPv6

Figure 2.10 Protocoles de mobilité

CHAPITRE 3

DÉMARCHES DE L'ENSEMBLE DU TRAVAIL DE RECHERCHE

Dans ce chapitre, nous présenterons les liens qui existent entre les articles proposés dans cette thèse et les objectifs de recherches énoncés au chapitre 1, plus précisément à la section 1.3.

Le premier article, qui s'intitule « *Client-Based Network-Assisted Mobile IPv6* », s'attaque à la gestion de la relève, afin d'optimiser la prise de décision, face à une possibilité de relève verticale. Pour s'y faire, nous avons débuté par une refonte du protocole MIPv6. Il faut comprendre que ce protocole, dans l'état actuel, incorpore énormément d'aspects, tels la sécurité, les mécanismes d'amorçage ou encore des mécanismes d'optimisation de route. Ces aspects, qui ne sont pas nécessaires au fonctionnement de base du protocole, polluent les spécifications et compliquent leur altération. Par exemple, si on considère l'aspect sécurité, le protocole de MIPv6 impose l'utilisation des protocoles IKE et IPSec pour chiffer la signalisation entre le MN et le HA. Or, de nouveaux protocoles de sécurité, qui ont été proposés plus récemment, sont plus efficaces que ceux imposés par MIPv6 (IKE version 2 (IKEv2) par exemple). Comme l'interface entre la partie sécurité et le reste du protocole n'est pas bien définie, la modification de MIPv6, afin d'incorporer de nouveaux protocoles de sécurité, s'avère être une tâche très compliquée. Ainsi, nous avons, en premier lieu, retiré tous les mécanismes qui ne sont pas nécessaires au fonctionnement de base du protocole. Le résultat obtenu est donc une nouvelle spécification qui est beaucoup plus légère (à titre indicatif, le nombre de pages des spécifications du protocole a été réduit d'environ la moitié).

Une fois le nouveau protocole, plus léger, obtenu, nous avons proposé le concept d'extensions afin de rétablir les autres fonctionnalités du protocole. Ainsi, pour ajouter une nouvelle fonctionnalité ou encore pour altérer un fonctionnement du protocole, des modules doivent être conçus à cette fin. De plus, pour les modules de sécurité, nous avons conçu une interface permettant la spécification des protocoles et des opérations à utiliser pour chiffrer tous les messages de signalisation. Ainsi, le protocole de base n'a pas besoin de connaître les détails des implémentations de la sécurité, il ne fait qu'exposer une interface claire qui doit être implémentée par le module de sécurité.

Afin de faire le lien entre le protocole de base et les différents modules et d'avoir une architecture qui est cohérente et compatible, nous avons également introduit le concept de profils. Un profil est un document qui spécifie :

– la révision du protocole de base qui doit être utilisée (plusieurs révisions du protocole

de base peuvent exister) ;
– un module de sécurité ;
– un certain nombre de modules d'extension.

Les profils assurent l'interopérabilité entre les nœuds qui les implémentent. Un nœud peut implémenter plusieurs profils. Deux nœuds qui n'implémentent pas au moins un profil commun sont considérés incompatibles et ne peuvent communiquer en utilisant notre protocole. Comme premier profil, nous avons proposé celui qui permet de retrouver toutes les fonctionnalités du protocole MIPv6 original.

Finalement, dans ce travail, nous avons conçu un module qui ajoute l'implication du réseau dans les décisions relatives aux relèves verticales. En proposant l'ajout d'un nouveau nœud (Proxy MN), le réseau s'assure du contrôle de la gestion des relèves verticales, tout en prenant en considération l'état du nœud mobile. Il s'agit donc d'un hybride entre les fonctionnalités de MIPv6 et ceux de PMIPv6. Un des avantages du module proposé est que le niveau d'implication du nœud mobile est ajustable par l'opérateur lors de l'implémentation du protocole, ce qui permet donc de convenir à la plupart des requis.

Le deuxième article, quant à lui, s'intitule « *Seamless handover for multicast Mobile IPv6 traffic* ». Il porte sur les perturbations qu'engendre une macro-mobilité, sur les applications multimédia en temps réél. Ces applications sont généralement déployées en utilisant la multidiffusion. Or, lorsqu'une relève verticale survient et que le nœud mobile change d'adresse IP, une interruption de l'expérience de l'usager, due à des pertes de paquets, en découle. La solution proposée introduit un nouveau nœud, le Multicast Buffering Agent (MBA), dont le rôle est de mettre en mémoire tampon les paquets perdus lors de la relève. Ainsi, lorsque le nœud recouvre la connectivité, il est en mesure de demander au MBA les paquets perdus et la relève devient donc transparente à l'usager.

Afin de s'assurer du bon fonctionnement de notre solution, les mémoires tampons, tant au niveau de l'application du nœud mobile, qu'au niveau du MBA, doivent êtres bien dimensionnées, ce qui fait l'objet d'une discussion dans l'article. Un sous-dimensionnement du tampon de l'application forcerait cette dernière à se suspendre, car elle serait en attente de paquets (son tampon étant vide). Un sous-dimensionnement du tampon du MBA signifierait une perte de paquets, car son tampon serait rempli à capacité avant que le nœud mobile ne regagne sa connectivité. Nous avons ensuite effectué des simulations et, en respectant le bon dimensionnement des tampons, nous avons obtenu le résultat escompté ; l'application en temps réel, que nous avons simulée, n'a pas subi d'interruption suite à une relève verticale (et donc à un changement d'adresse IP).

Dans le troisième article, qui s'intitule « *Dynamic Greenfield Fiber to the Home Planning* », le problème traité est celui de la planification des réseaux d'accès en fibre optique, de

bout en bout. Nous proposons un modèle de planification qui incorpore l'aspect dynamique et évolutif de ces réseaux. Ainsi, la planification est divisée en phases et la demande des clients, ainsi que le nombre de clients et de sites, varient d'une phase à l'autre. La résolution de ce modèle produit la solution optimale de la planification du réseau, en prenant en considération toutes les phases en même temps. Des simulations ont été effectuées sur des jeux de données générés aléatoirement, et les résultats démontrent la supériorité de notre solution par rapport aux méthodes séquentielles existantes.

Nos articles nous ont donc permis d'atteindre tous les objectifs énoncés dans cette thèse. Nos contributions ont amélioré le support des applications multimédia dans les réseaux de prochaine génération, tout en prenant en considération la mobilité des usagers. Ces améliorations portent autant sur l'architecture des réseaux que sur les protocoles utilisés.

CHAPITRE 4

CLIENT-BASED NETWORK-ASSISTED MOBILE IPv6

Auteurs : Georges Abou-Khalil et Samuel Pierre.
Revue : *International Journal of Communication Networks and Information Security*, vol. 2, no. 3, décembre 2010, pp. 224–230.

Abstract

With the growing number of mobile nodes and projections that this number will far exceed that of stationary nodes, mobility management becomes an important aspect of the next generation networks. Mobile operators are therefore looking to deploy a functional and optimized protocol that allows management of mobility while offering additional functionalities, such as simultaneous multi-access and flow mobility (important for Fixed-Mobile Convergence (FMC) for instance). Two major protocols exist that offer mobility management for Internet Protocol (IP) networks, Mobile IP v6 (MIPv6) and Proxy Mobile IP v6 (PMIPv6). However, both protocols have shortcomings that hinder their deployment on a massive scale. We therefore propose a new protocol, based on the current MIPv6 specifications, that addresses these shortcomings. It can be seen as a hybrid protocol offering simultaneously client and network mobility managements, which can be labeled "client-based network-assisted". We compare it to the existing two protocols and show that it doesn't suffer from their drawbacks.

4.1 Introduction

Mobility protocols are protocols designed to allow nodes to remain reachable while moving between networks. Regardless of its current point of attachment to the Internet, a Mobile Node (MN) stays reachable by a Correspondant Node (CN) through its home address. Mobile IP v6 (MIPv6) (Johnson *et al.*, 2004) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow such a behavior. It is seen as a client-driven protocol, as the decisions are taken by the MN. However, it suffers from multiple shortcomings, described in this paper. Proxy Mobile IP v6 (PMIPv6) (Gundavelli *et al.*, 2008) is a newer protocol that also offers mobility. All decisions are taken by the network, the MN is unaware of all mobility related mechanisms. It is therefore seen as a network-driven

protocol. PMIPv6 also suffers from some issues. Therefore, we propose a new protocol based on the MIPv6 specifications, which addresses the issues of both protocols. The rest of the paper is organized as follows. In Section 4.2, we review the state of the art of mobile Internet Protocol (IP) protocols suite. In Section 4.3, we detail our proposed solution. In Section 4.4, we compare our solution to the existing protocols. Finally, in Section 4.5, we recapitulate our work and conclude by presenting our future work.

4.2 State Of The Art Of Mobile IP Protocols Suite

4.2.1 Introduction

In the current versions of the IP, a node is assumed to have a fixed connection to the network and its IP address is used to identify the network to which it is attached. Therefore, packets sent to this node will be routed to the location corresponding to its IP network. If that node moves and keeps its IP address unchanged, that address will not reflect the new point of attachment. Therefore, the routing protocol used will be unable to route packets sent to that node, since the address is topologically incorrect. To remedy this situation, the node has to be reconfigured with a new IP address that is topologically correct in the new network. However, that operation will break all existing connections. Therefore, when a node moves without changing its address, it either becomes unreachable because of the loss of routing, or it loses current connections if it gets reconfigured with a new address.

Mobility management architectures are therefore introduced to enable mobility in IP network. Mobility management requires two parts, location management and hand-off management. Location management is responsible of keeping track of the position of a MN at all times, which allows it to be reachable from the outside. Hand-off management takes care of maintaining existing connections when the MN changes its point of attachment to the network.

We distinguish two types of mobility management, macromobility and micro-mobility. The objective of macro-mobility protocols is to allow users to move in large areas while maintaining both their reachability and their current connections. They also intervene when an inter-technology handover is executed (3G to WLAN for example). MIPv6 is the de facto macro-mobility protocol and is an IETF standard communications protocol. Micro-mobility protocols offer fast, seamless and local hand-off control in limited geographical areas. IP micro-mobility protocols are designed for environments where mobile hosts change their point of attachment to the network regularly, which introduces a significant overhead (increased delay, packet loss and signaling). Therefore, they complement macro-mobility protocols, such as MIPv6, by eliminating these overhead, which can hinder the proper functioning of many

protocols, notably real-time wireless applications (e.g., Voice over IP (VoIP)). Examples of some well known IP micro-mobility architecture include Handoff-Aware Wireless Access Internet Infrastructure (HAWAII), Cellular IP and Hierarchical MIP (HMIP) (Campbell *et al.*, 2002).

4.2.2 Mobile IP version 6 (IPv6)

MIP is an IETF standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. Two versions of MIP exist, Mobile IP v4 (MIPv4) (Perkins, 2010) and MIPv6. The former will not be discussed in this paper.

Overview

The basic operation of MIPv6 is illustrated in Figure 4.1. When the MN moves from its home network to a foreign network, it gets assigned a new address that is topologically correct, called Care-of-Address (CoA) (step 1). The mechanism by which the MN gets assigned a CoA is out of scope. Once the CoA is assigned, the MN registers it at its Home Agent (HA) by performing a Binding Update (BU). The HA then sends a Binding Acknowledgment (BA) back to the MN (step 2). When a CN tries to contact the MN, the HA intercepts the packets destined to the MN (step 3). It then tunnels those packets to the MN using the CoA. The MN then tunnels back its answer (step 4). MIPv6 also introduces a mechanism, called Route Optimization (RO), which allows the MN to perform a binding to the CN, allowing a direct communication between the two nodes, therefore bypassing the tunnel (step 5).

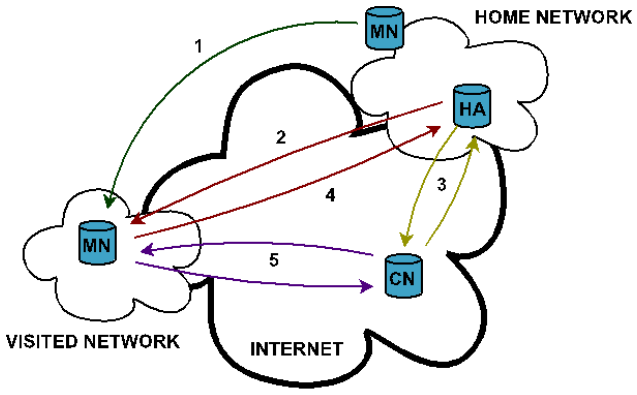


Figure 4.1 Overview of MIPv6

Issues

Even though MIPv6 is a mature standard, and has been for a long time, its deployment is very limited. This is due to several factors:

- MIPv6 requires IPv6 to be deployed. Even though IPv6 has been standardized more than a decade ago, its deployment has been negligible which has delayed the deployments of MIPv6. The introduction of Dual Stack MIPv6 (DSMIPv6) will probably help resolve this dependency by allowing deployment over IP version 4 (IPv4) networks.
- MIPv6 has not been chosen as a mobility solution by any Standards Developing Organization (SDO) who have either elected to create their own protocols (eg. General Packet Radio Service (GPRS), GPRS Tunneling Protocol (GTP) or picked other IETF mobility protocols (eg. MIPv4, PMIPv6). Therefore, there is no pressure on vendors to implement MIPv6 in their equipment.
- the MIPv6 specifications mandate the use of IP Security (IPSec) and Internet Key Exchange (IKE) for securing signaling between the MN and the HA (Arkko *et al.*, 2004). The interface between MIPv6 and IPSec is not well defined which leads to high implementation cost and complexity. Furthermore, the MN-HA security model requires the setup of one Security Association (SA) per MN, which makes the protocol very hard to deploy.
- There have been several extensions to MIPv6 (Fast Handovers for Mobile IPv6 (FMIPv6) (Koodli, 2009), Hierarchical MIPv6 (HMIPv6) (Soliman *et al.*, 2008), Optimizing MIPv6 (OMIPv6)), but there is no architecture that holds these extensions together. There is no exhaustive catalog of these extensions. It is unclear whether these extensions would work together or not (or even if they intended to work together). This causes a lot of confusion and incompatible implementations.
- MIPv6 requires signaling messages to be sent from the MN after each handover. It also requires periodic refresh messages to refresh bindings at the HA as well as to refresh key material for route optimized traffic signaling. Every data packet sent by the MN consumes an additional IPv6 header leading to extra overhead (40 bytes extra constitutes a large overhead, percentage wise, for small packets like VoIP). This overhead is typically incurred on a radio link where the spectrum is both limited and extremely expensive.
- Operators desire to be in control of the mobility management. Since MIPv6 does not involve entities in the access network, operators perceive this to be a threat. They may desire to make a multi-access terminal (a terminal that is capable of accessing different types of networks, such as 3GPP Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), Wireless Fidelity (WiFi)...) connect

to a lower bit-cost link or a less congested link when available. Furthermore, network nodes may have additional information about the dynamic conditions. This information can be utilized by network-assisted mobility protocols or sent to the MN as an update of an existing routing rule to make it reflect the dynamic conditions of the network.

4.2.3 Proxy Mobile IPv6

PMIPv6 is a new standard at the IETF. Sometimes referred to as network-based mobility management, it provides similar functionality to that of MIPv6, however it does not require any modifications to the MN's network stack, i.e. the mobility is taken care of by the network. As such, PMIPv6 eliminates all signaling on the radio interface, reducing therefore congestion and minimizing the impact on the MN energy consumption.

Overview

PMIPv6 is based on MIPv6 and introduces two nodes, the Local Mobility Anchor (LMA) and the Mobile Access Gateway (MAG). The LMA is the home agent for the MN in a PMIPv6 domain. The MAG is the entity that is responsible for detecting the mobile node's movements to and from the access link and sending the Proxy BU (PBU) messages to the LMA, who answers with a Proxy BA (PBA). It therefore acts as a proxy to the MN.

The mobile access gateway has the following key functional roles:

- It is responsible for detecting the MN's movements on the access link and for initiating the mobility signaling with the mobile node's local mobility anchor.
- It emulates the mobile node's home link on the access link by sending Router Advertisement (RA) messages containing the MN's home network prefix(es), each prefix carried using the Prefix Information option (Narten *et al.*, 2007).
- It is responsible for setting up the forwarding for enabling the MN to configure one or more addresses from its home network prefix(es) and use it from the attached access link.

Figure 4.2 illustrates the overview of a handover in PMIPv6. When the MAG detects the MN's attachment, it will send a PBU (step 1) to the LMA, who then answers with a PBA (step 2). When the MN migrates (step 3), the new MAG (nMAG) , after detecting the MN's attachment, sends a PBU (step 4) to the LMA, who then answers with a PBA (step 5). This handover is therefore performed without any interaction or knowledge from the MN.

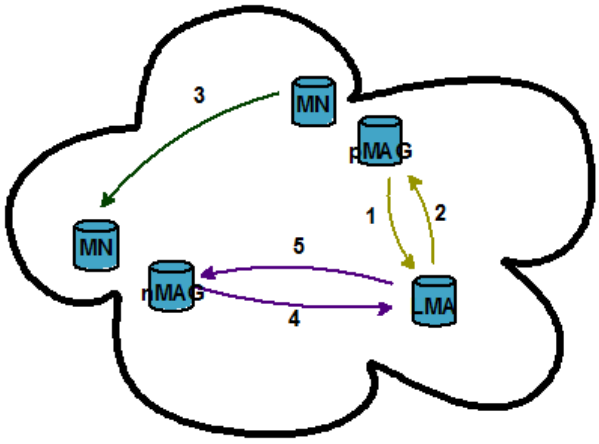


Figure 4.2 Overview of PMIPv6

Issues

PMIPv6 was touted as the replacement of MIPv6 that solves all of the issues mentioned earlier. Unfortunately, PMIPv6 introduces its own drawbacks:

- Poor (almost non-existent) multi-access support
- Issues with inter-technology hand-overs (some being addressed in (Le et Liebsch, 2009))
- No support for Simultaneous Multi-Access (SMA), which allows the terminal to be connected through multiple interfaces at the same time
- Higher operational complexity in the network.

4.3 Proposed Solution

In light of the multiple issues listed in the previous section, the need for a working mobility solution still exists. Our objective in this paper is to propose a new mobility solution that draws upon the strengths of both MIPv6 and PMIPv6, while addressing their shortcomings. We also address the need for a coherent architecture document that ties several extensions together.

Since our solution must be both client and network managed, we face two possible evolution paths: we can either evolve MIPv6 by introducing network mobility or we can evolve Proxy Mobile IP (PMIP) by introducing cooperation from the MN. Either path should provide us with a hybrid mobility solution that is both network and client driven. We chose to evolve MIPv6 because the main goal of PMIP is not to involve the MN in the mobility. Therefore, it felt more natural to evolve MIPv6 by introducing network-based mobility rather than evolving PMIP by introducing cooperation from the MN.

4.3.1 Overview of Our Solution

Contrary to MIPv6, our solution is highly modular and splits the functionalities in different documents. As a building block, we have taken the current MIPv6 specifications and removed all non-essential parts, thus producing a smaller, lighter document that we call the base module. This module is described in the following section. The rest of the functionalities will be described in modules, which can be seen as extensions to the base document. There are four types of modules: security modules, extension modules, bootstrap modules and profile modules. These modules are described in 4.3.4. Finally, to address the issue of the absence of a coherent architecture that ties these extensions together, we introduce the notion of profiles. A profile describes what extensions must be implemented by nodes that wish to support that particular profile, allowing an easier interoperability between nodes. Profiles are described in Section 4.3.5.

4.3.2 Base Module

The base module is the document describing the core mechanisms needed for a working MIP communication. It is much smaller than the current MIPv6 specifications and the goal is to keep it as light and stable as possible. Minor revisions to this document are allowed, if deemed necessary. These should only be done in justifiable cases (newly discovered vulnerabilities for example).

The removed components are the following:

– All mechanisms related to the bootstrapping.
– All mechanisms related to the security aspects.
– All mechanisms deemed non-essential, such as RO.

Because of the lack of bootstrapping mechanisms, the core document makes the following assumptions:

– The mobile has a home address.
– The MN knows the address of its HA.
– The MN knows the prefix of its home network.

These assumptions are insured by the bootstrap module as described in Section 4.3.4. The parameters can be either statically configured or dynamically obtained.

All security mechanisms present in the original MIPv6 specifications have been replaced with an interface that the base module offers and that must be implemented by security modules. The purpose of that security interface is to decouple the security mechanisms from the base specifications. This allows faster and easier development of different security schemes to be used by MIP, by moving the security implementation into security modules

(see Section 4.3.3), removing therefore the need to modify the base specifications every time a new security mechanisms is introduced.

The next sections describe the security interface to be implemented by security modules, as well as the security requirements for each type of message.

4.3.3 Security Interface

The security interface is comprised of four functions that must be implemented by the security modules.

Binding Updates

The mobile node must apply the function secureBU on BU before sending them. This function protects the integrity and the authenticity of these messages.

This function accepts the following parameters, in that order:

- The IPSec mode (either tunnel or transport).
- The IP header.
- The IP payload.
- The care-of address of the MN.
- The home address of the MN.
- The address of the HA.

The HA must then apply the function validateBU on the secure packet to validate it. It accepts the same parameters as secureBU.

Binding Acknowledgments

The home agent must apply the function secureBA on the BA messages. This function protects integrity and authenticity of these messages and therefore would be identical to secureBU.

This function accepts the same parameters as the secureBU function.

The MN must then apply the function validateBA on the secure packet to validate it. It accepts the same parameters as secureBU.

Binding Errors

The HA must apply the function secureBE on the Binding Error (BE) messages. This function protects integrity and authenticity of these messages and therefore would be identical to secureBU.

This function accepts the same parameters as the secureBU function.

The MN must then apply the function validateBE on the secure packet to validate it. It accepts the same parameters as secureBU.

Payload Packets

The MN and the CN must apply the function secureData on the payload packets. This function protects integrity and authenticity of these packets and may ensure their confidentiality.

This function accepts the same parameters as the secureBU function.

The HA must then apply the function validateData on the secure packet to validate it and decrypt it, if necessary. It accepts the same parameters as secureBU.

4.3.4 Modules

There are four types of modules that can interact with the base specifications: security modules, extension modules, bootstrap modules and profile modules.

Security Modules

Security modules specify the security mechanisms that must be used by all the nodes implementing the profile. Each security document describes exactly one security scheme. There may exist any number of security documents, and all interaction between a security module and the base specifications would be done through the defined security interface (see Section 4.3.3). Revisions for a particular security module are allowed as long as backward compatibility is maintained. If this requirement cannot be satisfied, a new module must be created.

Extension Modules

An extension module extends the functionality of the base specifications. The objective of such modules is usually to either enhance the functionalities of the base mechanisms or to add new mechanisms. Extension modules differ in nature and because of their non-deterministic heterogeneity, there is no defined interface in the base specifications that can be used by extension modules. Therefore, extension modules can specify new behaviors to existing nodes, as well as alter existing behaviors. They may also define new types of nodes. Revisions for a particular extension module are allowed as long as backward compatibility is maintained. If this requirement cannot be satisfied, a new module must be created.

Bootstrap Modules

A bootstrap module insures that all assumptions in Section 4.3.2 are fulfilled. More specifically, such a module provides one mechanism for each of the following issue:

- Assigning a home address to MN.
- Assigning HA to MN.
- Enabling a MN to know the prefix of its home network.

Profile Modules

A profile module describes all the modules that constitute a particular profile. Profiles are described in detail in the following section.

4.3.5 Profiles

A profile is a collection of MIP modules that allows vendors and SDOs to create a well-defined package of MIP that fulfills their needs. Profiles also insure interoperability between the different nodes communicating in MIP. New profiles are defined in profile modules (Section 4.3.4) and should be submitted to and approved by the IETF. Upon approval, a profile must be issued a unique identifier.

Specifically, a profile indicates which revision of the base specifications to use, which security module to use, which bootstrap module to use and which extension modules, if any, to use. Therefore, a node wishing to implement that profile must implement all the modules specified by that profile. Furthermore, a profile describes all the mechanisms by which the modules it includes interact. These mechanisms might otherwise be non-intuitive or non-existent. It is therefore the profile's responsibility to make sure that there are no ambiguities in how all the different modules it includes interoperate.

Different profiles cannot be assumed interoperable. It is possible to create different revisions for a same profile. These revisions would be numbered sequentially and each revision must be backward compatible with all previous revisions (ie. with a smaller revision number) of the same profile. If such compatibility cannot be insured, a new profile should be created instead.

A node implementing our solution must support one or more profiles. All nodes that support a same profile can therefore communicate. The revision to be used by the nodes is the highest one supported by all nodes. For example, a MN supporting Profile 1 Revision 5 can associate with a HA supporting Profile 1 Revision 7. In such a scenario, the revision used would be 5, which is the highest supported by both nodes (6 and 7 are not supported by the MN).

Extension Modules

The first profile we propose is a profile that is backwards compatible with MIPv6 (RFC3775). It includes the following modules:

- The core document.
- The security document describing the security mechanisms in MIPv6 (i.e. IKE, IPSec).
- The bootstrap document describing the bootstrap mechanisms in MIPv6 (i.e. Dynamic Home Agent Address Discovery (DHAAD)).
- The RO extension module describing the RO mechanisms in MIPv6.

Figure 4.3 is an overview of the MIPv6-compatible profile.

4.3.6 Mobile Node Proxy

In this section, we introduce a new entity whose role is to manage signaling on behalf of the MN. It allows the network to manage mobility while keeping the MN's involvement. It's effectively a hybrid between a client-based and a network-based solution and can be labeled as a "client-based network-assisted" solution. It therefore reduces the radio overhead of MIPv6 without completely relying on the network for mobility management. Another major advantage is that the MN Proxy approach allows the development of extension mechanisms without impacting the MN. For example, a well designed RO method between MN Proxy and CNs may not require any MN involvement.

Assumptions and requirements

It is assumed that:

- a secure link exists between the MN Proxy and the MN (how the link is secure is out of scope).
- a link failure detection mechanism is deployed on the link.
- the MN Proxy is located in the first IP hop, eliminating the need for discovery.

The following requirements must be satisfied:

- the proxying must be requested by the MN.
- a proxy node must be authorized by the MN to act as MN Proxy.
- the HA must be aware of the identity of the node proxying for the MN.
- the MN should be allowed to perform base MIP operation.
- the MN signaling has precedence over MN Proxy signaling.

New messages

We introduce the following new messages:

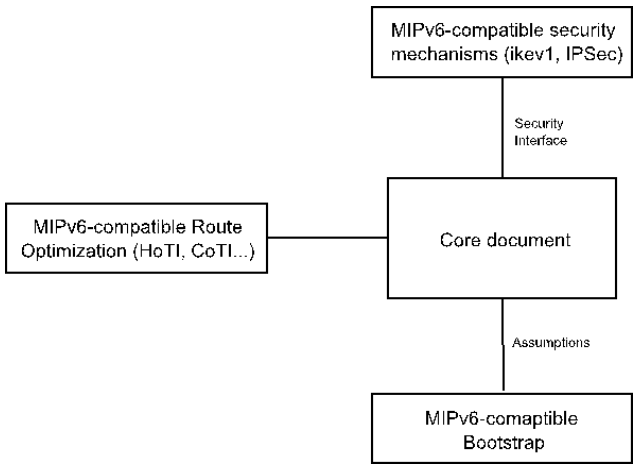


Figure 4.3 MIPv6-compatible profile

- Delegated BU (DBU), a BU message sent by the MN Proxy to the HA.
- Delegated BA (DBA), a back message sent by the HA to the MN Proxy in response of a DBU.
- Proxying Request Initiation (PRI), a message sent to request a node to act as MN Proxy for the MN
- Proxying Request Acknowledgment (PRA), a message sent by the MN Proxy in response to a PRI.

Operation overview

Since the MN Proxy is located in the first IP hop, there is no need for discovery per se. However, the MN needs to learn the capabilities of the MN Proxy. To request a proxying session, the MN sends a PRI message to the MN Proxy, who can then accept or reject that request based on local policies. Then, the MN Proxy sends a DBU to inform the HA that he is proxying for the MN. The DBU contains the chosen profile. Then, the HA replies with a DBA message to the MN Proxy. At this point, the MN Proxy performs all the operations described in the profile on behalf of the MN.

Route optimization with MN Proxy

One of the added values of the MN Proxy is that it allows the introduction of new functionalities to be run inside the network without any impact on the MN. We therefore proposed an implementation of RO that is fully managed by the network. It reuses the same mechanisms as those found in MIPv6, but the binding occurs between the MN Proxy and the CN. The MN remains oblivious to the bindings. The details of this method are described in

Figure 4.4.

The handover process, however, differs from the one found in MIPv6. When the MN moves, the new MN Proxy sends a BU to the HA. The HA must reply with a BA which will include the RO list option. This option lists the addresses of all the CNs using RO with the MN through the MN Proxy and is sent by the MN Proxy (inside a BU) to the HA when a new RO is established. Upon the reception of that option, the new MN Proxy is then able to trigger the RO process with the listed CNs. The handover process is depicted in Figure 4.5.

4.4 Comparison Between Our Solution, MIPv6 and PMIPv6

Our proposed solution is a hybrid that draws from both MIPv6 and PMIP, i.e. it offers both client and network mobility-managements. As such, it inherits advantages from both solutions. In the next sections, we compare our solution to the two existing protocols and show that it addresses their flaws.

4.4.1 Our solution vs MIPv6

Our solution distinguishes itself from MIPv6 on two aspects: it introduces network mobility management and it offers a modular architecture. Those characteristics prove to be essential in addressing the numerous flaws of which MIPv6 suffers (presented in Sec. 2.2.2) :

- Although our solution is also dependent on IPv6, it is very conceivable that a module is created to enable dual stack mode (akin to DSMIPv6 which would allow the solution to be deployed on IPv4-only networks).
- Being modular, our solution will be an attractive solution to SDOs as it will allow them to create a profile that is tailored to their needs and ensuring compatibility between equipment that wish to adhere to that profile. Furthermore, since all profiles share the same base module, it will allow easier integration of multiple profiles within a single equipment.
- By decoupling the security mechanisms from the core and by introducing a clear security interface between them, the complexity and implementation costs of developing new security modules are highly reduced.
- The role of a profile is to offer a mean of grouping together a set of extensions that would be approved and maintained, which should eliminate compatibility problems.
- The MN Proxy module offers our solution network management capabilities. Our solution will therefore see a reduction of the overhead incurred on the radio link, freeing more bandwidth for data. This is mainly due to the fact that the tunnel now ends at the MN Proxy instead of the MN, which eliminates an IPv6 header. For small packets (VoIP

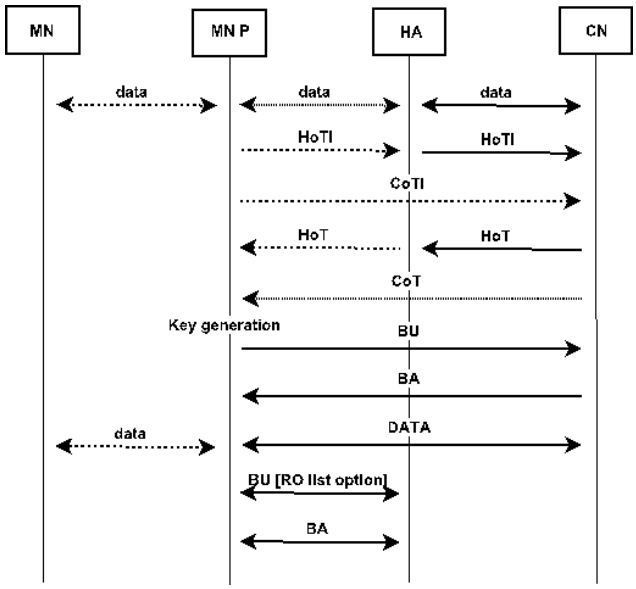


Figure 4.4 RO process

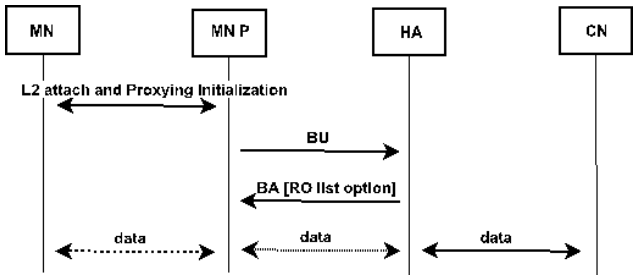


Figure 4.5 RO process when handover occurs

for example), this results in a considerable improvement (Figure 4.6). Furthermore, by eliminating the need for BU packets to reach the MN, an improvement on the latency will be gained. For example, for a packet of size 60 bytes, we see a reduction of 40% of overhead incurred on the radio link.

– Network mobility management also allows network operators more control and can increase the efficiency of the network by utilizing the additional information that the MN is unaware of.

4.4.2 Our solution vs PMIPv6

By allowing client mobility management, our solution solves the main drawbacks from which PMIP suffers. Mainly, it allows the client to notify the network when a new link is detected. This is crucial when multiple, inter-technology, access is required. Let's take an example to illustrate this problem. Say Bob is taking the bus back home and is on the phone with Alice. When Bob arrives home, it would be preferable that the conversation switches to his fixed service, using his private wireless network. Now, the problem we are facing is that, from the operator position, the connectivity ends at the client's modem. The wireless network is therefore hidden and link detection is therefore impossible to do by the network. This means that a pure network mobility management solution, such as PMIP, would not be able to go ahead with this inter-technology handover. With our solution, since the MN is solicited, it can alert the network which can then go ahead and hand-over the session. Table 4.1 shows a summary of the comparison between all three protocols.

4.5 Conclusion

In this paper, we proposed a new mobility protocol, based on MIPv6, that adds network assisted mobility while retaining the client based mobility-management of MIPv6. As a building block, we separated the core functionalities of MIPv6 from the other mechanisms

Table 4.1 Comparison betweens protocols

	MIPv6	PMIPv6	Our solution
Client mobility-management	Yes	No	Yes
Network mobility-management	No	Yes	Yes
Security interface	Not defined	Not defined	Well defined
Modular	No	No	Yes
Coherent mobility architecture	No	No	Yes
Multi-access support	Possible	Impossible	Possible
Radio link overhead	High	Low	Low

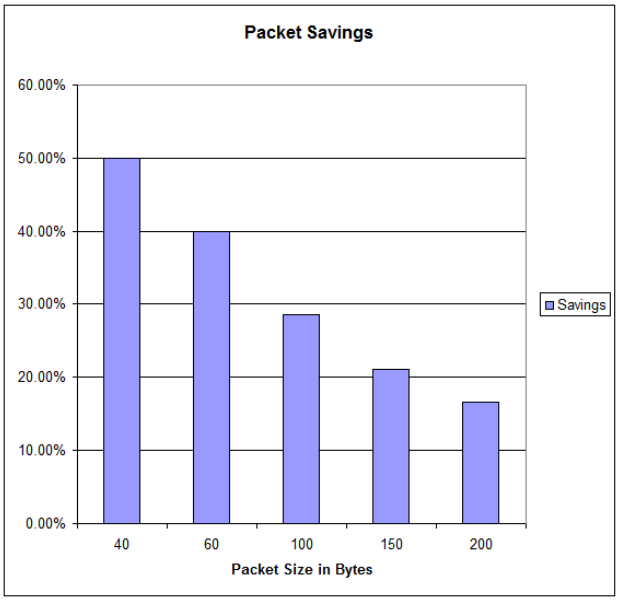


Figure 4.6 Bandwidth savings vs MIPv6

found in the current specifications. This step provided us with a lighter and more stable core document that turns the protocol into a modular one. It allowed us to create extensions which will interface with this core document. These extensions include bootstrapping modules, responsible of setting a proper environment for the protocol, security modules and other modules. We also introduced the notion of profiles, which allow interoperability between nodes.

The protocol we propose is the result of an evolution path from MIPv6 to introduce network mobility-management. This was achieved by introducing a new node, the MN Proxy, that handles mobility on the behalf of the MN, offering better performance than MIPv6, notably by reducing traffic on the radio link. Furthermore, by retaining the client's assistance in mobility, our proposed solution does not suffer from the shortcomings of PMIP, i.e. lack of Fixed-Mobile Convergence (FMC) for instance. Future work will therefore focus on new extensions to further improve the efficiency of our protocol, such as new security schemes and new mechanisms (multicast support for example).

CHAPITRE 5

SEAMLESS HANDOVER FOR MULTICAST MOBILE IPV6 TRAFFIC

Auteurs : Georges Abou-Khalil, Suresh Krishnan et Samuel Pierre.
Revue : Soumis dans le journal *International Journal of Wireless and Mobile Computing* en décembre 2012.

Abstract

Mobile IP v6 is an IETF protocol that manages mobility, allowing a Mobile Node to continue to be reachable after an IP address change, result of a handover. However, when multicast applications are used, this address change results in a disruption of the service, because of the packet loss that occurs while the Mobile Node is rejoining the multicast group. Hence, we propose a new multicast scheme that provides a seamless multicast service during a handover in a Mobile IP v6 network. The proposed scheme achieves its goal by adding a new node, denoted the Multicast Buffering Agent, whose role is to buffer the packets when the Mobile Node is performing the handover. These packets would otherwise be lost. We present an analysis of the buffer sizes to find the optimal sizes. Simulation results, obtained with OPNET, show that by properly sizing the buffers, seamless multicast handover can be achieved with the proposed scheme.

5.1 Introduction

With the rising popularity of multimedia services, operators are forced to ensure that their networks are capable of handling the sudden rise of bandwidth required to satisfy the demand. Increasing link capacity is only part of the solution; operators need to also implement optimization techniques to minimize bandwidth waste. Multimedia services fall into two categories: on-demand and live. Each type presents its own set of challenges. When dealing with on-demand multimedia services, such as video-on-demand, the biggest challenge is the enormous bandwidth requirement to satisfy the demand for audio and video, in a real-time network with real-time interaction. Customers are serviced individually and therefore must be allocated dedicated resources. This obviously presents scalability issues as the number of customers increases. An approach to solving this problem is implementing caching servers closer to customers. These servers would then cache the most popular services

(new movie releases, for instance), shortening therefore the traffic paths needed for those services. This reduces both required bandwidth and latency. On the other hand, live services, such as live streaming or videoconferencing, impose a different kind of challenge. In this case, caching is usually not a possibility as content is being received at the same time - or almost - as it is produced. However, since every customer subscribed to a feed receives the same data, the implementation of a proper multicast architecture becomes an essential mechanism for operators to deploy. Multicast is the mechanism allowing the transmission to a group of clients where only one copy of the data is sent by the source and intermediate nodes only duplicate this data when necessary. This greatly reduces wasted bandwidth, especially near the source. Implementing a proper multicast architecture presents its own set of challenges. For instance, as of today, it is still lacking deployment on a large scale. Some operators might deploy multicast natively in their network, however multicast traffic is seldom transferred between networks and is usually discarded by border gateways. This obviously hinders its wide adoption. Some solutions have been presented to overcome that issue, as we'll discuss in the next section. Another issue with multicast traffic, when combined with user mobility, is the lack of session continuity when a handover occurs. Horizontal handovers are usually not an issue since it occurs between different wireless access points that use the same underlying technology. It is therefore IP-agnostic and does not interfere with the proper functioning of multicast services (since the IP address remains the same). Vertical handovers, on the other hand, will disrupt traffic as they usually incur a change of IP address, which forces the Mobile Node (MN) to resubscribe with its new address. Proper measures therefore have to be taken to insure proper continuation of multicast services during a vertical handover.

In this paper, we present a solution that ensures a seamless and continuous multicast service for a MN, while a vertical handover is occurring. Our solution is based on packet buffering and introduces a new node, denoted Multicast Buffering Agent (MBA), acting as a multicast proxy while the MN is in transition. Although interactive services, such as video-conferencing, also benefit from proper multicast implementation, our solution is geared more towards live application (such as video streaming). The former, by its interactive nature, imposes far stricter requirements on latency, which inhibits the use of buffers. Live applications, on the other hand, are labeled as near real-time traffic, where a short delay (even in seconds) between the production and consumption of the traffic is acceptable and sometimes even necessary, to permit the amortization of packet jittering and to therefore enable a better user experience.

The rest of the paper is organized as follows: in Section 5.2, we explore the related works. In Section 5.3, we present the details of our solution. In Section 5.4, we present our simulation results. Finally, in Section 5.5, we conclude and discuss our future works.

5.2 Related works

In this section, we will review the most relevant works on different issues related to multicast deployment for Mobile IP (MIP) networks. As explained earlier, multicast is the mechanism that allows the transmission to a selection of clients while minimizing the number of sent packets, as the intermediate nodes will take care of packet duplication when necessary. As an example, let's consider the network shown in Figure 5.1. Assuming that the source wants to send a packet to all highlighted clients using multicast, it need not to send that packet more than once. Router 1 will then duplicate this packet, sending a copy to router 2 and router 3. Router 2 will then send 2 copies of that packet, one to each of the subscribed clients. Router 3 will also need to send 2 copies of that packet, one to the subscribed client and another to router 4. Finally, Router 4 will send a copy to each of the subscribed client to which it is attached. This gives us a total of 9 multicast packets, as opposed to 17 had the transmission method been in unicast. In that scenario, using multicast transmission yields a saving of 47% over unicast transmission. Multicast, however, presents its own set of challenges. Multicast issues related to mobility can be divided into two groups: multicast listener mobility issues and multicast source mobility issues Schmidt *et al.* (2010). The former deals with issues arising when the multicast listener (ie. the node subscribed to a multicast group) executes a handover and therefore changes its IP address. The latter deals with issues arising when the Multicast Source (MS) (ie. the node producing the stream) executes a handover and therefore changes its IP address. Only multicast listener mobility will be discussed in this paper, as our target application are live (streaming) applications, in which we assume a fixed source node.

5.2.1 Mobile IPv6 defined multicast solutions

Mobile IP v6 (MIPv6) Johnson *et al.* (2004) proposes two simple approaches for the multicast listener mobility problem. The first solution, called bi-directional tunneling, consists in encapsulating the multicast traffic in point-to-point unicast tunnels. The Home Agent (HA) receives the multicast traffic to which the MN is subscribed, encapsulates it in a point-to-point unicast tunnel and sends it to the MN. The MN then decapsulates them to retrieve the multicast packets. This method has two advantages. First, the reconnection time when a handover occurs is only influenced by the time needed to setup the tunnel. Not needing to rejoin the multicast tree (since the HA is the one who is natively receiving the multicast traffic) reduces considerably the reconnection latency for the MN. The second advantage is that this method will work regardless of the existence of multicast support in the networks. It allows multicast traffic to transit domains that are multicast-agnostic, by shielding its multi-

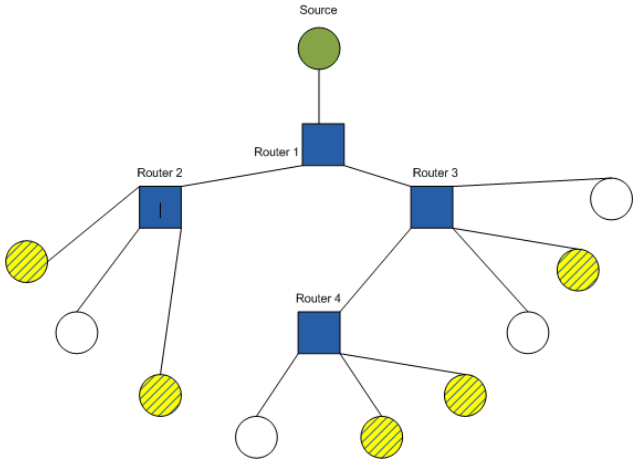


Figure 5.1 Multicast example

cast nature. However, because the multicast nature is lost, and traffic is now in unicast form, it suffers from tunnel convergence problem and may result in traffic duplication. Scalability becomes a big issue with this solution. We therefore lose the biggest advantage of multicast, which is to eliminate unnecessary packet duplication.

The second solution proposed by MIPv6 is called the remote subscription approach. Basically, this solution consists in the MN subscribing natively to the multicast groups. While this solution provides near optimal routing as it fully profits from the multicast benefits, it presents two major issues, both consequences of using multicast transmission natively. First, it requires multicast awareness from the visiting network and all transit networks. If that condition is not satisfied, then the MN will not be able to join the multicast tree. The other issue with that approach is that it suffers from slower handovers, relying on multicast routing to rejoin the multicast tree. The time it takes to rejoin a multicast tree is usually an order of magnitude higher than the time needed to establish a unicast tunnel. Table 5.1 summarizes the pros and cons of the two multicast solutions proposed by the MIPv6 standard.

In the next sections, more complex solutions will be presented, that are either based on

Table 5.1 MIPv6 existing multicast solutions

	Bidirectional tunneling	Remote subscription
Pros	- Very fast reconnection - Works regardless of multicast support	- Near optimal routing
Cons	- Unnecessary packet duplication	- Requires multicast support from end to end - Joining the multicast tree can be time consuming

one of the MIPv6 proposed solutions, or are a hybrid of both.

5.2.2 Other multicast solutions for MIPv6

Other solutions have been proposed for the MIPv6 multicast problem. Some of them, such as Hong-Ke Zhang (2007), rely on the existence of a node called a multicast agent, which holds the multicast context of MNs in the network. Multicast agents act as local tunneling proxies, allowing for some inter-agent handover when the MN moves. All these solutions therefore suppose that the context state was stored within a network node that is reachable before and after a move. However, such a condition cannot always be guaranteed. That can occur, for example, when the MN moves from one operator's network to another. In such a scenario, a backwards compatible way to recover from loss of connectivity must be implemented.

Other solutions which have been proposed are hybrid solutions, combining both tunneled and native multicast. One early hybrid architecture was introduced in Garyfalos et Almeroth (2005a). It relies on reactively operating proxy-gateways located at the Internet edges. An Intelligent Gateway Multicast was introduced as a bridge between mobility-aware native multicast management in access networks and mobility group distribution services in the Internet core, which may be operated on the network or application layer. Another approach was introduced in Wählisch et Schmidt (2007), called the Hybrid Shared Tree approach. It proposed a mobility-agnostic multicast backbone on the overlay.

More work is being done to develop general architectural approaches for hybrid multicast solutions Buford (2008b) and a common multicast API for a transparent access of hybrid multicast Wählisch et Schmidt (2007) that will require a detailed design in future work.

5.2.3 Multicast solutions for MIPv6 variants

Multiple protocols, based on MIPv6, have been presented to either enhance or extend the functionalities of MIPv6, such as Fast Handovers for Mobile IPv6 (FMIPv6) Koodli (2009), Hierarchical MIPv6 (HMIPv6) Soliman *et al.* (2008) and Proxy Mobile IP v6 (PMIPv6) Gundavelli *et al.* (2008), for which solutions have been proposed for multicast mobility issues. Although these solutions only work for a specific variant, we will review two of them, because they attempt to solve the multicast handover issue. The first work Leoleis *et al.* (2006) proposes an extension of the FMIPv6 protocol to integrate multicast handover support solution. This is accomplished by enabling the new access router to become a recipient of the multicast traffic of interest via tunneling, as well as by buffering the tunneled traffic for the period during which the mobile is unable to communicate, due to link layer commu-

nication unavailability. The second one min Kim *et al.* (Feb.) proposes a multicast scheme to prevent service interruption for multicast traffic in a PMIPv6 environment. It also uses buffering techniques to achieve this goal, by having the previous as well as the new Mobile Access Gateway (MAG) buffer the packets during the handover.

5.2.4 Large scale multicast support

As stated earlier, one of the challenges that multicast faces is that, while it might be supported inside most networks, it is seldom allowed to exit. This, in effect, creates multicast islands where each domain enables multicast support inside the network, but no inter-domain support is deployed. To overcome this problem, Automatic Multicast Tunneling (AMT) Bumgardner (2012) is a protocol that has been introduced that uses UDP-based encapsulation to overcome this obstacle. It works by enabling sites, hosts or applications that do not have native multicast access to a network with multicast connectivity to a source, to request and receive multicast traffic from a network that does provide multicast connectivity to that source. With such a protocol, it is therefore not unreasonable to assume multicast connectivity throughout the Internet.

5.3 Proposed solution

In this section, we present the details of our proposed solution, which provides seamless handover for multicast traffic in a MIPv6 network.

5.3.1 Assumptions

Our solution makes the following assumptions:
- Mobility is handled by MIPv6;
- Multicast support is ensured end-to-end (either natively or not);
- Packets are tagged with a sequence number (Real-time Transport Protocol (RTP) for example);
- Multicast traffic is real-time and is being buffered by the application (video streaming for example);
- Handovers can be predicted in advance (for proactive mode);
- The multicast traffic is not encrypted.

5.3.2 Overview of the proposed solution

The goal of our solution is to ensure seamless IP handover for multicast groups. We accomplish this by introducing a new node, denoted Multicast Buffering Agent (MBA), whose

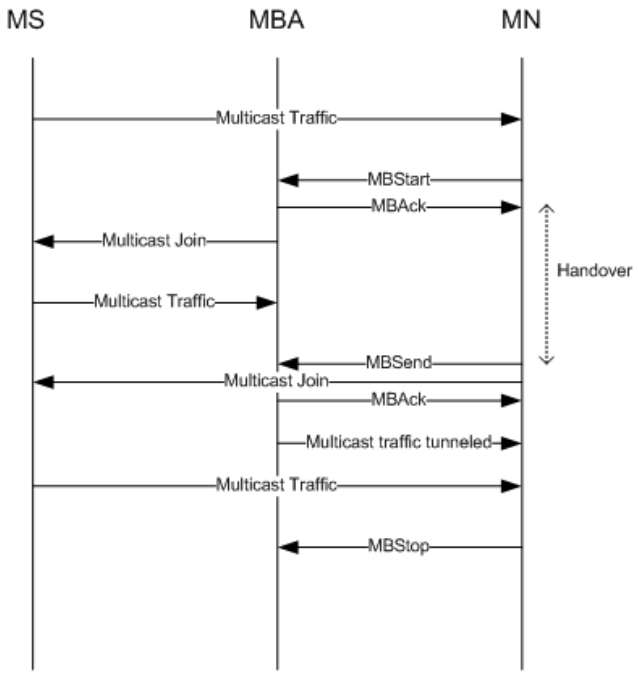


Figure 5.2 Sequence diagram (proactive mode)

role is to buffer the multicast packets while the MN is offline. We consider the MN being offline from the time it starts the handover process until the time it rejoins the multicast group and receives the first multicast packet. In standard MIPv6 implementation, these packets would be obviously lost, resulting in an interruption of the user experience. The flow of our solution is as follows. The MN is subscribed to one or more multicast groups. We also assume that the application is buffering the multicast data. As the MN is about to do a handover, it alerts the MBA by sending a Multicast Buffer Start (MBStart) packet, which contains the list of the multicast groups to which the MN is subscribed. Upon reception of this message, the MBA subscribes to these groups if needed, and starts buffering incoming packets. When the handover is complete, the MN sends a Multicast Buffer Send (MBSend) to the MBA from its new network attachment. This packet will contain the list of multicast groups that need to be recovered as well as the sequence number of the last packet received for each of the groups. Upon reception of this message, the MBA sends the corresponding packets to the MN, for each requested group. These packets are sent by unicast. To achieve seamless handover, without loss of packet or the need to pause and buffer, the buffers of both the application on the MN and the MBA need to be properly sized. A study on the impact of these buffers is presented later in this section.

5.3.3 Modifications to Mobile IPv6

In order to implement our proposed solution, a new node, the MBA, must be implemented, as well as modifications to the MN and to the HA. Other nodes (Correspondant Node (CN), intermediate routers and others) need not be modified.

Multicast Buffering Agent

The MBA is a new node that we introduce whose role is to serve as a proxy to the MN, while it's offline. It can be placed anywhere in the network, including being colocated with the HA. Each network can have one or multiple MBAs, for load balancing purposes. A MBA can redirect the MN to another MBA based on location, load, group subscriptions and/or other metrics. The address allocation of the MBAs as well as their discovery by the MNs is to be statically configured by the operators. Dynamic configuration and discovery could be possible, but is left out of scope.

New messages

Our solution also introduces fives new packets to the MIPv6 protocol, all of which are to be sent between the MN and the MBA:

- Multicast Buffer Start (MBStart);
- Multicast Buffer Send (MBSend);
- Multicast Buffer Stop (MBStop);
- Multicast Buffer Ack (MBAck);
- Multicast Buffer Error (MBError).

These new packets follow the same format as the mobility header defined by MIPv6.

A MBStart message is sent by the MN to notify the MBA that a handover is imminent and that it should start buffering the specified multicast groups. Therefore, it contains the address of at least one multicast group to which it is subscribed. In the case of a Source-Specific Multicast (SSM) group, it will also contain the list of the sources. Upon receiving this message, the MBA must either acknowledge with a MBAck or a indicate an error by responding with a MBError. Possible errors related to a MBStart are the following:

- MN is not authorized to use the MBA's services;
- Multicast group is not available to be buffered;
- Request must be differed to another MBA for various reason (message must therefore contain the address of the alternate MBA).

A MBSend message is used by the MN to the MBA to ask for transmission of buffered packets for the a multicast group. Therefore, it contains the address of the multicast group

as well as the sequence number of the first packet and the number of paquets that the MN wishes to receive. By settings the number of paquets to 0, the MN can request all buffered packets from a certain sequence number. Upon receiving this message, the MBA will send the requested buffered packets via unicast. The MBSend packet may contain the addresses of multiple groups. A MN can also send multiple MBSend messages for a same group. This is necessary, because by the time the MN rejoins the multicast group and starts receiving the packets natively, it might have to request for buffered packets multiple times to make sure no packet loss occurs. If the MBA cannot satisfy the request by the MN, it responds with a MBError. Possible errors related to a MBSend are the following:

- MN is not authorized to use the MBA's services;
- Requested packets have not been buffered;
- Request must be differed to another MBA for various reason (message must therefore contain the address of the alternate MBA).

A MBStop message is sent by the MN to inform the MBA that buffering is no longer needed for a certain multicast group. Therefore, it contains the addresses of the multicast groups in question. The MBA need not acknowledge this message. This allows the MBA to keep track of which multicast groups need to be buffered. The implementation of such tracking would require maintaining a database and is left out of scope.

5.3.4 Reactive mode

One of the assumptions enunciated in Section 5.3.1 is that the MN must be able to predict its handover in advance, so that it can alert the MBA to start buffering the needed groups. This assumption is only valid in certain scenarios. For example, if a MN is connected to a 3GPP Long Term Evolution (LTE) network and wants to handover to a WIFI network, the prediction is possible because the LTE network is still available. However, if that same MN is connected to a WIFI network and moves out of it, it will need to handover to the LTE network. In that case, it might not have enough time to predict the handover, depending on the speed at which it is exiting the WIFI coverage. Therefore, our solution, in its current state, cannot function properly because of the failure of the MN to alert the MBA that a handover is occuring.

To overcome this problem, we propose a modification to our solution where the MN need not alert the MBA prior to handover. We call this behaviour the reactive mode (the previous mode will be referred to as the proactive mode). In this mode, the MBA is constantly buffering the multicast group. Therefore, after the handover, the MN can just send an MBSend message to start receiving the multicast buffers, without having sent an MBStart prior to it. Once the handover is executed, the sequence of events of the reactive mode is

identical to the proactive mode.

The decision of which multicast groups are to be available in reactive mode is left to the network operator. This list could, for example, dynamically evolve depending on the popularity of the groups (which could be measured by the number of MBSend messages per group).

5.3.5 Buffer sizes

One of the key elements to the success of the proposed solution is the proper sizing of the buffers. Therefore, in this section, we will discuss the impact of the size of the application buffer of the MN as well as the size of the multicast buffer of the MBA. By properly sizing these buffers, our solution will allow the MN to achieve seamless handover. Undersized buffers will cause packet loss, which will most probably lead to a disruption in the service. Oversized buffers, on the other hand, will waste valuable ressources. In this study, we consider multicast traffic where both the packet rate and packet size are constant.

Let's suppose we have a MN subscribed to a certain multicast channel and that its application buffer can hold N packets. Now we suppose that, while the MN is offline, M packets are dequeued. If $N \geq M$, then the MN application buffer is properly sized and no packet loss will occur because of that buffer. However, if $M > N$, then the buffer is undersized since the MN would have dequeued all the packets in the buffer and would be waiting for further packets. This has two adverse consequences. First, the user experience will be disrupted while waiting for further packets (in a streaming application, this usually results in a forced pause). Second, the MN would have to either increase its application buffer size, or deliberately drop packets (thus inducing packet loss) to be able to rejoin the native multicast traffic, without constantly relying on the MBA. That is because its buffer would overflow otherwise, since it would be receiving more packets than it can buffer (thus would always be required to ask the MBA for missed packets).

The same reasoning can also be applied for the MBA multicast buffer. Let's suppose the MBA has a buffer of P packets for a certain multicast group. That buffer will hold the lost packets by the MN while it is offline. Therefore, it is important that P must be bigger than this number of packets, otherwise packet loss will occur as the MN will be asking for packets that have been buffered, but then discarded because of the overflow. The required buffer size therefore depends on multiple factors, such as packet rate, packet size and the time during which the MN is offline.

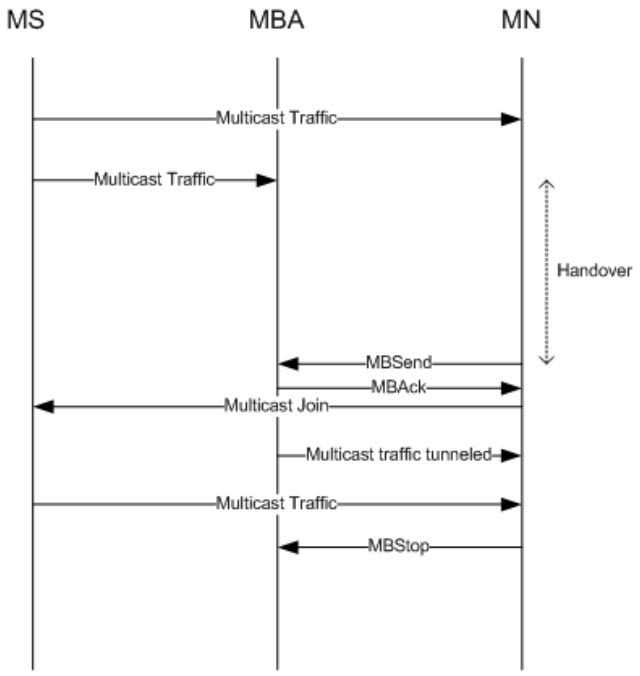


Figure 5.3 Sequence diagram (reactive mode)

5.3.6 Security

So far, we have assumed that the multicast groups to which the MN is subscribed are not encrypted. However, some groups require a subscription and will therefore not be viewable by everyone. This requires the MN to properly authenticate itself to receive the decryption key, if it has the proper authorization. That key will allow the MN to decrypt the multicast traffic. Because the MBA is proxying the MN, it needs to have the same authorization to the groups it's buffering, otherwise it would be incapable of performing its duty. The security aspect of the MBA is left out of scope in this paper.

5.3.7 Example scenario

In this section, we will illustrate the basic functioning of our solution with an example. Let's consider the following parameters:

- All multicast packets are of the same size;
- The multicast packet rate is 4 packets per second (both reception and consumption);
- The MBA is constantly buffering the multicast packets (reactive mode);
- The handover process takes 1 second;
- Rejoining the multicast tree after a handover takes 2 seconds.

The first step is to properly size the buffer. Since the MN will be offline for 3 seconds and the packet rate is 4 pk/s, the MN needs to be able to sustain a loss of 12 packets while being offline, which means that its application buffer needs to be able to contain at the very least 12 packets. In our example, we'll choose an application buffer size of 16 packets. Now, let's suppose that the MN is about to move. Just before starting the handover, the buffer state is shown in Table 5.2. Since the handover process takes 1 second, the MN will have dequeued 4 multicast packets. The buffer state, after the handover is over, is shown in Table 5.3 (E denotes empty cells). At that point, the MN will do two things simultanously. It will request the missing packets from the MBA by sending a MBSend, starting from packet 71, as well as rejoining the multicast group. We assume that the first operation is completed in less time than the packet rate. The result is that the MN will receive the 4 multicast packets it missed, from the MBA (Table 5.4). By the time the MN rejoins the multicast tree and receives the first packet, it will have dequeued 9 multicast packets. The buffer state at that point is shown in Table 5.5. The final step at that point is for the MN to request the 8 missing packets, starting from packet 75. Upon receiving those packets, the recovery is complete and the MN can then alert the MBA that it no longer needs buffering for that multicast group. This is shown in Table 5.6.

5.4 Simulation model and results

5.4.1 Overview

To simulate our model, we used the Optimized Network Engineering Tool (OPNET) software suite, developed by OPNET Technologies. It provides a comprehensive development environment for the specification, simulation and performance analysis of communication networks. OPNET provides four tools called editors to develop a representation of a system being modeled. These editors, the Network, Node, Process and Parameter Editors, are organized in a hierarchical fashion, which supports the concept of model level reuse. Models developed at one layer can be used by another model at a higher layer. The simulations were executed on a Windows XP desktop, featuring an Intel Core 2 CPU and 4GB of RAM.

Before implementing our solution, we considered the scenario depicted in Figure 5.4. That scenario illustrates how a traditional multicast handover occurs in a MIPv6 environment, using native multicasting (remote subscription). The following parameters are used in our simulations:

- The MN and the HA both implement MIPv6;
- The multicast traffic is at a rate of 15 packets per second.

Figure 5.4 illustrates a simple multicast handover scenario in a MIPv6 environment. In

Table 5.2 Initial buffer state

55	56	57	58	59	60	61	62
63	64	65	66	67	68	69	70

Table 5.3 Buffer state after handover

59	60	61	62	63	64	65	66
67	68	69	70	E	E	E	E

Table 5.4 Buffer state after first MBSend

59	60	61	62	63	64	65	66
67	68	69	70	71	72	73	74

Table 5.5 Buffer state after rejoiging multicast group

68	69	70	71	72	73	74	E
E	E	E	E	E	E	E	83

Table 5.6 Buffer state after recovery

68	69	70	71	72	73	74	75
76	77	78	79	80	81	82	83

that scenario, we have a MN that is initially located in its home network, served by the Home Router (HR), which also acts as its HA. The MN is subscribed to a multicast group, offered by a MS. At that time, the MN receives the packets natively through its home address. The MN then moves out of its home network (out of the range of the HA) and into a foreign network, served by a Foreign Router (FR). The MN will then execute a handover, where it will obtain a new address from the FR (Care-of-Address (CoA)) and register that address with the HA, so that it stays reachable through its home address. The MN will also rejoin the multicast group served by the MS using its new CoA.

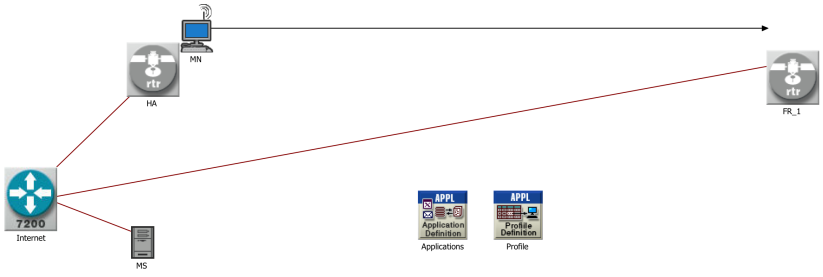


Figure 5.4 MIPv6 handover scenario

To implement that scenario, we used the following OPNET entities:

- One wlan_ethernet_router, which represents the HA, as well as the HR. This node has two interfaces (radio and ethernet) and implements MIPv6;
- One wlan_ethernet_router, which represents the FR. This node has two interfaces (radio and ethernet);
- One wlan_wkstn_adv, which represents the MN. This node has one interface (radio) and implements MIPv6;
- One CISCO7000 router, which represents the backbone;
- One ethernet_server, which represents the multicast server. This node has one interface (ethernet);
- One Application Config and one Profile Config to define the multicast application.

When simulating this scenario, we observe the following, as presented in Figure 5.5:

- From the start of the simulation until the 35s mark, the MN is receiving the multicast traffic natively;
- Between the 35s mark until the 45s mark, the MN is offline while doing the handover, hence not receiving any multicast traffic;
- From the 45s mark until the end of the simulation, the MN is receiving the multicast traffic tunneled through the HA.

As predicted, in that scenario, packet loss occurs while the MN is offline. That would translate in the MN having to stop the video feed to restart buffering. The user will therefore lose a part of the stream.

To implement our solution, we added a new node, the MBA, which is illustrated in Figure 5.6. In our simulation, we implemented the reactive mode, in which the MBA is already subscribed to the multicast group and constantly buffering. The flow of this simulation is similar to the previous one, except that when the MN is done with the handover, it will not

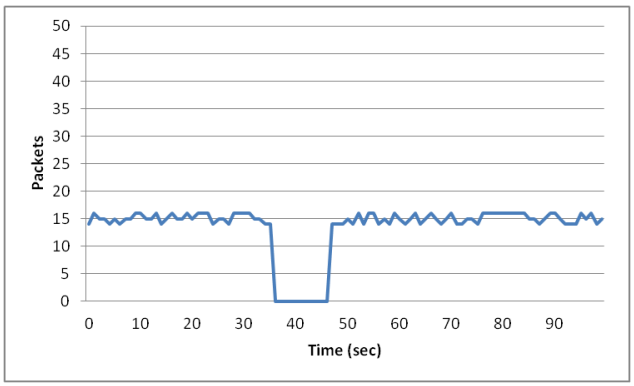


Figure 5.5 IP packets received with standard MIPv6 handover

only resubscribe to the multicast group, but also ask the MBA for the packets it missed while being offline. The MBA will then send those packets to the MN through unicast.

As shown in Figure 5.7, the MN receives a larger number of packets when it regains connectivity. These are the buffered packets sent in unicast by the MBA. This allows the application to keep running seamlessly, shielding the handover to the user. In this scenario, we properly sized the MBA multicast buffer to enable the seamless handover. The MN also required sending two MBSend requests : once it regained connectivity and once it received the first native multicast packet after rejoining the group. This proved sufficient to ensure the seamless handover.

We also experimented with shrinking the MBA buffer to observe its adverse effects. Figure 5.8 shows an example of such a scenario. The number of packets received by the MN when it regains connectivity is lower, because of the missing packets due to the buffer overflow on the MBA. This obviously results in a disruption of service, albeit a smaller one compared to the results obtained without the MBA. Figure 5.9 shows the correlation between the size of the MBA buffer and the packet loss. Note that the buffer size of 0 packet represents the simulations without the MBA (ie. standard MIPv6 multicast handover). Moreover, once the minimum size required is attained, no packet loss occurs. Increasing the size further will not have any benefits, unless we modify our scenario to increase the time during which the MN is offline.

5.5 Conclusion and future works

In this paper, we presented a method that provides seamless handover for real-time multicast traffic in a MIPv6 network. In a traditional MIPv6 environment, a vertical handover incurs packet loss, which results in a service interruption for multicast traffic. By implementing our solution, a new node, the MBA, is introduced and its role is to buffer the multicast traffic while the handover is occuring. That allows the MN to change IP addresses in a seamless manner, since it will be able to recover the packets as soon as it gets back connectivity.

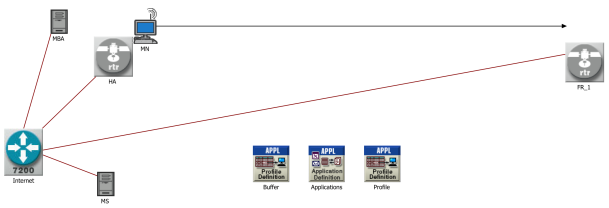


Figure 5.6 MIPv6 handover scenario with proposed solution

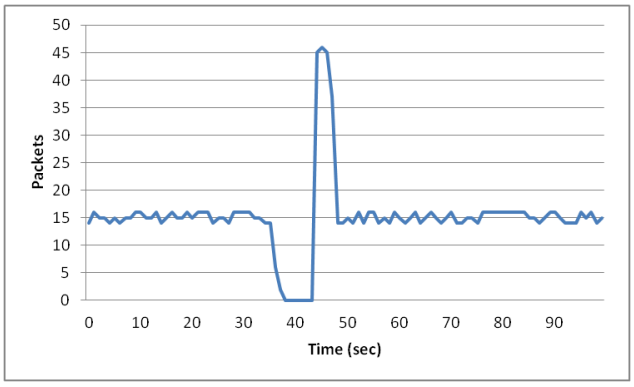


Figure 5.7 IP packets received with proposed solution

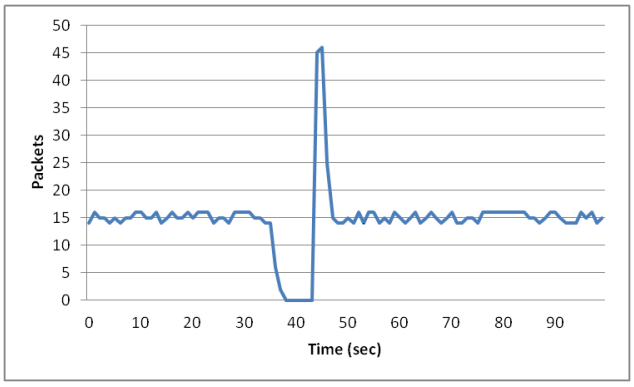


Figure 5.8 Undersized MBA buffer

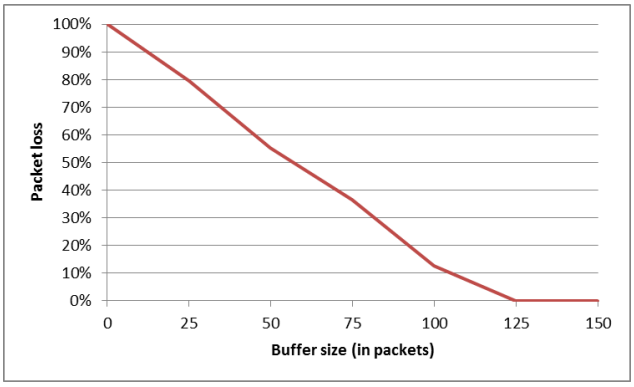


Figure 5.9 Buffer size vs packet loss

To achieve seamless handover, proper buffer sizing must be done, for which we have presented a discussion to find the optimal sizes. Finally, we presented our simulation results obtained with OPNET and that demonstrate the proper functioning of our solution.

Future works include the possibility to expand our solution to work with all real-time applications, notably the ones that have stricter requirements for latency (such as video-conferencing), as well as the aspects that were left out of scope (security, bootstrapping and others).

CHAPITRE 6

DYNAMIC GREENFIELD FIBER TO THE HOME PLANNING

Auteurs : Georges Abou-Khalil, Steven Chamberland et Samuel Pierre.
Revue : Soumis dans le journal *Computers & Operations Research* le 1er mai 2013.

Abstract

In recent years, operators have started deploying fiber optics in their access networks in order to offer higher bandwidth to their clients, keeping up with the evergrowing popularity of bandwidth-intensive applications. While multiple fiber-based technologies exist, one particular technology, Fiber to the Home (FTTH), is gaining momentum. By bringing the fiber optic link all the way to the client's premises, an operator can offer very high bandwidth and be more scalable than with other technologies. Its deployment, however, requires a higher investment. In brownfield environments, it may not be the most suitable technology to deploy, as operators are more inclined to leverage their existing infrastructure (usually copper-based or coaxial). But for greenfield deployment, no existing infrastructure is present, making therefore FTTH a more attractive option. One aspect that is often overlooked is that most deployments are executed in multiple phases, spanning multiple years. It then becomes very important to properly plan and size the network by considering all of these phases and to make sure that choices made in earlier phases do not have a detrimental impact on later phases.

We therefore propose, in this paper, a dynamic planning of FTTH networks, destined for a greenfield environment. The proposed solution is a mathematical integer linear model. We then simulate this model with randomly generated networks and compare our results to those obtained with existing methods, in order to evaluate its performance. Obtained results show an improvement in all simulated scenarios, up to 13%.

6.1 Introduction

The emergence, in recent years, of bandwidth-intensive applications, such as IP TeleVision (IPTV), Video on-Demand (VoD) and video-conferencing, have forced operators to enhance their networks, in order to account for the added requirements. One of their challenges is to properly plan their access networks, as they are often found to be the bottleneck of the

network, especially when bandwidth is concerned. Links found in traditional wired access networks are comprised of copper wires or coaxial cables, offering medium to low bandwidth. In 2012, the average speeds in the United States and in Canada are estimated to be under 10Mbps [1] and the adoption rate of broadband services offering over 10Mbps is estimated to be under the 20% mark[1]. Considering that a single IPTV stream usually requires between 6 and 10Mbps of bandwidth, it becomes critical for operators to upgrade their networks, to be able to satisfy the higher demand.

Multiple technologies are available to the operators that allow them to deploy access networks capable of satisfying the high bandwidth requirements. For telcos, the two most popular available technologies are Fiber to the Home (FTTH) and Fiber to the Node (FTTN). With a FTTH deployment, an optical fiber is run in an optical distribution network from the Central Office (CO) all the way to the subscriber's premises. With a FTTN deployment, an optical fiber is run to a cabinet serving a neighborhood, which then serves clients within a radius of usually under a mile. The clients are served using copper wires (often reusing existing infrastructures). A more in-depth review of these technologies is presented in the next section. A similar technology, called the Hybrid Fiber-Coaxial (HFC), is used by cable providers. FTTN and HFC are both hybrid technologies, as they integrate both fiber optic links and traditional links (copper or cable), offering higher bandwidth than traditional links, but are more limited compared to FTTH. In a brownfield deployment, they are attractive solutions, as they allow an operator to leverage its existing infrastructure, needing only to replace a portion of its access network.

In a greenfield deployment, however, the lack of existing infrastructure reduces considerably the cost advantage of hybrid solutions over FTTH. The long term advantages of FTTH outweigh the added cost it requires. A problem that operators encounter, however, is that the full access network will not necessarily be deployed in a single phase, but will instead be spread over several phases (following the growth of the population, for example). This dynamic aspect of the deployment should be accounted for while planning, as short-sighted choices made early on can have an adverse affect on the long term planning.

We therefore propose a dynamic planning of optical networks destined for greenfield deployment. Our proposed solution is an integer linear mathematical model that allows an operator to properly plan their deployment by taking into account current, as well as future, demands and costs. The rest of the paper is organized as follows: after we present an overview of the different access network technologies available in section 6.2, we review the most relevant related works in Section 6.3. Section 6.4 exposes the problem statement as well as the details of our mathematical model. Section 6.5 presents our numerical results and

1. http://www.akamai.com/stateoftheinternet/

comparatives. Finally, Section 6.6 concludes our work.

6.2 Overview of broadband access network technologies

In this section, we will briefly review the major broadband access technologies available for fixed line operators. A more in-depth review can be found at Corning (2005), including other technologies such as wireless and Broadband Power Lines (BPL).

6.2.1 Digital Subscriber Line (xDSL)

xDSL is the technology that allows the transmission of high speed data over existing copper telephone infrastructure. It does so by allocating different frequency ranges to the voice, upstream and downstream data.

One thing to note is that xDSL technologies are very sensitive to distance and that the further the client is, the lower the obtained bandwidth is. Table 6.1 presents an overview of the main characteristics of the most popular xDSL technologies, Asymmetric digital subscriber line (ADSL), Symmetric Speed Digital Subscriber Line (SDSL), Asymmetric digital subscriber line 2+ (ADSL2+) and Very High Speed Digital Subscriber Line (VDSL).

6.2.2 Fiber to the Node (FTTN) Networks

FTTN networks consist of a fiber feed from the CO to remote nodes that are placed close to the client's premises. From these nodes, the network usually consists of copper lines and a xDSL modem. The nodes therefore take care of the required optical-to-electrical conversion. Cabinets hosting access nodes require space and dedicated power, and must withstand extreme hot and cold weather, lightning and AC cross voltages.

Bandwidth offered by copper-based FTTN depend mostly on the distance between the access node and the client's premises (which dictates the length of the copper wires). When this distance is shorter than a thousand feet (300 meters), high bandwidth can usually be

Table 6.1 Overview of xDSL technologies

Technology	Max Upstream Capacity	Max Downstream Capacity	Max Distance
ADSL	640 Kbps	12 Mbps (0.3km)	5.4 km (1.5 Mbps)
SDSL	3 Mbps	3 Mbps	2.7 km (2 Mbps)
ADSL2+	1 Mbps	26 Mbps (0.3km)	3.6 km (4 Mbps)
VDSL	16 Mbps	52 Mbps (0.3km)	1.3 km (13 Mbps)

achieved using VDSL. This is sometimes referred to as Fiber to the Curb (FTTC), to emphasise the fact that the cabinet is installed closer to the customers. An example of a FTTN network is shown in Figure 6.1a.

6.2.3 Fiber to the Home (FTTH) Networks

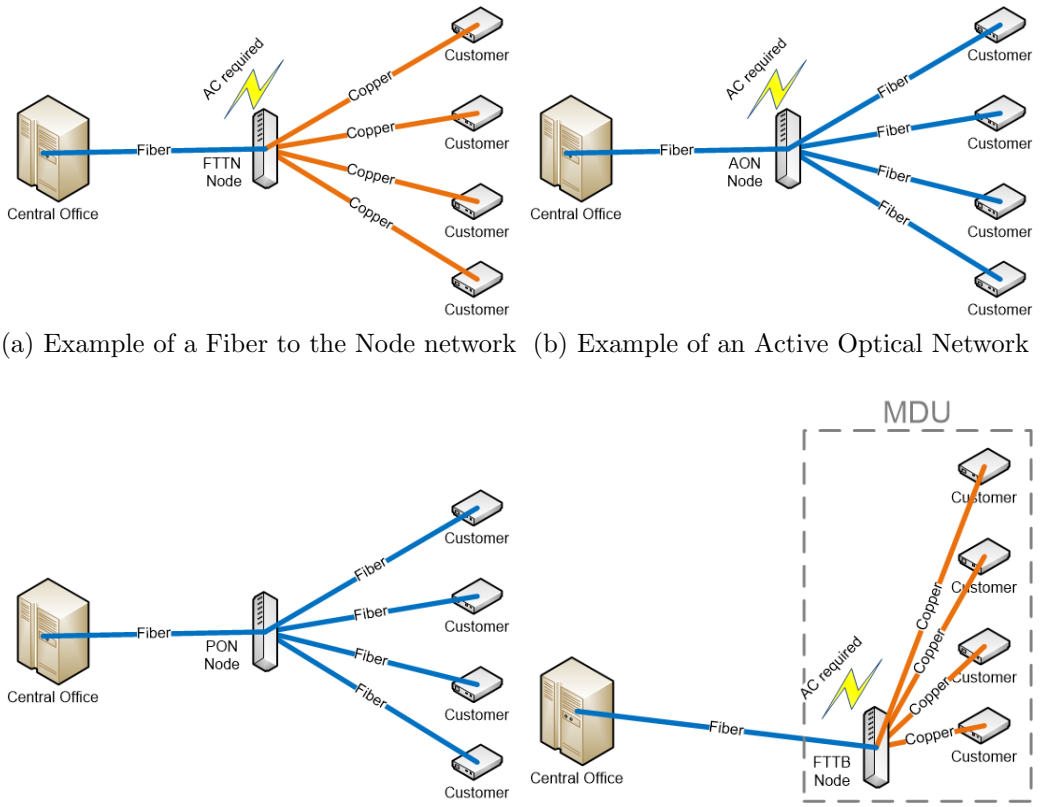
FTTH networks provide an optical fiber from the CO all the way to the subscriber's premises. Although the simplest distribution method is running a direct fiber (ie. one fiber for each subscriber), the more common deployment is to have fewer fibers leaving from the CO, which are then split into individual subscriber-specific fibers. These shared fibers are split relatively close to the subscribers. Two possible technologies are available to achieve such splitting: Active Optical Networks (AONs) and Passive Optical Networks (PONs). In a AON, the splitting is achieved using electrically powered network equipments, such as routers and switches. These equipments typically perform layer 2 switching or layer 3 switching (layer 3 routing usually occurs at the CO). An example of an AON is active ethernet, which employs optical ethernet switches to distribute the signal, effectively forming a single large switched ethernet network between the subscribers and the CO. These networks are akin to standard ethernet computer networks deployed in businesses. An example of a AON is shown in Figure 6.1b.

In comparison to AONs, PONs use unpowered optical splitters (beam splitters) to distribute the signal. The two major PON technologies are Gigabit PON (GPON) Hood (2012) and Ethernet Passive Optical Network (EPON) Beck (2005). Both carry signals over a single stand of fiber. The Optical Line Terminal (OLT) in the CO is connected to optical splitters, which then distribute the signal via multiple fibers that terminate in the Optical Network Terminals (ONTs) at the clients' premises. Downstream transmission (from the CO to the customers) is in broadcast mode, meaning that all the customers receive the same signal simultaneously. To allow the ONT to identify the client's data, an addressing scheme is used. Encryption is also desirable to prevent eavesdropping. As for the upstream transmission, Time-Divison Multiplexing (TDM) is used to control the transmissions of the ONTs, preventing any collisions on the fiber to the OLT. GPON and EPON share a lot of similarities, key differences being the bandwidth management and line rates. An example of a PON is shown in Figure 6.1c.

6.2.4 Fiber to the Building (FTTB) Networks

FTTB networks are a hybrid alternative to PONs and FTTNs. While an access node exists, akin to FTTN, it is placed at the customer's premises. The termination of the sub-

scribers can then be either xDSL, Gigabit Ethernet (GbE) or any other type of network technology desired (except that of optical nature). The main advantage that FTTB offers over FTTN is that the equipment cabinet need not be hardened, since its location is in a controlled environment. FTTB is usually used to serve multiple subscribers (Multiple Dwelling Units (MDU) being the most common examples), although it is possible to serve a single subscriber (which is rarely cost effective that way). An example of a FTTB network is shown in Figure 6.1d.



(a) Example of a Fiber to the Node network (b) Example of an Active Optical Network

(c) Example of a Passive Optical Network (d) Example of a Fiber to the Building network

Figure 6.1 Broadband access network technologies

6.3 Related works

6.3.1 Access network design

The design of telecommunications networks involves large and complex mathematical programming models (which are often mixed-integer programming models). A survey on local access network design models and solution methods can be found in Balakrishnan *et al.*

(1991) and Gavish (1991). The resulting models are often difficult to solve optimally, except for relatively small network configurations. They are usually decomposed into modules, which are then either solved optimally or approximated using heuristic methods. Exact solving usually involves methods like the Langrangian relaxation Shaw et Shaw (1994), dual ascent Balakrishnan et et al. (1989) or linear programming. Heuristics methods include simulated annealing Lukic (1999), tabu search Girard *et al.* (2001) and genetic algorithms Routen (1994).

6.3.2 Copper-based broadband access networks

Multiple copper-based technologies exist, which include xDSL, FTTC and FTTN. The term copper broadband access networks is generically used to refer to these technologies and was introduced in Carpenter *et al.* (2001). The main difference between them is the bandwidth they can offer. The general rule is that the shorter the copper, the higher the bandwidth. However, from a design point of view, there are no differences between the different technologies, only the values of some parameters differ. The copper broadband access network design problem can be found first in Carpenter *et al.* (1996) and then in Mazur (1999), where it is extensively studied. It is later restricted in Carpenter *et al.* (2001) where contiguity constraints are added to insure more practical solutions.

6.3.3 PON broadband access networks

Recently, work has been focusing more on PON networks. In Li et Shen (2008), the authors decompose the PON planning problem into two sub-problems: allocation with a clustering of Optical Network Units (ONUs) in order to determine the ONU to be connected to the same splitter and optimal sizing and placement of the splitters. They propose two heuristics to tackle the problem, the second one being based on the algorithm found in Cooper (1963). Their results show that their proposed algorithm reduces PON deployment costs by 50-70% compared to another method (benchmark sectoring scheme). Moreover, they examine the deployment of PONs throughout the location-allocation problem of splitters, and their work can be found in Lee *et al.* (2006). They model the problem using mixed-integer programming to determine optimal placement of nodes. This is done for both the single splitting problem and the distributed splitting problem (which includes multi-level splitters). They obtain their results using a column generation model, which they then compare to a lower bound obtained by Linear Programming (LP), after relaxing constraints. The obtained gap were however rather large (up to 81%). A relaxation of their objective function is proposed in Kim *et al.* (2011) and, combined with a local search heuristic, a

reduction of that gap was achieved. Mitcsenko *et al.* (2009) addresses the broadband optical access network design by minimizing deployment costs while taking operation issues into account, using detailed cost and network models of FTTx technologies that suit best to actual networks due to detailed cost metrics used instead of just minimizing fiber lengths. They present a heuristic solution that works fast even for large problem instances, providing results with a difference less than approximately 10-20% from the computed Integer Linear Programming (ILP) optimum for smaller cases where ILP could be used. Along with these algorithms, case studies of real-life network and service requirement instances (number of customers ranging from 400 to 20.000) are presented. Another proposed optimization scheme for PON planning is presented in Jaumard et Chowdhury (2012). The work is split into three phases. In the first phase, several potential equipment hierarchies are generated, where each equipment hierarchy is associated with an ONU partition such that a switching equipment is associated with each cluster, each ONU belongs to a single cluster. The splitting ratio of the equipment corresponds to the number of ONUs in the cluster. In the second phase, a column generation mathematical model is used to select the type and location of the switching equipment, for each equipment hierarchy, that leads to the minimum cost multi-stage equipment topology which accommodates all the traffic demand. The third phase selects the best hierarchy among all the generated and dimensioned hierarchies.

6.3.4 Dynamic access network planning

All work presented in the preceding sections assume a static planning (single phase). Some work have been proposed that tackle the dynamic (multiphase) problems. An example of an early work that introduces the dynamic aspect in network planning can be found in Shulman (1991). The goal is to find a time schedule and as well as the proper sizing for installing facilities at plant locations, in order to minimize the discounted cost of capital expenditures over the planning horizon. The problem is formulated as a combinatorial optimization one, that allows consideration of more than one facility type and finds the optimum mix of facilities in each location. It is then solved using a Lagrangian relaxation technique and the obtained results are shown to be within 3% of the lower bound for a wide range of input data. More recent works on dynamic planning include Dias *et al.* (2007) and Zhao *et al.* (2010). The former work considers the possibility of expanding or reducing the maximum available capacity at any given location during the planning horizon while the latter proposes a complete and generalized migration model towards FTTH.

6.4 Problem statement and optimization model

6.4.1 Problem statement

In this paper, we propose a new model for FTTH network planning that takes into consideration the dynamic aspect of such networks. To do so, we define a phase as an arbitrary period of time during which cost and demand, as well as the location of cabinets and clients, are fixed. By varying these parameters from one phase to another, we obtain a set of input data defining a dynamic network. Our goal is then to minimize the total cost of the network planning while considering all the phases at once. The total cost includes the cost of placing the splitters (including the cost of connecting them to the CO), as well as the cost of the links between the clients and the splitters. By considering all phases at once, we ensure that the optimal solution is obtained for the whole planning process.

Another approach to solving such a problem would be to solve optimally each phase sequentially, starting at phase 1, and feeding the obtained result of solving a phase as input for the next one. Although each phase is individually solved to obtain its optimal solution, no garantees can be made about the optimal solution of the whole process. Choices made in earlier phases can have adverse effects on later phases. By considering all the phases at once, we eliminate this short-sighted aspect of the planning. The same reasoning can be applied to another approach, which is to consider solely the final phase and then backtrack that solution onto earlier phases. Some choices made for the final phase might not be valid in earlier phases. The next section presents a simple example that illustrates these problems.

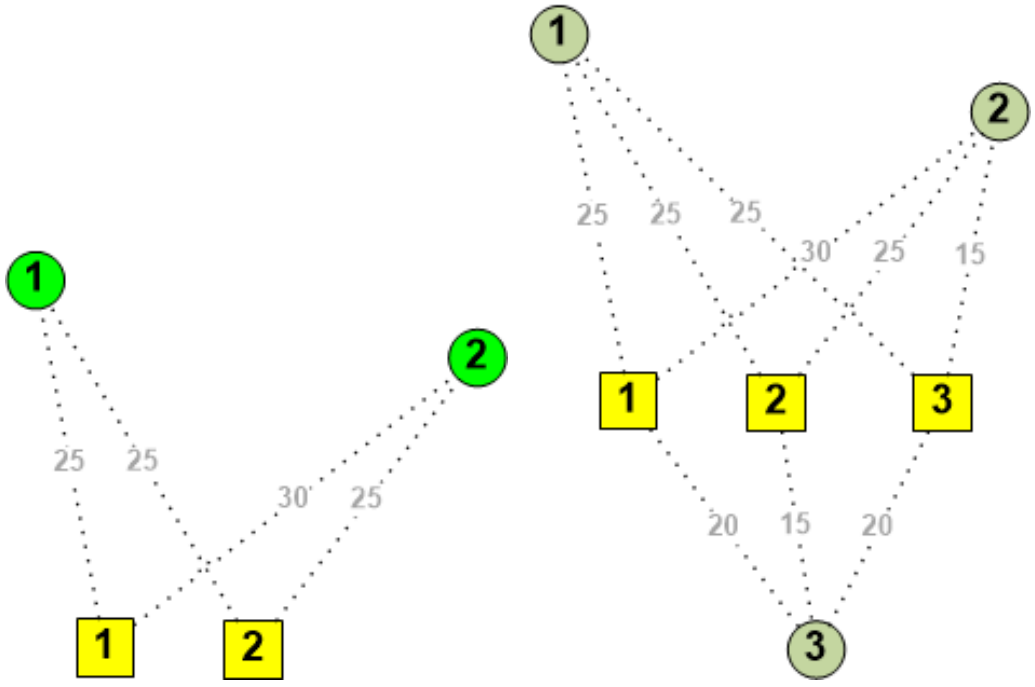
6.4.2 Example scenario

Let us consider a simple example of a network planning spanning two phases, illustrated at Figure 6.2. In phase one, we have two clients (square elements) and two sites where nodes can be installed (round elements). In phase 2, a third client is present, as well as a third site. All the costs of linking a client to a node in a particular site are shown. Now, let's assume the cost of installing a node is 50, and is the same for all sites at both phases. The optimal solution for this network, when considering all phases, is shown at Figure 6.3. For phase 1, we have a cost of 105 and, for phase 2, we have an added cost of 15. The total cost of the planning is 120.

Let us now consider the resolution done phase by phase, starting at phase 1 (we'll call it the sequential method). The obtained solution using that method is presented in Figure 6.4. As we can see, the obtained cost of the first phase is 100, which lower than the cost obtained at the first phase with the optimal solution. However, the added cost at phase 2 is 25, for a total cost of 125, wihch is higher than the optimal cost. This is due to the fact

that the choice of installing a node in site 1 instead of site 2, although better in the first phase, has a detrimental impact for phase 2. As we can see, the sequential method suffers from shortsightedness.

Another approach would be to consider solely phase 2 (the final phase) and then backtrack the choices onto earlier phases (in our case, phase 1). We'll call that approach the backtrack method. The optimal solution for phase 2 using that approach is shown in Figure 6.5. The problem with that approach is that the assignments cannot be backtracked, because of the absence of Site 3 in phase 1. Therefore, this approach yields solutions that are not directly feasible. It may then be possible to try and fix those assignments for earlier phases or to better guide it by altering the costs of certain links. But that involves additionnal work and is still not garanteed to give us the optimal solution.



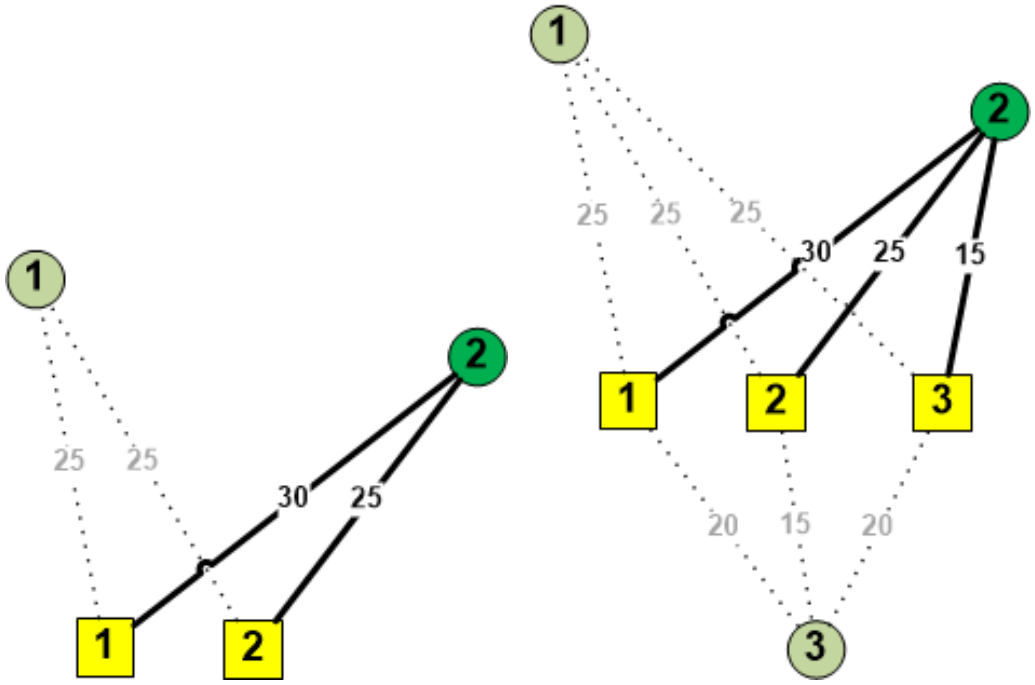
(a) Phase 1 (b) Phase 2

Figure 6.2 Example scenario

6.4.3 Optimization model

Overview

Our objective is to find the optimal network design that minimizes the total cost while satisfying the demand of all the clients, at all phases. Given a set of potential sites (ie. location of cabinets) and a set of demand points (ie. customers) over a discreet number



(a) Phase 1 (b) Phase 2

Figure 6.3 Optimal solution

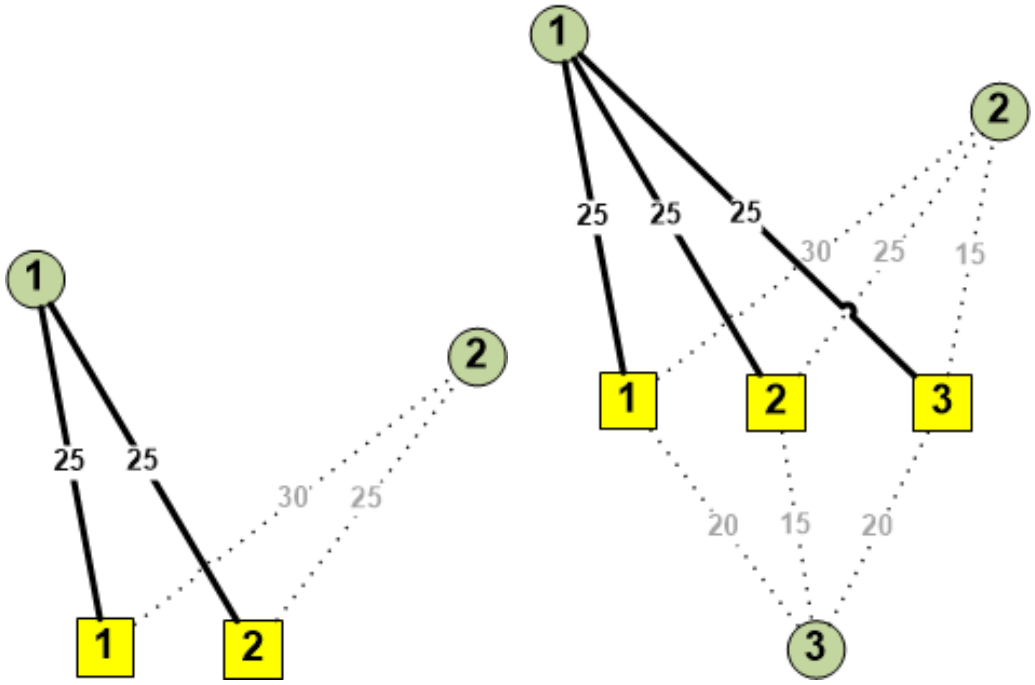
of phases, the resulting output will be, for each phase, a set of nodes (beam splitters) and links which result in the minimal cost of the entire planning. The result must also satisfy a number of constraints, such as the maximum capacity of a node or the maximum capacity of a cabinet.

Our model uses a tree topology to design the access network, where each demand point is served by a distribution tree, at each phase. A distribution tree is composed of a single node and all the clients that are served by it, including the links between the node and those clients. A solution will be composed of a number of distribution trees, per phase, with the number of trees equal to the number of nodes necessary for the planning. The theoretical upper limit of the number of trees is obtained in the worst case scenario, which is when each node is serving exactly one node (ie. each client is served by a dedicated node).

Sets

To model this problem, we first define the following sets:

- Let P be the set of discreet phases considered in the planning horizon ;
- Let D^p be the set of demand points at phase p ;
- Let S^p be the set of potential sites for installing nodes at phase p ;



(a) Phase 1 (b) Phase 2

Figure 6.4 Solution using sequential method

– Let T be the set of distribution trees .

Constants

We also define the following constants that are provided as input to our model:

– Let α be the maximum number of clients that can be served by one node (8, 16 or 32 for example) ;
– Let γ be the maximum bandwidth that a fiber optic link can support (in Mbps) ;
– Let θ^p be the demand per client (in Mbps) at each phase ;
– Let ω be the maximum number of splitters in a cabinet.

Costs

We also define the following costs that are provided as input to our model:

– Let a_i^p be the cost (in \$) of the installation of a node at the site $i \in S^p$ at phase $p \in P$, including the cost of its uplink to the CO ;
– Let $b_{i,j}^p$ be the cost (in \$) of installing a link between the site $i \in S^p$ and the client $j \in D^p$ at phase $p \in P$.

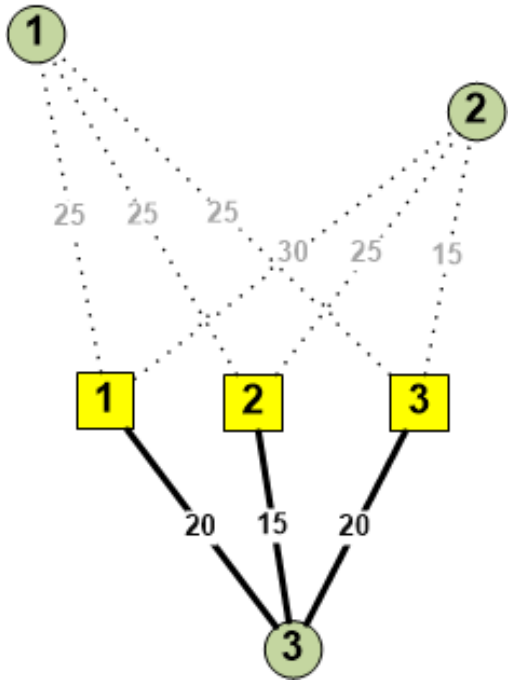


Figure 6.5 Solution using backtrack method

Decision Variables

Finally, we define the following decision variables:

- Let $z_i^{t,p}$ be a binary variable that is set true when a node is installed at the site $i \in S^p$ and used in the distribution tree $t \in T$ at phase $p \in P$;
- Let $y_i^{t,p}$ be a binary variable that is set true when a demand point $i \in S^p$ is served by the distribution tree $t \in T$ at phase $p \in P$;
- Let $l_{i,j}^p$ be a binary variable that is set true when a link exists between the site $i \in S^p$ and the client $j \in D^p$ at phase $p \in P$;
- Let $nl_{i,j}^p$ be a binary variable that is set true when a link exists between the site $i \in S^p$ and the client $j \in D^p$ at phase $p \in P$ and that same link is absent at phase $p-1$;
- Let ns_i^p be the number of nodes installed in the site $i \in S^p$ at the phase $p \in P$;

Objective Function

The objective is to minimize the total cost of the network and is formally defined as follows:

$$MIN \quad \sum_{i \in S^1} ns_i^1 * a_i^1 \tag{6.1}$$

$$+ \sum_{p \in P \setminus \{1\}} \sum_{i \in S^{p-1}} ns_i^p - ns_i^{p-1} * a_i^p \tag{6.2}$$

$$+ \sum_{p \in P \setminus \{1\}} \sum_{i \in [(S^{p-1}+1)..S^p]} ns_i^p * a_i^p \tag{6.3}$$

$$+ \sum_{i \in S^1} \sum_{j \in D^1} l_{i,j}^1 * b_{i,j}^1 \tag{6.4}$$

$$+ \sum_{p \in P \setminus \{1\}} \sum_{i \in S^{p-1}} \sum_{j \in D^{p-1}} nl_{i,j}^p * b_{i,j}^p \tag{6.5}$$

$$+ \sum_{p \in P \setminus \{1\}} \sum_{i \in [(S^{p-1}+1)..S^p]} \sum_{1 \in D^{p-1}} l_{i,j}^p * b_{i,j}^p \tag{6.6}$$

$$+ \sum_{p \in P \setminus \{1\}} \sum_{i \in S^{p-1}} \sum_{1 \in [(D^{p-1}+1)..D^p]} l_{i,j}^p * b_{i,j}^p \tag{6.7}$$

$$+ \sum_{p \in P \setminus \{1\}} \sum_{i \in [(S^{p-1}+1)..S^p]} \sum_{1 \in [(D^{p-1}+1)..D^p]} l_{i,j}^p * b_{i,j}^p \tag{6.8}$$

That cost is therefore the sum of the following eight parts:

1. The cost of installing nodes for the first phase
2. The cost of installing nodes in existing sites for phases other than phase one
3. The cost of installing nodes in new sites for phases other than phase one
4. The cost of installing links for the first phase
5. The cost of installing links between existing clients and existing sites for phases other than phase one (relocation of clients)
6. The cost of installing links between existing clients and new sites for phases other than phase one
7. The cost of installing links between new clients and existing sites for phases other than phase one
8. The cost of installing links between new clients and new sites for phases other than phase one

Constraints

Our model is subject to the following constraints:

$$\sum_{i \in S^p} z_i^{t,p} <= 1 \quad \forall p \in P \quad \forall t \in T \tag{6.9}$$

$$\sum_{i \in S^p} z_i^{t,p} <= z_i^{t-1,p} \quad \forall p \in P \quad \forall t \in T \backslash 1 \tag{6.10}$$

$$\sum_{i \in S^p} z_i^{t,p} >= y_j^{t,p} \quad \forall p \in P \quad \forall j \in D^p \quad \forall t \in T \tag{6.11}$$

$$\sum_{t \in T} y_j^{t,p} = 1 \quad \forall p \in P \quad \forall j \in D^p \tag{6.12}$$

$$z_i^{t,p} <= z_i^{t,p-1} \quad \forall p \in P \backslash 1 \quad \forall i \in S^{p-1} \quad \forall t \in T \tag{6.13}$$

$$ns_i^p <= \sum_{t \in T} z_i^{t,p} \quad \forall p \in P \quad \forall i \in S^p \tag{6.14}$$

$$l_{i,j}^p >= z_i^{t,p} + y_j^{t,p} - 1 \quad \forall p \in P \quad \forall t \in T \quad \forall i \in S^p \quad \forall j \in D^p \tag{6.15}$$

$$nl_{i,j}^p >= l_{i,j}^p - l_{i,j}^{p-1} \quad \forall p \in P \backslash 1 \quad \forall i \in S^p \quad \forall j \in D^p \tag{6.16}$$

$$\sum_{i \in S^p} l_{i,j}^p = 1; \quad \forall p \in P \quad \forall j \in D^p \tag{6.17}$$

$$ns_i^p <= \omega \quad \forall p \in P \quad \forall i \in S^p \tag{6.18}$$

$$\sum_{j \in D^p} y_j^{t,p} <= \alpha \quad \forall p \in P \quad \forall t \in T \tag{6.19}$$

$$\sum_{j \in D^p} y_j^{t,p} <= \gamma \quad \forall p \in P \quad \forall t \in T \tag{6.20}$$

$$z_i^{t,p} \in \{0,1\} \quad \forall p \in P \quad \forall t \in T \quad \forall i \in S^p \tag{6.21}$$

$$y_j^{t,p} \in \{0,1\} \quad \forall p \in P \quad \forall t \in T \quad \forall j \in D^p \tag{6.22}$$

$$l_{i,j}^p \in \{0,1\} \quad \forall p \in P \quad \forall i \in S^p \quad \forall j \in D^p \tag{6.23}$$

$$nl_{i,j}^p \in \{0,1\} \quad \forall p \in P \quad \forall i \in S^p \quad \forall j \in D^p \tag{6.24}$$

$$ns_i^p \geq 0 \quad , integer \quad \forall p \in P \quad \forall i \in S^p \tag{6.25}$$

Constraint (6.9) ensures that only one node can be placed at a time, in a distribution tree. Constraint (6.10) ensures that distributions trees are used in sequential order. Constraint (6.11) ensures that if there is at least one client in a tree then a node must also exist (ie. a tree cannot serve clients if a node doesn't exist). Constraint (6.12) ensures that each client is served by exactly one tree. Constraint (6.13) ensures that once a node is placed in a site, it cannot be removed. Constraint (6.14) calculates the value of the variable ns (numbers of nodes in a particular site, at each phase). Constraint (6.15) calculates the value of l (indicating if a link is present between a site and a client, at each phase). Constraint (6.16) calculates the value of nl (indicating if a new link is present between a site and a client, at each phase). Constraint (6.17) ensures that each client has exactly one link, at each phase. Constraint (6.18) ensures that the maximum number of nodes at each site is not violated. Constraint (6.19) ensures that each node cannot serve more than the limit. Constraint (6.20) ensures that the maximum bandwidth per node is satisfied. Finally, constraints (6.21) to (6.25) ensure the integrality of variables.

Notes

Since the number of required distribution trees cannot be known beforehand (only its upper limit is known), we have to estimate its value. If we choose a lower number than the required one, the obtained solution will be suboptimal, as it constraints the optimization search. However, if we choose a much higher number, it will considerably slow down the search (which is why we don't use the upper limit as value). Therefore, we have added an extra integer variable, nt^p, and the following equation which calculates the number of distribution trees that are in use by the solution:

$$\sum_{i \in S^p} \sum_{t \in T} nt^p = z_j^{t,p} \quad \forall p \in P \tag{6.26}$$

After solving the model, we then compare the largest value of nt^p to the size of the set T. If they are equal, there is a risk that T is undersized. We therefore increase its size and relaunch the simulation. However, if they are not equal, then the size of T is necessarly bigger, and the obtained result is the optimal one.

One aspect of the planning that is not found in the constraints is the limit on the lenghts of the links. Depending on the used technology, that limit can be relatively low (20 kms for example). The idea is that it will be taken care of by the soft constraint. Therefore, if a link is not possible because it would surpass the limit, its cost should be set to a very high

number, thereby discouraging its use in the solution.

6.5 Solution and numerical results

To solve our optimization model described in the previous section, we have implemented it using A Mathematical Programming Language (AMPL). AMPL is an algebraic modeling language for describing and solving high-complexity problems for large-scale mathematical computation. Its advantages include the fact that its notation is very similar to the mathematical notation of the problems, which eases their reading. It also allows the use of dozens of solvers such as CPLEX, FortMP, Gurobi, MINOS, IPOPT, SNOPT and KNITRO. Since our optimization model is a linear one, we have opted for CPLEX as the solver. All the simulations were run on a Core i5 CPU Machine with 8GB of RAM, running Windows 7.

In order to obtain our numerical results, we had to generate multiple scenarios and simulate them. AMPL allows seperate files for the model itself and the data. Therefore, we have developped a C++ program that allows us to generate different input data for our model. By specifying the number of phases, the number of clients per phase, as well as the number of potential sites per phase, our program will generate a scenario in which the clients and potentials sites are placed randomly in a 10km x 10km area. The CO is assumed to be located at the center of the area.

For our simulations, we have chosen to set the number of phases at 2. The maximum badwidth of a single fiber is set at 1Gbps. We have chosen to limit the number of nodes in a single site to 4, and each node can split a fiber to up to 4 clients (1:4 splitters). The demand for each client is set at 50Mbps for the first phase and 100Mbps for the second. The cost of laying fiber is set at 7,160$/km Chen *et al.* (2010) and the cost of a node is set at 900$ Chen *et al.* (2010), plus the cost of fiber between the node and the CO. Table 6.2 summarizes the different parameters and costs used in our simulations.

To evaluate the performance of our optimization model, we started by randomly generating multiple scenarios of different sizes. An example of such a scenario is shown at Figure 6.6 (units are in Meter). In phase 1, we have 3 sites and 5 clients, and that number increases to 6 sites and 10 clients in phase 2. The costs the links between clients and nodes at each site is presented in Tables 6.3 & 6.4.

Solving this scenario gives us a total cost of 306,520$, with 176,895$ for phase 1 and 129,625$ for phase 2. In phase 1, we have a total of 2 nodes installed, one in site 2 and one in site 3. An additional node is installed for phase 2 in site 4. The details of the solution are presented in Figure 6.7.

Then, we compared its result to the sequential method. To do so, we modified our soft

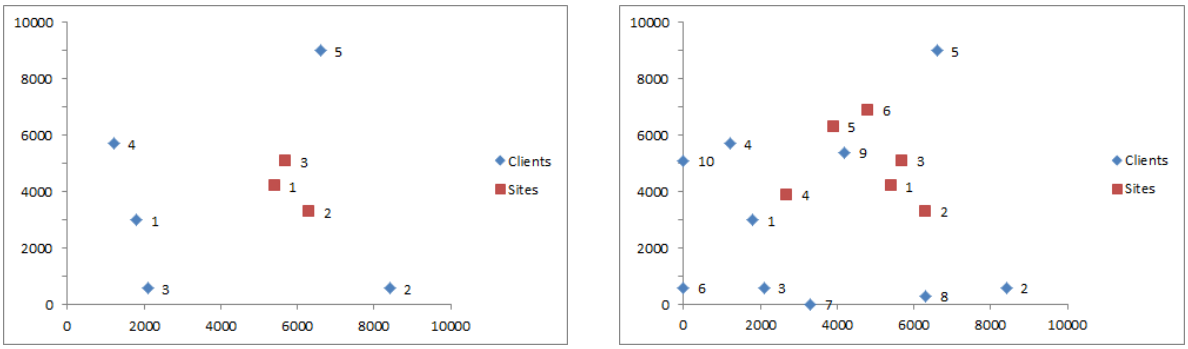
Table 6.2 Parameters and costs for the simulations

Parameter or Cost	Value
Size of area	10km x 10km
Number of phases	2
Maximum number of nodes in a site	4
Maximum number of clients per node	4
Maximum bandwidth per link	1Gbps
Demand per client at phase 1	50Mbps
Demand per client at phase 1	100Mbps
Cost of laying fiber	7,160$/km
Cost of node	900$

constraint in order to emphasize the cost of the first phase, by multiplying it by a large factor. We also added an additional integer variable and an additional constraint, whose sole purpose is to calculate the real cost of the planning. In phase 1, the obtained cost is 170,944$ and a total of 2 nodes were installed. This is better than with our result, which is not suprising since it is the optimal solution when the phase 1 is considered by itself. However, the cost of phase 2 is 144,975$ and 2 more nodes are needed. The obtained solution therefore gives us a total cost of 315,919$, which is higher than the cost obtained with our solution. This clearly demonstrates that choices made for phase 1 have an adverse effect at phase 2 (the need for 4 nodes instead of 3, for example). The details of the solution using the sequential method are presented in Figure 6.8.

Furethermore, we compared our results to the backtrack method, which aims to solve the last phase only (phase 2 in our case) and then backtrack the result onto earlier phases. To simulate this method, we once again modified the soft constraint in order to calculate the complete cost of phase 2 with no regards to phase 1. That result is then multiplied by a large factor and added to the real cost of the solution. With that method, we obtained a total cost of 399,885$, which is again higher than the cost obtained with our solution. As shown in Figure 6.9, some links made in phase 2 are not possible in phase 1, which then forces the solution to choose another link for these clients, degrading the total cost of the solution.

Table 6.5 presents the results of simulations on 16 randomly generated scenarios (scenario #4 being the one we presented earlier). Columns S1, S2, D1 and D2 correspond to the number of sites in phase 1, number of sites in phase 2, number of clients in phase 1 and number of clients in phase 2, respectively. Columns T1 and T2 correspond to the number of distribution trees necessary in phases 1 and 2, respectively. Columns O-Cost, S-Cost and B-Cost correspond to the costs obtained by solving the model using, respectively, our optimal



(a) Phase 1 (b) Phase 2

Figure 6.6 Scenario 1

Table 6.3 Cost of links for Scenario 1 (clients 1 to 5)

	Client 1	Client 2	Client 3	Client 4	Client 5
Site 1	27,170$	33,552$	34,966$	31,932$	35,425$
Site 2	32,291$	24,490$	35,749$	40,357$	40,868$
Site 3	31,714$	37,574$	41,261$	32,505$	28,657$
Site 4	9,113$	47,158$	24,015$	16,776$	45,969$
Site 5	28,006$	51,997$	42,798$	19,803$	27,339$
Site 6	35,229$	51,953$	49,076$	27,170$	19,803$

method, the sequential method as well as the backtrack method. The column S-Diff and B-Diff present the difference between the cost obtained using our optimal method and the costs obtained with the sequential method and the backtrack method. Finally, the computing time required for our method is presented in the last column. Figure 6.10 also presents the comparison of the three costs for all scenarios.

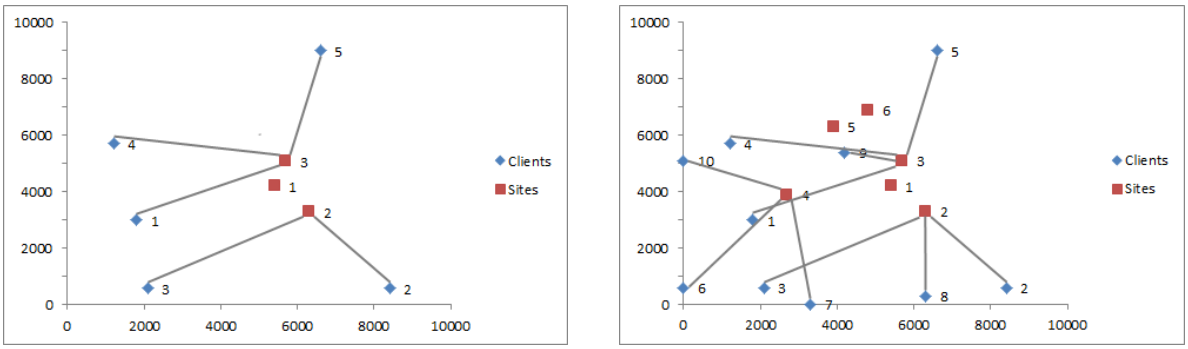
In all scenarios, the cost obtained using our method is an improvement over the costs obtained with the other two methods. The obtained gain over the sequential method varies from 1% to 13%, with an average of 6%. That average is around 16% when compared to the backtrack method.

6.6 Conclusion

In this paper, we present a new model to solve the dynamic planning of a FTTH network for a greenfield deployment. By dividing the planning into phases, an operator can better plan the evolution of its network and ensure that choices made in earlier phase do not have adverse results onto later phases. Numerical results effectuated on randomly generated scenarios show

Table 6.4 Cost of links for Scenario 1 (clients 6 to 10)

	Client 6	Client 7	Client 8	Client 9	Client 10
Site 1	46,468$	33,621$	28,657$	12,150$	39,197$
Site 2	49,076$	31,932$	21,480$	21,264$	46,913$
Site 3	51,997$	40,357$	34,635$	10,952$	40,812$
Site 4	30,528$	28,252$	36,452$	15,188$	21,155$
Site 5	49,450$	45,312$	46,269$	6,792$	29,215$
Site 6	56,708$	50,557$	48,461$	11,567$	36,705$

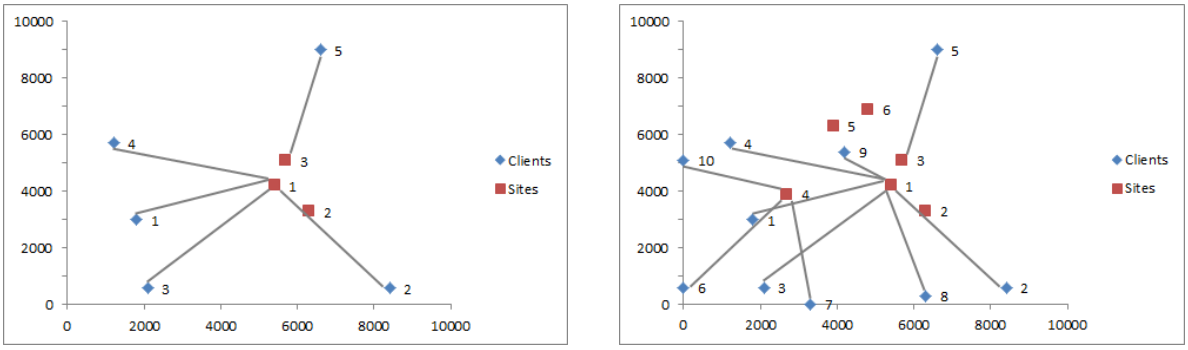


(a) Phase 1 (b) Phase 2

Figure 6.7 Optimal solution of Scenario 1

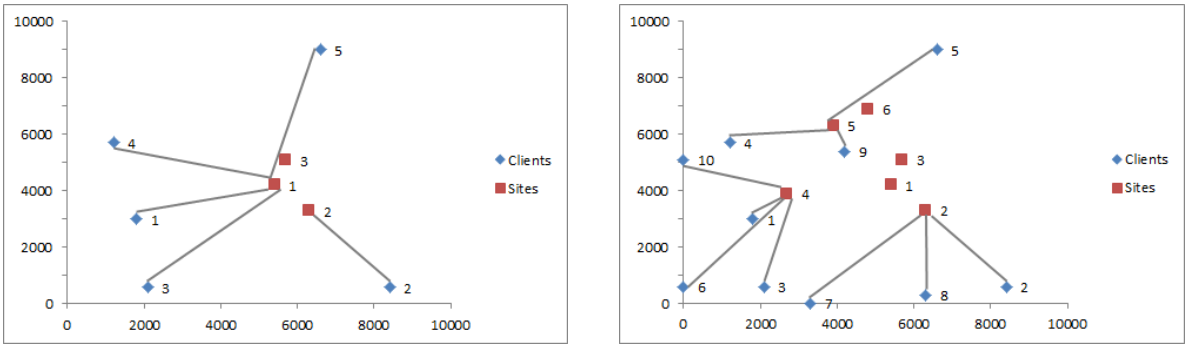
that our solution always improves the result obtained with methods that only consider one phase at a time.

Future works include extensions to our model to include aspects such as multi-level networks and cable grouping, as well as heuristics to approximate the solving of larger instances, since our problem is NP-hard (a polynomial reduction to the problem of capacitated minimum spanning tree, known to be NP-complete Garey et Johnson (1979), can be derived).



(a) Phase 1 (b) Phase 2

Figure 6.8 Solution of Scenario 1 using sequential method



(a) Phase 1 (b) Phase 2

Figure 6.9 Solution of Scenario 1 using backtrack method

Table 6.5 Simulation results

	S1	S2	D1	D2	T1	T2	O-Cost	S-Cost	B-Cost	S-Diff	B-Diff
1	2	4	4	8	2	3	$170,037	$195,477	$189,759	13.0%	10.4%
2	2	4	4	8	1	2	$192,572	$214,437	$226,039	10.2%	14.8%
3	2	4	4	10	2	3	$195,775	$209,747	$210,999	6.7%	7.2%
4	3	6	5	10	2	3	$306,520	$315,919	$399,885	3.0%	23.3%
5	3	6	5	10	2	4	$292,298	$296,757	$309,608	1.5%	5.6%
6	3	6	6	11	3	3	$286,051	$301,230	$346,862	5.0%	17.5%
7	3	6	8	12	2	3	$302,458	$313,373	$421,063	3.5%	28.2%
8	4	7	8	12	3	3	$226,946	$250,694	$268,066	9.5%	15.3%
9	4	7	10	15	4	4	$356,700	$379,827	$425,542	6.1%	16.2%
10	4	7	10	15	3	5	$367,952	$376,692	$470,842	2.3%	21.9%
11	4	8	10	17	3	5	$345,107	$349,466	$400,561	1.2%	13.8%
12	4	9	10	18	3	5	$368,780	$417,037	$428,309	11.6%	13.9%
13	4	10	12	20	4	6	$488,971	$520,671	$627,283	6.1%	22.0%
14	5	10	12	20	6	6	$431,441	$446,610	$595,828	3.4%	27.6%
15	5	10	12	22	4	6	$500,045	$501,837	$643,061	0.4%	22.2%
16	5	11	12	22	5	6	$524,141	$531,658	$655,200	1.4%	20.0%

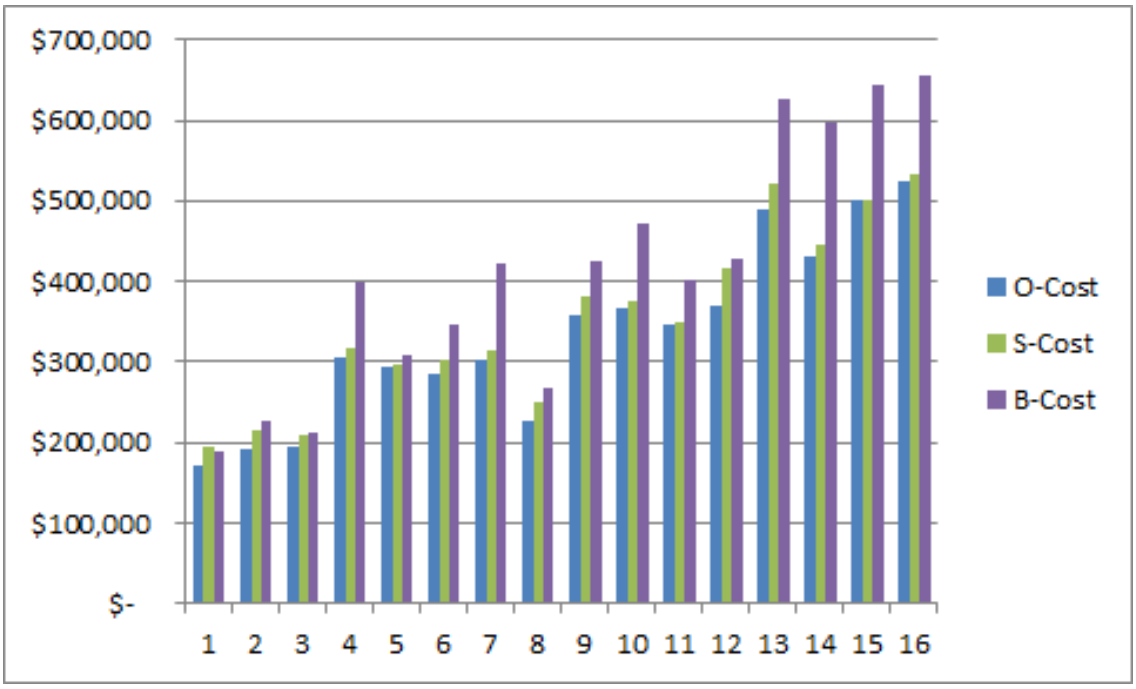


Figure 6.10 Comparison of obtained costs for 16 scenarios

CHAPITRE 7

DISCUSSION GÉNÉRALE

Dans ce chapitre, nous effectuerons une analyse critique de l'ensemble de notre travail. En plus de valider l'atteinte de nos objectifs, nous discuterons des différents choix que nous avons effectués, par rapport aux alternatives disponibles. Ce chapitre se divise en deux sections, soit une discussion portant sur les protocoles de mobilité et multidiffusion et une discussion sur la planification des réseaux d'accès.

7.1 Mobilité et multidiffusion

Comme nous l'avons vu au chapitre 2, les deux protocoles de mobilité les plus populaires sont Mobile IP v6 (MIPv6) et Proxy Mobile IP v6 (PMIPv6). Rappelons que leurs philosophies sont diamétralement opposées. Le premier donne au nœud mobile le contrôle exclusif de la gestion de la mobilité. Le deuxième, quant à lui, permet au réseau de complètement gérer la mobilité, en masquant les mécanismes du nœud mobile. Quand la mobilité est gérée par le mobile, les messages de signalisation qui sont envoyés représentent un gaspillage au niveau de l'interface radio, qui est la partie la plus dispendieuse du réseau. Par contre, quand la mobilité est gérée par le réseau, on perd certaines informations utiles, comme la détection des certains points d'accès, ce qui limite les mécanismes qui en dépendent, tel Fixed-Mobile Convergence (FMC). Notre objectif était donc de proposer un nouveau protocole hybride, qui combine les avantages des deux types de gestion, en éliminant leurs faiblesses.

Afin d'obtenir ce nouveau protocole, deux possilibités s'offraient. D'une part, on peut se baser sur MIPv6 pour y introduire l'implication du réseau. D'autre part, on peut se baser sur PMIPv6 pour y introduire l'implication du nœud mobile. Même si les deux approches permettraient d'atteindre notre objectif, nous avons opté pour la première. Le critère principal, qui a tranché le débat, est que la philosophie de PMIPv6 est d'avoir la gestion entièrement contrôlée par le réseau. Notre modification serait allée à l'encontre de cette philosophie et il était donc plus naturel de faire évoluer MIPv6 vers la solution hybide.

Une fois que nous avons choisi MIPv6 comme protocole de base, nous avons vite réalisé que ce protocole, dans son état actuel, était très difficilement modifiable. La séparation entre les différentes composantes n'étant pas clairement définie, il était impossible de faire de simples modifications sans revalider le document au complet. Pour cette raison, nous avons décidé, comme première étape, de procéder à la refonte. Cette ingénierie était un mal nécessaire et

nous a permis de restructuer le protocole vers une architecture modulaire et beaucoup plus claire. Ainsi, pour ajouter l'implication du réseau, nous avons proposé un nouveau module qui décrit les modifications à apporter au protocole.

Au niveau de la multidiffision, et de l'impact de la macro-mobilité, notre objectif était de permettre les relèves transparentes pour les applications multimédia en temps réel. Cet objectif a été atteint au chapitre 5. Un des choix qui a été effectué, tôt dans nos démarches, est celui de travailler sur MIPv6, plutôt que le protocole que nous avons proposé au chapitre 6. Les motivations derrière cette décision sont les suivantes :

1. L'adoption de notre protocole de mobilité n'étant pas garantie, il était préférable cibler un protocole plus connu, tel MIPv6, afin que notre solution ait une meilleure visibilité ;
2. Le simulateur utilisé pour évaluer le bon fonctionnement et la performance de notre solution, soit Optimized Network Engineering Tool (OPNET), offre déjà une implémentation de MIPv6, ce qui a réduit la complexité de l'implémentation de notre solution ;
3. L'adaptation de notre solution vers notre protocole de mobilité est une tâche relativement triviale, car le profil qui est compatible avec MIPv6 a déjà été implémenté.

Une autre décision qui a été prise pour ce travail est au niveau du type d'application à cibler. Le choix s'est arrêté sur les applications multimédia en temps réel mais qui ne sont pas de nature interactive, tels IPTV et Mobile IP TeleVision (MobileTV) (application quasi-temps réel). La motivation est que ces applications emploient la multidiffusion, qui est le mode de transmission que nous ciblons. De plus, puisqu'elles ne sont pas interactives, elles permettent l'utilisation de tampons, un aspect qui est crucial à notre solution.

7.2 Planification des réseaux d'accès filaires

Pour la problème de la planification des réseaux d'accès filaires, sujet qui est traité au chapitre 6, le choix de la technologie s'est arrêté sur les réseaux en fibre optique de bout en bout, soit la technologie FTTH. D'autres technologies intéressantes auraient pu également être considérées, tels FTTN et HFC. Si cette thèse portait uniquement sur la planification des réseaux d'accès filaires, chacune de ces technologies aurait fait l'objet d'un volet, ce qui aurait permis d'obtenir une comparaison de coût, afin de déterminer la meilleure technologie à déployer, dans différents scénarios.

Le choix de FTTH a été retenu car, pour l'environnement ciblé, soit sans infrastructure existante, nous croyons qu'il s'agit de la meilleure approche à moyen et long termes. En effet, les technologies sont plutôt vues comme des technologies transitoires, l'objectif ultime étant de déployer la fibre jusqu'au client. Ces hybrides sont attrayants lorsqu'une infrastructure existante est déjà en place, comme par exemple un réseau xDSL ou encore un réseau Cable

Television (CATV). Mais dans un environnement vierge, les économies offertes par les technologies hybrides sont bien moindres, justifiant ainsi le deploiement de FTTH. Ceci permet à l'opérateur d'investir dans une technologie qui est plus évolutive.

En conclusion, tous les objectifs de notre thèse ont été atteints, grâce aux trois contributions proposées. Certains choix ont dûs êtres effectués, à plusieurs niveaux, et chacun de ces choix a été motivé. De plus, nos choix vont dicter certaines limitations et travaux futurs, comme nous le verrons au prochain chapitre.

CHAPITRE 8

CONCLUSION ET RECOMMANDATIONS

Dans ce chapitre, nous effectuerons une récapitulation des travaux proposés dans cette thèse. Nous débuterons par un rappel des principales contributions ; les limitations seront ensuite discutées pour finalement en proposer des pistes de recherche pouvant faire l'objet de travaux futurs.

8.1 Contributions de la thèse

Cette thèse porte sur le support des application multimédia dans les réseaux de prochaine génération. Elle prend en compte également l'aspect de la mobilité, qui est de plus en plus prédominant chez les usagers. Plus précisément, les principales contributions de la thèse sont :

1. de proposer une refonte du protocole de mobilité Mobile IP v6 (MIPv6). Le résultat est un nouveau protocole avec uniquement les fonctionnalités de base, auquel s'ajoutent des modules permettant d'ajouter de nouvelles fonctionnalités ou de modifier le comportement de base. De plus, des modules de sécurité peuvent être conçus en implémentant une interface exposée par le protocole de base. Finalement, le concept de profil est proposé, permettant de regrouper les modules en une entitée qui assure l'interopérabilité des nœuds ;
2. de concevoir un module au protocole de base cité ci-haut, permettant à un réseau de prendre en charge la gestion de la mobilité des nœuds mobiles, en prenant en considération la collaboration de ces nœuds. Ce module introduit un nouveau nœud qui joue le rôle de proxy du nœud mobile et qui gère donc la mobilité à sa place. L'influence du nœud mobile sur les décisions peut être ajustée en modifiant les paramètres du nœud proxy ;
3. de proposer une modification au protocole MIPv6 pour améliorer la qualité de l'expérience des usagers mobiles pour des applications multimédia en temps réel. Plus spécifiquement, cette amélioration vise à obtenir des relèves transparentes, lors de macromobilité, pour les applications ciblées, soient celles qui utilisent les protocoles de multidiffusion et qui supportent le tamponnage des données (applications temps réel non interactives). La solution proposée ajoute un nouveau nœud, le Multicast Buffering Agent (MBA), dans le réseau qui est en charge de tamponner les paquets perdus par le nœud mobile lors de la relève. Une fois que le nœud mobile regagne sa connectivité,

il avertit le MBA, qui lui envoie les paquets ratés par unicast. Toutefois, même en présence du MBA, un sous-dimensionnement des tampons peut être à l'origine de perte de paquets, causant souvent une interruption du service offert à l'usager. De ce fait, une attention particulière se doit d'être portée quant à la taille des tampons, dans le but d'enrayer toute perte de paquets, garantissant ainsi une relève totalement transparente et assurant, du même coup, une meilleure qualité de l'expérience perçue par l'usager.

4. de concevoir un modèle mathématique décrivant la planification d'un réseau Fiber to the Home (FTTH) dans un environnement sans infrastructure existante, tout en considérant l'aspect dynamique et évolutif du réseau. Le résultat est un modèle mathématique linéaire en nombres entiers, qui permet, à un opérateur donné, d'effectuer la planification de son réseau d'accès tout en fibre, en prenant en considération l'expansion des clients au cours des différentes phases de la planification. Les résutlats obtenus, grâce à des simulations, ont amélioré ceux obtenus avec les méthodes existantes.

8.2 Limitations de la thèse

Cette section présente les limitations de chacune de nos contributions. Dans le chapitre 4, la limitation majeure de notre travail est plutôt d'ordre logistique. En effet, le concept de profils que nous proposons doit être géré par une entité centrale, qui doit leur attribuer des identificateurs uniques (nous proposons que cette entité soit Internet Engineering Task Force (IETF)). De plus, ce même concept de profil peut limiter l'interopérabilité, car chaque opérateur peut décider de proposer et implémenter un profil différent.

Dans le chapitre 5, la limitation majeure est que notre solution ne s'applique qu'aux applications en temps réel et dont les paquets peuvent être tamponnés. Ainsi, les applications en temps réel qui utilisent la multidiffusion mais qui ne permettent pas le tamponnages des données, telles que la vidéo-conférence, ne peuvent bénéficier de notre travail, car les délais engendrés par notre solution ne seraient pas acceptables. De plus, certains aspects, notamment la sécurité, n'ont pas été abordés par notre travail.

Finalement, dans le chapitre 6, notre modèle mathématique omet certains aspects avancés de la planification. Par exemple, nous ne traitons pas le cas de hiérarchies à plusieurs pâliers ou encore le partage des conduits de câbles. De plus, on note une limitation au niveau de la résolution du problème. En effet, la solution obtenue étant NP-difficile, notre résolution exacte se limite à des scénarios de petites tailles.

8.3 Travaux futurs

Nous concluons cette thèse avec la présentations de propositions de recherche qui peuvent être intéressantes à poursuivre. Certaines d'entre elles découlent des limitations énoncées ci-dessus. Premièrement, du côté du chapitre 4, de nombreux travaux futurs peuvent être envisagés. En effet, à cause de la nature modulaire du protocole que nous proposons, plusieurs nouveaux modules peuvent être conçus, comme par exemple :

- Des modules de sécurité ;
- Des modules d'amorçage ;
- Des modules d'optimisation de route.

Au niveau du chapitre 5, les applications visées sont celles qui opèrent en temps réel et qui permettent la mise en tampon des paquets. Il serait intéressant d'explorer la possibilité d'adapter la solution aux applications intéractives, telles que la vidéoconférence, qui utilise également la multidiffusion mais qui ne font pas usage de tampon. De plus, un autre travail envisageable, est la conception d'un module s'intégrant à la solution du chapitre 4 et offrant la même fonctionnalité.

Pour ce qui est du chapitre 6, plusieurs types de travaux futurs peuvent être envisagés. Du côté du modèle mathématique, des modifications sont envisageables pour ajouter certains nouveaux aspects tels que :

- des hiérarchies à plusieurs pâliers ;
- le partage des conduits de câbles.

Du côté de la résolution du problème, les solutions exactes sont obtenues seulement pour des jeux de données de petites à moyennes tailles. Pour de plus grands jeux de données, il faut plutôt approximer le problème en adoptant une approche heuristique. Par exemple, une résolution grâce à une heuristique basée sur la recherche de voisinage avec mouvements tabous peut trouver des solutions qui, à défaut d'être optimales, sont très bonne qualité. Leurs qualités peuvent généralement être quantifiées en comparant le coût de la solution à une borne inférieure, obtenue en relâchant une ou plusieurs contraintes.

Finalement, il serait intéressant d'explorer la planification dynamique d'autres technologies, telles que Fiber to the Node (FTTN), afin de comparer les résultats obtenus. Cela permettrait d'avoir des mesures quantitatives, permettant d'effectuer le bon choix, non seulement au niveau de la planification elle-même, mais également au niveau de la technologie adoptée. Ce choix variera sûrement en fonction des caractériques des réseaux à planifier, et il serait donc pertinent de tenter d'établir les critères qui font basculer le choix vers une technologie par rapport à une autre.

RÉFÉRENCES

ADAMS, A., NICHOLAS, J. et SIADAK, W. (2005). Protocol Independent Multicast - Dense Mode (PIM-DM) : Protocol Specification (Revised). RFC 3973 (Experimental).

ARKKO, J., DEVARAPALLI, V. et DUPONT, F. (2004). Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. RFC 3776 (Proposed Standard). Updated by RFC 4877.

BALAKRISHNAN et ET AL., M. (1989). A dual-ascent procedure for large-scale uncapacitated network design.

BALAKRISHNAN, A., MAGNANTI, T. L., SHULMAN, A. et WONG, R. T. (1991). Models for planning capacity expansion in local access telecommunications networks. *Annals of Operations Research*, 33, 239–284.

BECK, M. (2005). *Ethernet in the First Mile : The IEEE 802.3ah Efm Standard*. McGraw-Hill professional engineering : Communications engineering. McGraw-Hill.

BHATTACHARYYA, S. (2003). An Overview of Source-Specific Multicast (SSM). RFC 3569 (Informational).

BUFORD, J. (2008a). Hybrid Overlay Multicast Framework. IETF Internet Draft 02, SAM Research Group.

BUFORD, J. (2008b). Hybrid Overlay Multicast Framework.

BUMGARDNER, G. (2012). *Automatic Multicast Tunneling (Draft)*. IETF.

CAMERINI, P., GALBIATI, G. et MAFFIOLI, F. (1980). Complexity of spanning tree problems : Part i. *European Journal of Operational Research*, 5, 346 – 352.

CAMERINI, P., GALBIATI, G. et MAFFIOLI, F. (1983). On the complexity of finding multi-constrained spanning trees. *Discrete Applied Mathematics*, 5, 39 – 50.

CAMPBELL, A. T., GOMEZ, J., KIM, S., TURÁNYI, Z. R., VALKÓ, A. G. et YIH WAN, C. (2002). Internet micromobility.

CARPENTER, T., EIGER, M., SHALLCROSS, D. et SEYMOUR, P. D. (2001). Node placement and sizing for copper broadband access networks. *Annals OR*, 106, 199–228.

CARPENTER, T. J., EIGER, M., SHALLCROSS, D. et SEYMOUR, P. (1996). Automated design of fiber-to-the-curb and hybrid fiber-coax access networks. *National Fiber Optic Engineers Conference*.

CHEN, J., WOSINSKA, L., MACHUCA, C. et JAEGER, M. (2010). Cost vs. reliability performance study of fiber access network architectures. *Communications Magazine, IEEE*, 48, 56 –65.

COOPER, L. (1963). Location-Allocation Problems. *Operations Research*, 11, 331–343.

CORNING (2005). Broadband technology overview. Rapport technique, Corning.

COTTON, M., VEGODA, L. et MEYER, D. (2010). IANA Guidelines for IPv4 Multicast Address Assignments. RFC 5771 (Best Current Practice).

DIAS, J., CAPTIVO, M. E. et CLIMAO, J. (2007). Dynamic Location Problems with Discrete Expansion and Reduction Sizes of Available Capacities. *Investigacao Operacional*, 27, 107 – 130.

FENNER, B., HANDLEY, M., HOLBROOK, H. et KOUVELAS, I. (2006). Protocol Independent Multicast - Sparse Mode (PIM-SM) : Protocol Specification (Revised). RFC 4601 (Proposed Standard).

GAREY, M. R. et JOHNSON, D. S. (1979). *Computers and Intractability : A Guide to the Theory of NP-Completeness (Series of Books in the Mathematical Sciences)*. W. H. Freeman & Co Ltd.

GARYFALOS, A. et ALMEROTH, K. (2005a). A flexible overlay architecture for mobile ipv6 multicast. *Selected Areas in Communications, IEEE Journal on*, 23, 2194–2205.

GARYFALOS, A. et ALMEROTH, K. C. (2005b). A flexible overlay architecture for mobile ipv6. *Multicast', IEEE Journal on Selected Areas in Communications*, 23, 2194–2205.

GAVISH, B. (1982). Topological design of centralized computer networks—formulations and algorithms. *Networks*, 12, 355–377.

GAVISH, B. (1983). Formulations and algorithms for the capacitated minimal directed tree problem. *J. ACM*, 30, 118–132.

GAVISH, B. (1985). Augmented lagrangean based algorithms for centralized network design. *Communications, IEEE Transactions on*, 33, 1247–1257.

GAVISH, B. (1991). Topological design of telecommunication networks - local access design methods. *Annals of Operations Research*.

GIRARD, A., SANSO, B. et DADJO, L. (2001). A tabu search algorithm for access network design. *Annals of Operations Research*, 106, 229–26.

GOHAR, M., KOH, S.-J., UM, T.-W. et LEE, H.-W. (2010). Seamless multicast handover in pmipv6-based wireless networks. *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on*. vol. 1, 502–507.

GOUVEIA, L. et LOPES, M. (1997). Using generalized capacitated trees for designing the topology of local access networks. *Telecommunication Systems*, 7, 315–337.

GUNDAVELLI, S., LEUNG, K., DEVARAPALLI, V., CHOWDHURY, K. et PATIL, B. (2008). Proxy Mobile IPv6. RFC 5213 (Proposed Standard). Updated by RFC 6543.

GUPTA, R. et PIRKUL, H. (2000). Hybrid fiber co-axial {CATV} network design with variable capacity optical network units. *European Journal of Operational Research*, 123, 73 – 85.

HANDLEY, M., KOUVELAS, I., SPEAKMAN, T. et VICISANO, L. (2007). Bidirectional Protocol Independent Multicast (BIDIR-PIM). RFC 5015 (Proposed Standard).

HONG-KE ZHANG, BING-YI ZHANG, B. S. (2007). *Mobile IPv6 Multicast with Dynamic Multicast Agent (Draft)*. IETF.

HOOD, D. (2012). *Gigabit-capable Passive Optical Networks*. Wiley.

ITU-T (1999a). Asymmetric digital subscriber line 2 transceivers (adsl2)– extended bandwidth adsl2 (adsl2plus). Rapport technique, International Telecommunication Union.

ITU-T (1999b). Asymmetric digital subscriber line (adsl) transceivers. Rapport technique, International Telecommunication Union.

ITU-T (2003). Single-pair high-speed digital subscriber line (shdsl) transceivers. Rapport technique, International Telecommunication Union.

ITU-T (2004). Very high speed digital subscriber line transceivers (vdsl). Rapport technique, International Telecommunication Union.

JAUMARD, B. et CHOWDHURY, R. (2012). An efficient optimization scheme for wdm/tdm pon network planning. *Computer Communications*.

JOHNSON, D., PERKINS, C. et ARKKO, J. (2004). Mobility Support in IPv6. RFC 3775 (Proposed Standard). Obsoleted by RFC 6275.

KERSHENBAUM, A., BOORSTYN, R. et OPPENHEIM, R. (1980). Second-order greedy algorithms for centralized teleprocessing network design. *Communications, IEEE Transactions on*, 28, 1835–1838.

KIM, Y., LEE, Y. et HAN, J. (2011). A splitter location-allocation problem in designing fiber optic access networks. *European Journal of Operational Research*, 210, 425–435.

KLINCEWICZ, J. G. (1998). Hub location in backbone/tributary network design : a review. *Location Science*, 6, 307–335.

KOODLI, R. (2009). Mobile IPv6 Fast Handovers. RFC 5568 (Proposed Standard).

KYUNGJOO SUH, DONG-HEE KWON, Y.-J. S. et PARK, Y. (2004). Fast Multicast Protocol for Mobile IPv6 in the fast handovers environments. IETF Internet Draft 00, Mipshop.

LE, L. et LIEBSCH, M. (2009). Preliminary binding : an extension to proxy mobile ipv6 for inter-technology handover. *Proceedings of the 2009 IEEE conference on Wireless Communications & Networking Conference*. WCNC'09, 2079–2084.

LEE, Y., KIM, Y. et HAN, J. (2006). FTTH-PON Splitter Location-Allocation Problem. *Eigth INFORMS Telecommunication Conference*.

LEOLEIS, G. A., PREZERAKOS, G. N. et VENIERIS, I. S. (2006). Seamless multicast mobility support using fast mipv6 extensions. *Computer Communications*, 29, 3745 – 3765.

LI, J. et SHEN, G. (2008). Cost minimization planning for passive optical networks. *Optical Fiber communication/National Fiber Optic Engineers Conference, 2008. OFC/NFOEC 2008. Conference on*. 1 –3.

LUKIC, B. (1999). An approach of designing local access network using simulated annealing method. *In ConTEL'99 - 5th International Conference on Telecommunications*, 241–247.

MAKAYA, C. et PIERRE, S. (2008). An analytical framework for performance evaluation of ipv6-based mobility management protocols. *Wireless Communications, IEEE Transactions on*, 7, 972–983.

MAZUR, D. (1999). *Integer programming approaches to a multi-facility location problem*. Thèse de doctorat, Hopkins University, Baltimore.

MIN KIM, J., KYEUN RA, I. et SUNG KIM, H. (Feb.). A multicast scheme for provision of seamless service in proxy mobile ipv6 networks. *Advanced Communication Technology (ICACT), 2011 13th International Conference on*. 1259–1264.

MITCSENKO, A., PAKSY, G. et CINKLER, T. (2009). Topology design and capex estimation for passive optical networks. *Broadband Communications, Networks, and Systems, 2009. BROADNETS 2009. Sixth International Conference on*. 1 –8.

NARTEN, T., NORDMARK, E., SIMPSON, W. et SOLIMAN, H. (2007). Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Draft Standard).

PAPADIMITRIOU, C. H. (1978). The complexity of the capacitated tree problem. *Networks*, 8, 217–230.

PERKINS, C. (2010). IP Mobility Support for IPv4, Revised. RFC 5944 (Proposed Standard).

PUJOLLE, G. (2011). *Les réseaux*. Eyrolles.

ROUTEN, T. (1994). Genetic algorithm and neural network approaches to local access network design. *MASCOTS '94 : Proceedings of the Second International Workshop on Modeling, Analysis, and Simulation On Computer and Telecommunication Systems*. IEEE Computer Society, Washington, DC, USA, 239–243.

SCHMIDT, T., WAEHLISCH, M. et FAIRHURST, G. (2010). Multicast Mobility in Mobile IP Version 6 (MIPv6) : Problem Statement and Brief Survey. RFC 5757 (Informational).

SHAW, D. X. et SHAW, D. X. (1994). Reformulation, column generation and lagrangian relaxation for local access network design problems.

SHULMAN, A. (1991). An algorithm for solving dynamic capacitated plant location problems with discrete expansion sizes. *Oper. Res.*, 39, 423–436.

SOLIMAN, H., CASTELLUCCIA, C., ELMALKI, K. et BELLIER, L. (2008). Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. RFC 5380 (Proposed Standard).

SONI, S., NARASIMHAN, S. et LEBLANC, L. (2004). Telecommunication access network design with reliability constraints. *Reliability, IEEE Transactions on*, 53, 532–541.

THOMAS C. SCHMIDT, M. W. (2005). Seamless Multicast Handover in a Hierarchical Mobile IPv6 Environment (M-HMIPv6). IETF Internet Draft 04, Internet Draft.

UR REHMAN LAGHARI, K., CRESPI, N., MOLINA, B. et PALAU, C. E. (2011). Qoe aware service delivery in distributed environment. *Advanced Information Networking and Applications (WAINA), 2011 IEEE Workshops of International Conference on*. 837–842.

WAEHLISCH, M. (2013). A Common API for Transparent Hybrid Multicast. IETF Internet Draft 07, SAM Research Group.

WAEHLISCH, M. et SCHMIDT, T. C. (2007). Between underlay and overlay : On deployable, efficient, mobility-agnostic group communication services. *Internet Research*, 17, 519–534.

WÄHLISCH, M. et SCHMIDT, T. C. (2007). Between underlay and overlay : On deployable, efficient, mobility-agnostic group communication services. *Internet Research*, 17, 519–534.

ZHAO, R., ZHOU, L. et MACHUCA, C. (2010). Dynamic migration planning towards ftth. *Telecommunications Network Strategy and Planning Symposium (NETWORKS), 2010 14th International*. 1 –6.