

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE
SCIENTIFIQUE UNIVERSITE MOULOUD MAMMERI TIZI OUZOU



FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE
DEPARTEMENT D'ELECTRONIQUE

Mémoire de fin d'études

Présenté en vue de l'obtention
du diplôme d'Ingénieur d'état en Electronique
Option : Communication

Thème :

**Procédure d'implémentation d'un Call Center IP
dans le réseau GSM**

Proposé et dirigé par :

Mr . AIT BACHIR Y

Présenté par :

Melle. BENHAMICHE Yasmina

Année universitaire 2012/2013

Remerciements

Au terme de ce travail, je tiens à remercier tous ceux qui m'ont aidé dans sa réalisation ceux qui ont bien voulu le juger.

En premier lieu ,j'exprime ma profonde reconnaissance et mes sincères remerciements à Mr AIT BACHIR pour avoir accepté de diriger ce travail et pour ses précieuses recommandations , il m' a aidé à bien mener ce travail, malgré ses multiples obligations ,qu'il soit assuré de toute ma gratitude.

D'autre part , je voudrais remercier mes enseignants pour leur soutien et leur aide tout au long de l'année.

Mes remerciement vont également à l'équipe d'ORASCOM TELECOM ALGERIE en particulier à Mr GHANES pour m'avoir consacré du temps au tout début de mes recherches malgré ses multiples obligations .

je remercie les membres du jury qui ont accepté de juger mon travail .

finalement , je remercie tous ceux qui n'ont épargné aucun effort, de près ou de loin , pour me permettre d'accomplir mon travail.

Dédicaces

A Mes parents , à qui je dois beaucoup et qui m'ont permis de réaliser mes rêves .

A Ma proche famille, pour l'impact positif qu'exerça chacun de ses membres sur moi . je citerai mes adorables petits neveux " bichette et coco" une véritable source de bonheur et de réconfort .

A Ma Mimiche , cette grande sœur hors du commun .

A mon frère Skandou " le petit Einstein" pour son aide et son dévouement .

A Hamed pour son soutien et ses encouragements.

A la mémoire de mon très cher Sofiane.

A mes amis qui se reconnaîtront .

A tous ceux que j'aime.

TABLE DES MATIERES.

Introduction générale	1
-----------------------------	---

CHAPITRE I : Etude d'un call center IP.

I.1. Présentation d'un centre d'appel.....	2
I.2. Architecture d'un centre d'appels	3
I.3 Architecture technique	4
I.4. Environnement et matériel utilisés.....	5
I.5 Les différents types de centres d'appels	5
I.6. Objectifs et performance d'un call center.....	6
I.7. Les déterminants de la performance d'un centre d'appels	7
II. PABX et centre d'appels IP	9
II.1. Définition du PABX	9
II.1.2. Interfaces	10
II.1.3. Les différentes capacités de PABX	11
II.1.4. Mode de fonctionnement	11
II.1.5. Fonctionnement	12
II.1.6. Evolution des PABX	12
II.2. Le PABX en réseau	13
II.2.1. Nécessite d'interconnexion.....	13
II.2.2. Les supports d'interconnexion	13
II.2.3. L'interconnexion de Pabx	14
II.2.4. Accès au réseau public	14
II.2.5. ETUDE DES RESEAU PABX.....	16
II.2.6. Le choix du réseau PABX	16
III. Types de réseau PABX	17
II.1.1. Les PABX-IP (VoIP)	17
III.1.2.fonctionnement du réseau téléphonique PABX-IP/VoIP	17
III.1.3. Avantages des réseaux PABX-IP	17
III.1.4. Connexion d'un réseau/autocommutateur traditionnel au réseau IP	20
III.2. IPBX	20

III.2.1. Définition	20
III.2.2. Fonctionnement	21
III.2.3. Fonctionnalités IPBX.....	22
III.2.4. Les caractéristiques d'un IPBX	23
III.3. Les IP CENTREX	23
Conclusion	

CHAPITRE II : Optimisation de la téléphonie par la VOIP

Introduction.....	24
Partie I : La VOIP	24
I.1. Qu'est-ce que la VoIP	24
I.2. fonctionnement de la VoIP.....	24
I.3. Architecture d'une infrastructure VOIP.....	25
Partie II :Téléphonie sur IP	26
II.1. DEFINITION	26
II.2. Schémas de principe :	27
II.3. Fonctionnalités de la téléphonie sur IP :	27
II.4. Intérêts de la TOIP:	28
II.5. Les différents éléments pouvant composés un réseau de téléphonie sur IP	28
II.6. Fonctionnement de la téléphonie sur IP	31
II.6.1. Principe.....	31
II.6.2. Architecture de transmission VOIP	31
II.7.Mode d'accès et architecture	33
II.8. Signalisation et transport :	35
Partie v : Les problèmes clés de la téléphonie sur IP :	35
V.1. La QoS :	35
VI. Points forts et limites de la voix sur IP :	38
Partie III :	39
III.1. Protocoles liés à la ToIP	39
1.1. Signalisation	39

A. Protocole H323.....	40
A.1. Introduction	40
A.2. Fonctionnement.....	40
A.3. composants de H323:	41
A.4. Protocoles H 323 intervenant dans un appel H323	45
A.5. Exemple de l'utilisation du protocole H323 avec deux IPBX (deux constructeurs différents)	46
A.5.1. les étapes pour émettre un appel d'un site vers un autre site	47
A.5.2. Utilisation du Gatekeeper	48
B. Protocole SIP	49
B.1. Introduction	49
B.2. Architecture protocolaire.....	49
B.3. Fonctionnement	50
B.4. Les entités du système SIP	50
B.5. les différents éléments intervenant dans l'ouverture de session	53
B.6. Les réponses SIP	54
B.7. Structure des messages SIP.....	55
B.8. Sécurité et Authentification du protocole SIP.....	57
B.9. Comparaison SIP vs H323	57
1.2 . Protocoles de Transport	58
A. Protocole RTP	59
A.1. Introduction	59
A.2. Les fonctions de RTP	59
A.3. Entête RTP	60
B. Protocole RTCP	61
B.1. Introduction	61
B.2. Les fonctions du RTCP	61
B.3. Entête RTCP	62
B.4. Conclusion	63
III.2. Compatibilité de la TOIP et le réseau téléphonique classique	64
2 .1. Standard ENUM	64

III.3. Problématique ToIP avec les NAT et les pare-feux	65
3.1 Problème de NAT	65
3.2 Problème de pare-feux	66
4. ToIP et la sécurité des communications voix	70
4.1. Vulnérabilités de la ToIP	70
4.2. Exemples d'attaques sur l'infrastructure ToIP	71
4.3. Solutions de sécurité de la ToIP	71
5. La ToIP et IPv6	72
Conclusion	72

Chapitre III – Architecture et sécurisation.

I.1. Introduction	74
I.2. Scénarios	76
I.2.1. Call center mono-site avec son propre IPBX, utilisant un <i>Gateway</i> vers le PSTN pour ses communications vers l'extérieur.....	77
I.2.2. Call center mono-site avec son propre IPBX, utilisant un ITSP pour ses communications vers l'extérieur.....	77
I.2.3. Call center multi-site avec un ou plusieurs IPBX, n'utilisant que SIP	78
I.2.4. Services supplémentaires	78
II. Attaques contre la VoIP et bonnes pratiques de sécurisation	79
II.1. Attaques sur le protocole	79
II.2. Les vulnérabilités de l'infrastructure	85
III. Sécurisation et bonne pratiques	87
III.1. Sécurisation protocolaire	87
III.2. Cryptage aux points terminaux	88
III.2.1. Service de sécurités offertes par SRTP	88
III.2.2. Sécurisation de l'application	90
III.2.3. Sécurisation du système d'exploitation	90
Conclusion	

Chapitre IV - Interfaçage dans le réseau GSM.

Introduction.....	
I. Définition	93
I.1. Architecture GSM.....	94
I.1.1. Station Mobile (MS, Mobile Station)	94
I.1.2. Sous-système Radio (BSS, Base Station Subsystem)	95
I.1.3. Sous-système réseau (NSS, Network Subsystem)	95
I.1.4. Le réseau d'exploitation et maintenance	97
I.1.5. Réseau Sémaphore Numéro 7 appliqué au GSM.....	97
I.2. Interfaces GSM	97
I.3. Identités dans un réseau GSM	100
I.4. la liaison radio entre le téléphone mobile et la BTS	107
I.5. Acheminement des appels / Interactions entre les équipements.....	112
II. l'interfaçage du Call center avec le réseau GSM	113
II.1. Passerelles GSM numériques	114
II.1.1. Passerelles GSM PRI E1/T1	114
II.1.2. Passerelles GSM RNIS BRI (T0)	115
II.2. Passerelles GSM analogiques	116
II.3. Passerelle GSM VOIP pour PABX IP/ IPBX	116
Conclusion.....	117
Conclusion Générale	119
Annexe	
Glossaire	
Liste des tableaux et figures	
Bibliographie	

Introduction générale :

L'évolution rapide du marché de l'informatique et des télécommunications a fait naître une nouvelle forme de communication entre l'entreprise et ses clients. L'entreprise moderne est donc orientée vers une gestion efficace de son capital client véritable source de sa rentabilité et de sa pérennité. Ainsi se sont développés les numéros verts, les services clients, les services de réservation ... A la suite de ces évolutions , les centres d'appels ont connu une expansion considérable , moyen fiable de contact avec la clientèle. Ils connaissent depuis quelques années une croissance exponentielle .

L'évolution des centres d'appel, appelés aussi aujourd'hui "centres de contacts" ou "centres de relation client", correspond à une évolution de fond. Elle suit les changements survenus dans la culture d'entreprise notamment dans les modes de relation client et dans l'évolution du comportement des consommateurs.

Le développement de ces nouveaux services constitue un véritable enjeu économique pour l'entreprise. L'intégration de centres d'appels à des sites de commerce électronique est d'ores et déjà en place dans certains secteurs notamment dans la vente par correspondance. Tous les secteurs d'activité sont concernés par le développement de ce type de service, avec une dominante dans les domaines de l'informatique , des télécommunications, du tourisme, de la vente à distance et des finances.

Le développement de ce type de services conduit les entreprises à opérer des choix organisationnels. La recherche d'une meilleure productivité conduit certaines sociétés à regrouper en un seul lieu au niveau européen voire aussi dans les pays du Maghreb, leurs centres d'appels. Le choix s'opère notamment en fonction du multilinguisme, de l'existence d'une main d'œuvre diplômée disponible et des avantages pécuniaires que peut offrir le pays d'accueil .

L'interfaçage difficile entre les plates-formes TDM (Time Division Multiplexing) et les nouveaux modes de communication comme la collaboration par le Web, la messagerie texte, le courrier électronique et la vidéo (autant d'impératifs pour un centre de contact client du 21^{ème} siècle) empêche les centres d'appels traditionnelles d'atteindre leurs objectifs de service client et alourdit leurs coûts. Les plates-formes de téléphonie ouverte qui exploitent les réseaux de données IP normalisés ne connaissent pas ce type d'handicap.

L'infrastructure de centre de contacts IP apporte à l'entreprise un avantage décisif, elle est indépendante du lieu . Tant qu'ils disposent d'un accès au réseau IP LAN ou WAN de l'entreprise, ses agents peuvent travailler partout comme s'ils se trouvaient au siège social, et répondre le plus efficacement possible aux demandes de ses clients.

Avec un centre de contact IP, l'entreprise peut utiliser plus efficacement les compétences de ses employés en agence ou leur permettre de travailler à domicile et de devenir ainsi, à distance, de précieuses ressources d'information.

La souplesse d'un tel modèle permet à l'entreprise d'ajuster le nombre de ses agents en ligne en fonction des besoins : elle peut mettre en œuvre, de manière simple et

économique, des programmes d'assistance clientèle qui avec des opérateurs intervenant dans le monde entier pour fournir une assistance 24 heures sur 24, 7 jours sur 7.

Les réseaux IP d'interaction client offrent des possibilités tout aussi importantes pour le support de multiples méthodes de communication. Les forces du marché ont accéléré le recul du téléphone comme unique support interactif. L'utilisateur s'attend aujourd'hui à pouvoir choisir entre une collaboration Web, la messagerie texte, le courrier électronique ou des communications vidéo. Comme le développement de la plupart de ces fonctionnalités s'appuie sur des normes ouvertes, il est facile de les installer en toute transparence dans un centre de contact IP à architecture ouverte, et de les gérer de manière intégrée pour offrir aux clients une expérience unifiée sur l'ensemble des modes d'interactivité.

dans ce contexte, l'objectif de notre projet de fin d'études est de faire une recherche détaillée sur la procédure d'implémentation d'un Call center IP dans le réseau GSM.

C'est en prenant appui sur le stage effectué au sein de l'entreprise ORASCOM TELECOM ALGERIE basée à Dar el Beida que j'ai axé mon travail. Le présent rapport est organisé en quatre chapitres :

Le premier chapitre est scindé en deux parties : la première est consacrée à la présentation générale du call center ainsi que ses principales fonctionnalités. La seconde partie s'appuie sur le concept de migration du PABX vers un réseau PABX-IP/ VOIP. Le deuxième chapitre est essentiellement consacré à la VOIP et la TOIP ainsi que leurs fonctionnalités. Le troisième chapitre traitera les différentes architectures du Call center IP et des pratiques de sécurisation. Le dernier chapitre résumera les différentes interconnexions du call center avec le réseau GSM.

Enfin, nous avons retenu dans une conclusion générale, les grandes lignes de ce qui, à notre sens, mérite une attention toute particulière de la part des lecteurs.

Chapitre I

Etude d'un Call Center IP.



Chapitre I : Etude du call center

Introduction :

L'évolution du marché des télécommunications, le couplage de la téléphonie et de l'informatique, l'arrivée de la téléphonie mobile et d'Internet sont autant d'éléments moteurs du développement des centres d'appels. L'intégration des centres d'appels à des sites de commerce électronique est d'ores et déjà en place dans certains secteurs, transformant ce dernier en centre de contact multimédia, le nombre de web call-centers devraient s'accroître dans les prochaines années.

De ce fait, les centres d'appels remplissent de plus en plus de fonctions. Leurs missions tendent à se diversifier. Ils peuvent intervenir sur toute la chaîne du service client.

Les conséquences de ces évolutions en terme d'organisation ont été énormes. Les process s'industrialisent, Les technologies ont beaucoup évolué et le couplage de l'informatique à la téléphonie a permis d'apporter beaucoup plus d'efficacité en évitant les déplacements et en apportant une réponse immédiate.

La migration du call center vers ces nouvelles technologies a permis de personnaliser et de mieux suivre la relation client.

I.1. Présentation d'un centre d'appel:

Un centre d'appels ou « call center » en anglais ; est une entité dont la vocation est de gérer à distance la relation que les entreprises souhaitent entretenir avec leurs clients et prospects. « C'est un ensemble de moyens humains, organisationnels et techniques mis en place afin de répondre à la demande et aux besoins de chaque client adopté »

Ce concept met en jeu quatre composantes majeures à savoir :

- *La technologie* (téléphonie, informatique, logiciels, bases de données).
- *La logistique* (immobilier, mobilier, ergonomie de l'environnement matériel.).
- *Les ressources humaines* (téléopérateurs, superviseurs, formateurs...).
- *Une culture et des méthodes marketing* (stratégie de l'entreprise, relation client ...).

Ces composantes doivent être conçues en cohérence avec les différents canaux de distribution et d'information de l'entreprise pour gérer au mieux la relation avec les clients.

Un centre d'appel a pour principale vocation la gestion et la rationalisation de la relation client à distance qui peut être conservée dans une base de données informatiques.

En émission ou en réception d'appels, un centre d'appels est axé sur trois piliers, à savoir : La vente, Le support ou l'assistance technique et l'information.

Quelque soit son domaine d'activité, un centre d'appels doit apporter une valeur ajoutée identifiable et mesurable.

I-2 Architecture d'un centre d'appels

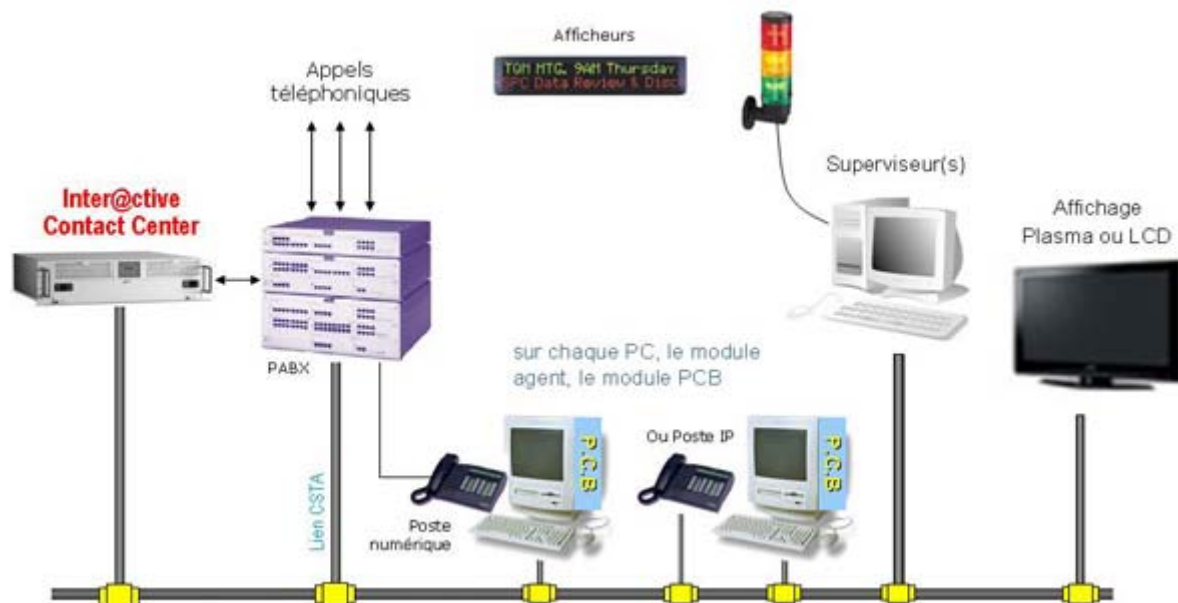


Figure 1: Architecture d'un Centre d'appels

Un centre d'appel comporte essentiellement :

I.2.1. Le PABX (Private Automatic Branch Exchange) : autocommutateur privé sur lequel viennent se greffer les autres technologies . premier filtre entre l'appelant et l'appelé, c'est un standard téléphonique amélioré qui constitue le centre névralgique d'un centre d'appel.

I.2.2 L'ACD (Automatic Call Distribution)

C'est un outil de routage permettant de gérer les appels entrants et de les transférer vers les téléopérateurs en fonction de leurs disponibilités. Son objectif principal est de minimiser le temps d'attente des clients.

I.2.3 Le SVI (Serveur Vocal Interactif)

il permet à un appelant, à la fois de transmettre des informations saisies soit manuellement à partir du clavier de son téléphone, soit grâce à la reconnaissance vocale, et d'obtenir des informations à partir d'une voix enregistrée ou synthétisée. Les centres d'appels ont recours aux serveurs vocaux, soit pour aiguiller les appels, soit pour fournir de l'information au client sans l'intervention d'un téléconseiller.

I.2.4 Le Prédictive Dialer(système prédictif)

C'est un outil d'émission d'appels. Ce système compose automatiquement, par anticipation, les numéros listés dans les fichiers du centre d'appels. Il détecte également les faux numéros, les répondeurs automatiques et programme le rappel des numéros occupés.

I.2.5 Le CTI (Couplage Téléphonie Informatique)

C'est un ensemble de logiciels permettant la réception automatique sur l'écran des données de l'appelant.

I.2.6 Le logiciel CRM

C'est un logiciel qui permet à chaque téléopérateur d'enrichir au fur et à mesure la base de donnée clients qui se transforme en instrument marketing de grande qualité.

I.2.7 Le logiciel de tableau bord

C'est un logiciel de mesure et de surveillance du flux d'appels en temps réel. Il facilite l'optimisation de la gestion du centre d'appel.

I.3 Architecture technique :

Application metier sur plateau de CALL CENTER :

Dans un call center ,les agents utilisent les applications suivantes

I.3.1 L'application de monitoring :

pour enregistrer les conversations des agents et des clients, dans le but d'améliorer la qualité, cet enregistrement se fait toujours de manière aléatoire et non ciblé, car l'écoute intentionnée d'une conversation est interdite.

1.3.2 L'application de fax :

La loi algérienne oblige l'identification des abonnées, de ce fait , le centre d'appels reçoit régulièrement de ses centres de services des fax numérisés qui sont archivés automatiquement sur les Serveurs du call-center en vue des identifications et activations.

I.3.3. L'application WFM :

Application de work force management : il s'agit d'un outils qui permet d'auditer le rendement de chaque agent instantanément permettant ainsi d'établir des stratégies de travail et de meilleure gestion des ressources humaines.

I.3.4. L'application d'auto-dialer :

application qui permet d'appeler automatiquement les clients pour des campagnes de nouveaux produits, d'identification, de bonus etc....

I.4. Environnement et matériel utilisés:

L'environnement de travail:

il doit tenir compte de l'acoustique « l'isolation phonique »avec des parois vitrées pour réduire les bruits périphériques et L'ergonomie c'est a dire « l'intégration fonctionnelle des outils pour offrir les meilleures conditions de travail.

L' espace:

il doit être éclairé , isolé, calme et adapté au dimensionnement de l'équipe et de toute la structure .Il est conseillé d'installer une salle de détente.

les ressources humaines:

Il s'agit principalement des téléconseillers qui doivent être dotés de qualités telles que la persuasion, la facilité verbale, la patience et l'assurance de soi.

Les superviseurs doivent être de bons et rigoureux techniciens du marketing direct car c'est eux qui dirigent les groupes de téléacteurs, assurent la gestion des flux téléphoniques et organisent la présence du personnel sur les plateaux.

Quant au coach, il assure le lien entre le plateau et les agences, élabore les scripts et actualise les données.

Sans oublier les informaticiens, les responsables, les statisticiens et les formateurs qui assurent une formation continue sur les produits et les services de l'entreprise.

I.5 Les différents types de centres d'appels :

1.5.1. L'internalisation :

On parle d'internalisation ou « Insourcing » d'un centre d'appels lorsque celui-ci est pris en charge au sein de l'entreprise. Le choix de cette alternative est conçu lorsque la firme souhaite maîtriser et contrôler l'ensemble des procédures et la totalité des informations provenant de ses clients. L'intégration est avantageuse dans la mesure où le téléopérateur peut à tout moment orienter son entretien téléphonique et satisfaire son client tout en gardant la confidentialité des informations échangées. Parallèlement, les responsables du centre travaillent en cohérence avec les autres départements de l'entreprise.

Le téléconseiller interne est bien formé pour répondre aux attentes des clients : ses prérogatives sont :

- *La téléprospection et prise de rendez-vous.
- *la télévente : qui exige une confidentialité des données.
- *Le help desk ou le support technique : qui exige une argumentation que seuls les spécialistes dûment formés au sein de l'entreprise peuvent fournir.

L'entreprise détient ainsi un contrôle continu sur ses employés assurant leur formation et évaluation de leur travail.

I.5.2. L'externalisation :

L'externalisation ou « out sourcing » est le fait de confier l'exploitation d'un centre d'appels à une société juridiquement et physiquement extérieure à l'entreprise. La sous-traitance est surtout utilisée pour assurer la régulation du fonctionnement du service consommateurs en particulier la gestion des appels entrants à certaines heures (soirées, nuits, week-ends...). Elle permet une bonne gestion de la relation client grâce à la compétence et au professionnalisme des téléopérateurs extérieurs. Ainsi s'instaure un véritable partenariat entre les différents départements de l'entreprise. Par ailleurs, la sous-traitance permet non seulement de minimiser les lourds investissements consentis par l'entreprise mais

également de faire face à tout imprévu. Le seul écueil reste la confidentialité avec le risque que le téléopérateur puisse divulguer des informations confidentielles.

I.5.3. Une solution mixte :

D'un autre point de vue, un centre d'appels peut être *formel* ou *informel*. Un centre d'appels *formel* dispose d'une identité bien déterminée dans l'organigramme de l'entreprise (locaux identifiés, architecture technique spécialisée, une organisation humaine spécifique, un responsable général, rattachement à une direction particulière ...)

Par contre, un centre d'appel informel ne dispose pas de ces attributs propres et dans ce cas, il n'existe pas de département pour la gestion des appels et les commerciaux peuvent traiter les appels tout en effectuant leurs tâches principales.

I.6. Objectifs et performance d'un call center :

Peu importe sa vision, sa stratégie ou encore ses ressources, la performance demeure l'objectif principal de toute entreprise. Elle se traduit par la *fidélisation et la satisfaction du client*, c'est l'aptitude à répondre à tous les appels, à toutes les demandes afin de garder le client. Ainsi la performance consiste à satisfaire le client et le fidéliser tout en augmentant le chiffre d'affaires dans une position meilleure que la concurrence. La qualité du service est un objectif important pour les dirigeants des centres d'appels, elle doit s'appuyer sur six caractéristiques :

- *L'accessibilité, La promptitude, La fiabilité, le choix des services, un personnel courtois ainsi qu'une assistance administrative.*

Un centre d'appels remplit trois rôles auprès de sa clientèle : Fournir de l'information précise sur un produit ou un service, conseiller pour les produits comptant un numéro vert puis finalement résoudre des problèmes et effectuer des transactions.

Pour bien informer, conseiller et gérer les réclamations, il est nécessaire de créer une base de données fiable grâce à l'information communiquée par le client.

I.6.1. Les missions en réception d'appels :

C'est principalement le service consommateur (service client) et l'assistance technique « help desk » : il est en permanence à l'écoute des clients car il informe, conseille et gère les réclamations.

L'assistance technique :

Les téléopérateurs fournissent une aide technique (help desk) aux consommateurs en répondant à leurs diverses demandes d'information concernant un produit particulier (installation d'un nouveau logiciel, problèmes de spécification ou de configuration ...) Ils prennent en charge les activités de types « help line » ou « hot line » traditionnellement assurées par le fabricant d'équipement ou le fournisseur de logiciel.

I.6.2. Les missions en émission d'appels :

Elles concernent essentiellement:

- Le télémarketing qui est un moyen de communication directe de l'entreprise avec ses différents publics
- La télévente qui consiste à vendre par téléphone des produits ou des services
- Le télé recouvrement dont l'objectif est de relancer par téléphone les clients n'ayant pas réglé leurs dernières créances.

I.6.3. La productivité :

Pour les gestionnaires, c'est répondre à un nombre maximal d'appels en un minimum de temps.

I.7. Les déterminants de la performance d'un centre d'appels :

Pour réussir, un centre d'appels doit maîtriser deux facteurs ; la technologie, les ressources humaines et dans chacun de ces facteurs il faut intégrer un mode de management.

La technologie utilisée est assez complexe et offre plusieurs possibilités de manipulation.

Elle se présente en tant qu'outil important aux mains des dirigeants afin d'optimiser la performance de la plateforme téléphonique .

Les ressources humaines, particulièrement les téléopérateurs, représentent les principales charges des calls centers, leur satisfaction influence celle des clients ainsi, ils jouent un rôle primordial dans la performance de ces derniers .

I.7.1 Evolution des technologie

Dans la première partie du chapitre , on a étudié les différentes composantes technologiques d'un centre d'appels d'une manière générale.

Dans cette section, on va déterminer le rôle de leur évolution dans l'amélioration des conditions de travail des agents et le rendement du call center.

I.7.1.1. Nouvelle génération de couplage téléphonique informatique

- Le traitement des appels télépho

Dans un centre d'appels, c'est l'ACD (Distributeur automatique des appels) qui prend la charge du traitement, de la gestion et de la distribution des appels vers un télé conseiller ou un groupe de téléopérateurs.

L'ACD s'avère un véritable outil d'optimisation et de fidélisation grâce à une bonne gestion des files d'attentes et une meilleure qualité d'accueil et d'écoute des clients.

- Le traitement de base de données :

La gestion des bases de données est automatique. L'ACD lie le script aux bases de données. Pendant l'entretien téléphonique, le téléopérateur voit s'afficher « l'historique du client » (nom, prénom, opérations du client avec l'entreprise, réclamations précédentes... il peut extraire un client d'une base de données de plusieurs millions de personnes, se concentrer sur l'ensemble des transactions que ce client a effectuées avec l'entreprise, mettre à jour les données et réinsérer le client dans la base en quelques secondes.

Enfin, la base de données améliore la productivité de l'entreprise et optimise le travail des agents. En effet, grâce à une codification claire le service marketing ,elle pourra mener des campagnes très ciblées auprès des clients potentiels.

Objectifs et avantages du CTI:

L'application CTI consiste à afficher à l'écran du téléconseiller toutes les informations disponibles sur un client à partir de la base de données du centre d'appels.

- **les objectifs d'un CTI :**

Généralement, le CTI cherche à atteindre quatre objectifs :

- ___ Augmenter la rentabilité de la société en automatisant des tâches longues et répétitives
- ___ Vendre plus aux clients existants en croissant leurs besoins et leurs niveau.
- ___ Fidéliser le portefeuille de clients en adaptant l'offre à leurs attentes.
- ___ Attirer une nouvelle clientèle.

- **Les avantages d'un CTI sont multiples :**

En effet, les appels traités sont suivis et enregistrés dans les centre d'appel . Le télé conseiller voit s'afficher sur son écran tous les enregistrements que possède l'entreprise dans ses bases de données. Le système CTI reconnaît le sujet abordé et propose au téléopérateur une synthèse du savoir de l'entreprise dans ce domaine. Ainsi , l'opérateur peut orienter la conversation et personnaliser l'entretien téléphonique en se concentrant sur les éléments les plus pertinents qui lui permettront de répondre au mieux aux besoins des clients de manière efficace et rapide .

1.7.1.2.Mesure et contrôle de la qualité du centre d'appels par l'ACD :

Les dirigeants d'un centre d'appels accordent une grande importance au contrôle de la qualité pour cela ils font appel a un superviseur qui s'assure de la qualité des services proposés aux clients.

L'affichage des statistiques fournies en temps réel par les logiciels de l'ACD autorise un suivi précis du fonctionnement d'un plateau ou d'un groupe de télé conseillers.

Grace à des écrans standards ,le superviseur peut vérifier instantanément le comportement des téléconseillers ainsi que leurs prestations. La mise en place d'un centre d'appels présente pour l'entreprise un véritable investissement. L'objectif d'un centre d'appels présents est de fidéliser la clientèle tout en augmentant le chiffre d'affaires de l'entreprise.

1.7.1.3. Le service vocal interactif (SVI) :

Comme nous l'avons déjà cité précédemment, un SVI accueille et oriente le client en lui proposant une succession de choix à valider sur le clavier de son téléphone vers l'interlocuteur le plus compétent.

Le SVI pourrait devenir l'outil incontournable pour effectuer des économies substantielles de main d'œuvre à condition que le centre d'appels puisse employer suffisamment de téléconseillers pouvant traiter un certain nombre d'appels.

II. PABX et centre d'appels IP :

II-1 Définition du PABX

Il s'agit généralement d'un boîtier ou d'un coffret central assurant le lien entre les réseaux téléphoniques et les communications internes du call center. Grâce à lui, tout appel est acheminé à son destinataire ou stocké sur une messagerie en cas d'absence de ce dernier. Il peut également s'agir d'une télécopie ou de tout autre fichier, le PABX gérant aussi bien la voix que les données. Plusieurs périphériques peuvent être connectés au PABX à l'aide d'interfaces : postes téléphoniques analogiques ou numériques, micro-ordinateurs en réseau..

Aujourd'hui, la gamme des PABX est des plus vastes. Cependant, qu'il soient intégrés dans le central téléphonique principal ou déportés dans un boîtier, il représente l'élément central qui :

- distribue les appels téléphoniques arrivés (qui peuvent être des appels SDA),
- autorise les appels téléphoniques départs (vers un ou plusieurs opérateurs de télécommunications, suivant les droits),
- gère les terminaux téléphoniques (ainsi que les appels internes), qui peuvent être des postes numériques ou analogiques,
- gère toutes les autres fonctionnalités ou options (CTI, CSTA, Taxation...)

II-2 Architecture et mode de fonctionnement

Le PABX se subdivise en deux sous-ensembles principaux :

- Le réseau de connexion à travers lequel s'effectue la connexion
- Les organes de commande qui effectuent les différents dialogues permettant l'établissement de la communication.

II-2-1 Architecture matérielle

Un autocommutateur privé possède sa propre intelligence pour faciliter la commutation des appels voix. Cette intelligence est gérée par au moins une unité centrale (CPU), avec des

processeurs d'entrées/sorties qui gèrent les interfaces de lignes et d'équipements de postes, avec également une mémoire vive (sauvegardée en général par une pile pendant à peu près cinq années). Il existe aussi des unités centrales équipées de disques durs, ainsi que des

modèles de CPU pouvant être dupliqués en temps réel, afin d'assurer la continuité du service téléphonique.

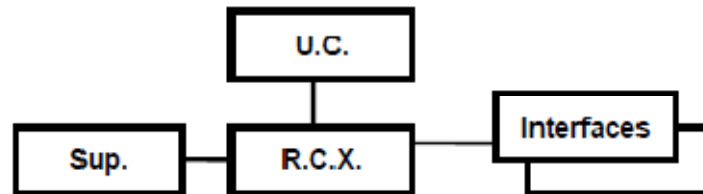


Figure 2 : architecture interne d'un Pabx

UC : Unité de commande

L'unité de commande d'un PABX est composée d'un microprocesseur, d'une mémoire RAM et d'une PROM. c'est l'élément du PABX qui assure les fonctions de commandes (recherche d'itinéraire, taxation, signalisation et la rupture de communications).

RCX : Réseau de Connexion, Il est constitué d'une matrice temporelle composée d'une mémoire de parole, d'une mémoire d'adresse et d'une base de temps. Son rôle est d'assurer les connexions mise en places entre les supports de communications.

Sup : Supervision, ou signaleurs

Ce sont les organes qui reçoivent et qui émettent des informations. il dépendent du système de signalisation utilisé dans le réseau. ainsi nous avons plusieurs dont voici quelques uns :

SS7 MFR2 (2 parmi 6) MFR1 et MF SOCOTEL (2 parmi 5)

II.1.2. Interfaces

Ils constituent l'accès à l'extérieur. Ce sont des joncteurs d'abonnés pour le raccordement des lignes. On a des joncteurs d'un réseau pour le raccordement sur le réseau public RTC. Ainsi nous distinguons deux types d'interfaces :

❖ Les interfaces internes

On a des cartes électroniques qui permettent le raccordement des lignes d'utilisateur sur le PABX.

- Carte d'utilisateur analogique
- Carte d'utilisateur numérique
- Carte d'utilisateur mobile (DECT).

Les interfaces internes sont deux types :

- Type analogique : Ils sont utilisés pour le raccordement des :
 - Postes simples ;
 - Des lignes analogiques
 - Des organes de signalisation et auxiliaire

- Type numérique : Ils sont utilisés pour le raccordement des :
 - Des postes numériques fonctionnant en bus avec un numéro SDA
 - modem RNIS
 - Routeurs
 - Postes « intelligents » communiquant avec le système par intermédiaire du clavier écran offrant une multitude de services.

❖ **Les interfaces externes** (accès au réseau public)

Il comporte les cartes RTC, les cartes RNIS, les passerelles GSM (accès direct au réseau mobile), carte IP (accès au réseau Internet). Ils sont utilisés pour avoir accès à l'extérieur. Plusieurs types de lignes peuvent être utilisés. On les séparera en deux catégories principales:

- lignes analogiques
- lignes numériques

L'utilisation de ces lignes sera détaillée plus loin.

II.1.3. Les différentes capacités de PABX

•**Les Autocommutateurs de petite capacité** (<50 postes) : il est comme son nom l'indique de capacité réduite, mais sur une carte de base, faisant office d'unité centrale, il est équipé de slots d'extensions lui permettant de recevoir d'autres cartes. Il peut faire cohabiter les deux modes analogique et numérique.

•**Les Autocommutateurs de moyenne capacité** (<128 postes) : sur une carte de base appelée fond de panier ou d'alvéole, viennent s'interconnecter différentes cartes avec des fonctions bien définies, ex :

- une alimentation
- une carte UC avec microprocesseur et mémoire
- carte lignes réseaux, RNIS analogique
- carte de postes de 4 à 16
- carte message

•**Les Autocommutateurs de forte capacité** (>300 postes) : sur le même principe que les moyennes capacités mais avec la faculté de se mettre en réseau. Il peut se composer de :

- une alimentation externe 48 V continu avec + à la masse
- une ou plusieurs unités centrales
- carte de postes de 16 à 32
- ventilateurs
- carte interface fibre optique

II.1.4. Mode de fonctionnement

Le PABX pour fonctionner a besoin de logiciels :

- le Logiciel de Base

Il permet à l'UC d'être fonctionnelle et permet aussi l'exploitation de toutes les ressources matérielles comme logicielles du PABX.

- Le logiciel de traitement d'appel

Il permet de détecter, d'analyser et de donner une suite qui peut être favorable ou défavorable à l'appel. Tout cela se fait à travers la réception d'un numéro d'émission du signal de la tonalité, la recherche d'itinéraire, l'ordre de connexion, l'émission du signal de sonnerie et l'ordre de déconnexion

- Le logiciel de maintenance

Il détermine la possibilité qu'a le PABX de faire lui-même des tests, de détecter des anomalies et de les signaler par édition sur télé imprimeur. Notons que la performance d'un PABX tient compte de :

- La capacité mémoire que celle-ci possède pour effectuer ses différentes fonctions.
- Le nombre de postes connectable
- Les services offerts

II.1.5. Fonctionnement

Un PABX, quel qu'il soit, est alimenté en courant faible (48 V continu) et possède une autonomie de quelques heures. Il alimente plusieurs postes qu'ils soient analogiques ou numériques. Le numéro de l'appelé est la seule source d'information de l'autocommutateur. Ce numéro doit être analysé, ou traduit en fonction du plan de numérotation. Ainsi les appels arrivés sur les lignes connectées au PABX sont distribués « selon la programmation effectuée » sur un poste faisant office de standard, ou sur un poste SDA directement. En règle générale, le premier chiffre indique que l'appelé est sur le même PABX que l'appelant. Les autres chiffres suivants désignent la ligne correspondant à l'appelé. Si le premier chiffre ne correspond pas aux chiffres de l'autocommutateur, cela signifie que l'appelé est sur un autre réseau (autocommutateur). Dans ce cas, le premier chiffre représente le numéro de l'autocommutateur de l'appelé ; et les derniers chiffres la ligne correspondant à l'appelé.

II.1.6. Evolution des PABX

Le PABX a connu plusieurs évolutions :

♦ La 1ère génération est apparue dans les années 1960. Elle permettait de transporter uniquement la voix et utilisait la commutation spatiale, c'est-à-dire qu'une fois un itinéraire établi, il sert de support exclusif à une seule communication. C'est le PABX électromécanique.

♦ La 2ème génération date du milieu des années 1970. Elle offre la commutation de données mais la voix et les données se trouvent sur des lignes séparées. Le réseau de connexion est temporel et les données sont reliées entre elles par l'intermédiaire d'une ligne multi-voie. Un intervalle de temps est régulièrement affecté à chaque connexion, ce qui simplifie le réseau. Il est dit PABX électronique.

♦ La 3ème génération correspond à l'avènement des réseaux numériques à intégration de service au début des années 1980. Elle est caractérisée par le multiplexage de la voix et des données sur le même port du PABX. La commutation est de type temporel mais les voix et

les données sont traitées différemment. Le raccordement au réseau public se fait grâce à des liaisons MIC (Modulation par impulsions codées) à 2Mbits/s. On l'appelle PABX numérique.

o Puis elle fut améliorée dans les années 1990 ce qui permis d'associer un commutateur de circuit à 64Kbits/s et un commutateur de paquet, chacun ayant son propre processeur. Ainsi les variations du tarif de données ne pénalisent pas la qualité des services téléphoniques.

♦La 4ème est intervenue avec les PABX-IP pour gérer les flux de paquet IP. Il est possible de connecter à la fois les téléphones numériques. Les octets étant encapsulés dans des paquets IP et des téléphones IP qui envoient directement des paquets IP

♦La 5ème génération est à l'étude avec un cœur complètement IP. On les appelle PCBX (fonctionnement sur l'ordinateur avec accès téléphonique sur Internet. Ce qui forme le couplage téléphonique informatique CTI(Computer telephonic integration)

II.2. Le PABX en réseau :

II.2.1. Nécessite d'interconnexion

L'apparition des PABX dans le monde des télécommunications constitue pour les entreprises une innovation très importante notamment les facilités offertes par ces derniers. Au vu de l'implantation sur plusieurs sites de certaines entreprises, L'interconnexion de plusieurs PABX a été mise en œuvre. Son objectif est d'exploiter au maximum les services offerts par ceux-ci. Ainsi cela permet :

- Au niveau technique: de partager des ressources, gestion du système téléphonique, et de permettre au PABX de dialoguer.
- Au niveau économique: de maîtriser le coût de communication, tout en offrant la gratuité des communications au sein de l'entreprise
- Au niveau sécurité: Supervision du canal, protection contre l'intrusion, suivi du trafic téléphonique

II.2.2. Les supports d'interconnexion :

Ce sont les moyens permettant d'assurer le transport de l'information entre les équipements. On les classe en deux grandes catégories.

❖ Les liaisons physiques

Ils sont :

De type analogique

- le câble à paires torsadées
- le câble coaxial

De type numérique

- la liaison MIC (Modulation par impulsion et codage
- le T2 (Accès primaire du RNISBE à 2.048Mbits/s avec 30 canaux B+16 canaux D)

- le T0 (Accès de base RNIS à 64 Kbits/s avec 02 canaux B+1 canal D)

Les canaux B pour la communication et le canal D pour la signalisation.

La fibre optique : support de transmission à débit est de type analogique ou numérique selon le type d'interface utilisé.

❖ les liaisons immatérielles

Ce sont des liaisons qui utilisent l'onde électromagnétique comme support de transmission de l'information. Ce sont :

- la BRL (boucle locale Radio)
- Les faisceaux hertziens
- Les satellites

Plusieurs techniques sont envisageables pour l'interconnexion. Les PABX sont raccordés aux RTC par un nombre de liaisons louées en rapport avec le trafic entrant et sortant.

II.2.3. L'interconnexion de Pabx :

L'interconnexion de PABX n'est nécessaire que pour les entreprises multi sites, l'objectif est de conserver au maximum les services des PABX. Plusieurs PABX peuvent s'interconnecter entre eux de manière homogène pour former un réseau (nœuds) mais peuvent être également interconnectés entre eux de manière hétérogène (pour les constructeurs différents par exemple). Un PABX peut fonctionner :

- En stand-alone (tout seul),
 - Ou en réseau homogène (mêmes machines, même protocoles, même versions équivalentes, échanges intelligents),
 - Ou en réseau hétérogène (même constructeur ou constructeur différent dialoguant sur des interfaces du même type QSIG ou RNIS avec un routage pseudo-intelligent qui dépend de la complexité du réseau et de la capacité de routage de chaque nœud),
 - Ou en réseau mixte (homogène sur une partie et hétérogène sur l'autre partie). On rappelle une fois encore qu'un central téléphonique privé permet d'effectuer du trafic téléphonique interne sans coûts de communications. Donc Il doit permettre aux usagers d'accéder au réseau public par des lignes dont le nombre est défini en fonction des besoins de ces derniers (les usagers) . Il est Installé chez l'utilisateur et peut être acheté ou loué chez un opérateur, sur le marché privé, auprès d'un fournisseur ou revendeur. Il a donc 2 faces distinctes :
- Côté réseau public;
 - Côté raccordements d'utilisateurs (internes).

II.2.4. Accès au réseau public (au central public)

Plusieurs types de lignes peuvent être utilisés. On les séparera en deux catégories principales:

- lignes analogiques.
 - lignes numériques.
- (voir les détails en annexe)

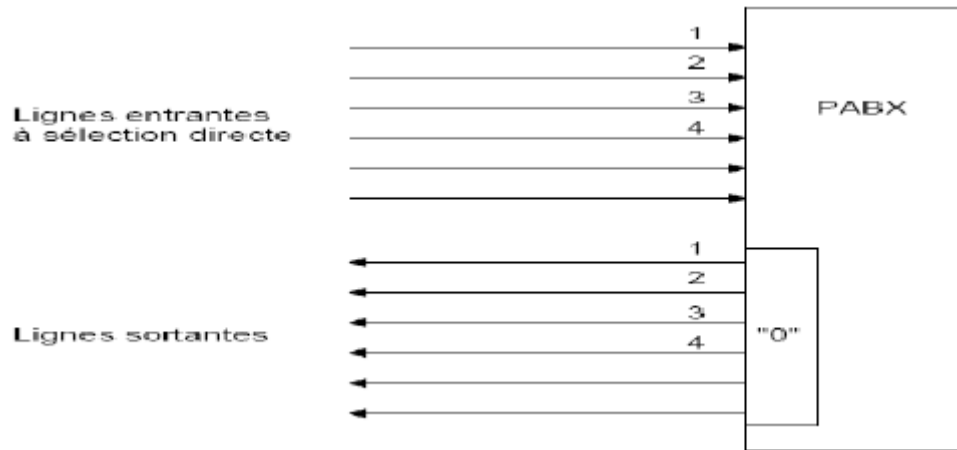


figure 3 :lignes e/s d'un Pabx

Quatre types d'exploitation des lignes peuvent être définis :

- ligne entrante.
Dans ce cas, on bloque, sur le PABX, la possibilité d'effectuer un appel sortant sur ces lignes. Cela se définit à choix pour les lignes analogiques simples, en multiple ou non, mais doit se programmer pour les lignes analogiques à sélection directe
- ligne sortante
. Dans ce cas, on ne publie tout simplement pas les numéros attribués à ces lignes. Elles ne sont donc jamais appelées.
- ligne double sens
. Dans ce cas, le numéro d'appel est connu et peut être atteint. Il est aussi possible d'effectuer du trafic sortant.
- ligne en multiple
Dans ce cas, les lignes peuvent être entrantes ou entrantes/sortantes. On associe au numéro principal, un nombre de lignes permettant l'acheminement du trafic entrant. Le nombre d'appels simultanés correspond au nombre de lignes en multiple. Ci-dessous, un exemple de combinaison des 4 types de lignes définis. Cela permet d'optimiser le trafic sur des lignes communes. Dans cet exemple, on peut recevoir 3 appels, deux sur un numéro multiple, un sur un numéro individuel. On peut sortir sur 3 lignes. Le nombre de communications avec le réseau public est de 4.

II.2.5. ETUDE DES RESEAU PABX

Ces dix dernières années les centres d'appels ont adopté massivement les standards d'Internet pour leurs réseaux informatiques de données, dont IP (Internet Protocol) le protocole de communication. En parallèle, le codage du signal « voix » permettant à cette dernière de devenir numérique (donnée), elle peut maintenant s'engouffrer sur les réseaux d'entreprises, d'opérateurs et sur Internet pour atteindre son destinataire.

les réseaux téléphoniques des entreprises sont bâtis autour des PABX (Private Automatic Branch Exchange) ou autocommutateurs. Ceux-ci assurent le transport des flux vocaux et la gestion des appels. Ces systèmes propriétaires ont été détrônés par des produits plus ouverts, surtout dans les centres d'appels.

Baptisés IPBX(Internet Protocol Branch Exchange), les nouveaux venus sont composés d'un gestionnaire d'appels et d'une passerelle d'accès au réseau public. Ils dissocient la gestion des appels et le transport des flux vocaux sur le réseau local

Une question importante pour comprendre une infrastructure de téléphonie sous IP est finalement de savoir où la voix se transforme en données :

1) après le terminal téléphonique au niveau du « central » de l'entreprise, PABX (Private Automatic Branch Exchange) ou PCBX (Private Computerized Branch Exchange), relié par une passerelle IP pour quitter l'entreprise, on parlera alors de PABX IP.

2) dès le terminal en le remplaçant par un téléphones IP flambant neuf qui exploite alors le réseau IP interne jusqu'au central de l'entreprise qui devient pour l'occasion un IPBX (Internet Protocol Branch Exchange)

3) ou finalement en supprimant le terminal de l'entreprise et en le remplaçant par le central d'échange d'un fournisseur externe, on parle alors d'IP Centrex - X pour eXchange - ce qui revient à connecter le réseau IP de l'entreprise à ce fournisseur, appelés aussi ITSP (Internet Telephony Service Provide) et par la même occasion à se libérer de l'offre d'un opérateur de téléphonie fixe traditionnel.

II.2.6. Le choix du réseau PABX

Pour tout projet, il convient d'en analyser les volets fonctionnels, techniques et financiers. Au plan fonctionnel :

Il s'agit de déterminer l'ensemble des services qui seront portés par le nouveau dispositif de convergence voix-données. Le téléphone peut en effet devenir un outil de communication multimédia, moins cher que l'outil informatique traditionnel (PC) et plus aisément déployable (exemple dans les entrepôts ou les usines). Le développement des réseaux locaux sans fil (Wifi) étend par ailleurs le champ de ces nouvelles applications à celui de la mobilité.

❖ Au plan technique :

Le réseau de l'entreprise, local (LAN) ou étendu (WAN), plus sollicité dans cette approche, doit avoir la capacité de supporter le trafic additionnel (la voix et les nouvelles applications). Le volume et la répartition des flux (notamment les pointes de trafic) permettront de dimensionner l'infrastructure entre le terminal téléphonique et l'IPBX, ou vers le IP Centrex.

Cependant, par construction, le protocole IP ne garantit pas un acheminement de tous les « paquets » dans l'ordre et dans des limites de temps. L'infrastructure globale - pas uniquement celle de l'entreprise - doit donc aussi viser à réduire le temps d'acheminement et la perte potentielle de paquets. Le choix d'un fournisseur de IP Centrex n'est donc pas neutre pour garantir une bonne qualité de service.

❖ **Au plan financier :**

Les coûts d'infrastructures IP représentent généralement un investissement initial plus élevé que les solutions classiques. Les coûts d'exploitation (maintenance, télécommunications) sont en revanche moins chers de 25% à 50% selon les cas.

Au-delà du court terme, il conviendra d'apprécier les incidences positives sur les investissements futurs qui auraient été nécessaires pour développer les nouvelles fonctionnalités (surtout si ces dernières représentent un réel avantage concurrentiel). En fonction de la capacité d'investissement de l'entreprise, le bilan financier peut faire ressortir que, dans certains cas, une solution progressive peut représenter le « bon » compromis (par exemple : pour certains sites, passage à un PABX IP pendant 2 ans puis bascule vers un IPBX ou un IP Centrex).

III. Types de réseau PABX :

III.1.1. Les PABX-IP (VoIP)

Un réseau PABX-IP ou VoIP remplace l'autocommutateur traditionnel ou le réseau téléphonique et attribue à chaque employé une extension personnelle, la possibilité de passer des appels conférence, de transférer et d'appeler d'autres collègues. Tous les appels sont passés par des paquets de données sur un réseau de données à la place du réseau téléphonique traditionnel. En utilisant la passerelle VoIP, vous pouvez vous connecter des lignes de téléphones existantes au PABX-IP et passer ainsi que recevoir des appels par le biais d'une ligne RTC normale. Pour cette raison les call center convertissent leurs réseaux traditionnels/autocommutateurs en réseau VoIP/PABX-IP à un rythme impressionnant.

III.1.2. fonctionnement du réseau téléphonique PABX-IP/VoIP

Un réseau téléphonique PABX-IP/VoIP est constitué d'un ou de plusieurs téléphones SIP / VoIP, d'un serveur PABX-IP et éventuellement d'une passerelle VoIP. Le serveur PABX-IP est similaire à un serveur proxy : les clients SIP, étant soit des soft phones ou du hardware téléphonique, enregistrés auprès d'un serveur PABX-IP, et lorsqu'ils désirent passer un appel, ils demandent au PABX-IP d'établir la connexion. Le PABX-IP possède un registre de tous les téléphones/usagers et de leur adresse SIP respectives et ainsi est capable de connecter un appel interne ou de router un appel externe soit par le biais d'une passerelle VoIP ou d'un fournisseur de service VoIP.

III.1.3. Avantages des réseaux PABX-IP :

- Installation et configuration bien plus faciles que celles d'un réseau propriétaire:

Un logiciel lancé sur un ordinateur peut prendre avantage de la puissance avancée de traitement de l'interface utilisateur et des fonctionnalités Windows de l'ordinateur. Quiconque a des connaissances de base en informatique et sur Windows, peut installer et configurer l'autocommutateur. Un système propriétaire nécessite souvent l'intervention d'un technicien bien formé sur ce système propriétaire !

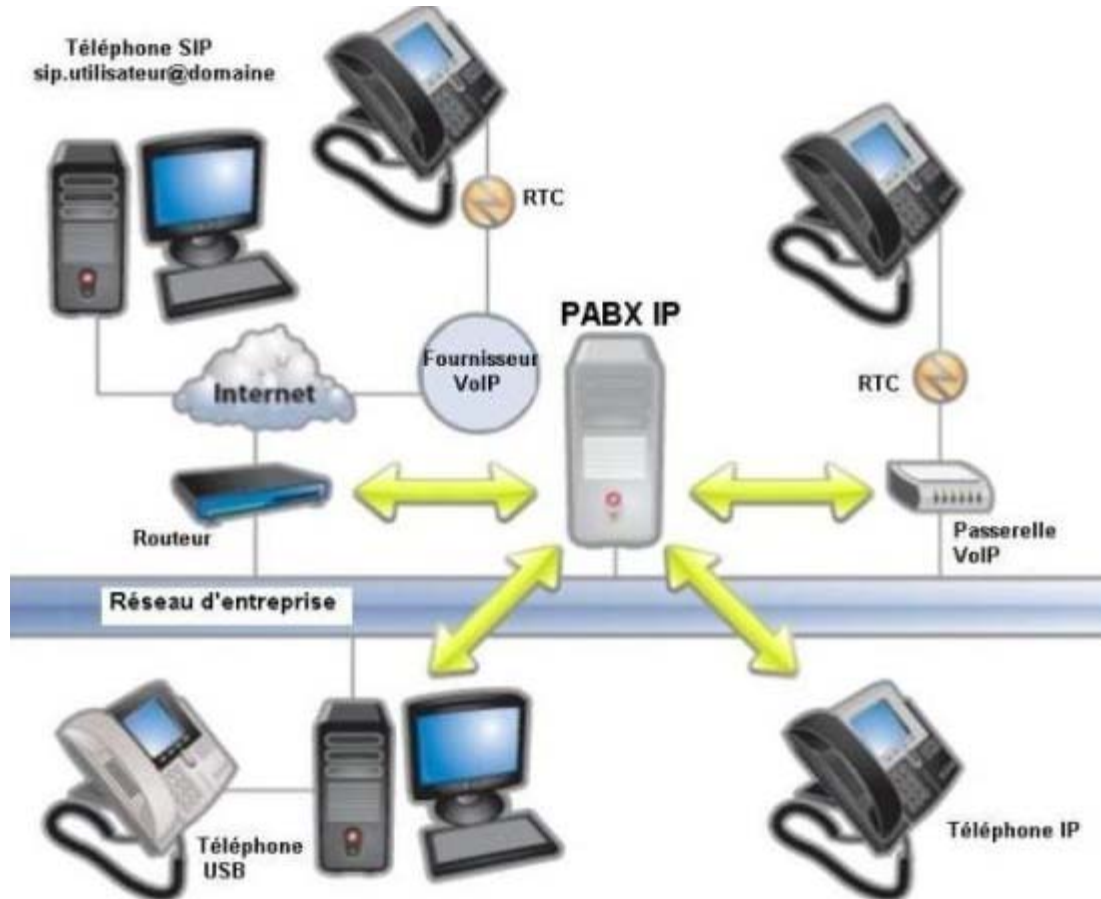


Figure 4 : Schéma d'un réseau Pabx IP

- Gestion facile via l'interface web de configuration :
Un réseau VoIP a une interface web de configuration qui vous permet une maintenance et un réglage faciles de votre réseau téléphonique. Les réseaux propriétaires ont, la plupart du temps, des interfaces compliquées que seuls les installateurs du réseau téléphonique peuvent utiliser efficacement.
- Réduction des coûts des appels :
Vous pouvez faire des économies substantielles en utilisant un fournisseur de service VoIP pour les appels longue distance et internationaux. Connectez facilement vos réseaux téléphoniques entre bureaux et filiales et téléphonez gratuitement.
- Aucun branchement téléphonique séparé nécessaire
 - il utilise le réseau informatique:

Un réseau VoIP vous laisse connecter le matériel téléphonique directement au port de réseau informatique standard (qu'il peut partager avec l'ordinateur adjacent). Les solutions téléphones peuvent être installés directement sur le PC. Cela signifie qu'il n'y a aucun réseau de branchement séparé à installer et maintenir pour le réseau téléphonique, vous donnant ainsi une plus grande flexibilité pour l'ajout d'utilisateurs/d'extensions. Si vous emménagez dans des locaux et n'avez pas encore installé les prises téléphoniques, vous pourrez faire des économies substantielles en installant uniquement un réseau informatique.

- **Aucun verrouillage de vendeur :**
 - Utilise des téléphones standard : les réseaux VoIP sont des standards ouverts – tous les réseaux VoIP utilisent SIP comme protocole. Cela signifie que vous pouvez utiliser Presque n'importe quel matériel téléphone VoIP SIP ou passerelle VoIP. A l'opposé, un réseau propriétaire nécessite souvent un téléphone propriétaire afin d'utiliser les fonctionnalités avancées, et des modules d'extension propriétaires pour l'ajout de fonctionnalités.
- **Adaptable :**
 - Les systèmes propriétaires sont faciles à agrandir : l'ajout de lignes téléphoniques ou d'extensions nécessite souvent des mises à jour du matériel très coûteuses. Dans certains cas vous devrez renouveler l'intégralité de votre réseau téléphonique. Il n'en est pas de même avec le réseau VoIP : un ordinateur normal peut facilement gérer un large nombre de lignes téléphoniques et d'extensions – il suffit d'ajouter des téléphones à votre réseau pour l'agrandir!
- **Meilleur service et productivité :**
 - Puisque les appels se font à partir d'ordinateur, il est plus facile pour les développeurs de s'intégrer avec les applications des entreprises. Par exemple : un appel entrant peut automatiquement amener à l'écran le fichier client de l'appelant. Améliorant ainsi de façon incroyable le service clientèle et réduisant aussi les coûts en passant moins de temps sur chaque appel. Les appels sortant sont directement passés à partir de Outlook, annulant la composition du numéro de téléphone
- **Le téléphone informatique plus facile à utiliser :**
 - Il est souvent difficile d'utiliser les fonctionnalités avancées des réseaux téléphoniques telles que les appels conférences avec les téléphones propriétaires. Cela n'est pas le cas avec téléphones SIP – toutes les fonctionnalités sont faciles à utiliser à partir d'un GUI.
- **Plus de fonctionnalités standards incluses :**
 - Puisque le réseau VoIP est basé sur un logiciel, il est plus simple pour les développeurs de le concevoir, d'ajouter et d'améliorer les jeux de fonctionnalités. C'est pourquoi la plupart des réseaux VoIP comportent des fonctionnalités riches et variées, y compris l'opérateur automatique, répondeur, appels en file d'attente bien d'autres. Ces options sont souvent coûteuses avec les systèmes propriétaires.
- **Meilleur contrôle via meilleur reporting :**

- Les paramètres VoIP enregistrent les informations des appels entrant et sortant sur une base de données sur votre serveur, vous permettant ainsi un reporting bien plus efficace de tous les appels et de tout le trafic.
- Meilleure vue d'ensemble de l'état actuel du système et des appels:
 - Les systèmes propriétaires nécessitent souvent des systèmes onéreux afin d'avoir une idée de ce qui se passe sur votre réseau. Même dans ce cas, les informations fournies sont – au mieux – cryptiques. Avec un système VoIP, vous définissez quels utilisateurs pourront visualiser l'état du réseau graphiquement par le biais du navigateur internet.
- Permet aux utilisateurs de brancher leur téléphone n'importe où dans le bureau :
 - Les utilisateurs prennent leur téléphone, le branche au port Ethernet le plus proche tout en conservant leur numéro !
- Itinérance des utilisateurs rendue facile :
 - Les appels peuvent être transférés n'importe où dans le monde grâce aux caractéristiques du protocole SIP.

III.1.4. Connexion d'un réseau/autocommutateur traditionnel au réseau IP :

Ainsi la passerelle VoIP permet de passer des appels par le biais de la VoIP. Les appels peuvent ensuite être passés via un fournisseur de service VoIP, ou dans le cas d'une entreprise avec plusieurs bureaux, les coûts des appels entre bureaux peuvent être réduits en les acheminant via Internet. Les passerelles VoIP sont disponibles sous forme d'unités externes ou sous forme de cartes PCI. La vaste majorité d'appareils sont des unités externes. Une passerelle VoIP possède un connecteur pour le réseau IP et un ou plusieurs ports pour pouvoir connecter les lignes téléphoniques.

III.2. IPBX :

III.2.1. Définition :

Un **IPBX** est un standard téléphonique utilisant le réseau IP pour les communications internes ou externes.

L'IP de **IPBX** signifie Internet Protocol d'où le terme de Voix sur IP ou VoIP par opposition au PABX (Private Automatic) qui utilise le réseau télécom traditionnel. Mais IPBX et PABX peuvent aussi emprunter tous les deux les mêmes fils. C'est le codage de la voix et des données qui fait la différence.

III.2.2. Fonctionnement

La technologie VoIP (Voice over IP) des standards IPBX permet de transformer le signal vocal émis vers un récepteur (IP phone ou soft phone), en données numériques circulant sur un réseau tel qu'Internet. Les informations sont transférées par paquets IP et sont reconverties en signaux sonores par l'appareil récepteur.

Les IPBX connaissent un succès croissant auprès des entreprises grâce à leurs faibles coûts de communication et au grand nombre de fonctionnalités qu'ils proposent. Ils sont amenés à remplacer tout autre type de standard de téléphone au cours des prochaines années.

Un IPBX ne peut fonctionner qu'avec un des deux types de téléphones suivants : IP phone ou soft phone.

Un IP phone dispose de ports Ethernet pour se connecter sur les ports réseau afin d'utiliser Internet comme support de communication. Un IP phone n'est donc qu'une évolution du téléphone classique, conçu pour fonctionner avec un IPBX.

Un soft phone est un IP phone sous forme de logiciel . Il s'agit donc avant tout...d'un logiciel.

III.2.3. Fonctionnalités IPBX

L'avantage principal du standard téléphonique IPBX est la réduction des coûts due à l'utilisation de la téléphonie sur IP :

- Le standard téléphonique IPBX est généralement moins cher à l'utilisation (appels téléphoniques) qu'un standard PABX.
- L'IPBX permet une réduction des coûts d'exploitation (maintenance et communications) de 25 à 50 %.

Au-delà de cette différence, les fonctionnalités d'un standard téléphonique IPBX sont généralement les mêmes que pour un standard téléphonique PABX.

Seul le réseau utilisé pour acheminer les données est différent : réseau téléphonique traditionnel pour le PABX et Internet pour l'IPBX.

Voici un tableau vous présentant les principales fonctionnalités pour un standard téléphonique IPBX.

Tableau 1 : Fonctionnalité d'un IPBX

FONCTIONNALITÉS		DESCRIPTION
MESSAGERIE	Vocale	Chaque poste téléphonique a sa propre messagerie vocale et a la possibilité de stocker les messages vocaux. La boîte vocale est consultable en externe (à l'aide de la SDA*).
	Unifiée	Elle joue le même rôle que la messagerie vocale, mais avec des mails. Vos messages vocaux ou fax atterrissent directement dans votre boîte mail de réception ou téléphone portable.
NUMÉROTATION	Numérotation abrégée collective	Possibilité d'appeler en externe (fixe ou mobile) en tapant un préfixe spécifique sur tous les postes raccordés au standard téléphonique. Exemple : le 588 pour contacter la société de maintenance.
	Numérotation abrégée individuelle	Possibilité d'appeler en externe (fixe ou mobile) à l'aide d'un préfixe spécifique par poste. Il s'agit généralement d'une manipulation de l'utilisateur.
	Plan de numérotation	Préfixes à taper pour différentes fonctionnalités voulues avant un appel. Exemple : Le 5, afin de consulter sa messagerie vocale. Le 0, pour les appels vers l'extérieur. Entre le 500 et 999 si vous souhaitez appeler un poste précis dans l'entreprise.
	Plan de suffixe	Préfixes que vous composez pour obtenir différentes fonctionnalités voulues pendant un appel. Exemple : Le 3, une conférence à 3.
IDENTIFICATION DE L'APPELANT (ANI) **		Sur votre ordinateur, les données de la personne appelant apparaissent juste avant son appel grâce à une base de données.
SÉLECTION DIRECTE À L'ARRIVÉE (SDA)		Un appel peut être orienté vers un poste interne sans avoir besoin de passer par l'accueil téléphonique de l'entreprise. Exemple : composer le 588 pour le poste 01.02.03.04.05.
<u>ATTENTE TÉLÉPHONIQUE</u>		La personne qui appelle est mise en attente de façon automatique (messages d'accueil) avant d'entrer en contact avec son correspondant.
LEAST COST ROUTINE (LCR)		Vous gérez dynamiquement différents opérateurs : suivant la destination et l'heure, l'IPBX utilise les liaisons qui coûtent le moins cher.
<u>SERVEUR VOCAL INTERACTIF</u>		La personne qui appelle est dirigée vers une sorte de standard automatique qui lui demande de composer un chiffre ou de parler pour identifier le poste vers lequel il veut être redirigé.
TAXATION (ACCÈS AUX STATISTIQUES)		Analyse de différentes données : Trafic appel entrant/sortant. Facturation par poste.

III.2.4. Les caractéristiques d'un IPBX :

Ces caractéristiques sont :

- L'évolutivité.
- La distribution et la redondance.
- Le support des standards de signalisation VoIP : H.323 et SIP au minimum.
- La disposition d'applications CTI ou la communication avec un serveur CT1.
- Disposer d'API ouvertes dans le cas où il comprendrait des applications CT1.
- Être gérable à travers une interface web.
- intégrer un serveur DHCP ou un proxy SIP pour la configuration automatique de
- terminaux H.323 ou SIP.
- Proposer un mécanisme d'autorisation à accéder à ses services.
- Maintenir un accès de secours sur le RTC.
- Limiter la bande passante et le nombre d'appels simultanés.
- Être inter opérable avec d'autres équipements (Gateway, gatekeepers, ...).
- Proposer un rapport qualité/prix intéressant.

III.3. Les IP CENTREX :

III.3.1. Définition :

On parle d'**IP Centrex** pour désigner la gestion externalisée via internet des lignes téléphoniques de l'entreprise.

Le Centrex est un IPBX hébergé, la plupart du temps par un opérateur de téléphonie fixe. Il permet aux entreprises de se décharger de la gestion et de la maintenance de leur standard téléphonique et offre les mêmes fonctionnalités qu'un PABX traditionnel. Le Centrex facilite le passage aux communications unifiées et permet aux entreprises multi-sites de supprimer les contraintes de distance dans la gestion de leur téléphonie.

Les offres des centres d'externalisation de la téléphonie professionnelle :

- Les mêmes fonctionnalités que les standards PABX ou standard IPBX,
- Une gestion des fonctions du standard déléguée à un prestataire externe et spécialisé,
- Un gain de place avec la suppression physique du standard sur le lieu de l'entreprise,
- Un investissement de départ quasi nul (les prestations sont facturées au mois et selon les fonctionnalités et le nombre de lignes choisies),
- Des frais de consommation réduits,
- Une solution clé en main, le prestataire s'occupe de tout y compris de l'installation du standard téléphonique (câblage, routeur et téléphones).

Conclusion :

La mise en place d'un centre d'appels optimise la productivité de toutes les activités de l'entreprise : en effet, elle permet :

- une amélioration de la qualité du service rendu aux clients grâce à une personnalisation de la relation avec eux
- Une satisfaction accrue des clients suite à un meilleur suivi de leurs comportements ;
- Une meilleure productivité des agents grâce au CTI et à la base données clients.
- Une réduction du coût des différentes prestations.
- Une augmentation du chiffre d'affaires de l'entreprise.
- Une valorisation de l'image de l'entreprise.
- Une meilleure connaissance du marché grâce aux fichiers clients.

Cependant, pour la conception d'un call center performant et moderne , une étude approfondie de tous les paramètres est indispensable a travers le recrutement de cadres compétents , la mise a niveau de toute l'infrastructure pour la migration vers les technologies de téléphonie IP.

CHAPITRE II :

Optimisation de la téléphonie par VOIP

CHAPITRE II : Optimisation de la téléphonie par la VOIP

Introduction:

La téléphonie sur IP est une technologie de communication vocale en pleine émergence. Elle fait partie d'un tournant dans le monde de la communication. En effet, la convergence du triple play (voix, données et vidéo) fait partie des enjeux principaux des acteurs de la télécommunication d'aujourd'hui.

La ToIP représente actuellement une véritable opportunité économiques pour les centres d'appels, telles que la diminution du coût en infrastructure, de la facture de téléphone ainsi que l'intégration de nombreux services.

La téléphonie sur IP est basée sur des standards ouverts : elle permet donc l'interaction avec les équipements téléphoniques standards. Toutefois, les aspects techniques sous-jacents à cette nouvelle technologie ne sont pas toujours bien maîtrisés. Les problèmes dus au NAT, les pare-feux, la sécurité ,sont des problèmes qui restent encore à dominer.

Ce chapitre est consacré à l'étude des protocoles associés à la téléphonie sur IP . On commence tout d'abord par présenter les principaux protocoles de signalisation et de transport de la ToIP et le protocole ENUM dont l'usage est encore incertain au sein des opérateurs de ToIP. Je traite ensuite les problèmes posés par les NAT et les pare-feux dans une architecture de ToIP et les exemples de solutions pour résoudre ces derniers. On présentera ensuite les vulnérabilités spécifiques à la ToIP et les mécanismes de sécurité. Et enfin nous terminerons en présentant l'état de l'art du déploiement du protocole IPv6 dans la ToIP.

Partie I : La VOIP

I.1. Qu'est-ce que la VoIP:

VoIP signifie Voice over Internet Protocol ou Voix sur IP (Protocole Internet). Comme son nom l'indique, la VoIP essaie de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur Internet. La VoIP peut utiliser du matériel d'accélération pour réaliser ce but et peut aussi être utilisée en environnement de PC.

Cette technologie est notamment utilisée pour supporter le service de téléphonie IP (« ToIP » pour Telephony over Internet Protocol) .La voix sur IP comprend ainsi les communications de PC à PC. Pour ce type de communication, chaque utilisateur doit disposer d'un logiciel approprié. Si la connexion passe par le réseau Internet, on parle alors de la téléphonie par internet. Deuxième catégorie de voix sur IP, les communications de PC à téléphonie (PC to Phone). Dans les deux cas, le PC communicant est appelé soft phone, terme qui insiste sur l'émulation du PC en téléphone grâce à un logiciel.

I.2. fonctionnement de la VoIP :

Le principe consiste à encapsuler un signal audio numérisé (en général, la voix) dans le protocole IP (Internet Protocol). La principale application est la téléphonie internet

(téléphonie IP). La Technique VoIP permet de construire un réseau téléphonique basé sur une plate-forme usuelle comme Windows ou Linux, et d'utiliser le réseau informatique classique (LAN/WAN+IP) avec des téléphones possédant une interface Ethernet. Le succès de la téléphonie sur IP repose en partie sur les coûts réduits des appels téléphoniques via le réseau Internet

I.3. Architecture d'une infrastructure VOIP:

I.3.1 Architecture hybride

Consiste à retenir une architecture hybride (circuit/voix sur IP). Cette solution présente l'avantage de ne pas remettre en cause l'infrastructure existante (terminaux et réseau téléphonique interne équipement PABX) tout en bénéficiant des avantages du transport de la voix sur IP pour les communications inter sites. La mise en œuvre d'une solution de voix sur IP peut se faire :

- Par l'ajout d'une carte IP sur un PABX si celui-ci est évolutif en IP
- Soit, par l'ajout d'un Gateway externe au PABX
- Soit, par un recours aux fonctionnalités de Gateway intégrées aux routeurs de génération.

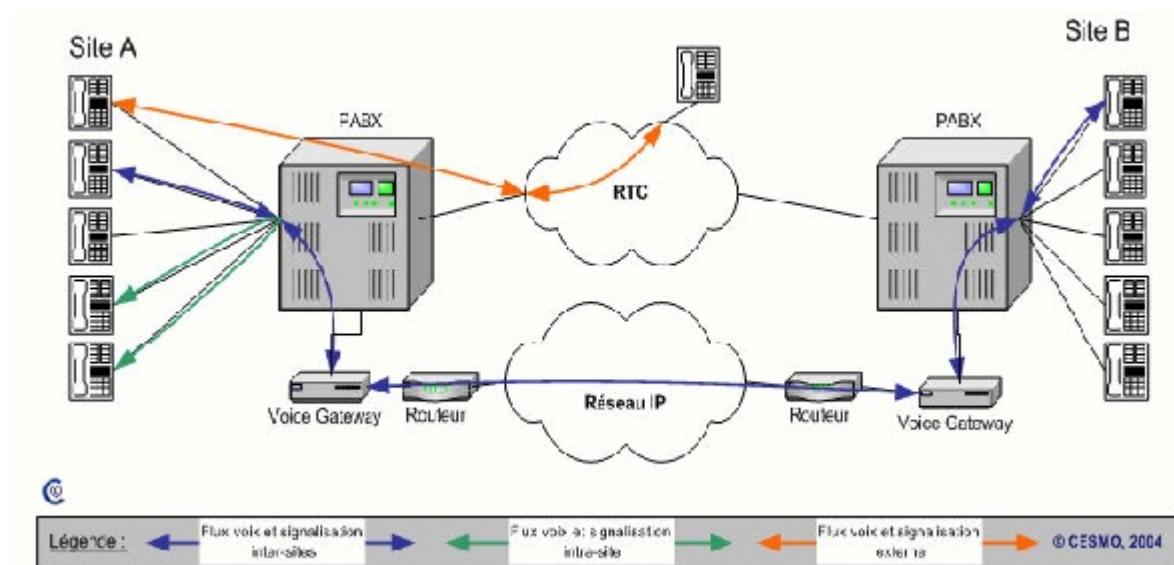


Figure5: Architecture Hybride

I.3.2. Architecture Full IP

Permet une migration complète de la téléphonie de l'entreprise sur IP, incluant les terminaux téléphoniques. Plus lourde qu'une solution hybride, une telle migration s'accompagne aussi de nombreux bénéfices en posant les bases de la convergence entre le système d'information et la téléphonie de l'entreprise.

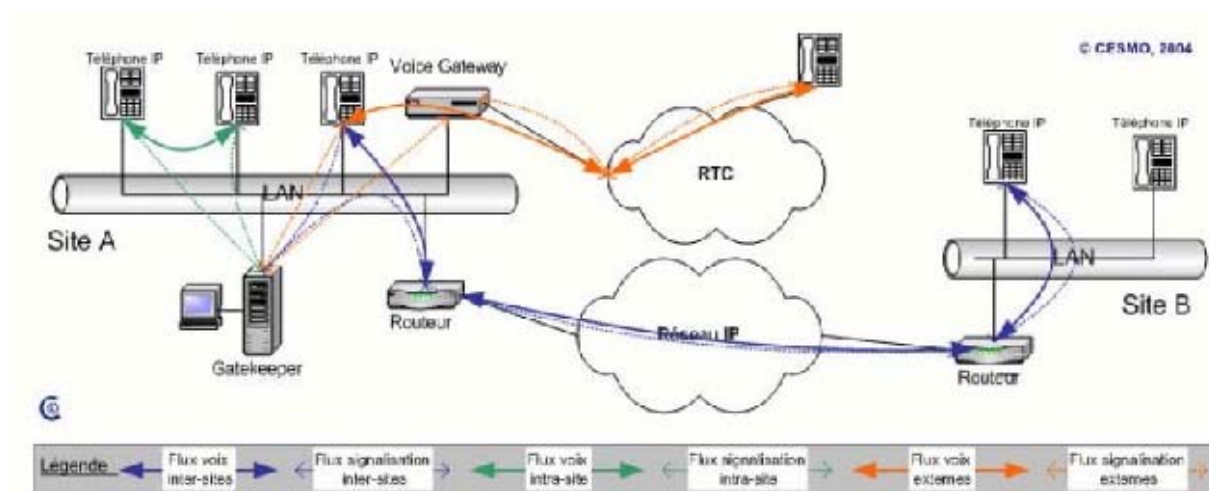


Figure 6: Architecture Full IP

I.3.3. Architecture de téléphonie sur IP de type Centrex :

Ici, il s'agit pour le call center de déporter le gatekeeper et la Voice Gateway sur le site du fournisseur de service. Il revient donc à déporter l'intelligence dans le cœur de réseau et le transit systématique de tous les flux voix par le site du fournisseur n'est donc plus nécessaire.

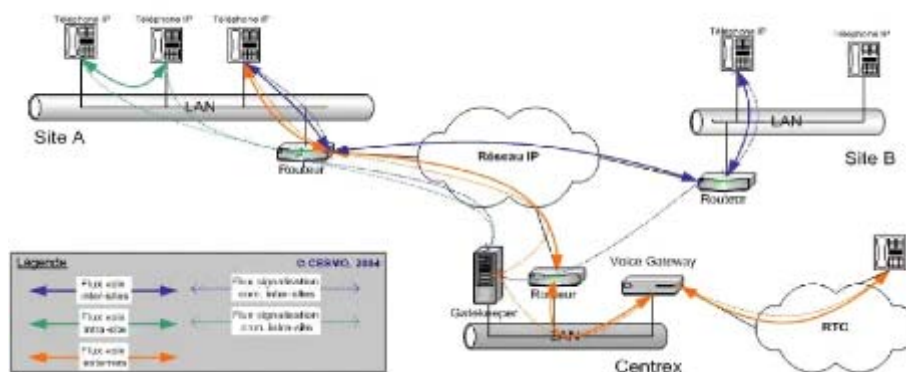


Figure 7 : Architecture de téléphonie sur IP de type Centrex

Partie II :Téléphonie sur IP

II.1. DEFINITION :

La téléphonie sur IP repose totalement sur un transport VoIP. La mise en œuvre de la VoIP offre là une première brique de migration vers la téléphonie sur IP.

La téléphonie sur IP (en anglais, telephony over IP ou IP telephony) est un mode de téléphonie dans lequel la voix est numérisée puis acheminée par le protocole TCP/IP sous

forme de paquet de données .Ce service de téléphonie est offert sur un réseau de télécommunications, public ou privé utilisant principalement le protocole IP.

En fait, la téléphonie sur IP utilise la même méthode (processus) que pour la transmission de l'information sur le réseau Internet. C'est-à-dire une fois la voix formatée, on peut la transmettre sur un lien Internet commun ou encore l'envoyer sur des liens dédiés.

La Téléphonie sur IP s'appuie sur des protocoles aptes au transport de la voix et des données, elle permet une infrastructure voix/données convergente

II.2. Schémas de principe :

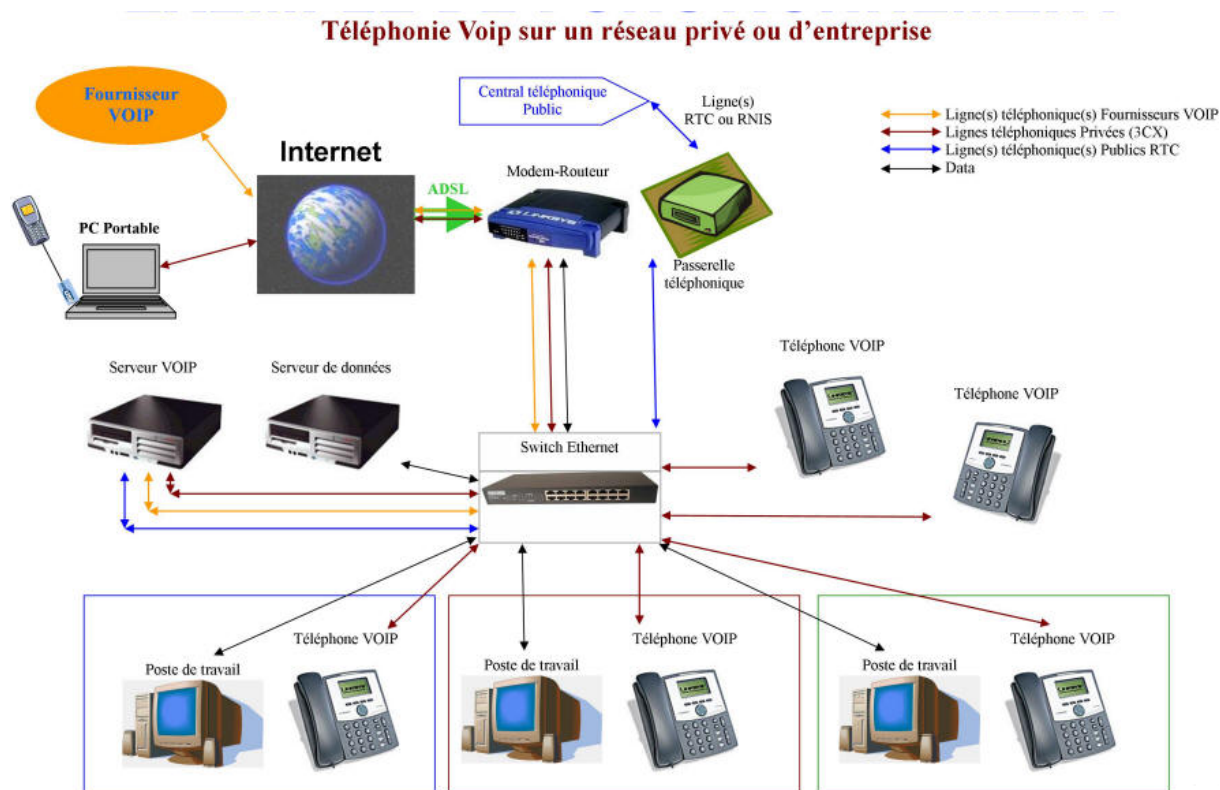


Figure 8 : Téléphonie VOIP sur un réseau privé

II.3. Fonctionnalités de la téléphonie sur IP :

- Un système de Téléphonie sur IP présente toutes les fonctionnalités proposées par les systèmes de téléphonie traditionnels, tout en offrant principalement en plus :

Une infrastructure convergente les mêmes câblages VDI, équipements actifs, liens opérateurs ou liens propriétaires IP, sont employés pour véhiculer voix et données.

- Aucune contrainte de localisation des utilisateurs pour l'exploitation du système de téléphonie sur IP.

- Une capacité d'intégration de tout type de liaisons IP WAN et de liaisons traditionnelles de télécommunications, RTC, RNIS, MIC T2...
- Une capacité d'intégration des anciens terminaux analogiques tels que : poste téléphonique analogique, modem, fax, minitel .
- Un déploiement et une administration simplifiés.
- Une messagerie unifiée (Voice/E-mail avec fonction Text to Speech), sur les systèmes de téléphonie IP les plus sophistiqués.

II.4. Intérêts de la TOIP:

- Les principaux intérêts de la Téléphonie sur IP :

Des économies d'installation et d'exploitation :

" Moins de câblage à installer, puisque le même câble est utilisé pour acheminer au poste de travail, les accès aux systèmes de téléphonie et d'informations (pour certains systèmes)

" Une seule infrastructure active à maintenir

" Réduction des coûts globaux de location des liaisons opérateur, du fait de la mutualisation de leur exploitation pour la transmission de la voix et des données

" Disparition des coûts de communication entre les sites et entre les utilisateurs et les sites, (interconnectés par des liaisons propriétaires IP ou des VPN IP)

Plus de contrainte de localisation des utilisateurs pour exploiter le système

Adaptable à tous les média physiques, Paires Torsadées, Fibres Optiques, WiFi et CPL

Une adaptabilité totale d'intégration des liaisons de communications TDM et IP

Une aisance de déploiement et d'administration inconnue des systèmes TDM

II.5. Les différents éléments pouvant composés un réseau de téléphonie sur IP

II.5.1. L'IPBX ou PABX - IP :

C'est un autocommutateur compatible avec la téléphonie sur IP. Il permet comme un commutateur téléphonique standard, d'établir une communication téléphonique entre deux abonnés distants c'est lui qui assure la commutation des appels et leurs autorisations, Il peut s'interconnecter avec d'autres PABX-IP ou PABX non IP de la même marque (réseau homogène) ou d'autres PABX d'autres marques (réseau hétérogène).

A l'intérieur d'une entreprise, l'IPBX définit le routage des paquets pour que la communication parvienne au bon poste de l'entreprise. Un PABX-IP peut être soit un autocommutateur auquel l'entreprise ajoute une carte d'extension IP, soit une machine nativement IP. Un autocommutateur IP qui sert de serveur de messagerie, capable de

stocker l'historique des communications ou éventuellement des messages. IPBX c'est la dernière génération de PABX, il s'intègre à la téléphonie sur IP.

II.5.2. Les Passerelles IP/RJ11 :

Les passerelles IP servent de liens entre les réseaux téléphoniques commutés (RTC) et les réseaux IP. Passerelle de voix sur IP est spécifiquement conçue pour permettre aux messages vocaux provenant d'un réseau téléphonique traditionnel d'être transmis sur un réseau utilisant le protocole IP, tout en leur offrant la possibilité d'effectuer le chemin inverse. Ce sont des boîtiers disposés à proximité des terminaux de téléphonie standard, permettant leur intégration au LAN Ethernet

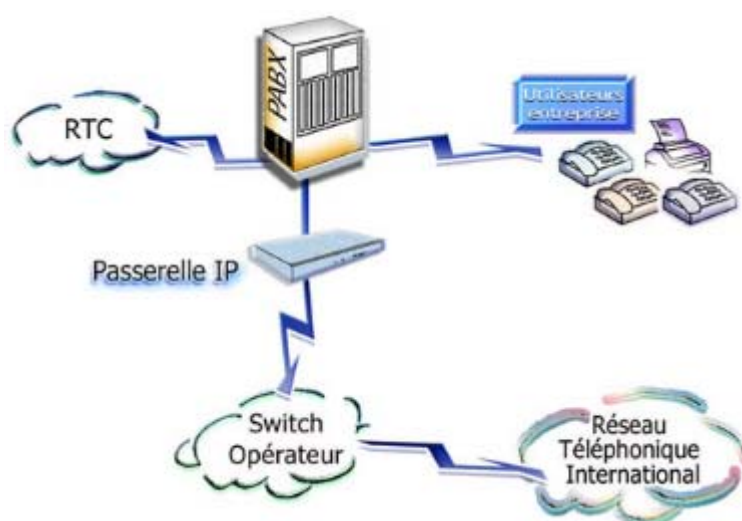


Figure 9 : Architecture d'un Passerelle IP

II.5.3. Le serveur de TOIP (exemple : Call Manager de Cisco):

il gère et traite les autorisations d'appels entre les terminaux IP ou soft phones et les différentes signalisations du réseau.

Il peut posséder des interfaces réseaux opérateurs (RTC-PSTN ou RNIS), sinon les appels externes passeront par la passerelle dédiée à cela (Gateway).

Il en existe différents modèles capables de gérer d'une vingtaine à plusieurs milliers d'utilisateurs. Suivant la capacité du système la fonction de gestion d'appels est intégrée dans un boîtier tout en un ou dans un serveur indépendant ou encore dans un routeur. Plusieurs serveurs peuvent être intégrés à un même système de téléphonie sur IP pour :

- Augmenter sa capacité de gestion et de traitement d'appels, sans limitation en nombre
- Assurer sa redondance avec ou sans partage de charge

II.5.4. Le Routeur Voix/Données :

il assure la commutation des paquets d'un réseau vers un autre réseau. Intégré dans un équipement multifonction ou en stand alone, il assure le rattachement au LAN, des liens IP et des liaisons opérateurs de type RTC, RNIS, T2, . C'est un élément important dont le dimensionnement en termes de capacité d'accueil d'interface et de routage constitue une des clés de la bonne intégration d'un système de téléphonie sur IP. Cet équipement doit supporter les VPN, les VLAN et les fonctions de QoS, pour permettre l'intégration d'un système de téléphonie sur IP

II.5.5. Le Switch:

il assure la distribution et commutation de dizaines de port Ethernet à 10/100 voire 1000 Mbits/s. Suivant les modèles, il peut intégrer la télé alimentation des ports Ethernet à la norme 802.3af pour l'alimentation des IP-phones ou des bornes WIFI en 48V.

II.5.6. Le Gatekeeper:

il effectue les translations d'adresses (identifiant H323 et @ IP du référencement du terminal) et gère la bande passante et les droits d'accès. C'est le point de passage obligé pour tous les équipements de sa zone d'action.

II.5.7. L'IP-PHONE:

c'est un terminal téléphonique fonctionnant sur le réseau LAN IP à 10/100 avec une norme soit propriétaire, soit SIP, soit H.323. Il peut y avoir plusieurs codecs pour l'audio, et il peut disposer d'un écran monochrome ou couleur, et d'une ou plusieurs touches soit programmables, soit préprogrammées. IL est en général doté d'un hub passif à un seul port pour pouvoir alimenter le PC de l'utilisateur (l'IP-PHONE se raccorde sur la seule prise Ethernet mural et le PC se raccorde derrière l'IP-PHONE).

II.5.8. Les Softphones:

Ce sont des logiciels intégrés aux PC des utilisateurs, qui assure toutes les fonctions téléphoniques et qui utilise la carte son et le micro du PC de l'utilisateur, et aussi la carte Ethernet du PC. Il est géré soit par le Call Manager, soit par le PABX-IP.

II.5.9. Le Serveur de Messagerie :

Cet équipement gère les messageries vocales du système de téléphonie sur IP, certains serveurs gèrent également les e-mails unifiée avec les messages vocaux, en retranscrivant sous forme de voicemail, les e-mails consultés par téléphone et sous forme d'e-mail les messages vocaux, lorsque l'utilisateur accède à sa messagerie à partir de son PC. Suivant les modèles la fonction de gestion des messageries est intégrée dans un boîtier tout en un ou dans un serveur indépendant.

II.5.10. Les Autres Equipements :

Ils existent de nombreux autres équipements et logiciels pouvant être intégrés à un système de téléphonie sur IP parmi lesquels nous pouvons citer, les postes IP d'audioconférence, les logiciels d'assistance personnel, de call-center avec ou sans passerelle web, de gestion d'e-mails, d'appels d'urgence.

II.6. Fonctionnement de la téléphonie sur IP :

II.6.1. Principe

Le principe de la téléphonie sur IP est la numérisation de la voix, c'est-à-dire le passage d'un signal analogique à un signal numérique. Celui-ci est compressé en fonction des codecs choisis, cette compression a comme but de réduire la quantité d'information qui est transmise sur le réseau. Le signal obtenu est découpé en paquets, à chaque paquet on ajoute les entêtes propres au réseau (IP, UDP, RTP....) et pour finir il est envoyé sur le réseau.

A l'arrivée, les paquets transmis sont réassemblés en supprimant d'abord les entêtes. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique afin que l'utilisateur puisse écouter le message d'origine.

II.6.2. Architecture de transmission VOIP

La technologie de la voix sur IP (VoIP pour Voice over IP) nous présente une architecture découpée en 8 grandes étapes :

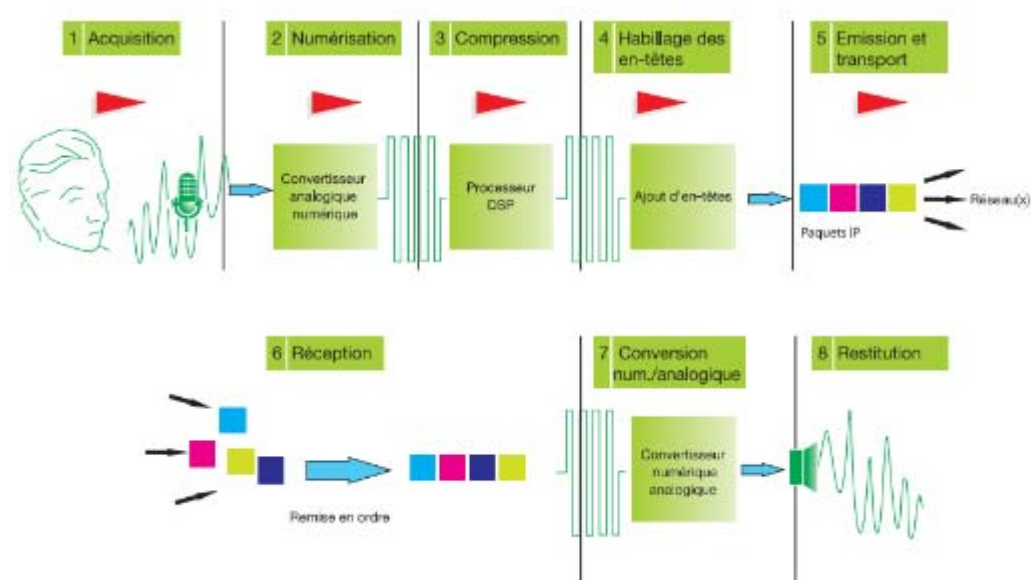


Figure 10 : 8 étapes de la voix à IP

a) Acquisition du signal

La VoIP suppose la transformation d'un signal continu analogique (la voix) en un signal discret numérique (composé d'une série de chiffres). La première étape consiste naturellement à capter la voix à l'aide d'un micro, qu'il s'agisse de celui d'un téléphone ou d'un micro casque.

b) Numérisation

La voix passe alors dans un convertisseur analogique numérique qui réalise deux tâches distinctes :

- l'échantillonnage du signal sonore, c'est-à-dire un prélèvement périodique de ce signal .
- la quantification, qui consiste à affecter une valeur numérique à chaque échantillon. Plus les échantillons sont codés sur un nombre de bits important, meilleure sera la qualité (on parle de «résolution») de la conversion. Généralement, la voix est échantillonnée à 8 kHz et chaque échantillon est codé sur 8 bits, ce qui donne un débit de 64 kbit/s (norme G711).

c) Compression

Le signal une fois numérisé peut être traité par un DSP (Digital Signal Processor) qui va le compresser, c'est-à-dire réduire la quantité d'informations (bits) nécessaire pour l'exprimer. Plusieurs normes de compression et décompression (Codecs) sont utilisées pour la voix. L'avantage de la compression est de réduire la bande passante nécessaire pour transmettre le signal.

d) Habillage des en-têtes

Les données «brutes» qui sortent du DSP doivent encore être enrichies en informations avant d'être converties en paquets de données à expédier sur le réseau. Trois «couches» superposées sont utilisées pour cet habillage :

***La couche IP**

La couche IP correspond à l'assemblage des données en paquets. Chaque paquet commence par un en-tête indiquant le type de trafic concerné, ici du trafic UDP.

***La couche UDP**

La deuxième couche, UDP, consiste à formater très simplement les paquets. Si l'on restait à ce stade, leur transmission serait non fiable : UDP ne garantit ni le bon acheminement des paquets, ni leur ordre d'arrivée.

***La couche RTP (Real Time Protocol) / RTCP (Real Time Control Protocol)**

Pour palier l'absence de fiabilité d'UDP, un formatage RTP est appliqué de surcroît aux paquets. Il consiste à ajouter des entêtes d'horodatage et de synchronisation pour s'assurer du réassemblage des paquets dans le bon ordre à la réception. RTP est souvent renforcé par RTCP qui comporte, en plus, des informations sur la qualité de la transmission et l'identité des participants à la conversation.

e) Emission et transport

Les paquets sont acheminés depuis le point d'émission pour atteindre le point de réception sans qu'un chemin précis soit réservé pour leur transport. Ils vont transiter sur le réseau (réseau local, réseau étendu voire Internet) en fonction des ressources disponibles et arriver à destination dans un ordre indéterminé.

f) Réception

Lorsque les paquets arrivent à destination, il est essentiel de les replacer dans le bon ordre et assez rapidement. Faute de quoi une dégradation de la voix se fera sentir. Ce point sera détaillé plus loin.

g) Conversion numérique analogique

La conversion numérique analogique est l'étape réciproque de l'étape 2, qui permet de transformer les données reçues sous forme de série discrète en un signal électrique «continu».

h) Restitution

Dès lors, la voix peut être retranscrite par le haut-parleur du casque, du combiné téléphonique ou de l'ordinateur.

II.7.Mode d'accès et architecture:

Selon le type de terminal utilisé (un ordinateur ou un téléphone classique), on distingue trois modes d'accès possibles de voix sur IP :

- La voix sur IP entre deux ordinateurs
- La voix sur IP entre un ordinateur et un téléphone
- La voix sur IP entre deux téléphones

les utilisateurs doivent être dans le même réseau IP (Internet ou Intranet de l'entreprise).

II.7.1. La voix sur IP entre deux ordinateurs :

C'est le cas le plus simple. Il suffit de disposer d'une carte son, de haut-parleurs et de microphones pour chacun des interlocuteurs. Il faut également connaître l'adresse IP de chacun des terminaux pour établir la communication.

Dans ce premier type de voix sur IP, les utilisateurs communiquent à partir d'un logiciel de voix sur IP qu'on appelle soft phone.

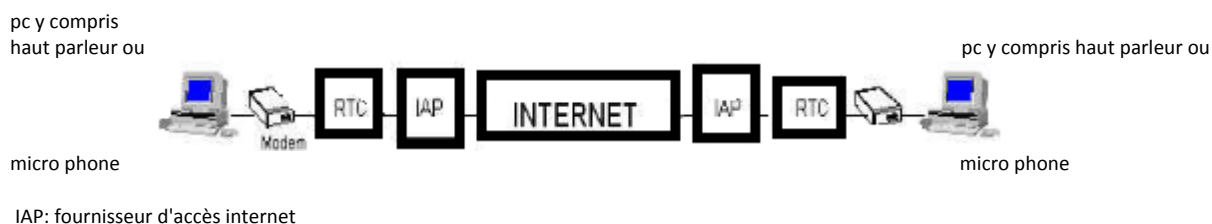


Figure 11 : Voix sur IP entre deux ordinateurs

II.7.2 la voix sur IP entre un PC et un téléphone :

Ce cas nécessite une conversion des signaux entre le RTC et le réseau IP. En effet, ces deux terminaux utilisant des technologies différentes (la commutation de circuits et la commutation de paquets), l'échange des informations nécessite une passerelle. L'utilisateur possédant un ordinateur et désirant appeler l'autre sur son téléphone doit se connecter à un service spécial sur Internet, offert par un fournisseur de service (un ISP) ou par son fournisseur d'accès à Internet (son IAP).

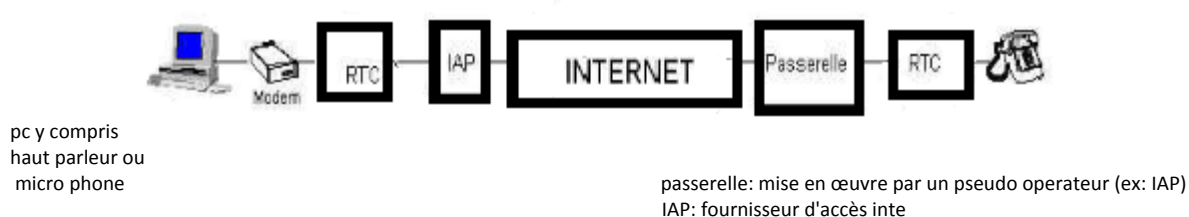


Figure 12 : Voix sur IP entre PC et un téléphone

II.7.3 La voix sur IP entre deux téléphones

C'est le cas le plus complexe car il nécessite deux conversions de signaux. On utilise des passerelles analogues entre le réseau téléphonique et le réseau. Un utilisateur appelle le numéro d'une passerelle et lui communique le numéro du correspondant qu'il cherche à joindre.



Figure 13 : Voix sur IP entre deux téléphones

II.8. Signalisation et transport :

La Téléphonie sur IP s'appuie sur deux protocoles différents :

1) la signalisation:

La Norme H323:

S'inspire de la commutation par paquets, c'est le standard intégré par tous les systèmes de téléphonie sur IP actuels. Elle définit les codecs suivants :

" **G711** : Codec PCM (Pulse Code Modulation), bien adapté aux réseaux locaux ou étendus à large bande, il permet d'encoder en 64 Kbps et de restituer une très bonne qualité de la voix, au détriment d'une bande passante élevée pour Internet.

" **G723.1** : Il encode et compresse le signal vocal avec un taux de compression élevés en 5,3 ou 6,4 Kbps, pour une restitution médiocre, bien qu'intelligible. Ce codec est à privilégier lorsque la bande passante disponible est limitée.

" **G729a** : Bien adapté aux postes de travail déportés utilisant l'Internet comme moyen de transport, ce codec encode et compresse le signal vocal avec un taux de compression moyen en 8 et 13 Kbps, pour une restitution de qualité acceptable.

Le Protocole SIP Session Initiation Protocol, contrairement à H323 ce protocole est inspiré de l'adressage informatique. SIP est destiné à remplacer H323.

2) le transport:

Afin d'acheminer les datagrammes voix sans délai vers leur destinataire, l'environnement H323 s'appuie sur deux protocoles de transport :

RTP Real Time Protocol:

ce protocole comporte un en-tête permettant la réservation de la bande passante du transport, mais n'intègre pas de dispositif de contrôle d'intégrité des données.

RTCP Real Time Control Protocol:

à l'instar de RTP ce protocole possède un en-tête pour la réservation de la bande passante, il intègre en plus des dispositifs de contrôle, notamment de détection de pertes de trames.

La téléphonie sur IP repose totalement sur un transport VoIP. La mise en œuvre de la VoIP offre là une première brique de migration vers la téléphonie sur IP.

Partie v : Les problèmes clés de la téléphonie sur IP :

V.1. La QoS :

La téléphonie est un service vital pour l'entreprise, les questions de qualité de service QoS « quality of service » sont donc particulièrement importantes.

La QoS a pour vocation d'assurer la disponibilité de la téléphonie en tout temps et d'assurer une transmission des conversations dans de bonnes conditions. La qualité du transport de la voix est affectée par les paramètres suivants :

- La qualité du codage
- Le délai d'acheminement (delay)
- La gigue (jitter)
- La perte de paquets (packet loss)
- L'écho

Toutes ces contraintes déterminent la QoS (Quality of Service ou Qualité de service). Le transport de la voix sur IP implique l'utilisation de nombreux protocoles : RTP, RTCP, H245, H225,...

V.1.1. Qualité du codage :

Généralement, plus le taux de compression est élevé par rapport à la référence de 64 Kb/s (G711), moins la qualité de la voix est bonne. Toutefois, les algorithmes de compression récents permettent d'obtenir des taux de compression élevés, tout en maintenant une qualité de la voix acceptable.

L'acceptabilité par l'oreille humaine des différents algorithmes est définie selon le critère MOS (Mean Operational Score), défini par l'organisme de normalisation internationale ITU (International Télécommunication Union / Union internationale des Télécommunications). Dans la pratique, les deux algorithmes les plus utilisés sont le G.729 et le G.723.1.

Le tableau ci-après montre une liste de codecs avec leur débit correspondant :

Nom du codec	Débit
G.711	64kbps
G.726	32kbps
G.726	24kbps
G.728	16kbps
G.729	8kbps
G.723.1	MPMLQ 6.3 kbps
G.723.1	ACELP 5.3k kbps

Tableau 2 : Correspondance entre les débits et les codecs

V.1.2. Délai d'acheminement : latence (Delay)

Selon la norme ITU G114, le délai d'acheminement permet :

- Entre 0 et 150 ms, une conversation normale
- Entre 150 et 300 ms, une conversation de qualité acceptable
- Entre 300 et 700 ms, uniquement une diffusion de voix en half duplex (mode talkie-walkie)
- Au-delà, la communication n'est plus possible

Précisons que le budget temps (latence) est une combinaison du délai dû au réseau et du délai lié au traitement de la voix par le codec (algorithmes de compression/décompression de la voix). Dans la pratique, si l'on enlève le temps dû aux algorithmes de compression, il est impératif que le réseau achemine la voix dans un délai de 100 à 200 ms. Or, la durée de traversée d'un réseau IP est dépendante du nombre de routeurs traversés ; le temps de traversée d'un routeur étant lui-même fonction de la charge de ce dernier qui fonctionne par file d'attente.

V.1.3. Gigue (Jitter) :

La gigue (variation des délais d'acheminement des paquets voix) est générée par la variation de charge du réseau (variation de l'encombrement des lignes ou des équipements réseau) et donc à la variation de routes dans le réseau. Chaque paquet est en effet susceptible de transiter par des combinaisons différentes de routeurs entre la source et la destination. Pour compenser la gigue, on peut utiliser des buffers (mémoire tampon) côté récepteur, afin de reconstituer un train continu et régulier de paquets voix.

Toutefois, cette technique a l'inconvénient de rallonger le délai d'acheminement des paquets. Il est donc préférable de disposer d'un réseau à gigue limitée.

V.1.4. Perte de paquets (packet loss) :

Lorsque les routeurs IP sont congestionnés, ils libèrent automatiquement de la bande passante en se débarrassant d'une certaine proportion des paquets entrants en fonction de seuils prédéfinis.

La perte de paquets est préjudiciable, car il est impossible de réémettre un paquet voix perdu, compte tenu du temps dont on dispose. Le moyen le plus efficace de lutter contre la perte d'informations consiste à transmettre des informations redondantes (code correcteur d'erreurs), qui vont permettre de reconstituer l'information perdue. Des codes correcteurs d'erreurs, comme le Reed Solomon, permettent de fonctionner sur des lignes présentant un taux d'erreur de l'ordre de 15 ou 20 %. Une fois de plus, ces codes correcteurs d'erreurs présentent l'inconvénient d'introduire une latence supplémentaire.

Certains, très sophistiqués, ont une latence très faible.

V.1.5. l'Écho :

L'écho est un phénomène lié principalement à des ruptures d'impédance lors du passage de 2 fils à 4 fils. Le phénomène d'écho est particulièrement sensible à un délai d'acheminement

supérieur à 50 ms. Il est donc nécessaire d'incorporer un équipement ou logiciel qui permet d'annuler l'écho.

VI. 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 coûteux 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 multiprotocoles 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 efficacité 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.

Partie III :

III.1. Protocoles liés à la ToIP

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.

Afin de rendre possibles les communications ToIP, les solutions proposées dopent la couche IP par des mécanismes supplémentaires nécessaires pour apporter la QOS nécessaire au flux voix de types temps réel, en plus de l'intelligence nécessaire à l'exécution de services.

A cet effet, il existe deux types de protocoles principaux utilisés dans la ToIP :

- ☐ Protocoles de signalisation
- ☐ Protocoles de transport

1.1. Signalisation

La signalisation correspond à la gestion des sessions de communication (ouverture, fermeture, etc.). Le protocole de signalisation permet de véhiculer un certain nombre d'informations notamment:

- ☐ Le type de demande (enregistrement d'un utilisateur, invitation à une session

multimédia, annulation d'un appel, réponse à une requête, etc.).

- ☐ Le destinataire d'un appel.
- ☐ L'émetteur.
- ☐ Le chemin suivi par le message.

Plusieurs normes et protocoles ont été développés pour la signalisation ToIP, quelques uns sont propriétaires et d'autres sont des standards. Ainsi, les principales propositions disponibles pour l'établissement de connexions en ToIP sont :

- SIP (Session Initiation Protocol) qui est un standard IETF (Internet Engineering Task Force) décrit dans le RFC 3261.
- H323 englobe un ensemble de protocoles de communication développés par l'UIT-T (Union Internationale des Télécommunications – secteur de la normalisation des Télécommunications).
- MGCP (Media Gateway Control Protocol) standardisé par l'IETF (RFC 3435).
- SCCP (Skinny Client Control Protocol) est un protocole propriétaire CISCO.

A. Protocole H323

A.1. Introduction

Avec le développement du multimédia sur les réseaux, il est devenu nécessaire de créer des protocoles qui supportent ces nouvelles fonctionnalités, telle que la visioconférence : l'envoi de son et de vidéo avec un souci de données temps réel. Le protocole H.323 est l'un d'eux.

H.323 est un protocole de communications englobant un ensemble de normes utilisées pour l'envoi de données audio et vidéo sur Internet. Il existe depuis 1996 et a été initié par l'ITU (International Communication Union), un groupe international de téléphonie qui développe des standards de communication.

A.2. Fonctionnement

Le protocole H.323 est utilisé pour l'interactivité en temps réel, notamment la visioconférence (signalisation, enregistrement, contrôle d'admission, transport et encodage). C'est le leader du marché pour la téléphonie IP. Il s'inspire du protocole H.320 qui proposait une solution pour la visioconférence sur un réseau numérique à intégration de service (RNIS ou ISDN en anglais), comme par exemple le service Numéris proposé par France Telecom. Le protocole H.323 est une adaptation de H.320 pour les réseaux IP. A l'heure actuelle, la visioconférence sur liaison RNIS est toujours la technique la plus déployée. Elle existe depuis 1990. Les réseaux utilisés sont à commutation de circuits. Ils permettent ainsi de garantir une Qualité de Service (QoS) aux utilisateurs (pas de risque de coupure du son ou de l'image). Aujourd'hui, c'est encore un avantage indiscutable. Par contre, comme pour le téléphone, la facturation est fonction du débit utilisé, du temps de communication et de la distance entre les appels.

A.3. composants de H323 : Il y a 4 composants dans un réseau complètement implémenté en H.323. Ces composants sont reliés à un cinquième, le réseau lui-même. La conception du réseau est laissée pour être définie par ceux qui réalisent l'implémentation. H.323 ne fournit aucune qualité de service (QOS) sur le réseau.

Composants H.323

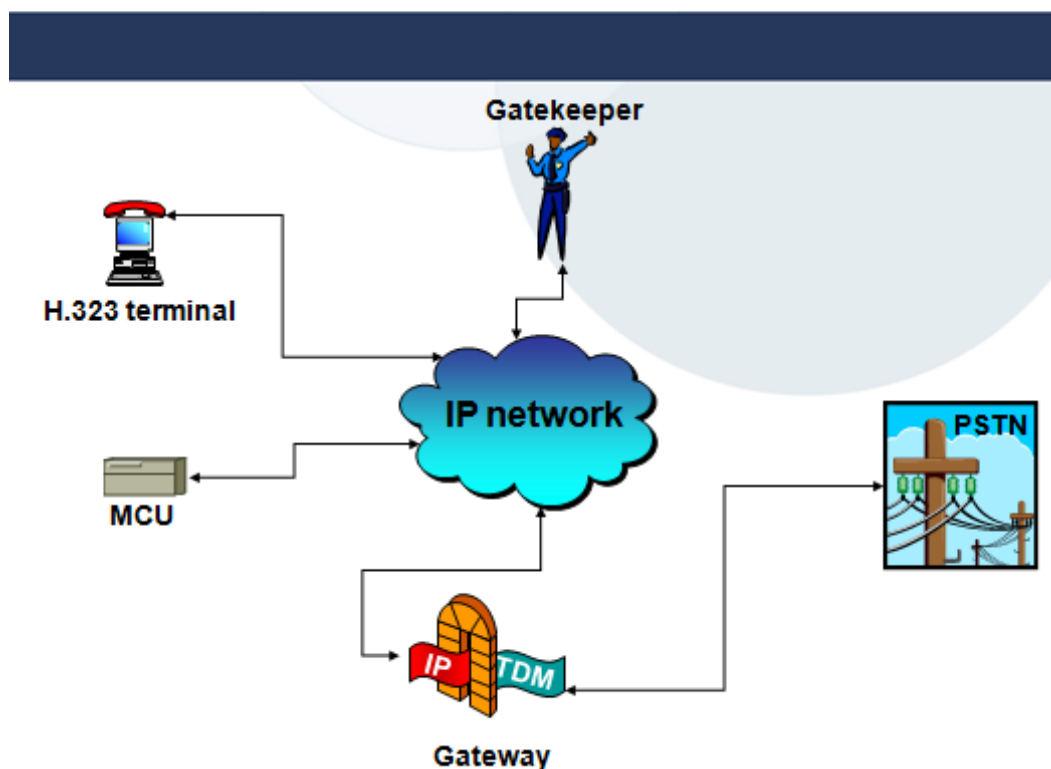


Figure 14 : Composants H323

A.3.1. Terminaux H323:

Les spécificités des terminaux sont présentées dans la figure ci-dessous. Notez que les codecs audio et vidéo s'interfaçent avec une section de retard de chemin de réception pour fournir les moyens de gérer la synchronisation. Le terminal est nécessaire pour transmettre les données de façon régulière mais il n'est pas là pour compenser la latence du réseau derrière l'utilisation au-delà du petit régulateur de jigue. Un régulateur de jigue assure que les paquets sont envoyés à une vitesse régulière même s'ils sont reçus irrégulièrement.

Au travers de cette méthode de modulation, une large latitude est donnée aux concepteurs d'équipements terminaux sous la spécification H 323.

Terminaux H.323

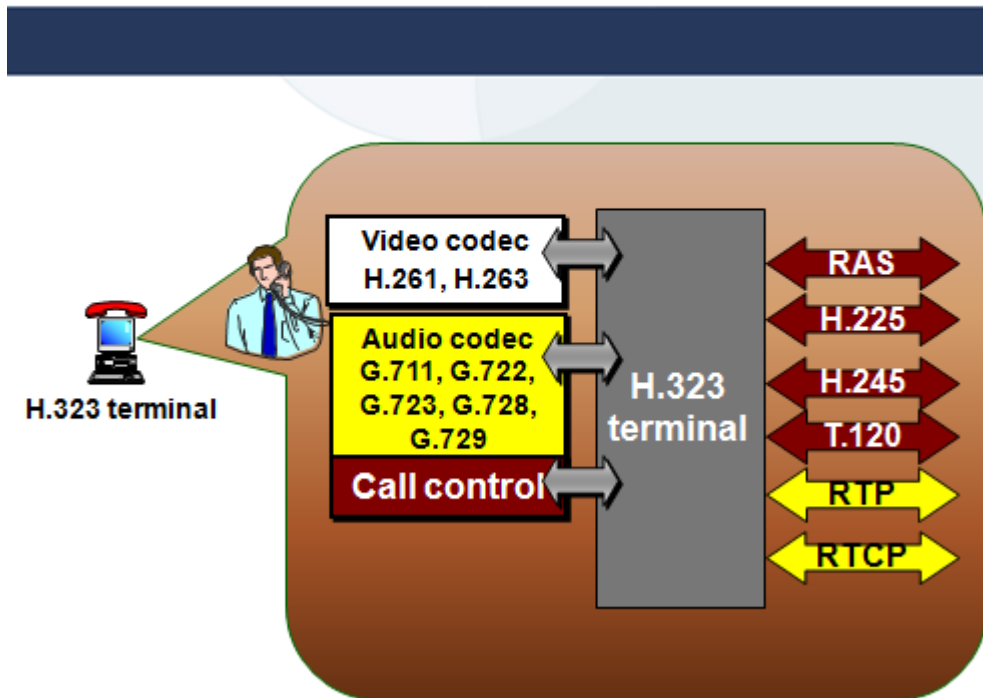


Figure 15 : Terminaux H 323

A.3.2. Passerelles H323:

- fait le pont entre le réseau téléphonique classique et le réseau téléphonique IP ,
- fournit beaucoup de services, et en particulier des fonctions de traduction entre des terminaux H323 et d'autres types de terminaux:
 - ___ la traduction entre les formats de transmissions (i.e H.221 à H.225.0)
 - ___ entre des procédures de communication (i.e.H 242 à H .245)
 - ___ entre les différents codecs audio et vidéo (G .72x et H .26x)
 - ___ enfin ,elle gère l'établissement et la fermeture des communications entre le réseau local et le réseau commuté.

Passerelles H.323

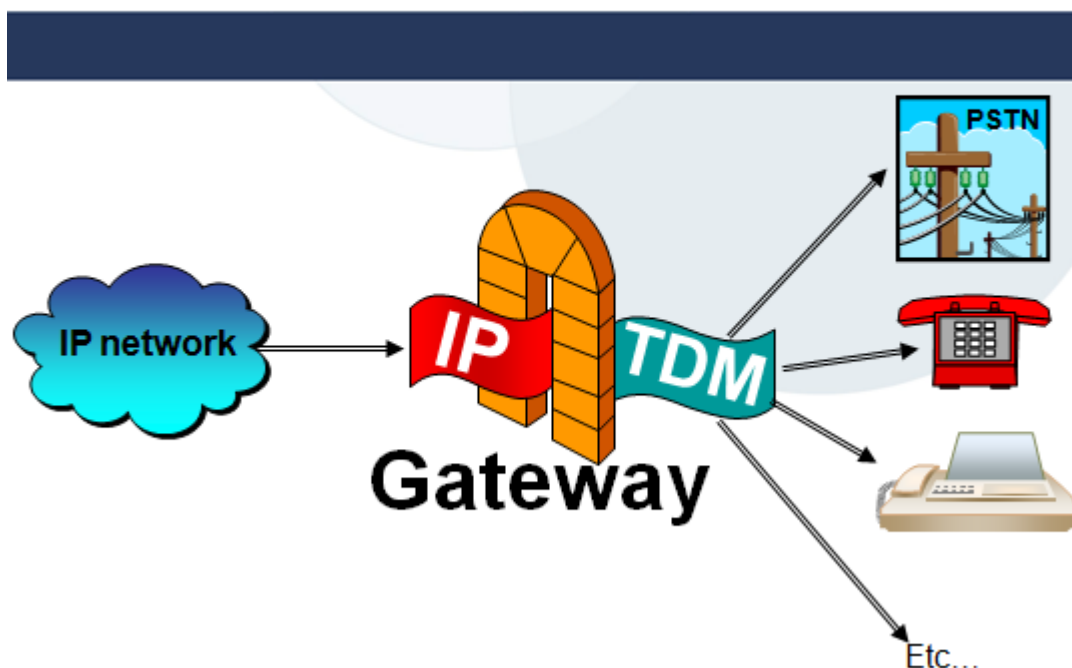


Figure 16 : Passerelle H323

A.3.3. la M.C.U :

Une MCU centralisée fournit du transcodage (protocoles de translation) de divers codecs et flux.

De base, la MCU fournit une fonction de mixage. La MCU prend l'information audio de chaque participant, les mélange et envoie le résultat de ce mélange à tous les participants. Ce n'est pas une fonction de multiplexage. Les sons d'origine sont perdus.

La méthode de distribution de la MCU est choisie par la passerelle ou par l'administrateur. Cela peut aussi bien être du multicast que du multi-unicast.

L'Unicast est souvent la méthode préférée puisqu'il peut traverser des réseaux routés alors que le Multicast ne le peut pas toujours.

A.3.3.1. Les composants MCU H323 :

Les MCU's ont deux composantes. La composante qui contrôle le H.225/H.245 est appelée le contrôleur multipoint (MC – Multipoint Controller).

La composante qui réalise la fonction de mixage est le processeur Multipoint (MP – Multipoint Processor). Un MP est une composante optionnelle du MCU.

Puisque les conférences H.323 peuvent intégrer de la voix, de la vidéo et des données T.120, les MPs les plus puissants peuvent réaliser les trois. Il est aussi possible d'avoir un MP uniquement voix ou un MP voix et vidéo.

Composants MCU H.323

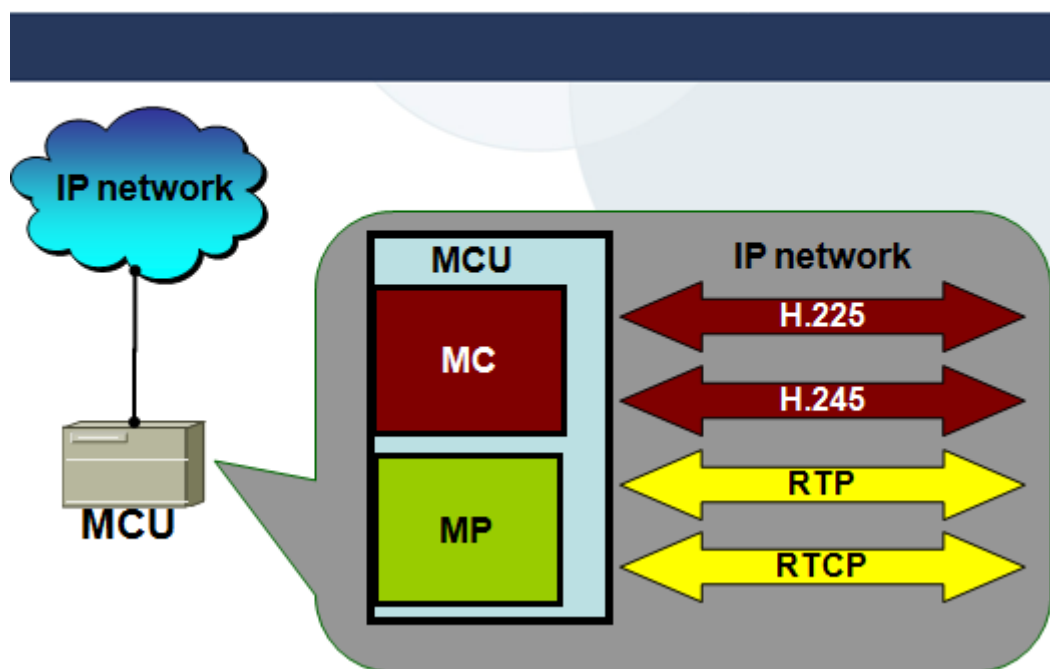


Figure 17 : composants MCU H323

A.3.4. Le GATEKEEPER :

fournit les services de contrôle et de gestion de contrôle des appels pour tous les terminaux enregistrés dans sa zone .

il a 3 fonctions obligatoires :

1. translation d'adresses (IP- MAC vers E.164)
2. admission d'appels : autorisation/ authentification : firewall
3. gestion de la bande passante : limitation du nombre d'appels dans la zone (LAN réseau IP)

Fonctions opérationnelles:

1. gestion de l'appel peut traiter la signalisation (H 245 Q 921)
2. services de (PBX virtuel.
3. routage et reroutage des appels non aboutis.

A.4. Protocoles H 323 intervenant dans un appel H323:

Ci-dessus (figure 18) sont listés les protocoles intervenant dans un appel H.323. RAS (Registration, Admission et Status Protocol) est un protocole supporté par UDP qui spécifie un jeu de commande permettant les communications entre le gatekeeper et les terminaux H.323, les passerelles et les MCUs.

L'enregistrement définit la procédure qu'une passerelle, un terminal ou une MCU suivra pour mettre à jour le gatekeeper. Les informations transmises à le gatekeeper contiennent les adresses E.164, les adresses IP, le port du RAS et le port du H.225.

L'admission est la procédure utilisée pour faire une requête de services à partir de le gatekeeper. Une requête d'admission typique demandera à le gatekeeper de traduire une adresse E.164 en adresse IP, de vérifier la bande passante disponible et de router l'appel.

Le statut est le process que le gatekeeper utilisera pour suivre la progression des appels, plus largement pour le temps de routage de date, la facturation, les rapports et les appels routés vers d'autres zones de le gatekeeper.

La session H.225 intervient dans l'établissement et le relâchement des appels. Il est très similaire au protocole RNIS Q.931. La session H.225 lance la session H.245.

Protocoles H.323

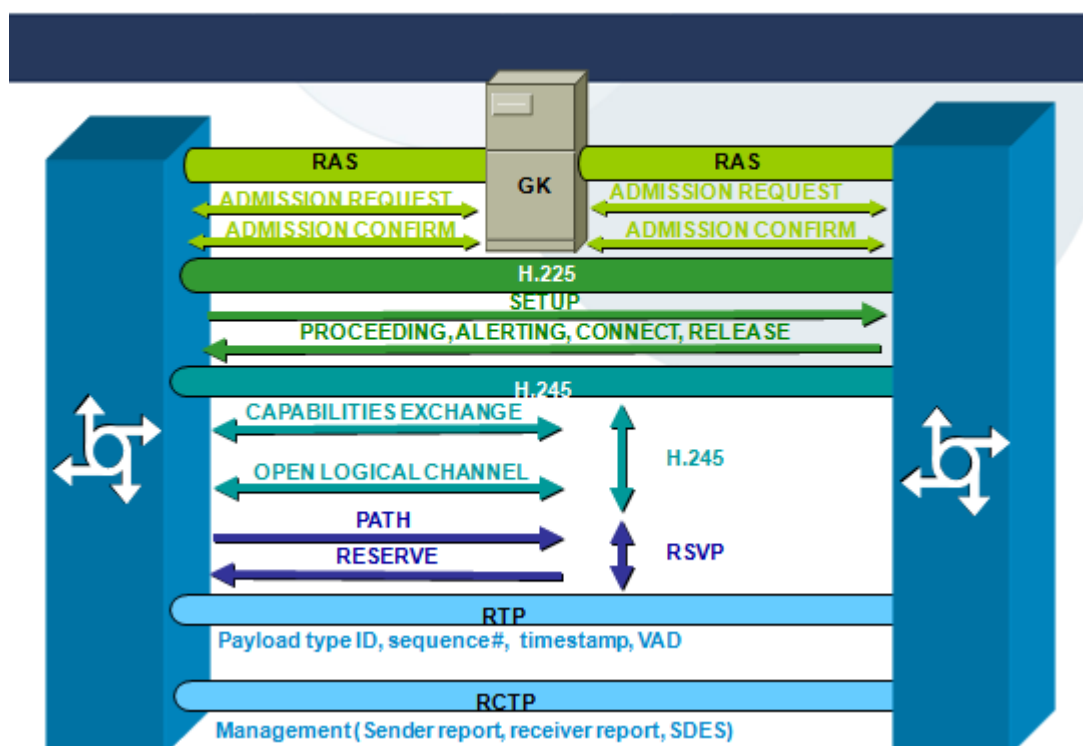


Figure 18 : protocoles H 323 intervenant dans un appel

H.245 détermine quel terminal va être amené à devenir maître/esclave. H.245 établit aussi le profil RTP. Cela inclut la sélection des ports RTP et RTCP, la sélection des codecs, les recommandations de taille du buffer pour la jigue et la taille en millisecondes des échantillons de voix. Puisque H.323 est vraiment un standard de conférence vidéo et voix, H.245 détermine aussi le profil RTP pour les canaux vidéo.

Les codecs recommandés pour H.323 sont listés dans le document précédent. Notez que le support de G.711 est nécessaire. Les autres sont uniquement recommandés.

Le protocole T.120 fournit un contrôle à distance des applications. C'est comme si vous aviez la main sur votre souris, votre clavier et que vous affichiez le résultat sur la station finale via le réseau ce qui permet de contrôler votre PC. Les mises en œuvre de T.120 restreignent votre accès aux seules applications auxquelles vous avez droit.

A.5. Exemple de l'utilisation du protocole H323 avec deux IPBX (deux constructeurs différents):

Enregistrement de chaque Gateway H323 vers le Gatekeeper.

1. Dans le Gatekeeper, il faut d'abord configurer le plan de numéro de chaque Gateway H323. Par exemple, dans l'exemple ci-dessus, on configure deux gateway H323 :
 - a. Alias1 associé à l'adresse ip = IP1 puis on associe à cet alias un plan de numérotation ; par exemple tous les numéros qui commencent par 3 (3XXX)
 - b. Alias2 associé à l'adresse ip = IP2 puis on associe à cet alias un plan de numérotation ; par exemple tous les numéros qui commencent par 4 (4XXX)
 - c. On peut aussi configurer le PSTN (si c'est demandé) : Ici, on imagine que seul le Gateway H323 = IP1 a une passerelle vers le RTC.
 - d. Seuls les numéros qui sont exploitables par le réseau peuvent être configurés (les HSDA ne sont pas obligatoirement nécessaires).
2. Chaque Gateway H323 s'enregistre vers le Gatekeeper. On doit configurer dans le IPBX, l'adresse IP du Gatekeeper.
3. Une fois que chaque Gateway H323 est enregistrée et tout le plan de numérotation est configuré, alors on peut commencer à exploiter le réseau IP en utilisant le protocole H323.

Les Gateway H323 s'enregistrent au Gatekeeper

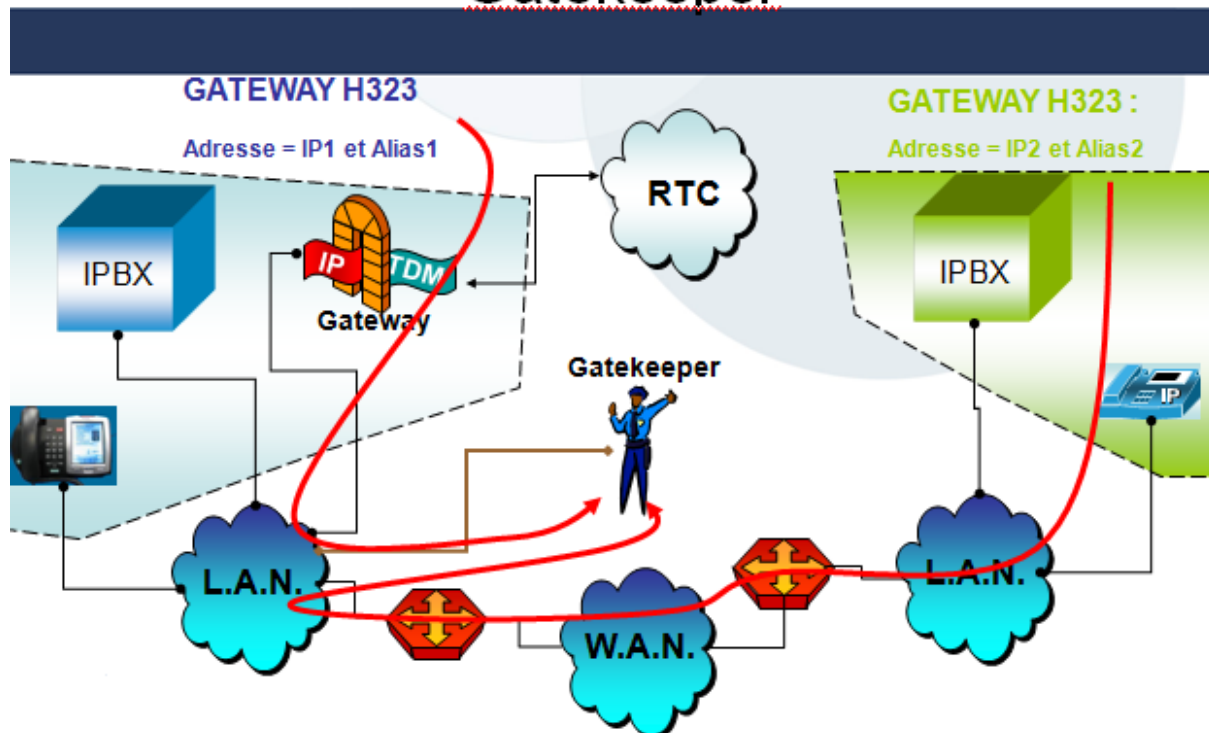


Figure 19 : Enregistrement de la gateway

A.5.1. les étapes pour émettre un appel d'un site vers un autre site :

1. Les postes IP s'enregistrent aux IPBX en envoyant des protocoles propriétaires (Skinny chez Cisco, ou Unistim chez Nortel)
 - a. Ces postes envoient soit :
 - i. Leur mac-adresse (chez Cisco)
 - ii. Leur numéro d'équipement (chez Nortel)
 - iii. Leur numéro téléphone (chez Alcatel)
2. Une fois que les IPBX reconnaissent les postes IP, ceux-ci reçoivent toutes leurs propriétés :
 - a. Leur numéro
 - b. Leur restriction
 - c. Le nom de l'utilisateur

Les postes IP s'enregistrent

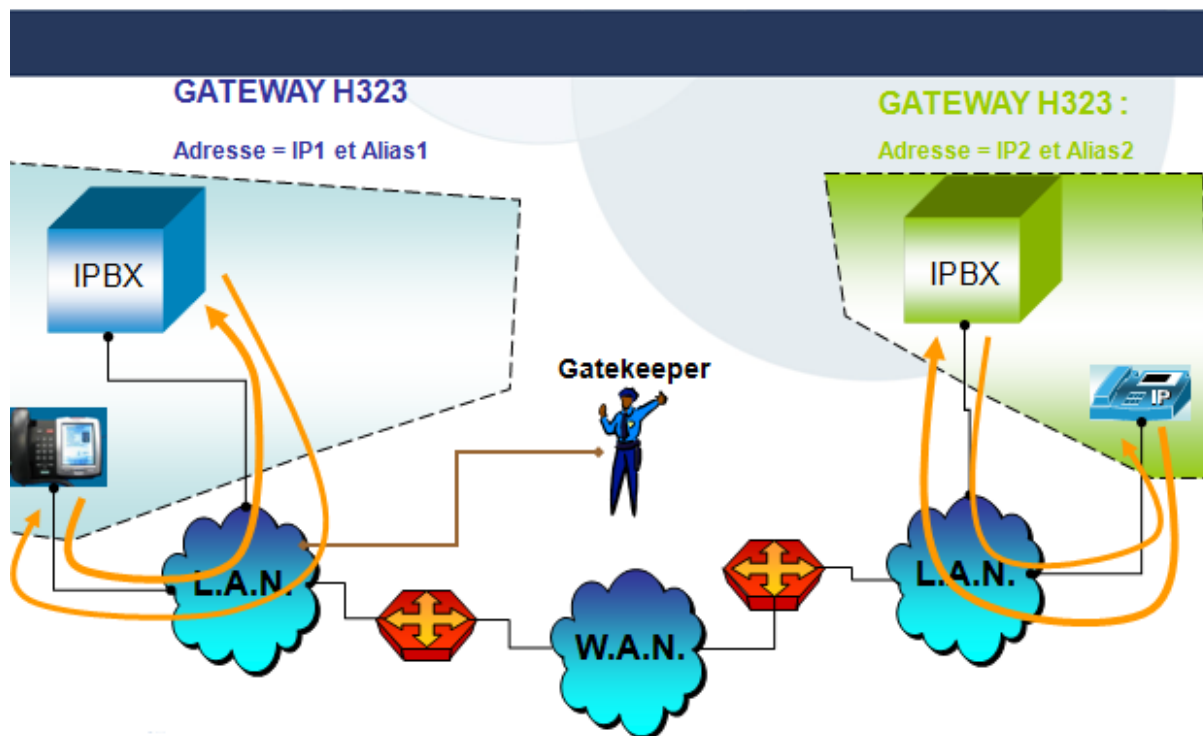


Figure 20 : Enregistrement des postes IP

A.5.2. Utilisation du gatekeeper:

1. Le Gateway H323 dont l'adresse IP est IP1 demande au Gatekeeper s'il connaît le poste 4000
2. Celui-ci lui indique l'adresse IP2

Une fois que le Gateway H323 connaît l'adresse ip du destinataire alors l'initialisation va se dérouler :

1. Le Gateway H323 (IP1) émet un *call setup* qui contient :
 - a. Le numéro de l'appelant
 - b. Le numéro de l'appelé
 - c. La négociation de l'ouverture du canal H245
 - d. La négociation du codec
2. Le Gateway H323 (IP2) répond par *call proceeding* qui indique que l'appel est en cours de traitement ou en file d'attente
3. Le IPBX2 vérifie si le poste 4000 existe :

- a. Si celui-ci n'existe pas, il peut envoyer l'appel vers une tonalité de débordement
 - b. Si celui-ci n'existe pas, il peut envoyer l'appel vers le standard
 - c. Si celui-ci n'existe pas, il peut envoyer l'appel vers un guide vocal
 - d. Si le poste existe alors le IPBX vérifie si il est disponible
4. Si le poste est disponible alors le IPBX2 demande au poste IP de sonner et envoie une information au IPBX que le poste est entrain de sonner (*call Alerting*).
 5. Dès que le poste décroche alors le IPBX2 informe l'IPBX1 par un *call connect*
 6. On peut alors dialoguer via le canal H245 et les protocoles RTP

B. Protocole SIP

B.1. Introduction

Le protocole SIP (Session Initialisation Protocol) a été initié par le groupe MMUSIC (Multiparty Multimedia Session Control) et désormais repris et maintenu par le Groupe SIP de l'IETF .SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Il a été conçu pour l'ouverture, le maintien et la terminaison de sessions de communications interactives entre des utilisateurs. De telles sessions permettent de réaliser de l'audio, de l'enseignement à distance et de la voix (téléphonie) sur IP essentiellement. Pour l'ouverture d'une session, un utilisateur émet une invitation transportant un descripteur de session permettant aux utilisateurs souhaitant communiquer de négocier sur les algorithmes et codecs à utiliser. SIP permet aussi de relier des stations mobiles en transmettant ou redirigeant les requêtes vers la position courante de la station appelée. Enfin, SIP est indépendant du médium utilisé et aussi du protocole de transport des couches basses.

B.2. Architecture protocolaire

SIP est un protocole indépendant des couches de transport, il appartient aux couches applications du modèle OSI. Le SIP gère la signalisation et l'établissement des sessions interactives de communication multimédias et multipartites. Il est aussi basé sur le concept Client / Serveur pour le contrôle d'appels et des services multimédias. Conçu selon un modèle de type IP, il est hautement extensible et assez simple en conception architecturale, de sorte qu'il peut servir de base à la création d'applications et de services. Il est basé sur le protocole HTTP et peut utiliser UDP ou TCP [8].

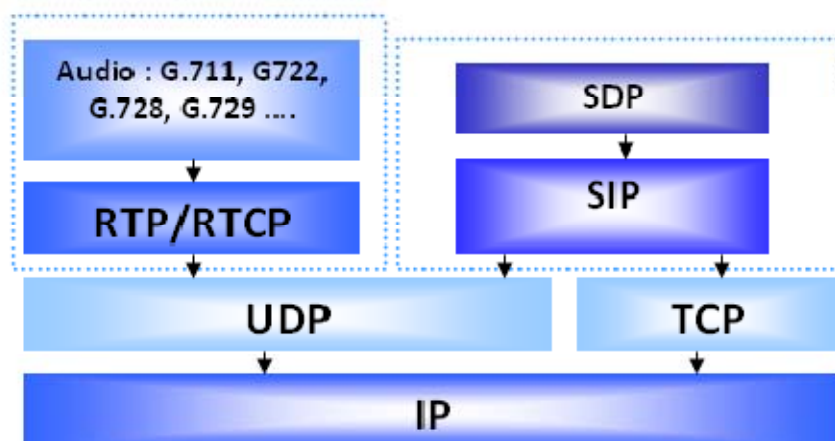


Figure 21 : pile SIP

B.3. 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 les parties appelant et appelé 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 M.C.U (Multipoint Control Unit)

Combinatoire : Plusieurs utilisateurs pleinement interconnectés en multicast via un réseau à maillage complet de connexions.

B.4. Les entités du système SIP:

Dans un système Sip on trouve deux types de composantes, les users agents (UAS, UAC) et un réseau de serveurs :

***L'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.

***L'U.A.C (User Agent Client)** - Il représente l'agent de la partie appelante. C'est une application de type client qui initie les requêtes.

Le relais mandataire ou PS (Proxy Server), auquel est relié un terminal fixe ou mobile, agit à la fois comme un client et comme un serveur. Un tel serveur peut interpréter et modifier les messages qu'il reçoit avant de les retransmettre :

***Le 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.

***Le 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.

***Le RG (Registrar)** - C'est un serveur qui accepte les requêtes Register et offre également un service de localisation comme le LS. Chaque PS ou RS est généralement relié à un Registrar.

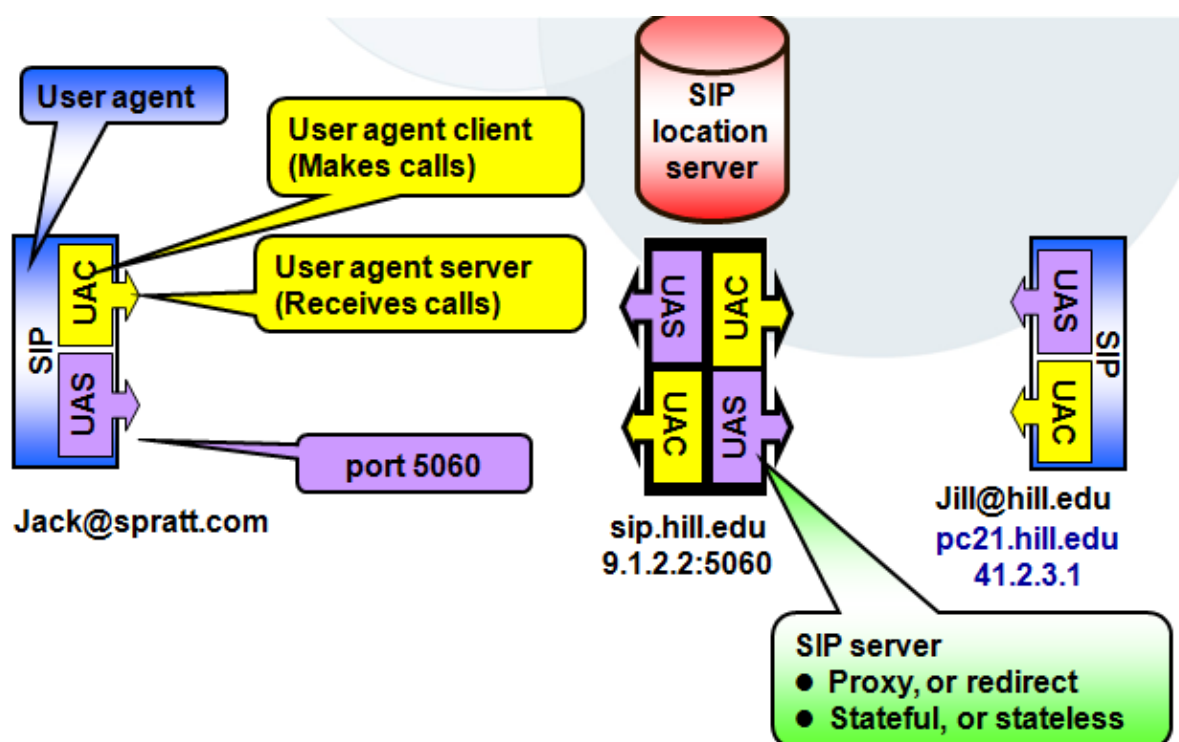


Figure 22 : Entités SIP

B.4.1. Exemple d'un enregistrement sur le SIP Registration:

Voici un exemple d'un utilisateur SIP, *jill@hill.edu*, qui s'enregistre à un serveur SIP en utilisant la méthode d'enregistrement.

La procédure d'enregistrement permet à l'utilisateur *jill@hill.edu* de recevoir des appels à partir de son *pc21.hill.edu*

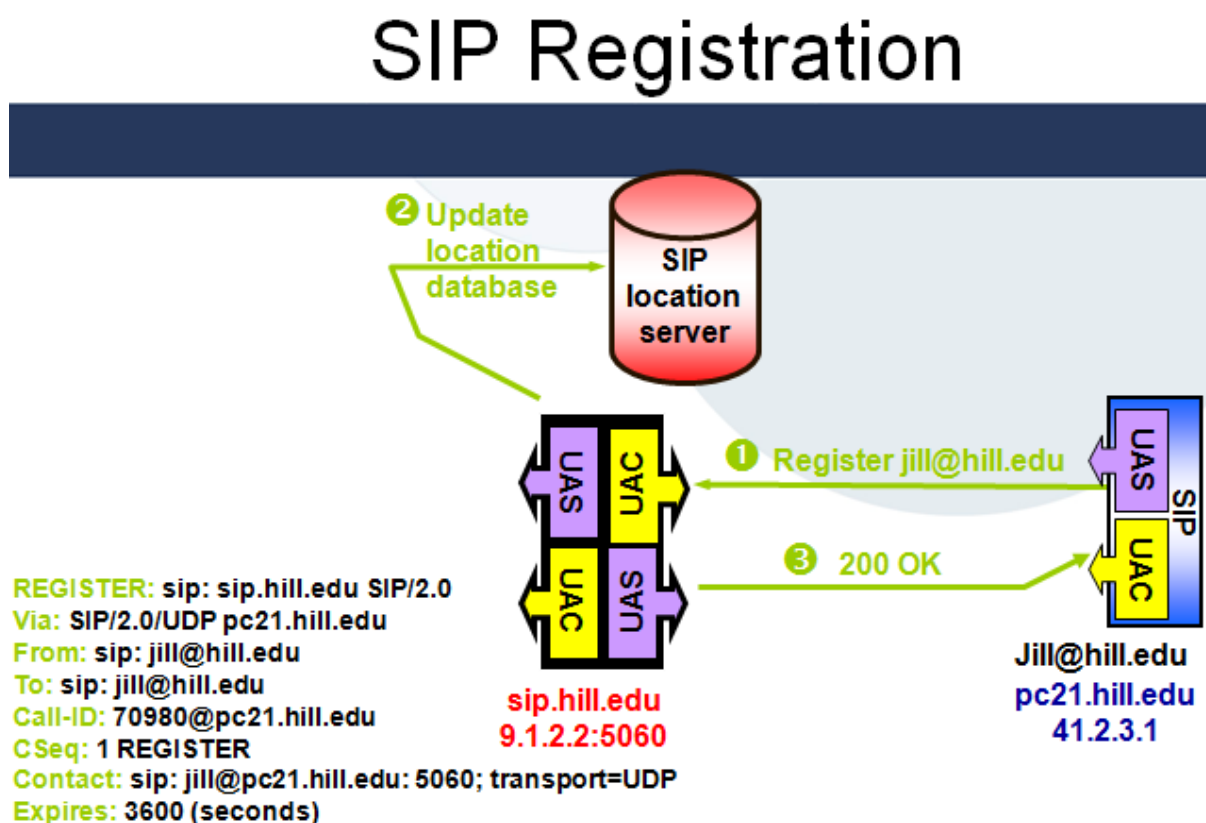


Figure 23 : SIP Registration

B.4.2. exemple d'utilisation d'un serveur proxy SIP :

Un utilisateur nommé jack@spratt.com veut appeler jill@hill.edu :

1. Résolution d'un nom pour connaître l'adresse IP via le DNS hill.edu
2. Une fois que l'adresse IP est connue alors jack@spratt.com peut lancer une invitation à jill@hill.edu en passant par le proxy SIP.
3. Le proxy SIP demande au serveur de location si dans la base de données du serveur location il y a jill@hill.edu et où il se trouve grâce au serveur Registrar
4. Une fois l'utilisateur jill@hill.edu localisé (pc21.hill.edu), le serveur proxy demande une résolution de nom pour avoir l'adresse IP du support de jill@hill.edu
5. Dès que l'adresse IP est connue alors le serveur Proxy peut envoyer une requête d'invitation à jill@hill.edu de la part de jack@spratt.com

6. Le serveur proxy va servir d'intermédiaire entre l'utilisateur jack@spratt.com et jill@hill.edu
 - a. jill@hill.edu envoie un message *100 trying* pour informer l'utilisateur jack@spratt.com que c'est en cours d'analyse
 - b. jill@hill.edu envoie un message *180 ringing* pour informer l'utilisateur jack@spratt.com que le poste est entrain de sonner et jack@spratt.com reçoit une sonnerie de retour
 - c. jill@hill.edu envoie un message *200 OK* pour informer l'utilisateur jack@spratt.com que jill@hill.edu a décroché et envoie également le codec qu'ils vont utiliser pour dialoguer ainsi que le port RTP que jill@hill.edu va utiliser dans le corps S.D.P (Session Description Protocol)
 - d. Jack@spratt.com envoie un message d'acquiescement (ACK) pour confirmer le début de la conversation

SIP Proxy Server

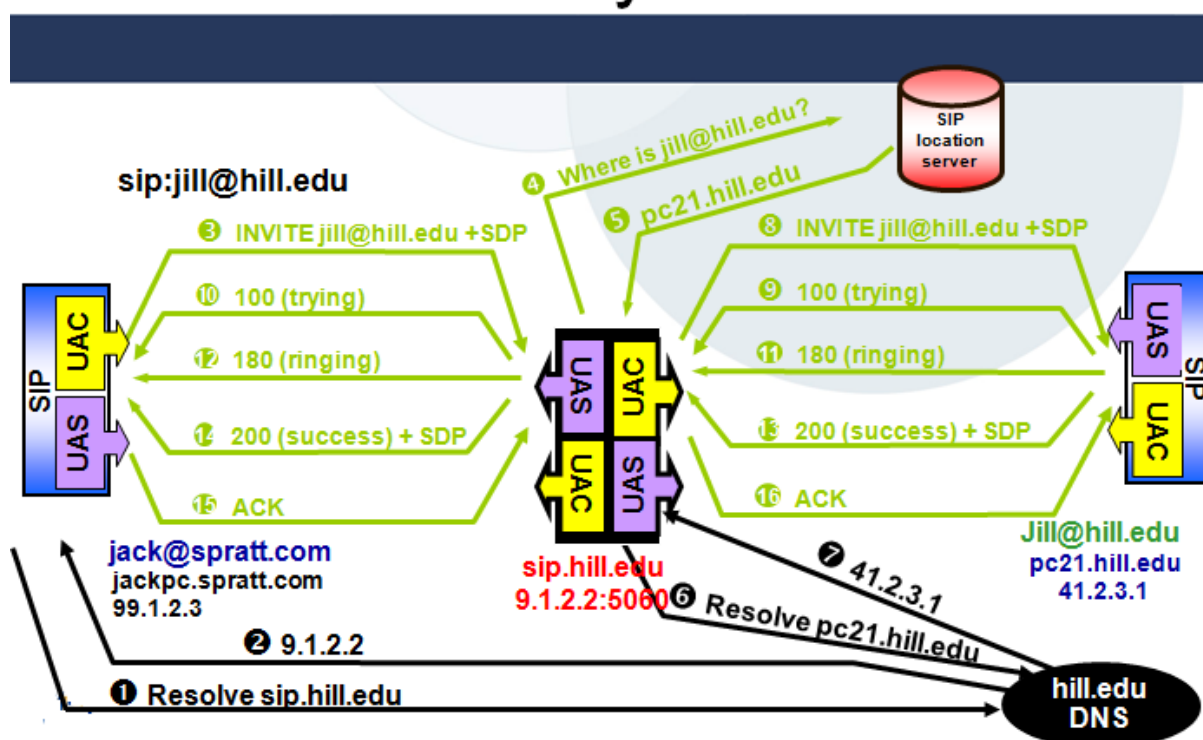


Figure 24 : SIP proxy server

B.5. les différents éléments intervenant dans l'ouverture de session :

Suivant nature des échanges, choix des protocoles les mieux adaptés (Rsvp, Rtp, Rtcp, Sap, Sdp).

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 vidéo).

Chaque utilisateur et sa machine est identifié par une adresse que l'on nomme Url Sip et qui se présente comme une Url Mailto.

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.

***Register** : cette méthode est utilisée par le client pour enregistrer l'adresse listée dans l'URL TO par le serveur auquel il est relié.

B.6. Les réponses SIP :

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, textbased (UTF-8), 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 éronnée 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.

- voir dans l'annexe un tableau recapitulatif des reponses SIP

B.7. Structure des messages SIP

Les messages SIP sont caractérisés par une ligne de début, plusieurs entêtes et le corps du message [8].

- Les entêtes des messages SIP

Les entêtes ont pour rôle de fournir des informations sur le message et de permettre le traitement du message. A cet effet, le protocole SIP est doté d'un certain nombre d'en-tête dont la structure dépend de la nature et du rôle de chaque en-tête. La structure générale d'un entête est articulée autour de plusieurs champs et chaque champ obéit à un format général : `nom_du_champ : valeur_du_champ`. Les types d'entête utilisés par les messages du protocole SIP sont au nombre de quatre:

- L'entête général

Il est toujours présent et contient les informations de base permettant le traitement du message.

Il a des champs obligatoires suivants :

- Via : il identifie l'entité de relais. En effet, chaque entité qui émet ou relaye un message SIP insère son identité afin de prévenir les boucles et indiquer le chemin de réponse.
- From : il identifie l'initiateur de la requête.
- To : il identifie le destinataire de la requête.
- Call-Id : c'est l'identificateur unique de la session.
- Cseq : il identifie la séquence d'un appel : par exemple plusieurs messages « invite » avec de Cseq différents.

- L'entête de requête

Cet en-tête est non toujours utilisé. Il contient des informations supplémentaires à destination du serveur SIP permettant le traitement de la requête par celui-ci.

- L'entête de réponse

Cet en-tête est non toujours utilisé tout comme l'entête de requête. Il contient des informations supplémentaires ajoutées par le serveur SIP permettant le traitement de la réponse.

- L'entête d'entité

Cet en-tête est toujours utilisé. Son rôle est de définir le type et le format des informations contenues dans les messages.

- Le corps du message

Il fournit suffisamment d'informations pour permettre la participation à une session multimédia. Ces informations sont : le codec, destination (adresse IP et port UDP), nom de la session, etc. Le message du corps est codé conformément au protocole SDP (Session Description Protocol). SDP est sans doute le protocole le plus important de l'architecture SIP, SDP a fait l'objet de la proposition de norme RFC 2327. C'est un protocole dont l'objectif est d'établir un descripteur de sessions multimédia à ouvrir, il porte les informations suivantes :

- Adresses de destination SIP: //UserX@ensa.ac.ma.
- Algorithmes de codage Audio et Vidéo.
- Type de trafic RTP.

Le schéma suivant illustre le scénario d'une communication SIP.

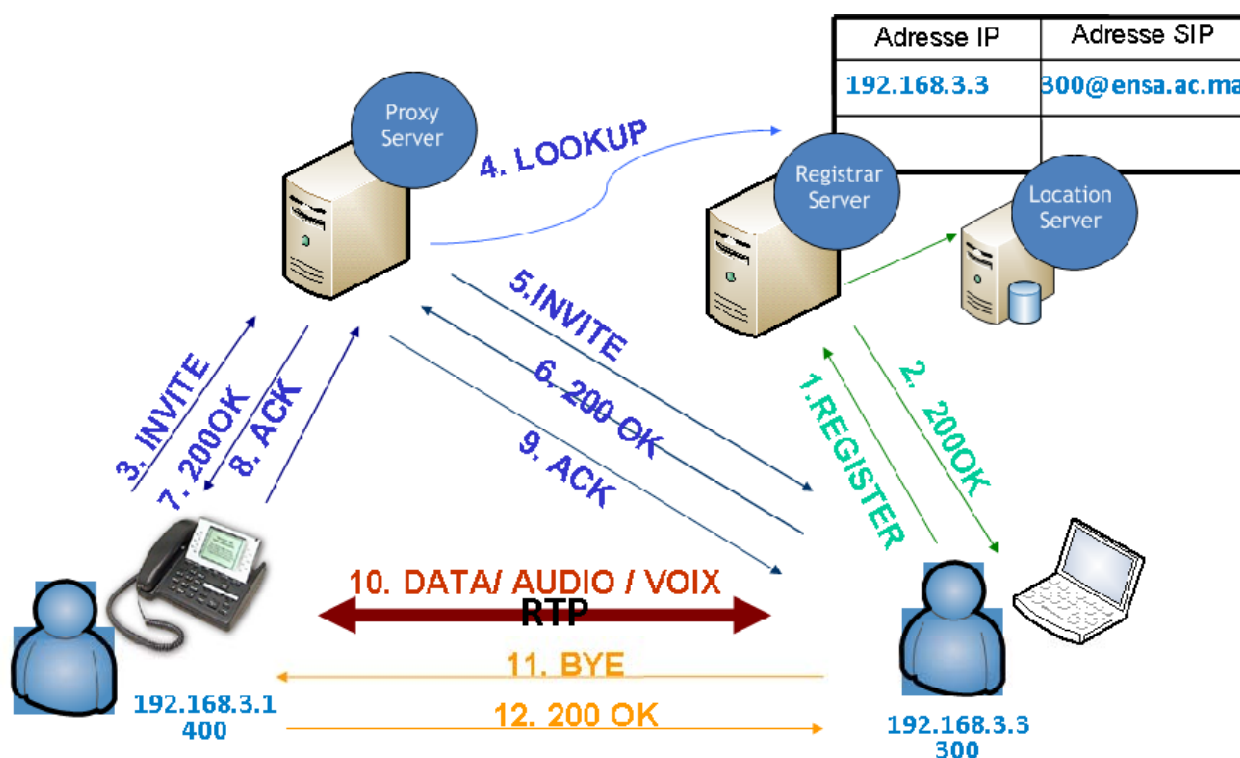


Figure 25 : exemple d'une communication SIP

B.8. Sécurité et Authentification du protocole SIP:

Les messages Sip peuvent contenir des données confidentielles, en effet le protocole Sip possède 3 mécanismes de cryptage :

- Cryptage de bout en bout du Corps du message Sip et de certains champs d'en-tête sensibles aux attaques.
- Cryptage au saut par saut (hop by hop) à fin d'empêcher des pirates de savoir qui appelle qui.
- Cryptage au saut par saut du champ d'en-tête Via pour dissimuler la route qu'a emprunté la requête.

De plus, à fin d'empêcher à tout intrus de modifier et retransmettre des requêtes ou réponses SIP, des mécanismes d'intégrité et d'authentification des messages sont mis en place. Et pour des messages SIP transmis de bout en bout, des clés publiques et signatures sont utilisées par SIP et stockées dans les champs d'en-tête Autorisation.

Une autre attaque connue avec TCP ou UDP est le « Deny of service », lorsqu'un Proxy Server intrus renvoie une réponse de code 6xx au client (signifiant un échec général, la requête ne peut être traitée). Le client peut ignorer cette réponse. Si il ne l'ignore pas et émet une requête vers le serveur "régulier" auquel il était relié avant la réponse du serveur "intrus", la requête aura de fortes chances d'atteindre le serveur intrus et non son vrai destinataire.

B.9. Comparaison SIP vs H323 :

Avantages Du Protocole H.323 :

Il existe de nombreux produits (plus de 30) utilisant ce standard adopté par de grandes entreprises telles Cisco, IBM, Intel, Microsoft, Netscape, etc.

Les cinq principaux logiciels de visioconférence Picturel 550, Proshare 500, Trinicon 500, Smartstation et Cruiser 150 utilisent sur Ip la norme H.323.

Un niveau d'interopérabilité très élevé, ce qui permet à plusieurs utilisateurs d'échanger des données audio et vidéo sans faire attention aux types de média qu'ils utilisent.

Avantages du protocole SIP :

Sip est un protocole plus rapide. La séparation entre ses champs d'en-tête et son corps du message facilite le traitement des messages et diminue leur temps de transition dans le réseau.

Nombre des en-têtes est limité (36 au maximum et en pratique, moins d'une dizaine d'en-têtes sont utilisées simultanément), ce qui allège l'écriture et la lecture des requêtes et réponses.

Sip est un protocole indépendant de la couche transport. Il peut aussi bien s'utiliser avec Tcp que Udp. De plus, il sépare les flux de données de ceux la signalisation, ce qui rend plus souple l'évolution "en direct" d'une communication (arrivée d'un nouveau participant, changement de paramètres...).

	SIP	H323
Nombre échanges pour établir la connexion	1,5 aller-retour	6 à 7 aller-retour
Maintenance du code protocolaire	Simple par sa nature textuelle à l'exemple de Http	Complexe et nécessitant un compilateur
Evolution du protocole	Protocole ouvert à de nouvelles fonctions	Ajout d'extensions propriétaires sans concertation entre vendeurs
Fonction de conférence	Distribuée	Centralisée par l'unité MC
Fonction de téléservices	Oui, par défaut	H.323 v2 + H.450
Détection d'un appel en boucle	Oui	Inexistante sur la version 1 un appel routé sur l'appelant provoque une infinité de requêtes
Signalisation multicast	Oui, par défaut	Non

Tableau 3 : Comparaison SIP _ H323

Donc : La simplicité, la rapidité et la légèreté d'utilisation, tout en étant très complet, du protocole Sip sont autant d'arguments qui pourraient permettre à Sip de convaincre les investisseurs. De plus, ses avancées en matière de sécurité des messages sont un atout important par rapport à ses concurrents.

1.2 . Protocoles de Transport :

Lors d'une communication ToIP, une fois la phase de signalisation réalisée, la phase de communication est initiée. Dans cette phase, un protocole de transport permet d'acheminer les données voix entre plusieurs utilisateurs vu que la couche TCP propose un transport fiable mais lent, et la couche UDP un transport rapide mais non fiable. La communauté IETF a mis en place un nouveau couple de protocole RTP (Real-Time transport Protocol) et RTCP (Real-Time Control Protocol) pour apporter la fiabilité à l'UDP tout en exploitant sa rapidité. RTP et RTCP sont les deux protocoles qui sont principalement utilisés pour le transport de flux média sur le réseau IP. RTP permet de transporter les données entre plusieurs utilisateurs en plus de la gestion temps réelle des sessions. Tandis que, RTCP est utilisé pour transmettre régulièrement des paquets de contrôle, qui contiennent diverses statistiques, ce qui permet de vérifier la qualité de transmission.

A. Protocole RTP :

A.1. Introduction :

Rtp 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 de Udp ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réels comme la parole numérique ou la visio-conférence 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.

A.2. Les fonctions de RTP :

Le protocole RTP, Real Time Transport Protocol, standardisé en 1996, 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 géré au niveau de l'application donc ne nécessite pas l'implémentation d'un Kernel ou de librairies. Comme nous l'avons dit dans l'introduction, Rtp est un protocole de bout en bout. Rtp est volontairement incomplet et malléable pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Rtp laisse la responsabilité du contrôle aux équipements d'extrémité.

Rtp, 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)
- 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 nombre. Cependant il est très important de savoir quel est le paquet qui a été perdu afin de pouvoir pallier à cette perte. Et ce par le remplacement par un paquet qui se compose d'une synthèse des paquets précédent et suivant.
- Identifier le contenu des données pour leur associer un transport sécurisé.
- 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 dépaquetisation afin que l'application soit décodée correctement.

En revanche, ce n'est pas "la solution" qui permettrait d'obtenir des transmissions temps réel sur IP. En effet, il ne procure pas de :

- Réserve de ressources sur le réseau (pas d'action sur le réseau, cf. RSVP);
- Fiabilité des échanges (pas de retransmission automatique, pas de régulation automatique du débit);
- Garantie dans le délai de livraison (seules les couches de niveau inférieur le peuvent) et dans la continuité du flux temps réel.

A.3. Entête RTP:

La figure ci-dessus représente l'en-tête complet du paquet RTP.

Elle contient toutes les informations nécessaires pour délivrer correctement le flux voix. L'en-tête est modifiable pour augmenter la qualité mais au risque d'une perte supérieure d'informations si un paquet est perdu.

L'entête d'un paquet Rtp est obligatoirement constitué de 16 octets sinon au minimum 12 octets. Cette entête précède le "payload" qui représente les données utiles.

Indépendamment du type de session RTP, des champs additionnels peuvent définir le profil RTP.

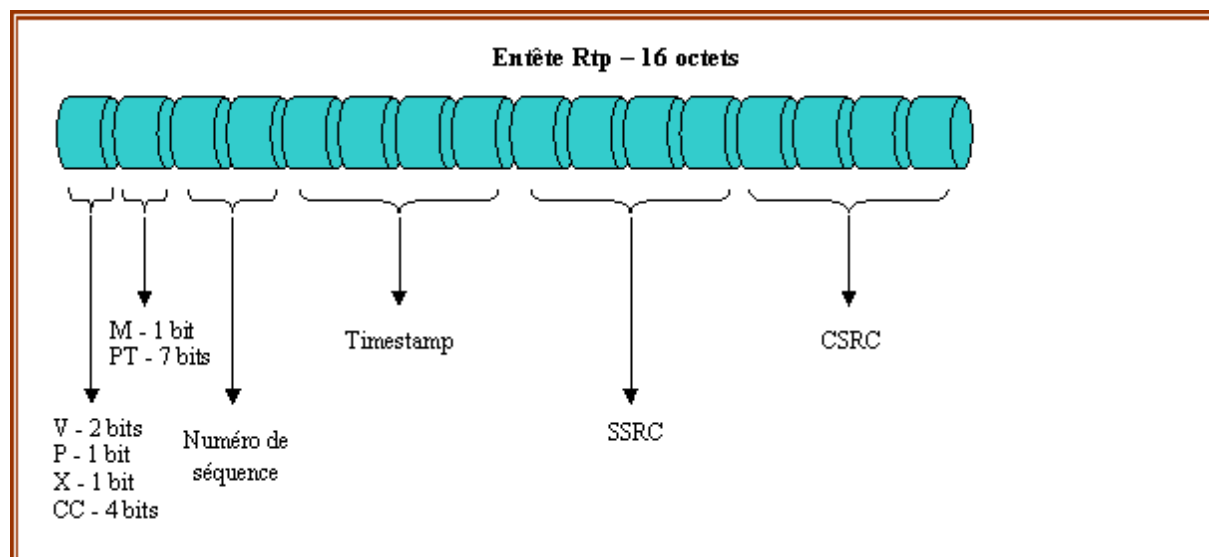


Figure 26 : Schema d'une partie de l'entete d'un paquet RTP

V : Ce champ, codé sur 2 bits, permet d'indiquer la version de Rtp. Actuellement, V=2.

P : Ce bit indique, si il est à 1, que les données possèdent une partie de bourrage.

X : Ce bit spécifie, si il est à 1, que l'entête est suivie d'une entête supplémentaire.

CC : Ce champ, codé sur 4 bits, représente le nombre de CSRC qui suit l'entête.

M : Ce bit, lorsqu'il est à 1, définit que l'interprétation de la Marque est par un profil d'application.

PT : Basé sur 7 bits, ce champ identifie le type du payload (audio, vidéo, image, texte, html, etc.)

Numéro de séquence : Ce champ, d'une taille de 2 octets, représente le numéro d'ordre d'émission des paquets. Sa valeur initiale est aléatoire et il s'incrémente de 1 à chaque paquet envoyé, il peut servir à détecter des paquets perdus.

Timestamp : Ce champ horodatage, de 4 octets, représente l'horloge système ou l'horloge d'échantillonnage de l'émetteur. Elle doit être monotone et linéaire pour assurer la synchronisation des flux.

SSRC : Basé sur 4 octets, ce champ identifie de manière unique la source de synchronisation, sa valeur est choisie de manière aléatoire par l'application.

CSRC : Ce champ, sur 4 octets, identifie les sources de contribution. La liste des participants ayant leur contribution (audio, vidéo) aux données du paquet.

B. Protocole RTCP :

B.1. Introduction :

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 :

B.2. Les fonctions du RTCP :

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.

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 suivre des chemins différents.

L'identification car 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, car 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:

200 : rapport de l'émetteur

201 : rapport du récepteur

202 : description de la source

203 : au revoir

204 : application spécifique

Ces différents paquets de supervision fournissent aux nœuds du réseau les instructions nécessaires à un meilleur contrôle des applications temps réel.

B.3. Entête RTCP :

Ce protocole définit cinq paquets de contrôle :

200 - SR (Sender Report) : Ce rapport regroupe des statistiques concernant la transmission (pourcentage de perte, nombre cumulé de paquets perdus, variation de délai (jitter), ...Ces rapports sont issus d'émetteurs actifs d'une session.

201 - RR (Receiver Report) : Ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.

202 - SDES (Source Description) : Carte de visite de la source (nom, e-mail, localisation).

203 - BYE : Message de fin de participation à une session.

204 - APP : Fonctions spécifiques à une application.

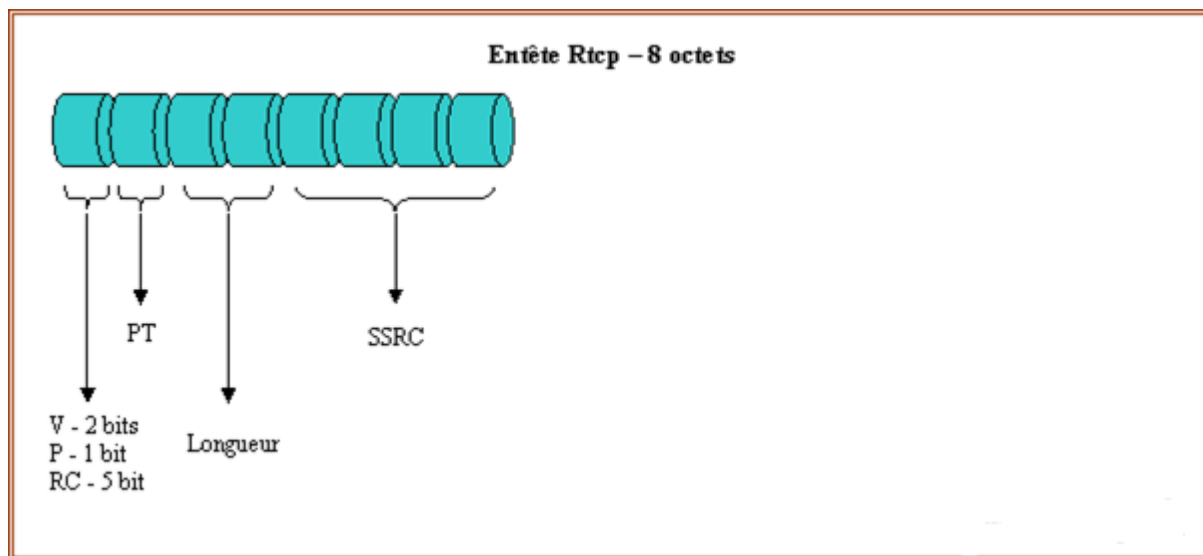


Figure 27 : En -tête des paquets RTCP

Voici l'en-tête commun à tous les paquets Rtcp.

V : Ce champ, codé sur 2 bits, permet d'indiquer la version de Rtp, qui est la même que dans les paquets Rtcp. Actuellement, V=2.

P : Ce bit indique, si il est à 1, que les données possèdent une partie de bourrage.

RC : Ce champ, basé sur 5 bits, indique le nombre de blocs de rapport de réception contenus en ce paquet. Une valeur de zéro est valide.

P T : Ce champ, codé sur 1 octet, est fixé à 200 pour identifier ce datagramme Rtcp comme SR.

Longueur : Ce champ de 2 octets, représente la longueur de ce paquet Rtcp incluant l'en-tête et le bourrage.

SSRC : Basé sur 4 octets, ce champ, représente l'identification de la source pour le créateur de ce paquet SR.

B.4. Conclusion

Rtp nécessite le protocole de transport Udp, (en-tête 8 octets), qui fournira les numéros de port source et destination nécessaire à la couche application. Pour l'instant le protocole Rtp se trouve au dessus de Udp, tandis que dans le futur, on aura une indépendance vis à vis des couches réseau.

En résumant, ces deux protocoles sont adaptés pour la transmission de données temps réel. Cependant, ils fonctionnent en stratégie bout à bout et donc ne peuvent contrôler l'élément principal de la communication : le réseau.

Ces protocoles sont principalement utilisés en visioconférence où les participants sont tour à tour émetteurs ou récepteurs. Pour le transport de la voix, ils permettent une transmission correcte sur des réseaux bien ciblés. C'est-à-dire, des réseaux qui implémentent une qualité de service adaptée. Des réseaux bien dimensionnés (bande passante, déterminisme des couches sous-jacentes, Cos, ...) peuvent aussi se servir de cette solution.

III.2. Compatibilité de la TOIP et le réseau téléphonique classique :

2 .1. Standard ENUM :

La fourniture à grande échelle du service ToIP suppose l'identification aisée des terminaux IP connectés au réseau désireux accéder à ce service. Cette identification est basiquement faite à travers les adresses IP. Afin d'étendre les possibilités d'adressage l'UIT-T a travaillé sur le standard ENUM.

ENUM (tElephone NUmber Mapping) est un protocole défini par l'IETF permettant d'utiliser un numéro de téléphone (E.1641) comme clé de recherche dans le DNS pour trouver la manière de joindre une personne (par exemple : n° de téléphone mobile, n° de fax, adresse de téléphonie IP, adresse e-mail, adresse de messagerie instantanée, etc.)

Le principe d'ENUM repose sur la création d'un nom de domaine Internet pour chaque numéro de téléphone du plan de numérotation international E.164. Les coordonnées que les utilisateurs souhaitent publier pour leur propre numéro de téléphone sont ensuite "stockées" dans le système des noms de domaine Internet (DNS) et ainsi rendues accessibles de manière globale pour tous.

Voici un schéma expliquant le principe de fonctionnement d'ENUM :

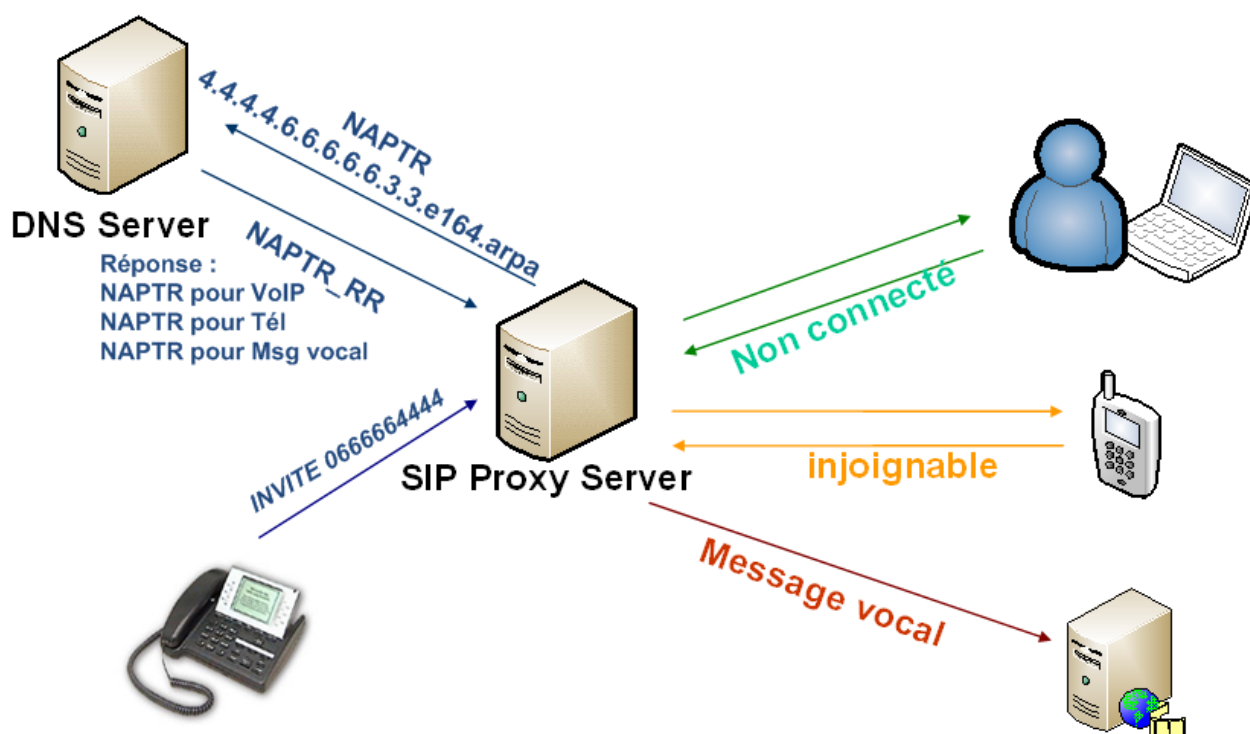


Figure 28 : exemple d'utilisation d'ENUM

III.3. Problématique ToIP avec les NAT et les pare-feux

Dans une architecture ToIP, les NAT et les pare-feux représentent un problème pour les flux de signalisation et média. L'objectif de ce paragraphe est de comprendre cette problématique et de présenter des exemples de solutions existantes pour résoudre ce problème.

3.1 Problème de NAT

Le mécanisme NAT (Network Address Translation) permet de faire correspondre les adresses IP internes souvent non routables d'un domaine à un ensemble d'adresses routables. Avec la ToIP, ce mécanisme représente un problème pour le transit des flux multimédia.

En effet, les informations utilisées pour la signalisation ou la communication sont incluses au niveau 4 et les couches supérieures du modèle OSI, tandis que les NAT travaillent sur la couche 3.

Voici un schéma expliquant le problème de NAT avec la ToIP :

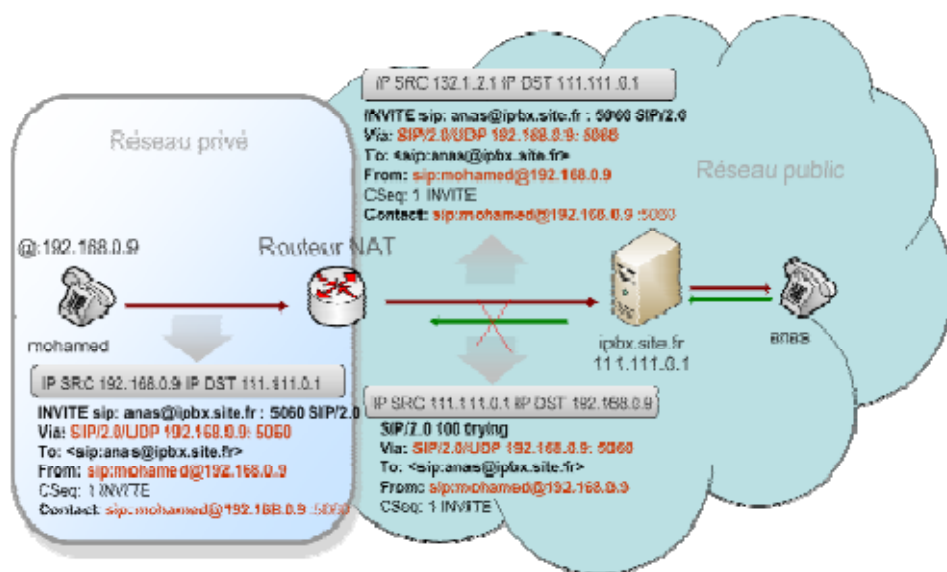


Figure 29 : problème de NAT avec SIP

Dans cet exemple, Mohamed ne pourra établir de communication avec Anas étant donné que l'IPBX n'arrive pas à relayer les réponses SIP de Anas. En effet, lors de la traduction d'adresse effectuée par le routeur NAT, seuls l'adresse et le numéro de port contenus dans l'entête du paquet IP sont modifiés. L'adresse et le numéro de port contenus dans le corps de la requête INVITE du message SIP ne sont pas modifiés. Hors cette adresse est non routable.

3.2 Problème de pare-feu :

Un pare-feu (firewall) est un équipement permettant d'assurer la sécurité d'un site en filtrant le trafic non désiré, il permet de filtrer les paquets venant du réseau public. Le mode de fonctionnement de la plupart des pare-feux pose un problème pour l'établissement des communications SIP.

SIP, par son fonctionnement interne qui permet la localisation des utilisateurs au sein d'un réseau et la négociation des paramètres de la session (codecs, port RTP, etc.), pose des problèmes pour les flux multimédias qui traversent les firewalls. En effet, dans l'architecture de SIP, plusieurs informations critiques telles que l'adresse IP ainsi que le port à utiliser sont contenues dans les messages SIP.

La problématique engendrée par l'utilisation de SIP au travers des pare-feux vient du fait que ceux-ci sont généralement déployés en utilisant des politiques de filtrage qui rejettent tous les paquets qui ne proviennent pas ou qui ne sont pas destinés à une adresse IP et un port définis. Ces politiques, qui sont généralement statiques, ne permettent pas la traversée d'un flux de données à des protocoles comme SIP qui peut négocier des adresses IP et des numéros du port inconnus par le pare-feu lors de l'établissement de session.

Afin de bien comprendre la problématique engendrée par les pare-feux pour les flux multimédias, voici le schéma d'un scénario d'établissement de session et comment le firewall bloque le contenu multimédia.

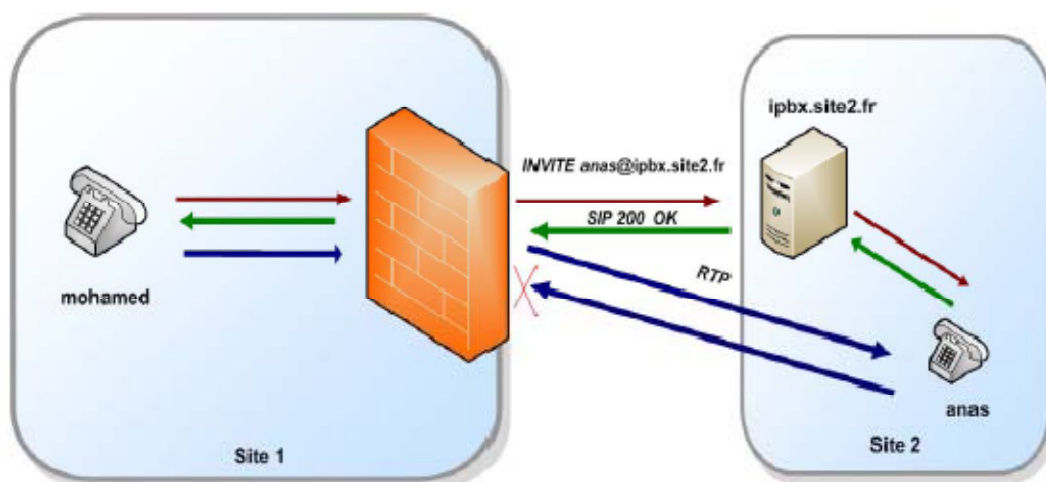


Figure 30 : problème du firewall avec la ToIP

Dans cet exemple, l'utilisateur SIP mohamed@poste.site.fr invite l'utilisateur anas@ipbx.site2.fr afin d'ouvrir une session. Mohamed envoie donc une requête d'invitation INVITE contenant les informations de la session à ouvrir à Anas. Anas répond avec le message 200 OK contenant des informations supplémentaires sur la session à ouvrir.

Comme on peut le constater, l'adresse ainsi que le port à utiliser lors de l'ouverture de la session audio sont contenus dans le corps des messages INVITE et OK. Ces deux informations servent à l'établissement du flux audio entre Mohamed et Anas. Dans notre exemple, Mohamed et Anas utilisent respectivement les ports 3456 et 5004. Par conséquent, comme le firewall a des règles de filtrage strictes et statiques, le contenu multimédia d'Anas sera donc tout simplement bloqué par le firewall.

Mohamed et Anas utilisent respectivement les ports 3456 et 5004. Par conséquent, comme le firewall a des règles de filtrage strictes et statiques, le contenu multimédia d'Anas sera donc tout simplement bloqué par le firewall.

3.3.1 Passerelle de la couche application (ALG) :

La technique de la passerelle applicative consiste à rendre « intelligents » les pare-feux et les routeurs NAT afin qu'ils soient en mesure d'interpréter un protocole spécifique. Plutôt que de vérifier uniquement l'entête du paquet à traiter, les passerelles réalisent une inspection complète des données dans le corps du paquet. Les passerelles agissent donc en tant que relais spécialisés pour un protocole précis (SIP par exemple).

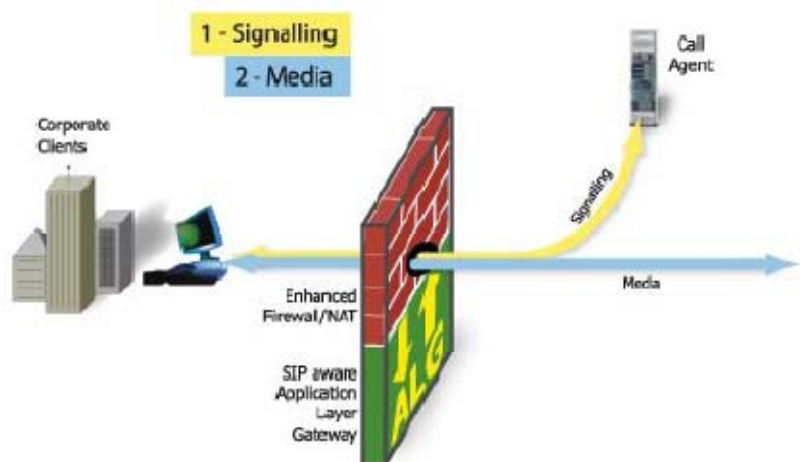


Figure 31 : technique de la passerelle d'application

Le pare-feu/routeur NAT va donc lire le contenu complet du paquet puis va modifier les adresses IP et ports inscrits dans le paquet afin de pouvoir transmettre le paquet dans le réseau public. Suite à cela, le pare-feu/routeur NAT ouvrira un « port d'accès » afin que la communication puisse avoir correctement.

3.3.2 STUN

STUN (Simple Traversal of UDP Through Network Address Translators) est un protocole développé par le groupe de travail de MIDCOM.

Cette technique se distingue des techniques des passerelles de la couche application par son indépendance face aux protocoles de communication.

STUN permet de traverser les routeurs NAT en affectant une adresse IP et un numéro de port public à un poste situé dans le réseau privé pour effectuer une communication de type UDP avec un réseau public. Pour ce faire, une série de requêtes à un serveur STUN est effectuée et les réponses du serveur servent à caractériser l'adresse IP et le numéro de port d'un poste à communiquer.

Combinant STUN à des protocoles tel que SIP, plusieurs problèmes liés aux routeurs NAT peuvent être solutionnés. Seul le cas où des routeurs NAT de type symétrique³ sont utilisés ne peut être traité en utilisant cette technique.

La figure suivante décrit le principe de fonctionnement du protocole STUN.

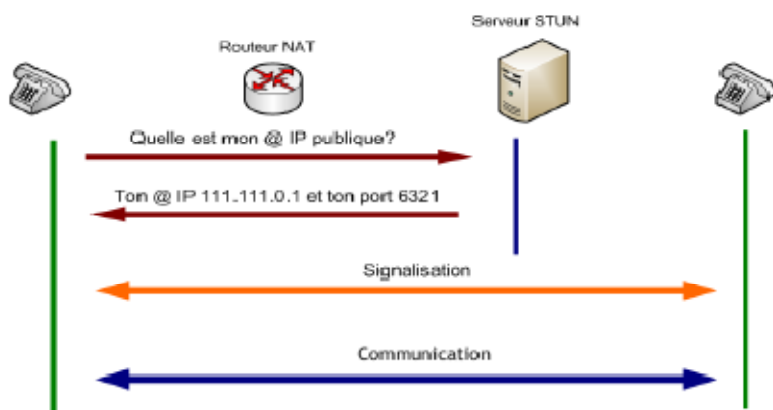


Figure 32 : principe de fonctionnement du protocole STUN

3.3.3 TURN

TURN (Traversal Using Relay NAT) est un mécanisme en cours développement et de standardisation auprès de l'IETF agissant en tant que serveurs de relais. Il a été développé afin de pallier les lacunes du protocole STUN.

Ce protocole permet à des clients qui sont dans des réseaux utilisant des routeurs NAT d'effectuer des connexions entre eux en passant par un serveur de relais.

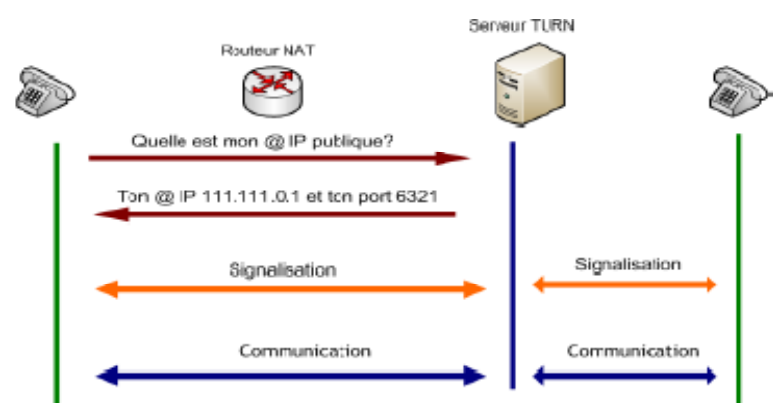


Figure 33 : principe de fonctionnement du protocole TURN

3.3.4. ICE

ICE (Interactive Connectivity Establishment) est une technologie en cours de développement par IETF qui consiste à intégrer STUN et TURN au sein des clients SIP pour déterminer toutes les connexions possibles entre deux postes.

NB: Un NAT symétrique est celui dans lequel la translation d'adresse est calculée en fonction de l'adresse IP et port de la source et de celui du destinataire.

3.3.5. Résumé des solutions

Le tableau qui suit résume les principes, avantages et inconvénients des solutions présentées :

solution	principe	Avantages	Inconvénients
ALG	Firewall et routeur NAT « intelligents » capables de travailler au niveau 7	Technique simple	- Temps de latence importants dus au traitement complet et individuel des paquets.
STUN	Détermine le couple (adresses, ports) publics qu'on doit utiliser dans le paquet SIP pour obtenir une réponse	- Protocole standardisé. - Peu d'infrastructure : seul 1 serveur doit être déployé pour effectuer les requêtes.	- il ne fonctionne pas avec les NATs symétriques
TURN	- Basé sur STUN pour l'échange de clés - Le serveur TURN sert de relais entre l'émetteur et le récepteur	- Technique simple	- Modification des programmes nécessaire pour qu'ils puissent intégrer TURN
ICE	- intègre STUN et TURN au sein des clients SIP pour déterminer toutes les connexions possibles entre deux postes.	Traverse tous types de NAT	- Temps d'établissement d'un appel long. - Modification des serveurs et clients pour le déploiement.

Tableau 4 : résumé des solutions de traversées les NAT et les pare-feux

4. ToIP et la sécurité des communications voix

La téléphonie sur IP, malgré ses très nombreux avantages, notamment financiers, comporte des risques majeurs en termes de sécurité des communications voix.

4.1. Vulnérabilités de la ToIP

Un appel téléphonique ToIP se décompose en deux phases : la signalisation qui permet d'établir l'appel, et la phase de transport des flux de medias qui transportent la voix.

Au cours de la phase de signalisation, les messages SIP codés en mode texte sont transmis de façon non chiffrée dans le réseau, ce qui permet à un pirate d'écouter facilement les messages SIP et d'accéder aux informations de transport des flux média.

En outre durant le transport des flux voix, le protocole RTP présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrement. Par voie de conséquence, plusieurs attaques ToIP peuvent avoir lieu.

4.2. Exemples d'attaques sur l'infrastructure ToIP

Il existe de nombreuses attaques possibles sur le réseau ToIP dont les plus répandues, sont :

- Dénis de service (attaque DoS) : l'objectif d'une attaque DoS est de rendre un élément du réseau indisponible. Un exemple de ce type d'attaque est l'envoi illégitime de paquets SIP BYE [17].
- Ecoute clandestine : L'objectif de cette attaque est d'écouter le trafic de signalisation et/ou de données, en utilisant des outils d'écoute réseau tels que VOMIT (Voice Over Misconfigured Internet Telephone), SiVuS (SIP Vulnerability Scanner), et WireShark [17].
- Détournement du trafic : l'attaquant redirige à son profit le trafic ToIP. Elle se base sur l'envoi d'un message de redirection indiquant que l'appelé s'est déplacé et donne sa propre adresse comme adresse de renvoi, de cette façon tous les appels destinés à l'utilisateur sont transférés à l'attaquant [17].
- Usurpation d'identité : Ce type d'attaque consiste à usurper l'identité de l'expéditeur du message SIP en modifiant l'identité de l'expéditeur d'un message [17].
- Vols de services : le pirate peut emprunter l'identité d'un utilisateur et l'utiliser pour faire passer des appels sur le réseau ToIP sans avoir payé le fournisseur de service [17].

4.3. Solutions de sécurité de la ToIP :

Les mécanismes de sécurité proposés dans une architecture ToIP sont :

- La sécurité de l'infrastructure IP: C'est le premier niveau de sécurité, car la sécurité de l'infrastructure ToIP est liée à la sécurité du réseau IP. Un exemple est la séparation logique des réseaux Data et Voix par des VLANs.
- L'authentification : L'authentification du téléphone IP par le serveur et l'authentification du serveur par le téléphone IP avant d'autoriser un quelconque appel. Il existe différents moyens d'authentification tels que: SIPS, IPsec.
- SIPS (Session Initiation Protocol Secure) : est un mécanisme de sécurité défini par RFC 3261 pour l'envoi de messages SIP au-dessus du protocole de sécurisation TLS (Transport Layer Security).
- IPsec (Internet Protocol Security) : est un ensemble de protocoles (couche 3 du modèle OSI) défini par IETF, permettant le transport sécurisé des données sur un réseau IP.
- Le chiffrement: c'est un moyen efficace de protéger les données. Plusieurs solutions peuvent être utilisées : le chiffrement des flux de signalisation avec SIPS, le chiffrement des flux voix avec SRTP, des solutions propriétaires.
- SRTP (Secure Real-time Transport Protocol): définit un profil de RTP, qui a pour but d'apporter le chiffrement, l'authentification et l'intégrité des messages, et la protection contre le replay de données RTP en unicast et multicast. SRTP a été conçu par Cisco et Ericsson, et est ratifié par l'IETF.

5. La ToIP et IPv6 :

IPv6 est le protocole Internet de nouvelle génération conçu par l'IETF. Il permet principalement de disposer d'un plus grand nombre d'adresses pour chaque élément du réseau. Il offre également une plus grande facilité de configuration et améliore les mécanismes de gestion de la mobilité IP. Il intègre nativement la sécurité, les classes de service et la diffusion multicast.

Le déploiement du protocole IPv6 pour le support de la ToIP va permettre d'éviter d'avoir recours aux NATs grâce à sa grande capacité d'adressage et de simplifier ainsi l'architecture. Néanmoins, la mise en place de la ToIP en IPv6 n'est pas encore répandue parce que la plupart des équipements de ToIP ne supportent pas encore cette version du protocole IP. Voici des exemples de solutions ToIP qui supportent IPv6: Kamailio (routeur d'appels), Linphone, Kphone et SJPhone (qui sont des « softphones », applications logicielles à installer sur un ordinateur).

Conclusion :

La téléphonie sur IP est une technologie qui utilise les réseaux informatiques comme support de communication. Les solutions ToIP sont de plus en plus basées sur des standards ouverts. Beaucoup de ces solutions utilisent SIP comme protocole de signalisation ToIP. Les principaux protocoles utilisés pour le transport de la voix sont : RTP et RTCP. Et pour garantir la compatibilité entre la ToIP et le réseau téléphonique classique, l'IETF a travaillé sur le standard ENUM.

Le déploiement de la technologie ToIP dans les réseaux actuels a provoqué l'apparition des nouvelles problématiques notamment au niveau des dispositifs de sécurité tels que les pare-feu et les routeurs NAT, ainsi que les vulnérabilités de ToIP en terme de sécurité. Les problèmes de NAT et de pare-feux ont été solutionnés en utilisant plusieurs techniques qui sont résumées dans le tableau 4, tandis que de nombreux mécanismes de sécurité ont été présentés notamment la sécurité de l'infrastructure IP, l'authentification, et le chiffrement. Dans le chapitre qui suit.

CHAPITRE III :

Architectures et sécurisation.

I.1. Introduction :

L'opportunité de migrer de la téléphonie classique vers la téléphonie IP, a offert plusieurs avantages aux centres d'appels, et leurs a permis de bénéficier de nouveaux services tel que la vidéoconférence et la transmission des données..... L'intégration de ces services dans une seule plateforme nécessite plus de sécurité.

Dans ce chapitre, nous dériverons des attaques qui menacent la VoIP, et nous détaillerons quelques unes. Nous finirons par une description des bonnes pratiques pour sécuriser les communications de type voix sur IP.

Le système VoIP utilise l'Internet, et particulièrement le protocole IP. De ce fait les vulnérabilités de celui-ci.

Les attaques sur les réseaux VoIP peuvent être classées en deux types :

Les attaques externes sont lancées par des personnes autres que celles qui participent à l'appel, et elles se produisent généralement quand les paquets VoIP traversent un réseau peu fiable et/ou l'appel passe par un réseau tiers durant le transfert des paquets, tant dis que les attaques internes s'effectuent directement du réseau local dans lequel se trouve l'attaquant.

Il existe deux principales classes de vulnérabilités sur un environnement VoIP. La première dépend des protocoles utilisés (SIP, H.323...) et la deuxième est reliée aux systèmes sur lesquels les éléments VoIP sont implémentés. Chaque protocole ou service a ses propres vulnérabilités.

Nous proposons, face aux innombrables configurations possibles de réseaux VoIP, une classification basée sur des tendances observées dans l'utilisation des systèmes tels que :

- **PBX : *Private Branch eXchange*** (Autocommutateur téléphonique privé), installation privée de commutation pouvant transmettre la voix; elle est située dans les locaux de l'organisme utilisateur final et offre sur place la connexion entre les terminaux qui y sont branchés, y compris le service de composition, et peut assurer les connexions entre ces terminaux et d'autres réseaux de communication, y compris le PTSN.
- **IP-PBX ou IPBX : *Internet Protocol PBX***, cette installation a toute les fonctions d'un PBX, mais fonctionne avec la communication IP par paquets. Pour SIP, il s'agit du *proxy*, du *registrar* et du service de localisation.
- **IP-enabled PBX** : Un PBX hybride pouvant également s'interfacer avec un système VoIP.
- **IP Centrex** : IP Centrex est un système ASP. L'IPBX est fourni par un tiers, avec éventuellement un *gateway* dans l'entreprise, pour fournir le service aux appareils non-VoIP.
- **IP Phones** : Ce terme est utilisé lorsque l'on parle indifféremment de *hardphones* ou de *softphones*.
- **ASP (*Application Service Provider*)** : Fournisseur de services

Un **premier niveau** de classification sépare les centres d'appels qui délèguent la problématique à un ASP tel que (désignés aussi comme des ITSP : *Internet Telephony Service Provider*) avec celles qui utilisent leur propre IPBX.

Dans le premier cas, la situation est relativement simple étant donné qu'on ne trouve que des « SIPphones » dans l'entreprise, et donc la sécurisation ne se fera qu'au niveau de ces téléphones et de la connexion avec l'ASP. Les centres d'appels qui possèdent leur propre IPBX et du matériel SIP présentent une situation plus complexe.

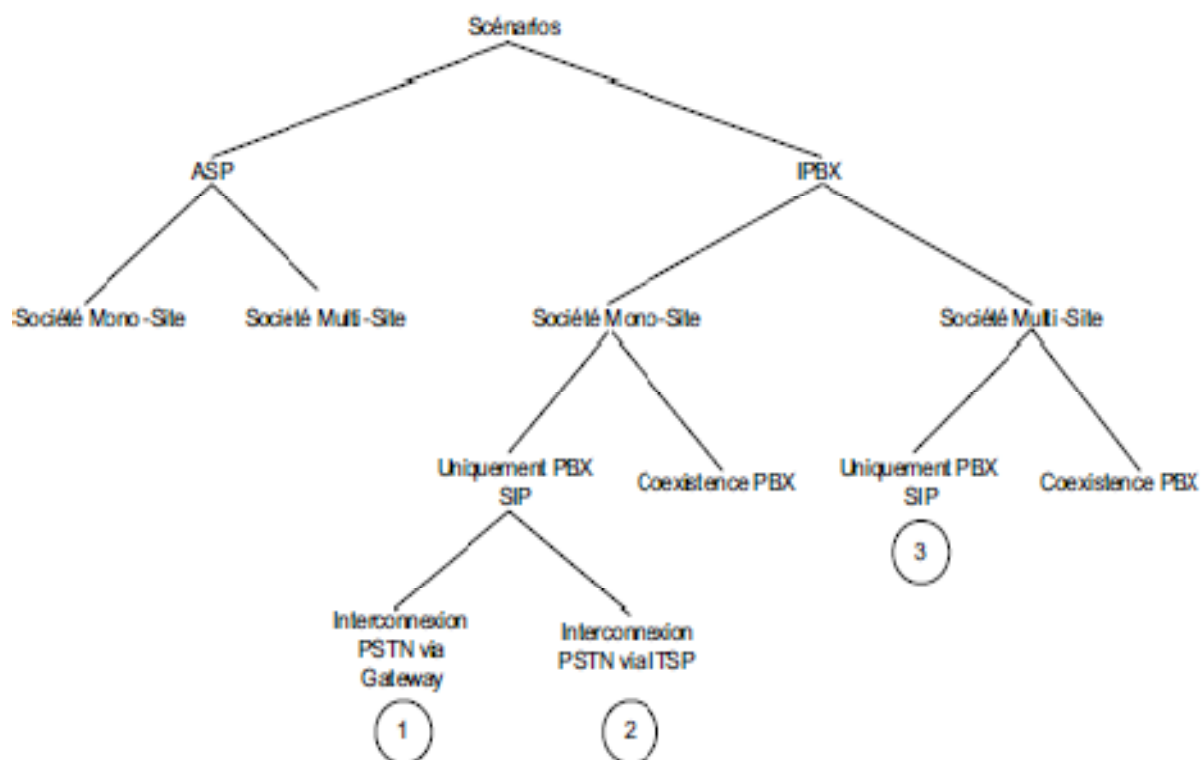


Figure 34 : Les architectures du call center

Un **deuxième niveau** distingue les centres d'appels mono-site et multi-site. Bien que les emplacements individuels d'une entreprise multi-site puissent souvent être traités comme un cas mono-site, on ajoute les problèmes supplémentaires de la communication entre les sites et le plan de numérotation local. Il est aussi possible que certains sites utilisent des services VoIP qui ne sont pas implémentés en local, mais qui sont utilisés depuis d'autres sites (typiquement le site principal). Ce cas dans le scénario ASP multi-site n'est pas significatif, car les services relatifs aux services de téléphonie sont fournis par le *provider* lui-même.

Finalement, parmi les centres d'appels qui possèdent leur IPBX, nous distinguons ceux qui avaient un système de téléphonie avec PBX, et qui l'ont gardé pour ne faire qu'une migration partielle vers la VoIP, et ceux qui n'utilisent plus que la VoIP. Pour ces derniers, il subsiste la question de la communication vers l'extérieur, qui peut se faire soit via un *gateway* vers le PSTN, soit par IP via un ITSP (*Internet Telephony Service Provider*).

De la figure ci-dessus, nous conservons 3 scénarios marqués par un cercle.

I.2. Scénarios:

Les 3 scénarios suivants nous semblent représentatifs des architectures utilisées aujourd'hui.

I.2.1. Call center mono-site avec son propre IPBX, utilisant un *gateway* vers le PSTN pour ses communications vers l'extérieur:

Dans cette situation, le centre d'appels communique en interne via VoIP, mais ne désire pas que ses communications passent par *internet*. Le *firewall+NAT* et l'*internet* montrés ici ne concernent donc que les données traditionnelles, et non les données VoIP. Toute communication entrante ou sortante passe donc via le *gateway* sur le PTSN.

Scénario 1 : Entreprise mono -site avec son propre IPBX , utilise un Gateway PSTN pour ses communications externes

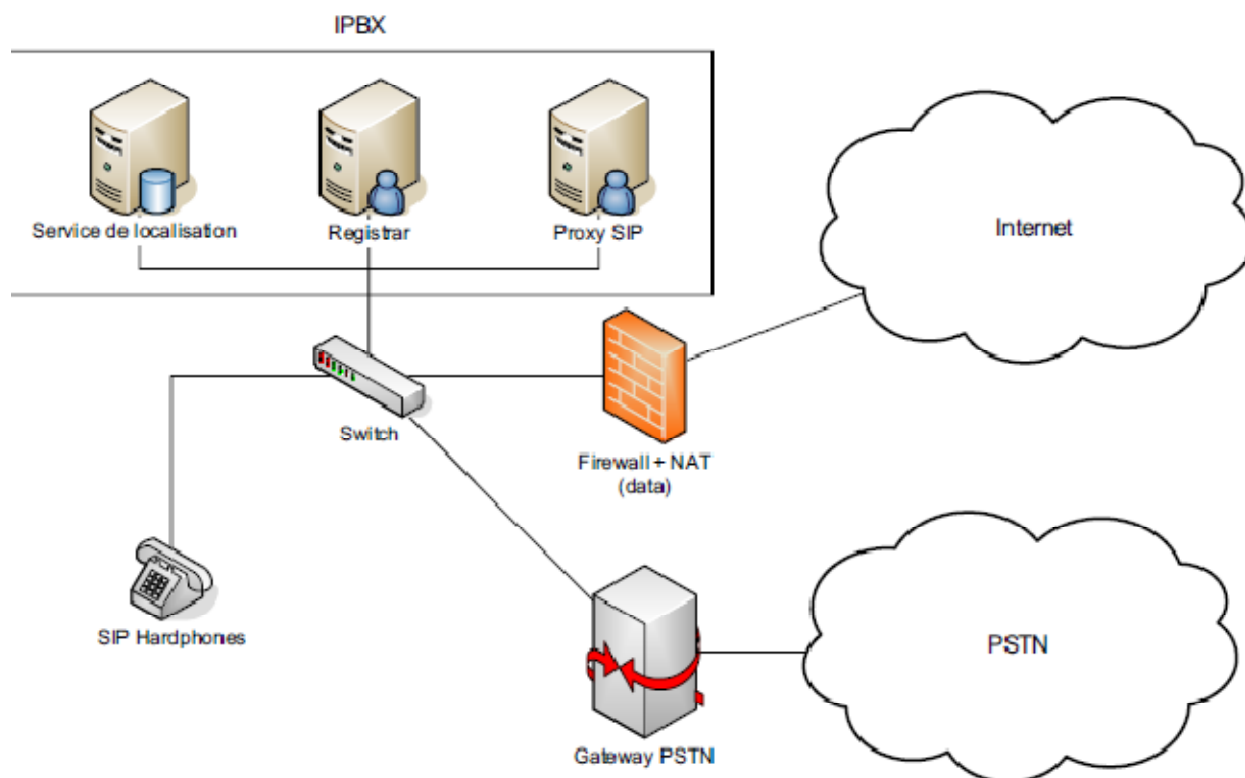


Figure 35 : Architecture call center du premier scenario

Cette situation est un bon exemple pour un centre d'appels qui désire profiter de la VoIP avec une communication gratuite au sein de ce dernier, mais sans faire passer ses communications VoIP sur *internet*. L'avantage réside dans le fait que les conversations ne peuvent pas se faire intercepter en dehors du réseau du centre, et qu'il ait un contrôle total sur la sécurité de ses communications. Par contre l'utilisation d'un *gateway* présente quelques risques (comme le vol de service ou le *toll fraud*).

I.2.2. Call center mono-site avec son propre IPBX, utilisant un ITSP pour ses communications vers l'extérieur :

L'entreprise maintient tous les services VoIP locaux dans le centre d'appels, mais fait partir toutes les communications sortantes vers un ITSP (c'est le proxy SIP qui s'en occupe). Cet ITSP devra prendre des décisions de routage, c'est-à-dire décider si le trafic doit continuer à passer sur *internet* ou bien passer sur le PSTN. Pour des raisons de haute disponibilité, l'entreprise peut disposer de serveurs (*proxy*, *registrar* et service de localisation) redondants.

Scénario 2 : Entreprise mono -site avec son propre IPBX , mais utilise un ITSP pour ses communications externes

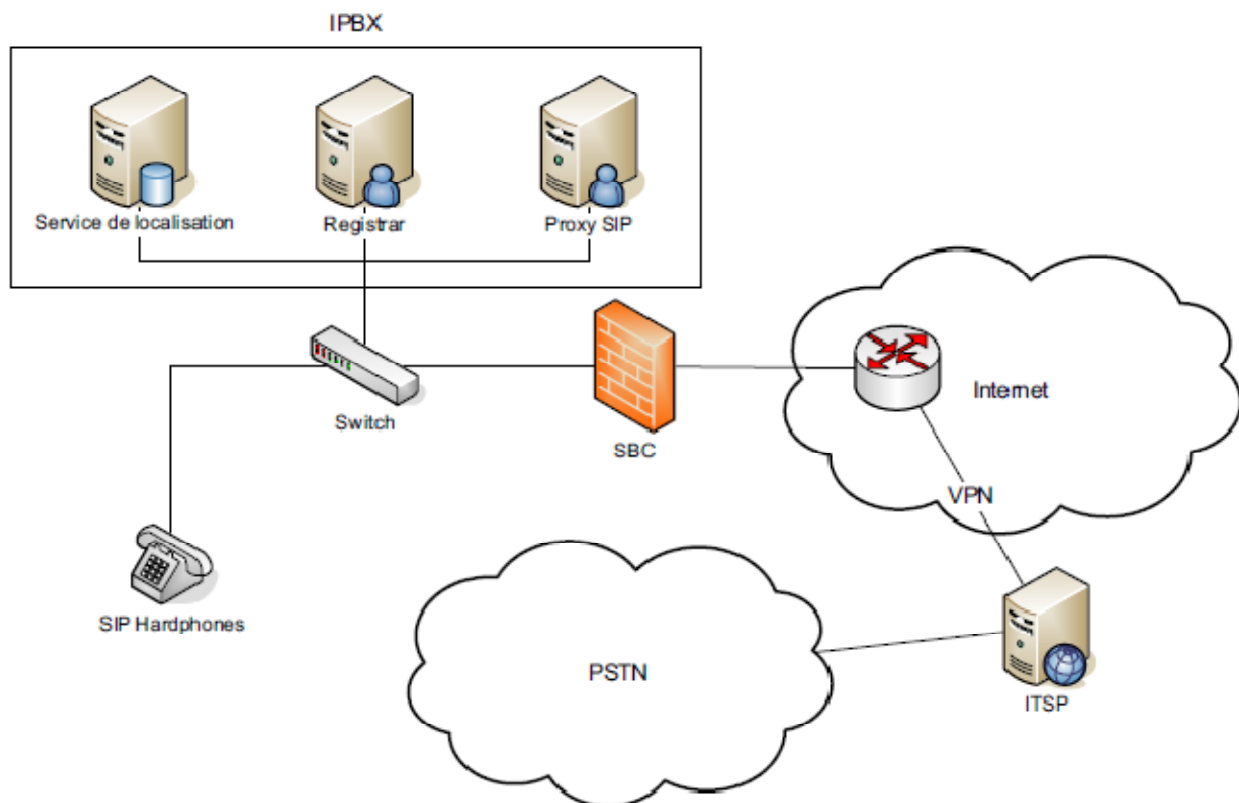


Figure 36 : Architecture call center du deuxième scénario

Le facteur prix est un argument essentiel pour les centres d'appels qui désirent *router* leur communication VoIP via *internet*. Utiliser un ITSP peut réduire le coût des communications vers l'extérieur. Mais ce choix a un inconvénient majeur dans la mesure où l'entreprise n'a aucun contrôle sur la sécurité et la QoS de ses communications entrantes et sortantes.

I.2.3. Call center multi-site avec un ou plusieurs IPBX, n'utilisant que SIP:

Une entreprise multi-site doit avoir une solution pour faire passer ses communications d'un site à l'autre. La solution retenue utilise un réseau privé virtuel VPN (*Virtual Private Network*). Etant donné qu'un SVPN (*Secure VPN*) dégrade la communication, d'autres solutions de VPN sont recommandés. On voit bien dans cet

exemple que certains sites doivent communiquer avec d'autre pour pouvoir utiliser certains services.

Scénario 3 : Entreprise multi -sites, certains sites doivent communiquer avec d'autres sites pour avoir accès à certains services (comme l'accès à l'extérieur)

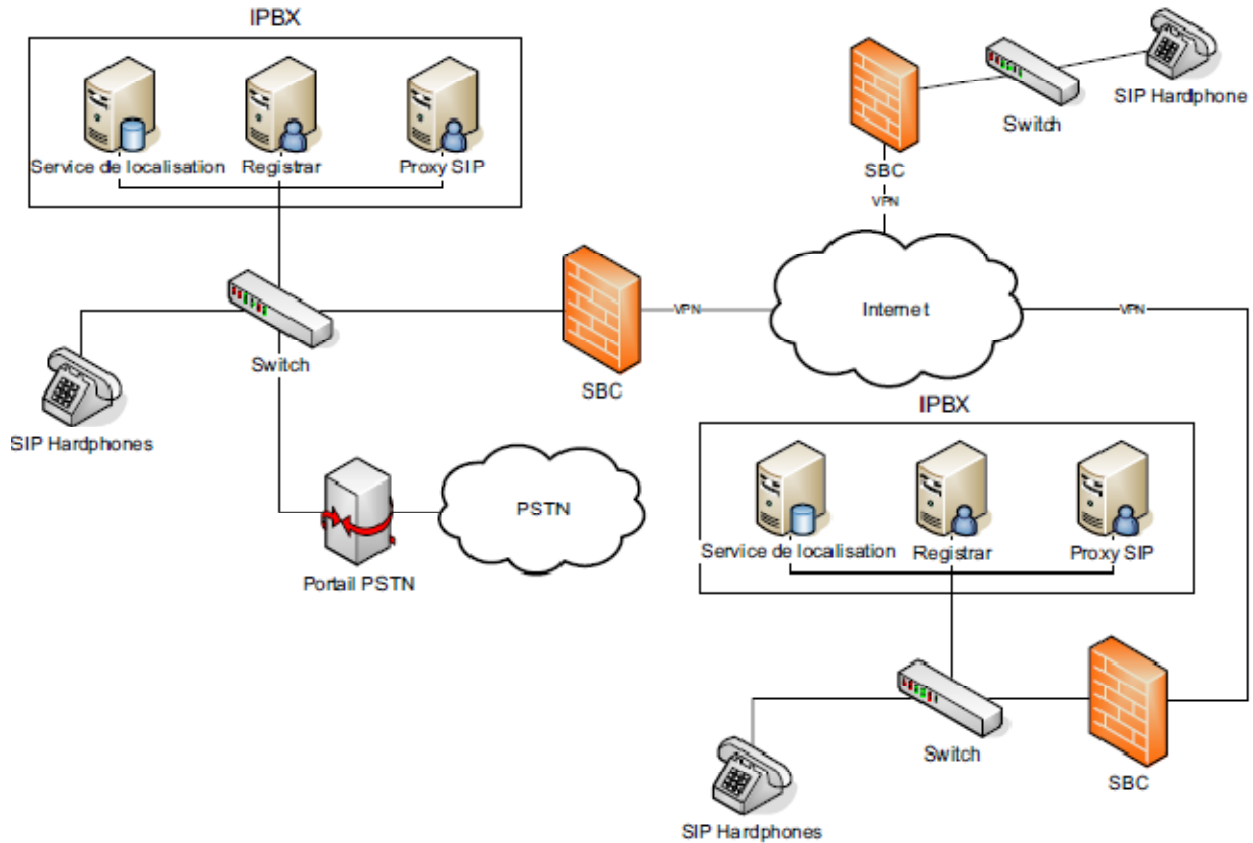


Figure 37 : Architecture call center du troisième scénario

Ce scénario est très similaire au premier étudié. Toutes les communications au sein de l'entreprise (quel que soit le site) sont gratuites, et il n'est pas nécessaire que tous les sites déploient du matériel coûteux pour profiter des différents services. De plus, si la communication inter-site est sécurisée, il n'y a pas plus de risque que dans un cas mono-site.

I.2.4. Services supplémentaires :

Le **softphone**, un téléphone SIP logiciel, est un élément problématique qu'on peut trouver dans certains réseaux. Il a le désavantage obligatoire de lier le réseau VoIP avec le réseau de données, et donc de rajouter toutes les vulnérabilités que l'on peut trouver dans un PC.

La **mobilité** va permettre à un employé (télétravailleur) d'utiliser le réseau téléphonique de l'entreprise via *internet* depuis chez lui ou encore depuis un hôtel alors qu'il est en déplacement. Cette communication doit être sécurisée, idéalement via VPN.

Des serveurs **ENUM**, de **redirection**, de **présence** ou de **conférence** peuvent être rajoutés dans des réseaux afin d'augmenter les fonctionnalités de la VoIP, ou permettre la messagerie instantanée. Le **voice-mail** ou le système de **réponse interactive** peut aussi être rajouté, mais ils ne sont pas nécessairement rajoutés au système VoIP. Il est possible pour un système qui utilise toujours un PBX que ces services y soient connectés.

Les services tels que **DNS**, **DHCP** et **NTP** ne peuvent être partagés avec le réseau DATA. Ils doivent posséder leurs propres serveurs sur le réseau VoIP .

Des serveurs **STUN** ou **TURN** peuvent être utilisés pour traverser le firewall et le NAT. Ces serveurs se situent hors du réseau protégé et risquent d'introduire de nouvelles vulnérabilités dans le réseau.

De manière générale il est recommandé d'avoir une certaine **redondance**. Ainsi il est possible qu'une entreprise dispose de plusieurs alternatives de transmission vers l'extérieur, ou même plusieurs *providers* en cas de problème. C'est aussi possible qu'une entreprise ait un *gateway* de secours en cas de panne pour pouvoir joindre les services d'urgence.

II. Attaques contre la VoIP et bonnes pratiques de sécurisation :

II.1. Attaques sur le protocole :

Un appel téléphonique VoIP est constitué de deux parties : la signalisation, qui instaure l'appel, et les flux de media, qui transporte la voix.

La signalisation, en particulier SIP, transmet les entêtes et la charge utile (Payload) du paquet en texte clair, ce qui permet à un attaquant de lire et falsifier facilement les paquets. Elle est donc vulnérable aux attaques qui essaient de voler ou perturber le service téléphonique, et à l'écoute clandestine qui recherche des informations sur un compte utilisateur valide, pour passer des appels gratuits par exemple. La signalisation utilise, en général, le port par défaut UDP/TCP 5060. Le firewall doit être capable d'inspecter les paquets de signalisation et ouvrir ce port afin de leur autoriser l'accès au réseau. Un firewall qui n'est pas compatible aux protocoles de la VoIP doit être configuré manuellement pour laisser le port 5060 ouvert, créant un trou pour des attaques contre les éléments qui écoutent l'activité sur ce port.

Le protocole RTP, utilisé pour le transport des flux multimédia, présente également plusieurs vulnérabilités dues à l'absence d'authentification et de chiffrement. Chaque entête d'un paquet RTP contient un numéro de séquence qui permet au destinataire de reconstituer les paquets de la voix dans l'ordre approprié.

Cependant, un attaquant peut facilement injecter des paquets artificiels avec un numéro de séquence plus élevé. En conséquence, ces paquets seront diffusés à la place des vrais paquets.

Généralement, les flux multimédias contournent les serveurs proxy et circulent directement entre les points finaux. Les menaces habituelles contre le flux de la voix sont l'interruption de transport et l'écoute clandestine.

Les protocoles de la VoIP utilisent TCP et UDP comme moyen de transport et par

conséquent sont aussi vulnérables à toutes les attaques contre ces protocoles, telles le détournement de session (TCP) (session Hijacking) et la mystification (UDP) (Spoofing), etc. Les types d'attaques les plus fréquentes contre un system VoIP sont :

II.1.1. Sniffing :

Un reniflage (Sniffing) peut avoir comme conséquence un vol d'identité et la révélation d'informations confidentielles. Il permet également aux utilisateurs malveillants perfectionnés de rassembler des informations sur les systèmes VoIP. Ces informations peuvent par exemple être employées pour mettre en place une attaque contre d'autres systèmes ou données.

Plusieurs outils requis pour le sniffing, y compris pour le protocole H.323 et des plugins SIP, sont disponibles en open source.

II.1.2. Suivre des appels :

Appelé aussi Call tracking, cette attaque se fait au niveau du réseau LAN/VPN et cible les terminaux (soft/hard phone). Elle a pour but de connaître qui est en train de communiquer et quelle est la période de la communication. L'attaquant doit récupérer les messages INVITE et BYE en écoutant le réseau et peut ainsi savoir qui communique, à quelle heure, et pendant combien de temps.

Pour réaliser cette attaque, L'attaquant doit être capable d'écouter le réseau et récupérer les messages INVITE et BYE.

II.1.3. Injection de paquet RTP :

Cette attaque se fait au niveau du réseau LAN/VPN. Elle cible le serveur registrar, et a pour but de perturber une communication en cours.

L'attaquant devra tout d'abord écouter un flux RTP de l'appelant vers l'appelé, analyser son contenu et générer un paquet RTP contenant un en-tête similaire mais avec un plus grand numéro de séquence et timestamp afin que ce paquet soit reproduit avant les autres paquets (s'ils sont vraiment reproduits). Ainsi la communication sera perturbée et l'appel ne pourra pas se dérouler correctement.

Pour réaliser cette attaque, l'attaquant doit être capable d'écouter le réseau afin de repérer une communication et ainsi repérer les timestamps des paquets RTP.

Il doit aussi être capable d'insérer des messages RTP qu'il a généré ayant un timestamp modifié.

II.1.4. Les Spam :

Trois formes principales de spams sont jusqu'à maintenant identifiés dans SIP:

- **Call Spam** : Ce type de spam est défini comme une masse de tentatives d'initiation de session (des requêtes INVITE) non sollicitées.

Généralement c'est un UAC (User Agent Client) qui lance, en parallèle, un grand nombre d'appels. Si l'appel est établi, l'application génère un ACK, rejoue une annonce préenregistrée, et ensuite termine l'appel.

- **IM (Instant Message) Spam** : Ce type de spam est semblable à celui de l'e-mail.

Il est défini comme une masse de messages instantanés non sollicités. Les IM spams sont pour la plupart envoyés sous forme de requête SIP. Ce pourraient être des requêtes INVITE avec un entête « Subject » très grand, ou des requêtes INVITE avec un corps en format texte ou HTML.

Bien-sûr, l'IM spam est beaucoup plus intrusif que le spam email, car dans les systèmes actuels, les IMs apparaissent automatiquement sous forme de pop-up à l'utilisateur.

- **Presence Spam** : Ce type de spam est semblable à l'IM spam. Il est défini comme une masse de requêtes de présence (des requêtes SUBSCRIBE) non sollicités. L'attaquant fait ceci dans le but d'appartenir à la " white list " d'un utilisateur afin de lui envoyer des messages instantanés ou d'initier avec lui d'autres formes de communications. L'IM Spam est différent du Presence Spam dans le fait que ce dernier ne transmet pas réellement de contenu dans les messages.

II.1.5. Le déni de service (DOS : Denial of service)

C'est, d'une manière générale, l'attaque qui vise à rendre une application informatique ou un équipement informatique incapable de répondre aux requêtes de ses utilisateurs et donc hors d'usage.

Une machine serveur offrant des services à ses clients (par exemple un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier, pour des raisons délibérément provoquées par un tiers, il y a déni de service.

Dans une attaque de type DoS flood attack, les ressources d'un serveur ou d'un réseau sont épuisées par un flot de paquets. Un seul attaquant visant à envoyer un flot de paquets peut être identifié et isolé assez facilement. Cependant l'approche de choix pour les attaquants a évolué vers un déni de service distribué (DDoS). Une attaque DDoS repose sur une distribution d'attaques DoS, simultanément menées par plusieurs systèmes contre un seul. Cela réduit le temps nécessaire à l'attaque et amplifie ses effets. Dans ce type d'attaque les pirates se dissimulent parfois grâce à des machines-rebonds (ou machines zombies), utilisées à l'insu de leurs propriétaires. Un ensemble de machines-rebonds, est contrôlable par un pirate après infection de chacune d'elles par un programme de type porte dérobée (backdoor).

Une attaque de type DoS peut s'effectuer à plusieurs niveaux soit :

a. Couche réseau :

- ❖ **IP Flooding** : Le but de l'IP Flooding est d'envoyer une multitude de paquets IP vers une

même destination de telle sorte que le traitement de ces paquets empêche une entité du réseau (un routeur ou la station destinatrice) de traiter les paquets IP légitimes. Si l'IP Flooding est combiné à l'IP Spoofing, il est impossible, pour le destinataire, de connaître l'adresse source exacte des paquets IP. De ce fait, à moins que le destinataire ne limite ses échanges avec certaines stations, il lui est impossible de contrer ce type d'attaques.

❖ **Fragmentation des paquets IP** : Par la fragmentation des paquets, il est possible de rendre hors service de nombreux systèmes d'exploitation et dispositif VoIP par le biais de la consommation des ressources. Il existe de nombreuses variantes d'attaques par fragmentation, parmi les plus populaires teardrop, opentear, nestea, jolt, boink, et Ping of death.

b. Couche transport :

❖ **L'UDP Flooding Attacks** : Le principe de cette attaque est qu'un attaquant envoie un grand nombre de requêtes UDP vers une machine. Le trafic UDP étant prioritaire sur le trafic TCP, ce type d'attaque peut vite troubler et saturer le trafic transitant sur le réseau et donc perturber de plus la bande passante. Presque tous les dispositifs utilisant le protocole SIP fonctionnent au dessus du protocole UDP, ce qui fait d'eux des cibles. De nombreux dispositifs de VoIP et de systèmes d'exploitation peuvent être paralysés grâce à des paquets UDP Flooding visant l'écoute du port SIP (5060) ou d'autres ports.

❖ **TCP SYN floods** est une attaque visant le protocole TCP et plus exactement la phase d'établissement de connexion. Celle-ci consiste en trois sous-étapes :

1. Le client envoie un paquet SYN au serveur.
2. Le serveur répond avec un paquet SYN-ACK.
3. Le client envoie un paquet ACK au serveur.

L'attaque consiste en l'envoi d'un grand nombre de paquets SYN. La victime va alors répondre par un message SYN-ACK d'acquittement. Pour terminer la connexion TCP, la victime va ensuite attendre pendant une période de temps la réponse par le biais d'un paquet ACK. C'est là le cœur de l'attaque parce que les ACK finaux ne sont jamais envoyés, et par la suite, la mémoire système se remplit rapidement et consomme toutes les ressources disponibles à ces demandes non valides. Le résultat final est que le serveur, le téléphone, ou le routeur ne sera pas en mesure de faire la distinction entre les faux SYN et les SYN légitimes d'une réelle connexion VoIP.

c. Couche applications :

❖ **SIP Flooding** : Dans le cas de SIP, une attaque DoS peut être directement dirigée contre les utilisateurs finaux ou les dispositifs tels que téléphones IP, routeurs et proxy SIP, ou

contre les serveurs concernés par le processus, en utilisant le mécanisme du protocole SIP ou d'autres techniques traditionnelles de DoS.

Voyons maintenant en détail les différentes formes d'attaque DoS :

❖ CANCEL

C'est un type de déni de service lancé contre l'utilisateur. L'attaquant surveille l'activité du proxy SIP et attend qu'un appel arrive pour un utilisateur spécifique. Une fois que le dispositif de l'utilisateur reçoit la requête INVITE, l'attaquant envoie immédiatement une requête CANCEL. Cette requête produit une erreur sur le dispositif de l'appelé et termine l'appel. Ce type d'attaque est employé pour interrompre la communication.

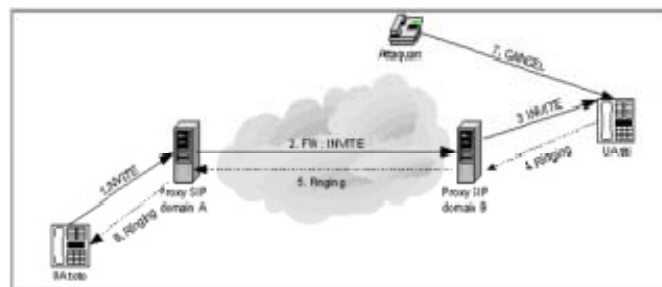


Figure 38 : Attaque DoS via une requête CANCEL

La figure suivante montre un scénario d'attaque DoS CANCEL, l'utilisateur toto initie l'appel, envoie une invitation (1) au proxy auquel il est rattaché. Le proxy du domaine A achemine la requête (2) au proxy qui est responsable de l'utilisateur titi. Ensuite c'est le proxy du domaine B qui prend le relais et achemine la requête INVITE (3) qui arrive enfin à destination.

Le dispositif de titi, quand il reçoit l'invitation, sonne (4). Cette information est réacheminée jusqu'au dispositif de toto. L'attaquant qui surveille l'activité du proxy SIP du domaine B envoie une requête CANCEL (7) avant que titi n'ait pu envoyer la réponse OK qui accepte l'appel.

Cette requête annulera la requête en attente (l'INVITE), l'appel n'a pas lieu.

❖ REGISTER

Le serveur d'enregistrement lui-même est une source potentielle de déni de service pour les utilisateurs. En effet ce serveur peut accepter des enregistrements de tous les dispositifs. Un nouvel enregistrement avec une «*» dans l'entête remplacera tous les précédents enregistrements pour ce dispositif. Les attaquants, de cette façon, peuvent supprimer l'enregistrement de quelques-uns des utilisateurs, ou tous, dans un domaine, empêchant ainsi ces utilisateurs d'être invités à de nouvelles sessions.

Notez que cette fonction de suppression d'enregistrement d'un dispositif au profit d'un autre est un comportement voulu en SIP afin de permettre le transfert d'appel. Le dispositif de l'utilisateur doit pouvoir devenir le dispositif principal quand il vient en ligne. C'est un mécanisme très pratique pour les utilisateurs mais également pour les pirates.

II.1.6. Détournement d'appel (Call Hijacking) :

Le Call Hijacking consiste à détourner un appel. Plusieurs fournisseurs de service VoIP utilisent le web comme interface permettant à l'utilisateur d'accéder à leur système téléphonique.

Un utilisateur authentifié peut changer les paramètres de ses transferts d'appel à travers cette interface web. C'est peut être pratique, mais un utilisateur malveillant peut utiliser le même moyen pour mener une attaque.

Exemple: quand un agent SIP envoie un message INVITE pour initier un appel, l'attaquant envoie un message de redirection 3xx indiquant que l'appelé s'est déplacé et par la même occasion donne sa propre adresse comme adresse de renvoi. A partir de ce moment, tous les appels destinés à l'utilisateur sont transférés et c'est l'attaquant qui les reçoit.

Un appel détourné en lui-même est un problème, mais c'est encore plus grave quand il est porteur d'informations sensibles et confidentielles.

II.1.7. L'écoute clandestine :

L'eavesdropping est l'écoute clandestine d'une conversation téléphonique. Un attaquant avec un accès au réseau VoIP peut sniffer le trafic et décoder la conversation vocale. Des outils tels que VOMIT (Voice Over Misconfigured Internet Telephones) permettent de réaliser cette attaque. VOMIT convertit les paquets sniffés en fichier .wav qui peut être réécouté avec n'importe quel lecteur de fichiers son.

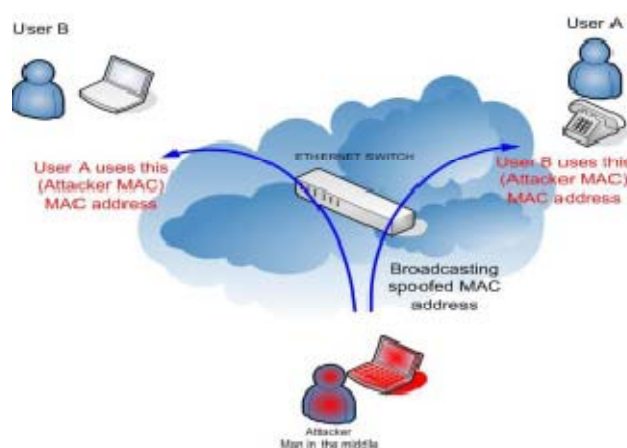


Figure 39 : Exemple de détournement d'appel " Man in the middle"

Le principe de l'écoute clandestine est montré dans la figure 39 comme suit :

1. déterminer les adresses MAC des victimes (client serveur) par l'attaquant
2. Envoi d'une requête ARP non sollicités au client, pour l'informer du changement de

l'adresse MAC du serveur VoIP à l'adresse MAC.

3. Envoi d'une requête ARP non sollicitée au serveur, pour l'informer du changement de l'adresse MAC du client à l'adresse MAC.

4. Désactiver la vérification des adresses MAC sur la machine d'attaque afin que le trafic puisse circuler entre les 2 victimes

II.2. Les vulnérabilités de l'infrastructure :

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs (proxy, register, etc.). Chaque élément, que ce soit un système embarqué ou un serveur standard tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur.

Chacun comporte un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde.

II.2.1. Faiblesses dans la configuration des dispositifs de la VOIP :

Plusieurs dispositifs de la VoIP, dans leur configuration par défaut, peuvent avoir une variété de ports TCP et UDP ouverts. Les services fonctionnant sur ces ports peuvent être vulnérables aux attaques DoS ou buffer overflow.

Plusieurs dispositifs de la VoIP exécutent également un serveur WEB pour la gestion à distance qui peut être vulnérable aux attaques buffer overflow et à la divulgation d'informations.

Si les services accessibles ne sont pas configurés avec un mot de passe, un attaquant peut acquérir un accès non autorisé à ce dispositif.

Les services SNMP (Simple Network Management Protocol) offerts par ces dispositifs peuvent être vulnérables aux attaques de reconnaissance ou attaques d'overflow.

Plusieurs dispositifs de la VoIP sont configurés pour télécharger périodiquement un fichier de configuration depuis un serveur par TFTP ou d'autres mécanismes. Un attaquant peut potentiellement détourner ou mystifier cette connexion et tromper le dispositif qui va télécharger un fichier de configuration malveillant à la place du véritable fichier.

II.2.2. Les téléphones IP :

Un pirate peut compromettre un dispositif de téléphonie sur IP, par exemple un téléphone IP, un softphone et autres programmes ou matériels clients. Généralement, il obtient les privilèges qui lui permettent de commander complètement la fonctionnalité du dispositif. Compromettre un point final (téléphone IP) peut être fait à distance ou par un accès physique au dispositif. Le pirate pourrait modifier les aspects opérationnels d'un tel dispositif:

La pile du système d'exploitation peut être changée. Ainsi la présence de l'attaquant ne

sera pas remarquée.

Aussi un firmware modifié de manière malveillante peut être téléchargé et installé. Les modifications faites à la configuration des logiciels de téléphonie IP peuvent permettre:

- ❖ Aux appels entrants d'être réorientés vers un autre point final sans que l'utilisateur soit au courant.
- ❖ Aux appels d'être surveillés.
- ❖ A l'information de la signalisation et/ou les paquets contenant de la voix d'être routés vers un autre dispositif et également d'être enregistrés et/ou modifiés.

De compromettre la disponibilité du point final. Par exemple, ce dernier peut rejeter automatiquement toutes les requêtes d'appel, ou encore, éliminer tout déclenchement de notification tel qu'un son, une notification visuelle à l'arrivée d'un appel. Les appels peuvent également être interrompus à l'improviste (quelques téléphones IP permettent ceci via une interface web).

D'autres conséquences possibles sont:

- ❖ Des backdoors pourraient être installés.
- ❖ Toutes les informations concernant l'utilisateur qui sont stockées sur le dispositif pourraient être extraites.

L'acquisition d'un accès non autorisé sur un dispositif de téléphonie IP peut être le résultat d'un autre élément compromis sur le réseau IP, ou de l'information récoltée sur le réseau.

Les softphones ne réagissent pas de la même façon aux attaques comparés à leur homologues téléphones IP. Ils sont plus susceptibles aux attaques dues au nombre de vecteurs inclus dans le système, à savoir les vulnérabilités du système d'exploitation, les vulnérabilités de l'application, les vulnérabilités du service, des vers, des virus, etc. En plus, le softphone demeure sur le segment de données, est ainsi sensible aux attaques lancées contre ce segment et pas simplement contre l'hôte qui héberge l'application softphone.

Les téléphones IP exécutent quant à eux leurs propres systèmes d'exploitation avec un nombre limité de services supportés et possèdent donc moins de vulnérabilités.

II.2.3. Les serveurs :

Un pirate peut viser les serveurs qui fournissent le réseau de téléphonie sur IP.

Compromettre une telle entité mettra généralement en péril tout le réseau de téléphonie dont le serveur fait partie.

Par exemple, si un serveur de signalisation est compromis, un attaquant peut contrôler totalement l'information de signalisation pour différents appels. Ces informations sont routées à travers le serveur compromis. Avoir le contrôle de l'information de signalisation permet à un attaquant de changer n'importe quel paramètre relatif à l'appel.

Si un serveur de téléphonie IP est installé sur un système d'exploitation, il peut être une cible pour les virus, les vers, ou n'importe quel code malveillant.

II.2.4 Les vulnérabilités du système d'exploitation :

Ces vulnérabilités sont pour la plupart relatives au manque de sécurité lors de la phase initiale de développement du système d'exploitation et ne sont découvertes qu'après le lancement du produit.

Une des principales vulnérabilités des systèmes d'exploitation est le buffer overflow. Il permet à un attaquant de prendre le contrôle partiel ou complet de la machine.

Les dispositifs de la VoIP tels que les téléphones IP, Call Managers, Gateway et les serveurs proxy, héritent les mêmes vulnérabilités du système d'exploitation ou du firmware sur lequel ils tournent.

Il existe une centaine de vulnérabilités exploitables à distance sur Windows et même sur Linux. Un grand nombre de ces exploits sont disponibles librement et prêts à être téléchargés sur l'Internet.

Peu importe comment, une application de la VoIP s'avère être sûre, celle ci devient menacé si le système d'exploitation sur lequel elle tourne est compromis.

III. Sécurisation et bonne pratiques :

On déjà vu que les vulnérabilités existe au niveau protocolaire, application et systèmes d'exploitation. Pour cela, on a découpé la sécurisation aussi en trois niveaux : Sécurisation protocolaire, sécurisation de l'application et sécurisation du système de l'exploitation.

III.1. Sécurisation protocolaire :

La prévalence et la facilité de sniffer des paquets et d'autres techniques pour la capture des paquets IP sur un réseau pour la voix sur IP fait que le cryptage soit une nécessité. La sécurisation de la VoIP est à la protection des personnes qui sont interconnecté.

IPsec peut être utilisé pour réaliser deux objectifs. Garantir l'identité des deux points terminaux et protéger la voix une fois que les paquets quittent l'Intranet de l'entreprise. VOIPsec (VoIP utilisant IPsec) contribue à réduire les menaces, les sniffeurs de paquets, et de nombreux types de trafic « vocal analyze ». Combiné avec un pare-feu, IPsec fait que la VOIP soit plus sûr qu'une ligne téléphonique classique. Il est important de noter, toutefois, que IPsec n'est pas toujours un bon moyen pour certaines applications, et que certains protocoles doivent continuer à compter sur leurs propres dispositifs de sécurité.

➤ **VoIP VPN**

Un VPN VoIP combine la voix sur IP et la technologie des réseaux virtuels privés pour offrir une méthode assurant la préservation de la prestation vocale. Puisque la VoIP transmet la voix numérisée en un flux de données, la solution VPN VoIP semble celle la plus approprié vu qu'elle offre le cryptage des données grâce a des mécanismes de cryptages, puisqu'elle permet d'offrir l'intégrité des paquets VoIP.

III.2. Cryptage aux points terminaux :

Vu que notre objectif est d'assurer la confidentialité et l'intégrité des clients, le mode choisie est donc le mode tunnel. Puisqu'il sécurise le paquet comme un tout (contrairement en mode transport qui ne sécurise que le payload IP). Le mode tunnel se base sur l'encapsulation de tout le paquet IP et ajoute un nouvel entête pour l'acheminement de ce dernier. Ce mode est généralement utilisé pour les routeur-to-routeur. En plus du mode tunnel, on choisi le protocole ESP qui lui a son tour va assurer le cryptage des données et donc la confidentialité contrairement au protocole AH qui lui ne permet que l'authentification des paquets et non le cryptage.

Dans ce cas, la solution qu'on propose est ESP mode tunnel qui sera appliqué uniquement sur les points de terminaison à la voix IP, c'est-à-dire le routeur. Ceci nous permettra donc de minimiser le nombre de machines qui seront impliquées dans le traitement engendré par la sécurité. De plus le nombre des clés nécessaires sera réduit.

➤ *Secure RTP ou SRTP*

SRTP est conçu pour sécuriser la multiplication à venir des échanges multimédias sur les réseaux. Il couvre les lacunes de protocoles de sécurité existants comme IPsec (IP Security), dont le mécanisme d'échanges de clés est trop lourd. Il aussi est bâti sur le protocole temps réel RTP (Real Time Transport Protocol). Il associe aussi une demi-douzaine de protocoles complémentaires. Il est donc compatible à la fois avec des protocoles d'initiation de session de voix sur IP tel que SIP (Session Initiation Protocol), ainsi que le protocole de diffusion de contenu multimédia en temps réel RTSP (Real Time Streaming Protocol). Mais, surtout, il s'adjoit les services du protocole de gestion de clé MIKEY (Multimedia Internet KEYing).

III.2.1. Service de sécurités offertes par SRTP :

Les principaux services offerts par SRTP sont :

- ❖ Rendre confidentielles les données RTP, que ce soit l'en-tête et la charge utile ou seulement la charge utile.
- ❖ Authentifier et vérifier l'intégrité des paquets RTP. L'émetteur calcule une empreinte du message à envoyer, puis l'envoie avec le message même.
- ❖ La protection contre le rejeu des paquets. Chaque récepteur tient à jour une liste de tous les indices des paquets reçus et bien authentifiés.

a. Principe de fonctionnement de SRTP :

Avec une gestion de clé appropriée, SRTP est sécurisé pour les applications unicast et

multicast de RTP. En théorie, SRTP est une extension du protocole RTP dans lequel a été rajoutée des options de sécurité. En effet, il a pour but d'offrir plusieurs implémentations de cryptographie tout en limitant l'overhead lié à l'utilisation des chiffrements. Il propose des algorithmes qui monopoliseront au minimum les ressources et l'utilisation de la mémoire. Surtout, il permet de rendre RTP indépendant des autres couches en ce qui concerne l'application de mécanismes de sécurité.

Pour implémenter les différents services de sécurité précités, SRTP utilise les composants principaux suivants :

- ❖ **Une clé maîtresse** utilisée pour générer des clés de session; Ces dernières seront utilisées pour chiffrer ou pour authentifier les paquets.

- ❖ **Une fonction** utilisée pour calculer les clés de session à partir de la clé maîtresse.

Des clés aléatoires utilisées pour introduire une composante aléatoire afin de contrer les éventuels rejets ou effets de mémoire.

SRTP utilise deux types de clés : clef de session et clef maîtresse. Par « clef de session » nous entendons une clef utilisée directement dans les transformations cryptographiques; et par « clef maîtresse », nous entendons une chaîne de bit aléatoire à partir desquelles les clefs de sessions sont dérivées par une voie sécurisé avec des mécanismes cryptographiques.

b. Format du paquet SRTP :

Un paquet SRTP est généré par transformation d'un paquet RTP grâce à des mécanismes de sécurité. Donc le protocole SRTP effectue une certaine mise en forme des paquets RTP avant qu'ils ne soient sur le réseau. La figure suivante présente le format d'un paquet SRTP

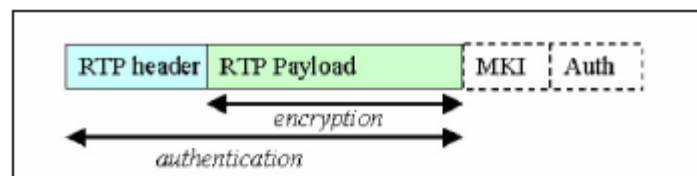


Figure 40 : Format d'un paquet SRTP

On remarque que le paquet SRTP est réalisé en rajoutant deux champs au paquet RTP :

- ❖ **SRTP MKI (SRTP Master Key identifier)** : sert à re-identifier une clef maîtresse particulière dans le contexte cryptographique. Le MKI peut être utilisé par le récepteur pour retrouver la clef primaire correcte quand le besoin d'un renouvellement de clefs survient.

- ❖ **Authentication tag** : est un champ inséré lorsque le message a été authentifié. Il est recommandé d'en faire usage. Il fournit l'authentification des en-têtes et données RTP et

indirectement fournit une protection contre le rejeu de paquets en authentifiant le numéro de séquence.

III.3.2. Sécurisation de l'application :

Plusieurs méthodes peuvent être appliquées pour sécuriser l'application, ces méthodes varient selon le type d'application (serveur ou client). Pour sécuriser le serveur il faut :

- L'utilisation d'une version stable, Il est bien connu que toute application non stable contient surement des erreurs et des vulnérabilités. Pour minimiser les risques, il est impératif d'utiliser une version stable.
- Tester les mises à jour des softwares dans un laboratoire de test. Il est très important de tester toute mise à jour de l'application dans un laboratoire de test avant de les appliquer sur le système en production
- Ne pas tester les correctifs sur le serveur lui-même:
- Ne pas utiliser la configuration par défaut qui sert juste à établir des appels. Elle ne contient aucune protection contre les attaques.
- Ne pas installer une application client dans le serveur.

Certains paramètres doivent être appliqués de manière sélective. Ces paramètres renforcent la sécurité de l'application, on peut les activer ou les interdire sur la configuration générale de l'application, comme on peut juste utiliser les paramètres nécessaires pour des clients bien déterminé et selon le besoin bien sûr. Ces paramètres protègent généralement contre le dénie de service et ces différentes variantes. Il est conseiller d'utiliser les paramètres qui utilise le hachage des mots de passe, et cela assure la confidentialité.

III.3.3. Sécurisation du système d'exploitation :

Il est très important de sécuriser le système sur lequel est implémenté le serveur de VoIP. En effet, si le système est compromis, l'attaque peut se propager sur l'application serveur. Celle-ci risque d'affecter les fichiers de configuration contenant des informations sur les clients enregistrés.

Il y a plusieurs mesures de sécurités à prendre pour protéger le système d'exploitation :

- utiliser un système d'exploitation stable. Les nouvelles versions toujours contiennent des bugs et des failles qui doivent être corrigés et maîtrisés avant.
- mettre à jour le système d'exploitation en installant les correctifs de sécurité recommandé pour la sécurité.
- Ne pas mettre des mots de passe simple et robuste. Ils sont fondamentaux contre les intrusions. Et ils ne doivent pas être des dates de naissances, des noms, ou des numéros de téléphones. Un mot de passe doit être assez long et former d'une combinaison de lettre, de chiffres et ponctuations.
- Ne pas exécuter le serveur VoIP avec un utilisateur privilège. Si un utilisateur malveillant arrive à accéder au système via une exploitation de vulnérabilité sur le serveur VoIP, il héritera tous les privilèges de cet utilisateur.

- Asterisk in CHROOT : empêcher le serveur VoIP d'avoir une visibilité complète de l'arborescence du disque, en l'exécutant dans un environnement sécurisé qui l'empêche d'interagir librement avec le système.
- Sauvegarde des fichiers log à distance : les fichiers log sont très importants, il est conseillé de les enregistrer sur un serveur distant.
- Installer seulement les composants nécessaires : pour limiter les menaces sur le système d'exploitation. Il vaut mieux installer sur la machine le système d'exploitation et le serveur.
- Supprimer tous programmes, logiciels ou des choses qui n'ont pas d'importance et qui peuvent être une cible d'attaque pour accéder au système.
- Renforcer la sécurité du système d'exploitation en installant des patches qui permettent de renforcer la sécurité générale du noyau.

On peut aussi utiliser les pare feu ou/et les ACL pour limiter l'accès à des personnes bien déterminé et fermer les ports inutiles et ne laisser que les ports utilisés (5060, 5061, 4569,...). Le pare feu (firewall) est un software ou hardware qui a pour fonction de sécuriser un réseau ou un ordinateur contre les intrusions venant d'autres machines. Le pare feu utilise le système de filtrage de paquet après analyse de l'entête des paquets IP qui s'échange entre les machines.

Le firewall peut être implémenté avec un ACL qui est une liste d'**Access Control Entry (ACE)** ou entrée de contrôle d'accès donnant ou supprimant des droits d'accès à une personne ou un groupe. On aura besoin d'ACL pour donner des droits à des personnes bien déterminés selon leurs besoins et leurs autorités.

Pour un serveur VoIP, il est important d'implémenter les ACL pour sécuriser le serveur en limitant l'accès à des personnes indésirables. Par exemple, seuls les agents enregistrés peuvent envoyer des requêtes au serveur. Il existe trois catégories d'ACL :

La liste de contrôle d'accès peut être installée en réseau sur les pare feu ou les routeurs, mais aussi ils existent dans les systèmes d'exploitation.

Conclusion :

La voix sur IP devient jour après jour plus ciblé. Il existe plusieurs autres attaques qui menace la sécurité du VoIP, celles citées dans ce chapitre sont les plus courantes . Mais en suivant certaines pratiques parmi les citées, on peut créer un réseau bien sécurisé.

Chapitre IV:

Interfaçage dans le réseau GSM

Introduction :

Etant donné le récent développement en téléphonie mobile, le budget en téléphonie des centres d'appels a augmenté de façon considérable. En effet, les appels passés à partir d'un réseau fixe vers un réseau mobile sont généralement plus chers que les appels entre deux réseaux mobiles, les passerelles GSM permettent d'économiser cette différence de prix.

De plus les demandes en appels internationaux bon marché de type VoIP sont de plus en plus importantes dans un centre d'appels. La passerelle de terminaison d'appels GSM VOIP est une solution alternative idéale pour les prestataires en terminaison d'appels vers des mobiles ou des fixes cherchant à accroître ou à diversifier leur activité.

mais avant d'en arriver à l'interconnexion du centre d'appels au réseau GSM, nous allons présenter brièvement ce dernier, nous aborderons son concept, son architecture et ses interfaces.

I. Définition

L'appellation GSM (Global System for Mobile Communications) regroupe deux types de réseaux cellulaires numériques de télécommunications pour abonnés mobiles :

- Le réseau GSM900 : il utilise des fréquences porteuses dans la gamme des 900 MHz et il a été le premier type de réseau mobile cellulaire numérique européen.
- Le réseau DCS1800 (Digital Cellular Telecommunications System) qui utilise des fréquences porteuses dans la gamme des 1800 MHz.

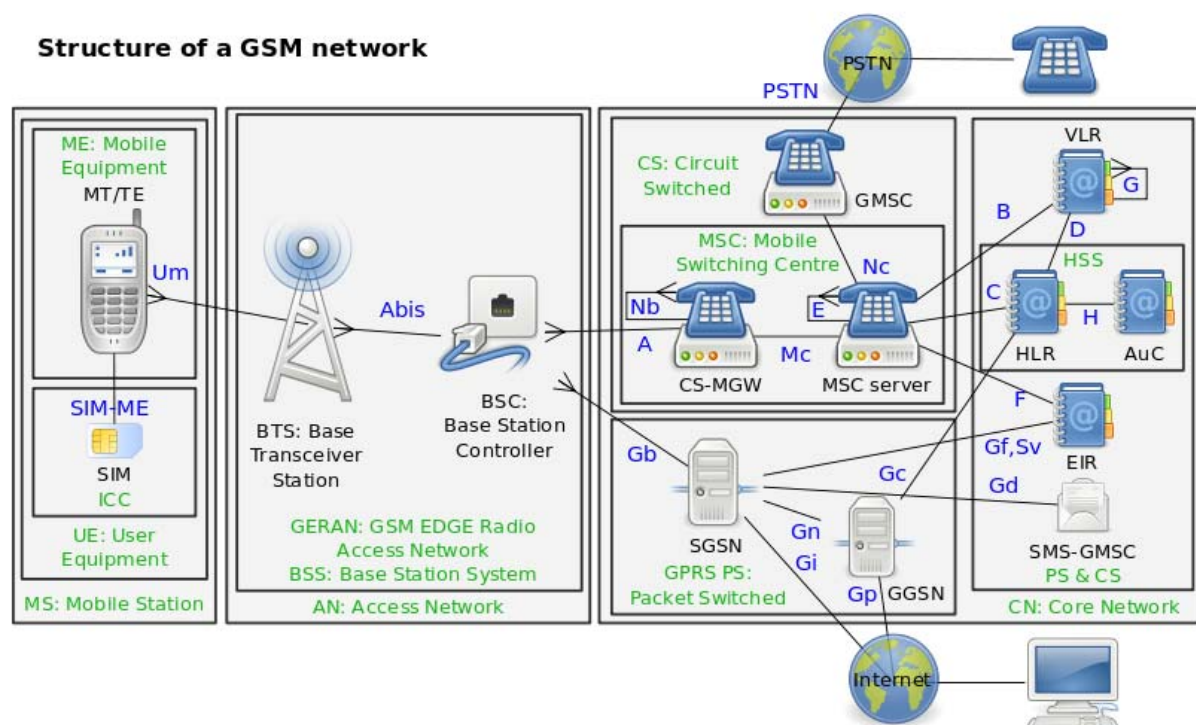


Figure 41 : Structure du réseau GSM

I.1. Architecture GSM

Pour que le système puisse offrir les services prévus, un ensemble de fonctions a été défini. Ces fonctions sont celles requises dans tout réseau mobile comme la numérotation, l'acheminement vers un usager mobile, le transfert de cellules, etc. Ces fonctions sont regroupées en entités fonctionnelles. Le système GSM est constitué des entités suivantes (Figure 42):

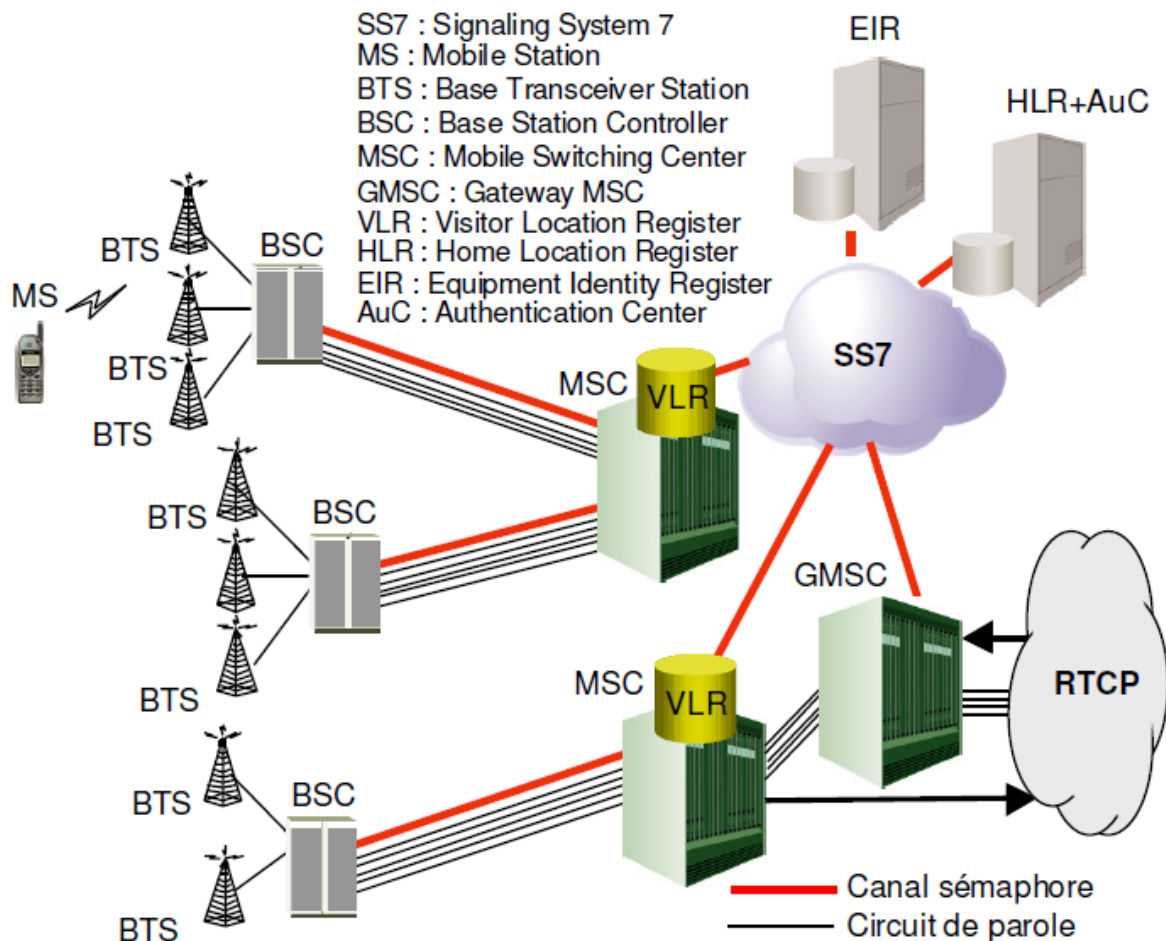


Figure 42 : Les entités du réseau GSM

I.1.1. Station Mobile (MS, Mobile Station) :

Le but d'un réseau GSM/DCS est d'offrir des services de télécommunication à des abonnés, quels que soient leurs déplacements à l'intérieur d'une zone de service, desservie par un opérateur ou éventuellement par plusieurs opérateurs ayant passé des accords mutuels. Pour ce faire, l'abonné mobile utilise une station mobile (MS, Mobile Station) qui est constituée de deux éléments séparables :

- Un équipement mobile qui fournit les capacités radio et logicielles nécessaires au

dialogue avec le réseau et demeure indépendant de l'abonné utilisateur.

- Une carte SIM (Subscriber Identification Module) qui contient les caractéristiques de l'abonné et de ses droits.

Lorsque la carte n'est pas présente dans le terminal, le seul service que peut accepter le réseau de la part de l'abonné mobile est le service d'urgence.

I.1.2. Sous-système Radio (BSS, Base Station Subsystem)

I.1.2.1. Base Transceiver Station (BTS)

La BTS (Base Transceiver Station) relie les stations mobiles à l'infrastructure fixe du réseau.

La BTS est composée d'un ensemble d'émetteur / récepteurs. Elle assure :

- La gestion du multiplexage temporel (une porteuse est divisée en 8 slots dont 7 sont alloués aux utilisateurs), et la gestion des sauts de fréquence.
- Des opérations de chiffrement.
- Des mesures radio permettant de vérifier la qualité de service ; ces mesures sont transmises directement au BSC.
- La gestion de la liaison de données (données de trafic et de signalisation) entre les mobiles et la BTS.
- La gestion de la liaison de trafic et de signalisation avec le BSC.

La capacité maximale typique d'une BTS est de 16 porteuses, soit 112 communications simultanées. En zone urbaine où le diamètre de couverture d'une BTS est réduit, cette capacité peut descendre à 4 porteuses soit 24 communications.

I.1.2.2. Base Station Controller (BTS)

Un BSC gère un ou plusieurs BTS et n'est relié qu'à un seul MSC. Pour le trafic abonné venant des BTS, le BSC joue le rôle de concentrateur. Pour le trafic venant du commutateur, il joue le rôle d'aiguilleur vers la BTS dont dépend le destinataire.

Un BSC utilise les mesures radio des BTS pour gérer la signalisation des "Handover" entre les cellules dont il a la responsabilité.

I.1.3. Sous-système réseau (NSS, Network Subsystem)

I.1.3.1. Mobile Switching Center (MSC)

Un MSC (Mobile Switching Center) est un commutateur qui réalise les fonctions de connexion et de signalisation pour les mobiles localisés dans une zone géographique appelée zone de localisation du MSC. La différence principale entre un MSC et un commutateur d'un réseau fixe est qu'un MSC doit prendre en compte l'impact de l'allocation des ressources radio aux mobiles et la mobilité des mobiles. Il doit posséder des ressources suffisantes pour réaliser au moins les procédures suivantes :

- Procédures pour l'enregistrement des localisations.
- Procédures requises pour les handovers.

Un MSC constitue l'interface entre le système radio et les réseaux fixes. Il réalise toutes les fonctions nécessaires à la mise en œuvre des appels de et vers les mobiles.

Dans la pratique, un MSC intègre les fonctionnalités d'un VLR.

I.1.3.2. Gateway MSC (GMSC)

Si le Réseau Téléphonique Commuté (RTC) doit router un appel vers un abonné mobile, l'appel est routé vers un MSC. Ce MSC interroge le HLR concerné, puis route l'appel vers le MSC sous lequel le mobile est localisé (il peut s'agir du même MSC). Un MSC qui reçoit un appel d'un autre réseau et qui assure le routage de cet appel vers la position de localisation d'un mobile est appelé Gateway MSC (GMSC).

I.1.3.3. Home Location Register (HLR)

Le HLR (Home Location Register) contient les informations relatives aux abonnés du réseau. Un réseau peut posséder plusieurs bases pour mettre en oeuvre le HLR en fonction des capacités de ces bases de données. Dans un HLR, chaque abonné est décrit par un enregistrement contenant le détail des options d'abonnement et des services complémentaires accessibles à l'abonné. A ces informations statiques se rajoutent des informations dynamiques telles que la dernière localisation connue du mobile (localisation permettant la taxation et le routage des appels vers le MSC sous lequel le mobile est localisé) et son état. Le HLR contient par ailleurs la clé secrète de l'abonné qui permet au service d'authentifier l'abonné. Cette clé est inscrite sous un format codé que seul l'AUC (Authentication Center) peut décrypter.

I.1.3.4. Visitor Location Register (VLR)

Le VLR (Visitor Location Register) est une base de données généralement associée à un commutateur MSC. Il est aussi possible de considérer un VLR partagé par plusieurs MSCs. Sa mission est d'enregistrer des informations dynamiques relatives aux abonnés actuellement connectés. Le réseau doit connaître à chaque instant la localisation des abonnés présents. Dans le VLR, chaque abonné est décrit en particulier par un identifiant et une localisation. Grâce à ces informations, le réseau est apte à acheminer un appel vers un abonné mobile. A chaque changement de zone de localisation d'un abonné, le VLR du MSC auquel est rattaché le mobile doit être mis à jour ainsi que l'enregistrement de cet abonné dans le HLR. Lorsqu'un appel doit être délivré, c'est le HLR qui est le premier interrogé afin de connaître la dernière localisation connue de l'abonné.

I.1.3.5. Authentication Center (AUC)

L'AUC (Authentication Center) est associé à un HLR et sauvegarde une clé d'identification pour chaque abonné mobile enregistré dans ce HLR. Cette clé est utilisée pour fabriquer :

- Les données nécessaires pour authentifier l'abonné dans le réseau GSM.
- Une clé de chiffrement de la parole (Kc) sur le canal radio entre le mobile et la partie fixe du réseau GSM.

L'AuC est une fonctionnalité généralement intégrée dans le HLR.

I.1.3.6. Equipment Identity Register (EIR)

Un EIR sauvegarde toutes les identités des équipements mobiles utilisés dans un réseau GSM. Cette fonctionnalité peut être intégrée dans le HLR.

Chaque poste mobile est enregistré dans l'EIR dans une liste :

- Liste "blanche" : poste utilisable sans restriction.
- Liste "grise" : poste sous surveillance (traçage d'appels).
- Liste "noire" : poste volé ou dont les caractéristiques techniques sont incompatibles, avec la qualité requise dans un réseau GSM (localisation non autorisée).

I.1.4. Le réseau d'exploitation et maintenance

Le réseau d'exploitation et maintenance comprend les centres d'exploitation maintenance (OMC : Operations and Maintenance Center) qui sont les entités fonctionnelles permettant à l'opérateur du réseau de contrôler son système. Un OMC-R (OMC-Radio) prend en charge la supervision et le contrôle d'un ensemble de BSC et BTS. Un OMC-S (OMC-Switching) permet de superviser et contrôler un ensemble de MSC/VLR. Au-delà des OMC-R et OMC-S, on peut trouver, si l'importance du réseau le justifie, un NMC (Network Management Centre) qui assure l'administration générale centralisée du réseau. Les fonctions suivantes peuvent être spécifiquement identifiées :

- Fonctions liées à la gestion commerciale ou administrative du réseau :
- Gestion de la sécurité,
- Gestion des performances,
- Gestion de la configuration,
- Maintenance, gestion des alarmes.

I.1.5. Réseau Sémaphore Numéro 7 appliqué au GSM

Le mode associé est utilisé entre les BSCs et les MSCs. Le protocole de signalisation utilisé est BSSAP (Base Station Subsystem Application Part).

Le mode quasi-associé s'applique au sous-système réseau (NSS, Network Subsystem).

Les MSCs, GMSCs, HLR et EIR sont considérés comme des SPs (Signaling Point) rattachés à des STPs (Signaling Transfer Point).

Les protocoles de signalisation considérés sont ISUP, MAP (Mobile Application Part), INAP (Intelligent Network Application Part) et CAP (CAMEL Application Part).

I.2. Interfaces GSM

Interfaces du réseau

Les interfaces sont des composantes importantes du réseau car elles assurent le dialogue entre les équipements et permettent leur interfonctionnement. La normalisation des interfaces garantit l'interopérabilité d'équipements hétérogènes produits par des constructeurs différents.

- o L'interface radio " **UM** " est localisée entre la station mobile et la station de base (MS * BTS). C'est l'interface la plus importante du réseau.

- o L'interface " **A-bis** " relie une station de base à son contrôleur (BTS * BSC).
- o L'interface " **A** " se situe entre un contrôleur et un commutateur (BSC * MSC).
- o L'interface " **X.25** " relie un contrôleur au centre d'exploitation (BSC * OMC).
Le support de la liaison est fourni par un réseau de transmission de données.
- o L'interface entre le commutateur et le réseau public (MSC * RTC/RNIS) est définie par le **protocole de signalisation n°7 du CCITT**.

Le BSC et le MSC disposent de l'interface A basée sur l'utilisation d'une ou plusieurs liaisons numériques à 2Mbit/s qui supportent le trafic ainsi que la signalisation nécessaire.

L'interface A est définie à la sortie du MSC et le débit du canal de parole y est égal à 64 kbit/s. Or, le débit correspondant sur l'interface radio est égal au plus à 16 kbit/s. Une fonction de transcodage (TRAU, Transcoder / Rate Adaptor Unit) pour la parole ou de conversion de débit pour les canaux de données est donc nécessaire. Le protocole de signalisation sur l'interface A est BSSAP (Base Station Subsystem Application Part) qui s'appuie sur un transport SS7.

Le BSC et la BTS partagent une interface Abis qui utilise au niveau physique des liens à 2 Mbit/s. le protocole LAPD (Link Access Protocol for the D channel) du RNIS est utilisé pour le transport de la signalisation.

La station mobile (MS) communique avec la BTS par le biais de l'interface radio Um qui utilise le protocole de signalisation LAPDm. Cela permet à la station mobile d'établir une connexion de niveau 2 avec la BTS pour fiabiliser le dialogue sur le canal dédié. Le sens montant désigne les activités radio de la station mobile vers le réseau; le sens descendant désigne les activités radio du réseau vers la station mobile.

Les interfaces B, C, D, E, F et G utilisent le protocole MAP (Mobile Application Part) qui s'appuie sur la pile de protocole SS7.

Lorsqu'un MSC interroge le VLR qui lui est dédié, par le biais de l'interface B.

Lorsqu'un mobile démarre une procédure de mise à jour de sa localisation avec un MSC, le MSC en informe son VLR toujours à travers l'interface B qui sauvegarde les informations appropriées.

Le GMSC et le HLR disposent de l'interface C permettant au GMSC d'interroger le HLR contenant les caractéristiques d'abonnement d'un abonné mobile, afin d'établir un appel vers sa station mobile.

L'interface D est utilisée entre VLR et HLR pour échanger les données relatives à la localisation d'un mobile ainsi que pour la gestion des caractéristiques de l'abonné. Lorsqu'un mobile met à jour sa localisation auprès d'un nouveau MSC/VLR, le nouveau VLR envoie au HLR les données relatives à la dernière localisation du mobile.

Lorsqu'une station mobile se déplace d'un MSC vers un autre pendant une communication, une procédure de transfert intercellulaire (handover) inter-MSC doit être exécutée afin de garantir la continuité de la communication. A cette fin, les MSCs doivent échanger des données afin d'initier puis de réaliser l'opération. L'interface F utilisée entre MSCs et

supportée par le protocole MAP est utilisée à cet effet.

L'interface F est utilisée entre MSC et EIR afin d'échanger des données pour que l'EIR puisse vérifier l'état de l'identité de l'équipement mobile.

Lorsqu'un abonné mobile se déplace d'une zone contrôlée par un MSC/VLR à une autre sous la responsabilité d'un autre MSC/VLR, une procédure de mise à jour de localisation a lieu. Cette procédure peut comprendre l'échange de signalisation entre VLRs sur l'interface G afin que le nouveau VLR puisse obtenir de l'ancien VLR, l'IMSI et les triplets d'authentification concernant la station mobile.

Par ailleurs lors d'appels provenant du RTC, l'interface de signalisation entre un Class 5 Switch (Commutateur d'accès du RTC) et le GMSC est ISUP/SS7. La même interface est utilisée entre un MSC et le RTC pour des appels de la station mobile à destination d'un abonné du RTC.

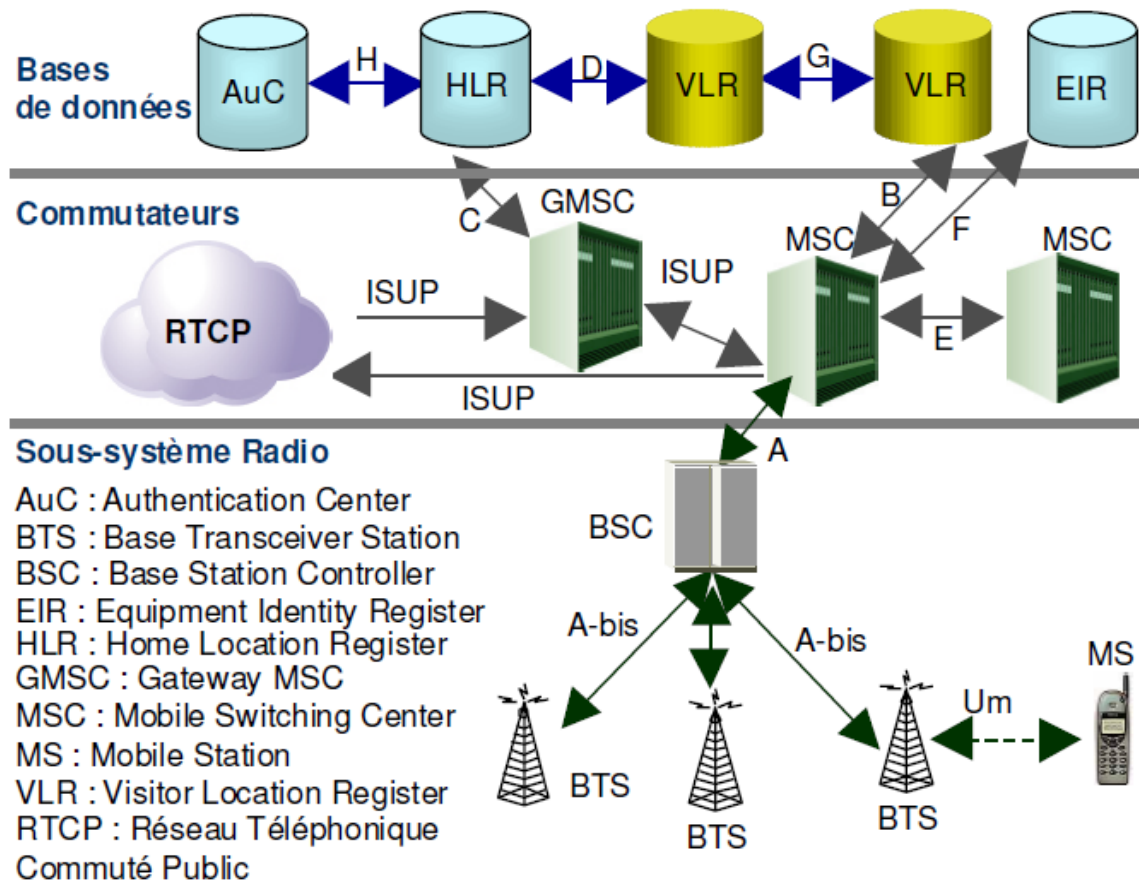


Figure 43 : Interfaces GSM

I.3. Identités dans un réseau GSM

I.3.1. IMSI

Lorsqu'un abonné souscrit à un abonnement mobile auprès d'un opérateur, un identifiant unique appelé IMSI (International Mobile Subscriber Identity) lui est affecté. Ce numéro d'IMSI a été préalablement stocké sur la carte SIM (Subscriber Identity Module). Un téléphone mobile ne peut être utilisé que si une carte SIM valide a été insérée dans l'équipement mobile car c'est la seule façon de facturer correctement un abonné mobile. Cet IMSI est un concept d'adressage spécifique au GSM ; il est différent du plan de numérotage RNIS.

Le numéro d'IMSI n'est pas connu de l'abonné mobile et n'est utilisé que par le réseau GSM.

L'IMSI est constitué de trois sous-champs :

- MCC (Mobile Country Code) : Il s'agit du code du pays du réseau GSM (208 pour la France). Le 1er Chiffre du champ MCC identifie le continent.
 - MNC (Mobile Network Code) : Il s'agit du code du réseau mobile. Il est codé sur 2 chiffres et identifie de manière unique le réseau GSM à l'intérieur d'un pays
 - MSIN (Mobile Subscriber Identification Number) : il s'agit du numéro d'identification du mobile. Il identifie l'abonné mobile à l'intérieur du réseau mobile.
- Les deux champs MCC et MNC permettent de déterminer de façon unique dans le monde le réseau mobile de l'abonné.

Les deux premiers chiffres du champ MSIN donnent l'indicatif du HLR de l'abonné au sein de son réseau mobile. Les MSC/VLR sont capables, à partir d'un IMSI quelconque, d'adresser le HLR de l'abonné correspondant.

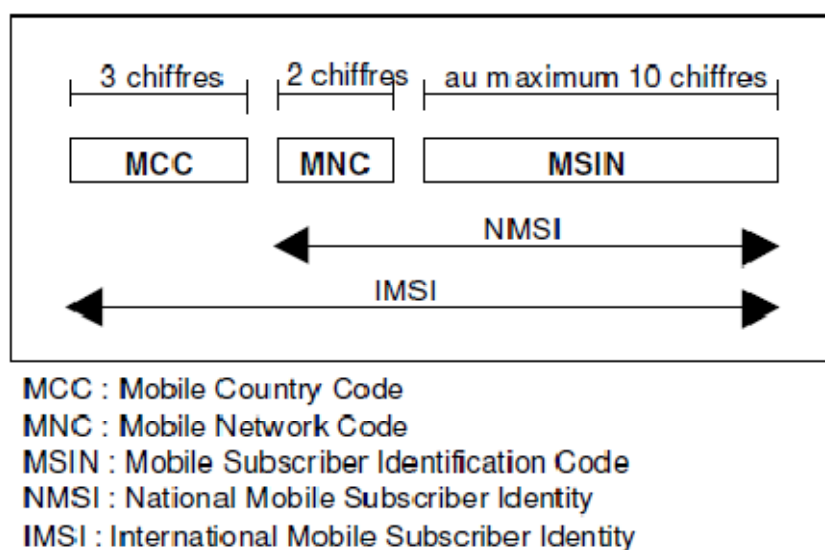


Figure 44 : Format de l'IMSI

I.3.2. MSISDN

Le numéro de téléphone associé à la station mobile est le MSISDN (Mobile Station ISDN Number).

Le MSISDN consiste en trois sous-champs :

- CC (Country Code) : Il s'agit du code du pays dans lequel l'abonné mobile a souscrit un abonnement (e.g., Code CC France = 33)
- NDC (National Destination Code) : Il s'agit du numéro national du réseau GSM dans lequel un client a souscrit un abonnement. (Orange France = 607, 608; SFR = 611 entre autres)
- SN (Subscriber Number) : En France le numéro MSISDN a la forme 33 6 AB PQ MCDU. 6 regroupe tous les abonnés mobiles. AB est l'indicatif Mobile GSM. PQ est le numéro de HLR logique dans le réseau GSM (à l'intérieur d'un même HLR physique, peuvent exister plusieurs HLR logiques identifiés par des valeurs PQ différentes). MCDU est le numéro de l'abonné dans le HLR.

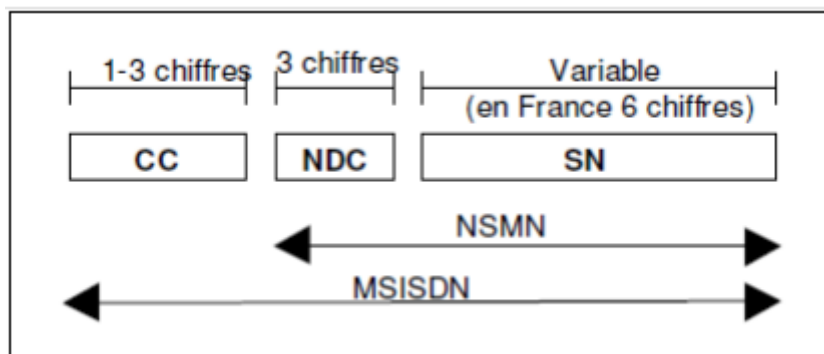


Figure 45 : Format du MSISDN

I.3.3. IMEI

L'IMEI (International Mobile Equipment Identity) identifie de façon unique un terminal mobile au niveau international. Il s'agit d'un numéro de série. Ce numéro est alloué par le constructeur du terminal mobile.

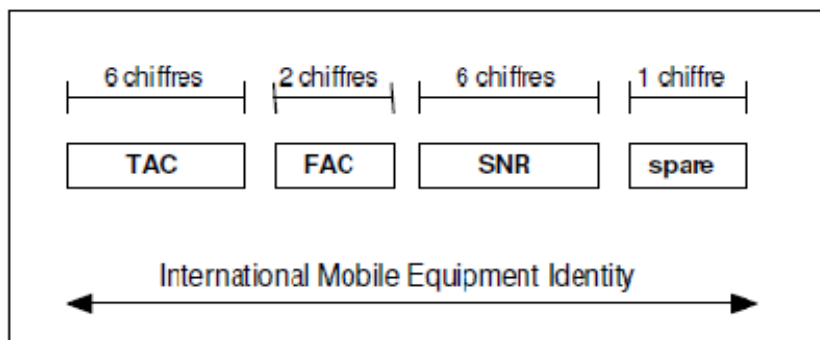


Figure 46 : Format de l'IMEI

L'IMEI est composé des éléments suivants :

- TAC (Type Approval Code) : Il s'agit d'un numéro indiquant la version de validation du matériel.
- FAC (Final Assembly Code) : Il s'agit du numéro qui identifie l'usine où a été assemblé le poste.
- SNR (Serial Number) : Il s'agit du numéro de série de l'appareil dans le TAC et le FAC.
- Spare (en réserve) : Ce chiffre doit être codé à "0" lorsqu'il est transmis par le mobile.

I.3.4. TMSI

De manière à conserver la confidentialité de l'identité de l'IMSI, le VLR alloue un numéro temporaire unique à chaque mobile se localisant dans sa zone de couverture ; ce numéro est appelé TMSI (Temporary Mobile Subscriber Identity). Le VLR est capable de corréler l'IMSI d'un mobile et son identité temporaire courante (TMSI).

A l'intérieur d'une zone gérée par un VLR, un abonné dispose donc d'un TMSI, attribuée au mobile de façon locale, c'est à dire pour la zone gérée par le VLR courant du mobile. Le TMSI est utilisé pour identifier le mobile lors des interactions station mobile __ réseau.

Le TMSI n'est connu que sur la partie MS __ MSC/VLR. Le HLR n'en n'a jamais connaissance. A chaque changement de VLR, un nouveau TMSI est attribué. L'utilisation du TMSI est optionnelle. On peut avoir recours à l'IMSI uniquement.

La structure et le codage du TMSI sont laissés à la discrétion d'accords entre l'opérateur GSM et les fabricants des postes mobiles utilisés par les abonnés du réseau de l'opérateur. Le TMSI est codé sur 4 octets.

Lorsqu'un mobile reçoit une identité temporaire (TMSI) d'un VLR (suite à une procédure d'authentification), il stocke cette identité sur sa carte SIM.

I.3.5. MSRN

Un numéro de roaming (numéro de réacheminement) est utilisé pour router les appels vers un mobile. Le MSRN (numéro de réacheminement) est un numéro PSTN (E164) attribué temporairement à la MS et qui permet d'acheminer l'appel vers le MSC dans l'aire duquel se trouve la MS ; tout se passe comme si la MS était un abonné du MSC. A la demande d'un GMSC au HLR concerné, un MSRN (Mobile Station Roaming Number) est alloué temporairement par le VLR qui possède les dernières informations de localisation de ce mobile.

Un numéro de réacheminement (MSRN) doit avoir la même structure que les MSISDN relatifs à une zone de localisation donnée, dans un réseau GSM et dans un pays donné.

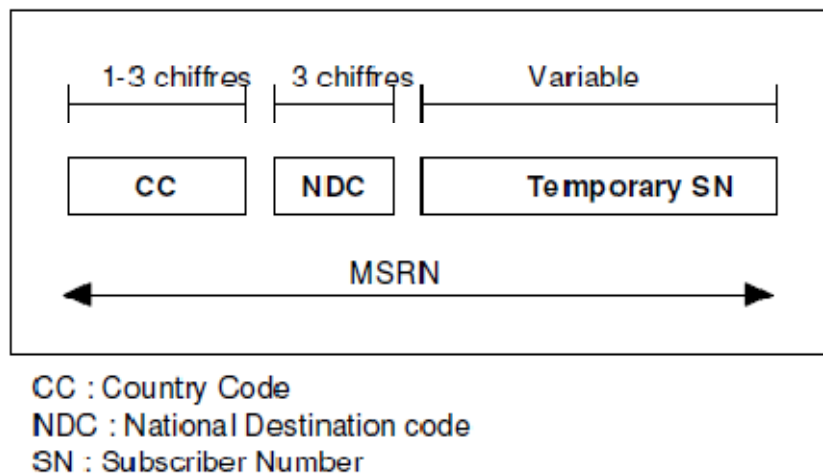


Figure 47 : Format du MSRN

I.3.6. LAI

Un réseau GSM est divisé en aires de service. Chaque MSC/VLR dans un réseau GSM contrôle une aire de service, composée d'un ensemble de zones de localisation (LAs, Location Areas), chaque LA représentant un ensemble de cellules. La figure 48 décrit de manière simplifiée un exemple de réseau GSM avec deux aires de services, celles du MSC/VLR1 et du MSC/VLR2. Le réseau est divisé en cinq zones de localisation.

- Les zones de localisation LA1 et LA2 sont sous le contrôle du MSC/VLR1. Elles constituent l'aire de service 1.
- Les zones de localisation LA3, LA4 et LA5 sont sous la responsabilité du MSC/VLR2. Elles forment l'aire de service 2.

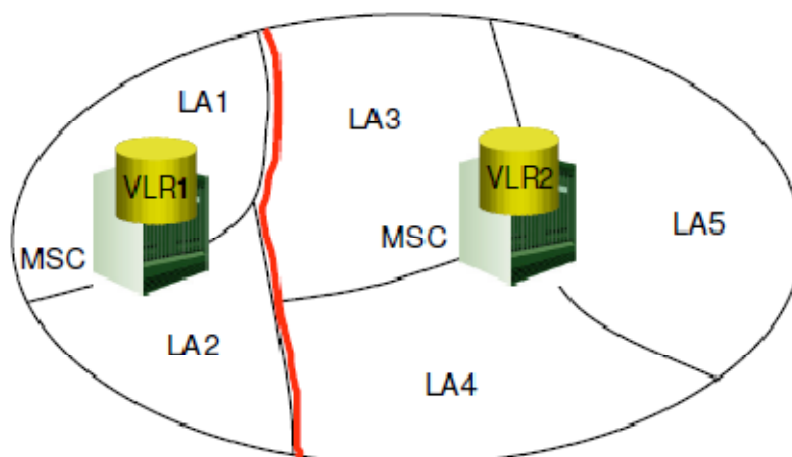


Figure 48 : Aire de service et zone de localisation

Une zone de localisation est identifiée par l'adresse LAI (Location Area Identification) composée des champs suivants :

- MCC : Il s'agit du code du pays du réseau GSM , champ également présent dans l'IMSI.
- MNC : Il s'agit du code du réseau mobile, champ également présent dans l'IMSI.
- LAC (Location Area Code) : il s'agit du code de la zone de localisation librement affecté par l'opérateur.

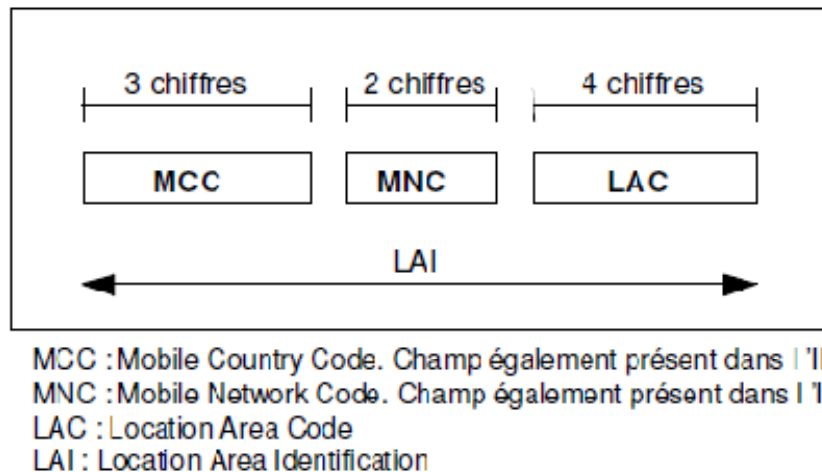


Figure 49 : Format du LAI

A la mise sous tension et ensuite lorsqu'il se déplace, la MS se met à l'écoute du canal BCCH de la cellule la plus puissante ; le BCCH (Broadcast Control Channel) diffuse l'identité de la LA. Le MS compare l'identité de la LA avec celle qui est mémorisée sur sa carte SIM. Si les identités sont identiques, la MS est correctement localisée et il ne se passe rien. Dans le cas contraire, la MS initie une procédure de mise à jour de localisation en signalant au réseau (VLR) l'identité de la nouvelle LA et son identité IMSI (ou TMSI).

Après localisation, la MS se met à l'écoute du canal de recherche PCH (Paging Channel) afin de pouvoir recevoir d'éventuels appels. En effet, lors d'un appel entrant, le VLR ne connaît que la LA courante du mobile. C'est la raison pour laquelle un avis de recherche (Paging) est émis sur cette LA.

I.3.7. CGI

La cellule au sein d'une zone de localisation est identifiée en rajoutant un numéro de cellule (CI, Cell Identity) à l'identification de la zone de localisation. L'identification globale de la cellule (CGI, Cell Global Identification) qui est unique, est donc la concaténation LAI+CI.

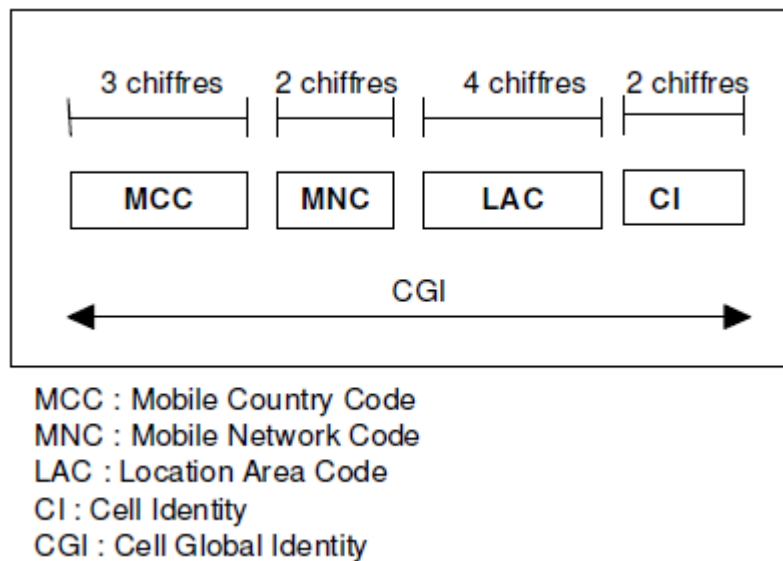


Figure 50 : Format du CGI

I.3.8. Identités pour l'authentification et le chiffrement

La sécurité GSM est adressée sur deux plans : authentification et chiffrement.

L'authentification empêche l'accès frauduleux par une station mobile clonée. Le chiffrement empêche l'écoute par un usager non autorisé.

Après que l'utilisateur se soit identifié au réseau, il doit être authentifié. Pour ce faire, une clé d'authentification individuelle K_i et un algorithme d'authentification A3 sont utilisés.

* L'AuC et la carte SIM contiennent K_i et A3. Pour initier le processus d'authentification, le réseau nominal d'un usager mobile génère un nombre aléatoire, RAND, d'une longueur de 128 bits. Ce nombre est envoyé à la station mobile.

* En appliquant l'algorithme d'authentification A3, le réseau (AuC) et la station mobile (Carte SIM) utilisent la clé K_i et le nombre RAND afin de produire un résultat (SRES)

.

* Le résultat SRES généré par la station mobile est envoyé au réseau nominal et comparé au résultat SRES généré par l'AuC.

* S'ils ne sont pas égaux, la demande d'accès de la station mobile est rejetée par le réseau.

* SRES et RAND générés par l'AuC sont envoyés au MSC/VLR qui les compare aux résultats soumis par la station mobile.

L'algorithme d'authentification A3 est spécifique à un opérateur GSM donné.

* Si la station mobile est acceptée, une clé de chiffrement K_c est produite par un algorithme de génération de clé de chiffrement A8 à partir de la clé K_i et du nombre RAND. Comme A3, A8 est spécifique au réseau nominal.

* Le système nominal (AuC) ayant généré Kc, l'envoie au MSC/VLR. Kc est une clé de chiffrement utilisée pour chiffrer / déchiffrer les données de signalisation et de trafic sur la voie radio entre la station mobile et la BTS.

* Un algorithme de chiffrement A5 présent sur la station mobile et la BTS est alors utilisé pour chiffrer / déchiffrer les données de signalisation et de trafic en utilisant Kc.

Cet algorithme A5 est normalisé et est le même pour tous les opérateurs mobiles.

- La carte SIM contient les informations Ki, A3, A8.

- L'AuC contient les informations A3, A8, IMSI/Ki.

- La station mobile et la BTS contiennent l'algorithme A5.

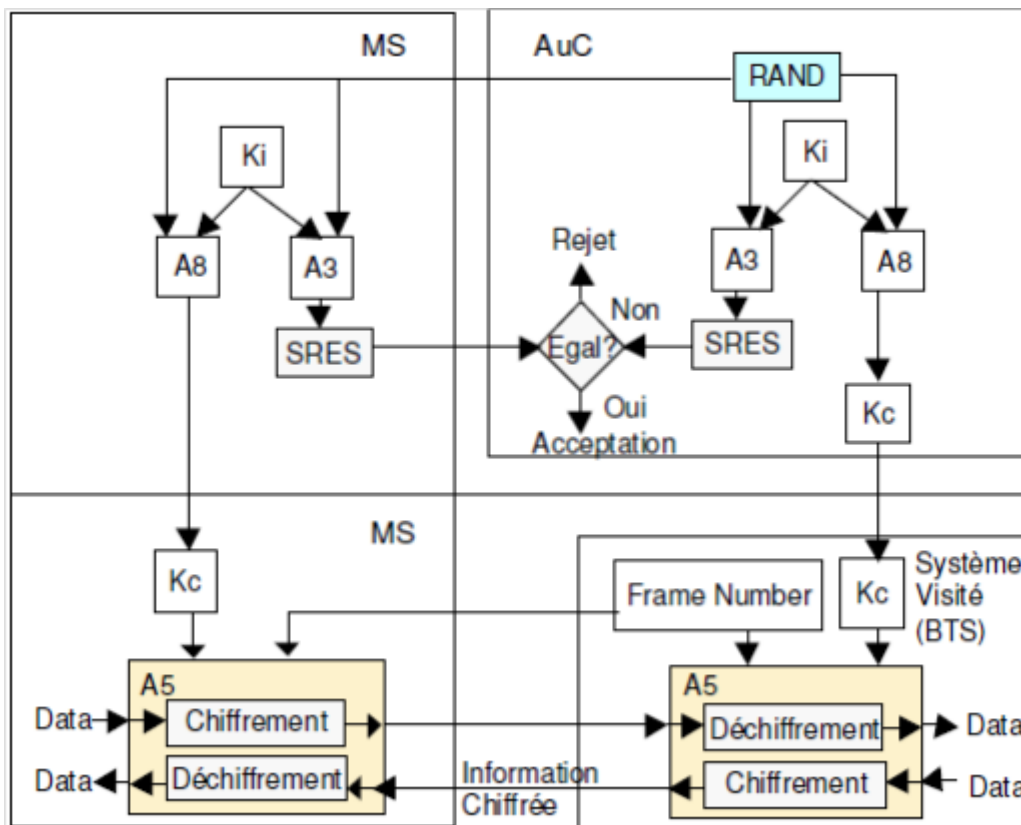


Figure 51 : Authentification et chiffrement .

I.3.9. Organisation des informations de l'abonné mobile

Les données de l'abonné sont stockées dans trois entités :

- L'entité HLR qui contient toutes les informations permanentes de souscription et certaines informations temporaires des usagers enregistrés sur ce HLR.
- L'entité VLR qui contient toutes les informations nécessaires pour le traitement d'appel et autres procédures pour les abonnés mobiles actuellement dans l'aire de localisation contrôlée par ce VLR.
- La carte SIM qui contient des informations permanentes liées aux services souscrits par l'abonné ainsi que des informations temporaires modifiées par le réseau au cours de la vie de la carte SIM.

L'IMSI est une information permanente. Elle est stockée dans le HLR, le VLR, et la carte SIM.

Le MSISDN est une information permanente présente dans les entités HLR et VLR.

Le TMSI est une information temporaire qui n'est stockée que dans le VLR et la carte SIM.

Le MSRN est une information temporaire générée et stockée dans le VLR.

Le LAI est une information temporaire présente sur le VLR et la carte SIM.

Le numéro de MSC/VLR est une information temporaire qui permet au HLR de connaître la localisation courante de la station mobile. Cette information est stockée dans le HLR.

La clé Ki est une information permanente stockée dans l'AuC et la carte SIM, l'AuC étant intégrée dans le HLR.

Le triplet (RAND, SRES, Kc) qui correspond à une information temporaire est calculé par l'AuC, et stocké dans le HLR et le VLR.

I.4. la liaison radio entre le téléphone mobile et la BTS :

La figure 52 représente le schéma général d'une communication entre un téléphone mobile GSM et un téléphone fixe ; cette communication repose sur :

- une liaison radio entre le téléphone mobile et une antenne-relais généralement installée sur un pylône ou un bâtiment ;
- une liaison entre l'antenne-relais et le téléphone fixe, essentiellement via des câbles et différents équipements faisant partie du réseau de téléphonie mobile GSM (ci-après « le réseau GSM ») et du réseau fixe.

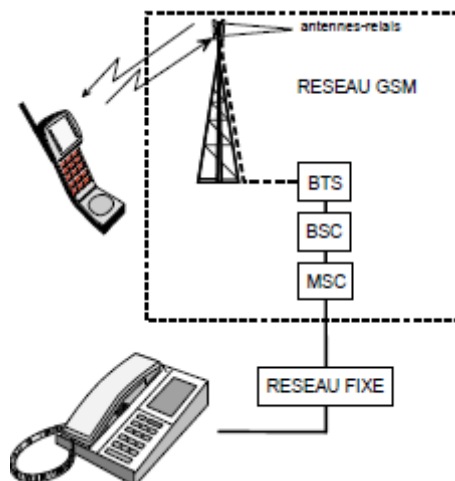


Figure 52: Schéma général d'une liaison entre un téléphone mobile GSM et un téléphone fixe

Une communication entre un téléphone mobile GSM et un téléphone fixe transite donc via une BTS, un BSC, le MSC et le réseau fixe. De même, une communication entre deux téléphones mobiles X et Y passera par la BTS la plus proche du

téléphone X, un BSC, le MSC, un second BSC, la BTS la plus proche du téléphone Y (le second BSC étant celui auquel la seconde BTS est reliée). Il est à noter qu'une communication entre deux téléphones mobiles très proches (abonnés d'un même opérateur) ne s'effectue jamais en « ligne directe », mais remonte toujours jusqu'à la BTS, le BSC et le MSC.

I.4.1. NUMERISATION DE LA VOIX

Les informations véhiculées via le réseau GSM sont transmises sous forme numérique, qu'il s'agisse d'une conversation téléphonique ou de données (SMS, accès au réseau Internet, ...). Le signal délivré par le microphone d'un téléphone mobile est un signal analogique qui est converti en un signal numérique constitué d'un « train » d'impulsions valant 0 ou 1. De même, le signal analogique fourni aux bornes de l'écouteur a été transmis sous forme numérique et a été retransformé en signal analogique par un convertisseur numérique–analogique.

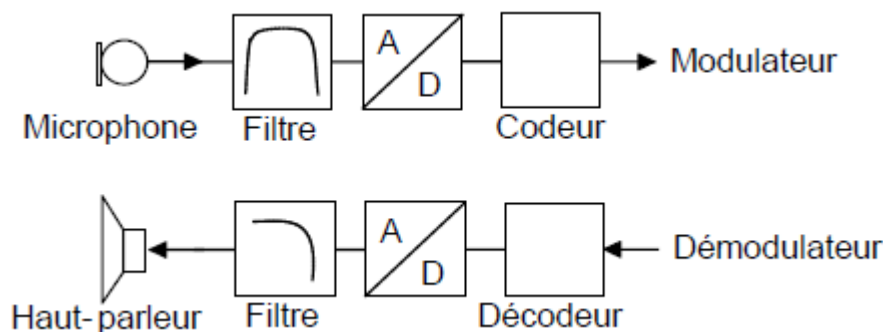


Figure 53 : Numérisation de la voix

La figure 53 décrit le processus de numérisation. Le signal de sortie du microphone subit un filtrage par un « passe-bande » 300 Hz–3,4 KHz et est ensuite échantillonné par un convertisseur analogique – numérique 13 bit à la cadence de 8.000 échantillons par seconde, ce qui donne un débit numérique de 104 kbit/s. La transmission d'un tel débit nécessiterait une bande passante beaucoup trop large. Les données binaires passent donc dans un codeur qui réalise deux fonctions :

- éliminer des données redondantes de manière à réduire le débit à transmettre ;
- ajouter des codes permettant la détection et la correction d'erreurs apparaissant lors de la transmission.

A la sortie du codeur, le débit binaire n'est plus que de 22,8 kbit/s, soit près de cinq fois moins .

Un principe inverse est utilisé à la réception. Le signal binaire à 22,8 kbit/s provenant du démodulateur (récepteur radio) est décodé pour reconstituer un signal numérique à 104 kbit/s, lequel est transformé en un signal analogique par un convertisseur numérique – analogique ; ce signal subit un filtrage par un « passe-bas » dont la fréquence de coupure est de 4 kHz ; il alimente l'écouteur du téléphone mobile.

I.4.2. TRANSMISSION PAR ONDES RADIO

La transmission entre le téléphone mobile et la BTS utilise une onde radio ; comme toute onde électromagnétique, elle comprend un champ électrique et un champ magnétique orientés perpendiculairement entre eux, ainsi qu'à la direction de propagation, comme illustré à la figure 54 ; ces champs varient sinusoïdalement dans l'espace et dans le temps. Les deux composantes de l'onde sont liées entre elles par la relation de proportionnalité suivante :

$$\frac{E}{H} = Z$$

où :

E : intensité du champ électrique en volts/mètre (V/m)

H : intensité du champ magnétique ampères par mètre (A/m)

Z : impédance caractéristique du milieu où l'onde se propage en ohms (Ω)

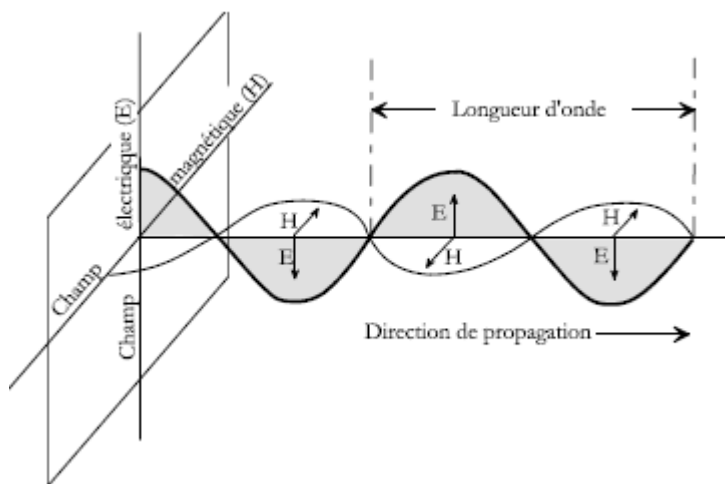


Figure 54: Onde électromagnétique plane

L'impédance caractéristique vaut 377Ω dans l'air, d'où :

$$\frac{E}{H} = 377 \Omega$$

l'intensité des champs électrique et magnétique présente une périodicité spatiale dont la longueur d'onde (c'est-à-dire la distance minimale entre deux points vibrant en phase) est liée à la fréquence du signal .

La densité de puissance S d'une onde plane (en W/m^2) est définie comme étant la puissance qui traverse une surface de $1 m^2$ perpendiculaire à la direction de propagation ; elle est donnée par :

$$S = E \cdot H \quad (4)$$

Compte tenu de la relation (2), lorsque l'onde se propage dans l'air, on peut écrire que :

$$S = \frac{E^2}{377} = 377 H^2 \quad (5)$$

Comme la puissance est transportée dans la direction de propagation, on peut représenter le flux de puissance par un vecteur $\mathbf{S}$ pointant dans cette direction : il est appelé vecteur de Poynting.

En principe, les relations (1), (2) et (5) ne sont valables que pour une onde plane, c'est-à-dire lorsqu'on est suffisamment loin de la source d'émission. Dans cette zone, la connaissance d'une des trois grandeurs (E , H ou S) permet, par simple calcul, de déterminer les autres grandeurs.

I.4.3. BANDES DE FREQUENCES

Les systèmes de téléphonie mobile GSM 900 et DCS 1800 fonctionnent respectivement à des fréquences voisines de 900 et 1800 MHz. Dans le cas du réseau GSM 900, la bande de fréquences comprise entre 880 et 915 MHz est utilisée pour la transmission du téléphone mobile vers l'antenne-relais, tandis que la bande comprise entre 925 et 960 MHz est utilisée dans le sens inverse. Dans la terminologie GSM, la transmission du téléphone mobile vers l'antenne-relais est appelée « voie montante » ou « up-link » ; la transmission de l'antenne-relais vers le téléphone mobile est, quant à elle, appelée « voie descendante » ou « down-link ».

Il faut signaler que les deux bandes de 10 MHz comprises entre 880 et 890 MHz, d'une part, et entre 925 et 935 MHz, d'autre part, sont souvent appelées « extended bands » pour des raisons historiques, car attribuées, à la téléphonie mobile, dans un second temps.

De manière similaire, les voies montantes et descendantes du DCS 1800 utilisent les bandes comprises entre 1710 et 1785 MHz, d'une part, et entre 1805 et 1880 MHz, d'autre part. L'affectation des différentes bandes est résumée dans le tableau 5. Les fréquences utilisables, ainsi que les bandes passantes associées, sont normalisées au niveau international .

Tableau 5: Bandes de fréquences des réseaux GSM 900 et DCS 1800

Normes	Voies	Bandes de fréquences (MHz)
GSM	Montante	890 - 915
	Descendante	935 - 960
GSM (« extended bands »)	Montante	880 - 890
	Descendante	925 - 935
DCS 1800	Montante	1.710 - 1.785
	Descendante	1.805 - 1.880

I.4.4. MODULATION

L'émission d'une onde électromagnétique de forme purement sinusoïdale ne permet la transmission d'aucune information ; pour que ce soit possible, il faut faire varier un des paramètres caractérisant la sinusoïde ; cette sinusoïde est appelée « fréquence porteuse » ou simplement « porteuse ». Les trois paramètres sur lesquels il est possible d'agir sont : l'amplitude, la fréquence ou la phase ; ce processus est appelé « modulation ».

La figure 55) représente les trois types de modulation dans le cas de signaux binaires (c'est-à-dire 1 ou 0) ; le diagramme A de la (figure 55) est une modulation d'amplitude de type « tout ou rien ». La transmission du bit 0 correspond à l'absence de porteuse. Inversement, le bit 1 correspond à la présence de la porteuse.

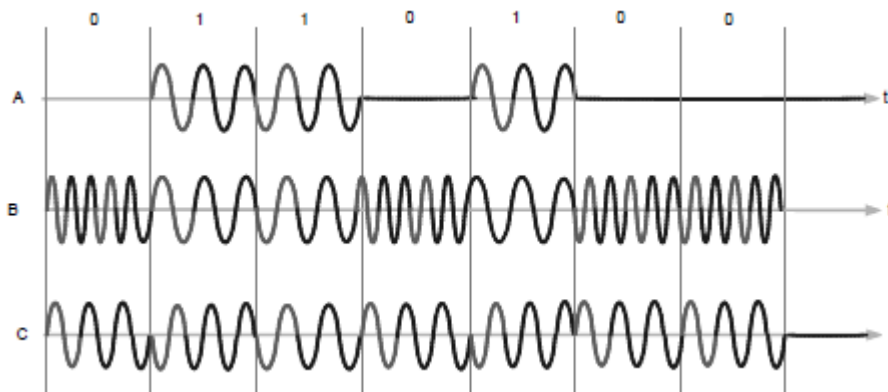


Figure 55: Modulations d'amplitude, de fréquence et de phase

Le diagramme B de la (figure 55) décrit le principe de la modulation de fréquence de type « tout ou rien » ; elle est désignée par l'abréviation FSK pour « frequency shift keying ». La transmission des bits 0 et 1 correspond à l'émission de deux fréquences différentes.

Le réseau GSM utilise la modulation GMSK (pour « gaussian minimum shift keying ») qui est une forme évoluée de la modulation FSK ; elle est réalisée en faisant passer le signal binaire, avant modulation, au travers d'un filtre passe-bas ; ce filtre passe-bas remplace les fronts montants et descendants par une transition progressive, ce qui diminue la largeur spectrale du signal modulé. Il en résulte que, pour un même débit binaire, la modulation GMSK a comme avantage d'occuper une largeur de bande moins importante que la modulation FSK classique. Une porteuse GSM modulée occupe une largeur de 200 kHz (100 kHz de chaque côté de la fréquence de la porteuse non modulée).

Le diagramme C de la (figure 55) correspond à la modulation de phase, donnée ici pour information. Les bit 0 et 1 sont transmis en faisant varier la phase de la porteuse.

I.4.5. MULTIPLEXAGE TEMPOREL - CANAUX DE TRANSMISSION

Une liaison entre un téléphone mobile et une antenne-relais utilise deux canaux de transmission : un pour la voie montante et un pour la voie descendante. Un canal est constitué d'une onde radio (la porteuse) dont la fréquence varie dans une plage de 200 kHz de largeur et pendant un huitième du temps.

I.5. Acheminement des appels / Interactions entre les équipements

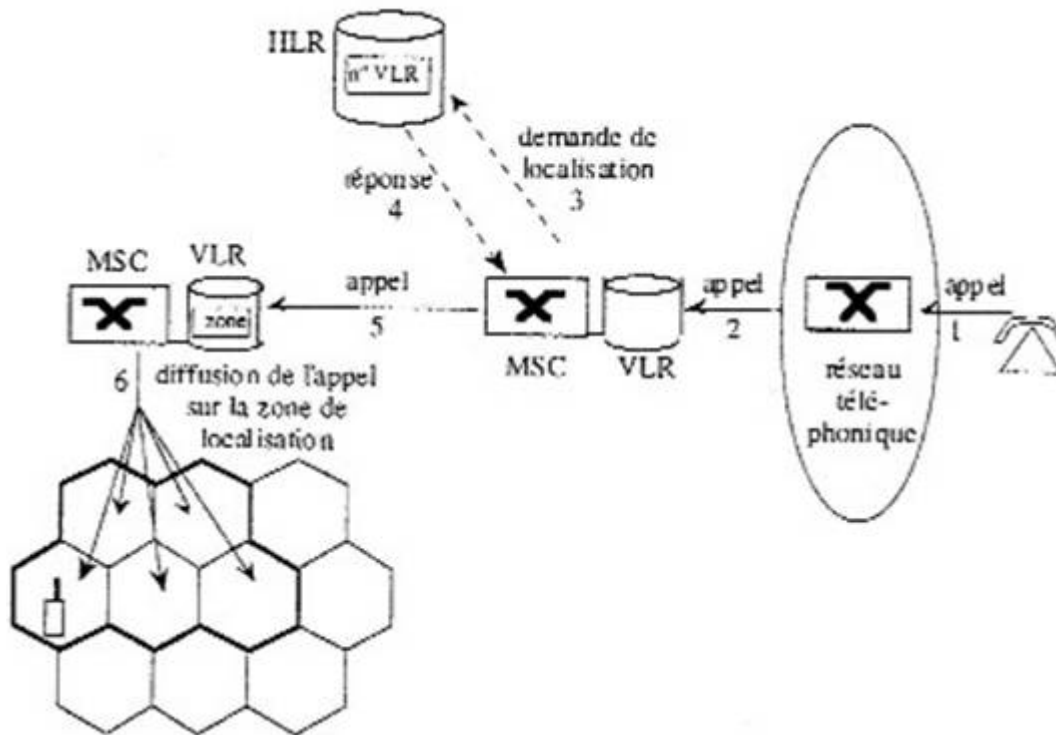


Figure 56 : Appel vers un mobile (simplifié)

Les messages 3 et 4 sont des messages du protocole MAP (non liés à un circuit).

Les messages 1, 2 et 5 sont des messages IAM (protocole ISUP ou équivalent).

Deux types d'appels illustrent les interactions entre les équipements du réseau, l'appel d'un abonné du réseau GSM vers un abonné du RTC/RNIS et l'appel d'un abonné du réseau RTC/RNIS vers un abonné du réseau GSM.

- **Appel d'un abonné du réseau GSM vers un abonné du RTC/RNIS**

Lorsqu'un usager appelle un correspondant à partir de son terminal mobile, celui-ci envoie un court message sur la fréquence montante de la voie balise. Ce message est reçu par la BTS et retransmis vers le BSC. Il s'ensuit alors un échange de signalisation entre le mobile et le MSC/VLR pour vérifier que l'abonné est autorisé à utiliser le réseau et à disposer du

service demandé. Une voie de communication est ensuite allouée au mobile et la connexion est établie lorsque le correspondant demandé fixe décroche.

- **Appel d'un abonné du réseau RTC/RNIS vers un abonné du réseau GSM**

Lorsqu'un abonné du RTC/RNIS numérote, le numéro composé est analysé par le commutateur dont dépend l'abonné, l'appel est systématiquement transféré au MSC le plus proche du demandeur fixe (cf. figure 3.25). Celui-ci interroge le HLR de l'abonné mobile demandé pour déterminer sa localisation et vérifier qu'il est autorisé sur le réseau. L'appel est ensuite routé vers le MSC/VLR où se trouve l'abonné mobile. Le MSC/VLR recherche la zone de localisation où est le mobile. Afin de commander la sonnerie du terminal demandé le contrôleur BSC fait diffuser un avis d'appel par l'ensemble des stations BTS de sa zone vers le terminal demandé,. Le mobile, en réponse, transmet un message dans la cellule où il se trouve. L'appel se poursuit par l'échange de signalisation entre le mobile et le MSC/VLR puis par l'établissement de la connexion lorsque l'abonné mobile décroche. Dans le même temps les bases de données VLR et HLR mettent à jour l'état de l'abonné.

II. l'interfaçage du Call center avec le réseau GSM :

Une passerelle GSM est un dispositif permettant au centre d'appels à trafic GSM important de réduire ses frais d'appel depuis les lignes fixes vers les réseaux GSM, elle se connecte au PABX de l'entreprise soit par connexion analogique, soit par connexion numérique. Les appels en provenance du réseau filaire sont donc routés par le PABX vers la passerelle donnant un accès direct aux réseaux cellulaires GSM/DCS.

Et grâce à la migration du PABX classique vers la technologie IP une troisième passerelle vient s'ajouter pour l'interfaçage, afin d'optimiser le rendement , et ce à l'aide d'une passerelle GSM VOIP.

Les passerelles GSM permettent de connecter les systèmes PABX/PABX IP aux réseaux cellulaires GSM de manière simple, rentable et rapide à l'aide d'interfaces RNIS BRI, PRI E1/T1, T0/S0, T2/S2 RNIS, RNIS ou VoIP .

la passerelle GSM fonctionne avec une carte SIM à l'intérieur (ou plusieurs). Elle se comporte comme un téléphone GSM classique.

II.1.Passerelles GSM numériques :

II.1.1. Passerelles GSM PRI E1/T1 :

II.1.1.1. PRESENTATION :

Les passerelles GSM PRI E1/T1 sont des passerelles GSM PRI RNIS modulaires dotées de 4 à 30 canaux GSM, elles se relient en coupure sur le T2 ou directement sur l'interface PRI RNIS

E1 ou T1 du PBX via des câbles de connexions standard et ne nécessitent aucune modification de l'installation téléphonique existante.

Connectée aux équipements d'un opérateur alternatif, la passerelle PRI peut diminuer le coût des terminaisons d'appel et ainsi augmenter les profits.

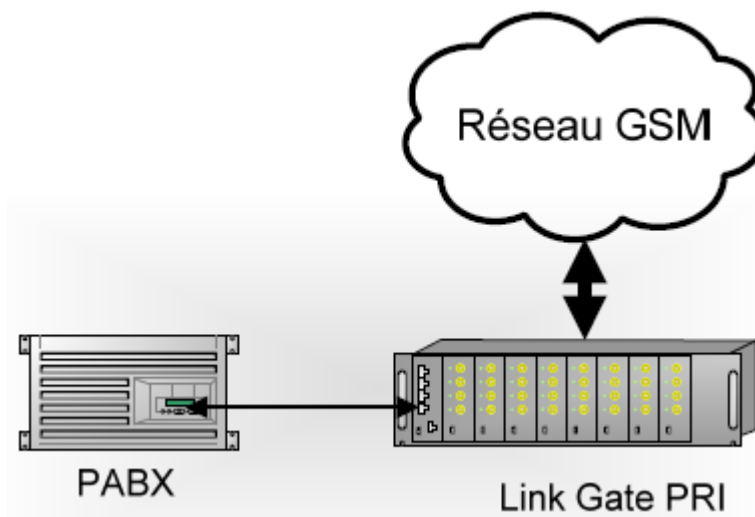


Figure 57 : Passerelle GSM PRI

II.1.1.2. Fonctionnalités :

Passerelle équipée de 8 canaux GSM , évolutive à 32.

- **Gestion des appels entrants et sortants par faisceaux** (Groupe de cartes SIM).

- **LCR intégré** : permet l'acheminement des appels sortants sur un faisceau GSM en fonction du numéro émetteur de l'appel et le numéro appelé.

La passerelle Link Gate PRI est capable de gérer jusqu'à 32 faisceaux regroupant de 1 à 32 cartes SIM. En fonction du numéro de l'appelant et du numéro appelé, l'appel est dirigé vers un faisceau dédié. Il est également possible de gérer les débordements en cascade vers d'autres faisceaux ou le réseau RNIS fixe.

Cette fonctionnalité est idéale pour les installations multi-sociétés et pour tout centre d'appels désirant optimiser ses coûts de communication.

- **Call Back** : permet à un collaborateur de se faire rappeler par la passerelle puis de pouvoir communiquer avec comme s'il était en interne.

- **Serveur SMS*** : Permet l'envoi et la réception de SMS.

- **Smart Call Back** : En cas d'appel sortant sans réponse, si l'appelé rappelle la passerelle, l'appel est automatiquement acheminé vers l'extension initiatrice du premier appel.

- **DISA** : Il est possible d'appeler la passerelle puis de composer un numéro interne pour joindre directement la personne souhaitée.

- **Gestion avancée des crédits de communication** sur chaque carte SIM en prenant en compte le report des minutes et le jour de facturation.
- **CDR** : Rapport Détaillé des Communications.
- **Statistiques** d'utilisation des modules GSM.
- **Configuration par PC** via une connexion USB ou Ethernet
- **Routeur intégré** : pour l'acheminement de certains appels vers le réseau fixe.

La passerelle Link PRI est capable d'analyser le numéro composé et de le router soit vers le réseau GSM, soit vers le réseau RNIS fixe.

Egalement, lorsque tous les modules GSM sont occupés, il est possible de router l'appel vers le réseau RNIS. Les appels arrivants du réseau fixe sont routés directement au PABX.

Cette fonctionnalité est idéale pour les entreprises désirant utiliser la passerelle GSM mais ne disposant pas d'accès T2 de libre sur l'autocommutateur.

II.1.1.3. Principaux avantages :

- Utilisation des interfaces RNIS PRI E1/T1 existantes pour les PABX
- compatible avec tous les PABX RNIS
- PABX relié directement au réseau GSM
- Connexion en coupure sur le T2 (topologie avec 3 interfaces) entre le PBX et le RTC
- Fonctionnalité avancée de routage à moindre coût (LCR)
- Système évolutif : de 4 à 30 appels simultanés
- Gestion et contrôle à distance via Internet

II.1.2. Passerelles GSM RNIS BRI (T0) :

En se connectant directement à l'interface BRI du PABX, la passerelle RNIS BRI exploite les PABX numériques existants et permet d'effectuer 2 à 16 appels GSM simultanés grâce à 2 B-canaux ou 4 BRI

II.1.2.1. Caractéristiques du système :

- Capacité : 2 ou 8 canaux GSM intégrés - 2 B-canaux ou 8 B-canaux

Configuration :

- Appels bidirectionnels (appels entrants et sortants)
- Le BRI peut être programmé en NT ou TE
- Restriction à l'accès interurbain
- MSN prédéfini

II.2. Passerelles GSM analogique :

Elles se raccordent à une sortie de ligne analogique standard libre par une simple fiche RJ11 (une ligne par passerelle). Idéalement, un programme de routage (LCR : least cost routing)

achemine les appels sortants à destination des mobiles vers les lignes allouées aux passerelles.

II.2.1. DESCRIPTION :

Passerelle analogique type LR (ligne réseau analogique)

- ✓ Permet d'effectuer une communication de téléphonie fixe vers un téléphone mobile
- ✓ Affichage du numéro appelant
- ✓ Module GSM tribande
- ✓ Module GPRS intégré

II.3. Passerelle GSM VOIP pour PABX IP/ IPBX :

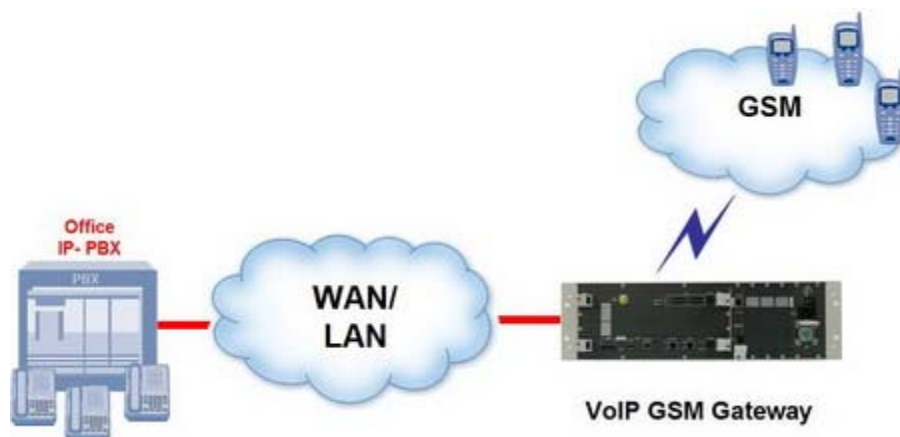


Figure 58 : Routage des appels GSM via la passerelle VOIP

Les passerelles GSM VoIP sont modulaires (de 4 à 30 ports GSM) et permettent de connecter les IP-PBX directement aux réseaux cellulaires GSM via des protocoles SIP ou H323.

Routage des appels GSM entrants/sortants via le VoIP

Les « hérissons », ou « passerelles mobiles » ou « GSM gateways » sont des équipements qui peuvent être raccordés à un commutateur et qui permettent d'écouler du trafic vers les réseaux mobiles en utilisant deux boucles locales radio au lieu d'une. La première boucle locale radio permet d'acheminer l'appel du « hérisson » jusqu'au réseau de l'opérateur

mobile ; la deuxième permet d'acheminer l'appel du réseau de l'opérateur mobile jusqu'au terminal mobile du destinataire de l'appel.

En d'autres termes, quand un téléopérateur appelle un mobile à partir d'un Pabx IP, l'autocommutateur va automatiquement router l'appel vers la passerelle GSM. Ainsi, l'appel sera réalisé au travers de la carte SIM intégrée à ladite passerelle. Le call center sera facturé par l'opérateur mobile au lieu de l'opérateur fixe. Il est possible d'utiliser plusieurs cartes SIM, dont plusieurs opérateurs mobiles. comme le montre le schéma ci-contre.

II.3.1Caractéristiques du système :

Capacité :

- Systèmes comptant de 4 à 30 canaux GSM (et/ou AMRC)
- Jusqu'à 30 canaux VoIP (SIP/H323)
- 1 SIM ou multiSIM ; 4 cartes SIM par port
- Configuration :
- Appels bidirectionnels (appels entrants et sortants)
- Fonctionnalités LCR
- Compatibilité avec les SMS (en option)
- Séparateur d'antenne intégré
- **Compatibilité PBX** : avec les systèmes IP des plus grands fabricants mondiaux
- Alimentation redondante (en option)
- Gestion Internet à distance
- Port série local

II.4. Conclusion :

Les passerelles GSM représentent un réelles avantages pour les centres d'appels; Ce sont de puissant outils pour réduire les frais téléphoniques et ce a travers la réduction des coûts d'appel fixe-mobileet de roaming nationaux et internationaux ainsi que la réduction des frais téléphoniques et d'installation pour les entreprises multi-sites.

Conclusion générale

Les avantages opérationnels réels d'un centre de contact IP pour l'activité de service clientèle de l'entreprise sont si considérables que les sociétés pourraient bien adopter la convergence pour leurs seuls mérites. Avec la voix sur IP (VOIP), l'entreprise fait converger ses réseaux voix et données sur une infrastructure unique. Non seulement le réseau unique est moins cher à acquérir et à exploiter, mais il permet également de configurer et d'administrer les règles de métier à partir d'un site unique et d'offrir ainsi à la clientèle une expérience cohérente. De plus, le réseau convergent VOIP autorise le déploiement et l'exploitation optimale des nouvelles applications, quels que soient leurs constructeurs, tout en aidant l'entreprise à les rentabiliser.

Pour introduire une nouvelle technologie sur un marché bien établi, il est indispensable d'assurer la compatibilité avec les technologies dominantes tels que les matériels et les logiciels de téléphonie pour lesquels les sociétés ont considérablement investi. Ceci est d'autant plus vrai sur le marché des centres d'appels.

Les technologies de voix sur IP sont des technologies matures et porteuses. Elles offrent une téléphonie IP sur le réseau local informatique (LAN) utilisant le câblage et le réseau informatique en place pour relier les composants actifs de son architecture et ses terminaux. L'administration du réseau en est simplifiée et centralisée, en ce qui concerne la téléphonie IP sur internet ou sur le réseau étendu (WAN) elle permet quant à elle la mobilité, le télétravail et les communications gratuites.

Dans le cas d'une entreprise multi-sites, la VOIP permet une Communication intersites gratuite ainsi que la mutualisation des ressources au niveau de l'ensemble des agences pour les systèmes de communications (IPBX) et passerelles sans oublier les abonnements opérateurs pour les appels entrants et sortants et les passerelles GSM.

La souplesse de la voix sur IP permet de desservir tout type de poste, nouveaux postes IP, softphones, reprise des anciens postes ainsi que la mise en œuvre de tout type d'accès opérateurs, qu'ils soient Centrex, opérateurs classiques ou GSM.

Un call center a la pointe de la technologie, avec un nouveau Standard d'accueil automatique muni d'applications informatiques, web et vocales interactives a vu le jour grâce à la technologie VOIP.

Conclusion générale

LISTES DES FIGURES :

Figure 1: Architecture d'un Centre d'appels

Figure 2 : architecture interne d'un Pabx

Figure 3 :lignes e/s d'un Pabx

Figure 4 : Schéma d'un réseau Pabx IP

Figure5: Architecture Hybride

Figure 6 : Architecture full IP

Figure 7 : Architecture de téléphonie sur IP de type Centrex

Figure 8 : Telephonie VOIP sur un reseau privé

Figure 9 : Architecture d'un Passerelle IP

Figure 10 : 8 étapes de la voix à IP

Figure 11 : Voix sur IP entre deux ordinateurs

Figure 12 : Voix sur IP entre PC et un téléphone

Figure 13 : Voix sur IP entre deux téléphones

Figure 14 : Composants H323

Figure 15 : Terminaux H 323

Figure 16 : Passerelle H323

Figure 17 : composants MCU H323

Figure 18 : protocoles H 323 intervenant dans un appel

Figure 19 : Enregistrement de la gateway

Figure 20 : Enregistrement des postes IP

Figure 21 : Pile SIP

Figure 22 : Entités SIP

Figure 23 : SIP Registration

Figure 24 : SIP proxy server

Figure 25 : exemple d'une communication SIP

Figure 26 : Schema d'une partie de l'entete d'un paquet RTP

Figure 27 : En -tête des paquets RTCP

Figure 28 : exemple d'utilisation d'ENUM

Figure 29 : problème de NAT avec SIP

Figure 30 : problème du firewall avec la ToIP

Figure 31 : technique de la passerelle d'application

Figure 32 : principe de fonctionnement du protocole STUN

Figure 33 : principe de fonctionnement du protocole TURN

Figure 34 : Les architectures du call center

Figure 35 : Architecture call center du premier scenario

Figure 36 : Architecture call center du deuxième scenario

Figure 37 : Architecture call center du troisième scenario

Figure 38 : Attaque DoS via une requête CANCEL

Figure 39 : Exemple de détournement d'appel " Man in the middle"

Figure 40 : Format d'un paquet SRTP

Figure 41 : Structure du réseau GSM

Figure 42 : Les entités du réseau GSM

Figure 43 : Interfaces GSM

Figure 44 : Format de l'IMSI

Figure 45 : Format du MSISDN

Figure 46 : Format de l'IMEI

Figure 47 : Format du MSRN

Figure 48 : Aire de service et zone de localisation

Figure 49 : Format du LAI

Figure 50 : Format du CGI

Figure 51 : Authentification et chiffrement

Figure 52: Schéma général d'une liaison entre un téléphone mobile GSM et un fixe

Figure 53 : Numérisation de la voix

Figure 54: Onde électromagnétique plane

Figure 55: Modulations d'amplitude, de fréquence et de phase

Figure 56 : Appel vers un mobile (simplifié)

Figure 57 : Passerelle GSM PRI

Figure 58 : Routage des appels GSM via la Passerelle VOIP

LISTES DES TABLEAUX :

Tableau 1 : Fonctionnalité d'un IPBX

Tableau 2 : Correspondance entre les débits et les codecs

Tableau 3 : Comparaison SIP _ H323

Tableau 4 : résumé des solutions de traversées les NAT et les pare-feux

Tableau 5: Bandes de fréquences des réseaux GSM 900 et DCS 1800

Glossaire :

Adaptateur IP : équipement qui permet de passer du monde IP au monde RTC

Adaptateur ATA : permet à un téléphone analogue d'être connecté au système VoIP .

ADSL: Asymmetric Digital Subscriber Line.

ATM : (RNIS large bande) technologie dédiée au WAN.

Borne DECT :pour la connexion sans fil

Codecs : Compression et Décompression.

CENTREX : Le Centrex est un IPBX hébergé

DHCP : dynamic host configuration protocol (protocole d'auto configuration IP). il a besoin de son propre serveur sur le réseau voip

DNS: domaine name system.

DOS: denial of service.

DSP: (Digital Signal Processor)

ENUM: telephone number mapping .

Flotte : c'est un service offert par les opérateurs permettant à un groupe d'utilisateur d'un réseau de pouvoir s'appeler entre eux à coût réduit.

ICE : (Interactive Connectivity Establishment)

IM (Instant Message).

IPBX : L'IPBX est la version IP du PABX traditionnel (on parle aussi de PABX IP ou PBX IP).

IPsec : (Internet Protocol Security)

IVR (Interactive Voice Response) réponse vocale interactive.

ITSP :internet telephony service provider.

ITU : (International Télécommunication Union / Union internationale des Télécommunications).

ISDN: integrated service digital network(réseau RNIS)

LAN (Local Area Network): réseau local ou groupe de réseaux locaux interconnectés soumis au même contrôle administratif.

MC : Multipoint Controller

Messagerie IP : système d'échange de message ou bureau de poste électronique

Messagerie unifiée : c'est le fait de centraliser tous ses messages dans sa boîte mail (mail, message vocal, fax...)

MGCP : (Media Gateway Control Protocol)

MMUSIC : (Multiparty Multimedia Session Control)

MOS : (Mean Operational Score).

MPLS : MultiProtocol Label Switching (MPLS) mécanisme de transport de données, opérant sur la couche de liaison de données du modèle OSI.

NAT: network address translation.

Open source : caractérise les logiciels dont le code source est modifiable librement et redistribuable sous certaines conditions.

Passerelle : point d'interconnexion avec la téléphonie traditionnelle (réseau RTC public, postes analogiques).

passerelle VOIP :

standard téléphonique relier les postes téléphoniques d'un établissement avec le réseau téléphonique public. elles sont de deux types

1. **Unités analogues :** sont utilisées pour la connexion des lignes téléphoniques analogues normales. Les unités analogues sont disponibles pour 2 à 24 lignes.

2. **Unités numériques :** permettent de connecter des lignes numériques, soit une ou plusieurs lignes BRI RSIN (Europe), PRI/E1 (Europe) ou T1 (États-Unis)

PABX (Private Branch eXchange) : est un échange téléphonique qui appartient à une société privée, au contraire de celui appartenant à une compagnie de téléphone ou un exploitant de réseau.

PCM : (Pulse Code Modulation).

PSTN (Public Switched Telephone Network) est le réseau résultant de l'interconnexion de tous les réseaux téléphoniques commutés du monde entier.

Réseau local (LAN) : il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau.

Réseau étendu (WAN ou MAN): il interconnecte plusieurs LANs à travers de grandes distances géographiques à caractère national ou international.

Roaming : permet à un abonné de pouvoir appeler ou de se faire appeler dans certains pays grâce aux accords d'interopérabilités entre les réseaux.

RNIS (Réseau Numérique à Intégration des Services.

RTP : (Real-Time transport Protocol)

RTCP : (Real Time Control Protocol)

RSVP : protocole qui prend en charge la QOS.

SCCP : (Skinny Client Control Protocol)

SRTP : (Secure Real-time Transport Protocol)

SVPN : (Secure VPN)

Serveur d'appels : équipement coeur permettant l'établissement des appels et la fourniture des services de téléphonie . Appelé aussi Gatekeeper, Soft Switch, Call Manager ou IPBX.

Soft phone : logiciel permettant de passer et recevoir des appels depuis un PC multimédia (casque + haut-parleur).

STUN : (Simple Traversal of UDP Through Network Address Translators)

SIP (Session Initiation Protocol) : il propose un standard pour initiation, modification et fermeture d'une session utilisateur interactive qui implique des éléments multimédia .

SiVuS : (SIP Vulnerability Scanner)

Téléphonie IP : ensemble des services de téléphonie en IP (terminaux et serveurs). Elle permet d'offrir les services associés aux échanges vocaux enrichis directement avec des équipements IP (terminaux, traitement de la communication, etc.)

Terminal IP ou IP phone : téléphone IP raccordé au LAN de l'entreprise (éventuellement sans fil Wi-Fi).

ToIP Wi-Fi La ToIP Wi-Fi désigne les réseaux de téléphonie IP s'appuyant sur la technologie de mobilité Wi-Fi. Les paquets IP circulent par ondes radio plutôt que par câbles.

Trafic de jonction : permet aux internes de deux centraux privés différents de pouvoir s'atteindre , directement , sans transiter par des téléphonistes et le réseau public.

TURN : (Traversal Using Relay NAT)

UTP :unshielded twisted pair (paire torsadée non blindée).

UAC : (User Agent Client)

VLAN : virtual local area network

Voix sur IP : technologie de transport de la voix sur un réseau IP. La voix sur IP consiste à transporter la voix sous forme numérique dans les réseaux IP.

VOMIT : (Voice Over Misconfigured Internet Telephone)

VPN : (*Virtual Private Network*).

VPN ToIP : un réseau privé virtuel (VPN) Se chargent de sécuriser les communications distantes entre deux sites donnés.

X25 : définit l'interface entre un ETTD (Équipement Terminal de Traitement de Données) et un ETCD (Équipement de Terminaison de Circuit de Données) pour la transmission de paquets.

Annexe :

Les Débits sur le LAN :

Les débits obtenus sur le LAN, suivant le codec H323 utilisé, sont répertoriés dans le tableau ci-dessous :

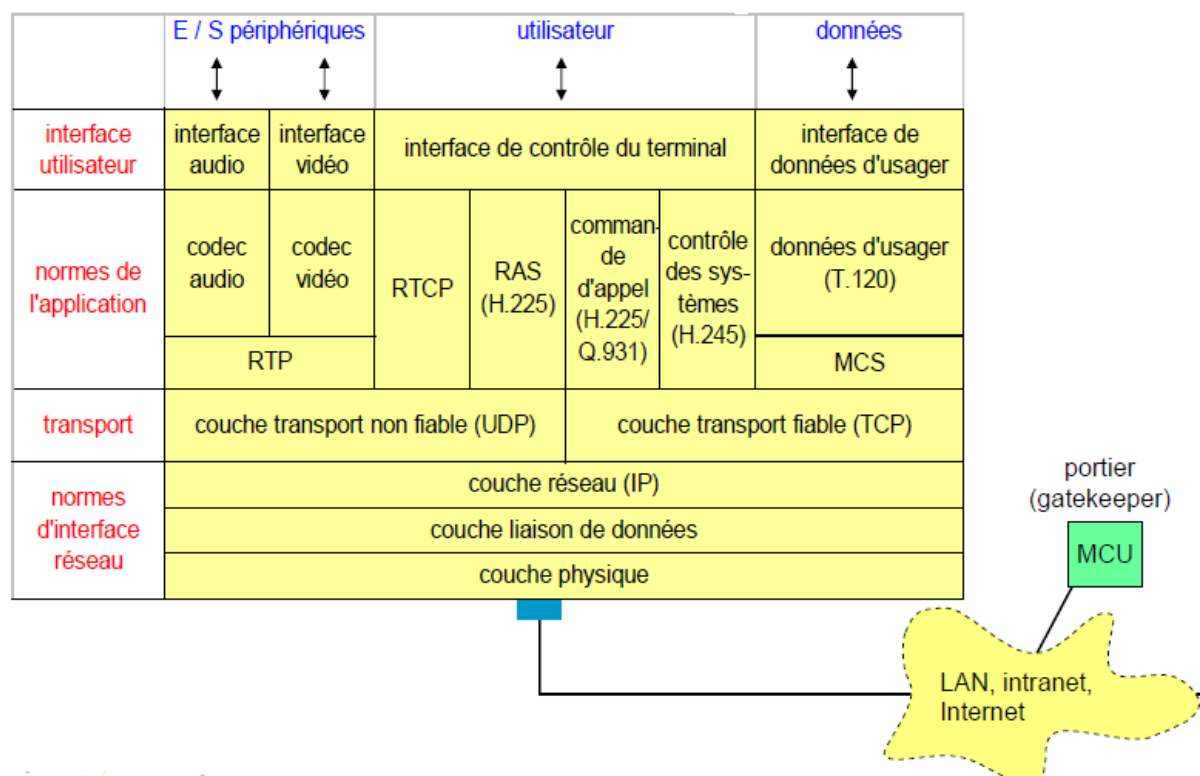
Algorithme de compression	Débit Codec (Kbps)	IP (Kbps)	Ethernet (Kbps)
G.711	64	74,6	78,4
G.729	8	18,6	22,4
G.723.1	5,3	16	19,7
G.723.1	6,4	17	20,8

Les Débits sur le WAN:

Les débits obtenus sur le WAN, suivant le codec H323 utilisé, sont répertoriés dans le tableau ci-dessous :

	Liaison Frame relay (Kbps)			Liaison PPP (Kbps)		
	G.711	G.729	G.723	G.711	G.729	G.723
Sans compression RTP	76	20	18,4	76	20	18,4
Avec compression RTP	65,8	9,8	8,2	65,8	9,8	2,2

Structure UIT pour les réseaux à commutation de paquets : H.323



6.1 -la pile de Protocole H323:

Signalisation	Transport	Codecs	Services	Sécurité
Signalisation d'enregistrement /contrôle d'admission RAS (H.225.0)	RTP/RTCP H.225.0	Audio G.711,G.722, G.723, G.728,G.729	Services supplémentaires H.450.x	H.235
Signalisation appel H.225.0		Vidéo H.261 H.263	Services de conférence H.323 H.332	
Signalisation connexion H.245		Data T120	Passerelle H.246	

Figure 6 : Pile de protocole H323

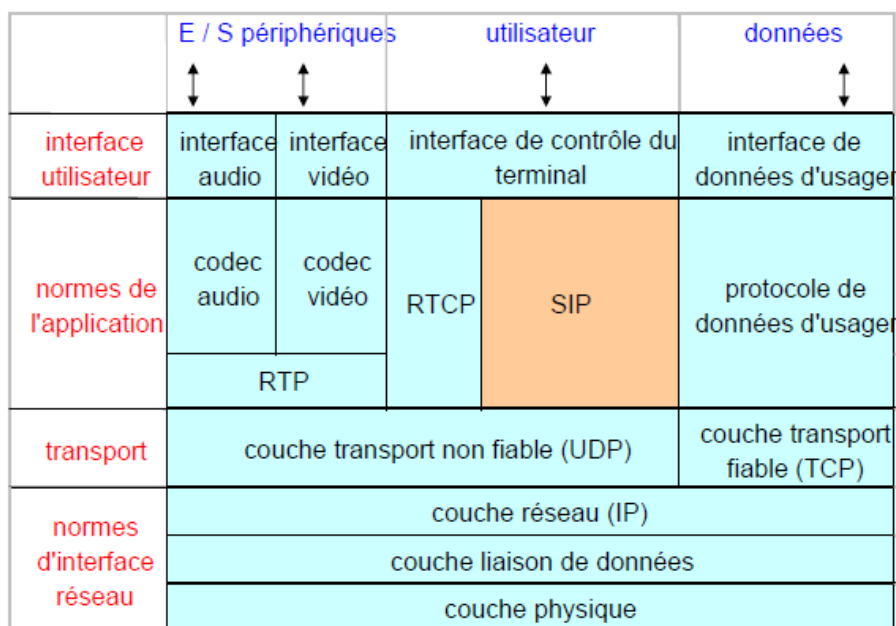
Tableau récapitulatif des réponses SIP:

Messages SIP (Réponses)

1xx	Informational (Not required)	4xx	Request Failure
100	Trying	400	BadRequest
180	Ringing	401	Unauthorized
181	CallsBeingForwarded	402	PaymentRequired
182	Queued	403	Forbidden
		404	NotFound
2xx	Successful	405	MethodNotAllowed
200	OK	406	NotAcceptable
		407	ProxyAuthenticationRequired
3xx	Redirection	408	RequestTimeout
300	MultipleChoices	409	Conflict
301	MovedPermanently	410	Gone
302	MovedTemporarily	411	LengthRequired
305	UseProxy	413	RequestEntityTooLarge
380	Alternative Service	414	Request-URITooLong
		415	UnsupportedMediaType
5xx	Server Failure	420	BadExtension
500	ServerInternalError	480	TemporarilyUnavailable
501	NotImplemented	481	CallLeg/TransactionDoesNotExist
502	BadGateway	482	LoopDetected
503	ServiceUnavailable	483	TooManyHops
504	GatewayTime-out	484	AddressIncomplete
505	VersionNotSupported	485	Ambiguous
		486	BusyHere
		6xx	Global Failures
		600	BusyEverywhere
		603	Decline
		604	DoesNotExistAnywhere
		606	NotAcceptable

Note: 1xx codes are not final
2xx - 6xx are final

Structure IETF pour les réseaux à commutation de paquets SIP



SIP : session initiation protocol

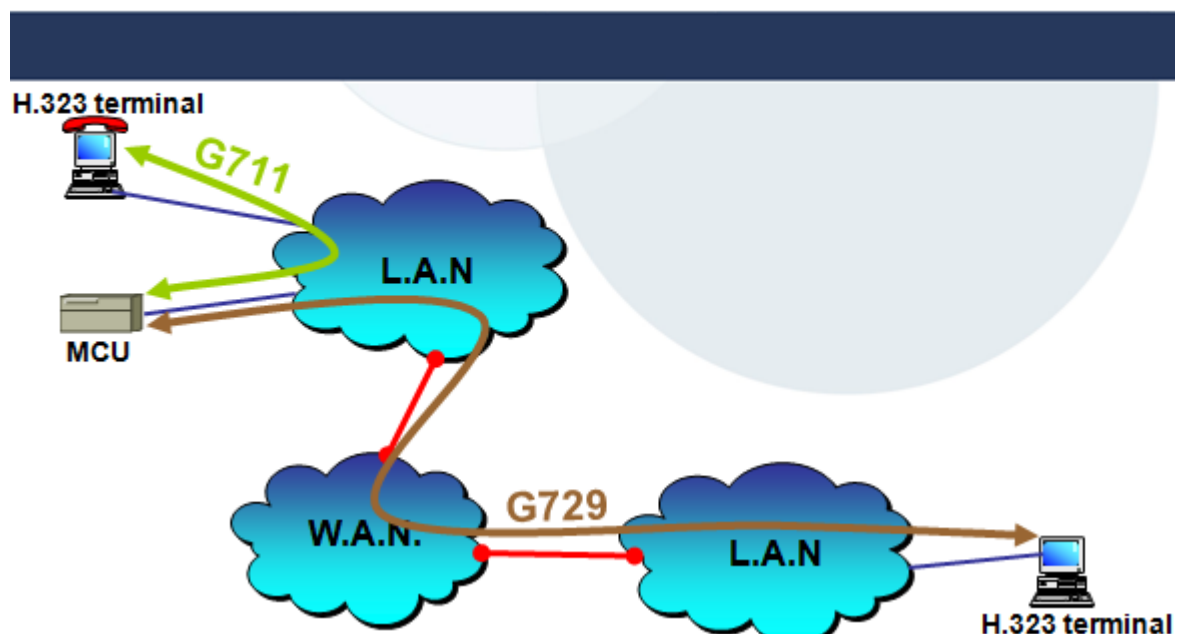
LAN, intranet, Internet

les champs necessaire du RTP :

Champs nécessaires

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ver		P	X	CC		M		PT							Sequence Number																
Timestamp																															
SSRC (Synchronization Source) Identifier																															
CSRC (Contributing Source) Identifier																															
Defined by the Profile																Length															
Header Extension (Optional)																															
Payload																															
x	x	x	x	x	x	x	x	x	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

Transcodage contrôlé par la MTU



Transcodage contrôlé par la MCU

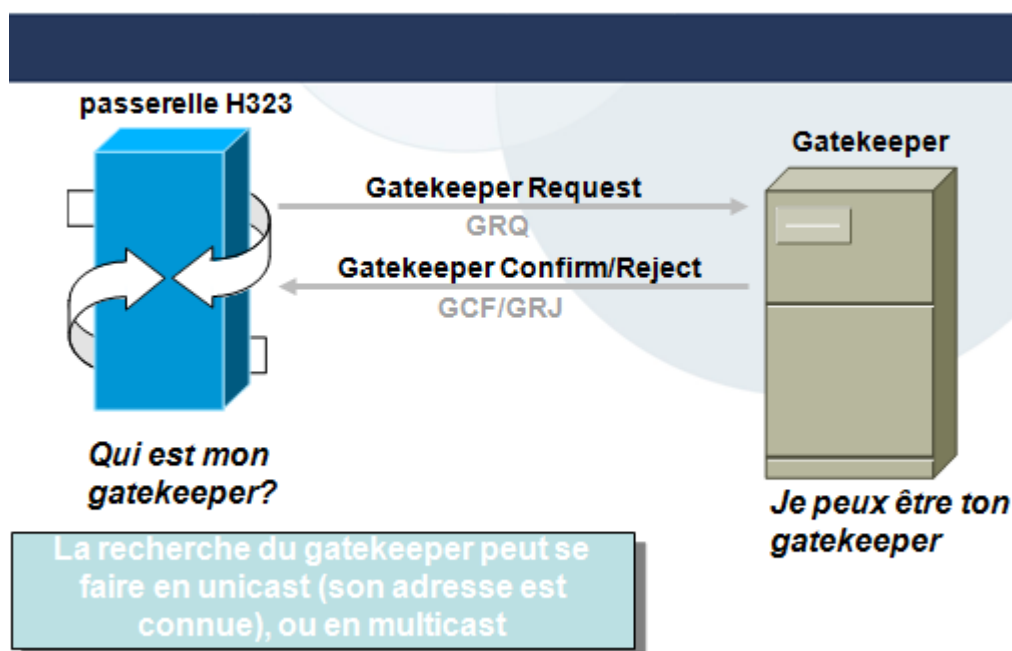
La fonction de transcodage de la MCU est utilisée par certains constructeurs pour traduire le G.711 en G.729 quand l'appel passe par un réseau WAN. En ayant une MCU réalisant cette tâche, les terminaux H.323 n'ont pas besoin d'être équipés avec des DSPs puissants qui doivent d'autre part réaliser la compression de la voix. De plus, la MCU procure le RTP rendant le réseau plus sécurisé. Notez que le G.729 est envoyé vers le « mixer » et ce dernier convertit le G.729 en G.711.

Découverte de la gatekeeper:

Avant qu'un terminal puisse s'enregistrer auprès d'une gatekeeper, il doit d'abord trouver la gatekeeper. Il y a trois méthodes pour permettre aux terminaux de trouver la gatekeeper :

- Chaque terminal est programmé avec l'adresse statique de la gatekeeper.
- La gatekeeper est identifiée avec un nom complet qui est manuellement saisi sur chaque terminal.
- Chaque terminal envoie un message à l'adresse multicast 224.0.1.41:1718. Cela nécessite que le réseau supporte le multicast et que la gatekeeper reconnaisse le terminal qui a envoyé le message multicast. Si l'administrateur a configuré la gatekeeper pour ne servir que certains terminaux, alors la gatekeeper supprimera sans prévenir le message. La méthode automatique de localisation d'une gatekeeper utilise l'adresse IP multicast 224.0.1.41:1718.

Découverte de la Gatekeeper



RAS = Registration/Admission/Status

Cette méthode apporte une aide pour la récupération d'urgence au cas où une gatekeeper tombe en panne et qu'une seconde gatekeeper doit être trouvée. Puisque la requête Multicast GRQ (GATEWAY REQUEST) sera reçue par toutes les gatekeepers, une seconde gatekeeper peut rapidement être localisée en utilisant cette technique. Cette technique réduit aussi la quantité d'administratif induit par la configuration de toutes les stations finales avec l'adresse IP valide de la gatekeeper.

La gatekeeper peut répondre à un message GCF (Gatekeeper Confirm), indiquant l'adresse IP unicast de la gatekeeper. Le message GCF peut aussi contenir les adresses IP de toutes les autres gatekeepers qui peuvent agir en tant que backup si l'une d'entre elles tombe en panne.

Si un terminal reçoit plusieurs messages GCF, il peut sélectionner n'importe quelle gatekeeper mais pas toutes.

Il est aussi possible pour une gatekeeper d'envoyer un message GRJ (GATEKEEPER REJECT) si elle n'a pas le droit d'enregistrer cette gatekeeper.

Messages échangés entre les composants H323 :

a. Le message RPQ:

Le message RRQ (REGISTRATION REQUEST) est la fiche d'information officielle contenant les données à ajouter dans la base de données de la gatekeeper. Si l'enregistrement aboutit, le terminal est intégré à la zone couverte par la gatekeeper.

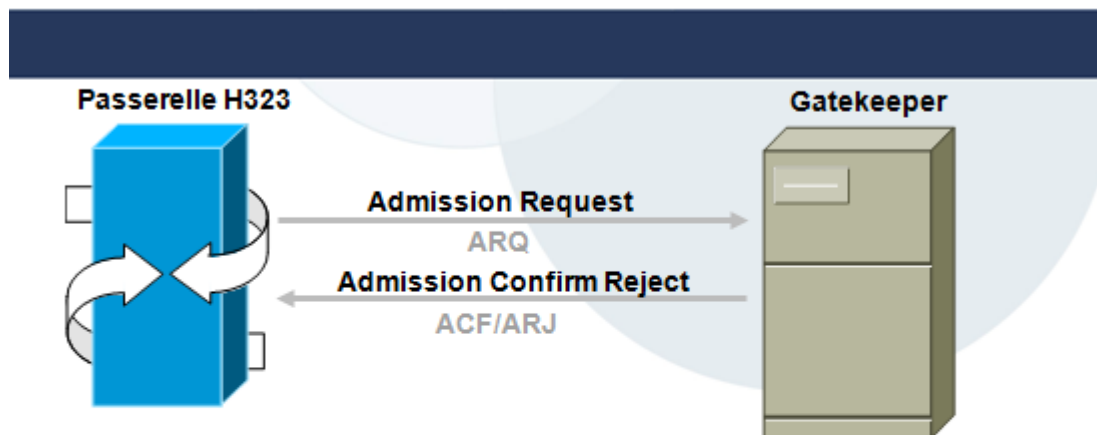
L'information d'enregistrement peut contenir plus d'informations que ce qui est présenté ci-dessus. L'enregistrement peut contenir des adresses E.164 multiples et les alias ce qui est le cas de la plupart des passerelles pouvant être servies par des téléphones multiples de trunks.

La requête d'enregistrement peut aussi contenir la durée de vie de certains enregistrements de sorte que quand la durée de vie expire, l'enregistrement prend fin. Cela permet à un périphérique de se réenregistrer périodiquement et de garder son enregistrement actif, ou simplement en ne se réenregistrant pas, de mettre fin à l'enregistrement.

- **Exemple d'admission request:**

La gatekeeper rend plus facile la mise en place des appels. Une fois que l'émetteur a composé le numéro du destinataire, le terminal H.323 envoie une requête ARQ (ADMISSION REQUEST) à la gatekeeper. Cette requête contient les informations clés listées ci-dessus pour identifier l'appelant et l'appelé.

Exemple : ADMISSION REQUEST



Où est 4000 ?

A cette adresse IP.

C'est le Gatekeeper qui fait l'association d'un numéro avec l'adresse IP (soit avec un terminal H323 soit avec la passerelle H323)

b. Le message Setup:

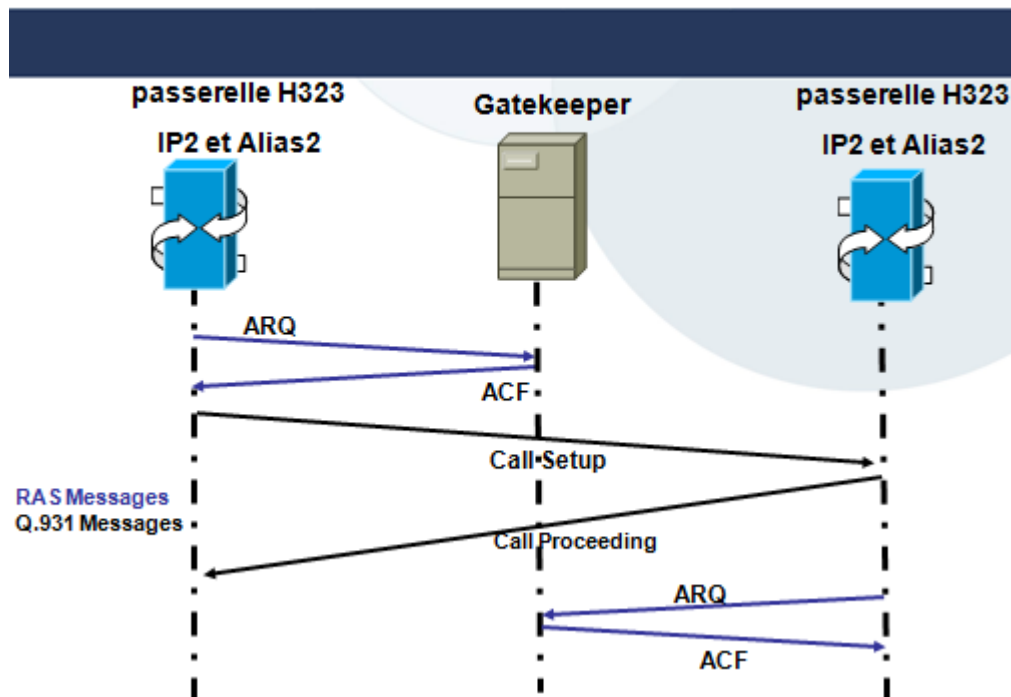
Puisque la gatekeeper fournit au terminal la socket H.225 de l'appelé, le message SETUP est envoyé directement à l'appelant. Le message SETUP contient au moins deux IE (Information Elements). Il y a les numéros de l'appelé et de l'appelant dans le message SETUP et son « self-explanatory ». Plusieurs constructeurs incluent maintenant les informations du profil RTP dans le message SETUP, qui sauvegarde plus tard les codecs de négociation de temps.

L'appelé n'est pas sûr que l'appelant est un appelant légitime. Plutôt que de supposer que l'appel est acceptable, l'appelé retourne un message de réponse évasif appelé CALL PROCEEDING. CALL PROCEEDING signifie que l'appel est en cours mais il n'est pas encore déterminé si le téléphone est libre ou occupé.

Le message ARQ confirme que la Gatekeeper est en train de se charger de l'appel. Cela permet de s'assurer qu'un utilisateur malicieux n'est pas en train de leurrer le système avec un faux message.

Le message ACF confirme que l'appel est valide et que la Passerelle H323 IP2-alias2 peut traiter la demande

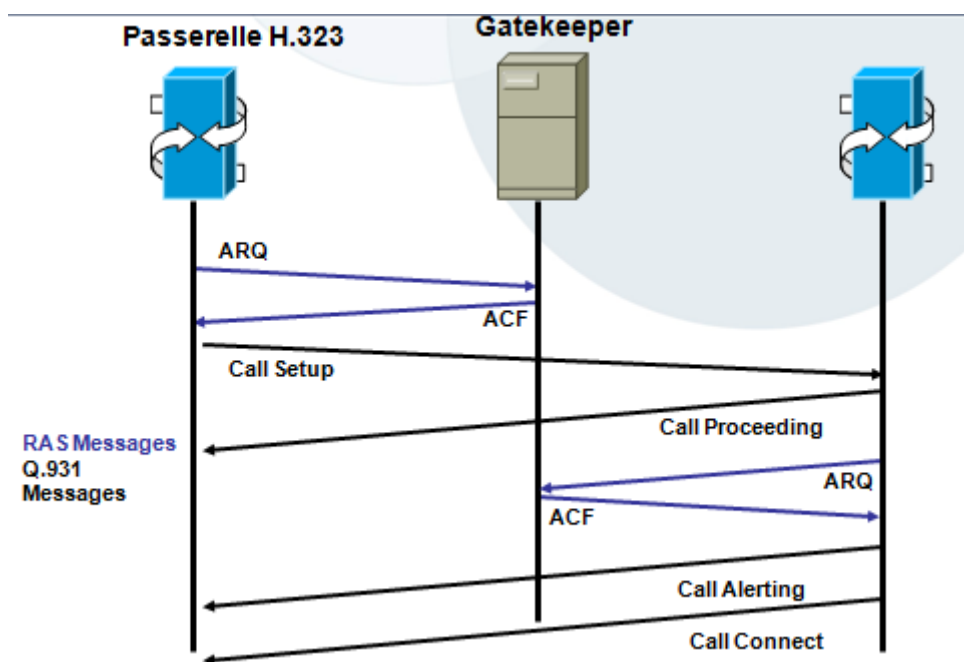
SETUP



c. le message Alerting et connect:

Le message ALERTING indique que le téléphone est en train de sonner. Puisque la gatekeeper utilise une signalisation finale directe, le message ALERTING est envoyé directement au terminal appelant. Si le routage contrôlé par la gatekeeper est activé, alors le message est routé vers la gatekeeper.

Le message CONNECT indique qu'on a répondu à l'appel.



BIBLIOGRAPHIE :

I.OUVRAGES :

1. Grinsec, la communication electronique tome 1.Edition EYROLL 1985
2. S H Hermouti et al , reseaux locaux et telephonie, edition MASSON
3. Jerome D : comment trouver sa voix sur IP . edition janvier 2006
- 4.Tim K , VOIP pour les nuls Avaya2005

II SITES INTERNET :

1. [http //www.Oreilly net.com](http://www.Oreilly_net.com)
- 2.[http//www .voipinfo.org /wikiasterix+tips+and+ triks.](http://www.voipinfo.org/wikiasterix+tips+and+triks)
3. [http//www.remichauchat.fr/project/Voip/bureau% 20 d'etude%20Voip.pdf](http://www.remichauchat.fr/project/Voip/bureau%20d'etude%20Voip.pdf)
- 4.[http//www.effort.com](http://www.effort.com)
- 5.[http//www.espacespourlesespaces.ca/glossaire/hi.htm.](http://www.espacespourlesespaces.ca/glossaire/hi.htm)
6. [http// iptel.org](http://iptel.org)Portail de la téléphonie sur IP
- 7.[http//fr .wikipedia.org/wiki/voix](http://fr.wikipedia.org/wiki/voix) sur réseau IP
- 8.[http:// dictionnaire.phpmyvisites.net/definition_telephonie8ip85109.htm](http://dictionnaire.phpmyvisites.net/definition_telephonie8ip85109.htm)
- 9.[wwwjournaldunet.com/solutions/050119](http://www.journaldunet.com/solutions/050119) terminologie toip.shtml

Résumé

L'objectif de notre projet de fin d'études est de faire une recherche détaillée sur la procédure d'implémentation d'un call center IP dans le réseau GSM.

C'est en prenant appui sur le stage effectué au sein de l'entreprise ORASCOM TELECOM ALGERIE que nous avons axé notre travail, le présent rapport est organisé en quatre chapitres :

Le premier chapitre est scindé en deux parties : la première est consacrée à la présentation générale du call center ainsi que ses principales fonctionnalités. La seconde partie s'appuie sur le concept de migration du PABX vers un réseau PABX IP / VOIP.

Le deuxième chapitre est essentiellement consacré à la VOIP et la TOIP ainsi que leurs fonctionnalités. Le troisième chapitre traitera les différentes architectures du Call Center IP et des pratiques de sécurisation. Le dernier chapitre résumera les différentes interconnexions du call center avec le réseau GSM.