Ministère des Enseignements Secondaire,
Supérieur et de la Recherche Scientifique
(MESSRS)

Université Polytechnique de Bobo–Dioulasso
(UPB)

Ecole Supérieure d'Informatique
(ESI)

Cycle des Ingénieurs en Travaux Informatiques
(CITI)

Option : Réseaux et Maintenance Informatiques
(RéMI)

Burkina Faso
Unité-Progrès-Justice

Centre SIG et Télédétection Adjaratou

05 BP 6154 Ouagadougou 05
Tel : 0022650458880 / 00022650367066
E-mail : siget-a@fasonet.bf

Projet de fin de cycle

THEME : ***ETUDE ET PROPOSITION DE SOLUTION POUR LA MISE EN PLACE D'UN SYSTEME DE COMMUNICATION ToIP AU CENTRE SIGET-A***

Présenté et soutenu par :
KIENTEGA Simon et SIDIBE Guéréguin Der Sylvestre
Etudiants en 3ième année ESI/RéMI

Maître de stage
Yassia SAVADOGO
Ingénieur en Réseaux et Système

Superviseur
M. Tiguiane YELEMOU
Enseignant à l'ESI

Année académique 2009 – 2010

DEDICACE

Nous dédions ce présent rapport à :

- *DIEU tout puissant qui a toujours veillé sur nous ;*
- *Nos parents respectifs qui nous ont toujours soutenus dans nos études ;*
- *Tous ceux qui nous ont apportés leur soutien*

REMERCIEMENT

Un grand merci à tout ceux qui d'une manière ou d'une autre nous ont soutenus dans l'établissement de ce document ; par le partage de connaissance, par leur encouragements pour tous les efforts fournis à notre endroit. Qu'ils voient en ce document le fruit de leur contribution.

Nos remerciements vont en particulier à :

- M. Patrice SANOU Directeur Général du centre de Système d'Information et de Télédétection Adjaratou (SIGET-A) qui a placé sa confiance en nous, en nous acceptant dans sa structure ;
- M. Tiguiane YELEMOU enseignant à l'ESI en sa qualité de superviseur ;
- M. Yassia SAVADOGO en sa qualité de maitre de stage pour son suivi et ses apports ;
- L'Ecole Supérieur d'Informatique pour la formation reçue ;
- L'ensemble du personnel de SIGET-A ;
- Nos chères familles, nos proches et nos connaissances qui nous ont apportés leur soutien de toute nature durant nos trois ans de formation dans la ville de SIA.

Sommaire

Table des figures

Table des tableaux

Liste des sigles et abréviations

ADLS: Asymetric Digital Subscriber Line

BIOS: Basic Input Output System

CAA: Commutateur à Autonomie d'Acheminement

CPU: Central Processing Unit

CTI: Commutateur de Transit International

CTP : Commutateur de Transit Principal

CTS : commutateur de Transit secondaire

ESI: Ecole Supérieure d'Informatique

FAI: Fournisseur d'Accès à Internet

FXO: Foreign eXchange Office

FXS: Foreign eXchange Station

HP: Hewlett Packard

HTTP: Hyper Text Transfer Protocol

IAX: Inter-Asterisk eXchange

IP-PBX ou IPBX: IP Private Branch eXchange

LAN: Local Area Network

LDAP: Lightweight Directory Access Protocol

NAT: Network address translator

ONATEL: Office National des Télécommunications

OSI: Open System Interconnect

PABX ou PBX: Private Automatic Branch eXchange

PC: Personal Computer

QoS: Quality of Service

RAM: Random Access Memory

RNIS : Réseau Numérique à Intégration de Service

RTC: Réseau Téléphonique Commuté

RTCP: real Time control Protocol

RTP: Real Time Protocol

SIG : Système d'Information Géographique

SIP: Session Initiation Protocol

SSL: Secure Socket Layer

TCP: Transmission Control protocol

ToIP: Telephony over Internet Protocol

UDP: User Datagram Protocol

UPB: Université Polytechnique de Bobo-Dioulasso

URL: Uniform Resource Locator

VoIP: voice Over IP

VLAN: Virtual LAN

VPN: Virtual Private Network

WAN: Wide Area Network

Avant propos

L'Université Polytechnique de Bobo-Dioulasso (UPB) fut créée en 1995 dans le but de décentraliser la formation universitaire qui était centrée à l'Université de Ouagadougou. Elle a pour objectif de donner une formation professionnelle aux étudiants.

L'UPB comprend actuellement cinq (05) instituts et une (01) école qui sont :

- L'institut de Développement Rurale (IDR)
- L'Institut Universitaire de Technologie (IUT)
- L'Institut des Sciences Exactes et Appliquées (ISEA)
- L'Institut des sciences de la Nature et de la Vie (ISNV)
- L'institut Nationale des Sciences de la Santé (INSSA)
- L'Ecole Supérieure d'Informatique (ESI)

L'Ecole Supérieure d'Informatique (ESI) dès sa création en 1991 a d'abord été implantée à Ouagadougou, et fut transférée ensuite au sein de l'UPB en septembre 1995. Sa mission première est d'accompagner le pays dans son ambition de s'approprier les technologies de l'information et de la communication. Elle a pour mission également la formation fondamentale, appliqué et/ou professionnelle dans les domaines de l'informatique, la formation continue. Elle a pour vocation, la recherche scientifique et technologique ainsi que la valorisation des résultats de la recherche, la diffusion de la culture de l'information dans le domaine relevant de sa compétence. La collaboration avec d'autres structures de formation et/ou de recherche pour la préparation des diplômés et la participation à des programmes internationaux de formations et de recherche.

L'ESI offre trois cycles de formation à savoir :

- Le cycle du Diplôme d'Etudes Approfondies (DEA) créé en 2003 et qui se trouve actuellement suspendu.
- Le cycle des Ingénieurs de Conception en Informatique (CICI)

- Le Cycle des Ingénieurs de Tavaux en Informatique (CITI) qui comprend deux filières: l'Analyse et Programmation (AP) qui existe depuis la création de l'école et le Réseau et Maintenance Informatique (RéMI) créé en octobre 2000 avec le soutien de la coopération Française.

Pour une formation efficiente, l'ESI intègre dans le cursus de formation un stage pratique de douze (12) semaines en entreprise.

Introduction générale

La téléphonie sur IP constitue actuellement une des plus importantes évolutions dans le domaine des télécommunications. Il y a quelques années, la transmission de la voix sur le réseau téléphonique classique ou RTC constituait l'exclusivité des télécommunications. Aujourd'hui, la donne a changé. La transmission de la voix via les réseaux IP constitue une nouvelle évolution majeure comparable à la précédente. Au delà de la nouveauté technique, la possibilité de fusion des réseaux IP et téléphoniques entraîne non seulement une diminution de la logistique nécessaire à la gestion des deux réseaux, mais aussi une baisse importante des coûts de communication ainsi que la possibilité de mise en place de nouveaux services utilisant simultanément la voix et les données.

Le présent thème soumis à notre étude entre dans le cadre de notre projet de fin de cycle de trois (03) mois en entreprise pour l'obtention du diplôme d'ingénieur de travaux en informatique, option Réseaux et Maintenance Informatiques. Exécuté au centre SIGET-A, sur une période allant du 25 octobre 2010 au 07 janvier 2011 n'ayant pas couvert les trois (03) mois prévus pour des contraintes de temps, il traite de la mise en place d'un système de communication ToIP.

Ce rapport s'articulera autour de quatre grandes parties essentielles :

La première partie consistera à la présentation de la structure d'accueil et du thème qui sera l'objet de notre travail.

La deuxième partie sera consacrée à l'étude du thème où nous allons parler des éléments clé nécessaires pour la mise en place d'un tel système et les différents aspects à prendre en compte pour une fiabilité du système.

La troisième partie sera question de la présentation de la solution

Enfin la quatrième partie traitera de l'évaluation des coûts pour la mise en place du système.

PREMIERE PARTIE : Présentation de la structure d'accueil et du thème

PREMIERE PARTIE : Présentation de la structure d'accueil et du thème

I. Présentation de la structure d'accueil

I.1. Historique

Toute expérience, si petite soit-elle est une propriété de la communauté à laquelle nous appartenons. Il devient alors un devoir de la rendre disponible à l'usage de la société. En Août 1995, lorsque après sa « graduation »il était sur la route du retour au Burkina et se prêtant à l'exercice de briefing final avec son program manager de African American Institute, Monsieur Patrice SANOU, concepteur du centre Adjaratou avait promis la valorisation des SIG de l'aide USAID au Burkina et en Afrique.
Dans cette optique, la formation a vite occupé une grande place dès le retour de l'intéressé. En effet, il fut l'expert principal du réseau PNGIM qui forma plusieurs structures nationales en SIG (BUNASOLS, Météorologie Nationale, Impôts/Cadastre, BUMIGEB, Université Ouagadougou, INSD, INERA, DRED, ARMEE, projets, indiv idus, etc.).
L'engouement se faisant grandissant, il fut indispensable en 2001 de créer une structure qui valorise et canalise l'ensemble des énergies développées pour que les SIG et la télédétection soient adoptés comme outils de production d'information, d'aide à la décision, donc de bonne gouvernance. La disparition brutale le 9 mars 2000 de la compagne du fondateur, Madame Adjaratou SANOU qui participait à la mise en œuvre de cette volonté scientifique, donnera une raison supplémentaire mais suffisante de fonder le 1er janvier 2001 le Centre SIG et Télédétection Adjaratou (SIGET-A), celle de rendre hommage à toutes les femmes qui participent anonymement aux inventions et initiatives du monde.
Depuis le 1er septembre 2008, le centre a franchi un seuil essentiel de son importance et de son rôle dans le développement de la géomatique. En ouvrant l'enseignement diplômant en technologies spatiales, le centre Adjaratou s'approprie sans adversaire le titre de « Leader de la géomatique en Afrique ».

I.2. Structuration

Le Centre SIGET-A est structuré de la façon suivante :

- **Le Conseil Scientifique (CS)**

  Il définit les normes scientifiques appliquées en expertise, formation et enseignement. Il assure le suivi contrôle de la mise en œuvre de ces normes dans les plans et programmes. Toute évaluation ou validation scientifique en expertise, formation et enseignement relève du domaine exclusif du conseil scientifique.

- **Le Conseil Général de Gestion (CGG)**

  Il est l'organe de contrôle des activités et de la gestion du centre. Il valide les programmes et plans d'action définis par la direction générale, statue sur les rapports financiers et moraux présentés par la direction générale.

- **La Direction générale**

  La Direction Générale du centre SIGET-Adjaratou est chargée du développement, de l'analyse et de la validation des relations de partenariat. Elle assure les investissements et le développement du groupe. Elle analyse, évalue et valide les activités, les rapports, les budgets.

- **L'Unité de Géo-information et des Télécommunications (UGITEL)**

  Cette unité s'occupe de l'expertise du centre en réalisant des études et recherches/développement. Elle assure le développement et l'application des technologies spatiales dans toutes les thématiques. L'UGITEL assure des formations courte durée et réalise les produits géomatiques (bases de données, cartes numériques et/ou analogiques).

- **L'Institut Supérieur d'Etudes Spatiales et Télécommunication (ISESTEL)**

Elle développe l'enseignement supérieur des technologies spatiales dans trois cycles: cycle « brevet de technologies spatiales », cycle « licence avancée de technologies spatiales » et le cycle « master scientifique de géo-information ».

La Bibliothèque des Technologies Spatiales (BTS)

La bibliothèque assure des missions assez spécifiques pour non seulement faire la promotion des technologies spatiales et offrir des prestations assimilées mais aussi créer les conditions documentaires d'amélioration de l'apprentissage. Ainsi, elle assure des activités de bureautique (internet, photocopie, impression, saisie, communication), de marketing des capacités du centre (enseignement, formation, expertise, distribution) et de vente de produits et outils géomatiques du centre (bases de données, cartes, logiciels ESRI), offre et gère une documentation technique, même électronique, au profit des étudiants et enseignants.

- **La Fondation Adjaratou pour la Géomatique (FAG)**

Cette fondation est une association de personnes présentes ou hors du centre voulant contribuer à la promotion de la géomatique. Elle s'occupe du développement et de la gestion des œuvres sociales et ou techniques au profit des étudiants, des enseignants et tout praticiens de la géomatique. Elle mène ainsi une action de recherche de bourses, aides et soutiens pour les étudiants en besoin pour la prise en charge de leurs études. Elle sponsorise aussi des formations géomatiques initiatiques au profit des étudiants et élèves. Elle développe toute relation utile au développement et à l'adoption de la géomatique.

I.3. Objectifs

Structure Privée Burkinabè de Recherche, de Formation et d'enseignement Technique et Scientifique, le Centre SIGET-Adjaratou est une Société à Responsabilité

Limitée (SARL) qui vise essentiellement la promotion de la Géo-information, une science qui utilise les technologies spatiales pour la connaissance, l'analyse, et la gestion automatisée (informatique) des données spatiales. Le centre assume cette mission à travers la formation, l'enseignement, l'appui conseil et la réalisation des études et recherches pour le développement et la bonne gouvernance.

I.4. Compétences technique

Le centre dispose de plusieurs compétences technique, tant sur le plan national qu'international.

Sur le plan national, nous avons des Géomaticiens/Cartographes, Géographes/Historiens, des Agronomes, des Pédologues/climatologues, des Environnementalistes, des Forestiers, Hydrauliciens des Sociologues/philosophes, des Economistes, etc.

Sur le plan international, nous avons GeoImages Solutions / Canada, Brown University / USA, etc.

I.5. Domaines d'activité

Le centre SIGET-A œuvre dans plusieurs domaines d'activités :

- **Formations / Enseignement supérieur**

  Nous avons La formation courte durée (1 à 3mois), la formation à la demande (1 à 3 semaines) et la formation diplômant (technicien supérieur, bachelor et master)

- **Etudes et applications des outils**

  Gestion et suivi des ressources naturelles, suivi écologique, gestion des catastrophes naturelles et humaines, analyse des sols, la photo interprétation, traitement d'images satellite, etc.

- **Travaux Régionaux importants**

  Nous pouvons citer la gestion du système d'information environnemental de la zone de l'Autorité du Liptako Gourma, celui pour l'aménagement du territoire de l'UEMOA et l'analyse de potentiels économiques de développement de réseaux de téléphonie mobile (Burkina, Niger, Tchad, Gabon, Sierra Leone, Zambie) de CELTEL/ZAIN International.

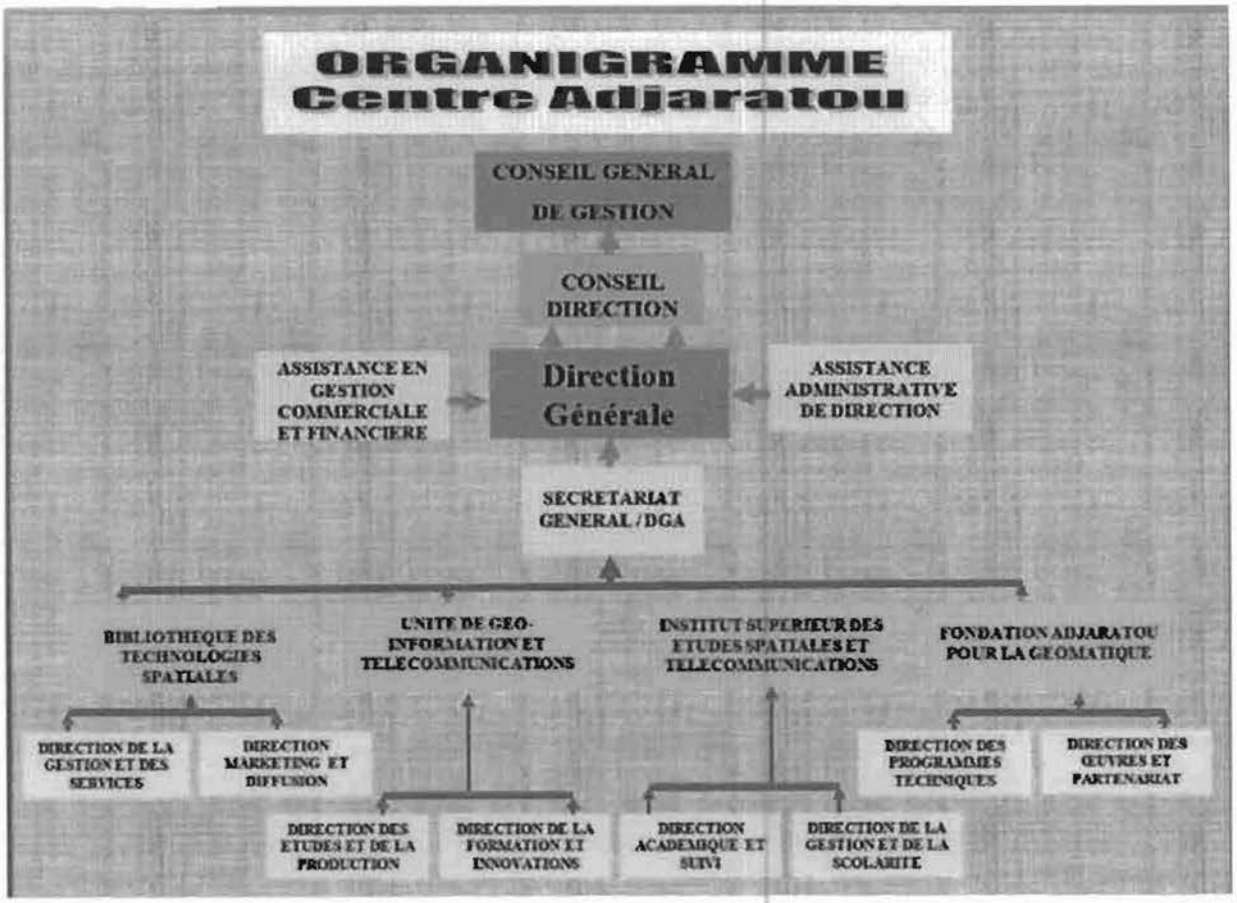
I.6. Partenaires

Le Centre SIG Et Télédétection Adjaratou (SIGET-A) entretien depuis sa création de multiples relations de partenariat, ce qui le positionne sans doute leader dans le domaine de télédétection dans la sous région. En effet, sur le continent Africain, nous pouvons citer : INFOCOM, BUNASOLS, Météorologie Nationale, BUMIGEB, Université Ouagadougou, INSD, INERA, ZAIN, PDRSO...

Le Centre SIGET-A travaille déjà en étroite collaboration avec un certain nombre d'institutions internationales présentes au Burkina Faso (l'Ambassade des Etats Unis, la GTZ...) et des partenaires internationaux tels que TECSULT pour le Canada, le Centre AGRHYMET pour le Sahel...) mais souhaiterait étendre le réseau de ses partenaires sur la scène internationale.

Le Centre est également le représentant exclusif d'IGE, PixoneerGeomatics, BERD, SCL et d'ESRI-France pour la distribution des logiciels de SIG et de Télédétection au Burkina Faso, le Mali et le Niger.

I.7. Organigramme



II. Présentation du thème

En vu de s'aligner au rang des nouvelles technologies et de bénéficier des nombreux avantages qu'offre la téléphonie sur IP notamment en matière de réduction des coûts de communications, plus intéressante pour les organismes multi-sites, le centre SIGET-A s'est vu intéressé par l'idée d'adoption de la technologie de transmission de la voix sur IP pour la communication entre ses différentes représentations à savoir celles de Bobo-Dioulasso en projet, du Mali et du Niger. La mise en place d'un tel projet requiert au préalable un certain nombre de matériels à savoir des IPBX, des terminaux téléphoniques IP, l'ensemble à installer sur les sites.

Il s'en suit la gestion des appels externes en les faisant transiter par le réseau RTC.

La mise en place d'une solution ToIP nécessite du matériel (ordinateur, terminaux téléphoniques, cartes téléphoniques, ...) et des logiciels (gestion des communications, terminaux téléphonique, ...). L'offre en matière de logiciels de téléphonie est élevée compte du potentiel économique que présente le marché de la ToIP. Dans cette offre de logiciels, on retrouve soit des logiciels propriétaires conçus par des sociétés dont les codes sources sont fermés ou des logiciels libres développés par des communautés de développeurs dont les codes sont accessibles à tout le monde. Qu'ils soient propriétaires ou libres, les logiciels offrent pratiquement les mêmes services et supportent les mêmes standards de la téléphonie sur IP, notamment en matière de protocole de signalisation et de codecs. Pour notre cas, nous axerons une recherche de solution basée sur les logiciels libres qui offrent l'avantage d'être le plus souvent gratuits.

L'objectif est de remplacer la solution téléphonique existante par une solution de voix sur IP qui apporte de nombreux avantages.

DEUXIEME PARTIE : Etude du thème

DEUXIEME PARTIE : ETUDE DU THEME

I. Etude de l'existant et besoin du centre

Le centre SIGET-A dispose de deux réseaux à savoir le réseau téléphonique pour la transmission de la voix et le réseau IP pour la transmission des données numérique.

I.1. Le réseau téléphonique interne

Le réseau téléphonique interne est constitué d'un PABX pour la gestion des appels internes et de terminaux téléphoniques classiques permettant de lancer les appels. A cela s'ajoute les téléphones portatifs de l'ONATEL qui ont un fonctionnement similaire aux téléphones portables en ce sens que la facturation de la communication n'est pas mensuelle. Ce dernier est indépendant du premier. Les équipements de téléphonie disponible sont donnés dans le tableau ci-dessous.

	Equipements	Caractéristiques
Directeur Général	Terminaux	✓ Panasonic KXTS500MXW ✓ HUAWEI ETS2258
Directrice Adjointe	Terminal	Panasonic KXTS500MXW
Secrétaire	Terminaux	✓ Panasonic KX-T7730 ✓ HUAWEI ETS2258
Département Expertise et Application Technologique	Terminal	Panasonic KXTS500MXW
Département Développement des connaissances	Terminal	Panasonic KXTS500MXW
Local Technique	✓ Terminal ✓ Spliter ✓ PABX	✓ Euroset ✓ HENR POUYET ✓ ADVANCED HYRID SYSTEM KX-TA308

Tableau 1 : Matériel de télécommunication

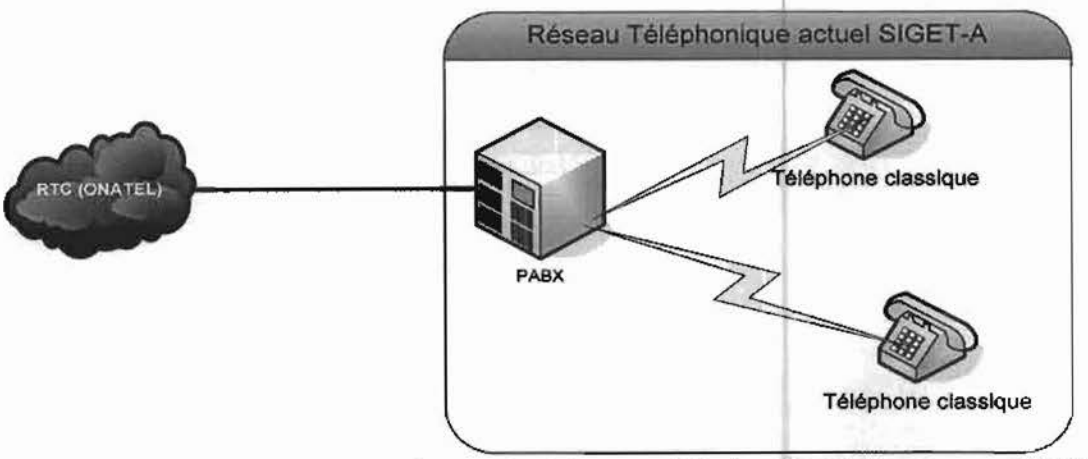


Figure 1 : Réseau téléphonique du centre SIGET-A

I.2. Le réseau IP

Le réseau IP est bâti sous la technologie wifi. Il est constitué d'un modem router wifi avec une connexion ADSL pour accès à internet. Tous les ordinateurs sont équipés chacun d'une carte d'extension wifi ou d'une clé wifi Dlink DW110. Les différents éléments entrant dans la constitution du réseau sont représentés dans les tableaux ci-dessous.

Tableau 2 : La Direction Générale

	ordinateur	caractéristiques	Périphérique
Directeur Général	HP		Imprimante HP Deskjet D 1460
Directrice Adjointe	DELL Optiplex 210L	Pentium IV RAM 512MO, DD OS : windows XP SP2	Onduleur Mercury 1100C, imprimante HP
Secrétariat	IBM	Pentium III RAM : 256MO, DD OS : Windows XP SP2	Imprimante HP Laserjet 1020, onduleur Mercury 1100C

Tableau 3 : La Boutique des Technologies Spatiales

Equipements	Marque	caractéristiques	périphériques
3 ordinateurs	Diplo	Pentium IV RAM: 512MO, DD: 40GO OS: Windows XP SP2	2 Imprimantes Scanner HP Deskjet F2180
2 ordinateurs		Pentium IV Dual	Imprimante HP Deskjet D1460 et HP Laserjet 1020
3 onduleurs	Mercury		
photocopieuse			
Imprimante A4 à A0	HP Designjet 500		

Tableau 4 : Le Département Développement des Connaissances

intitulés	équipements	Marque	caractéristiques
Salles de formations	18 ordinateurs	Fujitsu Siemens	Pentium R Dual RAM : 1Go, DD : OS : Windows XP SP2
	18 onduleurs	Mercury	
Salle d'étude	5 ordinateurs	Fujitsu Siemens	Pentium R Dual RAM : 1GO, DD OS : Windows XP SP2

Tableau 5 : Le Département Recherche et Innovation Technologique

intitulés	équipements	Marque	Caractéristiques
Laboratoire Technique	1 ordinateur	DELL Optiplex	Pentium IV RAM : 512MO ; DD : OS : Windows XP SP2
	1 imprimante		
	1 onduleur		
	1 Table de Numérisation		
Salle Etude et Collecte de Données	2 ordinateurs	IBM	Pentium IV RAM : 256MO ; DD OS : Windows XP SP2
	GPS		

Le réseau actuel du centre SIGET-A est illustré dans le schéma ci-dessous :

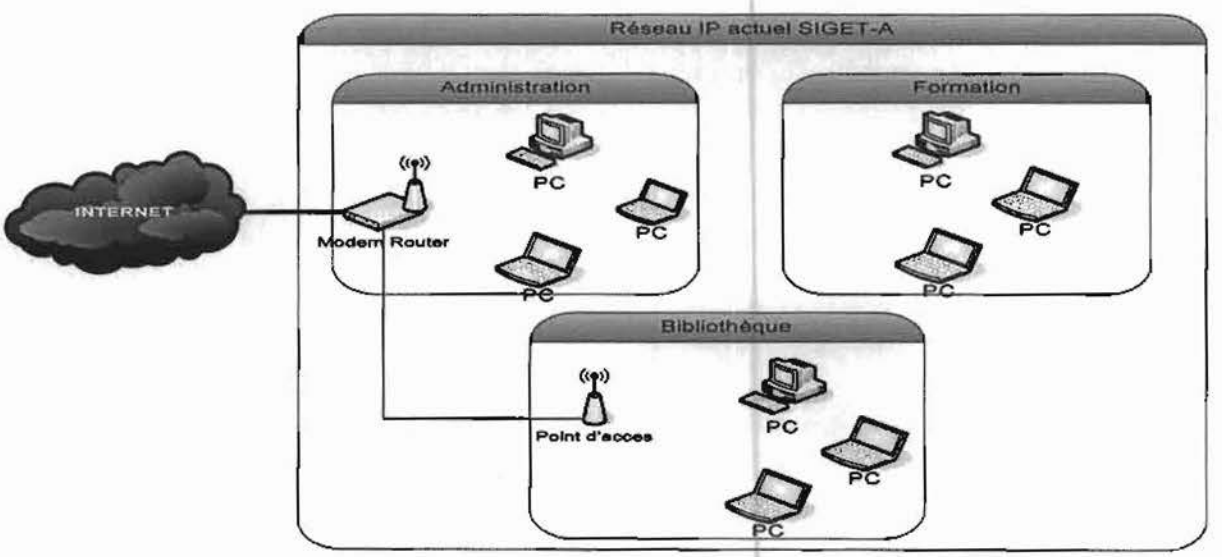


Figure 2 : Réseau IP de SIGET-A

Après une étude approfondie menée sur la mise en place du réseau du centre SIGET-A par nos collègues prédécesseurs M. MILLOGO Souleymane et M. BAYALA Béranger, qui

devra répondre aux exigences de la mise en place d'une vidéo conférence, l'architecture réseau suivant a été retenue.

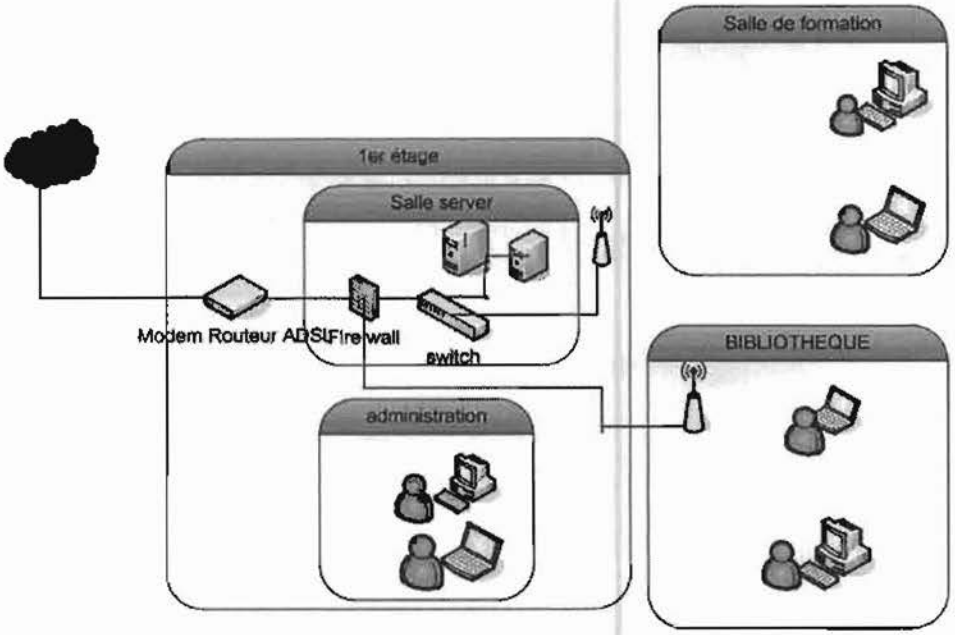


Figure 3 : Architecture réseau future

I.3. Besoin du centre SIGET-A

SIGET-A est un centre disposant de plusieurs représentations dans la sous région notamment au Mali et au Niger. En interne un projet d'installation d'une représentation à Bobo-Dioulasso est en vu. Le besoin d'organiser et de coordonner les activités entre ces différentes représentations nécessite une communication permanente intersites. Ces communications engendrent des factures à valeurs exorbitantes à la structure avec le système de téléphonie classique. Le centre SIGET-A, représentant exclusif d'IGE, PixoneerGeomatics, BERD, SCL et d'ESRI-France pour la promotion et la distribution des logiciels de SIG et de Télédétection au Burkina Faso, au Mali et au Niger, s'est montrer favorable à l'idée d'adoption d'une solution de mise en place d'un système de communication de Téléphonie sur IP qui couvrira ses différents sites; une technologie parfaitement adaptée aux organismes multi-sites pour une réduction considérable des frais de communications. Outre la réduction, cette technologie regorge encore bien

d'autres avantages qui seront présentés à la suite.

II. La téléphonie sur IP

II.1. Généralité sur la téléphonie

II.1.1. Historique

La téléphonie fait depuis longtemps partie de l'histoire. Du premier "téléphone à ficelle" à l'ouverture de la "boucle locale", retour rapide sur l'histoire de la téléphonie du 17éme siècle à nos jours.

C'est au 17éme siècle qu'un physicien anglais Robert Hooke évoqua pour la première fois le principe selon lequel il est possible de transmettre un son au travers d'un fil bien tendu et dont les extrémités étaient terminées par un tube de carton ayant un coté fermé par une membrane. Le premier téléphone était né : "le téléphone à ficelle". Depuis lors, ce concept a évidement subi de très nombreuses évolutions. Dès le 18éme siècle, un académicien des sciences présenta un mémoire intitulé "un moyen de communiquer entre deux endroits très éloignés". Ce principe était basé sur l'utilisation des propriétés acoustiques des tubes pour transmettre des sons de l'une à l'autre de leurs extrémités. Ce scientifique est à l'origine des tubes acoustiques qui se sont alors répandus très rapidement dans les châteaux et demeures bourgeoises.

Au 19éme siècle, un employé des télégraphes français publie pour la première fois une note sur "la possibilité de transmettre électriquement la parole". 20 ans plus tard, le 14 février 1876, un professeur de l'université de Boston, l'Américain Graham Bell, déposa aux États-Unis une demande de brevet sur ce même principe.

Ainsi suite à un essai sur une ligne de 10 kilomètres entre Boston et Malden que la commercialisation du téléphone vit le jour. Ce premier téléphone fut mis en service le 1er mai 1877. Elle avait une vocation privée, reliant le bureau d'un homme d'affaire à

son domicile. Graham Bell présenta alors son invention sous une nouvelle forme : le téléphone à main (the Hand Telephone).

Cependant avec la croissance des utilisateurs, il n'est plus concevable d'installer une ligne téléphonique entre chacun d'entre eux. C'est donc tout naturellement que naquit le premier réseau téléphonique qualifié de "commuté". Il n'était pas encore automatisé.

C'était alors une des opératrices (la téléphoniste) du central téléphonique (lieu d'interconnexion des utilisateurs) qui reliait physiquement les abonnés entre eux. Chaque utilisateur était alors identifié par son nom et son numéro d'abonné. C'est à la fin de ce siècle que le premier central semi-automatisé, le central électromécanique, fit son apparition.

Ainsi au 20ème siècle, une des premières innovations majeures fut l'automatisation complète des centraux téléphoniques. C'est à la fin des années 1970 que la majorité des téléphonistes et des centres électromécaniques furent remplacés par des commutateurs entièrement automatiques. Aucune opération manuelle n'était plus nécessaire pour relier deux abonnés. C'est la fin de l'électromécanique et le début de l'électronique.

II.1.2. Le Réseau Téléphonique Commuté

Le RTCP (Réseau Téléphonique Public Commuté ou simplement RTC) est le réseau téléphonique que nous utilisons quotidiennement pour nos communications vocales distantes. En effet, outre le fait de son rôle essentiel qui est de pouvoir transférer la voix, l'évolution technologique a permit un accroissement significatif du nombre de ses services, nous permettant d'utiliser de multiples services tel que la transmission et réception de fax, accéder à Internet etc.

II.1.2.1. Principe du réseau RTC

Le RTC utilise la commutation des circuits, mettant en relation deux abonnés à travers un canal dédié pendant toute la durée de l'échange.

Le RTC comprend deux (02) grandes parties :

- **Le réseau capillaire ou de distribution :** il comprend essentiellement la liaison d'abonné (paire métallique torsadée) qui relie l'installation de l'abonné au centre de transmission de rattachement.

- **Le réseau de transit**, effectuant le transport des communications entre les nœuds de transit concentrateurs/commutateurs. Il transporte le signal échantillonné à une fréquence de 8000 Hz (contrainte liée au théorème d'échantillonnage de Shannon).

On discerne généralement trois (03) fonctions au niveau de la gestion du réseau RTC :

- **la distribution :** cette section assure la transmission de la voix et de la signalisation.

- **La commutation :** c'est la fonction essentielle du réseau, elle consiste a mettre en relation deux (02) abonnés, maintenir la liaison pendant l'échange et libérer les ressources a la fin de celui-ci. C'est le commutateur qui détermine les paramètres de taxation et impute le cout de la communication à l'appelant.

- **La transmission :** c'est la partie support de télécommunication du réseau. Cette fonction est remplie soit par le système filaire (cuivre, fibre optique), soit par faisceaux hertziens, etc.

II.1.2.2 Architecture du réseau RTC

Le Réseau Téléphonique Commuté est organisé de façon hiérarchique à plusieurs niveaux appelés zones de concentration, illustré sur le schéma ci-dessous.

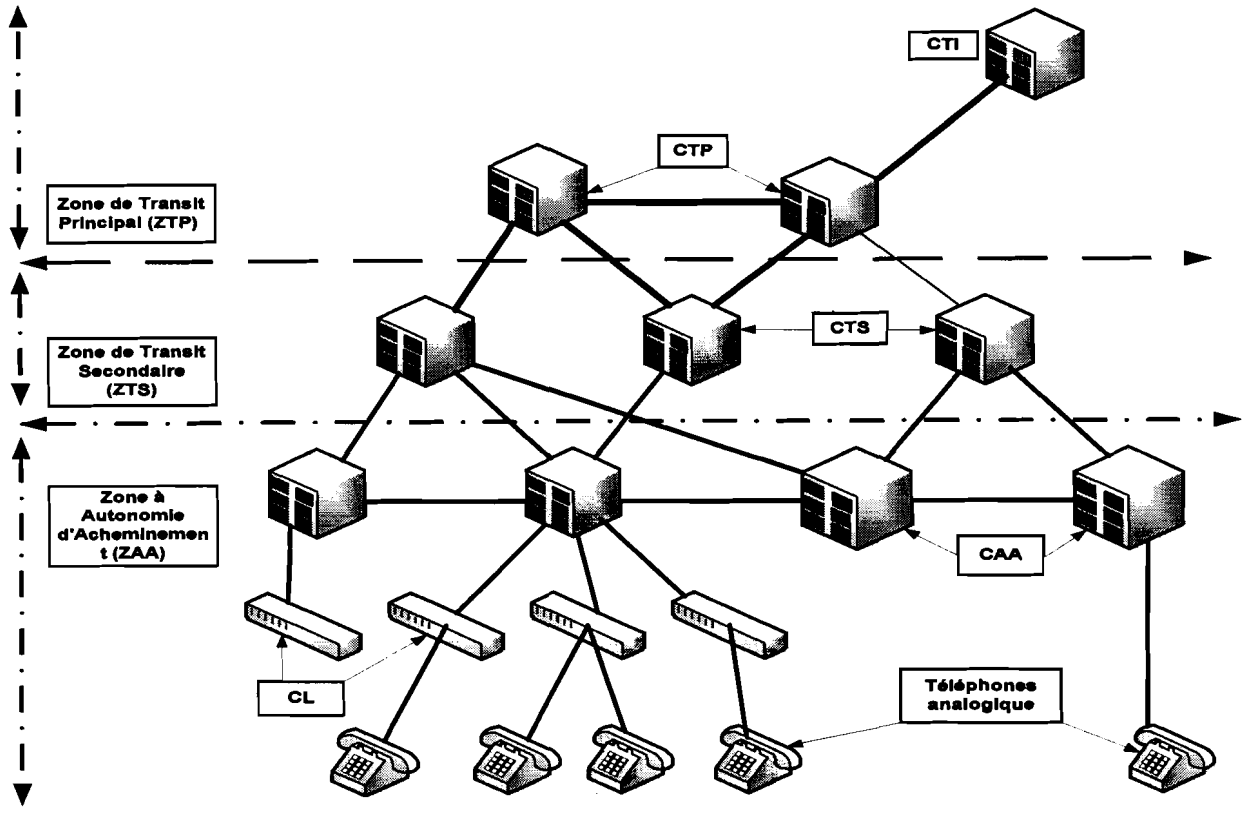


Figure 4 : Architecture du réseau RTC

CL : Commutateurs Locaux

CAA : Commutateurs à Autonomie d'Acheminement

CTS : Commutateurs de Transit Secondaire

CTP : Commutateur de Transit Principal

CTI : Commutateur de Transit International

On distingue :

- **la Zone à Autonomie d'Acheminement (ZAA) :** c'est la zone la plus basse de la hiérarchie qui comporte un ou plusieurs Commutateurs à Autonomie d'Acheminement (CAA) qui eux-mêmes desservent des Commutateurs Locaux (CL). Les commutateurs locaux ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finals. La ZAA (Zone à Autonomie

d'Acheminement) est un réseau étoilé, elle constitue "le réseau de desserte"[1] ;

- **la Zone de Transit Secondaire (ZTS) :** elle comporte des Commutateurs de Transit Secondaire (CTS) ; ces commutateurs assurent le brassage des circuits lorsqu'un CAA ne peut atteindre le CAA de destination ou lorsque le faisceau transversal reliant les deux CAA est congestionné ;

- **la Zone de Transit Principal (ZTP) :** cette zone assure la commutation des liaisons longues distances. Chaque ZTP comprend un Commutateur de Transit Principal (CTP). L'un des Commutateurs de Transit Principal (CTP) est relié au Commutateur de Transit International (CTI) qui gère les appels internationaux.

II.2. Qu'est-ce que la téléphonie sur IP?

II.2.1. Notions

La téléphonie sur IP (ToIP : Telephony over IP) est le fait d'utiliser le protocole IP pour transmettre la voix et gérer les fonctions téléphoniques. En matière de téléphonie sur IP, il faut distinguer les différentes interprétations de ce concept.

« La voix sur IP » qualifie les principes de transport de la voix sous forme de paquet IP entre deux points d'un réseau donné.

« La téléphonie sur IP » qualifie un service de communication entre deux terminaux téléphoniques IP (ou entre un terminal téléphonique IP et un IPBX), pour lesquels un ensemble de fonctionnalités de téléphonie sera mis en œuvre.

Qu'il s'agisse de communications d'ordinateur à ordinateur, d'ordinateur à téléphone, de téléphone à téléphone ou encore de PABX à PABX, la dénomination "Voix sur IP" est la plus utilisée pour décrire ces différentes formes de transmission de la voix au travers d'un réseau à commutation de paquets IP. Ainsi VoIP est la technologie utilisée pour transporter le service de téléphonie sur IP. La voix numérisée, compressée et

[1] Réseau de desserte : ensemble de liens filaires ou radioélectrique existant entre le poste d'abonné et le commutateur d'abonné au quel il est rattaché.

encapsulée en paquets est transmise dans le réseau IP comme tout autre paquet de donnée.

II.2.2. Principe de fonctionnement de la voix sur IP

De manière générale, le principe de la téléphonie sur le réseau de données par paquets commence par une numérisation de la voix. Le signal numérique correspondant est ensuite compressé. Cette compression permet de diminuer le débit, c'est à dire la quantité d'informations à transmettre. Puis, le signal obtenu est découpé en paquets de données qui sont transmis sur un réseau de données utilisant la même technologie. A l'arrivée, les paquets transmis sont réassemblés. Le signal de données ainsi obtenu est décompressé puis converti en signal analogique pour la restitution sonore à l'utilisateur.

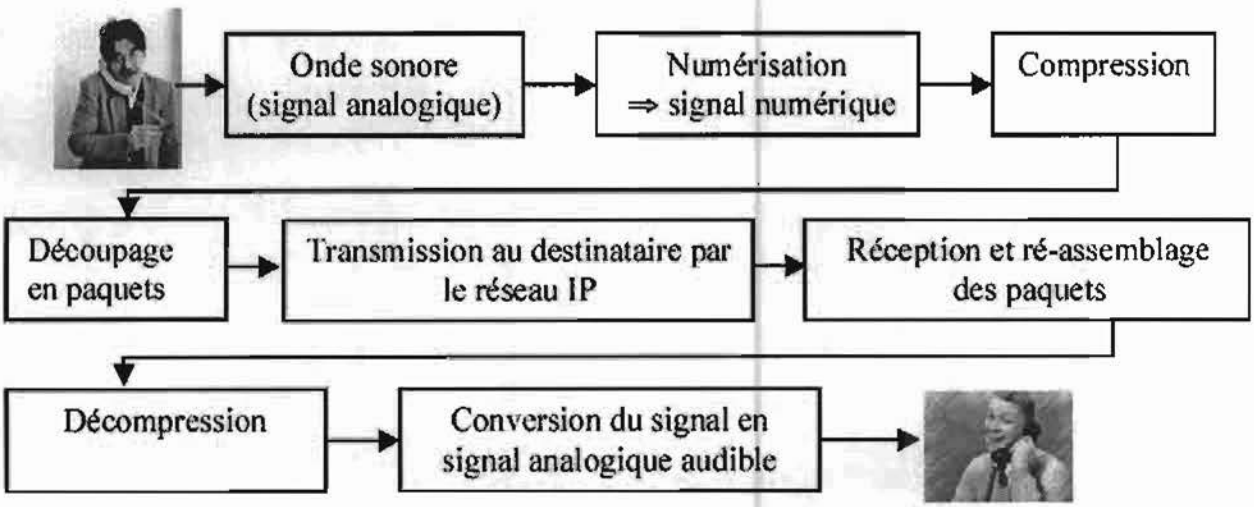


Figure 5 : processus de numérisation de la voix

Un réseau de données par paquets est un réseau basé sur le protocole IP, dans lequel les paquets sont acheminés par les nœuds du réseau qui comportent des routeurs jusqu'au lieu de l'abonné demandé. Les paquets arrivent alors à destination dans un ordre pouvant être différent de celui de l'émission car la durée de transmission de chacun des paquets est variable. C'est l'équipement d'arrivée qui est chargé de reconstituer le signal numérique.

II.3. Les protocoles de signalisation

Un protocole est un ensemble de spécifications décrivant les conventions et les règles à suivre dans un échange de données. Les protocoles de VoIP sont indispensables pour établir une communication. Il en existe plusieurs tels que H323, SIP, IAX, MGCP etc. Cependant les protocoles H323 et SIP sont les plus utilisés et c'est sur ceux que porteront notre étude à l'addition du protocole IAX de ASTERISK

II.3.1. Le protocole H323

H323 est un protocole de communication englobant un ensemble de normes utilisées pour l'envoi des données audio et vidéo sur Internet.
H323 normalise les procédures d'établissement et de gestion des appels, et établit une liste de codecs audio et vidéo obligatoires ou conseillés permettant aux deux parties de négocier entre elles et d'échanger des appels. Ce protocole est utilisé pour l'interactivité en temps réel, notamment la visioconférence (signalisation, enregistrement, contrôle d'admission, transport et encodage).

II.3.1.1. Architecture protocolaire

La pile protocolaire H323 est indépendante des réseaux et des protocoles de transport utilisés et fonctionne selon une stratégie de bout-en-bout qui lui confère une transparence vis-à-vis des évolutions du réseau. La figure 6 représente la pile protocolaire H323 dont la relation avec le modèle OSI est montrée à la figure 7

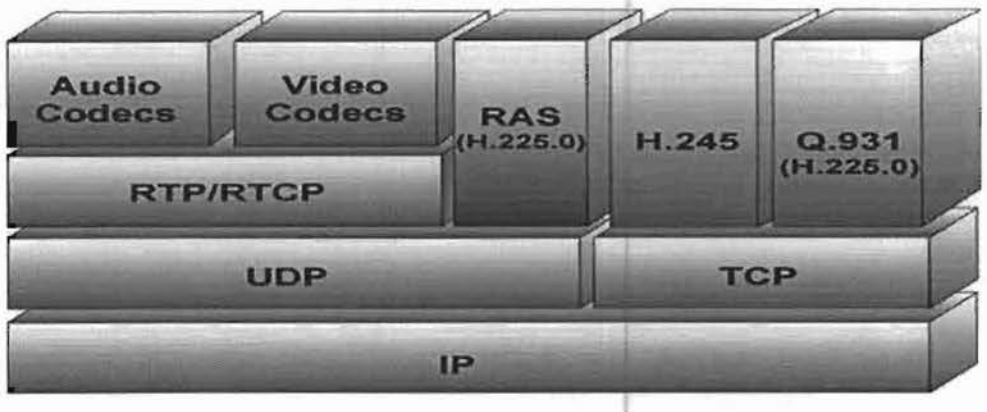


Figure 6 : Pile protocolaire H323

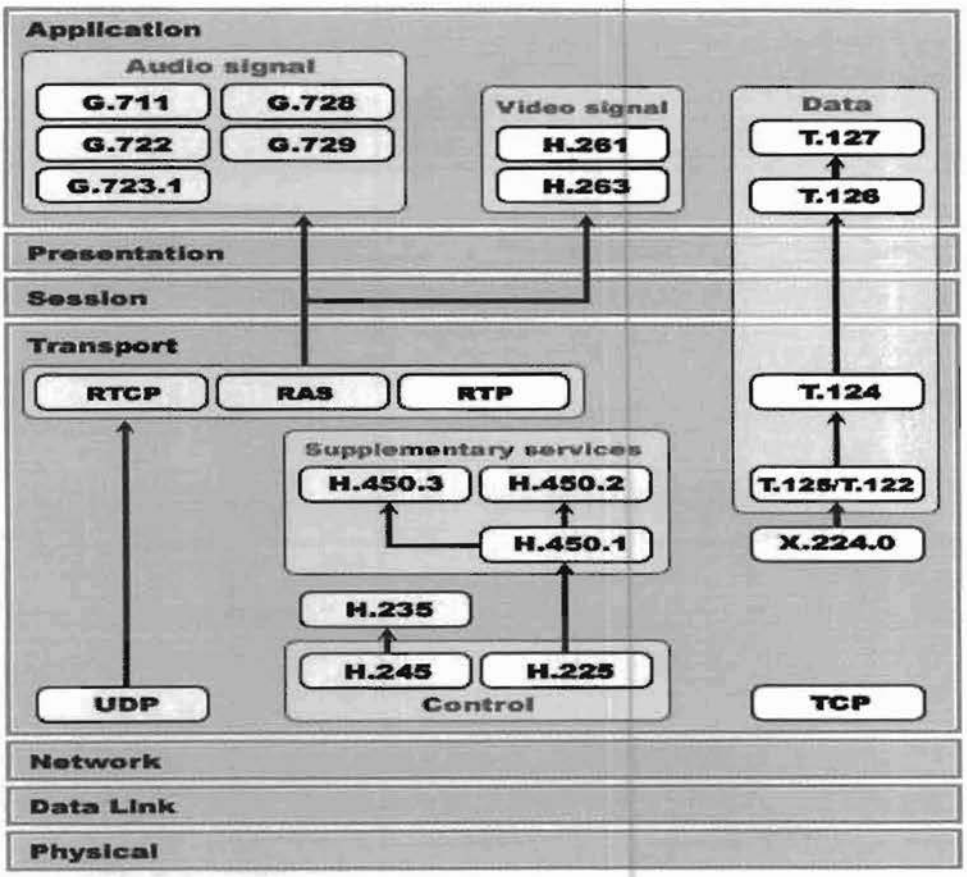


Figure 7 : Mise en évidence de la pile protocolaire H323 par rapport au modèle OSI.

II.3.1.2. Les équipements et fonctionnement du protocole H323

Le protocole H323 s'articule autour d'une architecture particulière qui concentre les fonctionnalités autour d'entités. Cette architecture est généralement composée des quatre catégories d'entités suivantes :

II.3.1.2.1. Les terminaux téléphoniques IP

Il existe deux types de terminaux téléphoniques IP :

- Les **hardphones** sont des postes téléphoniques totalement indépendants de l'équipement informatique de l'utilisateur. Ils sont destinés à remplacer l'équipement de téléphonie classique existant et présentent l'avantage de ne pas remettre en cause les mécanismes comportementaux d'un utilisateur par rapport à son téléphone.

Figure 8 : Téléphone IP

- Les **softphones** sont des applications permettant d'émuler un terminal téléphonique sur un PC (équipé d'un micro et d'un écouteur).

Figure 9 : Softphone

Ces deux types de terminaux disposent d'une interface réseau, d'un ou plusieurs CoDec audio (G711 obligatoire, G723 et G729 recommandés) et d'une couche logicielle répondant au standard de signalisation de référence (H323 ou SIP par exemple).

L'alimentation d'un terminal téléphonique IP peut se faire :

- soit localement : le poste dispose d'une alimentation indépendante sur une prise 230V.

- Soit à distance : dans ce cas, le poste téléphonique est télé-alimenté via

l'infrastructure de réseau local

- ✓ Soit par le commutateur Ethernet selon la norme 802.3af
- ✓ Soit par un équipement intermédiaire appelé MID — SPAN situé entre le switch et le panneau de câblage.

Figure 10 : MID-SPAN

Dans ces deux cas, l'alimentation du terminal reste un point sensible de l'architecture de téléphonie sur IP. L'alimentation électrique d'un téléphone IP doit répondre au besoin de continuité de service.

II.3.1.2.2. Le Gatekeeper

Le gatekeeper assume les fonctions de contrôle d'appels et de gestion des terminaux. Cet équipement détient l'intelligence du « réseau » H323 et donne les fonctionnalités de téléphonie aux terminaux distants.

Physiquement, un gatekeeper est un serveur informatique localisé sur le même réseau que les terminaux téléphoniques IP.

Les principes de communication sont les suivants :

- ➢ Un utilisateur souhaitant communiquer avec un autre utilisateur lance une requête vers le gatekeeper en composant le numéro de ce destinataire sur son terminal IP.
- ➢ Le gatekeeper assure la correspondance entre le numéro de l'appelé et son adresse IP et vérifie par une requête la disponibilité du terminal

destinataire.

- ✓ Si la disponibilité du destinataire est admise, le gatekeeper met en relation directe les deux terminaux en fournissant l'adresse IP du destinataire à l'appelant.
- ✓ Si le terminal destinataire ne se trouve pas sur le réseau local, le gatekeeper route l'appel vers la gateway pour accéder au terminal distant.

➢ Lorsque l'appel est terminé, le gatekeeper met à jour ses tables pour rendre les postes disponibles.

Ce principe de fonctionnement définit une architecture de communication non centralisée mettant en relation directe les interlocuteurs pendant toute la communication (flux voix). Les seules informations échangées avec le gatekeeper concernent la signalisation, qui permet l'établissement et la libération de l'appel.

II.3.1.2.3. La Voice Gateway

Une voice gateway est une passerelle permettant l'interconnexion entre un réseau à commutation de circuits (RTC) et un réseau en mode paquet (de type réseau IP).

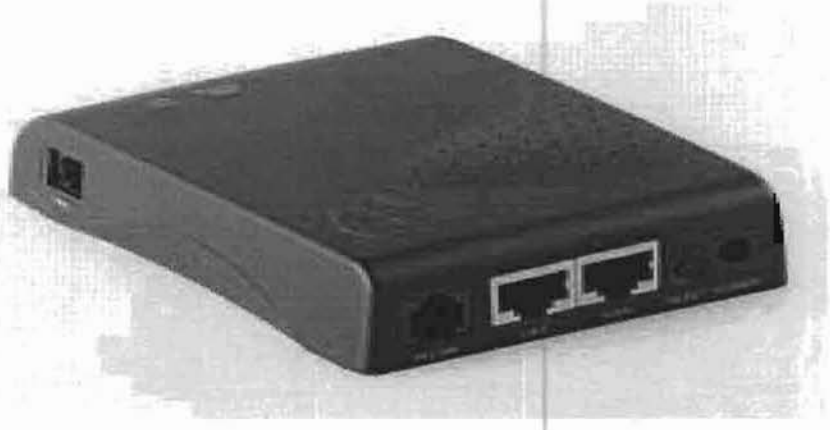


Figure 11: gateway

Ainsi, les voice gateways assurent la conversion des communications classiques en IP et vice-versa. Elles permettent d'assurer l'acheminement :

- Des appels sortants du réseau IP: cas d'un appelant disposant d'un téléphone IP mais souhaitant contacter un destinataire utilisant un téléphone classique
- Des appels entrants dans le réseau IP : cas d'un appelant disposant d'un téléphone classique mais souhaitant contacter un destinataire utilisant un téléphone IP.

Les processus clés d'une voice gateway sont:

- La translation de protocole (échanges d'informations de signalisation entre les deux réseaux),
- La conversion de formats d'informations (échanges de signaux audio « décodés »)
- Le transfert d'informations

II.3.1.2.4. Le MCU

Le MCU est un serveur permettant la gestion des connexions multiples (multicast). Il centralise les flux de tous les participants, les traite et les renvoie. Cet équipement est plus spécialement adapté à la visioconférence.

II.3.2. Le protocole SIP

SIP est un protocole de signalisation appartenant à la couche application du modèle OSI. Il a été conçu pour l'ouverture, le maintient et la terminaison de sessions de communication 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.

II.3.2.1. 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.

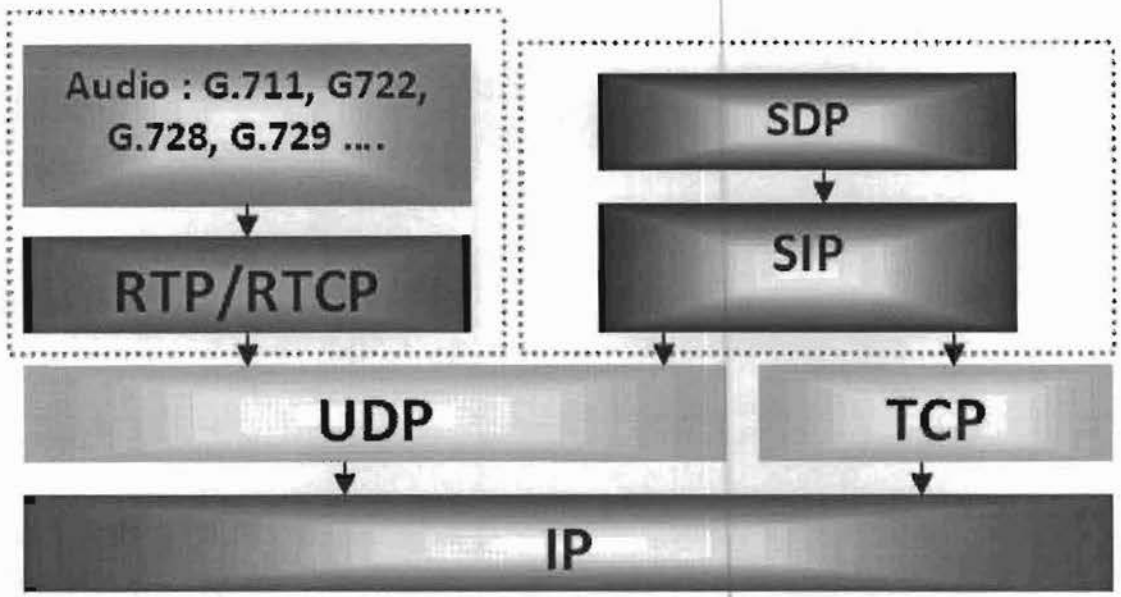


Figure 12 : Pile SIP

II.3.2.2. Les équipements du protocole SIP

SIP est un protocole simple et flexible orienté messages. Les principaux composants d'un système basé sur SIP sont :

- **Terminal SIP (User Agent Client ou UAC) :** peut être aussi bien un Softphone (logi ciel) qu'un Hardphone (téléphone IP). Les UAC sont capables d'émettre et de recevoir de la signalisation SIP.

- **Proxy Server :** encore appelé serveur mandataire auquel est relié un terminal fixe ou mobile, agit comme serveur envers le client et comme client envers les autres UAS.

- **Redirect Server:** ce serveur permet de rediriger les appels vers la position courante d'un utilisateur. Il réalise simplement une association d'adresses vers une ou plusieurs nouvelles adresses.

- **Location Serv er :** i l fournit la posit ion courante de s utilis ateurs dont la communication traverse les serveurs mandataire et de redirection auxquels il est rattaché.

- **Registrar Server :** ce serveur reçoit et accepte les inscriptions des utilisateurs (adresse IP, port, login).

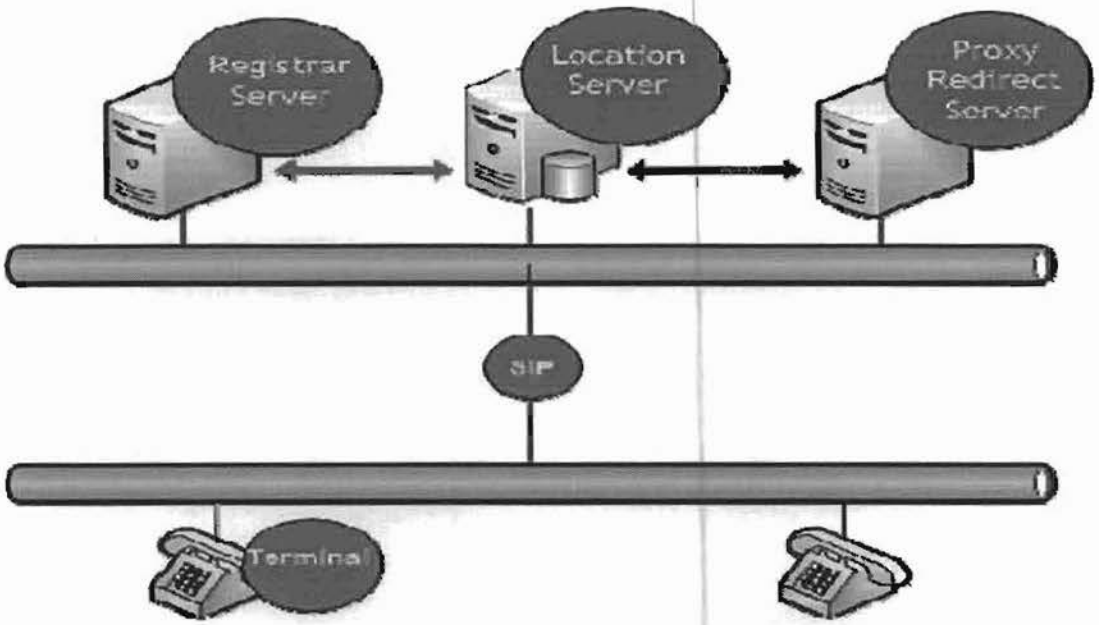


Figure 13 : Architecture SIP

II.3.2.3. Requêtes et Réponses SIP

SIP est un protocole de type client serveur. A cet effet, les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes et réponse SIP. Voici une liste exhaustive des requêtes SIP :

- **INVITE :** cette requête indique que l'application (ou utilisateur) correspondante à l'Url SIP spécifié est invitée à participer à une session.
- **ACK :** cette requête permet de confirmer que le terminal appelant a bien reçu une réponse définitive à une requête INVITE.
- **BYE :** cette requête est utilisée par le terminal de l'appelé pour signaler qu'il souhaite mettre un terme à la session.
- **CANCEL :** cette requête est envoyée par un terminal ou un serveur mandataire afin d'annuler une requête non validée par une réponse finale.
- **REGISTER :** cette méthode est utilisée par le client pour enregistrer l'adresse listée par le serveur auquel il est relié.

- **OPTIONS :** un serveur mandataire en mesure de contacter le terminal appelé, doit répondre à une requête OPTIONS en précisant ses capacités à contacter le même terminal.

A ces requêtes sont associées des réponses qui sont dans le même format que celles du protocole HTTP. Voici les plus importantes d'entre elles :

- **1XX :** messages d'informations (100 – essai, 180 – sonnerie, 183 – en cours)
- **2XX :** succès de la requête (200 –OK)
- **3XX :** redirection de l'appel, la demande doit être dirigée ailleurs
- **4XX :** erreur du client (La requête contient une syntaxe erronée)
- **5XX :** erreur du serveur (le serveur n'a pas réussi à traiter une requête correcte)
- **6XX :** echec général (606 – requête non acceptable par aucun serveur)

II.3.2.4. Fonctionnement

SIP intervient aux différentes phases de l'appel :

- Localisation du terminal de l'interlocuteur.
- Analyse du profil et des ressources du destinataire.
- Négociation du type de média (voix, audio, vidéo...) 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 : retour d'erreurs, etc.

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

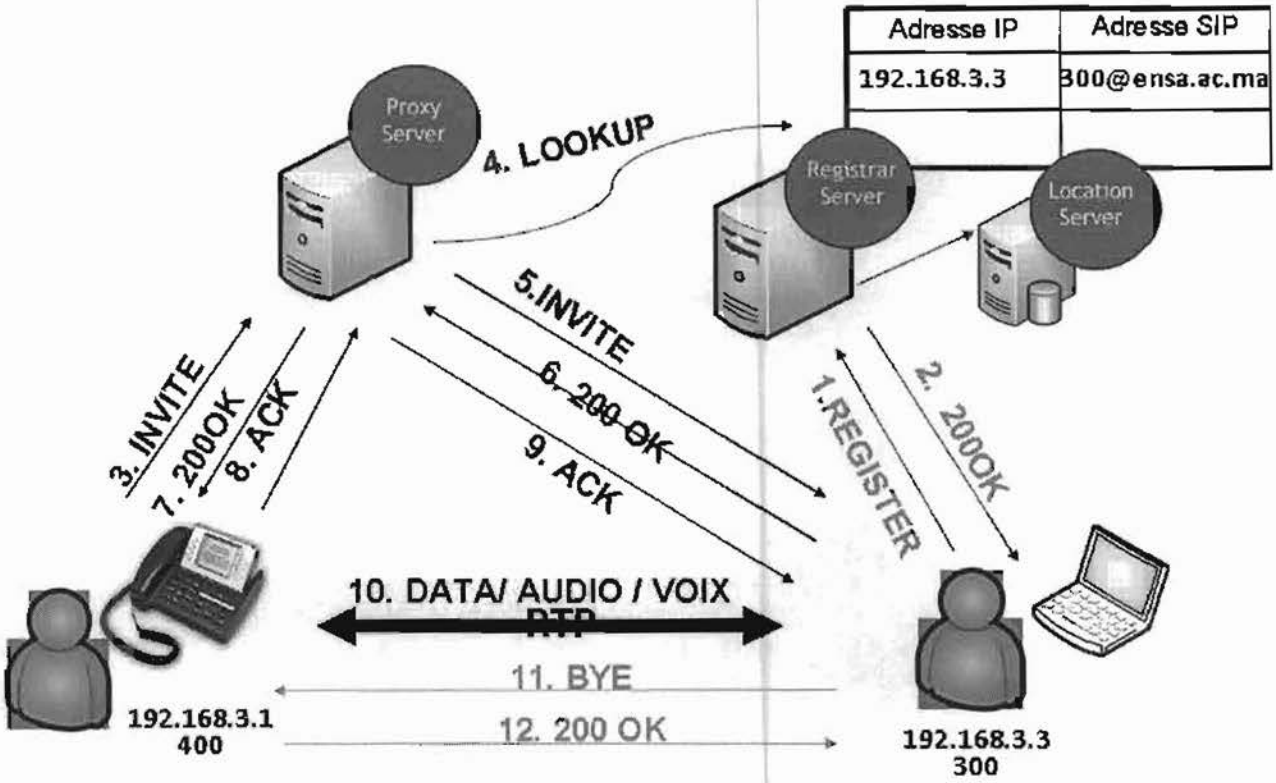


Figure 14 : exemple d'une communication SIP

II.3.3. Le protocole IAX2

Le protocole IAX2 est une alternative au protocole SIP. Il s'agit du protocole sur lequel s'appuie Asterisk bien que celui-ci soit en mesure de supporter les autres principaux protocoles VoIP tel que SIP.

En effet, le protocole SIP, en plus de sa fiabilité, est également célèbre pour sa principale limite qui est la difficulté à l'implémenter derrière un NAT. IAX2 ne rencontre nullement ce problème de NAT d'où son principal succès.

La popularité du PABX IP open source Asterisk ainsi que l'affranchissement des problèmes de NAT pour IAX2, ont littéralement permit que de plus en plus d'opérateurs supportent le protocole IAX2 et de nombreux équipements commencent à faire leur apparition.

II.3.4. Comparaison des protocoles H323 et SIP

Les deux protocoles SIP et H323 représentent les standards définis jusqu'à présent pour la signalisation à propos de la téléphonie sur Internet. Ils présentent tous les deux des approches différentes pour résoudre un même problème.

H323 est basé sur une approche traditionnelle du réseau à commutation de circuits. Quant à SIP, il est plus léger car basé sur une approche similaire au protocole http. Tous les deux utilisent le protocole RTP comme protocole de transfert des données multimédia.

Au départ, H323 fut conçu pour la téléphonie sur les réseaux sans QoS, mais on l'adopta pour qu'il prenne en considération l'évolution complexe de la téléphonie sur internet.

Pour donner une idée de la complexité du protocole H323 par rapport à SIP, H323 est défini en un peu plus de 700 pages et SIP quant à lui, en moins de 200 pages. La complexité de H323 provient encore du fait de la nécessité de faire appel à plusieurs protocoles simultanément pour établir un service, par contre SIP n'a pas ce problème.

SIP ne requiert pas de compatibilité descendante, SIP est un protocole horizontal au contraire de H323 : les nouvelles versions de H323 doivent tenir compte des anciennes versions pour continuer à fonctionner. Ceci entraîne pour H323 de traîner un peu plus de codes pour chaque version.

H323 ne reconnaît que les Codecs standardisés pour la transmission des données multimédias proprement dit alors que SIP, au contraire, peu très bien en reconnaître d'autres.

Ainsi, on peut dire que SIP est plus évolutif que H323.

	H323	**SIP**
Inspiration	Téléphonie	HTTP
Nombres d'échanges pour établir la connexion	6 à 7 aller-retour	1 à 5 aller-retour
Complexité	Elevée	Faible
Adaptabilité / Modularité protocolaires	Faible	Elevée
Implémentation de nouveaux services	Non	Oui
Adapté à Internet	Non	Oui
Protocoles de transport	TCP	TCP ou UDP
Coût	Elevé	Faible

Tableau 6 : Tableau comparatif entre h323 et SIP

II.4. Les protocoles de transport RTP et RTCP

Le couple RTP/RTCP (Real Time Protocol ou Real Time Transport Protocol/Real Time Control Protocol) a été développé par l'IETF pour le transport en temps réel, de la voix et de la vidéo encapsulé en paquets sur les réseaux IP. RTP est utilisé pour le transport de bout en bout des flux qui ont des contraintes de temps très fortes. RTCP est souvent associé à RTP pour le contrôle et la supervision du réseau

II.4.1. Les fonctions du protocole RTP

RTP a pour rôle d'organiser les paquets à l'entré et à la sortie du réseau pour un transport temps réel. Ainsi il permet :

- La synchronisation des flux par l'ajout des « timestamps » permettant de marquer sur les paquets le moment de leur envoi, ce qui permet de reconstituer les délais inter-paquets;

- La reconstitution de l'ordre des paquets émis et la détection des paquets perdus ;
- L'identification du contenu des informations afin de leur associer un transport sécurisé ;
- L'identification de la source, ce qui permet par exemple dans une communication multicast de ne plus diffuser le message vers le port expéditeur.

RTP est un protocole applicatif donc indépendant de la couche de transport, mais utilise habituellement UDP pour le transport car les contrôles de TCP rendent lentes les applications temps réels et le temps réel ne nécessite pas de retransmission pour les paquets. UDP ne permet la retransmission, donc RTP ne garantit pas la qualité de service suffisante. C'est pourquoi il est souvent couplé avec RTCP.

II.4.2. Les fonctions du protocole RTCP

RTCP a pour rôle l'envoi périodique des messages de contrôle à tous les participants d'une session. Ainsi :

- Les récepteurs envoient, via RTCP, un rapport sur QoS (Quality of Service) vers les émetteurs, qui contient les informations telles que le nombre de paquets perdus, les irrégularités de délais d'arrivée etc. ce qui permet à la source de s'adapter.
- Les paquets RTCP contiennent aussi les messages supplémentaires tels que l'adresse d'une messagerie électronique, le nom d'un participant à une conférence téléphonique ;
- RTCP contrôle la session c'est-à-dire qu'il permet aux participants d'indiquer leur départ lors d'une conférence téléphonique ou de fournir les indications sur une éventuelle modification ;
- Etc.

II.5. Les CODECS

Les codecs sont des chipsets qui font office de compresseurs/décompresseurs ou de codeurs/décodeurs. Certains termi naux téléphoniques IP n'acceptent qu'une partie ou même un seul codec, tout dépend du modèle de terminal et du constructeur. Le principe de fonctionnement de ces codecs est expliqué par le synoptique de transmission de la voix en mode paquet.

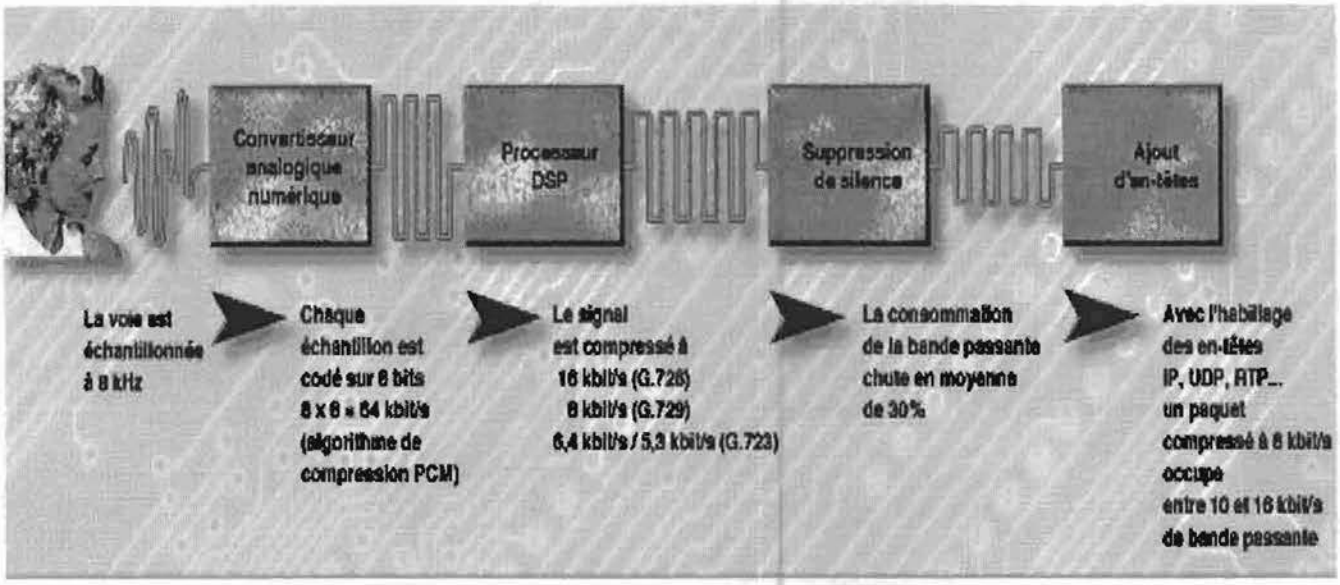


Figure 15 : Synoptique de transmission de la voix analogique en mode paquet

Les principaux codecs officiels avec leur taux de compression de la voix sont les suivants :

CoDec	Débit binaire (Kbps)	Délai de codage (ms)	MOS ou Qualité auditive perçue
G.711 PCM	64	0,125	4,1
G.726 ADPCM	32	0,125	3,85
G.728 LD-CELP	15	0,125	3,61
G.729 CS-ACELP	8	10	3,92
G.729a CS-ACELP	8	10	3,7
G.723.1 MP-MLQ	6,3	30	3,9
G.723.1 ACELP	5,3	30	3,65

Tableau 7 : tableau comparatif des caractéristiques des CoDecs ITU-T courants.

II.6. Pourquoi adopter le système téléphonie sur IP au lieu du système de téléphonie classique ?

Pour un opérateur ou une entreprise privée possédant son propre central téléphonique analogique, il existe de nombreux avantages à remplacer ce central traditionnel par un serveur de téléphonie IP.

II.6.1. Réduction des coûts

En déplaçant le trafic voix RTC vers le réseau privé WAN/IP les entreprises peuvent réduire sensiblement certains coûts de communications. Réductions importantes mises en évidence pour des communications internationales, ces réductions deviennent encore plus intéressantes dans la mutualisation voix/données du réseau IP intersites (WAN).

II.6.2. Disponibilité et mobilité

Une seule ligne de téléphone est généralement présente dans chaque local de l'entreprise. De plus, cette ligne est souvent associée à l'employé qui occupe le local. Pour se faire, en utilisant un softphone sur une station de travail ou poste téléphonique IP WIFI, chaque employé est accessible via son identifiant unique dans l'annuaire de l'entreprise, peu importe le local dans lequel il se trouve. En effet, sa ligne téléphonique "le suit" et n'est plus physiquement associée à un lieu unique.

En matière de mobilité interne, on constate que:

- il n'est plus nécessaire de manipuler les connexions physiques au PABX ou de changer le numéro de téléphone associé à un poste téléphonique lorsque celui-ci est déplacé ;
- les utilisateurs sont disponibles au travers d'un annuaire unique, que ce soit dans l'entreprise, une de ses filiales ou à travers le monde (voyageur fréquent)
- les utilisateurs ont l'opportunité d'associer leurs lignes avec n'importe quel poste de téléphone IP disponible
- Etc.

II.6.3. Simplification des infrastructures

Avec la VoIP, le souci d'avoir un réseau dédié pour la voix et un autre pour les données informatiques n'est plus qu'un souvenir. Le seul réseau informatique répond favorablement non seulement au transport des données mais aussi à celui de la voix. Cela permet à une entreprise d'économiser sur le câblage lors de l'extension ou de la mise en place d'un système communication (informatique et téléphonique).

II.6.4. Facilitation de l'intégration avec le système d'information

L'enregistrement des appels, le journal d'appel, la messagerie vocale se retrouvent sous forme d'information binaire avec la ToIP. Cette information est facilement manipulable et stockable pour les ordinateurs.

II.6.5. Nouveaux services et standard ouverts

Grâce aux efforts constants de standardisation des systèmes et des protocoles utilisés par les applications, il est désormais possible pour une entreprise de ne plus être "prisonnière" d'un seul fournisseur de solutions logicielle et/ou matérielle. Cela permet de plus une meilleure interopérabilité pour les communications entre les systèmes acquis par deux entreprises distinctes et qui auraient opéré des choix de produits différents.

II.6.6. Homogénéiser les services téléphoniques sur un ensemble de sites

Grâce à la centralisation du gestionnaire d'appels (principal c omposant d'un IPBX), le moindre site distant bénéficie de la même richesse de services téléphoniques que le siège de l'entreprise. En fait, un simple lien IP suffit, dès lors que la liaison est capable de véhiculer les flux. Même le poste d'un télétravailleur sera vu et géré comme un employé normal. Cette homogénéité peut-être mise à profit pour mettre en œuvre un centre d'appels virtuels, c'est-à-dire donc les agents sont géographiquement dispersés.

II.6.7. Intégration des structures

Avec la fusion des réseaux de données et de la voix, au niveau privé ou public, réunis en une structure unique, s'observe une utilisation plus efficace de cette dernière. Du point de vue d'Internet, le bénéfice du trafic de la voix en paquets est la meilleure utilisation du protocole IP, vu que celui-ci, déjà amplement diffusée actuellement, est responsable de la transmission de toutes les informations, mais peu pour les services de la voix.

II.7. PABX et IPBX

II.7.1. Le PABX

Un PABX (Private Automatic Branch eXchange) ou PBX en Anglais, est un autocommutateur privé, utilisé dans les entreprises pour assurer les communications internes et le lien avec le réseau téléphonique commuté global PSTN (Public Switched Telephone Network). Un autocommutateur est un central téléphonique, en d'autre terme, il représente l'élément central qui :

- Distribue les appels téléphoniques arrivés ;
- Autorise les appels téléphoniques départs ;
- Gère les terminaux téléphoniques ;
- Gère toutes les autres fonctionnalités ou options.

Un autocommutateur privé possède sa propre intelligence pour faciliter la commutation des appels vocaux.

II.7.2. L'IPBX

On désigne par IPBX (IPBX ou encore PBX IP) un système utilisé en entreprise qui assure l'acheminement de toute ou une partie des communications en utilisant le protocole internet (IP), en interne sur le réseau local (LAN) ou le réseau étendu (WAN) de l'entreprise.

Le IPBX est un ordinateur avec un système d'exploitation sur lequel on installe un ensemble de logiciels chargé de gérer les appels VoIP. Les PABX IP, non seulement supportent les mêmes services que ceux offerts par les PABX traditionnels, en général au minimum la quinzaine de services classiques (mise en garde, transfert, renvois, etc.), mais aussi offrent aussi de nouveaux services tels que :

- L'accès web aux messages vocaux;
- La musique en attente;
- Consultation des rapports des appels;
- La mise en place de conférence;
- La connexion avec d'autres IPBX;
- L'implémentation de serveur vocal interactif (SVI);
- etc.

En plus, les IPBX sont couplés à des passerelles qui permettent d'autres accès aux réseaux de télécommunication classiques (RTC, GSM, etc.).

III. Modes de communications dans un système de téléphonie VoIP

Dans un système de téléphonie VoIP la communication est établie selon trois modes.

III.1. La téléphonie d'ordinateur à ordinateur

Dans ce mode de communication, l'ordinateur doit être équipé d'un certain nombre d'accessoires au préalable à savoir un microphone, un haut-parleur, une carte son (full duplex) et un logiciel de téléphonie (stimulateur téléphonique) sur IP qui tient lieu de téléphone.

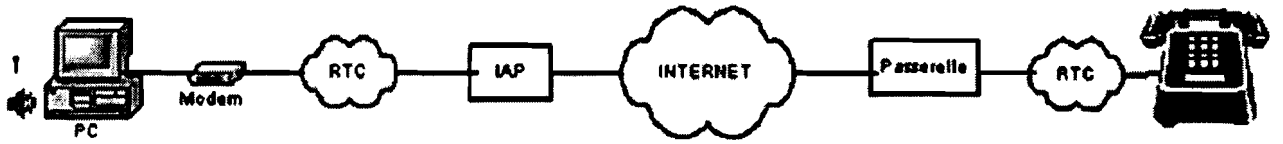
RTC:Réseau téléphonique commuté
IAP:Fournisseur d'accès à Internet

Figure 16 : Communication d'ordinateur à téléphone

III.2. La téléphonie d'ordinateur à téléphone

Ici l'un des correspondants est sur un PC et l'autre utilise un téléphone classique. Dans cette configuration, il faut passer via son fournisseur d'accès à Internet qui doit mettre en œuvre une "passerelle" (Gateway) avec le réseau téléphonique.

C'est cette passerelle qui se chargera de l'appel du correspondant et de l'ensemble de la "signalisation" relative à la communication téléphonique, du côté du correspondant demandé.



RTC:Réseau téléphonique commuté
IAP:Fournisseur d'accès à Internet

Figure 17 : Communication d'ordinateur à téléphone

III.3. La téléphonie de téléphone à téléphone

Dans ce mode de communication les interlocuteurs utilisent des téléphones analogiques. Pour faire dialoguer deux postes téléphoniques ordinaires via un réseau IP, des passerelles sont mises en place permettant ainsi d'accéder directement au réseau IP.

RTC:Réseau téléphonique commuté
IAP:Fournisseur d'accès à Internet

Figure 18 : Communication de téléphone à téléphone

IV. Architecture d'une infrastructure VOIP

L'architecture d'une infrastructure voix sur IP laisse à l'aperçu le degré de convergence entre réseaux. Il existe ainsi trois scénarios de mise en œuvre de la téléphonie sur IP en entreprise.

IV.1. Architecture hybride

Ce scénario 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 intersites.

L'architecture ainsi définie est la suivante :

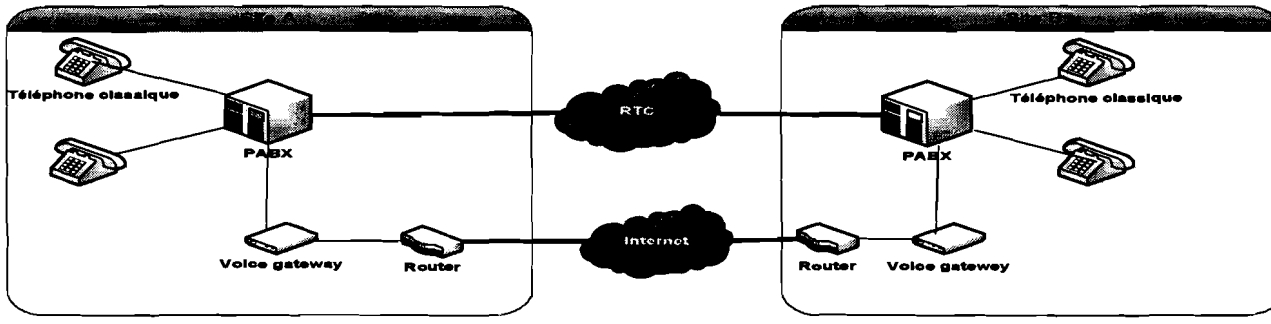


Figure 19 : **Architecture hybride**

IV.2. Architecture Full IP

Ce scénario constitue une migration complète de la téléphonie de l'entreprise sur IP, incluant les terminaux téléphoniques utilisateurs. 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.

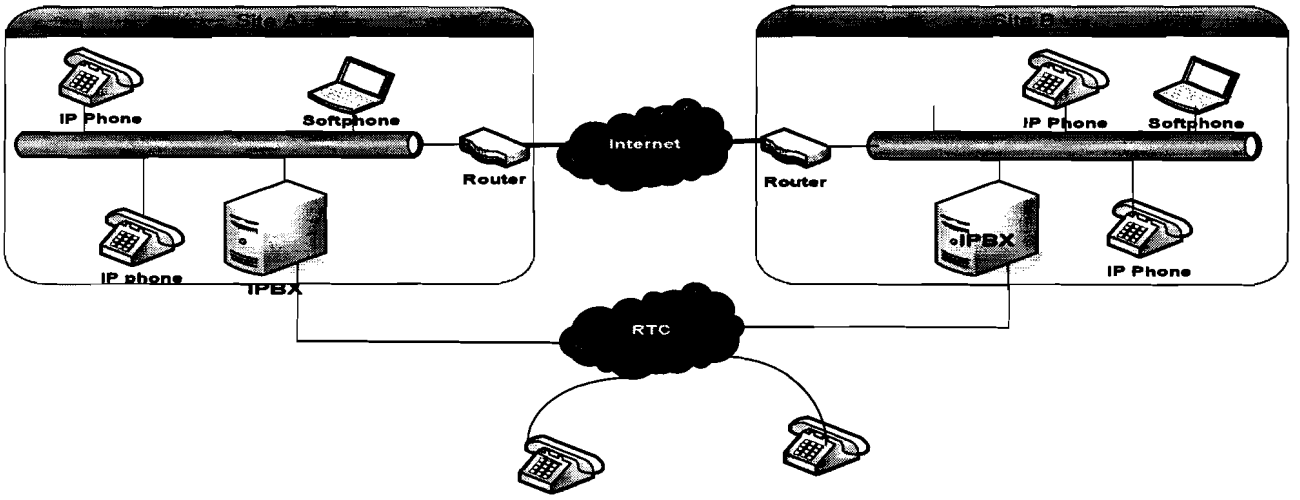


Figure 20 : Architecture full IP

IV.3. Architecture Centrex

La migration en Téléphonie sur IP peut constituer pour une entreprise l'occasion d'externaliser ses services de téléphonie auprès d'un fournisseur. Cette externalisation lui évite d'investir à la fois dans des équipements nouveaux, mais aussi dans des nouvelles compétences en termes d'administration et de maintenance.

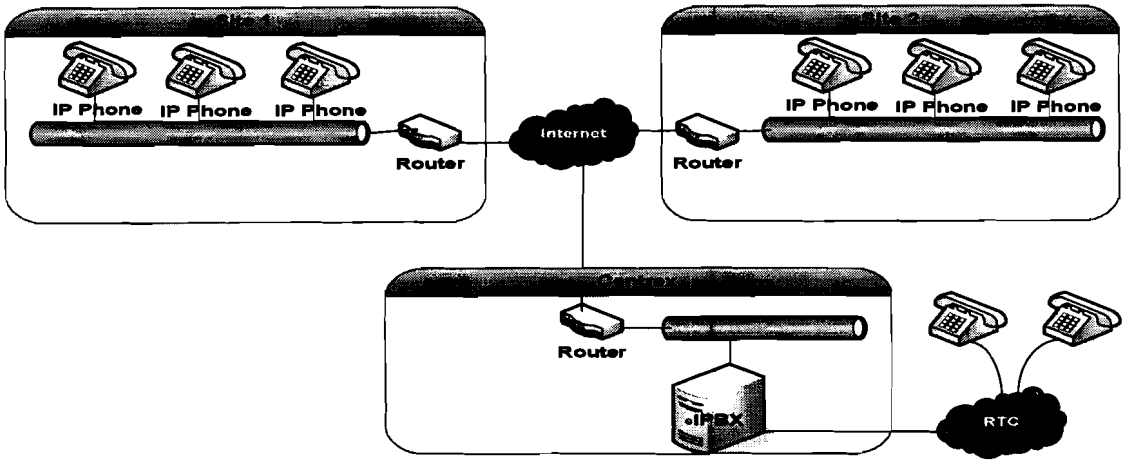


Figure 21 : Architecture Centrex

V. Qualité de service (Q.O.S)

V.1. Les facteurs affectant la qualité de la voix et les remèdes possibles.

La qualité de la voix est plus exigée par les utilisateurs. Tout service doit alors garantir une intelligibilité et une interactivité acceptable. Pour arriver à ce niveau de qualité il est nécessaire d'analyser les problèmes rencontrés sur le réseau de transport (IP dans notre cas) et sur les équipements terminaux.

V.1.1. La bande passante

Sur le réseau WAN (Wide Area Network) de l'entreprise, la ressource en bande passante est bien plus contrainte que sur le LAN. Une application gourmande en bande passante, telle qu'une application de messagerie ou de transfert de fichiers, peut donc rapidement compromettre la qualité de service des applications critiques, comme les progiciels de gestion intégrés ou les bases de données.

Pour pallier ces inconvénients, accroître la bande passante disponible ne constitue pas toujours la bonne solution. Il faut connaître l'ensemble des flux pouvant avoir une influence importante sur le transport de la voix permettant une meilleure gestion de l'allocation de la bande passante.

V.1.2. Le délai d'acheminement: latence (Delay)

C'est le temps de transmission d'un bout (de l'émetteur) à l'autre(au récepteur) des paquets transportant la voix. Pour garantir une conversation orale active, ce temps de transit sur le réseau ne doit excéder les 150ms. Il comprend le délai réseau (retard engendré par la propagation sur le support, la commutation et le séjour dans les files d'attente des routeurs, au séjour dans les tampons de compensation de gigue etc.) et des terminaux (temps de numérisation, de codage, de compression, de mise en paquet, de transmission, de décompression, de conversion numérique analogique, etc.)

Délai (de l'émetteur au récepteur)	Difficulté de communication
200ms	28%
450ms	35%
700ms	46%

Tableau 8 : Rapport entre délai et état de communication

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

V.1.3. Les pertes de paquets (Packets 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.

Cela permet également d'envoyer un signal implicite aux terminaux TCP qui diminuent d'autant leur débit au vu des acquittements négatifs émis par le destinataire qui ne

reçoit plus les paquets. Malheureusement, pour les paquets de voix, qui sont véhiculés au dessus d'UDP, aucun mécanisme de contrôle de flux ou de retransmission des paquets perdus n'est offert au niveau du transport. D'où l'importance des protocoles RTP et RTCP qui permettent de déterminer le taux de perte de paquet, et d'agir en conséquence au niveau applicatif.

V.1.4. La gigue (Jitter)

La gigue est la variance statistique du délai de transmission. En d'autres termes, elle mesure la variation temporelle entre le moment où deux paquets auraient dû arriver et le moment de leur arrivée effective. Cette irrégularité d'arrivée des paquets est due à de multiples raisons dont: l'encapsulation des paquets IP dans les protocoles supportés, la charge du réseau à un instant donné, la variation des chemins empruntés dans le réseau, etc.

Pour compenser la gigue, on utilise généralement des mémoires tampon (buffer de gigue) qui permettent de lisser l'irrégularité des paquets. Malheureusement ces paquets présentent l'inconvénient de rallonger d'autant le temps de traversée global du système. Leur taille doit donc être soigneusement définie, et si possible adaptée de manière dynamique aux conditions du réseau.

V.1.5. Les erreurs de séquence

Les erreurs de séquence se produisent lorsque les paquets arrivent côté récepteur dans un ordre différent de l'ordre d'envoi. Les paquets TCP/IP intègrent des clés pour indiquer leur position dans une séquence. Un poste émetteur, qu'il s'agisse d'un PC ou de tout autre périphérique TCP/IP, partage les paquets en datagrammes pour la transmission. Ces datagrammes se voient attribuer un numéro de séquence. Si les datagrammes empruntent différents chemins sur le réseau en raison d'une congestion ou d'une défaillance matérielle, ou si un problème de câblage provoque plusieurs retransmissions, il se peut que les paquets arrivent dans le désordre. Un grand nombre d'erreurs de séquences entraînera une dégradation perceptible de la

conversation.

V.1.5. Le phénomène d'Echo

C'est le délai entre l'émission du signal et la réception de ce même signal en réverbération. Cette réverbération est causée par les composants électroniques des parties analogiques. Un écho inférieur 50 ms n'est pas perceptible. Plus il est décalé dans le temps plus il est insupportable.

V.1.6. Les applications agressives

En effet, quel que soit le réseau considéré, il existera toujours des applications au comportement plus agressif, à savoir occupant une grande partie de la bande passante, voire la totalité, en fonction de leurs besoins. Généralement, même si elles sont importantes, ces applications ne sont pas urgentes (par exemple la réplication de base de données et la messagerie).

La majorité des applications des réseaux IP d'entreprise utilisent le protocole TCP (Transport Control Protocol) conçu pour octroyer un accès équitable à la bande passante du réseau.

V.2. Politique de mise en place d'une qualité de service

De la préparation au déploiement, on distingue trois étapes :

V.2.1. La caractérisation du trafic

Pour que l'administrateur ait une vue des flux circulant sur son réseau, un audit est indispensable. Il peut être réalisé sur la totalité ou sur un sous-ensemble représentatif des liaisons du réseau. Il sert à identifier les problèmes existants et à définir une politique de QoS qui tienne compte des éléments remontés lors de la phase d'étude.

V.2.2. La certification des flux

Selon les impératifs de l'entreprise, le responsable réseau définira une classification des divers flux et leur attribuera des niveaux de priorité. Cette phase doit impérativement être menée en concertation avec les différents utilisateurs du système d'information.

V.2.3. La définition des règles des flux

Selon la classification auparavant établie, le responsable réseau doit définir les règles de traitement des flux selon leur classe. Il s'agit, par exemple, de déterminer les priorités de routage ou des niveaux de bande passante minimale pour certaines applications. Avec l'architecture Diffserv (Differentiated Services), chaque classe de services est assortie d'un traitement spécifique en sortie du lien WAN.

VI. Sécurité VOIP

La course à la réduction des coûts d'une entreprise implique bien souvent la migration du service de téléphonie vers la "Voix sur IP". Cependant de nombreux paramètres sont bien souvent oubliés ou ignorés. Avant de franchir le pas, il est nécessaire d'étudier les nouvelles contraintes engendrées. Mis à part le surcharge du réseau de l'entreprise et la migration de nombreux équipements, la confidentialité des communications et l'efficacité des plans de secours sont remis en cause.
La convergence numérique va introduire de nouveaux services et par conséquent, de nouvelles vulnérabilités et de nouveaux vecteurs d'attaques.

VI.1. Les vulnérabilités de la Voix sur IP

Elles sont regroupées en deux points essentiels à savoir les attaques au niveau des protocoles et celles au niveau des applications.

VI.1.1. Attaques au niveau des protocoles

VI.1.1.1. L'écoute électronique

Elle consiste à capturer le trafic réseau d'un terminal IP et à le convertir en fichier exploitable qui peut être lu sur des lecteurs audio ordinaire. Comme exemple on a VOMIT (Voice Over Misconfigured Internet Telephones).

Les attaques basées sur l'écoute électronique sont possibles en raison de l'absence de chiffrement de la conversation transportée par le protocole de transport multimédia dans la plupart des configurations par défaut. C'est le cas lorsque le protocole RTP est utilisé comme couche de transport multimédia.

Pour bénéficier d'une protection plus efficace, il faut utiliser SRTP (Secure RTP), qui offre des fonctions de chiffrement et d'authentification.

VI.1.1.2. La relecture

Une attaque par relecture relit une session légitime (généralement capturée par l'interception du trafic réseau) d'une cible. Dans le cas d'un appel VoIP, les attaques par relecture peuvent se produire au niveau du protocole de signalisation SIP. Une attaque bien connue utilise des techniques de relecture pour pirater l'enregistrement. Le protocole SIP fait appel à la commande Register pour indiquer au logiciel de gestion des appels la localisation d'un utilisateur sur la base de l'adresse IP. L'auteur de l'attaque peut relire cette requête et y substituer une autre adresse IP, redirigeant ainsi tous les appels vers lui.

Les attaques par relecture sont rendues possibles par le fait que certaines parties du protocole SIP sont communiquées en texte clair. Pour se prémunir contre ce type d'attaques, il est désormais possible d'utiliser SIPS (SIP Over Transport-Layer Security). SIPS assure l'intégrité des données et fournit une fonction d'authentification entre l'utilisateur et le logiciel de gestion des appels.

VI.1.1.3. Le déni de service

Dans la mesure où VoIP est un service exécuté sur un réseau IP, il est exposé aux mêmes attaques par inondation (fooding) que d'autres services IP. Les attaques de l'infrastructure incluent des inondations TCP SYN ou UDP (User Datagram Protocol) des réseaux IPBX et VoIP ainsi que des appareils téléphoniques VoIP. Les attaques des protocoles de signalisation et de transport multimédia sont également bien connues de la communauté des pirates informatiques. Elles utilisent des outils tels qu'un « inondateur » (fooder) qui bombarde un téléphone IP de requêtes SIP INVITE pour épuiser ses ressources. Un autre type d'attaque est l'attaque par l'outil « Teardown », qui injecte une commande BYE dans le flux réseau et met fin à l'appel.

VI.1.1.4. La manipulation du contenu multimédia et des signaux

Une fois encore, dans la mesure où VoIP est un service exécuté sur un réseau IP, il est exposé aux mêmes attaques de manipulation réseau que d'autres services IP. A titre d'exemple, citons l'attaque « RTP InsertSound » qui permet à un intrus d'injecter des fichiers son dans un flux multimédia RTP (conversation vocale entre plusieurs téléphones IP)

VI.1.2. Attaques au niveau des applications

VI.1.2.1. Les appareils VoIP avec services en code source ouvert

De nombreux téléphones comportent un port de service qui permet aux administrateurs de recueillir des statistiques, des informations et des paramètres de configuration distante. Ces ports ouvrent la porte aux divulgations d'informations dont les auteurs d'attaques peuvent se servir pour obtenir des renseignements sur un réseau et identifier les téléphones VoIP.

VI.1.2.2. Les services web de téléphonie VoIP

La plupart des ports de service des téléphones VoIP qui exposent des données interagissent également avec des services web et sont généralement vulnérables à des

menaces courantes telles que la falsification des requêtes intersites et l'exécution forcée de scripts sur les sites web. Ces dernières consistent à insérer un lien dans une page web qui utilise les informations d'identification (généralement contenues dans un cookie) de la victime. A titre d'exemple, citons la vulnérabilité découverte dans les téléphones SIP de Snom Technology ; celle-ci permet aux utilisateurs de modifier les paramètres de l'appareil, d'afficher l'historique des appels ou même de passer des appels via une interface web intégrée.

Un pirate est en mesure de lancer une attaque s'il connaît l'adresse IP de l'appareil VoIP. En attirant un utilisateur téléphonique sur un site malveillant, le pirate peut s'emparer des informations d'identification de l'internaute et accéder au téléphone via son adresse IP comme s'il en était le propriétaire. Il s'agit d'une méthode particulièrement insidieuse car elle contourne le pare-feu.

VI.1.2.3. Le vishing

Avec la technologie VoIP Il est impossible de localiser avec précision l'origine d'un appel passé via Internet, tandis qu'il est très facile d'usurper l'identifiant de l'appelant. Les cybercriminels exploitent désormais cet anonymat en recourant à des techniques de « vishing », qui associent la technologie VoIP et l'usurpation d'identité dans ce cas précis, celle de l'appelant. Une attaque par vishing emprunte une identité tout à fait légitime pour demander à sa victime des renseignements.

VI.1.2.4. Le spam VoIP

La voix sur IP, au même titre qu'un service téléphonique standard, est également exposée aux communications indésirables et non sollicitées. Le spam VoIP est parfois désigné par le terme « SPIT » (Spam Over Internet Telephony), spam via la téléphonie Internet.

Ce type d'appels indésirables peut rapidement épuiser les ressources et engendrer une attaque par déni de service. Grâce aux enseignements tirés de la messagerie

électronique et des services téléphoniques traditionnels (authentification, listes d'autorisation, etc.), nous pouvons limiter les risques de spam via la téléphonie Internet.

VI.1.2.5. La fraude téléphonique VoIP

Ce type de fraude consiste à accéder à un réseau VoIP (gestionnaire d'appels ou passerelle) et à passer des appels non autorisés (généralement interurbains ou internationaux). Les auteurs d'attaques exploitent des noms d'utilisateur et mots de passe faibles, des passerelles ouvertes et d'autres vulnérabilités au niveau des applications que nous avons décrites précédemment.

VI.2. Solution de sécurité VoIP

La sécurité d'un réseau VoIP est basée sur celle du réseau IP sur lequel il est implémenté. Donc toutes les mesures prises pour sécuriser ce dernier doivent s'appliquer au réseau VoIP. En plus de ces mesures standards, on peut noter qu'il est nécessaire d'apporter certaines améliorations à un réseau VoIP.

VI.2.1. La sécurité de l'infrastructure IP

C'est le premier niveau de sécurité, car la sécurité de l'infrastructure de téléphonie VoIP est liée à la sécurité du réseau IP. Un exemple est la séparation logique des réseaux Data et Voix par des VLans.

VI.2.2. Les protocoles AAA (Authentification Autorisation Accounting)

Ces protocoles permettent aux utilisateurs ou aux équipements de s'authentifier auprès du système, de donner ou restreindre les droits de certains utilisateurs, de créer un compte pour chaque utilisateur. Le protocole RADIUS (Remote Authentification Dial In User Server) est un exemple de protocole AAA qui, en plus de la

sécurité, permet d'établir la liste de tous les appels en vue d'une taxation des utilisateurs. Il est normalisé par l'IETF ;

VI.2.3. Les protocoles SRTP et SPTCP

Les protocoles SRTP et SPTCP sont respectivement les versions sécurisées des protocoles RTP et RTCP. Ils ajoutent ainsi les options de chiffrements et de cryptographie dans ces protocoles. La mise en place de ces versions permet de résoudre le problème d'écoute.

VI.2.4. Les VPN (Virtual Private network)

La mise en place d'un VPN ou réseau privé virtuel entre les sites dans le cas d'une société multi-sites constitue une solution de sécurité. Une entreprise pour sécuriser ses trafics peut mettre en place un VPN administré par un opérateur télécom, plutôt que de transiter par le réseau public ou elle peut être interceptée ou écoutée.

V.II. Solutions envisageables

V.II.1. Gestion autonome des communications au niveau de chaque site

Cette solution permettra aux différents sites de gérer de façon autonome les appels internes grâce à un IPBX. Pour l'intercommunication entre sites il faut interconnecter les différents IPBX.

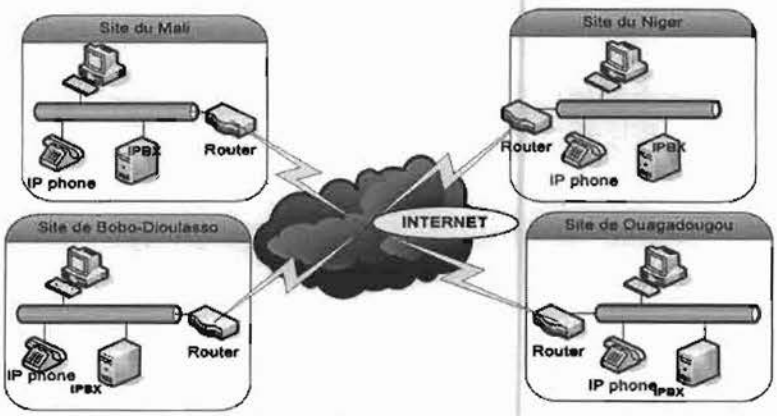


Figure 22 : Gestion autonome

Avantage

- Chaque site sera autonome et en cas de panne du système de communication d'un site les autres continueront à fonctionner.

Inconvénients

- Cout d'administration élevé par le fait qu'il faut pour chaque site un administrateur du système de communication.
- Nécessite plus de matériels.

V.II.2. Gestion centralisée des communications des différents sites

Tous les appels des différents sites sont gérés à partir d'un seul site à savoir le siège à Ouagadougou

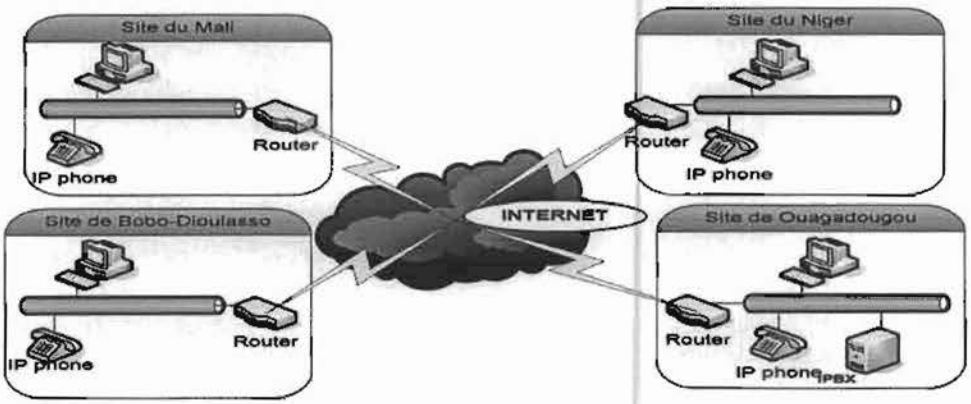


Figure 23 : Gestion centralisée

Avantages

- la réduction du coût d'administration.
- la réduction du nombre d'équipements à mettre en place.
- Optimisation du temps de déploiement

Inconvénient

- En cas de pannes tous les sites sont touchés.

Vue les avantages et les inconvénients que présente chaque solution et vu les moyens nécessités pour le déploiement et l'administration de chaque solution ; la centralisation des services de communication des différents sites au niveau du siège à Ouagadougou a été retenue.

TROSIEME PARTIE : Présentation de la solution

TROISIME PARTIE : Présentation de la solution retenue

I. Description de la solution

La solution que nous proposons, consistera, premièrement, à mettre en place un système de communication ToIP au sein du réseau local du siège du Centre SIGET-A à Ouagadougou. Ensuite, nous établirons une connexion de ce système avec le réseau téléphonique de l'ONATEL afin que les appels externes au site passent par ce réseau téléphonique. Enfin, nous relierons les représentations du centre que sont celles de Bobo-Dioulasso, du Mali et du Niger par VPN au siège à Ouagadougou.

I.1. Mise en place du système de communication local

La mise en place du système de communication local se fera par le déploiement et la configuration d'un IPBX (Trixbox), des téléphones IP et des softphones.

Les téléphones IP et les softphones, permettrons aux utilisateurs de recevoir ou d'émettre des appels, d'écouter leurs messages vocaux, etc. Ces équipements seront connectés au réseau local et leurs emplacements dépendront des utilisateurs. Les adresses IP des téléphones seront données par un serveur DHCP de l'entreprise.

La configuration logicielle du système consistera d'une part, à créer pour chaque utilisateur un compte SIP et à enregistrer son téléphone IP au niveau de l'IPBX ; et d'autre part à configurer le téléphone IP pour qu'il puisse s'enregistrer au niveau du compte SIP de son utilisateur.

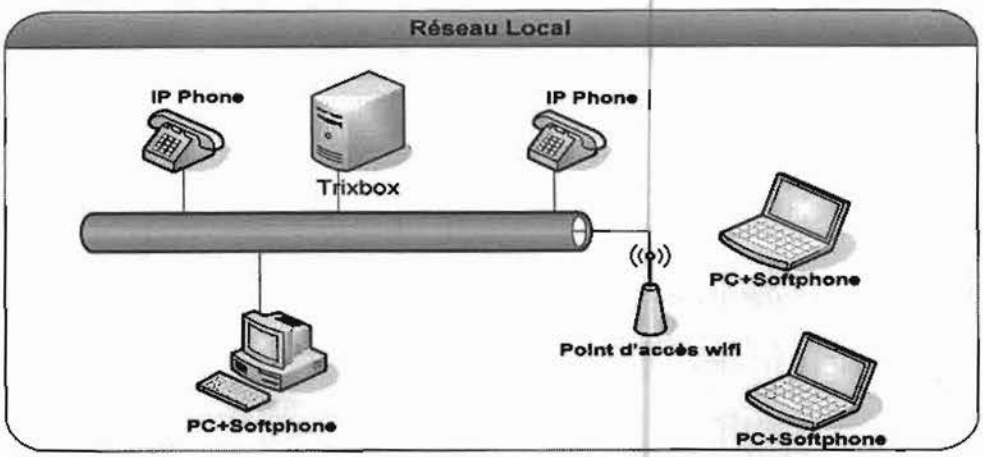


Figure 24 : Réseau ToIP local à mettre en place

I.2. Connexion du système de communication local au réseau téléphonique

Pour permettre à notre système de pouvoir communiquer avec le réseau téléphonique de l'ONATEL, nous avons besoin d'une carte TDM de type PCI. Cette carte se chargera d'adapter le signal en provenance du réseau téléphonique de l'ONATEL en un signal utilisable par notre IPBX et vis versa.

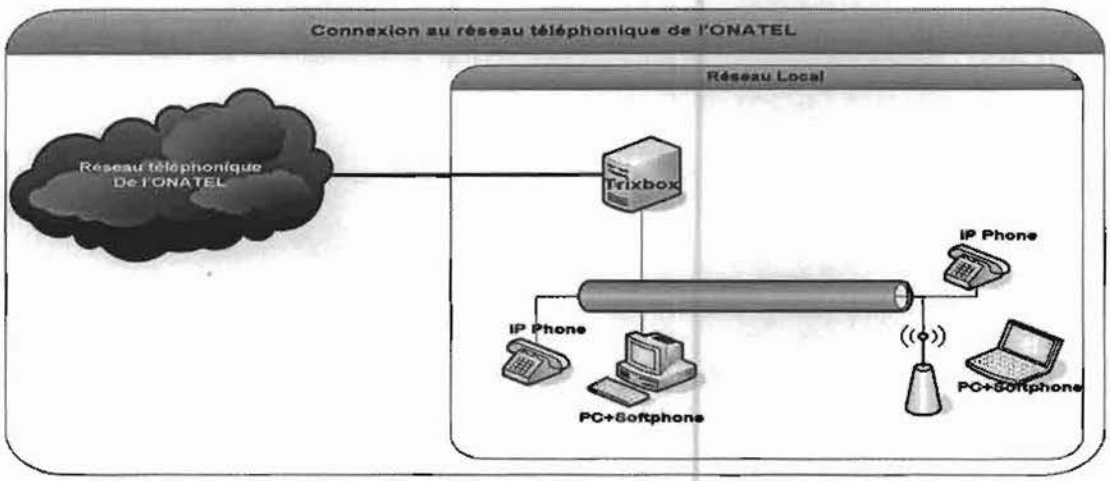


Figure 25 : Connexion au réseau téléphonique

I.3. Liaison VPN

I.3.1. VPN c'est quoi ?

VPN : Virtual Private Network ou RPV (Réseau Privé Virtuel) en Français une technique permettant à un ou plusieurs ordinateurs de communiquer de manière sûre tout en empruntant des infrastructures non sures comme Internet. Les VPN sont apparus suite à un besoin des entreprises de relier les différents sites de façon simple et économique.

I.3.2. Principe de fonctionnement

Un réseau VPN repose sur un protocole de tunnelisation. Ce protocole permet de faire circuler les informations de l'entreprise généralement de façon cryptée, d'un bout à l'autre du tunnel; ainsi les utilisateurs ont l'impression de se connecter directement sur le réseau de l'entreprise. Le principe du tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données au moyen d'algorithmes de cryptographie négociés entre le client et le serveur et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets et extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé alors qu'ils utilisent en réalité une infrastructure d'accès partagée telle que l'Internet. Les données à transmettre peuvent être prise en charge par un protocole différent d'IP, mais dans ce cas le protocole de tunneling encapsule les données en ajoutant un en-tête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

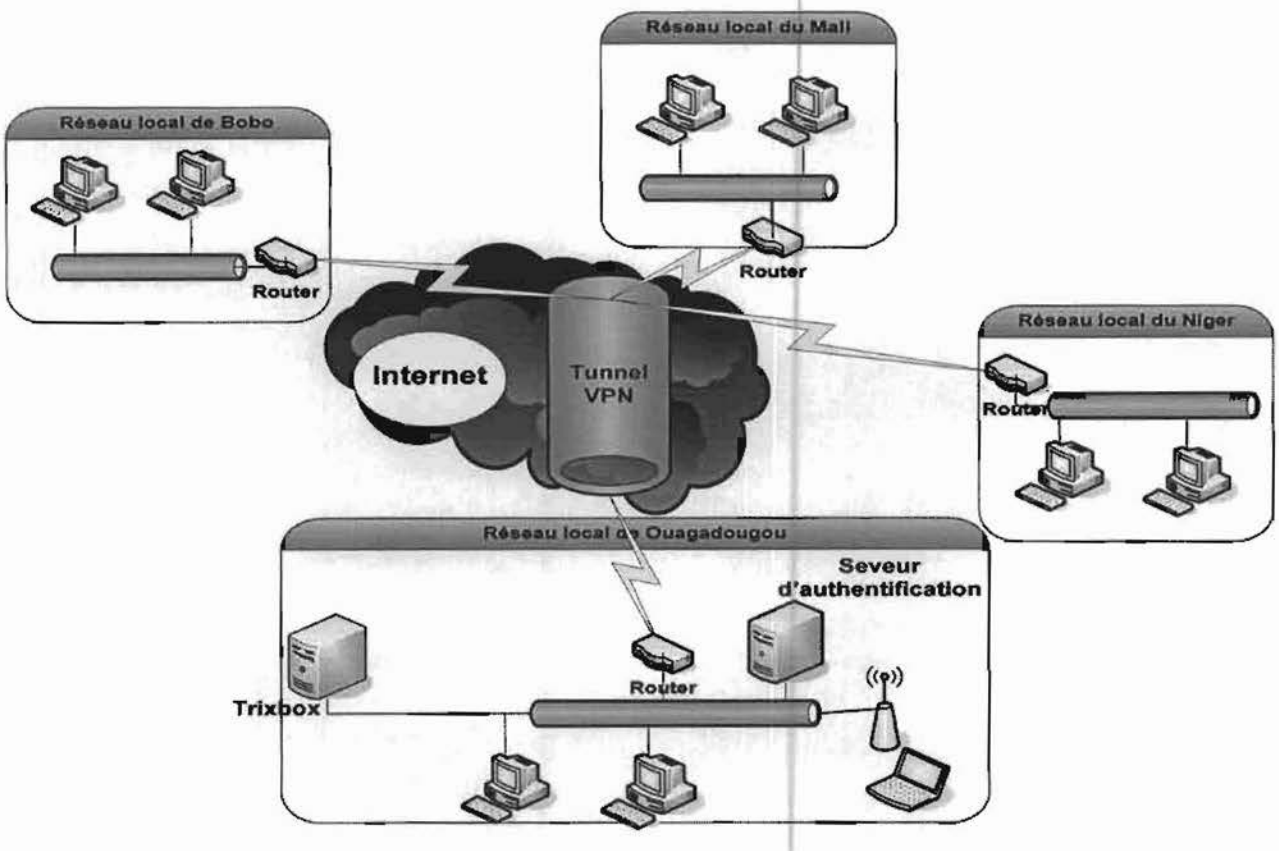


Figure 26 : VPN

I.4. Mise en place de politique d'authentification

Pour renforcer la sécurité du réseau local en ce qui est de la gestion des utilisateurs, nous avons décidé, en tenant compte d'une étude (Etude de la mise en place d'un Intranet et des Services multimédia basés sur la technologie wifi) qui a été menée au sein du Centre SIGET-A par MILLOGO Souleymane et BAYALA Béranger, de parler des protocoles AAA (Authentification, Authorization, Accounting) comme Radius et la gestion des annuaires pour la mise en place du système ToIP.

Nous avons retenu FreeRadius et OpenLdap dans le cadre de notre stage.

I.4.1. Radius

I.4.1.1. Définition

RADIUS (Remote Authentification Dial-In User Service) est un protocole

client/serveur permettant de centraliser des données d'authentification. En français on préfère souvent parler d'identification pour traduire l'anglais authentification, car l'identification effectuée par un serveur Radius est une vérification de nom d'utilisateur (attribut 1 User-Name) et de mot de passe (attribut 2 User-Password ou 3 Chap-Password).

I.4.1.2. Principe et fonctionnement

I.4.1.2.1. Principe

Le protocole RADIUS repose principalement sur un serveur (le serveur RADIUS), relié à une base d'identification (base de données, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

I.4.1.2.2. Fonctionnement

Le fonctionnement de RADIUS est basé sur un scénario proche de celui-ci :

- Un utilisateur envoie une requête 802.1x au NAS afin d'autoriser une connexion au réseau.
- Le NAS achemine la demande au serveur RADIUS.
- Le serveur RADIUS consulte la base de données d'identification (un annuaire LDAP a été mis en place pour répondre à ce besoin) afin de connaître le type de scénario d'identification demandé pour l'utilisateur.

Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

- ACCEPT : l'identification a réussi
- REJECT : l'identification a échoué
- CHALLENGE : le serveur RADIUS souhaite des informations supplémentaires de la

part de l'utilisateur et propose un « défi » (en anglais « challenge »)

- CHANGE PASSWORD : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

I.4.2. Ldap

I.4.2.1. Définition

Un annuaire est un système de stockage de données, dérivé des bases de données hiérarchisées, permettant en particulier de conserver les données pérennes, c'est-à-dire les données n'étant que peu mises à jour (historiquement, sur une base annuelle, d'où le nom), comme les coordonnées des personnes, des partenaires, des clients et des fournisseurs d'une entreprise. C'est pourquoi, grâce à des optimisations, un annuaire est beaucoup plus rapide en consultation qu'en mise à jour.

Lightweight Directory Access Protocol (LDAP) est un protocole permettant l'interrogation et la modification des services d'annuaire. Ce protocole repose sur TCP/IP. L'intérêt principal de LDAP est la normalisation de l'authentification. C'est l'opération Bind qui permet d'authentifier un utilisateur. De plus en plus d'applications possèdent un module d'authentification prenant en charge LDAP. C'est le cas du serveur RADIUS.

I.4.2.2. Fonctionnement

LDAP est basé sur un fonctionnement client-serveur (comme pour une base de données). Un client débute une session LDAP en se connectant sur le port TCP389 du serveur. Le client envoie ensuite des requêtes d'opération au serveur. Le serveur envoie des réponses en retour. À part quelques exceptions, le client n'a pas besoin d'attendre de réponse du serveur pour envoyer de nouvelles requêtes, et le serveur peut envoyer ses réponses dans n'importe quel ordre.

Ainsi LDAP fournit à l'utilisateur des méthodes lui permettant de :

- se connecter ;

- se déconnecter ;
- rechercher des informations ;
- comparer des informations ;
- insérer des entrées ;
- modifier des entrées
- supprimer des entrées

L'image ci-dessous présente l'étape de connexion d'un utilisateur à notre serveur Trixbox.

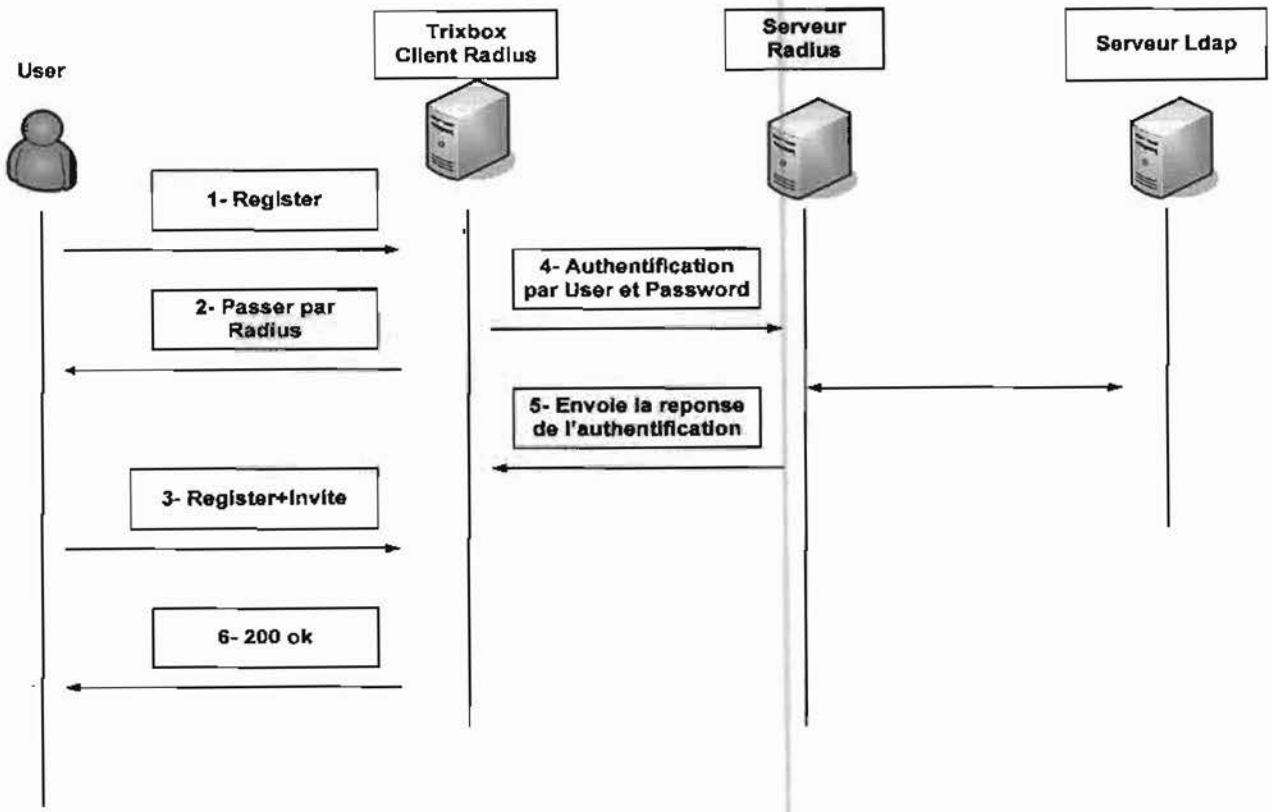


Figure 27 : Figure : Mode d'authentification

I.5. Réseau attendu

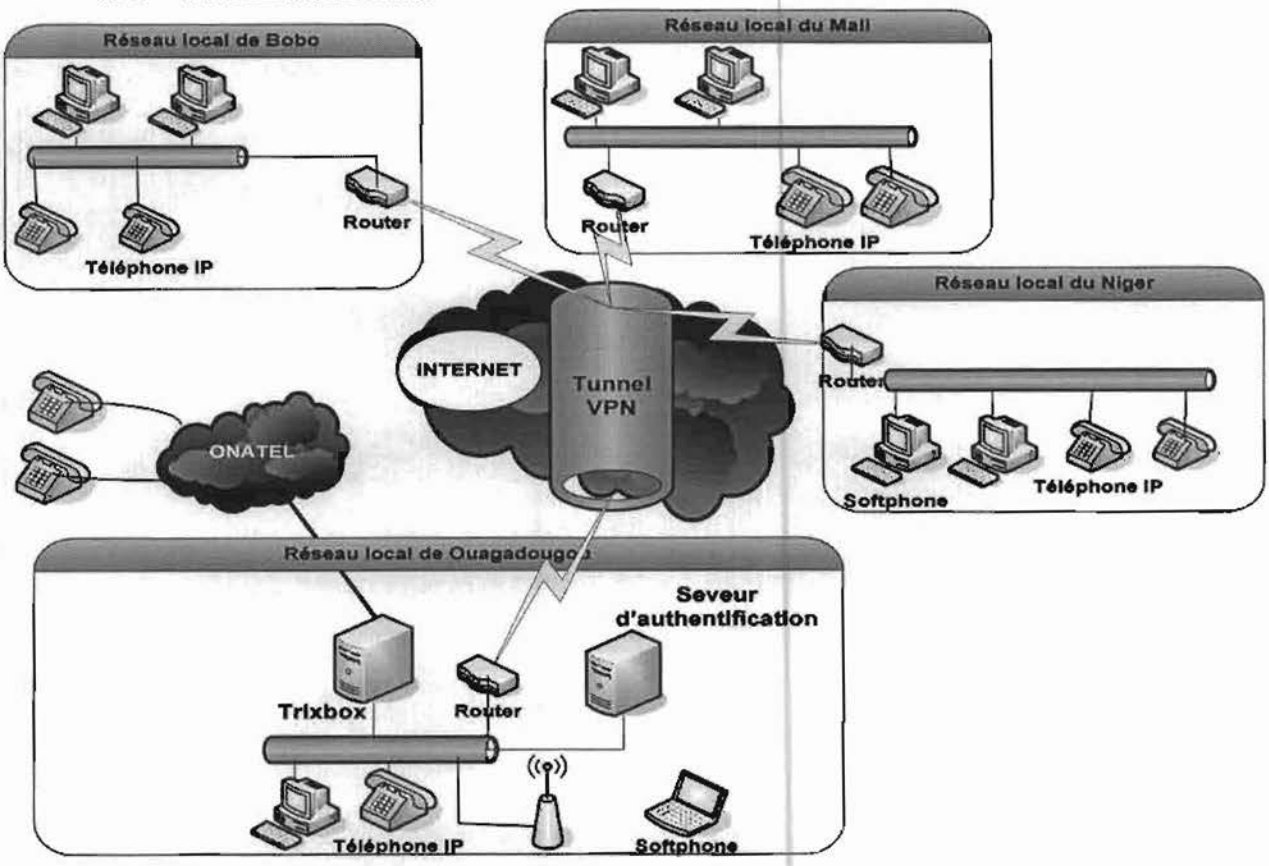


Figure 28 : Figure : Réseau Final

II. Logiciels et matériels requis

II.1. TRIXBOX CE

II.1.1. Présentation de Trixbox CE

La distribution Trixbox (anciennement appelé Asterisk@home) est un ensemble d'outils et d'utilitaires de télécommunication compilés pour devenir un véritable central téléphonique de haut de gamme. Trixbox est composé de :

- Cent Os qui un système d'exploitation basé sur le noyau Linux ;
- MySQL qui est serveur de base données libre ;
- Apache qui est un serveur Web ;
- Asterisk, qui est une plateforme de téléphonie sous licence GPL ;
- FreePBX qui est une interface graphique pour Asterisk ;

- Web MeetMe qui permet de mettre en place des conférences ;
- FOP (Flash Operator Panel) est une interface graphique, qui permet à un réceptionniste de savoir l'état des comptes, d'effectuer des transferts d'appels, etc. ;
- Pilotes pour cartes téléphoniques PCI ;
- Etc.

II.1.2. Pourquoi choisir Trixbox CE

Le choix de Trixbox CE peut-être résumé en ces points :

- La gratuité du logiciel ;
- Documentation abondante sur le web ;
- Facilité d'installation ;
- Conformité aux standards (protocoles et codecs) de la communication ToIP ;
- Possibilités d'interconnexion de plusieurs IPBX sous trixbox ;
- Possibilités d'interconnexion aux réseaux téléphoniques traditionnels ;
- Administration facile grâce à son interface web ;
- Stabilité ;
- Adapter pour des solutions dont le nombre d'utilisateurs inferieur à deux cents (200) ;
- La sécurité ;
- Etc.

II.2. Carte TDM22B

II.2.1. Petite explication sur la syntaxe des cartes TDM

Les cartes TDM sont des cartes TDM400P, modulables, c'est à dire que l'on peut y ajouter des modules FXO/FXS.

Les conventions de dénomination des bundles TDM est la suivante, TDM X Y B, où :

- X est le nombre de module FXS ;
- Y est le nombre de module FXO ;
- B signifie que le produit est un bundle ;

La TDM22B est, donc, une carte TDM400P avec 2 modules FXS et 2 modules FXO.

II.2.2. Explication sur FXO/FXS

FXS et FXO sont les noms donnés aux ports utilisés par des lignes téléphoniques analogiques (aussi connus sous le nom anglais de POTS - Plain Old Telephone Service)

- FXS : l'interface Foreign eXchange Subscriber est un port qui raccorde la ligne téléphonique de l'abonné. En d'autres termes, la « prise murale » qui fournit la tonalité, le courant de charge et le voltage de la sonnerie

- FXO : l'interface Foreign eXchange Office est un port qui reçoit la ligne téléphonique. C'est la prise du téléphone ou de la télécopieuse, ou la (les) prise(s) de votre réseau téléphonique analogue.

Le FXO offre un indicateur d'état raccroché/décroché (fermeture de circuit). Puisque le port FXO est raccordé à un appareil, tel un téléphone ou une télécopieuse, il est souvent appelé « périphérique FXO ».

Le FXO et le FXS vont toujours de paire, similaire à la prise mâle et femelle.

En l'absence d'autocommutateur, par exemple chez un particulier, les ports FXS représentent la prise téléphonique murale, sur laquelle on vient brancher un port FXO qui est la prise du téléphone.

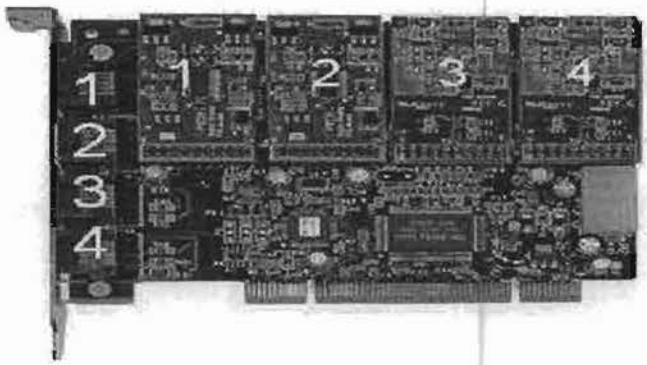


Figure 29 : carte TDM22B

II.3. Softphones

II.3.2. Ekiga

Ekiga, anciennement appelé GnomeMeeting est un logiciel de téléphonie sur IP (VoIP) et de visioconférence. Elle offre également un service de messagerie instantanée (chat). On peut citer comme autres fonctionnalités importantes :

- Support LDAP ;
- Historique des appels ;
- Possibilité de conférence vidéo plein écran ;
- Support des caméras Video4Linux, Video4Linux 2 et Firewire ;

Ekiga utilise les protocoles de communication standards et ouverts H323 et SIP, ce qui le rend compatible et interopérable avec les autres logiciels et appareils basés sur ces mêmes protocoles tels que : Swiss Voice, CISCO, SNOM, ... IP Phones, et aussi les logiciels tels que Windows Messenger, Netmeeting, SJPhone, Eyebeam, X-Lite, ... et aussi le populaire IPBX Asterisk, et les différents IPBX commerciaux et libres.

Figure 30 : Ekiga

II.3.2. X-Lite

X-Lite est un logiciel propriétaire gratuit client de téléphonie sur IP appelé également softphone, basé sur le protocole standard ouvert SIP.

X-Lite est un logiciel multiplateforme pour Mac OS X, Windows et Linux.

Associé à un compte SIP, il permet de bénéficier de tous les services téléphoniques traditionnels (conférence, double appels, etc..)

Figure 31 : X-lite

II.4. Autres matériels

Pour la mise en place du système de communication, nous avons besoin de cartes audio compatible full duplex, des casques munis de microphones et des téléphones IP.

III. Procédure de mise en place de la solution avec TRIXBOX

III.1. Installation

III.1.1. Pré-requis

III.1.1.1. Distribution Trixbox

Trixbox est téléchargeable sur le site http://www.trixbox.org en fichier ISO. A la fin du téléchargement, il faut le graver sur CD.

III.1.1.2. Matériel

Pour installer Trixbox, nous avons besoin d'au moins une machine PC i386, de 256 Mo de RAM et d'un disque dur de 10 Go.

III.1.2. Installation

L'installation de Trixbox est assez simple. Il faut, premièrement, paramétrer le BIOS de la machine hôte pour qu'elle puisse démarrer sur le CD contenant l'image de Trixbox. Ensuite, redémarrer la machine et suivre les différentes étapes.

NB : Trixbox ne cohabite pas avec un autre système d'exploitation sur un même disque dur.

- Tapez sur la touche ENTREE pour lancer l'installation

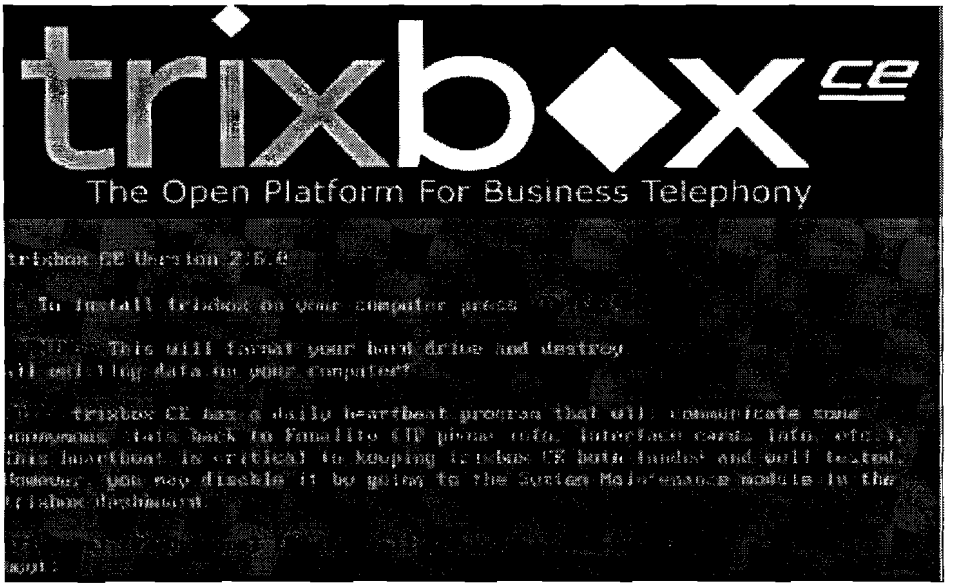


Figure 32 : Accueil d'installation

- Choix de la langue du clavier

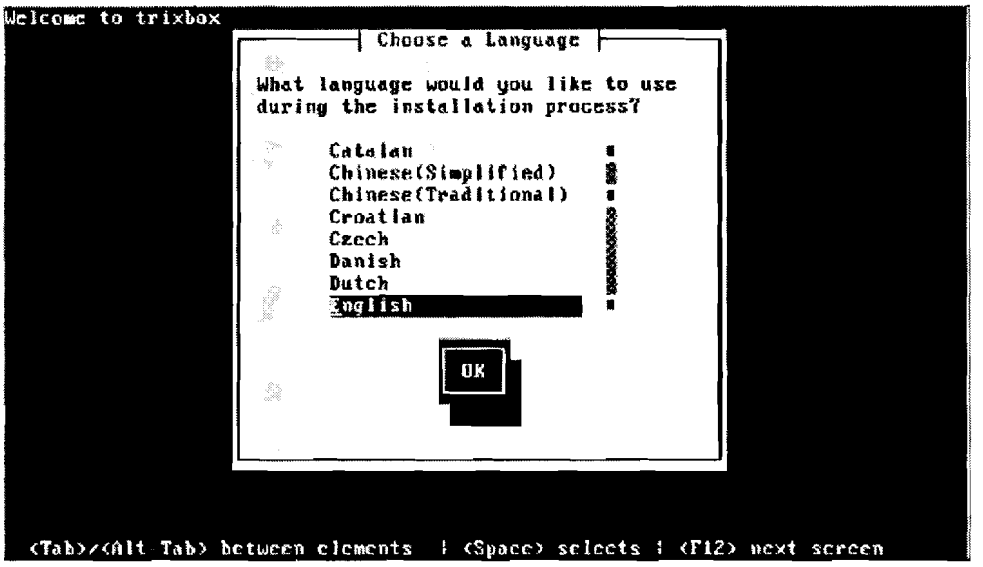


Figure 33 : choix de la langue du clavier

- Choix du fuseau horaire

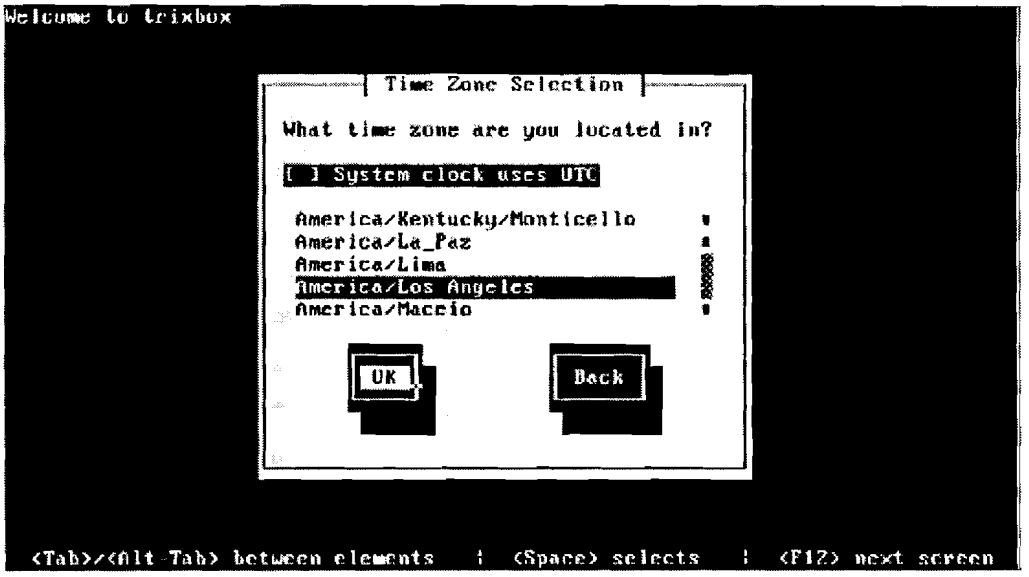


Figure 34 : Choix du fuseau horaire

- Choix du mot de passe administrateur

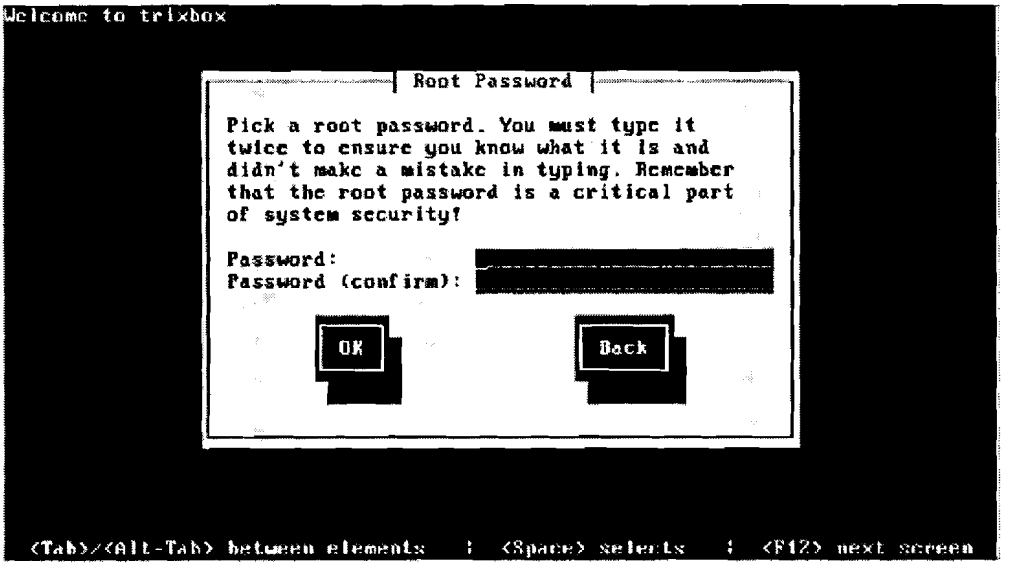


Figure 35 : Choix du mot de passe administrateur

L'installation commence dès la confirmation du mot de passe en formatant le disque dur. Comptez 30 min à 1h pour une installation complète et configurable.

A la fin de l'installation la machine éjecte le CD et se redémarre.

Après redémarrage, nous obtenons l'écran avec une invite de commande demandant de s'authentifier. Taper root et valider par la touche ENTREE puis saisir le mot de passe de choix à l'installation.

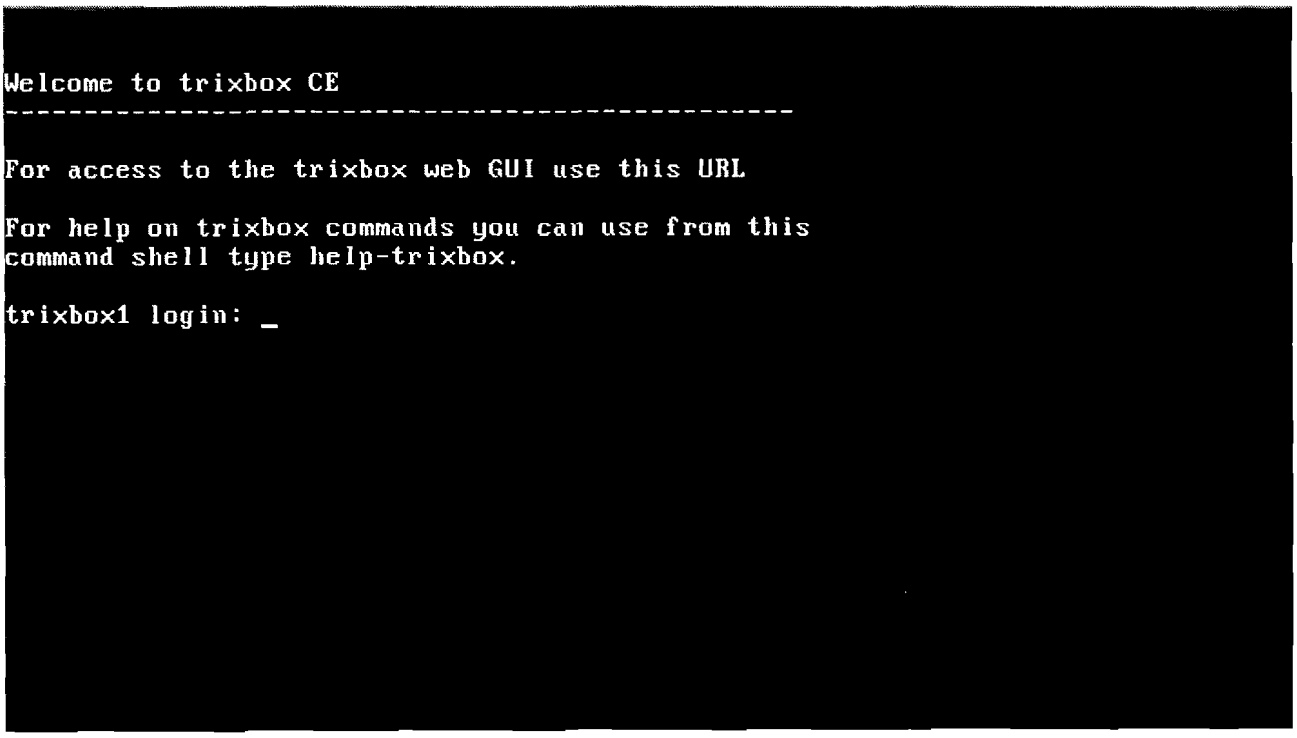


Figure 36 : connexion au compte root

Une fois l'authentification effectuée, vous pouvez commencer la configuration de serveur Trixbox.

III.2. Configuration

III.2.1. Obtenir de l'aide

Pour obtenir de l'aide, entrez help-trixbox à la suite du prompt. Vous obtiendrez un écran d'aide qui présente aussi les commandes nécessaires au changement de mot de passe des différents utilisateurs, par exemple passwd-maint pour l'utilisateur maint et passwd pour l'utilisateur root.

```
trixbox - HELP

Commands                Descriptions
------------------------------------------------------------------
system-config-network   configure ethernet interface
passwd-maint            set master password for web GUI
passwd                  set root password for console login
setup-cisco             create a SIPDefault.cnf in /tftpboot
setup-aastra            create a aastra.cfg in /tftpboot
setup-grandstream       setup for autoconfiguration of Grandstream
setup-linksys           setup for configuration of Linksys phones
setup-polycom           setup for polycom phones
setup-snom              setup for snom phones
setup-dhcp              set up a dhcp server
setup-rhino             setup tool for Rhino TDM cards
setup-samba             set up a Samba server (Microsoft file sharing)
setup-mail              configure postfix
setup-pstn              detect and setup supported PSTN interface cards
asterisk -r             Asterisk CLI
install-fail2ban        Install fail2ban, a useful security program.
install-postfix         Install postfix mail server (installed by default)
install-sendmail        Install sendmail mail server

[trixbox1.localdomain ~]# _
```

Figure 37 : Help-List

III.2.2. Configuration de l'interface réseau

Par défaut l'interface réseau est configurée pour prendre une adresse IP fournit par un serveur DHCP. Il nous faudra assigner une adresse IP statique à notre IPBX. Pour se faire, il suffit d'exécuter la commande system-config-network sur le Shell et l'image ci-dessous apparaît sur le moniteur.

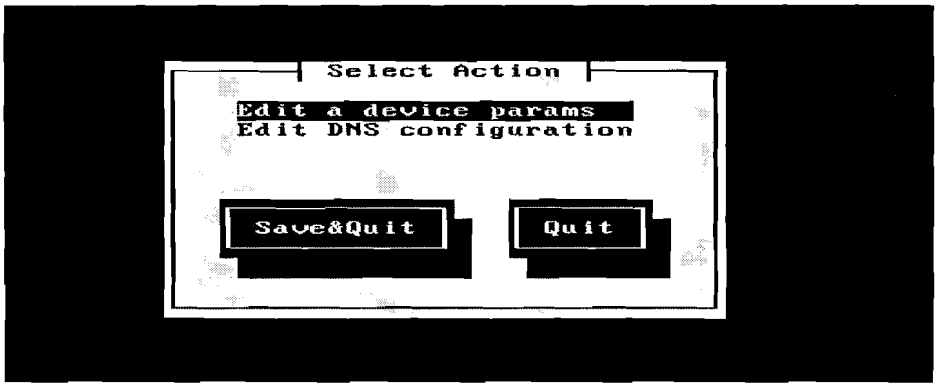


Figure 38 : Configuration de l'interface réseau

En pressant sur la touche ENTRER du clavier on obtient l'image ci-dessous, l'écran nous permettant d'éditer les paramètres de notre interface réseau.

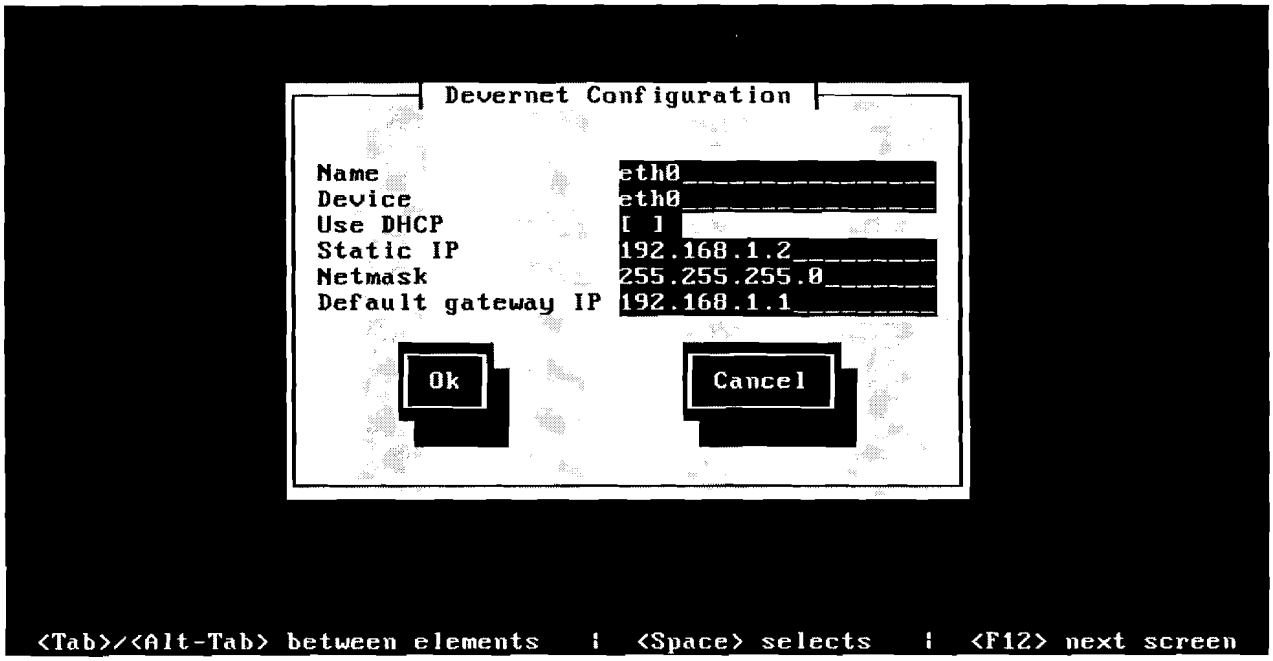


Figure 39 : Adressage-Statique

Pour naviguer entre les différents champs, utiliser la touche Tabulation et entrer l'adresse IP qui doit être donnée à votre serveur asterisk, le masque de sous réseau, la passerelle par défaut, et le DNS primaire, décocher l'option Use DHCP (la présence d'un astérisque dans les crochets témoigne que Use DHCP est cochée) grâce à la touche Espace comme dans l'exemple ci-dessus.

Dans le champ adresse IP (IP address), entrer l'adresse IP en tenant compte de votre plage d'adresse IP.

Masque de réseau (Netmask) : le plus souvent 255.255.255.0 (sauf cas de masque de sous réseau)

Passerelle par défaut : (Default gateway) : c'est l'adresse IP de votre routeur.

DNS primaire (primary nameserver) : si vous restez dans votre groupe de travail vous pouvez entrer l'adresse de votre passerelle par défaut. A la fin, validez par OK.

III.2.3. Configuration du mot de passe de l'utilisateur maint

L'utilisateur maint permet l'accès à l'interface web pour la configuration de Trixbox. Pour changer son mot de passe, il suffit d'exécuter la commande passwd-maint

et de rentrer le mot de passe choix. L'image ci-dessous apparaît sur le moniteur ;

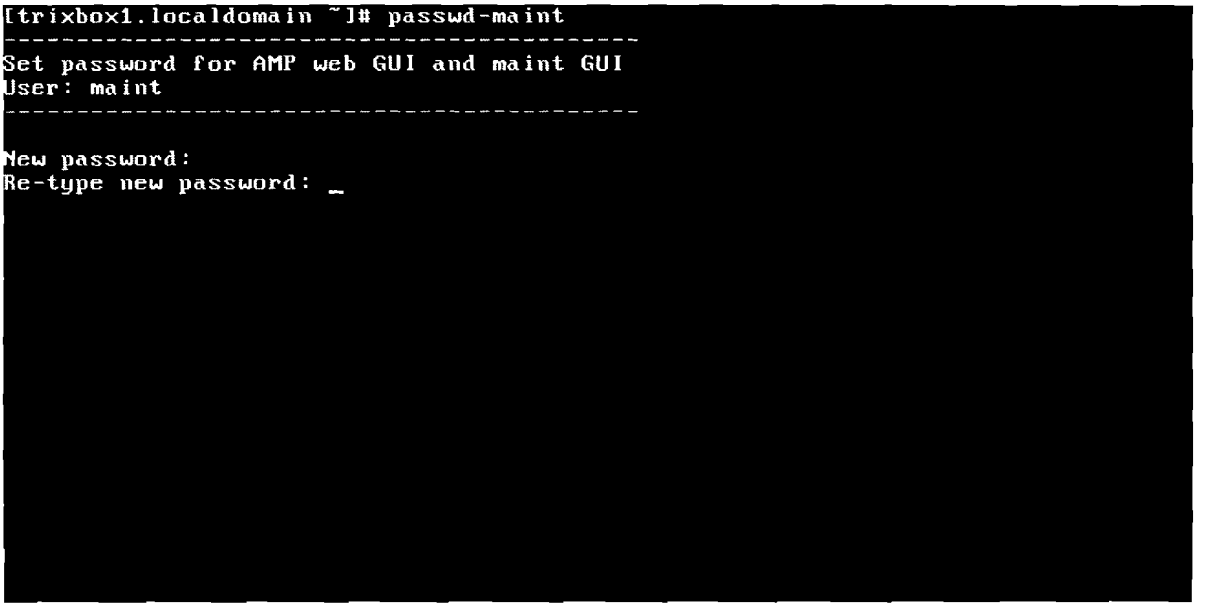


Figure 40 : Configuration du mot de passe de l'utilisateur maint

Une fois ces configurations terminées, redémarrer la machine pour que Asterisk puisse les prendre en compte en exécutant successivement les commandes suivantes :

- amportal stop
- shutdown -r now

III.2.4. Configuration de Trixbox par interface web

Pour pouvoir configurer Trixbox via interface web, nous utilisons un ordinateur quelconque qui est dans le même réseau que le serveur Trixbox et grâce à un navigateur web, nous entrons dans la barre d'adresse http://adresse-serveur-trixbox/ (par exemple http://192.168.1.2 dans notre cas). L'image ci-dessous apparaît sur l'écran présentant la page d'accueil.

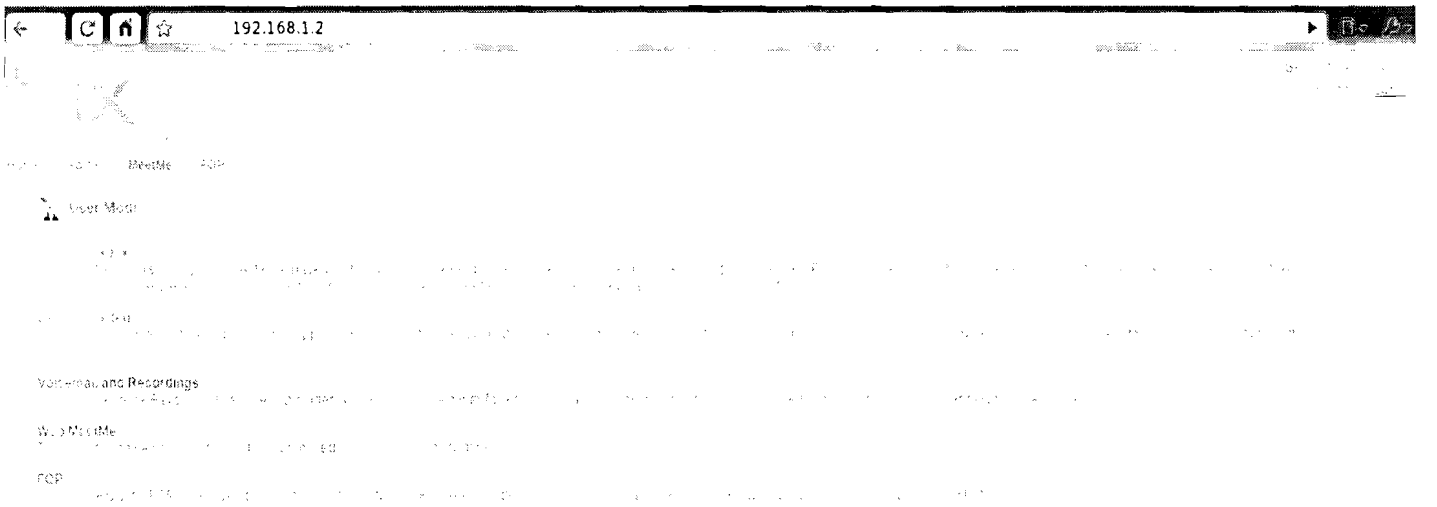


Figure 41 : Page d'accueil Trixbox

Une fois la connexion à l'interface web faite, nous basculons en mode admin en cliquant sur le bouton [switch] dans le coin supérieur droit de l'écran. Une fenêtre apparaît nous invitant à nous authentifier.

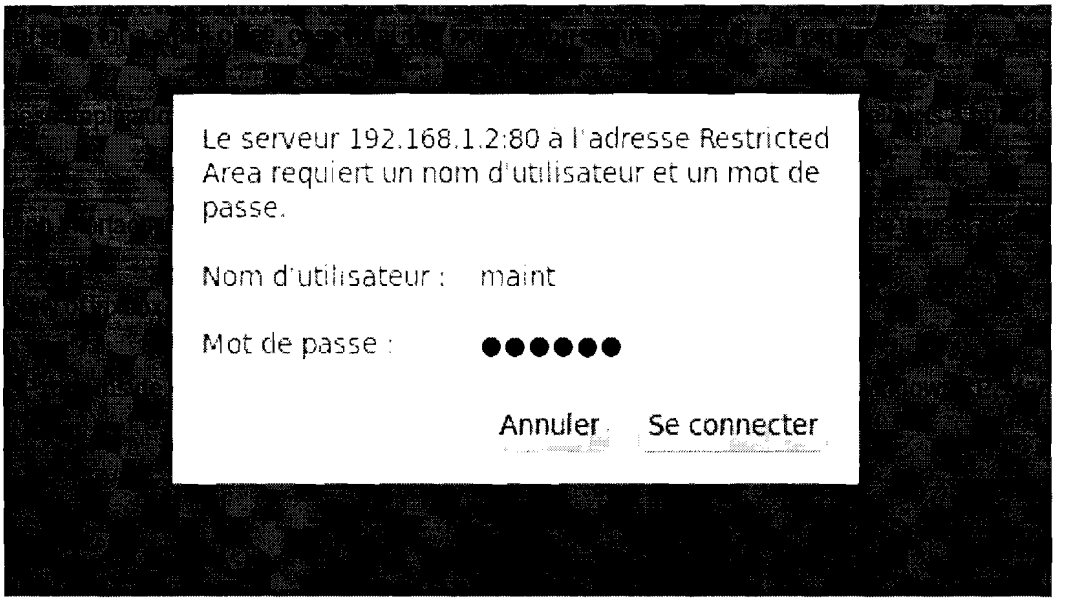


Figure 42 : Mode administrateur

III.2.5. Dial Plan (Plan de numérotation)

Afin de poursuivre notre configuration par la création des comptes et des routes

entrantes et sortantes, nous devons déterminer notre plan de numérotation. Dans notre cas, nous avons décidé d' attribuer à chaque utilisateur un numéro unique à quatre (04) chiffres sous cette forme 2XXX pour qu'ils puissent se joindre en composant ce numéro.

Ensuite, nous allons attribuer au canal de communication (trunk) vers l'extérieur du système ToIP, un index compris entre 1 et 100. Par exemple quand un utilisateur veut passer un appel externe à son système ToIP, il doit composer l'index du canal plus le numéro de téléphone de l'utilisateur externe. Le tableau ci-dessous donner un exemple d'attribution d'index.

Index	**Canal de communication**
03	Vers la ligne téléphonique de l'ONATEL

III.2.6. Ajout d'un terminal téléphonique

III.2.6.1. Création d'une extension SIP

Pour que chaque utilisateur du système ToIP ait un compte, nous devons créer pour lui une extension SIP qui c omportera son numéro téléphonique par lequel il pourra joindre les autres et être joint, son nom d'utilisateur et son mot de passe au niveau de notre IPBX. La description des différents paramètres à renseigner pour la configuration d'une extension SIP est donnée dans l'annexe 1.

III.2.6.2. Déclaration d'un téléphone IP

Chaque téléphone IP doit être au niveau de l'IPBX, notamment en précisant la marque, le model et l'adresse MAC du téléphone.

III.2.6.3. Configuration d'un téléphone IP

Pour qu'un utilisateur puisse passer ou recevoir des appels avec son téléphone IP, il faut configurer une ligne téléphonique de type SIP au niveau de ce dernier. La ligne

devra comporter entre autre, l'adresse IP de l'IPBX, le numéro de téléphone de l'utilisateur, le nom de l'utilisateur et son mot de passe.

III.2.7. Connexion du système de communication au réseau de l'ONATEL

III.2.7.1. Création d'un trunk ZAP

La création de trunk a pour but d'établir une connexion entre l'IPBX et notre canal de communication.

Pour cela, nous devons renseigner au niveau de l'IPBX le nom du trunk et le numéro du canal emprunté par les appels.

III.2.7.2. Création d'une route entrante

La création d'une route entrante (inbound route) permet de router l'appel de la ligne de l'ONATEL vers une extension téléphonique précise. La description des différents paramètres à renseigner pour la configuration d'une route entrante est donnée à l'annexe 2

III.2.7.3. Création d'une route sortante

La création d'une route sortante (outbound route) permet de router l'appel d'une extension téléphonique interne au système ToIP vers le canal de l'ONATEL. La description des différents paramètres à renseigner pour la configuration d'une route sortante est donnée à l'annexe 3.

III.2.8. Configuration des softphones

III.2.8.1. Configuration de X-Lite

Après avoir installé et configuré Trixbox, nous allons nous intéresser au poste client. Le poste client aura un micro/casque et du logiciel X-Lite. Pour ajouter une

extension SIP sur X-lite, nous cliquons sur le petit triangle encerclé de rouge puis sur SIP Account Settings.

Figure 43 : Xlite

Nous obtenons une nouvelle fenêtre comme suit :

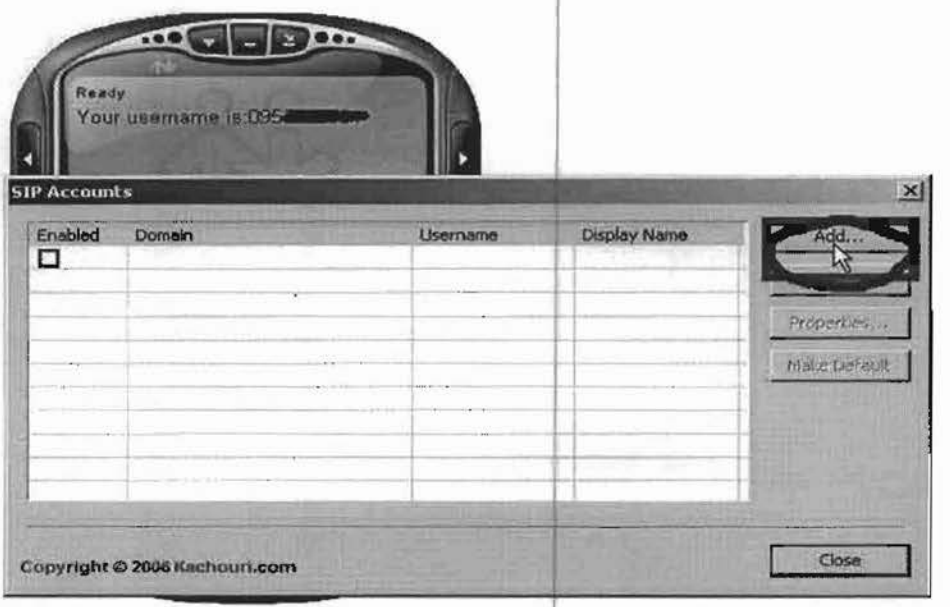


Figure 44 : Xlite Settings

A cette étape, nous cliquons sur le bouton **Add** encerclé en rouge ici. Une nouvelle fenêtre dans laquelle nous renseignerons les paramètres de l'extension s'ouvre. Les paramètres sont :

- Display Name : Libre à votre choix (votre nom, etc.) ;
- User name : Votre Login SIP ;
- Password : Votre mot de passe SIP ;
- Authorization user name: Votre Login SIP ;
- Domain : l'adresse du serveur ;
- Domain Proxy : Cochez « Register with domain and receive incoming calls ».

Compléments

1. Bouton d'accès au menu de configuration
2. Réduire la fenêtre
3. Quitter le programme
4. Affichage principal: état, appels, etc.
5. Accès au menu vidéo (option EyeBeam)
6. Liste des appels et des contacts
7. Ligne 1
8. Ligne 2
9. Accès au site de l'éditeur
10. Mettre en attente
11. Enregistrer
12. Réponse automatique
13. Conférence automatique
14. Ne pas déranger
15. Conférence
16. Appeler - prendre un appel
17. Raccrocher - terminer un appel
18. Touche Flash (fonctions dynamiques)
19. Recomposer le numéro précédent
20. Muet
21. Volume du haut-parleur
22. Volume du micro

Figure 45 : compléments xlite

III.2.8.2 Configuration de Ekiga

Au lancement du logiciel Ekiga, il faut suivre les différentes étapes de configuration de l'Assistant de configuration.

Figure 46 : Ekiga

Pour ajouter une extension SIP à Ekiga, il faut aller sur **Edit** puis **Accounts.** Une nouvelle fenêtre apparaît dans laquelle il faut cliquer sur **Accounts** puis **Add a SIP Account.** Ceci fait apparaître une dernière fenêtre invitant à renseigner les paramètres.

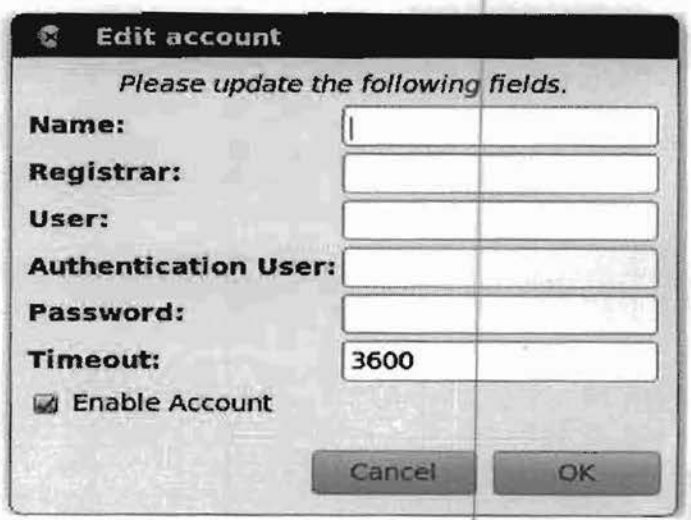


Figure 47 : Ekiga Settings

- **Name** : Libre à votre choix (votre nom, etc.) ;
- **Registrar :** l'adresse du serveur ;
- **User :** Votre Login SIP
- **Authentification User :** Votre Login SIP
- **Password :** Votre mot de passe SIP

QUATRIEME PARTIE : Evaluation des coûts

QUATRIEME PARTIE : Evaluation des coûts

Pour une mise en place du système étudié à sa dimension minimal on aura besoin au minimum du montant indique après estimation des coûts des équipements.

Désignation	Caractéristique	Quantité	Prix unitaire	Montant (F CFA)
Ordinateur Serveur	1 Go de RAM, 80Go disque dur, un processeur Core-duo d'Intel avec une mémoire cache 2 MB	1	800000	800000
Ordinateur Serveur	HP Proliant ML 500 quadricoeur, intel xéon	1	990000	990000
Système d'exploitation	Trixbox	-	-	Gratuit
Softphones	Ekiga, X-lite	-	-	Gratuit
Téléphones IP	Cisco IP phone 7940	-	75 000	
Carte téléphonique	Carte TDM22B	1	230000	230000
Main d'œuvre	-	-	-	600000
Montant Total	-	-	-	2620000

CONCLUSION

La téléphonie sur le protocole internet, toujours à l'état embryonnaire au Burkina Faso, est une innovation technologique dans le domaine de la télécommunication qui apporte avec elle de nombreux avantages tels que la réduction des coûts de communication, la disponibilité et la mobilité des employés, la simplification des infrastructures etc. La téléphonie sur IP gagne du terrain dans le domaine de communication. Beaucoup sont les entreprises qui s'orientent vers cette nouvelle technologie.

Notre travail a consisté à la proposition d'une solution de mise en place d'un système de communication global ToIP basé essentiellement sur les logiciels libres notamment la plateforme libre et gratuite « Trixbox CE» et les softphones « Ekiga et X-lite » dont l'abondance de documentation nous a fascinés.

La solution proposée s'est focalisée d'une part sur la gestion centralisée du système de communication ToIP et d'autre part sur la connexion de l'IPBX au réseau téléphonique publique de l'ONATEL.

Ce stage nous a permis de découvrir un autre type de service qu'offrent les réseaux informatiques. Nous saurons terminer sans dire « Vive le monde libre, vive les innovations technologiques»

ANNEXE

ANNEXE 1 : Extensions

Il y a essentiellement 3 types d'extension :

- SIP : pour connecter un client SIP.
- IAX2 : pour connecter un client IAX.
- ZAP : pour connecter un téléphone analogique grâce à une interface FXS ou un téléphone ISDN grâce à une interface ISDN.

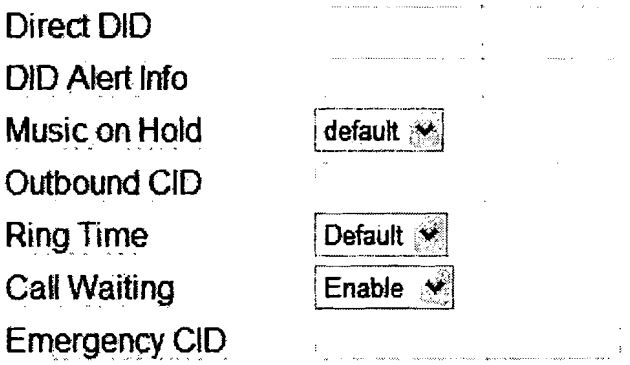
Certains de ces champs n'apparaissent pas lors de la création de l'extension mais seront visibles dès que l'on va sur la page de l'extension créée.

Add Extension

User Extension	
Display Name	
CID Num Alias	
SIP Alias	

- **User Extension**: Numéro de téléphone interne de l'extension.
- **Display Name**: Nom de l'extension, qui apparaîtra lorsqu'un appel est émis, il peut être effacé si l'appel passe par une ligne d'un opérateur téléphonique.
- **CID Num Alias**: Permet de changer le numéro de l'appelant pour les appels internes, il masque alors le numéro de l'extension.
- **SIP Alias**: Permet de recevoir des appels anonymes sur l'extension depuis l'intranet ou l'extranet. Par exemple si l'on met dans ce champ la valeur « toto », alors on peut appeler cette extension depuis n'importe quel endroit en appelant SIP/alias@domaine.com. Pour que cela fonctionne il faut par ailleurs que l'option Allow Anonymous Inbound SIP Calls? dans General Settings soit mise sur yes, ce qui, pour des questions de sécurité n'est pas conseillé.

Extension Options



- **Direct DID :** La valeur donnée ici est généralement un numéro mais peut être une chaîne de caractères. Les appels entrants, sur un trunk enregistré avec un DIDnumber qui a la même valeur, seront aiguillés vers cette extension. Par défaut, mettre la même valeur que User Extension.
- **DID Alert Info:** Ne fonctionne que si un Direct DID est spécifié. Il permet de faire sonner des téléphones SIP avec des sonneries particulières en fonction de la valeur de l'alerte. Il faut que cette fonctionnalité soit disponible sur le téléphone SIP.

- **Music on Hold:** Permet de choisir la musique d'attente.
- **Outbound CID :** Identité de l'appelant pour les appels émis depuis cette extension. Syntaxe « Mon nom » <0123456>. Il se peut qu'un opérateur téléphonique écrase ces informations.
- **Ring Time :** Nombre de secondes durant lesquelles l'extension sonnera avant que l'appel ne soit renvoyé vers la messagerie (si elle est activée pour l'extension). La valeur par défaut est celle spécifiée dans l'onglet General Settings (15 secondes).
- **Call Waiting:** Permet d'activer la mise en attente pour l'extension.
- **Emergency CID:** Permet de spécifier un numéro de téléphone qui sera transmis lors d'un appel vers les services d'urgence.

Device Options

This device uses sip technology.	
secret	1234
dtmfmode	rfc2833
canreinvite	no
context	from-internal
host	dynamic
type	friend
nat	yes
port	5060
qualify	yes
callgroup	
pickupgroup	
disallow	
allow	
dial	SIP/11
accountcode	
mailbox	11@default

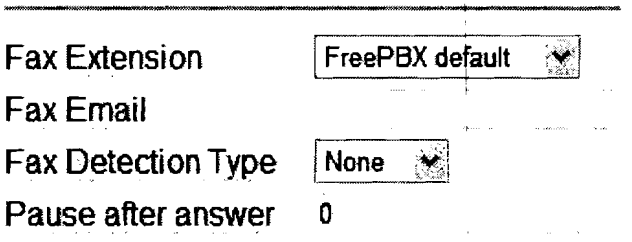
- **Secret:** Mot de passe de l'extension.
- **Dtmfmode**: Mode des fréquences vocales. Pour la France, laisser la valeur par défaut rfc2833.
- **Canreinvite:** Permet de spécifier si l'on souhaite utiliser les messages SIP REINVITE. Tous les flux audio (RTP stream) sont gérés par le processus Asterisk durant les appels. Les messages REINVITE permettent de rerouter les flux RTP afin que l'appel soit établi. Dans le cas d'utilisateurs à distance, ceci permet de réduire la charge des équipements. Il est conseillé d'utiliser cette fonction seulement après avoir testé toutes les autres fonctions dont on a besoin.
- **Host:** Valeurs possibles dynamiques ou une adresse IP. Si une adresse IP est spécifiée alors le client SIP ne pourra se connecter à cette extension qu'à condition qu'il ait cette adresse IP.
- **Type :** Valeurs: friend ou peer. Choisir friend si l'extension est un téléphone. Choisir peer pour les périphériques capables de transporter les appels tel qu'un

trunk.

- **Nat :** Valeurs: no ou yes. Utiliser cette dernière si l'extension se trouve derrière un NAT.
- **Port:** Ce champ n'a pas d'incidence dans le cas d'une extension.

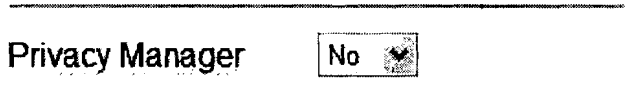
- **Qualify :** Valeur yes, no ou xx, xx étant un nombre de millisecondes, permet de considérer que le client est hors de portée si la latence est trop longue.
- **Callgroup:** Définit le groupe d'appel pour les appels vers ce dispositif.
- **Pickupgroup:** Permet de spécifier le groupe à vérifier lors d'un appel entrant. Si aucune valeur n'est inscrite, il sera utilisé le groupe spécifié dans sip.conf.
- **Disallow:** codecs interdits pour l'extension
- **Allow :** codecs autorisés pour l'extension
- **Dial :** SIP/user_extension par défaut.
- **Accountcode :** Ce champ est utilisé pour alimenter le "accountcode" de la CDR. Entrer un code de compte pour l'utilisation par un module de facturation
- **Mailbox :** Permet de configurer la boîte vocale liée à cette extension. On peut définir plusieurs boîtes vocales séparées par des virgules.
- **Custom Context :** Bien que ce module ne soit pas officiel, il est indispensable dans certaines situations. En effet, la règle des appels sortants est la même pour toutes les extensions, elle est donnée par les Inbound Routes. Donc, si par exemple on veut qu'une extension puisse appeler l'international et pas une autre, cela n'est pas possible. Avec Custom Contexts cela est possible. En effet en installant ce module, on pourra créer différents contextes et donner différents droits à chaque contexte. Ensuite pour chaque extension, on peut attribuer un des contextes créés. Voir http://www.manuel-freepbx.com/wiki/index.php?page=Custom+Contexts

Fax Handling



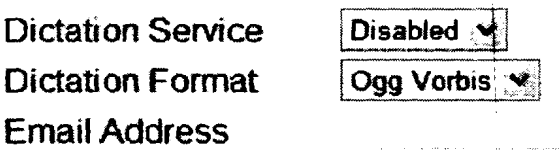
- **Fax Extension:** Destination des appels fax. La valeur peut être une extension, disabled, system (auquel cas les fax seront reçus par le système et renvoyés par email à l'adresse spécifiée dans le champ Fax Email) ou FreePBX default. Dans ce dernier cas, le fax sera traité selon la configuration spécifiée dans General Settings.
- **Fax Email**: Adresse destinataire des emails si la valeur de Fax Extension est system.
- **Fax Detection Type** : Permet de répondre automatiquement aux appels entrants et de jouer pendant un nombre de secondes déterminées dans le champ Pause after answer la musique de détection de fax. S'il n'y a pas de fax détecté, l'extension se mettra à sonner. Valeur : NVFAX pour les trunks SIP et IAX ou Zaptel pour les trunks ZAP.
- **Pause after answer** : Nombre de secondes pour la détection de fax avant le réacheminement de l'appel.

Privacy



- **Privacy Manager :** Si la valeur est yes, alors si un appel arrive sans CallerID, il lui sera demandé de composer son numéro à 10 chiffres (il y aura 3 tentatives) avant que l'extension se mette à sonner. Cela permettra d'avoir toujours un numéro affiché sur le téléphone en recevant un appel avant de décrocher, on peut alors décider répondre ou non.

Dictation Services

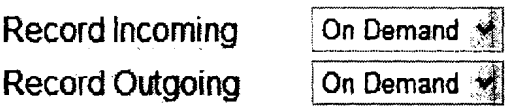


Permet de dicter des messages au système puis de les envoyer par email vers une adresse spécifiée dans la page de l'extension.

Ceci peut être utile par exemple pour une personne A qui demande souvent à une personne B des tâches à accomplir et qui ne veut pas l'appeler à chaque fois ou par exemple si cette dernière n'est pas tout le temps à son bureau. Il lui suffira alors de configurer son extension avec l'adresse email de la personne B pour la dictation et ensuite d'enregistrer les messages et de les lui envoyer.

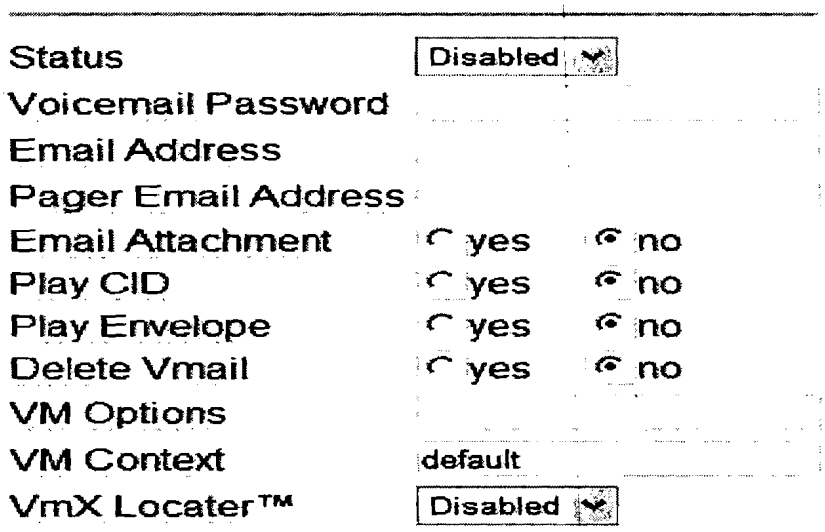
- **Dictation Service :** Activer ou désactiver le service.
- **Dictation Format :** Format d'enregistrement des messages.
- **Email Address :** Adresse email pour l'envoi des messages enregistrés.

Recording Options



- **Record Incoming** : Enregistrement des appels entrants.
- **Record Outgoing :** Enregistrement des appels sortants.

Voicemail & Directory



- **Status :** Activation de la messagerie.
- **Voicemail Password :** Mot de passe pour accéder à la messagerie. Pourra aussi être changé depuis le téléphone en composant *98.
- **Email Address :** Adresse vers laquelle seront envoyés les messages vocaux.
- **Pager Email Address :** Adresse vers laquelle seront envoyés des courts messages notifiant la présence de messages sur la messagerie.
- **Email Attachment :** Permet d'envoyer les messages du répondeur par mail.
- **Play CID :** Ajoute le numéro de téléphone de l'appelant dans le message.
- **Play Envelope** : Ajoute l'heure et la date dans le message.
- **Delete Vmail :** Le message sera supprimé du répondeur après être envoyé par mail.
- **VM Options : ...**
- **VM Contexe : ...**
- **VmX Locater™ :** S'il est mis sur Enabled, autorise l'utilisateur de l'extension de configurer les variables de la messagerie depuis le User Portal ARI.

ANNEXE 2 : Inbound Routes

Permet d'établir des règles de traitements des appels arrivant depuis les trunks.

Fonctionnement

Lorsqu'un appel arrive vers un trunk, l'aiguillage sera fait en fonction du DIDnumber avec lequel le trunk est enregistré et du CallerID de l'appelant si la ligne téléphonique transmet aussi le CallerID.

Le DIDnumber sera alors comparé aux numéros des extensions et des Direct DID des extensions. S'il ne trouve pas d'issue, il sera alors comparé aux caractéristiques des Inbound Routes, de la première vers la dernière. L'appel sera alors aiguillé selon la première route conforme à l'appel.

Configuration

Add Incoming Route

Description:
DID Number:
Caller ID Number:
OR

Zaptel Channel:

- **Description :** Nom donné à la route.
- **DID Number :** DIDnumber auquel doit être conforme l'appel entrant pour suivre cette route. A noter que ceci ne dépend pas de la personne qui appelle mais du trunk sur lequel arrive l'appel, en effet, le DIDnumber est spécifié dans le registration string du tunk, voir page trunk. On peut utiliser les wildcard (caractère qui permet de remplacer un ou plusieurs autres caractères) X, Z, N... dans le DIDnumber pour prendre en compte plusieurs numéros. Si DID Number est vide alors cette route prendra n'importe quel DID Number.

- **Caller ID Number:** Caller ID auquel doit être conforme l'appel entrant pour suivre cette route. Ceci dépend du numéro depuis lequel la personne appelle, et peut être inexistant si la ligne téléphonique dont on dispose ne donne pas l'identité de l'appelant. On peut utiliser les wildecard X, Z, N... dans le Caller ID Number pour prendre en compte plusieurs numéros. Si Caller ID Number est vide alors

cette route prendra n'importe quel Caller ID.

- **Zaptel Channel** : Canaux ZAP que prend cette route. Utile uniquement si on utilise des interfaces FXO

Fax Handling

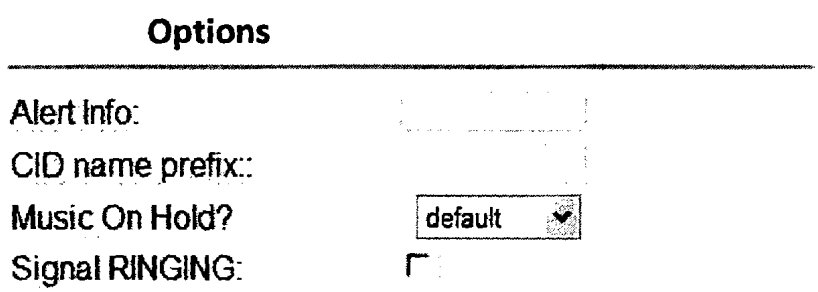
Fax Extension	FreePBX default
Fax Email	
Fax Detection Type	None
Pause after answer	0

- **Fax Extension**: Destination des appels fax. La valeur peut être une extension, disabled, system (auquel cas les fax seront reçus par le système et renvoyés par email à l'adresse spécifiée dans le champ Fax Email) ou FreePBX default. Dans ce dernier cas, le fax sera traité selon la configuration spécifiée dans General Settings.
- **Fax Email** : Adresse destinataire des emails si la valeur de Fax Extension est system.
- **Fax Detection Type**: Permet de répondre automatiquement aux appels entrants et de jouer pendant un nombre de secondes déterminées dans le champ Pause after answer la musique de détection de fax. S'il n y pas de fax détecté, l'extension se mettra à sonner. Valeur : NVFAX pour les trunks SIP et IAX ou Zaptel pour les trunks ZAP.
- **Pause after answer:** Nombre de secondes pour la détection de fax avant le réacheminement de l'appel.

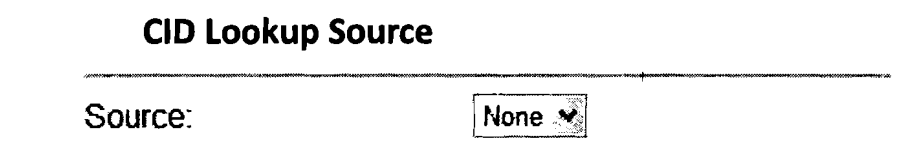
Privacy

Privacy Manager	No

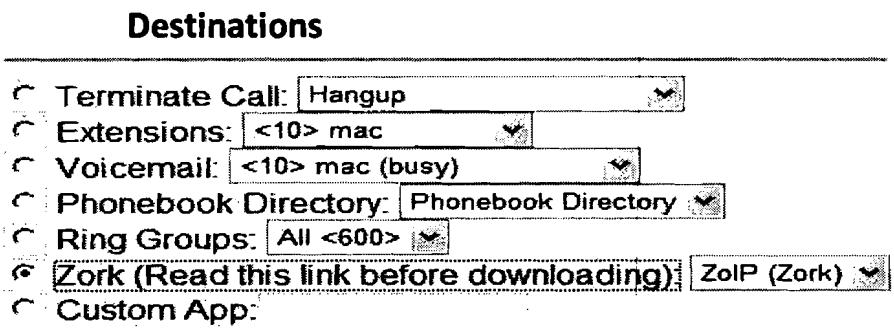
- **Privacy Manager**: Si la valeur est yes, alors si un appel arrive sans CallerID, il lui sera demandé de composer son numéro à 10 chiffres (il y aura 3 tentatives) avant que l'extension ne se mette à sonner. Cela permettra d'avoir toujours un numéro affiché sur le téléphone en recevant un appel avant de décrocher, on peut alors décider de répondre ou non.



- **Alert Info :** Ne fonctionne que si un Direct DID est spécifié. Permet de faire sonner des téléphones SIP avec des sonneries particulières en fonction de la valeur de l'alerte. Il faut que cette fonctionnalité soit disponible sur le téléphone SIP.
- **CID name prefix**: Permet de rajouter un préfixe au CallerID avant de l'aiguiller.
- **Music On Hold :** Musique d'attente pour les appels arrivant sur cette route.
- **Signal RINGING**: Quand un téléphone SIP reçoit un appel, il envoie un message Ringing à l'émetteur de l'appel avant de commencer à sonner. Mais si l'appel est orienté vers un IVR au lieu d'un téléphone, il n'y aura pas de message Ringing envoyé. Il se trouve que certains serveurs SIP ont besoin que le destinataire envoie le message Ringing avant le message Answer (envoyé quand on décroche). Dans le cas d'un IVR, il y aura directement le message Answer sans passer par le message Ringing. Donc si on rencontre un tel problème, il suffit de cocher cette case, et un message Ringing sera toujours envoyé avant un message Answer.



- **Source :** Cette ligne n'apparaît que si le module Caller ID Lookup est installé. Elle permet d'ajouter le nom de l'appelant en plus du numéro de l'appelant s'il est résolu dans la source sélectionnée.



Pour l'aiguillage des appels on a souvent affaire à des conditions contre lesquelles un appel est testé afin de déterminer sa destination. C'est le cas des Inbound Routes, IVR, Day Night Mode...

Le choix de la destination est en général proposé après la détermination des conditions. Il est introduit par exemple par :

- Set Destination.
- Destination for Orphaned Parked Calls.
- Destination if no answer.
- Fail Over Destination.

Il faut alors choisir parmi les possibilités proposées. Certaines n'existent que si le module correspondant est installé.

- **Terminate Call :** Termine la communication. Il y a le choix entre raccrocher, jouer le message « all circuits are busy now » puis raccrocher, jouer le message busy, jouer la tonalité de ligne raccrochée mais sans raccrocher ou mettre le correspondant indéfiniment en hold.
- **Extensions:** Oriente l'appel vers une extension.

- **Voicemail:** Oriente l'appel vers un répondeur.
- **Phonebook Directory :** Permet d'appeler les extensions en composant le nom de la personne rattachée à celles-ci depuis le pavé numérique du téléphone. Ce module n'est pas un annuaire en soi, mais il permet d'appeler des destinations à partir du nom qui leur est rattaché.

Il y a l'annuaire par défaut Company Directory généré automatiquement pour les extensions à partir de ce qui est écrit dans le champ Display Name sous le format Prénom Nom. On peut créer un autre annuaire avec des numéros externes grâce au module Phonebook.

- **Ring Groups :** Permet de choisir des groupes de téléphones pour les appels entrants. Les téléphones sonneront ensemble ou successivement lorsqu'un appel arrive vers ce groupe. Un Ring Group est vu comme une extension virtuelle, il a un numéro comme toute extension.
- **Zork :** ...
- **Custom App** : Utilise la commande Goto() pour envoyer le correspondant vers un custom context. Le nom du contexte doit commencer avec « custom-« et être au format custom-context, extension,priority. Exemple : custom-myapp,s,1.

ANNEXE 3 : Outbound Routes

Permet d'établir des règles de traitements des appels sortants vers les trunks.

Lorsqu'un appel sortant est émis, l'aiguillage sera fait en fonction du numéro appelé.

Le numéro appelé sera comparé aux règles autorisées dans chaque Outbound Route en commençant par la première route. Dès qu'une route autorisant ce numéro est rencontrée, l'appel sera traité par cette route.

A noter qu'il est possible d'arranger l'ordre de priorité des routes grâce aux flèches orientées vers le haut et vers le bas.

Par ailleurs, si l'on utilise le module Custom Contexts, l'ordre de priorité des routes défini dans cette page passera au second plan et n'aura d'effet que si les priorités des

routes, définies dans la page du contexte concerné au paragraphe Outbound Routes grâce à au champ Priority, ont la même valeur.

- **Route Name :** Nom à donner à cette route.
- **Route Password**: Mot de passe de la route, si l'on veut protéger cette route par mot de passe. Il sera demandé à l'appelant pour laisser passer son appel.
- **PIN Set :** Ce champ n'apparaît que si le module PIN Sets est installé. Si un PIN Set est spécifié alors le champ Route Password sera ignoré et les mots de passe de la route seront ceux spécifiés dans le PIN Set utilisé.
- **Emergency Dialing** : Indique que cette route est utilisée pour les appels d'urgence. Le Caller ID sera alors remplacé par le Emergency CID de l'extension.
- **Intra Company Route** : Si cette route est utilisée pour appeler un autre site de l'entreprise à travers les trunk, alors cette option permet d'utiliser les Caller ID interne au lieu de ceux externes.
- **Music On Hold**: Musique d'attente pour la route.
- **Dial Patterns :** Patterns autorisés par la route. Mettre un pattern par ligne. On peut utiliser les wildecards X (0-9), Z (1-9), N (2-9), le point qui désigne toute suite de chiffre longue d'au moins 1 caractère et la barre verticale ou pipe | qui indique un préfixe à enlever avant de passer le numéro au trunk. Par exemple: « 354|[13-68]NXXXX. » prend les numéros commençant par 345 ensuite un des chiffres 1,3,4,5,6 ou 8, ensuite un des chiffres de 2 à 9, enfin au moins 5 autres chiffres quelconques. Le numéro sera alors tronqué du préfixe 345 et passé au trunk de la route.

  « . » pour tous les numéros

  « 0|. » pour tous les numéros avec le 0 pour « sortir »
- **Dial patterns wizards** : Permet de rentrer des patterns préconfigurés pour les USA, on peut modifier ces modèles en modifiant le code source du web Freepbx.
- **Trunk Sequence** : Séquence de trunks pour aiguiller l'appel. La route orientera l'appel vers le premier trunk libre de la liste. Si la communication n'est pas

réussie, le système essayera le trunk suivant. A noter qu'un trunk est considéré occupé s'il y a autant de communications (entrantes ou sortantes)

BIBLIOGRAPHIE

Site web

http://www.wikipedia.fr du 26/08/2010 au 8/11/2010
http://www.frameip.com/voip le 26/11/2010
http://www.frameip.com/toip le 04/11/2010
http://www.mcafee.com le 17/11/2010
http://www.lb.refer.org le 20/12/2010
http://www.asterisk.org le 16/12/2010
http://www.trixbox.org le 02/11/2010
http://2003.jres.org le 28/10/2010
http://www.xmco.fr le 17/11/2010
http://www.cyber6tem.com le 28/11/2010
http://www.xlite.pour.free.fr le 04/12/2010
http://www.infolog.mr le 06-01-2011

Rapports de stage

Intégration de RADIUS dans un réseau VOIP avec ASTERISK produit par Selim Ben Ahmed de heig-vd(Haute Ecole d'Ingénierie et de Gestion du canton de Vaud)

Etude de la mise en place d'un Intranet et des Services multimédia basés sur la technologie wifi produit par MILLOGO Souleymane et BAYALA Berenger de l'Ecole Supérieure d'Informatique de l'Université Polytechnique de Bobo-Dioulasso

ETUDE ET MISE EN PLACE D UN SYSTÈME DE COMMUNICATION DE VOIP : APPLIQUE A UN PABX IP OPEN SOURCE, produit par Bassirou KASSE, UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

Etude et mise en œuvre du service pilote ToIP de RENATER produit par Mr Mohamed El Mahdi BOUMEZZOUGH

DEPLOIEMENT D'UNE SOLUTION VOIP POUR ENTREPRISES MULTISITES produit par Thibault Bergeras, François Jeudy, Eric Vence à ESME Sudria

Livres

Bulding Telephony System with Asterisk de David Gomillion et Barrie Dempster

Asterisk The Futer of Telephony 2nd Edition de Jim Van Meggelen, Leif Madsen et Jared Smith

Trixbox without Tears de Ben Sharif