Ministère de l'Enseignement Supérieur, de la Recherche Scientifique et de l'Innovation
(**MESRSI**)

Secrétariat Général

Université Nazi BONI (**U.N.B.**)

Ecole Supérieure d'Informatique (**E.S.I**)

N°-67

Cycle des Ingénieurs de Conception en Informatique (**CICI**)

MÉMOIRE DE FIN DE CYCLE

Thème : « **Téléphonie IP à l'Université Nazi BONI : passage à échelle, QoS et mesures de sécurité** »

Présenté et soutenu le 24 octobre 2017

Auteur : **M. KABRE Gu-wendkuuni Bonaventure**

Maître de stage

M. BAYALA Béranger
Administrateur Réseau
DPNTIC-Bobo

Directeur de mémoire

Dr YELEMOU Tiguiane
Enseignant chercheur
Ecole Supérieure d'Informatique

Année Académique 2015-2016

DEDICACE

REMERCIEMENTS

Nous exprimons nos vifs remerciements à l'endroit de toute l'équipe pédagogique de l'Ecole Supérieure d'Informatique (ESI) et des intervenants professionnels, qui ont tous assuré avec dévouement notre formation.

Nous remercions également la Direction pour la Promotion des Nouvelles Technologies de l'Information et de la communication (DPNTIC) de l'Université Nazi BONI (U.N.B.) et toute l'équipe technique, dont l'apport nous a permis d'acquérir une expérience enrichissante dans le milieu professionnel.

Nos remerciements vont particulièrement aux personnes suivantes :

- Pr Théodore TAPSOBA, Enseignant Chercheur à l'ESI et Vice-Président de l'U.N.B., qui nous a permis de travailler dans son laboratoire ;
- Dr Tiguiane YELEMOU, Enseignant chercheur à l'ESI et Directeur de la DPNTIC notre Directeur de mémoire ;
- M. Béranger BAYALA, Administrateur réseau à la DPNTIC, notre maître de stage.

Enfin nous témoignons de notre gratitude à tous ceux qui n'ont ménagé aucun effort pour l'aboutissement de notre formation.

GLOSSAIRE

ACE	Access Control Entry
ACK	Code indiquant un accusé de réception dans une transmission
ACL	Access Control List
ADSL	Asymmetrical Digital Subscriber Line
AH	Authentification Header
ARP	Address Resolution Protocol
CAN	Convertisseur Analogique Numérique
CLI	Commande Line Interface
CNA	Convertisseur Analogique Numérique
CPU	Central Processing Unit
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dial
DMZ	Démilitarized Zone
DNS	Domain Name Server
DNS	Domain Name System
DoS	Deny of Service
DSP	Digital Signal Processor
DTMF	Dual-Tone Multi-Frequency
ESI	EcoleSupérieured'Informatique
ESP	Encapsulated Security Payload
FAI	Fournisseur d'Accès Internet
FTP	File Transfert Protocol
FXO	Foreign eXchange Office est un port qui reçoit la ligne téléphonique
FXS	Foreign eXchange Subscriber
GPL	General Public Licence
GSM	Global System for Mobile Communications
HTTP	HyperText Transfer Protocol
IAX	Inter-Asterisk eXchange
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IM	Instant Message
IP	Internet Protocol
IP-PBX ou IPBX	IP Private Branch exchange
ISDN	Integrated Service Data Network
ITU	International Telecommunications Union
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MCU	Multipoint Control Unit
MD5	Message Digest 5

MIC	Modulation par Impulsion et Codage
MIKEY	Multimedia Internet KEYing
MKI	Master Key identifier
MMUSIC	Multiparty MultiMedia Session Control
NAT	Network Address Translator
NAT	Network Address Translation
ONATEL	Office National des Telecommunications
OS	Operating System
OSI	Open System Interconnect
PABX ou PBX	Private Automatic Branch eXchange
PSTN	Public Switched Telephony Network
QoS	Quality of Service
RAM	Random Access Memory
RFC	Request for Comment
RNIS	Réseau Numérique à Intégration de Service
RTC	Réseau Téléphonique Commuté
RTCP	Real-time Transport Control Protocol
RTP	Real-Time Transport Protocol
RTSP	Real Time Streaming Protocol
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SRTP	Secure Real-time Transport Protocol
SSL	Secure Socket Layer
TCP	Transport Control Protocol
TDM	Time Division Multiplexing
TFTP	Trivial File Transfert Protocol
TIC	Technologie de l'Information et de la Communication
TLS	Transport Layer Security
ToIP	Telephony over Internet Protocol
TTL	Transistor Transistor Logic,
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
U.N.B.	Université Nazi Boni
UPB	Université Polytechnique de Bobo
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	World Area Network

Table des matières

Liste des figures

Liste des tableaux

PREAMBULE

L'Ecole Supérieure d'Informatique (ESI) est la première école supérieure publique d'ingénierie informatique au Burkina Faso. Elle fut créée en 1991 en vue de satisfaire le besoin exprimé par le premier Schéma Directeur Informatique (1991-1995) «édification de compétences nationales par la formation de spécialistes (analystes et ingénieurs) concepteurs de système d'information». D'abord implantée à Ouagadougou, l'Ecole Supérieure d'Informatique (ESI) a ensuite été installée au sein de l'Université Polytechnique de Bobo-Dioulasso en septembre 1995. Elle forme en trois (03) ans des ingénieurs de travaux en Systèmes d'Information et en Administration Réseaux et Systèmes ; mais aussi en cinq (05) ans des ingénieurs de conception en Informatique. Depuis 2010, le cycle d'ingénieurs de travaux Informatiques a basculé dans le système dit LMD qui comporte six (06) semestres.

L'obtention de l'ingéniorat de conception en informatique est conditionnée par la validation des années du cycle d'Ingénieur de Conception en Informatiques (CICI) dont un stage pratique d'au moins quatre (04) mois en entreprise à la dernière année. A cet effet, nous avons été reçus à la DPNTIC de l'U.N.B. pour un stage de six (06) mois, traitant de la téléphonie IP à l'U.N.B. ; c'est-à-dire l'impact socio-économique, le passage à échelle, la qualité de service et les mesures de sécurité.

Résumé

En dépit des progrès techniques, les communications téléphoniques à l'Université Nazi BONI (U.N.B.) demeurent un sérieux problème. En effet, les acteurs de l'Université investissent énormément leurs propres ressources dans les communications et malgré cela, les réseaux téléphoniques des opérateurs sont souvent saturés ou inaccessibles. En plus la solution « voix sur IP » existante est rudimentaire. Fort de cela, la Direction pour la promotion de TIC (DPNTIC) nous a confié la mise en place d'une solution « Voix sur IP » sécurisée, prenant en compte tous les acteurs de l'université et offrant une bonne qualité de service.

Soucieux de la réussite de la mission qui nous est confiée et conscients des contraintes liées à cette mission, la démarche de résolution adoptée est basée sur l'évaluation des besoins et l'étude comparative de quelques solutions envisageables.

Ainsi, le serveur de « voix sur IP » Wazo a été choisi. Il est libre, gratuit et offre des fonctionnalités cadrant avec les besoins de l'université. Les techniques d'amélioration de la qualité de service proposées sont la différenciation de services, l'augmentation et optimisation de la bande passante, la prise en compte de la puissance de traitements des routeurs et l'harmonisation du câblage et des équipements. Afin de garantir une bonne sécurité, nous avons opté de gérer la sécurité physique, la sécurisation des serveurs, le chiffrement des appels, la séparation de flux, la sécurisation des protocoles, le filtrage et la supervision.

Pour une meilleure qualité de son infrastructure réseau, l'Université doit envisager de payer et d'appliquer les politiques de sécurité de la famille 2700x de la norme ISO (International Standard Organisation) 17799.

Abstract

Despite technical advances, telephone communications at Nazi BONI University (UNB) remain a serious problem. Indeed, the University's players invest heavily their own resources in communications and nevertheless, the telephone networks of the operators are often saturated or inaccessible. In addition, the VoIP solution does not meet the university's needs. On top of that, the Direction for the Promotion of ICT (DPNTIC) entrusted us with theimplementation of a solution of a secure "Voice over IP" solution, taking into account all the actors of the university and offering a good quality of service.

Concerned about the success of the mission entrusted to us and aware of the constraints linked to this mission, the resolution process adopted is based on the needs assessment and the comparative study of some possible solutions.

Thus, the Wazo "Voice over IP" server was chosen. It is free, free and offers features that fit with the needs of the university.The techniques of improving the quality of service proposed the differentiationof services, the increase and optimization of the bandwidth, taking into account the processing power of the routers and the harmonization of the cabling and the equipment. In order to ensure good security, we have chosen to manage physical security, servers security, call encryption, stream separation, protocol security, filtering and monitoring.

For a better quality of its network infrastructure,the University should consider paying and applying the security policies of the 2700x family of the International Standard Organization (ISO) Standard 17799.

INTRODUCTION GENERALE

La maîtrise de l'information est devenue aujourd'hui un enjeu stratégique de développement dans tous les secteurs de la vie. Les TICs ont contribué à la vulgarisation, l'élaboration et la transmission de l'information. Le téléphone, autrefois vu comme un produit de luxe, est devenu un outil indispensable, si bien qu'une privation à certains moments peut entraver la réalisation de certaines tâches. Même si les communications téléphoniques sont presque gratuites dans certains pays, elles demeurent très coûteuses dans les pays comme le nôtre. Heureusement, les avancées technologiques n'ont pas épargné le monde de la téléphonie. Consciente des nouvelles options qui s'offrent à elle, l'U.N.B. n'a ménagé aucun effort pour améliorer ses moyens de communications. C'est dans ce sens que le thème « ***téléphonie sur IP à l'Université Nazi BONI : passage à échelle, QoS et mesures de sécurité*** » nous a été soumis.

L'U.N.B. dépense pour trois (03) lignes téléphoniques. En plus, le coût de la communication repose sur le budget personnel des employés qui manifestent de plus en plus leur mécontentement face à cette situation. Malgré ces coûts, les réseaux téléphoniques sont souvent saturés ou inaccessibles. En plus la solution VoIP existante ne satisfait pas les besoins de l'Université. Elle est en phase expérimentale et n'est exploitable que par une dizaine de personnes. Cela ralenti considérablement le travail dans ce sens que l'U.N.B. est repartie sur cinq (05) sites dont les distances varient entre un (01) et dix-sept (17) kilomètres. Les étudiants quant à eux, ne disposent pas de plateformes de discussion leur permettant de se partager les informations et les connaissances.

Pour mener à bien ce projet, il faudra analyser l'existant, analyser les besoins en communication de l'UPB en se basant sur le cahier de charge. Après cela, il conviendra de voir dans quelle mesure l'on peut effectuer le passage à échelle et quels outils utiliser pour garantir une bonne QoS et une sécurité. L'objectif global de cette étude est de faciliter et d'améliorer la communication entre les acteurs tout en réduisant le coût.

Le présent document qui synthétise nos travaux réalisés sur ce thème s'articule autour de six parties. Dans une première partie, nous aborderons la présentation générale du thème et de la structure d'accueil. Dans la deuxième partie, nous exposerons les généralités sur la téléphonie sur IP. Dans la troisième partie, nous ferons une analyse de l'existant et les besoins en communication de l'Université. Dans la quatrième partie, nous procéderons au

dimensionnement et couplage VoIP-GSM; Dans la cinquième partie, nous gèrerons la QoS ; et sixièmement les mesures de sécurité.

CHAPITRE I: PRESENTATION GENERALE

I.1 Introduction

Le présent chapitre donne une description générale de l'environnement du stage. Il s'agira tout d'abord de décrire la structure d'accueil. Ensuite nous présenterons le projet en faisant cas de la problématique, des objectifs et des résultats attendus.

I.2 Présentation de la structure d'accueil

L'U.P.B. (Université Polytechnique de Bobo-Dioulasso), devenue U.N.B. (Université Nazi BONI) en Mai 2017, est un établissement public à caractère scientifique, culturel et technique. Elle est chargée d'enseignement supérieur et de recherche scientifique. Située à Bobo-Dioulasso, l'U.N.B. comprend des Unités de Formation et de Recherche (U.F.R.), une école et des instituts dont la mission est de transmettre le savoir et de former des hommes et des femmes qui répondront aux besoins du pays.

L'Université comprend plusieurs Vice-présidences dont celle en charge des enseignements et de l'innovation pédagogique (VP/EIP). Pour les questions relatives aux Technologies de l'Information et de la Communication (TIC), l'Université dispose d'une direction technique : la Direction de la Promotion des Nouvelles Technologies de l'Information et de la Communication (DPNTIC). La DPNTIC est constituée d'une direction, d'un secrétariat et d'un service technique aux compétences variées.

Dans l'exercice de ses fonctions, la DPNTIC développe des applications pour les différents services et directions de l'U.N.B. forme le personnel et conseille l'administration sur les questions ou des points qui ont trait au domaine des TIC. Outre cela, elle est chargée de la gestion de toute l'infrastructure réseau de l'U.N.B. et des services disponibles sur cette infrastructure, notamment la téléphonie.

I.3 Présentation du projet

L'avancée technologique a rendu indispensable l'utilisation de certains outils ; le plus probant étant le téléphone. L'utilisation du téléphone a atteint un niveau où une privation de ne serait-ce quelques minutes peut handicaper sérieusement certains travaux. En effet dans un pays où l'accès à internet est rare et chère, le téléphone demeure l'outil le plus rapide et le plus efficace

pour joindre quelqu'un d'autre. Les différents acteurs de l'université quant à eux, n'échappent pas à cette réalité. C'est dans cet ordre d'idée que la DPNTIC, structure chargée des TICs à l'U.N.B. s'est donnée aussi pour mission, l'amélioration des communications téléphoniques sur les différents sites de l'université.

I.3.1 Problématique

Le personnel de l'université rencontre beaucoup de difficultés dans les communications téléphoniques. Ces problèmes sont entre autres :

- la cherté de l'abonnement chez les opérateurs de téléphonie ;
- l'indisponibilité fréquente des réseaux des opérateurs de téléphonie, surtout sur le site de Nasso ;
- la difficulté d'organiser les rencontres ;
- la saturation occasionnelle des réseaux téléphoniques;
- l'impossibilité de passer des appels vidéo en local;
- la restriction de l'interphone.

Par ailleurs, d'autres préoccupations se font sentir au niveau des étudiants et mieux encore au niveau des ingénieurs de la DPNTIC. En effet, les étudiants travaillent régulièrement en groupes et ont besoin de communiquer entre eux. Le mieux pour eux serait d'avoir une plateforme leur permettant de rester permanemment en contact et de se partager les connaissances. Ils doivent pouvoir consulter leurs enseignants pour certains travaux.

Au vu de tous ces besoins la DPNTIC a mené des réflexions pour tenter de répondre à toutes les attendes de ces quinze mille (15 000) étudiants et trois-cent (300) fonctionnaires et contractuels avec les moyens qu'elle dispose tout en garantissant la sécurité et la qualité de service nécessaire ; d'où le thème « ***téléphonie sur IP à l'U.N.B. : impact socio-économique, passage à échelle, QoS et mesures de sécurité*** ».

I.3.2 Objectifs et résultats attendus

En termes d'objectifs, nous avons d'une part les objectifs globaux. Ce sont entre autre :

- faciliter la communication entre les différents acteurs de la vie de l'U.N.B. (enseignants, personnel atos, administrations, étudiants) en vue d'améliorer le rendement;
- réduire le coût de la communication;
- exploiter à bon escient les ressources de l'U.N.B.

D'autre part, il y a les objectifs opérationnels, qui s'identifient par :

- produire un document d'étude de l'opportunité, la faisabilité, la pertinence du service VoIP (Voice Over Internet Protocol) ou encore voix sur IP à l'U.N.B.;
- étendre (faire passer à l'échelle) le service VoIP à tous les sites et administration de l'université;
- optimiser la qualité de service de communication;
- sécuriser le service de communication VoIP ;
- veiller à la sûreté de la communication sur le site.

Parvenir à bout de ces objectifs nous permettra de palier les besoins en communication des acteurs l'Université Nazi BONI.

I.3.3 Acteurs du projet

Comme acteurs, nous avons en premier loge le comité de pilotage. C'est un groupe d'encadreurs chargés de veiller au bon fonctionnement du projet. Il a pour rôle de guider le groupe de travail, de valider les choix méthodologiques et les orientations générales, de définir les moyens à mettre en place pour la réalisation du projet, de coordonner les activités et de faire la validation finale du projet. Il est constitué de :

- Dr YELEMOU Tiguiane, Directeur de la DPNTIC ;
- M. BAYALA Béranger, administrateur réseaux de la DPNTIC.

Ensuite, vient le groupe de projet. Il est la cheville ouvrière du projet. Il est chargé de mener à bien les travaux dans les délais impartis, d'assurer la cohérence et la faisabilité des solutions proposées, de rendre compte au comité de pilotage et présenter les rapports. Le groupe de projet est essentiellement composé d'un étudiant en troisième année de cycle d'ingénieur de conception que nous sommes, KABRE Gu-wendkuuni Bonaventure.

Enfin, nous avons le groupe des utilisateurs. Ce sont les bénéficiaires directs du projet. On y rencontre le personnel de l'U.N.B., les enseignants missionnaires et les étudiants. Ils sont ceux-là qui ont exprimé les besoins qui ont fait l'objet de ce projet.

Pour mener à bien ce projet, le groupe de projet en accord avec le comité de pilotage a opté un planning prévisionnel de réalisation comme l'illustrent les diagrammes des Figures I.2 et I.4. la Figures I.3 et I.5 représentent le planning réel de réalisation. Ils ont été élaborés grâce au logiciel Gantt Project. Ils décrivent les durées (date de début et date de fin) des tâches, leur chronologie, ainsi que leurs dépendances mutuelles. Par exemple, la tâche « *mise en place* » ne peut

commencer que dix (10) jours après le début de la tâche « *dimensionnement* » selon le planning prévisionnel.

I.4 Conclusion

Suite aux difficultés rencontrées dans les communications téléphoniques sur les différents sites de l'Université, la DPNTIC a décidé d'approfondir la question de la Voix sur IP, surtout que l'infrastructure existante ne répond pas aux besoins de cette structure. C'est dans ce sens que le thème : « ***téléphonie sur IP à l'Université Nazi BONI : passage à échelle, QoS et mesures de sécurité*** » nous a été soumis. Ce chapitre nous a permis de comprendre les besoins réels de l'U.N.B. Dans la prochaine section, il sera question des généralités sur la VoIP

Figure I.2 : planning prévisionnel de réalisation

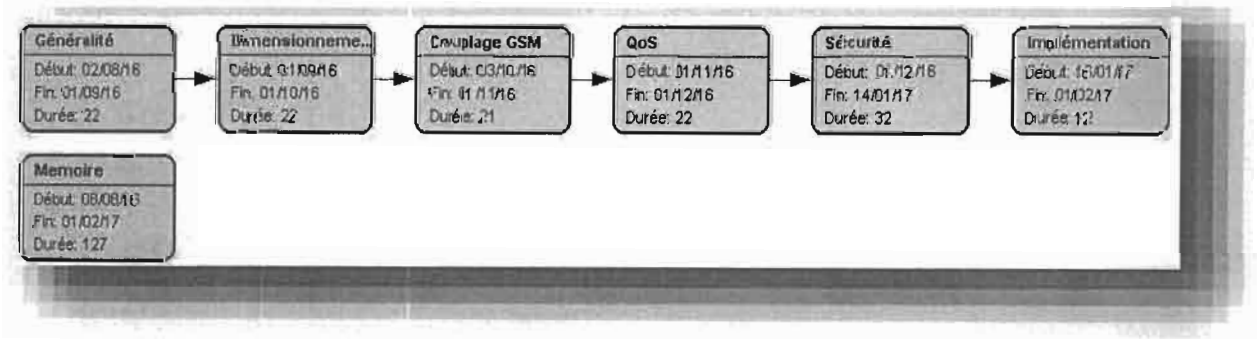

Figure I.3 : planning réel de réalisation

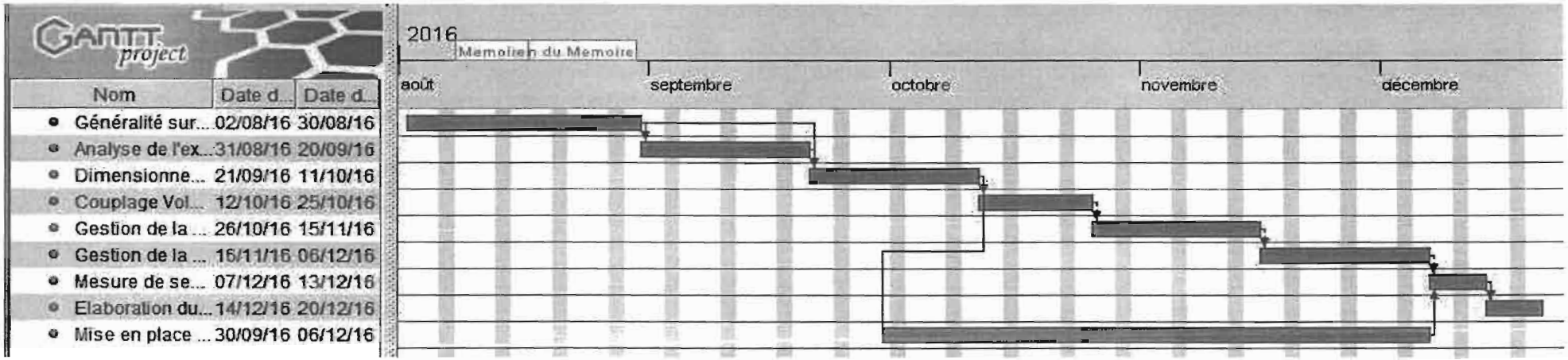

Figure I.4 : planning prévisionnel de réalisation

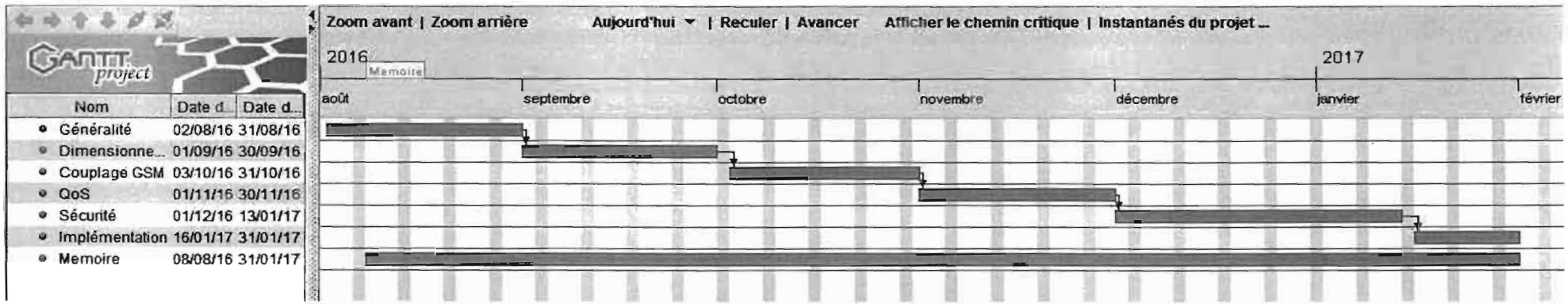

Figure I.3 : planning réel de réalisation

CHAPITRE II : GENERALITES SUR LA VOIP

II.1 Introduction

Ce chapitre a pour but de nous faire acquérir des connaissances théoriques sur la VoIP et par la même occasion, de nous familiariser avec le vocabulaire de la VoIP. Ainsi nous présenterons d'une part la VoIP, c'est-à-dire l'historique, la définition, l'architecture de base et le principe de fonctionnement ; et d'autre part, les protocoles utilisés. Enfin nous ferons cas de l'opportunité d'une telle technologie.

II.2 Présentation de la téléphonie sur IP

Cette section traite du volet théorique et technique de la technologie VoIP.

II.2.1 Historique

Du premier télégraphe de Chappe en 1790 au RTC actuelle, l'histoire des communications a connu de grands moments et de grandes avancées dûs à l'ingéniosité de certains et aux progrès technologique et électronique. Nous retiendrons quelques grandes dates telles que [1] :

- **1837 :** le premier télégraphe électrique inventé par Samuel Morse ;
- **1889 :** Almon B. Strowger (USA) invente le premier « sélecteur » automatique et donne ainsi naissance à la commutation téléphonique automatique ;
- **1938 :** Alec Reeves (Français) dépose le brevet des futurs systèmes à modulation par impulsion et codage (MIC) quantification et échantillonnage du signal à intervalles réguliers, puis codage sous forme binaire ;
- **1962 :** les premiers systèmes de transmission multiplex de type MIC permettant une liaison à 24 voies entre centraux téléphonique apparaissent aux Etats-Unis ; à la même époque en France on installe des MIC à 32 voies ;
- **1970** : un nouveau pas est franchi dans le domaine de la commutation électronique avec la mise en service en France, par le CNET, des premiers centraux téléphoniques publics en commutation électronique temporelle ;
- **1979 :** lancement du minitel en France ;

- **1987 :** le réseau numérique à intégration de services (RNIS) est mis en service en France ;
- **1990** : de nouveaux concepts apparaissent tels que la commutation temporelle asynchrone (ATM) et la hiérarchie numérique synchrone.

Durant les cinquante (50) dernières années, les entreprises ont utilisé des systèmes PBX traditionnels. Ces systèmes nécessitaient des réseaux de communication séparés pour les données et la voix. Cependant, la nouvelle révolution de la téléphonie sur IP appelée VoIP offre l'avantage de la convergence des réseaux de données et voix.

II.2.2 Définition

VoIP signifie Voice over Internet Protocol ou Voix sur IP. Comme son nom l'indique, la VoIP permet de transmettre des sons (en particulier la voix) dans des paquets IP circulant sur les réseaux internet. La VoIP peut être exploitée par des téléphones ou ordinateur grâce à des logiciel [1].

II.2.3 Architecture VoIP

Une infrastructure VoIP est composée d'équipements matériels et logiciels. Il n'existe pas de standard unique ; cependant il y a des références en la matière.

De façon générale la topologie d'un réseau de téléphonie IP comprend toujours des terminaux, un serveur de communication et une passerelle vers les autres réseaux. Chaque norme a ensuite ses propres caractéristiques pour garantir plus ou moins une bonne qualité de service. L'intelligence du réseau est aussi déportée soit sur les terminaux, soit sur les passerelles/Gatekeeper (contrôleur de commutation).

On retrouve les éléments communs suivants :

- **le routeur** : Il permet d'aiguiller les données et le routage des paquets entre deux réseaux. Certains routeurs, comme Cisco 2600, permettent de simuler un gatekeeper grâce à l'ajout de cartes spécialisées supportant les protocoles VoIP ;
- **la passerelle** : il s'agit d'une interface entre le réseau commuté et le réseau IP ;
- **le IPBX (Internet Private Branch eXchange)** : c'est le central de gestion des appels téléphoniques ;
- **les Terminaux** : Des PC ou des téléphones VoIP ou des smartphones [1][8].

Pour assurer le fonctionnement et la collaboration de ces différents équipements, des protocoles existent. Pour la suite, nous nous appesantirons sur les plus connus que sont H.323, SIP et

MGCP/MEGACO. Il existe donc plusieurs approches pour offrir des services de téléphonie et de visiophonie sur des réseaux IP. La Figure II.1 illustre une utilisation générale de la VoIP en entreprise [1]. Sur cette figure, IPBX est représenté par le contrôleur de communication.

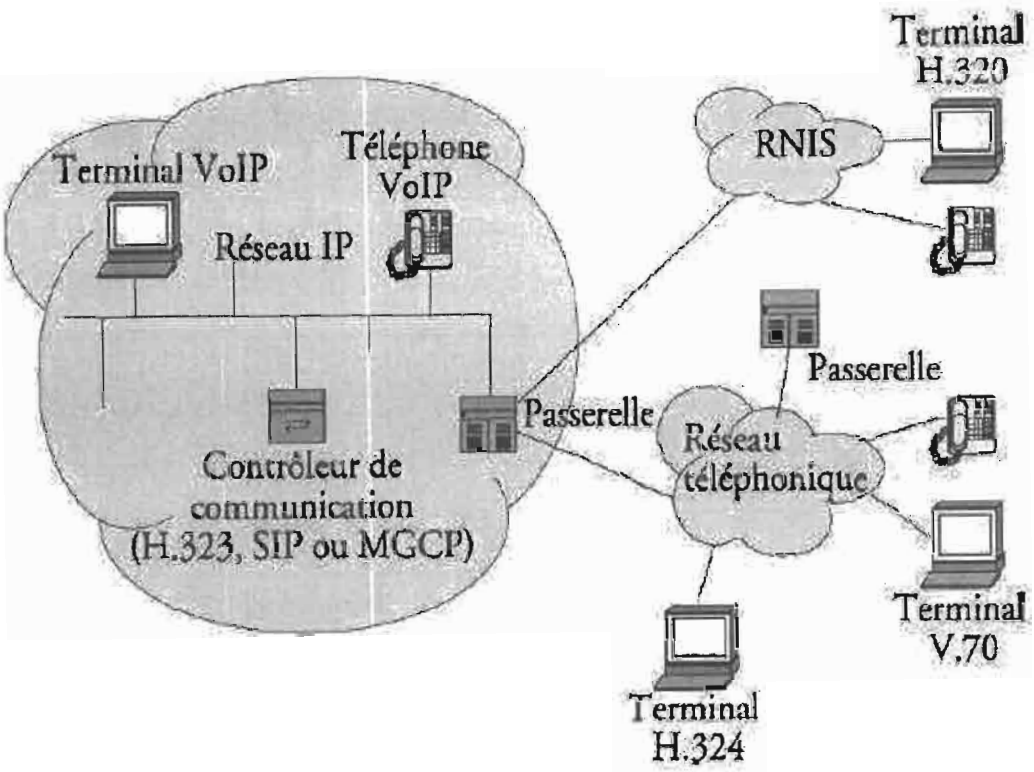

Figure II.1 : architecture de la VoIP en entreprise [1]

II.2.4 Principe de fonctionnement

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

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

Les passerelles ou gateways en téléphonie IP sont des ordinateurs qui fournissent une interface où se fait la convergence entre les réseaux téléphoniques commutés (RTC) et les réseaux basés sur la commutation de paquets TCP/IP. C'est une partie essentielle de l'architecture du réseau de téléphonie IP. Le gatekeeper est l'élément qui fournit de l'intelligence à la passerelle. Le gatekeeper est le compagnon logiciel de la gateway.

Une passerelle permet aux terminaux d'opérer en environnements hétérogènes. Ces environnements peuvent être très différents, utilisant diverses technologies telles que le Numéris, la téléphonie commutée ou la téléphonie IP. Les passerelles doivent aussi être compatibles avec les terminaux téléphoniques analogiques. La gateway fournit la possibilité d'établir une connexion entre un terminal analogique et un terminal multimédia (un PC en général).

Un gatekeeper quant à lui, a deux services principaux à savoir la gestion des permissions et la résolution d'adresses. Il est aussi responsable de la sécurité. Quand un client veut émettre un appel, il doit le faire à travers le gatekeeper. C'est alors que celui-ci fournit une résolution d'adresse du client de destination. Le gatekeeper répond aux aspects suivant de la téléphonie IP:

- **Le routage des appels** : en effet, le gatekeeper est responsable de la fonction de routage. Non seulement, il doit tester si l'appel est permis et faire la résolution d'adresse mais il doit aussi rediriger l'appel vers le bon client ou la bonne passerelle.
- **L'administration de la bande passante** : le gatekeeper alloue une certaine quantité de bande passante pour un appel et sélectionne les codecs à utiliser. Il agit en tant que régulateur de la bande passante pour prémunir le réseau contre les goulots d'étranglement (bottle-neck).
- **La tolérance aux fautes, sécurité** : le gatekeeper est aussi responsable de la sécurité dans un réseau de téléphonie IP. Il doit gérer les redondances des passerelles afin de faire aboutir tout appel. Il connaît à tout moment l'état de chaque passerelle et route les appels vers les passerelles accessibles et qui ont des ports libres.
- **La gestion des différentes gateways** : dans un réseau de téléphonie IP, il peut y avoir beaucoup de gateways. Le gatekeeper, de par ses fonctionnalités de routage et de sécurité, doit gérer ces gateways pour faire en sorte que tout appel atteigne sa destination avec la meilleure qualité de service possible.

Ainsi, le gatekeeper peut remplacer le classique PABX (Private Automatic Branch eXchange) et mieux encore, avec la possibilité d'implémenter autant de services qu'il désir.

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

II.3 Les protocoles utilisés

Nous distinguons les protocoles de signalisation des protocoles de transport.

II.3.1 les protocoles de signalisation

Les protocoles de signalisation ont la charge de régir les communications, de déterminer les appelés, de signaler les appelants, de gérer les absences, les sonneries etc... Ils peuvent aussi négocier le codec qui pourra être utilisé. Nous présenterons dans ce document, les protocoles les plus utilisés.

II. 3.1.1 H.323

II.3.1.1.1. Description

Le standard H.323 a été approuvé en 1996. Il assure les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Telecommunications Union). Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclue H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network).

II.3.1.1.2. Principe de fonctionnement

Une communication H.323 se déroule en cinq phases à savoir :

- l'établissement d'appel,
- l'échange de capacité et réservation éventuelle de la bande passante à travers le protocole RSVP (Ressource reservation Protocol),
- l'établissement de la communication audiovisuelle,
- l'invocation éventuelle de services en phase d'appel (par exemple, transfert d'appel, changement de bande passante, etc.),
- la libération de l'appel.

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

- **Les terminaux H.323 :** il peut s'agir d'un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet
- **Gateway ou les passerelles vers des réseaux classiques (RTC, RNIS, etc.) :** ils assurent l'interconnexion avec les autres réseaux
- **Gatekeeper ou les portiers :** c'est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H. Le Gatekeeper a pour fonction : la

translation des alias H.323 vers des adresses IP, le contrôle d'accès des utilisateurs, et la gestion de la bande passante.

- **Les MCU (Multipoint Control Unit) :** ils permettent aux utilisateurs de faire des visioconférences à trois terminaux et plus en «présence continue» ou en « activation à la voix ».

II.3.1.1.3. Avantages et inconvénients

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

- **la gestion de la bande passante**: H.323 permet une bonne gestion de la bande passante en posant des limites au flux audio/vidéo afin d'assurer le bon fonctionnement des applications critiques sur le LAN ;
- **la propriété de support multipoint**: il permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc.
- **la propriété support multicast**: il permet également de faire des transmissions en multicast ;
- **l'interopérabilité** : ce protocole permet aux utilisateurs de ne pas se préoccuper de la manière dont se font les communications ; les paramètres (les codecs, le débit…) sont négociés de manière transparente ;
- **la flexibilité** : une conférence H.323 peut inclure des terminaux hétérogènes (studio de visioconférence, PC, téléphones…) qui peuvent partager selon le cas, de la voix, de la vidéo et même des données.

Les inconvénients de la technologie H.323 sont :

- la complexité de mise en œuvre,
- les problèmes d'architecture en ce qui concerne la convergence des services de téléphonie et d'Internet,
- le manque de modularité et de souplesse,
- l'absence de moyen de sécurisation,
- la lente évolution du protocole depuis un certain temps.

II.3.1.2 SIP

II.3.1.2.1. Description

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF qui a été conçu pour établir, modifier et terminer des sessions multimédias. Il se charge

de l'authentification et de la localisation des multiples participants. Il se charge également de la négociation sur les types de média utilisables par les différents participants en encapsulant des messages SDP (Session Description Protocol)

II.3.1.2.2. Principe de fonctionnement

Les principales caractéristiques du protocole SIP sont :

- **Fixation d'un compte SIP :** c'est le fait d'associer un compte SIP à un serveur SIP (proxy SIP) dont l'adresse IP est fixe. Ce serveur lui allouera un compte et il permettra d'effectuer ou de recevoir des appels quelque soit son emplacement. Ce compte sera identifiable via son nom ou pseudo.
- **Changement des caractéristiques durant une session :** aux utilisateurs de modifier les caractéristiques d'un appel en cours. Par exemple, un appel initialement configuré en voix uniquement peut être modifié en voix plus vidéo.
- **Différents modes de communication :** ils permettent aux utilisateurs qui ouvrent une session de communiquer en mode point à point, en mode diffusif ou dans un mode combinant ceux-ci.
- **Gestion des participants :** de nouveaux participants peuvent joindre les participants d'une session déjà ouverte en participant directement. Il y'a aussi le transfert d'appels et la mise en attente
- **Négociation des médias supportés :** cela permet à un groupe durant un appel de négocier sur les types de médias supportés. Par exemple, la vidéo peut être ou ne pas être supportée lors d'une session.
- **Adressage :** les utilisateurs disposant d'un numéro (compte) SIP disposent d'une adresse ressemblant à une adresse mail (sip:numéro@serveursip.com)
- **Modèle d'échange :** le protocole SIP repose sur un modèle Requête/Réponse. Les échanges entre un terminal appelant et un terminal appelé se font par l'intermédiaire de requêtes. La RFC3261décrit les méthodes SIP consignées dans le Tableau II.1.

D'autres méthodes sont spécifiées dans plusieurs RFC associées à la RFC3261 comme l'illustre le Tableau II.2. Les requêtes SIP doivent recevoir une ou plusieurs réponses dont les codes sont spécifiés par la RFC3261 :

- **Codes d'erreurs :** il existe 6 classes de réponses, c'est-à-dire de codes d'état, représentées par le premier digit :
    - 1xx : la requête a été reçue et continue à être traitée (*Information*).

- 2xx : l'action a été reçue avec succès, comprise et acceptée (*Succès*).
- 3xx : une autre action doit être menée afin de valider la requête (*Redirection*).
- 4xx : la requête contient une syntaxe erronée ou ne peut pas être traitée par ce serveur (*Erreur du client*).
- 5xx : le serveur n'a pas réussi à traiter une requête apparemment correcte (*Erreur du serveur*).
- 6xx : la requête ne peut être traitée par aucun serveur (*Echec général*).

Tableau II.1 : requêtes RFC3261 entre terminal appelant et appelé

Méthode	Description
REGISTER	Méthode d'enregistrement permettant à un agent (UA-User Agent) de communiquer son adresse IP et l'URL où il peut être joint.
INVITE	Méthode utilisée pour établir des sessions de communication entre agents.
ACK	Méthode servant à accuser la réception d'autres requêtes ; par exemple la confirmation de la réception d'une requête de type *invite*
CANCEL	Annulation d'une requête en cours par un terminal ou un proxy.
BYE	Terminaison d'une session de communication entre agents.
OPTIONS	Requête permettant d'obtenir les informations relatives aux capacités d'un correspondant, sans pour autant établir d'appel.

II.3.1.2.3. Avantages et inconvénients

Le protocole SIP est ouvert, standard, simple et flexible. Voici en détails ces différents avantages :

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

- Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.

SIP est en train de devenir le protocole le plus apprécié parce qu'il est moins gourment en ressource, intègre des mesures de sécurité et est en perpétuelle évolution. Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau.

Tableau II.2 : autres requêtes RFC3261[12]

Méthode	Description
SUBSCRIBE	Requête d'abonnement aux évènements d'un autre agent identifié par son URI (RFC3265)
NOTIFY	Requête de notification d'un évènement consécutif à une requête d'abonnement (RFC3265)
REFER	Requête de redirection d'un appel vers un autre agent (RFC3515)
PRACK	Requête de sécurisation des réponses provisoires (RFC3262)
INFO	Requête d'information sur la session en cours (RFC2976)
MESSAGE	Requête d'envoi de messages instantanés (RFC3428)
UPDATE	Requête de modification d'une session en cours d'établissement (RFC3311)

II.3.1.3 autres protocoles de signalisation

II.3.1.3.1 IAX

Le protocole IAX2 est une alternative au protocole SIP. Il s'agit du protocole sur lequel s'appuie Asterisk (PBX open source) bien que celui-ci soit en mesure de supporter les autres principaux protocoles VoIP tel que SIP. IAX2 utilise un port UDP unique qui est le port 4569 (IAX1 utilisait le port 5036) et ceci marque l'une des grandes différences avec le protocole SIP. Il ne rencontre pas de problème de NAT d'où son principal succès. IAX2 est apparu longtemps après SIP, mais est en train de rattraper son retard.

De plus en plus d'opérateurs supportent le protocole IAX2 et de nombreux équipements commencent à faire leur apparition. Ce succès grandissant de IAX2 n'est cependant pas vraiment une menace pour SIP de la manière que SIP l'a été pour H323. Bien que de plus en plus supporté par les fabricants de matériels, IAX n'est pas standardisé et n'est pas très répandu.

II.3.1.3.2. MGCP

Le protocole MGCP (Media Gateway Control Protocol), ou protocole de contrôle des passerelles multimédias.

MGCP fonctionne selon une architecture centralisée permettant de faire communiquer et de contrôler différentes entités appartenant à des réseaux distincts [9]. Dans son modèle architectural, MGCP définit deux (02) importantes entités à savoir, le « *Call Agent* », qui sert à piloter et administrer les passerelles de manière centralisée et les « *passerelles* », qui maintiennent la connectivité entre réseaux de nature différente.

Le Call Agent

Le Call Agent, également appelé contrôleur de passerelles multimédias ou encore SoftSwitch, selon une terminologie non officielle mais courante, a pour fonction de contrôler les passerelles et de concentrer toute l'intelligence ainsi que la prise de décision dans le réseau. Entité logique, pouvant être localisée n'importe où dans le réseau, le Call Agent est spécifiquement responsable de l'établissement, de la maintenance et de la terminaison des appels établis entre des terminaux appartenant à des réseaux de natures différentes [9].

Il est possible d'avoir plusieurs Call Agents, chacun ayant en charge un parc de passerelles multimédias. Par exemple, chaque opérateur peut gérer ses propres passerelles par un Call Agent propriétaire.

Les passerelles multimédias

Selon le protocole MGCP, la notion de passerelle est assez floue et couvre un vaste ensemble de définitions, notamment les suivantes :

- Passerelle d'opérateur téléphonique, pour faire le lien entre un réseau téléphonique et un réseau IP.
- Passerelle résidentielle de type box (boîtier exploitant le modem, le câble ou les technologies xDSL), généralement mise à disposition par le FAI (Fournisseur d'Accès Internet). Ce boîtier fait la liaison entre le réseau IP des utilisateurs et le réseau d'accès téléphonique de l'opérateur.
- PBX d'entreprise faisant la liaison entre le réseau IP de l'entreprise et le réseau téléphonique RTC de l'opérateur.

Le protocole MGCP a pour rôle exclusif de transmettre de la signalisation entre le Call Agent et les passerelles. Les flux de données multimédias (voix, vidéo, données) entre deux

terminaux appartenant aux différents réseaux sont véhiculés de poste terminal à poste terminal, en passant uniquement par la passerelle. La passerelle multimédia a donc pour mission l'acheminement cohérent des données par la conversion du signal adaptation au support, la compression des données, la conversion de la signalisation, le multiplexage et la mise en paquets. La Figure II.2 illustre l'architecture MGCP ; les lettre X, Y ou Z représentant des réseaux quelconques (RNIS, ATM, IP, RTC, etc.) [9].

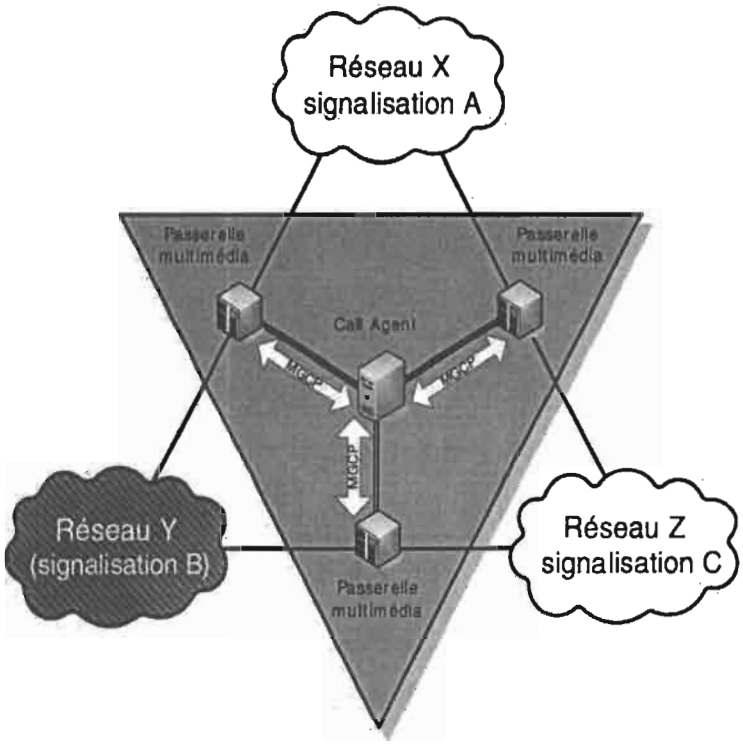

Figure II.2 : architecture MGCP [9]

Du fait de sa centralisation, cette architecture possède un point de vulnérabilité qu'est le serveur central. Néanmoins, le protocole a prévu, en cas de disfonctionnement de ce serveur, qu'une passerelle puisse basculer d'un contrôleur vers un autre.

Il convient de souligner que ce protocole est gourment en ressource en ce sens que l'établissement d'un appel nécessite plusieurs messages de signalisations. Les terminaux qui l'implémentent ne se connectent jamais directement entre eux, mais doivent impérativement au préalable en demander l'autorisation au centre de contrôle [9].

II.3.1.3.3 SCCP

Skinny Client Control Protocol (SCCP) est un protocole propriétaire de VoIP développé par CISCO. C'est un protocole plus léger que H323. Il permet en effet la signalisation et accord sur le type de transmission.

Comme bien d'autres protocoles de signalisations, SCCP utilise RTP/RTCP pour l'envoie de l'audio et la vidéo. Le fonctionnement du SCCP nécessite la mise en place d'un Call Manager ; il agit comme un proxy pour la signalisation appel lancé par d'autres protocoles tels que H.323, SIP, RNIS et / ou MGCP. Le CuCM (Cisco Unified Communication Manager) est un exemple de Call Manager. Il fonctionne comme un proxy/gateway et gère les protocoles comme SIP, H323, MGCP et SCCP.

SCCP est très simple comparativement aux autres protocoles. En plus il jouit d'une forte notoriété dû à son propriétaire. Cependant il demeure propriétaire, ce qui freine légèrement sa propagation.

Encore connus sous le nom de **protocoles de synchronisation**, ils sont utilisés systématiquement dans les applications multimédias interactives. Ces protocoles applicatifs sont chargés de transporter une information multimédia en temps réel au travers d'un réseau IP.

II.3.2 Les protocoles de transport

II.3.2.1 RTP

RTP (Real time Transport Protocol), comme son nom l'indique, est un protocole de transport temps réel de bout en bout des flots données audio et vidéo sur les réseaux IP. Il a été développé par l'IETF et standardisé en 1996 [1]. Il a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie en les numérotant. Ceci de façon à reformer le flux avec ses caractéristiques de départ. Il permet ainsi de :

- mettre en place un séquencement des paquets par une numérotation et ce afin de permettre ainsi la détection des paquets perdus. Cependant il est très important de savoir quel paquet a été perdu afin de pouvoir pallier à cette perte.
- identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux : c'est horodatage des paquets
- identifier la source (l'expéditeur du paquet). Ce qui est impératif dans le cas d'un multicast.
- Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation).

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

Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'y apporter une fiabilité. Ainsi il ne garantit pas le délai de livraison. Le protocole RTP utilise le protocole RTCP, Real-time Transport Control Protocol, qui transporte les informations supplémentaires suivantes pour la gestion de la session.

II.3.2.2. RTCP

RTCP est un protocole basé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. Le multiplexage des paquets de données RTP et des paquets de contrôle RTCP est assuré par le protocole UDP.

Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. Ces rapports comprennent le nombre de paquets perdus, la gigue (la variance d'une distribution et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS.

Ainsi, les paquets RTP ne transportent que les données des utilisateurs. Tandis que les paquets RTCP ne transportent que de la supervision. Il existe cinq (05) types de paquets de supervision:

- SR (Sender Report) : c'est le rapport de l'émetteur. Ce rapport regroupe des statistiques concernant la transmission comme le pourcentage de perte, le nombre cumulé de paquets perdus, la variation de délai encore appelée gigue.
- RR (Receiver Report) : c'est l'ensemble de statistiques portant sur la communication entre les participants. Ces rapports sont issus des récepteurs d'une session.
- SDES (Source Description) : c'est la carte de visite de la source, à savoir son nom, son e-mail et sa localisation.
- BYE : message de fin de participation à une session.
- APP : fonctions spécifiques à une application.

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

II.4 Autre facteur important : la fiabilité du service VoIP

Plusieurs facteurs sont importants à savoir, afin de mettre en place une solution VoIP plus ou moins sûr :

- **La fiabilité et la qualité sonore** : un des problèmes les plus importants de la téléphonie sur IP est la qualité de la retransmission. En effet, des désagréments tels la qualité de la reproduction de la voix du correspondant ainsi que le délai entre le moment où l'un des interlocuteurs parle et le moment où l'autre entend peuvent être extrêmement problématiques. De plus, il se peut que des morceaux de la conversation manquent (des paquets perdus pendant le transfert). Tout ceci peut être causé par la mauvaise qualité de la ligne ou bien le manque de ressource (bande passante) ou encore, incompatibilité de la VoIP et de l'infrastructure existante
- **Les communications blanches :** L'appelant compose un numéro de téléphone, et n'obtient pas la personne à l'autre bout du fil. Il y a juste un silence assourdissant. Il s'agit d'une communication blanche. Ce problème arrive quand on gère mal la file d'attente ou les situations d'engorgement. Celui-ci s'explique par le fait que la connexion soit établie, et les données non transportées.
- **Le décalage dans la conversation :** parfois, la communication est décalée. Concrètement, les sons parviennent à chaque utilisateur avec un temps de retard, ce qui rend la communication pénible et parfois incompréhensible. Cela est dû au délai de transit.
- **Les vols** : les attaquants qui parviennent à accéder à un serveur VoIP peuvent également accéder aux messages vocaux stockés et même au service téléphonique pour écouter des conversations ou effectuer des appels aux noms d'autres comptes. Ce phénomène résulte du manque de sécurisation conséquente de l'infrastructure VoIP.
- **Les attaques de virus** : si un serveur VoIP est infecté par un virus, les utilisateurs risquent de ne plus pouvoir accéder au service téléphonique. Le virus peut également infecter d'autres ordinateurs connectés au système.

II.5 Opportunité du service VoIP

La téléphonie sur IP exploite un réseau de données IP pour offrir des communications audio et vidéo au sein d'une structure. Cette convergence des services de communications sur un réseau unique, s'accompagne d'un certain nombre d'avantages. En effet, les coûts de l'infrastructure de réseau sont réduits, du fait que le déploiement s'effectue sur un unique réseau convergé voix et données sur tous les sites. Le téléphone et le PC (Personal Computer) partagent le même câble Ethernet, les frais de câblage sont réduits. L'ordinateur peut jouer aussi le rôle de téléphone, ce qui réduit le coût des équipements. Mieux encore, un ordinateur peut jouer le rôle de centre d'appel.

En plus, les frais d'administration du réseau sont également minimisés. Nul besoin d'administrateur de réseau de donnée et d'un administrateur de réseau téléphonique ; un seul peut bien assurer ces deux fonctions sans grandes difficultés. Pour des structures dont le nombre de site évolue, la VoIP constitue un énorme avantage.

Enfin, cette solution permet aux structures qui s'abonnent aux opérateurs de téléphonie de réduire leurs dépenses : C'est le cas de l'U.N.B.. Cette téléphonie se déploie aisément sur l'intranet des entreprises. Ainsi, les personnes autorisées peuvent se joindre dès lors qu'elles sont connectées au réseau de ladite structure. Dans le cas où certains utilisateurs voudront communiquer avec des personnes extérieures, la technologie prévoit dans son architecture, des passerelles vers d'autres réseaux.

II.5 Conclusion

La VoIP est une technologie qui consiste à faire transiter de la voix dans les canaux destinés aux données. Elle nécessite un certain nombre d'équipements matériels et de protocoles pour son fonctionnement. Cependant, pour une bonne qualité de service VoIP, il faut prioriser le service voix par rapport au données. Le dimensionnement au préalable n'est pas à négliger, car l'intégration du service voix impacte négativement sur l'infrastructure existante, tant coté ressource, que du volet sécurité.

CHAPITRE III : ETUDE DE L'EXISTANT ET DES BESOINS EN COMMUNICATION

III.1 Introduction

Dans ce chapitre, nous présentons le réseau informatique de l'U.N.B. Aussi, nous faisons cas de l'infrastructure de communication existante et ses limites. Nous y évaluons également les dépenses engendrées par la communication entre les différents acteurs de l'Université.

III.2 Infrastructure réseau de l'UPB

L'U.N.B. compte cinq (05) sites principaux à savoir celui de l'INSSA, de Nasso, du centre de calcul, de la cité universitaire de Belleville et le site du secteur 22. Cependant son réseau informatique est constitué de trois (03) entités car le site du secteur 22 et la cité n'en font pas partie. Les distances entre ces sites sont comprises entre un (01) et dix-sept (17) kilomètres.

III.2.1 Architecture et fonctionnement

Ces sites sont interconnectés par liaison radio (WiMAX). Cette liaison radio a une capacité avoisinant trente (30) Mbit/s. A cet effet, chaque site dispose d'une antenne émetteur/récepteur. La fibre optique et le câble FTP (File Transfert Protocol) sont utilisés pour interconnecter les différents bâtiments au sein d'un même site. Un seul routeur et des switchs Cisco assurent la communication sur ces différents sites. Les Figures III.1, III.2 et III.3 représentent respectivement les architectures réseau de Nasso, de l'INSSA et du centre de calcul.

Afin d'avoir un réseau évolutif et à même de répondre aux besoins de l'université, la DPNTIC prévoit l'augmentation de la capacité de son infrastructure réseau. Pour cela elle souhaite disposer d'une LS (Liaison Spécialisée) de 100 Mo de l'ONATEL. Pour un réseau plus performant, chaque site devra disposer d'un routeur. Cette architecture favorisera la modularité du réseau et donc, la gestion rapide et efficace des pannes et la disponibilité du réseau.

III.2.2 Services disponibles

Le réseau de l'université supporte déjà quelques services. Ils tournent sur des serveurs linux et sont utilisés dans la plupart du temps par des clients Windows. Ces services sont entre autre :

- La téléphonie sur IP ;
- La gestion de la bibliothèque ;
- La messagerie ;
- Le DNS ;
- La plateforme EAD
- Le web.

III.2.3 Politique de sécurité

Le réseau étant en développement il n'existe pas de politique de sécurité clairement définie. Cependant, certains services sont protégés par un pare-feu ASA. Celui-ci protège les services en local de l'insécurité due à Internet.

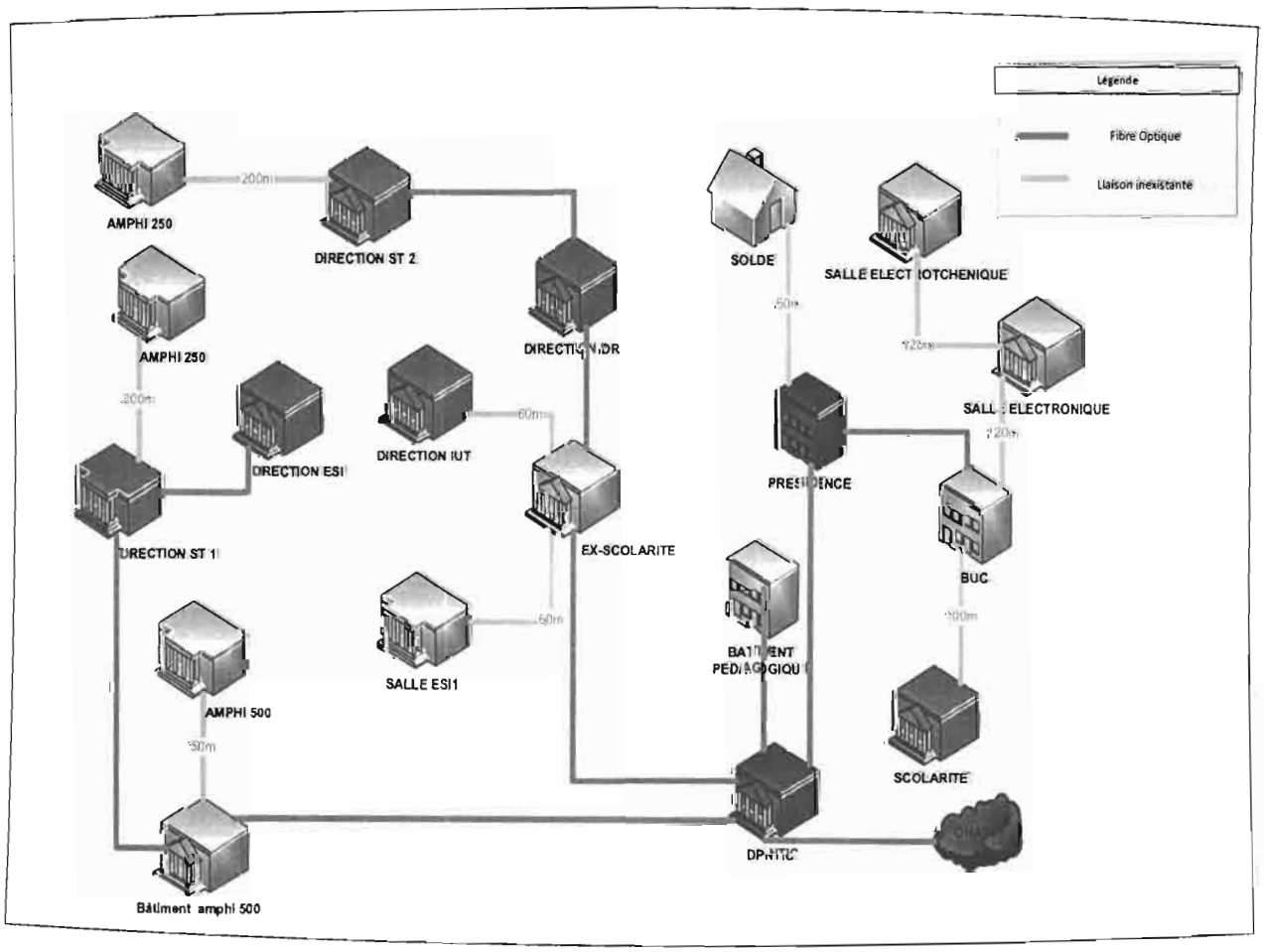

Figure III.1 Architecture réseau de Nasso

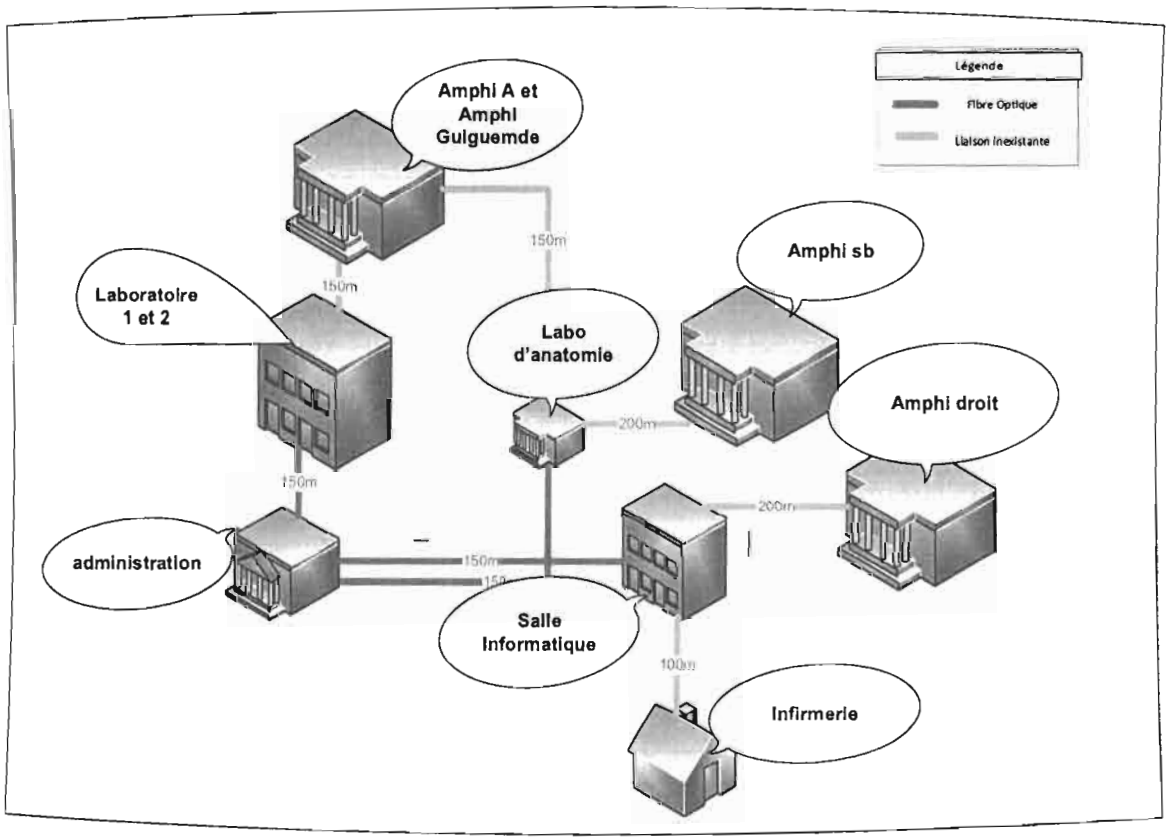

Figure III.2 Architecture réseau de l'INSSA

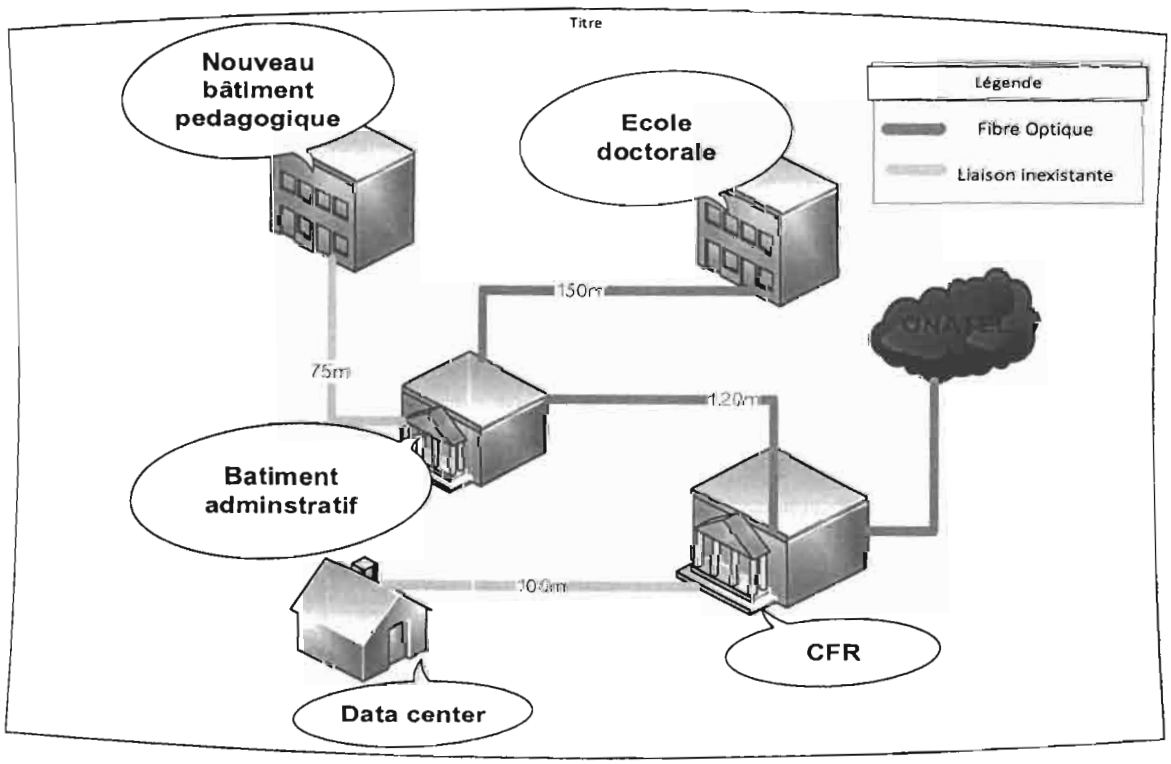

Figure III.3 Architecture réseau du centre de calcul

III.3 Architecture VoIP existant

La question de la VoIP à l'U.N.B. ne date pas de maintenant. En effet, en Février 2014, une solution VoIP avait été déjà mise en place. Ledit projet avait engendré une architecture prenant en compte quatre (04) U.F.R. en plus de la Présidence de l'U.N.B., de la bibliothèque centrale (BUC), du centre de formation et de recherche et de l'INSSA qui comporte chacune entre 2 à 20 utilisateurs.

Cette solution utilisait comme serveur VoIP Elastix qui, lui-même était autrefois basé sur Astérisk. Il était libre et totalement gratuit. Cependant, depuis sa version 4, notre serveur est désormais basé sur 3CX qui est un PBX Microsoft. Il quitte ainsi le monde du libre avec une version d'évaluation ne prenant en compte que quinzaine d'utilisateurs. Certaines de ses fonctionnalités se sont vues retranchées ou remplacées. Les anciens utilisateurs eux aussi se retrouvent difficilement si bien qu'il existe des certifications pour sa prise en main. Elastix, en plus de perdre ses fonctionnalités, a vu s'en aller une bonne partie de sa communauté ne jurant que pour le libre.

Les licences annuelles sont valables pendant douze (12) mois, puis doivent être renouvelées au même tarif. Le tarif est basé sur le nombre d'appels simultanés dont a besoin l'entreprise. En général on compte un appel simultané pour 3 à 4 extensions. Par exemple, une entreprise avec cinquante (50) extensions aura besoin d'une licence de seize (16) appels simultanés, comme le présente le Tableau III.1.

En plus, en matière de politique de sécurisation VoIP, notre infrastructure n'a prévu et mise en place que la restriction de l'accès au serveur par le module Netfilter : ce qui est une condition nécessaire mais non suffisante pour un niveau de sécurité acceptable. Aussi face aux besoins grandissants de l'U.N.B. et à l'interconnexion entre ses différents sites, cette solution n'a prévu qu'un nombre trop restreint d'utilisateurs. A cela s'ajoute l'absence de gestion de la QoS.

Toutes ces insuffisances ont conduit la DPNTIC à repenser à une solution prenant en compte tous les besoins actuels de l'U.N.B., et surtout facile à faire évoluer et dotée d'une politique de sécurité optimale. En somme elle voudrait un document de référence sur la mise en place et la gestion d'une infrastructure VoIP à grande échelle à l'U.N.B. ; d'où cette présente étude.

III.4 Impact social de la VoIP

La communication contribue tout d'abord à renforcer les liens sociaux entre les acteurs. Aussi communiquer permet de rompre la solitude et de chasser le stress. Le fait de se déplacer en longueur de journées pour transmettre certaines informations crée pas mal de frustration chez

le personnel, ce qui le rend désagréable et moins productif. La VoIP vient solutionner ce problème.

En plus cette technologique facilite l'organiser des travaux collaboratifs. Avec le système de visioconférence, les utilisateurs peuvent assurer leurs réunions à distance.

III.5 Besoin de communication

En matière de liaisons téléphoniques avec ONATEL, l'U.N.B. ne dispose que trois (03) postes, repartis sur les sites de Nasso, INSSA et le centre de calcul. Aussi, il n'y a que vingt-six (26) utilisateurs enregistrés sur le serveur VoIP. Outre ces canaux, le personnel est obligé d'utiliser ses propres moyens pour les besoins du service.

Selon les enquêtes menées dont les formulaires sont consignés dans les annexes 2 et 3 de ce document, un employé en moyenne investi par jour mille (1 000) franc CFA dans les appels téléphoniques dans le cadre de sa fonction. En prenant par exemple un total de trois cent (300) employés, nous avons un total de cent mille (300 000) franc CFA par jour pour le coût de la communication : ce qui est énorme.

En plus certains agents sont parfois obligés de se déplacer pour transmettre eux-mêmes des informations importantes. Cela a pour résultat, les abandons momentanés de postes, une dépense supplémentaire en énergie et surtout, une perte évitable de temps. Il y a alors un impact négatif sur la qualité des services prestés.

Du côté des étudiants il n'existe pas de plateforme mise en place par l'Université Nazi BONI, leur permettant de communiquer (appels, discussion instantanée, etc.). Ils se résolvent à créer des groupes sur les réseaux sociaux comme Facebook, Watsap, Viber, etc. Dans ce cas de scénario, il leur faut la connexion à Internet, ce qui n'est pas chose évidente pour eux tous, vu la cherté de l'abonnement.

En ce qui concerne les appels téléphoniques, un étudiant dépense en moyenne trois cent cinquante-six (356) francs CFA par jour pour joindre ses camarades et les enseignants. Ainsi, dix mille (10 000) étudiants dépensent en moyenne trois millions cinq-cents soixante mille (3 560 000) francs CFA par jour, dans les communications téléphoniques.

Tout cela nous amène à dire que l'Université gagnerait plus à investir dans les nouveaux moyens de communication comme la VoIP. Une telle solution permettra aux différents acteurs d'une part d'économiser en temps, en énergie et en argent ; et d'autre part, de renforcer leurs liens sociaux.

Cependant cette technologie ce doit d'être utilisée à bon escient. En effet la gratuité peut inspirer une utilisation abusive.

III.6 Conclusion

Le réseau informatique de l'Université est formé de trois (03) entités en raison de sa répartition géographique. La solution VoIP existante est loin de répondre aux besoins actuels de l'Université. L'architecture laisse comprendre que l'accent a été mis sur le « déploiement du service VoIP » que le dimensionnement ; la question de la sécurité n'a pratiquement pas été abordée. Du point de vue socio-professionnel, la VoIP est une solution opportune, mais doit être exploitée à bon escient. Dans le prochain chapitre nous ferons le dimensionnement et les grands choix technologiques qui s'imposent.

Tableau III.1 : les prix des licences Elastix [2].

	EUR			USD			GBP		
Version du produit	**Standard**	**Pro**	**Enterprise**	**Standard**	**Pro**	**Enterprise**	**Standard**	**Pro**	**Enterprise**
4 appels simultanés	149	189	298	149	189	298	129	169	258
8 appels simultanés	349	439	698	349	439	698	299	389	598
16 appels simultanés	699	879	1,398	699	879	1,398	625	779	1,250
32 appels simultanés	1,299	1,629	2,598	1,299	1,629	2,598	1,159	1,449	2,318
64 appels simultanés	2,499	3,129	4,998	2,499	3,129	4,998	2,229	2,789	4,458
128 appels simultanés	4,499	5,629	8,998	4,499	5,629	8,998	3,999	4,999	7,998
256 appels simultanés	7,499	9,379	14,998	7,499	9,379	14,998	6,679	8,349	13,358
512 appels simultanés	12,499	15,629	24,998	12,499	15,629	24,998	11,129	13,899	22,258
1024 appels simultanés	19,999	24,999	39,998	19,999	24,999	39,998	17,799	22,249	35,598

CHAPITRE IV : DIMENSIONNEMENT DU RESEAU VOIP

IV.1 introduction

Le réseau local existant est amené à supporter de nouveaux flux. Ces derniers ont des exigences strictes en latence et en stabilité du réseau. Dans ce chapitre, nous étudions la faisabilité de ce changement et nous évaluons les mises à niveau nécessaires en termes matériels et logiciels afin de garantir une QoS acceptable pour les utilisateurs des différents services de réseau.

IV.2 Solution logicielle

L'opérationnalisation d'une solution VoIP nécessite l'exploitation de plusieurs logiciels. Cependant, nous nous attarderons sur les serveurs PBX car c'est le « cerveau » de l'infrastructure et les téléphones IP. En effet ce sont eux qui permettront aux utilisateurs de communiquer. Plusieurs critères ont servi de base pour le choix de ces solutions.

D'abord, nous avons axé notre étude comparative sur les solutions les plus utilisées et les mieux appréciées, car généralement performantes. En effet, les applications les plus utilisées jouissent toutes autant d'une abondante communauté. Cela nous permet de bénéficier d'un soutien non négligeable dans les débogages et de partager aussi notre expérience à ceux qui en ont besoin. Nous ne saurons ignorer la forte documentation qui constitue un atout majeur dans l'avancement de nos travaux.

En plus, l'U.N.B. a des ressources financières limitées pour l'atteinte de ses objectifs, à savoir, donner une formation de qualité et dans les meilleurs conditions et délais. La DPNTIC ne reste pas indifférente à ce cri de détresse. Ainsi, cette étude a pour but d'améliorer les communications téléphoniques sur les différents sites de l'U.N.B. et à moindre coût ; d'où notre penchant pour les solutions moins onéreuses voire gratuites.

Aussi, la solution devra être capable de supporter la charge de l'université. En d'autres termes, elle doit pouvoir prendre en compte quinze-mille (15 000) utilisateurs et traiter correctement

mille-six-cents (1 600) appels simultanés. Le nombre d'appels simultanés a été calculé grâce à partir du temps moyen de communications issu des enquêtes dont les formulaires sont dans les annexes 2 et 3 de ce document.

Enfin, la DPNTIC est promotrice des solutions libres en raison de leur prise en main intégrale et facile, leur souplesse, leur évolution permanente en fonctionnalités et robustesse, leur transparence dans le fonctionnement et leur sécurisation effective. Ces logiciels libres sont pour la plupart gratuits. En somme, ils sont adaptés à notre contexte.

IV.2.1 Serveur IPBX

Selon le Wikipédia, dans l'industrie des télécommunications, on désigne par PABX IP (PBX IP ou encore IPBX), un autocommutateur téléphonique privé utilisant le protocole internet (IP) pour gérer les appels téléphoniques d'une entreprise, en interne sur son réseau local LAN (Local Area Network). Couplé à des technologies de voix sur IP, les communications téléphoniques pourront être acheminées sur le réseau étendu WAN (World Area Network) de l'entreprise.

Le logiciel libre a fait une incursion remarquée dans le monde de la téléphonie, par le biais de solutions PC-PBX (un ordinateur de type PC muni de cartes d'interface spécifiques) tournant sous Linux (ou un autre système libre) et équipées de logiciels Open Source comme Asterisk, Yate, VOCAL, etc. Chacune de ces plateformes possède des forces et évidemment des faiblesses.

Le Tableau IV.1 donne le résultat d'une étude comparative des plateformes les plus utilisées. Cette étude est basée sur les systèmes d'exploitation, les flux et les protocoles que supporte la plateforme. Cependant, une analyse plus poussée nous a conduit au choix d'Astérix comme serveur IPBX.

Tableau IV.1 : comparaison des IPBX les plus utilisés

Logiciel	Système d'exploitation	Flux	Protocole
FreeSWITCH	Unix, Windows, Sun Solaris, Mac OS X	audio, vidéo, chat	SIP, SIMPLE, XMPP, GoogleTalk (Jingle)), H.323, IAX, MRCP, Skype
Asterisk	Linux, Mac OS X	audio, vidéo, chat	SIP, H.323, IAX
SFLPhone	Linux	audio	SIP, IAX
Ekiga (anciennement GnomeMeeting)	Linux, Windows	audio, vidéo, chat	SIP, H.323
Jabbin	Linux, Windows	audio, chat	Jabber
KPhone	Linux	audio, vidéo, chat	SIP
Linphone	Linux, Windows, Mac OS X	audio, vidéo, chat	SIP
Jitsi	Linux, Windows, Mac OS X (Java)	audio, vidéo, chat	SIP, Jabber
Mumble	Linux, Windows	audio	
Twinkle	Linux	audio	SIP, IAX
QuteCom	Linux, Windows, Mac OS X	audio, vidéo, chat	SIP, Jabber
YATE	Linux, Windows	audio, vidéo, chat	SIP, Jingle, IAX, H.323
SIPInside	Windows	audio	SIP

IV.2.1.1 Présentation d'Astérix

Asterisk est une plateforme de téléphonie Open Source initialement conçue pour fonctionner sous Linux. Il rassemble plus de 100 ans de connaissance sur la téléphonie dans une robuste suite d'applications de télécommunications fortement intégrées.

C'est probablement l'un des outils les plus puissants, les plus flexibles et les plus extensibles fournissant tous les services de télécommunications. Asterisk est conçu pour s'interfacer avec n'importe quel dispositif logiciel ou matériel de télécommunication de manière cohérente et progressive. Il crée un environnement unique qui peut être façonné pour s'adapter à n'importe cas d'utilisation notamment en tant que:

- Gateway VOIP hétérogène supportant les protocoles MGCP, SIP, IAX, H.323, etc.
- Private Branch eXchange (PBX)
- Serveur vocal interactif (SVI)
- Serveur de téléconférence

- Translation de numéro
- Serveur de messagerie vocale
- Serveur de musique en attente
- Etc.

Asterisk peut fonctionner avec des cartes Zaptel ou des cartes non Zaptel de certains constructeurs. Ces cartes servent à sa connexion aux lignes téléphoniques classiques comme RTC. Il peut aussi fonctionner sans carte pour des communications uniquement basées sur les protocoles MGCP, SIP, IAX, H.323, etc.

Asterisk offre les avantages suivants:

- *Extensibilité*: grâce à l'interface AGI (Asterisk Gateway Interface), le programmeur peut ajouter des fonctionnalités à Asterisk avec différents langages de programmation comme Perl, PHP, C, Pascal.
- *Abondante documentation*: il existe plusieurs livres et sites dédiés à Asterisk et des mailing listes qui permettent aux utilisateurs de disposer des informations utiles sur le produit et trouver la solution aux problèmes qu'ils rencontrent.
- *Scalabilté*: il n'y a pas de taille minimale ou maximale pour un système Asterisk. On peut commencer avec un système de taille réduite et l'étendre au fur et à mesure que les besoins augmentent. Pour les grandes installations on peut déployer les fonctionnalités sur plusieurs serveurs.
- *Richesse des services offerts*: Asterisk offre la quasi-totalité des services de téléphonie et il est très rare de trouver aujourd'hui un produit Open source ou propriétaires disposant d'autant de fonctionnalités.

Cependant, il présente quelques inconvénients. Asterisk est un système très complexe et sa configuration n'est pas aisée à cause du nombre important de fichiers de configuration. De plus son administration à l'aide d'une interface graphique peut gêner son fonctionnement car celle tournant sous Xwindows crée beaucoup d'interruptions. [11]

Asterisk a connu ces dernières années, un développement remarquable. Jadis connu uniquement en sa version *Asterisk Now*, qui est un système basique, il existe maintenant sous forme de distributions officielles. Ces distributions sont considérées comme des versions plus complètes, du fait qu'ils incluent directement les paquets nécessaires pour une gestion plus efficace d'une

centrale téléphonique. Les distributions les plus célèbres jusqu'en fin 2016 étaient Xivo et Elastix.

Autrefois exclusivement sur Cent Os, la plateforme Elastix a fait des progrès remarquables en sa version 5. En effet, celle-ci tourne sur Debian 8.0.6 et intègre de nouvelles fonctionnalités manquantes dans ses versions antérieures. Elle est compatible avec la plupart des matériels VoIP. Cependant, il existe plusieurs types de licences en fonction du nombre d'appels simultanés. La licence gratuite n'en autorise que huit (08). A cela s'ajoute le fait qu'Elastix 5 soit basé sur 3CX (solution Microsoft) que sur Astérix. Elastix quitte ainsi le monde du libre, ce qui a entrainé la perte d'une grande partie de sa communauté.

Le PBX Xivo était fonctionnellement plus riche que ses concurrents. Il est basé sur Debian et intègre tous les protocoles de signalisations. En plus il est compatible avec les matériels de nombreux constructeurs, et jouie d'une forte communauté. Le nombre d'appels simultanés n'est pas limité. Cependant, la distribution a rencontré un problème suite à une mésentente entre son créateur et l'entreprise pour laquelle il travaillait. A l'issue de cet incident, ce dernier a décidé de changer de stratégie et crée ainsi un nouveau produit en Janvier 2017 appelé Wazo, qui est un fork de XiVO. Ce produit, en plus d'intégrer toutes les fonctionnalités et prometteur de son prédécesseur, ajoute d'autres paramètres de sécurité et une mise à niveau facile de l'ancienne version vers la nouvelle. Avec autant d'atout, il se révèle pour nous être le meilleur choix

IV.2.1.2 Présentation de Wazo

Wazo est une solution de communication unifiée IP libre sous licence GPLV3 pour les entreprises basée sur le logiciel Asterisk, donc hérite de ses avantages. Elle est interopérable avec la plupart des systèmes de téléphonie du marché et elle permet à tous les utilisateurs de bénéficier d'un ensemble de services évolués comme :

- un serveur d'auto configuration de terminaux téléphoniques de constructeurs différents,
- un système complet de routage d'appels adapté aux besoins des centres d'appels,
- un service d'unification des communications permettant la réception des messages vocaux et des fax dans sa messagerie électronique,
- le service de pont conférence multi-utilisateurs permettant à tout abonné de disposer de ce service, de le superviser et d'administrer les personnes invitées à sa conférence.

Ce PBX est un ensemble complet de fonctionnalités de téléphonie administrative répondant aux besoins des entreprises et collectivités. Ci-après la liste non exhaustive des fonctionnalités offertes : Gestion des utilisateurs, gestion des groupes, transfert d'appel, renvoi d'appel, messagerie vocale, import de fichiers sons, ne pas déranger, filtrage d'appel, interception d'appel, chuchotement, parcage d'appel, mise en attente, annuaire, pré-décroché, droit d'appel, historique des appels, répertoire, etc.

Il dispose également de fonctions de centre d'appels permettant de gérer des scénarios de distribution téléphonique évolués comme :

- la gestion de services vocaux évolués (SVI),
- la gestion de calendriers horaires d'ouverture et fermeture,
- la gestion de files d'attentes et de dissuasion,
- la gestion de priorités,
- le routage des appels sur compétence,
- un accès aux données métiers pour enrichir le contexte de l'appel,
- la gestion des agents et groupes d'agents « login/logout/retrait »,
- les files d'attente,
- l'enregistrement des communications,
- la supervision temps réel de l'activité du centre d'appels est intégrée à l'interface,
- XiVO Client (voir exemple ci-dessous).

Wazo bénéficie d'un serveur de provisioning permettant de déployer automatiquement un ensemble de téléphones SIP supportés. Il supporte une quarantaine de terminaux téléphoniques issus de différents constructeurs. Lors du déploiement des terminaux, le firmware du téléphone et la configuration propre à chaque utilisateur sont téléchargés automatiquement depuis le serveur au premier démarrage du poste sur le réseau. L'installation de Wazo est présenté dans l'annexe.

IV.2.2 Protocole de signalisation, Codec et Soft-phone

Nous avons choisi le protocole SIP pour l'établissement et la terminaison des communications. En plus des avantages évoqués dans la section II.2.1.2, ce protocole offre la possibilité de sécuriser les communications en utilisant du SSL.

Afin de gagner en bande passante, nous avons opté pour l'utilisation du G.729 comme compresseur/décompresseur. En effet il permet une compression de 8kbit/s par communication

avec une assez bonne qualité de la voix (4/5). Partant de là, on peut avoir théoriquement 1000 communications simultanées avec un débit de 8Mbit/s.

Un soft-phone est un logiciel permettant de simuler un téléphone IP sur un ordinateur. Plusieurs sont les soft-phones compatibles avec notre serveur PBX. Cependant, nous préconisons l'utilisation de XiVO-client, qui est une solution multiplateforme (Windows, Linux, MacOs, Android, etc.) et qui est implémenté par les développeurs de Wazo.

IV.3 Infrastructures physique

L'U.N.B. compte environ quinze-mile (15 000) étudiants et trois-cent (300) employés. Le choix du matériel doit se faire en conséquence.

IV.3.1 Machine serveur

En termes de caractéristiques souhaitées pour un serveur, la plus importante est la mémoire RAM. Les études ont montré que l'initiation d'une session nécessite 240 kilo octets (Ko) de mémoire. Donc le nombre maximal de session est égal à la mémoire RAM disponible (en Ko) divisée par 240. Ainsi, pour mille-six-cent (1 600) sessions simultanées consomment trois-cent-quatre-vingt-et-quatre (384) Mo de RAM. Cependant, il faut noter que ce calcul ne prend pas en compte les services nécessaires au fonctionnement du système d'exploitation.

IV.3.2 Routeurs

La puissance de calcul des routeurs et pare-feu est un élément à prendre en compte afin d'éviter les situations d'engorgement. Pour ce présent projet, il est nécessaire d'avoir des routeurs capables de gérer au moins mille-six-cent (1 600) sessions simultanées. Pourtant, les routeurs Cisco 2901 et le Firewall ASA 5512 VO4 dont est équipé le réseau de l'UPB supportent chacun, au moins dix mille (10 000) sessions simultanées. Cette performance satisfait largement les besoins pour la mise en place de la solution.

IV.3.3 Les Switchs et IP Phones

Les exigences s'étendent jusqu'aux switchs. La VoIP nécessite des swichts de type Fast Ethernet, c'est-à-dire ayant un débit avoisinant les centaines de MBps. Mais cela est un acquis car les switchs dont dispose l'Université sont du Gigabit Ethernet.

Notre serveur IPBX étant compatible avec la plupart des IP Phone nous ne posons pas trop de restriction concernant leur choix. L'U.N.B. dispose déjà d'une centaine d'IP Phones.

IV.4 La bande passante disponible

Dans la planification de capacité, le calcul de la bande passante est un facteur important à considérer pour une bonne qualité vocale. En VoIP, la gestion de la bande passante est

étroitement liée au choix et paramétrage du codec. Le codec G729 a retenu notre attention, car il a un faible débit (8 Kbit/s) avec une assez bonne qualité vocale (MOS = 3.92). Le calcul de la bande passante consommée par communication nous permettra de confirmer notre choix.

La bande passante requise pour une communication G729 (8 Kbit/s débit du Codec) avec RTP, PPP Multilink et une taille de charge utile de 20 Octets par défaut est de:

- Taille totale paquet (octets) = (En-tête Multilink PPP (6 Octets)) + (En-tête IP/UDP/ RTP compressé (2 Octets)) + (Charge utile voix (20 Octets)) = 28 Octets
- Taille totale paquets en bits = 28 x 8 = 224 bits
- PPS = (Débit du Codec 8Kbit/s) / (160 bits) = 50 paquets par seconde
- Bande passante par communication =
  (Taille du paquet Voix 224 bits) x 50 PPS = 11,2 Kbit/s

Afin de laisser une marge dans nos prévisions, nous prendrons 12 Kbit/s comme bande passante consommée par communication. Ainsi, avec 6 Mbits de bande passante, l'on peut garantir cinq cent (500) communications simultanées. Pendant les heures critiques (1 600 communications simultanées), la bande passante nécessaire s'élève à 19.2 Mbits. Ce qui ne posera pas de problème, car les différents sites sont interconnectés avec du WiMax.

IV.5 Problématique de la haute disponibilité

Le but de ce travail, comme jadis posé, est de permettre à ce que les acteurs de l'U.N.B. profitent de la bonne information au bon moment. En d'autres termes cette étude doit permettre d'éradiquer les problèmes rencontrés dans le système de communication précédent, à priori l'indisponibilité du réseau et de réduire les coûts en communication. Donc notre système se doit d'être opérationnel à temps plein.

Afin d'atteindre cet objectif, nous avons conclu après analyse, l'utilisation de deux (02) serveur BPX, quand bien même qu'un seul suffisait pour gérer parfaitement toute les communications. Cette architecture présentée dans la Figure IV.1 permettra de résoudre le problème de la haute disponibilité. Les deux serveurs seront configurés de sorte à ce que l'un prenne en charge toutes les communications si l'autre est en panne. Dans le cas contraire une répartition de charge se fait entre les serveurs afin de réduire le risque de panne.

En plus pour une bonne stabilité du réseau, chaque site doit avoir un routeur. Ces cinq (05) routeurs formeront la couche distribution. Deux autres routeurs seront reliés chacun aux cinq. Ces deux constitueront la couche distribution et aurons un accès à Internet. La Figure IV.2

illustre bien la topologie de cette architecture. Par ailleurs, nous préconisons la limitation du nombre de communications simultanées, afin d'éviter les situations d'engorgement.

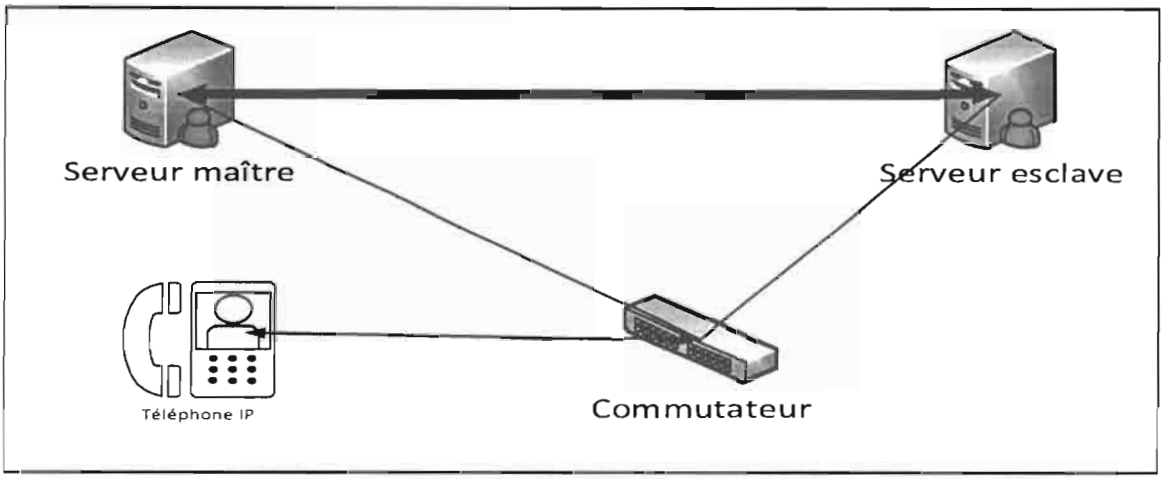

Figure IV.1 : représentation du serveur maître et du serveur esclave

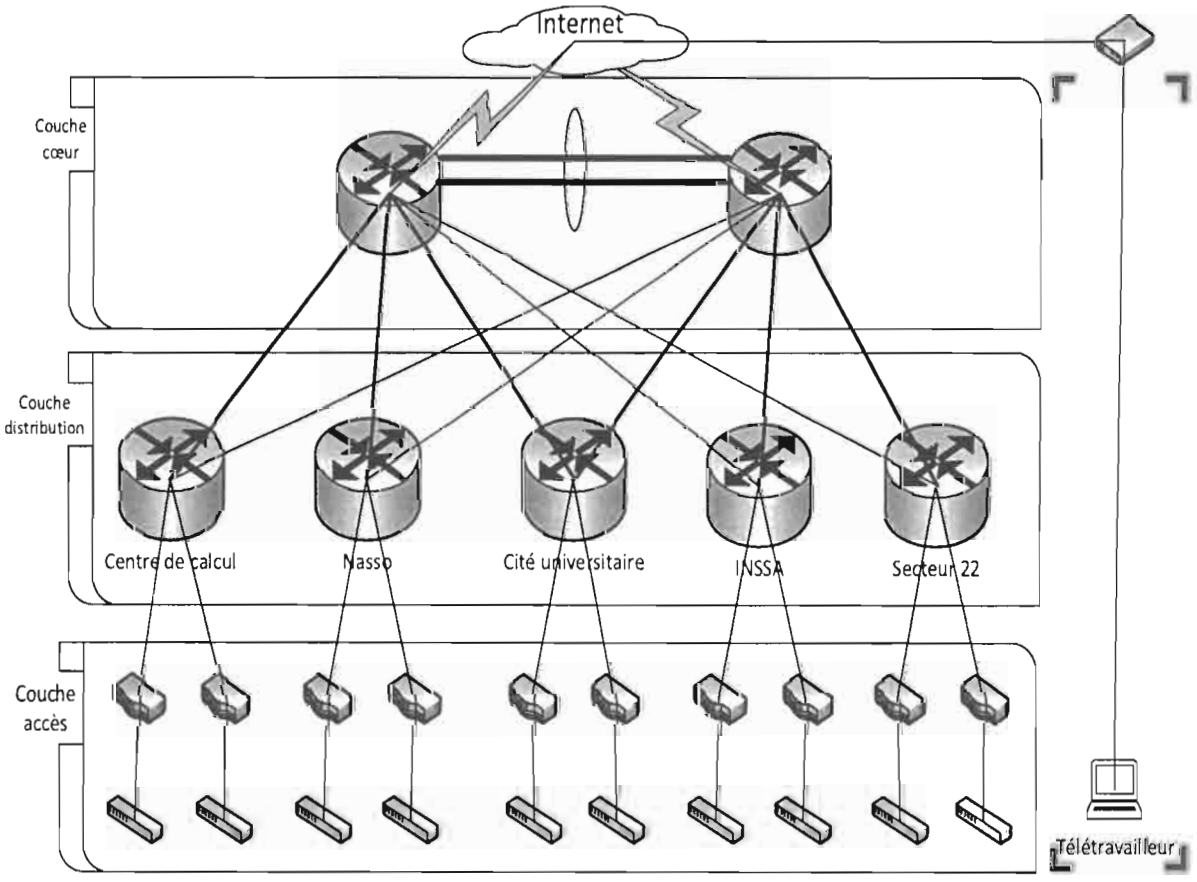

Figure IV.2 : proposition d'architecture logique de la couche cœur du réseau de l'U.N.B.

IV.6 Couplage VoIP-GSM

Le couplage est un pont que l'on crée entre le réseau de l'opérateur et le réseau VoIP.

IV.6.1 Pourquoi faire le couplage

Le couplage consiste à permettre à des utilisateurs de passer des appels vers l'extérieur du réseau de l'U.N.B., c'est-à-dire, sur le GSM. Cela, afin d'éviter le personnel d'utiliser ses moyens personnels pour les besoins du service. En effet pour certaines tâches, il est indispensable de contacter des personnes extérieures.

Tous les utilisateurs ne sont pas sont pas autorisé à passer sur la passerelle VoIP-GSM. Seuls quelques responsables sont autorisés à communiquer avec l'extérieur dans le cadre de leurs fonctions. Cette liste doit être communiquée par la DRH et est susceptible de modification.

IV.6.2 Choix de la passerelle

Plusieurs passerelles sont compatibles avec notre serveur IPBX. Cependant PORTech et VoiceBlue ont retenu notre attention tant par leurs performances que par leur efficacité. Dans le fond, ces derniers possèdent des fonctionnalités presque similaires.

Après analyse, notre choix s'est porté sur 2N® VoiceBlue Next. Elle fait partie de la nouvelle génération des passerelles VoIP et possède de nombreux atouts à savoir :

- le portail GSM jusqu'à quatre (4) canaux,
- le client SIP standard,
- Smart Voice Routing - Least Cost Routing (LCR) (routage des appels en fonction des coûts les plus bas),
- le routage intelligent des appels entrants,
- la qualité de pointe du transfert du signal vocal (EFR super sound)

En plus, c'est un dispositif de routage à moindre coût, très efficace, basé sur un routage en fonction de l'heure, de l'indicatif ou des minutes disponibles, ce qui est une solution à la problématique « qui autoriser à utiliser la passerelle et quand ? »

Enfin, par rapport aux produits concurrents, 2N® VoiceBlue apporte un avantage unique que sont les fonctions 2N® Mobility Extension et CallBack grâce auxquelles, l'on peut utiliser les fonctions avancées SMS en cas d'appel en absence, etc. Cependant, cette solution n'est pas gratuite. La Figure IV.3 illustre l'architecture de base de déploiement de 2N® VoiceBlue. [22].

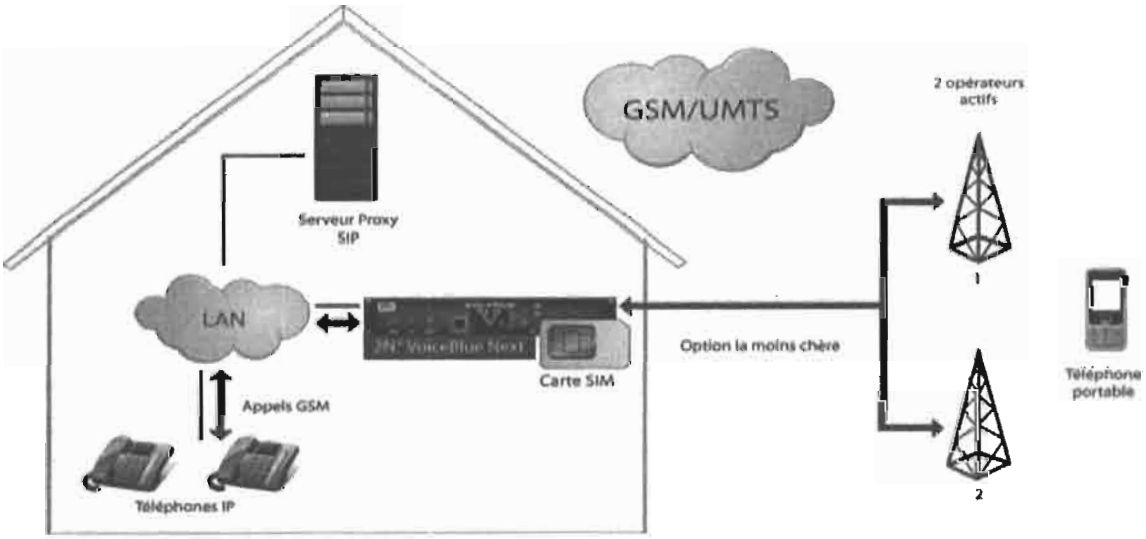

Figure IV.3 : architecture de déploiement de 2N® VoiceBlue

IV.7 Mise en œuvre

La mise en œuvre prévoit trois (03) scénarii d'utilisation. En local le système peut être exploité via le wifi avec les smartphones et des ordinateurs équipé de soft phones. L'on peut utiliser aussi les IP Phone et les ordinateurs de bureau via le les câbles réseau. Le système offre la possibilité de passer des appels hors du réseau local de l'université. Cela se fait en passant par la passerelle VoiceBlue. La Figure IV.4 illustre architecture de déploiement de cette solution.

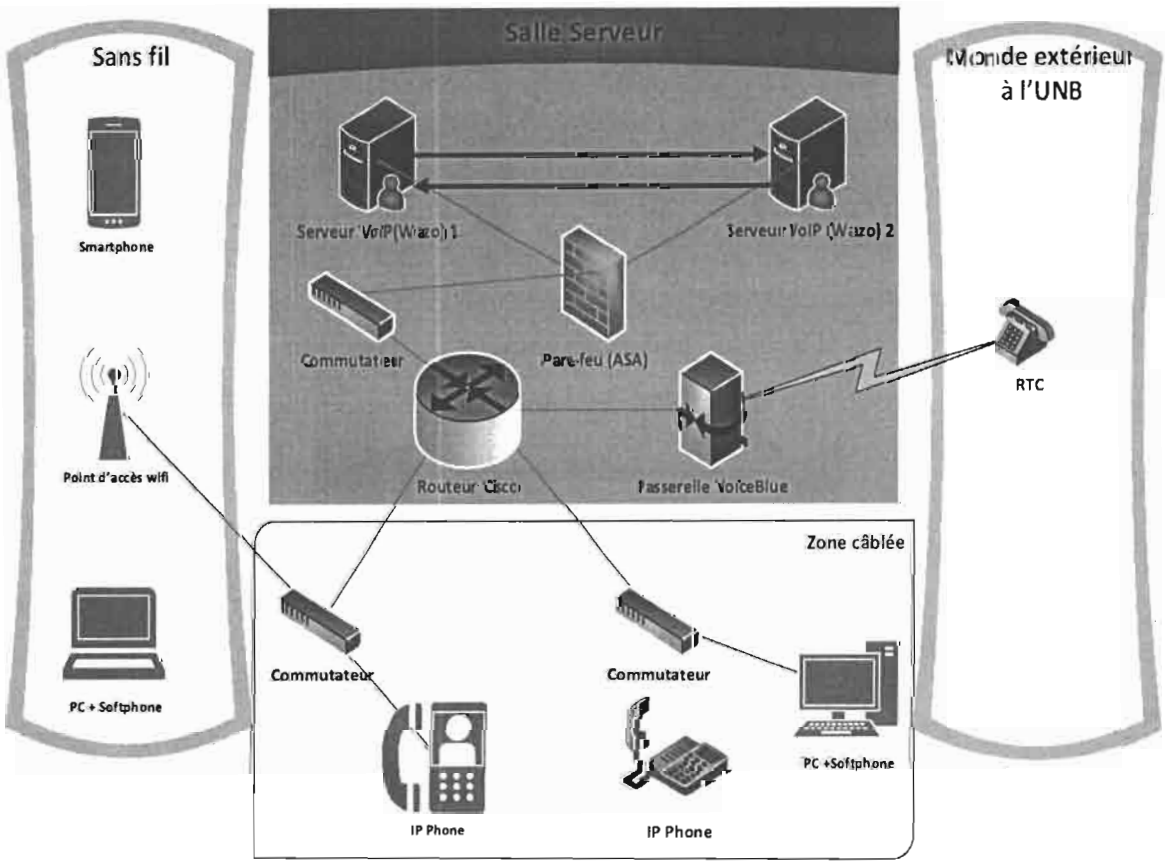

Figure IV.4 : architecture de mise en œuvre de la solution

IV.8 Conclusion

Pour répondre aux besoins de l'U.N.B., nous avons choisi le PBX Wazo, le soft-phone XiVO-Client et le codec G729. L'Université dispose d'un énorme avantage du point de vu équipements (IP Phones, Router, Switch, pilonnes WiMax, etc.). Cependant, il faudra que la DPNTIC prenne le contrôle du réseau UPB+ et opérationnalise les interconnexions entre les différents sites pour que cette étude puisse être bien bénéfique. En plus, pour garantir la haute disponibilité, il convient d'adopter une architecture comme proposé dans la Figure IV.1. Par ailleurs, afin de permettre aux utilisateurs de passer des appels vers l'extérieur, nous avons choisi la passerelle VoiceBlue. Dans le prochain chapitre, nous procèderons à la gestion de la QoS.

CHAPITRE V : GESTION DE LA QOS

V.1 Introduction

Dans ce chapitre nous exposerons des mesures à mettre en œuvre afin de garantir une bonne QoS. Pour cela, il est nécessaire de comprendre la notion même de « qualité de service » et ses critères d'appréciation. Nous présenterons aussi les moyens utilisés pour mesurer cette QoS.

V.2 Etude théorique des exigences QoS de VoIP

V.2.1 Notion de qualité de service

La qualité de service (QDS) ou quality of service (QoS) est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, débit, délais de transmission, gigue, taux de perte de paquets…

La qualité de service est un concept de gestion qui a pour but d'optimiser les ressources d'un réseau (en management du système d'information) ou d'un processus (en logistique) et de garantir de bonnes performances aux applications critiques pour l'organisation. La qualité de service permet d'offrir aux utilisateurs des débits et des temps de réponse différenciés par applications (ou activités) suivant les protocoles mis en œuvre au niveau de la structure [24].

Pour une infrastructure VoIP, gérer la QoS revient à prioriser le flux voix par rapport au flux donnée. Pour cela, il nous faudra d'abord séparer les flux. Plusieurs critères d'appréciation de qualité de service existent.

Les aspects déterminants pour la qualité de la voix sur un réseau sont le traitement de la voix, la clarté, le délai de bout en bout et l'écho. [4] [7]. En effet, lors de l'émission du signal, la voix est traitée, c'est à dire codée et éventuellement compressée, avant d'être transmise. La clarté fait allusion à la mesure de fidélité de la voix reçue par rapport à la voix émise. Le délai quant à lui, fait référence au temps de propagation de la voix à travers le réseau de l'émetteur vers le récepteur. Le son émis par l'émetteur et qui lui revient est l'écho.

La transmission de données classiques (fichiers, messages, transactions …) ne supporte aucune perte en ligne sous peine de graves conséquences pour l'interprétation et l'utilisation de ces données par l'équipement récepteur, mais elle supporte en revanche une dérive importante en

termes de durée d'acheminement. Le comportement attendu pour la voix est exactement inverse 1% ou 2% de perte de données de voix en ligne ne sont pas trop gênants pour la qualité du service de VoIP, cependant, une variation fréquente de 100 ms sur le délai de transit est catastrophique et rend le service inutilisable.

Nous présenterons par la suite les principaux paramètres influents en VoIP, dont l'ordre les échantillonnages (codecs), le délai de transit, la gigue de phase et les pertes de données.

V.2.2 Les différents échantillonnages

Le paramètre d'échantillonnage ou codec (pour compression / décompression) est structurant en VoIP. Le codec détermine à quelle vitesse la voix est échantillonnée et dimensionne le flux de données numériques que va générer la transformation d'un échantillon temporel de voix analogique. Les codecs sont répertoriés par leur nom à l'ITU. Les codecs les plus utilisés et leurs vitesses d'échantillonnage consignés dans le Tableau V.1.

Tableau V.1 : vitesse d'échantillonnage des codecs [7]

Codec	Vitesse
G.711	64 kbps
G.726	32 kbps
G.726	24 kbps
G.728	16 kbps
G.729	8 kbps
G.723.1 MPMLQ	6.3 kbps
G.723.1 ACELP	5.3 kbps

Le choix du codec est un compromis entre la qualité de service souhaité et la capacité de l'infrastructure IP à délivrer une bande passante et des paramètres de QoS qui vont impacter cette qualité. Le paramètre le plus déterminant auquel on s'intéresse pour commencer est la bande passante que l'on met au regard du nombre de communications simultanées à écouler. Le choix du codec G.711 permet de bénéficier à un réseau constant, de la meilleure qualité de service, tandis que les compressions G.726, G.728, G.729 et G.723 apportent avec elles des diminutions initiales de la QoS, immédiatement reflétées dans le score MOS de mesure de la qualité que nous étudierons plus tard.

V.2.3 Le délai de transit

Le délai de transit (ou end-to-end delay dans la dénomination anglo-saxonne) est un des paramètres critiques influençant fortement la QoS d'un service de voix sur IP. C'est le temps que va mettre en moyenne un paquet IP contenant un échantillon de voix pour traverser l'infrastructure entre deux interlocuteurs. Ce temps de transit comporte quatre composantes :

- le délai d'échantillonnage ;
- le délai de propagation ;
- le délai de transport ;
- le délai des buffers de gigue.

Le délai d'échantillonnage est la durée de numérisation de la voix à l'émission puis de conversion en signal voix à la réception. Ce temps dépend du type de codec choisi et varie de quelques millisecondes avec le codec G.711 (échantillonnage 64 kbps), et à plus de 50 ms en G.723 (échantillonnage 6,3 ou 5,3 kbps). C'est une des raisons pour laquelle le choix du codec impacte le score MOS d'appréciation de la clarté de la voix, indépendamment des autres caractéristiques de l'infrastructure [4].

Le délai de propagation est la durée de transmission en ligne des données numérisées. Cette durée est normalement très faible par rapport aux autres composantes du délai de transit, de l'ordre de quelques millisecondes.

Le délai de transport est la durée passée à traverser les routeurs, les commutateurs et les autres composants du réseau et de l'infrastructure de téléphonie IP. L'ordre de grandeur est de plusieurs dizaines de millisecondes, voir centaines de millisecondes.

Le délai des buffers de gigue est le retard introduit à la réception en vue de lisser la variation de temps de transit, et donc de réduire la gigue de phase. L'ordre de grandeur est de 50 ms. Les éléments d'infrastructure, notamment les routeurs, peuvent également mettre en œuvre des buffers de gigue [4].

La qualité de la conversation se dégrade au fur et à mesure que le délai de transit s'accroit. Pour un délai deux-cent (200) ms la difficulté déjà à 28%, pour quatre-cent-cinquante (450) ms à 35% et sept-cent (700) ms à 46%.

V.2.4 La gigue de phase

La variation de temps de transit, ou gigue de phase, est la conséquence du fait que tous les paquets contenant des échantillons de voix ne vont pas traverser le réseau à la même vitesse. Cela crée une déformation de la voix.

La gigue de phase est indépendante du délai de transit. Le délai peut être court et la gigue importante ou inversement. La gigue est une conséquence de congestions passagères sur le réseau, ce dernier ne pouvant plus transporter les données de manière constante dans le temps. La valeur de la gigue va de quelques ms à quelques dizaines de ms. Cependant, pour une bonne conversation, elle doit être constante et rester inférieure à cent (100) ms.

V.2.5 Le phénomène d'écho

C'est le délai entre l'émission du signal et la réception de ce signal reverbéré. Il n'est pas perceptible s'il est moins de cinquante (50) ms.

V.2.6 La perte de données

La transmission de la voix par paquets s'appuie sur le protocole RTP (real-time transport protocol). Ce dernier permet de transmettre sur IP les paquets de voix en reconstituant les informations même si la couche de transport change l'ordre des paquets. Il utilise pour cela des numéros de séquence et s'appuie sur UDP.

Les contraintes temps réel de délai de transit évoquées plus haut rendent inutile la retransmission des paquets perdus : même retransmis, un datagramme RTP arriverait bien trop tard pour être d'une quelconque utilité dans le processus de reconstitution de la voix. En voix sur IP on ne retransmet donc pas les données perdues. Ces pertes de données VoIP sont dues aux congestions sur le réseau, qui entraînent des rejets de paquets tout au long du réseau. Elles peuvent être dues à une gigue excessive qui va provoquer des rejets de paquets dans les buffers de gigue du récepteur, ceux-ci ne pouvant pas accueillir tous les paquets arrivés en retard [4].

Une perte de données régulière mais faible est moins gênante en voix sur IP que des pics de perte de paquets espacés mais élevés. En effet l'écoute humaine s'habituera à une qualité moyenne mais constante et en revanche supportera peu de soudaines dégradations de la QoS.

V.3 Techniques de gestion de la QoS VoIP

La voix et les données n'ont pas les mêmes exigences en termes de délais de transmission des paquets. Par exemple, un retard d'une (01) minute d'un paquet transportant de la donnée est sans inconvénient majeur. Par contre, une interruption de trente (30) seconde lors d'une

conversation est intolérable. Donc il est nécessaire de trouver des solutions pour que les paquets voix soient véhiculés dans les délais recommandés.

V.3.1 Définition de classe de service

Cette méthode consiste à différencier les types de paquets (voix, vidéo, mail, web,...) afin de créer des priorités de traitement et de sorte à pouvoir réserver la bande passante en conséquence. La mise en place la plus courante est la création deux réseaux virtuels : un réseau pour les données et un autre pour la voix. C'est une configuration qui consiste à faire passer la voix et les données sur un même support physique mais par des canaux logiques différents. Elle constitue un principe de base pour une gestion de la QoS : on ne peut prioriser la voix si elle transite par le même canal (logique) avec les données.

La Figure V.1 décrit la création de deux VLANs (Virtual Local Area Network) dans un commutateur. Ces VLANs ont pour identifiants 10 et 20. Après cette étape, il faut affecter ces VLANs à des ports différents. La Figure V.2 donne un exemple de cette configuration avec affectation du VLAN 10 au port 0/1 et du VLAN 20 au port 0/2.

```
Switch#enable
Switch#vlan database
Switch(vlan)#vlan 10 name vlan10
Switch(vlan)#vlan 20 name vlan20
Switch(vlan)#exit
Switch#
```

Figure V.1 : créations des VLANS 10 et 20

```
Switch#configure terminal
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#end
Switch#
```

Figure V.2 : Affectation des VLAN 10 et 20 aux ports

V.3.2 La bande passante et la puissance de traitements des routeurs

Ce procédé a pour but l'amélioration du temps de transit des paquets dans le réseau. Les différents bâtiments du site de Nasso et du centre de calcul sont interconnectés par fibre optique et des commutateurs FastEthernet (des centaines de Mbits/s). Cependant les différents sites sont interconnectés par de la liaison radio. En plus de constituer un goulot d'étranglement, ces liaisons sont simplement non opérationnelles. Afin d'avoir une bonne QoS, l'on se doit d'harmoniser et le câblage, et les équipements.

Pour une bonne efficacité des routeurs dans le traitement, il y'a d'une part la puissance de calcul de ces derniers. En général, un routeur peut traiter jusqu'à 100 000 paquets par seconde. Il est envisagé d'augmenter cette puissance de traitement des routeurs. On parle de Giga Routeurs et de Tétra routeurs qui peuvent traiter un million et un milliard de paquets par seconde. D'autre part, il y'a l'architecture même du réseau. La figure IV.2 illustre une architecture permettant de décharger les routeurs et d'éviter le risque de déni de service.

V.4 Outils de vérification de la QoS

V.4.1 La méthode MOS

La méthode MOS est une mesure subjective de la QoS voix par des opérateurs humains. Elle n'a pas pour objet de fournir des données objectives mais d'obtenir une appréciation de la clarté de la voix reçue grâce à une enquête auprès d'un panel d'usagers ou d'opérateurs représentatifs. Cette méthode est définie par la spécification ITU P800 (MOS Mean Opinion Score, pour « note moyenne d'appréciation »). Son application est coûteuse, mais reste conseillée en dernier recours lors de problèmes de plainte des utilisateurs du service de téléphonie. Elle s'applique aussi bien à la téléphonie traditionnelle qu'à la VoIP [4].

V.4.2 Calcul du facteur R de l'E-model

L'ETSI (European Telecommunications Standard Institute) a développé un modèle de calcul de la qualité de transport de la voix de bout en bout, de la bouche de l'émetteur à l'oreille du récepteur, connu sous le nom de E-model (référence ETSI : ETR 250). Ce modèle a été standardisé par l'ITU sous la référence G.107. Le principe de l'E-model consiste à calculer une grandeur unique R en fonction des paramètres suivants :

$$\mathbf{R = R0 - Is - Id - Ie + A}$$

Le principe de la formule est de partir d'un certain capital de QoS, égal à R0, et de lui imputer les dommages causés par les différents aspects de la transmission. Les différents coefficients utilisés dans la formule de R sont les suivants :

- ***R0*** est la valeur que l'on obtiendrait si la transmission était parfaite. C'est le « capital initial de QoS ». Comme le simple fait de numériser la voix à l'émission pour la reconvertir en signal analogique à la réception provoque une dégradation, la recommandation attribue à R0 une valeur par défaut de 94,3, correspondant à une valeur MOS de 4,5.
- ***Is*** intègre les dommages qui sont simultanés à l'émission de la voix, dus notamment aux conditions d'émission. Il est important de noter que Is et R0 ne différent pas entre la téléphonie classique et la ToIP.
- ***Id*** intègre le délai de transit comprenant toutes les composantes citées plus haut sauf le délai d'échantillonnage.
- ***Ie*** intègre la probabilité qu'un paquet soit retransmis sur le réseau, ainsi que les facteurs de distorsion introduits par le codage de la voix.

Le facteur R ainsi calculé de 0 à 100 permet de déduire directement un coefficient MOS de zéro (0) à cinq (5). Dans la réalité les valeurs de R oscillent entre 50 et 93,2, soit la limite basse acceptable pour le récepteur, et la limite haute liée aux possibilités techniques de transformation de la voix humaine en signal. La moyenne de la valeur R sur les services en production se situe dans la fourchette de soixante-et-dix (70) à quatre-vingt (80).

V.4.3 Conversion R / MOS

Le graphique de la Figure V.3 présente la courbe MOS = f (R). Le facteur MOS est la perception humaine tirée d'un protocole de test précis. L'inflexion vers le haut indique qu'à partir d'un certain niveau de qualité, l'augmentation de celle-ci, reflétée par le facteur R, est moins perçue par l'utilisateur. On observe le même phénomène en bas de la courbe, une diminution de R étant moins perçue par l'utilisateur quand la qualité est déjà très dégradée.

Le Tableau V.2 présente la correspondance entre les valeurs de R et le la qualité de la voix transmise (nous avons conservé la terminologie anglo-saxonne de la recommandation ITU-T) :

Le codec introduit donc une composante dans Ie, dont les valeurs sont données dans le Tableau V.3 [4].

En cas de transcodages multiples les coefficients ***Ie*** se cumulent, ce qui rend cette opération extrêmement coûteuse en termes de bilan de QoS. Le taux de perte de données influera d'autant plus sur ***Ie*** que l'on aura choisi un codec lent.

A est un coefficient de prise en compte de facteurs d'amélioration du réseau. Le principe est de considérer que le fait d'avoir une facilité d'accès au service de téléphonie permet de supporter quelques désagréments : par exemple A = 10 pour les mobiles. On accepte sur un téléphone portable des imperfections que l'on ne tolèrerait pas en téléphonie fixe [4].

Tableau V.2 : correspondance R-qualité [4]

Coefficient R	Qualité de transmission de la voix
90-100	Best
80-90	High
70-80	Medium
60-70	Low
0-60	Very poor

Tableau V.3 : composant des codecs dans le Ie [4].

Codec	Débit codec	Coefficient Ie	Facteur R « intrinsèque »
G.711 PCM	64 kbps	0	94.3
G.726 ADPCM	32 kbps	7	87.3
G.726 ADPCM	24 kbps	25	69.3
G.728 LD-CELP	16 kbps	7	87.3
G.729 CS-ACELP	8 kbps	10	84.3
G.723.1 MP-MLQ	6.3 kbps	15	79.3

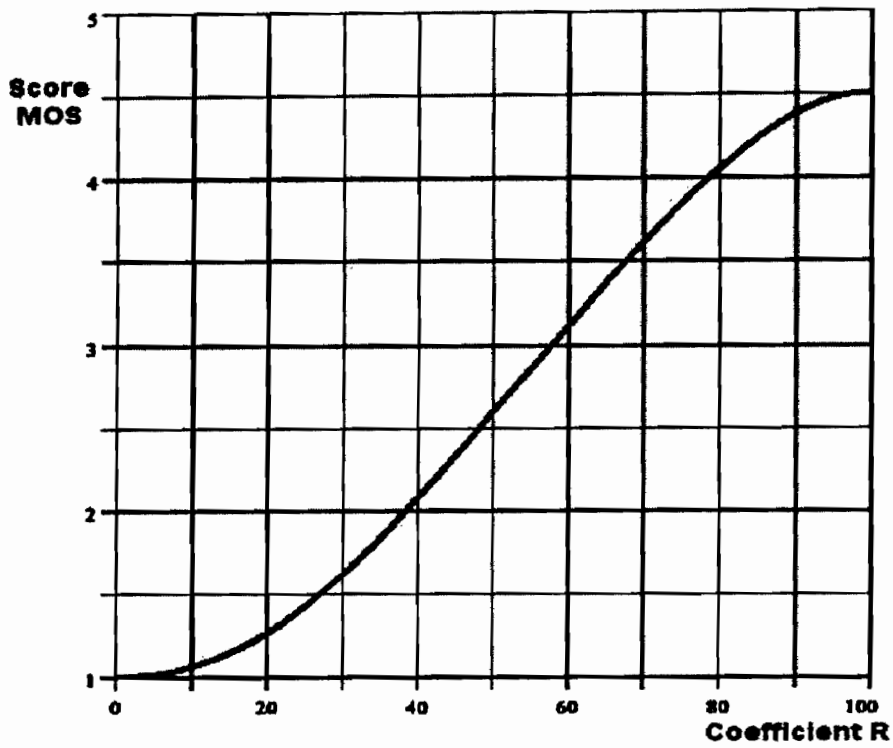

Figure V.3 : conversion R

V.5 Impact négatif du service VoIP sur les autres services

La priorisation de la VoIP a indéniablement des répercussions les autres services surtout quand la bande passante disponible est faible. En rappelle, la voix et les données n'ont pas les même exigences. La voix est plus requière un délai de transmission assez bref, tandis que les données se doivent d'être intègre à la réception afin d'être utile.

Une infrastructure VoIP est composée de téléphones IP, Gateway, serveurs (proxy, register, etc.). Chaque élément, que ce soit un système embarqué ou un serveur standard tournant sur un système d'exploitation, est accessible via le réseau comme n'importe quel ordinateur. Chacun comporte un processeur qui exécute des logiciels qui peuvent être attaqués ou employés en tant que points de lancement d'une attaque plus profonde. Pour ainsi dire, la VoIP peut s'avérer néfaste pour les services existants. Cette situation peut être issue de causes différentes.

D'abord, il peut exister une incompatibilité entre l'architecture réseau existant et celle requise par la VoIP. Dans ce cas, une mauvaise étude peut amener à adapter l'infrastructure de façon unilatérale, c'est en tenant compte uniquement de la VoIP. Ceci peut entraîner un disfonctionnement des services existants.

En plus un nouveau service nécessite de nouveaux moyens. L'exigence en bande passante de la téléphonie sur IP est plus élevée que les données ordinaires. Les exigences de cette

technologie se font ressentir même au niveau des routeurs et des serveurs ; c'est-à-dire des appareils de grandes capacité avec une puissance de calcul acceptable. Un manquement à ces obligations peut se révéler fatal pour les autres services, surtout pour une utilisation de cette téléphonie à grande échelle.

Aussi, du fait de la gratuité de la communication, les utilisateurs risquent de passer plus de temps au téléphone qu'à accomplir les tâches qui leur sont assignées. Cela a pour conséquence une hausse de la consommation de la bande passante. Etant donné que la voix est priorisée par rapport aux données, en situation d'engorgement, les autres services seront simplement inutilisables

Enfin une mauvaise configuration de la VoIP peut provoquer un disfonctionnement générale. Cela peut rendre certains services critiques indisponibles.

V.6 Simulation de 500 sessions de communications simultanées

La notion de qualité de service est une notion subjective, de ressenti utilisateur face à l'utilisation d'un système informatique. Il n'est pas trivial de mesurer cette QoS. Cependant des performances jugées acceptables existent. Pour ce projet, nous optons pour l'utilisation d'Iperf. Ce logiciel de mesure de performance réseau, disponible sur de nombreuses plateformes (Linux, BSD, Mac, Windows...) se présente sous la forme d'une ligne de commande à exécuter sur deux machines disposées aux extrémités du réseau à tester.

Il permet de générer en sortie un rapport sur le débit (moyen, minimum et maximum) et le délai. L'idée générale et de faire un plan de test avec les différentes configurations possible en terme d'utilisation et de QoS et de regarder les valeurs obtenues en sorties. La Figure V.4 illustre le fonctionnement d'Iperf. Iperf doit être lancé sur deux machines se trouvant de part et d'autre du réseau à tester. La première machine lance Iperf en « mode serveur » (avec l'option -s), la seconde en « mode client » (option -c). Par défaut le test réseau se fait en utilisant le protocole TCP (mais il est également possible d'utiliser le mode UDP avec l'option -u) comme le présente la figure V.1.

En plus, il peut être utile d'utiliser un logiciel de capture réseau tel que Wireshark. En effet, grâce à ce dernier, nous pouvons sauvegarder les flux et les filter/analyser avec les nombreux modules disponibles.

Outre cela, Wazo dispose d'un module d'administration permettant de suivre en temps réel la consommation en ressources.

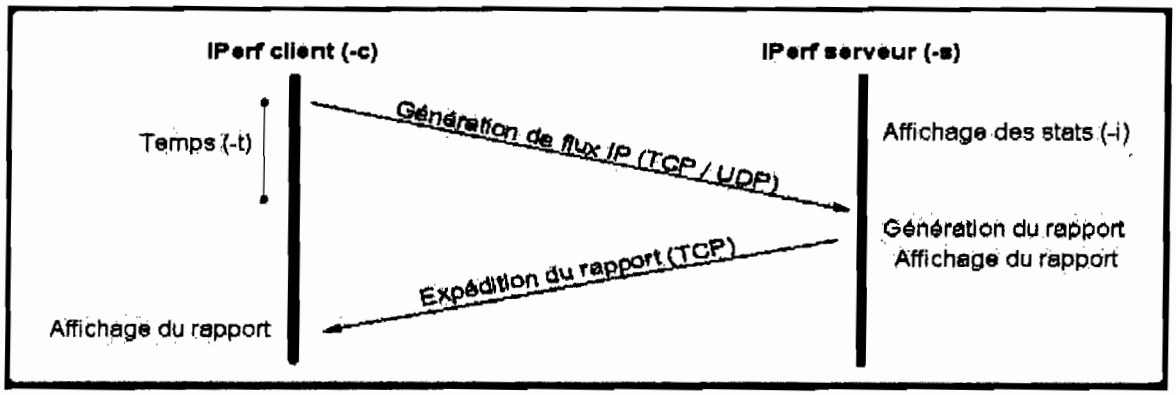

Figure V.4 : principe de fonctionnement d'IPerf

V.7 Conclusion

La gestion QoS consiste en la priorisation du trafic voix par rapport à celui des données. Les critères d'appréciations les plus importants sont le débit, la gigue, la latence. La différenciation des services, l'augmentation de la bande passante, la puissance de traitement des routeurs et l'harmonisation des équipements sont autant de facteurs à prendre en compte afin de garantir une bonne qualité de service VoIP. Une mauvaise gestion de la QoS peut entrainer un disfonctionnement des autres services, surtout quand les ressources sont limitées. Dans le prochain chapitre, nous traiterons la question sur la gestion de la sécurité de l'infrastructure VoIP.

CHAPITRE VI : GESTION DE LA SECURITE

VI.1 Introduction

Dans ce chapitre, nous présentons les différentes menaces qui pèsent sur notre service VoIP et les moyens pour les contrecarrer. Par la suite, nous exposerons l'impact de ce nouveau service sur la sécurité des services existant, tel que la messagerie, le web et le DNS.

VI.2 Les différents types d'attaques

Les risques qui menacent les infrastructures VoIP sont nombreux. Outre les risques intrinsèquement liés à la téléphonie traditionnelle, ces nouveaux systèmes héritent des problèmes d'insécurité liés aux protocoles qu'ils emploient. Ces risques sont entre autre [25] :

- l'envoi massif de paquets réseaux pour perturber le flux du protocole de signalisation Voix ;
- l'envoi massif de paquets réseaux pour perturber le flux Voix ;
- l'envoi massif de paquets TCP/UDP/ICMP à destination du téléphone IP pour fragiliser sa pile IP ;
- l'exploitation des failles et des faiblesses d'implémentation des protocoles Voix (signalisation ou média) ;
- l'exploitation des failles ou faiblesses d'implémentation du système d'exploitation supportant l'IP PBX ;
- le déni de Service sur l'accès sans fil ;
- le déni de Service sur les services réseaux ;
- l'injection de paquets Voix ;
- la modification des paquets Voix
- la modification de la qualité de service ;
- la modification des VLAN ;
- l'utilisation des techniques de "social engineering" pour contourner les limitations imposées par l'administrateur ;
- la connexion d'un téléphone IP frauduleux ;
- l'attaque de type "cache poisoning" ;

- le détournement des appels ToIP ;
- le vol de données des applications ToIP (ex taxation) ;
- l'écoute des conversations ;
- l'interception des protocoles de signalisations ;
- la fraude téléphonique (on retrouve le même type de faiblesse que sur un système classique) ;
- l'utilisation détournée de la messagerie ou accès aux données utilisateurs ;
- l'attaque sur les systèmes d'authentification utilisateurs présents dans une solution de ToIP.

Ces attaques visent généralement, soit à interrompre le service VoIP, soit à voler des données et/ou services.

VI.2.1 La reconnaissance

Il s'agit tout simplement de mener une enquête sur le réseau et le système téléphonique installé pour les connaître le mieux possible. Elle a pour but de trouver des points de vulnérabilité ou encore des informations directement en relation avec un bug déjà référencé. Des méthodes comme le scan de ports, de plages d'adresses IP ou de numéros de téléphone, la reconnaissance de système via le "fingerprinting" peuvent être utilisées.

Une reconnaissance positive sur un réseau permet de connaître son plan d'adressage IP, les serveurs opérationnels avec les versions installées, les protocoles utilisés dans l'entreprise, les versions d'IOS, etc.

Une fois ces informations réunies, une attaque peut être lancée sur un point bien particulier comme un périphérique réseau, un service Windows ou Unix…

VI.2.2 The Man In The Middle (MITM)

MITM est une attaque au cours de laquelle la personne malveillante a la capacité de lire, insérer ou modifier les messages échangés entre les deux parties, et cela sans qu'elles n'en soient conscientes. Ce type d'attaque peut notamment être utilisé pour réaliser des écoutes ou encore des dénis de service.

VI.2.3 Le déni de service (aussi connu sous le nom DoS)

Le DoS est une attaque sur un système informatique, un réseau, qui peut provoquer une interruption du service initialement rendu à l'utilisateur à cause d'une réduction de la bande passante du système, ou de l'utilisation de toutes les ressources système. Ce type d'attaque peut être réalisé de nombreuses façons. On remarque cependant trois schémas de base :

- la réduction des ressources informatiques comme la bande passante, l'espace disque ou la puissance CPU ;
- la perturbation des tables de routage ;
- la perturbation d'éléments physiques du réseau.

VI.3 Mesures de sécurité

Nous proposons plusieurs solutions conjointes afin de garantir un certain niveau de sécurité de notre système.

VI.3.1 La sécurité physique

La sécurité physique est une partie essentielle de tout environnement sécurisé. Elle doit permettre la limitation des accès aux bâtiments et équipements ainsi qu'à toutes les informations qu'ils contiennent, évitant ainsi les intrusions inopportunes, le vandalisme, les catastrophes naturelles, et les dommages accidentels (pic d'intensité électrique, température trop élevée…).

Aussi, Les prises LAN présentes dans la plupart des bureaux permettent non seulement un accès beaucoup plus simple au réseau, mais évitent aussi et surtout aux pirates de se faire remarquer. Même avec le chiffrement des communications mis en place, un accès physique aux serveurs Voix ou aux passerelles peut permettre à un attaquant d'observer le trafic (qui appelle qui ? à quelle fréquence ? etc.). Ainsi, une politique de contrôle d'accès pour restreindre l'accès aux composants du réseau de VoIP via des badgeuses, serrures, service de sécurité, etc., permettra d'établir un premier périmètre sécurisé.

En plus, lors de la mise en place d'un système de VoIP, l'alimentation électrique doit être étudiée en détail pour éviter toute interruption de service due à une coupure de courant. Deux possibilités peuvent être utilisées pour alimenter le poste IP :

- brancher le téléphone sur le secteur via un transformateur,
- utiliser le protocole PoE (Power over Ethernet – alimentation électrique du poste via le réseau informatique).

VI.3.2 La sécurisation des serveurs

L'ensemble des serveurs participant à une solution de VoIP doit respecter une procédure de mise en place standard et être sécurisé avant toute connexion au réseau.

La sécurisation des serveurs comprend notamment :

- la suppression des comptes inutiles,
- la vérification du bon niveau de droit des différents comptes,

- la suppression des services inutiles,
- la suppression des logiciels ou modules inutiles,
- le bon niveau de correction par rapport aux publications des éditeurs/constructeurs.

Par ailleurs, nous recommandons un audit régulier des serveurs en production afin de vérifier le bon fonctionnement de ceux-ci et s'assurer que les utilisateurs ne détournent pas les serveurs de leurs fonctionnalités initiales, provoquant alors une baisse du niveau de sécurité.

La voix sur IP repose sur un grand nombre de services fournis par le réseau pour fonctionner correctement (diffusion de la configuration, supervision de la solution, localisation des utilisateurs, …). On retrouve notamment les services comme DNS, DHCP, LDAP, RADIUS, HTTP, HTTPS, SNMP, SSH, TELNET, NTP et TFTP. Il y a aussi ainsi la gestion dynamique de la qualité de service. Idéalement, les services utilisés par l'infrastructure communication devraient être dédiés et les serveurs, bien sécurisés. A cet effet, des configurations existent pour élever le niveau de sécurité du serveur Astérisk.

D'abord il faudra changer des ports par défaut pour les protocoles SIP, IAX2, SSH. Pour le SIP la modification peut être faite dans le fichier sip.conf dans la section « general », pour **SSH** dans le fichier /etc/ssh/sshd_config et pour IAX dans le /etc/asterisk/iax.conf

Ensuite il est judicieux d'interdire le login « root » à ssh. Il faut créer le nouvel utilisateur avec la permission d'accès par ssh :

 # useradd < nouvel_utilisateur >
 # passwd < pass >
 # gedit /etc/ssh/sshd_config

Ajouter la ligne

AllowUsers <novel_utilisateur>
Changer ***PermitRootLogin yes*** pour ***PermitRootLogin no***

En plus il est important d'établir des IP autorisés pour les clients VoIP. Cette configuration peut être effectuée dans le fichier sip.conf. Pour chaque nouveau client VOIP il faut indiquer l'adresse IP ou la plage des adresses IP autorisées

L'Interdiction d'accès à Asterisk sans authentification s'avère capitale. A cet effet l'option *allowguest=yes* autorise n'importe quel appel entrant SIP sans authentification ou autre

restriction, et le passe au contexte déclaré par défaut pour les appels SIP. L'option *allowguest* ne devrait jamais être mise sur *yes*

Afin de palier le déni de service, nous configurerons une limitation du nombre des appels simultanés. Dans la configuration de clients SIP il faut établir le paramètre.

```
call-limit=1
```

Par ailleurs, il faut veiller à différencier vos noms d'utilisateurs de vos extensions SIP. Il est conseillé de choisir un nom d'utilisateur SIP différent de l'extension.

Une bonne pratique contre les attaques de type DoS consiste à limiter les trafics sur le serveur en ne laissant passer que celui voix. Cette solution se met en place en paramétrant le pare-feu *Netfilter* du noyau Linux à travers la commande *iptables* comme le monte la configuration suivante :

- Autoriser le trafic entrant du protocole SIP grâce son numéro de port

```
#i ptables - A INPUT-p udp  -m udp –dport 5060 –j ACCEPT
```

- Autoriser le trafic entrant du protocole RTP

```
# iptables -A INPUT -p udp -m udp –dport 10000:20000 -j ACCEPT
```

- Interdire tout autre trafic entrant UDP

```
#i ptables - A INPUT -p UDP -j DROP
```

- Limiter le nombre de requêtes de synchronisation par seconde

```
#i ptables –A INPUT -p tcp –syn –m limit –limit 1/s –j ACCEPT
```

VI.3.3 Fail 2 ban

Fail 2 Ban est un outil propre aux systèmes Linux, permettant de se protéger contre les attaques de brute force ayant pour but de permettre à un attaquant de s'authentifier. Il est possible de configurer Fail2Ban pour qu'il protège Asterisk.

Fail2Ban n'est donc pas un outil propre à Asterisk. Il est utilisé pour se protéger contre les attaques de brute force d'authentification (SSH, Apache, FTP, etc…). Dans le cas d'Asterisk, Fail2Ban va analyser les logs d'Asterisk, à la recherche de tentatives de connexions échouées.

Si Fail2Ban détecte plus de trois (03) connexions échouées, il bloque l'IP source du client qui tente de se connecter. Le blocage se fait à l'aide d'une règle IP table.

Il est bien entendu possible de paramétrer le nombre de connexion menant à un blocage. De même qu'il est possible de paramétrer le temps de blocage, ou l'intervalle de temps de recherche de Fail2Ban. Par exemple : bloquer un client pendant 1h après 5 tentatives d'authentifications manquées en 10 mins. [12]

VI.3.4 L'authentification des utilisateurs

Afin de renforcer la sécurité d'accès au serveur, nous proposons une authentification LDAP pour tout utilisateur. En effet tout utilisateur devra s'authentifier de prime à bord auprès du serveur LDAP Radius. Cette mesure met le serveur de téléphonie un peu plus à l'abri. Wazo intègre parfaitement cette fonctionnalité

VI.3.5 Sécurisation des Protocoles

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

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

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

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

VI.3.6 La séparation et la sécurisation des flux

La séparation logique des flux voix et data à l'aide de VLAN est une mesure fortement recommandée. Elle doit permettre d'éviter que les incidents rencontrés sur l'un des flux ne puissent perturber l'autre. Les VLAN ou réseaux locaux virtuels, peuvent être représentés comme une séparation logique d'un même réseau physique. Cette opération se fait au niveau 2 du modèle OSI.

La mise en place de plusieurs VLAN permet de mieux gérer la qualité de service. Elle permet aussi d'organiser les postes utilisateurs selon leurs situations physiques dans les bâtiments, le service auquel appartient l'utilisateur. Un renforcement de la sécurité peut être réalisé en mettant en place un filtrage inter-VLAN, n'autorisant que les utilisateurs d'un VLAN à y accéder. Toutes ces manœuvres diminuent le risque de déni de service.

VI.3.7 Chiffrement des appels

La sécurisation des appels peut être intéressante à mettre en place, afin de protéger nos appels téléphoniques. Nous pouvons chiffrer le flux de signalisation ainsi que le flux audio. De cette manière, nous pouvons assurer la confidentialité. Pour sécuriser les appels, il nous faut chiffrer deux éléments.

D'une part l'on peut sécuriser le flux SIP (la signalisation) avec TLS. Le protocole TLS permet de créer un tunnel entre un ordinateur et un serveur. Ce tunnel sécurisé permet un échange d'informations en contournant les dispositifs de sécurité installés pour un serveur ou un ordinateur. Passant outre les systèmes de protection il est alors possible que des actions malveillantes soient menées au travers du point d'entrée du tunnel. Afin de limiter les risques, il est techniquement possible de filtrer les contenus d'un tunnel TLS par la mise en place d'un dispositif qui authentifie le client et le serveur. Deux tunnels sont alors mis en place, un depuis le client vers le dispositif d'authentification et le second du dispositif vers le serveur. Ce système permet alors une analyse et une sécurisation transparente des contenus transférés par le tunnel TLS [13]

D'autre part, le flux RTP (la voix) peut être sécurisé grâce avec Secure RTP (SRTP). Pour le cryptage et le décryptage du flux de données, SRTP (avec SRTCP) standardise l'utilisation du chiffrement AES, bien que n'importe quel chiffrement puisse être utilisé. AES qui à l'origine peut être utilisé dans deux modes de chiffrement, dont le mode bloc (CBC), est ici utilisé en

mode comptage (CTR), car il s'agit d'un chiffrement de flux. AES travaille sur des blocs de 128 bits.

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

- SRTP MKI (SRTP Master Key identifier) : sert à ré-identifier une clef maîtresse particulière dans le contexte cryptographique. Le MKI peut être utilisé par le récepteur pour retrouver la clef primaire correcte quand le besoin d'un renouvellement de clefs survient.
- Authentication tag : est un champ inséré lorsque le message a été authentifié. Il est recommandé d'en faire usage. Il fournit l'authentification des en-têtes et données RTP et indirectement fournit une protection contre le rejet de paquets en authentifiant le numéro de séquence.

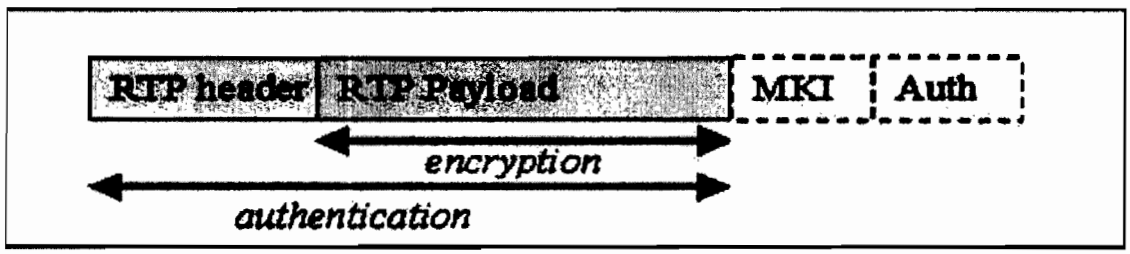

Figure VI.1 : le format d'un paquet SRTP

Les différentes clefs utilisées par SRTP (authentification, chiffrement) dérivent d'une seule et unique clef maitresse (« master key »). Il y a donc nécessité d'échanger la « master key ». Il existe plusieurs protocoles d'échange de clef utilisables avec SRTP. A ce propos, protocole ZRTP décrit une méthode d'échange de clefs utilisant Diffie-Hellman. La négociation d'un secret partagé, qui servira à générer les clefs et le "sel" pour le chiffrement de la session, se fait dans le flux RTP, préalablement établi par un protocole de signalisation tel que SIP. ZRTP est donc indépendant du protocole de signalisation. ZRTP ne nécessite pas d'infrastructure PKI, ou l'utilisation d'un tiers de confiance. Il utilise des clefs différentes à chaque établissement d'une nouvelle session (à l'exception des modes particuliers Preshared et Multistream). L'entête ZRTP se constitue comme ainsi présenté dans la Figure VI.1.

VI.3.8 Le VPN

Une autre solution pour crypter le trafic dans notre réseau, est l'implémentation d'un VPN (Virtual Private Network) au sein des machines utilisées pour la VoIP. Un VPN permet de véhiculer du trafic crypté grâce à des clés de cryptage ce qui rend leur déchiffrage presque impossible par une tierce partie. Il permettra donc de contourner les attaques d'écoute clandestine.

L'outil que nous avons choisi pour la mise en place d'un VPN est OpenVPN. C'est un logiciel «open source» permettant de créer un réseau virtuel basé sur SSL. Il peut être utilisé afin de relier deux réseaux ou plus via un tunnel chiffré à travers l'Internet. Il permet la génération des certificats pour les utilisateurs. Dans notre contexte, le VPN sera utilisé uniquement pour les appels vers le réseau Internet.

VI.3.9 Filtrage

De nombreuses possibilités de protection d'un l'environnement de téléphonie. Parmi celles-ci, il y a l'utilisation d'un ASA de la famille 5500 faisant l'intermédiaire entre un réseau voix sécurisé et un réseau voix non sécurisé.

Ce firewall offre de nombreuses possibilités à savoir la gestion du chiffrement, gestion VPN- ; de plus il met les serveurs à l'abri dans son DMZ (Demilitared Zone), ce qui permet de mieux protéger la téléphonie.

Il existe deux modules sur un ASA permettant de traiter des flux voix spécifiques.

D'abord, le TLS Proxy est un intermédiaire entre deux équipements communicant directement ensemble 'en utilisant des flux cryptés'.

Ensuite, le Phone Proxy est une évolution du TLS Proxy permettant d'utiliser le chiffrage natif sur les IP Phones pour réaliser des appels sécurisés depuis l'extérieur vers l'intérieur de la zone protégée. Ce peut aussi être utilisé pour maintenir une séparation entre les flux voix chiffrés et les données quand les téléphones sont sur le même VLAN 'data'. C'est la solution idéale pour protéger des Softphones, car ils utilisent généralement le VLAN 'data' pour les communications.

En terme de volumétrie maximum, le pare-feu ASA 5580 dont dispose l'université, peut supporter jusqu'à treize-mille (13000) sessions simultannées. Cette valeur est configurée grâce à la commande :

```
# tls-proxy maximum-sessions –nb de sessions–
```

VI.3.10 La supervision

Elle permet d'avoir une vue d'ensemble du réseau. Les outils permettant la supervision des réseaux doivent normalement pouvoir être adaptés pour superviser l'ensemble de l'infrastructure convergente téléphonie sur IP et Data. C'est l'un des grands avantages de l'unification des infrastructures. Par ailleurs, il est recommandé de séparer le trafic généré par les solutions de supervision du reste des applications.

Les systèmes de détection d'intrusion réseau ou NIDS (Network-based Intrusion Detection Systems) ont pour but d'alerter les administrateurs de la solution en cas de trafic anormal ou jugé malicieux. Pour ce projet, nous utiliserons zabbix pour la supervision.

Par sa polyvalence, Zabbix peut superviser et vérifier les statuts d'une multitude de services réseaux, ou systèmes (serveurs), tout en surveillant au niveau matériel de nombreux types d'équipements présents au sein d'une infrastructure IT, comme un routeur, une imprimante, un téléphone IP, etc. grâce à l'utilisation du protocole SNMP. Il supporte également le protocole IPMI, et dispose d'outils d'auto-découverte d'équipements. Il intègre par défaut la gestion de cartes (réseaux) et de graphiques, tous visualisables depuis une même interface. [17][18]

Par ailleurs il est primordial de sensibiliser les utilisateurs sur l'exploitation de la solution et les risques qui y sont liés ; car tout système informatique, quoique sécurisé côté protocoles, demeure en danger tant que les utilisateurs ignorent les bonnes méthodes pour garantir son intégrité.

VI.4 Coût du projet

Le coût de mise en œuvre de ce projet regroupe le coût de matériels et logiciels, ainsi que le coût de l'ingénierie. Le Tableau VI.1 donne plus de détails concernant ce coût. Certains éléments comme les ordinateurs serveurs et les téléphones sont déjà acquis. Par conséquent, nous ne les prenons pas en compte dans le calcul de coûts.

Tableau VI.1 : Coût du projet

Désignation	Caractéristiques	Quantité	Prix unitaire(F CFA)	Montant
IPBX	Wazo 17	02	gratuit	gratuit
Passerelle VoIP-GSM	VoiceBlue	01	900 120	900 120
Softphone	X-lite	-	Gratuit	Gratuit
Softphone	Wazo client	-	Gratuit	Gratuit
Numéro court	-	01	300 000	300 000
Ingénierie	-	01	3 600 000	3 600 000
Total				4 800 120

VI.5 Conclusion

Toute infrastructure VoIP est en proie à multiples attaques. A cet effet, nous avons trouvé une dizaine de mesures pour lui assurer un certain niveau de protection. Ces mesures vont de la sécurité physique à la sécurisation des protocoles en passant par la mise en place des pare-feux et la sécurisation des systèmes d'exploitation tout en respectant les bonnes pratiques pour les configurations des serveurs PBX. Cependant, force est de noter qu'il n'y a pas de sécurité absolue. Les utilisateurs, par l'adoption des bonnes pratiques doivent contribuer à la sécurisation du système VoIP.

CONCLUSION GENERALE

Le projet d'étude de la solution VoIP à l'U.N.B. auquel nous avons participé à la DPNTIC est énoncé dans ce document en six phases. Le cadre général et le contexte du stage et les généralités sur la Voix sur IP ont été les premiers éléments abordés. Ils nous ont permis de comprendre que les acteurs de l'université rencontraient souvent des difficultés dans les communications téléphoniques sur ses différents sites et que la VoIP pourrait être une solution idéale. Ensuite nous avons fait une étude de l'existant afin de mieux appréhender les insuffisances. A l'issue de cette analyse, il s'est révélé que la solution VoIP existante était loin de répondre au besoin actu ; d'où la nécessité de faire un nouveau dimensionnement. La gestion de la QoS et de sécurité était alors une question récurrente qui ne pouvait rester sans réponse.

Les acteurs de L'UPB dépensent énormément dans les communications téléphoniques. Malgré ce coût exorbitant, les réseaux téléphoniques des opérateurs sont souvent saturés ou inaccessibles. Cela ralenti considérablement le travail dans ce sens que les sites sont distants. En plus la solution VoIP existante ne prend en compte qu'une vingtaine d'utilisateurs. De plus il n'y a pas de politique de sécurité garantissant la confidentialité Pour mener à bien ce projet, nous avons élaboré des formulaires d'enquêtes contenus dans les annexe 1 et 2 afin de comprendre les problèmes rencontrés dans les communications téléphoniques sur les différents sites de l'U.N.B., les moyens investis, et le temps mis. Cela nous a permis d'estimer le nombre moyen et maximum d'appels simultanés. Tous ces éléments ont été déterminants pour le dimensionnement. Le plus important à ce niveau a été le choix du serveur BPX, du protocole de signalisation et du codec.

Comme IPBX, Wazo, fork de xivo a été choisi avec SIP comme protocole de signalisation et le codec G729. Il présente de nombreuses fonctionnalités répondant parfaitement au cahier de charges. Mieux encore, il intègre des mécanismes de sécurité comme l'authentification LDAP, la sécurisation des protocoles SIP et RTP, le chiffrement des appels. Il gère par défaut la haute disponibilité avec le principe des serveurs maître/sclave. Afin de renforcer la sécurité, nous préconisons la mise en place du VPN pour les IP Phones, la protection du serveur par un proxy, le filtrage, la supervision, la configuration du « fail 2 ban » et sensibilisation des utilisateurs.

La mise en place de cette solution permettra d'avoir une infrastructure VoIP sécurisée prenant en compte tous les acteurs de l'Université sans exception. En plus la solution est facile à faire évoluer. Cependant une interconnexion opérationnelle entre les différents sites est nécessaire.

Pour ce faire la prise en main du réseau UPB+ par la DPNTIC est indispensable. L'intégration de l'authentification par certificat à l'avenir ne sera pas de trop.

Référence bibliographique

[1] http://www.frameip.com/voip/ consulté le 04/08/2016 à 10h16.

[2] https://www.3cx.fr/ordering/tarifs/licences-annuelles/ consulté le 03/05/2017 à 9h30.

[3] Marguerite Fayçal « Sécurisation de la téléphonie sur IP » ; AUF ; décembre 2004.

[4] Accellent, « La Qualité de Service de la Voix sur IP : Principes et Assurance » ;

[5] https://technet.microsoft.com/fr-fr/library/dd425274(v=office.13).aspx consulté le 20/08/2016 à 03h30.

[6] http://ipbx.pro/le-concept-de-t-voip/ consulté le 09/09/2016 à 10h45.

[7] Abossé AKUE-KPAKPO, «La Voix sur le Réseau IP», Togotel.

[8] Rebha BOUZAIDA, « Étude et Mise en place d'une Solution VOIP Sécurisée » ; mémoire de fin d'étude de Master Professionnel en Nouvelles Technologies des Télécommunications et Réseaux ; 2011.

[9] Laurent OUAKIL & Guy PUJOLLE, « Téléphonie sur P », Eyrolles, 2008.

[10] Jonathan BRIFFAUT & Alexandre MARTIN, « La VoIP: Les protocoles SIP, SCCP et H323 »

[11] http://www.blog.saeeed.com/2011/03/logiciels-de-telephonie-ip-vocal-asterisk-yate-comparaison/ consulté le 03/05/2017 à 10h10.

[12] https://www.networklab.fr/fail-2-ban/ consulté le 05/09/2016 à 02h40.

[13] https://www.networklab.fr/chiffrement-des-appels/ consulté le 05/09/2016 à 15h00.

[14] https://reflets.info/securiser-une-communication-voip-avec-zrtp/ consulté le 12/01/2017 à 8h10.

[15] https://tsrit.com/2013/09/06/securite-aserisk-ou-quelques-moyens-dattaquer-votre-serveur-voip/ consulté le 03/05/2017 à 12h30.

[16] https://support.blackphone.ch/customer/fr/portal/articles/1644773-pourquoi-avons-nous-besoin-zrtp-si-nous-avons-d%C3%A9j%C3%A0-srtp-n-est-ce-pas-srtp-assez-bon- consulté le 13/02/2017 à 11h00.

[17] https://www.monitoring-fr.org/solutions/zabbix/ consulté le 13/02/2017 à 11h15.

[18] http://forum.hardware.fr/hfr/systemereseauxpro/Reseaux/nagios-zabbix-sujet_8158_1.htm consulté le 13/02/2017 à 11h20.

[19] Nicolas FISCHBACH « (In) sécurité de la Voix sur IP (VoIP) »

[20] http://alainfaure.net/2014/02/28/architecture-toip-voip-et-securisation-avec-un-firewall-asa-cisco-famille-5500/ consulté le 14/02/2017 à 7h30.

[21]https://www.voip-info.org/wiki/view/How+to+connect+VoIP+GSM+gateway+to+Asterisk+PBX consulté le 10/01/2017 à 22h20.

[22] https://www.2n.cz/fr/produits/passerelles-gsm/passerelles-gsm-voip/voiceblue-next/etudes-de-cas/ consulté le 10/01/2017 à 23h00.

[23] http://www.asterisk-france.org/archives_net/showthread.php?t=9967 consulté le 16/01/2017 à 13h30.

[24] https://fr.wikipedia.org/wiki/Qualit%C3%A9_de_service consulté le 03/05/2017 à 9h30.

[25] Cédric Baillet, « Sécurisation de la téléphonie sur IP », Orange

ANNEXES

Annexe1 : Mise en place de la solution

Installation de Wazo

Notre solution fonctionne sous un environnement Debian. Cependant, il existe essentiellement deux manières de l'installer.

D'une part, Wazo peut être par téléchargement de paquets. Dans ce cas on utilise la commande wget est pour les obtenir, et sh pour les installer. L'avantage de cette méthode est que l'administrateur est libre de choisir les paquets à installer. Cependant il devra connaître tous les paquets nécessaires au bon fonctionnement du système c'est-à-dire les serveurs de messagerie, DNS, DHCP, Base Donné... En plus la difficulté de ce procédé réside en la gestion des incompatibilités.

D'autre part, la solution peut être mise en place en installant de l'ISO. En effet, le CD de Wazo est système d'exploitation Debian dans lequel est empaqueté initialement notre serveur VoIP avec tous les logiciels complémentaires nécessaires. Ainsi, en installant le système d'exploitation, on dispose de la solution, prête à être configurée. Cette solution nous parait la meilleure, car elle nous épargne les problèmes d'incompatibilité. Le seul inconvénient est qu'après installation, le SE démarre en mode console pendant que le serveur est censé être accessible à travers une interface web. Pour y remédier, nous avons installé l'interface graphique Gnome.

Par ailleurs, il existe des serveurs physiques sur lesquels la solution est déjà opérationnelle. Mais ceux-ci sont payants.

Peu importe la méthode utiliser, la configuration (installation) reste la même. Avant toute configuration, wazo est accessible à travers l'adresse locale 127.0.0.1. La figure VII.1 illustre sa page d'accueil. Il existe en effet trois étapes importantes dans la configuration préliminaire du serveur.

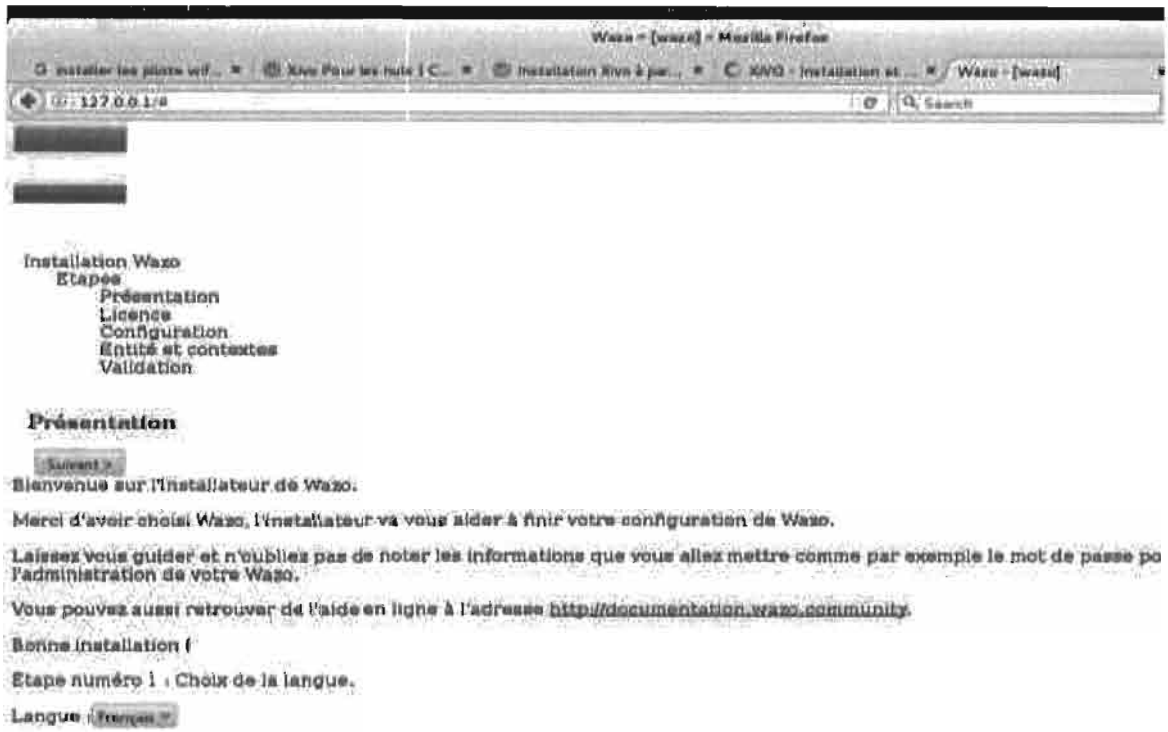

Figure VII.1 : écran d'accueil d'installation de Wazo

Etape configuration

Cette étape possède deux camps délicats : le mot de passe de l'administrateur et l'adresse IP de l'interface VoIP. L'administrateur serait amené à réinitialiser les configurations si toutefois il venait à oublier une de ces informations. La figure VII.2 nous présente le wizard de cette étape.

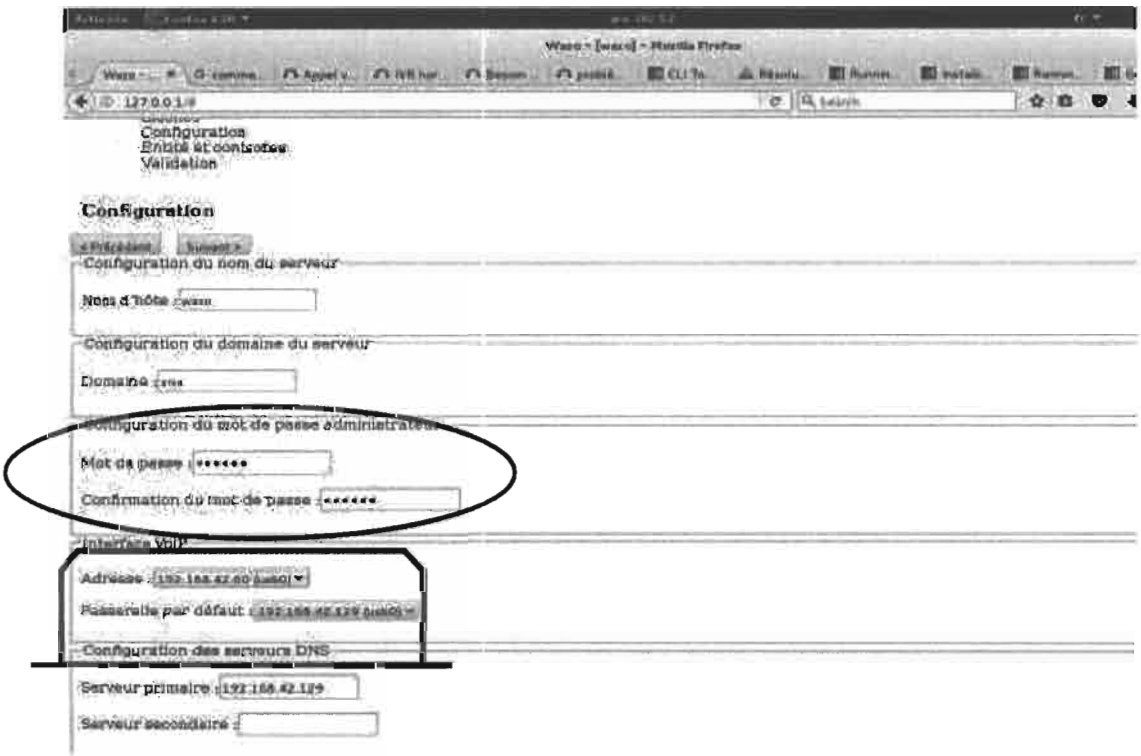

Figure VII.2 : étape configuration

Etape entité et contexte

Il s'agit ici, de donner un nom à notre téléphonie et de faire les premiers paramétrages de contexte des appels internes, entrant et sortant. Les appels internes sont les appels qui se déroulent exclusivement dans le réseau VoIP. Les appels entrant sont ceux d'un autre réseau vers la l'UPB(VoIP). Enfin, les appels sortant sont ceux quittant de notre réseau vers l'extérieur.

Pour cette étape, nous avons juste configuré le contexte des appels internes, par le renseignement de la plage de numérotation. Notre système prévoit gérer dix mille (10 000) utilisateurs. Donc nous avons opté de commencer la numérotation à 00101. La figure VII.3 nous permet de mieux appréhender cette partie.

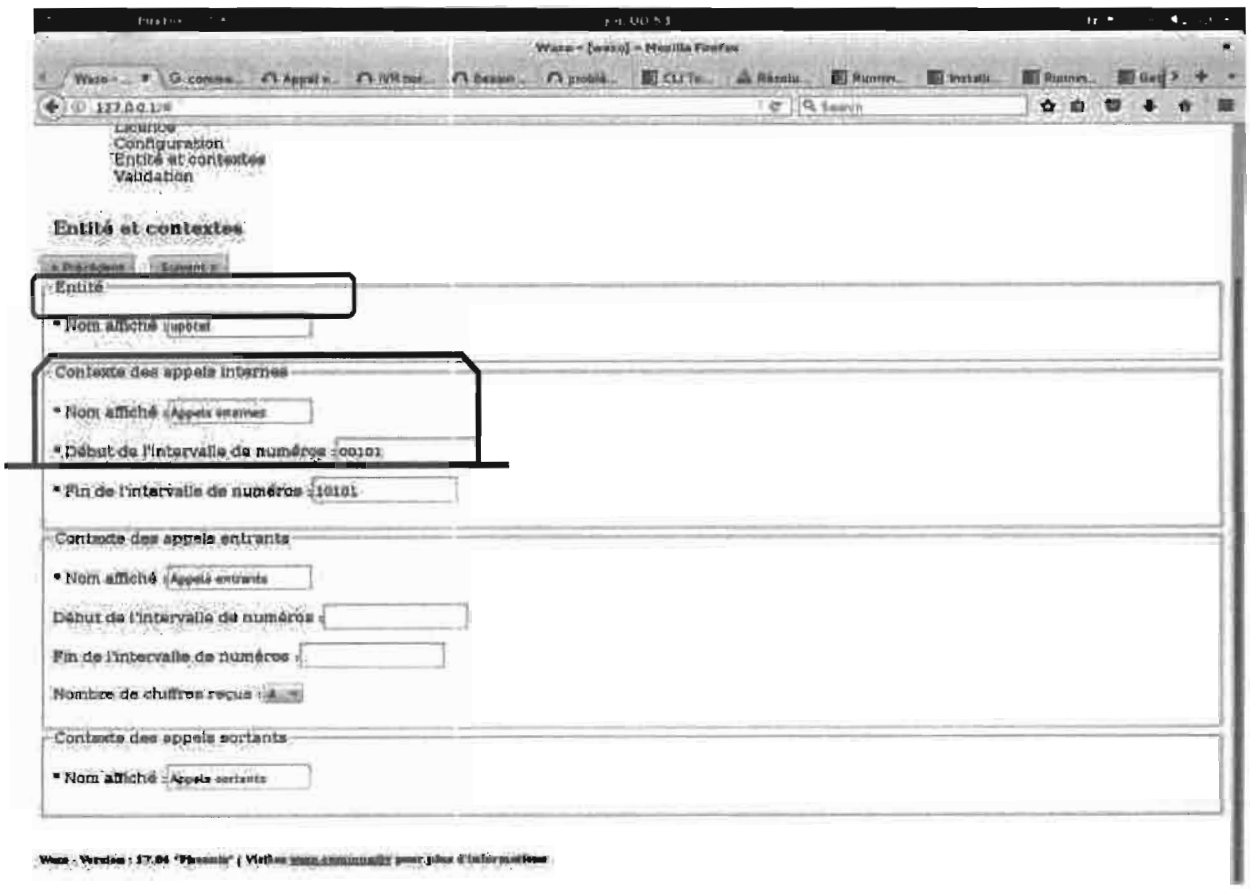

Figure VII.3 : étape entité et contextes

Etape validation

Cette étape permet à l'utilisateur de vérifier si toutes les informations renseignées sont correctes, en les lui affichant, comme nous le montre la figure VII.4 ; après quoi il pourra enfin terminer l'installation.

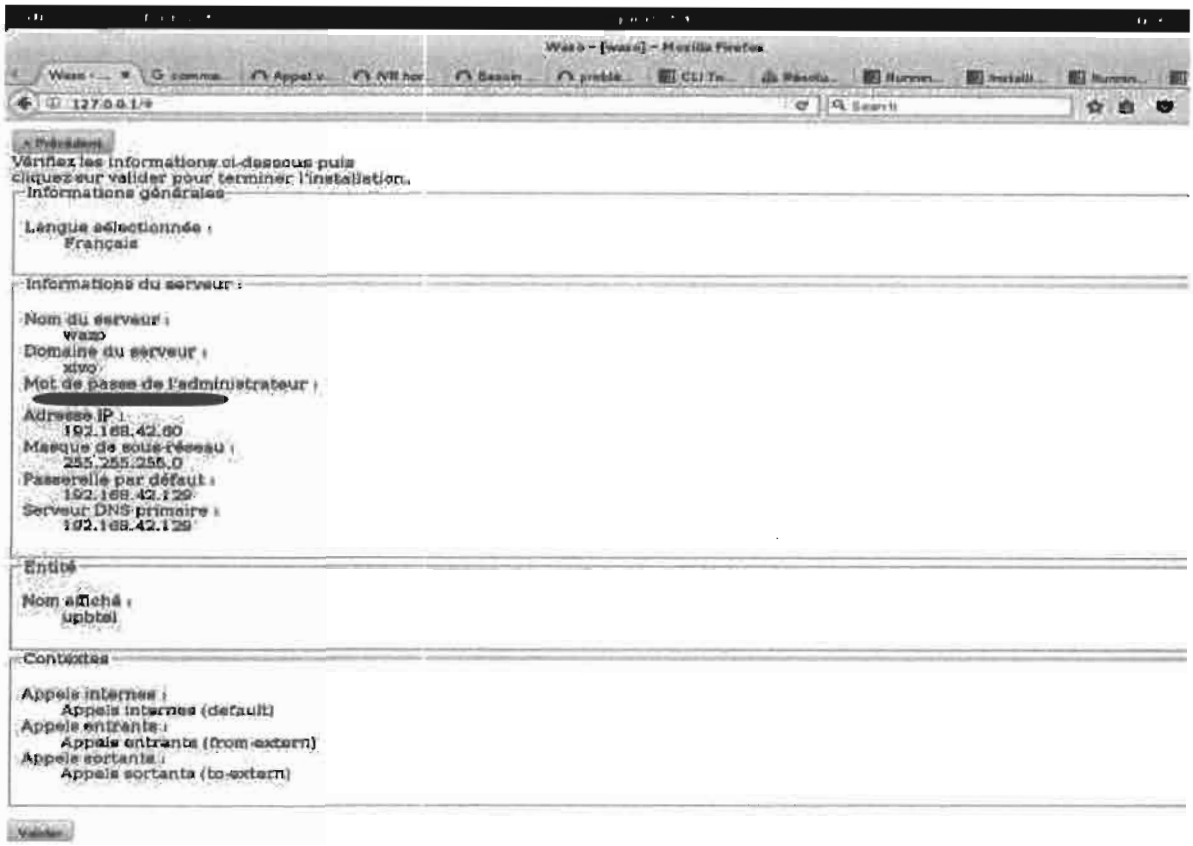

Figure VII.4 : Etape validation

Il faut noter que deux étapes n'ont pas été illustrées par des exemples. Il s'agit en effet de l'acceptation des conditions d'utilisations et du choix de la langue. Pour ce cas-ci, nous avons choisi l'anglais car tous les tutoriels sur les configurations sont en anglais.

Configuration de base pour permettre à deux téléphones de communiquer

Nous distinguons ici trois types d'appels :

Appels internes : affichage du nom de l'appelé

De manière générale, il est plus intéressant pour un utilisateur de voir afficher lors d'un appel interne, le nom de l'appelé que son numéro. La configuration de l'affichage du nom de l'appelé s'effectue dans les paramètres du protocole de signalisation (SIP). Deux modifications sont nécessaires. Il s'agit entre autre de :

- Trust the Remote-Party-ID: **yes**,
- Send the Remote-Party-ID: PAI

Annexe2 : formulaire d'enquête pour le personnel

UPB- ESI & DPNTIC

Ce questionnaire à pour objectif d'évaluer les coûts supportés par les acteurs de l'UPB et les difficultés rencontrées dans les communications téléphoniques, en vue d'étudier l'opportunité d'un nouveau système de communication.

1. **Quel poste occupez-vous ?**

2. **Quel problème rencontrez-vous dans les communications (appels téléphoniques) sur le site de Nasso ?**

Telmob	Orange	Télécel
☐ Perte fréquente de réseau	☐ Perte fréquente de réseau	☐ Perte fréquente de réseau
☐ Réseau totalement inaccessible	☐ Réseau totalement inaccessible	☐ Réseau totalement inaccessible
☐ Saturation fréquente du réseau	☐ Saturation fréquente du réseau	☐ Saturation fréquente du réseau
☐ Aucun problème de communication	☐ Aucun problème de communication	☐ Aucun problème de communication

3. **Combien dépensez-vous en moyenne par jour dans les appels téléphoniques (téléphones portables) pendant les heures de service pour joindre vos collègues ou collaborateurs?**

☐ Moins de 500fr ☐ Entre 500fr et 999fr ☐ Entre 1000fr et 1999fr

☐ Entre 2000fr et 4999fr ☐ Entre 5000fr et 10 000fr Plus d☐0 000fr

4. **Combien dépensez-vous en moyenne par jour dans les appels téléphoniques (téléphones portables) en dehors des heures de service pour joindre vos collègues ou collaborateurs?**

☐ Moins de 500fr ☐ Entre 500fr et 999fr ☐ Entre 1000fr et 1999fr

☐ Entre 2000fr et 4999fr ☐ Entre 5000fr et 10 000fr ☐ Plus de 10 000fr

5. **Combien d'appels passez-vous en moyenne par jour pendant les heures de service, entre collègues ou collaborateurs avec le téléphone portable?**

☐ Entre 0 et 5 ☐ Entre 6 et 10 ☐ Entre 11 et 20 ☐ Plus de 20

6. **Combien de temps dure en moyenne chaque appel (juste une estimation) ?**

☐ Moins d'une minute ☐ entre une et deux minutes

☐ Entre 03 et 05 minutes ☐ plus de 05 minutes

7. **Utilisez-vous la téléphonie IP mise en place par la DPNTIC ?**

☐ Oui ☐ Non

8. **Combien d'appels passez-vous en moyenne par jour pendant les heures de service, entre collègues ou collaborateurs avec cette téléphonie IP?**

☐ Entre 0 et 5 ☐ Entre 6 et 10 ☐ Entre 11 et 20 ☐ Plus de 20

9. **Combien de temps dure en moyenne chaque appel avec cette téléphonie IP ?**

☐ Entre 01 et 05 minutes ☐ entre 05 et 10 minutes ☐ plus de 10 minutes

10. Quel est votre niveau de satisfaction dans l'usage de cette téléphonie IP (si vous en avez) ?

☐ Pas satisfaisant ☐ Peu satisfaisant ☐ Satisfaisant

☐ Légèrement satisfaisant ☐ Très satisfaisant

11. Que diriez-vous s'il y avait un système vous permettant de communiquer avec toute autre personne (personnel & étudiant) sur n'importe lequel des sites de l'UPB sans frais ?

☐ Excellent ☐ acceptable ☐ nul

12. Avez-vous un :

☐ Ordinateur ? ☐ Smartphone (Android, IPhone, tablette)?

Annexe3 : formulaire d'enquête pour les étudiants

Questionnaire

Ce questionnaire à pour objectif d'évaluer les coûts supportés par les acteurs de l'UPB et les difficultés rencontrées dans les communications téléphoniques, en vue d'étudier l'opportunité d'un nouveau système de communication.

1. Dans quelle filière étudiez-vous ?

2. Quelle responsabilité avez-vous à l'UPB ?

☐ Délégué de classe ☐ membre d'une association /mouvement ☐ aucune

3. Quel problème rencontrez-vous dans les communications (appels téléphoniques) sur le site de Nasso ?

Telmob	Orange	Télécel
☐ Perte fréquente de réseau	☐ Perte fréquente de réseau	☐ Perte fréquente de réseau
☐ Réseau totalement inaccessible	☐ Réseau totalement inaccessible	☐ Réseau totalement inaccessible
☐ Saturation fréquente du réseau	☐ Saturation fréquente du réseau	☐ Saturation fréquente du réseau
☐ Aucun problème de communication	☐ Aucun problème de communication	☐ Aucun problème de communication

4. Combien de temps dure en moyenne chaque appel (juste une estimation) ?

☐ Moins d'une minute ☐ entre une et deux minutes

☐ Entre 03 et 05 minutes ☐ plus de 05 minutes

5. Combien dépensez-vous en moyenne par jour dans les appels téléphoniques (téléphones portables) sur le campus pour joindre vos camarades et/ou l'administration qui sont aussi sur le campus? (*Cette question est destinée aux étudiants de l'UPB*)

☐ Moins de 500fr ☐ Entre 500fr et 999fr ☐ Entre 1000fr et 1999fr

6. **Combien de d'appels passez-vous en moyenne par jour sur le campus, entre étudiants et/ou l'administration avec le téléphone portable?**

☐Entre 0 et 5 ☐ Entre 6 et 10 ☐Entre 11 et 20 ☐Plus de 20

7. **Combien de SMS passez-vous en moyenne par jour sur le campus, entre étudiants avec votre téléphone portable?**

☐Entre 0 et 5 ☐ Entre 6 et 10 ☐Entre 11 et 20 ☐Plus de 20

8. **Que diriez-vous s'il y avait un système vous permettant de communiquer avec toute autre personne (personnel & étudiant) sur n'importe lequel des sites de l'UPB sans frais ?**

☐Excellent ☐acceptable ☐nul

9. **Avez-vous un :**

☐Ordinateur ? ☐ Smartphone (Android, IPhone, tablette, BlackBerry)?