

Chapitre 3

**Les protocoles de VOIP et
panorama des produits**

CHAPITRE 3 : LES PROTOCOLES DE VOIP ET PANORAMA DES PRODUITS

1. Introduction

La voix sur IP constitue actuellement l'évolution la plus importante du domaine des Télécommunications. Avant 1970, la transmission de la voix s'effectuait de façon analogique sur des réseaux dédiés à la téléphonie. La technologie utilisée était la technologie électromécanique. Dans les années 80, une première évolution majeure a été le passage à la transmission numérique. La transmission de la voix sur les réseaux informatiques à commutation de paquets IP constitue aujourd'hui une nouvelle évolution majeure comparable aux précédentes.

L'objectif de ce chapitre est l'étude de cette technologie et de ses différents aspects. On parlera en détail de l'architecture de la VoIP, ses éléments et son principe de fonctionnement. On détaillera aussi des protocoles VoIP de signalisation et de transport ainsi que leurs principes de fonctionnement et de leurs principaux avantages et inconvénients.

2. Définition de VoIP

VoIP signifie textuellement Voix sur IP, (Voice Over IP) est une technique qui permet de communiquer par voix à distance via le réseau Internet, ou tout autre réseau acceptant le protocole TCP/IP comme (Ethernet, RNIS, PPP, etc.). La téléphonie sur IP ou ToIP (Telephony over IP) est un service de téléphonie qui transporte les flux voix des communications téléphoniques sur un réseau IP. A la différence de la VoIP où l'on ne fait qu'établir une communication « voix », la ToIP intègre l'ensemble des services associés à la téléphonie : double appel, messagerie, renvoi d'appel, FAX, etc. [17]

3. Architecture VoIP

La VoIP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. En effet, chaque constructeur apporte ses normes et ses fonctionnalités à ses solutions. Les trois principaux protocoles sont H.323, SIP et MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. Certaines placent l'intelligence dans le réseau alors que d'autres préfèrent une approche égale à égale avec l'intelligence répartie à la périphérie. Chacune ayant ses avantages et ses

inconvenients. La **figure 1** décrit, de façon générale, la topologie d'un réseau de téléphonie IP. Elle comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir une plus ou moins grande qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/contrôleur de commutation, appelées Gatekeeper. On retrouve les éléments communs suivants : [17]

3.1. Le routeur

Permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs permettent de simuler un Gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP.

3.2. La passerelle

Permet d'interfacer le réseau commuté et le réseau IP.

3.3. Le PABX

Est le commutateur du réseau téléphonique classique. Il permet de faire le lien entre la passerelle ou le routeur, et le réseau téléphonique commuté (RTC). Toutefois, si tout le réseau devient IP, ce matériel devient obsolète.

3.4. Les Terminaux

Sont généralement de type logiciel (software phone) ou matériel (hardphone), le softphone est installé dans le PC de l'utilisateur. L'interface audio peut être un microphone et des haut-parleurs branchés sur la carte son, même si un casque est recommandé. Pour une meilleure clarté, un téléphone USB ou Bluetooth peut être utilisé.

Le hardphone est un téléphone IP qui utilise la technologie de la Voix sur IP pour permettre des appels téléphoniques sur un réseau IP tel que l'Internet au lieu de l'ordinaire système PSTN. Les appels peuvent parcourir par le réseau internet comme par un réseau privé. Un terminal utilise des protocoles comme le SIP (Session Initiation Protocol) ou l'un des protocoles propriétaire tel que celui utilisée par Skype. .[17]

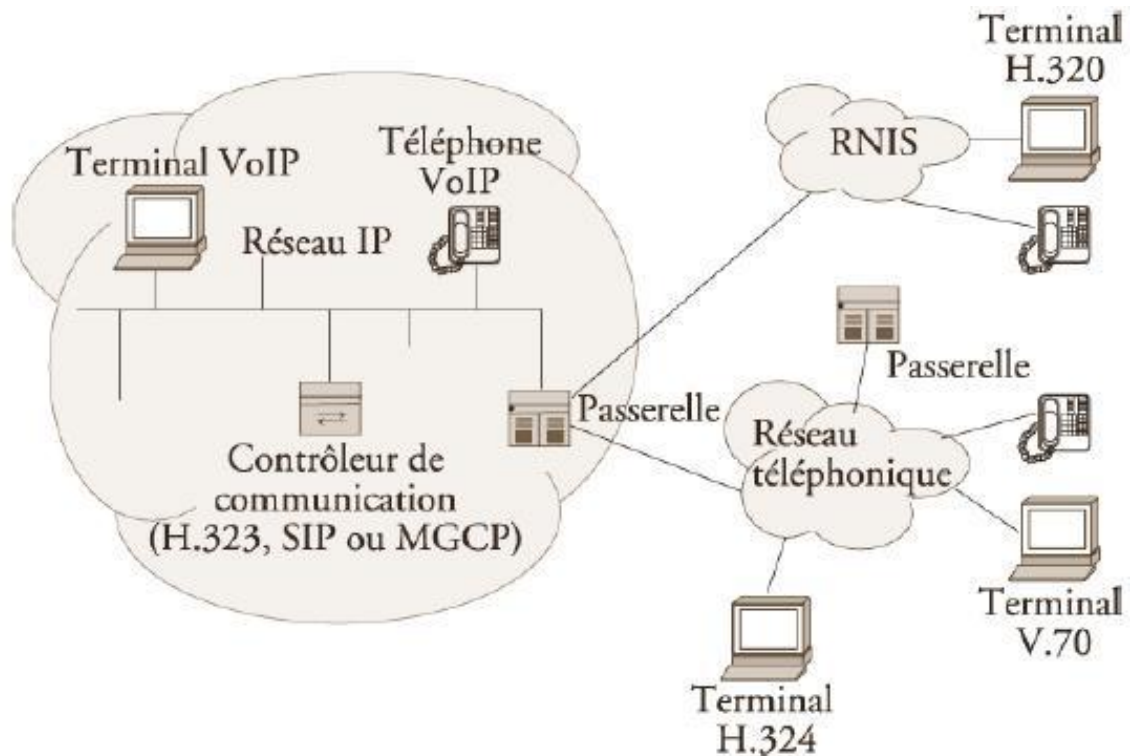


Figure 3.1 : Architecture générale de la voix sur IP [14]

4. Principe de fonctionnement

Depuis nombreuses années, il est possible de transmettre un signal à une destination éloignée sous forme de données numériques. Avant la transmission, il faut numériser le signal à l'aide d'un CAN (convertisseur analogique-numérique). Le signal est ensuite transmis, pour être utilisable, il doit être transformé de nouveau en un signal analogique, à l'aide d'un CNA (convertisseur numérique-analogique).

La VoIP fonctionne par numérisation de la voix, puis par reconversion des paquets numériques en voix à l'arrivée. Le format numérique est plus facile à contrôler, il peut être compressé, routé et converti en un nouveau format meilleur. Le signal numérique est plus tolérant au bruit que l'analogique.

Les réseaux TCP/IP sont des supports de circulation de paquets IP contenant un en-tête (pour contrôler la communication) et une charge utile pour transporter les données.

Il existe plusieurs protocoles qui peuvent supporter la voix sur IP tel que le H.323, SIP et MGCP. Les deux protocoles les plus utilisées actuellement dans les solutions VoIP présentes sur le marché sont le H.323 et le SIP. [18]

5. Les Protocoles de signalisation

5.1. Le protocole H.323

Le standard H.323 fournit, depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Telecommunications Union) pour les réseaux qui ne garantissent pas une qualité de service (QoS), tels qu'IP sur Ethernet, Fast Ethernet et Token Ring. Il est présent dans plus de 30 produits et il concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. H.323 traite également de l'interfaçage entre le LAN et les autres réseaux.

Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclut H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network).

Plus qu'un protocole, H.323 crée une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories : la signalisation, la négociation de codec, et le transport de l'information.

- Les messages de signalisation sont ceux envoyés pour demander la mise en relation de deux clients, qui indique que la ligne est occupée ou que le téléphone sonne, etc. En H.323, la signalisation s'appuie sur le protocole RAS pour l'enregistrement et l'authentification, et le protocole Q.931 pour l'initialisation et le contrôle d'appel.
- La négociation est utilisée pour se mettre d'accord sur la façon de coder les informations à échanger. Il est important que les téléphones (ou systèmes) utilisent un langage commun s'ils veulent se comprendre. Il s'agit du codec le moins gourmand en bande passante ou de celui qui offre la meilleure qualité. Il serait aussi préférable d'avoir plusieurs alternatives de langages. Le protocole utilisé pour la négociation de codec est le H.245
- Le transport de l'information s'appuie sur le protocole RTP qui transporte la voix, la vidéo ou les données numérisées par les codecs. Les messages RTCP peuvent être utilisés pour le contrôle de la qualité, ou la renégociation des codecs si, par exemple, la bande passante diminue.

Une communication H.323 se déroule en cinq phases : l'établissement d'appel, l'échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource reservation Protocol), l'établissement de la communication audio-visuelle,

l'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.) et enfin la libération de l'appel.

5.1.1. Rôle des composants

L'infrastructure H.323 repose sur quatre composants principaux : les terminaux, les Gateways, les Gatekeepers, et les MCU (Multipoint Control Units).

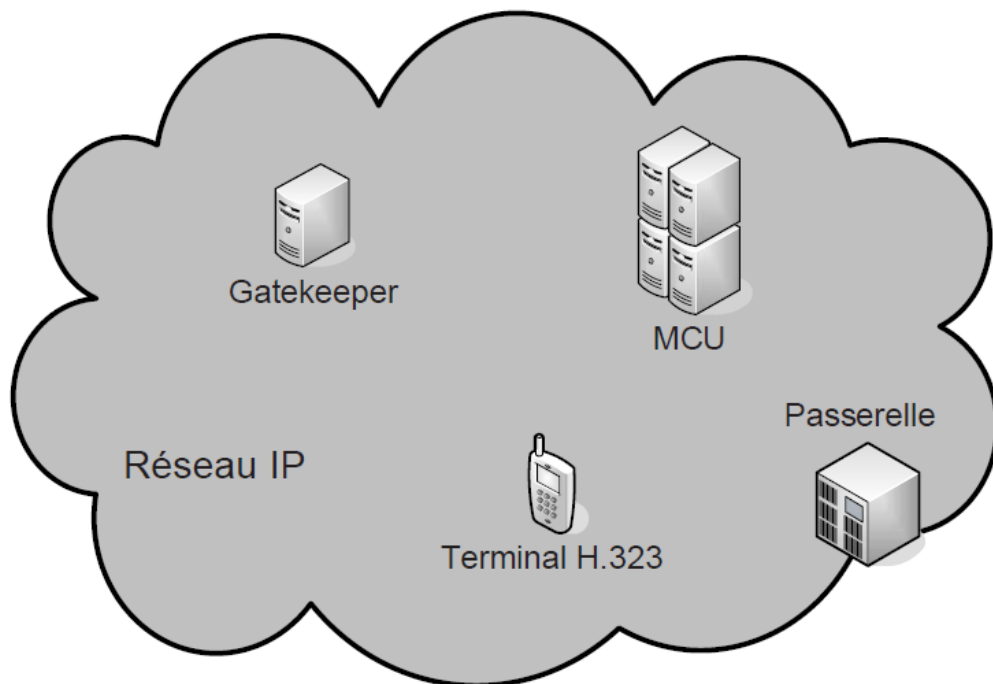


Figure 3.2 : Les composants de l'architecture H.323 [19]

- **Les terminaux H.323**

Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en oeuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications. Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s – G.723.1 et H.263).

- **Gateway ou les passerelles**

Les passerelles H.323 assurent l'interconnexion avec les autres réseaux, ex : (H.320/RNIS), les modems H.324, téléphones classiques, etc. Elles assurent la correspondance de signalisation

de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio).

- **Gatekeeper ou les portiers**

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 (voir figure 3.3 ci-dessous), 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 dès 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.

Le Gatekeeper a pour fonction :

- ✓ La translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status) ;
- ✓ Le contrôle d'accès, en interdisant les utilisateurs et les sessions non autorisés ;
- ✓ Et la gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées. Concrètement une fraction de la bande passante est allouée à la visioconférence pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint adhoc.

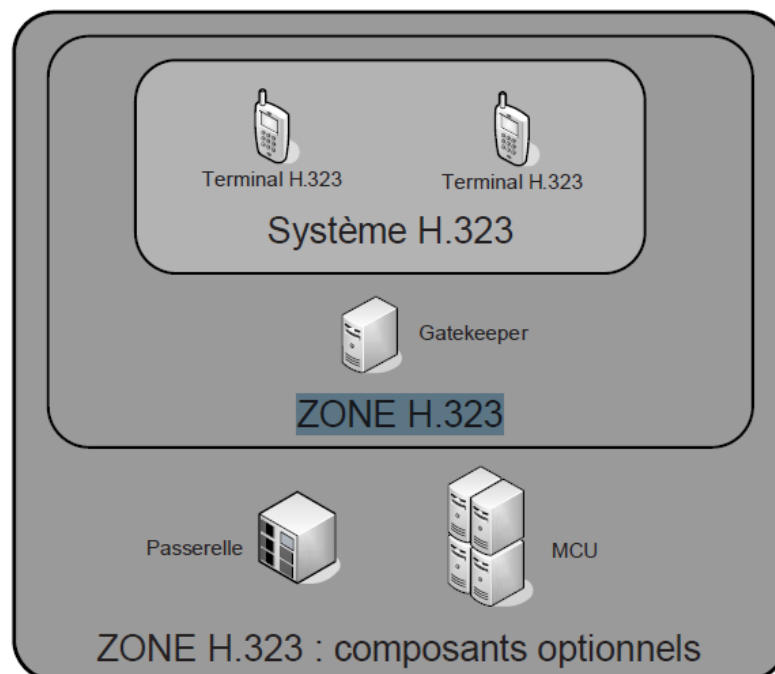


Figure 3.3 : La zone H.323 [19]

- **Les MCU**

Les contrôleurs multipoint appelés MCU (Multipoint Control Unit) offrent 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.

5.1.2. Avantages et inconvénients de la technologie H.323

La technologie H.323 possède des avantages et des inconvénients. Parmi les avantages, nous citons :

- **Codec standards** : H.323 établit des standards pour la compression et la décompression des flux audio et vidéo. Ceci assure que des équipements provenant de fabricants différents ont une base commune de dialogue.
- **Interopérabilité** : Les utilisateurs veulent pouvoir dialoguer sans avoir à se soucier de la compatibilité du terminal destinataire. En plus d'assurer que le destinataire est en mesure de décompresser l'information, H.323 établit des méthodes communes d'établissement et de contrôle d'appel.
- **Indépendance vis à vis du réseau** : H.323 est conçu pour fonctionner sur tout type d'architecture réseau. Comme les technologies évoluent et les techniques de gestion de la bande passante s'améliorent, les solutions basées sur H.323 seront capables de bénéficier de ces améliorations futures.
- **Indépendance vis à vis des plates-formes et des applications** : H.323 n'est lié à aucun équipement ou système d'exploitation.
- **Support multipoint** : H.323 supporte des conférences entre trois points terminaux ou plus sans nécessiter la présence d'une unité de contrôle spécialisée.

- **Gestion de la bande passante** : Le trafic audio et vidéo est un grand consommateur de ressources réseau. Afin d'éviter que ces flux ne congestionnent le réseau, H.323 permet une gestion de la bande passante à disposition. En particulier, le gestionnaire du réseau peut limiter le nombre simultané de connexions H.323 sur son réseau ou limiter la largeur de bande à disposition de chaque connexion. De telles limites permettent de garantir que le trafic important ne soit pas interrompu.
- **Support multicast** : H.323 supporte le multicast dans les conférences multipoint. Multicast envoie chaque paquet vers un sous-ensemble des destinataires sans réplication, permettant une utilisation optimale du réseau.

Les inconvénients de la technologie H.323 sont :

- La complexité de mise en œuvre et les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet, ainsi qu'un manque de modularité et de souplesse.
- Comprend de nombreuses options susceptibles d'être implémentées de façon différentes par les constructeurs et donc de poser des problèmes d'interopérabilité.

5.2. Le Protocole SIP

5.2.1. Description générale du Protocole SIP

Le protocole Sip (Session Initiation Protocole) a été initié par le groupe MMUSIC (Multiparty Multimedia Session Control) et désormais repris et maintenu par le groupe SIP de l'IETF donnant la Rfc 3261 rendant obsolète la Rfc 2543. Sip est un protocole de signalisation appartenant à la couche application du modèle Osi. Son rôle est d'ouvrir, modifier et libérer les sessions. L'ouverture de ces sessions permet de réaliser de l'audio ou vidéoconférence, de l'enseignement à distance, de la voix (téléphonie) et de la diffusion multimédia sur Ip essentiellement. Un utilisateur peut se connecter avec les utilisateurs d'une session déjà ouverte.

Pour ouvrir une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de s'accorder sur la compatibilité de leur média, Sip permet donc de relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée. Enfin, SIP possède l'avantage de

ne pas être attaché à un médium particulier et est sensé être indépendant du protocole de transport des couches basses

5.2.2. Principe de fonctionnement

SIP intervient aux différentes phases de l'appel :

- Localisation du terminal correspondant,
- Analyse du profil et des ressources du destinataire,
- Négociation du type de média (voix, vidéo, données...) et des paramètres de communication,
- Disponibilité du correspondant, détermine si le poste appelé souhaite communiquer, et autorise l'appelant à le contacter.
- Etablissement et suivi de l'appel, avertit la partie appelante et appelée de la demande d'ouverture de session, gestion du transfert et de la fermeture des appels.
- Gestion de fonctions évoluées : cryptage, retour d'erreurs, ...

Avec SIP, les utilisateurs qui ouvrent une session peuvent communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci. SIP permet donc l'ouverture de sessions en mode :

- ❖ **Point à Point** : Communication entre 2 machines, on parle d'unicast.
- ❖ **Diffusif** : Plusieurs utilisateurs en multicast, via une unité de contrôle **MCU** (Multipoint Control Unit)
- ❖ **Combinatoire** : Plusieurs utilisateurs pleinement interconnectés en multicast via un réseau à maillage complet de connexions.

Voici les différents éléments intervenant dans l'ouverture de session :

- Suivant la nature des échanges, choix des protocoles les mieux adaptés (RSVP, RTP, RTCP).
- Détermination du nombre de sessions, comme par exemple, pour véhiculer de la vidéo, 2 sessions doivent être ouvertes (l'une pour l'image et l'autre pour la audio).
- Chaque utilisateur et sa machine est identifié par une adresse que l'on nomme URL SIP et qui se présente comme une Url Mail.
- Requête Uri permettant de localiser le proxy server auquel est rattaché la machine de l'appelé.

- Requête SIP, une fois le client (machine appelante) connecté à un serveur SIP distant, il peut lui adresser une ou plusieurs requêtes SIP et recevoir une ou plusieurs réponses de ce serveur. Les réponses contiennent certains champs identiques à ceux des requêtes, tels que : Call-ID, Cseq, To et From.

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** : Cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête Invite.
- **Options** : Un proxy server en mesure de contacter l'UAS (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 à fin d'annuler une requête non validée par une réponse finale comme, par exemple, 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.
- **Registrier** : cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL TO par le serveur auquel il est relié.

Une réponse à une requête est caractérisée, par un code et un motif, appelés code d'état et raison phrase respectivement. Un code d'état est un entier codé sur 3 bits indiquant un résultat à l'issue de la réception d'une requête. Ce résultat est précisé par une phrase, expliquant le motif du refus ou de l'acceptation de la requête. Le code d'état est donc destiné à l'automate gérant l'établissement des sessions SIP et les motifs aux programmeurs. Il existe 6 classes de réponses et donc de codes d'état, représentées par le premier bit :

- 1xx = Information - La requête a été reçue et continue à être traitée.
- 2xx = Succès - L'action a été reçue avec succès, comprise et acceptée.
- 3xx = Redirection - Une autre action doit être menée afin de valider la requête.

- 4xx = Erreur du client - La requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur.
- 5xx = Erreur du serveur - Le serveur n'a pas réussi à traiter une requête apparemment correcte.
- 6xx = Echec général - La requête ne peut être traitée par aucun serveur.

5.2.3. Rôle des composants

Dans un système SIP on trouve deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (PS, RS, LS, RG), (figure 3.4):

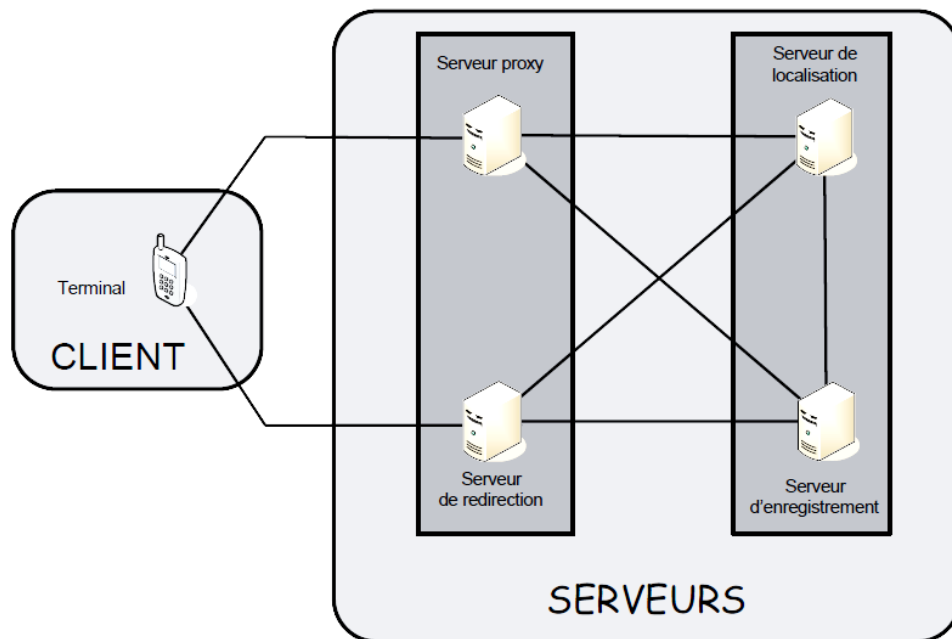


Figure 3.4 : Architecture de SIP [19]

- ❖ **UAS (User Agent Server)** : Il représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur (**figure 3.5**).
- ❖ **UAC (User Agent Client)** : Il représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes (**figure 3.5**).

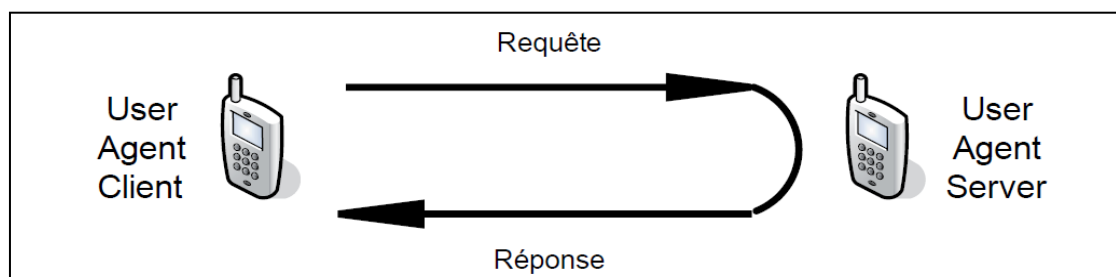


Figure 3.5 : Communication entre UAC et UAS [19]

❖ **RG (Registrar)**

Est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une **URI**, qui seront stockées dans une base de données (**figure 3.6**). [20]

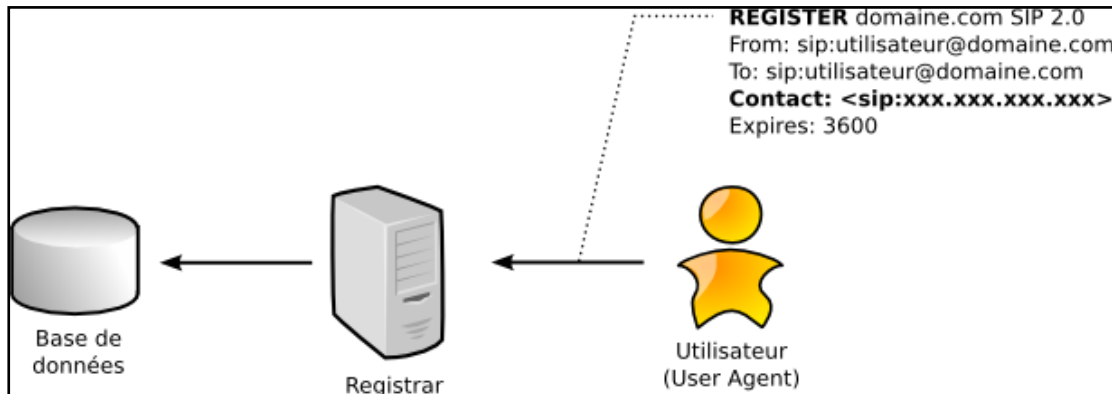


Figure 3.6 : Enregistrement d'un utilisateur [20]

Les URI SIP sont très similaires dans leur forme à des adresses email :

sip:utilisateur@domaine.com. Généralement, des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI

❖ **PS (Proxy Server)**

Un Proxy SIP sert d'être l'intermédiaire entre deux User Agents qui ne connaissent pas leurs emplacements respectifs (adresse IP). En effet, l'association URI-Adresse IP a été stockée préalablement dans une base de données par un Registrar. Le Proxy peut donc interroger cette base de données pour diriger les messages vers le destinataire. La (**figure 3.7**) montre les étapes de l'interrogation du proxy la base de données. [7]

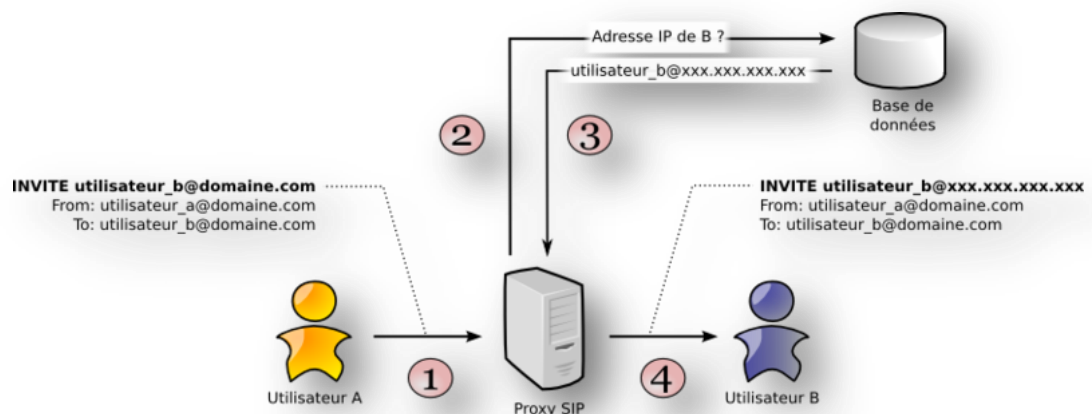


Figure 3.7 : Principe du protocole SIP [20]

Le Proxy se contente de relayer uniquement les messages SIP pour établir, contrôler et terminer la session (voir **figure 3.8**). Une fois la session établie, les données, par exemple un

flux RTP pour la VoIP, ne transitent pas par le serveur Proxy. Elles sont échangées directement entre les User Agents.

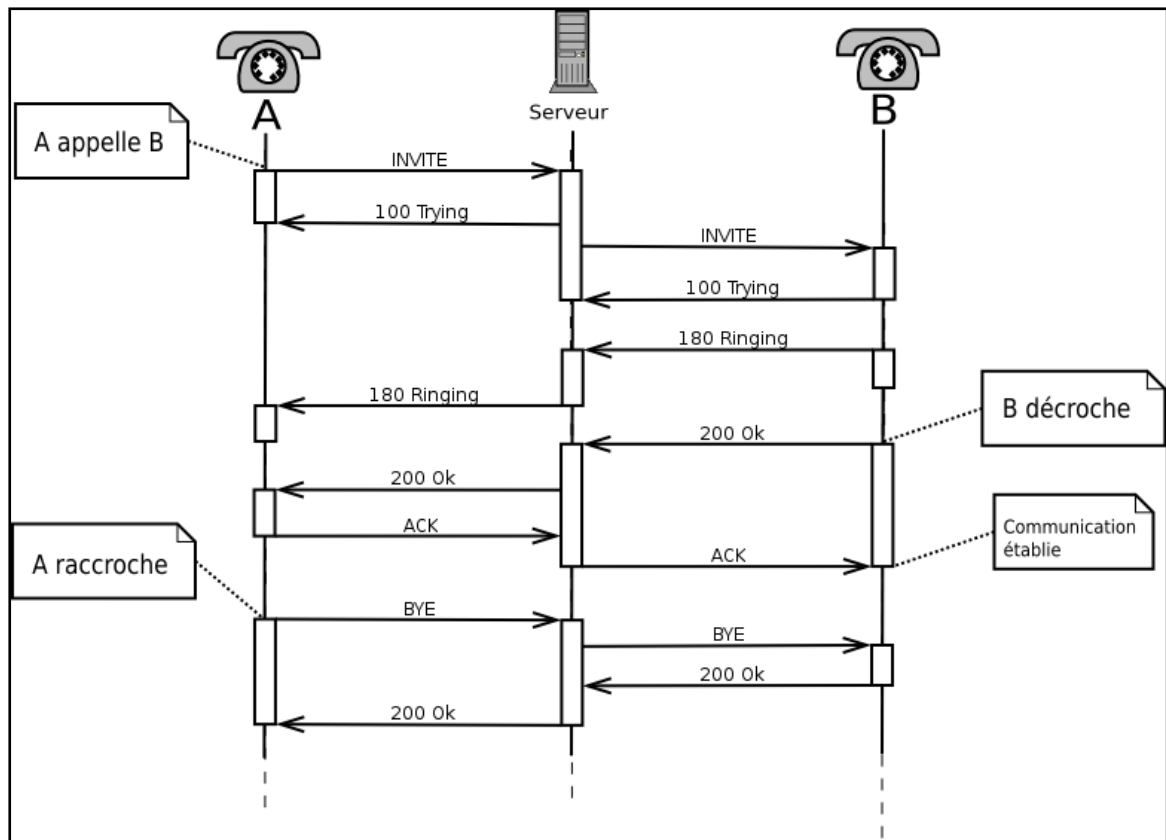


Figure 3.8 : Session SIP à travers un proxy [20]

- ❖ **RS (Redirect Server) :** Il réalise simplement une association (mapping) d'adresses vers une ou plusieurs nouvelles adresses. (Lorsqu'un client appelle un terminal mobile - redirection vers le PS le plus proche - ou en mode multicast - le message émis est redirigé vers toutes les sorties auxquelles sont reliés les destinataires). Notons qu'un Redirect Server est consulté par l'UAC comme un simple serveur et ne peut émettre de requêtes contrairement au PS.
- ❖ **LS (Location Server) :** Il fournit la position courante des utilisateurs dont la communication traverse les RS et PS auxquels il est rattaché. Cette fonction est assurée par le service de localisation.

5.2.4. Avantages et inconvénients du protocole SIP

Ouvert, standard, simple et flexible sont les principales atouts du protocole SIP, voilà en détails ces différents avantages :

- Ouvert : les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- Standard : l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- Simple : SIP est simple et très similaire à http.
- Flexible : SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).
- Téléphonie sur réseaux publics : il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.
- Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau. Un autre inconvénient est le faible nombre d'utilisateurs : SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

6. Les Protocoles de transport

Nous décrivons deux autres protocoles de transport utilisés dans la voix sur IP à savoir l'RTP et le RTCP

6.1. Le protocole RTP

6.1.1. Description générale du protocole RTP

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF afin de faciliter le transport temps réel de bout en bout des flots données audio et vidéo sur les réseaux IP, c'est à dire sur les réseaux de paquets. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réels comme la parole numérique ou la visioconférence constitue un véritable problème pour Internet. Qui dit application temps réel, dit présence d'une certaine qualité de service (QoS) que RTP ne garantie pas du fait qu'il fonctionne au niveau Applicatif. De plus RTP est un protocole qui se

trouve dans un environnement multipoint, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

6.1.2. Les fonctions du protocole RTP

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ. RTP est un protocole de bout en bout, volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. Il permet ainsi de :

- Mettre en place un séquençement des paquets par une numérotation et ce afin de permettre ainsi la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est pas un gros problème si les paquets ne sont pas perdus en trop grands nombres. Cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte.
- Identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets : possibilité de resynchronisation des flux par le récepteur)
- L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast l'identité de la source doit être connue et déterminée.
- Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

6.1.3. Avantages et inconvénients du protocole RTP

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.); de détecter les pertes de paquets; et d'identifier le contenu des paquets pour leur transmission sécurisée.

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garanti pas le délai de livraison.

6.2. Le protocole RTCP

6.2.1. Description générale du protocole RTCP

Le protocole RTCP est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP.

Le protocole RTP utilise le protocole RTCP, Real-time Transport Control Protocol, qui transporte les informations supplémentaires suivantes pour la gestion de la session.

Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la *gigue* : c'est à dire les paquets qui arrivent régulièrement ou irrégulièrement) et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS.

Parmi les principales fonctions qu'offre le protocole RTCP sont les suivants :

- Une synchronisation supplémentaire entre les médias : Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.
- L'identification des participants à une session : en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique.
- Le contrôle de la session : en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement.

Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de participants de l'application. On peut dire que les paquets RTP ne transportent que les données

des utilisateurs. Tandis que les paquets RTCP ne transportent en temps réel, que de la supervision.

On peut détailler les paquets de supervision en 5 types:

- **SR (Sender Report)** : Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (gigue), etc.). Ces rapports sont issus d'émetteurs actifs d'une session.
- **RR (Receiver Report)** : Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- **SDES (Source Description)** : Carte de visite de la source (nom, e-mail, localisation).
- **BYE** : Message de fin de participation à une session.
- **APP** : Fonctions spécifiques à une application.

6.2.2. Points forts et limites du protocole RTCP

Le protocole RTCP est adapté pour la transmission de données temps réel. Il permet d'effectuer un contrôle permanent sur une session et ces participants. Par contre, il fonctionne en stratégie bout en bout, et il ne peut pas contrôler l'élément principal de la communication dans le réseau.

7. Points forts et limites de la voix sur IP

Différentes sont les raisons qui peuvent pousser les entreprises à s'orienter vers la VoIP comme solution pour la téléphonie. Les avantages les plus marqués sont :

- **Réduction des coûts** : En effet le trafic véhiculé à travers le réseau RTC est plus couteux que sur un réseau IP. Réductions importantes pour des communications internationales en utilisant le VoIP, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP intersites (WAN). Dans ce dernier cas, le gain est directement proportionnel au nombre de sites distants.
- **Standards ouverts** : La VoIP n'est plus uniquement H323, mais un usage multi-protocoles selon les besoins de services nécessaires. Par exemple, H323 fonctionne en mode égale à égale alors que MGCP fonctionne en mode centralisé. Ces différences de conception offrent immédiatement une différence dans l'exploitation des terminaisons considérées.

- **Un réseau voix, vidéo et données (à la fois) :** Grace à l'intégration de la voix comme une application supplémentaire dans un réseau IP, ce dernier va simplifier la gestion des trois applications (voix, réseau et vidéo) par un seul transport IP. Une simplification de gestion, mais également une mutualisation des efforts financiers vers un seul outil.
- **Un service PABX distribué ou centralisé :** Les PABX en réseau bénéficient de services centralisés tel que la messagerie vocale et la taxation. Cette même centralisation continue à être assurée sur un réseau VoIP sans limitation du nombre de canaux. Il convient pour en assurer une bonne utilisation de dimensionner convenablement le lien réseau. L'utilisation de la VoIP met en commun un média qui peut à la fois offrir à un moment précis une bande passante maximum à la donnée, et dans une autre période une bande passante maximum à la voix, garantissant toujours la priorité à celle-ci.

Les points faibles de la voix sur IP sont :

- **Fiabilité et qualité sonore :** un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission qui n'est pas encore optimale. En effet, des désagréments tels la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert) sans être en mesure de savoir si des paquets ont été perdus et à quel moment.
- **Dépendance de l'infrastructure technologique et support administratif exigeant :** les centres de relations IP peuvent être particulièrement vulnérables en cas d'improductivité de l'infrastructure. Par exemple, si la base de données n'est pas disponible, les centres ne peuvent tout simplement pas recevoir d'appels. La convergence de la voix et des données dans un seul système signifie que la stabilité du système devient plus importante que jamais et l'organisation doit être préparée à travailler avec efficience ou à encourir les conséquences.
- **Vol :** les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et au même au service téléphonique pour écouter des conversations ou effectuer des appels gratuits aux noms d'autres comptes.

- **Attaque de virus** : si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au réseau téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

8. Panorama de quelques produits

8.1. WELLX

WellX Telecom est une société High-Tech 100% française concevant et développant une nouvelle génération de PABX.

WellX commercialise une gamme complète de solutions téléphoniques pour l'entreprise intégrant une grande variété d'applications à fortes valeurs ajoutées telles que de la téléphonie sur IP, de la messagerie vocale, l'Email, une passerelle Fax, un standard automatique, l'enregistrement des conversations, l'accès Internet. [21]

8.2. AVAYA

Avaya a installé plus de 7 millions de lignes téléphoniques IP. Malgré son passé dans la téléphonie traditionnelle, Avaya installe maintenant plus de lignes de téléphonie sur IP que de lignes traditionnelles. Pour le 7ème trimestre consécutif, Avaya est le leader mondial en téléphonie sur IP avec 21% de parts de marché. [22]



Figure 3.9: les équipements Avaya pour la TOIP. [22]

8.3. 3CX Phone System pour Windows

3CX Phone System est un PBX IP logiciel pour MS Windows qui remplace les PBX téléphoniques traditionnels, et offre aux employés la possibilité de passer, recevoir et transférer des appels. Le PBX IP supporte toutes les fonctionnalités d'un PBX traditionnel. Le PBX IP est aussi appelé Système Téléphonique de VoIP, PABX IP ou Serveur SIP. Les appels sont envoyés comme des paquets de données sur le réseau informatique au lieu du réseau téléphonique traditionnel. Les téléphones partagent le réseau avec des ordinateurs. Il est possible alors de supprimer les postes téléphoniques traditionnels. Avec l'utilisation d'une passerelle VoIP (voix sur IP), vous pouvez connecter les lignes téléphoniques existantes à un PBX IP et continuer de passer et recevoir des appels téléphoniques via la ligne RTC / RNIS traditionnelle. Les sociétés commencent leurs systèmes traditionnels de téléphonie / PBXs vers des PBXs IP à une vitesse fulgurante : les ventes d'équipements de téléphonie IP augmentent chaque année de plus de 50 % et devraient atteindre 15 Milliards de \$ par an à la fin 2007. 3CX Phone System utilise les téléphones logiciels ou matériels au standard SIP, et fournit la commutation d'appel interne, aussi bien que les appels en provenance et vers le réseau traditionnel ou via un service de voix sur IP (VoIP). [23]

❖ Comment fonctionne un Système Téléphonique IP

Un Système Téléphonique VoIP, aussi appelé PBX IP, consiste en un ou plusieurs téléphones au standard SIP, un PBX IP et en option une Passerelle VoIP. Le Serveur PBX IP est l'équivalent d'un serveur proxy : Les clients SIP, étant des téléphones logiciels ou matériels, enregistrés auprès du serveur PBX IP. Lorsqu'ils souhaitent passer un appel, ils demandent au serveur PBX IP d'établir la connexion. Le PBX IP a une liste d'adresses de tous les téléphones/utilisateurs et leur adresse SIP correspondante et est ainsi capable de connecter un appel interne ou acheminer un appel externe via une passerelle VoIP ou un fournisseur de services VoIP. La figure illustre comment le PBX IP s'intègre sur le réseau et comment il utilise le réseau RTC / RNIS ou Internet pour connecter les appels.

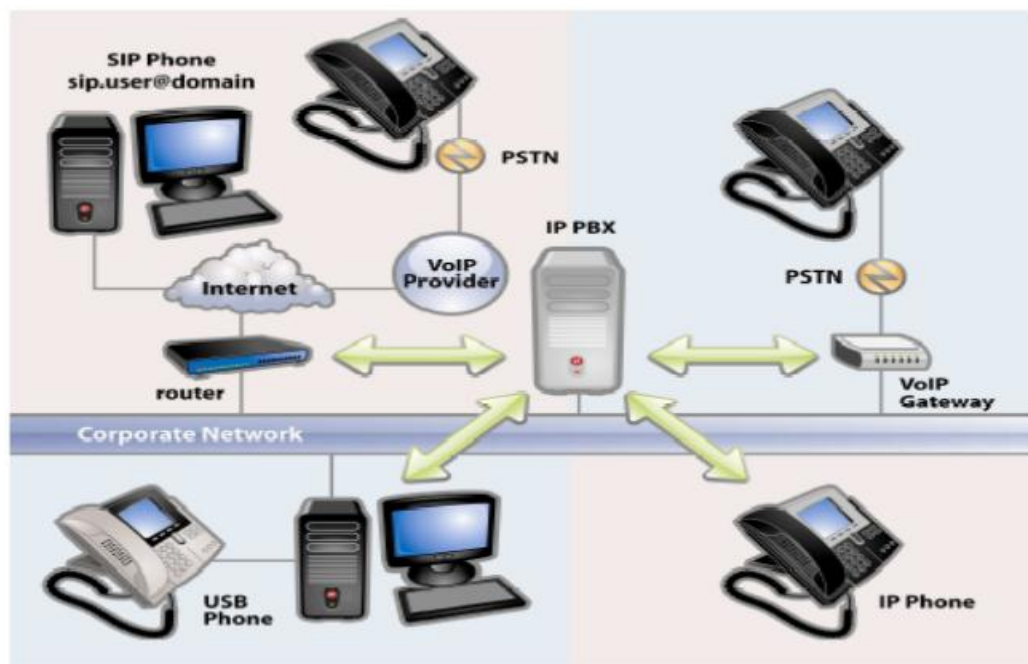


Figure 3.10: Vue d'ensemble d'un système téléphonique. [22]

❖ Téléphones logiciels SIP

Un téléphone SIP logiciel est un programme permettant d'utiliser le microphone et Les haut-parleurs de votre ordinateur, ou un casque micro pour téléphoner. Des exemples de logiciels SIP sont : SJPhone de SJlabs, X-Lite de Counterpath, ou 3CX VoIP Phone for Windows.

❖ Téléphones Matériels SIP

Un téléphone SIP ressemble et se comporte comme un téléphone classique. Il s'agit d'un mini ordinateur qui se connecte directement au réseau informatique. Comme ils ont un mini hub, ils peuvent partager une prise informatique avec un ordinateur, supprimant la nécessité d'une prise supplémentaire pour le téléphone. Des exemples de téléphone SIP sont : GrandStream GXP-2000, Thomson ST2030 ou CISCO 7940.

❖ Téléphones analogiques utilisant un adaptateur ATA

Si vous voulez utiliser votre téléphone existant avec un système téléphonique VoIP, vous pouvez utiliser un adaptateur ATA. Un adaptateur ATA vous permet de le connecter à la prise Ethernet du réseau puis de raccorder le téléphone à l'adaptateur. Cela permettra à votre ancien téléphone classique d'être vu comme un téléphone SIP par votre Système Téléphonique VoIP. [23]

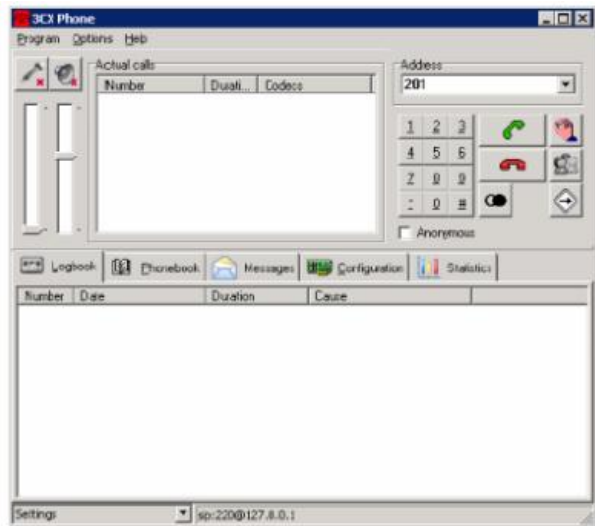


Figure 3.11: Téléphone logiciel 3CX Phone

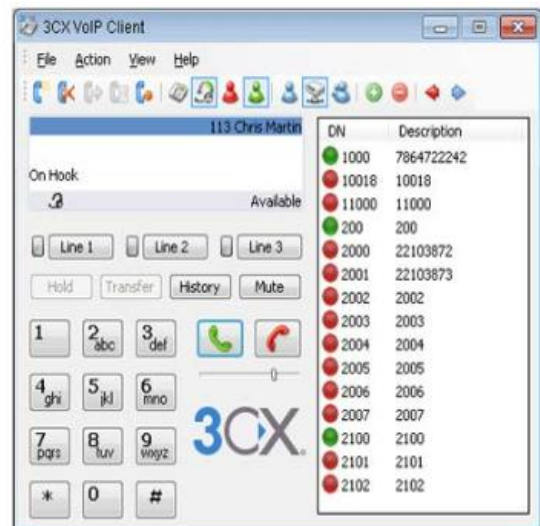


Figure 3.12: Téléphone logiciel 3CX VOIP Client



Figure 3.13: Téléphone SIP [23]



Figure 3.14: Adaptateur ATA [23]

8.4. Cisco IP Phone 7960G - téléphone VoIP

Le téléphone IP 7960G est le téléphone idéal pour les dirigeants d'entreprise et leurs collaborateurs directs. Le téléphone IP 7960G peut gérer six lignes téléphoniques grâce à ces six boutons programmables et possède quatre touches de fonctionnalités interactives qui guident l'utilisateur au sein des fonctionnalités téléphoniques sur l'écran LCD du téléphone. Les capacités

graphiques de l'écran permettent de présenter à l'utilisateur les informations des appels et lui offrent un accès intuitif aux fonctionnalités. [24]

❖ Caractéristiques principales

- Logiciels compatibles : Cisco CallManager 3.3(3) ou plus récent.
- Codecs vocaux : G.711, G.729a.
- Protocoles VoIP : H323, MGCP, SCCP, SIP.
- Fonctions principales : Commutateur Ethernet intégré.
- Nombre de ports réseau : 2 x Ethernet 10/100Base-TX.

- Description du produit : Cisco IP Phone 7960G - téléphone VoIP.
- Identification de l'appelant , Fonction boîte vocale, Appel en instance, Renvoi automatique, Transfert d'appel, Mise en attente d'appel, Micrologiciel évolutif, Fonctionnement par menu, Réglage du volume et Réglage de la sonnerie : Oui
- Fonctions supplémentaires : Navigateur Web
- Fonctions principales : Commutateur Ethernet intégré
- Qualité de service : IEEE 802.1Q (VLAN)
- Attribution des adresses IP : DHCP
- Protocoles réseau : TFTP
- Fonctions vocales: Génération de bruit de confort, détection d'activité vocale
- Connexions : 1 x prise pour casque d'écoute.[24]



Figure 3.15: Terminal SIP CISCO 7960G.[24]

9. Conclusion

Comme on a pu le voir tout au long de ce chapitre, la VoIP est la solution la plus rentable pour effectuer des conversations. Actuellement il est évident que la VoIP va continuer à évoluer.

La téléphonie IP est une bonne solution en matière d'intégration, fiabilité et de coût. On a vu que la voix sur IP étant une nouvelle technologie de communication, elle n'a pas encore de standard unique. Chaque standard possède ses propres caractéristiques pour garantir une bonne qualité de service. En effet, le respect des contraintes temporelles est le facteur le plus important lors de transport de la voix.

C'est sûrement que la téléphonie IP va continuer de se développer durant les années et va aussi fournir des produits et des servi ces plus développer que ce sont exister actuellement, pour arrivée à une image très confortable selon les besoins des utilisateurs.