

Université de Maroua  
\*\*\*\*\*  
Institut Supérieur du Sahel  
\*\*\*\*\*  
Département d'Informatique  
et des Télécommunications  
\*\*\*\*\*



The University of Maroua  
\*\*\*\*\*  
The Higher Institute of the Sahel  
\*\*\*\*\*  
Department of Computer Science  
and Telecommunications  
\*\*\*\*\*

## INFORMATIQUE ET TELECOMMUNICATIONS

# DÉPLOIEMENT ET EXPANSION D'UN RÉSEAU WIFI POUR LA VISIOCONFÉRENCE MULTIPLE: CAS DE PASTEL TELECOMS

Mémoire présenté et soutenu en vue de l'obtention du Diplôme  
D'INGENIEUR DE CONCEPTION EN INFORMATIQUE OPTION RESEAUX

Par

**WONYOU MINKA PIERRE DIEUDONNE**

*Ingénieur de Travaux en Sécurité et Administration Réseaux*

Matricule: 12X361S

Sous la Direction de

**Prof. MOTAPON OUSMANOU**

Maître de conférences

Devant le jury composé de:

**Président: Prof. MOHAMADOU HALIDOU**

**Rapporteur: Prof. MOTAPON OUSMANOU**

**Examineur: Prof. EMVUDOU WONO YVES**

**Invité: M. AGBANOU GERARD**

**Année Académique 2014 / 2015**

## ÉPIGRAPHE

«D'abord ils vous ignorent, ensuite ils se moquent de vous, puis ils vous combattent, puis vous gagnez....»

Mahatma Gandhi

## **DEDICACE**

A Mes parents

## REMERCIEMENTS

Seuls mon courage et ma volonté n'auraient jamais suffi pour arriver au bout de ce travail. C'est pourquoi, je tiens à adresser un grand remerciement à tous ceux qui de près ou de loin m'ont assisté dans la rédaction de ce mémoire.

Tout particulièrement je voudrais remercier:

- Le président du jury: Prof. MOHAMADOU HALIDOU
- L'examineur: Prof. EMVUDO WONO YVES
- L'encadreur: Prof. MOTAPON OUSMANOU
- Le corps enseignant de l'institut supérieur du sahel, en particulier:
  - Le Chef de Département d'informatique et des télécommunications: Le Dr Olivier VIDEME BOSSOU, et les enseignants du département d'informatique et des Télécommunications pour toutes les connaissances qu'ils m'ont transmis durant ma formation.
  - Le Directeur Général de PASTEL SA de Douala monsieur Jean Louis DJOB et tout son personnel pour la confiance qu'ils m'ont accordée durant tout mon stage.
  - Mon encadreur professionnel: M. AGBANOU GERARD pour ses conseils, ses remarques et à la réalisation de ce travail.
  - A toute la grande famille MINKA, particulièrement à Monsieur et Madame MINKA, MINKA Sylvie, MINKA Ruth, NYECMECK MINKA Christine, le Prof BASSOM Roger pour leur contribution morale, matérielle et financière durant ma formation.
  - Mes cousins et cousines MASSOGUE Joseph, NJEMB Vieux, Ngo MOMNOUGUI Pélagie, pour tout le soutien qu'ils m'ont apportés durant ma période de stage.
  - Mes amis FEWOU Arouna, SAP Serge, HEU Hiasynte, DJEUNOU Donna, KEPSEU Jaspers, ASSAMBOU, ANGO Jean, MUNTHO Christelle, EMBOLO LOBE Carine, MANG-EGRE, TAPÉ Calvin, SAMPA pour toute aide financière et morale qu'ils ont pu m'apporter.
  - Tous ceux qui, de près ou de loin ont contribué à mon éducation, qu'ils reçoivent ici l'expression de ma profonde gratitude.

# TABLE DES MATIERES

ÉPIGRAPHE .....	I
DEDICACE .....	II
REMERCIEMENTS.....	III
RESUME.....	VII
ABSTRACT .....	VIII
LISTE DES TABLEAUX.....	IX
LISTE DES FIGURES .....	X
GLOSSAIRE.....	XII
INTRODUCTION GENERALE .....	1
CHAPITRE 1: CONTEXTE ET PROBLEMATIQUE .....	3
1.1 PRESENTATION DE L'ENTREPRISE .....	3
1.1.1 Historique .....	3
1.1.2 Technologie.....	3
1.1.3 Présentation du Service technique .....	3
1.1.4 Organigramme de l'entreprise .....	4
1.2 CONTEXTE .....	5
1.3 PROBLEMATIQUE .....	5
1.4 METHODOLOGIE .....	5
1.5 OBJECTIFS A ATTEINDRE .....	6
CHAPITRE 2: GÉNÉRALITÉ SUR LE WIFI .....	7
INTRODUCTION.....	7
2.1 DEFINITION ET PRESENTATION.....	7
2.1.1 Usages du wifi.....	7
2.1.2 Avantages du wifi en particulier et du sans fil en générale.....	8
2.1.3 Normes du réseau wifi.....	8
2.1.4 Architectures du réseau wifi.....	9
2.1.5 Topologie des réseaux wifi .....	10
2.1.5.1 Les réseaux ad hoc .....	10
2.1.5.2 LES RESEAUX MESH.....	10
2.2 COUCHES ET ROLES DU RESEAU WIFI .....	11
2.3 TECHNIQUES D'ETALEMENT ET DE MODULATION .....	12

2.3.1 FHSS ( <i>Frequency Hopping Spread Spectrum</i> ) .....	12
2.3.2 DSSS ( <i>Direct Sequence Spread Spectrum</i> ) .....	13
2.3.3 La modulation OFDM .....	13
2.4 LES ATTAQUES D'UN RESEAU WIFI .....	16
2.4.2 L'intrusion .....	17
2.4.3 Le déni de service ( <i>dos: denial of service</i> ).....	17
2.5 LES TECHNIQUES DE SECURITE DU WIFI .....	18
2.5.1 Le cryptage WEP .....	19
2.5.2 Le cryptage WPA .....	20
2.5.3 Le cryptage 802.11i (WPA2).....	20
2.5.4 Les VLAN.....	21
2.5.5 Protocole VPN .....	22
CONCLUSION.....	22
<b>CHAPITRE 3: DÉPLOIEMENT ET EXPANSION DU RESEAU WIFI .....</b>	<b>23</b>
INTRODUCTION.....	23
3.1 DIMENSIONNEMENT DES EQUIPEMENTS .....	23
3.1.1 Les matériels d'interconnexion et leurs caractéristiques .....	23
3.1.1.1 Le point d'accès .....	23
3.1.1.2 Les routeurs .....	24
3.1.1.3 Choix de l'antenne .....	24
3.1.2.1 Simulateur Netstumbler .....	28
3.1.2.2 Simulateurs professionnels .....	28
3.1.3 Le choix de la bande de fréquences .....	30
3.1.4 Le choix et rôle des modèles de propagation .....	30
3.1.4.1 Modèle D'Okumura- Hata .....	31
3.1.4.2 Modèle COST 231 Hata.....	31
3.1.4.3 Le modèle de propagation en espace libre.....	32
3.1.5 Le bilan de liaison.....	33
3.2 DIMENSIONNEMENT EN CAPACITE .....	34
3.2.1 Détermination de la portée d'un AP .....	35
3.2.2 Détermination du trafic par abonné .....	36
3.3 LA MISE EN ŒUVRE DU WIFI .....	37
3.3.1 Déploiement des sites.....	37
3.4 EXPANSION DU RESEAU WIFI .....	41
3.4.1 L'étude de l'environnement .....	42
3.4.1.1 Le dégagement minimal.....	42
3.4.1.2 La hauteur minimale.....	43
3.4.2 Les perturbations radio.....	44

3.4.2.1 L'absorption et la réflexion .....	44
3.4.2.2 La diffraction.....	45
CONCLUSION.....	47
<b>CHAPITRE 4: MISE EN PLACE D'UNE PLATEFORME DE VISIOCONFERENCE MULTIPLE .....</b>	<b>48</b>
INTRODUCTION.....	48
4.1.1 Définition .....	48
4.1.2 Fonctionnement.....	48
4.1.3 Différents modes de transmission en visioconférence.....	49
4.1.3.1 Mode de visioconférence sur IP .....	50
4.1.4 Les protocoles et les codecs de fonctionnement de la visioconférence .....	50
4.1.4.1 Le Protocole H.323 .....	50
4.1.4.2 Protocole SIP .....	54
4.2 PROTOCOLES DE TRANSPORT .....	57
4.2.1 Protocole RTP.....	57
4.2.2 Protocole RTCP .....	58
4.3 LES CODECS.....	59
4.3.1 Codecs audio.....	59
4.3.2 Codecs vidéo.....	59
4.4 ÉQUIPEMENTS DE LA VISIOCONFERENCE .....	60
4.5 INSERTION DE LA VISIOCONFERENCE AU RESEAU WIFI.....	60
4.5.1 Étude d'astérisik de trixbox.....	61
4.5.2 Présentation de BigBluebutton .....	61
4.5.2.1 Fonctionnalités de bigbluebutton.....	62
4.5.2.2 Composants de bigbluebutton .....	63
CONCLUSION.....	63
<b>CHAPITRE 5: RESULTATS ET COMMENTAIRES .....</b>	<b>65</b>
INTRODUCTION.....	65
5.1. INSTALLATION DE BIGBLUEBUTTON.....	65
5.2 INSTALLATION DETAILLE DES MODULES DE BIGBLUEBUTTON .....	65
5.3 MISE A JOUR DES PACKAGES ET INSTALLATION DES COMPOSANTS DE BIGBLUEBUTTON.....	66
CONCLUSION.....	70
BIBLIOGRAPHIE.....	72
ANNEXES .....	A

## RESUME

Le présent travail effectué en entreprise porte sur le déploiement et l'expansion d'un réseau wifi pour la visioconférence multiple. Cette entreprise étant installée sur deux sites à DOUALA, cette solution permet aux personnels des deux sites (la direction technique et la direction générale) de maintenir la communication sans se déplacer, et aussi de voir son interlocuteur comme s'il était en face. Le déploiement du réseau wifi au sein du site technique, nous a permis de ressortir le type de matériels, le modèle de propagation, le choix de la bande de fréquence, le bilan de liaison, la capacité et la portée d'un accès point. Ensuite l'insertion de la visioconférence pour pallier la difficulté des techniciens à se regrouper pour les réunions; nous a permis de greffer sur notre serveur des modules libres open source comme: asterisk, tomcat6, red5, Mysql, nginx, bigbluebutton. Enfin, l'usage du serveur de visioconférence sur notre réseau wifi, a permis les communications en temps réel entre les techniciens et l'administration, l'exécution des tâches qui se fait désormais sans perte de temps produisant ainsi les gains à l'entreprise. Ceci étant face à la rentabilité et à l'efficacité de ses solutions, nos résultats à savoir: l'accès à internet, les appels en VOIP, le chat, le partage de bureau ont pu franchir la phase de tests et nous attendons à présent qu'une autorisation et des améliorations pour un usage à but commercial.

**Mots-clés:** WIFI, portée, capacité, fréquence, propagation, bilan de liaison, visioconférence, SIP, H323, VOIP, bigbluebutton. Asterisk, tomcat6, red5, mysql, nginx.



## **ABSTRACT**

This work focuses on enterprise deployment and expansion of a wireless network for multiple video conferencing. This company is installed at two sites in DOUALA; this solution allows staff at both sites (technical leadership and overall direction) to maintain communication without moving, and also to see the speaker as if he were in front. The deployment of the wireless network in the Technical site, has allowed us to highlight the type of materials, the propagation model, the choice of the frequency band, the link budget, capacity and range of a hotspot. Then the insertion of video conferencing to overcome the difficulty of technicians to come together for meetings; allowed us to piggyback on our server free open source modules such as: asterisk, tomcat6, red5, Mysql, nginx, BigBlueButton. Finally, the use of videoconferencing server on our wireless network enabled real-time communication between technicians and administration, the performance of the tasks now done without wasting time producing gains in business. Having faced the profitability and efficiency of its solutions, our results are: internet access, VOIP calls, chats, desktop sharing could cross the testing phase and we expect this that authorization and improvements for Commercial profit use.

Keywords: wireless, range, capacitance, frequency, propagation, link budget, conferencing, SIP, H323, VOIP, BigBlueButton. Asterisk, tomcat6, red5, mysql, nginx

## **LISTE DES TABLEAUX**

TABLEAU 1: QUELQUES NORMES WIFI [2].....	9
TABLEAU 2: CARACTERISTIQUES DES STANDARDS DE SECURITE Wi-Fi [5] .....	21
TABLEAU 3: BILAN DE LIAISON DU DEPLOIEMENT DU WIFI .....	34
TABLEAU 4: LES PRINCIPAUX CODECS [2] .....	60

# LISTE DES FIGURES

FIGURE 1: ARCHITECTURE D'UN RESEAU WIFI [1] .....	10
FIGURE 2: TOPOLOGIE AD HOC [1].....	10
FIGURE 3: TOPOLOGIE EN INFRASTRUCTURE [1].....	11
FIGURE 4: COUCHES WIFI [8].....	12
FIGURE 5: PROBLEME DE LA STATION CACHEE [2].....	14
FIGURE 6: METHODE D'ACCES AU SUPPORT [2].....	15
FIGURE 7: ILLUSTRATION DE LA FRAGMENTATION [1].....	15
FIGURE 8: REPRESENTATION DES INTERFERENCES ENTRE LES AP [3].....	16
FIGURE 9: CONNEXION DE DEUX SITES A TUNNEL VPN [5] .....	22
FIGURE 10: LE POINT D'ACCES [3].....	24
FIGURE 11: ROUTEUR D-LINK [3] .....	24
FIGURE 12: ANTENNE OMNIDIRECTIONNELLE [7] .....	25
FIGURE 13: ANTENNE SECTORIELLE [7] .....	25
FIGURE 14: ANTENNE DIRECTIONNELLE DE TYPE YAGI [7] .....	26
FIGURE 15: DIAGRAMME DE RAYONNEMENT [3] .....	27
FIGURE 16: POLARISATION DE L'ANTENNE DE L'EMETTEUR ET DU RECEPTEUR [3] .....	27
FIGURE 17: INFORMATIONS SUR LES DIFFERENTS AP .....	29
FIGURE 18: RAPPORT SUR LA QUALITE DU SIGNAL SUR LE BRUIT D'UN AP. ....	30
FIGURE19: DEBIT THEORIQUE MAXIMAL DU SIGNAL EN FONCTION DE LA PORTEE [3] .....	35
FIGURE 20: ARCHITECTURE DU SITE D'AKWA .....	38
FIGURE 21: CHOIX DES FREQUENCES ET DES CANAUX.....	38
FIGURE 22: ENTREE DES PARAMETRES DES AP .....	39
FIGURE 23: TEST DE CONNECTIVITE .....	39
FIGURE 24: ARCHITECTURE DU SITE DE BALI.....	40
FIGURE 25: ENTREE DES PARAMETRES D'AP.....	40
FIGURE 26: TEST DE CONNECTIVITE .....	41
FIGURE 27: SYNOPTIQUE SUR L'EXPANSION DU RESEAU WIFI.....	42
FIGURE 28 : ELLIPSOÏDE DE FRESNEL ET LE DEGAGEMENT MINIMAL [3] .....	43
FIGURE 29: LA HAUTEUR MINIMALE POUR UNE CONNEXION DE POINT A POINT [3].....	44
FIGURE 30: ABSORPTION ET REFLEXION [1] .....	45
FIGURE 31: LA DIFFRACTION [1] .....	46

FIGURE 32: ARCHITECTURE GLOBALE DE L'EXPANSION DU RESEAU WIFI.....	46
FIGURE 33: DIFFERENTES NORMES DU PROTOCOLE H323 [2].....	54
FIGURE 34: ARCHITECTURE POINT A POINT (ASTERISK) [19].....	62
FIGURE 35: ARCHITECTURE POINT A MULTIPOINT (BIGBLUEBUTTON)[19].....	63
FIGURE 36: ECRAN D'ACCUEIL DU SERVEUR .....	66
FIGURE 37: ECRAN DU SERVEUR APRES REDEMARRAGE DES SERVICES.....	68
FIGURE 38: TEST DE FONCTIONNEMENT DU SERVEUR.....	68
FIGURE 39: INTERFACE DU SERVEUR BIGBLUEBUTTON.....	69
FIGURE 40: FONCTIONNALITES DU BIGBLUEBUTTON .....	69

## **GLOSSAIRE**

**AP:** Access point

**AES:** Advanced Encryptions Standard

**BSS:** Basic Service Set

**BSSID:** Basic Service Set Identify

**CSMA/CA:** Carrier Send Multiple Access with Collision Avoidance

**CTS:** Clear to send

**DCF:** Distribution Coordination Function

**DMT:** Discrète Multitone Modulation

**DS:** Distribution System

**DSL:** Digital Subscriber Line

**DSSS:** direct sequence spread spectrum

**ESS:** Extended Service Set

**ESSID:** Extended Service Set Identify

**FHSS:** frequency hopping spread spectrum

**IAX:** Inter-Asterisk Exchange

**IEEE:** institute of Electrical and Electronics Engineers

**IETF:** Institute Engineers Task Force

**IP:** internet protocol

**IPBX:** internet protocol private exchange

**ITU:** International Telecommunication Union

**LLC:** Logical Link Control

**LOS:** Line of Sight

**MAC:** Medium Access Control

**MCU:** Multipoint Control Units

**NAV:** Network Allocation Vector

**OFDM:** Orthogonal Frequency Division Multiplexing

**PABX:** private automatic branch exchange

**PLCP:** Physical Layer Convergence Protocol

**PMD:** Physical Medium Dependent

**PSTN:** Public Switched Telephone Network

**QOS:** Quality of Service  
**RFC:** Requests for Comment  
**RNIS:** Réseau Numérique à Intégration de Service  
**RTC:** Réseau Téléphonique de Commuté  
**RTCP:** Real-time Transport Control Protocol  
**RTP:** Real-Time Transport Protocol  
**RTS:** Request to send  
**SDP:** Session Description Protocol  
**SIP:** Session Initiation Protocol  
**SRTP:** Secure Real-time Transport Protocol  
**SSID:** service set identifier  
**TCP:** Transport Control Protocol  
**TDM:** Time Division Multiplexing  
**TKIP:** Temporal Key Integrity Protocol  
**TLS:** Transport Layer Security  
**UAC:** User Agent Client  
**UAS:** User Agent Server  
**UDP:** User Datagram Protocol  
**URL:** Uniform Resource Locator  
**VLAN:** Virtual Local Area Network  
**VPN:** virtual private network  
**WAN:** World Area Network  
**WDS:** wireless distributed system  
**WEP:** wired equipment privacy  
**WIFI:** Wireless Fidelity  
**WLAN:** wireless local area network  
**WMAN:** Wireless Metropolitan area network  
**WPA:** Wi-Fi protected access  
**WPAN:** wireless personal area network  
**WWAN:** wireless wide area network

## INTRODUCTION GENERALE

Les réseaux sans fil sont en plein développement du fait de la flexibilité de leur interface, qui permet à un utilisateur de changer de place tout en restant connecté. Les communications entre équipements terminaux peuvent s'effectuer directement ou par le biais de stations de base, appelées points d'accès, ou AP (Access Point). Les communications entre points d'accès peuvent être hertziennes ou par câble. Les débits de ces réseaux se comptent en dizaines de mégabits par seconde. Dans le souci de maintenir la communication tout en étant mobile, plusieurs Ingénieurs ont mené les études sur ce domaine à savoir: Michel Duchâteau [11] sur l'analyse et simulation d'un réseau sans fil. Arnaud Dupont FOTSO [13] sur la mise en place d'un réseau wifi avec authentification basé sur les certificats. Kwaté Kwaté Rodrigue [12] sur le déploiement d'un réseau wifi longue portée avec une plateforme de TOIP. Mais les travaux menés par ces Ingénieurs quoique très pertinents sur le maintien de la mobilité, et de la téléphonie, ne s'intéressent pas à la possibilité de voir son interlocuteur en temps réel comme s'il était en face. D'où l'objet de notre étude sur le thème: Déploiement et Expansion d'un réseau wifi pour la visioconférence multiple.

La visioconférence consiste à s'entretenir avec une ou plusieurs personnes au même moment en utilisant des terminaux. Elle doit être conforme aux normes internationales telles que SIP, H.323 et utilise des codecs comme G722, H 623. Ceci étant PASTEL TELECOMS ne disposant pas d'un système de visioconférence, nous avons travaillé sur la mise en œuvre d'un tel système afin de permettre à cette société de pouvoir offrir ce service aux entreprises clientes.

Le besoin d'interconnecter les deux sites de l'entreprise tout en permettant aux techniciens de participer aux réunions sans contrainte de temps, nous a concédé de déployer et d'étendre le réseau wifi en suivant un certain nombre d'étapes à savoir: le choix de matériels, du modèle de propagation, de la bande de fréquence, le bilan de liaison, la capacité et la portée d'un point d'accès. Ensuite l'insertion de la visioconférence, nous a permis d'implémenter un serveur, auquel nous avons inséré les modules à savoir: asterisk, tomcat6, red5, mysql, nginx, bigblubutton. A la fin de notre

travail, nous avons effectué des tests dont les résultats ont été acceptés par l'encadrement technique de PASTEL. Ces résultats nous ont permis d'effectuer la téléphonie, le chat, le partage du bureau, etc.

Dès lors le présent mémoire s'étend sur cinq chapitres.

Le premier chapitre présente l'entreprise dans laquelle nous avons passé cinq mois de stage. Détaille le contexte dans lequel nous avons travaillé et ressort les motivations qui nous ont poussées à choisir le thème de notre mémoire.

Le deuxième chapitre introduit le réseau wifi et ses variantes, décrit et explique son architecture et son fonctionnement. Les différents types de modulation et les techniques de sécurité.

Le troisième chapitre s'intéresse au déploiement du réseau wifi qui va nous permettre de faire l'audit du site, le choix du matériel, le dimensionnement des équipements, la simulation avec un outil de planification, le dimensionnement en capacité. Cette partie nous permet également de faire l'extension de notre réseau wifi.

Le quatrième chapitre, s'intéresse à la mise en place d'une plateforme de visioconférence multiple, les protocoles de transport, leurs avantages et leurs inconvénients, les codecs pour la voix et la vidéo.

Le cinq chapitres, présente et commente la procédure d'installation de la visioconférence, la configuration des clients, et le texte de communication entre plusieurs interlocuteurs.



# **CHAPITRE 1: CONTEXTE ET PROBLEMATIQUE**

## **1.1 Présentation de l'entreprise**

La connaissance d'une entreprise nécessite une bonne vue d'ensemble de sa situation actuelle et de son passé en prenant en considération l'environnement interne et externe dans lequel elle évolue. Nous verrons dans cette partie l'historique de l'entreprise, la technologie et son identification.

### **1.1.1 Historique**

PASTEL S.A. a été créé en 1996, après la loi du 26 juillet 1996 libéralisant le secteur des télécommunications. Elle installe sa base de Douala en 1998, mais les activités ne pourront démarrer qu'en 2004. PASTEL S.A. offre au grand public le service téléphonique avec vitesse de (64 kbps), et le service internet avec un débit de transmission des données de (256kbps).

### **1.1.2 Technologie**

PASTEL S.A. a implémenté au Cameroun une technique permettant le transfert de la voix à travers le réseau IP connu sous l'acronyme VOIP (Voice Over Internet Protocole) cette technique permet lors de l'émission d'un appel, de numériser la voix puis de la découper en paquets IP qui seront dans le réseau local ou internet afin d'être transmis au destinataire. Le but est de permettre la transmission des flux de voix, données et images au sein d'un même réseau avec une qualité de service optimale. PASTEL S.A. peut ainsi fournir à sa clientèle des services téléphoniques à moindre coût.

### **1.1.3 Présentation du Service technique**

La Base PASTEL est en réalité la direction ou le service technique de PASTEL S.A. situé à Bali, elle est gérée par un responsable technique avec pour mission de:

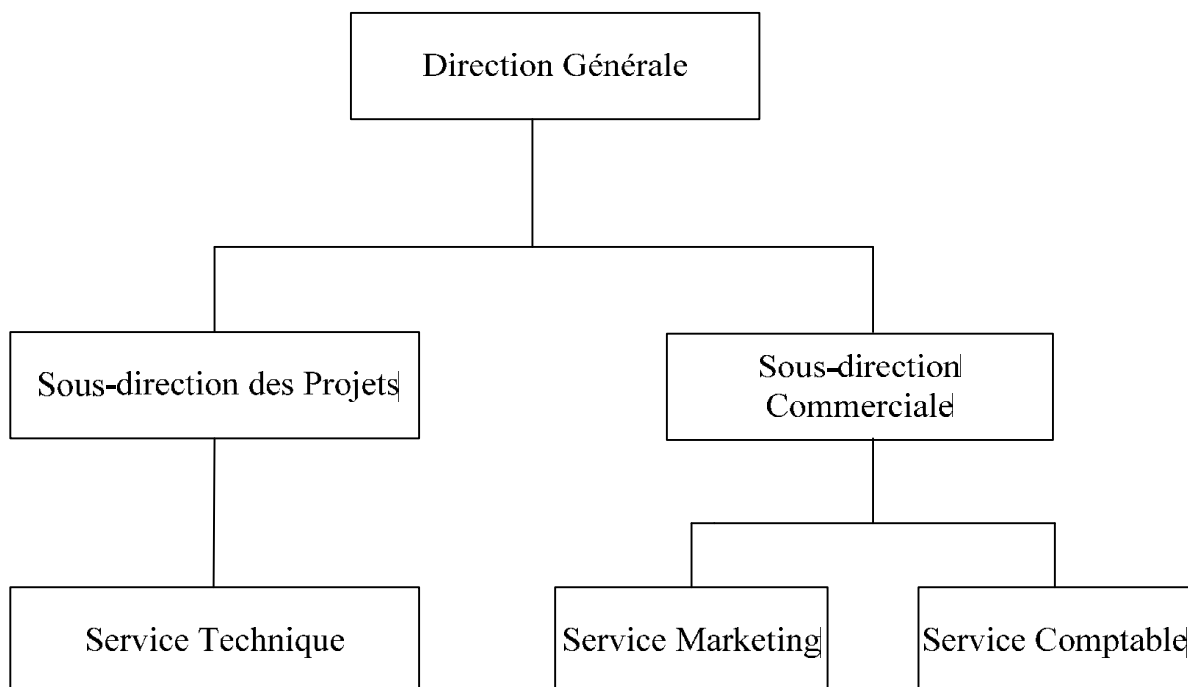
- Veiller au bon fonctionnement des équipements et d'assurer leur pérennité;
- Etudier et prévoir les moyens de production technique;
- Proposer les investissements nécessaires au développement ou à l'amélioration de la qualité de la communication;

Optimiser les moyens de production déjà mis en place;  
Veiller à la bonne qualité des services offerts sur la radio;  
Assurer une technologie et un avantage concurrentiel sur la radio.

Pour la réalisation de ce travail PASTEL s'est entouré d'ingénieurs, de techniciens qui s'attachent jour après jour à satisfaire sa clientèle. Les activités de la base PASTEL S.A, sont réalisées grâce à la compétence et au dévouement du personnel technique.

#### 1.1.4 Organigramme de l'entreprise

L'entreprise PASTEL Télécom est une structure qui s'échelonne de manière suivante:



La Direction Générale: qui se charge d'administrer les sous-directions de projets et commerciale en vue de s'assurer de leur bon fonctionnement.

La Sous-Direction des Projets: gère en son sein les services techniques dont la tâche est de réaliser les travaux de l'entreprise.

La Sous-Direction Commerciale: gère en son sein deux services à savoir le service marketing et le service comptable en vue de s'assurer de la bonne marche des opérations marketing et comptable.

## **1.2 Contexte**

La société PASTEL, dans le souci d'évoluer, s'est dotée un nouveau bâtiment destiné aux techniciens. Mais le bâtiment n'ayant pas de service internet, cela va entraîner les retards dans la découverte des mails, et aussi dans l'exécution des tâches. La fréquence des réunions n'étant pas négligeable, cela cre une contrainte absolue de temps et mobilise tout le monde.

## **1.3 Problématique**

Face à ces deux situations à savoir: l'indisponibilité du service internet et la difficulté à tenir les réunions, il en découle donc la problématique suivante:

Comment relier la direction technique et la direction générale afin qu'ils puissent accéder à internet?

Quelle disposition mettre sur pied pour faciliter les réunions sans que les techniciens se déplacent?

## **1.4 Méthodologie**

Pour résoudre les problèmes posés ci-dessus, nous allons procéder par quelques étapes:

❖ Le déploiement du réseau wifi au sein du bâtiment technique nécessite:

- ✓ L'audit des sites
- ✓ Etude et dimensionnement des équipements
- ✓ Choix de la bande de fréquence
- ✓ Choix du type de propagation
- ✓ Outil de simulation pour la planification
- ✓ Dimensionnement en capacité
- ✓ Taux de trafic par abonné
- ✓ Capacité d'abonnés par cellule

❖ L'expansion du réseau wifi entre nos deux sites nécessite:

- ✓ Une étude de l'environnement
- ✓ Une étude des perturbations radio

❖ En fin la mise en place d'une plateforme de visioconférence nécessite:

- ✓ Une installation et une configuration de l'IPBX

✓ Une installation des caméras IP.

### **1.5 Objectifs à atteindre**

Durant notre période de stage à PASTEL, les objectifs dont nous étions fixés sont les suivants:

📌 Déployer un réseau wifi pour avoir le service internet.

📌 Extension de notre réseau wifi entre nos sites.

📌 Usage de la visioconférence appliquée à notre réseau wifi pour permettre une communication vidéo/audio en temps réel, tout en éviter les contraintes de temps lors des réunions.

En sommes, cette partie nous a permis de connaître au mieux le cadre de travail dans lequel nous avons évolué pendant plus de cinq mois, de ressortir la problématique à laquelle l'entreprise fait face et d'essayer de la résoudre. La résolution des difficultés rencontrées, nous ont permis d'étudier en particulier le réseau wifi avant toute implémentation.

## **Chapitre 2: GÉNÉRALITÉ SUR LE WIFI**

### **Introduction**

Nous entendons par réseau sans fils un réseau ou au moins deux terminaux se connectent et communiquent entre eux par voie hertzienne directement ou indirectement. Les technologies des réseaux sans fils peuvent être classées en quatre types: Les WPAN (Wireless Personal Area Network), les WMAN (Wireless Metropolitan Area Network), les WWAN (Wireless Wide Area Network) et enfin les WLAN (Wireless Local Area Network) [2] qui constitueront le point culminant de notre étude dans ce chapitre.

### **2.1 Définition et Présentation**

Wifi est le nom courant pour Wireless Fidelity, et correspond à la norme IEEE 802.11. Cette norme de réseau informatique sans fil a été définie par le consortium IEEE (Institut of Electrical and Electronics Engineers) en 1999. Le nom “Wifi” est une marque déposée par le wireless Ethernet Compatibility Alliance. [2]

Le LAN sans fil (WLAN) est un système de transmission des données conçu pour assurer une liaison indépendante de l’emplacement des périphériques informatiques qui composent le réseau et utilisant les ondes radio plutôt qu’une infrastructure câblée. Dans l’entreprise, les LAN sans fil sont généralement implémentés comme le lien final entre le réseau câblé existant et un groupe d’ordinateurs clients (réseaux internes). Mais avec les prouesses de la technologie Wifi, un déploiement à des kilomètres est possible (réseaux externes). Cet aspect que nous développerons rendra possible l’expansion d’un WLAN entre deux sites et son exploitation à des fins intéressants (visioconférence).

#### **2.1.1 Usages du wifi**

Le Wifi permet:

- D’étendre un réseau existant (pont Wi-Fi).
- Partager une ressource (Switch / Accès Internet, Imprimante, serveur, disques durs).

- Réaliser un portail d'accès authentifié (Hot Spot)
- Utiliser des objets communiquant (lecteur de flux RSS, localisation)
- Accéder à une ressource mobile
- Déployer un réseau urbain alternatif aux opérateurs (les villes Internet)
- Supporte les transmissions de la voix et d'image

### **2.1.2 Avantages du wifi en particulier et du sans fil en générale**

Comme tout réseau sans fil le WIFI offre des avantages très importants comme:

- La mobilité
- Simplicité d'installation
- Facilité de desservir les zones inaccessibles par d'autres solutions de desserte
- Le coût est très réduit relativement à ses concurrents
- L'interconnectivité avec les réseaux filaires
- La fiabilité bien que les interférences liées aux ondes radio puissent dégrader les performances d'un réseau sans fil elles restent tout de même très réduites.
- La possibilité avec les versions récentes comme le 802.11g, n, s et autres, d'offrir des débits allant de 54 Mbits à près de 600 Mbits.
- La liberté de ses fréquences apporte un avantage dans le déploiement car cela épargne des procédures parfois très longues pour l'obtention d'une licence d'exploitation d'une bande de fréquence par les autorités.

### **2.1.3 Normes du réseau wifi**

Nous distinguons plusieurs variantes du Wifi, sur lesquelles nous expliquons en détail quelques-unes. Le 802.11b et le 802.11g sont compatibles entre eux et fonctionnent tous deux avec les ondes radio d'une fréquence de 2,4 GHz. Le 802.11b atteint un débit de 11 Mb/s et le 802.11g monte à 54 Mb/s. Le 802.11a n'est pas compatible avec le 802.11b et le 802.11g, car il fonctionne avec les ondes radio d'une fréquence de 5 GHz. Il permet d'atteindre 54 Mb/s. Le 802.11n permet d'atteindre un débit réel supérieur à 100 Mb/s. Il est capable de fonctionner à 2,4 GHz ou à 5 GHz et est compatible avec le 802.11b/g et le 802.11a. Malheureusement, la plupart des équipements 802.11n disponibles aujourd'hui n'utilisent que la bande de fréquences de 2,4 GHz (et ne sont donc pas compatibles avec le 802.11a). Aujourd'hui la variante du

Wifi de loin la plus utilisée est le 802.11g. Mais elle est rapidement rattrapée par le 802.11n

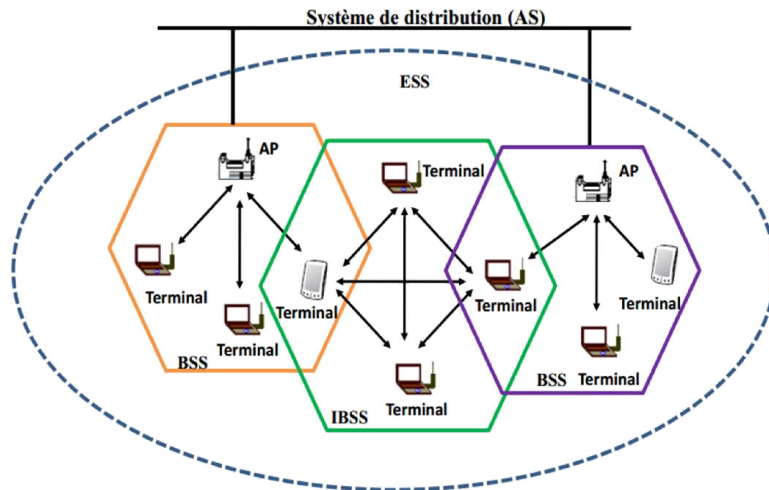
Variante	Débit Max.	Fréquence	Canaux	Modulation radio
802.11 <sup>a</sup>	2 Mb/s	2,4 GHz	3	FHSS ou DSSS
802.11a	54 Mb/s	5 GHz	19	OFDM
802.11b	11 Mb/s	2,4 GHz	3	DSSS ou HR-DSSS
802.11g	54 Mb/s	2,4 GHz	3	DSSS ou HR-DSSS ou OFDM
802.11n	> 100 Mb/s	2,4 GHz ou 5 GHz	3 ou 19	DSSS ou HR-DSSS ou OFDM avec MIMO

**Tableau 1: Quelques normes wifi [2]**

#### **2.1.4 Architectures du réseau wifi**

Une cellule est centrée autour de sa base radio (AP: Access Point). Lorsqu'un mobile quitte une cellule (BSS: Basic Service Set), pour maintenir la communication, il doit être accueilli par une autre cellule. Les techniques de gestion de la mobilité sont différentes selon que le mobile est un mobile voix (téléphone) ou un mobile données (station).

Une communication téléphonique peut être interrompue quelques millisecondes sans nuire à l'intelligibilité de la conversation (temps de basculement d'une cellule vers une autre). Dans un service de données, la moindre interruption provoque une erreur de transmission. Dans ces conditions, le basculement d'une cellule ne peut avoir lieu que dans la zone de recouvrement des cellules et en fin de transmission d'un paquet, on parle alors de roaming. Chaque cellule, BSS (Basic Service Set), est contrôlée par une base radio, (AP, Access Point). Le réseau peut comporter une ou plusieurs cellules autonomes ou être le prolongement d'un réseau Ethernet traditionnel. La liaison entre les différents AP peut être filaire ou radio (WDS, Wireless Distribution System). L'ensemble forme un seul réseau 802.11 désigné sous le terme ESS (Extended Service Set). Un ESS est identifié par un ESSID représenté sur 32 octets, qui sert de nom au réseau. La connaissance du ESSID est nécessaire pour se connecter au réseau.



**Figure 1: Architecture d'un réseau wifi [1]**

## 2.1.5 Topologie des réseaux wifi

### 2.1.5.1 Les réseaux ad hoc

Les réseaux « ad hoc » s'affranchissent de toute infrastructure. La communication a lieu directement de machine à machine. Une machine pouvant éventuellement servir de relais pour diffuser un message vers une station non vue par la station d'origine. Actuellement, les réseaux ad hoc ne fonctionnent qu'en mode point à point. Le routage est également utilisé. Le principe du routage reste cependant identique, lorsqu'une station veut joindre une autre, elle inonde le réseau, son message est répété par toutes les stations jusqu'à la station de destination. Le destinataire acquitte le premier message reçu qui emprunte en retour la même voie qu'à l'aller. Chaque machine apprend ainsi la route pour joindre le destinataire.



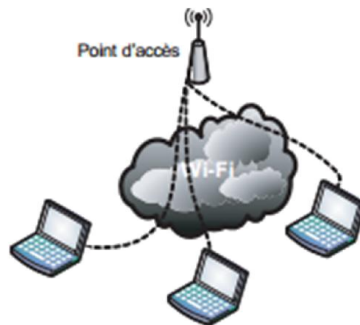
**Figure 2: Topologie ad hoc [1]**

### 2.1.5.2 Les réseaux mesh

Les réseaux mesh (meshed networks) sont des réseaux ad-hoc dans lesquels les points de routage sont immobiles. Les clients sont rattachés par un réseau sans fil sur les points d'accès, et les points d'accès sont reliés entre eux par des liaisons sans fil.



Les réseaux IEEE 802.11b ou Wifi et Hiperlan fonctionnent en général selon ce mode.



**Figure 3: Topologie en infrastructure [1]**

## **2.2 Couches et rôles du réseau wifi**

La norme 802.11 s'attache à définir les couches basses du modèle OSI pour une liaison sans fil utilisant des ondes électromagnétiques. La couche physique (notée parfois couche PHY), qui propose le codage de l'information. La couche liaison de données, constituée de deux sous-couches : le contrôle de la liaison logique (Logical Link Control, ou LLC) et le contrôle d'accès au support (Media Access Control, ou MAC).

La couche physique gère essentiellement la transmission des bits sur le support de communication, les niveaux électriques et les modulations.

Elle se subdivise en deux sous couches.

La couche PLCP (Physical Layer Convergence Protocol). prend en charge l'écoute du canal et signal à la couche MAC que le canal est libre.

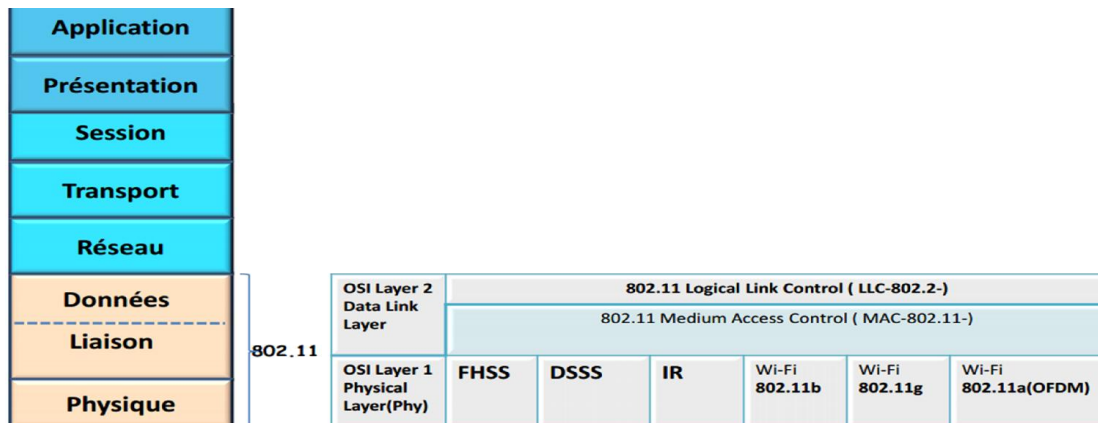
La couche PMD (Physical Medium Dependent). Elle s'occupe de l'encodage des données et gère la modulation.

La couche liaison de données gère la fiabilité du transfert des informations, le découpage en trames, la protection contre les erreurs, les trames d'acquittement et la régulation du trafic.

La couche liaison de données est composée essentiellement de deux sous-couches, LLC (Logical Link Control) et MAC (Medium Access Control)

La couche LLC gère les erreurs, le trafic, le flux, et la liaison au support. Elle utilise les mêmes propriétés que la couche LLC 802.2

La couche MAC 802.11 gère le partage du support.



**Figure 4: Couches wifi [8]**

## 2.3 Techniques d'étalement et de modulation

A cause des perturbations dues essentiellement aux fours à micro-ondes, il a fallu protéger la transmission radio contre les brouillages. Nous procédions pour cela aux techniques d'étalement de spectre qui consistent à utiliser une bande de fréquence beaucoup plus large que celle qui est nécessaire. Les techniques d'étalement de spectre, en plus de satisfaire aux conditions réglementaires, améliorent la fiabilité, accélèrent le débit et permettent à de nombreux produits non concernés de se partager le spectre sans coopération explicite. La norme IEEE 802.11 en dispose de deux:

### 2.3.1 FHSS (Frequency Hopping Spread Spectrum)

L'étalement de spectre par saut de fréquence FHSS a été développé par l'armée pour une transmission de données. L'idée est de répartir le signal d'information sur une bande passante plus large pour rendre plus difficile son brouillage ou son interception. Le signal est transmis à tout le réseau en une suite apparemment aléatoire de fréquences radio, sautant d'une fréquence à une autre par intervalle de temps fixe. La bande des 2,4 GHz est divisée en 75 sous-canaux de 1 MHz. L'émetteur et le récepteur s'accordent sur un schéma de saut, et les données sont envoyées sur une séquence de sous-canaux. Chaque conversation sur le réseau 802.11 s'effectue suivant un schéma de saut différent, et ces schémas sont définis de manière à minimiser le risque que deux expéditeurs utilisent simultanément le même sous-canal. Les techniques FHSS sont limitées à un débit de 2 Mbps. Les systèmes FHSS s'étalent sur

l'ensemble de la bande des 2,4 GHz, ce qui signifie que les sauts doivent être fréquents et représentent en fin de compte une charge importante.

### **2.3.2 DSSS (Direct Sequence Spread Spectrum)**

Le principe de l'étalement du spectre par séquence direct est de coder chaque bit du signal original par plusieurs bits dans le signal transmis à l'aide d'une séquence d'étalement appelée "shipping" ou séquence de Barker. DSSS divise la bande des 2,4 GHz en 14 canaux de 22 MHz.

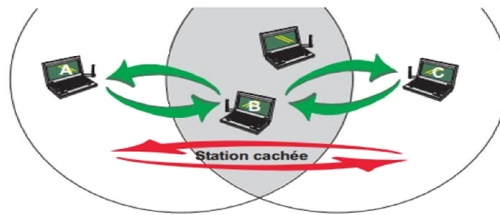
### **2.3.3 La modulation OFDM**

La modulation OFDM (Orthogonal Frequency Division Multiplexing) ou encore DMT (Discrete MultiTone modulation) [6] utilisée notamment dans les techniques DSL (Digital Subscriber Line) repose sur le principe du multiplexage fréquentiel. Le canal de transmission est découpé en sous-canaux, chaque sous-porteuse transporte N bits ou symboles. L'OFDM en répartissant le flux binaire sur N porteuses, divise par N la rapidité de modulation de chaque porteuse réduisant ainsi les effets de l'interférence de symboles et optimisant l'utilisation du spectre radiofréquence. L'optimisation de l'occupation de l'espace fréquentiel conduit à définir des porteuses proches les unes des autres, engendrant ainsi un risque d'interférences entre porteuses adjacentes, aussi pour minimiser ce risque, les sous-porteuses sont définies de telle manière que le maximum de puissance de leur spectre corresponde au minimum de puissance des porteuses voisines. L'utilisation de multi porteuses autorise aussi à adapter le débit aux conditions de propagation.

- **Technique d'accès au support wifi**
- **Notion de station cachée**

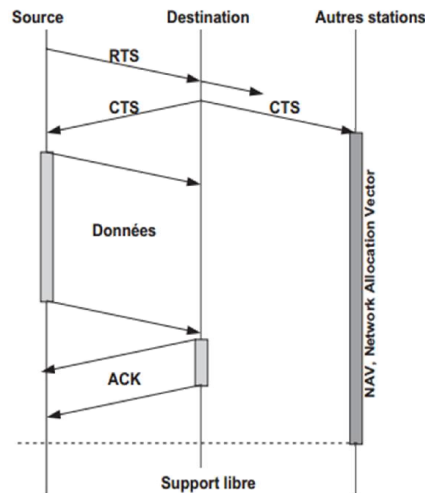
À l'instar d'Ethernet, les stations d'un réseau sans fil se partagent le même média. Le protocole CSMA utilisé dans les réseaux Ethernet n'est pas applicable tel quel. La station A doit transmettre des données à destination de la station B. La station A écoute le support, si celui-ci est libre, elle émet. Cependant, dans le même temps, la station C désire aussi transmettre des données à B ou à une autre machine de la zone d'interférence. La station C est hors de portée de A (station cachée), elle n'entend pas

le message de A, et considère le support libre, elle transmet ses données. Les données de A et de C sont polluées, il y a collision et dans ce cas on parle de station cachée



**Figure 5: Problème de la station cachée [2]**

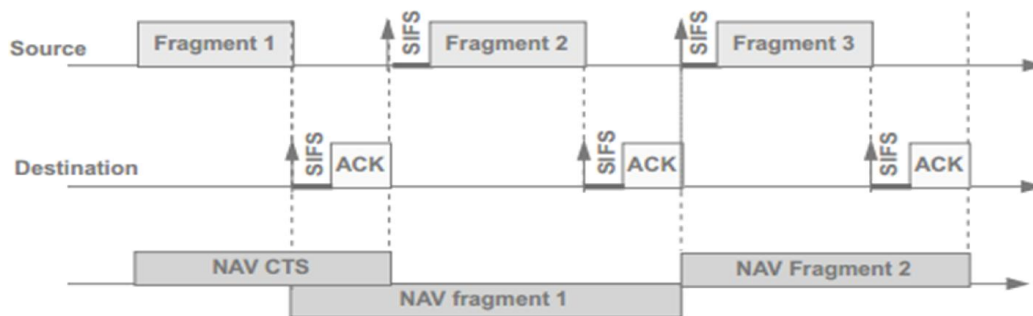
L'algorithme d'accès ou DCF (Distributed Coordination Function) est une version adaptée du CSMA, le CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance, signifiant à prévention de collision). [2] Détecter une collision nécessite une transmission de type full duplex, or, en environnement radio, la puissance d'émission éblouirait le récepteur, cette approche est irréalisable à coût raisonnable. Il est donc impératif d'implémenter un mécanisme qui rend la probabilité de collision aussi faible que possible c'est l'objet du CSMA/CA dont le principe est illustré ci-dessous. Un mécanisme d'accusé de réception complète le système. Une station qui veut émettre écoute le support (CSMA). Si le support est occupé, elle diffère son émission. Si le support est libre, elle émet un petit paquet (RTS, Request To Send) qui contient les adresses source et destination ainsi qu'une durée correspondant au temps d'émission des données et au délai d'acquittement (réservation d'une tranche canal). Si le support est libre, la station destination répond (CTS, Clear To Send), le message comporte les mêmes informations que le RTS. Ainsi, la station C (station cachée de A) qui n'a pas reçu le message de A, reçoit celui de B qui comporte les mêmes informations, elle est donc informée de la demande de réservation de bande formulée par A. Toutes les stations recevant le RTS ou le CTS arment une temporisation (Virtual Carrier Sense) correspondant au temps de réservation demandé (NAV, Network Allocation Vector). La probabilité de collision est d'autant plus faible que le message est court. À cet effet, la norme IEEE 802.11 introduit la segmentation au niveau MAC.



**Figure 6: Méthode d'accès au support [2]**

#### ▪ Mécanisme de fragmentation

Les transmissions hertziennes sont d'autant plus sensibles aux perturbations que la trame émise est grande. Aussi, pour améliorer la fiabilité des réseaux 802.11, la couche MAC implémente un mécanisme de fragmentation et de réassemblage. Ce mécanisme diminue la probabilité qu'une trame émise soit erronée, mais aussi améliore le rendement de transmission, en effet, la retransmission d'un fragment est moins coûteuse en bande passante que celle de l'intégralité de la trame d'origine. La figure ci-dessous illustre le principe de la fragmentation, on remarquera que l'indication de durée contenue dans chaque fragment protège la séquence d'émission du fragment en cours, mais aussi celle du fragment suivant.

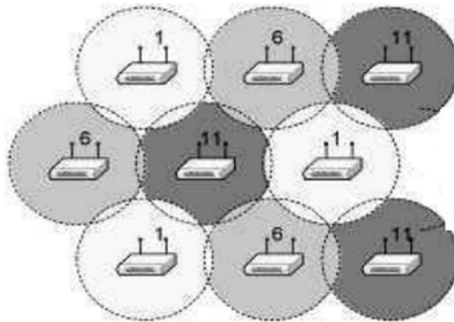


**Figure 7: Illustration de la fragmentation [1]**

#### ▪ Limitation des interférences entre AP

Pour limiter les interférences entre nos AP, nous avons fait varier les canaux afin que chaque cellule n'interfère pas avec les cellules voisines. Seul le SSID reste le même pour que les utilisateurs puissent passer d'une cellule à une autre sans rupture

de connexion. Avec le 802.11b, le 802.11g et le 802.11n à 2,4 GHz, on dispose de treize canaux. Les canaux voisins se superposent de sorte que seuls trois canaux indépendants peuvent être utilisés au même endroit. On choisit en général les canaux 1, 6 et 11. Le schéma suivant montre à quoi doit ressembler notre déploiement pour limiter les interférences entre les AP.



**Figure 8: Représentation des interférences entre les AP [3]**

#### ▪ Limitation du recouvrement des cellules

Un premier axe d'amélioration consiste à utiliser des antennes directionnelles ou sectorielles pour concentrer le signal vers la zone à couvrir, en essayant d'éviter le débordement vers les cellules voisines. En complément, nous utilisons les AP qui nous permettent de diminuer la puissance du signal émis tout en s'assurant que la couverture dans la cellule ne soit pas détériorée. Un AP qui autorise des stations éloignées à s'associer à lui, ces stations seront des sources d'interférences pour les autres AP utilisant le même canal. Ainsi, il est intéressant de diminuer la sensibilité de l'AP pour empêcher des stations distantes de s'y associer. Le réseau wifi, malgré ses très nombreux avantages, comporte des risques majeurs en termes de sécurité.

## 2.4 Les attaques d'un réseau wifi

L'intégration des services dans un réseau nécessite plus de sécurité. Bref, la sécurité n'est pas une paranoïa d'experts cherchant à valoriser leur spécialité : c'est une réalité. C'est ainsi que pour lutter efficacement contre les attaques dans le réseau, nous allons définir rapidement les catégories d'attaques contre lesquelles nous devons nous prémunir : l'espionnage, l'intrusion, le déni de service.

### 2.4.1 L'espionnage

Sans doute la première attaque, qui vient à l'esprit lorsque l'on parle des technologies sans fil, est l'écoute : un pirate se poste à proximité et surveille les

échanges. On dit qu'il « sniffe » le réseau sans fil. Dans les réseaux filaires, ceci est rendu difficile par le fait qu'il faut d'abord se brancher physiquement au réseau avec un câble avant de pouvoir écouter quoi que ce soit. Avec le Wifi, chacun peut écouter ce qui est transmis par les autres. Il suffit pour cela de disposer d'un adaptateur Wifi gérant le mode monitor, c'est-à-dire capable de lire tous les messages, et pas uniquement ceux qui lui sont adressés. Ensuite, il faut utiliser un logiciel d'analyse du réseau, du type Ethereal, pour « sniffer » tout ce qui se passe sur le réseau. Écouter une communication Wifi est à la portée de presque tout le monde. L'espionnage peut aboutir à la divulgation d'informations confidentielles: mots de passe, documents secrets, numéros de cartes bancaires, etc. Aussi, pour sécuriser les échanges, il est indispensable de crypter les communications avec un algorithme aussi puissant que possible, sans que cet algorithme ne ralentisse trop la communication.

#### **2.4.2 L'intrusion**

Une autre attaque consiste à s'introduire au sein du réseau Wifi pour consulter, voire, modifier les données du système informatique (bases de données, fichiers, e-mails...) ou encore pour profiter de la connexion à Internet. Une intrusion réussie permet au pirate de se comporter exactement comme un utilisateur normal : au point qu'il est souvent difficile de s'apercevoir qu'une intrusion a eu lieu ou même qu'elle est en cours, car tout se passe comme si un utilisateur normal accédait au système. Il s'agit donc d'une attaque extrêmement dangereuse. L'intrusion est bien sûr tout à fait triviale si aucune sécurité n'est mise en œuvre: il suffit de s'associer normalement à l'un des AP du réseau, et il peut tout faire. En revanche, si l'association impose un mécanisme d'identification avant d'autoriser l'ouverture d'une session sur le réseau, le pirate aura essentiellement deux options:

- ouvrir une nouvelle session en se faisant passer pour un utilisateur légitime.
- détourner une session existante (hijacking).

#### **2.4.3 Le déni de service (dos: denial of service)**

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

clients (par exemple un serveur web) doit traiter des requêtes provenant de plusieurs clients. Lorsque ces derniers ne peuvent en bénéficier, pour des raisons délibérément provoquées par un tiers, il y a déni de service. Dans une attaque de type dos les ressources d'un serveur ou d'un réseau sont épuisées par un flot de paquets. Un seul attaquant visant à envoyer un flot de paquets peut être identifié et isoler assez facilement. Cependant l'approche de choix pour les pirates a évolué vers un déni de service distribué (ddos). Une attaque ddos repose sur une distribution d'attaques dos, simultanément menées par plusieurs systèmes contre un seul. Cela réduit le temps nécessaire à l'attaque et amplifie ses effets. Dans ce type d'attaque les pirates se dissimulent parfois grâce à des machines-rebonds (ou machines zombies), utilisées à l'insu de leurs propriétaires. Un ensemble de machines-rebonds, est contrôlable par un pirate après infection de chacune d'elles par un programme de type porte dérobée (backdoor).

## **2.5 Les techniques de sécurité du wifi**

La première fonction d'un système d'information est de stocker et de permettre l'échange de données. Sécuriser un système d'information consiste donc à réduire le risque que les données soient compromises ou qu'elles ne puissent plus être échangées. En outre, dans les réseaux sans fil, le support est partagé. Tout ce qui est transmis peut donc être intercepté. Pour permettre aux réseaux sans fil d'avoir un trafic aussi sécurisé que dans les réseaux filaires, des groupes de travaux ont mis au point les premières solutions de sécurité, des mécanismes de cryptage et des protocoles de sécurité.

### **➤ La supervision radio**

Il peut également être intéressant d'installer des sondes Wifi ou d'exploiter les fonctions de supervision radio offertes par certains AP, pour détecter les AP non sécurisés. La supervision radio peut permettre de détecter des AP non sécurisés, voire même certains types d'attaques Wifi, comme par exemple le spoofing d'adresse MAC ou certaines attaques Dos. Bien entendu, ce n'est qu'une mesure palliative, et non préventive: elle ne peut pas être utilisée seule.



### ➤ **Masquer le SSID**

Comme nous pouvons constater, il est parfois conseillé de masquer le SSID du réseau sans fil. Un passant équipé d'un matériel Wifi classique ne saura pas qu'un réseau sans fil se trouve à proximité ou en tout cas ne saura pas s'y associer facilement. Toutefois, il ne s'agit que d'une protection très faible, car il suffit de sniffer les ondes radio au moment où un utilisateur légitime se connecte : le SSID se trouve alors en clair dans sa requête d'association. En outre, chaque utilisateur légitime devra saisir manuellement le SSID du réseau sur son ordinateur.

### ➤ **Le filtrage par adresse MAC**

Un autre mécanisme pour repousser les « petits » pirates consiste à limiter l'accès au réseau sans fil à une liste d'équipements donnés, identifiés par leur adresse MAC. De nombreux AP disposent de cette fonction de filtrage par adresse MAC. Les adresses autorisées sont souvent stockées dans chaque AP, ce qui signifie qu'il faut modifier tous les AP lorsque l'on souhaite ajouter ou retirer une adresse MAC.

Le filtrage par adresse MAC a deux inconvénients majeurs:

- Il est assez lourd à mettre en œuvre pour une moyenne ou grosse entreprise car il faut conserver la liste des adresses MAC de tous les équipements susceptibles de se connecter au réseau sans fil.
- Plus grave encore, il est assez simple pour un pirate de sniffer le réseau, de noter les adresses MAC d'utilisateurs légitimes, puis de « spoofer » (imiter) une adresse MAC légitime. Bref, cela ne sert qu'à arrêter les petits pirates et les simples curieux.

Avec ces deux inconvénients, on peut affirmer que le filtrage par adresse MAC n'est pas vraiment utile d'être mis en œuvre.

## **2.5.1 Le cryptage WEP**

Première solution de cryptage à avoir été standardisée par l'IEEE, Wired Equivalent Privacy (WEP) [5] signifie « sécurité équivalente au filaire ». Malheureusement, dans la pratique, la solution WEP ne s'est pas montrée à la hauteur de sa définition: à peine quelques mois après sa publication, des failles importantes ont été découvertes dans le WEP et exploitées presque immédiatement dans des attaques contre des réseaux Wifi. Des outils sont même disponibles gratuitement sur Internet

qui permettent de casser la clé WEP, c'est-à-dire, en possédant suffisamment de paquets cryptés, de retrouver quelle clé WEP a servi au cryptage. Il suffit alors à un pirate de configurer son propre adaptateur avec cette clé WEP pour rendre le cryptage tout à fait inutile. Le WEP a un autre problème majeur: tout le monde partage la même clé WEP. Cela signifie que si la clé doit être changée, il faut le faire sur tous les postes et dans tous les AP. Ceci impose une énorme lourdeur de gestion. C'est d'autant plus grave que pour assurer une sécurité minimale, il faut changer la clé régulièrement, en particulier à chaque fois qu'elle risque d'avoir été compromise, ou lorsqu'un employé quitte la société. En outre, une seule indiscretion d'un employé suffit à compromettre la sécurité pour toute la société. Enfin, puisque tous les employés ont la même clé, rien n'empêche un employé mal intentionné d'espionner ou d'attaquer ses collègues.

### **2.5.2 Le cryptage WPA**

La Wifi Alliance défini par l'association des constructeurs à partir du standard 802.11 va décider de ne pas attendre la parution du 802.11i, ni accepter que chaque constructeur définisse sa propre solution. C'est ainsi qu'elle définit la solution Wireless Protected Access (WPA): il s'agit d'une version allégée du standard 802.11i. Il existe deux variantes du WPA: le WPA Personal, également appelé WPA-PreShared Key (WPA-PSK) et le WPA Enterprise. [5] Le WPA-PSK suppose la configuration d'une clé partagée dans tous les AP et équipements connectés au réseau. Le WPA Enterprise repose sur le protocole 802.1x et un serveur d'authentification RADIUS.

Le WPA repose sur le cryptage Temporal Key Integrity Protocol (TKIP) qui a été conçu de telle sorte qu'il soit possible de le mettre en œuvre dans les AP existants, par le biais d'une simple mise à jour de firmware (le microprogramme contenu dans l'AP). Tout en reposant sur l'algorithme RC4, il corrige toutes les failles du WEP et peut être considéré comme très robuste. Toutefois, il n'a été défini que pour servir de transition vers le 802.11i, qui est la solution la plus sûre.

### **2.5.3 Le cryptage 802.11i (WPA2)**

Le 802.11i permet d'utiliser un nouvel algorithme de cryptage, l'Advanced Encryption Standard (AES), [5] qui est sans doute l'un des algorithmes les plus puissants aujourd'hui. Malheureusement, l'AES est plus exigeant en puissance de

calcul que le RC4. Pour cette raison, un matériel plus performant est nécessaire pour le mettre en œuvre. Dès 2004, avant la parution du 802.11i, des AP assez robustes pour gérer l'AES ont vu le jour : dès la publication du 802.11i, en juin 2004, ils ont pu être mis à jour. Les AP antérieurs devront malheureusement être remplacés si l'on souhaite bénéficier de la meilleure solution de sécurité qui soit en Wifi.

	WEP	WPA	802.11i
Chiffrement	RC4	RC4	AES
Longueur de la clé	40/104 bits	128 bits	128 bits
Intégrité des données	CRC-32	Michael	CBC-MAC
Intégrité des en-têtes	Non	Michael	CBC-MAC
Contrôle des attaques par rejeu	Non	Vecteur d'initialisation	Vecteur d'initialisation
Gestion des clés	Non	802.1X	802.1X
Taille du vecteur d'initialisation	24 bits	48 bits	48 bits
Clé par paquet	Non	Oui	Possible

**Tableau 2: Caractéristiques des standards de sécurité Wi-Fi [5]**

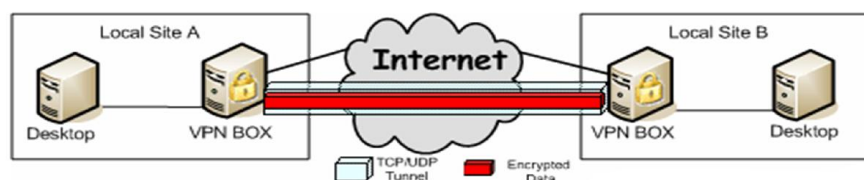
#### 2.5.4 Les VLAN

Les réseaux virtuels ou VLAN (Virtual Local Area Network) autorisent une répartition et un partage optimal des ressources de l'entreprise. Les VLAN associent un port à un identifiant, et ne peuvent communiquer que les machines raccordées à des ports de même identifiant. Pour les AP ou les commutateurs qui le permettent, il est bon d'associer le trafic sans fil à un VLAN particulier. Ceci facilitera par la suite la maintenance et l'administration du réseau car tout le trafic provenant du réseau sans fil sera clairement identifié. En outre, certains AP peuvent associer un utilisateur donné à un VLAN particulier au moment de l'identification grâce au protocole RADIUS. Par exemple, lorsqu'un techniciens se connecte au réseau sans fil, il peut automatiquement être associé au VLAN numéro 10 qui lui donne accès aux serveurs spécifique aux techniciens de l'entreprise. Si un comptable se connecte, il peut être associé au VLAN numéro 20 qui lui donne accès aux serveurs réservés aux comptables. Enfin, si un simple visiteur se connecte, il peut être associé au VLAN numéro 30, lui donnant uniquement un accès limité et contrôlé à Internet. Différentes politiques de qualité de service (QoS) peuvent être mises en œuvre sur les différents VLAN, ainsi un visiteur

n'aura droit qu'à une très faible bande passante, alors que les techniciens en auront suffisamment pour participer, par exemple, à des vidéoconférences.

### 2.5.5 Protocole VPN

VPN: Virtual Private Network ou RPV (réseau privé virtuel) est une technique permettant à un ou plusieurs postes distants de communiquer de manière sûre, tout en empruntant les infrastructures publiques. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites, de façon simple et économique. Jusqu'à l'avènement des VPN, les sociétés devaient utiliser des liaisons spécialisées. Créé en 2002, Openvpn est un outil *open source* utilisé pour construire des VPNs site à site avec le protocole SSL/TLS ou avec des clefs partagées. Son rôle est de "tunneliser", de manière sécurisée, des données sur un seul port TCP/UDP à travers un réseau non sûr comme Internet et ainsi établir des VPNs.



**Figure 9: Connexion de deux sites à tunnel VPN [5]**

La solution VPN étant la seule à réellement offrir un niveau important de protection avant l'arrivée du WPA et du WPA2. Dans le cas où les AP Wifi ne gèrent pas le WPA ou le WPA2, cette solution est sans doute l'une des plus appropriées.

### Conclusion

En somme l'étude générale du réseau wifi, nous a permis de tenir compte des paramètres tels que: les normes, les techniques de modulation et d'étalement, la gestion des interférences, le recouvrement des cellules, le type de sécurité à prendre pour pouvoir bien planifier et étendre nos équipements.

## **CHAPITRE 3: DÉPLOIEMENT ET EXPANSION DU RESEAU WIFI**

### **Introduction**

Pour permettre toute communication entre des sites distants, une solution consisterait à une interconnexion par fibre optique, par ondes radio WIMAX, par VSAT et bien d'autres supports de transmission. Mais toutes ses techniques suscitées sont d'autant plus onéreuses que les dirigeants des services administratifs n'auraient pas assez de fonds à dépenser pour s'en acquérir. Dans l'optique de proposer un service, fiable, et à moindre coût de mise en place, nous avons donc opté pour le WIFI. Le déploiement du réseau wifi passe par un certain nombre d'étapes: Le dimensionnement des équipements, le dimensionnement en capacités, et enfin la mise en œuvre.

### **3.1 Dimensionnement des équipements**

Le dimensionnement permet de déterminer la portée maximale d'une station de base en utilisant les modèles de propagation conformément au terrain d'étude. Ceci afin de prédire la couverture de la cellule et faire un bilan de liaison. Le but du dimensionnement est d'optimiser la disposition des sites radio (minimiser le coût de l'infrastructure du réseau) dans une zone géographique précise. Dans cette partie, il sera question pour nous de faire l'évaluation du matériel, le site Survey, le choix de la bande de fréquences, le choix du modèle de propagation, le bilan de liaison.

#### **3.1.1 Les matériels d'interconnexion et leurs caractéristiques**

##### **3.1.1.1 Le point d'accès**

Les points d'accès (AP) sont le cœur d'un réseau sans fil de type Infrastructure. Ils gèrent de nombreuses fonctions telles que l'authentification et l'association des stations, ou encore l'acheminement des paquets Wifi entre les stations associées.

Pour chaque site, nous avons axé notre choix sur un point d'accès sans fil de type WDS (Wireless Distribution System) régi par l'IEEE sous la norme 802.11s qui rend possible l'extension d'un réseau Wifi interne, et nous permet aussi de maîtriser:

- La gestion du hand-over : un utilisateur peut alors passer sans déconnexion d'un AP à un autre. Pour cela, les AP communiquent entre eux via le système de distribution (DS) qui est un réseau filaire.
- Le filtrage des périphériques autorisés, en fonction de leur adresse MAC.
- Le cryptage des données échangées et l'authentification des périphériques grâce aux protocoles WEP, WPA ou WPA2.



**Figure 10: Le point d'accès [3]**

### **3.1.1.2 Les routeurs**

Ils permettent le choix du meilleur chemin. Pour nos sites, nous utilisons les routeurs Cisco, moins chères et plus répandus sur les marchés.



**Figure 11: Routeur D-Link [3]**

### **3.1.1.3 Choix de l'antenne**

Les antennes servent à la fois à l'émission et à la réception du signal électromagnétique: à l'émission, elles transforment en ondes électromagnétiques les signaux électriques générés par l'émetteur; à la réception, elles transforment en courant électrique une onde électromagnétique émise par une autre antenne, de sorte qu'un récepteur pourra l'interpréter. La communication en Wifi ne nécessite pas de câble, cependant il faut bien un équipement de rayonnement des ondes, c'est le rôle des antennes. Il existe différents types d'antennes. Nous allons tout d'abord voir les 3 grandes types d'antennes qui existent; puis nous verrons comment choisir l'antenne adéquate à notre installation.

Les antennes omnidirectionnelles: sont habituellement attachés à un point d'accès Wifi (AP). Ils ont un modèle de rayonnement à 360-degrés et fonctionnent normalement comme concentrateur ou passage central d'un réseau. Elles ont un champ

verticalement polarisé. Le gain d'une antenne omnidirectionnelle est normalement bas, autour de 3 à 12 dBi. En pratique, elles sont employées pour des liens Point-à-MultiPoint. Il est tout à fait possible d'envisager des liens de 1 à 5 kilomètres.



**Figure 12: Antenne omnidirectionnelle [7]**

Les antennes sectorielles: sont habituellement attachées à un point d'accès WiFi (AP) mais sont conçus pour fonctionner avec un gain plus élevé (10 à 19 dBi) que les antennes omnidirectionnelles. Au contraire des antennes omnidirectionnelles, les antennes sectorielles couvrent seulement un secteur de l'azimut typiquement de 60° à 120°. Des antennes sectorielles, sont utilisées pour les liaisons Point-à-Multi-Point. Elles sont typiquement employées pour des liens de 6 à 8 kilomètres.



**Figure 13: antenne sectorielle [7]**

Les antennes directionnelles qui font l'objet de notre choix sont normalement trouvées chez les clients distants pour les liaisons point à point. Le type d'antenne directionnelle que nous utilisons est l'antenne yagi qui se compose d'un dipôle (parfois appelé un radiateur ou un élément conducteur), d'un ensemble d'éléments directeurs, et

aussi d'un réflecteur. L'antenne est normalement enfermée dans un cylindre en plastique pour la protection.



**Figure 14: Antenne directionnelle de type yagi [7]**

Afin de ne pas se tromper dans le choix de notre antenne, il était important pour nous de prendre en considération plusieurs paramètres.

➤ **La directivité**

C'est la valeur normalisée de l'intensité de rayonnement relativement à une antenne isotrope. Il exprime la capacité de l'antenne d'émission à concentrer son rayonnement dans une direction donnée. Nos antennes rayonnent de façon directionnelle puisqu'elles concentrent le signal dans une direction donnée.

L'antenne directionnelle permet au récepteur, de recevoir un signal d'une puissance plus importante que si l'antenne était parfaitement omnidirectionnelle.

➤ **Le gain**

Par définition, c'est le rapport entre la puissance qu'il faudrait fournir à une antenne isotrope et celle fournie à l'antenne étudiée pour produire la même intensité de rayonnement dans la direction d'intérêt. Le gain est mesuré en décibels. Plus une antenne passive concentre le signal dans un faisceau étroit, plus le gain de l'antenne est élevé.

➤ **La Pire**

La puissance du signal perçu par un observateur est plus grande si ce signal est concentré en direction de l'observateur grâce à une antenne directionnelle et non diffusé de façon homogène dans l'espace. Si l'on remplace une antenne directionnelle par une antenne parfaitement omnidirectionnelle, il faut alors augmenter la puissance de l'émetteur pour que le récepteur perçoive la même puissance qu'auparavant. La

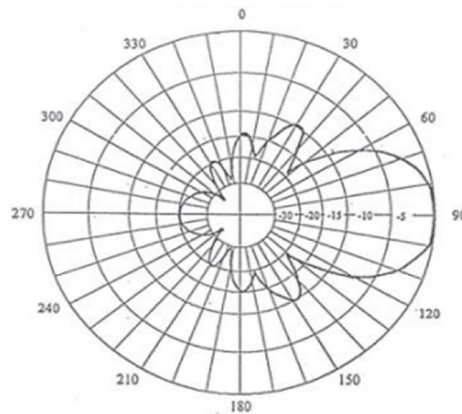


puissance de cet émetteur omnidirectionnel équivalent est appelée la puissance isotrope rayonnée équivalente (PIRE). Voici la formule permettant le calcul de la PIRE:

**PIRE** = Puissance de l'émetteur - atténuation dans le câble + Gain de l'antenne.

#### ➤ Diagramme de rayonnement

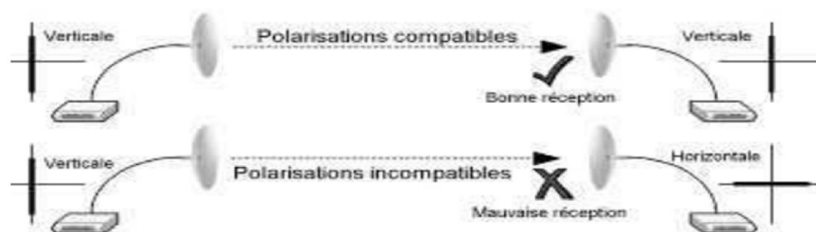
On appelle diagramme de rayonnement, la distribution surfacique de la puissance rayonnée à une distance fixe de l'antenne. Le modèle de rayonnement que nous avons préféré pour l'antenne yagi, est le rayonnement vertical.



**Figure 15: Diagramme de rayonnement [3]**

#### ➤ La polarisation

Les antennes Wifi entraînent une polarisation du signal qui peut être horizontale, verticale, selon un axe incliné, ou encore circulaire droite ou gauche (dans le sens des aiguilles d'une montre ou non). Dans notre choix la polarisation verticale est celle que nous avons adoptée puisqu'elle est moins atténuée que la polarisation horizontale.



**Figure 16: Polarisation de l'antenne de l'émetteur et du récepteur [3]**

### 3.1.2 Le site Survey

Pour savoir combien d'AP installer et où les placer, la solution la plus simple consiste à réaliser ce qu'on appelle un site Survey. Cela consiste à installer un ou plusieurs AP aux endroits qui paraissent les plus adaptés, puis à mesurer le signal en se

déplaçant dans les locaux. Il n'est pas nécessaire de connecter les AP au réseau, mais simplement de les alimenter en électricité et de les allumer. Si nous observions des zones d'ombre, des interférences ou encore un débit insuffisant, nous déplaçons les AP et nous recommençons. Bien que cela soit une solution assez artisanale. Elle est assez fiable pour s'assurer que la couverture radio est bonne. Néanmoins les outils que nous pouvions utiliser pour réaliser un site Survey sont très nombreux. Nous allons essayer d'énumérer quelques-uns:

#### **3.1.2.1 Simulateur Netstumbler**

L'usage de l'outil d'analyse Netstumbler, téléchargeable gratuitement sur [www.stumbler.net](http://www.stumbler.net). S'installe sur un PC portable (sous Windows uniquement). Il nous fournit de nombreuses informations sur la couverture radio, dont en particulier le niveau du signal, le RSB, le canal, le SSID et le BSSID de chaque AP à proximité. Malheureusement, il ne fonctionne pas avec tous les adaptateurs Wifi.

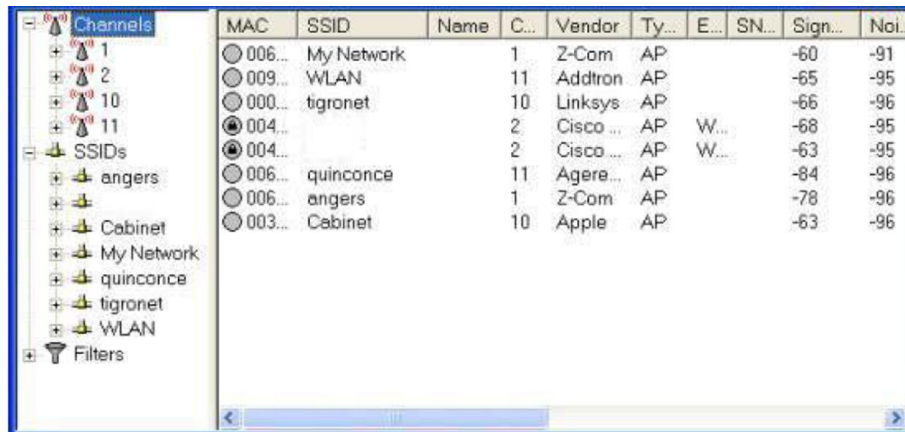
#### **3.1.2.2 Simulateurs professionnels**

Les logiciels commerciaux spécialisés dans l'audit de sites sont nombreux. Citons quelques-uns des plus répandus: Air Défense, AirMagnet, Finisar, Network Associates, WildPackets et YellowJacket. Ils sont disponibles pour PC portable. En plus des paramètres indiqués par NetStumbler (niveau du signal, RSB, canal, SSID, BSSID). Ces logiciels permettent d'obtenir de nombreuses autres informations importantes, dont en particulier le débit réel grâce à un mode actif dans lequel le logiciel s'associe au réseau sans fil et réalise des transferts de données avec lui-même. Donc sans qu'il soit nécessaire de connecter l'AP au réseau filaire. Par ailleurs, l'analyse des interférences et des pertes de paquets est souvent assez fine. Certains produits sont même de véritables analyseurs de spectre de fréquences radio et peuvent détecter toutes les interférences avec précision (dans le produit Yellow Jacket, par exemple). Certains sont couplés à une base de connaissance qui fournit un grand nombre de conseils pratiques pour la résolution de problèmes. Elle est particulièrement complète dans le produit AirMagnet. Bref, ce type d'outils d'analyse est très utile pendant le site Survey. Mais aussi et surtout après l'installation du réseau sans fil, pour détecter d'éventuels problèmes apparus après l'installation : de nouvelles sources

d'interférences, des tentatives d'intrusion dans le système ou encore des points d'accès pirates. Le prix de ces logiciels est assez élevé, ce qui explique sans doute en grande partie pourquoi les audits de site sont encore de loin la solution préférée par les entreprises pour préparer les déploiements.

### ❖ Simulation et Interprétation des résultats

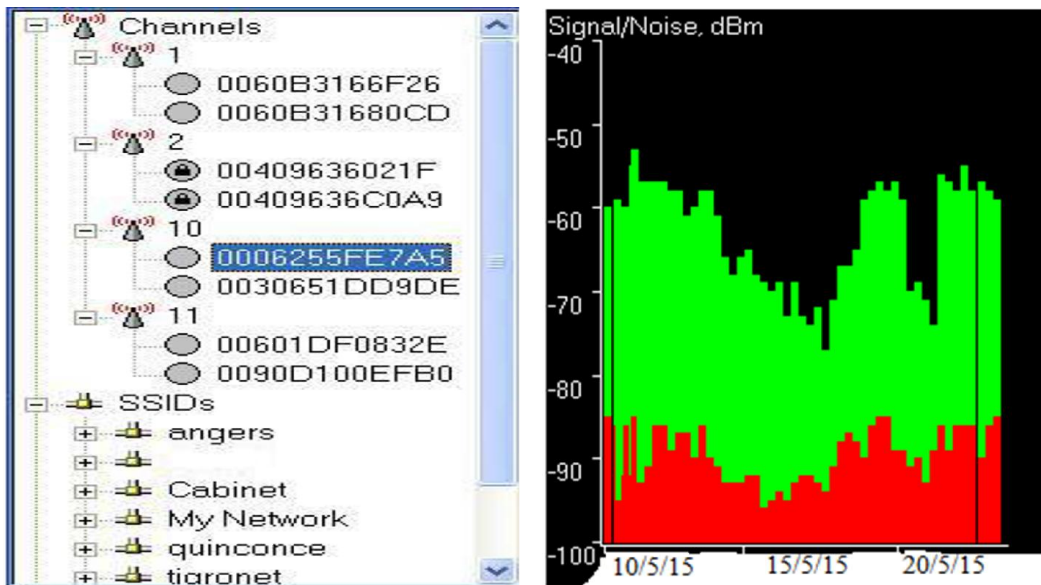
Après l'installation de Netstumbler, nous obtenons une interface qui nous donne toutes les informations sur les points d'accès qui sont sur la zone de couverture.



MAC	SSID	Name	C...	Vendor	Ty...	E...	SN...	Sign...	Noi...
006...	My Network		1	Z-Com	AP			-60	-91
009...	WLAN		11	Addtron	AP			-65	-95
000...	tigronet		10	Linksys	AP			-66	-96
004...			2	Cisco ...	AP	W...		-68	-95
004...			2	Cisco ...	AP	W...		-63	-95
006...	quinconce		11	Agere...	AP			-84	-96
006...	angers		1	Z-Com	AP			-78	-96
003...	Cabinet		10	Apple	AP			-63	-96

**Figure 17: Informations sur les différents AP**

Ainsi nous pouvons voir les différents AP qui couvrent notre zone, leur adresse MAC, leur SSID, le canal qu'ils occupent, le signal, et le bruit afin de pouvoir éviter les interférences. Pendant l'écoute nous voyons une fenêtre qui contient les informations concernant les points d'accès détectés. La présence d'un petit cadenas, indique que le réseau est crypté. Mais quand nous cliquons dans l'arborescence sur un point d'accès nous obtenons une courbe de signal qui nous indique la qualité du rapport signal sur bruit.



**Figure 18: Rapport sur la qualité du signal sur le bruit d'un AP.**

Avec la qualité du signal sur la droite. Il est important de noter que le rouge représente le bruit et le vert représente le bon signal. Ainsi lorsque la qualité du signal avoisine les -90 dBm, le réseau est inexploitable.

### 3.1.3 Le choix de la bande de fréquences

La sélection de la bande de fréquence à utiliser a une influence capitale sur le dimensionnement et la planification d'un réseau. A basses fréquences, les caractéristiques de propagation du signal sont meilleures, seulement la bande passante disponible est limitée. Ainsi dans notre cas le choix des bandes sans licence 2.4Ghz et 5Ghz a été adopté pour le déploiement du réseau wifi.

### 3.1.4 Le choix et rôle des modèles de propagation

Les modèles de propagation simulent la manière avec laquelle les ondes radio se propagent dans l'environnement d'un point à l'autre. Afin de modéliser exactement le comportement des ondes radio, les caractéristiques de l'environnement telles que la topologie du terrain (par exemple, colline ou appartement), la couverture au sol telle que des bâtiments et des arbres doivent être considérées. Dans la suite nous allons énumérer quelques modèles de propagation et indiquer celui que nous avons utilisé.

#### ▪ Types de modèles de propagation

Dans ce paragraphe, nous rappelons plusieurs modèles de propagation applicables à l'architecture multi cellules.

Typiquement, le scénario est le suivant:

Les cellules < 100 m de rayon;

Des antennes directionnelles sont installées, au-dessous des toits (2-10 m);

Condition d'une grande couverture de cellule (80-90%).

Le canal sans fil est caractérisé par :

Perte due au chemin;

Caractéristiques d'évanouissement;

Interférence Co-canal et entre les canaux adjacents.

Il est à noter que ces paramètres sont arbitraires, et seulement une caractérisation statistique est possible. Les paramètres des modèles de propagation ci-dessus dépendent des éléments tel que: Le terrain, la densité des arbres, la hauteur d'antenne, la largeur du faisceau, et la vitesse du vent.

Les modèles de propagation varient selon que l'émetteur et le récepteur seraient ou non en ligne de vue ou en d'autres termes en environnement LOS ou NLOS.

#### **3.1.4.1 Modèle D'Okumura- Hata**

C'est une méthode de prédiction pleinement empirique basée sur une série de mesure faite à l'intérieur et hors de la ville de TOKYO entre 200MHZ et 2GHZ.

Ce modèle est utilisé pour les zones urbaines, sous urbaines et rurales. Il représente le modèle de perte de chemin le plus utilisé pour la prédiction de l'intensité du signal et la simulation dans des environnements macros cellulaires.

Pour un terrain en milieu urbaine.

$$PLA(d) = 47.95\text{Log}_{10}(0.01d) + 94.76 \text{ (dB)}$$

Pour un terrain en milieu sous urbaine.

$$PLB(d) = 43.75\text{Log}_{10}(0.01d) + 94.76 \text{ (dB)}$$

Pour un terrain en milieu rurale.

$$PLC(d) = 41.16\text{Log}_{10}(0.01d) + 94.76 \text{ (dB)}$$

#### **3.1.4.2 Modèle COST 231 Hata**

Ce modèle est utilisé pour les macros cellules. Il est essentiellement fait pour les fréquences inférieures à 2 GHz. Dans le but de l'utiliser pour des fréquences supérieures jusqu'à 6GHz, on lui a introduit des corrections.

Le résultat est donné par l'équation suivante :

$$h(\text{db}) = 46.3 + 33.9 \log(f_c) - 13.2 \log(h_{bs}) - A(h_m) + (44.9 - 6.55 \log(h_{bs})) \log(d) + C_m$$

Avec:

$f_c$ : fréquence porteuse du signal en GHz

$h_{bs}$  : hauteur de la BS en mètres.

$h_m$  : hauteur du mobile en mètres.

$d$  : distance entre la BS et le mobile en Km

$C_m$  : terme constant ( $C=0$  dB pour les zones sous urbaines,  $C=3$  dB pour les zones urbaines).

$A(h_m)$ : est un terme correctif dépendant de la hauteur de l'antenne du mobile.

Pour les villes de taille moyenne ou petite.

$$A(h_m) = (1.1 * \log(f_c) - 0.7) * h_m - (1.56 * \log(f_c) - 0.8) \text{dB}.$$

Pour les villes de grande taille:

$$A(h_m) = 3.2 * \log(11.75 * h_m) - 4.97 \text{dB}.$$

Après notre Site Survey, étant donné la situation de nos deux sites, nous avons remarqué que le modèle de propagation approprié était celui en espace libre puisque les antennes émettrice et réceptrice sont en visibilité directe.

### 3.1.4.3 Le modèle de propagation en espace libre

Elle représente l'atténuation subie par le signal pendant la traversée de l'air, toutefois sans y rencontrer un obstacle d'une autre nature. Le modèle de l'affaiblissement du parcours espace libre est habituellement le point de référence duquel tous les modèles de propagation prennent origine. Ce modèle se base sur l'équation de Friis qui montre que la puissance reçue chute beaucoup et elle est calculée comme étant le carré de la distance séparant l'émetteur et le récepteur. En environnement LOS ; le modèle Free Space ou modèle de Friis est spécifié. L'équation suivante montre le pathloss en fonction de la distance:

$$A = 20 \times \log\left(\frac{4\pi}{\lambda}\right) + 20 \times \log(d) \quad (1)$$

$d$  est la distance entre l'émetteur et le récepteur, en mètres.

$\lambda$  est la longueur d'onde du signal, en mètres.

Ou encore :

$$PL(d)=32.4+20\text{Log}(d)+20\text{Log}(f_c) \quad (2)$$

Avec :

d: distance en Km

$f_c$ : fréquence en GHz

### 3.1.5 Le bilan de liaison

Lors des systèmes de transmission par onde radio, le bilan de liaison sert à évaluer l'ensemble des pertes que l'onde émise va subir, ainsi que le rapport signal sur bruit à l'entrée du récepteur.

Dans le cadre du déploiement de notre réseau wifi entre le site d'AKWA et celui de BALI le bilan de liaison, évalué pour le cas d'usage d'antenne Yagi nous a permis de faire les choix qui conviennent.

Nous désirons porter un signal de puissance 100 mW fourni par un AP. Ce signal est émis via une antenne liée à l'AP par un câble, coaxial ayant une atténuation minimale de 0.215 à 1 dB/m d'atténuation. Estimons la longueur totale du câble utilisé (chez l'émetteur et le récepteur) à 20 mètres, ce qui nous donne 4.3 dB, d'atténuation. Le rayon maximal à couvrir serait d'environ 1 Km. L'équation de propagation de FRIIS nous donne la relation:  $P_r = P_e * G_e * G_r / L$  (3)

Considérant  $G_r = G_e$ , nous devons déterminer une approximation des pertes L. Les pertes en espace libre sont données par la relation  $L_{esp} = (4 * \pi * d * f / \lambda)^2$ . (4) Soit  $L_c = 4.3\text{dB}$  la valeur des pertes dans les câbles. Estimons l'ensemble des autres pertes  $L_1$  (Perte de couplage, perte d'alignement, d'inclinaison ...) à 0.5dB, nous obtenons donc un total de pertes  $L = L_{esp} + L_1 + L_c$ . Une application numérique successive à 2.4 GHz permet d'obtenir:  $\lambda = \text{longueur d'onde (célérité/fréquence)} = 12.5\text{cm}$

Pour  $D = 1\text{Km}$ , on a :  $L_{esp} = 100.04 \text{ dB}$

Marge de gain :  $M = 2\text{dB}$

On a donc  $L = 104.84 \text{ dB}$

NB : Les valeurs de pertes sont choisies aux valeurs maximales pour prendre en considération la marge de gain du récepteur et l'améliorer. Cette marge de gain

permet d'anticiper sur les fluctuations qui dégraderaient la qualité de la transmission du milieu de propagation. Ces pertes nous permettront de déterminer les gains d'antennes nécessaires à la transmission du signal pour une portée évaluée à 1 Km. Ainsi, d'après la relation (1) nous pourrions poser:

$$G_e = G_r = (L * P_r / P_e)^{1/2} \quad (5)$$

Pour un AP TP-LINK W5110G émettant à une puissance de 100mW (20dbm), avec un seuil de réception de -90dBm la valeur du gain d'antenne à concevoir vient tout simplement après application numérique, soit :  $G_e = G_r = 10.24 \text{ dB}$

En effet, afin de déterminer la portée maximale à atteindre, le seuil de réception (puissance minimale du signal pouvant être captée par une antenne) ne doit pas être inférieur à celle-ci. Sinon le signal ne sera pas reçu. Le signal émis ne va pas en dehors du rayon estimé et ceci vient délimiter le rayon de surveillance et bien entendu améliorer le contrôle du signal émis.

Seuil de sensibilité	-90 dBm
Marge	2 db
Puissance d'émission du signal	100mW
Gain d'émission	10.24dB
Gain de réception	10.24dB
Pertes d'inclinaison et de couplage	0.5dB
Pertes de propagation	104.84dB
Fréquence	2.4 GHZ
Modèle de propagation	Espace libre
Portée maximale de couverture	1 km environ

**Tableau 3: Bilan de liaison du déploiement du wifi**

### **3.2 Dimensionnement en capacité**

En théorie chaque point d'accès peut supporter 50 personnes, mais dans la cadre de notre travail nos points d'accès servent 20 personnes. 12 personnes dans le site d'AKWA et 8 dans le site de BALI.



Pour un déploiement limité par la capacité, il était nécessaire pour nous de déployer les AP avec un espacement entre ceux-ci suffisant pour servir tous les utilisateurs dans le système. Ainsi avec les données mises à notre disposition par l'administrateur, nous avons pu ressortir les services et les débits moyens des utilisateurs.

Les services offerts à l'externe sont:

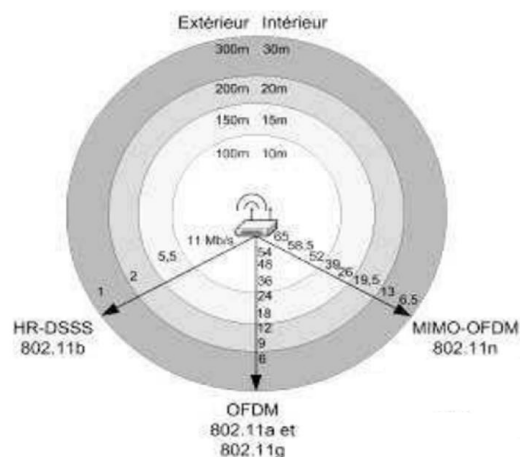
La navigation internet	= 32 kb/s
VOIP sur Skype	= 168kb/s
Le service mail	= 56Kb/s

Et les services offerts en local sont:

La téléphonie sur IP	= 64Kb/s
La visioconférence	= 128kb/s

### 3.2.1 Détermination de la portée d'un AP

Pour la couverture de nos sites, au vu de nos bâtiments nous avons utilisé trois AP: Mais la portée de l'AP dépend de la qualité du bâtiment et des interférences dus au signal. A l'intérieur et à l'extérieur de chaque bâtiment nous avons une portée et un débit qui sont illustrés par la figure ci-dessous.



**Figure19: Débit théorique maximal du signal en fonction de la portée [3]**

De fait, avec un émetteur 802.11g à 20 dBm et un bon récepteur, on peut en théorie, en conditions idéales (pas de bruit ni d'obstacles), obtenir un débit de 11 Mb/s jusqu'à 100 mètres environ, mais au-delà le débit tombera à 5,5 Mb/s, puis à 2 Mb/s et enfin à 1 Mb/s jusqu'à plus de 300 m. Dans la pratique, la portée est souvent plus faible. En outre, le débit réel est souvent deux ou trois fois plus faible que le débit

théorique. Par ailleurs, le débit maximal que l'on peut atteindre est proportionnel à la largeur de la bande de fréquence utilisée. Or, plus on se situe sur des fréquences élevées, plus on a de la place pour exploiter des bandes de fréquences larges, donc plus le débit est important. Cependant, dans le cas du Wifi, les canaux de communication définis pour le 2,4 GHz ont une largeur de 22 MHz alors que les canaux du 5 GHz ont une largeur de 20 MHz. Le débit maximal que l'on peut théoriquement atteindre est donc plus ou moins identique dans les deux cas. Ceci explique pourquoi le 802.11a et le 802.11g offrent tous les deux le même débit maximal, malgré le fait que le 802.11a exploite des fréquences plus élevées que le 802.11g. Cependant, il y a plus de canaux disponibles pour communiquer dans le 5 GHz que dans le 2,4 GHz, donc la capacité totale du 802.11a est plus importante.

### 3.2.2 Détermination du trafic par abonné

Le trafic d'un usager se définit comme le taux d'occupation de la ligne. Généralement, les problèmes de capacité sont inhérents à la liaison descendante (DL). C'est pour cela que nous nous intéressons au lien descendant lors de l'évaluation des besoins en trafic.

$$TDL/abonné = \sum_{i=1}^{ns} (Ds - Dl) \times T0 \quad (6)$$

TDL/abonné : Trafic moyen par abonné pour le lien descendant (Kb/s).

DS-DL: Débit moyen par service.

T0: Taux d'occupation du service.

Ns : Nombre de services.

Il est question dans ce paragraphe d'évaluer si nos points d'accès peuvent supporter le trafic sur internet et en local.

Après une observation faite sur une heure, nous avons obtenu de l'administrateur les valeurs suivantes:

La navigation internet	= 113 Mb/h
VOIP sur Skype	= 591Mb/h
Le service mail	= 197Mb/h
La téléphonie sur IP	= 225Mb/h
La visioconférence	= 450Mb/h

D'après notre formule, nous constatons que le trafic moyen par abonné est de 1576Mb/h ce qui est largement inférieur au débit que le point d'accès supporte pour la même période d'observation. Par conséquent nous pouvons conclure que nos points d'accès peuvent supporter le trafic en local comme sur internet. Ainsi le nombre maximum d'utilisateurs qui peuvent provoquer une saturation sur un point d'accès serait de 25 personnes.

### **3.3 La Mise en œuvre du wifi**

Nous allons aborder le cas du déploiement au sein des locaux de l'entreprise. Dans ce contexte, l'emploi de multiples AP est obligatoire pour obtenir à la fois:

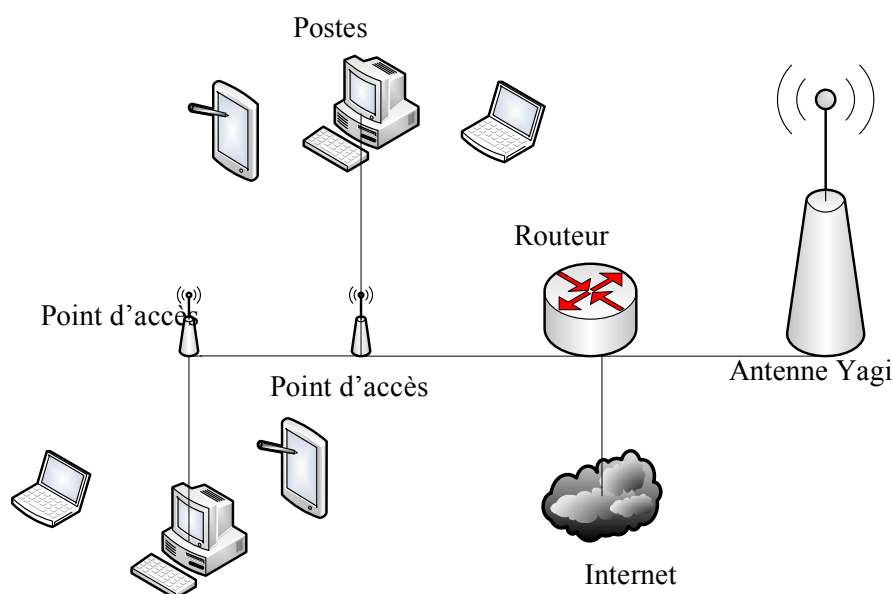
Une bonne couverture radio et éviter ainsi les zones d'ombre.

Une bonne capacité, c'est-à-dire un débit suffisant pour chaque employé, en fonction des applications prévues.

Pour obtenir un bon débit, il était nécessaire pour nous d'utiliser deux points d'accès pour le site D'AKWA puisque le bâtiment est sur deux niveaux, nous avons installé à chaque niveau un AP pour une bonne répartition des charges et pour une bonne couverture des deux niveaux.

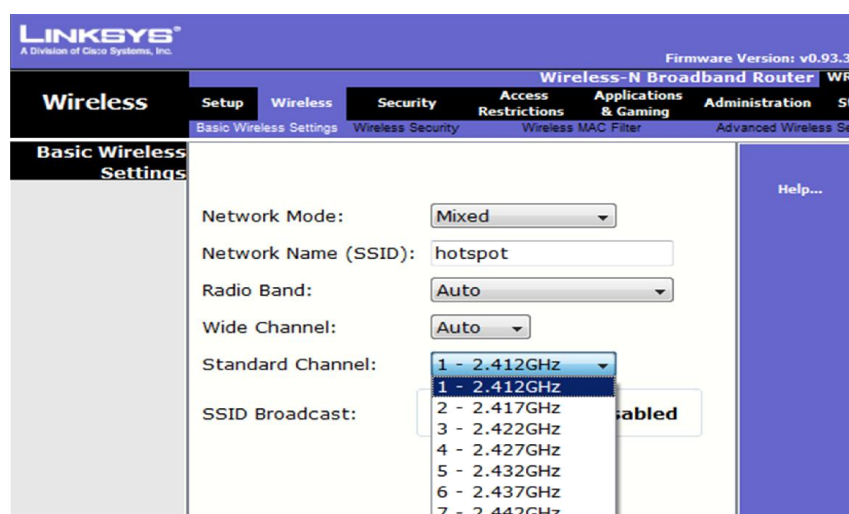
#### **3.3.1 Déploiement des sites**

Pour le déploiement de nos sites, nous utilisons d'abord le simulateur Cisco packet tracer pour vérifier la faisabilité de nos installations, avant de passer à la matérialisation qui sera représentée par Microsoft Visio.

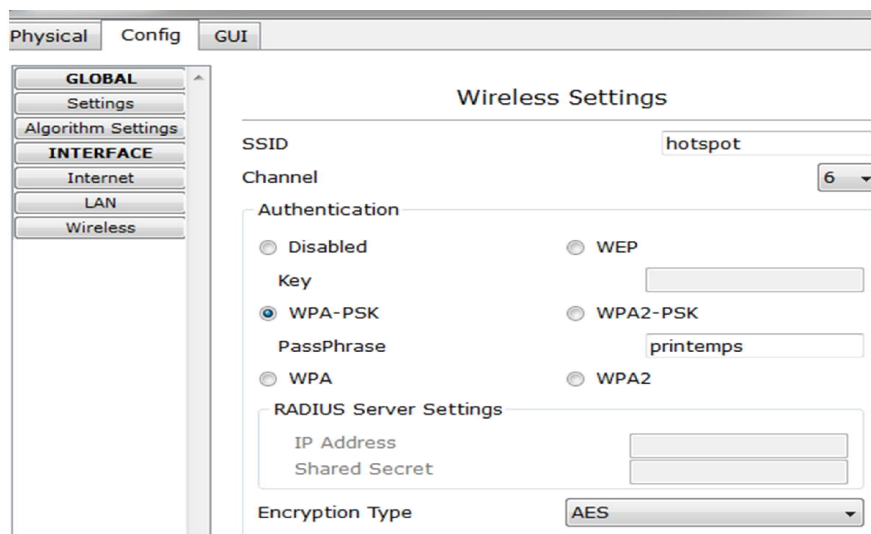


**Figure 20: Architecture du site d'AKWA**

Nous avons utilisé deux AP linksys que nous avons relié par un câble Ethernet. Nous avons mis chaque AP sur un canal pour éviter les interférences entre les AP. Mais nous avons utilisé la même plage d'adresse pour signifier que nous sommes dans le même sous réseau. Nous avons également utilisé un SSID, deux mots de passe pour éviter qu'une machine ne puisse confondre le point d'accès auquel elle doit s'associer. Ensuite nous relierons nos AP au routeur qui va permettre de router les paquets vers internet et d'internet vers nos machines.



**Figure 21: Choix des fréquences et des canaux**



**Figure 22: Entrée des paramètres des AP**

D'après le test de connectivité, nous constatons que le Ping entre les machines situées de part et d'autre des accès point se fait avec succès. Et par conséquent la communication est possible.

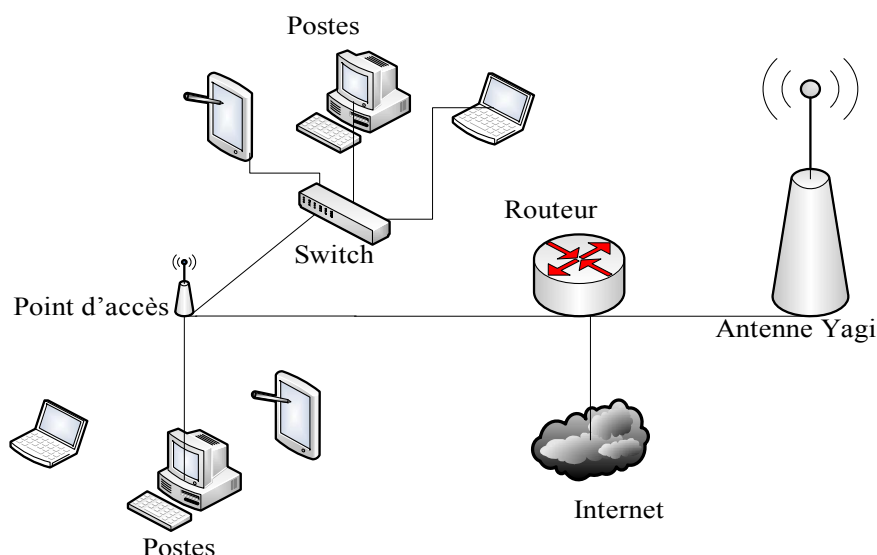
```
PC>PING 192.168.0.101

Pinging 192.168.0.101 with 32 bytes of data:

Reply from 192.168.0.101: bytes=32 time=40ms TTL=128
Reply from 192.168.0.101: bytes=32 time=15ms TTL=128
Reply from 192.168.0.101: bytes=32 time=15ms TTL=128
Reply from 192.168.0.101: bytes=32 time=21ms TTL=128

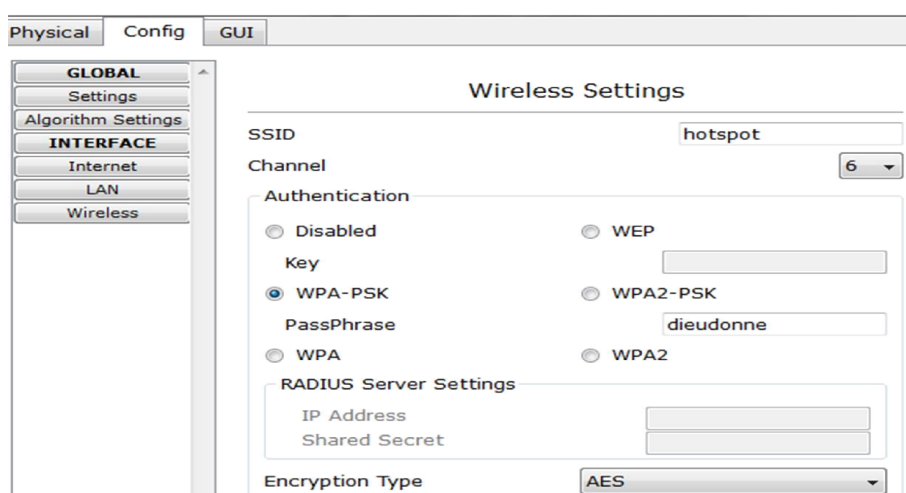
Ping statistics for 192.168.0.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 15ms, Maximum = 40ms, Average = 22ms
```

**Figure 23: Test de connectivité**



**Figure 24: Architecture du site de BALI**

Nous avons utilisé un accès point, que nous avons relié à un Switch pour pouvoir augmenter le nombre d'utilisateurs fixe. Et évidemment à un routeur qui va permettre de router les paquets vers internet et d'internet vers nos machines. Techniquement nous utilisons une plage d'adresse pour toutes les machines dans le site. Une sécurité WPA personnelle, un SSID, un mot de passe et les commandes au niveau de l'interface du routeur pour prendre en considération le routage des paquets.



**Figure 25: Entrée des paramètres d'AP**

Une fois fini notre déploiement, nous passons à la phase de test de connectivité; pour s'assurer que les utilisateurs peuvent communiquer sans souci. Ainsi lorsque cela est fait sans problèmes, nous concluons avec certitude que la communication est possible.

```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.0.5: bytes=32 time=24ms TTL=128
Reply from 192.168.0.5: bytes=32 time=18ms TTL=128
Reply from 192.168.0.5: bytes=32 time=18ms TTL=128
Reply from 192.168.0.5: bytes=32 time=16ms TTL=128

Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 24ms, Average = 19ms
```

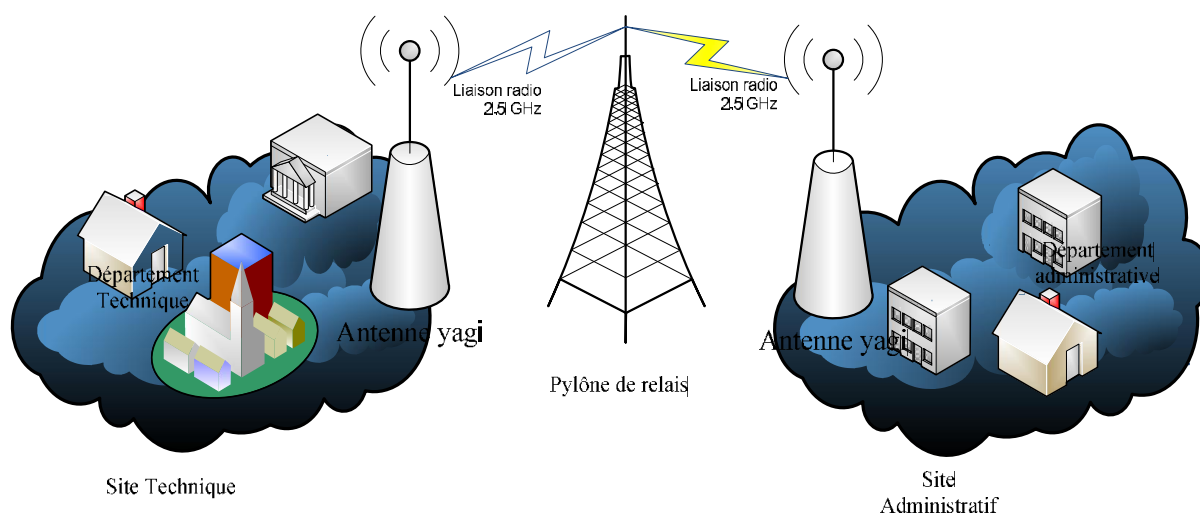
**Figure 26: Test de connectivité**

En sommes, après le déploiement de nos sites, il était question pour nous de pouvoir étendre notre réseau wifi pour prendre une seule connexion chez le fournisseur d'accès internet.

### **3.4 Expansion du réseau wifi**

L'interconnexion de nos deux sites pour une plateforme de visioconférence via la transmission de la voix et de la vidéo en temps réel nécessite des débits importants. En outre, puisque nos différents sites sont distants de plusieurs mètres, une solution de liaison par onde Wifi serait idéale. En effet, grâce au WDS (Wireless Distribution System) régit par l'IEEE sous la norme 802.11n, il devient possible d'étendre un réseau Wifi interne à des Kms selon des débits très supérieurs à 2Mbits/s. Cette solution très économique est avantageuse du même point de vue que tout réseau WLAN Wifi, présente aussi les mêmes inconvénients que ce dernier, notamment son déploiement sans licence. Nous prévoyions à cet effet les politiques de sécurité en envisageant que l'on puisse être confronté à un éventuel déplacement. Pour permettre la communication entre nos sites, une solution consiste à une interconnexion par fibre optique. Une autre à l'usage des amplificateurs ou des antennes relais en vue de régénérer le signal partant d'un point d'émission à la réception. Mais pour des raisons de cout, nous avons estimé qu'ils étaient judicieux d'utiliser des antennes relais.

Nous allons tout d'abord ressortir le schéma synoptique de notre expansion, ensuite tenir compte des effets environnementale, les perturbations radio, et enfin le schéma simplifié de notre expansion.



**Figure 27: Synoptique sur l'expansion du réseau wifi**

D'après notre schéma, nous avons utilisé deux antennes directionnelles de type yagi au sein de chaque site et nous les avons relié à un accès point à l'aide de câbles coaxiale. Nous utilisons ensuite un pylône de relais qui reçoit l'onde émis sous forme de signal électromagnétique augmente sa puissance et le revoie à l'antenne réceptrice.

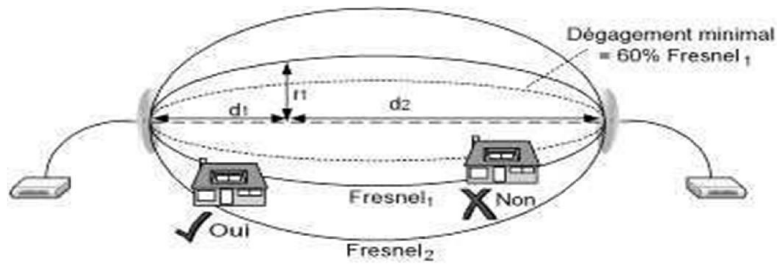
### 3.4.1 L'étude de l'environnement

L'idéal pour une connexion de point à point est que les deux stations soient en vision directe, ou Line of Sight (LOS), avec aussi peu d'interférences multipath que possible. Ainsi, avec les ondes radio, la notion de vision directe est bien plus floue qu'avec la lumière visible. Le fait qu'aucun obstacle ne se trouve sur l'axe entre l'émetteur et le récepteur, ne garantit pas une bonne propagation des ondes. Il faut également qu'aucun obstacle ne se trouve à proximité de cet axe, sinon une partie importante de l'énergie du signal sera perdue.

#### 3.4.1.1 Le dégagement minimal

Nous considérons que l'énergie transmise de l'émetteur radio vers le récepteur se propage essentiellement au sein d'un ellipsoïde de révolution (zone de Fresnel) délimitée par la « surface de Fresnel ». L'ellipsoïde de Fresnel comporte une infinité de zones, mais celle qui nous intéresse est la première zone de Fresnel délimitée par la première surface de Fresnel.





**Figure 28 : Ellipsoïde de Fresnel et le dégagement minimal [3]**

Puisque l'essentiel de l'énergie du signal est diffusé dans la première zone de Fresnel, nous évitons tout obstacle au cœur de cette zone. En pratique, nous allons dégager au moins 60 % de cette zone (au centre) pour avoir une bonne réception. Ainsi nous obtenons le dégagement minimal  $d_{min}$ , en tout point de l'axe entre l'émetteur et le récepteur, par la formule suivante:

$$d_{min} = 60 \% \times \sqrt{\lambda \times \frac{d_1 \times d_2}{d_1 + d_2}} \quad (7)$$

Dans notre cas où les deux stations sont distantes de 1 000 mètres et qu'un obstacle se situe non loin d'un point de l'axe situé à 300 mètres de l'émetteur, nous pouvons calculer la distance minimale entre ce point de l'axe et l'obstacle par la formule suivante :

$$d_{min} = 60 \% \times \sqrt{0,125 \times \frac{700 \times 300}{700 + 300}} \cong 3,07 \text{ m} \quad (8)$$

Ainsi on s'assure que l'obstacle est bien à plus de 3 mètres de l'axe entre l'émetteur et le récepteur, sinon une partie importante du signal sera perdue. Par exemple, si la moitié de la zone de Fresnel est obstruée par un obstacle, alors plus de 75 % de la puissance du signal est perdue. Ce qui est énorme car le signal porte alors deux fois moins loin.

### 3.4.1.2 La hauteur minimale

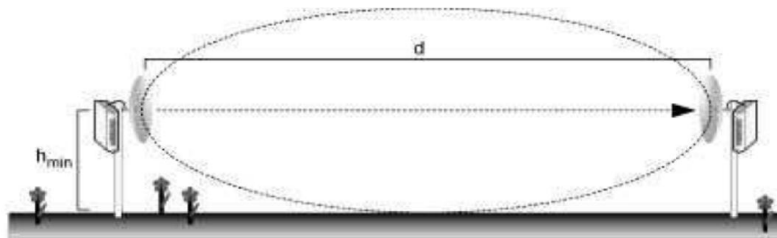
Bien entendu, le sol lui-même est un obstacle, donc nous devons faire le calcul pour chaque point où le sol est susceptible d'être dans la zone « interdite ». Si le sol est plat et que les antennes sont toutes deux à la même hauteur, alors le point pour lequel nous devons faire le calcul est à mi-chemin entre l'émetteur et le récepteur, là où

l'ellipsoïde est le plus large. À partir de la formule précédente, nous trouvons la hauteur minimale à laquelle nous installons nos deux antennes pointées l'une vers l'autre sur un terrain plat.

$$h_{\min} = 30 \% \times \sqrt{\lambda \times d} \quad (9)$$

d est la distance entre les stations.

Dans notre cas, les stations sont à une distance  $d = 1\,000$  mètres l'une de l'autre. Donc nous calculons qu'elles doivent être installées au moins à 3,35 mètres de hauteur (idéalement sur un mât ou sur le toit d'un bâtiment).



**Figure 29: La hauteur minimale pour une connexion de point à point [3]**

### 3.4.2 Les perturbations radio

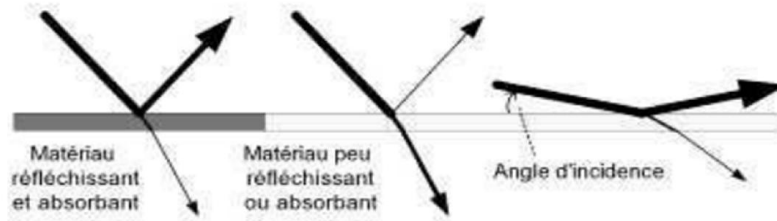
Malgré une étude satisfaisante sur l'environnement auquel nous avons étendu notre réseau, un certain nombre de perturbations ceux sont invités pour troubler nos prédictions. Il s'agit: du bruit, des obstacles, des réflexions et la diffraction.

#### ➤ Le bruit

Le bruit peut perturber énormément les communications en provoquant une perte importante de paquets. Mais nous avons pu avoir le RSB suffisamment élevé, pour que la communication soit possible, avec une puissance importante du signal de réception.

#### 3.4.2.1 L'absorption et la réflexion

Lorsqu'un obstacle se situe entre l'émetteur et le récepteur, les ondes radio sont en partie reflétées et en partie ou en totalité absorbées par l'obstacle. La portion du signal qui parvient à traverser l'obstacle est donc affaibli. C'est donc pour cette raison que nous sommes obligés d'éviter les obstacles lors de notre expansion.

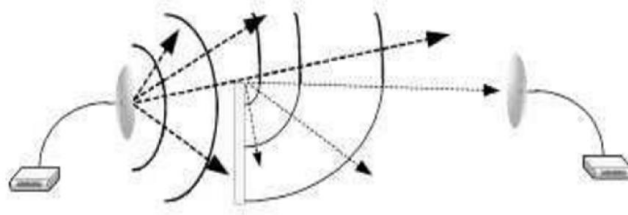


**Figure 30: Absorption et réflexion [1]**

Pour limiter ce problème, une solution simple consiste à placer nos antennes en hauteur. En outre, si nous pouvons positionner les utilisateurs de telle sorte qu'ils ne soient pas entre leur ordinateur et l'AP, nous améliorons nettement la réception. Puisque l'absorption et la réflexion dépendent naturellement de l'épaisseur de l'obstacle et du matériau dont il est constitué : bois, béton, métal, plastique, verre, eau ou autres, à titre indicatif, le béton et le métal absorbent davantage le signal que le plastique ou le verre. Un mur de 50 cm de béton est suffisant pour absorber la majeure partie du signal Wifi, alors que plusieurs façades successives en plastique laisseront en général passer une bonne partie du signal. Un point important: l'eau absorbe très nettement les ondes à 2,4 GHz. La première conséquence de cette observation est le fait qu'une liaison Wifi à l'extérieur est assez sensible à la météo. Un jour de pluie ou de brouillard, la connexion risque d'être interrompue ou perturbée; de même, le bois, selon sa teneur en eau, arrêtera plus ou moins le signal. Pour finir, les êtres humains, qui sont constitués en grande partie d'eau, absorbent une partie importante du signal Wifi.

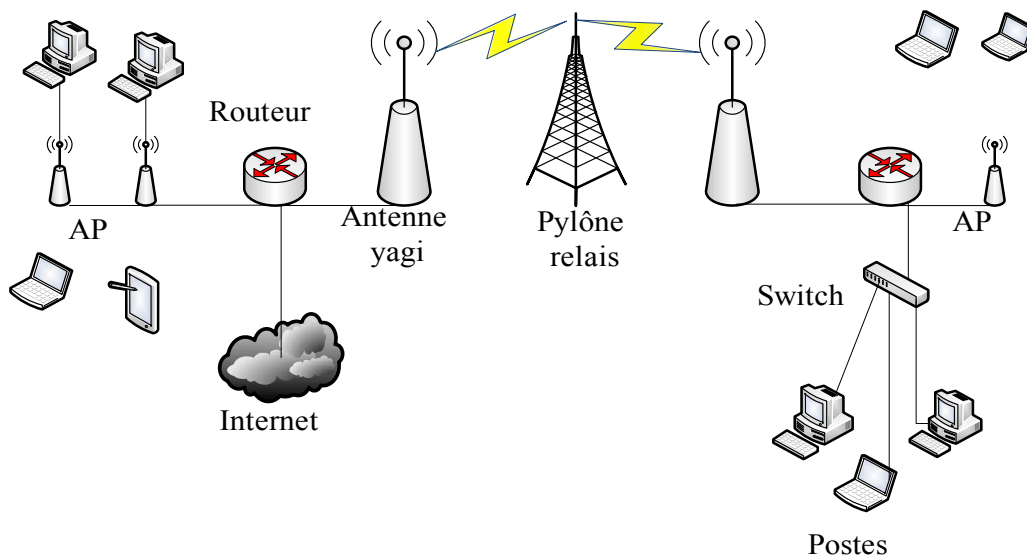
#### **3.4.2.2 La diffraction**

Elle peut être expliquée brièvement par le principe de Huygens-Fresnel: chaque point par lequel passe une onde peut être considéré comme une nouvelle source de l'onde, émise dans toutes les directions. En l'absence d'obstacles, la somme des ondes émises donne un front d'onde qui se propage normalement, dans une direction, car les ondes émises dans les autres directions s'annulent mutuellement. Toutefois, dès que le front de l'onde se heurte à un obstacle, les ondes émises par les points situés aux extrémités de cet obstacle se propagent dans toutes les directions et ne sont plus annulées par les ondes voisines: l'obstacle peut ainsi être contourné, en particulier si ses bords sont saillants.



**Figure 31: La diffraction [1]**

Notons que les phénomènes de diffraction sont d'autant plus importants que la longueur d'onde est grande, donc la fréquence faible. Il y a donc plus de diffraction pour les fréquences de 2,4 GHz que pour les fréquences de 5 GHz. Mais curieusement le 802.11b et le 802.11g contournent donc mieux les obstacles que le 802.11a.



**Figure 32: Architecture globale de l'expansion du réseau wifi**

Lors de l'expansion de notre réseau, nous avons utilisé un certain nombre d'équipements à savoir: les points d'accès qui permettent aux utilisateurs de se connecter au réseau. Les routeurs qui permettent de router nos paquets sur internet. Les antennes yagi qui permettent d'émettre et de recevoir l'onde radio. Le pylône de relais qui permet de relayer et d'amplifier le signal électromagnétique venant des deux antennes côté émission et réception. Par la suite, compte tenu des paramètres environnementaux nous avons positionné nos antennes à 3.35m sur un mat au-dessus de la toiture des bâtiments. Nous avons également veillé à ce qu'il n'y ait pas d'obstacles de part et d'autre des deux côtés de la surface de propagation des ondes. Enfin après la

fourniture du service internet par un FAI (Fournisseur d'Accès Internet), nous passons à des vérifications qui se sont avérées concluantes puisque le service internet était disponible au sein des deux sites et la communication par mail se faisait de façon claire. Mais jusqu'à ce moment nous étions dans l'incapacité de faire la visioconférence, raison pour laquelle par la suite, nous allons axer notre travail sur l'étude et l'interopérabilité entre la technologie wifi et l'application à la visioconférence.

## **Conclusion**

Au terme de ce chapitre il ressort que cette technologie peut être utilisée comme support de transmission de toutes formes d'ondes et peut atteindre des objectifs de couverture et de qualité très intéressants, il suffira juste d'appliquer certaines techniques comme: L'amélioration du gain des antennes en les rendant fortement directives, se rassurer au maximum lors du déploiement que le premier ellipsoïde de Fresnel est bien dégagé entre l'émetteur et le récepteur.

## **CHAPITRE 4: MISE EN PLACE D'UNE PLATEFORME DE VISIOCONFERENCE MULTIPLE**

### **Introduction**

Notons tout d'abord que le wifi, étant une technologie de la norme 802.11 permettant des connexions et des communications distantes, fait aussi l'objet d'une possibilité d'insertion de diverses applications dont l'une est la visioconférence qui incorpore dans ses fonctionnalités l'audioconférence et les appels vidéo ceci en vue de faciliter les échanges entre les différentes filiales d'une entreprise.

#### **4.1.1 Définition**

La visioconférence est une technologie qui permet, à partir d'un ordinateur, de communiquer avec un interlocuteur distant et de le voir en temps réel dans une fenêtre virtuelle à l'écran. Elle permet à ses participants, disséminés sur plusieurs sites distants, de communiquer en bénéficiant d'une transmission du son, de l'image et de tout autre type de données. Cette technologie permet donc une collaboration accrue entre les différents acteurs de la chaîne de valeur de toute entreprise. La visioconférence supprime une partie des inconvénients liée à la distance, puisqu'elle autorise le travail sur un fichier ou une application de manière simultanée. C'est finalement un peu comme si les participants se trouvaient dans la même salle et travaillaient en face à face.

#### **4.1.2 Fonctionnement**

La voix de chaque participant est captée par un microphone branché à son ordinateur. L'image de chaque participant est captée par une caméra branchée sur son ordinateur. Ce son et cette image sont transmis aux autres participants grâce à l'application de visioconférence, via le réseau Internet.

Les usages les plus courants sont:

- ✓ L'apprentissage et la formation à distance.
- ✓ La retransmission de séminaires et d'événements.
- ✓ La télé-ingénierie et la télé-médecine.
- ✓ Le conseil par des experts.
- ✓ La conférence personnelle.

✓ Les réunions de travail.

Les applications liées à l'utilisation de la visioconférence sont nombreuses. Le principe reste le même: la communication est facilitée alors que les interlocuteurs sont éloignés géographiquement, la possibilité de "voir et entendre à distance" en temps réel, et la possibilité de travailler conjointement sur le même support, ce qui en fait un outil complet pour le travail à distance. Lors des transmissions vidéo et son, le risque d'avoir une image saccadée est grand. Il y a plusieurs raisons à cela. D'abord, plus l'image est grande, plus elle est lourde en informations et donc longue à transférer. Ainsi, en réduisant la taille de la vidéo, l'image sera déjà bien meilleure. Deuxièmement, cela dépend de la qualité de service (QOS) et du débit de transmission. Plus le débit sera élevé, meilleure sera la qualité de l'image. Enfin, la webcam véhicule uniquement les points qui changent d'une image à l'autre. En bougeant peu, juste les lèvres, l'image sera bonne. A l'inverse, en bougeant les mains ou en se déplaçant, l'image sera moins nette.

#### **4.1.3 Différents modes de transmission en visioconférence**

Pour établir une visioconférence entre deux sites, deux modes de transmission sont aujourd'hui privilégiés : le réseau Numérique d'une part et les réseaux IP, c'est à dire le réseau Internet dans son aspect mondial, et les réseaux informatiques locaux (de type Ethernet par exemple...) qui y sont connectés. Des différences fondamentales existent. Les deux modes de diffusion sont technologiquement très différents et s'appuient sur deux familles de normes spécifiques: l'un est plus ancien, et bien ancré dans les habitudes, le second est plus récent et se développe actuellement de manière importante même s'il n'est pas toujours le plus performant. Les liaisons entre les sites distants sont en temps réel et en full duplex (les liaisons sont bidirectionnelles et chaque site est simultanément émetteur et récepteur). Les débits sont identiques dans les deux sens. La majorité des matériels commercialisés peuvent fonctionner sous IP. Un grand nombre d'entre eux adoptent la double compatibilité IP et RNIS.

Cependant, notre étude portera sur le mode de visioconférence sur IP qui répond plus aisément à nos attentes de part l'efficacité de ses différents protocoles à savoir H.323 et SIP.

#### **4.1.3.1 Mode de visioconférence sur IP**

Dans le cadre d'une visioconférence sous IP, les échanges sont symétriques. Le débit pour chacune des directions est la somme des débits nécessaires pour l'audio, la vidéo, et les données. La qualité d'une visioconférence est également tributaire des caractéristiques du réseau informatique local. Sur un réseau de type Ethernet, les débits sont élevés, dans la majorité des cas 100 Mb/s. Même si la bande passante disponible est à partager entre tous les utilisateurs du réseau. Elle est généralement suffisante pour assurer le transit des données nécessaires à une visioconférence.

#### **4.1.4 Les protocoles et les codecs de fonctionnement de la visioconférence**

Pour ces deux méthodes de transmission, des normes spécifiques ont été établies afin de garantir l'interopérabilité de tous les matériels de visioconférence. La norme H323 concerne les réseaux à commutation de paquets, c'est à dire notamment aux réseaux IP. Elles ont été développées par l'ITU (International Télécommunication Union). Les deux normes ou encore protocoles H.323 et SIP correspondent à un assemblage de normes spécifiques pour tous les domaines concernés. Ces dernières peuvent être identiques pour H.323 et SIP ou bien différentes.

##### **4.1.4.1 Le Protocole H.323**

Le standard H.323 fournit, depuis son approbation en 1996, un cadre pour les communications audio, vidéo et de données sur les réseaux IP. Il a été développé par l'ITU (International Télécommunications Union) pour les réseaux qui ne garantissent pas une qualité de service (QoS), tels qu'IP sur Ethernet, Fast Ethernet et Token Ring. Il est présent dans plus de 30 produits et il concerne le contrôle des appels, la gestion multimédia, la gestion de la bande passante pour les conférences point-à-point et multipoints. H.323 traite également de l'interfaçage entre le LAN et les autres réseaux. Le protocole H.323 fait partie de la série H.32x qui traite de la vidéoconférence au travers différents réseaux. Il inclut H.320 et H.324 liés aux réseaux ISDN (Integrated Service Data Network) et PSTN (Public Switched Telephone Network). Plus qu'un protocole, H.323 crée une association de plusieurs protocoles différents et qui peuvent être regroupés en trois catégories: La signalisation, la négociation de codec, et le transport de l'information.



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

Le terminal peut être un ordinateur, un combiné téléphonique, un terminal spécialisé pour la vidéoconférence ou encore un télécopieur sur Internet. Le minimum imposé par H.323 est qu'il mette en œuvre la norme de compression de la parole G.711, qu'il utilise le protocole H.245 pour la négociation de l'ouverture d'un canal et l'établissement des paramètres de la communication, ainsi que le protocole de signalisation Q.931 pour l'établissement et l'arrêt des communications.

Le terminal possède également des fonctions optionnelles, notamment, pour le travail en groupe et le partage des documents. Il existe deux types de terminaux H.323, l'un de haute qualité (pour une utilisation sur LAN), l'autre optimisé pour de petites largeurs de bandes (28,8/33,6 kbit/s – G.723.1 et H.263).

- **Gateway ou les passerelles vers des réseaux classiques (RTC, RNIS, etc.)**

Les passerelles H.323 assurent l'interconnexion avec les autres réseaux: (H.320/RNIS), les modems H.324, téléphones classiques, etc. Elles assurent la correspondance de signalisation de Q.931, la correspondance des signaux de contrôle et la cohésion entre les médias (multiplexage, correspondance des débits, transcodage audio).

- **Gatekeeper ou les portiers**

Dans la norme H323, Le Gatekeeper est le point d'entrée au réseau pour un client H.323. Il définit une zone sur le réseau, appelée zone H.323 (voir figure 3 ci-dessous), regroupant plusieurs terminaux, Gateways et MCU dont il gère le trafic, le routage LAN, et l'allocation de la bande passante. Les clients ou les Gateway s'enregistrent auprès du Gatekeeper dès l'activation de celui-ci, ce qui leur permet de retrouver n'importe quel autre utilisateur à travers son identifiant fixe obtenu auprès de son Gatekeeper de rattachement.

- **Les fonctions du Gatekeeper:**

La translation des alias H.323 vers des adresses IP, selon les spécifications RAS (Registration/Admission/Status).

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

La gestion de la bande passante, permettant à l'administrateur du réseau de limiter le nombre de visioconférences simultanées.

Concrètement une fraction de la bande passante est allouée à la visioconférence pour ne pas gêner les applications critiques sur le LAN et le support des conférences multipoint.

- **Les MCU**

Les contrôleurs multipoint appelés MCU (Multipoint Control Unit) offrent aux utilisateurs la possibilité de faire des visioconférences à trois terminaux et plus en « présence continue » ou en « activation à la voix ». Une MCU consiste en un Contrôleur Multipoint (MC), auquel est rajouté un ou plusieurs Processeurs Multipoints (MP). Le MC prend en charge les négociations H.245 entre tous les terminaux pour harmoniser les paramètres audio et vidéo de chacun. Il contrôle également les ressources utilisées. Mais le MC ne traite pas directement avec les flux

audio, vidéo ou données, c'est le MP qui se charge de récupérer les flux et de leurs faire subir les traitements nécessaires. Un MC peut contrôler plusieurs MP distribués sur le réseau et faisant partie d'autres MCU.

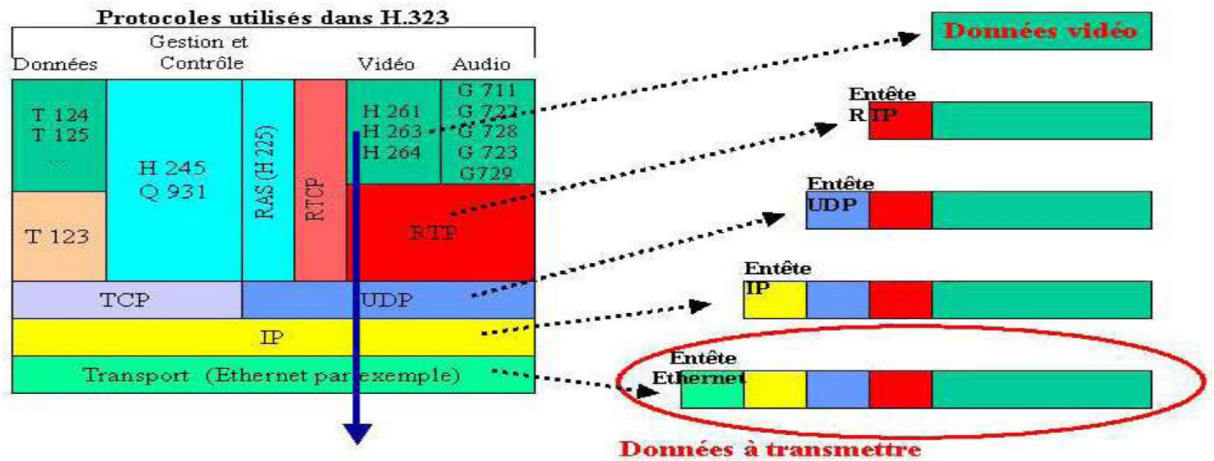
### ➤ **Avantages de la technologie H323**

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

- ❖ 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.
- ❖ Chaque terminal H.323 peut procéder à l'ajustement de la bande passante et la modification du débit en fonction du comportement du réseau en temps réel (latence, perte de paquets et gigue).
- ❖ Support Multipoint: H.323 permet de faire des conférences multipoint via une structure centralisée de type MCU (Multipoint Control Unit) ou en mode ad-hoc. Support Multicast: H.323 permet également de faire des transmissions en multicast.
- ❖ Interopérabilité: H.323 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.
- ❖ 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 grâce aux spécifications T.120.

### ❖ **Les inconvénients de la technologie H.323:**

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



**Figure 33: Différentes normes du protocole H323 [2]**

#### 4.1.4.2 Protocole SIP

Le protocole SIP (Session Initiation Protocol) est un protocole normalisé et standardisé par l'IETF (décrit par le RFC 3261 qui rend obsolète le RFC 2543, et complété par le RFC 3265) qui a été conçu pour établir, modifier et terminer des sessions multimédia. 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). SIP ne transporte pas les données échangées durant la session comme la voix ou la vidéo. SIP étant indépendant de la transmission des données, tout type de données et de protocoles peut être utilisé pour cet échange. Cependant le protocole RTP (Real-time Transport Protocol) assure le plus souvent les sessions audio et vidéo. SIP remplace progressivement H323. SIP est le standard ouvert de VOIP, interopérable, le plus étendu et vise à devenir le standard des télécommunications multimédia (son, image, etc.). Skype par exemple, qui utilise un format propriétaire, ne permet pas l'interopérabilité avec un autre réseau de voix sur IP et ne fournit que des passerelles payantes vers la téléphonie standard. SIP n'est donc pas seulement destiné à la VOIP mais pour de nombreuses autres applications telles que la visiophonie, la messagerie instantanée, la réalité virtuelle ou même les jeux vidéo.

##### ➤ Principe de fonctionnement

Puisque on choisira le protocole SIP pour effectuer notre travail, on s'approfondira à expliquer les différents aspects, caractéristiques qui font du protocole

SIP un bon choix pour l'établissement de la session, les principales caractéristiques du protocole SIP sont:

- **Fixation d'un compte SIP**

Il est important de s'assurer que la personne appelée soit toujours joignable. Pour cela, un compte SIP sera associé à un nom unique. Par exemple, si un utilisateur d'un service de voix sur IP dispose d'un compte SIP et que chaque fois qu'il redémarre son ordinateur, son adresse IP change, il doit cependant toujours être joignable. Son compte SIP doit donc être associé 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 quel que soit son emplacement. Ce compte sera identifiable via son nom (ou pseudo).

- **Gestion des participants**

Durant une session d'appel, de nouveaux participants peuvent rejoindre les participants d'une session déjà ouverte en participant directement, en étant transférés ou en étant mis en attente (cette particularité rejoint les fonctionnalités d'un PABX par exemple, où l'appelant peut être transféré vers un numéro donné ou être mis 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). Le numéro SIP est unique pour chaque utilisateur.

- **Rôle des composants**

Dans un système SIP on trouve deux types de composantes, les agents utilisateurs (UAS, UAC) et un réseau de serveurs (Registrar, Proxy).

L'UAS (User Agent Server) représente l'agent de la partie appelée. C'est une application de type serveur qui contacte l'utilisateur lorsqu'une requête SIP est reçue. Et elle renvoie une réponse au nom de l'utilisateur.

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

Le Registrar est un serveur qui gère les requêtes REGISTER envoyées par les Users Agents pour signaler leur emplacement courant. Ces requêtes contiennent donc une adresse IP, associée à une URI, qui seront stockées dans une base de données.

Les URI SIP sont très similaires dans leur forme à des adresses email: sip:utilisateur@domaine.com. Des mécanismes d'authentification permettent d'éviter que quiconque puisse s'enregistrer avec n'importe quelle URI.

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

#### ➤ **Avantages et inconvénients**

- Ouvert, standard, simple et flexible sont les principaux atouts du protocole SIP, voilà en détails ces différents avantages :
- Ouvert: les protocoles et documents officiels sont détaillés et accessibles à tous en téléchargement.
- Standard: l'IETF a normalisé le protocole et son évolution continue par la création ou l'évolution d'autres protocoles qui fonctionnent avec SIP.
- Flexible: SIP est également utilisé pour tout type de sessions multimédia (voix, vidéo, mais aussi musique, réalité virtuelle, etc.).
- Téléphonie sur réseaux publics: Il existe de nombreuses passerelles (services payants) vers le réseau public de téléphonie (RTC, GSM, etc.) permettant d'émettre ou de recevoir des appels vocaux.
- Points communs avec H323 : l'utilisation du protocole RTP et quelques codecs son et vidéo sont en commun.
- Par contre une mauvaise implémentation ou une implémentation incomplète du protocole SIP dans les User Agents peut perturber le fonctionnement ou générer du trafic superflu sur le réseau.

- Un autre inconvénient est le faible nombre d'utilisateurs: SIP est encore peu connu et utilisé par le grand public, n'ayant pas atteint une masse critique, il ne bénéficie pas de l'effet réseau.

## **4.2 Protocoles de Transport**

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

### **4.2.1 Protocole RTP**

RTP (Real time Transport Protocol), standardisé en 1996, est un protocole qui a été développé par l'IETF afin de faciliter le transport temps réel de bout en bout des flots de données audio et vidéo sur les réseaux IP, c'est à dire sur les réseaux de paquets. RTP est un protocole qui se situe au niveau de l'application et qui utilise les protocoles sous-jacents de transport TCP ou UDP. Mais l'utilisation de RTP se fait généralement au-dessus d'UDP ce qui permet d'atteindre plus facilement le temps réel. Les applications temps réels comme la parole numérique ou la visioconférence constitue un véritable problème pour Internet. Mais qui dit application temps réel, dit présence d'une certaine qualité de service (QoS). RTP est un protocole qui se trouve dans un environnement multipoint, donc on peut dire que RTP possède à sa charge, la gestion du temps réel, mais aussi l'administration de la session multipoint.

#### **• Fonctions de RTP**

Le protocole RTP a pour but d'organiser les paquets à l'entrée du réseau et de les contrôler à la sortie. Ceci de façon à reformer les flux avec ses caractéristiques de départ. RTP est un protocole de bout en bout, volontairement incomplet et pour s'adapter aux besoins des applications. Il sera intégré dans le noyau de l'application. Il laisse la responsabilité du contrôle aux équipements d'extrémité. Il est aussi un protocole adapté aux applications présentant des propriétés temps réel. IL permet ainsi de: Mettre en place un séquençement des paquets par une numérotation et ce afin de permettre ainsi la détection des paquets perdus. Ceci est un point primordial dans la reconstitution des données. Mais il faut savoir quand même que la perte d'un paquet n'est pas un gros problème si les paquets ne sont pas perdus en trop grands nombres. Cependant il est très important de savoir quel est le paquet qui a été perdu afin de



pouvoir pallier à cette perte. Identifier le contenu des données pour leurs associer un transport sécurisé et reconstituer la base de temps des flux (horodatage des paquets: possibilité de resynchronisation des flux par le récepteur). L'identification de la source c'est à dire l'identification de l'expéditeur du paquet. Dans un multicast l'identité de la source doit être connue et déterminée. Transporter les applications audio et vidéo dans des trames (avec des dimensions qui sont dépendantes des codecs qui effectuent la numérisation). Ces trames sont incluses dans des paquets afin d'être transportées et doivent, de ce fait, être récupérées facilement au moment de la phase de segmentation des paquets afin que l'application soit décodée correctement.

#### ➤ **Avantages et inconvénients**

Le protocole RTP permet de reconstituer la base de temps des différents flux multimédia (audio, vidéo, etc.); de détecter les pertes de paquets; et d'identifier le contenu des paquets pour leur transmission sécurisée. Par contre, il ne permet pas de réserver des ressources dans le réseau ou d'apporter une fiabilité dans le réseau. Ainsi il ne garantit pas le délai de livraison.

#### **4.2.2 Protocole RTCP**

Le protocole RTCP est fondé sur la transmission périodique de paquets de contrôle à tous les participants d'une session. C'est le protocole UDP (par exemple) qui permet le multiplexage des paquets de données RTP et des paquets de contrôle RTCP. Le protocole RTP utilise le protocole RTCP, Real-time Transport Control Protocol, qui transporte les informations supplémentaires suivantes pour la gestion de la session. Les récepteurs utilisent RTCP pour renvoyer vers les émetteurs un rapport sur la QoS. Ces rapports comprennent le nombre de paquets perdus, le paramètre indiquant la variance d'une distribution (plus communément appelé la gigue: c'est à dire les paquets qui arrivent régulièrement ou irrégulièrement) et le délai aller-retour. Ces informations permettent à la source de s'adapter, par exemple, de modifier le niveau de compression pour maintenir une QoS. Parmi les principales fonctions qu'offre le protocole RTCP sont les suivants: Une synchronisation supplémentaire entre les médias: Les applications multimédias sont souvent transportées par des flots distincts. Par exemple, la Voix, l'image ou même des applications numérisées sur plusieurs niveaux hiérarchiques peuvent voir les flots gérées et suivre des chemins différents.



L'identification des participants à une session: en effet, les paquets RTCP contiennent des informations d'adresses, comme l'adresse d'un message électronique, un numéro de téléphone ou le nom d'un participant à une conférence téléphonique. Le contrôle de la session: en effet le protocole RTCP permet aux participants d'indiquer leur départ d'une conférence téléphonique (paquet Bye de RTCP) ou simplement de fournir une indication sur leur comportement. Le protocole RTCP demande aux participants de la session d'envoyer périodiquement les informations citées ci-dessus. La périodicité est calculée en fonction du nombre de participants de l'application. On peut dire que les paquets RTP ne transportent que les données des utilisateurs. Tandis que les paquets RTCP ne transportent en temps réel, que de la supervision.

### **4.3 Les codecs**

On appelle CODEC l'entité chargée de la compression des données audio ou vidéo dans un sens et de leur décompression dans le sens contraire. On distingue les codecs audio et vidéo.

#### **4.3.1 Codecs audio**

Les codecs les plus utilisés ici sont:

G722: Normalisée par l'Union Internationale des Télécommunications (UIT-T) permet d'obtenir en voix sur IP une qualité de voix "haute définition".

G711: c'est une norme de compression audio de l'UIT-T. Elle est la base de transport de la voix sur le réseau téléphonique commuté (RTC) ou sur le RNIS et est également utilisée pour le transport de la voix avec peu de compression dans les réseaux IP.

#### **4.3.2 Codecs vidéo**

H263: développé pour la transmission de la vidéo sur des lignes à très bas débits, pour des applications de visiophonie via le réseau téléphonique commuté de type H.324. Elle a ensuite été intégrée dans les protocoles de visioconférence sur IP du type H.323 mais aussi SIP.

MPEG-4: il réalise l'intégration de trois secteurs: la télévision, l'informatique, et les télécommunications. On peut l'appliquer dans la communication en temps réel, le multimédia mobile et la téléconférence.

Codec	Date de normalisation	Débit Voix (kb/s)	Débit Total en trame IP (kb/s)	Retard algorithmique	Qualité note sur 5*	Commentaires
G.711	1972	64	80 à 100	0,125 ms	4,1	Qualité téléphonique, débit maximum, délais minimum
G.726	1990	16 à 40	32 à 56		3,85	Libre, bon compromis
G.729	1995	8	25 à 30	15,0 ms	3,92	Soumis à licence, bon compromis
G.723.1	1995	6,3 / 5,3	20 à 25	37,5 ms	3,9 / 3,65	Soumis à licence, bande passante minimale
GSM-EFR	1995	13	-		4	À titre de référence, la téléphonie mobile (GSM)

**Tableau 4: Les principaux codecs [2]**

#### 4.4 Équipements de la visioconférence

Pour notre travail nous avons besoins des équipements suivants:

- Un Switch 8 ports.
- Trois webcams servant à effectuer des captures de flux vidéo.
- Trois casques avec microphone permettant d'effectuer et d'écouter les communications.
- Un IPBX permettant d'assurer la commutation des appels audio et vidéo.
- Quatre ordinateurs : un serveur et trois clients.
- Un codec qui permet d'effectuer la compression et la décompression de l'audio et de la vidéo ceci pour permettre une meilleure qualité dans la restitution de l'image et du son.
- Trois Soft phones qui sont des logiciels libres permettant la communication sur un réseau IP.

Etablir une plateforme de visioconférence sur IP est possible aujourd'hui avec plusieurs applications que nous allons étudier avant de faire un choix sur la solution à adoptée.

#### 4.5 Insertion de la visioconférence au réseau wifi

Diverses applications permettant la visioconférence sont disponibles sous licence ou non. A cet effet, pour répondre aux diverses attentes, nous allons d'abord effectuer une étude de quelques IPBX.

- **choix d'IPBX**

Un IPBX est un PABX (*Private Automatic Branch eXchange*) autrement dit un standard automatique qui achemine votre appel sur le poste désiré après que vous ayez composé un numéro de poste. Pourtant l'IPBX a la particularité de fonctionner avec des liaisons IP (internet Protocol) à l'aide de nouvelles normes de signalisation (SIP, H323 ...) qui transitent par le réseau internet.

Un IPBX (Internet Protocol Private Branch eXchange) est autocommutateur logiciel permettant de gérer les appels téléphoniques entre des postes logiciels ou non reliés à internet. Pour déployer une telle plateforme tout en minimisant les coûts, une solution consistera à utiliser des applications gratuites ou libres (open source); ce qui vient orienter notre choix vers les solutions Linux qui peuvent être AstérisK, Trixbox ou bigbluebutton.

#### **4.5.1 Étude d'astérisK de trixbox**

Trixbox est un ensemble d'outils et d'utilitaires de télécommunication compilés pour devenir un IP PBX. AstérisK est le cœur de son système téléphonique car c'est lui qu'il faut paramétrer et configurer pour pouvoir effectuer la téléphonie. Il fonctionne avec plus d'une centaine d'hôtes d'où son avantage devant les PABX habituels, il ne demande pas une topologie particulière du réseau, fonctionne suivant l'architecture client-serveur.

Les principales fonctionnalités d'AstérisK sont les suivantes:

- Routage des appels et transfert d'appels.
- Contrôle des appels et Conférence.
- Gestion des files d'attente et Détail des appels CdR (Call detail Records),
- Service vocal interactif (standard téléphonique) et boîtes vocales.

#### **4.5.2 Présentation de BigBluebutton**



Bigbluebutton est un système Open source de web conférence qui permet aux entreprises de pallier aux engorgements pendant les réunions et d'offrir les cours de recyclage en ligne, avec une bonne qualité de la voix et de la vidéo à un coût réduit. Cette plateforme contient de nombreux outils utiles

pour une installation au sein des institutions éducatives et pour le monde de la formation et de l'éducation. Il est constitué de plusieurs composants open source et fonctionne sous les environnements tels que: Linux, Mac, et Windows. Avec bigbluebutton, la voix et la vidéo sont basées sur Asterisk offrant de multiples fonctionnalités tels que: les appels audio et vidéo, le transfert d'appel, etc.

#### 4.5.2.1 Fonctionnalités de bigbluebutton

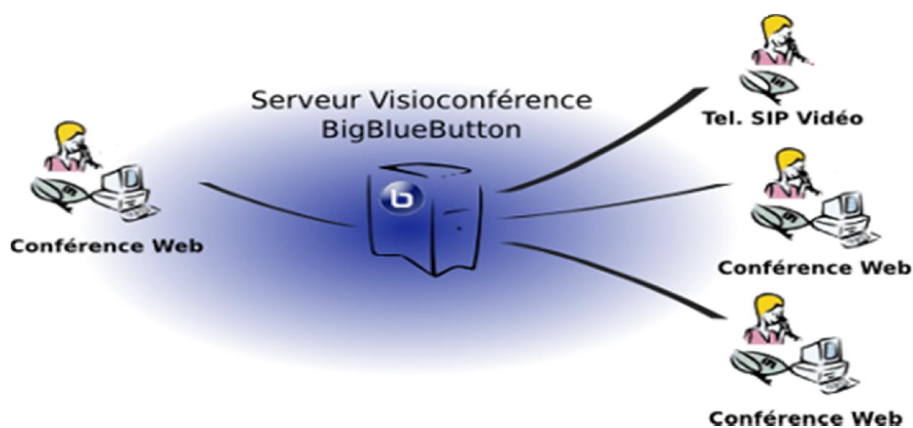
Composé de 14 Open Source dont Asterisk et il intègre les fonctionnalités suivantes:

- Conférence audio
- Conférence vidéo
- Chat
- Gestion des participants de la visioconférence
- Partage du bureau de travail
- Afficher un document bureautique (PDF, Power Pointe, Images, etc.)
- Voir tous les participants
- Levez la main
- Suivre les présentations
- Partager sa vidéo
- Voir le curseur du présentateur
- Rendre muet ou Ejecter un participant
- Partager des fichiers
- Accorder le droit de présentateur

L'une des particularités de cette application est son architecture:



**Figure 34: Architecture point à point (Asterisk) [19]**



**Figure 35: Architecture point à multipoint (bigbluebutton)[19]**

Asterisk est chargé de gérer la conférence audio alors que l'application bigbluebutton gère la conférence vidéo par l'intermédiaire d'un serveur Open Source Red5. L'architecture multipoint supporte de nombreux matériels standards du marché tel que les PC équipés de webcams, les téléphone IP SIP (équipés en vidéo - Codecs H263/H264) et les caméras IP/SIP.

#### **4.5.2.2 Composants de bigbluebutton**

Les composants de bigbluebutton sont:

- ✓ Asterisk;
- ✓ Tomcat;
- ✓ MySQL;
- ✓ NGINX;
- ✓ Red5;

Ainsi, ses composants utilisent le port 1935 pour RTMP (Vidéo Streaming), 9123 pour le partage de bureau (avec Xuggler), et le port 80 pour le serveur web Nginx.

En interne, le serveur Red5 Flash utilise le port 5080, le serveur java Tomcat6 utilise le port 8080, Asterisk utilise le port UDP 5060 pour l'interface SIP (Plus port 6079-6099 et les ports RTP 3000-3029). L'interface de gestion Asterisk utilise le port 5038.

### **Conclusion**

En sommes cette partie du travail, nous à permit de bien discerner les différents protocoles de communications, les codecs pour la compression et la décompression de la voix. L'importance du logiciel bigbluebutton, son architecture et ses fonctionnalités.

Mais pour parfaire notre travail, il est important pour nous de suivre l'étape de la réalisation de notre application.

## CHAPITRE 5: RESULTATS ET COMMENTAIRES

### Introduction

La réalisation de cette application aussi exigeante, nous a permis de maîtriser les commandes linux, d'avoir une très bonne connexion internet pour le téléchargement des paquets, de leurs mettre à jour, et de l'installation du serveur à la visioconférence multiple. Cette partie nous a aussi permis de greffer d'autres modules sur notre serveur à savoir: Astrisk pour la téléphonie, Nginx pour le chat, Tomcat6 pour le partage du bureau, Mysql pour la base de données. Une fois fini cette application, nous avons effectué des tests dont les résultats acceptés par l'encadrement technique de PASTEL feront l'objet de la suite de ce chapitre, avec quelques détails d'installations.

### 5.1. Installation de bigbluebutton

Pour commencer, nous aurons besoin d'un ordinateur exécutant Ubuntu soit une machine physique ou une machine virtuelle (VM) ayant les caractéristiques ci-dessous:

- Système d'exploitation: linux distribution Ubuntu ou Cent os;
- Un processeur de 1Ghz ou plus selon le trafic désiré;
- Une mémoire vive d'au moins 512MO;
- Une carte réseau;

Et une connexion Internet. Dans la suite de notre travail notre module sera installé sur un pc virtuel (VMware).

### 5.2 Installation détaillée des modules de bigbluebutton

- Téléchargez la machine virtuelle;
- Télécharger bigbluebutton-vm-2010-07-15.zip;
- Démarrer la machine virtuelle;
- Créer un nouveau PC sur le disque existant dans le répertoire contenant bigbluebutton;
- s'assurer que la mise en réseaux est fixée.
- Double cliquer sur l'icône de bigbluebutton

Le programme va installer automatiquement UBUNTU et définir la mise en réseaux (obtenir une adresse IP d'un serveur DHCP). Quand ces étapes s'achèvent,

bigbluebutton affiche l'interface d'authentification demandant le login et le mot de passe. Initialement les informations entrées sont les suivantes:

User-id: firstuser

Password: default

Après la réinitialisation du mot de passe par défaut nous obtenons le message d'accueil suivant:

```
bbb-vm-20111203-21 login: firstuser
Password:
Last login: Sat Dec  3 21:30:39 UTC 2011 on tty1
Linux bbb-vm-20111203-21 2.6.32-23-generic-pae #37-Ubuntu SMP Fri Jun 11 09:26:5
5 UTC 2010 i686 GNU/Linux
Ubuntu 10.04 LTS

Welcome to Ubuntu!
 * Documentation:  https://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

#
# To launch BigBlueButton, open the following URL
#
#      http:///
#
# If this computer's IP/hostname changes, you can update
# all of BigBlueButton's configuration files with
#
#      bbb-conf --setip <host>
#
# Type 'bbb-conf -h' for more options.

firstuser@bbb-vm-20111203-21:~$ ifconfig eth0 192.168.0.1
SIOCSIFADDR: Permission denied
SIOCSIFFLAGS: Permission denied
firstuser@bbb-vm-20111203-21:~$ sudo su
[sudo] password for firstuser:
root@bbb-vm-20111203-21:/home/firstuser#
```

**Figure 36:** Ecran d'accueil du serveur

### 5.3 Mise à jour des packages et installation des composants de bigbluebutton

L'exécution des différentes commandes pour mettre à jour les fichiers et installer les différents modules nécessite que nous soyons d'abord en administrateur avec la commande: `sudo -i`

- Mise à jour du fichier `/etc/apt/source-list`

Apt-get update

Apt-get upgrade

- Installation de mysql

Aptitude install mysql-server



- Installation de tomcat

*Aptitude install tomcat6*

- Installation de red5

*Aptitude -y install chkconfig*

*Aptitude install chkconfig red5 on*

*Aptitude install chkconfig asterisk on*

- Installer asterisk

*Aptitude install asterisk*

#### - Modification des extensions

*Wget http://bigbluebutton.org/0.70/bbb\_extension.conf*

*mv bbb\_extension.conf/etc/asterisk/*

*echo« "# include \"bbb\_extensions.conf\" » /etc/asterisk/extensions.conf*

- Installation de appKonference

*Wget http://bigbluebutton.org/downloads/.070/32bit/app\_Konference.so*

*Mv app\_konference.so/usr/lib/asterisk/modules/*

*Chmod755/usr/lib/asterisk/modules/app\_konference.so*

- Configuration de Nginx

*Wget http://bigbluebutton.org/downloads/.070/nginx-bigbluebutton.conf*

*Catnginx-bigbluebutton.conf | sed "s/192.138.0.51/<YOUR-IP> /" > /etc/nginx/sites-available/bigbluebutton.conf*

- Activer BigBlueButton nginx

*Ln -s /etc/nginx/sites-available/bigbluebutton /etc/nginx/sites-enabled/bigbluebutton*

- Installer bbb-web

*Aptitudes install bbb-web*

*Cd /var/lib/tomcat6/webapps*

*Cp /tmp/bigbluebutton.war /bigbluebutton.war*

Après redémarrage des services, nous obtenons la page ci-dessous

```
* Setting sensors limits [ OK ]
Loading DAHDI hardware modules:
FATAL: Error inserting dahdi (/lib/modules/2.6.32-33-generic-pae/updates/dkms/dahdi.ko): Invalid module format
dahdi: error dahdi_dummy: error dahdi_transcode: error
Error: missing /dev/dahdi!
* Starting Apache ActiveMQ service activemq [ OK ]
Starting OpenOffice headless server
Starting nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
configuration file /etc/nginx/nginx.conf test is successful
nginx.
Starting Asterisk PBX: asterisk.
* Starting Tomcat servlet engine tomcat6 [ OK ]
* Starting Red5 Server red5
```

**Figure 37:** Ecran du serveur après redémarrage des services

Après avoir redémarré le serveur, on tape les commandes suivantes:

# **sudo -i**: pour passer en super utilisateur

# **ifconfig -a**: pour voir les interfaces activés

# **ifconfig eth6 192.168.200.10**: pour fixer le 192.168.200.10 comme adresse IP du serveur

#**ping @** de la machine physique (192.168.200.11): pour tester la connectivité entre la machine physique et le serveur.

# **bbb-conf -setip eth6 192.168.200.10**: pour forcer tous les serveurs à écouter sur l'adresse 192.168.200.10

# **bbb-conf -check**: pour vérifier si tous les modifications ont été prisent en compte.

```
bigbluebutton-vm-dev i386 x
root@bbb-vm-20110909-17:~# bbb-conf -check
Current Configuration:
Kernel version: 2.6.32-33-generic-pae
Memory: 1002 MB

/var/www/bigbluebutton/client/conf/config.xml:
    Port test (tunnel): 192.168.200.10
    Red5: 192.168.200.10

/etc/nginx/sites-available/bigbluebutton
    server name: 192.168.200.10
    port: 80
    bbb-client dir: /var/www/bigbluebutton

/var/lib/tomcat6/webapps/bigbluebutton/WEB-INF/classes/bigbluebutton.properties
(bbb-web)
    bbb-web host: 192.168.200.10

/var/lib/tomcat6/webapps/bigbluebutton/demo/bbb_api_conf.jsp (API demos)
    bbb-web-api host: 192.168.200.10

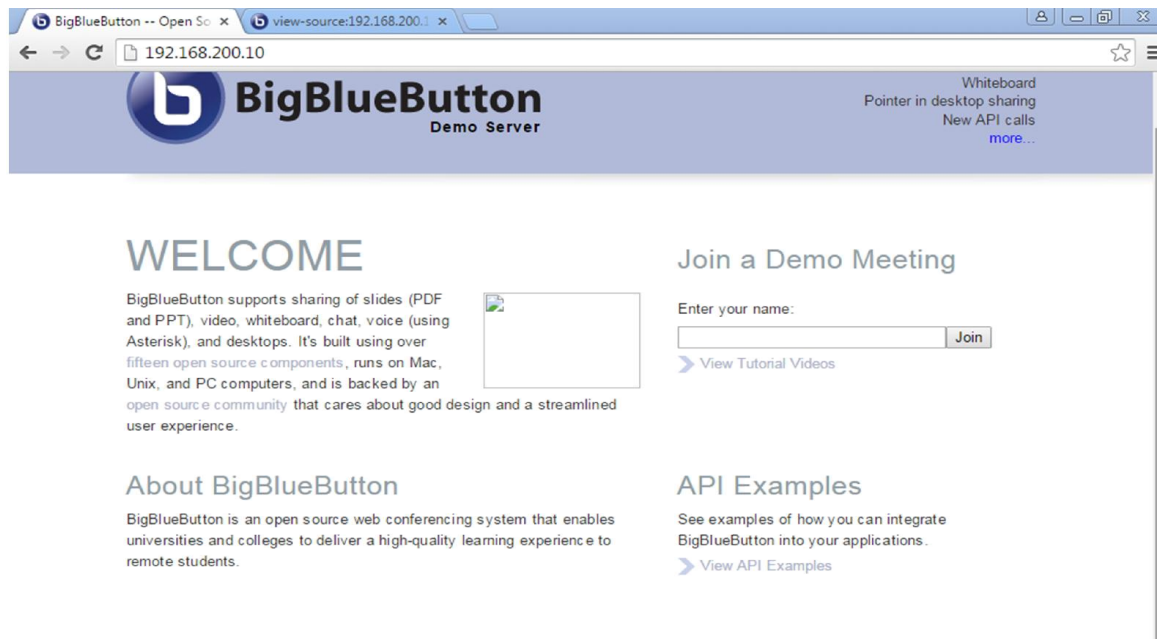
/etc/asterisk/bbb_extensions.conf (asterisk)
    voice conf application: conference

** Potential Problems **

root@bbb-vm-20110909-17:~#
```

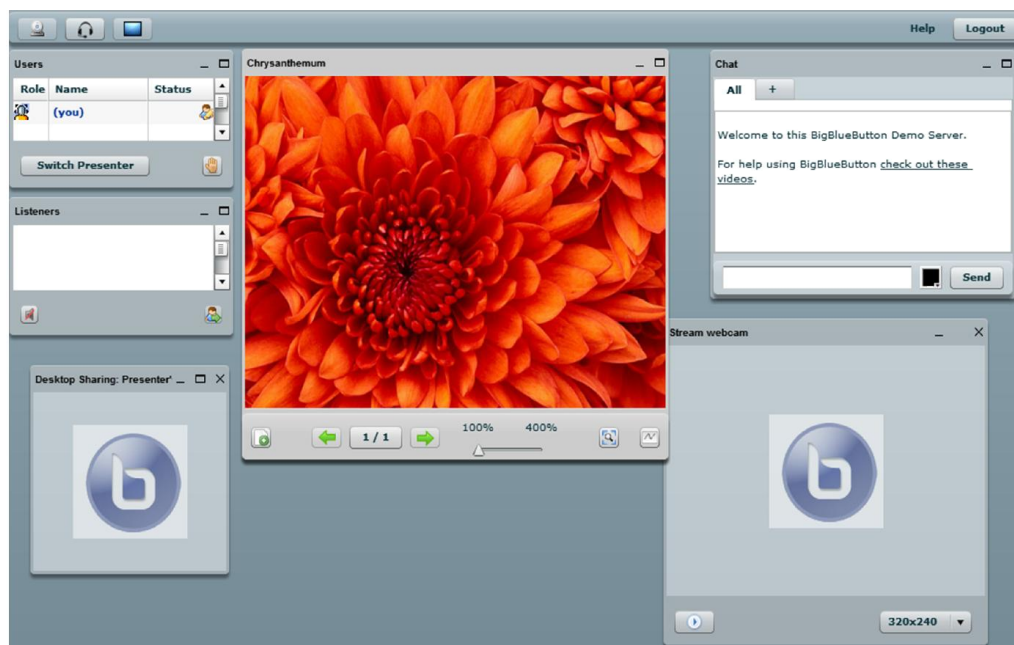
**Figure 38:** Test de fonctionnement du serveur

Ensuite on se connecte au serveur à partir d'un navigateur et on obtient la page si dessous:



**Figure 39: Interface du serveur bigbluebutton**

Lorsque nous obtenons l'interface de notre serveur, nous pouvons passer à l'usage des différentes fonctions de notre serveur.



**Figure 40: Fonctionnalités du bigbluebutton**

Il faut noter que comparativement à d'autres outils de visioconférences ou nous devons avoir des softphones ou téléphones logiciels, cette plateforme a la particularité de permettre à ses clients, de juste se connecter via une page web, avec un navigateur tel que Mozilla Firefox, Internet Explorer et tout autre navigateur intégrant au préalable Adobe Flash Player.

## **Conclusion**

Tout au long de ce chapitre nous avons pris la peine de bien mettre en évidence nos acquis techniques via l'implémentation de la visioconférence multiple avec les services de téléphonie sur IP classique à savoir émission et réception d'appels, le chat, le partage de bureau. Nous sortons de là très aguerrit et pensons pouvoir mieux faire.

## CONCLUSION ET PERSPECTIVES

En sommes le travail qui nous avait été soumis consistait à déployer et à étendre le réseau wifi entre la direction administrative et la direction technique, ensuite appliquer de la visioconférence à notre wifi afin de pouvoir communiquer en audio et en vidéo entre les employers et les différent responsables. Ainsi notre travail avait été organisé comme suit: au premier chapitre nous avons présenté le contexte dans lequel nous avons travaillé, et la méthodologie adopté. Le deuxième chapitres introduit le réseau wifi et ces variantes, décrit et explique son architecture et son fonctionnement. Au troisième chapitres nous nous sommes appliqués sur le dimensionnement des équipements, le dimensionnement en capacités, et enfin la mise en œuvre de notre réseau. Au quatrième chapitre nous avons axé notre étude sur l'interopérabilité entre le réseau wifi et l'application à la visioconférence sur IP. L'étude des protocoles et des codecs pour effectuer une bonne communication. Enfin au cinquième chapitre, nous analysons les résultats obtenus de l'application réalisée. Ce projet est très important pour l'entreprise dans la mesure où il facilite les réunions et diminue le cout des communications. Ceci nous a permis de mieux connaitre l'intégralité du déploiement et de l'extension du wifi, ensuite l'application à la visioconférence, et enfin d'acquérir un grand nombre de connaissances aussi bien d'un point de vue technique que juridique.

Néanmoins nous avons rencontrés un certain nombre de difficultés comme l'installation du serveur bigbluebutton qui nécessitait un grand débit pour télécharger les paquets et les mises à jour qui se font en ligne de commande sur Internet. Ceci étant, ce projet n'est pas parfait et peut donc subir des modifications tant dans le fond que la forme. C'est pourquoi en perspectives, d'autres fonctionnalités peuvent être rajoutées comme:

- ✓ L'enseignement à distance.
- ✓ La télé-ingénierie et la télémédecine

## BIBLIOGRAPHIE

### 1-) Ouvrages:

- [1] Guy Pujolle, *Les Réseaux*, 6<sup>ème</sup> édition, Éditions EYROLLES, Paris, France, 2008.
- [2] Claude Servin, *Réseaux & Télécoms*, 2<sup>ème</sup> édition, Éditions DUNOD, Paris, France, 2003.
- [3] Aurélien Geron, *Wifi Professionnel*, 3<sup>ème</sup> édition, Éditions DUNOD, Paris, France, 2004.
- [4] Jean-Luc Montagnier, *Pratique des réseaux d'entreprise*, 1<sup>ème</sup> édition, Éditions EYROLLES, Paris, France, 1999.
- [5] Cédric Liorens, Laurent Levier, Denis Valois, *Tableaux de bord de la sécurité réseau*, 2<sup>ème</sup> édition, Éditions EYROLLES, Paris, France, 2003.

### 2-) Supports de cours :

- [6] Alain DJIMELI, *Réseaux sans fils*, 2011-2012, Réseaux et Télécoms.
- [7] Alex CHIMÈ, *Antennes et Propagations*, 2011-2012, Réseaux et Télécoms.
- [8] TERDAM VALENTIN, *Réseaux sans fils*, 2012-2013, Administration et sécurité des réseaux.
- [9] TERDAM VALENTIN, *planification des Réseaux sans fils*, 2014-2015.

### 3-) Thèses et mémoires :

- [10] JEROME ROUSSELOT, Mémoire de fin d'études: *Déploiement d'un réseau sans fil pour des instituts de microfinance dans le cadre de la coopération au développement*. Université libre de Bruxelles Faculté des Sciences Appliquées 2004 -2005.
- [11] MICHEL DUCHATEAU, Mémoire de fin d'études: *Analyse et simulation du déploiement d'un réseau sans fil à l'ULB*, université libre de Bruxelles Faculté des Sciences Appliquées 2004-2005.

[12] KWATÈ KWATÈ Rodrigue, Mémoire de fin d'étude: *Déploiement d'un réseau wifi longue portée avec une plateforme de TOIP*. Institut universitaire de technologie FOTSO Victoire de BANDJOUN, 2010-2011

[13] Arnaud Dupont FOTSO, Mémoire de fin d'étude: Mise en place d'un réseau wifi avec authentification basé sur les certificats. Institut Africain d'Informatique, 2008.

#### **4-) Articles du web**

[14] BOUREDJI Zouhir. Le Wifi: réseau local sans fil. CERIG/EFPG [en ligne].2003, Disponible sur <http://cerig.efpg.inpg.fr/Note/2003/wifi.htm> (consulté le 2-04 - 2015).

[15] NACHURY Ludovic. Les 10 travaux du Wifi. 01net [en ligne]. 2003, disponible sur <http://www.01net.com/article/204808.html> (consulté le 2-04-2015).

[16]<http://www.clubic.com/article-80766-4-dossier-guide-securite-wifi-wep-wpa-crack-hack.html>,consultéle07-05-2015

[17][http://www.itrainonline.org/itrainonline/mmtk/wireless\\_fr/07\\_Radio\\_Link\\_Calculations/07\\_fr\\_mmtk\\_wireless\\_radio-link\\_slides.pdf](http://www.itrainonline.org/itrainonline/mmtk/wireless_fr/07_Radio_Link_Calculations/07_fr_mmtk_wireless_radio-link_slides.pdf) ,( consulté le 26-05-2015)

[18]<http://www.voipinfo.org/wiki/index.php?page=Asterisk+iax+rsa+auth>, (consulté le 26-06-2015)

[19] [www.bigbluebutton.org](http://www.bigbluebutton.org) (télécharger le paquetage) (consulté le 01/08/2015)

## ANNEXES

### Commandes des routeurs

```
.
!  
interface Serial0/0  
  ip address 192.168.1.1 255.255.255.0  
!  
interface Serial1/0  
  no ip address  
  shutdown  
!  
interface Ethernet2/0  
  ip address 192.168.0.1 255.255.255.0  
  duplex auto  
  speed auto  
!  
interface FastEthernet3/0  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
router ospf 1  
  log-adjacency-changes  
  network 192.168.0.0 0.0.0.255 area 1  
  network 192.168.1.0 0.0.0.255 area 1  
!
```

Ces commandes entrées au niveau du routeur permettent aux différents paquets qui circulent dans le réseau de suivre le bon chemin.

```
sudo: option requires an argument -- 'u'  
usage: sudo -h | -K | -k | -L | -U  
usage: sudo -v [-AknS] [-p prompt]  
usage: sudo -l [|] [-AknS] [-g groupname:#gid] [-p prompt] [-U username] [-u  
username:#uid] [-g groupname:#gid] [command]  
usage: sudo [-AbEHknPS] [-C fd] [-g groupname:#gid] [-p prompt] [-u  
username:#uid] [-g groupname:#gid] [VAR=value] [-i|-s] [<command>]  
usage: sudo -e [-AknS] [-C fd] [-g groupname:#gid] [-p prompt] [-u  
username:#uid] file ...  
firstuser@bbb-vm-20110909-17:~$ sudo -i  
[sudo] password for firstuser:  
root@bbb-vm-20110909-17:~# ifconfig -a  
eth6      Link encap:Ethernet  HWaddr 00:0c:29:25:80:1a  
          BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)  
          Interrupt:17 Base address:0x1080  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:690 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:690 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:95608 (95.6 KB)  TX bytes:95608 (95.6 KB)  
  
root@bbb-vm-20110909-17:~#
```

Cet écran permet à l'administrateur d'introduire l'adresse de son serveur, en permettant ainsi sa machine physique d'être en réseau avec son serveur.