Conception et validation d'une architecture de signalisation pour la garantie de qualité de service dans l'Internet multi-domaine, multi-technologie et multi-service

Stelian-Florin Racaru

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par *l'Institut National des Sciences Appliquées Toulouse*
Discipline ou spécialité : *Informatique et Télécommunications*

Présentée et soutenue par *Stelian Florin RACARU*
Le *14 octobre 2008*

Titre :
Conception et validation d'une architecture de signalisation pour la garantie de qualité de service dans l'Internet multi-domaine, multi-technologie et multi-service

---

JURY
Christian FRABOUL - Président
Francis LEPAGE - Rapporteur
Abdelhamid MELLOUK - Rapporteur
Olivier DUGEON - Examinateur
Michel DIAZ - Examinateur
Christophe CHASSOT -Examinateur
Laurent BARESSE - Invité

Ecole doctorale : *Mathématiques Informatique Télécommunication de Toulouse*
Unité de recherche : *Laboratoire d'Analyse et d'Architecture des Systèmes*
Directeur(s) de Thèse : *Michel DIAZ et Christophe CHASSOT*

A tous qui ont contribué à l'aboutissement de ces travaux

To all those who made this work possible

Ce n'est pas la fin.
Ce n'est même pas le commencement de la fin
Mais, c'est peut-être la fin du commencement.

Winston Churchill

Remerciements

Les travaux présentés dans ce mémoire ont été effectués au Laboratoire d'Analyse et d'Architecture des Systèmes du Centre National de la Recherche Scientifique (LAAS-CNRS), dirigé successivement depuis mon entrée par Messieurs Malik GHALLAB et Raja CHATILA, à qui je souhaite exprimer mes remerciements pour leur accueil.

Je tiens à remercier également Monsieur Jean-Pierre COURTIAT et Monsieur François VERNADAT responsables du groupe Outils et Logiciels pour la Communication (OLC), pour m'avoir permis de réaliser ces travaux au sein de leur équipe.

Je suis également très reconnaissant pour le temps accordé par l'ensemble des membres du jury de ma thèse et pour leurs remarques constructives :

- Monsieur Christian FRABOUL, Professeur à l'Institut National Polytechnique de Toulouse
- Monsieur Francis LEPAGE, Professeur à l'Université Henri Poincaré, Nancy
- Abdelhamid MELLOUK, Maître des Conférences à l'Université de Paris 12
- Olivier DUGEON, Chercheur Expert Senior à France Telecom R&D, Lannion
- Michel DIAZ, Directeur de Recherche au LAAS-CNRS, Toulouse
- Christophe CHASSOT, Professeur à l'Institut National des Sciences Appliquées, Toulouse
- Laurent BARESSE, Chef de projet – Architecte, à AKKA Informatique & Systèmes Sud, Toulouse

Je tiens également à témoigner toute ma gratitude à Messieurs Francis LEPAGE et Abdelhamid MELLOUK qui m'ont fait l'honneur d'accepter la tâche de rapporter sur ces travaux. Je remercie tout particulièrement à Christian FRABOUL, président du jury, pour ses commentaires ainsi que son soutien pendant les années passées à l'ENSEEIHT en tant qu'élève ingénieur au Département des Télécommunications et Réseaux et Mastère Recherche (DEA Réseaux et Télécommunications).

J'exprime ma profonde reconnaissance à Monsieur Michel DIAZ, qui a dirigé cette thèse, pour m'avoir fait profiter de son expérience, pour ses conseils avisés et les réflexions que nous avons pu mener tout au long de ces années. Je lui suis également reconnaissant pour la confiance qu'il m'a témoignée et l'apport tant sur le plan professionnel que sur le plan personnel.

Je souhaite aussi vivement remercier Christophe CHASSOT, codirecteur de thèse, pour ses remarques pertinentes sur mon travail, ses nombreux encouragements et sa relecture de ce mémoire. Je lui remercie également de m'avoir offert l'opportunité de découvrir le monde de la recherche à travers mon stage de DEA.

Les travaux développés dans cette thèse ont effectués essentiellement dans le cadre du projet européen EuQoS (End-to-end Quality of Service support over heterogeneous networks). Je tiens à remercier l'ensemble des acteurs du projet, avec qui j'ai réellement apprécié

travailler. En particulier je remercie les équipes de l'Université de Coimbra (Luis CORDEIRO), Telefonica I&D (Marian CALLEJO), Silogic-groupe AKKA (Laurent BARESSE et Jean-Philippe DARMET), l'Université de Varsovie (Jarek SLIWINSKI) et l'Université de Bern (Marc BROGLE). Je remercie également Roberto WILIRICH, chercheur à l'Université Fédérale de Santa Catarina (Brésil) et Mathieu GINESTE (doctorant au LAAS-CNRS) pour leur support dans la réalisation des expérimentations du projet.

Je remercie vivement les personnes qui ont contribué directement à l'aboutissement de ces travaux. Tout d'abord, je tiens à remercier Guillaume AURIOL (ancien doctorant du groupe OLC du LAAS-CNRS), pour ses conseils et son support au début de mon séjour au LAAS. Je remercie Philippe OWEZARSKI pour son soutien, en particulier pour la mise en place de la plate-forme d'expérimentation utilisée pour la validation des propositions apportées par cette thèse. Je tiens à remercier Nicolas Van WAMBEKE (aussi appelé Agent 19.17) et Eraldo DA SILVA pour les travaux menés conjointement. Je remercie également les stagiaires que j'ai co-encadrés avec mes directeurs de thèse : Frederic FOK et Vincent GONIN.

Mes remerciements vont également à tous les membres du groupe OLC, permanents, doctorants et stagiaires pour leur accueil et bonne humeur. En particulier, je remercie mes collègues avec qui j'ai partagé un bureau (Khalil, André, Guillaume, Francesco, Nicolas, Ion, Silvia, Najla) pour l'ambiance amicale et les discutions eues (d'un niveau intellectuel élevé « en fait ») et dont un tableau blanc garde les traces. Merci également à la XB-Team (Fred, Baptiste, Pascal, Thierry, Momo, Ihsane) pour les moments de détente partagés dans les après-midi de travail, à Slim, Karim, Momo, Jorge, François pour les activités sportives effectuées ensemble.

Mes remerciements s'adressent également à Gina pour sa disponibilité, sa gentillesse et son aide précieux dans les préparatifs des tâches administratives.

Je remercie également les doctorants et autres membres des différents services techniques et administratifs (en particulier le service Informatique et Instrumentation) du LAAS-CNRS et les collègues de l'ENSICA qui m'ont permis de travailler dans d'excellentes conditions. Je salue en particulier les membres de l'équipe de football du LAAS-CNRS et les amis du groupe Tolérance aux fautes et Sûreté de Fonctionnement informatique. Merci encore à tous ceux qui m'ont accompagné et soutenu au cours de ces dernières années : ma famille, mes nombreux amis de Toulouse et d'ailleurs.

Enfin je pense très fort à une personne qui m'est très chère et qui a partagé avec moi ces dernières années étant mon soutien le plus efficace, Ana. Je ne lui remercierai jamais assez pour son soutien sans faille, sa patience et sa compréhension.

Table de matières

Introduction

Contexte

Ces dernières années, les évolutions technologiques conjointes de l'informatique et des télécommunications ont conduit à une modification profonde du paysage de la communication sur Internet :

- Les types de trafic et d'applications distribuées ont évolué passant d'applications textuelles de type transfert de fichiers ou échange de mail entre utilisateurs et serveurs fixes, à des applications multimédia (audio, vidéo) temps-réel, distribuées, coopératives ou mobiles (voix sur IP, vidéo à la demande, visioconférence, jeux interactifs, etc.). Ces applications présentent de nouveaux besoins en qualités de service (QoS) exprimables notamment en termes de bande passante garantie ou de délai de transit borné.
- Parallèlement, l'Internet est devenu la solution d'interconnexion de toutes les technologies réseaux (fixes ou mobiles, à échelle locale ou grande distance), et sa gestion est désormais assurée par de nombreux opérateurs appliquant de façon indépendante des politiques de routage, de sécurité ou de gestion des ressources. L'Internet apparaît donc aujourd'hui comme une interconnexion réseaux multiples qui s'appuient sur des technologies hétérogènes. Ces réseaux sont gérés dans le cadre de domaines indépendants vis à vis (en particulier) de la gestion de la qualité de service offerte sur les transferts des données de leurs clients.

Problématique

Conçu à la base pour des applications sans contraintes de débit ni de délai sur le transfert des données, le service offert par l'Internet (au niveau IP), connu sous le nom de *best-effort*, ne permet pas de prendre en compte la QoS requise par les nouvelles applications. Deux modèles précurseurs (IntServ et DiffServ) ont été proposés par l'IETF pour que de nouveaux services soient offerts.

Le modèle DiffServ, seul envisageable à grande échelle, laisse cependant ouverts deux problèmes importants, qu'il est nécessaire de résoudre pour offrir des garanties de QoS de bout en bout :

- le premier problème, qui concerne le provisionnement, est relatif au dimensionnement des ressources de chaque domaine, qu'il s'agit d'adapter aux besoins des clients potentiels.
- le second problème est relatif à la disponibilité des ressources sur le chemin de donnée ; sa solution nécessite qu'un contrôle d'admission (CAC) soit mis en place au sein de chaque domaine.

A l'échelle de plusieurs domaines, le provisionnement et le CAC sont plus difficiles à mettre en œuvre car :

- les domaines traversés par les données n'offrent pas les mêmes performances et le provisionnement doit tenir compte des caractéristiques des services sur chaque domaine ;

- le CAC doit être effectué sur chaque domaine et sur les liens inter-domaine pour assurer la disponibilité des ressources de bout en bout ;
- enfin, provisionnement et CAC nécessitent l'échange de données de contrôle tout au long du chemin emprunté par les données. Il est donc nécessaire de définir les protocoles d'échanges de ces données définissant ce qu'on appelle la signalisation intra ou inter-domaines.

Contributions

Les travaux décrits dans ce mémoire s'inscrivent dans cette problématique de la gestion de la QoS dans l'Internet multi-domaine et multi-technologie. Ils visent à répondre au besoin de maîtrise de la QoS, incluant la signalisation inter-domaine, qui couplée au provisionnement et au CAC permettent d'offrir des garanties de QoS de bout en bout aux nouvelles applications distribuées dans l'Internet.

Nous détaillons la conception, la spécification, l'implémentation et la validation d'une architecture de signalisation pour la QoS dans un environnement Internet multi-domaine hétérogène. Plus précisément, nos contributions portent sur :

- la proposition d'une architecture de signalisation inter-domaine qui a pour objectif d'installer et maitriser une QoS de bout-en-bout ; ;
- la proposition d'un modèle de provisionnement à la demande basé sur la signalisation précédente qui vise la découverte et la sélection automatique des services disponibles le long du chemin de données ;
- une étude pour l'extension de notre signalisation dans un environnement mobile ;
- l'adaptation et l'intégration de nos propositions dans le cadre défini par le groupe NSIS (Next Step In Signaling) de l'IETF;
- l'intégration de nos propositions dans l'architecture générale proposée dans le cadre du projet européen EuQoS ;
- l'implémentation et le déploiement de nos propositions sur des plateformes réelles, en particulier à échelle européenne dans le cadre du projet EuQoS ;
- des expérimentations et des mesures de performances visant à valider le bien fondé de nos propositions.

La solution soutenue repose sur l'hypothèse de l'existence de plusieurs classes de services (au sens DiffServ) en plus du service best-effort traditionnel sur chaque domaine. A l'intérieur de chaque domaine, les ressources sont supposées être gérées de manière indépendante et l'administration est déléguée à une entité logique, qui possède la connaissance des politiques internes, de la disponibilité des ressources, et qui réalise un contrôle d'admission basé sur ces politiques.

La maitrise de la QoS de bout en bout s'appuie sur un protocole de signalisation inter-domaine, laissant libre aux administrateurs le choix de l'implémentation d'une solution intra-domaine. Par ailleurs, nous prenons en compte un principe fondamental des réseaux de nouvelle génération, consistant en la séparation du plan de service (description des services en termes de composants logiciels, de leur composition et de leur représentation) du plan de contrôle (signalisation mise en place pour la gestion et la maintenance du réseau).

Plan du mémoire

Outre l'introduction, ce mémoire s'articule autour de quatre chapitres :

- Le chapitre 1 présente un état de l'art des propositions récentes qui visent à garantir une QoS dans l'Internet. Il donne un aperçu des difficultés liées à l'hétérogénéité d'un environnement multi-domaine. Nous introduisons les notions essentielles liées à la QoS ainsi que les perspectives des réseaux de nouvelle génération. Un état de l'art détaillé de la signalisation dans l'Internet est finalement fourni ainsi que le positionnement de nos travaux.
- Le chapitre 2 développe les contributions principales de cette thèse à savoir : une architecture de signalisation inter-domaine pour la QoS intégrée dans une architecture de communication, une proposition d'adaptation du protocole NSIS standardisé à l'IETF pour les domaines à QoS administrés par des entités spécifiques et une proposition de provisionnement dynamique des ressources qui repose sur la signalisation précédente.
- Dans le chapitre 3, nous présentons l'instanciation de notre proposition dans le cadre du projet européen EuQoS. Nous décrivons l'architecture générale du projet, l'implémentation des protocoles que nous avons effectuée, ainsi que leur intégration à cette architecture.
- Le chapitre 4 décrit les tests et les mesures de validation. Ces tests ont été réalisés d'une part sur une plate-forme d'expérimentation du LAAS-CNRS, et d'autre part sur un réseau de test européen (via le réseau GEANT) impliquant les différents partenaires du projet EuQoS.
- En conclusion générale, nous résumons les contributions de nos travaux et nous dégageons les perspectives de cette thèse.

1. Etat de l'art sur la gestion de la qualité de service dans les réseaux de nouvelle génération

Dans un premier temps, ce chapitre introduit les concepts généraux liés à la qualité de service (section 1.1). Nous présentons ensuite les caractéristiques relatives à la technologie sous jacente, au routage et au niveau transport de l'Internet (1.2). La section 1.3 présente les modèles précurseurs conçus pour offrir des garanties de QoS, à savoir IntServ et DiffServ. Par la suite (sections 1.4 et 1.5), nous décrivons les mécanismes associés à la QoS : le provisionnement des ressources, le contrôle d'admission, en détaillant la signalisation. La section 1.6 illustre les propositions d'architectures conceptuelles pour la mise en place de la QoS dans les réseaux de nouvelle génération ainsi que les projets de recherche internationaux menés ces dernières années.

1.1. Concepts fondamentaux sur la QoS

1.1.1. Evolutions de l'Internet

Ces dernières années, les évolutions conjointes dans les domaines de l'informatique et des télécommunications ont conduit à une transformation substantielle du monde des communications et par conséquence de l'Internet.

Le trafic Internet a profondément changé, passant de données essentiellement textuelles à des données qui manipulent plusieurs médias (texte, audio, vidéo). Ainsi, de nouveaux types d'applications, à la fois multimédia, multi utilisateurs et coopératives se sont développés. Ces applications présentent des caractéristiques et des contraintes nouvelles et de ce fait, elles demandent des services de communication autres que ceux offerts par l'Internet actuel. Comparativement aux applications *classiques*, ces nouvelles applications présentent des besoins exprimables en termes de délai borné ou de bande passante garantie, mais peuvent parfois tolérer des pertes de part la nature continue des média qu'elles manipulent. En quelques années, l'Internet, multi-technologie et multi-domaine (au sens opérateur du terme), est devenu une plate-forme incontournable pour le transfert de l'information. A titre illustratif, la Figure 1 montre l'évolution de l'Internet dans la dernière décennie, en nombre d'utilisateurs et en quantité du trafic véhiculé.

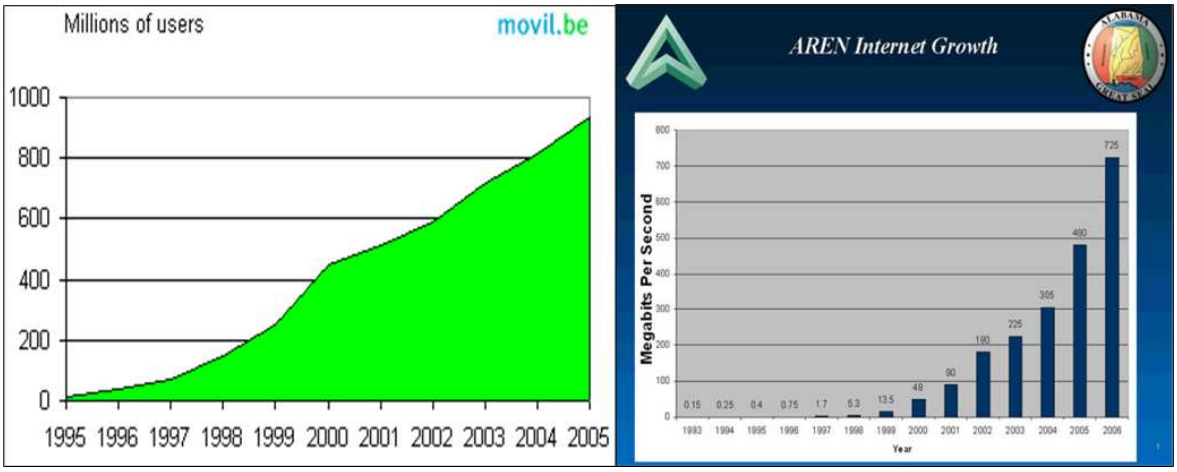


Figure 1 : Croissance de l'Internet

Cependant, l'architecture de l'Internet (TCP/IP), initialement conçue pour assurer le transfert fiable des données et sans déséquencement pour des applications sans contraintes particulières de délai ni de débit (transfert de fichiers, web statique, messagerie électronique), présente clairement une inadéquation au nouveau contexte applicatif. La volonté d'offrir de nouveaux services de communication et d'optimiser l'utilisation des ressources des réseaux sous jacents a motivé nombreux travaux de recherche, dont ceux présentés dans ce mémoire, dans le but d'offrir de nouvelles garanties de QoS.

1.1.2. Qualité de service (QoS) : définitions et terminologie

Différentes propositions ont été apportées pour définir la notion de QoS offerte par un réseau. La QoS peut être définie selon plusieurs critères : performance, disponibilité, fiabilité, sécurité, etc. Plusieurs définitions de la QoS ont été proposées par les divers organismes de standardisation ainsi que par la communauté Internet. La QoS a été définie par le standard ISO-9000 [ISO9000-00] comme « le degré pour lequel un ensemble de caractéristiques inhérentes satisfont les exigences». Un autre standard, ISO 8402 [ISO8402-00], définit la QoS comme « la totalité des caractéristiques d'une entité qui portent sur ses aptitudes à satisfaire les besoins applicatifs fixés ou implicites». La recommandation ITU-T X.902 [ITU-T-Rec.X.902-95] la définit comme « l'ensemble des qualités liées au comportement collectif d'un ou plusieurs objets ». La recommandation ITU-T E.800 [ITU-T-Rec.E.800-93] introduit le concept utilisateur / service par « l'effet collectif de la performance du service qui détermine le degré de satisfaction de l'utilisateur de service ». Particulièrement dans le domaine de l'informatique et des systèmes de communication, la QoS est définie comme « l'ensemble des caractéristiques qualitatives et quantitatives d'un système multimédia distribué nécessaires pour accomplir les fonctionnalités requises par une application » [Vogel95].

Par ailleurs, une grande majorité de la communauté scientifique définit la QoS suivant deux points de vue :

- le point de vue utilisateur : les caractéristiques quantitatives et qualitatives attendues et perçues d'un service ;
- le point de vue fournisseur : la qualité prévue et effectivement fournie.

Dans [Gozdecki03], les auteurs donnent une vue d'ensemble sur la terminologie QoS dans les réseaux IP et rappellent les définitions les plus utilisées dans la littérature, notamment les standards ITU (International Telecommunications Union), ETSI (European Telecommunications Standard Institute) et IETF (Internet Engineering Task Force). Le modèle général adopté de la terminologie est celui de [Hardy01] qui propose trois notions de QoS : intrinsèque, perçue et évaluée.

- la QoS intrinsèque résulte des choix techniques effectués dans le réseau ;
- la QoS perçue résulte de l'expérience des utilisateurs. Elle reflète donc une composante subjective. Une QoS avec les mêmes paramètres intrinsèques peut être perçue différemment par les divers utilisateurs.
- la QoS évaluée apparait quand le client continue ou non d'utiliser un service, ce qui dépend de plusieurs facteurs (prix, relation avec le fournisseur, service après vente etc.). Aucun des organismes ITU, ETSI ou IETF ne s'intéressent à ce type de QoS.

L'ITU et l'ETSI se focalisent principalement sur la QoS perçue, en introduisent la notion de « performance réseau » pour la partie technique. Les travaux de l'IETF visent la QoS intrinsèque, résultant de ses objectifs de développement de l'architecture Internet. La notion de QoS considérée par l'IETF est similaire à celle de performance réseau définie par l'ITU et l'ETSI.

1.1.3. Paramètres et métriques de QoS

Lorsque les besoins en QoS des utilisateurs sont exprimés dans un langage non-technique, la QoS intrinsèque est représentée par l'intermédiaire de paramètres. Dans les réseaux de paquets (notamment IP), les paramètres suivants sont les plus répandus :

- la bande passante, terme du domaine électronique utilisé par abus de langage, qui indique le débit d'information, exprimé généralement en octets par seconde (B/s) ou en bits par seconde (bit/s ou bps) ;
- le délai subi par les paquets, de bout en bout ou sur une portion du réseau, exprimé en millisecondes ;
- la gigue, qui exprime la variation du délai de transfert des paquets ;
- le taux de pertes, défini généralement comme le rapport entre le nombre de paquets perdus et le nombre total de paquets émis.

Les exigences des applications multimédia peuvent être spécifiées en termes de ces paramètres de base. Le Tableau 1 décrit les exigences proposées par la recommandation ITU-T G1010 [ITU-T-Rec.G.1000-01] pour les principaux types de données.

Medium	**Application**	**Degree of symmetry**	**Typical amount of data**	**Key performance parameters and target values**		
				One-way delay (Note)	**Delay variation**	**Information loss**
Data	Web-browsing – HTML	Primarily one-way	~10 KB	Preferred < 2 s /page Acceptable < 4 s /page	N.A.	Zero
Data	Bulk data transfer/retrieval	Primarily one-way	10 KB-10 MB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Transaction services – high priority e.g. e-commerce, ATM	Two-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	Command/control	Two-way	~ 1 KB	< 250 ms	N.A.	Zero
Data	Still image	One-way	< 100 KB	Preferred < 15 s Acceptable < 60 s	N.A.	Zero
Data	Interactive games	Two-way	< 1 KB	< 200 ms	N.A.	Zero
Data	Telnet	Two-way (asymmetric)	< 1 KB	< 200 ms	N.A.	Zero
Data	E-mail (server access)	Primarily one-way	< 10 KB	Preferred < 2 s Acceptable < 4 s	N.A.	Zero
Data	E-mail (server to server transfer)	Primarily one-way	< 10 KB	Can be several minutes	N.A.	Zero
Data	Fax ("real-time")	Primarily one-way	~ 10 KB	< 30 s/page	N.A.	$<10^{-6}$ BER
Data	Fax (store & forward)	Primarily one-way	~ 10 KB	Can be several minutes	N.A.	$<10^{-6}$ BER
Data	Low priority	Primarily	< 10 KB	< 30 s	N.A.	Zero

	transactions	one-way				
Data	Usenet	Primarily one-way	Can be 1 MB or more	Can be several minutes	N.A.	Zero

Tableau 1 : Cibles de performance pour les applications

D'autres caractéristiques peuvent être associées aux paramètres de QoS :

- la portée : de bout-en-bout ou locale ;
- la granularité : par flux, par session, par agrégat ;
- la direction : unidirectionnelle, bidirectionnelle ;
- la garantie : absolue, statistique.

Les paramètres de la QoS perçue sont plus difficiles à exprimer et quantifier. Nous pouvons en citer : le support pour le service, la sécurité, la disponibilité, le temps de connexion etc.

Les Classes de Service (Class of Service - CoS) représentent une modalité de gestion du trafic dans un réseau en regroupant les types de flux similaires. Les classes ainsi considérées seront traitées de manière unique en termes de paramètres de service. Les classes de services constituent une manière simple et évolutive pour gérer le trafic. Divers types de classes de services sont définis à différents niveaux de l'architecture Internet : application, réseau, etc.

Le groupe de travail « IP Performance Metrics » de l'IETF vise à définir des métriques standard de QoS, performance, fiabilité dans le transfert de données sur Internet. Ces métriques sont la connectivité, le délai et les pertes dans un seul sens et aller-retour, la variation du délai, les pertes, la réorganisation des paquets, la capacité des liens, etc.

La recommandation ITU-T Y.1541 [ITU-T-Rec.Y.1541-06] définit des paramètres similaires à ceux décrits par IETF, dont les principaux sont :

- IPTD (IP Packet Transfert Delay) : le délai de transfert d'un paquet ;
- IPDV (IP Packet Delay Variation) : la variation du délai entre deux paquets consécutifs;
- IPLR (IP Packet Loss Ratio): le rapport entre le nombre de paquets perdus sur l'ensemble des paquets transmis ;
- IPER (IP Packet Error Rate) : le rapport entre le nombre de paquets erronés sur le nombre total de paquets transmis.

La recommandation ITU-T Y.1541 défini les objectifs de performances réseaux pour différentes classes (Tableau 2).

Network performance parameter	**Nature of network performance objective**	**QoS Classes**					
		Class 0	**Class 1**	**Class 2**	**Class 3**	**Class 4**	**Class 5 Unspecified**
IPTD	Upper bound on the mean IPTD	100 ms	400 ms	100 ms	400 ms	1 s	U
IPDV	Upper bound on the $1 - 10^{-3}$ quantile of IPTD minus the minimum IPTD)	50 ms	50 ms	U	U	U	U
IPLR	Upper bound on the packet loss probability	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	1×10^{-3}	U

IPER	Upper bound	1×10^{-4}	U

Tableau 2 : Les performances des classes réseau Y.1541

1.2. Caractéristiques de l'Internet multi-domaine

1.2.1. Introduction

Par définition multi-technologie, l'Internet est aujourd'hui de fait multi-domaine, chaque fournisseur et administrateur assurant chacun de façon autonome la gestion de leur réseau et de leurs services. Cette indépendance renforce le caractère hétérogène de l'Internet, et accroit la difficulté de maîtriser la QoS pour des communications traversant plusieurs domaines.

Après avoir précisé la notion de domaine, cette section présente les caractéristiques de l'Internet multi-domaine relatives à ses technologies réseau support ainsi qu'à ses principaux protocoles de niveaux réseau et transport de l'architecture OSI[1] .

1.2.2. Notion de domaine et de système autonome (AS)

Un *domaine* représente un ensemble d'ordinateurs et équipements dans un réseau gérés de manière unique par une seule entité administrative. La RFC 1136 [Hares89] définit un domaine administratif comme un groupement d'hôtes, routeurs et réseaux dans l'Internet gérés par une seule organisation.

Un *système autonome* (AS : Autonomous System) est un ensemble de réseaux sous l'administration d'une seule entité qui a une politique de gestion (notamment de routage) commune et spécifique. Cette notion est donc administrative et l'indépendance de gestion concerne en premier lieu la politique de routage [Hawkinson96], mais s'applique aussi aux politiques de sécurité ou de gestion de la QoS. Notons qu'un numéro d'AS unique est attribué par l'IANA (Internet Assigned Numbers Authority) à chaque AS, son utilisation principale étant dans la mise en œuvre du routage inter-domaine.

Les systèmes autonomes se classent en trois catégories suivant leurs interconnexions et leurs opérations :

- Un AS *Multihome* est un AS qui a des connexions avec plusieurs autres AS, mais ne permet pas de transférer de trafic entre ces AS ;
- Un *AS stub* est un AS qui n'est connecté qu'à un seul autre AS. Le trafic est soit généré, soit terminé dans un tel AS ;
- Un *AS de transit* est un AS qui fournit des connexions aux différents réseaux séparés.

Dans la suite de ce mémoire, nous utiliserons de façon équivalente, les termes de « système autonome » et de « domaine ».

1.2.3. Technologies sous-jacentes

Pour mettre en place l'infrastructure nécessaire, les opérateurs s'appuient sur différentes technologies filaires et sans fil. Nous décrivons brièvement dans les paragraphes suivants celles que nous avons utilisées dans nos travaux.

[1] Modèle OSI («Interconnexion de systèmes ouverts») d'interconnexion en réseau des systèmes ouverts est un modèle de communications entre ordinateurs proposé par l'ISO (Organisation internationale de normalisation)

1.2.3.1. LAN, Ethernet

Ethernet est un standard de transmission de données pour un réseau local, normalisé sous le nom d'IEEE 802.3 et classé dans la couche liaison de données du modèle OSI (bien qu'il implémente des fonctionnalités de la couche physique). Toutes les machines du réseau Ethernet sont connectées à une même ligne logique de communication, toute information envoyée par un équipement étant reçue par tous les autres, même si cette information était destinée à une seule machine. Les postes connectés sur un réseau Ethernet doivent donc filtrer ce qui leur est destiné ou non.

1.2.3.2. xDSL

Le terme DSL signifie Digital Subscriber Line (ligne numérique d'abonné) et regroupe l'ensemble des technologies mises en place pour un transport numérique de l'information sur une simple ligne de raccordement téléphonique. L'idée est de mettre à profit la partie non utilisée du spectre d'une ligne téléphonique (dont la voix n'utilise qu'une partie) pour transporter des données. Les technologies xDSL sont divisées en deux grandes familles, suivant le rapport entre bande passante ascendante, de l'utilisateur vers le réseau, (*upload*) et bande passante descendante, du réseau vers l'utilisateur, (*download*) : celle utilisant une transmission symétrique (SDSL) et celle utilisant une transmission asymétrique (ADSL).

1.2.3.3. Wi-Fi

Wi-Fi est une technologie sans fil normalisé IEEE 802.11 dont le nom est promulgué par Wi-Fi Alliance qui veille à l'interopérabilité des équipements certifiés. La norme définit les deux couches basses du modèle OSI (physique et liaison de données) en utilisant des ondes radio sur la fréquence de 2.4 GHz. Conçu pour les réseaux locaux sans fil (WLAN), cette norme permet des communications entre différents dispositifs en hauts débits (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g et jusqu'à 540 Mbit/s théoriques pour le futur 802.11n). Il existe deux modes de connexion et d'exploitation dans un réseau local sans fil : le mode infrastructure (les postes équipés d'une carte Wi-Fi sont connectés entre eux via un ou plusieurs Points d'Accès - AP- ou hotspots qui agissent comme des concentrateurs), et le mode ad-hoc (connexion directe entre les équipements Wi-Fi, sans utiliser un matériel tiers).

1.2.3.4. Satellite

Les systèmes satellitaires sont déployés de plus en plus dans des zones ou l'infrastructure de communication est peu développée, peu habitées ou bien difficile à couvrir par les autres technologies. Grace à ses avantages (couverture globale, flexibilité d'utilisation de la bande passante, déploiement pratique des services), l'intégration du satellite comme composant d'un Internet s'appuyant sur des réseaux physiques hétérogènes a une légitimité. Les inconvénients principaux sont le coût de départ relativement élevé, la fiabilité réduite en cas de contexte exceptionnel (interférences, conditions climatiques) et le délai de propagation de l'ordre de 600 ms aller-retour. Les débits sur un lien satellitaire peuvent aller jusqu'à 100 Mbps en réception et 2 Mbps en émission.

1.2.4. Le routage dans l'Internet

Le routage représente le processus qui permet de trouver le chemin que doit emprunter une information sur un réseau afin de parvenir à sa destination. Le routage est un mécanisme vital pour Internet car il permet de passer les paquets de proche en proche pour arriver à la destination. Chaque dispositif intermédiaire, appelé routeur, possède une table de routage (remplie statiquement ou le plus souvent dynamiquement) qui est utilisée pour retrouver le meilleur chemin vers la destination. Nous distinguons deux types de protocoles de routage :

- *Interior Gateway Protocol* (IGP), utilisé à l'intérieur d'un système autonome ;
- *Exterior Gateway Protocol* (EGP), utilisé pour échanger des informations de routage entre systèmes autonomes.

1.2.4.1. Routage intra-domaine

Les protocoles de type IGP se divisent en deux catégories : à vecteur de distance (distance-vector) et à état de lien (link-state). Les protocoles à vecteur de distance utilisent l'algorithme de Bellman-Ford ([Bellman58] et [Ford62]) et les routeurs n'ont pas la connaissance de la topologie complète du réseau. D'autre part, pour les protocoles à état de lien, chaque routeur possède la cartographie complète du réseau, la meilleure route étant calculée localement.

1.2.4.1.1. RIP

Routing Information Protocol (RIP) est un protocole à vecteur de distance qui utilise comme métrique le nombre de sauts. Défini initialement au sein de l'IETF dans la [Hedrick88], il a été redéfini dans les nouvelles versions : RIPv2 [Malkin98] ou RIPng [Malkin97]. Il présente quelques inconvénients (temps de convergence, passage à l'échelle, nombre maximal de saut) qui font que RIP est remplacé soit par EIGRP (Enhanced Interior Gateway Routing Protocol, propriétaire CISCO), soit par des protocoles à état de lien (OSPF ou IS-IS).

1.2.4.1.2. OSPF

OSPF (Open Shortest Path First) est un protocole de routage pour IP issu des travaux du groupe IGP de l'IETF (la version standardisé la plus récente est RFC 2328 [Moy98]). Un réseau OSPF est hiérarchique et il peut être divisé en zones, connectées à une zone centrale (Area 0). Il utilise une variante de l'algorithme de Dijkstra [Dijkstra59] pour calculer la route optimale à partir de l'arbre de plus court chemin. Chaque routeur garde une base de données, mise à jour périodiquement, qui contient la topologie du réseau. Cette base, appelée LSDB (Link State DataBase) est mise à jour périodiquement sur tous les routeurs. La dernière version d'OSPF est OSPFv3 [Coltun99] et présente la compatibilité avec IPv6.

1.2.4.1.3. IS-IS

IS-IS (Intermediate System to Intermediate System), développé par Digital Equipement Corporation, est également un protocole IGP à état de lien standardisé par l'OSI [ISO10589]. Etendu pour l'Internet IP, il a été intégré par l'IETF [Oran90] et [Callon90]. Plusieurs entités coexistent dans un réseau IS-IS : les systèmes terminaux (End System), les systèmes intermédiaires (Intermediate System – les routeurs), les zones (ensemble de routeurs) et les domaines (ensemble de zones). Par rapport à l'OSPF qui est utilisé plutôt dans les réseaux des grandes entreprises, IS-IS est adopté particulièrement par les fournisseurs.

1.2.4.2. Routage inter-domaine

Les protocoles de type EGP permettent d'échanger des informations de connectivité et d'accessibilité des réseaux dans l'Internet entre systèmes autonomes (AS). Actuellement, le seul représentant réellement déployé de cette famille est le protocole BGP (Border Gateway Protocol).

1.2.4.2.1. BGP

BGP est le protocole utilisé pour échanger des informations de routage entre les systèmes autonomes. La version actuellement standardisé par l'IETF ([Perkins07]) est BGPv4. BGP supporte l'agrégation pour limiter les tables de routage et aussi le routage sans classe (Classless

Inter-Domain Routing - CIDR). Les métriques ne sont pas les mêmes que celles utilisée en IGP, mais elles dépendent de la route, des politiques des opérateurs ou bien des diverses règles réseau.

Les voisins BGP sont les routeurs avec lesquels une session BGP est établie. Ils sont configurés manuellement et la connexion utilise le protocole TCP sur le numéro de port 179. Deux entités BGP échangent des messages pour ouvrir et maintenir les paramètres d'une session. BGP ne nécessite pas de mise à jour périodique des tables de routage ; des messages sont envoyés lorsque la table de routage change. En revanche, un routeur BGP doit retenir la totalité des tables de routage courantes de tous ses pairs durant le temps de la connexion. BGP est constitué de deux parties : quand il est exécuté entre deux routeurs au sein du même système autonome, il s'agit d'IBGP (Interior BGP) ; d'autre part, EBGP (Exterior BGP) est le nom donné quand la session est établie entre système autonomes différents (voir Figure 3).

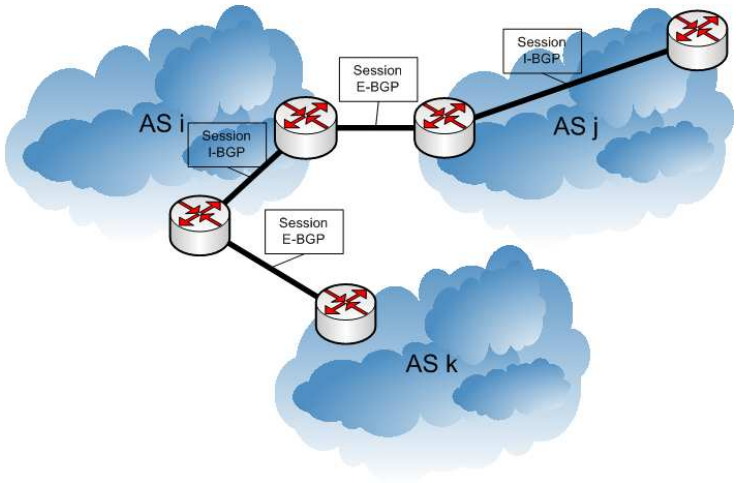


Figure 2 : Protocole BGP

Les paragraphes précédents permettent de souligner un point important du déploiement des protocoles adaptés au multi-domaine. En effet, BGP est déployé indépendamment de l'IGP choisi au niveau des domaines.

1.2.4.3. Routage à QoS

Le routage à QoS (QoS Routing) est une des pistes de recherche dans le cadre de l'IETF. L'objectif principal ce ces travaux et d'intégrer les métriques de la QoS et les critères de choix d'un chemin dans les différents protocoles de routage existants. La RFC 2386 [Crawley98] évoque trois évolutions envisageables des protocoles de routage : (1) supporter différentes classes de service, (2) éviter les changements fréquents de routes et (3) profiter de l'existence de routes alternatives.

Le routage à QoS détermine les routes à la fois par la connaissance des ressources disponibles dans le réseau et les demandes en QoS d'un flux. Les protocoles de routage à QoS présentent des mécanismes dynamiques qui ajoutent des critères de QoS au processus de choix des routes. Les techniques de routage à QoS sont utilisées conjointement avec des mécanismes de réservation de ressources, contrôle d'admission ou ingénierie de trafic.

[Boucadair05] présente une proposition de routage inter-domaine à QoS, Q-BGP (QoS Enhanced BGP). Ce protocole repose sur la version de base de BGP pour échanger des informations sur les performances relatives à la QoS. C'est une version enrichie de ce protocole qui a été retenue dans l'architecture du projet EuQoS présenté dans le chapitre 3, dans lequel nous la présentons plus en détail.

1.2.4.4. MPLS et Traffic Engineering

L'acheminement traditionnel des paquets dans les routeurs s'effectue suivant l'adresse IP de destination contenue dans l'entête des paquets IP. Dans un souci de simplification et de rapidité du routage, un groupe de travail à l'IETF a proposé un nouveau protocole : MPLS (Multi Protocol Label Switching) [Rosen01]. MPLS est un protocole de commutation des paquets (basé sur un protocole CISCO de commutation de tags), qui utilise des labels (étiquettes) pour acheminer les paquets.

Un label de 20 octets identifie le trafic à l'intérieur d'un réseau MPLS. Ce label est associé à un groupe de paquets acheminés de la même manière, sur le même chemin et qui suivent le même traitement, ce qui constitue une classe spécifique de trafic appelé « Forwarding Equivalence Class » (FEC). Une FEC correspond à une plage d'adresses destination, à un certain type de trafic, une priorité etc. Le mécanisme de commutation de labels doit être associé à un contrôle d'admission pour garantir un niveau de qualité bien défini. Les frontières d'un réseau MPLS sont régies par des routeurs spéciaux appelés Label Edge Routers (LER). Les LERs appliquent un label aux paquets entrants dans le réseau et l'enlèvent à la sortie. Les routeurs du cœur d'un réseau MPLS, appelés Label Switch Routers (LSR) commutent les paquets suivant les labels et le chemin ainsi suivi porte le nom de Label Switched Path (LSP). La Figure 4 présente un exemple de domaine MPLS :

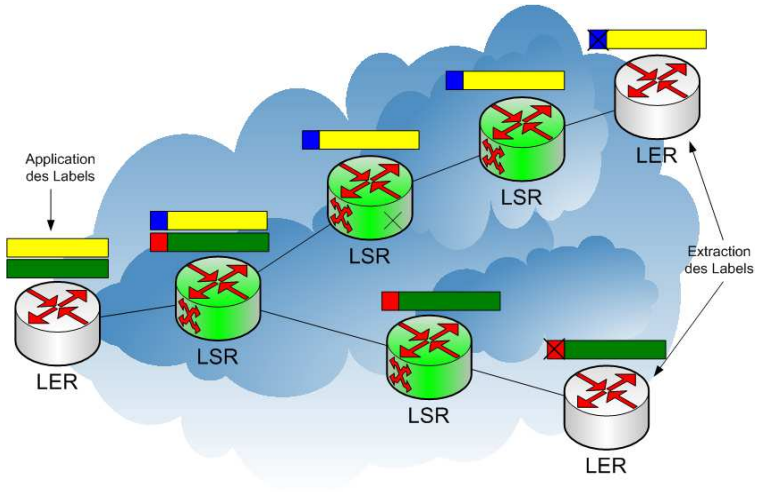


Figure 3 : Réseau MPLS

MPLS présente l'avantage de différencier les divers flux de données (association des étiquettes différentes) ce qui le rend très attractif pour les fournisseurs et son utilisation est répandue principalement dans le cœur du réseau.

MPLS est utilisé conjointement avec des mécanismes d'ingénierie de trafic (Traffic Engineering - TE). L'ingénierie de trafic définit l'ensemble des techniques appliquées afin de contrôler et de réguler la distribution du trafic dans un réseau. L'objectif des opérateurs est d'optimiser l'utilisation des ressources (bande passante) afin de mieux dimensionner le réseau, d'éviter les congestions, de récupérer après une disfonctionnement etc.

1.2.5. Les protocoles de Transport dans l'Internet

Pour répondre aux exigences des nouvelles applications (ex. multimédia et temps réel), deux approches d'optimisation des protocoles sont envisagées dans les différents travaux de recherche :

- la première approche consiste à s'adapter, au niveau des couches hautes (Transport, Application) de l'architecture TCP/IP, à la variabilité des ressources du réseau ;
- la deuxième approche propose une révision de l'architecture TCP/IP en vue de maîtriser les problèmes de bande-passante et de délai.

Une des pistes de recherche explorées a été de repousser la complexité vers les extrémités de la communication (terminaux utilisateurs) et par conséquent d'introduire des mécanismes d'adaptation dans les couches hautes de l'architecture Internet : application et transport. Ces solutions visent à répondre aux exigences des applications et à s'adapter aux caractéristiques (type des flux, contraintes temporelles, fiabilité). Notons que ces solutions n'offrent aucune garantie, ni temporelle ni de débit, sur le transfert de données.

De nombreux travaux se sont attachés à proposer de nouveaux protocoles et mécanismes de niveau transport. Les protocoles initiales (Transmission Control Protocol - TCP et User Datagram Protocol - UDP) présentent des limites conceptuelles qui les rendent inadéquats aux applications temps réel. Les mécanismes de reprise de perte et le contrôle de congestion de TCP engendrent une augmentation non maitrisée du délai et aussi une variation importante du débit d'émission. D'autre part, UDP ne met en œuvre ni des mécanismes de gestion de l'ordre ni de la fiabilité et de ce fait ne répond pas aux besoins des applications multimédia.

SCTP (Stream Control Transmission Protocol [Stewart07] et DCCP (Datagram Congestion Control Protocol [Kohler06]) sont actuellement développés à l'IETF, pour répondre aux limitations ou enrichir les fonctionnalités des protocoles UDP et TCP.

Le protocole ETP (Enhanced Transport Protocol [Exposito03]), conçu au LAAS-CNRS, vise à permettre l'assemblage dynamique de *micro-protocoles*, dédiés chacun à une fonction spécifique (contrôle des pertes partiellement fiable, contrôle de congestion TCP-friendly [Floyd06], …). Il permet ainsi d'offrir les services de transport les plus adaptés aux besoins des applications et au contexte réseau sous-jacent. ETP a été instancié dans EuQoS de sorte à fournir un ensemble de services EQ-ETP adaptés aux classes de services réseau considérées dans EuQoS, dans le but d'optimiser la QoS des transferts de données.

Sur ces bases, la section suivante présente les modèles précurseurs de gestion de la QoS qui ont été proposés pour l'Internet, en soulignant les limites et les problèmes ouverts.

1.3. Modèles précurseurs pour la garantie de la QoS

L'IETF (Internet Engineering Task Force) a créé successivement deux groupes de travail, IntServ et DiffServ pour l'étude et la proposition des nouveaux services IP. Ces propositions essayent de répondre (en tout ou partie) aux principaux problèmes comme le provisionnement des services, la signalisation nécessaire, etc.

1.3.1. IntServ

1.3.1.1. Présentation générale

L'IETF a d'abord créé le groupe de travail « Integrated Services » (IntServ). Ce groupe a introduit une extension de l'architecture Internet composée d'une part d'un modèle de service, appelé modèle IS (Integrated Services) et d'autre part d'un cadre d'implémentation pour la mise en œuvre de ce modèle [Braden94]. Deux types de service ont été proposés pour répondre aux besoins des applications temps réel (garanti et assuré).

Pour la mise en place de ces services, une réservation des ressources est nécessaire dans tous les routeurs au long du chemin de données. Cette procédure est réalisée par l'intermédiaire d'un protocole de signalisation appelé RSVP (Resource ReSerVation Protocol), présenté dans la section 1.5.3.1.1.

Le modèle IntServ définit une architecture capable de prendre en charge la qualité de service sans toucher au protocole IP. Dans un réseau IntServ, un flux de données identifie un ensemble de paquets qui reçoivent une certaine qualité de service et qui est défini par une « session » déterminée par les adresses IP destination, le protocole de transport et les numéros de port. Chaque flux peut être servi par différentes classes de service implantées dans les routeurs traversés. Le trafic best-effort ne reçoit aucun traitement spécifique dans les routeurs, et les paquets sont acheminés suivant la disponibilité des ressources.

Le cadre d'implémentation proposé par le groupe IntServ repose sur quatre fonctions principales, l'ordonnancement des paquets, le contrôle d'admission, la classification des paquets et la signalisation :

- l'ordonnanceur est en charge de l'acheminement des différents paquets ;
- le « classifieur » réalise une correspondance avec le niveau de QoS requis pour les paquets appartenant à différents flux ayant comme objectif le contrôle de trafic ;
- le contrôle d'admission comprend la décision d'accepter ou de rejeter un nouveau flux par rapport à la QoS demandée. Cette QoS est spécifiée par un ensemble de paramètres appelés FlowSpec. On distingue deux parties dans le FlowSpec : le TSPEC (spécification du trafic) et le RSPEC (spécification de la requête, les garanties nécessaires pour le flux). Ces informations sont transportées par le protocole de réservation RSVP qui a pour but de créer et maintenir les états spécifiques pour chaque flux dans les hôtes terminaux et dans tous les routeurs au long du chemin ;
- la signalisation mise en place permet de réserver les ressources le long du chemin de données dans les routeurs.

Dans le cadre d'IntServ, deux nouvelles classes de service en plus du best-effort ont été définies : Guaranteed Service (GS) [Shenker02] et Controlled Load (CL) [Wroklawski97a].

- GS propose un service exprimable de manière quantitative en termes de bande passante et de délai maximal. Il garantit que tous les paquets arriveront avec un délai maximal et ils ne sont pas perdus dans les files d'attentes en cas de congestion (si le flux respecte les paramètres réservés). Il est à remarquer que GS n'offre aucune garantie sur le délai moyen, mais seulement sur le délai maximal. Ce type de service se prête à des applications temps réel avec des contraintes fortes sur le délai de transmission.
- CL propose un service de bout-en-bout exprimable de manière qualitative en terme de bande passante : il garantit un transfert de données équivalent à un réseau peu chargé, non-congestionné. Les garanties offertes par le CL sont d'ordre statistique et les applications qui utilisent ce service doivent fournir une estimation du trafic qu'elles vont générer (dans le TSPEC). Les applications susceptibles d'utiliser ce service sont sensibles aux conditions de surcharge du réseau qui entraine une dégradation sensible de la qualité.

Le niveau de QoS fourni par les classes de service est programmable pour chaque flux (per-flow) suivant les requêtes des applications. Ces requêtes sont passées aux routeurs en utilisant un protocole de réservation tel que RSVP. L'API[2] RSVP [Braden97] permet de préciser le

[2] Application Programming Interface (Interface de Programmation Applicative)

profil de trafic qui nécessite la réservation des ressources ainsi que le service IP requis (GS ou CL).

1.3.1.2. Limites des propositions IntServ

L'approche IntServ présente plusieurs limites importantes.

- Tous les routeurs au long du chemin ainsi que les systèmes terminaux doivent être capables de fournir des requêtes de QoS en utilisant le protocole RSVP. L'inconvénient principal de RSVP provient du fait qu'il oblige à maintenir des informations d'état sur chaque flux dans chaque nœud du chemin liant l'émetteur au récepteur. Lorsque le nombre d'usagers (flux) augmente, le nombre d'états devient conséquent, et le trafic est d'autant plus saturé que les rafraîchissements entre routeurs deviennent importants. Le maintien des états dans les routeurs ainsi que le contrôle d'admission augmentent les besoins en ressources et rajoutent de la complexité dans les nœuds du réseau. Cela nuit aux performances du système dans son ensemble. *C'est pourquoi IntServ est plus adapté à des réseaux de petite taille comme les réseaux locaux (LAN).*
- D'autre part, IntServ ignore la structure multi-domaine de l'Internet. L'existence de plusieurs domaines administrés indépendamment les uns des autres, impose une gestion locale de manière autonome vis-à-vis de leurs politiques internes, du routage, de la sécurité et bien sûr de la qualité de service différente qui devient difficile à déployer.

1.3.2. DiffServ

1.3.2.1. Présentation générale

Le modèle DiffServ [Blake98] a été conçu pour répondre aux limites d'IntServ. L'idée de base est de fournir une qualité de service non par flux, mais par classe de paquets IP tout en repoussant (le plus possible) la complexité du traitement en bordure du réseau afin de ne pas en surcharger le cœur. DiffServ définit la notion de « classe » comme un ensemble de paquets identiquement marqués. Afin d'éviter le problème du passage à l'échelle inhérent aux solutions IntServ, le choix a été fait de traiter un nombre limité de classes (agrégats).

Pour l'identification des classes, DiffServ définit un champ de remplacement dans l'en-tête IP, champ appelé DiffServ Code Point (DSCP) qui remplace les champs déjà existants : Type of Service (TOS) dans l'en-tête IP version 4 ou Traffic Class dans l'en-tête IP version 6. Plus exactement, seulement six bits sur 8 sont utilisés. Les deux autres bits (réservés) sont utilisés pour la notification explicite de la congestion.

Dans les paragraphes suivants, nous présentons d'abord deux autres notions importantes de la proposition DiffServ : la notion de domaine et la notion de contrat de service (SLA). Nous décrivons ensuite les principes généraux, de l'architecture DiffServ.

1.3.2.2. La notion de domaine DiffServ

Par définition, l'Internet est constitué d'une interconnexion de réseaux. Cependant, plusieurs de ces réseaux sont souvent rassemblés sous une même autorité administrative (par exemple dans les grandes entreprises, les centres de recherches, les universités, ...) et constituent un domaine. [Nichols98] désigne par domaine, un ensemble de nœuds (hôtes et routeurs) administrés de façon homogène.

Dans un domaine, on distingue les nœuds internes et les nœuds frontières : les premiers ne sont entourés que de nœuds appartenant au domaine alors que les seconds sont connectés à des

nœuds frontières d'autres domaines (Figure 4). Si on considère le sens de communication de la source vers la destination, les nœuds de frontières peuvent être d'entrée (ingress) dans le domaine ou de sortie (egress).

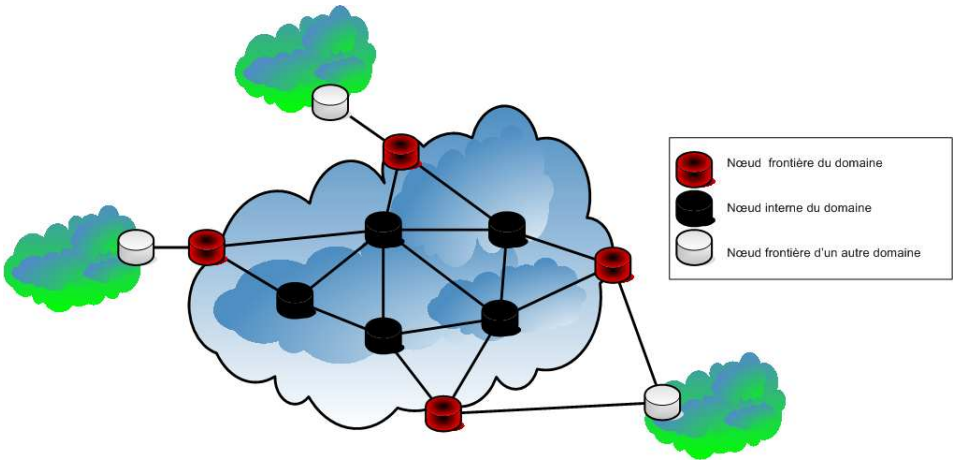


Figure 4 : Distinction des nœuds d'un domaine DiffServ

1.3.2.3. La notion de SLA (Service Level Agreement)

L'utilisation des services DiffServ implique pour le client la souscription d'un contrat avec le fournisseur des services : ce contrat s'appelle un Service Level Agreement (SLA).

Contrairement à ce qui se passe avec RSVP, ce contrat est signé avant toute connexion au réseau, et non à l'établissement d'une session (établir une session RSVP revient en effet à passer un contrat avec les routeurs intermédiaires, qui garantissent certaines propriétés du transport de données tant que le trafic respecte un certain profil). Les spécifications techniques du SLA sont contenues dans le SLS (Service Level Specification). Le SLA contient les informations suivantes :

- le trafic que l'utilisateur peut injecter dans le réseau fournisseur (en termes de volume de données, de débit moyen, d'hôtes source ou destination, …) ;
- les actions entreprises par le réseau en cas de dépassement de trafic (rejet, surtaxe, remise en forme du trafic) ;
- la QoS que le fournisseur s'engage à offrir au trafic généré ou reçu par l'utilisateur (ou les deux). Celle-ci peut s'exprimer notamment en termes de délai, de bande passante, de fiabilité ou de sécurité.

Pour le moment, seuls des contrats statiques, c'est-à-dire peu susceptibles de changer dans le temps, sont établis, la gestion des contrats dynamiques dont les caractéristiques varient rapidement étant plus complexe.

1.3.2.4. La notion de comportement (PHB : Per Hop Behavior)

Au sein d'un domaine DiffServ, tous les nœuds (hôtes et routeurs) d'un domaine implémentent les mêmes classes de service et les mêmes comportements ou Per Hop Behavior: PHB vis-à-vis des paquets des différentes classes. Un comportement inclut le routage, les politiques de service des paquets (notamment la priorité de passage ou de rejet en cas de congestion) et éventuellement la mise en forme du trafic entrant dans le domaine. Les nœuds internes ne doivent pas conserver d'états en mémoire (contrairement à la proposition IntServ) ; ils ne font que transmettre les paquets selon le comportement défini pour leur classe. Nous verrons dans les chapitres suivants qu'il est possible, sous couvert de certaines hypothèses concernant le

trafic global, de caractériser (au moins statistiquement) les services obtenus entre deux nœuds frontières. Les nœuds frontières se chargent de marquer les paquets selon le code réservé à chaque classe, comme nous allons le voir dans la partie suivante.

La RFC 2475 [Blake98] définit le PHB comme le comportement d'acheminement observable de l'extérieur qui s'applique aux données dans un nœud DiffServ. Le système marque les paquets conformément aux codes DSCP et tous les paquets ayant le même code seront agrégés et soumis au même traitement particulier.

Plusieurs PHB standard ont été définis :

- Le PHB par default (default PHB, défini en [Nichols98]) : spécifie que les paquets marqués avec la valeur DSCP « 000000 » utilisent le service « traditionnel » best-effort dans un nœud DiffServ. De plus, si un paquet arrive dans un nœud et son code DSCP ne correspond à aucun PHB, ce paquet recevra le PHB par default
- Assured Forwarding (AF) PHB (défini en [Heinanen99]) : établit une méthode pour laquelle l'agrégation détermine différents niveaux d'assurances sur l'acheminement des paquets. Quatre classes AF1, AF2, AF3, et AF4 ont été ainsi définies avec des différents niveaux de traitement (rejet) en cas de congestion du réseau.
- Expedited Forwarding (EF) PHB (défini en [Jacobson99]) : a pour but d'offrir un service robuste avec peu de pertes, avec gigue et délai petits et une bande passante garantie (service premium). Pour assurer l'efficacité du système, ce service devrait être réservé pour un certain type d'applications (critiques, multimédia, temps réel). La valeur recommandée pour le code DSCP EF PHB est '101110'.

1.3.2.5. La notion de Bandwidth Broker

La RFC 2638 [Nichols99] introduit la notion de Bandwidth Broker (BB), entité définie comme ayant la connaissance des politiques et de la disponibilité des ressources d'un domaine. De plus, il alloue la bande passante en tenant compte d'un ensemble de règles et stratégies. Il est à noter qu'un BB est en charge d'un seul domaine administratif (ou d'une portion de domaine). Pour avoir des garanties de QoS au long du chemin de données qui traverse plusieurs domaines, il est nécessaire d'avoir une communication entre les BBs adjacents ce qui permet de construire le chemin de bout-en-bout sur la base des SLA établis entre les domaines.

Plusieurs types d'architectures de déploiement ont été proposés pour les BBs [Schelen98], [Nichols99], [Terzis99], [Qbone01]. Elles peuvent être classées de la façon suivante :

- une seule entité est en charge de la gestion du domaine ;
- un BB est distribué entre plusieurs entités. Les tâches effectuées par ces entités peuvent être identiques ou hiérarchisée ;
- une structure hybride est également envisagée qui combine les avantages des deux architectures précédentes.

L'efficacité d'un BB dépend de l'interopérabilité de ses composants. Les fonctions sont distribuées horizontalement (entre tous les domaines impliqués sur le chemin de données) et verticalement (au sein de chaque domaine). A titre d'exemple, la Figure 5 illustre les principaux composants du BB proposé pour le QBone [QBone01] ; elle comporte :

- une interface d'accès pour les utilisateurs et l'administrateur, afin de gérer les différentes requêtes provenant de l'intérieur du domaine;
- un module qui réalise le contrôle d'admission ;
- des composants pour la communication intra et inter-domaine ;

- une base de données qui contient toutes les informations concernant la topologie du réseau, les contrats établis avec les clients et les domaines adjacents, les politiques, les ressources disponibles, les allocations actuelles, les informations relatives à l'authentification, l'autorisation, la comptabilité et la tarification ;
- les informations liées au routage ;
- un système de gestion de politiques et du réseau.

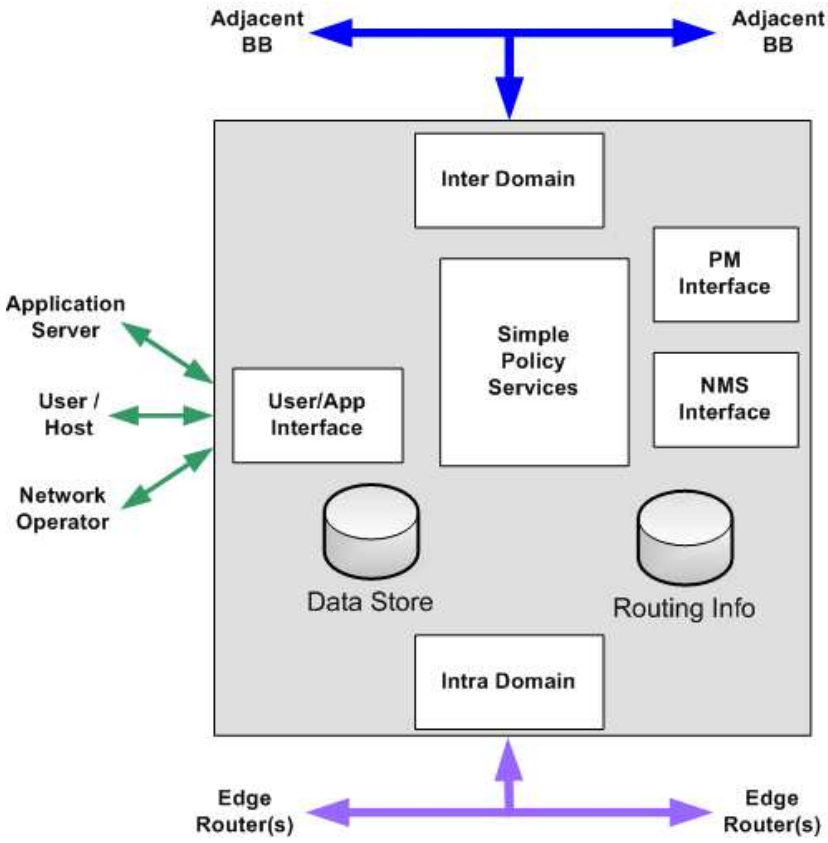


Figure 5 : Architecture du Bandwidth Broker propose pour le QBone

1.3.2.6. Problèmes ouverts

La proposition DiffServ est actuellement considérée comme la plus adaptée pour la gestion de la QoS dans l'Internet. Cependant, elle présente plusieurs problèmes (paramétrage des PHB, établissement des accords entre administrateurs des différents domaines, …). Le passage au multi-domaine (Figure 6) accroit les difficultés de gestion de la QoS pour plusieurs raisons :

- Dans un premier temps, le provisionnement est plus complexe, car il inclut aussi le dimensionnement des ressources de chaque domaine par rapport aux contrats SLA/SLS avec les domaines adjacents.
- Ensuite, le contrôle d'admission doit être prolongé sur les liens inter-domaines pour assurer la disponibilité des ressources de bout en bout.
- Finalement, les domaines de l'Internet étant hétérogènes, ils peuvent offrir des services différents. En conséquence, une signalisation multi-domaine doit être donc mise en place pour gérer la continuité de la qualité de service pour une communication traversant plusieurs domaines.

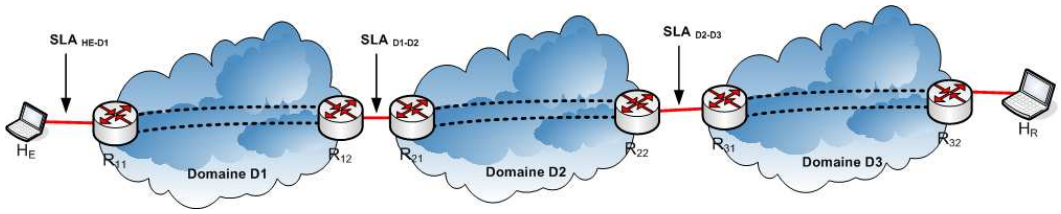


Figure 6 : Internet multi-domaine

Nous précisons ces difficultés et les besoins associés dans la section suivante.

1.4. Provisionnement et contrôle d'admission pour la QoS

1.4.1. Provisionnement des ressources pour la QoS

Le provisionnement de service consiste à accorder le dimensionnement des ressources du réseau en fonction des contrats établis avec les divers clients et du trafic véhiculé. On considère un service bien provisionné si le réseau est capable d'assurer le transfert de la communication d'un point d'entrée (souscription de contrat) vers un (ou plusieurs) point(s) de sortie dans les conditions spécifiées dans la souscription tout en respectant les performances annoncées. Le problème de provisionnement comporte deux parties :

- Dans le cas intra-domaine, le provisionnement consiste pour l'administrateur à définir l'infrastructure (les ressources) nécessaire pour la mise en œuvre des contrats de services avec les clients. Ces clients peuvent être des particuliers, des entreprises/universités ou bien d'autres fournisseurs. Nous précisons que nos travaux n'abordent pas cet aspect, le choix des mécanismes étant libre pour les administrateurs de domaines.
- La deuxième découle de la nature multi-domaine de l'Internet. Il est à noter que les domaines traversés par une communication n'offrent ni les même capacités, ni les même performances. Il est donc nécessaire de connaître les caractéristiques des services fournis par les domaines impliqués le long du chemin de données pour faire un choix de concaténation de services (un par domaine) sur le chemin suivi par les données, qui répond aux besoins en QoS.

L'objectif du provisionnement est d'ajuster le dimensionnement des ressources du réseau à partir des contrats souscrits avec les divers clients. Le provisionnement comporte deux aspects : mono-domaine (lié à la gestion des ressources internes à chaque domaine) et multi-domaine (lié à la découverte des services et au choix d'une concaténation qui satisfait les exigences du trafic). Nous présentons dans la section suivante les différentes approches pour répondre au problème de provisionnement.

1.4.1.1. Surprovisionnement

Une des solutions considérées pour assurer une qualité de services est le surprovisionnement. Une politique de surprovisionnement consiste à s'assurer que les capacités des liens sont supérieures au volume de trafic à écouler sur les liens. Dans le cas du mono-domaine, cette opération se traduit par un ajustement adopté par le fournisseur sur le surdimensionnement des ressources qui engendre la disponibilité des ressources. Pour le multi-domaine, le problème est plus complexe car il s'avère que le surdimensionnement n'est pas envisageable à cette échelle. Outre le fait que cette solution est très coûteuse pour les opérateurs, elle engendrerait une explosion des accords de pairs. Cette approche ignore non seulement la volonté d'optimiser la

bande passante mais aussi n'offre pas de solution pour le développement des services futurs. Ces remarques nous amènent à conclure que le surdimensionnement n'apporte pas une réponse aux problèmes de garantie de QoS. Avec les nouvelles applications et les nouveaux usages qui se développent, tels que les applications interactives, la visioconférence ou la voix sur IP, les très gros transferts de fichiers, il devient important de ne plus seulement provisionner les ressources, mais aussi d'adapter la manière dont les données sont transportées dans le réseau. Ceci est de plus vrai dans les réseaux sans fil ou ad-hoc déployés dans des situations d'urgence (médicales, militaires) où la qualité de service est primordiale.

1.4.1.2. Provisionnement intra-domaine

Une des solutions pour le provisionnement intra-domaine repose sur une approche basée sur des politiques. Cette vision, fortement étudiée dans le cadre de l'IETF (groupe de travail « Policy Framework » http://www.ietf.org/html.charters/OLD/policy-charter.html) permet l'administration des réseaux à base des règles abstraites qui spécifient dans un langage de haut niveau ce que le réseau doit faire au lieu de définir comment le faire. Cette architecture offre une large flexibilité et repose sur un serveur de règles qui met en place les politiques à adopter [Pujole04]. Deux entités s'échangent des informations dans cette approche : un serveur de règles (Policy Deployment Point) et ses clients (Policy Enforcement Point) qui exécutent les politiques et les décisions. Dans [Trimintzios03] l'utilisation de politiques de haut-niveau vise l'ingénierie de trafic et elles sont utilisées pour piloter les algorithmes de mise en œuvre des solutions DiffServ sur MPLS. Dans [Cortes03], les politiques sont appliquées dans chaque domaine par un Resource Mediator, sauvegardées dans des bases de données et ensuite utilisées à plusieurs niveaux de l'architecture.

Toutes les solutions présentées sont statiques et la durée de validité des services est relativement longue. Pour répondre à ce problème, [Haddadou06] présente une architecture qui a pour objectif de prendre en compte le provisionnement pour des services à court terme en étendant le protocole COPS (décris dans la section 1.5.3.2.2) et introduisant une entité supplémentaire de signalisation dans le PDP (point de décision).

Dans [Engel03], la gestion n'est pas assurée par l'intermédiaire de politiques : une gestion globale est réalisée à l'aide d'un agent de contrôle des ressources (RCA) qui est en charge de la surveillance, du contrôle et de la distribution des ressources dans le domaine.

1.4.1.3. Provisionnement inter-domaine

Dans le cas d'un environnement multi-domaine, le problème est plus difficile car la portée du service implique plusieurs domaines hétérogènes et gérés par différents fournisseurs. Ceci rejoint le besoin de découvrir et de composer les services offerts par chaque domaine au long du chemin de données pour assurer la QoS requise. Deux points de vue ont été adoptés dans la littérature :

- un provisionnement « statique », qui suppose que la découverte et le choix sont faits préalablement à la requête de service.
- un provisionnement « dynamique », qui a pour objectif de construire dynamiquement, au moment de la requête, le service de bout-en-bout le mieux adapté aux besoins applicatifs.

Dans [Mantar04] les auteurs proposent une solution qui établit préalablement des tunnels (appelés « pipes ») de bout-en-bout à l'aide d'un protocole de signalisation basé sur SIBBS (voir section 1.5.3.2.1 pour les détails de ce protocole). Les tunnels sont construits entre le routeur de bordure de sortie du domaine source et les routeurs de bordure d'entrée dans les

domaines destination ; il est possible de mettre à jour sa capacité suivant le volume de trafic à écouler. Les pipes sont préétablis et dimensionnés en avance et ne concernent qu'une série limitée de services prédéfinis et identiques, ce qui suppose une forte homogénéité des domaines. De plus, l'automatisation des pipes n'est pas considérée, ce qui rend cette approche plutôt statique.

Dans un contexte multi fournisseurs, [Howart05] introduit les concepts de c-SLS (customer SLS) entre un client et son fournisseur et p-SLS (peer SLS) entre deux fournisseurs. Le modèle, repris en détail dans [Howart06], définit aussi la notion de classe QoS locale (l-QC) et de classe de bout-en-bout (e-QC). Une e-QC est obtenue par la composition de deux l-QC adjacentes, la concaténation pouvant ainsi être étendue par la suite.

D'autres propositions font l'hypothèse que les performances et la portée des services ne sont pas définies à l'avance. Il est donc nécessaire de découvrir les services disponibles et leurs performances le long du chemin de données, puis de choisir ceux les mieux adaptés et enfin de les invoquer.

[Füzesi03] propose une architecture (Network Architecture for Inter-Domain Services - NAIS) qui sépare la fourniture du service de l'invocation du service. Dans ce contexte, les opérateurs s'échangent et négocient des services similaires aux circuits virtuels ou réseaux privés virtuels. Ces services ont pour but d'agréger le trafic et ils ont une longue durée, de plusieurs mois ; en revanche, leur mise en place peut prendre aussi un temps considérable.

[Yang05] propose un provisionnement réalisé sur la base d'un vecteur de service obtenu par la composition des services disponibles dans chaque routeur sur le chemin de données. L'architecture impose à l'utilisateur de récupérer à l'aide de messages de test « probe » les services et à chaque routeur de marquer les paquets suivant le choix effectué. Pour autant, cette proposition ne prend pas en compte l'hétérogénéité d'un contexte multi-domaine.

[Gao04] présente une architecture conçue sur trois niveaux (gestion, contrôle et données) qui vise à résoudre les problèmes liés à l'hétérogénéité notamment dans un environnement mobile en utilisant le même mécanisme de sondage (« probe ») du réseau.

[Auriol04] introduit une architecture de communication capable de récupérer les services disponibles et de prendre en compte aussi le niveau Transport dans l'évaluation des performances. Une requête exprime les besoins des applications en termes de QoS sans préciser la classe de service. Les services disponibles au long des domaines ainsi que leurs performances sont découverts par l'intermédiaire d'une signalisation appropriée. Le choix d'une concaténation des services disponibles est effectué en fonction des besoins en QoS à satisfaire. Il est suivi par la réservation des ressources correspondantes sur chaque domaine. Nous considérons aussi le cas d'un provisionnement dynamique à la demande, en étendant les résultats illustrés en [Auriol04] pour optimiser le provisionnement inter-domaine.

1.4.2. Contrôle d'admission

Le provisionnement ne suffit pas à garantir la disponibilité des ressources à tout instant sur le chemin de données. Pour garantir que le trafic reçoit le service adéquat un mécanisme de contrôle d'admission (CAC) de connexion doit être mis en place. Les performances se détériorent rapidement si les demandes dépassent la capacité du réseau : pour éviter ce problème, le CAC assure qu'un nouveau flux de données admis ne provoque pas une dégradation de la QoS. En d'autres termes, chaque nouveau flux susceptible de recevoir une QoS est soumis à un contrôle d'admission qui décide si celui-ci est accepté ou rejeté. Ce mécanisme assure la limitation de la charge et la vérification que les ressources sont

disponibles pour satisfaire les besoins d'un nouveaux flux sans pénaliser les communications existantes. Le CAC doit être complété par un mécanisme de protection du trafic conforme qui garantit qu'une nouvelle connexion ne pénalise les performances des communications existantes. Le CAC concerne les équipements réseau impliqués sur le chemin de données (bande passante, buffers) et distingue deux aspects : le contrôle de la disponibilité à l'intérieur d'un domaine ainsi que sur les liens inter-domaines dans le cas du multi-domaine.

Il est à remarquer que la décision peut être prise suivant différentes techniques, un schéma générique pour le contrôle d'admission étant illustré en [Soldatos05].

A l'intérieur d'un domaine, le CAC consiste à assurer la disponibilité des ressources entre un point d'entrée et les points de sorties. Pour le passage au multi-domaine, le contrôle d'admission doit être prolongé sur les liens inter-domaines au regard des accords de pairs « peering » entre les domaines et de l'état courant des réservations.

[Mykoniaty03] adopte un contrôle d'admission orienté mesures qui est basé sur une estimation périodique de la disponibilité des ressources. La solution repose sur une séparation de la souscription et de l'invocation. La disponibilité des ressources est estimée en utilisant des fonctions de l'ingénierie de trafic sur une matrice de disponibilité de ressources (RAM - Resource Availability Matrix). Les ressources estimées ne sont pas réservées physiquement, ce problème étant laissé ouvert. L'application de trois politiques est utilisée en fonction de la charge du réseau : (1) la situation nominale consiste à accepter une nouvelle requête qui selon l'estimation n'engendre pas une congestion ; (2) la seconde politique est appliquée suite à une congestion rejette tous les nouveaux flux et (3) un contrôle plus restrictif est effectué dans une situation de relaxation précédant le retour à une situation nominale.

[Engel03] propose un contrôle assuré par un module spécifique appelé Resource Control Agent (RCA). Le RCA interagit avec les agents de contrôle d'admission (ACA – Admission Control Agent) qui se situent en bordure du réseau. Les ACA agissent indépendamment et réalisent un CAC dans les limites d'un trafic d'entrée / sortie acceptable pour chaque classe au niveau des routeurs de bordure.

[Yang03] présente une architecture où le contrôle d'admission est effectué par les systèmes d'extrémités. La solution, couplée avec le provisionnement illustré dans [Yang05], repose sur le choix d'un vecteur de service (services récupérés avec des paquets de test du réseau). Les auteurs mettent en avant le degré de satisfaction des performances de bout-en-bout et la diminution du coût pour les utilisateurs finaux.

[Kelly00] suit la même optique d'utilisation des messages de test (« probe ») pour effectuer un contrôle d'admission dans les équipements de bordure ou les terminaux utilisateurs. Les auteurs proposent un modèle mathématique applicable à l'Internet par le marquage des paquets de test par exemple en utilisant les informations de congestion explicite dans l'en-tête IP.

[Jiang06] adopte un contrôle d'admission implicite dans les domaines DiffServ basé sur les informations contenues dans le champ DSCP de l'en-tête IP. La solution consiste à effectuer un CAC sur chaque routeur, spécifique pour chaque classe EF et AF.

Pour une communication qui traverse plusieurs domaines il est nécessaire d'effectuer le contrôle d'admission sur les liens inter-domaines, mais aussi de le prolonger de domaine en domaine. Une première approche consiste à poursuivre l'approche IntServ en impliquant les routeurs de bordure dans le CAC. Cette approche a été adoptée par [Salsano03] qui propose l'utilisation d'un protocole qui étend BGRP [Pan00].

Une approche hiérarchique pour répondre au problème de CAC repose sur le concept de gestionnaires de domaines de type Bandwith Broker introduit dans [Nichols99]. En considérant les domaines fortement hétérogènes, ce sont des entités qui ont la connaissance des disponibilités de ressources et sont en charge de leur gestion d'une manière plus hiérarchique, les routeurs n'ayant plus cette responsabilité. Une communication (signalisation) entre les BB est nécessaire pour mettre en œuvre le CAC inter-domaine le long du chemin de données (Figure 7).

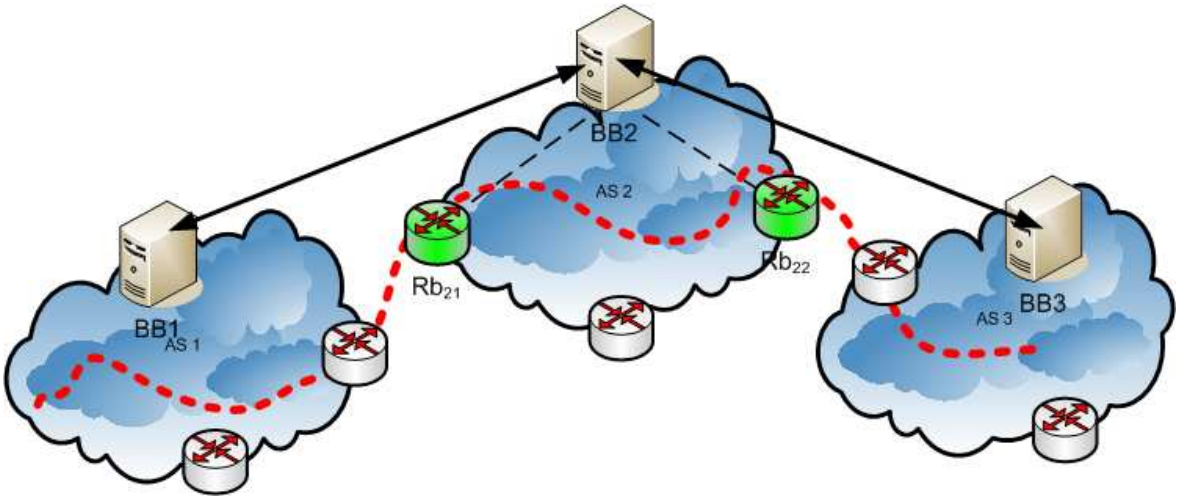


Figure 7 : Architecture multi-domaine à base de Bandwidth Broker

Dans cette approche, le contrôle d'admission est hiérarchisé à l'intérieure d'un domaine et un échange des messages est nécessaire entre les BBs (performances du service, information sur le trafic, disponibilité, etc.). Cet échange constitue la signalisation inter-domaine.

[Mantar04] répond au problème du CAC par l'établissement et le dimensionnement au préalable des tunnels (pipes) prédéfinis. Une nouvelle requête reçue par le BB du premier domaine implique juste la vérification de la disponibilité suivant la destination et la classe de service requise. Ce premier BB ne communique pas avec ses BB pairs, et le contrôle reste local. Une nouvelle réservation est envisageable en cas d'échec, ce qui implique une signalisation appropriée et aussi un fort couplage entre les domaines réalisé dans la phase initiale de provisionnement.

L'architecture présentée dans [Jia01] utilise toujours la notion de Bandwidth Broker et un protocole de signalisation basé sur SIBBS (protocole décrit dans la section 1.5.3.2.1). Pour le contrôle d'admission, les auteurs proposent un algorithme à contraintes multiples fondé sur la méthode Bellman-Ford (MCBF) [Bellman58] [Ford62], avec la signalisation associée.

Dans la section suivante, nous présentons en détails les concepts de la signalisation pour la qualité de service dans l'Internet.

1.5. Signalisation pour la QoS

1.5.1. Introduction

La signalisation est un concept clef dans les architectures qui visent à offrir de la QoS. Les diverses propositions convergent vers la nécessité d'avoir une signalisation intra-domaine et inter-domaine. La signalisation concerne plusieurs aspects comme le routage, la sécurité, la surveillance (monitoring), mais nous ne traitons dans nos travaux (et par la suite dans ce mémoire) que la signalisation pour la qualité de service. Dans un environnement multi-

domaine, une signalisation est requise pour la découverte des services et de leurs performances le long du chemin de données, ainsi que pour l'évaluation de la disponibilité des ressources.

Deux axes de recherches sont suivis pour répondre aux besoins en signalisation des solutions pour le provisionnement et le contrôle d'admission :

- une signalisation couplée au chemin de données (« on-path ») dont le représentant le plus abouti est RSVP ;
- une signalisation découplée du chemin de données (« off-path »), que nous adoptons aussi dans le cadre de nos travaux, qui implique des équipements en charge de la gestion de la QoS, notamment les entités de type Bandwidth Broker.

L'approche couplée au chemin de données assume une homogénéité de bout-en-bout de l'architecture Internet et le fonctionnement identique des équipements sur le chemin de données. Ses principaux inconvénients sont le passage à l'échelle (car ils introduisent une consommation des ressources importante des routeurs) et l'hypothèse d'homogénéité des domaines. De plus, des états doivent être gardés dans chaque routeur au long du chemin.

L'hétérogénéité de l'Internet et l'environnement multi-domaine ont favorisé le découplage de la signalisation intra-domaine (pour réserver les ressources à l'intérieur d'un domaine) de celle inter-domaine (pour la réservation entre domaines). Cette séparation (illustrée dans [Vali04]) conduit à une plus grande flexibilité dans le processus d'allocation des ressources. Dans nos travaux, nous nous intéressons particulièrement à la signalisation inter-domaine, laissant le choix aux opérateurs d'implanter la solution la mieux adaptée à l'intérieur du domaine.

Après avoir introduit les concepts généraux sur la signalisation, nous donnons dans les paragraphes suivants un panorama des protocoles proposés pour supporter ce besoin. Nous différencions dans un premier temps les protocoles proposés pour le niveau applicatif de ceux proposés pour le niveau réseau.

1.5.2. Protocoles de signalisation de niveau applicatif

Les mécanismes de signalisation peuvent intervenir à plusieurs niveaux de l'architecture Internet. Au niveau applicatif, une signalisation est nécessaire entre les clients pour négocier une série de paramètres pour la mise en place d'une communication : les capacités des terminaux (en particulier les codecs), la localisation des terminaux (adresses IP, numéros de port), les protocoles transport utilisés etc. Nous présentons succinctement dans les paragraphes suivants, les protocoles de signalisation les plus utilisés actuellement : SIP, RTSP et H323.

1.5.2.1. SIP

SIP (Session Initiation Protocol) [Rosenberg02] est un protocole utilisé pour établir, modifier et fermer une session applicative sur les réseaux IP. Il est indépendant du protocole de transport sous-jacent et il a été conçu pour interopérer avec d'autres protocoles de l'IETF : RTP (Real Time Transport Protocol [Schulzrinne03]), SDP (Session Description Protocol [Handley98]), DNS (Domain Name System [Mockapetris83]) etc. SIP fonctionne selon le modèle client-serveur et les messages échangés ont un format texte. Le corps des messages contient les informations relatives à la session et utilise généralement le protocole Session Description Protocol (SDP [Handley98])

1.5.2.2. RTSP

RTSP (Real Time Streaming Protocol) est aussi un protocole de niveau applicatif utilisé pour des applications multimédia dans le but d'établir et de contrôler des flux synchronisés

[Schulzrinne98]. L'envoi et le transfert des données ne font pas partie de RTSP, qui par contre propose des mécanismes pour choisir les canaux transport (UDP, UDP multicast, TCP). L'ensemble des média est défini dans une description standard de type SDP ou SMIL (Synchronized Multimedia Integration Language - http://www.w3.org/AudioVideo/). RTSP offre des fonctionnalités permettant aux utilisateurs finaux d'accéder directement au contenu multimédia et d'en contrôler la diffusion (lecture, avance rapide, suspension etc.).

1.5.2.3. H.323

H.323 [ITU-T-Rec.-H323-06] fait partie d'un ensemble de recommandations standardisées par l'ITU-T ayant pour but de définir des protocoles de communication pour des applications multimédia sur des réseaux à commutation de paquets. H.323 spécifie une pile de protocoles qui incluent la signalisation, la négociation, le transport des données vidéo et audio. La signalisation dans H.323 est basée sur le protocole RAS (Registration Admission Status) pour l'enregistrement et l'authentification et sur la recommandation ITU-T Q.931 pour l'initialisation et le contrôle d'appel. Pour la négociation des codecs, le protocole utilisé est H.245.

Bien que H.323 soit le précurseur des protocoles pour les sessions multimédia, SIP s'impose de plus en plus dans le monde Internet grâce à sa complexité réduite et à sa ressemblance avec HTTP (HyperText Transfer Protocol [Fielding99]).

1.5.3. Protocoles de signalisation de niveau réseau

Pour assurer la QoS dans le réseau, une signalisation est nécessaire pour la configuration des équipements, le CAC,… Suivant le modèle de gestion de la QoS, la signalisation se décline en deux catégories : couplée au chemin de données (« on-path ») et découplée du chemin de donnés.

1.5.3.1. Signalisation couplée au chemin de données

Cette section présente une série de protocoles de signalisation pour la QoS qui adopte l'approche couplée au chemin de données. Dans un premier temps nous décrivons le précurseur de ces protocoles, Resource Reservation Protocol (RSVP), issu des travaux du groupe IntServ. Ensuite nous décrivons brièvement d'autres propositions, qui ont essayé de répondre aux limitations de RSVP (en particulier lié au passage à l'échelle vis à vis du nombre de flux à traiter).

1.5.3.1.1. RSVP

Dans le modèle IntServ, la qualité de service est garantie par l'intermédiaire d'une réservation préalable des ressources dans chaque routeur sur le chemin de données. Afin de réserver les ressources réseau (bande passante et mémoire tampon) nécessaires à l'obtention de ces services, l'approche IntServ utilise un protocole de réservation de ressources : RSVP [Braden97]. Ce protocole propage la demande de réservation à tous les routeurs sur le chemin des données (de façon dynamique afin de s'adapter aux changements de route). Chaque routeur est en charge d'accepter ou non la réservation en tenant compte des ressources disponibles localement et de la caractérisation du trafic fournie avec la réservation. Une API a été définie pour accéder à ces services, la RAPI.

Les applications qui demandent les services GS ou CL d'IntServ utilisent le protocole RSVP pour réserver les ressources et configurer les équipements sur le chemin de données. Dans un premier temps, le message PATH est envoyé par l'application émettrice vers le récepteur (voir Figure 8). Ce message contient une spécification du trafic (TSPEC) à QoS qui sera utilisé par

l'application. Chaque routeur sur le chemin de données traite ce TSPEC et achemine plus loin le message PATH. Une spécification additionnelle (ADSPEC) peut être ajoutée par les routeurs pour signaler certaines contraintes sur les ressources. Une fois le signal PATH arrivé au récepteur, il répond avec le message RESV. Ce signal permet de réserver effectivement les ressources au retour. Le message RESV contient la spécification des ressources réservées (RSPEC). Une fois le chemin configuré, la transmission des données (du flux pour lequel les ressources ont été réservées) peut commencer. Tous les routeurs classifient chaque paquet rentrant pour lui fournir le service adéquat. Cette classification est basée sur plusieurs informations : adresse source et destination, numéros de port, etc.

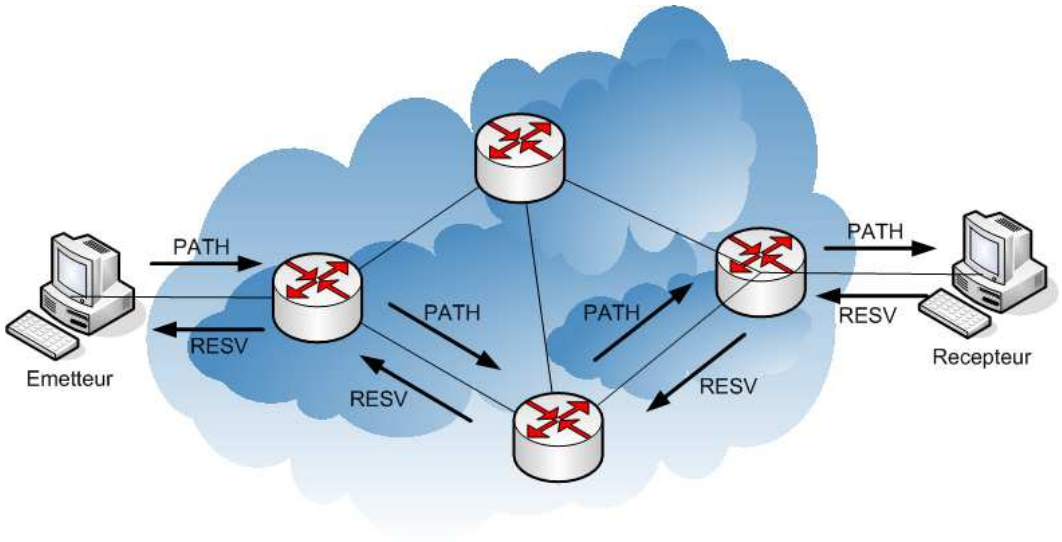


Figure 8 : Fonctionnement du protocole RSVP

Les réservations RSVP sont unidirectionnelles, initiées par le récepteur, les communications bidirectionnelles nécessitant des réservations séparées. Une autre caractéristique importante de RSVP est le maintien des états (appelés « soft-state ») dans tous les routeurs. Les réservations mémorisées dans les routeurs expirent si elles ne sont pas rafraichies par des messages périodiques. Outre les messages PATH et RESV, le protocole RSVP utilise les messages TEARDOWN (pour libérer explicitement les ressources sans attendre l'expiration des minuteurs - « timers »), ERROR et CONFIRMATION pour ajouter de la fiabilité.

Les inconvénients principaux de RSVP résident dans sa complexité et son manque de résistance au facteur d'échelle (une des limites du modèle IntServ). Rappelons que tous les routeurs au long du chemin doivent implémenter RSVP et maintenir un contexte même si aucune réservation n'est effectuée. Plusieurs travaux visent à proposer des protocoles basés sur RSVP en simplifiant ses mécanismes.

1.5.3.1.2. YESSIR

Le protocole YESSIR (YEt another Sender Session Internet Reservation) [Pan98] propose un mécanisme de réservation des ressources au long du chemin de données en simplifiant le modèle RSVP (réduction du contrôle et du traitement, flexibilité au niveau utilisateur). Les requêtes de réservation sont initiées pas l'émetteur, unidirectionnelles et de bout-en-bout.

1.5.3.1.3. Boomerang

Boomerang [Feher99] est un protocole de réservation de ressources qui utilise un seul type de message pour l'installation et la libération des ressources. Tous les mécanismes de gestion de la

réservation sont concentrés dans le nœud initiateur (IN). Il supporte la réservation initiée par l'émetteur ainsi que celle initiée par le récepteur. Le multicast n'est pas supporté et le seul mode de réservation possible est celui unidirectionnel.

1.5.3.1.4. BGRP

BGRP (Border Gateway Reservation Protocol) [Pan00] se propose d'agréger la réservation des ressources inter-domaine pour des flux unicast. L'objectif est de réduire la charge, le nombre d'états et la bande passante. BGRP construit un arbre pour chaque domaine et réunit les réservations de toutes les sources dans le réseau pour limiter les informations retenues dans les routeurs, particulièrement dans les domaines du cœur. BGRP est déployé dans les routeurs de bordure et il utilise également des soft-states pour maintenir les réservations.

1.5.3.2. Signalisation découplée du chemin de données

1.5.3.2.1. SIBBS

Le protocole SIBBS (Simple Inter-domain Bandwidth Broker Protocol) [QBone01] a été défini par le groupe de travail signalisation de QBone. Il a pour objectif d'être utilisé dans un environnement DiffServ basé sur l'existence de Bandwidth Brokers. Dans la plate-forme QBone, chaque réseau DiffServ supporte un ou plusieurs services. SIBBS est un protocole simple dont le but est de communiquer entre les Bandwidth Broker. Il est basé sur l'échange de deux principaux PDUs (Figure 9) :

- RAR (Resource Allocation Request) ;
- RAA (Resource Allocation Answer).

Le message RAR inclut l'identifiant du service global, des informations relatives à la requête de qualité de service (classe de service, bande passante), les adresses IP source et destination, un champ d'authentification et d'autres paramètres du service. Le message RAA contient la réponse à un PDU RAR. La communication entre les Bandwidth Brokers est supposée fiable, assurée par exemple par le protocole TCP.

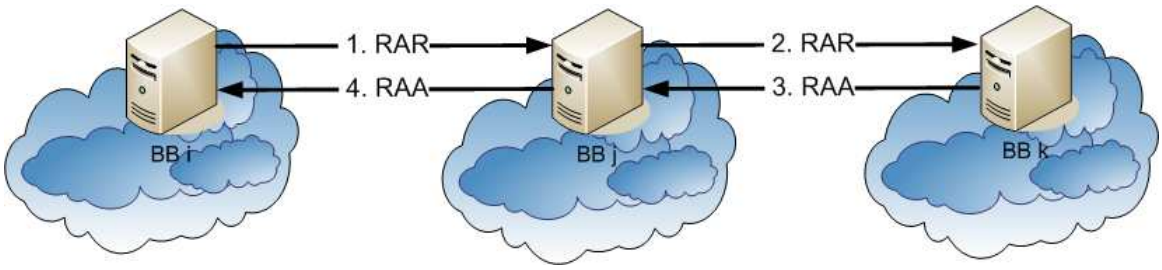


Figure 9 : Illustration du protocole SIBBS

Recevant un message RAR, un Bandwidth Broker : i) authentifie la requête comme provenant d'un pair ; ii) vérifie que la requête reçue respecte les SLS existant, iii) évalue la disponibilité des ressources à l'intérieur de son domaine pour répondre aux besoins du flux de données et iv) accepte cette nouvelle connexion si toutes les conditions relatives aux politiques internes du domaine sont respectées.

Si une requête est acceptée, le message RAR est propagé de manière récursive vers sa destination par tous les Bandwidth Brokers des domaines impliqués le long du chemin de données. En supposant les ressources disponibles, le dernier Bandwidth Broker répond avec un RAA positif, message qui est acheminé jusqu'au Bandwidth Broker d'origine, qui conclut à l'admission de la requête. Le maintien des ressources est assuré par des messages de rafraichissement émis périodiquement.

Pour la configuration des différents équipements (routeurs), SIBBS ne spécifie pas un protocole particulier mais il peut s'appuyer sur les propositions de SNMP, DIAMETER ou COPS. De plus, SIBBS ne précise pas comment identifier le prochain Bandwidth Broker.

1.5.3.2.2. COPS et COPS-SLS

COPS est un protocole basé sur le schéma client – serveur, destiné aux réseaux basés sur des politiques. Les composants du protocole COPS sont le PDP (Policy Decision Point) et le PEP (Policy Enforcement Point). Le PDP est l'entité centrale en charge de prendre les décisions (pour lui et pour les autres nœuds du réseau). Le PEP est le point ou les politiques seront appliquées, un routeur par exemple (voir Figure 10). En cas d'absence d'un serveur de politiques, un PDP Local (LPDP) peut être utilisé.

COPS est un protocole de type requête-réponse qui permet à un PEP (routeur) d'interroger son PDP sur les actions à réaliser suite à l'apparition d'un événement (par exemple l'arrivée d'un message de signalisation).

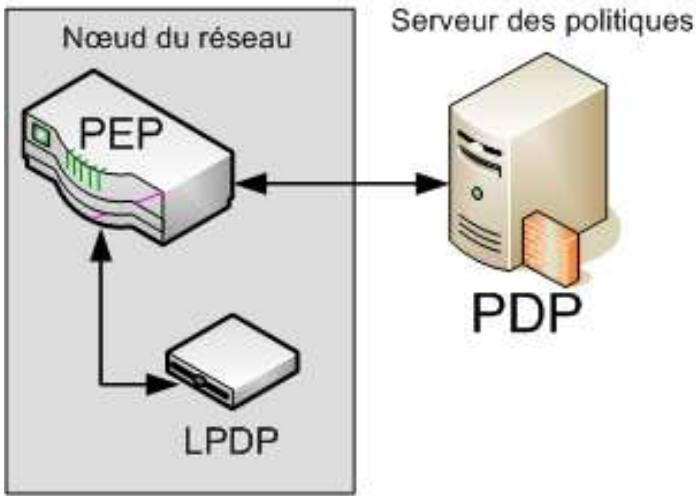


Figure 10 : Protocole COPS

COPS-SLS [Nguyen02] et [Nguyen03] est une extension du protocole Common Open Policy Service (COPS) [Durham02] pour la gestion des SLS (Service Level Specification) dans un environnement multi-domaine. COPS-SLS a le même comportement que SIBBS : une requête est propagée d'un Bandwidth Broker à un autre sur le chemin de données. Chaque Bandwidth Broker a un double rôle :

- PDP pour le domaine précédent, Bandwidth Broker qui envoie la requête ;
- PEP par rapport au domaine suivant.

Par rapport à SIBBS, le protocole COPS-SLS, ajoute quelques fonctionnalités comme la renégociation des classes de service dans le cas d'une demande d'admission échouée. Par contre, COPS-SLS ne précise pas comment découvrir le Bandwidth Broker suivant ou l'identification des routeurs de bordure.

1.5.4. Signalisation générique – NSIS

1.5.4.1. Introduction

Le besoin en signalisation dans l'Internet ne concerne pas uniquement la qualité de service, mais également la sécurité, la mobilité, ou la métrologie. Pour répondre à ces différents

besoins, le groupe de travail NSIS (Next Step in Signaling) a été crée à l'IETF (http://www.ietf.org/html.charters/nsis-charter.html) dans le but de définir un cadre générique pour la signalisation.

Ce groupe de travail mène une activité importante sur la standardisation d'une solution générale pour la signalisation. Dans [Brunner04] les spécifications principales sur les besoins des protocoles de signalisation et le comportement vis-à-vis de la mobilité sont définies. Le groupe a aussi spécifié un cadre générique pour une signalisation dans l'Internet, solution qui distingue deux niveaux :

- le niveau NTLP (NSIS Transport Layer Protocol) est dédié au transport de la signalisation entre les entités NSIS, indépendamment de l'objet de la signalisation (QoS, sécurité, mesures, etc.) ;
- le niveau NSLP (NSIS Signaling Layer Protocol) est spécifique aux applications de signalisation qui ciblent un certain objectif. Chacune de ces applications définit ses propres messages et leur enchainement de messages.

Cette approche découple le transport de la signalisation d'objet de la signalisation proprement dite. L'architecture NSIS est présentée dans la Figure 11 :

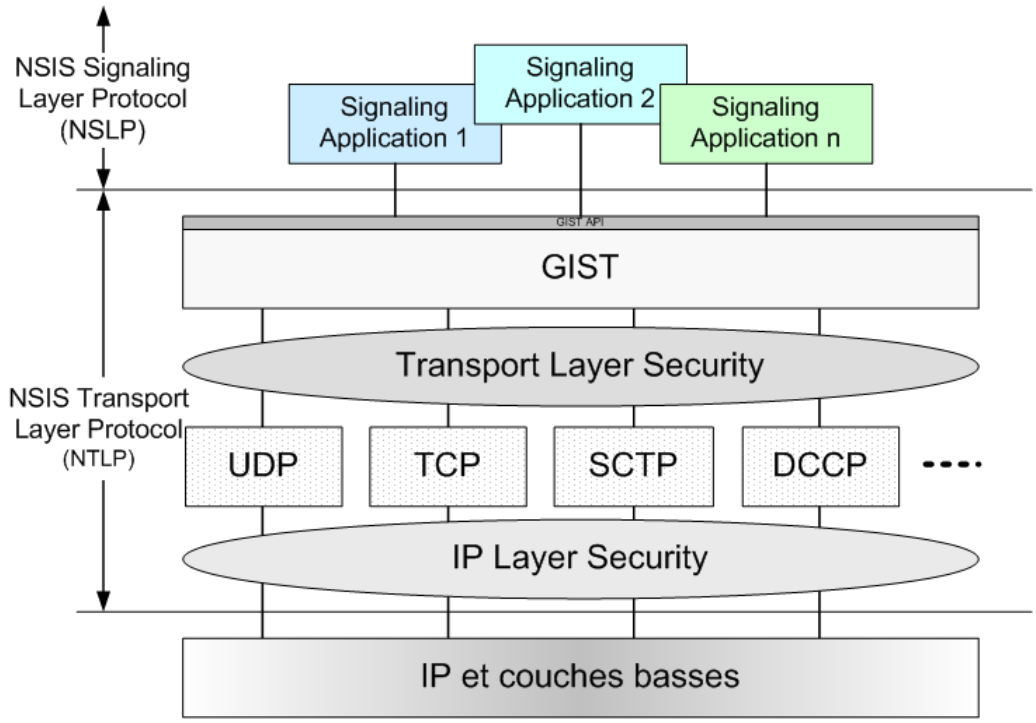


Figure 11 : Architecture NSIS

La philosophie de NSIS est de réutiliser les mécanismes de RSVP. Ainsi, dans sa version actuelle, NSIS suit l'approche couplée du chemin de données (« on-path ») qui implique que les entités de signalisation se trouvent sur le chemin de données. La signalisation est effectuée saut par saut entre les entités NSIS (NE), les dispositifs ne supportant pas NSIS acheminant simplement les messages sans les traiter. La Figure 12 décrit le fonctionnement de NSIS. Chaque hôte et aussi une partie des routeurs sur le chemin de données implémentent une entité NSIS (NE) qui échange des messages de signalisation.

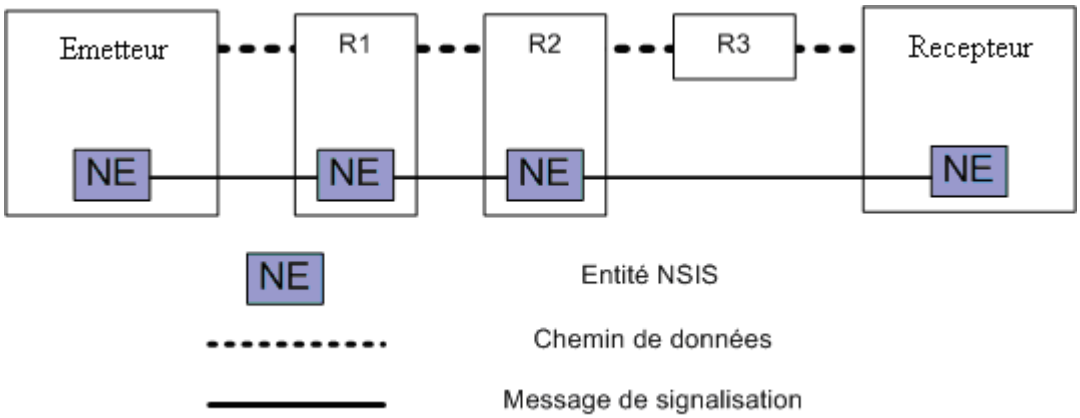


Figure 12 : Signalisation NSIS

1.5.4.2. NTLP : le protocole GIST

Au niveau NTLP, un protocole appelé GIST (General Internet Signaling Transport) a été spécifié [Schulrzine06]. GIST est responsable du transfert des messages entre les entités de signalisation. Le fonctionnement de GIST est le suivant : suite à la réception d'un message de signalisation (comprenant les informations relatives au flux de données), le niveau GIST prend en charge de transférer ce message vers la prochaine entité NSIS. Pour établir une association GIST entre deux NE, une séquence de négociation en trois étapes (« three-way handshake ») est utilisée. L'association ainsi créée pourra être réutilisée pour différentes sessions ultérieures. En réception, GIST achemine le message directement à la prochaine NE où il transfère ce message au niveau NSLP pour traitement. Notons que GIST ne regarde ni ne modifie la charge utile (payload) du message NSLP. GIST utilise deux modes de fonctionnement :

- le mode datagramme (D-mode) pour encapsuler des petits messages peu fréquents ;
- le mode connexion (C-mode) utilisé pour les protocoles de transport orientés « stream », comme TCP et plus récemment SCTP, ce qui permet de rajouter des fonctionnalités comme la fiabilité et la sécurité (avec TLS par exemple sur TCP).

Comme RSVP, GIST garde des états relatifs à une session, les « soft-state ». Chaque état se voit associé un minuteur (« timer » en anglais) redémarré à chaque mise à jour d'état. Si un timer expire, l'état est supprimé et les ressources associées sont relâchées. GIST garde deux tables d'états : MRS (Message Routing State) pour les flux individuels et MAS (Message Association State) pour les associations entre les entités NSIS pair.

1.5.4.3. NSLP

NSLP est spécifique pour divers types de signalisation, indépendants les uns des autres. Plusieurs protocoles de niveau NSLP ont été définis dans le cadre du groupe de travail NSIS, en particulier :

- QoSNSLP [Manner06] fournit des fonctionnalités similaires à RSVP par l'installation des états au long du chemin de données en vue de contrôler la QoS de bout en bout;
- [Stiemerling06] propose une signalisation pour la configuration des entités de translation d'adresse (NAT) et pare-feux (Firewall) suivant les besoins des flux.

1.6. Architectures conceptuelles

Sur les bases précédentes, plusieurs architectures ont été proposées pour la mise en œuvre des mécanismes de gestion de la QoS. Nous présentons brièvement dans la section suivante les

modèles des réseaux de nouvelle génération (NGN) ainsi que plusieurs projets de recherche conduits dans un contexte international.

1.6.1. Les réseaux de nouvelle génération (NGN)

1.6.1.1. Présentation générale

A la fin des années '90 les acteurs de télécommunication ont introduit les concepts fondamentaux des réseaux de nouvelle génération. La recommandation ITU-T Y.2001 [ITU-T Y.2001] définit les réseaux de prochaine génération, en accord avec le projet GII (Global Information Infrastructure), comme « réseaux en mode paquet, en mesure d'assurer des services de télécommunication et d'utiliser de multiples technologies de transport à large bande à qualité de service imposée et dans lequel les fonctions liées aux services sont indépendantes des technologies sous-jacentes liées au transport » [Y.2001]. D'autre part, ETSI à proposé pour définition dans [ETSI/GA38(01)18] : « NGN est un concept pour définir et déployer des réseaux qui, à cause de leur séparation formelle en plusieurs niveaux et plans et de l'utilisation des interfaces ouvertes, offrent aux opérateurs et fournisseurs de service une plate-forme qui évolue pas-à pas pour créer, déployer et gérer des services innovants ».

Les caractéristiques communes des réseaux de nouvelle génération, globalement agréées sont : la généralisation des réseaux à commutation des paquets et la convergence vers « tout IP », la séparation nette entre les fonctions de contrôle et les fonctions de transport, le découplage service / transport, l'ubiquité, la flexibilité et la convergence des fonctions de gestions.

1.6.1.2. Architecture NGN ITU-T

L'architecture fonctionnelle des réseaux NGN décrite par l'ITU-T dans la recommandation Y.2012 est illustrée dans la Figure 13. Il est à remarquer que la définition des différentes fonctions dans chacun des plans de services et de transport est clairement séparée. L'ANI (Application Network Interface) fournit un point d'accès entre les applications et les éléments NGN. De la même manière, l'interaction entre l'utilisateur et les réseaux NGN et entre les réseaux NGN se réalise par l'intermédiaire des UNI (User Network Interface) et NNI (Network Network Interface).

Les services fournis aux applications (utilisateurs) sont assurés, grâce aux fonctions de support d'application et de service, comme des fonctions de commande connexes. Les opérations des fonctions de commande de service incluent l'enregistrement, l'authentification et l'autorisation, sur la base des profils utilisateurs stockés dans une base de données.

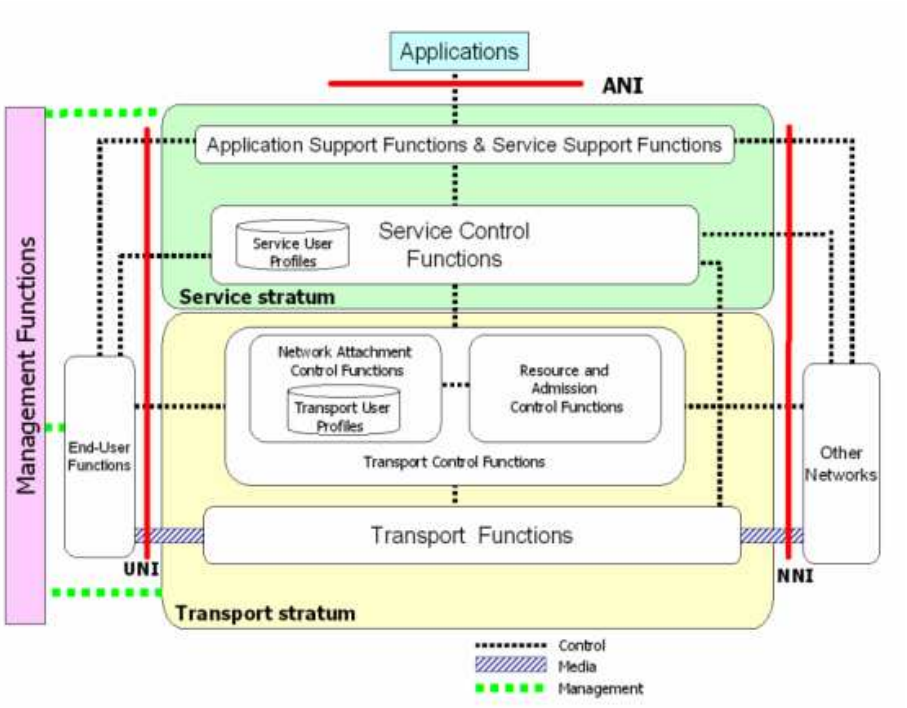


Figure 13 : Architecture NGN ITU-T

Les fonctions du plan de transport impliquent tous les niveaux horizontaux en distinguant les fonctions de réseaux d'accès, les fonctions de bordure, les fonctions transport central et les fonctions passerelle. Le plan transport fournit la connectivité (IP) des composants NGN sous le contrôle des fonctions de commande de transport, notamment les fonctions de commande de rattachement au réseau (NACF, *Network Attachment Control Function*), ainsi que les fonctions de contrôle de ressources et d'admission (RACF, *Resource and Admission Control Function*). RACF assure le contrôle en fonction des politiques de gestion, des mécanismes d'admission et de la disponibilité des ressources.

Les fonctions de gestion (Management Functions) constituent une composante de base de l'architecture NGN, afin d'offrir le niveau de service attendu. Ses actions se retrouvent au niveau des deux plans de service et de transport et comprennent divers champs : gestions de performance, de configuration, de sécurité, de fautes, de taxation etc.

1.6.1.3. Architectures IMS

IMS (IP Multimedia Subsystem) propose un cadre architectural pour des applications multimédia sur IP, défini initialement pour les réseaux mobiles par 3GPP (3rd Generation Partnership Project) pour la norme UMTS. Ces concepts ont été repris par 3GPP, 3GPP3 et TISPAN et actualisé pour prendre en compte d'autres types de réseaux. Selon 3GPP [3GPP], IMS n'a pas pour but de standardiser des applications, mais de permettre le déploiement sur une infrastructure commune filaire ou sans fil (convergence fixe-mobile). Pour faciliter l'intégration avec Internet, IMS propose l'utilisation des protocoles standards IETF tel que SIP [Rosenberg02] ou Diameter [Calhoun03]. L'IMS n'est pas un réseau unique, mais une interconnexion de plusieurs réseaux avec infrastructures différentes interopérables grâce aux éléments IMS.

Les travaux communs avec ETSI-TISPAN ont conduit à l'ouverture de l'IMS vers les réseaux fixes. Cette convergence fixe-mobile (FMC) est l'un des axes principaux des domaines des télécommunications. TISPAN étend l'architecture initiale IMS en rajoutant des composants spécifiques pour supporter l'interopérabilité entre différents réseaux.

Les architectures NGN fournissent un cadre pour la mise en œuvre des services évolués avec des caractéristiques innovantes : QoS, souplesse de la taxation, intégration et convergence fixe-mobile.

1.6.2. Projets de recherche

1.6.2.1. Introduction

Du fait de la convergence vers un réseau unique de communication, dont la principale caractéristique est l'hétérogénéité, l'objectif d'offrir d'autres services en dehors du classique « best-effort » impose une remise en cause du modèle de service des paquets IP et du modèle architectural de l'Internet. Nous avons identifié les principaux axes des recherches pour la QoS correspondant aux besoins associés que nous avons aussi suivis dans nos travaux : le provisionnement des ressources, le contrôle d'admission et la signalisation. De nombreux travaux ont traité ces problèmes soit de manière indépendante, soit dans le cadre d'architectures, souvent issues de grands projets internationaux.

Plusieurs initiatives (Internet2 aux Etats-Unis et l'Initiative « Next Generation Networks » en Europe) ont été menées depuis quelques années conduisant à la réalisation de grands projets. Le groupe Internet2 QoS (http://qos.internet2.edu/wg/) a eu pour mission de supporter le développement et le déploiement des applications et technologies réseaux avancées avec un trafic IP différencié. L'Initiative NGN (www.ngni.org/qos/htm), sponsorisée par la Commission Européenne a démarré en 2001 et son principal objectif a été d'encourager les groupes de travail pour mieux préparer la transition de l'Internet actuel vers un réseau de nouvelle génération qui offrira des services évolués avec un niveau élevé de qualité de service, de performance et de sécurité. Dans ce contexte, plusieurs projets de recherche ont eu pour but d'élaborer des propositions sur la QoS principalement dans un environnement DiffServ.

1.6.2.2. QBone

Le projet QBone (qbone.internet2.edu) [Qbone01], lancé en 1999 aux Etats-Unis est un pionnier qui avait pour objectif le déploiement et le test des mécanismes de QoS évolutifs dans un environnement Internet multi-domaine. QBone visait la mise en œuvre d'un service Premium (équivalent à une ligne louée) à l'échelle de l'Internet. Le projet n'a pas abouti aux résultats initialement ciblés et a ensuite visé un objectif de service moins performant ne nécessitant pas de mécanismes complexes ([QBone-qbss] et [QBone-ass]).

En Europe, trois projets menés conjointement dans le cadre de « Premium IP cluster » (http://st.inf.tu-dresden.de/aquila/files/pip-cluster.htm), AQUILA, TEQUILA et CADENUS ont proposé les premières architectures fonctionnelles dans le but d'offrir une QoS de niveau IP dans l'Internet multi-domaine.

1.6.2.3. AQUILA

Les objectifs principaux du projet AQUILA (« Adaptative Resource Control for QoS Using an IP-based Layered Architecture » - www.ist-aquila.org) visaient la conception et l'implémentation d'une architecture de QoS dans un environnement IP. La solution AQUILA est basée sur la proposition d'un niveau de contrôle des ressources en privilégiant une architecture de type DiffServ. De plus, AQUILA propose l'utilisation d'une boite à outils pour faciliter la mise en place de la QoS par les utilisateurs finaux. Pour répondre au problème de provisionnement, AQUIILA adopte une approche orienté agent qui configure automatiquement les équipements à partir d'une base de données. La solution, décrite en [Engel03], propose une gestion globale d'un domaine via un agent qui a pour rôle de surveiller et contrôler les

ressources. Pour le contrôle d'admission, AQUILA propose une vue qui implique principalement les routeurs de bordure d'un domaine, le routeur de cœur ne gardant que des états par agrégat. [Salsano03]

1.6.2.4. TEQUILA

Le projet TEQUILA (« Traffic Engineering for Quality of Service in the Internet at Large Scale » - www.ist-tequila.org) visait à obtenir des garanties quantitatives de QoS en étudiant la définition des services et des outils d'ingénierie de trafic. Les axes principaux de recherche de Tequila comprenaient la spécification des SLS et des schémas d'ingénierie de trafic intra et inter-domaine. Le provisionnement des ressources dans TEQUILA repose sur une approche basé sur des politiques qui visent à l'ingénierie de trafic pour gérer la mise en place des solutions DiffServ sur MPLS [Trimintzios02] et [Trimintzios03]. Concernant le contrôle d'admission, TEQUILA adopte une approche orienté mesure, basé sur une estimation et une prédiction de la charge qui conditionne l'acceptation d'une nouvelle requête.

1.6.2.5. CADENUS

Le projet CADENUS (« Creation and Deployment of End-user Services in Premium IP Networks » - wwwcadenus.fokus.frankhofer.de) ciblait la conception et le développement des solutions pour la configuration et le provisionnement des services pour les utilisateurs finaux avec des garanties de QoS dans un environnement Premium IP. L'architecture CADENUS propose un ensemble des modules fonctionnels qui agissent à l'interface entre l'utilisateur et le fournisseur. CADENUS adopte également une approche basée sur des politiques pour le provisionnement : ces politiques sont déployées jusqu'au niveau des équipements réseau [Cortes03].

1.6.2.6. MESCAL

Le projet MESCAL (« Management of End-to-end Quality of Service Across the Internet et Large » - www.mescal.org) a étendu les résultats du projet TEQUILA en étudiant plus spécifiquement le problème du provisionnement dans un contexte multi-domaine. La solution proposée vise à valider une architecture basée sur un nouveau concept de contrat client-fournisseur et d'accords de pairs qui permettent le déploiement et la fourniture de la QoS inter-domaine. Les objectifs de MESCAL couvrent la proposition de « business model », la spécification et l'implémentation des algorithmes et protocoles de l'architecture inter-domaine, l'évolution des protocoles de routage existants et la proposition d'une approche qui s'appuie sur des politiques et ingénierie de trafic. MESCAL approfondit les solutions de provisionnement étudiées dans TEQUILA, dans un contexte multi-domaine en proposant un modèle de concaténation en cascade entre les domaines adjacents. La solution repose sur l'utilisation du protocole Q-BGP et sur la définition de classe de QoS étendue (e-QC) définie récursivement comme la concaténation d'une classe locale (l-QC) et d'une e-QC d'un domaine adjacent [Boucadair05], [Howart06].

1.6.2.7. ENTHRONE

Le projet ENTHRONE (« End-to-End QoS through Integrated Management of Content, Networks and Terminals » - www.ist-enthrone.org) adresse les problèmes de génération, protection, distribution et utilisation de contenus multimédia et la gestion des ressources dans un environnent géographiquement distribué. Le projet propose une solution intégrée pour la gestion de divers services audio-visuels incluant la protection du contenu, la distribution sur le réseau et la réception au niveau des terminaux utilisateurs dans le but d'offrir une QoS de bout-en-bout sur des domaines hétérogènes. ENTHRONE propose un modèle qui sépare les

fournisseurs de contenu (CP), les consommateurs (CC), les fournisseurs de service (SP) et les opérateurs réseaux (NO) [Kourtis04]. Les opérateurs sont en charge du provisionnement de service par le biais des techniques d'ingénierie de trafic dans un contexte IMS. L'architecture détaillée dans [Ahmed04] implique l'engagement des ressources suite à la souscription d'un SLA et le provisionnement s'applique pendant des cycles périodiques (la possibilité d'un provisionnement dynamique étant en cours d'étude).

1.6.2.8. NETQOS

Le projet NETQOS (Policy Based Management of Heterogeneous Networks for Guaranteed QoS www.netqos.eu) a pour objectif le développement d'une solution automatique de gestion de la QoS basée sur des politiques qui vise un environnement hétérogène mono-domaine. Le but est de proposer une architecture autonome, auto-configurable qui repose sur des politiques de gestion, capables de répondre aux besoins dynamiques de QoS des utilisateurs qui peuvent évoluer pendant une communication.

1.6.2.9. DAIDALOS

Le projet DAIDALOS (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services www.ist-daidalos.org) a pour but de proposer une nouvelle architecture sur IPv6 orientée utilisateur, flexible et facile à administrer. DAIDALOS vise à intégrer des technologies réseaux hétérogènes qui permettent aux fournisseurs de services et aux opérateurs d'offrir des nouveaux services performants. Les activités du projet se concentrent particulièrement sur les réseaux mobiles 3G, mais les technologies complémentaires sont aussi envisagées.

1.6.2.10. EuQoS

Sur la base de plusieurs contributions, le projet européen EuQoS (« End-to-end Quality of Service support over heterogeneous networks » - www.euqos.eu), dans le cadre duquel ont été menés les travaux décrits dans ce mémoire, a proposé, développé et testé une architecture globale de gestion de la QoS de bout-en-bout dans un environnent Internet multi-domaine hétérogène. EuQoS concentre l'effort sur la signalisation intra et inter-domaine, et sur le contrôle d'admission spécifique aux différentes technologies sous-adjacentes. Nous allons discuter en détail la solution EuQoS dans le chapitre 3.

Le Tableau 3 résume ces principaux projets de recherche.

Nom Projet	***Mots clefs***	***Références***
QBone	Bandwidth Broker DiffServ, signalisation inter-domaine	http://qos.internet2.edu/wg/documents-informational/draft-i2-qbone-arch-1.0/ http://qbone.internet2.edu/bb/parameter-requirementsV2.html
AQUILA	Contrôle d'admission, multi-domaine, BGRP	[Salsano02], [Engel03], [Nikolouzou03], [Dabrowski03]
TEQUILA	Traffic engineering, end-to-end provisioning, SLS	[Trimintzios02], [Flegkas02], [Trimintzios03]
CADENUS	provisionnement, médiation de service, middlebox	[Cortes03]
MESCAL	QoS inter-domaine, ingénierie de trafic, composition de CoS	[Howart05], [Levis05], [Boucadair05], [Howart06]
ENTHRONE	services audio-visuels, fournisseurs de	[Kourtis2004]

	contenu, MPEG-21	[Ahmed04]
DAIDALOS	mobilité, identité virtuelle, ubiquité	[Calderon06], [Roussaki07], [Doolin08]
NETQOS	automatisation, adaptation de la QoS, politiques, mono-domaine	[Miloucheva06] [Chassot06], [VanWambeke07]
EUQOS	QoS de bout-en-bout, signalisation, réseaux hétérogènes, multi-domaine	[Dugeon05], [Masip-Bruin07] [Cordeiro08]

Tableau 3 : Projets de recherche

1.7. Conclusion

Nos travaux visent à proposer une architecture de signalisation qui a pour but la maîtrise de la qualité de service dans un environnement Internet multi-domaine hétérogène. Le contexte ciblé est celui de la convergence sur IP du monde des télécommunications et celui des réseaux, dans une architecture unifiée. Ce chapitre a présenté un état de l'art des propositions associées à la problématique ciblée dans nos travaux :

- Les évolutions de l'Internet et les besoins des nouvelles applications ;
- Les paramètres et les métriques de la qualité de service ;
- La maitrise de l'hétérogénéité d'un environnement multi-domaine ;
- Les architectures de nouvelle génération ;
- La signalisation inter-domaine comme support pour le provisionnement et le contrôle d'admission.

Le Tableau 4 résume les différentes propositions suivant les critères dégagés précédemment : le provisionnement, le contrôle d'admission et la signalisation. Nous rappelons ensuite le positionnement des travaux décrits par la suite dans ce mémoire. Les limitations principales de ces propositions se manifestent dans un premier temps dans l'ignorance du contexte multi-domaine et sur les considérations de l'homogénéité sur les équipements au long du chemin de données. Les mécanismes de réservation de ressources ne sont pas couplés avec un contrôle d'admission ou un provisionnement dynamique à la demande. Les solutions proposées privilégient la mise en place au préalable des dispositifs qui fixent les services et les performances sur le chemin des données.

	Provisionnement	***Contrôle d'admission***	***Signalisation***
Travaux connexes	- Statique : basé sur politiques : projets TEQUILA et CADENUS ; Agent de contrôle : projet AQUILA, tunnels (pipes) [Mantar04], Classe de services étendus [Howart05], ENTHRONE - Dynamique : intra-domaine [Hadadou06], inter-domaine [Füzesi03], avec des messages de probation [Yang03]	- Basé estimation [TEQUILA], agent de contrôle [AQUILA]; - CAC sur les systèmes d'extrémité [Kelly00], [Yang04] ; - Centralisé [Nichols99] [Jia01]	Applicative : • SIP • H323 • RTSP - Couplée au chemin de données : • RSVP, • NSIS, • YESSIR, • BGRP - Découplée du chemin de données : • SIBBS, • COPS-SLS.

Positionnement de nos travaux	- Provisionnent dynamique, à la demande - Dans le cadre du projet EuQoS, « loose model » et «hard-model »	Contrôle d'admission hiérarchique, distribué, basé sur la réservation des ressources avec une basé de données	- Signalisation complètement découplée du chemin de données, entre les BBs - signalisation hybride dans le contexte NSIS, HyPath

Tableau 4 : Résumé état de l'art

Bien que la communauté de recherche soit très active sur les protocoles de signalisation, le déploiement multi-domaine dans les réseaux reste limité. D'une part les obstacles techniques ont retardé la mise en place, d'autre part la réticence des opérateurs qui préfèrent encore attendre et s'appuyer sur le surprovisionnement avec les avancées dans la fibre optique. Il est à noter aussi que les modèles de marché (« business models ») actuels ne sont pas encore adaptés pour une négociation dynamique de la QoS.

Les travaux décrits dans cette thèse s'articulent autour du thème de la signalisation inter-domaine, signalisation qui vise le provisionnement et le contrôle d'admission. Nous traitons la signalisation inter-domaine en étendant le modèle de Bandwidth Broker (BB). Cette communication entre les BB pose un problème d'identification du prochain BB sur le chemin de données. L'avantage d'une telle approche est qu'elle permet d'avoir une vision globale sur la disponibilité des ressources au niveau de chaque domaine. Une deuxième contribution de nos travaux a été proposée dans le cadre de NSIS (conjointement avec l'Université de Coimbra) et vise à répondre au problème d'hétérogénéité dans un environnement multi-domaine lorsque ces domaines n'implémentent pas tous la solution NSIS.

Une contribution importante de cette thèse a été réalisée dans le cadre du projet EuQoS, en particulier sur l'approche de signalisation. Nous avons participé à la spécification, à l'implémentation et aux tests des solutions proposées par l'architecture EuQoS. Ces contributions seront détaillées dans les chapitres 3 et 4.

Notre solution vise à offrir et maitriser une qualité de service et se positionne sur les différents points suivants :

- Sur le plan du provisionnement des services, notre proposition repose dans un premier temps sur l'invocation dynamique de services bien connus (General Well Known Services - GWKS) dans le cadre du projet EuQoS. Dans un deuxième temps, nous étendons ce contexte en considérant que les services et leurs performances ne sont pas connus à l'avance, donc une découverte est nécessaire, suivi du choix et de l'invocation de la concaténation la mieux adaptée ;
- Concernant le contrôle d'admission, nos travaux ne s'intéressent pas particulièrement aux algorithmes de mise en œuvre ; nous proposons un CAC hiérarchique et distribué sur les domaines traversés, basé sur un dépôt de connaissances (base de données qui contient une représentation de la topologie du domaine) des ressources, qui vise à répondre rapidement à une requête de service sans les réserver physiquement. Ce mécanisme consiste à avoir une vision haut-niveau de la disponibilité des ressources dans le domaine entre chaque paire de points d'entrée et de sortie.
- Sur le plan de la signalisation, nous proposons un protocole de signalisation « off-path » entre des entités en charge de la gestion des domaines (AS). Ce protocole est intégré dans une architecture dont font partie les mécanismes évoqués aux points précédents. De plus, nous avons participé avec l'Université de Coimbra dans le cadre

du groupe de travail NSIS de l’IETF à la proposition d’une solution qui a pour but de répondre au problème d’hétérogénéité des domaines qui implémentent le protocole NSIS et de ceux qui le font pas.

Nos propositions ont pour but aussi d’introduire le minimum de contraintes pour les administrateurs de domaines par le découplage des signalisations intra et inter-domaine, le contrôle d’admission basé sur une cartographie de haut niveau de la disponibilité des ressources, et la définition des interfaces sans imposer une implémentation spécifique à l’intérieur du domaine.

2. Contributions à la signalisation pour la qualité de service dans l'Internet multi-domaine

Ce chapitre présente nos contributions à la signalisation pour la QoS dans l'Internet multi-domaine. Ces contributions consistent en :

- une proposition de protocole de signalisation découplée du chemin de données (signalisation « off-path ») ;
- une proposition de protocole de signalisation hybride, à la fois couplée (« on-path ») et découplée (« off-path ») du chemin de données, visant à permettre la coexistence de domaines NSIS et non-NSIS. Cette proposition s'inscrit dans le cadre du groupe de travail NSIS de l'IETF et a été mené conjointement avec l'Université de Coimbra, Portugal ;
- une proposition de provisionnement à la demande qui vise à découvrir dynamiquement les services disponibles au long du chemin de données, puis à sélectionner la séquence de classes de service (une par domaine et non forcément la même pour l'ensemble des domaines impliqués) la plus adaptée aux besoins en QoS et aux exigences / préférences des utilisateurs ou des fournisseurs de service ;
- une étude pour le déploiement de la signalisation précédente dans un environnement mobile. Ces travaux récents visent à répondre au problème de la continuité de la QoS suite à la mobilité en y intégrant la signalisation pour la réservation des ressources.

Les deux premières propositions ont été appliquées dans le cadre du projet EuQoS (présenté dans le Chapitre 3). La troisième proposition est issue des travaux antérieurs du groupe OLC du LAAS-CNRS que nous étendons par : 1) la formalisation d'un modèle de découverte et de concaténation des classes de services, 2) l'adaptation de la signalisation pour la prise en compte des besoins associés et 3) l'évaluation en simulation des bénéfices induits. La quatrième contribution concerne des travaux récents réalisés dans le cadre d'une collaboration avec l'Université de Santa Catarina du Brésil.

Ce chapitre est structuré de la manière suivante :

- La section 2.1 expose d'abord le contexte et les hypothèses sous jacentes à nos travaux, puis présente le cadre architectural dans lequel s'inscrivent nos propositions.
- La section 2.2 présente la proposition de protocole de signalisation « off-path » et sa spécification en UML 2.0 ;
- La section 2.3 présente notre approche de provisionnement de service dynamique qui repose sur la signalisation précédente.
- En section 2.4, nous présentons notre proposition de signalisation hybride couplée/découplée du chemin de donnée dans le cadre de NSIS.
- Enfin, la section 2.5 présente des travaux en cours qui visent à intégrer la signalisation proposée dans un contexte de mobilité.

2.1. Contexte des travaux

Actuellement, aucune des propositions existantes dans la littérature ne répond complètement au problème de la garantie de qualité de service dans l'Internet. La difficulté provient d'une part de la diversité des applications (et par conséquent de leurs besoins) et d'autre part de la

structure de l'Internet, hétérogène à plusieurs niveaux. Par définition multi-réseau et multi-domaine, l'Internet actuel (et futur) est devenu multi-technologie et multi-service. Garantir la qualité de service nécessite de tenir compte de la nature très hétérogène et dynamique de l'Internet. De plus, il est essentiel de définir de nouveaux systèmes et mécanismes dans l'Internet pour prendre en compte et maîtriser la QoS.

Notre proposition est basée sur quelques règles fondamentales de conception :

- Un tel système complexe ne peut pas être développé sans concevoir l'architecture de manière globale en définissant à la fois les composantes fonctionnelles et leurs interfaces ;
- Etant donné la distribution géographique et l'hétérogénéité de l'Internet, une solution identique pour tous les sous-systèmes ne peut pas être retenue ; il est par exemple nécessaire de prendre en compte l'hétérogénéité des technologies sous-jacentes dans chaque domaine.
- Dans la réalisation de l'architecture, seulement les interfaces principales seront définies dans le but de laisser un degré de liberté significatif aux opérateurs, aux administrateurs des domaines, mais aussi aux concepteurs des solutions.

2.1.1. Définitions

Exposons d'abord quelques définitions sur lesquelles reposent nos propositions.

1. *Domaine à QoS*. Un domaine à QoS est un domaine qui offre des garanties de qualité de service (par exemple sur le débit borné, sur le débit, etc.).

2. *Domaine sur provisionné (Over provisionned Domain)*. Un domaine « surprovisionné » est un domaine capable d'acheminer toute communication vers le domaine suivant en introduisant une modification bien définie et acceptée des propriétés de QoS. Par conséquent, le domaine dispose des ressources nécessaires pour répondre aux besoins de tous les flux le traversant, quels que soient les points d'entrée et de sortie.

Soit :

- R l'ensemble des routeurs de bordure du domaine D ;
- N le nombre de routeurs de bordure ;
- R_i et R_j deux routeurs de bordure, $i, j \in \{1,..N\}$;
- C l'ensemble des communications qui traversent le domaine D ;
- $C_{IN}(k)$ (respectivement $C_{OUT}(k)$) une communication qui rentre (respectivement sort) du domaine D ;
- $\Pr op\ (C_{IN}(k))$ les caractéristiques de la communication rentrante $C_{IN}(k)$;

Il vient alors que :

$$\forall R_i, \forall R_j, \forall C_{IN}(k) \text{ avec } \Pr op_i(C_{IN}(k)) \text{ alors}$$
$$\lambda_1 \le (\Pr op_i(C_{OUT}(k))) = F_j(\Pr op_i(C_{IN}(k))) \le \lambda_2$$

où la fonction F définit une modification des caractéristiques de la communication et $\lambda_1 et \lambda_2$ sont les seuils définis et garantis. En d'autres termes, quel que soit le point d'entrée R_i d'une communication $C_{IN}(k)$, qui a les propriétés $\Pr op_i(C_{IN}(k))$, le domaine est apte à transférer cette communication vers les prochains domaines via un point de sortie R_j en insérant une

modification des caractéristiques $F_j(\Pr op_i(C_{IN}(k)))$ bornée. Par exemple, le délai entre les routeurs R_i et R_j est borné, garanti et inférieur à une valeur bien définie.

3. *Domaine Contrôlé (Controlled Domain)*. Un domaine contrôlé n'est pas surprovisionné mais il dispose d'une fonction de contrôle qui permet de filtrer et de sélectionner un sous ensemble de toutes les communications entrantes que le domaine est capable d'acheminer avec une modification connue et acceptée.

Sous les mêmes hypothèses que dans le point précédent, on considère un sous ensemble de communications $C^* \subseteq C$ tel que :

$$\forall R_i, \forall R_j, \forall C^*_{IN}(k) \text{ avec } \Pr op_i(C^*_{IN}(k))$$
$$\lambda_1 \le F_j(\Pr op_i(C^*_{IN}(k))) \le \lambda_2$$

Il en résulte qu'un domaine à QoS est soit un domaine sur provisionné, soit un domaine contrôlé. Pour garantir la QoS sur le chemin de données, tous les domaines traversés doivent être des domaines à QoS (soit contrôlés soit surprovisionnés). Dans l'Internet, la séquence des domaines suivis par les données est obtenue par le protocole BGP (Border Gateway Protocol), le protocole de routage inter-domaine «de-facto» de l'Internet. Par conséquent, afin d'être facile à déployer, nos propositions reposent sur l'utilisation des informations du protocole BGP, en particulier celles relatives à la séquence des domaines traversés par la communication. Notons cependant que nos propositions sont indépendantes de la version de BGP.

2.1.2. Internet multi-domaine à base de Bandwidth Broker

Notre approche de la signalisation repose sur un modèle d'Internet multi-domaines qui étend le concept de Bandwidth Broker (BB), entité déjà décrite dans la section 1.3.2.5. Le rôle principal d'un BB est de contrôler la QoS au sein de chaque domaine (en particulier dans les domaines contrôlés présentés dans les paragraphes précédents).

Les fonctionnalités remplies par un BB sont relatives à :

- la gestion des requêtes de QoS et l'allocation de ressources ;
- la réalisation du contrôle d'admission inter et intra-domaine ;
- la mise en œuvre de la signalisation nécessaire pour l'installation et la maîtrise de la QoS dans tous les domaines sur le chemin de données ;

Notons que le chapitre 3 illustre un modèle évolué de BB, implémenté dans le cadre du projet européen EuQoS et appelé Resource Manager.

2.1.3. Représentation de la topologie sous-jacente

Un de nos objectifs est de pouvoir implémenter nos propositions de signalisation sur tous les domaines indépendamment de la technologie sous-jacente. Afin de nous affranchir de la dépendance technologique, nous en proposons une représentation abstraite (cartographie).

Notre proposition d'abstraction repose sur des travaux antérieurs [Chassot03] [Auriol04] qui caractérisent les performances à l'intérieur d'un domaine par un ensemble de paramètres définis entre chaque couple de routeurs de bordure. Les performances des services (réseau) sont caractérisées par une fonction de répartition du délai. Notons que le choix de cette caractérisation ne modifie pas le fonctionnement de notre protocole de signalisation. De plus, nous ne formulons pas ici de proposition d'algorithme spécifique de contrôle d'admission,

mais laissons ouvert le choix d'un tel mécanisme pour les administrateurs du domaine. Nous considérons donc une représentation de haut-niveau de la topologie réseau physique (équipements et liens). Cette représentation est indépendante de la technologie sous-jacente et elle est sauvegardée dans une base de données gérée par le Bandwidth Broker. Nous réduisons la topologie d'un domaine aux seuls routeurs de bordure et aux liens intra et inter-domaines les reliant, en considérant les performances de ces liens. Ceci permet par la suite d'effectuer un contrôle d'admission plus rapide et par conséquent d'accélérer le processus de signalisation et de réservation des ressources.

Considérons la topologie d'un domaine (système autonome) constituée de routeurs R (routeurs de cœur R_C et routeurs de bordure R_B), des liens entre ces routeurs et des liens inter-domaines avec les routeurs R_B des domaines adjacents (L_{INT} et L_{EXT} respectivement). En conséquence, la topologie est composée d'un ensemble de routeurs et liens :

$$\tau = \{\mathrm{R}, \mathrm{L}\} = \{\langle \mathrm{R_C}, \mathrm{R_B} \rangle, \langle \mathrm{L_{INT}}, \mathrm{L_{EXT}} \rangle\}$$

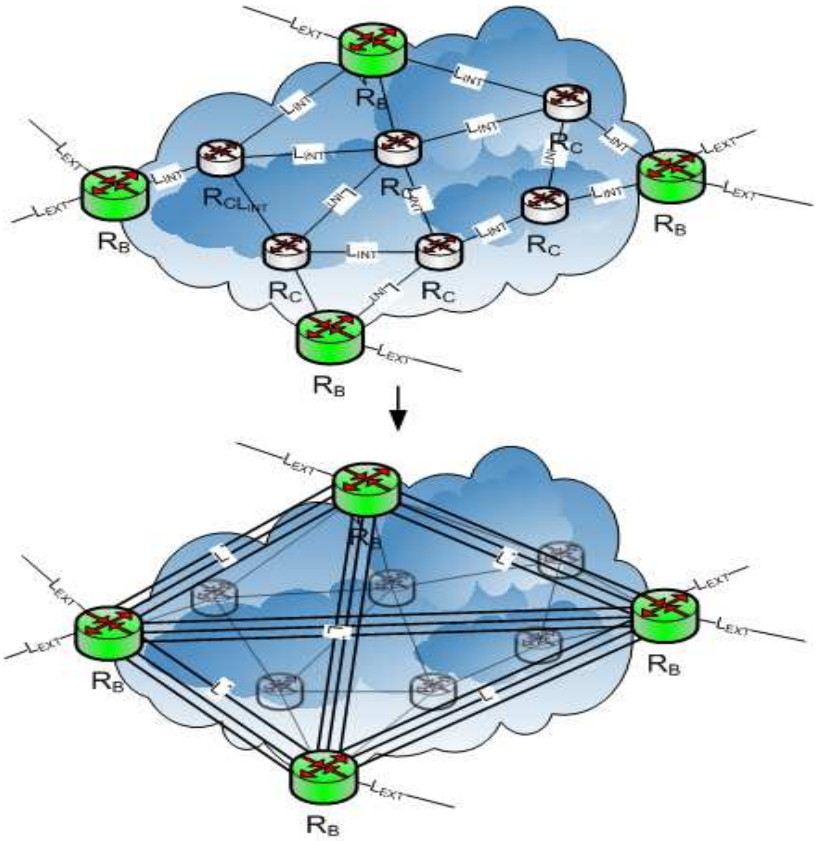


Figure 14 : Représentation de la topologie sous-jacente

Nous considérons une représentation de cette topologie réelle obtenue par l'élimination des routeurs et des liens internes. Dès lors, nous obtenons une topologie abstraite $\tau_A = \{\mathrm{R_B}, \mathrm{L}^*, \mathrm{L}\}$ où L^* désignent l'ensemble des liens entre les routeurs de bordure (c.à.d. tous les chemins possibles entre chaque paire de routeurs de bordure), voir Figure 14.

Mathématiquement, nous décrivons cette correspondance entre les deux topologies comme une projection de la topologie τ :

$$\tau_A = \mathrm{Projection}(\tau / \{R_C, L_{INT}\})$$

Notons que cette abstraction de la topologie réelle minimise de manière significative le volume de données permettant de représenter l'état du réseau et la disponibilité des ressources à un moment donné. Ceci résulte du fait que nous sauvegardons les valeurs des différentes propriétés (métriques) entre chaque paire de routeurs de bordure et non pas toute les valeurs intermédiaires entre tous les routeurs internes. Evidement, à l'intérieur de chaque domaine, la cohérence entre les deux représentations doit être gardée.

Considérons un ensemble de propriétés (bande passante, délai, taux de pertes) P sur l'ensemble τ, noté $\mathrm{P}(\tau)$.

Ces propriétés doivent vérifier la relation suivante :

$$P_k(\tau_A) \Rightarrow P_k(\tau)$$

Cela signifie que la validité d'une propriété valide sur la topologie abstraite τ_A implique la même propriété appliquée sur la topologie réelle ($P_k(\tau_A)$ est bornée, par exemple le délai est inférieur à une certaine borne max). Notons que l'exactitude de la correspondance entre les deux topologies dépend de la modélisation réalisée. Les détails d'une telle approche peuvent être trouvés en [Htira07] qui décrit un algorithme d'optimisation d'une telle correspondance.

2.1.4. Contrôle d'admission

Le contrôle d'admission est une des tâches majeures que le Bandwidth Broker doit effectuer, dans le but de décider si une nouvelle requête de QoS peut être acceptée ou non. Le contrôle d'admission peut s'appuyer sur des algorithmes variés et utiliser différentes métriques telles que le délai, le taux de perte ou la gigue. Pour répondre au problème de contrôle d'admission, nous avons suivi une approche basée sur des réservations.

Cette approche présume une réservation (par flux ou par classe) dans certains équipements réseau. Un nouveau flux est accepté si les ressources sont disponibles pour le transférer en tenant compte des réservations existantes.

Concernant l'activation de la réservation, deux types de requêtes sont considérés :

- les requêtes immédiates : la réservation des ressources est effective juste après le résultat de la réservation ;
- les requêtes en avance : les ressources sont réservées pour une utilisation ultérieure (dans un futur proche ou bien une activité périodique) et de ce fait ne demandent pas une installation immédiate. L'exemple classique de scénario qui utilise ce système de requête est la planification (périodique ou non) des audio et visioconférences.

Nos travaux se centrent principalement sur le premier schéma ; néanmoins, la signalisation que nous proposons permet de gérer les deux possibilités.

Dans notre approche, nous divisons le contrôle d'admission en deux étapes :

- Etape 1 : à partir des informations disponibles dans la base de données et d'informations de routage (topologie réseau, disponibilité des ressources, chemin emprunté par les données), un contrôle d'admission de haut-niveau est réalisé sur la base de la représentation topologique illustrée dans la section 2.1.3. Nous désignons ce procédé sous le terme de « pré-réservation ». Comme décrit auparavant, nous supposons que les indications fournies par la base de données sont cohérentes et

fiables vis-à-vis de l'état physique d'occupation des ressources sur le réseau dans le domaine (et sur les liens inter-domaines).

- Etape 2 : après avoir eu confirmation de la disponibilité des ressources sur tous les domaines impliqués dans le chemin de données (par le biais du protocole de signalisation qui propage les requêtes de BB en BB), la réservation est confirmée et les équipements réseau, en particulier les routeurs, sont configurés pour garantir les ressources au niveau dépendent de la technologie.

2.2. Signalisation découplée du chemin de données

2.2.1. Concepts généraux

Tel qu'introduit dans le chapitre 1, plusieurs propositions visant à offrir la QoS ont été avancées. Le point commun à ces propositions est la nécessité de mettre en œuvre un protocole de signalisation entre les équipements impliqués dans la gestion de la QoS, en particulier les BB dans le modèle d'Internet multi-domaine que nous considérons.

Plusieurs activités ont été menées dans le contexte des deux perspectives suivantes, illustrées dans la Figure 15 :

- la première, qui prolonge la vue RSVP, repose sue le couplage fort entre le chemin de données et le chemin suivi par la signalisation. Dans cette approche, les entités impliquées dans le processus de signalisation se trouvent forcement sur le chemin de données. On parle de signalisation couplée au chemin de donnée ou « on-path » ;
- la deuxième découple ces deux chemins de données et de signalisation et prend en compte une gestion plus hiérarchique des domaines. Les entités de signalisation peuvent ne pas être situées sur le chemin de données mais ont la connaissance de celui-ci. On parle de signalisation découplée du chemin de donnée ou « off-path » ;

Dans nos travaux, nous avons adopté l'approche off-path en considérant des domaines hétérogènes (vis-à-vis de la mise en place de la QoS suivant la technologie, de la signalisation NSIS ou non, des services, etc.) et administrés par un équipement central, le Bandwidth Broker.

Pour la signalisation découplée du chemin de données, la solution actuellement explorée dans NSIS [Hancock05b], consiste à détourner les paquets de signalisation vers des entités en charge du contrôle du réseau. En entrée d'un domaine, tout routeur de bordure intercepte les paquets de signalisation et les transmet à cette entité. Après traitement, une réponse est retournée au routeur, et la signalisation reprend (message vers la prochaine entité NSIS).

Notre proposition est différente : elle permet une communication directe entre les BB, et repose sur une utilisation des tables BGP, supposées accessible par les BB. Notons que nous avons proposé avec l'Université de Coimbra une approche hybride qui vise à combiner les deux concepts, couplé et découplé du chemin de données, dans le cadre de NSIS. Cette contribution est présentée dans la section 2.4.

Rappelons aussi que notre proposition est également indépendante de la solution de routage intra-domaine et de la technologie réseau sous-jacente.

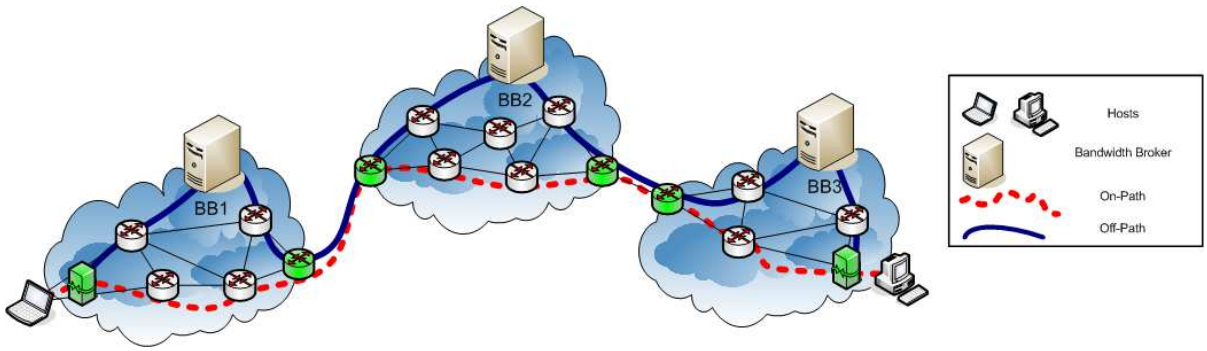


Figure 15 : Signalisation multi-domaine « on-path » et « off-path » dans l'Internet à base de BB

Notre proposition s'appuie sur les hypothèses suivantes :

- homogénéité du modèle de gestion de la QoS à l'échelle du multi-domaine. Un tel modèle comprend une méthode pour offrir des garanties pour un flux de données. Il inclut des mécanismes de provisionnement, de contrôle d'admission et une architecture. Il définit aussi le comportement des mécanismes de gestion des ressources. Nous pouvons citer des exemples de tels modèles : IntServ, DiffServ, ou bien ceux définis dans le cadre de NSIS [Bader07] [Ash08].
- connaissance, au niveau de chaque BB, de la disponibilité des ressources ainsi que des services supportés pour tout couple de routeurs de bordure ;
- unicité de décision du BB au sein chaque domaine.

Les équipements impliqués dans la signalisation sont :

- les entités qui initient la requête de ressources ; elles sont supposées clientes des domaines d'accès respectifs. Ces entités peuvent être le terminal utilisateur, un proxy ou une « home gateway »[3] [HomeGatewayInitiative08] ;
- les Bandwidth Brokers de chaque domaine ;
- les équipements réseau à configurer (en particulier le routeur de bordure d'entrée dans un domaine type DiffServ).

2.2.2. Découverte du prochain Bandwidth Broker

Le mécanisme de signalisation proposé repose sur l'échange de messages entre les BB de chaque domaine. Du point de vue d'un BB, l'identification du prochain BB est nécessaire dans le but de lui acheminer les messages de signalisation. Dans le cas d'une signalisation découplée du chemin de donnée avec interaction directe des BB, nous considérons que cette information est disponible dans une base de données locale sans précision supplémentaire sur les mécanismes dont cette information est acquise. Nous donnons dans cette section quelques solutions possibles pour l'obtention de l'identifiant (adresse IP) d'un Bandwidth Broker.

Dans le cas d'une signalisation couplée au chemin de données, ce problème est résolu simplement, car les entités se trouvent sur le chemin suivi par le message. Plusieurs approches sont possibles dans ce cas :

- utilisation de messages de tests « probe » (couplés aux protocoles de routage) ;
- utilisation des fonctionnalités évoluées des protocoles de routage (par exemple la distribution des capacités des nœuds dans OSPF) ;

[3] Un « Home Gateway » définit un équipement sous la gestion du fournisseur de service qui connecte un réseau domestique (notamment un environnement à domicile) à l'Internet (www.homegatewayinitiative.org).

- emploi d'un mécanisme de découverte de service. SLP (Service Location Protocol) [Guttman99] est un candidat pour ce type de recherche, car il permet la découverte des service dans un réseau local sans avoir une configuration préalable.

Dans le cas d'une signalisation découplée du chemin de données, le prochain Bandwidth Broker sur le chemin de données se trouve dans des domaines distincts (notés AS dans ce qui suit), administrés par des entités différentes. Une collaboration entre les AS est donc requise dans ce cas ; il s'agit donc de trouver l'identifiant (adresse IP par exemple) du BB dans le prochain AS. Rappelons que le chemin, en termes d'AS parcourus par les données, est trouvé par le biais du protocole BGP.

Chaque AS est identifié par un numéro unique attribué par IANA (Internet Assigned Numbers Authority). L'enchainement des AS entre la source et la destination est découvert en interrogeant les routeurs BGP, via le champ « AS Path ».

Plusieurs solutions sont alors envisageables pour l'identification du prochain BB :

- passage de l'identifiant du BB lors de la mise en place des accords de peering entre les AS et de leur enregistrement dans la base de données gérée par ces BB. Cette solution simple ne nécessite pas l'interrogation d'entités externes au domaine ;
- utilisation basée sur des mécanismes type DNS (Domain Name Service), qui permettent la récupération des informations (plus spécifiquement d'une adresse IP) à partir d'un nom de domaine :
  - introduction d'un nouvel espace de nom (tel que proposé dans CASP [Schulrzine03]) de type NUMERO_AS.as.nom_AS (par exemple 2200.as.renater). Plus exactement, cette procédure permet de trouver l'adresse du BB en charge d'un domaine (AS) à partir du numéro de cet AS.
  - utilisation des enregistrements définis par DNS, NAPTR [Mealling00] et SRV [Gulbrandsen00] (exploités par le protocole SIP). NAPTR (Naming Authority Pointer) donne accès à des règles de ré-écriture de l'information, permettant des correspondances entre un nom de domaine et une ressource (dans notre cas le service offert par un Bandwidth Broker). Les enregistrements SRV permettent de définir de manière générale les serveurs des services dans un domaine.

Le choix d'un tel mécanisme n'a pas d'impact sur nos propositions de signalisation. En conséquence, nous n'optons pas pour une solution particulière, laissant libre l'utilisation de celle la mieux adaptée du point de vue des fournisseurs et concepteurs de services.

2.2.3. Spécification et modélisation UML

2.2.3.1. PDU et règles d'échange

Cette section présente les différents PDU (Protocol Data Unit) de notre protocole ainsi que leur enchainement. Précisons que nous ne définissons ici que les principales informations transportées par ces messages. Le contenu de chaque PDU sera présenté dans le chapitre 3 qui fournit les détails de l'implémentation réalisé dans le cadre du projet EuQoS.

Notre protocole de signalisation inter-domaine définit six PDU :

- RESERVE : utilisé pour demander la réservation des ressources. Il contient les informations nécessaires pour l'identification du flux et la QoS requise ;
- MODIFY : utilisé pour mettre à jour une réservation existante ;

- RESPONSE : utilisé pour répondre à un message RESERVE ou MODIFY ;
- REFRESH : utilisé pour rafraichir une réservation existante.
- RELEASE : utilisé pour libérer les ressources réservées.

Trois types d'échanges sont distingués :

- le premier type concerne les échanges entre l'initiateur de la requête de réservation (terminal client, proxy ou home-gateway) et le premier BB sur le chemin de données. Ces échanges sont effectués à l'intérieur du même AS.
- le deuxième type implique les BBs de chaque domaine au long du chemin des données.
- le dernier type d'échanges intervient à l'intérieur des domaines afin de configurer les équipements réseaux pour réserver les ressources nécessaires. Ce type d'échange peut être implémenté à l'aide de protocoles standards comme COPS (Common Open Policy Service [Durham02]), SNMP (Simple Network Management Protocol [Harrington02]), TELNET (TErminaL NETwork [Postel83]) ou bien des solutions spécifiques en fonction de la technologie sous-jacente.

Concernant les échanges entre l'initiateur de la requête et le BB de son domaine, plusieurs possibilités sont illustrées dans la littérature. Nous avons étudié et implémenté différentes solutions :

- utilisation des services web basé sur le protocole SOAP/XML (réservation à partir d'une page web) ;
- utilisation de la technologie JAVA RMI (Remote Method Invocation) ;
- utilisation d'une API qui s'appuie des échanges TCP/IP (sockets) ;
- utilisation du protocole NSIS.

Notons que ces solutions ont été étudiées dans le cadre du projet EuQoS également, les services web étant retenus pour accéder aux fonctionnalités du plan de services et le protocole NSIS pour la communication avec le RM.

La Figure 16 illustre le déroulement d'une requête qui aboutit positivement :

- la vérification de la disponibilité des ressources et le contrôle d'admission sont effectués durant la phase 1.
- suite aux réponses des BBs, la réservation est entérinée par la configuration des équipements au retour, une fois les réponses arrivées.
- la phase 3 montre le maintien d'une réservation auprès d'un BB qui propage des messages REFRESH.

Le mécanisme de mise à jour des ressources est similaire à celui de réservation.

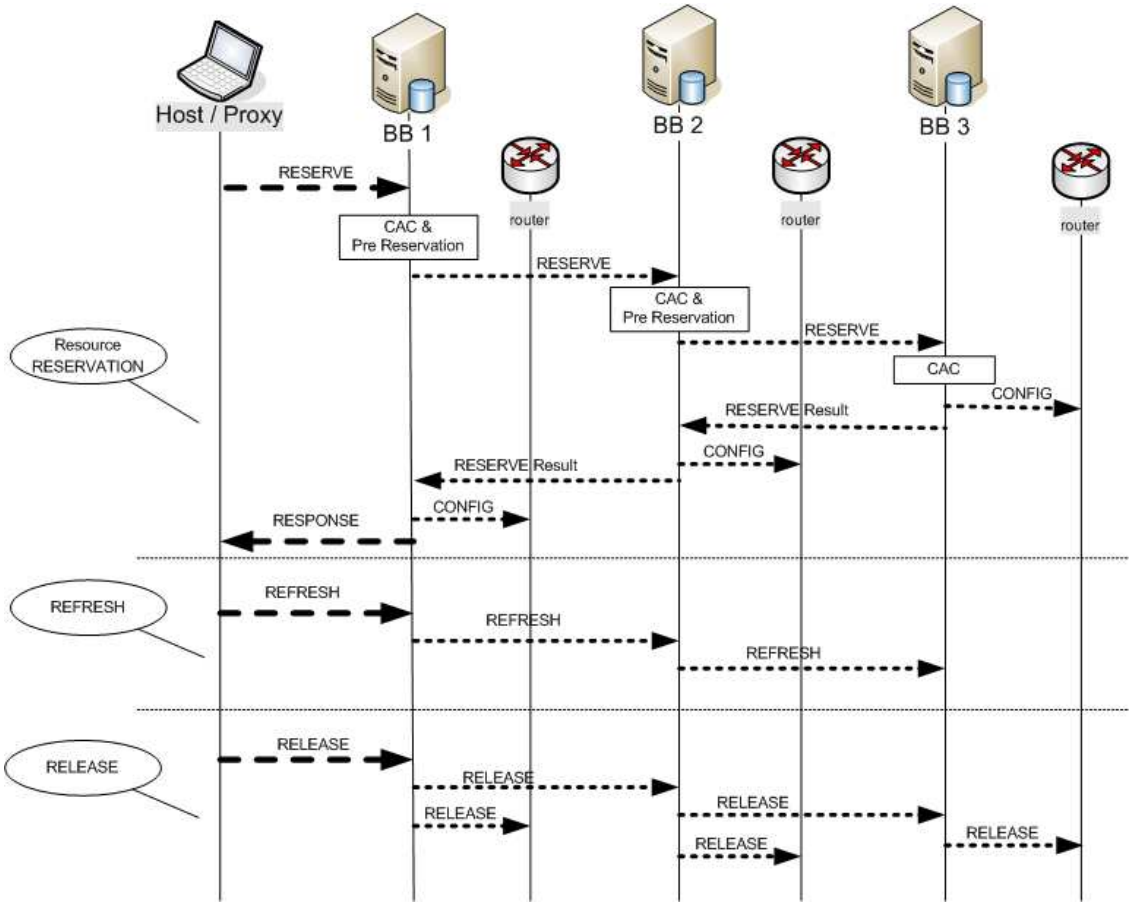


Figure 16 : Enchainement des messages de signalisation

Une des propriétés de notre protocole est le support pour la réservation initiée par le récepteur. Ce type de réservation est nécessaire pour répondre aux besoins de plusieurs applications courantes qui se développent de plus en plus sur Internet. Le scenario de réservation s'adapte par exemple à la vidéo à la demande (le récepteur initie la communication avec le serveur qui envoie flux de données) ou bien pour les réservations bidirectionnelles (visioconférence). Ce scénario est illustré dans la Figure 17.

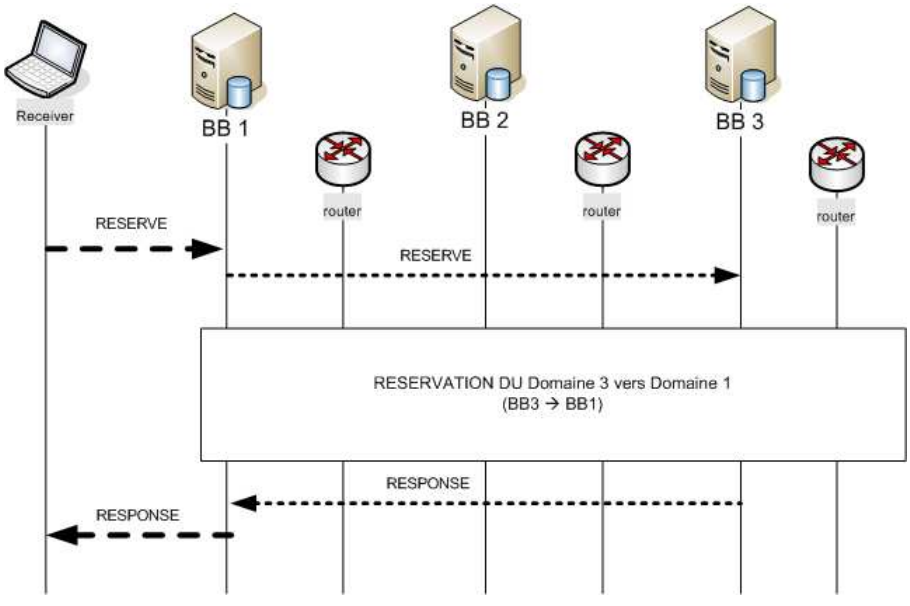


Figure 17 : Réservation initiée par le récepteur

Dans le cas d'une communication bidirectionnelle, les échanges pour la réservation dans les deux sens se déroulent en parallèle, en gardant un identifiant de session.

Nous avons choisi de spécifier et de modéliser notre architecture un utilisant UML 2.0. Cette spécification a été réalisée à l'aide de l'outil TauG2 de la société Telelogic. Notons que cet outil a été retenu également pour la spécification dans le projet EuQoS.

Nous introduisons dans un premier temps les principaux concepts liés à UML.

2.2.3.2. UML (Unified Modeling Language)

UML est un langage de modélisation graphique très utilisé, standardisé par l'OMG (Object Management Group – www.omg.org) qui repose sur l'approche objet pour la description des systèmes. Le formalisme UML est arrivé à la version 2.1.2 (novembre 2007) et l'OMG travaille à présent sur la version 2.2. UML est l'aboutissement de la fusion de plusieurs langages objet existants (Booch, OMT, OOSE), et son développent continu est soutenu par une grande communauté d'industriels et chercheurs. Il est à noter qu'UML ne se limite pas à la modélisation des logiciels, mais couvre un spectre très large de domaines comme la modélisation du processus, l'ingénierie des systèmes et encore d'autres métiers par l'introduction de profils définis dans la norme 2.0. (SysML – Systems Modeling Language ou Domain Specific Modeling).

La modélisation objet consiste à concevoir un modèle du système à réaliser suivant une approche qui décrit des objets et les relations entre eux. Ce modèle repose sur la définition des éléments du monde réel et des concepts propres au domaine applicatif auquel fait partie le système (indépendamment de sa mise en œuvre). UML offre un cadre générique et visuel de modélisation, d'analyse et de conception itératives et incrémentales, qui guide l'utilisateur à l'aide d'un formalisme graphique extensible (méta modèles, profils, stéréotypes). [OMGL07]. Remarquons qu'UML n'est pas une méthode par lui-même, il propose un cadre général sur lequel se déploient différentes méthodologies, la plus connue étant Unified Process [Kendall02].

Le modèle UML est composé de 13 diagrammes dépendants hiérarchiquement qui se complètent pour donner différentes vues du système à modéliser (voir Figure 18) :

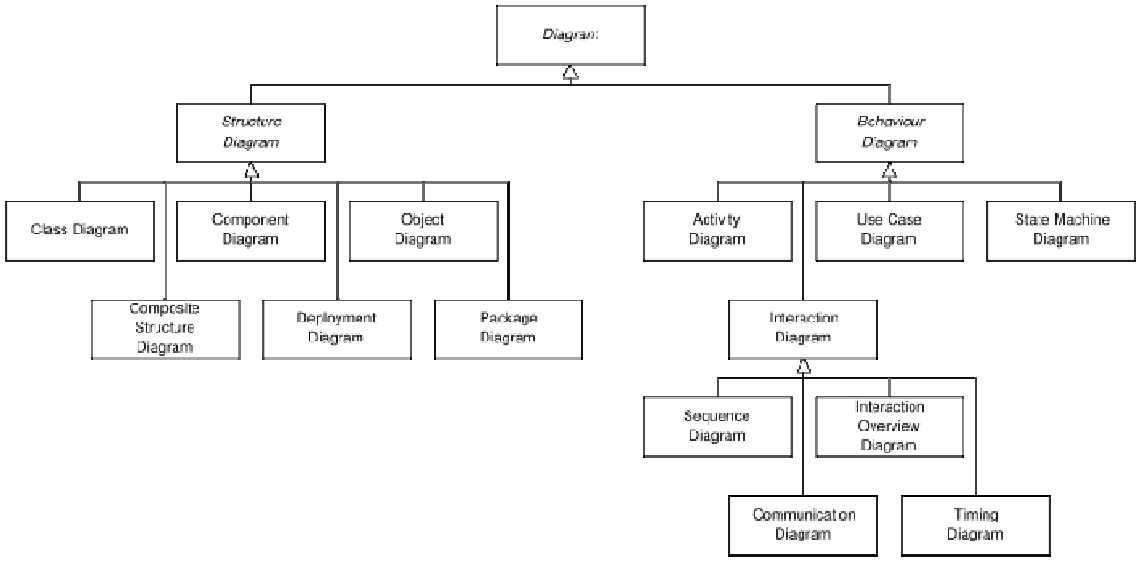


Figure 18 : Digrammes UML 2

On distingue trois types de diagrammes : structurels, comportementaux et d'interaction décrits brièvement dans les paragraphes suivants :

- Diagrammes Structurels ou Diagrammes statiques (Structure Diagram) :
  - Diagramme de classes (Class diagram) : il décrit la structure du système, les classes et leurs relations ;
  - Diagramme d'objets (Object diagram) : il sert à représenter les instances de classes (objets) utilisées dans différents contextes possibles ;
  - Diagramme de composants (Component diagram) : il permet d'illustrer le système divisé en composants (fichiers, bibliothèques, bases de données...) ;
  - Diagramme de déploiement (Deployment diagram) : il sert à représenter les éléments matériels (ordinateurs, périphériques, réseaux, systèmes de stockage...) et la manière dont les composants du système sont répartis sur ces éléments matériel ainsi que leurs interactions ;
  - Diagramme des paquetages (Package Diagram) : un paquetage étant un conteneur logique permettant de regrouper et d'organiser les éléments dans le modèle UML, ce diagramme sert à représenter la hiérarchie des paquetages ainsi que les dépendances entre paquetages ;
  - Diagramme de structure composite (Composite Structure Diagram) : il permet de décrire la structure interne des classes (boîte blanche) et les relations entre les sous-composants d'une classe ;
- Diagrammes Comportementaux (Behavior Diagram) :
  - Diagramme des cas d'utilisation (Use Case Diagram) : il permet de délimiter le système, d'identifier les fonctionnalités qu'il doit fournir et les possibilités d'interaction entre le système et les acteurs (intervenants extérieurs au système) ;
  - Diagramme états-transitions (State Machine Diagram) : il permet de décrire sous forme de machine à états finis le comportement du système et l'évolution de ses composants.
  - Diagramme d'activité (Activity Diagram) : il permet de décrire sous forme de flux ou d'enchaînement d'activités le comportement du système ou de ses composants.
- Diagramme d'interactions ou Diagrammes dynamiques, un sous-ensemble de diagrammes comportementaux (Interaction Diagram) :
  - Diagramme de séquence (Sequence Diagram) : représentation chronologique du déroulement des traitements et des messages échangés entre les éléments du système et/ou de ses acteurs ;
  - Diagramme de communication (Communication Diagram) : représentation simplifiée des informations combinées du diagramme de classe et de séquence se concentrant sur les échanges de messages entre les objets ;
  - Diagramme global d'interaction (Interaction Overview Diagram) : permet de décrire les enchaînements possibles entre les scénarios préalablement identifiés ;
  - Diagramme de temps (Timing Diagram) : permet de décrire le comportement des objets ou données au cours du temps.

Ces diagrammes sont d'une utilité variable selon les circonstances et ne sont pas nécessairement tous produits lors d'une modélisation. De plus amples détails sur l'utilisation d'UML sont disponibles dans [Doldi03] [Roques06].

Nous présentons ci-après la spécification de notre proposition de protocole de signalisation en utilisant dans un premier temps les diagrammes de cas d'utilisation, de séquence, et d'état transition, les plus utilisés en UML. Dans les chapitres suivants, nous décrivons aussi les diagrammes de classe, de paquetage ainsi que le diagramme de structure composite utilisé par l'outil TauG2 dans la simulation de notre modèle.

2.2.3.3. Spécification des cas d'utilisation

Dans un premier temps nous présentons le diagramme des cas d'utilisation. Ce diagramme a pour objectif de délimiter le système et d'illustrer les interactions avec le monde extérieur (voir Figure 19).

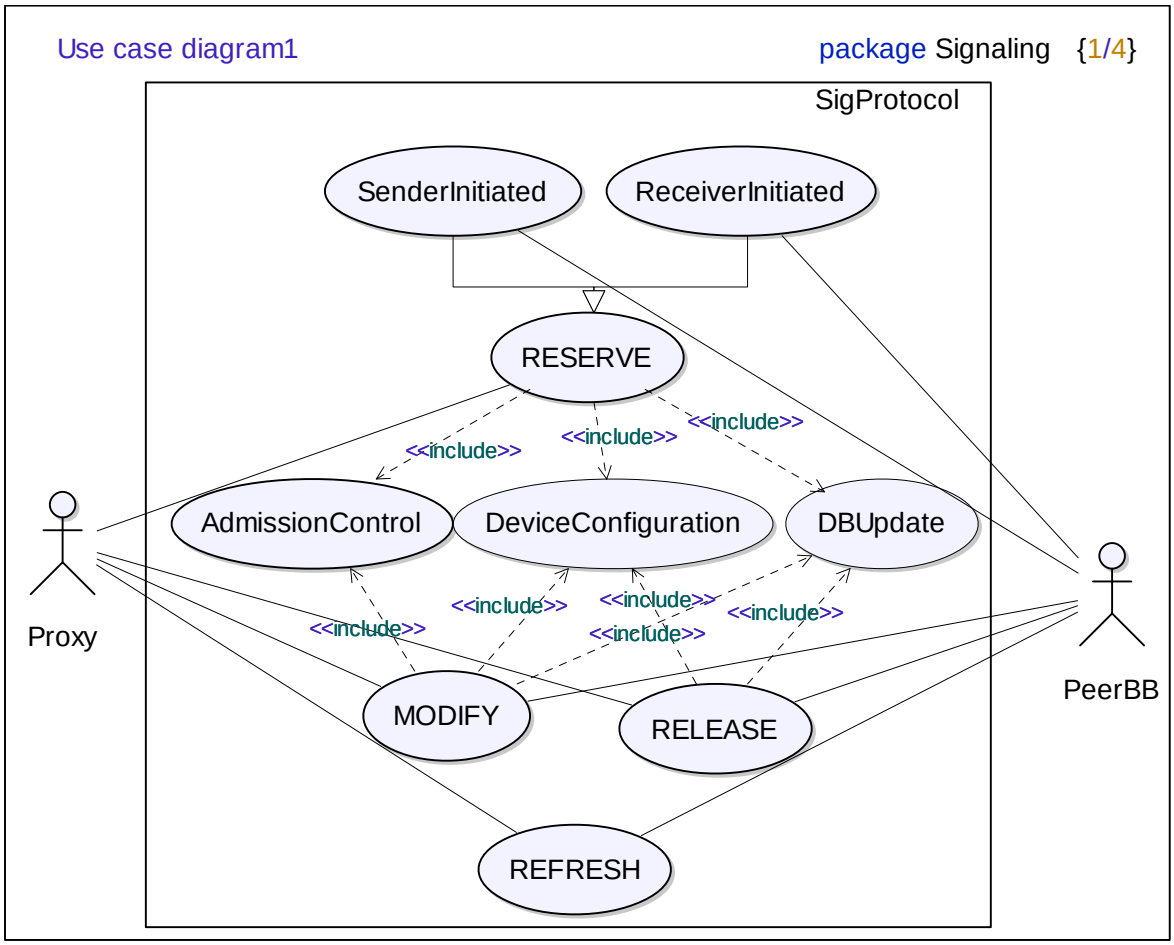


Figure 19 : Diagramme de cas d'utilisation BB

Une application peut demander au système de réserver (RESERVE) ou de libérer (RELEASE) les ressources nécessaires à ses besoins. Dans les cas d'une communication bidirectionnelle ou bien pour certaines applications dont le flux de données est descendant (d'un serveur vers un client, telle que les applications de vidéo à la demande), la réservation est initiée par le récepteur des données. Le BB peut aussi être invoqué par un autre BB (d'un domaine avec lequel il a un contrat de service).

Notons que des sous cas d'utilisation peuvent intervenir dans les processus de réservation ou libération : contrôle d'admission, configuration des équipements, mise à jour des bases de données.

2.2.3.4. Spécification des diagrammes comportementaux

L'enchainement des messages entre les BB est décrit dans les diagrammes de séquence suivants. La Figure 20 décrit les PDU échangés entre les BB des domaines impliqués dans la communication (nous prenons également un exemple avec trois domaines identique à celui illustré dans les paragraphes précédents).

Suite à l'invocation du service de réservation (requête RESERVE), chaque BB évalue la disponibilité des ressources sur son domaine (et le lien inter-domaine). Les requêtes sont acheminées ensuite jusqu'au BB du dernier domaine le long du chemin. Les confirmations (RESPONSE) sont ensuite propagées et la réponse et retournée à l'entité qui a initié la réservation (application ou proxy).

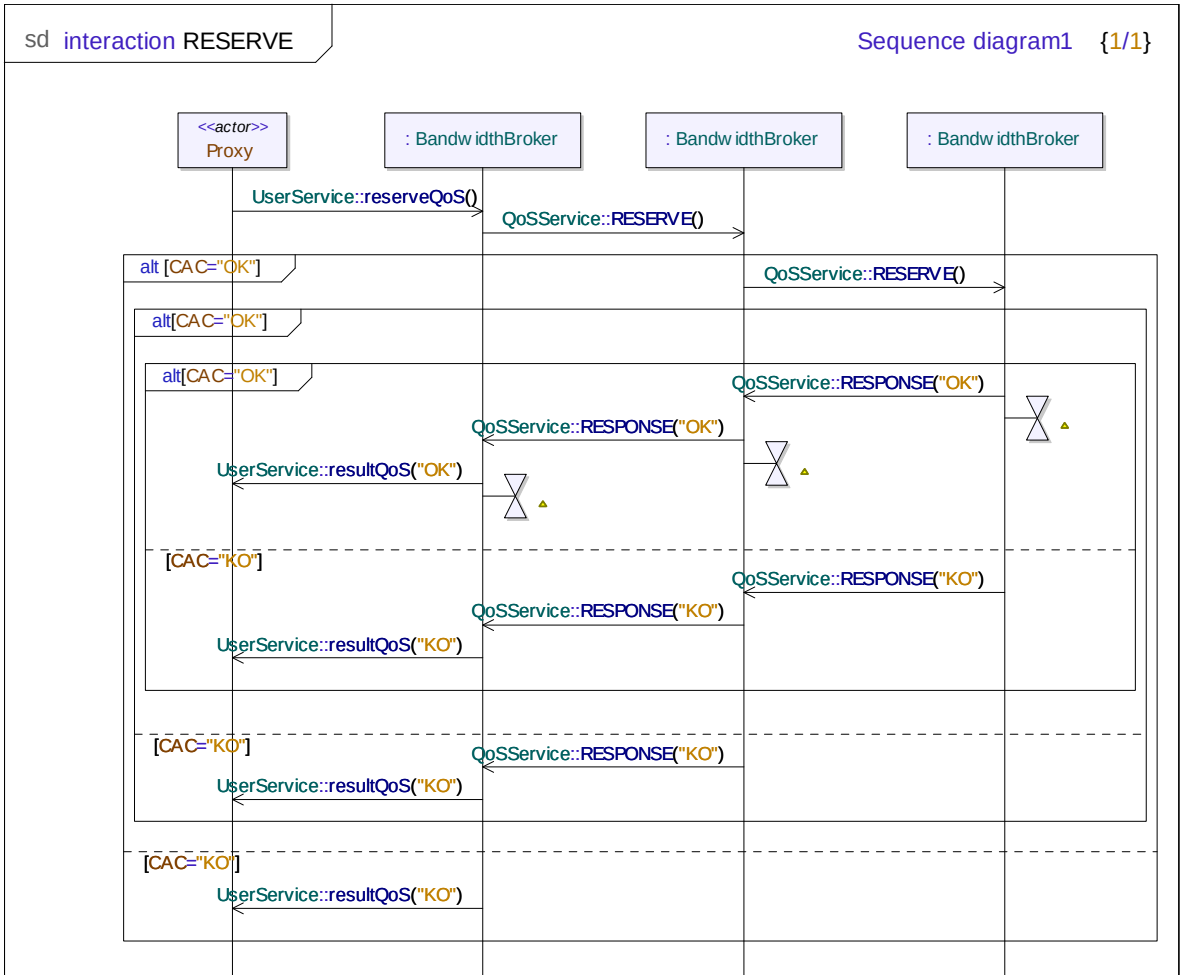


Figure 20 : Diagramme de séquence: réservation

Le diagramme précédent (Figure 20) expose également les cas où la réservation n'a pas abouti (requête non conforme au contrat, ressources non disponibles, etc.). Dans ce cas, le BB informe l'émetteur de l'échec – le message RELEASE(KO) en remonte jusqu'au domaine d'origine – et toutes les pré-réservations sont relâchées. Nous remarquons également l'activation d'un minuteur après chaque réservation les états étant rafraichis périodiquement. Cette procédure ainsi que celle de libération de ressources est illustrée dans la Figure 21.

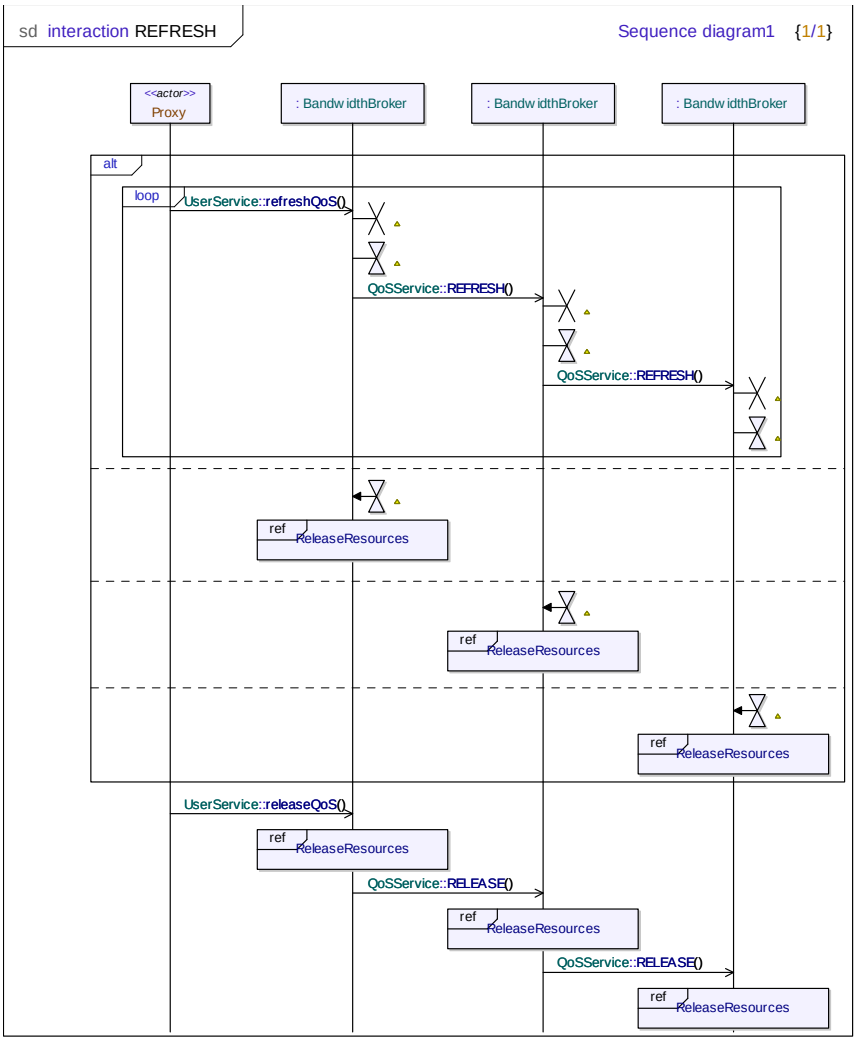


Figure 21 : Diagramme de séquence libération des ressources

Le comportement de chaque BB est décrit par les diagrammes d'état de la Figure 22 qui reprend le comportement dans le cas d'une réservation et illustre les transitions entre les différents états du BB. Suite à la réception d'une requête de réservation de ressources, chaque BB effectue les actions suivantes :

- il vérifie que la requête respecte le contrat de service entre son domaine et le client émetteur de la requête ;
- il évalue la disponibilité des ressources dans son domaine et sur le lien inter-domaine ;
- dans le cas où les ressources sont disponibles, une pré-réservation des ressources est mise en place ;
- il identifie le prochain BB et lui propage la requête de réservation.

Dans le cas d'une réservation réussie dans tous les domaines, une réponse positive – RESPONSE(OK) – est remontée de proche en proche par chaque BB. La réservation est entérinée (via le module d'allocation) ce qui entraine une configuration des différents équipements réseau pour garantir la QoS pour les flux respectifs.

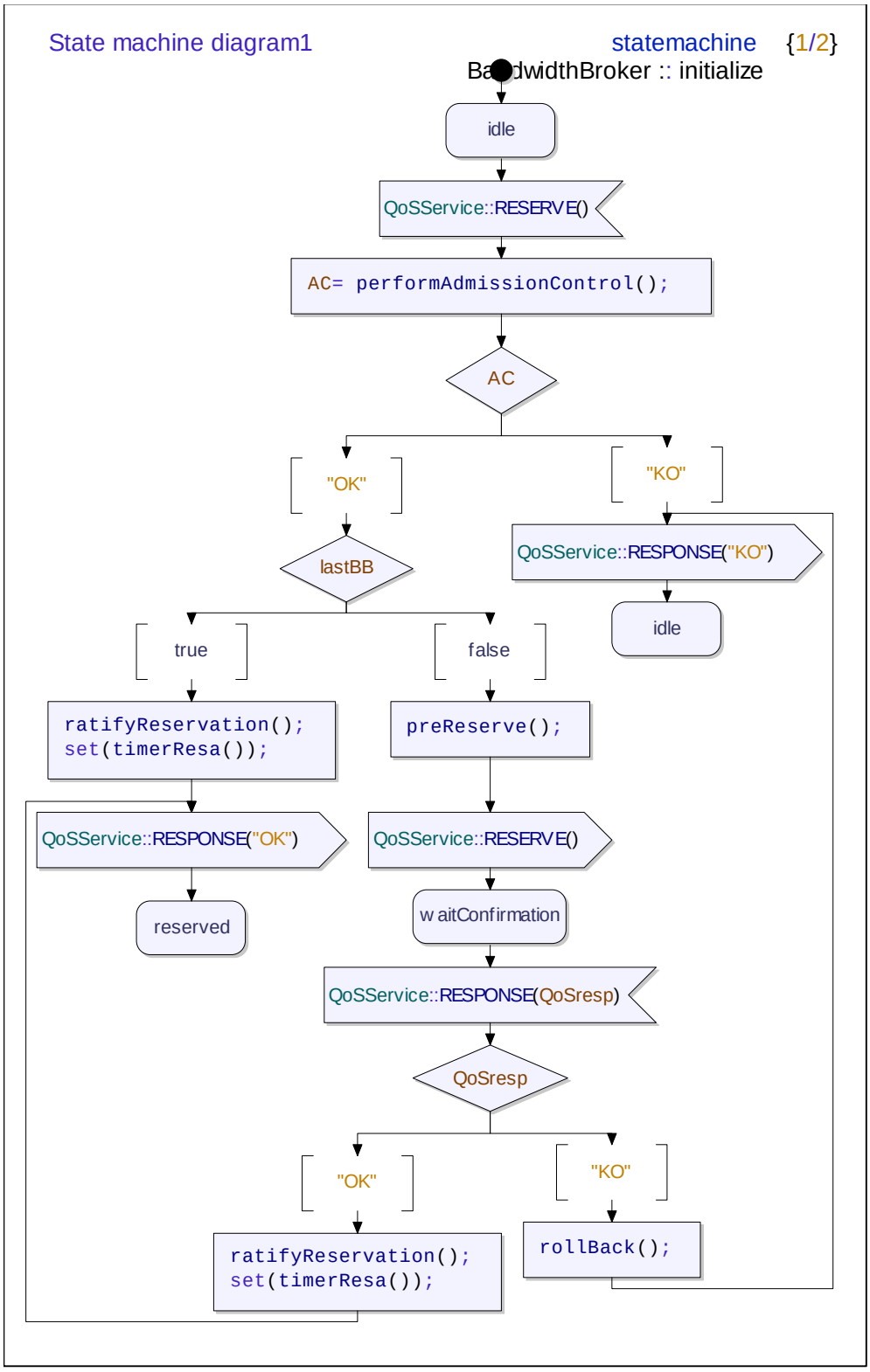


Figure 22 : Diagramme d'état réservation

Le rafraichissement et la libération des ressources sont décrits dans le diagramme état transition illustré dans la Figure 23.

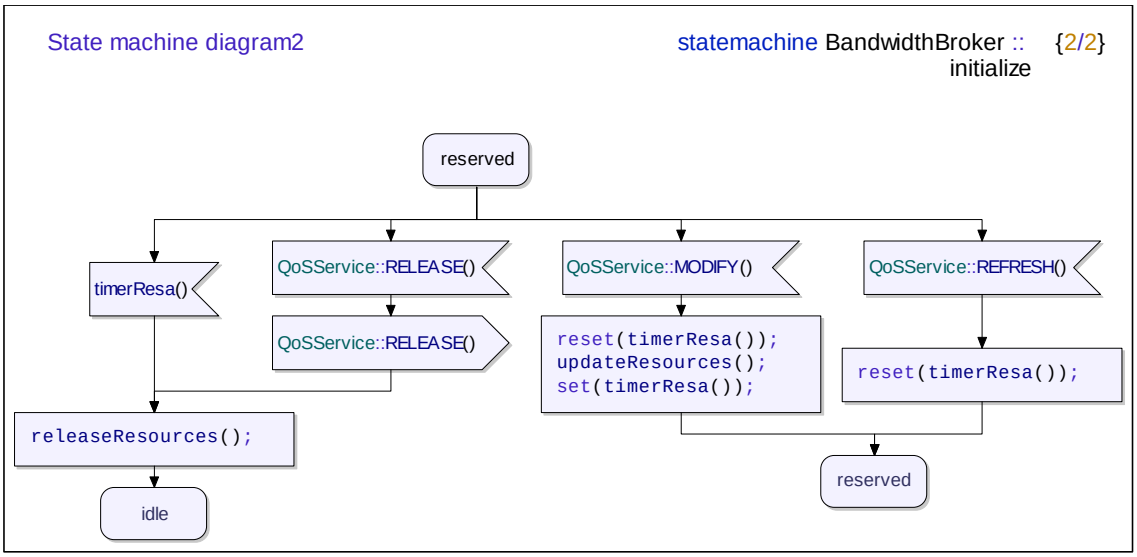


Figure 23 : Diagramme d'état – comportement de BB

2.2.4. Prise en compte des domaines surprovisionnés

Dans cette section, nous montrons comment gérer la prise en compte de domaines surprovisionnés. Ces domaines disposent des ressources nécessaires pour assurer la QoS, mais ne sont pas nécessairement administrés par un Bandwidth Broker.

Si un BB est configuré dans un domaine surprovisionné (ayant comme fonctionnalité par exemple d'accepter toutes les requêtes entrantes, avec les considérations d'autorisation, authentification et sécurité adjacentes), toutes les opérations décrites dans la section 2.2.3.1 restent valables. La signalisation détaillée précédemment s'applique sans aucun changement (Figure 24).

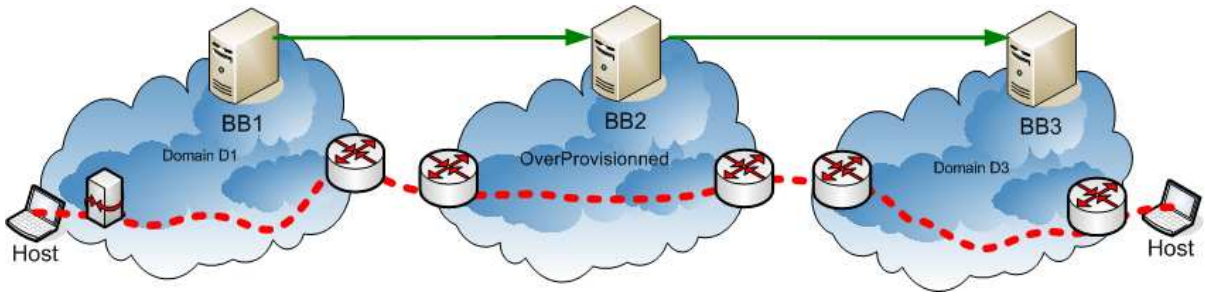


Figure 24 : Domaine surprovisionné avec Bandwidth Broker

Si un domaine surprovisionné n'est pas géré par un BB, alors plusieurs difficultés surviennent : ce domaine ne participe pas à la signalisation inter-domaine, découverte d'un BB d'un domaine non adjacent, contrôle d'admission sur les liens inter-domaines.

Une première solution repose sur la capacité d'un BB à récupérer l'adresse d'un Bandwidth Broker d'un domaine non adjacent (en utilisant par exemple un des mécanismes présentés dans le paragraphe 2.2.2). A partir de la connaissance des types de chaque domaine (contrôlé ou surprovisionné) au long du chemin, un BB peut propager les messages de signalisation à un autre BB après un domaine surprovisionné. Rappelons que la succession des AS traversés jusqu'à la destination est obtenu par le biais du protocole BGP. La signalisation est donc transparente au niveau des domaines surprovisionnés (voir Figure 25). Toutefois un contrôle d'admission reste à la charge des deux BB pour les liens inter-domaines. Notons que le trafic

injecté dans un domaine est soumis aux contraintes spécifiées dans les SLA entre les domaines.

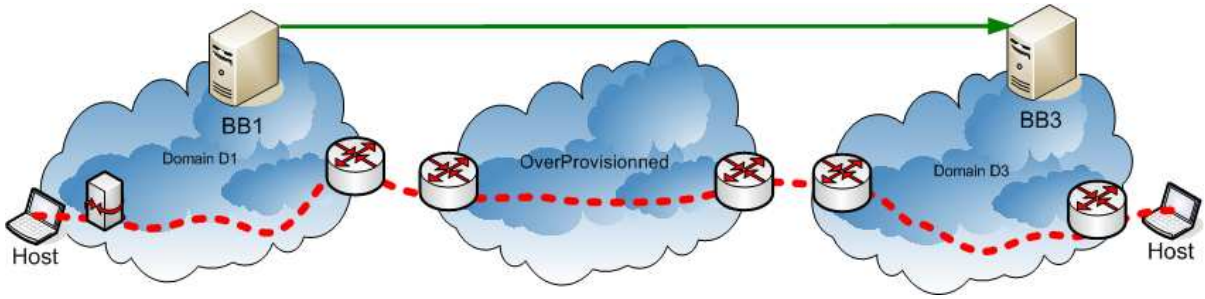


Figure 25 : Domaine surprovisionné sans Bandwidth Broker

Une autre solution repose sur la participation active des domaines surprovisionnés. Il s'agit de créer des tunnels (MPLS par exemple) entre les domaines qui encadrent les domaines surprovisionnés. Ces tunnels, activés à la mise en place des SLAs ou bien créés dynamiquement, sont établis entre les routeurs de bordure des domaines contrôlés. La Figure 26 illustre cette approche.

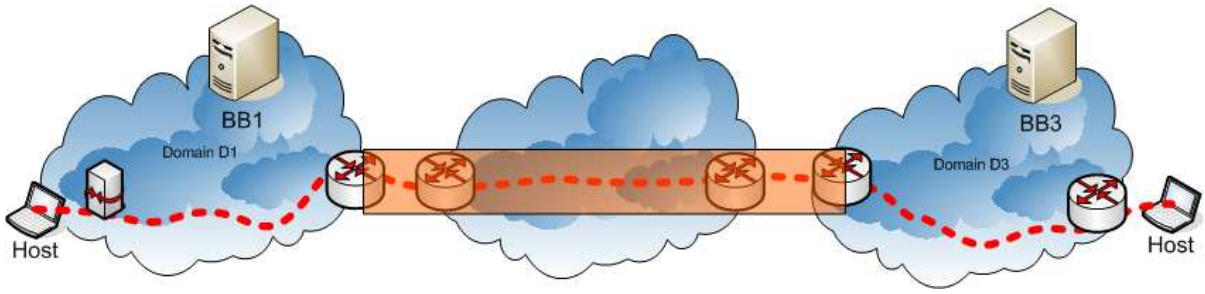


Figure 26 : Domaines surprovisionnés avec tunnel

Un tunnel ainsi créé peut être interprété comme un lien inter-domaine (avec des caractéristiques de QoS bien définies) entre les domaines 1 et 3, les deux domaines étant considérés comme adjacents du point de vue du protocole de signalisation. Les messages de signalisation sont donc échangés entre les BB de ces domaines, configurés préalablement pour prendre en compte ce changement. Plus de détails sur la mise en place d'une telle solution (mise en place des tunnels avec de performances bien définies entre les routeurs de bordure de deux AS) sont fournis dans le chapitre 3 qui présente l'approche du provisionnement dite « hard-model », étudiée dans le projet EuQoS.

2.3. Sélection dynamique des classes de services

Cette section aborde le provisionnement dynamique des services dans un environnement multi-domaines. Nous y proposons une solution qui repose sur la signalisation précédente, dans un contexte de routage non orienté QoS. L'approche est de construire, au moment de la requête d'invocation, le service le mieux adapté résultant de la concaténation des classes de service (CoS) offertes par les domaines situés sur le chemin de donnée.

2.3.1. Introduction

Afin de garantir une QoS de bout-en-bout dans l'Internet, il est impératif de prendre en compte l'hétérogénéité des services offerts par les domaines au long du chemin de données. Il en résulte qu'un choix de concaténation des services répondant aux besoins en QoS des utilisateurs doit être fait. Ce choix est une partie du provisionnement des services et fait

l'objet de cette section. Notre proposition nécessite d'adapter la signalisation pour permettre la découverte des classes de services (CoS) sur chaque domaine. Le choix de concaténation de ces CoS est fonction des besoins en QoS à satisfaire et des différents critères de préférences (orientés utilisateur ou fournisseur).

Comme présenté dans le chapitre 1, deux solutions sont étudiées pour considérer le provisionnement de bout-en-bout :

- la première adopte une approche statique, dans laquelle les fournisseurs offrent des services avec des performances prédéfinies ;
- la deuxième solution suit une approche « à la demande » et vérifie dynamiquement les propriétés du service de bout-en-bout qui répondent aux conditions requises par les applications. L'idée est d'invoquer au moment de l'expression de la requête, le service qui répond le mieux aux nécessités de QoS.

Notre proposition s'inscrit dans le deuxième point de vue, en considérant une concaténation des services basée sur l'expression quantitative des besoins en QoS. Nous proposons un modèle de provisionnement dynamique, qui permet de rapatrier les caractéristiques des services au long du chemin, de choisir la concaténation la mieux adaptée et d'invoquer ensuite le service ainsi obtenu.

Par rapport à la section 1.4.1, notre contribution diffère de [Füzesi03] qui propose aussi un provisionnement dynamique, par le fait que le choix de concaténation est effectué au moment de la requête de QoS et non à la souscription. De plus, nous décrivons un modèle de caractérisation des services applicable à l'échelle du multi-domaine. Nous suivons une approche similaire à [Yang05] mais dans un contexte multi-domaine hétérogène.

Le provisionnement dynamique s'appuie sur un protocole de signalisation couplé à un algorithme optimisé de sélection de la meilleure concaténation de service qui (1) répond aux besoins en QoS des flux et (2) respecte un ensemble de préférences bien définies qui guide le choix. Après avoir présenté la formalisation de notre proposition, nous décrivons les changements nécessaires apportés à la signalisation présentée dans ce chapitre ainsi qu'une instanciation possible de cette contribution.

2.3.2. Formalisation

Notre proposition de provisionnement dynamique repose sur les hypothèses suivantes :

- modèle d'Internet multi-domaine à QoS à base de Bandwidth Broker ;
- sélection d'un seul chemin inter-domaine (donné par BGP, sans routage à QoS) ;
- existence de plusieurs classes de services (CoS) par domaine et possibilité de faire un choix parmi ces CoS ;
- connaissance de la disponibilité des ressources et des performances pour chaque CoS entre tout couple de routeurs de bordure du domaine.

Au sein d'un domaine *D*, chaque CoS *i* est caractérisée par :

- une bande passante disponible Bw_{iD} ;
- un coût pour l'utilisateur C_{iD} ;
- une fonction de QoS $Fqos_{iD}$ qui représente la caractérisation de la QoS fournie entre chaque couple de routeur de bordure. Nous illustrons par la suite un exemple d'une telle fonction issue des travaux de [Auriol04] ;

Pour répondre au problème de provisionnement dynamique, nous proposons une approche qui :

- découvre au moment de la requête de QoS des services (CoS) et leurs disponibilités sur les domaines impliqués dans la communication ;
- évalue d'abord les performances de bout-en-bout de tous les choix possibles résultant de la concaténation de ces services ;
- puis choisit et invoque celui le plus adapté qui répond les besoins en QoS exprimés dans la requête en respectant au mieux un ensemble de préférences. Ces préférences portent sur plusieurs critères, groupés en deux catégories : orientées utilisateurs (par exemple coût le moins cher), et orientées fournisseur (par exemple maximisation du profit, optimisation de l'utilisation des ressources). Le problème du choix se pose ainsi sous la forme d'un problème d'optimisation.

Nous illustrons dans la suite l'approche qui choisit la concaténation la moins coûteuse pour l'utilisateur, tout en respectant les exigences en QoS (Figure 27).

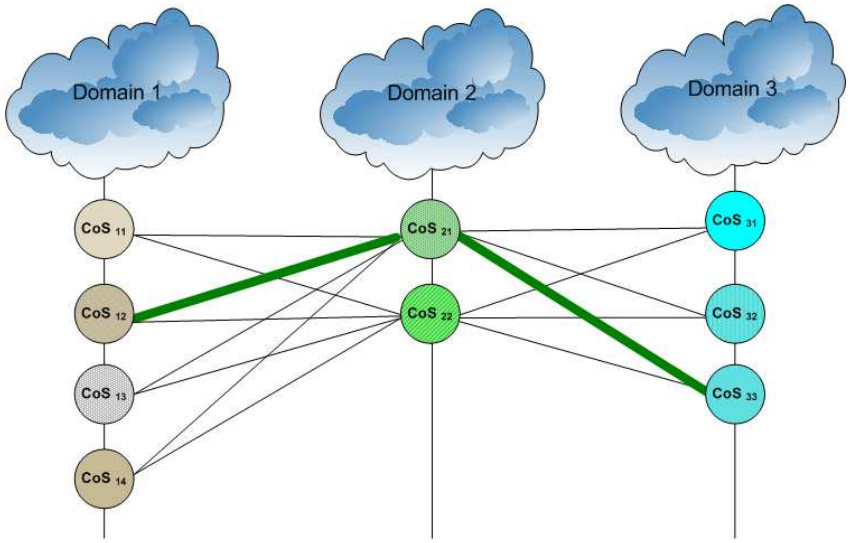


Figure 27 : Exemple concaténation des classes de service

Supposons une communication qui traverse N domaines à QoS, chacun offrant un maximum de M classes de service. En prenant en compte les conditions requises par la requête utilisateur (en termes de bande passante et d'autres paramètres de QoS), les relations à remplir par la concaténation des CoS choisies sont :

$$1) Bandwidth \leq \underset{i=1}{\overset{N}{Min}}\left(Bw_{Di}\right)$$
$$2) F_{target} > \left(Fqos_{1D} \circ Fqos_{2D} \circ .. \circ Fqos_{ND}\right)$$

où « o » représente une relation de composition générale entre fonctions (une instanciation spécifique sera donnée dans les paragraphes suivants).

Ces conditions traduisent le fait que la bande passante « Bandwidth » requise pour le flux à transmettre doit être disponible sur chaque domaine Di et que les besoins en QoS (F_{target}) sont satisfaits par la concaténation choisie. L'objectif est de choisir un vecteur [CoS1, CoS2, …, CoSN] (une CoS sur chaque domaine impliqué dans le chemin de données) qui remplit

les conditions 1) et 2) et qui de plus, maximise une fonction QoS(D) concernant les préférences exigées.

$$\underset{D}{Max}\, QoS(D)$$

Dans notre instanciation, la fonction qui minimise le coût (en tenant compte en même temps des contraintes précédentes) est :

$$\underset{D}{Max}\, QoS(D) = \sum_{i=1}^{N} \underset{j=1}{\overset{M}{Min}}\left(C_{ij}\right)$$

2.3.3. Exemple

La caractérisation usuelle des performances d'un service DiffServ (de l'entrée à la sortie d'un domaine) est souvent donnée en termes de borne supérieure sur le délai et éventuellement de gigue [Gode01]. L'inconvénient de ce modèle est qu'il conduit à une caractérisation « sous optimale » lorsque l'on considère le service de bout en bout fourni par plusieurs domaines consécutifs.

Dans des travaux précédents [Chassot03], [Auriol03], la caractérisation des performances du service IP entre deux routeurs de bordure est exprimée par une fonction de répartition du délai de transit. En considérant le délai de transit X de chaque paquet entre deux routeurs de bordure comme une variable aléatoire, la fonction de répartition F_X est définie par $F_X(t) = P(X < t)$: où P représente, pour un paquet quelconque, la probabilité que son délai de transit soit inférieur à t[4].

Cette caractérisation présente un intérêt pour différents types de besoins applicatifs, par exemple :

- pour un besoin en fiabilité partielle τ_r indépendamment du temps (streaming vidéo sans contrainte forte sur le délai), la QoS requise est satisfaite si $\tau_r \leq \lim F(t \to \infty)$;
- pour un besoin en fiabilité partielle τ_d, et une contrainte de délai borné supérieurement *b* (jeux distribués), la QoS requise est satisfaite si : $\tau_d < F(b)$;
- pour un besoin en gigue bornée *g* et en délai de transit moyen borné supérieurement d_m (audio), la QoS requise est satisfaite si : $g \geq k.\sigma$ et $d_m \leq \bar{x}$, $\bar{x}$ et σ désignant respectivement la valeur moyenne et l'écart type du délai observé, k étant une constante dépendant de la loi de probabilité du délai.

Notre étude s'appuie sur une telle caractérisation entre chaque paire de routeurs de bordure de tous les domaines. La procédure de concaténation est décrite dans les sections suivantes.

2.3.3.1. Adéquation au contexte du mono-domaine

Des mesures réalisées dans un environnement DiffServ mono-domaine nous ont permis d'enregistrer la distribution du délai de transit des paquets entre deux routeurs de bordure, et d'estimer ainsi la fonction de répartition. En outre, nous avons montré que pour les classes de services autres que le BE, une telle fonction pouvait être considérée comme indépendante (1)

[4] Cette fonction peut capturer l'information relative au taux de pertes : un paquet perdu eut être considéré comme acheminé avec un délai infini.

de la quantité[5] de flux à QoS circulant dans le réseau, et (2) de la topologie de celui-ci, pour une charge en trafic BE donnée et une route donnée [Chassot02] [Auriol03] [Auriol04].

Dans la suite, nous supposons que cette information est disponible au niveau de chaque domaine (au sein d'une entité telle qu'un BB), pour tous les couples possibles de routeurs de bordure.

2.3.3.2. Composition inter-domaines

Dans un contexte multi-domaine, il s'agit de caractériser les performances résultant de la concaténation de plusieurs classes de service le long d'un chemin de données impliquant plusieurs domaines (Figure 28).

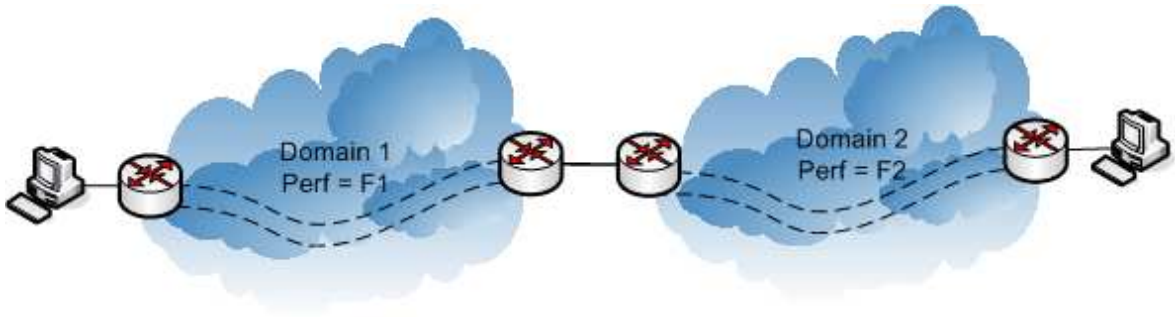


Figure 28 : Composition multi-domaine

Dans le cas de deux domaines successifs D_1 et D_2, soient X_1 et X_2 les délais de transit d'un même paquet traversant chacun des domaines, et $F_1(t)$ et $F_2(t)$ leurs fonctions de répartition respectives. Sous l'hypothèse d'indépendance en probabilité des délais de transit expérimentés dans chaque domaine, la fonction de répartition $F_{1,2}(t)$ du délai de transit de bout en bout $X_{1,2} = X_1 + X_2$, est égale à la dérivée du produit de convolution des fonctions de répartition de chacun des deux domaines traversés : $F_{1,2}(t) = \frac{d}{dt}(F_1(t) * F_2(t))$.

La généralisation à la traversée de *n* domaines se fait à partir du résultat obtenu avec *n–1* domaines grâce à la propriété d'associativité du produit de convolution :

$$F_{1,n}(t) = \frac{d}{dt}\left(F_{1,n-1}(t) * F_n(t)\right),$$

où : $F_{1,i}(t)$ désigne la fonction de répartition du délai des paquets traversant les domaines D_1, D_2, …, D_n.

Ainsi, il est possible d'obtenir pour chacun des services résultant de la concaténation des classes offertes dans chaque domaine, une caractérisation des performances que l'on peut espérer observer de bout en bout. Ce résultat permet d'envisager qu'une application puisse déterminer la ou les concaténations de classes qui répondent à ses besoins en QoS.

2.3.4. Signalisation associée

La mise en œuvre de la récupération des disponibilités de classes de service sur le chemin de données, nécessite (en dehors de l'algorithme de concaténation présenté précédemment) un mécanisme de signalisation. Nous allons analyser dans cette section les implications sur la signalisation présentée précédemment pour prendre en compte le modèle de provisionnement

[5] Nombre et charge

dynamique. Nous définissons un nouveau PDU dans le protocole de signalisation : REQUEST. Il permet d'interroger les Bandwidth Brokers sur le chemin de données et de récupérer les services disponibles et leurs caractéristiques dans chaque domaine. L'enchainement des messages de signalisation est donné dans la Figure 29. Nous distinguons trois phases dans cette approche : (1) la découverte des services disponibles, (2) la réservation du service le mieux adapté et (3) la libération des ressources.

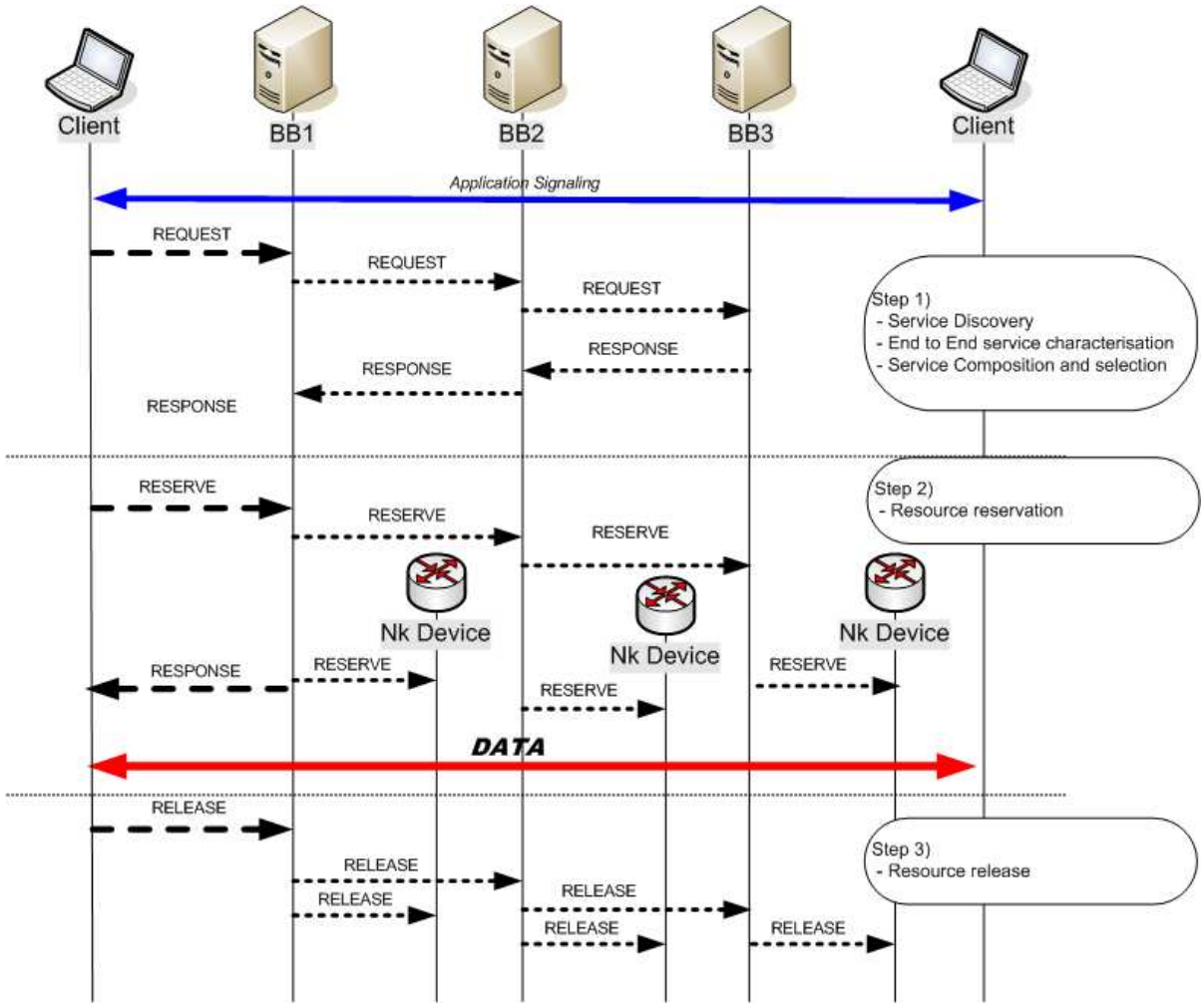


Figure 29 : Signalisation modifiée pour le provisionnement dynamique

Le choix de concaténation se résout en trois étapes :

1) découverte des classes de service et de leurs performances auprès de chacun des domaines du (des) chemin(s) inter-domaine(s) :
2) évaluation par le biais de la convolution, du modèle de performance (i.e. la fonction de répartition du délai de transit) de l'ensemble des classes disponibles de bout en bout sur le(les) chemin(s) ;
3) choix de la classe la moins coûteuse qui satisfait la QoS requise ; l'algorithme correspondant s'appuie sur les principes introduits précédemment au travers d'une représentation approximée de la fonction de répartition.

Le contrôle d'admission est couplé au choix précédent :

- durant l'étape 1 précédente, une pré-réservation des ressources nécessaires est effectuée au niveau du BB de chaque domaine, pour chacune des classes disponibles

sur le chemin de donnée ; chaque BB vérifie la conformité de la requête vis à vis du contrat souscrit en entrée, compte tenu de l'état courant d'utilisation de ce contrat ;
- à l'issue du choix de l'étape 2, les pré-réservations pour la classe retenue sont confirmées, et les autres sont libérées.

Nous avons proposé une solution au problème du choix de concaténation des services permettant de satisfaire une requête de QoS pour des données applicatives ayant à traverser plusieurs domaines. Comparativement aux autres travaux, notre proposition vise à minimiser l'utilisation des ressources du réseau en découvrant les performances des services disponibles sur le chemin de données au moment de la requête applicative, et en effectuant le choix de la concaténation de service répondant au plus prêt aux besoins applicatifs, en prenant compte en même temps d'un ensemble de préférences orientées utilisateur ou fournisseur .

2.3.5. Evaluation des bénéfices du provisionnement dynamique

2.3.5.1. Spécification

Nous présentons dans cette section les simulations réalisées pour évaluer notre proposition de provisionnement de service dynamique. Notons que dans ces simulations, nous illustrons l'approche qui cherche à minimiser le coût pour l'utilisateur sur les concaténations retenues.

Nous comparons notre algorithme à celui classique qui associe statiquement (c'est-à-dire à l'avance) une classe de service à un type d'application et essaye de réserver les ressources au long du chemin pour cette classe. Rappelons que dans notre approche, une requête de service ne spécifie pas une CoS spécifique mais contient un ensemble de paramètres de QoS.

Les spécifications de nos tests sont les suivantes :

- nous considérons trois types d'applications ayant des besoins en QoS bien définis ; chaque requête de QoS formulée l'est pour l'un de ces types d'applications ;
- nous considérons que chaque domaine implante les trois mêmes classes de service (CoS1, CoS2 et CoS3) et nous considérons que les garanties en QoS de ces classes suivent la relation : QoS(CoS3)> QoS(CoS2)> QoS(CoS1). Le coût de ces CoS suit la même relation, ce qui signifie que le prix de la classe CoS3 sont plus important que celui deCoS2 et que le prix de CoS2 est plus important que celui de CoS1 ;
- Nous considérons trois scénarios d'allocation de la bande passante pour chaque CoS (identique pour chaque domaine) :
  - Scénario 1 : 80% CoS1, 10% CoS2 et 10% CoS3
  - Scénario 2 : 60% CoS1, 20% CoS2 et 20% CoS3
  - Scénario 3 : 40% CoS1, 30% CoS2 et 30% CoS3
- le nombre de requêtes de QoS applicatives pour ces scénarios est de 300000 reparties uniformément sur tous les domaines et l'arrivée de ces requêtes suit une loi de Poisson. La durée de chaque communication suit une loi uniforme de moyenne égale à trois minutes (cf. études sur www.onetel.fr). ;
- chaque requête de réservation traverse plusieurs domaines (la destination est choisie aléatoirement).

Notre algorithme de test a été implémenté en Java. La durée des tests est de 24 heures avec collecte de résultats toutes les secondes.

2.3.5.2. Résultats et analyse

Dans un premier temps, nous analysons le nombre de clients acceptés sur chaque domaine. Nous appelons « client » une requête de service engendrée sur chaque domaine (BB) par les requêtes applicatives initiales. Ainsi une requête de QoS pour un flux donné conduit à plusieurs « clients » si le flux traverse plusieurs domaines.

Les résultats illustrés dans la Figure 30 et la Figure 31 présentent le nombre de clients dont la requête de QoS a été acceptée et le nombre total de clients ayant effectué une requête sur chaque domaine.

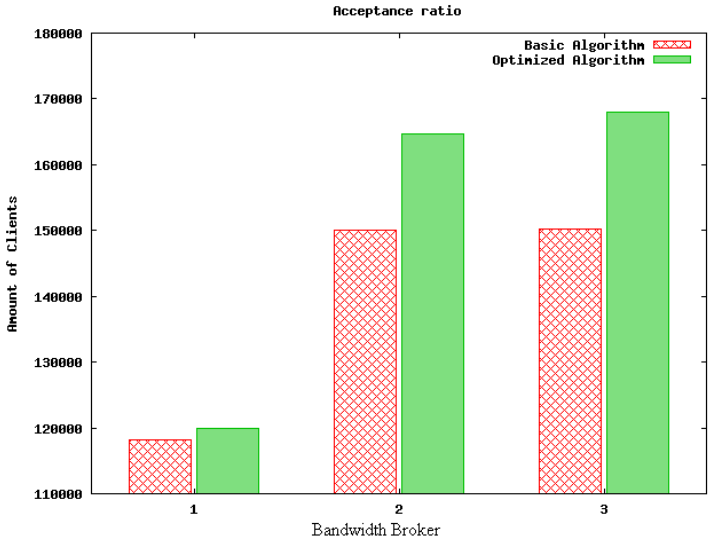


Figure 30 : Nombre de client acceptés

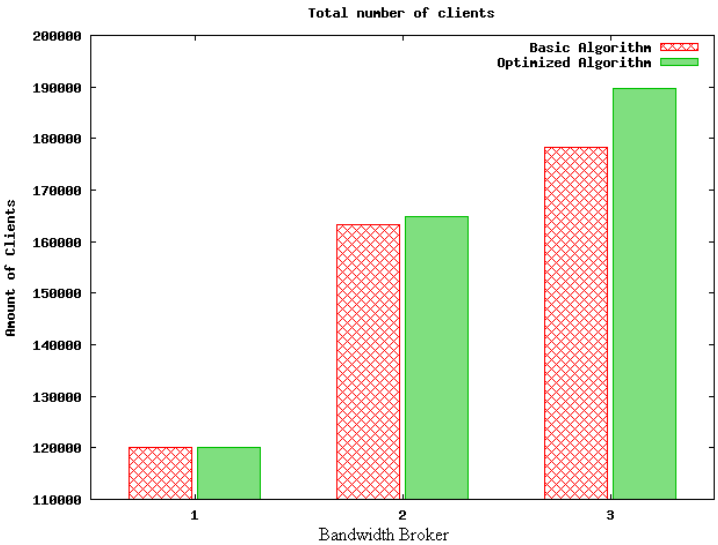


Figure 31 : Nombre Total de clients sur chaque BB

Nous pouvons observer qu'avec notre modèle, le nombre de clients acceptés ainsi que le nombre total de clients est plus grand sur chaque BB comparativement à l'algorithme classique (respectivement 0.7%, 1% et 6% - 2%, 9% et 14%). Ceci s'explique par le fait que plusieurs requêtes, potentiellement satisfaisables, sont engendrés et reçues par le BB dans notre approche. Une requête de QoS de notre solution ne fait pas référence à une CoS particulière est cherche les services et leur disponibilités sur chaque domaine. Dans, l'approche classique, la CoS est fixé en amont et si les ressources ne sont pas disponibles

pour cette CoS, la requête n'est pas propagée au prochaine BB. Comparativement au modèle général classique, notre solution ne se résume pas au choix d'une seule CoS au long du chemin de données, mais acquiert les performances de toutes les CoS disponibles et cherche à trouver la meilleure concaténation. Cette flexibilité explique aussi le fait qu'un nombre plus grand de requêtes peut être traité et satisfait. Ce nombre dépend également du choix de l'algorithme de composition des services. Avec notre approche, nous pouvons choisir des CoS distinctes dans chaque domaine (pas las même CoS sur tous les domaines) ce qui engendre une répartition différente de la disponibilité des ressources.

L'arrivée d'un nombre plus petit de clients sur le premier BB s'explique par le fait que nous avons fait le choix de repartir les clients sur les trois domaines et le chemin suivi par les données est du domaine 1 vers les domaines 2 et 3.

Les résultats suivants illustrent l'occupation de la bande passante sur chacun des domaines. La Figure 32 illustre l'occupation de la bande passante totale (toutes les CoS confondues) sur les BB. Nous remarquons qu'avec notre approche, nous obtenons une meilleure occupation de la bande passante, ce qui implique que les revenus des fournisseurs peuvent être augmentés.

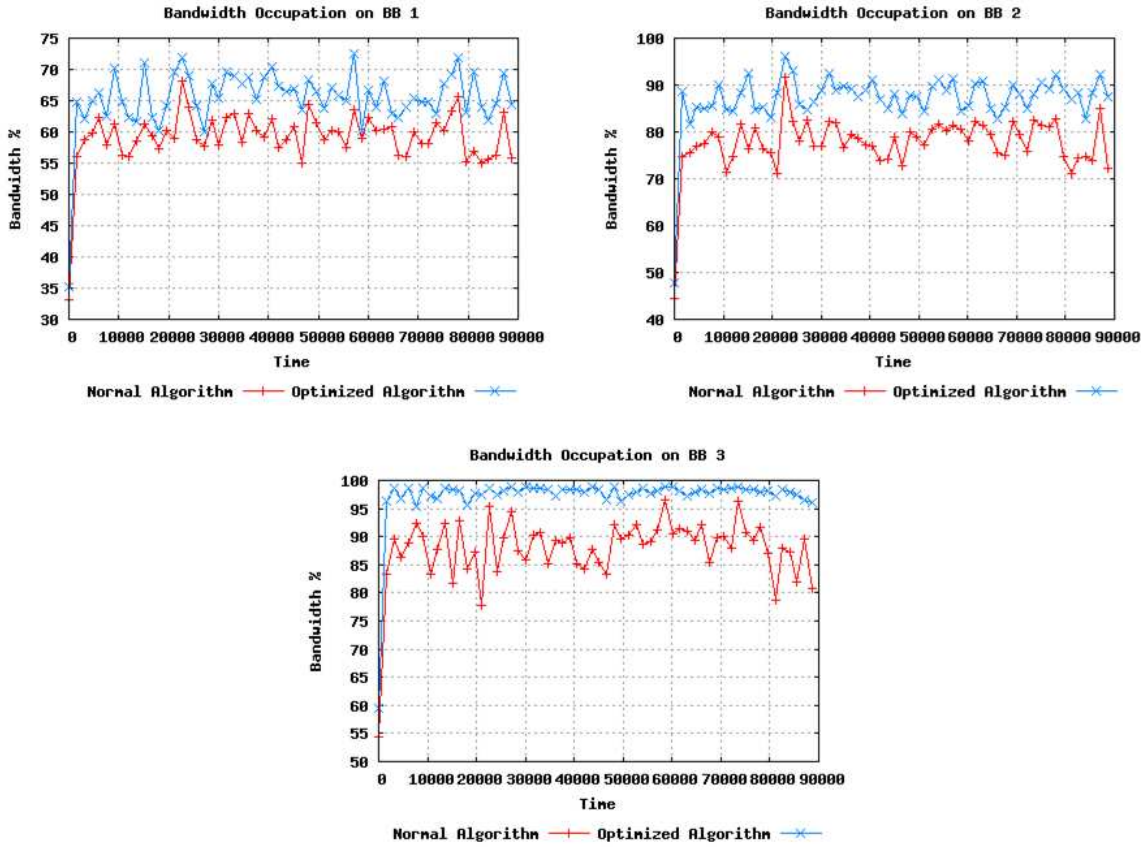


Figure 32 : Occupation de la bande passante totale

Nous avons également analysé l'occupation de la bande passante pour chaque classe de service (CoS) séparément. La Figure 33 montre l'occupation de la bande passante pour la CoS1, les résultats pour les CoS2 et CoS3 étant similaires (la différence est plus évidente si les proportions de chaque CoS sont grandes).

Nous avons effectué par la suite un ensemble de simulations en changeant la proportion de chaque CoS. Les effets sont comparables, notre approche offrant des meilleurs résultats en termes de nombre de clients, de requêtes satisfaites et d'occupation de la bande passante.

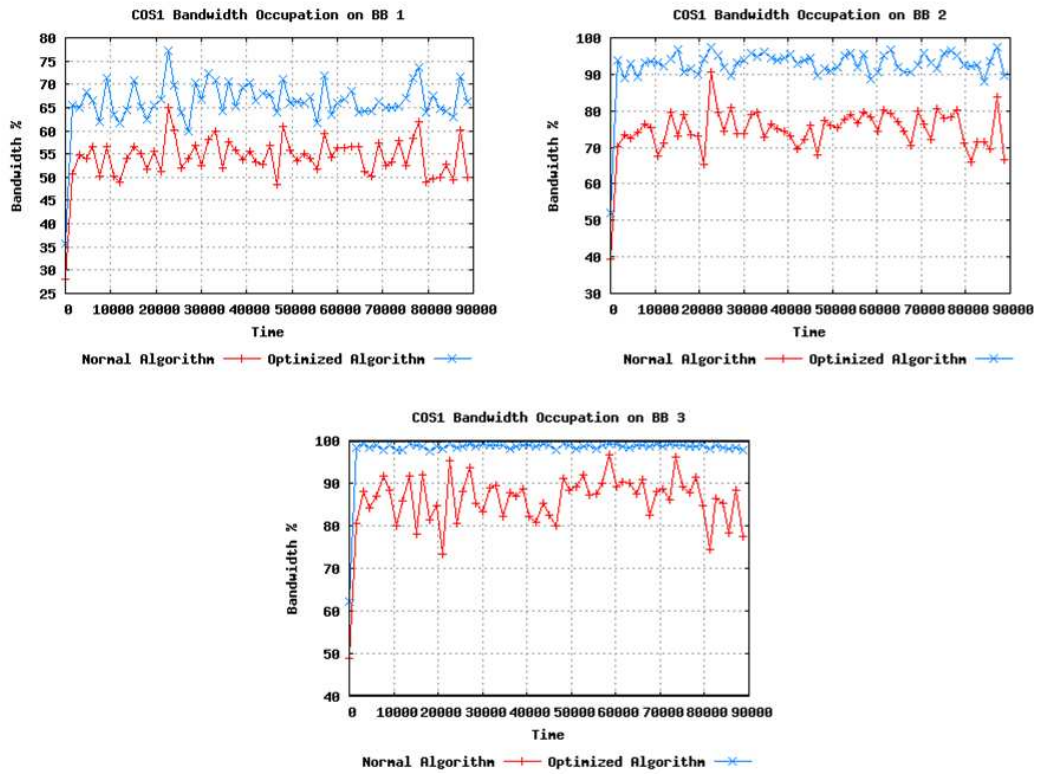


Figure 33 : Occupation de la bande passante par COS1

2.3.6. Conclusion

Dans cette section, nous avons décrit les simulations qui ont permis d'évaluer notre proposition de provisionnement dynamique. Nous avons comparé notre algorithme qui crée dynamiquement le service par la composition des classes disponibles au long du chemin de données avec l'algorithme classique qui choisit a priori une classe de service et réserve les ressources pour cette classe sur les domaines traversés.

Nous avons montré qu'avec ce type de provisionnement, le degré de satisfaction des clients est amélioré (le taux de rejet est inférieur), et une meilleure occupation de la bande passante est constatée. Les fournisseurs bénéficient ainsi d'une augmentation des profits liés au nombre accru de clients acceptés et d'une meilleure utilisation de leurs ressources.

2.4. HyPath (Hybrid on-path off-path for end-to-end signaling across NSIS and non-NSIS domains)

2.4.1. Introduction

Cette section présente l'intégration du protocole présenté dans la section 2.2 dans le cadre de NSIS de l'IETF, afin d'étendre le déploiement ultérieur. Ces travaux ont été menés conjointement avec la Faculté des Sciences et Technologies de l'Université de Coimbra, Portugal. Les contributions issues de ces études ont été présentées lors des réunions de l'IETF, sous la forme de plusieurs versions d'un draft, arrivé actuellement à la sixième version.

Dans cette étape, nous nous plaçons dans le cadre architectural défini par NSIS. De plus, nous considérons un environnement multi-domaine qui prend en compte d'une part l'existence des Bandwidth Brokers et d'autre part des domaines qui n'implémentent pas une

signalisation NSIS (que nous appelons par la suite domaines non NSIS). Nous proposons une solution hybride pour la prise en compte d'une signalisation couplée et découplée du chemin de données. Nous présentons une approche qui s'intègre dans le framework NSIS pour la signalisation des domaines contrôlés par de Bandwidth Broker et aussi qui associe l'interconnexion des domaines NSIS et non-NSIS.

Nous avons évoqué auparavant la nécessité d'avoir une signalisation découplée du chemin de données dans le but d'interagir et d'échanger des informations entre des entités particulières au sein d'un domaine. Ces entités (Bandwidth Brokers) gèrent les ressources du domaine en suivant des politiques et règles autonomes et effectuent les réservations pour les flux acceptés. La solution actuellement explorée dans NSIS [Hancock05b] consiste à détourner les paquets de signalisation (identifiés avec le drapeau RAO - Router Alter Option [Katz97]) vers une autre entité du domaine. Nous proposons une approche de signalisation hybride (couplée/découplée du chemin de données) qui repose sur ce concept d'interception : en entrée d'un domaine, tout routeur de bordure intercepte les paquets de signalisation et les redirige vers le BB (qu'il est supposé connaitre). Après traitement, le BB retourne ces paquets au routeur, qui continue la signalisation. Le dialogue entre les BB s'effectue donc sans nécessiter de leur part la connaissance explicite de leur adresse respective. Le besoin d'une signalisation hybride (couplée-découplée du chemin de données) n'est pas résolu dans NSIS tel qu'il est défini actuellement à l'IETF. La signalisation des BB n'est pas considérée spécifiquement, la version courante de NSIS n'étant pas adéquate pour notre approche car elle suit la solution couplée (« on-path ») au chemin de données.

Le challenge de notre proposition est de ce fait de répondre au besoin suivant : comment réaliser la signalisation entre tous les Bandwidth Brokers des domaines sur le chemin de données dans le cadre NSIS, et de plus comment résoudre le problème d'une hétérogénéité avec des domaines ne supportant pas NSIS. Nous appelons cette solution de signalisation plus générale hybride « HyPath » (Hybrid on-path off-path for end-to-end signaling across NSIS and non-NSIS domains). Nous précisons que notre approche suppose pour une garantie de bout-en-bout, l'existence des domaines à QoS (voir section 2.1.1, notamment contrôlés) au long du chemin de données.

HyPath est donc nécessaire dans les Bandwith Brokers et les routeurs de bordure pour répondre aux besoins d'une signalisation hybride (couplée et découplée du chemin de données) de bout-en-bout. Les principales fonctionnalités de HyPath sont :

- Dans le Bandwidth Broker
  - Pilotage de la signalisation hybride ;
  - Récupération et analyse des messages ;
  - Découverte de routeurs de bordure ;
  - Propagation des messages vers les Bandwidth Broker voisins ;
  - Interaction avec des modules externes : base de données, routage ;
- Dans le routeur de bordure
  - Possibilité d'initier la signalisation ;
  - Interception des messages de signalisation ;
  - Déviation de la signalisation vers le Bandwidth Broker ;
  - Réception de la réponse du Bandwidth Broker et continuation de la signalisation.

2.4.2. Proposition HyPath

Rappelons que NSIS est spécifié suivant une solution modulaire à deux niveaux (voir section 1.5.4) : le niveau transport de la signalisation (NTLP) et le niveau signalisation applicative (NSLP). Cette approche permet la séparation du transport des messages de signalisation de la signalisation proprement dite. De plus, cette conception facilite la création de plusieurs types de protocoles au niveau NSLP et l'utilisation du NSIS pour différents objectifs : QoS, sécurité… La solution que nous avons proposée consiste à étendre les mécanismes de base de NSIS avec une nouvelle fonctionnalité appelée HyPath, mais l'insertion de HyPath ne doit pas interférer et changer le comportement de la spécification actuelle du NSIS, et donc doit transparente dans l'architecture NSIS.

Nous avons fait le choix de concevoir HyPath comme une extension du niveau NTLP, notamment comme une nouvelle méthode de routage des messages (Message Routing Method) dans GIST [Schulzrinne05] (Figure 34) : les versions du draft présentées à l'IETF détaillent notre proposition de traitement et d'acheminement des messages HyPath. Le fonctionnement HyPath est présenté dans les paragraphes suivants.

De plus, une interaction avec des modules externes (en particulier BGP) est nécessaire pour prendre en compte les contraintes de routage inter-domaine.

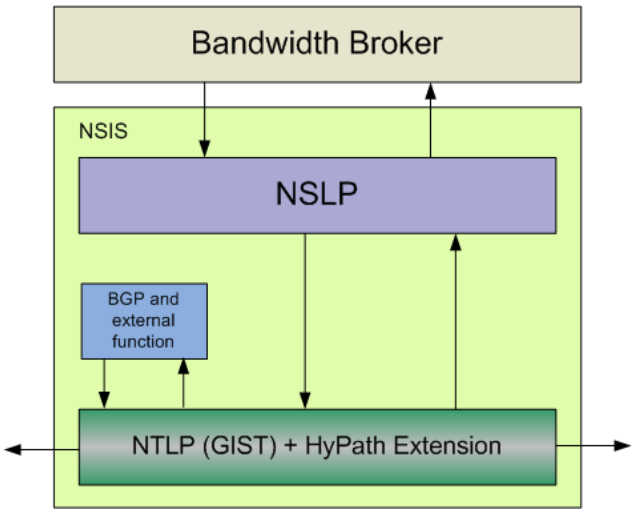


Figure 34 : Proposition architecturale HyPath

HyPath est instancié dans les routeurs de bordure et les Bandwidth Brokers ; les échanges en HyPath ont lieu donc entre ces entités ; les autres équipements NSIS qui ne sont pas configurés avec HyPath doivent transporter et acheminer les données (appelés objets) HyPath de manière transparente, sans les traiter. La Figure 35 illustre ce mécanisme dans lequel les routeurs de bordure (BR) implémentent HyPath, et les routeurs intermédiaires internes ne supporte pas HyPath.

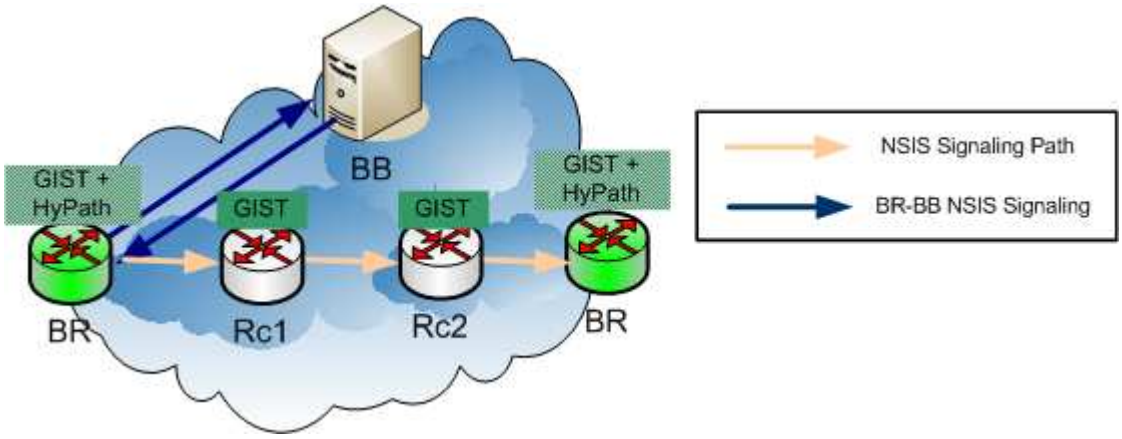


Figure 35 : HyPath à l'intérieur d'un domaine NSIS

Un message reçu par Rc1 est acheminé après traitement vers Rc2 comme un message NTLP (GIST) standard. Cette approche permet le transfert des informations HyPath par les routeurs qui n'implémentent pas cette fonctionnalité sans les supprimer. De plus, le traitement classique GIST n'est pas affecté par l'introduction de HyPath.

Le fonctionnement HyPath est décrit dans la section suivante. Nous présentons d'abord le fonctionnement entre domaines NSIS. Ensuite nous étendons la proposition pour un environnement hétérogène NSIS et non-NSIS.

2.4.3. Fonctionnement dans les domaines NSIS

L'objectif principal de notre proposition HyPath est d'étendre la spécification actuelle du NSIS avec des nouvelles fonctionnalités pour permettre la signalisation entre les Bandwidth Brokers. Avec HyPath, la signalisation découplée du chemin de données (off-path) devient transparente.

La Figure 36 présente le déroulement du protocole de signalisation avec le mécanisme HyPath intégré dans la suite NSIS et implémenté dans les routeurs de bordure et les Bandwidth Brokers.

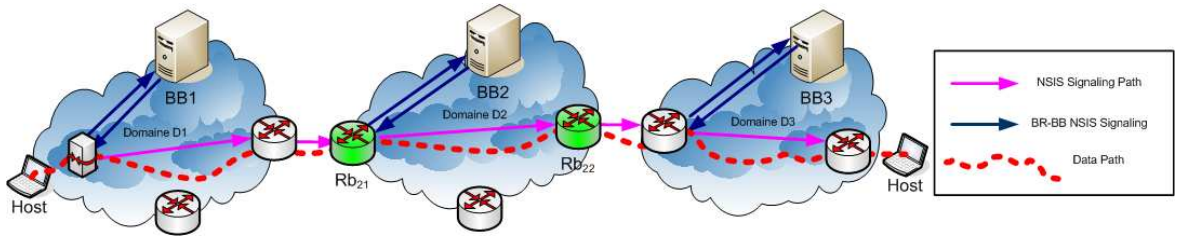


Figure 36 : Processus de signalisation HyPath

Dans le cas de la signalisation HyPath, le problème de découverte du prochain Bandwidth Broker est résolu par l'interception des messages dans le routeur d'entrée du domaine et leur déviation vers son Bandwidth Broker, de la manière suivante. Quand un utilisateur effectue une requête de réservation des ressources, les fonctionnalités de base de NSIS, i.e. les réservations dans les routeurs, ne doivent pas être modifiées. En même temps, le protocole NSIS doit être capable de « signaler » tous les Bandwidth Brokers des domaines impliqués dans le chemin de données. Pour ceci, les paquets de signalisation NSIS sont envoyés vers la destination. Les routeurs de bordure en entrée de chaque domaine (qui implémentent impérativement HyPath) interceptent les messages de signalisation. Ensuite, ces messages sont réorientés vers le Bandwidth Broker (dont l'adresse est supposée connue) au lieu de

suivre les opérations du NSIS classique (voir Figure 36). Après le traitement du message reçu (similaire à celui détaillé dans la section 2.2), le Bandwidth Broker continue la signalisation, en renvoyant un message NSIS au routeur de bordure. Celui-ci reprend la signalisation NSIS classique sur le chemin de données vers le prochain nœud pair NSIS (et par la suite vers le prochain domaine et la destination). Ce mécanisme se déroule dans chaque domaine, jusqu'au dernier et les ressources sont réservées de bout-en-bout au long du chemin de données.

L'architecture proposée remplit toutes les exigences pour réaliser une signalisation de bout-en-bout dans un contexte NSIS. En outre, aucun changement dans la définition des niveaux NSLP et NTLP n'est nécessaire, l'insertion de HyPath étant transparente. De cette manière, les messages de signalisation suivent le chemin de données et de plus tous les Bandwidth Brokers des domaines sont « signalés ».

2.4.4. Extension pour l'intégration des domaines non-NSIS

Proposons dans cette section une solution hybride générique qui gère à la fois les domaines NSIS et non-NSIS, c.à.d. généralise les deux approches précédentes : la solution NSIS étendue avec HyPath est utilisée dans les domaines NSIS, et dans le cas des domaines non-NSIS, l'interception des messages ne pouvant être réalisées dans les routeurs de bordure, une communication directe entre les Bandwidth Brokers doit être utilisée. Rappelons que HyPath est implanté dans les routeurs de bordure et les Bandwidth Brokers et que l'échange des messages pour les domaines non NSIS peut se faire aussi en NSIS-HyPath.

L'inconvénient de l'approche décrite dans la section précédente réside dans le fait que les routeurs de chaque domaine (en particulier les routeurs de bordure) et les Bandwidth Brokers doivent implémenter NSIS. En pratique, cette hypothèse forte est difficile à déployer à cause de l'hétérogénéité des solutions de signalisation inter et intra-domaine. Cette réflexion nous a conduit à proposer une solution plus générale, adéquate dans un contexte multi-domaine hétérogène, capable d'interconnecter des domaines NSIS et des domaines non-NSIS (qui n'utilisent pas NSIS comme protocole de signalisation).

L'hypothèse NSIS dans tous les routeurs de bordure écartée, le mécanisme de signalisation repose sur une communication directe entre les Bandwidth Brokers. La Figure 37 illustre la signalisation dans un environnement non-NSIS (solution détaillée précédemment dans la section 2.3) :

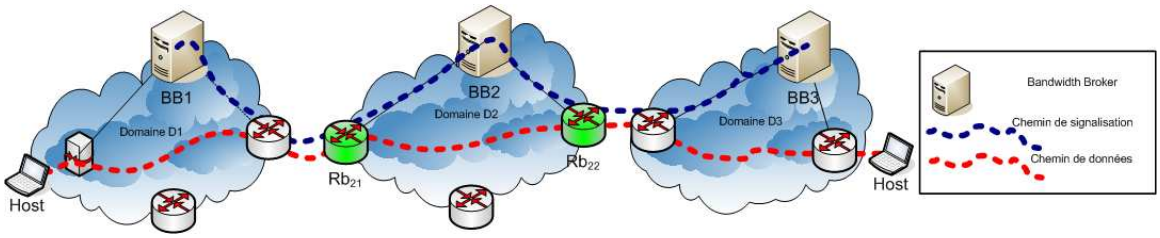


Figure 37 : Signalisation dans les domaines non-NSIS

Les messages de signalisation sont acheminés de BB en BB directement, cette solution étant complètement découplée du chemin de données. La signalisation passe par conséquent par les BBs des domaines, et ne suit pas le même chemin que les données (en revanche elle passe par les mêmes domaines).

Cette solution doit être cohérente avec les fonctionnalités externes au protocole de signalisation : découverte des routeurs de bordure et du prochain Bandwidth Broker, interaction avec les protocoles de routage, BGP en particulier. Par conséquent, nous

proposons une solution hybride qui permet la signalisation de bout-en-bout dans un environnement multi-domaine NSIS et non-NSIS.

La Figure 38 présente les détails de la signalisation hybride proposée :

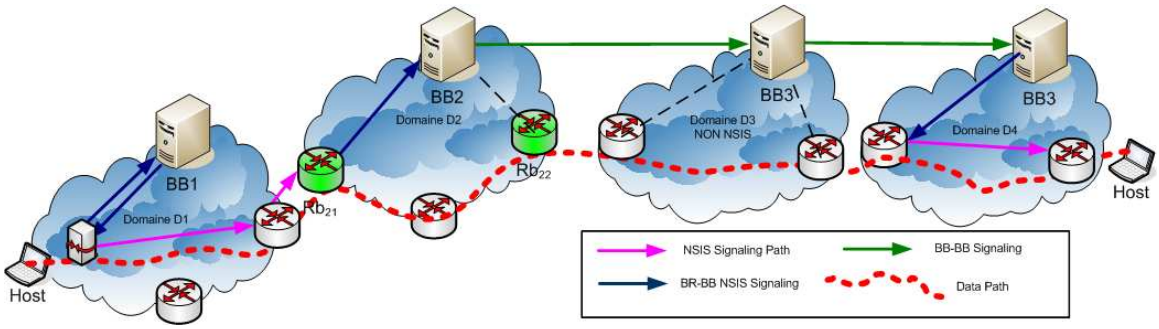


Figure 38 : Signalisation hybride

La difficulté d'une telle approche hybride réside principalement dans la continuité de la signalisation entre deux domaines qui implémentent des solutions différentes : NSIS et non-NSIS. Par exemple, lors d'un passage d'un domaine NSIS à un domaine non-NSIS, le routeur de bordure ne supportant pas HyPath, le message n'est pas intercepté et n'est pas redirigé vers le Bandwidth Broker.

Pour palier ce problème, le Bandwidth Broker d'un domaine NSIS doit vérifier la nature du domaine suivant (NSIS ou non-NSIS), avant de continuer la procédure de signalisation. Cette information est disponible suite aux accords d'association entre les domaines (agréments-SLA). Si le prochain domaine est un domaine non-NSIS, le message sera envoyé directement à son Bandwidth Broker. Dans le cas contraire, le mécanisme NSIS-HyPath sera utilisé (voir section 2.4.3). La redirection des messages off-path et ensuite leur réinsertion sur le chemin de données sont effectuées dans les domaines NSIS.

2.4.5. Prise en compte de domaines surprovisionnés

Dans la proposition NSIS, le problème de domaines surprovisionnés trouve une solution directe. Ayant la certitude que tous les domaines au long du chemin sont à QoS, les messages NSIS traverseront de manière transparente les domaines surprovisionnés. Ils seront interceptés dans le routeur de bordure en entrée du prochain domaine NSIS et la signalisation reprend les opérations HyPath. Evidement, pour les cas des domaines hétérogènes (NSIS, non-NSIS), la solution repose sur l'étude présentée dans la section 2.2.4.

2.4.6. Conclusions

La proposition HyPath, menée conjointement avec l'Université de Coimbra dans le cadre du groupe de travail NSIS de l'IETF, a eu pour objectif d'enrichir le framework NSIS avec la capacité de supporter une signalisation hybride, couplée et découplée du chemin de données et de faciliter par conséquent l'interaction avec des domaines qui ne supporte pas la signalisation NSIS. Elle nécessite une configuration étendue de NSIS dans les routeurs de bordure et dans les Bandwidth Brokers de chaque domaine. Pour répondre au problème d'hétérogénéité de la signalisation, notre solution utilise :

- L'interception et le déroutement des messages en entrée du domaine vers le Bandwidth Broker dans les domaines NSIS ;
- Une communication directe entre les Bandwidth Brokers entre les domaines non-NSIS.

Cette spécification a été présentée dans le cadre du groupe de travail NSIS de l'IETF, le concept étant approuvé et accepté pour une analyse future. Un draft Internet qui est arrivé à la sixième version présente l'avancement de la spécification. Pour supporter ces travaux, une implémentation est réalisée par l'Université de Coimbra, avec également une implémentation du GIST (utilisée en particulier dans le cadre du projet EuQoS).

2.5. Signalisation et mobilité

2.5.1. Contexte de mobilité considéré

Dans les dernières années, les réseaux mobiles et sans fil ont connu un grand essor en matière d'implantation et de couverture, ces types de réseaux étant de plus en plus répandus (Bluetooth, GSM, Wi-Fi…). De plus en plus, les applications deviennent distribuées, coopérative et mobiles. La gestion de la mobilité des terminaux est un challenge imposé par les applications aux réseaux de nouvelle génération. La continuité de service est un des objectifs, ce qui implique le maintient de la connectivité quand un terminal mobile passe d'un point d'accès à un autre (handover), qui peut produire des perturbations sur les communications en cours. Par conséquent, assurer la qualité de service dans un environnement mobile représente un des défis actuels auquel il faut répondre.

Plusieurs problèmes inhérents issus de l'association entre QoS et mobilité ont été évoqués dans la littérature [Chaskar03] : délai important pour le rétablissement de la réservation après hand-off, duplication possible des réservations, augmentation de la probabilité de blocage, augmentation des couts pour fournir la QoS. La coordination entre la gestion de la mobilité et celle de la QoS constitue l'axe de notre étude, menée dans le cadre d'une collaboration avec l'Université Fédérale de Santa-Catarina (UFSC), Brésil. Nous allons présenter brièvement quelques scénarios de mobilité et leur influence sur la QoS des communications existantes. Le but de cette étude est d'analyser la signalisation présentée antérieurement dans le cadre de la mobilité, mais aussi dans le cas de changement de route (suite à une défaillance par exemple). Les scénarios choisis visent les changements topologiques dû à la mobilité des terminaux et traitent à la fois la micro mobilité (à l'intérieur d'un domaine) et la macro mobilité (entre domaines différents).

Ce travail s'intéresse à l'impact de la mobilité dans un modèle de gestion de la QoS inter-domaine de bout-en-bout en analysant le maintien des réservations déjà établies et montre comment la continuité de service peut être obtenue à l'aide d'une signalisation adéquate.

2.5.2. Scénarios de mobilité examinés

Rappelons dans un premier temps le mécanisme d'IP Mobile tel que décrit dans [Perkins02] sans optimisation de route. Un nœud mobile (MN) en communication avec un nœud correspondant (CN) maintient une adresse IP appelée « home address » (*HoA*) et il est susceptible de changer de point d'accès dans le contexte de mobilité. Chaque MN reçoit une nouvelle adresse, appelée « care-of address » (C*oA*), associée avec le sous-réseau visité. La gestion de la localisation est à la charge de deux agents, « Home et Foreign Agent » (*HA* et *FA*). Chaque nouvelle *CoA* est reliée à la *HoA* et enregistrée dans une table maintenue dans le *HA* (voir Figure 39). Le HA agit au nom du MN en capturant les paquets à destination de son HoA et en les acheminant vers sa nouvelle CoA. Cette configuration est la « triangulation standard » illustrée en [Perkins02] avec une CoA associé à un FA. Tous les paquets en provenance du CN vers la HoA sont déviés par le HA vers le FA (par le biais d'un tunnel) et ensuite acheminés au MN. Le FA pourrait être éliminé du schéma si le MN utilisait directement une CoA allouée par DHCP [Droms97] par exemple. Les paquets de

MN vers le CN sont envoyés directement, bien que des mécanismes de « reverse-tunneling » puissent être mis en place. Cette procédure peut incorporer des instruments d'optimisation de route pour le chemin entre CN et MN afin d'éviter le tunnel HA-FA-MN qui risque d'être pénalisant autant lors de sa création (encapsulation IP sur IP) que par ses performances.

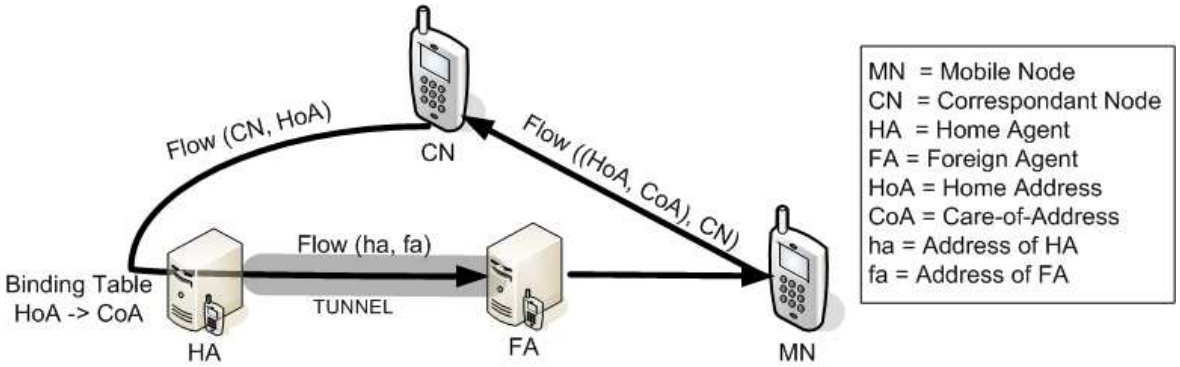


Figure 39 : Mécanisme de triangularisation IP Mobile

Présentons l'impact de la (micro et macro) mobilité sur la QoS et sur la signalisation par trois scénarios différents, illustrés dans la Figure 40.

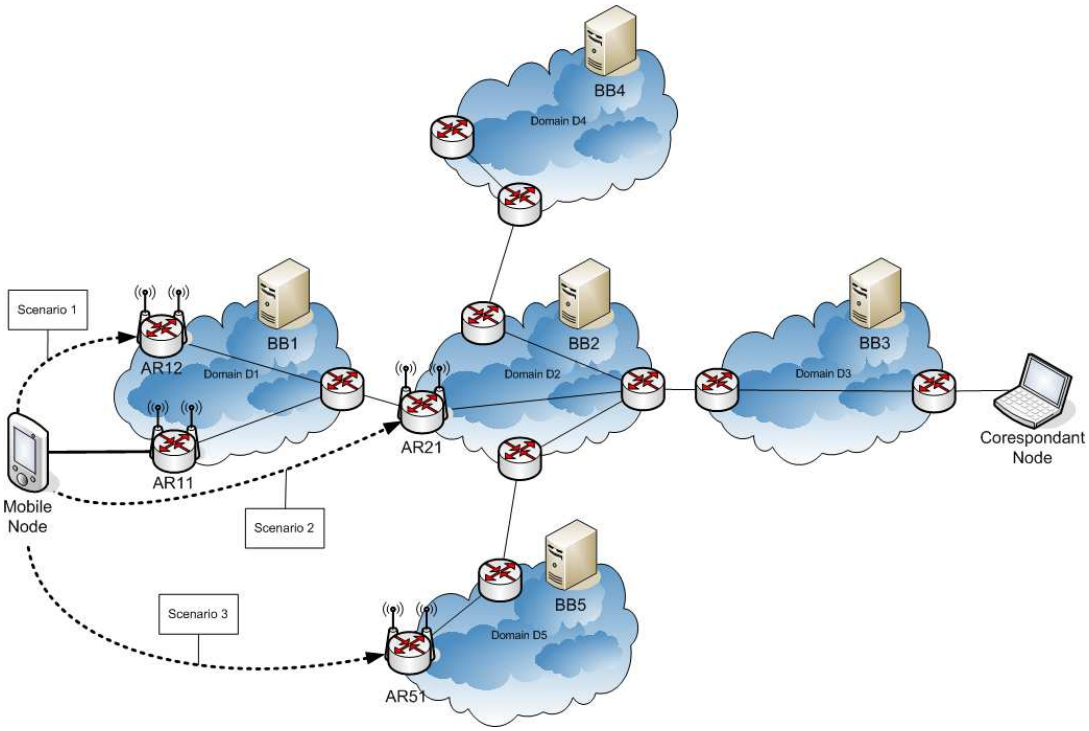


Figure 40 : Scénarios d'étude pour la mobilité

- Scenario 1 : un nœud mobile (MN) en communication avec un nœud correspondant (CN) change de point d'accès, d'AR11 à AR12, à l'intérieur d'un même domaine ;
- Scénarios 2 : Le MN change de point d'accès, d'AR11 à AR21, AR21 se trouvant dans un autre domaine, et le nouveau chemin étant une partie du chemin initial ;
- Scénarios 3 : Le MN passe du point d'accès AR11 à un nouveau point d'accès (AR51) dans un autre domaine ce qui engendre un nouveau chemin inter-domaine vers la destination (l'introduction de nouveaux domaines sur le chemin des données).

Pour simplifier, considérons le terminal mobile comme l'initiateur de la signalisation pour la QoS et que dans cette étude, nous n'examinons pas les problèmes liés à l'AAA

(authentification, autorisation accounting). La signalisation que nous avons proposée se prête à deux approches envisageables pour la réservation des ressources sur le nouveau chemin et la libération sur l'ancien :

- La première repose sur le mécanisme de soft-state, qui nécessite le rafraichissement périodique des réservations. Une manière simple et élégante de prendre en compte la mobilité est de réserver les ressources sur le chemin dépendant du nouveau point de rattachement du terminal sans se soucier des anciennes réservations. Celles-ci seront libérées suite à l'arrivée à l'échéance des minuteurs (timers) sur l'ancien chemin de données. Les performances de ce mécanisme dépendent de la configuration du timer, son ajustement pouvant limiter la double réservation.
- La seconde approche implique une libération explicite des ressources (l'envoi d'un message RELEASE).

Remarquons que dans les deux solutions, la nouvelle réservation est associée à la même session existante avant le handover (même identifiant de session). Evidement la solution la plus simple consiste à libérer les ressources sur l'ancien chemin et à réserver le nouveau chemin lors du changement de point d'accès. Cette solution n'est pas optimale (en termes de temps et de nombre d'opérations effectuées) et de plus dans un environnement mobile peut conduire à une coupure du service. En outre, si la réservation pour le nouveau chemin, peut se faire à l'avance (mécanismes de prévision), la qualité de service peut être assurée lors du handover. L'inconvénient de cette procédure est la complexité et le coût de sa mise en ouvre (maintien des anciennes réservations jusqu'à la confirmation sur le nouveau chemin, modèle de QoS qui admet une double réservation). Notons que la réservation sur le nouveau chemin pourrait ne pas être garantie due à l'absence des ressources.

2.5.2.1. Scenario 1

Le premier scenario implique la mobilité au sein d'un même domaine. Une fois que le MN détecte le changement de rattachement du point d'accès, il envoie un message à son Bandwidth Broker (nouveau message MODIFY par exemple). Si le chemin inter-domaine (et les routeurs de bordure) reste inchangé, aucune signalisation inter-domaine n'est nécessaire. Notons que cela conduit à un nouveau chemin intra-domaine et de plus peut engendrer une modification du chemin inter-domaine (suivant les politiques du domaine prises en compte par le protocole BGP) mais nous ne traitons pas ce dernier point ici car il sera discuté par la suite dans le scénario 3. Pour les réservations intra-domaine (dans les deux sens), il est nécessaire de (1) réserver les ressources associées au nouveau point d'accès du terminal (AR12), (2) maintenir les réservations pour les liens communs et (3) libérer ceux qui sont plus utilisées.

Concernant le sens de communication du CN vers le MN, aucune signalisation inter-domaine n'est nécessaire, car le CN continue à utiliser la HoA du MN comme destination. Le chemin de CN vers MN est composé de deux parties : CN-HA et HA-FA-MN. Comme pour la portion CN-HA, les ressources sont déjà réservées préalablement, et la réservation doit seulement être mise à jour pour HA-FA-MN, en intra-domaine donc.

2.5.2.2. Scenario 2

Après le rattachement du terminal au point d'accès AR21, le chemin inter-domaine change pour les deux sens de communication. Nous supposons, pour ce scénario, que le nouveau chemin est une portion du chemin initial, le cas général étant traité dans le scénario 3. Dès que le MN repère le changement, il envoie un message (MODIFY) au Bandwidth Broker 2 pour la mise à jour des réservations associées aux communications en cours du terminal.

Concernant le sens MN-CN, aucune réservation ne doit être effectuée du point de vue inter-domaine. Par contre les ressources entre l'AS1 et l'AS2 doivent être libérée (message RELEASE du BB2 au BB1). De la même manière qu'au scénario précédent, le BB2 gère la libération et la réservation intra-domaine sur l'AS 2.

En ce qui concerne les flux du CN vers MN, deux cas possibles sont à traiter :

- Suivant le schéma sans optimisation de route, les ressources pour le tunnel HA-FA-MN doivent être réservées (AS1 et AS2 sont impliqués). Une signalisation est mise en place donc entre les Bandwidth Brokers respectifs ;
- Si un mécanisme d'optimisation de route est pris en compte, la signalisation suit la procédure standard (signalisation inter-domaine initiée par le récepteur, voir section 2.2.3) pour la réservation sur le nouveau chemin et la libération des anciennes réservations qui ne sont plus utilisées (AS1).

2.5.2.3. Scenario 3

Ce scénario, le plus général, porte sur la mobilité vers un autre domaine avec changement du chemin inter-domaine. Suite à la détection de rattachement au nouveau point d'accès (AR51), le MN initie une procédure de réservation auprès du Bandwidth Broker 5. Une signalisation inter-domaine doit être mise en place pour la réservation des ressources sur le nouveau chemin et la libération des anciennes non utilisées. Pour le sens CN-MN, dans la situation de la triangulation sans optimisation de route, les ressources entre CN et HA sont maintenues et une nouvelle réservation est lancée pour la portion HA-FA-MN (similaire au scenario 2). Dans le cas contraire, une signalisation standard est requise pour l'établissement du nouveau chemin et la libération des anciennes ressources.

2.5.2.4. Optimisation de la signalisation

Ce mécanisme de réservation et libération tout au long du chemin (inter-domaine) de données peut être coûteux en temps d'exécution. Pour répondre à ce problème, le groupe de travail NSIS propose une solution qui utilise les réservations existantes sur le chemin et essaye de minimiser les nouvelles opérations de libération / réservation. L'idée dans l'approche couplée au chemin de données est de trouver le routeur « cross-over ». Le routeur cross-over est le premier nœud commun entre l'ancien et le nouveau chemin. Pour optimiser la procédure de signalisation, les ressources sont réservées jusqu'au routeur cross-over et libérées juste sur la portion non utilisée. Nous suivons une approche similaire à celle-ci, mais à l'échelle du domaine. Nous cherchons donc à découvrir le premier domaine cross-over sur le chemin de donnée (Figure 41), en supposant que le reste du chemin inter-AS reste inchangé.

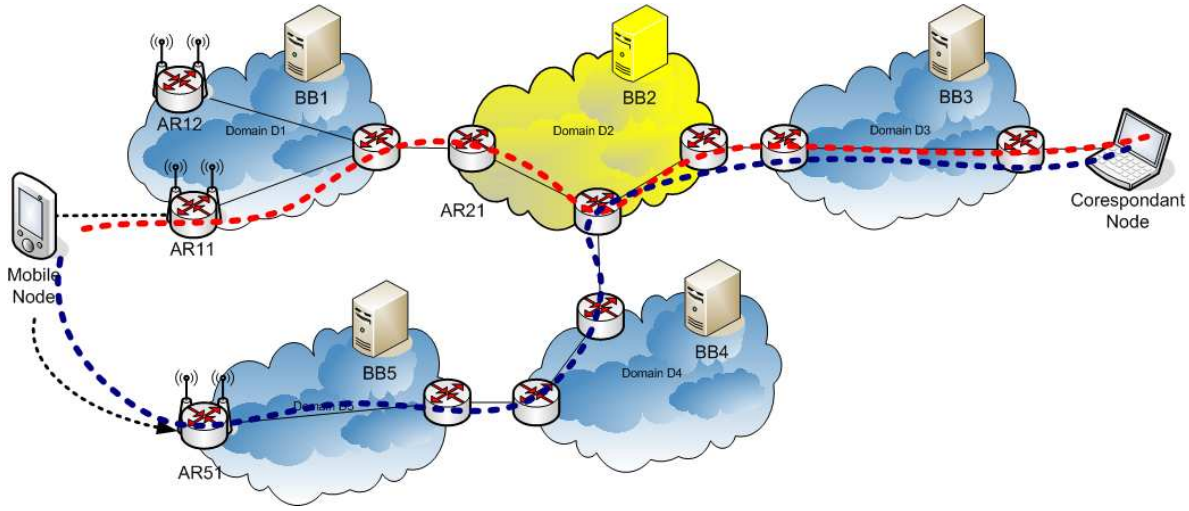


Figure 41 : Domaine « Cross-Over » dans le changement de la signalisation

Ce modèle permet donc d'optimiser la gestion des ressources suite à une macro mobilité (la micro mobilité étant confinée à l'intérieur d'un domaine). Les ressources seront donc réservées jusqu'au Bandwidth Broker du domaine cross-over et relâchées sur la branche qui n'est plus utilisée par la suite. Il est à noter que les domaines cross-over pour le trafic en amont et en aval peuvent être différents (du fait de la non-symétrie des chemins). Une procédure de signalisation (et recherche du domaine cross-over) doit être donc entamée aussi suivant le schéma initié par le récepteur, telle que décrite dans la section 2.2.3.

2.5.2.5. Conclusions

Cette section a traité le problème de la signalisation pour la QoS dans un contexte multi-domaine qui vise à assurer la continuité du service suite à la modification de la topologie causée par la mobilité. Elle a illustré une étude pour la faisabilité de l'approche proposée qui est de mettre en place des mécanismes de signalisation conceptuellement simples qui étendent la signalisation initiale afin de garantir la QoS de bout-en-bout dans un environnement mobile.

2.6. Conclusions

Les travaux présentés dans ce chapitre visent à proposer une architecture de signalisation pour la garantie de la qualité de service dans un environnent multi-domaine hétérogène. L'objectif était d'optimiser d'une part l'utilisation des ressources du système de communication et d'autre part d'introduire le minimum de contraintes pour les administrateurs et les fournisseurs de services.

Nous avons tout d'abord défini le modèle multi-domaine qui constitue le support pour l'architecture de signalisation. Dans un second temps nous avons présenté l'enchainement des PDU et la spécification en UML2.0 de la signalisation proposée. Nous avons participé avec l'Université de Coimbra aux travaux qui ont pour objectif de proposer une signalisation hybride couplée et découplée du chemin de données (« on-path/off-path ») dans le cadre du groupe de travail NSIS de l'IETF. Enfin, nous avons décrit une proposition ayant pour but de mettre en place un provisionnement de service dynamique à la demande qui récupère dans un premier temps les services disponibles au long du chemin de données et qui choisi une concaténation qui répond aux besoins en QoS en optimisant diverses préférences orientées utilisateur ou fournisseur.

Comparativement aux autres signalisations qui suivent la même approche, notre proposition répond non seulement aux besoins de contrôle d'admission mais aussi prend en compte l'hétérogénéité de l'Internet à plusieurs niveaux (multi-domaine, multi-technologie et signalisation) et les domaines surprovisionnés. De plus, nous répondons aussi aux problèmes liés au provisionnement dynamique des services par un mécanisme de découverte des classes de services et de leurs performances au long du chemin de données.

Les deux premières contributions ont été réalisées en partie dans le cadre du projet européen EuQoS. Dans les chapitres suivant nous illustrons leur application, les intégrons dans l'architecture proposée par le projet, et donnons les résultats obtenus suite à leur déploiement sur une plate-forme de test.

3. La signalisation dans le projet EuQoS

Ce chapitre présente dans un premier temps le projet européen EuQoS (www.euqos.eu) qui a constitué le cadre contractuel de cette thèse. Il décrit ensuite comment notre proposition de signalisation hybride HyPath a été intégrée dans l'architecture du projet. Les principales contributions des travaux de cette thèse dans le cadre du projet EuQoS sont :

- la participation à la définition et à la conception de l'architecture générale ;
- la spécification d'une partie de cette architecture (en particulier la signalisation) et son intégration en vue de la simulation avec le logiciel TAU du modèle UML du système EuQoS dans la première phase du projet ;
- la contribution à la conception de la structure de la base de données du RM (RM-DB) ;
- l'implémentation du composant CallController qui prend en charge la signalisation et le contrôle d'admission dans l'architecture EuQoS ;
- l'implémentation de l'interface EQ-SAP qui décrit le service de QoS à la demande offert par EuQoS.
- L'installation, l'administration et la validation d'une plate-forme européenne de test (« testbed ») au LAAS (décrite en détail dans le chapitre 4).
- La participation active à l'intégration et au test du code sur la plate-forme distribuée de mise au point du projet ;

La structure du chapitre est la suivante :

- dans un premier temps (section 3.1), nous introduisons les objectifs et l'organisation du projet. Nous décrivons son architecture générale en précisant les concepts et les mécanismes utilisés ;
- La section 3.2 donne une vue globale de la communication entre les sous-systèmes et les modules d'EuQoS. L'objectif des solutions proposées est de réduire la complexité du système en considérant plusieurs niveaux (verticalement et horizontalement) et en définissant de façon détaillée les interfaces entre ces niveaux.
- La section 3.3 présente en détail la signalisation du système EuQoS, sa spécification et son intégration dans l'architecture définie dans le projet.

3.1. Architecture EuQoS pour la garantie de QoS

3.1.1. Présentation du projet

EuQoS (« End-to-end Quality of Service support over heterogeneous networks ») [Dugeon05] est un projet européen IST[6] du sixième Programme Cadre pour la Recherche et le Développement. La motivation principale du projet est liée à l'utilisation croissante de l'Internet comme infrastructure globale de communication et à la volonté des opérateurs d'offrir de nouveaux services à valeur ajoutée avec QoS garantie.

L'objectif principal d'EuQoS a été de concevoir, de développer, d'implémenter et de démontrer une architecture permettant de garantir la qualité de service de bout-en-bout dans un environnement le plus général possible, multi-opérateur, multi-service et multi-

[6] Information Society Technologies

technologie. De plus, EuQoS a visé un éventail large d'applications nécessitant de la QoS, à savoir : voix sur IP, vidéoconférence, vidéo-streaming, télé-enseignement, télé-engineering et télé-médecine. Le résultat du projet est le « Système EuQoS », déployé sur un ensemble de plates-formes de tests européennes, hétérogènes du point de vue des technologies sous jacentes, et interconnectées par l'intermédiaire du réseau GEANT[7] et des *réseaux nationaux pour l'enseignement et la recherche* (NREN *National Research and Education Network*, par exemple le réseau RENATER pour la France). Rappelons que le projet GEANT est mené par un consortium constitué de 32 NREN et de l'association TERENA (*Trans-European Research and Education Networking Association*), la coordination du projet étant assurée par DANTE (*Delivery of Advanced Network Technology to Europe*).

Le consortium du projet EuQoS se compose de 24 partenaires :

- 5 opérateurs télécommunication : Telefonica I&D (TID), France Telecom (FTR&D), Portugal Telecom Inovação (PTIN), Polish Telecom R&D (PTRD) Polska Telefonia Cyfrowa (PTC-ERA) ;
- 6 corporations : Siemens Business Services (C-LAB SBS), Soluziona, Datamat, Juniper, Ericssons, Hospital Divino Espirito Santo (HDES);
- 5 PME : Martel, Silogic, RedZinc, Telscom AG, PointerCom;
- 8 laboratoires de recherche et universités : LAAS-CNRS, University of Bern, Technical University of Catalonia (UPC), Warsaw University of Technology (WUT), University of Paderborn (UoP-CLAB), University of Coimbra (UoC), University of Rome (UoR/CRMPA), University of Pisa (CPR).

EuQoS a conçu, déployé et validé une architecture globale, qui intègre un large ensemble de mécanismes divers et cohérents, totalement intégrés : autorisation, authentification, négociation de service, contrôle d'admission, signalisation, surveillance et métrologie, ingénierie de trafic et optimisation des ressources.

L'organisation des taches (*Work Packages - WP*) a été la suivante :

- WP 1 - Business Model and System Design. Le rôle du WP1 était de concevoir le système EuQoS en prenant en compte les technologies existantes ou en cours d'étude. D'une part, le WP1 a identifié et conçu les éléments principaux de l'architecture (les fonctions, les composants, les interfaces) et a étudié le modèle de marché (« Business Model ») pour créer des nouvelles relations entre les utilisateurs et les fournisseurs de réseaux et de services.
- WP 2 - Validation of the EuQoS System. L'objectif de ce WP était double: d'une part valider les capacités du système à garantir la QoS par l'intermédiaire des outils de simulations développés par les partenaires du projet ; d'autre part, proposer des outils de surveillance et de mesure pour valider l'architecture déployée sur une plate-forme européenne.
- WP 3 - Implementation of the EuQoS System. L'objectif principal du WP3 a été l'implémentation de l'architecture EuQoS. Ces travaux ont été menés en plusieurs étapes qui ont conduit à 5 prototypes intégrés, déployés et démontrés lors des diverses revues.
- WP 4 - Adaptation of Applications. Les travaux de ce WP ont porté sur la conception des applications et/ou leur adaptation au système EuQoS, avec trois objectifs : (1) l'identification des besoins en QoS pour les applications ; (2) le développement des modules d'adaptation pour les applications existantes dans le but

[7] GEANT est le réseau pan-européen à très haut débit dédié à la recherche et à l'éducation en Europe.

de prendre en compte le système EuQoS et (3) l'intégration dans l'architecture EuQoS de nouvelles applications multimédia déployées sur différents réseaux d'accès.

- WP 5 - EuQoS Pan European trials. WP5 a défini le déploiement, les tests et les mesures sur une plate-forme européenne (en relation avec les WP3 et WP4). Le rôle de ce WP est d'identifier les types d'environnement réseaux à utiliser (« testbeds »), de les configurer, de réaliser leur interconnexion via une plate-forme paneuropéenne, de mener des campagnes des tests et de mesurer et analyser les résultats.
- WP 6 - Dissemination, Standards and Training. Les objectifs du WP étaient multiples: (1) développer un ensemble d'outils qui compose un environnement d'enseignement à distance pour différents types de public ; (2) concevoir et adapter le contenu des enseignements à fournir ; (3) publier et rendre accessible le contenu des divers cours; (4) disséminer les résultats scientifiques et techniques ; (5) contribuer aux activités de standardisation, en particulier à l'IETF.
- WP 7 - Project Management. Le rôle du WP7 était la coordination interne du projet et son administration.

Les travaux décrits dans cette thèse s'inscrivent principalement dans les WP1, WP3, WP5 et WP6, mais nous avons également participé dans le cadre du WP2 aux travaux de surveillance et de mesure, et dans le WP4 à l'intégration des applications réalisées avec la signalisation d'EuQoS.

3.1.2. Architecture générale

Cette section a pour objectif de présenter les concepts généraux de l'architecture EuQoS. Elle introduit les notions utilisées, la structure et les composants du système global. Par rapport aux travaux précédents, l'architecture EuQoS a pour fort intérêt d'offrir une solution générale, qui intègre dans une vision globale un ensemble de mécanismes : signalisation, contrôle d'admission, surveillance, ingénierie de trafic allocation des ressources, etc. De plus, le système EuQoS, en prenant en compte les propositions et les standards existants, a développé une solution modulaire multi-niveau, dont chaque composante a des fonctionnalités précises. EuQoS a permis de reconsidérer et de concevoir sur des nouvelles bases les propositions architecturales antérieures. De plus, il les a étendu pour les intégrer dans une architecture complète, cohérente et ouverte.

L'architecture du projet repose sur les principes suivants (Figure 42) :

- La prise en compte d'un contexte général, multi-domaine, ces domaines étant tous hétérogènes du point de vue de leurs technologies sous-jacentes ;
- La gestion du domaine par une entité fonctionnelle, étendant les Bandwidth Brokers, appelée Resource Manager (RM) ;
- La distinction de trois plans pour la gestion de la qualité de service : Plan de Service, Plan de Contrôle et Plan de Transport ;
- La définition des « Classes de services Réseau » de bout-en-bout, multi-domaines (end-to-end CoS), qui seront alors associées à des familles d'application dont les valeurs des paramètres de QoS sont bien définies ;
- L'utilisation d'un mécanisme de routage prenant en compte la QoS, le protocole utilisé étant EQ-BGP, une variante enrichie du protocole BGP standard ;
- La distinction des deux entités dans le cadre du système, le client EuQoS (logiciels situés dans le terminal utilisateur) et le serveur EuQoS (le cœur qui met en place les mécanismes pour la garantie de QoS tout au long du chemin des données) ;

- L'adaptation ou l'extension de protocoles standards ou en cours de développement (en particulier ceux de l'IETF), reconsidérés pour prendre en compte les besoins de garantie de QoS. Ainsi dans le cadre d'EuQoS de nouveaux protocoles ont été conçus et développés, tels que EQ-SIP, EQ-NSIS ou EQ-BGP.

3.1.2.1. Les plans de gestion et de déploiement de la QoS

L'architecture du système EuQoS a été conçue suivant un principe modulaire qui vise à réduire sa complexité et à coordonner efficacement ses sous-systèmes : le modèle de gestion de la QoS a été divisé verticalement (Plan de Service, Plan de Contrôle et Plan de Transport) et horizontalement (suivant les domaines et les Systèmes Autonomes). Ce modèle est donné dans la Figure 42.

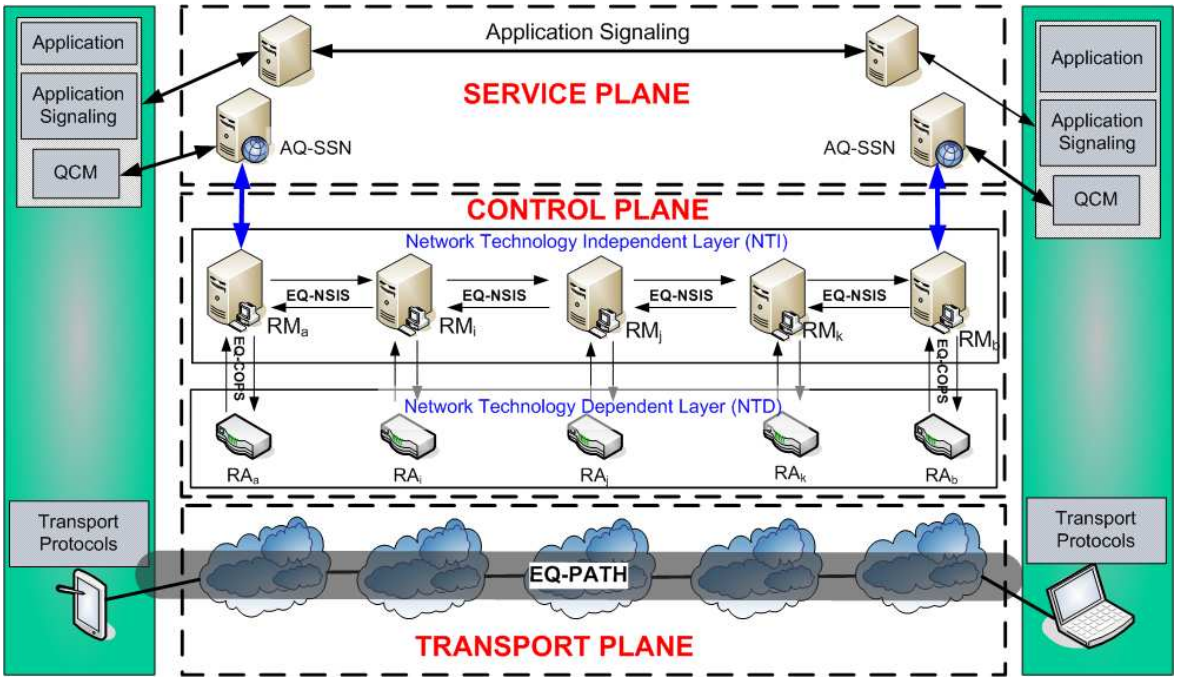


Figure 42 : Architecture générale EuQoS

Le **plan de service** offre différents interfaces pour accéder aux services proposés par EuQoS (communication directe pour les applications totalement compatibles EuQoS, interface WEB ouverte, extension du protocole NSIS). Il permet de plus de déclencher le processus respectivement de choix et de réservation des ressources applicatives et réseau (voir section 3.3). En outre, ce niveau est aussi responsable de la sécurité, de l'authentification, de l'autorisation et de la tarification (SAAA). Par ailleurs, il fournit un mécanisme de filtrage des requêtes de QoS selon les profils et droits des utilisateurs.

Le **plan de contrôle** assure la gestion de la QoS tout au long du chemin des données. Il implémente des mécanismes pour la translation des paramètres de QoS fournis par les niveaux supérieurs en paramètres spécifiques à chaque domaine et gère les processus réservation des ressources sur ce chemin. Dans l'architecture EuQoS, le plan de contrôle a été divisé en deux niveaux :

- Un niveau générique, indépendant de la technologie sous jacente (NTI-Network Technology Independent) ;
- Un niveau dépendant de la technologie sous jacente (NTD-Network Technology Dependent), donc spécifique à chaque type de réseau.

Cette séparation vise à faciliter l'interconnexion de nouveaux domaines et des nouvelles technologies par leur intégration simple au niveau NTD, niveau réalisé et implanté par chaque concepteur ou administrateur de domaine, de manière optimale en fonction de la technologie. Le niveau NTI, qui constitue l'idée majeure du projet EuQoS, est ainsi défini comme générique pour tous les domaines[8], afin de fournir les interfaces nécessaires pour les interconnexions avec les domaines adjacents (communication horizontale) d'une part et avec les composants spécifiques à l'intérieur de chaque domaine (communication verticale) d'autre part.

Le **plan de transport** est composé d'un ensemble de mécanismes et équipements qui sont gérés par les entités du plan de contrôle. Le rôle du plan de transport est de « construire » le chemin suivi par les données et traversant plusieurs domaines et technologies. Ce chemin porte le nom d'EQ-Path, sa création étant détaillée dans la section 3.1.3 relative au provisionnement dans EuQoS.

3.1.2.2. Composants logiciels

La Figure 43 détaille les composantes de l'architecture EuQoS, leur localisation (coté client ou serveur), ainsi que les méthodes de communication entre ces différents composants, notamment les protocoles utilisés pour transporter l'information.

Le client EuQoS, localisé sur l'équipement utilisateur, est constitué des modules suivants :

- l'application qui exprime des besoins en QoS ;
- le module « Application Signaling » qui permet d'échanger des informations de signalisation entre les terminaux utilisateurs.
- le module QCM (Quality Control Module), qui prend en charge l'adaptation des paramètres au système EuQoS et l'invocation du service offert par le serveur. Tous ces composants appartient au plan de service ;
- le module « Transport Protocols », situé dans le plan de transport et dans la couche OSI transport (voir section 1.2.5), qui fournit, en plus des protocoles classiques (TCP, UDP) des mécanismes, des protocoles et des services enrichis (tel que ETP, présenté dans la section 1.2.5), pour le transfert de données.

[8] Il est a remarqué que certains fonctionnalités du NTI peuvent dépendre de l'implémentation spécifique à chaque domaine (les mécanismes de métrologie, d'ingénierie de trafic, etc). En revanche, pour faciliter l'interconnexion, les interfaces ne doivent pas être modifiées, seule leur implémentation étant variable.

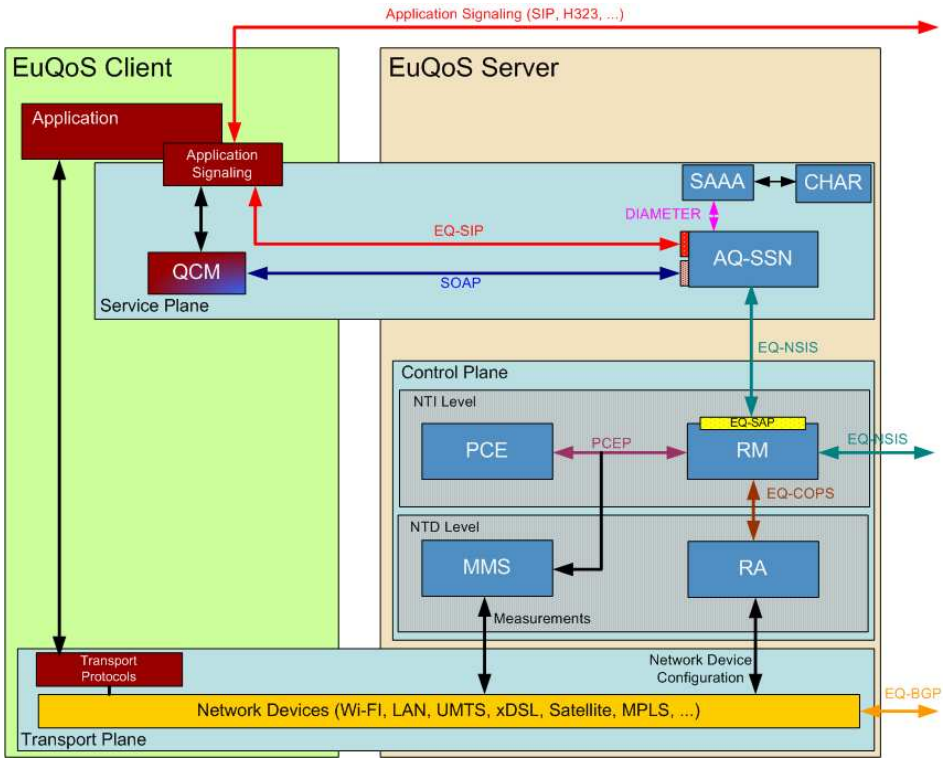


Figure 43 : Composants de l'architecture EuQoS

Le serveur EuQoS implante les trois plans détaillés précédemment :

- le plan de service est composé de trois sous modules :
  - AQ-SSN (Application Quality Service Signaling Negotiation) qui offre l'accès au service EuQoS pour ses utilisateurs. Il fournit une interface basée sur SOAP (Simple Object Access Protocol - http://www.w3.org/TR/soap/) ;
  - CHAR (charging), qui prend en compte la tarification du service ;
  - SAAA qui est en charge de l'authentification, de l'autorisation des utilisateurs et de la comptabilité. Il communique les données récoltées au module de tarification (CHAR) et échange des messages avec AQ-SSN par le protocole Diameter ;
- le plan de contrôle est constitué des niveaux NTI et NTD :
  - Le niveau NTI comprend deux composants principaux : le Resource Manager (RM) en charge de la gestion du domaine et le Path Computation Element (PCE) [Farel06] en charge du provisionnement réseau. Ces deux éléments communiquent par l'intermédiaire du PCEP (Protocole PCE).
  - Le niveau NTD implante des fonctionnalités liées à la gestion spécifique de la QoS suivant la technologie sous-jacente ; il est constitué de deux modules, le Resource Allocator (RA), en charge du traitement des requêtes de QoS et le Monitoring et Measurement System (MMS), pour assurer la surveillance et la métrologie du réseau. La communication entre les modules RM et RA s'effectue par le biais du protocole EQ-COPS.
- le plan de transport a pour but d'assurer le transfert des données sur le chemin traversant plusieurs domaines. Il présente des interfaces avec les composants du NTD (RA et MMS) et intervient dans le transfert des données du client. Ses modules n'étant pas indispensables à la compréhension de nos travaux, ils ne seront pas donnés ici.

Toutes ces composantes fournissent les fonctions principales du système EuQoS [D121] :

- Signaling and Service Negociation (SSN), qui permet la négociation des services et l'installation des ressources en utilisant une signalisation adaptée.
- Connection Admission Control (CAC), qui décide si une nouvelle connexion est acceptée en fonction de la requête de QoS et de l'état actuel du réseau.
- Monitoring, Measurement, Fault Management (MMFM), qui assure la surveillance du réseau, rassemble des informations sur la topologie et la disponibilité des ressources pour soutenir le CAC, et gère les défaillances.
- Trafic Engineering and Resource Optimisation (TERO), dont l'objectif principal est de contrôler et d'optimiser le processus de routage et l'utilisation des ressources.

3.1.2.3. Les classes de service de bout-en-bout d'EuQoS (e2e CoS)

Afin de garantir les propriétés de QoS, EuQoS a défini dans le réseau des classes de services. Ces classes sont associées à des familles d'applications et leurs paramètres de QoS ont une portée de bout en bout pour les réseaux (e2e CoS), pour tous les domaines. La solution proposée consiste donc à définir des e2e CoS suivant les objectifs de QoS et les profils de trafic associés (real time - RT, non real time – NRT, …).

L'implémentation de ces e2e CoS s'appuie sur la mise en place de garanties sur la communication, qui doivent être spécifiées de manière quantitative en termes de paramètres techniques, et traduites en différentes actions au niveau des équipements. Une correspondance entre ces e2e CoS et des classes réseaux spécifiques (telles que AF et EF de DIffServ par exemple) est réalisée au sein de chaque domaine. La Figure 44 illustre la correspondance proposée entre les différents niveaux dans l'architecture EuQoS.

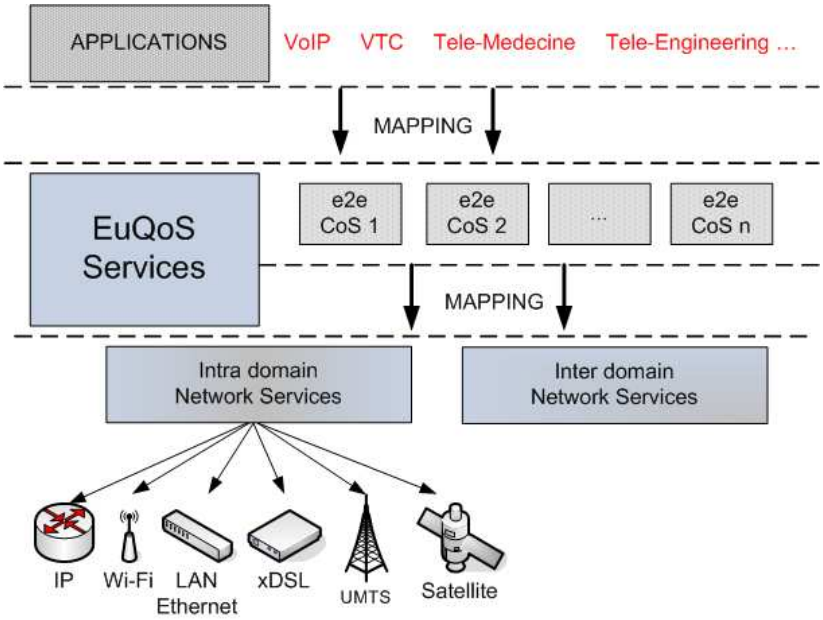


Figure 44 : La correspondance des classes de services dans l'architecture EuQoS

De fait, EuQoS s'appuie sur les définitions de l'ITU-T [ITU-T-Y.1541] et de l'IETF [Babiarz06] pour ses CoS, ainsi supposées connues par les applications (utilisateurs), implémentées et maintenues par les fournisseurs, indépendamment du type de réseau sous jacent.

Ces e2e CoS constituent donc des valeurs bien définies pour les paramètres de QoS et déployées dans les réseaux, pour toutes les différentes technologies, et en particulier celles

étudiées dans EuQoS (xDSL, LAN, Wi-Fi, UMTS, Satellite ou réseau de cœur). Le Tableau 5 résume la solution adoptée, la dénomination des e2e CoS, les types de trafic (agrégats) associés, les objectifs de QoS visés ainsi que la correspondance pour les applications développées dans EuQoS :

Trafic Aggregate	End-to-end Class Of Service	QoS Objectives			EuQoS Applications							
		IPLR	Mean IPTD	IPDV	Nexuiz	VoIP	VTC	VoD	Medigraf			
									VTC	Collaboration	Data transfer	Chat
CTRL	Network Control	10^{-3}	100 ms	50ms								
Real Time	Telephony	10^{-3}	100/350 ms (local/long distance)	50ms		**X**						
	Signalling	10^{-3}	100 ms	U								
	MM Conferencing	10^{-3}	100 ms	50ms								
	RT Interactive	10^{-3}	100/350 ms (local/long distance)	50ms	**X**		**X**		**X**			
	Broadcast Video	10^{-3}	100ms	50ms								
Non Real Time (Assured Elastic)	MM Streaming	10^{-3}	1s non critical	U				**X**				
	Low Latency Data	10^{-3}	400 ms	U								
	OAM	10^{-3}	400 ms	U								
	High Throughput Data	10^{-3}	1s non critical	U							**X**	
Elastic	Standard	U	U	U								**X**
	Low Priority Data	U	U	U								

Tableau 5 : Les Classes de Service de bout-en-bout dans EuQoS

Le délivrable [D113] fournit de plus amples détails sur les e2e CoS EuQoS. Une mise en œuvre pour chaque technologie considérée est donnée également dans l'annexe du [D113].

3.1.2.4. Définition des EQ-Path

Un des objectifs principaux d'EuQoS étant la création des chemins à QoS garantie, de bout-en-bout, à travers plusieurs domaines (AS), le projet a défini la notion de chemins, les « EQ-Path ». Un EQ-Path est donc un chemin entre le domaine source et le domaine destination qui offre des garanties de QoS. Chaque EQ-Path est associé à un ensemble de paramètres de QoS, en particulier à une e2e CoS.

3.1.2.5. Protocole EQ-BGP

Afin de définir ces chemins, EuQoS a adopté un modèle de routage à QoS, considérant une route inter-domaine pour chaque CoS requise. De ce fait, il propose l'utilisation d'un protocole de routage inter-domaine à QoS, EQ-BGP (Enhanced QoS Broder Gateway Protocol) [D111], [D113], [Masip07]. EQ-BGP est une variante enrichie du protocole de routage inter-domaine utilisé actuellement dans l'Internet, BGP-v4, décrit dans le chapitre 1. Son objectif est d'établir et d'annoncer des routes qui assurent la continuité du service et répondent aux besoins des différentes e2e CoS. Pour cela, un routeur EQ-BGP annonce à ces voisins les destinations joignables et fournit de plus des informations sur les CoS disponibles,

ceci avec des paramètres de QoS (IPDV, IPTD, IPLR). En prenant en compte les politiques et les capacités intra et inter-domaine, EQ-BGP choisit la route considérée comme la meilleure (notée « best ») et la propage à ses voisins. En conséquence, EQ-BGP fournit des chemins à QoS entre les paires de domaines source et destination. Ces informations sont ensuite utilisées dans le processus d'invocation des ressources pour : (1) vérifier dans un premier temps s'il existe un chemin (enchainement des domaines) vers la destination, chemin qui offre la CoS considérée, et (2) découvrir le prochain domaine sur le chemin de données pour acheminer la requête.

En outre, ces informations peuvent être utilisées par le module TERO pour l'optimisation des routes. Il est à remarquer que le protocole EQ-BGP permet également d'établir des routes disjointes pour chaque CoS de bout-en-bout entre couples de domaines.

3.1.3. Provisionnement

De manière globale, le provisionnement a pour but de construire les EQ-Path à travers plusieurs domaines dans le cas le plus général. Dans EuQoS, ce processus suit deux modèles, respectivement appelés « loose model » et « hard model ». Nous exposons dans les paragraphes suivants ces deux approches et ensuite nous les comparerons.

3.1.3.1. Provisionnement Loose Model

Dans l'approche « loose model » l'EQ-Path est construit partant du chemin fourni par le protocole de routage inter-domaine EQ-BGP. Suivant le « loose model », les ressources sont provisionnées indépendamment à l'intérieur de chaque domaine, et une signalisation devra être mise en place au moment de la requête de QoS (processus d'invocation) afin d'associer des ressources à l'EQ-Path.

Le principal avantage du « loose model » est qu'il introduit un couplage minimal entre les domaines impliqués sur l'EQ-Path. Il n'implique que l'existence d'accords entre les domaines pairs et la possibilité de mettre en place la signalisation EuQoS. L'inconvénient majeur du « loose model » consiste dans le nombre de messages de signalisation échangés lors d'une réservation/libération des ressources à chaque requête de QoS.

3.1.3.2. Provisionnement « Hard Model »

La deuxième approche proposée dans EuQoS adopte la vision des opérateurs de télécommunication et est fondée sur le concept d'EQ-Link. Un EQ-Link est un lien virtuel entre deux routeurs de bordure, potentiellement dans des domaines non adjacents (mécanisme de tunnel). L'EQ-Link présente des caractéristiques de QoS bien définies entre ces deux nœuds : les EQ-Links sont associés à une CoS spécifique pour laquelle les ressources sont réservées en avance. Ainsi, un EQ-Path peut être construit dans le processus de provisionnement par la demande d'établissement d'un EQ-Link entre deux de ces réseaux (domaines). Les EQ-Link qui traversent plusieurs domaines sont considérés comme des liens inter-domaines par les autres modules de l'architecture. Par la suite, nous verrons que le mécanisme de signalisation n'est pas affecté par la création des EQ-Links. En pratique, les EQ-Links EuQoS sont établis en tant que tunnels, par exemple DiffServ MPLS-TE, et peuvent traverser plusieurs AS. La mise en place du provisionnement « hard-model » repose sur l'architecture Path Computation Element (PCE), du groupe de travail dans le cadre de l'IETF [http://www.ietf.org/html.charters/pce-charter.html]. L'annexe de [D122] détaille le mécanisme d'établissement des EQ-Link dans EuQoS.

L'approche de provisionnement « hard model » présente de bonnes propriétés vis-à-vis du facteur de passage à l'échelle : il réduit le nombre de messages de signalisation échangés. En fait, la signalisation n'est nécessaire que dans le domaine d'accès, à l'entrée de l'EQ-Link (pour le contrôle d'admission). Néanmoins, ce type de provisionnement nécessite une forte coopération entre les AS et sa mise en place est plus complexe. De plus, il n'est applicable que dans certains réseaux de cœur, e.g. ceux qui implémentent des mécanismes de type DiffServ MPLS-TE.

3.1.3.3. Comparaison entre les approches « loose » et « hard »

Le Tableau 6 résume les principaux avantages et inconvénients des solutions de provisionnement adoptées dans le projet EuQoS.

	Loose Model	***Hard Model***
Avantages	- Couplage minimal entre les domaines ; - Contraintes minimales concernant le déploiement sur les différentes technologies et politiques opérateurs	- Résistance au facteur de passage à l'échelle (signalisation réduite, dans les domaines d'accès et CAC en entrée de l'EQ-Link) - Optimisation du provisionnement en profitant des chemins multiples possibles sur la base des CoS
Inconvénients	- Un contrôle d'admission par-flux et nécessaire dans les RM de chaque AS sur l'EQ-Path - Volume important des messages de contrôle d'admission échangés	- Procédure de mise en place complexe - Fort couplage entre les domaines

Tableau 6 : Comparaisons «loose model » - « hard model »

L'architecture finale du projet EuQoS, capable d'intégrer les deux approches, propose ainsi un cadre général et flexible, qui permet l'adoption et l'intégration des deux solutions exposées précédemment. En général, les EQ-Links ne sont pas établis de bout-en-bout (entre deux domaines d'accès), mais ils couvriront une portion de l'EQ-Path. Par conséquent, un EQ-Path peut être construit, de manière souple, de divers segments qui alternent les modèles « loose » et « hard ». En outre, la présence des EQ-links dans l'EQ-Path est transparente dans le processus de réservation, en particulier pour la signalisation et le contrôle d'admission, comme nous allons le voir.

3.1.4. Contrôle d'admission (CAC) dans EuQoS

3.1.4.1. Introduction

Le contrôle d'admission est un élément clé de l'architecture EuQoS, compte tenu de la diversité des technologies couvertes. Pour atteindre son but, EuQoS considère plusieurs types de CAC, repartis sur les niveaux NTI et NTD :

- Un CAC intra-domaine, inter-domaine et de bout-en-bout (e2e) indépendant des technologies réseaux sous jacents. Le processus de vérification des ressources est réalisé sur les données présentes dans une base de données.
- Un CAC lié à la technologie sous jacente, qui implante le contrôle d'admission spécifique à chaque type de réseau. Le processus de vérification de la disponibilité met alors en œuvre des algorithmes dépendants de la technologie réseau. (LAN, xDSL, Wi-Fi, UMTS ou Satellite).

De plus, les modules de CAC manipulent des paramètres de QoS à plusieurs niveaux. Ces paramètres, précisés dans les contrats (SLA, voir section 1.3.2.3) établis avec les clients, sont spécifiés dans les SLS (Service Level Specification voir section 1.3.2.3). Différents aspects des SLS ont été définis dans l'architecture proposée dans EuQoS :

- a-SLS : paramètres reçus par le RM, en particulier le premier sur l'EQ-Path;
- e-SLS : paramètres du SLS relatifs au chemin de bout-en-bout ;
- d-SLS : paramètres à QoS concernant le domaine géré par le RM (intra-domaine) ;
- i-SLS : paramètres liés à la partie inter-domaine ;
- r-SLS : paramètres passés au prochain RM.

En tenant compte de cette structure, le CAC a été divisé en sous-modules répartis de manière hiérarchique dans les composantes RM et RA. Ces modules sont le CAC de bout en bout (End-to-End CAC), le CAC à l'intérieur d'un domaine (Intra Domain CAC), le CAC inter-domaine (Inter Domain CAC) et le CAC de la technologie sous-jacente (UN CAC). La portée de chacun de ces types de contrôle d'admission est illustrée dans la Figure 45.

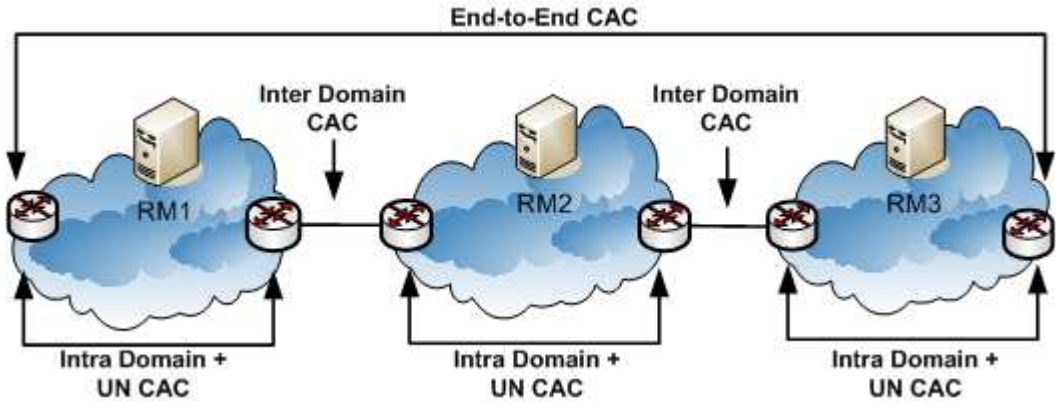


Figure 45 : Portée du contrôle d'admission

3.1.4.2. CAC de bout en bout (End-to-end CAC)

Ce module prend en charge la vérification de l'existence d'un chemin de bout-en-bout (EQ-Path) correspondant à la CoS e2e requise dans les paramètres de QoS. Notons que l'EQ-Path est examiné une seule fois pour trouver la séquence de domaines entre la source et la destination. Bien que le module e2e CAC soit implémenté par tous les RM, il est sollicité seulement dans le RM du premier domaine sur le chemin de données.

3.1.4.3. CAC intra-domaine (intra domain CAC)

Même si un EQ-Path qui répond aux besoins en QoS a été trouvé, il est possible qu'au moment de la requête les ressources ne soient pas disponibles tout au long du chemin.

Le CAC intra-domaine est spécifique à chaque domaine ; il est donc difficile de définir un mécanisme générique efficace applicable à toutes les technologies. Une solution serait d'adopter une démarche similaire à celle que nous avons proposée dans le chapitre 2, en tenant compte que ce module agit au niveau indépendant de la technologie. L'approche adoptée en EuQoS a été de laisser l'implémentation de ce module à chaque administrateur de

domaine qui pourra aussi tenir compte du type de réseau sous jacent, par exemple en délégant le CAC au RA.

3.1.4.4. CAC inter-domaine (inter domain CAC)

Pour garantir la QoS de bout en bout, le CAC doit être prolongé sur les liens inter-domaines. EuQoS défini un module spécifique qui prend en charge la vérification de la disponibilité des ressources sur ces liens inter-domaines (sur chaque lien de peering du « loose model » et sur chaque lien virtuel crée du « hard model »).

3.1.5. Principe de signalisation dans EuQoS

La signalisation jouant un rôle primordial dans EuQoS, introduisons dans cette section les notions de base, sur lesquelles nous reviendrons en détail dans la section 3.3. Le processus de signalisation intervient dans les phases de réservation, transfert ou libération des ressources et peut être initié par les terminaux utilisateurs, des proxys applicatifs (AQ-SSN, Home Gateway) ou des éléments réseaux (routeurs ayant des fonctionnalités avancées).

EuQoS divise la fonction de signalisation, appelée SSN (Signaling and Service Negotiation) en trois parties afin de gérer au mieux la QoS : Application SSN (A-SSN), Resource Manager SSN (RM-SSN) et Resource Allocator SSN (RA-SSN).

3.1.5.1. Signalisation Applicative (A-SSN)

A-SSN gère la signalisation de niveau applicatif, en particulier sur le premier et le dernier domaine. Pour établir, maintenir et fermer des sessions avec des garanties de QoS, il est nécessaire que les applications expriment leur besoins et pour cela qu'elles interagissent avec le système. Les principales fonctionnalités remplies par les modules du niveau A-SSN sont :

- l'identification des exigences en QoS ;
- la négociation et la définition des caractéristiques entre les terminaux utilisateurs ;
- l'initiation et la libération des ressources coté serveur.

Pour répondre à ces besoins, une interaction avec le plan de contrôle est impérative, en particulier avec le RM. Par ailleurs, EuQoS permet d'intégrer des applications utilisant leurs mécanismes propres de signalisation.

3.1.5.2. Signalisation niveau indépendant de la technologie (RM-SSN)

RM-SSN fournit les mécanismes nécessaires pour la mise en place de la réservation sur tous les domaines au long du chemin de données : les fonctions de signalisation agissent de RM en RM (au niveau indépendant de la technologie). Le module en charge de piloter ces mécanismes est le CallController (module détaillé dans la section 3.3.2), qui utilise, pour la signalisation un protocole appelé EQ-NSIS. EQ-NSIS met en œuvre une signalisation découplée du chemin de données et repose sur le mécanisme HyPath présenté dans le chapitre 2.

Les principales fonctionnalités du RM-SSN sont :

- l'activation et la négociation des paramètres avec les domaines adjacents pour atteindre le niveau de QoS requis ;
- la vérification de la disponibilité des ressources (via le CAC) ;
- le support pour les modules MMFM et TERO ;
- la gestion des sessions en cours ;

- la libération des ressources.

3.1.5.3. Signalisation niveau dépendant de la technologie (RA-SSN)

RA-SSN assure le support pour la signalisation et le CAC intra-domaine au niveau dépendant de la technologie. La communication entre le RA et le RM utilise le protocole COPS, et pour configurer les équipements différentes approches sont envisageables : COPS, SNMP, CLI.

La Figure 46 identifie les modules et les différentes approches de signalisation exposées précédemment.

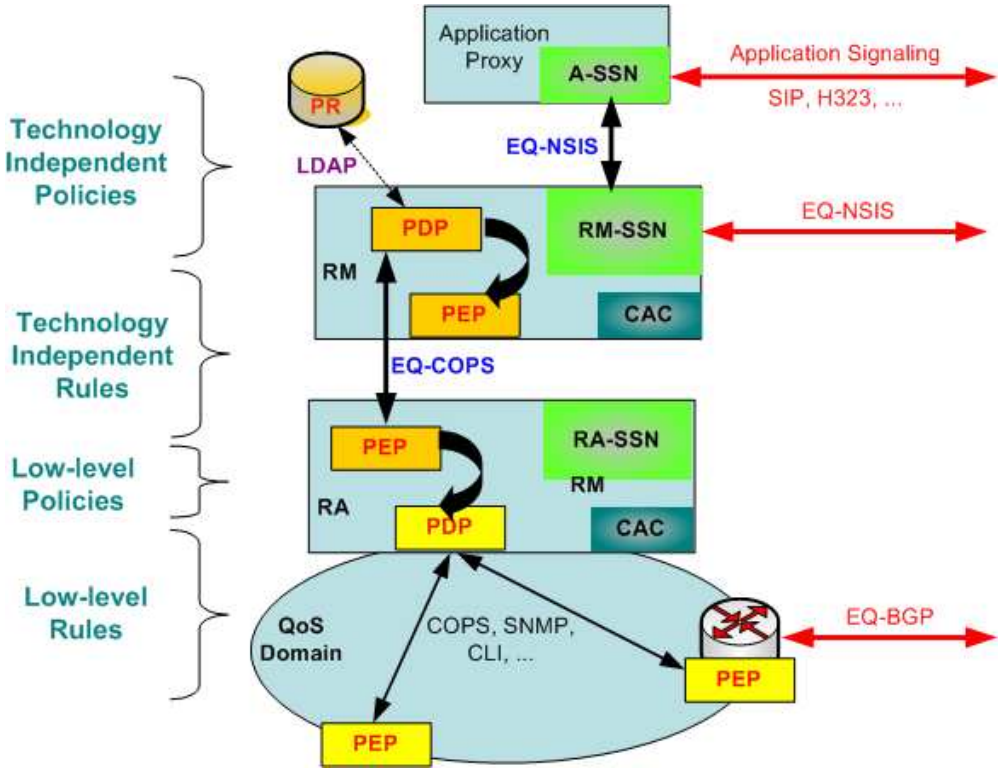


Figure 46 : Signalisation dans EuQoS

Attirons l'attention sur la terminologie utilisée dans le projet : A-SSN, RM-SSN et RA-SSN désignent les fonctions de signalisation, qui sont mises en œuvre respectivement par les modules AQ-SSN, RM-SSN et RA-SSN.

3.2. Définition des interfaces entre les composantes EuQoS

3.2.1. Concepts généraux

Afin de présenter synthétiquement les modules, cette section introduit une représentation hiérarchique simplifiée de l'architecture EuQoS. Ce nouveau modèle, structuré en couches (Figure 47,) cache la complexité de la structure interne de chaque couche (composantes et algorithmes) par une vue boîte noire, et seules les interactions et les interfaces (services) offertes par chaque niveau sont illustrées.

Chaque niveau réalise ses protocoles et interagit verticalement avec les niveaux adjacents, et horizontalement avec le niveau correspondant d'un domaine adjacent. Observons qu'il n'y a

pas de recouvrement de niveau (cross-layering), chaque niveau offrant le service de niveau « N » au niveau supérieur (« N+1 ») et utilisant le service fourni par le niveau immédiatement inférieur (« N-1 »). De la même manière, les messages échangés entre les différents domaines ne le sont qu'entre les entités de niveau « N ».

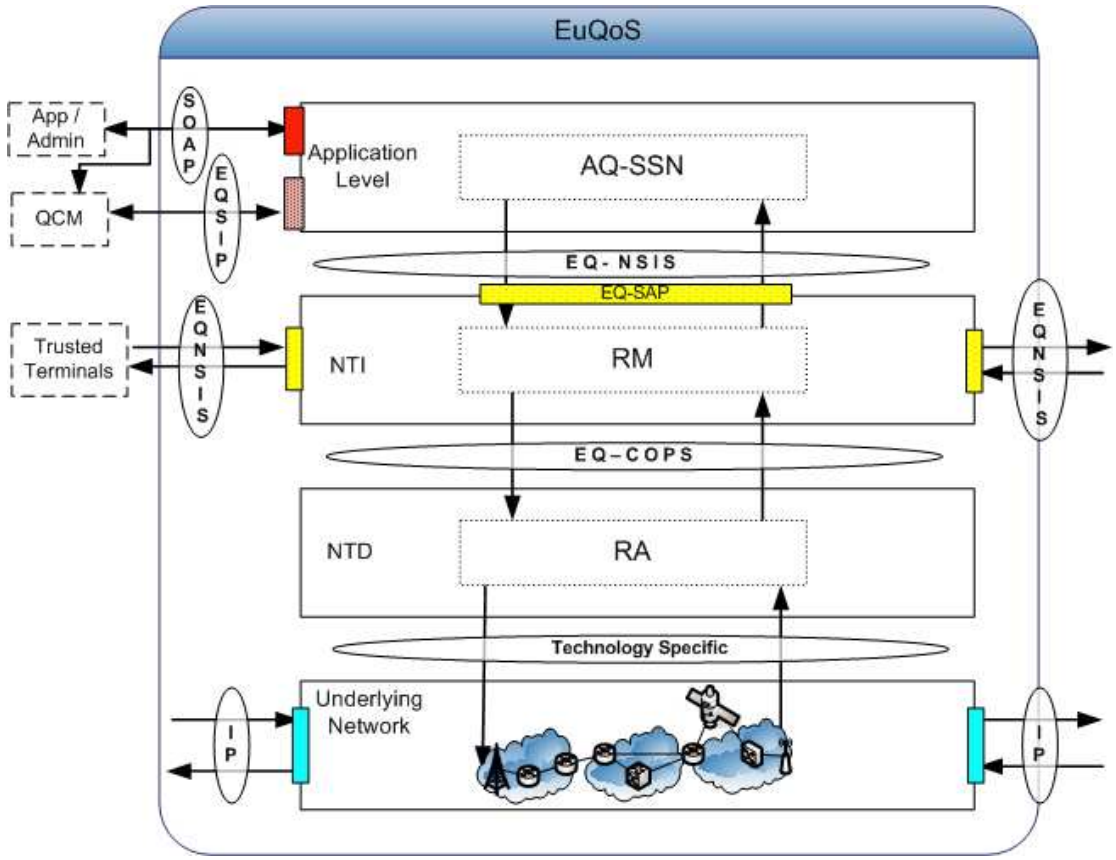


Figure 47 : Modèle Architecture EuQoS

Quatre niveaux sont représentés dans la Figure 47 :

- Le niveau Applicatif regroupe les modules AQ-SSN (avec QSSN et SSM), SAAA et CHAR. Il reçoit les requêtes d'invocation des terminaux clients et interagit avec le niveau inférieur, le NTI.
- Le niveau NTI, représenté par le RM et le PCE, est le cœur du système EuQoS. Il communique horizontalement avec le niveau NTI des domaines adjacents, et peut recevoir les requêtes des terminaux ou proxys via l'interface EQ-SAP (EuQoS Service Access Point, détaillé dans la section 3.2.2.3). Sur le plan vertical, il offre des services au niveau applicatif et utilise ceux fournis par le niveau NTD.
- Le niveau NTD correspond au modules RA et MMS. Notons qu'il n'a pas d'interaction horizontale et qu'il offre des services au niveau NTI.
- Le niveau technologie réseau couvre le plan de transport physique du système EuQoS. Il assure les connexions réelles entre les domaines et fournit le support technologique pour le transport de l'information.

3.2.2. Description des interfaces entre les modules EuQoS

Décrivons maintenant les services et les interfaces offerts par chaque niveau ainsi que les protocoles utilisés pour la communication entre les différents composants, en détaillant les

interfaces à l'intérieur du niveau NTI car nous avons participé activement à leur définition et implémentation.
Cette architecture permet de gérer plusieurs cas d'utilisation pour l'invocation du service de QoS:

- Cas 1 : par des applications qui peuvent s'intégrer dans l'architecture EuQoS en utilisant le protocole EQ-SIP ;
- Cas 2 : par des applications ayant leur propre négociation applicative et qui peuvent s'intégrer dans l'architecture EuQoS en utilisant le module QCM ;
- Cas 3 : par toute autre application (notamment celles déjà existantes) qui ne s'intègre pas directement dans EuQoS mais qui peut utiliser autre entité afin de réserver les ressources à sa place via une interface WEB ;
- Cas 4 : par des entités dites « de confiance », via l'interface EQ-SAP implémentée par le CallController dans le RM.

Nous allons décrire dans un premier temps le service de QoS à la demande offert pas EuQoS. Rappelons que le service de QoS à la demande permet d'établir, modifier et fermer une session EuQoS. Il supporte des transactions requête-réponse et fournit un transfert fiable des messages. Dans ce contexte, deux points d'accès sont définis pour utiliser le service :

- L'interface fournie par AQ-SSN aux clients, implémentée en utilisant le protocole SOAP.
- L'interface RM-API (EQ-SAP) fournie par le RM (plus exactement le module CallController décrit dans la section 3.3.2) aux terminaux ou proxys connus comme étant « de confiance » (par exemple une home gateway fournie par l'opérateur) qui utilise le protocole EQ-NSIS. Cette même interface est utilisée pour recevoir les messages du plan de service (AQ-SSN) et pour communiquer avec les RM adjacents.

Le Tableau 7 résume le service offert par EuQoS pour établir des sessions à QoS. Ce service de QoS à la demande peut être invoqué soit via les interfaces exposées par le niveau applicatif (AQ-SSN) en utilisant le protocole SOAP, soit plus directement via l'interface EQ-SAP, en utilisant le protocole EQ-NSIS.

	Application QoS Service	***EQ-SAP***
Module qui fourni le service	AQ-SSN	RM (CallController)
Module qui utilise du service	QCM et administrateur via une interface web	AQ-SSN et terminaux de confiance (e.g. « home gateway »)
Conditions requises	Ce service doit offrir des transactions requêtes-réponse et fournir un transfert fiable des messages	Ce service doit offrir des transactions requêtes-réponse et fournir un transfert fiable des messages
Informations échangées	Requêtes : - PerformReservation - ModifyReservation - StopReservation Réponses : - QoSAnswer pour « perform » et « modify » - résultat de l'arrêt de la	Requêtes : - PerformReserveCommit - ModifyReservation - StopReservation Réponses : - Confirmation ou la disponibilité des ressources pour « perform » et

	réservation	« modify » - Pas de réponse pour stop, la libération étant considérée réussie

Tableau 7 : Service offert par le système EuQoS

3.2.2.1. Interface fournie par QCM

L'interface fournie par QCM (Quality Control Module) aux applications est donnée dans la Figure 48. Les premiers services sont utilisés dans le cas 1, les autres dans le cas 2. Les détails des paramètres ainsi que les diagrammes de classes sont présentés dans [Track 2-06]. Pour le cas 4, l'invocation du service fournit par EQ-SAP se fait par des entités authentifiées et autorisées (telles que le « home gateway ») via le protocole EQ-NSIS.

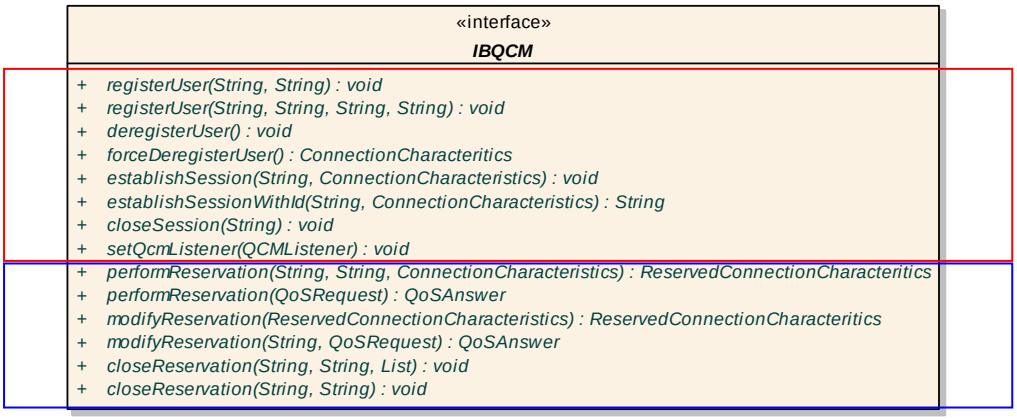


Figure 48 : Interface fournie aux applications par EuQoS

Les services offerts sont les suivants (les 4 premiers dans le cas1, les autres dans le cas 2) :

- *registerUser*, permet l'enregistrement d'un utilisateur EuQoS dans le système ;
- *deregister* et *forceDeregister* sont utilisés pour le dé-enregistrement ;
- *establishSession*, permet à un utilisateur enregistré d'établir une session ;
- *closeSession*, utilisé pour fermer une session en cours ;
- *performReservation*, permet à une application, qui met en place sa signalisation propre, de réserver les ressources ;
- *modifyReservation*, permet de modifier les paramètres d'une réservation ;
- *closeReservation*, utilisé pour fermer une session et libérer les ressources.

Pour une description complète des paramètres échangés, [Track 2-06] contient les autres diagrammes, notamment ceux de classe qui décrivent le type et le nombre de paramètres. Nous reproduisons dans la Figure 49 le diagramme de classe qui détaille les paramètres de QoS requis par le système EuQoS pour réserver les ressources. Nous retrouvons les paramètres spécifiques utilisés dans les messages de signalisation pour mettre en place le contrôle d'admission : le débit, le délai, la gigue, le taux de pertes.

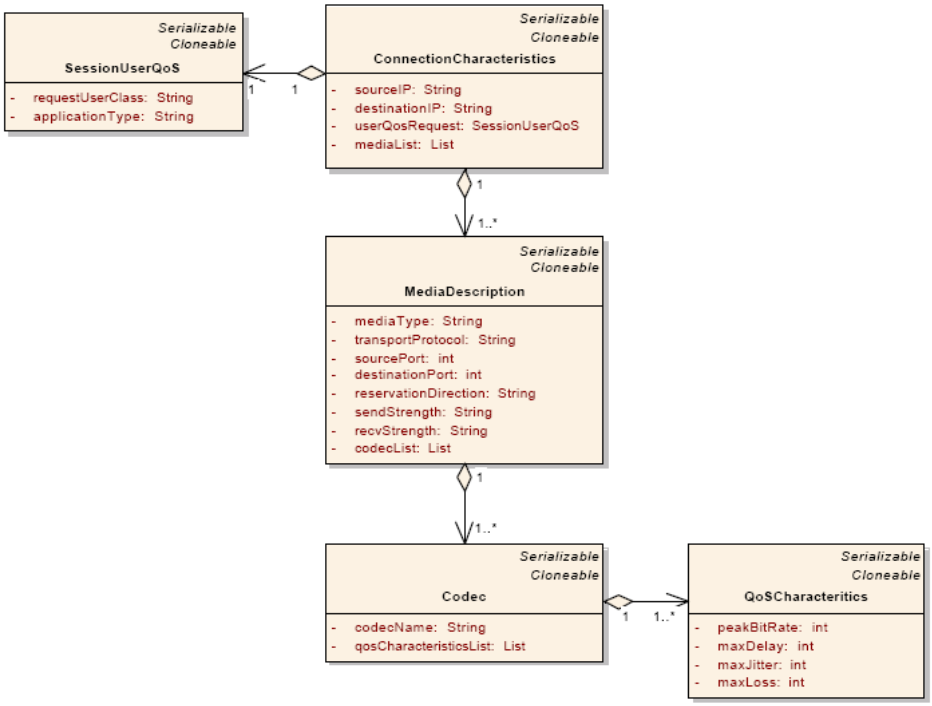


Figure 49 : Diagramme de classe paramètres de QoS

3.2.2.2. Interface fournie par AQ-SSN

La Figure 50 présente le service et les primitives fournis par le module AQ-SSN. Ce service est accessible via une page web ou une implémentation SOAP.

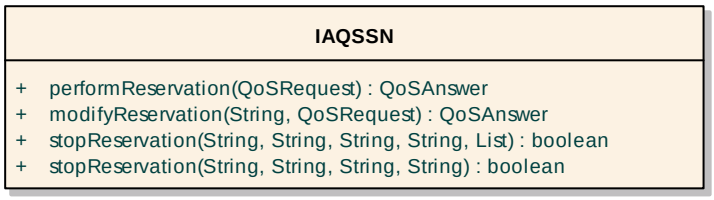


Figure 50 : Interface fournie par AQ-SSN

Les services offerts (*performReservation*, *modifyReservation* et *stopReservation*) ont le même rôle que leurs homonymes présentés précédemment pour le module QCM.

La structure de la requête de réservation (« QoS Request ») est présentée dans le diagramme de classe de la Figure 51.

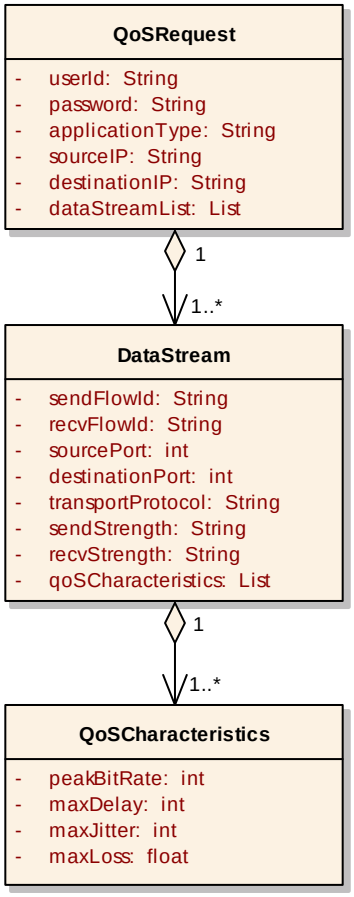


Figure 51 : Structure de la requête de QoS

L'interface entre le NTI et le NTD permet de demander, de confirmer ou de libérer des ressources pour un seul flux. Le protocole COPS est utilisé pour échanger ces messages.

3.2.2.3. Interface fournie par le RM (EQ-SAP)

L'interface EQ-SAP (EuQoS Service Access Point) constitue le service fondamental offert par EuQoS. Cette interface, décrite dans [SLSSpec06], fournit un point d'accès générique au système EuQoS et gère la communication entre AQ-SSN et RM, ainsi que celle entre les RM. Nous avons implémenté et intégré cette interface dans l'architecture du système et nous revenons sur son implémentation dans le chapitre suivant. Cette section présente donc les primitives (illustrées dans la Figure 52) et les paramètres utilisés par EQ-SAP.

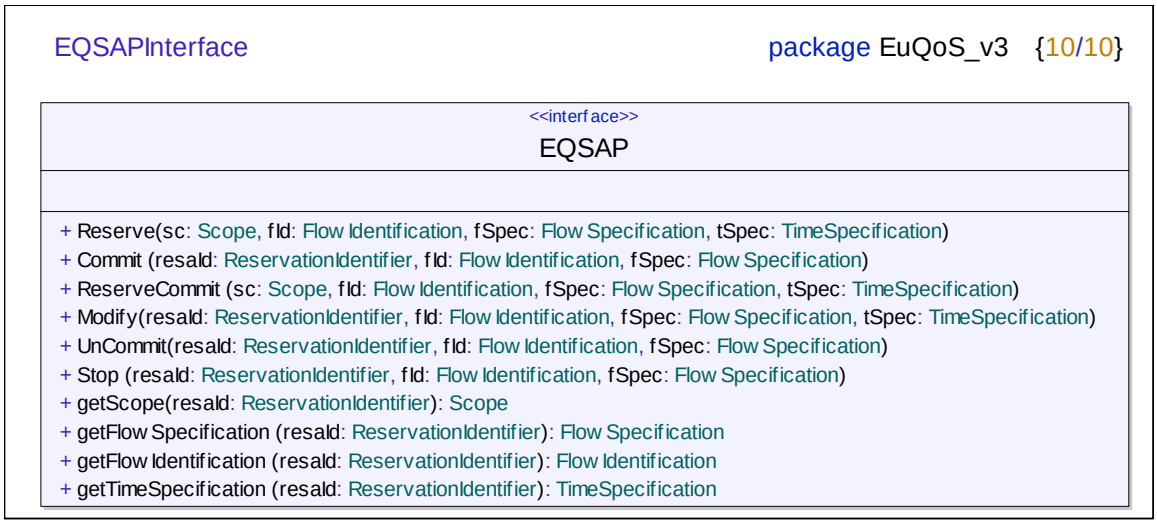


Figure 52 : Interface EQ-SAP

- *Reserve* : permet de réserver les ressources pour garantir la QoS pour une session entre deux nœuds. La QoS correspondante sera confirmée ultérieurement par la primitive « Commit ». Un identifiant de réservation est fourni par le système pour les associations suivantes ;
- *Commit* : permet d'entériner une réservation antérieure, en utilisant l'identifiant obtenu lors de l'appel « Reserve » ;
- *ReserveCommit* : équivalent à l'appel successif des deux primitives précédentes
- *Modify* : permet de modifier les paramètres de QoS initialisés pour une réservation
- *UnCommit* : permet de libérer les ressources associées à une réservation activée par la primitive « Commit » ;
- *Stop* : utilisée pour libérer les ressources associées à une réservation en rétablissant l'état de configuration avant l'appel à la primitive « Reserve ».

Les paramètres utilisés sont classés en quatre catégories :

- « Flow Specification » : spécifie la QoS que le flux va recevoir
- « Flow Identification » : identifie le flux qui recevra la QoS
- « Scope » : représente la portée de la QoS (où elle sera appliquée)
- « Time Specification » : renseigne quand la QoS sera appliquée.

La Figure 53 présente la structure EQ-SAP [SLSSpec06] et détaille les paramètres utilisés évoqués précédemment. La spécification d'un flux comprend la classe de trafic, la description de la classe de service (nom, type, spécification du trafic en termes d'IPTD, d'IPDV, d'IPER et d'IPLR ou le traitement à appliquer en cas d'excès : rejet ou remarquage des paquets). Un flux est identifié soit par un marqueur (type et valeur), soit par le 5-tuple adresse source (ou masque), adresse destination (ou masque), port source (ou intervalle), port destination (ou intervalle) et protocole de transport. La spécification temporelle comprend le temps de début et de fin ou la durée, le temps entre deux activations de la réservation (« offset ») et l'intervalle de répétition. Le « Scope » comprend les adresses IP pour identifier où la QoS est appliquée.

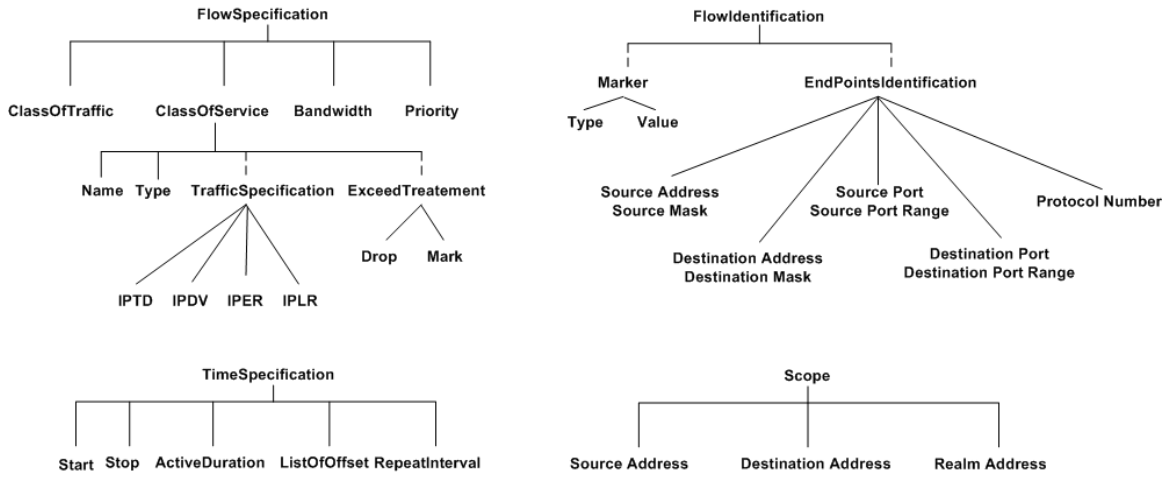


Figure 53 : Structure EQ-SAP

3.3. *La signalisation dans EuQoS*

Après avoir décrit les interfaces offertes par chaque niveau, cette section présente nos contributions sur la signalisation, en particulier le CallController et le fonctionnement général du processus d'invocation (nous reviendrons dans le chapitre 4 sur les simulations réalisées et les tests avec l'implémentation).

3.3.1. Architecture du Resource Manager (RM)

Le Resource Manager (RM), localisé au niveau indépendant de la technologie (NTI), est l'entité centrale du plan de contrôle intervenant principalement dans les processus d'invocation et de provisionnement. Le RM, constitué de plusieurs modules articulés autour d'une base de données commune, et il participe aux fonctions SSN, CAC, TERO et MMFM (voir Figure 54).

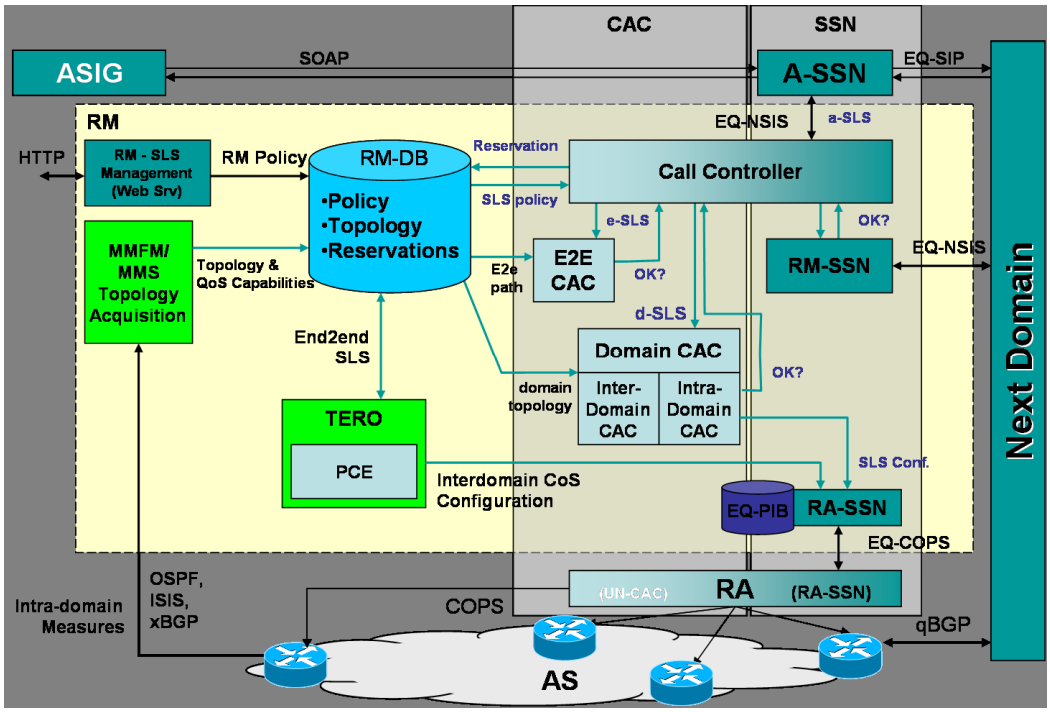


Figure 54 : Architecture du Resource Manager

Les modules composant le RM sont les suivants :

- « CallController » représente la composante centrale du RM. Il prend en charge le processus de réservation/libération des ressources en pilotant les autres modules du RM. Il met en place la signalisation, déclenche les mécanismes de contrôle d'admission et de sauvegarde des informations dans la base de données. Par conséquent, il interagit avec la plupart des modules du RM, et il communique de plus avec les CallController pairs (des RM adjacents).
- « E2ECAC » permet de vérifier l'existence d'un EQ-Path entre les domaines source et destination compatible avec les paramètres de QoS requis.
- « DomainCAC » applique des algorithmes de contrôle d'admission et met en place des politiques opérateurs à l'intérieur du domaine et sur les liens inter-domaines.
- « MMFM » gère les mécanismes de surveillance, mesures et détection des défaillances.
- « TERO » prend en charge les procédures d'ingénierie de trafic et d'optimisation de route. Le client PCC (Path Computation Client) est une partie de TERO et il communique avec PCE pour le provisionnement de type « hard model ».
- La base de données (« RMDB ») sauvegarde toutes les informations nécessaires au fonctionnement des modules : topologie du réseau, utilisation des ressources, accords entre les AS, historique des réservations ou défaillances. Bien qu'elle soit représentée comme un dépôt central, cette base de données peut être distribuée sur plusieurs serveurs afin d'éviter des multiples connexions à un même serveur.

Le RM communique avec les modules suivants :

- AQ-SSN et terminaux de confiance, par le protocole EQ-NSIS ;
- RM pairs, par le protocole EQ-NSIS ;
- MMS, par des sockets TCP ;
- PCE, par le protocole PCEP ;
- RA, par le protocole EQ-COPS.

Le RM, cœur du système EuQoS, remplit des fonctionnalités similaires au RACF (Resource and Admission Control Functions) en NGNs. Une comparaison détaillée entre l'architecture et les fonctions NGN se trouve dans [D112].

3.3.2. CallController

Le CallController est le composant fondamental du RM intervenant dans le processus d'invocation, le CAC et la signalisation inter-domaine. Il est présenté en détail maintenant car nous avons eu la responsabilité de sa conception, spécification et implémentation. Le positionnement du CallController vis-à-vis des fonctions de CAC et de signalisation en EuQoS est illustré dans la Figure 55 pour ses trois fonctions essentielles :

- gestion des requêtes de QoS ;
- contrôle des modules de CAC ;
- mise en place de la signalisation inter-domaine.

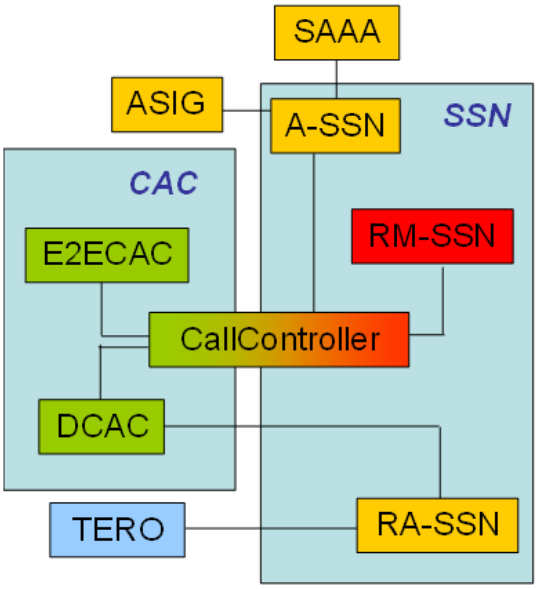


Figure 55 : Positionnement du CallController

La Figure 56 illustre l'architecture du CallController, qui peut être invoqué de plusieurs manières via EQ-NSIS : (1) par un message du module AQ-SSN, (2) par un CallControler d'un domaine adjacent (adjacent ou bien liés par un EQ-Path si un provisionnement « hard model » est mis en place) et (3) par des entités de confiance.

Le fonctionnement du CallController repose sur la coopération entre plusieurs sous-modules principaux : les Session Manager, SLS Splitting, Signaling Manager et CAC Manager.

Le Session Manager est responsable de la gestion des requêtes qui arrivent sur le RM, en vérifiant la conformité des messages avec le modèle de QoS implémenté (présence des paramètres nécessaires, intégrité des informations, identification des routeurs de bordure, du chemin inter-domaine de la communication).

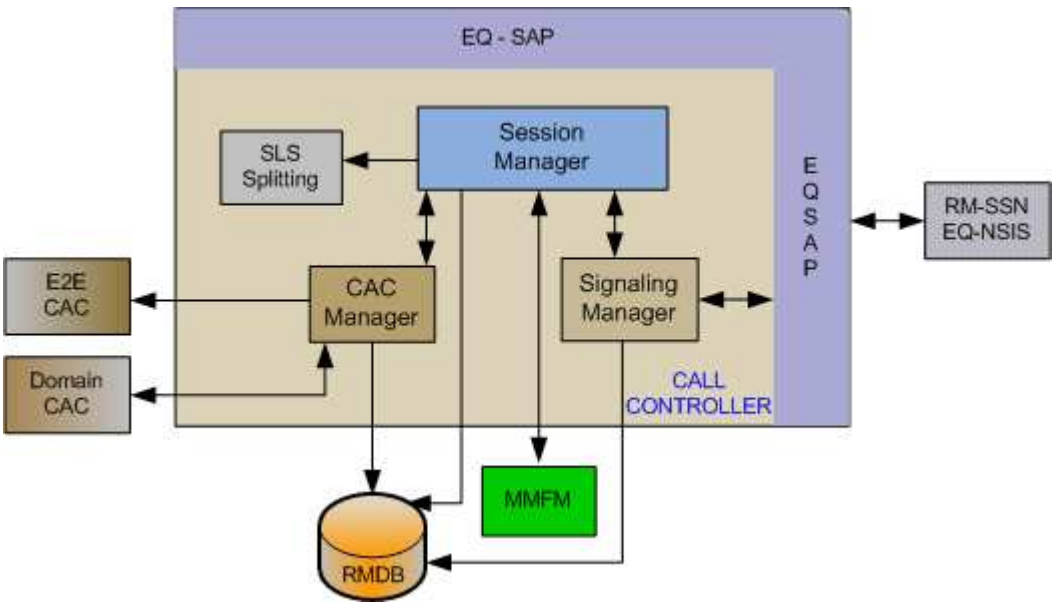


Figure 56 : Structure interne du CallController

En particulier, le CallController reçoit deux types de paramètres : (1) les paramètres de QoS spécifiés par un SLS (bande passante, délai, taux de pertes, gigue) et (2) les paramètres

relatifs à l'identification des flux : adresse IP, numéros de port, protocoles de transport, identifiants de sessions.

Le rôle du module « SLS splitting » est de séparer ou composer les différents types de SLS[9], présentés en section 3.1.4. Sur réception d'un *a-SLS* dans le premier RM, le CallController analyse le message et extrait les informations pour invoquer l'E2ECAC (*e-SLS*) et le DCAC (*d-SLS*). Par la suite il est amené à construire le *r-SLS*, envoyé au prochain RM, en utilisant la formule :

$$r\text{-}SLS(i+1) = r\text{-}SLS(i) - i\text{-}SLS(i)$$

avec $r\text{-}SLS(1) = a\text{-}SLS$ et *i représente le* i^{em} RM

Le CAC Manager assure la synchronisation des modules de contrôle d'admission. Il interagit avec les modules E2ECAC (de manière synchrone) et DCAC (de manière asynchrone) pour activer le contrôle d'admission.

Le Signaling Manager gère la signalisation inter-domaine par l'intermédiaire du protocole EQ-NSIS. En particulier, il déclenche les réservations initiées par le récepteur et bidirectionnelles (voir Section 1.7). Notons que le CallController prend en charge également la libération et la modification de ressources (cette fonctionnalité n'a pas été implémentée dans la version finale du prototype EuQoS pour des raisons techniques, certains algorithmes de CAC dépendant de certaines technologies ne mettant pas en œuvre ce mécanisme).

Enfin, le CallController interagit avec l'E2ECAC, le DCAC et le MMFM en utilisant les interfaces présentées dans la Figure 57.

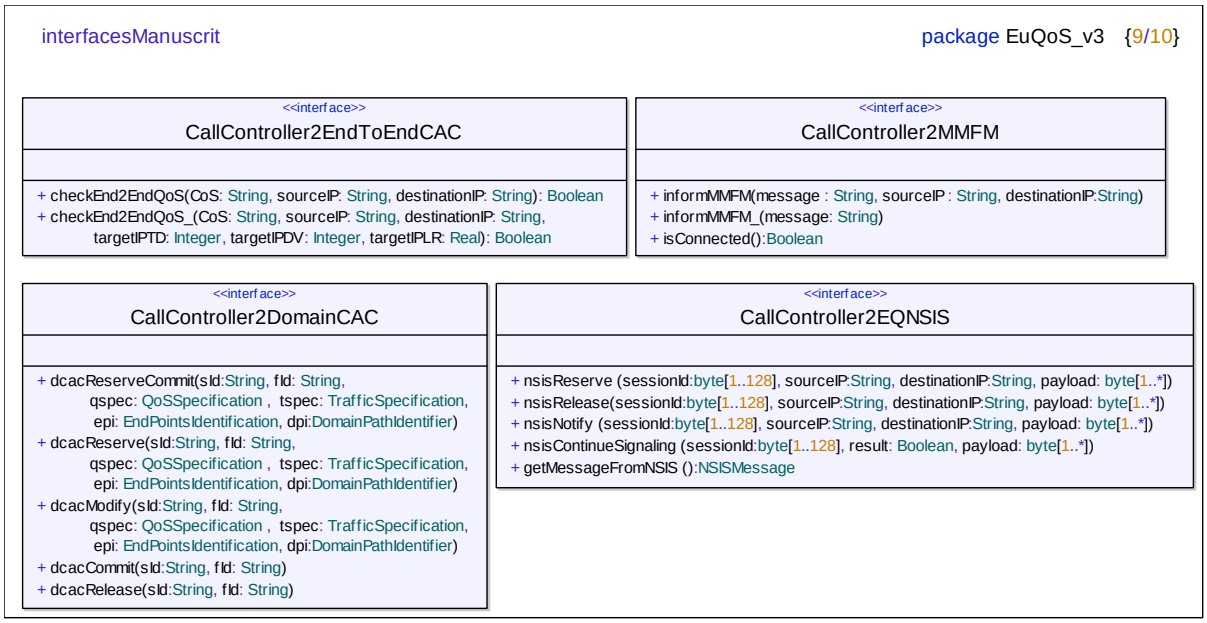


Figure 57 : Interface entre CallController et les modules adjacents

Rappelons que le CallController utilise la base de données du RM (RMDB) pour sauvegarder ou retrouver ses informations et que, pour des raisons de mise à l'échelle, il ne garde des états relatifs à la communication que pendant le processus de réservation (par la suite il utilise la RMDB ou EQ-NSIS).

[9] Rapellons que le SLS représente la partie du contrat SLA qui défini les paramètres technique.

3.3.3. Spécification de la signalisation

Le consortium EuQoS ayant décidé de modéliser dans une première phase le système en UML, nous avons modélisé la signalisation et eu la responsabilité de l'intégration des modèles UML des principales composantes du système. Néanmoins, à la vue de la complexité de l'architecture EuQoS, nous ne détaillons dans ce mémoire que les mécanismes de signalisation, centre de nos travaux. Pour plus d'informations, le lecteur pourra se référer à [D112] et [D121].

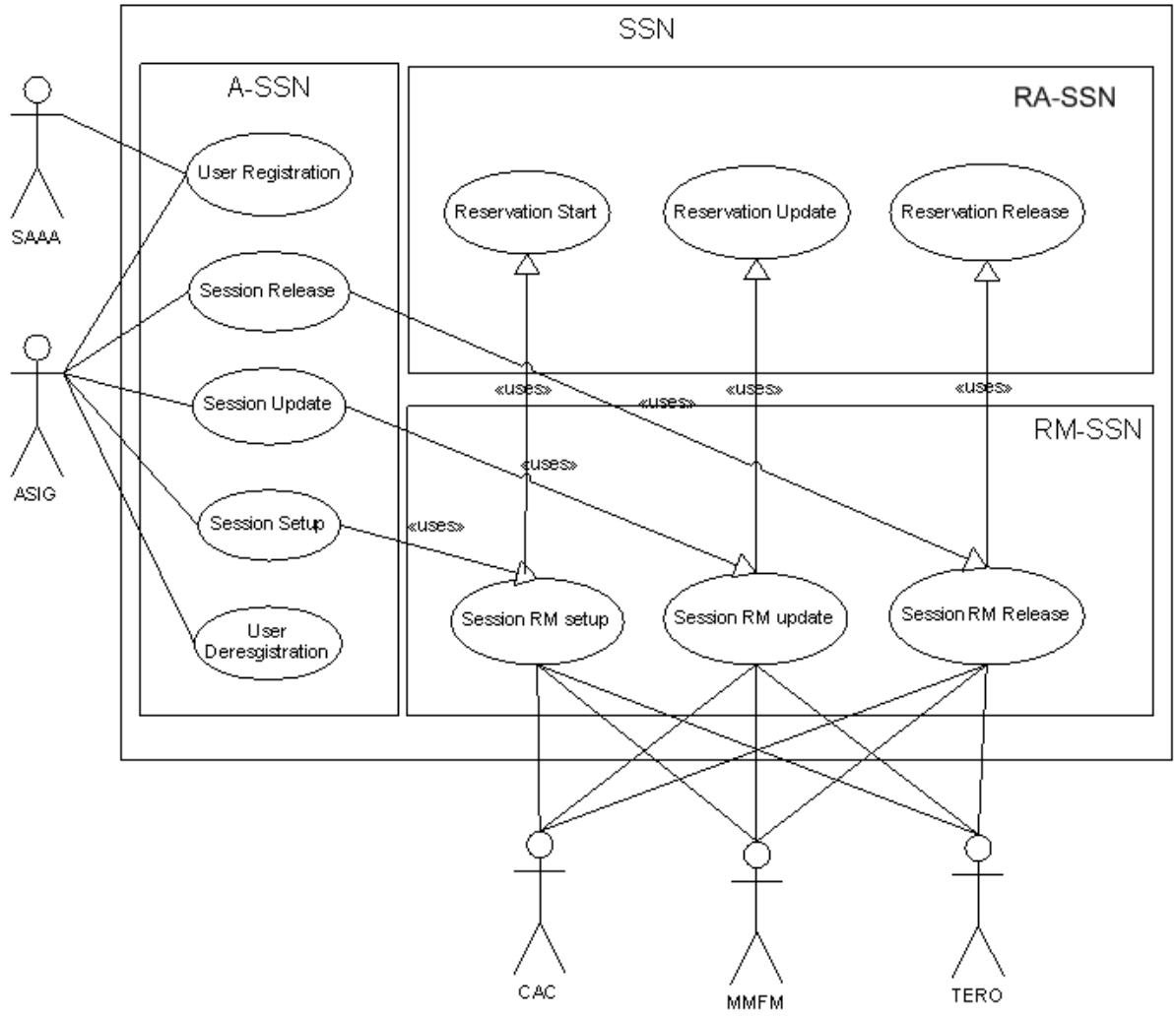


Figure 58 : Diagramme Use Case

Le diagramme de cas d'utilisation de la Figure 58 reprend les informations de la section 3.1.5 et décrit les actions possibles entre les fonctions SSN. Il illustre les différentes interactions entre les modules de l'architecture et la fonction de signalisation. Par exemple, une première étape consiste à s'enregistrer dans le système, « UserRegistration ». Ensuite, la demande de réservation est reçue au niveau A-SSN qui lance la réservation RM-SSN, « SessionRM setup ». Enfin, la fonction RA-SSN est invoquée pour réserver les ressources au niveau dépendant de la technologie par « ReservationStart ».

Pour des raisons de compréhension et clarté, nous séparons par la suite, dans les diagrammes présentés, la signalisation applicative de celle du RM et du RA. L'enchaînement des

messages au niveau applicatif (fonction A-SSN) est illustré dans le diagramme de séquence de la Figure 59. Les paramètres utilisés sont détaillés dans le document [Track 2-06].

Suite à la réception d'une requête de réservation, le module AQ-SSN interagit avec le SAAA pour authentifier le profil utilisateur. Ensuite, un filtrage est mis en place par le module Q-SSN. Une fois la confirmation du RM arrivée, le SAAA est informé de la mise en place des ressources (qui propage au module de CHAR ces informations) et la réponse est envoyée à l'entité initiatrice.

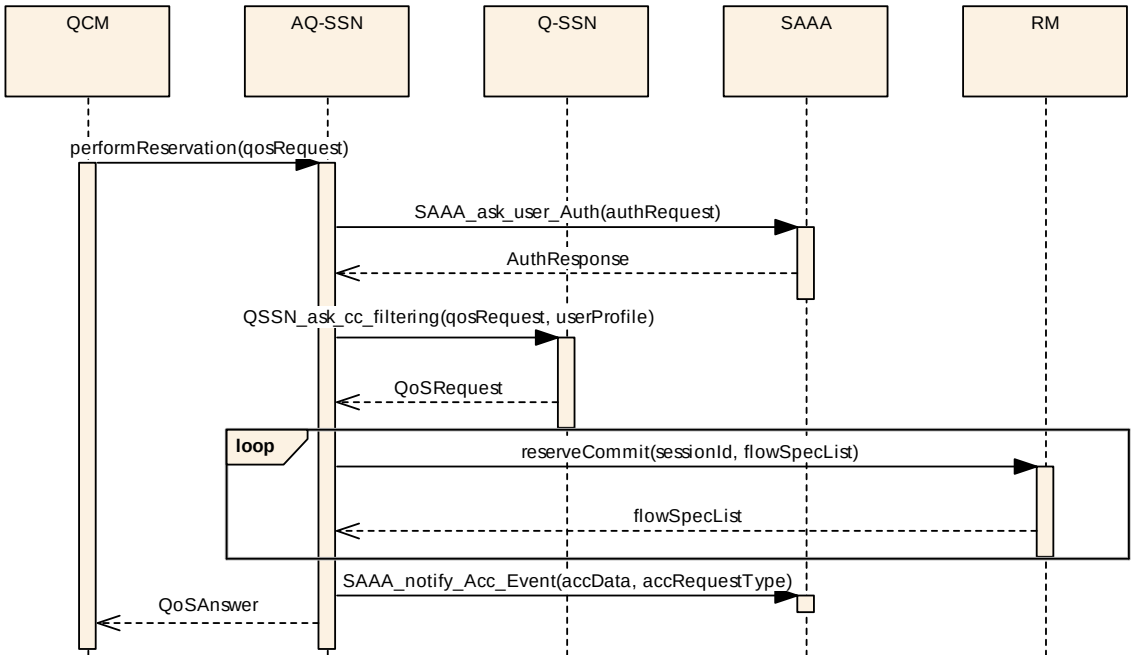


Figure 59 : Diagramme de séquence-réservation niveau A-SSN

Le diagramme de séquence de la Figure 60 présente le mécanisme de libération des ressources, au niveau applicatif. Les mêmes modules sont impliqués, et l'enchaînement similaire. Notons qu'AQ-SSN ne garde pas des états sur les réservations en cours (le module est « stateless »). [Track 2-06] contient également un diagramme de séquence complet (que nous ne reprenons pas pour des raisons d'espace) qui permet de visualiser tous les échanges applicatifs pour l'initialisation d'une session EuQoS entre les modules sur les sites source et destination.

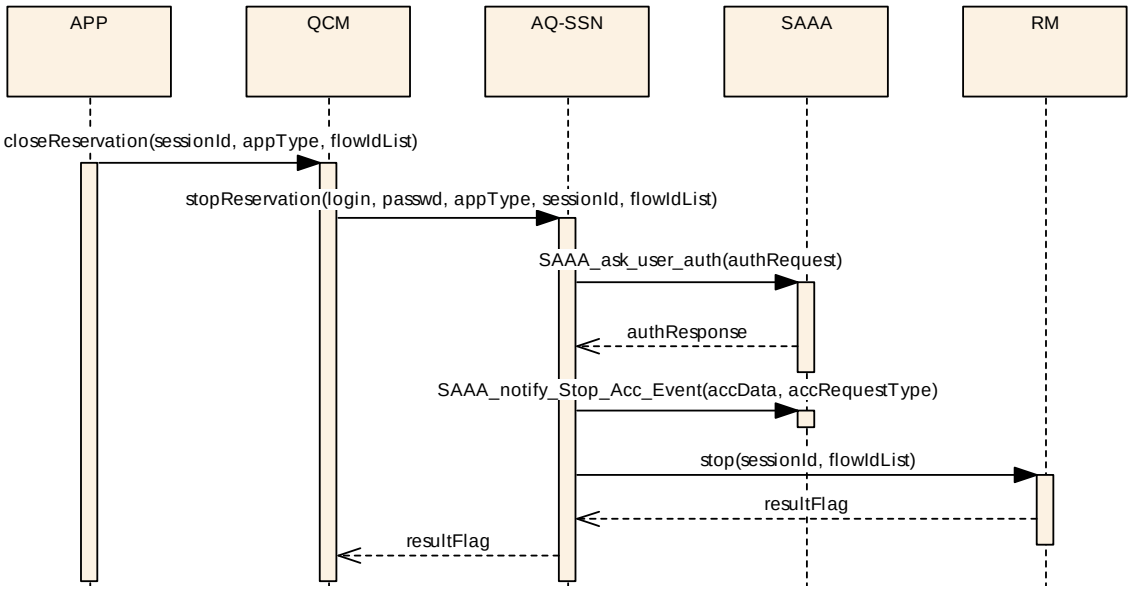


Figure 60 : Diagramme de séquence-libération au niveau A-SSN

Le diagramme de séquence de la Figure 61 illustre le déroulement du processus de signalisation au sein d'un domaine. Suite à la réception d'une requête de demande de service, le CallController dans le RM démarre le processus de réservation.

Dans un premier temps, il interroge le module E2ECAC sur l'existence d'un EQ-Path vers la destination. Ensuite, il retrouve (sur la base des informations de la base de données et les paramètres d'identification de flux) les points d'entrée et de sortie dans le domaine. Même si un EQ-Path existe entre les domaines source et destination, il est possible que les ressources ne soient pas disponibles au long de ce chemin pour satisfaire les besoins du flux concerné ; par conséquent, il effectue un contrôle d'admission intra-domaine et met en place une signalisation inter-domaine pour vérifier les ressources et la concordance des exigences en QoS auprès des RM de tous les domaines : le CallController active le module DCAC qui à son tour lance les modules dépendants de la technologie (RA) via COPS pour effectuer le CAC spécifique à chaque type de réseau ; notons que le contrôle d'admission sur le lien inter-domaine avec le domaine adjacent est effectué également pendant cette phase.

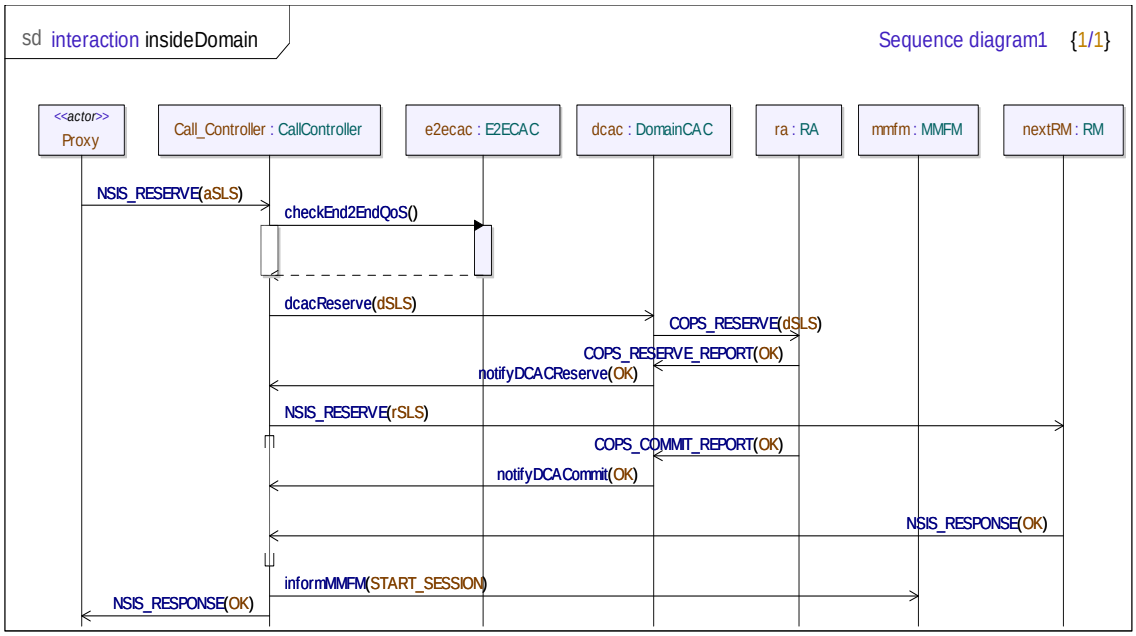


Figure 61 : Signalisation intra-domaine dans EuQoS

Remarquons que la succession des messages se déroule de manière asynchrone : le CallController fait une requête de réservation de ressources et la réponse du RA arrive en deux étapes : la première, un CAC basé sur les informations de la base de données est retourné et par la suite, après la configuration des équipements (réservation entérinée) une confirmation finale est renvoyée et propagée jusqu'au CallController.

Le premier message permet au CallController de continuer la signalisation inter-domaine, et, ainsi la configuration physique des équipements peut s'effectuer en parallèle dans tous les domaines. Ce mécanisme rejoint la proposition faite au chapitre 2, section 2.3, et a été implémentée et validée dans le prototype EuQoS.

Le digramme de séquence illustré dans la Figure 62 présente l'enchainement des messages pour mettre en place la signalisation inter-domaine dans EuQoS.

Au niveau inter-domaine, la communication entre les RM est basée sur le protocole EQ-NSIS. Les messages échangés entre les CallControllers (RESERVE, RESPONSE, RELEASE, NOTIFY) sont transportés par cette signalisation complètement découplée du chemin de données, entre les RM de chaque domaine. Il s'agit de la version HyPath, présentée dans Chapitre 2. Notons que pour des raisons techniques (utilisation des équipements commerciaux), le mécanisme d'interception de paquets n'a pas été totalement intégré dans l'implémentation finale du système EuQoS.

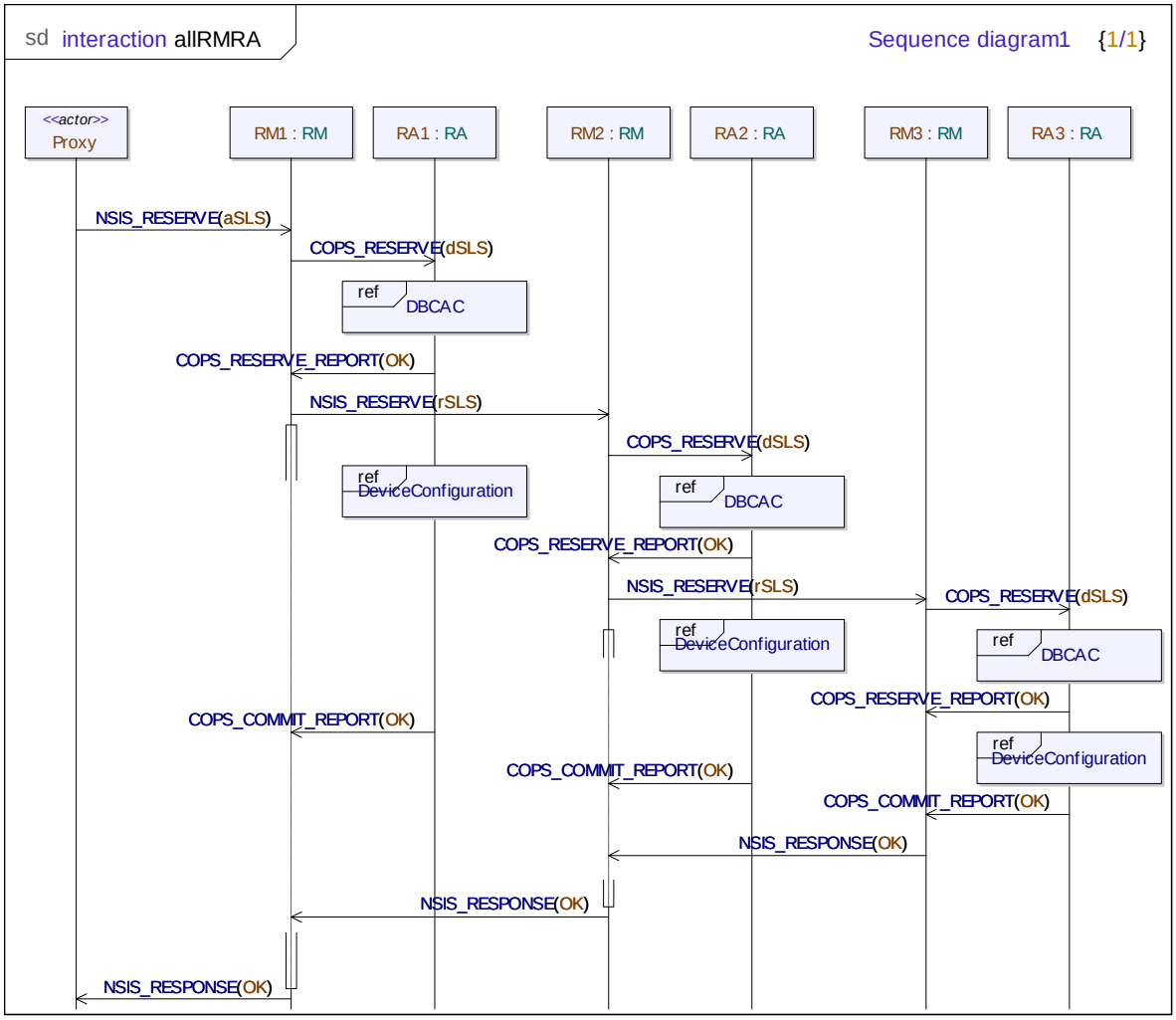


Figure 62 : Signalisation inter-domaine dans EuQoS

De façon identique, dans le cas d'une réservation initiée par le récepteur (vidéo à la demande), ou pour des communications bidirectionnelles, la procédure de réservation est illustrée dans la Figure 63.

Le CallController qui reçoit la requête de réservation se trouve dans le domaine de destination et le chemin de données peut ne pas être symétrique ; de plus il n'a pas la connaissance de ce chemin. Il est donc nécessaire qu'il informe le CallController du domaine source pour commencer la procédure de réservation, en utilisant un message NOTIFY, propagé par les entités EQ-NSIS de chaque RM, sans le remonter au CallControllers des domaines intermédiaires.

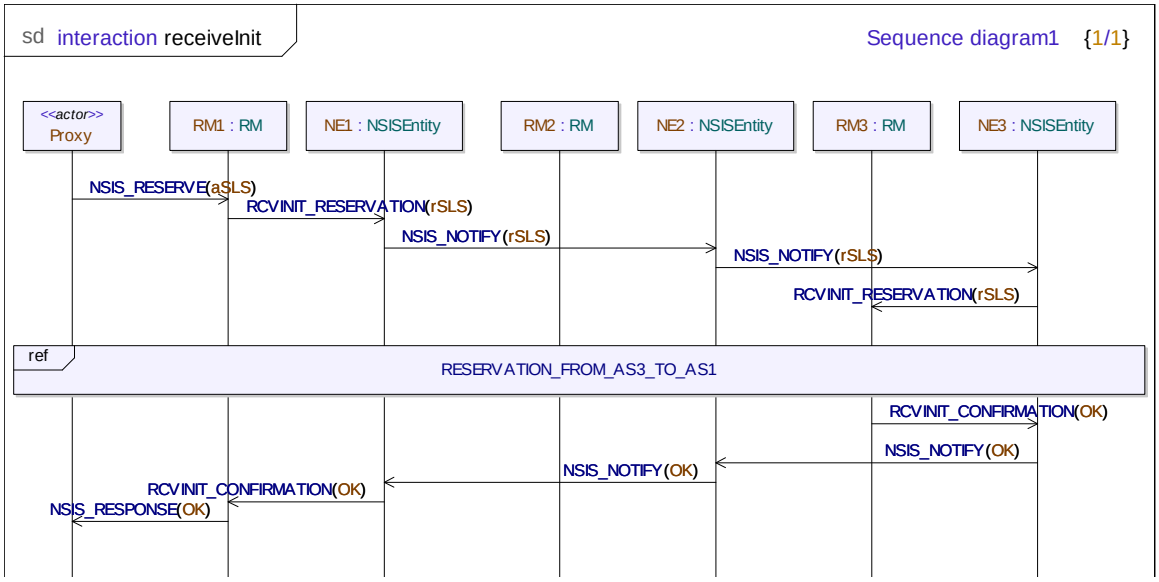


Figure 63 : Réservation initiée par le récepteur

3.4. Conclusions

Ce chapitre a tout d'abord décrit le projet européen IST EuQoS auquel nous avons participé. Dans la première section nous avons présenté l'architecture de QoS proposée dans le cadre de projet. Par la suite nous avons illustré les solutions apportées par EuQoS pour répondre aux besoins que nous avions dégagés dans l'état de l'art : provisionnement, contrôle d'admission et signalisation. Nous avons présenté par la suite les interfaces et les services offerts par les composantes principales du système EuQoS.

Nous avons insisté sur le mécanisme de signalisation dont nos travaux représentent une contribution majeure. La section 3.3 a illustré les composantes impliquées ainsi que l'enchaînement des messages et des opérations dans le processus de signalisation. Le CallController, module central du Resource Manager, met en place et gère cette signalisation ainsi que le contrôle d'admission.

Le système EuQoS proposant une approche innovante, sa réalisation est complexe en termes de conception et déploiement. Notre participation dans le cadre du projet a porté dans un premier temps sur la conception. Par la suite, nous nous sommes investis autant dans son implémentation, son déploiement et son test.

Le chapitre suivant détaille donc les simulations, l'implémentation et les tests ayant permis de valider l'implémentation que nous avons menée.

4. Simulations, déploiement et expérimentations

Ce chapitre présente les travaux de simulation, de déploiement et d'évaluation, liés à nos contributions à la signalisation dans le cadre du projet EuQoS. Ces travaux portent sur :

- la validation en simulation (outil TauG2 de la société Telelogic) du modèle UML des modules et des protocoles spécifiés ;
- l'implémentation des modules, des interfaces et des PDU échangés, ainsi que l'intégration et le déploiement de la signalisation dans l'architecture EuQoS ;
- les expérimentations réalisées sur une plate-forme locale au LAAS-CNRS puis sur une plate-forme européenne réalisée dans le cadre du projet EuQoS.

Ce chapitre est structuré comme suit :

- la section 4.1 décrit les travaux de simulation réalisés à l'aide de l'outil TauG2. Nous présentons dans un premier temps les diagrammes utilisés pour générer les traces de simulations; nous exposons et nous analysons ensuite les résultats fournis par le logiciel ;
- dans la section 4.2, nous détaillons nos travaux d'implémentation dans le projet EuQoS. Nous présentons en particulier le module CallController ainsi que le format de messages échangés dans le processus de signalisation ;
- la section 4.3 décrit les expérimentations réalisées autour du CallController et de la signalisation inter-domaine. Nous présentons d'abord les plates-formes sur lesquelles nos prototypes ont été déployés. Nous détaillons ensuite les spécifications et les résultats des tests de performance et de QoS effectués sur ces prototypes.

4.1. Simulations

4.1.1. Le logiciel Tau

Cette section présente les simulations réalisées à l'aide de l'outil TauG2 (www.telelogic.com/products/tau). TauG2 est une suite intégrée de logiciels qui permet de modéliser des systèmes complexes en utilisant UML2.0, de simuler les modèles et de générer du code C ou Java. Plus précisément, TauG2 offre des capacités de modélisation graphique qui permettent de :

- spécifier tous les aspects de la conception d'un système ;
- simuler et de vérifier le comportement du système modélisé ;
- définir, générer et exécuter des tests sur ces modèles ;
- générer du code (C, Java) à partir d'un modèle ;
- automatiser la gestion de la documentation.

TauG2 supporte les standards de l'industrie en matière de modélisation graphique (UML, SysML et SDL), de conformité, d'intégration et de tests (TTCN-2, TTCN-3). Basé sur UML 2.1, TauG2 permet de concevoir des systèmes et de valider leur spécification par le biais d'une simulation dynamique, paramétrable et maîtrisable du modèle. Le comportement du système est ainsi étudié en amont, les éventuelles erreurs de conception étant corrigées avant la phase d'implémentation. Notons que TauG2 ne permet pas de faire une vérification formelle du modèle, mais il fournit la possibilité de créer et de jouer des scenarios évolués,

de surveiller des paramètres, et de réaliser des traces d'exécutions. La simulation utilise le modèle UML (les diagrammes) afin de compiler et d'exécuter le système. Ces traces prennent la forme des diagrammes de séquence ou diagrammes d'état.

4.1.2. Spécification

Dans le chapitre 2, nous avons présenté des diagrammes UML (diagramme de séquence, d'état) associés à la spécification de nos propositions de protocoles de signalisation. Nous détaillons dans cette section les diagrammes utilisés par TauG2 pour la vérification du modèle, en particulier les diagrammes de structure composite, introduits à partir de la version UML 2.0. Sur la base des diagrammes de structure composite[10]et des diagrammes d'état, TauG2 permet de réaliser des simulations pour vérifier fonctionnellement le modèle UML.

Pour nos simulations, nous utilisons un modèle d'Internet multi-domaine (les types de domaines considérés dans EuQoS sont illustrés dans la Figure 64) similaire à celui présenté dans le chapitre 2. Nous considérons en exemple de trois domaines qui implantent le système EuQoS pour la mise en place de garanties de QoS. Les domaines se déclinent en deux domaines d'accès et un domaine de cœur : nous considérons un premier domaine d'accès Wi-Fi, un domaine de cœur et un deuxième domaine d'accès xDSL.

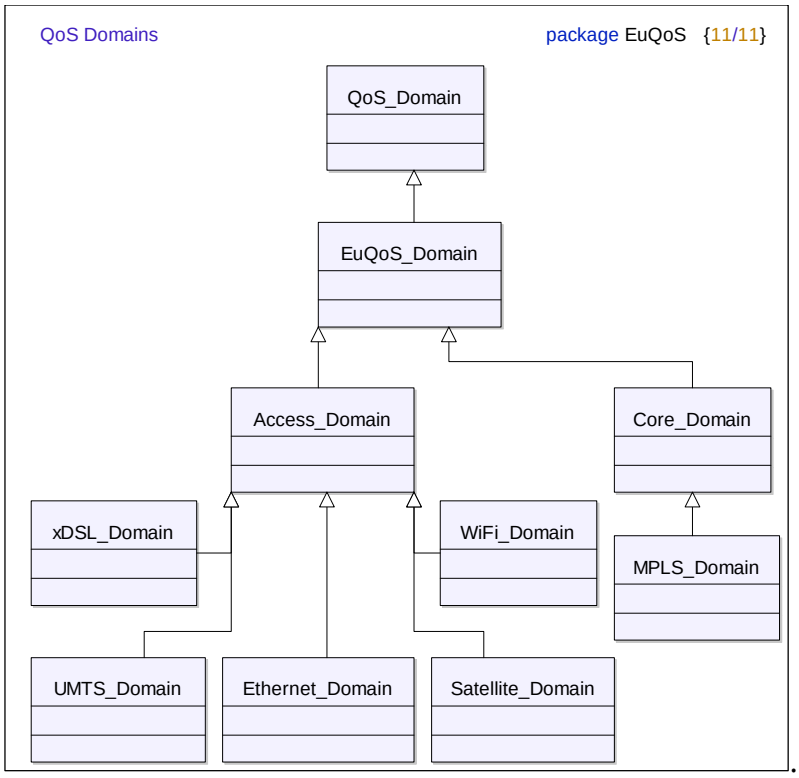


Figure 64 : Diagramme de classe domaine QoS

La Figure 65 donne le diagramme de structure composite pour un domaine EuQoS : RM, RA et réseau sous-jacent (Underlying Network, UN) et leur interconnexion.

[10] Rappelons que ce type de diagramme illustre la structure interne d'une classe et ses interactions avec d'autres composantes du système. Il représente la configuration et les relations entre les classes qui définissent le comportement du système.

Ce diagramme fait apparaître les liaisons avec les autres domaines au niveau RM (via EQNSIS) et avec le réseau sous jacent (UN) via le protocole IP. Il illustre également les interfaces entre les différents modules (EQSAP, RMtoRA, RAtoRM, RAtoUN, DeviceToDevice). Ces interfaces sont implémentées par les ports de communication entre les modules, en entrée ou en sortie.

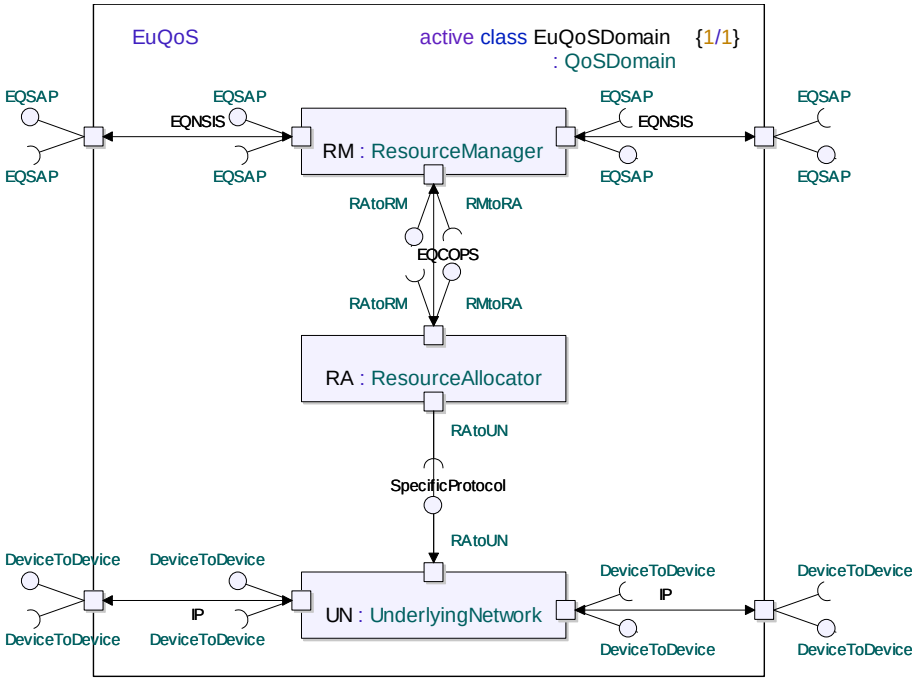


Figure 65 : Diagramme de Structure Composite Domaine EuQoS

Le diagramme de la Figure 66 représente la structure interne du RM.

Nous retrouvons les modules détaillés dans le chapitre 3 : CallController, End2EndCAC, DomainCAC, RMDB. Le diagramme illustre également les connexions entre les différents modules du RM ainsi que les ports de communications avec les modules adjacents.

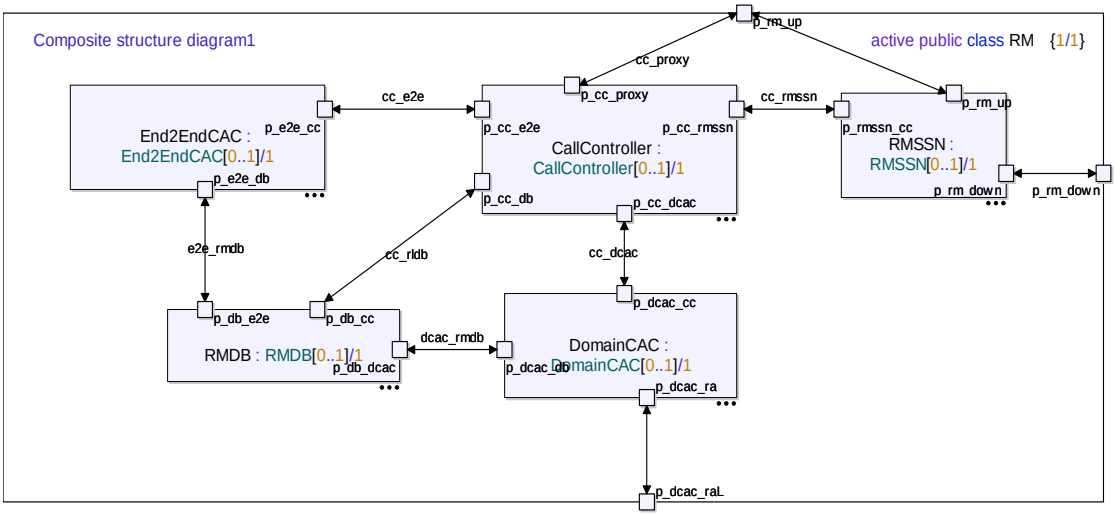


Figure 66 : Diagramme de Structure Composite RM

La Figure 67 illustre le diagramme de structure composite utilisé pour la simulation d'un environnement multi-domaine. Il détaille les interfaces entre les domaines ainsi qu'entre les clients et le système EuQoS.

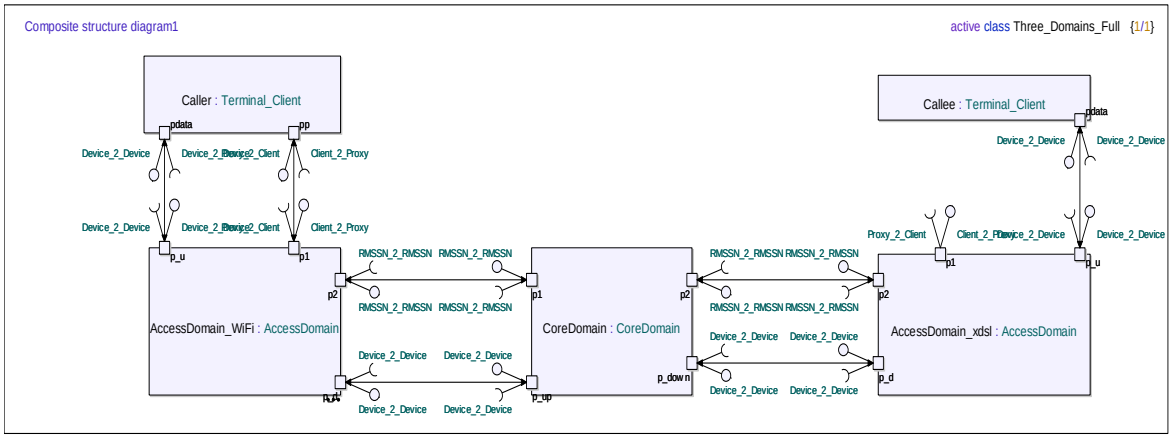


Figure 67 : Diagramme de Structure Composite pour trois domaines

Nous avons défini et effectué différents jeux de tests, qui visaient à simuler la signalisation à plusieurs niveaux : applicatif, intra et inter-domaine. Ces scénarios ont eu pour but de confirmer le comportement dans les cas d'une réservation réussie, réservation échouée, libération des ressources, etc. Les principaux scénarios testés sont résumés dans le Tableau 8.

Scénario	Type de tests	
1	Réservation réussie	Signalisation Applicative
2	Réservation échouée	
3	Expiration des timers	
4	Libération des ressources	
5	Réservation intra-domaine	Signalisation intra-domaine
6	Ressources insuffisantes	
7	Libération des ressources	
8	Problème configuration équipement	
9	Réservation réussie	Signalisation inter-domaine
9	Libération des ressources	
10	RM (CallController) dans le premier domaine	
11	RM (CallController) dans un domaine de cœur	
12	RM (CallController) dans le dernier domaine	

Tableau 8 : Scénarios simulés

4.1.3. Résultats

A partir de ces diagrammes de structure composite et des diagrammes d'états transitions, le logiciel TauG2 permet de simuler le modèle en jouant différents scénarios. Nous avons effectué plusieurs simulations avec un, deux et trois domaines.

A titre illustratif, nous présentons dans cette section le déroulement de la signalisation au sein d'un domaine, ainsi que le scénario nominal qui aboutit à une réservation pour trois domaines.

Notons que TauG2 permet de tester le système de manière incrémentale pour éviter les éventuels risques de blocage ou toute autre erreur de conception. Il est possible également de surveiller l'évolution des paramètres dans le temps ou de suivre la trace état par état Nous

avons ainsi pu suivre l'évolution des différentes variables (bande passante disponible, nombre de connexions), ce qui nous a permis d'analyser la manière dont les ressources sont gérées et mises à jour.

4.1.3.1. Trace intra-domaine

Nous présentons ici la trace obtenue en choisissant une vue à l'intérieur de chaque domaine (Figure 68). Nous y retrouvons les messages échangés entre les composants du RM et du RA ainsi que leurs états.

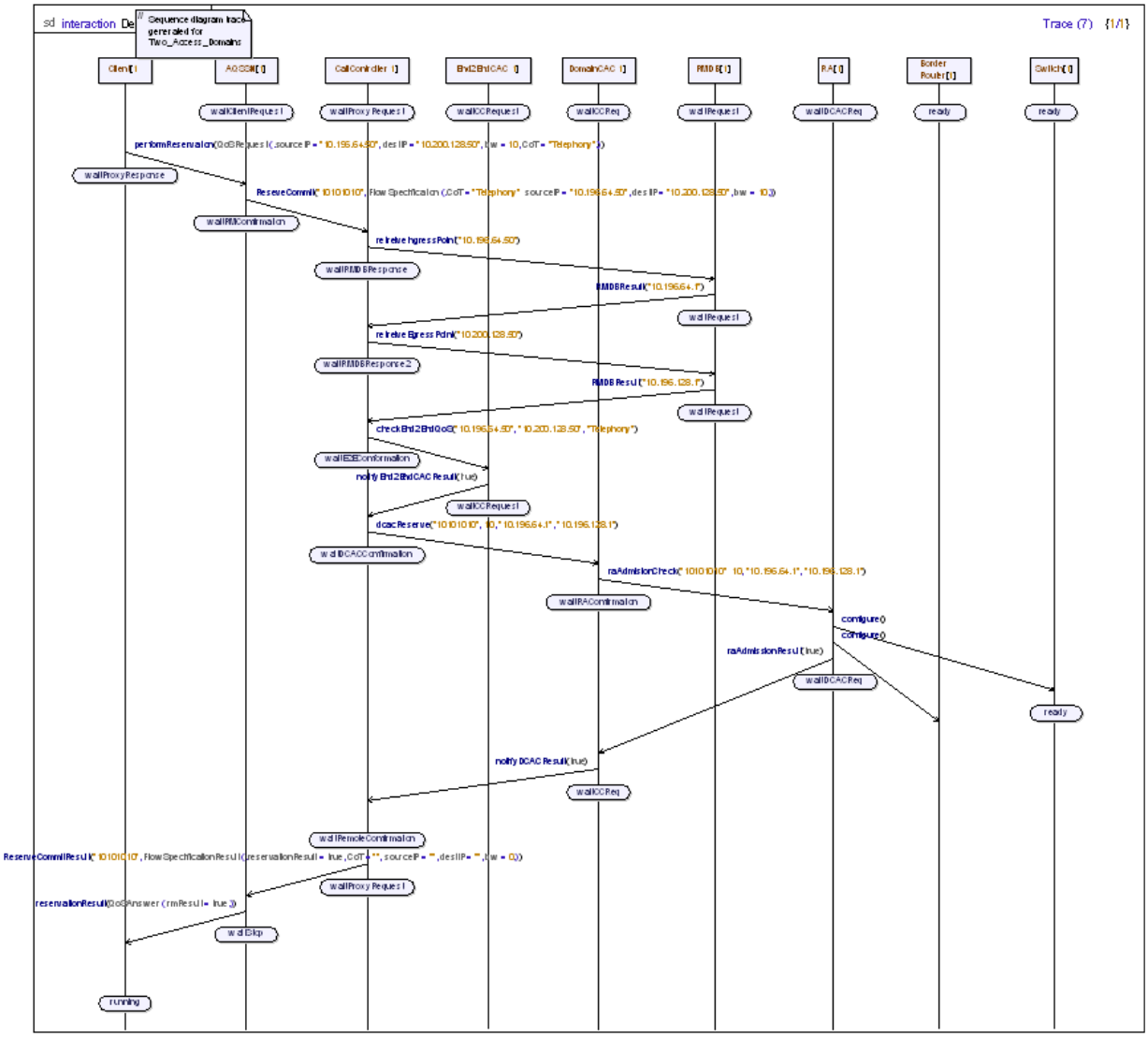


Figure 68 : Trace intra-domaine

4.1.3.2. Trace inter-domaine

Par souci de clarté, nous ne donnons que les messages entre le RM et le RA d'un même domaine et entre les RM des domaines adjacents pour une simulation avec trois domaines (Figure 69). Au sein de chaque domaine, l'enchainement est similaire à celui présenté dans la Figure 68.

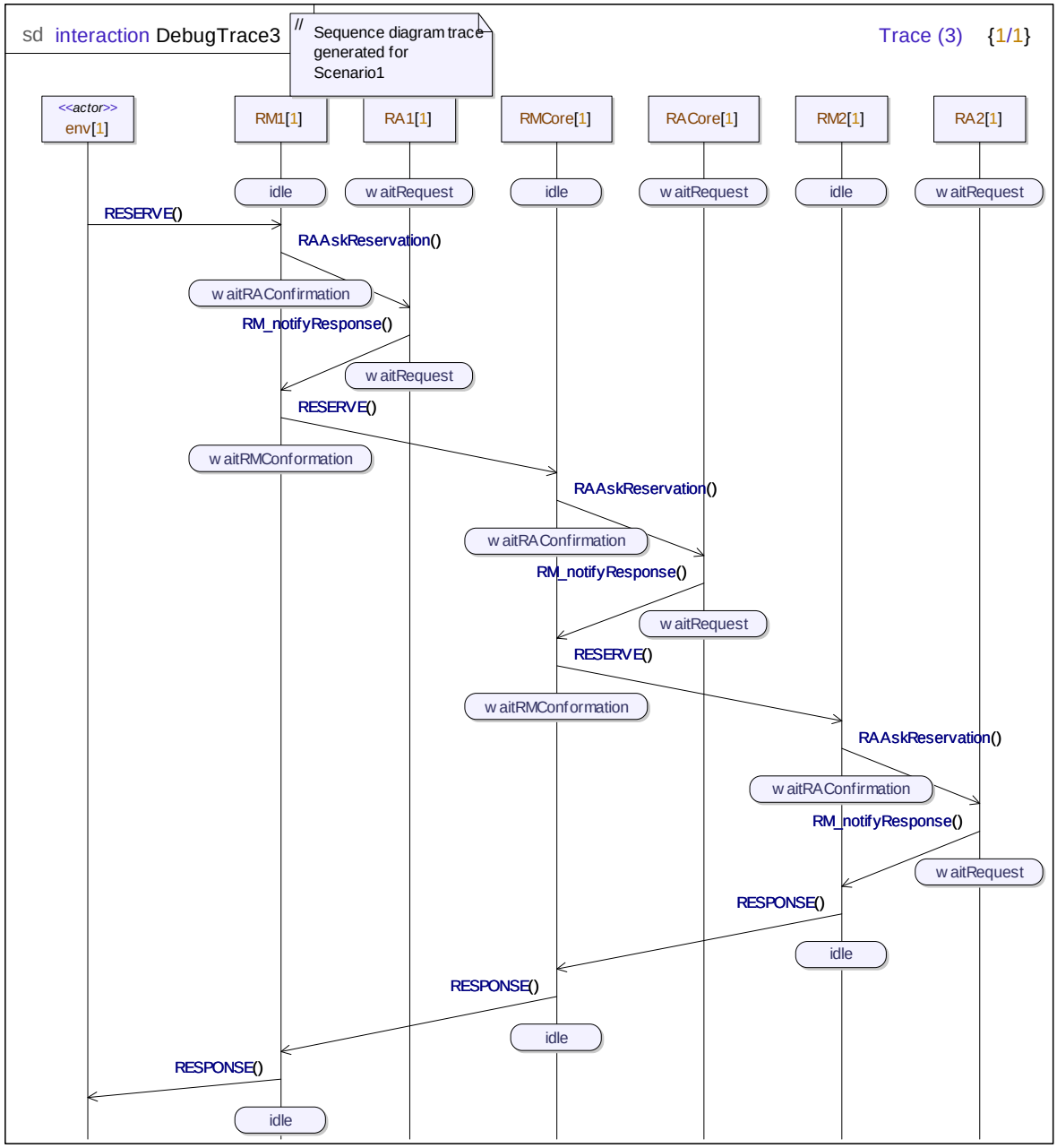


Figure 69 : Trace inter-domaines

4.1.4. Conclusions

Dans cette section nous avons présenté les simulations réalisées avec l'outil TauG2 autour de nos contributions à la signalisation (intra et inter-domaine) dans système EuQoS.

Ces simulations ont permis une validation fonctionnelle de l'architecture proposée. De plus, la possibilité de manipuler plusieurs scénarios (les sauvegarder et les rejouer ultérieurement) et de faire varier les paramètres a permis de mener étude détaillée du comportement du système, en particulier de la signalisation.

Dans la section suivante, nous présentons les détails sur l'implémentation de nos propositions réalisée dans le cadre du projet européen EuQoS. Nous détaillons le module CallController ainsi que le format des messages (PDUs) utilisé par l'interface EQ-SAP.

4.2. Implémentation

4.2.1. Introduction

De Mars 2005 à Décembre 2007, notre effort d'implémentation dans le cadre du projet EuQoS a conduit à la réalisation et au déploiement de cinq prototypes successifs[11]. Ces prototypes ont été tous testés, validés et démontrés lors des quatre revues du projet EuQoS, soit lors des manifestations IST (à Bruxelles 2005 et Helsinki 2006).

De manière quantitative, le nombre de lignes de code que nous avons produit en ne considérant que l'implémentation réalisée pour le dernier prototype EuQoS, s'élève approximativement à 20000. Ce travail inclut le module CallController, le codage des messages de signalisation, l'interface EQ-SAP, auxquels sont à ajouter le développement des outils de tests ou les implémentations intermédiaires des prototypes antérieurs.

Le Tableau 9 résume nos contributions pour chacun des prototypes.

Prototype	Contributions
Prototype #0	• Définition et implémentation minimale des interfaces entre les modules du RM • Protocole de signalisation basé sur socket TCP • Intégration
Prototype #1	• Première version du CallController • Interface locale avec ASSN • Utilisation de NSIS • Démonstration en revue de projet et manifestation IST Bruxelles 2005
Prototype #2	• Utilisation des mécanismes RMI entre AQ-SSN et CallController • Messages au format XML • Version enrichie du CallController • Démonstration en revue de projet Lannion juin 2006
Prototype #3	• Interface socket TCP entre AQSSN et CallController • Nouvelles interface avec DomainCAC • Première implémentation d'EQ-SAP • Version évoluée du CallController • Démonstration IST Helsinki 2006
Prototype #4	• Version complète d'EQ-SAP • Utilisation d'EQ-NSIS pour communiquer entre AQ-SSN et le RM • Nouveaux schéma multi-domaine pour l'invocation et la réservation • Démonstration en revue de projet en octobre 2007 (Bruxelles) et en février 2008 (Varsovie)

Tableau 9 : Contributions sur les prototypes EuQoS

[11] Rappelons que nos contributions principales concernent le module CallController, l'interface EQ-SAP, le codage des messages de signalisation entre les RM et l'interconnexion entre l'AQ-SSN et le RM.

Le premier prototype du protocole de signalisation a été basé sur l'utilisation des sockets TCP, implémentation de la contribution décrite dans la section 2.3. Dans les prototypes suivants, l'échange des messages de signalisation a reposé sur une implémentation du protocole EQ-NSIS, une variante modifiée de la solution NSIS étudiée à l'IETF et développée par l'Université de Coimbra.

4.2.2. CallController

Dans le chapitre 3, nous avons présenté les fonctionnalités et les caractéristiques du module CallController. De plus, nous avons illustré ses interfaces avec les autres modules ainsi que les protocoles utilisés. Cette section a pour objectif de donner plus de détails d'implémentation et de préciser la structure interne du CallController.

La Figure 70 présente le diagramme de paquetage UML (Package Diagram) qui montre la structuration du module en paquetages et leurs dépendances[12].

Nous y retrouvons :

- un paquetage « core » qui contient les classes principales de traitement,
- un paquetage « management » incluant les classes de gestion de session,
- un paquetage « signaling » qui regroupe les classes en charge de la signalisation,
- et un paquetage « mmfm » qui gère la communication avec le module MMFM.

Deux autres paquetages sont représentés :

- « utils » pour toutes les classes additionnelles qui interviennent dans le traitement réalisé par le CallController,
- et « stub » qui permet d'instancier les modules connexes avec des objets « stub » (c'est à dire qui implantent des fonctionnalités limitées) pour tester les actions du CallController.

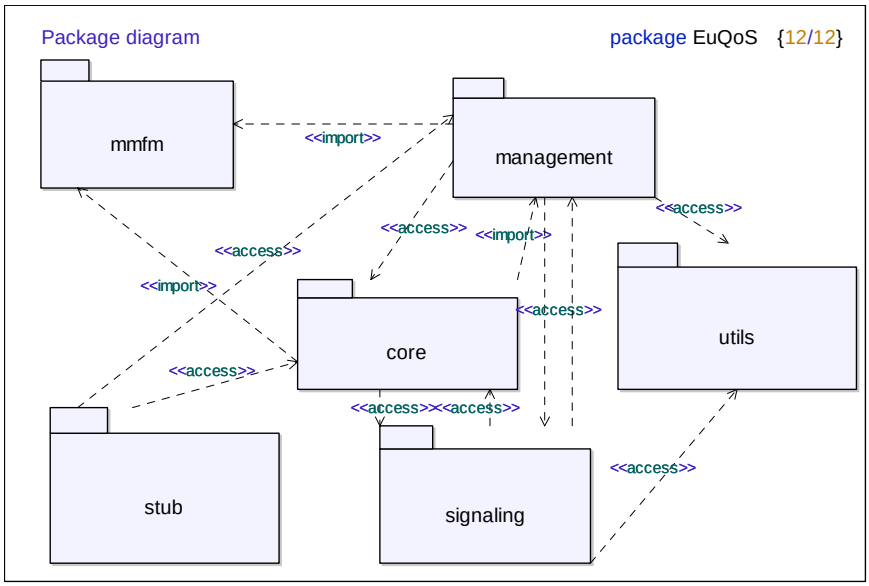


Figure 70 : Diagramme de paquetage CallController

[12] Notons que les dépendances « import » et « access » permettent d'importer les déclarations d'un paquetage pour éviter d'utiliser les noms complets. La différence majeure entre les deux termes est que l'importation est transitive, ce qui rend visible toutes les déclarations des autres paquetages importés.

La Figure 71 illustre les flux de données dans le CallController.

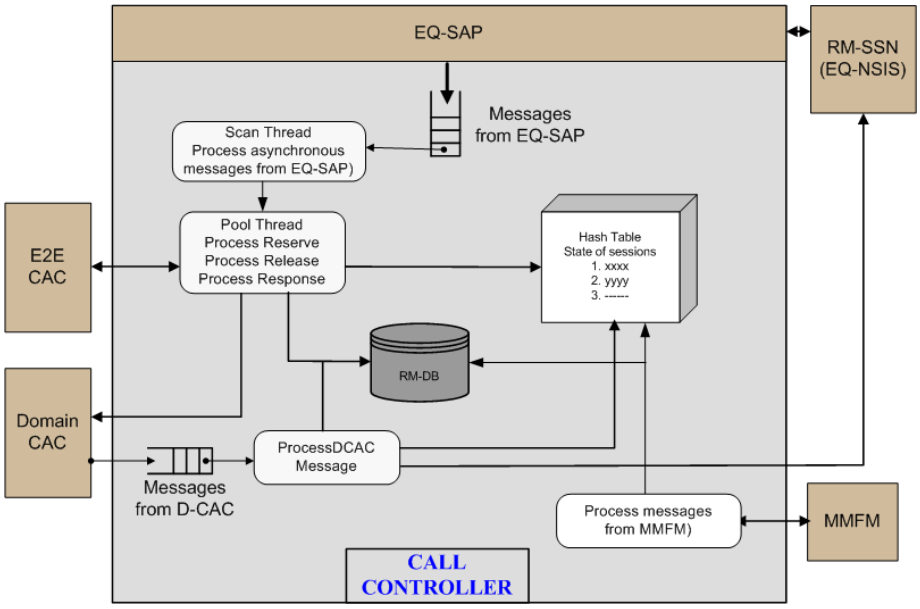


Figure 71 : Les flux de données dans le CallController

Dans le CallController, plusieurs tâches se déroulent en parallèle : le traitement d'une nouvelle requête, la réponse à une requête existante, la réponse du module RA par l'intermédiaire du DomainCAC, la communication avec le module MMFM.

Ces activités sont implantées à l'aide du mécanisme « thread pool » qui permet d'allouer successivement des threads pour exécuter les différentes tâches. La taille (nombre de threads lancés) est paramétrable au lancement du système.

4.2.3. Format des PDUs

Nous présentons dans cette section le format des messages échangés entre le module AQ-SSN et le CallController et ceux échangés entre les RM (en particulier entre les CallControllers) adjacents. Ces messages sont basés sur la définition de l'interface EQ-SAP décrite dans la section 3.2.2.3.

La structure de l'interface EQ-SAP est donnée au moyen du diagramme de classe de la Figure 72, qui reprend les paramètres présentés dans le chapitre 3 en détaillant leur description :

- FlowSpecification (spécification de la QoS d'un flux) ;
- Scope (l'emplacement d'application de la QoS) ;
- TimeSpecification (durée de l'application de la QoS)
- FlowIdentification (identification du flux).

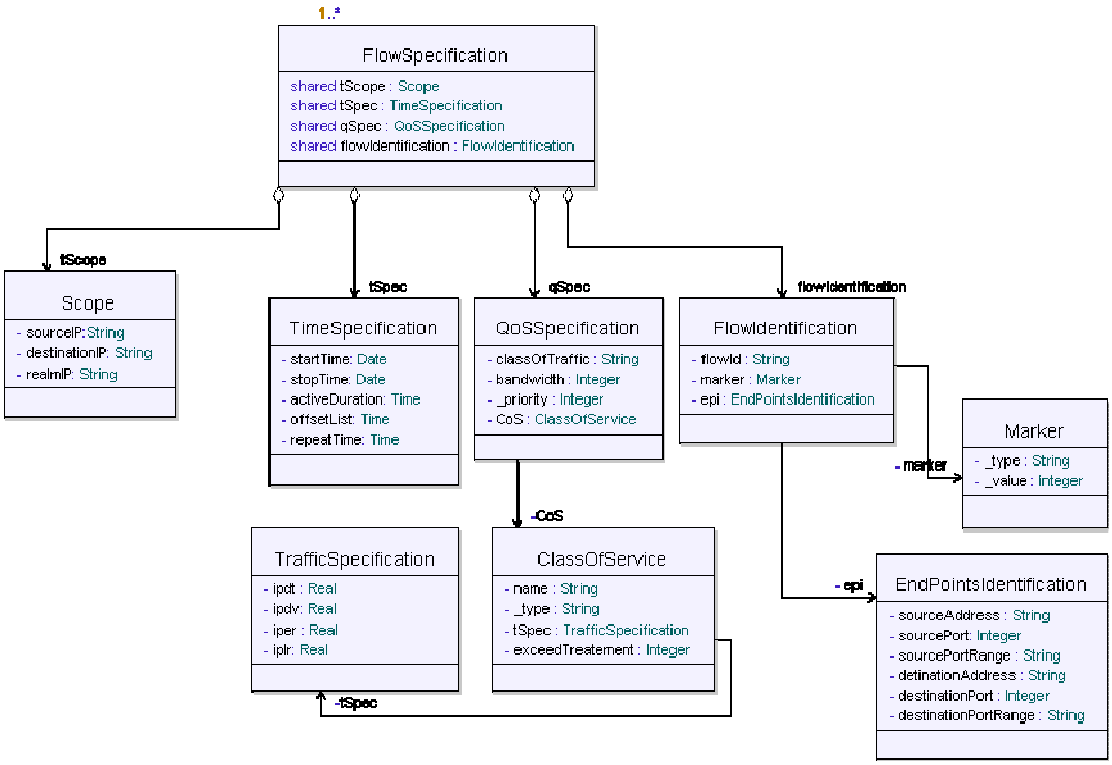


Figure 72 : Diagramme de classe - Structure EQSAP

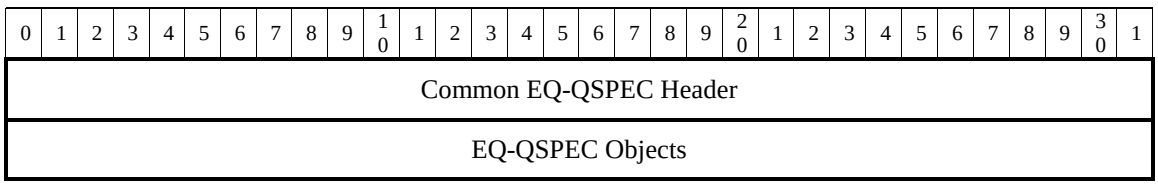
Cette structure décrit les informations nécessaires aux modules du système EuQoS pour la mise en place de la QoS.

Pour les transporter, nous avons analysé les travaux du groupe NSIS [Ash07] qui fournit une proposition d'objet transporté par le NSLP, appelé QSPEC. Sur les bases de ce format, notre solution prend en compte les paramètres EuQoS (qui utilise un modèle de QoS différent de celui de NSIS car le modèle NSIS est on-path). Nous appelons cette proposition une EQ-QSPEC.

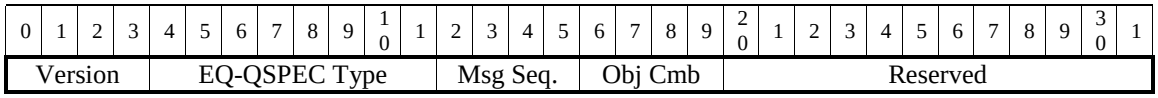
Cette section présente le codage utilisé en insistant sur les modifications introduites par rapport à la définition NSIS.

4.2.3.1. Format général d'un message EQ-QSPEC

Le format général d'un PDU EQ-QSPEC est le suivant :



L'en-tête EQ-QSPEC est de longueur fixe (4 octets), et a la structure suivante :



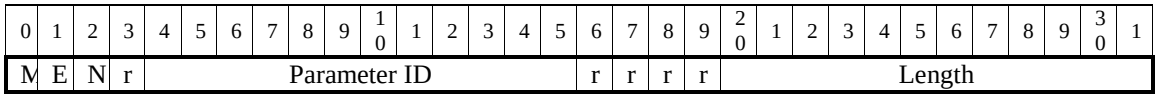
Les champs « Version », « Type », « Message Sequence » et « Object Combination » ont la même sémantique que ceux du draft [Ash07] :

- le champ « Version » identifie le numéro de l'EQ-QSPEC. Dans NSIS, ce numéro est attribué par l'IANA (Internet Assigned Numbers Authority).
- le champ « Type » identifie une EQ-QSPEC particulière.
- le champ « Message Sequence » identifie la séquence des messages et prend les valeurs :
  - « 0 » : réservation initiée par l'émetteur ;
  - « 1 » : réservation initiée par le récepteur ;
  - « 2 » : interrogation sur la disponibilité des ressources (resource query).
- le champ « Object Combination » prend des valeurs de 1 à 3 et indique la combinaison des objets dans les messages échangés (des exemples se trouvent dans [Ash07]).

4.2.3.2. Les paramètres EQ-QPSEC

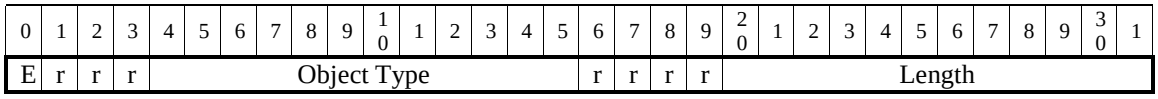
Une EQ-QSPEC est une collection d'objets qui ont le même format et qui contiennent différents paramètres.

Le format de codage adopté pour une EQ-QSPEC est basé sur la description utilisée par NTLP (GIST) de NSIS, nommée Type-Length-Value (TLV Type-Longueur-Valeur). L'en-tête commun pour tous les paramètres est formé de quatre octets (32 bits) :



Les bits M, E et N sont utilisés pour définir le traitement à appliquer au paramètre. Le drapeau M signifie que le paramètre doit être pris en compte, le drapeau E indique une erreur ou une réservation échouée et le drapeau N notifie un objet non supporté. Les bits « r » sont réservés. Plus de détails sur ces drapeaux se trouve dans [Ash07].

Le format d'un objet EQ-QSPEC est le suivant :



Le drapeau "E" indique si une erreur s'est produite au niveau du traitement de l'objet. Le draft NSIS [Ash07] définit quatre types d'objets :

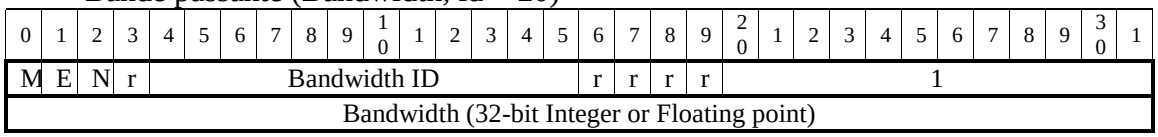
- « 0 » : QoS Désirée (Desired QoS)
- « 1 » : QoS Disponible (Available QoS)
- « 2 » : QoS Réservée (Reserved QoS)
- « 3 » : QoS Minimale acceptable (Minimum QoS)

Notons que suite aux difficultés rencontrées dans la mise en place de certains RA (Resource Allocator), les objets « QoS Disponible » et « QoS Minimale » n'ont pas été implémentés. De plus, nous rajoutons un autre type, identifié par « 4 » qui code l'identification d'un flux. Ceci est nécessaire pour envoyer explicitement dans l'EQ-QSPEC les informations permettant d'identifier le flux : adresses IP, numéros de port, protocole.

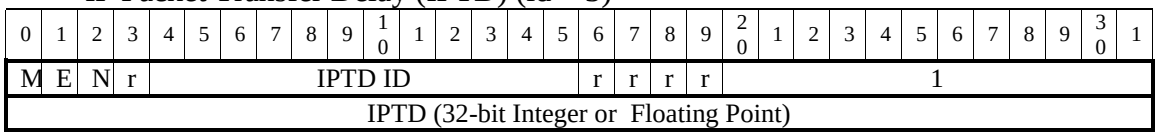
Après avoir présenté la spécification EQ-SAP dans le chapitre 3, nous définissons dans les paragraphes suivants le format de ces paramètres, tels que nous les avons implémentés dans

EuQoS. A tire d'exemple, nous présentons ci-dessous le format des quelques paramètres. L'intégralité de ces définitions est disponible dans [Racaru08] :

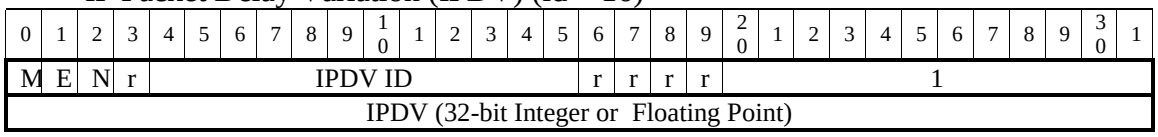
- Bande passante (Bandwidth, id = 20)



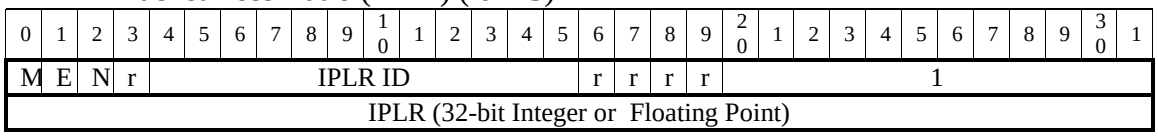
- IP Packet Transfer Delay (IPTD) (id = 3)



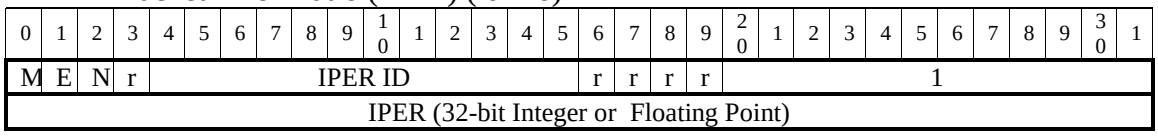
- IP Packet Delay Variation (IPDV) (id = 16)



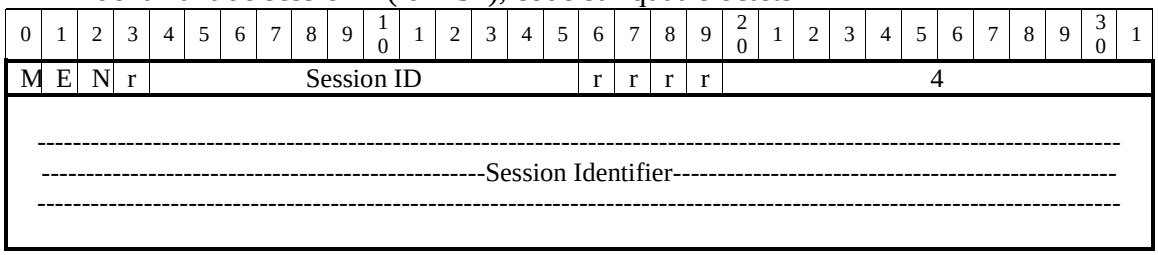
- IP Packet Loss Ratio (IPLR) (id = 5)



- IP Packet Error Ratio (IPER) (id = 6)



- Identifiant de session[13] (id = 31), codé sur quatre octets



Le format des messages échangés entre les CallControllers de chaque RM est le suivant :

- Reserve = (Flow Identifier, Desired QoS, [Available QoS], [Minimum QoS]) :
- Flow Identifier = (SessionId, FlowId, EndPointIdentification | Marker);
- EndPointIdentification = (adresse IP source, numéro port source, adresse IP destination, numéro port destination, numéro de protocole) ;
- Marker non utilisé.
- QoS Désirée = (Classe de Trafic, Classe de Service, Bandwidth, Priorité)
- Classe de Service = (Nom, Type, TrafficSpecification, [Exceed Treatement]).

[13] Remarquons qu'une session peut contenir plusieurs flux.

- TrafficSpecification = (IPDT, IPDV, IPER, IPLR, Average Packet Length).
- Response = (FlowIdentifier, QoS Réservée)
- Release = (FlowIdentifier, QoS Désirée avec une valeur de la bande passante = 0)

Compte tenu de ces valeurs, dans l'implémentation du dernier prototype EuQoS, la taille d'un message (charge utile) de réservation est de 148 octets et la taille d'un message de release (identique à celle de réponse) est de 146 octets. A ces valeurs s'ajoutent les en têtes et les données EQ-NSIS.

4.3. Expérimentations

Après avoir décrit les simulations et les détails de l'implémentation, nous présentons dans les paragraphes suivants les expérimentations menées pour la validation de nos prototypes.

Les objectifs de ces expérimentations sont : la validation fonctionnelle de la signalisation (paragraphe 4.4.3), la validation intégrale du système par le biais d'une application à QoS (paragraphe 4.4.4), la mesure des performances de protocole de signalisation (paragraphes 4.4.5 et 4.4.6) et du module CallController (paragraphe 4.4.7).

4.3.1. Plate-forme LAAS

Une plate-forme d'expérimentation a été conçue et mise en place au LAAS-CNRS. Cette plate-forme, appelée « LAASNEXTEXP », est indépendante du réseau du LAAS et elle est raccordée directement à RENATER[14], et à travers RENATER aux autres réseaux européens de la recherche (voir Section 4.4.2 pour plus de détails). De cette manière, LAASNEXTEXP permet de réaliser des tests dans un environnement réel multi-technologie, multi-domaine ainsi que dans un environnement émulé.

La Figure 73 illustre ce réseau expérimental dans sa globalité.

Notons que LAASNEXTEXP est mutualisée entre plusieurs projets de recherche :

- EuQoS sur lequel nous revenons par la suite ;
- MetroSec (www.laas.fr/METROSEC) pour mener des études sur la détection de problèmes de sécurité à l'aide des outils de la métrologie ;
- SatSix (www.ist-satsix.org) pour l'émulation d'un réseau d'accès satellite ;
- NetQoS (www.netqos.eu) pour l'émulation d'un domaine à QoS géré par des politiques adaptatives.

[14] Réseau National de télécommunications pour la Technologie l'Enseignement et la Recherche

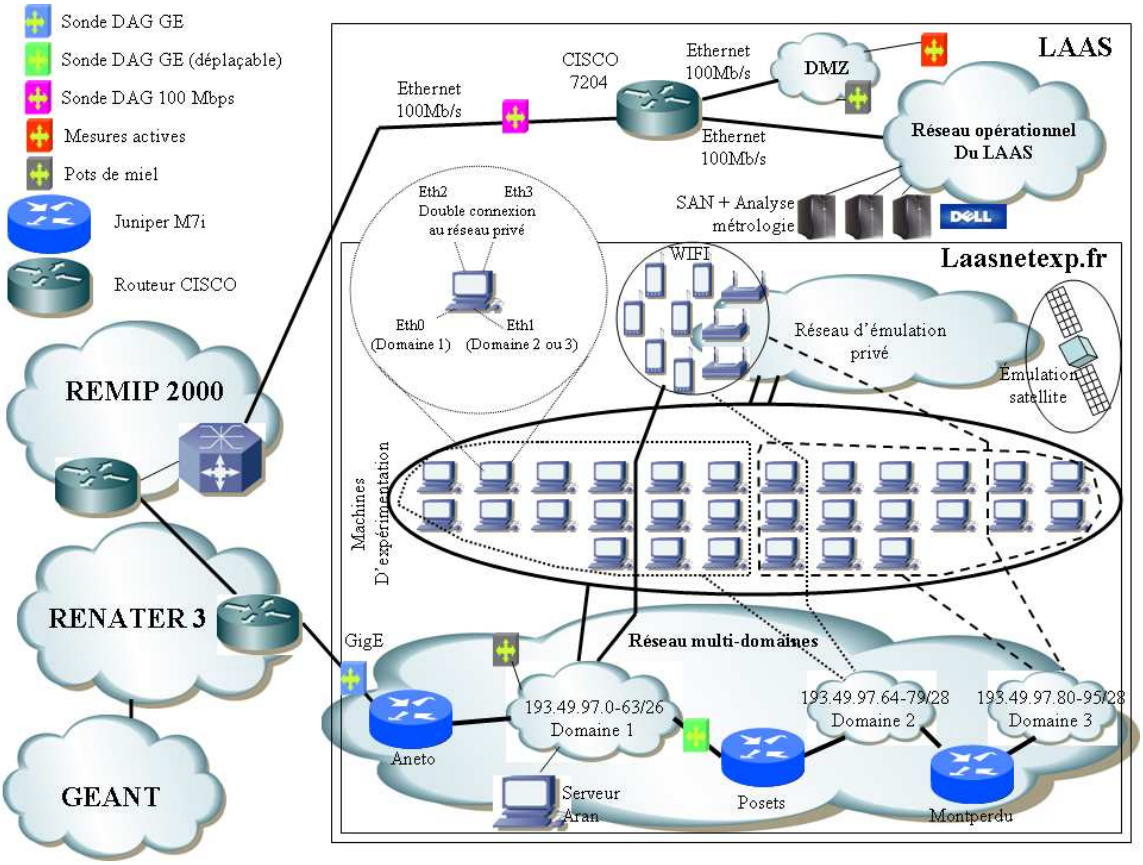


Figure 73 : Plate-forme LAASNEXTEXP

La plate-forme globale est composée de trois domaines avec des adresses publiques qui émulent différentes technologies interconnectées par le biais de plusieurs équipements réseaux : trois routeurs JuniperM7i, six commutateurs (switches) CISCO Catalyst 2960G, 2970 et WS-C6504-E. Elle peut fonctionner en IPv4 ou IPv6 et accéder aux services de multicast. Les machines qui forment la plate-forme sont des DELL PowerEdge 750, 850, 1850, 3850, 6650 et 6850.

La configuration choisie pour tester nos propositions d'architecture est illustrée dans la Figure 74 :

- nous émulons des domaines à QoS, gérés chacun par un Resource Manager (RM) ;
- le domaine satellite se trouve physiquement sur le site de l'ENSICA à Toulouse et il est relié à la plate-forme par l'intermédiaire d'un lien gigaoctet ;
- la partie de la plate-forme utilisée pour les tests EuQoS est composée de 8 ordinateurs PowerEdge 750 avec un processeur Pentium(R) 4, 3,00Ghz et 1 Go RAM, deux commutateurs et trois routeurs.

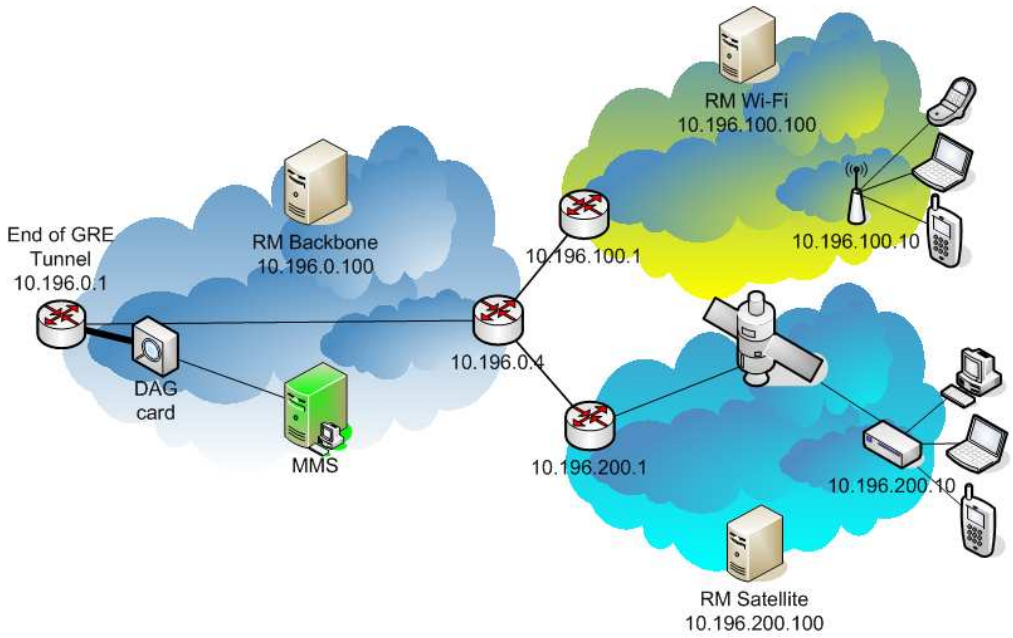


Figure 74 : Configuration d'expérimentations

4.3.2. Plate-forme européenne du projet EuQoS

Cette section décrit la plate-forme européenne utilisée pour les tests et les mesures dans EuQoS afin de tester l'architecture dans un environnement similaire aux réseaux réels.

Pour atteindre cet objectif, plusieurs plates-formes de tests (dont celle du LAAS décrite précédemment) ont été mises en place et interconnectées par le réseau GEANT. Les sites impliqués dans cette opération sont représentés dans la Figure 75.

Six pays et douze réseaux accèdent ainsi à GEANT par l'intermédiaire de réseaux nationaux de la recherche (NREN) et ont participé à cette plate-forme : TID, UPC et SOLUZIONA en Espagne (REDIRIS), FTRD et LAAS-CNRS en France (RENATER), PTIN et FTUOC (RCTS) au Portugal, UoB en Suisse (SWITCH), UoP en Italie (GARR) et PTRD, PTC et WUT en Pologne (PIONIER).

GEANT offre un service Premium IP (PIP) et des réseaux privés virtuels de niveau 2 (L2VPN). Ces deux services ont été utilisés dans le cadre du projet EuQoS : PIP pour l'évaluation de la QoS dans le cœur du réseau et L2VPN pour isoler le routage spécifique du système EuQoS de celui utilisé par GEANT (BGP4+). Notons également qu'EuQoS ne s'intéresse pas au multicast réseau, mais implémente un multicast QoS au niveau applicatif.

Comme le service L2VPN n'était pas supporté par tous les NREN, la solution adoptée a consisté à établir des tunnels entre les différents sites de tests inventoriés auparavant (Figure 76). Cette solution repose sur les tunnels GRE (Generic Routing Encapsulation) [Farinacci00] entre chaque couple de partenaires impliqués dans les tests.

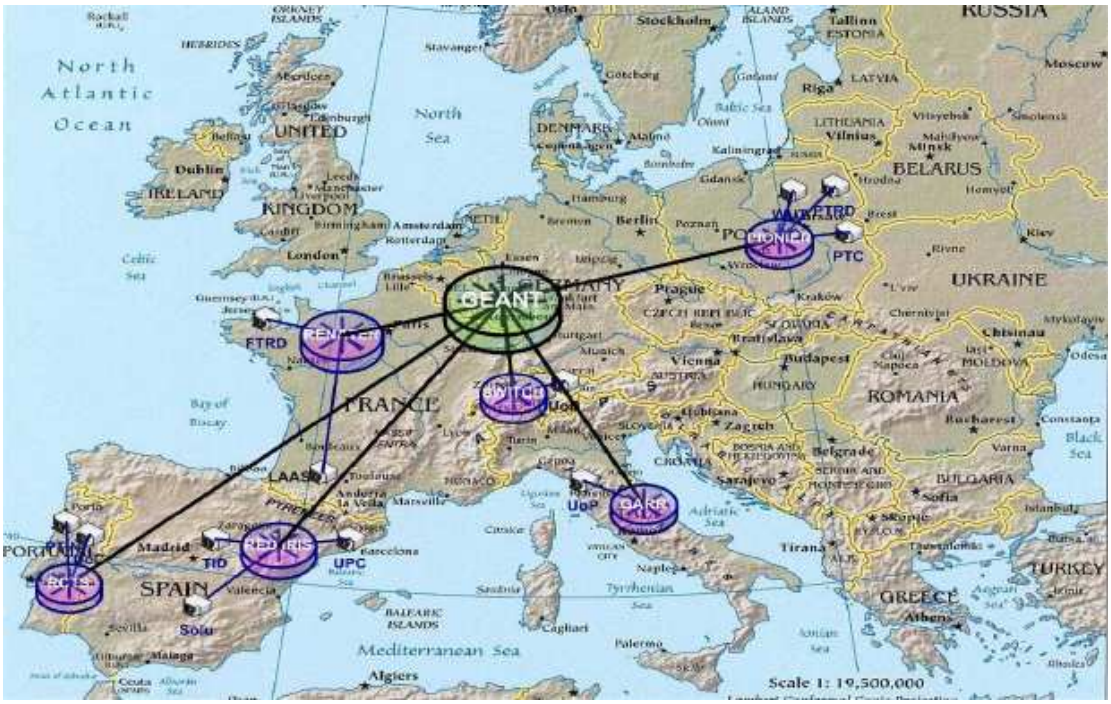


Figure 75 : Plate-forme de test EuQoS

Comme GEANT et les NREN ne supportent pas de mécanismes pour la mise en place dynamique de QoS (mécanisme de routage notamment), le choix retenu a été de masquer le routage à QoS du projet EuQoS (EQ-BGP) dans le réseau GEANT (en utilisant les tunnels GRE). Des sessions EQ-BGP privées ont été établies de cette manière entre les routeurs de tous les sites participants (full-mesh) qui ne sont pas visibles par les autres routeurs GEANT (Figure 76).

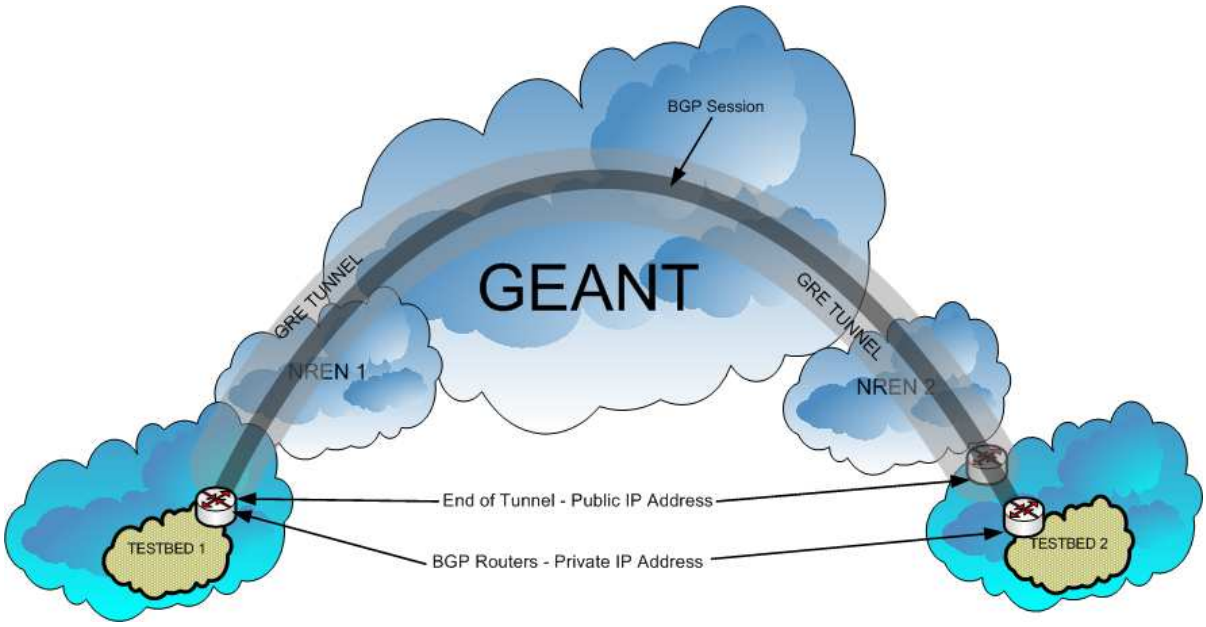


Figure 76 : Tunnel GRE et session EQ-BGP

Cette solution présente plusieurs avantages :

- les extrémités des tunnels étant bien définies, ceci permet de placer des sondes pour la métrologie ;

- les sessions EQ-BGP privées permettent d'utiliser un routage à QoS qui n'est pas supporté par GEANT ;
- de plus, ces sessions sont facilement paramétrables, ce qui donne la possibilité de créer des topologies multi AS variées.

De plus, chaque partenaire s'est vu attribué une plage d'adresses privées de classe A (10.x.x.x/16) et un numéro d'AS privé (pour ne pas interférer avec le routage NREN/GEANT). Le domaine LAAS a utilisé le numéro d'AS 65504 et des adresses dans la plage 10.196.0.0/16. Les détails de chaque site EuQoS sont donnés dans le délivrable [D511].

Plusieurs types de tests ont été réalisés sur cette plate-forme européenne dans le cadre du projet EuQoS :

- caractérisation en termes de débit sur le réseau entre les sites avec différents types de flux (TCP et UDP) ;
- tests de bout-en-bout pour évaluer le temps d'établissement de connexion, en utilisant des applications VoIP avec SIP et VoD ;
- performances du protocole EQ-BGP, etc.

Nous avons installé les outils et les logiciels nécessaires et nous avons participé à tous ces tests de validation, intégration ou de performance. Nous focalisons la suite de ce chapitre sur les tests concernant la signalisation. Les autres résultats obtenus sont disponibles dans les délivrables [D512, D513, D521, D522].

Les tests présentés ci-après ont été réalisés sur la plate-forme décrite au début de cette section, entre le site du LAAS et ceux de Telefonica (TID), de Portugal Télécom (PTIN), de Polish Télécom (PTRD), de l'Université de Varsovie (WUT), de l'Université de Bern (UoB), et de l'Université de Coimbra (UoC). Nous avons étendu ces tests avec une plate-forme mise en place à l'Université Fédérale de Santa Catarina (UFSC) Brésil, qui a été associée aux expérimentations du projet EuQoS.

4.3.3. Tests fonctionnels

4.3.3.1. Spécification

Nous considérons dans ce paragraphe le déploiement et les tests de l'implémentation présentée en début de ce chapitre. La topologie utilisée pour ces tests est illustrée Figure 77. Ces tests ont été réalisés entre la plate-forme de LAAS qui comporte deux AS (AS1 et AS2) et respectivement TID, PTIN, et PTRD (AS3).

Figure 77 : Topologie pour les tests fonctionnels

Pour valider le déploiement du système, nous avons défini plusieurs scénarios permettant d'étudier le comportement du RM et du CallController vis-à-vis de la réservation des ressources.

Ces scénarios de tests, résumés dans le Tableau 10, visent à valider les phases d'invocation des services, de réservation réussie, d'échec de réservation et de libération des ressources. Notons que ces scénarios ont été affinés et développés pour valider l'ensemble des modules. Ces détails se trouvent dans le délivrable D5.2.3 [D523].

Les résultats dans le cas nominal de tous ces scénarios ont validé le comportement du RM, et du module CallController en particulier.

Scénario	Type de tests	
1	Connexion initiée par l'émetteur	Réservation réussie
2	Connexion initiée par le récepteur	
3	Connexion bidirectionnelle	
4	Requête irrégulière (impossible à analyser)	Réservation échouée
5	Paramètres de la requête incorrects	
6	Ressources insuffisantes	
7	Problème configuration équipement	
8	Libération des ressources suite à une requête explicite	Libération
9	Libération des ressources suite à un problème (message d'EQ-NSIS)	
10	CallController dans le premier domaine (d'accès)	Comportement en fonction de la topologie
11	CallController dans un domaine de cœur	
12	CallController dans le dernier domaine	

Tableau 10 : Scénarios de tests

4.3.3.2. Résultats et analyse

Les scénarios 1 à 3 ont confirmé le bon fonctionnement des modules dans le cas d'une réservation qui aboutit positivement, en considérant différents contextes d'exécution : communication initiée par l'émetteur, par le récepteur, communication bidirectionnelle pour laquelle le chemin suivi par les données peut ne pas être symétrique.

Les scénarios de 4 à 7 ont confirmé le fonctionnement du système dans les situations où la réservation des ressources échoue : les ressources ne sont pas disponibles, la configuration des équipements n'a pas abouti (problème matériel), ou des cas spéciaux ont survenu, par exemple une requête formulée de façon incorrecte (impossible à traiter par le RM), ou des paramètres fournis ne permettant pas de continuer le processus de réservation (adresses IP incorrectes par exemple).

Les scénarios 8 et 9 ont permis de valider la libération des ressources dans le cas d'une requête explicite, ou bien dans une situation particulière due à un problème dans le réseau détecté par EQ-NSIS qui propage une demande au CallController.

Enfin, les scénarios 10 à 12 ont permis de valider le comportement du module CallController, qui est différent en fonction du positionnement du domaine (premier ou dernier domaine sur le chemin de données, ou domaine du cœur).

Ces scénarios ont été effectués dans un premier temps avec une application de test conçue dans le cadre du projet par la société Silogic (aujourd'hui AKKA Technologies

Informatiques et Systèmes). Cette application permet de générer des requêtes d'invocation de QoS paramétrables, ce qui a offert la possibilité de tester les scénarios évoqués. De plus, il est possible d'effectuer des requêtes de QoS à l'aide d'une page WEB, les paramètres de QoS étant décrits dans un fichier XML.

Dans un deuxième temps, plusieurs applications ont été intégrées avec le système EuQoS : application de visioconférence (Platine) développée par le LAAS et Silogic, de vidéo à la demande par l'Université de Paderborn, Medigraf (application de télé-médecine) par Portugal Telecom, et le jeu open-source multi utilisateur Nexuiz, adapté par l'Université Technologique de Varsovie (WUT). Notons que ces expérimentations ont été complétées par le test d'une solution de multicast applicatif (impléméntée par l'Université de Bern) qui intègre la signalisation proposée.

4.3.3.3. Conclusion

Les tests ainsi réalisés ont confirmé d'une part le bon fonctionnement des divers modules et protocoles, et d'autre part l'intégration réussie avec le système des différentes applications qui ont des besoins en QoS. L'utilisation de trois domaines a également permis de considérer l'adéquation dans un environnement multi-domaine.

4.3.4. Tests de garantie de QoS

4.3.4.1. Spécification

Ce paragraphe décrit les tests réalisés entre le LAAS et WUT en Pologne en intégrant tous les modules du système EuQoS, en particulier des RA réels pour la technologie Wi-Fi. Leur objectif principal était de vérifier que le système est capable, suite à la signalisation et à la configuration des équipements, de garantir les ressources pour une application temps réel.

Nous avons analysé les performances de bout en bout obtenues pour l'application de jeux multi-utilisateur Nexuiz, distribuée entre les sites de WUT et de LAAS[15] :

- Nexuiz fait partie des applications interactives dont les besoins en QoS correspondent au service EuQoS fourni par la classe de service (CoS) de bout en bout « RTInteractive » [16] : IPTD < 100 msec, IPDV < 50 msec et IPLR < 10^{-3} ;
- le trafic Nexuiz est échangé entre le serveur de jeux localisé au LAAS et des clients localisés à Varsovie sur la plate-forme de WUT ;
- l'application Nexuiz a été adaptée par WUT au système EuQoS pour être capable d'effectuer une invocation du service à QoS offert par EuQoS;
- les performances mesurées sont les paramètres IPTD, IPDV et IPLR.

Nous comparons les performances obtenues dans les trois cas suivants :

1. le trafic Nexuiz utilise la CoS de bout en bout « Standard » (équivalente au best-effort) sans trafic de fond (c'est à dire susceptible de générer une dégradation de QoS). Ce scénario constitue la référence de notre étude par la suite ;
2. le trafic Nexuiz utilise la CoS de bout en bout « Standard » avec trafic de fond ;
3. le trafic Nexuiz utilise la CoS de bout en bout « RTInteractive » avec trafic de fond.

[15] Notons qu'un tunnel PIP sur GEANT a été établi entre ces deux domaines afin de garantir la continuité de la QoS sur GEANT.
[16] Les CoS de bout en bout définies dans EuQoS sont décrites au Chapitre 3.

Le scénario utilisé pour ces tests est présenté dans la Figure 78 : il implique deux domaines d'accès (Wi-Fi WUT 10.203.0.0/16 et LAN Ethernet LAAS 10.196.0.0/16), des machines synchronisées par NTP[17] utilisant une antenne GPS[18]. La configuration du point d'accès Wi-Fi[19] contrôlé par un RA est la suivante : niveau physique 11Mbps, mode B seul activé, préambule long avec extension Wireless MultiMedia (WMM) aussi activée.

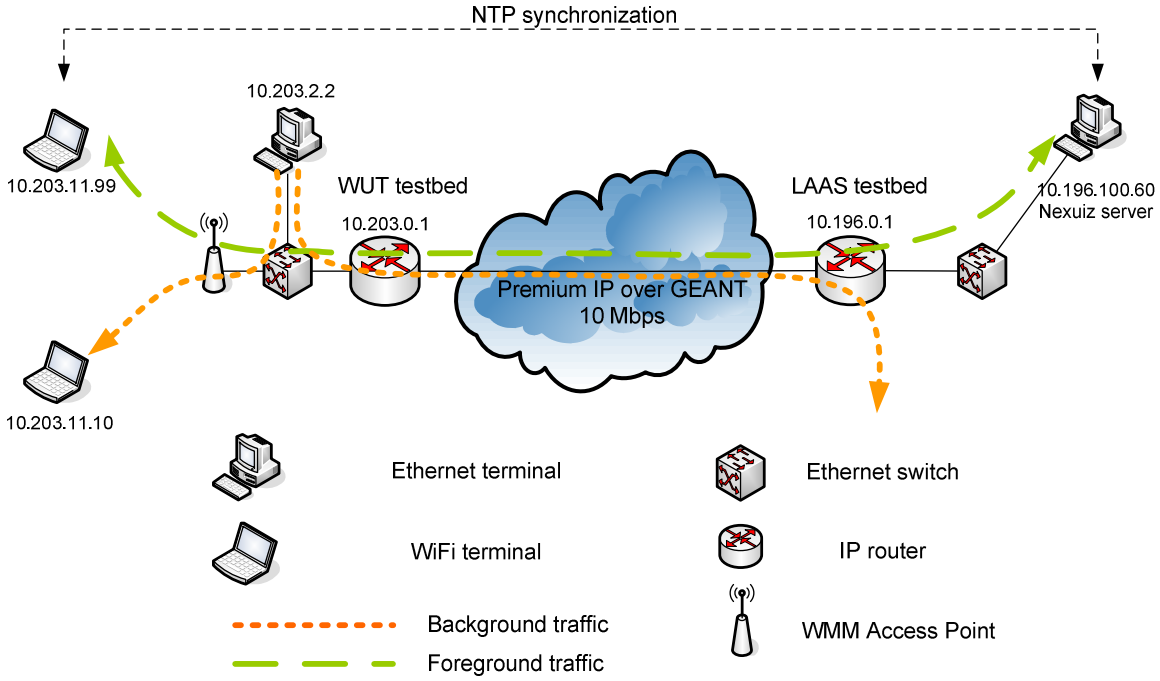


Figure 78 : Scénario de test pour l'application Nexuiz

Nous nous intéressons au trafic dans le réseau d'accès WUT (technologie Wi-Fi), d'abord dans le cas d'une utilisation de la CoS Standard, et puis d'une réservation pour la CoS RTInteractive.

Les outils utilisés sont :

- l'application Nexuiz pour le trafic premier plan ; le débit crête de cette application est estimé à 128 kbps.
- le générateur de trafic MGEN (http://cs.itd.nrl.navy.mil/work/mgen/) pour l'injection du trafic de fond,
- Tcpdump (www.tcpdump.org) pour la capture des paquets,
- et Packet Trace Analyser (outil développé dans le cadre d'EuQoS) pour l'analyse des traces.

Les tests ont eu une durée de 30 minutes.

Les paramètres du trafic de fond pour les scénarios 2) et 3) sont résumés dans le Tableau 11. Ces paramètres sont issus des simulations et utilisés lors des différents tests dans le cadre du projet.

From [IP]	To [IP]	Peak Bit Rate	Packet Length	Packet Intensity	Traffic profile	e2e CoS

[17] Network Time Protocol
[18] Global Positioning System
[19] Modèle Linksys WRT54G version 2.0

		[kbps]	[bytes]	[1/s]		
10.203.2.2	10.203.11.10	5640	1500	470	Poisson	Standard
10.203.2.2	10.196.0.1	9600	1500	800	Periodic	Standard
10.203.2.2	10.196.0.1	234	200	146	Poisson	Telephony
10.203.2.2	10.196.0.1	228	1500	19	Poisson	RTInteractive

Tableau 11 : Paramètres du trafic de fond

4.3.4.2. Résultats et analyse

Les résultats obtenus sont présentés dans le Tableau 12.

Case	Direction	mean IPTD [ms]	IPDV [ms]	IPLR	Packets sent
1	WUT→LAAS	28.1	6.9	0*	27868
	LAAS→WUT	28.7	8.9	0*	30025
2	WUT→LAAS	358.6	9275	5.4×10^{-2}	34632
	LAAS→WUT	46.0	551.9	2.9×10^{-3}	36284
3	WUT→LAAS	30.7	28.4	6.2×10^{-4}	26004
	LAAS→WUT	29.5	17.3	0	28509

Tableau 12 : Résultats pour les tests avec Nexuiz

L'analyse de ce tableau permet de tirer les conclusions suivantes :

- les résultats du scénario 1 sont acceptables compte tenu des besoins en QoS de Nexuiz, c'est à dire : IPTD < 100 msec, IPDV < 50 msec et IPLR < 10^{-3};
- les résultats du scénario 2 ne sont pas acceptables ; de plus, du point de vue du client, l'expérience et le contrôle de jeu se sont avérés totalement insatisfaisants ;
- les résultats du scénario 3 sont acceptables pour Nexuiz.

4.3.4.3. Conclusion

Ces différents résultats permettent de justifier la nécessité d'assurer des garanties des QoS pour des types particuliers de trafic. Nous avons montré le bon fonctionnement du système EuQoS dans ce premier exemple d'invocation, de signalisation et de configuration des équipements réseau pour la mise en place des garanties de QoS.

4.3.5. Tests de performance (avec NSIS)

L'objectif des tests suivants est d'évaluer l'implémentation du dernier prototype EuQoS en termes de nombre de requêtes traitées. Ce prototype a été déployé sur la plate-forme décrite dans la section 4.3.2. Sur ces bases, nous analysons les performances du système et repérons les limites de l'implémentation actuelle.

4.3.5.1. Spécification

Une première phase de tests (décrite dans le délivrable [D523]) a été réalisée par TID pour l'étude du plan de service et du plan de contrôle (en particulier le RM). Le scénario utilisé comportait un seul domaine et l'objectif était de fournir les premiers résultats sur le délai d'établissement et de fermeture d'une session EuQoS.

Nous avons étendu ce scénario à une topologie composée de trois domaines en nous intéressant au délai d'établissement d'une session et au temps de traitement dans chaque RM.

La topologie utilisée pour ces tests est illustrée dans la Figure 79 : trois domaines, deux au LAAS et un autre successivement sur chacun des deux sites partenaires (UoC et UoB) interconnectés par le tunnel GRE sur GEANT. Du point de vue topologique, le tunnel GRE est considéré comme un simple lien inter-domaine.

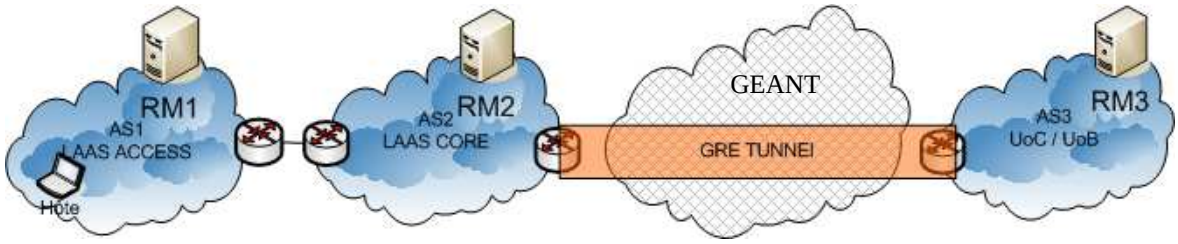


Figure 79 : Topologie de test

Le Tableau 13 résume les caractéristiques des machines utilisées :

Machine	Matériel	Système Exploitation
LAAS-RM1 AS 1 10.196.100.100	Dell Power Edge 750 Intel P4 3,00GHz 1Go RAM	Linux Debian Kernel 2.4.27 Java 1.5.0_11
LAAS-RM2 AS2 10.196.0.100	Dell Power Edge 750 Intel P4 3,00 GHz 1Go RAM	Linux Fedora Core 5 Kernel 2.6.15 Java 1.5.0_11
UoB RM AS3 10.195.0.5	Intel P4 1,8GHz 1Go RAM	Fedora Core 4 Kernel 2.6.17 Java 1.4.2_10
UoC RM AS 10.202.0.101	Intel P4 3,00GHz 512 Mo RAM	Debian Kernel 2.6.8 Java 1.4.2_04

Tableau 13 : Description des machines

Pour évaluer les performances du système, en particulier des RM, nous avons développé un outil qui permet de générer des requêtes de réservation de ressources. Cet outil est paramétrable en termes de :

- nombre de requêtes (unidirectionnelles) par seconde ;
- durée du test ;
- QoS requise.

Pour ces tests, nous avons émulé le RA (à partir des résultats de mesures sur des équipements réels et utilisés également pour d'autres tests décrits dans le [D523]) :

- la réponse pour le contrôle d'admission est modélisée par une loi exponentielle de moyenne 50 millisecondes ;
- la configuration des équipements suit une loi exponentielle de moyenne 700 msec.

4.3.5.2. Résultats et analyse

Les figures suivantes illustrent les résultats obtenus pour les tests effectués entre LAAS et UoB d'une part et entre LAAS et UoC d'autre part.

La Figure 80 et la Figure 81 fournissent le temps de réponse entre l'envoi de la requête et la réception de la réponse. Ce temps inclut le temps de traitement sur chaque RM au long du chemin de données et le temps de transfert entre ces RM. La Figure 82 et la Figure 83 donnent le temps d'exécution sur chaque RM.

Nous pouvons constater que le temps d'établissement d'une session varie entre 1,6 secondes et 3,7 secondes pour les tests LAAS-UoB et entre 1,6 et 2,5 secondes pour les tests LAAS-UoC.

Remarquons l'évolution faible de la courbe jusqu'à 20 requêtes par seconde. Pour un nombre de requêtes supérieur, le prototype #4 utilisé n'est pas suffisamment performant, les requêtes n'ayant plus de réponse ou d'autres requêtes ne pouvant plus être traitées.

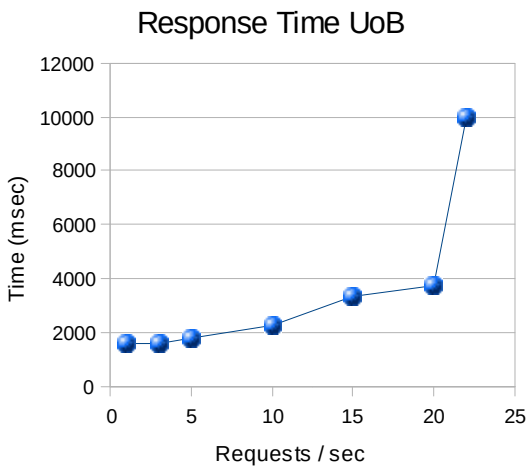


Figure 80 : RTT LAAS UoB

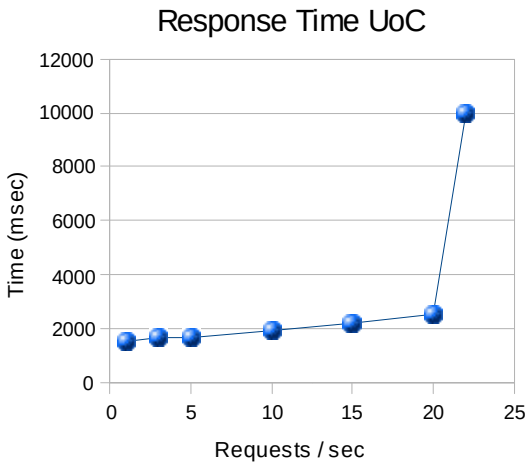


Figure 81 : RTT LAAS UoC

La Figure 82 et la Figure 83 illustre le temps de traitement dans un RM.

Il est à noter que ce temps est légèrement supérieur sur le premier RM du au fait que plusieurs opérations qui s'exécutent sur celui-ci ne sont pas effectuées par les autres RM, en particulier la vérification du CAC de bout-en-bout par le module « End-to-END CAC », avec des accès supplémentaires à la base de données RMDB.

Le temps de traitement dans les RM est similaire dans les deux cas, bien que les caractéristiques des machines soient différentes. Nous pouvons en conclure que dans ce prototype du système, le nombre de requêtes supportées par seconde est de 20.

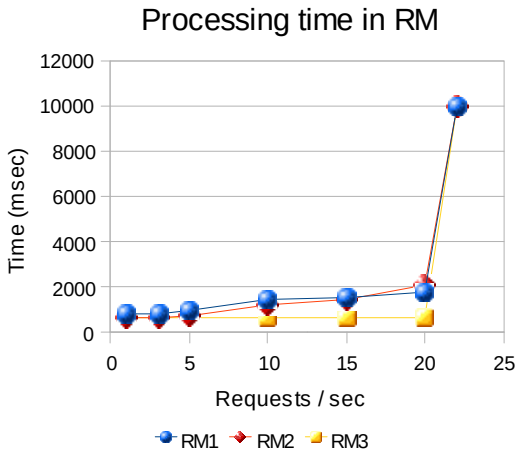


Figure 82 : Traitement sur les RM LAAS UoB

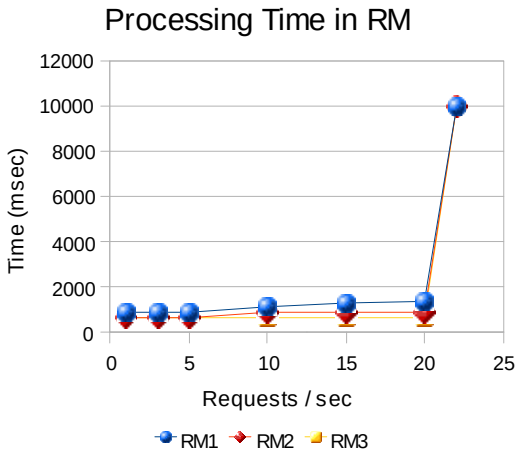


Figure 83 : Traitement sur les RM LAAS UoC

Ces résultats confirment ceux réalisés par TID, décrits dans le délivrable [D523] : le système peut répondre à une charge de 20 requêtes par seconde. Ces tests ont identifié plusieurs problèmes de l'implémentation (mise à l'échelle, compatibilité avec les versions Java, non respect de la spécification) et ont fourni également des recommandations pour les développements futurs.

4.3.5.3. Conclusion

Suite à ces résultats et aux analyses effectuées, il a apparu qu'une limite du système était liée à l'implémentation actuelle de NSIS (une nouvelle version sera bientôt disponible).

Nous avons décidé de simplifier l'architecture et de remplacer NSIS par un protocole qui implémente mois de fonctionnalités, basé sur des sockets TCP, déjà utilisé dans la première version du prototype EuQoS.

Notons que par cette implémentation de la signalisation, nous ne bénéficions plus des avantages de NSIS (sécurité, modularité, protocole transactionnel), mais elle nous permet d'augmenter et analyser le nombre de requêtes de réservation.

Ces tests sont décrits dans les paragraphes suivants.

4.3.6. Test de performance (sans NSIS)

4.3.6.1. Spécification

Ces tests ont été effectués en deux étapes : 1) en local sur la plate-forme du LAAS en rajoutant un troisième domaine, et 2) avec l'Université Fédérale de Santa Catarina à Florianópolis, Brésil (UFSC).

Pour ces tests, la même topologie à trois domaines que dans les cas précédents a été utilisée. Les caractéristiques de la machine RM de UFSC sont les suivantes : processeur Pentium P4 à 1,8 GHz, 1Go RAM et le système d'exploitation Linux Debian avec la version du noyau 2.6.18. Les sections suivantes reproduisent les mêmes types de graphiques que pour les tests précédents (temps de réponse sur le client et temps de traitement dans le RM).

4.3.6.2. Résultats et analyse

La Figure 84 et la Figure 85 illustrent le temps d'établissement des sessions. Nous pouvons observer une évolution considérable sur le nombre de requêtes que le RM peut gérer en parallèle.

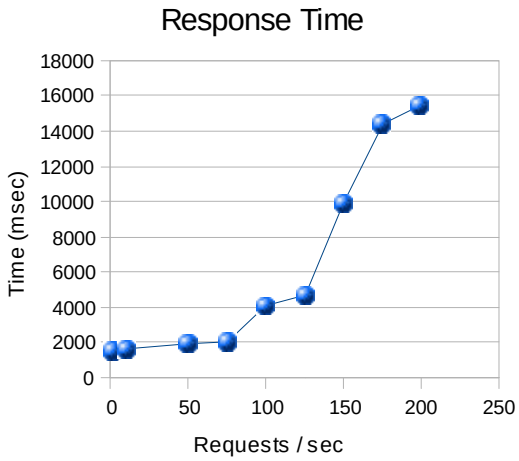


Figure 84 : RTT tests locaux

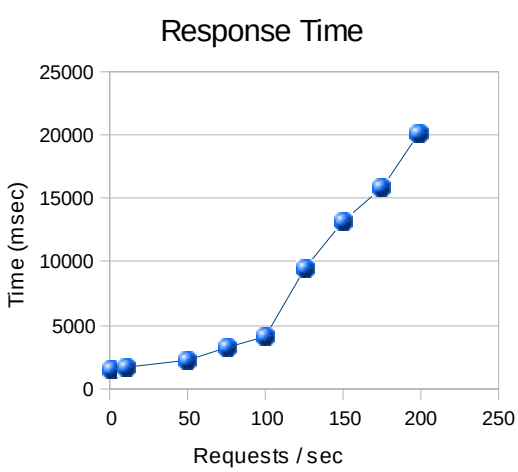


Figure 85 : RTT UFSC

Nous remarquons l'arrivée des réponses en un temps inférieur à 4 secondes (pour les tests en local) et 4.7 secondes pour les tests avec UFSC, différence qui s'explique d'une part par l'utilisation d'une machine plus puissante pour le RM3 au LAAS, et d'autre part par le délai plus important entre les machines situées en France et au Brésil.

Notons que pour une charge moyenne du système de réservation, la recommandation ITU-T [ITU-T-E721] définit la valeur du délai moyen souhaité pour l'établissement des connexions à : 3 secondes pour les communications locales, 5 secondes pour celles interurbaines et 8 secondes pour les communications internationales (les valeurs pour une charge de 95% sont respectivement de 6, 8 et 11 secondes).

Concernant le temps de traitement dans chaque RM, nous remarquons qu'il reste dans des limites acceptables, au dessous de 750 msec pour une charge de moins de 125 requêtes par seconde. Les résultats obtenus sont illustrés dans la Figure 86 et la Figure 87. Pour ces cas, remarquons également que le traitement dans le premier RM prend plus de temps que dans les deux autres RM (pour les mêmes raisons que celles présentées dans la section 4.4.5).

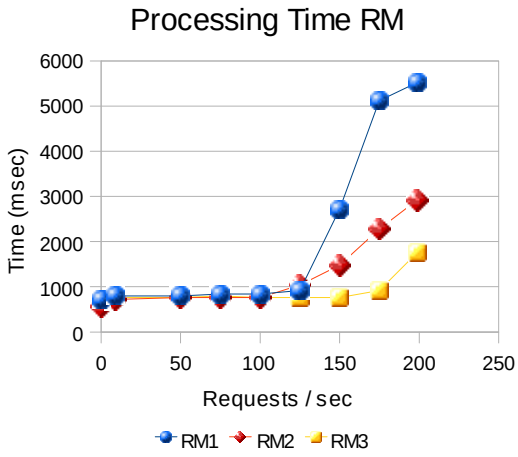


Figure 86 : Traitement dans les RM local

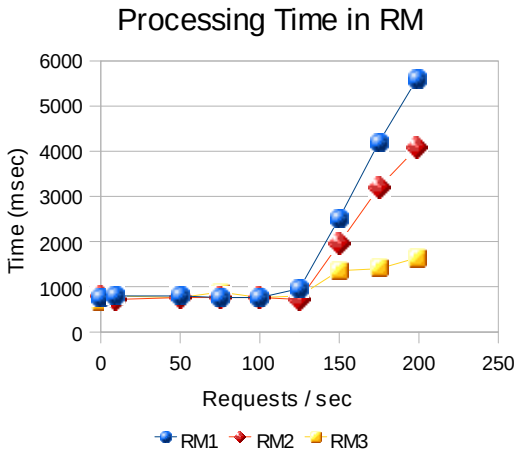


Figure 87 : Traitement dans les RM avec UFSC

Dans les mêmes figures, nous remarquons que le temps de traitement dans les RM ne change pas de manière significative entre les tests locaux et distants.

Nous pouvons également observer que le temps de traitement dans les RM est relativement réduit par rapport au RTT, ce qui nous amène à considérer que la part la plus importante du délai est introduite par les files d'attente existantes entre les modules qui communiquent de manière asynchrone et par la gestion des threads, et non pas par le traitement (du CallController en particulier) proprement dit.

4.3.6.3. Conclusion

Les résultats obtenus lors de ces tests ont révélé que le temps d'attente dans les files d'attentes (communication asynchrone entre les modules, gestion des pools des threads) était important. Lors des différents tests où nous avons paramétré différemment la taille de certaines files, nous avons remarqué une amélioration des performances au détriment de la consommation de mémoire.

Une des perspectives immédiates de ces travaux est de revoir cette implémentation ainsi que le paramétrage de files d'attentes. De plus, il serait intéressant d'utiliser une nouvelle version de la machine virtuelle Java et d'analyser à nouveau les performances.

Ces remarques nous ont conduit à considérer un nouveau type de test pour évaluer le CallController seul, sans les modules adjacents.

4.3.7. Tests de performance CallController seul

Cette section a pour but d'évaluer les performances du module CallController en termes de nombre de requêtes traitées simultanément. Nous suivons la même méthodologie et reproduisons les mêmes graphiques que dans les tests précédents.

4.3.7.1. Spécification

Nous avons remplacé les modules réels E2ECAC, DCAC, MMFM par des modules « stub » pour ne plus avoir à faire passer les messages entre ces modules. Par ailleurs, nous avons utilisé le même outil pour envoyer des requêtes à un CallController, en utilisant la même implémentation TCP au lieu de NSIS.

La Figure 88 illustre le scénario de ce test qui est similaire aux précédents : une machine qui héberge un outil de génération de requêtes envoyées vers le RM1.

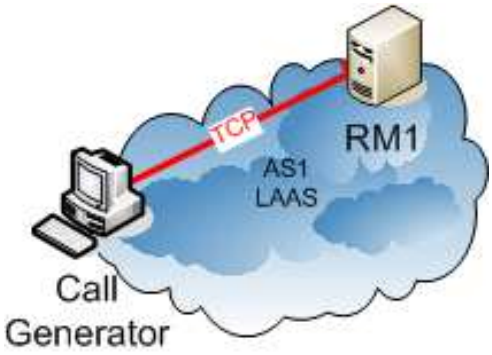


Figure 88 : Scénario pour les tests de charge du CallController

4.3.7.2. Résultats et analyse

Nous donnons ici les résultats pour trois échantillons de tests effectués dans des conditions similaires.

La Figure 89 illustre le temps de réponse pour le scénario considéré. Notons qu'il est possible d'obtenir jusqu'à 200 requêtes par seconde qui reçoivent une réponse au dessous de 7 secondes.

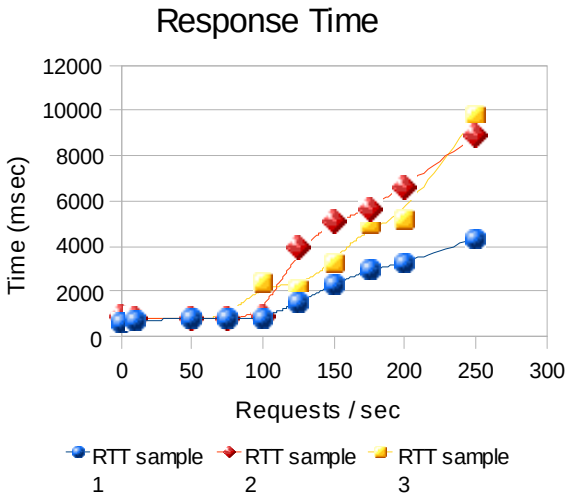


Figure 89 : Temps de réponse charge

Dans la Figure 90, nous analysons le temps de traitement dans le CallController.

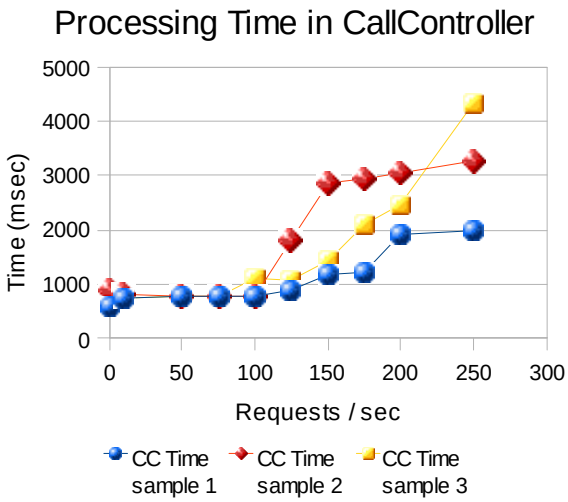


Figure 90 : Traitement dans le CallController

La Figure 91 fournit une répartition du délai pour lequel 99% des requêtes ont reçu la réponse (ce qu'on appelle quantile 99). Remarquons que pour une charge jusqu'à 150 requêtes par seconde, ce délai est inférieur à 11 secondes.

Nous pouvons en conclure que dans l'implémentation actuelle, le CallController est capable de fournir des résultats acceptables pour une charge de 100 requêtes par seconde.

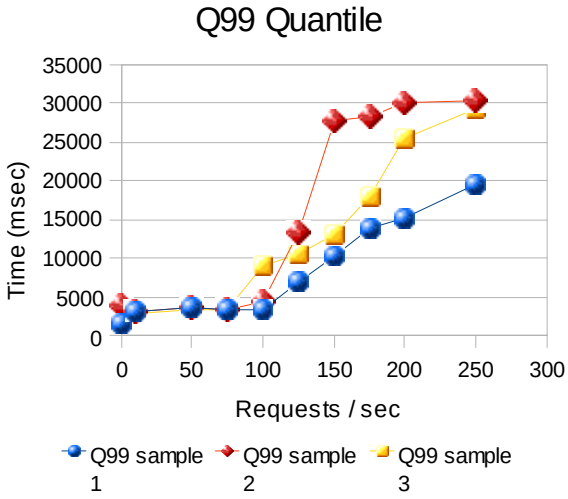


Figure 91 : Quantile 99

4.3.7.3. Conclusion

Les résultats obtenus ont confirmé que le temps de traitement dans le CallController ne représentait pas une partie importante du temps total de traitement des requêtes. La majeure partie du temps est passé en attendant que les requêtes soient traitées dans les files d'attente entre les modules, les files de traitement des threads ou des sockets.

Une des perspectives immédiates qui se dégage est donc d'améliorer le mode de communication inter-module.

4.3.8. Conclusion sur l'ensemble des tests

Nous avons présenté dans cette section trois types de tests :

- des tests fonctionnels ont tout d'abord été réalisés sur la plate-forme du projet EuQoS entre le LAAS et d'autres partenaires (TID, UoC, WUT, UoB) :
- dans un premier temps, le système a été intégré et déployé sur ces sites ;
- ensuite, différents tests ont permis de valider le comportement du système en jouant plusieurs types de scénarios (voir Tableau 10).
- des tests sur la QoS offerte suite à la signalisation mise en place dans l'architecture EuQoS ont ensuite été effectués :
- des tests spécifiques entre paires de partenaires ont été effectués en fonction de la technologie sous jacente. Nous avons illustré les tests réalisées entre LAAS et WUT avec une application adaptée pour prendre en compte les classes de services EuQoS (jeu interactif avec des contraintes temps réel). Nous avons montré qu'en présence du trafic en arrière-plan, les flux EuQoS qui ont réservé les ressources sont protégés par rapport aux flux « best-effort ».
- des tests de performance pour étudier le comportement de la signalisation vis-à-vis de la mise à l'échelle ont enfin été effectués :
- divers problèmes ont été identifiés au niveau de l'implémentation actuelle qui ont un impact sur les performances du système, en particulier au niveau de la gestion des threads, de la mémoire et des files d'attente.

L'ensemble de ces tests a permis d'évaluer l'architecture EuQoS. L'intégration et le déploiement sur une plate-forme distribuée ont validé le fonctionnement du système en termes de performance (nombre de requêtes de service traitées simultanément), QoS assurée dans le réseau. De plus, plusieurs applications ont été adaptées et intégrées en EuQoS.

4.4. Conclusion

Ce chapitre a suivi une démarche incrémentale afin de valider le fonctionnement de l'architecture de signalisation dans le cadre du projet EuQoS.

Dans un premier temps, nous avons effectué des simulations à l'aide de l'outil TAUG2 qui offre une fonctionnalité de jeu des scénarios. Ces simulations nous ont permis de faire une validation fonctionnelle de l'architecture protocolaire et ainsi de préciser un squelette pour l'implémentation en Java.

Dans un deuxième temps nous avons détaillé l'implémentation ainsi que le format des messages échangés entre les CallControllers des différents RM. Nous avons insisté sur les fonctionnalités de différents prototypes implémentés dans le cadre du projet EuQoS, en particulier ceux du CallController et de ses interfaces avec les modules adjacents.

Par la suite, nous avons déployé cette implémentation sur une plate-forme de tests qui a été interconnectée par GEANT à d'autres sites dans le projet EuQoS. Sur chaque site un ou plusieurs domaines ont été créés en s'appuyant sur diverses technologies. Nous avons effectué des tests de performance, pour le RM et plus spécifiquement pour le CallController. Nous avons mis en évidence l'importance des paramètres de l'implémentation (files d'attente, nombre de threads, paramètres de l'exécution) sur l'efficacité du processus d'invocation des ressources. Ceci nous a permis de préciser les limitations de l'implémentation actuelle et de caractériser les pistes les plus significatives pour l'amélioration du prototype.

Nous avons montré également un exemple d'intégration avec une application temps réel (jeu distribué) qui à été modifiée pour l'adapter au système EuQoS. Ces tests ont été effectués entre le LAAS et WUT en Pologne sur un réseau d'accès Wi-Fi, en utilisant une classe de service de bout-en-bout EuQoS, RTInteractive. Ceci nous a permis de vérifier le bon fonctionnement du système suite à la signalisation et à la réservation mises en place, notamment pour la protection du trafic réservé par rapport aux flux standard (best-effort).

Conclusion Générale

Les progrès technologiques de l'informatique et des télécommunications ont favorisé l'apparition de nouveaux types d'application. Pour répondre aux besoins et contraintes de ces applications ainsi que dans un souci d'offrir des services évolués, les communautés réseaux et télécommunication ont initié des nouvelles actions :

- L'IETF a proposé deux architectures IntServ et ensuite DiffServ pour la prise en compte de plusieurs services au niveau IP ;
- Plusieurs propositions ont visé également l'adaptation des couches hautes (Transport et Application) de l'architecture TCP/IP pour répondre au mieux aux besoins ;
- Plus récemment, dans le monde des télécommunications, une nouvelle approche d'architectures de communication connait une effervescence remarquable : les réseaux de nouvelle génération (Next Generation Network - NGN). Ces architectures se déclinent suivant l'organisme de standardisation (ITU-T, 3GPP, ETSI-TISPAN) et reposent sur des protocoles existants en introduisant des nouvelles fonctionnalités pour l'introduction des nouveaux services.
- Plusieurs projets de recherche aux Etats-Unis et en Europe ont essayé d'intégrer les évolutions précédentes dans le but d'offrir des architectures de communication avec des garanties de QoS dans un environnement plus ou moins hétérogène.

Le dénominateur commun de ces propositions est constitué par la nécessité d'une signalisation pour la mise en place des garanties de QoS. A présent, les propositions de gestion de la QoS dans un environnement multi-domaine s'appuient sur plusieurs modèles, le plus générique étant celui qui repose sur le concept de Bandwidth Broker étendu. La coopération entre ces Bandwidth Brokers au long du chemin impose également une signalisation, plus particulière, découplée du chemin de données. Nos travaux s'inscrivent dans ce modèle et visent à répondre aux besoins de signalisation et provisionnement de service dans l'Internet multi-domaine et multi-technologie.

I. Bilan

Les contributions apportées par ces travaux ont été présentées en plusieurs étapes :

- Dans un premier temps nous avons proposé une solution pour une signalisation complètement découplée du chemin de données et liée au contrôle d'admission et au provisionnement. Nous avons défini et spécifié cette solution en UML afin de réserver les ressources dans un contexte multi-domaine. Nous avons présenté les fonctionnalités nécessaires pour son intégration avec des mécanismes de contrôle d'admission ou de configuration des équipements réseau ainsi que les messages échangés entre les entités impliquées.
- Dans un deuxième temps, nous avons présenté une proposition de signalisation hybride dans le cadre des travaux du groupe NSIS (Next Step In Signaling) de l'IETF. Cette proposition, menée en collaboration avec l'Université de Coimbra vise à répondre au problème d'hétérogénéité des domaines qui implantent ou non la suite des protocoles NSIS. Cette solution s'intègre dans l'architecture NSIS et prend en compte donc l'interopérabilité des domaines NSIS et non-NSIS.
- Par la suite nous avons présenté une étude pour l'extension de cette signalisation dans un environnement mobile (en détaillant les implications de trois scénarios sur le protocole initial).

- Nous avons proposé ensuite un modèle de provisionnement dynamique qui a pour objectif la découverte des services disponibles au long du chemin de données et de choisir une concaténation des ces services qui prend en compte des critères d'optimisation des préférences orientées utilisateur ou fournisseur. Cette solution vise à trouver les classes de services disponibles sur chaque domaine, à en sélectionner une concaténation qui répond au mieux aux besoins applicatifs, et ensuite à réserver les ressources pour le service ainsi obtenu. Nous avons proposé une formalisation et nous avons comparé notre solution avec celle classique qui choisit en premier une classe de service et essaye ensuite de réserver les ressources pour cette classe sur tous les domaines.
- Nous avons montré par la suite comment les deux premières propositions ont été intégrées dans le cadre d'une architecture à QoS complexe, celle du projet européen EuQoS. Après avoir introduit l'architecture et les concepts généraux du projet, nous avons décrit les contributions apportées : participation à la conception et à la spécification du système, définition d'une partie des interfaces, implémentation d'une partie des composants, déploiement sur une plate-forme paneuropéenne, et enfin tests, validation et démonstration des prototypes réalisés.

II. Perspectives

Ces travaux ouvrent la voie à diverses perspectives de recherche liées à l'extension de nos contributions sur la signalisation. Nous dégageons deux types de perspectives : des perspectives immédiates qui dérivent directement des ces travaux et des perspectives à moyen et plus long terme qui visent à intégrer ou adapter nos propositions à des architectures standard (telles que les NGN par exemple).

Les perspectives immédiates des travaux présentés dans cette thèse sont :

- de revoir l'implémentation actuelle de plusieurs modules de l'architecture EuQoS) afin d'améliorer les performances du système. Les principaux points à considérer concernent principalement l'implémentation des différents protocoles et interfaces entre les modules, et le traitement des requêtes (gestion des threads, de la mémoire, dimensionnement des files d'attente, etc.) ;
- d'étendre l'intégration avec NSIS, à l'IETF. La solution actuellement étudiée dans le groupe de travail NSIS a pour objectif de fournir une solution couplée au chemin de données. Par la suite, cette proposition intégrera des options pour la participation à la signalisation des entités telles que les contrôleurs de ressources (de type Bandwidth Broker) ;
- d'aborder le contexte hétérogène le plus général en intégrant les domaines surprovisionnés qui ne participent pas directement aux règles de signalisation ou ne sont pas conformes avec notre modèle de gestion de la QoS. Une telle intégration apporterait un niveau supplémentaire d'hétérogénéité au modèle d'Internet ;
- de finaliser l'intégration de la signalisation proposée dans un environnent mobile.

A plus long terme, les principales perspectives sont :

- la possibilité d'accroitre l'interaction entre les différentes couches de l'architecture multi-niveaux en associant les informations des couches hautes avec celles de l'état du réseau. Par exemple, l'intégration globale et l'évaluation des nouveaux services

offerts par des protocoles de transport tels que DCCP, SCTP ou ETP et les protocoles de routage serait une des pistes à évaluer ;

- l'intégration de la signalisation proposée dans un contexte de multicast réseau. Rappelons que dans le cadre d'EuQoS, le système intègre une solution de multicast applicatif, de type pair-à-pair qui utilise les mécanismes de réservation proposés dans l'architecture du projet. Ceci peut être étudié selon plusieurs angles, suivant que les destinataires reçoivent ou non la même QoS ;
- la prise en compte des problèmes de sécurité. La signalisation qui s'appuie sur NSIS, hérite des mécanismes offerts par celui-ci (TLS - Transport Layer Security, IPSec - IP Security). D'autre part, de plus en plus de fonctionnalités telles que les NAT (Network Address Translation) ou les Pare-feux (Firewall) doivent être prises en compte et sont donc à intégrer dans l'architecture.

Bibliographie

[3GPP06] 3rd Generation Partnership Project (2006). Technical specification group services and system aspects, IP Multimedia Subsystem (IMS). Technical Report.

[Ahmed05] Ahmed, T., Asgari, A., Borcoci, E., Kormentzas, G., Kourtis, A., Mehaoua, A., & Xilouris, G. (2005). Enthrone Core Networking Elements for End-to-end QoS Provision over Heterogeneous Settings. IST Mobile Summit 2005.

[Auriol03] Auriol, G., Chassot, C., & Diaz, M. (2003). Evaluation des performances d'une architecture de communication à gestion automatique de la qualité de service. In 10ème Colloque Francophone sur l'Ingénierie des Protocoles (CFIP'03).

[Auriol04] Auriol, G., Chassot, C., & Diaz, M. (2004). Architecture de communication à gestion automatique de la QoS en environnement IP à services différenciés. Technique et Science Informatique (TSI), 23.

[Ash07] Ash, G. Bader, G., Kappler C., and Oran, D. (2007). QoS NSLP QSPEC Template, IETF Draft <draft-ietf-nsis-qspec-19.txt>

[Ash08] Ash, G., Morton A, Dolly M., Tarapore P., Dvorak C., and El Mghazli Y. (2008) Y.1541-QOSM -- Y.1541 QoS Model for Networks Using Y.1541 QoS Classes, IETF draft <qos classes, draft-ietf-nsis-y1541-qosm-06>. 2008.

[Babiarz06] Babiarz, J., Chan, K., & Baker, F. (2006). Configuration Guidelines for DiffServ Service Classes. IETF RFC 4594.

[Bader07] Bader, A., Westberg, L., Karagiannis, G., Kappler, C., & Phelan, T. (2007). RMD-QoSM - The Resource Management in Diffserv QoS Model, IETF draft <draft-ietf-nsis-rmd-12.txt>.

[Bates00] Bates, T., Chandra, R., & Chen, E. (2000). BGP Route Reflection - An Alternative to Full Mesh I-BGP, IETF RFC 2796.

[Bellman58] Bellman, R. (1958). On a routing problem. Quarterly of Applied Mathematics, pages 87-90.

[Bernet00] Bernet, Y., Ford, P., yavatkar, R., Baker, F., Zhang, L., Speer, M., Braden, R., Davie, B., Wroclawsli, J., & Felstaine, E. (2000). A framework for Integrated Services Operation over Diffserv Networks. IETF RFC 2998.

[Blake98] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., & Weiss, W. (1998). An Architecture for Differentiated Services. IETF RFC 2475.

[Bosch05] Bosch, S. (2005). NSLP for Quality-of-Service Signalling, IETF Draft <draft-ietf-nsis-qos-nslp-09.txt>.

[Boucadair05] Boucadair, M. (2005). QoS-Enhanced Border Gatewsay Protocol, IETF Draft <draft-boucadir-qos-bgp-spec-01.txt>.

[Braden94] Braden, R., Clark, D., & Shenker, S. (1994). Integrated Services in the Internet Architecture : An Overview, IETF RFC 1633.

[Braden97] Braden, R., Zhang, L., Berson, S., Herzog, S., & Jamin, S. (1997). Resource Reservation Protocol (RSVP) - version 1 Functional Specification. IETF RFC 2205.

[Brunner04] Brunner, M. (2004). Requirements for Signalling Protocols. IETF RFC 3726.

[Calhoun03] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J (2003). Diameter Base Protocol. IETF RFC 3588.

[Callon90] Callon, R. (1990). Use of OSI IS-IS for Routing in TCP/IP and Dual Environments, IETF RFC 1195.

[Camarillo02] Camarillo, G., Marshall, W., & Rosenberg, J. (2002). Integration of Resource Management and Session Initiation Protocol. IETF RFC 3312.

[Chakravorty06] Chakravorty, S. (2006). IPv6 Label Switching Architecture, IETF Draft <draft-chakravorty-6lsa-02.txt>.

[Chaskar03] Chaskar, H. (2003). Requirements of a Quality of Service (QoS) Solution for Mobile IP, IETF RFC 3583.

[Chassot02] Chassot C, Garcia F, Auriol G, Lozes A, Lochin E, Anelli P. (2002) Performance Analysis for an IP Differentiated Services Network. International Communication Conference (ICC'02).

[Chassot03] Chassot C, Auriol G, Diaz M. (2003) Automatic Management of the QoS within an Architecture Integrating new Transport and IP Services in a DiffServ Internet. 6th IFIP/IEEE International Conference on Management of Multimedia Networks and Services (MMNS'03)

[Chassot06] Chassot, C., Guennoun, K., Drira, K., Armando, F., Exposito, E., and Lozes, A. (2006). Towards Autonomous Management of QoS through Model-driven Adaptability in Communication-Centric Systems. International Transactions on Systems Science and Applications.

[Clark90] Clark, D. and Tennenhouse, D. (1990). Architectural Considerations for a New Generation of Protocols. IEEE SIGCOMM 90 (Symposium on Communication Architectures and Protocols), pages 200-208.

[Cochennec02] Cochennec, J.-Y. (2002). Activities on Next-Generation Networks under Global Information Infrastructure in ITU-T. IEEE Communication Magazine.

[Coltun99] Coltun, R., Ferguson, D., & Moy, J. (1999). OSPF for IPv6, IETF RFC 2740.

[Cortese03] Cortese, G. (2003). CADENUS : Creation and Deployment of End User Services in Premium IP Networks. IEEE Communication Magazine, 41.

[Crawley98] Crawley, E., Nair, R., Rajagopalan, B., & Sandick, H. (1998). A Framework for QoS-based Routing in the Internet. IETF RFC 2386.

[Dabrowski03] Dabrowski, M. & Strohmeier, F. (2003). Measurement based Admission Control in AQUILA Network and Improvements by Passive Measurements. In Art-QoS Warshaw.

[Davie02] Davie, B., Charny, A., Benet, J., Benson, K., Boudec, J. Y. L., Courtney, W., Davari, S., Firoiu, V., & Stiliadias, D. (2002). An Expedited Forwardong PHB (per-hop behaviour). IETF RFC 3246.

[Dijkstra59] Dijkstra, E. W. (1959). A Note on Two Problems in Connections with Graphs. Numerische Matematik, pages 269-271.

[Doldi03] Doldi, L. (2003). UML 2 Illustrated : Developing Real-Time and Communication Systems. TMSO.

[Doolin08] Doolin, K., Robert Mullins, Rafael Morón Abad, and Gómez, M. (2008). Supporting Ubiquitous IMS-based Teleconferencing through Discovery and Composition of IMS and Web Components. Journal of Network and Systems Management (JNSM, Springer).

[Droms97] Droms, R. (1997). Dynamic Host Configuration Protocol, IETF RFC 2131.

[Dugeon05] Dugeon, O., Morris, D., Monteiro, E., Burakowski, W., and Diaz, M. (2005). End to end Quality of Service over Heterogeneous Networks (EuQoS). In Proceedings of Network Control and Engineering for QoS, Security and Mobility, NETCON 2005

[Durham02] Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R., & Sastry, A. (2002). The COPS (Common Open Policy Service) Protocol, IETF RFC 2748.

[Engel03] Engel, T., Graner, H., Koch, B., Winter, M., Sampatakos, P., Venieris, I., Ricciato, H., & Salsano, S. (2003). AQUILA : Adaptative Resource Control for QoS using an IP-based Layered Architecture. IEEE Communication Magazine, 41 : 46-53.

[ETSI-ETR 1994] ETSI-ETR (1994). Network Aspects (NA) ; General Aspects of Quality of Service (QoS) and Network Performance (NP). Technical Report Second Edition, European Telecommunications Standards Institute (ETSI).

[ETSI/GA38(01)18 2001] ETSI/GA38(01)18 (2001). Conclusion from the Next Generation Networks Starter Group. Technical report, European Telecommunications Standards Institute (ETSI).

[Exposito03] Exposito, E. (2003). Spécification et mise en oeuvre d.un protocole de transport orienté Qualité de Service pour les applications multimédia. PhD thesis, INP Toulouse.

[Farrel06] Farrel, A., Vasseur, J. P., & Ash, J. (2006). A Path Computation Element (PCE)-based Architecture. IETF RFC 4655.

[Farinacci00] Farinacci, D., Li, T., Hanks, S., Meyer, D., Traina, P., (2000). Generic Routing Encapsulation (GRE). IETF RFC 2784.

[Feher99] Feher, G., Nemeth, K., Maliosz, M., Cselenyi, I., Bergkvist, J., Ahlard, D., & Engborg, T. (1999). Boomerang : A Simple Protocol for Resource Reservation in IP Networks. In IEEE RTAS.

[Fielding99] Fielding, R., Irvine, UC., Gettys, G., Mogul J., Frystyk, H., Masinter, L. Leach, P., Berners-Lee, T. (1999). Hypertext Transfer Protocol - HTTP/1.1. IETF RFC 2616.

[Finberg02] Finberg, V. (2002). A Practical Architecture for Implementing end-to-end QoS in a IP Network. IEEE Communication Magazine, 40(1) : pages 122-130.

[Flegkas02] Flegkas, P., Trimintzios, P., and Pavlou, G. (2002). A Policy-based Qualifty of Service Management System for IP Diffserv Networks. IEEE Network, Special Issue on Policy-Based Networking.

[Floyd06] Floyd S., Kohler, E., Padhye and J.(2006). Profile for Datagram Congestion Control Protocol (DCCP), Congestion Control ID 3: TCP-Friendly Rate Control (TFRC), IETF RFC 4342.

[Fogelstroem 07] Fogelstroem, E., Jonsson A., Perkins C.(2007). Mobile IPv4 Regional Registration, IETF RFC 4857.

[Ford62] Ford, L. R., Fulkerson D. R. (1962). Flows in Networks. Princeton University Press.

[Forouzan03] Forouzan B., A. (2003). TCP/IP Protocol Suite.

[Füzesi03] Füzesi, P., Németh, K., Borg, N., Holmberg, R., & Cselényi, I. (2003). Provisioning of QoS enabled Inter-domain Services. Computer Communication.

[Gao04] Gao, X.,Wu, G., & Miki, T. (2004). End-to-end QoS Provisioning in Mobile Heterogeneous Networks. IEEE Wireless Communication.

[Giordano03] Giordano, S., Salsano, S., den Berghe, S. V., Ventre, G., & Giannakopoulos, D. (2003). Advanced QoS Provisionning in IP Networks : The European premium IP projects. IEEE Communication Magazine, 41(1) : pages 30-37.

[Gode01] Goderis, D, T'joens Y, Jacquenet C, Memenios G, Pavlou G, Egan R, Griffin D, Georgatsos P, Georgiadis L, Van Heuven P. (2001). Service Level Specification Semantics, Parameters and Negotiation Requirements. Internet draft, work in progress.

[Gozdecki03] Gozdecki, J., Jajszczyk, A., & Stankiewicz, R. (2003). Quality of Service Terminology in IP Networks. IEEE Communication Magazine, 41(3) : pages 153-159.

[Grossman02] Grossman, D. (2002). New Terminology and Clarification for Diffserv, IETF RFC 3260.

[Gulbrandsen00] Gulbrandsen, A., Vixie, P., Esibov, L. (2000) A DNS RR for Specifying the Location of Services (DNS SRV). IETF RFC 2782.

[Guttman99] Guttman, E., Perkins, C., Veizades, J., Day, M., (1999) Service Location Protocol, Version 2. IETF RFC 2608.

[Haddadou06] Haddadou, K., Ghamri-Doudane, S., Ghamri-Doudane, Y., & Agoulmine, N. (2006). Designing Scalable On-demand Policy-based Resource Allocation in IP Networks. IEEE Communication Magazine.

[Hancock05a] Hancock, R. (2005). A Problem Statement for Path-decoupled Signalling in NSIS. IETF draft, work in progress.

[Hancock05b] Hancock, R., Karagiannis, G., Lounghney, J., & den Bosch, S. V. (2005). Next Steps In Signaling (NSIS) : Framework. IETF RFC 4080.

[Handley98] Handley, M. and Jacobson, V. (1998). SDP: Session Description Protocol, IETF RFC 2327.

[Hardy01] Hardy, W. C. (2001). QoS Measurements and Evaluation of Telecommunication Quality of Service. Wiley.

[Hares89] Hares, S., Katz, D. (1989) Administrative Domains and Routing Domains A Model for Routing in the Internet. IETF RFC 1136.

[Harrington02] Harrington, D., Presuhn, R. and Wijnen B., (2002) An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, STD 62, IETF RFC 3411.

[Hawkinson96] Hawkinson, J. & Bates, T. (1996). Guidelines for Creation, Selection, and Registration of an Autonomous System (AS), IETF RFC 1930.

[Hedrick88] Hedrick, C. (1988). Routing Information Protocol, IETF RFC 1058.

[Heinanen99] Heinanen, J., Baker, F., Weiss, W., & Wroclawski, J. (1999). Assured Forwarding PHB Group. IETF RFC 2597.

[HomeGatewayInitiative08] Home Gateway Initiative (2008). Home Gateway Technical Requirements : Residential Profilev1:0:Technical Report.

[Howarth05] Howarth, M., Flekgas, P., Pavlou, G., Wang, N., Trimintzios, P., Griffin, D., Griem, J., Boucadair, M., Morand, P., Asgari, A., and Georgatos, P. (2005). Provisioning for Interdomain Quality of Service : The MESCAL Approach. IEEE Communication Magazine, 43.

[Howarth06] Howarth, M., Boucadair, M., , Flegkas, P., Wang, N., Pavlou, G., Morand, P., Coadic, T., Griffin, D., Asgari, A., and Georgatos, P. (2006). End-to-end Quality of Service Provisionning through Inter-provider Traffic Engineering. Computer Communication, 29(6) : pages 683-702.

[IPCLuster] IST Premium IP Cluster.

[ISO8402-00] ISO8402 (2000). Quality Management and Quality Assurance Vocabulary. Technical Report, International Organization for Standardization.

[ISO9000-00] ISO9000 (2000). Quality Management Systems – Fundamentals and Vocabulary. Technical Report, International Organization for Standardization.

[ITU-T-Rec .E.800-93] ITU-T-Rec.E.800 (1993). Terms and Definitions Related to Quality of Service and Network Performance Including Dependability. Technical Report, International Telecommunication Union.

[ITU-T-Rec. H.323-06] ITU-T-Rec.H323 (2006) Systèmes de communication multimédia en mode paquet. Technical Report, International Telecommunication Union.

[ITU-T-Rec. G.1000-01] ITU-T-Rec.-G.1000 (2001). Communications Quality of Service : A Framework and definitions. Technical Report, International Telecommunication Union.

[ITU-T-Rec. G.707-03] ITU-T-Rec.-G.707 (2003). G.707 : Network Node Interface for the Synchronous Digital Hierarchy (SDH). Technical Report, International Telecommunication Union.

[ITU-T-Rec. X.902-95] ITU-T-Rec.-X.902 (1995). Information Technology - Open Distributed Processing - Reference Model: Foundations. Technical Report, International Telecommunication Union.

[ITU-T-Rec. Y.1541-06] ITU-T-Recommendation-Y.1541 (2006). Network Performance Objectives for IP-based Services. Technical Report, International Telecommunication Union.

[ITU-T-Rec. Y.2001-04] ITU-T-Rec.-Y.2001 (2004). General Overview of NGN. Technical Report, International Telecommunication Union.

[ITU-T-Rec. Y.2012-06] ITU-T-Rec.-Y.2012 (2006). Functional Requirements and Architecture of the NGN. Technical report, International Telecommunication Union.

[ITU-T-Rec. Y.2171-06] ITU-T-Recommendation-Y.2171 (2006). Admission Control Priority Levels in Next Generation Networks. Technical Report, International Telecommunication Union.

[ITU-T-Rec. H.323-06] ITU-T-Rec.H323 (2006) Systèmes de communication multimédia en mode paquet. Technical Report, International Telecommunication Union.

[Jacobson99] Jacobson, V. (1999). An Expedited forwarding PHB. IETF RFC 2598.

[Jia01] Jia, Y. and Chen, M. (2001). A New Architecture of Providing End-to-end Quality of Service for Differentiated Services Network. In IEEE MilCom 2001.

[Katz97] Katz, D. (1997). IP Router Alert Option, IETF RFC 2113.

[Kelly00] Kelly, F., Key, P., & Zachary, S. (2000). Distributed Admission Control. IEEE Journal on Selected Areas in Communication.

[Kendall02] Kendall, S. (2002). The Unified Process Explained.

[Kohler06] Kohler, E., Handley, M., & Floyd, S. (2006). Datagram Congestion Control Protocol (DCCP), IETF RFC 4340.

[Kourtis04] Kourtis, A., Skianis, C., Kormentzas, G., Xilouris, G., Negru, D., Mehaoua, A., Ahmed, T., Borcoci, E., Asgari, H., Eccles, S., & Doeu_, E. L. (2004). Provisioning of End-to-end in Diverse Environments : The ENTHRONE view. WSEAS Transaction on Communication, 2 : pages 626-631.

[Levis05] Levis, P., Boucadair, M., Morand, Pavlou, G., & Trimintzios, P. (2005). A New Perspective Internet. Communications Software and Systems.

[Malis99] Malis, A. & Simpson, W. (1999). PPP over SONET/SDH, IETF RFC 2615.

[Malkin97] Malkin, G. & Minnear, R. (1997). RIPng for IPv6, IETF RFC 2080.

[Malkin98] Malkin, G. (1998). RIP version 2, IETF RFC 2453.

[Manner05] Manner, J. & Fu, X. (2005). Analysis of Existing Quality of Service Signaling Protocols. IETF RFC 4094.

[Manner07] Manner, J., Karagiannis, G., & McDonald, A. (2007). NSLP for Quality-of-Service Signaling, IETF Draft draft-ietf-nsis-qos-nslp-15.txt.

[Mantar04] Mantar, H., Hwang, J., Okumus, T., and Chapin, S. (2004). A Scalable Model for Inter Bandwidth Broker Resource Reservation and Provisioning. IEEE Journal on Selected Areas in Communication, 22.

[Mealling00] Mealling, M., Daniel, R., (2000). The Naming Authority Pointer (NAPTR) DNS Resource Record. IETF RFC 2168.

[Millis84] Millis, D. L. (1984). Exterior Gateway Protocol Formal Specification. IETF RFC 904.

[Miloucheva06] Miloucheva, I., Hetzer, D., Pascottoand, R., and Jonas, K. (2006). Resource Reservation in Advance for QoS based Mobile Applications. International Review on Computers and Software (I.RE.CO.S.).

[Mockapetris83] Mockapetris, P. (1983) Domain Names - Implementation and Specification. IETF RFC 883.

[Moy98] Moy, J. (1998). OSPF version 2, IETF RFC 2328.

[Mykoniati03] Mykoniati, E., Charalampous, C., Georgatos, T. D., Godersi, D., Trimintzios, P., Pavlou, G., & Gri_n, D. (2003). Admission Control for Providing QoS in Diffserv IP Networks : The TEQUILA Approach. IEEE Communication Magazine, 41(1) : pages 38-44

[MPLS-Charter] MPLS-Charter. http://www.ietf.org/html.charters/mpls-charter.html.

[Nguyen02] Nguyen, T. T., Boukhatem, N., Doudane, Y., & Pujolle, G. (2002). COPS-SLS . A Service Level Negotiation Protocol for the Internet. IEEE Communication Magazine, 40.

[Nguyen03] Nguyen, T. T., Boukhatem, N., Doudane, Y., & Pujolle, G. (2003). COPS-SLS Usage for Dynamic Policy-based QoS Management over Heterogeneous IP Networks. IEEE Communication Magazine, 17.

[Nichols98] Nichols, K., Blake, S., Baker, F., and Black, D. (1998). Definition of the Differentiated Service Field (DS Field) in the IPv4 and IPv6 headers. IETF RFC 2474.

[Nichols99] Nichols, N. (1999). A Two-bit Differentiated Services Architecture for the Internet. IETF RFC 2638.

[OMG07] OMG (2007). Uml 2.1.2 Superstructure and Infrastructure. Technical Report.

[Oran90] Oran, D. (1990). OSI IS-IS Intra-domain Routing Protocol, IETF RFC 1142.

[Pan98] Pan, P. and Schulzrinne, H. (1998). YESSIR : A Simple Reservation Mechanism for the Internet. In Proceedings of NOSSDAV98.

[Pan00] Pan, P., Hahne, E., and Schulzrinne, H. (2000). BGRP : A Tree-based Aggregation Protocol for Inter-domain Reservations. Journal of Communications and Networks, 2(2) : pages 157-167.

[Perkins02] Perkins, C. (2002). IP Mobility Support for IPv4, IETF RFC 3344.

[Perkins07] Perkins. C., Calhoun, P., Bharatia, J., (2007) Mobile IPv4 Challenge/Response Extensions (Revised). IETF RFC 4721.

[Polk06] Polk, J. (2006). Extending the Session Initiation Protocol (SIP) Reason Header for Pre-emption Events. IETF RFC 4411.

[Pongpaibool04] Pongpaibool, P. and Kim, H. (2004). Providing End-to-end Service Level Agreement across Multiple ISP Networks. Computer Networks, 46(1) : pages 3-18.

[Postel83] Postel J. and Reynolds, J (1983).Telnet Protocol Specification. IETF RFC 854

[QBone01] QBone Signaling Work Group (2001). Qbone Signaling Design Team, Final Report. Technical Report.

[Qbone abe] QBone Alternative Best Effort (ABE) http://qbone.internet2.edu/.

[Qbone-qbss] QBone Scavenger Service (QBSS) Definition, http://qos.internet2.edu/wg/wg-documents/qbss-definition.txt

[Racaru08] Racaru, S.F., Dugeon, O., Diaz, M. (2008) EuQoS QSPEC template (EQ-QSPEC). QoS parameter specification to be transported by the signaling protocol », EuQoS IST Project Report.

[Rekhter95] Rekhter, Y. and Li, T. (1995). A Border Gateway Protocol 4 (BGP-4), IETF RFC 1771.

[Rekhter06] Rekhter, Y., Li, T., and Hares, S. (2006a). A Border Gateway Protocol 4 (BGP-4). IETF RFC 4271.

[Roques06] Roques, P. (2006). UML 2 par la pratique - Études de cas et exercices corrigés. Eyrolles ISBN 2-212-12014-1.

[Rosen01] Rosen, E., Viswanathan, A., and Callon, R. (2001). Multiprotocol Label Switching Architecture, IETF RFC 3031.

[Rosenberg02] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnson, A., Peterson, J., Sparks, R., Handley, M., and Schooler, E. (2002). SIP : Session Initiation Protocol. IETF RFC 3261.

[Salsano02] Salsano, S., Vincenzo Genova, Fabio Ricciato, and Eichler, G. (2002). Inter-domain QoS signaling: the BGRP Plus Architecture, IETF Draft <draft-salsano-bgrpp-arch-00.txt>.

[Sarangan06] Sarangan, V. and Chen, J. C. (2006). Comparative Study of Protocols for Dynamic Service Negotiation in the Next-Generation Internet. IEEE Communication Magazine, 44(3) : pages 151-156.

[Schelen98] Schelen, O. (1998). Quality of Service Agents in the Internet. PhD Thesis, Lulea University of Technology.

[Schelen02] Schelen, O., Bless, A. C. R., and Dugeon., O. (2002). Path-coupled and Path-decoupled Signalling for NSIS., IETF Draft draft-schelennsis-opopsig-01.txt.

[Schulzrinne98] Schulzrinne, H, Rao, A., Lanphier, R., (1998). Real Time Streaming Protocol (RTSP). IETF RFC 2326.

[Schulzrinne03] Schulzrinne, H., Casner, S., Frederick, R., and Jacobson, V. (2003). RTP : A Transport Protocol for Real-time Applications, IETF RFC 3550.

[Schulzrinne05] Schulzrinne, H. and Hancock, R. (2005). GIST : General Internet Signalling Transport, IETF Draft draft-ietfnsis-ntlp-09.

[Schulzrinne06] Schulzrinne, H. and Polk, J. (2006). Communication Resource Priority for the Session Initiation Protocol (SIP). IETF RFC 4412.

[Shenker97] Shenker, S., Partridge, C., and Guerin, R. (1997). Specification of Guaranteed Quality of Service. IETF RFC 2212.

[Shenker97] Shenker, S. and Wroclawski, J. (1997). General Characterisation Parameters for Integrated Service Network Elements. IETF RFC 2215.

[Soldatos05] Soldatos, J., Vayias, E., and Kormentzas, G. (2005). On the Building Blocks of Quality of Service in Heterogeneous IP Networks. IEEE Communication Surveys and Tutorials, 7(1) : pages 70-89.

[Stewart00] Stewart, R., Xie, Q., Morneault, K., Sharp, C., Schwarzbauer, H., Taylor, T., Rytina, I., Kalla, M., Zhang, L., and Paxson, V. (2000). Stream Control Transmission Protocol, IETF RFC 2960.

[Stewart04] Stewart, R., Ramalho, M., Xie, Q., Tuexen, M., and Conrad, P. (2004). Stream Control Transmission Protocol (SCTP) Partial Reliability Extension, IETF RFC 3758.

[Stewart07] Stewart, R. (2007). Stream Control Transmission Protocol, IETF RFC 4960.

[Stiemerling07] Stiemerling, M., Tschofenig, H., Aoun, C., and Davies, E. (2007). NAT/Firewall NSIS Signaling Layer Protocol (NSLP), IETF Draft <draft-ietf-nsis-nslpnatfw-16.txt>.

[Tanenbaum02] Tanenbaum, A. S. (2002) Computer Networks (4th Edition).

[Terzis99] Terzis, A., Ogawa, J., & Zhang, L. (1999). A Two-tier Resource Management Model for the Internet. IEEE Global Internet.

[Terzis00] Terzis, A., Krawczyk, J., Wroclawski, J., and Zhang, L. (2000). RSVP Operation over IP Tunnels. IETF RFC 2746.

[Trimintzios03] Trimintzios, P., Pavlou, G., Flegkas, P., Georgatos, P., Asgari, A., and Mykoniati, E. (2003). Service Driven traffic Engineering for Intradomain QoS Management. IEEE Network, 17(3) : pages 29-36.

[Vali04] Vali, D., Paskalis, S., Merakos, L., and Kaloxylos, A. (2004). A Survey of Internet QoS Signalling. IEEE Communication Surveys and Tutorials, 6(4) : pages 32-43.

[Vogel95] Vogel, A., Kerhervé, B., Bochmann, G. V., and Gecsei, J. (1995). Distributed Multimedia and QoS : A Survey. IEEE Multimedia, 2 : pages 10-19.

[Vohra07] Vohra, Q. and Chen, E. (2007). BGP Support for Four-octet AS Number Space, IETF RFC 4893.

[Wambeke07] Wambeke, N. V., Armando, F., Chassot, C., & Exposito, E. (2007). A model-based Approach for Self-Adaptive Transport Protocols. Elsevier Computer Communication's Special Issue on End-to-end Support over Heterogeneous Wired-Wireless Networks.

[Wroclawski97a] Wroclawski, J. (1997a). Specification of the Controlled-load Network Element Service. IETF RFC 2211.

[Wroclawski97b] Wroclawski, J. (1997b). The Use of Resource Reservation Protocol with the Integrated Service. IETF RFC 2210.

[Yang03] Yang, J., Ye, J., and Papavassiliou, S. (2003). A New Differentiated Service Model Paradigm via Explicit Endpoint Admission Control. In IEEE International Symposium on Computers and Communication (ISCC'03).

[Yang04] Yang, J., Ye, J., and Papavassiliou, S. (2004). Enhancing End-to-end QoS Granularity in Diffserv Networks via Service Vector and Explicit Endpoint Admission Control. In IEEE Proceeding Communications.

[Yang05] Yang, J., Ye, J., and Papavassiliou, S. (2005). A Flexible and Distributed Architecture for Adaptative End-to-end QoS Provisioning in Next Generation Networks. IEEE Journal in Selected Areas in Communications, 23(2).

[Zimmermann80] Zimmermann, H. (1980). OSI Reference Model - the ISO Model of Architecture for Open System Interconnection. IEEE Transaction on Communication, 28(4).

Délivrables projet EuQoS
http://www.euqos.eu/documents.php?idfolder=262

[D111] D1.1.1: Definition of Business, Communication and QoS models - Intermediate

[D112] D1.1.2: System Design: Functions, Interfaces Specification

[D113] D1.1.3: Business models and system design specification

[D121] D1.2.1: EuQoS exploitation cookbook - intermediate

[D211] D2.1.1: Definition of monitoring equipment and software and location points

[D212] D2.1.2: Validation of the EuQoS system by simulation

[D213] D2.1.3: Developing the monitoring and measurement system

[D213] D2.1.4: Deploying the monitoring and measurement system in testbeds

[D221] D2.2.1: First validation of the EuQoS system by simulation (Phase 2)

[D311] D3.1.1: Extended QoS API and Middleware layer for phase 1 application use-cases

[D312] D3.1.2: Implementation Report - Preliminary

[D313] D3.1.3: Implementation Report

[D324] D3.2.4: Phase 2. Implementation report-Prototype#4 Final

[D411] D4.1.1: Integrated EuQoS system Software architecture for application use cases

[D412] D4.1.2: Application Plug-Ins for application use cases for selectedaccess networks

[D511] D5.1.1: Technical requirements for trials, tasks scheduling

[D512] D5.1.2: Connectivity and performance tests report

[D513] D5.1.3: First individual based EuQoS System test report

[D514] D5.1.4: Testbed integration test plan

[D515] D5.1.5: Trial report

[D524] D5.2.4: EuQoS system demonstrations report for phase 2

[SLSSpec06] Teissere C., Becam D., Dugeon D., Fournis Y., Statiotis S. (2006) SLS Interface Specification. EuQoS IST European Project Report.

[Track2-06] Darmet, J.P., Baresse, L., Lizzi, Y., Méaude, F., Diaz, M. (2006) Track 2 Detailed Design. EuQoS IST European Project Report.

Bibliographie de l'auteur

Revues Internationales avec comité de lecture

« The EuQoS system: a solution for QoS routing in heterogeneous networks », IEEE Communications Magazine, Vol.45, N°2, pp.96-103, Février 2007, X.MASIP-BRUIN, M.YANNUZZI, R.SERRAL-GRACIA, J.DOMINGO-PASCUAL, J.ENRIQUEZ-GABEIRAS, M.A.CALLEJO RODRIGUEZ, M.DIAZ, S.F.RACARU, G.STEA, E.MINGOZZI, A.BEBEN, W.BURAKOWSKI, E.MONTEIRO, L.CORDEIRO

Conférences Internationales avec comité de lecture

« Quality of service management in heterogeneous networks », International Conference on Communication Theory, Reliability, and Quality of Service (CTRQ 08) S.F.RACARU, M.DIAZ, C.CHASSOT

« Inter-domain QoS signaling under mobility » IEEE/IFIP Network Operations and Management Symposium (NOMS 08), E.SSILVA, S.F.RACARU, J.M.FARINES, M.DIAZ

« Hybrid on-path off-path approach for end-to-end signalling across NSIS and non-NSIS domains (HyPath) », Networking'2006. Workhop Towards the QoS Internet, L.CORDEIRO, M.CURADO, E.MONTEIRO, S.F.RACARU, M.DIAZ, C.CHASSOT

« Signalling concepts in heterogeneous IP multi-domains networks », International Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN06). C.CHASSOT, A.LOZES, S.F.RACARU, M.DIAZ

« A user-based approach for the choice of the IP services in the multi domains DiffServ internet », 1st International Workshop on Service Oriented Architecture in Converging Networked Environments (SOCNET06), C.CHASSOT, A.LOZES, S.F.RACARU, G.AURIOL, M.DIAZ

« Heterogeneity and signalling in IP multi domains », International Conference on Networking and Services (ICNS'06), C.CHASSOT, M.DIAZ, S.F.RACARU, A.LOZES

« On multi-domain connection admission control in the EuQoS system », 15th IST Mobile & Wireless Communication Summit 2006, W.BURAKOWSKI, M.DIAZ, O.DUGEON, A.PIETRABISSA, S.F.RACARU, G.SANTORO, H.TARASIUK

Conférences Nationales avec comité de lecture

« Signalisation dans l'Internet multi-domaine hétérogène », Colloque de l'Ecole Doctorale Informatique et Télécommunications (EDIT'2007), S.F.RACARU

« Composition de services IP dans l'internet DiffServ multi-domaine », Colloque de l'Ecole Doctorale Informatique et Télécommunications (EDIT'2006), S.F.RACARU

Drafts IETF

« GIST extension for hybrid On-path Off-path signaling (Hypath). Draft-cordeiro-nsis-hypath-05 », 71th IEFT Meeting, Philadelphia, (USA), 9-14 mars 2008, L.CORDEIRO, M.CURADO, E.MONTEIRO, VBERNARDO, D.PALMA, S.F.RACARU, M.DIAZ, C.CHASSOT

« GIST extension for hybrid On-path Off-path signaling (Hypath). Draft-cordeiro-nsis-hypath-04 », 69th IEFT Meeting, Chicago (USA), 22-27 Juillet 2007, L.CORDEIRO, M.CURADO, E.MONTEIRO, VBERNARDO, D.PALMA, S.F.RACARU, M.DIAZ, C.CHASSOT

« GIST extension for hybrid On-path Off-path signaling (Hypath). Draft-cordeiro-nsis-hypath-03 », 68th IETF Meeting, Prague (République Tchèque), 18-23 Mars 2007, L.CORDEIRO, M.CURADO, E.MONTEIRO, VBERNARDO, S.F.RACARU, M.DIAZ, C.CHASSOT

« Hybrid on-path off-path approach for end-to-end signalling accross NSIS domains (HyPath) Ver.02 », 67th IETF Meeting, San Diego, (USA) 5-10 Novembre 2006, L.CORDEIRO, M.CURADO, E.MONTEIRO, S.F.RACARU, M.DIAZ, C.CHASSOT

« Hybrid on-path off-path approach for end-to-end signalling accross NSIS domains (HyPath) Ver.01 », 66th IETF Meeting, Montréal (Canada), 9-14 Juillet 2006, L.CORDEIRO, M.CURADO, E.MONTEIRO, S.F.RACARU, M.DIAZ, C.CHASSOT

« Hybrid on-path off-path approach for end-to-end signalling accross NSIS domains (HyPath) Ver.00 », 65th IETF Meeting, Dallas (USA), 19-24 Mars 2006, L.CORDEIRO, M.CURADO, E.MONTEIRO, S.F.RACARU, M.DIAZ, C.CHASSOT

Rapports Projets européen IST EuQoS N° 004503 :

« Definition of business, communication and QoS models - Intermediate. D1.1.1 », EuQoS Partners

« Business models and system design specification. D1.1.3 », EuQoS Partners J.ENRIQUEZ-GABEIRAS, M.DIAZ, S.F.RACARU

« Phase 2. Implementation report-Prototype#4 Final. D3.2.4 », J.ENRIQUEZ-GABEIRAS, M.A.CALLEJO RODRIGUEZ, S.F.RACARU L.CORDEIRO, S.F.RACARU

« Implementation report - Preliminary. D3.1.2 », E.ANGORI, G.MARTUFI, S.F.RACARU

« Implementation report. D3.1.3 », G.MARTUFI, E.ANGORI, L.CORDEIRO, S.F.RACARU, A.GIORGINI, Y.LIZZI, M.A.CALLEJO RODRIGUEZ

« EuQoS system demonstrations report for phase 2. D5.2.4 », O.DUGEON, J.ENRIQUEZ-GABEIRAS, M.A.CALLEJO RODRIGUEZ, M.BROGLE, L.BARESSE, J.SLIWINSKI, L.BISTI, S.F.RACARU, R.SERRAL-GRACIA, J.DOMINGO-PASCUAL, J.PONTE, J.CARAPINHA

« EuQoS standardization summary. D6.1.4 », L.DAIRAINE, M.DIAZ, S.F.RACARU, C.CHASSOT, J.LACAN, J.CANTILLO

« System design: functions, interfaces and API specification », E.ANGORI, G.MARTUFI, S.F.RACARU, M.DIAZ

« Testbed integration test plan release 2 », F.J.R.SALGUERO, P.A.ARANDA GUTIERREZ, P.OWEZARSKI, S.F.RACARU, R.SERRAL-GRACIA, J.DOMINGO-PASCUAL, P.CAPELLA, M.DABROWSKI, J.SLIWINSKI, M.BROGLE, D.MILIC, Z.KOPERTOWSKI, L.CORDEIRO, A.GEBREHIWOT, M.SOMMANI, M.OBUCHOWICZ, A.FLIZIKOWSKI, K.BRONARSKI, P.CABAN, S.TKACZ, J.CARAPINHA, R.ROMERO SAN MARTIN

« EuQoS software installation manual », M.CARUSIO, L.CORDEIRO, S.F.RACARU, G.MARTUFI, E.ANGORI, A.GIORGINI, Y.LIZZI, M.A.CALLEJO RODRIGUEZ, F.J.R.SALGUERO, G.G.DE BLAS, I.FRESNO, G.MASSARI, I.JAHNICH, M.DITZE, J.SLIWINSKI, A.BEBEN, E.MINGOZZI, L.BISTI, S.ARDON, E.DI SANTO, G.SANTORO, O.DUGEON, N.CARAPETO

« EuQoS QSPEC template (EQ-QSPEC). QoS parameter specification to be transported by the signaling protocol », S.F.RACARU, O.DUGEON, M.DIAZ

« EuQoS standardization summary », L.DAIRAINE, M.DIAZ, S.F.RACARU, C.CHASSOT, J.LACAN, J.CANTILLO, F.BOAVIDA, L.CORDEIRO, M.CURADO, E.MONTEIRO, O.DUGEON, E.LOCHIN, G.JOURJON, D.MORRIS, J.GABEIRAS

« Testbed integration test plan », O.DUGEON, F.J.R.SALGUERO, P.A.ARANDA GUTIERREZ, P.OWEZARSKI, S.F.RACARU, G.AURIOL, N.LARRIEU, R.SERRAL-GRACIA, J.DOMINGO-PASCUAL, P.CAPELLA, M.DABROWSKI, J.SLIWINSKI, M.BROGLE, D.MILIC, Z.KOPERTOWSKI, L.CORDEIRO, A.GEBREHIWOT, M.SOMMANI, M.OBUCHOWICZ, A.FLIZIKOWSKI, K.BRONARSKI, P.CABAN, S.TKACZ, R.ROMERO SAN MARTIN

« Trial report », O.DUGEON, F.J.R.SALGUERO, M.A.CALLEJO RODRIGUEZ, G.GARCIA DE BLAS, P.OWEZARSKI, S.F.RACARU, R.SERRAL-GRACIA, J.DOMINGO-PASCUAL, L.JAKAB, P.CAPELLA, M.DABROWSKI, J.SLIWINSKI, M.BROGLE, D.MILIC, Z.KOPERTOWSKI, T.CISZKOWSKI, L.CORDEIRO, A.GEBREHIWOT, M.SOMMANI, M.OBUCHOWICZ, D.WEDRYCHOWICZ, E.M.SILVA, R.ROMERO SAN MARTIN

« Deploying the monitoring and measurement system in testbeds », P.OWEZARSKI, S.F.RACARU, M.DABROWSKI, A.BEBEN, J.SLIWINSKI, D.DUDA, R.SERRAL-GRACIA, L.JAKAB, J.DOMINGO-PASCUAL, G.GARCIA DE BLAS, A.GEBREHIWOT, K.BRONARSKI, M.BROGLE, D.MILIC, T.CISZKOWSKI, J.KOWALCZYK, E.M.SILVA, I.BORGES

« First individual based EuQoS system test report », M.DABROWSKI, D.MILIC, M.BROGLE, J.B.ALVAREZ, H.D.MANAIA, P.OWEZARSKI, S.F.RACARU, R.SERRAL-GRACIA, A.PINIZZOTTO, M.CARMO, C.TOMASZ, K.BONARSKI

« Connectivity and performance tests report for local and pan-European (across GEANT) testbed design for the Trial », P.OWEZARSKI, S.F.RACARU, G.AURIOL, N.LARRIEU

« Connectivity and performance tests report for local and pan-European (across GEANT) testbed design for the trial », P.OWEZARSKI, S.F.RACARU, G.AURIOL, N.LARRIEU

« Technical requirements for the trial, tasks and scheduling. P.OWEZARSKI, S.F.RACARU, G.AURIOL, N.LARRIEU

Autres

« Proposition d'architecture pour la maîtrise de la QoS de bout en bout dans un environnement IP DiffServ multi-domaine » (Rapport LAAS n°04719), G.AURIOL, S.F.RACARU, C.CHASSOT

« Dynamic Service Composition over Heterogeneous Networks », (Rapport LAAS n°08278), S.F.RACARU, N.VAN WAMBEKE, C.CHASSOT, M.DIAZ. Submitted to DSOM08.

« Dynamic end-to-end QoS provisioning over heterogeneous networks », (Rapport LAAS n°08064), S.F.RACARU, C.CHASSOT, N.VAN WAMBEKE, M.DIAZ

« Composition de services IP dans l'internet DiffServ multi-domaine », (Rapport LAAS n°06361), S.F.RACARU, C.CHASSOT, A.LOZES, M.DIAZ

« SLS-aware and BGP-based signaling architecture for multimedia applications », (Rapport LAAS n°05299), G.AURIOL, C.CHASSOT, M.DIAZ, S.F.RACARU

AUTEUR : Stelian Florin RACARU

TITRE : Conception et validation d'une architecture de signalisation pour la garantie de qualité de service dans l'Internet multi-domaine, multi-technologie et multi-service

DIRECTEUR DE THESE : Michel DIAZ et Christophe CHASSOT

LIEU ET DATE DE SOUTENANCE : LAAS-CNRS, Salle Europe, le 14 octobre 2008

RESUME

Depuis quelques années, les évolutions technologiques conjointes de l'informatique et des télécommunications ont conduit à une modification substantielle des communications et des réseaux. Une des conséquences de ces progrès est la convergence vers une infrastructure unique de transfert de données. Porté par son développement continu, l'Internet (IP) se révèle comme solution pour l'interconnexion des différentes technologies hétérogènes, petite ou grande distance, fixe ou mobiles, l'infrastructure globale pour tout type de communication. De ce contexte résulte la problématique générale de nos travaux qui est de définir et de mettre en œuvre des nouveaux mécanismes, protocoles et architectures pour répondre aux besoins des applications émergentes. Nos contributions s'inscrivent dans ce thème de la maîtrise de la garantie de la Qualité de Service (QoS) de bout en bout dans un environnement Internet hétérogène à plusieurs niveaux : multi domaine, multi technologie et multi service. Nous adressons le besoin des nouvelles architectures en signalisation inter domaine couplée au provisionnement et au contrôle d'admission pour répondre aux besoins du trafic et des services actuels. Dans ce cadre, nous avons participé à la conception, l'implémentation, le déploiement et la validation de l'architecture du projet européen IST EuQoS (« End-to-end Quality of Service support over heterogeneous networks »).

MOTS CLE : Qualité de service, signalisation, architecture, Internet hétérogène

---

Conception and validation of a signalling architecture for Quality of Service guarantees over the multi-domain, multi-technology and multi-service Internet

Abstract

During the last years, computer science and telecommunications joint technological evolutions led to a perspective change in the area of communications and networks. One of the consequences of this progress is the convergence towards a sole infrastructure for data exchange. Due to its continuous development, Internet (IP) appears as the solution for interconnecting different heterogeneous technologies, short or long distance, fixe or mobile, the global infrastructure for communication transport. Internet supports many new types of applications: dynamic, multimedia, real time, distributed, potentially multi-user, mobile, such as voice over IP (VoIP), video on demand (VoD), visio conference, interactive games, etc. The general concerns addressed by our work result from this context. Our objective is to define and implement new mechanisms, protocols and architectures to answer the needs of emergent applications. Our proposals contribute to mastering the end-to-end Quality of Service (QoS) in a multi-level heterogeneous environment, by addressing the current need of inter-domain signalling coupled with provisioning and admission control, to meet the traffic requirements. In this context, we participated in the design, development, deployment and validation of the architecture defined within the European project IST EuQoS ("End-to-end Quality of Service support over heterogeneous networks").

KYWORDS: Quality of Service, signalling, architecture, heterogeneous Internet

---

DISCIPLINE ADMINISTRATIVE : Informatique et Télécommunications

LAAS CNRS - 7 avenue du Colonel Roche - 31077 Toulouse Cedex 4