REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE NATIONALE POLYTECHNIQUE

Département Electronique

Projet de fin d'études

Pour l'obtention du diplôme

D'Ingénieur d'Etat en Electronique

THÈME

Déploiement d´un service de téléphonie IP pour un campus universitaire

Etudié par :

NEMMOUCHI Saad

Proposé et dirigé par :

Mr. R.SADOUN

Juillet 2010

Ecole Nationale Polytechnique, 10, AV. Hassen Badi, El-Harrach, Algérie

Remerciements

Nous exprimons notre profonde gratitude, notre grand respect et notre sincère reconnaissance à notre promoteur monsieur R.SADOUN, chargé de cours à l'Ecole Nationale Polytechnique d'Alger pour avoir assumé la lourde responsabilité de nous encadrer, de nous avoir orienté et conseiller tout au long de ce travail ainsi pour la confiance qu'il nous a accordée .

Nous tenons à remercier Monsieur A.Belouchrani Professeur à l'Ecole Nationale Polytechnique d'Alger, d'avoir accepté de présider le jury.

Nos remerciements vont aussi à Monsieur L.Abdeloued Professeur à l'Ecole Nationale Polytechnique d'avoir bien voulu accepter d'examiner notre travail.

Nous remercions tous les enseignants de l'Ecole Nationale Polytechnique d'Alger, spécialement ceux des départements des Sciences Fondamentales et d'Electronique, pour leur apport en savoir.

Finalement, on remercie toute personne qui m'a soutenu de prés ou de loin tout au long de mon parcours pour la réalisation de ce travail.

Je dédie mon travail à ma Tante, ma grande mère et mon frère Salah qui m'ont soutenu sans relâche, dans toutes les circonstances, tout au long de mon parcours d'études.

Je dédie, aussi, ce travail à mes beaux frère, mes sœurs et à toute ma famille pour leur soutien.

Je dédie ce travail à tous mes amis pour leur soutien tout au long de mon parcours.

Enfin je dédie ce travail à ma chère et très spéciale promotion.

NEMMOUCHI Saad ``FOUZI''

ملـــــــــخص:

إن هذا العمل عبارة عن عرض لخدمة هاتف (إبي) في حرم جامعي. كما يمثل تطبيق لإنشاء و تهيئة موزع هاتف (إبي) في هذا الهدف, بدأنا في عملنا بعرض تطور الهاتف مع الزمن و أدخلنا تصورات هاتف (إبي), ثم عرضنا مختلف البروتوكولات و هندسة الشبكات الخاصة بهاتف (إبي), في النهاية قمنا بتهيئة شبكة هاتف (إبي) استيرسك على مستوى المدرسة الوطنية المتعددة التقنيات.

الكلمات المفتاحية: هاتف (إبي), البروتوكول SIP, البروتوكول H323, البروتوكول MGCP, إبي, استيرسك, IPBX, X-LITE, استيرسك ناو.

Résumé : Le travail présent porte sur le déploiement d´un service de téléphonie IP pour un campus universitaire. Il prend pour application l´installation et la configuration d´un serveur de téléphone IP. Dans ce but, nous avons commencé notre travail par l'exposition de l'évolution de la téléphonie au fil du temps, et une introduction des concepts de la téléphonie IP. Ensuite, nous avons exposé les différents protocoles et les architectures des réseaux dédiés à la téléphonie IP. Enfin nous avons configuré et déployé un serveur du téléphone IP « ASTERISK » au niveau de l´école nationale polytechnique.

Mot clés :

Téléphonie IP - protocole SIP - protocole H323 - protocole MGCP - IP -Asterisk – IPBX –AsteriskNOW-X-lite

Abstract: The present work focuses on the deployment of an IP telephony service for a university campus. It is for application installation and configuration of a server IP phone. To this end, we began our work by the exhibition of the evolution of telephony over time, and we introduce the concepts of IP telephony. Then, we exposed the various protocols and network architecture to dedicate IP telephony. Finally we have configured and deployed a server IP Phone "ASTERISK" at the National Polytechnic School.

Key words:

IP Telephony - SIP - H323 Protocol - MGCP - IP-Asterisk - IP PBX, AsteriskNOW-X-lite

Sommaire

Listes des figures :

Listes des figures

Liste des tableaux

Liste des tableaux :

Introduction

Introduction Générale

La Voix sur IP (en anglais, Voice over IP ou VoIP) est le nom d´une technologie de télécommunication vocale en pleine émergence qui transforme la téléphonie traditionnelle. Cette technologie marque un tournant dans le monde de la communication en permettant de transmettre la voix sur un réseau numérique et sur Internet.

C´est en 1996 que naquit la première version Voix sur IP, appelée H323. Depuis, la technologie Voix sur IP a progressé à mesure que les entreprises découvraient ses avantages pour accroître la productivité et l´efficacité de leurs réseaux.

L'objectif de la Voix sur IP est d'appliquer à la voix le même traitement que les autres types de données circulant sur Internet. Grâce au protocole IP, des paquets de données, constitués la voix numérisée, y sont transportés. En effet, à force de transférer des fichiers d´information en temps de plus en plus réel, les utilisateurs d´Internet en vinrent à transférer la voix, en temps suffisamment réel pour faire compétition au téléphone traditionnelle. Dans cette banalisation des données voix, deux contraintes majeures sont présentes : transmettre ces paquets dans le bon ordre et le faire dans un délai raisonnable.

La téléphonie IP est une technologie appelée à se généraliser au cours des prochaines années, auront un impact majeur sur la façon dont les gens communiquent, au bureau comme à la maison.

Ce rapport a notamment pour objectifs de fournir des renseignements permettant de mieux connaître cette nouvelle technologie, d´identifier ses atouts, ses inconvénients, et d´évaluer si elle constitue une voie d´avenir pour les centres de relations clientèles des grands organismes. Ce travail touche a résoudre la problématique de la réalisation d´un téléphone sur un réseau local au niveau de l'école nationale polytechnique.

Dans ce but, et pour arriver à répondre à cette problématique, le travail est organisé selon le plan suivant, une introduction ; dans le premier chapitre, des généralités sur la technologie de la téléphonie sur IP sont exposées. En deuxième chapitre, on expose les différents protocoles et les architectures des réseaux dédiés à la téléphonie IP. Le troisième chapitre renferme le test du programme utilisé pour la réalisation et le déploiement de la téléphonie IP au niveau du centre de calcul de l'école nationale polytechnique.

Chapitre I

I.1-Introduction

Dans ce chapitre, nous allons montrer l'évolution de la téléphonie au fil du temps,
Passant des réseaux à commutation de circuits aux réseaux à commutation de paquets, et on introduite les concepts de la téléphonie, ceci dans le but de comprendre son évolution spectaculaire au fil du temps jusqu'a sont intégration au réseau IP. La naissance de la première version voix sur IP appelée H323 en 1996, a abouti à de nombreuses évolutions ou de nouveaux standards ont vu le jour.

I.2- Problématiques de la Téléphone IP :

La téléphonie est un des moyens de communication préférés des êtres humains, et le nombre de terminaux téléphoniques vendus dans le monde ne cesse d'augmenter.

La figure I.1 illustre le nombre de terminaux pouvant servir de terminal téléphonique. On peut noter que le nombre des terminaux mobiles dépasse largement celui des terminaux fixes. On peut également noter que le nombre de terminaux fixes continue d'augmenter, nettement moins que celui des mobiles. La figure indique en outre le nombre de terminaux, fixes ou mobiles, intégrant des fonctions multimédias. Toutes ces courbes révèlent la croissance globale de la téléphonie.

La téléphonie a été une véritable poule aux œufs d'or pour les opérateurs, qui ont longtemps maintenu leurs tarifs à des niveaux assez élevés, alors même que leurs infrastructures étaient largement amorties.

Aujourd'hui, la position de ces opérateurs est rapidement menacée par l'arrivée massive de la téléphonie sur IP, dont la tarification tend vers la gratuité. En France, fin 2006, la téléphonie sur IP représente déjà près de 50 % du marché de la téléphonie. Aux environs de 2015, on estime que près de 100 % du transport de la parole s'effectuera par l'intermédiaire de paquets IP.

Nous donnerons au cours des sections qui suivent quelques indications sur les problématiques techniques de la téléphonie par paquets. Nous examinerons ensuite les premières grandes caractéristiques de cette technologie et terminerons en présentant les différents environnements de la téléphonie IP : grand public, opérateurs et entreprises. **[1]**

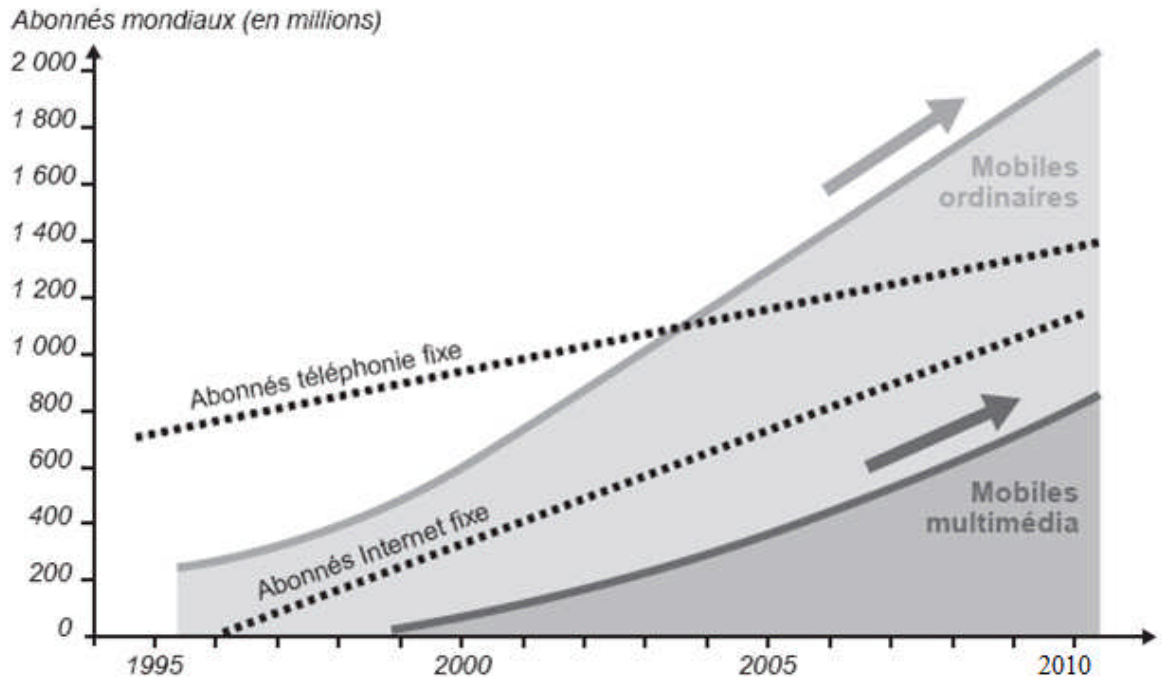


Figure I.1: Abonnés aux réseaux télécommunications (source UMTS Forum)

I.3- La téléphonie par circuit et par paquets

Dans la communication à transfert de paquets, toutes les informations à transporter sont découpées en paquets pour être acheminées d'une extrémité à une autre du réseau. Cette technique est illustrée à la figure I.2.

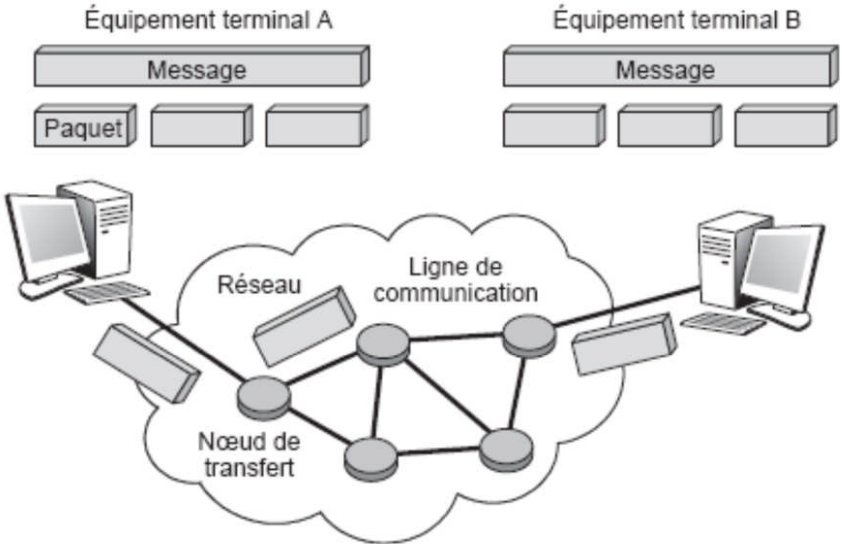


Figure I.2: La technique de transfert de paquets

L'équipement terminal A souhaite envoyer un message à B. Le message est découpé en trois paquets, qui sont émis de l'équipement terminal vers le premier nœud du réseau, lequel les envoie à un deuxième nœud, et ainsi de suite, jusqu'à ce qu'ils arrivent à l'équipement terminal B. Dans l'équipement terminal les paquets rassemblés reconstituent le message de départ.

Le paquet peut en fait provenir de différents médias. Sur la figure I.2, nous supposons que la source est un message composé de données, comme une page de texte préparée au moyen d'un traitement de texte. Le terme message est cependant beaucoup plus vaste et regroupe toutes les formes sous lesquelles l'information peut se présenter. Cela va d'une page Web à un flot de parole téléphonique représentant une conversation.

Dans la parole téléphonique, l'information est regroupée pour être placée dans un paquet, comme illustré à la figure I.3. Le combiné téléphonique produit des octets, provenant de la numérisation de la parole, c'est-à-dire le passage d'un signal analogique à un signal sous forme de 0 et de 1, qui remplissent petit à petit le paquet. Dès que celui-ci est plein, il est émis vers le destinataire. Une fois le paquet arrivé à la station terminale, le processus inverse s'effectue, restituant les éléments binaires régulièrement à partir du paquet pour reconstituer la parole téléphonique.

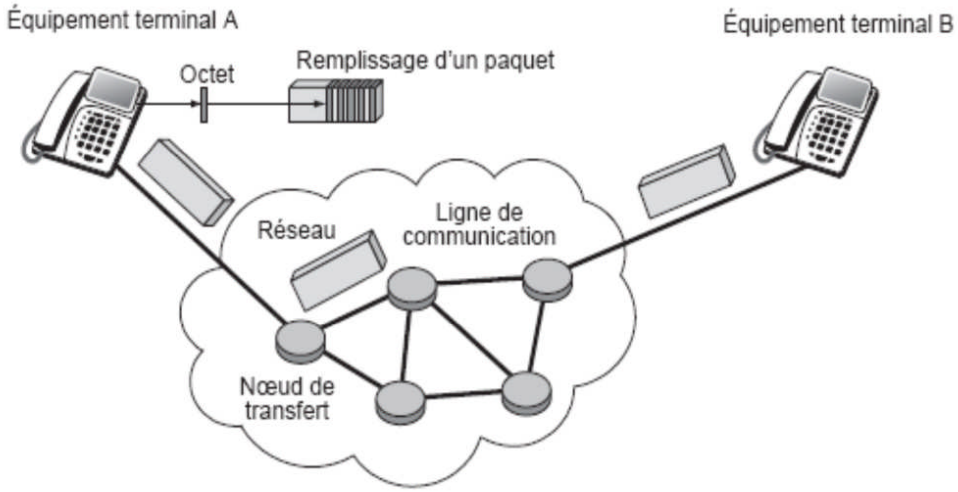


Figure I.3 : Un flot de paquets téléphoniques

Le réseau de transfert est lui-même composé de nœuds, appelés nœuds de transfert, reliés entre eux par des lignes de communication, sur lesquelles sont émis les éléments binaires constituant les paquets. Le travail d'un nœud de transfert consiste à recevoir des paquets et à déterminer vers quel nœud suivant ces derniers doivent être acheminés.

Le paquet forme donc l'entité de base, transférée de nœud en nœud jusqu'à atteindre le récepteur. Ce paquet est regroupé avec d'autres paquets pour reconstituer l'information transmise. L'action consistant à remplir un paquet avec des éléments binaires en général regroupés par octet s'appelle la mise en paquet, ou encore la paquétisation, et l'action inverse, consistant à retrouver un flot d'octets à partir d'un paquet, la dépaquétisation.

L'architecture d'un réseau est définie principalement par la façon dont les paquets sont transmis d'une extrémité du réseau à une autre. De nombreuses variantes existent pour cela, comme celle consistant à faire passer les paquets toujours par la même route ou, au contraire, à les faire transiter par des routes distinctes de façon à minimiser les délais de traversée.

Pour identifier correctement toutes les composantes nécessaires à la bonne marche d'un réseau à transfert de paquets, un modèle de référence a été mis au point. Ce modèle définit une partition de l'architecture en sept niveaux, prenant en charge l'ensemble des fonctions nécessaires au transport et à la gestion des paquets. Ces sept couches de protocoles ne sont pas toutes indispensables, notamment aux réseaux sans visée généraliste. Chaque niveau, ou couche, offre un service au niveau supérieur et utilise les services du niveau inférieur.

Pour offrir ces services, les couches disposent de protocoles qui appliquent les algorithmes nécessaires à la bonne marche des opérations, comme l'illustre la figure I.4.

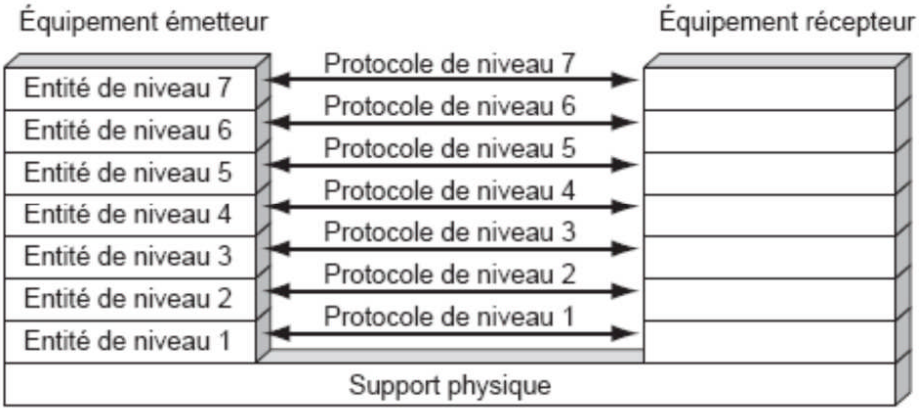


Figure I.4 : Architecture protocolaire d'un réseau à sept niveaux

Nous supposons ici que l'architecture protocolaire est découpée en sept niveaux, ce qui est le cas du modèle de référence. Nous ne décrirons que succinctement les couches basses qui nous intéressent.

Le niveau 3 représente le niveau paquet : il définit les algorithmes nécessaires pour que les entités de niveau 3, les paquets, soient acheminées correctement de l'émetteur au récepteur. Le niveau 7 correspond au niveau application. Le rôle du protocole de niveau 7 est de transporter correctement l'entité de niveau 7, le message utilisateur, de l'équipement émetteur à l'équipement récepteur.

Le niveau 2, ou niveau trame, permet de transférer le paquet sur une ligne physique. En effet, un paquet ne contenant pas de délimiteur, le récepteur ne peut en déterminer la fin ni identifier le commencement du paquet suivant. Pour transporter un paquet, il faut donc le mettre dans une trame, qui, elle, comporte des délimiteurs. On peut aussi encapsuler un paquet dans un autre paquet, lui-même encapsulé dans une trame.

Il est important de distinguer les mots paquet et trame de façon à bien différencier les entités qui ne sont pas transportables directement, comme le paquet IP, et les entités transportables directement par la couche physique, comme les trames Ethernet ou ATM.

Dans la téléphonie sur IP, une suite d'octets de téléphonie est encapsulée dans un paquet IP de niveau 3, lui-même encapsulé dans une trame véhiculée sur le support physique.

Cependant, comme la téléphonie est une application temps réel, les paquets ne peuvent attendre trop longtemps dans le réseau. Il faut donc introduire des contrôles afin de permettre une traversée rapide du réseau. **[2]**

I.4- La problématique de base de la téléphonie

La voix sur IP adresse deux types d'applications : celles qui, comme la téléphonie, mettent en jeu une interaction humaine, laquelle implique un temps de transit très court, et celles qui transportent des paroles unidirectionnelles, qui n'exigent pas de temps réel. Cette dernière catégorie rassemble essentiellement des transferts de fichiers contenant de la parole. Dans ce PFE, nous nous intéressons uniquement à la parole téléphonique.

La téléphonie transportée par paquets, et plus particulièrement par paquet IP, permet d'intégrer dans un même réseau les services de données et la téléphonie. Les entreprises sont de plus en plus nombreuses à intégrer leur environnement téléphonique dans leur réseau à transfert de paquets. Les avantages de cette intégration sont, bien sûr, la baisse des frais de

communication, mais aussi la simplification de la maintenance de leurs réseaux, qui passent de deux (téléphonie et données) à un seul (données).

La difficulté de la téléphonie par paquets réside dans la très forte contrainte temporelle due à l'interaction entre individus. Le temps de latence doit être inférieur à 300 ms si l'on veut garder une interaction humaine acceptable. Si l'on souhaite une bonne qualité de la conversation, la latence ne doit pas dépasser 150 ms.

Un cas encore plus complexe se produit lorsqu'il y a un écho, c'est-à-dire un signal qui revient dans l'oreille de l'émetteur. L'écho se produit lorsque le signal rencontre un obstacle, comme l'arrivée sur le combiné téléphonique. L'écho qui repart en sens inverse est numérisé par un codec (codeur-décodeur) et traverse sans problème un réseau numérique. La valeur normalisée de la latence de l'écho étant de 56 ms, pour que l'écho ne soit pas gênant à l'oreille, il faut que le temps allé ne dépasse pas 28 ms, en supposant un réseau symétrique prenant le même temps de transit à l'aller qu'au retour. Il faut donc que, dans les équipements terminaux, les logiciels extrémité soient capables de gérer les retards et de resynchroniser les octets qui arrivent. Les équipements modernes, comme les terminaux GSM, possèdent des suppresseurs d'écho évitant cette contrainte temporelle forte.

Une autre caractéristique essentielle de la téléphonie provient du besoin d'avertir par une sonnerie la personne qui est appelée. La communication téléphonique est pour cela décomposée en deux phases : une première permettant d'avertir le destinataire, et une seconde correspondant au transport de la parole proprement dite. Il existe en réalité une troisième phase, qui consiste en la finalisation de la communication lorsqu'un des deux terminaux raccroche. Cette phase utilise le même type de protocole que la première : un protocole de signalisation.

I.5- Comparaison avec la téléphonie classique

La téléphonie classique, dite par circuit, présente les mêmes contraintes temporelles que la téléphonie par paquet. Le temps de transit doit être limité pour satisfaire le besoin d'interactivité entre individus.

La limitation du temps de transit entre l'émetteur et le récepteur est relativement simple à réaliser dans une technologie circuit. Les ressources étant réservées, la voie est toujours dégagée sur le circuit, et les ressources appartiennent uniquement aux signaux qui transitent entre l'émetteur et le récepteur. En revanche, dans un transfert de paquets, aucune ressource

n'est réservée, et il est impossible de savoir quel sera le temps d'attente des paquets dans les nœuds de transfert.

Dans la première génération de téléphonie, les signaux étaient analogiques. Ils parcouraient le circuit sous la même forme que le son sortant de la bouche et n'utilisaient que 3 200 Hz de bande passante. Ils sont ensuite devenus numériques.

Dans la téléphonie traditionnelle numérique, le signal analogique est numérisé grâce à un codeur-décodeur, appelé codec. Le codec transforme le signal analogique en une suite de 0 et de 1. Le temps de transit est du même ordre de grandeur que le transfert du signal analogique, car le signal ne s'arrête nulle part. La seule perte de temps pourrait provenir du codec, mais ces équipements très rapides ne modifient pas fondamentalement le temps de transit. En revanche, dans un réseau à transfert de paquets, de nombreux obstacles se dressent tout au long du cheminement des informations binaires.

L'élément le plus contraignant de l'application de téléphonie par paquet reste le délai pour aller d'une extrémité à l'autre, puisqu'il faut traverser les deux terminaux, émetteur et récepteur, de type PC par exemple, ainsi que les modems, les réseaux d'accès, les passerelles, les routeurs, etc.

On peut considérer que le temps de traversée d'un PC et de son codec demande quelques millisecondes, la paquétisation de 5 à 16 millisecondes, la traversée d'un modem quelques millisecondes également, celui d'un routeur ou d'une passerelle de l'ordre de la milliseconde (s'il n'y a aucun paquet en attente) et celui d'un réseau IP quelques dizaines de millisecondes.

L'addition de ces temps montre que la limite maximale de 300 ms permettant l'interactivité est rapidement atteinte. La figure I.5 illustre ce processus.

Le déroulement d'une communication téléphonique sur IP parcourt les cinq grandes étapes suivantes :

I.5.1- Mise en place la communication.

Une signalisation démarre la session. Le premier élément à considérer est la localisation du récepteur *(*User Location*)*. Elle s'effectue par une conversion de l'adresse du destinataire (adresse IP ou adresse téléphonique classique) en une adresse IP d'une machine qui puisse joindre le destinataire (qui peut être le destinataire lui-même). Le récepteur peut être un combiné téléphonique classique sur un réseau d'opérateur télécoms ou une station de travail (lorsque la communication s'effectue d'un combiné téléphonique vers un PC). Le

protocole DHCP (Dynamics Host Configuration Protocol) et les passerelles spécialisées *(*gatekeeper*)* sont employés à cette fin.

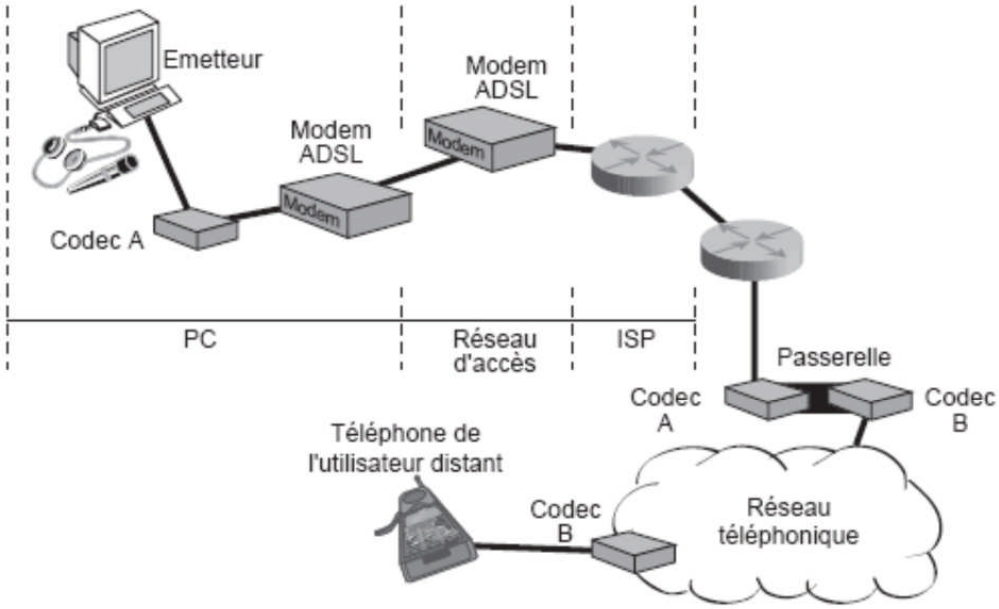


Figure I .5 : Équipements à traverser par une communication téléphonique sur IP

I.5.2- Établissement de la communication

Cela passe par une acceptation du terminal destinataire, que ce dernier soit un téléphone, une boîte vocale ou un serveur Web. Plusieurs protocoles de signalisation sont utilisés pour cela, en particulier le protocole SIP (Session Initiation Protocol) de l'IETF. Comme son nom l'indique, SIP est utilisé pour initialiser la session. Une requête SIP contient un ensemble d'en-têtes, qui décrivent l'appel, suivis du corps du message, qui contient la description de la demande de session. SIP est un protocole client-serveur, qui utilise la syntaxe et la sémantique de HTTP. Le serveur gère la demande et fournit une réponse au client.

Trois types de serveurs gèrent différents éléments : un serveur d'enregistrement (Registration Server), un serveur relais (Proxy Server) et un serveur de redirection (Redirect Server). Ces serveurs travaillent à trouver la route : le serveur proxy détermine le prochain serveur (Next-Hop Server), qui, à son tour, trouve le suivant, et ainsi de suite. Des champs supplémentaires de l'en-tête gèrent des options, comme le transfert d'appel ou la gestion des conférences téléphoniques.

I.5.3 - Transport de l'information téléphonique

Le protocole RTP (Real-time Transport Protocol) prend le relais pour transporter l'information téléphonique proprement dite. Son rôle est d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie de façon à reformer le flot avec ses caractéristiques de départ (vérification du synchronisme, des pertes, etc.). C'est un protocole de niveau transport, qui essaye de corriger les défauts apportés par le réseau.

I.5.4 - Changement de réseau

Un autre lieu de transit important de la Téléphone IP est constitué par les passerelles, qui permettent de passer d'un réseau à transfert de paquets à un réseau à commutation de circuits, en prenant en charge les problèmes d'adressage, de signalisation et de transcodage que cela pose. Ces passerelles ne cessent de se multiplier entre FAI et opérateurs télécoms.

I.5.5 - Arrivée au destinataire

De nouveau, le protocole SIP envoie une requête à la passerelle pour déterminer si elle est capable de réaliser la liaison circuit de façon à atteindre le destinataire. En théorie, chaque passerelle peut appeler n'importe quel numéro de téléphone. Cependant, pour réduire les coûts, mieux vaut choisir une passerelle locale, qui garantit que la partie du transport sur le réseau téléphonique classique est le moins cher possible.

Cet exemple classique illustre la relative complexité de la téléphonie sur IP. De nombreuses variantes existent, mais elles ne diffèrent que par les protocoles utilisés. À cette complexité s'ajoutent les problèmes liés à la traversée du réseau, qui doit garantir des temps de transit acceptables pour que l'application téléphonique puisse se dérouler dans de bonnes conditions. [3]

I.6- Les avantages de la TOIP

Et donc voici les principales motivations pour déployer la téléphonie sur IP (Source Sage Research 2003, sondage auprès de 100 décisionnaires IT). **[4]**

Motivations	**Pourcentage**
Réduction de coûts	75 %
Nécessité de standardiser l'équipement	66 %
Hausse de la productivité des employés dans une entreprise	65 %
Autres bénéfices de productivité	64 %
Hausse du volume d'appels à traiter	46 %

Tableau I.1 - Les motivations pour déployer un réseau téléphonie IP

I.7- Les solutions de Téléphone IP [5]

Le développement de la Téléphone IP a vu se succéder sur plusieurs années différentes générations de services et de configurations.

La première génération de téléphonie IP grand public a été proposée par des opérateurs alternatifs afin d'offrir des communications internationales à tarif local. Ce service consiste à rassembler un grand nombre de voies téléphoniques classiques sur le commutateur local et à les encapsuler dans un même paquet IP. Ce paquet IP peut devenir assez important suivant le nombre de voix multiplexées et le nombre d'octets de chaque voix.

L'utilisateur se connecte en local sur le commutateur de l'opérateur historique. L'opérateur alternatif récupère les différentes voix et les multiplexes sur Internet ou sur une même liaison IP, transatlantique par exemple. À la sortie du réseau IP, les voies de parole retrouvent leur composition normale sur le commutateur local et sont envoyées de façon classique aux destinataires au travers de la boucle locale de l'opérateur de télécommunications.

Si la téléphonie locale est gratuite, comme aux États-Unis, le coût total est approximativement égal à la tarification locale de départ. Les opérateurs de téléphonie classique suivent plus ou moins les mêmes principes, tout en tentant de préserver une marge bénéficiaire importante. D'où une chute des prix beaucoup plus lente.

Cette solution est illustrée à la figure I.6

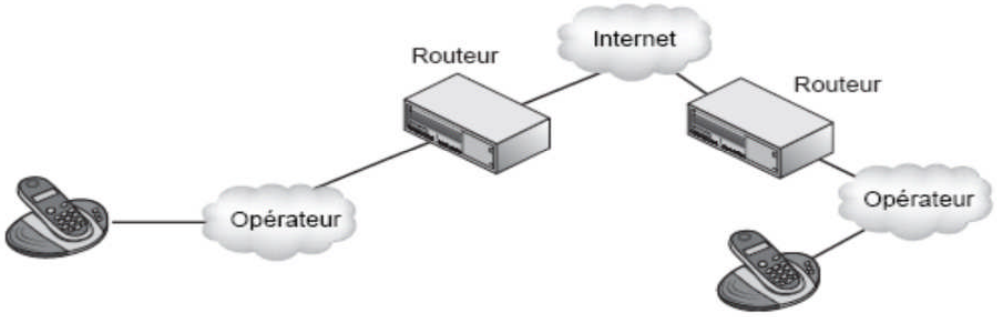


Figure I. 6 : La première génération de téléphonie sur IP

La deuxième génération a vu les opérateurs de télécommunications offrir des accès Internet au travers de la boucle locale via des modems standards permettant des débits de l'ordre de 50 Kbit/s.

Sur cet accès Internet peuvent être raccordés des ordinateurs personnels. Si l'ordinateur est équipé d'un micro et d'un haut-parleur, il est possible d'utiliser l'ordinateur personnel comme téléphone et de faire transiter les paquets de téléphonie sur Internet après les avoir acheminés sur la boucle locale de l'opérateur. Cette amélioration est illustrée à la figure I.7.

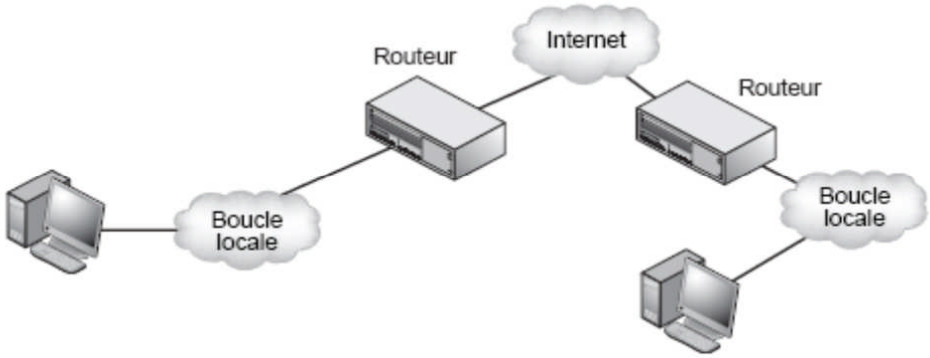


Figure I.7 : La téléphonie au travers de l'ordinateur personnel

Dans la troisième génération, au lieu d'utiliser l'ordinateur comme téléphone, un combiné analogique est connecté au PC, équipé d'une carte d'acquisition de la parole téléphonique.

L'ordinateur personnel joue ici le rôle d'une passerelle, transformant le signal analogique du combiné en un flux d'octets de téléphonie numérisés par un codec intégré à l'ordinateur. Les octets sont envoyés par un modem vers le routeur de l'opérateur, auquel revient la charge de la paquétisation et de l'envoi des paquets IP.

Cette étape est illustrée à la figure I.8.

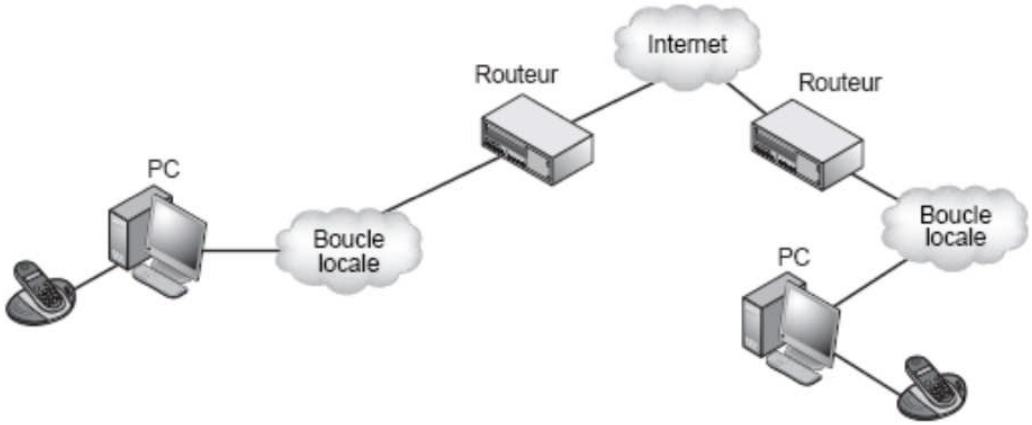


Figure I .8 : Téléphonie IP utilisant l'ordinateur personnel comme intermédiaire

La quatrième génération est caractérisée par l'arrivée de modems ADSL munis de plusieurs prises, chacune prenant en charge un média particulier et un protocole associé.

Le modem ADSL permet de connecter des téléphones standards. Les conversions nécessaires sont effectuées dans le modem, qui devient de ce fait une véritable InternetBox, le travail spécifique de la partie modem devenant mineur par rapport à l'ensemble des fonctionnalités réseau réalisées.

La boucle locale de l'opérateur transporte les paquets IP. Pour sa part, le téléphone demeure analogique.

Cette solution est illustrée à la figure I.9.

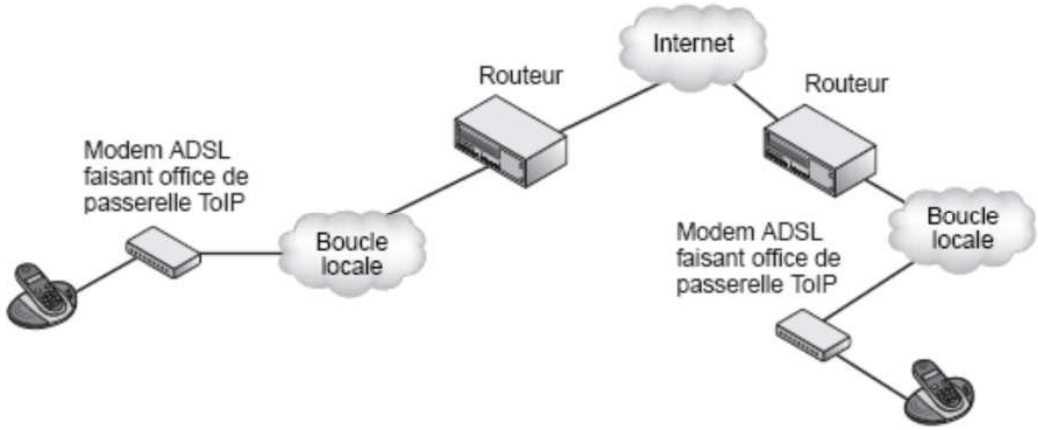


Figure I .9 : Apparition du modem ADSL dans la chaîne de transmission de la téléphonie

La cinquième génération du processus aboutit à de la téléphonie IP de bout en bout. La paquétisation est repoussée dans l'équipement terminal de l'utilisateur. Le téléphone devient un téléphone IP.

La figure I.10 illustre cette solution. Le téléphone IP n'est pas connecté directement sur la boucle locale de l'opérateur mais sur le réseau d'entreprise, lui-même connecté à l'opérateur. Le téléphone IP fait en réalité office de routeur. Il intègre en outre un codec et assure la paquétisation IP et l'encapsulation des paquets IP dans une trame Ethernet. La trame Ethernet est ensuite transmise sur le réseau d'entreprise.

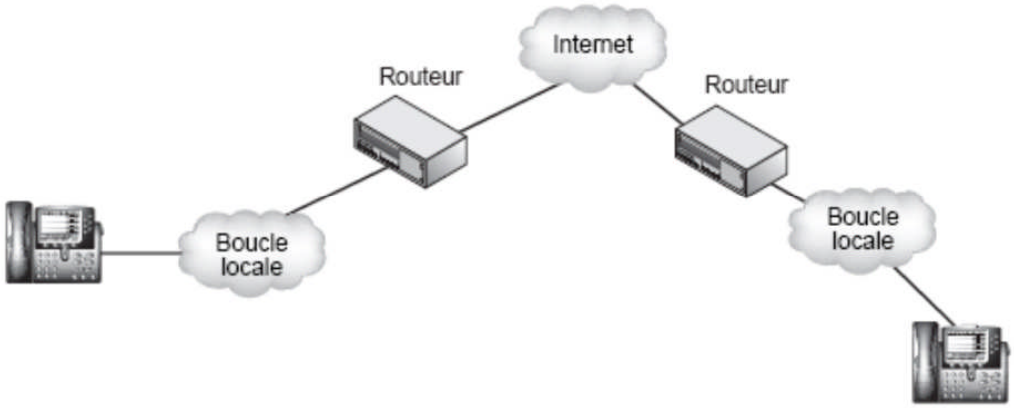


Figure I.10- La téléphonie IP de bout en bout

Avec l'arrivée massive d'ordinateurs personnels suffisamment puissants pour émuler un téléphone IP, la ToIP est devenue une téléphonie de bout en bout gratuite, puisque la téléphonie devient une application comme une autre transitant par l'intermédiaire du modem ADSL.

Du fait de cette configuration, de nouvelles applications ont fait leur apparition pour proposer des services grand public. Parmi celles-ci, Skype ou MSN (Microsoft Network) proposent de la téléphonie sur IP de bout en bout.

Il faut dans les deux cas disposer d'un modem ADSL aux deux extrémités de la communication afin que le débit soit acceptable sur la boucle locale. Skype fait appel à une technique P2P (Peer-to-Peer) à des fins de simplicité et pour ne pas avoir à implémenter un contrôle centralisé. La signalisation de MSN est gérée par une base de données centralisée mais qui peut être distribuée sur plusieurs sites.

Le modem ADSL joue le rôle de codec et de paquétiseur. Le téléphone est branché sur une prise spécifique reliée au codec. La télévision et les données ont leur propre prise spécifique.

En cas d'utilisation d'un logiciel de téléphonie sur l'ordinateur portable, le flux de téléphonie est multiplexé avec l'ensemble des données et n'est pas traité de façon spécifique. On appelle cette solution, le Double-Play lorsqu'il y a un canal de données et un canal téléphonique et Triple-Play lorsqu'un canal de télévision est ajouté *(*voir figure I.11*)*.

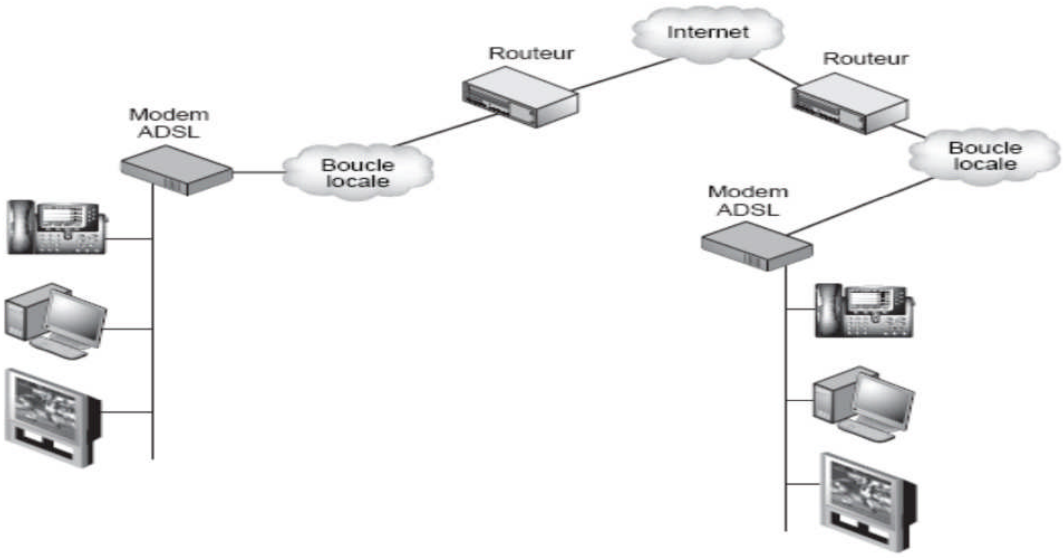


Figure I.11 : Le Triple-Play

Si l'on ajoute un canal supplémentaire, comme le canal de mobilité provenant d'un terminal mobile de type GSM/Wi-Fi, on parle de Quadruple-Play. Lorsque ce téléphone est situé près d'un modem incorporant un réseau Wi-Fi, le mobile se connecte en Wi-Fi. S'il n'est pas situé dans une zone Wi-Fi, le téléphone utilise le mode GSM. Il est possible de commencer à téléphoner en Wi-Fi et de continuer en GSM lorsqu'on sort de la zone Wi-Fi. En sens inverse, le téléphone peut éventuellement repasser en Wi-Fi.

Cette solution est illustrée à la figure I.12.

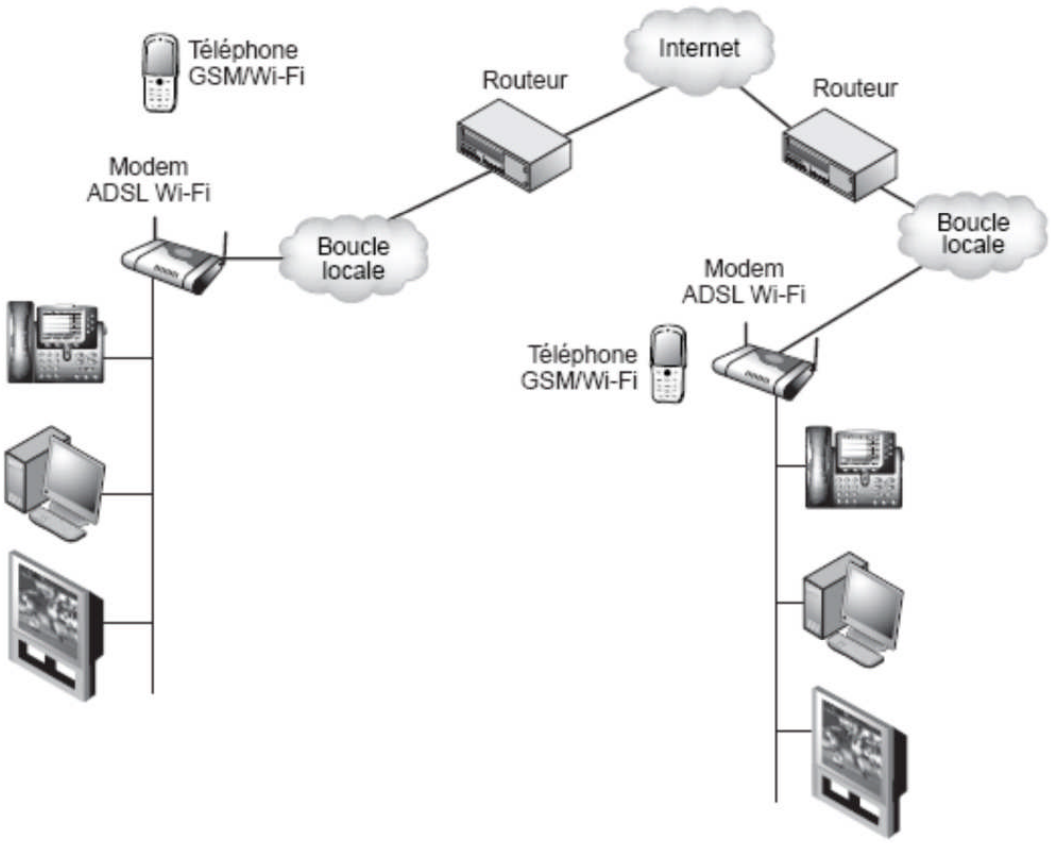


Figure I.12 : Le Quadruple-Play

La figure I.13 illustre la génération suivante, dite Penta-Play, dédiée à la vidéo mobile. Sur un mobile à écran vidéo, un utilisateur peut se connecter sur un réseau Wi-fi et regarder la télévision. La connexion avec le modem ADSL s'effectue en mode hertzien de type Wi-Fi.

Dans cette solution comme dans la précédente, le téléphone GSM/Wi-Fi peut se connecter à tous les modems de l'opérateur Internet auquel l'utilisateur a souscrit.

La téléphonie sur IP est encore peu présente dans le monde de la communication mobile, mais elle devrait se généraliser dès que les accès Internet lui seront ouverts, ce que les opérateurs interdisent aujourd'hui. Ce déploiement s'effectuera par l'intermédiaire de l'Internet hertzien, mais prendra son essor véritable avec l'arrivée des produits Wi Max.

Pour le moment, les réseaux de mobiles peuvent transporter des paquets IP, qui ne sont jamais qu'un ensemble d'éléments binaires au même titre que toutes autres suites d'éléments binaires. Il est donc possible de mettre en place des applications de téléphonie sur un terminal mobile assez puissant. Le coût de la communication étant celui du transport des données, la téléphonie n'est plus qu'une application parmi les autres.

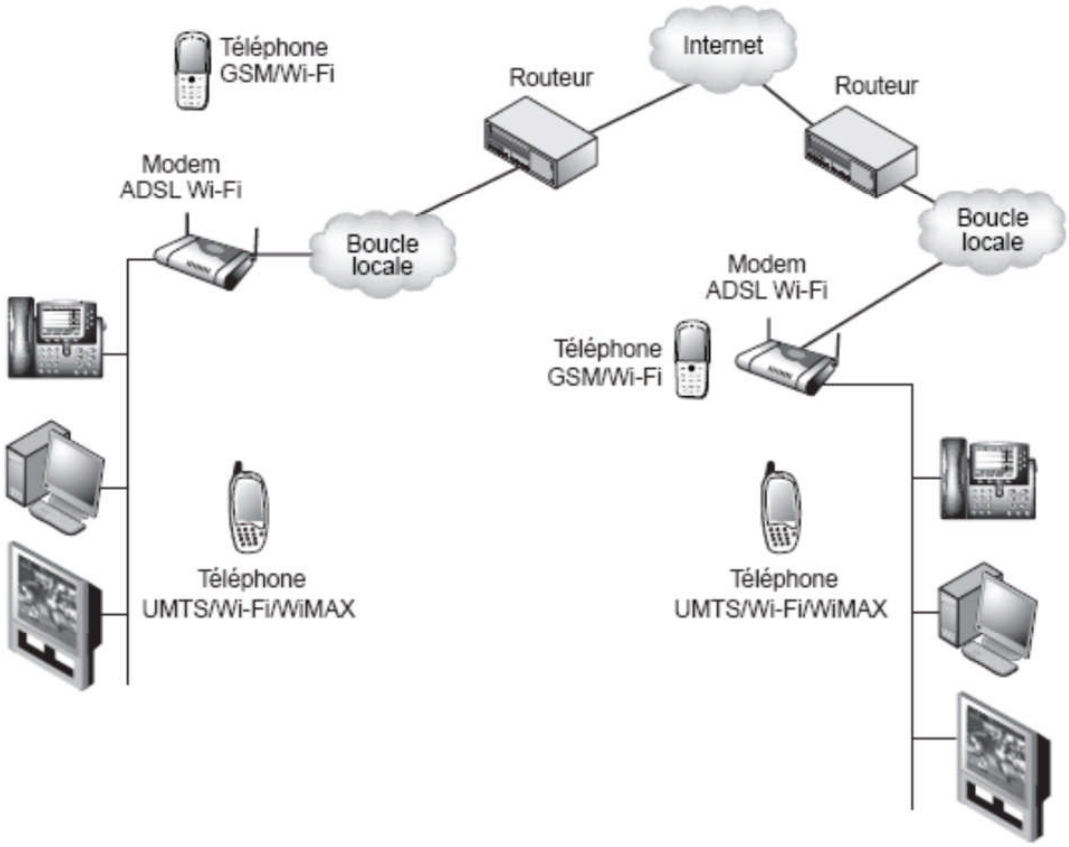


Figure I.13 : **Le Penta – Play**

I.8- Problématiques de la mise en place de la TOIP en entreprise :

Cinq questions principales se posent :

- **Sécurité.** Autrefois, les réseaux étaient fortement sécurisés grâce à la notion de circuit. En entrant dans le monde IP, la téléphonie rencontre un monde encore mal sécurisé, qui connaît des problèmes d'authentification, de confidentialité et d'intégrité.
- **Disponibilité.** Autrefois, les réseaux avaient une disponibilité dite à cinq « neuf », signifiant qu'ils fonctionnaient 99,999 % du temps. Les meilleurs réseaux des opérateurs IP n'ont généralement qu'une disponibilité à trois « neuf » (99,9 % du temps). De nombreux autres réseaux IP ne sont disponibles qu'à 99 % du temps.
- **Gestion.** Les trois réseaux de la génération précédente (données, parole, vidéo) possédaient trois systèmes de gestion relativement simples. Avec l'intégration, il n'y a plus qu'un seul système de gestion, de ce fait assez complexe.

- **Contrôle.** Autrefois les réseaux étaient contrôlés par des algorithmes assez simples. L'intégration des différents flux dans le même réseau complexifie énormément le contrôle de l'ensemble.
- **Qualité de service.** La qualité de service étant liée à l'infrastructure, la nouvelle génération de réseaux doit être capable de prendre en charge les qualités de service de chaque application transitant sur le même réseau, ce qui n'est pas facile. **[6]**

I.9 - Les contraintes du téléphone IP

Une communication téléphonique est une application de temps très réel donc qui impose des contraintes au réseau que n'imposent pas les applications traditionnelles telles que FTP, Web et même telnet. La littérature sur le sujet convergze vers les contraintes suivantes :

- Délai de transmission (temps de latence) : il faut que le temps de transport des données entre l'émetteur et le récepteur soit faible. Un retard est supportable jusqu'à 300 ms, il devrait être inférieur à 150 ms pour une bonne interactivité. Ce retard est engendré principalement par les routeurs traversés (dépend de la charge du réseau) mais aussi par le traitement des éléments logiciels (lors des compressions, codages…) dans les équipements d'extrémité.
- Bande passante : sans compression, la voix nécessite 64 Kbps de bande passante, avec compression on peut descendre jusqu'à 5 Kbps. Dans ce dernier cas la qualité du son est moins bonne et le temps de traitement pour la compression et la décompression au départ et à l'arrivée augmente ainsi le temps de latence.
- La perte de paquets : la voix supporte bien les pertes de paquets par rapport à d'autres applications. On considère que le taux de pertes doit être inférieur à 20 %. A noter que la retransmission des paquets erronés ou perdus est inutile car elle induirait un temps de latence trop important.
- La gigue : c'est une variation du délai de transmission de l'information. Elle provient de la variation de la charge du réseau (si la taille des files d'attente dans les routeurs augmente le temps de latence augmente et inversement), éventuellement des routes différentes utilisées (IP est un mode sans connexion où un flot de datagrammes peut emprunter des chemins différents lors d'un même appel téléphonique). Cette gigue ne doit pas être trop importante. On peut diminuer celle-ci en ajoutant des mémoires tampons dans le chemin, mais cela peut engendrer une augmentation du temps de latence.
- L'écho : sur le chemin, différents équipements peuvent induire des phénomènes d'écho. Les

passerelles H323 par exemple assurent la transmission du signal entre un réseau 4 fils (Ethernet) en un réseau 2 fils (téléphone analogique) ce qui provoque des phénomènes électroniques d'écho. Il faut que les équipements aient des fonctions d'annulation d'écho.

Le réseau RTC bâti autour du mode connecté où on réserve une bande passante de 64 Kbps à chaque communication téléphonique, avec des commutateurs téléphoniques construits pour la voix, suit depuis de nombreuses années ces contraintes. Les équipements d'extrémités (téléphones) sont aussi adaptés aux caractéristiques de ce réseau. Mais dans notre problématique, pour prendre en compte toutes ces contraintes il faut que :

- Les logiciels et les équipements d'extrémités soient performants : induisent peu de temps de latence, ne créent pas d'écho…
- Le réseau IP traversé de bout en bout ait des qualités de services : peu de temps de latence, assez de bande passante, peu de gigue… Si sur un réseau local GigaEthernet peu chargé on peut s'attendre à avoir ces qualités sans trop de problème, par contre sur les réseaux WAN et MAN il sera nécessaire d'avoir des mécanismes de qualités de services IP (IntServ, Diffserv) implémentés sur tout le chemin.

I.10 - Conclusion

La téléphonie reste une des applications dominantes du monde des réseaux, et ce pour encore de nombreuses années, en raison notamment de l'émergence de nouveaux et immenses marchés, comme celui de la Chine. L'application de téléphonie ne représente plus mi-2008 que 30 % en moyenne du chiffre d'affaires des opérateurs, tout en n'occupant que 4 % du débit total des communications.

À cette même date (mi-2008), la ToIP mobilise près de 65 % des débits téléphoniques dits terrestres (excluant les mobiles). Le passage vers le tout-IP téléphonique, permettant d'intégrer les services de données et la téléphonie dans un même réseau.

Cependant, la qualité est très variable en fonction des efforts effectués par les gestionnaires de réseaux d'entreprise et les opérateurs de réseaux de télécommunications. Les problèmes à résoudre sont nombreux et parfois complexes. La ToIP n'est pas une application simple à mettre en œuvre dans le contexte de l'intégration de tous les services de télécommunications sur le même réseau. **[6]**

La figure 1.14 illustre la place que tiendra la ToIP dans les années à venir.

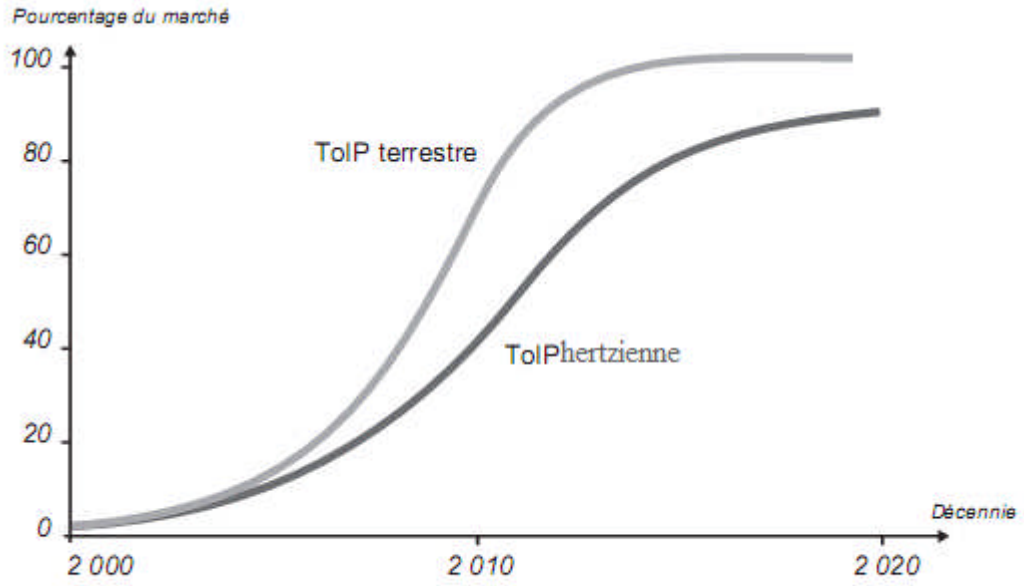


Figure I.14 : Évolution de la ToIP sur vingt ans

En 2010, pratiquement tout le marché de la téléphonie terrestre sera passé en IP. Si l'on considère la téléphonie hertzienne, sa montée en puissance sera beaucoup plus longue. Avec l'UMTS et ses successeurs, le monde de la téléphonie hertzienne suit les traces du GSM, qui n'est pas une solution IP native. Il faudra donc attendre l'extension massive des réseaux sans fil IP de types Wi-Fi, WiMax et autres WiMedia et WiRAN avant de rejoindre les courbes terrestres. Il est à noter que l'UMTS apporte une solution de téléphonie par paquet mais non-IP.

Chapitre II

II.1- Introduction

Dans ce chapitre on expose les différents protocoles et les architectures des réseaux dédiés à la téléphonie IP. Cette évolution spectaculaire s'est faite avec la naissance de plusieurs protocoles, nous allons donner leurs architectures, leurs spécificités, et les services qu'ils offrent. Nous citerons les plus utilisés comme le H .323, SIP, IAX et le MGCP.

II.1.1 – IAX (protocole Inter-Asterisk eXchange)

Un test de connaissance en matière d´Asterisk (qui sera traité dans le 3ème chapitre) consiste à prononcer le nom de ce protocole.les nouveaux disent << hey-hey-ex>>, ceux qui savent disent <<iiks>>.IAX est un protocole ouvert, qui signifie que n´importe qui peut télécharger et développer mais ce n´est pas encore un standard.

Dans Asterisk, IAX est supporté par le module chan_iax.so

II.1.2 – H.323

Le protocole de l´Union Internationale des Télécommunication (UIT) a été conçu à l´origine pour fournir un mécanisme de transport IP pour la vidéoconférence.il est devenu standard dans les équipements de vidéoconférence bases sur IP et il a aussi connu brièvement la gloire comme protocole VoIP. Bien que le débat pour déterminer quel protocole détermine le monde de VoIP entre SIP, H.323 et IAX soit mouvementé, dans Asterisk (qui sera traité dans le 3ème chapitre), H.323 est devenu obsolète en faveur d´IAX et de SIP. H .323 n´a pas eu beaucoup de succès parmi les utilisateurs et les entreprises bien qu´il le protocole le plus utilisé chez les opérateurs.

Le protocole H323 est une norme stabilisée avec de très nombreux produits sur le marché (terminaux, gatekeeper, Gateway, logiciels). Il existe actuellement 5 versions du protocole (V1 à V5).

II.1.3 – MGCP

MGCP (Media Gateway Control Protocol) nous vient aussi de l´IETF. Bien que le déploiement de MGCP soit plus important que ce que l´on pourrait croire, il perd rapidement du terrain devant des protocoles comme SIP et IAX. Mais Asterisk supporte les protocoles de manière rudimentaire.

MGCP est défini dans la RFC 3435. Il a été conçu pour rendre le terminal (tel qu'un téléphone) aussi simple que possible et fait en sorte que toute la logique et le traitement de l'appel soient gérés par des passerelles média et des agents d'appel. À la différence de SIP, MGCP utilise un modèle centralisé. Les téléphones MGCP ne peuvent pas appeler directement un autre téléphone MGCP. Ils doivent toujours passer par une sorte de contrôleur.

Asterisk supporte MGCP à l'aide du module *chanjngcp.so* et les terminaux sont définis dans le fichier de configuration *mgcp.conf*. Puisqu'Asterisk ne fournit que des services d'agent d'appel basiques, il ne peut pas émuler un téléphone MGCP (pour s'enregistrer sur un autre contrôleur MGCP en tant qu'agent utilisateur par exemple).

Si vous avez quelques téléphones MGCP , vous serez capable de les utiliser avec Asterisk. Si vous prévoyez de mettre des téléphones MGCP en production sur un système Asterisk, gardez à l'esprit que la communauté est passée à des protocoles plus populaires et que vous devrez prévoir les coûts du support logiciel en conséquence. Si possible (par exemple avec les téléphones Cisco), vous devriez passer vos téléphones MGCP à SIP.

II.1.4 – SIP

SIP (Session Initiation Protocol) a changé le monde de la VoIP. D'abord considéré tout au plus comme une idée intéressante, SIP semble maintenant pouvoir détrôner H.323 en tant que protocole VoIP de premier choix, et certainement aux terminaisons du réseau. Le principe de SIP est que chaque terminaison est un pair et le protocole négocie les capacités communes entre eux. Ce qui rend SIP irrésistible est sa relative simplicité avec une syntaxe similaire à celle de protocoles tels que HTTP et SMTP. SIP est supporté par Asterisk avec le module *chan_sip.so.* **[7]**

On va s´intéresser au protocole SIP.

II.2- Architecture d´un réseau dédie à la téléphonie sur IP

Il existe deux types d'architecture réseaux téléphoniques sur IP est qui représentées par :

II.2.1- Les architectures centralisées

Qui considère que l'intelligence et les fonctionnalités sont uniquement localisées au sein du réseau.Ainsi, les terminaux utilisateurs (téléphones analogiques, GSM, etc.) sont "Ignorants" et offrent peu ou pas de fonctionnalités propres. Par exemple, si un abonné désire Faire un transfert inconditionnel d'appels vers un autre poste, c'est au central téléphonique de

L'opérateur (ou le PABX privé) qu'incombe cette tâche. Dans ce mode de fonctionnement, il sera par exemple impossible pour l'abonné de savoir qui a tenté de le joindre sans faire appel à son opérateur.

Les caractéristiques d'une telle architecture sont les suivantes:

- L'intelligence est au sein du réseau.
- Les terminaux des utilisateurs sont relativement "ignorants".
- La gestion est centralisée.
- Peu de possibilités de fonctionnalités sur les terminaux utilisateurs.

Les relations au sein d'une architecture centralisée sont souvent qualifiées de "maître/esclave".

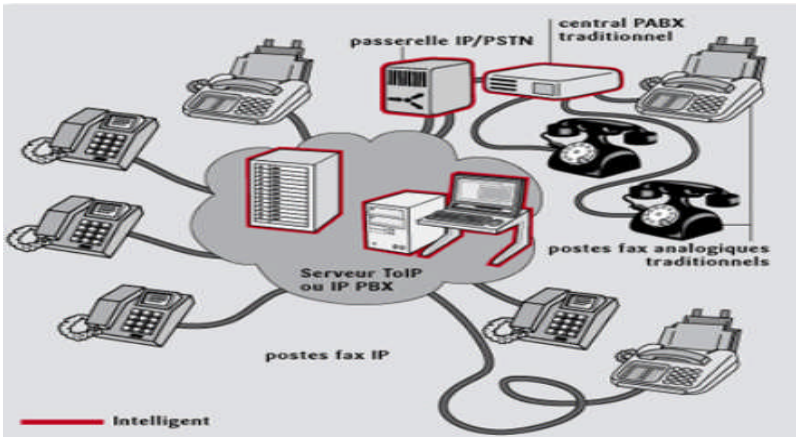


Figure II.1 : Architecture d'un réseau VOIP centralisée

Parmi les protocoles existants pour ce type d'architecture

- Media Gateway Control Protocol (MGCP): standard IETF (RFC3435) dont les fondements sont issus de propositions faites par Cisco et Telcordia. MGCP décrit une architecture de signalisation où l'intelligence nécessaire à l'établissement d'une communication réside à l'extérieur de la passerelle, au sein d'une entité appelée le "Call Agent".
- Skinny Client Control Protocol (SCCP): protocole propriétaire développé par CISCO. Ce protocole est utilisé pour le CISCO Call Manager et les téléphones IP. **[16]**

II.2.1.1- Le protocole MGCP

MGCP (Media Gateway Control Protocol), décrite par la RFC 3435, se différencie donc de SIP et H.323 par son architecture CLIENT / SERVEUR ou plus précisément maître /esclave. Ainsi la gestion des services d'appels est centralisée et assuré coté maitre tandis que les terminaux coté clients ne gèrent que les fonctionnalités basiques d'appels et vont recevoir les instructions du maitre.

Ce type de fonctionnement est très utile dans un environnement où l'opérateur désire garder le contrôle des services sur l'abonné (ce dernier a en effet qu'un poste capable de recevoir les instructions de l'opérateur).

II.2.1.2 - Architecture du protocole MGCP

L'architecture du protocole MGCP repose donc sur 2 entités :

• Les terminaux MGCP situés coté client sont des passerelles chargé de recevoir et rapporter les instructions du contrôleur central (call agent).

• Le Call agent est le « chef d'orchestre » du réseau MGCP, il va se charger de commander et fournir des instructions aux passerelles MGCP.

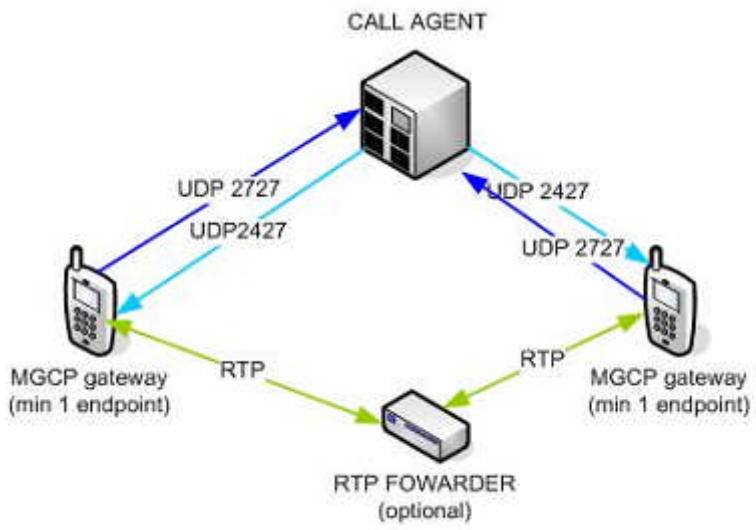


Figure II.2 - Aperçu connexion call agent et terminaux MGCP

II.2.1.3 - Méthode de connexion d'un terminal MGCP vers le call agent

MGCP est majoritairement utilisé pour le contrôle des passerelles, une passerelle est constituée d'un un ou plusieurs endpoints, qui établiront une connexion permanente avec le call agent. En général un poste simple est constitué de deux endpoints dédiés à la ligne du combiné et à l'affichage de l'écran LCD dans le cadre de la gestion des services via l'affichage. MGCP utilise une nomenclature simple pour désigner les endpoints ainsi par exemple pour une gateway possédant 3 endpoints (2 lignes+ affichage) nous aurons :

- aaln/1@nom-gateway
- aaln/2@nom-gateway
- disp/aaln/1@nom-gateway

Note : les endpoints d'affichages (display) sont obligatoirement liés à un endpoint de ligne.

Le nom de la gateway est l'identifiant fourni par le terminal qui permet au call agent contacté de valider si ce terminal fait parti de son réseau MGCP. Ce nom peut être l'adresse MAC du terminal, son adresse IP ou un nom DNS.

Le choix de l'adresse MAC se révèle être la plus simple à mettre en place dans un réseau relativement complexe (présence de NAT, IP dynamique, pas de serveur DNS dédié aux terminaux). L'adresse IP du terminal peut être utilisée si ce dernier possède une IP statique et directement atteignable par le call agent. Le Nom DNS se révèle utile lorsque le déploiement des terminaux se fait dans un réseau où tous les terminaux iront interroger le même serveur DNS, dans un environnement multi abonné (fournisseur DNS hétérogène), cette méthode d'authentification est évidemment impossible à mettre en place.

La déclaration d'un nouveau terminal se fait donc au niveau du call agent en précisant

- le nom de la gateway (MAC, IP, DNS)
- le nombre d'endpoints
- le nom de ces endpoints

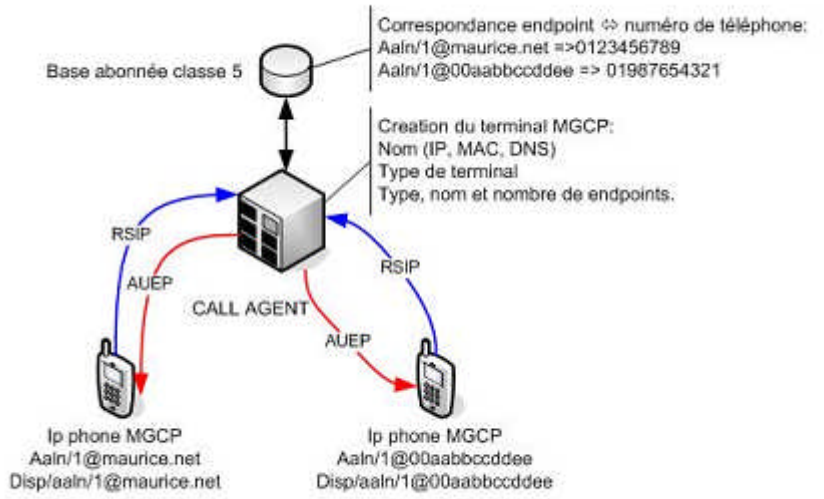


Figure II.3 - Méthode de connexion d'un terminal MGCP vers le call agent

Le terminal est connecté à un réseau IP, celui-ci va envoyer un message RSIP (restart in Progress) informant le call agent qu'il est disponible.

Ce message RSIP contient le nom de la gateway, ainsi que les endpoints présents sur le terminal. Le call agent est alors informé de la présence du terminal. Au fil du temps ce dernier va également s'assurer que le terminal est toujours actif en envoyant une requête à intervalle régulier dénommé AUEP (cette requête peut être comparée au proxy keep alive en SIP permettant de s'assurer que le terminal est toujours actif et également maintenant la session NAT valide.). Ainsi lorsque l'abonné décroche son terminal, l'endpoint de ligne associé va envoyer une commande NOTIFY contenant les informations sur l'événement (décroché du combiné, saisie de digit…).Le call agent va alors analyser la commande et envoyer au terminal une commande CREATE CONNEXION qui va créer une connexion sur le endpoint du terminal avec des paramètres comme l'identifiant de l'appel, le codec souhaité, les délais de paquetisation, la bande passante autorisée…).L'abonné compose son appel, les instructions sont envoyées au call agent qui va interroger la base de données et relayer l'appel soit sur l'endpoint de ligne associé à une abonnée MGCP faisant partie du même opérateur (présence de son endpoint dans la base abonnée) ou sur une gateway si l'appel est destiné à un abonné externe situé sur le PSTN qu'il soit TDM ou MGCP. Une fois l'appel terminée, le call agent envoie une commande DELETE CONNEXION, si le raccroché provient de l'appelé, ou le terminal envoie un NOTIFY si cela vient de l'appelant.

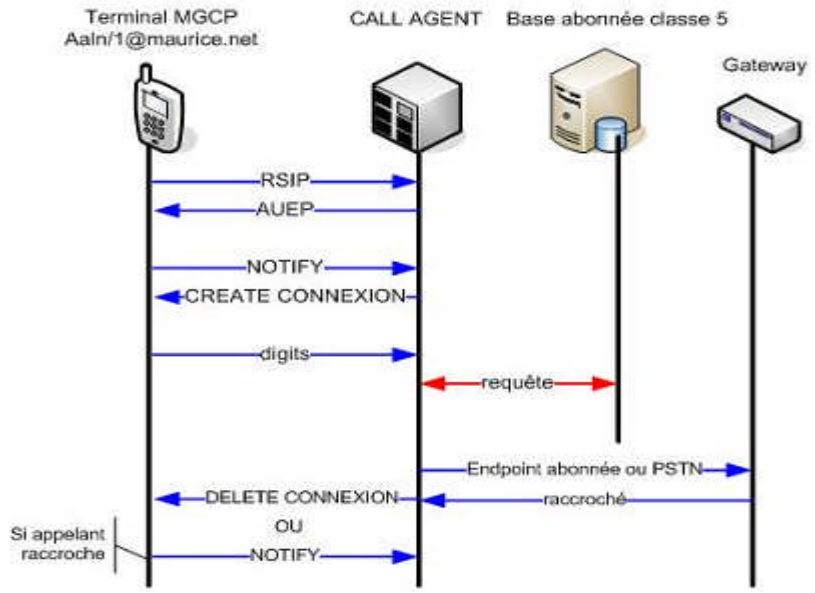


Figure II.4 : Les messages échangés entre le terminal et le call agent

Les services contrairement aux protocoles SIP ne sont pas directement gérés par le terminal mais plutôt par le call agent. **[17]**

II.2.2- Les architectures distribuées

Dans ce modèle, les architectures informatiques sont scindées en de multiples entités, afin de déléguer les tâches à accomplir aux systèmes les plus adaptés à leur réalisation, Dans un mode distribué, les terminaux utilisateurs offrent en outre de nombreuses fonctionnalités et services. Ainsi, si un abonné désire utiliser un service de rejet d'appels sélectif, il peut le faire directement via un terminal qui lui est associé, sans intervention d'une tierce partie.

Les caractéristiques d'une telle architecture sont:

- Intelligence distribuée entre les terminaux utilisateurs et les équipements de signalisation disponibles au sein du réseau,
- Les terminaux sont les téléphones IP, les PC ou les passerelles VoIP,
- Les systèmes sont flexibles et il est aisé d'ajouter un nouveau service,

Les relations au sein d'une architecture distribuée sont souvent qualifiées de "client/serveur".

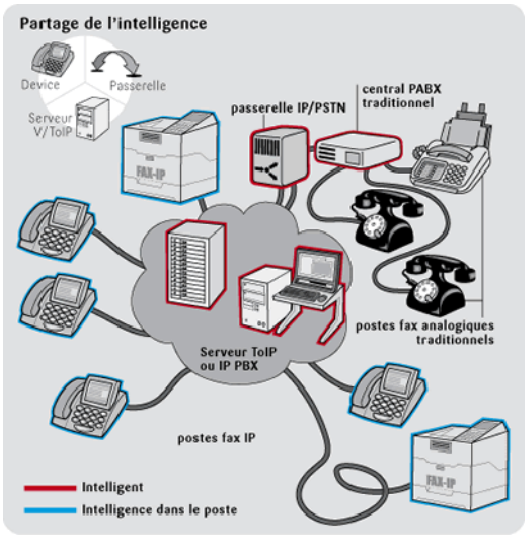


Figure. II.5 Architecture d'un réseau VOIP distribué

Les protocoles les plus présents sur le marché utilisant l'architecture distribué sont le H323 et le SIP

II.2.2.1- La standardisation SIP (Session Initiation Protocol) [8]

L'IETF s'intéresse à la téléphonie sur IP et travaille à la mise au point d'un protocole chargé de la gestion de sa signalisation depuis 1995.

En 1997, la première version de ce protocole, nommé SIP, est dévoilée au public. Entretemps, l'UIT lui avait volé la vedette avec H.323, sorti en 1996, qui avait bénéficié de la faveur des industriels et dont les implémentations logicielles, notamment NetMeeting de Microsoft, assuraient la célébrité.

Pendant plusieurs années, l'IETF n'a pas été un acteur visible dans le domaine de la ToIP. Plus le protocole tardait à voir le jour, plus l´handicap par rapport à son concurrent H.323 s'amplifiait. Si le protocole H.323 possède aujourd'hui la maturité que lui confèrent son avance et ses nombreuses expérimentations, sa gestion demeure laborieuse et reste peu adaptée au monde Internet. Or c'est à ce niveau qu'intervient SIP, dont la force principale vient de son extrême simplicité, même à grande échelle.

Le protocole SIP a été conçu pour s'adapter à Internet, en particulier pour que le réseau supporte des montées en charge du nombre d'utilisateurs. Pour cela, l'architecture SIP repose

sur plusieurs serveurs distincts, qui distribuent la charge du réseau en communiquant entre eux, un peu à la manière des serveurs DNS sur Internet. Lorsque le nombre d'utilisateurs croît, il suffit d'ajouter des serveurs disposant de fonctions dédiées pour collaborer avec ceux déjà en place.

Cette approche se révèle hautement évolutive et flexible puisque de nouvelles fonctionnalités peuvent à tout moment être déployées, sans avoir à modifier les composants existants.

II.2.2.1.1- Compatibilité [9]

L'un des grands atouts de SIP est sa capacité à s'intégrer à d'autres protocoles standards du monde IP. En tant que standard ouvert, il offre un service modulaire, prévu pour fonctionner avec différentes applications, telles que la téléphonie, la messagerie instantanée, la vidéoconférence, la réalité virtuelle ou même le jeu vidéo.

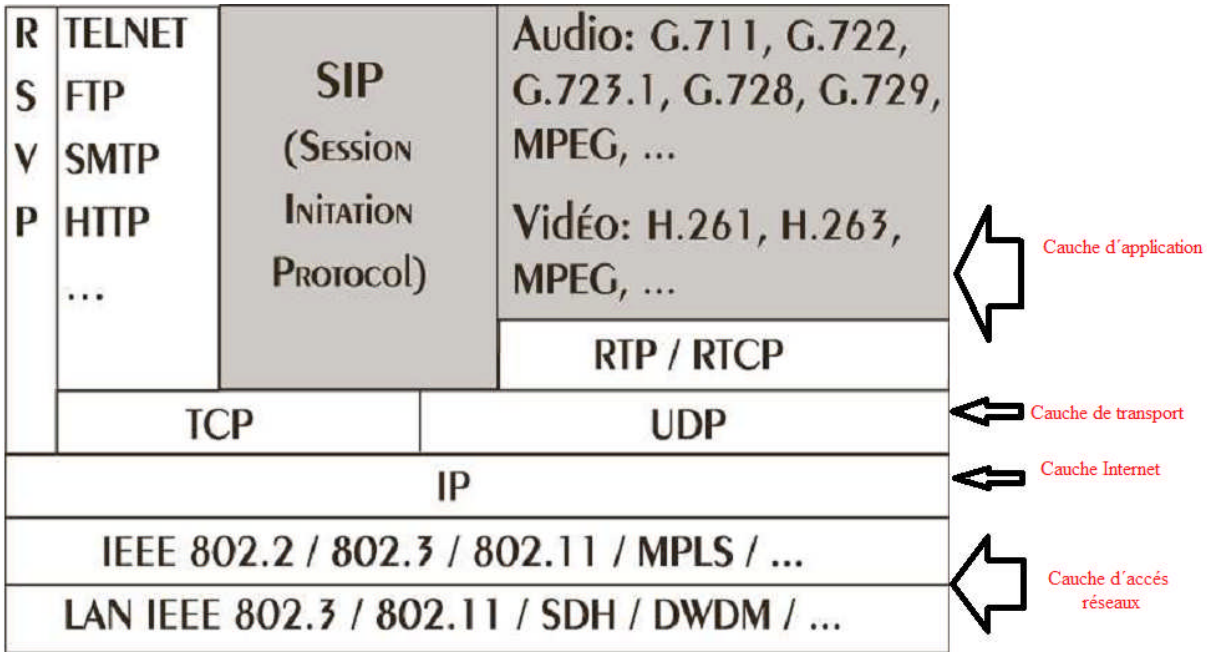


Figure II.6.A : la pile protocolaire SIP.

En fait, plus qu'une simple compatibilité, c'est la possibilité de l'utiliser en conjonction avec d'autres protocoles qui caractérise SIP. Le protocole s'insère comme une partie d'un ensemble plus générique, intitulé Internet Multimédia Conferencing Suite. À l'image de H.323, SIP est peu à peu devenu un protocole dit parapluie, qui encadre et rassemble plusieurs autres protocoles.

SIP peut notamment se déployer ou s'intégrer aux protocoles suivants :

- RTP (Real-time Transport Protocol), RFC 3550, qui se charge du transport des flux temps réel.

- RTCP (Real-time Transport Control Protocol), RFC 3550, qui fournit des informations dynamiques sur l'état du réseau.
- RTSP (Real-Time Streaming Protocol), RFC 2326, pour contrôler la diffusion de flux multimédias en temps réel.
- SDP (Session Description Protocol), RFC 2327, qui fournit la description d'une session, c'est-à-dire les paramètres utilisés dans une communication SIP
- SAP (Session Avertissement Protocol), RFC 2974, pour les communications multicast, qui permet d'ajouter les spécifications d'une nouvelle session.
- MIME (Multipurpose Internet Mail Extension), RFC 2045, standard pour les descriptions de contenus, utilisé sur Internet.
- RSVP (Resource reSerVation Protocol), RFC 2205, pour obtenir des garanties de qualité de service et effectuer des réservations de ressources.
- HTTP (HyperText Transfer Protocol), RFC 2616, pour le traitement des pages Web sur Internet (on peut inclure des adresses SIP directement dans des pages Web).
- MGCP (Media Gateway Control Protocol), RFC 3435, pour le contrôle des passerelles assurant la connectivité entre un réseau IP et un réseau téléphonique.

II.2.2.1.2-Modularité

Comme expliqué précédemment, le protocole SIP se veut modulaire. Son objectif est de constituer une brique de base pouvant se combiner avec le maximum d'autres protocoles. C'est la raison pour laquelle il a été conçu d'une manière indépendante de la couche de transport.

Les protocoles TCP et UDP sont donc tous deux supportés pour l'envoi de messages SIP. UDP est généralement préférable pour laisser à l'application le contrôle des retransmissions de messages, et donc l'enchaînement des messages. Pour sa part, TCP est préférable pour la traversée de pare-feu, dans la mesure où les ports utilisés avec SIP sont dynamiques et où la notion d'état de connexion n'existe pas avec UDP

Mais il ne s'agit là que de recommandations. Aucune règle n'est fixée, et même avec UDP, il existe des moyens de contourner le filtrage des pare-feu.

II.2.2.1.3- Architecture de SIP

Contrairement à H.323, largement fondé sur une architecture physique, le protocole SIP s'appuie sur une architecture purement logicielle.

L'architecture de SIP s'articule principalement autour des cinq entités suivantes :

- terminal utilisateur ;
- serveur d'enregistrement ;
- serveur de localisation ;
- serveur de redirection ;
- serveur proxy.

La figure (II.6.B) illustre de façon générique les communications entre ces éléments. Un seul terminal étant présent sur cette figure, aucune communication n'est possible. Nous nous intéressons en fait ici aux seuls échanges entre le terminal et les services que ce dernier est susceptible d'utiliser lors de ses communications.

On peut schématiquement observer qu'il existe deux catégories de services : l'un fourni au niveau de l'utilisateur (par le terminal), l'autre fourni au niveau des serveurs du réseau. Ces derniers sont répartis en deux classes : les serveurs de redirection et proxy, qui facilitent le routage des messages de signalisation et jouent le rôle d'intermédiaires, et les serveurs de localisation et d'enregistrement, qui ont pour fonction d'enregistrer ou de déterminer la localisation des abonnés du réseau.

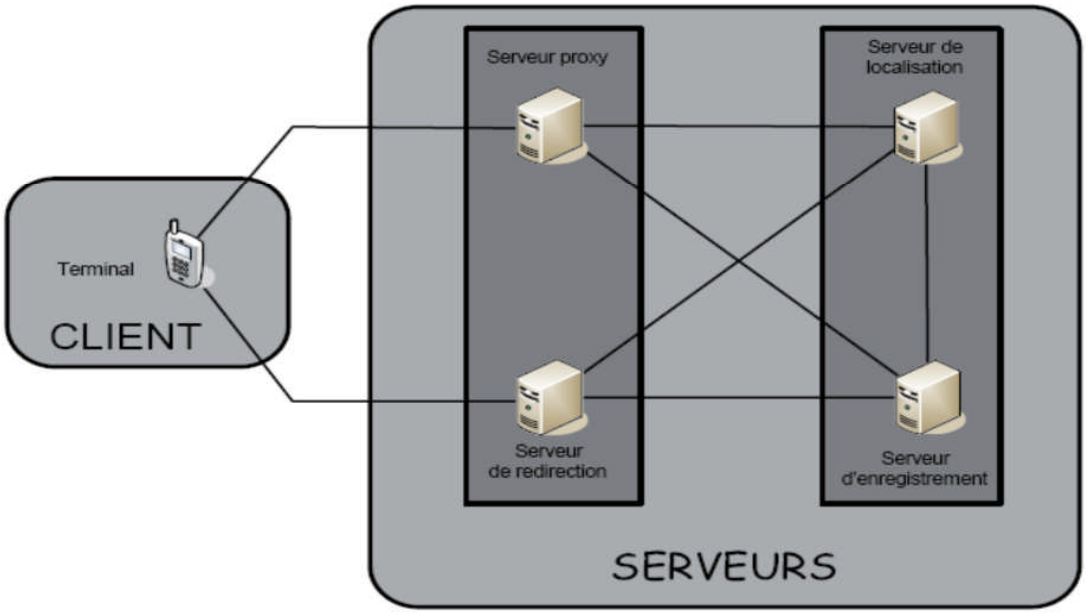


Figure II.6.B : Architecture de SIP

II.2.2.1.4- L'adressage SIP [10]

L'objectif de l'adressage est de localiser les utilisateurs dans un réseau. C'est une des étapes indispensables pour permettre à un utilisateur d'en joindre un autre.

Pour localiser les utilisateurs, il faut pouvoir les identifier de manière univoque. SIP propose des moyens très performants pour nommer les utilisateurs, grâce au concept d'URI, classique sur Internet, que nous allons détailler avant de voir son utilisation par SIP.

- **URI (Universal Ressource Identifier)**

Un URI définit une syntaxe permettant de désigner de manière unique, formelle et normalisée une ressource, qu'il s'agisse d'un document textuel, audio, vidéo ou plus généralement d'une entité logique ou physique.

Une ressource décrite par un URI peut être déplacée ou même supprimée. L'URI correspondant n'en conserve pas moins de manière permanente la valeur descriptive de la ressource.

Considérons un exemple. Deux personnes portant le même nom de famille et le même prénom sont susceptibles d'être confondues si on les recherche dans un annuaire. En plus du nom de la personne, qui peut être partagé par d'autres, son âge, sa profession ou sa localisation sont des paramètres susceptibles d'évoluer et qui ne constituent donc pas des propriétés discriminantes. L'attribution d'un identifiant unique à chaque individu assure une identité unique et permet de le différencier des autres avec certitude.

C'est, par analogie, toute la vocation d'un numéro de Sécurité sociale. À la syntaxe près, un numéro de sécurité sociale est une forme d'URI. Une adresse e-mail est également une forme d'URI.

La figure II.7 illustre quelques exemples d'attributs non discriminants et discriminants qui peuvent constituer ou non des URI.

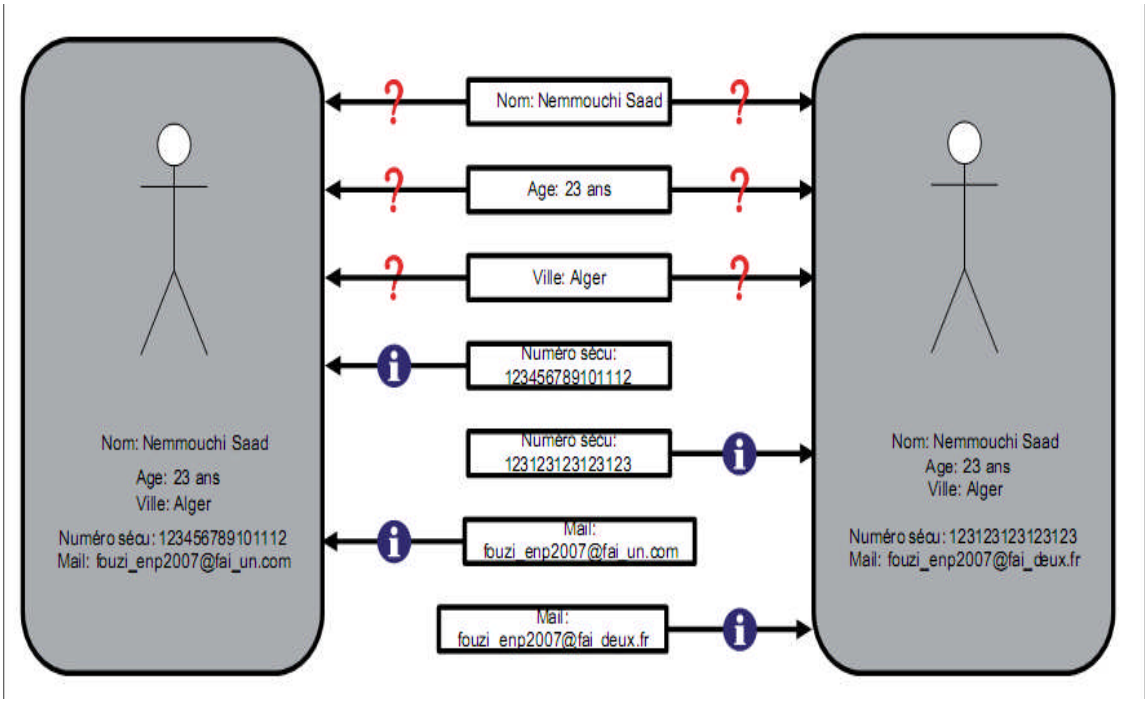


Figure II.7 : Paramètres non discriminants et discriminants

➢ Format des adresses SIP

Tout utilisateur SIP dispose d'un identifiant unique. Cet identifiant constitue l'adresse de l'utilisateur permettant de le localiser.

Le format d'une adresse SIP (ou URL SIP) respecte la RFC 3986 (nommée Uniform Resource Identifier: Generic Syntax) et se présente sous la forme suivant :

sip : identifiant[:mot_de_passe]@serveur[?paramètres]

Les parties entre crochets sont optionnelles.
On distingue dans cette adresse plusieurs parties :

- Le mot-clé *sip* spécifie le protocole à utiliser pour la communication.
- La partie *identifiant* définit le nom ou le numéro de l'utilisateur.
- La partie *mot_ dejpasse* est facultative. Le mot de passe peut être utile pour s'authentifier auprès du serveur
- La partie *serveur* spécifie le serveur chargé du compte SIP dont l'identifiant précède l'arobase.
- La partie *paramètres* est facultative. Les paramètres permettent soit de modifier le comportement par défaut, soit de spécifier des informations complémentaires

- Le tableau II.1 fournit quelques exemples d'adresses SIP commentées

Tableau II.1: Exemples d'adresses SIP

Adresse SIP	Commentaire
<sip:guy.laurent@123.123.123.123>	C'est le format le plus commun. L'identifiant de l'utilisateur est spécifié par un nom ou un pseudonyme, *guy.laurent*. Après l'arobase est spécifiée l'adresse IP du serveur en charge de la gestion du compte de *guy.laurent*. Cette adresse IP étant fixe, il n'est pas nécessaire de la résoudre par un DNS, et il est possible de contacter directement ce serveur. L'IP fixe n'est généralement pas pratique, car une adresse fixe oblige le fournisseur d'accès à conserver ses mécanismes d'adressage ou à avertir ses utilisateurs de toute modification.
<sip:+33145555555:mon_pass123@ ma_passerelle_rtc>	Le premier nombre *(+33145555555)* est le numéro de téléphone du correspondant. On peut supposer qu'il s'agit d'un numéro géographique et que le correspondant est actif dans le réseau RTC. Pour joindre ce réseau, il faut passer par une passerelle, donnée juste après l'arobase, dont le nom est *ma_passerelle_rtc*. L'utilisation d'un mot de passe *(mon_pass123)* permet à l'appelant de s'authentifier auprès du serveur *ma_passerelle_rtc* pour avoir le droit d'émettre l'appel (notamment pour la facturation)
<sip:guy. laurent@sip_ietf.org:12345?sub- ject=Confirmation_RendezVous;tran sport=tcp:54321>	Cette adresse est semblable à la première, mais avec des paramètres supplémentaires. Elle comporte un nom d'utilisateur (toujours *guy.laurent)* et un serveur à contacter pour être mis en contact avec l'utilisateur. Le serveur étant nommé *sip_ietf.org*, son nom devra être résolu par un DNS afin de déterminer son adresse IP. Il sera contacté sur le port 12345. Cette adresse fournit les informations complémentaires suivantes : - Un sujet, qui indique le motif de l'appel : *Confirmation_RendezVous*. En même temps que le terminal appelé sonnera, le nom de l'appelant et le sujet de son appel pourront être affichés sur le terminal, sous réserve que ce dernier supporte ce service. - Un protocole de transport imposé : *tcp*. Par défaut, c'est le protocole UDP qui est utilisé dans les communications. - Un port à utiliser pour la communication : *54321*. Par défaut, c'est le port 5060 qui est utilisé.

➢ Localisation et résolution d'une adresse SIP

D'une manière générale, une adresse SIP spécifie un utilisateur et un nom de domaine. Pour localiser l'utilisateur, il faut d'abord contacter le serveur gérant le domaine puis solliciter ce serveur pour déterminer la position de l'utilisateur.

Si la partie indiquant le serveur de domaine contient une adresse IP, ce serveur est joint directement. À défaut, l'adresse IP du serveur sera déterminée après une résolution DNS. La demande de localisation de l'utilisateur s'effectue auprès du serveur de domaine ainsi contacté. La position de l'utilisateur peut être référencée de manière absolue ou relative.

Le cas simple consiste en une position absolue, spécifiant une adresse IP localisant l'utilisateur. Le cas plus complexe consiste en une position relative, spécifiant une autre adresse SIP. Dans ce cas, il faut répéter l'opération de résolution de cette nouvelle adresse SIP depuis le début : contacter le serveur SIP gérant le domaine puis lui demander la position de l'utilisateur.

Dans le cas illustré à la figure II.8, il s'agit de localiser l'utilisateur *David* à partir de son adresse SIP *david.dad@dom_A.fr*. Cet utilisateur possède une autre adresse SIP, qui est *dav@dom_B.fr*. L'une correspond à une adresse professionnelle, l'autre à une adresse personnelle. Naturellement, l'utilisateur souhaite rester joignable sur ces deux adresses simultanément.

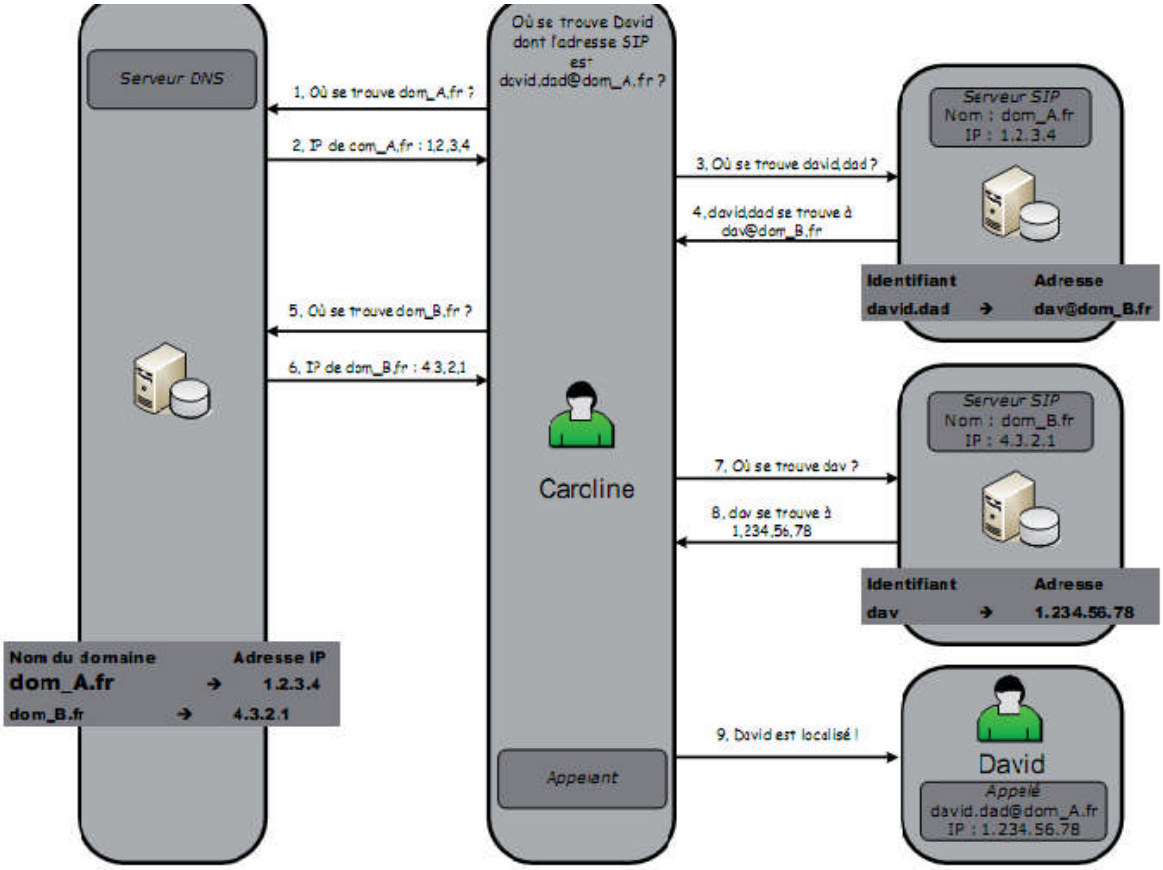


Figure II.8: Principe de localisation à partir d'une adresse SIP

Pour que l'exemple soit valide, il faut considérer que, préalablement à la localisation, l'utilisateur *David* s'est enregistré auprès du serveur SIP gérant le domaine *dom_A.fr* .en lui fournissant son identifiant *(david.dad)* et une adresse SIP associée *(dav@dom_B.fr).*

Notons que le serveur indiqué dans la partie domaine d'une adresse SIP peut être un serveur SIP de type proxy ou une passerelle permettant de joindre des utilisateurs d'un réseau non-IP.

II.2.2.1.5- Les messages SIP

Les messages se composent de requêtes et de réponses qui sont échangés au format texte. Chaque message contient une adresse (URI), un ensemble d'en-tête, et un corps.

Il existe donc 5 types d'URI SIP (FROM, COURANTE, TO, CONTACT, EXTERNAL).

Les messages SIP sont échangés entre deux entités sur un mode client/serveur. En effet, l'entité appelante émet une requête vers l'entité appelée. Celle-ci répondra par un autre message envoyé à l'appelant. Dans ce contexte, l'appelant est considéré comme un UAC et l'appelé comme un UAS et l'échange de message comme une transaction.

En-tête

Accept : Utilisé dans les messages INVITE, OPTIONS et REGISTER qui permet d'indiquer les types de média qui seront acceptés dans la repense à ce message

Allow : Indique les méthodes valides supportées par les entités identifiées par la requête URI. **Via** : ce champ représente le chemin parcouru par la requête, lors de l'envoie de la requête il contient initialement l'URI de l'émetteur de cette requête. Ensuite, à chaque fois qu'un Serveur mandataire fait suivre la requête celui-ci rajoute sa propre URI dans ce champ. **Max-Forwards** : nombre maximum de sauts

To : URI du destinataire du message

From : URI de l'expéditeur du message

Call-ID : identifiant unique représentant la session SIP

Cseq : contient un entier et un nom de méthode, l'entier est généré aléatoirement une première fois puis est ensuite incrémenté à chaque nouveau message.

Contact : contient une ou plusieurs URI représentant une route directe pour contacter l'expéditeur

Content-Type : description du corps du message

Content-Length : taille en octet du corps du message

branch,tag : utilisés pour des raisons d'identification

D'après le modèle client/serveur, les messages sont classés en deux catégories :

Les requêtes : Elles constituent les messages définissant la qualité de la transaction (invitation, demande d'information, souscription etc....).

Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes :

- INVITE : cette requête indique que l'application (ou utilisateur) correspondante à L'URL SIP spécifié est invité à participer à une session. Le corps du message décrit cette session (par ex : média supportés par l'appelant). En cas de réponse favorable, l'invité doit spécifier les médias qu'il supporte.
- ACK : permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête INVITE.
- OPTIONS : un proxy server en me sure de contacter un terminal appelé, doit répondre à une requête OPTIONS en précisant ses capacités à contacter le même terminal.
- BYE : cette requête est utilisée par le terminal de l'appelé à fin de signaler qu'il souhaite mettre un terme à la session.
- CANCEL : cette requête est envoyée par un terminal ou un proxy server afin d'annuler une requête non validée par une réponse finale Si une machine ayant été invitée à participer à une session, et ayant accepté l'invitation ne reçoit pas de requête ACK, alors elle émet une requête CANCEL.
- REGISTER : cette méthode est utilisée par un client pour enregistrer son adresse auprès du serveur auquel il est relié.

Les réponses : Elles constituent les informations renvoyées par le serveur au client ou par le client au serveur et concernent autant l'évolution de la transaction que les erreurs pouvant survenir (transport, serveur, client, etc.). On distingue les réponses provisionnelles, qui donnent une information optionnelle, et les réponses finales qui clôturent une transition.

Une transaction SIP est initiée par une requête, suivie d'une ou plusieurs réponses provisionnelles

- 1 XX : provisoire/informationnelle, le traitement de la requête est en cours.
- 2XX : succès : la requête a été bien reçue, comprise et acceptée,
- 3XX : redirection vers une autre entité. D'autres actions doivent être entreprises.
- 4XX : erreur client. La requête est syntaxiquement erronée ou n'a pas pu être traitée.
- 5XX : erreur serveur : le serveur n'a pas su traiter une requête.
- 6XX : erreur générale : la requête ne peut être traitée par aucun

Voici deux exemples (les plus simples possibles) d'en-tête de message

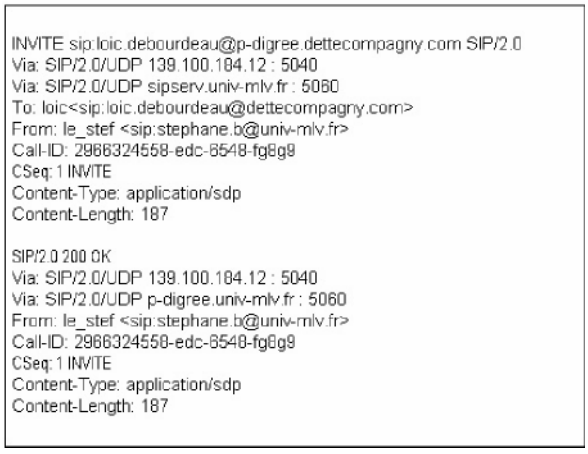


Figure II.9 Exemple d'une requête et repense SIP

II.2.1.1.6- Scénarios de communication [11]

Nous allons illustrer la succession chronologique des messages de requêtes et de réponses dans les six scénarios classiques suivants :

- Initialisation d'une communication directe.
- Enregistrement d'un terminal.
- Initialisation d'une communication avec un serveur proxy.
- Localisation par un serveur de redirection et initialisation d'appel directe.
- Modification dynamique d'une communication SIP
- Terminaison d'une communication.

- **Initialisation d'une communication directe**

Une communication peut s'effectuer directement entre deux correspondants, sans faire intervenir d'autre entité.

Dans ce cas, l'appelant doit connaître la localisation (sous forme d'adresse IP) de la personne qu'il souhaite contacter.

La figure II.10 illustre ces scénarios.

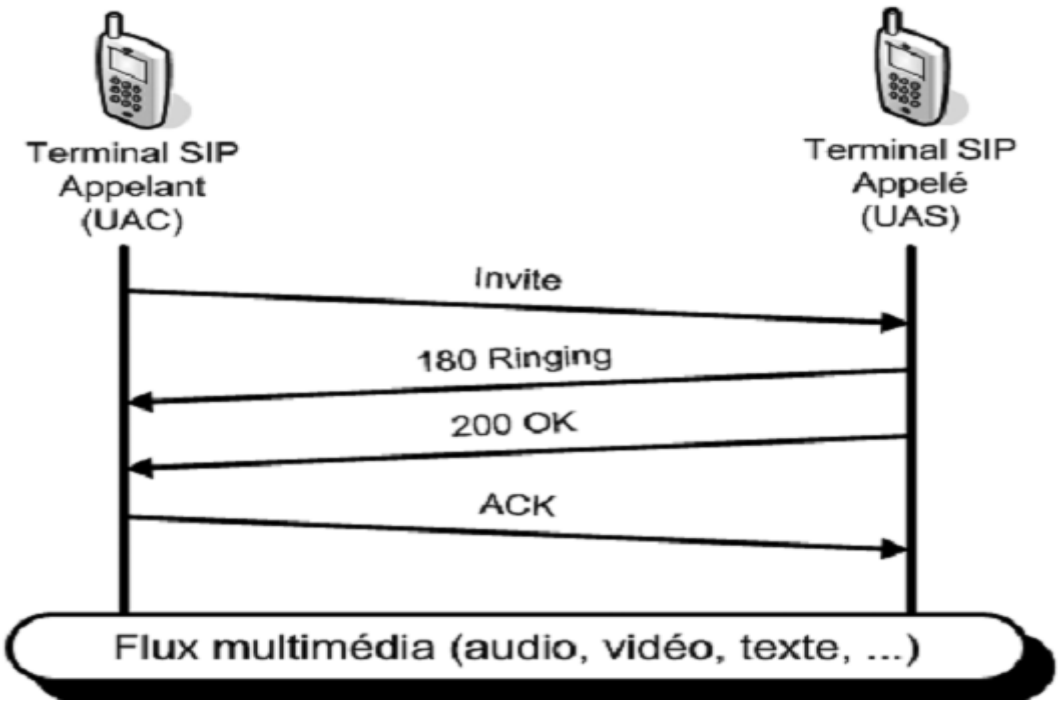


Figure II.10 : Initiation d'une communication directe

Cette communication reflète la simplicité d'utilisation du protocole SIP. Quatre étapes seulement suffisent à mettre en relation les deux utilisateurs :

1. L'appelant (UAC) envoie un message (requête INVITE) proposant à son correspondant (UAS) d'initier une communication. Ce message contient les paramètres désirés pour établir la communication.
2. Dès que l'appelé accepte l'appel (en décrochant), l'UAS informe l'appelant (par une réponse définitive *200* OK) que l'appel peut débuter. Ce message contient les paramètres que l'UAS supporte pour la session.
3. L'UAC retourne à l'UAS un message d'acquittement (requête ACK) lui indiquant qu'il a pris note que l'appel peut débuter. Ce message comporte les paramètres fixés pour la session, qui tiennent compte de ces possibilités et de celles de l'UAS.

Les intervenants sont ensuite mis en relation et peuvent communiquer.

- **Enregistrement d'un terminal**

Lorsqu'un terminal est activé dans un réseau, sa première action consiste à se déclarer auprès d'un serveur d'enregistrement, de manière à être disponible si un appelant souhaite le joindre.

Ce scénario est illustré à la figure II.11.

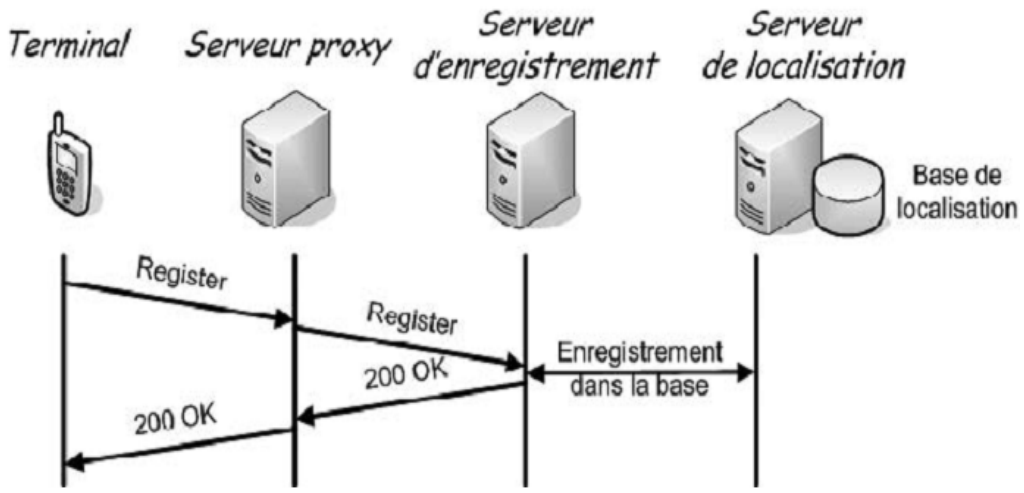


Figure II.11: Enregistrement d'un terminal SIP

Le serveur de localisation maintient dans sa base de données une entrée associant l'identifiant d'un utilisateur avec sa position dans le réseau (adresse IP du terminal de l'utilisateur, port utilisé par l'application SIP et identifiant de l'utilisateur sur ce poste).Cette entrée sera du type indiqué au tableau II.2

Tableau II.2 Entrée dans le serveur de localisation permettant de localiser un utilisateur

Utilisateur	Localisation	Délai d'expiration
sip:albert@mon_domaine.fr	*sip:albert@132.227.155.155:12345*	*48 minutes*

Notons la présence d'un délai d'expiration, ici arbitrairement fixé à 48 minutes (par défaut, une entrée est valable pendant une heure). Périodiquement, le terminal doit rafraîchir son entrée à l'aide de la requête REGISTER afin de manifester sa présence. À défaut, l'entrée est effacée.

➢ Initialisation d'une communication SIP avec un serveur proxy

Les étapes et messages envoyés pour initier une session entre deux correspondants dans le cas où un proxy est utilisé sont illustrés à la figure II.12.

Dans cet exemple, Anne souhaite ouvrir une session avec Brigitte. Comme elle ne connaît pas la localisation de cette dernière, elle sollicite son proxy afin de la déterminer.

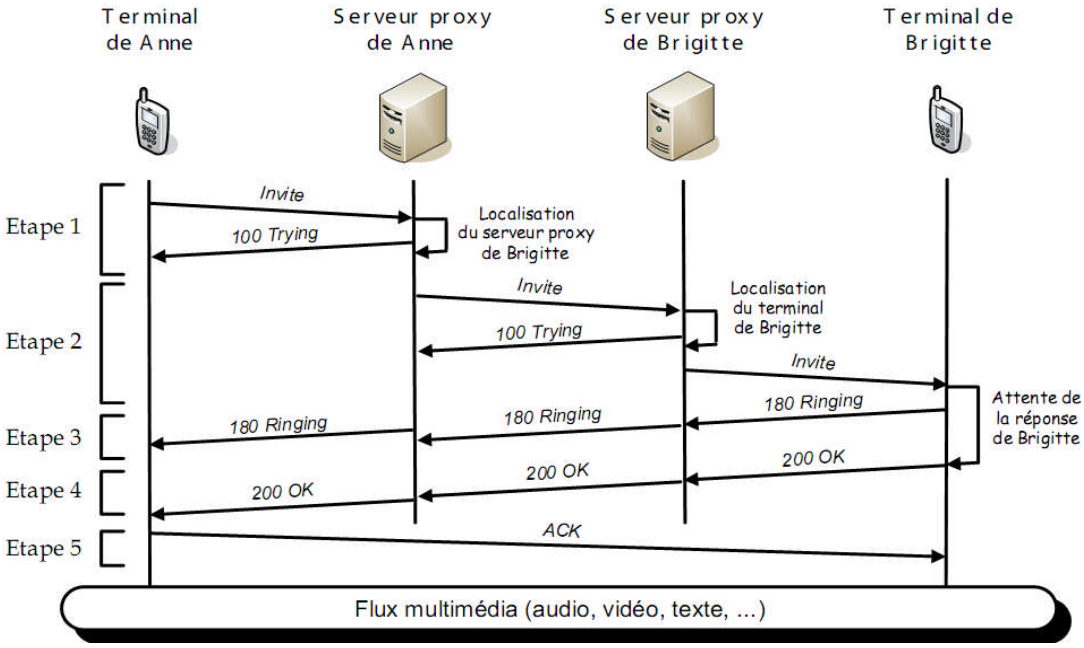


Figure II.12: Initiation d'un appel avec un proxy

Auquel il ajoute sa propre adresse réseau (en plus de celle d'Anne, qui y figure initialement). Le serveur proxy de Brigitte informe le serveur proxy d'Anne (par un message de réponse temporaire *100* TRYING) de la réception de la requête et de la tentative d'initialisation. Parallèlement, il recherche la localisation du terminal de Brigitte en utilisant le service de localisation. Une fois la position du terminal dans le réseau trouvée, il lui transmet l'invitation d'Anne. À nouveau, ce message est conforme à l'original, et seul le champ VIA a été enrichi de l'adresse du serveur proxy de Brigitte.

3. Le terminal de Brigitte sonne. Le téléphone de Brigitte (éventuellement un soft-phone) reçoit l'invitation et la fait connaître à l'utilisateur Brigitte, le plus souvent par une sonnerie. En parallèle, il indique à son proxy (par un message *180* RINGING) que l'appel est en train d'être notifié à Brigitte et que la communication est en attente de son acceptation. Ce message informatif est relayé jusqu'à l'émettrice Anne, qui reçoit

généralement un retour audio ou visuel (une tonalité de sonnerie particulière le plus souvent). L'utilisation du champ d'en-tête VIA permet de remonter de proche en proche jusqu'à Anne selon le même chemin.

4. Brigitte répond au téléphone. On suppose le cas où Brigitte a choisi de répondre à l'appel. À l'instant où elle décroche, l'UAS retourne à l'UAC un message *200* OK pour l'informer que l'appel est accepté. Ce message est relayé par les différents proxy. À ce stade, la communication n'a pas encore débuté, et aucun son n'est transmis.

5. Le terminal d'Anne confirme les paramètres d'appel. En tenant compte des capacités prises en charge par les correspondants, le terminal d'Anne envoie un message d'acquittement ACK qui spécifie les paramètres définitifs à utiliser lors de cette session. Notons que le message d'acquittement peut passer directement d'un interlocuteur à l'autre, sans transiter par les serveurs proxy. À ce stade, chacun des utilisateurs a pu apprendre la localisation exacte de son interlocuteur, et il n'est donc plus nécessaire de recourir aux serveurs proxy. Toutes les transactions qui suivent sont effectuées directement, de poste utilisateur à poste utilisateur. Ainsi, les serveurs proxy sont sollicités au minimum. De la même manière, pour ne pas saturer les serveurs proxy inutilement, les flux de données multimédias ne transitent jamais par eux.

À réception de ce message, la communication entre les interlocuteurs peut débuter. Tous ces échanges n'ont réclamé que quelques millisecondes, imperceptibles pour les intervenants.

Globalement, on retrouve dans cet appel, les trois phases fondamentales de l'appel direct entre les correspondants :

1. Requête INVITE : invitation de l'appelant.
2. Réponse *200* OK : acceptation par l'appelé.
3. Acquittement ACK : confirmation par l'appelant.

Il s'agit des trois messages nécessaires à la modification dynamique d'une communication SIP. Les autres messages concernent essentiellement la localisation ou sont à titre informatif.

- **Localisation par un serveur de redirection et initialisation d'appel directe**

La figure II.13 illustre le scénario où un serveur de redirection est utilisé par le terminal appelant afin de localiser son correspondant et pour l'échange qui s'ensuit. L'objectif est

toujours de mettre en relation le terminal d'Anne avec celui de Brigitte, mais par un autre moyen.

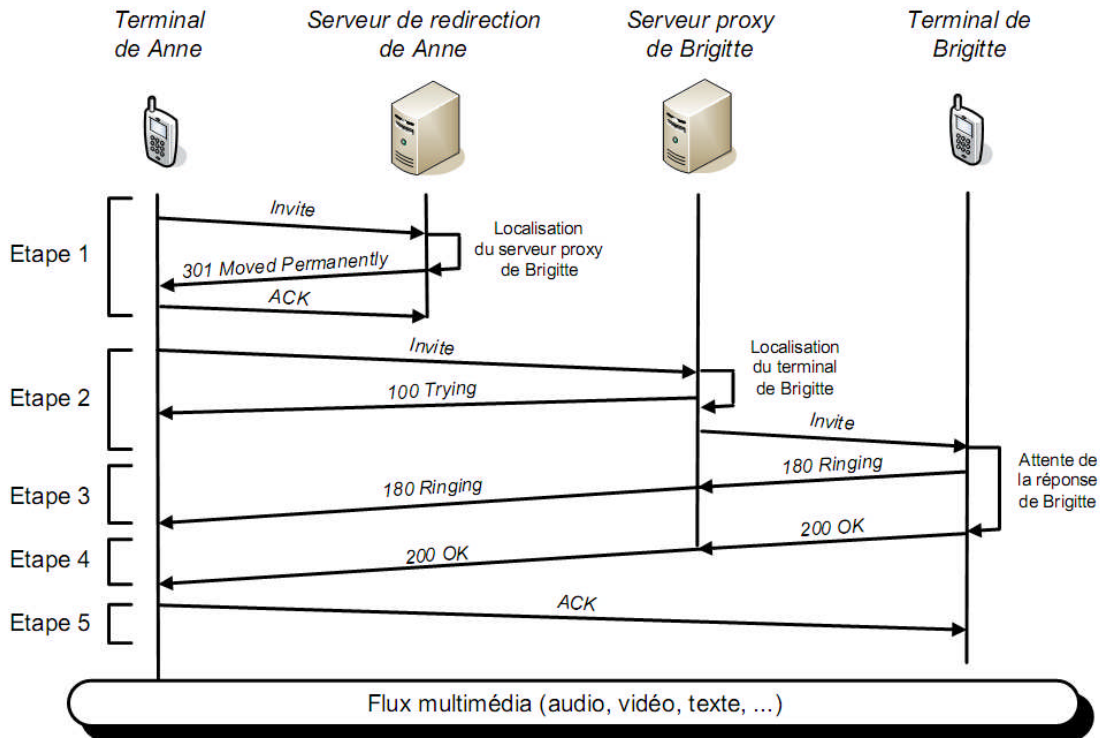


Figure II.13: Localisation avec un serveur de redirection et initialisation d'appel

Dans la première étape, le terminal d'Anne sollicite le serveur de redirection pour déterminer la localisation du terminal d'Anne. Une fois cette recherche effectuée, la réponse est envoyée directement au terminal d'Anne, lequel initie l'appel lui-même, en contactant le serveur proxy de Brigitte.

Les étapes qui suivent sont identiques à celles du scénario précédent avec l'initialisation d'appel par un serveur proxy, si ce n'est que ce dernier n'intervient pas dans les échanges intermédiaires.

- **Modification d'une communication SIP**

Lorsqu'un utilisateur est en communication, il peut arriver qu'il souhaite modifier les paramètres de cette communication tout en la conservant active. Par exemple, s'il commence un téléchargement et que son débit risque de diminuer en conséquence, il peut souhaiter utiliser un codec moins gourmand. Dans un autre cas, l'utilisateur peut vouloir enrichir la communication audio avec une diffusion vidéo. Ou encore, il peut souhaiter inviter à une

conférence un nouveau correspondant, qui ne supporte pas le codec utilisé par les autres conférenciers.

Ces cas sont parfaitement envisageables avec le protocole SIP, qui offre, rappelons-le, une très grande souplesse. À tout moment, l'appelant ou l'appelé peut envoyer un nouveau message d'invitation, avec la requête INVITE, afin de renégocier les paramètres de la communication. Bien sûr, dans ce contexte, le message n'a pas pour objectif d'inviter à une nouvelle session, mais d'utiliser de nouveaux paramètres.

C'est pour cette raison qu'on nomme RE-INVITE ce type de requête d'invitation. Du reste, la communication en cours n'est pas interrompue par la réception de cette requête. S'il accepte les modifications sollicitées dans la requête d'invitation, le récepteur confirme son accord par l'envoi d'une réponse *200* OK, qui sera ensuite acquittée par le demandeur, comme pour l'initiation d'une communication. Dans ce contexte, cette requête ne fait pas sonner le poste de l'interlocuteur puisque la communication est déjà en cours.

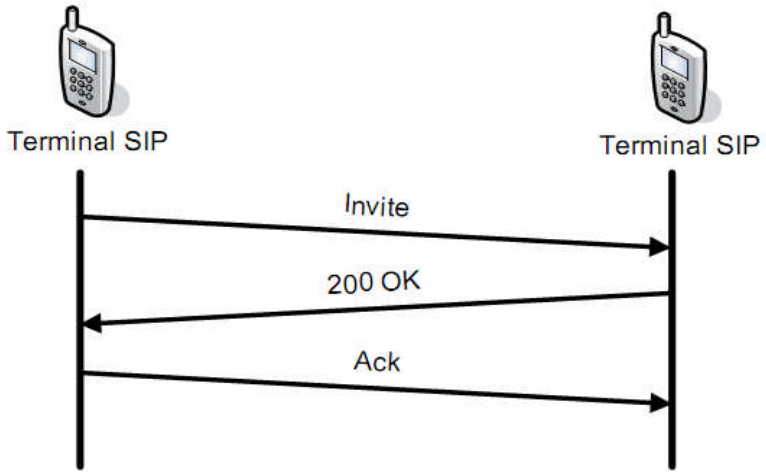


Figure II.14 : Requête réinvite acceptée

Dans le cas contraire, où le récepteur ne supporte pas ou ne souhaite pas accepter la modification de la session en cours, il reste libre de le faire, sans pour autant mettre fin à la communication, en envoyant un message de réponse *488* NOT ACCEPTABLE HERE, comme l'illustre la figure II.15.

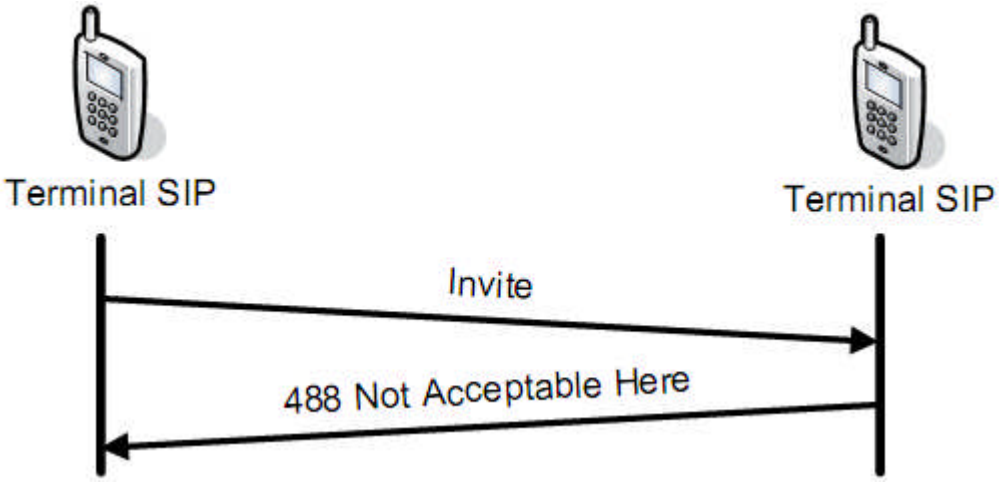


Figure II.15 : Requête réinvite refusée

Le demandeur qui en prend connaissance ne peut effectuer la modification désirée et doit soit se contenter des paramètres de la session actuelle, soit faire une nouvelle offre, en suggérant l'utilisation d'autres paramètres.

- **Terminaison d'une communication SIP**

  La figure II.16 illustre la terminaison d'une session à l'initiative de n'importe quelle entité souhaitant mettre fin à l'appel.

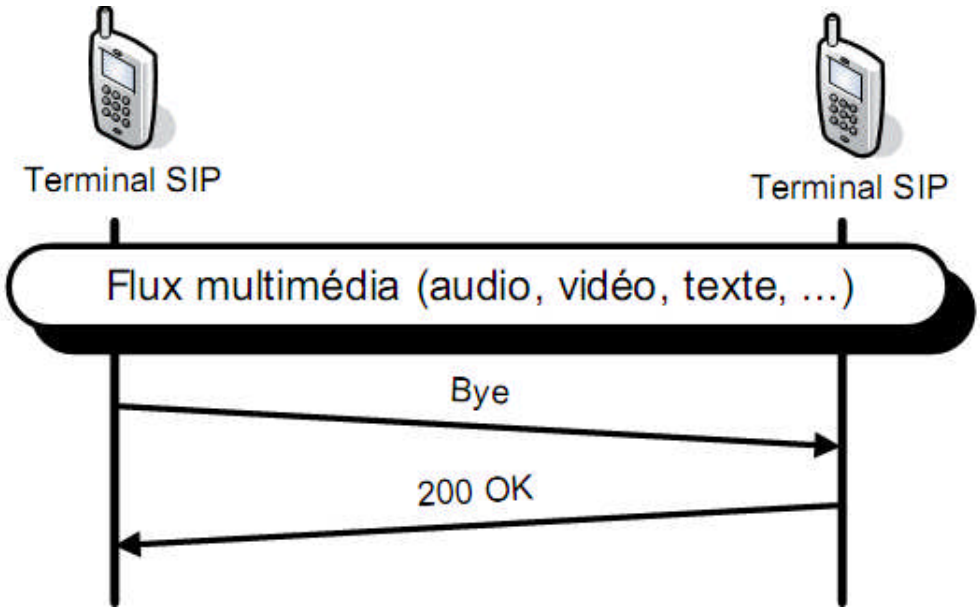


Figure II.16: Terminaison d'une communication

Cette opération ne comporte que les deux étapes très simples suivantes :

1. Un message (requête BYE) est envoyé pour indiquer au correspondant que la session va être clôturée.
2. Le correspondant répond à cette requête en validant la prise en compte de cette demande par une réponse 200 OK.

   La communication entre les intervenants est alors rompue.

II.2.2.2 - La signalisation H.323 [12]

La signalisation désigne la transmission d'un ensemble de signaux et d'informations de contrôle échangés entre les intervenants d'une communication. Ces intervenants peuvent être des entités en bout de liaison (terminaux) ou des entités intermédiaires de contrôle et de gestion des communications. Leurs échanges permettent l'initiation, la négociation, l'établissement, le maintien et la fermeture de la connexion.

Il convient de distinguer deux types de transferts pour comprendre à quoi correspond la signalisation :

- Le transfert de données brutes ;

- Le transfert d'informations de contrôle.

Le transfert de données brutes concerne les échanges de données binaires d'un poste vers un autre. L'objectif de ce transfert est de reproduire à l'identique des données en les faisant transiter par un réseau. Par exemple, deux correspondants peuvent s'échanger un fichier audio MP3 ou des images bitmap, comme à la figure II.17, où l'utilisateur Alain envoie des données vers le poste de Béatrice

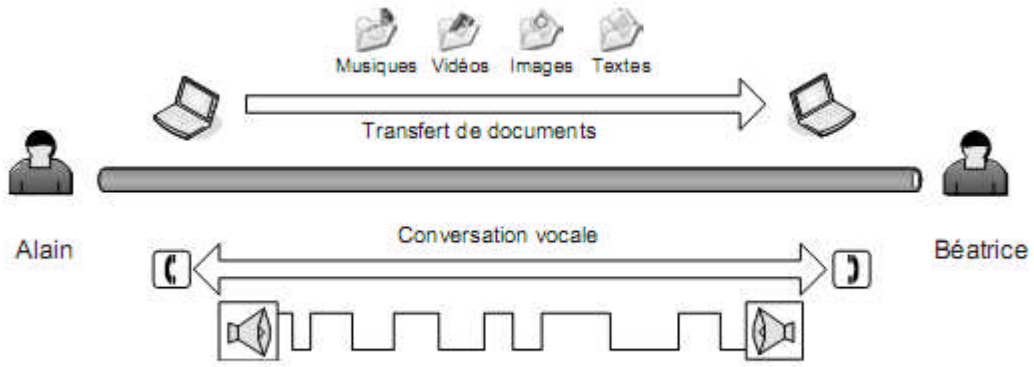


Figure II.17 transfert des données brutes

Le transfert d'informations de contrôle concerne les échanges de type protocolaire exécutant une action prédéfinie, et donc nécessairement limitée en possibilités. L'objectif de ce transfert est d'assurer la maîtrise et la gestion du flux.

Dans le cas typique d'une application de téléphonie, lorsqu'une personne en appelle une autre, elle n'a initialement pas de « données » à lui transmettre, mais veut simplement être mise en relation avec son correspondant. Cette mise en relation nécessite d'abord de localiser l'appelé, puis de faire sonner son poste, afin de lui signaler l'appel. Pour la localisation comme pour l'avertissement d'appel, on parle de signalisation.

La figure II.18 illustre quelques exemples de messages de signalisation transportant des requêtes et réponses à caractère descriptif.

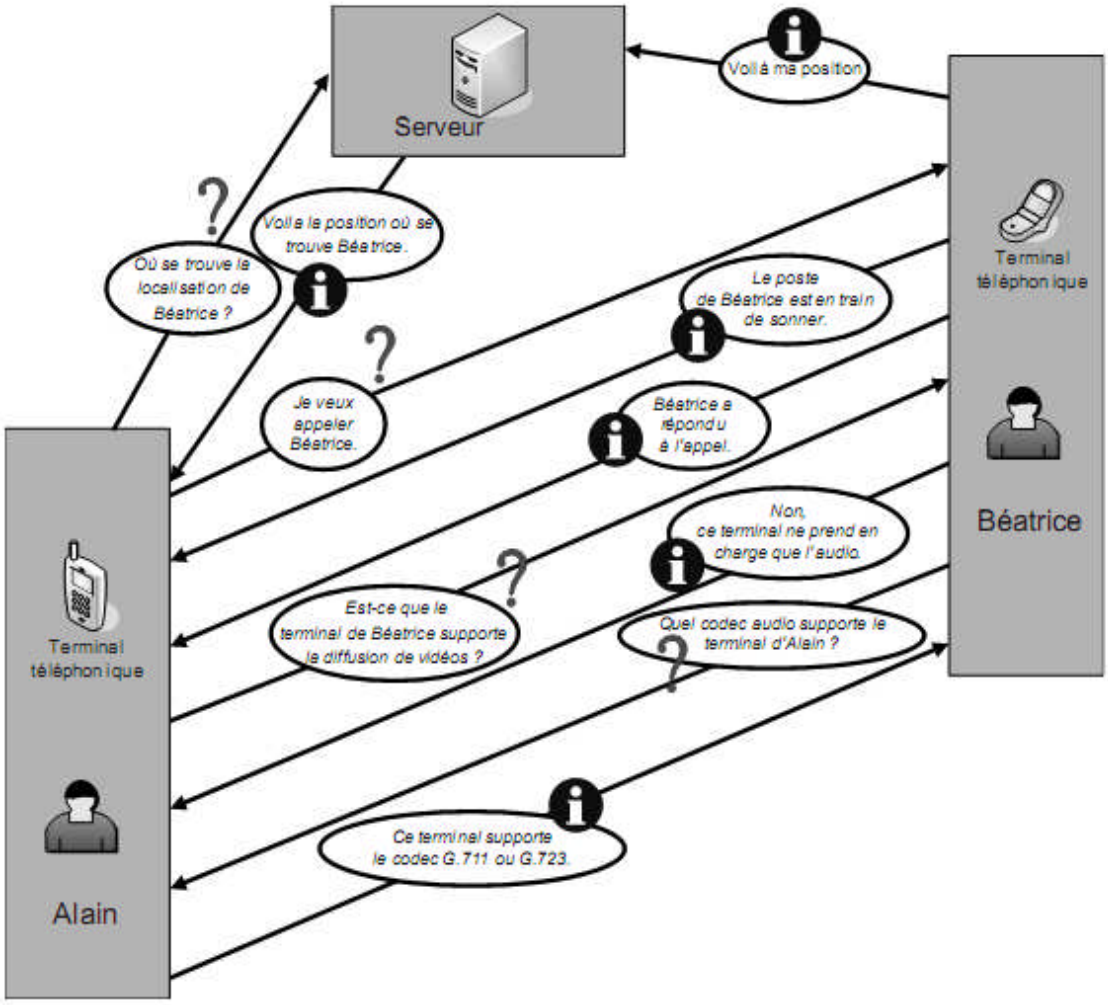


Figure II.18 : Transfert d´information de contrôle

Dans le modèle OSI, la signalisation téléphonique correspond à une fonctionnalité de niveau 7 (couche applicative). Elle n'est donc jamais assurée par les entités réseau de routage pur, comme les routeurs et commutateurs, qui fonctionnent à des couches inférieures. Des entités dédiées sont exploitées à ces fins : il s'agit de serveurs au niveau du cœur du réseau et des terminaux (téléphone, ordinateur ou PDA, par exemple) en bordure de réseau, au niveau de l'utilisateur.

II.2.2.2.1- Architecture et fonctionnalités du protocole H.323 [13]

Le protocole H.323 s'articule autour d'une architecture particulière décrite dans ce qui suit. Cette architecture concentre les fonctionnalités autour d'entités, ce qui explique pourquoi le protocole H.323 est considéré comme fortement centralisé.

Une architecture H.323 est généralement composée des quatre catégories d'entités suivantes :

- **Terminaux (au minimum deux).**

Il existe différents types de terminaux selon les modes d'utilisation :

- Les systèmes de groupe permettent d'équiper des salles de réunion et de supporter des visioconférences impliquant plusieurs utilisateurs. Selon les modèles ils se connectent en ISDN et/ou en IP.
- Les systèmes individuels se trouvent sous la forme de visiophones autonomes ou directement intégrés dans le poste de travail.

Le respect du standard H.323 permet de garantir un contrôle sur l'utilisation des ressources réseau et des contraintes de qualité de service. Tous les terminaux H.323 doivent supporter :

- Le protocole H.245, pour négocier l'ouverture et l'utilisation des canaux ainsi que les paramètres de la communication.
- Le protocole Q.931 (version allégée) pour la signalisation et l'établissement d'appels
- Le protocole RAS (Registration/Admission/Status), qui est le protocole utilisé par le terminal pour communiquer avec le Gatekeeper.
- Les protocoles RTP/RTCP pour les flux audio et vidéo.

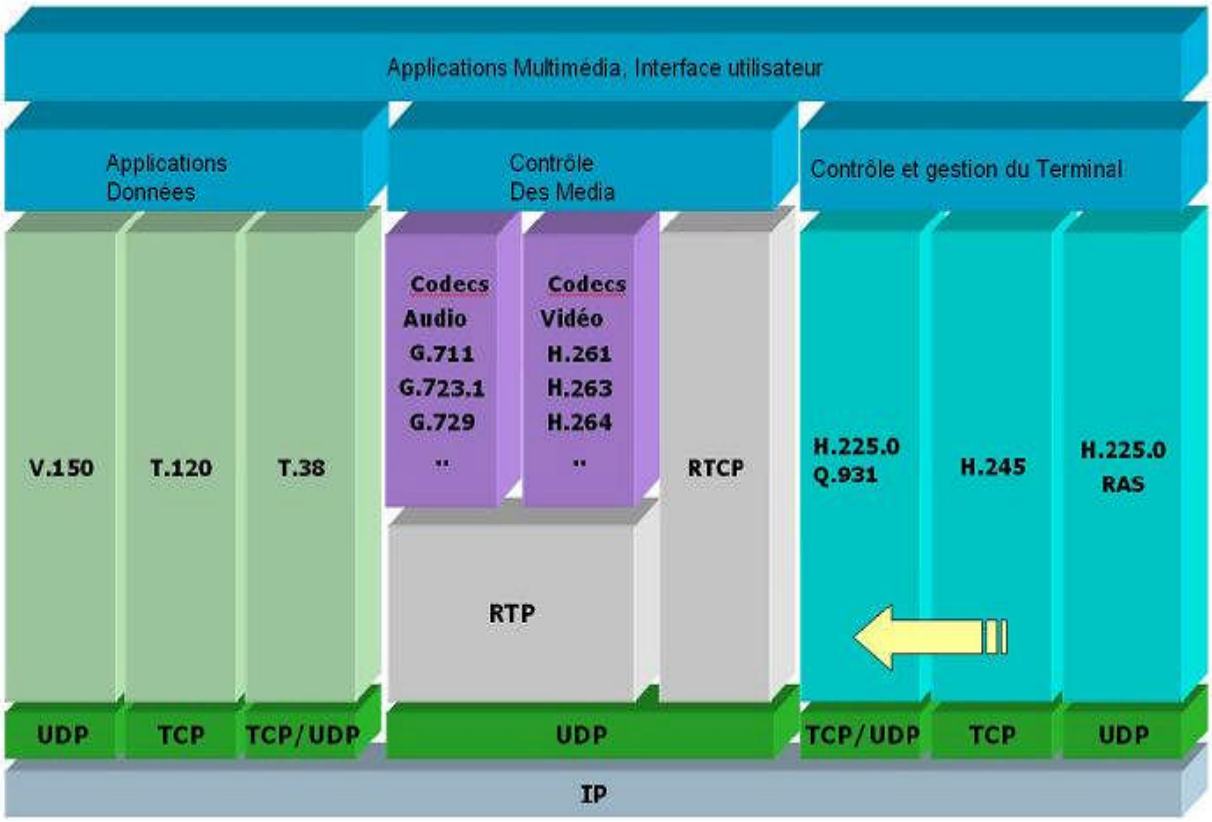


Figure II.19 Pile protocolaire H.323

➢ Le Gatekeeper

Dans la norme H323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H.323, regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dés l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe obtenu auprès de son Gatekeeper de rattachement.

Les Gatekeepers assurent :

1. La translation des alias H.323 vers des adresses IP, selon les spécifications RAS.

2. Le contrôle d'accès, en interdisant les utilisateurs et les sessions non autorisés.

3. La gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées. Concrètement on alloue une fraction de la bande passante à la visioconférence pour ne pas gêner les applications critiques sur le LAN.

4. Le support des conférences multipoint ad hoc. Dans le cas ou cette fonctionnalité est implémentée

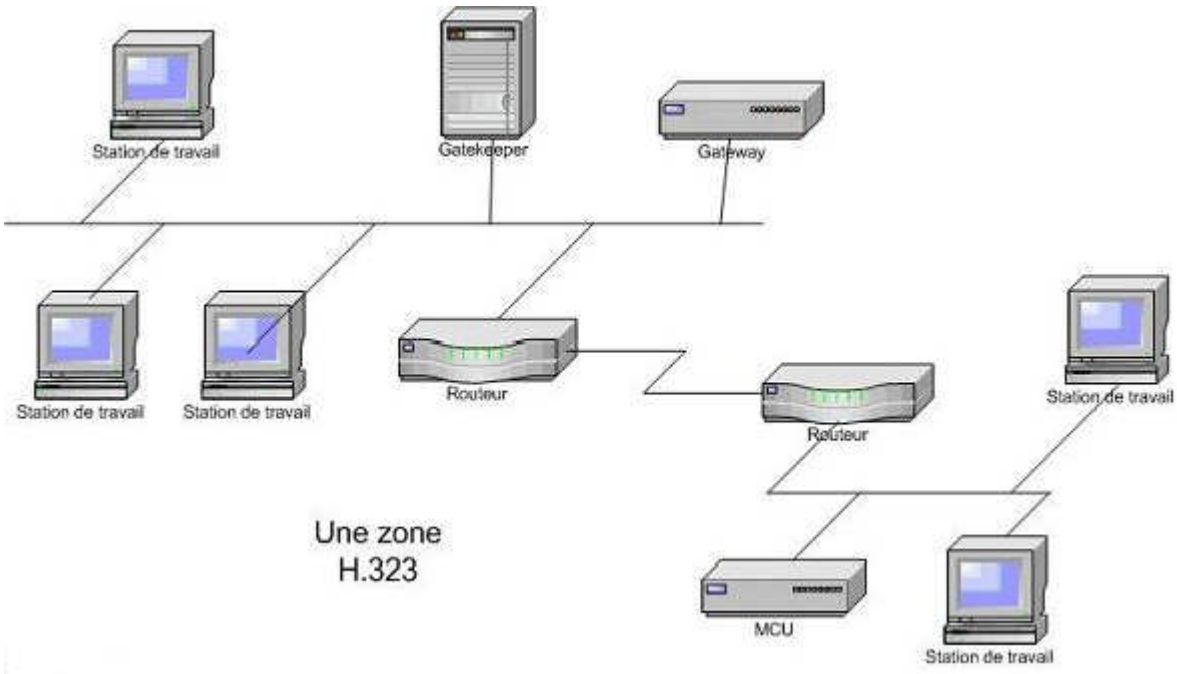


Figure II.20 : Gatekeeper

- **La Gateway**

Les Gateways assurent l'interconnexion entre le monde IP/H.323 et les autres types de terminaux (ISDN/H.320 ou RTC/H.324). Elle assure la translation des formats de transmission (ex. H.225 vers H.221) et les procédures de communications (ex. H.245 vers H.242). Les terminaux communiquent avec la Gateway via les protocoles H.245 et Q.931.

- **La MCU (Multipoint Control Unit)**

La MCU offre aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints

(MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées. Mais le MC ne traite pas directement avec les flux audio, vidéo ou données, c'est le MP qui se charge de récupérer les flux et de leurs faire subir les traitements nécessaires. Un MC peut contrôler plusieurs MP distribués sur le réseau et faisant partie d'autres MCU.

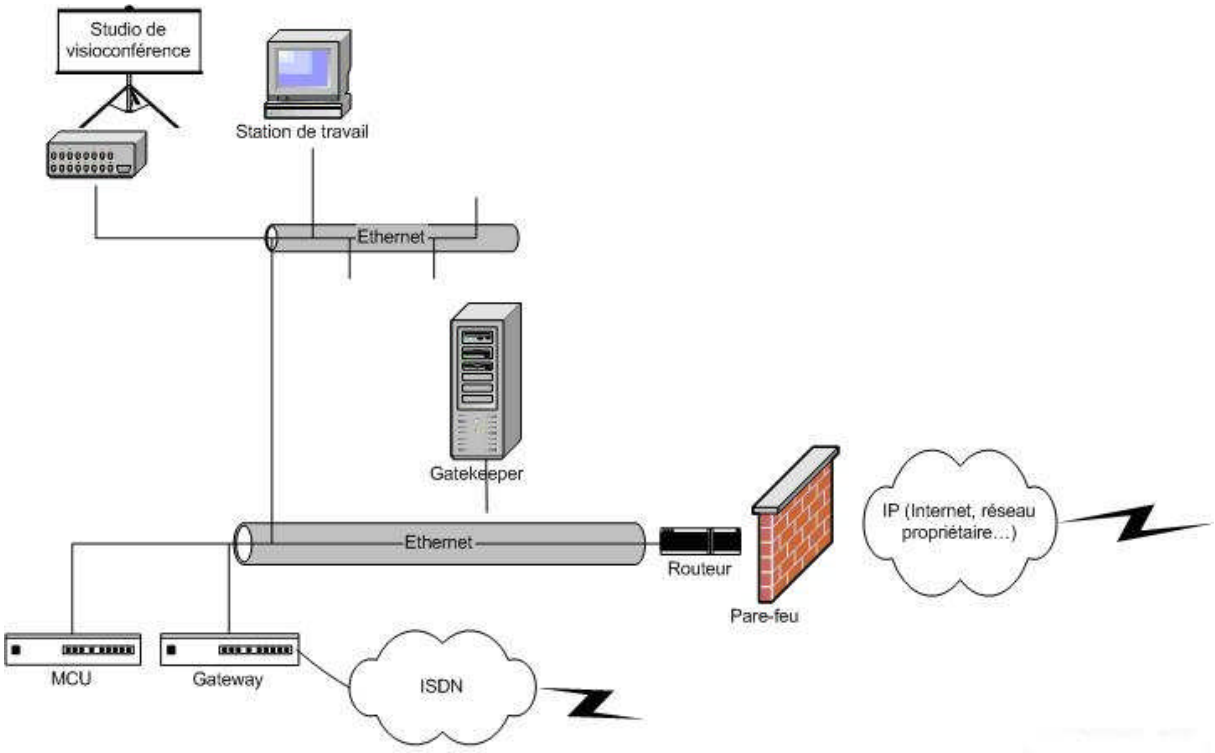


Figure II.21 : Architecture et fonctionnalités du protocole H.323

II.2.2.2.2 - Protocoles secondaires ou associés [14]

Plus qu'un protocole, H.323 ressemble davantage à une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories :

- La signalisation.
- La négociation de codec.
- Le transport de l'information.

Les messages de signalisation sont ceux que l'on envoie pour demander d'être mis en relation avec une autre personne, qui indiquent que la ligne est occupée, que le téléphone sonne... Cela comprend aussi les messages que l'on envoie pour signaler que tel téléphone est connecté au réseau et peut être joint de telle manière, le H323 utilise plusieurs protocoles dont :

- H.225.0, en système de communications, est une sous-norme de H.323, ce dernier étant défini par l'UIT-T. Les principaux objectifs du H.225.0 sont les suivants :

  - Gestion d'un appel : établissement, contrôle et fin d'un appel de type H.323
  - La signalisation s'appuie sur le protocole RAS (*Registration Admission Status*)
  - L'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel

- H.245 Le protocole utilisé pour la négociation de codec.

Pour transmettre les paquets, on utilise RTP, standardisé en 1996. Il est un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur), de détecter les pertes de paquets et en informer la source, et d'identifier le contenu des données pour leurs associer un transport sécurisé. En revanche, ce n'est pas "la solution" qui permettrait d'obtenir des transmissions temps réel sur IP. pas de fiabilisation des échanges (pas de retransmission automatique, pas de régulation automatique du débit) et de garantie dans le délai de livraison (seules les couches de niveau inférieur le peuvent) et dans la continuité du flux temps réel. Bien qu'autonome, RTP peut être complété par RTCP. Ce dernier apporte un retour d'informations sur la transmission et sur les éléments destinataires. Ce protocole de contrôle permet de renvoyer à la source des informations sur les récepteurs et ainsi lui permettre, par exemple, d'adapter un type de codage ou encore de modifier le débit des données.

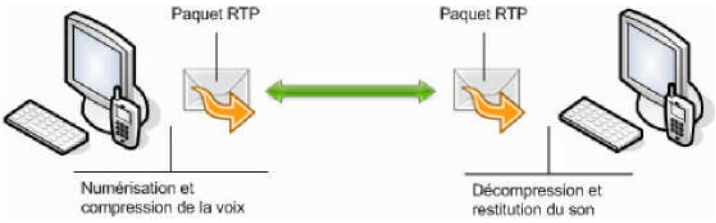


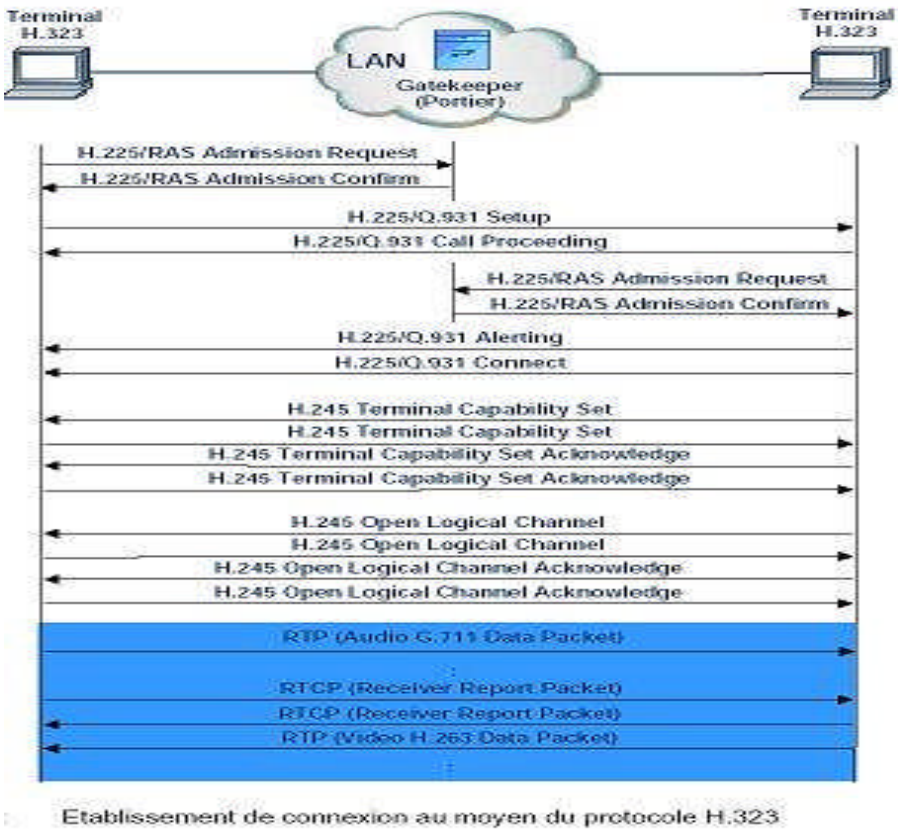
Figure II.22. Transmission de paquet par le protocole RTP

II.2.2.2.3 - Les communications H.323

Les communications en H.323 sont un mélange de flux audio, vidéo, données et contrôle de paquets. Les fonctionnalités audio et la signalisation Q.931, RAS et H.245 sont essentiels, alors que la vidéo et le partage de données sont optionnels car à la base H.323 était bien une généralisation de la téléphonie classique au monde IP. Lorsqu'un élément de l'architecture a le choix entre les algorithmes (codecs audio et vidéo) à utiliser pour encoder ou décoder les flux multimédia, il opte pour celui négocié durant l'échange H.245 qui précède toute communication. Cependant H.323 permet de faire des communications asymétriques en transcodant les flux hétérogènes.

- **Les flux de Contrôle**

Les fonctions de contrôle d'appels sont le cœur de n'importe quel élément H.323 Il y a trois canaux de contrôle regroupés au sein d'une seule couche de contrôle : Le canal de contrôle H.245, le canal de signalisation Q.931, le canal RAS. Ces flux, une fois transformés en messages assurent l'établissement de l'appel, l'échange des paramètres de la communication, l'indication du contenu et des descriptions des canaux logiques audio et vidéo. Le canal de contrôle H.245 assure plus particulièrement l'ouverture et la fermeture de ces canaux logiques, la négociation des paramètres et le contrôle de flux. Il n'y a qu'un seul canal de contrôle entre deux terminaux H.323. Le canal Q.931 établit les connexions entre ces terminaux alors que RAS qui n'est utilisé qu'en présence du Gatekeeper assure le contrôle d'admission, l'enregistrement de l'utilisateur, les changements de débits et des états entre les terminaux et le Gatekeeper dont ils dépendent.



Etablissement de connexion au moyen du protocole H.323

Figure II.23 Exemple d'un échange protocolaire H.323

La première phase se sert du protocole H.225/RAS. Le terminal qui lance l'établissement d'appel (setup) requiert, au préalable, l'autorisation de la part du Gatekeeper. Ensuite, par l'intermédiaire du protocole Q.931, il ouvre la connexion vers le partenaire. Le partenaire doit également demander son admission au Gatekeeper, avant de confirmer l'établissement de connexion. Lorsque les deux terminaux ont achevé la phase de connexion, une phase d'échange de paramètres, basée sur H.245, se déroule. Aussitôt que le canal logique est disponible, la communication audio et vidéo peut débuter. Elle utilise les protocoles RTP (Real Time Protocol) et RTCP (Real Time Control Protocol).

- **Le flux audio**

Le signal audio résulte de la numérisation et de la compression de la voix. Le codec principal normalisé par l'ITU est le G.711 basé sur l'algorithme de compression PCM, classiquement utilisé dans la téléphonie. Les autres codecs sont optionnels.

G.711 permet de transmettre la voix à un débit de 56 kbps ou 64 kbps.

- **Le flux vidéo**

Le codec vidéo principal utilisé en H.323 est le H.261. Son implémentation flexible lui permet de s'adapter à la bande passante disponible et de fonctionner à n'importe quel débit. Par exemple, pour une bande passante de 128 kbps, le codec G.728 utilisera 16kbps et le codec H.261 en utilisera 100kbps, selon le débit des données et la taille des entêtes. H.263 utilise l'estimation du mouvement dans l'image, la prédiction des trames et une table de Code d'Huffman optimisée pour les bas débits.

- **Le flux de données**

Le partage de données (tableau blanc, transfert de fichiers) est optionnel. L'ITU a normalisé les spécifications T.120 pour l'intégrer à la norme H.323. Il concerne les échanges point à point et multipoint et est parfaitement interopérable à partir de la couche réseau.

II.2.1.2.4- Implémentation d'une architecture H323

Il existe plusieurs manières d'implémenter une architecture H.323

- De nombreux messages sont optionnels et dans la pratique on peut choisir de ne pas les utiliser tous. Par exemple, si l'authentification n'est pas une préoccupation, on peut se passer des messages RAS.
- Il est également possible d'enchaîner les messages de plusieurs manières différentes. On peut par exemple ouvrir les canaux RTP sans attendre le message « connect » qui indique que la personne appelée a bien décroché.

• On peut décider que les messages H.225, H.245 et RTP passent par des chemins différents : Par exemple la signalisation traversera plusieurs Gatekeeper qui participent au contrôle et au routage de l'appel alors que le flux RTP passe directement d'un poste à l'autre.

a) Communication « Point à Point >> de deux clients simples

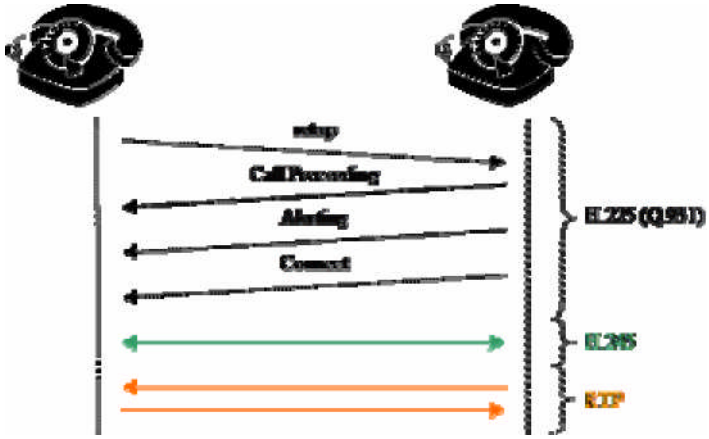


Figure II.24 : Communication point a point

L'appelant entre l'adresse IP du destinataire dans le champ du logiciel réservé à cet effet. Les protocoles de signalisation proposent au logiciel du destinataire d'établir la communication et transmet son ID H323.Le logiciel du destinataire répond soit « occupé » soit « libre ».Si « libre », l'appelant énumère ses possibilités de codecs audio et vidéo (si disponibles).Le destinataire énumère les codecs compatibles à l'appelant pour accord. Si accord, d'autres ports TCP et UDP sont négociés pour l'audio (UDP), la vidéo (UDP) et les données (TCP)

b) Communication « Point à Point >> entre deux clients enregistrés auprès d'un Gatekeeper

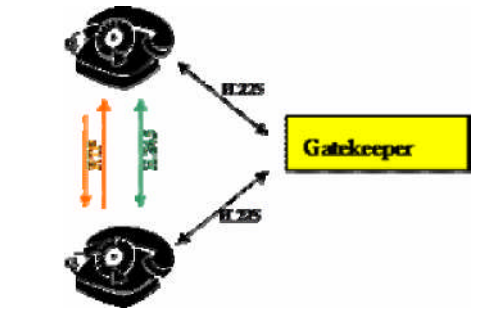


Figure II.25 Communication point a point enregistrés au prêt d'une gatekeeper

À l'ouverture du logiciel, le client A s'enregistre auprès du Gatekeeper en lui transmettant son ID H323 et son adresse IP. Le client B fait de même. Le client A entre l'ID de connexion du client B dans le champ du logiciel réservé à cet effet. Le logiciel du client A demande l'autorisation au Gatekeeper pour se connecter au client B Si le Gatekeeper accepte, celui-ci demande au client B son état (déjà en conversation ou non).Si état compatible, le Gatekeeper transmet l'adresse IP du client B au client A. Le Gatekeeper informe le client B qu'une communication va avoir lieu avec le client A. Le client A entre directement en négociation avec le client B avec les protocoles de contrôle de communication. Le client A énumère ses possibilités de codecs audio et vidéo (si disponibles).L'appelé énumère les codecs compatibles à l'appelant pour accord. Si accord, d'autres ports TCP et UDP sont négociés pour l'audio (UDP), la vidéo (UDP) et les données (TCP).Tous les flux sont ensuite transmis indépendamment les uns des autres sans passer par le Gatekeeper mais directement entre les clients .À la fermeture d'une session, le Gatekeeper est informé de la fin de connexion, les ports sont libérés et les transmissions de contrôles stoppés.

c) Communication multipoints

Les MCU ont des capacités de traitements du signal (diffusion, enregistrement, mixage, ...) ils sont utilisés pour :

- Permettre la conférence en mixant les flux audio
- Diffuser des messages réseau comme la tonalité, le bip de mise en attente

- Voir réaliser des fonctions élémentaires de messagerie vocale

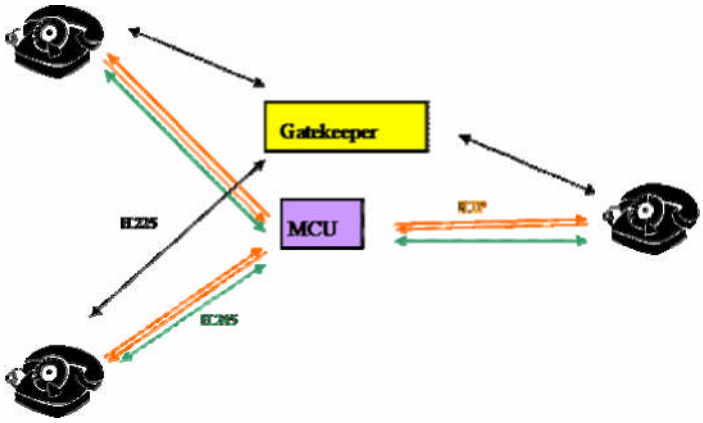


Figure II.26: Communication multipoint

Le MCU s'annonce auprès du Gatekeeper et lui énonce ses possibilités :

Nombre de clients possibles. Débits (en octets/secondes) possible par client ou débit total maximal. L'ID 11323 de connexion**.** Les communications seront ensuite traitées comme au cas 2, le MCU devenant alors un « simple client >> au vu des appelants ; la différence se trouvant simplement dans le nombre de communications acceptées avant transmission du message « occupé >>.Les principaux ports utilisés par le protocole 11.323 sont 1720 TCP et suivants, les autres sont négociés dynamiquement

d) Communication entre plusieurs Gatekeeper

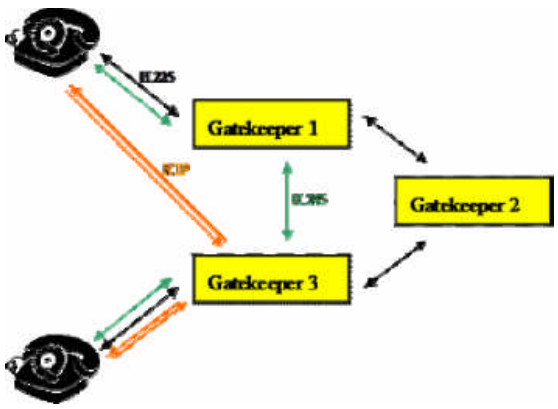


Figure II.27 : Communication avec plusieurs Gatekeeper

Dans cet exemple chaque terminal est rattaché à un gatekeeper de proximité. Tous les gatekeeper de proximité sont rattachés à un gatekeeper qui a une connaissance générale du réseau et qui réalise le routage. On a choisi de faire passer le flux 11245 par les gatekeeper de proximité et le flux RTP par l'un des gatekeeper de proximité **[15]**

II.3 Conclusion

Le protocole H323 est le plus connu et se base sur les travaux de la série H.320 sur la visioconférence sur RNIS. C'est une norme stabilisée avec de très nombreux produits sur le marché (terminaux, gatekeeper, gateway, logiciels). Il existe actuellement cinq versions du protocole (V1 à V5). Le protocole SIP est natif du monde Internet (HTTP) et il est un concurrent direct de l'H323. A l'heure actuelle, il est moins riche que H.323 au niveau des services offerts, mais il suscite actuellement un très grand intérêt dans la communauté Internet et télécom. Le protocole MGCP est complémentaire à H.323 ou SIP, et traite des problèmes d'interconnexion avec le monde téléphonique.

Tableau II.2 comparaison entre les trois protocoles

	H323	SIP	MGCP
Inspiration	Téléphonie	HTTP	&
Nombres d'échanges pour établir la connexion	6 à 7 aller-retour	1 à 5 aller-retour	3 à 4 aller-retour
Complexité	Elevée	Faible	Elevée
Adaptabilité / Modularité protocolaires	Faible	Elevée	Modérée
Implémentation de nouveaux services	NON	OUI	NON
Adapté à Internet	NON	OUI	NON
Protocoles de transport	TCP	TCP ou UDP	TCP ou UDP
Coût	Elevé	Faible	Modéré
Avantages	- Maturité du protocole (Version 4) - Beaucoup de constructeurs utilisent H323	- Interopérabilité très bonne - Bonne gestion de la mobilité	- Bien pour les opérateurs voulant faire du RTC-IP-RTC ou RNIS-IP-RNIS
Inconvénients	- Manque d'interopérabilité entre les différentes implémentations - Difficultés avec les Firewall - Support des fonctions avancées de la téléphonie très complexe	- En pleine maturation - Problème avec la translation d'adresses	- Service supplémentaire de téléphonie inexistant - En pleine maturation
Solution utilisant ce protocole	Livecom	Wengo, Yahoo! Messenger, MSN Messenger, Gizmo, Xlite	Les boîtes : Freebox AsilaBox

Chapitre III

III.1- Introduction

L'objectif de ce chapitre consiste l'étude et le déploiement de la téléphonie IP. Les deux chapitres précédents ont étudié les deux parties nécessaires à la compréhension et la mise en œuvre de la TOIP à un niveau d'abstraction élevé.

III.2- Architecture du réseau existant

L´architecture de réseau où sera déployé notre solution de téléphonie IP est donnée ci-dessous (Figure III.1).

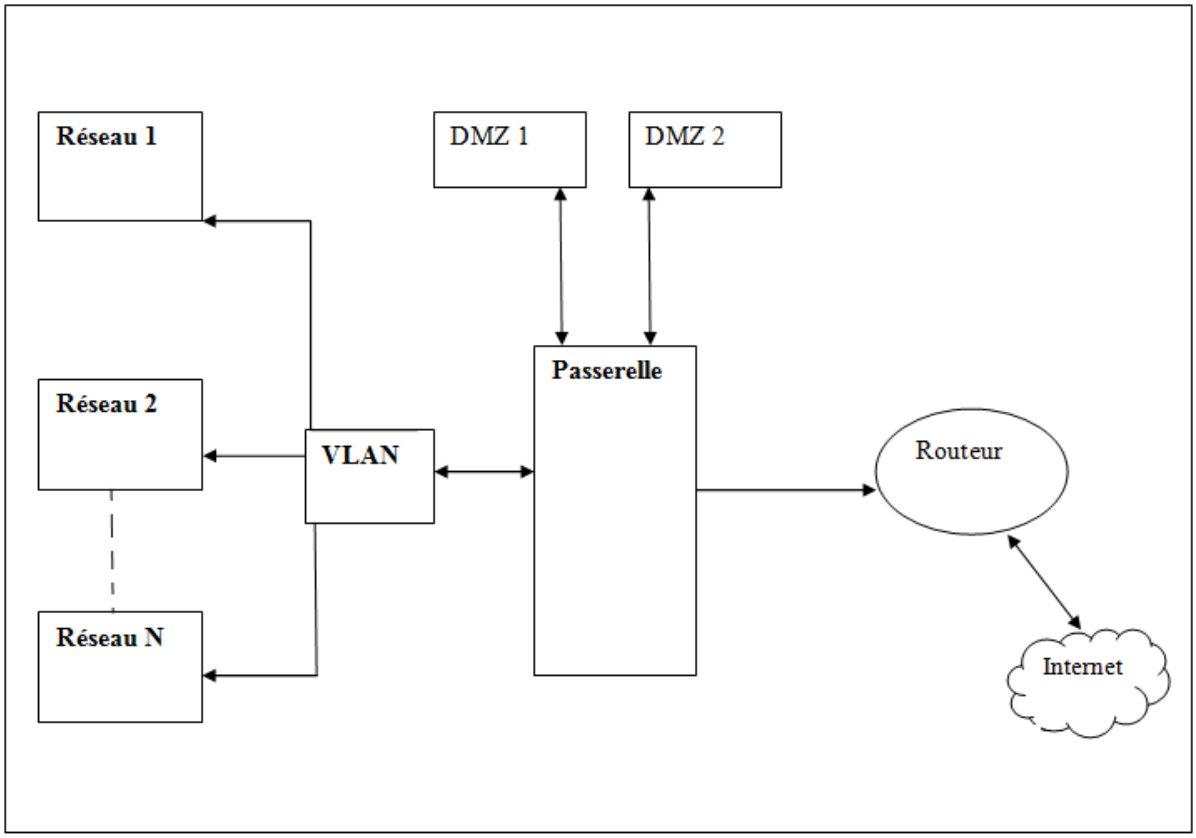


Figure III.1 : architecture du réseau de l´école

On y distingue :

Passerelle :(en anglais, gateway) est un dispositif permettant de relier plusieurs réseaux informatiques, comme par exemple un réseau local et Internet. Ainsi, plusieurs ordinateurs ou l'ensemble du réseau local peuvent accéder à Internet par l'intermédiaire de la passerelle. Elle effectue donc le routage des paquets à l'instar du routeur, mais peut également effectuer des traitements plus évolués sur ceux-ci. Le plus souvent, elle sert également de pare-feu, et de proxy.

VLAN :(Virtual Local Area Network ou Virtual LAN, en français Réseau Local Virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique. En effet dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

DMZ : (**zone démilitarisée**) est un sous-réseau isolé par un pare-feu. Ce sous-réseau contient des machines se situant entre un réseau interne (LAN - postes clients) et un réseau externe (typiquement, Internet). Le nom provient à l'origine de la zone coréenne démilitarisée. Elle se définit aussi comme une zone, un sous-réseau voire une plage d'adresses IP (ou une seule adresse IP) sur un réseau n'étant pas soumise aux règles d'un pare-feu. La DMZ permet à ses machines d'accéder à Internet et/ou de publier des services sur Internet sous le contrôle du pare-feu externe. En cas de compromission d'une machine de la DMZ, l'accès vers le réseau local est encore contrôlé par le pare-feu interne.

Routeur : est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.
Lorsqu'un utilisateur appelle une URL, le client Web (navigateur) interroge le serveur de noms, qui lui indique en retour l'adresse IP de la machine visée.

III.3- Intégration de la téléphonie IP

Pour intégrer une solution de téléphonie IP pour ce réseau. Plusieurs solutions sont possibles aussi bien propriétaires que libre. On cite :

- **Asterisk :** est un PABX open source pour les systèmes UNIX originellement créé en 1999 par Mark Spencer fondateur de la société Digium. Il est aussi disponible sous Microsoft Windows

- **CISCO UC (Unified Communication)** : est un standard intelligent et ouvert, il associe l'infrastructure intelligente à une suite applicative de communication et de collaboration, qui offre la capacité d'améliorer la manière avec laquelle les individus, les groupes interagissent et effectuent des tâches.

-**CallWeaver** : CallWeaver (anciennement connu sous le nom d'OpenPBX) est un logiciel PBX open source qui se veut multiplateforme et libre. Celui-ci, originalement dérivé d'Asterisk, a vu le jour en Septembre 2005. L'idée est survenue au sein de la communauté suite à la pression continue exercée par Digium (entreprise privée) sur Asterisk afin de le contrôler pour ses intérêts personnels. Aujourd'hui, de plus en plus de développeurs tournent leur attention vers CallWeaver (ou autres systèmes similaires), et essayent de participer à son développement.

-**SipX :** SipX est un autocommutateur IP libre pour Linux, Il est Open Source. Il fournit la plupart des fonctionnalités ou services d'un autocommutateur (PABX) classique. Il peut se connecter avec le réseau téléphonique commuté (RTC) par l'intermédiaire des passerelles de VoIP. Sipx fonctionne avec des téléphones ou passerelles utilisant le protocole SIP (Session Initiation Protocol). Ce logiciel est développé par des programmeurs de Pingtel réunis au sein de SIPFoundry.

-**Bayonne :** peut être utilisé comme un système téléphonique de type PABX pour des PME. Cette fonctionnalité est prévue pour la version 1.0 de Bayonne.

Dans ce projet on a intégré la solution Asterisk. Cette application se base elle-même sur des produits libres, Elle se distingue par ses possibilités d´extension (RTC, annuaire).

Le déploiement d'Asterisk consiste à réaliser les 2 schémas illustrés par les figure (III.2.a et III.2.b).

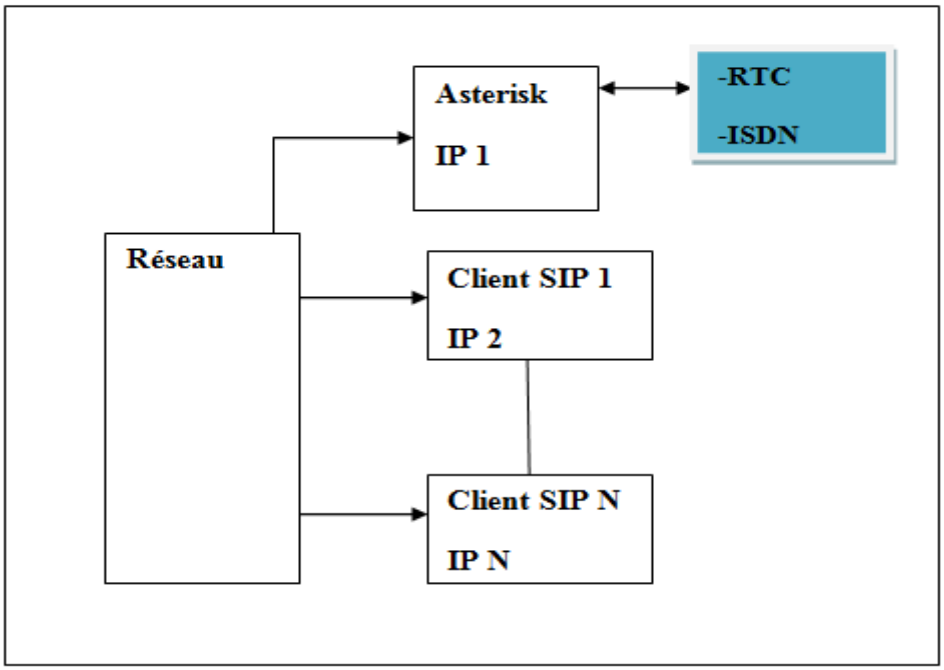


Figure III.2.a : schéma de déploiement d´Asterisk sur le réseau local

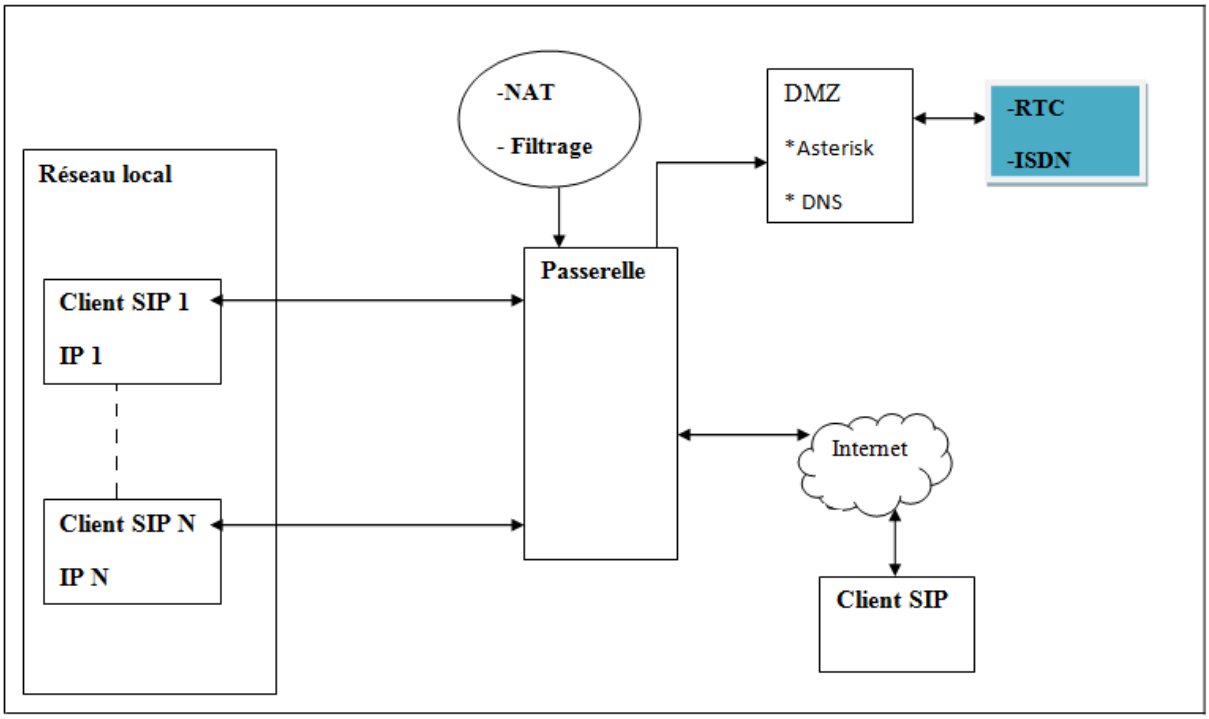


Figure III.2.b : schéma de déploiement d´Asterisk sur un réseau a architecture avancée

Pour la mise en œuvre de ces deux architectures, On a fait appel aux outils suivants

- **Virtual box :** pour l´implémentation d´un serveur virtuel.
- **WIRESHARK** (Ethereal): comme outil d´analyse du trafic réseau.

- **ASTERISK** ou **ASTERISKNOW** (SERVEUR) : couplé à linux pour l´implémentation du serveur VoIP.
- **X-lite** (softphone) : comme client VoIP

III .4- Asterisk et AsteriskNow

III .4.1- Asterisk

Asterisk est un PBX logique complet, Il se compile sous le système d'exploitation Linux et fournit toutes les fonctionnalités d'un PBX traditionnel. Il permet l'accès à des applications de téléphonie aux éléments d'un réseau. Son développeur est Mark SPENCER de Digium.

Néanmoins, Asterisk n'a besoin d'aucun matériel additionnel pour la voix sur IP. Pour l'intercommunication avec l'équipement numérique et analogue de téléphonie, Asterisk doit être muni d'un certain nombre de dispositifs câblés construits par les commanditaires d'Asterisk ''Digium''.

III.4.1.1- INSTALLATION DU PBX ASTERISK

On télécharge la dernière version des codes source Asterisk à partir du site ftp.digium.com/pub. Ces fichiers sont au format compressé tar.gz. Vous aurez besoin des packages suivant :

- asterisk-1.2.0.tar.gz
- asterisk-addons-1.2.0.tar.gz
- asterisk-sounds-1.2.0.tar.gz
- libpri-1.2.0.tar.gz

On déplacer et compile les sources dans le répertoire /usr/src:

```
# cd /usr/src/
# tar  zxvf libpri-1.2.0.tar.gz
# tar zxvf asterisk-1.2.0.ta.gz
# tar zxvf asterisk-sounds-1.2.0.tar.gz
```

Apres décompression nous aurons les répertoires suivants : libpri, asterisk. asterisk-sounds.

III.4.1.2-Compilation libpri

On va dans le répertoire libpri

```
#cd/usr/src/libpri-1.2.0
```

On exécute les commandes:

```
# make clean
```

make

make install

III.4.1.3-Compilation d'asterisk :

On va dans le répertoire d'Asterisk
#cd /usr/src/asterisk-1.2.0
On exécuter les commandes:
make clean
make
make install
make samples

III.4.1.4-Installation d´un module additionnel

Le package asterisk-sounds

#cd/usr/src/asterisk-sounds

#make install

III.4.1.5-Installation de la documentation

make progdocs

III.4.1.6- Démarrage d'Asterisk

Exécuter les commandes :

#asterisk -vvvvc

ou :

/usr/sbin/asterisk -vvvc

Pour Asterisk c'est fini. Il faut maintenant configurer nos softphone pour après pouvoir faire des appels.

III.4.1.7 –Interface de commande

Les commandes CLI

Le binaire asterisk est, par défaut, situé dans /usr/sbin/asterisk. Si vous lancez /usr/sbin/asterisk, il sera chargé comme un daemon, il y'a aussi quelque options à paramétrer qui nous permettent de se connecter à l'interface en ligne de commande CLI d'asterisk, paramétrer la quantité d'information afficher dans le terminale pour explorer la gamme complète d'options, il faut lancer asterisk avec l'option –h

/usr/sbin/asterisk-h

Et pour démarrer Asterisk et se connecter à la CLI on utilise la commande suivante :

/usr/sbin/asterisk-cvvv

III.4.2- Asterisknow (Asterisk interface graphique)

C´est une distribution linux customisée avec Asterisk, qui permet d'installer et contrôler un serveur VoIP facilement et rapidement.

Dans notre travail on a utilisé la version AsteriskNOW-1.0.2.1.

III.4.2.1-Installation d'Asterisk GUI

Pour l´installation d´AsteriskNow on suit les étapes suivantes :

- on télécharge l´image AsteriskNow-1.0.2.1.iso à partir du site

http://www.digium.com/svn/asterisk-gui.

- on utilise Virtual box pour installer AsteriskNow dans une machine virtuelle.

Figure III.3 installation d'AsteriskNow par Virtual box

- d´après l´étude de notre plan d´adressage. On édite la configuration réseau de notre serveur comme suit :

  -IP : 192.168.0.50

-masque IP : 255.255.255.0

-passerelle : 192.168.0.1

-DNS : 192.168.0.1

-reseau : 192.168.0.0

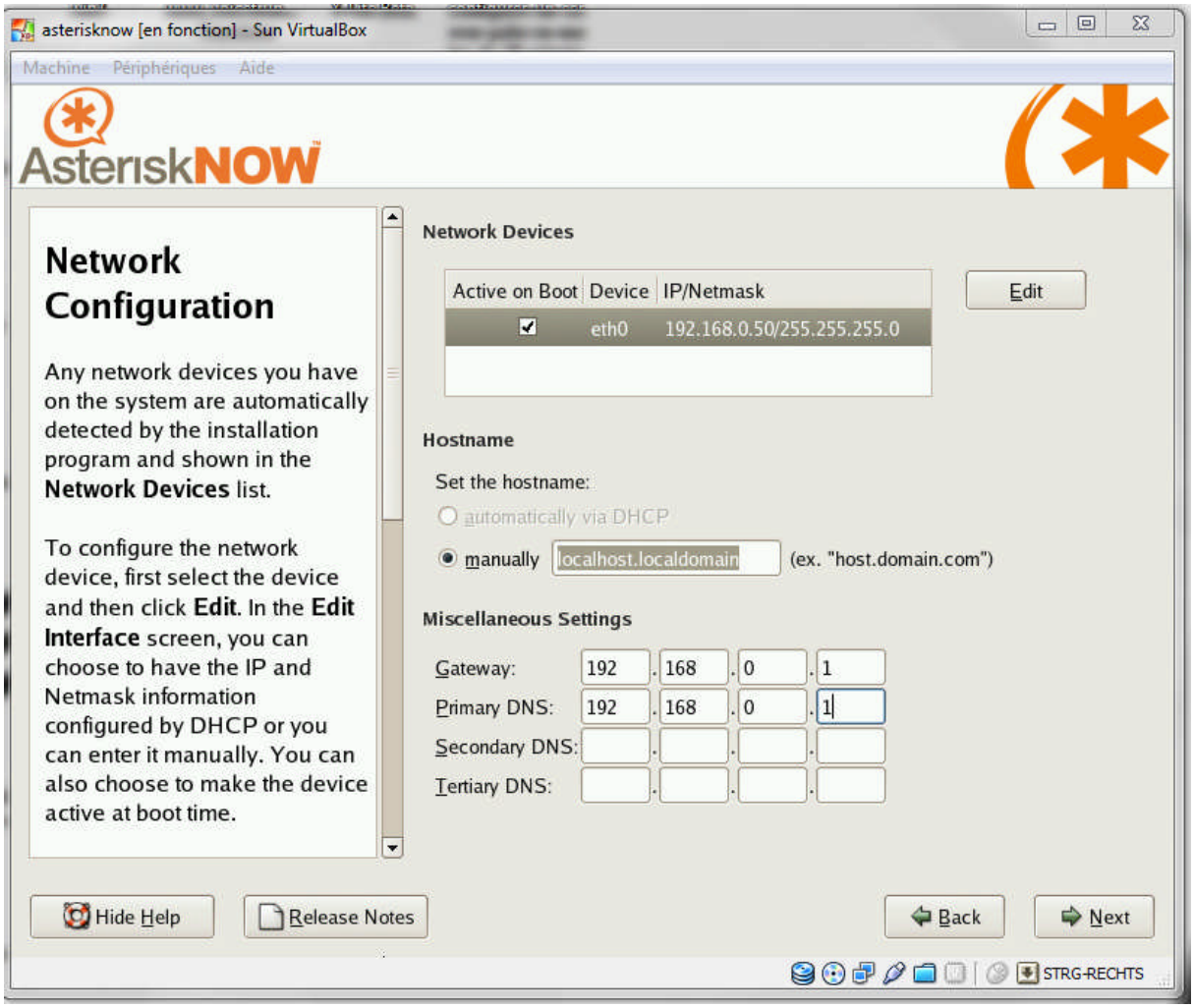


Figure III.4.la configuration réseau d´ AsteriskNow

- après la fin de l´installation on lance notre serveur AsteriskNow

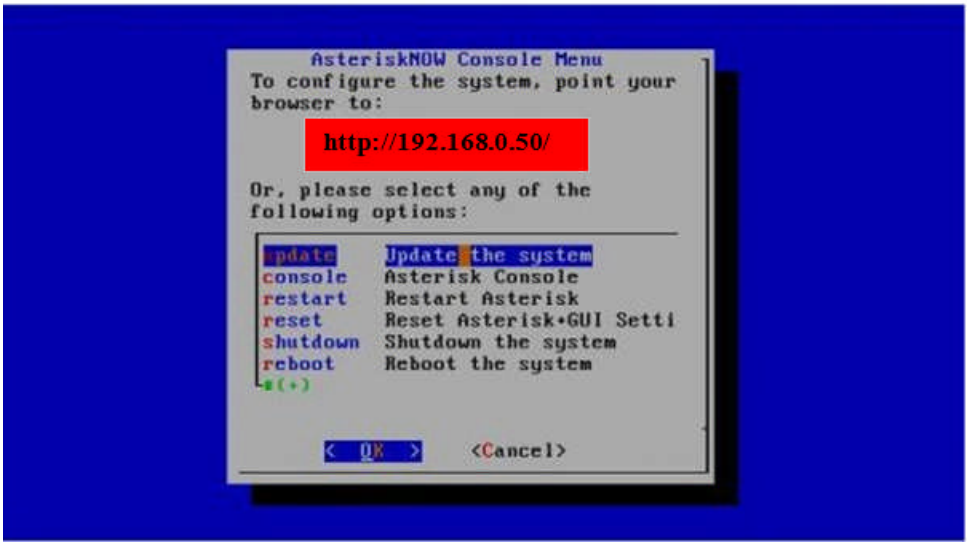


Figure III.5-le menu d AsteriskNow

III .4.2.2-la configuration et l´utilisation d AsteriskNow

Pour utiliser le GUI, on accède à cette adresse :

http:// 192.168.0.50 /asterisk/static/config/cfgbasic.html

On utilise le login administrateur et le mot de passe que vous avez enregistré lors de l'installation d´AsteriskNow, une fois connecté par le biais du serveur web sur l'interface graphique on peut rajouter des utilisateurs et configurer les sortes de codecs utilisés comme nous pouvons configurer la boite vocale et des conférences audio et choisir le protocole de communication soit SIP, IAX, comme montré sur la figure.

Dans la case **FILE EDITOR,** on fait la configuration SIP et EXTENSION

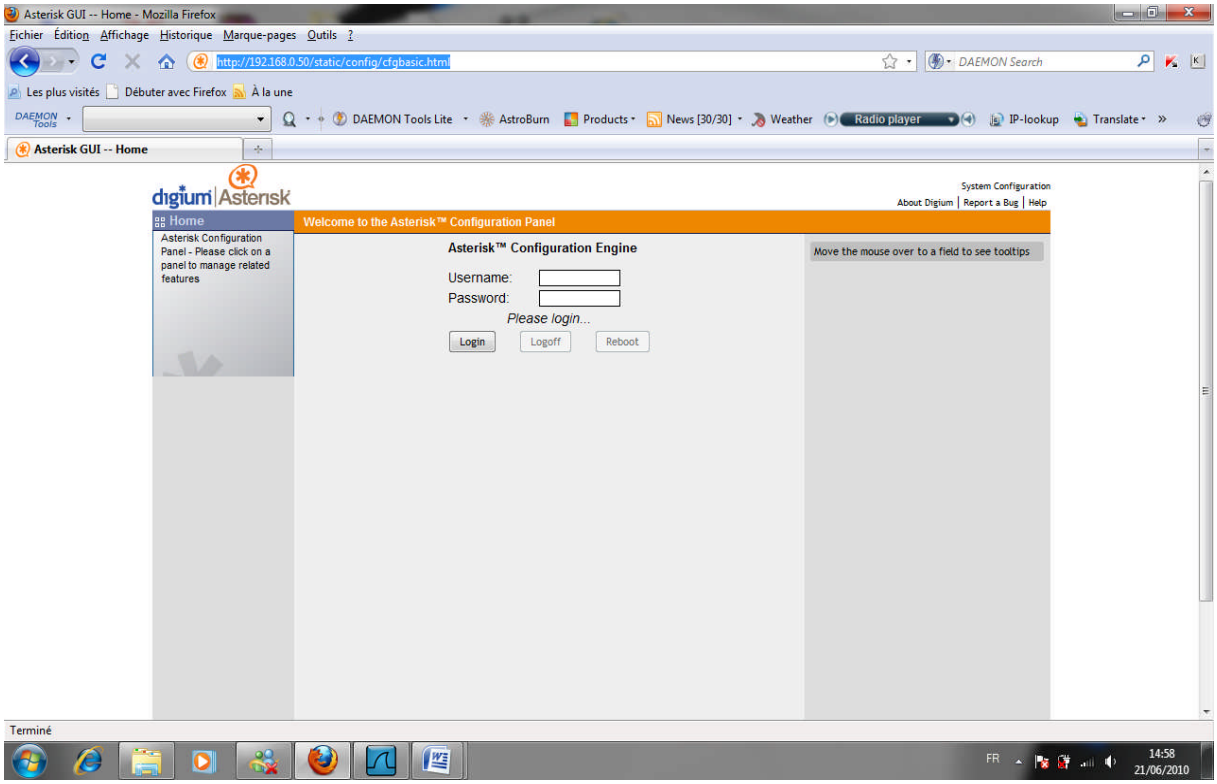


Figure III.6- Interface graphique pour configure les paramètres Asterisk

III.4.3-Fonctionnalités :

Asterisk offre les fonctionnalités suivantes :

- Messagerie vocale
- Conférence téléphonique
- Répondeur vocal interactif
- Mise en attente d'appels
- Services d'identification de l'appelant
- VoIP

III.4.4- Architecture interne :

Asterisk est composé d'un noyau central de commutation, de quatre API (Interface de programmation d'applications) de chargement modulaire des applications téléphoniques, des Interfaces matérielles, de traitement des formats de fichier, et des codecs. Il assure la commutation transparente entre toutes les interfaces supportées, permettant à cette commutation de relier entre eux une diversité de systèmes téléphoniques en un unique réseau commuté.

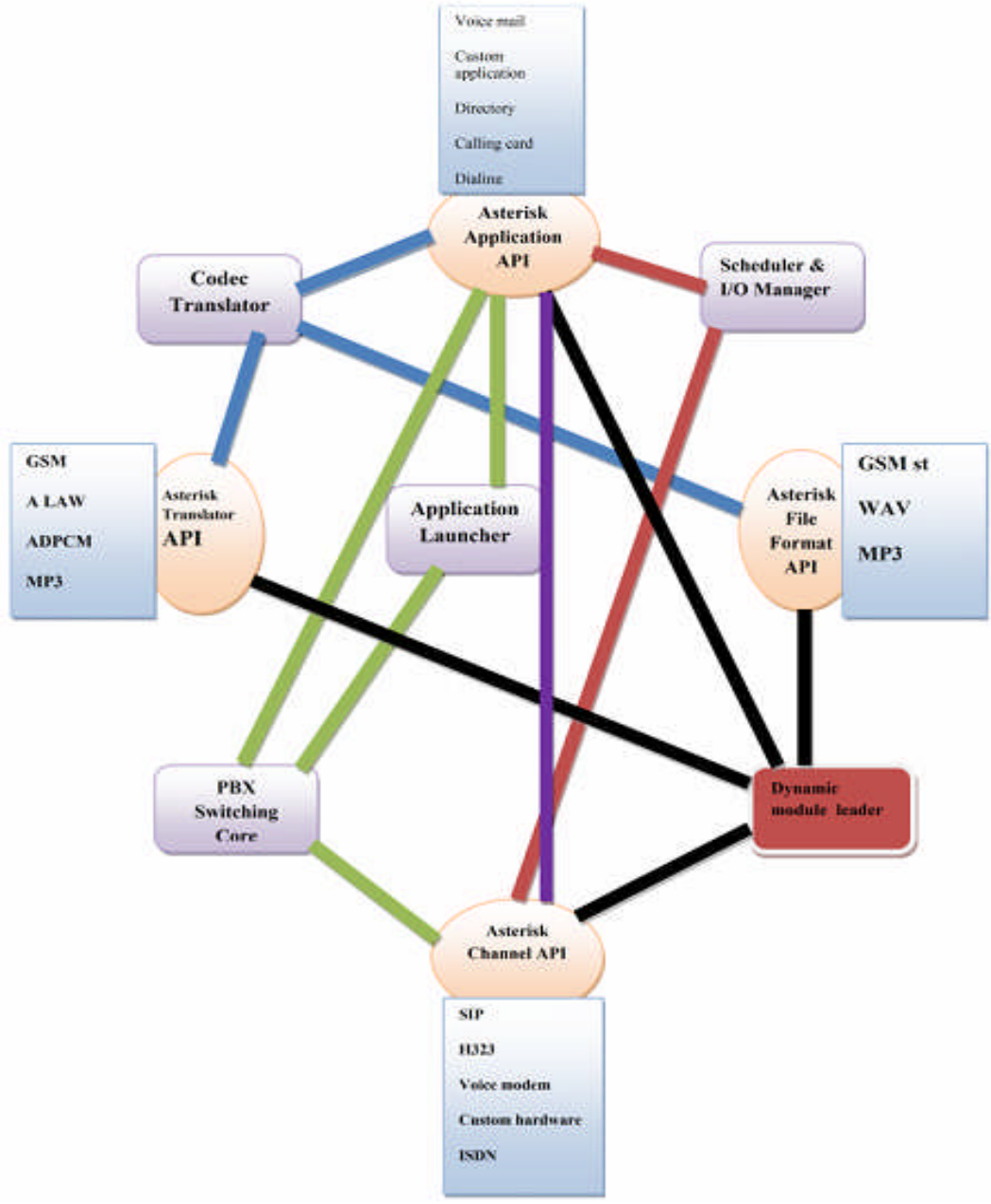


Figure III.7 Architecture interne d´ Asterisk

III.4.4.1-Principales fonctions

- **PBX Switching Core :** Système de commutation de central téléphonique privé, reliant ensemble les appels entre divers utilisateurs et des tâches automatisées. Le noyau de commutation relie d'une manière transparente des appels arrivant sur diverses interfaces de matériel et de logiciel.
- **Application Launcher :** les applications qui assurent des services pour des usagers, tels que la messagerie vocale, la lecture de messages et le listage de répertoires (annuaires).
- **Codec Translator :** Utilise des modules de codec pour le codage et le décodage de divers formats de compression audio utilisés dans l'industrie de la téléphonie. Un certain nombre de codecs sont disponibles pour palier aux divers besoins et pour arriver au meilleur équilibre entre la qualité audio et l'utilisation de la bande passante.
- **Scheduler & I/O Manager :** Ils traitent la planification des tâches de bas niveau et la gestion du système pour une performance optimale dans toutes les conditions de charge.

III.4.4.2-Les APIs

- **Asterisk Application API :** Elle autorise différents modules de tâches à être lancé pour exécuter diverses fonctions. Communication, audioconférence, pagination, liste d'annuaire, messagerie vocale, transmission de données intégrée, et n'importe quelle autre tâche qu'un système PBX standard exécute actuellement ou exécuterait dans l'avenir, sont mises en œuvre par ces modules distincts.
- **Asterisk Translator API :** Charge les modules de codec pour supporter divers formats de codage et de décodage audio tels que le GSM, la Mu-Law, l'A-Law, et même le MP3.
- **Asterisk Channel API :** Cette API gère le type de raccordement sur lequel arrive un appelant, que ce soit une connexion VoIP, un RNIS, un PRI, une signalisation de bit dérobé, ou une autre technologie. Des modules dynamiques sont chargés pour gérer les détails de la couche basse de ces connexions.
- **Asterisk File Format API :** Elle permet la lecture et l'écriture de divers formats de fichiers pour le stockage de données dans le file system. Sa particularité modulaire

permet à Asterisk d'intégrer de façon continue le matériel de commutation téléphonique actuellement mise en œuvre, et les technologies de Voix par paquet en constante augmentation, émergeant aujourd'hui.

La capacité de charger des modules de codec permet à Asterisk d'être compatible avec le codec extrêmement compact nécessaire à la Voix sur IP sur des connexions lentes comme un modem téléphonique tout en maintenant une haute qualité audio sur des types de connexion moins "étroites".

III.4.5-Fonctionnement évolué

Asterisk ne permet pas seulement l'utilisation d'équipements traditionnels de téléphonie, il augmente aussi en nombre leurs capacités. En utilisant le protocole de voix sur IP Inter-Astérix eXchange (IAX ou inter central Asterisk) .Asterisk mêle progressivement la voix et le trafic de données à travers des réseaux disparates. Tant que l'on transporte la voix par paquets, il est possible d'envoyer des données telles que des documents URL et des images, en conformité avec le trafic Voix, permettant ainsi une intégration plus grande des informations. **[18]**

III.4.6- Asterisk en réseau

Un réseau de téléphonie IP local doit intégrer : un serveur de téléphonie IP et des terminaux permettant la communication qui peuvent être soit des téléphones matériel IP ; soit des téléphones analogiques munis d'un adaptateur qui les transforme en téléphones IP ou même des téléphones logiciels (softphone) installés sur ordinateur. Asterisk peut assurer le routage des appels, les services et toutes les fonctions d'un serveur VoIP, en plus de la possibilité de se connecter à différents réseaux téléphoniques existants.

Un serveur Asterisk peut en effet être connecté à un réseau téléphonique :

- soit à un réseau téléphonique commuté (RTC)
- soit à un réseau RNIS (ISDN)

Ces connexions ne peuvent être possibles qu'après avoir équiper le serveur Asterisk de cartes spécialisées disponibles selon le nombre de lignes à connecter. Des cartes qu'il faut, bien évidemment configurer au niveau des fichiers de configurations d'ASTERISK.

III.4.7-Configuration de sip.conf et extensions.conf

Dans ce projet on a choisi le protocole SIP.

Asterisk doit aussi reconnaitre nos softphone pour cela les fichiers sip.conf et extensions.conf doivent être configuré

/ etc/asterisk/sip.conf

[general] ; configuration globale

port=5060 ; port d'écoute du protocole SIP

*** Début de configuration des clients***

[fouzi] ; Nom de connexion du client

username=fouzi ; nom d'utilisateur

secret=monCodeSecret ; mot de passe du compte

type= friend ; type de compte associé.

host=dynamic ; définition du mode d'attribution d'IP

nat=yes ;_ activation du NAT

context=interne ; permet de relayer vers les règles de routage dans extensions.conf

callerid= fouzi e <101> ; Identité de l'appelant et numéro d'extension

Puis dans le fichier /etc/asterisk/extensions.conf ajoutez les lignes suivantes:

Exten => **numero_du_telephone1**, 1, Dial (SIP/Phone1, 20, tr)

Exten => **numero_du_telephone2**, 1, Dial (SIP/Phone2, 20, tr)

Il existe trois types de comptes dans Asterisk :

- peer : Compte permettant uniquement d'appeler
- user : Compte permettant d'être appeler uniquement
- friend : Compte permettant d'appeler et d'être appeler

III.5-Les softphone (X-lite)

Ils jouent le rôle d'un téléphone IP de manière logiciel. Il requière un système de son (carte son, baffles, micro,...) pour l'utiliser. Ces clients permettent de remplacer des téléphones IP matériels onéreux. Beaucoup de clients sont plus au moins évolues, cependant certains sont

des clients propriétaire et ne sont pas utilisables avec Asterisk. Alors dans notre étude nous allons utiliser:

- **X-lite :** Ce client est un des plus abouti en termes de fonctionnalités, de fiabilités et de simplicité. Il permet la gestion de contacts et de groupes et fait également la messagerie instantanée. Il existe en version payante (EyeBeam) (Plusieurs comptes SIP, support de la vidéo,...). Il fonctionne également sous Windows. **[20]**

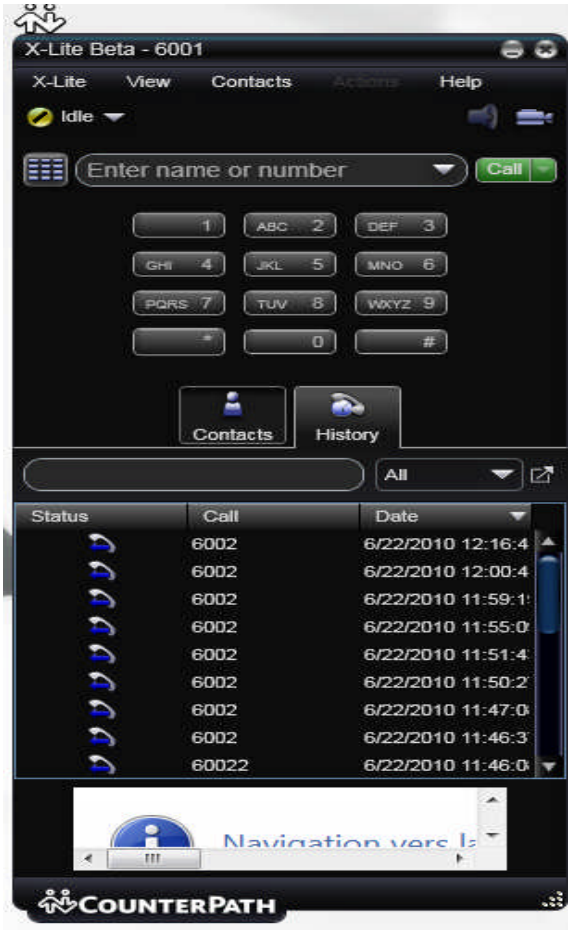


Figure III.8. X-lite (softphone)

III.5.1- configuration de X-lite

La fenêtre de configuration des comptes SIP s'ouvre, cliquez sur "X-lite" puis sur ``SIP Account´´ pour ajouter vos paramètres personnels.

Veuillez indiquer les paramètres comme ceci :

- Account Name = votre nom
- User ID= votre identification
- Password = Votre mot de passe SIP

• Authorization user name = Votre Login SIP

• Domain = 192.168.0.50 :5060

• Domain Proxy = 192.168.0.50 :5060

• Appliquez les modifications et quittez le menu des comptes SIP.

5060 c´est le port SIP.

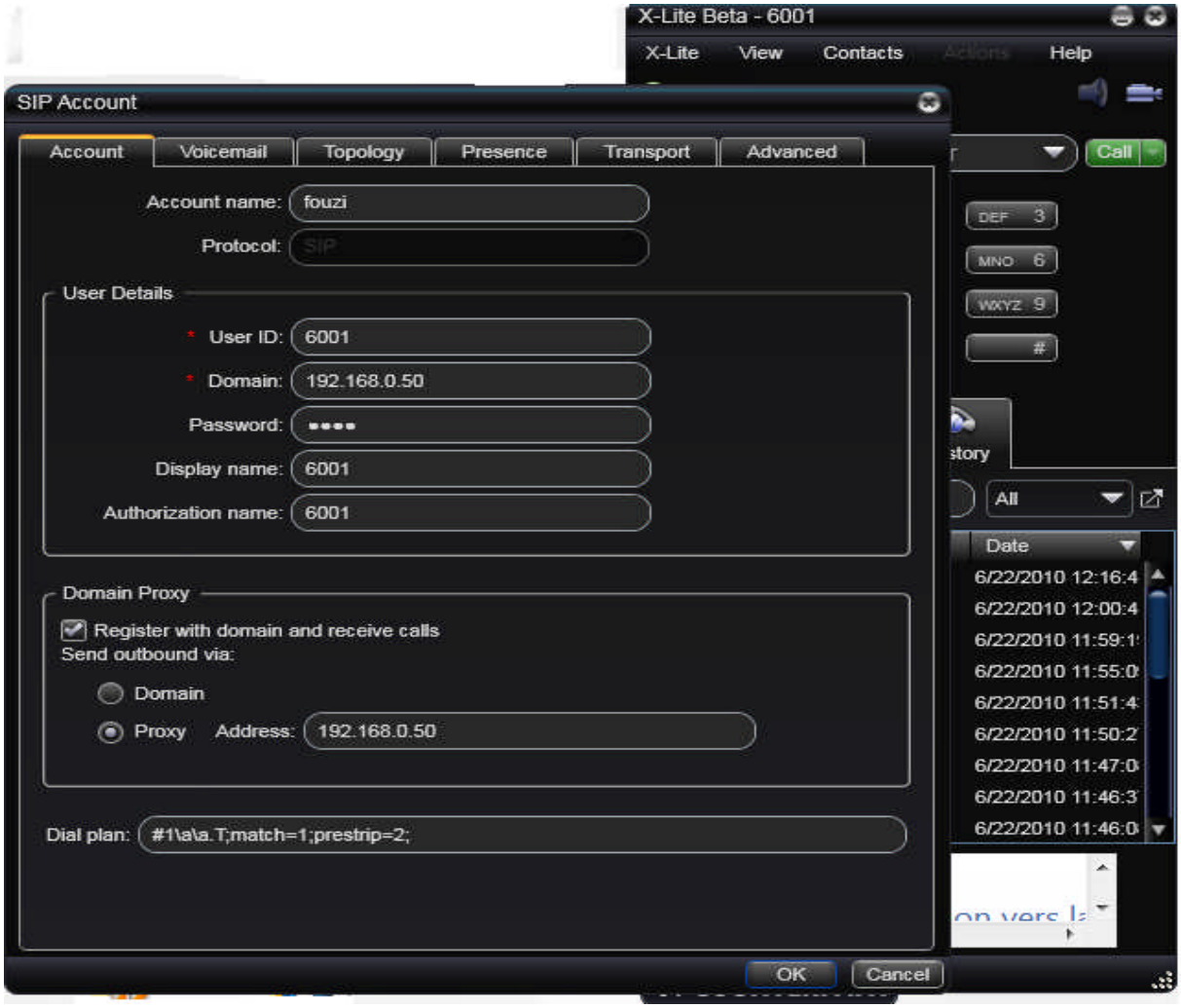
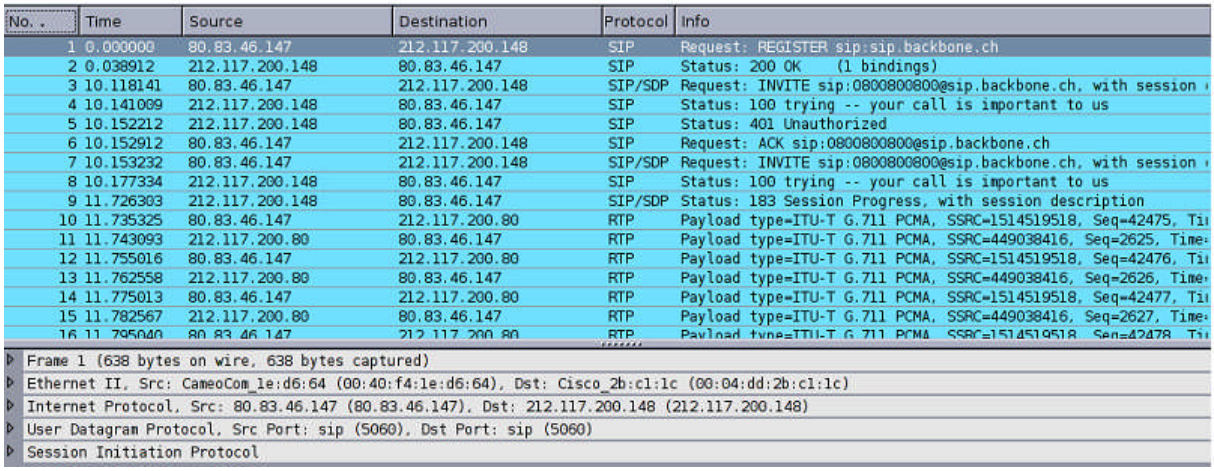


Figure III.9. Interface graphique pour configurer X-lite

III.7-Analyseur de trafic Wireshark

Wireshark est un outil d'analyse réseau qui va nous permettre d'analyser de bout en bout, c'est à dire de suivre de l'émission à la réception le trafic VoIP établi lors des tests en charge.



No.	Time	Source	Destination	Protocol	Info
1	0.000000	80.83.46.147	212.117.200.148	SIP	Request: REGISTER sip:sip.backbone.ch
2	0.038912	212.117.200.148	80.83.46.147	SIP	Status: 200 OK (1 bindings)
3	10.118141	80.83.46.147	212.117.200.148	SIP/SDP	Request: INVITE sip:0800800800@sip.backbone.ch, with session
4	10.141009	212.117.200.148	80.83.46.147	SIP	Status: 100 trying -- your call is important to us
5	10.152212	212.117.200.148	80.83.46.147	SIP	Status: 401 Unauthorized
6	10.152912	80.83.46.147	212.117.200.148	SIP	Request: ACK sip:0800800800@sip.backbone.ch
7	10.153232	80.83.46.147	212.117.200.148	SIP/SDP	Request: INVITE sip:0800800800@sip.backbone.ch, with session
8	10.177334	212.117.200.148	80.83.46.147	SIP	Status: 100 trying -- your call is important to us
9	11.726303	212.117.200.148	80.83.46.147	SIP/SDP	Status: 183 Session Progress, with session description
10	11.735325	80.83.46.147	212.117.200.80	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1514519518, Seq=42475, Ti
11	11.743093	212.117.200.80	80.83.46.147	RTP	Payload type=ITU-T G.711 PCMA, SSRC=449038416, Seq=2625, Time
12	11.755016	80.83.46.147	212.117.200.80	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1514519518, Seq=42476, Ti
13	11.762558	212.117.200.80	80.83.46.147	RTP	Payload type=ITU-T G.711 PCMA, SSRC=449038416, Seq=2626, Time
14	11.775013	80.83.46.147	212.117.200.80	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1514519518, Seq=42477, Ti
15	11.782567	212.117.200.80	80.83.46.147	RTP	Payload type=ITU-T G.711 PCMA, SSRC=449038416, Seq=2627, Time
16	11.795040	80.83.46.147	212.117.200.80	RTP	Payload type=ITU-T G.711 PCMA, SSRC=1514519518, Seq=42478, Ti

Frame 1 (638 bytes on wire, 638 bytes captured)
Ethernet II, Src: CameoCom_1e:d6:64 (00:40:f4:1e:d6:64), Dst: Cisco_2b:c1:1c (00:04:dd:2b:c1:1c)
Internet Protocol, Src: 80.83.46.147 (80.83.46.147), Dst: 212.117.200.148 (212.117.200.148)
User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
Session Initiation Protocol

Figure III.10- analyseur réseau Wireshark

D´aprés le test de wireshark.On obtient le schéma suivant :

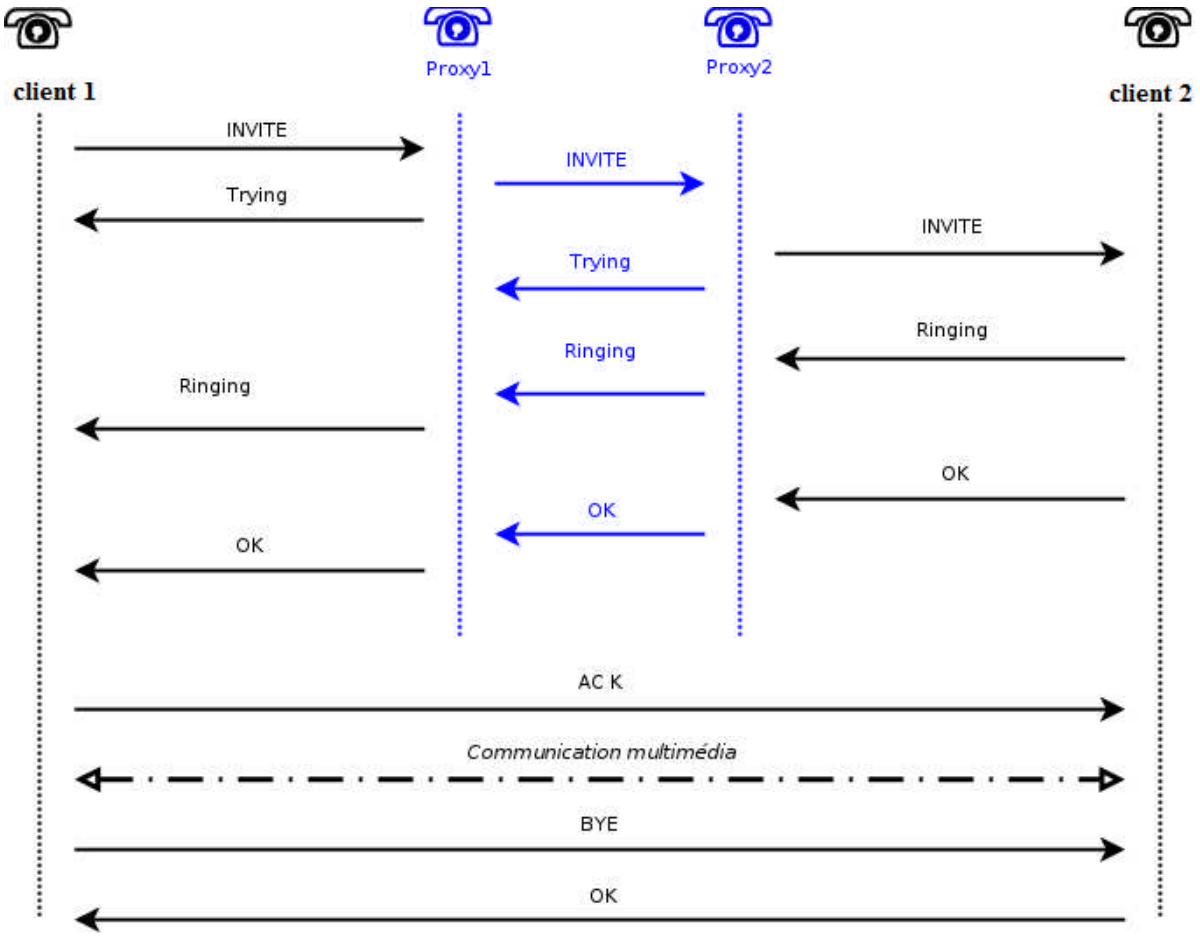
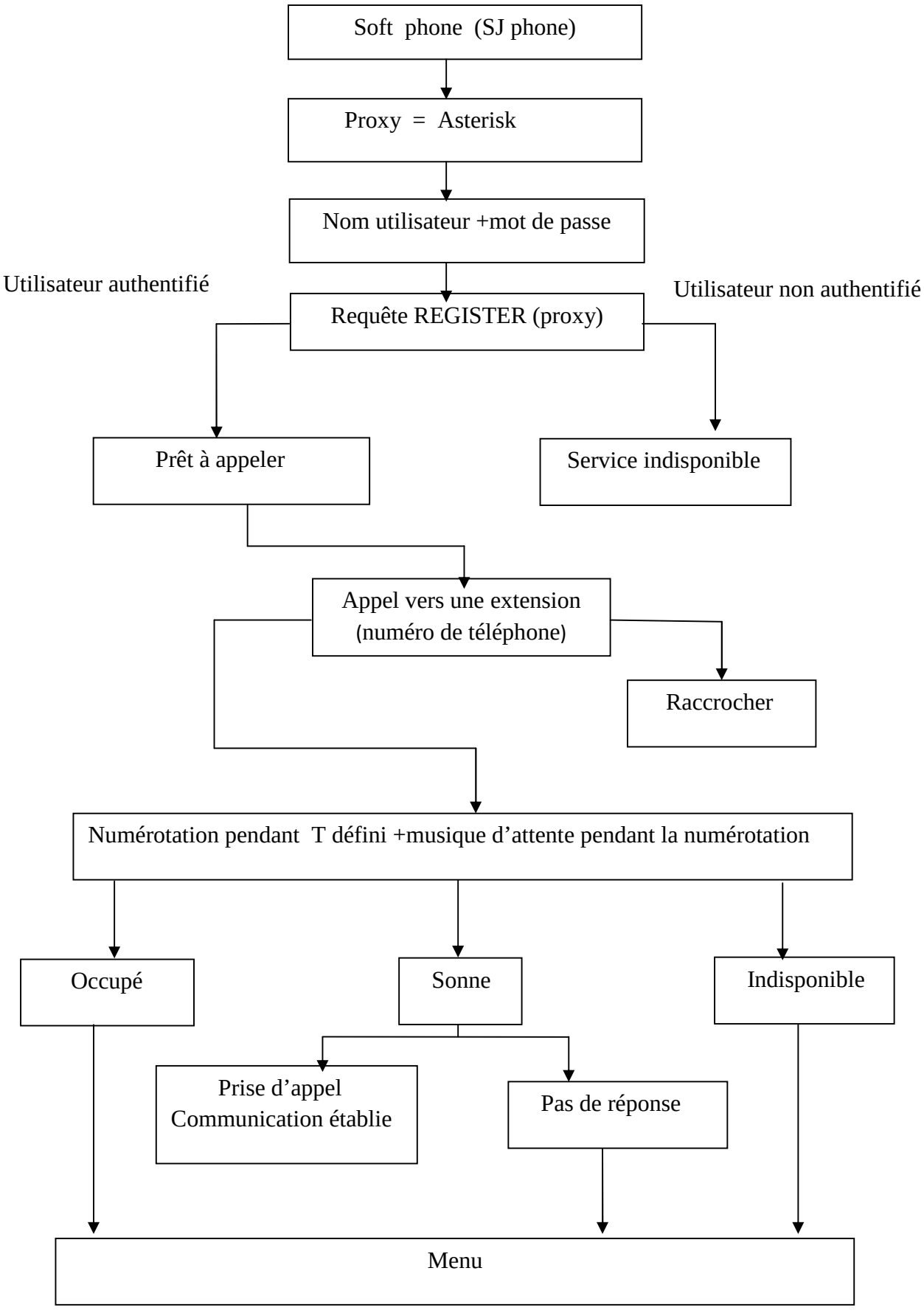


Figure III.11- schéma de communication

III.8 -schéma de l'acheminement d'appel



III.9-conclusion

A travers cette application, nous avons pu voir en premier lieu l'architecture interne d'Asterisk, et les différentes architectures en réseaux qui peuvent l'intégrer. Nous avons constaté qu'il présente une flexibilité remarquable vu sa capacité à supporter différentes technologies. Nous avons abordé, ensuite, les notions principales qui nous ont permis d'installer, configurer notre solution.

Nous avons fini avec un exemple d'applications que nous avons utilisées pour mettre en œuvre quelques unes des fonctionnalités des PBX à savoir : la musique d'attente, la messagerie vocale, …….).

Conclusion générale

Dans ce mémoire, nous avons eu à faire une configuration, et une réalisation d´un service de téléphone IP en configurant le serveur Asterisk du centre de calcul de l´école, et avec des softphone, on a instauré une communauté de postes clients pour leurs permettre de communiquer dans un réseau local.

Pour cela, on a suivi le téléphone IP dans son développement avec ses différents protocoles, son concept en prenant en compte les problématiques de la sécurité, la disponibilité, la gestion, le contrôle et la qualité de service.

L´architecture dédiée à la téléphonie IP est regroupée dans deux types principaux : architecture centralisée et ce qui nous intéresse plus l´architecture distribuée qui est régie par les protocoles H.323 et SIP, ce dernier a été l´objet de notre étude.

Finallement, notre travail a vu l´implantation du service Asterisk dans le serveur de l´école ce qui a donné la possibilité d´établir une télécommunication dans le réseau local de l´école. La technologie Asterisk permet d´offrir de nombreuses possibilités de développement dans le domaine de la téléphonie.

Perspective

‘ …N’oublions pas que les gouttes d’eau remplissent les océans…’

La téléphonie IP est une technologie de grande envergure, chaque jour nous assistons à de nouvelles améliorations (telle que la qualité de voix….) pour s´adapter aux exigences des clients.

Dans cette évolution, plusieurs technologies apparaissent à l´horizon, ce qui nous a permis d´établir de nouvelles perspectives d´utilisation du téléphone IP telles que :

- ✓ L´installation et la configuration des hardphones.
- ✓ L´étude de la nouvelle technologie qui lie les différents réseaux de communication (téléphone IP, GSM, téléphone fixe).

API (Interface de programmation d'applications - Applications Programming Interface) : Une API a pour objet de faciliter le travail d'un programmeur en lui fournissant les outils de base nécessaires à tout travail à l'aide d'un langage donné. Elle constitue une interface servant de fondement à un travail de programmation plus poussé.

Commutation de circuits : La commutation de circuits est un des modes d'établissement pour une liaison de télécommunication. C'est le moyen historique le plus ancien utilisé dans les équipements de commutation de ligne de téléphone. Un chemin physique ou logique est établi entre deux équipements et bloqué pour toute la durée de la communication.

CRM : Le CRM est un ensemble de processus et d'outils permettant une approche globale qui vise à apporter une réponse adaptée aux attentes du client ou du prospect, par l'intervenant compétent, au moment opportun et à travers le bon canal. Cette stratégie client peut être appuyée par des outils permettant de mieux gérer l'ensemble des composantes de la relation client : Les ventes (SFA ou Sales Force Automation), le marketing et le service client (Support, Hot Line, SAV).

DHCP (Dynamic Host Configuration Protocol) :DHCP est un terme anglais désignant un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres TCP/IP d'une station, notamment en lui assignant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS et des serveurs de noms NBNS (connus sous le noms de serveurs WINS sur les réseaux de la société Microsoft).

Diffserv : Le modèle IntServ est difficilement applicable dans le cas de grands réseaux. En effet, il est difficile de maintenir un état de ressources réseau pour chaque flux si le chemin emprunté change fréquemment. cela est du au fait que le routage est indépendant de la gestion de QoS. Ce problème de stabilité ne se pose pas dans les réseaux ATM grâce à l'utilisation d'un routage hiérarchique incluant la QoS: PNNI hiérarchique.Le modèle DiffServ consiste à classer le trafic grâce à un code présent dans le paquet IP. On applique ensuite des traitements différenciés aux différentes classes de trafic. Nous avons donc affaire à une granularité moins fine mais qui devient en revanche plus scalable.

DNS (Domain Name System) : est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine et, plus généralement, de trouver une information à partir d'un nom de domaine.

Fibre optique : une fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire la lumière et sert dans les transmissions terrestres et océaniques de données. Elle a un débit d'informations nettement supérieur à celui des câbles coaxiaux et supporte un réseau « large bande » par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

HTML (HypertextMarkupLanguage) : est un langage informatique de balisage conçu pour écrire les pages Web, et notamment pour créer de l'hypertexte, d'où son nom. HTML permet de structurer sémantiquement le contenu des documents et d'inclure et lier des ressources multimédia, sans compromettre l'accessibilité du Web avec une très large gamme d'équipements. Il peut être utilisé conjointement avec des langages de programmation comme Java Script et des feuilles de style comme les feuilles de style en cascade (CSS). HTML est une application du Standard GeneralizedMarkupLanguage (SGML), tandis qu'une évolution appelée XHTML est une application de l'Extensible MarkupLanguage (XML).

IEEE 802.11 :IEEE 802.11 est un terme qui désigne un ensemble de normes concernant les réseaux sans fil qui ont été mises au point par le groupe de travail 11 du Comité de normalisation LAN/MAN de l'IEEE (IEEE 802). Le terme 802.11x est également utilisé pour désigner cet ensemble de normes et non une norme quelconque de cet ensemble comme pourrait le laisser supposer la lettre « x » habituellement utilisée comme variable. Il n'existe donc pas non plus de norme seule désignée par le terme 802.11x. Le terme IEEE 802.11 est également utilisépour désigner la norme d'origine 802.11, et qui est maintenant appelée parfois 802.11legacy (legacy en anglais veut dire héritage)

IETF: Internet Engineering Task Force. Comité de réflexion concernant les normes à utiliser pour les échanges sur Internet.

IntServ : Le modèle Intserv / RSVP Le but du groupe de travail Intserv de l'IETF est la transformation de l'Internet actuel en un réseau à intégration de services. L'architecture Intserv s'organise autour du concept de flot de données correspondant à un ensemble de paquets résultant d'une application utilisatrice et ayant un besoin d'une certaine QoS. Afin de satisfaire la QoS requise, Intserv propose d'effectuer une réservation des ressources nécessaires à l'établissement de celle-ci via le protocole de réservation de ressources nommé RSVP. Le signal RSVP étant constitué par l'information de contrôle de la QoS, celui-ci propose des directives afin de mettre en place la réservation mais ne dit pas comment la mettre en place,

ce domaine étant réservé aux routeurs du réseau qui prennent en compte la signalisation RSVP

IP (Internet Protocol) :IP est un protocole utilisé pour le routage des paquets sur les réseaux. Son rôle est de sélectionner le meilleur chemin à travers les réseaux pour l'acheminement des paquets. IP est un protocole de niveau 3 du modèle OSI (niveau 2 du modèle TCP/IP)permettant un service d'adressage unique pour l'ensemble des terminaux connectés.

IP gateways (passerelle IP) : Machine ou équipement routeur permettant de changer de réseau IP

IP-PBX (Internet Protocol - PrivateBranch eXchange) :IP-PBX est la version "IP" du PABX. Il gère la plupart des communications en interne grâce à l'infrastructure réseau de l'entreprise. Il sert aussi (quand la fonction est incluse dans le système) de lien avec les lignes téléphoniques externes. Certains IPbx sont logiciels alors que d'autres ne sont que des boîtes noires bourrées d'électronique. Il a, de plus, la possibilité de faire toutes les fonctions classiques présentes sur un PABX (renvois d'appels, mises en attente avec musique, etc.).

IVR (Interactive Voice Response) : un IVR est un système de réponse automatique personnalisable proposant à l'appelant une liste de services. L'IVR (Interactive Voice Response) est une technologie permettant une interaction entre un téléphone et une base de données afin d'obtenir des informations ou de générer des actions en pressant des touches sur le téléphone. Ce système peut être utilisé par exemple pour saisir un code PIN ou le numéro de téléphone d'un correspondant.

LAN (Local Area Network) : un réseau local est un réseau informatique reliant des ordinateurs (mais aussi d'autres types de matériels comme des imprimantes par exemple) déployé à une échelle géographique limitée.

Linux : est le nom du noyau de système d'exploitation libre, multitâche, multiplate-forme et multi-utilisateur de type UNIX créé par Linus Torvalds, souvent désigné comme le noyau Linux. Par extension, Linux désigne couramment le système d'exploitation libre combinant le noyau et un ensemble d'utilitaires systèmes. Pour désigner cet ensemble, la Free Software Foundation (FSF) soutient la désignation GNU/Linux afin de rappeler que le noyau Linux est généralement distribué avec de nombreux logiciels ainsi que l'infrastructure du projet GNU. Pour l'utilisateur final, Linux se présente sous la forme d'une distribution Linux, c'est-à-dire

du système d'exploitation accompagné d'une collection de logiciels très variés. Originellement développé pour les compatibles PC, Linux est utilisé sur tous types de matériel, du téléphone portable au superordinateur. Son premier marché est celui des serveurs informatiques, suivi par les systèmes embarqués. Sa part d'utilisation sur ordinateur personnel est de l'ordre dupourcent. La mascotte de Linux est Tux, un manchot.

MAN : Réseau métropolitain (MAN -Metropolitan Area Network)
• Généralement dans une même ville (entre le LAN et le WAN)
• Support de transmission : câble coaxial ou fibre optique vitesse > 1 Mbps

Messagerie instantanée : est un dispositif informatique qui permet l'échange instantané de messages textuels entre plusieurs ordinateurs connectés au même réseau informatique, le plus communément celui de l'Internet. Contrairement au courrier électronique, ce moyen de communication est caractérisé par le fait que les messages externes s'affichent en quasi-temps-réel et permettent un dialogue interactif.

PABX ou PBX : Un PABX sert principalement à relier les postes téléphoniques d'un établissement (lignes internes) avec le réseau téléphonique public (lignes externes). Il permet en plus la mise en œuvre d'un certain nombre de fonctions notamment relier plus de lignesinternes qu'il n'y a de lignes externes, permettre des appels entre postes internes sans passer par le réseau public, programmer des droits d'accès au réseau public pour chaque poste interne, proposer un ensemble de services téléphoniques (conférences, transferts d'appel, renvois, messagerie, appel par nom...), gérer les SDA (Sélection Directe à l'Arrivée), gérer la ventilation par service de la facture téléphonique globale (taxation), apporter des services de couplage téléphonie informatique (CTI) tels que la remontée de fiche essentiellement via le protocole CSTA.

PDA :PDA est un assistant personnel ou ordinateur de poche est un appareil numérique portable, souvent appelé par son sigle anglais PDA pour Personal Digital Assistant. La première utilisation publique de ce terme remonte au 7 janvier 1992 lors du Consumer Electronics Show à Las Vegas (Nevada) où John Sculley (alors PDG d'Apple) présenta le Newton. Selon la définition qu'on leur donne, les premiers PDA (qui n'en portaient donc pas encore le nom) sont le Wizard OZ-7000 de Sharp, le Portfolio d'Atari (1989), le Refalo de Kyocera (1990) ou le Series 3 de Psion (1991).

Q.931 : La recommandation ITU-T Q.931 traite des procédures pour établir, maintenir et terminer une connexion RNIS. Les fonctions et procédures sont décrites de manière générale dans les recommandations Q.930/I.450.

QoS (Qualité de Service) : est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transit, taux de perte de paquets…Son but est ainsi d'optimiser les ressources du réseau et de garantir de bonnes performances aux applications critiques. La Qualité de Service sur les réseaux permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par application. Elle permet ainsi aux fournisseurs de services (départements réseaux des entreprises, opérateurs…) de s'engager formellement auprès de leurs clients sur les caractéristiques de transport des données applicatives sur leurs infrastructures IP.

SCCP (Skinny Client Control Protocol) : est un protocole de communication. Le H.323 étant trop rigoureux pour certaines utilités de la téléphonie IP (comme le renvoi d'appel, le transfert, la mise en attente), Cisco a mis en place ce protocole beaucoup plus léger qu'est le SCCP (il utilise le port 2000). L'avantage de Skinny est qu'il utilise des messages prenant très peu de bande passante c'est pourquoi il est utilisé pour les communications entre les téléphones IP et le CallManager ainsi que pour contrôler une conférence.

Serveurs de messageries : Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie, soit un courrielleur web, qui se charge de contacter le serveur pourenvoyer ou recevoir les messages. La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

TCO (Total Cost of Ownership, traduisez Coût total de possession) :TCO représente le coût global d'un bien (un système informatique par exemple) tout au long de son cycle de vie, en prenant non seulement en compte les aspects directs (coûts matériels tels qu'ordinateurs, infrastructures réseaux, etc. ou logiciels tels que le coût des licences), mais également tous les coûts indirects (coûts cachés) tels que la maintenance, l'administration, la formation des utilisateurs et des administrateurs, l'évolution, le support technique et les coûts récurrents (consommables, électricité, loyer, etc.).

TCP/IP : La suite des protocoles Internet est l'ensemble des protocoles qui constituent la pile de protocoles utilisée par Internet. Elle est souvent appelée TCP/IP, d'après le nom de deux de ses protocoles : TCP (Transmission Control Protocol) et IP (Internet Protocol), qui ont été les premiers à être définis. Le document de référence sur ce sujet est le RFC 1122

UMTS : Universal Mobile Télécommunications System. Système de téléphonie mobile de troisième génération (3G). Elle permet des débits numériques jusqu'à 2 Mbps.

VMware :un VMware est un système qui crée un environnement clos dans lequel sont disponibles un ou deux processeur(s), des périphériques et un BIOS virtuel. Selon les concepteurs, le microprocesseur n'est émulé que quand c'est nécessaire, c'est-à-dire quand la VM (machine virtuelle) tourne en mode noyau ou en mode réel, mais pas pour le mode utilisateur (user mode) ou le Mode virtuel 8086.

WAN:Réseauétendu (WAN -Wide Aera Network) Réseauétendu (WAN -Wide Aera Network) .

• quelques centaines Km maximum entre 2 stations

• Structures ayant plusieurs sites éloignés géographiquement (systèmes de réservation de places géographiquement (systèmes de réservation de places d'avion, systèmes bancaires, agences gouvernementales provinciales

• Vitesse moins importante que sur un LAN

WAV : WAV (ou WAVE), une contraction de WAVEform audio format, est un standard pour stocker l'audio digitale de Microsoft et IBM. C'est le format le plus courant pour l'audio non compressé sur les plates-formes de Microsoft, mais il est bien courant sur les systèmes GNU/Linux aussi.

Wi Max : Technologie de communication électronique haut débit sans fil, le WiMAX est encore jeune : les premiers équipements certifiés commencent seulement à apparaître, et - en France - l'attribution des licences par l'ARCEP a eu lieu en juillet 2006.

WI-FI : est l'abréviation de Wireless Fidelity.Le WiFi est le nom d'une norme donnée à un type de réseau sans fil développé pour les communications informatiques.
Il permet de supprimer les câbles et de résoudre les problèmes de distances, d'obstacles…
La liaison utilise des ondes radioélectriques.

WiRAN : (Wireless Regional Area Network IEEE 802.22) est prévu pour sortir fin 2008 ou début 2009 en bénéficiant des évolutions de la téléphonie 3G et des recherches sur la 4G. Le WiRAN pourrait utiliser les bandes de fréquence libérées par la fin de la télévision analogique (qui cède le pas à la TNT) qui sont particulièrement intéressantes pour les réseaux car sur des fréquences moins élevées que les réseaux informatiques et de téléphone. Ces fréquences comprises entre 54 et 862 MHz, permettent des portées plus longues et traversent mieux les murs. Une seule antenne de 1 W pourrait ainsi couvrir jusqu'à 1 million d'utilisateurs, permettant des coûts de déploiement bien plus faible que pour les autres réseaux informatiques.

WLAN : Un réseau sans fil est un réseau informatique qui connecte différents postes entreeux par ondes radio.

XML (Extensible MarkupLanguage) : est un langage informatique de balisage générique. Le World Wide Web Consortium (W3C), promoteur de standards favorisant l'échange d'informations sur l'Internet, recommande la syntaxe XML pour exprimer des langages de balisages spécifiques (exemples : XHTML, SVG, XSLT).

Bibliographie

Bibliographie et Webographie

[1] S. CHAKRABORTY, J. PEISA, T. FRANKKILA, P. SYNNERGREN: IMS Multimedia Telephony over Cellular Systems: VoIP Evolution in a Converged Telecommunication World, Wiley, 2007.

[2] B. DOUSKALIS, Putting VoIP to Work: Softswitch Network Design and Testing, Prentice Hall, 2001.

[3] L. HARTE: Introduction to IP Telephony: Why and How Companies are Upgrading Private Telephone Systems to use VoIP Services, Althos, 2006.

[4] http://www.frameip.com/voip/#4_-_Les_avantages.

[5] J. D. CIOARA: Cisco IP Telephony, Cisco Press, 2006.

[7], [18] Asterisk la telephonie open source, Edition O'reilly, Année: 2006

Jim Van Meggelen ,Leif Madsen et Jared Smith.

[8] J. F. DURKIN: Voice-Enabling the Data Network: H.323, MGCP, SIP, QoS, SLAs, and Security, Pearson Education, 2002.

[6], [9], [10], [12] Laurent Ouakil, Guy Pujolle : Téléphonie sur IP 2006.

[11] L. HARTE, D. BOWLER: Introduction to SIP IP Telephony Systems: Technology Basics, Services, Economics, and Installation, Althos, 2004

[13] http://www.europainternet.info/mmqos/index.php/Sujet/letellij

Bibliographie

[14], [16] http://www.awt.be/web/ser/index.aspx?page=ser,fr,lex,000,000&alpha=T

[15] http://fr.wikipedia.org/wiki/H.323

[17] http://www.supinfo-projects.com/fr/2006/voip_telecom/4/

[19] Asterisk the future of telephony. Edition O'reilly ; Année: 2007 ;Jim Van Meggelen ,Leif Madsen et Jared Smith

[20] Asterisk Hacking. Edition: Syngress; Année: 2007 ;Johnny long et Larry chaffin