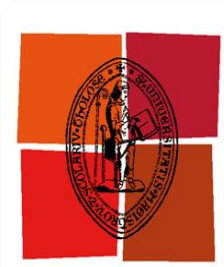
Architectures réseaux pour le partage de contenus multimédias avec garantie de qualité de service

Mohamed Mahdi



Université de Toulouse

THÈSE

En vue de l'obtention du

DOCTORAT DE L'UNIVERSITÉ DE TOULOUSE

Délivré par :
Université Toulouse III Paul Sabatier (UT3 Paul Sabatier)

Discipline ou spécialité :

Systèmes Informatiques Critiques

Présentée et soutenue par :
Mohamed MAHDI

le : mercredi 16 novembre 2011

Titre :

Architectures réseaux pour le partage de contenus multimédias avec garantie de qualité de service

---

Ecole doctorale :
Systèmes (EDSYS)

Unité de recherche :
Laboratoire d'Analyse et d'Architecture des Systèmes

Directeur(s) de Thèse :

Michel DIAZ & Olivier DUGEON

Rapporteurs :

M. Jean-Jacques Pansiot
Mme. Ana Rosa Cavalli

Membre(s) du jury :

M. Abdelhamid Mellouk - Examinateur
Mme. Béatrice Paillassa - Examinatrice
M. Thierry Gayraud - Examinateur
M. Christophe Chassot - Invité

Remerciements

Les travaux présentés dans ce mémoire ont été effectués au Laboratoire d'Orange Labs à Lannion, dirigés par Monsieur Olivier DUGEON, Ingénieur de recherche, à qui je souhaite exprimer mes remerciements.

Je tiens également à remercier Monsieur Michel DIAZ, mon Directeur de thèse, pour sa confiance et ses encouragements continus tout au long de ces trois années. Je le remercie également pour ses remarques pertinentes sur mon travail et sa relecture de ce mémoire.

Dans le contexte de mes travaux de recherche, j'ai eu des discussions enrichissantes avec plusieurs collègues d'Orange Labs ; qu'ils en soient grandement remerciés.

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

- Jean-Jacques Pansiot, Professeur à LSIIT à l'Université de Strasbourg,
- Ana Rosa Cavalli, Professeur à l'INSTITUT TELECOM/ TELECOM SudParis,
- Abdelhamid MELLOUK, Professeur à l'Université de Paris 12,
- Olivier DUGEON, Ingénieur de Recherche 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
- Béatrice Paillassa, Professeur à l'Institut National Polytechnique deToulouse,
- Thierry Gayraud, Maître de Conférences à l'Université Paul Sabatier - Toulouse III.

Finalement, je remercie mes parents, mes frères et mes sœurs pour leur affection qui m'a été extrêmement précieuse durant cette expérience.

Table des matières

Chapitre 5 Conclusion et perspectives

Table des figures

Liste des tableaux

Chapitre 1

Introduction Générale

Sommaire

1.1 Contexte de recherche

Aujourd'hui, les équipements multimédias sont de plus en plus nombreux dans les réseaux domestiques. Ils supportent de plus en plus les technologies UPnP [1] et DLNA [2] permettant à l'utilisateur de partager aisément (i.e. de façon Plug'n Play) ses contenus multimédias entre ses différents équipements (i.e. partage de photos entre une console de jeux comme la PS3 et un téléphone mobile comme le iPhone). Le besoin d'étendre le partage de contenus à des échanges inter-réseaux domestiques, et ce de manière simple est également présent.. En effet, l'évolution de la société a donné naissance à des familles géographiquement dispersées qui maintiennent le lien familial via l'utilisation de technologies de communication performantes. Par exemple, les utilisateurs recourent, pour partager leurs expériences personnelles, à échanger leurs fichiers multimédia (photo, vidéo, musique). Plusieurs services sont proposés actuellement notamment à partir de service web (DailyMotion, Facebook, Youtube, Weezo…) ou de service «peer-to-peer » (BitTorrent, Emule,..). Cependant, ces services présentent plusieurs lacunes surtout au niveau de la sécurité, de la confidentialité des fichiers partagés ainsi que de la qualité de service (QoS) proposée au client.

La thèse s'inscrit dans le cadre du projet collaboratif Celtic Feel@Home qui a pour mission d'étudier et de maquetter un nouveau service de partage de contenus multimédias. Ce service est basé sur la notion de communauté d'utilisateurs représentant un groupe d'utilisateurs. Il s'agit pour un client de gérer aisément, comme il le fait avec un logiciel de messagerie instantanée, ses réseaux sociaux (famille, amis, associatif, …) afin de pourvoir partager aisément des contenus multimédias directement au sein de ses communautés sans être obligé de déposer ses contenus sur un serveur externe. Il s'agit également de pouvoir accéder à ses propres contenus multimédias présents dans son réseau domestique depuis son téléphone mobile ou en situation de nomadisme. Les contenus sont ainsi ré-internalisés chez le client et non pas mis à disposition sur des serveurs de contenus centralisés. Le service de partage de contenus, visé par ce projet, suppose une mise en place des ressources réseaux (adressage, routage, acheminement, bande passante, authentification, sécurisation, protection, …) nécessaires au bon acheminement des données afin de garantir une qualité de service optimale.

1.2 Problématique

La thèse se propose d'étudier l'architecture du plan de contrôle du réseau nécessaire pour réaliser le service de partage de contenus multimédias étudié dans le projet Feel@Home. L'offre réseau permettra de proposer un service de partage de contenus multimédia, entre les réseaux domestiques des utilisateurs, simple et ce depuis n'importe quels équipements de la sphère domestique, comme le montre la Figure 1.1. Le service étudié dans Feel@Home se propose d'être transparent aux technologies utilisées par les clients notamment les technologies UPnP A/V et DLNA afin de ne pas modifier leurs terminaux.

La thèse prendra en compte plusieurs contraintes et devra résoudre plusieurs verrous technologiques. Nous les avons groupés sur deux thématiques. La première consiste à établir une session sécurisée entre les équipements distants. La deuxième concerne la réservation de la QoS pour cette session afin de répondre aux exigences réseau du service de partage lors de l'envoi des contenus.

Les principaux défis posés par la mise en place de ces sessions sont:

- La définition des fonctions d'authentification, de sécurité et de confidentialité que le plan de contrôle doit offrir. En premier lieu, l'authentification des clients doit vérifier la gestion des droits à l'accès aux contenus partagés ; ensuite, les contenus des clients doivent être protégés dans le cas des communautés privés afin de respecter la vie privée et la confidentialité, …
- Le choix de la (des) technologie(s) (IMS, VPN, P2P, Multicast, …) la (les) mieux adaptée(s) à la gestion de plusieurs millions de communautés privées : il faut à la fois

résoudre les problèmes d'adressage réseau, de gestion des profils et de configuration de la QoS.

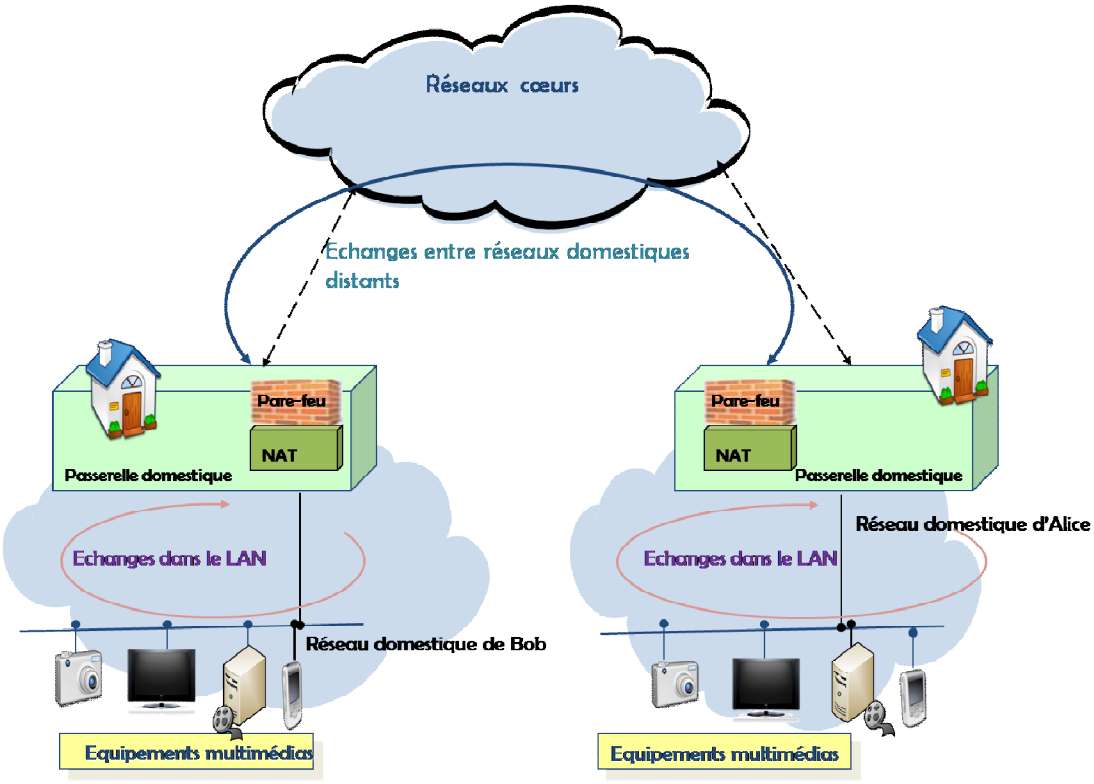


Figure 1.1 Cadre de travail

Afin d'offrir de la QoS aux sessions établies par le service de partage il faudra définir :

- Les mécanismes de contrôle des ressources réseaux et de transport temps réel à utiliser, aussi bien dans les réseaux domestiques que dans les réseaux cœurs (réseaux longues distances interconnectant les réseaux domestiques): le partage de contenus multimédias peut nécessiter beaucoup de ressources réseaux (ex. diffusion d'un film issue d'un caméscope) qu'il faudra contrôler et configurer au mieux en fonction des disponibilités du réseau et cela de façon transparente pour le client. La qualité de service perçue par le client (QoE) et la qualité de service côté réseau (QoS) devront ainsi être prises en compte dans le choix des mécanismes réseaux à mettre en œuvre ;
- Une solution pour offrir une QoS de bout en bout. Par le terme de bout en bout, nous voulons dire le fait d'offrir une garantie de QoS dans les réseaux domestiques des deux clients (émetteur et récepteur) et dans les réseaux cœurs. Cela nécessite un couplage entre les mécanismes de QoS choisis à mettre en place dans les réseaux des clients et ceux déployés dans les réseaux cœurs.

1.3 Contributions de la thèse

Les travaux de cette thèse ont conduit à la conception, l'implémentation et la validation d'un système de session à la demande qui répond aux contraintes exprimées par le service de partage de contenus à distance spécifié dans le projet Feel@Home. Nous avons décomposé ce système en deux sous systèmes : le premier traitera la problématique d'accès à distance entre les réseaux domestiques; le deuxième proposera une solution de gestion de QoS de bout en bout pour les sessions établies par le premier sous système.

Les principaux axes de nos contributions portent sur :

- La conception d'une architecture fonctionnelle générique pour le sous système d'accès à distance;
- La proposition de deux déclinaisons techniques possibles de ce sous système. Nous avons choisi d'implémenter une seule déclinaison que nous avons intégrée dans la maquette du service du projet Feel@Home. Pour la deuxième déclinaison nous nous sommes contentés d'une simulation pour valider le bien fondé de cette solution ;
- La réalisation d'une étude de performances de nos propositions pour s'assurer de l'aptitude de notre système à passer à l'échelle ;
- La proposition d'une solution permettant au sous système d'accès à distance de réserver de la QoS de bout en bout pour ses sessions ;
- L'intégration du système de session à la demande dans l'architecture globale proposée dans le cadre du projet Feel@Home.

1.4 Organisation du manuscrit

En conséquence, la thèse s'articule autour de trois chapitres :

Le chapitre 2 est consacré à l'état de l'art concernant les deux problématiques majeures auxquelles nous avons apportés des solutions, à savoir l'accès à distance pour le partage de contenus et la gestion de QoS de bout en bout.

Dans une première partie, nous présentons les technologies de partage de contenus dans les réseaux domestiques, sur lesquels nous nous sommes basés en les étendant afin d'offrir un service de partage à distance. Nous étudions par la suite les architectures réseaux d'accès à distance standardisées, utilisées pour le partage de contenus. Dans la deuxième partie de ce chapitre, nous présentons les principales techniques de gestion de QoS dans les réseaux domestiques ainsi que dans les réseaux cœurs.

Le chapitre 3 sera dédié à la présentation du sous système d'accès à distance pour le partage de contenus. Nous présentons sa conception et nous expliquons les choix techniques que nous avons pris pour répondre aux contraintes exprimées par les services de partage de contenus. Nous exposons aussi l'apport de notre solution au niveau du projet Feel@Home.

Sur la base du bilan des techniques de QoS présenté dans le chapitre de l'état de l'art, nous proposons dans le chapitre 4 une étude de la problématique de la gestion de QoS de bout en bout. Nous débutons ce chapitre en présentant les techniques qui correspondent le mieux aux besoins de notre système, que ce soit au niveau des réseaux domestiques ou dans les réseaux cœurs. Ensuite, nous proposons des solutions pour coupler les techniques de QoS déployées dans les différentes portions du chemin des données (réseaux domestiques & réseaux cœurs) afin de synchroniser la gestion des ressources et rendre cohérent la garantie de QoS de bout en bout.

Le chapitre 5 conclura ce mémoire par un résumé de nos contributions. Finalement, nous clôturons ce travail par présenter les perspectives de travaux futurs qui découlent de nos propositions.

Chapitre 2

Le partage de contenus à distance

Sommaire

2.1 Introduction

Dans ce chapitre, nous présentons le concept d'un service de partage de contenus multimédias à distance. Nous avons identifié deux principaux défis pour réaliser un tel service, à savoir :

i. la mise en relation réseaux entre les terminaux distants ;
ii. la réservation des ressources réseaux nécessaire pour l'échange des contenus multimédias qui sont généralement volumineux.

La première partie de ce chapitre expose l'état de l'art des principales solutions offertes par les technologies actuelles (WEB, P2P, IMS, VPN) qui permettent le partage de contenus multimédias à distance.

Dans une deuxième partie, nous traitons la problématique de la gestion de la qualité de service (QoS). Nous allons présenter dans cette partie les principaux protocoles qui permettent de fournir une garantie de QoS, que ce soit dans les réseaux Locaux (Local Area Network LAN) ou dans les réseaux d'opérateurs, afin d'avoir les outils nécessaires pour concevoir un service qui offre de la QoS de bout en bout.

2.2 Partage de contenus multimédias dans les réseaux locaux

Souvent les techniques de partage à distance tentent de reprendre des technologies utilisées à l'intérieur des réseaux locaux pour les adapter à la problématique de partage de contenus à distance. Donc, pour bien comprendre ces solutions, nous allons exposer dans cette section les technologies les plus utilisées dans le contexte des réseaux locaux, à savoir UPnP A/V (Universal Plug and Play Audio Video) et DLNA (Digital Living Network Alliance).

Mais, tout à d'abord nous allons commencer par expliquer les contraintes liées au partage de contenus dans un tel contexte.

2.2.1 Contraintes du partage de contenus dans les réseaux locaux

Les réseaux locaux IP actuels (domestiques et d'entreprises) interconnectent divers terminaux électroniques : ordinateurs, imprimantes, téléviseurs, appareils photo, mobiles…Dans ce cadre, les utilisateurs ont exprimé de nouveaux besoins tels que :

- afficher un contenu vidéo/audio stocké dans un serveur média sur le téléviseur ;
- lancer des impressions à partir de son appareil photo ;
- contrôler les appareils de son réseau domestique avec une commande universelle ou avec un téléphone mobile.
- …

Le challenge majeur de tous ces scénarii0 est l'interopérabilité entre les différents types d'équipements, tant au niveau logiciel (i.e. système d'exploitation) que matériel (mac, pc, appareil photo…). L'Universal Plug'n Play forum (UPnP forum) a été créé pour proposer des protocoles pour ces scénarii qui s'affranchissent de l'obstacle de l'interopérabilité.

2.2.2 UPnP

2.2.2.1 UPnP Forum

Ce forum a formé plusieurs groupes de travails pour proposer des spécifications pour les principaux scénarii exprimés par les utilisateurs des réseaux locaux. Cependant, tous les groupes de travail se basent sur une spécification commune, l'UPnP Device Architecture [3], qui définit le fonctionnement et l'architecture réseau des protocoles promulgués par le forum UPnP.

La standardisation du protocole de base d'UPnP l'a distingué comme « *le premier standard international pour l'interopérabilité des appareils sur les réseaux IP* ». En effet, ce standard permet la communication pair-à-pair de périphériques réseaux. Il s'appuie sur le protocole HTTP. Cela lui permet une réelle indépendance vis-à-vis du système d'exploitation et du type des réseaux (Wifi, Ethernet…).

2.2.2.2 Notions de bases des protocoles UPnP

Les principaux concepts de l'architecture UPnP sont basés sur la notion de périphérique (*device*) et de service.

Les périphériques (devices)

Un *device* est un dispositif qui offre un ou plusieurs services. Le service est l'unité de contrôle la plus élémentaire. Elle propose des actions et elle est décrite par des variables d'états. Il existe deux types de *devices* :

- *Controled Device* ou *Device* : ce dispositif offre un ensemble de services aux équipements connectés au réseau. Il peut aussi embarquer une liste de *devices* logiques qui eux-mêmes offrent leurs propres services;
- *Control Point* : ce dispositif est chargé de mettre en relation les *devices* UPnP. Pour ce faire, il utilise les services annoncés par les *devices*. Il peut être embarqué dans un *device* ou bien dans un équipement à part.

L'UPnP *device* est installé sur un équipement proposant des ressources. Il offre des services utilisables par le point de contrôle. Ainsi, le *device* doit annoncer les services qu'il peut offrir. Ces informations sont mises en forme via le langage XML. Le point de contrôle peut récupérer la description des services via une simple requête HTTP GET. Ce mécanisme est possible grâce au mini serveur Web embarqué dans les équipements UPnP.

Service

Un service se compose d'un ensemble d'actions agissant sur des variables d'état. Ces services utilisent le principe de souscription. Ainsi, un point de contrôle ayant souscrit à un service est notifié de tous les changements des variables d'état. Une fois la souscription réalisée, le service enverra à tous ses souscripteurs les modifications que subit son état. A l'instar du *device*, chaque service doit communiquer sa description au format XML.

La Figure 2.1 représente l'organisation d'un UPnP *device*.

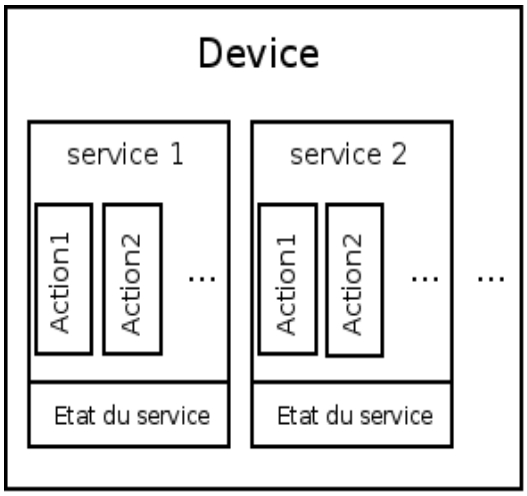


Figure 2.1: Organisation d'un *device* UPnP

Les points de contrôles (Control Points)

Ce composant est plus simple que le device. Il ne contient pas de services. Il est chargé de souscrire aux services des *devices* qui l'intéressent. Les services diffusant régulièrement les changements d'état qu'ils subissent, le point de contrôle se contente de réagir à ces informations ou de provoquer les changements d'états.

2.2.2.3 Fonctionnement général du protocole UPnP

La communication entre les *devices* et les points de contrôles se fait en six étapes. Nous allons les détailler une par une.

L'adressage

Cette étape permet aux composants UPnP d'obtenir une adresse IP. Par défaut, la découverte de la configuration réseau se fait via un client DHCP [4]. En cas d'échec, le composant utilise le mécanisme « automatique IP » (mécanisme qui retourne une adresse IP arbitraire). Une fois que le composant dispose d'une adresse IP valide, il entame la phase de découverte.

La découverte

Cette procédure est basée sur le protocole SSDP[1] (Simple Service Discovery Protocol) [5] qui utilise le mode de diffusion multicast sur l'adresse 239.255.255.250 pour échanger ses messages. Elle diffère cependant entre un *device* et un point de contrôle.

Lorsqu'un nouveau *device* s'attache au réseau, il envoie des messages d'annonce en multicast (SSDP NOTIFY). Ces messages décrivent les informations essentielles concernant le *device*, à savoir son type, son identifiant et un pointeur (URL) vers le fichier XML contenant la description détaillée du *device*. De plus, tous les services et *devices* embarqués dans ce nouveau *device* envoient des annonces pour décrire leurs aptitudes respectives.

Afin de savoir quels sont les *devices* disponibles dans le réseau, tous les points de contrôle peuvent écouter l'adresse multicast (239.255.255.250) sur le port standard (1900) que les *devices* utilisent pour envoyer leurs annonces. Sinon, les points de contrôle peuvent envoyer en *broadcast* des messages SSDP de recherche (M-SEARCH) pour obliger les *devices* à envoyer leurs annonces.

La description

Après l'étape de découverte, le point de contrôle ne connaît que des informations très limitées sur les *devices* et les services disponibles dans le réseau. Pour apprendre plus de détails concernant leurs aptitudes, le point de contrôle doit récupérer le fichier de description du *device* ou du service depuis l'URL indiqué dans le message d'annonce envoyé pendant la phase de découverte. Une requête HTTP GET est envoyée à cet effet. La réponse à cette requête sera formulée par le serveur web embarqué dans le *device*.

Le fichier de description d'un *device* contient des informations sur le constructeur, des définitions de tous les *devices* embarqués, l'URL du fichier de présentation du *device*, et une énumération de tous les services supportés et leurs URLs de contrôles.

Le fichier décrivant un service expose les informations concernant ses actions (nom, arguments d'entrée, arguments de sortie) et ses variables d'état.

[1] Une spécification de l'IETF implémentant un mécanisme de découverte via du multicast

Le contrôle

Une fois que le point de contrôle connaît toutes les informations nécessaires sur les *devices* et leurs services, il peut les contrôler. L'interaction avec les services se fait via des requêtes SOAP (Simple Object Access Control) [6] envoyées à l'URL de contrôle du service. La requête permet la réalisation d'une action du service.

A la fin de l'action, le point de contrôle reçoit le résultat de l'action. Ce résultat peut être un code d'erreur ou les nouvelles valeurs des variables d'état du service.

La notification d'événements

L'état du service est représenté par la valeur de ses variables d'état. Ainsi, lorsqu'une de ces variables change, le service publie la mise à jour à ses souscripteurs. Les points de contrôle qui souhaitent être tenus au courant de ces modifications doivent s'abonner au service.

Ce système de notification utilise la technique GENA [7] (General Event Notification Architecture).

La présentation

Si le *device* met à disposition une page de présentation, l'utilisateur peut la parcourir avec un navigateur internet. L'URL de cette page est déclarée dans le fichier de description du *device*. Elle permet à l'utilisateur de visualiser l'état du *device* et éventuellement de le contrôler.

Pour récapituler cette partie, la Figure 2.2 résume les six phases d'interaction entre un point de contrôle et un *device*.

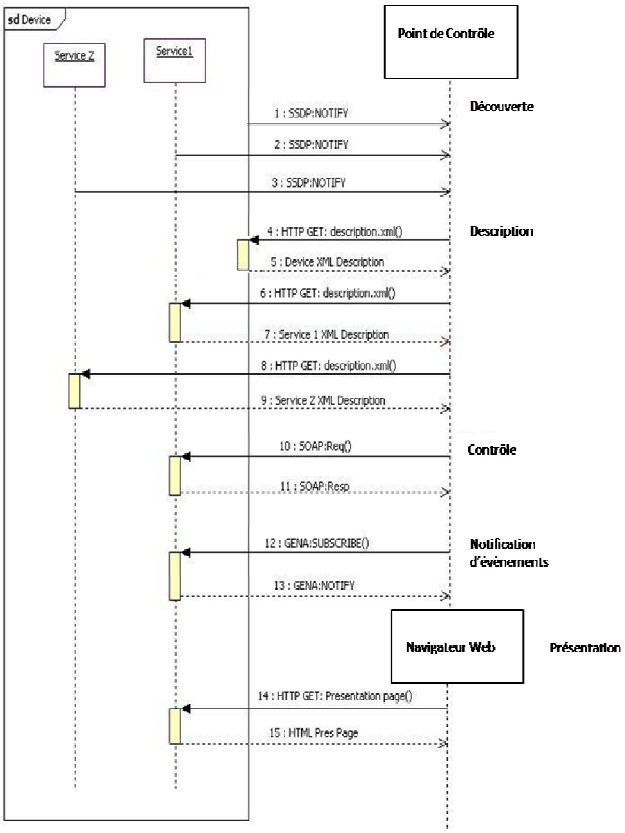


Figure 2.2 Interaction entre *device* et point de contrôle

2.2.2.4 Spécifications UPnP

Sur la base de cette architecture générique, plusieurs groupes de travail dans le Forum UPnP ont spécifié de nouveaux services en définissant des *devices* ou/et des services dédiés au contexte traité. Leurs spécifications sont :

- UPnP A/V: traite le contexte de partage de contenus multimédias dans les réseaux domestiques;
- UPnP QoS : traite la gestion de la QoS dans les réseaux domestiques;
- UPnP RA: traite la problématique réseau de l'accès à distance ;
- UPnP IGD: définit un service de configuration des paramètres de la passerelle réseau des réseaux domestiques (Home Gateway HGW).

Dans ce chapitre, nous allons détailler les trois spécifications qui sont en relations avec nos travaux: UPnP A/V, UPnP QoS et UPnP RA.

2.2.3 UPnP Audio Video (A/V)

Pour traiter la problématique de partage de contenus multimédias dans les réseaux locaux, le Forum UPnP a créé le groupe de travail UPnP A/V. Ce dernier propose une spécification permettant la mise en relation de plusieurs équipements multimédias pour échanger des contenus (audio, vidéo ou photo). Deux *devices* ont été définis: Media Server et Media Renderer. De même, le fonctionnement du point de contrôle a été aussi détaillé dans le cadre ce service.

La Figure 2.3 représente l'architecture d'UPnP A/V. Elle se veut indépendante des formats utilisés par les *devices* et des protocoles choisis pour véhiculer le contenu multimédia. Cependant, cette architecture ne fonctionne qu'au sein d'un même réseau IP.

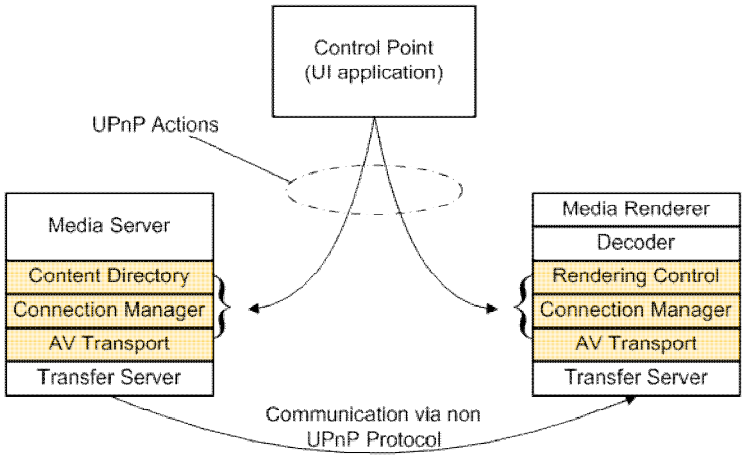


Figure 2.3 UPnP A/V Architecture

Media server

Ce *device* met à disposition les contenus multimédias. Il doit implémenter les services suivants:

- Content Directory Service (CDS) : Il offre au point de contrôle A/V toutes les actions nécessaires pour obtenir des informations sur les contenus que le Media Serveur partage dans le réseau. En utilisant ce service, le point de contrôle A/V va connaître les méta-informations concernant chaque contenu comme le titre, la taille, la date de création, etc. En plus de ces informations, le point de contrôle A/V peut connaître les protocoles de transport et les formats que le Media Serveur supporte, pour un contenu donné.
- Connection Manager Service (CMS) : Il met à disposition les actions nécessaires à l'établissement et au suivi du transfert du contenu choisi.

- AVTransport Service (AVTS) : C'est un service optionnel. Il fournit des actions pour la lecture évoluée de contenu et la gestion de transferts multiples (ex. avance / retour rapide, pause, … lors de la lecture d'un contenu multimédia).

Nous trouvons notamment ce type de *device* sur les disques durs multimédias équipés de connectivité réseau ou sur certains logiciels permettant la transformation d'un ordinateur en serveur multimédia.

Media Render

Ce *device* contient le lecteur de contenu. Il doit implémenter les services suivants:

- Connection Manager Service (CMS) : Il offre les mêmes fonctionnalités que le service CMS du *Media Server*. En effet, il permet surtout au point de contrôle A/V de connaître les protocoles de transports et les formats de fichiers que supporte le *Media Renderer*. Et par conséquent, le point de contrôle sait s'il pourra lire le contenu choisi.
- Rendering Control Service (RCS) : Il offre au point de contrôle A/V toutes les actions nécessaires au réglage des paramètres de lecture du média, tel que le volume du son, le contraste…
- AVTransport Service (AVTS) : C'est un service optionnel. Il fournit les mêmes actions que le service du *Media Server* de même nom.

Point de contrôle A/V

La spécification UPnP A/V définit deux modèles : le modèle « à trois boites » illustré dans la Figure 2.4 et le modèle « à deux boites ». Dans le modèle « à trois boites » le point de contrôle A/V se situe dans un équipement distinct de celui du *Media Server* et du *Media Renderer*. Alors que dans le modèle à « deux boites » le point de contrôle A/V est embarqué dans un *device,* que ce soit un *Media Server* ou un *Media Renderer*. Lorsqu'il est implémenté dans le *Media Renderer* on parle alors de *Media Player*.

Indépendamment du modèle, le fonctionnement du point de control A/V est le même. Dans un premier temps, il se charge de découvrir les *devices* multimédias dans le réseau, conformément à la procédure définie dans la spécification UPnP Device Architecture (étapes 1-2). Ensuite, il va obtenir les protocoles de transfert utilisables par les *devices* souhaitant échanger des contenus (Media server & Media Renderer) afin de choisir un protocole commun entre eux (étapes 3-4). Il prépare après la communication entre les deux entités (étapes 5-12). Pour cela, il va régler le média, le protocole et les paramètres de transfert à utiliser. A la fin du transfert, il va fermer les connexions entre les deux entités (étapes 13-14).

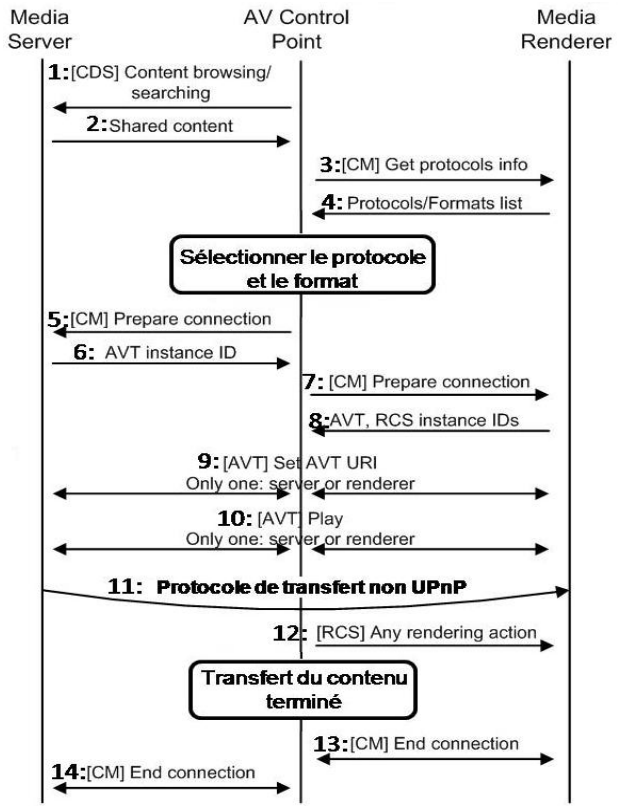


Figure 2.4 Interactions entre point de control, media Server et Renderer dans le modèle trois boîte

2.2.4 DLNA

Les industriels qui voulaient utiliser le standard UPnP A/V pour produire des équipements compatibles se sont vite rendu compte qu'il fallait se mettre d'accord sur les détails optionnels du standard et ceux laissés au choix du constructeur. Ils ont alors créé le consortium DLNA pour assurer une meilleure interopérabilité de leurs solutions que ce que la certification UPnP permet.

Ce consortium ne définit pas de nouveaux standards en tant que tel, mais reprend à son compte les standards UPnP A/V tout en fixant un cadre plus strict pour l'implémentation et la certification. En particulier, le consortium DLNA a élaboré des profils de partages qui, lorsqu'ils sont utilisés par des équipements DLNA, garantissent une excellente interopérabilité. Ces profils fixent les détails du standard UPnP A/V comme les codecs, les protocoles, l'encodage … Pour assurer ce haut niveau d'interopérabilité, le consortium a mis au point une certification très stricte basée sur une batterie de tests. Chaque équipement doit réussir tous les tests pour obtenir la certification DLNA. Donc, un utilisateur qui achète un produit certifié DLNA sera sûr qu'il peut se connecter avec les autres produits DLNA présents dans son LAN.

DLNA a fait la distinction entre les *devices* du réseau domestique et les *devices* mobiles. Cette différentiation est due aux capacités limitées des équipements mobiles. Cependant, les fonctionnalités sont les mêmes et concordent avec la spécification d'UPnP A/V.

Les *devices* DLNA du réseau domestique sont:

- Digital Media Server (DMS) ;
- Digital Media Player (DMP) ;
- Digital Media Renderer (DMR) ;

- Digital Media Controller (DMC);
- Digital Media Printer (DMPr).

Les *devices* DLNA mobiles sont :

- Mobile Digital Media Server (M-DMS);
- Mobile Digital Media Player (M-DMP);
- Mobile Digital Media Uploader (M-DMU);
- Mobile Digital Media Downloader (M-DMD);
- Mobile Digital Media Controller (M-DMC).

Dans le reste du mémoire, nous nous plaçons dans le cas le plus général, donc nous ne parlerons que d'UPnP A/V.

2.3 Partage de contenus à distance

Dans cette partie nous allons exposer les travaux de standardisation et de normalisation sur la problématique d'accès à distance.

2.3.1 Spécification et contraintes d'un service de partage à distance

Pour pouvoir juger les solutions actuelles de partage de contenus à distances, nous allons tout d'abord définir les caractéristiques que nous attendons d'un tel service:

- Offrir une connectivité sécurisée entre les terminaux distants qui s'échangent des contenus ;
- Garantir un certain niveau de QoS pour le transfert des contenus ;
- Résoudre le conflit d'adressage privé entre les réseaux domestiques;
- Résoudre la traversé des Pare-feux et des NAT (Network Address Translation) ;
- Assurer la confidentialité des contenus partagés.

Sécurité

Pour qu'un service de partage soit largement adopté, il doit assurer une sécurité forte. En effet, l'utilisateur, lorsqu'il échange des contenus concernant sa vie privée (photos et vidéos autoproduites), doit pouvoir contrôler à qui et dans quelles conditions il partage ses contenus. De plus, la connexion entre les terminaux distants doit se faire d'une manière sécurisée pour que la sécurité des réseaux domestiques ne soit pas compromise.

Garantie de la qualité de service

Les contenus multimédias autoproduits par les utilisateurs sont généralement volumineux. L'échange de ces contenus demande alors au service de partage d'assurer une protection des réseaux utilisés (réseau domestique, réseau d'opérateur) contre la surcharge et une configuration des équipements réseaux adéquate afin de répondre aux contraintes d'envoi de ces contenus.

Conflit d'adressage privé entre réseaux domestiques

En général, les réseaux domestiques des utilisateurs sont construits autour d'une passerelle domestique (Home Gateway HGW), surtout dans le cas des accès xDSL. Cet équipement permet de connecter le réseau local (Local Area Network LAN) à internet via le réseau de l'opérateur. L'adressage réseau utilisé dans les LANs appartient à des plages d'adresses privées non routables dans l'Internet public. Ainsi, les passerelles domestiques implémentent une fonction de translation d'adresses réseaux (Network Address Translation NAT) afin de faire correspondre les adresses privées des équipements dans le LAN avec l'adressage public utilisé à l'extérieur.

Si cette fonction NAT résout partiellement le problème de pénurie d'adressage IPv4, elle introduit un grand défi pour connecter deux réseaux LANs. En effet, dans le but de simplifier la gestion des passerelles domestiques, les opérateurs les configurent avec la même plage d'adressage privée pour tous leurs clients (ex. 192.168.1.0/24). Aussi, lorsque deux LANs sont connectés, par exemple avec un tunnel VPN (Virtuel Private Network), l'équipement qui veut récupérer un contenu du LAN visité ne pourra pas déterminer si l'équipement stockant le contenu est dans son LAN ou dans le LAN visité, vu que les deux LANs utilisent la même plage d'adresses. En plus, il y a une probabilité non nulle q'un conflit d'adressage existe si l'équipement du LAN visiteur utilise une adresse IP déjà attribuée à un autre équipement dans le LAN visité.

Traversé du Pare-feu & du NAT

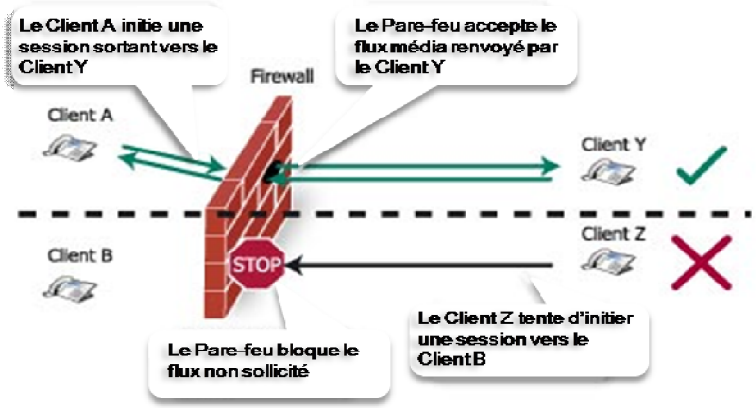


Figure 2.5 Problème de la traverse du Pare-feu

En connectant deux LANs distants, les messages échangés doivent traverser deux pare-feux et deux NAT. Un premier pare-feu se situe dans le LAN du visiteur et un deuxième dans le LAN à visiter. En effet, la sécurité des LAN repose principalement sur le pare-feu situé dans la passerelle domestique. Le fonctionnement d'un pare-feu consiste à refuser toute connexion entrante via un équipement externe du LAN si celle-ci n'a pas été préalablement initiée par un équipement du LAN. On peut bien sûr ajouter des exceptions sous la forme de règles dans le pare-feu autorisant un équipement externe (identifié par son adresse IP, par un numéro de port sur la passerelle domestique …) à accéder au LAN. De ce fait, le passage des messages du premier pare-feu ne causera pas de problème. Mais ajouter une règle dans le pare-feu du LAN visité pour accepter les requêtes de connexion venant du LAN visiteur constituera un défi de sécurité majeur. Il est toujours possible d'ajouter manuellement des règles statiques dans le pare-feu pour autoriser un utilisateur donné à accéder à un réseau différent du sien, mais cela engendre un trou dans la protection du réseau de l'utilisateur. Si cela peut-être acceptable pour un très petit nombre d'autorisations, cela devient ingérable pour un grand nombre d'utilisateurs visitant le LAN. De plus, l'allocation dynamique des adresses IP telle qu'elle est réalisée par les opérateurs pour les accès de type xDSL, rend la gestion des règles du pare-feu rapidement obsolète. Au final, l'utilisateur sera tenté d'ouvrir l'accès à son LAN sans contrôler qui lui rend visite. Cela revient à partir de chez soi en laissant la porte fermée, mais non verrouillée à clé. Les conséquences de cette faille peuvent être des attaques de déni de service, spoofing, etc.…

Une fois le Pare-feu passé, reste le problème de rediriger les messages vers le terminal qui héberge le contenu sollicité. La solution de la configuration statique peut être aussi envisagée, mais au prix d'une rigidité de l'accès ou d'une trop grande permissivité. Cela imposera par exemple à l'utilisateur de dédier un seul terminal comme serveur multimédia pour partager ses contenus avec les autres et de le localiser dans une zone dédiée (type DeMilatarized Zone – DMZ) pour éviter la compromission du reste du LAN ou des autres équipements.

Dans ce que suit, nous allons commencer par présenter l'architecture d'accès à distance réalisée dans le cadre du groupe de travail UPnP Remote Access (UPnP RA) et les travaux qui se sont inspirés de cette architecture. Nous passerons ensuite en revue les travaux proposés par l'organisme de standardisation HGI et pour finir nous exposerons les solutions de partages de contenus offertes dans le monde du Web et par les Frameworks pair-à-pair (P2P).

2.3.2 Solution UPnP RA

Le groupe de travail UPnP Remote Access (UPnP RA) a été créé par le forum UPnP pour étudier un service d'accès à distance [8]. Les deux principaux scénarii traités sont : le scénario permettant à un utilisateur de se connecter à son propre LAN dans une situation de nomadisme, le second traitant l'interconnexion des LANs. Pour les deux scénarii, l'interaction des *devices* distants avec ceux du LAN visité se doit d'être similaire à celle des *devices* connectés au même LAN.
La Figure 2.6 représente les principaux composants de l'architecture UPnP RA. Elle se base sur la mise en place d'un tunnel de transport sécurisé entre les équipements distants (tunnel IPSEC, TLS, ..). Dans cette architecture, deux nouvelles notions ont été introduites, le Remote Access Client (RAC) qui est l'équipement physique qui initie l'appel vers le LAN distant et le Remote Access Server (RAS) qui est l'équipement physique qui reçoit les appels de l'extérieur. Les *devices* en commun entre ces deux équipements sont :

- le Remote Access Transport Agent (RATA) : son rôle est d'établir une communication sécurisée entre les deux équipements.
- le Remote Access Discovery Agent (RADA) : son rôle est de permettre aux deux extrémités du tunnel de connaître les *devices* accessibles de l'autre côté. En effet, les *devices* RADA se synchronisent (RADASync service) pour que le *device* distant soit annoncé dans le LAN visité et que ce dernier connaisse les *devices* qu'il peut utiliser dans le LAN.

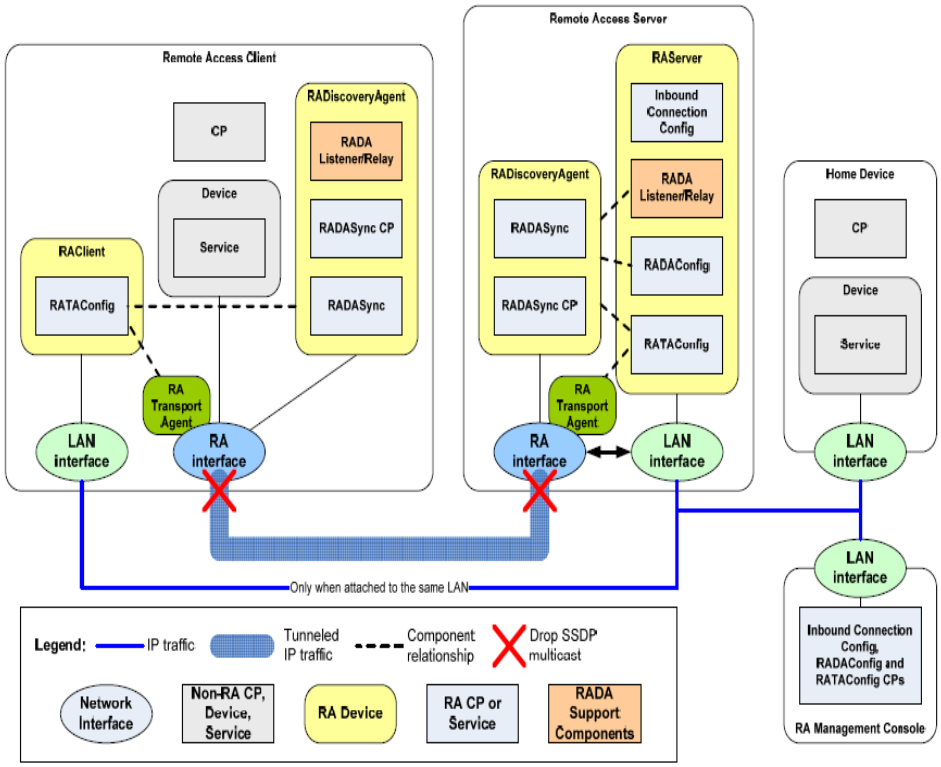


Figure 2.6 UPnP RA Architecture [5]

En plus de ces *devices* en commun, chacun des RAS et RAC implémente un *device* spécifique :

- le *device* RAClient [9] : permet essentiellement de configurer les *credentials* nécessaires pour authentifier l'équipement lors de sa connexion au LAN depuis l'extérieur, en utilisant le service RATAConfig ;
- le *device* RAServer [10]: Ce *device* UPnP permet principalement à l'utilisateur, grâce au service RADAConfig, de configurer la liste des Remote Access Client qui peuvent accéder au LAN et la liste des *devices* accessibles de l'extérieur. En plus, comme pour le RAClient, le service RATAConfig permet la configuration des *crédentials* nécessaires à l'établissement des tunnels sécurisés.

Cette architecture constituait une base solide pour plusieurs travaux traitant des services de partage de contenus à distance. Cependant, la solution proposée offre une sécurisation rigide en imposant aux *devices,* souhaitant se connecter à un réseau distant, de se connecter au préalable à ce réseau afin d'effectuer une phase de pré-configuration consistant principalement à échanger les clefs d'authentification. Si elle est bien adaptée au nomadisme (je souhaite accéder à mon LAN lorsque je suis à l'extérieur de ma maison), cette sécurisation ne peut être retenue pour le scénario d'interconnexion entre deux LANs distants.

La problématique de la traversé du NAT ne se pose pas lors de la communication entre les équipements du LAN et l'équipement distant puisqu'ils sont reliés par un tunnel. Tout se passe comme si l'équipement distant, une fois durement authentifié, était directement raccordé au LAN. Mais la localisation du RAS peut de nouveau faire surgir le problème du NAT. En effet, dans le cas où le RAS est embarqué dans la passerelle domestique, ce dernier aura un accès direct à l'interface WAN et donc n'aura pas de problème pour communiquer avec le RAC de l'extérieur. Sauf que, dans le cas où le RAS se trouve dans un équipement autre que la passerelle domestique il faudra trouver une solution pour rediriger les messages entrant du RAC vers l'équipement RAS.

Finalement, vu que cette architecture est générique à tous les services d'accès à distance, elle n'a pas traité la problématique de la gestion de la QoS et l'a déléguée aux services qui vont l'utiliser.

Ces limitations ont été étudiées par ERICSON dans leur service de partage de contenus baptisé HIGA (Home IMS GAteway) [11, 12]. Comme les solutions de ce service sont offertes par le framework IMS (IP Multimedia Subsystem), donnons d'abord un petit aperçu sur IMS. IMS est un framework pour les réseaux d'accès qui permet l'interconnexion des réseaux hétérogènes. Il est standardisé par les opérateurs réseaux. Il offre un ensemble de services réutilisables (AAA, VoIP, IP TV, …) qui facilitent la conception de nouveaux services et l'interopérabilité avec les services existants grâce à l'utilisation des protocoles standardisés :

- SIP (Session Initiation Protocol) [13] utilisé pour l'établissement de session, la gestion de la mobilité et la souscription aux services;
- DIAMETER [14] utilisé pour l'accès et la gestion des profils des différents services, des stratégies (policy) des trafics et de la facturation des données.

L'un des points forts d'IMS est le fait qu'il sépare la signalisation du plan de transport. Dans le plan de signalisation d'IMS, il y aussi une séparation fonctionnelle entre les entités de ce plan:

- Contrôle des sessions : assuré par les nœuds CSCF (Call Session Control Function);
- Stockage des profils et authentification des clients: assuré par le HSS (Home Subscribe Server) ;
- Couche métier des services : assurée par les AS (Application Server) qui sont sollicités par les CSCF.

Pour garantir la QoS pendant le transport des trafics des sessions établies, IMS a défini l'entité RACS (Resource and Admission Control Subsystem). Le RACS réalise le contrôle d'admission et permet la réservation des ressources pour protéger les trafics existants et garantir la QoS pour le

transfert des nouveaux flux. Cette fonctionnalité est réutilisée dans la solution HIGA d'ERICSON afin de réserver les ressources nécessaires à l'acheminement du trafic entre le *device* distance et le LAN visité.

La synergie entre l'IMS et l'UPnP est assurée par le bloc fonctionnel nommé HIGA, déployé dans la passerelle domestique. L'utilisation d'IMS permet de surmonter la contrainte de configuration hors ligne des *devices*, imposée par l'architecture UPnP RA. La solution consiste à établir une session sécurisée entre le *device* distant et le HIGA. La gestion des droits d'accès au LAN et l'authentification sont fournis par le Framework IMS, en dédiant un AS spécifique à ce service. Les messages SDP [15] (Session Description Protocol) encapsulés dans la signalisation SIP sont utilisés pour informer le RAServer et le RAClient des adresses IP et des ports du tunnel à mettre en place. La signalisation SIP sert aussi à la négociation des profils VPN et des protocoles de gestion de clefs à employer lors de l'établissement du tunnel entre le RAC et le RAS. Une fois le tunnel mis en place, le *device* distant et celui dans le LAN visité pourront communiquer comme défini dans l'architecture UPnP RA.

2.3.3 Solution HGI

HGI (Home Gateway Initiative) [16] a été fondé par les fournisseurs de services et les constructeurs d'équipements digitaux des réseaux domestiques. Ses efforts de standardisation ont pour but de définir la manière d'acheminer les services IP externes vers les équipements des réseaux domestiques. Les équipements pris en compte dans le réseau domestique sont des équipements IP génériques, et non seulement UPnP.

HGI a publié des spécifications de blocs logiciels et matériels que la passerelle domestique doit embarquer pour connecter le LAN aux services IP externes. Parmi les services supportés, on retrouve le service d'accès à distance. La spécification publiée par HGI pour ce service a divisé les cas d'utilisations en deux groupes :

- l'accès aux contenus stockés dans le LAN depuis l'extérieur ;
- le contrôle des équipements du LAN à distance (i.e. démarrer la vidéo surveillance).

HGI propose trois approches pour le service d'accès à distance. Ces trois approches utilisent quatre nouveaux blocs fonctionnels à embarquer dans la passerelle domestique:

- RA-Config : assure l'administration des listes des droits d'accès aux équipements du LAN (ACL : Access Control List) ;
- Device Discovery : permet la découverte des équipements du LAN et de ses services. Cette fonctionnalité peut utiliser le protocole UPnP ou autre ;
- Synchronization : assure la synchronisation des services entre la passerelle domestique et les équipements distants ;
- Remote Access Transport : transfère le trafic de/vers l'équipement local vers/depuis l'équipement externe.

2.3.3.1 Approche IMS

HGI préconisant le support de l'IMS dans la passerelle domestique pour le service VoIP (Voice over IP), c'est naturellement que la première approche a consisté à utiliser le Framework IMS pour authentifier les appelants et router la signalisation SIP afin de permettre la mise en place du tunnel media avec la passerelle domestique. Les autorisations d'accès aux équipements du LAN sont faites au niveau de la passerelle domestique (ACL) en se basant sur les identifiants IMS des utilisateurs. Le tunnel média peut être sécurisé en utilisant le mécanisme de gestion des clefs défini dans la négociation SDP.

Cette approche a inspiré plusieurs travaux qui ont proposé d'étendre l'UPnP A/V pour le partage de contenus à distance. Ils utilisent la signalisation SIP pour échanger les messages UPnP entre les équipements distants. Dans ces solutions [17, 18, 19, 80], la passerelle domestique embarque

un « SIP User Agent (UA) » et un « SIP/UPnP Adapter ». Le rôle des SIP UA est d'établir une session entre les deux passerelles domestiques, alors que les SIP/UPnP Adapters jouent le rôle de proxy. L'adaptation est dictée par la différence entre UPnP A/V et SIP : UPnP A/V utilise HTTP comme protocole de contrôle et de transport alors que SIP utilise respectivement UDP et RTP (Real-Time Transport Protocol). Le SIP/UPnP Adaptateur fait la conversion des messages de signalisation entrants et sortants dans la passerelle domestique (HTTP <-> SIP). Une autre adaptation est réalisée pendant la phase de transport du contenu (HTTP <-> RTP).

L'inconvénient majeur de ces solutions est leur consommation des ressources mémoire et CPU (Central Processing Unit) de la passerelle domestique. Sachant que la passerelle domestique est un petit équipement réseau ayant comme principale fonction le routage des paquets réseaux, elle a des ressources en mémoire et en processeur très limitées. Il s'agit d'un équipement de type embarqué et non d'un ordinateur en termes de puissance de traitement. Donc, la conception de cette solution peut se heurter à des problèmes de mise en œuvre.

2.3.3.2 Approche Web

La deuxième approche proposée par HGI pour le service d'accès à distance est une solution orientée Web. Dans cette solution, l'équipement externe recherche l'adresse IP publique de la passerelle domestique à visiter en interrogeant un serveur DNS (Domain Name Server). Ensuite, il se connecte à un serveur web embarqué dans la passerelle domestique. L'authentification se fait dans la passerelle domestique avec un système de nom d'utilisateur/mot de passe. Une fois authentifié, l'équipement peut accéder à l'ensemble d'équipements auxquels il a droit via le web serveur.

Cette solution présente certaines limitations : elle contraint par exemple le client à utiliser un équipement qui contient un navigateur web, pour accéder à distance aux équipements. Cela éliminera alors les équipements UPnP A/V et limitera l'expérience utilisateur. La deuxième contrainte est que le serveur web à embarquer dans la passerelle domestique demande des ressources importantes en CPU et en mémoire vu qu'il implémente toute la couche logique du service. Sachant que la passerelle domestique possède des ressources limitées, cette solution aura des performances modestes.

2.3.3.3 Approche gérée par opérateur

A la différence des deux précédentes approches, celle-ci n'ajoute pas de nouvelles fonctions à la passerelle domestique. Toutes les fonctions de contrôles et la logique du service sont prises en charge par un tiers de confiance qui est l'opérateur de service. Ce dernier se connecte à la passerelle domestique afin de permettre l'accès à distance et le contrôle de l'équipement voulu dans le LAN visité. Une règle est ajoutée dans le pare-feu de la passerelle domestique afin d'autoriser les messages de l'opérateur. Ici, il est aisé de filtrer qui envoie ces messages car ils émanent tous de l'opérateur de service qui est reconnu par son adresse IP publique. Il est à signaler que dans cette solution tout le trafic de signalisation et de données passe par la plate-forme centrale de l'opérateur.

Une telle solution risque d'être non adéquate pour un grand nombre d'utilisateurs puisque la plate-forme de l'opérateur peut devenir un goulot d'étranglement.

2.3.4 Solutions Web & P2P

Nous pouvons trouver un grand nombre de service de partage de contenus sur internet. Les plus connus sont : Youtube pour le partage des vidéos, DailyMotion pour le partage de la musique et Picassa ou Flickr pour le partage des photos.

Comme nous pouvons le constater, ces services sont souvent dédiés à un seul type de contenus. Les contenus partagés avec ces services sont stockés dans des serveurs externes aux LANs des

utilisateurs, ce qui entraine la perte de la confidentialité des contenus, voire de leur propriété. De plus, les solutions P2P (Bittorent, Emule …) n'offrent pas une sécurité et une authentification fortes afin que les utilisateurs puissent contrôler les personnes avec lesquelles ils partagent leurs contenus. Toutefois, la dernière famille des applications P2P permet de configurer facilement un serveur Web à domicile (i.e. Weezo) avec un contrôle d'accès, mais elle a les mêmes limitations que la solution HGI « gérée par opérateur».

Un dernier défaut que nous pouvons mentionner concernant ces solutions est l'absence du support de la QoS pendant la phase de transfert puisque les fournisseurs de services Web et de solutions P2P n'ont pas d'accord avec les opérateurs réseaux pour réserver des ressources pour leurs trafics.

2.4 Gestion de la Qualité de Service

Comme nous l'avons vu dans la section précédente, il y a une croissance en termes d'offres de services de partage de contenus multimédias. La question qui se pose est : comment proposer un nouveau service de partage qui peut se distinguer des services actuels ? Une manière de se distinguer est d'offrir une garantie de la Qualité de Service (QoS) nécessaire pendant le transfert des contenus. Afin d'assurer cette fonction de gestion de QoS, nous allons identifier les besoins nécessaires à un tel service.

En premier lieu, il est important de pouvoir identifier le chemin emprunté par les données de ce service. Il peut être divisé en trois grandes portions : le réseau domestique (LAN) source hébergeant le contenu partagé, le réseau cœur et le LAN qui contient l'équipement consommateur du contenu. Les réseaux domestiques sont limités en ressources réseaux et centralisés autour d'un seul équipement qui est la passerelle domestique, d'où la nécessité d'un mécanisme de gestion de QoS dans ce type de réseau. Au niveau des réseaux de cœur, la solution actuelle des fournisseurs de service réseau (NSP) est le surdimensionnement de leurs réseaux de transport afin qu'ils puissent acheminer tous types de trafics. Néanmoins, avec l'augmentation des trafics des services d'Internet cette solution ne sera pas suffisante, surtout si les données que nous voulons acheminer ont des contraintes de QoS assez exigeantes. L'utilisation de mécanismes de garantie de QoS s'impose aussi dans cette portion du chemin des données.

2.4.1 Contraintes de la gestion de QoS

L'expression de la QoS ne se fait pas de la même manière par l'utilisateur et par les applications. L'utilisateur évalue la QoS avec des termes non techniques par exemple en trois niveaux : Or, Argent, Bronze. Elle peut également être dérivée de la Qualité d'Expérience (QoE) qui correspond directement à ce que l'utilisateur ressent de l'usage du service. Alors qu'au niveau des applications, elles ont besoin de paramètres plus spécifiques pour demander de la QoS au réseau. Les principaux paramètres de QoS [20] sont :

- **Le débit** qui désigne la quantité d'information que l'application envoie par unité de temps, mesuré en bit/s. On peut le confondre avec la notion de la bande passante (Bp). Mais dans ce mémoire, nous allons utiliser le terme de Bp pour caractériser la capacité d'écoulement d'un lien ;
- **Le délai** exprimé en milliseconde, qui désigne le temps écoulé pour transmettre une quantité de données élémentaire entre deux nœuds dans le réseau;
- **Le taux de perte** qui indique la probabilité maximale que les données n'arrivent pas à destination ;
- **La gigue** qui exprime la variation du délai de transmission.

Les besoins en QoS d'un service de partage de contenus varient selon le scénario appliqué :

- Echange de musique : la contrainte forte de ce scénario est le délai et le taux de perte. Les encodages (notamment le MP3) actuels permettent de s'affranchir de la contrainte du débit sans pour autant pénaliser l'expérience utilisateur.
- Echange de vidéo : la contrainte forte de ce scénario est le débit et le taux de perte et en second lieu vient le délai et la gigue. En effet, avec un débit trop faible, la vidéo ne pourra pas être rendue en mode diffusé (streaming) et l'utilisateur devra attendre qu'elle soit complètement téléchargée rendant l'expérience de partage caduc.
- Echange de photos : c'est le scénario le moins contraignant, car il s'accommode d'un débit et un délai quelconques, mais il demande un faible taux de perte. Cependant, le débit à une influence sur la QoE : si le débit est trop faible l'utilisateur devra attendre trop longtemps pour visualiser dans de bonnes conditions un diaporama et trouvera donc le service peu agréable à l'usage.

Dans cette partie, nous passerons en revue les architectures de gestion de QoS standardisées dans les réseaux LAN ainsi que dans les réseaux cœurs.

2.4.2 Gestion de la QoS dans le LAN

Trois standards ont traité la gestion de la QoS au niveau des réseaux domestiques : HGI [74], UPnP avec sa spécification UPnP QoS [21, 22, 23] et le standard AVB (Audio Video Bridging) [24].

2.4.2.1 Solution HGI pour la gestion de QoS

HGI a abordé la problématique de la gestion de la QoS au sein de l'un de ses groupes de travail. La solution proposée vise à garantir la QoS pour les trafics des fournisseurs de service transitant par la passerelle domestique. En effet, HGI a défini les fonctions de QoS à intégrer dans la passerelle domestique pour que les constructeurs les implémentent et les mettent à disposition des fournisseurs de services, ces derniers (fournisseurs de services) prenant en charge leurs configurations pour renseigner les caractéristiques de leur trafic. Pour cela HGI a défini la notion de services « gérés » (Managed Services) pour lesquels le fournisseur de service s'engage à garantir un niveau de QoS donné, par opposition aux services « non gérés » (Unmanaged Services). Un service géré ne concerne pas seulement un trafic entrant ou sortant vers un serveur du fournisseur de service, cela s'applique également aux transferts locaux : par exemple, si un utilisateur télécharge un film depuis un serveur VoD (Vidéo à la demande) de son fournisseur pour le consulter plus tard, le trafic engendré en local lors du visionnage du film sera considéré comme appartenant au service « géré » et recevra donc une QoS appropriée.

La solution fonctionne sur la base de la classification des paquets en fonction des services, effectuée par la reconnaissance d'une «signature du service». Cette classification de service est utilisée pour aiguiller le paquet vers la file d'attente appropriée, et peut être utilisée pour définir le marquage de niveau 2 pour une technologie particulière (Ethernet, WiFi, PLT). Il est également possible de supprimer des paquets sur la base de cette classification.

Les principales notions de la solution HGI sont:

- Identifier les services (paquet par paquet) sur la base de leur '*signature*'. HGI a proposé plusieurs techniques pour l'identification: utilisant l'adresse IP, les ports, l'adresse MAC, ...;
- Implémenter plusieurs files d'attentes dans chaque interface de la passerelle domestique et supporter les disciplines de gestion de files d'attente Weighted Round Robin et Strict Priority;
- Gérer la QoS de tous les trafics entrants, sortants et intra LAN (entre les équipements du LAN) ;

- Pas de dépendances des autres nœuds du réseau. Les fonctions de QoS n'agissent que sur la passerelle domestique;
- Prendre en compte la co-existence de ce schéma de QoS avec les autres schémas d'architecture de gestion de QoS, que ce soit dans le LAN ou dans d'autres portions du réseau.

Ayant une solution gérée par fournisseur de service, HGI ne propose pas de solution complète de la QoS dans le LAN. HGI traite de la même manière, en BEST EFFORT, tous les services « non gérés ». Cependant, elle peut former un élément clé de la gestion de la QoS et peut coexister avec les solutions qui seront nécessaires dans les réseaux domestiques, tels qu'UPnP QoS et AVB, et dans les réseaux cœurs.

2.4.2.2 UPnP QoS

La spécification UPnP QoS examine l'aspect QoS dans les réseaux IP domestiques. Le Forum a publié trois versions de la spécification UPnP QoS. Les deux premières versions [21, 22] proposent une solution basée sur la différenciation des flux (priorisation) pour assurer une meilleure performance lors du transfert des contenus multimédias dans un LAN congestionné. Néanmoins, cette méthode de priorisation n'est pas toujours suffisante, car il n'y a pas de différentiation entre deux services de même priorité. De même, la possibilité de préempter une priorisation peut perturber un service en cours d'utilisation. La version 3 d'UPnP QoS [23] a défini alors une solution basée sur la réservation des ressources (QoS paramétrée). Cette version présente aussi une solution hybride qui utilise la priorisation et la réservation de ressources ensembles. Les versions sont rétro-compatibles.

L'architecture UPnP QoS, quelque soit la version, a défini trois nouveaux services :

- QosManager service [25] : Il fournit au Point de Contrôle UPnP un ensemble d'actions pour demander, résilier ou mettre à jour la qualité de service pour un flux de données spécifique. Dans le cas où la méthode utilisée est la réservation de ressources, le QosManager a pour rôle de vérifier la disponibilité des ressources réseaux en se basant sur les caractéristiques du flux. Il interagit avec tous les équipements du LAN intervenant dans l'acheminement du flux pour prendre la décision d'accepter ou pas le nouveau flux.
- QosPolicyHolder service [26] : C'est un répertoire de stockage des règles (stratégies) de QoS à appliquer dans le réseau. Il est utilisé dans la solution par priorisation ou hybride. Son rôle est d'affecter efficacement les indices d'importance aux flux entrants dans le réseau. Il permet aussi de prendre la décision dans le choix des flux à suspendre en cas de congestion, si la préemption est sollicitée. Il est interrogé exclusivement par le QosManager.
- QosDevice service [27] : Il doit être implémenté par les équipements sources, destinations et situés sur le chemin emprunté par les données. Il offre une interface au QosManager pour récupérer les informations de QoS sur l'équipement et pour gérer ses ressources.

L'architecture de gestion de QoS, proposée dans la spécification UPnP QoS, définit un ensemble de concepts clefs.

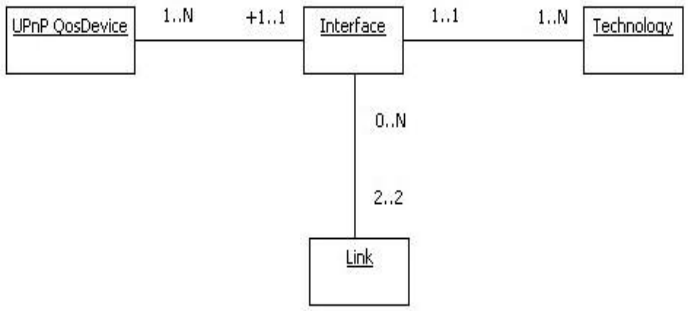


Figure 2.7 Interface et lien UPnP QoS

La Figure 2.7 présente ces concepts, d'interface, de lien et de technologie dont le service QosDevice a besoin.

Chaque service QosDevice possède au minimum une *interface* qui est le point d'interconnexion entre l'équipement et le réseau. Une *interface* utilise une seule *technologie* comme l'Ethernet, CPL (Courants Porteurs en Ligne) ou WiFi. Un *lien* est une connexion directe entre deux équipements pour l'échange de données (peut être bidirectionnel). Dans une *interface*, les *liens* sont identifiés avec leurs identifiants LinkId. Une *interface* peut contenir des *liens* multiples, alors qu'au niveau du QosDevice, un *lien* n'appartient qu'à une seule *interface*.

Les deux derniers concepts sont l'*UPnP Path* et le *QosSegment*. Un *UPnP Path* est composé d'une séquence ordonnée de QosDevices, de la source à la destination.

Le *Path* peut être divisé en sous ensembles d'*interfaces* interconnectées et qui sont gérées par le même mécanisme d'admission. Ces sous-ensembles sont nommés *QosSegment*. Ce concept est introduit afin de cacher au QosManager la dépendance à la couche 2 pendant la mise en place de la QoS au niveau du *segment*.

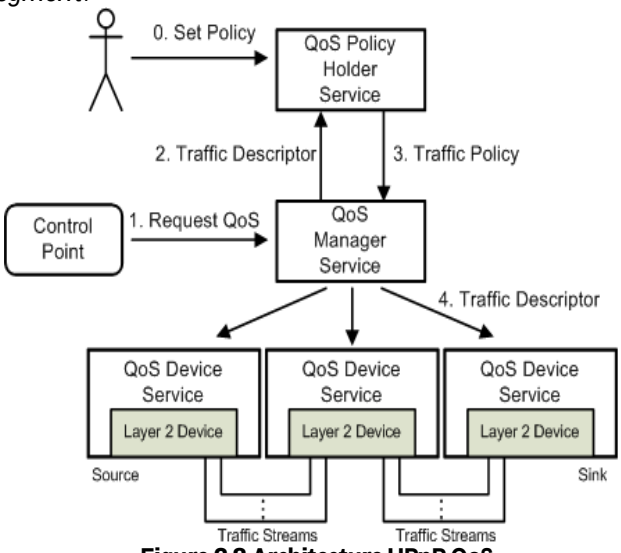


Figure 2.8 Architecture UPnP QoS

La mise en place de la QoS avec UPnP QoS se passe en quatre étapes, comme présenté dans la Figure 2.8:

- La requête de QoS est envoyée par un Control Point vers un QosManager (plusieurs QosManagers peuvent coexister dans le même LAN). Cette demande contient un descripteur de trafic (TrafficDescriptor) qui détaille les informations identifiant le trafic et ses paramètres.
- Le QosManager envoie ensuite une requête au QosPolicyHolder, contenant les informations sur le trafic, pour déterminer les règles à appliquer pour la priorisation.

Le QosPolicyHolder renvoie la règle adéquate au QosManager. Dans le cas d'une demande de réservation paramétrée, le QosManager sollicite directement les QosDevices impliqués sans solliciter le QosPolicyHolder.

- Le QosManager envoie ensuite un message aux QosDevices concernés par le transport du flux, leur indiquant les réservations de ressources ou de priorisation à effectuer. Si le réseau est congestionné et qu'il est nécessaire d'arrêter certains trafics, le QosManager utilise la réponse du QosPolicyHolder afin de choisir les trafics à arrêter.
- Les QosDevices sollicités par le QosManager vont, soit appliquer la ou les règles de priorisation, soit effectuer le control d'admission sur les QosSegments concernés et réserver par la suite les ressources si elles sont disponibles. Une confirmation ou infirmation est envoyée en retour au QosManager.
- Le résultat de l'application de la QoS (succès ou échec) est ensuite renvoyé au point de contrôle ayant invoqué la demande.

La gestion in fine de la QoS est du ressort des seuls QosDevices. C'est en effet à eux de décider si le flux peut être admis ou non, de réserver les ressources et surtout de configurer les files d'attentes et autre mécanismes de transmission de façon adéquate pour que la QoS soit effectivement rendue telle que demandée. Le problème est que l'UPnP forum n'a pas standardisé de mécanisme particulier ni émis de recommandations, et au final laisse les fabricants libres de leur implémentation du QosDevice.

UPnP QoS offre une architecture ouverte et générique pour la gestion de QoS dans le LAN. Mais, elle impose à tous les équipements réseaux qu'elle gère d'implémenter la pile IP. Cette condition élimine alors la possibilité de gérer de la QoS sur certains équipements, par exemple les commutateurs (switch) niveau 2 ou bien les équipements CPL qui n'ont pas de pile IP.

Tout de même, la notion de QosSegment introduite dans UPnP QoS v3 permet l'intégration d'autres technologies pour gérer la QoS au niveau 2, comme par exemple AVB. De même, il est possible de gérer un QosSegment avec seulement un QosDevice attaché à ce QosSegment.

Dans la dernière partie de cette section, nous allons présenter le standard AVB.

2.4.2.3 Audio Video Bridging (AVB)

Le groupe de travail IEEE 802.1 Audio Video Bridging (AVB) a défini un ensemble de standard, au niveau de la couche liaison, dédié au réseau IEEE 802 afin de permettre l'échange des flux audio et vidéo. La coopération de ces standards vise à respecter les contraintes des applications temps réel et à préserver le réseau d'éventuelles congestions pour protéger les ressources déjà réservées.

Les principaux protocoles définis par ce groupe de travail sont :

- IEEE 802.1 Qat Stream Reservation Protocol (SRP) [28]: gère le contrôle d'admission des flux dans un réseau bridgé. Il définit les protocoles nécessaires à la réservation des ressources pour les flux de données.
- IEEE 802.1 Qav Forwarding and Queuing for Time-Sensitive Streams [29] : propose des techniques de gestion de files d'attente dans les bridges pour diminuer le temps d'attente des messages dans le réseau.
- IEEE 802.1AS [30] : assure la synchronisation entre la source et le récepteur d'un flux.

Les mécanismes AVB

i. Le contrôle d'admission

Le standard SRP propose un mécanisme de réservation de ressources et des fonctions d'admission d'appel pour protéger le réseau d'une éventuelle congestion.

Architecture de SRP : SRP utilise trois protocoles de signalisation : Multiple Stream Registration Protocol (MSRP), Multiple VLAN Registration Protocol (MVRP) [31] et Multiple MAC Registration Protocol (MMRP) [32], qui coopèrent pour réserver des ressources à leurs flux.

Les protocoles obligatoires dans ce standard sont MSRP et MVRP ; l'utilisation de MMRP est optionnelle. En utilisant l'enregistrement MMRP, les terminaux qui proposent des flux et les bridges intermédiaires auront la possibilité de localiser les potentiels receveurs et les chemins pour y accéder.
MSRP hérite ses fonctionnalités de base du protocole MRP (Multiple Registration Protocol) [31]. En effet, MRP définit un mécanisme générique d'annonce d'attributs dans un réseau bridgé. L'architecture fonctionnelle de MSRP est illustrée par la Figure 2.9. Elle décrit l'exemple d'un Bridge à deux ports ainsi qu'un terminal.

Chaque port comporte un composant « MSRP participant » qui est composé de deux composants « application MSRP» et « MRP Attribut Declaration » (MAD) :

- Application MSRP: Elle applique les règles de traitement des nouvelles requêtes reçues depuis les applications (cas du terminal) ou le réseau (cas du bridge).
- Composant MAD: Il offre un mécanisme de signalisation aux applications MSRP pour propager leurs unités de données MSRPDU échangées entre les « MSRP participants » présents dans le réseau.

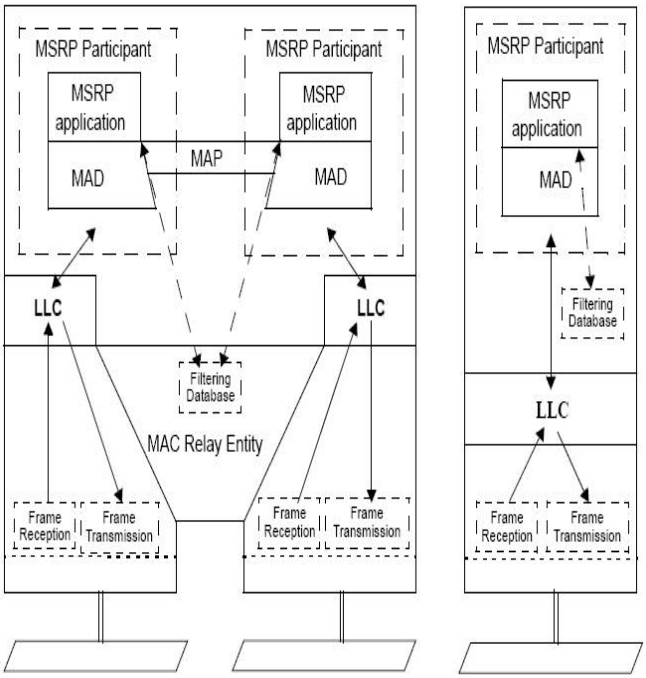


Figure 2.9 Architecture fonctionnelle dans SRP [25]

Dans les bridges il y a un composant spécifique appelé « MRP Attribute Propagation » (MAP): il permet aux MSRP participants d'un bridge d'avoir la même vision sur les déclarations des ressources et des réservations existantes qui transitent dans le bridge. Il propage les informations entre les « MSRP participants ». Les règles de propagation sont déduites des informations de filtrage du bridge (Filtering Database).

SRP définit deux nouvelles entités logiques:

- Talker : Terminal qui envoie des flux ;

- Listener : Terminal qui reçoit des flux.

Le même équipement peut être Talker et Listener en même temps.

Fonctionnement des terminaux : SRP permet d'annoncer ou d'annuler deux types de déclarations, à savoir les déclarations d'offre « offering declaration » et les déclarations de demande « asking declaration ». Une déclaration donnée est propagée à toutes les applications MSRP participantes des terminaux et des bridges dans le réseau. SRP utilise le mécanisme de signalisation MSRP pour échanger ces déclarations.

Les Talkers initient des déclarations d'offre pour annoncer les flux qu'ils peuvent procurer. La propagation de ces déclarations permet aux Listeners et aux Bridges de connaître les Talkers et leurs flux.

Comme ces déclarations sont propagées dans le sens descendant (downstream), elles peuvent être utilisées pour collecter les informations de QoS le long du chemin entre les Talkers et les Listeners.

Selon la disponibilité des ressources, les déclarations sont classifiées en déclarations « Talker Advertise » et déclarations « Talker Failed ». Une déclaration d'offre « Talker Advertise » signifie que la déclaration du flux n'a pas rencontrée de limitations en ressources réseaux. Cette déclaration continue d'être annoncée par le Talker tant que les ressources sont disponibles dans le réseau.

Une déclaration « Talker Failed » est une déclaration qui a rencontré une limitation de ressources le long du chemin de données. Le Listener qui reçoit ce type de déclaration sait qu'il ne peut pas recevoir le flux annoncé dans cette déclaration.

Un Listener qui reçoit une déclaration « Talker Advertise » peut alors envoyer une déclaration de demande pour recevoir le flux annoncé. Cette déclaration aussi permet de collecter les informations de QoS, mais dans le sens montant (upstream), du Listener vers le Talker. Les déclarations des Listeners qui arrivent aux Talkers comportent trois états possibles:

- Listener Ready : Un ou plusieurs Listeners ont demandé de s'enregistrer à ce flux et il y a suffisamment de ressources réseaux le long de tous les chemins du Talker vers le Listener pour recevoir le flux. Alors, il peut commencer à envoyer ses données sachant qu'il aura les ressources nécessaires pour acheminer son flux vers tous ses destinataires ;
- Listener Ready Failed : Deux Listeners ou plus ont demandé de s'enregistrer au flux. Il y a des ressources pour envoyer au moins le flux vers un Listener, mais les ressources ne suffisent pas pour envoyer le flux à tous les demandeurs.
- Listener Asking Failed : Un ou plusieurs Listeners demandent de s'enregistrer au flux, mais l'état du réseau ne permet d'envoyer le flux à aucun des Listeners.

Fonctionnement du Bridge: A la réception d'une déclaration d'offre au niveau d'un Bridge, elle est transmise du *composant MAD* à l'*application MSRP* qui enregistre cette déclaration d'offre identifiée par l'attribut StreamID. L'application MSRP vérifie si ses ressources disponibles suffisent pour transférer le flux décrit par cette déclaration. Dans le cas positif, elle est propagée par le *composant MAP* vers les *MSRP participants* concernés par cette déclaration. Ensuite, l'application MSRP envoie un « Talker Advertise » par les ports adéquats. Dans le cas où il n'y a pas assez de ressources, un « Talker Failed » est envoyé.

A la réception d'une déclaration de demande d'un Listener, l'application MSRP vérifie tout d'abord si elle a enregistré une déclaration d'un Talker correspondant au StreamID indiqué dans cette déclaration. Si le flux n'est pas enregistré, la déclaration n'est pas prise en compte. Ensuite,

l'*application MSRP* calcule s'il y a des ressources qui permettent l'envoi du flux. Si le bridge a encore les moyens réseaux pour assurer la QoS décrite dans la requête, il réserve les ressources demandées et transfère un « Listener Ready » à la source du flux. Sinon, il envoie selon la situation un « Listener Ready Failed » ou un « Listener Asking Failed ».

ii. Gestion des priorités des flux

Les trafics temps réel ont besoin d'un temps de transmission et de latence déterministe et minimal. Le mécanisme de réservation de ressources proposé par le standard SRP n'est pas suffisant. Il faut en plus un mécanisme qui permette de différencier les flux temps réel des autres flux pour leur donner une certaine priorité lors de l'envoi. Ce mécanisme est étudié par le standard 802.1 Qav. Il propose trois principaux blocs fonctionnels. Le premier est la gestion des files d'attentes pour les ports de transmission. Le deuxième est la classification des flux en classe de service et le dernier est l'arrangement des flux (traffic shaping).

iii. Synchronisation

La fonction d'arrangement des flux du protocole 802.1 Qav nécessite une synchronisation entre les nœuds du réseau AVB. Cette problématique est étudiée dans le standard 802.1 AS.

802.1 AS définit un protocole d'échange d'informations de date qui permet aux terminaux connectés au réseau AVB de se synchroniser avec une horloge de référence (Grand Master Clock). Le standard a prévu deux méthodes de sélection de l'horloge de référence : la première automatique avec un algorithme d'élection entre les horloges présentes dans le réseau ; la deuxième est statique et permet à l'administrateur de désigner l'horloge de référence de son service.

Les premiers travaux d'évaluation de ce standard [33] démontrent son fort potentiel même s'il est encore à un stade non finalisé. La faiblesse de ce standard vient de la contrainte que seul un Listener a le droit de réserver de la QoS pour un flux déjà annoncé par un Talker. Plusieurs scénarii ne peuvent pas remplir cette condition. Prenons l'exemple où nous voulons réserver de la QoS pour regarder une chaine TV en haute définition. La source du flux est à l'extérieur du LAN et donc elle ne peut s'annoncer en tant que Talker. D'où l'impossibilité de réserver de la QoS dans ce scénario. Malgré cela, les industriels portent un grand intérêt à AVB et ont créé le consortium AVnu Alliance [34].

2.4.3 Gestion de la QoS dans les réseaux cœur IP

L'étude des techniques de gestion de la QoS dans les réseaux cœurs IP révèle un grand nombre de solutions et de standards traitant cette thématique. Cependant, nous pouvons distinguer deux principales stratégies que ces solutions utilisent pour garantir la QoS. La première stratégie est d'éviter le phénomène de congestion dans le réseau. Les solutions optant pour cette stratégie doivent implémenter une fonction d'admission d'appel afin de n'accepter que les appels que le réseau peut acheminer, avec la QoS demandée. La deuxième stratégie consiste à gérer la congestion. Cette stratégie utilise la différentiation de trafic pour offrir la QoS au flux les plus importants en cas de congestion.

Dans cette partie, nous présentons les solutions standardisées les plus abouties, illustrant ces deux stratégies. La première partie passera en revue les modèles de QoS destinés à internet. Dans la deuxième partie, nous présenterons le modèle de QoS proposé par l'IP Multimedia Subsystem (IMS). Et pour terminer, nous exposerons la technique de l'ingénierie du trafic.

2.4.3.1 Modèles de QoS pour Internet

L'internet offre seulement le service dit au mieux (best-effort) qui ne garantie aucune QoS (délais limité, réservation de débit, contrôle de flux, …). Plusieurs travaux ont été conduits pour proposer une solution qui offre des services avec QoS applicables à l'échelle d'un grand réseau comme internet.

Nous exposons dans ce qui suit les modèles étudiés au sein de l'IETF (Internet Engineering Task Force) et qui ont été la base de plusieurs travaux dans ce domaine. Nous terminons cette partie par la présentation des travaux du projet européen EuQoS [63], qui ont proposé des améliorations aux modèles de l'IETF.

Modèle Integrated Services (IntServ)

L'objectif de ce modèle est de d'offrir une QoS déterministe pour chaque flux. Le modèle définit les services qu'il offre, les fonctions à mettre en place pour fournir ces services et le protocole de signalisation pour demander de la QoS (RSVP Ressource Reservation Protocol [37]).

IntServ identifie deux nouveaux services ; le service Garanti (GS) [38] offrant une bande passante déterministe et un délai limité et le service à Charge Contrôlée (CL) [39] qui est équivalent à un service Best-Effort dans un environnement non surchargé.

Dans ce modèle, les routeurs et les stations intègrent quatre fonctions de QoS, à savoir *un contrôleur d'admission* qui vérifie s'il y a suffisamment de ressources disponibles qui peuvent être attribuées aux flux sans affecter les flux existants ; *un classificateur de paquets* qui classe chaque paquet entrant dans sa classe spécifique; *un ordonnanceur de paquets* qui sélectionne les prochains paquets à transmettre en fonction des différentes classes de service et *un agent du protocole de réservation RSVP* pour émettre et traiter les messages de réservation.

Pour qu'une application demande de la QoS à son flux de données, elle doit contacter son agent RSVP afin d'envoyer un message de signalisation appelé PATH décrivant les caractéristique du flux à l'aide d'un Tspec (Trafic Specification). Les routeurs RSVP qui reçoivent ce message utilisent leurs fonctions de contrôle d'admission pour authentifier la demande et vérifier leurs ressources disponibles. Les routeurs enregistrent un état de la demande, ajoutent leurs informations au message (champs AD_SPEC) et le transmettent vers le prochain nœud. Il est à signaler qu'à ce stade, les routeurs ne réservent aucunes ressources et attendent une confirmation. En effet, en recevant le message PATH, le destinataire aura une vue détaillée des ressources disponibles dans tous les nœuds qui constituent le chemin. En fonction de ces informations, il choisit une classe de service pour ce flux (GS, CL) et répond avec un message RESV dans le sens inverse pour confirmer la réservation de ressources dans les routeurs. Du côté de la source du flux, à la réception d'un message RESV d'acceptation, l'application émettrice de la demande peut commencer à envoyer les données avec la classe de service acceptée par le réseau.

Le fait que les routeurs traitent les réservations de QoS flux par flux rend ce modèle inadapté aux réseaux à grande échelle devant traiter plusieurs millions de flux. Une autre faiblesse de ce modèle est qu'il impose aux opérateurs qui veulent l'adopter dans leurs réseaux une nouvelle stratégie de facturation par réservation.

Modèle NSIS

Plusieurs travaux de recherches ont essayé d'améliorer le modèle IntServ afin de le rendre adapté au passage à l'échelle. A cause de cet intérêt scientifique pour IntServ, l'IETF a créé un groupe de travail « Next Steps in Signalling (NSIS) » [56] afin de résoudre les problèmes de ce

modèle dans les réseaux à grande échelle. La grande nouveauté que NSIS a apportée est la séparation en deux couches du traitement des messages de signalisation, au niveau applicatif et au niveau transport.

- NSIS Transport Layer Protocol (NTLP) : cette couche est implémentée par le protocole « General Internet Signalling Transport (GIST) » [40], qui est un protocole générique pour la transmission des différents messages de signalisation NSIS des couches applicatives. A la différence de RSVP, les routeurs qui sont sur le chemin de transfert de données ne sont pas tous obligés de l'implémenter. Mais, GIST possède du protocole RSVP son aspect « On-Path » puisque les messages de signalisation GIST empruntent le chemin de données du flux à transmettre ;
- NSIS Signaling Layer Protocols (NSLP) : cette couche implémente les fonctionnalités spécifiques à l'application à laquelle elle est dédiée, tel que le format des messages et les traitements des messages échangés entre les différents nœuds. Une version consacrée à la QoS, QoS-NSLP est définie dans [41].

Cette séparation en couches offre au protocole NSIS une grande flexibilité. Cependant, les protocoles NSLPs et plus précisément celui qui est dédié à la QoS souffrent du même problème de passage à l'échelle que leur petit frère RSVP. En cœur de réseau, un routeur peut être amené à gérer les états de millions de flux. De plus, le groupe de travail ayant mis beaucoup de temps pour produire les standards sans pour autant remplir leur missions (telle que définies dans le charter du groupe) ont conduit les instances dirigeantes de l'IETF à publier les RFC du groupe NSIS en mode expérimental. Autrement dit, c'est une façon polie de mettre en sommeil le travail et il y a peu de chance que ces RFC soient un jour implémentés.

Modèle DiffServ

Le modèle DiffServ [42] fait partie des solutions qui proposent de faire de l'agrégation de flux dans les réseaux cœurs. Il propose d'implémenter dans le réseau cœur un système de différentiation de trafic. En plus des trafics Best-Effort, le modèle identifie deux classes de services:

- service *Expédié* (EF) [43] : Il garantit un délai et une gigue minimums mais ne permet pas de réserver un débit ni d'assurer un taux de perte. Il est conçu pour répondre aux contraintes des flux temps réel et interactif ;
- service *Assuré* (AF) [44]: Il garantit un taux de perte minimal mais ne s'engage pas sur le délai ou la gigue. Il est plus adapté aux applications de transfert de données.

La Figure 2.10 illustre les fonctions à implémenter dans les différents nœuds pour mettre en place ce système de différentiation de classes de services. Il n'a pas besoin d'un protocole de signalisation pour demander de la QoS. En plus, pour s'adapter aux réseaux à grande échelle, ce modèle a décidé de concentrer la complexité des traitements dans les routeurs de bordure. Ces derniers auront pour taches de classifier les flux par type de service et de les marquer en fonction de ces types. Ils doivent aussi vérifier que les flux EF respectent bien leurs contrats.

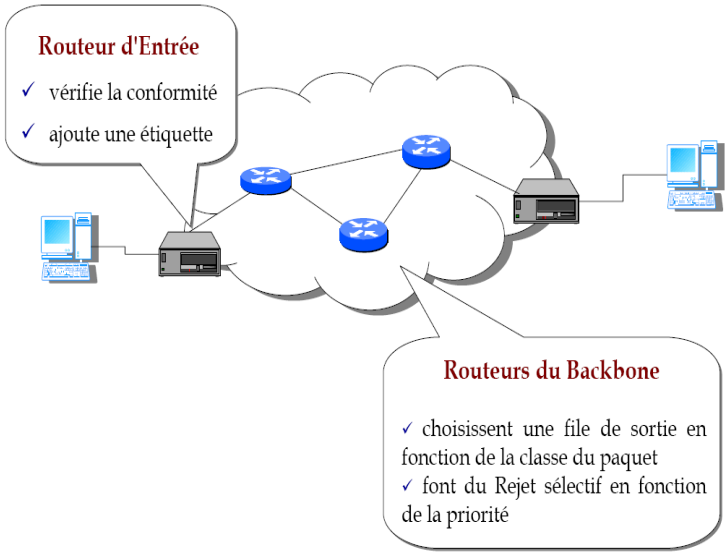


Figure 2.10 Modèle DiffServ

Le traitement dans les routeurs à l'intérieur du domaine est plus simple. Les paquets sont classés selon leurs étiquettes définies par le routeur de bordure. Un ordonnanceur distribue les ressources entres les files. En cas de congestion, les paquets de faible priorité sont rejetés et le comportement du modèle se rapproche alors du service Best-Effort.

Pour éviter la congestion, DiffServ a recommandé d'insérer une nouvelle entité centralisée dans le réseau cœur baptisé « Bandwith Broker » (BB) [45] afin d'assurer la fonction de contrôle d'admission. Cependant, cette nouvelle version du modèle souffrait de deux problèmes majeurs. Les interfaces offertes aux applications pour formuler les requêtes n'ont jamais été standardisées empêchant alors son adoption par un grand nombre de services. L'autre problème consiste à l'adaptation des décisions des BBs aux changements de la topologie du réseau. Cette adaptation demande le maintient à jour de la vision de la topologie qui est encore un défi non résolu pour les réseaux à grande échelle.

Flow Aware et PCN

Afin d'éviter la congestion dans un domaine DiffServ, l'IETF a créé le groupe de travail « Congestion and Pre-congestion Notification (PCN) » [46,82] pour proposer des solutions en vue de protéger les flux admis en situation de congestion avérée ou imminente. PCN s'est inspiré de la technique dite « Flow Aware » [47]. Cette technique part du principe qu'un flux de données est une entité indivisible, et qu'une fois qu'un flux est admis par le réseau, il sera acheminé sans lui appliquer aucun traitement spécifique. Un contrôle du nombre de flux admis s'impose alors, afin d'éviter la congestion. Si le flux n'est pas accepté, tous les paquets de ce flux seront rejetés par le réseau. Le principe de base consiste pour un routeur de bordure à envoyer des messages spécifiques vers le routeur de bordure de destination afin d'avoir une connaissance de l'état du réseau, notamment au niveau de la congestion, vers ce routeur de destination.

L'idée principale est d'effectuer de l'admission et du rejet des flux au niveau des routeurs d'entrée dans le domaine. La décision repose sur les paramètres de détection de congestion et de pré-congestion et est prise localement par le routeur de bordure. La solution finale est encore en chantier, vu le nombre de défis à résoudre, par exemple, la détection de la fin des sessions qui est fortement liée au type de l'application, le volume de données du flux (débit, durée) ou bien la corrélation entre les flux des applications multi flux tel que la visioconférence (flux vidéo + flux audio). En effet, le mécanisme risque de rejeter un des flux d'une même application rendant ainsi son utilisation impossible.

Modèle EuQoS

Le projet européen EuQoS s'est penché sur la problématique de la gestion de la QoS inter-domaines dans les réseaux à grande échelle telle qu'Internet. Les travaux de ce projet ont donné naissance à une nouvelle architecture réseau générique pour la mise en place de la QoS dans un contexte d'inter-domaines, de multi-technologies et de multiservices. Cette architecture propose une découpe en deux plans : un plan de service et un plan de contrôle. Le plan de service forme la couche de négociation entre les applications et les fonctions du réseau. La nouvelle signalisation utilisée dans ce plan (EQ-SIP) est basée sur le protocole SIP. Le plan de contrôle est en charge de négocier et d'appliquer les demandes de QoS dans les équipements du réseau.

Pour concevoir une architecture le plus générique et extensible possible, l'équipe de EuQoS a découpé le plan de contrôle en deux couches : une première couche indépendante de la technologie, qui est une couche d'abstraction. Elle facilite l'interaction inter-domaines et inter-technologies. La deuxième couche est dépendante à la technologie et pilotée par la première couche d'abstraction.

Le potentiel de cette architecture est mis en évidence à l'aide d'un prototype développé au sein du projet EuQoS [64]. Mais, il reste un grand travail de normalisation avant que cette architecture ne soit adoptée. Nous citons par exemple la définition, dans le plan de service, d'une interface standard aux applications afin qu'elles demandent de la QoS au réseau en toute sécurité.

2.4.3.2 La QoS dans IMS

L'idée de transformer le service best effort des réseaux IP en introduisant de la QoS de bout en bout était l'une des motivations des concepteurs de l'IP Multimedia Subsystem IMS. Le fait de prévoir dans l'architecture IMS un sous-système (entité) spécifique pour gérer la QoS rend possible la prise en charge de nouveaux services tels que les services multimédias et les services temps réel.

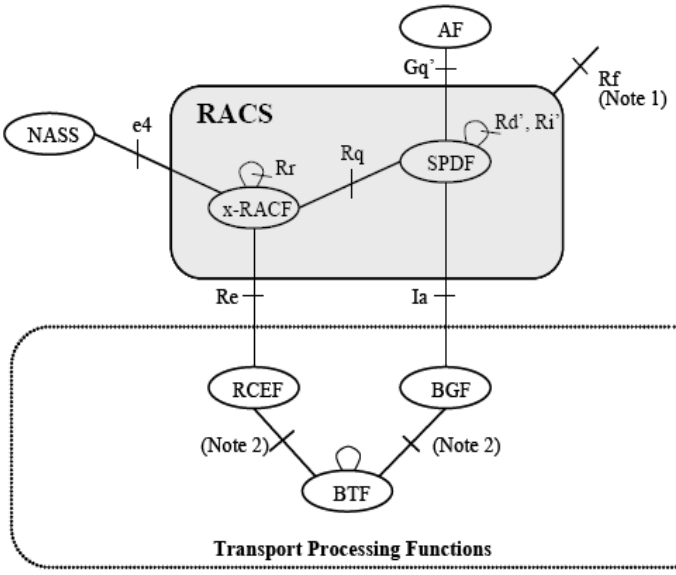


Figure 2.11 Position du RACS dans l'architecture IMS [29]

La spécification du Resources Admission Control Subsystem (RACS) est détaillée dans [35, 36]. La Figure 2.11 représente l'architecture fonctionnelle du RACS et les fonctions avec lesquels il

peut interagir. Nous allons commencer par présenter le contexte qui englobe le RACS et nous poursuivrons ensuite avec ses fonctionnalités.

Fonction du plan de service

Fonction Applicative (AF)

Certains services utilisent une signalisation applicative pour demander de la QoS au réseau. L'architecture IMS a pris en compte ce type de service et a défini l'entité Application Function (AF) pour désigner le nœud applicatif qui aura la responsabilité de formuler la requête au RACS via une interface dédiée (Gq').

Les principales informations qu'un AF doit fournir au RACS sont : un identifiant du flux à traiter (clientId et/ou adresse IP), le débit à garantir et éventuellement la classe de service qui indique les caractéristiques de QoS au niveau de la couche de transport de données. Le plus souvent dans l'IMS, cette fonction est assurée par le Call Session Control Function (CSCF).

Fonctions du plan de transport

i. Resource Control Enforcement Function (RCEF)

Cette entité fonctionnelle est déployée habituellement dans les routeurs de bordure (nœud d'accès). Elle peut être déployée dans le réseau d'accès comme dans le réseau cœur. Cet élément logique appartient aux fonctions de traitement de transport qui appliquent les stratégies et politiques de QoS commandées par le RACS, tel que le marquage de paquet et la réservation de ressources. Il peut aussi déclencher une admission d'appel dans le RACS, pour permettre la gestion de la QoS à partir du plan de transport.

En fonction de la technologie utilisée dans le réseau géré par cette fonction, elle peut proposer un ou plusieurs mécanismes de mise en place de QoS tel que :

- les mécanismes QoS purement de niveau 2, exemple la technique des VP/VC dans les réseaux ATM ou la technique des tags VLAN dans les réseaux Ethernet ;
- les mécanismes intermédiaires entre niveau 2 et 3, exemple la technique MPLS;
- les mécanismes purement de niveau 3, exemple la technique DiffServ ;
- les mécanismes mixtes entre niveau 3 et 2, exemple DiffServ dans l'ATM ou DiffServ avec MPLS.

ii. Border Gateway Function (BGF)

C'est une passerelle de paquet IP au niveau du plan de transport. Elle est située à la limite entre deux réseaux, par exemple entre le réseau d'accès et le réseau de cœur (C-BGF) ou entre deux réseaux cœurs (I-BGF). Elle peut offrir en plus de ses fonctionnalités de transport de flux standards, des services de mise en place de QoS qui complètent ceux du RCEF. Cette entité peut gérer la QoS à l'échelle du micro-flux (différentiation de flux ou réservation de ressources, contrôle de dépassement de débit …).

Le lien entre le RACS et cette fonction n'est pas obligatoire, donc il se peut que le RACS n'ait pas recours à ses services.

Fonctions du RACS

i. Generic Resource Admission Control Function (X-RACF)

Il y a deux spécialisations de cette fonction, l'Access-RACF (A-RACF) déployée dans le réseau d'accès et la Core-RACF (C-RACF) déployée dans le réseau cœur. En plus d'agir sur une partition de réseau différente, la principale différence entre ces deux types de RACF est que le premier

vérifie le profil QoS du client pendant son admission d'appel alors que le deuxième ne permet pas cette vérification. L'A-RACF récupère ce profil au moment de l'attachement du client au réseau.

L'admission d'appel dans le RACS se fait en deux étapes. Tout d'abord, on vérifie que la demande de QoS est compatible avec le profil du client, en tenant compte aussi de ses réservations existantes. Si ce premier test est passé avec succès, on poursuit par la vérification de la disponibilité des ressources dans le réseau. Pendant cette phase, les x-RACFs peuvent coopérer entre eux, dans le cas où le x-RACF n'a pas une vision complète de la topologie et/ou des ressources entrant en jeu dans la nouvelle réservation. Si l'un de ces tests échoue, le x-RACF refuse la demande de QoS. Dans le cas positif, il envoie une requête au RCEF pour mettre en place la nouvelle réservation. Dans cette requête, le x-RACF désigne le mécanisme de QoS à utiliser et précise les paramètres de QoS du (des) flux désigné(s) dans la requête.

Le service d'admission d'appel du x-RACF peut être sollicité par la fonction « Serving Policy Decision Function » SPDF (défini dans ce qui suit), si la demande de QoS est déclenchée au niveau applicatif, ou bien par le RCEF si la demande de QoS est déclenchée au niveau transport.

ii. Serving Policy Decision Function (SPDF)

Comme son nom l'indique, le SPDF applique aux requêtes provenant de la couche applicative (AF), les règles de politiques définies par l'opérateur. Cette fonction masque aux différents AFs la topologie du réseau sous-jacent et la technologie utilisée pour offrir une vue commune de telle façon qu'ils n'aient pas à se soucier des couches inférieures.

A la réception d'une requête de QoS (réservation, modification), le SPDF vérifie tout d'abord l'éligibilité de l'AF à demander les ressources présentes dans sa requête en se basant sur les politiques qu'il stocke. Ensuite, il va déterminer les étapes du traitement à réaliser pour cette requête. Quels sont les x-RACFs qu'il va contacter ? Est-ce qu'il aura recours au service des BGFs ou pas ? Et dans le cas positif dans quel ordre il va faire appel aux x-RACF et aux BGF? Ce rôle de coordination peut se faire dynamiquement pour chaque requête en se référant aux règles de politiques de l'opérateur ou bien se fait statiquement avec une configuration au préalable.

Prenons le cas simple où le SPDF utilise un seul x-RACF et un seul BGF. Le SPDF envoie au x-RACF une requête de contrôle d'admission. L'x-RACF vérifie les ressources dans le segment qu'il gère et éventuellement applique la configuration adéquate dans le cas où il trouve les ressources nécessaires. Une fois que le SPDF reçoit un message de confirmation du x-RACF, il complète le traitement en envoyant une commande de configuration au BGF (marquage de paquet, réservation de bande passante, ..) pour tenir compte de la nouvelle requête. A la fin, le SPDF communique à l'AF avec le résultat final (succès/ échec).

Malgré les efforts des opérateurs dans la standardisation de l'IMS, la gestion de la QoS reste partielle et incomplète. Premièrement, le lien du RACS avec la couche applicative est très liée au protocole de signalisation de l'interface Gq' (DIAMETER). Cette dépendance par rapport au protocole de cette interface rend le RACS peu adapté pour certains services qui ne l'utilisent pas forcément, tel que les services Web.

Une autre limitation du RACS est qu'il est focalisé sur la partie traitant le réseau d'accès (A-RACF). En partant du principe que les réseaux cœurs actuels sont suffisamment surdimensionnés, les opérateurs ont repoussé à plus tard l'étude de l'interconnexion à l'inter domaine et la partie traitant le réseau cœur (C-RACF).

2.4.3.3 L'ingénierie de Trafic

Le caractère Best-Effort de l'IP est dû au choix de la méthode utilisée pour router les paquets. Cette méthode consiste à trouver le plus court chemin vers la destination sans prendre en compte l'état réel des liens. Ceci peut provoquer des situations de congestion dans certaines routes et des dégradations de la qualité de service, même s'il reste encore un moyen d'acheminer le trafic sur d'autres routes moins utilisées.

La discipline de l'ingénierie de trafic se propose de limiter les risques de congestion en optimisant l'utilisation des ressources du réseau et en appliquant des mécanismes de contrôle d'acheminement du trafic afin de maximiser la quantité de données acheminées en prenant compte les contraintes de QoS des flux.

L'ingénierie de trafic prend en entrée une matrice des trafics à transmettre avec leurs caractéristiques (débit, délai, gigue, …) et la topologie du réseau, et en sortie, elle produit un ensemble de routes qui assurent le transfert de tous ces trafics avec les QoS demandées.

La technique la plus connue dans le cadre de cette discipline est la technique de partage de charge. La technique ECMP (Equal Cost Multi Path) peut être introduite dans les protocoles IGP (Interior Gateway Protocol) pour améliorer le rendement du routage IP. En effet, lorsqu'un routeur trouve, pour une destination donnée, plusieurs chemins à coût égal (en nombre de saut), il partage son trafic vers cette destination équitablement entre ces différents chemins. Pour éviter d'éventuelles pertes de séquences des données des flux temps réels, ce mécanisme s'assure que le trafic d'un même flux prend une seule route.

Cette technique apporte une certaine amélioration au routage IP, mais elle n'est pas suffisante pour en garantir la QoS, parce que, d'une part elle ne prend pas en compte les caractéristiques des flux à transmettre, et d'autre part, elle n'a d'impact que sur les chemins à coûts égaux.

Afin de remédier aux limitations du routage IP, des études en ingénierie de trafic proposent de passer en mode connecté et à utiliser un routage explicite indépendant des routes IP standards (route la plus courte). La technologie MPLS "Multi Protocol Label Switch" [48] permet d'émuler le mode de transfert connecté dans tous les types de réseaux (IP, ATM ou autre). Il est indépendant des couches réseau et liaison utilisées. Dans MPLS, le routage s'effectue sur la base d'un label (MPLS Shim Header) [49] qui est inséré entre l'entête réseau (i.e IP) et mac (i.e ATM). Les routeurs MPLS maintiennent des tables de routage sur la base des labels MPLS. Ces tables sont créées manuellement ou avec le protocole de distribution de label (LDP Label Distribution Protocol) [50]. En utilisant la technique de commutation de label, MPLS permet de construire des chemins unidirectionnels appelés LSP (label Switch Path), qui sont indépendants du routage IP. Dans les domaines MPLS, les routeurs de bord (Label Edge Router LER) sont chargés d'ajouter les labels aux paquets entrants et de les enlever à la sortie du domaine.

Les tunnels MPLS constituent une bonne solution technique pour mettre en place les chemins de transfert de données produits par l'ingénierie de trafic. Cependant, il manque à cette technologie des mécanismes effectifs de mise en place de ces tunnels, qui permettent l'allocation des ressources dans les routeurs par lesquels ils passent. Cette adaptation de MPLS à l'ingénierie de trafic est plus connue sous le nom MPLS-TE [51].

Architecture MPLS-TE

MPLS-TE se base sur trois notions fondamentales :

- la topologie TE (Traffic Engineering) : c'est un graphe représentant la topologie du réseau, incluant les paramètres d'ingénierie de trafic tels que les bandes passantes maximales, disponibles et réservables de chaque lien ;

- les tunnels MPLS-TE : ce sont des LSP MPLS routés explicitement et à qui on fait correspondre un ensemble de contraintes d'ingénierie de trafic (la bande passante, le délai maximum, le nombre de sauts maximum, …) ;
- le routage par contrainte : c'est l'ensemble des mécanismes nécessaires pour calculer les routes des tunnels MPLS-TE sur la base de leurs contraintes TE et en prenant compte les ressources disponibles dans le réseau.

Routage des tunnels MPLS-TE

Il y a trois modes de calcul des routes des tunnels :

- statique : l'administrateur du domaine définit explicitement le placement des tunnels. Cette solution n'est pas acceptable pour mettre en place un service dédié à un grand nombre de clients ;
- distribué : le calcul du chemin est réalisé au niveau du routeur de tête du tunnel. Ce mode distribué peut passer à l'échelle, du fait que le calcul est distribué sur un grand nombre de nœuds, mais il possède certaines limitations, comme le fait que les routeurs n'ont pas toujours la vue complète du réseau;
- centralisé : un serveur est chargé du calcul de la route des tunnels à l'aide d'algorithmes de routage par contraintes. Un groupe de travail s'est formé à l'IETF pour standardiser cette solution. Il propose le protocole « Path Computation Element Protocol - PCEP » [52] pour calculer le placement des tunnels. Ce protocole permet à un « Path Computation Client -PCC » de demander au « Path Computation Element - PCE » [53] de lui calculer la route d'un tunnel MPLS-TE. L'inconvénient majeur de cette solution est sa faible réactivité aux changements de topologie à cause des temps de calcul qui peuvent être très longs si on a un grand nombre de tunnels à placer.

Mais dans la majeure partie des cas, MPLS-TE est utilisé pour provisionner les réseaux et non pour établir des connections en temps-réels. On serait de plus confronté au même problème que RSVP, à savoir le passage à l'échelle lorsqu'il faut gérer plusieurs millions de tunnels.

Signalisation dans MPLS-TE

Une fois le chemin du tunnel établi, il reste à effectuer l'annonce de ce tunnel à travers le réseau à l'aide d'un protocole de signalisation. Une concurrence s'est installée entre le protocole RSVP-TE [54], extension de RSVP, et le protocole CR-LDP [55], extension de LDP, pour standardiser la mise en place des MPLS-TE. C'est le protocole RSVP-TE qui a été finalement retenu.

Avec RSVP-TE, le routeur de tête envoie un message « Path » vers la destination, contenant la route explicite et les paramètres TE (id tunnel/LSP, source/dest, BP,…). A la réception d'un message « Path », le routeur destination répond avec un message « Resv » qui alloue la bande passante et distribue les labels. Les tables MPLS sont donc mises à jour dans les LSR. Un mécanisme de rafraîchissement d'état est nécessaire pour maintenir les états des LSP dans les LSR.

Nous pouvons constater après cette présentation que l'architecture MPLS-TE est la plus finie en termes de gestion de QoS. Il existe tout de même une critique à l'égard de cette technologie, c'est qu'elle n'est pas adaptée à tous les types de réseaux de transports, par exemple les réseaux d'accès radio.

2.5 Conclusion

Le contexte ciblé dans cette thèse étant celui des services de partage de contenus à distance, les études menées tout au long de ce travail de thèse visent à proposer un système réseau d'accès à distance sécurisé et de plus capable de gérer la QoS de bout en bout.

Ce chapitre a présenté les techniques déjà existantes pour les deux principales problématiques de notre travail :

- Les techniques d'accès à distance pour les services de partage de contenus;
- Les techniques de gestion de QoS dans les LANs et dans les réseaux de cœur.

Au niveau des services de partages, nous avons commencé par expliquer les contraintes à résoudre pour réaliser un tel service. Nous avons ensuite présenté les travaux proposés par les deux organismes de standardisation, UPnP RA et HGI, qui ont proposé des architectures d'accès à distance.

La solution UPnP RA consiste à mettre en place un tunnel sécurisé entre l'équipement connecté à l'extérieur du LAN et son LAN d'origine pour lui permettre d'utiliser les services UPnP présents dans son réseau.

Cette architecture est très générique mais pas forcément adaptée au partage de contenus, car par exemple la question de la gestion de la QoS n'est pas traitée. De même se pose des problèmes de conflits d'adresses lorsque l'on connecte deux réseaux domestiques via un tunnel sécurisé. Reste également à gérer l'échange sécurisé des clefs de chiffrement des tunnels. Plusieurs travaux ont repris cette architecture pour l'adapter à la réalisation de leurs services de partage de contenus. Nous avons surtout évoqué la solution HIGA d'ERICSON qui utilise le Framework IMS pour améliorer la technique d'échange de clef nécessaire pour établir le tunnel entre les équipements distants. En effet, UPnP RA impose une configuration préalable des clefs aux équipements désirant accéder au LAN depuis l'extérieur. HIGA a proposé d'établir une session IMS entre l'équipement et le LAN pour s'échanger les clefs, ce qui permet plus de flexibilité pour établir le tunnel sécurisé. L'utilisation d'IMS permet aussi de gérer la QoS via le sous-système RACS.

La solution HGI a défini une architecture fonctionnelle pour connecter les passerelles domestiques de deux LANs distants afin de mettre en relation les équipements derrière ces passerelles. L'architecture HGI offrait trois variantes : une utilisant IMS, une pilotée par l'opérateur et une troisième orientée Web. Etant plus adaptée pour le partage de contenus, la première variante a inspiré un bon nombre de travaux pour étendre l'utilisation d'UPnP A/V à l'extérieur du LAN. L'idée directrice de ces propositions était d'utiliser la signalisation IMS pour échanger les messages UPnP A/V entre les équipements distants, ce qui a imposé de faire une correspondance entre les protocoles utilisés par ces deux technologies : SIP d'un coté (IMS) et HTTP de l'autre (UPnP A/V).

Si les solutions citées jusque là sont compliquées à déployer pour une grande communauté d'utilisateurs, les solutions Web et P2P que nous avons exposées sont faciles à mettre en place. Cependant, elles souffrent d'une grande carence de sécurité et de confidentialité.

De plus, la remarque générale pour toutes les solutions actuelles est qu'elles n'offrent pas de solution de QoS de bout en bout.

Dans la dernière partie de ce chapitre, nous avons présenté les techniques de gestion de QoS. Dans un premier temps, nous avons exposé trois standards de gestion de la QoS pour les LANs : HGI, UPnP QoS et AVB. Par la suite, nous avons passé en revu les solutions de gestion de QoS dans les réseaux cœurs. Nous avons identifié trois principaux courants de standardisation: la QoS offerte par l'IMS (RACS), les architectures définies par l'IETF pour mettre en place la QoS dans l'Internet et la technique de l'ingénierie de trafic.

Même si aucune de ces architectures n'offre une solution complète pour la gestion de la QoS de bout en bout, elles forment une boîte à outils assez complète pour réaliser un service qui offre

une telle QoS de bout en bout. En particulier, un tel service nécessite un couplage entre les techniques de QoS dans le LAN et celles choisies au niveau des réseaux de cœur.

Dans le reste de ce mémoire, nous allons exposer nos solutions aux problématiques identifiées dans la thèse, à savoir l'accès à distance et la réservation de QoS dans le cadre d'un service de partage de contenus à distance. Les travaux d'études de ce chapitre nous ont été d'une grande utilité pendant la définition et la réalisation de nos solutions. En effet, ils nous ont permis d'identifier les manquements et erreurs à éviter, et les mécanismes nécessaires à la réalisation de nos solutions.

Chapitre 3

Système d'accès à distance pour le partage des contenus multimédias

Sommaire

3.1 Introduction

3.1.1 Problématique du service de partage de contenus

Dans le chapitre précédent nous avons identifié les deux verrous technologiques à résoudre dans ce travail de thèse : (i) l'accès à distance aux équipements pour le partage de contenus et (ii) la réservation de la QoS pour le transfert de ces contenus. Ce chapitre, nous a permis de comprendre les contraintes réseaux spécifiques qu'un service de partage de contenus nécessite. Nous avons aussi recensé les solutions existantes pour cette problématique, surtout celles proposées par les organismes de standardisation telle qu'UPnP et HGI. Nous avons montré les limitations de ces solutions et leurs inadéquations au contexte de partage de contenus. Dans le service de partage de contenus que nous étudions, l'utilisateur doit avoir la possibilité de donner l'accès à ses contenus, stockés dans sa maison, pour un ensemble de personnes qu'il désigne. Il doit aussi avoir la possibilité d'accéder à ses propres contenus depuis l'extérieur. Le service de partage proposé doit remplir l'ensemble des contraintes d'un service de partage à distance que nous avons identifiées dans l'état de l'art :

- la sécurité de l'accès;
- la confidentialité des contenus échangés;
- la garantie de la QoS pendant le transfert des contenus;
- la résolution du conflit d'adressage entre les réseaux locaux des utilisateurs et la traversé des pare-feux & des NAT.

De plus, l'expérience utilisateur de ce service doit être identique aux échanges des contenus dans les réseaux locaux avec DLNA et UPnP A/V. En effet, les principales étapes d'utilisations de ce service sont :

- Etablissement d'une session sécurisée vers un réseau local distant: pendant cette phase le client doit être authentifié et autorisé avant de lui permettre d'établir des sessions avec le correspondant distant ;
- Parcourt des répertoires partagés : une fois que le client a établi une session sécurisée vers le réseau local distant, il commence par parcourir les répertoires aux quels le propriétaire de ce réseau lui a donné accès ;
- Consommation des contenus : après l'étape de parcours des répertories, le client choisit un contenu pour le visualiser ;
- Fermeture de la session : à la fin de sa visite du réseau local distant, le client ferme la session pour préserver la sécurité du réseau de son correspondant et libérer les ressources qu'ils ont été allouées.

3.1.2 Décomposition du problème

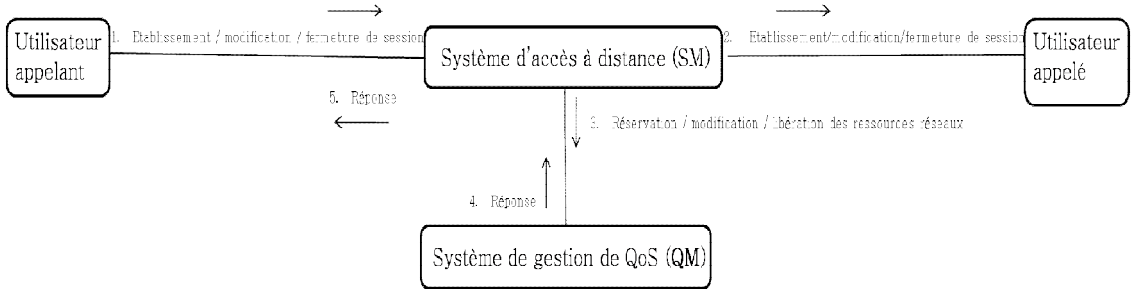


Figure 3.1 Décomposition du problème

Notre contribution dans la réalisation de ce service a consisté à spécifier une architecture du plan de contrôle du réseau permettant de résoudre les verrous technologiques que nous avons identifié. Pour simplifier le traitement de notre problématique, nous avons découpé notre travail en deux systèmes comme le montre la figure 3.1:

- Système d'accès à distance (Session Manager **SM**): Il définit une architecture réseau pour l'accès à distance à un réseau local distant pour permettre l'établissement des sessions sécurisées entres des terminaux distants. Cette architecture couvre les contraintes exprimées par le service de partage : sécurité, résolution de conflit d'adressage, traversé du pare-feu et des NAT.
- Système de gestion de QoS (QoS Manager **QM**): Il est en charge de garantir un niveau de QoS suffisant pour les sessions établies par le système d'accès à distance et assurer une garantie d'expérience (Quality of Experience **QoE**) élevée pour les utilisateurs du service.

Outre l'analyse fonctionnelle de ces systèmes et leur intégration dans l'architecture générale du service de partage, nous avons participé au sein du projet Feel@Home à l'étude de leur réalisation technique.

Dans ce chapitre nous allons exposer le nouveau système d'accès à distance. Nous commençons la présentation par une analyse fonctionnelle du système dans son cadre général qui est le projet européen Feel@Home. Après cette étape de spécification, nous exposons l'étude technique pour la réalisation de notre système. Nous expliquons dans cette partie les deux solutions techniques que nous avons proposée: une basée sur le Framework IMS et une deuxième dédiée au déploiement sur internet en utilisant des relais applicatifs HTTP (proxy).

3.2 Analyse fonctionnelle du système d'accès à distance

Etant donné que le système d'accès à distance que nous étudions est une brique du service de partage de contenus du projet Celtic Feel@Home, nous débutons cette partie par la présentation de l'architecture générale de ce dernier service. Ensuite, nous exposons une spécification fonctionnelle haut niveau du système d'accès à distance et nous donnons enfin les implémentations proposées dans le cadre du projet Feel@Home.

3.2.1 Contexte général : système Feel@Home

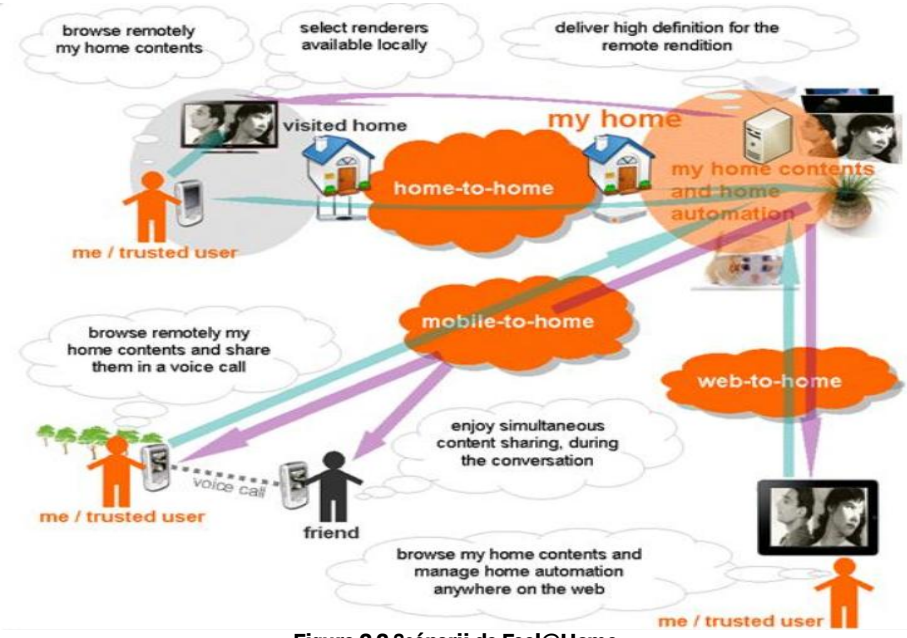


Figure 3.2 Scénarii de Feel@Home

Le scénario principal étudié par Feel@Home est le partage de contenus à distance au sein d'une grande communauté d'utilisateurs. D'autre scénarii sont étudiées (Figure 3.2), tel que le partage des services de la maison avec d'autre utilisateurs ou la commande des équipements de la maison à distance (Home automation). La contribution de cette thèse s'est limitée au scénario

du partage de contenus à distance, mais en étudiant de façon générique la problématique de l'accès à distance à une maison (quelque soit l'objet auquel nous souhaitons accéder).

Indépendamment de la technique à utiliser, le projet s'est fixé l'objectif de définir une architecture fonctionnelle générique pour la réalisation de son système.

Un seul choix technologique a été pris dans cette architecture, il consiste à utiliser UPnP A/V comme technologie pour la gestion des contenus dans la maison. Ce choix a un impact dans l'architecture de Feel@Home, vu qu'il impose l'utilisation de l'architecture UPnP. Cependant, ce choix a été guidé par l'état du marché dans le domaine du partage de contenus multimédias dans un réseau local. UPnP A/V et DLNA sont effet les deux standards largement implémentés par l'industrie multimédia, que ce soit au sein des TV, des consoles de jeux, des ordinateurs, des téléphones, des tablettes ….

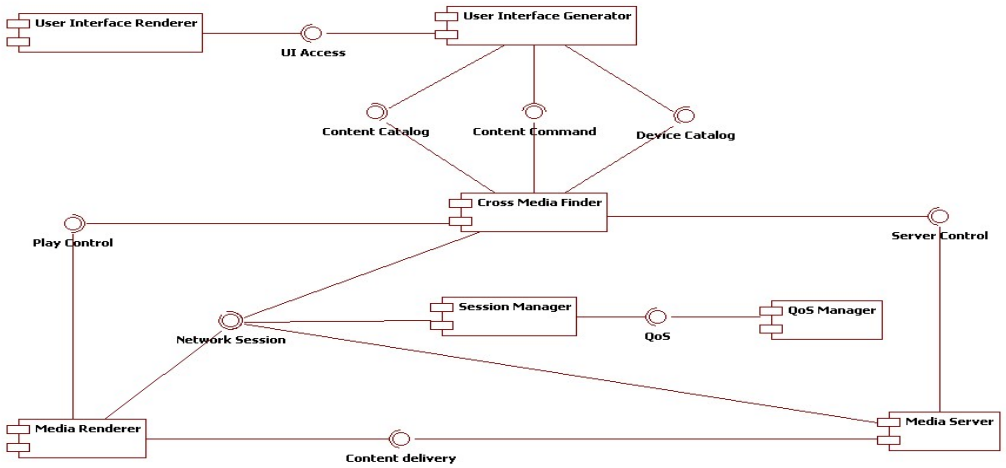


Figure 3.3 Diagramme de composantes du système Feel@Home

La figure 3.3 illustre tous les composants du système Feel@Home entrant en jeu dans le scénario du partage de contenus:

User Interface Renderer : Il affiche l'interface (GUI Graphic User Interface GUI) qu'offre le système Feel@Home à ses utilisateurs. Ce composant reçoit et transfère les requêtes des utilisateurs. Ce composant peut être un navigateur web (i.e. dans le cas d'un accès web) ou une application UPnP (Control Point A/V ou Media Player).

User Interface Generator : Le serveur qui génère les GUI à présenter à l'utilisateur.

Media Server : A cause du choix de la technologie de gestion de contenus dans le réseau domestique, ce composant va jouer le rôle d'un serveur de média UPnP A/V;

Media Renderer : Pour la même raison que précédemment, ce composant va jouer le rôle d'un lecteur de contenus media UPnP A/V.

Cross Media Finder (CMF): Ce composant implémente la partie métier (logique) du service de partage de Feel@Home. L'expérience de l'utilisateur distant avec ce service doit être la même que celle offerte par UPnP A/V en local. Le **CMF** va s'annoncer dans le LAN comme un Serveur UPnP A/V Virtuel (VMS) qui permettra à l'utilisateur via le Point de Contrôle UPnP A/V standard de:

- Annoncer dans le LAN la liste des amis avec lesquels il partage ses contenus. Ils vont être présentés comme les répertoires du VMS;

- Parcourir les répertoires que ses amis lui partagent;
- Récupérer des contenus distants et les jouer sur le lecteur de médias local.

Le **CMF** embarque aussi une interface qui permet au client de configurer ses règles de partage.
Session Manager (SM) : Ce composant correspond à notre système d'accès à distance. Il a en charge la gestion des sessions entre les équipements distants pour permettre au **CMF** d'accomplir ses fonctionnalités. Le **SM** doit gérer les droits d'accès aux contenus de la maison pour garantir leur confidentialité. En plus, il prend en charge la résolution de la problématique de la traversée du NAT et du Pare-feu. Ce composant peut aussi déclencher une réservation de QoS pour les sessions établies.

QoS Manager (QM): Ce composant correspond à notre système de gestion de QoS de bout-en-bout. Il offre la possibilité de réserver des ressources réseaux pour le transfert des contenus multimédias entre les équipements distants.

L'interaction entre ces composants se fait à travers les interfaces suivantes :

User Interface Access (UI Access) : Interface pour récupérer et afficher la GUI dans le User Interface Renderer. Elle est implémentée par le User Interface Generator.

Content Catalogue: Interface pour récupérer le catalogue de l'utilisateur qui correspond à la liste des amis qui lui partagent des contenus.

Content Commande : Interface pour commander la récupération du contenu (play, stop, etc).

Player Control : Cette interface permet le contrôle du lecteur de contenu (Media Renderer). Cela inclue la sélection du contenu, la négociation du protocole de transport et la commande de l'affichage du contenu.

Server Control : Interface entre le Media Server et le **CMF** pour localiser et configurer les contenus à partager dans le LAN.

Content Delivery : Interface permettant l'envoi du contenu directement du Media Server vers le Media Renderer.

Network Session : Interface responsable de l'établissement de la relation entre le Media Renderer et le Media Server indépendamment de la technologie réseau utilisée.

QoS : Interface en charge de la réservation, la configuration et la garantie de la QoS.

3.2.2 Etude fonctionnelle du système d'accès à distance

La présentation du cadre général du système d'accès à distance nous a permis d'identifier les acteurs externes à ce système. Ces acteurs sont :

- L'administrateur: Entité chargée de la gestion des ressources réseaux et responsable des souscriptions des clients au service Feel@Home;
- Le client: L'utilisateur final de ce système est le composant **CMF**.

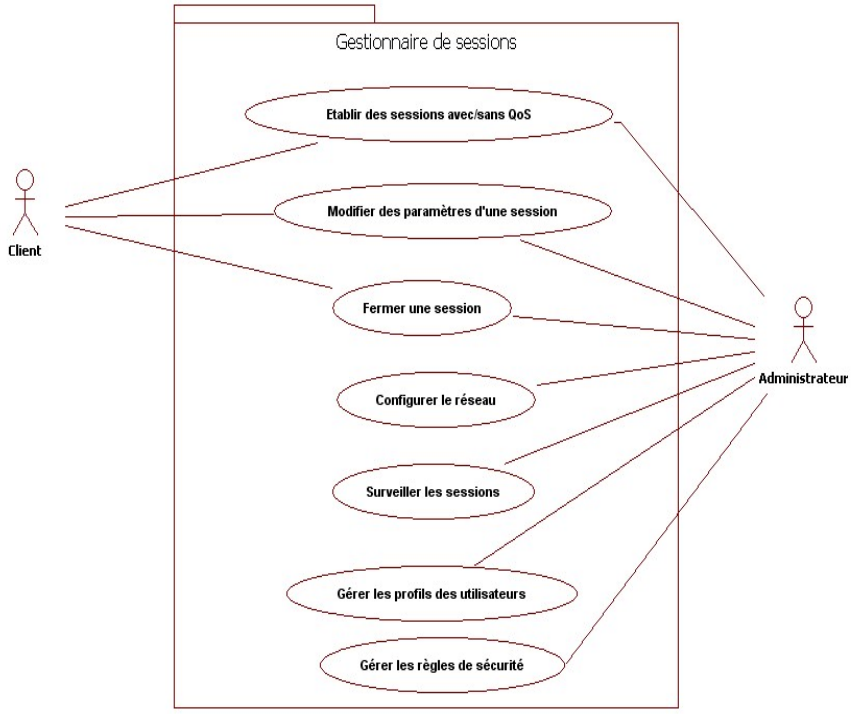


Figure 3.4 Diagramme de cas d'utilisation du système d'accès à distance

Le système d'accès à distance a pour objectif de résoudre la première problématique identifiée dans le chapitre de l'état de l'art, qui consiste à mettre en relation des équipements distants pour permettre l'échange des contenus multimédias.

La figure 3.4 décrit les cas d'usage de notre système:

- Etablir des sessions avec/sans garantie de QoS : Le client a la possibilité d'établir une session avec un correspondant distant en toute sécurité. Le client peut demander de la QoS à cette nouvelle session. La gestion de QoS des sessions est prise en charge par le composant **QM** que nous détaillerons dans le chapitre suivant ;
- Modifier des paramètres d'une session : Le client peut modifier les paramètres de sa session en fonction de son utilisation. Par exemple, pendant la phase de parcours des répertoires distants l'utilisateur n'a pas besoin de réserver de la QoS, mais, pendant la phase de la récupération du contenu, il aura besoin d'une garantie de la QoS pour répondre aux contraintes réseaux qu'impose le transfère de ce contenu (bande passante, délai limité);
- Fermer une session : A la fin de la communication, le client (source/destination) doit terminer sa session pour libérer les ressources allouées à cette session;
- Configurer le réseau: L'administrateur prépare son réseau en configurant les ressources dans son réseau pour l'éventuel trafic qui va être généré par les clients du service pendant la phase d'invocation;
- Surveiller les sessions: L'administrateur peut surveiller les sessions de ses clients ;
- Gestion des profils des clients: L'administrateur sauvegarde pour chaque client un profil. Ce profil contient ses données d'authentification et ses droits (les contenus auxquels il peut accéder, le degré de QoS auquel il a droit …) ;
- Gérer les règles de sécurité : Le système doit définir des règles de sécurité, que le client (**CMF**) peut configurer, afin de garantir la confidentialité des contenus des clients et la sécurité de leur réseau.

En étudiant les cas d'utilisation du système d'accès à distance, nous pouvons les répertorier en deux groupes:

- ceux dédiés à la configuration et à la gestion du service de partage de contenus (configurer le réseau, surveiller les sessions, gérer les profils) ;
- et ceux dédiés à la phase d'invocation (utilisation) du service de partage de contenus (établir/modifier/libérer une session).

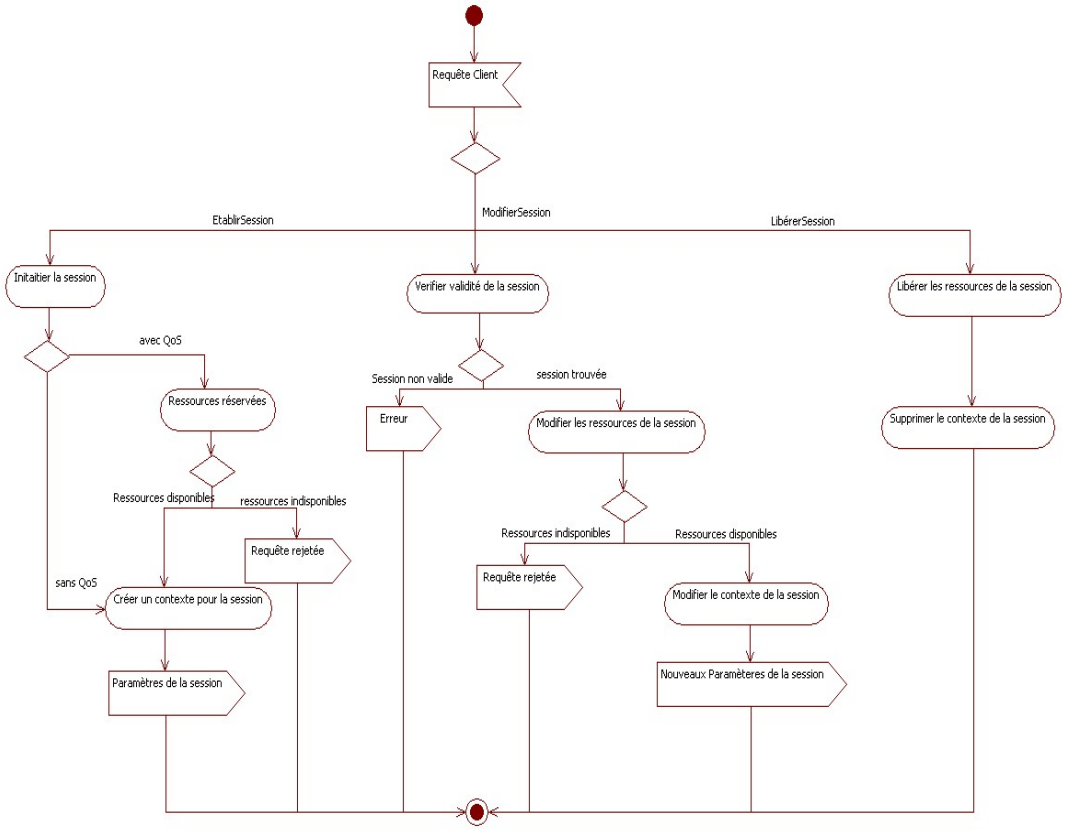


Figure 3.5 Diagramme d'activité du système d'accès à distance

Afin de concevoir une architecture générique de ce système, indépendante de la technologie, nous avons défini le comportement de ce système pendant sa phase d'invocation. Ce comportement est illustré par le diagramme d'activité de la figure 3.5.

Le système d'accès à distance peut recevoir trois types de requêtes pendant cette phase:

- Requête de réservation: Pour établir une nouvelle session, le client (**CMF**) envoie une requête à son **SM**. Ce dernier initie la session en démarrant la phase de négociation des paramètres entre les deux protagonistes de la session. Ensuite, si le client a demandé une garantie de la QoS, il va essayer de mettre en place une réservation de bout-en-bout en envoyant une requête au **QM**. Si la réservation a réussi, les paramètres de la nouvelle session seront transmis au client. Un message de rejet est envoyé à la source si la négociation avec le destinataire a échoué ou bien si l'éventuelle réservation de ressources n'a pas abouti. Si l'établissement de la session se termine avec succès, le **SM** crée un contexte pour cette nouvelle session et renvoie ses paramètres au client (**CMF**);
- Requête de modification : Lorsque le client (**CMF**) a besoin de modifier les paramètres de l'une de ses sessions, il envoie une requête de modification à son **SM**. Ce dernier vérifie l'existence de la session : s'il ne trouve pas le contexte de la session demandée un signal d'erreur est retourné, sinon il essaie d'effectuer la modification attendue (ex. envoi d'une

requête de réservation de ressources au **QM**). Le résultat de la modification est renvoyé dans le message de réponse ;

- Requête de libération : Une fois que le client (**CMF**) a terminé l'utilisation de sa session, il envoie une requête de libération à son **SM**. A la réception de cette requête, le **SM** libère les ressources allouées à cette session et supprime le contexte associé.

3.2.3 Réalisations du service de partage de contenus à distance de Feel@Home

Pendant cette phase, trois solutions techniques ont été proposées. En effet, le partenaire **Telefonica** a étudié une implémentation de ce service de partage en proposant un composant **SM** basé sur la technologie des VPNs.

La réalisation du **SM** dans la solution de **Telefonica** consiste à déployer un serveur central qui gère les règles de sécurité. Pour établir des communications sécurisées entre les clients, chaque maison doit initialiser un VPN permanent avec le serveur central afin de s'enregistrer au service de partage et être joignable depuis l'extérieur. De cette façon, toutes les communications entre les maisons distantes passeront systématiquement par le serveur central. Cela permettra de résoudre le problème de conflit d'adressage IP privé et la traversée du NAT et du pare-feu.

La sécurisation vient de l'utilisation des VPNs, mais aussi du stockage des règles de sécurité dans le serveur central. En effet, avant que ce dernier ne mette en relation deux correspondants (c.-à-d. transmettre l'adresse virtuelle privé du destinataire à la source), le serveur central vérifie que le demandeur possède bien le droit d'accéder à la maison et au contenu désigné.

Cette solution présente cependant un goulot d'étranglement qui est le serveur central. Le traitement de tous les trafics des clients (signalisations et données) par ce nœud risque de le surcharger et de diminuer ses performances, surtout pour un grand nombre d'utilisateurs. Un autre problème dans cette solution provient du stockage des droits d'accès aux contenus sur le serveur central. Le nombre potentiel de ces droits est très élevé et il peut devenir très délicat de les synchroniser et de récupérer l'information associée dans un délai acceptable.

Dans notre étude nous avons proposé des solutions permettant de contourner ses limitations tout en offrant le même niveau de sécurisation d'accès. En effet, nous avons proposé deux réalisations techniques du **SM**, que nous présenterons dans la section suivante, la première en utilisant le Framework IMS et la deuxième purement basée sur HTTP et dédiée à une application sur l'Internet

3.3 Réalisation du système d'accès à distance

Notre approche pour réaliser le système d'accès à distance, a été de proposer une architecture fonctionnelle de ce système indépendante de la technologie à utiliser, ceci afin d'éviter les lacunes des solutions rencontrées dans l'état de l'art. Ensuite, nous sommes passés à l'étude des technologies les plus adéquates pour la réalisation de cette architecture. Tout au long de cette partie, nous expliquerons plus en détail la méthode et l'approche choisie.

3.3.1 Architecture du système d'accès à distance

Après la modélisation UML (Unified Modeling Langage) [57] haut niveau de notre système d'accès à distance et de son contexte, nous étions en mesure d'élaborer une architecture fonctionnelle générique qui prenne en compte les besoins fonctionnels identifiés dans cette modélisation.

Nous avons tout d'abord étudié le déploiement des différentes fonctions sur les trois réseaux concernés : les deux réseaux domestiques et le réseau du fournisseur de service (par la suite nous généraliserons notre approche à ***N*** fournisseurs de service). Une fois la distribution des

fonctions réalisées, nous avons élaborés les différentes relations entre ces fonctions et ainsi nous avons pu produire les diagrammes de séquences des différents messages échangés. Ce premier cycle nous a permis de raffiner la constitution des différentes macro-fonctions avant d'instancier notre modèle sur le Framework IMS et sur une base HTTP.

La figure 3.6 illustre l'exemple où Bob partage des contenus avec Alice. La solution se base sur deux composants distribués entre le réseau cœur (**SM-WAN**) et le réseau LAN du client (**SM-LAN**).

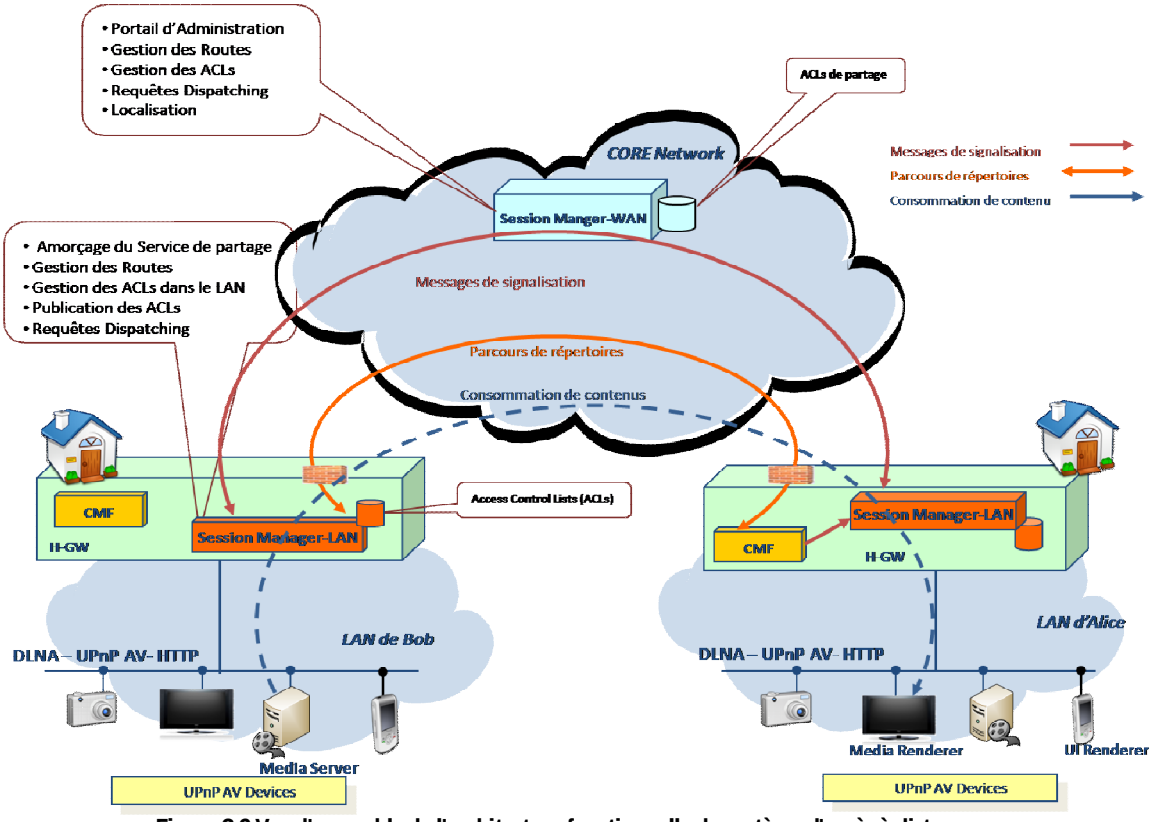


Figure 3.6 Vue d'ensemble de l'architecture fonctionnelle du système d'accès à distance

Afin de garantir la sécurité des échanges, nous avons défini deux types de Liste de Contrôle d'Accès (ACL Access Control List) qui régissent les droits d'accès :

- Règles de partage : Elles autorisent un utilisateur distant à accéder au LAN du client;
- Règles de filtrage : Elles désignent la liste des utilisateurs distants qui ont le droit d'accéder à un répertoire donné. Elles servent aussi à contrôler certaines actions UPnP: par exemple si le client partage des contenus avec un ami, le **SM** lui permettra alors d'effectuer des actions UPnP telles que BROWSE (parcours de répertoire) et GET (récupération de contenu) sur la liste de répertoires auxquels il a le droit d'accéder; mais par défaut le **SM** interdira pour des raisons de sécurité les autres actions UPnP comme DELETE (suppression de contenu) et MOVE (déplacement de contenu). Toutefois, le client pourra autoriser tous les types d'actions UPnP pour des utilisateurs privilégiés (ex. le propriétaire accédant de l'extérieur à sa maison).

Les deux types d'ACL sont stockés dans le composant du LAN (**SM-LAN**), alors que seules les règles de partage sont exportées dans le composant du réseau cœur (**SM-WAN**). La sauvegarde de ce type d'ACL à l'extérieur du LAN nous permet d'assurer la sécurité des réseaux des clients en vérifiant au moment de l'établissement de la session si l'appelant a le droit d'accéder au LAN désigné. La décision de ne pas exporter les règles de filtrage dans le réseau cœur nous évite le

problème de synchronisation de ces règles et diminue la complexité du traitement à réaliser par ce composant. Ainsi ce dernier aura une meilleure performance et une meilleure aptitude au passage à l'échelle pour gérer une grande communauté de clients. Mais au-delà de la considération technique, c'est également une contrainte juridique qui nous a poussés à ce constat. En effet, un fournisseur de service est responsable de toutes les données publiées y compris les métadonnées (tag, type, vignette …) associés à ces contenus. La liste des ACLs de filtrage peut être assimilée à des métadonnées donc soumises à contrôle. Ainsi, en plus du problème de synchronisation viendrait s'ajouter le problème de contrôle qui saturerait ainsi rapidement les performances du système.

De plus, pour améliorer les performances du nœud central, **SM-WAN**, nous avons décidé d'échanger les flux médias pendant la phase consommation des contenus directement en mode point-à-point entre les deux réseaux locaux distants et sans passer par le **SM-WAN**.

Le tableau 3.1 résume les fonctions des deux composants du **SM**. Dans ce tableau nous n'avons pas détaillé les fonctions qui font le lien avec le système de gestion de QoS pour la mise en place de la QoS de bout-en-bout, car nous allons les étudier en détail dans le chapitre 4.

Tableau 3.1 Fonctions du système d'accès à distance

Composant	Fonctions	Description
SM-LAN	**Amorçage du Service de partage**	▪ Enregistrer la maison du client au lancement du service de partage de contenus afin qu'elle soit accessible de l'extérieur.
	Gestion des ACLs dans le LAN	▪ Gérer les règles de filtrage et de partage dans la maison.
	Publication des ACLs	▪ Exporter les règles de partage vers le composant du réseau cœur.
	Gestion des Routes	▪ Lancer la négociation afin d'établir une session sécurisée entre l'appelant et l'appelé. ▪ Mettre en place les règles de routage dans le LAN émetteur du contenu (configuration du NAT& pare-feu) pour permettre l'échange de données point-à-point sans passer par le composant **SM-WAN**.
	Requêtes Dispatching	▪ Identifier et filtrer les requêtes entrantes. ▪ Rediriger les requêtes entrantes vers l'équipement stockant le contenu. Cela nécessite le stockage d'information d'indexation des contenus dans le LAN.
SM-WAN	**Portail d'Administration**	▪ Gérer les profils des clients. ▪ Surveiller les sessions des clients.
	Gestion des ACLs	▪ Configurer les règles de partage.
	Gestion des Routes	▪ Authentifier l'appelant. ▪ Identifier les requêtes de l'appelant. ▪ Vérifier les règles de partage de l'appelant.
	Requêtes Dispatching	▪ Transférer les messages de négociation entre les deux extrémités de la session.
	Localisation	▪ Localiser les maisons par rapport à un identifiant.

Cette architecture fonctionnelle est utilisable pour l'accès du client à son LAN en situation de nomadisme. Il suffit d'embarquer le composant **CMF** et les deux fonctions du **SM-LAN** :

« Amorçage du service » et « Gestion des Routes », dans l'équipement utilisé (i.e. ordinateur portable).

3.3.2 Implémentation IMS du système d'accès à distance

3.3.2.1 Présentation de la solution IMS

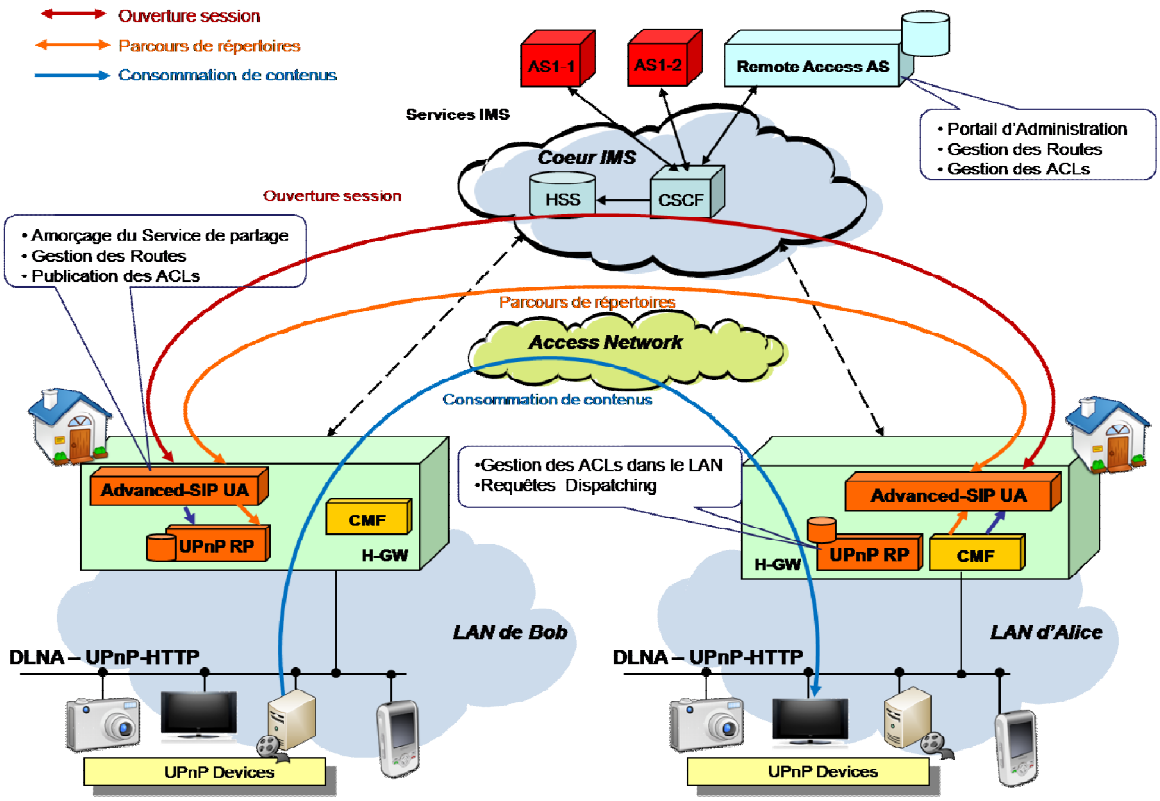


Figure 3.7 Architecture de la solution IMS

L'architecture IMS permet d'établir des sessions sécurisées entre deux nœuds distants pour l'échange de flux médias, sous la demande d'un SIP User Agent (SIP UA). Même si l'IMS a été conçue à la base pour l'utilisation des protocoles RTP et RTSP (Real Time Streaming Protocol) [67] très employés par les services de Voix sur IP, il peut être adopté pour transporter tous types de flux médias. En effet, la signalisation SDP (Session Description Protocol) envoyée dans les messages SIP est utilisée pour décrire le type des flux médias échangés dans cette session. Comme nous l'avons vu dans la partie état de l'art, les organismes de standardisation (HGI) ont proposé d'utiliser un adaptateur SIP/UPnP dans les deux réseaux locaux distants à mettre en relation. Vu qu'UPnP utilise le protocole HTTP pour la signalisation et le transfère des flux, cette adaptation impose d'effectuer la correspondance entre SIP et HTTP au niveau de la signalisation et RTP (RTSP) et HTTP au niveau du transfert des flux. Les contraintes d'implémentations ont empêché les constructeurs d'équipements réseaux de proposer des passerelles domestiques avec de telles fonctionnalités qui sont dignes d'un ordinateur plus que d'un équipement réseau embarqué possédant peu de ressources mémoire et de calcul.

Afin d'éviter cette adaptation, nous proposons d'utiliser IMS pour établir une session HTTP sécurisée en place de la session RTP standard établie par la signalisation SIP. Nous utilisons les messages SDP embarqués dans SIP pour indiquer aux deux correspondants que la session à mettre en place est une session HTTP. Ainsi, à la fin de la négociation SIP, les deux équipements UPnP distants pourront utiliser leur session HTTP pour s'échanger du contenu directement sans

passer par une plate-forme centrale dans le réseau de cœur (**SM-WAN**), comme si ils étaient rattachés au même réseau domestique.

La figure 3.7 illustre l'implémentation de notre architecture générique d'accès à distance utilisant l'IMS.

Nous avons implémenté le composant **SM-WAN** sur la base d'un Application Server (AS) IMS que nous nommons par la suite RA-AS (Remote Access Application Server). Un déclencheur sera ajouté dans le nœud CSCF dans le cœur IMS pour transférer les messages de signalisation SIP de notre service de partage vers le RA-AS. Ces messages seront identifiés par le domaine utilisé (i.e. feelathome.org). Les fonctions d'authentifications des appelants, la localisation et la fonction « Requêtes Dispatching » sont déjà implémentées par le Framework IMS.

Pour la fonction de « Gestion des ACLs », nous avons réutilisé les fonctionnalités de gestion de présence de l'IMS. Les règles de partage sont stockées dans le RA-AS en tant qu'indication de présence. Par exemple pour autoriser Alice à accéder au LAN de Bob le RA-AS maintien l'information que la ressource « maison de Bob » est présente pour le client « Alice ». Ces informations de présence sont respectivement publiées et notifiées par les messages SIP PUBLISH et SIP NOTIFY. Un utilisateur accède à la liste de ses amis en souscrivant au service à l'aide du message SIP SUBSCRIBE. En retour, il reçoit cette liste via les messages SIP NOTIFY. Une nouvelle autorisation est effectuée à l'aide d'un message SIP PUBLISH. Ce fonctionnement est similaire à celui utilisé par les mécanismes de messagerie instantanée reposant sur SIP (i.e. JABBER).

Afin d'assurer la sécurité des LANs des clients, le RA-AS prendra en charge la fonction de « Gestion des Routes » en se basant sur les informations de présence stockées. Un portail est aussi déployé dans le RA-AS pour permettre à l'administrateur de créer et de gérer les profils de ses clients.

Nous avons séparé le composant **SM-LAN** en deux parties : un « Advanced SIP-UA » qui est un SIP User Agent et un « UPnP Reverse Proxy » (UPnP RP) qui est un proxy applicatif inverse. Nous avons personnalisé ces deux éléments comme suit, afin qu'ils implémentent les fonctions du composant **SM-LAN**.

La fonction d' « Amorçage du service de partage » est assurée par l' « Advanced SIP-UA ». En effet, en vue de lancer le service de partage, ce composant doit s'enregistrer auprès du serveur RA-AS déployé dans l'IMS. Cette étape permet non seulement d'authentifier et d'enregistrer l'utilisateur mais surtout de rendre la maison du client visible à ses amis. L' « Advanced SIP-UA » implémente aussi la fonction « Gestion des Routes » qui permettra aux clients d'établir des sessions HTTP sécurisées avec des correspondants distants. La dernière fonction prise en charge par ce composant est la « Publication des ACLs ».

Finalement, l'« UPnP RP » assurera les fonctions de « Gestions des ACLs » et de « Requêtes Dispatching ».

Dans la suite, nous présentons une description détaillée de notre solution IMS. Nous exposons au début la spécification des SDP que nous proposons pour l'établissement des sessions HTTP. Nous enchainons ensuite par la description détaillée du fonctionnement de notre système pendant toutes les phases d'utilisation du service de partage de contenus. Et pour terminer, nous présentons le processus de validation réalisé qui consiste à une simulation UML du système spécifié.

3.3.2.2 Description détaillé de la solution IMS

Spécification du SDP

Pour négocier les paramètres de la session HTTP, nous avons défini des messages SDP spécifiques à notre système de partage. Il s'agit plus de transporter des paramètres nécessaires à l'établissement de la session HTTP que de nouveau message proprement dit. Les attributs des messages SDP sont utilisés pour décrire les médias portés par la session SIP (qui sera modifiée selon que l'utilisateur parcours le catalogue ou qu'il récupère un contenu). Un premier média est initialisé avec la session SIP (message SIP INVITE) pour le parcours du catalogue puis un deuxième média est ajouté suite à la modification de la session SIP (message SIP RE-INVITE) pour la consommation du contenu. Ces nouveaux paramètres s'inscrivent dans un bloc « m= ». Aussi, nous avons défini de nouvelles propriétés privés en utilisant l'attribut standard « a= » du protocole SDP comme suit :

a=FHUser :<User Name> Ce champ désigne le nom de l'utilisateur (ou bien son identifiant) qui souhaite accéder à une maison distante. Il sera utilisé par la fonction «Gestion des Routes » du RA-AS et au niveau de l'UPnP RP pour vérifier les droits de cet utilisateur.

a=FHSession :<Catalog | Content > Une session comportant un premier flux est utilisée au début pour parcourir les répertoires distants partagés par les amis de l'utilisateur. Donc, par défaut la valeur de ce champ est positionnée à « Catalog ». Lorsque le client choisit de récupérer un contenu donné, le système doit modifier la session afin d'ajouter un nouveau flux; la valeur de ce champ est alors positionnée à « Content ».

a=FHIpClient :<IP address> Ce champ permet de transmettre dans le SDP l'adresse IP publique de la passerelle domestique de l'appelant. Cette adresse IP va servir à configurer le pare-feu de la passerelle domestique de l'appelé. À son tour, le SIP UA de l'appelé se sert de ce champ pour transmettre son adresse IP public à l'appelant.

a=FHUrl :<UPnP URL> Ce champ indique l'URL direct pour récupérer le contenu choisi, sans passer par le RA-AS.

Nous recommandons aussi de mettre les deux champs standards indiquant la nature de l'application et le protocole de transport comme suite : « m=upnp » et «m=application http ».

Fonctionnement détaillé de la solution IMS

Gestion des règles de sécurité

i) Récupération de la liste des partages

Lorsque le client lance son service de partage à distance, son « Advanced SIP-UA » s'enregistre dans le cœur IMS de son fournisseur de service. Il souscrit ensuite au service de partage de contenus en envoyant un message SIP SUBSCRIBE vers le RA-AS. En retour, il récupère, via des messages SIP NOTIFY, la liste des contacts qui partagent des contenus avec lui. Ce fonctionnement est la procédure standard de la gestion de présence de l'IMS. En effet, le RA-AS, en plus de la gestion du service d'accès à distance implémente un service de gestion de présence.

ii) Configuration d'un nouveau partage

Notre système d'accès à distance permet à l'utilisateur de gérer ses règles de sécurité, qui définissent ses partages. La figure 3.8 illustre cette procédure.

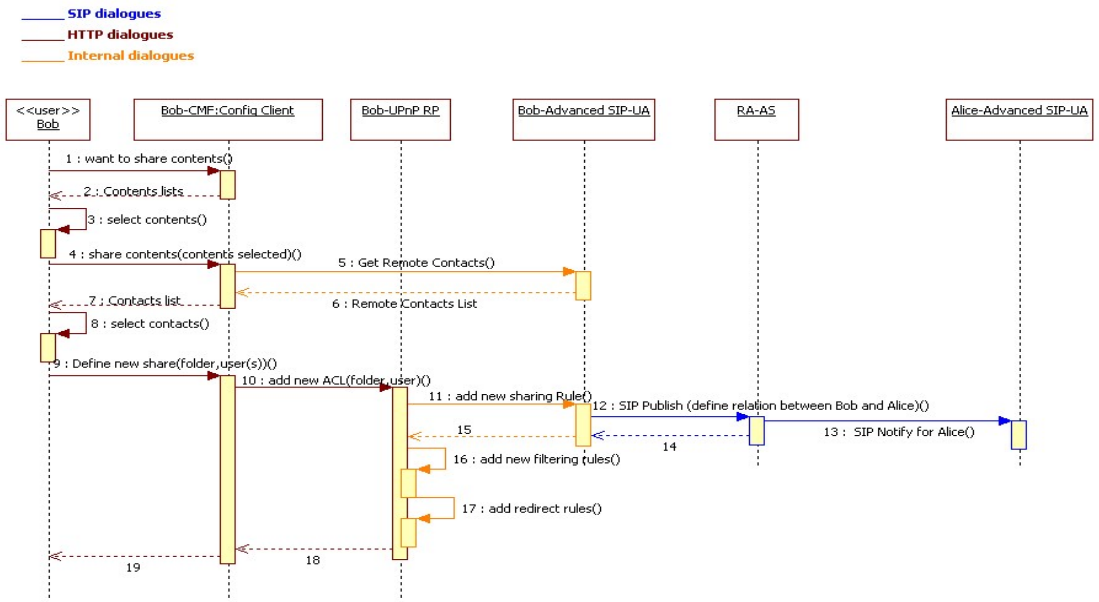


Figure 3.8 Configuration d'un nouveau partage avec un ami distant : solution IMS

Tout d'abord, avec son **CMF** (fonction Client de configuration), l'utilisateur sélectionne les contenus à partager (étapes 1-3) et les contacts avec qui il les partages (étapes 4-8). Ensuite, le **CMF** adresse la requête de l'utilisateur à son **SM-LAN** et plus précisément à son « UPnP RP » afin d'ajouter les règles nécessaires pour ce nouveau partage. L' « UPnP RP » demande à son « Advanced SIP-UA » d'exporter une nouvelle règle de partage au RA-AS (étape 11). L'« Advanced SIP-UA » envoie alors un message SIP PUBLISH au RA-AS (étape 12). Lorsque le RA-AS reçoit ce message, il met à jour sa base de données de présence et envoie un message SIP NOTIFY à l'« Advanced SIP-UA » de l'utilisateur concerné par ce partage (étape 13).

Lorsque le composant « UPnP RP » reçoit une réponse positive de son « Advanced SIP-UA », il stocke les nouvelles règles de filtrage et les informations d'indexation des contenus de ce nouveau partage (étapes 16-17). L'utilisateur peut préciser les actions UPnP A/V qu'il autorise pour ce partage. Par défaut, les actions DELETE et MOVE sont interdits pour des raisons de sécurité. Mais, il peut les autoriser pour des personnes privilégiées. Avec cette configuration, nous assurons que les requêtes reçues seront correctement acceptées et redirigées vers le bon UPnP Media Server stockant le contenu.

Et dans le cas où quelqu'un ajoute un nouveau partage pour le client pendant qu'il est connecté au service de partage, son « Advanced SIP-UA » reçoit un SIP NOTIFY de la manière décrite précédemment. De cette façon, l' « Advanced SIP-UA » maintient une liste à jour des LANs distants accessibles.

La sécurité repose sur deux briques essentielles. La première est la fonction d'identification et d'authentification de l'IMS qui ne laissera que les utilisateurs dûment authentifiés accéder au service de partage de contenus et donc de s'enregistrer auprès du RA-AS. En effet, grâce au mécanisme de gestion de présence, un utilisateur ne connait que les correspondants qui partagent des contenus avec lui. La deuxième brique de sécurité est assurée par la fonction « Gestion des Routes » du RA-AS qui effectue un filtrage sur la liste des correspondants avec lesquels un utilisateur peut établir une session.

Etablissement d'une nouvelle session

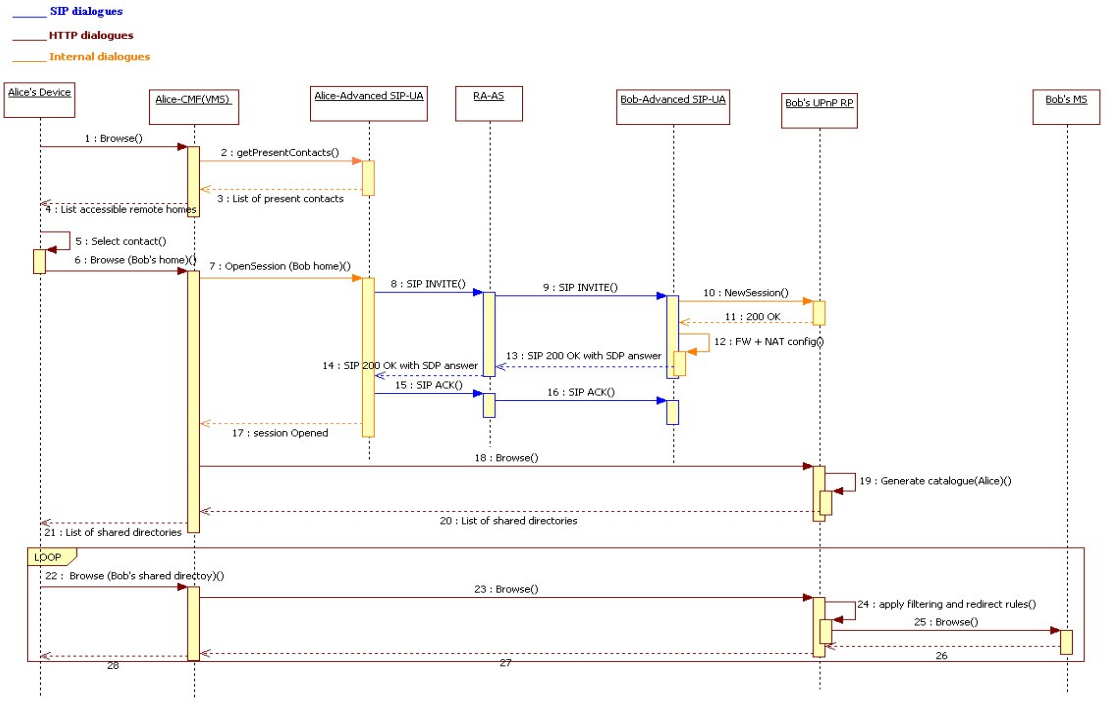


Figure 3.9 Parcours de répertoires distants : solution IMS

La figure 3.9 illustre l'établissement d'une nouvelle session entre deux utilisateurs (Alice et Bob) en vue de parcourir la liste des contenus partagés. Dans l'architecture du service de partage de Feel@Home, nous avons pris la décision de présenter la liste des LANs distants comme un VMS (Virtual UPnP Media Server) annoncé par le composant **CMF**. Ce choix avait pour but de concevoir un service de partage distant transparent aux équipements UPnP A/V et DLNA standards. Ainsi, quand le client souhaite parcourir le VMS (Virtuel Media Server) représentant ses partages distants, son **CMF** doit juste récupérer cette liste auprès de son « Advanced SIP-UA » (étapes 1-4).

Une fois que l'utilisateur (c.-à-d. Alice) a choisi son correspondant (Bob), il demande à son **CMF** (fonction VMS) de parcourir le catalogue que Bob partage avec elle (étapes 5-6). Par catalogue, nous voulons dire la liste des répertoires accessibles par l'utilisateur distant. Ce catalogue est construit dynamiquement en fonction des droits que Bob a octroyés à Alice. S'il s'agissait d'un autre utilisateur qu'Alice, le catalogue pourrait être différent. Le **CMF** d'Alice demande alors à son **SM-LAN** (composant : Advanced SIP-UA) d'ouvrir une nouvelle session vers le LAN de Bob (étape 7). A cette fin, un message SIP INVITE est envoyé par l'« Advanced SIP-UA » d'Alice vers celui de Bob. Le cœur IMS (nœud CSCF) transfère ce message vers le RA-AS tel que prévu par la règle de routage des messages SIP configurée par le fournisseur de service. Ainsi, le RA-AS va pouvoir vérifier qu'Alice a bien le droit d'accéder au LAN de Bob (étape 8). Si le RA-AS ne trouve pas une règle de partage concernant Alice vis à vis des contenus de Bob, un message SIP ERROR (Unauthorized ou Forbidden) est retourné à Alice. La session prend alors fin. En théorie, ce cas de figure ne doit pas se présenter dans la mesure où le **CMF** d'Alice ne présente que les contacts qui partagent au moins un contenu avec Alice (Cf. Gestion des règles de sécurité). Sinon, le message SIP INVITE est routé par l'IMS vers le LAN de Bob (étape 9).

L' « Advanced SIP-UA » de Bob accepte la requête d'ouverture d'une nouvelle session, vu qu'elle est authentifiée et autorisée par le cœur IMS. Le cœur IMS et le RA-AS joue le rôle de tiers de confiance vis-à-vis de Bob. A la réception de cette requête, l' « Advanced SIP-UA » configure le pare-feu de sa passerelle domestique afin d'autoriser les requêtes HTTP entrantes provenant du

LAN d'Alice et ajoute des règles de NAT de façon à rediriger ses requêtes vers l' « UPnP RP » (étape 12). Outre cette configuration, l' « Advanced SIP-UA » négocie les paramètres HTTP avec son « UPnP RP » (étape 10). En effet, le catalogue et les flux média sont échangés entre les deux LANs en utilisant HTTP pour éviter l'adaptation RTP/HTTP. Le résultat de cette négociation sera remis à l' « Advanced SIP-UA » d'Alice dans un message SIP 200 OK (étapes 13-16). La réponse d'établissement de la session est ensuite transférée au **CMF**. A ce stade, le **CMF** peut envoyer directement des requêtes de parcours HTTP vers le LAN de Bob. Ces requêtes seront correctement acceptées et redirigées vers l' « UPnP RP » qui aura la tâche de construire dynamiquement le catalogue de contenus que Bob partage avec Alice en se basant sur ses règles de filtrages (étapes 18-21). C'est durant ces échanges que les paramètres « a= » convoyés par les messages SDP prennent toute leur importance : le paramètre **FHIpClient** est utilisé dans la configuration du pare-feu et du NAT, **FHUrl** pour indiquer comment joindre la maison de Bob, **FHUser** pour construire dynamiquement le catalogue. Alice peut par la suite parcourir tous les répertoires retournés dans la réponse reçue par le **CMF** et choisir un contenu à regarder parmi ceux stockés dans ces répertoires (étapes 22-28).

Toutefois, le parcours d'un répertoire de contenus est différent de celui du catalogue de la maison. En effet, le **SM-LAN** ne peut pas indexer tous les contenus du LAN. Etant donné que la plupart des Media Server UPnP A/V mettent à jours fréquemment les index de leurs contenus (i.e. ajout/suppression d'un contenu), la synchronisation de ces index par le **SM-LAN** diminuera considérablement sa performance. De même, certains serveurs UPnP A/V mettent à jour leur index au démarrage. Donc, nous avons convenu d'appliquer les règles de filtrages uniquement sur les répertoires à partager. Et comme ces répertoires peuvent être stockés dans des Media Serveur différents, le **SM-LAN** (composant : UPnP RP) sauvegarde alors des règles de redirection qui permettent par la suite de retrouver le Media Server UPnP A/V qui contient le répertoire demandé.

Effectivement, lorsqu'Alice demande à parcourir un répertoire (i.e. le répertoire de photos) que Bob partage (étape 22), le **CMF** envoie une requête directe à l' « UPnP RP » de Bob (étape 23). Ce dernier vérifie toujours dans ses règles de filtrage si Alice peut accéder au répertoire désigné dans la requête (étape 24). La réponse à cette requête ne sera pas produite par l' « UPnP RP » mais par le Media Serveur UPnP A/V qui stocke ce répertoire. La requête est redirigée vers le Media Serveur adéquat grâce aux règles de redirection maintenues par l' « UPnP RP » (étape 25).

Comme nous pouvons le constater, nous n'avons pas eu recours à l'adaptation de la signalisation HTTP, utilisée par l'UPnP A/V, en signalisation SIP puisque notre proposition consistait à transférer cette signalisation entre les LANs distants via la session sécurisée établie avec IMS. Cela nous permettra de réduire la consommation de notre système en termes de CPU et mémoire au niveau de la passerelle domestique.

Modification des paramètres d'une session pour la récupération de contenu

La figure 3.10 illustre la consomation d'un contenu par l'utilisateur distant. Cette étape fait suite à la consultation du catalogue décrite précedemment.

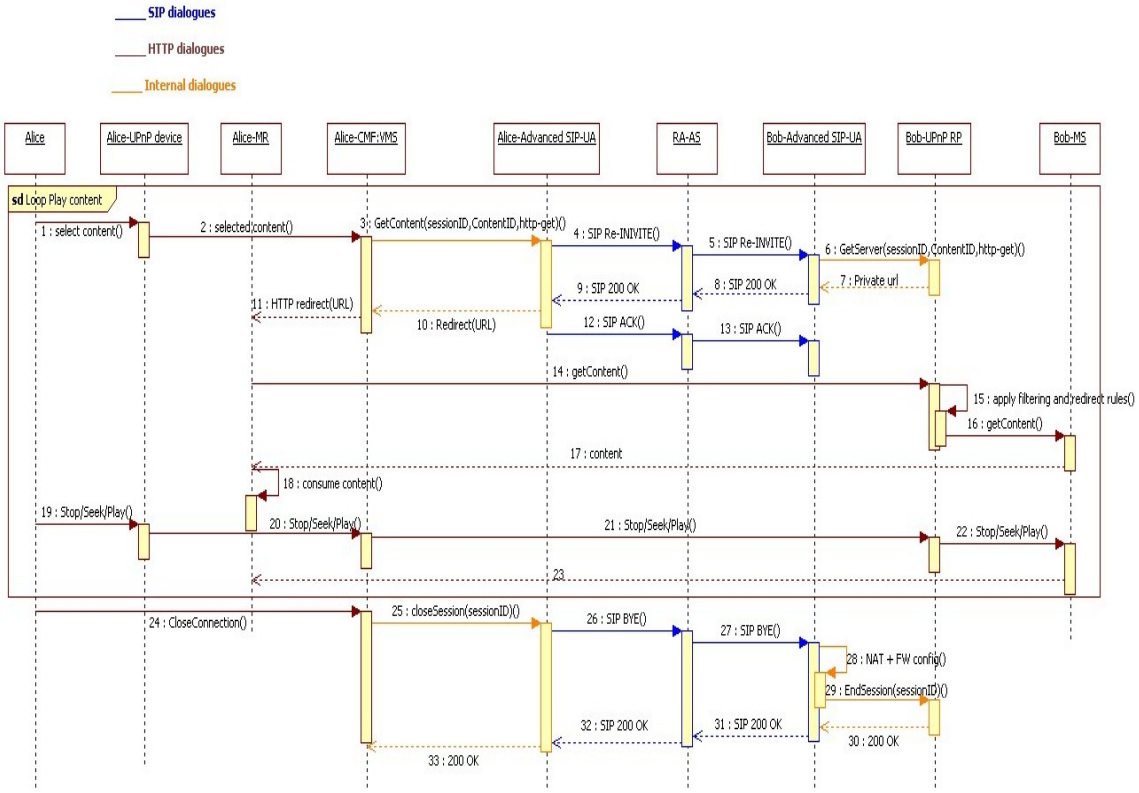


Figure 3.10 Lecture de contenu distant : solution IMS

Dès que l'utilisateur (Alice) choisit un contenu à jouer, son **CMF** contacte son **SM-LAN** pour lui demander de modifier la session établie pour récupérer ce contenu (étapes 1-3). Cette modification de la session SIP servira à ouvrir un nouveau média HTTP et éventuellement à réserver de la QoS pour ce média. A ce stade, les caractéristiques du contenu sont connues, donc le **CMF** peut décrire la QoS nécessaire au transfert. Nous détaillerons cette procédure de gestion de la QoS dans le chapitre suivant.

Un message SIP RE-INVITE est donc envoyé de l'«Advanced SIP-UA» vers la maison de Bob (étape 4). De la même manière que pour les messages SIP INVITE, ce message est transféré par le cœur IMS vers le RA-AS pour vérifier les droits de l'utilisateur à modifier cette session (i.e. demande de la QoS). La réponse à cette requête de modification sera forgée par l' « UPnP RP » du destinataire et contient les paramètres du nouveau média HTTP pour le transfert de contenu demandé. Cette réponse contient aussi un « HTTP redirect » qui pointe vers l'URL direct du Media Serveur stockant le contenu (étapes 6-10). La réponse de l' « UPnP RP » est relayée par l' « Advanced SIP-UA » dans la partie SDP du message SIP 200 OK (e.g. **a=FHUser**:bob.legrand@orange.fr; **a=FHSession**:Content; **a=FHUrl** :http://193.21.33.15/$0/$5/video12.avi).

A ce niveau et avec son **CMF**, Alice choisit un Media Renderer UPnP A/V pour lire le contenu indiqué par l'URL reçue dans le HTTP redirect (étape 11). La requête du Media Renderer d'Alice sera traitée par l' « UPnP RP » de Bob qui vérifie la méthode HTTP demandée par l'équipement distant et la transfère par la suite vers le Media Serveur stockant le contenu (étapes 15-16). Finalement, le flux média est transmis directement au Media Renderer distant depuis le Media Serveur de Bob (étape 17).

Alice a la possibilité de suspendre/arrêter/avancer la lecture du média reçu avec son UPnP *device* comme si le Media Serveur était rattaché à son LAN (étapes 19-23). Si Alice veut regarder

d'autres contenus partagés par Bob, elle répète cette procédure (étapes 1-23) autant qu'elle le souhaite. Le SIP-REINVITE sert alors aussi bien pour la fermeture du média précédent que pour l'ouverture du nouveau média. Il peut donc y avoir une modification des règles de NAT et du pare-feu (mise à jour du champ HTTP redirect).

Fermeture d'une session

Lorsqu'Alice termine la consultation du catalogue de Bob, elle demande à son **CMF** de fermer la session établie avec le LAN de Bob (Fig. 3.9 étape 24). Ce dernier déclenche alors la procédure de fermeture de session au niveau de son **SM-LAN** (Advanced SIP-UA). Un message SIP BYE est envoyé vers le LAN de Bob. Ce message est transféré par le cœur IMS au RA-AS pour libérer les éventuelles ressources réservées à cette session et relayer ensuite le message vers l' « Advanced SIP UA » de Bob (étape 27).

A la réception de la requête de fermeture, l'«Advanced SIP-UA» supprime les règles du pare-feu & NAT ajoutées au moment de l'ouverture de la session (étape 28). A la fin, l'«Advanced SIP-UA» contacte son « UPnP RP » pour effacer le contexte des médias HTTP d'Alice (étapes 29-30) et envoie un message SIP 200 OK comme réponse au **CMF** d'Alice.

Echange inter-opérateurs

L'IMS a l'avantage d'avoir été conçu dans une optique multi-opérateurs. Avec cette solution, il est aussi possible de partager des contenus entre des utilisateurs gérés par des opérateurs différents. L'IMS est capable de router les messages entre les réseaux de plusieurs opérateurs en se basant sur le SIP URI (Unified Resource Identifier). Pour réaliser ce scénario, chaque opérateur doit déployer dans son domaine un RA-AS et ajouter un déclencheur dans son réseau pour transférer les messages SIP du service de partage vers son RA-AS.

Une synchronisation entre les RA-AS est nécessaire lorsqu'un client d'un opérateur A ajoute un nouveau partage pour un client d'un opérateur B. Quand le RA-AS de l'opérateur A ajoute une nouvelle règle, il la transfère au RA-AS de l'opérateur B pour notifier son client de ce nouveau partage. A nouveau, nous utilisons les mécanismes standards de la gestion de présence pour échanger les notifications.

Si le client de l'opérateur B veut mettre en place une session pour accéder aux contenus du client de l'opérateur A, le RA-AS de l'opérateur B vérifie que son client peut contacter le client de l'autre domaine avant que le cœur IMS de B ne route la signalisation SIP vers le réseau de A. Les droits du client de B sont vérifiées par le RA-AS de l'opérateur A. Une fois que le deuxième RA-AS donne son accord à l'établissement de la session, le message SIP INVITE est délivré au destinataire.

Le comportement des étapes restantes pour l'établissement de la session demeurent les même.

3.3.2.3 Simulation UML

Environnement de simulation

Nous avons choisi l'outil TauG2 [58] pour réaliser nos simulations. Cet outil possède un ensemble de logiciels permettant la modélisation des systèmes complexes avec le langage UML et il offre la possibilité de simuler le modèle spécifié. La simulation UML proposée par TauG2 repose sur la définition de tests à l'aide des diagrammes de structures UML.

La définition des scénarii est réalisée à l'aide d'une interface graphique pour en faciliter la description. Les traces d'exécution de ces scénarii sont présentées à l'utilisateur sous formes de diagrammes de séquences ou bien de diagrammes d'états. L'utilisateur se trouve en mesure de

détecter les erreurs et corriger aisément son scénario afin de vérifier les paramètres et les états des différents composants du système au cours de la simulation.

Rappelons que la simulation fournie par TauG2 ne constitue pas une preuve formelle du modèle. Elle nous permet de détecter des erreurs de conception afin de les corriger avant de passer à la phase d'implémentation. Une validation par simulation ne nous permet que de terminer alors la phase de modélisation UML de notre système avec une certaine garantie, a priori non totale, dépendant de l'effort de simulation, que le modèle conçu ne présente pas de défauts de conception.

Scénarii de simulation

Afin de réaliser nos simulations, nous avons repris la conception du service de partage définie dans Feel@Home. Nous avons alors défini les machines d'états de tous les composants de ce service. Dans cette section, nous allons nous contenter de présenter les machines d'états des composants de notre système d'accès à distances SM.

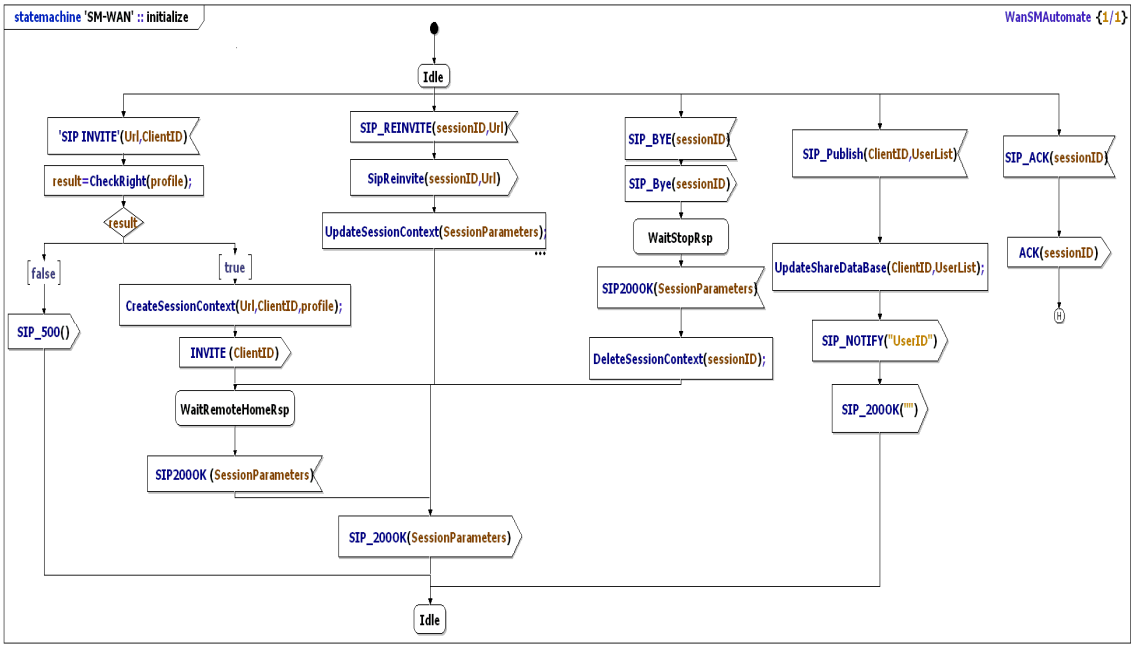


Figure 3.11 Machine d'état du RA-AS sans gestion de QoS

La Figure 3.11 présente la machine d'états du RA-AS. Comme nous pouvons le constater, cette machine ne comporte pas la phase d'authentification de l'utilisateur vu que celle-ci est assurée d'une façon très forte par le Framework IMS. Nous n'avons pas aussi intégré les fonctionnalités du portail d'administration (i.e. la création/suppression de compte pour un client) dans ce diagramme. Les fonctionnalités que nous avons détaillées sont essentiellement la gestion des droits d'accès et la gestion d'une session entre deux réseaux domestiques distants. Ces fonctionnalités nous ont permis de valider tous les scénarii que nous avons définis.

Pour le composant « Advanced SIP-UA », nous avons défini deux machines d'états distinctes. L'une contient le traitement des requêtes provenant de l'intérieur du LAN (Fig. 3.12) et l'autre la réception des requêtes reçues de l'extérieur du LAN (Fig3.13).

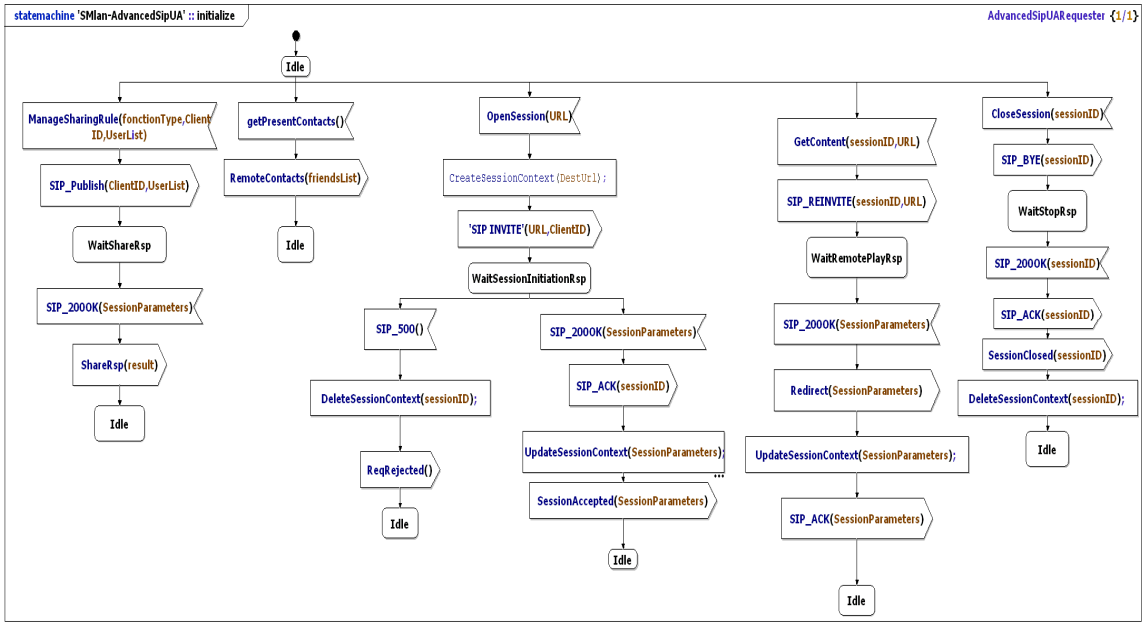


Figure 3.12 Machine d'états de l'Advanced SIP UA côté LAN

La première machine d'états de l'« Advanced SIP-UA » décrit le comportement de ce composant lorsqu'il est sollicité par le CMF (i.e., l'ouverture/modification/fermeture de session ; la récupération de la liste des LANs distants accessibles) et par l' « UPnP RP » (ajout/mise à jour de règles de partage dans le RA-AS).

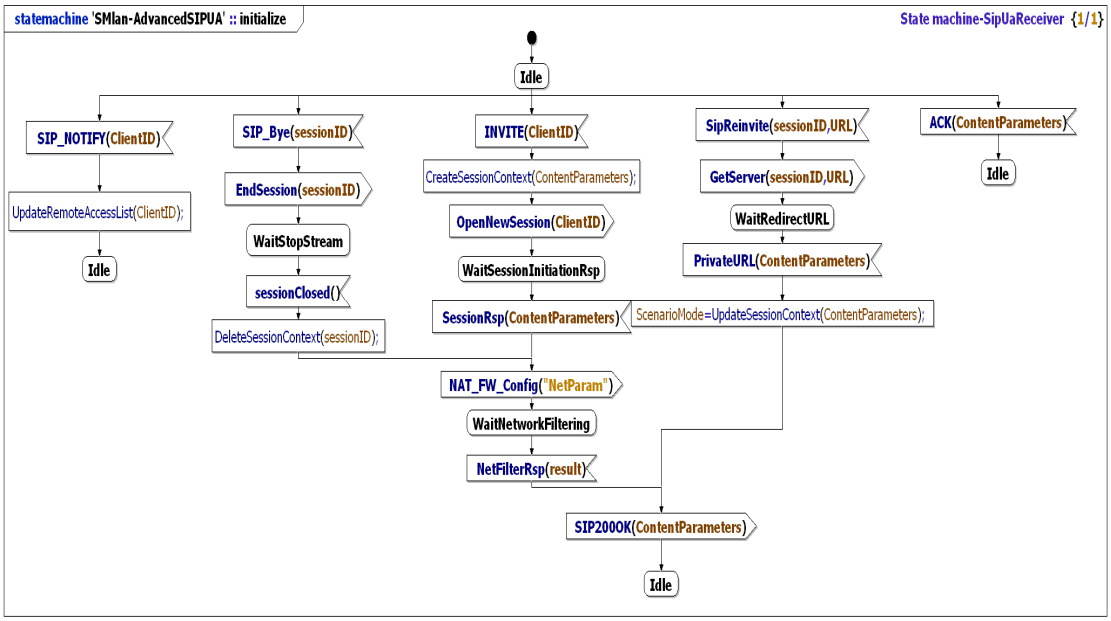


Figure 3.13 Machine d'états de l'Advanced SIP UA côté RA-AS

La deuxième machine d'état décrit le comportement du composant « Advanced SIP-UA » lorsqu'il reçoit des requêtes de l'extérieur du LAN provenant du RA-AS (ouverture/modification/fermeture de session).

La Figure 3.14 représente le comportement du composant « UPnP RP ». Les clients de ce composant sont :

- Le client de configuration du CMF pour configurer les partages (AddNewACLentry,

DeleteACLentry) ;

- L' « Advanced SIP-UA » pour ouvrir/fermer une session http (OpenNewSession, EndSession), ou bien utiliser une session http existante (H2HBrowse, GetServer) ;
- Un Media Server distant pour récupérer un contenu dans le LAN (GetContent) ;

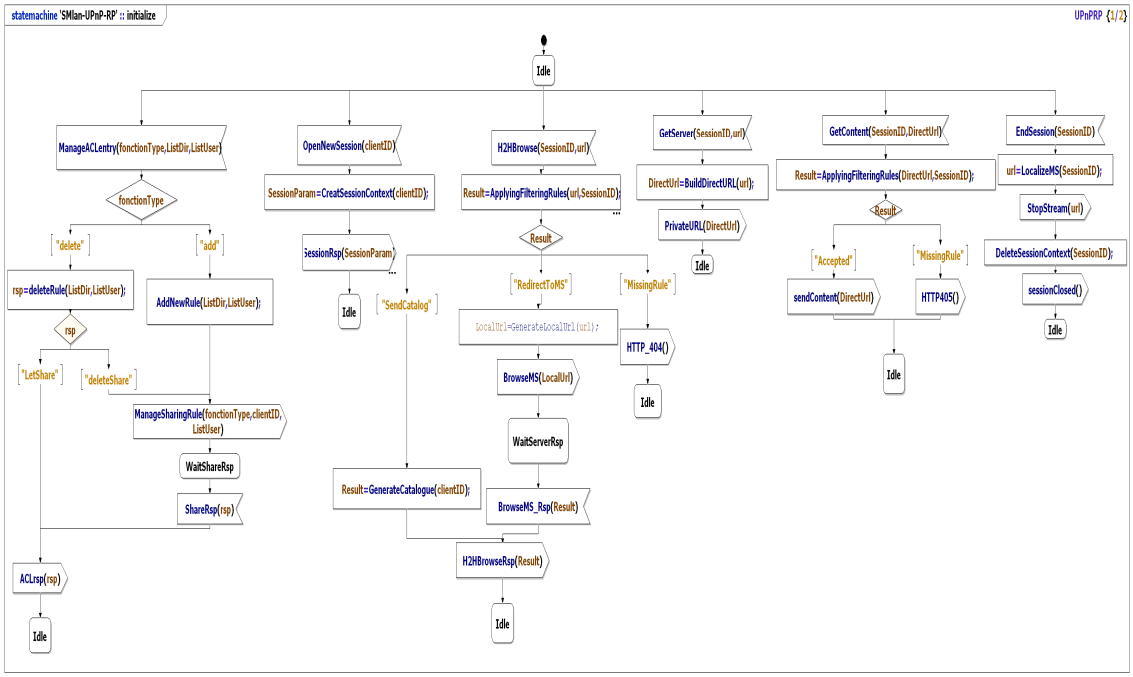


Figure 3.14 Machine d'états de l'UPnP-RP

Une fois les machines d'états de tous les composants du service de partage spécifiés, nous avons défini une série de tests dans le but de mettre en évidence puis corriger les erreurs de conception de ce service. Le tableau 3.2 liste cette série de tests. Nous avons réalisé deux types de scénario : les scénarii de configuration (i.e. ajout/suppression de partage) et les scénarii d'invocation (i.e. ouverture d'une nouvelle session).

Tableau 3.2 Scénarii simulés

Scénario	Description	Type
1	Ajout d'un nouveau partage.	Configuration
2	Suppression de partage.	Configuration
3	Parcours d'un catalogue distant.	Invocation
4	Parcours d'un répertoire distant.	Invocation
5	Lecture de contenu distant.	Invocation
6	Fermeture de session.	Invocation
7	Echec d'établissement d'une session à cause d'absence de droit d'accès au LAN désigné.	Invocation
8	Echec de lecture du contenu distant à cause d'absence de droit d'accès au contenu désigné.	Invocation

La première étape avant de débuter des simulations avec TauG2 est de préciser le diagramme de structure des composants entrant en jeu dans la simulation. Donc pour lancer nos simulations, nous avons proposé deux diagrammes de structures, un pour chaque type de scénario.

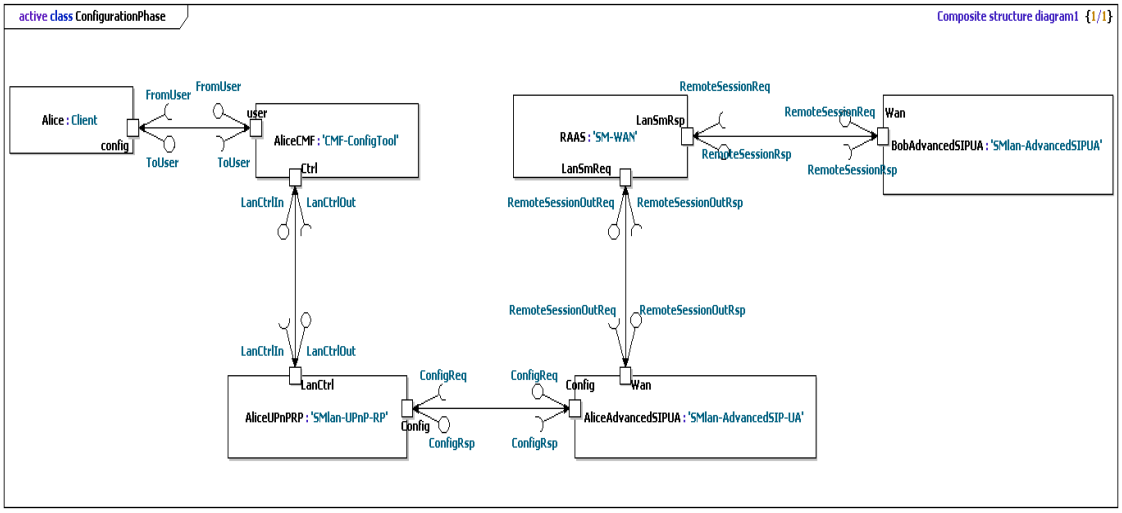


Figure 3.15 Diagramme de structure des composants entrant en jeu pendant la phase de configuration

La Figure 3.15 représente le diagramme de structure pour les scénarii de configuration (1&2). Ce diagramme est constitué d':

- un composant qui simule le comportement du client ;
- un Client de configuration du CMF, un « UPnP RP » et un « Advanced SIP-UA », du côté du LAN de l'utilisateur désirant configurer un partage ;
- un composant RA-AS ;
- un « Advanced SIP UA » du côté du LAN du client destinataire.

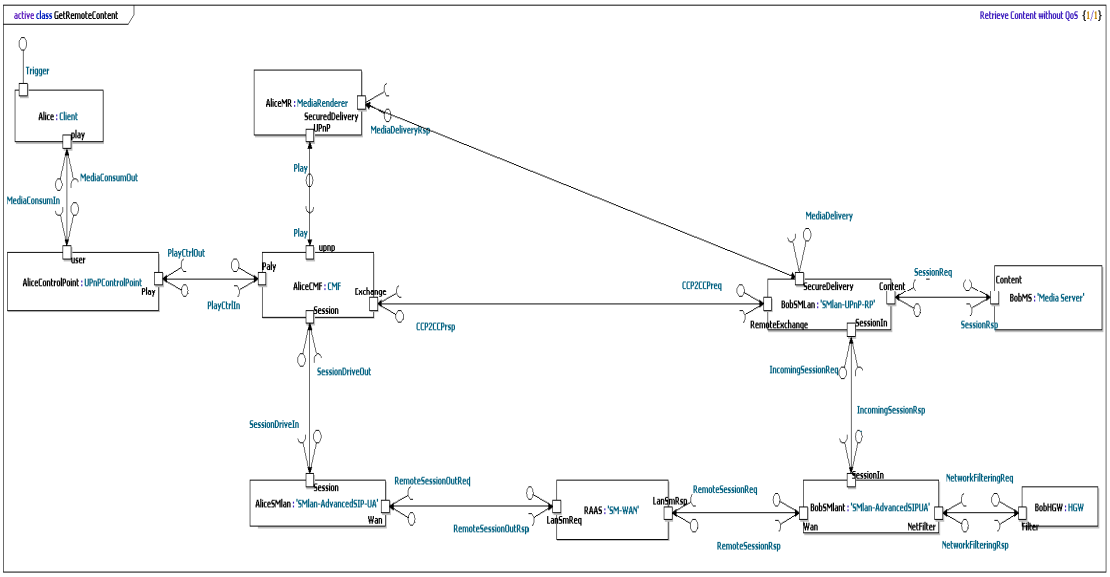


Figure 3.16 Diagramme de structure des composants entrant en jeu pendant la phase d'invocation

La Figure 3.16 représente le diagramme de structure pour les scénarii d'invocation (3, 4, 5, 6, 7&8). Il est constitué d' :

- un composant qui simule le comportement du client appelant (Alice);
- un **CMF** et un Advanced SIPUA, du côté du LAN de l'utilisateur appelant désirant accéder à des contenus distants ;
- un composant qui simule le comportement d'un point de contrôle UPnP A/V standard dans le LAN ;
- un composant qui simule le comportement d'un Media Renderer UPnP A/V;

- un composant RA-AS ;
- un « Advanced SIP-UA » et un « UPnP-RP » du côté du LAN du client destinataire (Bob);
- un composant qui simule le comportement d'un Media Server UPnP A/V;
- un composant qui simule le comportement de la passerelle domestique dans le LAN du destinataire (Bob);

Résultat des simulations

Nous avons choisi de générer les traces de nos simulations sous forme de diagrammes de séquences afin de les comparer avec celles que nous avons produites pendant la phase de conception.

A titre illustratif, nous exposons dans la suite les traces des principaux scénarii de tests. Elles sont produites respectivement par le scénario d'ajout d'un nouveau partage (Fig. 3.17), le scénario de parcours d'un catalogue distant (Fig. 3.18), le scénario de parcours d'un répertoire distant (Fig. 3.19), le scénario de lecture d'un contenu distant (Fig. 3.20) et le scénario de fermeture de session (Fig. 3.20).

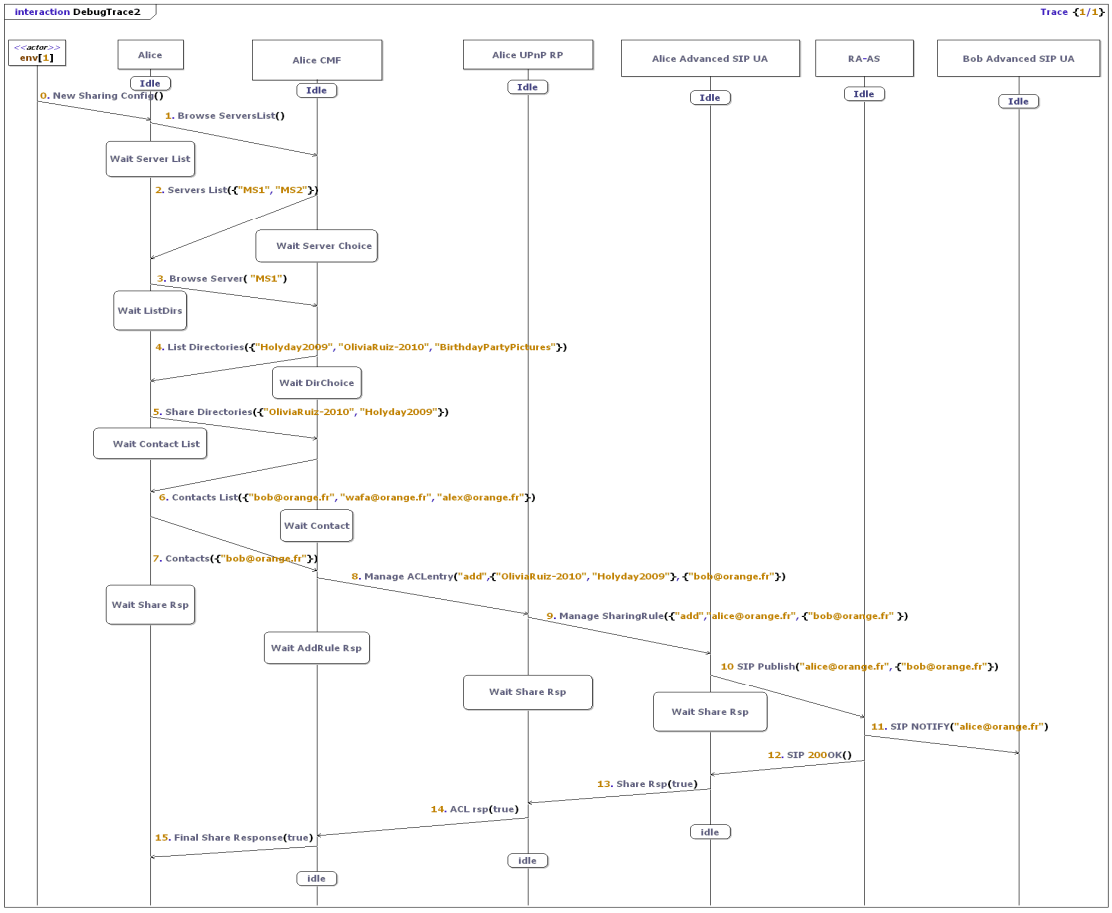


Figure 3.17 Trace de simulation d'un scénario d'ajout d'un nouveau partage

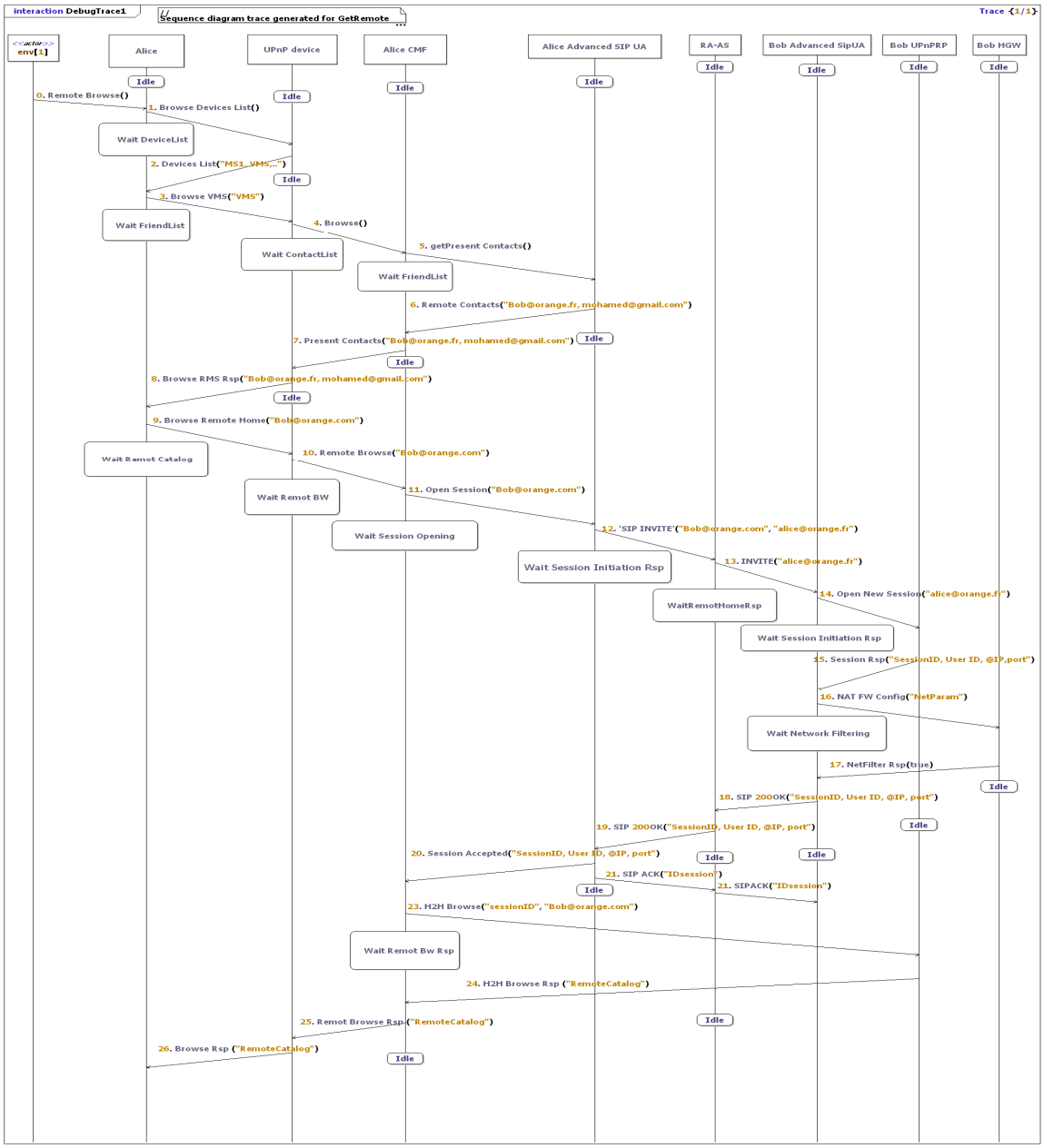


Figure 3.18 Trace de simulation d'un scénario de parcours d'un Catalogue distant

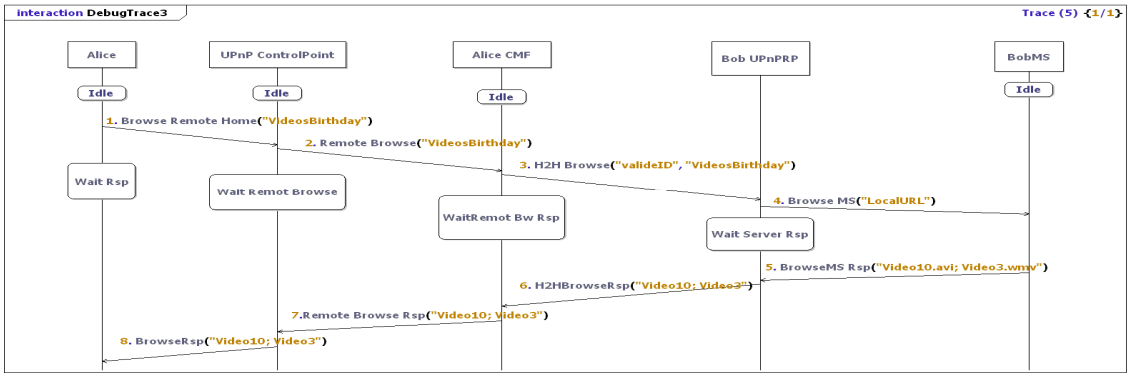


Figure 3.19 Trace de simulation d'un scénario de parcours d'un répertoire distant

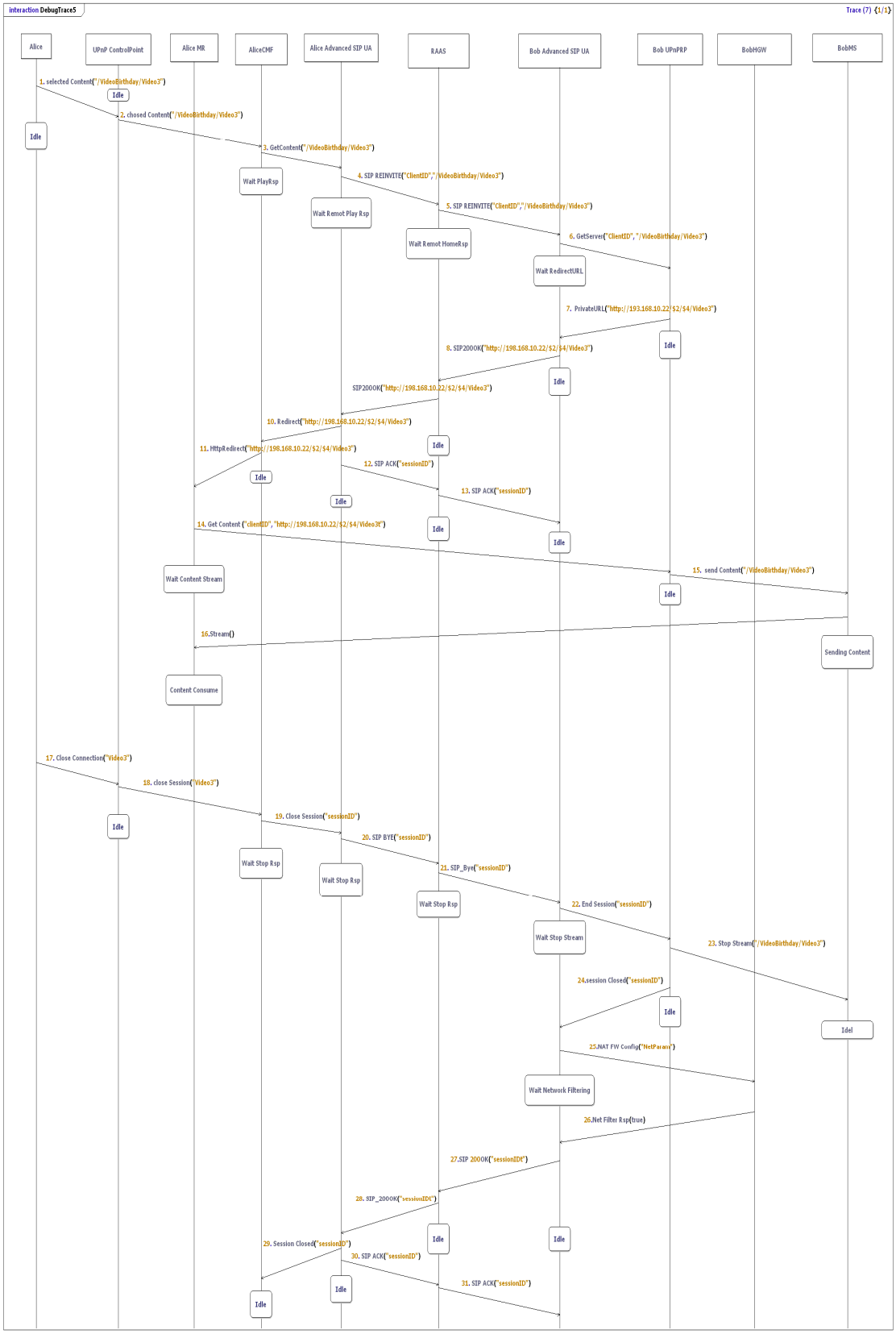


Figure 3.20 Trace de simulation des scénarii de Lecture de contenu distant & de fermeture de session

La simulation UML avec TauG2 nous a permis de valider fonctionnellement l'architecture proposée. Avec les traces fournies par l'exécution des scénarii de simulation, nous avons détecté quelques erreurs dans les machines d'états de nos composants. Ces erreurs ont provoqué le blocage de la procédure de mise en place des sessions. Nous avons alors pu les corriger et nous avons vérifié nos corrections en rejouant les mêmes scénarii.

3.3.3 Implémentation du système d'accès à distance pour l'Internet

3.3.3.1 Présentation de la solution HTTP

Comme nous avons pu le constater, l'utilisation du Framework IMS pour implémenter notre architecture d'accès à distance a facilité le déploiement du service de partage, car il permet l'utilisation d'un grand nombre de fonctionnalités déjà réalisées et offertes par ce Framework (i.e. authentification, localisation, QoS ...). Néanmoins, le choix d'IMS présente une limitation architecturale, puisqu'une telle solution ne peut être fournie que par la seule technologie IMS, et qu'elle ne peut être déployée que par un opérateur de télécommunication.

Dans cette section, nous allons présenter une autre conception et implémentation de notre architecture, qui sera maintenant cohérente avec le monde de l'internet. Nous avons nommé cette solution « Solution HTTP », car elle utilise directement le protocole HTTP pour gérer les sessions et pour le transport des flux.

L'idée principale de cette implémentation est de transmettre les messages de signalisation UPnP A/V (HTTP) entre les LANs distants à l'aide d'une chaine de proxys applicatifs situés : dans la maison appelante, dans le cœur du réseau et un dans la maison appelée (proxy inverse qui accepte les requêtes entrantes au LAN).

Cette chaine va garantir la sécurité des LANs des clients et mettre en place la configuration réseau nécessaire pour préparer le transfert du contenu directement de maison à maison, sans passer par le nœud central.

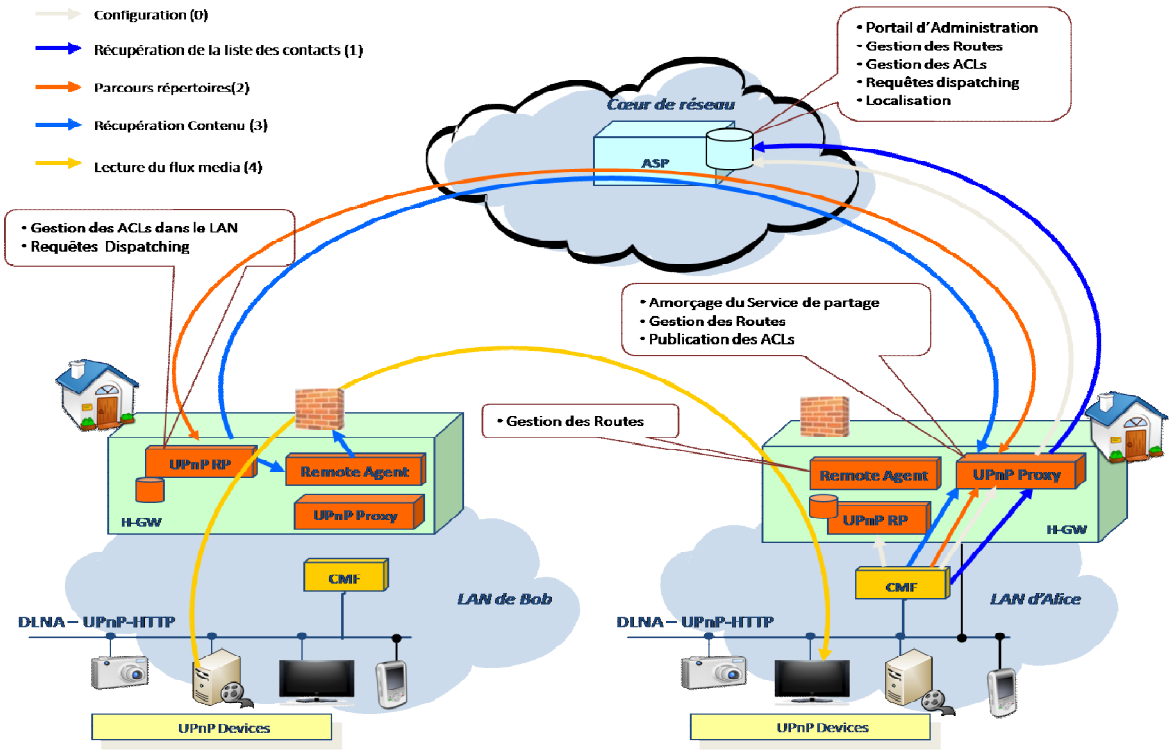


Figure 3.21 Architecture de la solution HTTP

L'architecture de la solution HTTP est illustrée par la Figure 3.21.

Dans cette solution, le composant **SM-WAN** (figure 3.22) est implémenté sous forme d'une plate-forme de services que nous avons appelée ASP « Authentication & Security Proxy Server ». Cette plate-forme est composée de trois éléments : un relais applicatif sécurisé (Proxy HTTPS), un service web et un serveur de noms dynamique (Dyn DNS) [68].

Le Proxy HTTPS assurera la fonction de la « Gestion de Routes » (c.-à-d. authentifier le client et vérifier son droit à effectuer la requête demandée). Généralement, les Proxy HTTPS possèdent des mécanismes d'authentification basés sur des certificats ou des systèmes nom d'utilisateur /mot de passe. Mais, il est possible de configurer ces outils afin d'utiliser d'autres systèmes d'authentification que l'opérateur ou le fournisseur de services utilisent déjà pour leurs clients.

Une fois que la fonction de « Gestion de Routes » a authentifié et autorisé la requête, le proxy HTTPS la relaie vers sa destination (Fonction « Requête Dispatching »).

La fonction de « Localisation » est prise en charge par le composant Dyn DNS qui permettra au Proxy HTTPS de trouver l'adresse IP publique de la maison destination. Cette fonction est spécialement utile dans le cas où le client est abonné à un fournisseur d'accès qui offre un accès xDSL allouant des adresses IP dynamiques (e.g. DHCP qui change l'adresse de la passerelle domestique chaque jour). Ainsi, chaque fois que la passerelle domestique obtient une nouvelle adresse, elle doit l'envoyer au Dyn DNS pour mettre à jour la base de données.

Le dernier élément formant l'ASP est un Web Service standard. Il implémente le « Portail d'administration » qui gère les profils des utilisateurs (i.e. identifiant, mot de passe, …). Il assure aussi la fonction de « Gestion des ACLs ». En effet, grâce à ce Web Service, le client aura la possibilité de configurer ses règles de partages, maintenues dans une base de données dans l'ASP. Avec cette base de données le Proxy HTTPS pourra vérifier les droits d'accès aux LANs distants.

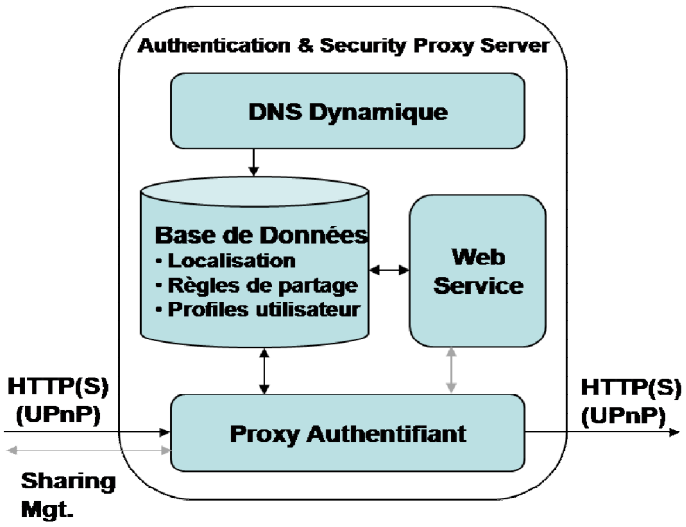


Figure 3.22 Composants du SM-WAN dans la solution HTTP

Nous avons décomposé le **SM-LAN** en trois éléments :

- Un UPnP Proxy (proxy applicatif) qui va traiter les requêtes sortantes du LAN (fonction « Gestion de Routes ») ;
- un UPnP Reverse Proxy (proxy inverse) qui va prendre en charge les requêtes entrantes au LAN (fonction « Requêtes Dispatching ») ;
- et un « Remote Agent » qui aura la tâche de configurer le pare-feu de la passerelle

domestique.

Pour rendre la maison accessible, le SM-LAN (UPnP Proxy) implémente la fonction d'« Amorçage du service ». La technique utilisée pour cette fonction est d'envoyer des messages de rafraichissement (i.e. keep alive) au Web Service de l'ASP pour lui indiquer que le LAN est accessible de l'extérieur pour la liste de ses amis. La gestion de cette liste et des règles de filtrage dans le LAN se fait de la même manière que dans la solution IMS à l'aide de l'UPnP RP (fonction « Gestions des ACLs »).

La fonction de « Publication des ACLs » est assurée nativement par l'UPnP Proxy. En effet, nous avons juste besoin que ce dernier relaie les requêtes de configuration du CMF vers le Web Service de l'ASP.

3.3.3.2 Description détaillée de la solution HTTP

Avant de commencer à utiliser le service de partage, le client doit être enregistré dans l'ASP. Pendant cette phase, l'utilisateur ou l'administrateur crée un compte pour le nouveau client en utilisant le portail d'administration de l'ASP. Si le Proxy HTTPS utilise les certificats pour l'authentification, l'administrateur envoie au client son certificat à la fin de cette phase.

Dans cette partie, nous allons expliquer plus en détail le fonctionnement de cette solution pendant toutes ses étapes d'utilisation.

Gestion des règles de sécurité

Configuration d'un nouveau partage

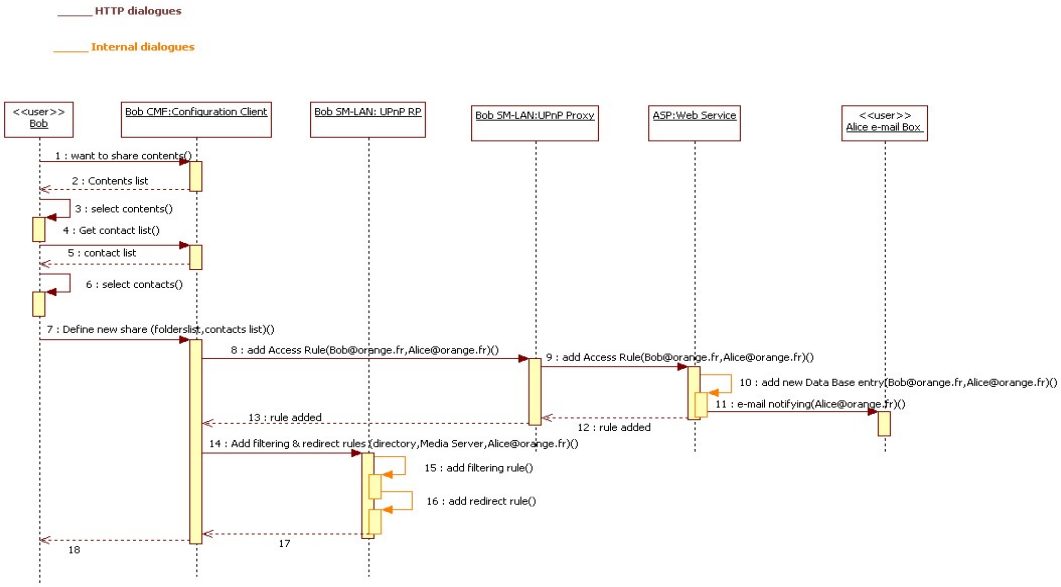


Figure 3.23 Configuration d'un nouveau partage : solution HTTP

Le premier cas d'utilisation de notre système d'accès à distance est la configuration des règles de sécurité (partage & filtrage). La Figure 3.23 illustre la réalisation de cette procédure.

Cette procédure reste inchangée, du point de vue « expérience utilisateur », entre la solution IMS et la solution HTTP : le client choisit avec son **CMF** (fonction client de configuration) la liste des contenus à partager (étapes 1-3) et la liste des contacts avec qui il les partage (étapes 4-6). Mais pour mettre en place ce nouveau partage, le **CMF** envoie une requête HTTP au Web Service de l'ASP via l'«UPnP Proxy», afin de mettre à jour sa base de données des règles de partage (étapes

8-12). La plate-forme ASP notifie le correspondant du client de ce nouveau partage (étape 13). Cette notification peut se faire à l'aide d'un simple e-mail, ou bien lorsque l'utilisateur se connecte à son service de partage. Pour terminer la configuration de ce partage, le **CMF** demande à l'«UPnP RP» d'ajouter les règles de filtrage et de redirection nécessaires (étapes 14-17). L'utilisateur peut aussi configurer les actions UPnP autorisées pour ce partage (e.g. action : BROWSE, MOVE).

Récupération de la liste des partages

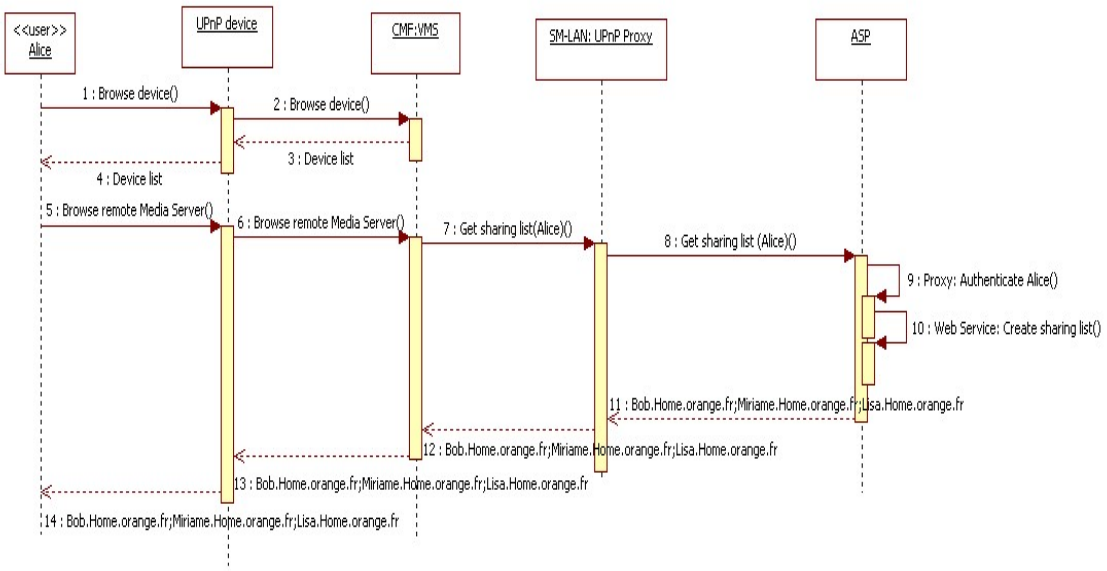


Figure 3.24 Récupération de la liste des réseaux domestiques accessibles à distance : solution http

Dans notre conception du service de partage à distance, nous avons convenu de présenter la liste des partages comme les répertoires d'un UPnP A/V Media Serveur standard annoncé par le **CMF** (fonction VMS). La figure 3.24 illustre la récupération de cette liste des partages. Le client (c.-à-d. Alice) réalise un BROWSE du VMS annoncé par le **CMF,** en utilisant un UPnP A/V Control Point standard (étapes 1-6).

Afin de construire la réponse à cette requête, le **CMF** envoie une requête de récupération de règles de partage au Web Service de l'ASP (étape 7). Cette requête est relayée par l'UPnP Proxy qui est configuré pour utiliser l'ASP comme proxy HTTPS pour toutes requêtes sortantes du LAN (étape 8). Dans l'ASP, le proxy HTTPS authentifie l'émetteur de la requête, puis redirige la requête vers le Web Service de la plate-forme ASP (étape 9). Le Web Service formule alors la liste des partages du client (c.-à-d. Alice) en se basant sur la base de données des droits d'accès de l'ASP (étape 10). Le Web Service retourne alors cette liste dans un format XML compatible avec les recommandations UPnP A/V (étape 11).

La réponse de l'ASP est reçue par le **CMF,** via l'UPnP Proxy (étapes 11-12), puis la transfère à son tour au *device* UPnP d'Alice sans réaliser aucune modification, car elle est UPnP A/V compatible (étape 13). Le client est maintenant capable de choisir, parmi cette liste, le LAN qu'il veut visiter. En effet, chaque maison partageant au moins un contenu avec l'utilisateur est présenté comme un répertoire du serveur de Média du **CMF** (VMS). Tout se passe pour le lecteur UPnP A/V comme si il avait à sa disposition dans le LAN un média serveur UPnP A/V qui comporte plusieurs répertoires (un par maison distante).

Etablissement de session

Comme pour la solution IMS, la première session établie avec un LAN distant sert à récupérer le catalogue et à parcourir les répertoires partagés par l'appelé à son visiteur. Les messages échangés pendant cette phase sont des fichiers XML non volumineux (sous format UPnP A/V) qui peuvent être envoyés avec le protocole HTTP. Nous avons alors pris la décision de ne pas établir une session point-à-point entre les LANs pendant cette phase et de faire relayer ces messages par l'ASP. En effet, contrairement à la solution IMS qui permet la mise en relation sécurisée de deux maisons, la solution HTTP n'offre pas de sécurisation permanente, mais juste pour un échange HTTP (i.e. envoie d'une requête HTTP GET et réception de la réponse). On pourrait qualifier la solution de «state less» en comparaison à la solution IMS qui est « state full ». Ce choix nous permet également de minimiser le temps d'ouverture des ports du pare-feu de la passerelle domestique et donc d'offrir plus de sécurité; et d'autre part de simplifier le fonctionnement des différents composants de notre système **SM** dans le LAN et dans le WAN. Ainsi, tous les messages échangés entre les deux maisons vont systématiquement passer par le proxy authentifiant du réseau. Dans cette partie, nous présenterons le rôle de notre système dans la mise en relation réseaux de deux LANs distants pour récupérer un catalogue ou pour parcourir un répertoire dans un LAN distant.

i) Parcours de catalogue distant

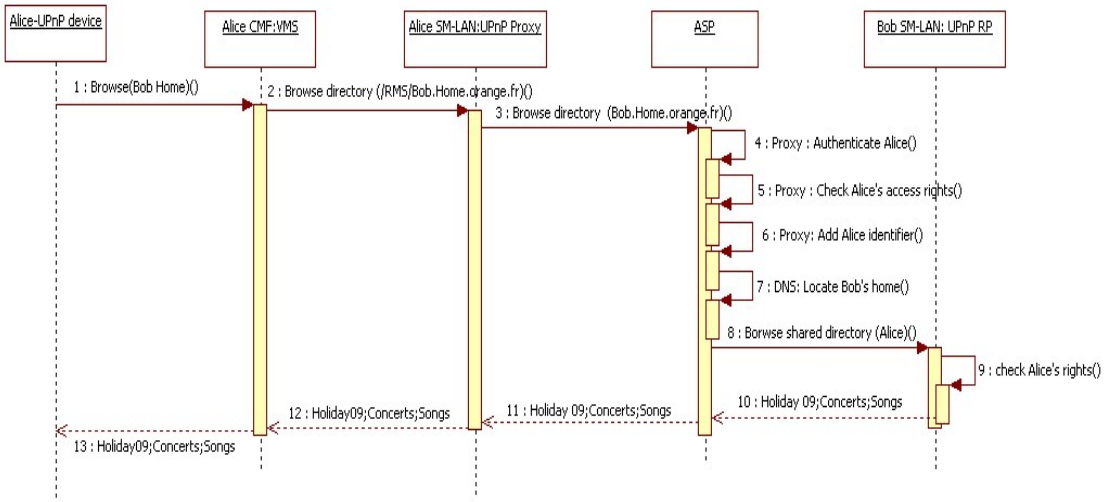


Figure 3.25 Parcours de catalogue distant : solution HTTP

Après le choix du correspondant (i.e. Bob), l'utilisateur (i.e. Alice) demande à son **CMF** (fonction VMS) de parcourir le catalogue que Bob partage avec elle (Fig. 3.25 étape 1). Le **CMF** (fonction VMS) formule une requête UPnP BROWSE standard pour parcourir le répertoire désignant la maison de Bob. Il demande à son **SM-LAN** (fonction UPnP Proxy) de transférer cette requête à la maison de Bob (étape 2). Comme d'habitude l'UPnP Proxy transfère ce message sortant du LAN vers le proxy de l'ASP grâce à sa configuration par défaut (étape 3).

En recevant ce message, l'ASP authentifie de nouveau Alice (étape 4). A ce stade, l'authentification peut être explicite (envoie d'un crédential ou nom_utilisateur / mot_de_passe dans la requête HTTP) ou implicite (en utilisant un cookie fourni par l'ASP suite à la première authentification qui a permis de récupérer la liste des amis). Il identifie la requête comme une requête inter-LANs, et procède à la vérification des droits de l'appelant (Alice) à accéder au LAN désigné dans la requête (LAN de Bob) (étape 5). Si l'ASP ne trouve pas de règle de partage indiquant qu'Alice a le droit d'accéder au LAN de Bob, il rejette la demande d'Alice et retourne un message d'erreur au **CMF** (« 404 not Found » ou « 500 unauthorized »). A nouveau ce cas d'erreur ne doit pas se produire dans la mesure où l'ASP n'a renvoyé à Alice que la liste des personnes qui partagent au moins un contenu avec elle. Cette vérification permet de rejeter

toute tentative d'usurpation du système (e.g. je force le contact avec Tom même si il n'est pas dans la liste proposée par l'ASP car je sais qu'il partage des contenus avec Bob). Dans le cas où Bob donne l'accès à son LAN à Alice, l'ASP localise le LAN de Bob à l'aide de son DNS dynamique (étape 7) et redirige ensuite la requête de BROWSE au LAN de Bob (étape 8). Afin d'éviter l'usurpation d'identité, l'ASP insère l'identifiant d'Alice dans la requête qu'il transfère à Bob (étape 6). Nous avons inséré cette information dans un champ entête (header X-FH-USER) de la requête HTTPS. De même que l'ASP vérifie que l'on contacte une maison qui partage effectivement au moins un contenu avec l'utilisateur, l'ASP est tiers de confiance pour l'identité du demandeur. Sans cette vérification, un utilisateur (e.g. Alice) pourrait se faire passer pour le propriétaire de la maison visitée (e.g. Bob) afin d'accéder à l'ensemble des contenus de la maison visitée.

Pour renforcer la sécurité des LAN des clients, au lancement du service de partage, la fonction « Remote Agent » du **SM-LAN** configure le pare-feu de la passerelle domestique pour qu'il n'accepte que les requêtes HTTPS entrantes en provenance de l'ASP. Il configure aussi le NAT de la passerelle domestique de sorte que les requêtes de l'ASP soient traitées par l'UPnP RP.

A l'aide de l'identifiant incorporé dans la requête, l'UPnP RP reconnaît l'appelant et vérifie dans ses règles de filtrage si Alice a le droit d'envoyer ce type de requête (étape 9). Ensuite, il construit dynamiquement le catalogue d'Alice à partir des règles de filtrage (étape 10). La réponse est relayée par l'ASP (composant proxy HTTPS) vers la maison d'Alice (fonction UPnP Proxy), dans un format XML compatible avec les recommandations UPnP A/V (étapes 11-12).

De la même manière que pour la récupération de la liste de partage, le **CMF** transfère la réponse reçue de son **SM-LAN** à l'UPnP *device* d'Alice sans aucune modification puisqu'elle est au format UPnP A/V (étape 14). Ce dernier peut l'interpréter de façon standard et présenter à Alice le catalogue sous la forme d'une liste des répertoires de contenus partagés par Bob.

ii) Parcours d'un répertoire distant

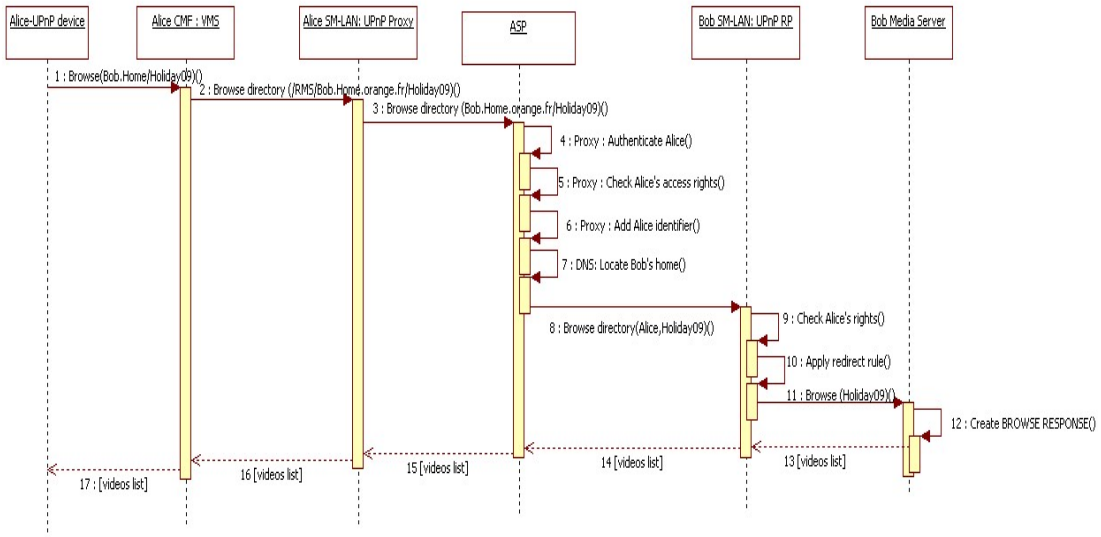


Figure 3.26 Parcours de répertoire distant : solution http

Pour les mêmes raisons évoquées dans la solution IMS, l'UPnP RP ne sauvegarde pas tous les index des contenus partagés et maintient à la place des règles de redirections pour retrouver le Media Serveur qui stocke le contenu. C'est pour cette raison que la procédure de parcours d'un répertoire distant est légèrement différente de celle d'un parcours de catalogue.

En effet, le traitement de la requête d'un utilisateur (i.e. Alice) pour parcourir un répertoire parmi la liste qu'elle a reçu est le même dans le LAN appelant (voir figure 3.26 étapes 1-3) et dans l'ASP (étapes 4-8). La différence de traitement se situe au niveau du LAN appelé. Lorsque l'UPnP RP reçoit une requête sur un répertoire, il vérifie le droit de l'appelant à émettre cette action, afin de filtrer les requêtes interdites (e.g. DELETE et MOVE si on n'est le propriétaire ou l'administrateur) (étape 9). En plus, il vérifie dans ses règles de filtrage le droit de l'appelant à accéder à ce répertoire (étape 10). A nouveau, une attaque pourrait consister à forger des requêtes UPnP A/V non sollicitées, soit portant sur un répertoire existant mais non partagé, soit pour une action non autorisée (e.g. suppression ou déplacement). Si l'une de ces vérifications échoue, l'UPnP RP renvoi via l'ASP, un message d'erreur au correspondant (i.e. 500 unauthorized). Si la requête passe avec succès ces vérifications, l'UPnP RP envoie la requête de BROWSE au Media Serveur adéquat, grâce à ses règles de redirection, pour produire la réponse à cette requête (étapes 11-12). En effet, comme pour la solution IMS, c'est le Média Serveur UPnP A/V qui construit directement la réponse. L'UPnP RP se contente alors juste de remettre en forme (la fonction proxy remplace les identifiants locaux par des identifiants publiques) avant de renvoyer la réponse vers l'UPnP Proxy de l'appelant via l'ASP et par la suite au *device* UPnP de l'utilisateur via le **CMF** (étapes 13-17).

A la fin de cette procédure Alice récupère la liste des contenus stockés dans le répertoire qu'elle a choisi de parcourir. Elle peut répéter cette procédure (étapes 1-17) autant qu'elle souhaite jusqu'à ce qu'elle sélectionne un contenu à regarder.

Modification d'une session pour la récupération d'un contenu distant

Pour éviter que l'ASP soit un goulot d'étranglement à cause du volume du trafic des contenus multimédias échangés, nous allons configurer les deux maisons distantes de sorte que cet échange se déroule en direct (i.e. en point à point). Ainsi, la session utilisée pour récupérer le catalogue ou parcourir un répertoire, doit être modifiée de manière à mettre en relation directe les deux LANs. Lors de cette modification, le client peut demander la réservation de la QoS pour le transfert de son contenu. La figure 3.27 représente la procédure de récupération d'un contenu distant sans mise en place de QoS. Nous traiterons la problématique de gestion de la QoS pour cette solution dans le chapitre suivant.

La procédure de récupération d'un contenu est lancée lorsque l'utilisateur (i.e Alice) indique à son CMF le contenu à lire et le Media Renderer sur lequel le contenu doit s'afficher (étape 1). Le CMF formule alors une requête UPnP GET standard pour récupérer le contenu choisi et demande à son «UPnP Proxy» de le transférer au LAN appelée (i.e. LAN de Bob) (étape 2). L'«UPnP Proxy» renvoi cette requête sortante à l'ASP. Vu que c'est une requête inter-LANs, elle subit le même traitement que les requêtes de récupération de catalogue ou de parcours de répertoire : authentification, vérification des droits d'accès au LAN désigné, ajout de l'identifiant de l'utilisateur, localisation du LAN distant et transfert de la requête à sa destination (étapes 5-9).

Du côté de la maison de Bob, la requête est traitée par l'«UPnP RP». Après la vérification habituelle des droits d'accès au contenu et du type de la requête (étape 10), l'«UPnP RP» contacte son «Remote Agent» pour ajouter dynamiquement une règle dans le pare-feu de la passerelle domestique qui permettra d'accepter les requêtes HTTP en provenance directe du LAN d'Alice (étapes 11-13). L'adresse IP public du LAN d'Alice, utilisée pour mettre en place cette règle de pare-feu, est insérée par l'«UPnP Proxy» d'Alice dans l'en-tête de la requête HTTPS de lecture du contenu (étape 3).

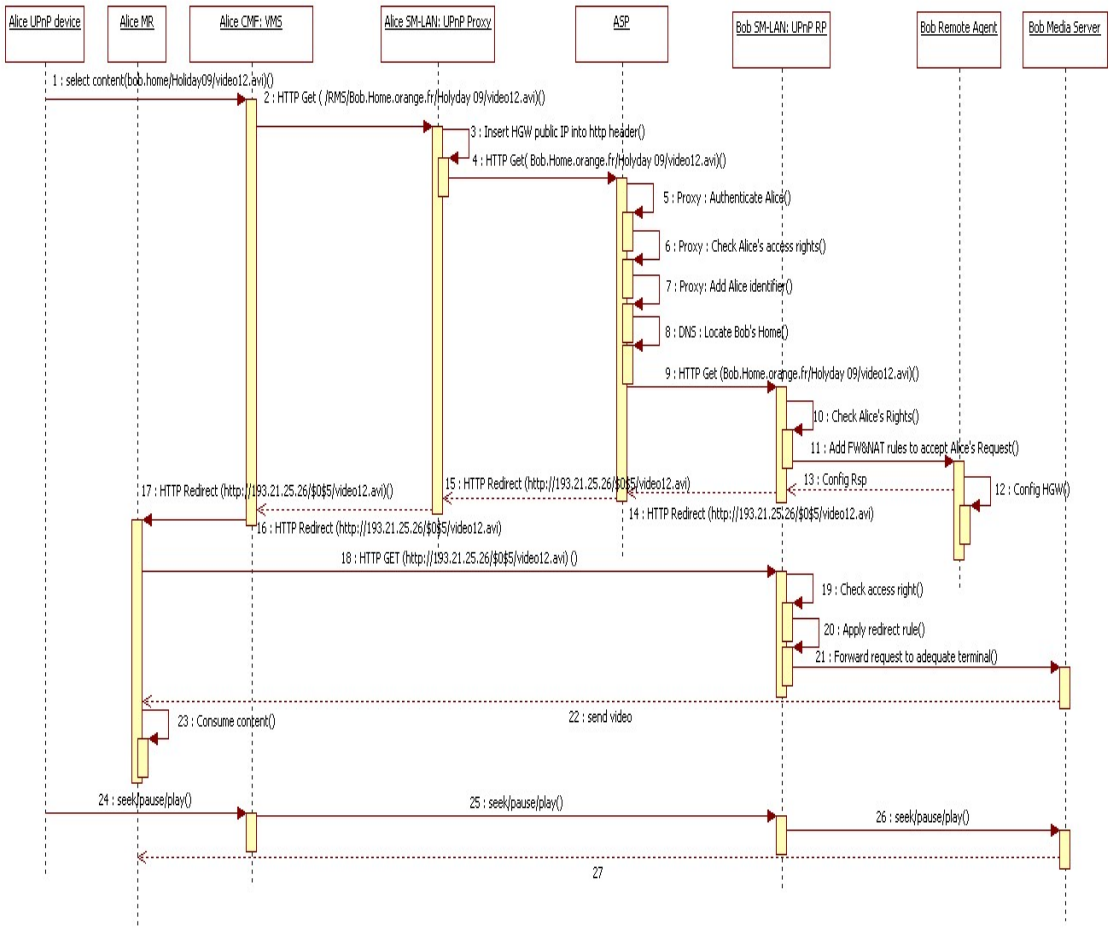


Figure 3.27 Récupération de contenu distant : solution HTTP

Une fois la configuration du pare-feu terminée, l'«UPnP RP» répond à la requête d'Alice avec un message « HTTP REDIRECT» standard contenant la nouvelle URL qui permet de récupérer directement le contenu situé dans le LAN de Bob. Cette nouvelle URL est formée avec l'adresse IP public de la passerelle domestique de Bob et la localisation directe du contenu dans le LAN ex. http://193.21.25.26/$0/$5/vidéo12.avi[2]. Ce message de redirection est envoyé à l'«UPnP Proxy» d'Alice via l'ASP (étapes 14-16). Il est ensuite relayé au CMF qui l'envoi à son tour au Media Renderer qu'Alice a choisi (étape 17). Dans ce message, le Media Renderer d'Alice retrouve les paramètres nécessaires (adresse IP, port) pour récupérer le contenu directement du LAN de Bob (étape 18). La requête de ce terminal sera acceptée du côté du LAN de Bob, grâce à la configuration dynamique que nous avons réalisée dans le pare-feu de sa passerelle domestique. Elle sera traitée par l'«UPnP RP» qui vérifie la requête émise par Alice (i.e. droit d'accès et méthode HTTP utilisée) et la renvoie ensuite vers le Media Serveur adéquat (étapes 19-21). Le Media Serveur transmet alors le flux directement au Media Renderer d'Alice (étape 22).

Alice est en mesure de suspendre/reprendre/avancer le flux reçu avec son device UPnP, via son CMF, comme si elle regardait un contenu en local (étapes 24-27). Pour consulter les autres contenus que Bob partage avec elle, Alice reprend cette procédure (étapes 1-23).

[2] L'indexation des fichiers n'est pas standardisée ni par DLNA ni par UPnP A/V. Nous avons repris dans cet exemple un format d'indexation courant de type ${Numéro Répertoire}.

Note : Une version moins sécurisée mais plus performante a tout d'abord été étudiée. Elle diffère de la présentation de la figure 3.27 par le fait que l'accès aux contenus ne passe par les proxys des réseaux LAN «UPnP RP». En plus de la règle dans le pare-feu, cette version ajoute une deuxième règle de NAT afin que la requête HTTP GET entrante soit directement redirigée vers le bon Media Serveur sans passer par l'UPnP RP. Si l'augmentation de performance est évidente (pas de traitement des flux dans les passerelles domestiques), cette solution présente un trou de sécurité. En effet, une fois la configuration dans le pare-feu et le NAT de la passerelle domestique effectuée, l'utilisateur du LAN visiteur a un accès direct au Media Serveur du LAN visité. Il peut donc en toute impunité parcourir le serveur, y compris les répertoires non partagés avec lui, effectuer tous types d'actions (MOVE, DELETE, …) et visualiser tous les contenus. A cela s'ajoute deux difficultés techniques. La première est que certain Media Serveur vérifie que le Media Renderer se situe bien dans le même LAN (via l'adresse IP) et refuse d'envoyer le contenu si le Media Renderer est localisé dans un autre réseau que le sien. La deuxième est la détection de la fin de lecture du contenu en cas de problème. Nous avons donc privilégié la sécurité et la robustesse de la solution quitte à diminuer les performances de la solution (qui se sont avérées finalement acceptable lors de la phase de réalisation).

Fermeture d'une session

Dans le but de préserver la sécurité du LAN visité, nous devons supprimer la règle de pare-feu ajoutée dynamiquement dans la passerelle domestique à la fin de la consommation du contenu. Pour détecter la perte de connectivité entre les LANs, nous utilisons un mécanisme de temporisation. En effet, du côté du LAN visité l'«UPnP RP» déclenche une temporisation dés qu'il demande au «Remote Agent» d'ajouter une nouvelle règle dans le pare-feu. Cette temporisation doit être réarmée du coté du LAN appelant par l'«UPnP Proxy» en envoyant périodiquement des messages de rafraichissement (keep alive). Ce mécanisme de rafraichissement est lancé lorsque l'«UPnP Proxy» reçoit une requête « HTTP REDIRECT » qui indique que l'utilisateur va commencer la récupération d'un contenu. Si la temporisation maintenue par l'UPnP RP n'est pas réarmée à temps, ce dernier déduit qu'il y a eu une perte de connectivité avec le LAN correspondant et demande alors à son «Remote Agent» de supprimer la règle de pare-feu pour la session en question. Il envoie également un message d'erreur vers le LAN appelant. Même si ce message n'arrive pas à destination, l'«UPnP Proxy» détecte que le rafraichissement de la temporisation n'est plus acquitté et va donc pouvoir notifier le Media Render d'Alice que le média n'est plus disponible.

Pour fermer la session d'une manière appropriée, le **CMF** (fonction VMS) surveille l'activité UPnP dans son LAN. Lorsqu'il détecte que le Media Renderer a terminé la consommation du contenu distant, il envoi un requête UPnP A/V stop. L'«UPnP Proxy» arrête alors l'envoi des messages de rafraichissement au LAN de Bob et transfère la requête vers l'«UPnP RP» du côté du LAN de l'appelé. En recevant la requête UPnP stop, l'«UPnP RP» contacte le «Remote Agent» pour supprimer la règle de pare-feu associée à la session de l'appelant et demande au Media Serveur d'arrêter l'envoi du flux média.

3.3.3.3 Prototype développé et déploiement

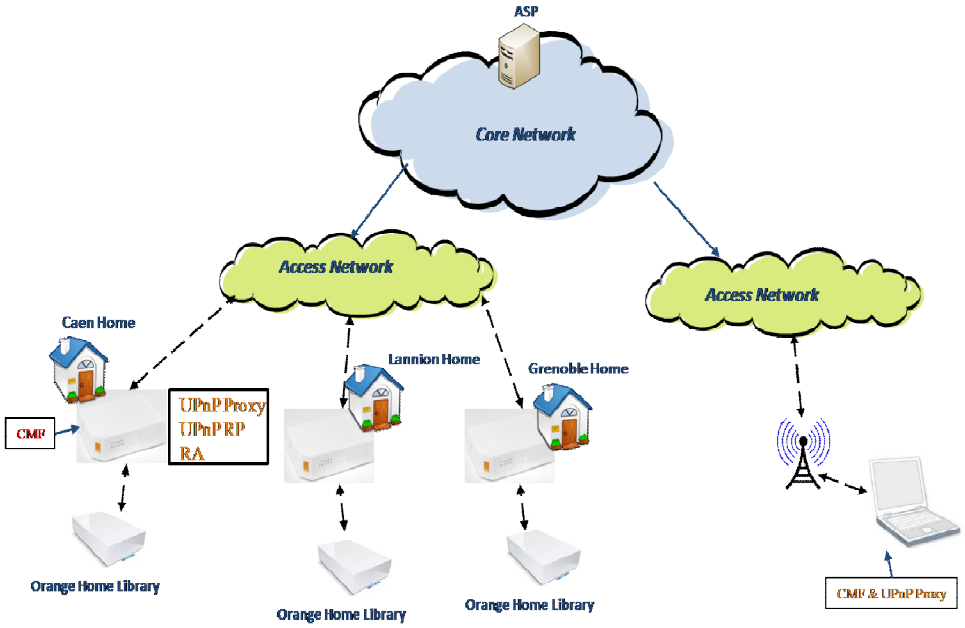


Figure 3.28 Banc de tests de la solution http du service de partage de contenus à distance

Nous avons développé un premier prototype de cette solution dans le cadre du projet Feel@Home. Le but de ce prototype était de démontrer la faisabilité de la solution proposée.

En premier lieu, pour le WAN, nous avons implémenté le composant ASP en se basant sur un ensemble d'outils libres :

- Un proxy Squid [59] en tant que proxy HTTPS authentifiant ;
- Un serveur ICAP (Internet Content Adaptation Protocol) [60] Greasyspoon [61] : nous avons rattaché Greasyspoon au proxy squid pour rajouter aux requêtes reçues un en-tête HTTP (Cookie) contenant l'identifiant de l'utilisateur;
- MySQL [62] comme base de données pour stocker les profils des utilisateurs et leurs règles de partage;
- Un serveur DNS Bind [69] associé à Gnudip [70] (un outil de mise à jour de serveur DNS) pour mettre en place un serveur DNS dynamique afin de localiser les adresses IP publiques des passerelles domestiques des clients. Pour améliorer la performance de cette procédure de résolution d'adresse IP, nous avons proposé une autre réalisation de ce composant (dyn DNS) en utilisant un Web Service qui maintient les adresses IP publiques dans la base de données MySQL.

Le dernier composant de l'ASP est un web service que nous avons développé pour implémenter les fonctionnalités du portail d'administration (i.e. créer / supprimer / modifier les comptes des utilisateurs) et interagir avec le composant du LAN (avec le **SM-LAN**) afin de gérer les règles de partages des utilisateurs (i.e. ajouter/supprimer des règles de partage, et obtenir la liste des amis).

Du côté du LAN, les composants « UPnP Proxy » et « UPnP Reverse Proxy », ont été totalement implémentés avec le langage C pour qu'ils soient intégrés dans la passerelle domestique.

Nous avons repris l'outil Netfilter [65] pour implémenter les fonctions du « Remote Agent » (i.e. la commande du pare-feu et du NAT de la passerelle domestique). En effet, les passerelles domestiques utilisées sont basées sur le noyau Linux qui utilise Netfilter pour l'implémentation du pare-feu et du NAT.

Finalement, une première version du **CMF** a été écrite avec le langage « Java » et déployée sur un ordinateur. Plusieurs autres versions de ce composant ont été développées en C pour que ce composant soit aussi intégré dans la passerelle domestique.

Nous avons déployé ce prototype sur plusieurs sites de France Telecom R&D pour simuler le partage de contenus à distance entre maisons distantes.

Nous avons ensuite réalisé des tests fonctionnels du service de partage de contenus, et plus spécialement :

- l'ajout de règle de partage ;
- la récupération de la liste des maisons accessibles à distance ;
- le parcours de répertoires distants ;
- et la récupération de contenus distants.

Nous avons enfin testé l'accès en situation de nomadisme décrite dans la figure 3.28. Dans ce scénario, nous avons installé les composants **CMF** et UPnP Proxy sur un ordinateur portable que nous avons connecté à internet avec un accès ADSL, pour accéder à nos propres contenus (i.e. sur le site de Lannion) et à ceux de nos amis.

Il faut souligner que notre solution de partage de contenus s'intègre d'une manière transparente avec les logiciels et les équipements UPnP A/V standards. Dans le scénario maison-à-maison, nous avons réutilisé des produits commerciaux. A savoir une set-top box Orange qui intègrent un Media Player UPnP A/V (fonctions Control Point et Media Renderer), un Home Library Orange comme Media Serveur UPnP A/V pour partager les contenus, une PS/3 comme serveur et lecteur ainsi que plusieurs TV comme player.

Dans le scénario de nomadisme, nous nous sommes servis d'un logiciel libre UPnP A/V pour utiliser notre service de partage. Avec ce logiciel, nous avons détecté un UPnP A/V Media Serveur appelé «Shared Home Zone» qui est le Media Serveur annoncé par le **CMF** (VMS) (Fig. 3.29.a). En parcourant ce Media Serveur, nous récupérons la liste des amis qui partagent des contenus avec nous.

Comme le montre la Fig. 3.29.b, cette liste est composée de trois maisons : notre maison (sur le site de FT R&D Lannion), le site FT R&D à Grenoble et la maison de Stéphane (sur le site de FT R&D Caen). La Fig. 3.29.c illustre le catalogue que Stéphane a partagé avec nous.

a. Detect UPnP Remote MS

b. Browse UPnP Remote MS

c. Browse Remote catalogue

Figure 3.29 Exécution d'un parcours de catalogue distant : solution HTTP

a. Browse Remote Directory b. Retrieve picture

Figure 3.30 Exécution d'un parcours de répertoire distant : solution HTTP

La Fig. 3.30.a présente un exemple de réponse à une requête de parcours de répertoire d'images. Enfin, la Fig. 3.30.b montre la lecture d'une des images stockées dans ce répertoire.

3.3.3.4 Etude de performance

Le prototype développé nous a d'abord servi à valider fonctionnellement notre solution HTTP. Ensuite, une deuxième étape a été d'étudier le passage à l'échelle de cette solution. Dans cette étude, nous avons considéré un seul point d'étranglement de notre système qui est l'ASP. En effet, c'est le seul module qui doit traiter un grand nombre de sessions. La méthode de validation est la simulation à événement discret. Toutes les fonctions déployées dans les LANs n'ont à traiter que quelques sessions simultanément. Dans la pratique, une seule session pour un appelant et de une à moins d'une dizaine de sessions pour un appelé. De plus, les capacités réseaux de la maison appelée étant limitées, la gestion de la QoS (voir chapitre suivant) limite le nombre de sessions à une à deux, trois selon les usages et la capacité. La performance est plus du fait de la réalisation des modules logiciels à destination de la passerelle domestique qui est un équipement ayant de faible capacité mémoire et CPU. Or, la réalisation a démontré que le système fonctionnait parfaitement dans de telles conditions sans perturber le bon fonctionnement de la passerelle domestique. La consommation mémoire et CPU reste très limité comme pour un processus standard : quelques Mo en fonctionnement, une empreinte sur disque inférieure à 256 ko et une consommation CPU inférieure à 1%.

Environnement et modèle de simulation

Dans cette évaluation, nous avons utilisé le simulateur libre ns3 [66], un simulateur à évènements discrets dédié à la simulation des systèmes informatiques.

La première étape de cette évaluation a été de définir un modèle qui représente notre plate-forme ASP. La figure 3.31 présente notre modèle, représenté par un graphe étiqueté. Pour le composant «DNS dynamique», nous avons modélisé la réalisation utilisant un web service, vu qu'elle a offert de meilleures performances que celle utilisant un serveur de nom (Bind associé à Gnudip).

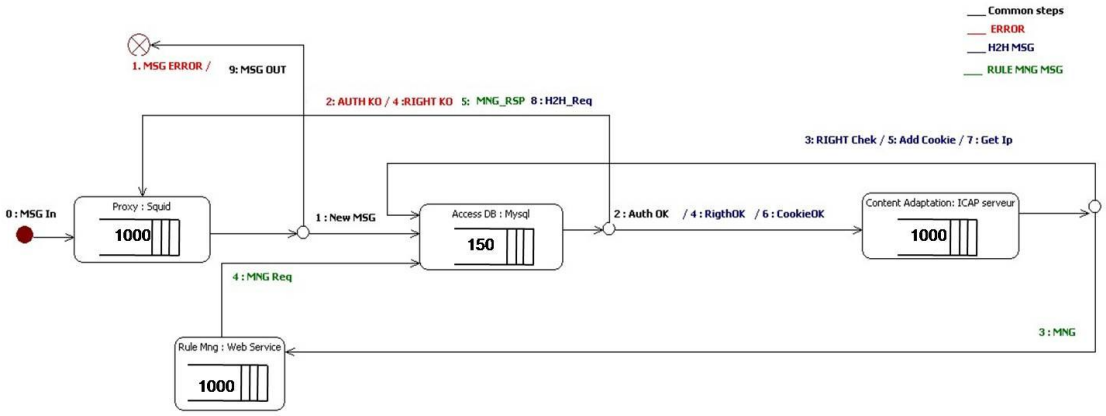


Figure 3.31 Modèle globale de la simulation de l'ASP

Chaque nœud du graphe simule un processus de l'ASP. Les étiquettes des arcs sont les états que nous affectons à un message tout au long de son traitement dans l'ASP. Nous avons spécifié quatre nœuds dans notre modèle, caractérisés chacun par sa capacité (c.à.d. la taille de sa file d'attente) et son temps de traitement pour chaque type de message. Le Tableau 3.3 résume les caractéristiques et la signification des quatre nœuds du modèle. Le système a été modélisé à l'aide d'une représentation de files d'attentes en tandem (décomposition du fonctionnement de l'ASP en plusieurs serveurs). Une file d'attente se dégage cependant; il s'agit de la modélisation de la base de données. En effet, les différents serveurs de l'ASP sollicitent à un moment ou un autre la base de données. C'est donc sur cette file d'attente que s'est porté toute notre attention.

Tableau 3.3 Caractéristiques des nœuds du modèle de l'ASP

Nœud	Capacité	Temps de traitement	Description
Squid	1000	0.03 ms	Simule le temps de traitement des requêtes entrantes par le proxy de l'ASP.
ICAP Serveur	1000	0.03 ms	Simule le processus responsable de : (i) l'identification de la requête, (ii) la vérification des droits d'accès et (iii) la résolution d'adresse du LAN destinataire.
Web Service	1000	0.03 ms	Simule le web service responsable de la gestion des droits d'accès : ajout, suppression, récupération de règles.
MySQL	150	• Nouvelle requête: 5ms ; • Requête déjà traitée:0.05ms.	Simule l'accès à la base de données pour récupérer : les règles de partage, l'identifiant de l'utilisateur (cookie) et l'adresse IP publique du LAN destinataire.

Conformément à la spécification que nous avons définie pour l'ASP, notre modèle implémente deux procédures de traitement des requêtes:

- Une procédure dédiée aux requêtes de gestions des règles de partages, dont les états sont étiquetés en « verts » dans le graphe de la figure 3.31.
- Une procédure dédiée aux requêtes inter-LANs (i.e. les parcours de catalogues, parcours de répertoires, récupérations de contenu) dont les états sont étiquetés en « bleu » dans le graphe de la figure 3.31.

Les états en commun entre ces deux procédures sont étiquetés dans la figure 3.31 en « noir ». Les deux procédures de traitements des requêtes et la gestion des cas d'erreurs dans l'ASP sont données et caractérisées dans ce qui suit :

a. Traitement des requêtes inter-LANs

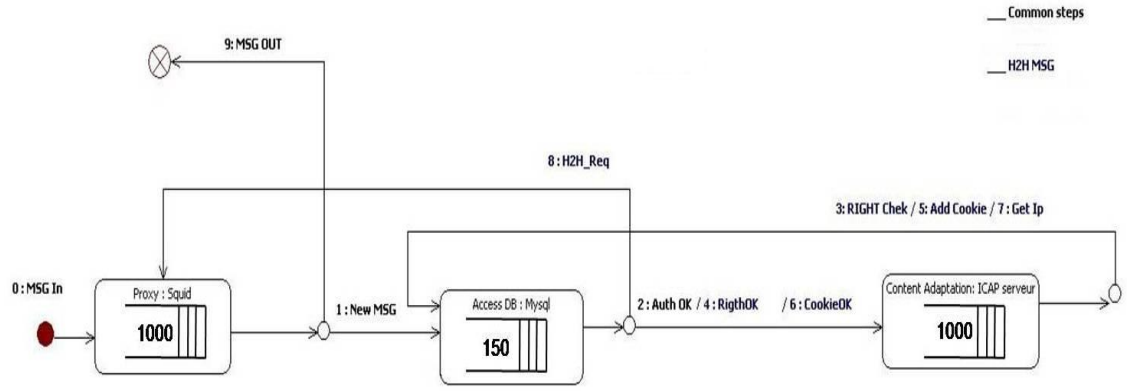


Figure 3.32 Procédure de traitement des messages inter-LANs dans l'ASP

Pour détailler la procédure de traitement des messages inter-LANs dans l'ASP, nous l'avons représentée dans la Fig 3.32. Cette procédure est constituée de 9 étapes :

- Etape 0 : Nous associons à chaque nouvelle requête entrante dans l'ASP l'étiquette **MSG_In** ;
- Etape 1 : Le Proxy vérifie si la requête est bien formulée. Après cette vérification, la requête prend l'état **New_MSG** et elle est passée au serveur MySQL;
- Etape 2 : Au niveau du serveur MySQL, nous vérifions l'identifiant de l'utilisateur. Si ce test est passé avec succès la requête sera étiquetée **Auth_OK** et passée au serveur ICAP;
- Etape 3 : Le serveur ICAP identifie la requête comme une requête inter-LANs, donc il la passe au serveur MySQL pour vérifier les droits de l'émetteur de la requête à accéder à la maison désignée. A la sortie de cette étape, la requête est étiquetée **RIGHT_Check**;
- Etape 4 : Nous vérifions dans la base MySQL s'il existe une règle autorisant le client à accéder à la maison destination. Si cette règle existe, la requête est étiquetée **RIGHT_OK** puis transférée au serveur ICAP;
- Etape 5 : Après la vérification des droits d'accès, le serveur ICAP ajoute l'identifiant du client émetteur de la requête dans l'en-tête. Pour récupérer l'identifiant du client, il transmet la requête au serveur MySQL et l'étiquette avec **Add_Cookie** ;
- Etape 6 : Nous récupérons l'identifiant du client de la base de données MySQL et nous l'ajoutons dans l'en-tête de la requête. La requête est alors étiquetée par **Cookie_OK** et passée au serveur ICAP;
- Etape 7 : La dernière étape de traitement d'une requête inter-LANs au niveau du serveur ICAP est de retrouver l'adresse IP publique du LAN destination. Comme cette information est stockée dans la base de données MySQL, le serveur ICAP étiquète la requête avec **GetIp** et la transmet au serveur MySQL ;
- Etape 8 : Une fois l'adresse publique du LAN destination récupérée de la base de données MySQL, la requête est remise au Proxy pour la transférer à sa destination. La requête est étiquetée **H2H_Req** ;
- Etape 9 : L'étiquète **H2H_Req** indique au Proxy la fin du traitement d'une requête inter-LANs. Elle est alors sortie de l'ASP et étiqueté **MSG_OUT**.

Les files d'attentes simulant la base de données MySQL et le serveur ICAP sont donc celles qui vont être le plus sollicitées et donc sujettes le plus rapidement à saturation lors de l'évaluation de performance.

b. Traitement des requêtes de gestion

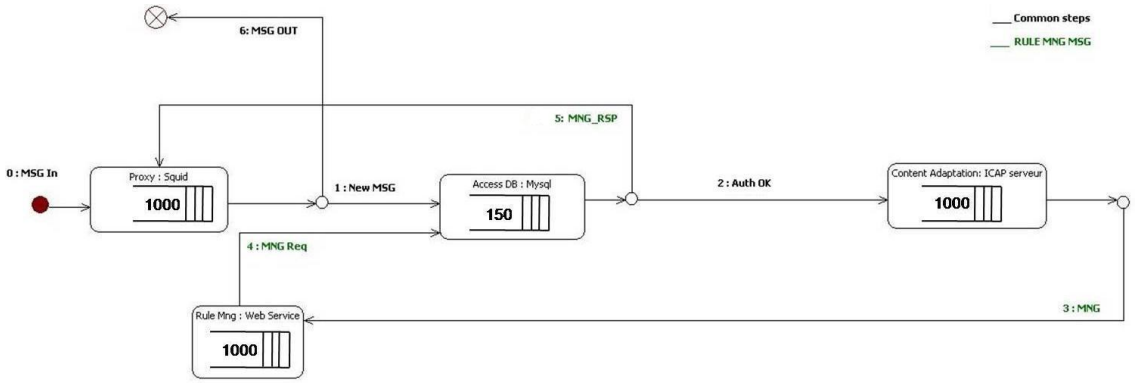


Figure 3.33 Procédure de traitement des messages de gestion dans l'ASP

La procédure de traitement d'une requête de gestion des règles de partages (requête de « gestion ») dans l'ASP est illustrée dans la Fig.3.33. Les étapes 0, 1 & 2 de cette procédure sont identiques à celles de la procédure de traitement des requêtes inter-LANs.

- Etape 3 : Le serveur ICAP identifie la requête comme une requête de gestion, il l'étiquète **MNG** et la passe au Web Service ;
- Etape 4 : Le Web Service identifie la requête de gestion qu'il a reçu (ajout de règle, suppression de règle, récupération de règle). Elle est alors passée au serveur MySQL pour récupérer/ mettre à jour les informations de la base de données. A la fin de cette étape, la requête est étiquetée **MNG_Req** ;
- Etape 5 : Cette étape modélise la phase de récupération / mise à jour des informations de la base de données demandée dans la requête de « gestion ». C'est la dernière phase de traitement des requêtes de « gestion », nous les étiquetons alors avec **MNG_RSP** ;
- Etape 6 : L'étiquète **MNG_Rsp** indique au Proxy la fin du traitement d'une requête de « gestion ». Elle est alors sortie de l'ASP et étiquetée **MSG_OUT**.

Ici, les différents serveurs sont sollicités plus modérément. Cependant, la phase de gestion est celle qui sera le plus fréquemment utilisée, donc susceptible de saturer le serveur ASP.

c. Les cas d'erreur

Les cas d'erreurs, signalé dans la Fig. 3.31 en rouges, sont :

- une requête mal formée (MSG_ERROR);
- une requête mal authentifiée (AUTH_KO);
- une requête inter-LANs qui manque de droit (RIGHT_KO).

Résultats des simulations

Critères d'évaluation

Pour valider l'aptitude de l'ASP au passage à l'échelle, nous avons mesuré deux critères de l'ASP :

- le temps de traitements des requêtes ;
- le taux de rejet des requêtes.

Le temps de traitement de la requête correspond à la différence entre l'instant ou l'ASP reçoit la requête et l'instant où il émet la réponse correspondante.

Le taux de rejet correspond au pourcentage des requêtes supprimées dans les files d'attentes des nœuds de notre modèle. La politique de suppression des requêtes dans l'ASP consiste à supprimer la nouvelle requête reçue, dans le cas où la file réceptrice est pleine.

Hypothèses de la simulation

Hypothèse 1 : La taille de la population de notre service de partage de contenus est de 1 Million. En heure de pointe, 10% de cette population est actif. Donc, nous aurons au maximum 100 000 clients utilisant notre service simultanément.

Hypothèse 2 : Il y a trois types de scénarii possibles pendant l'heure de pointe. Le tableau 3.4 décrit ces scénarii et le nombre de requêtes que chacun génère pendant une heure, classé par type de requête. Nous supposons que pour chaque scénario, l'utilisateur parcourt cinq répertoires en moyenne avant de choisir le contenu à récupérer.

Tableau 3.4 Description des scénarii réalisés par les clients pendant une heure

Type du scénario	Description	Get Friend List	Browse Catalogue	Browse Directory	Get Content
1. Photo	Regarder un diaporama de 100 photos.	1	1	5	100
2. Music	Ecouter 10 morceaux de musiques	1	1	5	10
3. Vidéo	Regarder une vidéo.	1	1	5	1

Hypothèse 3 : Ces scénarii sont équiprobables. Nous pouvons alors calculer le taux maximal d'arrivée de chaque type de requêtes pendant l'heure de pointe. Nous les résumons dans le tableau 3.5.

Hypothèse 4 : Chaque scénario a été composé de sorte à durer une heure.

T_{REQn} : Taux d'arrivée de $Type_n$, sachant que les types des requêtes sont : requête *GetFriendList* ; requête *Browse Catalogue* ; requête *Browse Directory* ; requête *Get Content* ;
D : Durée de la simulation ;
NbrClient : Nombre de clients pendant la solution (c.-à-d. 100 000) ;
$NbrReq_n$: Nombre de requête de type *n* générées dans la simulation ;
$NbrReq_{n/Sci}$: Nombre de requête de type *n* générées dans la simulation par le scénario de type « *i* » (i.e. photo, music ou vidéo).

$$T_{REQn} = NbrReq_n / D$$

$$T_{REQn} = [(NbrReq_{n/Sc1} * 0.33 + NbrReq_{n/Sc2} * 0.33 + NbrReq_{n/Sc3} * 0.33) * NbrClient] / D$$

$$T_{REQn} = [(\sum_{i=1}^{3} NbrReq_{n/Sci}) * 100000 * 0.33] / 3600.$$

Tableau 3.5 Taux maximums d'arrivée des requêtes pendant l'heure de pointe

	Get Friend List	Browse Catalogue	Browse Directory	Get Content
Taux maximal d'arrivé	28 req/s	28 req/s	138 req/s	1018 req/s
Pourcentage par type	2%	2%	12%	84%

Ainsi le taux total maximal de requêtes que l'ASP peut recevoir en heure de pointe est de 1212 req/s (28+28+138+1018).

Hypothèse 5 : L'arrivé des requêtes reçues par l'ASP suit une loi de Poisson parce que l'arrivé des clients est indépendante.

Description des simulations

Nous voulons vérifier si l'ASP est capable de traiter plus de 1200 Req/s, qui correspondent au taux maximal de requêtes que l'ASP peut recevoir en heure de pointe pour une base installée de 1 Million d'utilisateurs.

Nous produisons alors avec quatre générateurs de requêtes (i.e. un pour chaque type de requête) des demandes à l'ASP avec des taux que nous faisons varier lors des différentes itérations. Les proportions pour chaque type de requête sont indiquées dans le tableau 3.5. Nous augmentons le taux d'arrivée des requêtes à chaque itération de 100 req/s jusqu'à atteindre 1300 req/s. Nous mesurons dans ces simulations les indicateurs « temps de traitement » (figure 3.32) et le « taux de rejet » (Fig. 3.33) pour les différents types de requêtes.

Interprétation des résultats

La figure 3.34 fournit le temps de traitement des requêtes dans l'ASP. La première analyse de cette courbe montre que le temps de traitement le plus élevé concerne les requêtes de récupération de la liste des amis. Nous expliquons ce résultat par le fait que les informations (mot de passe, identifiant, …) sont récupérées pour la première fois dans la base de données, et donc le temps d'accès est le plus long.

Le temps de traitement le plus rapide est pour les requêtes de récupération de contenu (Get content), car toutes les informations (mot de passe, identifiant, règle de partage, adresse ip publique du destinataire) sont déjà récupérées de la base de données pendant le passage des requêtes de parcours et sont stockées dans la mémoire cache du serveur de base de données. Donc le temps d'accès à ces informations est plus rapide qu'une recherche sur le disque.

La dernière constatation est que le temps de traitement reste toujours inférieur à 500 ms, même pour les requêtes les plus lentes, et donc il est tout à fait acceptable pour assurer l'interactivité.

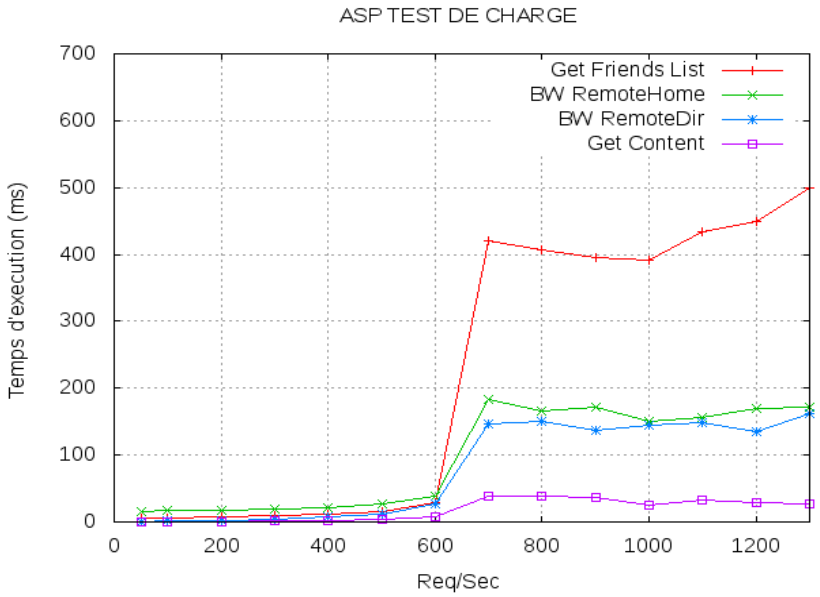


Figure 3.34 Temps de traitement des requêtes dans l'ASP

La figure 3.35 trace le taux de rejet des requêtes au niveau de l'ASP. Nous constatons qu'à partir de 700 req/s l'ASP commence à rejeter des requêtes (3%). Ce taux de rejet augmente d'une façon presque linéaire avec le taux d'arrivé des requêtes. Nous supposons qu'un taux de rejet acceptable pour un tel service doit être inférieur à 2%, et nous avons conclu alors que la capacité maximale de l'ASP est de 600 req/s.

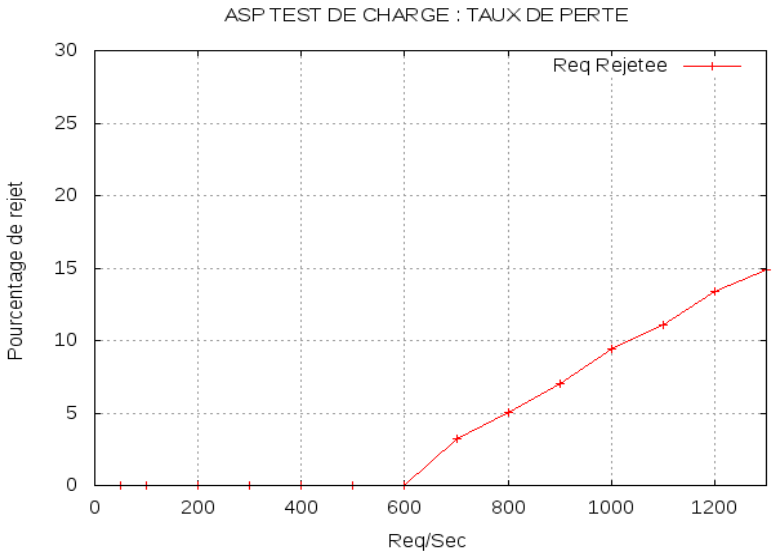


Figure 3.35 Taux de rejet des requêtes dans l'ASP

Dimensionnement de l'ASP

Une fois le calcul de la capacité d'une instance unique de l'ASP (600 req/s) obtenu par simulation, connaissant le taux d'arrivée maximal des requêtes (1212 req/s) que nous souhaitons atteindre, nous trouvons que, pour servir une population de 1 million d'utilisateurs, il faut déployer deux instances de l'ASP derrière un répartiteur de charge (load balancer). La seule modification à apporter à la spécification de l'ASP pour mettre en place cette duplication, est au niveau de l'ajout/suppression des règles de partages et de la mise à jour des informations des profils des clients. Afin de maintenir la cohérence de ces informations, elles doivent être mises à jour simultanément dans les deux instances de bases de données. De cette manière, les deux instances de l'ASP seront autonomes. Une deuxième piste d'amélioration de l'ASP, consiste à configurer les différents modules logiciels de sorte à réduire le taux de perte (file d'attente quasi sans perte) quitte à ce que le temps de traitement d'une requête soit allongé. En effet, la simulation nous a montré que le temps de traitement restait inférieur à 500 ms ce qui reste tout à fait acceptable.

3.3.3.5 Test du service de partage par des collaborateurs d'Orange : Field User Trail

Avant de mettre en production un nouveau service, Orange organise des tests des nouveaux services par ses collaborateurs. La solution HTTP de notre service de partage est actuellement dans cette phase de test. L'implémentation testée a repris les développements du prototype livré dans le cadre de Feel@Home. Les améliorations de la version actuelle ont porté surtout sur l'optimisation des composants à déployer dans le LAN et le WAN. En particulier une version compacte à déployer uniquement sur le PC d'une maison a été réalisée car il nous a été impossible d'accéder facilement au firmware des LiveBox de production déployées chez les clients afin d'y ajouter nos modules logiciels. De même, une nouvelle version de l'ASP a été installée en tenant compte des résultats de la simulation (deux instance de l'ASP derrière un switch L4 en partage de charge).

Les premiers retours nous ont amenés à modifier le composant de gestion des partages. En effet, il nous a été très difficile de déterminer les pannes et les erreurs qui pouvaient intervenir entre le composant **CMF** et les composants SM-LAN. En particulier, plusieurs problèmes de communication de ces deux composants dans le LAN nous ont été rapportés rendant l'expérience utilisateur inadaptée. De ce fait, une nouvelle version a été conçue. Le **CMF** a été coupé en deux et ses fonctions réparties entre le **SM-WAN** et le **SM-LAN,** de sorte à ne posséder que deux composants bien identifiés et un diagnostic d'erreurs simplifié.

Une deuxième période de test a été conduite à l'automne 2011 et progressivement élargie à de vrais utilisateurs (hors personnel Orange) localisés aussi bien en France qu'en Espagne. Les premiers retours sont très positifs montrant à la fois la pertinence du service et les choix d'implémentations.

3.5 Conclusion

Dans ce chapitre, nous avons exposé un nouveau système d'accès à distance qui permet le partage de contenus multimédias. En premier lieu, nous avons situé notre système dans son cadre général qui est le service de partage de contenus à distance étudié dans le projet Feel@Home. Ensuite, nous avons présenté l'architecture fonctionnelle de ce système et son intégration dans le service de partage de Feel@Home.

Nous avons découpé notre système en deux composants : un est déployé dans le réseau cœur (**SM-WAN**) et un deuxième dans les LANs des utilisateurs (**SM-LAN**). Grâce au composant **SM-WAN**, nous protégeons les LANs des utilisateurs de l'accès non autorisé à leurs réseaux domestiques et de l'usurpation d'identité des appelants. La sécurisation des LANs est complétée par le **SM-LAN** qui ajoute dynamiquement des règles dans le pare-feu de la passerelle domestique pour permettre aux utilisateurs autorisés par le **SM-WAN** d'accéder directement à ce LAN. Notre système garantit aussi la confidentialité des contenus partagés par le service de partage. En plus, du fait que les contenus restent stockés dans les LANs des utilisateurs, le système permet à l'utilisateur de préciser pour chaque ami la liste des contenus auxquels il peut accéder.

En second lieu, nous avons proposé la description de la réalisation technique du système spécifié. Nous avons développé deux déclinaisons techniques de notre système. La première solution utilise le Framework IMS et la deuxième est cohérente avec l'esprit d'internet en utilisant des relais applicatifs HTTP (proxy).

Dans la première solution, nous utilisons l'IMS pour établir des médias HTTP sécurisées entre les deux extrémités de la communication. L'échange de contenus se fait point-à-point entre les utilisateurs pour éviter l'engorgement du **SM-WAN**. Cette solution a été validée avec des simulations UML à l'aide de l'environnement TauG2. Nous avons publié ces travaux dans la conférence internationale ICIN 2010 et l'article a reçu le prix du meilleur papier. Ces travaux ont aussi été proposés et acceptés par le groupe de travail WG5 de l'organisme de standardisation ETSI TISPAN [71, 72]. La norme résultante devrait être publiée d'ici fin 2011.

Dans la deuxième déclinaison, nous avons proposé d'implémenter notre système avec des relais applicatifs HTTP. Le **SM-LAN** a été implémenté principalement par deux proxys : un proxy pour transférer les appels sortants vers le **SM-WAN** et un proxy inverse pour accepter les appels entrants. Le proxy central, qui implémente le **SM-WAN**, a pour mission de certifier la signalisation qui permet la mise en place d'une session sécurisée entre les deux correspondants pour que l'échange de contenus s'effectue, comme dans la solution IMS, en point-à-point. Nous avons développé un prototype de cette solution dans le cadre du projet Feel@Home. Des tests de charges ont été conduits à l'aide de simulations pour déterminer l'aptitude de la solution au passage à l'échelle. Avec ces tests, nous avons pu déterminer la capacité de notre système et par

la suite dimensionner les ressources à mettre en place pour un déploiement pour un grand nombre d'utilisateurs. Les résultats de ces travaux on été publiés dans la conférence internationale FMN 2010. Nous avons aussi déposé un brevet pour protéger cette solution. Enfin, cette solution a été la base de nos contributions au standard UPnP Remote Access v2 qui permet la communication Home-to-Home via des proxys de sessions localisés dans chaque maison. Le proxy du réseau cœur est optionnel dans cette norme laissant la possibilité aux opérateurs de déployer soit une solution basée sur l'utilisation de VPN soit via une architecture conforme à celle proposée dans cette thèse pour sécuriser l'établissement des sessions entre les réseaux domestiques.

Dans le chapitre suivant, nous allons étudier la deuxième problématique de la thèse qui est la réservation de QoS pour le transfert des contenus échangés par le service de partage à distance. Nous présenterons les solutions que nous avons proposées et leurs intégrations dans le système d'accès à distance présenté dans ce chapitre.

Chapitre 4

Gestion de la QoS pour le service de partage de contenus à distance

Sommaire

4.1 Introduction

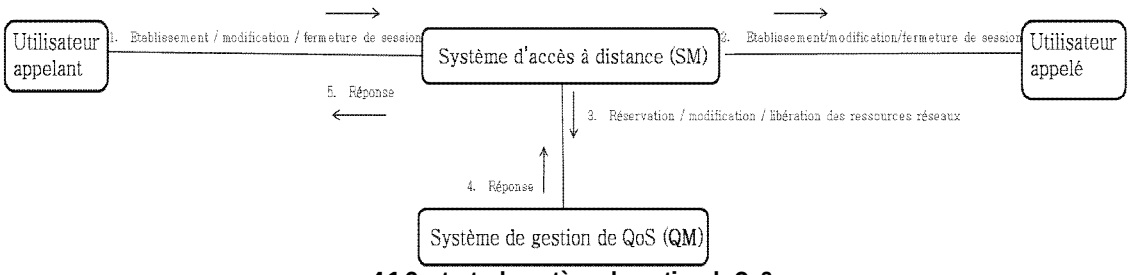
Dans le chapitre précédent nous avons présenté notre nouveau système d'accès à distance qui traite la première problématique de notre travail de thèse. Ce chapitre aborde la deuxième problématique qui est la gestion de la QoS pour le transfert des flux échangés par le service de partage de contenus à distance étudié dans le cadre du projet Feel@Home. Nous proposons un système que nous appellerons par la suite «système de gestion de QoS» ou «QoS Manager (QM)».

Dans la réalisation de notre système de gestion de QoS, nous avons adopté la même méthodologie que celle utilisée pour la réalisation de notre système d'accès à distance. Nous avons commencé par une étude fonctionnelle de notre système afin de bien identifier les interfaces et le rôle de ce système. Sur la base de cette étude, nous avons élaboré une architecture fonctionnelle générique de notre système que nous avons intégrée dans l'architecture du service de partage étudié. Finalement, nous avons proposé une étude technique de l'implémentation de cette architecture.

4.2 Analyse fonctionnelle du système de gestion de QoS

Pour commencer cette étude fonctionnelle, nous allons rappeler le cadre de notre système de gestion de QoS.

4.2.1 Contexte général



4.1 Contexte du système de gestion de QoS

Notre système de gestion de QoS constitue la brique qui se charge de la gestion de QoS dans le service de partage de contenus à distance étudié dans le projet Feel@Home. Le principal scénario de ce service de partage de contenus est l'échange de contenus entre LANs distants. Dans ce scénario, l'objectif que nous nous sommes fixé est de garantir la QoS sur tout le chemin emprunté pare les flux de données échangés. Il est sollicité pour cet effet par le système d'accès à distance (voir figure 4.1).

En premier lieu, il est important de fixer les contraintes que nous devons prendre en compte dans l'élaboration de notre système de gestion de QoS. La nature même des réseaux par lesquels transitent les flux de données de notre service de partage ne nous permet pas d'envisager toutes les solutions possibles. En particulier, nous devons prendre en compte le fait que les réseaux domestiques sont protégés par des pare-feux et qu'ils utilisent le même plan d'adressage privé. Ceci nous impose les mêmes restrictions qu'il s'agisse de la mise en place du service de partage ou de la gestion de la QoS. Aussi, une signalisation de bout en bout type NSIS ou RSVP n'est pas envisageable car elle ne pourrait que très difficilement franchir les pare-feux et gérer les conflits d'adresses. Nous devons donc raisonner en partition de réseau et non globalement. A noter que NSIS a bien prévu une signalisation de configuration des pare-feux, mais cela nous obligerait à combiner deux signalisation en une : la gestion de la QoS (via QoS-NSLP) et la traversée du NAT (via NAT/Firewall NSLP), ce qui alourdirait le processus sans toutefois résoudre la problématique de l'adressage privée.

Ainsi, nous avons distingué trois portions de réseaux différents dans ce chemin de données : le

LAN visité (où se trouve le contenu à récupérer), le réseau cœur (ou réseau de l'opérateur) et le LAN du visiteur (où le contenu va être visualisé). Dans un premier temps nous considérons que le réseau cœur est géré par un seul acteur, puis nous généraliserons ce cas lorsque le réseau cœur est constitué en réalité de plusieurs réseaux d'opérateurs gérés par plusieurs acteurs. Au niveau du LAN visité, en plus de la gestion de la QoS dans le réseau domestique, il faut prévoir un contrôle des flux envoyés vers l'extérieur de ce LAN. En effet, les ressources du lien montant sont souvant limitées en bande passante surtout dans les connexions ADSL, il nous faut donc appliquer une admission d'appel sur la voie montante pour ne pas accepter trop d'appel du service de partage afin d'éviter une saturation de ce lien.

Une fois posé ce constat, notre système de gestion de QoS devra non seulement s'assurer que les mécanismes utilisés soient cohérents entre eux, mais surtout qu'ils soient synchronisés tant au point de vue de la mise en place de la QoS que du traitement des cas d'erreurs et de la terminaison du service.

En plus de la réservation de ressources réseaux, le système de gestion de QoS doit gérer les droits des utilisateurs à envoyer des requêtes de QoS, dans chaque portion de réseau du chemin de données. L'administrateur du réseau d'opérateur doit vérifier les droits de l'utilisateur à initier une réservation de ressources dans le réseau de cœur. De la même manière, l'utilisateur doit être capable de configurer les droits de ses contacts à réserver des ressources réseaux dans son LAN. En effet, l'utilisateur peut partager des contenus avec un ami et ne pas lui autoriser de réserver des ressources dans son réseau domestique.

Dans ce chapitre, nous ne proposons pas de nouvelles techniques de mise en place de la QoS, que ce soit dans les LANs ou dans les réseaux de cœur. Le but de l'étude étant de réutiliser les mécanismes existants (exposées au chapitre 2) tout en nous concentrant sur l'étude d'un système de gestion de la QoS de bout en bout (du Media Server jusqu'au Media Renderer) cohérent (assurant une continuité de la garantie quelque soit le réseau et la technologie employés). Dans cette étude nous allons désigner parmi les technologies que nous avons présentées dans l'état de l'art, la (les) technologie(s) la (les) plus adaptée(s) à notre contexte de partage de contenus pour mettre en place la QoS, que ce soit dans les LANs ou dans les réseaux cœurs. Notre contribution porte essentiellement sur la mise en cohérence et la synchronisation des différentes signalisations pour la mise en place de la QoS.

4.2.2 Etude fonctionnelle du système de gestion de QoS

4.2.2.1 Contraintes du système de gestion de QoS

En se basant sur les besoins de QoS de notre système, identifiés pendant la phase de spécification, nous avons défini les caractéristiques des trois classes de services que ce système devra utiliser :

- Classe Audio : Utilisée par le scénario d'échange de musique. La contrainte forte de cette classe est le délai et le taux de perte. Un débit de l'ordre de quelques centaines de Kbits/seconde, correspondant au débit d'encodage standard (e.g. mp3), nous permet d'avoir une expérience utilisateur acceptable ;
- Classe Vidéo : Utilisée par le scénario d'échange de vidéo. La contrainte forte de cette classe est le débit et le taux de perte et en second lieu vient le délai et la gigue. Pour assurer une expérience d'utilisation acceptable de ce scénario, le débit demandé par cette classe de service est exprimé en MégaBits/seconde et correspond à nouveau au débit d'encodage standard (e.g. mp4, dvix);
- Classe Donnée : Utilisée par le scénario d'échange de photos. C'est la classe de service la moins contraignante, car elle s'accommode d'un débit et d'un délai quelconques, mais elle demande un faible taux de perte. Une expérience utilisateur acceptable consiste à télécharger la photo (n+1) pendant que l'on consulte la photo n, ce qui donne un temps

de téléchargement ne devant pas dépasser quelques secondes (e.g. 10 à 30) soit un débit de l'ordre du Mbit/s pour des photos de 2 à 5 Mo.

Par la suite, il nous sera possible d'ajouter de nouvelles classes de service. Par exemple, dans le cas d'une utilisation pour la domotique (Home Automation), nous définirons la classe Domotique qui nécessite peu de débit mais une interaction forte (faible délai et gigue) et un taux de perte très faible afin de s'assurer que les commandes passées ont bien été reçues et exécutées.

4.2.2.2 Etude des cas d'utilisation du système

La première étape, dans la conception du système de gestion de QoS (**QM**), était de définir ses cas d'usages. Les acteurs externes à ce système sont (voir figure 4.2) :

- L'administrateur : Entité chargée de la gestion des ressources du réseau. Nous pouvons distinguer deux types d'administrateurs. L'administrateur du réseau de l'opérateur et l'administrateur du LAN qui n'est autre que l'utilisateur du service de partage. Nous avons fait cette différenciation parce que l'administrateur du réseau de l'opérateur n'a pas le droit de commander les ressources réseaux des LANs des clients et réciproquement;
- Le système d'accès à distance (**SM**) : c'est l'utilisateur final du système.

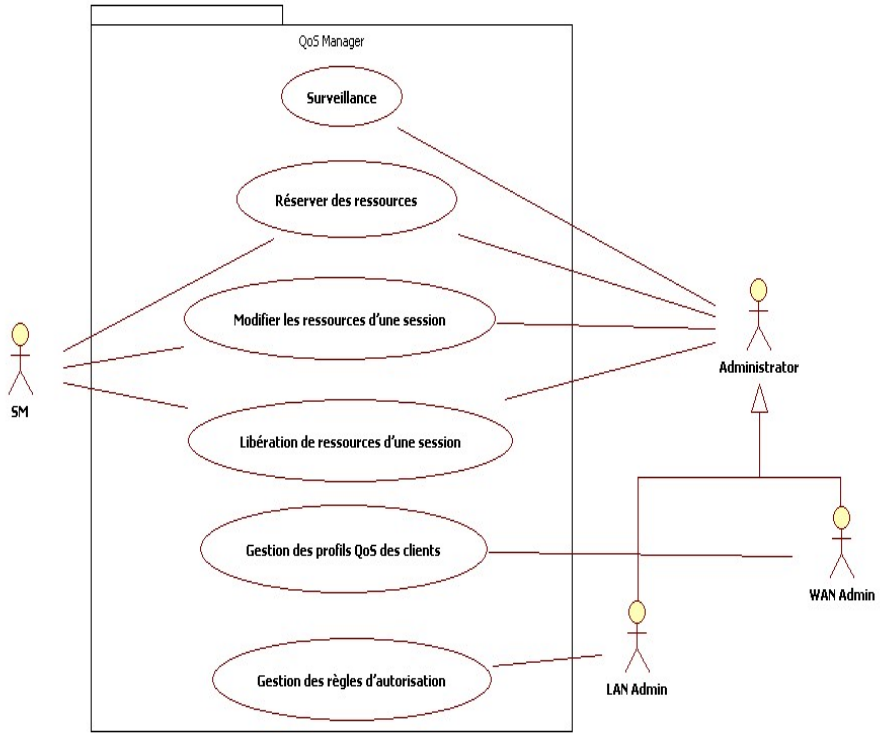


Figure 4.2 Diagramme de cas d'utilisation du système de gestion de QoS

Comme le montre la Figure 4.2, le **QM** doit assurer les cas d'utilisation suivants:

Réserver des ressources :

Le principal cas d'utilisation du **QM** est la réservation des ressources réseaux pour une session donnée. La réservation doit se faire sur les trois portions du chemin de données. Les deux acteurs externes du système peuvent déclencher cette fonction :

- Le **SM** doit être en mesure de réserver de la QoS pour une session déjà établie. Par exemple, avant de commencer le transfert d'un contenu, le **SM** s'adresse à son **QM** pour

modifier les paramètres de QoS de la session. Pour mettre en place la QoS voulue, le **QM** aura besoin d'une description de la QoS demandée pour cette session (bande passante, délais…) et des paramètres réseaux des différents portions de cette session, dans les deux LANs et dans le réseau de cœur (adresses IP, ports, …) ;

- Pour provisionner son réseau, l'administrateur peut demander au **QM** d'allouer des ressources pour l'éventuel trafic de ses clients. Par exemple, l'utilisateur peut demander à son **QM** de réserver des ressources dans son réseau domestique pour le trafic de son service de partage. De même, l'administrateur du réseau de l'opérateur peut préparer son réseau en allouant des ressources pour acheminer le trafic qui va être généré par les clients de son service de partage.

Modifier les ressources d'une session :

Le **SM** et l'administrateur doivent avoir la possibilité de modifier les paramètres d'une session. Les paramètres modifiables sont toutefois limités à ceux influençant la QoS de la session. En effet, il n'est pas autorisé de modifier la source ou la destination de la session en cours.

Libération de ressources d'une session :

La libération des ressources préalablement réservées peut intervenir dans les deux situations suivantes :

- A la fin de l'utilisation d'une session, le **SM** demande à son **QM** de libérer les ressources réseaux réservées à cette session ;
- L'administrateur, en cas de congestion de son réseau, peut reprendre des ressources à des sessions actives. Cette procédure, appelée préemption, peut être déclenchée par l'administrateur du réseau de l'opérateur, dans la portion réseau cœur, ou bien par l'utilisateur du service, dans son LAN.

Gestion des profils QoS des clients :

L'administrateur du réseau de cœur associe à chaque utilisateur un profil qui désigne les fonctions et les niveaux de QoS auxquels il a droit.

Gestion des règles d'autorisation :

Le système doit gérer des règles qui permettent à l'utilisateur de désigner quels autres utilisateurs ont le droit de demander de la QoS dans son LAN.

Surveillance :

La fonction de surveillance permet à l'administrateur de vérifier l'état de son réseau et donc de prévenir les cas de congestion. En plus, cela nous assure non seulement la cohérence de la QoS par l'aboutement des mécanismes de gestion de la QoS utilisés dans chaque réseau, mais également la vérification de la synchronisation des états (réservé, libéré, disponible, …) de la réservation dans chaque portion de réseau.

4.2.2.3 Architecture fonctionnelle générique du système de gestion de QoS

Après l'identification et la description des cas d'utilisation du système de gestion de QoS, nous allons décrire dans cette section l'architecture fonctionnelle générique de ce système et son intégration dans l'architecture globale du service de partage de contenus. Cette architecture est indépendante de la technologie à utiliser pour réaliser le système : elle a pour but de définir les principaux blocs fonctionnels qui vont constituer le système et leurs déploiements dans les différentes portions du chemin de données. Elle définira aussi l'interface entre ce système et le système d'accès à distance.

Sur la base de l'expression des besoins réalisée pendant la phase d'étude du contexte général, nous avons défini deux types de Liste de Contrôle de la QoS (QoS Control List QCL) pour gérer les droits de demande de QoS dans les LANs et dans les réseaux de cœur :

- Règle d'autorisation de QoS dans le réseau cœur : Ce type de QCL est géré par l'administrateur du service de partage et maintenu dans le profil du client lors de son inscription. Elle indique si l'utilisateur a le droit de solliciter la QoS désignée dans sa requête au niveau du réseau de cœur.
- Règle d'autorisation de QoS dans le LAN : Nous avons défini ce type de QCL pour permettre à l'utilisateur de donner le droit à chacun de ses contacts de réserver de la QoS dans son réseau. Elles sont stockées dans le LAN de l'utilisateur et ne sont pas publiés dans le réseau de l'opérateur car nous ne souhaitons pas que l'administrateur du service de partage puisse commander la réservation des ressources des réseaux des clients.

L'étude de l'état de l'art nous a montré que les techniques de gestions de QoS dans les LANs ne sont pas les mêmes que celles utilisées dans les réseaux de cœur, vu la différence entre ces deux types de réseaux. Cela nous a poussés à découper le système de gestion de QoS (**QM**) en deux composants : **QM-LAN**, déployé dans les LANs des utilisateurs, et **QM-WAN**, déployé dans le réseau de l'opérateur, comme le montre la figure 4.3.

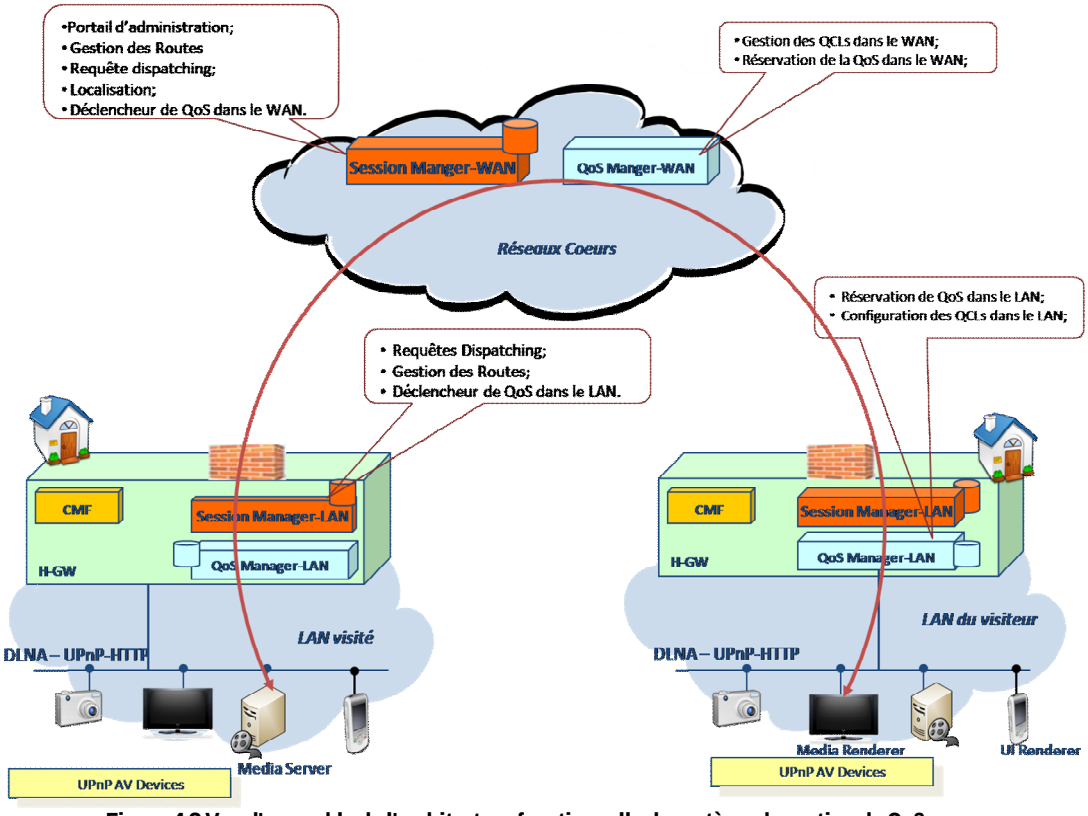


Figure 4.3 Vue d'ensemble de l'architecture fonctionnelle du système de gestion de QoS

Les fonctions entrant en jeu dans la commande de la réservation des ressources réseaux sont résumées dans le tableau 4.1. Certaines fonctions du système d'accès à distance, qui étaient utilisées pour l'établissement des sessions entre les LANs distants, ont été réajustées pour permettre la mise en place de la QoS. Dans le tableau 4.1, nous décrivons le rôle de ces fonctions dans la procédure de réservation de QoS sans rappeler leurs rôles dans la mise en place des sessions. Finalement, nous avons ajouté de nouvelles fonctions au **SM**, spécialement conçues pour la commande de la QoS.

Tableau 4.1 Fonctions entrant en jeu dans la procédure de réservation de QoS de bout en bout

Composant	Fonction	Description
QM-LAN	**Configuration des QCLs dans le LAN**	▪ Gérer les règles d'autorisations qui désignent le droit de chaque contact extérieur à réserver de la QoS dans le LAN.
	Réservation de la QoS dans le LAN	▪ Vérifier dans la base des QCLs si l'utilisateur distant a le droit d'émettre la requête de QoS reçue ; ▪ Prendre en charge la vérification des ressources réseaux disponibles dans le LAN et la configuration nécessaire pour mettre en place la QoS demandée ; ▪ Désigner les caractéristiques de QoS à demander dans le WAN et le LAN distant.
SM-LAN	**Requêtes Dispatching**	▪ Identifier les requêtes de QoS entrantes au LAN. ▪ ▪ diriger les requêtes entrantes vers le **QM-LAN**.
	Gestion des Routes	▪ Transférer la demande de QoS vers un LAN distant via le réseau de cœur.
	Déclencheur de QoS dans le LAN	▪ Déclencher la procédure de réservation de QoS de bout en bout.
QM-WAN	**Gestion des QCLs dans le WAN**	▪ Gérer les règles d'autorisations qui désignent le droit de chaque utilisateur à réserver de la QoS dans le WAN ; ▪ Vérifier dans la base des QCLs si l'utilisateur a le droit d'émettre la requête de QoS reçue.
	Réservation de la QoS dans le WAN	▪ Prendre en charge la vérification des ressources réseaux disponibles dans le WAN et la configuration nécessaire pour mettre en place la QoS demandée.
SM-WAN	**Portail d'administration**	▪ Implémenter l'interface utilisateur (UI) pour configurer les QCLs dans le **QM-WAN** ;
	Gestion des Routes	▪ Authentifier l'initiateur de la réservation ; ▪ Identifier les requêtes de QoS ; ▪ Vérifier les droits de l'appelant à envoyer une requête de QoS au LAN distant demandé.
	Requête dispatching	▪ Transférer la requête de réservation vers le LAN distant.
	Localisation	▪ Localiser le LAN distant.
	Déclencheur de QoS dans le WAN	▪ Rediriger les requêtes de QoS vers le **QM-WAN**.

Pour mieux comprendre l'interaction entre les composants du **SM** et du **QM** pendant la procédure de réservation de QoS, nous allons présenter le diagramme de séquence haut niveau du principal cas d'utilisation « réservation de ressources » de notre système de gestion de QoS.

La figure 4.4 décrit le scénario où la procédure de réservation de QoS est déclenchée dans le LAN du visiteur. Le fait de choisir d'amorcer la réservation de la QoS dans le réseau du visiteur et non dans le réseau visité, nous permet de faire plusieurs tentatives de réservation de QoS de bout en bout (en cas d'échec de réservation) avant de demander au réseau visité (l'appelé) de renvoyer le lien direct de récupération du contenu. Cela est possible si le Media Serveur UPnP A/V, qui contient le contenu choisi, supporte la fonction de ré-encodage.

Dans ce cas, le Media Serveur envoie dans sa réponse aux requêtes de parcourt des répertoires, la liste des contenus et leurs caractéristiques : le débit et particulièrement les encodages possibles pour chaque contenu. Si ce principe n'est pas obligatoire dans UPnP A/V, il est supporté dans les profils DLNA et donc implémenté par tous équipements certifiés DLNA. Dans ce cas, si la procédure de réservation de QoS de bout en bout échoue par manque de ressources, nous pouvons essayer de réserver moins de ressources en utilisant un autre encodage du contenu.

Dans ce scénario, l'évènement de déclenchement est la réception d'une demande de récupération de contenu au niveau du **SM-LAN** du visiteur (étape 1-2). Nous avons choisi cet événement car à ce stade le **SM-LAN** a la possibilité de connaitre les caractéristiques du contenu à transporter dans la session, et donc les paramètres de QoS à transmettre au **QM-LAN** pour demander la réservation de ressources.

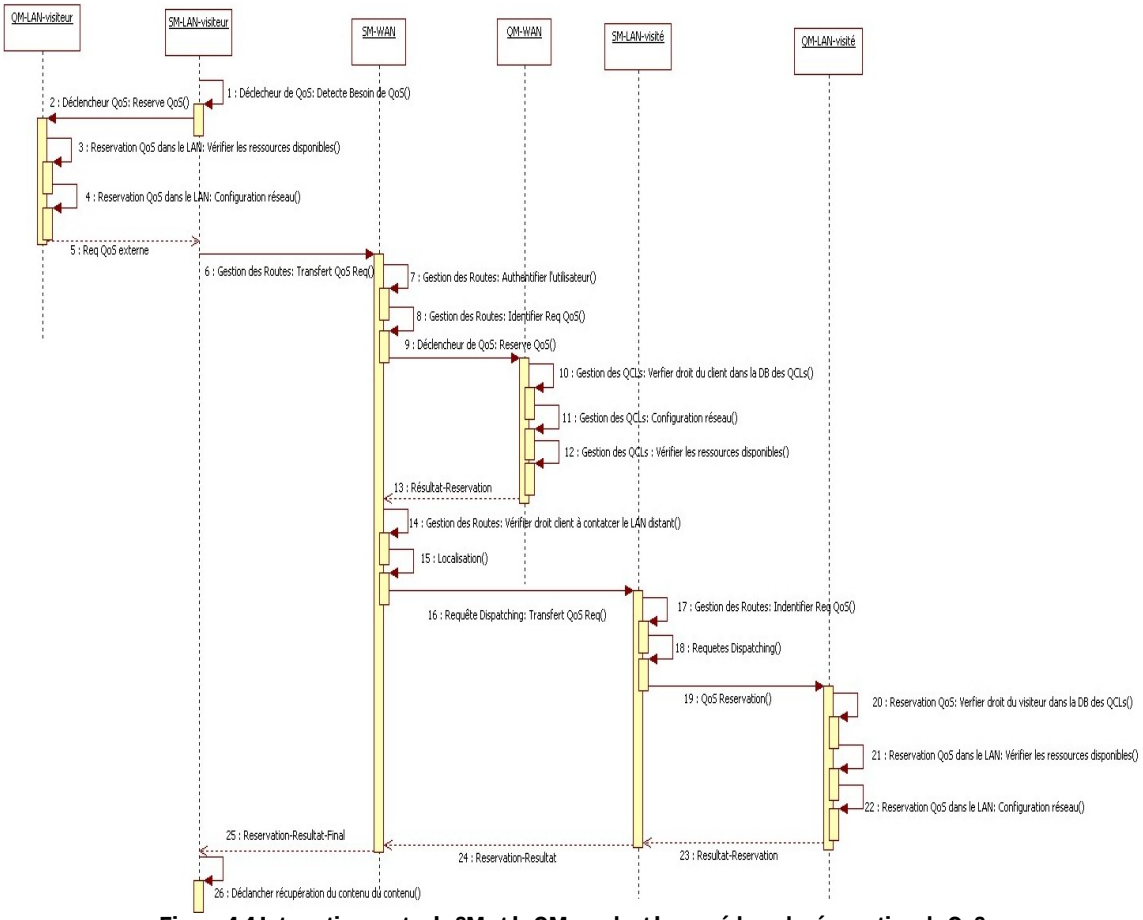


Figure 4.4 Interactions entre le SM et le QM pendant la procédure de réservation de QoS

A la réception de cette demande, le **QM-LAN** dans le LAN du visiteur vérifie la disponibilité des ressources dans son réseau (étape 3). Si ce test échoue, le **QM-LAN** renvoi un message d'erreur à son **SM-LAN**. Sinon, le **QM-LAN** met en place la réservation en effectuant la configuration réseau nécessaire (étape 4)[3]. Ensuite, le **QM-LAN** répond avec les caractéristiques de QoS qu'il a réussi à réserver, nécessaires pour déclencher la réservation de ressource dans le réseau de cœur et dans le LAN visité (étape 5). L'échange de la demande de QoS inter-maisons nous renvoie à la problématique de la sécurisation de la signalisation pour mettre en place les sessions entre les

[3] [3] Une variante peut consister à attendre l'accusé de réception avant de mettre en place la QoS ou réaliser la configuration en parallèle de la transmission de la requête au réseau cœur.

maisons, notamment la traversée du pare-feu et du NAT. En effet, les pare-feux des passerelles domestiques rejetteront ces requêtes entrantes dans leurs réseaux si elles ne sont pas authentifiées. De plus, ces requêtes doivent être correctement redirigées vers le composant qui gère la QoS dans le LAN, du fait de l'utilisation du NAT dans les réseaux domestiques. Finalement, il est également nécessaire à ce niveau de gérer le problème de l'adressage privée. En effet, la gestion de la QoS impose de connaitre les adresses de la source et de la destination du flux. Ici, il s'agit d'adresses privées. Il est donc nécessaire de découper cette relation en introduisant la partie du réseau cœur caractérisée elle par l'utilisation d'adresses publiques. Nous avons donc bien trois segments:

- adresse privée du MediaServer dans le LAN visité / adresse publique de la passerelle domestique du LAN visité ;
- adresse publique de la passerelle domestique du LAN visité / adresse publique de la passerelle domestique du LAN visiteur ;
- adresse publique de la passerelle domestique du LAN visiteur / adresse privée du MediaRender du LAN visiteur.

Vu que notre système d'accès à distance a déjà proposé des solutions à cette problématique, nous allons le réutiliser pour transférer cette signalisation de mise en place de la QoS. Les requêtes de QoS sortantes du LAN sont alors relayées vers le LAN destination via le **SM-WAN**, de la même manière que les requêtes sortantes du système d'accès à distance (étape 6). Le **SM-LAN** aura alors une tâche supplémentaire à effectuer qui consiste à remplacer les adresses privées dans la requête de QoS initiale par les adresses publiques connues du réseau cœur.

Lorsque ce type de requêtes arrive au **SM-WAN**, ce dernier authentifie comme d'habitude l'émetteur de la requête (étape 7). Il identifie ensuite le type de la requête (requête QoS) et la transfère vers le **QM-WAN** (étape 8-9). Comme dans le LAN, le **QM-WAN** vérifie dans sa base de QCLs l'aptitude de l'utilisateur à demander de la QoS (étape 10). Par la suite, il vérifie la disponibilité des ressources de son réseau pour répondre à cette demande (étape 12). Si l'une de ces vérifications échoue, le **QM-WAN** renvoi un message d'erreur à son **SM-WAN**, qui le transmet par la suite au **SM-LAN** initiateur de cette réservation. Ce dernier peut réessayer de relancer cette procédure en demandant moins de ressources. Dans le cas du succès de la réservation de QoS dans le WAN, le **SM-WAN** relaie cette demande de QoS vers le LAN destination, une fois le droit de l'émetteur à transmettre des requêtes au LAN de destination vérifié (étapes 14-16).

Dans le LAN visité, le pare-feu de la passerelle domestique accepte la requête de QoS parce qu'elle est authentifiée et autorisée par le **SM-WAN**. Et grâce à la configuration par défaut du NAT, la requête en provenance du **SM-WAN** est redirigée vers le **SM-LAN** pour qu'elle soit traitée par ce dernier. Le **SM-LAN** identifie tout à d'abord le type de la requête comme une requête de QoS (étape 17) et la transmet à son **QM-LAN** (étapes 18-19). Au préalable, comme dans le réseau du visiteur, le **SM-LAN** aura pris soin de modifier la requête initiale pour remplacée les adresses publiques par les adresses privées correspondantes. Le **QM-LAN** vérifie dans sa liste de QCLs si l'initiateur de la session qui demande de la QoS a bien le droit de réserver des ressources réseaux dans son réseau (étape 20). Le **QM-LAN** vérifie ensuite l'état de son réseau et met en place la configuration nécessaire (étapes 21-22). Le résultat de la réservation finale, de bout en bout, est relayé du **SM-LAN** du LAN visité par le **SM-WAN** vers le **SM-LAN** du visiteur (étapes 23-25). En cas de réponse positive, le **SM-LAN** déclenche la procédure de récupération du contenu comme vue au chapitre 3 (étape 26), sinon il réessaye de lancer une autre réservation avec moins de ressources.

4.3 Réalisation du système de gestion de QoS

Dans cette section, nous allons décrire la phase de réalisation de notre système de gestion de QoS de bout en bout et son intégration dans le service de partage de contenus à distance. Nous commençons par la présentation de l'étude de la mise en place de la QoS dans le LAN. Ensuite,

nous enchainons avec l'étude de la brique de gestion de QoS dans le WAN. Et à la fin de cette section, nous présentons l'assemblage de ces briques et leur intégration dans le système d'accès à distance.

4.3.1 QoS dans le réseau local

Pour étudier la QoS dans les réseaux domestiques des utilisateurs, nous allons décrire les scénarii possibles pour la mise en place de la QoS dans notre contexte de partage de contenus à distance. Par la suite, nous étudierons l'adaptation des techniques de gestion de la QoS que nous avons identifiées lors de l'étude de l'état de l'art, en vu de les réutiliser dans notre système de gestion de la QoS.

Dans toute cette section, nous prenons comme hypothèse que le **QM-LAN** est déployé dans la passerelle domestique. Nous avons pris ce choix pour faciliter la synchronisation de la QoS entre les trois portions du chemin de données du service de partage (ç.-à-.d. LAN visiteur, WAN, LAN visité), vu que la passerelle domestique délimite ces trois portions. De plus, comme cet équipement est sur le chemin de données, il sera de toute façon nécessaire, au minimum, d'interagir avec lui pour la configuration de la QoS. Enfin, les études normatives sur le sujet place la passerelle domestique au cœur du dispositif de gestion de la QoS et lui font jouer le rôle d'acteur central.

4.3.1.1 Topologie du LAN

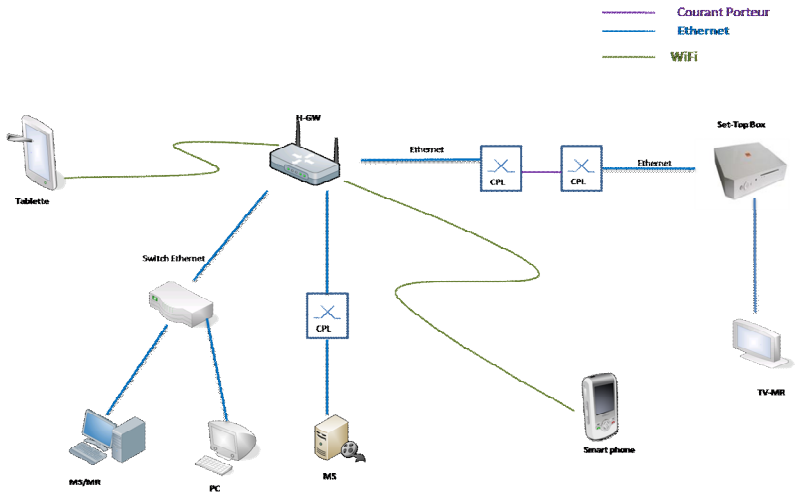


Figure 4.5 Topologie ciblée d'un réseau LAN

La figure 4.5 représente la topologie et les technologies que nous envisageons de supporter dans nos scénarii. La topologie tourne autour d'un nœud central qui est la passerelle domestique.

La télévision est généralement raccordée à un décodeur (Set-top Box) qui implémente les fonctions d'un Media Renderer (MR). Les autres équipements multimédias sont raccordés au réseau LAN avec trois types de lien couramment rencontrés dans les réseaux domestiques :

- WiFi (IEEE 802.11) [73] : Les routeurs commercialisées proposent des réseaux WiFi à infrastructure (le Point d'accès du réseau est la passerelle domestique);
- CPL (Courants Porteurs en Ligne) : Le CPL permet aux équipements du LAN de se raccorder en utilisant le réseau électrique de la maison ;
- Ethernet : L'équipement peut être raccordé directement à la passerelle domestique ou bien derrière un commutateur Ethernet.

Nous avons sélectionné ces trois technologies représentatives des réseaux domestiques car elles nécessitent chacune un mécanisme différent pour la gestion de la QoS. Il nous a paru alors indispensable dans notre étude de proposer une solution de mise en cohérence des mécanismes

de gestion de QoS de ces trois technologies dans notre proposition de gestion de la QoS de bout en bout.

4.3.1.2 Scénarii de mise en place de la QoS dans le LAN

Dans le service de partage de contenus que nous étudions, la réservation de QoS dans les LANs des clients s'échangeant des contenus, ne se fait pas de la même manière dans le réseau du visiteur que dans le réseau visité.

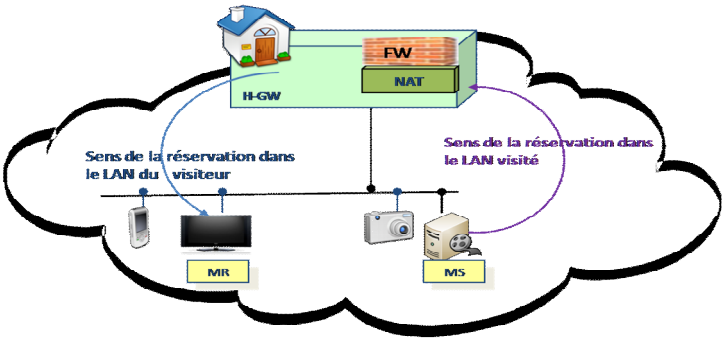


Figure 4.6 Scénarii de réservation de QoS dans le LAN

Réservation de QoS dans le réseau visité

Dans le réseau domestique visité, le **QM-LAN** doit réserver des ressources pour le trafic allant du Média Serveur (MS), qui contient le contenu à transférer, vers la passerelle domestique comme le montre la figure 4.6. Autrement dit, il s'agit d'une réservation de QoS pour un flux sortant (du point de vue du réseau domestique).

Le **QM-LAN** doit être en mesure de supporter les différentes technologies que le client peut utiliser pour raccorder son MS au LAN : Ethernet, WiFi, CPL.

Réservation de QoS dans le réseau du visiteur

Comme le montre la figure 4.6, le sens du trafic que le service de partage génère dans le réseau domestique du visiteur est l'inverse du sens du trafic dans le réseau visité i.e. un flux entrant. Dans ce cas de figure, le trafic provient de l'extérieur de la maison vers le Media Renderer (MR). Donc, le **QM-LAN** doit réserver pour ce trafic des ressources à partir de la passerelle domestique vers le MR en question.

Le **QM-LAN** doit aussi être en mesure de supporter les différentes technologies que le client peut utiliser pour raccorder son MR au LAN : Ethernet, WiFi ou CPL.

4.3.1.3 UPnP QoS Vs AVB

Afin d'implémenter le composant **QM-LAN**, nous avons étudié l'aptitude des technologies UPnP QoS et AVB à réaliser les cas d'utilisation que nous avons identifié.

Audio Video Bridging

Pour gérer la QoS dans le LAN en utilisant AVB, nous devons inclure dans tous les équipements intégrant un UPnP Média Serveur des briques « AVB Talker », et dans les équipements UPnP Média Renderer des briques « AVB Listeners » et de plus dans les CPL et les Switchs des « bridges AVB ». Finalement, le **QM-LAN** doit intégrer les fonctions d'« AVB Listener » et « AVB Talker ».

Gestion des règles d'autorisation

Le groupe de travail AVB n'a pas traité dans ses protocoles la problématique de gestion des

règles d'autorisation de réservation de QoS. Donc, nous devons implémenter cette fonctionnalité du **QM-LAN** au niveau de la couche applicative de ce composant.

Surveillance

L'AVB propose une solution distribuée pour gérer la QoS dans le LAN. De ce fait, cette solution ne définit pas une entité ou une technique pour détenir une vision globale du réseau et donc pour surveiller les trafics transférés. Cette fonction doit alors être développée au niveau de la couche applicative dans le **QM-LAN**.

Réservation de ressources

AVB, avec son standard SRP, offre aux applications multimédias un ensemble de protocoles (MSRP, MMRP, MVRP) pour réserver des ressources réseaux dans le LAN. Pour donner plus de flexibilité aux applications, AVB leur permet d'annoncer leurs flux médias avec des protocoles « haut niveau » (couche service) afin de les signaler aux applications des destinataires potentiels. Cependant, cette étape est optionnelle. Dans notre contexte de partage de contenus, UPnP A/V utilise le protocole SSDP pour annoncer des services dans le LAN, nous avons alors choisi de réutiliser ce même protocole pour annoncer les flux AVB dans le LAN.

Réservation dans le LAN visité

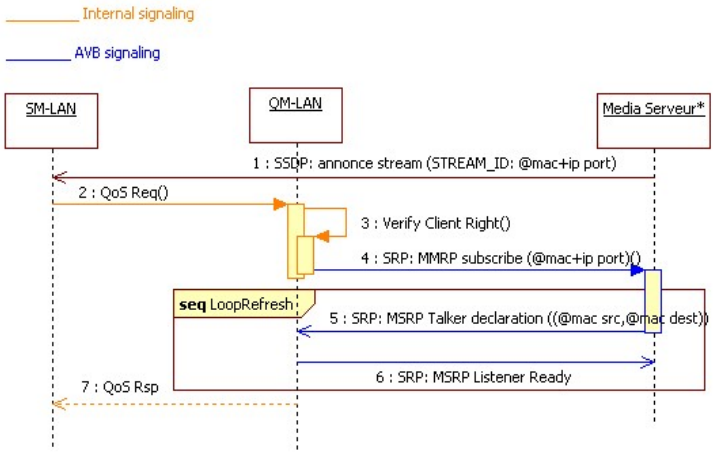


Figure 4.7 Réservation de ressources réseau dans le LAN visité, avec AVB

Dans le LAN visité, l'annonce des flux est prise en charge par les Media Serveurs (MS) qui partagent les contenus vu qu'ils possèdent leurs caractéristiques. Comme les MS ne peuvent pas annoncer tous leurs contenus comme des flux dans le réseau, nous avons décidé que les MS annoncent trois flux représentant les trois classes de services de notre service de partage: la classe « Données » pour l'envoi des photos ; une classe « Audio » pour l'envoi des morceaux de music et la classe « Vidéo » pour l'envoi des vidéos. Avec ces annonces, le **SM-LAN** aura connaissance des MS (adresses mac, classes de service, Stream ID) qui proposent de la QoS pour le transfert de leurs contenus (Figure 4.7 étape 1).

Dans ce scénario, la requête de réservation est reçue par le **SM-LAN** depuis le WAN. La requête désigne la classe de service et la bande passante demandée pour la session. Le **SM-LAN** cherche dans sa liste d'annonce de flux si le MS désigné dans la requête a annoncé la classe de service indiquée par l'émetteur. Si la vérification réussie, il relaie la requête de QoS à son **QM-LAN** (étape 2) pour déclencher la réservation de ressources, sinon il répond à la requête de QoS externe avec un message d'erreur.

Lorsque le **QM-LAN** reçoit une requête de QoS du **SM-LAN**, il vérifie dans sa liste de QCLs si l'émetteur de la requête a le droit de réserver la QoS demandée dans son LAN (étape 3). En cas d'échec de cette vérification, le **QM-LAN** renvoie un message d'erreur à son **SM-LAN**. Sinon, le **QM-LAN** va jouer le rôle d'un « AVB Listener » en envoyant une requête « MMRP subscribe » pour s'abonner au flux du MS (étape 4). Cette étape est optionnelle dans la procédure de réservation de ressources dans le standard AVB, mais elle évite à l'émetteur du contenu d'inonder le LAN avec ses déclarations de réservation AVB en indiquant les adresses destinations (@ mac destination) de la réservation (étape 5). Ceci est possible en activant l'option de « Talker pruning » dans la requête envoyée. Si la déclaration du MS parvient au **QM-LAN** à l'état « Talker Advertise » cela signifie que la réservation de ressources a réussi (étape 5). Donc le **QM-LAN** confirme la réservation en répondant au MS avec un « Listener Ready ». En même temps le **QM-LAN** renvoie à son **SM-LAN** l'information du succès de la réservation (étape 6). Dans le cas où la déclaration du MS ne trouve pas assez de ressources réseau, le **QM-LAN** reçoit un « Talker Failed » et déduit alors que la réservation a échoué. Le **QM-LAN** renvoie dans ce cas à son **SM-LAN** un message d'erreur.

Dès que le MS reçoit un message « Listener Ready » il peut commencer à envoyer son flux vers la destination, mais dans notre contexte le MS doit attendre la requête au niveau service UPnP A/V pour commencer à envoyer son flux.

Pour maintenir cette réservation, le MS doit envoyer périodiquement une déclaration du flux (Talker Advertise) vers son « Listener » qui est le **QM-LAN**.

Réservation dans le LAN du visiteur

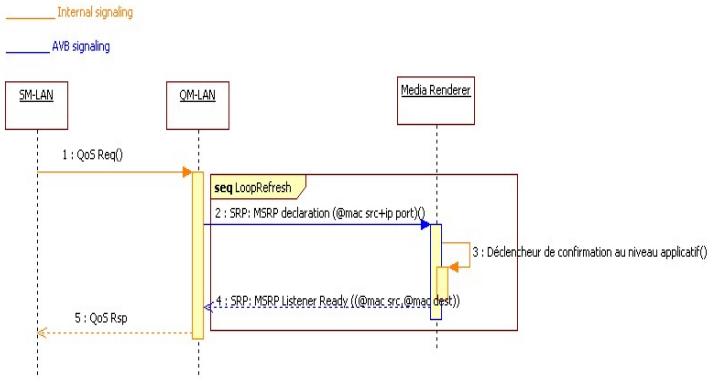


Figure 4.8 Réservation de ressources réseau dans le LAN visiteur, avec AVB

Du côté du LAN du visiteur, l'origine du flux n'est pas dans le LAN, donc nous ne pouvons pas l'annoncer. Dans ce scénario, nous sommes alors contraints de supprimer les deux étapes optionnelles de l'annonce des flux avec SSDP et de l'enregistrement MMRP.

Comme la réservation doit se faire de la passerelle domestique vers le Media Renderer, le **QM-LAN** va jouer le rôle d'un « AVB Talker ». En effet, lorsque ce dernier reçoit une requête de QoS demandant de réserver des ressources avec certaines caractéristiques QoS (i.e. classe de service et bande passante) vers un MR de son réseau, il envoie dans le LAN une déclaration de flux « MSRP : Talker» en diffusion sur le LAN (i.e. sans activer l'option Talker pruning).

Cette déclaration permet de pré-réserver de la QoS dans le LAN et de s'assurer qu'il y a des ressources suffisantes pour ce flux. Pour confirmer la réservation, il faut que l'équipement du MR s'abonne à ce flux. Sauf que l'enregistrement du MR pour ce flux demande un déclencheur au niveau applicatif de l'équipement, ce qui implique la modification de l'application UPnP A/V Renderer du client. Cette solution ne correspond pas à notre objectif car nous voulons que notre

service de partage reste transparent au service UPnP A/V standard.

Nous pouvons déduire de cette étude que l'utilisation de l'AVB pour la réservation de QoS dans ce scénario (du côté du LAN du visiteur) n'est pas très adapté et complexe à intégrer dans notre service de partage puisqu'elle nécessite une modification au niveau des applications UPnP A/V des clients.

Libération des ressources

Pour libérer les ressources d'une réservation, le receveur du flux (Lsitener) se désabonne de l'annonce de l'émetteur (Talker).

Modification de ressources

Si l'utilisateur change le type des contenus qu'il consomme, le **SM** doit modifier la réservation de ressources de la session utilisée. Par exemple, si l'utilisateur consommait des photos et veut récupérer ensuite du même LAN distant une vidéo, le **SM** doit demander plus de ressources réseau pour envoyer la vidéo sélectionnée.

Cependant, dans ces situations AVB n'offre pas aux applications une primitive pour modifier les paramètres d'une réservation donnée. Donc, la solution pour modifier une réservation est d'annuler l'ancienne réservation et d'initier une nouvelle avec les paramètres voulus. Ce n'est cependant pas une contrainte très forte. En effet, l'arrêt de la consultation des photos aura pour effet automatique le désabonnement au flux, et donc, la libération des ressources. La sélection de la vidéo déclenchera automatiquement l'abonnement au flux vidéo et donc la négociation de ressources correspondante.

UPnP QoS

Pour garantir la QoS dans le LAN avec UPnP QoS, tous les équipements entrant en jeu pendant l'envoi du flux doivent implémenter le service « UPnP QosDevice », à savoir la passerelle domestique, les Media Renderer, les Media Serveur et la Set-Top Box.

Dans le cas où le flux passe par des équipements de niveau 2 (i.e. équipement CPL), UPnP QoS v3 a défini le principe de l'UPnP QosSegment afin de déléguer la gestion de la QoS de ce segment à une autre technologie, par exemple la technologie AVB.

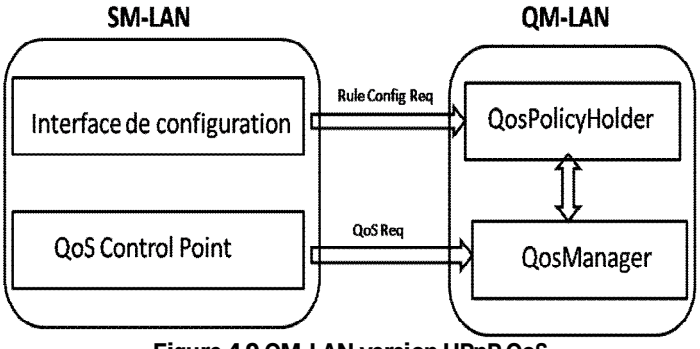


Figure 4.9 QM-LAN version UPnP QoS

Comme le montre la figure 4.9, le **QM-LAN** est composé par :

- Un service « UPnP QosManager » pour commander la réservation de QoS dans le LAN ;
- Un service « UPnP QosPolicyHolder » pour gérer la stratégie de gestion de QoS dans le LAN et notamment les règles d'autorisations de QoS des clients.

Pour initier la gestion de QoS dans le LAN, le **SM-LAN** intègre un point de contrôle UPnP QoS afin d'envoyer des demandes de QoS vers le **QM-LAN**.

Gestion des règles d'autorisation

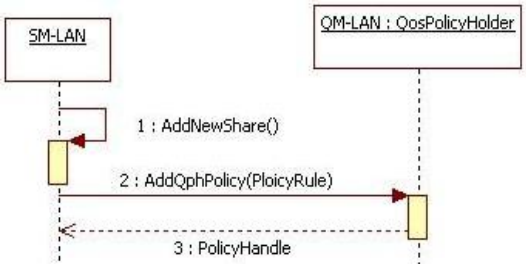


Figure 4.10 Configuration des QCLs avec UPnP QoS

Grâce à son service « UPnP QosPolicyHolder », le **QM-LAN** a la possibilité de configurer les QCLs: règles définissant le droit de chaque contact distant à réserver de la QoS dans le LAN. Avec ce service le **QM-LAN** offre à son client final, qui est le **SM-LAN**, une interface pour gérer ces règles. Cependant, la signification et la représentation des règles exprimant les besoins des applications des clients, stockées dans le service « UPnP QosPolicyHolder », ne sont pas définies par la spécification UPnP QoS et laissées à la guise de l'utilisateur ou plus exactement du constructeur. Cette thématique de recherche est traitée dans un doctorat au LAAS-CNRS à l'aide des ontologies. Ces travaux ont aussi contribué au projet Feel@Home [75]. Pour nos besoins, nous sauvegardons juste l'information : « un client A » est autorisé ou non à demander de la QoS dans le LAN.

Cette procédure de configuration peut être déclenchée par le **SM-LAN**, au moment où l'utilisateur définit un nouveau partage.

Surveillance

Avec son service « UPnP QosManager », le **QM-LAN** peut récupérer les informations de QoS à partir des équipements de son réseau, en envoyant des requêtes à leurs services « UPnP QosDevice ». Les informations collectées permettent au **QM-LAN** de constituer une vision de l'état de son réseau et donc de le surveiller.

Réservation de ressources

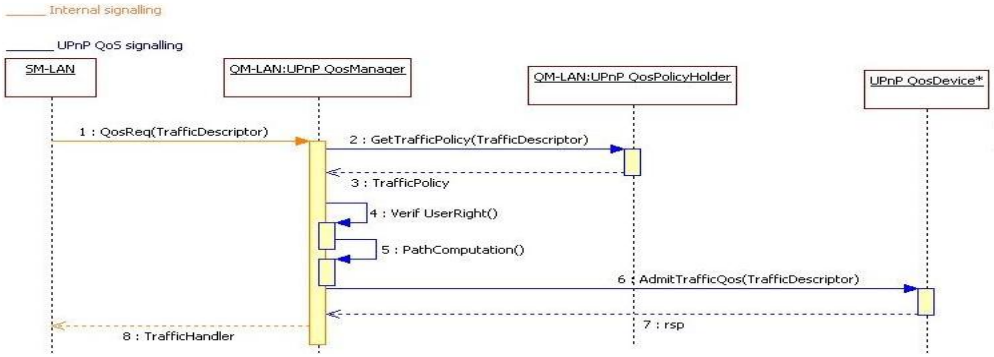


Figure 4.11 Réservation de ressources dans le LAN, avec UPnP QoS

A la différence d'AVB, UPnP QoS commande la QoS dans le LAN d'une manière centralisée à l'aide du service « UPnP QosManager ». Donc le sens de la réservation n'a pas d'impacte sur la cinématique de la réservation. La figure 4.11 représente la signalisation à réaliser pour mettre en place la QoS qui est identique pour les deux scénarii identifiés dans la première partie de cette section.

Avec son Point de contrôle UPnP QoS, le **SM-LAN** formule une requête de QoS vers son **QM-LAN** (étape 1). Cette requête intègre la description du trafic à transmettre (i.e. adresse source, adresse destination, bande passante…) et l'identifiant du demandeur de la réservation. Dans le

QM-LAN, le service «UPnP QosManager» reçoit la requête du **SM-LAN** et commence par récupérer la politique à appliquer à cette requête à partir de son service «UPnP QosPolicyHolder» (étapes 2-3). La réponse de ce dernier permet au service « UPnP QosManager » de vérifier si le demandeur de QoS a le droit de réserver des ressources réseaux dans le LAN (étape 4). Au cas où la vérification échoue, le **QM-LAN** renvoie un message d'erreur à son **SM-LAN**. Si cette vérification réussit l'«UPnP QosManger» détermine les équipements entrant en jeu dans le transfert de ce flux dans le LAN (UPnP Path) (étape 5). Ensuite, il envoie une requête d'admission d'appel (AdmitTrafficQos) vers les services «UPnP QosDevice» embarqués dans ces équipements (étape 6) situés sur le chemin de données et identifiés précédemment. Ce type de requêtes permet d'initier les deux modes de demandes de QoS permis par UPnP QoS à savoir l'admission d'appel et la différenciation des flux (priorisation)[4]. Lorsque le service «UPnP QosManager» reçoit toutes les réponses des « QosDevice » qu'il a contactés, il envoie la réponse de la réservation au **SM-LAN** (étapes 7-8).

Modification de ressources

Si le **SM-LAN** a besoin de modifier les ressources allouées à une session, il envoie une requête de mise à jour à son **QM-LAN** (i.e. UPnP UpdateTrafficQoS Req). Le traitement de cette requête sera identique à celle d'une nouvelle réservation, au niveau du service « UPnP QosManager » : i) il récupère du service «UPnP QosPolicyHolder » la politique à appliquer à cette requête, ii) vérifie le droit du demandeur à émettre cette requête iii) et finalement demande aux services «UPnP QosDevice » des équipements qui participent au transfert du flux de la session en question de mettre en place une nouvelle configuration pour assurer les nouveaux critères de QoS exprimés dans cette requête.

Libération des ressources

Pour libérer les ressources réseaux d'une session terminée, le **SM-LAN** envoie une requête de libération (i.e. UPnP ReleaseTrafficQos Req) à son **QM-LAN**. A la réception de cette requête, le service « UPnP QosManager » du **QM-LAN** contacte les services « UPnP QosDevice » des équipements concernés par cette réservation pour libérer les ressources allouées à cette session.

Bilan sur la gestion de la QoS dans le LAN

Avant de passer à l'étude de la QoS dans le réseau de cœur, nous donnons ici un premier bilan sur l'étude de la gestion de QoS dans le LAN. En effet, nous avons constaté que la technologie AVB présente quelques limitations pour la réalisation de notre composant **QM-LAN** (i.e. absence de la gestion de la politique de QoS dans le LAN, difficulté de déclencher une réservation de ressources à partir du receveur du flux).

De l'autre côté, la technologie UPnP QoS, avec sa gestion centralisée de la QoS, est plus adaptée à réaliser les scénarii que nous avons envisagé de prendre en compte. Comme notre service de partage s'appuie sur UPnP, il est relativement aisé d'ajouter le support de la gestion de QoS via UPnP QoS (ce qui est également préconisé par le standard dans le scénario de l'utilisation d'UPnP QoS conjointement avec UPnP A/V). Cependant, la seule limitation pour UPnP QoS est le besoin d'une autre technologie pour réserver de la QoS dans les réseaux CPL. En effet, les CPL sont des équipements de niveau 2 seulement. De ce fait, il n'embarque pas de pile protocolaire de niveau 3, et donc ne peuvent pas supporter ni UPnP ni UPnP QoS.

Même si les deux technologies présentent chacune des points forts et des points faibles, il est clair que la technologie UPnP QoS est mieux adaptée qu'AVB et plus facile à intégrer dans notre système d'accès à distance. C'est pourquoi notre décision est d'opter pour l'utilisation d'UPnP

[4] Dans le cas d'une demande de priorisation des flux, le service QoS Manager aura au préalable récupéré du service QoSPolicyHolder la politique de priorisation à mettre en place durant l'étape 2 en plus de la vérification des droits de l'utilisateur.

QoS dans le LAN pour réaliser notre système **QM-LAN** tout en supportant AVB pour les équipements de niveau 2 seulement en tant que relais de mise en place de la QoS via la notion d'UPnP QoS segment.

4.3.2 QoS dans les réseaux de cœur

Dans cette partie, nous allons présenter la réalisation du composant **QM-WAN** à intégrer au **SM-WAN** pour garantir la QoS dans le réseau de cœur. Comme la technologie utilisée dans le **SM-WAN** a un impact sur les choix nécessaires à la réalisation du **QM-WAN**, nous organisons cette partie en deux sections, la première présentant la réalisation du **QM-WAN** pour la version de **SM-WAN** utilisant le Framework IMS et la deuxième présentant la réalisation du **QM-WAN** à intégrer dans la solution « *HTTP*».

4.3.2.1 Gestion de la QoS avec l'IMS

Dans la réalisation IMS de notre système d'accès à distance, nous avons utilisé une plate-forme centrale déployée dans le cœur IMS que nous avons nommé **RA-AS** (Remote Access Application Server). Cette plate-forme implémente les fonctions du composant **SM-WAN** de notre système d'accès à distance. Pour facilité l'intégration du **QM-WAN** avec le **SM-WAN**, nous avons choisi de déployer ce nouveau composant dans la même plate-forme en ajoutant les fonctionnalités du **QM-WAN** au **RA-AS**, comme le montre la figure 4.12.

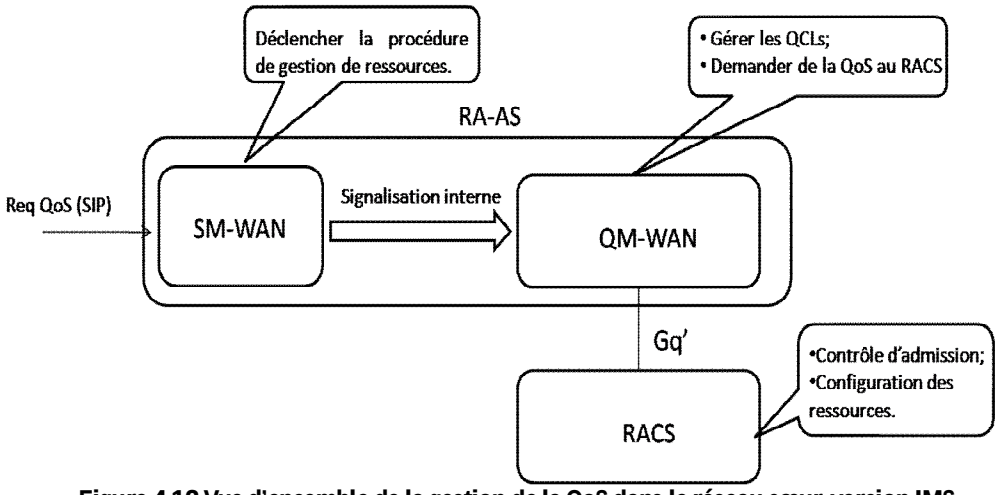


Figure 4.12 Vue d'ensemble de la gestion de la QoS dans le réseau cœur, version IMS

Gestion des règles d'autorisation

Pour la fonction « Gestion des QCLs dans le WAN», nous continuons à utiliser les fonctionnalités du serveur de présence de notre plate-forme **RA-AS**. En effet, nous envisageons de stocker les règles d'autorisation de QoS (QCL) en tant qu'indication de présence. Donc, si un utilisateur a le droit de réserver de la QoS dans le WAN, la ressource « QoS» sera présente pour cet utilisateur. La configuration de ce paramètre se fait au moment de l'inscription du client au service de partage de contenus.

Gestion de la QoS dans le WAN

La procédure de traitement des requêtes de QoS dans le WAN se déroule comme suit :

i. Détection de la demande de QoS

Le rôle du **SM-WAN** dans la procédure de traitement d'une requête de QoS est de détecter la demande de QoS envoyée par le client et de la transférer au **QM-WAN**. Comme nous échangeons les paramètres de la session dans le SDP de la signalisation SIP, nous utiliserons aussi le SDP pour échanger les paramètres de QoS. Le champ « a=**FHSession** » du SDP désigne le statut de la

session. Nous définissons une nouvelle valeur de ce champ « ContentWithQoS » pour indiquer au **RA-AS** que cette session a besoin de la QoS. Donc, lorsque le **SM-WAN** reçoit une requête avec un statut « ContentWithQoS » il en déduit qu'il doit demander de la QoS et donc transfère la requête à son **QM-WAN**.

ii. Contrôle d'admission au niveau service

Lorsque le **QM-WAN** reçoit une requête de QoS (i.e. réservation, modification, libération de ressources), il commence par extraire les paramètres de QoS transmis dans le SDP (i.e. userID, classService, bande passante, adresse IP source, adresse IP destination, ...). Il vérifie tout d'abord dans sa base de données de QCLs si l'émetteur de la requête (userID) a le droit de demander de la QoS. En d'autres termes, le **QM-WAN** vérifie si la ressource « QoS » est présente pour l'utilisateur en question. Après cette vérification, avec les paramètres extraits du SDP, le **QM-WAN** envoi une requête de QoS vers le **RACS** de son domaine pour mettre en place la demande reçue (réservation, modification, libération).

iii. Mise en place de la demande de QoS

Afin de permettre à notre service de partage de contenus de réserver de la QoS dans le réseau cœur, l'administrateur du réseau doit configurer son **RACS** (i.e. fonction SPDF) de façon à accepter les requêtes de QoS en provenance de la plate-forme **RA-AS** via l'interface Gq'.

En effet, pour réaliser la fonction du **QM-WAN**, « Réservation de la QoS dans le WAN », nous avons eu recours à la fonction **RACS** du cœur IMS. Cette fonction permet au **QM-WAN** de vérifier la disponibilité des ressources pour assurer le transfert du trafic avec les paramètres de QoS exprimés dans la requête. Une fois la requête admise, le **RACS** commande les ressources nécessaires et renvoie une réponse au **QM-WAN** client.

4.3.2.2 Gestion de la QoS pour la solution « HTTP»

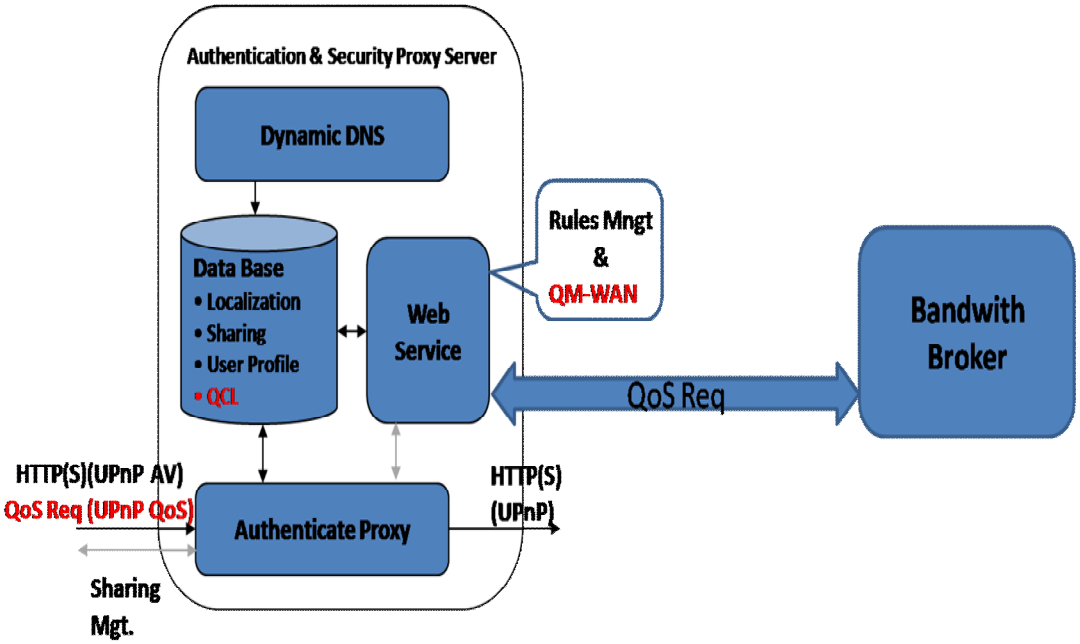


Figure 4.13 Vue d'ensemble de la gestion de la QoS dans le réseau cœur, version http

Dans la réalisation « HTTP» de notre système d'accès à distance, nous avons utilisé une plate-forme centrale déployée dans le réseau cœur que nous avons nommé **ASP** (Authentication & Security Proxy Server). Cette plate-forme implémente les fonctions du composant **SM-WAN**. Comme dans la solution IMS, nous avons choisi de déployer le composant **QM-WAN** dans la

même plate-forme centrale (i.e. **ASP**) afin de faciliter son intégration.

Gestion des règles d'autorisation

Nous avons ajouté dans le composant « Web Service » de l'**ASP** un nouveau module pour implémenter la fonction « Gestion des QCLs dans le WAN ». Les règles d'autorisation de QoS dans le WAN seront stockées dans la base de données de l'**ASP**, comme le montre la figure 4.13. La configuration de ces règles est faite par l'administrateur du service au moment de l'inscription de l'utilisateur au service de partage de contenus.

Gestion de la QoS dans le WAN

Les étapes de la procédure de traitement des requêtes de QoS dans le WAN est la même que pour la solution IMS :

i. Détection de la demande de QoS

Afin de permettre à l'**ASP** de savoir si la session en cours demande de la QoS ou pas, nous avons choisi d'insérer un nouvel entête (FHqoS) dans les requêtes HTTP envoyées vers l'**ASP** et qui peut prendre deux valeurs : YES, NO. Lorsque l'**ASP** reçoit une requête contenant ce type d'entête avec la valeur « YES », la fonction « Requête Dispatching » de l'**ASP** déduit que la session demande de la QoS et renvoie alors la requête au **QM-WAN**.

ii. Contrôle d'admission au niveau service

La fonction du **QM-WAN** qui vérifie le droit du client à demander de la QoS dans le WAN est prise en charge par un nouveau module dans le composant « Web Service » de l'**ASP**. Ce module vérifie dans la base de données de l'**ASP** s'il y a une règle qui autorise le client à réserver des ressources dans le réseau de cœur. Ensuite, le **QM-WAN** procède à la dernière étape du traitement de la requête de QoS qui est la mise en place de la demande.

iii. Mise en place de la demande de QoS

Rappelons que notre objectif n'est pas de proposer de nouvelles techniques de gestion de QoS dans le WAN. Il consiste plutôt à commander la mise en place de la QoS. Donc la réalisation de cette fonction nous renvoie aux techniques de gestion de QoS pour les réseaux de cœur IP proposées dans l'état de l'art.

Etant donné que notre service de partage de contenus s'adresse au grand public, l'utilisation des techniques de réservation de QoS par flux n'est pas recommandée parce qu'elles n'auront pas une bonne performance dans un tel contexte. Les techniques d'agrégation des flux seront plus adaptées à notre service. Notre étude de l'état de l'art nous a démontré que le modèle DiffServ, standardisée par l'IETF, offre l'environnent le plus complet dans cette famille de techniques. En effet, DiffServ défini les mécanismes nécessaires pour implémenter nos trois classes de services (i.e. Audio, Vidéo, Données) et de les gérer dans un réseau IP. Et pour éviter la congestion de notre réseau, le modèle DiffServ recommande l'utilisation d'un nœud centrale (i.e. Bandwith Broker) pour effectuer un contrôle d'admission pour vérifier la disponibilité des ressources pour le nouveau flux et donc protéger les trafics existants du réseau. Comme le montre la figure 4.11, ce nœud sera sollicité par le composant **QM-WAN** de l'**ASP**.

4.3.3 Intégration de la QoS de bout en bout

A ce stade, nous avons terminé l'étude de la réalisation des deux composants constituant notre système de gestion de QoS : le **QM-LAN** et le **QM-WAN**. Dans le LAN, nous avons décidé d'utiliser le standard UPnP QoS pour le composant **QM-LAN**, alors que pour le composant **QM-WAN**, nous avons défini deux implémentations : une pour la réalisation « IMS » du système d'accès à distance et une pour la réalisation «HTTP».

Maintenant, nous sommes en mesure d'entamer l'étude de l'intégration de ces composants dans le système d'accès à distance pour offrir la QoS de bout en bout à notre service de partage de contenus à distance.

Dans cette section, nous allons mettre l'accent sur la synchronisation de la commande de la QoS entre les différentes portions du chemin de données du service de partage.

4.3.3.1 Solution IMS avec QoS de bout en bout

Dans ce qui suit, nous allons décrire l'interaction entre les composants du système d'accès à distance (**SM**) dans l'environnement IMS et ceux du système de gestion de QoS (**QM**) pour offrir la QoS aux sessions de notre service de partage de contenus. Pour commencer, nous allons revenir sur la procédure de configuration des partages de notre système d'accès à distance, en tenant compte de la problématique de QoS. Ensuite, nous présenterons les modifications à apporter aux différentes procédures de gestion des sessions (ouverture, modification, fermeture) pour leur ajouter la gestion de la QoS. La solution présentée ci-après s'appuie sur les capacités de gestion de la QoS de l'environnement IMS exposée précédemment. En particulier, nous avons utilisé la signalisation SIP non seulement pour transporter la demande de QoS entre les deux réseaux domestiques, mais également pour synchroniser les demandes et traiter les cas d'erreurs.

Configuration d'un nouveau partage avec QoS

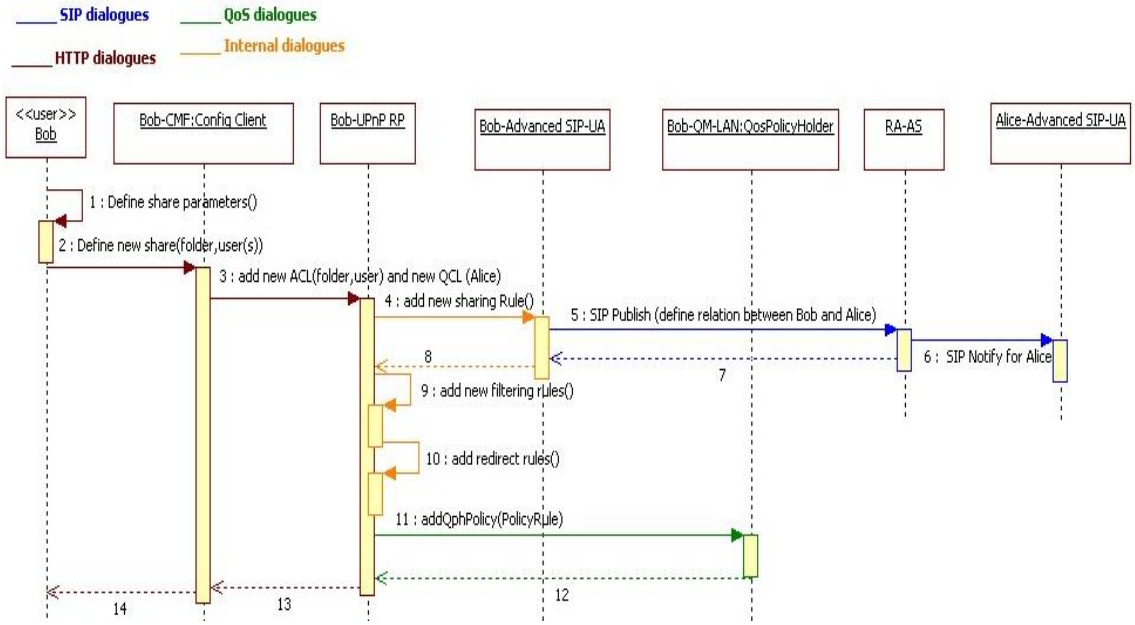


Figure 4.14 Configuration d'un nouveau partage avec QoS, solution IMS

Le système de gestion de QoS (**QM**) permet de gérer les règles d'autorisation qui définissent les droits des clients à réserver des ressources dans le réseau cœur et dans les réseaux des clients (QCL - QoS Control List).

La configuration des autorisations des clients à réserver de la QoS dans le réseau cœur est prise en charge par l'administrateur du service. Elle est définie pendant l'inscription du client au service de partage. Cela permet au système de gestion de réseau de vérifier si l'utilisateur dispose de suffisamment de ressources et des équipements nécessaire à la gestion de QoS avant de lui accorder ce droit. Il est en effet inutile d'essayer de gérer de la QoS si la configuration de

base ne le permet pas. Outre l'aspect technique et la sécurité, un opérateur pourrait vendre le service de partage à distance à un tarif plus élevé si celui-ci inclut le support de la QoS. C'est donc bien à la souscription du contrat, et selon les options choisies, que l'utilisateur aura le droit ou non d'accéder à la gestion de la QoS.

Les QCLs dans le LAN servent à définir le droit d'un visiteur à demander de la QoS dans le LAN qu'il visite. Nous avons modifié la procédure de configuration des nouveaux partages afin de permettre à l'utilisateur de configurer ses QCLs. La nouvelle procédure de configuration d'un partage est illustrée dans la figure 4.14.

Lorsque le client (i.e. Bob) définit un nouveau partage avec une amie (i.e. Alice) avec l'interface de configuration de son **CMF**, il doit indiquer si le client avec qui il partage la liste de contenus qu'il a désignée peut réserver des ressources dans son réseau domestique (étapes 1-4). La procédure de configuration des règles de sécurité dans le LAN et dans le WAN au niveau du système d'accès à distance(**SM**) reste inchangée : i) le **SM-LAN** publie une règle de partage dans le **RA-AS** (étapes 5-8), ii) et il ajoute ensuite les règles de filtrages et de redirection dans son composant « UPnP RP » (étapes 9-10). A la fin de cette procédure le **SM-LAN** (composant UPnP RP) envoie une requête à son **QM-LAN** (service QosPolicyHolder) pour ajouter une règle d'autorisation à réserver de la QoS dans son LAN pour ce client: une nouvelle entrée est alors ajoutée dans la base des QCLs du **QM-LAN** (étapes 11-12).

Avec cette configuration, les règles de sécurisation (ACLs) permettent au système d'accès à distance de garantir la sécurité du LAN de Bob et la confidentialité de ses contenus. Et avec les règles d'autorisation de QoS (QCLs) le **SM** pourra également gérer les droits des clients à réserver des ressources réseaux dans le réseau de cœur et dans les LANs.

Gestion des sessions avec garantie de QoS

A l'ouverture d'une nouvelle session entre deux maisons distantes, l'initiateur de la session n'a pas besoin d'allouer des ressources réseaux parce que la première phase d'utilisation de la session est consacrée au parcours des répertoires distants qui ne nécessite pas de ressources particulières. Cependant, lorsque le client commence la consommation des contenus distants, il aura besoin de réserver des ressources pour garantir la QoS lors de leurs transferts. Dans cette partie, nous allons décrire la procédure de récupération de contenu avec garantie de QoS de bout en bout. Et pour clôturer cette partie nous présenterons la procédure de fermeture d'une session ayant réservé des ressources.

Récupération des contenus avec réservation de ressources

La réponse du Media Serveur UPnP A/V distant à une requête de parcours de répertoire contient les caractéristiques des contenus inclus dans ce répertoire (i.e. codec, bande passante). Si cette caractéristique est optionnelle en UPnP A/V, elle est obligatoire en DLNA puisque dans ce standard, un Media Server doit annoncer les contenus selon un maximum de 4 encodages possibles. Il est ainsi aisé de déduire de ces encodages les ressources nécessaires à l'acheminement du flux. Avec ces informations, le **SM-LAN** du visiteur aura le choix de demander ou pas de la QoS pour récupérer le contenu que l'utilisateur choisira parmi cette liste. La figure 4.15 ci-après illustre la signalisation nécessaire pour récupérer un contenu distant avec réservation de ressources réseaux de bout en bout.

De point de vue utilisateur, la procédure de récupération du contenu ne change pas : avec son terminal UPnP, le client choisit un contenu à regarder parmi la liste des contenus qu'il a reçue à la fin de la procédure de parcours des répertoires distants (étape 1). Le terminal UPnP envoie alors au **CMF** (fonction VMS) une requête de récupération du contenu choisi (étape 2). Le **CMF** contacte par la suite son **SM-LAN** pour chercher le contenu distant (étape 3).

Le traitement de cette requête au niveau du **SM-LAN** change selon la configuration de ce composant. En effet, le fait de demander ou pas de la QoS pour le transfert des contenus peut être un paramètre de configuration du **SM-LAN**. De cette manière, l'administrateur du service de partage de contenus aura la possibilité de proposer à ses clients des offres avec ou sans garantie de QoS.

Dans le cas où le client a souscris au service de partage de contenus avec QoS, la procédure de récupération dans le **SM-LAN** devient comme suit :

i. Déclenchement de la réservation des ressources réseaux dans le LAN du visiteur

Avant d'envoyer la demande de récupération du contenu vers le LAN visité via le **SM-WAN**, la fonction « Advanced SIP UA » du **SM-LAN** contacte le composant « UPnP RP » pour déclencher la réservation de QoS pour ce contenu (étape 5). Le composant « UPnP RP » intègre un point de contrôle UPnP QoS pour formuler des requêtes de QoS (Request TrafficQos) vers le service « UPnP QosManager » du **QM-LAN**. Les paramètres de ces requêtes (Traffic Descriptor) sont récupérés à partir de la réponse à la requête du parcours du répertorie du Media Serveur distant stockant le contenu.

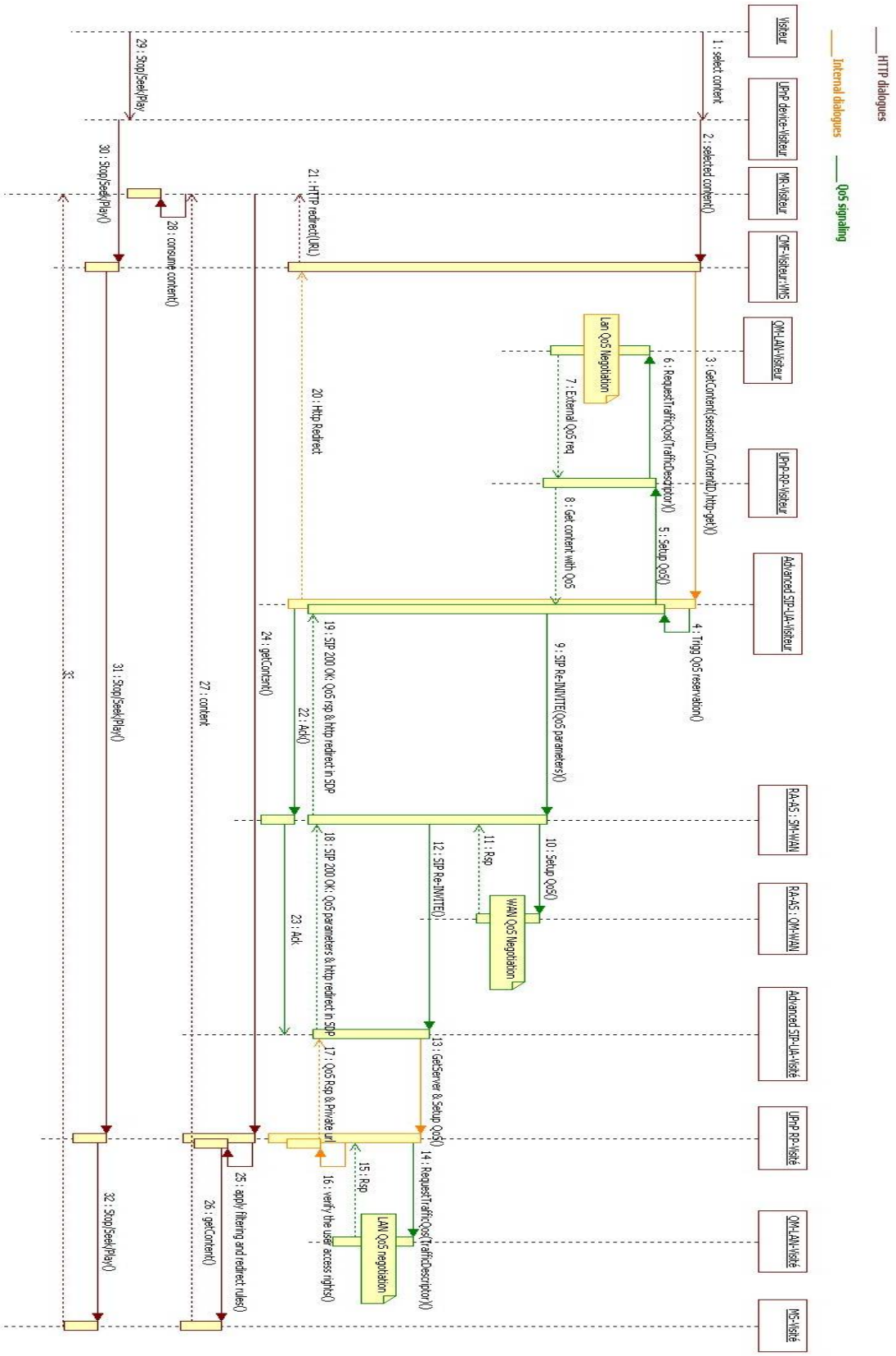


Figure 4.15 Récupération d'un contenu distant avec garantie de la QoS, solution IMS

Vu que la requête du **SM-LAN** au **QM-LAN** sera envoyée au nom de l'administrateur du réseau domestique, elle aura tous les droits nécessaires pour qu'elle soit acceptée par le **QM-LAN**. Les détails de la procédure de traitement d'une requête de réservation dans le **QM-LAN** sont dans la section 4.3.2.2 (paragraphe UPnP QoS).

Dans sa réponse à la demande de réservation de la fonction « UPnP RP » du **SM-LAN**, le **QM-LAN** indique les ressources qu'il a réussi à allouer à cette demande (i.e. bande passante, gigue). L' « UPnP RP » relaie ces paramètres à la fonction « Advanced SIP UA ».

ii. Envoi de la requête de récupération avec demande de QoS

Afin de modifier les paramètres de la session pour la préparer au transfert du contenu, le **SM-LAN** envoie une requête SIP RE-INVITE. Sauf que pour la procédure de récupération avec QoS, l'« Advanced SIP UA» inclut dans le SDP de cette requête les paramètres de QoS qu'il a reçus de son « UPnP RP » afin de demander des ressources réseaux dans le WAN et dans le LAN destination (étape 9) en cohérence avec ce qui a été réservé dans son réseau local. Les champs du SDP qui renseignent les informations de QoS sont les suivants :

a=FHSession : < Catalog|Content|ContentWithQoS > La valeur *ContentWithQoS* est utilisée pour signaler au **SM-WAN** et **SM-LAN** qu'il faut réserver des ressources réseaux à cette session ;

a=FHCoS : < Video|Audio|Data|BestEffort > Ce champ désigne la classe de service associée à cette session ;

a=FHUser : <User Name> Ce champ désigne le nom de l'utilisateur (ou bien son identifiant) et sera utilisé par le composant **QM-WAN** du **RA-AS** et au niveau du **QM-LAN** pour vérifier les droits de cet utilisateur à réserver de la QoS respectivement dans le WAN et dans le LAN visité;

b : < bandwith > Nous utilisons le paramètre standard, mais optionnel, du SDP pour indiquer la bande passante à réserver.

Dans le cas de l'IMS, l'Advanced SIP UA place les adresses publiques utilisées dans le cadre de cette session afin que le réseau cœur puisse réserver des ressources entre les deux réseaux domestiques identifiés par les adresses publiques des deux passerelles domestiques.

iii. Traitement de la requête de récupération dans le WAN

Lorsque le **RA-AS** (composant **SM-LAN**) reçoit une requête SIP RE-INVITE avec un champ « a=FHSession » contenant la valeur « *ContentWithQoS* », il déclenche la procédure de réservation de QoS dans le WAN pour la session désignée dans ce message en envoyant une requête à son composant **QM-WAN** (étape 10).

Le **QM-WAN** vérifie le droit du demandeur (a=FHUser) à solliciter des ressources et contacte ensuite le **RACS** pour vérifier la disponibilité des ressources pour cette demande. Dans le cas où ces deux tests réussissent, le **RACS** configure les équipements nécessaires pour garantir la QoS à cette session (les détails de la procédure de réservation sont dans la section 4.3.1.1). Dans le cas où l'une des vérifications dans le **QM-WAN** ou dans le **RACS** échoue, un message d'erreur est envoyé au **SM-WAN** dans le **RA-AS**. Ce dernier envoi à son tour un message d'erreur SIP (SIP 500 Server Internal Error) à l'initiateur du message SIP RE-INVITE. Ce message aura alors pour effet de libérer les ressources préalablement réservées dans le réseau local. Pour cela, l' «Advanced SIP UA» contacte son «UPnP RP» pour mettre fin à cette session qui à son tour va contacter son **QM-LAN** en lui indiquant de libérer les ressources associées à cette session.

Si la demande de réservation de ressources du **SM-WAN** se termine avec succès, il transfère le message SIP RE-INVITE vers la maison destination (étape 12).

iv. Traitement de la requête de récupération dans le LAN visité

A la réception d'un message SIP RE-INVITE dans le LAN destination, l'«Advanced SIP UA» vérifie la valeur du champ «a=FHSession». Si elle prend la valeur «Content» il déclenche la procédure de récupération de contenu sans réservation de ressources comme nous l'avons décrite dans le chapitre précédent. Si elle prend la valeur «ContentWithQoS» il déclenche la procédure de récupération de contenu avec réservation de ressources.

La première étape de cette procédure consiste à récupérer les paramètres de QoS du contenu à transférer à partir du SDP inclus dans le message SIP. La deuxième étape va consister à réaliser l'opération de translation d'adresse inverse en remplaçant les adresses publiques par les adresses privées i.e. spécifier que la réservation porte depuis l'adresse privée de la passerelle domestique jusqu'à l'adresse privée du Media Renderer. Ensuite, l'«Advanced SIP UA» sollicite son «UPnP RP» pour allouer les ressources demandées pour cette session en plus de la récupération de l'URL direct du contenu à transmettre (étape 13).

Avec les paramètres de QoS renseignés par l'«Advanced SIP UA», l'«UPnP RP» formule une requête de réservation (UPnP RequestTrafficQos) au service «UPnP QosManager» du **QM-LAN** (étape 14). Ce composant vérifie dans la liste de QCLs détenue dans son service «UPnP PolicyHolder» si le demandeur de la réservation a le droit d'allouer des ressources dans son LAN. Il vérifie par la suite la disponibilité des ressources réseaux dans son LAN avant de configurer les équipements nécessaires pour mettre en place la demande reçue (la procédure de réservation des ressources avec le composant **QM-LAN** est décrite en détail dans la section 4.3.2.3).

Si l'«UPnP RP» reçoit une réponse négative à sa demande de QoS, il envoie un message d'erreur à son «Advanced SIP UA» qui répond au LAN du visiteur par un message d'erreur SIP pour indiquer la cause du rejet (SIP 4xx[5]). Lorsque le **SM-LAN** du visiteur reçoit ce message d'erreur, il a la possibilité d'essayer de réserver moins de ressources ou bien de fermer la session pour libérer les ressources qu'il a allouées dans le WAN et dans son LAN.

Dans le cas où le **QM-LAN** du LAN visité réussit à mettre en place la demande de QoS émise par le visiteur, le **SM-LAN** vérifie dans sa base de règles de filtrage, comme dans la procédure de récupération sans QoS, si le visiteur a le droit d'accéder au contenu qu'il a désigné (étape 16). Si ce test réussi, l' « UPnP RP » déduit de ses règles de redirection l'URL directe pointant vers le Media Serveur stockant le contenu. Il inclut cette URL dans la réponse qu'il renvoie à son « Advanced SIP UA » avec les paramètres de QoS qu'il a réussi à établir (étape 17).

L'«Advanced SIP UA» du LAN visité intègre ces paramètres (URL de redirection et paramètres de QoS) dans le SDP du message SIP 200 OK qu'il transmet au LAN du visiteur via le **RA-AS** (étapes 18-19). En recevant cette réponse, l'«Advanced SIP UA» du LAN du visiteur aura la confirmation de la réussite de la réservation des ressources de bout en bout nécessaires au transfert du contenu qu'il veut récupérer. Il répond alors à son **CMF** avec une requête de redirection «HTTP» pointant vers l'URL directe du contenu distant (étape 21). Le **CMF** contacte alors le Media Renderer choisi par l'utilisateur afin de lui demander de commencer la récupération du contenu indiqué par l'URL renseignée par son **SM-LAN** (fonction Advanced SIP UA) (étape 22).

La requête du Media Renderer du visiteur est envoyée directement vers le LAN visité où le composant «UPnP RP» vérifie la méthode HTTP réclamée par l'équipement distant (étapes 24-25) avant de la transmettre au Media Serveur stockant le contenu (étape 26). Le flux est ensuite transféré directement vers le Media Renderer distant. La QoS sera garantie tout au long du

[5] Il n'existe pas de code spécifique pour indiquer l'absence de ressources en SIP. Un message 480 « Temporarely Unavailable » semble le code le plus approprié en indiquant dans le corps du message qu'il s'agit des ressources réseaux qui ne sont pas disponible.

chemin de ce flux (les deux LANs des clients et la partie WAN) grâce à la réservation effectuée par le **QM** (**QM-WAN** et les **QM-LAN**).

De façon similaire au traitement des cas d'erreurs de réservation de ressources dans le réseau de l'opérateur, si la demande de QoS échoue dans le LAN visité, un message d'erreur SIP est retourné à l'appelant (i.e. l'« Advanced SIP UA » du LAN visiteur). Ce message sera bien évidemment traité par l'IMS du réseau cœur et aura pour conséquence de libérer les ressources précédemment allouées par le RACS. Ce message sera ensuite acheminé vers le réseau LAN visiteur qui procédera de même avec la réservation locale.

A noter qu'il est également possible de négocier nativement la bande passante, donc l'encodage, en une seule passe en SIP. Pour ce faire, le SDP du message SIP devra comporter autant de demandes (i.e. au sens de notre service de partage de contenus) que d'encodages disponibles (ceux-là même fournis dans la réponse du Media Server suivant la norme DLNA). Lors des différentes étapes de demande de QoS, les encodages ne pouvant être satisfait par manque de ressources seront retirés de la liste des codecs présents dans le SDP. C'est le procédé standard utilisé par SIP pour établir une communication VoIP lorsque que plusieurs codecs sont spécifiés dans le SDP. Au final, le demandeur reçoit une liste des encodages pouvant être supportés et pour lesquels une réservation de ressources a été effectuée. La liste des codecs est triée par ordre décroissant de ressources de sorte à ce que le premier codec dans la liste en retour soit le meilleur possible que le réseau supporte. Comme le message 200 OK transporte le SDP issue de la négociation finale, chaque réseau (Cœur, puis LAN visiteur) va pouvoir ajuster la bande passante réservée. Par exemple, si le LAN du visiteur réserve 10Mbit/s, ainsi que le réseau cœur, mais que le LAN visité ne dispose que de 7 Mbit/s, le réseau cœur et le LAN visiteur vont ajuster leur réservation à cette dernière valeur.

Le traitement des messages SIP nous permet ainsi de parfaitement synchroniser les demandes de réservations entre les 3 portions de réseaux, que ce soit au niveau du traitement des erreurs ou de l'ajustement de la bande passante.

Modification des ressources d'une session

Le visiteur peut continuer à utiliser la même session pour récupérer d'autres contenus sans avoir à la modifier, si les nouveaux contenus possèdent les mêmes caractéristiques (i.e. catalogue de photos, répertoires de music ou répertoires de vidéos). Il répète alors la procédure de récupération de contenu sans déclenchement de réservation de QoS décrite dans le chapitre précédent.

Mais, si le nouveau contenu n'a pas les mêmes caractéristiques du dernier contenu transféré avec la session, le **SM-LAN** déclenche la procédure de récupération de contenu avec modification de ressources. Les étapes de cette procédure sont identiques à celles de la procédure de récupération de contenu avec réservation de ressources décrite dans la section précédente. La seule différence entre les deux procédures est que les **SMs** (**SM-LAN**, **SM-WAN**) envoient des requêtes de modification de réservation aux **QMs** (**QM-LAN**, **QM-WAN**) au lieu de requêtes de réservation.

Fermeture de session avec libération des ressources

A la fin de l'utilisation de la session, le **CMF** du visiteur demande à son **SM-LAN** de fermer la session avec le LAN visité (étape 7). Si le **SM-LAN** a réservé des ressources pour cette session, il va commencer par libérer les ressources de cette session dans son LAN (étapes 10-11). Et avant d'envoyer le message SIP BYE, l'«Advanced SIP UA» du visiteur inclut dans le SDP de sa requête de fermeture de session une information demandant la libération des ressources de cette session (champ «a=FHSession : ContentWithQoS»).

Cette requête est relayée par le **RA-AS** vers le LAN visité. Les composants **QM-WAN** et **QM-LAN** du LAN visité seront sollicités respectivement par le **RA-AS** et l'«UPnP RP» pour relâcher les ressources allouées à cette session. L'«UPnP RP» du LAN visité termine cette procédure par la suppression des configurations du pare-feu ajoutées pour cette session afin de préserver la sécurité de son LAN (étape 16).

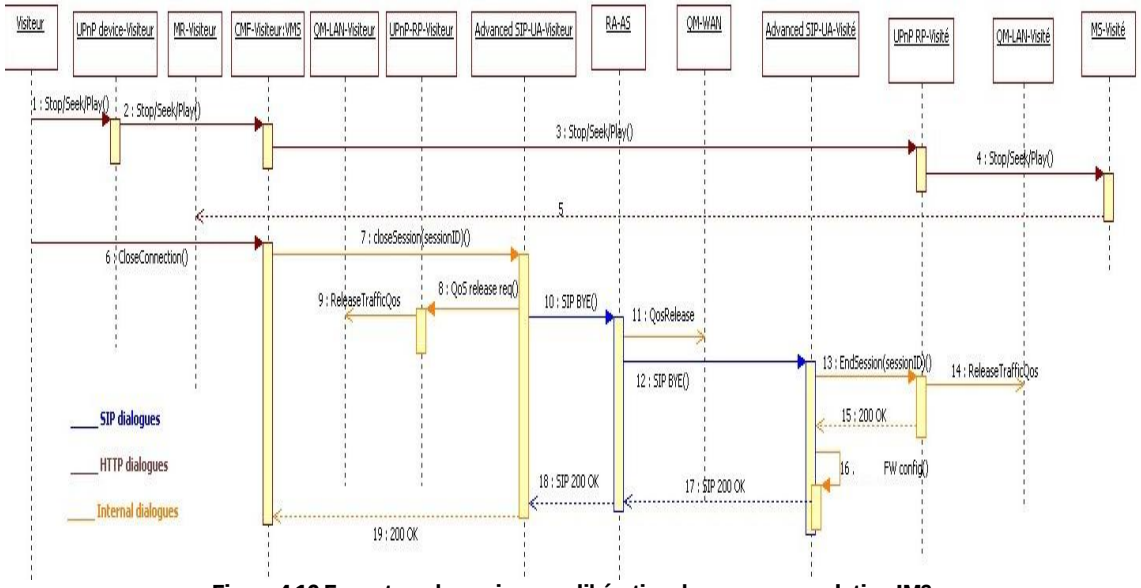


Figure 4.16 Fermeture de session avec libération de ressources, solution IMS

Simulation UML de la solution IMS avec QoS de bout en bout

Dans cette partie, nous présentons les travaux de la simulation UML réalisés pour valider fonctionnellement l'intégration de ce système dans le service de contenus à distance. Nous avons alors repris notre modèle de simulation UML du service de partage de contenus auquel nous avons ajouté les composants du système de gestion de QoS. Nous avons utilisé le même environnement de simulation qui est le simulateur TauG2.

La première étape a consisté à réaliser les machines d'état des deux composants **QM-LAN** et **QM-WAN** et de modifier les machines d'états des composants impactés par l'intégration de ces composants, à savoir : l'«UPnP RP», l'«Advanced SIP UA» et le **RA-AS**.

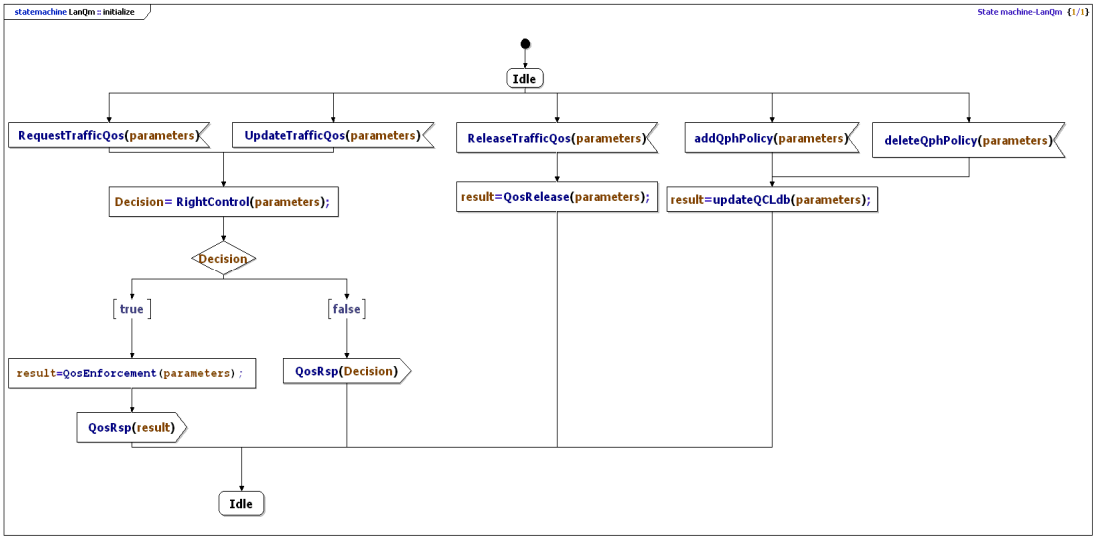


Figure 4.17 Machine d'états du composant QM-LAN

La figure 4.17 représente la machine d'états du composant **QM-LAN** pour modéliser les étapes de la gestion des requêtes de mise en place de la QoS et de mise à jour de la base des QCLs dans le LAN. Nous n'avons pas découpé ce composant en service QosManager et service QosPolicyHolder car le but de nos simulations était juste de valider la signalisation de la mise en place de la QoS de bout en bout, la parfaite synchronisation des réservations et en particulier le traitement des cas d'erreur

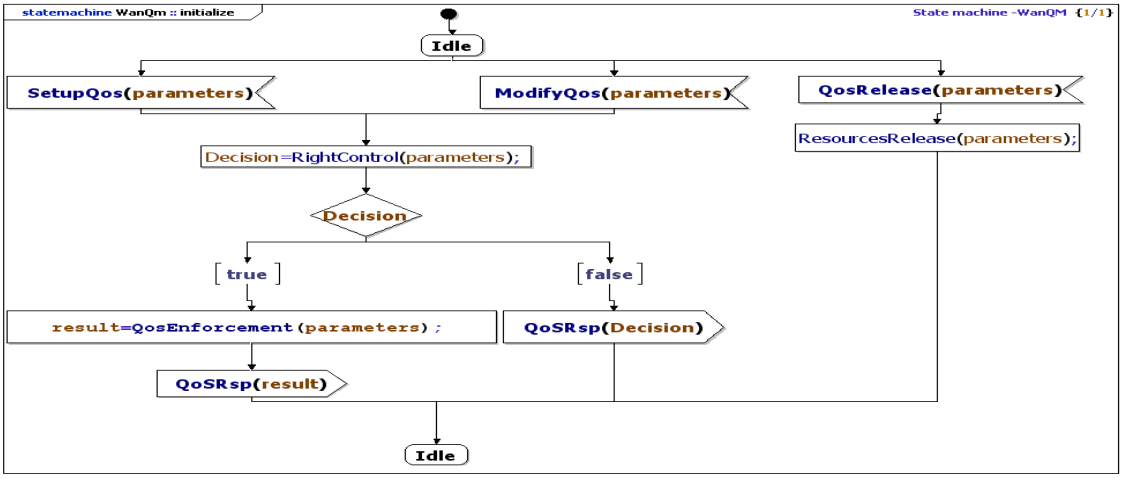


Figure 4.18 Machine d'états du composant QM-WAN

La figure 4.18 illustre la machine d'états du composant **QM-WAN**. Cette machine ne comporte pas la procédure d'ajout et suppression des QCLs dans le WAN car nous l'avons intégrée dans le portail d'administration de la plate-forme **RA-AS**.

La nouvelle machine d'état du **RA-AS** (composant **SM-WAN**) qui prend en charge la gestion de QoS est présentée dans la figure 4.19. Les modifications apportées à l'ancienne machine d'états se situent au niveau des traitements des messages SIP RE_INVITE et SIP BYE. Elles consistent à détecter, pendant l'analyse des SDPs de ces messages, si la QoS doit être gérée pour cette session et déclencher en conséquence la procédure de demande de ressources réseaux au niveau du **QM-WAN**.

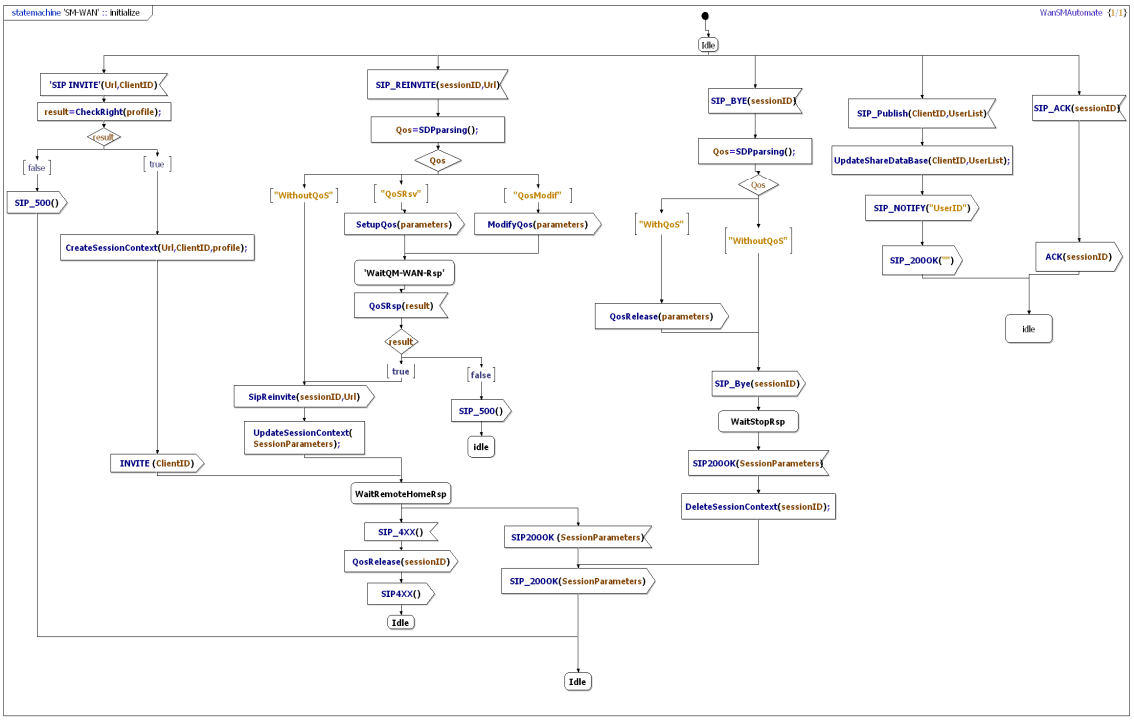


Figure 4.19 Machine d'états du composant RA-AS, avec prise en charge de la QoS

Dans la figure 4.20, nous présentons les ajouts et les modifications amenées à la machine d'états du composant « UPnP RP » et qui consistent à gérer les requêtes de mise à jour de la base des QCLs dans le LAN et à formuler des requêtes de QoS au **QM-LAN**. Par soucis de lisibilité de la Figure 4.20, nous avons supprimé les procédures de traitements de requêtes de gestion des ACLs qui restent identiques à celle de l'ancienne machine d'états de ce composant (sans QoS).

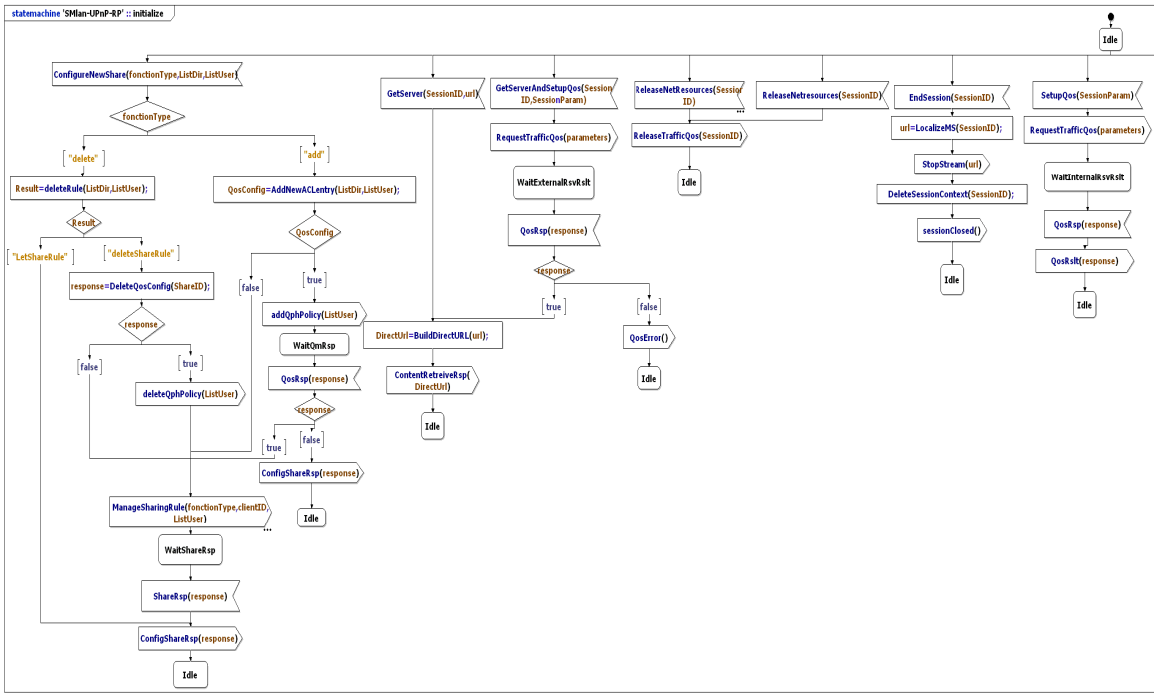


Figure 4.20 Machine d'états du composant UPnP RP, avec prise en charge de la QoS

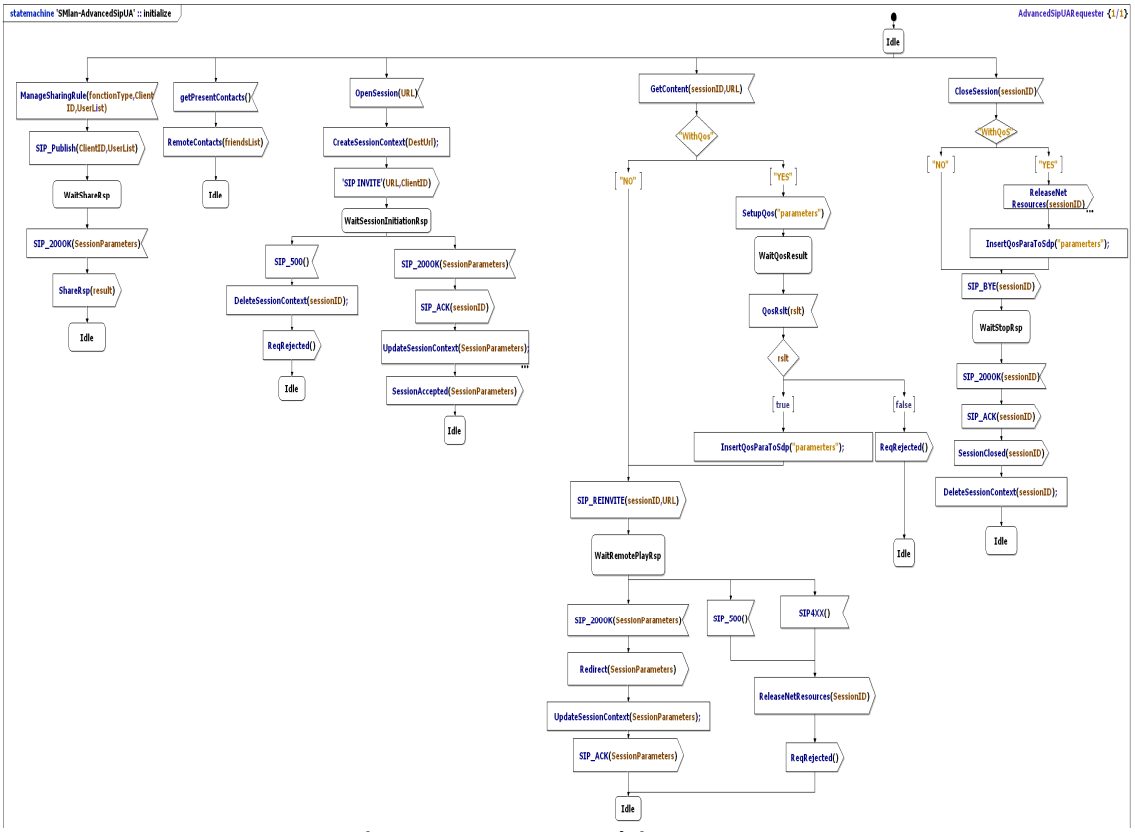


Figure 4.21 Machine d'états du Advanced SIP UA côté LAN, avec prise en charge de la QoS

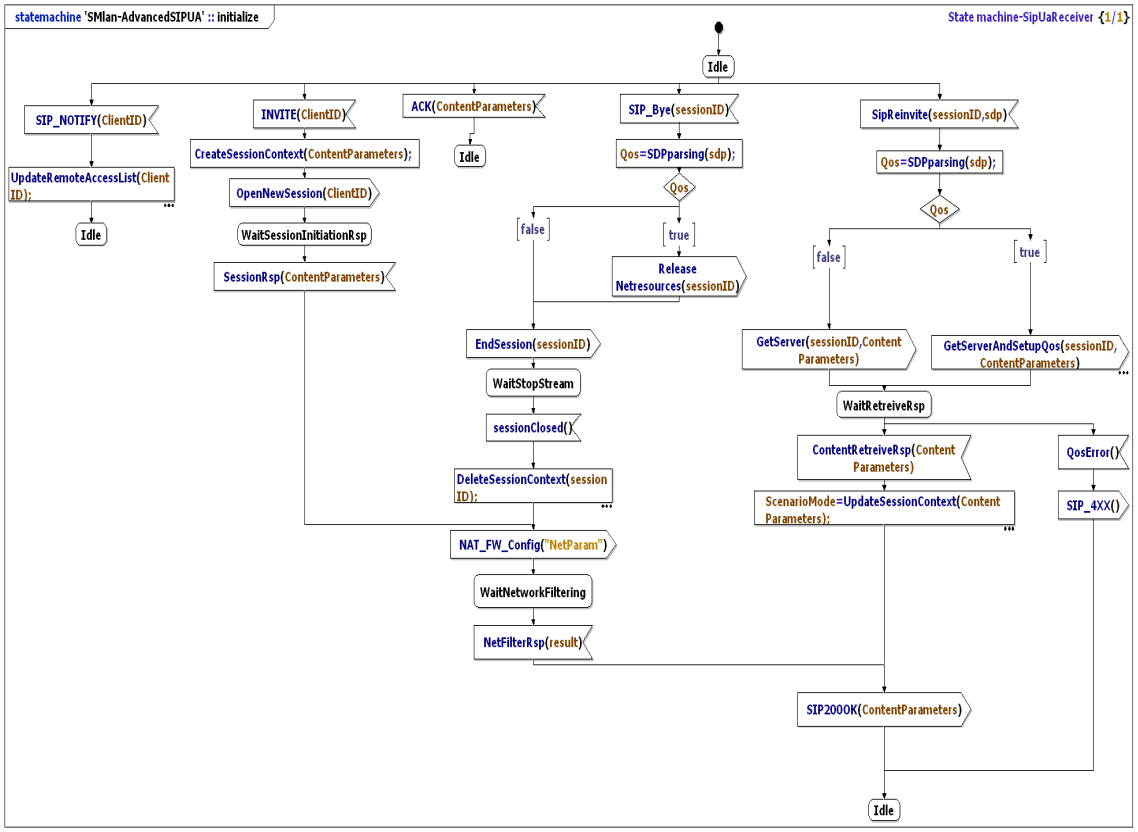


Figure 4.22 Machine d'états du Advanced SIP UA côté WAN, avec prise en charge de la QoS

Les figures 4.21 et 4.22 illustrent les deux machines d'états du composant « Advanced SIP UA » qui décrivent respectivement son comportement lorsqu'il est sollicité par le **CMF** (requête interne) et le **RA-AS** (requête externe au LAN). Dans la première machine d'états, nous avons ajouté la fonctionnalité d'intégration des informations de QoS dans le SDP des messages SIP RE-INVITE et SIP BYE, afin de prendre en charge la gestion des ressources au niveau du WAN et du LAN du visiteur. Dans la deuxième machine d'états, nous avons modifié la fonction d'analyse du SDP pour prendre en charge l'extraction des informations de QoS au niveau du LAN visité et donc déclencher la procédure de gestion de QoS nécessaire (réservation, modification, libération).

Scénarii de simulation

Après la spécification des machines d'états des composants du système de gestion de QoS et l'ajout des modifications nécessaires sur les composants concernés par l'intégration de ce système dans le service de partage de contenus à distance, nous avons précisé une série de tests dans le but de mettre en évidence puis corriger les erreurs de conception et d'intégration de ce système dans ce service de partage. Le tableau 4.2 résume cette série de tests. Comme dans la validation du système d'accès à distance, nous avons distingué deux types de scénario : les scénarii de configuration (i.e. ajout d'un partage avec prise en charge de la QoS) et les scénarii d'invocation (i.e. récupération de contenu distance avec réservation de la QoS).

Tableau 4.2 Scénarii simulés, avec prise en charge de la QoS

Scénario	Description	Type
1	Ajout d'un nouveau partage avec configuration de QoS.	Configuration
2	Suppression de partage avec configuration de QoS.	Configuration
3	Récupération de contenu distant avec succès de la réservation de la QoS de bout en bout.	Invocation
4	Fermeture de session avec libération des ressources réseaux.	Invocation
5	Echec d'établissement d'une session à cause des ressources insuffisantes dans le LAN du visiteur.	Invocation
6	Echec d'établissement d'une session à cause d'absence du droit de demander de la QoS dans le réseau WAN.	Invocation
7	Echec d'établissement d'une session à cause des ressources insuffisantes dans le WAN.	Invocation
8	Echec d'établissement d'une session à cause d'absence du droit de demander de la QoS dans LAN désigné.	Invocation
9	Echec d'établissement d'une session à cause des ressources insuffisantes dans le LAN visité.	Invocation

Avant de lancer les simulations avec le simulateur TauG2, il faut commencer par définir le diagramme de structures des composants entrant en jeu dans la simulation. Pour nos tests, nous avons défini deux diagrammes de structures, un pour chaque type de scénarii, représentés dans les figures 4.23 et 4.24. Nous retrouvons dans ces diagrammes les composants **QM-LAN** et **QM-WAN** du système de gestion de QoS et leurs interfaces de communication avec les composants du service de partage de contenus à distance, à savoir l'«UPnP RP», l'«Advanced SIP UA» et le **RA-AS**.

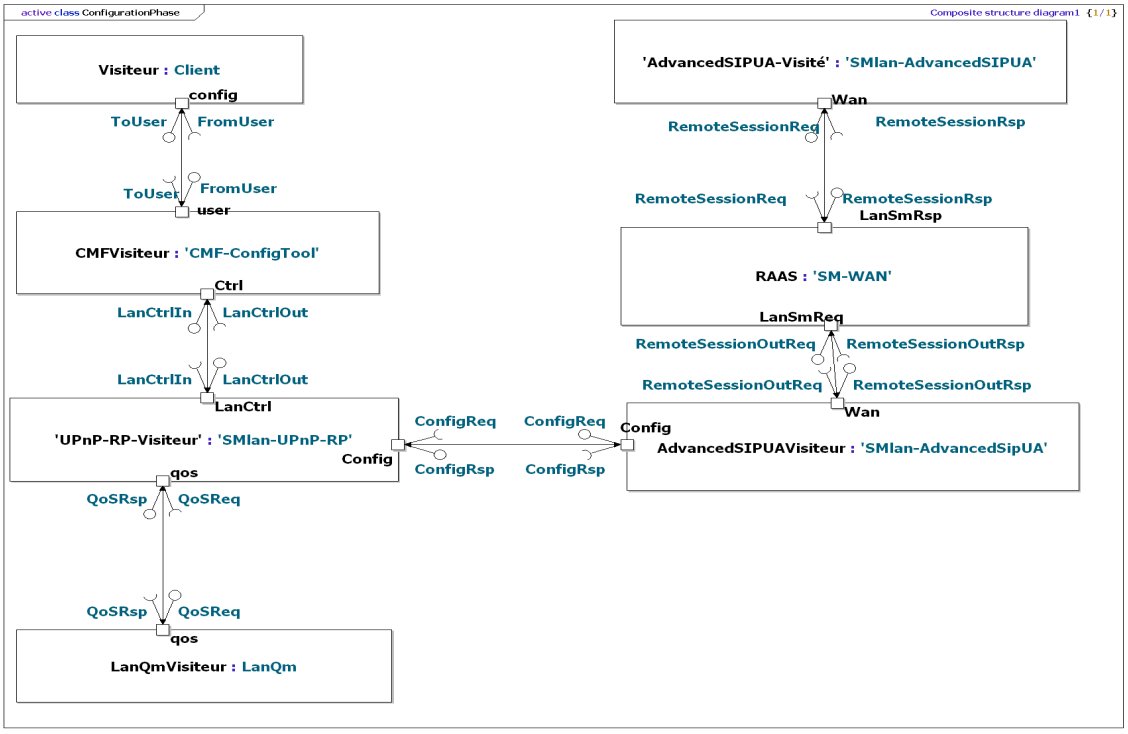


Figure 4.23 Diagramme de structure des composants des scénarii de configuration

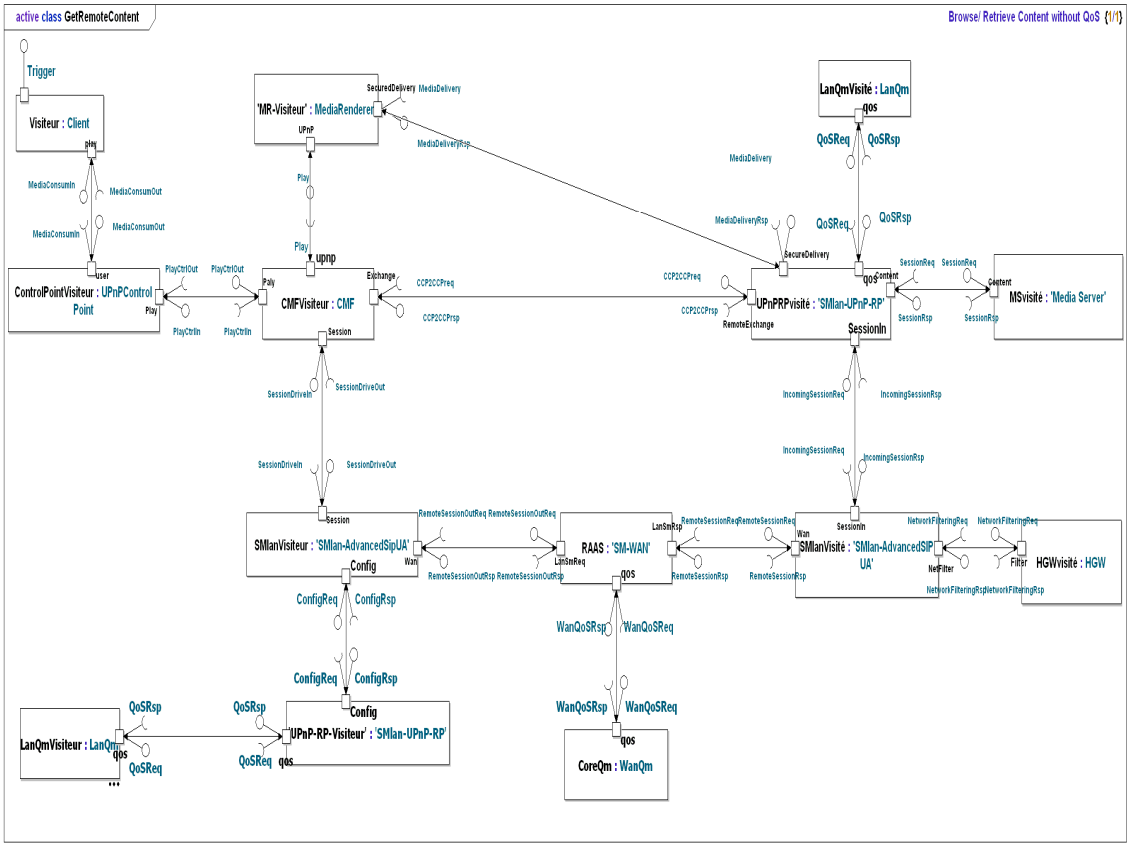


Figure 4.24 Diagramme de structure des composants des scénarii d'invocation

Résultats des simulations

Nous avons produit des traces de simulations sous forme de diagrammes de séquences pour les comparer avec les diagrammes que nous avons définis pendant la phase de conception. Dans le reste de cette section, nous présentons des exemples de ces traces. Ils représentent les traces des principaux scénarii de tests : le scénario d'ajout d'un nouveau partage avec configuration de QoS (Figure 4.25), le scénario de récupération d'un contenu distant avec garantie de la QoS de bout en bout (Figure 4.26) et le scénario de fermeture d'une session avec libération de ses ressources réseaux (Figure 4.27).

Cette phase de simulation UML avec TauG2 a servi de phase de validation fonctionnelle du système de gestion de QoS et de son intégration dans le service de partage de contenus à distance. Les diagrammes de séquences générés par l'exécution des scénarii de simulation nous ont permis de déceler des erreurs dans les machines d'états de certains composants. Ces erreurs étaient des erreurs de blocages ou de mauvais traitements des messages de signalisation échangés entres les différents composants du service. Nous avons corrigé ces erreurs et nous avons validé ses corrections en relançant de nouveau les mêmes scénarii.

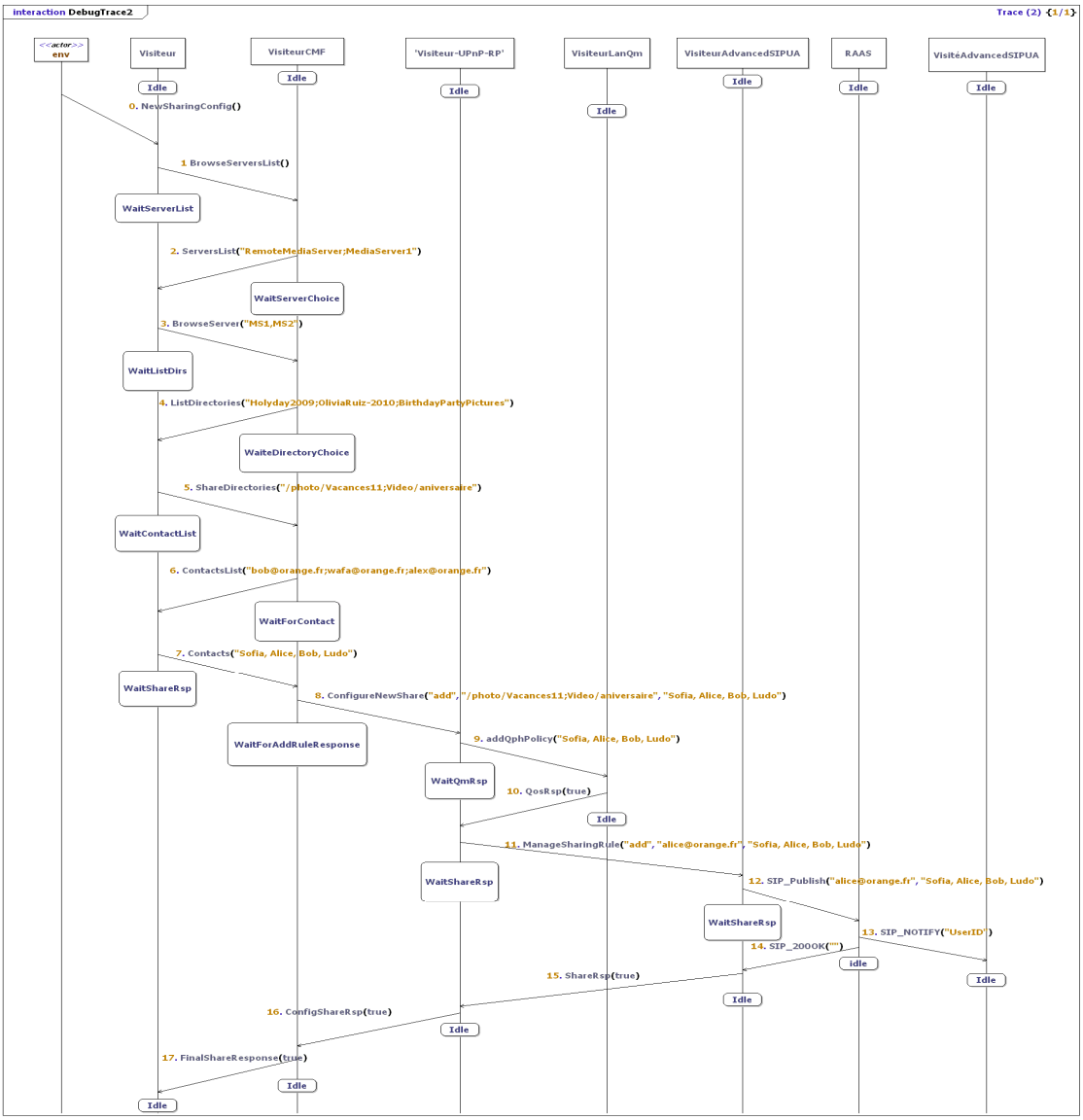


Figure 4.25 Trace de simulation d'un scénario d'ajout d'un partage avec configuration de QoS

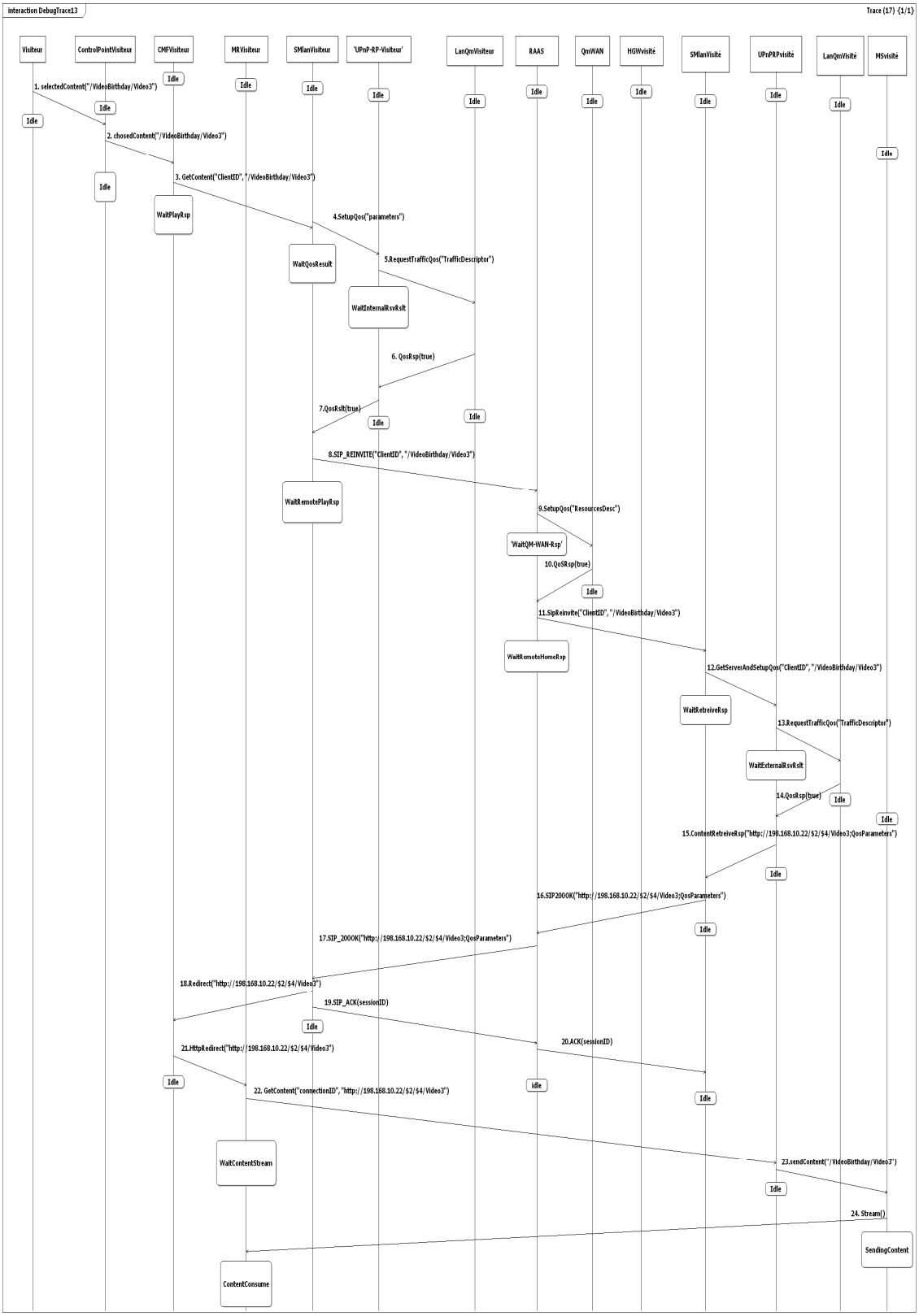


Figure 4.26 Trace de simulation d'un scénario de récupération d'un contenu distant avec succès de la réservation de la QoS de bout en bout

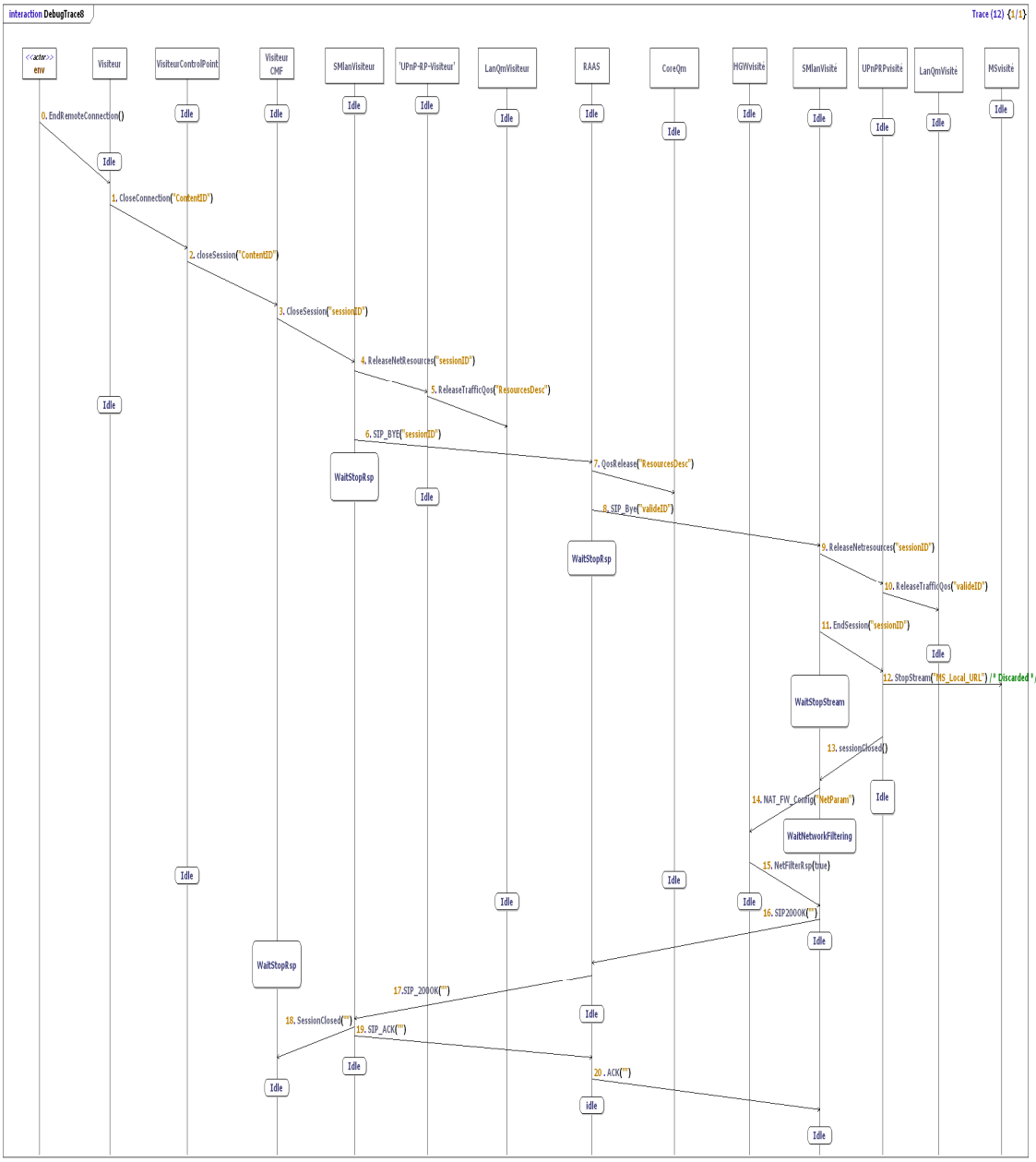


Figure 4.27 Trace de simulation d'un scénario de fermeture de session avec libération de ces ressources réseaux

4.3.3.2 Solution HTTP avec QoS de bout en bout

Dans cette section, nous présentons l'intégration du système de gestion de la QoS dans la réalisation «HTTP» du système d'accès à distance pour qu'il prenne en charge la garantie de la QoS des sessions du service de partage de contenus à distance. Nous commençons par la présentation de la nouvelle procédure de configuration des partages de notre système d'accès à distance avec la prise en compte de la QoS. Puis, nous décrivons les modifications entrainées par l'ajout de la QoS aux différentes procédures de gestion des sessions (ouverture, modification, fermeture). Contrairement à l'IMS, nous n'avons pas pu reposer notre solution sur la gestion de la QoS native du protocole HTTP car elle est inexistante. Aussi, afin de transporter les paramètres de demande de la QoS, d'assurer la synchronisation tant des réservations que des cas d'erreurs, nous avons réutilisé le proxy HTTP élaboré pour le service de partage de contenus. Cette fois-ci, au lieu de transporter de façon transparente et sécurisé les messages UPnP A/V, nous avons

utilisé notre ASP pour transporter les messages UPnP QoS.

Configuration d'un nouveau partage avec QoS

Les QCLs (QoS Control List), gérées par le système de gestion de QoS, permettent à l'utilisateur de contrôler les droits des clients à demander des ressources réseaux dans le WAN et dans les LANs qu'ils visitent. La configuration des QCLs dans le WAN et dans les LANs se fait respectivement par l'administrateur du service de partage de contenus à distance et les utilisateurs de ce service.

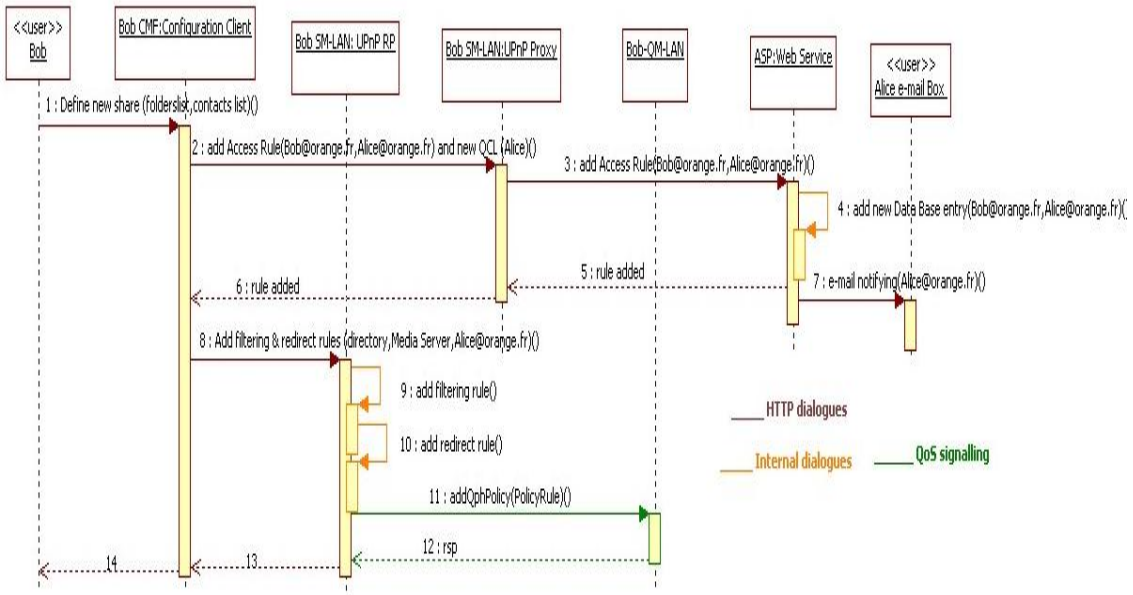


Figure 4.28 Configuration d'un nouveau partage avec QoS, solution HTTP

Dans le WAN, l'administrateur du service de partage sauvegarde dans la base de données de l'**ASP** le droit de l'utilisateur à réserver des ressources dans le réseau de cœur au moment de l'inscription du client au service.

L'utilisateur du service de partage configure les autorisations de réservation de QoS de ses contacts distants dans son LAN (QCL) pendant la définition de ses partages. La nouvelle procédure de partage de contenu incluant la configuration des QCLs dans le LAN est illustrée dans la figure 4.28.

En effet, l'interface de configuration du **CMF** offre la possibilité de désigner qui parmi les contacts de ce nouveau partage ont le droit de demander des ressources réseaux pendant la récupération des contenus de ce partage (étape 1). Le **CMF** demande à son **SM-LAN** (composant UPnP Proxy) de relayer la requête d'ajout des règles d'accès dans l'**ASP** (étapes 2-6). Le **CMF** envoie par la suite une requête de configuration des règles de filtrages et de redirection dans le LAN vers son **SM-LAN** (fonction UPnP RP), mais il joint en plus à cette requête une demande d'ajout de règles d'autorisation de réservation de QoS pour l'ensemble des contacts désigné par l'utilisateur (étape 8). L'«UPnP RP» contacte alors son **QM-LAN** (service QosPolicyHolder) pour insérer de nouvelles entrées dans la base des QCLs détenue dans le **QM-LAN** (étapes 11-12).

La nouvelle procédure de configuration des partages garde les mêmes propriétés de sécurisation du LAN des clients avec la configuration des ACLs (au niveau du LAN et du WAN), mais ajoute en plus la gestion des droits des utilisateurs externes au LAN à réserver des ressources et leurs droits à réserver des ressources dans le réseau de cœur.

Gestion des sessions avec garantie de QoS

Dans cette partie, nous décrivons les modifications apportées aux procédures de gestion des sessions pour la prise en charge de la QoS, à savoir la procédure de récupération de contenus distants, la procédure de modification des ressources d'une session et la procédure de fermeture d'une session (voir figure 4.27). La procédure d'ouverture de session reste inchangée car les sessions nouvellement ouvertes par le système d'accès à distance ne demandent pas de ressources réseaux vu qu'elles seront utilisées pour récupérer les réponses des requêtes de parcours de répertoires (les réponses sont sous formes de fichiers XML de faible taille, i.e. ~ k octets).

Récupération des contenus avec réservation de ressources

Si le **SM-LAN** est configuré pour prendre en charge la QoS, le composant « UPnP Proxy » déclenche la procédure de réservation de QoS de bout en bout lorsqu'il reçoit le message de récupération du contenu du composant **CMF** (fonction VMS) (étapes 1-4).

Les caractéristiques du contenu à transférer du LAN distant (i.e. codec, bande passante) se trouvent dans les réponses du Media Serveur distant aux requêtes de parcours des répertoires. Ces réponses sont reçues au niveau du LAN du visiteur par la fonction «UPnP RP» de son **SM-LAN**, qui les relaie au **CMF**. Ces paramètres de QoS peuvent alors être sauvegardés dans la fonction « UPnP RP » afin de les utiliser au moment de l'initiation de la procédure de réservation des ressources réseaux ; ou bien ils peuvent être renseignés par le **CMF** dans sa requête de récupération de contenu envoyée à l'«UPnP Proxy». Nous recommandons la première solution (maintenir les informations de QoS dans l'UPnP RP) car elle n'entraine pas de modifications dans les composants autres que ceux du système d'accès à distance.

La figure 4.29 représente la procédure de réservation de ressources réseaux de bout en bout pendant la récupération d'un contenu distant. Les principales étapes de cette procédure sont :

i. Réservation des ressources réseaux dans le LAN du visiteur

Connaissant les caractéristiques du contenu à transférer dans la session, l'«UPnP RP» du visiteur (fonction UPnP QoS Control Point) envoie une requête de réservation de QoS (UPnP RequestTrafficQos) vers le service « UPnP QosManager » de son **QM-LAN** (étape 5). Puisque le **QM-LAN** contrôle l'identité du demandeur de QoS en se basant sur la base des QCLs détenues par le service « UPnP QosPolicyHolder » du **QM-LAN**, l'«UPnP RP» envoie la requête de réservation de ressources au nom de l'administrateur du réseau. De cette manière, l' « UPnP RP » s'assure que le premier contrôle sur l'identité sera réussi. Cependant, l'«UPnP QosManager» vérifie si les ressources disponibles dans son LAN seront suffisantes pour assurer la QoS demandée dans la nouvelle requête, avant d'appliquer la configuration nécessaire dans les équipements de son réseau.

Dans sa réponse à la fonction «UPnP RP» du **SM-LAN**, le service « UPnP QosManager » indique les ressources qu'il a réussi à allouer à la requête reçue. Si cette réponse est positive, l'«UPnP RP» enchaine les autres étapes de la procédure de réservation de ressources de bout en bout, sinon il suspend le processus de récupération du contenu distant en envoyant un message d'erreur au composant «UPnP Proxy».

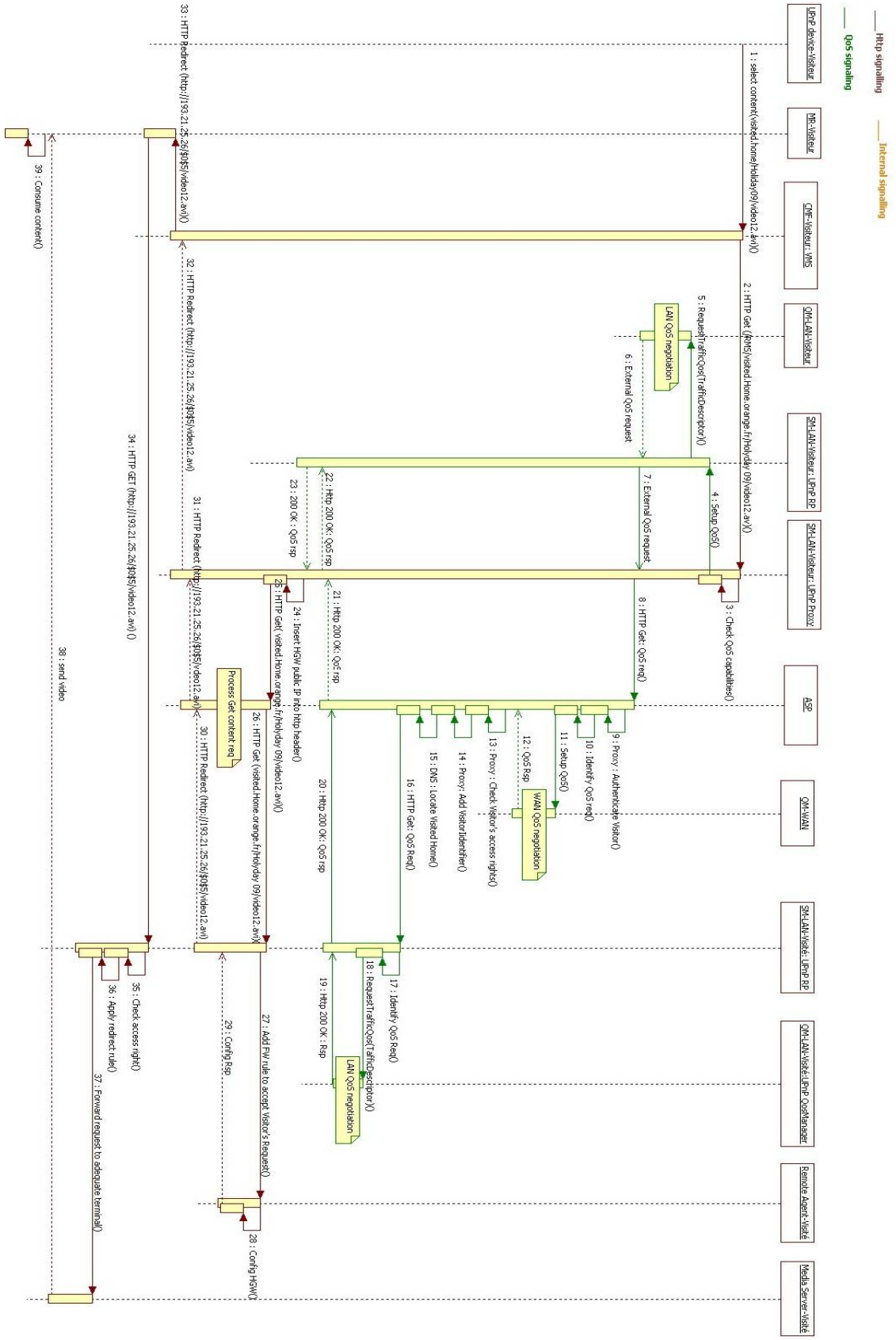


Figure 4.29 Récupération d'un contenu distant avec garantie de la QoS, solution HTTP

ii. Envoi des requêtes de réservation de QoS dans le réseau de cœur et le LAN destination

L'«UPnP RP» du visiteur (fonction UPnP QoS Control Point) inclut, dans une requête de réservation UPnP QoS, les paramètres de QoS que son **QM-LAN** a réussi à réserver. Nous nous plaçons dans le cas de figure où le point de contrôle UPnP QoS est situé dans un réseau domestique et le « QoS Manager » dans un autre (comme dans le cas d'utilisation d'UPnP A/V entre les deux réseaux domestiques). Cette requête sera destinée au **QM-WAN** et **QM-LAN** du LAN à visiter via l'**ASP**. Ainsi, nous transmettons au réseau cœur une demande cohérente par rapport à ce qui a déjà été alloué dans le réseau domestique du visiteur. Elle est relayée par le composant « UPnP Proxy » du visiteur comme une requête HTTP externe normale, en l'envoyant vers le Proxy centrale de l'**ASP** (étapes 7-8). Au préalable, comme dans le cas de l'IMS, l'«UPnP RP» aura translaté les adresses privée en adresses publiques dans la requête de QoS.

Toutefois, l'**ASP** et le **SM-LAN** dans le LAN destination doivent identifier la requête en tant que requête de QoS pour la transférer respectivement au **QM-WAN** et au **QM-LAN** destination. En conséquence, l'«UPnP RP» du visiteur intègre dans sa requête de QoS une entête HTTP «FHqos» avec la valeur «YES» pour qu'elle soit reconnue par l'**ASP** et le **SM-LAN** destination. Ceci permet à l'**ASP** de traiter différemment les messages UPnP A/V des messages UPnP QoS qu'il doit relayer via sa fonction proxy.

iii. Traitement de la requête de demande de QoS dans le réseau de cœur

Lorsque l'**ASP** reçoit une requête de QoS en provenance du LAN du visiteur, le proxy de l'**ASP**, comme c'est le cas pour toutes les requêtes qu'il reçoit, authentifie l'émetteur de la requête (étape 9). Ensuite, à l'aide de l'entête HTTP «FHqos», l'**ASP** identifie la requête comme une requête de demande de QoS (étape 10). La requête est alors transférée au composant **QM-WAN** de l'**ASP** (étape 11).

Le **QM-WAN** commence par extraire, de la requête UPnP QoS reçue, les paramètres nécessaires pour vérifier la possibilité d'accepter cette requête (i.e. identité de l'émetteur, bande passante demandée, classe de service, adresse IP source et destination). La première étape de la procédure d'admission de la requête dans le **QM-WAN** consiste à vérifier dans la liste de QCLs stockée dans la base de données de l'**ASP** si le client a le droit d'allouer des ressources réseaux dans le réseau de cœur. Par la suite, le **QM-WAN** sollicite son « Bandwiht Broker » pour s'assurer de la disponibilité des ressources dans son réseau.

Si les ressources disponibles ne sont pas suffisantes pour satisfaire la requête reçue ou le **QM-WAN** ne trouve pas de règle autorisant le client à demander des ressources réseaux, il renvoie vers le demandeur un message d'erreur. Sinon, le **QM-WAN** complète le traitement de cette requête en configurant les équipements nécessaires pour mettre en place cette requête (les détails de la procédure de traitement des requêtes dans le **QM-WAN** ont été exposés dans la section 4.3.2.2). Si la réservation de ressources dans le réseau cœur est inférieure (notamment au niveau de la bande passante) à la demande initiale, le **QM-WAN** va modifier la requête UPnP QoS initiale afin, à nouveau, de propager une requête de QoS cohérente.

Si la demande de réservation de ressources se termine avec succès dans le **QM-WAN**, l'**ASP** continue le processus de réservation de ressources de bout en bout en transférant la requête UPnP QoS du demandeur vers sa destination (étapes 13-16). Cependant, avant de relayer la requête, l'**ASP** vérifie dans sa liste d'ACLs si le demandeur a le droit d'accéder au LAN réclamé dans la requête afin de préserver la sécurité des LANs des clients.

iv. Traitement de la requête de demande de QoS dans le LAN visité

Comme toutes les requêtes externes au LAN, la requête UPnP QoS du visiteur est traitée par le composant « UPnP RP » du **SM-LAN** dans le LAN visité. L' « UPnP RP » accepte la requête entrante parce qu'elle est authentifiée et autorisée par l'**ASP**.

Grâce à l'entête HTTP « FHqos » intégré dans cette requête, l'«UPnP RP» reconnaît qu'il a reçu une requête de QoS d'un point de contrôle UPnP QoS externe (étape 17) et non d'un point de contrôle UPnP A/V. Vu que la requête est déjà en format UPnP QoS, l'«UPnP RP» ne fait que translater les adresses IP publiques source et destination de cette requête en adresses IP privés (*adresse source* : adresse privé du Media Serveur stockant le contenu à récupérer ; *adresse destination* : adresse privé de la passerelle domestique) avant de la relayer vers le service « UPnP QosManager » de son **QM-LAN** (étape 16).

Le contrôle d'admission de la requête externe se fait en deux étapes au niveau du **QM-LAN**. Tout d'abord, le service «UPnP QosManager» s'assure via son service « UPnP QosPolicyHolder» que le contact externe possède une autorisation pour la réservation de ressources réseaux dans son LAN. Ensuite, l'«UPnP QosManager» examine la disponibilité de son réseau pour garantir le transfert du nouveau flux avec les caractéristiques décrites dans la requête (les détails de la procédure de réservation des ressources avec le composant **QM-LAN** ont été exposés dans la section 4.3.2.3). Le résultat de la réservation est retourné au LAN de l'initiateur de la demande de QoS via l'**ASP** (étapes 19-22). Cette dernière étape nous permet de nouveau de s'assurer de la cohérence des réservations et de synchroniser le cas échéant le volume de ressources à réserver dans chaque partition de réseau. Pour cela, l'ASP sollicite de nouveau son **QM-WAN** pour vérification et confirmation et l'«UPnP RP» du réseau visiteur sollicite en retour son **QM-LAN**.

Lorsque l'«UPnP RP» du LAN du visiteur reçoit la réponse à sa demande de QoS externe, il la communique au déclencheur de cette demande qui est son «UPnP Proxy» (étape 23). Si le résultat de la réservation est négatif, l'«UPnP RP» peut refaire une nouvelle tentative de réservation si le contenu distant est proposé par le Media Serveur distant avec un autre encodage qui demande moins de ressources réseaux. Sinon, l'«UPnP RP» libérer les ressources déjà allouées à cette requête, dans son LAN et dans le réseau de cœur. De la même façon que pour la solution basée sur l'IMS, il est possible de spécifier un intervalle de ressources à réserver (bande passante minimale et maximale) dans la requête UPnP QoS de sorte à réaliser la réservation en une seule passe.

Dans le cas où le résultat de la réservation est positif, l'«UPnP Proxy» peut terminer la procédure de récupération du contenu distant en exécutant les mêmes étapes de la procédure de récupération de contenu sans QoS (étapes 24-33) : i) il relaie la requête du **CMF** à l'**ASP**, ii) l'**ASP** vérifie le droit du demandeur à accéder au LAN distant et transfère après la requête au LAN destination, iii) le **SM-LAN** distant (composant UPnP RP) s'assure que le visiteur a le droit d'accéder au contenu désigné dans la requête avant de répondre au visiteur avec l'URL directe pour récupérer le contenu.

Le Media Renderer peut alors chercher le contenu directement dans le LAN distant (étapes 34-39). Le flux de ce contenu aura une garantie de QoS au moment de son transfert grâce à la réservation préalable du **QM** (**QM-WAN** et les **QM-LAN**).

Modification des ressources d'une session

Si le visiteur utilise une même session pour visionner des contenus avec les mêmes caractéristiques de QoS, son **SM-LAN** exécute la procédure de récupération de contenu sans demande de QoS puisqu'il n'a pas besoin de modifier les paramètres de QoS de la session.

Mais, si le nouveau contenu choisi n'a pas les mêmes caractéristiques que le dernier contenu

transféré avec cette session, le **SM-LAN** doit modifier les paramètres de QoS de la session avant de récupérer le contenu. Donc, l'«UPnP Proxy» déclenche la procédure de modification de ressources de cette session. Les étapes de cette procédure sont identiques à celles de la procédure de réservation de ressources de bout en bout décrite dans le paragraphe précédent (étapes 4-23). La différence entre les deux procédures c'est que les **SMs** envoient (**SM-LAN**, **SM-WAN**) des requêtes de modification de réservation (requête UpdateTrafficQos) aux **QMs** (**QM-LAN**, **QM-WAN**) au lieu des requêtes de réservation.

A la fin de la procédure de modification de ressources, le visiteur peut alors récupérer avec cette session son nouveau contenu directement du LAN distant avec une garantie de QoS lors du transfert du flux de ce contenu.

Fermeture de session avec libération des ressources

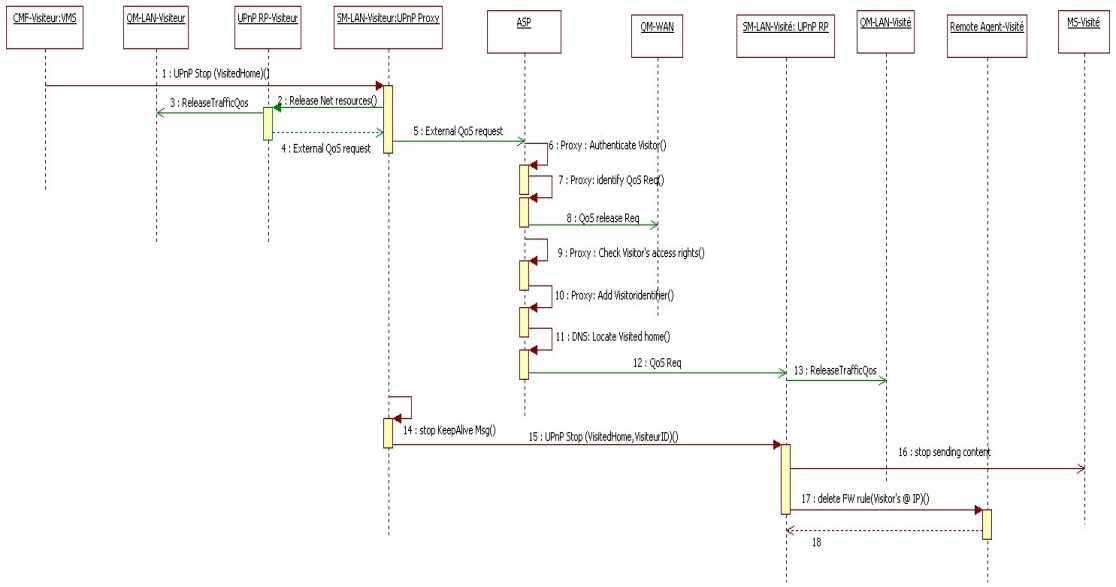


Figure 4.30 Fermeture de session avec libération de ressources, solution Http

A la fin de l'utilisation d'une session ouverte avec un LAN distant, le **CMF** du visiteur doit contacter son système d'accès à distance (**SM**) pour lancer une procédure de fermeture de session. D'une part, pour préserver la sécurité du LAN visité, le **SM** doit supprimer la règle du pare-feu ajoutée dans la passerelle domestique du LAN visité permettant au visiteur l'accès direct au LAN de l'appelé. D'autre part, le système de gestion de QoS (**QM)** doit libérer les ressources réseaux qu'il a allouées à cette session dans le LAN du visiteur, le réseau de cœur et le LAN visité. Cette procédure est illustrée dans la Fig. 4.30.

La procédure de fermeture de session est déclenchée dans le LAN du visiteur, lorsque le **CMF** envoie une requête UPnP A/V stop à son **SM-LAN** (composant UPnP Proxy) (étape 1). Etant donné que le **SM-LAN** est configuré de façon à gérer la QoS, le composant « UPnP Proxy » contacte son composant «UPnP RP» (fonction UPnP QoS Control Point) afin de demander la libération des ressources de cette session (étapes 2-3). L'«UPnP RP» sollicite alors le service « UPnP QosManager » du **QM-LAN** pour libérer les ressources réseaux de cette session dans son LAN (étapes 2&3)**.** Il reste après la libération des ressources réseaux allouées dans le réseau de cœur et dans le LAN visité. Comme pour la demande de réservation de ressources réseaux de bout en bout, l'«UPnP RP» formule avec sa fonction point de contrôle UPnP QoS une requête UPnP QoS de libération de ressources et la relaie avec l'«UPnP Proxy» au LAN destination via l'**ASP** (étape 4). Comme pendant la procédure de demande de QoS, l'«UPnP RP» insère dans cette requête externe l'entête «FHqos» avec la valeur «YES». Cet entête permettra à l'**ASP** et au **SM-LAN**

du côté visité de savoir que c'est une requête de QoS.

En effet, la requête de libération de ressources sera authentifiée et par la suite reconnue au niveau de l'**ASP**. Elle sera alors transférée vers le composant **QM-WAN** de l'**ASP** pour terminer la réservation des ressources réseaux de cette session (étapes 5-8). L'**ASP** termine après le traitement de la requête de QoS inter-LANs (UPnP ReleaseTrafficQos) avant qu'il la transfère à destination (étapes 9-12): il i) vérifie le droit du visiteur à accéder au LAN réclamé dans la requête, ii) insère l'identifiant du visiteur dans la requête iii) et localise le LAN distant.

L'«UPnP RP» du côté du LAN visité accepte la requête de libération de ressources (requête ReleaseTrafficQos) en provenance de l'**ASP**. Avec l'entête « FHqos », il la reconnaît comme une requête de QoS. Comme elle est déjà en format UPnP QoS, il la transfère au service « UPnP QosManager » de son **QM-LAN** pour la traiter (étape 13). Cette étape termine la phase de libération des ressources réseaux associées à cette session dans tout son chemin de données (LAN visiteur, réseau de cœur et LAN visité).

Pour terminer la procédure de fermeture de session, le **SM-LAN** du visiteur exécute les étapes de fermeture de session standard (session sans QoS) (étapes 14-18): i) il arrête l'envoi des messages de rafraîchissement (keepAlive) vers le LAN destination, ii) envoie vers le LAN visité la requête UPnP A/V stop. En recevant cette requête, le **SM-LAN** dans le LAN visité supprime la règle de pare-feu pour préserver la sécurité de son LAN et demande à son Media Serveur d'arrêter l'envoi du flux média.

4.4 Conclusion

Dans ce chapitre nous avons présenté un système qui permet de garantir la QoS aux flux échangés par le service de partage de contenus à distance étudié dans Feel@Home. Nous avons appelé ce système « système de gestion de QoS ». Il propose une architecture réseau pour la commande de la mise en place d'une QoS cohérente tout au long du chemin de données des flux du service de partage de contenu à distance, soit dans les réseaux domestiques et dans les réseaux cœurs.

La première étape de la réalisation de ce système de gestion de QoS était de proposer une architecture fonctionnelle générique indépendante de la technologie à utiliser pour implémenter ce système. Cette étude fonctionnelle nous a permis de bien définir les cas d'utilisation du système, les principaux blocs fonctionnels qui le constituent et ses interfaces avec les composants du service de partage de contenus à distance et plus précisément avec le système d'accès à distance.

L'architecture proposée repose sur deux principaux composants : les **QM-LAN** et **QM-WAN** déployés respectivement dans les LANs des clients et dans le réseau de cœur. Le composant **QM-LAN** prend en charge la gestion de la QoS dans le LAN de l'utilisateur. Il offre aussi la possibilité à l'utilisateur de désigner parmi la liste de ses contacts distants ceux qui ont le droit de réserver des ressources réseaux dans son LAN. Le composant **QM-WAN** assure la gestion de la QoS dans le réseau de cœur. La collaboration entre les **QM-LANs** des LANs des visiteurs, le **QM-WAN** et les **QM-LANs** des LAN visités offre, aux flux échangés entre les LANs des clients du service de partage de contenus à distance, une garantie de QoS de bout en bout. Le système d'accès à distance participe à cette collaboration en permettant aux **QM-LANs** et **QM-WAN** de s'échanger la signalisation de mise en place de la QoS d'une manière sécurisée.

Ensuite, nous sommes passés à l'étude de la réalisation technique des composants du système de gestion de QoS. Pour le composant **QM-LAN**, nous avons examiné l'aptitude des technologies UPnP QoS et AVB à implémenter ce composant. Cette étude a révélée que la technologie UPnP QoS répond le plus aux fonctionnalités que nous avons définies pour le **QM-LAN**. Cette technologie était aussi plus facile à intégrer dans le service de partage de contenus à distance vu

le choix de l'utilisation d'UPnP A/V dans le LAN. Pour ces raisons, nous avons choisi d'utiliser UPnP QoS dans l'implémentation du composant **QM-LAN**.

La réalisation du composant **QM-WAN** était liée à la technologie utilisée dans le réseau de cœur dans le système d'accès à distance. Nous avons alors proposé deux réalisations du **QM-WAN**: une pour la version du système d'accès à distance utilisant l'environnement IMS et une deuxième pour la solution « HTTP» de ce système.

La première version du **QM-WAN** se base sur la fonction **RACS** de l'IMS. Pour cette version, nous sommes revenus à notre modèle de simulation UML du service de partage de contenus. Nous avons ajouté à ce modèle les composants du système de gestion de QoS. Par la suite, nous avons réalisé une série de simulations pour valider fonctionnellement l'intégration de ce système dans le service de partage de contenus à distance.

Dans la deuxième version, dédiée à la solution « HTTP», nous avons recommandé l'utilisation du modèle DiffServ de l'IETF pour implémenter ce composant. Nous verrons dans le dernier chapitre qu'il est envisageable d'utiliser d'autres techniques, telles que MPLS.

Dans la dernière section de ce chapitre, nous avons mis l'accent sur l'intégration des composants du système de gestion de QoS dans l'architecture générale du service de partage de contenus à distance afin que ce service offre à ses clients une garantie de QoS. Nous avons décrit dans cette section les modifications introduites par l'intégration du système de gestion de QoS aux procédures d'utilisation du service de partage de contenus à distance :

- Configuration des partages avec QoS ;
- Récupération de contenus distants avec réservation de ressources réseaux ;
- Modification des ressources d'une session ;
- Fermeture de session avec libération de ses ressources réseaux.

Chapitre 5

Conclusion et perspectives

Sommaire

Cette dernière décennie, la révolution numérique a eu un grand impact sur la société moderne. Elle a construit un nouveau paradigme dans la façon dont nous nous comportons et nous vivons ensemble. Très peu d'aspects de l'activité humaine pourraient être considérés comme non touchés par les possibilités offertes par l'ère numérique. Par exemple, récupérer des informations, acheter des biens sur Internet, communiquer et échanger des contenus multimédias avec des amis sont les exemples les plus marquants qui ont considérablement modifié notre vie quotidienne.

Dans cette thèse, nous nous sommes intéressés aux services de partage de contenus entre des utilisateurs connectés à des réseaux domestiques distants. Elle s'intègre dans le projet européen Feel@Home. Ce projet a étudié et proposé un nouveau service de partage de contenus à distance qui offre la sécurisation des réseaux de ces clients ainsi que la confidentialité de leurs contenus, et qui aussi garantit la QoS lors du transfert de ces contenus.

5.1 Bilan

Les travaux de cette thèse ont contribué à la définition de l'architecture du plan de contrôle du réseau nécessaire à la réalisation du service de partage de contenus multimédias étudié dans le projet Feel@Home. Les deux principales problématiques que nous avons traitées dans ce mémoire sont :

- L'architecture réseaux d'accès à distances pour le service de partage de contenus;
- La garantie de QoS pour les flux échangés par le service de partage de contenus.

5.1.1 Architecture réseau d'accès à distance

L'étude des architectures réseaux d'accès à distance dans la littérature nous a montré leur insuffisance et inadéquation à notre contexte de partage de contenus. D'abord, ils ne prennent pas en compte la problématique de gestion de QoS et ils sont généralement complexes à intégrer aux technologies utilisées dans les réseaux domestiques de clients (UPnP AV et DLNA). La sécurité et la confidentialité sont soit absentes, soit tributaires de la plate-forme d'hébergement, et souvent dépendantes du contrat d'utilisation ou de licence (couramment modifié au détriment de l'utilisateur : cf. CLUF de Facebook par exemple). Finalement, les solutions dans la littérature sont mal adaptées au déploiement à une grande échelle (plusieurs millions d'utilisateurs).

Afin d'éviter les lacunes et limitations de ces solutions, nous avons commencé nos études par la proposition d'une architecture générique fonctionnelle pour l'accès à distance qui soit indépendante de la technologie à utiliser pour l'implémenter. Cette architecture a servi pour bien définir les blocs fonctionnels et leurs interfaces avec le service de partage de contenus. Les deux grandes briques de cette architecture sont :

- Le **SM-WAN**: déployé dans le réseau cœur, il protège les réseaux domestiques des utilisateurs du service de partage de l'accès non autorisé et de l'usurpation d'identité des contacts distants ;
- Le **SM-LAN**: déployé dans les réseaux domestiques des utilisateurs, il complète la sécurisation offerte par le **SM-WAN** en ajoutant dynamiquement des règles dans les pare-feux des passerelles domestiques afin d'accepter les demandes d'accès des contacts distants authentifiés et autorisés par le **SM-WAN**. Il assure aussi la confidentialité des contenus grâce au filtrage qu'il effectue sur les contenus que chaque contact a le droit de récupérer de son réseau.

Dans un deuxième temps, nous avons proposé deux réalisations techniques de notre architecture fonctionnelle. La première solution se base sur le Framework IMS. Dans cette solution, nous utilisons l'IMS pour établir des sessions *HTTP* sécurisées entre les deux correspondants distants. Le **SM-WAN** est basé sur un serveur de présence IMS. L'établissement

de sessions *HTTP* permet au service de partage d'être compatible avec les technologies les plus déployées dans les réseaux des clients, à savoir DLNA et UPnP A/V, qui se basent toutes les deux sur ce protocole lors de la signalisation et du transfert des contenus.

La deuxième réalisation technique de cette architecture est plus adaptée au déploiement sur Internet car elle s'appuie sur l'utilisation des relais applicatifs *HTTP* (proxy). Nous avons implémenté le **SM-LAN** avec deux proxys: un proxy qui relaie les messages de signalisation sortant du LAN vers le **SM-WAN** et un deuxième proxy inverse pour traiter les requêtes entrantes au LAN. Le **SM-WAN** est basé autour d'un proxy qui a pour mission d'authentifier les initiateurs des sessions et de vérifier leur droit à accéder au LAN désigné dans leur requête. Comme dans la solution IMS, les sessions *HTTP* établies servent à échanger les flux de données en mode point-à-point entre les utilisateurs afin d'éviter l'engorgement du **SM-WAN**. Nous avons maquetté cette solution dans le cadre du projet Feel@Home. D'autres versions de cette maquette ont été produites au sein des laboratoires d'Orange Labs pour tester le service de partage avant un possible déploiement au grand public. Ces versions sont en cours de test (FUT – Field User Trial) au niveau d'Orange Labs France et Orange Espagne. Nous avons aussi conduit des simulations pour tester la capacité du nœud central, qui est le **SM-WAN**, à passer à l'échelle. Les résultats de ces tests nous ont permis de dimensionner les ressources à déployer dans ce nœud pour servir un grand nombre d'utilisateurs (plusieurs dizaines de million).

Outre le test auprès d'utilisateurs (FUT – Field User Trial), notre solution a donné lieu à plusieurs contributions en normalisation. Ainsi, le SM-LAN et SM-WAN sont décrits dans le standard UPnP-RAv2 publié en Aout 2011 (version proxy http) et seront publiés prochainement dans la prochaine version des standards de l'ETSI/TISPAN (version IMS).

5.1.2. Gestion de la QoS dans le service de partage de contenus à distance

Afin de garantir la QoS pendant le transfert des contenus entre les utilisateurs du service de partage à distance, nous avons proposé une architecture réseau pour commander la mise en place de la QoS de bout en bout, tout au long du chemin de données emprunté par les contenus (dans les réseaux des clients et dans les réseaux cœurs). Nous avons adopté la même méthodologie que celle que nous avons utilisée pour réaliser l'architecture d'accès à distance. Nous avons commencé par définir une architecture fonctionnelle générique et indépendante de la technologie pour identifier les blocs fonctionnels de cette architecture et ses interfaces avec les composants du service de partage et notamment ceux utilisés dans l'architecture d'accès à distance.

L'architecture de QoS proposée repose sur deux composants :

- Le **QM-LAN**: déployé dans les réseaux des utilisateurs, il prend en charge la gestion de la QoS dans les réseaux domestiques. Il permet aussi à l'utilisateur de désigner parmi ses contacts ceux à qui il accorde le droit de réserver des ressources dans son réseau. Pour implémenter ce composant, nous avons examiné les technologies AVB et UPnP QoS. Le résultat de cette étude a démontré que la technologie UPnP QoS était plus adaptée et plus complète pour réaliser ce composant.
- Le **QM-WAN**: déployé dans le réseau cœur, il assure la gestion de la QoS dans le WAN. Il coopère aussi avec les QM-LANs dans les réseaux domestiques des utilisateurs pour offrir au service de partage une QoS de bout en bout. Nous avons proposé deux réalisations techniques pour ce composant, la première à l'aide de la fonction RACS de l'IMS et une deuxième basée sur le modèle DiffServ de l'IETF.

Nous utilisons l'architecture d'accès à distance pour échanger d'une manière sécurisée les messages de signalisation échangés entre les **QM-LANs** et **QM-WAN**. En effet, dans la dernière partie de la thèse, nous avons mis l'accent sur l'intégration des composants **QM-LAN** et **QM-WAN** dans l'architecture d'accès à distance pour qu'elle prenne en charge la gestion de QoS de bout en

bout et notamment proposer une solution pour résoudre la problématique de traversé des pare-feux et des NAT.

5.2 Perspectives

Nous avons proposé une architecture réseau d'accès à distance adaptée au contexte du partage de contenus à distance. Toutefois, il reste des évolutions à apporter à cette architecture:

*Indexation des contenus dans le LAN au niveau du **SM-LAN***

Certains Media Serveur UPnP, lors du redémarrage, changent l'indexation de leurs données. Il est donc important d'être capable de vérifier au démarrage des Media Serveurs s'il y a eu une mise à jour de l'indexation des données et donc le cas échéant de notifier le **SM-LAN** pour les mettre à jour. Il est donc souhaitable, pour une meilleure expérience utilisateur, de pouvoir proposer une solution de gestion des index indépendamment de l'indexation réalisée par chaque Media Server. De plus, une telle indexation permettrait de développer un moteur de recherche distribuée. Par exemple, vous souhaitez trouver une photo, une musique, un film sans forcément savoir où il est localisé. Le moteur de recherche permettrait alors à l'utilisateur de lancer une recherche parmi tous les index de ses amis afin de trouver le contenu souhaité.

Généralisation de l'utilisation de l'architecture d'accès à distance

En plus des améliorations, pour mieux adapter nos solutions au contexte des services de partage de contenus, nos travaux sur l'architecture réseau d'accès à distance peuvent être repris dans le contexte de la domotique et de la commande des équipements à distance.

En effet, les sessions sécurisées établies vers les réseaux distants des utilisateurs peuvent servir à commander à distance des équipements de la maison ou à commander des équipements d'un réseau local d'entreprise. Notre architecture fonctionnelle générique peut être adaptée et réutilisée pour mettre en place des sessions sécurisées pour commander les équipements distants. Les modifications majeures à effectuer sont au niveau du composant **SM-LAN** pour l'adapter à l'utilisation de la session. Actuellement, nous étudions à Orange Labs les cas d'utilisation suivants :

- Energie : effectuer des diagnostiques sur l'installation électrique, relever automatiquement la consommation électrique dans les maisons des clients ou récupérer des informations sur l'état des équipements électriques à distance;
- Domotique : offrir aux clients un service sécurisé de commande des équipements de leur maison, tel que la fermeture des volets, la commande du chauffage de l'éclairage …
- Industrie : permettre aux acteurs distants impliqués, d'obtenir les informations nécessaires caractérisant certains équipements locaux de l'usine et ensuite éventuellement de les manipuler en vue d'une optimisation distribuée ou globale.

Nous avons vu au chapitre 4 que le **SM-WAN** et le **SM-LAN** peuvent aiguiller différemment les requêtes suivants leur type (dans notre cas entre le partage des contenus et la gestion de la QoS). Il est donc aisé d'envisager d'étendre puis de généraliser le mécanisme d'aiguillage afin d'offrir un Framework simple à des tiers via des interfaces programmables (API).

Amélioration du système de gestion de QoS

Transcodage à la volée

Le transcodage peut être utilisé pour adapter le contenu à un équipement donné, comme par exemple un téléphone mobile, ou bien à cause de l'insuffisance des ressources réseaux. Il peut être réalisé soit dans le réseau cœur, soit dans la maison dans laquelle est stocké le contenu. Nous recommandons de réaliser le transcodage des contenus dans le réseau domestique afin de

le réaliser au plus près de l'équipement dans lequel ils sont stockés.

Définition d'une nouvelle classe de service

Les contraintes de QoS exprimées par les sessions utilisées pour la commande des équipements à distance sont différentes de celles des classes de services que nous avons définies pour le service de partage de contenus. En effet, si elles ne demandent pas beaucoup de débit, elles ont besoin d'un court délai de transmission, d'une gigue restreinte et d'un faible taux de perte pour assurer une interaction forte. Nous devons alors définir une nouvelle classe de service afin que notre système de gestion de QoS la prenne en compte.

Gestion de la QoS dans la solution IMS

Pour la solution IMS, nous avons étudié la mise en place de sessions sécurisées dans un cadre de multi-opérateurs, mais nous n'avons pas étudié la gestion de la QoS dans ce cas de figure. En effet, au niveau de la gestion de la QoS, nous avons pris comme hypothèse que le réseau de cœur est géré par un seul opérateur et donc une seule autorité administrative. Nous devons donc considérer le cas où le réseau de cœur est géré par plusieurs opérateurs.

Avec l'IMS, il est prévu de supporter la gestion de la QoS entre plusieurs opérateurs. La modification à apporter concerne la phase de « mise en place de la demande » puisque la nouvelle demande de QoS concerne deux **RACS** (ou plus). La spécification de la fonction **RACS** prévoit la coopération entre **RACS** pour réserver des ressources pour les sessions entre plusieurs opérateurs. Lorsqu'un **RACS** reçoit une demande de QoS impliquant plusieurs domaines, l'étape de l'admission d'appel demande la coopération de tous les **RACS** de ces domaines. Et après cette vérification, ces **RACS** peuvent configurer les ressources de leurs réseaux et le **RACS** initiateur de cette réservation renvoie alors une réponse à son **QM-WAN** client. Des mécanismes de cette réservation inter-opérateurs restent à spécifier, surtout dans notre contexte où nous avons envisagé d'avoir une QoS cohérente tout au long le chemin de donnée de nos flux.

De la même manière, l'IMS a prévu de distinguer la gestion des ressources dans le réseau de cœur et les réseaux d'accès. Pour ce faire, la fonction RACF (Resource Admission and Control Function) du **RACS** peut se décliner en A-RACF (Access RACF) et C-RACF (Core RACF) gérant respectivement le réseau d'accès et le réseau de cœur. Donc, il faut étudier plus en détail la phase de mise en place de la QoS dans le WAN pour coordonner la QoS au niveau du réseau d'accès et au niveau du réseau cœur.

Gestion de la QoS dans la solution HTTP

Dans le chapitre 4 nous avons proposé une solution de gestion de la QoS dans le réseau de cœur basé sur l'utilisation du modèle DiffServ. Une autre solution pourrait être envisagée à l'aide de l'ingénierie de trafic en utilisant l'environnement MPLS-TE.

Les tunnels MPLS-TE peuvent être utilisés pour établir des connexions avec une certaine QoS à l'inter-domaine pour échanger le trafic du service de partage. Comme dans la solution IMS, plusieurs défis restent à surmonter, telles que la coordination de la réservation d'une QoS cohérente dans les domaines entrant en jeu dans la transmission des flux :

- Le calcul du meilleur chemin : centralisé ou distribué ;
- La signalisation à utiliser ;
- Le traitement des cas d'erreur selon le mode du calcul du chemin …

L'opérateur peut aussi provisionner son réseau en établissant des tunnels MPLS-TE entre ses principaux points de collecte afin de les réutiliser pour échanger les trafics générés par le service de partage de contenus. Un contrôle d'admission sur les trafics envoyés dans ses tunnels est nécessaire pour ne pas les congestionner.

Finalement, nous pouvons envisager l'utilisation de la technologie MPLS-TE pour mettre en place des tunnels qui garantissent la QoS directement entre les deux passerelles de domestiques des clients. Ces tunnels seront ré encapsulés dans des tunnels de niveau supérieur (par utilisation de la propriété de label stacking de MPLS) déjà préparés par l'opérateur pour le service de partage. Cette perspective soulève certains problèmes. Le premier est la capacité de cette solution à passer à l'échelle surtout pour un service dédié au grand public. Le deuxième est la sécurisation de la signalisation initiée par les passerelles domestiques pour mettre en place les tunnels MPLS.

Liste des Publications

O.Dugeon, M.Mahdi, R.Bars, R.Carbou. *Extended UPnP multimedia contents delivery with HTTP proxy*. 3rd International Workshop on FUTURE MULTIMEDIA NETWORKING 2010, Krakow, Poland, Juin 2010.

M.Mahdi, O.Dugeon, R.Bars, B.Lamer. *New UPnP Service for Multimedia Remote Sharing with IMS Framework*. 14th International Conference on Intelligence in Next Generation Networks 2010, Berlin, Germany, Octobre 2010.

Ce papier a été récompensé par le prix du meilleur papier.

M.Mahdi. *Système de session à la demande pour le transfert de contenu multimédia*. 11e Congrès EDSYS 2010, Toulouse, France, Mai 2010.

Brevet

O.Dugeon, M.Mahdi, R.Bars. *Procéder de partage de contenus multimédias entre réseaux domestiques*. INPI No 09 59255.

Glossaire

AAA: Authentication, Authorization, Accounting.
AVB: Audio Video Bridging.
ACL: Access Control List.
AS: Application Server.
ASP: Authentication & Security Plateform.

BGF: Border Gateway Function.

CPU: Central Processing Unit.
CPL : Courant Porteur en Ligne.
CSCF: Call Session Control Function.

DNS: Domain Name Server.
DHCP: Dynamic Host Configuration Protocol.
DMS: Digital Media Server.
DMP: Digital Media Player.
DMR: Digital Media Renderer.
DMC: Digital Media Controller.
DMPr: Digital Media Printer.
DLNA: Digital Living Network Alliance.

ETSI: European Telecommunications Standards Institute.

HGI: Home Gateway Initiative.
HIGA: Home IMS Gateway.
HSS: Home Subscribe Server.
HGW: Home Gateway.
HTTP: HyperText Transfer Protocol.

IP: Internet Protocol.
IEEE: Institute of Electrical and Electronics Engineers.
IETF: Internet Engineering Task Force.
IMS: IP Multimedia Subsystem.

LAN: Local Area Network.
LDP: Label Distribution Protocol.
LER: Label Edge Router.
LSP: label Switch Path.

M-DMS Mobile: Digital Media Server.
M-DMP Mobile: Digital Media Player.
M-DMU Mobile: Digital Media Uploader.
M-DMD Mobile: Digital Media Downloader.
M-DMC Mobile: Digital Media Controller.
MPLS: Multi Protocol Label Switch.
MRP: Multiple Registration Protocol.
MSRP: Multiple Stream Registration Protocol.
MVRP: Multiple VLAN Registration Protocol.
MMRP: Multiple MAC Registration Protocol.
NAT: Network Address Translation.

NSIS: Next Steps in Signaling.

PCN: Congestion and Pre-congestion Notification.

QoE: Quality of Experience.
QoS: Quality of Service.
QM: QoS Manager.
QM-LAN: QoS Manager in Local Area Network.
QM-WAN: QoS Manager in Wide Area Network.

RACS: Resource and Admission Control Subsystem.
RA-AS: Remote Access Application Server.
RSVP: Ressource Reservation Protocol.
RTP: Real-Time Transport Protocol.
RCEF: Resource Control Enforcement Function.
RACF: Resource Admission Control Function.

SOAP: Simple Object Access Protocol.
SSDP: Simple Service Description Protocol.
SDP: Session Description Protocol.
SIP: Session Initiation Protocol.
SIP UA: SIP User Agent.
SRP: Stream Reservation Protocol.
SM: Session Manager.
SM-LAN: Session Manger in Local Area Network.
SM-WAN: Session Manager in Wide Area Network.
SPDF: Serving Policy Decision Function.

UPnP: Universal Plug and Play.
UPnP A/V: UPnP Audio/Video.
UPnP QoS: UPnP Quality of Service.
UPnP RA: UPnP Remote Access.
UPnP IGD: Internet Gateway Device.
UPnP RP: UPnP Reverse Proxy.
UDP: User Datagram Protocol.

VoD: Video on Demand.
VPN: Virtual Private Network.
VoIP: Voice over IP.

WAN: Wide Area Network.

XML: Extensible Markup Language.

Bibliographie

[1] UPnP Forum. *Upnp av architecture v1.0*. Jun 2002.

[2] Digital Living Network Alliance. *Dlna home networked device interoperability guidelines v1.0.* Jun 2004.

[3] UPnP Forum. *Upnp device architecture v1.1*. Oct 2008.

[4] R. Droms. *Dynamic host configuration procotol (dhcp),* RFC2131. Mar 1997.

[5] T. Cai, P. Leach, Y. Gu, S. Albright. *Simple Service Discovery Protocol,* internet draft. Oct 1999.

[6] Simple Object Access Control. *http://www.w3.org/TR/soap/*.

[7] J. Cohen, S. Aggarwal, Y. Y. Goland. *General Event Notification Architecture Base: Client to Arbiter,* internet draft. Jun 1999.

[8] UPnP Forum. *Remote access architecture v1.0*. Sept 2009.

[9] UPnP Forum. *Raclient v1.0*. Sept 2009.

[10] UPnP Forum. *Raserver v1.0.* Sept 2009.

[11] T. Cagenius, A. Fasbender, J. Hjelm, U. Horn, I. Más Ivars and N. Selberg. *Evolving the TV experience: Anytime, anywhere, any device*. Technical Report 3. 2006.

[12] A. Fasbender, M. Gerdes, J. Hjelm, B. Kvarnstrom, J. Petersson, and Robert Skog. *Virtually at home: High-performance access to personal media.* Technical Report 2, Nov 2008.

[13] G. Camarillo A. Johnston J. Peterson R. Sparks M. Handley J. Rosenberg, H. Schulzrinne and E. Schooler. *Session initiation protocol (sip),* RFC3261. Jun 2002.

[14] P. Calhoun, J. Loughney, E. Guttman, G. Zorn and J. Arkko, *Diameter Base Protocol*, RFC3588, Sept 2003.

[15] M. Handley and V. Jacobson. *Session description protocol (sdp),* RFC2327. Apr 1998.

[16] HGI. *Home gateway requirements: Residential profile, home gateway initiative*. Apr 2008.

[17] B. Diraison, D. Mischler, L Toutaint. *Systermin@l: Consumer devices for ims/tispan deployment*. Broadband Multimedia Systems and Broadcasting, 2009. BMSB '09. IEEE International Symposium. May 2009.

[18] S.Chintada, P.Sethuramalingan, G.Goffin. *Converged services for home using a sip/upnp software bridge solution.* 5th IEEE Consumer Communications and Networking Conference, 2008. CCNC 2008. Jan 2008.

[19] B. Kumar and M. Rahman. *Mobility support for universal plug and play (upnp) devices using session initiation protocol (sip)*. 3rd IEEE Consumer Communications and Networking Conference, 2006. CCNC 2006. Jan. 2006.

[20] Y.1541. *Network Performances Objectives for IP-based Services.* ITU-T. Jan 2005.

[21] UPnP Forum. *Upnp qos architecture :1*. Mar 2005.

[22] UPnP Forum. *Upnp qos architecture :2*. Oct 2006.

[23] UPnP Forum. *Upnp qos architecture :3*. Nov 2008.

[24] IEEE 802.1 Audio/Video Bridging Task Group. *http://www.ieee802.org/1/pages/ avbridges .html*. Mar 2008.

[25] UPnP Forum. *Upnp qosmanager :3*. Nov 2008.

[26] UPnP Forum. *Upnp qospolicyholder :3*. Nov 2008.

[27] UPnP Forum. *Upnp qosdevice :3*. Nov 2008.

[28] IEEE P802.1Qat. *Draft 4.2 standard for local and metropolitan area networks virtual bridged local area networks amendment xx : Stream reservation protocol (srp)*. Dec 2009.

[29] IEEE P802.1Qav. *D4.0 vblan amendment12. draft standard for local and metropolitan area networks timing and synchronization for time-sensitive applications in bridged local area networks*. Dec 2010.

[30] IEEE P802.1AS. *Draft standard for local and metropolitan area networks, timing and synchronization for time-sensitive applications in bridged local area networks*. Jun 2008.

[31] IEEE 802.1ak. *Virtual bridged local area networks amendment 7: Multiple registration protocol.* Jun 2007.

[32] IEEE 802.1QTM. *IEEE standard for local and metropolitan area networks, virtual bridged local area networks.* May 2006.

[33] J. Imtiaz, J. Jasperneite, L. Han. *A Performance Study of Ethernet Audio Video Bridging (AVB) for Industrial Real-time Communication,* 14th IEEE international conference on Emerging Technologies Factory Automation. ETFA'09. Sept 2009.

[34] AVnu Alliance. *http://www.avnu.org/* .

[35] TISPAN. *Etsi ts 182 019 : Resource and admission control sub-system (racs).* 2006.

[36] TISPAN. *Es 282 003: Final draft resource and admission control sub-system (racs)*. Jul 2009.

[37] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin. *Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification*, RFC 2205 (Updated by RFCs 2750, 3936, 4495). Sep 1997.

[38] S. Shenker, C. Partridge and R. Guerin. *Specification of Guaranteed Quality of Service*, RFC 2212. Sep, 1997.

[39] J. Wroclawski. *Specification of the Controlled-Load Network Element Service*, RFC2211. Sep 1997.

[40] H. Schulzrinne and R. Hancock. *GIST: General Internet Signalling Transport*, RFC5971. Oct 2010.

[41] J. Manner, G. Karagiannis, and A. McDonald. *NSLP for Quality-of-Service Signaling*, draft-ietf-nsis-qos-nslp-16.txt. Feb 2008.

[42] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss. *An Architecture for Differentiated Service*, RFC 2475 (updated by RFC 3260). Dec 1998.

[43] B. Davie et al. *An Expedited Forwarding PHB (Per-Hop Behavior)*, RFC 3246. Mar 2002.

[44] J. Heinanen, F. Baker, W. Weiss, J. Wroclawski. *Assured Forwarding PHB Group*,RFC 2597 (Updated by RFC 3260). Jun 1999.

[45] K. Nichols, V. Jacobson and L. Zhang. *A Two-bit Differentiated Services Architecture for the Internet*, RFC 2638. Jul 1999.

[46] M. Menth and F. Lehrieder. *Performance Evaluation of PCN-Based Admission Control*, In Proc. 16th International Workshop on Quality of Service. 2008. IWQoS'08, Enschede, June, 2008.

[47] S. Oueslati and J. Roberts *A new direction for quality of service: Flow aware networking*, In Proc. NGI'05, Rome. Apr 2005.

[48] E. Rosen, A. Viswanathan and R. Callon. *Multiprotocol Label Switching Architecture*, RFC 3031. Jan 2001.

[49] E. Rosen et al. *MPLS Label Stack Encoding*, RFC 3032 (Updated by RFCs 3443, 4182). Jan 2001.

[50] L. Anderson, P. Doolan, N. Feldman, A. Fredette, and B. Thomas. *LDP Specification*, RFC 3036. Jan 2001.

[51] J. Agogbua M. O'Dell D. Awduche, J. Malchom and J. McManus. *Requirements for traffic engineering over mpls*, rfc 2702,. Sep 1999.

[52] J. Ash and J.L. Le Roux. *Path Computation Element (PCE) Communication Protocol Generic Requirements*, RFC 4657. Sep 2006.

[53] J.P.V.A Farrel and J. Ash. *A Path Computation Element (PCE)-Based Architecture*, RFC 4655. Aug 2006.

[54] D. Gan T. Li V. Srinivasan D. Awduche, L. Berger and G. Swallow. *Rsvp-te : Extension to rsvp for lsp tunnels*, rfc 3209 (updated by rfcs 3936, 4420, 4874). Dec 2001.

[55] B. Jamoussi et al. Constraint-based lsp setup using ldp, rfc 3212 (updated by 3468). Jan 2002.

[56] R. Hancock, G. Karagiannis, J. Loughney, and S. Van den Bosch. *Next Steps in Signaling (NSIS): Framework*, RFC 4080. Jun 2005.

[57] Object Management Group. *OMG Unified Modeling Language Specification*. Septembre, 2001.

[58] Telelogic, *www.telelogic.com/products/tauUT.*

[59] Squid, *http://www.squid-cache.org/.*

[60] J. Elson and A. Cerpa. *Internet Content Adaptation Protocol (ICAP)*, rfc 3507. Apr 2003.

[61] Greasyspoon , *http://greasyspoon.sourceforge.net/.*

[62] Mysql, *http://www.mysql.fr/.*

[63] José Enríquez Gabeiras, Torsten Braun, Michel Diaz. End to End Quality of Service Over Heterogeneous Networks. Springer, 2008.

[64] Stelian-Florin Racaru. *Conception et validation d'une architecture de signalisation pour la garantie de qualité de service dans l'Internet multi-domaine, multi-technologie et multiservice*. Rapport de thèse, Université de Toulouse, 2008.

[65] Netfilter, *http://www.netfilter.org/.*

[66] NS3, *http://www.nsnam.org/.*

[67] H. Schulzrinne, A. Rao and R. Lanphier. *Real Time Streaming Protocol (RTSP)*, rfc 2326. Apr 1998.

[68] P. Vixie, S. Thomson, Y. Rekhter and J. Bound. *Dynamic Updates in the Domain Name System (DNS UPDATE)*, rfc 2136. Apr 1997.

[69] BIND, *http://doc.ubuntu-fr.org/bind9.*

[70] GNUDIP, *http://gnudip2.sourceforge.net/.*

[71] TISPAN. Etsi ts 185 003 V3.1.1 *: Customer Network Cateway (CNG), Architecture and Reference Points*. Juin 2010.

[72] TISPAN. Etsi ts 185 010 V3.0.4 : *Customer Premises Networks: Protocol Specification (Stage 3)*. Sept 2010.

[73] IEEE P802.1, Standard *for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Nov. 1997.

[74] HGI. HGI-GD013-R2 HGI Guideline Document: QoS white paper, *home gateway initiative*. Juin 2009.

[75] J. Gómez, E. Exposito, (CNRS). *Definition of the QoS requirements for the Community Network D6.3.1*. Sept 2010.

[76] S. Mizuno, T. Haruyama, H. Yamada, T. Abe, M. Kawashima, and O. Mizuno. *Adopting IPsec to SIP Network for On-Demand VPN Establishment between Home Networks*. Global Telecommunications Conference, IEEE GLOBECOM 2008. Dec 2008.

[77] T. Haruyama, S. Mizuno, M. Kawashima, and O. Mizuno. *Dial-to-Connect VPN System for Remote DLNA Communication.* 5th IEEE Consumer Communications and Networking Conference. CCNC 2008. Jan 2008.

[78] T. Abe, S. Mizuno, T. Haruyama, H. Chiba, and O. Mizuno. *On-Demand VPN Service between Home Networks for NGN Users*. 12th International Conference on Intelligence in Next Generation Networks, ICIN 2008. Oct 2008.

[79] K. Jung-Tae, O. Yeon-Joo, L. Hoon-Ki, P. Eui-Hyun and P. Kwang-Roh. *Implementation of the DLNA Proxy System for Sharing Home Media Contents*. Consumer Electronics, IEEE Transactions. Feb 2007.

[80] X. Yan, M. Xiaojun, C. Renlei, and Z. Guanghua. *Extending IMS Services to UPnP Home Network*. 2nd International Conference on Internet Multimedia Services Architecture and Applications 2008, IMSAA 2008. Dec 2008.

[81] R. Anane. *Autonomic Behaviour in QoS Management*. 3rd International Conference on Autonomic and Autonomous Systems 2007, ICAS07. Jun 2007.

[82] P. Eardley, Ed. *Pre-Congestion Notification (PCN) Architecture, rfc 5559. June 2009.*

Titre : Architectures réseaux pour le partage de contenus multimédias avec garantie de qualité de service.

Résumé : Le succès des services de partage de contenus multimédias sur internet témoigne de l'intérêt des utilisateurs à partager leurs expériences personnelles à travers des fichiers multimédias (photo, vidéo, musique). Les solutions actuelles sont basées essentiellement sur des serveurs web et souffrent d'un manque de QoS, de sécurité et de confidentialité. Plusieurs travaux de recherche ont été menés pour proposer des architectures réseaux d'accès à distance pour de tels services. Ils sont soit trop complexes pour être utilisés par des services dédiés au grand public, soit inadaptés au contexte de partage de contenus.

Dans cette thèse nous présentons un système de mise en relation réseau entre équipements distants pour permettre l'échange de contenus multimédias, ceci en garantissant à la fois la sécurité, la confidentialité et la qualité de service. Étant donné que ces contenus sont gourmands en ressources réseaux, le système proposera une garantie de QoS de bout en bout pour les sessions établies. Il offrira également une sécurisation de la mise en relation et des échanges. Nous avons défini une architecture générique de notre système. Ensuite, nous avons proposé deux déclinaisons techniques, leur conception et leur implémentation, une première utilisant le Framework IMS (IP Multimédia Subsystem) et une deuxième adaptée au déploiement sur internet. Le système conçu constitue la brique réseau du service de partage de contenus à distance étudié dans le cadre du projet européen Feel@Home (« Full Extended Experience of living at Home »).

Mots clés : Architecture réseau d'accès à distance, partage de contenus à distance, sécurité, garantie de QoS, IMS, HTTP.

Title: Network architectures for multimedia content sharing with guaranteed quality of service

Abstract: The success of multimedia content sharing services on the Internet attests the users' interest to share their personal experiences through media files (photo, video, music). Current solutions are mainly based on web servers and suffer from a serious lack of security and privacy. Several research studies have been conducted to provide network remote access architectures for this service. They are either very complicated to use by services dedicated to the public, or inappropriate for the context of content sharing.

This thesis presents a set of architectures and systems for network session establishment between remote devices to exchange multimedia content, which guarantees security, confidentiality and QoS. As the multimedia contents can be greedy in network resources, the system will guaranteed an end to end QoS for session established. It will also secure the session establishment and content exchange. We have defined two generic architectures for such a system. Then we have proposed two technical realizations for these architectures, one using the Framework IMS (IP Multimedia Subsystem) and a second one adapted to the deployment on the Internet. Our system was integrated to the remote content sharing service studied in the european project Feel@Home ("Full Extended Experience of Living at Home").

Keywords: Network remote access architecture, remote sharing content, security, QoS management, IMS, HTTP.