HAL
open science

Ufa : an ultra flat architecture for future mobile networks

Khadija Daoud Triki

To cite this version:

Khadija Daoud Triki. Ufa : an ultra flat architecture for future mobile networks. Other [cs.OH]. Institut National des Télécommunications, 2011. English. NNT : 2011TELE0007 . tel-00665221

HAL Id: tel-00665221

https://theses.hal.science/tel-00665221v1

Submitted on 1 Feb 2012

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Ecole Doctorale EDITE

Thèse présentée pour l'obtention du diplôme de Docteur de Télécom & Management SudParis

Doctorat conjoint Télécom & Management SudParis et Université Pierre et Marie Curie

Spécialité:

Informatique et Télécommunication

Par

Khadija DAOUD TRIKI

UFA: UNE ARCHITECTURE ULTRA PLATE POUR LES RESEAUX MOBILES DU FUTUR

Soutenue le 18 février devant le jury composé de:

Jean-Marie Bonnin	Pr. Télécom Bretagne	Rapporteur
Khaldoun Al Agha	Pr. Université ParisSud Orsay	Rapporteur
Guy Pujolle	Pr. Université Paris 6	Examinateur
Philippe Martins	Pr. Télécom ParisTech	Examinateur
Thomas Noel	Pr. Université Louis Pasteur Strasbourg	Examinateur
Noel Crespi	Pr. Télécom SudParis	Directeur de thèse
Karine Guillouard	Dr.Orange Labs	Encadrante

Thèse n°2011TELE0007

Ecole Doctorale EDITE

Thesis submitted in partial satisfaction of the requirements for the degree of Doctor of Télécom & Management SudParis

Joint PhD Télécom & Management SudParis and *Université Pierre et Marie Curie*

Specialization:

Computer and Telecommunication Science

Presented by

Khadija DAOUD TRIKI

UFA: AN ULTRA FLAT ARCHITECTURE FOR FUTURE MOBILE NETWORKS

Defended on the 18th of February, committee in charge:

Jean-Marie Bonnin	Pr. Télécom Bretagne	Reviewer
Khaldoun Al Agha	Pr. Université ParisSud Orsay	Reviewer
Guy Pujolle	Pr. Université Paris 6	Examiner
Philippe Martins	Pr. Télécom ParisTech	Examiner
Thomas Noel	Pr. Université Louis Pasteur Strasbourg	Examiner
Noel Crespi	Pr. Télécom SudParis	Thesis director
Karine Guillouard	Dr.Orange Labs	Thesis supervisor

Thesis n° 2011TELE0007

To my family,
To Ines.

Remerciements

Je tiens tout d'abord à remercier les membres du jury pour le temps qu'ils ont consacré dans l'évaluation de cette thèse.

J'exprime ma grande gratitude à Noël Crespi, mon directeur de thèse, pour les conseils qu'il a pu me donner tout au long de cette thèse.

Mes remerciements chaleureux s'adressent à Karine Guillouard, mon encadrant de thèse à Orange Labs, pour son soutien et sa disponibilité. Sa rigueur et ses compétences techniques m'ont aidé à mettre en valeur le travail de recherche fait dans cette thèse.

Je remercie vivement mon collègue Philippe Herbelin, pour son enthousiasme, le recul et les conseils qu'il apporté à ces travaux.

Ma profonde reconnaissance va à Arnaud Saveaux, mon responsable hiérarchique à Orange Labs, pour son soutien et la confiance qu'il m'accordée. Merci aussi à tous mes collègues, en particulier Eric Njedjou, qui ont soutenu ma démarche pendant ces 3 années.

Enfin, toute ma gratitude va à mes parents, ma famille et mes amis pour leurs encouragements, en particulier mon mari pour sa grande patience et son aide. Je dédie spécialement cette thèse à ma fille, Inès, pour tous les moments d'absence que j'ai eus envers elle en préparant ce "livre".

Paris, le 26 novembre 2010
Khadija Daoud Triki

Résumé

L'explosion du volume de trafic de données dans les réseaux mobiles, prévue pour les années 2010-2020, est communément admise par les communautés académique et industrielle. La capacité de ces réseaux à supporter cette croissance de trafic, couplée à une forte pression sur la réduction des coûts, est un enjeu majeur pour les opérateurs.

Les réseaux mobiles, déployés ou en cours de standardisation, répondent à un modèle en couches, avec: (1) un réseau d'accès, mono ou multi technologies, offrant une connectivité IP aux utilisateurs; (2) une couche de contrôle de service, telle que l'IMS, la solution standardisée la plus aboutie aujourd'hui; (3) une couche d'interaction (PCC), entre le réseau d'accès et la couche de contrôle de service, permettant le contrôle des politiques réseau. Ce modèle est très centralisé et comporte plusieurs types de nœuds réseau hiérarchisés. Il est à l'origine de problèmes de passage à l'échelle et de qualité de service (délai d'accès au service, délai de handover, difficulté d'adapter le service aux ressources). La résolution de ces problèmes augmente encore la complexité du modèle, ce qui nous a conduit à le revisiter.

Dans cette thèse, un nouveau modèle pour les futurs réseaux mobiles est proposé: Ultra Flat Architecture (UFA). UFA utilise l'IMS comme solution unifiée pour le contrôle de tout type d'applications, SIP ou non. L'architecture est dite "plate" puisqu'elle réduit le nombre de nœuds réseau à 3 principalement: (1) une Gateway UFA offrant une connectivité physique au terminal et regroupant à la fois l'ensemble des fonctionnalités du réseau d'accès, de la couche de contrôle de service (IMS) et de la couche de contrôle des politiques réseau; (2) une Gateway permettant le support des services non-SIP; et enfin (3) le terminal.

Après la conception de l'architecture, notre contribution s'est focalisée sur la spécification des trois procédures principales d'UFA: l'enregistrement/authentification, l'établissement de service et la mobilité. Nous avons optimisé les deux premières procédures par rapport aux procédures standardisées de l'IMS. Par exemple, la procédure d'établissement de service présente un délai réduit et permet une configuration du service ou de la couche de transport selon les ressources disponibles dans le réseau. Nous avons aussi spécifiquement développé une procédure de mobilité pour UFA. Pour un terminal en mobilité, cette procédure se base sur le transfert, d'une Gateway UFA à une autre, des contextes de toutes les couches OSI liés à ce terminal, et sur la détermination proactive par la Gateway UFA des paramètres de toutes les couches du terminal, nécessaires à son attachement à la nouvelle Gateway UFA.

La dernière partie de la thèse consiste à évaluer le modèle UFA et les procédures proposées. Nous avons d'abord mesuré, à l'aide de modèles analytiques, le délai d'établissement de service dans UFA et dans le modèle existant. Les résultats montrent qu'UFA fournit de meilleures performances, et mettent en évidence sa grande capacité de passage à l'échelle. Nous avons ensuite implémenté UFA sur une maquette. Au-delà de la validation de ses concepts, nous avons relevé, pour les applications (e.g. voix, vidéo) transportées sur le protocole RTP/UDP, un délai de handover performant. Enfin, nous nous sommes intéressés aux applications (e.g. streaming) transportées sur le protocole SCTP. Nous avons montré, par simulation avec NS2, l'intérêt de l'architecture UFA et de sa procédure de mobilité dans l'amélioration des performances de ces applications, en cas de mobilité. Ainsi, tous les résultats obtenus montrent le grand intérêt d'UFA et des architectures plates plus généralement.

Mots clés: architectures plates, IMS, SIP, SCTP, handover.

Abstract

The exponential growth of data volume in the mobile networks, foreseen for 2010-2020, is admitted by both the academic and industrial communities. The capability of these networks to support this data growth, coupled with strong pressure on reducing the costs, is a serious challenge for the operators.

Mobile networks, deployed or under standardization, have a layered model, with: (1) an IP access network, mono or multi technologies, providing IP connectivity to users; (2) a service control overlay network, like the IMS, the most complete and standardized solution; and (3) an interaction layer (PCC), between the IMS and the IP access network, for policy control. This model is very centralized and contains many hierarchical network node types. It causes scalability issues and QoS problems (service access delay, handover delay, and a service non-adaptation to network resources). Solving these problems increases the model complexity, which has lead us to review it.

In this thesis, a new model for future mobile networks has been proposed: Ultra Flat Architecture (UFA). UFA uses the IMS, as a unified solution, to control any service type, SIP or not. It is called "flat" as it reduces the number of network node types to 3 mostly: (1) a UFA Gateway providing physical connectivity to the terminal, and gathering the functions of the IP access network, the IMS and the policy control layer; (2) a Gateway to handle non-SIP native services; and finally (3) the terminal.

After the architecture design, my contribution has been focused on specifying three main procedures for UFA: the registration/authentication procedure, the service establishment procedure and the mobility procedure. The two first procedures are optimized compared to the IMS standardized ones. For example the service establishment allows the delay reduction and the configuration of the service or the transport layer according to the resources available in the network. The mobility procedure has been specifically designed for UFA. It uses the SIP protocol for any application type. For a terminal in mobility, it is based on the transfer, from one UFA Gateway to another, of the all OSI-layers contexts related to that terminal, and on a proactive determination of the all OSI-layers parameters, necessary for the terminal attachment to the new UFA Gateway.

The final part of this thesis consists in evaluating the UFA model and the proposed procedures. Firstly, the service establishment delay has been measured in UFA and in the existing model, using analytical models. Results show that UFA outperforms the existing model, and highlight UFA superior scalability. Secondly, based on UFA implementation on a testbed, UFA concepts have been proved. Moreover, a good handover delay performance has been measured for applications transported over RTP/UDP. Finally, special attention has been given to applications transported over SCTP. UFA advantages in enhancing the performances of these applications have been shown. All of the obtained results show the interest of UFA and of flat architectures more generally.

Key words: flat architectures, IMS, SIP, SCTP, handover.

Contents

List of publications **1**

Definitions **3**

Introduction **5**

A new ecosystem for Mobile Network Operators 5

Research problems 6

Thesis contributions 7

I State of the art **11**

1 Are current mobile networks ready for the new ecosystem? **13**

1.1 Mobile networks layered model 14

1.2 IP-AN//PCC//IMS model 15

1.2.1 IP-Access Network (IP-AN) 15

1.2.2 IMS: a concrete service control overlay network 18

1.2.3 PCC: An IMS - IP-AN interaction layer for policy control 19

1.3 Examples of IP-ANs and their interaction with PCC and IMS (IP-ANs//PCC//IMS) 22

1.3.1 (GSM and UMTS)//PCC//IMS 22

1.3.2 GAN//PCC//IMS 23

1.3.3 I-WLAN//PCC//IMS 24

1.3.4 (Inter I-WLAN - 3GPP mobility)//PCC//IMS 25

1.3.5 WiMAX//PCC//IMS 26

1.3.6 EPS//PCC//IMS 28

1.4 Is IP-AN//PCC//IMS model ready for the new ecosystem? 29

1.5 Service/application classification and impact of the transport protocol on mobility management . . . 33
1.6 Conclusion . . . 34

2 Main network procedures in the IP-AN//PCC//IMS model 35
2.1 Service access procedure in the IP-AN//PCC//IMS model . . . 36
2.1.1 Phase 1: registration/authentication . . . 36
2.1.2 Phase 2: service establishment . . . 42
2.1.3 Problems / state of the art / other possible solutions . . . 47
2.2 Mobility procedure during services in the IP-AN//PCC//IMS model . . . 53
2.2.1 Description of ISC mobility procedure . . . 53
2.2.2 Problems / state of the art / other possible solutions . . . 54
2.3 Conclusion . . . 59

II Proposal of a new model for future mobile networks 63

3 UFA: a new model for mobile networks 65
3.1 Ultra Flat Architecture (UFA) model . . . 65
3.1.1 IMS in UFA . . . 66
3.1.2 Policy control in UFA . . . 67
3.2 UFA detailed control functions and nodes . . . 68
3.2.1 UFA Gateway . . . 68
3.2.2 Terminal (MN/CN) . . . 70
3.2.3 SIPcrossSCTP Gateway (SxS_GW) . . . 71
3.3 How UFA fulfills the model requirements? . . . 71
3.4 Conclusion . . . 73

4 Main network procedures in UFA 75
4.1 Service access procedure in UFA . . . 75
4.1.1 Phase 1: registration/authentication . . . 75
4.1.2 Phase 2: service establishment . . . 78
4.2 Mobility procedure during services in UFA . . . 84
4.2.1 Detailed flow chart for mobility procedure (SIP/non-SIP native services) . . . 85
4.3 Conclusion . . . 90

III Evaluation of UFA model 91

5 Performance of service establishment in UFA 93

5.1 Service establishment delay 93
5.1.1 Definition and requirements 93
5.1.2 Components 94
5.2 Node delay per node and message (D_{sig}) 95
5.3 Service establishment delay evaluation in UMTS//PCC//IMS and UFA 97
5.3.1 Inputs 97
5.3.2 Numerical results 97
5.4 Conclusion 103

6 Implementation and performance of UFA mobility procedure for SIP native services 105

6.1 Implemented ISC and UFA and their handover delay components 105
6.2 Testbed architecture 108
6.3 Testbed configuration and implementation 109
6.3.1 Layer 2 109
6.3.2 IP 109
6.3.3 SIP 109
6.3.4 Implementation challenges 109
6.4 Testbed traces 112
6.5 UFA performances 112
6.5.1 Handover delays measurements on the testbed in UFA and Implemented ISC for low-delay links 112
6.5.2 Handover delays in UFA for different network scenarios: comparison between testbed measurements and analytical values 117
6.6 Conclusion 119

7 Performance of UFA mobility procedure for non-SIP native services 123

7.1 SCTP 123
7.1.1 Overview 123
7.1.2 SCTP mechanisms for data transmission and congestion control 124
7.2 Mobile SCTP 126
7.3 Problems encountered by SCTP-transported services during hard handover when used with m-SCTP 127
7.3.1 Problems 127
7.3.2 Related work 129
7.4 Comparison between UFA, m-SCTP and other SIP-based solutions 130
7.4.1 UFA and m-SCTP 130
7.4.2 UFA and other SIP-based solutions handling SCTP-transported services . . 131

7.5 Different options for SCTP configuration in UFA 131
7.6 Performance evaluation 132
7.6.1 Simulation model and inputs 132
7.6.2 SCTP behavior analysis 133
7.6.3 Performance results 134
7.7 Conclusion 137

IV Conclusion and future work 139

8 Conclusion and future work 141
8.1 Thesis summary 141
8.2 Future work 143

V Appendices 145

A SIP, SDP and mobility management with SIP 147
A.1 SIP 147
A.1.1 SIP architecture 147
A.1.2 Transactions and dialogs 148
A.1.3 Addresses within SIP 148
A.1.4 SIP messages format 148
A.2 SDP 150
A.3 Example of service management with SIP: establishment, mobility execution, termination 151

B IPsec Security Association contexts 153

C QoS preconditions 155

D Solutions for handover delay optimization considering MIP-based mobility procedure 157

E Establishment and handover message flows based on the testbed traces 161
E.1 Establishment 161
E.2 Handover 162

F PJSIP 169
F.1 Architecture of SIP programs 169
F.2 Examples of UFA SIP messages handling with SIP programs 170

VI Résumé étendu en français **173**

G Résumé étendu en français **175**

VII Acronyms **185**

List of Figures **195**

List of Tables **197**

Bibliography **198**

List of publications

Journal papers

- Z.Faigl, L.Bokor, P.Neves, R.Pereira K.Daoud, P.Herbelin, "Evaluation of two integrated signalling schemes for the Ultra Flat Architecture using SIP, IEEE 802.21, and HIP/PMIP protocols", accepted in Elsevier comnet 2010 [119].

International conference papers

- K. Daoud, P.Herbelin, Noel Crespi, "UFA: an ultra flat architecture for high bitrate services in mobile networks", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2008 [38].
- K. Daoud, P.Herbelin, N.Crespi, "One-Node-Based Mobile Architecture For a Better QoS Control", in proceedings of IFIP Wireless Days 2008 [85].
- K. Daoud, P.Herbelin, K.Guillouard, N.Crespi, "Performance and implementation of UFA: A SIP-based Ultra Flat Architecture Mobile Network Architecture", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2009 [81].
- K. Daoud, K.Guillouard, P.Herbelin, N.Crespi, "A Network-Controlled Architecture for SCTP Hard Handover", in proceedings of Vehicular Technology Conference (VTC-fall), 2010 [116].
- Z.Faigl, L.Bokor, P.Neves, R.Pereira K.Daoud, P.Herbelin, "Evaluation and Comparison of signalling Protocol Alternatives for the Ultra Flat Architecture", in proceedings of the fifth international conference on systems and networks communications (ICSNC) 2010 [118].

Demonstrations

- K.Daoud, P. Herbelin, "UFA proof of concept", Salons de la recherche de France Télécom, December 2010.

Patents registration

- P.Herbelin, K.Daoud, J.Pons, "Procédés nécessaires à la mobilité des terminaux mobiles rattachés à des stations de base en s'appuyant sur l'implémentation d'un protocole de niveau 4 à 7 du modèle OSI", october 2007, currently the registration request is extended at the international level [80].

- P.Herbelin, K.Daoud, C.Léveque, "Procédés et terminaux de communication pour améliorer le transfert de connexion entre des cellules appartenant à des réseaux différents" , March 2009, currently the registration request is extended at the international level [86].
- K.Daoud, P.Herbelin, "Utilisation du protocole SIP pour la distribution des flux non-SIP établis entre deux nœuds utilisateurs joignables par différents chemins réseau", May 2009, currently the registration request is extended at the international level [87].

Definitions

Here is a set of words that will be used in the report.

`3GPP` : 3rd Generation Partnership Project (3GPP). It is a standardization body that produces Technical Specifications (TS) and Technical Reports (TR) for the 3G Mobile System, based on evolved GSM core networks and the radio access technologies.

`3GPP Release` : It reflects a version of the 3GPP specifications. Release x roughly means that the version is produced in 200x, except Release 4 that was finished in 2001, Release 5 in 2002, Release 6 in 2005.

`3GPP services` : Services available through an access network standardized within 3GPP e.g. GSM, UMTS, EPS.

`Anchor` : A network node through which the traffic passes. There are two kinds of anchors: the **data anchor** related to the user traffic, and the **signalling anchor** related to the signalling traffic.

`Bearer` : A transmission path characterized by its capacity, delay, bit error rate, etc. It may transport different `data flows`.

`Bearer endpoint` : A bearer endpoint terminates a `bearer`. It treats the `bearer` establishment, modification and release requests. The bearer endpoint applies rules on the data flows transported over the `bearer`.

`CN` : Correspondent Node. An equipment that allows users to access network services. It acts as the `MN` corresponding node during a call and is not mobile.

`CoN` : Connectivity Node. The first node in the network providing physical connectivity to the user. For UMTS, it is the NodeB (NB).

`Context` : A set of information related to a user. A context is established through a dedicated procedure. It enables the handling of user or signalling traffic, without need to perform the said procedure from scratch.

`Data flow` : A set of packets, matching a specific source and destination (IP address+ transport port). This set of packets is generated by an application.

`Function` : A function has a specific role within the network. Its definition cannot be independent of the `organic architecture`.

`Handover` : When a UE moves during communication, it may change of `Connectivity Node`. This action is called handover.

`MN` : Mobile Node. An equipment that allows users to access network services. The MN is mobile.

`Node` : A node is a part of the network. It implements a set of `functions`. It is physically independent of the other nodes, and communicates with them based on standardized interfaces.

`Organic architecture` : An organic architecture is a set of `nodes` within a network.

`Route` : The physical path, within a network, towards the location of a given `MN`. When the `MN` moves during communication, this route may change. In this case, the route information shall be updated to enable data delivery to the new MN location.

`Service` : In this report, a service is a mix of one or many applications (e.g. voice, video, etc). A service may be controlled through a `session`.

`Session` : A session is characterized by the name, the location of the participants to this session, and the `service` used by these participants. It is managed through a set of signalling between the participants that enables to negotiate the characteristics of the session and to establish, modify or release the session.

Introduction

A new ecosystem for Mobile Network Operators

Over the past years, Mobile Network Operators (MNOs) have been able to control the data traffic volume in their respective networks and have had satisfying business models. Indeed, most of the applications were charged on the duration or volume basis and were low bitrate consuming. The situation is changing now and the telecommunication ecosystem is undergoing a deep transformation with a plethora of different players, competing, each one, on its market segment to deliver the best services to customers at the cheapest price. Each player in this chain creates needs and requirements with regard to the other players.

Firstly, MNOs are offering high bitrates on their radio interfaces thanks to the HSPA radio technology [1]. In the future, they will provide higher bitrates with the LTE [2] and WiMAX [3] technologies.

Secondly, manufacturers are designing very attractive and ergonomic devices such as the iPhone, BlackBerry, and Internet tables. These devices, benefiting from the high bitrate radio interfaces, generate a substantial amount of traffic and require more and more bandwidth in the mobile networks. According to Cisco [4], it is expected in 2014, that smartphones will generate about 21% of the overall traffic. They have also predicted that USB dongles, these cards plugged into laptops and allowing to download and view rich media contents for example, will generate 70% of the overall traffic (figure 1).

Thirdly, the service provider efforts in enhancing application ergonomics, and the increasing popularity of devices with high quality screens, increase people's interest for on-line internet services related to entertainment, general knowledge, professional life, health care delivery, etc. People enjoy playing mobile games, sending instant messages, watching news, maintaining their social or professional networks (e.g. Facebook) and sharing high volume contents like video films. These uses create on the one hand, the need for new applications and higher performance devices, and on the other hand, require more capacity in the networks.

The above elements also show that an **exponential traffic increase** is expected in the mobile networks in the forthcoming years. Cisco [4] estimates that "mobile data traffic will double every year through 2014, increasing 39 times between 2009 and 2014. Mobile data traffic will grow at a compound annual growth rate (CAGR) of 108 percent between 2009 and 2014, reaching 3.6 Exabyte per month by 2014". Intel [5] predicts that "traffic will be multiplied by 350 from 2010 to 2020". Although these estimations are different, they confirm the traffic growth trend.

Despite the traffic explosion, **MNO revenues are likely to stagnate or fall**. The historic MNO business models, charging users on the duration or volume basis, are no longer valid because of the intense pressure on the prices. Among others, the reason is that, with the IP network convergence,

all services are transported transparently over IP and obey the fixed/broadband access business models with flat fees.

Figure 1: Cisco forecasts for traffic generated by dongles (laptops) and smartphones (from [4])

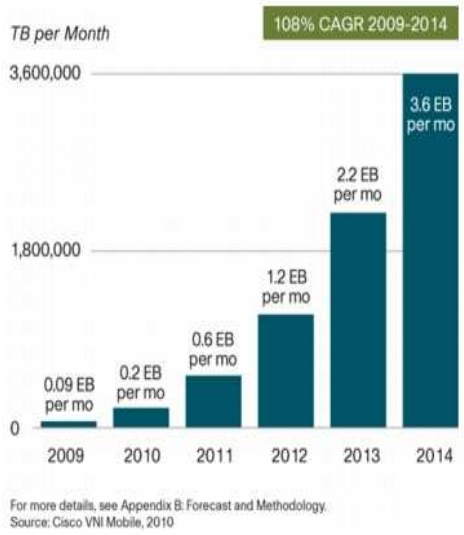


Figure 2: Cisco forecasts for mobile data growth (from [4])

Research problems

Based on the previous section, it appears that MNOs will face an enormous challenge: while device and service providers revenues are increasing, MNOs have to handle the increasing traffic volume on their network and offer QoS to their subscribers at the lowest cost. This leads onto several questions: How are MNOs going to face this challenge? Are current mobile networks armed enough to exit this situation, in other words, are they ready to face this challenge? If not, is there an immediate solution?

The main motivation in this research work lies in these questions. It aims at the definition of the main requirements that have to be fulfilled by a mobile network to get away from this situation, and at the proposal of short and long term solutions allowing MNOs to regain a healthy position in the telecommunication ecosystem. Four criteria are considered in investigating the readiness of MNOs for the new ecosystem. They are:

- **Scalability**: scalability is one of the major criteria that has to be studied in case of an exponential data growth. Scalability is tied to economic aspects. It means that, in case of data growth, network investments due to node duplication have to remain profitable. The network must be scalable in many dimensions. Firstly, it must be the least sensitive to traffic growth or easily cope with it, without impacting the QoS or operators revenues. Secondly, it must be flexible and accept additional functions, without introducing complexity that could increase OPEX costs for example. Thirdly, it must be as independent as possible of services, but provides means for service control (see service control below). These three dimensions are considered in this thesis.

- **Service control**: mobile networks should not be simple "dump pipes". They should allow for operators other revenues than those based on volume consumption. Service control is an important toolbox enabling operators to build intelligent business models. It provides the network with information about the subscriber, the requested service and contextual information (e.g. location). This information could be useful to perform control functions or offer added-value services; for example: tune the QoS and the offered bandwidth on the network according to the requested service, or control the access to the service according to user subscription, or again perform service-based charging, etc.

  Service control offers MNOs the possibility to replicate what Google and others provide, such as targeted advertising or customized services to users in relation to their Internet searches, TV viewing, etc. MNOs have also the possibility of monetizing their bandwidth with regard to service providers by selling them a specific bandwidth and QoS for a certain number of requests sent by users towards service providers servers. Thus, revenues can be shared in a balanced way between MNOs and service providers.

- **QoS**: QoS is an important element on which MNOs should bet in order to attract users and distinguish their networks from others. MNOs should provide users with a QoS corresponding to their subscription and to the requested services. This has to be done as economically as possible while saving resources. In this report, two global QoS indicators are considered: the performance to access the service and the performance of the service once it is established. These indicators have been studied by investigating the service access and the mobility procedures.

  Service control allows and eases an optimal QoS handling. Indeed, it may be used to determine QoS rules for data flows so that resources can be reserved on the network accordingly. In the opposite way, according to the resources available in the network, services can be adapted so that users are offered a minimal service.

  QoS can be, in some way, one of the scalability dimensions. Indeed, respecting QoS requirements may impose duplicating network nodes, even when they are not fully loaded.

- **Service and network convergence**: this criterion is important for an operator as it allows cost reduction.

  Service convergence means that the same services can be accessed from any IP access network. It enables to share service platforms between different IP access networks, instead of being dedicated to each IP access network, which optimizes service costs.

  Network convergence means that the same network architecture (nodes and interfaces) and the same means (protocols, methods) are used to access services, whatever the type of physical connectivity they support.

Thesis contributions

This thesis was begun in 2007. It is among the first works highlighting the changing ecosystem and focusing on the impact of exponential traffic growth on current mobile networks. Since then, many white papers [6, 7, 8] raised the same problems and indicated the urgent need for MNOs to review their architectures and business models.

Proposals made in this thesis have been used to feed additional studies in the P1857 Eurescom project in 2009 [9], and have enabled to propose research areas for the MEVICO Celtic European project in 2010 [10].

This work covered various research fields: ranging from network architectures with analysis and conception, to detailed procedure specifications and thorough performance analysis.

The major contributions of this thesis are the following:

Specifying requirements for mobile networks to face the ecosystem challenges

I have analyzed the capability of mobile networks to face the ecosystem challenges i.e. support the data volume increase. As the analysis should not be limited to a specific network, I have proposed a generic network model leveraging different IP access networks (IP-AN), as well as their interaction with the service control overlay network (IMS), through the policy control layer (PCC). This model is named IP-AN//PCC//IMS. Then, I have carried out the model analysis based on the following criteria: scalability, service control, QoS, service and network convergence. For the two last criteria, a detailed description of the service access and mobility procedures has been made.

Based on the IP-AN//PCC//IMS model analysis, I was able to identify different problems. Solutions in state of the art or those I proposed, cannot solve these problems simultaneously and without making the model more complex.

Despite this, I defined a set of generic requirements that have to be fulfilled by a mobile network in order to be able to face the new ecosystem challenges.

Proposing a new model for future mobile networks

Based on the defined requirements, I reviewed the IP-AN//PCC//IMS model and proposed a new model for future mobile networks, called UFA (Ultra Flat Architecture). UFA is defined from an architectural and procedural point of view.

UFA fulfills the different requirements. It is scalable, service and network convergent, provides service control, and ensures QoS. Its main idea is to rely on distributed anchor nodes instead of centralized ones, as in the IP-AN//PCC//IMS model. It also uses the same service control solution (IMS) for all applications. Therefore, it is entirely based on SIP. It is called flat as it reduces the number of network node types, and gathers, in the same node, the IP access network functions, the policy control functions and the IMS functions. These UFA properties have enabled the definition of smart and efficient service access and mobility procedures for UFA. A large variety of applications has been considered while specifying these procedures. These applications differ from the protocol controlling them (SIP or not) and the protocol transporting them (RTP/UDP, SCTP, TCP) on the transfer plane.

UFA enables a low delay to access services, a low handover delay and allows to tune simultaneously all-OSI layers in the mobile and corresponding nodes. This has the advantage, among other things, to adapt the application to the resources available in the network.

Evaluating the proposed model

To prove the IP-AN//PCC//IMS problems and show UFA advantages, I used different implementation and evaluation methods.

Firstly, based on analytical models, the service establishment delay has been measured in UFA and compared to IP-AN//PCC//IMS, considering different network load situations. Results show UFA advantages.

Secondly, UFA has been implemented on a testbed. UFA handover delays have been measured on this testbed and compared to a reference procedure used with IP-AN//PCC//IMS, for real time applications transported over RTP/UDP (e.g. voice+video). The testbed has enabled to validate UFA concepts. Measurements have shown that UFA mobility procedure outperforms the reference procedure.

Thirdly, UFA (architecture and mobility procedure) has been proposed to manage the mobility of applications transported over SCTP, replacing thus Mobile SCTP (m-SCTP), which is till now the best known mobility protocol for these applications. It has been demonstrated, using NS2 simulations, that UFA outperforms m-SCTP. Indeed, with m-SCTP contrary to UFA, SCTP considers that data losses are due to congestion (instead of handover) and retransmits them after a timeout period, causing a high handover delay and degradation of resource usage.

Thesis organization

Part I of this thesis analyses the readiness of current mobile networks for the new ecosystem, with chapter 1 focusing on the scalability and service control criteria and chapter 2 focusing on QoS and service and network convergence criteria. It also formulates a set of requirements to be fulfilled by mobile networks models, in order to face the challenges of the new ecosystem.

Part II proposes a new model (UFA) for mobile networks, based on the set of requirements defined in part I. Chapter 3 describes UFA, and chapter 4 specifies its procedures.

Part III, including chapters 5, 6 and 7, validates UFA model and measures its performances.

Part I

State of the art

CHAPTER 1

Are current mobile networks ready for the new ecosystem?

Mobile networks represent important investments for operators. With the new telecommunication ecosystem and the exponential data growth, the first question that comes to mind, concerns the mobile networks capability to cope with the investments increase, while granting proportional revenues for operators and ensuring QoS to users.

The introduction of this report has defined four criteria in order to answer the question raised previously. These crieteria are: the networks scalability, the service control support by these networks, the QoS they offer, and the service and network convergence support. This chapter focuses on the two first criteria. It also formulates the requirements making these criteria met.

Among other factors, the scalability of a network is tied to its organic architecture. Indeed, depending on the number of node types in the network, the functions they implement, and the way they interact, the network may be more or less scalable. Therefore, in this chapter, the mobile network organic architectures are focused on.

This chapter is structured as follows:

In section 1.1, a generic model for mobile network organic architectures has been drawn, based on different proposals in the literature [11, 12, 13]. This model has a layered structure, and is constituted of an IP access network (IP-AN) providing IP connectivity to users, one or more overlay networks bringing additional features to the IP-AN, and interaction layers between the IP-AN and the overlay networks.

In section 1.2, a specific model for mobile network organic architectures [13, 14], having a layered structure, is detailed. In this specific model, noted as **IP-AN//PCC//IMS**, IMS is a service control overlay network and PCC is an IMS - IP-AN interaction layer for policy control. The IP-AN part of this model leverages different IP-AN examples standardized within 3GPP and WiMAX bodies.

In section 1.3, the IP-AN//PCC//IMS model presented in section 1.2 is confirmed through different IP-AN examples standardized within 3GPP and WiMAX bodies.

In section 1.4, the scalability and the service control criteria are studied for the IP-AN//PCC//IMS model.

In section 1.5, two service types on which the next chapters will focus are defined. Finally, section 1.6 provides a conclusion.

1.1 Mobile networks layered model

Network functions cannot be defined simultaneously. Moreover, there is a need to implement these functions in separate nodes, to ease their evolution and deployment. This explains the fact that a network is structured in a layered model as described hereafter, and in the figure 1.1:

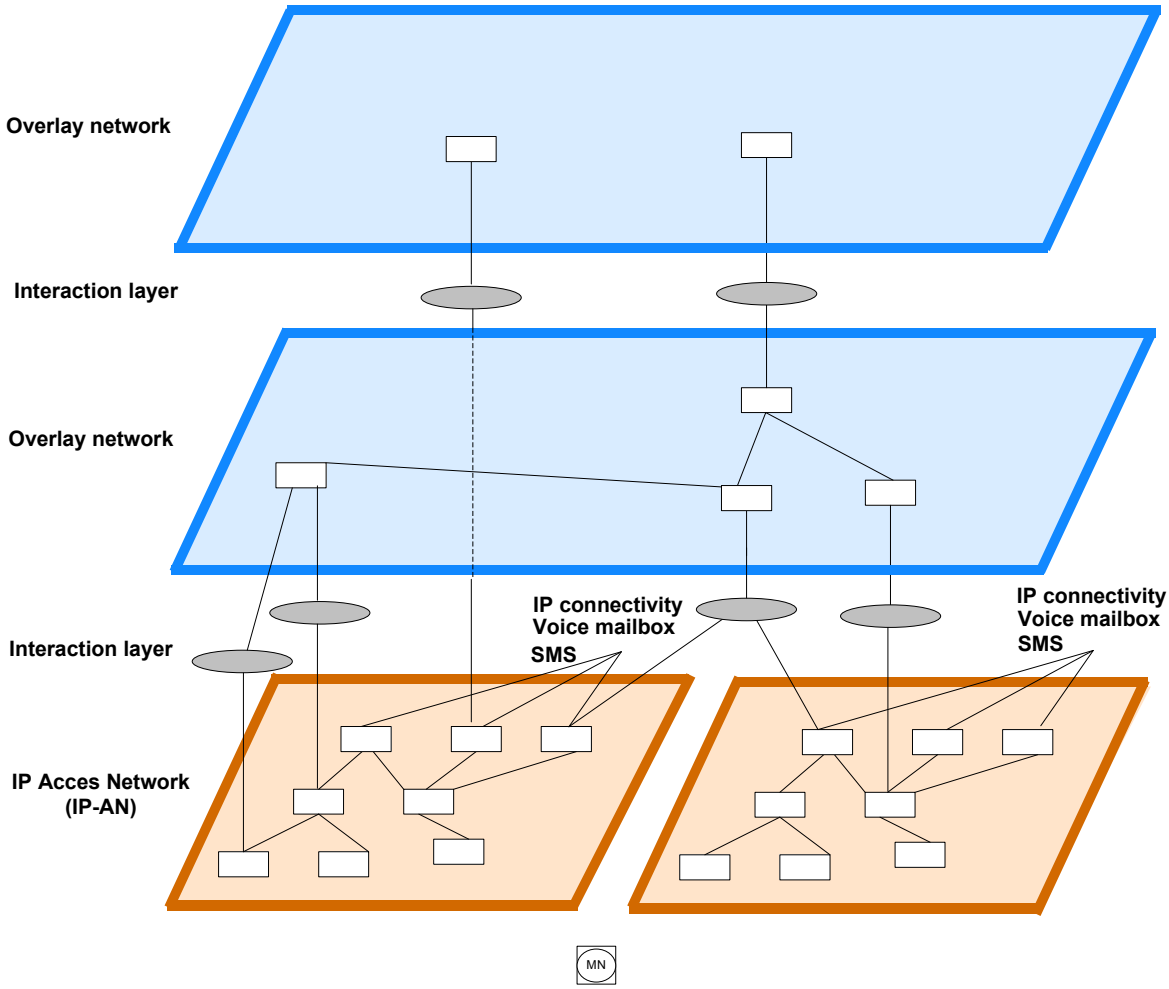


Figure 1.1: Mobile networks layered model

- **IP-Access Network (IP-AN)**: This is the basic layer of a network. It is the collection of network nodes and functions deployed by an operator, in order to provide its clients network services (such as connectivity to the internet), and access to other services (such as SMS, voice mailbox, etc). A MN can benefit from these services using one or many IP-ANs simultaneously or successively, whatever their access technology. There are many examples of IP-ANs defined in 3GPP and WiMAX standards. In section 1.2.1, a model for these examples is provided.

- **Overlay networks**: These are layers on top of IP-ANs. Overlay networks are recognized as a viable alternative to overcome in a cost effective manner the limitations of existing networks with regard to some lacking functions [11] such as: QoS [12], adaptive service delivery [15, 16], multicast, routing, security [15], mobility [17], etc. The basic idea of overlay networks is to form a network of specialized nodes implementing the lacking functions without modifying the underlying network. It is possible to have many overlay networks on top of a given IP-AN, each one dedicated to a set of functions.

As described in the introduction of this report, service control allows operators to build intelligent business models. It can provide the IP-AN with information about the subscriber, the requested service and contextual information (e.g. subscriber location). This information is useful to perform control functions on the service or IP-AN levels, and offer added-value services. More than these advantages, service control has a central role as it particularly facilitates the deployment of other overlay networks, such as those responsible for service customization or adaptive service delivery (transcoding, caching). For these reasons, **service control overlay networks are important**. In section 1.2.2, a concrete example of a service control overlay network (IMS) is detailed.

- **Interaction layers**: An overlay network interacts with an IP-AN through interaction layers, that allow to attain a set of objectives:
  - Enable IP-ANs-related decisions: thanks to the information and orders received from the service control layer, operators can: (1) authorize or block data in the IP-AN; (2) allocate bearers not exceeding the service demand, user subscription and IP-AN capabilities; (3) respect their engagement towards users by ensuring them the QoS, for which they have subscribed, etc. These functions are gathered under the name **policy control**. In section 1.2.3, an interaction layer for policy control between the IP-AN and the IMS is described.
  - Enable service-based charging: this function can be performed by correlating the service description and the related data volume consumed in the IP-AN.
  - Enable service-related decisions: this function allows to take decisions on the service level based on information from the IP-AN. For example, based on the IP-AN load, the user service can be downgraded.
  - Optimize procedures, by correlating information from the IP-AN and the service control overlay network.

1.2 IP-AN//PCC//IMS model

The previous section has highlighted the interest of service control overlay networks, and policy control interaction layers. Therefore, this section details one of the most common mobile networks model, supporting these features and having a layered structure. In this model, noted as **IP-AN//PCC//IMS**, IMS is a concrete service control overlay network and PCC is an IMS - IP-AN interaction layer for policy control.

IMS and PCC are described based on [13, 14]. A model for different IP-AN examples standardized within 3GPP and WiMAX bodies is provided. IP-AN, PCC and IMS organic architectures are focused on, as they condition the model scalability.

Note: IP-AN, PCC and IMS are defined within standards (3GPP, WiMAX). Sometimes, in these standards, the physical nodes name contains the word "Function". In this report, the same convention as in the standards is followed, which explains the fact that some of the names with the word "Function" are associated to nodes.

The description mainly focuses on the handling of packet data services.

1.2.1 IP-Access Network (IP-AN)

An IP-AN[1] is a set of functions implemented on the transfer plane over which user data passes, and on the control plane. Generally, IP-ANs offering the same services have the same functions.

[1] called IP-CAN in 3GPP specifications

Although their organic architecture may differ regarding their node types and number, and the way their nodes implement functions and interact, their organic architectures obey to the same model.

This section details the IP-ANs transfer and control planes functions; then it provides a model for their organic architectures, on the transfer plane. The model for the control plane will be given in section 1.3, while describing the different IP-ANs examples.

1.2.1.1 IP-AN control and transfer plane functions

Transfer plane functions

- These functions include basically the means to transfer data to the MN whatever be its location in the coverage of the IP-AN. It may also encompass **header compression**, **data anchoring**, **policy enforcement**, and **data ciphering** functions.

Control plane functions

- **Access control**: is the process by which a network deduces whether and how a user is allowed to access the services of an IP-AN. It includes **authentication** functions (secure identification of the service requester), **authorization** functions (determination of the services the requester can access to), **admission control** functions (determine if the requested resources are available). It also comprises **IP address allocation** mechanisms, responsible for allocating an IP address to the MN once it is authenticated and authorized to use the IP-AN services.
- **Mobility management**: when a user is moving during a communication, two functions are involved: **handover decision** and **handover execution**. Handover is executed thanks to signalling protocols updating the route information in the network towards the new MN location. The node in the network, receiving handover execution signalling is called **signalling mobility anchor**.

  When a user is in idle state, mobility management includes the tools for **user reachability**, that determine its location in case of incoming calls. Reachability function is very tied to **registration** and **location update** functions, that update the mapping between the user identity and its physical location.
- **Radio resource management**: these are functions related to radio resource allocation, according to the radio conditions, service type, user priority, load criterion, etc.
- **Network management**: these functions include inter-node load balancing and anchor node selection.

1.2.1.2 A model for IP-AN organic architectures

Figure 1.2 presents a model for the IP-AN organic architectures on the transfer plane. It also shows that control plane functions can be implemented in the same nodes as the transfer plane nodes, or in separate nodes.

The model is centralized and hierarchical. It is constituted of different nodes on different levels. A node on level x is called $\mathbf{Node_x}$. A $Node_x$ connects and manages a number of $Node_{x-1}$.

Within a $Node_x$, data traffic related to a given MN may be identified by: the IP address allocated to the MN, a tunnel identifier, a bearer identifier or a mapping between these identifiers.

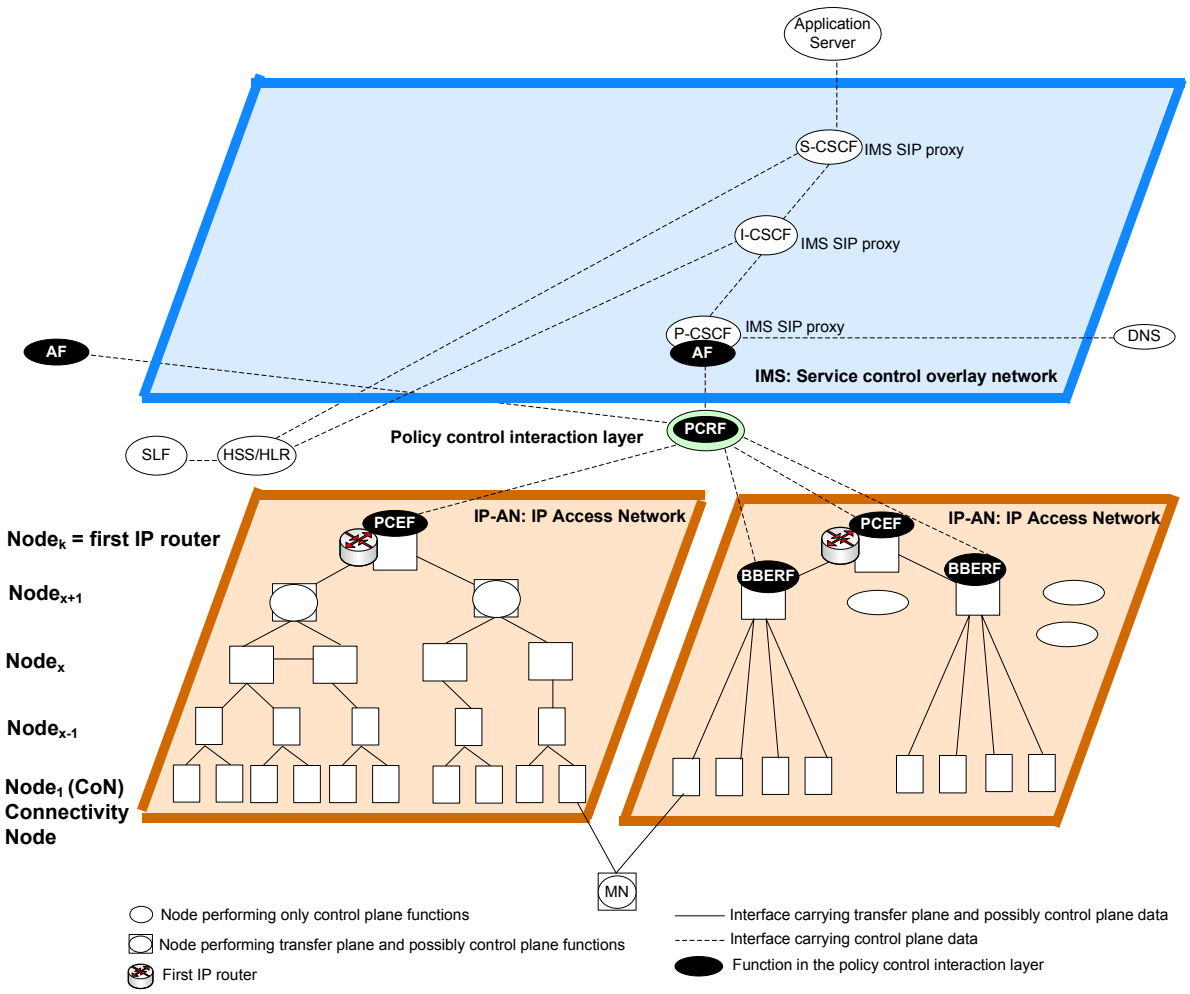


Figure 1.2: A common mobile networks layered model: IP-AN//PCC//IMS

When a MN moves between two Node$_{x-1}$, there are many possibilities for routing the traffic to the MN:

- If the two Node$_{x-1}$ are managed by the same node Node$_x$, then traffic continues to pass through Node$_x$, which takes the role of a **data anchor** for mobility between Node$_{x-1}$.
- If the two Node$_{x-1}$ are managed by two different Node$_x$:
  - either the old Node$_x$ remains on the data route and forwards the traffic to the new Node$_x$, which itself forwards the traffic to the new Node$_{x-1}$;
  - or the old Node$_x$ is no more on the data route, and data traffic passes through the new Node$_x$, which forwards the traffic to the new Node$_{x-1}$. This imposes that Node$_{x+1}$ managing the two Node$_x$ acts as a **data anchor** for mobility between Node$_x$.

In the IP-AN organic architecture, there are two particular Node$_x$:

- The **First IP router** is the upper node within the IP-AN architecture. Within this node, a MN is mainly identified by its IP address making it reachable from the internet. The first IP router anchors data traffic between the internet and MNs, and even between MNs attached to the same IP-AN.

- The **Connectivity Node (CoN)** is the lower node within the IP-AN. It is the first hop connecting the MN to the IP-AN (e.g. eNB).

1.2.2 IMS: a concrete service control overlay network

IP Multimedia Subsystem (IMS) [13], being developed by 3GPP, is a concrete service control overlay network currently capturing more and more interest for two reasons:

1. IMS implements standardized and open interfaces towards the service platforms. This enables the integration of different services developed by various third party vendors. It also makes easier the adoption of services such as instant messaging, video conferencing, VoIP, application sharing, etc.
2. IMS implements a unique and standardized interface towards the IP-ANs. This enables service convergence, meaning that users can access IMS-based services from any IP-AN.

Whereas IMS has been first specified by 3GPP in Release 5 as a service control layer for the UMTS IP-AN specifically, the service convergence feature has been made gradually possible in Release 6 and Release 7. IMS accomplishes a set of tasks during the **service access procedure**, which comprises two phases: (1) the **registration and authentication phase**, and (2) the **service establishment phase**. To accomplish these tasks, IMS relies on SIP protocol [18] (all SIP terminology is given in appendix A). As shown in figure 1.2, IMS includes SIP proxy nodes called Call Service Control Functions (CSCF), and interacts with charging-related nodes, databases and Application Servers.

1.2.2.1 Call Service Control Function (CSCF)

The CSCFs are SIP proxies with additional functions playing an important role during service access procedure. There are three kinds of CSCF: the Proxy-CSCF (P-CSCF), the Interrogating-CSCF (I-CSCF) and the Serving-SCSF (S-CSCF).

- **Proxy-CSCF (P-CSCF)**: The P-CSCF is the first SIP proxy in the IMS, intercepting SIP signalling traffic sent by the MN. It can be located either in the visited network or in the home network.

  The MN needs to discover the P-CSCF IP address to be able to send SIP messages to the IMS. The P-CSCF establishes an IPsec Security Association[2] (SA) with the MN, in order to ensure the integrity and the confidentiality of SIP messages received from the MN. The P-CSCF discovery and IPsec SA building are performed during registration/authentication phase (more information is in section 2.1).

  During the service establishment phase, the P-CSCF checks whether the requested service is authorized for the MN, based on its own policies and current IP-AN capabilities. It also interacts with policy control functions (see section 1.2.3) that authorize the service and allow to correctly establish the bearer transporting the service on the IP-AN (more information is in section 2.1).

- **Serving CSSF (S-CSCF)**: The S-CSCF is located in the home network and acts as a SIP registrar. It maintains a binding between the user logical identity[3] and its physical address[4]. The S-CSCF intervenes during the registration/authentication phase, by retrieving

[2] A set of information that describes a particular secure connection between one node and another
[3] address of record, see A.1.3
[4] address of contact, see A.1.3

user authentication data and service profile from the HSS (described below). During the service establishment phase, if the requested service is not in line with the user service profile, the S-CSCF rejects the service. The S-CSCF has the capability to decide whether a request should be routed to a specific Application Server (AS) (defined below) or not.

- **Interrogating-CSCF (I-CSCF)**: The I-CSCF is located at the edge of an operator home domain. It hides the S-CSCF and intervenes only during the registration/authentication phase as follows. When the P-CSCF receives SIP REGISTER request from a MN, it determines the I-CSCF IP address by DNS mechanisms based on the Request-URI domain name contained in the request. The P-CSCF then forwards the request to the I-CSCF. The I-CSCF assigns a S-CSCF to the MN by interrogating the HSS (described below) and forwards the SIP REGISTER request to the S-CSCF. After that, the I-CSCF is no more on the path of SIP requests sent by the MN.

1.2.2.2 Databases

The main databases the IMS interacts with, are the Home Subscriber Data (HSS) and the Subscription Locator Factor Function (SLF).

- **HSS**: The HSS is an evolution of the HLR (Home Location Register) which is a GSM/GPRS database. It is the central data storage for user-related information and includes among other items, the user identities, the authentication and security data, the user profile and the S-CSCF assigned to the registered users.
- **SLF**: When multiple and separately addressable HSS are deployed, the SLF is used to find the address of the HSS that holds a given user.

1.2.2.3 Application Servers

The IMS interacts with Application Servers (AS). An AS hosts and executes services such as Presence, Push to Talk. An AS is located in the user home network or in a third party network. It interfaces with the S-CSCF using SIP, and may impact SIP sessions. Depending on the services it provides, it can act either as a SIP proxy, a SIP User Agent, or a SIP Back-to-Back User Agent.

1.2.3 PCC: An IMS - IP-AN interaction layer for policy control

As described in section 1.1, the interaction between the service control overlay network and the IP-AN enables to achieve different objectives among them, policy control. This section presents a 3GPP normalized solution for policy control, called Policy and Charging Control (PCC) [14]. PCC deals with policy control and charging. In the following, only policy control aspects are detailed.

Work on PCC has begun from Release 5. In few words, PCC enables to authorize the service and to calculate the corresponding policy rules to be enforced on the IP-AN level. These rules are related mainly to the QoS authorized for the service on the IP-AN, and the service-related data flows authorized to pass through the IP-AN.

PCC introduces four groups of functions (figure 1.2), whose definitions are tied to their locations: the AF (Application Function) which is in the service control layer, the PCRF (Policy and Charging Rules Function) which is in an independent node containing the main policy control functions, the PCEF (Policy and Charging Enforcement Function) and the BBERF (Bearer Binding and Event

Reporting Function) which are in the IP-AN. The PCRF has standardized interfaces towards the AF, PCEF and BBERF. In this way, the PCRF can be shared between different IP-ANs and different service control layers (IMS or others).

1.2.3.1 AF (Application Function)

The AF is located in the service control layer, within the nodes located on the session signalling path. The AF is specific to the service control layer. For IMS, it is within the P-CSCF; otherwise it can be within a streaming server or an FTP server.

The AF identifies the data flows (applications) related to the service and maintains the mapping between the `session identifier` and the `data flow descriptors` (source/destination IP addresses and source/destination transport ports).

As shown in figure 1.3, the AF translates the service description, contained in the session signalling, into a standardized format (Service Information (`SI`)). Then, it sends the `SI` to the PCRF to ask for its authorization and for the formulation of policy rules towards the IP-AN (more information is in section 2.1).

When the service control layer is the IMS, the `session identifier` is the `SIP dialog identifier`, the service is generally described through the Session Description Protocol (`SDP`) (see section A.2), and the `Data flow descriptors` are deduced from the `SDP`.

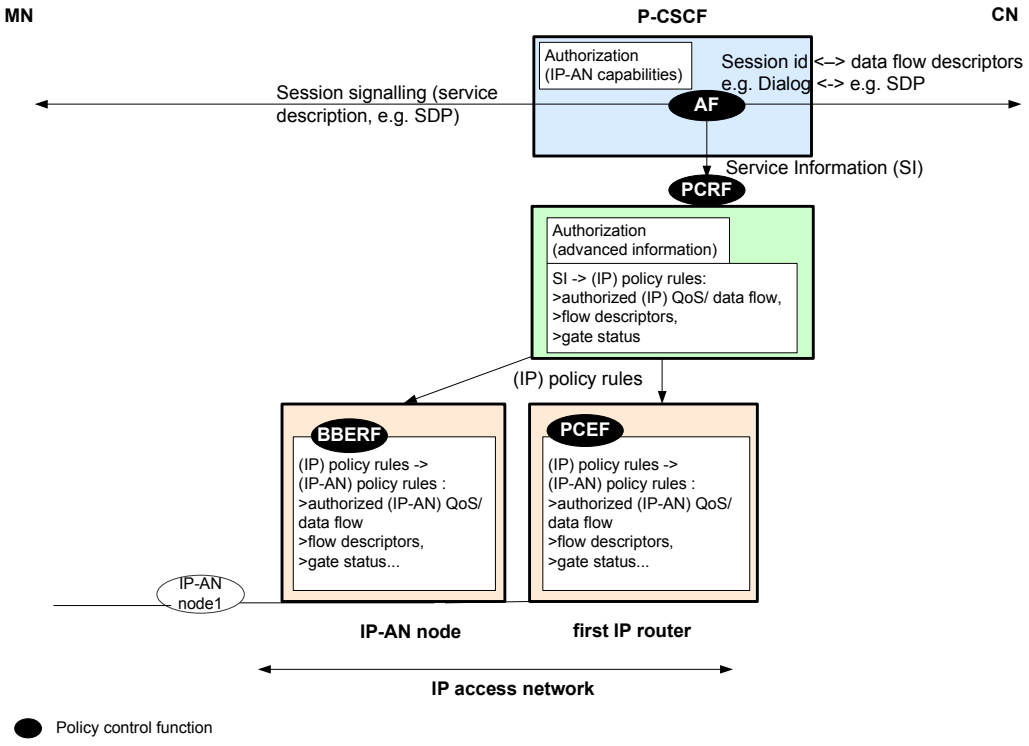


Figure 1.3: Policy control functions in the IP-AN//PCC//IMS model

1.2.3.2 PCRF (Policy and Charging Rules Function)

The PCRF includes the main functions of the PCC. It is located within a node independent of the service control layer and the IP-AN.

As shown in figure 1.3, the PCRF receives the Service Information (`SI`) from the AF. It may authorize the service based on advanced information. It also calculates for the `SI`, the `(IP) policy rules` and sends them to the PCEF and BBERF, located in the IP-AN.

The `(IP) policy rules` are calculated for the IP level, to ensure their independence from IP-ANs specificities. They include (more information is in section 2.1):

- The `data flow descriptors` identifying the data flows, generated by the applications which are parts of the service.
- The `authorized (IP) QoS` corresponding to the QoS authorized for the service on the IP level.
- The `events configuration` identifying the events that shall be reported by the IP-AN to the PCRF.
- The `gates status` indicating for each data flow whether the related traffic is authorized or not to pass through the IP-AN.

1.2.3.3 PCEF (Policy and Charging Enforcement Function) and BBERF (Bearer Binding and Event Reporting Function)

The PCEF is located in the IP-AN, in the first IP router. Its role is to translate the `(IP) policy rules`, received from the PCRF, into `(IP-AN) policy rules` understandable by the IP-AN, specifically the bearer level (figure 1.3).

The `(IP-AN) policy rules` include the same elements as the `(IP) policy rules`, except for the `authorized (IP) QoS` that is converted into `authorized (IP-AN) QoS`.

The PCEF enforces/applies the `(IP-AN) policy rules` on the IP-AN, that includes the bearers supporting the data flows. The PCEF possibly enforces the `(IP) policy rules`. Indeed, the `authorized (IP) QoS` may be needed to perform local IP scheduling, in addition to the IP-AN scheduling performed based on the `authorized (IP-AN) QoS`.

This PCEF role was defined in Release 5 and was valid until Release 7. It supposes two elements: (1) the first IP router is the bearer endpoint and (2) the bearer endpoint does not change for a given MN whatever be its mobility. Based on these two elements, a single enforcement point (PCEF) within the IP-AN, located in the first IP router, is an appropriate and optimized choice.

For some IP-AN cases, the two stated elements are not fulfilled: the first IP router is not the bearer endpoint but just represents the IP layer, and the bearer endpoint may change during MN mobility. There is thus a need for a second enforcement function (BBERF) within an IP-AN node ending the bearer, and a procedure sending the policy rules from the source bearer endpoint to the target bearer endpoint during MN mobility.
For the stated IP-AN cases, the PCEF in the first IP router is used to enforce the `(IP) policy rules` on the IP layer and the BBERF is used to enforce the `(IP-AN) policy rules` on the bearer level, and to handle the change of the bearer endpoint during MN mobility.

As it will be shown in the next sections, the need for the BBERF was identified only from Release 8 since, before that Release, 3GPP has been working only on UMTS as IP-AN (for UMTS the first IP router i.e. the GGSN is the bearer endpoint). In Release 8, when defining EPS IP-AN, the BBERF has been introduced since the first IP router i.e. the P-GW may be not the bearer endpoint (see section 1.3).

1.3 Examples of IP-ANs and their interaction with PCC and IMS (IP-ANs//PCC//IMS)

This section provides examples of existing IP-ANs, to prove and illustrate the IP-AN model (described in section 1.2) and its interaction with the PCC and the IMS. The objective is also to track in the time the origin of this model and be able to analyze its readiness for the new ecosystem in section 1.4.

For each IP-AN, I give the location of the first IP router, the names of the different nodes and the functions they implement among those described in section 1.2.1.1. I also provide the location of the policy control enforcement functions (PCEF and BBERF (if present)) in the IP-AN nodes. IMS nodes will be indicated in the figures for the sake of completeness, although they are independent of the IP-ANs.

1.3.1 (GSM and UMTS)//PCC//IMS

GSM (Global System for Mobile communications) [19] is a mobile system introduced by the European standardization body ETSI since 1991. It first offered circuit switched services, then packet switched services providing access to the internet and other services. The latter have been enabled thanks to the introduction of a packet core network[5] (General Packet Radio Service), called **GPRS**, and by bringing some enhancements to the GSM radio access network, renamed **GERAN** (GSM EDGE Radio Access Network). GPRS and GERAN have been defined by ETSI then by 3GPP. 3GPP is an international standardization body born following the cooperation between regional standardization bodies, including the ETSI.

In order to offer higher bitrates on the radio interface, another radio access network called **UTRAN** (Universal Terrestrial Radio Access Network) [20] has been introduced by 3GPP in 1999. The combination of UTRAN and GPRS constitute the 3G mobile network, called **UMTS** (Universal Mobile Telecommunication System) [21].

Both GERAN and UTRAN are constituted of two types of nodes (figure 1.4): (1) the Connectivity Nodes (BS for GERAN and NB for UTRAN) and (2) the Connectivity Node controllers (BSC for GERAN and RNC for UTRAN). The **Connectivity Node controller** connects and controls about hundred of Connectivity Nodes and performs radio resource management, data ciphering and compression. It acts as a **data anchor** for mobility between Connectivity Nodes. It also acts as a **signalling anchor**, as it receives mobility related signalling when the user moves between two CoNs.

GPRS [22] includes two nodes (figure 1.4): the GGSN (Gateway GPRS Serving Node) and the SGSN (Serving GPRS Serving Node). The **GGSN** is the first IP router. It acts as a **data anchor** for mobility between SGSNs, and as a **signalling anchor** since it receives mobility related signalling (GTP [23]) when the user moves between two SGSN. The GGSN terminates the bearers allocated to MNs. The **SGSN** is the node that serves the MN, meaning that it performs access control functions and interacts for this objective with the HSS maintaining subscriber and authentication information. The SGSN also stores security keys for each MN, orchestrates bearer establishment and performs user reachability and GGSN selection functions. The SGSN acts as a **data anchor** for mobility between RNC/BSC. It also acts as a **signalling anchor**, since it receives mobility related signalling (GTP [23]) when the user moves between two RNCs.

In UMTS, the PCEF is located in the GGSN. The BBERF is not needed as the GGSN is the bearer endpoint and does not change during MN mobility.

[5] connected to the GSM radio access network

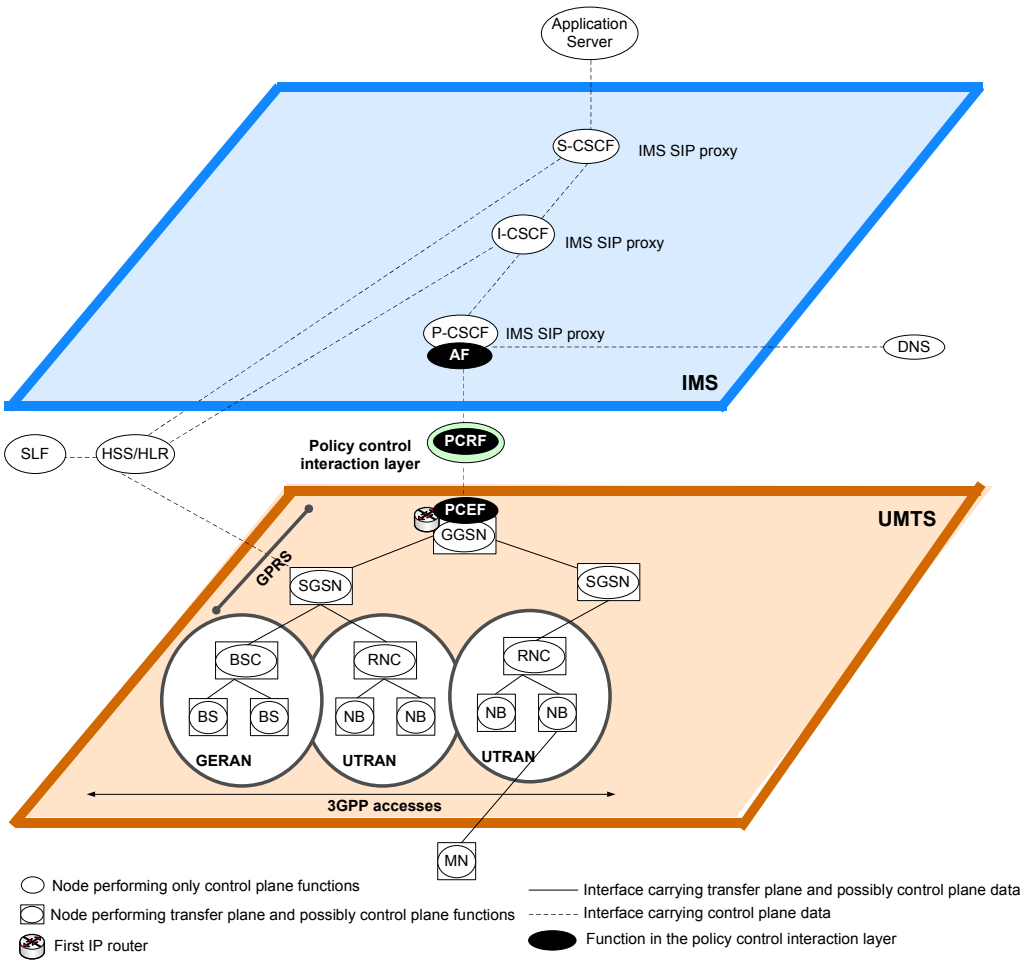


Figure 1.4: (GSM and UMTS)//PCC//IMS

1.3.2 GAN//PCC//IMS

Generic Access Network (GAN) [24], formerly known as UMA (Unlicensed Mobile Access), was introduced by 3GPP in Release 6. It was motivated by operators who wish to increase the 3GPP service[6] coverage and provide subscribers with higher bitrates at a low cost.

Using the same device, GAN subscribers can access to 3GPP services from any non-3GPP access (fixed or wireless) and move between 3GPP and non-3GPP accesses. To do this, a new node called GANC (GAN Controller) is introduced (figure 1.5). The GANC is situated in the access network and connects the non-3GPP Connectivity Nodes to the GPRS packet core network, by emulating BSC/RNC functions. The **GANC** acts as a **data anchor** for mobility between non-3GPP Connectivity Nodes. The **SGSN** acts as a **data anchor** for mobility from (RNC/BSC) to GANC. It also acts as a **signalling anchor**, since it receives mobility related signalling (GTP [23]) when user moves from (RNC/BSC) to GANC.

To secure the access to GPRS, the GANC implements a security gateway that authenticates users and maintains an IPsec SA with them. This security gateway is connected to a 3GPP AAA server, connected itself to the HSS. The SGSN authentication functions are maintained to secure the access to 3GPP services.

[6]services also available through an IP-AN standardized within 3GPP e.g. GSM, UMTS, EPS.

In case of GAN, as for the UMTS, the PCEF is located in the GGSN. The BBERF is not needed as the GGSN is the bearer endpoint and does not change during MN mobility.

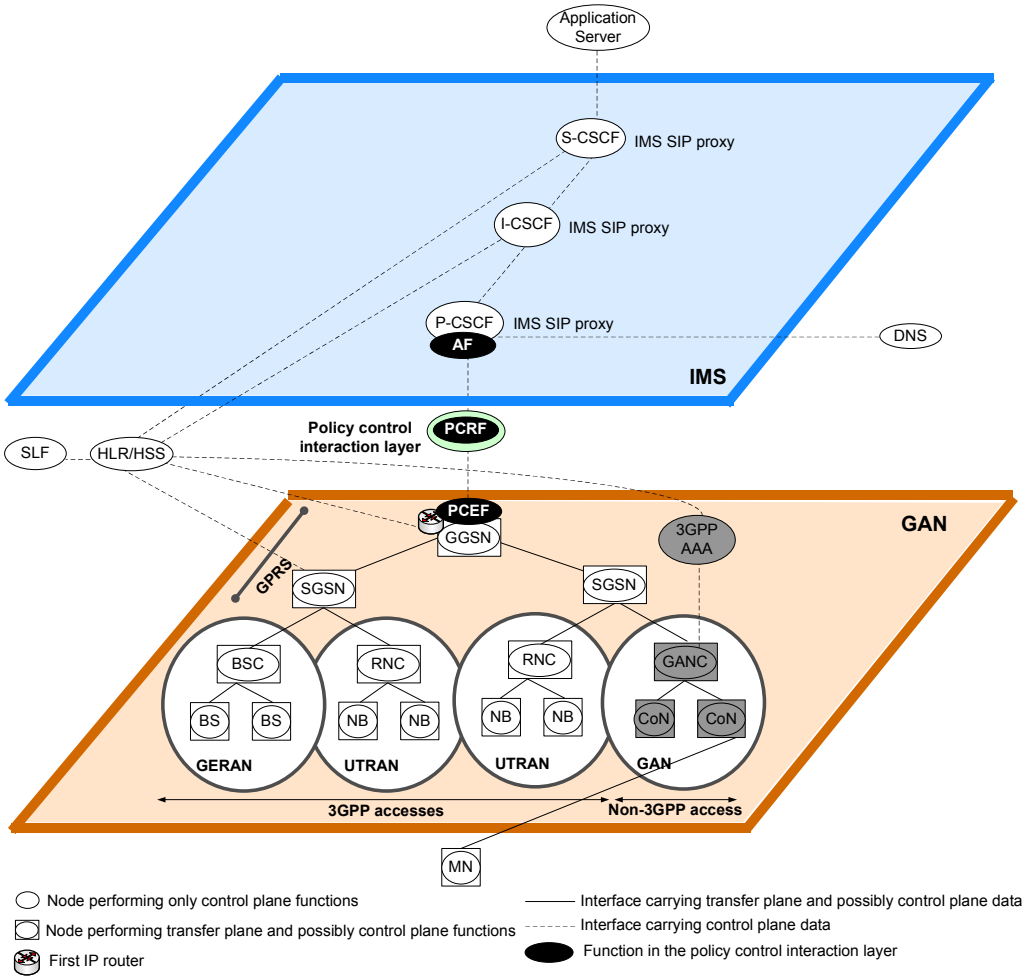


Figure 1.5: GAN//PCC//IMS

1.3.3 I-WLAN//PCC//IMS

Wireless Local Area Network (WLAN) Interworking (I-WLAN) [25] is another IP-AN defined within 3GPP in Release 6. It has the same purpose as GAN, apart from mobility between 3GPP accesses and non-3GPP accesses which is not provided.

In terms of architecture, I-WLAN introduces two nodes (figure 1.6): the PDG (Packet Data Gateway) and the WAG (WLAN Access Gateway). The **WAG** is an intermediate node of this IP-AN. It connects the WLAN Connectivity Nodes and routes the packets to the PDG based on filtering and QoS information received from the 3GPP AAA server, which is connected to the HSS. The **PDG** is the first IP router. It is also connected to the 3GPP AAA server. The PDG uses information received from HSS, through 3GPP AAA server, to authorize users to access 3GPP services. As the route between the MN and the PDG may be not secured, an IPsec SA is established between them.

In I-WLAN, the PCEF function is located in the PDG. As the notion of bearer does not exist in I-WLAN, the PCEF enforces the policy rules only on the IP layer using QoS tools (DSCP marking, traffic shaping, etc.).

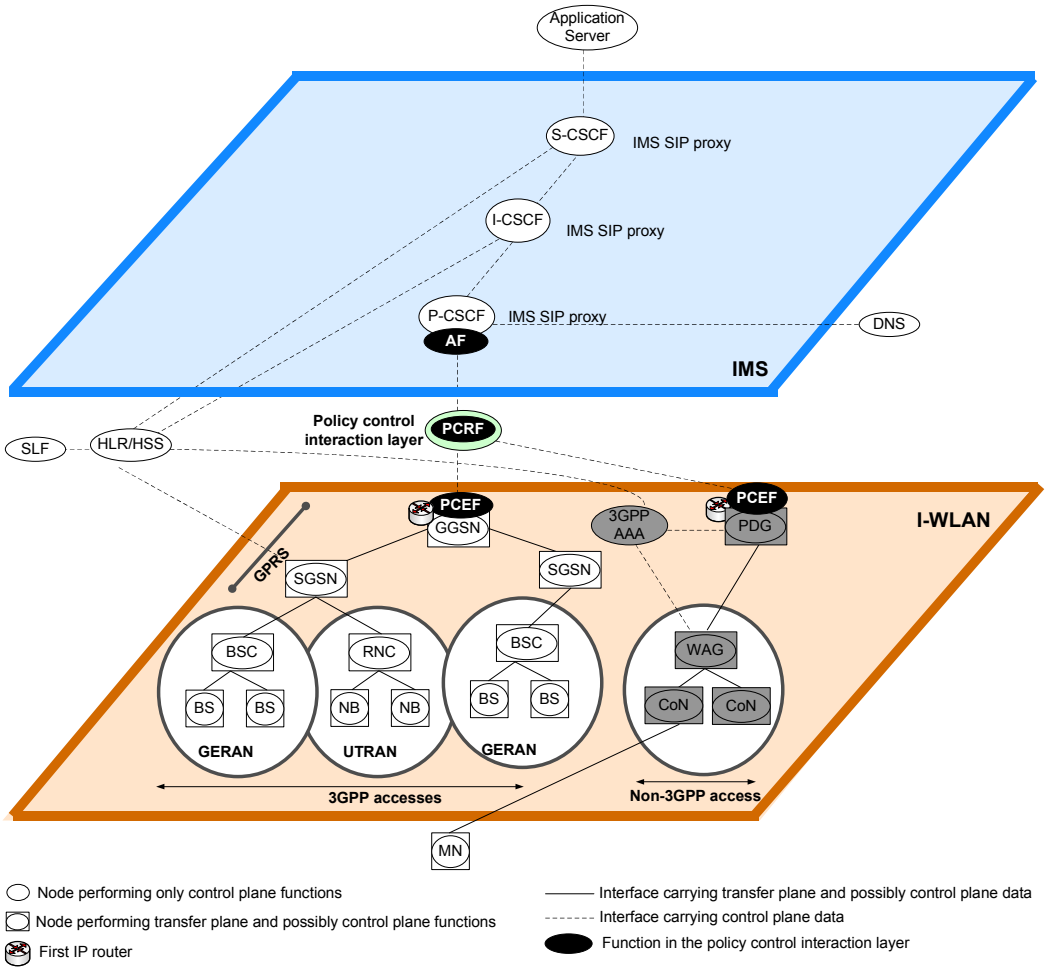


Figure 1.6: I-WLAN//PCC//IMS

1.3.4 (Inter I-WLAN - 3GPP mobility)//PCC//IMS

I-WLAN IP-AN, previously described, just enables access to 3GPP services. To also have mobility between I-WLAN and 3GPP accesses, 3GPP has introduced in Release 8 a standardized solution [26] using a protocol from the Mobile IP (MIP) [27] family. This solution is called inter I-WLAN - 3GPP Mobility (figure 1.7).

In the (Inter I-WLAN - 3GPP Mobility) IP-AN, shown in figure 1.7, the **Home Agent** introduced by Mobile IP protocol, is connected to the GGSN and PDG. It acts as the first IP router (the GGSN and PDG are no more the first IP routers, but just intermediate nodes).

The Home Agent acts as a **data anchor** for mobility between 3GPP access and I-WLAN. It also acts as a **signalling anchor**, as it receives mobility related signalling when the user moves between the 3GPP access and I-WLAN. It is also connected to the 3GPP AAA server to authorize mobility service.

3GPP has preferred not to define PCC enforcement functions for the (Inter I-WLAN - 3GPP Mobility) IP-AN. However, if it has to do it, in theory, the PCEF would be in the Home Agent (the first IP router) and the BBERF would be in the GGSN and PDG.

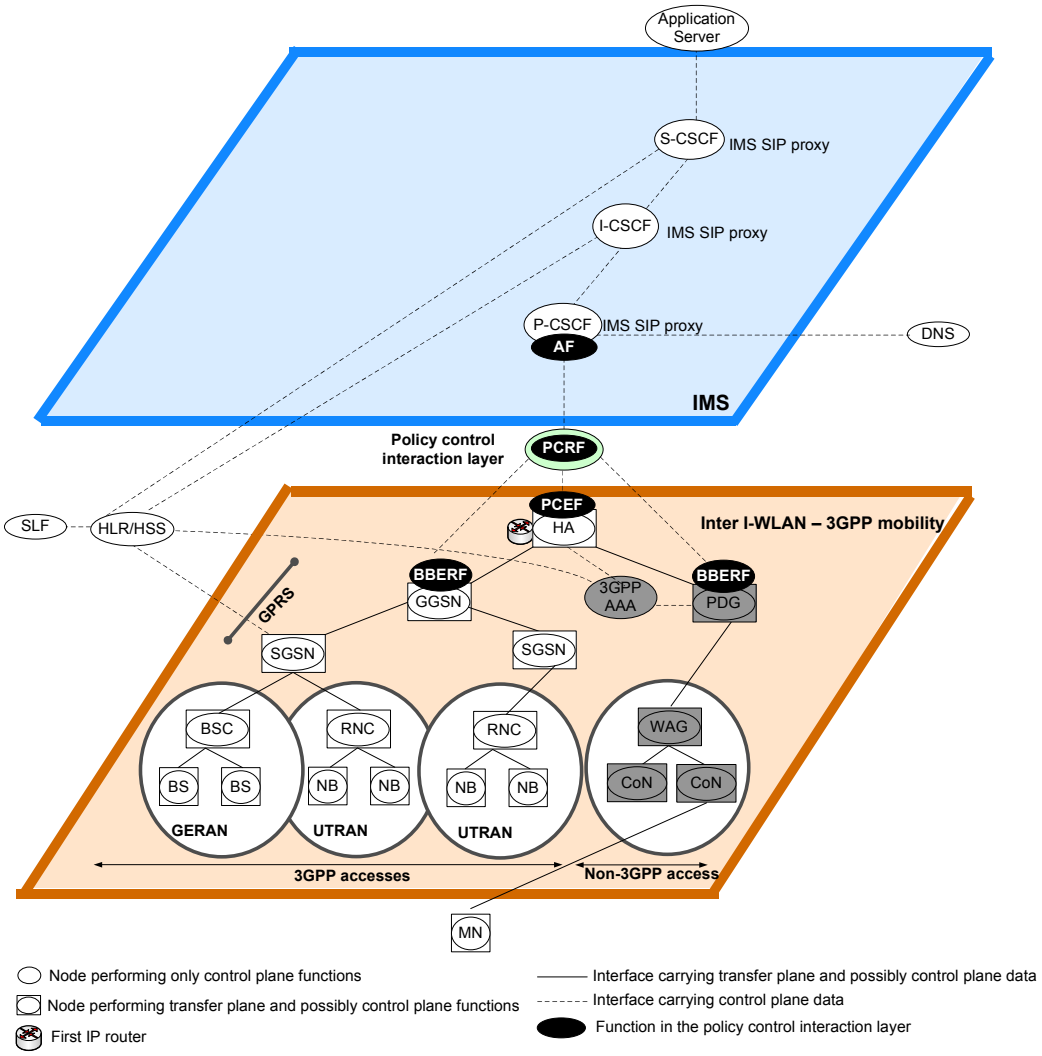


Figure 1.7: (Inter I-WLAN - 3GPP mobility)//PCC//IMS

1.3.5 WiMAX//PCC//IMS

Worldwide Interoperability for Microwave Access (WiMAX) is an IP-AN developed by WiMAX forum based on the IEEE 802.16e-2005 specification for the radio physical interface. WiMAX is now in its Release 1.5. The WiMAX network reference model [3] partitions the end-to-end WiMAX into a CSN (Connectivity Service Network) and an ASN (Access Service Network), as shown in figure 1.8.

The **CSN** includes the IP address allocation mechanisms, the first IP router, and the AAA server performing user authentication. The CSN acts as a **data anchor** for mobility between ASNs. It also acts as a **signalling anchor** if it receives mobility related signalling when the user moves between ASNs. This occurs when a protocol from the Mobile IP (MIP) [27] family is supported between the MN and the CSN.

The ASN provides authentication relay functions, stores security keys for each user, manages bearers (called service flow in WiMAX terminology), ensures route update, reachability, header compression and radio resource management functions. It comprises Connectivity Nodes and ASN Gateways. When the CSN does not act as a signalling and data anchor for mobility between ASN, to handle mobility, the ASN acts as a **signalling** and **data anchor** for mobility between ASN.

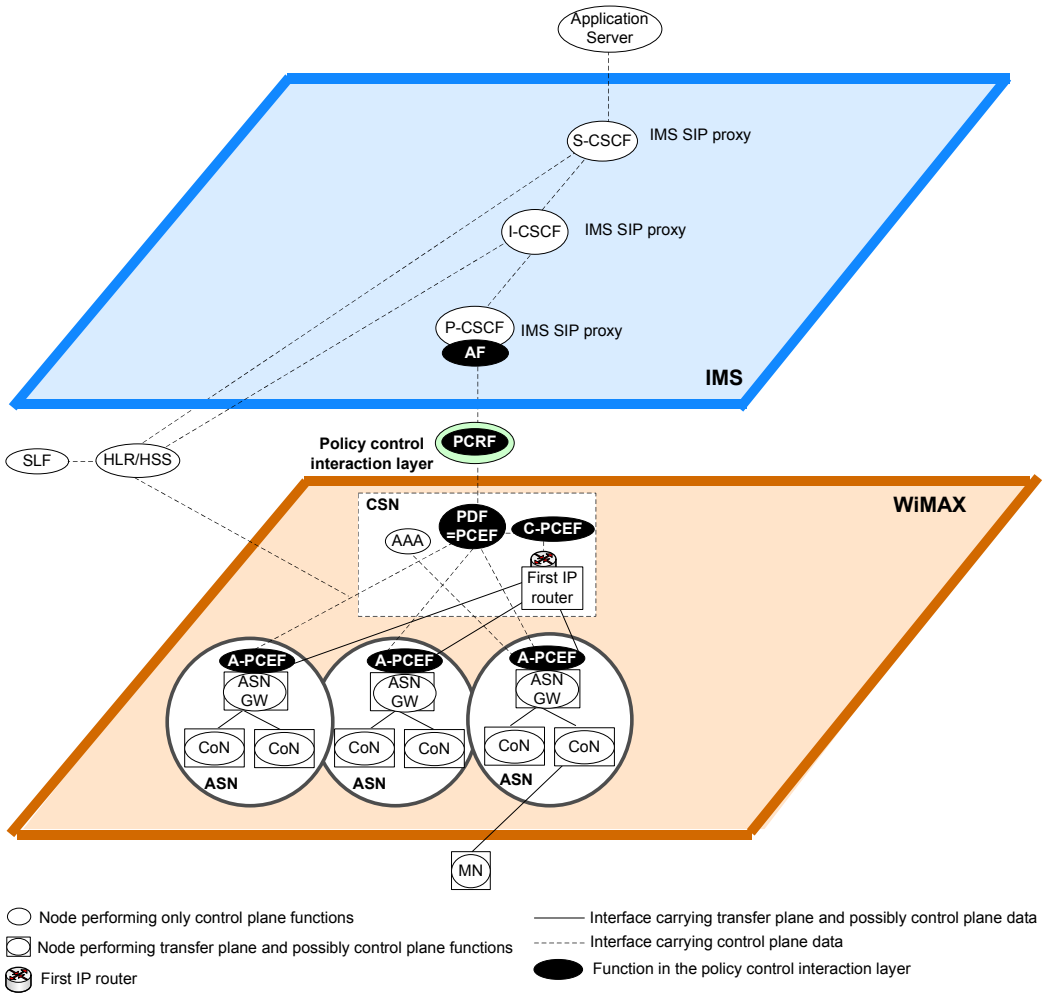


Figure 1.8: WiMAX//PCC//IMS

In the spring of 2007, WiMAX forum began the work of applying the 3GPP PCC interaction layer, defined by 3GPP, to WiMAX architecture. However, at that time, the considered 3GPP Release (Release 7), has not yet defined the BBERF and supposed that: (1) the first IP router is the bearer endpoint, and (2) the bearer endpoint does not change for a given MN whatever its mobility. These two elements are not fulfilled in WiMAX IP-AN, as the bearer endpoint is not in the first IP router, but in the ASN and changes during MN mobility.

For these reasons the WiMAX forum was constrained to modify the WiMAX architecture to make it interworking with the defined PCC Release 7 architecture. The modification consists of [28] introducing a node in WiMAX IP-AN that implements the 3GPP PCEF functions. This node, called PDF (policy distribution function), relays the policy rules to the CSN and the ASN.
The CSN enforces the received policy rules on the IP layer through a new defined enforcement function, called C-PCEF.

The ASN enforces the received policy rules on the bearers through a new defined enforcement function, called A-PCEF.

1.3.6 EPS//PCC//IMS

EPS (Evolved Packet System) is an IP-AN introduced by 3GPP in Release 8. It offers high data rates and network convergence. The high data rates are enabled mainly through the definition of a new radio access network called **LTE** (Long Term Evolution). The network convergence is provided by the definition of a new packet core network called **EPC** (Evolved Packet Core) connecting different types of radio access types (3GPP or non-3GPP (WiFi, WiMAX, ADSL, etc.)) (figure 1.9).

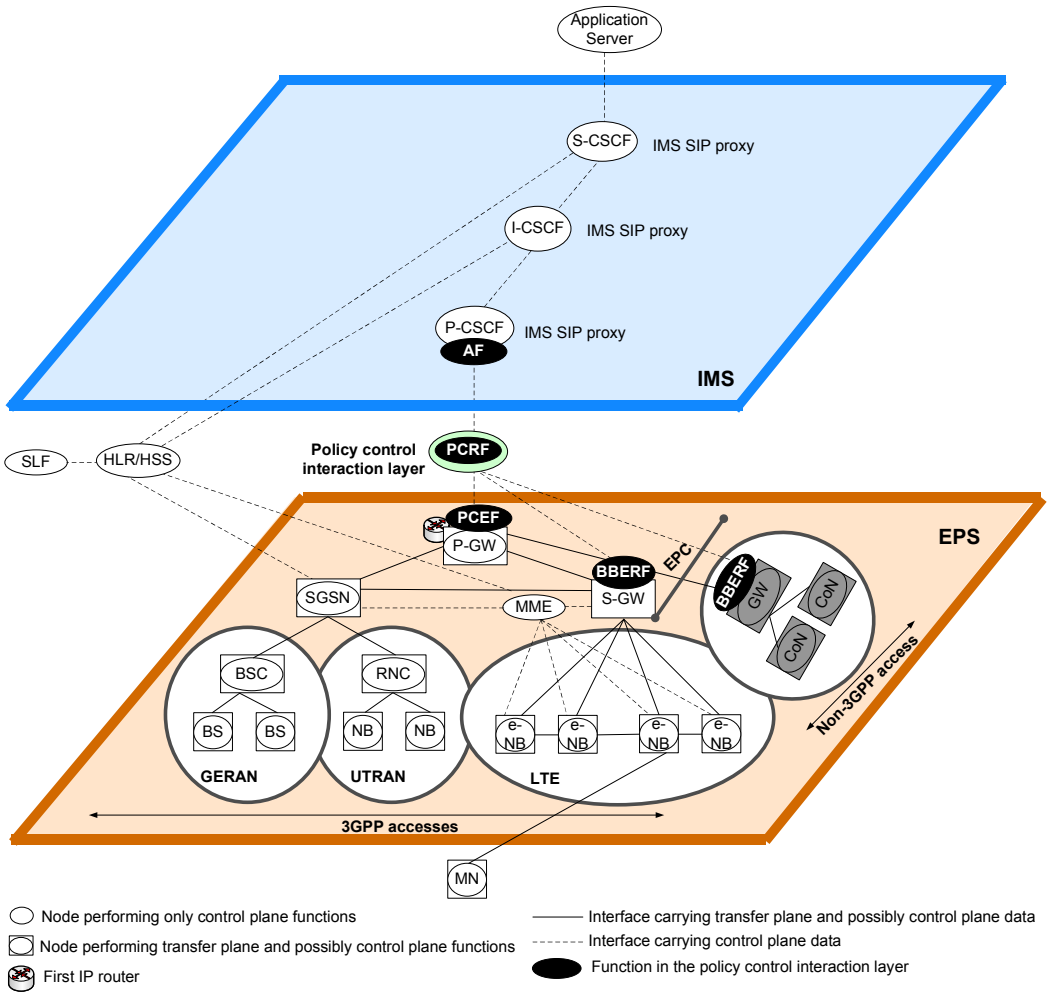


Figure 1.9: EPS//PCC//IMS

- **LTE** is considered as **flat** compared to UTRAN in UMTS, as it is only composed of Connectivity Nodes containing all the radio intelligence. Remember that UTRAN is composed of Connectivity Node controllers and Connectivity Nodes.
- **EPC** provides IP connectivity to users independently of the radio access they are using (3GPP or non-3GPP radio accesses (WiMAX, ADSL, etc.)) as well as mobility between radio accesses. It mainly introduces three nodes which are: the P-GW (Packet Data Network Gateway), the S-GW (Serving Gateway) and the MME (Mobility Management Entity) (figure 1.9).

- The **P-GW** is the first IP router. It can be assimilated to the GGSN in UMTS in terms of functions. It acts as a **signalling anchor** and **data anchor** for mobility between 3GPP accesses, or between 3GPP and non-3GPP accesses. Mobility related signalling is ensured through GTP [23]) a protocol from the Mobile IP (MIP) family.
- The **S-GW** performs most of the SGSN transfer plane functions. It is the **data anchor** for mobility between LTE Connectivity Nodes, and between LTE and UTRAN Connectivity Nodes.
- The **MME** gathers SGSN control plane functions and a few RNC control plane security functions. It is a **signalling anchor** for MN mobility between LTE Connectivity Nodes, and between LTE Connectivity Nodes and UTRAN.

The MME and the S-GW are two separate nodes. This separation aims at dimensioning each node based on a single criterion. Indeed, the traffic load due to mobility-related signalling does not have the same characteristics as the one due to the user data.

Regarding the interaction with PCC, the PCEF is located in the P-GW and enforces the policy rules on the IP layer and the BBERF is located in the S-GW and the other non-3GPP gateways and enforces the policy rules on the bearer level, if any.

1.4 Is IP-AN//PCC//IMS model ready for the new ecosystem?

This section discusses the readiness of the IP-AN//PCC//IMS model for the new ecosystem, focusing on the scalability and service control criteria. It also, when possible, formulates requirements enabling to overcome the identified problems.

Service control

IMS offers service control. However, it only applies to applications controlled by SIP. For the other applications, service control can be provided using the Application Functions (AF) of PCC or Deep Packet Inspection [29]. Nevertheless, these two last solutions are cost effective as they are specific to each application type. On the other hand, given the efforts spent on specifying IMS, I find it very interesting to extend IMS to all applications, and make them controlled by SIP. The state of the art encourages to take this direction: (1) recently, in [30], IMS has been extended to IPTV services, while these services are natively controlled by RTSP (Real Time Streaming Protocol). (2) [31, 32] show the interest of SIP for all applications to ensure QoS and security functions for them.

> *Requirement 1: the service control shall be provided to all applications in a cost effective manner. IMS is a service control solution already available for SIP native applications. It is proposed to extend it to all applications.*

Scalability

Scalability is one of the major criteria that has to be studied in case of exponential data growth. Firstly, some observations related to this criterion are made based on the IP-AN examples provided in the previous section. Afterwards, a deep analysis is performed.

Based on the examples given in the previous sections, it can be noted that:

- The IP-AN (UMTS, GAN, I-WLAN, inter I-WLAN - 3GPP mobility, EPS) model is **hierarchical. It is characterized by a centralized signalling and data anchor (first IP router) and different intermediate signalling and data anchors**. **This design was lead by mobility management constraints**. Indeed, the reason behind having many levels of signalling anchors is to hide the MN mobility from the higher levels, when it moves at the micro level (e.g. in UMTS, when the user moves between two NBs, it is not necessary to inform the GGSN about that). Also, the reason behind having many data anchors on different levels, is to offer mobility procedures with a good performance. Actually, mobility involving high level nodes require more steps, and thus more time for its execution.
- PCC, the IMS - IP-AN interaction layer for policy control, was first simple[7] with a single enforcement point, but gets more and more complex with additional interfaces and additional enforcement points in the IP-AN. This is due to the new IP-AN characteristics, consisting in that the bearer endpoint and the first IP router are two separate nodes. This complexity goes against IP-AN scalability, as more interfaces induce more CAPEX and OPEX costs.

Scalability is tied to economic aspects. It means that, in case of data growth, network investments due to node duplication have to remain profitable and operators revenues mustn't be impacted. A network must be scalable in many dimensions. Firstly, it must be the least sensitive to traffic growth or cope easily with it, without impacting operators revenues. Secondly, it must be flexible and accept additional functions without introducing complexity that could increase OPEX costs for example. Thirdly, it must be as independent as possible from the services, but provide the means for service control.

> *Requirement 2: the mobile network has to be scalable. It means that, in case of huge data growth, network investments shall remain profitable for operators.*

Undoubtedly, several indicators exist to measure network scalability. The following indicators are chosen to draw a first picture on a network scalability:

- The number of nodes on the transfer plane: these nodes are crossed by the transfer plane traffic, and may also be crossed by control plane traffic.
- The number of nodes on the control plane: these nodes are crossed by the control plane traffic only.
- The number of interfaces: these are the interfaces between nodes. They are crossed by the transfer plane, and possibly the control plane traffic.

The above elements are computed in table 1.1 for the IP-ANs examples described in section 1.3. For the number of nodes on the transfer plane, the MN is counted. For the number of nodes on the control plane, the IMS nodes are counted, even if they are the same for all of the examples. The HSS is counted. The SLF and the DNS are not taken into account. For the number of interfaces, interfaces with the PCRF are considered as they depend on the IP-AN. For the integrated IP-ANs (defined below), nodes and interfaces are counted on the integrated access part and not for the whole network.

IP-ANs can be divided into two categories: (1) Simple IP-ANs (GSM and UMTS, WiMAX) that involve single 3GPP access type. (2) Integrated IP-ANs (GAN, EPS, I-WLAN, Inter I-WLAN - 3GPP mobility) that integrate other access types (ADSL, WiFi, etc.) to the 3GPP access type

[7] in Release 5 and 7

(to the simple IP-ANs), in order to enlarge the 3GPP service coverage. Integrated IP-ANs may or may not provide mobility between the 3GPP access types and the integrated access types.

Different observations can be made: (1) Simple IP-ANs have a significant number of nodes and interfaces. (2) Integrated IP-ANs are more complex than the simple IP-ANs (e.g. GAN vs UMTS) in terms of additional nodes and interfaces. Moreover, they cause a higher data volume on the first IP router, that converges traffic from different access types. (3) The complexity of integrated IP-ANs increases when these ones enable the mobility between the 3GPP access types and the integrated access types ((Inter I-WLAN - 3GPP mobility) vs I-WLAN). This is due to the fact that mobility (e.g. in Inter I-WLAN - 3GPP mobility) is ensured by protocols from the Mobile IP family, and such protocols introduce signalling and data anchors. (4) As described before, EPS is flatter than UMTS as its radio access part (LTE) contains only one node (e-NB). In addition, the fact that the control plane functions and the transfer plane functions are separated in different nodes (MME and P-GW), can lead to conclude that EPS is more scalable than the other IP-ANs. Nevertheless, the additional interfaces caused by this separation and the high load of the P-GW (first IP router) should not be neglected when listing the causes of scalability issues.

Scalability criteria	**WiMAX**	**UMTS**	**GAN**	**EPS**	**I-WLAN**	**Inter I-WLAN - 3GPP mobility**
	//PCC//IMS					
Number of nodes on the transfer plane	4	5	5	4	4	5
Number of nodes on the control plane	8	5	6	6	6	6
Number of interfaces	12	11	14	14	12	15

Table 1.1: IP-AN//PCC//IMS model analysis

As already said, whatever the IP-AN type, simple or integrated, it is is characterized by a **centralized signalling and data anchor (first IP router), and different intermediate signalling and data anchors**. These anchors are solicited even if the user does not move. Moreover, they maintain a set of contexts per user, useful for traffic treatment. These contexts are mostly redundant. In each anchor, user packets are decapsulated/encapsulated and processed according to the stored contexts. Thus, the higher the number of nodes is, the higher the processing delay is. In addition, as the centralized first IP routers are responsible for a high number of users, they represent sensitive points of failure and may cause disruptions in a large area. The PCRF and P-CSCF have the same problems, as they are located behind the first IP router. All of these last limitations are agreed commonly, by the research community [33, 34, 35, 36, 37, 38].

To anticipate more and more subscribers in the future, **duplicating the first IP routers, the P-CSCFs and the PCRFs is not enough.** Indeed, as data traffic comes in bursts and is unpredictable, the first IP routers have to be over provisioned, causing more network costs and thus scalability issues. To overcome these shortcomings, a short term solution is to perform inter first IP router load balancing. This requires supplementary features in the network: (1) algorithms to calculate the load of the first IP routers, (2) a function responsible for selecting the least loaded first IP router, (3) a protocol to exchange the first IP routers load information, (4) a simple and optimal mobility procedure between the first IP routers (e.g. between GGSNs in UMTS or between PDG in EPS), aiming at moving users from the most loaded first IP routers to the least loaded first IP routers. This procedure is not defined today for first IP routers handling the same IP-AN type.

It can also be useful for the case of users moving at high speed. If inter-first IP router mobility is not implemented, when moving at high speed, the user will remain attached to the initial first IP router through which the call has been initiated, while he is connected to a Connectivity Node, which is far from the initial first IP router. This means that we have to configure the path between the Connectivity Node and the initial first IP router, leading to higher configuration and transport link costs.

> *Requirement 3: a simple and optimal mobility procedure between the first IP routers, handling the same IP-AN type (e.g. between GGSNs in UMTS) or different IP-AN types, has to be supported.*

For the mobility between the first IP routers, using data and signalling anchor-based protocols from the Mobile IP family [27], would take us back to the initial hierarchical and centralized model and increase scalability issues [38]. I have identified **ISC** (IMS Service Continuity) [39], the IMS-based mobility procedure introduced by 3GPP in Release 8 (begin 2009), as an **attractive solution**, to handle the required mobility procedure. Firstly, ISC only requires signalling (SIP) anchors (and not data and signalling anchors). Secondly, ISC enables more optimized data routing than Mobile IP [40]. Thirdly, ISC also handles the case of mobility between P-CSCFs. The case study targeted by 3GPP with ISC, is to provide a mobility solution between first IP routers handling different IP-AN types (e.g GGSN in UMTS and PDG in I-WLAN). However, nothing prevents us from using ISC also for mobility between first IP routers from the same IP-AN type.

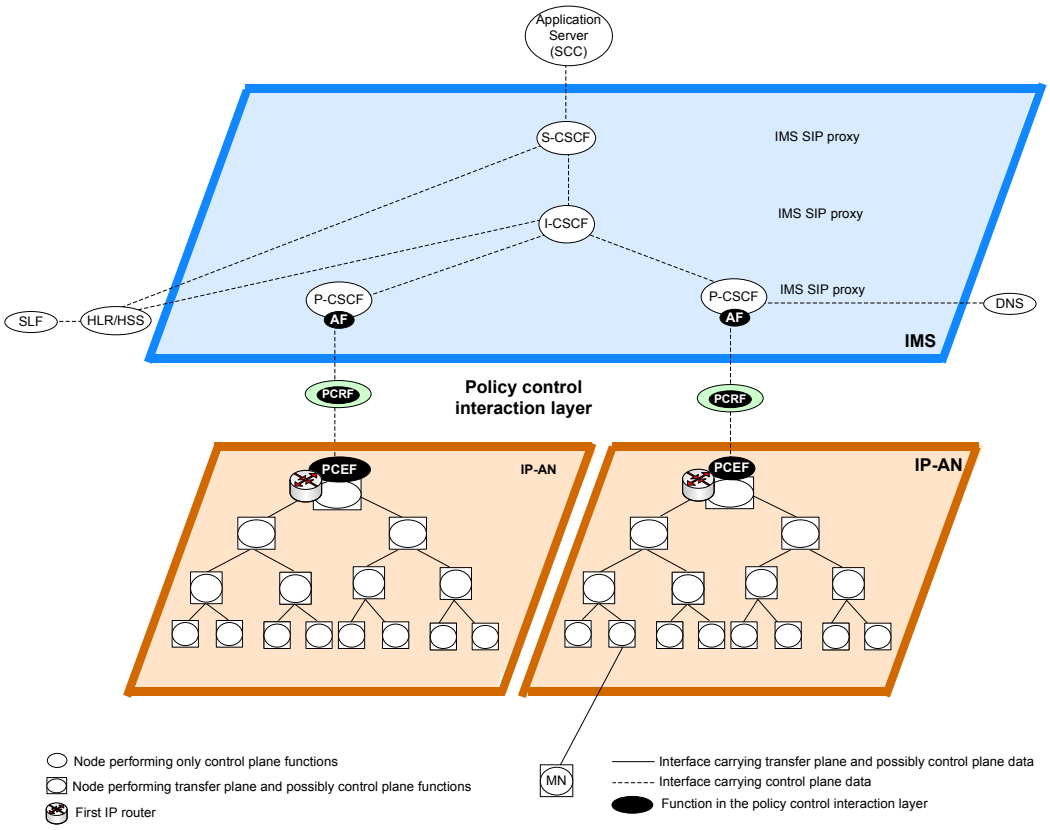


Figure 1.10: IMS Service Continuity (ISC)

As shown in section A.3, SIP has the capability to manage mobility. ISC relies on this capability, and in addition allows operators to control and customize mobility service. These last functions are performed using a SIP anchor implemented in an Application Server called Centralization and Continuity Application Server (SCC AS) (see figure 1.10).

As a conclusion, given the fact that ISC relies on IMS and is the most interesting mobility solution among the existing ones, in chapter 2, considerations will be given to further investigate the IP-AN//PCC//IMS model readiness for the ecosystem.

1.5 Service/application classification and impact of the transport protocol on mobility management

In the previous section, the IMS has been chosen as a solution to provide service control for all applications. As a number of applications are not natively controlled by SIP, there is a need to extend them and make them controlled by SIP. It was also decided in this chapter to consider ISC as a mobility solution.

Based on these assumptions, this section identifies two pertinent service types that will be dealt with in the next chapters.

- Services whose application(s) are transported over RTP/UDP and controlled by SIP. These services are shortly called **SIP native services** in the rest of the document. Table 1.2 gives examples of these services.
- Services whose application(s) are transported over SCTP and natively controlled by a protocol different from SIP (HTTP, RTSP, ...). These services are shortly called **non-SIP native services** in the rest of the document. Table 1.2 gives examples of these services. Their applications should be controlled by SIP.

Transport protocol on the transfer plane	**Control protocol on the control plane**	**Example**
-RTP/UDP -TCP -SCTP	-SIP -HTTP -RTSP -FTP	-voice (SIP native) -video (SIP native) -Real Media (1) (non-SIP native) -Windows Media (1) (non-SIP native) -HTTP streaming (Apple) (2) (non-SIP native) -WEB (non-SIP native) -FTP (non-SIP native) -File transfer between two endpoints within a SIP session (3) (non-SIP native)
Notes (1): A streaming application controlled by HTTP and transported over TCP [41, 42] (2): Apple application. Apple proposes to replace the conventional RTSP by HTTP (3): based on [43, 44]		

Table 1.2: Service types

The reason for associating the transport protocol to these service types is that the transport protocol impacts mobility management. Let us look how ISC, or more generally SIP-based mobility solutions, can be used for these applications depending on their transport protocol:

-Applications transported over RTP/UDP adapts to the change of MN IP address (due to mobility). SIP signalling is sent by the MN to the CN (Corresponding Node) to inform the CN about the IP address it should consider for the MN destination address.

-Applications transported over TCP are bound to the initial MN and CN IP addresses, and are disconnected following the MN IP address change. To avoid this, the IP address change shall be hidden from TCP. IP tunnels allow that, they are used on the transfer plane between the MN and the CN or between the MN and a data anchor node. SIP signalling can be sent to the CN/ signalling anchor to inform it about the new MN IP address [45, 46]. The signalling anchor informs the data anchor about the MN IP address, that should be considered for the IP tunnel.

-Applications transported over SCTP adapts to the change of MN IP address. SCTP is a connection oriented protocol similar to TCP (see more details in chapter 7). Thanks to its multihoming feature, it supports MN IP address change and do not need IP tunnels. SIP can be used to notify the CN/signalling anchor about the change of MN IP address, as proposed in [45, 46, 47].

For non-SIP native services, I choose to consider SCTP instead of TCP as these two protocols are similar, but SCTP does not need tunnels contrary to TCP, which avoids scalability issues.

1.6 Conclusion

This chapter was aimed at providing a first analysis of mobile networks readiness for the new telecommunication ecosystem, considering the scalability and service control criteria.

The scalability of a network depends on many factors, among them its organic architecture. Therefore, the first step to analyze mobile networks scalability, was to draw a model for their organic architectures. This model, noted as **IP-AN//PCC//IMS**, is constituted of: an IP access network (IP-AN) providing IP connectivity to users, IMS as a service control overlay network, and PCC as an IMS - IP-AN interaction layer for policy control. The IP-AN part of this model leverages different IP-AN examples: UMTS, GAN, I-WLAN, inter I-WLAN - 3GPP mobility, EPS.

It has been pointed out that the IP-AN model is led by mobility management constraints. It is hierarchical, characterized by a centralized signalling and data anchor (first IP router), and different intermediate signalling and data anchors. The IMS and PCC nodes are centralized too, as they are in the IP network, behind the IP-AN first IP router. In case of data growth, IP-AN nodes at all levels, PCC and IMS nodes should be duplicated, causing high network costs.

To face these issues, it has been concluded that, at least, a mobility procedure between the first IP routers handling or not the same IP-AN type (e.g between GGSNs in UMTS or between P-GWs in EPS) shall be supported. This procedure will enable to provide inter-first IP router load balancing and avoid their over provisioning. ISC, a 3GPP mobility procedure based on SIP and IMS, has been identified as an optimal solution allowing such a procedure.

Service control is already provided by the IMS, but it is restricted to SIP native services. To make IMS more profitable, it has been proposed in this chapter to extend it to all applications.

To go more in depth in the readiness study, the IP-AN//PCC//IMS model is going to be analyzed in the next chapter focusing on the QoS and service and network convergence criteria.

CHAPTER 2

Main network procedures in the IP-AN//PCC//IMS model

The last chapter has dealt with the readiness of the IP-AN//PCC//IMS model for the new telecommunication ecosystem, with regard to the scalability and the service control criteria. This chapter focuses on the QoS and service and network convergence criteria.

QoS is an important element on which operators shall bet, in order to attract users and distinguish their networks from others. Operators shall provide users with a QoS corresponding to their subscription and their requested services, in a cost effective way.

Global QoS indicators can be the performance to access the service, and the performance of the service once it is established.
The first indicator i.e. the performance to access the service, involves the paging procedure and/or the service access procedure.
The second indicator i.e. the performance of the service once it is established, involves the service access procedure and the mobility procedure. Indeed, during the service access procedure, a bearer reflecting a certain QoS, is allocated to the service. Moreover, mobility procedure may disturb the service delivery, if it causes packet losses and/or an inadequacy between the ongoing service and the new bearer on the target network.
For these reasons, the service access and mobility procedures are analyzed in this chapter. The paging procedure is left for further studies. As QoS is the focus of this chapter, the case of services requiring a guaranteed bandwidth, imposed by the user profile and/or the applications requirements, is considered.
The previous chapter has concluded that a mobility procedure is needed between the IP-Access Networks (IP-AN) first IP routers, to face the exponential traffic growth. It has selected the IMS Service Continuity (ISC) procedure, as an optimized procedure to fulfill this requirement within the IP-AN//PCC//IMS model. Therefore, ISC is considered in this chapter to study the mobility procedure.

In addition to QoS, service and network convergence are important for an operator as they enable to reduce costs. Service convergence means that the same service can be accessed from any IP-AN. It enables to share service platforms between different IP access networks instead of being dedicated to each IP access network, optimizing thus the service costs. Network convergence means that IP-ANs have the same network architecture (nodes, interfaces) and provide the same means (protocols, methods) to access network services, whatever the type of physical connectivity they support.

In the IP-AN//PCC//IMS model, service convergence is ensured thanks to the IMS. IP-ANs do not provide network convergence, otherwise they would have the same architecture. However, it is proposed in this chapter to determine to which measure these IP-ANs could be network convergent, by studying the protocols and means used for the registration/authentication phase of the service access procedure.

This chapter is organized as follows. Section 2.1 describes the service access procedure and analyses the network convergence criterion for the authentication/registration phase. It also details the service access procedure, its QoS problems, and provides the state of the art of the proposed solutions. Section 2.2 does the same as section 2.1, for the ISC mobility procedure. Finally, section 2.3 synthesizes the main problems and solutions for both procedures and formulates the requirements to be fulfilled by a network model, in order to be ready for the new ecosystem.

2.1 Service access procedure in the IP-AN//PCC//IMS model

This section describes the service access procedure, details its QoS problems and provides the state of the art of the proposed solutions. Two phases are necessary to access services in the IP-AN//PCC//IMS model. Phase 1 is related to the user registration/authentication. Phase 2 is related to the service establishment.

2.1.1 Phase 1: registration/authentication

The registration/authentication phase aims at checking and preparing the user to access IP-AN//PCC//IMS services. It involves 6 steps (named **ATH**) as shown in figure 2.1. Each step is in reality a set of messages.

The main steps are the registration/authentication to the IP-AN (ATH_1) and the registration/authentication to the IMS (ATH_5). As the IP-AN and the IMS are independent, and the IMS services are considered to be supplementary to IP-AN services, registration/authentication is performed separately to each of these two levels (IP-AN and IMS), based on different user identities (**IP-AN user ID** and **IMS user ID**). The other registration/authentication steps enable, among other things, to prepare ATH_1 and ATH_5.

In the following, the different registration/authentication steps are described based on [13], while giving the particularity of each IP-AN. Figure 2.1 depicts these steps as well as the contexts they create in the IMS, IP-AN and MN nodes, considering @IP1 as the MN IP address, @P-CSCF as the P-CSCF IP address and @S-CSCF as the S-CSCF IP address.

Section 2.1.1.7 summarizes the protocols and means employed to execute these (registration/authentication) steps in each IP-AN. It also analyzes to what extent each IP-AN supports service and network convergence.

2.1.1.1 Step ATH_0: layer 2 attachment to IP-AN

The Mobile Node (MN) attaches to the IP-AN at layer 2 level in order to have a physical connectivity.

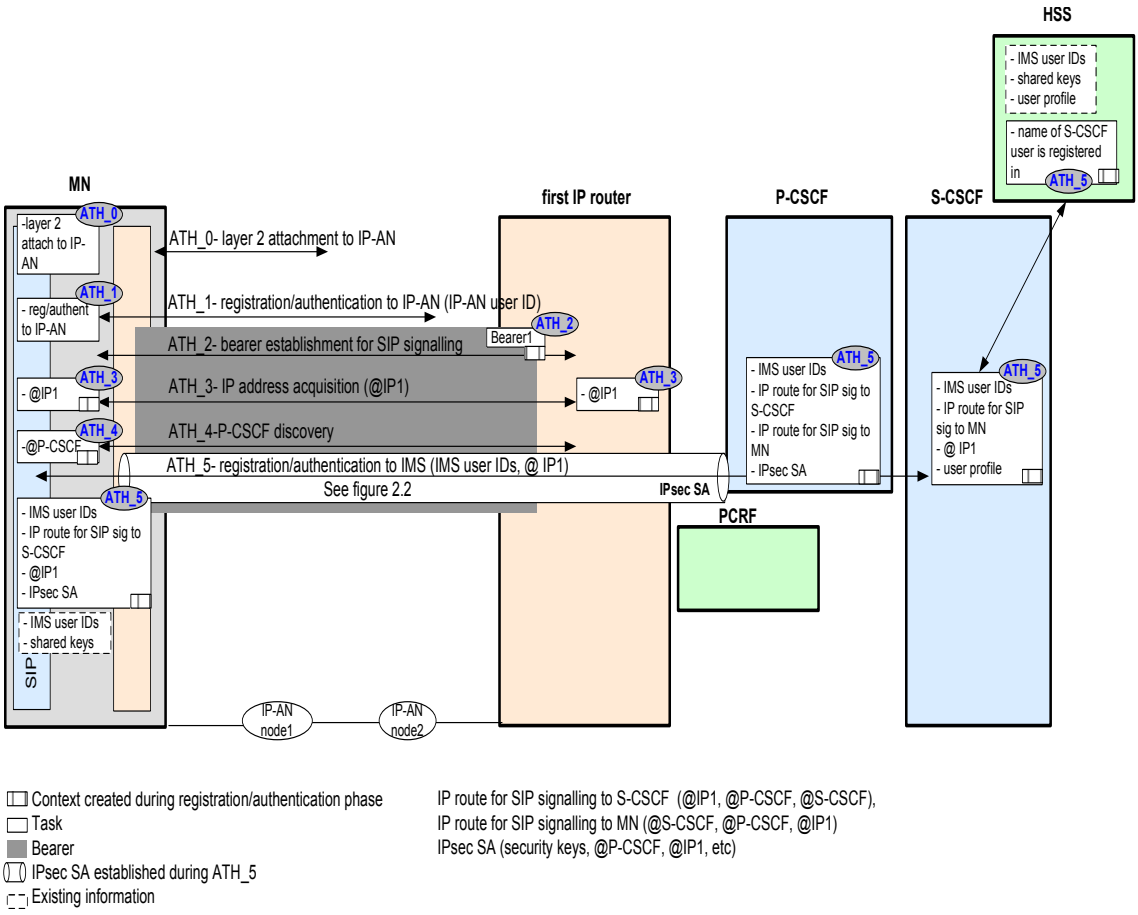


Figure 2.1: Phase 1: registration/authentication

2.1.1.2 Step ATH_1: registration/authentication to the IP-AN

This step consists in registering and authenticating the user in the IP-AN. Registration consists in communicating the user location to the IP-AN and authentication consists in checking the user subscription to IP-AN services based on its **IP-AN user ID**.

During user authentication, a **Security Association (SA)**[1] is built between the MN and an IP-AN node. It aims at ensuring the integrity and confidentiality of the user data, exchanged between the MN and the IP-AN.

AKA (Authentication and Key Agreement) [48] is used as an authentication method during this ATH_1 step for most of the IP-ANs: UMTS [49], EPS [29], I-WLAN [25] and WiMAX [3]. WiMAX, in addition to AKA, uses other methods. AKA enables to build the Security Association material (security keys) in the MN and another node in the network.

Generally, AKA is based on the user identities and on shared keys stored within the MN and a network database (HSS in our case). It is a challenge-response authentication method, where the user is challenged to provide a right response. If it does, it is authenticated.

[1] A set of information that describes a particular secure connection between one node and another. It includes ciphering and integrity keys.

Although the same authentication method (AKA) is used in UMTS, EPS, I-WLAN and WiMAX, these IP-ANs differ from the **protocol** employed to authenticate the user and to exchange the elements of the AKA method between the MN and the IP-AN. This protocol is Session Management for UMTS [50], EAP for I-WLAN [25] and WiMAX [3].

The IP-AN node terminating the SA and the layer on which the SA is applied, depend on the IP-AN. In UMTS, EPS and WiMAX, the SA is on layer 2. It is respectively between the MN and the RNC [51], between the MN and the eNB [29], and between the MN and the ASN GW [3]. In GAN [24] and I-WLAN [25], the SA is on the IP level and consists in an IPsec SA [52]. It is respectively between the MN and the GANC and between the MN and the PDG.

In UMTS, WiMAX and EPS, authentication/registration requests or any other requests are routed in the IP-AN hop by hop. On the contrary, in **I-WLAN**, the MN sends directly authentication/registration requests to the PDG (see section 1.3.3 for PDG definition). Indeed, the network between the Connectivity Node and the PDG may be not completely under the operator control. The MN needs thus to **discover the PDG IP address** before sending the authentication/registration requests.

In I-WLAN, contrary to the other IP-ANs, ATH_1 step enables also to allocate an IP address to the MN. ATH_3 step (see below) is thus performed at the same time as ATH_1, which saves time.

2.1.1.3 Step ATH_2: bearer establishment for SIP signalling

During this step, a bearer (bearer1) is established between the MN and the first IP router. This bearer will be used to transport SIP signalling sent and received by the MN beginning from ATH_5 step.

For I-WLAN, there is no explicit bearer establishment between the MN and the PDG. The bearer is configured locally in the PDG, based on local information, if any.

2.1.1.4 Step ATH_3: IP address acquisition

The MN asks for an IP address (@IP1) and configures itself with this address. After this step, it becomes able to communicate with the internet i.e. nodes external to the IP-AN.

Depending on the IP-AN, as shown hereafter, different protocols can be used for IP address acquisition. These protocols are equivalent, however when their related signalling flow enables to execute simultaneously other ATH steps (e.g. first and second protocol in the following), the global authentication/registration delay can be reduced. Protocols to perform ATH_3 can be:

- The protocol used for ATH_1 step (registration/authentication to the IP-AN), as performed in I-WLAN [53] using EAP/IPsec protocols.
- The protocol used for ATH_2 step (bearer establishment for SIP signalling), as in UMTS [49] using Session Management protocol.
- DHCP (IPv4 or IPv6) [54, 55]. This protocol is specified for UMTS [49], EPS [29] and WiMAX [3].
- Stateless IPv6 configuration [56]. This protocol is specified for UMTS [49] and EPS [29].

2.1.1.5 Step ATH_4: P-CSCF discovery

The MN discovers the P-CSCF IP address, which will allow it to execute ATH_5 step.

Depending on the IP-AN, as shown hereafter, different protocols can be used for P-CSCF discovery [13, 57]. These protocols are equivalent, however when their related signalling flow enable to execute simultaneously other ATH steps (e.g. first protocol in the following), the global authentication/registration delay can be reduced. Protocols to perform ATH_4 can be:

- The protocol used for ATH_2 (bearer establishment for SIP signalling), as in the case of UMTS using Session Management protocol [49].
- DHCPv4 [54] directly, or DHCPv4 with DNS [58, 59, 60]. This protocol is specified for UMTS, EPS, I-WLAN and WiMAX [13, 61].
- DHCPv6 [55] directly or DHCPv6 with DNS [55, 62]. This protocol is specified for UMTS, EPS, I-WLAN and WiMAX [13, 61].
- Using configuration information already available in the MN. This means is specified for UMTS, EPS, I-WLAN.

2.1.1.6 Step ATH_5: 3GPP registration/authentication to the IMS

The Registration/authentication to the IMS [63] consists in registering and authenticating the user in the IMS. Registration consists in communicating the user location (@IP1) to the IMS. Authentication consists in checking the user subscription to IMS services, based on its **IMS user identities** (**IMS user IDs**).

During user authentication, a **Security Association (SA)**[2] is built between the MN and the P-CSCF. It aims at ensuring the integrity and the confidentiality of SIP signalling exchanged between the MN and the P-CSCF. Practically and according to the 3GPP standard [63], IPsec [52] is thought as the best means to build this Security Association.

Similarly to ATH_1 step, the authentication method used in ATH_5 is **AKA**. **SIP** is used to perform ATH_5 and to transport the elements of AKA.

The MN initiates this procedure by sending a SIP REGISTER request to its home network through the P-CSCF discovered in step ATH_4. As there could be many S-CSCF within a home network, an appropriate S-CSCF responsible for the MN is selected by the I-CSCF and the HSS. Thus, during ATH_5 step, **the S-CSCF is determined and the IP route for SIP signalling between the MN and the S-CSCF is discovered** and transported to the MN, P-CSCF and S-CSCF within SIP headers. Subsequent SIP requests (e.g. SIP INVITE) follow the discovered route i.e. they are source-routed without need for further discovery operations.

The registration/authentication to the IMS (ATH_5) set **contexts** in the IMS and MN nodes, as shown in the figure 2.1. These contexts are:

- In the MN: IMS user identities, IP route for SIP signalling to S-CSCF (@IP1, @P-CSCF, @S-CSCF), @IP1, IPsec SA.

[2] A set of information that describes a particular secure connection between one equipment and another

- In the P-CSCF: IMS user identities, IP route for SIP signalling to S-CSCF (@IP1, @P-CSCF, @S-CSCF), IP route for SIP signalling to MN (@S-CSCF, @P-CSCF, @IP1), IPsec SA.
- In the S-CSCF: IMS user identities, IP route for SIP signalling to MN (@S-CSCF, @P-CSCF, @IP1), @IP1, user profile.
- In the HSS: name of S-CSCF user is registered in.

The IPsec SA context is defined with two databases as described in appendix B.

In the following, the detailed message flow for the step registration/authentication to the IMS (ATH_5) is provided (figure 2.2). It is useful to understand how the state of the art (page 47) optimizes this step.

3GPP ATH_5 is based on **two rounds of SIP REGISTER/SIP OK**. In the first round, the user is challenged to provide the response expected by the AKA method [63, 64], and the security and ciphering keys necessary for the Security Association are deduced. In the second round, the user is completely authenticated:

1. The MN sends to the P-CSCF an initial SIP REGISTER request containing its IMS user IDs and its current location (@IP1). The P-CSCF forwards this request to the I-CSCF, which asks the HSS to provide it with the name of the S-CSCF responsible for user registration/authentication. When the I-CSCF gets the S-CSCF name, it forwards it the SIP REGISTER request.
2. The S-CSCF downloads from the HSS a quintet corresponding to the received IMS user IDs. The quintet contains among other information: *random challenge*, *expected response*, *ciphering and integrity keys*. The *expected response* and the *integrity and ciphering keys* are calculated mainly based on the *challenge* and the keys shared between the MN and the HSS.
3. In order to authenticate the user IMS user ID, the S-CSCF rejects the initial REGISTER request by sending a SIP UNAUTHORIZED response containing the quintet information except the *expected response*. The P-CSCF removes the *integrity and ciphering keys* and forwards to the MN the SIP UNAUTHORIZED message containing the *random challenge*.
4. The MN calculates the *response* and the *integrity and ciphering keys* based on the *random challenge* and the shared keys stored in it. It then sends a second REGISTER request containing its IMS user IDs, its location (@IP1) and the calculated *response*.
5. When the S-CSCF receives *response*, it checks whether it is equal to the already stored *expected response*. If yes, the user is successfully authenticated. The S-CSCF then informs the HSS that the user is now registered. The HSS stores the S-CSCF name, the MN is registered to, and sends the user profile to the S-CSCF.
6. The S-CSCF sends SIP OK message to the MN via the P-CSCF.

In step 4 of the previous exchanges, the P-CSCF and the MN locally build the IPsec SA that is constituted of the: IP addresses, transport ports, integrity and encryption algorithms, *integrity and ciphering keys*.

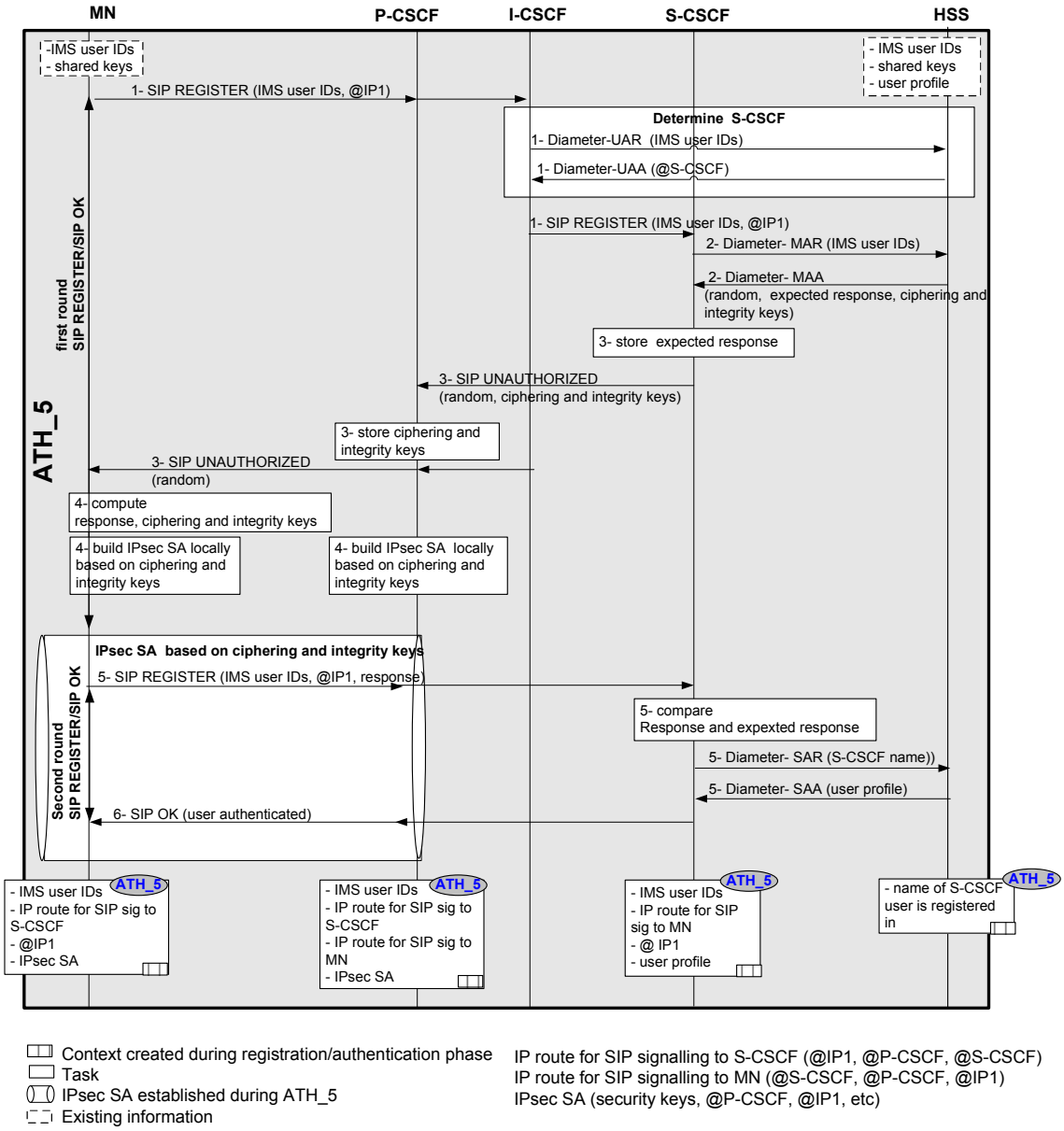


Figure 2.2: Registration/authentication to the IMS detailed message flow (3GPP ATH_5)

2.1.1.7 Summary on registration/authentication phase - analysis of service/network convergence criterion

This section summarizes for each IP-AN, the protocols used to perform the different registration/authentication steps (see table 2.1). It also analyzes to what extent the different IP-ANs support service and network convergence.

Requirement 4: service and network convergence shall be provided.

In the IP-AN//PCC//IMS model, service convergence is ensured thanks to the IMS. Regarding network convergence, some of the registration/authentication steps enable that, as shown in table 2.1:

- ATH_1 step enables somehow a network convergence since it is based on the same AKA method for all IP-ANs.
- ATH_2 step is specific to each IP-AN.
- ATH_3 and ATH_4 steps enable network convergence when they are based on the DHCP and DNS protocols.

Thus, the studied networks provide network convergence only regarding ATH_1, ATH_3 and ATH_4.

<table>
<tr><th></th><th>ATH_1: registration /authentication to IP-AN</th><th>ATH_2: bearer establishment for SIP signalling</th><th>ATH_3: IP address acquisition</th><th>ATH_4: P-CSCF discovery</th><th>ATH_5: registration /authentication to IMS</th></tr>
<tr><td rowspan="4">UMTS and EPS</td><td rowspan="4">Session Management protocol (1),
AKA method</td><td colspan="3">Session Management protocol and possibly DNS</td><td rowspan="4">SIP</td></tr>
<tr><td colspan="2">Session Management protocol</td><td>DHCP</td></tr>
<tr><td>Session Management protocol</td><td>DHCP or IPv6 stateful autoconfiguration</td><td>DHCP and possibly DNS</td></tr>
<tr><td>Session Management protocol</td><td colspan="2">DHCP and possibly DNS</td></tr>
<tr><td>I-WLAN</td><td colspan="3">EAP,
AKA method</td><td>DHCP and possibly DNS</td><td>SIP</td></tr>
<tr><td>WiMAX</td><td>EAP,
AKA method</td><td>WiMAX specific protocols</td><td>DHCP or MIP</td><td>DHCP and possibly DNS</td><td>SIP</td></tr>
<tr><td colspan="6">Notes
(1): Session Management protocol is specific to GPRS and EPC [49, 29].
ATH_0 step is not shown in this table. It is obviously specific to each IP-AN.</td></tr>
</table>

Table 2.1: Protocols and means to execute the different registration/authentication steps in each IP-AN

2.1.2 Phase 2: service establishment

The service establishment phase aims at establishing a service between the MN and the CN (Corresponding Node). A SIP session is used to negotiate, among other things, the service characteristics. Then, resources are established in the IP-AN according to the negotiated service.

For the sake of simplicity, SIP native services defined in section 1.5 are considered. The Session Description Protocol (`SDP`) [65] is used to describe these services. It is assumed that these services require a guaranteed bandwidth, imposed by the user profile and/or the applications requirements. A video call is considered as a typical service example. The `SDP` for video call contains the application names (voice, video), codecs and the `data flow descriptors`, as shown in table A.3.

In the following, the different service establishment steps (named **Estb**) are described. Figure 2.3 depicts these steps as well as the contexts they create. Each step is in reality a set of messages.

Figure 2.4 shows the end-to-end message flow for the service establishment phase, considering UMTS as an IP-AN example. Note that there is no document in the 3GPP standard giving a service establishment end-to-end message flow. Indeed, 3GPP has two types of documents (high level specifications and per-interface detailed specifications) without a clear interaction between them. To draw figures 2.3 and 2.4, [13, 14] are considered for the high level specifications and [49, 51, 57, 66, 67, 68, 69] are considered for the per-interface detailed specifications.

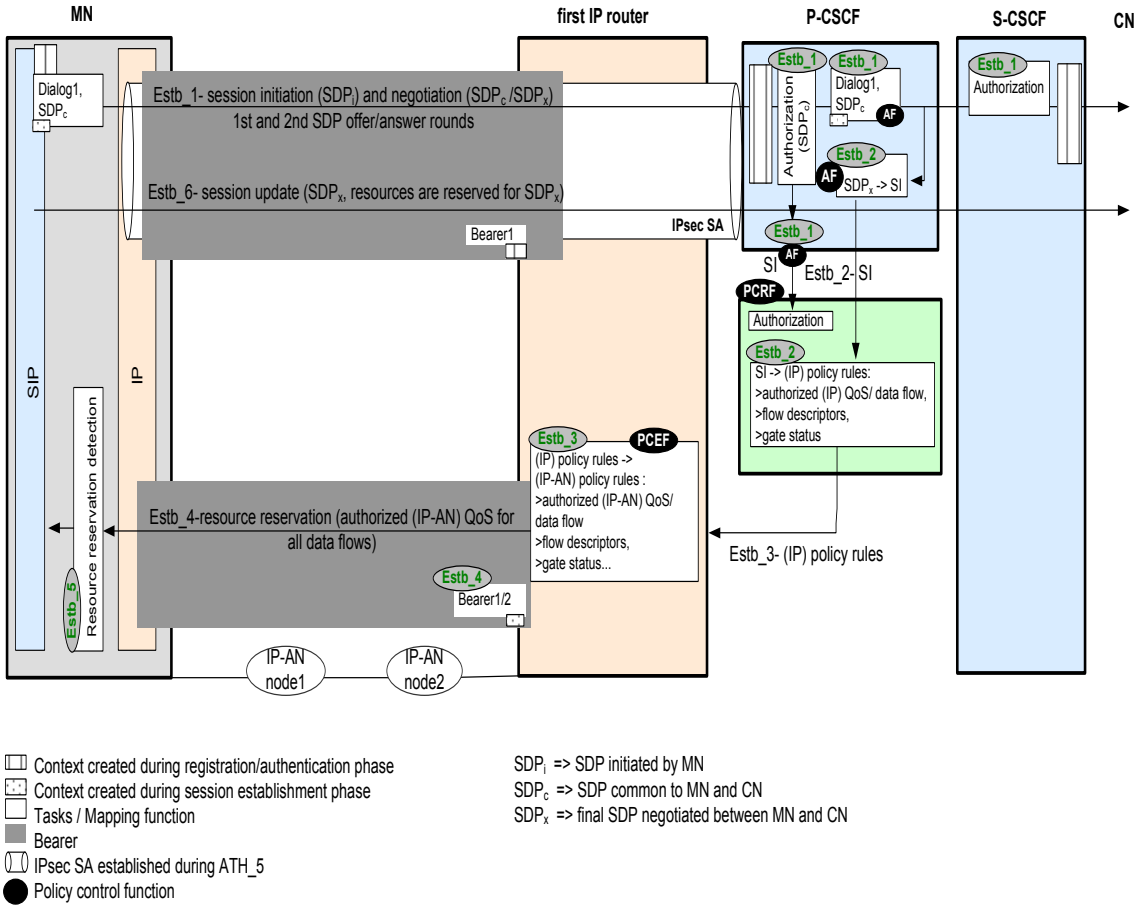


Figure 2.3: Phase 2: service establishment

2.1.2.1 Step Estb_1: session initiation and negotiation

During this step, the MN initiates a video call service towards the CN. The MN and the CN negotiate the service characteristics based on their common capabilities and preferences. Negotiation is performed through two SDP offer/answer (see section A.2 for SDP) rounds, after which the MN and the CN meet on a final SDP (SDP_x). The IMS SIP proxy nodes (P-CSCF and S-CSCF) and the policy control function (PCRF) intervene during this step to authorize or not the requested service.

To avoid call failure, the service is not established at this step and the CN is not informed of the incoming call (its phone does not ring) until the resource availability is checked on the IP-AN's CN and MN sides (i.e. until step Estb_4 for MN).

In greater detail, as shown in figure 2.4, this session initiation and negotiation step (Estb_1) is executed as follows:

- A first SDP offer/answer round is performed using the SIP INVITE/SIP SESSION PROGRESS messages.
  The MN sends a SIP INVITE message including a first SDP offer. This offer ($\texttt{SDP}_\texttt{i}$[3]) contains the list of applications (voice, video) and codecs per application, supported by the MN and proposed to the CN to be part of the service. This SDP offer indicates that resources are not reserved on the MN and CN sides, using QoS preconditions (see appendix C). The CN answers with a SIP SESSION PROGRESS message containing an SDP answer ($\texttt{SDP}_\texttt{c}$), which reflects the (common) applications and codecs the CN supports among those in $\texttt{SDP}_\texttt{i}$.
  During this first round, the P-CSCF, S-CSCF and PCRF authorize the service respectively according to the IP-AN capabilities[4], user profile and advanced information. To authorize the service, the PCRF needs to receive from the P-CSCF the Service Information (`SI`). It is the policy control function AF in the P-CSCF that deduces the `SI` from the $\texttt{SDP}_\texttt{c}$. `SI` is described in step Estb_2.
- The second `SDP` offer/answer round is performed, using the SIP PRACK/SIP OK messages. The MN and the CN meet on a single codec, among the ones in $\texttt{SDP}_\texttt{c}$, for each application, which gives $\texttt{SDP}_\texttt{x}$. This enables, in Estb_4, to only reserve resources corresponding to the codecs that will be really used by the MN and the CN for the call.

2.1.2.2 Step Estb_2: policy rules calculation for the IP level

After Estb_1 step, the AF deduces the Service Information (`SI`) from $\texttt{SDP}_\texttt{x}$ and relays it to the PCRF. The `SI` has a format independent of the IMS and `SDP`, as the PCRF is designed to interact with any service control overlay network and not with the IMS only.

The `SI` contains [68]:

- The name of the applications, within the service, willing to generate data flows (voice, video, etc).
- The codec of each application or any other information about the bandwidth required by the application.
- The `data flow descriptors` (source and destination (IP address+ transport port)).

When the PCRF receives the `SI`, it deduces the `(IP) policy rules`. To facilitate the PCRF sharing by many IP-AN, these rules are calculated in an IP-AN-independent form i.e. at the IP level.

The `(IP) policy rules` include:

- The `data flow descriptors`: source and destination (IP address+ transport port) of the data flows constituting the service.
- The `authorized (IP) QoS` that corresponds to the sum of the `authorized (IP) QoS per data flow`. The latter contains the maximum and guaranteed bandwidths, that can be requested on the IP-AN transfer plane for the data flow. These bandwidths are calculated

[3] voice(codec1, codec2), video(codec1, codec2)

[4] The MN has included in the SIP INVITE message the IP-AN type (e.g. "IEEE-802.11", "3GPP-GERAN", "3GPP-UTRAN-FDD") and the cell type (e.g. "utran-cell-id-3gpp", "i-wlan-node-id"). Based on that, the P-CSCF can authorize the service according to IP-AN capabilities

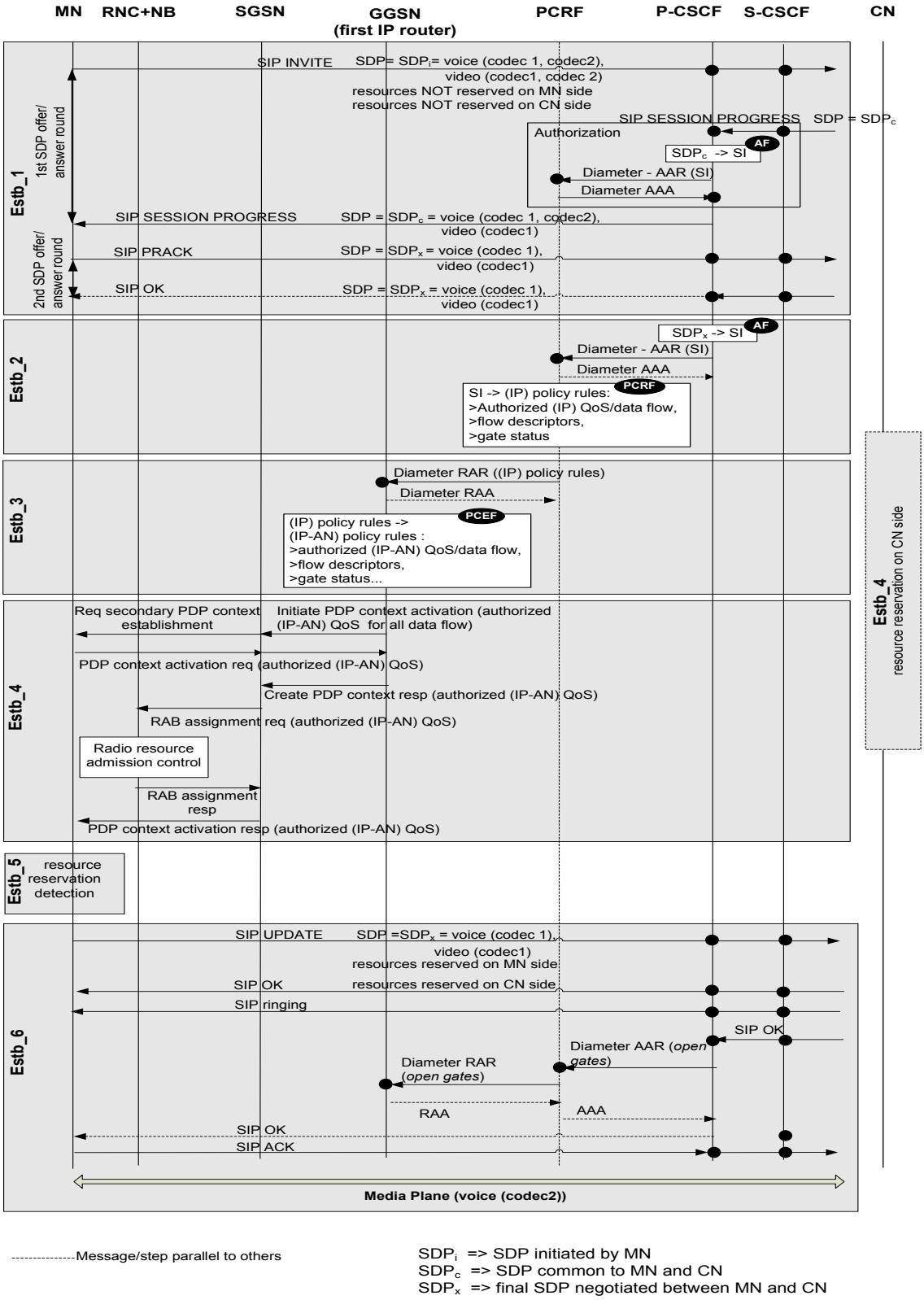


Figure 2.4: End-to-End message flow for service establishment (phase 2) considering UMTS as an IP-AN example

using specific algorithms within the PCRF, based on the codec or the bandwidth information provided by the `SI`.

- The **`events configuration`** that represents the events to be reported by the IP-AN to the PCRF with regard to the bearer supporting the data flows (e.g. bearer release).
- The **`gate status`** indicates, for each data flow, whether the related traffic is authorized or not to pass through the IP-AN.

Detailed messages for Estb_2 are given in figure 2.4.

2.1.2.3 Step Estb_3: policy rules calculation for the IP-AN level

The PCRF sends the `(IP) policy rules` to the PCEF (located within the GGSN for example), which deduces the `(IP-AN) policy rules`.

The **`(IP-AN) policy rules`** have the same elements as the `(IP) policy rules`, except for the `authorized (IP) QoS` that is converted to the **`authorized (IP-AN) QoS`** (a term understandable by the IP-AN).

Detailed messages for and Estb_3 are given in figure 2.4.

2.1.2.4 Step Estb_4: resource reservation

The PCEF enforces the `(IP-AN) policy rules`. It reserves on the IP-AN the resources corresponding to the `authorized (IP-AN) QoS`.

Depending on the IP-AN and on the `authorized (IP-AN) QoS`, this resource reservation step may correspond to the establishment of a second bearer (bearer2) or to the reconfiguration of the first bearer (bearer1) established for SIP signalling during ATH_2 step (see section 2.1.1). This means that we will have either two bearers where bearer1 is for SIP signalling and bearer2 is for data, or one bearer where bearer1 is for SIP signalling and data.

2.1.2.5 Step Estb_5: resource reservation detection

When the MN detects that resources are reserved on its side, it locally informs SIP about that.

2.1.2.6 Step Estb_6: session update

The SIP layer in the MN informs the CN that resources are reserved on its side for $\mathtt{SDP_x}$, using QoS preconditions (see appendix C). If the resources are also reserved on the CN side, the CN is alerted of the incoming call and a SIP RINGING message is sent to the MN. Finally, the service takes place.

The P-CSCF orders, via the PCRF, the PCEF to open the gates and allow the data flows defined by $\mathtt{SDP_x}$ to pass through the IP-AN.

The MN and the CN can thus exchange data at the end of this step.

Detailed messages for Estb_6 are given in figure 2.4.

2.1.3 Problems / state of the art / other possible solutions

The previous sections have described the **service access procedure, constituted of a registration/authentication phase and a service establishment phase**. This section identifies the performance problems of these phases, that are: a high access delay and a service non-adaptation to the IP-AN available resources. I detail each problem and give the state of the art of the proposed solutions or provide my own solutions.

2.1.3.1 High access delay

The registration/authentication and the service establishment phases induce a high access delay, that is mainly due to:

1. The high number of messages, tasks and mapping functions executed during these phases.
2. The fact that these phases involve centralized nodes (first IP router, P-CSCF, PCRF and S-CSCF) that may be overloaded by a high number of users.
3. The nature of the protocol (SIP) used to execute most of these steps. SIP is an application layer protocol with text-based messages containing a large number of headers and header parameters, including extensions and security-related information. This allowed the flexible characteristic of the IMS in orchestrating different applications and setting up different sessions with different requirements, however the drawback is the high time necessary to process SIP messages.
4. The independence between the IMS and the IP-AN, that generates a redundancy between some steps e.g. the step registration/authentication to the IP-AN (ATH_1) and the step registration/authentication to the IMS (ATH_5) or the step policy rules calculation for the IP level (Estb_2) and the step policy rules calculation for the IP-AN level (Estb_3).

Chapter 5 gives numerical results for the service establishment delay and proves the negative impact of centralized nodes on this delay.

Some solutions are proposed to reduce these delays as presented hereafter.

- **Mapping between the IP-AN and the IMS user IDs to reduce the delay of the step registration/authentication to the IMS (ATH_5)**

  Authors in [70] and [63] propose solutions for an optimized ATH_5 step, with less messages than the 3GPP ATH_5 step presented in section 2.1.1.6.

  The principles of the proposed solutions are: (1) an initial binding between the IP-AN user ID (e.g. IMSI in UMTS) and the IMS user IDs is set in the HSS network database and in the MN, (2) during ATH_5, the S-CSCF checks directly or indirectly that the user trying to register/authenticate using IMS user IDs, has an IP-AN user ID compliant with the binding in the HSS. [70] and [63] differ in the way this checking is performed during the ATH_5 step:

  - In [70], as shown in figure 2.5, the SGSN inserts in the ATH_5 SIP REGISTER message, natively containing the IMS user IDs, the IP-AN user ID of the user sending this message. Indeed, as the SGSN is involved in the step registration/authentication to the IP-AN (ATH_1), it is able to insert such information. Then, when the S-CSCF receives the SIP REGISTER message containing the IP-AN user ID and the IMS user IDs, it asks the HSS to check this mapping. If the result is positive, registration/authentication to the IMS is accomplished. Thus, there is no need to perform a second round of SIP REGISTER/SIP OK exchange as in the 3GPP ATH_5 (see figure 2.2).

– In [63], as shown in figure 2.6, during the step IP address acquisition (ATH_3), the GGSN adds in the HSS a mapping between the IP-AN user ID and the IP address (@IP1) acquired by the MN. This enables to deduce in the HSS a mapping between the IMS user IDs and @IP1, based on the already existing IMS user IDs - IP-AN user ID mapping. Then, in ATH_5, when the S-CSCF receives the SIP REGISTER message natively containing the IMS user ID and @IP1, it asks the HSS to check this mapping. If the result is positive, registration/authentication to the IMS is accomplished. Thus, there is no need to perform a second round of SIP REGISTER/SIP OK exchange as in the 3GPP ATH_5 (see figure 2.2).

These solutions bring a gain of 50% of signalling volume compared to the 3GPP ATH_5 step [70]. However, it presents a **major drawback** as it does not enable to establish the IPsec SA between the MN and the P-CSCF.

- **Parallel step execution**
  The service establishment phase is shown by figure 2.4. Its delay can be reduced by executing some steps in parallel. A first possibility is to begin the step resource establishment (Estb_4) at the same time as the step session initiation and negotiation (Estb_1), e.g. as soon as the first round of `SDP` offer/answer is performed. However, this may lead to reserve more resources in the IP-AN than needed.

  A second possibility is that, as proposed in [71], the CN sends the SIP RINGING message to the MN as soon as resource reservation is completed on its side (i.e. possibly before receiving the SIP UPDATE message from the MN informing that resources are reserved on the MN side). This possibility increases the probability of ghost calls (in case resources are not available on the MN side).

  As a conclusion, whatever the possibility for delay reduction, QoS will be badly impacted.

- **Less time for the step resource reservation (Estb_4)**
  The service establishment phase is shown by figure 2.4. Its delay can be reduced by compressing the time consumed by the step resource reservation (Estb_4). The only way to do that is to reduce the number of IP-AN node types, since the admission control task performed by each of these nodes consumes time.
  The patent [72], recently disclosed, brings this last idea; however, it does not develop an IP-AN with a reduced number of IP-AN node types. It considers the case of UMTS and EPS IP-ANs and supposes that only one node in these IP-ANs performs admission control and is involved in Estb_4. In addition, it claims that, in Estb_4, reconfiguring bearer1 with `authorized IP-AN QoS` and not establishing a new bearer (bearer2) from scratch helps to reduce Estb_4 delay. In my opinion, reconfiguration does not save a considerable amount of time, especially in the case of a high number of nodes in the IP-AN, since each of these nodes has to be reconfigured. In UMTS [51, 22], the procedure for bearer reconfiguration is almost the same as the procedure for bearer establishment from scratch.

2.1.3.2 Service non-adaptation to the IP-AN available resources

With SIP and IMS, services can be a mix of different application types (e.g. voice+video+file transfer). Moreover, for the same application, different codecs can be proposed.

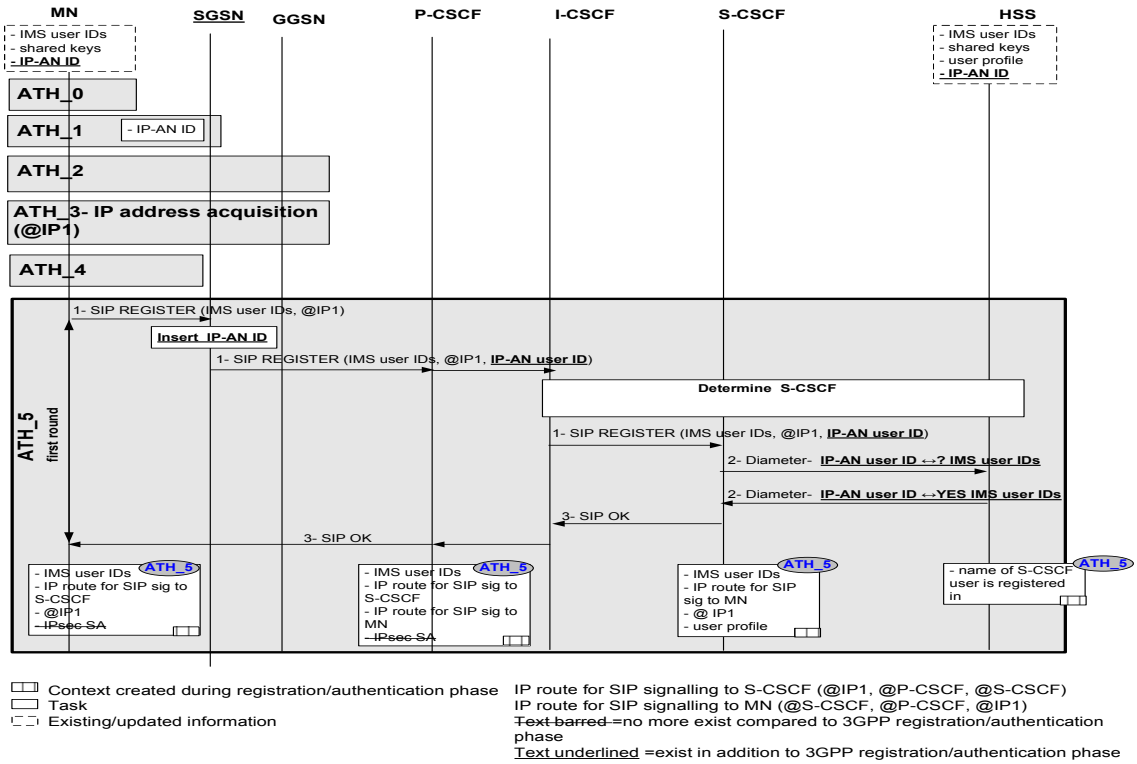


Figure 2.5: Registration/authentication to the IMS detailed message flow in [70])

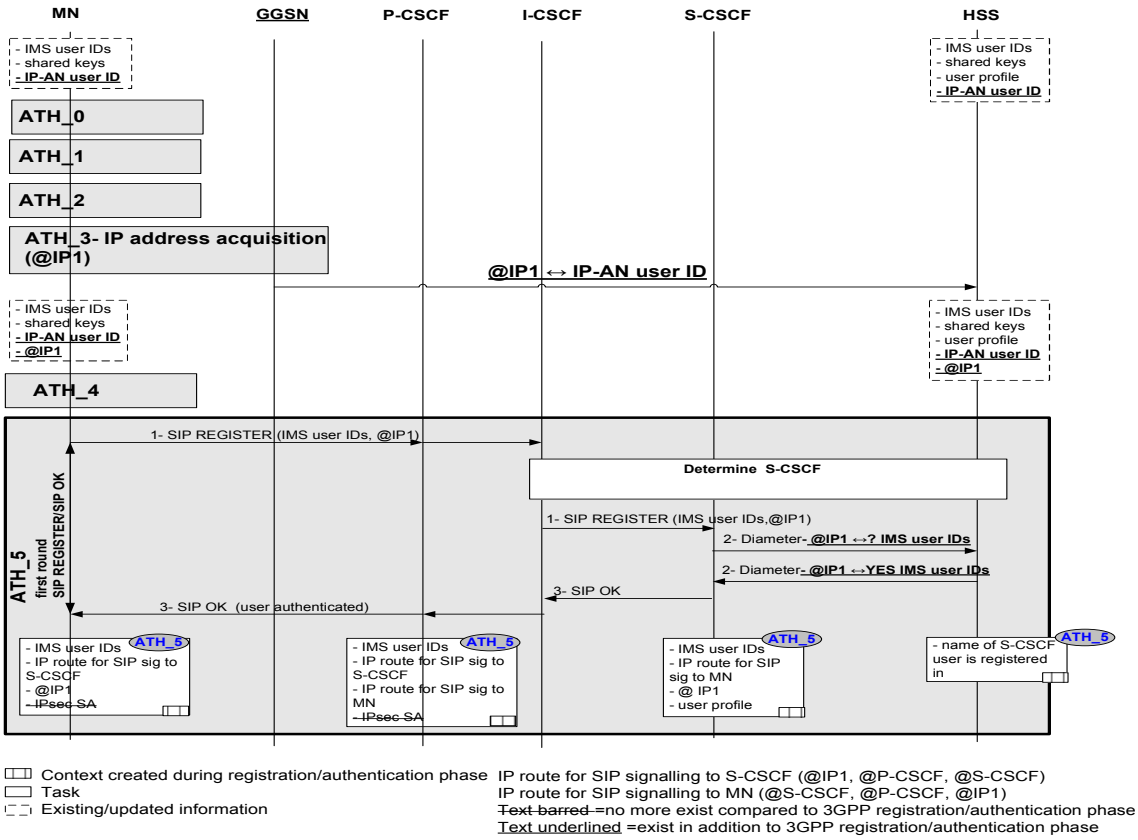


Figure 2.6: Registration/authentication to the IMS detailed message flow in [63]

Service adaptation shall be possible according to the network resource availability. When resources are partially available, it should be possible to downgrade the service by eliminating one or more applications from the service, or by choosing the least bitrate consuming codec for the different applications. When resources become available for the initial requested service, it should be possible to upgrade the service.

To perform service adaptation, one immediate solution is to establish one bearer per data flow/application based on the `authorized (IP-AN) QoS per data flow`[5]. In this case, if for a given bearer, the step resource reservation (Estb_4) fails because of resource problems, the MN can easily recognize in the step resource reservation detection (Estb_5) that the related application cannot be established because of resource problems. Thus, service adaptation can be easily performed in the step session update (Estb_6). Practically, this solution cannot be considered since it increases the number of active bearers and their related contexts within the different IP-AN nodes. This may impact IP-AN performances and increase its cost. The best way to go about it, is to: (1) try to establish one global bearer (bearer2), or reconfigure bearer1, for the sum of data flows constituting the service, based on the `authorized (IP-AN) QoS`; (2) then, if the requested resources are not entirely available, adapt the service. Based on this last assumption, solutions for service adaptation are presented hereafter. They are classified depending on whether the network supports bearer renegotiation or not.

- **Case 1: the network supports resource renegotiation**
  During the step resource reservation (Estb_4), a given IP-AN node may be not able to satisfy `authorized (IP-AN) QoS`. Resource renegotiation is the capability of this node to propose an alternate QoS (`modified (IP-AN) QoS`) and of the other nodes to meet on it. This capability is executed through Estb_4a step, shown in figures 2.8 and 2.7. When this capability is supported, there are two solutions to perform service adaptation, depending on whether it is initiated by the network or by the MN.

  - **Solution 1: service adaptation is initiated by the network**
    This solution is shown in figure 2.7. I propose that, when the PCEF receives the `modified (IP-AN) QoS` in Estb_4a, it determines the data flows set matching it, based on the `authorized (IP-AN) QoS per data flow` (already available through the step Estb_3). Then, accordingly, the PCEF performs a **reverse mapping function** to calculate, for the data flows set, the `modified (IP) policy rules` that it sends to the PCRF. The PCRF and AF also perform **reverse mapping functions** to deduce respectively the `modified SI` and $\mathtt{SDP_0}$. Finally, the P-CSCF updates the session (Estb_6) i.e. sending a SIP UPDATE message containing $\mathtt{SDP_0}$ towards the MN and the CN. The service is thus adapted.
  - **Solution 2: service adaptation is initiated by the MN**
    This solution is shown in figure 2.8. Based on $\mathtt{SDP_c}$, the MN, implementing the AF+PCRF+PCEF functions beforehand determines the `SI`, the `authorized (IP) QoS per data flow` and the `authorized (IP-AN) QoS per data flow`.
    Then, in Estb_4a, when the PCEF in the MN receives the `modified (IP-AN) QoS`, it determines, through an evolved resource reservation detection step (Estb_5), the data flows set matching with it, based on the `authorized (IP-AN) QoS per data flow`. Subsequently, as for solution 1, the PCEF+PCRF+AF in the MN perform **reverse mapping functions** to deduce the `modified (IP) QoS`, the `modified SI` and $\mathtt{SDP_0}$. In Estb_6 step, the MN updates the session i.e. sending a SIP UPDATE message containing $\mathtt{SDP_0}$ towards the CN. The service is thus adapted.

[5]This means that we would have many bearers2, each one for a data flow.

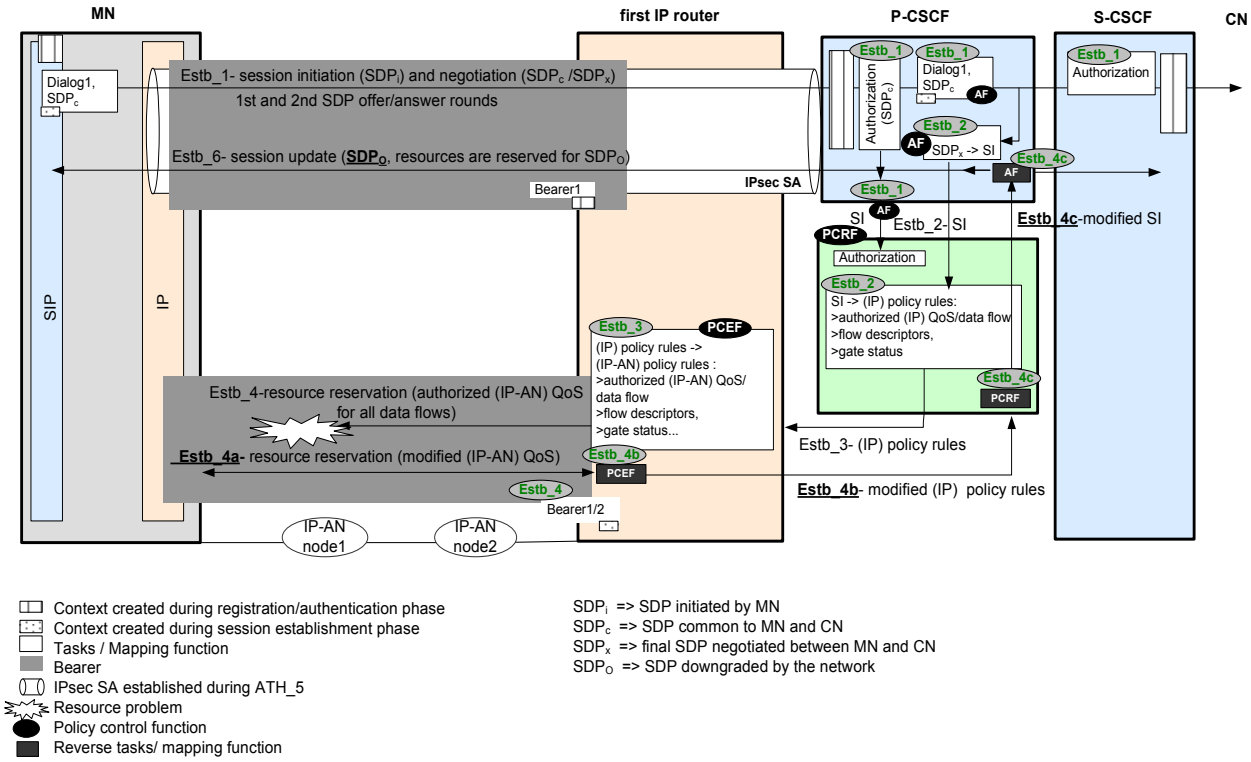


Figure 2.7: case 1/solution 1: the network supports resource renegotiation/ service adaptation is initiated by the network

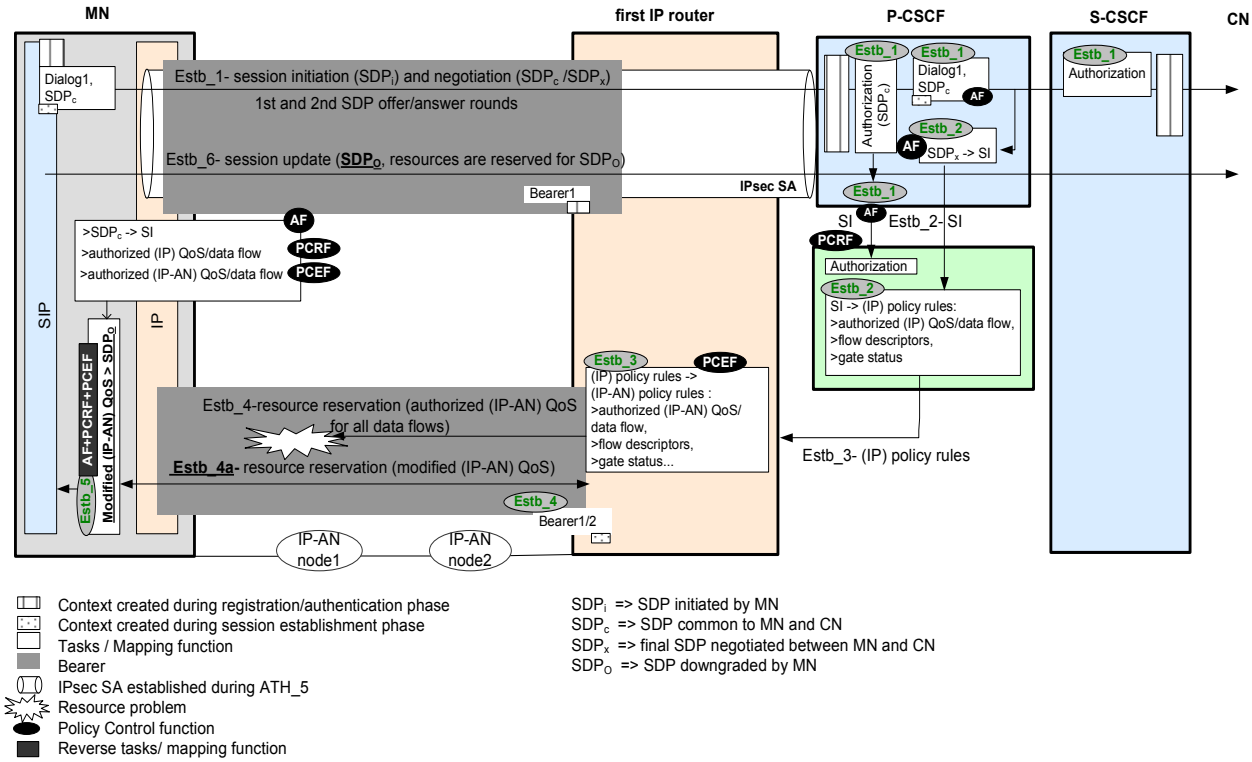


Figure 2.8: case 1/solution 2: the network supports resource renegotiation/ service adaptation is initiated by the MN

Solution 1 (initiated by the network) is more coherent than solution 2 (initiated by the MN), with the policy control principles, whose functions are located in the network[6]. Moreover, solution 1 does not require as much additional intelligence or as many functions as solution 2, but just reverse mapping functions. Despite this, solution 1 remains complex because of the need to support resource renegotiation by the network, and to specify new messages on the interfaces PCEF-PCRF and PCRF-AF. Note that, it is not planned to specify the resource renegotiation feature for LTE/EPC as mentioned in [29]; contrary to UMTS, where it has been specified since Release 4 [73].

- **Case 2: the network does not support resource renegotiation but a Resource Manager (RM) node**
  When the resource renegotiation capability is not supported, the only means to obtain the IP-AN resource information is to introduce a network node responsible for collecting this information from the different IP-AN nodes performing admission control [74]. This node is called **Resource Manager (RM)**. Resource information in the RM are assumed to be very precise and related to the end-to-end path, between the cell the MN is attached to, and the first IP router. Two solutions are possible to use the RM for service adaptation.

  - **Solution 1: service adaptation is implicitly performed based on policies received from the network, before the service establishment phase**
    This solution [75] requires network policy servers connected to the RM. When the policy servers detect that resources are temporally unavailable in the network, they order the MNs to reduce the requirements of their future service establishment requests (e.g. the number and the type of applications).
  - **Solution 2: service adaptation is performed during the service establishment phase**
    This solution is inspired from [76] that suggests to link the RM to the policy control function, the PCRF. During the step `(IP) policy rules` calculation (Estb_2) (refer to figure 2.3 to understand this solution), based on the resource information received from the RM, the PCRF compares the `authorized (IP) QoS` with the resources available on the end-to-end path on which the bearer is going to be established. If they are not matching, the PCRF deduces a `modified (IP) QoS` and the corresponding `modified (IP) policy rules`. The latter are sent to: the P-CSCF that deduces the `modified SI` and the corresponding $\mathtt{SDP_0}$, and to the PCEF that deduces the `modified (IP-AN) policy rules` and establishes resources accordingly. Finally, the P-CSCF sends the $\mathtt{SDP_0}$ to the MN.

  Solution 1 and solution 2 are both complex as they require additional nodes and interfaces. Solution 1 is difficult to apply if we need to perform a precise and a customized service adaptation per MN. Indeed, this would require specific policies for each MN, without knowing what kind of service it is going to launch.

- **Comparison between case 1 supporting resource renegotiation and case 2 introducing a Resource Manager (RM)**
  Case 1 and case 2 solve the problem of service non-adaptation; however each of them has some drawbacks. Case 1 introduces complexity and increases the service establishment delay, due to the resource renegotiation step (Estb_4a) in which the numerous IP-AN nodes should meet on a common `modified (IP-AN) QoS`. In case 2, the RM shall get resource information from the

[6] In reality, policy control could have been located in the MN, but this option was not retained by 3GPP because, among other reasons, this would have required a high number of updates from the network to the MN concerning, for example, the algorithms necessary for building the policy rules.

numerous IP-AN nodes performing admission control (for example in UMTS: GGSN, SGSN, RNC, NB). This requires the definition of new interfaces and procedures between each of the IP-AN nodes and the RM, causing a huge standardization effort. An additional standardization effort is also needed in case 2 to define a uniform resource information format allowing its exploitation (e.g. decide whether resources are available or not). Indeed, resource information is specific to each node and manufacturer and depends on node internal admission control algorithms. Note that during LTE standardization within 3GPP, Resource Manager-based solutions have been largely debated but finally not retained because of their complexity.

2.2 Mobility procedure during services in the IP-AN//PCC//IMS model

Chapter 1 has concluded that a mobility procedure is needed between the first IP routers to perform inter first IP router load balancing. It has selected the IMS Service Continuity (ISC) procedure as the most optimized procedure to fulfill this requirement for the IP-AN//PCC//IMS model. Therefore, ISC is considered in this section for the mobility procedure.

This section describes the ISC mobility procedure, details its QoS problems and provides the state of the art of proposed solutions.

2.2.1 Description of ISC mobility procedure

As explained in section 1.4, in the IMS Service Continuity (ISC) mobility procedure [39], mobility is executed by SIP and controlled by an Application Server interacting with IMS, called Service Centralization and Continuity Application Server (**SCC AS**).

To **control mobility**, the SCC AS inserts itself on the signalling path between the MN and the CN from the initial service establishment through the source IP-AN (IP-AN1): it terminates the SIP dialog (dialog1 on figure 2.9) initiated by the MN and establishes a second SIP dialog (dialog2 on figure 2.9) with the CN[7]. Then, when the MN initiates a mobility to a target IP-AN (IP-AN2), the SCC AS first checks whether the MN mobility request is compliant with the home operator policies (e.g. forbidden target networks, priority of target networks, etc). If yes, it coordinates the SIP signalling exchanged over the two SIP dialogs in order to inform the CN about the new MN location on IP-AN2.

In ISC, **mobility is decided and initiated by the MN** based on a set of criteria such as radio conditions, user preferences and home operator policies sent through configuration messages from the SCC AS to the MN.

As it can be noted from figure 2.9, **during the ISC mobility procedure, user-related contexts are set in the IP-AN, PCRF and IMS nodes (S-CSCF, P-CSCF2, PCRF2, first IP router2 and MN) so that user related traffic can be handled in IP-AN2**. These contexts are set as if a new service access procedure occurred through target IP-AN2.

ISC mobility procedure to IP-AN2 is executed in three phases through IP-AN2, as shown in figure 2.9. Note that there is no 3GPP specification giving the end-to-end message flow for this procedure: [39] gives the high level message flow and [77] gives the messages exchanged between the MN and the SCC AS:

[7]with this behavior, the SCC AS acts a **B2BUA** (Back-to-Back User Agent). See section A.1.1 for more information about B2BUA

- **Phase 1: registration/authentication through IP-AN2**
  The MN performs registration/authentication through IP-AN2. This phase is the same as phase 1 described for the service access procedure in section 2.1.1. It enables to mainly register and authenticate the user to IP-AN2, and to the IMS with regard to its new location.

- **Phase 2: service establishment on IP-AN2**
  This phase aims at authorizing the service in IMS through IP-AN2, calculating the policy rules and establishing the corresponding resources in IP-AN2. This phase is almost the same as phase 2 described for the service access procedure in section 2.1.2. Messages related to the step session initiation and negotiation (Estb_1) are not exchanged with the CN, but with the SCC AS, as the aim here is not to negotiate the service with the CN. In Estb_1, a SIP dialog (dialog3) is created with the SCC AS through IP-AN2.

- **Phase 3: updating the session with regard to the new MN IP address acquired on IP-AN2**
  This phase overlaps with phase 2 and consists in using SIP signalling to inform the CN about the new MN address (@IP2), acquired during phase 1-ATH_3 through IP-AN2.
  In phase 2-Estb_6, when the MN sends a SIP UPDATE message to indicate that resources are reserved in IP-AN2 and containing @IP2, the SCC AS intercepts this message and sends a SIP Re-INVITE message (similarly to the procedure indicated in section A.3) to the CN to indicate @IP2. Thus, the CN can send data flows to this address through IP-AN2.

2.2.2 Problems / state of the art / other possible solutions

The previous section has described the ISC mobility procedure. This section identifies the ISC mobility procedure performance problems, that are: the incompatibility with load-based handovers, the high handover delay and the service non-adaptation to the IP-AN available resources. In the following, I detail each problem and give for each one the state of the art of the proposed solutions or provide my own solutions.

2.2.2.1 Incompatibility with load-based handovers

Load-based handovers are profitable for operators as they allow them to use efficiently their networks while offering the best QoS to their subscribers. A simple example is to use these handovers to perform inter-IP-AN load balancing, by moving users from a very loaded IP-AN to a lesser loaded IP-AN.

ISC supposes that mobility procedure is always initiated and decided by the MN. Therefore, to support load-based handovers in ISC, load information should be sent to all MNs so that they can initiate a mobility accordingly. This solution may require a Resource Manger RM node, as introduced in section 2.1.3, to extract the load information from the IP-AN nodes and send it to MNs. It imposes that the MNs are able to exploit load information and take appropriate decisions. Moreover, as load information is dynamic, sending it to all MNs would induce a high amount of signalling. For these reasons, this solution is not viable.

To avoid the drawbacks of the previous solution, [74] proposes another solution where the load-based handover decision is taken by the network and sent to the MNs, so that they can initiate a mobility. This solution is based on a new node, called Mobility Manager, that receives from the RM the resource information and from the different MNs the radio signal strengths measured on the different neighboring cells.

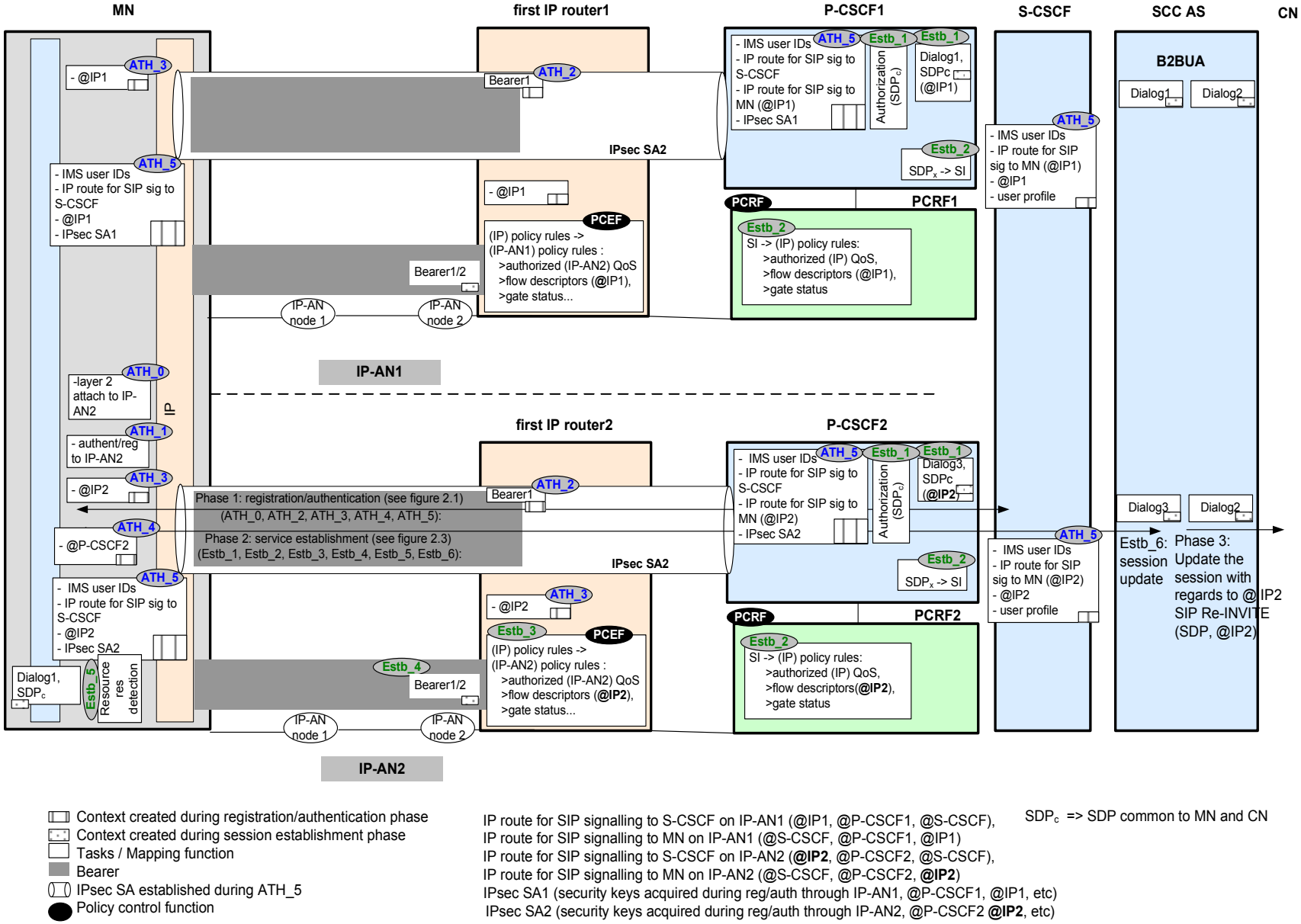


Figure 2.9: ISC mobility procedure

In case of overload on a given IP-AN, the Mobility Manager first selects the users to move from that IP-AN. Then, it selects for each user the least loaded (target) IP-AN and the (target) cell in that IP-AN the user shall attach to. The target cell is selected based on load information and on the feasibility, from a radio point of view, for the user to attach to it. Target IP-AN and target cell are sent by the Mobility Manager to the MN within a handover order.

In case of coverage loss detection for a given user, the Mobility Manager first selects the least loaded (target) IP-AN and the (target) cell in that IP-AN the user shall attach to. Target IP-AN and target cell are sent to the MN within a handover order.

This solution is complex as it requires new nodes (the RM and the Mobility Manager) and interfaces. Moreover, it worsens the handover delay problem (see next section). [74] briefly admits this last drawback.

2.2.2.2 High handover delay and service non-adaptation to the IP-AN available resources

The ISC mobility procedure involves almost the same phases as the service access procedure. Therefore, it has almost the same kinds of problems: high handover delay, service non-adaptation to the IP-AN available resources.

In section 1.4, ISC has been chosen to execute mobility between first IP routers. When these first IP routers handle the same IP-AN type, the MN performs mobility between cells having small overlapping zones, instead of cells having large overlapping zones as it can the case of mobility between routers from different IP-AN types.

The case of cells with small overlapping zones is the most restricting one. It results in most cases into (**hard handover**) scenarios. Therefore, it is very important to have a handover with a reduced delay as the MN may lose IP-AN1 coverage while it is executing ISC mobility procedure over IP-AN2 (see figure 2.10). A high handover delay would heavily impact user experience as it would cause packet dropping for ongoing applications. Chapter 6 provides measurements for this delay considering a simplified version of ISC procedure.

The state of the art provides solutions dealing with the high handover delay problem, considering **SIP-based mobility procedure** or **MIP-based mobility procedure**. For the service non-adaptation problem, no solutions are provided in a mobility context.

[78] treats the handover problem for the **MIP-based mobility procedure** and claims that the proposed solutions also apply for the the **SIP-based mobility procedure**. The analysis of these solutions proves the contrary, as shown in the appendix D.

Solution 1 hereafter is based on [79], it is provided for **SIP-based mobility procedure**. Solution 2 hereafter is proposed by myself for the ISC mobility procedure.

Solution 1: transfer of partial ATH_5 and partial Estb_1 contexts after handover to IP-AN2

SIP-based mobility procedure is quite similar to the ISC mobility procedure shown in figure 2.9, but does not require an SCC Application Server. It includes the same phase 1 and phase 2 as ISC. Phase 3 is slightly different in the fact that the SIP Re-INVITE message updating the MN IP address is sent directly from the MN to the CN, and not from the SCC AS to the CN.

Reference [79] optimizes the SIP-based mobility procedure, mainly the step registration/authentication to the IMS (ATH_5) and the step session initiation and negotiation (Estb_1). Instead of executing these steps through IP-AN2 as performed in the SIP-based mobility proce-

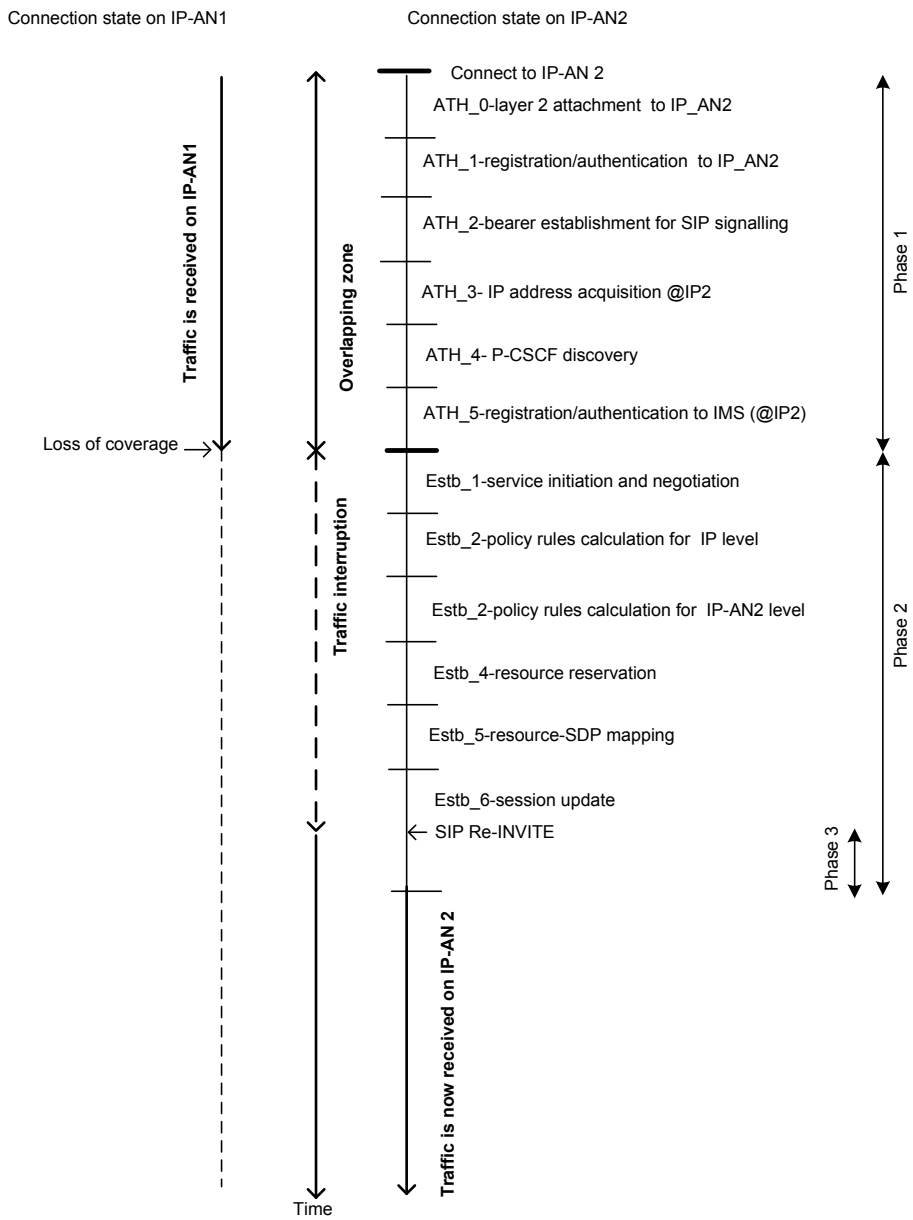


Figure 2.10: Timing diagram for ISC mobility procedure

dure, it proposes to transfer a part of their related contexts from P-CSCF1 to P-CSCF2, once the MN has performed a handover to IP-AN2.

The whole mobility procedure seems to be executed as follows: the MN attaches to IP-AN2 (ATH_0), registers/authenticates to IP-AN2 (ATH_1); establishes a bearer for SIP signalling on IP-AN2 (ATH_2); acquires an IP address on IP-AN2 (ATH_3); discovers the P-CSCF2 (ATH_4); **asks for partial ATH_5 and partial Estb_1 contexts transfer**; reserves resources in IP-AN2 (Estb_4); sends a SIP Re-INVITE message to the CN to update the MN IP address (@IP2).

The procedure by which the MN asks for the partial ATH_5 and partial Estb_1 contexts transfer is as follows (please refer to figure 2.9 for the understanding of this procedure):

1. The MN sends to P-CSCF2 a new message (SIP Re-REGISTER) including P-CSCF1 and S-CSCF addresses.

2. The P-CSCF2 requests P-CSCF1 to transfer the contexts related to the SIP dialog (dialog1) (partial Estb_1 context) and to the IPsec SA1 (partial ATH_5 context), already established between the MN and the P-CSCF1 through IP-AN1.
3. When the contexts are transferred, P-CSCF2 forwards the SIP Re-REGISTER message to S-CSCF. The S-CSCF updates the MN address (@IP2) as well as the IP route for SIP signalling to MN (@IP2).
4. The S-CSCF responds to the MN via P-CSCF2 with a SIP OK message to acknowledge the SIP Re-REGISTER message.

After this context transfer, ATH_5 context is completely established in the MN, P-CSCF2 and S-CSCF. Then, the MN sends to the CN a SIP Re-INVITE message through IP-AN2 to update its IP address. As P-CSCF2 contains the dialog1 context, it is able to treat this message and forward it to the S-CSCF.

Solution 1 is incomplete:

- It does not mention the necessity of updating the transferred context (SIP dialog and IPsec SA) with the new MN address (@IP2).
- Estb_2 and Estb_3 steps for policy rules calculation are not mentioned in the overall procedure description. [79] pretends to simplify the resource reservation step (estb_4) without giving clear explanation. Estb_5 and Estb_6 steps confirming resource reservation and updating the session are not mentioned.

Solution 1 has the following **drawback**:

- The SIP Re-REGISTER message is sent to P-CSCF2 outside of any IPsec SA (IPsec SA1 context is active in P-CSCF2 only after the reception of SIP Re-REGISTER message). This presents security issues since a "bad user" masquerading as the MN could send such messages.

Solution 2: Proactive ATH_3 and ATH_4 steps and transfer of Estb_1 and ATH_5 contexts before handover to IP-AN2

The previous solution is incomplete. I propose in the following a complete solution based on proactive step execution and context transfer (before handover).

Before handover, while the MN is on IP-AN1 (refer to figure 2.9 for the understanding of this procedure):

1. The MN receives an event about imminent subnet change.
2. The MN performs proactive **ATH_3** to acquire @IP2.
3. The MN performs proactive **ATH_4** to discover P-CSCF2.
4. The MN notifies S-CSCF about (handover need, @P-CSCF2, @IP2).
5. The S-CSCF orders P-CSCF1 to transfer to P-CSCF2 **Estb_1** context (dialog and `SDP`) and the whole **ATH_5** context[8] after updating them with @IP2.
6. P-CSCF2 deduces the `SI` and sends it to PCRF2 (**Estb_2**).

[8] IPsec SA, IP route for SIP signalling, ...

7. PCRF2 deduces the `(IP) policy rules` and sends them first IP router 2 (**Estb_3**).

Then on IP-AN2:

8. The MN attaches to IP-AN2 (**ATH_0**).
9. The MN registers/authenticates to IP-AN2 (**ATH_1**).
10. The MN establishes a bearer for SIP signalling on IP-AN2 (**ATH_2**).
11. First IP router 2 reserves resources on IP-AN2 (**Estb_4**) according to the received `(IP) policy rules`.
12. The MN detects that resources are reserved on IP-AN2 (**Estb_5**).
13. The MN updates the session (**Estb_6**).
14. The CN is informed about MN @IP2 (**phase 3**).

As it can be concluded, an important number of steps has to be performed before and after the handover. Therefore, the problem of high handover delay in case of cells with small overlapping zones remains unsolved.

2.3 Conclusion

This chapter has explained the service access and mobility procedures and presented their performance problems. Table G.1 gives a global view of these problems and their corresponding solutions, identified from the state of the art or based on my own proposals.

Service access procedure (authentication/registration + service establishment)	
High access delay	Solution: Mapping between the IP-AN user ID and the IMS user IDs to reduce the delay of the step registration/authentication to the IMS (ATH_5) [70, 63] (-) Does not enable to establish the IPsec SA between the MN and the P-CSCF.
	Solution: parallel step execution: e.g. begin the step resource reservation (Estb_4) at the same time as the step service initiation/negotiation (Estb_1) (-) QoS is badly impacted: increase of ghost calls probability, resource over-reservation.
	Solution: less time for the step resource reservation (Estb_4): e.g. by reducing the number of nodes in the IP-AN [72]. (-) IP-ANs with this feature do not exist.
Service non-adaptation to the IP-AN available resources	**Case 1: the network supports resource renegotiation + solution 1 or solution 2** (-) high delay because of resource renegotiation Solution 1: service adaptation is initiated by the network (-) need of reverse (PCEF+PCRF+AF) mapping functions, and new message specification. Solution 2: service adaptation is initiated by the MN (-) need, in the MN, of the (AF+PCRF+PCEF) and of reverse (PCEF+PCRF+AF) mapping functions => duplication of functions, not in line with network-oriented policy control.

	Case 2: the network does not support resource renegotiation but a Resource Manager (RM) node collecting resource information from IP-AN nodes + solution 1 or solution 2 (-) new node (RM) and interfaces => increase of scalability issues (-) high standardization effort to meet on a common resource information definition (-) require a fine resource information related to the end-to-end path between the cell, the MN is attached to and the first IP router. Solution 1: service adaptation is performed implicitly based on policies received from the network before the service establishment phase [75] (-) difficult to apply this solution if we need to perform a precise and a customized service adaptation per MN. Solution 2: service adaptation is performed during the service establishment phase: the PCRF is linked to the RM [76].
ISC mobility procedure	
Incompatibility with load-based handovers	Solution: decisions for load-based handover are taken by the MN, based on load information received from the network => need of a Resource Manager in the network to extract resource information and send it to the MN (-) high amount of signalling on the radio interface
	Solution: decisions for load-based handover are taken by the network and sent to the MN [74] => need of a Resource Manager and a Mobility Manager in the network (-) additional network nodes and interfaces => increase of scalability issues (-) does not solve high handover delay
Service non-adaptation to IP-AN available resources	see service access procedure
High handover delay	Solution 1: transfer of partial ATH_5 and partial Estb_1 contexts after handover (-) security issues, incomplete solution
	Solution 2: Proactive ATH_3 and ATH_4 steps and transfer of Estb_1 and ATH_5 contexts before handover to IP-AN2 (-) still have the handover delay problem in case of cells with small overlapping zones
Notes In this table the solutions for each problem are stated, then the drawbacks (-) of each solution are provided.	

Table 2.2: Summary of the solutions proposed to solve service access and mobility procedures problems

As it can be deduced from table G.1, the proposed solutions inevitably require additional intelligence or introduce more complexity in either the MN, or the IP access network (IP-AN), or the policy control (PCC) functions, or the IMS service control overlay network. Moreover, they do not solve simultaneously all of the problems. On the contrary, a solution for a given problem amplifies the other problems. For example, solutions for the high access delay problem degrade QoS, or solutions for the service non-adaptation problem increase the access delay. Last but not least, even though the problems in the service access procedure are similar to those of the mobility procedure, the state of the art looks at these two procedures separately.

A global solution has to be defined, which solves all of the identified problems simultaneously. To progress in the definition of this solution, the best way to go about it, is to analyze the causes of these problems and then deduce the requirements that have to be fulfilled in order to avoid them:

- The high delay in the service access procedure is due to: (1) the high number of messages, tasks and mapping functions involved in this procedure; and (2) the fact that this procedure involves a high number of IP-AN nodes and centralized nodes (first IP router, P-CSCF and

S-CSCF) could induce an important queuing delay in these nodes. ISC mobility procedure suffers from a high handover delay, due to the same factors as the service access procedure, as it involves the same steps. This leads to the following requirements:

> *Requirement 5: the service access procedure shall be optimized, in terms of necessary signalling messages, tasks and mapping functions.*
> *Requirement 6: the number of nodes within the mobile network model shall be reduced, in order to enhance the service access delay and the handover delay.*
> *Requirement 7: centralized nodes shall be avoided i.e. nodes shall be rather distributed.*

- Service non-adaptation problem is due to the fact that the resource availability information related to each IP-AN node is not easily available to the service control overlay network (IMS) responsible for service adaptation. This leads to the following requirement:

> *Requirement 8: a tight interaction between the service control layer (IMS) and the network layer (IP-AN) shall be possible, without making the network more complex. This would allow a reactive service adaptation.*

- Solutions for load-based handovers are not simple when considering the ISC mobility procedure because the handover decision is taken by the MN and the latter lacks load information.

> *Requirement 9: load information as well as other handover decision inputs shall be made easily available to the handover decision function.*

The above list of requirements shows that the IP-AN//PCC//IMS model shall be reviewed, mainly the number of nodes and the interaction between the IP-AN, PCC and IMS.

Part II

Proposal of a new model for future mobile networks

CHAPTER 3 UFA: a new model for mobile networks

In part I, the current mobile networks readiness for the new telecommunication ecosystem has been studied, based on the service control, scalability, QoS and service and network convergence criteria. To analyze the scalability criterion, a generic model (IP-AN//PCC//IMS) for the mobile network organic architectures has been provided.
Service control criterion has been discussed considering the IMS as a way to provide it.
QoS criterion has been treated with regard to two indicators, that are the performance to access the service, and the performance of the service once it is established. As these indicators involve the service access and the mobility procedures, these ones have been studied.

The analysis performed in part I, has enabled to formulate different requirements that have to be fulfilled by a mobile network model. It has shown that, for the IP-AN//PCC//IMS, even though some solutions may exist, they are not very efficient as they introduce complexity on the network model and/or the Mobile Node. Moreover, they do not solve simultaneously all of the problems. The analysis has also concluded that, to fulfill easily the requirements, the layered mobile networks model (IP-AN//PCC//IMS) shall be reviewed, mainly the number of network node types and the interaction between the IP-AN, PCC and IMS.

This chapter provides an answer to this last conclusion. It proposes a new model, called Ultra Flat Architecture (UFA), where the number of network node types is reduced and the interaction between the IP-AN, PCC and IMS is simplified. UFA is a flat architecture, and is based on SIP and IMS functions.

Section 3.1 of this chapter describes the UFA organic architecture, focusing on how the policy control and the IMS functions are considered in it. Section 3.2 describes, in greater detail, the UFA nodes and functions. Section 3.3, demonstrates how UFA fulfills the requirements of the mobile network model. Finally, section 3.4 concludes.

3.1 Ultra Flat Architecture (UFA) model

UFA (Ultra Flat Architecture) is a new model for mobile networks [38, 80, 81]. Figure 3.1 shows the UFA organic architecture. UFA is constituted of a single layer containing the IP-AN, PCC and IMS functions, unlike the IP-AN//PCC//IMS model having separate layers (figure 1.10). Moreover, UFA is **flatter** than the the IP-AN//PCC//IMS model, as it contains less node levels.

UFA is based on **SIP** and **IMS** to provide service control for all services. Thus, non-SIP native services are extended to be controlled by SIP protocol. This has required an interaction between SIP protocol and these services in the MN and CN.

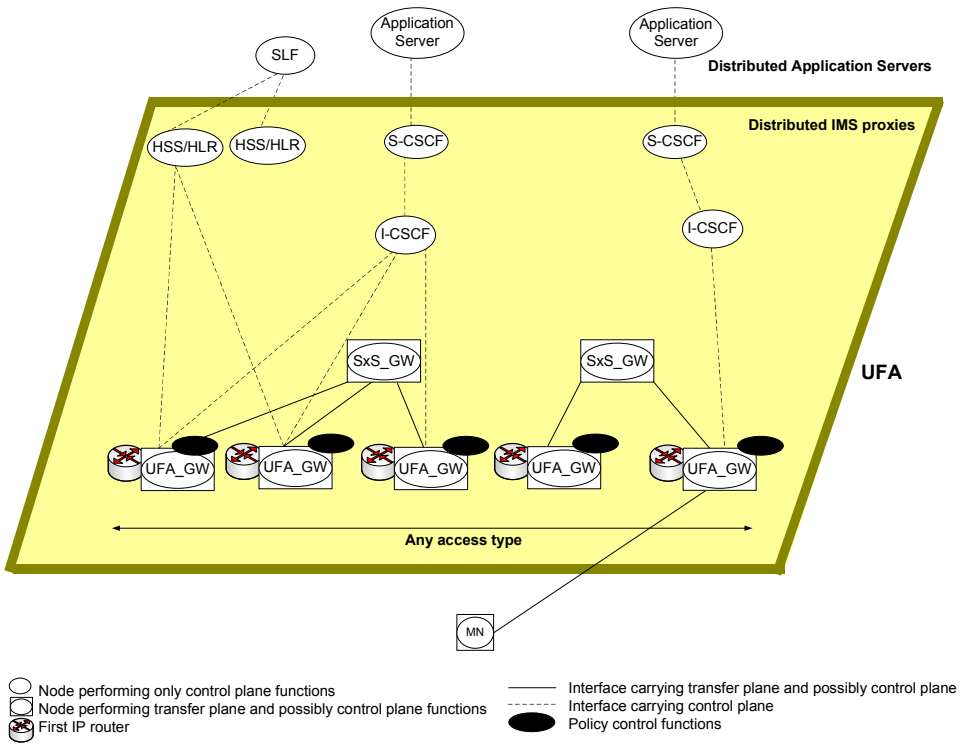


Figure 3.1: Ultra Flat Architecture (UFA) model

UFA is constituted of 5 network nodes: the I-CSCF, the S-CSCF, the HSS and two new nodes, that are:

- UFA Gateway (UFA_GW): the UFA_GW is the main node in UFA. It gathers the classical IP-AN node functions (e.g. NB, RNC, SGSN and GGSN functions for UMTS), policy control functions, P-CSCF functions, SCC AS functions and new introduced functions that control the service access and mobility procedures. This means that the UFA_GW controls the session and offers at the same time physical connectivity (UFA_GW is the CoN) and IP connectivity (UFA_GW is the first IP router) to users. Mobility is ensured between the UFA_GWs acting as the first IP routers.
- SIPcrossSCTP Gateway (SxS_GW): this node handles, for non-SIP native services, the cases where the interaction between SIP protocol and non-SIP native services is not supported in the CN. More details are provided in section 3.2.3.

3.1.1 IMS in UFA

IMS functions in UFA are the same as in the IP-AN//PCC//IMS model.

The P-CSCF functions are co-located with the IP-AN functions in the UFA_GW. During the authentication/registration phase, as for the IP-AN//PCC//IMS, an IPsec SA between the MN and the UFA_GW is built, in order to secure the SIP signalling exchanged between them (more information is in section 4.1).

During the service establishment phase, as for the IP-AN//PCC//IMS model, the P-CSCF functions in the UFA_GW check whether the requested service is authorized for the MN, based on its own policies and current IP-AN capabilities. The P-CSCF also interacts with the local policy control functions.

The I-CSCF and S-CSCF functions are in separate nodes as for the IP-AN//PCC//IMS model. Given the fact that the UFA_GWs are distributed, nothing prevents from distributing the S-CSCF i.e. making them on low levels in the network hierarchy and responsible for small users number. This allows a better load distribution.

3.1.2 Policy control in UFA

The aim of policy control is to simply authorize the service and calculate the policy rules to be enforced on the IP-AN level, so that the bearer transporting the service can be correctly established. However, in the IP-AN//PCC//IMS model, numerous function groups (AF, PCRF, PCEF, BBERF, see section 1.2.3) are necessary to ensure this role, as the objective is also to enable the independence of the PCRF node (which implements the main group of policy control functions). The PCRF receives and sends information independent of the service control layer and from the IP-AN. Thus, it can be shared between different service control layers and different IP-ANs. In UFA, the notion of independence cannot not be applied as IMS and IP-AN functions are gathered in the same node (UFA_GW). Therefore, the AF and PCRF in the UFA_GW are simplified. The PCEF and BBERF are replaced by a new enforcement function, called (UFA Policy Control and Enforcement Function, UPCEF), that calculates the policy rules and enforces them.

The policy control functions in UFA are shown in figure 3.2. They are, compared to the IP-AN//PCC/IMS ones defined in section 1.2.3, :

- **AF**: The AF has a simplified role as it does not translate the service description, contained in the session signalling, to Service Information `SI`. The AF directly sends the service description to the PCRF. The AF only identifies the data flows related to the service and maintains the mapping between the `SIP dialog identifier` and the `data flow descriptors` (source/destination IP addresses and source/destination transport ports), deduced from the service description.
- **PCRF**: The PCRF has a simplified role as it does not translate the `SI` to the `(IP) policy rules`. The PCRF directly sends the received service description to the UPCEF. It only authorizes the service according to advanced information.
- **UPCEF** (UFA Policy Control and Enforcement Function): it is a new function introduced for UFA. As shown in figure 3.2, the UPCEF directly deduces the `(UFA) policy rules` from the service description (`SDP`, or equivalent for non-SIP native services) and enforces them. The UPCEF interacts with other control functions in the UFA_GW, as it will be described in section 3.2.1.

The `(UFA) policy rules` contain the `(IP-AN) policy rules` (defined in section 1.2.3) and possibly some elements of the `(IP) policy rules` (defined also in section 1.2.3). More specifically, the `(UFA) policy rules` contain:

- The `authorized (IP-AN) QoS`.
- The `data flow descriptors`.
- The `event configuration`.
- The `gate status`.
- Possibly the `authorized (IP) QoS`. The `authorized (IP) QoS` may be needed to perform local IP scheduling, in addition to the IP-AN scheduling performed based on the `authorized (IP-AN) QoS`.

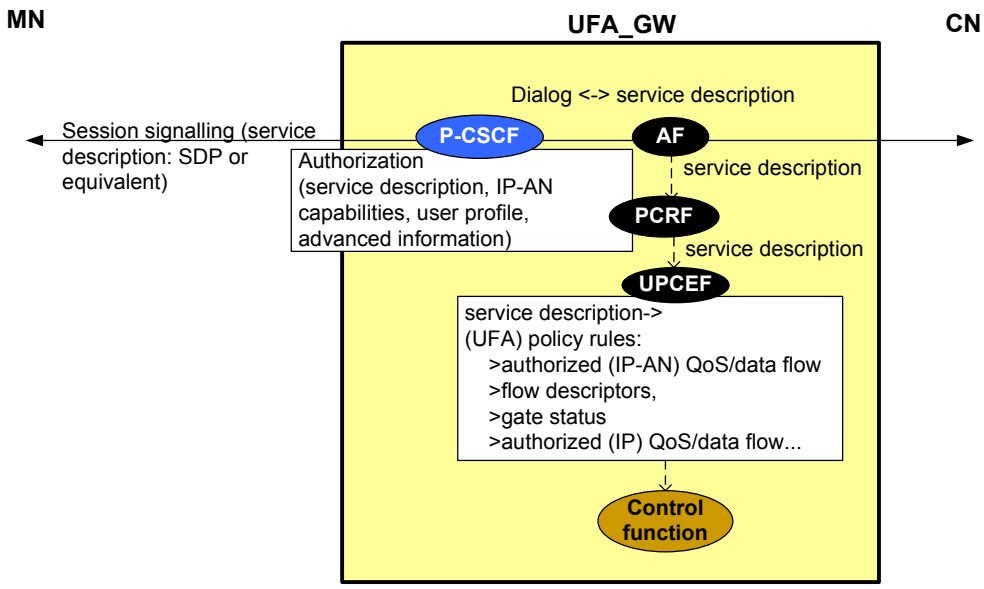


Figure 3.2: Policy control functions in UFA

3.2 UFA detailed control functions and nodes

Most of the UFA control functions are within the network, specifically in the UFA_GW. The MN and the CN act as slaves to the network intelligence.

This section describes the UFA_GW, emphasizing on its control functions. It also details the other UFA nodes on the control and transfer planes (figure 3.3).

3.2.1 UFA Gateway

The UFA Gateway (UFA_GW) control functions are within a controller module. This module generates decisions regarding the service access and mobility procedures. Decisions are enforced by acting on SIP messages, thanks to the SIP Back-to-Back User Agent (B2BUA) (see figure 3.3).

- The **Controller** contains the SCC AS functions (described in section 2.2.1), the IMS functions, the policy control functions (described in section 3.1), and other control functions adding more intelligence to the UFA_GW. These control functions enable to:
  - Decide on mobility from the current UFA_GW to a target UFA_GW in case of coverage loss, current overload or better conditions detected on the target UFA_GW. The interaction with the SCC AS functions enable to decide whether the handover decision is compliant with the the home operator policies.
  - During service establishment phase or mobility procedure, determine:
    - The **service configuration** for SIP native services, or the **SCTP layer configuration** for non-SIP native services, the CN should have:
      - The **service configuration** for SIP native services contains, among other things, information about the **service adaptation** (i.e. downgrade or upgrade), based on the UFA_GW available resources.
      - The **SCTP layer configuration** for non-SIP native services contains, among other things, the **SCTP congestion control parameters**. It is assumed that

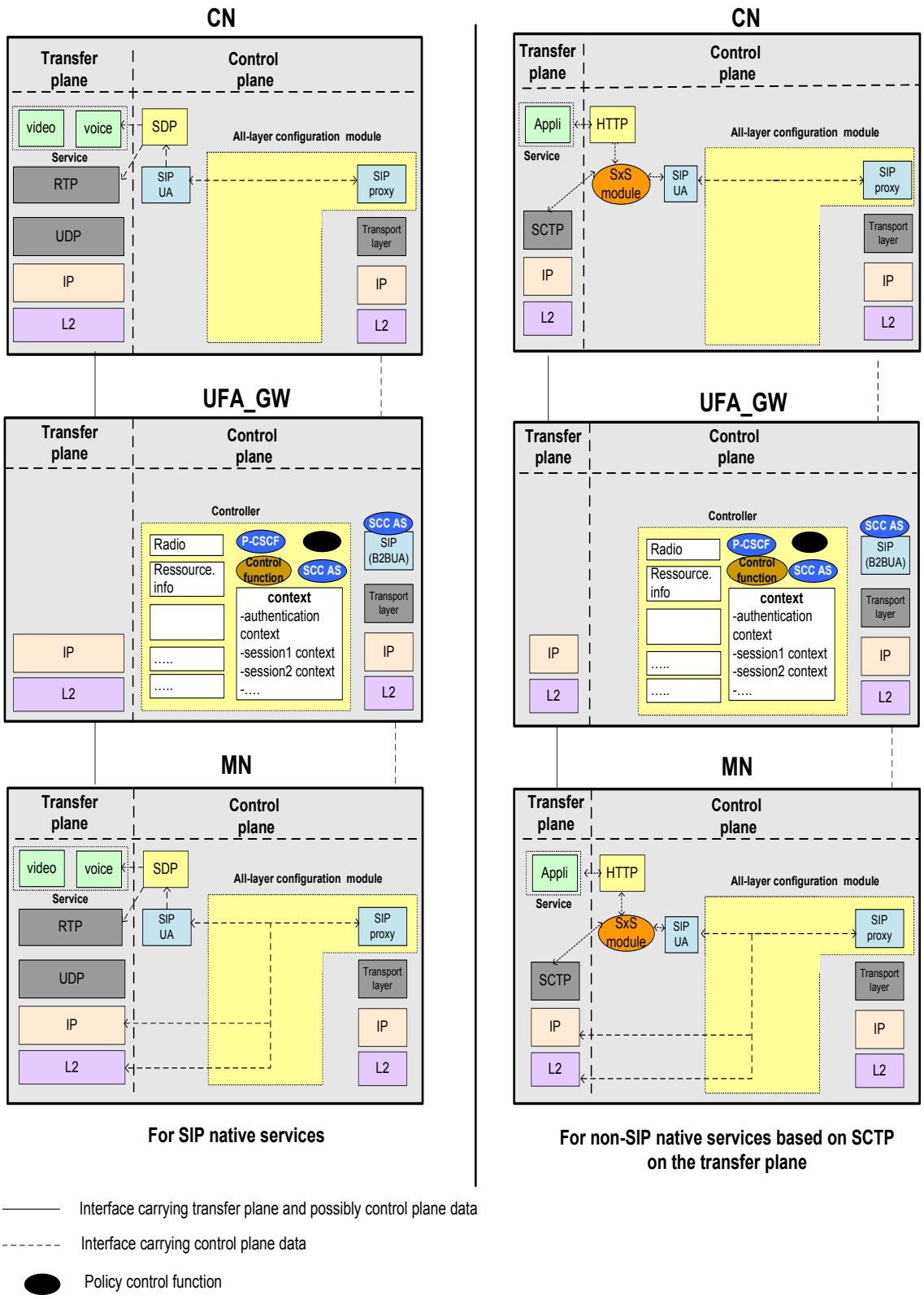


Figure 3.3: UFA control and transfer planes

non-SIP native services, transported over SCTP on the transfer plane, do not need service adaptation (e.g. HTTP streaming apple). They adapt their bitrate to the available bandwidth. However, to use efficiently the available bandwidth, SCTP layer needs to be configured with optimal values for its congestion control parameters (see chapter 7 for all necessary details about SCTP).

  * The **all-OSI layer configuration** the MN should have. It includes, among other things, the service[1] configuration for SIP native services or the SCTP layer configuration for non-SIP native services.

The Controller then communicates these configurations to the B2BUA, which sends them within SIP messages to the MN and CN.

To trigger the previous actions, the Controller receives and treats inputs coming from other internal sub-modules (figure 3.3). The Radio sub-module collects the radio measurements, sent by the MNs about their current UFA_GW and neighboring ones. These measurements enable to trigger a handover based on coverage criterion. The Resource information sub-module calculates the UFA_GW available resources in order to trigger a handover based on load criterion or to adapt the service.

The controller also stores the contexts generated following the service access procedure.

- The **Back-to-Back User Agent (B2BUA)** is quite similar to the SCC AS B2BUA with added/modified features. Like the SCC AS B2BUA, it terminates the SIP dialog (dialog1) initiated by the MN and establishes a second SIP dialog (dialog2) with the CN. Unlike the SCC AS B2BUA, it modifies the content of SIP messages exchanged between the MN and the CN or builds SIP messages that are sent to the MN and CN based on decisions and configuration information received from the Controller.

3.2.2 Terminal (MN/CN)

In addition to the classical SIP UA responsible for controlling applications, the MN/CN implements UFA specific modules on the control plane. As shown in figure 3.3, these modules are:

- **SIP proxy**: As described in the previous section, SIP messages received from the UFA_GW may contain configuration information. The SIP proxy in the MN/CN is responsible for filtering and extracting the different layer-related configuration information and relaying them to the all-layer configuration module.
- **All-layer configuration module**: It receives the different layer-related configuration information from the SIP proxy and relays each part to its concerned layer (layer 2, IP, SIP UA). For non-SIP native services, the SIP UA relays the received information to the SIPcrossSCTP module.
- **SIPcrossSCTP module (SxS module)**: This module within the UFA_GW is specific to non-SIP native services. It is responsible for the interaction between the service, SIP and SCTP. It has a central role in making non-SIP native services controlled by SIP. It locally detects the service related events (establishment, release) and triggers the equivalent events on the SIP level. For example, when a service is going to be launched, it establishes a SIP session and fills equivalent `SDP` fields (service name, flow descriptors).

  It receives from the SIP UA, the SCTP-related configuration information sent by the UFA_GW, and relayed to it by the all-layer configuration module. Then, it enforces this configuration by interacting with SCTP.

[1] means all applications constituting the service

3.2.3 SIPcrossSCTP Gateway (SxS_GW)

The support of non-SIP native services in UFA requires that the MN and the CN implement both SIP and SxS module. However, if the CN lacks these functions, to handle non-SIP services over UFA, a proxy network node, called SIPcrossSCTP Gateway (SxS_GW), is needed. When the MN initiates a non-SIP native service, SIP signalling is sent to the CN. The SxS_GW, intercepts this signalling and translates it to service specific signalling (e.g. RTSP or HTTP), that it sends to the CN. Thus, the SxS_GW anchors the control plane traffic. It also anchors the data plane traffic.

3.3 How UFA fulfills the model requirements?

This section demonstrates how UFA fulfills the model requirements, determined in chapters 1 and 2. It also discusses UFA benefits and limitations.

- *Requirement 1: the service control shall be provided to all applications, in a cost effective manner. IMS is a service control solution already available for SIP native applications. It is proposed to extend it to all applications.*

  Service control is ensured in UFA for all services using IMS functions. Non-SIP native applications are controlled by SIP through the SxS module in the MN/CN and possibly the SxS Gateway in the network.

- *Requirement 2: the mobile network has to be scalable. It means that, in case of hudge data growth, network investments shall remain profitable for operators.*

  We have chosen in section 1.4, three elements enabling to measure the network scalability: the number of nodes on the transfer plane, the number of nodes on the control plane, the number of interfaces. These elements are measured for UFA in table 3.1.

Scalability criteria	**UFA**
Number of nodes on the transfer plane	3
Number of nodes on the control plane	3
Number of interfaces	8

Table 3.1: UFA model analysis

Table 3.1 compared to table 1.1, giving the same elements for the IP-AN//PCC//IMS, points out that UFA is less centralized and hierarchical. Indeed, it contains less node types, less network levels and less interfaces. In case of data growth, only small number of node types and interfaces need to be duplicated, saving CAPEX and OPEX costs.

UFA is **flat** and introduces **distributed signalling and data anchors**, that are the UFA_GWs and the SxS_GWs. This enables to better distribute the traffic load, unlike the centralized anchors. UFA_GWs distribution enables to distribute the S-CSCF and the Application Servers (e.g. TV servers), which enhances their scalability and reduces the delay for accessing the Application Servers content.
The UFA_GWs are "natural" anchors as they offer physical connectivity to users. They are also **temporary** anchors as they do not stay on the path towards the MN, when this latter moves. Indeed, after MN mobility, the traffic passes through a new UFA_GW, the MN is physically attached to, and the old one is no more on the control or transfer plane path.
The temporary anchors have been made possible in UFA, thanks to the use of SIP

protocol for mobility management, instead of tunneling-based protocols, like GTP or MIP.
Thanks to the reduction of network node types in UFA, redundant context information and tasks necessary to handle an ongoing call are deleted. Thus, the network processing delay is reduced.

The basic UFA_GW function is providing physical connectivity to users (capacity, coverage). Connectivity is a vital network part and one of the most dimensioning criteria. In case of data growth, UFA_GWs will be duplicated to satisfy the connectivity criteria. However, this may cause an important UFA cost, as by duplicating the UFA_GWs due to connectivity criterion, UFA intelligence may be duplicated unnecessarily (we may have several thousands of UFA_GWs within a network, like the NBs in UMTS). To overcome this drawback, one solution is to share the UFA_GW intelligence among different Connectivity Nodes (CoNs). A layer 2 handover will be then needed between the different CoNs belonging to the same UFA_GW. This layer 2 handover may be local if we consider distributed CoNs (distributed Base Stations). Distributed Base stations [82] allow to split the two parts of a base station that are, the Base Base Unit (BBU) and the Remote Radio Head (RRH) performing frequency modulation. It also allows to locate these two parts in different sites: the RRH on the roof near the radio antenna, and the BBU at almost 10 km far from the RRH. This distribution is made possible thanks to the standardization of the RRH-BBU interface [82] and to the use of the fiber on this interface. It enables to gather different BBUs on the same site and to aggregate on the same fiber the different radio signals towards the different RRHs [83]. When using distributed Base Stations, UFA intelligence can be co-located with the BBUs. The layer 2 handover is thus local. Distributed Base Stations, independently of UFA, enable to reduce network OPEX as the BBUs are co-located. Moreover, it enables a secure solution since the BBUs are located in protected sites and the signal on the BBU-RRH is protected. Indeed, the Security Association is between the MN and the BBU.

- *Requirement 3: a simple and optimal mobility procedure between the first IP routers, handling the same IP-AN type (e.g. between GGSNs in UMTS) or different IP-AN types, has to be supported.*

  This requirement is fulfilled in UFA, as a mobility between the UFA_GWs, acting as the first IP routers, is specified (see chapter 4).

- *Requirement 4: service and network convergence shall be provided.*

  UFA is service convergent as it relies on IMS. It is network convergent as it uses the same nodes, protocols (EAP for authentication, IPsec for integrity and ciphering, SIP for service establishment and mobility procedures), methods (AKA for authentication) and interfaces, whatever the radio technology (more details are in chapter 4).

Requirement 5: the service access procedure shall be optimized, in terms of necessary signalling messages, tasks and mapping functions.

From an architecture point of view, UFA optimizes the service access procedure. Indeed, the fact that UFA enables to determine the all-OSI layer configuration for the MN, indicates that different layers can be configured simultaneously, enabling thus to gain time. Moreover, as said for requirement 2, since redundant context information is removed, the number of tasks to be executed according to this context is reduced. Finally, as policy control functions are simplified in UFA, the number of mapping functions is reduced. Chapter 4 describes the service access procedure for UFA. Comparing figures 2.4 and 4.4, it can be deduced that UFA saves: 6 Diameter messages, Estb_4 step and 2 SIP messages.

- *Requirement 6: the number of nodes within the mobile network model shall be reduced in order to enhance the service access and the handover delay.*

  In UFA, the number of nodes are reduced, as already commented in requirement 2. The benefits of that, compared to the IP-AN//PCC//IMS model, are proven and evaluated in chapter 5 for the access delay, and in chapter 6 for the handover delay.

- *Requirement 7: centralized nodes shall be avoided i.e. nodes shall be rather distributed in order to enhance the access and the handover delays.*

  In UFA, there are no centralized anchors but only distributed and temporary anchors, as already commented in requirement 2. The benefits of that, compared to the IP-AN//PCC//IMS model, are proven and evaluated in chapter 5 for the access delay.

- *Requirement 8: a tight interaction between the service control layer (IMS) and the network layer (IP-AN) shall be possible, without making the network more complex. This would allow a reactive service adaptation solution.*

  The tight interaction is ensured in UFA thanks to the co-location, in the UFA_GW, of SIP layer with IP and layer 2, both having the knowledge of resource information. This interaction is performed simply without requiring any external interface. Moreover, it enables during the establishment or mobility phases, to adapt, according to the available resources, the service for SIP native services and the SCTP congestion control parameters for non-SIP native services. More details are in chapter 4.

- *Requirement 9: load information as well as other handover decision inputs shall be made easily available to the handover decision function.*

  The UFA_GW is responsible for handover decision. As shown in figure 3.3, it interacts with internal sub-modules providing radio-related inputs and resource/load information inputs. It also interacts with the SCC AS internal functions regarding the home operator policies.

3.4 Conclusion

Part I of this thesis has defined a set of requirements and guidelines that have to be fulfilled by a mobile network model, in order to face the challenges of the new ecosystem. This chapter has introduced an Ultra Flat Architecture (UFA) model fulfilling these requirements.

UFA is a flat architecture based on SIP. As for current mobile networks, it implements IMS and policy control functions. However, it is constituted of a single layer implementing these functions. It reduces the number of node types and interfaces, and only requires distributed and temporary anchors, instead of centralized ones.

In addition, UFA introduces new control functions in the network in order to better handle the QoS. The terminal (MN/CN) does not need to be intelligent, it just executes the orders received from the network.

UFA contains the I-CSCF, S-CSCF and the HSS nodes and two new nodes that are the UFA Gateway (UFA_GW) and the SIPcrossSCTP Gateway (SxS_GW). The UFA_GW is the main UFA node, it gathers classical IP-AN nodes functions (e.g. NB, RNC, SGSN and GGSN functions for UMTS), policy control functions, P-CSCF functions, SCC AS functions and new functions. The SxS_GW can be necessary to handle the case of non-SIP native services.

From an architecture point of view, UFA fulfills the 9 model requirements. The next chapter illustrates how UFA fulfills these requirements from a procedure point of view.

CHAPTER 4 Main network procedures in UFA

To evaluate the QoS criterion in the IP-AN//PCC//IMS model, the service access and mobility procedures have been studied (chapter 2). For the same reasons, these procedures are studied for UFA in this chapter. Beyond that, the purpose of this chapter is also to: (1) provide an exhaustive UFA specifications, (2) allow an objective comparison with the IP-AN//PCC//IMS model from a procedure and QoS point of view, for example regarding the access delay or the handover delay, and (3) demonstrate how UFA fulfills the model requirements from a procedure point of view.

In UFA, the service access and mobility procedures are described for SIP native and non-SIP native services. They are based on SIP for the two kinds of services, to respect the service control requirement (requirement 1) and the network convergence requirement (requirement 4). It is assumed that these two kinds of services require a guaranteed bandwidth, imposed by the user profile and/or the applications requirements.

This chapter is organized as follows: section 4.1 describes the service access procedure for UFA; section 4.2 describes the mobility procedure for UFA; and section 4.3 provides a conclusion.

4.1 Service access procedure in UFA

As for IP-AN//PCC//IMS, two phases are necessary to access services in UFA. Phase 1 is related to the user registration/authentication. Phase 2 is related to the service establishment.

4.1.1 Phase 1: registration/authentication

Section 2.1.1 has presented, for the IP-AN//PCC//IMS model, the steps of the registration/authentication phase. Table 2.1 (page 42) has also provided the means employed to execute each of these steps, considering different IP-AN examples.

For UFA (figure 4.1), the same registration/authentication steps, as those for the IP-AN//PCC//IMS model, have to be executed. Some choices, based on what is used for the different IP-AN examples, are made (for ATH_1 and ATH_3) to fulfill the mobile network model requirements. Some other steps (ATH_4 and ATH_5) are optimized thanks to the flat UFA model.

The step **ATH_0** regarding layer 2 attachment to UFA IP-AN and the step **ATH_2** regarding bearer establishment for SIP signalling, are executed in the same manner as in the IP-AN//PCC//IMS model.

The step **ATH_1** regarding the registration/authentication to UFA IP-AN, and the step **ATH_3** regarding the IP address acquisition, are executed similarly to I-WLAN//PCC//IMS (table 2.1), using EAP protocol and AKA method. The reasons for this choice are: (1) In I-WLAN, ATH_1 and ATH_3 are executed simultaneously which enables to reduce the global registration/authentication delay. (2) EAP is independent of the radio technology, therefore it is compliant with the network convergence requirement. (3) In I-WLAN, the Security Association, established in ATH_1 between the MN and the PDG to protect the user traffic, is at the IP level (IPsec). Hence, it enables network convergence.

UFA model enables to optimize the step **ATH_4** regarding the P-CSCF discovery and the step **ATH_5** regarding the registration/authentication to the IMS. Indeed, the fact that the P-CSCF and the first IP router functions are co-located in the UFA_GW enables to perform ATH_4 implicitly, meaning that no messages are needed to discover the P-CSCF IP address (the UFA_GW IP address has been discovered during ATH_1). The P-CSCF and the IP-AN functions co-location enables to use the Security Association, built between the MN and the UFA_GW in ATH_1, to secure SIP signalling (part of ATH_5 step) in addition to the user traffic.

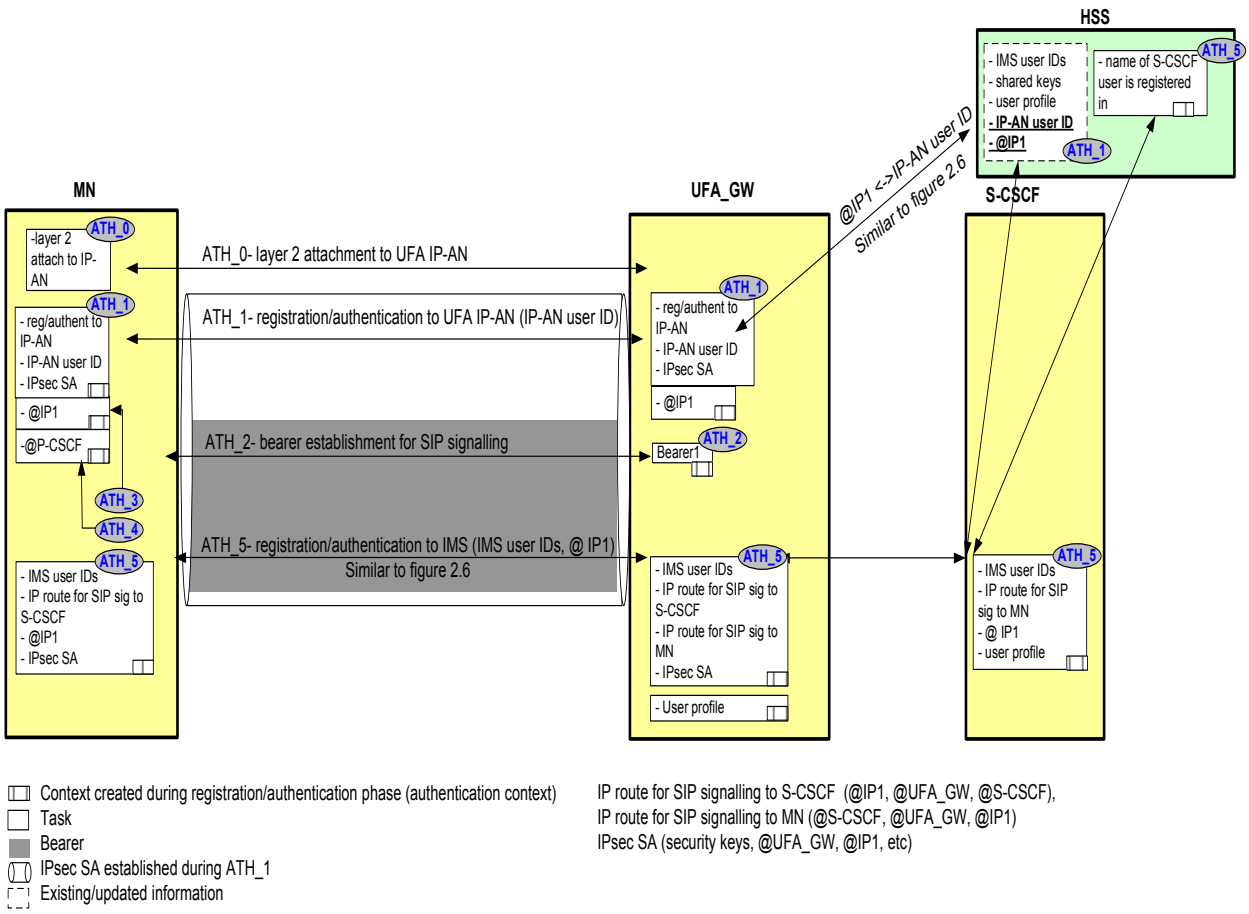


Figure 4.1: Registration/authentication to UFA

The detailed description of the registration/authentication steps in UFA is given hereafter:

ATH_0: layer 2 attachment to UFA IP-AN

The MN attaches to the UFA_GW at layer 2 level in order to have a physical connectivity.

ATH_1: registration/authentication to UFA IP-AN
First, as for I-WLAN, the MN needs to discover the UFA_GW IP address. It uses DHCP [54, 55] or the stateless IPv6 configuration (the content of Router Advertisement) [56].
Then, the MN uses EAP and the AKA authentication method, to authenticate itself. During this step, an IP address is allocated to the MN and an IPsec SA is built between the MN and the UFA_GW.

ATH_2: bearer establishment for SIP signalling
A bearer (bearer1) is established between the MN and the UFA_GW to transport SIP signalling that will be be sent/received by the MN beginning from ATH_5.

ATH_3: IP address acquisition
The MN has already acquired its IP address in ATH_1. Therefore, this step has been already performed implicitly.

ATH_4: P-CSCF discovery
The MN knows the P-CSCF IP address through ATH_1 step. Indeed, in ATH_1, it has discovered the UFA_GW which implements P-CSCF functions. Therefore, this step has been already performed implicitly.

ATH_5: registration/authentication to IMS
The delay of this step is reduced compared to the IP-AN//PCC//IMS model.

In the IP-AN//PCC//IMS model, ATH_5 (figure 2.2) requires two rounds of SIP REGISTER/SIP OK messages. Moreover, during this step, an IPsec SA is built between the MN and P-CSCF to secure SIP messages.

In UFA, ATH_5 is performed with only one round of SIP REGISTER/SIP OK messages, based on the same principles of the solutions presented in section 2.1.3.1 (page 47). These principles are: (1) an initial binding between the IP-AN user ID (e.g. IMSI in UMTS) and the IMS user IDs, is set in the HSS network database and in the MN, (2) during ATH_5, the S-CSCF checks directly or indirectly that the user trying to register/authenticate using IMS user IDs has an IP-AN user ID compliant with the binding in the HSS. It is proposed, in UFA, that the S-CSCF performs this checking similarly to [63] (figure 2.6).

Indeed, as shown in figure 4.1, during ATH_1 when the MN acquires its IP address (@IP1), the UFA_GW informs the HSS that the user having the IP-AN user ID has @IP1. The HSS deduces a mapping between the IMS user ID and @IP1, based on the already existing IMS user ID - IP-AN user ID mapping. Then, in ATH_5, when the S-CSCF receives the SIP REGISTER message natively containing the IMS user ID and @IP1, it asks the HSS to check this mapping. If the result is positive, registration/authentication to IMS is accomplished. Thus, there is no need to perform a second round of SIP REGISTER/SIP OK exchange.

The drawback of the solutions presented in section 2.1.3.1 (page 47) for the IP-AN//PCC//IMS model, is that they don't enable the establishment of the IPsec SA between the MN and the P-CSCF. In UFA, as the P-CSCF functions are within the UFA_GW, the same IPsec SA built during ATH_1 between the MN and UFA_GW can be used to secure SIP signalling. **Thus, the drawback of the state of the art is eliminated**.

I propose that, during the step authentication/registration to the IMS (ATH_5), the user profile is sent from the S-CSCF to the UFA_GW to ease local decisions.

At the end of the registration/authentication phase, an **authentication context** is built in the MN, UFA_GW, S-CSCF and HSS, as shown in figure 4.1.

4.1.2 Phase 2: service establishment

In UFA, the service establishment procedure is applicable for SIP native and non-SIP services. Each non-SIP native service is controlled through a SIP session launched when the service is launched. It is described in SIP messages using a content type "text-plain", I call `SDPN` (Session Description Protocol for Non-SIP native services). The `SDPN` is the equivalent of the `SDP`[1] for SIP native services. As shown in table 4.1, it provides the `service name` and the `data flows descriptors` and may contain the SCTP congestion control parameters, whose use is detailed in the following.

In the IP-AN//PCC//IMS model, as described in section 2.1.2 and figure 2.3, the service establishment phase for SIP native services requires 6 steps: Estb_1: session initiation and negotiation; Estb_2: policy rules calculation for the IP level; Estb_3: policy rules calculation for the IP-AN level; Estb_4: resource reservation; Estb_5: resource reservation detection; and Estb_6: session update.
Moreover, in this model, service establishment suffers from a high access delay and a service non-adaptation to IP-AN resources.

In UFA, the service establishment procedure is guided and controlled by the network, more specifically the UFA_GW. The reduction of the number of nodes to a single node (UFA_GW), and the co-location of different layers (SIP, IP, layer 2) and different control functions in the UFA_GW has led to two advantages. Firstly, the service establishment is performed in only one step (**Estb_UFA**) replacing the 6 steps of the IP-AN//PCC//IMS model, which saves the access delay. Secondly, the service or SCTP congestion control parameters can be adapted according to the available resources.

4.1.2.1 Step Estb_UFA: a single step for service establishment in UFA

During Estb_UFA, the Source UFA_GW (UFA_GW_S) performs different tasks, as indicated in figures 4.2 and 4.3 respectively for SIP natives services and non-SIP native services. **It is worth to mention that these tasks are almost the same for the two kinds of services and differ only regarding the use of `SDP` or `SDPN`, that contain respectively information about the service adaptation or the SCTP congestion control parameters tuning** (see chapter 7 for all necessary details about SCTP). For the sake of simplicity, for non-SIP native services the CN is considered as the sender.

UFA_GW_S tasks are:

1. The UFA_GW_S authorizes the service based on: the initiated `SDP`/`SDPN` ($\mathtt{SDP_i}$/$\mathtt{SDPN}_i$), UFA_GW_S capabilities, user profile and advanced information.

2. The UFA_GW_S involves policy control functions to calculate the `(UFA) policy rules`, mainly the `authorized (IP-AN) QoS` defined in section 3.1.2, corresponding to $\mathtt{SDP_i}$ or $\mathtt{SDPN_i}$ and:

   - For SIP native services, it compares the `authorized (IP-AN) QoS` to its available resources. When the latter is inferior to the former, it proposes a **service adaptation** by eliminating some of the applications proposed to be part of the service, or tuning their codecs. To do that, it treats and modifies the `SDP` ($\mathtt{SDP_0}$) based on the algorithm provided in section 4.1.2.2. A video call issued from voice and video applications can be considered as a typical service example.

     Finally, the `(UFA) policy rules` are updated to take into account $\mathtt{SDP_0}$.

[1] `SDP` example for a video call is provided in table A.3.

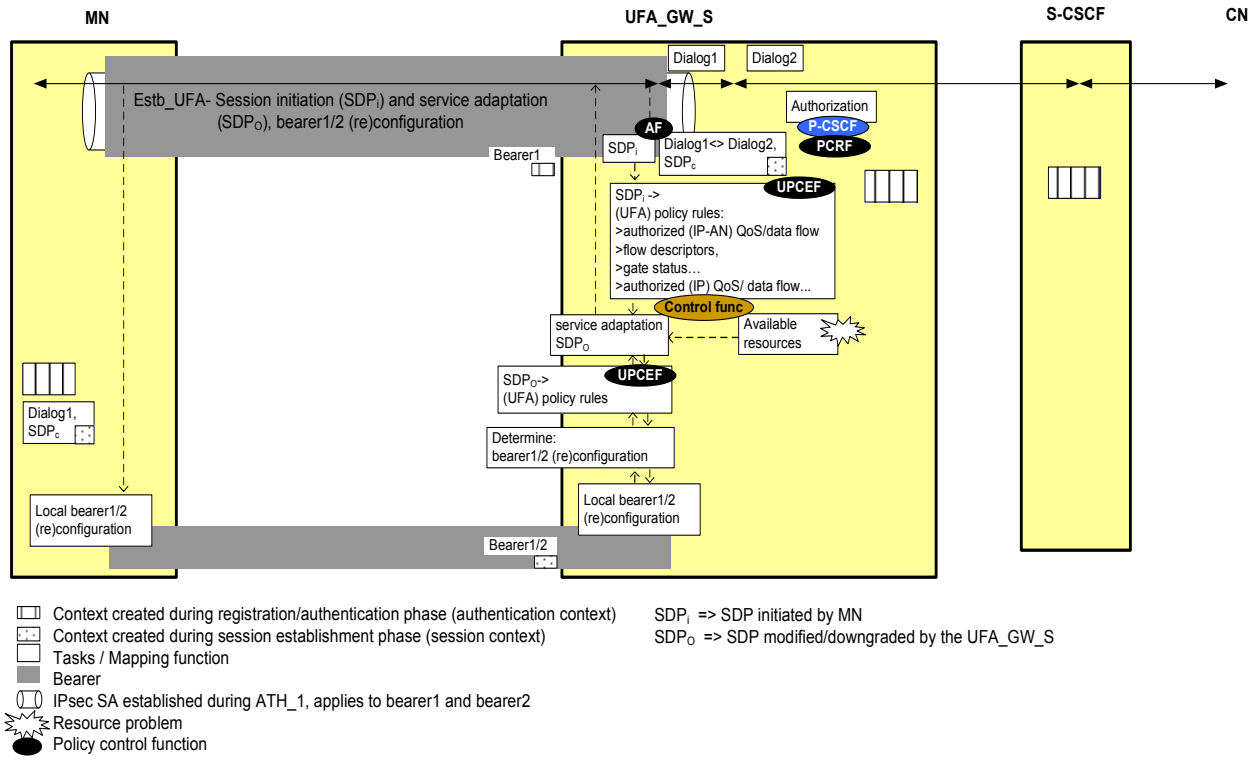


Figure 4.2: Service establishment in UFA for SIP native services

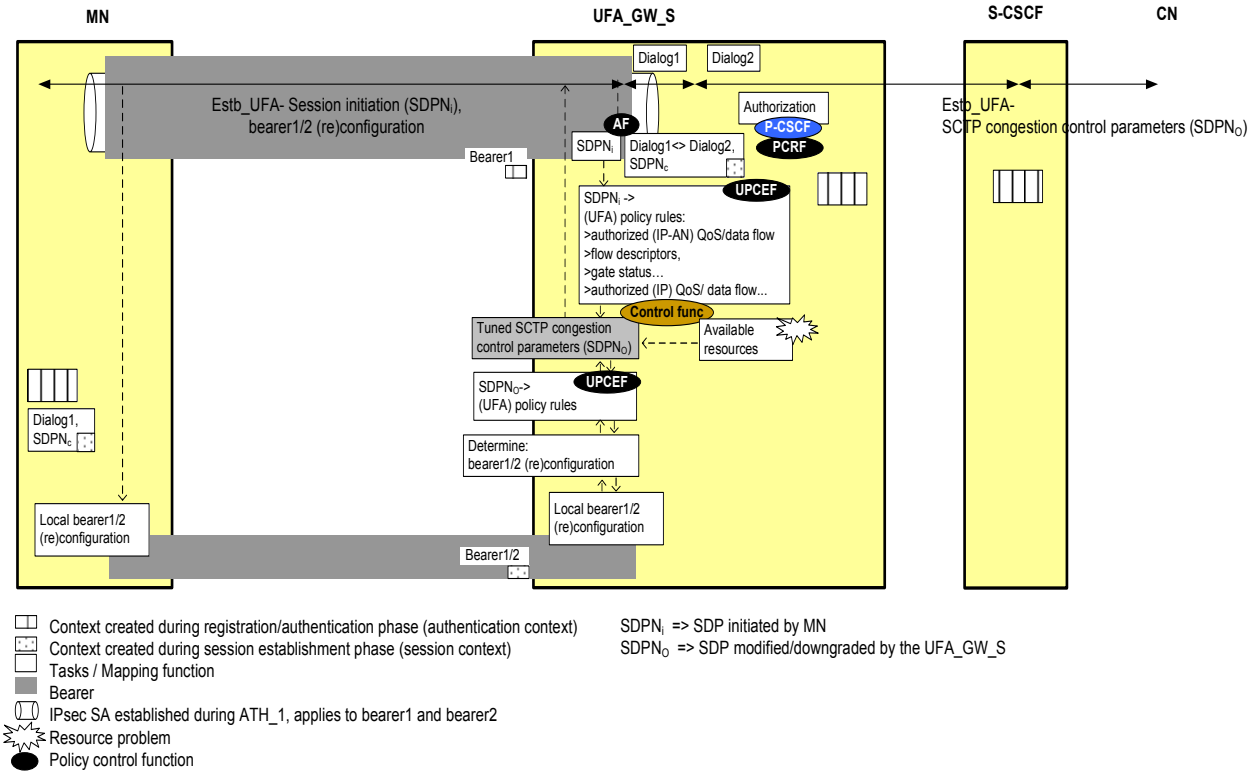


Figure 4.3: Service establishment in UFA for non-SIP native services

- For non-SIP native services, it allocates a bandwidth considering the `authorized (IP-AN) QoS` and the available resources. Then, it determines/tunes **SCTP congestion control parameters** values based on the algorithm provided in section 4.1.2.3. These values enable a rapid and efficient use of the allocated bandwidth. Tuned **SCTP congestion control parameters** are inserted in `SDPN` ($\mathtt{SDPN_0}$) within SCTP_optim field (see table 4.1), which is sent to the data sender CN.

  Finally, the `(UFA) policy rules` are updated according to $\mathtt{SDPN_0}$. Note that if tuning is not applied, SCTP considers initial default values (`cwnd`=2MTU , `ssthresh`=65536bytes, `RTO`=3s) for data transmission.

3. The UFA_GW_S determines for $\mathtt{SDP_0}$/$\mathtt{SDPN_0}$ the reconfiguration of bearer1 established during ATH_2, or the configuration of the new bearer (bearer2) to be established.

4. The UFA_GW_S sends $\mathtt{SDP_0}$/$\mathtt{SDPN_0}$ and bearer (re)configuration to the MN, which enforces them.

5. For SIP native services, the UFA_GW_S deduces during service establishment the `SDP` common to MN and CN ($\mathtt{SDP_c}$) independently of its resources. This $\mathtt{SDP_c}$ is used by the UFA_GW_S during the call to upgrade the service, if resources become available. It can be also used by a target the UFA_GW to upgrade the service (see section 4.2). For non-SIP native services, there is no common `SDPN`, however $\mathtt{SDPN_i}$ is noted $\mathtt{SDPN_c}$ is the following.

Field	**Meaning**
Service name	e.g. www.google.com, www.streaming.com
`Data flow descriptors`	source and destination (IP address+ transport port)
SCTP_optim >`cwnd` >ssthresh >RTO	This field is inserted by the UFA_GW in some messages sent to the data sender (CN). It is tuned by the UFA_GW and contains the configuration that shall be considered by the data sender regarding its congestion control parameters (`cwnd`, `RTO`, `ssthresh`).

Table 4.1: `SDPN`: Session Description Protocol for Non-SIP native services

As explained in section 3.2.1, the above UFA_GW_S tasks are performed thanks to the Controller and the B2BUA. When the UFA_GW_S, the MN is attached to, receives SIP INVITE message for service establishment, the B2BUA intercepts the message and creates a second SIP INVITE message towards the CN. This corresponds to the building of two SIP dialogs[2]: dialog1 between the MN and the UFA_GW_S and dialog2 between the UFA_GW_S and the CN. The B2BUA binds the two SIP dialogs related to the established session. The B2BUA detailed behavior with regard to the creation of dialog2 based on dialog1 is given in appendix E.

During service establishment, the UFA_GW_S stores the **session context** that is constituted of the two SIP dialogs (dialog1, dialog2) and $\mathtt{SDP_c}$/$\mathtt{SDPN_c}$.

4.1.2.2 Algorithm for SIP native service adaptation

This algorithm allows the UFA_GW to adapt SIP native services to its available resources. It calculates a new `SDP` ($\mathtt{SDP_0}$) based on the requested one as follows:

[2]see definition in appendix A

For each application within the service (m line in the requested SDP, see section A.2)

Mark the application as not satisfied

For each codecx=codec1,.., codeci proposed for the application

If (there are resources for codecx),

Put codecx in the first position in the list of codecs

Mark the application as satisfied

Exit

If the application is not satisfied put the port to 0

4.1.2.3 Algorithm for tuning SCTP congestion control parameters for non-SIP native services

This algorithm allows the UFA_GW to set SCTP congestion control parameters (`cwnd`, `ssthresh`, `RTO`) values that enable a rapid and efficient use of the allocated bandwidth $Xput_{GW-MN}$. The reasons for this setting are provided in chapter 7, more specifically in sections 7.3.1.2 and 7.5.

cwnd=BDP=RTT_{CN-MN} * $Xput_{GW-MN}$

RTO=3s

ssthresh=BDP

Where

RTT_{CN-MN}= RTT_{GW-CN} + RTT_{GW-MN}

RTT is the round trip time. RTT_{GW-MN} part is calculated considering the transmission of a packet having a length of 1500 bytes. RTT_{CN-GW} part can be determined based on measurements performed by the UFA_GW as described in [84].

In addition to calculating SCTP congestion control parameters, the UFA_GW checks whether its free buffer size is compliant with the rule of thumb (buffer_size = BDP) and allocates it accordingly (see explanation in section 7.1.2.3).

4.1.2.4 Detailed flow chart for SIP native service establishment (Estb_UFA)

This section illustrates the detailed flow chart of the service establishment in UFA [85], considering the case of a SIP native services (video call). To be generic and exhaustive, it is assumed that each of the MN and CN are attached to a UFA_GW (respectively UFA_GW(MN) and UFA_GW(CN)).

Estb_UFA step is similar to the Estb_1 step in the IP-AN//PCC//IMS model, detailed in section 2.1.2 and figure 2.4. However there is a major difference consisting in that, in Estb_UFA, the service characteristics are negotiated not only according to the MN and CN capabilities but also according to the resource availability in the UFA_GW(MN) and UFA_GW(CN). Moreover, Estb_UFA is accompanied with resource reservation (bearer configuration).

As shown in figure 4.4, in **Estb_UFA**, there are two rounds of `SDP` offer/answer exchanges:

- In the first round (SIP INVITE/SIP SESSION PROGRESS), 7 sub-steps (UE1-UE7) are performed:

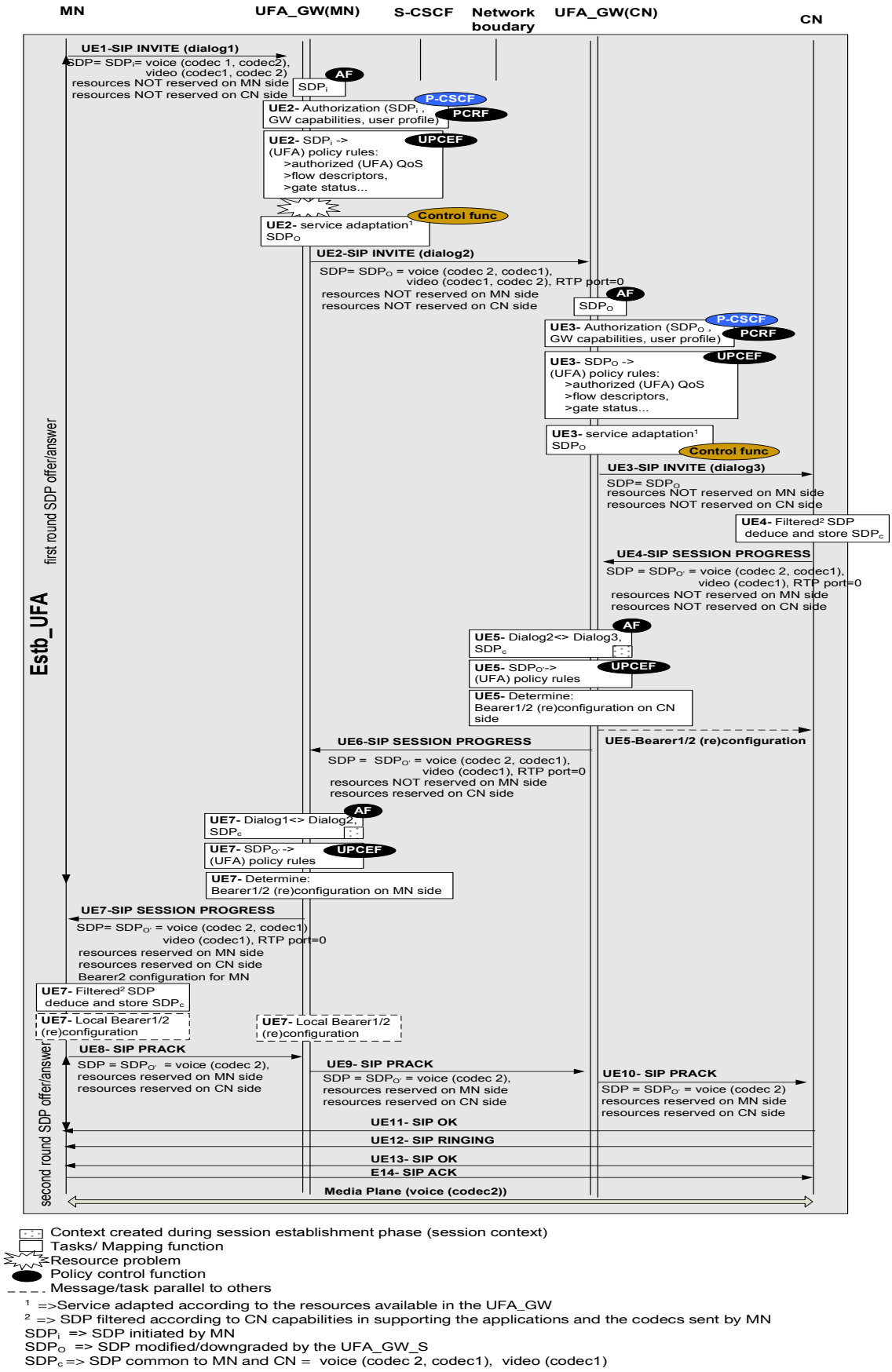


Figure 4.4: Detailed message flow for service establishment in UFA for SIP native services

- UE1: The MN sends a SIP INVITE message including a first SDP offer. This offer (SDP_i[3]) contains the list of applications (voice, video) and codecs per application supported by the MN and proposed to the CN to be part of the requested service. SDP_i indicates that resources are not reserved on the MN and CN sides (e.g. by means of QoS preconditions (see appendix C)).
- UE2: The UFA_GW(MN) authorizes the service based on the: initiated SDP (SDP_i), IP-AN capabilities, user profile and advanced information. Then, it calculates the `(UFA) policy rules`, mainly the `authorized (IP-AN) QoS` defined in section 3.1.2, corresponding to SDP_i. It compares the `authorized (IP-AN) QoS` to its available resources. When the latter is inferior to the former, it proposes a new **service adaptation** by eliminating some of the applications proposed to be part of the service, or tuning their codecs. To do that, it modifies the SDP (SDP_0) based on the algorithm provided in section 4.1.2.2.

  In figure 4.4, the UFA_GW(MN) has resources only for voice(codec2) and has no resources for video. Consequently, it proposes another SDP (SDP_0[4]) in which: -for voice, codec2 is set in the first position before codec1 and, -for video, RTP port is set to 0. Although video cannot be provided, its codecs are not removed in order to allow the CN (in UE4) and the UFA_GW(CN) (in UE5-6) to determine the SDP common to MN and CN (SDP_c).
- UE3: The UFA_GW(CN) does the same as the UFA_GW(MN) in UE2. If necessary, it proposes **service adaptation** and modifies the SDP. For this purpose, it interprets the received SDP (SDP_0) as the fact that resources shall be available only for voice(codec2), since codec2 is in first position for voice and RTP port is 0 for video.

  In figure 4.4, the UFA_GW(CN) can provide resources for voice(codec2). Therefore, it forwards the received SDP (SDP_0) without modification to the CN.
- UE4: After receiving UE3, the CN filters the SDP (SDP_0) by determining the SDP common to MN and CN (SDP_c), independently of the modifications of UFA_GW(MN) and UFA_GW(CN). To do that, it shall ignore that RTP port is 0 for video.

  In figure 4.4, the CN does not support the video (codec2), it removes it and stores SDP_c[5]. Then, it sends back the SDP answer (SDP_0,[6]) to the MN.
- UE5-6: When the UFA_GW(CN) gets the SDP_0,, it also deduces SDP_c independently of the UFA_GW(MN) and UFA_GW(CN) previous modifications. Then, it updates the `(UFA) policy rules` on the CN side according to SDP_0, (i.e. for voice(codec2)) and determine the corresponding bearer1/2 (re)configuration on the CN side. At this step, it sends to the CN the bearer (re)configuration and indicates in SDP_0, that resources are reserved on the CN side.
- UE7: When the UFA_GW(MN) receives SDP_0,, it also deduces and stores SDP_c. Then, it updates the `(UFA) policy rules` according to SDP_0, (i.e. for voice(codec2)) and determine the corresponding bearer1/2 (re)configuration. At this step, it sends to the MN the bearer (re)configuration and SDP_0,.

  When the MN receives the SIP message, it filters SDP_0, to deduce and store SDP_c. Then, it (re)configures locally the bearer1/2 according to the received configuration.

- In the second round (SIP PRACK/SIP OK), 5 sub-steps (UE8-UE12) are performed:

[3] SDP_i=voice(codec1, codec2), video(codec1, codec2)
[4] SDP_O=voice(codec2, codec1), video(codec1, codec2), RTP port=0
[5] SDP_c=voice(codec2, codec1), video(codec1)
[6] SDP_0,=voice(codec2, codec1), video(codec1), RTP port=0

  - UE8-9-10: The MN sends back a last SDP offer $SDP_{0'}$ confirming that voice(codec2) is chosen and that resources are reserved on the MN side (e.g. by means of QoS preconditions (see appendix C)).
  - UE11-12: When the CN gets UE10 with the SDP offer $SDP_{0'}$, it recognizes that resources are now reserved on the MN side. Therefore, it alerts the CN user about the incoming call and sends a SIP RINGING message to the MN.

4.2 Mobility procedure during services in UFA

In the IP-AN//PCC//IMS model, as described in section 2.2, the ISC mobility procedure is incompatible load-based handovers, induces a high handover delay and does not enable service adaptation. Even solutions with proactive step execution and/or context transfer cannot solve efficiently these problems.

UFA mobility procedure, introduced in [38, 80, 81], solves the above problems and brings additional advantages:

- Mobility is controlled, decided and executed by the UFA_GWs. It takes into account different kinds of inputs, including the load information. A UFA_GW_S may decide to hand a MN to a target UFA_GW (UFA_GW_T) because of coverage loss, overload situation or better conditions detected on the UFA_GW_T.
- Mobility is based on a proactive context transfer. It is efficient as all of the contexts to be transferred are co-located in the UFA_GW. Mobility procedure includes two phases:
  - A preparation phase initiated by the UFA_GW_S to the UFA_GW_T, aiming at predetermining:
    * The **service configuration** for SIP native services, or the **SCTP layer configuration** for non-SIP native services, the CN should have after the MN handover. The service configuration contains, among other things, information about the **service adaptation** (i.e. downgrade or upgrade), based on the UFA_GW available resources. The SCTP layer configuration contains, among other things, information about the optimal SCTP congestion control parameters.
    * The **all-OSI layer configuration** the MN should have after its handover. As the UFA_GW implements all layers, determining this configuration is possible.
  - An execution phase aiming at providing the MN and the CN with the predetermined configurations.

  Hence, as for the establishment phase, mobility procedure enables service adaptation for SIP native services or SCTP congestion control parameters tuning for non-SIP native services, according to the UFA_GW_T available resources.
- Mobility procedure is based mainly on SIP and is independent of the radio technology. It can be intra-technology or inter-technology depending on whether the UFA_GW_S and the UFA_GW_T implement the same radio access technology or not.
- Mobility is performed on a per-service basis meaning that: (1) if a given MN has many ongoing services, for each service the MN will receive a dedicated service configuration or SCTP layer configuration, (2) when handover is inter-technology, the UFA_GW_S may decide to only transfer a set of services to a UFA_GW_T. The way to fulfill this objective has been patented in [86, 87], and is integrated in the UFA mobility procedure description provided below.
- Mobility procedure is the same for SIP native and non-SIP native services.

4.2.1 Detailed flow chart for mobility procedure (SIP/non-SIP native services)

The detailed flow chart for UFA mobility procedure is provided hereafter, and is drawn in figures 4.5 and 4.6, respectively for SIP native and non-SIP native services. **It is worth to mention that this procedure is almost the same for the two kinds of services and differ only regarding the use of `SDP` or `SDPN`, that contain respectively information about service adaptation or SCTP congestion control parameters.** For the sake of simplicity, for non-SIP native services, the CN is considered as the sender.

To be generic, it is supposed that the MN have a set of ongoing services and is equipped with two radio access interfaces called Interface_Name_Source and Interface_Name_Target.

The ongoing services pass through Interface_Name_Source attached to UFA_GW_S. During handover, a given service is transferred to UFA_GW_T through Interface_Name_Target.

For the particular case where the MN is equipped with only one interface (Interface_Name_Source=Interface_Name_Target), if there is a need for mobility, all ongoing services are inevitably transferred to UFA_GW_T.

Mobility procedure contains a preparation phase and an execution phase, described hereafter.

A **preparation phase**, including the messages 1-4 in figures 4.5 and 4.6:

1. The MN has, through the UFA_GW_S, an ongoing service described by $\mathtt{SDP_0}/\mathtt{SDPN_0}$ according to the establishment phase described in section 4.1.2. The UFA_GW_S detects the need of handover, it sends to a set of target UFA_GW (UFA_GW_T) candidates a RESOURCE QUERY REQUEST that includes the user profile, part of the authentication context, and the $\mathtt{SDP_c}/\mathtt{SDPN_c}$. This would allow the candidates to propose a service adaptation/SCTP congestion control parameters according to their resources and independently of $\mathtt{SDP_0}/\mathtt{SDPN_0}$.

2. Similarly to the behavior of UFA_GW_S during the service establishment phase (section 4.1.2), each of the UFA_GW_T candidates calculates the `(UFA) policy rules`, mainly the `authorized (IP-AN) QoS` defined in section 3.1.2, corresponding to $\mathtt{SDP_c}/\mathtt{SDPN_c}$ and:

   - For SIP native services, it compares the `authorized (IP-AN) QoS` to its available resources. When the latter is inferior to the former, it proposes a new **service adaptation** by eliminating some of the applications proposed to be part of the service, or tuning their codecs. To do that, it modifies the `SDP` ($\mathtt{SDP_q}$), based on the algorithm provided in section 4.1.2.2.
   - For non-SIP native services, it allocates a bandwidth considering the `authorized (IP-AN) QoS` and the available resources. Then, it determines/tunes **SCTP congestion control parameters** values according to the algorithm provided in section 4.1.2.3. These values enable a rapid and efficient use of the allocated bandwidth. These are inserted in `SDPN` ($\mathtt{SDPN_q}$) within SCTP_optim field (see table 4.1).

   Each of the UFA_GW_T candidate answers with a RESOURCE QUERY RESPONSE containing $\mathtt{SDP_q}/\mathtt{SDPN_q}$.

3. The UFA_GW_S then selects a UFA_GW_T among the UFA_GW_T candidates, based on the $\mathtt{SDP_q}/\mathtt{SDPN_q}$. Then, it pursues handover preparation by transferring authentication and session contexts to the selected UFA_GW_T using CONTEXT TRANSFER message.

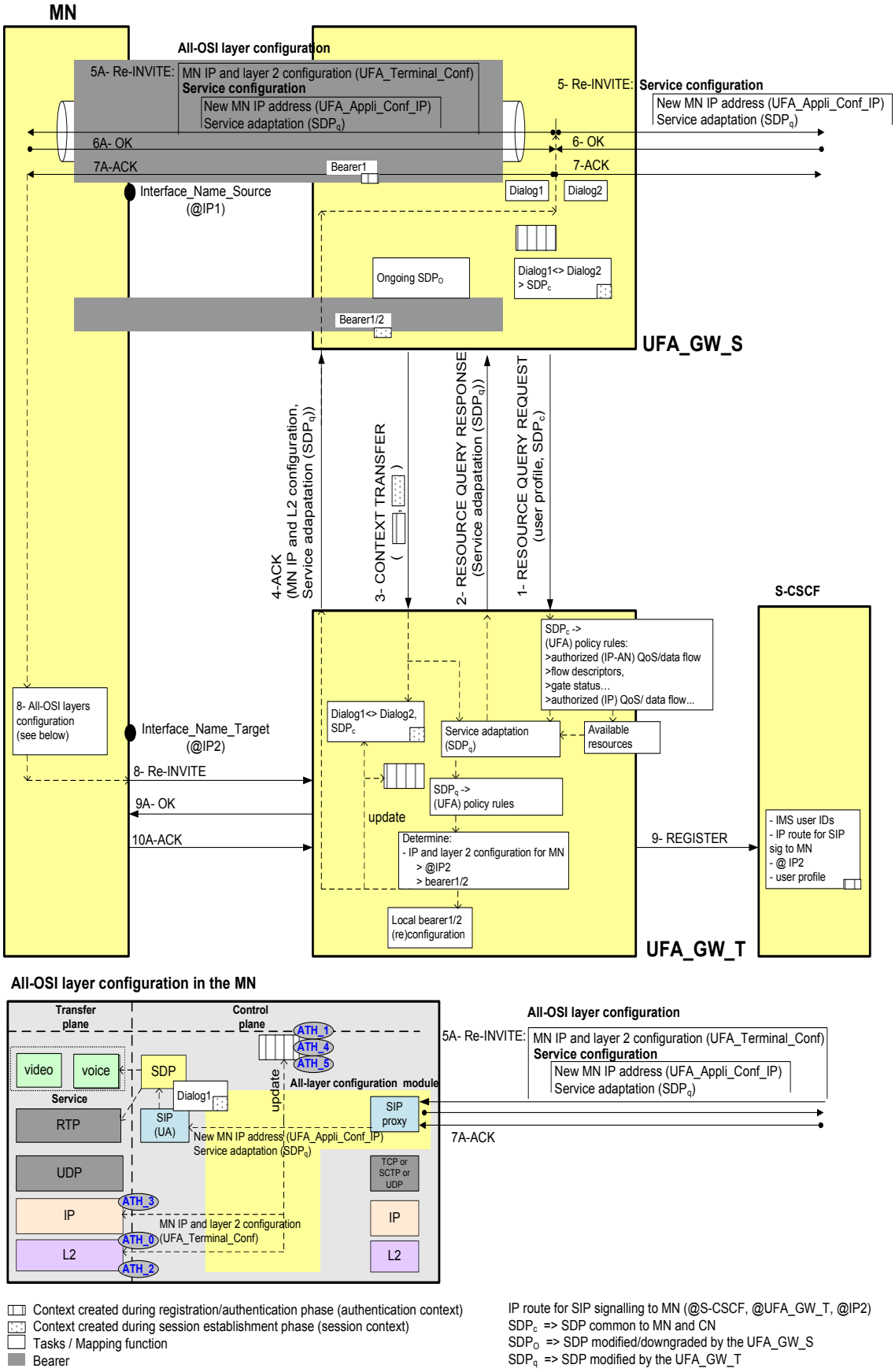


Figure 4.5: Mobility procedure for SIP native services

4. The UFA_GW_T confirms the $\mathtt{SDP_q}$/$\mathtt{SDPN_q}$. It also updates the `(UFA) policy rules` and determines the **MN IP and layer 2 configurations** (defined in table 4.2) necessary for the MN to attach to the UFA_GW_T. When determining the IP configuration, the UFA_GW_T checks the uniqueness of the IP address (@IP2) allocated to the MN .

   Then, based on the MN IP and layer 2 configurations, the UFA_GW_T updates the received contexts. The IPsec SA part of the authentication context is updated as described in [88]. The UFA_GW_T sends back an ACK message containing the MN IP and layer 2 configuration and information about the service adaptation/SCTP congestion control parameters (contained in $\mathtt{SDP_q}$/$\mathtt{SDPN_q}$).

An **execution phase**, including the messages 5A-7A, 5-7, 8-10A in figures 4.5 and 4.6:

5. Based on the received ACK message, the UFA_GW_S builds and sends simultaneously two SIP Re-INVITE messages (5, 5A) to the CN and MN respectively.
   - The SIP Re-INVITE (5) message towards the CN contains information about the **service configuration** for SIP native services, or the **SCTP layer configuration** for non-SIP native services. It concerns:
     - The **new MN IP address** (mainly) that shall be considered by RTP/UDP/IP (for SIP native services) or SCTP/IP (for non-SIP native services) to send and receive data related to the service.
       New MN IP address is contained within a specific SIP header (UFA_Appli_Conf_IP) depicted in table 4.3. Its use by the CN is explained by the same table.
     - The **service adaptation** reflected by $\mathtt{SDP_q}$ for SIP native services; or the **SCTP congestion control parameters** reflected by $\mathtt{SDPN_q}$ for non-SIP native services.
   - The SIP Re-INVITE (5A) message towards the MN contains information about **all-OSI layer configuration**. It concerns:
     - The **MN IP and layer 2 configuration** received by the UFA_GW_S from the UFA_GW_T in ACK message. The elements of this configuration are inserted in a specific SIP header (UFA_Terminal_Conf) depicted in table 4.3. Its use by the MN is also depicted by the same table.
     - The **service**[7] **configuration** for SIP native services, or the **SCTP layer configuration** for non-SIP native services. It concerns:
       * The **new MN IP address** (mainly) as described for message 5. The use of this address by the MN is explained in table 4.3.
       * The **service adaptation** reflected by $\mathtt{SDP_q}$ for SIP native services. For non-SIP native service, **SCTP congestion control** parameters do not need to be configured as the MN is assumed to be the receiver and not the sender.
6. After receiving message 5 (resp. message 5A), the CN (resp. MN) answers using a SIP OK message 6 (resp. message 6A).
7. After receiving message 6 (resp. message 6A) from the CN (resp. MN), the UFA_GW_S answers to the CN (resp. MN) with SIP ACK message 7 (resp. message 7A).

[7] means all applications constituting the service.

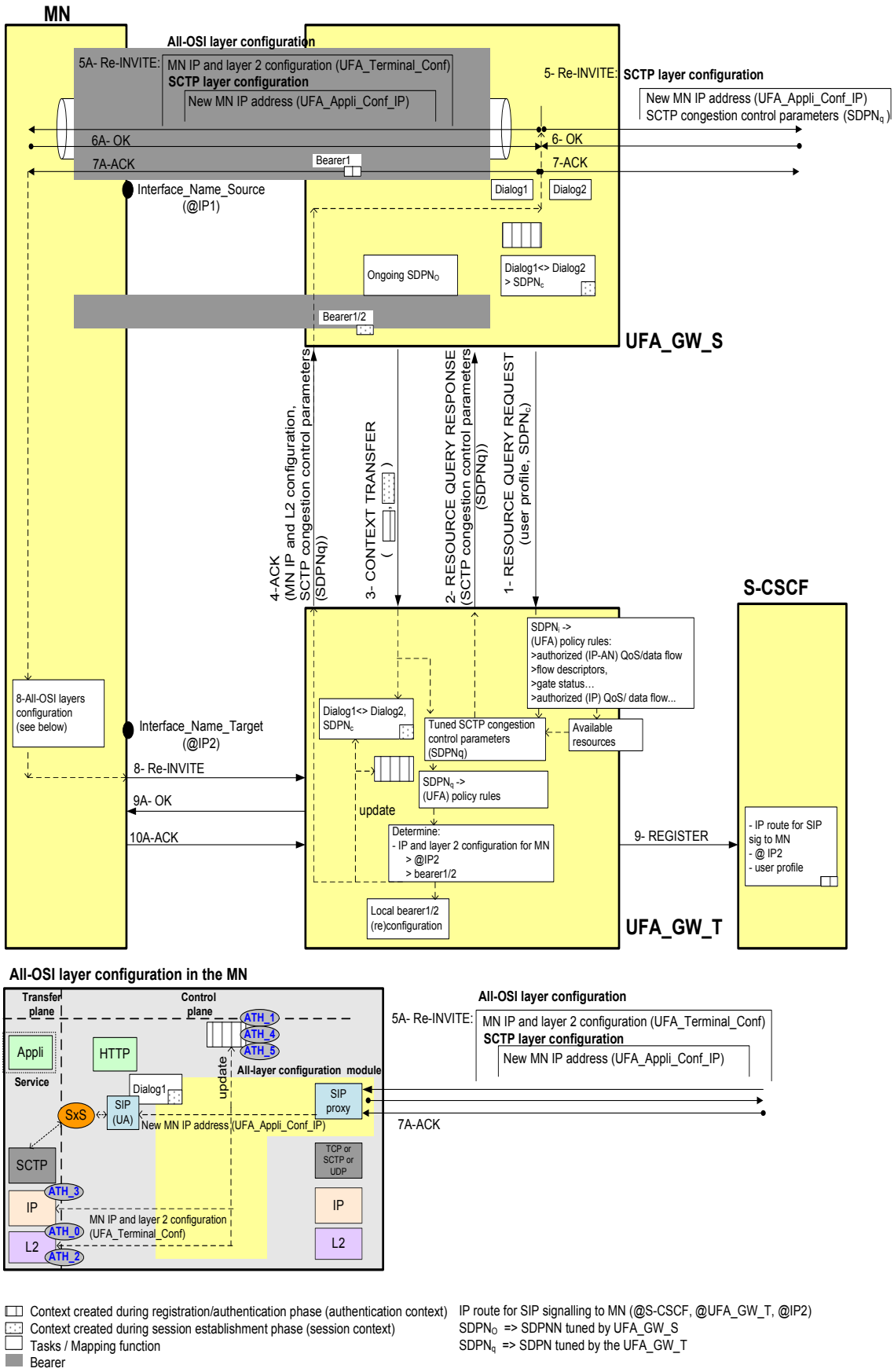


Figure 4.6: Mobility procedure for non-SIP native services

Field	Meaning
Interface_Name_Target	The interface to be activated on the MN to handle the service subject to handover. This interface will be attached to UFA_GW_T.
>UFA_GW_T_MAC_Addr >UFA_GW_T_IP_Addr >UFA_GW_T_IP_Local Addr >UFA_GW_T_Netmask >Add_IP_Addr (=@IP2) >UFA_GW_T_ESSID >UFA_GW_T_Channel >bearer2	These fields give the **MN IP and layer 2 configurations** necessary for MN Interface_Name_Target to attach to UFA_GW_T at the IP and layer 2 levels. These fields are used as follow: -UFA_GW_T_MAC_Addr, UFA_GW_T_IP_Addr and UFA_GW_T_IP_Local Addr are used to configure the MN neighbor table [56]. -UFA_GW_T_IP_Addr and UFA_GW_T_Netmask are used to configure the default IP route. -Add_IP_Addr is the new MN address (@IP2) on Interface_Name_Target. -the layer 2 example considered here is WiFi.
Interface_Name_Source	The current MN interface that handles the service subject to handover.
>Del_IP_Addr	0 or 1 -If 0, this field indicates that the current IP address (Del_IP_Addr) on the Interface_Name_Source shall not be removed. This occurs when other services are kept on this interface.

Table 4.2: UFA_Terminal_Conf header

Field	Applicability	Meaning
Add_IP_Addr (=@IP2)	SIP native services non-SIP native services	The new MN IP address. This field gives the new MN IP address after attachment to UFA_GW_T -For MN this address can be used by RTP/UDP/IP or SCTP/IP as a source address. -For CN, this address shall be considered by the RTP/UDP/IP or SCTP/IP layer as the MN destination address. For SIP native services, this information is also in the 'c' filed of `SDP`.
Del_IP_Addr	only non-SIP native services (concerns SCTP layer)	This field is related to the current MN address (@IP1). As SCTP supports multihoming, adding a new IP address (@IP2) to the SCTP association do not remove the current IP address (@IP1). However, during mobility, @IP1 is no more available. This field indicates explicitly the action of keeping or deleting @IP1 in the SCTP association. -If it is equal to 1, it indicates that @IP1 on MN is no more available, i.e. for MN, this address shall no more be used as a source address; and for CN, this address shall no more be used as a destination address => SCTP association shall be updated with this information. -If it is equal to 0, it indicates that @IP1 on MN is still available, i.e. for MN, this address can be still used as a source address; and for CN, this address can still be used as a destination address => SCTP association shall be updated with this information.

Table 4.3: UFA_Appli_Conf_IP header

8. When the CN receives message 7, it configures its service/SCTP layer with the received configuration, and begins sending data to the new MN address. For non-SIP native services, the CN first transmits the data not acknowledged (transmitted but not acknowledged as it may be lost during handover), then new data (never transmitted) (explanation is given in chapter 7, more specifically in section 7.5).

When the MN receives message 7A, it configures its OSI layers according to the information received in message 5A and updates authentication and session contexts (figures 4.5 and 4.6).

The MN then sends a SIP Re-INVITE message to the UFA_GW_T to indicate its attachment.

9. When the UFA_GW_T detects the MN attachment, it sends a SIP REGISTER message to the S-CSCF to update the authentication context.

To decrease packets losses during handover, after UFA_GW_S sends message 5A to the MN telling it to attach to UFA_GW_T, it **forwards** the data received from the CN to UFA_GW_T. UFA_GW_T **buffers** all data received from UFA_GW_S and CN until the MN attachment (i.e. reception of message 8).

4.3 Conclusion

This chapter has specified the service access procedure, including the registration/authentication and the service establishment phases, and the mobility procedure for UFA. Many aspects of these procedures are naturally optimized, due to UFA properties consisting in gathering the main network functions in the UFA_GW.

In the registration/authentication phase, inspired from the I-WLAN//PCC//IMS model, radio-independent methods and IP-based protocols have been chosen to make UFA network convergent. The co-location of the P-CSCF and the first IP router in the UFA Gateway (UFA_GW), has enabled to reduce the number of messages to perform this phase and to share the same IPsec Security Association for SIP (IMS) and and user data.

The service establishment phase is defined for SIP native and non-SIP native services. For non-SIP native services, the contribution is related to two independent aspects: the first one is to make these services controlled by SIP, thanks to the introduction of the SIPcrossSCTP module both in the Mobile Node and Correspondent Node, and the second aspect is to tune SCTP congestion parameters using the network-based UFA mechanisms. The service establishment phase is based on a single step allowing at the same time to: (1) adapt the service or tune SCTP congestion control parameters, based on the UFA_GW available resources, and (2) configure the necessary resources in the network. These allow, among other things, to reduce the service establishment delay.

The mobility procedure for UFA is optimal, as the contexts generated by the registration/authentication and the service establishment phases are mostly gathered in the UFA_GW. Mobility procedure is simple and consists in transferring proactively the contexts located in the source UFA_GW to the target UFA_GW, and in updating these contexts with the new MN configuration determined by the target UFA_GW.

Part III

Evaluation of UFA model

CHAPTER 5 Performance of service establishment in UFA

As stated in chapter 2 section 2.1.3, one of the IP-AN//PCC//IMS main disadvantages, is the long service establishment delay, caused by the high number of node types and its centralized and hierarchical architecture. Chapter 3 has defined a flat model (UFA), whose one of the requirement is to reduce the service establishment delay.

The objective of this chapter is to quantitatively compare the service establishment delay in IP-AN//PCC//IMS and UFA [85]. It is also to prove the IP-AN//PCC//IMS scalability issues and the negative impact of its centralized and hierarchical architecture on the service establishment delay. For this purpose, the service establishment delay is measured for different network load situations. UMTS is considered as an IP-AN example.

This chapter is organized as follows: section 5.1 defines the service establishment delay; section 5.2 models the node delay, which is an important service establishment delay component that depends on the network load; section 5.3 evaluates the service establishment delay in both UMTS//PCC//IMS and UFA, and finally section 5.4 provides a conclusion.

5.1 Service establishment delay

5.1.1 Definition and requirements

The message flow for the service establishment phase is shown in figure 2.4 for UMTS//PCC//IMS, and in figure 4.4 for UFA. To be generic, the MN and CN are both supposed to be connected to a mobile network, as indicated in figure 5.1.

ITU [89] defines the service establishment delay as the time perceived by the caller, between the initiation of the call and the reception of the ringing tone from the called party. This delay is also called Post-Dialing Delay (PDD). According to this definition, the service establishment delay, in our case, is the delay between the SIP INVITE message and the SIP RINGING message.
The upper bound of this delay for circuit switched calls is fixed by ITU [89] to 3.0s, 4.0s and 7.9s respectively for local, national and international calls.

5.1.2 Components

As shown in figures 2.4 and 4.4, the service establishment phase involves a set of SIP and Diameter [67, 69] messages. For the sake of simplicity, the term "signalling" is used for these messages.

The service establishment delay is divided into four components:

1. The radio delay component, that is due to the transmission on the radio interface of all signalling messages involved in the service establishment phase.
2. The network delay component, that is due to the transmission on the network interfaces of all signalling messages involved in the service establishment phase (from the NB to the GGSN on the MN and CN sides, and in the backbone connecting the MN and CN mobile networks).
3. The resource reservation delay component, that corresponds to the 4th step of the service establishment phase in UMTS//PCC//IMS (Estb_4 in figure 2.4), and to the step local bearer1/2 reconfiguration of the service establishment phase in UFA (UE7 in figure 4.4).
4. The node delay component, that is introduced by all of the network nodes while treating the signalling messages involved in the service establishment. It is the sum of node delay per node and message defined in section 5.2.

Figure 5.1 illustrates the radio, network and node delay components.

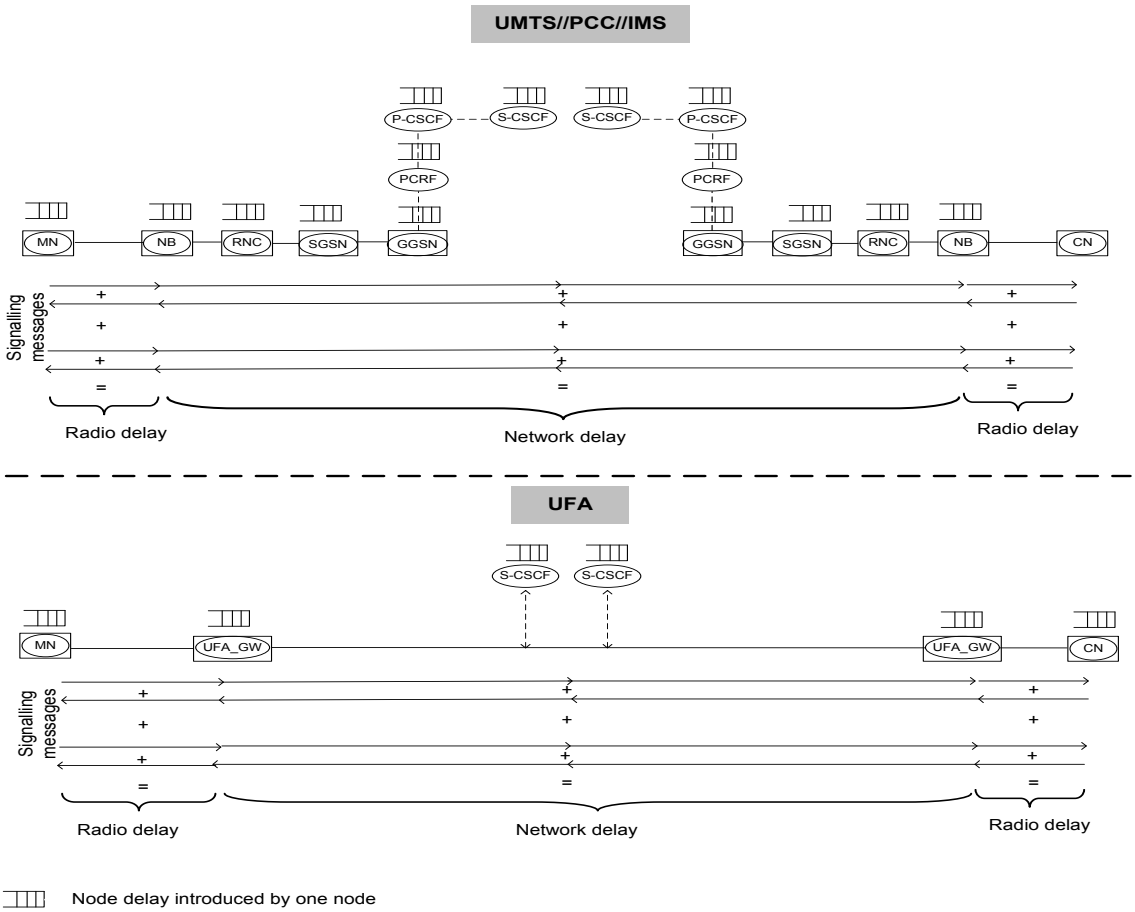


Figure 5.1: Radio, network and node delay components within the service establishment delay

To determine the impact of the IP-AN//PCC//IMS centralized architecture, the service establishment delay is studied for different network load situations i.e. different numbers of service requests. On the contrary to the radio, network and resource establishment delays[1], the node delay is the only delay impacted by the network load.

5.2 Node delay per node and message (D_{sig})

When a given signalling message is received by a node, it is first queued then it is processed. The delay between the moment the message arrives in the node queue and the moment it is completely processed, is called the **node delay per node and message** and noted as $\mathbf{D_{sig}}$. The more the queue contains signalling messages, the higher D_{sig} is. As performed in [90, 91, 92] for a similar problem, D_{sig} is estimated using classical queuing theory.

Nodes within the UMTS//PCC//IMS and UFA models are divided into two categories, depending on the number of traffic types they treat, and the traffic type priorities:

1. Nodes treating signalling messages only (such as the P-CSCF, S-CSCF and PCRF). Assuming Poisson arrivals and Poisson processing times for service requests, the queue in these nodes for the SIP INVITE message (initiating the service) can be modeled by M/M/1.
2. Nodes treating signalling and transfer plane traffics (such as the MN, CN, NB, RNC, SGSN, GGSN and UFA_GW). According to 3GPP specifications [22, 51], signalling shall be mapped on the interactive class. Therefore, it has a lower priority than the conversational and streaming traffics. For such situation of priority-based queues, Poisson arrivals and General distribution of processing times for service requests are more realistic. Thus, the queue in these nodes for the SIP INVITE message can be modeled by M/G/1.

For the sake of simplicity, signalling messages like the SIP SESSION PROGRESS, SIP PRACK, etc. are assumed to have the same node delay as the SIP INVITE message [90, 91, 92]. Note that this assumption is not very rigorous, as the poisson process (applying for the SIP INVITE message) supposes that events are memoryless, whereas the stated messages are dependent on each other, e.g. they are triggered by the SIP INVITE message.

Formulas for the SIP INVITE message node delay per node are given below, based on the parameters defined in table 5.1. In that table, the traffic $\boldsymbol{p}$, having a priority higher than the signalling traffic one, has a constant load ρ_p. This assumption, considered also in [90, 91, 92], is just for simplification. Indeed, this traffic may be generated by the service requests we are considering (e.g. a VoIP request generates VoIP traffic). In this case, it would be variable and depends on the service request arrival rate (λ_{sig}) and on the bitrate they generate on the transfer plane.

1) In a node with M/M/1 queue, the node delay for a SIP INVITE message is [93, 94]:

$$D_{sig} = \frac{1}{\mu_{sig} - \lambda_{sig}} = \frac{1}{1 - \rho_{sig}} \tag{5.1}$$

2) In a node with M/G/1 queue with a pre-emption[2], the node delay for a SIP INVITE message in presence of a traffic with a higher priority, is [93, 94]:

[1] assuming interfaces dimensioned for a given number of service requests.

[2] In a preemptive priority queue, if a job arriving at the queue finds a job of lower priority in service, the arriving job preempts the job being served and begins service immediately. A preempted job will resume service, at the point at which its service was suspended, as soon as there are no higher priority jobs remaining in the queue.

Parameter	Definition
λ_{sig}	The service request (SIP INVITE messages) arrival rate within a node.
μ_{sig}	The service request (SIP INVITE messages) processing rate within a node. $1/\mu_{sig}$ is the processing delay and represents the node rapidity (CPU) to execute different tasks for a given signalling message.
ρ_{sig}	The load of SIP INVITE messages within a node. It is given by $\rho_{sig} = \lambda_{sig}/\mu_{sig}$.
μ_p	The processing rate within a node of the traffic p having a higher priority than the signalling traffic. $1/\mu_p$ is the processing delay.
ρ_p	The load within a node of the traffic p having a higher priority than the signalling traffic.

Table 5.1: Node delay parameters

$$D_{sig} = \frac{1/\mu_{sig}(1-\rho_p-\rho_{sig})+R}{(1-\rho_p)\times(1-\rho_p-\rho_{sig})} \tag{5.2}$$

$$R = 1/2(\lambda_p\overline{S_p^2} + \lambda_{sig}\overline{S_{sig}^2}) \tag{5.3}$$

$\overline{S_{sig}^2}$ is the second moment of $1/\mu_{sig}$, it is given by $\overline{S_{sig}^2}$=$v(S_{sig})$+ $[E(S_{sig})]^2$=$[E(S_{sig})]^2(1+c_v^2)$, where $v(S_{sig})$ is the variance and c_v is the deviation coefficient. The same applies for $\overline{S_p^2}$. We [90, 91, 92] assume that c_v =0.05, which gives:

$$R = 0.501(\rho_p/\mu_p + \rho_{sig}/\mu_{sig}) \tag{5.4}$$

The above formula give the node delay per node and message, considering λ_{sig} as the service request arrival rate within a node. For the $Node_x$, the arrival rate $\lambda_{sig}^{Node_x}$ depends on the number ($N^{Node_{x-1}}$) of $Node_{x-1}$ connected to this node, and on the arrival rate ($\lambda_{sig}^{Node_{x-1}}$) of the messages in $Node_{x-1}$ (figure 5.2). It is given by:

$$\lambda_{sig}^{Node_x} = N^{Node_{x-1}} * \lambda_{sig}^{Node_{x-1}} \tag{5.5}$$

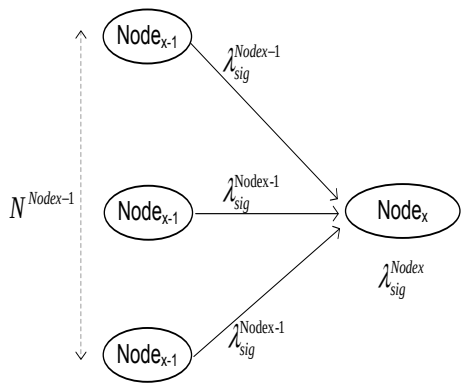


Figure 5.2: Service requests arrival rate within a node

5.3 Service establishment delay evaluation in UMTS//PCC//IMS and UFA

In this section, the service establishment delay is evaluated for UMTS//PCC//IMS and UFA, using Matlab simulations [95].

All messages shown in figures 2.4 and 4.4 are considered. Parallel messages or steps indicated in the message flows are not counted.

5.3.1 Inputs

Simulations are based on the inputs given in table 5.2. The setting of these inputs is explained by:

- **Number of nodes** ($N^{Node_{x-1}}$): typical values are used, based on a real network deployed by an operator.
- **signalling processing delay** ($1/\mu_{sig}$): the values considered are based on inputs provided by the constructors.
  - The signalling processing delay is high in the nodes P-CSCF, PCRF, S-CSCF, as they implement SIP or Diameter layer and execute at these layers an important number of time-consuming tasks, for each received signalling message. In the P-CSCF and PCRF, the values take also into account the conversion SIP-Diameter and vice-versa.
    In the other nodes, like the NB, RNC, SGSN and GGSN, the signalling processing delay is on the contrary low, as these nodes only execute layer 2 and IP related tasks with regard to signalling messages.
  - The signalling processing delay is higher in the UFA_GW than in the other nodes (e.g; P-CSCF in UMTS//PCC//UMTS), as SIP, IP and layer 2 are present in this node.
- ***p* traffic processing delays** ($1/\mu_p$): the values considered are based on inputs provided by the constructors.
- **Resource reservation delay**: in UMTS//PCC//IMS, the value considered is based on measurements carried out on a deployed network. In UFA, this delay can be null as the bearer1/2 (re)configuration (see figure 4.4) is executed in parallel to other messages. However, it is set to 0.5s as a maximal value.
- **Network delay**: this delay corresponds to local or national calls.

5.3.2 Numerical results

Generally, the capacity of an equipment can be evaluated from: (1) a QoS point of view i.e. the maximum number of service requests for which a certain QoS (bandwidth, service establishment delay) can be guaranteed, or (2) a load point of view i.e. the maximum amount of traffic not causing the equipment overload (ρ>1).

The NB or UFA_GW capacity from a QoS point of view is about 200[3] services. However, such a value could not be tested for the evaluation of the service establishment delay in UMTS//PCC//IMS, since the P-CSCF becomes overloaded with 111360 service requests per hour, generated by **120** service requests in the NB or UFA_GW.

[3]considering HSPA technology and for a VoIP service

Parameter	**UMTS//PCC//IMS**								**UFA**		
Node	**MN**	**NB**	**RNC**	**SGSN**	**GGSN**	**P-CSCF**	**PCRF**	**S-CSCF**	**MN**	**UFA_GW**	**S-CSCF**
$N^{Node_{x-1}}=$ number of $Node_{x-1}$ per $Node_x$	x (N1)	58 NB per RNC	4 RNC per SGSN	4 SGSN per GGSN	1 GGSN per P-CSCF	1 P-CSCF	1 PCRF per P-CSCF	1 S-CSCF per P-CSCF	x (N1)	928 UFA_GW per S-CSCF	1
λ_{sig} (per hour)	λ_{sig}^{MN} (N1)	λ_{sig}^{NB} 1..120	(N2)	(N2)	(N2)	(N2)	(N2)	(N2)	λ_{sig}^{MN}	$\lambda_{sig}^{UFA_GW}$ 1..120	(N2)
$1/\mu_{sig}$(ms)	10	2	5	5	8	30	30	10	10	40	10
$1/\mu_p$(ms)	5	2	5	5	8	NA	NA	NA	5	10	NA
ρ_p	0.7	0.7	0.7	0.7	0.7	NA	NA	NA	0.7	0.7	0.7
Radio bitrate (kbps)	128		NA	NA	NA	NA	NA	NA	128		NA
signalling messages length (bytes)	calculated for each message based on [57] that gives signlalling flows										
Network delay (ms) (N3)	70								70		
Resource establishment delay (s)	2.5								0.5		

Notes:
(N1): x and λ_{sig}^{MN} are such that they respect: x* $\lambda_{sig}^{MN} = \lambda_{sig}^{NB}$ or $\lambda_{sig}^{UFA_GW}$
(N2): deduced based on $\lambda_{sig}^{Node_x}=N^{Node_{x-1}} * \lambda_{sig}^{Node_{x-1}}$ (equation 5.2)
(N3): defined for one message and on one side (MN or CN) e.g. from NB to GGSN + backbone part, or from UFA_GW to the backbone.

Table 5.2: Simulation inputs

Therefore, first of all the service establishment delay in UMTS//PCC//IMS and UFA are compared, considering 120 service requests in the NB and UFA_GW maximum. Then, as the UFA_GW implements the P-CSCF and GGSN functions, its capacity from a load point of view, is evaluated and compared to the P-CSCF and GGSN ones in UMTS//PCC//IMS.

Figure 5.3 shows the service establishment delay for UMTS//PCC//IMS and UFA, and figure 5.4 shows the components of this delay (radio, network, resource reservation and node delay, as defined in section 5.1.2).

- The service establishment delay in UMTS//PCC//IMS evolves from 8s to 18s; whereas it remains almost constant in UFA (4,2s). Thus, UFA enables at least a delay reduction of 50%.
- The radio and network delay components in UFA, are lower than the ones in UMTS//PCC//IMS, as less messages are required in the UFA service establishment phase. Indeed, comparing figures 2.4 and 4.4, it can be deduced that UFA enables to save 6 Diameter messages, Estb_4 step and 2 SIP messages.
- The node delay component is the highest component among all of the service establishment delay components, for UFA and UMTS//PCC//IMS.

  The node delay component is higher in UMTS//PCC//IMS than in UFA, as the centralized nodes in the UMTS//PCC//IMS model have to treat an important number of service requests.

Delays interpreted above are due to all messages involved in the service establishment phase. Delays for a specific message are also studied. The SIP SESSION PROGRESS message is chosen, as it is treated by all nodes[4] in the UMTS//PCC//IMS model.

[4]It is considered that this message is also treated also by the PCRF. The conversion SIP-Diameter is taken into account in the processing delay value

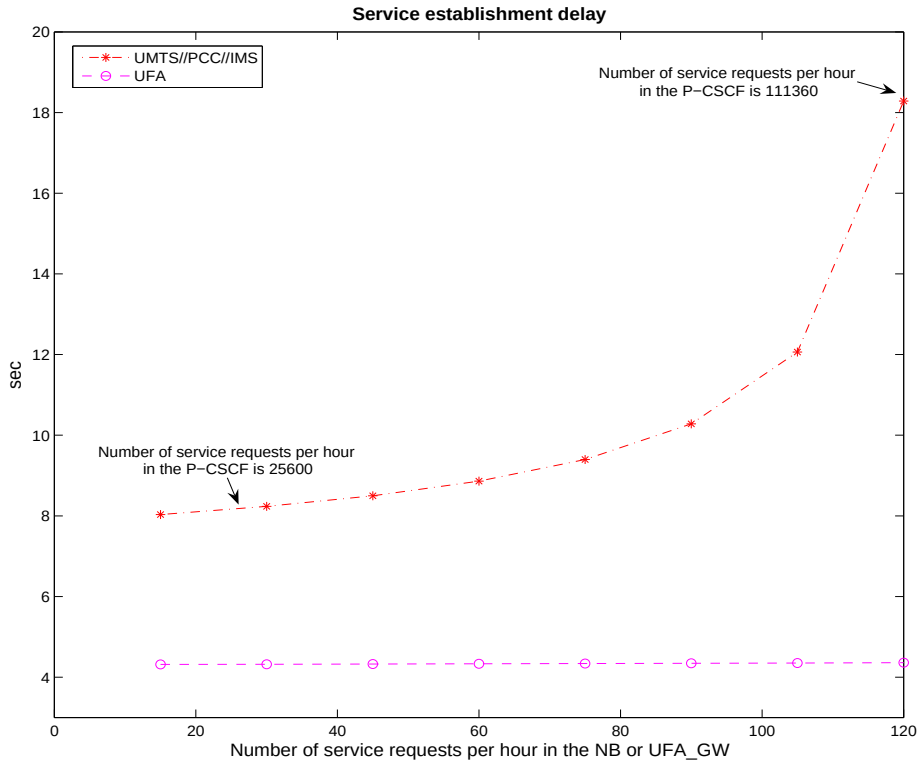


Figure 5.3: Service establishment delay in UMTS//PCC//IMS and UFA

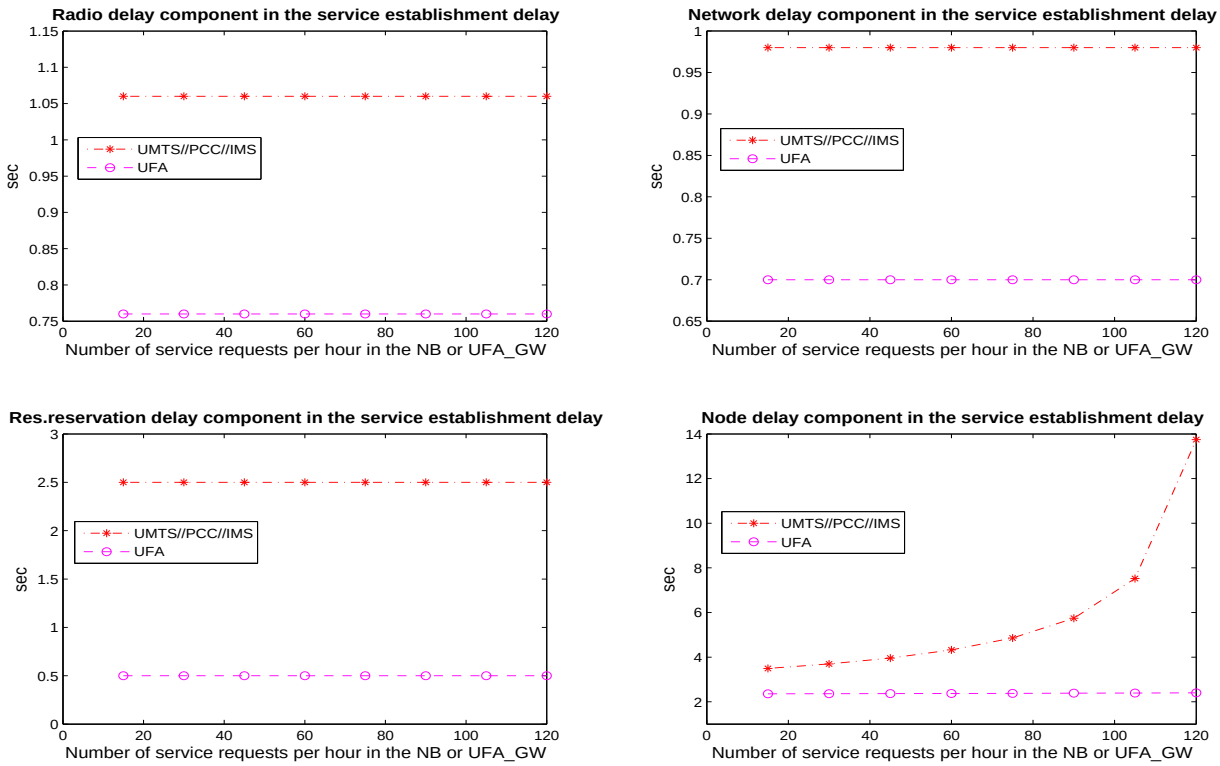


Figure 5.4: Components of service establishment delay in UMTS//PCC//IMS and UFA

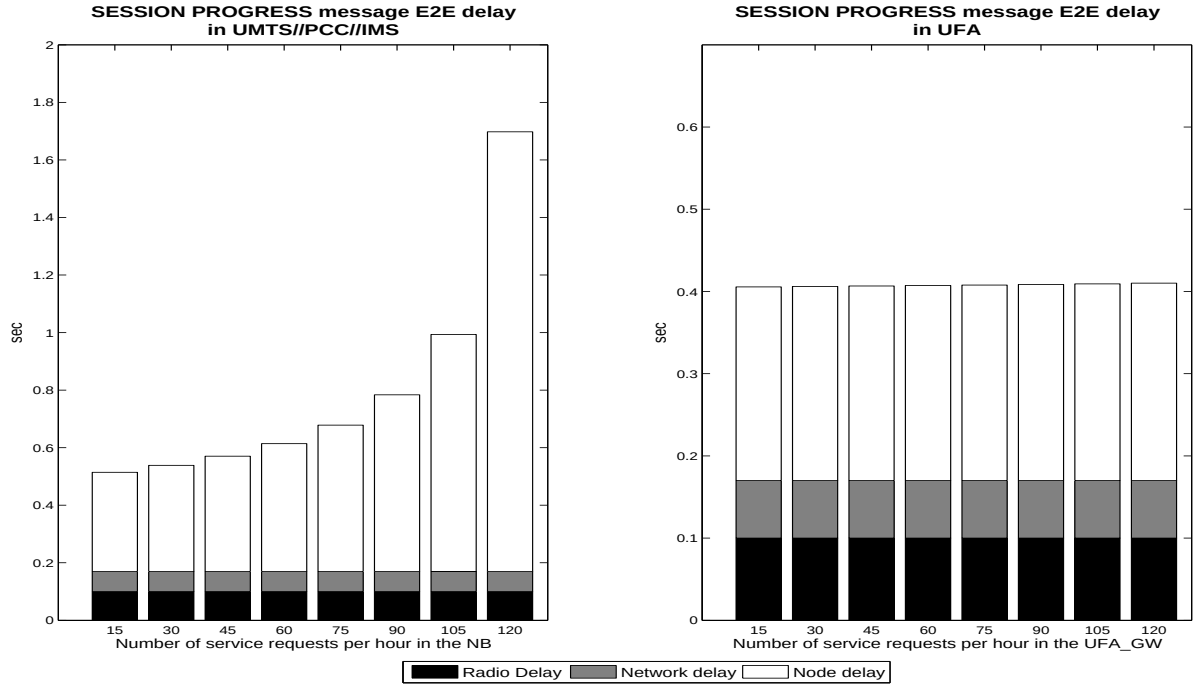


Figure 5.5: SESSION PROGRESS message end-to-end delay in UMTS//PCC//IMS and UFA

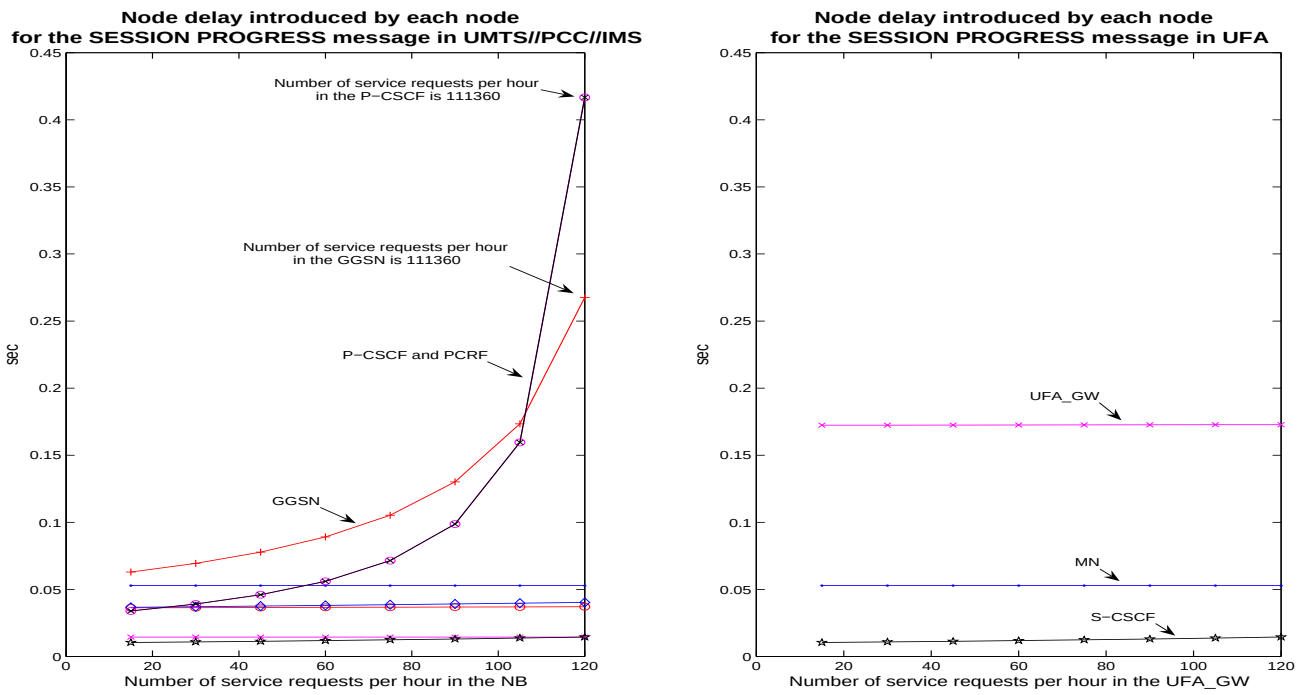


Figure 5.6: Node delay introduced by each of the UMTS//PCC//IMS nodes and UFA nodes for the SESSION PROGRESS message

Figure 5.5 illustrates the end-to-end delay[5] and the delay components for the SIP SESSION PROGRESS message. Figure 5.6 shows the node delay introduced by each node (NB, RNC, ...), for the SIP SESSION PROGRESS message.

Figure 5.5 shows that the node delay introduced by the sum of all nodes is an important component in the SESSION PROGRESS message end-to-end (E2E) delay. Figure 5.6 shows that although the P-CSCF and PCRF in UMTS//PCC//IMS are dedicated to signalling traffic only, the node delays they have introduced are high. These delays are the highest ones compared to those introduced by the other nodes, and increase exponentially when the service request number increases. As explained before, this is due to the fact that these nodes are centralized i.e. receive a high amount of service requests. Indeed, 120 service requests per NB generates 111360 service requests in the P-CSCF and PCRF. Moreover, the high signalling processing delay in these nodes, impacts the node delay they introduce.
The node delay introduced by the GGSN is also high. The first reason is that the GGSN receives a high amount of service requests (120 service requests per NB generates 111360 service requests in the GGSN). The second reason is that the GGSN treats, in addition to signalling, a high load of traffic (ρ_p =0.7), having a priority higher than the signalling one. It has been checked that when ρ_p =0.5, the node delay introduced by the GGSN becomes lower.

On the contrary to the P-CSCF, PCRF and GGSN, the UFA_GW introduces a relatively constant node delay (figure 5.6). Indeed, signalling traffic is due to 120 service requests only. Moreover, its related traffic is not important compared to the traffic p load (ρ_p =0.7).

Going back to figure 5.3, in UFA, the service establishment delay is a bit higher than the ITU recommendations for circuit switched local calls (3s). In UMTS//PCC//IMS, the service establishment delay is much higher than the ITU recommendations even for a low number of service requests (8s for 20 service requests per NB). Moreover, it increases rapidly (18s for 120 service requests per NB), as the P-CSCF, PCRF and GGSN introduce a high node delay. To prevent this delay from being very high, the number of service requests treated by the P-CSCF, PCRF and GGSN has to be reduced. This means that the operator shall deploy more P-CSCFs and GGSNs, confirming thus the UMTS//PCC//IMS scalability issues. This also means that the P-CSCF, PCRF and GGSN have a capacity limited by the service establishment delay requirement.

As presented in the beginning of this section, the P-CSCF in UMTS//PCC//IMS becomes overloaded for a number of service requests near 111360. As the UFA_GW implements P-CSCF and GGSN functions, in the following, the UFA_GW capacity from a load point of view is evaluated and compared to the P-CSCF and GGSN ones in UMTS//PCC//IMS.

Figure 5.7 gives the node delay introduced by the UFA_GW for the SESSION PROGRESS message. The UFA_GW becomes overloaded for a number of requests near 25600[6]. This capacity is lower than the P-CSCF one, since the UFA_GW treats, in addition to signalling, a high load of traffic (ρ_p =0.7), having a priority higher than the signalling one. The UFA_GW capacity is also lower than the GGSN one (>111360[7]). This is due to the fact that the signalling processing delay in the GGSN is lower than in the UFA_GW.

Figure 5.8 shows that the service establishment delay for UFA remains below 6s for a number of service requests around 18000 service requests. This result is given for information, as in any way the UFA_GW will not treat such amount of service requests. Indeed, it is limited by its physical (radio) capacity (the UFA_GW acts as a connectivity node).

[5] from CN to MN
[6] a higher number of service requests leads to have ρ>1
[7] for 111360 service requests in the GGSN, ρ<1

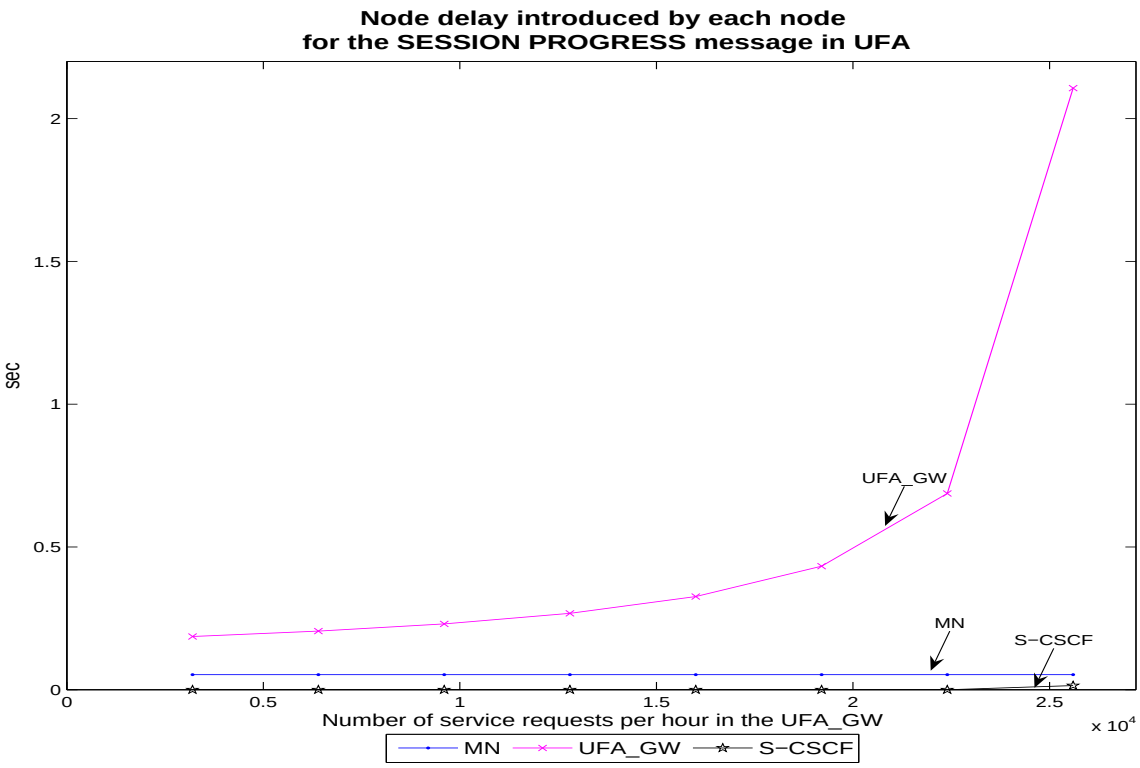


Figure 5.7: Node delay introduced by each of the UFA nodes for the SESSION PROGRESS message, in case of a high number of service requests

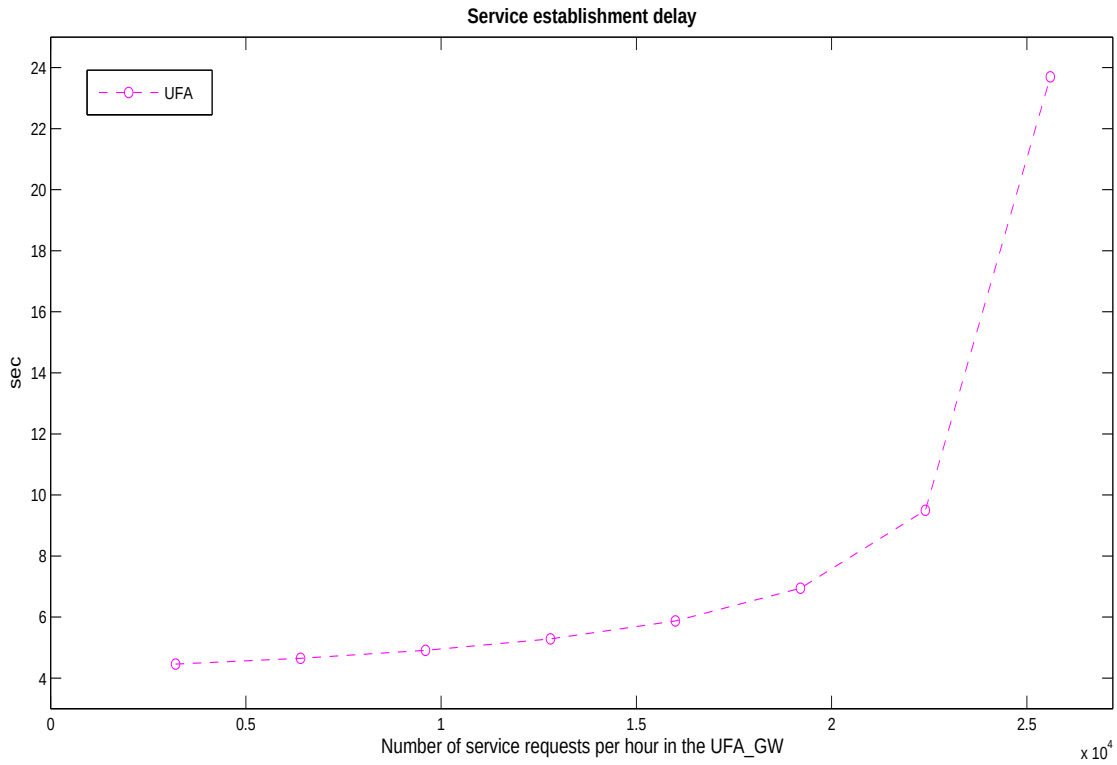


Figure 5.8: Service establishment delay in UFA in case of a high number of service requests

5.4 Conclusion

In this chapter, the service establishment delay is evaluated in both IP-AN//PCC//IMS and UFA models, for different network load situations. This evaluation has proved the IP-AN//PCC//IMS scalability issues and the negative impact of its centralized and hierarchical architecture on the establishment delay. Indeed, this latter increases exponentially when the number of service requests increases. On the contrary, in UFA, the service establishment delay is not very sensitive to the number of service requests.

Additionally, this evaluation has emphasized the benefits of UFA compared to IP-AN//PCC//IMS. Firstly, UFA enables a reduction of 50% in terms of service establishment delay in low load situations and much more in high load situations. Secondly, the UFA Gatway capacity is limited by the physical connectivity and not the service establishment delay (QoS) requirmements, contrary to IP-AN//PCC//IMS network whose capacity is limited by the service establishment delay requirments.

CHAPTER 6 Implementation and performance of UFA mobility procedure for SIP native services

Chapter 2 has outlined the issue of a long handover delay in the ISC mobility procedure used with the IP-AN//PCC//IMS model, and chapters 3 and 4 have defined the UFA model enabling the reduction of this delay. The objective of this chapter is to compare the handover delays in these two models, and therefore to further prove the feasibility of UFA concepts. For these purposes, a testbed is used to implement UFA and a simplified version of ISC mobility procedure, called here **Implemented ISC**.

This chapter is organized as follows. Section 6.1 describes the Implemented ISC and compares it with UFA in terms of implementation cost and handover delay components. Section 6.2 describes the testbed. Section 6.3 provides hints on the testbed configuration and implementation. Section 6.4 briefly speaks about the testbed message flow traces. Section 6.5 compares the handover delays in UFA and Implemented ISC, considering low-delay links. It also provides the UFA handover delays as measured on the testbed for different network scenarios, corresponding to different link delays. To validate these measurements, they are compared to analytical values obtained through mathematical formulas modeling the handover delay. Finally, section 6.6 concludes.

6.1 Implemented ISC and UFA and their handover delay components

Implemented ISC is a simplified version of the whole ISC mobility procedure provided in section 2.2 and illustrated in figure 2.9. It does not implement either the IMS functions (P-CSCF, S-CSCF) or the SCC AS ones, but just a simple mobility procedure similar to the one described in section A.3. Table 6.1 positions the Implemented ISC mobility procedure compared to the whole ISC one, in terms of executed steps.

Implemented UFA contains the nodes defined in section 3.2, except the SIPcrossSCTP Gateway as we are not dealing with the non-SIP native services. Regarding the UFA Gateway (UFA_GW), composed of the Back-to-Back User Agent (B2BUA) and the Controller, it does not implement: the P-CSCF functions, the radio sub-module responsible for collecting radio measurements from the Mobile Nodes (MN), and the resource information sub-module. UFA service establishment and mobility procedures, described in sections 4.1.2 and 4.2, are implemented except the service

adaptation function and messages 3-RESOURCE QUERY REQUEST and 4-RESOURCE QUERY RESPONSE of the mobility procedure. Data transfer between the UFA Gateways, and data buffering in the Target Gateway (UFA_GW_T) during the the Mobile Node mobility are not implemented.

In terms of implementation cost, Implemented ISC has required 2650 line codes in the terminal (MN/CN). UFA has required 2900 and 5300 line codes respectively in the terminal and the UFA Gateway. This means that the UFA implementation cost is 309% higher than the Implemented ISC, which isn't considered as being very expensive, given the various advantages of UFA compared to ISC, as discussed in chapters 3 and 4.

Implemented ISC and UFA are compared in terms of handover delays. To measure these delays, the hard handover case is considered as it is the most restricting one (see section 2.2.2.2). The handover delay is measured at the application level (**Appli_HO_Delay**). It is the delay in the MN between the last application data (D) packet received before handover, and the first application data packet received after handover.

To allow a deep analysis of UFA and implemented ISC, the components of their handover delays defined in table 6.1 and shown in figures 6.1 and 6.2, are evaluated.

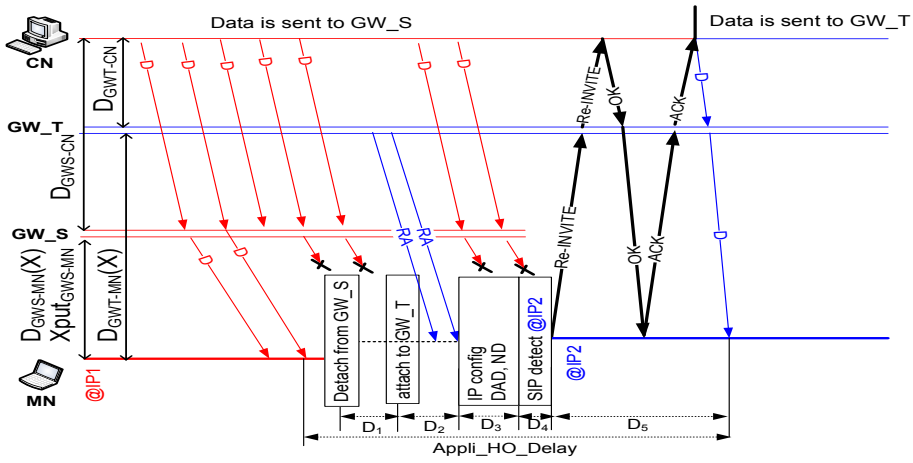


Figure 6.1: Handover delay components in Implemented ISC mobility procedure

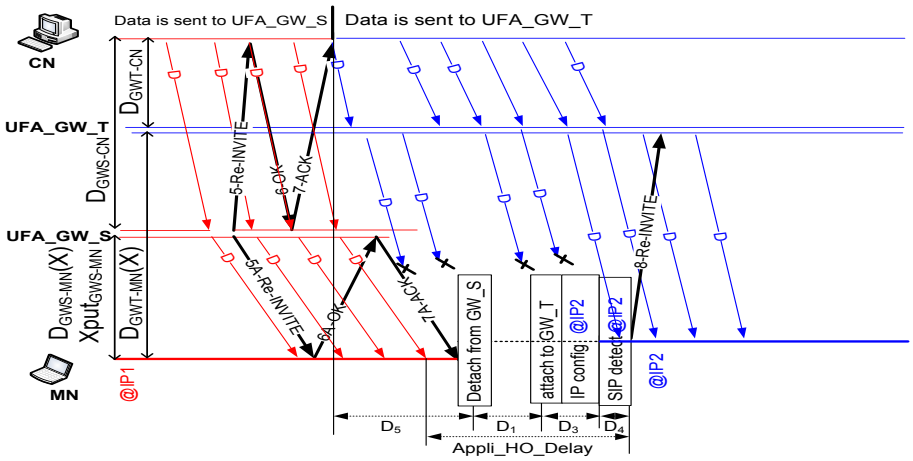


Figure 6.2: Handover delay components in UFA mobility procedure

	Implemented ISC			UFA
	Whole ISC procedure (figure 2.10)	**Implemented ISC compared to whole ISC**	**Handover delay components in Implemented ISC (figure 6.1)**	**Handover delay components in UFA (figure 6.2)**
Phase 1	**ATH_0**: layer 2 attachment to IP-AN	Implemented (see section 6.3.1)	$\mathbf{D_1}$: the time necessary for the MN to configure its layer 2 and attach to the target Gateway.	$\mathbf{D_1}$: the time necessary for the MN to configure its layer 2 and attach to the Target UFA Gateway.
	ATH_1: registration /authentication to IP-AN	Not implemented		
	ATH_2: bearer establishment for SIP signalling	Not implemented		
	ATH_3: IP address acquisition	stateless IPv6 configuration (see section 6.3.2)	$\mathbf{D_2}$: the time necessary for the MN to receive IP configuration (Router Advertisements) from the Target Gateway.	the equivalent of $\mathbf{D_2}$ does not exist for UFA as the MN does not need to wait for the reception of its IP configuration from the target UFA Gateway. Its IP configuration is determined during handover preparation and is sent to it by the source UFA Gateway within the message 5A SIP Re-INVITE.
			$\mathbf{D_3}$: the time necessary for the MN to configure its IP layer based on the information received in the Router Advertisements. This time includes delay due to DAD (Duplicate Address Detection) procedure.	$\mathbf{D_3}$: the time necessary for the MN to configure its IP layer with the IP configuration information received in message 5A (SIP Re-INVITE).
	ATH_4: P-CSCF discovery	Not implemented		
	ATH_5: registration /authentication to IMS	Not implemented		
Phase 2	**Estb_1**: session initiation and negotiation	Phase 2 and phase 3 are reduced to a simple SIP Re-INVITE message sent from the MN to the CN as defined in section A.3	$\mathbf{D_4}$: the time necessary for the MN to detect at SIP level the acquisition of a new IP address and then to build message 8 (SIP Re-INVITE).	$\mathbf{D_4}$: the time necessary for the MN to detect at SIP level the change of IP address and build SIP Re-INVITE message (8).
	Estb_2, Estb_3 policy rules calculation for the IP and IP-AN levels		$\mathbf{D_5}$: the time induced by SIP signalling and impacting the application handover delay. It includes delay between sending SIP INVITE and receiving data from the CN.	$\mathbf{D_5}$: the time induced by SIP signalling and impacting the application handover delay. It corresponds to the time difference between the reception of message 7 (ACK) by the CN and message 7A (ACK) by the MN. Indeed, the CN begins data transmission to the MN through the Target UFA Gateway after the reception of message 7, and the MN attaches to the Target UFA Gateway after the reception of message 7A.
	Estb_4: resource reservation			
	Estb_5: resource reservation detection			
	Estb_6: session update			
Phase 3	SIP Re-INVITE from the SCC AS to the CN			

Table 6.1: Implemented ISC and UFA, and their handover delay components

6.2 Testbed architecture

The testbed used to implement ISC and UFA is described by figure 6.3. It consists of:

- Correspondent Node (CN): A desktop running Fedora Core 7 with kernel version 2.6.23.
- 2 Gateways (GW): Two desktops running Ubuntu 8.10 with kernel version 2.6.28.2. They act as WiFi Access points and have 3com Wireless a/b/g PCi adapters based on *Atheros* chipsets. For UFA, these GWs are called **UFA Gateways (UFA_GWs)**. For Implemented ISC, these Gateways are simply called **Gateways (GW)**.
- Mobile Node (MN): A laptop running Ubuntu 8.10 with kernel version 2.6.28.2. It has a PCMICIA wireless Netgear a/b/g card based on *Atheros* chipset. It uses a WiFi link to connect to the GWs.

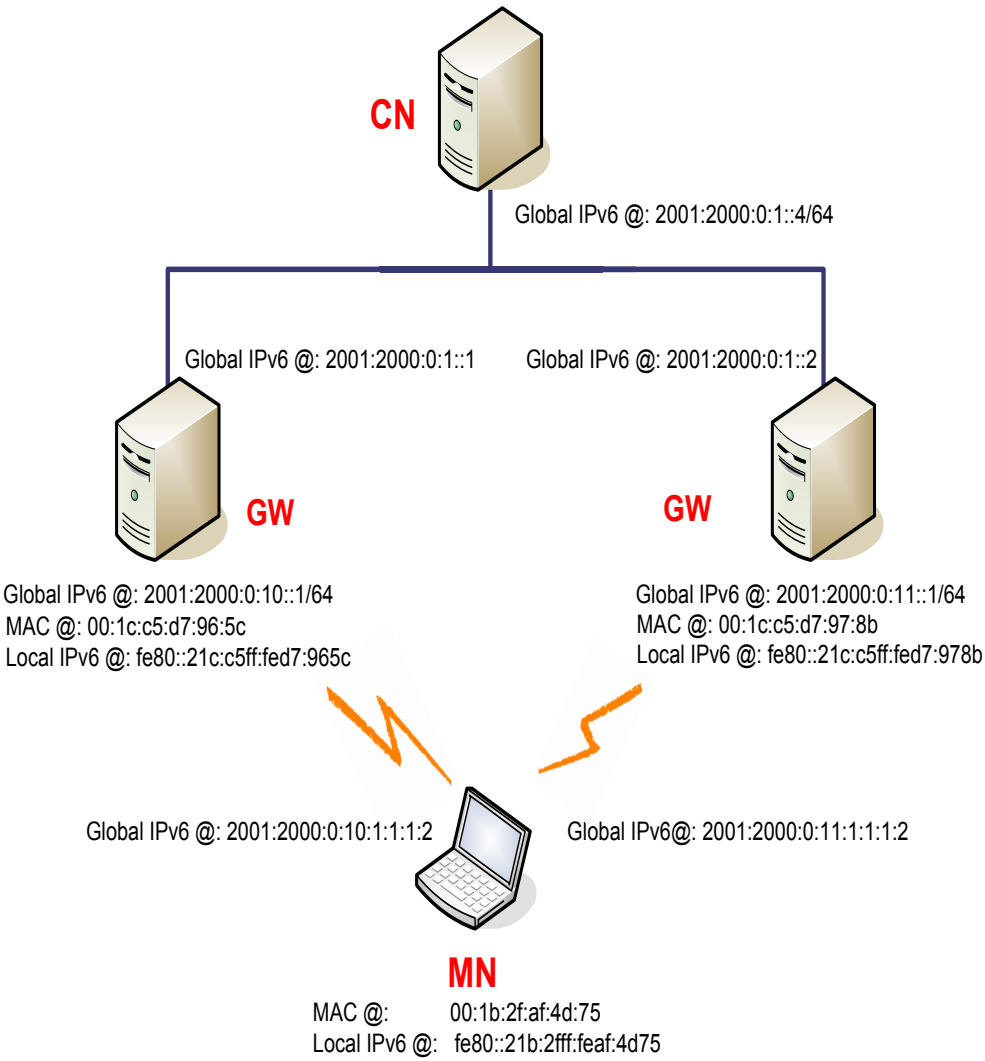


Figure 6.3: Testbed architecture

6.3 Testbed configuration and implementation

This section provides hints on testbed configuration and procedures implementation in UFA and Implemented ISC.

6.3.1 Layer 2

Layer 2 configuration is the same for UFA and Implemented ISC. The Wireless cards within the Gateways and the Mobile Node use a *Madwifi* driver (madwifi-0.9.4 branch) [96], thus they can be configured easily using *Madwifi* wireless tools.

Both Gateways are configured to run in master mode. One Gateway is configured to use channel 1 and the other one is configured to use channel 6. A periodic background scanning (every 20s) is activated on the MN. All of these last configurations allow the MN to speed its attachment to a given Gateway, and therefore to reduce the delay D_1 (table 6.1).

6.3.2 IP

The testbed is configured with IPv6 as shown in figure 6.3. There are many possible IP address allocation mechanisms: stateless IPv6 configuration [56] or DHCP [54, 55] or static address allocation.

In UFA, the static address allocation mechanism is chosen as it is the simplest one and does not impact the handover delay (the MN IP address is allocated proactively during handover preparation). The MN has the IP address 2001:2000:0:10:1:1:1:2 or 2001:2000:0:11:1:1:1:2 depending on the Gateway to which it is attached (see figure 6.3).

In implemented ISC, the MN IP address is allocated based on stateless IPv6 configuration.

6.3.3 SIP

Most of the required functions in UFA and implemented ISC are within SIP layer. PJSIP library [97] is used to develop these functions in the terminal (MN and CN) and the UFA Gateways. It enables to realize different SIP-based applications thanks to its core programs or APIs. For UFA and implemented ISC, implementation is performed in the PJSIP core programs as the available APIs do not provide enough flexibility, especially to develop the UFA Gateway Back-to-Back User Agent module.

In the terminal (MN/CN), to manage the application, a Media Controller program is used. It is based on the PJMEDIA PJSIP sub-library, and is inspired from the PJMEDIA application example named "Remote Streaming" [98]. It receives, reads or generates application packets.

As application, an RTP voice streaming is used. The CN is the server and the MN is the client. When the CN receives information about the new MN IP address (e.g. through SIP INVITE message), the Media Controller updates the MN IP destination address.

The architecture of SIP programs for UFA and Implemented ISC is given in appendix F.

6.3.4 Implementation challenges

In UFA, as described in section 4.2 and illustrated by figure 4.5, the MN executes the handover after receiving message 7A (SIP ACK), based on the all-OSI layer configuration received in mes-

sage 5A (SIP Re-INVITE). Implementation steps regarding the consideration/enforcement of this configuration by the MN are shown in figure 6.4.

In the MN (figure 4.5), when the SIP proxy receives the all-OSI layer configuration, it extracts the different layer-related configuration information and sends them to the all-layer configuration module. This latter relays each layer-related configuration information to the concerned layer. How each layer is configured and at what moment is described hereafter (figure 6.4):

- IP and layer 2 are configured in parallel to optimize the delay D_1+D_3 (see table 6.1). For this purpose, a thread for IP configuration is used. This thread first deletes the IP configuration acquired under the Source UFA Gateway (UFA_GW_S), then it adds/enforces IP configuration necessary to attach to the Target UFA Gateway (UFA_GW_T).
- After receiving the new MN IP address, which is a SIP-related configuration information, SIP updates the dialog and the IP socket (used for sending SIP messages) with this address, and sends message 8 (SIP Re-INVITE) to the Target UFA Gateway. However, these tasks cannot be executed before the completion of layer 2 and IP configurations; otherwise they fail. Therefore, some means are used to detect the completion of layer 2 and IP configurations, as shown in figure 6.4:
  - The Linux *Iwevent* command is used to detect when the layer 2 configuration is completed. *Iwevent* displays wireless events received through the Netlink sockets[1] [99]. When the Target UFA Gateway MAC address is displayed, the MN layer 2 is assumed as being completely attached to the Target UFA Gateway.
  - A program "*detect that IP configuration is completed*" is used. This program is based on Netlink sockets. When a new address is added to a given interface, the Netlink socket reports to the user space an *RTM_NEWADDR* event. To detect the event of IP address addition, this program has to be launched before the commands "*IP configuration: Add the new IP configuration*" adding the new IP configuration are executed.

In the Implemented ISC solution, mobility is initiated by the MN which attaches to the Target UFA Gateway following the command: `iwconfig ath0 essid UFA-BS channel 6 ap 00:1C:C5:D7:97:8B`, entered directly into the MN. Once it is attached at layer2 level to the Target UFA Gateway, it receives the Router Advertisements, and its IP layer is configured accordingly. SIP needs to detect when a new IP address is acquired and to know this IP address, in order to be able to send the SIP Re-INVITE message to the CN (figure 6.1) (the new MN IP address is used to update the SIP dialog and IP socket, and to fill the SIP Re-INVITE message with this information). The same program "*detect that IP configuration is completed*" used in UFA, is used for this aim. The Linux *Iwevent* command is not needed as IP and layer 2 configurations are performed sequentially and not in parallel.

Another challenge encountered in UFA concerns the delay due to neighbor table setting in the MN and the Target UFA Gateway. Neighbor tables associate the IP address and the MAC address of the first IP hop. For example, in the MN, it associates the IP address and the MAC address of the Target UFA Gateway. This allows the MN to send the data to the CN via the Target UFA Gateway. In the Target UFA Gateway, the neighbor table associates the IP address and the MAC address of the MN. This allows the Target UFA Gateway to send the data received from the CN to the MN.

[1] NETLINK is a facility in Linux to make the user-space and the kernel communicate between each others. NETLINK is an extension of the standard socket implementation. Using NETLINK, an application can send/receive information to/from different kernel features, such as networking, to check their current status and control them.

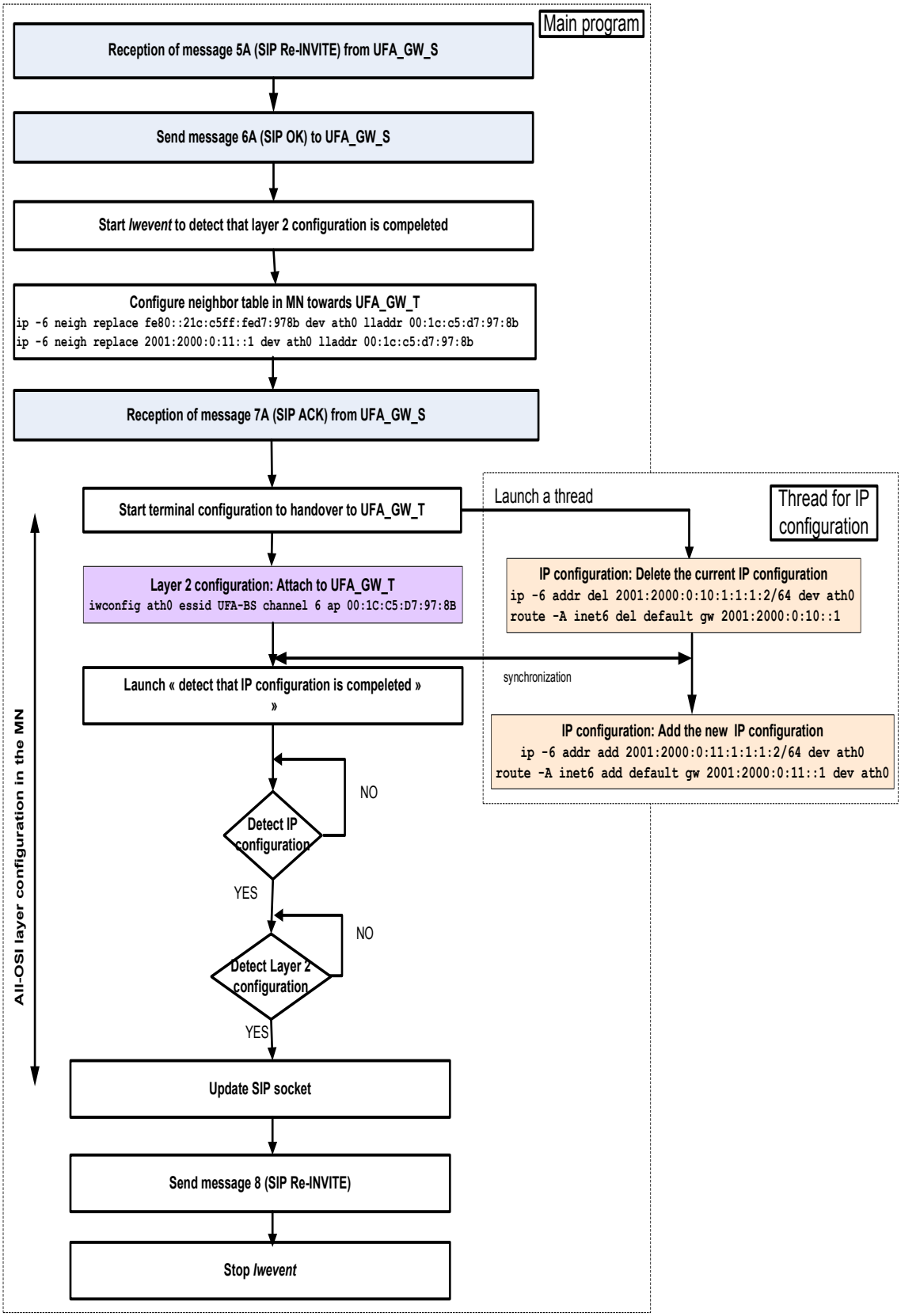


Figure 6.4: Implementation of all-OSI layer configuration in the UFA Mobile Node

Without any optimization, to set its neighbor table, a node broadcasts neighbor solicitation messages [56]. Based on the received response, it fills its table. However, for UFA, the time consumed by these messages impacts the handover delay. To save this time, the neighbor table in the Target UFA Gateway is configured (using Linux *ip -6 neigh* command) during handover preparation, based on the MN MAC address communicated by the Source UFA Gateway to the Target UFA Gateway in message 3 (CONTEXT TRANSFER) (figure 4.5).
Similarly, neighbor table in the MN is configured based on the MAC address, IP global and local addresses of the Target UFA Gateway, received within UFA_Terminal_conf header (table 4.2).

In Implemented ISC, neighbor table in the MN is set based on the received router Advertisements. In the Target Gateway, it is initialized using classical means (i.e. based on neighbor solicitation messages). Means to set this table in Implemented ISC as done for UFA are not easy to implement, as this would require to modify the ISC mobility procedure.

6.4 Testbed traces

Appendix E provides traces collected on the testbed during the establishment and mobility procedures. These traces detail the content of SIP messages exchanged between the MN and the CN, and the behavior of the UFA_GW Back-to-Back User Agent regarding these messages.

6.5 UFA performances

This section aims at analyzing UFA performances. The first part (6.5.1) compares UFA and Implemented ISC handover delays, based on measurements carried out on the testbed considering low-delay links. The second part (6.5.2) provides the UFA handover delays as measured on the testbed for different network scenarios, corresponding to different link delays. To validate these measurements, they are compared to analytical values obtained through mathematical formulas modeling the handover delay in UFA.

6.5.1 Handover delays measurements on the testbed in UFA and Implemented ISC for low-delay links

Handover delay components for Implemented ISC and UFA are defined in table 6.1. This section provides the measurements of these components on the testbed [81].

6.5.1.1 Tools and method to measure the handover delays

Before providing the component measurements, the tools and method used to measure them on the testbed are detailed in this section.

Tools used are:

- An airmagnet sniffer[2] [100] that measures the layer 2 attachment delay to the Target Gateway (D_1).
- A Wireshark [101] that analyzes the messages exchanged on a given interface machine, is used on the MN, CN and UFA Gateways interfaces.

[2] a tool that can verify, audit and analyze a WiFi interface

- SIP logs that are generated by dedicated programs on the MN, CN and UFA Gateways.
- Pings are sent each 5ms from the MN to the CN.

The handover delay components defined in table 6.1 for Implemented ISC, are measured using the following method. Once the MN is handed from the Source Gateway to the Target Gateway:

1. D_1 is read on the sniffer.
2. The application handover delay (Appli_HO_Delay) is deduced on the MN wireshark, based on RTCP (Real Time Control Protocol) packets that provide the number of application packets lost during handover. Appli_HO_Delay is also measured on the MN wireshark based on the time difference between the last application packet received before handover and the first application packet received after handover.
3. D_1+D_2+D_3 is measured on the MN wireshark, based on the delay between the last ping "echo request" sent by the MN with the old IP address and the first "echo request" sent by the MN with the new IP address. Then, D_2 +D_3 is deduced, as D_1 is known from the last step. D_2 is calculated on the MN wireshark based on D_1 and on the number of Router Advertisements received by the MN before performing DAD (sending neighbor solicitation message). D_3 is finally deduced.
4. D_4 is read on the MN SIP logs. It is the the delay between detecting the event of acquiring a new IP address and the event of building the SIP Re-INVITE message.
5. D_5 is deduced on the MN wireshark. It is the delay between sending SIP Re-INVITE and receiving data from the CN.

The handover handover delay components defined in table 6.1 for UFA, are measured using the following method. Once the MN is handed from Source UFA Gateway to the Target UFA Gateway:

1. D_1 is read on the sniffer.
2. The application handover delay (Appli_HO_Delay) is deduced on the MN wireshark using the same method as Implemented ISC.
3. (D_1+D_3) is measured on the MN wireshark, based on the delay between the last ping "echo request" sent by the MN with the old IP address and the first ping "echo request" sent by the MN with the new IP address. D_3 is deduced, as D_1 is known.
4. D_4 is read on the MN SIP logs. It is the delay between detecting the event of acquiring a new IP address and the event of building the SIP Re-INVITE message (8).

6.5.1.2 Handover delay measurements on the testbed

On the testbed, the application handover delay and the handover delay components are measured for a streaming voice sending data packets over RTP/UDP, each 20ms, from the CN to the MN.

For Implemented ISC, handover delays measured on the testbed are as follows:

- The **number of lost packets** is **61** based on RTCP packets as shown in figure 6.5.

- The application handover delay **Appli_HO_Delay** is **1220ms** based on the number of lost packets (61*20ms). Figure 6.6 shows that Appli_HO_Delay is **1238ms** (packets 350 -> 381). The difference between the two results (1220ms and 1238ms) may be due to the fact that the 1220ms calculation only takes into account the number of lost packets, and does not consider the interval of time until the MN receives new data packets (data packets are sent each 20ms).
- $\mathbf{D_1}$ is **60ms**.
- $\mathbf{D_2}$ is **100ms**. It has been observed that the MN does not consider the first received Router Advertisement, which explains the obtained 100ms instead of 50ms maximum (RA periodicity is 30-50ms).
- $\mathbf{D_3}$ is **1020ms**.
- $\mathbf{D_4}$ is **13ms**.
- $\mathbf{D_5}$ is **45ms**. Although the very low-delay links, D_5 is not low. It is due to the neighbor discovery procedure performed by the target Gateway after receiving the first data packets from the CN to forward to the MN.

For UFA, handover delays measured on the testbed are as follows:

- The **number of lost packets** is **4** based on RTCP packets as shown in figure 6.7.
- The application handover delay **Appli_HO_Delay** is **80ms** based on the number of lost packets (4*20ms). Figure 6.8 shows that Appli_HO_Delay is **60ms** (packets 952 -> 957). The difference between the two results (80ms and 60ms) may be due to the fact that wireshark captures packets while the MN interface is not completely attached.
- $\mathbf{D_1}$ is **60ms** as in Implemented ISC.
- $\mathbf{D_2}$ does not exist for UFA, as commented in table 6.1.
- $\mathbf{D_3}$ is **20ms**, it corresponds to the delay necessary for the MN to enforce the IP configuration received from the Source UFA Gateway. Compared to Implemented ISC, D_3 is lower in UFA as it does not include the delay due to Duplicate Address Detection. Indeed, in UFA, the uniqueness of the MN IP address has been checked proactively by the Target UFA Gateway during handover preparation procedure.
- $\mathbf{D_4}$ is **70ms**. This delay does not impact the application handover delay (Appli_HO_Delay value (80ms)) measured on the testbed, as buffering in the Target UFA Gateway in not implemented. Indeed, D_4 represents the delay in the MN at the SIP layer to detect the new IP address and send message 8 (SIP Re-INVITE) to the Target UFA Gateway (UFA_GW_T). If this latter has buffered any data received from the CN or the Source UFA Gateway (UFA_GW_S), the reception of message 8 would trigger data sending to the the MN.

  D_4 value is different from the one obtained in Implemented ISC, even though it is expected to be the same. The difference can be explained by the fact that *Iwevent* (figure 6.4) employed in UFA to detect the completion of layer 2 configuration, is not very reactive.
- $\mathbf{D_5}$ is **0ms** as messages 7A and 7 (SIP Re-INVITE) are received at the same time by the MN and the CN (delay on the links UFA Gateway-MN and UFA Gateway-CN links is low).

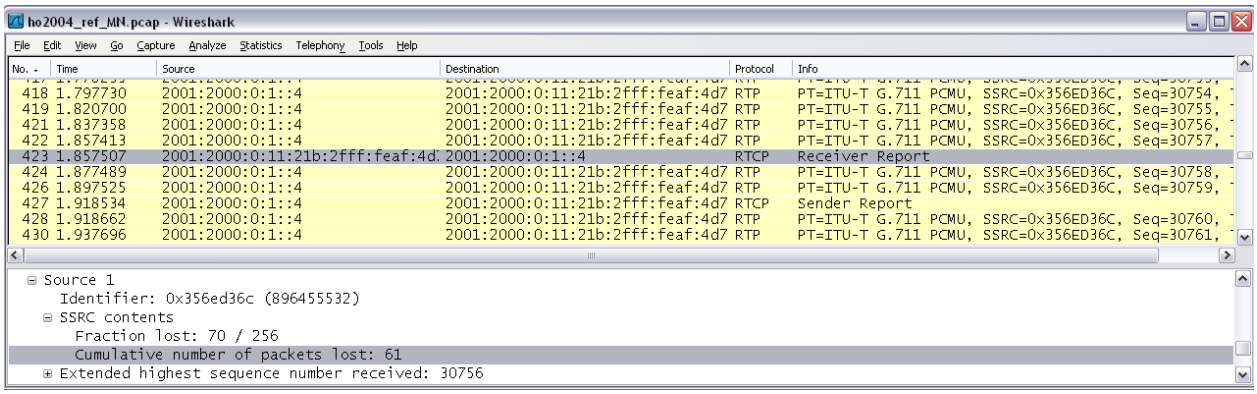


Figure 6.5: Number of lost packets in Implemented ISC on the MN wireshark

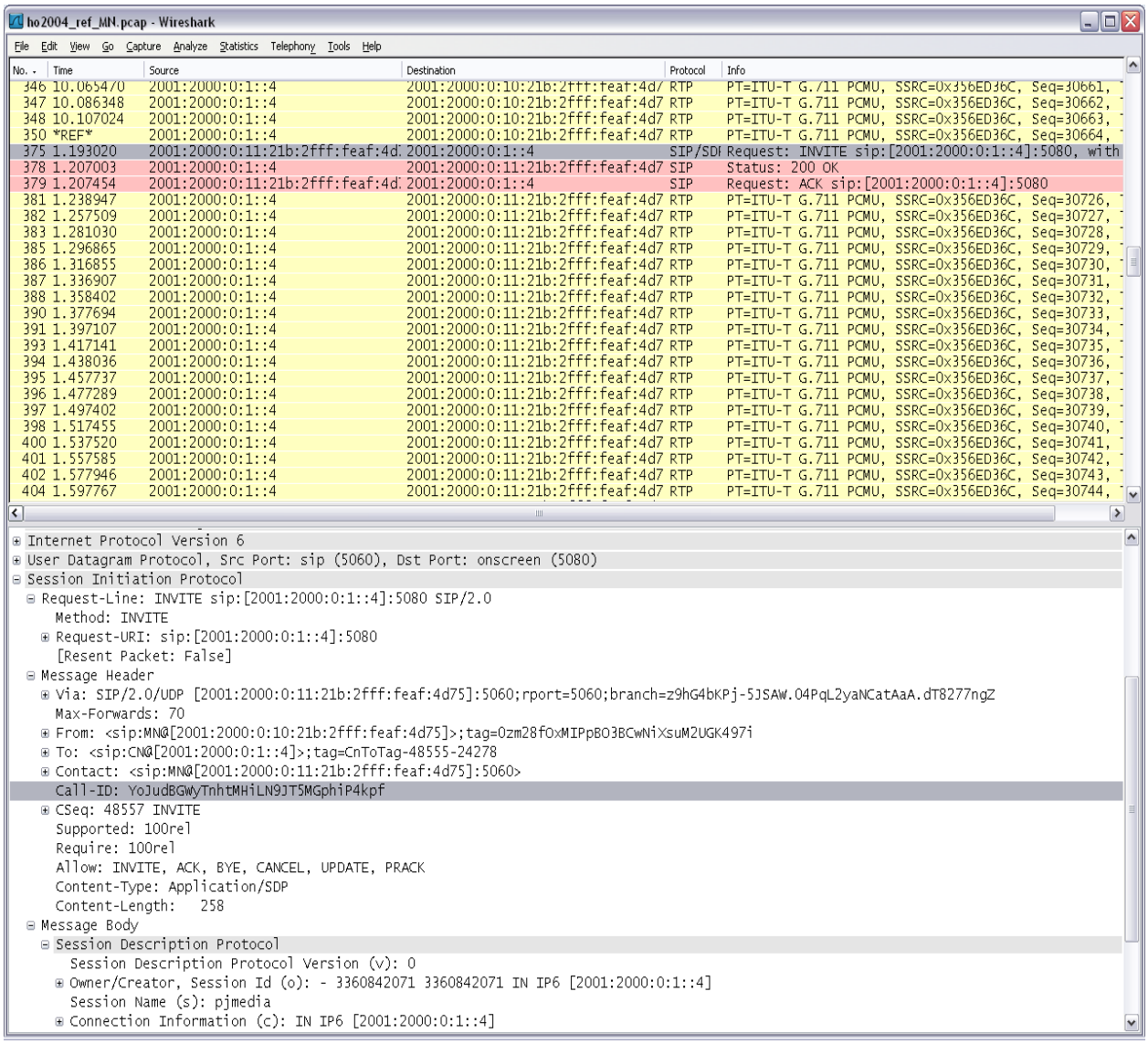


Figure 6.6: Application handover delay in Implemented ISC on the MN wireshark

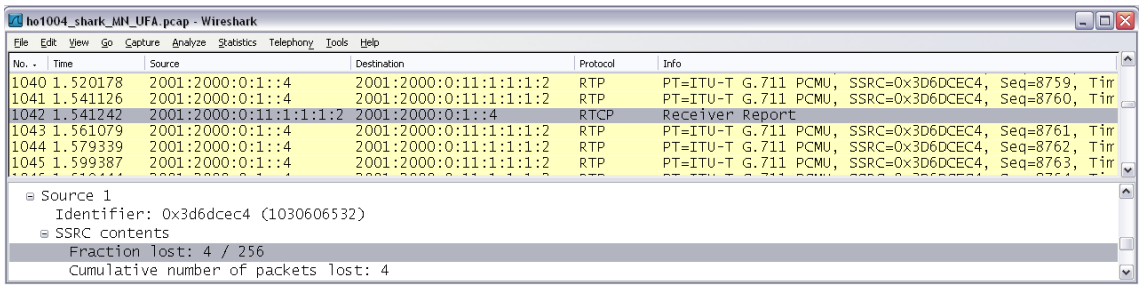


Figure 6.7: Number of lost packets in UFA on the MN wireshark

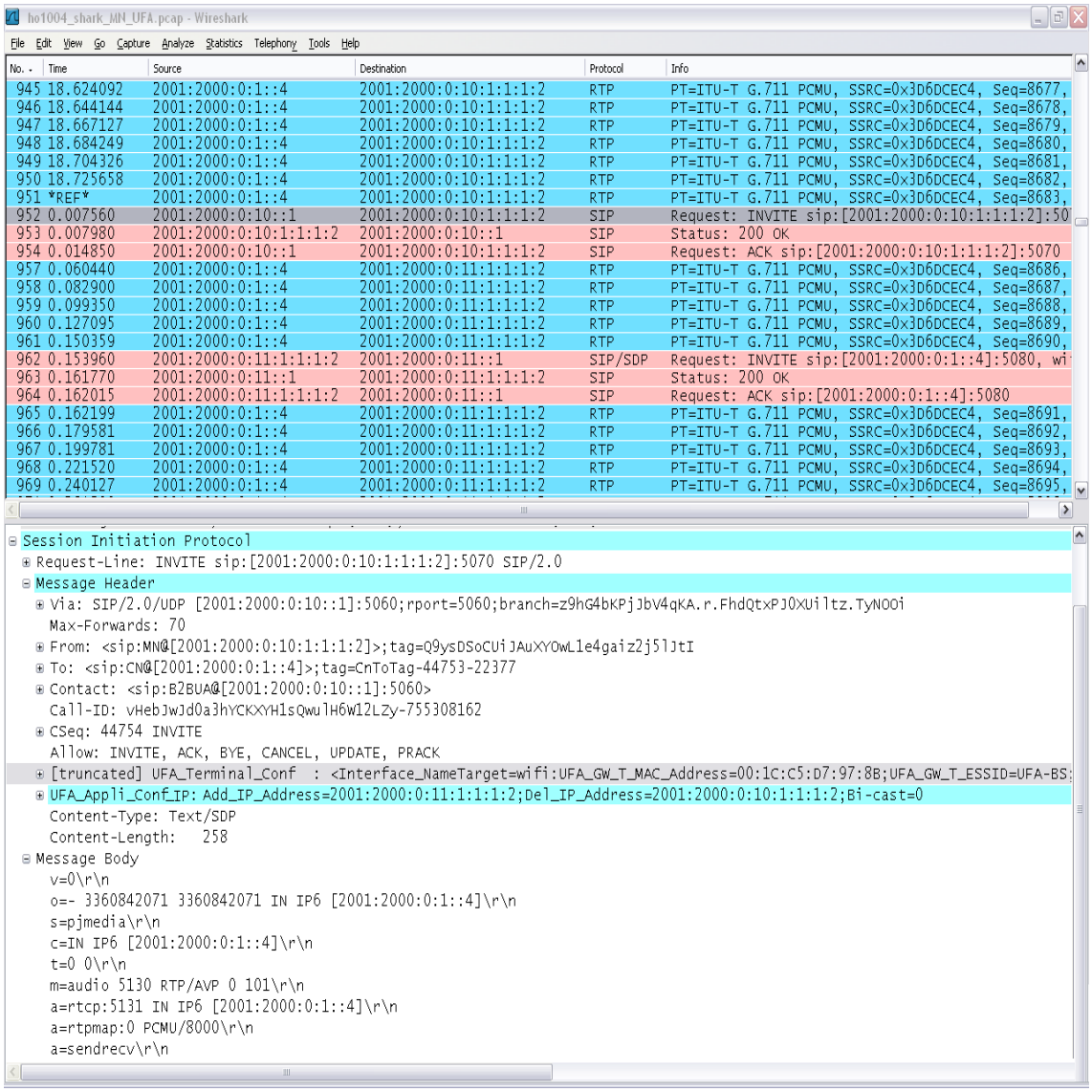


Figure 6.8: Application handover delay in UFA on the MN wireshark

6.5.2 Handover delays in UFA for different network scenarios: comparison between testbed measurements and analytical values

To better analyze UFA performances, this section provides the handover delays as measured on the testbed for different network scenarios, corresponding to different delays on the links between the UFA Gateways and the MN or the CN. To validate these measurements, they are compared to analytical values obtained through mathematical formulas modeling the handover delay in UFA.

6.5.2.1 Network scenarios

Network scenarios are obtained by varying the following network parameters:

- $\mathbf{D_{GWS\text{-}CN}}$ (resp. $\mathbf{D_{GWT\text{-}CN}}$): the propagation delay of a packet over the link between the Source UFA Gateway and the CN (resp. Target UFA Gateway and the CN). It is assumed that packets on this link are only impacted by this propagation delay and not by the link bandwidth.

  This delay is independent of the packet length, however the notation $\mathbf{D_{GWS\text{-}CN}(X)}$ (resp. $\mathbf{D_{GWT\text{-}CN}(X)}$) is used to show which packet X is being dealt with.

- $\mathbf{Xput_{GWS\text{-}MN}}$ (resp. $\mathbf{Xput_{GWT\text{-}MN}}$): the bandwidth allocated to a given data flow over the link Source UFA Gateway-CN (resp. Target UFA Gateway-CN). The delay of packet X within this data flow is $\mathbf{D_{GWS\text{-}MN}(X)}$ (resp. $\mathbf{D_{GWT\text{-}MN}(X)}$).

On the testbed, the variation of the previous parameters is achieved thanks to Linux *tc qdisc* commands.

6.5.2.2 Length of UFA mobility procedure messages

To calculate the delay of the different messages involved in the UFA mobility procedure, their length have to be known. Table 6.2 provides this information, based on the traces obtained on the testbed.

Message name	**From**	**> To**	**Message length (bytes)**
3-CONTEXT TRANSFER Transferred context	UFA_GW_S	> UFA_GW_T	1383
4-ACK Configuration for the MN	UFA_GW_T	> UFA_GW_S	163
5A-SIP Re-INVITE	UFA_GW_S	> MN	1229
6A-SIP OK	MN	> UFA_GW_S	544
7A-SIP ACK	UFA_GW_S	> MN	494
5-SIP Re-INVITE	UFA_GW_S	> CN	929
6-SIP OK	CN	> UFA_GW_S	535
7-SIP ACK	UFA_GW_S	> CN	497
8-SIP ACK	MN	> UFA_GW_T	877

Table 6.2: Length of handover messages in UFA

6.5.2.3 Evaluation

According to section 4.2 and figure 6.2:

- The CN begins data transmission to new MN IP address (@IP2) only after the reception of message 7 (ACK).
- The MN configures its layers and attaches to the Target UFA Gateway only after the reception of message 7A (ACK).

$\mathbf{D_5}$ is defined as the time difference between the reception of message 7 by the CN and the reception of message 7A by the MN. When D_{GWS-CN}(5+6+7)< <D_{GWS-MN}(5A+6A+7A) (i.e. D_5< <0), the CN transmits data towards @IP2 a lot earlier, before the MN attachment to the Target UFA Gateway. This causes a considerable data losses, as buffering is not implemented in the Target UFA Gateway. To optimize the handover performance, implementation is modified so that, when D_{GWS-CN}(5+6)< <D_{GWS-MN}(5A+6A), the Source UFA Gateway delays message 7 (ACK) sending to the CN until the reception of message 6A (OK) from the MN (see figures 6.9, 6.10, 6.11). D_5 is thus reduced to D_{GWS-CN}(7)-D_{GWS-MN}(7A).

When D_{GWS-MN}(5+6)>D_{GWS-CN}(5A+6A) (figure 6.12), to avoid losing the connectivity with the MN in hard handover situation, the Source UFA Gateway does not delay message 7A (ACK) sending to the MN until the reception of message 6 (OK) from the CN.

Table 6.3 shows the application handover delay (Appli_HO_Delay) values obtained on the testbed, each point is an average of 10 tests.
To validate these measurements, they are compared to analytical values obtained based on mathematical formulas modeling the application handover delay (Appli_HO_Delay) in UFA. Appli_HO_Delay depend on the following parameters:

- D_5: as already said, it is the time difference between the reception of message 7 by the CN and the reception of message 7A by the MN.
  - When D_{GWS-CN}(5+6)< D_{GWS-MN}(5A+6A);
    D_5 = D_{GWS-CN}(7)-D_{GWS-MN}(7A).
  - When D_{GWS-CN}(5+6)> D_{GWS-MN}(5A+6A);
    D_5 = D_{GWS-CN}(5+6+7)-D_{GWS-MN}(5A+6A+7A). I suppose that in this case D_5 >0.
- D_{GWS}(D): the delay of a data packet (D) sent from the CN to the MN through the Source UFA Gateway,
  D_{GWS}(D)= D_{GWS-CN}(D) + D_{GWS-MN}(D).
- D_{GWT}(D): the delay of a data packet (D) sent from the CN to the MN through the Target UFA Gateway,
  D_{GWT}(D)= D_{GWT-CN}(D) + D_{GWT-MN}(D).

Formulas and explanation for Appli_HO_Delay are given below:

- If (D_{GWS-MN}(5+6)) < (D_{GWS-MN}(5A+6A))
  - If D_{GWS-MN}(7) < D_{GWS-MN}(7A) i.e. D_5 <0 : the MN disconnects from the Source UFA Gateway before the CN has received message 7 (ACK)
    - If $|D_5|$ < D_{GWS}(D): the MN has continuously received packets from the CN until its disconnection. Appli_HO_Delay depends in this case on D_1+D_3 (the layer2 and

IP disconnection delays) compared to $D_{GWT}(D) - |D_5|$ (**case 1**, figure 6.9).

$$Appli_HO_Delay = max[(D_1 + D_3); (D_{GWT}(D) - |D_5|)] \tag{6.1}$$

* If $|D_5| > D_{GWS}$(D): the MN has not received packets from the CN during $|D_5| - D_{GWS}(D)$ before its disconnection. Appli_HO_Delay depends in this case on D_1+D_3+$|D_5| - D_{GWS}(D)$ compared to $D_{GWT}(D) - |D_5|$ (**case 2**, figure 6.10).

$$\begin{aligned} Appli_HO_Delay = max[(D_1 + D_3 + |D_5| - D_{GWS}(D)); \\ (D_{GWT}(D) - D_{GWS}(D))] \end{aligned} \tag{6.2}$$

– If $D_{GWS-CN}(7) > D_{GWS-MN}$(7A) i.e. $D_5 > 0$: the MN has continuously received packets from the CN until its disconnection. Appli_HO_Delay depends in this case on D_1+D_3 compared to $D_{GWT}(D) + D_5$ (**case 3**, figure 6.11).

$$Appli_HO_Delay = max[(D_1 + D_3); (D_{GWT}(D) + D_5)] \tag{6.3}$$

- If (D_{GWS-MN}(5+6)) > (D_{GWS-MN}(5A+6A)): the MN has continuously received packets from the CN until its disconnection. Appli_HO_Delay depends in this case on D_1+D_3 compared to $D_{GWT}(D) + D_5$ (**case 4**, figure 6.12).

$$Appli_HO_Delay = max[(D_1 + D_3); (D_{GWT}(D) + D_5)] \tag{6.4}$$

Appli_HO_Delay values obtained using the above mathematical formulas are also given in table 6.3. They are calculated considering the message lengths given in table 6.2 and for voice packets having a length of 176bytes.

It can be observed that the values obtained by the testbed and the values obtained by analytical calculation are quiet similar, proving the correctness of UFA implementation and the above formulas.

When the delay (D_{GW-CN}) between the UFA Gateway and the CN, and the throughput ($Xput_{GW-MN}$) on the UFA Gateway-MN link, cause delays in the same range value, whether these delays are low[3] or high[4], the application handover delay (Appli_HO_Delay) remains near 100ms, which is almost the value obtained for low-delay links. This is explained by the fact that, in these cases, messages 7 and 7A are received almost at the same time by the MN and the CN. However, when D_{GW-CN} is very high[5], even though it causes a delay in the same range value as $Xput_{GW-MN}$, Appli_HO_Delay is higher than 100ms. This is due to the fact that data packets sent by the CN after reception of message 7 take a long time to arrive to the MN.

It is also worth noting that delays obtained with UFA, whatever the network scenario, remain inferior to the handover delays obtained with Implemented ISC for low-delay links (1220ms).

6.6 Conclusion

By means of testbed, this chapter has proved the UFA model concepts and confirmed the good performances of the UFA mobility procedure compared to a simple version of the ISC mobility procedure, used in the IP-AN//PCC//IMS model.

[3]e.g. D_{GW-CN}=10ms; $Xput_{GW-MN}$=1Mbps causing a delay of 8ms for 1000bytes-length packet
[4]e.g. D_{GW-CN}=50ms; $Xput_{GW-MN}$=100kbps causing a delay of 80ms for 1000bytes-length packet
[5]e.g. D_{GW-CN}=100ms; $Xput_{GW-MN}$=100kbps causing a delay of 80ms for 1000bytes-length packet

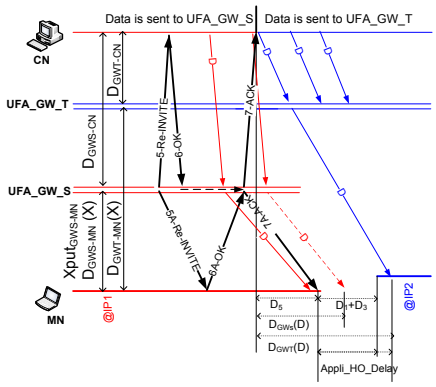


Figure 6.9: Case 1 of UFA handover delay

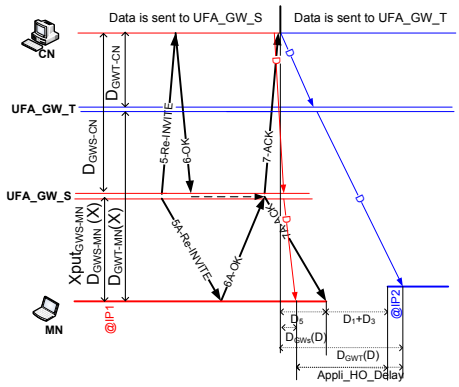


Figure 6.10: Case 2 of UFA handover delay

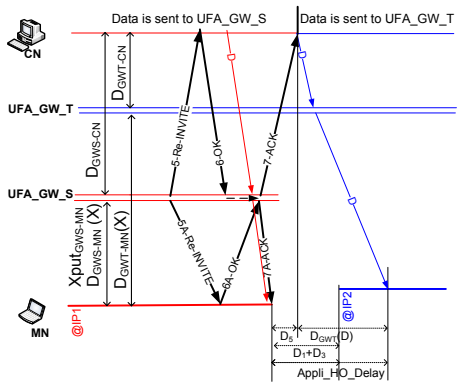


Figure 6.11: Case 3 of UFA handover delay

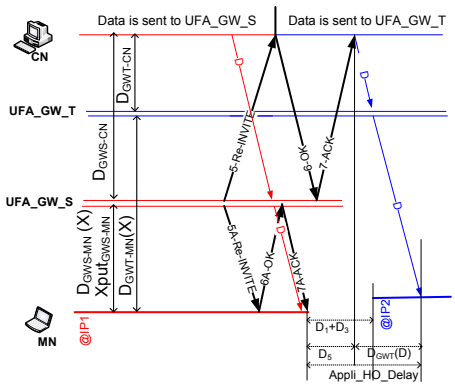


Figure 6.12: Case 4 of UFA handover delay

D_{GWS-CN}= D_{GWT-CN}= D_{GW-CN}	$Xput_{GWS-MN}$= $Xput_{GWT-MN}$= $Xput_{GW-MN}$	Appli_HO_Delay obtained by testbed	Appli_HO_Delay obtained by analytical calculation	
10ms	50kbps	100ms	107ms	case 1
	100kbps	100ms	80ms	case 1
	1Mbps	100ms	80ms	case 4
	5Mbps	105ms	80ms	case 4
50ms	50kbps	120ms	107ms	case 1
	100kbps	101ms	80ms	case 3
	1Mbps	179ms	183ms	case 4
	5Mbps	210ms	198ms	case 4
100ms	50kbps	160ms	148ms	case 3
	100kbps	242ms	232ms	case 4
	1Mbps	360ms	383ms	case 4
	5Mbps	400ms	398ms	case 4

Table 6.3: UFA handover delays for different network scenarios

The considered service type is a SIP native one, more specifically a voice stream. On the application level, UFA provides a handover delay 12 times inferior than the Implemented ISC. This delay is

about 80ms for low-delay links and corresponds to the delay necessary for the MN to be reconfigured at the layer 2 and IP levels.

Handover delay components have been also measured and compared, for UFA and Implemented ISC, considering low-delay links. D_1 is the time necessary for the MN to configure its layer 2 and attach to the Target Gateway, it is 60ms for both UFA and Implemented ISC. D_2 is the time, once the MN is attached to the Target Gateway, necessary for receiving the IP configuration information; its is 0ms for UFA and 100ms for Implemented ISC. D_3 is the time necessary for the MN to configure its IP layer with the received configuration; its is 20ms for UFA and 1020ms for Implemented ISC. D_4 is the time necessary for the MN to detect at the SIP level the acquisition of a new IP address and build a SIP Re-INVITE; it is 70ms for UFA and 13ms for Implemented ISC. These components are independent of the service type (SIP native or non-SIP native).

When the link between the UFA Gateway and the CN, and the link between the UFA Gateway and the MN, have delays in the same range value, the handover delay in UFA as measured on the testbed remains near 100ms. In order to confirm the correctness of these measurements, they have been compared to analytical values obtained based on mathematical formulas modeling the handover delay in UFA. It has been found out that both kinds of results are quiet similar. Thus, testbed implementation and specifications are correct. In addition, these formulas can be used to deduce the handover delays for any SIP native service and delays on the links.

It is worth remarking that UFA handover delays are compliant with the 3GPP requirements for a handover between two e-NB. Indeed, 3GPP mandates for this case that the interruption time (application handover delay) varies between 30ms and 100ms, similarly to a circuit switched handover in GERAN (based on [102, 103, 104]).

CHAPTER 7

Performance of UFA mobility procedure for non-SIP native services

As described in chapter 4, UFA introduces a common SIP-based mobility procedure for SIP native[1] and non-SIP native[2] services. The performances of this procedure for these two types of services are different, as SCTP reacts to data losses differently from RTP/UDP. Indeed, SCTP data transmission and congestion control mechanisms consider by default, that packet losses are due to congestion (when in fact these losses are due to handovers) and retransmits them after a timeout.

In this chapter, non-SIP native services are called **SCTP-transported services**, as the focus is on SCTP aspect of these services.

Mobile SCTP (m-SCTP) [105] is the classical protocol used to manage the mobility of SCTP-transported services, instead of the UFA mobility procedure. Therefore, to evaluate the UFA mobility procedure performances and show its benefits for these services, m-SCTP is considered as a reference case. The hard handover scenario is considered as it is the most restricting one (see section 2.2.2.2).

This chapter is organized as follows. Section 7.1 presents SCTP and its data transmission and congestion control mechanisms. Section 7.2 describes m-SCTP. Section 7.3 details SCTP performance problems during hard handovers when used with m-SCTP and provides the related work. Section 7.4 compares UFA with other mobility management solutions such as m-SCTP or SIP-based ones. Section 7.5 presents different options for SCTP layer configuration in UFA. Section 7.6 evaluates the UFA performances compared to m-SCTP. Finally, section 7.7 concludes.

7.1 SCTP

7.1.1 Overview

SCTP is introduced in RFC [106]. An **SCTP association** can be established between two endpoints each one characterized by one SCTP port and more than one IP address, unlike a TCP connection where each endpoint is characterized by one TCP port and only one IP address. Thus, within the same association, an SCTP endpoint can reach its peer endpoint through different paths corresponding to the different peer endpoint IP addresses. This SCTP multihoming feature was

[1] Services whose application(s) are transported over RTP/UDP and controlled by SIP

[2] Services whose application(s) are transported over SCTP and natively controlled by a protocol different from SIP (HTTP, RTSP, ...)

designed to add resilience to network failures. An endpoint chooses a **primary path** to send packets to its peer endpoint. The alternate paths, called **secondary paths** and considered as backup paths, are used to retransmit the packets lost on the primary path or to transmit new packets when a failure is detected on the primary path. Like TCP, SCTP ensures a reliable data transmission. It also provides congestion control services by adapting the amount of data injected in the network according to the network congestion state. This ensures the network stability and minimizes the packet losses.

7.1.2 SCTP mechanisms for data transmission and congestion control

SCTP mechanisms for data transmission and congestion control rely on data acknowledgments (SACKs). Each time a receiver receives data from the sender, it sends back a SACK.

These mechanisms also rely on parameters maintained by the receiver and the sender as indicated in figure 7.1:

- The receiver is characterized by its buffer size. It calculates the free size of its buffer (`a_rwnd`) and forwards it to the sender within the SACKs.
- The sender maintains: the congestion window size (`cwnd`), the Retransmission TimeOut (`RTO`), the slow start threshold (`ssthresh`), and the `peer_rwnd`.

  `Cwnd`, `RTO` and `ssthresh` reflect the network congestion state. As paths towards the receiver may have different congestion states, each path has its specific `cwnd`, `RTO`, `ssthresh` parameters (for instance, in figure 7.1, `cwnd` for IP dest1 and `cwnd` for IP dest2).

  The `peer_rwnd` is the free size of the receiver buffer assessed by the sender, it is independent of the data path.

SACKs contain among other things the following information:

- The Transmission Sequence Number (TSN) of the last packet received in sequence before a gap in the received TSNs occurs (`Cumulative TSN Ack`),
- The TSN blocks related to sequenced packets received just after a gap (`Gap Ack Blocks`),
- The `a_rwnd` calculated by the receiver and reflecting the free size of its buffer,
- The duplicate TSNs related to packets received more than once.

7.1.2.1 Sliding window and congestion control algorithms

An SCTP sender uses a sliding window for data sending. The sliding window size (`wnd`) represents the maximum size of a data packet block a sender can send without requiring the reception of any SACK for this block (see figure 7.1). Each time a packet is acknowledged, the window slides along this packet and equivalent sized packets can be injected in the network. To avoid overflowing the receiver buffer and the network, `wnd` value is the smallest of the `peer_rwnd` and `cwnd` values.

`Cwnd` as well as `RTO` and `ssthresh` are the **congestion control parameters**. They evolve according to congestion control algorithms. At the beginning of data transmission, as network conditions are unknown, SCTP on the sender side initiates `cwnd`, `RTO` and `ssthresh` to the following default values (`cwnd`=2MTU , `ssthresh`=65536bytes, `RTO`=3s). Then, to probe network capacities rapidly and while `cwnd` is inferior to `ssthresh`, `cwnd` is increased exponentially according to the **slow start algorithm**. During this first phase, if a received SACK advances the `Cumulative TSN Ack`, `cwnd`

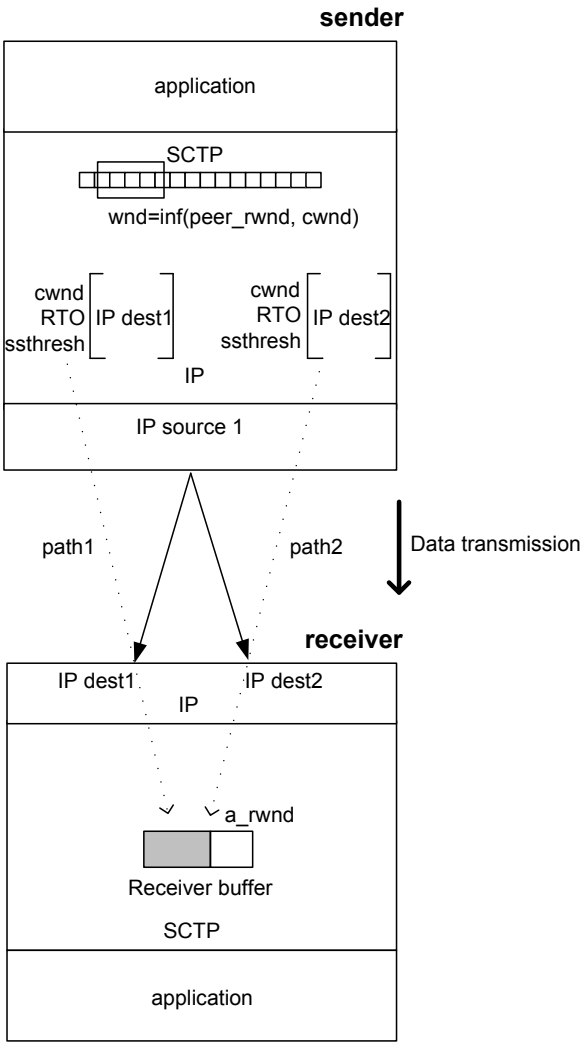


Figure 7.1: SCTP parameters on the sender and receiver sides

is increased by the smallest of the size of acknowledged data and the size of one MTU; otherwise `cwnd` remains constant. Once `cwnd` reaches `ssthresh`, it is linearly increased according to the **congestion avoidance algorithm**. During this second phase, if a received SACK advances the `Cumulative TSN Ack`, the size of acknowledged data is cumulated. When this size attains the value of the current `cwnd` and if the size of data in flight (i.e. data transmitted but not acknowledged yet) is at least equal to `cwnd`, `cwnd` is increased by one MTU.

The `peer_rwnd`, representing the free size of the receiver buffer, is assessed by the sender as follows. Initially, the `peer_rwnd` is equal to the receiver buffer size. Each time a packet is transmitted (or retransmitted) to a peer, the sender subtracts the packet size from the `peer_rwnd` current value. When a packet is marked for retransmission, either because of T3-rtx timer expiration (see next section) or because of fast retransmit (see also next section), the packet size is added to the `peer_rwnd` current value. When a SACK is received, the `peer_rwnd` is set to `a_rwnd` contained in the received SACK, minus the size of data in flight (deduced from `Cumulative TSN Ack` and *Gap Ack Blocks* contained also in the received SACK).

7.1.2.2 Retransmission management

Each time a packet is sent on a given path, SCTP on the sender side triggers a retransmission timer (`T3-rtx`). If the retransmission timer reaches (`T3-rtx` expiration) the Retransmission TimeOut (`RTO`) and the SACK acknowledging this packet is not received yet, the packet is considered as lost due to network congestion and SCTP falls back to the slow start algorithm on that path with (`cwnd`=1MTU, `ssthresh`=`ssthresh`/2, `RTO`=`RTO`*2). The lost packet is retransmitted on one of the secondary paths, if available, considering the congestion control parameters of that path. However, if the sender receives 3 SACKs indicating that this packet is missing (through `Gap Ack Blocks` field), even if the current `T3-rtx` has not expired yet, the sender considers that the packet is lost and applies **fast retransmit algorithm** by retransmitting immediately the missing packet on a secondary path and reinitiating congestion control parameters on the current path to (`cwnd`=`cwnd`/2, `ssthresh`=`cwnd`/2, `RTO`=`RTO`*2). On the current path, congestion avoidance is applied. When many packets are to be retransmitted, only the first one is fast retransmitted, the others are retransmitted according to the secondary path congestion control parameters.

During data transmission, if there are no many packet losses, the different parameters maintained on the sender's and receiver's sides described above evolve until reaching a steady state where they fluctuate around a constant value.

7.1.2.3 Optimal SCTP and network parameters for a maximum bandwidth usage

The optimal `cwnd` size that allows a maximum bandwidth usage, is equal to the product of the bottleneck link bandwidth with the sender-receiver link round trip time (RTT) [107]. It is named BDP (bandwidth delay product).

Let us consider a Correspondent Node (CN) sending data to a Mobile Node (MN) connected to a Gateway router (GW). The link GW-MN is the bottleneck link, it offers the bandwidth $Xput_{GW-MN}$ to the SCTP-transported service. In this case the optimal `cwnd` size is:

$$cwnd = BDP = RTT_{CN-MN} * Xput_{GW-MN} \tag{7.1}$$

This value cannot be reached if the network is not well configured. According to the rule of thumb [108], the Gateway should have a buffer with a size at least equal to BDP. Indeed, with a buffer size below BDP, multiple packets will be dropped causing a repetitive congestion avoidance phases triggered by fast retransmit, leading to a small `cwnd` size.

7.2 Mobile SCTP

To handle the mobility of SCTP-transported services, a new extension of SCTP called Mobile SCTP (m-SCTP) has been introduced in RFC [105]. It takes benefit from SCTP multihoming feature and makes possible the dynamic addition and deletion of IP paths to an established association. This is performed through the usage of m-SCTP signalling messages (ASCONF). As shown in figure 7.2, when the MN acquires a new IP address, it informs the CN using an ASCONF(ADD IP) message, so that the CN can consider the new address as a secondary path. Then, if the MN wants its new address to be considered by the CN as a primary path, it sends an ASCONF(SET PRIMARY) message to the CN. If the MN does not want the CN to use one of its addresses anymore (e.g. it loses the address), it informs the CN using an ASCONF(DELETE IP) message.

After receiving an ASCONF(ADD IP), to become able to send data to the new MN IP address, the CN needs to perform path verification towards that address. Path verification consists in sending a HEARTBEAT message to the new address and waiting for the reception of HEARTBEAT ACK. On the MN side, the MN is allowed to use its new acquired IP address for data sending only after receiving the ACK response to the ASCONF(ADD IP) message, confirming that the CN has received the ASCONF(ADD IP) message.

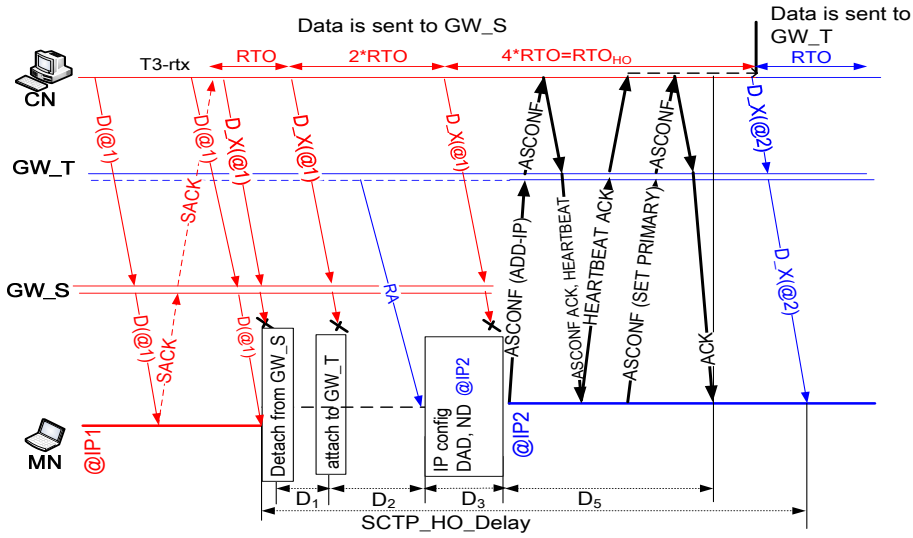


Figure 7.2: Handover delay components with m-SCTP mobility procedure

7.3 Problems encountered by SCTP-transported services during hard handover when used with m-SCTP

7.3.1 Problems

SCTP encounters a set of problems during hard handover when used with m-SCTP. We consider scenarios where the MN is receiving data from the CN and performing hard handover from one gateway (GW) to another one, both GWs belonging to different IP subnets.

7.3.1.1 Problems due to handover delays

As illustrated in figure 7.2, the hard handover includes different delay components:

- (D_1) the delay necessary for the MN to detach from the Source Gateway (GW_S) and attach at layer 2 to a Target Gateway (GW_T),
- (D_2) the delay necessary to receive IP subnet information through Router Advertisement (RA) for example,
- (D_3) the delay necessary for the MN to configure its interface with a new IP address and be able to use it (including DAD [56]),
- (D_5) the delay necessary to exchange m-SCTP signalling messages (ASCONF(ADD IP), ASCONF ACK, HEARTBEAT, HEARTBEAT ACK, ASCONF(SET PRIMARY), ASCONF ACK).

The **network handover delay** is the layer 2 and IP disconnection delay and is equal to (D_1+D_2+D_3). During this period, the MN is not able to receive data. The **transport handover delay** (**SCTP_HO_Delay**) is the delay perceived by SCTP layer on the MN side. It represents the time between the last packet received before handover and the first packet received after handover.

Note that D_1, D_2, D_3 are the same as the ones defined for Implemented ISC in chapter 6 for SIP native services, as they are independent of the service type. Therefore, the network handover delay (D_1+D_2+D_3) in case of m-SCTP is about 1180ms. To be generic, the SCTP behavior is described hereafter for different network handover delay cases.

Case 1: high network handover delay
High network handover delay in our context means that (D_1+D_2+D_3) value has led to retransmission timer (`T3-rtx`) expiration at least once before the reception of the HEARTBEAT ACK by the CN (knowing that the minimal `RTO` value is 1s in the RFC [106]).

During (D_1+D_2+D_3) period i.e. before receiving ASCONF(ADD IP), the CN continues to transmit data on the old MN IP address (@IP1) which is no more reachable. Each time `T3-rtx` expires, the CN retransmits the non-acknowledged packet towards the same address (the only one known by SCTP layer) after setting (`cwnd`=1MTU, `ssthresh`=`ssthresh`/2, `RTO`=`RTO`*2) and arming `T3-rtx` with the new `RTO` value. When the MN performs its network handover and the CN receives the ASCONF(ADD IP) (containing the new MN IP address (@IP2)) and the HEARTBEAT ACK, the CN still has to wait that the `T3-rtx` it holds for @IP1 reaches the current `RTO` value, RTO_{HO}, before being able to use @IP2 for retransmitting the data lost on @IP1 [106, 109, 110] (see figure 7.2).

Thus, the larger the network handover delay (D_1+D_2+D_3) is, the higher the number of `T3-rtx` expiration is, the higher RTO_{HO} is, and the higher the transport handover delay is.

Case 2: low network handover delay
Low network handover delay in our context means that (D_1+D_2+D_3) value hasn't led to any `T3-rtx` expiration in the CN, before the reception of the HEARTBEAT ACK message. In this case, when the CN receives the ASCONF(ADD IP), ASCONF(SET PRIMARY) and the HEARTBEAT ACK messages, it immediately transmits new packets towards the new MN IP address (@IP2) [106, 109]. When the MN receives these packets, it generates SACKs acknowledging them and indicating the missing packets (lost during handover) through the `Gap Ack Blocks` field. When these SACKs are received by the CN and missing packets have been indicated to the CN three times, the fast retransmit algorithm is triggered.

Thus, missing packets are retransmitted on a given path using slow start algorithm. During the recovery period, as the `Cumulative TSN Ack` field of SACK does not increase, the `cwnd` associated with that path remains constant [106, 111] instead of increasing exponentially. Consequently, even for low network handover delay SCTP performances are decreased.

7.3.1.2 Problems due to link change after handover

Another problem encountered by SCTP concerns the bandwidth under-utilization on the new link after handover. Indeed, following the reception of ASCONF(ADD IP) by the CN, the path CN-MN through @IP2 is initiated with initial values for SCTP congestion control parameters (`cwnd`=2MTU, `ssthresh`=65536, `RTO`=3s). Therefore, a period of time is necessary for the congestion window `cwnd` to reach its optimal value BDP (see section 7.1.2.3) enabling the maximum usage of the bandwidth

allocated by the Target Gateway. This problem is more critical for low network handover delays as the `cwnd` is slowed down during the recovery period instead of increasing exponentially.

Note that TCP suffers from a similar problem during handover, with slight differences. Unlike SCTP, after the MN handover, TCP on the CN side has not a new path to the MN. This means that it continues to send data to the MN with the values of congestion control parameters used on the old link established through the Source Gateway. If the new link through the Target Gateway has not the same characteristics as the old one, congestion control parameters are not likely to be adapted to the new one. A period of time will be necessary for the congestion window `cwnd` to reach its optimal value BDP (see section 7.1.2.3) on the new link.

7.3.2 Related work

As explained previously, the long transport handover delay problem has two causes: (1) the long network handover delay (D_1+D_2+D_3), and (2) the waiting time for `T3-rtx` expiration. Most of the references in the state of the art studying SCTP performances assume a high network handover delay and try to eliminate the second cause of the problem. [110] proposes an improvement consisting in triggering a particular SCTP configuration, called **m-SCTP+**, consisting in the following. Upon the reception of ASCONF(SET PRIMARY), the CN stops the ongoing `T3-rtx` and immediately retransmits the lost packets (for which `T3-rtx` has expired at least once). [109] proposes the same idea as [110], but lost packets are priorly determined by the CN, which sends a probe packet to the MN. Although the stated references show relatively good performances compared to the basic m-SCTP, they present two disadvantages: (1) they require cross-layering mechanism in the MN to rapidly detect hard handover and send ASCONF(SET PRIMARY) message, (2) ASCONF(SET PRIMARY) can be sent by the MN in other cases than hard handover, therefore the suggested SCTP configuration may be not needed and even undesirable. A more reactive solution with explicit information regarding the handover events and the required SCTP configuration shall be defined.

With regard to the first cause of the high transport handover problem, which is the high network handover delay, reference [109] proves that low network handover delays lead to better SCTP performances. To this end, it compares on the one side m-SCTP applying the improvement described above and considering 1,5s as the network handover delay, and on the other side FMIP [112] considering 0.5s as the network handover delay. Results show that FMIP has better results, due to the reduced network handover delay and to the absence of packet losses during handover, as these ones are tunneled from the old Gateway to the new Gateway. Although [109] shows the interest of FMIP, it does not precise whether FMIP is used for services transported over TCP or SCTP. Moreover, FMIP is not a good candidate from my point of view as it does not solve bandwidth under-utilization problem on one hand, and on the second hand it introduces tunnels which amplifies scalability issues.

Concerning the link bandwidth under-utilization problem, in [113], authors address this problem for TCP as well as the long transport handover delay problem. They criticize a set of solutions given in the state of the art and propose a TCP-HO solution where the MN reports to the CN handover events and the BDP of the new link through the Target Gateway. The CN stops transmission during one RTT and then begins transmission with `cwnd` equal to BDP. Reference [114] proposes a similar solution for SCTP by introducing a QoS measurement field within the ASCONF message sent to the CN, so that SCTP can adapt its `cwnd` accordingly. The drawback of [113, 114] is that they do not specify how the MN gets the QoS/BDP of the new link. This information requires that the MN communicates with the Target Gateway to negotiate the allocated bandwidth. Nevertheless, the delay necessary for this communication with the Target Gateway will increase the network handover delay.

7.4 Comparison between UFA, m-SCTP and other SIP-based solutions

7.4.1 UFA and m-SCTP

M-SCTP is only an end-to-end mobility signalling protocol: it does not provide tools to optimize mobility execution and relies on the MN mechanisms. The above analysis has proven that the MN mechanisms are not sufficient to deal with SCTP performance issues as they lack the necessary information to perform on-time and fine tuning of SCTP configuration.

On the contrary, UFA provides an optimized mobility management procedure with network-controlled mechanisms enabling to solve simultaneously the problems due to handover delays and link change, and to tune SCTP configuration during handover. Let us remind the main principles of UFA mobility procedure already detailed in section 4.2 and illustrated in figure 4.6. UFA mobility procedure enables during a preparation phase to pre-determine the SCTP layer configuration the CN should have consequently to the MN handover, and the all-OSI layers configuration the MN should have after its handover. These configurations are sent to the MN and the CN during the execution phase:

- The SCTP layer configuration contains the new MN IP address and the SCTP congestion control parameters (`cwnd`, `RTO`, `ssthresh`; considering the CN is the sender) to be communicated to SCTP layer. Congestion control parameters are calculated by the Target UFA Gateway according to the algorithm defined in section 4.1.2.3.
- The all-OSI layers configuration contains the MN IP and layer 2 configurations to be communicated to IP layer and layer 2, and the new MN IP address to be communicated to the SCTP layer.

Once the MN and the CN receive these configurations, they apply them.

During the MN handover, the Source UFA Gateway transfers the data packets received from the CN to the Target UFA Gateway. The Target UFA Gateway buffers the data packets received from the Source UFA Gateway and the CN until the MN attachment (reception of message 8 (Re-INVITE)).

Handover delay components for UFA non-SIP native services, are shown in figure 7.3. D_1 and D_3 are the same as the ones defined in chapter 6 for SIP native services, as they are independent of the service type. Therefore, the network handover delay (D_1+D_3) for UFA is about 80ms, as measured in chapter 6.

Compared to m-SCTP, UFA:

- **e**nables a reduced network handover delay. Indeed, the network handover delay for UFA is 80ms for UFA and 1180ms for m-SCTP.
- **p**rovides SCTP layer in the MN and the CN with explicit information regarding handover events and the required configuration. Moreover this configuration concerns the IP address and the SCTP congestion control parameters.
- enables the determination of SCTP configuration without impacting the handover delay.

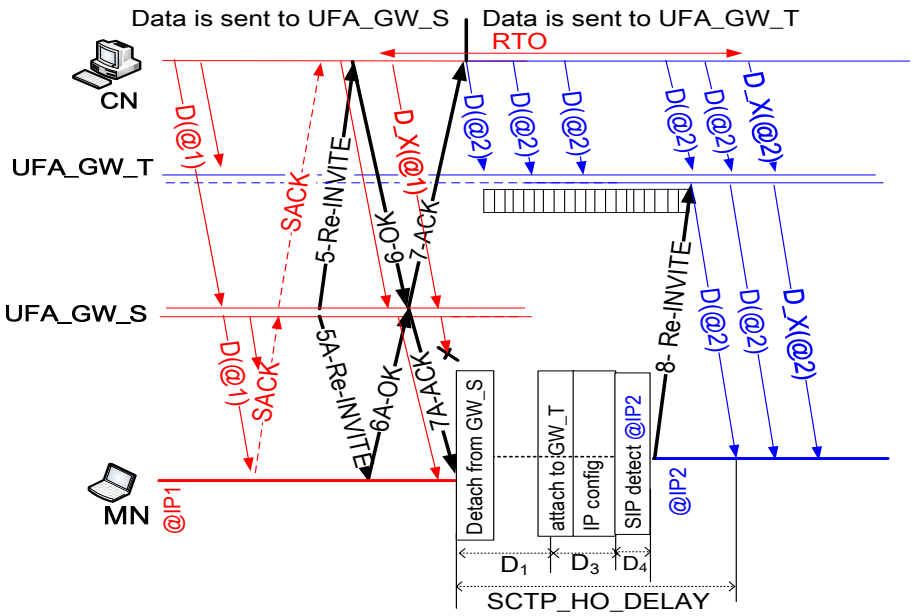


Figure 7.3: Handover delay components with UFA mobility procedure, for non-SIP native services

7.4.2 UFA and other SIP-based solutions handling SCTP-transported services

SIP has been already proposed to interact with SCTP-transported or TCP-transported services in many references [46, 47, 115] dealing with mobility management. There is one common point between these references and UFA and two important differences. The common point is the use of SIP to replace other mobility signalling protocols such as MIP or m-SCTP. The first difference is that these references do not solve SCTP problems described in section 7.3. The second difference is that, in these references, SIP is used without the support of a network-controlled architecture.

7.5 Different options for SCTP configuration in UFA

In UFA, the Source UFA Gateway sends to the CN the SCTP layer configuration, that contains: the new MN IP address and the SCTP congestion control parameters (`cwnd`, `RTO`, `ssthresh`). When this configuration information is received, SCTP enforces it according to three incremental configuration options, depending on which element of this information is considered. The reason behind the definition of these incremental options is to separately evaluate the benefits of each of them, and to ease the comparison with m-SCTP in the next section. Note that the procedure described in section 4.2 covers the most complete option (SxS++).

SCTP configuration options in UFA are [116]:

- **SxS** which is the minimal and basic configuration of SCTP, to support mobility for SCTP-transported services. It supposes the consideration of the new MN IP address only, described in table 4.3. This SxS configuration option replaces m-SCTP ASCONF signalling in terms of functions.
- **SxS+** which is based on SxS and additionally solves the performance problems raised in section 7.3.1.1 (case 2), as the handover delay in UFA is low. SxS+ triggers on the CN side

after receiving message 7 (ACK), immediate sending of lost packets before any new packet, preventing thus `cwnd` from remaining constant.

- **SxS++** which is based on SxS+ and additionally solves the link bandwidth under-utilization problem raised in section 7.3.1.2. With SxS++, SCTP congestion control parameters are enforced by SCTP layer: `cwnd` is set to the BDP corresponding to the bandwidth allocated by the Target UFA Gateway in order to gain time necessary to attain this value; `ssthresh` is set to the same BDP instead of the initial default value 65536bytes to keep the network stability; and `RTO` is set to 3s like the initial default value.

7.6 Performance evaluation

This section [116] evaluates by simulation UFA handover performances through a comparison with m-SCTP and its improved configuration m-SCTP+, described in section 7.3.2. For UFA, the different SCTP configuration options (SxS, SxS+, SxS++) are considered.

Section 7.6.1 details the simulation model and inputs. Section 7.6.2 provides practical cases and numerical values for the different SCTP behaviors in m-SCTP and UFA explained in the previous sections. Finally, section 7.6.3 gives the performance results.

7.6.1 Simulation model and inputs

A simulation model is constructed using the Network Simulator 2.33 tool [117]. For m-SCTP, ASCONF messages and the SCTP behavior when receiving ASCONF messages are implemented as described in the RFC [105] and in sections 7.2 and 7.3. For UFA, SIP protocol, UFA handover messages (3, 4, 5, 6, 7, 5A, 6A, 7A), as well as the different SCTP configuration options are implemented. When necessary, the Source UFA Gateway delays message 7 (ACK) sending to the CN until the reception of message 6A (OK) from the MN, as proposed in section 6.5.2.3. Data transfer from the Source UFA Gateway to the Target UFA Gateway during handover is not implemented. Buffering in the Target UFA Gateway of data received from the CN, until the MN attachment (message 8) is implemented. SIP handover messages (5, 7, 5A and 7A) are prioritized in the Source UFA Gateway compared to the data traffic, so that they can be sent on time. It has to be noted that in chapter 5, SIP traffic has been considered as having a lower priority than conversational and streaming traffic. This hypothesis should also have been considered in this chapter, as non-SIP native services may be assimilated to conversational or streaming traffic. However, we observed that in that case SIP handover messages are blocked in the UFA Gateway buffer and take a long time to arrive to the MN and the CN.

During a given simulation time (500 seconds), the MN downloads a file from the CN. Hard handover for the MN is simulated by periodically switching between two Gateways. The switching periodicity determines the handovers number (**HO_nbr**) occurring during data downloading.

Simulation inputs and parameters are as follows:

- D_{GW-CN} and $Xput_{GW-CN}$ which are respectively the propagation delay and the bandwidth on the links between the CN and the Source Gateway or the Target Gateway (figure 7.4).
- D_{GW-MN} and $Xput_{GW-MN}$ which are respectively the propagation delay and the bandwidth allocated to the MN, on the links between the Source Gateway or the Target Gateway and the MN (figure 7.4).
- The receiver buffer size in the MN is 65536bytes.

- The network handover delay (D_1+D_2+D_3) for m-SCTP and m-SCTP+ is 2s, in the same range as the values measured on the testbed for Implemented ISC.
- The network handover delay (D_1+D_3) for UFA is 80ms, as measured on the testbed.
- For UFA D_4 is 70ms, as measured on the testbed (see section 6.5.1.2).
- The length of UFA handover messages is the same as the one measured on the testbed and given in table 6.2.

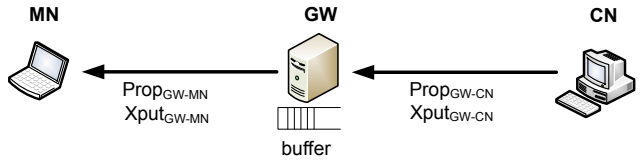


Figure 7.4: Network parameters

Simulations are conducted using the different network scenarios given in table 7.1.

Parameter	**Sc1**	**Sc2**
D_{GW-CN} (ms)	10	100
$Xput_{GW-CN}$ (Mbps)	10	10
D_{GW-MN} (ms)	2	2
$Xput_{GW-MN}$ (Mbps)	1	variable (0.1...3)
HO_nbr	variable (1...13)	6

Table 7.1: Considered network scenarios (Sc) for simulation

7.6.2 SCTP behavior analysis

Figure 7.5 provides the TSN (Transmission Sequence Number) of the packets sent by the CN side during handover for m-SCTP and UFA SxS, considering the network scenario Sc1 and HO_nbr=6. Packets lost during handover are those contained in the source Gateway buffer before the MN detachment and those sent by the CN after that time to the Source Gateway.

Based on flags indicated on figure 7.5 and on packet traces obtained through the simulator log files, the following analysis is provided to emphasize and illustrate the SCTP behavior explained in section 7.3:

- For m-SCTP, the MN detaches from the Source Gateway at 71s and attaches to the Target Gateway 2s later at 73s. Packets (TSN 5859-5866) are lost. As the CN does not receive SACK, it stops data transmission until `T3-rtx` (1s) expiration at 72.008s where it retransmits (flag E) the packet (TSN 5859) via the Source Gateway and triggers a second timer with `RTO` equal to 2 s. Even though the CN receives HEARTBEAT ACK at 73.037s, it retransmits the packet (TSN 5859) via the Target Gateway only after the `T3-rtx` expiration at 74.008s (flag F).
- For SxS, the Source UFA Gateway sends at 71s messages 7 (ACK) and 7A (ACK) respectively to the CN and the MN. The MN detaches from the Source UFA Gateway at 71.031s after receiving 7A and attaches to the Target UFA Gateway at 71.182s. Packets (TSN 5861 - 5866) are lost.

  When the CN receives message 7 at 71.032s, as `T3-rtx` has never expired, it immediately transmits 2 packets (`cwnd`=2MTU) to the MN via the Target UFA Gateway (flag A). These

ones are buffered in the Target UFA Gateway until the MN attachment. When they are transmitted to the MN and acknowledged, new packets can be sent (flag B) and at third indication for each of the missing packets (TSN 5861 - 5866) through `Gap Ack Blocks` filed, fast retransmit is triggered to retransmit them (flag C). When lost packets are recovered, new packets are transmitted (flag D).

Figure 7.6 shows the evolution of `cwnd` for the different UFA SCTP configurations considering the network scenario Sc2 with $Xput_{GW-MN}$= 1Mbps. Contrary to SxS++ where `cwnd` is directly set to BDP (28550bytes) after handover, in SxS `cwnd` needs 4.3s to reach BDP. This time period (4.3s) is composed of two parts. In the first part (3s), `cwnd` remains constant (3MTU) and cannot increase as SCTP is retransmitting lost packets detected through `GAP Ack Blocks` field (see section 7.3.1.1, case 2). In the second part (1.3s), as all lost packets have been retransmitted, `cwnd` increases rapidly because of the slow start mode until reaching 65536bytes (`ssthresh`).

SxS+, contrary to SxS, enables to skip the 3s time period and to reach BDP in 1.3s as the CN transmits lost packets first, avoiding thus `cwnd` from being slowed down.

7.6.3 Performance results

To compare the different solutions, different key performance indicators are measured, such as the transport handover delay, the mean bandwidth and the volume of data downloaded during the simulation time (500s). Only results regarding the downloaded data volume indicator are given, as this indicator is the most global and pertinent one contrary to the transport handover delay. Indeed, the transport handover delay impacts the volume of downloaded data but is not enough to reflect it, as this latter depends on `cwnd` evolution which may remain constant after handover instead of increasing exponentially (see section 7.6.2).

Firstly, m-SCTP, m-SCTP+, SxS, SxS+ and SxS++ are compared for the network scenario Sc1 (see table 7.1), considering different values for the handover number (HO_nbr). A HO_nbr value corresponds to a given MN velocity. For example, HO_nbr=6 corresponds to a pedestrian walking at 5km/h in an area covered by 100m-diameter cells or a user in a car traveling at 51km/h in 1km-diameter cells.

Figure 7.7 gives the additional data volume m-SCTP+, UFA, SxS+, SxS++ enable to download compared to m-SCTP. For m-SCTP, the downloaded data volume is 62, 61, 60, 59, 57 Mbytes for HO_nbr equal to 1, 3, 6, 9, 13 respectively.

It can be observed that all UFA configuration options enable to download more data than m-SCTP. Moreover they are more efficient than m-SCTP+, considered in the state of the art as the best improvement to m-SCTP performance. Indeed, m-SCTP+ enables a gain ranging from 0.2% to 2% compared to m-SCTP, whereas UFA enables a gain ranging from 0.4% to 7.8% compared to m-SCTP.

For this network scenario Sc1, SxS+ and SxS++ do not provide remarkable gains compared to SxS as both D_{GW-CN} and BDP are low, which enable packets lost in SxS to be recovered rapidly (SACKs are returned rapidly) and `cwnd` to attain rapidly BDP.

Therefore, the performances of SxS, SxS+ and SxS++ are compared using the network scenario Sc2 (see table 7.1) that considers higher values for D_{GW-CN} and BDP (higher value for $Xput_{GW-MN}$). The receiver buffer size in the MN is set to 200000bytes, in order to take into account the high bandwidths ($Xput_{GW-MN}$ equal to 2Mbps or 3Mbps). Figure 7.8 shows the additional data volume SxS+ and SxS++ enable to download compared to SxS. For SxS, the downloaded data volume is

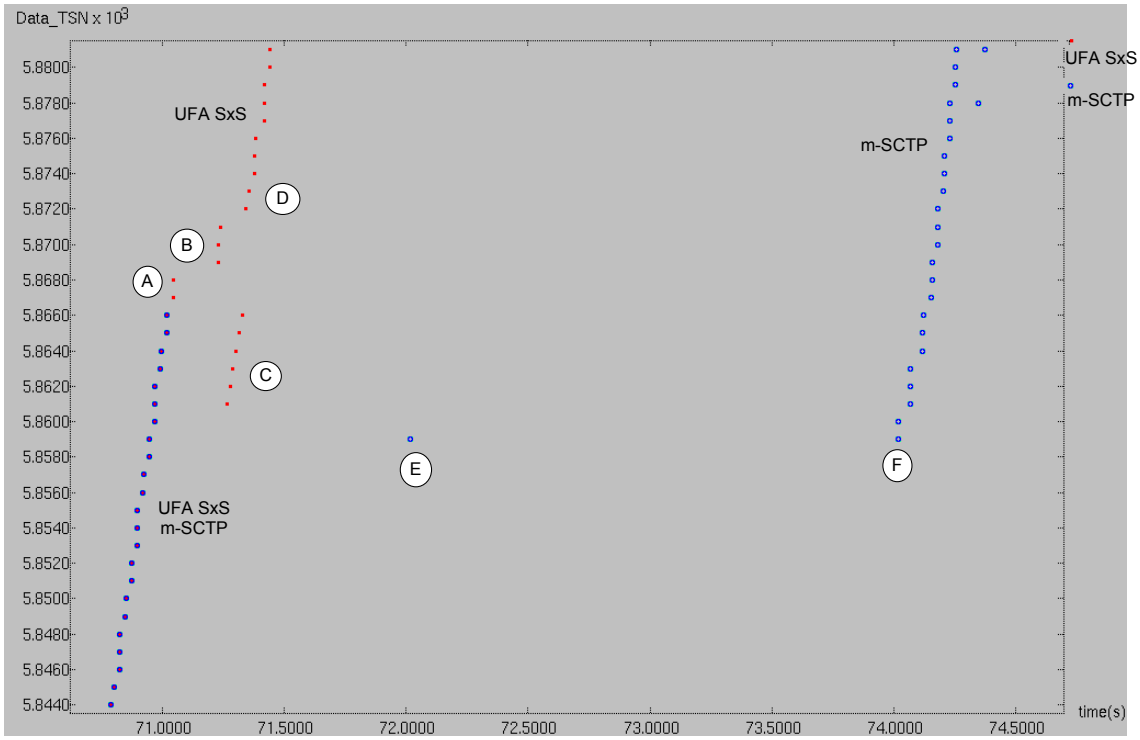


Figure 7.5: TSN on the CN side for m-SCTP and UFA SxS configuration option in the network scenario Sc1

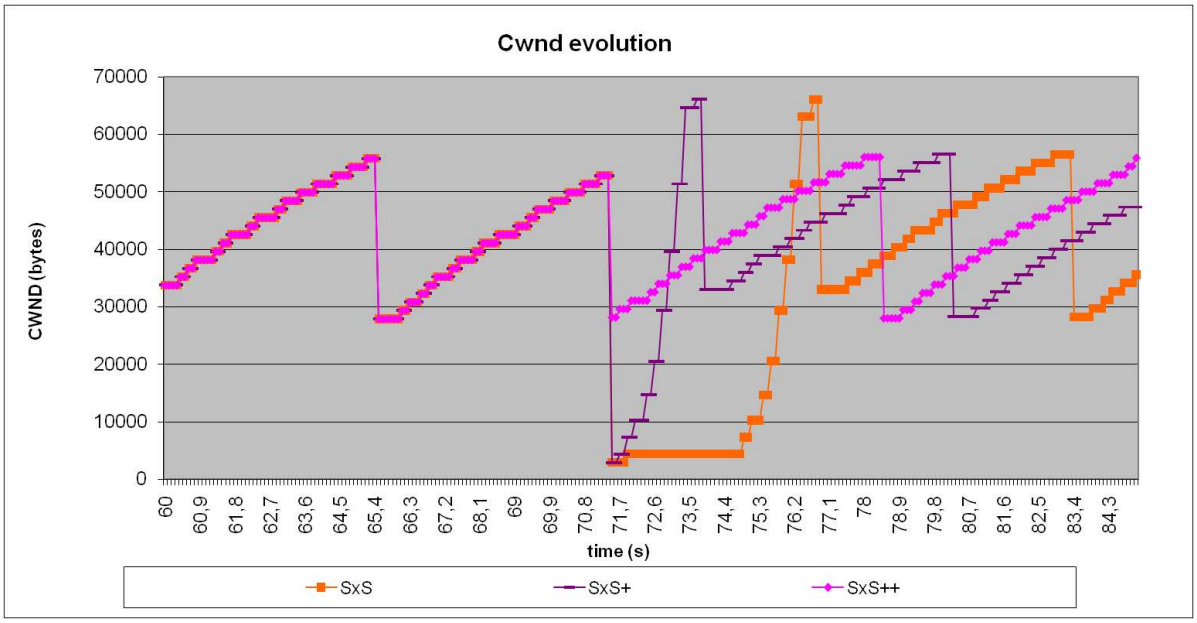


Figure 7.6: `Cwnd` for the different UFA SCTP configuration options in the network scenario Sc2

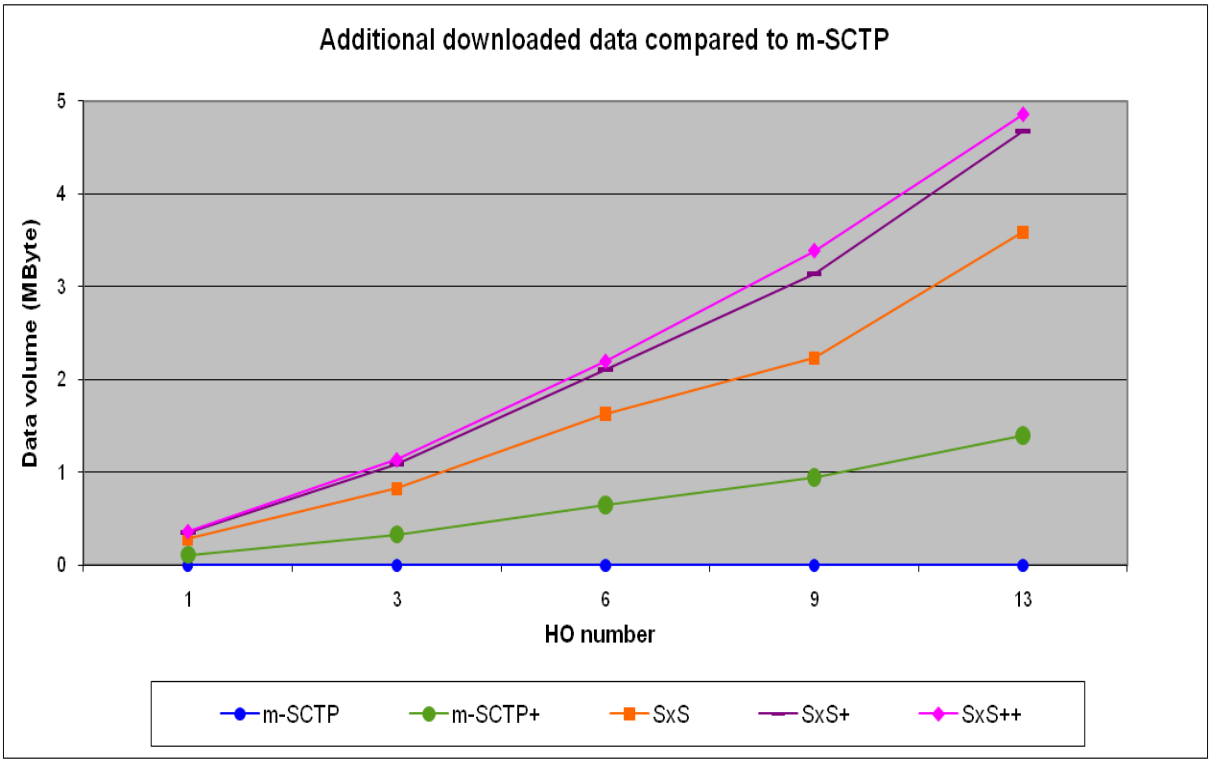


Figure 7.7: Comparison of m-SCTP, m-SCTP+, SxS, SxS+, SxS++ in the network scenario Sc1

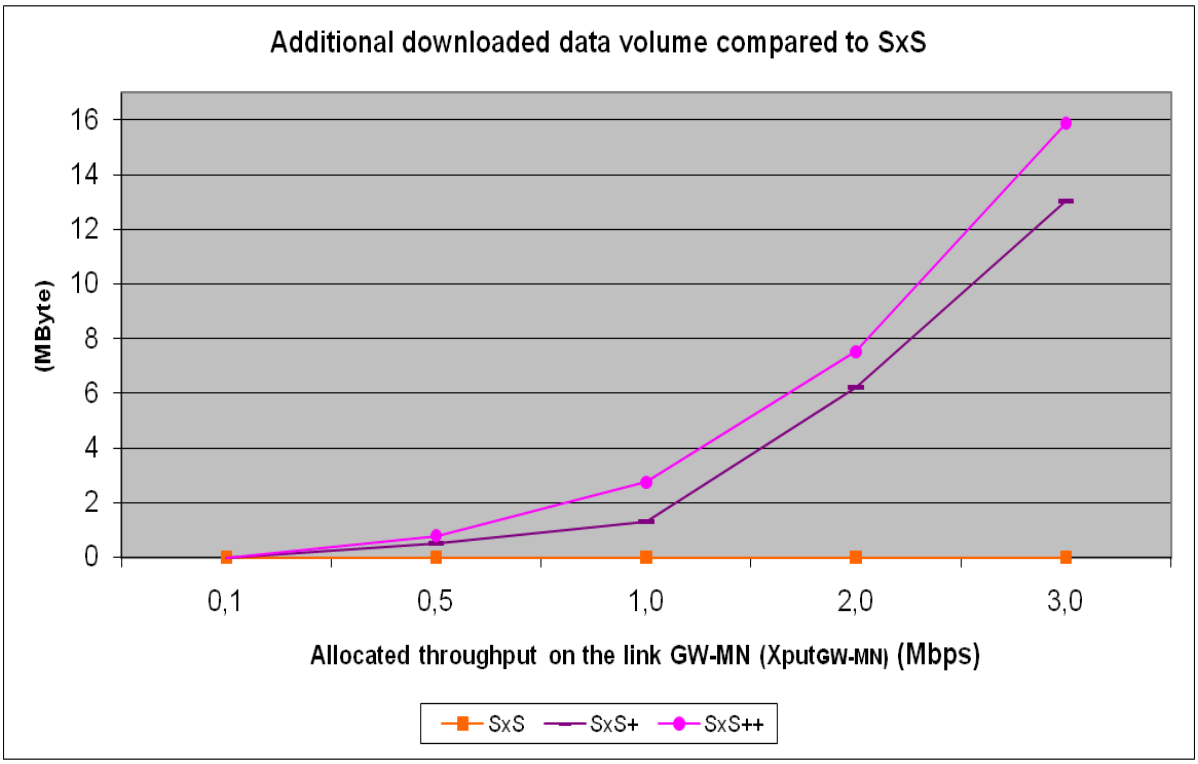


Figure 7.8: Comparison of SxS, SxS+, SxS++ in the network scenario Sc2

6, 28, 57, 116, 168 Mbytes for $Xput_{GW-MN}$ equal to 0.1, 0.5, 1, 2, 3 Mbps respectively. It can be observed that, compared to SxS:

- SxS+ enables a gain varying from 2% to 7% for $Xput_{GW-MN}$ varying from 1 to 3Mbps, and
- SxS++ enables a gain varying from 4% to 9% for $Xput_{GW-MN}$ varying from 1 to 3Mbps.

Thus, SxS+ and SxS++ provide better performances than SxS. Moreover, the benefits of SxS+ compared to SxS are more important than those of SxS++ compared to SxS, given the fact that SxS+ enables to skip the important time period during which `cwnd` is constant (see figure 7.6).

In general, although the additional downloaded data volume may appear relatively low (1...14Mbps), this one shall not be neglected as it has been calculated for a short downloading time period (simulation time=500s) and for a single MN. The gain for an operator is important as it is proportional to the number of MNs and to the duration of data downloading (higher than 500s).

7.7 Conclusion

This chapter has underlined the strengths of UFA compared to m-SCTP and other SIP-based solutions managing the mobility of SCTP-transported services and optimizing their performances during handover. UFA relies on SIP, a network-controlled mobility procedure and cross-layer mechanisms to optimally drive SCTP configuration on the MN and the CN during handover. Three incremental UFA SCTP configuration options are conceived. The first option, shortly named SxS, is the basic one. It configures SCTP layer with the new MN IP address and reduces the handover delay. In SxS+ based on SxS, SCTP on the CN side is enhanced by immediately sending lost packets through the new link, before new packets. SxS++ based on SxS+, additionally updates SCTP congestion control parameters according to the new link bandwidth.
SxS++ solves simultaneously the problems encountered by SCTP-transported services when used with m-SCTP, that are packet losses due to handover delays and bandwidth under-utilization due to link change after handover.

All UFA SCTP configuration options have been implemented and compared to m-SCTP and its best improvement (m-SCTP+), proposed in the state of the art to deal with the problems due to handover delays. Performance results are promising:

(1) All UFA SCTP configuration options provide better performances than m-SCTP.

(2) SxS is even better than enhanced m-SCTP solutions (m-SCTP+).

(3) Both SxS+ and SxS++ improve UFA performance.

The gain obtained with UFA configuration options is important for an operator; it is proportional to the number of MNs and the duration of data downloading.

UFA principles can be also applied for TCP-transported services for configuring their congestion control parameters, but in this case a solution has to be defined to hide the IP address change from TCP.

Part IV

Conclusion and future work

CHAPTER 8 Conclusion and future work

8.1 Thesis summary

This thesis has highlighted the importance of flat network models in enhancing the readiness of mobile network operators for the new telecommunication ecosystem, characterized by an exponential traffic increase. Different steps, given below, have been necessary to reach such a conclusion.

Specifying requirements for mobile networks to face the ecosystem challenges

- **Characterizing the new telecommunication ecosystem**: the work in this thesis has started with characterizing the new telecommunication ecosystem in which mobile networks evolve. It has also raised the need to analyze the mobile networks readiness to face the challenges of this ecosystem. The first challenge is the exponential traffic increase due to the high bitrate radio interfaces, the emergence of high bitrate applications and the increasing number of mobile users. The second challenge is the stagnation of operator revenues due to the adoption of new business models based on flat rates. Part of these challenges has been the object of [38, 80].

- **Modeling current mobile networks and analyzing their readiness for the new ecosystem**: mobile networks have been modeled in order to analyze their readiness for the new ecosystem. Mobile networks model (IP-AN//PCC//IMS) includes the IP access network (IP-AN) offering IP connectivity to users, the IMS providing service control for the IP-ANs, and the PCC ensuring the interaction between the IP-AN and the IMS with regard to the policy control function.

  Current IP access networks are characterized by a centralized anchor node (first IP router) and different intermediate anchor nodes implementing specific functions and hiding the users mobility from the higher level anchor nodes. IMS and PCC nodes are inevitably centralized, as they are located in the IP network behind the IP access network.

  Four criteria have been considered in analyzing this IP-AN//PCC//IMS network model: service control, scalability, service and network convergence, QoS. It has been observed that, to meet these criteria, this model needs to implement additional functions at the expense of more complexity and a non-idealistic solution.

  The model is not scalable as it is centralized and contains numerous node types and interfaces. Moreover, it lacks a mobility procedure between the centralized anchors (first IP routers),

which are initially designed to be unchanged whatever the user mobility is (e.g. GGSN in UMTS).

The model suffers from the following QoS problems: a long delay to access services, a high handover delay between the centralized nodes (e.g. GGSN), and a service non-adaptation to the resources available in the IP Access network. These problems are due to a high number of signalling messages involved in the service access and mobility procedures, the fact that these messages cross the IP-AN//PCC//IMS centralized nodes, and the fact that the service control layer (responsible for service adaptation) doesn't interact well with the resource information located in the different IP access network nodes.

Part of this analysis has been published in [38, 80, 81, 85].

- **Specifying requirements for mobile networks to face the ecosystem challenges**:

  The analysis of how the IP-AN//PCC//IMS model meets the defined criteria (service control, scalability, QoS, service and network convergence), has led to setting respectively different requirements. These have to be fulfilled by a mobile network in order to face the ecosystem challenges better:

  - Requirement 1: the service control shall be provided to all applications in a cost effective manner. IMS is a service control solution already available for SIP native applications. It is proposed to extend it to all applications.
  - Requirement 2: the mobile network has to be scalable. It means that, in case of huge data growth, network investments shall remain profitable for operators.
  - Requirement 3: a simple and optimal mobility procedure between the first IP routers, handling the same IP-AN type (e.g. between GGSNs in UMTS) or different IP-AN types has to be supported.
  - Requirement 4: service and network convergence shall be provided.
  - Requirement 5: the service access procedure shall be optimized, in terms of necessary signalling messages, tasks and mapping functions.
  - Requirement 6: the number of nodes within the mobile network model shall be reduced in order to enhance the service access and the handover delay.
  - Requirement 7: centralized nodes shall be avoided i.e. nodes shall be rather distributed in order to enhance the access and the handover delays.
  - Requirement 8: a tight interaction between the service control layer (IMS) and the network layer (IP-AN) shall be possible, without making the network more complex. This would allow a reactive service adaptation solution.
  - Requirement 9: load information as well as other handover decision inputs shall be made easily available to the handover decision function.

  Part of these requirements have been stated in [38, 80, 81, 85].

Proposing a new model (UFA, Ultra Flat Architecture) for future mobile networks

The above requirements have incited me to review the IP-AN//PCC//IMS network model and to define a new model, called UFA (Ultra Flat Architecture).

UFA is a flat model that uses IMS as a unified service control layer for all applications. Therefore, it is entirely based on SIP. In UFA, the classical IP-AN node functions (e.g. NodeB, RNC, SGSN

and GGSN functions for UMTS), the policy control functions and the IMS functions, are gathered within the same node, which is the UFA Gateway.

The UFA model relies on distributed and temporary anchors, which allows the traffic load distribution. UFA flat model enables the removal of redundant user context information and the definition of smart and optimized service access and mobility procedures. These procedures are based on SIP and are controlled by the network. The reduction of the network node types is useful in reducing the access and handover delays. Moreover, the resource information and the service control functions gathered in the same node, made it possible to tune the service or the transport layer configuration in the mobile and corresponding nodes.

The first UFA proposal was in [38, 80]. It was then enhanced and completed in [81, 85, 116].

Evaluating UFA architecture

In this thesis, UFA concepts have been demonstrated and its performances have been evaluated regarding different criteria and using different means:

- The service access delay in the IP-AN//PCC//IMS and UFA models have been compared using an analytical approach and considering different network load situations. Results have shown that UFA provides a reduction of 50% in terms of service access delay in low load situations, and much more in high load situations. They have also confirmed the IP-AN//PCC//IMS scalability issues, and the negative impact of its centralized and hierarchical architecture on the access delay. Part of these results have been published in [85].
- UFA concepts have been proved through their implementation and evaluation on a testbed. UFA handover delay has been measured and compared to the IMS Service Continuity (ISC) procedure, applicable in the IP-AN//PCC//IMS model. Results have shown that UFA provides, for applications transported over RTP/UDP, a handover delay 12 times inferior than ISC, at the application level. These results have been given in [81].
- UFA interest has been proved for applications transported over SCTP. Indeed, UFA architecture and mobility procedure enhances the performances of these applications during user mobility. It has been demonstrated that, mobile SCTP protocol, the best known solution handling the mobility of these applications till now, is not enough to obtain a good performance for these applications, and that UFA, as a complete architecture, is well adapted.

Proposing other signalling alternatives for UFA

As described previously, UFA presented in this report relies on SIP protocol. Other signalling alternatives have been introduced for UFA e.g. based on the Host Identity Protocol (HIP). [118] compares the SIP-based alternative and the HIP-based one and shows that the SIP-based one is better than the HIP-based one, especially for SIP native applications. Other alternatives are proposed and compared in [119].

8.2 Future work

Flat architecture models will be the main characteristic of future mobile networks. This thesis has presented a possible flat model (UFA). Future work related to UFA, as well as future research topics related to other flat architectures are presented in the following:

- Paging solution for UFA: in classical networks, a terminal can be reached (in case of an incoming call for example), only if it has an always-on context in the network i.e. it has an active IP address and is registered in IMS with its active IP address. This solution can be applied in UFA. However, it would require an important signalling load as the terminal will have to update its IP address in the IMS each time it moves from a UFA Gateway to another. Therefore, optimal registration update and paging procedures have to be defined.

- Other models than UFA: UFA is a first proposal for the model requirements defined in chapters 1 and 2 of this thesis. Other models obeying to the defined requirements can be defined, particularly those based on two nodes instead of one. For example: the UFA Gateway continues to implement the same functions defined for it, except the physical connectivity. Other nodes will offer this connectivity. Another example is to separate the UFA Gateway transfer and control planes into two nodes. This would very likely ease the dimensioning of these two nodes as they have different dimensioning criteria. Nevertheless, a new interface will be needed between both nodes.

  The different identified models shall be then compared.

- Tools for scalability evaluation: in chapter 1, the scalability of mobile networks is evaluated regarding the number of nodes and interfaces. These criteria are simplistic and other criteria have to be defined and considered, especially when evaluating the different new model proposals. A first list of criteria could be: the number of active contexts per node, the signalling load of the different network nodes to execute the network procedures, the data load of the different network nodes.

Part V

Appendices

APPENDIX A

SIP, SDP and mobility management with SIP

A.1 SIP

The Session Initiation Protocol (SIP) is a session protocol that allows to manage and integrate different kinds of applications such as Presence, Instant Messaging, distributed games, white boards, etc. With SIP, two or more participants can establish or modify sessions to get access to these applications part of the final service. SIP allows to support MN mobility by informing CN about the new MN IP address.

SIP was designed by Henning Schulzrinne (Columbia University) and Mark Handley (University College London). The latest version of the specification is RFC 3261 [18] from the IETF SIP Working Group, which has been finalized in 2002.

A.1.1 SIP architecture

SIP defines a number of logical entities, namely User Agents, redirect servers, proxy servers and registrars.

- The SIP **User Agent** (UA) is the endpoint of SIP signalling (requests and responses) and application data flows. The User Agent Client (UAC) is the caller that initiates SIP requests, and the User Agent Server (UAS) redirects, rejects, or accepts the SIP requests.
- The **redirect server** receives SIP requests and returns a response that indicates where the requester should send the request next.
- The **proxy server** receives and forwards SIP messages. It can interpret or rewrite certain parts of SIP messages that do not disturb the state of a request or dialog (see definition below) at the endpoints, including the body.
- The **registrar** is a server that accepts SIP REGISTER requests. These servers are used to store explicit binding between a user address of record (SIP address) and the address of the terminal where the user is wishing to receive requests.
- The **Application Server** (AS) is an entity in the network that provides users with a service. Typical examples of such servers are presence and conferencing servers.

- The **Back-to-Back-User-Agent** (B2BUA) is a proxy where a UAS and a UAC are glued together. The UAS terminates the request as a normal UAS. The UAC initiates a new request that is somehow related to requests received on the UAS side. The way the UAC builds the new request based on the received request is internal to the B2BUA and is not standardized. This entity is almost like a proxy, but it breaks all the rules that govern the way a proxy can modify a request. It maintains dialog state and must participate in all requests sent on the dialogs it has established.

A.1.2 Transactions and dialogs

- A **transaction** is a request and all its related provisional responses until the final response indicating whether the request has succeeded or not.
- A **dialog** represents a peer-to-peer SIP relationship between two User Agents, that persist for some time. The dialog facilitates sequencing of SIP messages between the User Agents and proper routing of requests between both of them. A dialog is identified at each UA mainly with a Call-ID value. It is characterized by: the value of its headers (*Request URI*, *To*, *From*, *Call-ID*, *via*, etc) and the body.

A.1.3 Addresses within SIP

SIP relies on two types of addresses:

- The **Address of Record** which is the logical address of a user/resource. It can be a SIP URI (Uniform Resource Identifier) or TEL URI. The SIP URI has the format of an email address.
- The **Address of Contact** which is the physical address of a terminal. A user having an address of record will have an address of contact for his terminal.

A.1.4 SIP messages format

The SIP message is made up of 3 parts: the start line, the message headers and the body. Table A.1 shows these items in the SIP INVITE request massage.

A.1.4.1 Start line

The start line content varies depending on whether the SIP message is a request or a response. For requests, it is referred to as a **request line**; and for responses, it is referred to as a **status line**.

The **request line** has three components: a method name, a Request URI and the protocol version:

- The **method name** indicates the name of the request. The INVITE, CANCEL, ACK and BYE methods are used for session creation, modification and termination. The REGISTER method is used to register a certain user address of contact. The OPTIONS request is used as a poll for querying servers and their capabilities.
- The **request URI** is a SIP or a SIPS URI that identifies a user/resource the request is addressed to.
- The protocol version: refers to the version of SIP e.g. SIP/2.0.

The **status line** has three components: the protocol version, the status code and the reason phrase:

- The **protocol version** is identical to the protocol version in the request line.
- The **status code** is a three-digit code that identifies the nature of the response. It indicates the outcome of the request. 1xx-indicates a provisional/informational response and 2xx-indicates a success response.
- The **reason phrase** is a free text field providing a short description of the status code. It is mainly aimed at human users.

```
//Request line
INVITE sip:callee.smith@nokia.com SIP/2.0
//SIP headers
Via: SIP/2.0/UDP pcscf.example.com: 5060; branch=z9hG4bK8542.1
Max-Forwards: 69
From: caller <sip:caller@nokia.com>;tag=312345
To : callee <sip:callee@nokia.com>
Call-ID: 105637921
CSeq: 1 INVITE
Contact: sip:caller@[5555::1:2:3:4]
Content-Type: application/sdp
Content-Length: 159
//SIP body e.g SDP
...
...
```

Table A.1: SIP INVITE request message

A.1.4.2 SIP Headers fields

Header fields contain information related to the initiator of the request or to the responder. The format of the header fileds is: Header-name: header value.

There are different kinds of headers as shown in Table A.2.

SIP header	Meaning
Request URI (within the request line)	indicates the user or resource to which this request is being addressed. In the UAC, the initial Request URI is populated with the value in the *To* header. For subsequent requests, the *Request URI* is equal to the first URI from the received *route set* header or to the remote user. The proxies change the *Request URI* to the next hop URI to route the request.
To	specifies the address of record of the request receiver. Usually the user will suggest the *To* header field through a human interface, perhaps inputting the URI manually or selecting it from some sort of address book. Frequently, the user will not enter a complete URI, but rather a string of digits or letters (for example, bob). The *To* header is not changed by the proxies at the opposite to *Request URI* header.

From	indicates the address of record of request initiator. Like the *To* header field, it contains a URI and optionally a display name.
Call-ID	identifies the dialog, possibly with the *From Tag* and the *To Tag*. Note that the *From Tag* is added by the caller when sending the first dialog request, and the *To Tag* is added by the callee when sending the response to the first received request.
Cseq	identifies the method to which the request and the response are associated to
Max-Forwards	specifies the maximum nodes crossed by a SIP Request or Response
Contact	indicates the address of contact of the message sender.
Via	traces the path taken by a request so far, and indicates the path that should be followed in routing the response related to that request.
Record-Route	it is inserted by proxies in a request to force the subsequent requests in the dialog to be routed through the proxy.
Route	it is contained within requests. It is used to force routing the request through the listed set of proxies. It can be a copy of the Record-Route received within a response.
Route Set	it is a collection of ordered SIP URI which represent a list of proxies that must be traversed when sending a particular request. A *Route Set* can be learned, through headers like Record-Route, or it can be configured.

Table A.2: SIP headers

A.1.4.3 Message Body

The message body (payload) describes elements controlled by the session. It carries any text-based information. Session Description Protocol (SDP) (see below) is a typical example of a message body.

A.2 SDP

The Session Description Protocol (SDP) is a session protocol intended to describe on the transfer plane the service controlled by the SIP session. SDP is published in RFC 4566 [65] in July 2006.

It is a text-based protocol. When describing a service, the caller and the callee indicate their respective "receive" capabilities in terms of application types and application formats. They also specify the IP address used to send and receive applications data flows and the transport port used to each application data flow. Capability exchange can be performed during the session set-up or for an ongoing session.

Using the **SDP offer/answer** mechanism, two users agree on the application types and formats they want to use for a specific service. One of the caller/callee proposes an offer and the other answers whether it supports the overall/ a part/ or none part of this offer.

Table A.3 provides an example of SDP for a video call. SDP contains different lines, we give hereafter the main ones:

- The ***c* line** indicates the IP address the SDP sender is going to use for the application streams.
- The ***m* line** contains the application type, the transport protocol, the transport port used for the application). Lines following the m line contain more information about the application format.

```
v=0
o=- 2987933615 2987933615 IN IP6 IN IP6 5555::1:2 : 3 : 4
s=-
//c field
c = IN IP6 5555: :1:2:3:4
t=907165275 0
//m line 1: audio application
m=audio 3458 RTP/AVP 0 96 97 98
//a lines for audio formats (codecs): PCMU, G726, AMR
a=rtpmap:0 PCMU
a=rtpmap:96 G726-32/8000
a=rtpmap:97 AMR-WB
a=rtpmap:98 telephone-event
//m line 2: video application
m=video 3400 RTP/AVP 99 100
//a lines for video formats (codecs): H263, MP4V-ES
a=rtpmap:99 H263
a=fmtp:99 profile-level-id=0
a=rtpmap:100 MP4V-ES
```

Table A.3: example of SDP for a video call

`Data flow descriptors` are deduced from the *c* line (IP address) and the *m* line (transport port).

A.3 Example of service management with SIP: establishment, mobility execution, termination

The main steps for service establishment, mobility execution and service termination with SIP are (Figure A.1)

1. The MN initiates a session towards the CN by sending him a SIP INVITE messaage. It indicates in the *contact* field the IP address to be used by the CN to send SIP answers, and in the SDP *c* line the IP address to be used by the CN to send him data flows. It also inserts a *via* or a *route* header to indicate the first proxy to which the request should be sent.

2. When the CN accepts the call, a SIP 200 OK response is generated and sent to the MN. In this message the CN puts in the *contact* field and *c* line its IP address as the MN did.

3. Upon the receipt of the CN response, the MN sends a SIP ACK message to acknowledge the reception of the SIP 200 OK response.

4. Applications flows are exchanged.

5. When the CN moves and gets a new IP address, it sends a SIP Re-INVITE or SIP UPDATE message with a *contact* field and *c* line containing its new IP address.

6. When the CN receives the SIP Re-INVITE, it takes into account the new MN IP address and sends a SIP 200 OK answer and the data flows towards this address.

7. Upon the reception of the CN response, the MN sends a SIP ACK message to acknowledge the reception of the SIP 200 OK response.

8. After the MN hangs up, a BYE request is generated and sent to the CN to terminate the session.

9. The CN confirms that the session is over with a 200 OK response. The service is ended too.

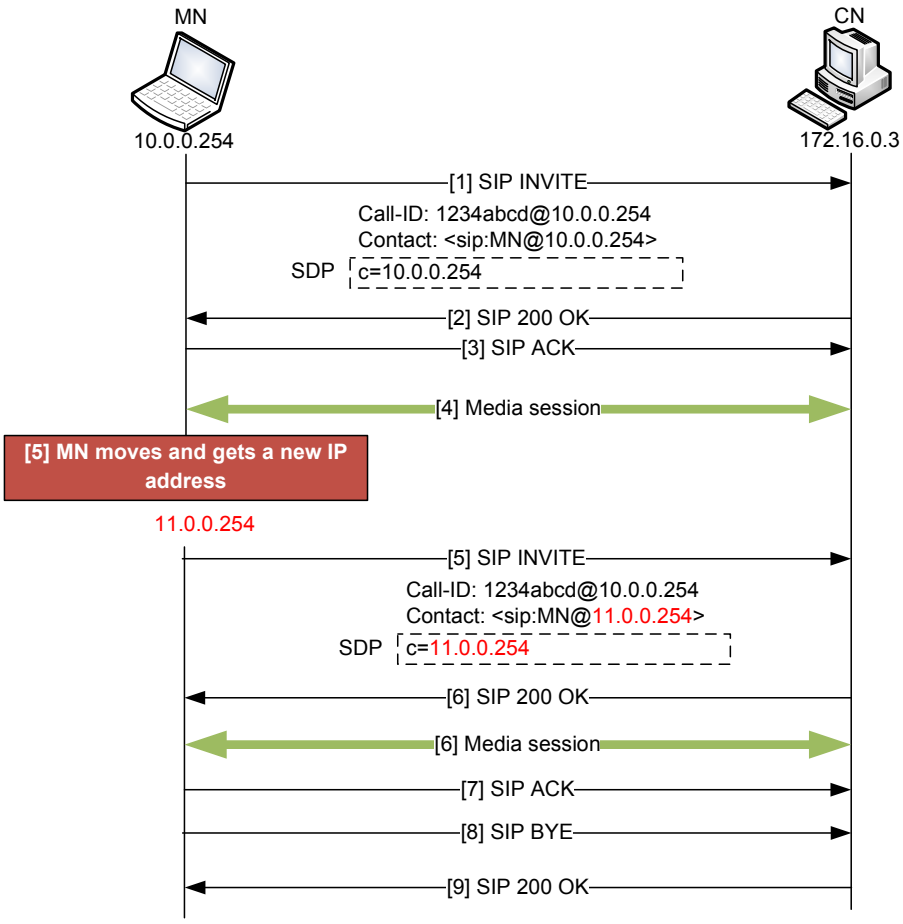


Figure A.1: Example of service management with SIP: establishment, mobility execution, termination

APPENDIX B IPsec Security Association contexts

In IPsec terminology, the outbound traffic is the traffic that needs to be protected by IPsec, and the inbound traffic is the traffic that needs IPsec decapsulation. A security association is identified uniquely by the Security Parameter Index (SPI) contained within IPsec databases and IPsec header.

Entities terminating IPsec SA use two main contexts/databases [120, 52]:

- The Security Policy Database (SPD) maintains the list of security policies (service) to apply to inbound/outbound traffic. It is consulted during the processing of all inbound or outbound traffic and contains:
  - The traffic selectors that identify the packets to which a security policy shall be applied. They are the IP source address, the destination IP address, the source port, the destination port and the next layer of the received packets.
  - The security policies which are:
    - For outbound traffic :
      - Protect, bypass or discard the traffic.
      - If protect, and a SA do not exist (not already created) for that traffic, then a SA shall be created. Else, if a SA exists, a link to SAD (see below) is provided.
      - IPsec mode (tunnel/transport) for the SA to be created, if tunnel mode: local/remote tunnel address.
      - AH/ESP algorithms for the SA to be created.
    - For inbound traffic: the way to search the related Security association (SA) in the SAD (based on SPI, or based on SPI and remote IP address).
- The Security Association Database (SAD) contains the description of the SAs existing for inbound and outbound traffic. This description indicates how to process the traffic:
  - For outbound traffic, it contains: AH/ESP algorithms/keys, IPsec mode, tunnel header.
  - For inbound traffic, it contains: SPI, AH/ESP algorithms/keys, IPsec mode, tunnel header, and selectors. After applying the AH and ESP algorithms as specified in the SAD, the obtained packet shall be compared to the selectors identified by the SAD. If they don't match, the packet shall be discarded.

APPENDIX C

QoS preconditions

QoS preconditions have been defined by the IETF in [121]. It defines the conditions to meet before establishing a call. They are included in the SDP for each *m* line and indicate the desired "des" state of a condition (e.g. qos) and its current "curr" state. When the current state is equal to the desired state, the condition is met and the call can be established.

Two examples of SDP are provided for a given *m* line (e.g. voice) with QoS preconditions.

In the first example, the MN indicates that currently (**curr**) there are no resources (**qos**) reserved (**none**) on the MN (**local**) and CN (**remote**) sides and that resources shall (**des**, **mandatory**) be reserved on the MN side. Such SDP can be sent for example during the setep Estb_1 described in chapter 2.

m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local none
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos none remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=rtpmap:96 telephone-event
a=maxptime:20

In the second example, resources are reserved on the MN side (e.g. during the step Estb_6 described in chapter 2). Therefore, the MN sends an SDP where the line " **a=curr:qos local none** " of the previous example changes to "**a=curr:qos local sendreceive**". If resources are not available, the media port is set to 0 meaning that the media is canceled.

m=audio 3456 RTP/AVP 97 96
b=AS:25.4
a=curr:qos local sendreceive
a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos mandatory remote sendrecv
a=rtpmap:97 AMR
a=fmtp:97 mode-set=0,2,5,7; mode-change-period=2
a=rtpmap:96 telephone-event
a=maxptime:20

APPENDIX D

Solutions for handover delay optimization considering MIP-based mobility procedure

This appendix is complementary to section 2.2.2.2.

The patent [78], based on [122, 123], treats the handover delay problem for a MIP-based mobility procedure.

The **MIP-based mobility procedure** involves three phases as shown in figure D.1. Phase 1 and 2 are the same as the ISC mobility procedure 2.2.1). Phase 3 is different and considers MIP instead of SIP to execute mobility and update the new MN address (@IP2). With MIP, when the MN acquires @IP2 (Care of Address) during phase1-ATH_3, it informs the Home Agent[1] (HA). The HA maps the old MN address (@IP1) acquired on IP-AN1 to the new MN address (@IP2). Then, when HA receives data to forward to @IP1 (example from the CN), it tunnels this data to @IP2. Thus, the HA acts as a signalling and data anchor.

When MIP-based procedure is executed, contexts are set in the MN, first IP router2, PCRF2, P-CSCF2, S-CSCF as follows (figure D.1):

- The `SDP`, part of Estb_1 context, in P-CSCF2 is related to @IP2 when considering the MN source address. The aim is to correctly set the `data flow descriptors` in the IP-AN2 PCEF, where the MN is recognized with @IP2..
- The rest of contexts are related to @IP1 when considering the MN source address. Indeed, in [78], the HA hides @IP2 from P-CSCF2, S-CSCF, and CN.

Note the difference between MIP-based procedure and SIP-based procedure (presented in section 2.2.2.2): in the last one, the MN is recognized with @IP2 in all nodes and contexts.

[1] An additional network node

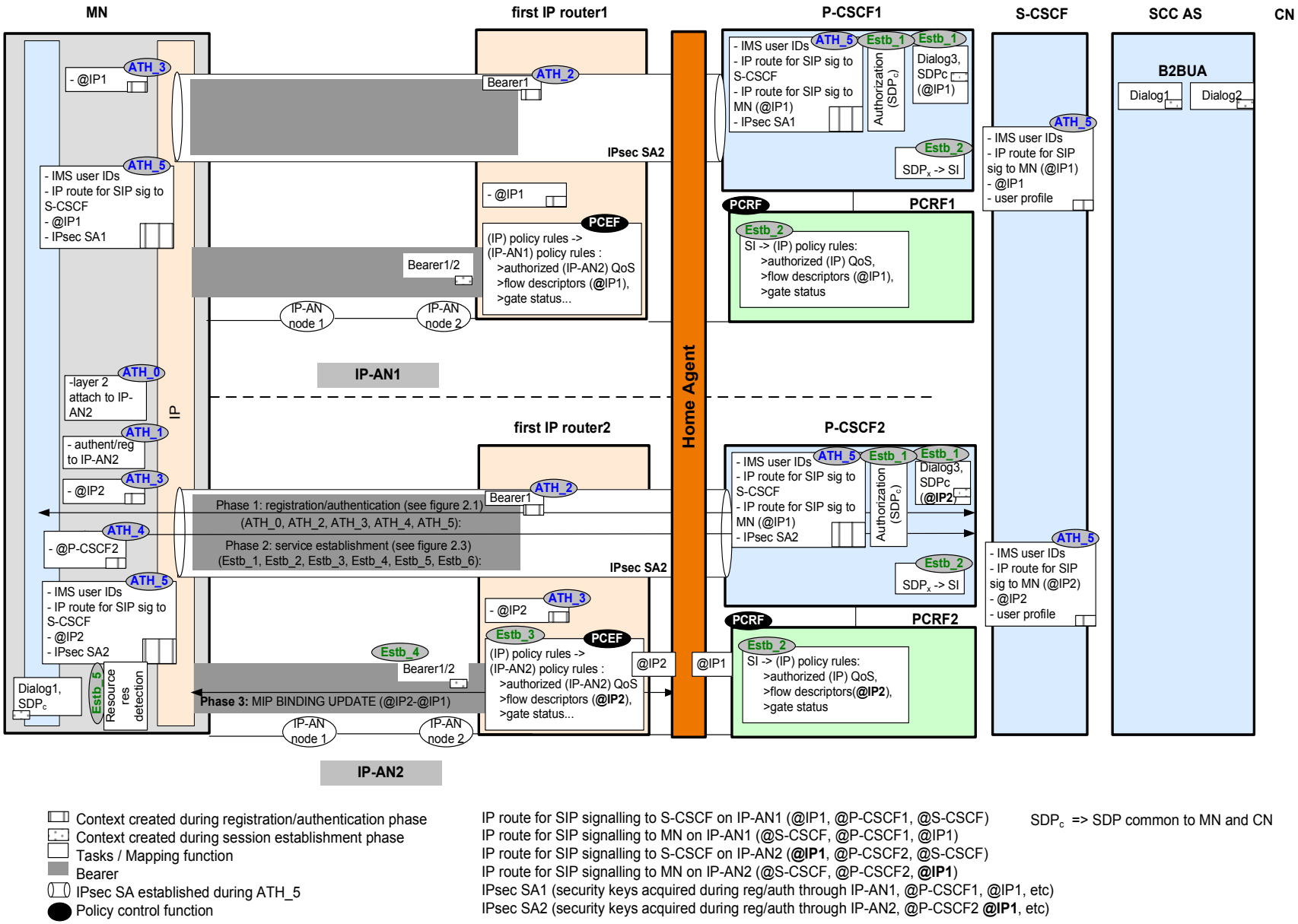


Figure D.1: MIP-based mobility procedure

The patent [78] proposes solutions to optimize the handover delay for the MIP-based procedure described above, and claims that these solutions can be used to optimize handover delay in a **SIP-based procedure**. It provides two types of solutions: **solutions with steps or contexts transfer performed before handover while the MN is on IP-AN1 (proactive)**, and solutions with steps and contexts transfer performed after handover (reactive). Only the first kind of solutions is detailed hereafter (solution 3 and solution 4 just after), as the second kind of solutions is similar to solution 1 described above. I include comments for the anomalies I detected in these proposed solutions.

solution 3: Proactive ATH_4, ATH_5, ATH_3 steps and transfer of partial Estb_1 context before handover to IP-AN2

Before handover, while the MN is attached to IP-AN1 (refer to figure D.1 for the understanding of this procedure):

1. The MN receives an event about imminent subnet change.
2. The MN proactively performs P-CSCF discovery (**ATH_4**).

   Comment: As P-CSCF determination depends on the IP-AN, discovery procedure should pass through IP-AN2. Therefore, in my opinion, the previous step is not enough and the MN should receive explicit information about IP-AN2.
3. The MN proactively performs registration/authentication to the IMS (**ATH_5**), as if it is connected to IP-AN2: this step is performed with the S-CSCF and P-CSCF2. As a result, ATH_5 contexts are built in the MN, P-CSCF2 and S-CSCF (i.e. IP route for SIP signalling, IPsec SA2, binding of IMS identities to @IP1).
4. The MN proactively acquires a new IP address in IP-AN2 (@IP2) (**ATH_3**).
5. After step 3, the S-CSCF orders P-CSCF1 to transfer the Service Information (`SI`) (deduced from the `SDP` part of Estb_1 context) to P-CSCF2.
   Accordingly, P-CSCF2 executes parts of **Estb_2** and **Estb_3** steps by ordering PCRF2 to configure and open the gates in the first IP router2.

   Comment: The other parts of the steps **Estb_2**, **Estb_3**, **Estb_4** with regard to the calculation of `authorized (IP) QoS`, calculation of `authorized (IP-AN2) QoS` and resource reservation in IP-AN2 are not mentioned.

   Comment: As stated above, the `SDP/SI` contexts in P-CSCF2 shall be related to @IP2. However the `SI` transferred from P-CSCF1 to P-CSCF2 is related to @IP1. As P-CSCF2 is not aware of @IP2, it can not update the `SI` with @IP2.
6. The MN proactively performs **phase 3**. It executes mobility to its Home Agent using MIP to bind @IP2 on @IP1.

After attachment to IP-AN2:

7. Traffic goes through IP-AN2.

Comment: solution 3 can not be applied with the same order of steps for SIP-based or ISC procedure optimization, contrary to what is claimed in the patent. In this solution, the ATH_5 context is related to @IP1. However, for SIP-based procedure, all MN contexts are related to @IP2. Therefore, the transferred context shall be updated with @IP2. This require that P-CSCF2 interacts with first IP router2 to get @IP2, causing thus additional delay.

solution 3 has the following **drawback**:

- The execution of the different proactive steps requires time especially as they pass through centralized nodes. Therefore, they should be launched on time before MN attachment to IP-AN2. In case of cells will small overlapping zones, the event triggering these steps shall not be based only on IP-AN1 coverage loss or IP-AN2 coverage detection. Other triggers (e.g. based on the MN movement anticipation) shall be available causing thus more complexity.

Solution 4: Proactive ATH_4 and ATH_3 steps and transfer of partial Estb_1 and partial ATH_5 contexts before handover to IP-AN2

This solution is provided to optimize the MIP-based mobility solution, as solution 3 [78]. While in solution 3, ATH_5 step is executed proactively between the MN and P-CSCF2, in solution 4, a part of ATH_5 context is transferred from P-CSCF1 to P-CSCF2 before MN handover.

Before handover and while the MN is attached to IP-AN1 (refer to figure D.1 for the understanding of this procedure):

1. The MN receives an event about imminent subnet change.
2. The MN proactively performs P-CSCF discovery (**ATH_4**).

   Comment: As P-CSCF determination depends on the IP-AN, the previous step is not enough and the MN should receive explicit information about IP-AN2.
3. The MN notifies S-CSCF about handover as well as about @P-CSCF2.
4. The S-CSCF orders P-CSCF1 to transfer Service Information (`SI`) context (deduced from `SDP`, **Estb_1** context) and IPsec SA context (partial **ATH_5** context) to P-CSCF2.
   Accordingly, P-CSCF2 executes parts of **Estb_2** and **Estb_3** steps by ordering PCRF2 to configure and open the gates in the first IP router2.

   Comment: The other parts of the steps **Estb_2**, **Estb_3**, **Estb_4** with regard to the calculation of `authorized (IP) QoS`, calculation of `authorized (IP-AN2) QoS` and resource reservation in IP-AN2 are not mentioned.

   Comment: As previously stated, the `SDP/SI` contexts in P-CSCF2 shall be related to @IP2. However the `SI` transferred from P-CSCF1 to P-CSCF2 is related to @IP1. As P-CSCF2 is not aware of @IP2, it can not update the `SI` with this address.
5. The MN proactively acquires a new IP address in IP-AN2 (@IP2) (**ATH_3**).

After attachment to IP-AN2:

6. The MN performs informs the home agent about @IP2, using a MIP BINDING UPDATE message.
7. The MN sends a SIP REGISTER to S-CSCF to inform it about @IP2 and update the IP route for SIP signalling. This completes ATH_5 step.
8. Traffic goes through IP-AN2.

Comment: The solution can not be applied as it is for IP-based or ISC procedure optimization for the same reasons as those given in solution 3.

solution 4 has the following **drawback**:

- Compared to solution 3, solution 4 reduces the number of proactive steps, by using context transfer. However, solution 4 remains incomplete and do not cover all of the steps.

APPENDIX E

Establishment and handover message flows based on the testbed traces

In order to show the results of UFA implementation and illustrate some of UFA behaviors e.g. the actions performed by the UFA B2BUA module, this appendix provides traces collected on the testbed during establishment and mobility procedures and comment them.

E.1 Establishment

-Figure E.1:

- MN fills the content of SIP INVITE message by putting:
  - CN SIP URI in the: *Request URI* and *To* header.
  - Its SIP URI in the *From* header.
  - Its IP address in the: *Via* header, *Contact* header, and *c* field of SDP.
- When UFA_GW_S receives SIP INVITE message related to a first dialog (dialog1), it creates a new SIP INVITE related to a second dialog (dialog2) with:
  - *Request URI*, *To* and *From* headers are the same as the ones in the received SIP INVITE message.
  - New *Call-ID* and *From Tag* are used to identify dialog2.
  - New *Via* header to direct CN responses to UFA_GW_S.
  - UFA_GW_S IP address in the *Contact* header.

-Figure E.2:

- CN answers with a SIP SESSION PROGRESS message. It adds its *Tag* to the *To* header and puts its address in the *Contact* header.
- When UFA_GW_S receives the SIP SESSION PROGRESS message, it creates another SIP SESSION PROGRESS message towards the MN as a part of dialog1. It adds its *Tag* to the

To header and puts its IP address in the *Contact* header.
UFA_GW_S registers dialog1 and dialog2 contexts based respectively on the SIP SESSION PROGRESS sent to MN and SIP SESSION PROGRESS received from CN.

E.2 Handover

-Figure E.3:
UFA_GW_S sends to UFA_GW_T TRANSFER CONTEXT (3) message containing: dialog1 context, dialog2 context.

I have chosen SIP to transport this message. Any other protocol could have been chosen, example the context transfer protocol (CXTP) [124].

-Figure E.4:
UFA_GW_T replies to UFA_GW_S with OK message containing IP and layer 2 configuration for MN as defined in table 4.2.

-Figure E.5:

- UFA_GW_S sends a SIP INVITE to MN updating dialog1 and containing UFA_Terminal_Conf and UFA_Appli_Conf_IP headers as defined in tables 4.2 and 4.3.
- UFA_GW_S sends a SIP INVITE to CN updating dialog2 and containing UFA_Appli_Conf_IP header and new MN address in the SDP *c* field. Note that the new MN IP address in the UFA_Appli_Conf_IP header and in the SDP *c* field has the function i.e. updating the data flow destination address in the CN. I preferred to dedicate a specific header for this address to make the solution common to SIP native and non-SIP native services, and also to be able to propose some enhancements through this header like bi-casting (with *c* field, this feature is not possible).

-Figure E.6:
MN sends a SIP INVITE to UFA_GW_T. This message contains the new MN address in the *Via* and *Contact* headers and in the *c* field of SDP.

MN

2001:2000:0:10:1:1:1:2

INVITE

```
INVITE sip:[2001:2000:0:1::4]:5080 SIP/2.0  //Dialog1
Via: SIP/2.0/UDP  [2001:2000:0:10:1:1:1:2]:5070; rport=5070;
branch=z9hG4bKPj-EcrSj1QaYcFZ4bPyASNNtTbu6mqJgrv
Max-Forwards: 70
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUi
To: <sip:CN@[2001:2000:0:1::4]>
Contact: <sip:MN@[2001:2000:0:10:1:1:1:2]:5070>
Call-ID: vHebJwJd0a3hYCKXYH1sQwulH6W12LZy-755308162
CSeq: 44753 INVITE
Supported: 100rel
Require: 100rel
Allow: INVITE, ACK, BYE, CANCEL, UPDATE, PRACK
Content-Type: Application/SDP
Content-Length:   300

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:10:1:1:1:2]
s=pjmedia
c=IN IP6 [2001:2000:0:10:1:1:1:2]
t=0 0
m=audio 5120 RTP/AVP 0 8 101
a=rtcp:5121 IN IP6 [2001:2000:0:10:1:1:1:2]
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

2001:2000:0:10::1

UFA_GW_S

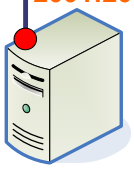
2001:2000:0:1::1

INVITE

Ethernet

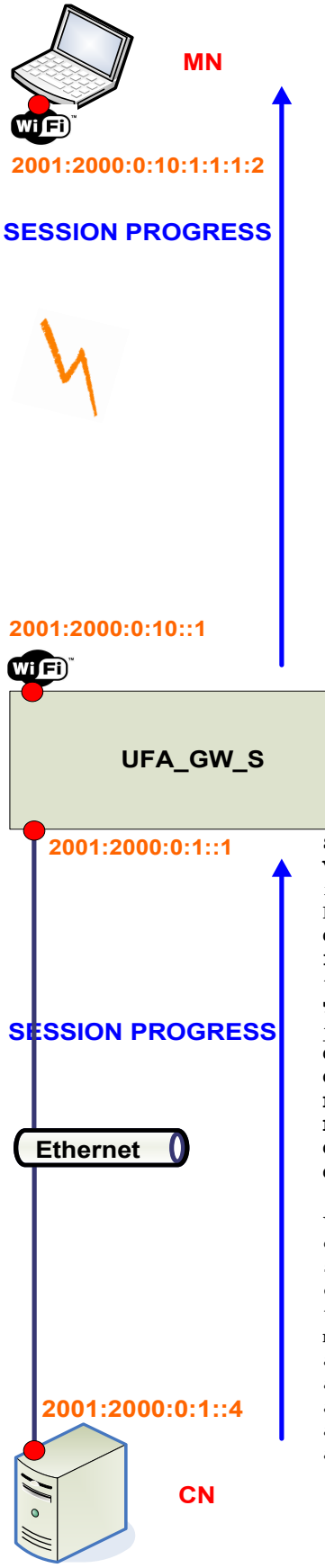
```
INVITE sip:[2001:2000:0:1::4]:5080 SIP/2.0  //Dialog2
Via: SIP/2.0/UDP [2001:2000:0:1::1]:5065;rport=5065;
Branch: z9hG4bKPjBntFKHEBPE2QL14ZptYmJBXqyA9r2XQv
Max-Forwards: 70
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUiJAu
To: <sip:CN@[2001:2000:0:1::4]>
Contact: <sip:B2BUA@[2001:2000:0:1::1]:5065>
Call-ID: 8CtP9egisP4zFKjJeZFXB-pbrm.PncaW-1633135711
CSeq: 29588 INVITE
Supported: 100rel
Require: 100rel
Allow: INVITE, ACK, BYE, CANCEL, UPDATE, PRACK
Content-Type: Application/SDP
Content-Length:   300

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:10:1:1:1:2]
s=pjmedia
c=IN IP6 [2001:2000:0:10:1:1:1:2]
t=0 0
m=audio 5120 RTP/AVP 0 8 101
a=rtcp:5121 IN IP6 [2001:2000:0:10:1:1:1:2]
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

2001:2000:0:1::4



CN

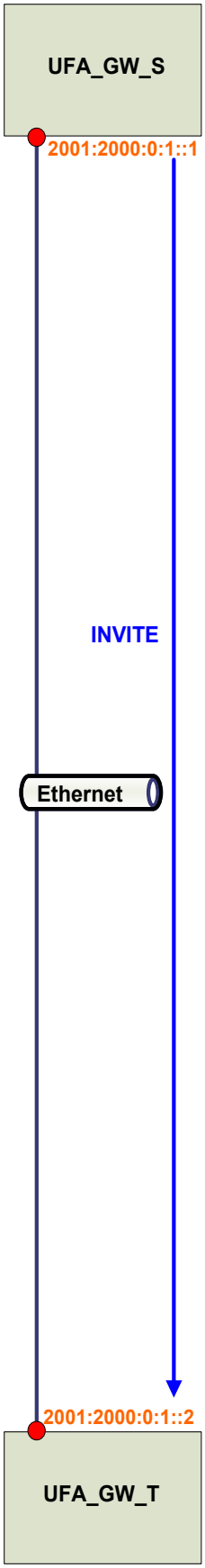
Figure E.1: SIP INVITE message during service establishment in UFA




```
SIP/2.0 183 Session Progress  //Dialog1
Via: SIP/2.0/UDP [2001:2000:0:10::1]:5060; rport=5060;
received=2001:2000:0:10:1:1:1:2;
branch=z9hG4bKPj-EcrSj1QaYcFZ4bPyASNNtTbu6mqJgrv
Call-ID: vHebJwJd0a3hYCKXYH1sQwulH6W12LZy-755308162
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUi
To: <sip:CN@[2001:2000:0:1::4]>;
tag=CnToTag-44753-22377
CSeq: 44753 INVITE
Contact: <sip:B2BUA@[2001:2000:0:10::1]:5060>
Require: 100rel
RSeq: 22377 INVITE
Content-Type: Application/SDP
Content-Length:   258

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:1::4]
s=pjmedia
c=IN IP6 [2001:2000:0:1::4]
t=0 0
m=audio 5130 RTP/AVP 0 101
a=rtcp:5131 IN IP6 [2001:2000:0:1::4]
a=rtpmap:0 PCMU/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

```
SIP/2.0 183 Session Progress  //Dialog2
Via: SIP/2.0/UDP [2001:2000:0:1::1]:5065;rport=5065;
received=2001:2000:0:1::1;
branch=z9hG4bKPjBntFKHEBPE2QL14ZptYmJBXqyA9r2XQv
Call-ID: 8CtP9egisP4zFKjJeZFXB-pbrm.PncaW-1633135711
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUiJAu
To: <sip:CN@[2001:2000:0:1::4]>;
tag=CnToTag-29588-14794
CSeq: 29588 INVITE
Contact: <sip:CN@[2001:2000:0:1::4]:5080>
Require: 100rel
RSeq: 14794 INVITE
Content-Type: Application/SDP
Content-Length:   258

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:1::4]
s=pjmedia
c=IN IP6 [2001:2000:0:1::4]
t=0 0
m=audio 5130 RTP/AVP 0 101
a=rtcp:5131 IN IP6 [2001:2000:0:1::4]
a=rtpmap:0 PCMU/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

Figure E.2: SIP SESSION PROGRESS during service establishment in UFA




```
INVITE sip:[2001:2000:0:1::2]:6000 SIP/2.0
Via: SIP/2.0/UDP [2001:2000:0:1::1]:6000; rport=6000;
branch=z9hG4bKPjbudBl6wIkvnf6D4cJ2xv6lVLZZBjt7it
Max-Forwards: 70
From: <sip:UFA_GW_S@[2001:2000:0:1::1]>;tag=0zm28fOxMIPpBO3BCwNiXsuM2UGK497i
To: <sip:UFA_GW_T@[2001:2000:0:1::2]>
Contact: <sip:UFA_GW_S@[2001:2000:0:1::1]:6000>
Call-ID: YoJudBGWyTnhtMHiLN9JT5MGphiP4kpf
CSeq: 48555 INVITE
Content-Type: Text/Plain
Content-Length:  1404

MN_Header  //Dialog1 context
INVITE sip:[2001:2000:0:1::4]:5080 SIP/2.0
Via: SIP/2.0/UDP [2001:2000:0:10:1:1:1:2]:5070;rport=5070;
branch=z9hG4bKPj-EcrSj1QaYcFZ4bPyASNNtTbu6mqJgrv
Max-Forwards: 70
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUiJAuXYOwL1e4gaiz2j5lJtI
To: <sip:CN@[2001:2000:0:1::4]>;
tag=CnToTag-44753-22377
Contact: <sip:MN@[2001:2000:0:10:1:1:1:2]:5070>
Call-ID: vHebJwJd0a3hYCKXYH1sQwulH6W12LZy-755308162
CSeq: 44753 INVITE
Supported: 100rel
Require: 100rel
Allow: INVITE, ACK, BYE, CANCEL, UPDATE, PRACK
Content-Type: Application/SDP
Content-Length:   300
MN_Header_End

CN_Header   //Dialog2 context
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 2001:2000:0:1::1]:5065;rport=5065;received=2001:2000:0:1::1;
branch=z9hG4bKPjBntFKHEBPE2QL14ZptYmJBXqyA9r2XQv
Call-ID: 8CtP9egisP4zFKjJeZFXB-pbrm.PncaW-1633135711
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUiJAuXYOwL1e4gaiz2j5lJtI
To: <sip:CN@[2001:2000:0:1::4]>;
tag=CnToTag-29588-14794
CSeq: 29588 INVITE
Contact: <sip:CN@[2001:2000:0:1::4]:5080>
Require: 100rel
RSeq: 14794 INVITE
Content-Type: Application/SDP
Content-Length:   258
CN_Header_End

ORI_SDP //SDPc
v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:1::4]
s=pjmedia
c=IN IP6 [2001:2000:0:1::4]
t=0 0
m=audio 5130 RTP/AVP 0 101
a=rtcp:5131 IN IP6 [2001:2000:0:1::4]
a=rtpmap:0 PCMU/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
ORI_SDP_End

SID=1
```

Figure E.3: CONTEXT TRANSFER message (3) during handover in UFA

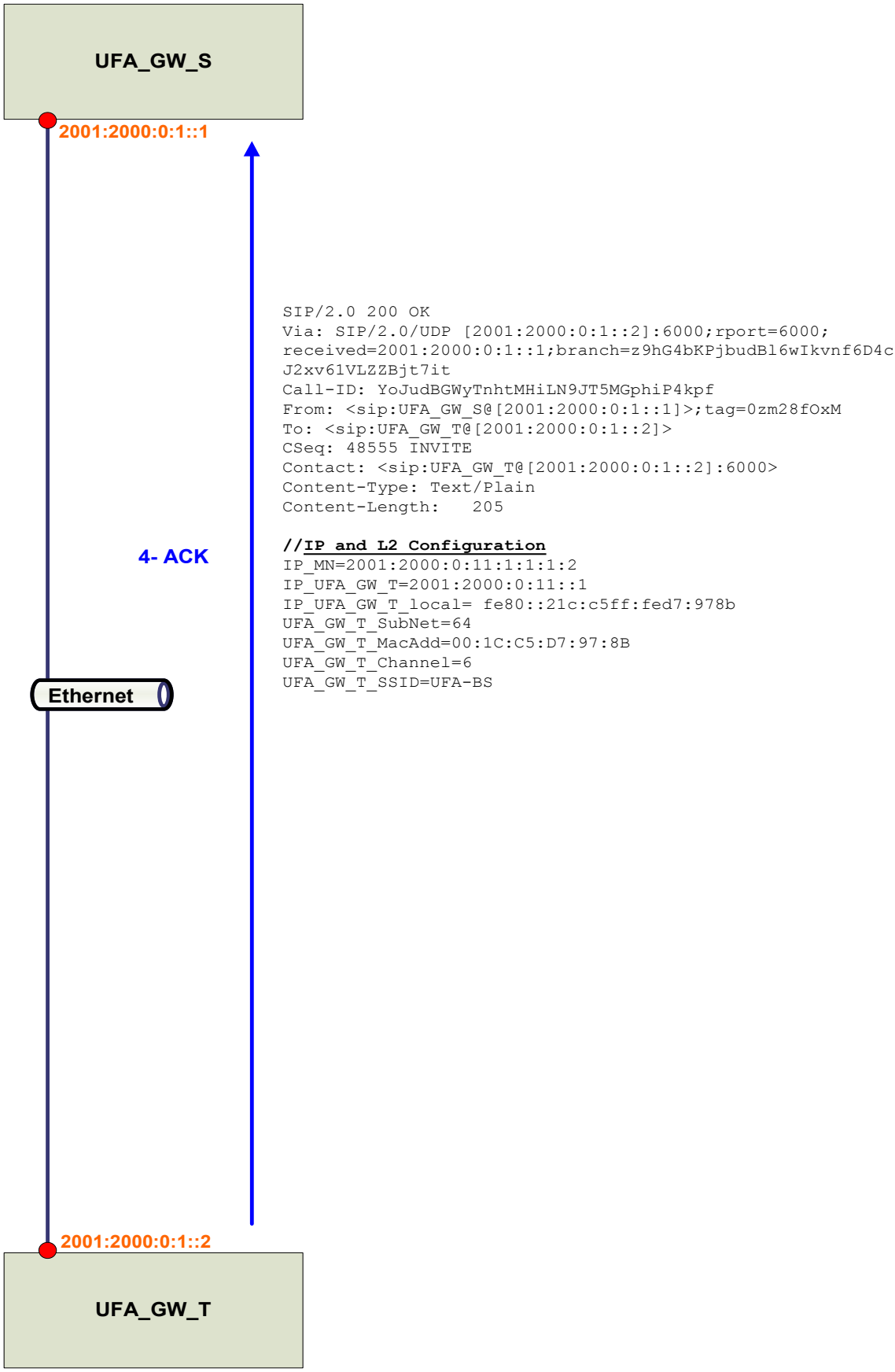
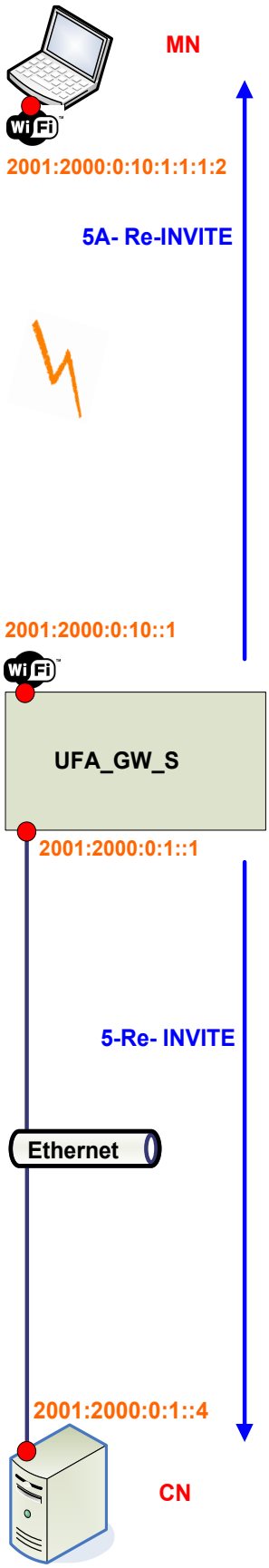


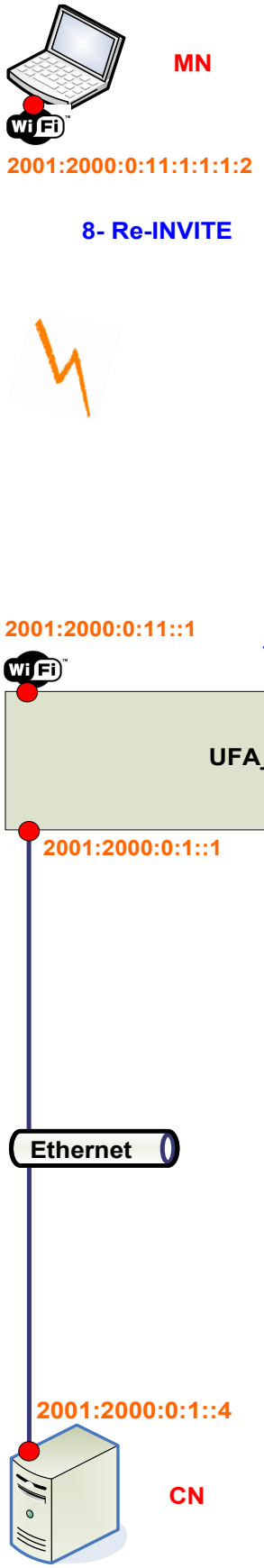
Figure E.4: ACK message (4) during handover in UFA




```
INVITE sip:[2001:2000:0:10:1:1:1:2]:5070 SIP/2.0  //Dialog1
Via: SIP/2.0/UDP [2001:2000:0:10::1]:5060;rport=5060;
branch=z9hG4bKPjJbV4qKA.r.FhdQtxPJ0XUiltz.TyNOOi
Max-Forwards: 70
From: sip:MN@[2001:2000:0:10:1:1:1:2]>;
tag=Q9ysDSoCUi
To: <sip:CN@[2001:2000:0:1::4]>;
tag=CnToTag-44753-22377
Contact: <sip:B2BUA@[2001:2000:0:10::1]:5060>
Call-ID: vHebJwJd0a3hYCKXYH1sQwulH6W12LZy-755308162
CSeq: 44754 INVITE
Allow: INVITE, ACK, BYE, CANCEL, UPDATE, PRACK
UFA_Terminal_Conf: <Interface_NameTarget=wifi;
UFA_GW_T_MAC_Address=00:1C:C5:D7:97:8B; UFA_GW_T_ESSID=UFA-BS;
UFA_GW_T_Channel=6; Add_IP_Address=2001:2000:0:11:1:1:1:2;
UFA_GW_T_IP_Address=2001:2000:0:11::1; IP_UFA_GW_T_local=
fe80::21c:c5ff:fed7:978b; UFA_GW_T_Netmask=64>
<Interface_Name_Source=wifi; Del_IP_Address=2001:2000:0:10:1:1:1:2>
UFA_Appli_Conf_IP: Add_IP_Address=2001:2000:0:11:1:1:1:2;
Del_IP_Address=2001:2000:0:10:1:1:1:2
Content-Type: Application/SDP
Content-Length :   258

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:1::4]
s=pjmedia
c=IN IP6 [2001:2000:0:1::4]
t=0 0
m=audio 5130 RTP/AVP 0 101
a=rtcp:5131 IN IP6 [2001:2000:0:1::4]
a=rtpmap:0 PCMU/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

```
INVITE sip:[2001:2000:0:1::4]:5080 SIP/2.0   //Dialog1
Via: SIP/2.0/UDP [2001:2000:0:1::1]:5065; rport=5065;
branch=z9hG4bKPjcU-Qz8shxTfUwrRhaQxQJAaCznxujUit
Max-Forwards: 70
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>; tag=Q9ysDSoCUiJAu
To: <sip:CN@[2001:2000:0:1::4]>;
tag=CnToTag-29588-14794
Contact: <sip:B2BUA@[2001:2000:0:1::1]:5065>
Call-ID: 8CtP9egisP4zFKjJeZFXB-pbrm.PncaW-1633135711
CSeq: 29589 INVITE
Allow: INVITE, ACK, BYE, CANCEL, UPDATE, PRACK
UFA_Appli_Conf_IP: Add_IP_Address=2001:2000:0:11:1:1:1:2;
Del_IP_Address=2001:2000:0:10:1:1:1:2;
Content-Type: Application/SDP
Content-Length:   258

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:11:1:1:1:2]
s=pjmedia
c=IN IP6 [2001:2000:0:11:1:1:1:2]
t=0 0
m=audio 5130 RTP/AVP 0 101
a=rtcp::5131 IN IP6 [2001:2000:0:11:1:1:1:2]
a=rtpmap:0 PCMU/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a
```

Figure E.5: Re-INVITE messages (5 and 5A) during handover in UFA




```
INVITE sip:[2001:2000:0:1::4]:5080 SIP/2.0  // Dialog1
Via: SIP/2.0/UDP [2001:2000:0:11:1:1:1:2]:5070;rport=5070;
branch=z9hG4bKPjis5BjG6UzuZfqPEntu2eNpgc08LcRyTX
Max-Forwards: 70
From: <sip:MN@[2001:2000:0:10:1:1:1:2]>; tag=Q9ysDSoCUi
To: <sip:CN@[2001:2000:0:1::4]>; tag=CnToTag-44753-22377
Contact: <sip:MN@[2001:2000:0:11:1:1:1:2]:5070>
Call-ID: vHebJwJd0a3hYCKXYH1sQwulH6W12LZy-755308162
CSeq: 44755 INVITE
Supported: 100rel
Require: 100rel
Allow: INVITE, ACK, BYE, CANCEL, UPDATE, PRACK
Content-Type: Application/SDP
Content-Length:   258

v=0
o=- 3360842071 3360842071 IN IP6 [2001:2000:0:11:1:1:1:2]
s=pjmedia
c=IN IP6 [2001:2000:0:11:1:1:1:2]
t=0 0
m=audio 5130 RTP/AVP 0 101
a=rtcp::5131 IN IP6 [2001:2000:0:11:1:1:1:2]
a=rtpmap:0 PCMU/8000
a=sendrecv
a=rtpmap:101 telephone-event/8000
a
```

Figure E.6: Re-INVITE message (8) during handover in UFA

APPENDIX F PJSIP

F.1 Architecture of SIP programs

As said in chapter 6, most of the required UFA and ISC functions are within SIP layer. PJSIP library [97] is used to develop these functions in MN, CN and UFA_GW (for UFA). It enables to realize different SIP-based applications thanks to its core programs or APIs. For UFA, implementation is performed in the PJSIP core programs as the available APIs do not provide enough flexibility to develop the UFA_GW B2BUA module.

In MN/CN, a Media Controller program based on the PJMEDIA PJSIP sub-library is used. It is inspired from the PJMEDIA application example named "Remote Streaming" [98]. It receives, reads or generates application packets. In UFA and Implemented ISC, an RTP voice streaming application is used. The CN is the server and the MN is the client. When CN receives information about new MN IP address, the Media Controller updates the MN IP destination address.

The architecture of SIP programs based on PJSIP library for UFA and Implemented ISC is divided into many parts (figure F.1).

- A memory zone composed of:
  - Two structures pjsip_rx_data (rdata) and pjsip_tx_data (tdata) used by PJSIP library to treat the rdata information related to a received SIP message, or to create tdata information related to a SIP message to transmit.
  - One "dialog" structure to keep data about the SIP session(s) managed by the program.
- "PJLIB" offers an abstraction of the operation system.
- "Transport" receives incoming messages and transmits them to the parser. It also receives messages from the endpoint and transmits them to an external destination.
- "Parser" reads and decomposes an incoming SIP message and stores its elements in the pjsip_rx_data (rdata). It also retrieves data from from pjsip_tx_data (tdata) and creates accordingly a SIP message. It is called by the "transport" element for any incoming or outcoming SIP message.
- "Endpoint" acts as a dispatcher between the "transport" and the registered "modules".
- "Module" is a structure stored in the endpoint, that provides links between the endpoint and the application thanks to callback functions.
- "Application" is the applicative part of the program. It treats incoming and outcoming SIP messages and non SIP actions. It contains:

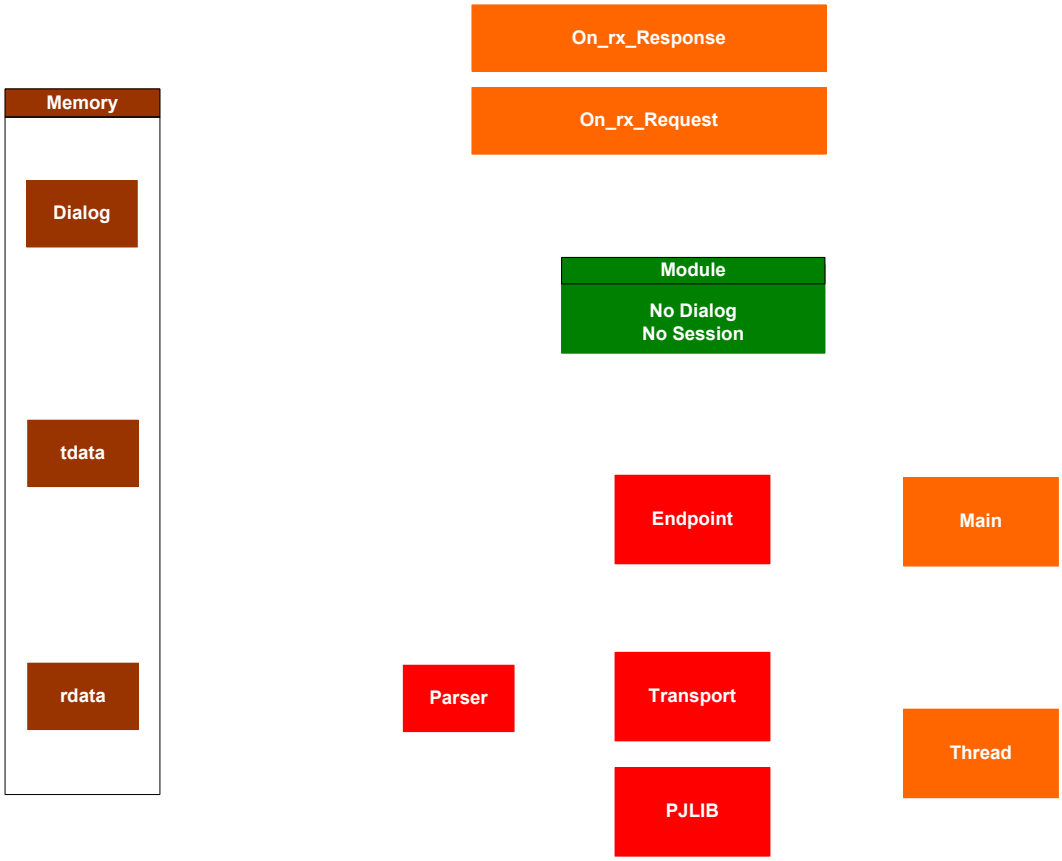


Figure F.1: Architecture of SIP programs based on PJSIP library

- Two callbacks "On_rx_request" and "On_rx_response" treating incoming and outcoming SIP messages.
- A "main" function to initiate PJSIP library, the "module" and "dialog" structure.
- "Threads" that enable to realize different actions in parallel to the main program.

F.2 Examples of UFA SIP messages handling with SIP programs

The following figures provide how SIP INVITE for service establishment is handled by MN, UFA_GW and CN.

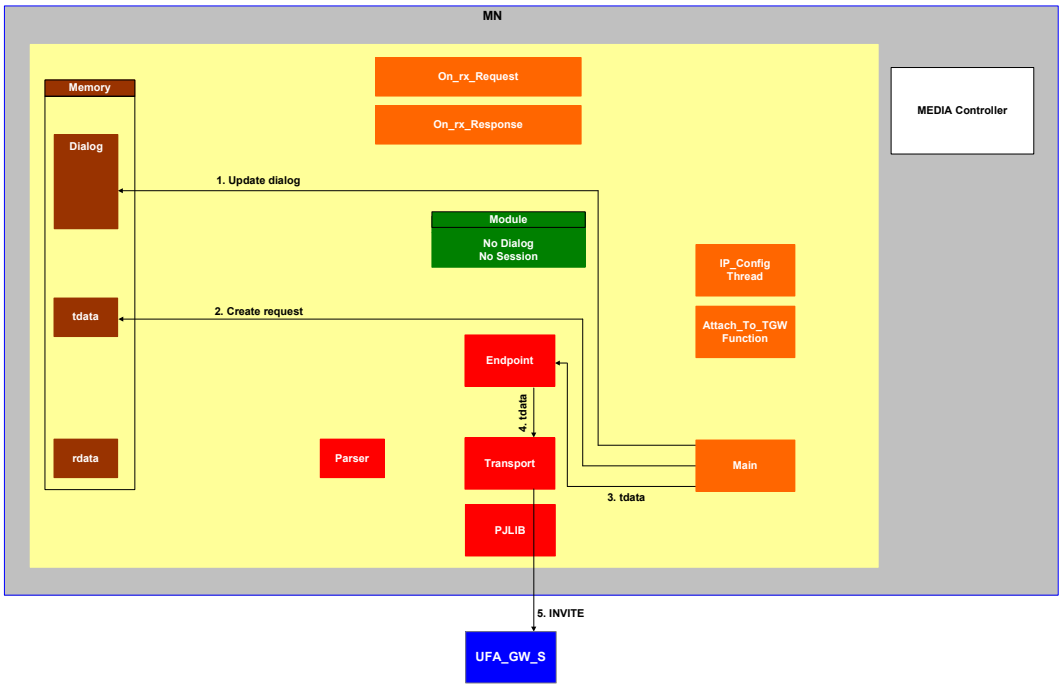


Figure F.2: Handling of SIP INVITE message by MN

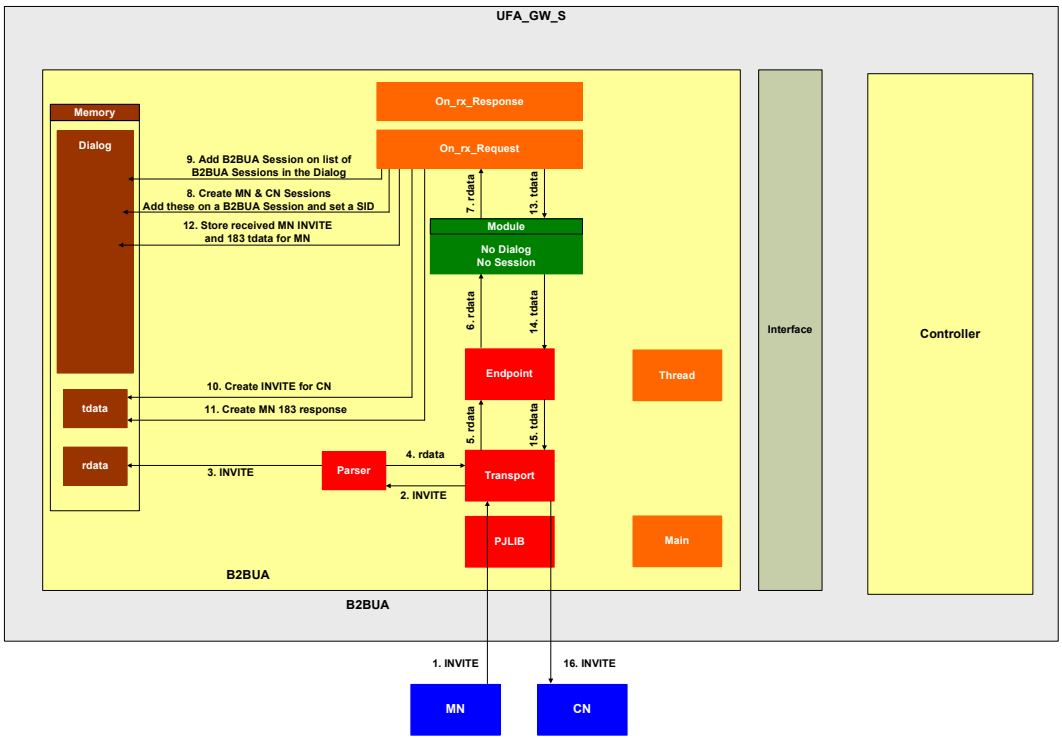


Figure F.3: Handling of SIP INVITE message by UFA_GW

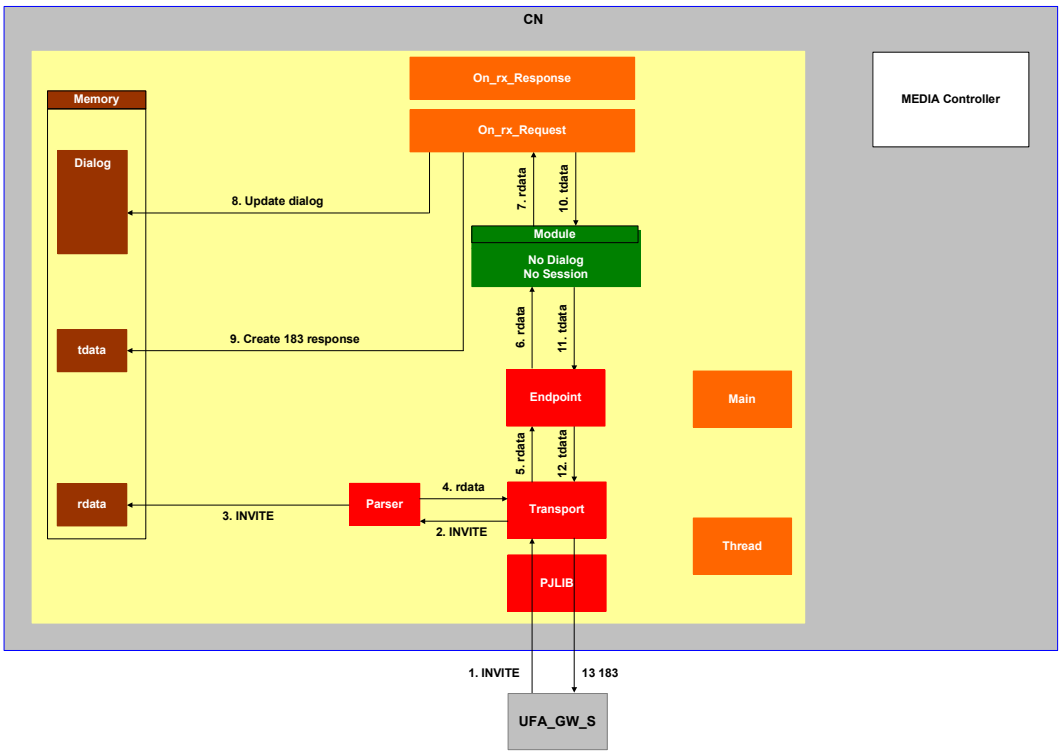


Figure F.4: Handling of SIP INVITE message by CN

Part VI

Résumé étendu en français

APPENDIX G

Résumé étendu en français

Introduction

Un nouvel écosystème pour les opérateurs de réseaux mobiles

Au cours des dernières années, les opérateurs de réseaux mobiles (MNO) ont été en mesure de contrôler le volume de données sur leurs réseaux respectifs. La situation est en train de changer et l'écosystème des télécommunications connaît une transformation profonde avec un pléthorat d'acteurs différents essayant de fournir les meilleurs services aux clients au meilleur prix.

Premièrement, les MNOs offrent des débits plus importants sur leurs interfaces radio grâce aux technologies radio HSPA, LTE et WiMAX. Deuxièmement, les fabricants conçoivent des terminaux très attrayants et ergonomiques comme l'iPhone, BlackBerry, et les tablets Internet. Ces dispositifs, bénéficiant d'une interface radio haut débit, génèrent une quantité importante de trafic et nécessitent une bande passante de plus en plus dans les réseaux mobiles. Troisièmement, les efforts des fournisseurs de service dans l'amélioration de l'ergonomie des applications, et la popularité croissante des appareils avec des écrans de haute qualité, accroît l'intérêt des gens pour les services en ligne sur Internet.

Les éléments ci-dessus montrent qu'une augmentation exponentielle du trafic est attendue dans les réseaux mobiles dans les prochaines années. Cisco [4] estime que le trafic de données mobile va doubler tous les année jusqu'en 2014.

Problèmes

Sur la base de la section précédente, il apparaît que les MNOs seront confrontés à un énorme défi: gérer l'augmentation du volume de trafic sur leur réseau tout en offrant une QoS à leurs abonnés au plus bas coût.

Ce travail de recherche vise à la définition des exigences à remplir par un réseau mobile pour affronter ce défi, et à la proposition de solutions à court et long terme permettant aux MNOs de retrouver une bonne situation dans l'écosystème des télécommunications. Trois critères sont pris en compte pour mesurer la capacité des réseaux mobiles à affronter les défis de l'écosystème. Ils sont:

- La mise à l'échelle: Ce critère signifie qu'en cas de croissance du volume de données, les investissements réseau doivent rester profitables.

- Le contrôle de service: les réseaux mobiles ne doivent pas être de simples tuyaux. Ils permettre aux MNOs des bénéfices autres que ceux basés sur le volume de données consommé. Le contrôle de service est une boîte à outils importante permettant aux opérateurs de construire des modèles de facturation intelligents. Il fournit au réseau des informations sur l'abonné, le service demandé et les informations contextuelles (localisation, par exemple). Cette information pourrait être utile pour effectuer des fonctions de contrôle, offrir des services à valeur ajoutée, et monétiser le réseau.
- La qualité de service (QoS): la QoS est un élément important sur lequel les MNOs doivent miser pour attirer les utilisateurs et distinguer les réseaux des autres. Dans ce rapport, deux indicateurs de la QoS sont considérés: la performance d'accès au service et la performance de ce service dès qu'il est établi.

Organization de la thèse

La partie I de la présente thèse (chapitres 1 et 2) analyse la capacité des réseaux mobiles actuels à affronter les défis de l'écosystème, avec le chapitre 1 portant sur les critères de mise à l'échelle et de contrôle de service et le chapitre 2 se concentrant sur le critère de qualité de service. Cette partie formule également une série d'exigences à remplir par un modèle de réseau mobile.

La Partie II propose un nouveau modèle (UFA) pour les réseaux mobiles, basé sur l'ensemble des exigences définies dans la partie I. Le chapitre 3 décrit UFA, et le chapitre 4 précise ses procédures.

La Partie III, incluant les chapitres 5, 6 et 7, valide le modèle UFA et mesure ses performances.

Chapitre 1: La capacité des réseaux mobiles courants à affronter les défis de l'écosystème

Les réseaux mobiles courants représentent des investissements importants pour les opérateurs. Avec le nouvel écosystème et la croissance exponentielle des données, la première question qui vient à l'esprit, est relative à la capacité de ces réseaux à faire face à l'augmentation des investissements, tout en garantissant des bénéfices pour les opérateurs et assurant la qualité de service aux utilisateurs.

L'introduction de ce rapport a défini trois critères, afin de répondre à la question précédente. Ces critères sont: la mise à l'échelle, le contrôle de service et la qualité de service. Ce chapitre se concentre sur les deux premiers critères. Parmi d'autres facteurs, la mise à l'échelle d'un réseau est lié à son architecture organique. En effet, selon le nombre de types de nœds dans le réseau, les fonctions qu'ils mettent en œuvre, et le façon dont ils interagissent, le réseau peut être plus ou moins passer à l'échelle. Par conséquent, dans ce chapitre, nous nous concentrons sur l'architecture organique de ces réseaux.

Dans la section 1.1 de ce rapport, un modèle générique pour les architectures organiques de réseaux mobiles a été établi, sur la base de différentes références dans la littérature. Ce modèle a une structure en couches, et est constitué d'un réseau d'accès IP (IP-AN) fournissant une connectivité IP aux utilisateurs, un ou plusieurs des réseaux en "overlay" apportant des fonctions supplémentaires à la couche IP-AN, et des couches d'interaction entre l'IP-AN et les réseaux overlay.

Dans la section 1.2, un modèle spécifique pour les architectures organiques de réseaux mobiles, ayant un modèle en couches, est détaillé. Dans ce modèle (figure G.1, noté IP-AN//PCC//IMS, l'IMS est une couche de contrôle de service et le PCC est une couche d'interaction entre l'IMS et l'IP-AN assurant le contrôle des politiques réseau.

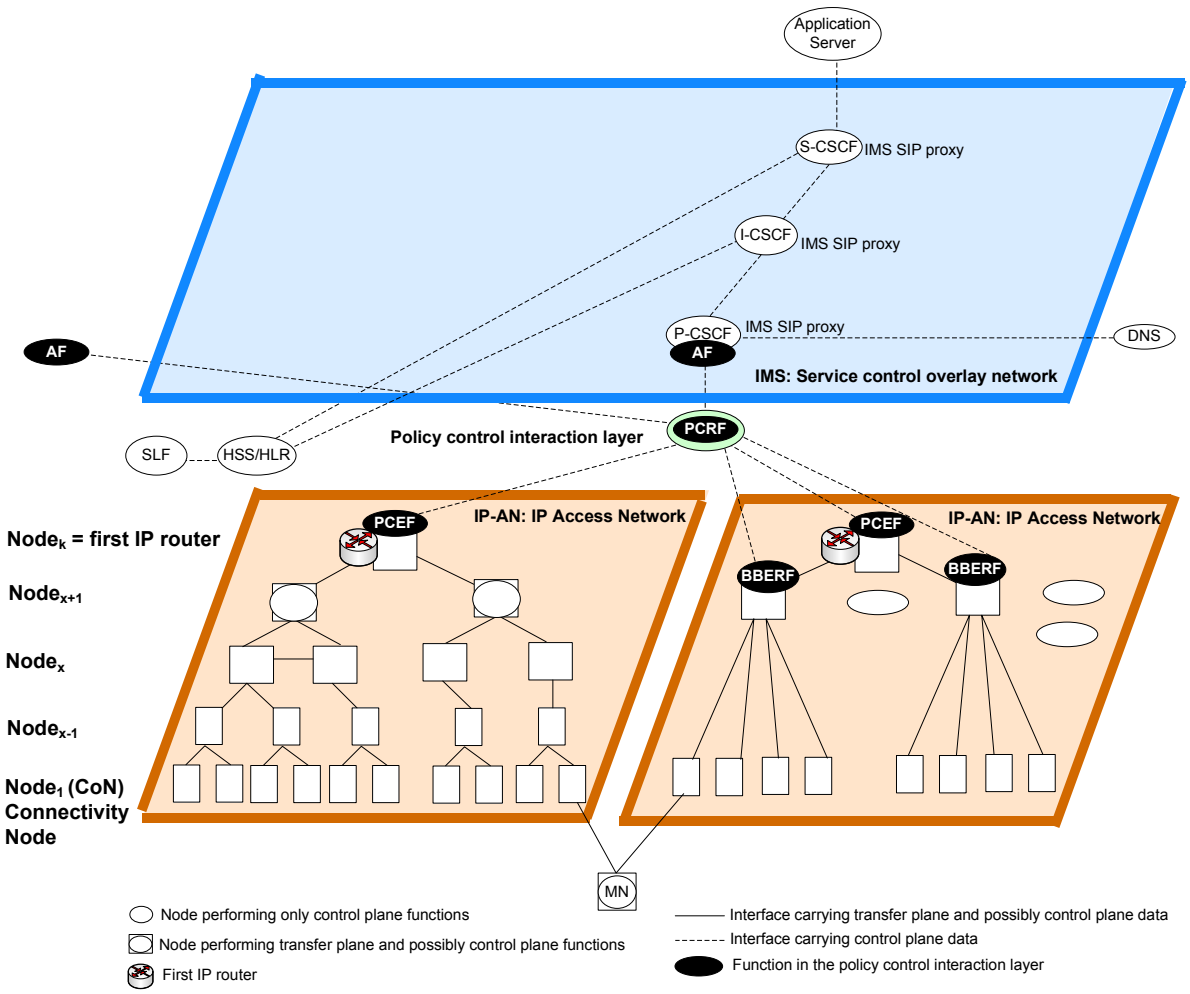


Figure G.1: IP-AN//PCC//IMS

Dans la section 1.3, le modèle IP-AN//PCC//IMS présenté dans la section 1.2 est confirmée par différents exemples normalisés au sein des organismes 3GPP et WiMAX.

Dans la section 1.4, les critères de mise à l'échelle et de contrôle de contrôle de service sont étudiés pour le modèle IP-AN //PCC//IMS. L'IMS offre un contrôle de service. Toutefois, il s'applique uniquement aux applications contrôlées par SIP. Pour les autres applications, le contrôle de service peut être fourni en utilisant d'autres moyens. Néanmoins, ces deux dernières solutions sont chères car elles sont spécifiques à chaque type d'application. D'autre part, étant donné les efforts consacrés pour la spécification de l'IMS, il est intéressant de l'étendre à toutes les applications IMS, et de les contrôler par SIP.

La mise à l'échelle d'un réseau est liée aux aspects économiques. Cela signifie que, en cas de croissance du volume de données, les investissements dans le réseau doivent rester profitable pour l'opérateur.

Exigence: le réseau mobile doit pouvoir passer à l'échelle facilement.

Les réseaux d'accès actuels sont caractérisés par un nœud d'ancrage centralisé gérant la signalisation et les données (premier routeur IP), et de différents nœuds intermédiaires d'ancrage grénat aussi la signalisation les données. Ces ancres sont sollicités, même si l'utilisateur ne se déplace pas. En outre, ils maintiennent un ensemble de contextes par utilisateur, utile pour le traitement du trafic.

Ces contextes sont pour la plupart redondants. Dans chaque nœud d'ancrage, les paquets sont décapsulés/encapsulés et traités conformément aux contextes stockés. Ainsi, plus le nombre de nœuds est élevé, plus le délai de traitement est élevé. En outre, comme les premiers routeurs IP sont centralisés, ils sont responsables d'un nombre élevé d'utilisateurs et représentent des points sensibles du réseau pouvant provoquer des perturbations dans une grande surface.

Pour anticiper l'explosion de trafic dans l'avenir, la duplication des premiers routeurs IP ne suffit pas. Pour combler ces lacunes, une solution à court terme est d'assurer un partage de charge entre ces routeurs. Cela nécessite des fonctionnalités supplémentaires dans le réseau telle qu'une procédure de mobilité optimale entre les premiers routeurs IP (par exemple entre les GGSNs en UMTS). Cette procédure n'est pas définie aujourd'hui par le 3GPP.

> *Exigence : une procédure de mobilité simple et optimale entre les routeurs IP appartenant au même type d'IP-AN (par exemple entre GGSN dans l'UMTS) ou différents IP-AN doit être assuré.*

Pour la mobilité entre les premiers routeurs IP, l'utilisation des protocoles de mobilité de la famille Mobile IP, nous ramène au modèle initial hiérarchique et centralisée et à une augmentation des problèmes de mise à l'échelle. J'ai identifié ISC (IMS continuité des services) [39] comme solution intéressante pour gérer la mobilité. En effet, ISC ne nécessite qu'une ancre de signalisation et non une ancre de signalisation et de données.

ISC repose sur SIP pour gérer la mobilité et en plus permet aux opérateurs de contrôler et de personnaliser service de mobilité.

Dans la section 1.5, deux types de services sont définis. Ces deux types sont:

- Les services dont les application(s) sont transportéss sur RTP/UDP et contrôlées par SIP. Ces services sont appelés les services natifs SIP.
- Les services dont les application(s) sont transportés sur le protocole SCTP et qui sont nativement contrôlés par un protocole différent de SIP (HTTP, RTSP, ...). Ces services sont appelés services non natifs SIP.

Chapitre 2: Les principales procédures dans le modèle IP-AN//PCC//IMS

Ce chapitre met l'accent sur la qualité de service. Les indicateurs de qualité de service peuvent être la performance d'accès au service et la performance du service une fois qu'il est établi. Pour ces raisons, les procédures d'accès aux services et de mobilité sont analysées dans ce chapitre.

Dans la suite nous résumons l'ensemble des problèmes et solutions pour les deux procédures et formulons les exigences à remplir par un modèle de réseau, afin de mieux affronter le nouvel écosystème.

Procédure d'accès au service (authentification/enregistrement + établissement de service)	
Un long délai d'accès au service	Solution: Mapping entre les identifiants IP-AN et IMS de l'utilsateur [70, 63] (-) Ne permet pas d'établir le tunnel IPsec entre le MN and le P-CSCF pour sécuriser la signalisation SIP.
	Solution: Exécution parallèle des étapes: e.g. commencer l'étape réseravation de ressource au même moment que l'étape d'initiation/négotiation du service (-) La QoS est impactée e.g sur-réservation de ressources.

	Solution: moins de temps pour l'étape réservation de ressources: e.g. en impliquant moins de types de nœuds dans cette étape [72]. (-) La solution n'est pas concrètement réalisable.
Non-adaptation de service aux ressources disponibles dans l'IP-AN	**Case 1: le réseau supporte la renégotiation de ressources + solution 1 ou solution 2** (-) un long délai à cause de la renégotiation de ressources Solution 1: l'adaptation de service est initié par le réseau (-) besoin de functions PCC "inverses" et de nouveaux messages. Solution 2: l'adaptation de service est initié par le MN (-) besoin dans le MN de fonctions PCC avancées et "inverses" => duplication de fonctions, n'est pas en ligne avec un PCC orienté réseau.
	Case 2: le réseau ne supporte pas la renégotiation de ressources mais un nouveau nœud (RM) qui collecte les informations de disponibilité des ressources des nœuds IP-AN + solution 1 or solution 2 (-) un nouveau nœud (RM) et interfaces => augmentation des problèmes de mise à l'échelle Solution 1: l'adaptation du service est effectuée implicitement en se basant sur les politiques reçues du réseau avant la phase d'établissement de service [75] (-) difficulté d'appliquer cette solution si on a besoin d'effectuer une adapatation de service précise et personnalisé par MN. Solution 2: l'adaptation du service est effectuée durant la phase d' éstablishment de service [76].
Procédure de mobilité ISC	
Incompatibilité avec les handovers basés sur la charge	Solution: les décisions de handover sont pris par le MN, basées sur l'information de charge reçue du réseau=> besoin d'un nœud (RM) dans le réseau pour extraire cette information et l'envoyer au MN (-) une grande charge de signalisation sur l'interface radio
	Solution: les décisions de handover sont prises par le réseau et envoyées au MN [74] => besoin d'un nœud (RM) dans le réseau pour extraire cette information et d'un autre nœud pour prendre la décision (-) nœuds réseau et interfaces additionnelles => augmentation des problèmes de mise à l'échelle (-) ne résout pas le problème de long délai de handover
Non-adaptation de service aux resources disponibles dans l'IP-AN	voir procédure d'accès au service
Un long délai de handover	Solution: exécution proactive des étapes et transfer des contextes avant handover (-) le problème de délai de handover n'est pas résolu vu le nombre d'étapes

Table G.1: Résumé des solutions proposées pour résoudre les prblèmes des procédures d'accès au service et de mobilité

Comme on peut le déduire du tableau précédent, les solutions proposées introduisent de la complexité dans le MN ou dans le réseau. De plus, ils ne résolvent pas simultanément tous les problèmes. Au contraire, une solution pour un problème donné amplifie les autres problèmes.

Une solution globale doit être définie. Pour progresser dans la définition de cette solution, la meilleure façon de s'y prendre, est d'analyser les causes de ces problèmes et ensuite en déduire les exigences qui doivent être remplies en vue de les éviter:

- Le long délai d'accès au service est dû à: (1) le nombre élevé de messages, les tâches et les fonctions de mapping impliquées dans cette procédure, et (2) le fait que cette procédure implique un nombre élevé de nœuds IP-AN et de nœuds centralisés (premier routeur IP) pourrait induire un retard important dans la file d'attente de ces nœuds. La procédure de mobilité ISC souffre aussi d'un long délai, dû aux mêmes facteurs que la procédure d'accès au service, car elle implique les mêmes étapes. Cela conduit aux exigences suivantes:

  Exigence: la procédure d'accès aux services doit être optimisée, en termes de messages de signalisation et de fonctions de mapping.

  Exigence: le nombre de nœuds dans le modèle de réseau mobile doit être réduit, afin d'améliorer le délai d'accès au service et le délai de handover.

  Exigence: les nœuds centralisés doivent être évités.

- Le problème de non-adaptation de service est dû au fait que les informations sur la disponibilité des ressources relatives à chaque nœud IP-AN n'est pas facilement accessible à l'IMS, qui est responsable de l'adaptation des services. Cela conduit à l'exigence suivante:

  Exigence: une interaction étroite entre l'IMS et l'IP-AN doit être possible, sans rendre le réseau plus complexe. Cela permettrait une adaptation réactive du service.

- Les solutions pour les handovers baséess sur la charge ne sont pas simples car la décision de handover est prise par le MN et celui-ci manque d'informations de charge.

  Exigence: l'information de charge doit être aisément accessible à la fonction de handover.

  La liste d'exigences ci-dessus montre que le modèle IP-AN//PCC//IMS doit être examiné, principalement le nombre de types de nœuds et l'interaction entre l'IP-AN, le PCC, et l'IMS.

Chapitre 3 et 4: UFA: un nouveau modèle pour les réseaux mobiles du futur

L'analyse menée dans les chapitres précédents a permis de conclure que le modèle en couches (IP-AN//PCC//IMS) doit être réexaminé, notamment de nœuds et l'interaction entre l'IP-AN, le PCC, et l'IMS.

Les chapitre 3 et 4 fournissent une réponse à cette dernière conclusion. Il propose un nouveau modèle, appelé Ultra Flat Architecture (UFA), où le nombre de types de nœud de réseau est réduit et l'interaction entre l'IP-AN, le PCC, et l'IMS est simplifiée. La figure G.2 montre son architecture organique. UFA est constituée d'une seule couche contenant les fonctions de l'IP-AN, le PCC, et l'IMS. UFA est basé sur SIP et IMS pour assurer le contrôle de service pour tous les services. Ainsi, les services non-natifs SIP sont étendus pour être contrôlés par le protocole SIP. Cela a exigé une interaction entre protocole SIP et ces services dans le MN et le CN.

UFA introduit est de constitué de 5 nœuds de réseau: l'I-CSCF (proxy IMS), le S-CSCF (proxy IMS), le HSS (base de données) et de deux nouveaux nœuds, qui sont:

- UFA Gateway (UFA_GW): la UFA_GW est le nœud principal de UFA. Il regroupe les fonctions de l'IP-AN (par exemple NB, RNC, SGSN et GGSN fonctions pour l'UMTS), les fonctions de contrôle des politiques réseau (PCC) et les fonctions de l'IMS (le proxy P-CSCF). Cela signifie que la UFA_GW offre le contrôle de la session et offre en même temps la connectivité physique et IP aux utilisateurs. La UFA_GW est le premier routeur IP pour les utilisateurs.

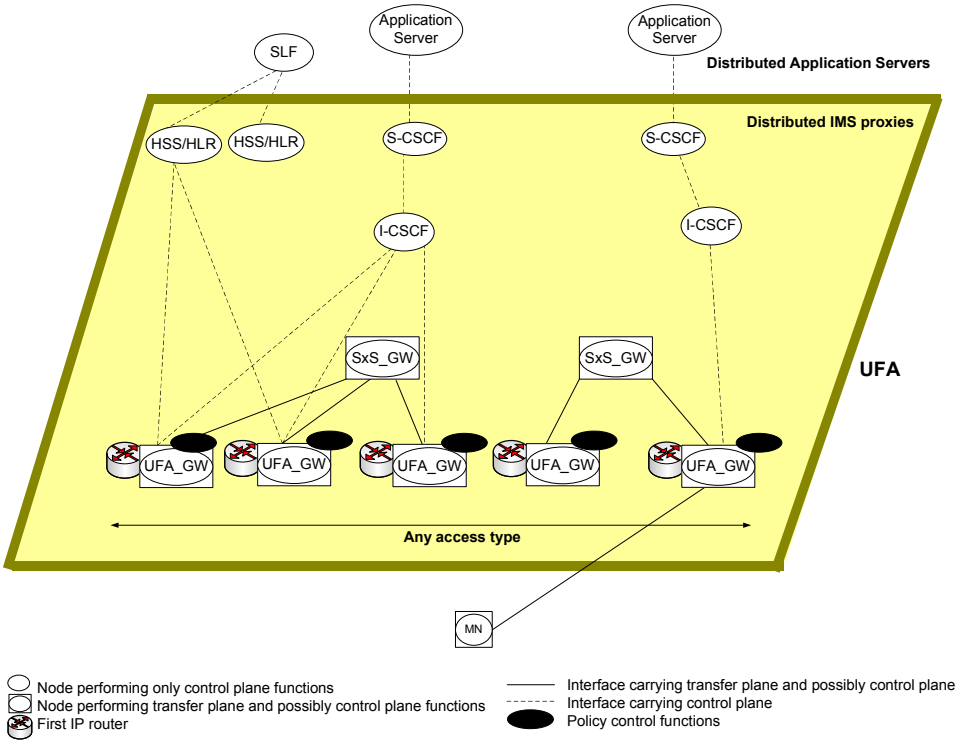


Figure G.2: Ultra Flat Architecture (UFA) model

- SIPcrossSCTP Gateway (SxS_GW): ce nœud est dédié aux services non-natifs SIP, spécialement lorsque l'interaction entre le protocole SIP et ces services n'est pas assurée par le CN.

La UFA_GW est le noeud principal de UFA. Elle assure les fonctions suivantes:

- Décider du moment de handover du mobile de la UFA_GW actuelle à une UFA_GW cible.
- Pendant la phase d'établissement de service ou de la procédure de mobilité, déterminer:
  - Pour le CN: La configuration du service pour les services natifs SIP, ou la configuration de la couche SCTP pour les services non natifs SIP:
    - La configuration du service pour les services natifs SIP contient, entre autres, des informations sur l'adaptation du service, sur la base des ressources disponibles dans la UFA_GW.
    - La configuration de la couche SCTP pour les services non natifs SIP contient, entre autres, une adaptation des valeurs de contrôle de congestion de SCTP. En effet, il est supposé que les services non-natif SIP, transportés sur SCTP sur le plan de transfert, n'ont pas besoin d'adaptation de service. Toutefois, pour utiliser efficacement la bande passante disponible, la couche SCTP doit être configuré avec des valeurs optimales pour les paramètres de contrôle de congestion .
  - Pour le MN: La configuration de toutes les couches OSI. Cette configuration comprend, entre autres, la configuration des services pour les services natifs SIP ou la configuration de la couche SCTP pour les services non natifs SIP.

UFA permet d'optimiser les délais d'accès aux services pour plusieurs raisons: (1) il y a moins de types de noeuds dans UFA, (2) les noeuds sont distribués ce qui consomme moins de temps

traitement, (3) la UFA_GW concentre la majorité des fonctions réseau ce qui permet de prendre plusieurs décisions liés à l'établissement de service en même temps.

La procédure de mobilité de UFA s'applique dans le cas d'un handover mono technologie ou multi technologie. Elle est basé sur le transfert du contexte de toutes les couches d'une UFA_GW à l'autre, et sur la reconfiguration de toutes les couches du mobile, en se basant sur des données fournis par la UFA_GW cible.

Chapitres 5, 6, 7: Evaluation des performances de UFA

Délai d'établissement de service

Le délai d'établissement de service a été mesuré dans UFA et comparé à celui du modèle IP-AN//PCC//IMS, en considérant une configuration réseau réelle et plusieurs situations de charge réseau. Une charge réseau est dûe à un nombre de requêtes d'établissement de service à l'entrée de la UFA_GW ou du Node B dans le cas du modèle IP-AN//PCC//IMS.

La courbe donnée par la figure G.3 montre que avec UFA le délai d'établissement de service est constant et est de 4s. Pour IP-AN//PCC//IMS, ce délai est plus élevé et varie de 8s à 18s selon la charge réseau. Cette augmantation rapide de délai est dû aux noeuds centralisés du modèle. Par exemple, pour 30 requêtes à l'entrée du Node B, Le proxy P-CSCF de IP-AN//PCC//IMS doit traiter 25600 requêtes.

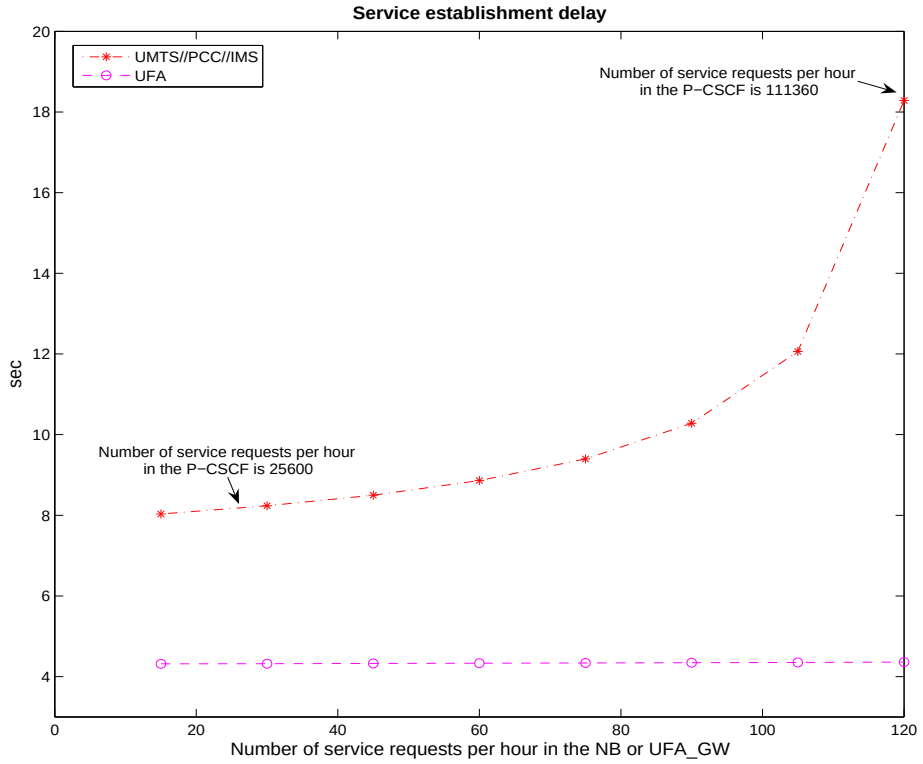


Figure G.3: Service establishment delay in UMTS//PCC//IMS and UFA

Implémentation et évaluation de la procédure de mobilité pour les services natifs SIP

Afin de prouver le concept de UFA et d'évaluer les performances de sa procédure de mobilité, celle-ci a été implémentée sur une maquette matérielle réelle.

La mesure des performances de la procédure de mobilité, montre qu'on a un délai de déconnexion réseau de 80ms et un délai de coupure pour une application voix de 100ms, ce qui est tout à fait acceptable.

Evaluation de la procédure de mobilité pour les services non natifs SIP

La procédure de mobilité de UFA a été évaluée pour les services non natifs SIP transportés sur le portocoles SCTP au niveau du plan de transfert. Pour celà une solution de référence a été considérée, il s'agit de m-SCTP.

m-SCTP est une extension de SCTP qui permet de gérer de bout en bout la mobilité des applications transportées sur SCTP. Il présente des problèmes de performance qui sont:

- Un long délai de handover mesuré au niveau SCTP, dû à un long délai de déconnexion réseau. En effet m-SCTP est souvent utilisé seul pour la gestion de la mobilité, et sans aucun outil pour optimiser le délai de déconnexion réseau.
- Une sous-utilisation de la bande disponible suite à un handover car les paramètres de contrôle de congestion de SCTP sont initiés à leur valeurs par défaut.

UFA résout ces problèmes puisque elle réduit le délai de déconnexion réseau et elle adapte de façon proactive les paramètres de contrôle de congestion de SCTP à la bande disponible suite à un handover.

Figure G.4 montre le volume additionnel que permet de télécharger UFA par rapport à m-SCTP. Nous remarquons que UFA offre une amélioration qui varie de 0,5% à 8%. Pour un nombre de handover égal à 6, nous observons que UFA permet de télécharger 2 Moctets en plus. Cette valeur ne doit pas être négligée puisqu'elle est calculée pour une courte durée de simulation (500s) et elle correspond à un seul utilisateur.

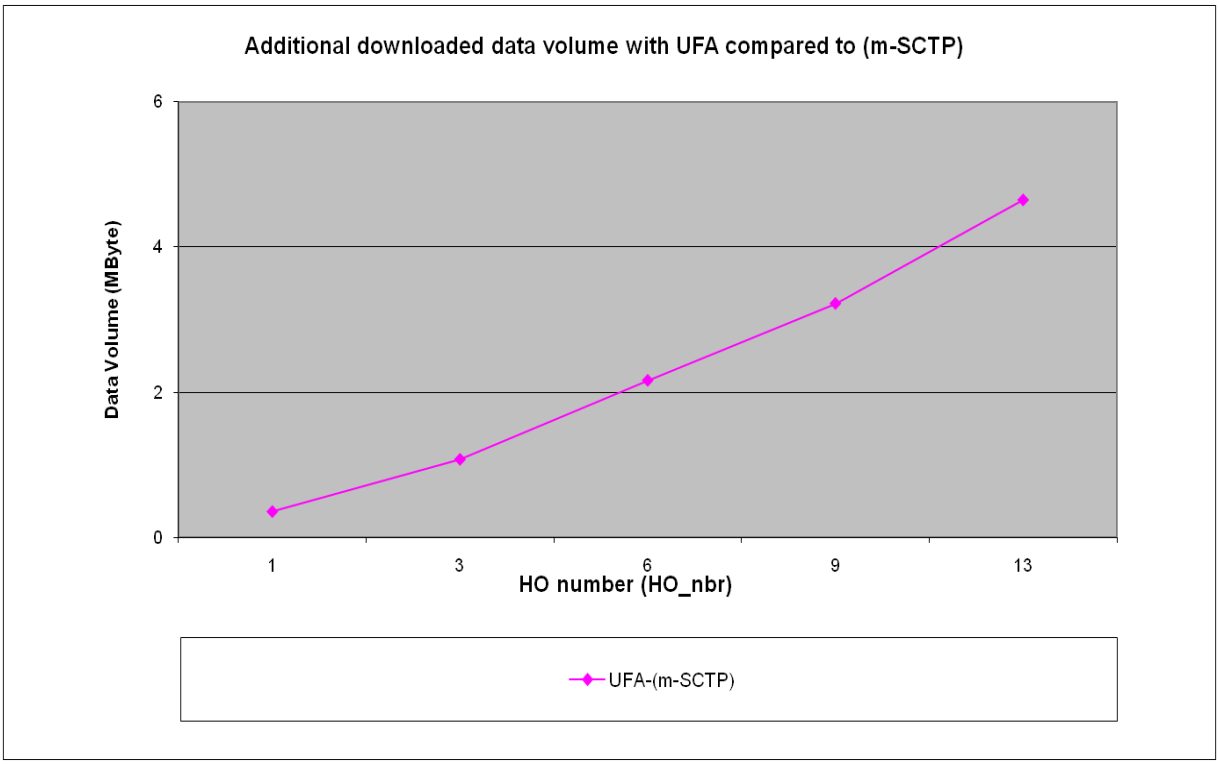


Figure G.4: Volume additionnel téléchargé avec UFA par rapport à m-SCTP

Part VII

Acronyms

3G Third generation

3GPP 3rd Generation Partnership Project

A

AAA Authentication Authorization and Accounting

ACK Acknowledgment

ADSL Asymmetric Digital Subscriber Line

AF Application Function

AH Authentication Header

AKA Authentication and Key Agreement

AMR Adaptive Multi-Rate

AS Application Server

ATH Authentication

B

B2BUA Back to Back User Agent

BBERF Bearer Binding and Event Reporting Function

BDP Bandwidth Delay Product

BS Base Station

BSC Base Station Controller

C

CAGR Compound Annual Growth Rate

CK Ciphering Key

CN Correspondent Node

CoN Connectivity Node

CSCF Call Session Control Function

cwnd congestion window

D

DAD Duplicate Address Detection

DHCP Dynamic Host Configuration Protocol

DiffServ Differentiated Services

DNS Domain Name Server

DSCP DiffServ Code Point

E

EAP Extensible Authentication Protocol

EDGE Enhanced Data Rates for GSM Evolution

EPC Evolved Packet Core

EPS Evolved Packet System

ESP Encapsulating Security Payload

F

FMIP Fast Mobile IP

FTP File Transfer Protocol

G

GAN Generic Access Network

GANC Generic Access Network Controller

GERAN GSM EDGE Radio Access Network

GGSN Gateway GPRS Support Node

GIBA GPRS-IMS-Bundled Authentication

GPRS General Packet Radio Service

GSM Global System for Mobile Communications

GTP GPRS Tunneling Protocol

GW GateWay

H

HA Home Agent

HLR Home Location Register

HO Handover

HSPA High Speed Packet Access

HSS Home Subscriber Server

HTTP HyperText Transfer Protocol

I

I-CSCF Interrogating CSCF

I-WLAN WLAN Interworking

ID Identity

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IK Integrity Key

IKE Internet Key Exchange

IMPI IMS Private Identity

IMPU IMS Public Identity

IMS IP Multimedia Subsystem

IMSI International Mobile Subscriber Identity

Intserv Integrated service

IP Internet Protocol

IP-AN IP-Access Network

IP-CAN IP-Connectivity Access Network

IPsec IP security

IPTV IP Television

IPv4 Intrenet Protocol version 4

IPv6 Internet Protocol version 6

ISC IMS Service Continuity

ITU International Telecommunication Union

M

m-SCTP mobile Stream Control Transmission Protocol

MAC Media Access Control

Mbps Mega Bytes per second

MIP Mobile IP

MIPv6 Mobile IP version 6

MMS Multimedia Message Service

MN Mobile Node

MNO Mobile Network Operator

MTU Maximum Transmission Unit

N

NAT Network Address Translation

NB NodeB

ND Neighbor Discovery

NS2 Network Simulator

O

OPEX OPerational EXpenditure

OSI Open Systems Interconnection

P

P-CSCF Proxy-CSCF

PCC Policy Control and Charging

PCEF Policy and Charging Enforcement Function

PCMCIA Personal Computer Memory Card International Association

PCRF Policy and Charging Rules Function

PDG Packet Data Gateway

PDP Packet Data Protocol

Q

QoS Quality of Service

R

RA Router Advertisement

RAB Radio Access Bearer

RAN Radio Access Network

RAN Radio Access Network

RAND Random

reg registration

RFC Request For Comment

RM Resource Manager

RNC Radio Network Controller

RRC Radio Resource Control

RSVP Resource ReSerVation Protocol

RTCP RTP Control Protocol

RTO Retransmission TimeOut

RTP Real-Time Protocol

RTSP Real Time Streaming Protocol

RTT Round-Trip Time

S

S-CSCF Serving-Call Session Control Function

S-CSCF Serving-CSCF

SA Security Association

SAD Security Association Database

SCC Session Centralization and Continuity

SCTP Stream Control Transmission Protocol

SDP Session Description Protocol

SGSN Serving GPRS Support Node

SI Service Information

sig signalling

SIP Session Initiation Protocol

SLF Subscription Locator Function

SMS Short Message Service

SPD Security Policy Database

ssthresh slow start threshold

SxS SIPcrossSCTP

T

TCP Transmission Control Protocol

TR Tecchnical Reports

TS Technical Specifications

TSN Transmission Sequence Number

U

UA User Agent

UAC UA Client

UAS User Agent Server

UDP User Datagram Protocol

UFA Ultra Flat Architecture

UMTS Universal Mobile Telecommunications System

UPCEF UFA PCEF

URI Uniform Resource Identifier

USB Universal Serial Bus

UTRAN Universal Terrestrial Radio Access Network

V

VoIP Video over IP

W

WAG WLAN Access Gateway

WCDMA Wideband Code-Division Multiple Access

WiFi Wireless Fidelity

WiMAX Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Network

X

XRES Expected Response

List of Figures

1 Cisco forecasts for traffic generated by dongles (laptops) and smartphones (from [4]) 6

2 Cisco forecasts for mobile data growth (from [4]) 6

1.1 Mobile networks layered model 14

1.2 A common mobile networks layered model: IP-AN//PCC//IMS 17

1.3 Policy control functions in the IP-AN//PCC//IMS model 20

1.4 (GSM and UMTS)//PCC//IMS 23

1.5 GAN//PCC//IMS 24

1.6 I-WLAN//PCC//IMS 25

1.7 (Inter I-WLAN - 3GPP mobility)//PCC//IMS 26

1.8 WiMAX//PCC//IMS 27

1.9 EPS//PCC//IMS 28

1.10 IMS Service Continuity (ISC) 32

2.1 Phase 1: registration/authentication 37

2.2 Registration/authentication to the IMS detailed message flow (3GPP ATH_5) . . 41

2.3 Phase 2: service establishment 43

2.4 End-to-End message flow for service establishment (phase 2) considering UMTS as an IP-AN example 45

2.5 Registration/authentication to the IMS detailed message flow in [70]) 49

2.6 Registration/authentication to the IMS detailed message flow in [63] 49

2.7 case 1/solution 1: the network supports resource renegotiation/ service adaptation is initiated by the network 51

2.8 case 1/solution 2: the network supports resource renegotiation/ service adaptation is initiated by the MN 51

2.9 ISC mobility procedure 55

2.10 Timing diagram for ISC mobility procedure 57

3.1 Ultra Flat Architecture (UFA) model 66

3.2 Policy control functions in UFA 68

3.3 UFA control and transfer planes 69

4.1 Registration/authentication to UFA 76
4.2 Service establishment in UFA for SIP native services 79
4.3 Service establishment in UFA for non-SIP native services 79
4.4 Detailed message flow for service establishment in UFA for SIP native services . . 82
4.5 Mobility procedure for SIP native services 86
4.6 Mobility procedure for non-SIP native services 88

5.1 Radio, network and node delay components within the service establishment delay 94
5.2 Service requests arrival rate within a node 96
5.3 Service establishment delay in UMTS//PCC//IMS and UFA 99
5.4 Components of service establishment delay in UMTS//PCC//IMS and UFA 99
5.5 SESSION PROGRESS message end-to-end delay in UMTS//PCC//IMS and UFA 100
5.6 Node delay introduced by each of the UMTS//PCC//IMS nodes and UFA nodes for the SESSION PROGRESS message 100
5.7 Node delay introduced by each of the UFA nodes for the SESSION PROGRESS message, in case of a high number of service requests 102
5.8 Service establishment delay in UFA in case of a high number of service requests . . 102

6.1 Handover delay components in Implemented ISC mobility procedure 106
6.2 Handover delay components in UFA mobility procedure 106
6.3 Testbed architecture 108
6.4 Implementation of all-OSI layer configuration in the UFA Mobile Node 111
6.5 Number of lost packets in Implemented ISC on the MN wireshark 115
6.6 Application handover delay in Implemented ISC on the MN wireshark 115
6.7 Number of lost packets in UFA on the MN wireshark 116
6.8 Application handover delay in UFA on the MN wireshark 116
6.9 Case 1 of UFA handover delay 120
6.10 Case 2 of UFA handover delay 120
6.11 Case 3 of UFA handover delay 120
6.12 Case 4 of UFA handover delay 120

7.1 SCTP parameters on the sender and receiver sides 125
7.2 Handover delay components with m-SCTP mobility procedure 127
7.3 Handover delay components with UFA mobility procedure, for non-SIP native services 131
7.4 Network parameters 133
7.5 TSN on the CN side for m-SCTP and UFA SxS configuration option in the network scenario Sc1 135

7.6 `Cwnd` for the different UFA SCTP configuration options in the network scenario Sc2 135
7.7 Comparison of m-SCTP, m-SCTP+, SxS, SxS+, SxS++ in the network scenario Sc1 136
7.8 Comparison of SxS, SxS+, SxS++ in the network scenario Sc2 136

A.1 Example of service management with SIP: establishment, mobility execution, termination 152

D.1 MIP-based mobility procedure 158

E.1 SIP INVITE message during service establishment in UFA 163
E.2 SIP SESSION PROGRESS during service establishment in UFA 164
E.3 CONTEXT TRANSFER message (3) during handover in UFA 165
E.4 ACK message (4) during handover in UFA 166
E.5 Re-INVITE messages (5 and 5A) during handover in UFA 167
E.6 Re-INVITE message (8) during handover in UFA 168

F.1 Architecture of SIP programs based on PJSIP library 170
F.2 Handling of SIP INVITE message by MN 171
F.3 Handling of SIP INVITE message by UFA_GW 171
F.4 Handling of SIP INVITE message by CN 172

G.1 IP-AN//PCC//IMS 177
G.2 Ultra Flat Architecture (UFA) model 181
G.3 Service establishment delay in UMTS//PCC//IMS and UFA 182
G.4 Volume additionnel téléchargé avec UFA par rapport à m-SCTP 184

List of Tables

1.1 IP-AN//PCC//IMS model analysis 31

1.2 Service types 33

2.1 Protocols and means to execute the different registration/authentication steps in each IP-AN 42

2.2 Summary of the solutions proposed to solve service access and mobility procedures problems 60

3.1 UFA model analysis 71

4.1 `SDPN`: Session Description Protocol for Non-SIP native services 80

4.2 UFA_Terminal_Conf header 89

4.3 UFA_Appli_Conf_IP header 89

5.1 Node delay parameters 96

5.2 Simulation inputs 98

6.1 Implemented ISC and UFA, and their handover delay components 107

6.2 Length of handover messages in UFA 117

6.3 UFA handover delays for different network scenarios 120

7.1 Considered network scenarios (Sc) for simulation 133

A.1 SIP INVITE request message 149

A.2 SIP headers 150

A.3 example of SDP for a video call 151

G.1 Résumé des solutions proposées pour résoudre les prblèmes des procédures d'accès au service et de mobilité 179

Bibliography

[1] 3GPP, "High Speed Downlink Packet Access (HSDPA)", TS 25.308, Release 9.

[2] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)", TS 36.300, Release 9.

[3] WMF-T32-001-R015v01, "WiMAX Forum Network Architecture: Architecture Tenets, Reference Model and Reference Points Base Specification", Release 1.5, November 2009.

[4] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update", http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

[5] N.G.Panagiotidis, "Network 2020 vision from "Telco" To QOE service provider", http://www.bloobble.com/broadband-presentations/presentations?itemid=2328

[6] G.Chua, "Mobile networks at the tipping point: The data explosion and next generation network challenge", White paper spensored by Juniper Networks, http://www.thenewnetworkishere.com/pdfs/juniper-lte-and-epc-transformation.pdf.

[7] "Future Mobile Networks: LTE, backhaul, femtocells, optimization and other strategies to address network congestion", Informa Telecoms & Media, May 2010, http://www.telecomsmarketresearch.com/research/TMAAAVNS-Future-Mobile-Networks–2nd-edition—-Informa-Telecoms—Media.shtml

[8] C.Davies, J.Dawson, T.Cripps, J.Green, "Telecoms in 2020", Ovum, http://www.ovum.com/go/content/s,78583.

[9] "Ultra Flat Architecture for high bitrate services in fixed mobile convergent networks", P1857 Eurescom project, January 2009- May 2010, http://www.eurescom.eu/Public/Projects/P1800-series/P1857/default.asp.

[10] "Mobile Networks Evolution for Individual Communications Experience", MEVICO celtic project, May 2010-2012, http://www.celtic-initiative.org/Projects/MEVICO/abstract.asp

[11] N.Niebert, A.Schieder, H.Abromiwicz, G.Malmgren, J.Sacks, U.Horn, H.Karl, "Ambiant Networks: An architecture for communication networks beyond 3G", IEEE Wireless Communications Magazine, April 2004.

[12] L.Subramanian, I.Stoica, H.Balakrishnan, R.H. Katz "OverQoS: An Overlay based Architecture for Enhancing Internet QoS", in proceedings of the 1st conference on Symposium on Networked Systems Design and Implementation (NSDI)- Volume 1, San Francisco, CA, March 2004.

[13] 3GPP, "IP Multimedia Subsystem (IMS)", TS 23.228, Release 9.

[14] 3GPP, "Policy Control and charging architecture", TS 23.203, Release 9.

[15] E.Lavinal, N.Simoni, M.Song, B.Mathieu, "A next-generation service overlay architecture", Annals of Telecommunications, volume 64, Numbers 3-4/April 2009.

[16] S.Schmid, F.Hartung, M.Kampmann, S.Herborn, J.Rey, "SMART: Intelligent Multimedia Routing and Adaptation based on Service Specific Overlay Networks", in proceedings of Eurescom Summit, Ubiquitous Services and applications, 2005.

[17] H.Badis, K.Al Agha, "Fast and efficient vertical handoffs in wireless overlay networks", in proceedings of 15th IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2004.

[18] J.Rosenberg, et al., "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[19] ETSI, "General description of a GSM Public Land Mobile Network (PLMN)", GSM 01.02, R97.

[20] 3GPP, "UTRAN overall description", TS 25.401, Release 9.

[21] 3GPP, "General Universal Mobile Telecommunications System (UMTS) architecture", TS 23.101, Release 9.

[22] 3GPP, "GPRS Service description", TS 23.060, Release 7.

[23] 3GPP, "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", TS 29.060, Release 9.

[24] 3GPP, "Generic Access Network (GAN)", TS 43.318, Release 9.

[25] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description", TS 23.234, Release 9.

[26] 3GPP, "Mobility between 3GPP-Wireless Local Area Network (WLAN) interworking and 3GPP systems", TS 23.327, Release 9.

[27] C.Perkins, "IP Mobility Support for IPv4", RFC 3344, August 2002.

[28] WiMAX Forum, "Network Architecture: Architecture, detailed Protocols and Procedures Policy and Charging Control", WMF-T33-109-R015v01, Release 1.5, November 2009.

[29] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", TS 23.401, Release 9.

[30] ETSI TS 182.082, "IPTV functions supported by the IMS subsystem", version 2.0.0.

[31] S.Guha, P.Francis, "Towards a Secure Internet Architecture Through signalling". Technical report, http://www.guha.cc/ saikat/pub/cucs06-nutss.pdf, Cornell University, 2006.

[32] J.Chan , B.Landfeldt , R.Liu , A.Seneviratne, "A home-proxy based wireless internet framework in supporting mobility and roaming of real-time services", IEICE Transactions on Communications, vol.E84-B, NO.4 April 2001.

[33] P.Bertin, S.Bonjour, JM.Bonnin, "A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures", procceedings of IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2008.

[34] M.Matuszewski, M.Martin, "A distributed IP multimedia subsystem", IEEE International Symposium on a In World of Wireless, Mobile and Multimedia Networks, WoWMoM 2007.

[35] M.Fisher, F.Anderson, A.Göspel, G.Schäfer, M.Schäfler, "A distributed IP mobility approach for 3G SAE", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2008.

[36] S.Sim, S.Han, J.Parck, S.Lee, "Seamless IP mobility support for flat architecture mobile WiMAX Networks", IEEE Communication Magazine, June 2009.

[37] P.Agrawal, et.al, "IP Multimedia Subsystems in 3GPP and 3GPP2: Scalability issues", IEEE Communications Magazine, January 2008.

[38] K.Daoud, P.Herbelin, Noel Crespi, "UFA: an ultra flat architecture for high bitrate services in mobile networks", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2008.

[39] 3GPP, "IP Multimedia Subsystem (IMS) Service Continuity", TS 23.237, Release 9.

[40] T.Chiba, H.Yokota, A.Idoue, A.Dutta, K.Manousakis, S.Das, H.Schulzrinne "Trombone Routing Mitigation Techniques for IMS/MMD Networks", Wireless Communications and Networking Conference (WCNC), 2007.

[41] B.Wang, J.Kurose, P.Shenoy, D.Towsley, "Multimedia Streaming via TCP: An Analytic Performance Study", ACM Transactions on Multimedia Computing, Communications, and Applications; Volume 4 Issue 2, May 2008.

[42] J.Merwe, S.Sen, C.Kalmanek, "Streaming Video Traffic : Characterization and Network Impact", in proceedings of the 7th International Web Content Caching and Distribution Workshop, 2002.

[43] D.Yon, G.Camarillo, "TCP-Based Media Transport in the Session Description Protocol (SDP)", RFC 4145, September 2005.

[44] M.Garcia-Martin et al., "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer", RFC 5547, May 2009.

[45] S.Baba, J.Chen, A.Dutta, Y.Shobatake, F.Vakil, "A method and system for host mobility management", Patent US 7184418 B1, February 2007.

[46] H.Miyajima, L.Zhang, H.Hayashi, T.Fuji, "An implementation of enhanced All-SIP mobility", in proceedings of IEEE 19th Personal, Indoor and Mobile Radio Communications (PIMRC), 2008.

[47] Y-S.Chen, K-L.Chui, R-H.Hwang, "SmSCTP: SIP-Based MSCTP Scheme for Session Mobility over WLAN/3G Heterogeneous Networks", in proceedings of IEEE Wireless Communications and Networking Conference (WCNC), 2007.

[48] 3GPP, "Security architecture", TS 33.102, Release 9.

[49] 3GPP, "GPRS service description", TS 23.060, Release 9.

[50] 3GPP, "Mobile radio interface layer 3 specification", TS 24.008, Release 9.

[51] 3GPP, "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling", TS 25.413, Release 9.

[52] S.Kent, R.Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[53] 3GPP, "3G Security; Wireless Local Area Network (WLAN) interworking security", TS 33.234, Release 9.

[54] R.Droms, "Dynamic Host Configuration Protocol", RFC 2131, march 1997.

[55] H.Schulzrinne, B.Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC 3319, July 2003.

[56] T.Narten, E.Nordmark, W.Simpson, H.Soliman, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 4861, September 2007.

[57] 3GPP, "Signalling flows for the IP multimedia call control based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)", TS 24.229, Release 9.

[58] H.Schulzrinne, "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers", RFC 3361, August 2002.

[59] J.Kempf, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[60] J.Rosenberg, H.Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

[61] WiMAX Forum, "Network Architecture: Architecture, detailed Protocols and Procedures IP Multimedia Subsystem (IMS) Interworking", WMF-T33-101-R015v01, Release 1.5, November 2009.

[62] R.Droms, "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.

[63] 3GPP, "Access security for IP-based services", TS 33.203, Release 9.

[64] 3GPP, "IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signalling flows and message contents", TS 29.228, Release 9.

[65] M.Handley, V.Jacobson, C.Perkins, "SDP: Session Description Protocol", RFC 4566, July 2006.

[66] 3GPP, "Signalling System No. 7 (SS7) security gateway; Architecture, functional description and protocol details", TS 29.204, Release 9.

[67] 3GPP, "Policy and charging control over Gx reference point", TS 29.212, Release 9.

[68] 3GPP, "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping", TS 29.213, Release 9.

[69] 3GPP, "Policy and charging control over Rx reference point", TS 29.214, Release 9.

[70] Yi-Bing Lin, Ming-Feng Chang, Meng-Ta Hsu, and Lin-Yi Wu, "One-Pass GPRS and IMS Authentication Procedure for UMTS", IEEE Journal on selected areas in communications, Vol. 23, NO. 6, June 2005.

[71] S.Zaghoul et al, "Extending QoS from radio acces to an all-IP core in 3G networks: an operator's perspective", IEEE communications magazine, September 2007.

[72] A.C Mahendran, J.Wang, H.Jin, "Method and apparatus for optimized session setup with network-initiated QoS policy control", patent US 2009/0190471 A1, July 2009.

[73] 3GPP, "UTRAN Iu interface Radio Access Network Application Part (RANAP) signalling", TS 25.413, Release 4.

[74] P.Chiron, E.Njedjou, P.Seité, K.Goss, E.Melin, P.Roux, "Architectures for IP-based network assisted mobility management accross heterogenous networks", IEEE wireless Communications magazine, April 2008.

[75] V.Hilt, G.Camarillo, J.Rosenberg, "A framework for session initiation protocol (SIP) session policies", ietf draft-ietf-sip-session-policy-framework-07, April 2008.

[76] M.I.Corici, F.Carvallo de Gouveia, T.Megedanz, "A network controlled QoS model over the 3GPP system architecture evolution", second international on wireless broadband and ultra wideband communications (AusWireless), 2007.

[77] 3GPP, "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) service continuity, stage3", TS 24.237, Release 9.

[78] A.Dutta, G.Abhrajit, S.Das, D.Chee, K.Manousakis, J.Lin, T.Chiba, H.Yokota, A.Idoue, S.Li, "P-CSCF fast handoff for IMS/MMS handoff", International patent, WO 2008/033381 A2, March 2008.

[79] K.Lynggaard, E.Vestergaard, H.Peter, G.Kuhn, "Optimized Macro Mobility within the 3GPP IP Multimedia Subsystem", Second International Conference on Wireless and Mobile Communications (ICWMC'06), 2006.

[80] P.Herbelin, K.Daoud, J.Pons, "Patent: Procédés nécessaires à la mobilité des terminaux mobiles rattachés à des stations de base en s'appuyant sur l'implémentation d'un protocole de niveau 4 à 7 du modèle OSI", October 2007, currently the registration request is extended at the international level.

[81] K.Daoud, P.Herbelin, K.Guillouard, N.Crespi, "Performance and implementation of UFA: A SIP-based Ultra Flat Architecture Mobile Network Architecture", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2009.

[82] Common Public Radio Interface (CPRI): interface specification v4.1, feb. 2009, http://www.cpri.info.

[83] Z.Yan, L.Lei, M.Chen "WIISE - a completely flat and distributed architecture for future wireless communications systems", Wireless Word Research Forum 21.

[84] R.Fracchia, C.Casetti, C.-F.Chiasserini, M.Meo, "A wise extension of SCTP for wireless networks", in proceedings of IEEE International Conference on Communications (ICC), 2005.

[85] K.Daoud, P.Herbelin, N.Crespi, "One-Node-Based Mobile Architecture For a Better QoS Control", in proceedings of IFIP Wireless Days 2008.

[86] P.Herbelin, K.Daoud, C.Léveque, "Patent: Procédés et terminaux de communication pour améliorer le transfert de connexion entre des cellules appartenant à des réseaux différents" , Mars 2009, currently the registration request is extended at the international level.

[87] K.Daoud, P.Herbelin, "Patent: Utilisation du protocole SIP pour la distribution des flux non-SIP établis entre deux nœuds utilisateurs joignables par différents chemins réseau", May 2009, currently the registration request is extended at the international level.

[88] F.Allard, J.M.Bonnin, "An application of the context transfer protcol: IPsec in a IPv6 mobility environment", International Journal Communication networks and distributed systems, Vol.1, No.1, 2008.

[89] ITU, "Network grade of service parameters and target values for circuit-switched public land mobile services in the Evolving ISDN", E.771, 1991.

[90] H.Fathi, S.S.Chakraborty, R.Prasad, "Optimization of SIP Session Setup Delay for VoIP in 3G Wireless Networks", IEEE Transactions on Mobile Computing archive, Volume 5, Issue 9, pages 1121-1132, 2006.

[91] N.Banerjee, K.Basu, S.K.Das, "Hand-off Delay Analysis in SIP-based Mobility Management in Wireless Networks", in proceedings of the 17th International Symposium on Parallel and Distributed Processing, 2003.

[92] N.Banerjee, W.Wu, K.Basu, S.K.Das, "Analysis of SIP-based mobility management in 4G wireless networks", Elsevier, computer communications, volume 27, Issue 8, Pages 697-707, May 2004.

[93] L.Klienrock, QUEUING SYSTEMS volume I: therory, John WileySons, 1975.

[94] http://www.netlab.tkk.fi/opetus/s383143/kalvot/english.shtml, priority queues.

[95] Matlab simulator, http://www.mathworks.fr/.

[96] "The madwifi project", http://madwifi-project.org/

[97] "Open Source SIP stack and media stack for presence, instant messaging, and multimedia communication", http://www.pjsip.org/.

[98] Remote Streaming, an PJMEDIA example application to stream media file to remote peer using RTP, http://www.pjsip.org/pjmedia/docs/html/page_pjmedia_samples_streamutil_c.htm.

[99] J.Salim, H.Khosravi, A.Kleen, A.Kuznetsov, "Linux Netlink as an IP Services Protocol", RFC 3549, July 2003.

[100] "Airmagnet tool", http://www.airmagnet.com/products/wifi_analyzer/.

[101] "Wireshark tool", http://www.wireshark.org/.

[102] "3GPP Long-Term Evolution / System Architecture Evolution Overview", U.Barth, Alcatel, september 2009, http://www.ikr.uni-stuttgart.de/Content/itg/fg524/Meetings/2006-09-29-Ulm/01-3GPP_LTE-SAE_Overview_Sep06.pdf.

[103] "Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)", TR 25.913, Release 9.

[104] J.Sanchez and M.Thouine, "UMTS", Hermes, second edition, 2004.

[105] R.Stewart et al., "Stream Control Transmission Protocol (SCTP) Dynamic Address Reconfiguration", RFC 5061, September 2007.

[106] R.Stewart, "Stream Control Transmission Protocol", RFC 4960, September 2007.

[107] Y.Qia et al, "The performance of TCP/IP for networks with high bandwidth-delay products and random loss", IEEE/ACM transactions on networking, vol.5, NO.3, June 1997.

[108] G.Appenzeller, I.Keslassy, N.Mckeown, "Sizing router buffers", SIGCOMM 2004.

[109] M.Chang, M.Lee, H.Lee, "An enhancement of transport layer apporach to mobility support", Lecture notes in computer science (LNCS), volume 3391, 2005.

[110] M.Honda, H.Sakakibara, Y.Nishida, H.Tokuda, "SmSCTP: A Fast Transport Layer Handover Method Using Single Wireless Interface", in proceedings of the 12th IEEE Symposium on Computers and Communications (ISCC 2007), 2007.

[111] Yuansong Qiao, Enda Fallon, Liam Murphy, John Murphy, Austin Hanley, Xiaosong Zhu, Adrian Matthews, Eoghan Conway, and Gregory Hayes, "SCTP Performance Issue on Path Delay Differential", in proceedings of the 5th international conference on Wired/Wireless Internet Communications, Lecture Notes In Computer Science; Vol. 4517, 2007.

[112] R.Koodli, "Fast Handovers for Mobile IPv6", RFC 4068, July 2005.

[113] X.Wu, M.Choon Chan, A.L.Ananda, "TCP Handoff: A practical enhancement for heterogenous mobile environments", in proceedings of IEEE International Conference on Communications (ICC), 2007.

[114] M.Afif, P.Martins, S.Tabbane, P.Godlewski, "Radio aware SCTP extension for Handover in EGPRS", in proceedings of IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2006.

[115] G.De Marco, S.Loreto, L.Barolli, "Performance Analysis of IP Micro-mobility Protocols in Single and Simultaneous Movements", Embedded and ubiquitous computing (EUC Workshops), Lecture notes in computer science (LNCS), vol 3823, pp.443, 2005.

[116] K.Daoud, K.Guillouard, P.Herbelin, N.Crespi, "A Network-Controlled Architecture for SCTP Hard Handover", in proceedings of Vehicular Technology Conference (VTC-fall), 2010.

[117] "Network Simulator NS2", http://www.isi.edu/nsnam/ns/.

[118] Z.Faigl, L.Bokor, P.Neves, R.Pereira K.Daoud, P.Herbelin, "Evaluation and Comparison of signalling Protocol Alternatives for the Ultra Flat Architecture", in proceedings of the fifth international conference on systems and networks communications (ICSNC) 2010.

[119] Z.Faigl, L.Bokor, P.Neves, R.Pereira K.Daoud, P.Herbelin, "Evaluation of two integrated signalling schemes for the Ultra Flat Architecture using SIP, IEEE 802.21, and HIP/PMIP protocols", accepted in Elsevier comnet 2010.

[120] 3GPP, "IP network layer security", TS 33.210, Release 9.

[121] G.Camarillo, W.Marshall, J.Rosenberg, "Integration of Resource Management and Session Initiation Protocol", RFC 3312, October 2002.

[122] A.Dutta, T.Zhang, K.Taniuchi, Y.ohba, H.Schulzrinne, "MPA assisted Optimizd Proacive Handoff Scheme", in proceedings of the Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous05), 2005.

[123] A.Dutta, Y.Ohba, K.Taniuchi Tari, H.Schulzrinne, "A Framework of Media-Independent Pre-Authentication (MPA) for Inter-domain Handover Optimization", IETF draft, draft-ohba-mobopts-mpa-framework-05, July 2007.

[124] J.Loughney et al., "Context Transfer Protocol (CXTP)", RFC 4067, July 2005.

Copyright by Khadija Daoud Triki, 2010
All rights reserved

Résumé

L'explosion du volume de trafic de données dans les réseaux mobiles, prévue pour les années 2010-2020, est communément admise par les communautés académique et industrielle. La capacité de ces réseaux à supporter cette croissance de trafic, couplée à une forte pression sur la réduction des coûts, est un enjeu majeur pour les opérateurs.

Les réseaux mobiles, déployés ou en cours de standardisation, répondent à un modèle en couches, avec: (1) un réseau d'accès, mono ou multi technologies, offrant une connectivité IP aux utilisateurs; (2) une couche de contrôle de service, telle que l'IMS, la solution standardisée la plus aboutie aujourd'hui; (3) une couche d'interaction (PCC), entre le réseau d'accès et la couche de contrôle de service, permettant le contrôle des politiques réseau. Ce modèle est très centralisé et comporte plusieurs types de nœuds réseau hiérarchisés. Il est à l'origine de problèmes de passage à l'échelle et de qualité de service (délai d'accès au service, délai de handover, difficulté d'adapter le service aux ressources). La résolution de ces problèmes augmente encore la complexité du modèle, ce qui nous a conduit à le revisiter.

Dans cette thèse, un nouveau modèle pour les futurs réseaux mobiles est proposé: Ultra Flat Architecture (UFA). UFA utilise l'IMS comme solution unifiée pour le contrôle de tout type d'applications, SIP ou non. L'architecture est dite "plate" puisqu'elle réduit le nombre de nœuds réseau à 3 principalement: (1) une Gateway UFA offrant une connectivité physique au terminal et regroupant à la fois l'ensemble des fonctionnalités du réseau d'accès, de la couche de contrôle de service (IMS) et de la couche de contrôle des politiques réseau; (2) une Gateway permettant le support des services non-SIP; et enfin (3) le terminal.

Après la conception de l'architecture, notre contribution s'est focalisée sur la spécification des trois procédures principales d'UFA: l'enregistrement/authentification, l'établissement de service et la mobilité. Nous avons optimisé les deux premières procédures par rapport aux procédures standardisées de l'IMS. Par exemple, la procédure d'établissement de service présente un délai réduit et permet une configuration du service ou de la couche de transport selon les ressources disponibles dans le réseau. Nous avons aussi spécifiquement développé une procédure de mobilité pour UFA. Pour un terminal en mobilité, cette procédure se base sur le transfert, d'une Gateway UFA à une autre, des contextes de toutes les couches OSI liés à ce terminal, et sur la détermination proactive par la Gateway UFA des paramètres de toutes les couches du terminal, nécessaires à son attachement à la nouvelle Gateway UFA.

La dernière partie de la thèse consiste à évaluer le modèle UFA et les procédures proposées. Nous avons d'abord mesuré, à l'aide de modèles analytiques, le délai d'établissement de service dans UFA et dans le modèle existant. Les résultats montrent qu'UFA fournit de meilleures performances, et mettent en évidence sa grande capacité de passage à l'échelle. Nous avons ensuite implémenté UFA sur une maquette. Au-delà de la validation de ses concepts, nous avons relevé, pour les applications (e.g. voix, vidéo) transportées sur le protocole RTP/UDP, un délai de handover performant. Enfin, nous nous sommes intéressés aux applications (e.g. streaming) transportées sur le protocole SCTP. Nous avons montré, par simulation avec NS2, l'intérêt de l'architecture UFA et de sa procédure de mobilité dans l'amélioration des performances de ces applications, en cas de mobilité. Ainsi, tous les résultats obtenus montrent le grand intérêt d'UFA et des architectures plates plus généralement.

Mots clés: architectures plates, IMS, SIP, SCTP, handover.