REPUBLIQUE DEMOCRATIQUE DU CONGO

ENSEIGNEMENT SUPERIEUR ET UNIVERSITAIRE

UNIVERSITE CATHOLIQUE DE BUKAVU

(U.C.B)

B.P. 285 Bukavu

FACULTE DES SCIENCES

DEPARTEMENT DES SCIENCES DE L'INFORMATIQUE

Conception d'un réseau MAN interconnectant différents Hôpitaux publics pour l'échange des fichiers : cas de la ville de Bukavu.

Par : BIRINDWA BYAMUNGU Moise

Mémoire présenté et défendu en vue de l'obtention du diplôme de licence en sciences de l'informatique, Option Réseaux et Télécommunications.

Option : Réseau et Télécommunications

Directeur : Dr. NIYONSABA Thérence

Encadreur : Ass. Jovianne BIRINDWA

Année académique : 2021-2022

Table des matières

EPIGRAPHES III
DEDICACE IV
REMERCIEMENTS V
LISTE DES SIGLES ET ACRONYMES VI
LISTE DES TABLEAUX VII
LISTE DES FIGURES VIII
RESUME IX
ABSTRACT X
INTRODUCTION GÉNÉRALE 1
1. **Contexte général et concepts** 1
2. **Problématique** 2
3. **Hypothèses** 3
4. **Délimitation et Objectifs** 3
5. **Choix et intérêt du sujet** 4
6. **Méthodologie** 5
7. **Subdivision du travail** 5

Chapitre 1 : ÉTAT DES LIEUX ET ANALYSE 7
1.1. CADRE D'ETUDE 7
1.1.1. L'hôpital général de référence de Bagira 7
1.1.2. L'hôpital provincial général de référence de Bukavu 8
1.1.2.a. Situation géographique 8
1.1.2.b. Organigramme de l'HPGRB 9
1.1.2.c. Architecture réseau existante 10
1.1.3. L'hôpital de Ciriri 11
1.1.4. L'hôpital général de Kadutu. 11
1.2. GENERALITE SUR LES RESEAUX INFORMATIQUE 12
1.2.1. Définitions 12
1.2.2. Les types de réseaux 13
1.2.3. Les différentes catégories des réseaux (Les structures des réseaux) 14
1.2.4. Equipements d'Interconnexion des réseaux 15
1.2.5. Présentation de la Technologie WiMAX 16
1.2.6. Le modèle OSI 29
1.3. Analyse de l'existant et identification des problèmes 31
1.3.1. Cahier des charges 31

1.3.2. Analyse de l'existant 32
1.4. Conclusion **35**
Chapitre 2 : **REVUE DE LA LITTÉRATURE ET DESCRIPTION DE L'APPROCHE** **37**
2.1. Etat de la question 37
2.2. Outils de travail (matériels et logiciels) 39
2.3. Description et justification de l'approche 41
2.4. Conclusion 42
Chapitre 3 : **APPLICATION DE LA MÉTHODOLOGIE ET PRÉSENTATION DES RÉSULTATS AVEC ANALYSE** **43**
3.1. Structure de l'équipe de travail (les Moyens humains). 43
3.2. Moyens matériels 44
3.3. Nombre de sites à installer 44
3.4. Stratégie de collecte des données 45
3.5. Présentation des résultats 46
Etape 1 : **Liaison des sites et configuration MAN** 46
Etape 2 : **Configuration des équipements et services** 48
Etape 3 : Mise en place de serveur SFTP 53
Etape 4 : Connexion au Serveur SFTP 60
3.6. **Estimation du coût pour la mise en œuvre des solutions proposées** 62
3.7. Discussion des résultats 66
3.7.1. Contributions théoriques et pratique 66
3.7.2. Limites de l'étude et pistes de recherche futures 66
3.8. Conclusion 67
Conclusion Générale **68**
Bibliographie **70**
ANNEXES **73**

EPIGRAPHES

« L’expérience ce n’est pas ce qui arrive aux hommes, c’est ce que les hommes font de ce qui leur arrive » - Aldous Huxley

DEDICACE

A nos très chers parents, BIRINDWA Jean-Petit et NGALYA Rosette

Pour tant d'amour et de soutien. Avec l'espoir de ne jamais vous décevoir que ce modeste travail reste et soit l'exaucement de vos vœux tant formulés et de vos prières quotidiennes.

REMERCIEMENTS

Au seuil de ce travail de fin d'étude universitaire, qu'il nous soit permis de remercier très sincèrement le bon Dieu des armées, source de toute intelligence par son amour et sa grâce qu'il n'a cessé de nous combler tout au long de ce stage.

Nos remerciements s'adressent aux membres des corps académique et scientifique de l'Université Catholique de Bukavu pour la formation de qualité qu'ils ne cessent de manifester à notre égard et leurs sages conseils, en particulier à notre équipe d'encadrement Dr. NIYONSABA Thérence et à l'enseignante Mme Jovianne BIRINDWA qui, en dépit de leurs charges, ont assuré l'encadrement et la direction de l'élaboration de ce travail ; qu'ils trouvent ici notre juste reconnaissance autant pour les brillantes corrections que pour les conseils adressés à notre égard.

Nous signifions nos vifs remerciements à nos parents BIRINDWA Jean-Petit et NGALYA Rosette qui nous ont fait montrer de leur tendre affection durant toute la période de notre cursus et qui nous ont encadré tant moralement que matériellement pour la réussite de ce travail ;

Nos sentiments vont aussi à nos frères et sœurs et à nos éternels compagnons de prédilection qui ont contribué à l'accomplissement de ce travail de mémoire.

Enfin, que nos bienfaiteurs, amis et connaissances que nos souvenirs ont oubliés trouvent à travers ces lignes l'expression de notre profonde gratitude.

LISTE DES SIGLES ET ACRONYMES

ATM	: Asynchronous Transfer Mode
BS	: Base Station
DSL	: Digital Subscriber Line
FUSC	: Full Usage of Subchannels)
ISO	: International Organization for Standardization
Qté	: Quantité
HPGRB	: Hôpital Provincial Général de Référence de Bukavu
HGRB	: Hôpital Général de Référence de Bagira
LAN	: Local Area Network
LLC	: Logical Link Control
LOS	: Line Of Sight
MAC	: Media Access Control
MAN	: Métropolitain Area Network
MIB	: Management Information Base
OFDM	: Orthogonal Frequency Division Multiplexing
OFDMA	: Orthogonal Frequency Division Multiple Access
PHY	: Physical
P2P	: Peer to Peer
PUSC	: Partial Usage of Subchannels
R D Congo	: République Démocratique du Congo
RAM	: Random Access Memory
SC	: Single Carrier
SFTP	: Secure File Transfert Protocole
SGBD	: Système de Gestion de Base de Données
S.I.	: Systèmes d'Information
SS	: Subscriber Station
U.P.	: Unified Process
UCB	: Université Catholique de Bukavu
TIC	: Technologies de l'Information et de la Communication
WAN	: Wide Area Network
WiFi	: Wireless Fidelity
WiMAX	: Worldwide Interoperability for Microwave Access

LISTE DES TABLEAUX

Tableau 1 L'évolution des différentes normes d'IEEE 802.16x 23
Tableau 2 PC utilisés 32
Tableau 3 Les équipements d'interconnexion de l'HPRB 33
Tableau 4 Forces et faiblesses du système existant de tous les hôpitaux publics de la ville de Bukavu 34
Tableau 5 les équipements à installer 44
Tableau 6 Coordonnées Géographiques des sites à installer 45
Tableau 7 Estimation financière du projet 63
Tableau 8 coût de la formation par Hôpital 66
Tableau 9 Les Equipements à installer par Site 76

LISTE DES FIGURES

Figure 1 Architecture Réseau interne de l'HPGRB *10*
Figure 2 Topologie Intranet de l'HPGRB *10*
Figure 3 Schema d'un MAN [43] *14*
Figure 4 Historique du WIMAX *18*
Figure 5 Exemple d'un réseau WIMAX avec les deux variantes fixe et mobile [51] *19*
Figure 6 Exemple d'un réseau WiMax *21*
Figure 7 Architecture End to End [45] *22*
Figure 8 Structure en couche du standard IEEE802.16 ..... *24*
Figure 9 Description fréquentielle de l'OFDMA *26*
Figure 10 Architecture OSI *29*
Figure 11 Schéma représentatif d'un transfert de données SFTP *40*
Figure 12 Vue satellitaire de différentes liaisons *46*
Figure 13 Architecture d'interconnexion des hôpitaux publics de la ville de Bukavu *47*
Figure 14 Proposition de l'architecture du réseau MAN *47*
Figure 15 Architecture Globale du Réseau *48*
Figure 16 Installation du serveur SFTP *54*
Figure 17 Activation du serveur SFTP *54*
Figure 18 Lancement et vérification des statuts *55*
Figure 19 Création des groupes d'utilisateurs *55*
Figure 20 Création d'un utilisateur et l'affecté à son groupe *56*
Figure 21 Création d'un utilisateur et l'affecté à son groupe *56*
Figure 22 Création des répertoires pour le partage des fichiers *57*
Figure 23 Définition des autorisations sur les fichiers *57*
Figure 24 Attribution des fichiers à leurs propriétaires respectifs *58*
Figure 25 Configuration du démon ssh *58*
Figure 26 Connexion d'un utilisateur au serveur via le terminal *59*
Figure 27 Installation et configuration du pare feu UFW *59*
Figure 28 Installation et configuration du pare feu UFW 2 ..... *60*
Figure 29 Connexion au serveur sftp via l'interface graphique *60*
Figure 30 Connexion au serveur sftp via l'interface graphique 2 ..... *61*
Figure 31 Connexion au server sftp via l'application fileZila *61*
Figure 32 Liaison RENA-BAGIRA *74*
Figure 33 Liaison RENA CIRIRI *74*
Figure 34 Liaison RENA-HPGRB *75*
Figure 35 Liaison RENA-Hôpital de Kadutu *75*

RESUME

La nécessité d'aller plus vite et d'être de plus en plus pointu dans le traitement de l'information a favorisé l'introduction de l'informatique dans tous les domaines d'activités voir même dans le domaine médical. Ainsi, ce travail portant sur la conception d'un réseau Man interconnectant différents Hôpitaux publiques de la ville de Bukavu pour l'échange des fichiers a été développée par cinq objectifs de recherches dont : présenter et étudier les bonnes pratiques et les étapes à suivre pour réaliser la meilleure conception d'un réseau qui répond aux exigences en matière de réseau d'entreprise, contrôler et authentifier les différents utilisateurs souhaitant accéder au réseau, journaliser quotidiennement les informations sur les utilisateurs qui se connectent, positionner de façon adéquate le point d'accès et sécuriser les données qui transitent sur le réseau.

Ce texte présente un état de l'art, des techniques existantes de la mise en place d'un réseau d'interconnexion. Pour bien mener le développement de ce travail, nous avons présenté l'état de l'art de la technologie WiMAX qui nous a permis de combler certaines défaillances d'interconnexion en permettant aux utilisateurs d'avoir un accès haut débit à Internet sans avoir besoin de se connecter sur les BLR filaires (câbles) mais plutôt une connexion longue distance et sans fil. Le SSH file transfer protocol (abrégé en SFTP) nous a semblé le mieux indiqué pour assurer le transfert de données en toute sécurité entre les hôpitaux publics souhaitant communiquer ou échanger les informations liées à des recherches cliniques, les innovations médicales et pharmaceutiques, la sécurité sanitaire, la qualité des soins, la pathologie des patients transférés d'un hôpital à un autre, ... Après, nous introduisons l'Architecture de réseau MAN d'interconnexion des hôpitaux publics de la ville de Bukavu. Ensuite, nous montrons les simulations du réseau réalisé au sein des hôpitaux publics de la ville de Bukavu en survolant toutes les configurations nécessaires pour la réalisation de ce travail.

Ces résultats ont été discutés par rapport aux résultats des différents auteurs pour déceler la concordance de nos résultats et ceux de nos prédécesseurs et avions donné quelques suggestions pour améliorer cette configuration dans les hôpitaux de la ville Bukavu.

Mots clés : Réseau informatique, WiMAX, SFTP, MAN, Interconnexion, Simulation, configuration.

ABSTRACT

The need for going more quickly and to be increasingly pointed in the data processing supported the introduction of data processing into all the spheres of activities see even in the medical field.Thus, this bearing work on the design of a Man network inter-connecting various Hospitals public of the town of Bukavu for the exchange of the files was developed by five objectives of research of which: to present and study the good practices and the stages to follow to carry out the best design of a network which fulfills the requirements as regards corporate network, to control and authenticate the various users wishing to reach the network, to daily journalize information on the users which are connected, to position in an adequate way the access point and to make safe the data which forward on the network.

This text presents a state of the art, existing techniques of the installation of an interconnected network.For undertaking the development of this work well, we presented the state of the art of the WiMAX technology which enabled us to fill certain failures of interconnection while making it possible to the users to have an access high flow to Internet without needing to connect itself on the telegraphic BLR but rather a connection long distance and without wire.The SSH File Transfer Protocol (shortened in SFTP) seemed to us indicated best to ensure the transfer of data in full safety between the public hospitals wishing to communicate or to exchange information related to clinical research, the medical and pharmaceutical innovations, medical safety, the quality of the care, the pathology of the patients transferred from a hospital to another… Afterwards, we introduce the Network architecture MAN of interconnection of the public hospitals of the town of Bukavu.Then, we show simulations of the network carried out within the public hospitals of the town of Bukavu by flying over all the configurations necessary for the realization of this work.

These results were discussed compared to the results of the various authors to detect the agreement of our results and those of our predecessors and had given some suggestions to improve this configuration in the hospitals of the Bukavu city.

Key words:Data-processing network, WiMAX, SFTP, MAN, Interconnection, Simulation, configuration.

INTRODUCTION GÉNÉRALE

1. Contexte général et concepts

Aujourd'hui, les réseaux informatiques et les ordinateurs constituent des outils essentiels au succès d'une entreprise, peu importe sa taille. D'où, la nécessité d'aller plus vite et d'être de plus en plus pointu dans le traitement de l'information a favorisé l'introduction de l'Informatique dans tous les domaines d'activités même dans le domaine médical [43]. Aucun domaine n'échappe à cette révolution technologique, qui au fil des jours s'affiche comme un outil indispensable de travail [9]. La multiplication des réseaux locaux ayant ainsi entraîné le besoin d'interconnexion, c'est pourquoi, cetains auteurs [21] estiment qu'un nouveau challenge s'offre donc aux professionnels de l'informatique qu'est celui d'interconnecter les réseaux locaux entre eux afin que l'emplacement géographique ne soit plus un handicap pour l'accès aux informations.

L'expression et le thème de constitution d'un réseau ou des périphériques connectés les uns aux autres revient régulièrement à la une de l'actualité et l'acquisition des connaissances relatives à ces termes fait partie des compétences indispensables à la vie courante d'un informaticien et le secteur médical n'échappe pas à cette tendance [7]. Cette nouvelle technologie permet aux hôpitaux de réaliser des tâches avec une bonne précision et cela avec une grande vitesse et facilite l'homme dans ses différentes tâches [40] C'est pourquoi, à présent nous avons la possibilité de réaliser des tâches à distance en utilisant les réseaux de télécommunication qui nous permettent de communiquer à une distance bien déterminée selon le protocole utilisé.

Cependant, en R.D. Congo, le rôle des réseaux a sensiblement évolué ces dernières années dans le domaine médical, il ne se limite pas au transfert de l'information en toute sécurité mais aujourd'hui il contribue largement à la rationalisation des utilisateurs et à l'optimisation des performances applicatives [54]. Dans ce contexte, nous essayons dans ce travail de mémoire d'implanter au sein de différents hôpitaux publics de la ville de Bukavu un réseau MAN à partir des outils de sécurités SFTP afin de permettre à deux ordinateurs distants de ces derniers de communiquer et d'échanger des fichiers médicaux comme s'ils faisaient partie d'un même réseau local.

2. Problématique

Aujourd'hui, les réseaux informatiques sont de plus en plus répandus et complexes. Dans les hôpitaux publics de la R.D.Congo, les systèmes informatiques se retrouvent intégrés de plus en plus dans le système de santé. Chaque consultation de patient produit des informations médicales, personnelles et confidentielles (pathologie, identité, etc.) qui doivent être idéalement partagées avec l'accord du patient entre les différents acteurs de sa santé. Si les informations médicales des patients intéressent les médecins pour suivre l'évolution d'une maladie ou d'une pathologie, les médecins épidémiologistes qui surveillent l'état de santé des populations et l'évolution des pratiques médicales trouvent un intérêt à utiliser des dossiers médicaux électroniques si ceux-ci sont bien renseignés par les praticiens qui en ont la charge.

Les Hôpitaux publics de la R.D.Congo espèrent ainsi faire d'importantes économies en ayant la possibilité d'installer rapidement des antennes qui pourraient raccorder environ 30 hôpitaux avec des lignes de type T1 et des centaines de ménages avec des liens de type DSL-1Mbit/s [36]. Mais ces espoirs sont limités par quelques réalités physiques du terrain et la couverture inefficace dans une région densément peuplée étant d'environ 3 Km à 10Mbit/s [3]. En plus, la portée des ondes est aussi affectée par les objets pouvant se trouver entre les antennes, les interférences radioélectriques ainsi que le déplacement trop rapide des utilisateurs [40].

En effet, des grands défis continuent ainsi à gangrener les hôpitaux du Sud-Kivu et plus précisément ceux de la ville de Bukavu. Cependant, notre descente au sein des hôpitaux publics de la ville de Bukavu dont : l'hôpital général de référence de Bagira, l'hôpital provincial général de référence de Bukavu, l'hôpital de Ciriri et l'hôpital général de Kadutu, nous avons pu remarquer qu'ils éprouvent plusieurs difficultés dans la gestion centralisée de leurs données et informations ainsi que dans les échanges des fichiers entre eux avec comme conséquence le manque de segmentation du réseau. Plus encore, nous y avons pu remarquer des domaines défaillants étendus ; c'est pourquoi, dans ces hôpitaux, les défaillances des liaisons et des périphériques affectent de vastes zones du réseau et la sécurité déployée dans les hôpitaux publics de la ville de Bukavu est trop faible n'empêchant pas tout le trafic non autorisé ou indésirable.

Enfin, nous avons pu observer que les hôpitaux publics de la ville de Bukavu ne disposent pas des moyens de transmission et de réception des flux des données médicales efficaces entres eux faisant ainsi l'emplacement géographique de ces hôpitaux un handicap pour l'accès aux informations médicales pourtant cette interconnexion devrait constituer pour eux la boussole

des services de transmissions à distance. En plus, dans ces hôpitaux, vu la fragilité du réseau actuel aux différentes attaques internes et externes, nous avons perçu que la nécessite de protéger les données sur les patients et les services disponibles dans chaque hôpital s'avère tellement indispensable.

Cette situation suscite une interrogation qui est celle de savoir : Quelle est la stratégie à prendre pour assurer une interconnexion ou une liaison optimale des différents hôpitaux publics distants dans la ville de Bukavu ?

3. Hypothèses

L'hypothèse est une proposition de réponse aux questions qu'on se pose à propos de l'objet de recherche formulée en des termes tel que l'observation et l'analyse puissent fournir une réponse [50]. Elle est donc une proposition provisoire, une présomption qui demande d'être vérifiée.

En guise de prévision de réponse à cette question, nous formulons l'hypothèse suivante : La conception et la mise en place d'un réseau ou support moins encombrant et facile d'installation propulsant les technologies d'interconnexion sans fil MAN à partir de WiMAX bâti d'un protocole SFTP pour l'échange des fichiers serait la meilleure orientation à prendre pour assurer une liason optimale des différents hôpitaux publics distants de la ville de Bukavu.

4. Délimitation et Objectifs

Ce travail est délimité sur le plan spatial, temporel et sur le plan de son contenu.

Sur le plan spatial, ce travail porte sur les hôpitaux publics de la ville de Bukavu, une ville où nous considérons comme impératif et urgent de trouver les solutions aux problèmes d'accès aux services de communication et de la santé. Ces hôpitaux sont entre autres : l'hôpital général de référence de Bagira, l'hôpital provincial général de référence de Bukavu, l'hôpital général de référence de Ciriri et l'hôpital général de référence de Kadutu.

Sur le plan temporel, nos recherches seront effectuées au courant de l'année 2022, ce qui veut dire que notre travail se fera en coupe instantanée.

Et **sur le plan de son contenu**, ce travail se limite à développer ou à concevoir un réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu pour l'échange des fichiers.

Par ailleurs, les objectifs de ce travail sont doubles. Ce travail a pour objectif principal de concevoir un réseau sécurisé MAN interconnectant différents Hôpitaux publics de la ville de Bukavu à partir du protocole SFTP pour l'échange des fichiers.

Les objectifs fonctionnels de ce travail s'énoncent comme suit :

- contrôler et authentifier les différents utilisateurs souhaitant accéder au réseau,
- journaliser quotidiennement les informations sur les utilisateurs qui se connectent ;
- positionner de façon adéquate le point d'accès ;
- sécuriser les données qui transitent sur le réseau,

Les objectifs non fonctionnels de ce travail sont entre autres :

- présenter et étudier les bonnes pratiques et les étapes à suivre pour réaliser la meilleure conception d'un réseau qui répond aux exigences en matière de réseau d'entreprise,

- faire un diagnostic de différents problèmes du réseau local existant dans les hôpitaux publics de Bukavu et proposer un nouveau réseau sécurisé répondant aux exigences de l'entreprise
- donner toutes les informations nécessaires aux différents utilisateurs souhaitant accéder au réseau.
- planifier la mise en place d'un serveur central.
- une fois le réseau installé, nous réaliserons des tests afin de vérifier son bon fonctionnement

5. Choix et intérêt du sujet

Vu le réseau local existant dans les hôpitaux de Bukavu dont la majorité présente une topologie linéaire, sans liaison redondante et offrant très peu de sécurité où il n'y a pas de pare-feu dynamique donc ne faisant que le filtrage et n'empêchant pas tout le trafic non autorisé ou indésirable. Notre choix dans ce thème est alors de concevoir un nouveau réseau MAN répondant aux exigences de l'entreprise interconnectant différente Hôpitaux publiques de la ville de Bukavu et de configurer un protocole SFTP pour l'échange des fichiers.

D'un autre point de vue, ce travail est intéressant sur deux plans :

- **Sur le plan personnel**, notre travail de mémoire revêt un intérêt dans la mesure où il nous permettra de creuser nos connaissances sur le monde de développement d'un réseau sans fil MAN à partir de WiMAX configuré d'un protocole SFTP pour l'échange des fichiers.
- **Du point de vue scientifique**, ce mémoire vient compléter les autres travaux empiriques disponibles menés et ayant traités la même thématique que la nôtre sur la conception d'un réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu pour l'échange des fichiers en permettant à d'autres chercheurs de se saisir des différentes notions en rapport avec notre thématique de recherche.

6. Méthodologie

Pour mener cette étude, nous avons recouru à quelques méthodes dont la méthode expérimentale et la méthode ascendance ; nous avons aussi recouru aux enquêtes à partir de la technique d'observation et la technique documentaire. La technique d'observation nous a permis de décrire les problèmes qui continuent à gangrener dans la gestion centralisée des données et informations ainsi que dans l'interaction entre les hôpitaux publics de Bukavu. La technique documentaire nous a amené et permis dans le cadre de réalisation de ce travail à passer en revue des différents documents (ouvrages, publications, autres travaux scientifiques, …) abordant l'objet de notre étude.

7. Subdivision du travail

Mis à part l'introduction et la conclusion générales, ce présent travail sera structuré en trois chapitres :

Dans le premier chapitre portant sur l'état des lieux et analyse, nous exposerons comme première partie la présentation des hôpitaux publics et les généralités de notre étude en définissant les mots clés de notre travail et comme deuxième partie l'état de l'art.

Dans le second chapitre qui est axé sur la revue de la littérature et la description de l'approche, nous y présenterons notre état de la question et la Modélisation en donnant la méthode informatique utilisée au premier point et la modélisation proprement-dite au deuxième point.

Le troisième et dernier chapitre sera la partie de l'implémentation, présentation du logiciel, mise en place du logiciel. Ce chapitre présentera le réseau MAN conçu interconnectant différents hôpitaux publics de la ville de Bukavu et les configurations du protocole SFTP pour l'échange

des fichiers en toute sécurité et la démarche à suivre dans son exécution. Enfin, nous clôturerons ce travail par les limites et perspectives d'avenir.

Chapitre 1 : ÉTAT DES LIEUX ET ANALYSE

Dans ce chapitre sont présentées brièvement quelques notions théoriques utiles dans ce sujet de mémoire. D'abord, on commence par la généralité sur le réseau informatique où on présente le réseau MAN. Les équipements et les protocoles réseaux sont présentés dans le reste de ce chapitre. Enfin nous décrivons l'état de l'art en donnant les définitions des concepts clefs du sujet et le fonctionnement de l'objet d'étude.

1.1.CADRE D'ETUDE

Le cadre d'étude de ce travail portera sur une brève présentation de différents hôpitaux publics de la ville Bukavu. Il s'agit entre autres de : l'hôpital général de référence de Bagira, l'hôpital provincial général de référence de Bukavu, l'hôpital de Ciriri et l'hôpital général de Kadutu.

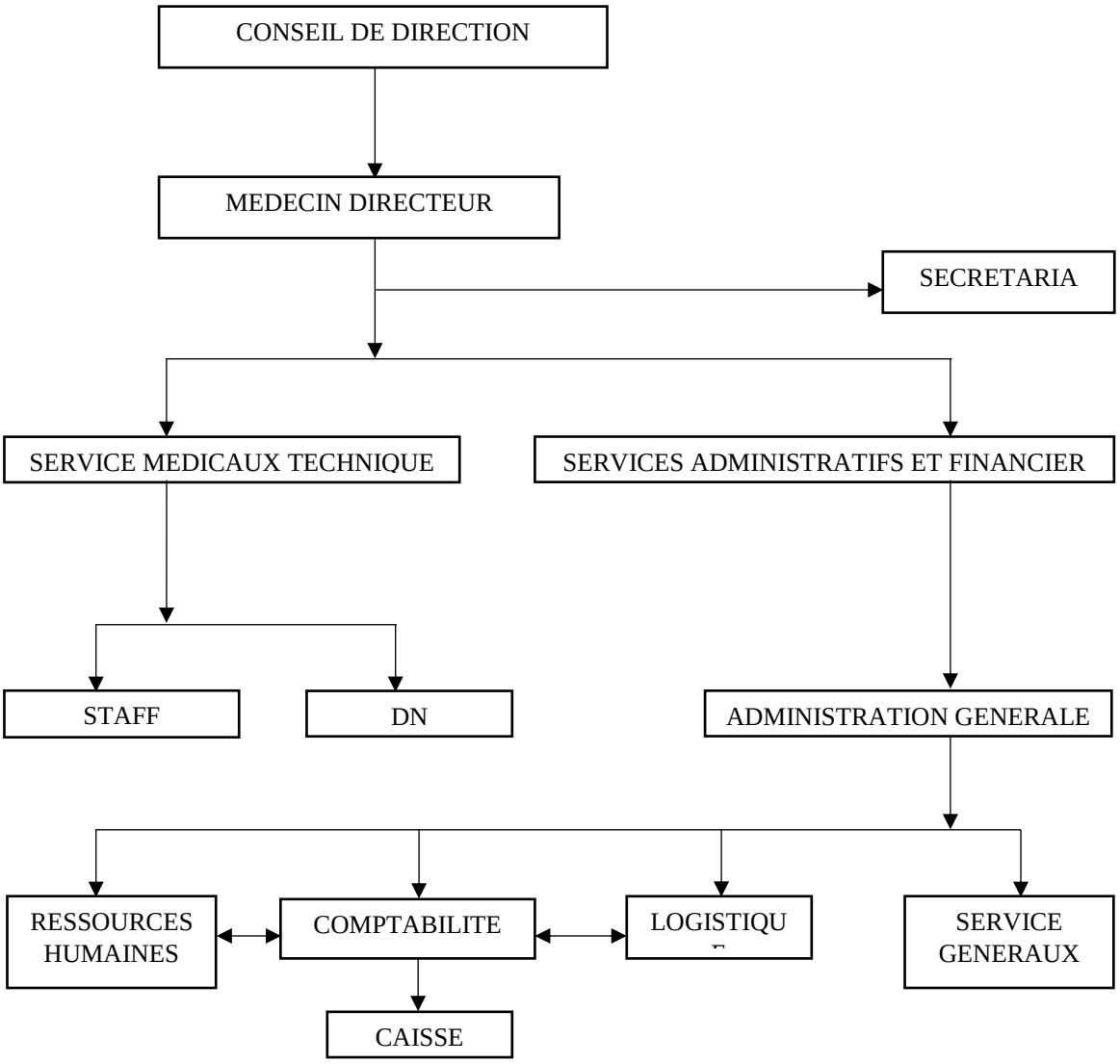
le ministère de la santé donne à ces hôpitaux les missions suivantes : D'assurer les soins de référence secondaire aux malades provenant des hôpitaux généraux de référence des zones de santé ; d'assurer l'encadrement des jeunes professionnels diplômés et des stagiaires en cours de formation dans les universités ; les instituts supérieurs de techniques médicales et les instituts d'enseignement de science de Santé du niveau secondaire, de servir de milieu de recherche dans le domaine de la santé.

1.1.1. L'hôpital général de référence de Bagira

1.1.1.a. Situation géographique

L'Hôpital Général de Référence de Bagira est situé à proximité de Eglise Catholique Bagira et de la maison communale de Bagira.

1.1.1.b. Organigramme



1.1.2. L'hôpital provincial général de référence de Bukavu

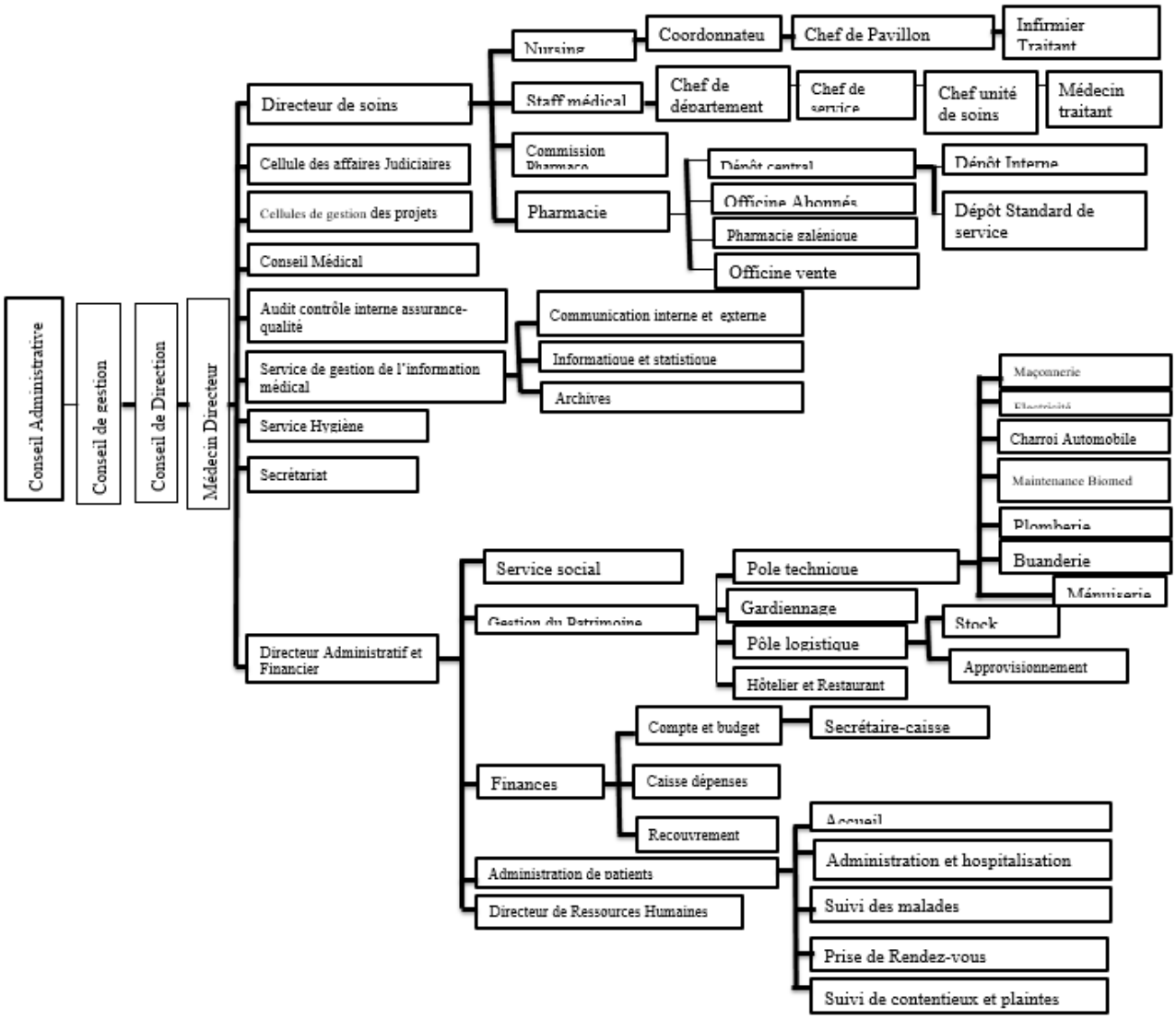
1.1.2.a. Situation géographique

L'HPGRB est situé au carrefour de trois communes urbaines qui composent la ville de Bukavu. Il est situé à plus ou moins 500m de la place de l'indépendance sur Avenue MICHOMBERO ; sur la route qui mène vers l'aéroport de KAVUMU et la ville de GOMA. Il est situé à une altitude de 1500m du niveau de la mer et est soumis à un climat des montagnes. La température varie entre 15°C en raison de pluie et 250°C à 30°C en saison sèche.

Il est limité :

- A l'Ouest par la colline de Karhale sur laquelle sont bâtis L'ISTM, l'ISDR et l'ECONOMAT GENERAL de l'archidiocèse de Bukavu.
- A l'Est par la route qui mène vers GOMA et à 200m du lac Kivu
- Au Nord ; la clinique universitaire de Bukavu
- Au Sud par le camp des employés de la SNCC

1.1.2.b. Organigramme de l'HPGRB



1.1.2.c. Architecture réseau existante

L'HPGRB dispose d'une infrastructure réseau sur laquelle repose la distribution de l'application et services conforme au standard international. Il possède un réseau internet et intranet sur une architecture essentiellement Client-Serveur.

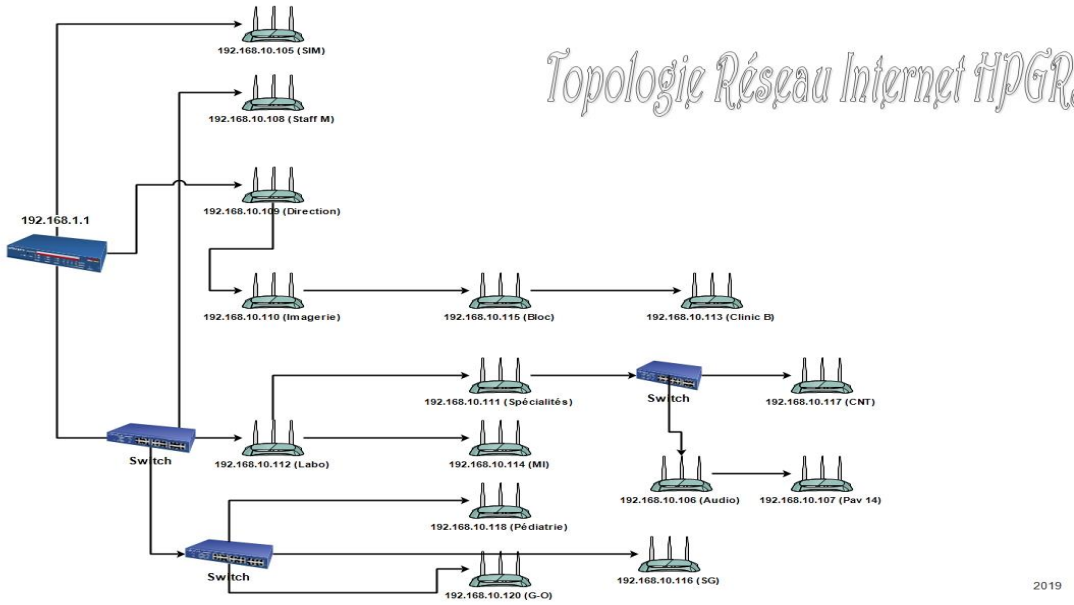


Figure 1 Architecture Réseau interne de l'HPGRB

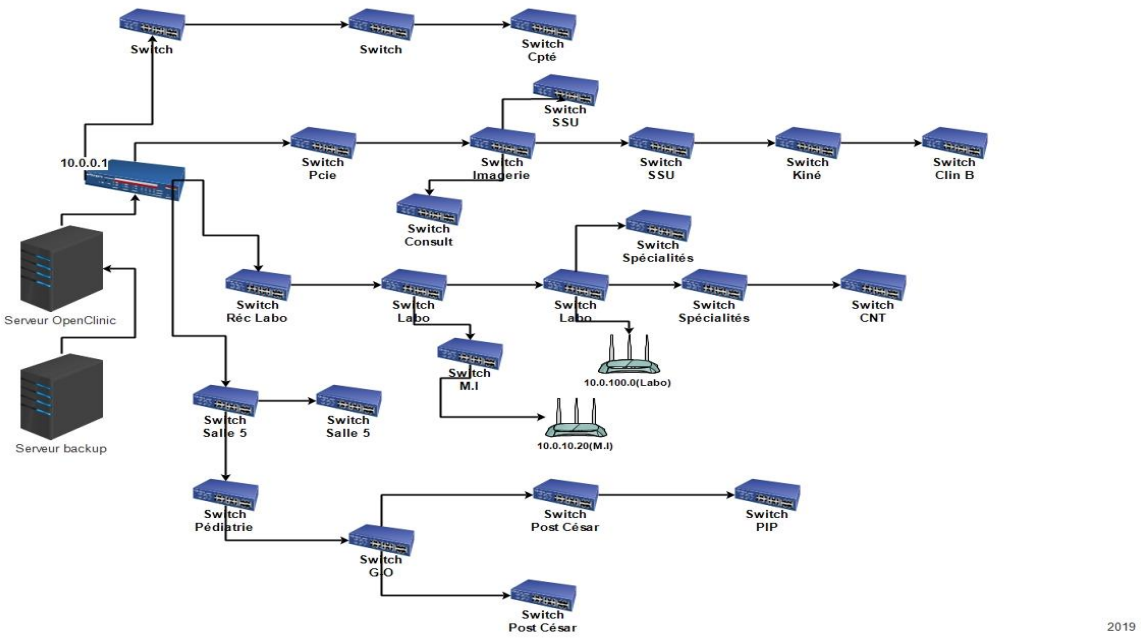


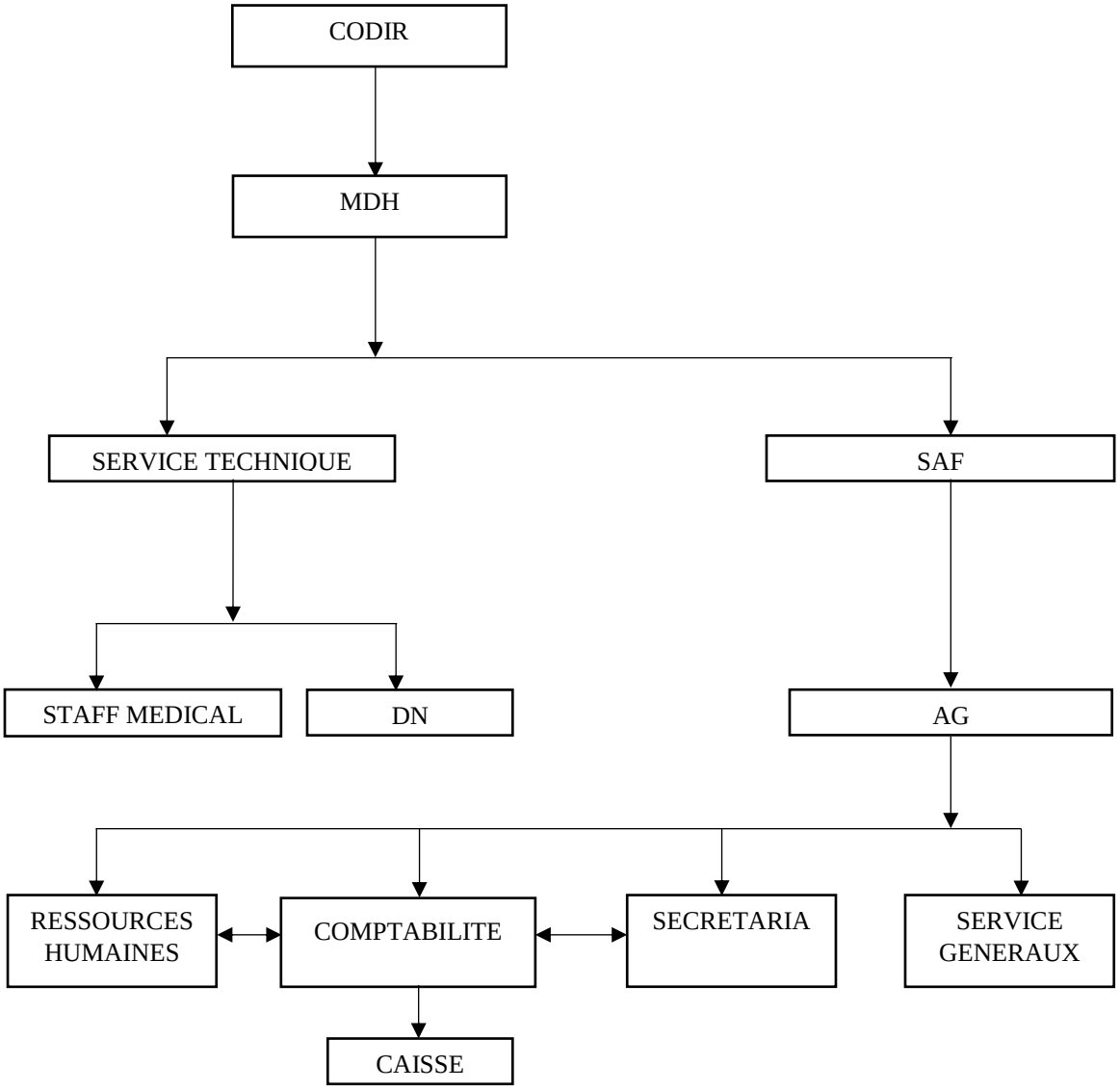
Figure 2 Topologie Intranet de l'HPGRB

1.1.3. L'hôpital de Ciriri

1.1.3.a. Localisation

L'Hôpital General de Référence Dr RAU CORIRI et est située à proximité de Marché de Mulwa et Collège Amani.

1.1.3.b. Organigramme



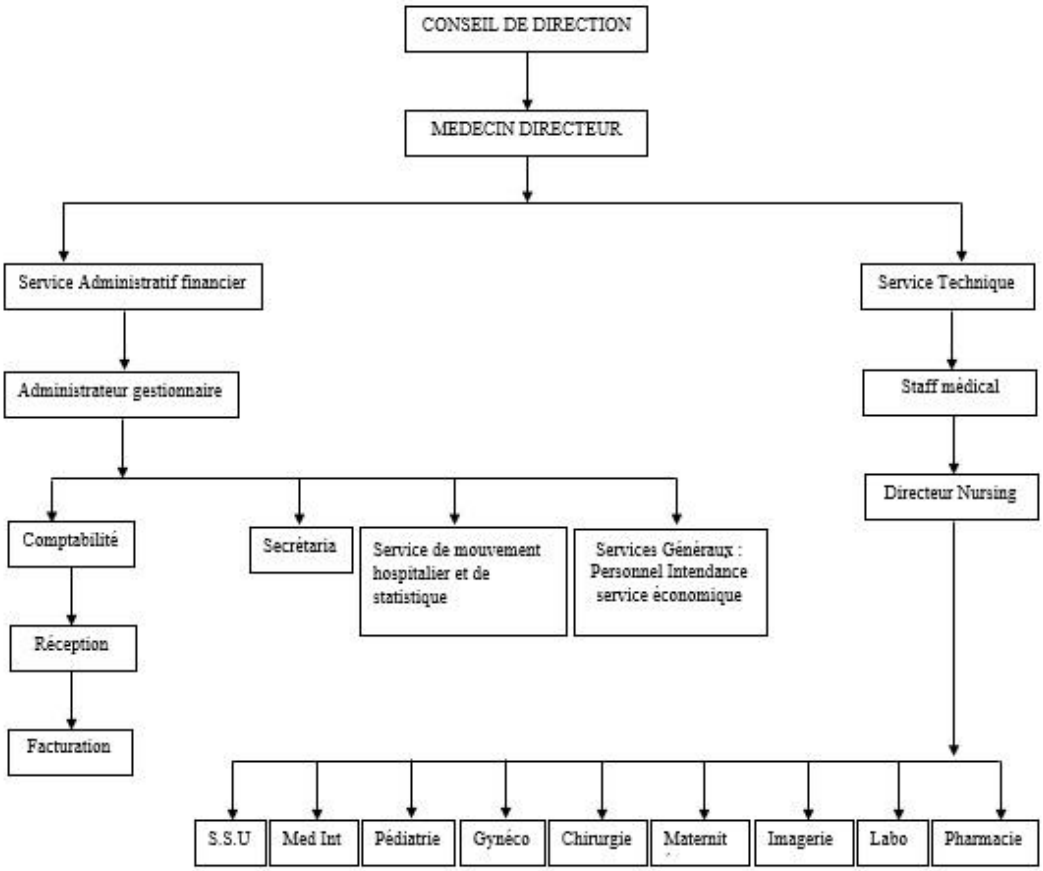
1.1.4. L'hôpital général de Kadutu.

1.1.4.a. Localisation

Cet hôpital est situé au Nord par la rivière WESHA qui la sépare de la zoné de santé de BAGIRA ; à l'est par la rivière KAWA et la route principale de l'avenue INDUSTRIELLE qui la sépare

de la zone de santé Urbaine d'IBANDA ; à l'ouest par la rivière KAWA qui la sépare de la zone de santé Rurale de KABARE ; au Sud-ouest par la zone de santé de NYANTENDE. Il a une superficie d'environ 15m et est constitué d'un relief montagneux, d'un climat humide, avec une température de 15C ; il est situé entre 1500m et 2190m d'altitude.

1.1.4.a. Organigramme



1.2. GENERALITE SUR LES RESEAUX INFORMATIQUE

1.2.1. Définitions

Un réseau informatique est un ensemble d'ordinateurs reliés entre eux grâce à des lignes physiques et échangeant des informations sous forme de données numériques (valeurs binaires, c'est-à-dire codées sous forme des signaux pouvant prendre deux valeurs : 0 et 1). [6]. C'est donc un ensemble d'ordinateurs et de périphériques connectés les uns aux autres. Un système informatique quant à lui est un ensemble de matériels et de logiciels destinés à réaliser des tâches mettant en jeu le traitement automatique des informations [25].

Notons que deux ordinateurs connectés ensemble constituent à eux seuls un réseau. Il permet ainsi de faire circuler des éléments entre chacun de ces objets selon des règles et protocoles bien définis [54]. Les réseaux informatiques permettent aux utilisateurs de communiquer entre eux et de transférer des informations. Ces transmissions de données peuvent concerner l'échange de messages entre utilisateurs, l'accès à distance à des bases de données ou encore le partage de fichiers [32].

En effet, nous pouvons dire qu'en reliant toutes les stations de travail, les périphériques, les terminaux et les autres unités de contrôle du trafic, le réseau informatique a permis aux entreprises de partager efficacement différents éléments (des fichiers, des imprimantes…) et de communiquer entre eux, notamment par courrier électronique et par messagerie instantanée. Il a permis aussi de relier les serveurs des données, de communication et de fichiers.

1.2.2. Les types de réseaux

En fonction de la localisation, la distance et le débit, les réseaux sont classés en trois types : On distingue différents types de réseaux (privés) selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue [43]. On fait généralement trois catégories de réseaux. Ainsi, les systèmes et réseaux interconnectés se subdivisent en réseaux locaux (LAN pour Local Area Network), réseaux dits métropolitains (MAN pour Métropolitain Area Network) et réseaux étendus (WAN pour Wide Area Network) [6].

Cette classification est essentiellement basée sur une notion de distance physique. Nous parlons de LAN lorsque les distances concernées sont de l'ordre de quelques dizaines de mètres, la plus longue distance ne pouvant pas dépasser quelques centaines de mètres. Lorsque la distance dépasse quelques centaines de mètres jusqu'à atteindre quelques kilomètres, nous parlons de MAN. Lorsque la distance est au-delà de quelques kilomètres nous avons alors affaire à un WAN [44]. Dans présent travail de mémoire, seul le réseau MAN sera étudié et utilisé pour interconnecter différents hôpitaux publics de la ville de Bukavu.

MAN C'est un réseau métropolitain qui désigne un réseau composé d'ordinateurs habituellement utilisés dans les campus ou dans les villes [6]. Ainsi, un MAN permet à deux nœuds (ordinateurs) distants de communiquer comme s'ils faisaient partie d'un même réseau local. Les MAN (*Metropolitan Area Network*) interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Un réseau MAN est formé

de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

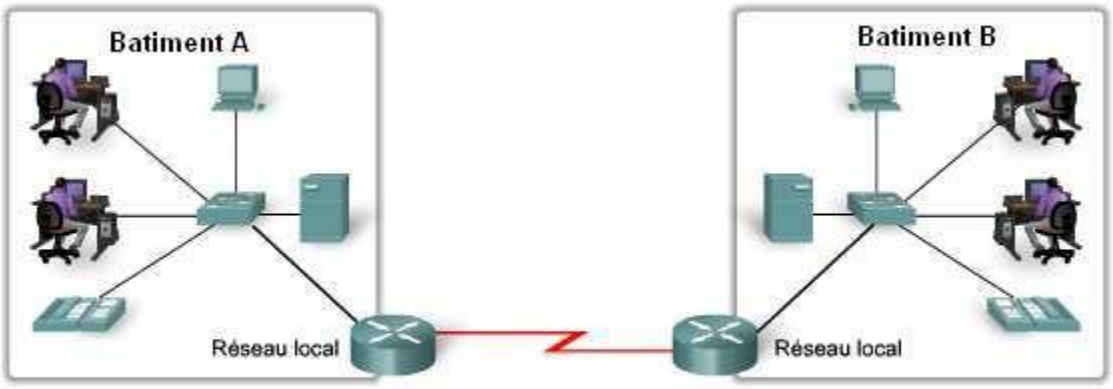


Figure 3 Schema d'un MAN [43]

1.2.3. Les différentes catégories des réseaux (Les structures des réseaux)

Nous distinguons deux catégories de réseaux : Réseaux poste à poste (Peer to Peer= P2P) et les réseaux avec serveur dédié (Server/client) [6]. Dans présent travail, nous allons utiliser cette deuxième catégorie de réseau.

1.2.3.a. Le réseau poste à poste

Dans une architecture d'égal à égal (appelée aussi « poste à poste », en anglais peer to peer, notée P2P), il n'y a pas de serveur dédié. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources. Un ordinateur relié à une imprimante pourra donc éventuellement la partager afin que tous les autres ordinateurs puissent y accéder via le réseau. L'application célèbre de ce type de réseau est celle du partage des fichiers (musiques ou films) entre une communauté d'utilisateurs reliés par internet [21].

Dans cette architecture, chaque poste ou station fait office de serveur et les données ne sont pas centralisées, l'avantage majeur d'une telle installation est son faible coût en matériels (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines (>10 postes) il devient impossible à gérer. Par exemple : Si on a 4 postes et 10 utilisateurs, chaque poste doit contenir les 10 mots de passe afin que les utilisateurs puissent

travailler sur n'importe quel poste. Mais si maintenant il y a 60 postes et 300 utilisateurs, la gestion des mots dépasse devient périlleuse [43].

1.2.3.b. Le réseau client/serveur

Il ressemble un peu au réseau poste à poste mais cette fois-ci, on y rajoute un poste plus puissant, dédié à des tâches bien précises. Cette nouvelle station s'appelle serveur. Le serveur centralise les données relatives au bon fonctionnement du réseau. Dans l'exemple précédant, c'est lui qui contient tous les mots de passe. Ainsi ils ne se trouvent plus qu'à un seul endroit. Il est donc plus facile pour l'administrateur du réseau de les modifier ou d'en créer d'autres. L'avantage de ce type de réseau est sa facilité de gestion des réseaux comportant beaucoup de postes. Son inconvénient majeur est son coût souvent très élevé en matériel [43].

En effet, en plus de postes de travail il faut se procurer un serveur qui coûte cher car c'est une machine très puissante et perfectionnée. De plus la carte réseau que nous mettons est de meilleure qualité que celle des postes de travail. De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une authentification via un annuaire, des bases de données, des applications etc [43].

1.2.4. Equipements d'Interconnexion des réseaux

Il est bon ici de rappeler que l'interconnexion est un mécanisme qui consiste à mettre en relation, indépendamment de la distance qui sépare et des protocoles qu'elle utilise, des machines appartenant à des réseaux physiquement distincts.

Dans cette section, nous allons juste citer les principaux équipements matériels mis en place dans les réseaux locaux que sont :

- **Les répéteurs**, permettant de régénérer un signal
- **Les concentrateurs (hubs),** permettant de connecter entre eux plusieurs hôtes
- **Les ponts (bridges),** permettant de relier des réseaux locaux de même type
- **Les commutateurs (switches)** permettant de relier divers éléments tout en segmentant le réseau

- **Les passerelles (Gateway),** permettant de relier des réseaux locaux de types différents
- **Les routeurs,** permettant de relier de nombreux réseaux locaux de telle façon à permettre la circulation de données d'un réseau à un autre de la façon optimale
- **Les B-routeurs**, associant les fonctionnalités d'un routeur et d'un pont [23].

1.2.5. Présentation de la Technologie WiMAX

Les zones rurales et même dans des milieux un peu reculés ont toujours été difficiles à desservir par les réseaux de télécommunication du fait de l'utilisation des câbles. Le Wifi qui a connu une évolution importante ces dernières années et son coût de plus en plus abordable devrait constitue la solution à ce problème. Le Wifi étant limite par sa portée, il sera uniquement utilisé pour les WLAN. La technologie WIMAX a donc pour mission de combler certaines défaillances d'interconnexion en permettant aux utilisateurs d'avoir un accès haut débit à Internet sans avoir besoin de se connecter sur les BLR filaires (câbles) mais plutôt une connexion longue distance et sans fil. Elle vise donc à fournir une connexion Internet à haut débit sur une zone de couverture de plusieurs kilomètres de rayon

Le WIMAX est complémentaire au Wifi et fait partie des réseaux WMAN. Cette technologie futuriste pourrait être employée dans les milieux urbains denses pour offrir des services larges bandes car l'utilisation des câbles serait encombrante. Elle est donc basée sur de nouvelles techniques de modulation, de codage et d'accès [45]. De ce fait Internet est un outil de travail incontournable dans la mesure où il intéresse le grand public, les entreprises, les universités, les organismes internationaux et autres. Bien qu'Internet offre des multiples services, pour en bénéficier il faut pouvoir y accéder. Plusieurs technologies en permettent l'accès. A savoir : le Satellite, les réseaux câblés, les réseaux mobiles et les réseaux sans fils. Dans la suite de notre travail nous allons présenter la technologie WIMAX.

1.2.5.a. Généralités sur le WIMAX

Le *WiMAX* a d'abord été conçu pour desservir des réseaux pouvant couvrir une municipalité entière. Ce type de réseau est aussi connu sous l'acronyme MAN « *Metropolitan Area Network* ». Les LAN « *Local Area Network* » sont des réseaux locaux, tel le *WiFi*, tandis que les PAN « *Personal Area Network* », sont des réseaux personnels, tel le *Bluetooth*. Les WAN « *Wide Area Network* » sont des réseaux couvrant de très longues distances [21]; [35] [4]; [56]. Chaque type de réseau a des caractéristiques propres ainsi que des besoins particuliers. Par exemple, un

réseau de type WAN qui dessert souvent plusieurs grands clients corporatifs doit avoir des mécanismes de gestion qui permettent de garantir une fiabilité, de segmenter les communications pour garantir la confidentialité, permettre la redondance et facturer adéquatement l'utilisation.

Les réseaux locaux, à l'opposée, n'ont pas à se préoccuper de tous ces éléments de coûts mais en contrepartie, ils doivent assurer un service très fragmenté et variable entre plusieurs types d'ordinateurs et de périphériques. Le *WiMAX* se trouve à mi-chemin ([11] Coupechoux, Godlewski, & Martins, n.d). Il doit à la fois tenir compte d'une importante transmission d'informations mais aussi distribuer ces informations de façon sécurisée à des clients indépendants, tout en comptabilisant les coûts associés à chacun [24] [34].

Il est à noter que le forum WiMAX est un consortium crée en 2003, sous l'impulsion d'Intel pour assurer l'interopérabilité et la compatibilité entre les différents équipements exploitant les normes WMAN les plus en vue : IEEE 802.16 et ETSI *HyperMan.* C'est un forum ouvert constitué essentiellement d'équipementiers et d'opérateurs télécoms qui est assimilable à la WiFi Alliance pour le protocole 802.11

- **Définition, origine et types de WIMAX**

Le WIMAX qui a pour acronyme : **Worldwide Interoperabilty for Microwave Access** est une norme basée sur le standard de transmission radio IEEE 802.16 valide par l'organisme mondial de normalisation IEEE [4]; [11] [45]. Il est développé per le WiMAX forum qui rassemble une soixantaine d'industriels dont Intel, Alvar ion, NOKIA, SIEMENS… Le standard 802.16 possède comme premier sous ensemble le 802.16 valide en 2001, qui opérait dans la bande de fréquence de 10 à 66 GHz. Cette version du standard fonctionnait en visibilité direct entre l'émetteur et le récepteur. Elle a été améliorée en 2003 et a été appelé le 802.16a qui a vais introduit une extension de la bande de fréquence de 2 à 11 GHz et permet une communication sans nécessité de ligne de vue. L'arrivée du 802.16-2004 en juin 2004 a permis d'intègres de nouvelles techniques plus robuste et plus efficaces [34].

Après la liaison fixe point à point la technologie WiMAX a évolué vers la mobilité (le ROAMING). En effet la version 802.016e sortie en 2005 intègre le ROAMING. Grace à son débit et à sa couverture le WiMAX sera à la portée d'un nombre élevé d'utilisateurs du fait de son cout d'installation et d'utilisation relativement faible. La demandes des utilisateurs étant de plus en plus orientes vers les applications larges bandes le WIMAX est désigné pour supportes

tous ces services sur un même terminal, car son haut débit, ses techniques très avances de multiplexage et de modulation et sa qualité de service élevé vont lui permettre d'offrir des services très variés [34].

La norme 802.16 a connu de nombreuses évolutions au fur et à mesure qu'elle gagne en popularité. Destinées originellement à desservir les zones les plus éloignées en haut débit en tant que réseau d'accès, cette norme s'oriente de plus en plus vers la mobilité notamment dans la version 802.16e. Le WiMAX est principalement fondé sur une topologie en étoile bien que la topologie maillée soit possible. La communication peut être réalisée en ligne de vue (LOS : Line Of Sight) ou non (NLOS). La dernière mouture du standard qui nous intéresse ici est le standard IEEE 802.16 2005 qui couvre les terminaux mobiles et définit des mécanismes évolués de gestion des handovers**.** Basé sur le standard IEEE 802.16, le WiMAX est une technologie de transmission haute débit par ondes radio. Contrairement au Wi-Fi destiné à l'origine à la mise en place de réseaux locaux, le WiMAX est conçu dès le départ pour la couverture des surfaces importantes [34].

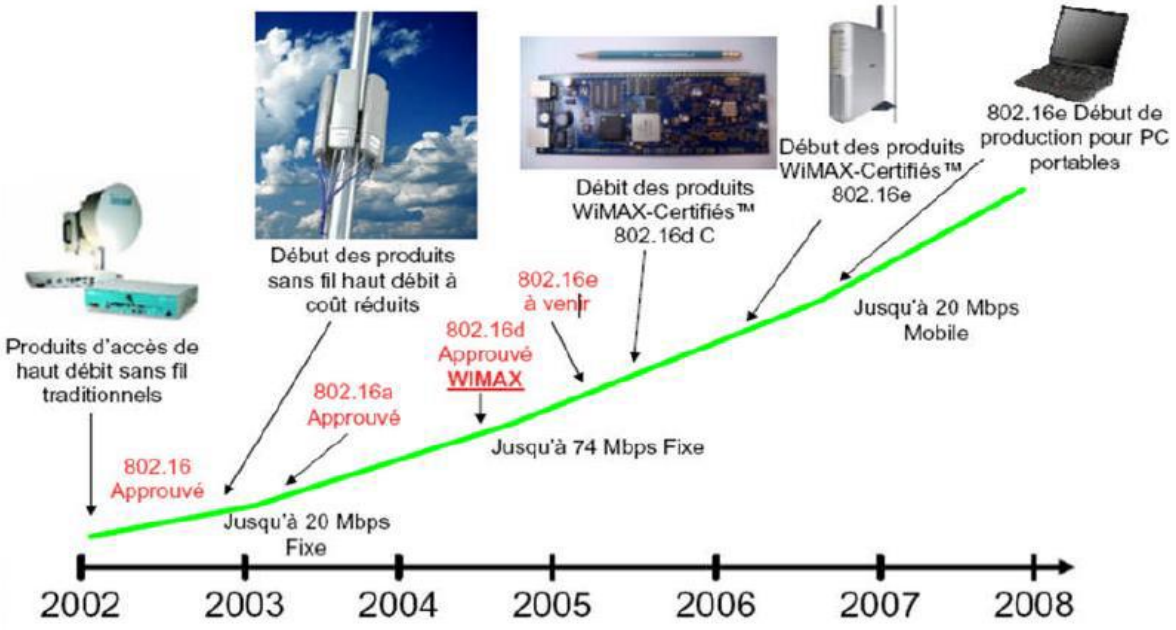


Figure 4 Historique du WIMAX

La norme 802.16 est porteuse beaucoup de promesses : avec une grande couverture, une grande efficacité spectrale et un débit important, le WIMAX représente une vraie alternative des systèmes nécessitant des connections câblées, comme le DSL (Digital Subscriber Line) par exemple. Le réseau WiMAX étant basé sur différentes versions de la norme 802.16 et existe dans deux configurations **fixe** et **mobile**. La configuration fixe est utilisée pour concurrencer

les technologies d'accès DSL. La configuration mobile peut concurrencer les hots spots du WiFi comme elle peut également concurrencer les réseaux cellulaires. Ainsi le WiMAX est considéré comme une technologie B3G (Beyond 3G) [34].

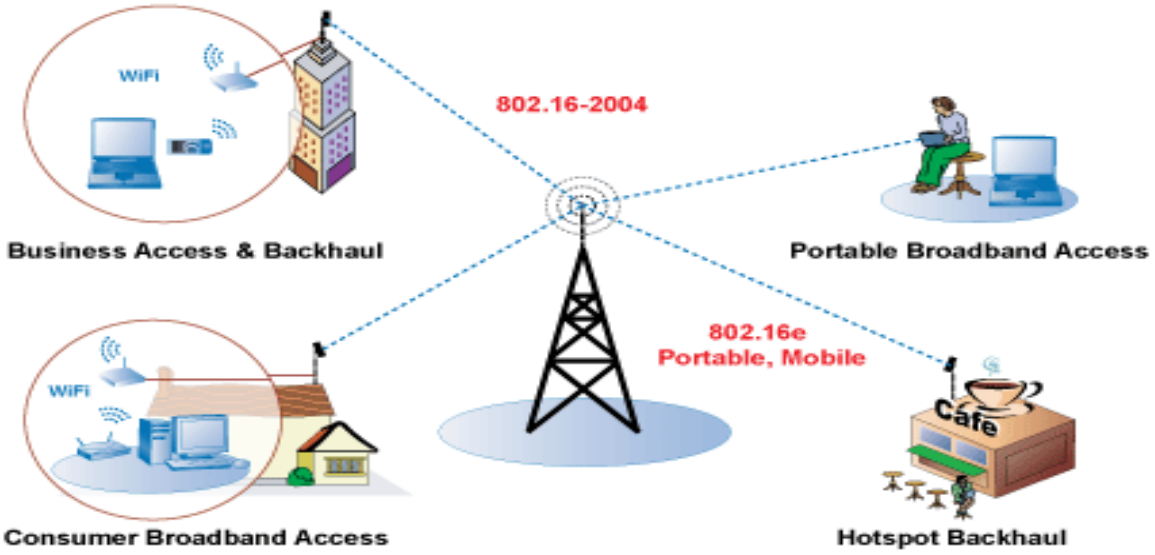


Figure 5 Exemple d'un réseau WIMAX avec les deux variantes fixe et mobile [51]

- **WIMAX FIXE-IEEE 802.16-2004**

Le standard IEEE 802.16-2004 est prévu pour un usage fixe, c'est-à-dire un usage via une antenne fixée sur le toit par exemple, semblable aux antennes TV. Le WIMAX opère dans les bandes de fréquence 2.5 GHz et 3.5 GHz, pour lesquelles une licence d'exploitation est nécessaire, ainsi que la bande libre des 5.8 GHz. Le débit théorique est de 75 Mbits par seconde sur une portée de 10 km**.**

- **WIMAX MOBILE-802.16e-2005**

En anglais Wimaxtable, c'est le standard IEEE 802.16e. Il prévoit la possibilité de connecter des clients mobiles au réseau internet. On peut ainsi imaginer à terme la possibilité pour les téléphones mobiles de se connecter à ce réseau haut débit. Le débit théorique est plus faible que le WIMAX fixe mais permettra néanmoins d'atteindre 30 Mbits par seconde sur une distance de plus de 3 km

- **Apport de WIMAX**

L'objectif du WIMAX est de fournir une connexion Internet à haut débit sur une zone de couverture de plusieurs kilomètres de rayon. Le standard WIMAX possède l'avantage de permettre une connexion sans fil entre une station de base et des milliers d'abonnés sans nécessiter de ligne visuelle directe LOS ou NLOS. Dans la réalité le WIMAX ne permet de franchir que de petits obstacles tels que des arbres ou une maison mais ne peut en aucun cas traverser les collines ou les immeubles. Le débit réel lors de la présence d'obstacles ne pourra ainsi excéder 20 Mbit/s.

Les premiers déploiements en WIMAX devraient permettre à des zones isolées, mal desservies par le DSL ou le câble ou souhaitant tirer profit d'une connexion sans fil, de disposer d'un accès Internet large bande. Le développement du WIMAX pourrait donc jouer un rôle important dans l'aménagement numérique du territoire. Le débit et la portée présentent les atouts du WiMax. Il fonctionne à 70 Mbit/s maximum théoriquement dans des conditions extrêmement favorables, 12 Mbits/s pratiquement et peut couvrir des zones de rayon allant jusqu'à 50 Km [3] [11][34]. Le standard IEEE802.16 vise à offrir donc un moyen de communication sans-fil à la fois innovant, rapide à déployer et à bas coût. En plus de cela, il entretient une interopérabilité complète avec l'ensemble des produits existants chez tous les constructeurs respectant les normes de l'IEEE

- **Architecture du WIMAX**

Le réseau WIMAX est formé d'un ensemble d'équipement connecté au backbone internet ou à un réseau IP prive ou à un réseau mobile. Les deux équipements que nous trouvons dans le réseau sont la station de base (WIMAX base station ou BS) et l'équipement d'abonne (WIMAX subscriber terminal ST). Le réseau peut être subdivisé en deux sous réseaux : le backhaul et le réseau proprement dit. Le backhaul constitue le réseau formé par l'ensemble des BS interconnectés point à point entre elles. Une visibilité directe est nécessaire pour connecter deux BS. Le réseau d'accès représente la liaison radio entre une BS et l'ensemble des ST qui lui sont connecté. Cette liaison est généralement qualifiée de point a multipoint. Ce sous réseau permet l'accès des abonnes dans le réseau global. Avec une propagation en NLOS cette connexion BS – ST ne nécessite pas une visibilité directe (norme IEEE 802.16-2004) [45].

L'architecture de la technologie WIMax se compose donc principalement de stations de base (*BS, Base Station),* et des stations mobiles (SS, *Subscriber Station*). La station de base joue le rôle d'une antenne centrale chargée de communiquer et de desservir les stations mobiles qui, à

leur tour, servent les clients utilisant le WIFI ou l'ADSL. La figure (6) représente l'architecture générale d'un réseau d'accès à large bande.

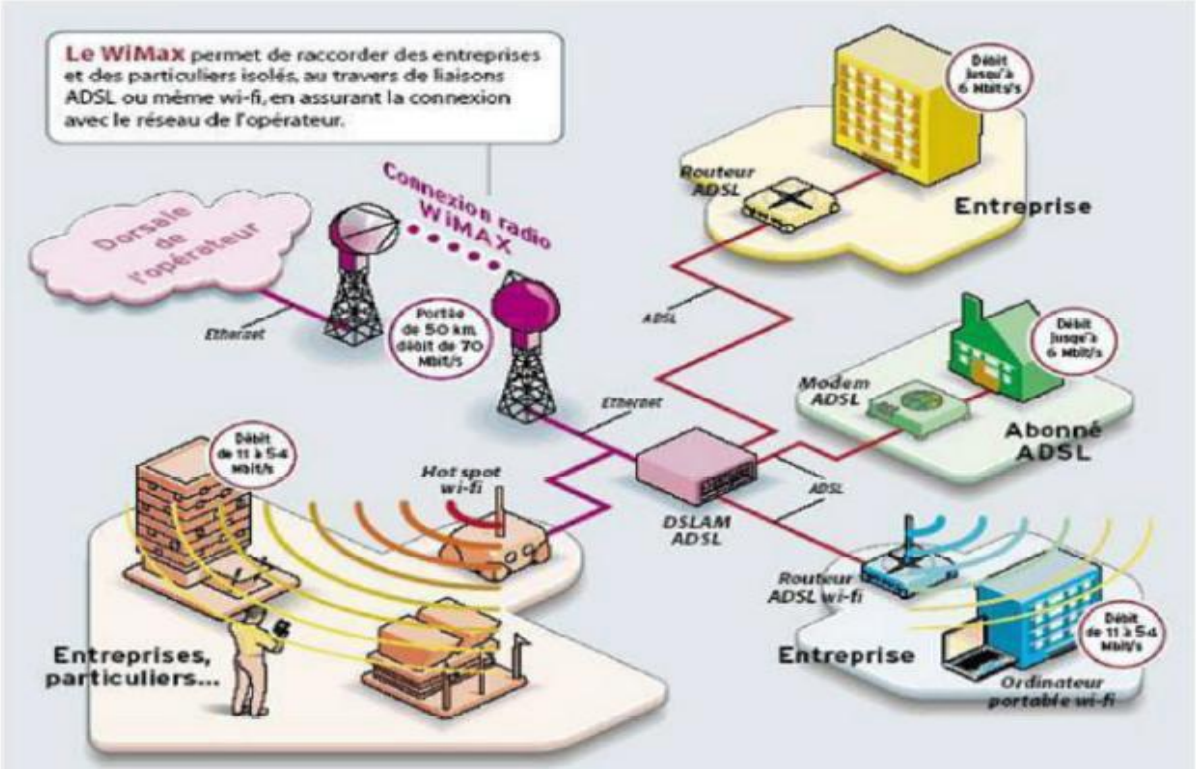


Figure 6 Exemple d'un réseau WiMax

La Figure 6 illustre un exemple d'un réseau WiMAX avec ses deux variantes, à savoir fixe et mobile. Tel que le montre la figure 6, ce réseau se compose essentiellement d'une station de base, qui joue le rôle d'un noeud émetteur, et des stations réceptrices qui jouent le rôle des clients WiMAX. Nous allons ultérieurement présenter le principe de fonctionnement d'un tel type de réseau [41]

L'architecture End to End montre la place du réseau WIMAX dans représentation plus générale du réseau. Elle présente les différents segments du réseau : UE, NAP, NSP, et le réseau internet. L'UE est composée de l'ensemble des équipements d'abonnées connecté au réseau WIMAX. Le NAP est le réseau composé des bs WIMAX et les NSP représentent les fournisseurs de services.

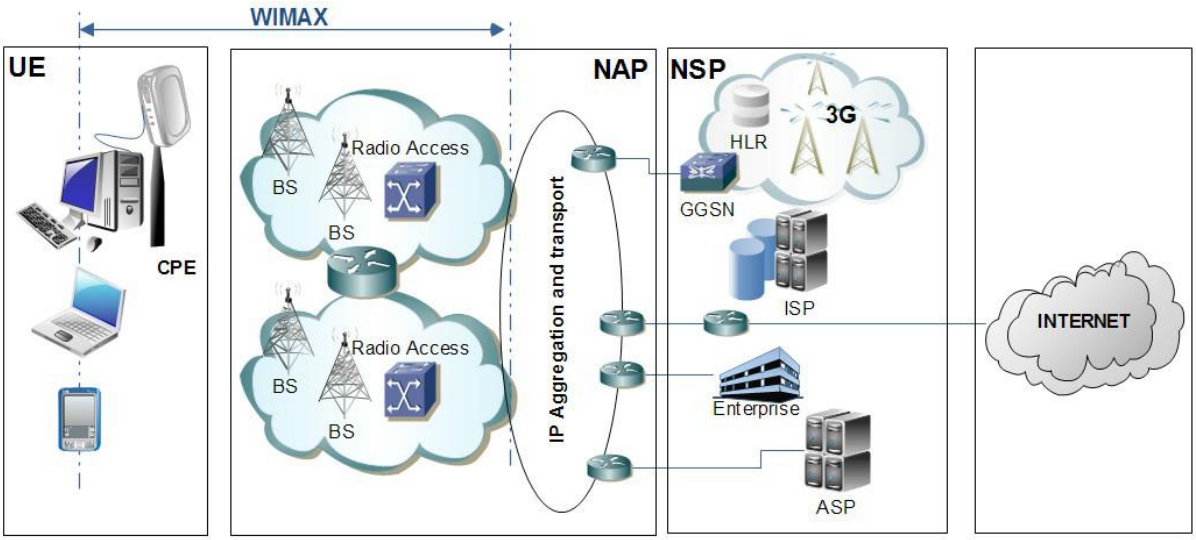


Figure 7 Architecture End to End [45]

Le réseau WIMAX est ainsi située entre les parties UE et NAP et offre aux utilisateurs un accès fournisseurs de services via le réseau de transport.

- **Bande passante**

La bande de fréquence du WIMAX est de 2-60 GHz subdivisée en plusieurs sous bandes avec ou sans licences. Dans la 2-11 GHz la bande des 2.5 GHz ainsi que celle des 3.5 GHz sont avec licence, alors que celle des 5.8 GHz est sans licence. L'avantage des systèmes travaillant avec les bandes à licences est que ces dernières offres plus de puissance en downlink et donc supporte mieux les antennes indoor. L'octroi d'une licence peu prendre du temps et coute souvent cher, ce qui entraine la plupart des fournisseurs a utilisé les bandes sans licences. Ceci donne encore un avantage a utilisé les bandes avec licence car leur nombre réduit, cela diminue les interférences. Cette bande de fréquence 2-11 GHz correspond aux fréquences basses du WIMAX. C'est cela qui règle le problème de communication en ligne du vue (du LOS au NLOS) [4].

La bande 5.8 GHz est la plus utilisée dans le monde car elle est gratuite et les ISP peuvent les exploiter gratuitement. Dans la bande de fréquences 10-66 GHz, en raison de la longueur d'onde courte, la propagation par visibilité directe "LOS" (Line of Sight) est nécessaire et par conséquent l'effet de propagation multi-trajets est négligé. Dans cette bande de fréquence la norme permet de fournir des débits jusqu'à 120 Mbit/s. La disponibilité abondante de la bande passante est également une autre raison pour utiliser cette gamme de fréquences. Contrairement aux gammes de fréquences inférieures, où les bandes de fréquences sont souvent moins de

100MHz de large, la plupart des bandes de fréquences supérieures à 20 GHz peut fournir plusieurs centaines de mégahertz de bande passante. En outre, les canaux à l'intérieur de ces bandes sont en général 25 ou 28 MHz de large [56]

- **Les différentes normes.**

Le WIMAX est une famille des normes, qui définit des connexions à haut débit par voie radio. Le développement des normes de 802.16 et leurs spécificités techniques sont expliqués dans le tableau 2.1, Le standard IEEE 802.16 **e** est la version la plus avancé et la plus intéressant. Cette version apporte la mobilité [11] [34].

L'évolution du standard IEEE 802.16 est ainsi regroupée dans le Tableau suivant :

Standard	**Description**	**Publié**	**Statut**
IEEE std 802.16-2001	Définit des réseaux métropolitains sans fil utilisant des fréquences supérieures à 10 GHz (jusqu'à66 GHz)	8 avril 2002	Obsolètes
IEEE std 802.16c-2002	Définit les options possibles pour les réseaux utilisant les fréquences entre 10 et 66 GHz.	15 janvier 2003	
IEEE std 802.16a-2003	Amendement au standard 802.16 pour les fréquences entre 2 et 11 GHz.	1er Avril 2003	
IEEE std 802.16-2004 (également désigné 802.16d)	Il s'agit de l'actualisation (la révision) des standards de base 802.16, 802.16a et 802.16c.	1er octobre 2004	Obsolète/actifs
IEEE 802.16e (également désigné IEEE std 802.16e-2005)	Apporte les possibilités d'utilisation en situation mobile du standard, jusqu'à 122 km/h.	7 décembre 2005	Actifs
IEEE 802.16	Spécifie la MIB (Management Information Base), pour les couches MAC (Media Access Control) et PHY (Physical)	22 janvier 2006	
IEEE 802.16m	Débits en nomade ou stationnaire jusqu'à 1Gbit/s et 100Mbits/s en mobile grande vitesse. Convergence des technologies WIMAX, WiFi et 4G.		En cours

Tableau 1 L'évolution des différentes normes d'IEEE 802.16x

- **Etude technique de WiMAX**
  - **Etude en couches**

Comme avec toutes les normes IEEE 802.x, les protocoles définis concernent les deux couches les plus basses du modèle OSI (couche physique et Liaison de donnée). La couche liaison de données étant divisée en deux sous couches : MAC (Media Access Control) et LLC (Logical Link Control). L'architecture de couches et de protocoles définie dans le WiMAX/802.16 est

montrée dans la figure 6. On peut voir que la norme 802.16 définit seulement la couche physique et la couche MAC. La couche MAC elle-même divisée en trois sous couches : CS (sous couche de convergence), CPS (sous couche des parties communes du MAC) et SS (sous couche de sécurité) [56].

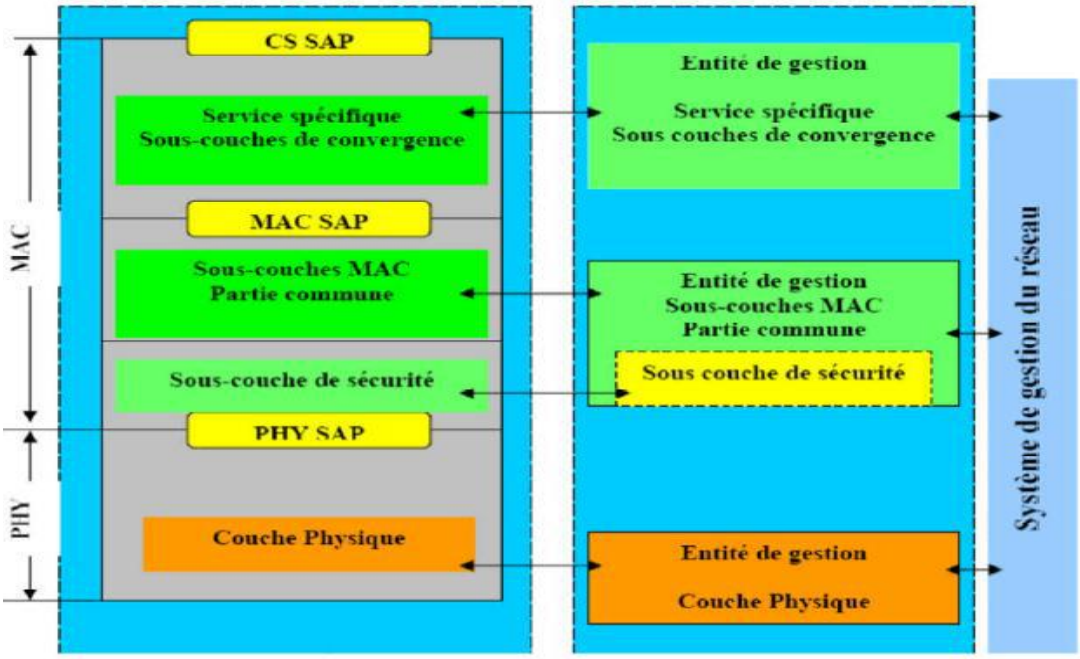


Figure 8 Structure en couche du standard IEEE802.16

- **La couche MAC**

La couche MAC prend en charge le transport des cellules ATM (Asynchronous Transfer Mode) mais aussi celui des paquets IP et joue un rôle important dans la gestion de la qualité de service (QoS). Elle est composée principalement de trois sous-couches :

- **La sous-couche SSCS** : La sous-couche de convergence spécifique (Service Specific Convergence Sublayer)
- **La sous-couche CPS** : La sous-couche commune (MAC Common Part Sublayer)
- **La sous-couche PS** : La sous-couche sécurité (Privacy Sublayer).

- **La couche physique**

Dans les spécifications 802.16-2004 la modulation utilisée est l'OFDM. La couche PHY comme dans d'autre norme a pour but de réaliser les mécanismes de modulation et de démodulation, le codage et le décodage, de détection et de correction d'erreur. Comme toutes les technologies utilisant la voie hertzienne le WiMAX est soumis aux interférences du milieu

dans lequel les ondes se propagent. Plusieurs techniques permettent d'atténuer la perturbation du signal par le bruit environnant. Ces techniques ont évolué avec les versions du WiMAX

La couche physique pour la spécification 11-66 GHZ se base sur une propagation « en ligne de vue » (LOS) càd les stations qui communiquent ensemble sont visibles l'une de l'autre directement sans obstacles. Pour la spécification 2-11 GHZ, la couche physique a été implémentée pour répondre au cas où les stations communiquent « en non ligne de vue » (NLOS), dans le cas des environnements urbains avec la présence d'obstacles entre deux stations. Pour répondre à ces spécifications, trois types d'interfaces de transmission ont été définies :

- **SC (Single Carrier) :** elle définit une transmission sur un seul canal de fréquence.
- **OFDM (Orthogonal Frequency Division Multiplexing) :** cette interface utilize plusieurs bandes de fréquence qu'elle divise en plusieurs porteuses pour la transmission d'un signal. Chaque bande est utilisée à des fins différentes.
- **OFDMA (Orthogonal Frequency Division Multiple Access) :** similaire à l'OFDM, cette interface offre un plus grand nombre de porteuses du fait du multiplexage effectué sur la fréquence. Dans ce qui suit, nous allons aborder les différentes techniques de multiplexage et duplexage qui peuvent être mises en œuvre au niveau de la couche physique de la norme 802.16. Nous pouvons ainsi les représenter dans les figures suivantes :

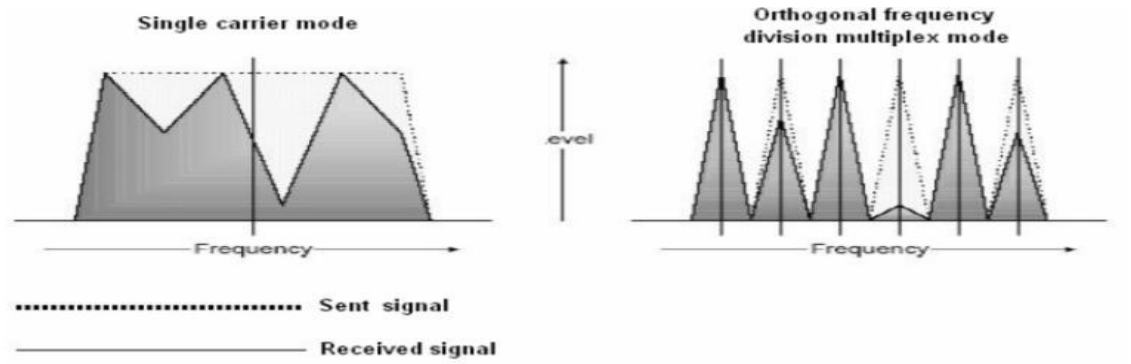


Figure 9 : Modulation simple porteuse (à gauche) Modulation OFDM (à droite) (Différence entre les signaux SC et OFDM reçus)

L'OFDM permet l'utilisation optimale de la bande de fréquence et opère à des débits très élevés du fait de la transmission de plusieurs symboles en une fois. Mais néanmoins elle a comme

inconvenants, la consommation de puissance importante et les erreurs de synchronisations induise des déphasages sur le symbole reçu.

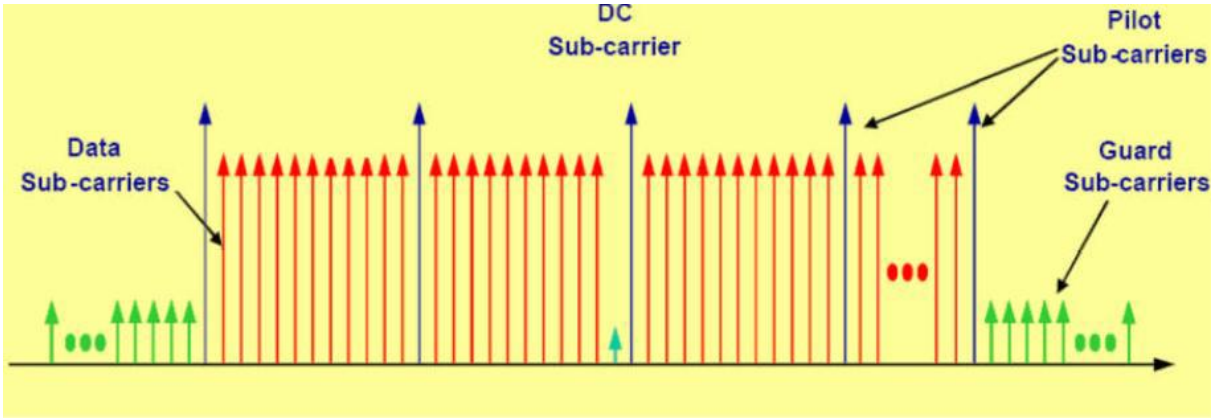


Figure 9 Description fréquentielle de l'OFDMA

Le symbole OFDMA est divisé en sous canaux (*subchannels*), de supporter l'accès multiple, et pour une meilleure adaptation aux techniques avancées des antennes. Pour le *downlink* on dispose de deux modes d'utilisation des subchannels *:* FUSC (*Full Usage of Subchannels*) et PUSC (*Partial Usage of Subchannels*)

Pour l'*uplink*, on fait la permutation premièrement (partition en des *subchannels*), ensuite on fait l'attribution des porteuses pilotes et des porteuses données dans chaque *subchannel*. D'autres types de permutation peuvent être aussi utilisées, dont on peut citer l'AMC (Advanced Modulation and Coding) et le TUSC (Tile Usage of Subchannels).

Un slot dans l'OFDMA est la plus petite unité d'allocation des données possible. Pour qu'il soit bien défini, il exige les 2 dimensions : temps et *subchannels*. La définition des slots OFDMA dépend de la structure du symbole OFDMA, qui varie pour l'*uplink* et le *downlink*, pour le FUSC et le PUSC, et pour les permutations des sous porteuses. Par exemple si on utilise le mode PUSC pour l'*uplink* avec une certaine permutation, le slot utilisé est égal à 1 *subchannel* x 3 symboles OFDM.

- **Système de gestion**

Le système de gestion permet d'effectuer les opérations d'administration, de maintenance, et de configuration nécessaire pour une bonne exploitation du réseau. Il est base comme la plut part des réseaux de télécommunication sur le modèle de management TMN qui prend en compte les cinq fonctions de management appelées FCAPS.

- **Fault** : gestion des erreurs. Elle détecte et corrige les erreurs des unités de réseau comme les équipements des abonnés.
- **Configuration :** gestion de la configuration. Elle permet de suivre les changements survenus dans le réseau et d'identifier chaque équipement
- **Accounting :** gestion des couts. Elle permet de gérer les données comptables en vue de facturer les communications.
- **Performance :** gestion des performances. Elle offre une source continue de supervision es performances et d'allocation des ressources du réseau.
- **Security :** elle contrôle l'accès aux ressources du réseau, la fiabilité des communications, le cryptage et le décryptage des donnes qui circulent sur le réseau.

Techniques de Duplexage

La transmission de signaux WiMAX se fait sous forme de trames. Deux modes de duplexage sont possibles : fréquentiel (FDD ou Frequency Division Duplexing) dans lequel les liens montants et descendants fonctionnent sur différents canaux (50 à 100 MHz) et temporel (TDD ou Time Division Duplexing) dans lequel les liens montants et descendants partagent un canal ; mais ne transmettent pas simultanément (Figure 9). Cependant, le mode TDD est préféré au mode FDD [4].

A. TDD (time division duplex)

Ici l'émission et la réception se font sur le même canal a des périodes de temps différentes. Donc uplink et downlink sur le même canal. Cela veut dire que l'utilisateur soit est entrain de recevoir soit d'émettre soit inactif et dans ce dernier cas la ressource peut être alloue à un autre usager. C'est un multiplexage temporel dans les deux sens de transmission sur une seule fréquence. Les voies montantes et descendantes utilisent à tour de rôle la même fréquence. Les avantages du TDD sont entre autres : elle est adaptée pour les cellules de petite taille, elle est plus convenable pour l'internet et les interférences sont très réduites. Ses inconvénients sont : les équipements coutent chers et la synchronisation est très complexe.

B. FDD (Frequency division duplex)

Ici une paire de fréquence est allouée à chaque utilisateur, une fréquence pour l'uplink et une pour le downlink. Ici les communications peuvent se faire de manière simultanée. Le WiMAX utilise le HFDD (Half- Duplex FDD). Le HFDD mixe les liens pour offrir tour à tour du full et du Half Duplex [52].

Les Avantages du FDD sont : elle supporte la mobilité, elle est utilisée dans les cellules larges, elle est adaptée pour le type d'accès symétrique, les délais d'accès sont réduits, les équipements sont moins chers. Ses inconvénients sont entre autres : elle utilise une très grande bande de fréquence et elle a une forte présence des interférences.

Notons ici que, les modes FDD et TDD supportent tous les deux, une adaptation du profil de "burst" dans lequel les options de codage et de modulation peuvent être assignées dynamiquement aux rafales de "burst". Cette adaptation dynamique est fonction des conditions d'émission-réception radio.

1.2.5.b. La sécurité et la qualité de service [45].

Le WIMAX possède un système de sécurité très avancé. Avant de communiquer les SS doivent être authentifiés et autorisés à rejoindre le réseau. L'authentification et l'autorisation se font dès la base de la connexion. Et de plus chaque connexion est identifiée par un identifiant de connexion le CID (Connection Identity). Nous pouvons aussi noter que les méthodes de modulation, de codage et de multiplexage constituent une seconde barrière de sécurité des transactions sur l'interface air BS-SS.

Pour la qualité de service (QoS), les connexions de WIMAX sont accompagnées d'une multitude de services. Un flux de service est un flux bidirectionnel de données qui garantit une certaine qualité de service. Le WIMAX supporte quatre types de flux de services :

- **Unsolicited grant service (UGS**) : Ce service est désigné pour supporter des services dépendant du délai de temps de latence tel que la VoIP. Il offre une garanti strict du débit et du temps de latence, et c'est un service offert en ATM.
- **Real time polling service (RTPS)** : Ce service supporte des paquets de données de taille variable. Ce sont généralement des flux multimédias comme la vidéo. Il offre des garantis pour les débits mais ne tient pas trop compte du temps de latence.
- **Non real time polling service (NRTPS)** : Ce service garantit uniquement le débit il est destiné pour des applications ne dépendant pas du temps de latence tel que les emails.
- **Best effort service (BES)** : Ce service ne donne aucune garanti mais offre toutes les possibilités pour n'importe quelle application. Il est surtout destiné pour les applications comme l'accès au web.

1.2.6. Le modèle OSI

Le modèle OSI a été conçu par l'ISO (International Organization for Standardization) pour fournir un cadre pour concevoir une suite de protocoles pour système ouverts [22]. Le modèle OSI décrit donc la manière dont deux éléments d'un réseau (station de travail, serveur, etc.) communiquent, en décomposant les différentes opérations à effectuer en sept étapes successives, qui sont nommées [43]. Ce modèle est un modèle de référence en ce qui concerne les réseaux. Il décrit les concepts et les démarches à suivre pour interconnecter des systèmes, en décomposant les différentes opérations à effectuer en sept étapes successives, qui sont nommées : physique, liaison, réseau, transport, session, présentation, application.

Schéma de sept couches OSI

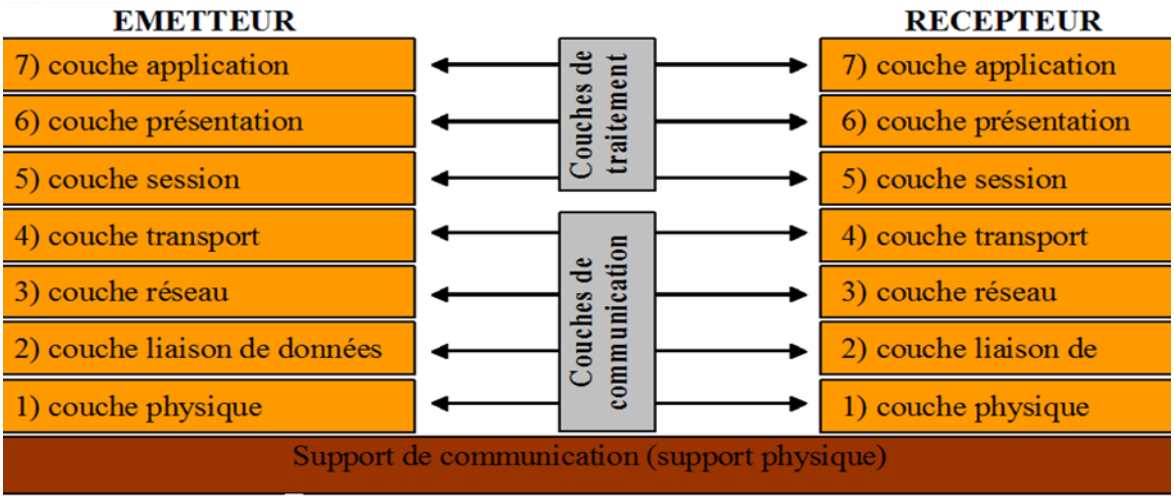


Figure 10 Architecture OSI

Le modèle comporte sept couches succinctement présentées ci-dessus de bas en haut. Ces couches sont parfois réparties en deux groupes.

On distingue :

- Les couches basses (1-4) relatives au transfert de l'information ;
- Les couches hautes (5-7) relatives au traitement réparti de l'information ;

Les couches basses sont plutôt orientées communication et sont souvent fournies par un système d'exploitation c'est-à-dire que les couches hautes sont plutôt orientées application et réalisées par des bibliothèques ou un programme spécifique. Dans le monde IP, ces trois couches sont

rarement distinguées que toutes ses fonctions sont considérées comme partie intégrante du protocole applicatif [15].

- **Couche1 : (Physique)** Elle s'occupe de la transmission des bits de façon brute sur un canal de communication. Cette couche doit garantir la parfaite transmission des données. L'unité d'information typique de cette couche est le bit, représenté par une certaine différence de potentiel.
- **Couche2 : (Liaison de données)** Elle va transformer la couche physique en une liaison a priori exempte d'erreurs de transmission pour la couche réseau. Elle fractionne les données d'entrée de l'émetteur en trames, transmet ces trames en séquence et gère les trames d'acquittement renvoyées par le récepteur. L'unité d'information de la couche liaison de données est la trame.
- **Couche 3 : (Réseau)** Elle assure l'acheminement, le routage (choix du chemin à parcourir à partir des adresses), des blocs de données entre les deux systèmes d'extrémités, ainsi elle contrôle également l'engorgement du sous-réseau.
- **Couche 4 : (Transport)** Elle assure le contrôle du transfert de bout en bout des informations entre les deux extrémités, afin de rendre le transport transparent pour les couches supérieures, elle assure le découpage des messages en paquets pour le compte de la couche réseau et les constitue pour les couches supérieures. Un des tout derniers rôles à évoquer est le contrôle de flux. C'est l'une des couches les plus importantes, car c'est elle qui fournit le service de base à l'utilisateur, et c'est par ailleurs elle qui gère l'ensemble du processus de connexion, avec toutes les contraintes qui y sont liées.
- **Couche 5 : (Session)** Elle assure l'échange de données, entre deux applications distantes. Elle réalise le lien entre les adresses logiques et les adresses physiques des tâches réparties. Elle assure surtout la synchronisation de l'échange (qui doit parler, qui parle…) entre deux programmes d'application devant coopérer. Dans ce dernier cas, ce service d'organisation s'appelle la gestion du jeton. Elle assure aussi la reprise de l'échange en cas d'erreurs.
- **Couche 6 : (Présentation)** Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut faire la mise en forme des données, la conversion des codes (ASCII), pour délivrer à la couche application un message compréhensible. Elle peut aussi assurer le décryptage et la compression de données.

- **Couche 7 : (Application)** Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie.

1.3. Analyse de l'existant et identification des problèmes

Cette section a pour rôle de montrer les besoins du client, ainsi que les besoins fonctionnels et non fonctionnels de la future application, de préciser les livrables et les risques les plus critiques du projet. L'étude préalable débute par l'analyse de la situation et permet de proposer une architecture globale de la situation, en tenant compte des orientations de gestion, d'organisation et de choix technique. L'étude de l'existant conduit à une évaluation des fonctions, des structures et des systèmes qui composent l'établissement. Toutefois cette étude a pour but de découvrir les points fort et les points faibles du système étudié et de concevoir un nouveau système dans différents hôpitaux publics de la ville de Bukavu dont : l'hôpital général de référence de Bagira, l'hôpital provincial général de référence de Bukavu, l'hôpital de Ciriri.et l'hôpital général de Kadutu.

1.3.1. Cahier des charges

Cette section a pour but d'établir les spécifications du système à implémenter. A cette fin, nous nous efforcerons à définir aussi précisément que possible les besoins des futurs utilisateurs du système. Ce préalable nous permettra de détailler le cahier des charges en inventoriant chaque fonctionnalité du programme. Le cahier des charges qui accompagne ce travail de mémoire pour sa bonne réalisation est aussi riche et prometteur que le thème. En effet les contraintes globales que nous devons respecter sont les suivantes : identifier les différents services des hôpitaux publics de la ville de Bukavu, proposer un plan d'adressage, configurer le routeur Microtik, assurer la sécurité optimale des connexions et les logiciels utilisés doivent bénéficier d'une licence libre et gratuite.

a. ***L'intitulé :*** mise en place un réseau MAN en faisant un diagnostic des différents problèmes du réseau local existant dans les hôpitaux publics de Bukavu et proposer un nouveau réseau sécurisé répondant aux exigences de l'entreprise.
b. ***L'objet :*** réaliser la meilleure conception d'un réseau reliant les hôpitaux publics et qui répond aux exigences en matière de réseau d'entreprise.

c. ***Organismes d'accueil*** *:* les hôpitaux publics de Bukavu ; il s'agit de : l'hôpital général de référence de Bagira, l'hôpital provincial général de référence de Bukavu, l'hôpital de Ciriri et l'hôpital général de Kadutu.

d. ***Les utilisateurs et leurs attentes*** **:** Afin de définir précisément les fonctionnalités que devra offrir le réseau, une analyse des besoins a été menée lors des rencontres au cours desquelles les différents utilisateurs potentiels des différents hôpitaux ont eu l'occasion d'évoquer leurs attentes dans le cadre de leurs missions respectives. Les utilisateurs potentiels peuvent être classés en fonction de leur poste de travail ; leurs besoins étant directement liés à ce dernier.

1.3.2. Analyse de l'existant

Notre étude de l'existant consiste à mettre à plat, de façon aussi claire que possible, l'analyse qualitative et quantitative du système d'information actuel des différents hôpitaux de la ville de Bukavu. En effet, pour faire le déploiement des solutions d'interconnexion, il est essentiel de disposer des informations précises sur l'infrastructure réseau physique et les problèmes qui ont une incidence sur le fonctionnement du réseau. Il s'agira donc pour nous de rassembler les informations relatives à l'organisation de l'existant. Ici, nous allons faire l'inventaire de tous les outils informatiques, du réseau de Télécommunication et des services qui feront l'objet d'interconnexion des différents hôpitaux publics de la ville de Bukavu.

a. Matériels et logiciels utilisés

Le recensement des outils informatiques associés aux départements, et services informatiques des différents hôpitaux publics de la ville de Bukavu nous a donné les résultats qui suivent : (Nb : la majorité des PC dans ces hôpitaux fonctionnent sous Windows 8.1 et 10)

Hôpital	**Nbre Pcs**	**Marques**	**Types**	**HDD**	**RAM**
Hôpital général provincial de référence de Bukavu	O7	Dell et HP	Core17	1 terra	8Go
Hôpital général de référence de Bagira	03	Dell	Core15	500G0	4Go
Hôpital général de référence de Kadutu	04	Dell	Core15	500G0	4Go
Hôpital général de référence de CIRIRI	06	HP	Core17	1 terra	8Go

Tableau 2 PC utilisés

Source : Nos recherches sur terrain

Types de terminaux	Modèles	Nombres
Routeur Microtique	Huawei	02
Switches (48ports)	Alcatel	03
Point d'accès Wifi	D-Link	06
Prise Jack Rj45	D-Link	20

Tableau 3 Les équipements d'interconnexion de l'HPRB

b. Les applications utilisées

Les applications des hôpitaux publics de la ville de Bukavu sont diverses et installées sur les serveurs contenus en salle machine en mode client-serveur sur les autres machines. Il s'agit entre autres de : messageries, applications Web, le multimédia et l'IoD qui est une machine à rayon X et imagerie, moniteurs connectés, compteurs d'énergie, … Ceci pour améliorer les soins des patients les hôpitaux publics de la ville de bukavu dispose de deux applications (Microsoft Dynamics Navision et HikVision IP CAM) qui feront l'objet d'interconnexion depuis des hôpitaux publics de la ville de Bukavu à l'intérieur et en dehors.

c. Critique de l'existant et propositions des pistes de solution :

La critique de l'existant est un jugement objectif portant sur l'organisation actuelle de l'entreprise qui vient d'être présentée. De ce fait, le diagnostic de l'existant vise à faire une analyse sur les avantages et les inconvénients du système existant. L'étude de l'existant vise à permettre aux utilisateurs de : comprendre le fonctionnement du système actuel, dégager ses forces, dégager ses faiblesses et insuffisances, connaître les souhaits des utilisateurs, recenser les contraintes à considérer lors de la conception du futur système. Après une analyse du système, le diagnostic nous permettra de cerner le problème et de proposer des solutions.

Tableau 4 Forces et faiblesses du système existant de tous les hôpitaux publics de la ville de Bukavu

Forces	**Faiblesses**
- Posséder un fonctionnement simple - Facile à mettre en œuvre - Moins vulnérables car une des connexions peut être débranchée sans paralyser le reste du réseau - Ce logiciel est léger et ne consomme pas de ressource système - Réduire le gaspillage de temps - Moins couteux et meilleur rendement - Le temps d'accès est déterminé	- Si un nœud (une station), ne fonctionne plus, le réseau est en panne. - Si un câble est défectueux tous les ordinateurs connectés qui se trouvent en dessous sont paralysés - Un plan d'adressage réseau peu optimal - Il existe trop de nœud d'interconnexion, ce qui accroit la perte de connectivité. - Il n'existe pas de serveur d'antivirus, ni de serveur de messagerie (Exchange) pour assurer les échanges ;

Source : nos investigations

Lors de notre descente sur le terrain, la première tâche a été de rencontrer différentes personnes qui entretiennent directement ou indirectement une relation avec le service informatique des différents hôpitaux publics de la ville de Bukavu. Ces dernières ont toutes affirmé qu'il y a des différents problèmes communs au sein de ces hôpitaux comme par exemple : il n'y a pas de segmentation du réseau actuel, donc impossible d'isoler ou filtrer le trafic, le type de conception existant ne permet pas d'extensibilité (c.à.d. le réseau ne peut donc pas s'étendre sans que cela ait un impact sur les performances), une panne sur un matériel du réseau peut entrainer la non-disponibilité d'une partie du réseau. En plus, des domaines défaillants étendus c'est-à-dire que les défaillances de liaisons et de périphériques affectent de vastes zones du réseau et enfin, la sécurité déployée est trop faible, il y'a pas pare-feu dynamique donc il ne fait que le filtrage et n'empêche pas tout le trafic non autorisé ou indésirable. Il n'y a pas aussi de système IDS ou IPS implémenté sur le réseau dans les hôpitaux publics de la ville de Bukavu.

Comme solution à ces problèmes, le réseau que nous envisageons développer et mettre en place reproduira quelques fonctionnalités manquantes dans la solution existante, qui sera le noyau mais extensible d'un futur réseau riche avec des modules complémentaires plus conviviales permettant l'interconnexion des différents hôpitaux publics de la ville de Bukavu dans l'échange des données ; ceci en concevant un réseau viable et de qualité. Ainsi, le réseau doit

être disponible et fonctionnel en permanence, même en cas de rupture de liaison, de panne matérielle ou de surcharge. Il doit offrir un accès fiable aux applications et des temps de réponse raisonnables d'un hôte à l'autre. Il doit être sécurisé c'est-à-dire les données transmises sur le réseau doivent être protégées, de même que celles stockées sur les périphériques qui y sont connectés. Le réseau doit ainsi être aussi facile à modifier pour pouvoir s'adapter à la croissance et aux besoins de l'entreprise et les pannes occasionnelles étant inévitables, le dépannage du réseau doit être facile. Enfin, la détection et la résolution des problèmes ne doivent pas prendre trop de temps.

d. Types de fichiers partagés dans les hôpitaux publics de Bukavu

Les hôpitaux et les systèmes de santé profitent d'une explosion des technologies de l'information pour mieux gérer leurs installations, améliorer les soins aux patients et maîtriser les coûts. Cet afflux de données fait peser sur les équipes informatiques des hôpitaux une énorme responsabilité : gérer le pool croissant des informations de santé dans le respect des normes et en toute sécurité, de sorte qu'il soit toujours accessible et protégé.

Qu'il s'agisse de données patientes numériques, sous forme de dossier médical partagé (DMP) ou de dossier médical électronique (DME), d'examens et d'imagerie médicale, ou encore d'enregistrements de vidéosurveillance, les établissements de soins de santé ont besoin d'une solution fiable de stockage, de protection et d'accès aux données.

Les fichiers que peuvent se partager ces hôpitaux publics de la ville de Bukavu sont entre autres : les recherches cliniques et pharmaceutiques, les informations sur la sécurité sanitaire, les dossiers médicaux électroniques des patients transférés d'un hôpital public à un autre, etc. A noter que ces fichiers seront transférés soit sous format texte, image, audio, ...

En bref, toutes les informations peuvent être transférées en utilisant le mode de diffusion simplex

1.4. Conclusion

Le but de cet exercice de réflexion théorique à la fois délicat et intellectuellement passionnant sur l'articulation entre la présentation du cadre d'étude et la critique de l'existant était de fournir une indication suffisamment élaborée et claire des objectifs et enjeux sur le sujet, ses objectifs

et enjeux ainsi que sur la façon dont il serait conduit dans les hôpitaux publics de la ville Bukavu. Dans ce long processus de conception, nous avons tenu compte des objectifs et exigences, de la capacité du réseau déjà en place et aussi des nouvelles technologies que nous devrions intégrer. Tout ce travail nous a permis d'avoir une base sur laquelle nous pourrions nous appuyer pour proposer des solutions adaptées et qui répondent aux attentes des utilisateurs

Nous espérons, avoir fait ressortir ce lien dialectique au terme de cette partie. Nous nous attèlerons maintenant à faire ressortir les démonstrations empiriques auxquelles confronter la réflexion théorique qui a été faite. C'est ce à quoi la deuxième partie et notamment la troisième partie (à travers une étude de cas) vont s'attacher.

Chapitre 2 : REVUE DE LA LITTÉRATURE ET DESCRIPTION DE L'APPROCHE

La mise en place optimale d'un réseau MAN, exige une connaissance suffisante en matière d'architecture informatique et de liaison d'interconnexion, tant sur le plan général des infrastructures réseaux qu'au niveau spécifique des télécommunications. La présente partie de l'étude s'efforce d'apporter cette indispensable connaissance. Elle consiste en une réflexion purement théorique sur le sujet et expose la démarche méthodologique adoptée pour le traiter.

Ce chapitre se divise en trois sections. La première se consacre à la revue de la littérature ou l'état de question, la deuxième à la présentation des différents outils de travail qui seront utilisés dans l'étude et leurs rôles respectifs et la troisième section porte exclusivement sur la description et la justification de l'approche méthodologique choisie dans l'étude.

2.1. Etat de la question

La conception d'un réseau MAN interconnectant différentes institutions pour l'échange des fichiers a déjà fait l'objet de plusieurs travaux de recherche :

DENAGNON Franck (2018) dans son travail portant sur la mise en place d'un VPN (Site - to -Site) au sein d'une entreprise comme la société de routes et bâtiments. Ce projet lui a permis de mieux appréhender les problèmes liés aux réseaux locaux dont ceux relatifs au déploiement d'un réseau VPN comprenant plusieurs sites distants tout en garantissant une qualité de service. D'où, l'auteur est parvenu à aboutir à la mise en place d'une interconnexion entre cinq sites distants à travers un VPN afin de faciliter les échanges de données au sein de la société SOROUBAT et de ce fait de mieux gérer le système d'information de l'entreprise.

ANDRIANTSALAMA nomentsoa nampoina (2016) dans son mémoire de fin d'études intitulé : « conception et mise en place de réseau hiérarchique a haute disponibilité au sein du MFB ». Dans cette étude, l'auteur essaie de présenter et d'étudier les bonnes pratiques et les étapes à suivre pour réaliser la meilleure conception d'un réseau qui répond aux exigences en matière de réseau d'entreprise. Nous retrouvons dans son travail l'efficacité des protocoles de haute disponibilité : STP au niveau commutateur, HSRP et Etherchannel[1] au niveau routeur qui gèrent

[1] STP : Spanning Tree Ptotocol. C'est un protocole réseau de niveau 2 permettant de déterminer une topologie réseau sans boucle dans les LAN.

en plus les partages de charge et les redondances. Ils permettent une fiabilité du réseau en cas de panne (coupure de lien, défaillance d'un équipement) tout en offrant un débit supérieur au cœur du réseau.

Michaël G. L. fOLANE et Marius G-W BAMOGO (2006) dans leur travail portant sur l'étude et réalisation de l'interconnexion des sites de la SONAPOST situés à Ouagadougou par la technologie WiMAX. Dans leur travail, il apparaît clairement que la mise en place de ce nouveau système d'interconnexion des sites de la SONAPOST avec cette technologie WiMAX leur offrira la possibilité de disposer d'un réseau d'entreprise performant. Pour eux, il appartient maintenant à cette société de procéder à l'installation d'un VSAT (Very Small Aperture Terminal) pour un accès au réseau Internet. Cela leur permettra ainsi d'être totalement indépendant des opérateurs de télécommunications locaux et servira de même à l'interconnexion des sites au plan national.

Nassif Matta (2011) dans son projet portant sur la conception et installation d'un système de surveillance dans une menuiserie avec émission d'alarme à distance. Dans ce projet, il explique que la méthode utilisée repose sur le fait d'installer des capteurs à multi-paramètres (fumée, température, infrarouge, mouvement, bris de vitre …), et les relier à un module centralisé qui gère l'ensemble de ces détecteurs et déclenche, en fonction de la situation, une certaine signalisation d'alarme et ajiste convenablement à chaque événement détecté. La présence d'une ligne téléphonique permet au système d'appeler le responsable sur son téléphone et lui informer de la situation grâce à des messages vocaux numériques préconfigurés. Ainsi, conçu pour une utilisation commerciale, son système permet de gérer jusqu'à 104 entrées analogiques, et 32 cartes d'accès utilisant le protocole RS485. Le système scrute donc les entrées analogiques, et les cartes d'accès et active une sirène en cas d'alarme général puis compose les numéros de téléphones des responsables pour les informer. L'alarme peut être silencieux c.à.d. sans activation de la sirène. Enfin, la réalisation matérielle et logicielle de ces maquettes suivie d'une phase de validation et de tests avait donné des résultats satisfaisants.

De ce qui précède, nous constatons qu'aucune étude à notre connaissance n'aborde directement la question de la conception d'un réseau MAN interconnectant différents hôpitaux publics de la

Le HSRP ou Hot Standby Router Protocol est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de Niveau 3permettant une continuité de service.
EtherChannel est une technologie d'agrégation de liens utilisée principalement sur les commutateurs de Cisco

ville de Bukavu pour l'échange des fichiers ni dans la période récente avec toutes les dimensions censées caractériser cette interconnexion. De ce fait, contrairement aux études ci-haut citées, dans cette étude, il s'agit de concevoir un réseau sécurisé MAN interconnectant différents hôpitaux publics de la ville de Bukavu à partir du protocole SFTP[2] pour l'échange des fichiers.

2.2. Outils de travail (matériels et logiciels)

Cette section présente les différents outils de travail qui seront utilisés dans l'étude et donne avec précision leurs rôles respectifs. Pour modéliser un système d'information, différents métiers (utilisateurs, experts, organisateurs, informaticiens, ...) interviennent ensemble dans un processus de développement, constitué de différentes activités exercées dans un environnement organisationnel et basé sur différents outils et techniques [1]. Ces outils et techniques aident à la mise en œuvre des modèles, langages, … [28].

Sachant que L'interconnexion des réseaux est la possibilité de faire dialoguer plusieurs sous réseaux initialement isolés, par l'intermédiaire de périphériques spécifiques (récepteur, concentrateur, pont, routeur, modem), dans ce cas, des équipements spécifiques sont donc nécessaires. De ce fait, dans présent travail, des outils de sécurités SFTP nous a semblé le plus adopté afin de permettre à deux ordinateurs distants des hôpitaux publics de la ville de Bukavu de communiquer et d'échanger des fichiers médicaux comme s'ils faisaient partie d'un même réseau local.

Le SSH file transfer protocol (abrégé en SFTP) assure le transfert de données en toute sécurité entre deux personnes souhaitant communiquer. C'est une étape bien souvent incontournable dans de nombreux processus de travail en entreprise : par exemple, les collaborateurs d'un service externe qui envoient leurs résultats à la centrale, l'architecture du serveur du réseau d'une entreprise qui est maintenue à jour et sécurisée à distance, ou encore un réparateur qui envoie ses instructions en ligne sur place. Pour y parvenir, les données doivent être transférées dans les deux sens sur le serveur de l'entreprise par le biais d'une connexion Internet.

Il faut noter que plus la norme de sécurité est faible, plus le risque d'attaques (vol ou manipulation de données) ou d'injection de logiciels malveillants dans le système de l'utilisateur est élevé. Avec le FTP, la sécurité est très faible : le nom d'utilisateur et le mot de

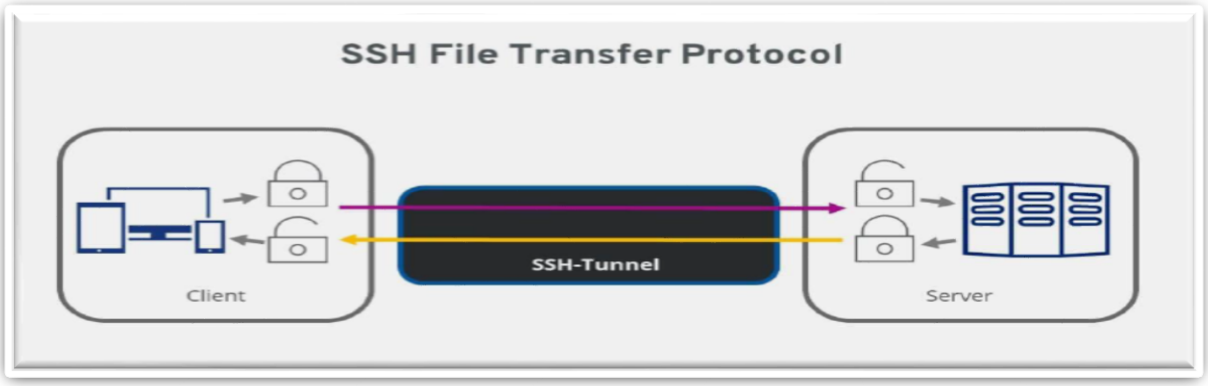
[2] Protocole SFTP ou *Secure File Transfert Protocol* est comme son nom l'indique, un protocole de transfert de fichier sécurisé

passe sont transmis en texte clair, sans chiffrage. Les hackers peuvent donc lire les identifiants et accéder sans autorisation au client et au serveur FTP, avec les conséquences qui en découlent. C'est pourquoi, Le SFTP a été développé pour offrir une alternative clairement améliorée sur le plan de la sécurité et se protéger d'éventuelles attaques.

Il garantit une authentification sûre des personnes souhaitant communiquer entre elles. Dès qu'un client tente de se connecter, le serveur vérifie son identité à l'aide du SSH. L'identification s'appuie sur des certificats et sur le système de clés publique et privée. L'accès est autorisé uniquement si la clé du client SFTP est compatible avec la « serrure » du serveur SFTP, et si le serveur vérifie que le client a « verrouillé » les données avec une clé adaptée. Cette clé se compose d'une suite de lettres, de chiffres et de caractères spéciaux générée au hasard et respectant un nombre de bits fixe. Il s'agit d'un protocole cryptographique, qui permet de communiquer des messages chiffrés même via une connexion Internet non sécurisée.

L'accès SSH sur le serveur de l'hôte est obligatoire pour une connexion réussie avec le protocole SSH file transfer protocol. C'est là que sont mises à disposition les données d'accès pour l'utilisateur SFTP : adresse du serveur, nom d'utilisateur et mot de passe. Ces données sont saisies dans le programme (S) FTP utilisé par le client. Lors de la première connexion, le logiciel FTP affiche la clé de vérification et l'enregistre pour une utilisation ultérieure. Ainsi, le client s'authentifie à chaque connexion au serveur. Lorsqu'une page ou un hacker « s'authentifie » sur ce canal sans clé ou avec une mauvaise clé, la connexion est immédiatement interrompue. Ainsi, un transfert de données SFTP se présente de la manière suivante :

Figure 11 Schéma représentatif d'un transfert de données SFTP



Source : [5]

Avec le chiffrage bidirectionnel, le SSH file transfer protocol fait transiter les données dans un tunnel SSH. Entre le client et le serveur, ainsi que dans le sens inverse, il existe ce que l'on

appelle un tunnel SSH, dans lequel s'opèrent l'authentification et le transfert des données. Ce tunnel est chiffré de bout en bout, afin qu'aucun hacker ne puisse mettre la main sur les données, quelles qu'elles soient. Ainsi, le destinataire reçoit des données intactes. Si un pirate essaie toutefois de manipuler les données du transfert, SSH identifie cette opération et interrompt immédiatement la connexion [59].

Le transfert de données avec SSH file transfer protocol protège des risques suivants :

- Modification de l'adresse IP d'un lot de données, aussi connue sous le nom d'usurpation d'adresse IP
- Redirection du nom de l'ordinateur d'origine vers l'adresse IP d'un hacker (DNS spoofing)
- Interception des données en clair par un hacker
- Manipulation des données transférées par un hacker

En bref, SSH file transfer protocol : Ce protocole (abrégé en SFTP, en français *protocole de transfert de données sécurisé*) garantit le transfert de données chiffré entre un client et un serveur (et inversement) en une seule connexion. Les données de connexion tout comme les données transférées sont chiffrées à l'aide de clés basées sur le protocole SSH.

2.3. Description et justification de l'approche

Pour mener cette étude, nous avons recouru à quelques méthodes dont la méthode expérimentale et la méthode ascendance ; nous avons aussi recouru aux enquêtes à partir de la technique d'observation et la technique documentaire.

2.3.1. Techniques

Dans ce présent travail, nous avons fait recours à trois techniques pour réaliser la démarche appliquée. La technique d'observation ainsi que la technique documentaire.

2.3.1.a. La technique d'observation

La technique d'observation est utilisée pour expliquer un phénomène via les descriptifs de comportements, des situations réelles et des faits constantes. [51]

Dans ce présent travail, la technique d'observation nous a permis de décrire les problèmes qui continuent à gangrener dans la gestion centralisée des données et informations ainsi que dans l'interaction entre les hôpitaux publics de Bukavu.

2. La technique documentaire

La technique documentaire est l'ensemble des étapes permettant de chercher, identifier et trouver des documents relatifs à un sujet par l'élaboration d'une stratégie de recherche. [32]. Cette technique nous a amené et permis dans le cadre de réalisation de ce travail à passer en revue des différents documents (ouvrages, publications, autres travaux scientifiques, …) abordant l'objet de notre étude.

2.4. Conclusion

Cette partie de nos recherches, est une partie charnière qui a eu pour effet de mieux appréhender la teneur de notre projet tout en cernant mieux les contours. De ce fait, dans cette partie, nous avons présenté notre méthodologie en justifiant nos choix. La phase de justification de l'approche a consisté surtout à présenter le scénario pour la mise en place d'un réseau MAN interconnectant différents hôpitaux publics de la ville de Bukavu dont : l'hôpital général de référence de Bagira, l'hôpital provincial général de référence de Bukavu, l'hôpital de Ciriri.et l'hôpital général de Kadutu. Elle nous a permis également de faire un choix des modèles en fonction du contexte dans lequel on se trouve. Ainsi, nous avons présenté l'état de l'art de la technologie WiMAX, nous avons défini les différents aspects des couches Physique (PHY) et MAC du standard 802.16. Un point très important sur la conception du réseau est aussi la sécurité sur le réseau. Dans le prochain chapitre, nous allons appliquer ces études en présentant la structure du modèle qu'on a développé pour interconnecter les hôpitaux publics de la ville de Bukavu pour l'échange des fichiers.

Chapitre 3 : APPLICATION DE LA MÉTHODOLOGIE ET PRÉSENTATION DES RÉSULTATS AVEC ANALYSE

Après le choix de notre modèle et sa modélisation, la mise en œuvre du système d'interconnexion est indispensable car elle va permettre au groupe des utilisateurs d'avoir une idée concrète du système futur. Nous aborderons dans cette partie une présentation succincte des participants, la structure de l'équipe de travail, la stratégie de collecte des données, la présentation des résultats et de quelques prototypes de la structure d'interconnexion. Ensuite, nous décrirons les exigences pour la mise en œuvre des solutions proposées et l'estimation du coût pour la mise en œuvre des solutions proposées pour assurer de l'interconnexion de différents hôpitaux publics de la ville de Bukavu.

3.1. Structure de l'équipe de travail (les Moyens humains).

Dans ce travail, il a été défini un programme d'exécution des tâches en vue de la réalisation du plan. Celui-ci met en synergie plusieurs moyens humains qui seront défini dans cette section. Nous définissons de ce fait 3 équipes de travail pour l'exécution dudit projet : le groupe de pilotage qui est dans notre cas l'encadreur de ce travail, le groupe de projet le maître d'œuvre qui est l'étudiant rédacteur et le groupe des utilisateurs qui sont les différents hôpitaux bénéficiaires du projet.

Ainsi, le maître d'œuvre est l'auteur du projet ; il assure la direction des travaux et en est l'architecte. Une fois son projet validé par le maître d'ouvrage qui auprès de lui tient un rôle de patron, le maître d'œuvre est responsable du bon déroulement des travaux et joue un rôle de conseil dans le choix des différents hôpitaux qui vont les réaliser. Il est de ce fait responsable du suivi des délais et des budgets selon les modalités définies dans le cahier des clauses administratives particulières.

Dans notre cas, dans les hôpitaux publics de la ville de Bukavu, le département informatique de chaque hôpital tient ce rôle pour ce qui est du projet réel de conception d'un réseau les interconnectant entre eux. Le maître d'ouvrage, qui se comporte dans ce cas comme le commanditaire du projet reviendra aux responsables de chaque hôpital. C'est pourquoi, en principe, une fois le projet réalisé et livré, il est important de déléguer d'ordinaire la responsabilité du suivi du système mis en place à un personnel spécial de Département Informatique de chaque hôpital.

3.2. Moyens matériels

Les équipements définis dans le tableau ci-après ont été choisi selon les principes de :

- ✓ Performances, haute sécurité et fiabilité haut de gamme ;
- ✓ Configuration rapide et facile ;
- ✓ Prise en charge d'un éventail extrêmement large d'applications sur une même plateforme

Tableau 5 les équipements à installer

Equipements	**Quantité**
Antenne Nano station	5
Point d'accès Wifi	9
Machine ordinateur	121
Prise Ethernet	100
Machine Serveur	1
Câble Ethernet	
Alimentation POE	5
Routeur Cisco	5
Switch CISCO Small Business SG 350X	10
Onduleur UPS 2000 VA (Pour armoire informatique	08

Ces équipements sont à installer dans chaque site (voir Annexes). Et donc chaque site comprend un certain nombre d'équipement selon le besoin. Il faut noter aussi que, ces équipements doivent être fournis par les quatre hôpitaux et installés par leurs services.

3.3. Nombre de sites à installer

Nous aurons à installer cinq (5) sites selon les coordonnées suivantes :

Tableau 6 Coordonnées Géographiques des sites à installer

Sites	Longitudes	Latitudes	Altitudes	Distances Km
RENATELSAT	28,8410621	-2,5009489	1760,4519166	
HPGR de Bukavu	28,8496462	-2,4948274	1487,8393669	1,136
HGR de Kadutu	28,8489113	-2,5202182	1638,022205	2,313
HGR de Bagira	28,8297435	-2,4705086	1618,3291679	3,536
HGR de CIRIRI	28,8355551	-2,5234231	1931,8608725	2,596

Source : nos réalisations dans Google Earth

3.4. Stratégie de collecte des données

Aujourd'hui, pour analyser et collecter ses données, il faut d'abord bien poser les problèmes à résoudre, déterminer les modèles à construire ou à utiliser, et identifier les programmes informatiques capables de vous permettre de résoudre ces problèmes, ces programmes étant bien évidemment fonction d'un type donné d'ordinateur [53]. La collecte des données est un processus qui permet d'obtenir l'information nécessaire pour chaque unité sélectionnée de l'étude [18]. C'est pourquoi, quel que soit le type d'évaluation menée ou de projet, il est essentiel de bien choisir les méthodes de collecte et d'analyse des données et de les appliquer correctement [48].

Dans ce travail, nous avons recouru aux enquêtes qui se sont effectuée par l'observation et la technique documentaire dans le but de couvrir chacune des hypothèses que nous avions à tester, afin de décrire les problèmes d'interconnexion des différents hôpitaux de la ville de Bukavu et de se saisir de certaines informations et documents qui nous ont servis comme pièces de référence. En plus, la technique documentaire nous a permis dans le cadre de réalisation de ce travail à passer en revue des différents documents (ouvrages, publications, autres travaux scientifiques, …) abordant l'objet de notre étude. Enfin, pour bien mener à port ce travail, ***WiMAX*** configuré d'un protocole SFTP pour l'échange des fichiers nous a semblé le produit le plus performant se présentant comme l'évolution du Wi-Fi avec une capacité bien supérieure et pouvant opérer sur des fréquences réglementées ou non.

3.5. Présentation des résultats

Cette section a pour objet d'exposer l'œuvre réalisée. C'est pourquoi, après avoir fait le choix de notre maquette et fait sa modélisation, la mise en œuvre du système d'interconnexion par l'implémentation est indispensable car elle va permettre au groupe des utilisateurs et celui de pilotage d'avoir une idée concrète du système futur. L'installation, la configuration des serveurs et des équipements d'interconnexion (routeurs et switch) se feront de façon identique sur les cinq sites distants. Les quatre hôpitaux publics de la ville de Bukavu ayant besoin d'une connexion MAN entre eux, nous allons créer une liaison avec l'antenne RENATELSAT.

Etape 1 : **Liaison des sites et configuration MAN**

D'abord, nous allons configurer les liens entre le commutateur multicouche de la couche distribution et le commutateur de celle de l'accès. On utilise l'agrégation de lien avec le protocole SFTP avec la technologie Ethernet ainsi que la simulation du réseau MAN sur les routeurs et commutateurs CISCO.

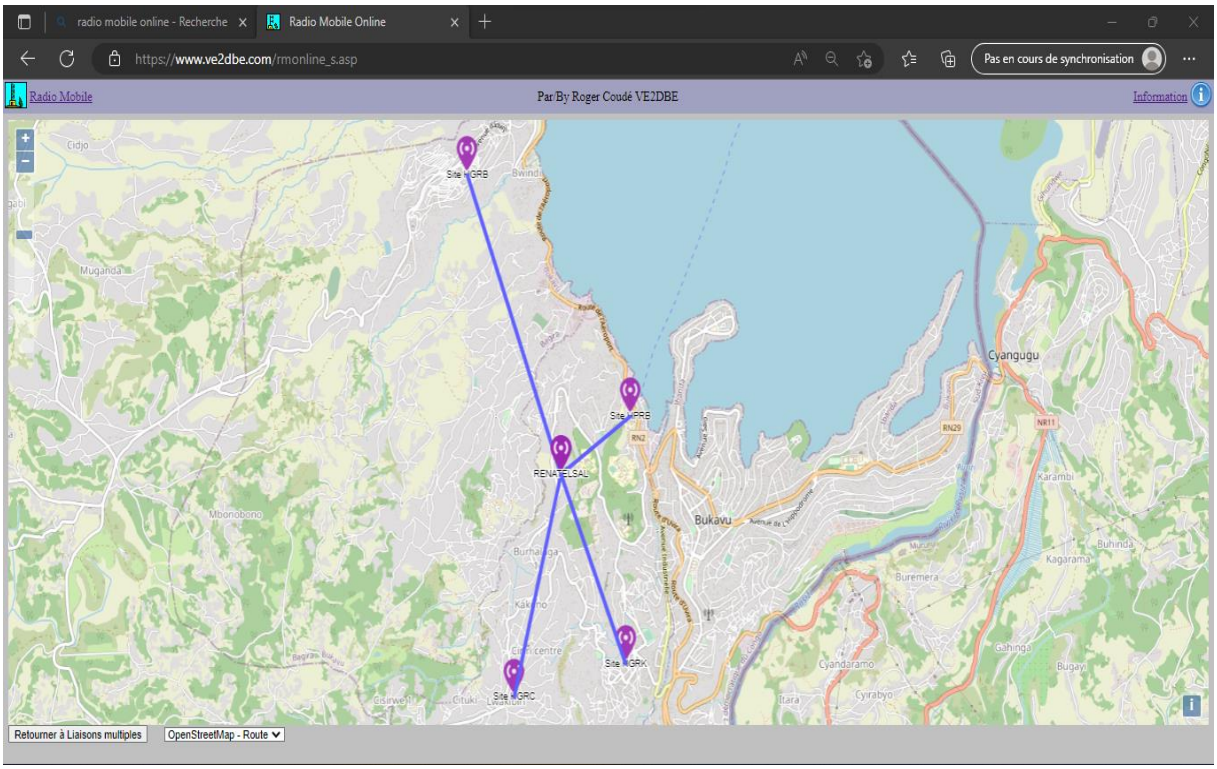


Figure 12 Vue satellitaire de différentes liaisons

De cette figure, nous observons la liaison de tous les sites à partir de l'antenne RENA. De ce fait, l'architecture de l'interconnexion des bâtiments de réseau MAN se présente comme suit :

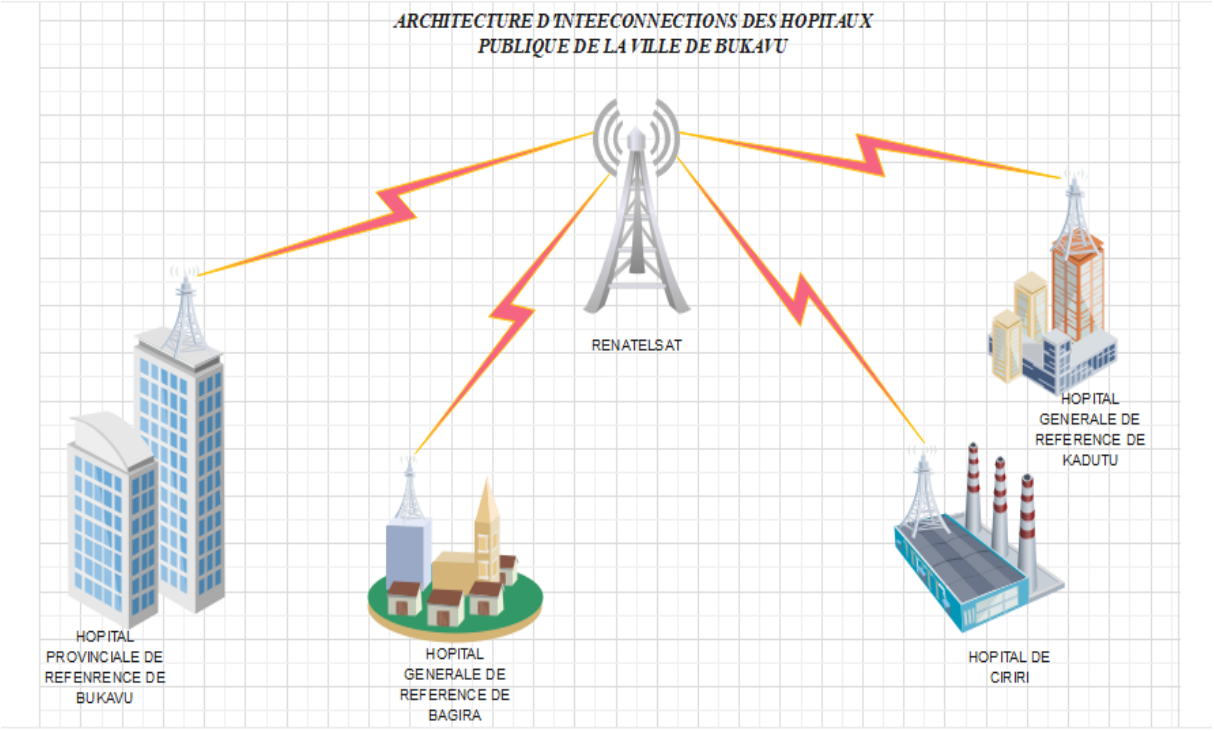


Figure 13 Architecture d'interconnexion des hôpitaux publics de la ville de Bukavu

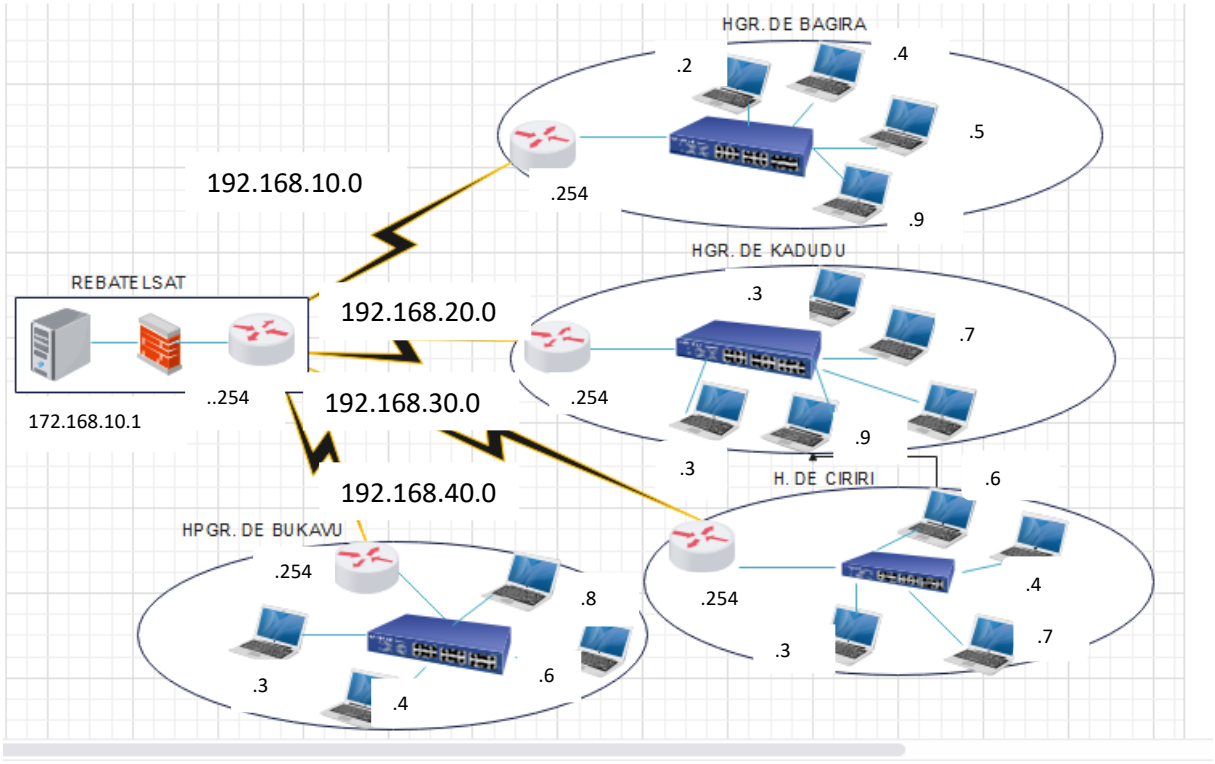


Figure 14 Proposition de l'architecture du réseau MAN

La figure ci haut représente l'architecture des différents hôpitaux publics de la ville de Bukavu interconnectés grâce à un réseau MAN. Nos sites n'étant pas interconnectés entre eux, nous avons eu du mal à présenter l'ancien architecture.

C'est cette architecture proposée qui nous a poussé à simuler dans Cisco. Cette étape permet de relier les ordinateurs et les périphériques de ces hôpitaux publics entre eux. Ainsi, l'architecture globale de réseau se présente comme suit :

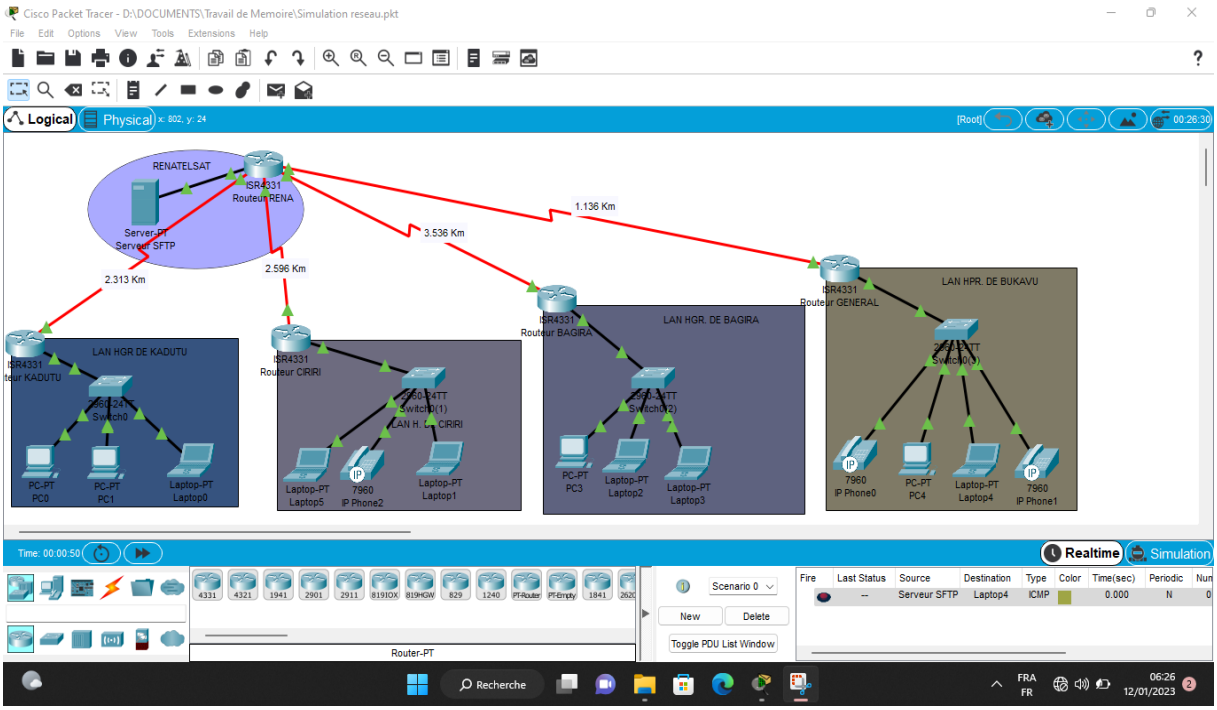


Figure 15 Architecture Globale du Réseau

De cette figure, nous constatons la simulation du réseau MAN dans CISCO. Il configure le lien entre les différents hôpitaux de la ville de Bukavu. Ceci permet de relier les ordinateurs et les périphériques situés à proximité de ces hôpitaux entre eux. Cette étape nous a permis d'évaluer le protocole, l'architecture réseau et de prévoir leur fonctionnement. Il faut quand-même noter que, la réalisation de ce réseau informatique est extrêmement simple car il y a peu d'hôtes sur le réseau.

Etape 2 : **Configuration des équipements et services**

Comme dit précédemment, l'installation, la configuration des serveurs et des équipements d'interconnexion (routeurs et switch) se feront de façon identique sur les cinq sites distants.

Dans notre exemple, nous allons effectuer une configuration de base qui nous permettra de communiquer sur le réseau local entre PC de différents hôpitaux puis d'accéder à internet.
Les étapes de configuration seront les suivantes :

1. **Configuration du réseau MAN dans le routeur RENATELSAT**

```
routeur-rena>!--- Configuration du reseau MAN
routeur-rena>en
Password:
routeur-rena#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
routeur-rena(config)#int s0/1/0
routeur-rena(config-if)#ip address 10.10.10.1 255.192.0.0
routeur-rena(config-if)#no shut
routeur-rena(config-if)#exit
routeur-rena(config)#int s0/2/0
routeur-rena(config-if)#ip address 10.10.74.1 255.192.0.0
% 10.0.0.0 overlaps with Serial0/1/0
routeur-rena(config-if)#ip address 10.74.10.1 255.192.0.0
routeur-rena(config-if)#no shut
routeur-rena(config-if)#exit
routeur-rena(config)#int s0/1/1
%Invalid interface type and number
routeur-rena(config)#int sl/1/1
%Invalid interface type and number
routeur-rena(config)#int s0/1/0
routeur-rena(config-if)#ip address 10.138.10.1 255.192.0.0
routeur-rena(config-if)#no shut
routeur-rena(config-if)#exit
routeur-rena(config)#int s0/2/1
routeur-rena(config-if)#ip address 10.202.10.1 255.192.0.0
routeur-rena(config-if)#no shut
routeur-rena(config-if)#
routeur-rena(config-if)#end
routeur-rena#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
routeur-rena#
%SYS-5-CONFIG_I: Configured from console by console

routeur-rena#
```

2. **Configuration du nom et du mot de passe pour le routeur RENA**

```
Router>!--- Configuration du roureur renatelsat
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname routeur-rena
routeur-rena(config)#!--- Ajouter un mot de passe pour entrer dans le mode privilege
routeur-rena(config)#enable secrete 1234
                                    ^
% Invalid input detected at '^' marker.

routeur-rena(config)#enable secret 1234
routeur-rena(config)#!--- Activation du service encryption-password pour cacher le mot de passe
routeur-rena(config)#service password-encryption
routeur-rena(config)#exit
routeur-rena#
%SYS-5-CONFIG_I: Configured from console by console

routeur-rena#exit
```

La connexion au routeur s'effectue par le **port console** en utilisant les **lignes virtuelles**. Ces ports virtuels sont utilisés pour les connexions telnet ou ssh. Si un mot de passe n'est pas configuré les accès distants ne sont pas autorisés. Par défaut, les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Nous allons donc tout d'abord activer le service encryption-password, les mots de passe apparaitront alors chiffrés lorsque les commandes d'affichage de la configuration sont entrées.

3. Configuration du réseau local de BAGIRA

```
ROUTEUR-BAGIRA>!--- Configuration du Routeur de Bagira
ROUTEUR-BAGIRA>en
Password:
ROUTEUR-BAGIRA#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ROUTEUR-BAGIRA(config)#inf s0/1/0
                       ^
% Invalid input detected at '^' marker.

ROUTEUR-BAGIRA(config)#int s0/1/0
ROUTEUR-BAGIRA(config-if)#ip address 10.202.10.2 255.192.0.0
ROUTEUR-BAGIRA(config-if)#int g0/0/0
ROUTEUR-BAGIRA(config-if)#ip address 192.168.30.254 255.255.255.0
ROUTEUR-BAGIRA(config-if)#exit
ROUTEUR-BAGIRA(config)#!--- Configuration du routage pour l'acces au serveur SFTP
ROUTEUR-BAGIRA(config)#ip route 172.168.0.0 255.255.0.0 10.202.10.1
ROUTEUR-BAGIRA(config)#
ROUTEUR-BAGIRA(config)#end
ROUTEUR-BAGIRA#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ROUTEUR-BAGIRA#
%SYS-5-CONFIG_I: Configured from console by console

ROUTEUR-BAGIRA#
```

4. Configuration du réseau local de CIRIRI

```
ROUTEUR-CIRIRI>!--- Configuration du routeur de CIRIRI
ROUTEUR-CIRIRI>en
Password:
ROUTEUR-CIRIRI#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ROUTEUR-CIRIRI(config)#int s0/1/0
ROUTEUR-CIRIRI(config-if)#ip address 10.74.10.2 255.192.0.0
ROUTEUR-CIRIRI(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed state to up

ROUTEUR-CIRIRI(config-if)#no shut
ROUTEUR-CIRIRI(config-if)#exit
ROUTEUR-CIRIRI(config)#int g0/0/0
ROUTEUR-CIRIRI(config-if)#ip address 192.168.20.254 255.255.255.0
ROUTEUR-CIRIRI(config-if)#no shut
ROUTEUR-CIRIRI(config-if)#exit
ROUTEUR-CIRIRI(config)#!--- configuration du routage pour l'acces au serveur SFTP
ROUTEUR-CIRIRI(config)#ip route 172.168.0.0 255.255.0.0 10.74.10.1
ROUTEUR-CIRIRI(config)#
ROUTEUR-CIRIRI(config)#end
ROUTEUR-CIRIRI#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ROUTEUR-CIRIRI#
%SYS-5-CONFIG_I: Configured from console by console
```

5. Configuration du réseau local de KADUTU

```
ROUTEUR-KADUTU>en
Password:
ROUTEUR-KADUTU#!--- Configuration du routeur de Kadutu
ROUTEUR-KADUTU#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ROUTEUR-KADUTU(config)#int s0/1/0
ROUTEUR-KADUTU(config-if)#ip address 10.10.10.2
% Incomplete command.
ROUTEUR-KADUTU(config-if)#ip address 10.10.10.2 255.192.0.0
ROUTEUR-KADUTU(config-if)#no shut
ROUTEUR-KADUTU(config-if)#int g0/0/0
ROUTEUR-KADUTU(config-if)#ip address 192.168.10.254 255.255.255.0
ROUTEUR-KADUTU(config-if)#no shut
ROUTEUR-KADUTU(config-if)#exit
ROUTEUR-KADUTU(config)#!--- Configuration du routage pour L'acce au SERVEUR SFTP
ROUTEUR-KADUTU(config)#ip route 172.168.10.0 255.255.0.0 10.10.10.1
%Inconsistent address and mask
ROUTEUR-KADUTU(config)#ip route 172.168.0.0 255.255.0.0 10.10.10.1
ROUTEUR-KADUTU(config)#
ROUTEUR-KADUTU(config)#end
ROUTEUR-KADUTU#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ROUTEUR-KADUTU#
%SYS-5-CONFIG_I: Configured from console by console

ROUTEUR-KADUTU#
```

6. Configuration du réseau local de Général

```
ROUTEUR-GENERAL>en
Password:
ROUTEUR-GENERAL#!--- Configuration du routeur de L'hopital general
ROUTEUR-GENERAL#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ROUTEUR-GENERAL(config)#int s0/1/0
ROUTEUR-GENERAL(config-if)#ip address 10.138.10.2 255.192.0.0
ROUTEUR-GENERAL(config-if)#no shut
ROUTEUR-GENERAL(config-if)#exit
ROUTEUR-GENERAL(config)#int g0/0/0
ROUTEUR-GENERAL(config-if)#ip address 192.168.40.254 255.255.255.0
ROUTEUR-GENERAL(config-if)#no shut
ROUTEUR-GENERAL(config-if)#exit
ROUTEUR-GENERAL(config)#!--- Configuration du routage pour l'acces au seurveur SFTP
ROUTEUR-GENERAL(config)#ip route 172.168.0.0 255.255.0.0 10.138.10.1
ROUTEUR-GENERAL(config)#
ROUTEUR-GENERAL(config)#end
ROUTEUR-GENERAL#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
ROUTEUR-GENERAL#
%SYS-5-CONFIG_I: Configured from console by console

ROUTEUR-GENERAL#
```

Chaque site étant une image d'un petit réseau disposant d'un accès à internet, la configuration se fera en deux étapes dont : la configuration du réseau local du serveur et la configuration du routage au serveur.

7. Configuration du switch générale

```
%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up


Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname swicth-generale
swicth-generale(config)#enable secrete 1234
                       ^
% Invalid input detected at '^' marker.

swicth-generale(config)#enable secret 1234
swicth-generale(config)#service password-encryption
swicth-generale(config)#vlan 10
swicth-generale(config-vlan)#name VLAN-MAN-GEN
swicth-generale(config-vlan)#exit
swicth-generale(config)#int vlan 10
swicth-generale(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

swicth-generale(config-if)#ip address 192.168.40.1 255.255.255.0
swicth-generale(config-if)#no shut
swicth-generale(config-if)#exit
swicth-generale(config)#int range f0/1-12
swicth-generale(config-if-range)#switchport mode acces
swicth-generale(config-if-range)#switchport acces vlan 10
swicth-generale(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

swicth-generale(config-if-range)#no shut
swicth-generale(config-if-range)#exit
swicth-generale(config)#end
swicth-generale#
%SYS-5-CONFIG_I: Configured from console by console

swicth-generale#
```

Nous créons et configurons les VLAN10 avec respectivement l'adresse du site de l'hôpital général 192.168.40.1 et un masque de 255.255.255.0. Tout en signalant qu'il est absolument

inutile de configurer et d'attribuer une IP à chaque VLAN créer sur un switch, sauf dans le cas d'un switch niveau 3. Cependant, cela permet dans une certaine mesure de tester le routage inter-vlan sans avoir besoin de connecter de machine sur le switch. Une fois que les VLANs sont créés, il convient de leur attribuer un ou plusieurs ports à partir de certaines commandes.

8. Configuration du réseau local du serveur

```
routeur-rena>en
Password:
routeur-rena#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
routeur-rena(config)#!--- configuration du reseau lacal du serveur
routeur-rena(config)#int gig0/0/0
routeur-rena(config-if)#ip adress 172.168.10.254 255.255.0.0
                           ^
% Invalid input detected at '^' marker.

routeur-rena(config-if)#ip address 172.168.10.254 255.255.0.0
routeur-rena(config-if)#no shut

routeur-rena(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up

routeur-rena(config-if)#exit
```

9. Configuration du routage au serveur

```
routeur-rena>en
Password:
routeur-rena#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
routeur-rena(config)#!--- Configuration du routage pourque le serveur accede au different reseau local
routeur-rena(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.2
routeur-rena(config)#ip route 192.168.20.0 255.255.255.0 10.74.10.2
routeur-rena(config)#ip route 192.168.30.0 255.255.255.0 10.202.10.2
routeur-rena(config)#ip route 192.168.40.0 255.255.255.0 10.138.10.2
routeur-rena(config)#
routeur-rena(config)#end
routeur-rena#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
routeur-rena#
%SYS-5-CONFIG_I: Configured from console by console

routeur-rena#
```

Nous faisons la configuration du routage pour que les réseaux puissent communiquer. Avant de commencer à configurer, il faut toujours s'assurer que les deux routeurs peuvent se joindre.

Etape 3 : Mise en place de serveur SFTP

Contrairement à FTP, les ordinateurs Windows ne disposent pas d'un client standard (Batch, n.d). Les différents hôpitaux doivent donc pour cela installer du **software supplémentaire**. Il fait signaler qu'il existe des clients software SFTP gratuits et payants. Les systèmes Linux proposent des packages standard d'une implémentation open source de SSH (OpenSSH). Tout

le trafic entre un client et un serveur est entièrement chiffré, depuis le processus d'identification jusqu'à l'envoi de fichiers. Étant donné cette protection, SFTP convient très bien à l'échange **sécurisé** de fichiers entre les diffèrent hôpitaux publics de la ville de Bukavu.

Ainsi, l'activation du serveur SFTP s'est faite à partir des étapes suivantes :

1. **Installation du serveur SFTP**

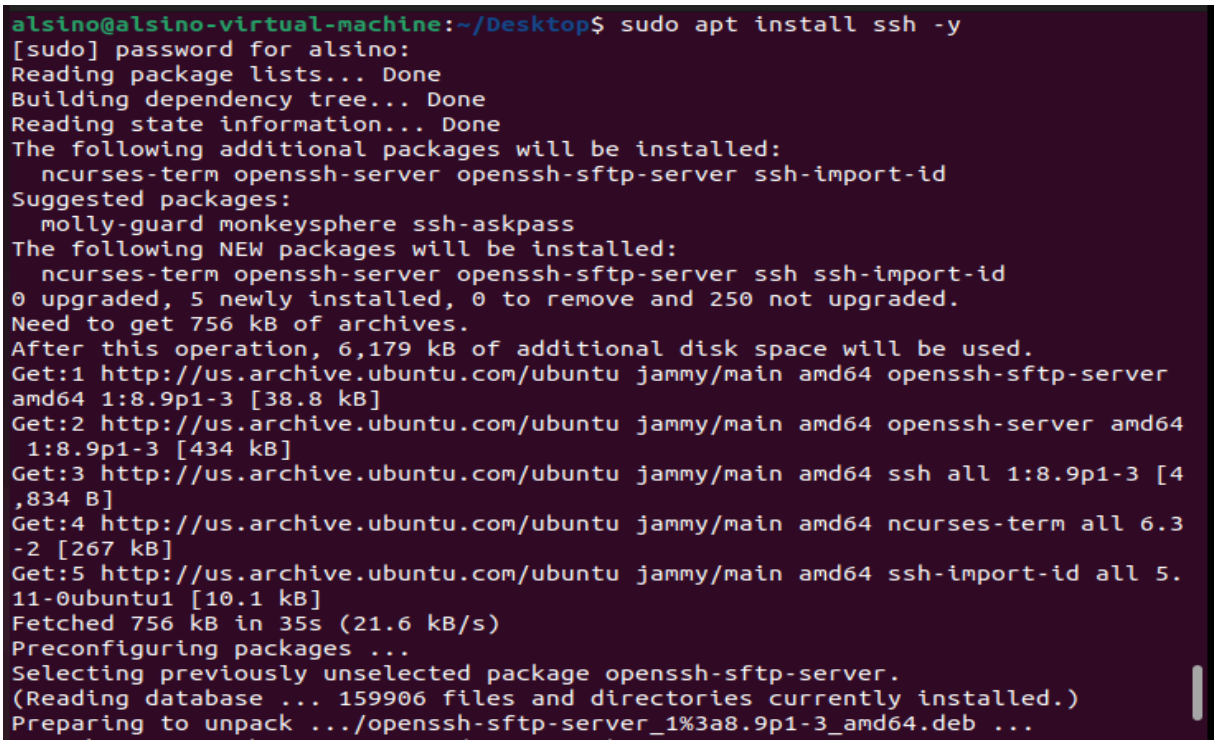


Figure 16 Installation du serveur SFTP

2. **Activation du serveur SFTP**

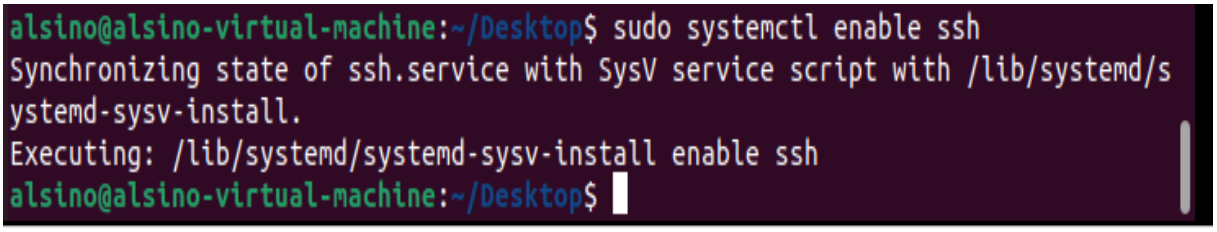


Figure 17 Activation du serveur SFTP

Tout comme le client, chaque serveur SFTP dispose également d'une paire de clés. Lors de l'établissement d'une connexion avec un serveur, celui-ci transmettra sa clé publique (également appelée host key) au client. C'est alors à l'utilisateur final qu'il appartient d'accepter

cette clé. À partir de ce point, la connexion sécurisée peut être établie et l'utilisateur peut s'identifier. L'authentification sur le serveur SFTP se fait via le nom d'utilisateur et la clé publique.

3. Lancement et vérification des statuts

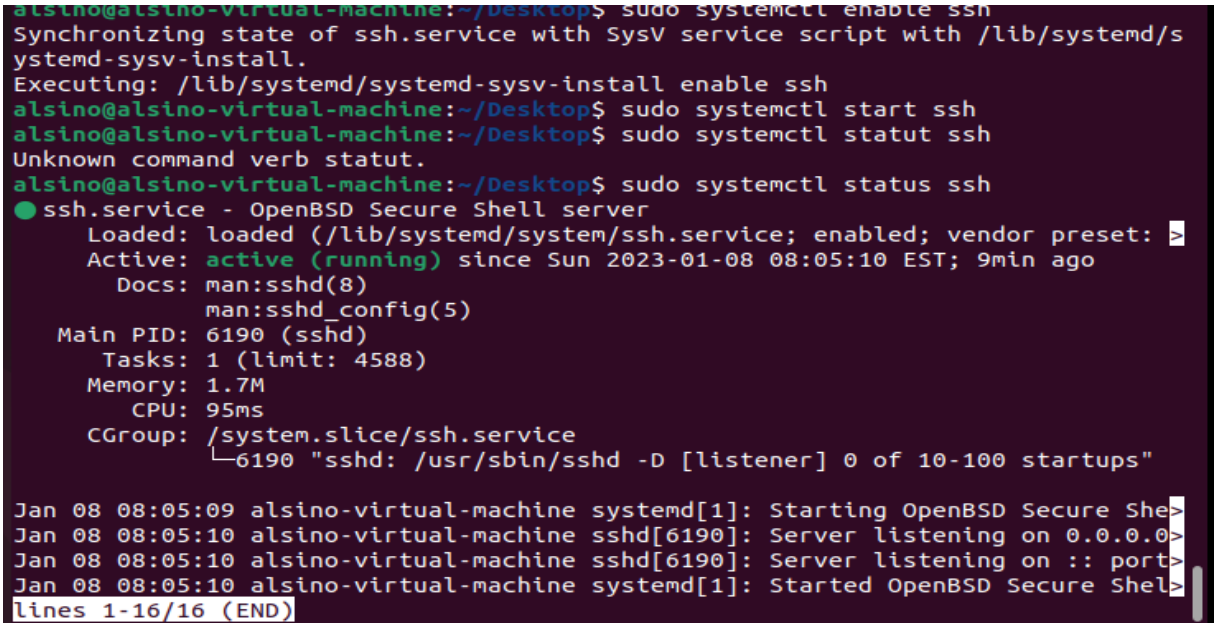


Figure 18 Lancement et vérification des statuts

4. Création des groupes d'utilisateurs

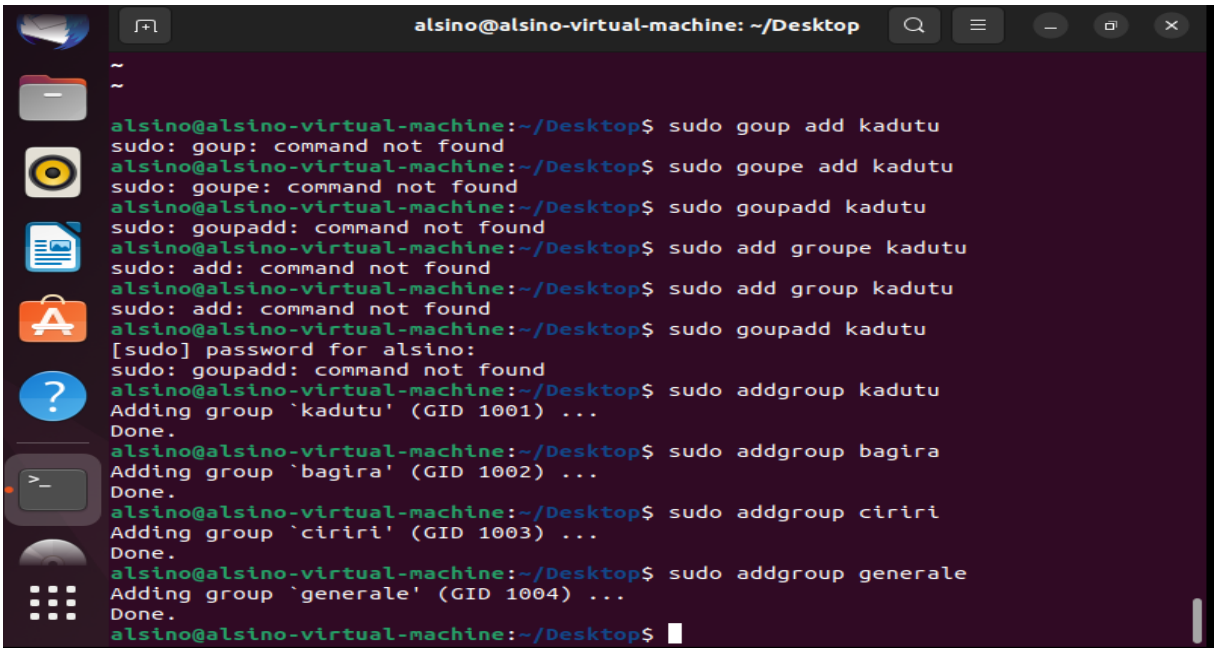


Figure 19 Création des groupes d'utilisateurs

Il existe plusieurs conditions pour s'identifier comme utilisateur via SFTP. Bien entendu, on dispose toujours d'un nom d'utilisateur. À côté de cela, une paire de clés électroniques remplace le mot de passe au sens classique du terme. Cette paire de clés comporte une clé privée et une clé publique. La clé privée reste chez celui qui l'a créée et sera de préférence encore protégée par un mot de passe additionnel. La clé publique peut être envoyée à toute partie adverse qui souhaite identifier le détenteur de la clé privée.

5. Création d'un utilisateur et l'affecté à son groupe

Figure 20 Création d'un utilisateur et l'affecté à son groupe

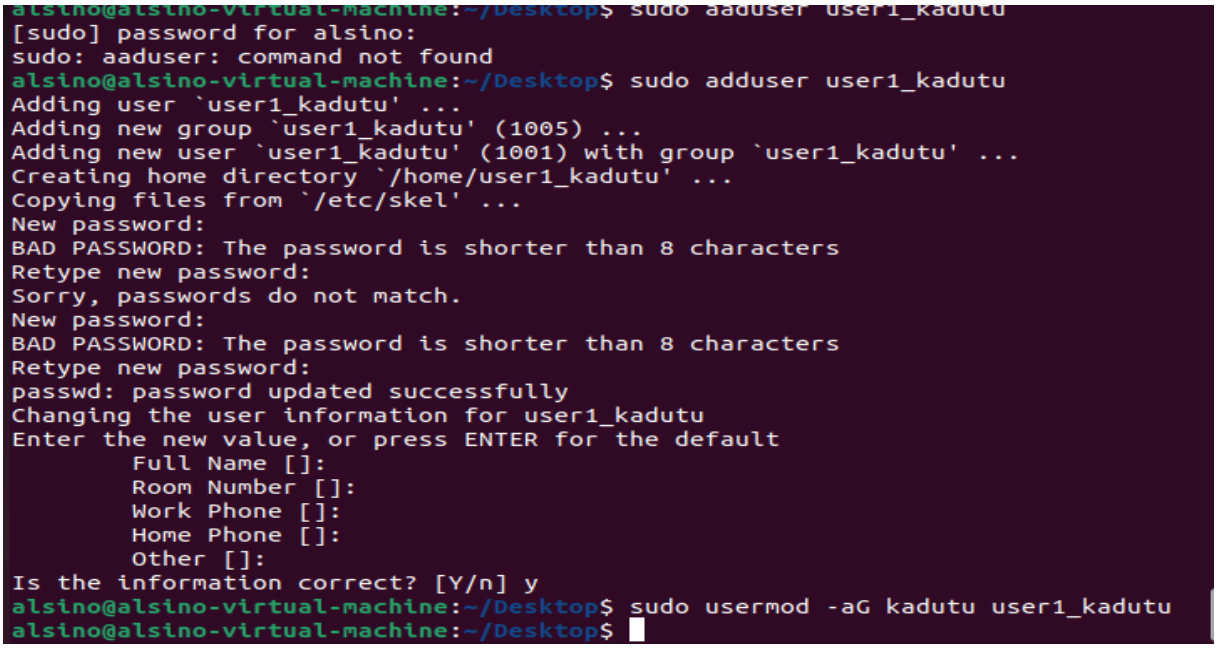


Figure 21 Création d'un utilisateur et l'affecté à son groupe

Maintenant que SFTP est configuré, il faut l'associer à un utilisateur. Généralement, lorsqu'on créer un nouvel utilisateur, on lui attribue le shell "bash". Ici on lui a attribué le shell "rssh". N'oubliez pas de lui créer un mot de passe à huit caractères

6. Création des répertoires pour le partage des fichiers

Le SFTP permet d'effectuer certaines opérations telle que : du côté du client, on peut : Supprimer et créer des fichiers, envoyer et recevoir des fichiers et déplacer et renommer des fichiers. Du côté du serveur, on peut : Gérer l'espace alloué à chaque client, administrer les accès de chaque utilisateur sur chaque fichier ou dossier, ajouter, supprimer, modifier les paramètres de chaque groupe ou utilisateur.

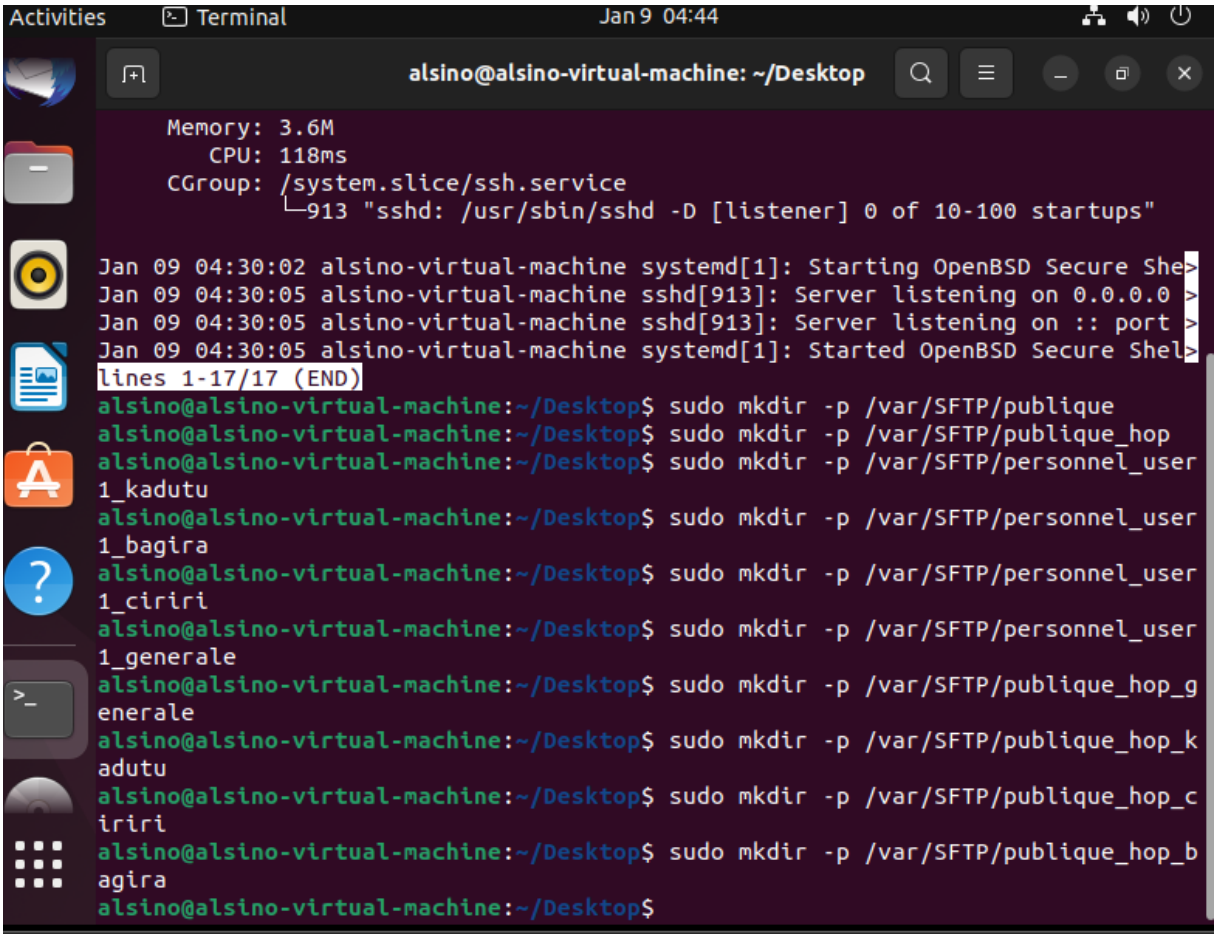


Figure 22 Création des répertoires pour le partage des fichiers

7. Définition des autorisations sur les fichiers

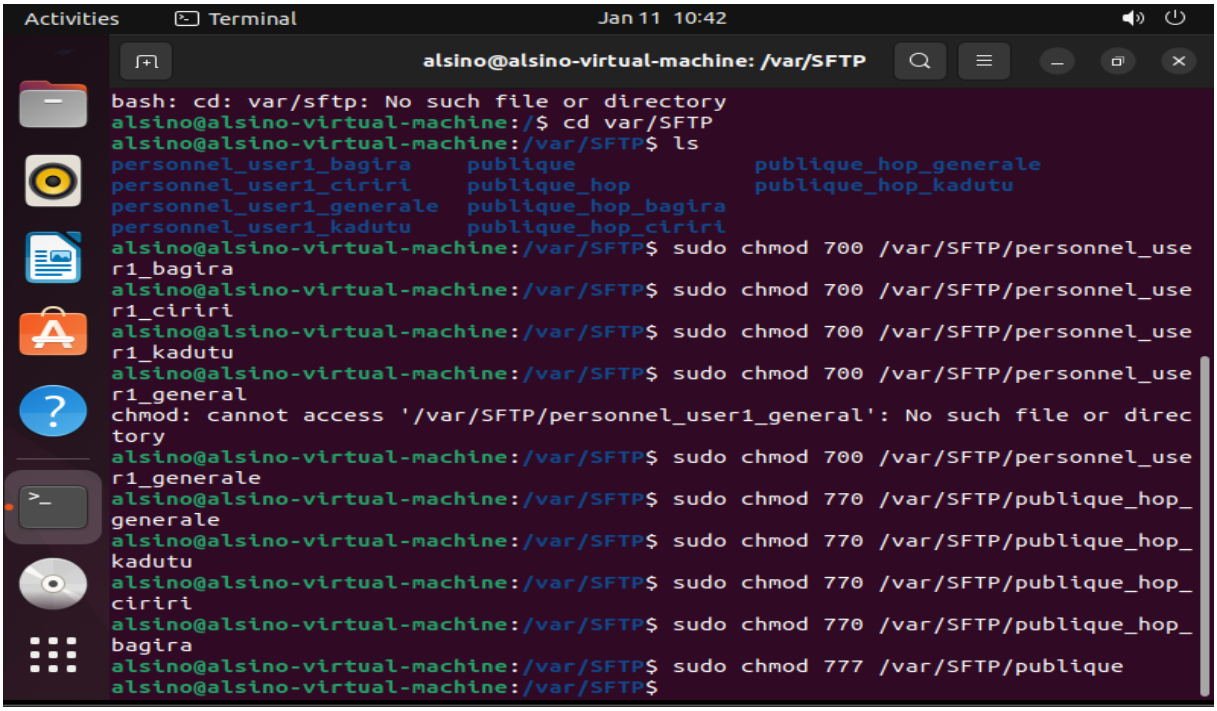


Figure 23 Définition des autorisations sur les fichiers

8. Attribution des fichiers à leurs propriétaires respectifs

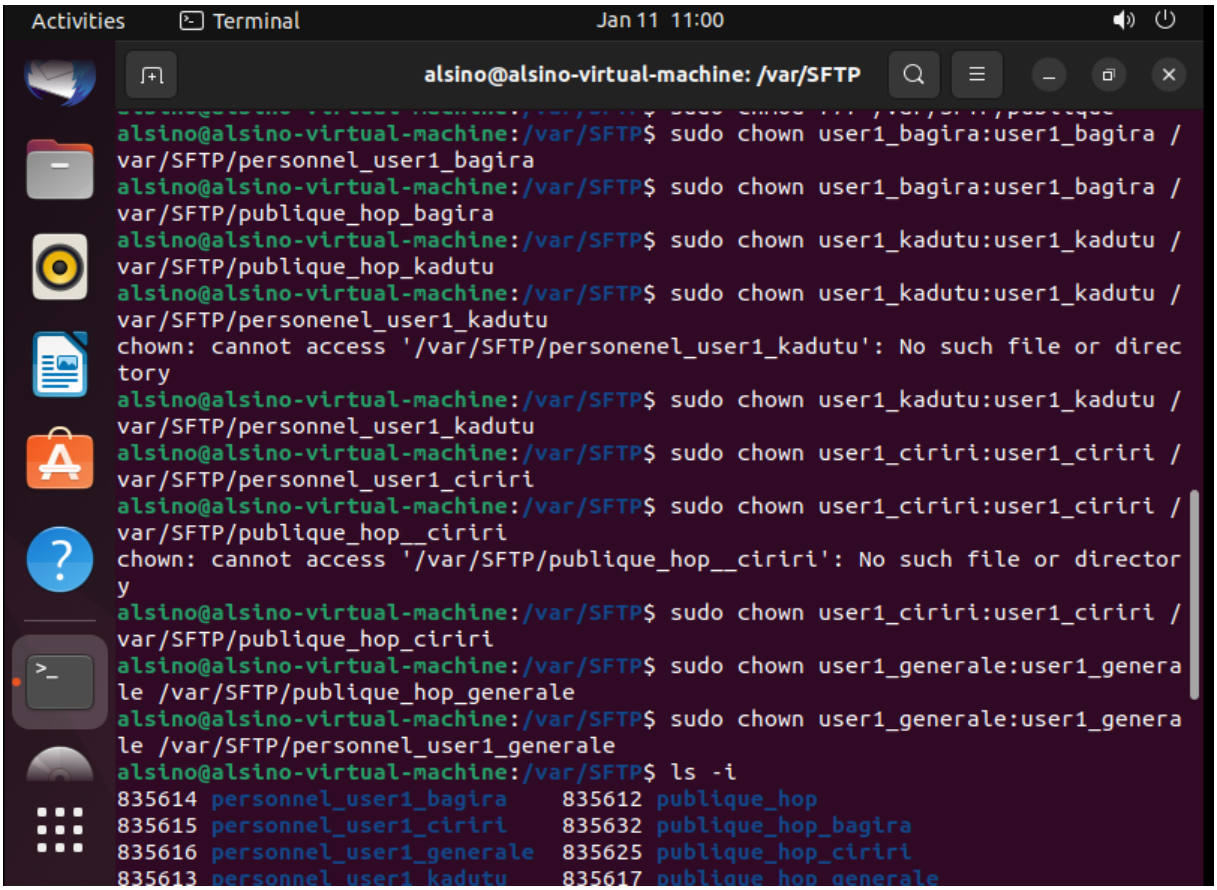


Figure 24 Attribution des fichiers à leurs propriétaires respectifs

9. Configuration du démon ssh

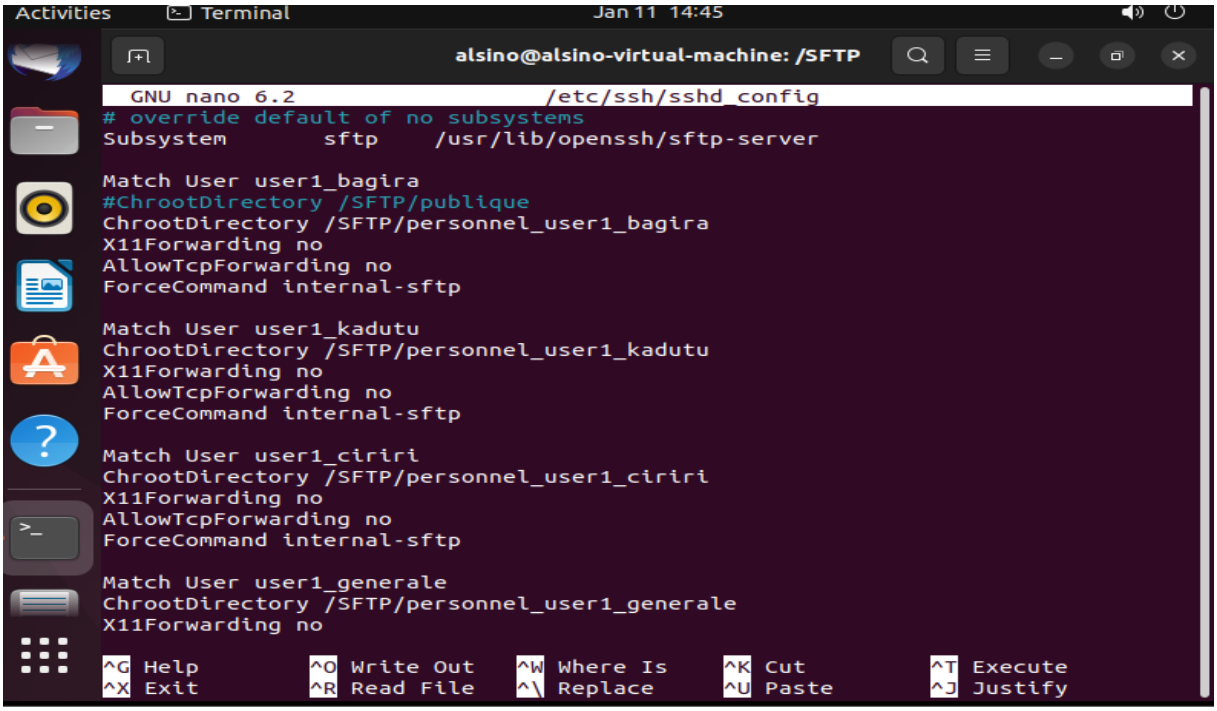


Figure 25 Configuration du démon ssh

10. Connexion d'un utilisateur au serveur via le terminal

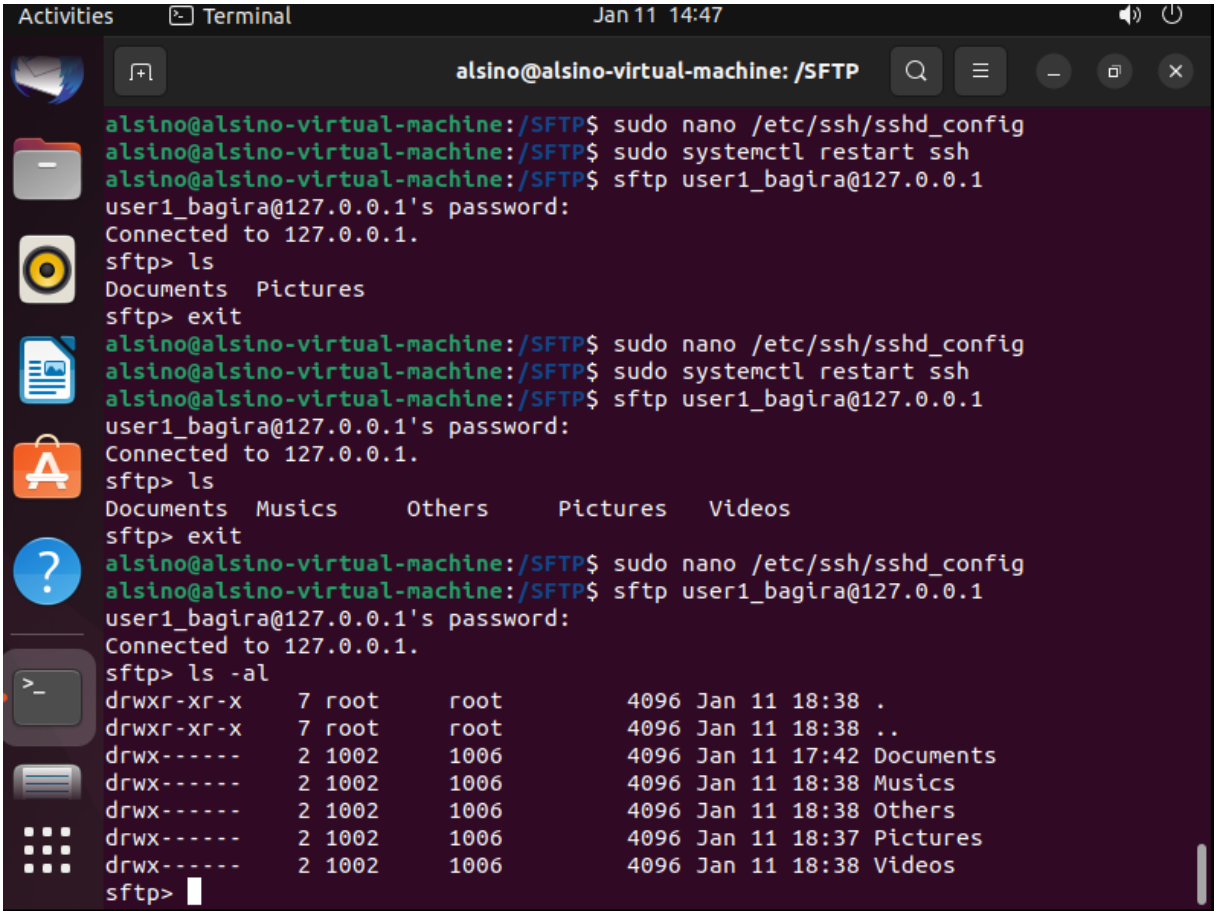


Figure 26 Connexion d'un utilisateur au serveur via le terminal

11. Installation et configuration du pare feu UFW

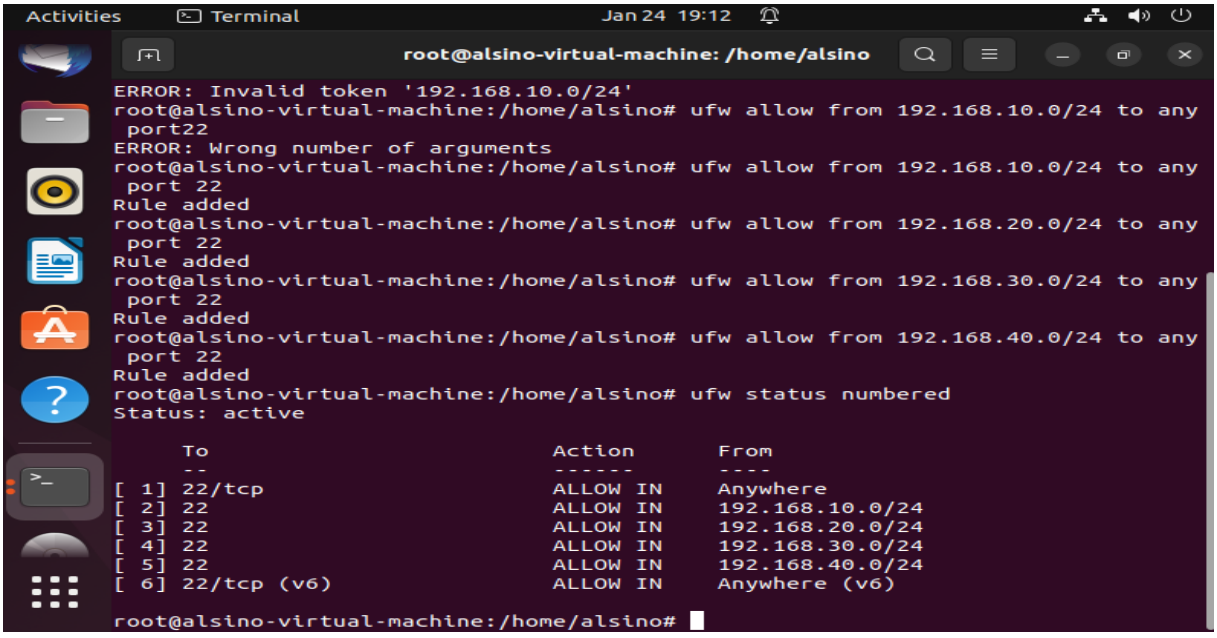


Figure 27 Installation et configuration du pare feu UFW

L'installation et la configuration du pare feu nous a permis d'avoir différents composants matériels et logiciels qui contrôlent le trafic intérieur/extérieur selon notre politique de sécurité.

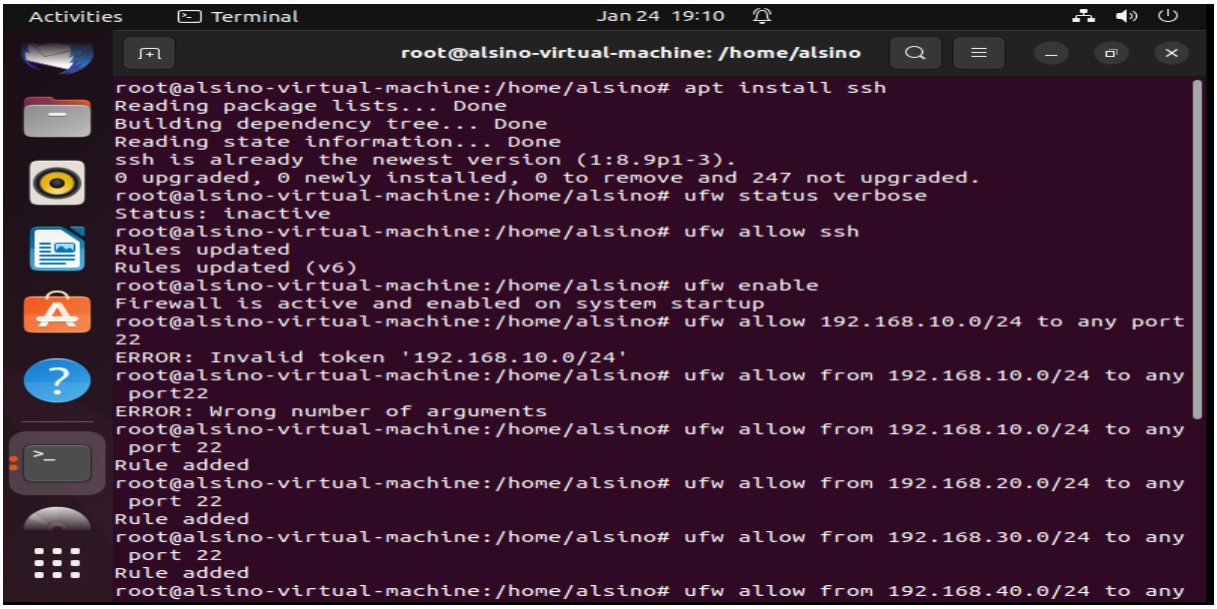


Figure 28 Installation et configuration du pare feu UFW 2

Ceci nous permettra, d'être un guichet de sécurité qui est un point central de contrôle de sécurité plutôt que de multiples contrôles dans différents logiciels clients ou serveurs. D'appliquer une politique de contrôle d'accès. D'enregistrer le trafic en construisant des journaux de sécurité. Et d'appliquer une défense en profondeur

Etape 4 : Connexion au Serveur SFTP

Maintenant que les comptes sont créés, il faut essayer de se loger avec le client sftp. La ligne de commande étant peu maniable, il nous a été pratique d'utiliser des clients SFTP graphiques.

1. **Connexion au serveur sftp via l'interface graphique**

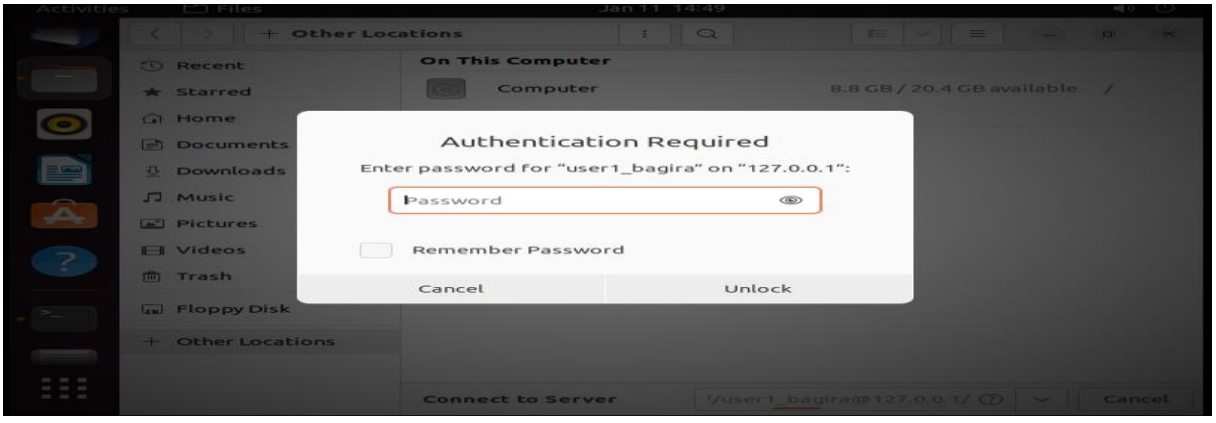


Figure 29 Connexion au serveur sftp via l'interface graphique

Ici, il est demandé au client d'insérer son mot de passe avant de se connecter au serveur

Une fois le mot de passe vérifié, l'interface graphique suivant s'affiche :

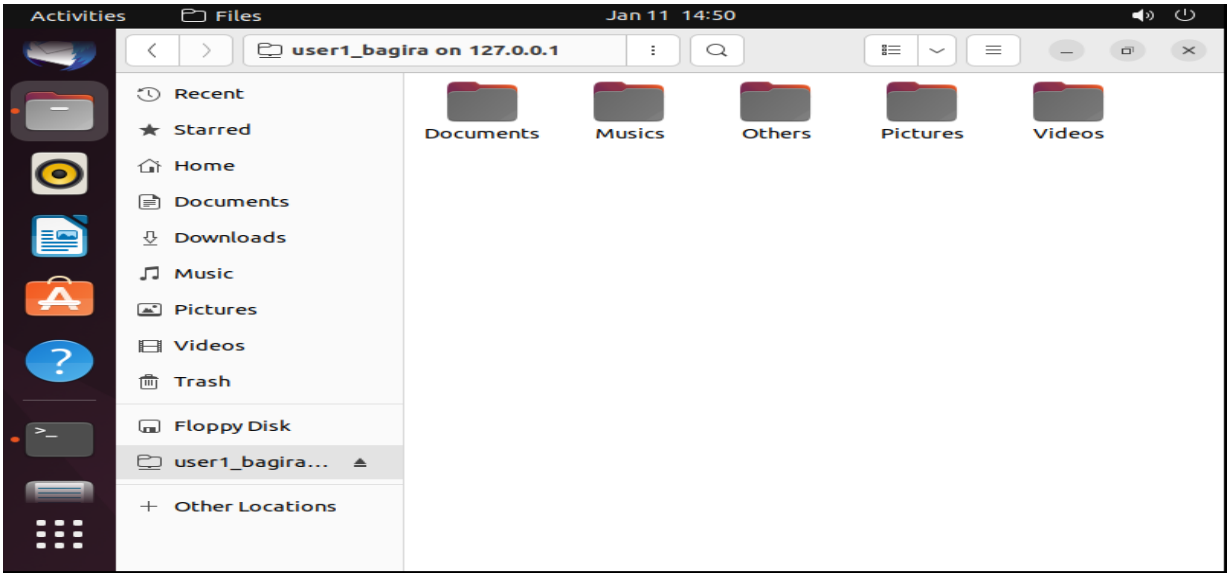


Figure 30 Connexion au serveur sftp via l'interface graphique 2

2. Connexion au server sftp via l'application fileZila

L'image suivante montre comment configurer Filezilla à utiliser SFTP :

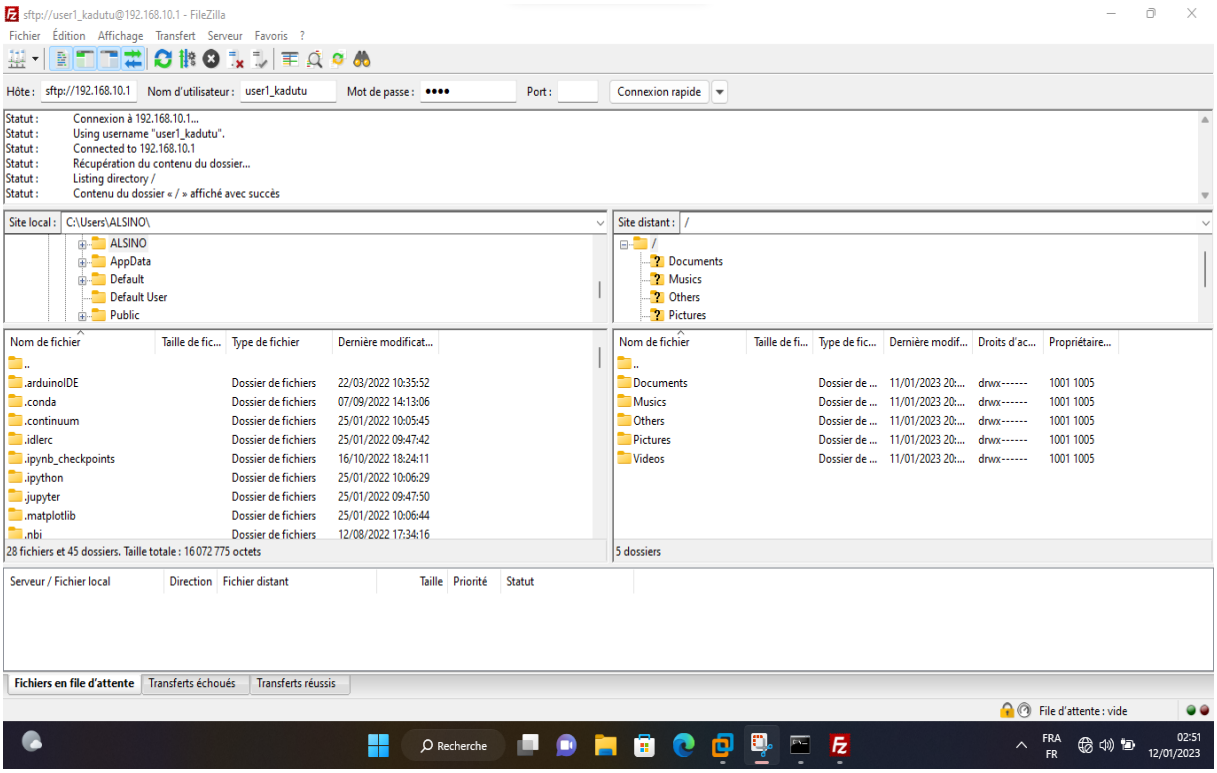


Figure 31 Connexion au server sftp via l'application fileZila

Une fois FileZile installée aux différentes machines des hôpitaux publics de la ville de Bukavu, une boîte de dialogue apparaît, ce qui va vous permettre de vous connecter au serveur sftp. Les

informations concernant le serveur SFTP sur lequel on veut se connecter sont les suivantes : Adresse du Serveur qui correspond à l'adresse IP du serveur SFTP sur lequel on veut se connecter. Bien entendu cela peut aussi correspondre à un nom de domaine dont on administre le serveur ftp à distance, le Port d'administration du serveur ftp, le Mot de passe et toujours se connecter à ce serveur. L'option de se connecter rapidement au serveur permet de stipuler si on effectue toujours la connexion sur ce serveur. A choisir si vous n'avez pas plusieurs serveurs ftp à administrer. On clique sur le bouton OK pour effectuer la connexion à l'interface d'administration du serveur SFTP. De cette image, nous constatons que si vous administrez un serveur ftp sur un réseau local, vous devez spécifier le mot dépasse qui protège la partie administration du serveur.

3.6. **Estimation du coût pour la mise en œuvre des solutions proposées**

Ici, il est question de moyens financiers concernant le coût de réalisation de ce projet en utilisant la méthode ascendante en tant que méthode d'estimation des couts des projet. Le choix des équipements à installer se fera en tenant compte des enjeux économiques, des bouleversements que l'interconnexion peut imposer dans les habitudes des utilisateurs et de l'expérience du groupe de projet. Le présent tableau apporte un résumé des dépenses à effectuer en termes de matériels, cette facture fera foi de bilan financier :

Tableau 7 Estimation financière du projet

Coût des matériels et logiciels						
Ordre	**Désignation**	**Quantité**	**Caractéristiques**	**Prix Unitaire ($)**	**Prix Total ($)**	**Justification**
1	Antenne WiMax omnidirectionnel	1	- Nano Station - Gain 13dbi - Fréquences utilisées : 4-5GHz - Distance : 10Km - Bande passante : 75Mbs	340,1 [5]	340,1	Nous avons choisi d'utiliser une antenne WiMax omnidirectionnel pour qu'il soit en liaison avec tous les autres antennes
2	Antenne WiMax	4	- Nano Station - Gain 7dbi - Fréquences utilisées : 4-5GHz - Distance : 10Km - Bande passante : 75Mbs	205.01 [5]	820.04	
3	Point d'accès Wifi	9	- Nano Station - Gain 7dbi - Fréquences utilisées : 2.4GHz - Bande passante : 300Mbs	19.45 [5]	175.09	
4	Machine serveur système	1	- DELL - Processeur : Intel 3.5 GHz - Mémoire RAM : 16GB - Disque dur : 2TB - Système d'exploitation : Ubuntu	250 [5]	250	Il nous servira de Serveur SFTP

5	Machine ordinateur	120	- DELL - Processeur : Intel 2.5 GHz - Mémoire RAM : 8GB - Disque dur : 500GB - Système d'exploitation : Windows 10	250 [5]	30000	
6	Prise Ethernet	100	- Murale - Dimension : 86x86mm	7.5 [5]	750	
7	Câble Ethernet	4	- Cat6 UTP - longueur 500m	75 [5]	300	
8	Routeur Microtik	5	- Fonction Modem : oui - nombre de port : 5 - Type de port : GigaEhernet	64 [5]	320	
9	Switch 24 ports	10	- Sisco - nombre des Port : 24 POE - mode de transmission : Full duplex et half diplexe	64 [5]	640	
10	Alimentation POE	5		20 [5]	100	Permettra d'alimenter les différentes antenne
11	Connecteur RJ45	20		10 [5]	200	
Sous total 1					**33720.23**	

1	Frais de transports	500	
2	Main d'œuvre	2500	Estimation de la main d'œuvre
Sous total 2		3000	**Sous total 2**
Total du Projet		**33720.23**	**Total du Projet**
Ordre/désignation		**Couts en dollars ($)**	**Ordre/désignation**

Source : nos calculs

De ce tableau ci-haut, les estimations du coût liées à la mise en œuvre des équipements de ce projet d'interconnexion des hôpitaux publics de la ville de Bukavu s'élèvent à **33 720,23$.** Mais, pour assurer une utilisation facile de l'application l'équipe du projet propose une formation pour les utilisateurs. Le coût proposé par l'équipe sera détaillé dans le tableau ci-dessous

Tableau 8 coût de la formation par Hôpital

Nombre d'utilisateurs	Nombre d'heures	Prix unitaire de l'heure	Coût total
5	10	5	500

Source : nos calculs

3.7. Discussion des résultats

Dans cette section, nous allons parler brièvement de différentes contributions théoriques et pratiques de cette étude.

3.7.1. Contributions théoriques et pratique

Bien que nos résultats concordent avec ceux de certains auteurs ([1] Adidou, 2017; [9] Cipière, 2016; [22] Franck, 2018; [21] Folane & Bamogo, 2006; [34] Kenza, 2018), nous constatons qu'aucune étude à notre connaissance n'aborde directement la question de conception d'un réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu pour l'échange des fichiers. De ce fait, contrairement aux études des auteurs ci-haut cités, dans cette étude, nous avons conçu un réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu à partir du protocole SFTP facilitant ainsi l'échange des fichiers entre eux.

De l'étude qui précède, il apparaît clairement que la mise en place de ce réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu sera d'un grand apport pour ces hôpitaux dans l'échange des informations. Dans ce travail, à l'aide des différentes phases et activités préconisées par WiMax et après analyse des différents protocoles, nous avons retenu une architecture d'interconnexion entre les différents hôpitaux. En somme cette étude nous a permis de mettre en pratique et d'approfondir les connaissances reçues au cours de nos cinq années de marathon académiques. Cette expérience s'est bien déroulée, et a été pour nous une véritable opportunité d'apprendre, de découvrir et d'être plus efficace entant qu'ingénieur informaticien en devenir.

3.7.2. Limites de l'étude et pistes de recherche futures

Cette étude se limite à concevoir un réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu facilitant ainsi l'échange des fichiers entre eux en toute sécurité. Notre réseau est conçu pour le partage des informations de santé entre différents acteurs de santé et permettre ainsi aux hôpitaux publics de la ville Bukavu de réaliser des tâches dont la prise en charge des patients ou des victimes de traumatisme, l'amélioration des soins, les recherches cliniques, avec une bonne précision et cela avec une grande vitesse et facilite ses agents dans ses différentes tâches. En appréciant les résultats de ce travail, les besoins auxquels cette

interconnexion répond ainsi que les objectifs sur lesquels nous nous sommes fixés, notre travail a abouti à une amélioration du système d'information mis en place par les hôpitaux publics de la ville de Bukavu et résoudre ainsi les difficultés dans la gestion centralisée de ses données et informations ainsi que dans les échanges des fichiers sur les recherches cliniques, les innovations médicales et pharmaceutiques, la sécurité sanitaire, la qualité des soins, …

Enfin, étant donné que nul ne peut se prétendre aborder un domaine dans son ensemble, nous souhaiterons venir : améliorer les interfaces graphiques, établir un système de sécurité des bases de données, mettre en place un VPN au sein des hôpitaux et une architecture de sécurité des services Intranet / Internet ou même d'un réseau hiérarchique à haute disponibilité au sein des hôpitaux publics de la ville de Bukavu. Ainsi, en toute humilité, nous restons très attentifs à toutes questions, suggestions et remarques constructives. C'est pourquoi, bien que nous ayons accablé le primordial attendu de ce travail, d'autres paramètres à aborder sont toujours offerts aux chercheurs ultérieurs. Il s'agit par exemple, la mise en place d'un réseau WAN interconnectant tous les hôpitaux de la ville de Bukavu voir même ceux de la province du Sud-Kivu en général, ou soit faire une étude de réalisation de l'interconnexion des sites des Hôpitaux Publics de la RDC par la technologie WIMAX.

3.8. Conclusion

Nous avons vu dans ce chapitre que le réseau actuel des hôpitaux publics de la ville de Bukavu ne correspond plus aux exigences du réseau, que ce soit au niveau de la performance, de la disponibilité, de la sécurité ou de la facilité de gestion. Nous avons donc vu, après, les différentes étapes nécessaires à la conception du nouveau réseau des hôpitaux publics. Ce chapitre nous a montré la simulation du réseau réalisé au sein des hôpitaux publics de la ville de Bukavu. Il nous a permis de survoler toutes les configurations nécessaires pour la réalisation de ce travail. Nous avons utilisé ici le protocole SFTP comme outil de sécurité des données et la technologie WiMAX pour combler certaines défaillances d'interconnexion car de nos jours il faisait partie des outils de simulation de réseau puissant et indispensable et permettre ainsi aux ordinateurs distants de ces hôpitaux de communiquer et d'échanger des fichiers médicaux et autres (les recherches cliniques, les innovations médicales et pharmaceutiques, la sécurité sanitaire, la qualité des soins) comme s'ils faisaient partie d'un même réseau local. Nous avons pu voir qu'il y a quand même des différences entre la réalisation et la simulation avec les manques d'option et d'équipements du logiciel de simulation.

Conclusion Générale

Les réseaux informatiques et les ordinateurs constituent aujourd'hui des outils essentiels au succès des entreprises voir même des hôpitaux, peu importe sa taille. Par l'utilisation de protocoles appropriés, on arrive à soulever les problèmes posés tout en configurant les équipements. Ainsi dit, l'objectif de ce travail de mémoire de fin d'études intitulé « conception d'un réseau MAN interconnectant différents Hôpitaux publiques de la ville de Bukavu pour l'échange des fichiers » est de faire un diagnostic de différents problèmes du réseau local existant dans les hôpitaux publics de Bukavu et proposer un nouveau réseau MAN sécurisé répondant aux exigences de l'entreprise.

Il a été vu que les hôpitaux publics de la ville de Bukavu éprouvent plusieurs difficultés dans la gestion centralisée de leurs données et informations ainsi que dans les échanges des fichiers entre eux avec comme conséquence le manque de segmentation du réseau avec des domaines défaillants étendus et la sécurité déployée dans ces hôpitaux est trop faible n'empêchant pas tout le trafic non autorisé ou indésirable. Cette situation a suscité une interrogation qui est celle de savoir quelle est la stratégie à prendre pour assurer une interconnexion ou une liaison optimale des différents hôpitaux publics distants dans la ville de Bukavu ? Ainsi, nous avons formulé notre hypothèse en précisant que la conception et la mise en place d'un réseau ou support moins encombrant et facile d'installation propulsant les technologies d'interconnexion sans fil MAN à partir de WiMAX bâti d'un protocole SFTP pour l'échange des fichiers serait la meilleure stratégie et orientation à prendre pour assurer une liaison optimale des différents hôpitaux publics distants de la ville de Bukavu

Ainsi, pour atteindre nos résultats (objectifs) et bien mener à port ce travail, le produit encore plus performant pouvant opérer sur des fréquences réglementées nous a semblé plus adéquate à notre contexte qu'est la technologie ***WiMAX***. En plus, pour mener cette étude, nous avons recouru aux enquêtes à partir de la technique d'observation et la technique documentaire. La technique d'observation nous a permis à décrire les problèmes qui continuent à gangrener dans la gestion centralisée des données et informations ainsi que dans l'interaction entre les hôpitaux publics de Bukavu. La technique documentaire nous a amené et permis dans le cadre de réalisation de ce travail à passer en revue des différents documents (ouvrages, publications, autres travaux scientifiques, …) abordant l'objet de notre étude.

Motivé par le souci de réaliser cette étude, nous avons présenté notre méthodologie en justifiant nos choix. Ainsi, nous avons présenté l'état de l'art de la technologie WiMAX. Cette technologie nous a permis de combler certaines défaillances d'interconnexion en permettant aux utilisateurs d'avoir un accès haut débit à Internet sans avoir besoin de se connecter sur les BLR filaires (câbles) mais plutôt une connexion longue distance et sans fil. Le SSH file transfer protocol (abrégé en SFTP) nous a semblé le mieux indiqué pour assurer le transfert de données en toute sécurité entre deux personnes souhaitant communiquer.

Enfin, nous avons passés aux différentes étapes nécessaires à la conception du nouveau réseau des hôpitaux publics. Nous avons montré la simulation du réseau réalisé au sein des hôpitaux publics de la ville de Bukavu. On a retrouvé l'efficacité des protocoles de haute disponibilité : SFTP au niveau commutateur et Ethernet au niveau routeur qui gèrent en plus les partages de charge et les redondances. L'installation, la configuration des serveurs et des équipements d'interconnexion (routeurs et switch) se sont faites de façon identique sur les cinq sites distants. Les quatre hôpitaux publics de la ville de Bukavu ayant besoin d'une connexion MAN entre eux, nous avons créés une liaison avec l'antenne RENATELSAT.

Au cours de notre travail, nous nous sommes heurtés à certaines difficultés entre autres : Pour ce qui est de la documentation, nous n'avons pas trouvé assez des documents qui parlant de la conception d'un réseau MAN interconnectant les hôpitaux, ce qui a rendu notre travail moins facile à réaliser et les hôpitaux publics de la ville de Bukavu qui sont notre milieu de recherche, n'ont pas encore fait l'objet de recherche pour ce qui est de la conception de réseau les interconnectant entre eux pour l'échange des fichiers. C'est pourquoi nous admettons que nos théories et nos réflexions bien qu'empiriques ne soient pas des vérités indubitables et définitives. Elles sont susceptibles d'être réfutées par des modèles plus robustes ou par des observations postérieures divergentes qui seraient liées à l'évolution des technologies, elles-mêmes en constante mutation.

Bien que nous ayons épuisé l'essentiel attendu de ce travail, d'autres paramètres à aborder sont toujours offerts aux chercheurs ultérieurs. C'est le propre de toute proposition intellectuelle de s'attendre à être un jour ou l'autre dépassée. Mais elle peut tout aussi bien être plus tard renforcée par d'autres approches et mises en place. De ce fait, en toute humilité, nous restons très attentifs à toutes questions, suggestions et remarques constructives.

Bibliographie

[1] Adidou, A. (2017). *Réalisation d'une application de gestion pour une ligne d'assamblage.* Algéri: Université Abou bekr Belkaid.

[2] AdmiSco. (2019). Logiciel complet pour l'administration scolaire. *Evollutiion pllanniing*, 1-121.

[3] Alcatel. (2014). *WiMAX, making ubiquitous high-speed data services a reality.* Wireless Broadband Access.

[4] Alecu, F. (2010). The WiMAX Technology. *Oeconomics of Knowledge*, 2-9.

[5] Amazone.com. (2023). Récupéré sur http://www.amazone.com

[6] Amirouche, M. (2018). Internet. 1-10.

[7] Bassem, C. (2017). Conception et réalisation d'une application web de gestion des notes à l'IELSHT. *Sciences et Technologies de l'Information et de communication, IV*(2), 1-75.

[8] Batch. (n.d). Mettre en place un canal SFTP. *Manuel D'Utilisateur*, 1-36.

[9] Cipière, S. (2016). *Un systeme de mediation distribué pour l'e-santé et l'épidémiologie.*

[10] Cipière, S. (2017). *Un système de médiation distribué pour l'e-santé et l'épidémiologie.* Paris: L'archive ouverte pluridisciplinaire HAL,.

[11] Coupechoux, M., Godlewski, P., & Martins, P. (n.d). *Introduction à WiMAX.* Paris: Département Informatique et Réseaux.

[12] Cylia, S., & Abdelatif, O. (2015). Conception et réalisation d'une application web pour la gestion des étudiants d'une école privee. Cas d'étude : "ISA School". 1-70.

[13] Drissa, I., & Ibrahim, T. (2010). *Gestion des inscriptions en ligne à l'Université Polytechnique de Bobo-Dioulasso.* BOBO-DIOULASSO: Universite Polytechnique De Bobo-Dioulasso.

[14] Duchateau, F. (2021). *Modélisation - niveau conceptuel.* Lyon: Université Claude Bernard Lyon 1.

[15] Elhadari, Z. (n.d). *Reseaux informatiques.* Centre de BTS Dakhla.

[16] Equipe Firewalling. (n.d). *Conception et mise en place d'une architecture de sécurité des services Intranet / Internet.*

[17] Faustin, P. (2014). *ModeEmploi_JMerise.* Paris: Université Paris-Est Marne-la-Vallée.

[18] Fellegi, I. P. (2013). Méthodes et pratiques d'enquête. *Statistique Canada, X*(12-587), 1-434.

[19] Flory, A., & Rolland, C. (2000). la conception des systèmes d'information : état de l'art et nouvelles perspectives. *Nouvelles perspectives des systèmes d'information*, 3-41.

[20] Flory, A., & Rolland, C. (n.d). la conception des systèmes d'information : état de l'art et nouvelles perspectives. *Laboratoire d'informatique appliquée*, 1-29.

[21] Folane, M., & Bamogo, M. (2006). interconnexion des sites de la SONAPOST situés à Ouagadougou par la technologie WiMAX. *Reseaux et maintenance informatiques*, 1-81.

[22]Franck, D. (2018). *mise en place d'un vpn (site-to-site) au sein d'une entreprise : cas de la soroubat (societe de routes et batiments).* Abindjan: Ecole Supérieure de Génie Informatique.

[23]François, D. (2010). *Approche méthodologique de la mise en place d'un réseau multiservice.* Paris: L'archive ouverte pluridisciplinaire HAL.

[24]Frédéric, A. N. (2011). *Planification d'un réseau WiMAX avec prise en compte des contraintes de qualité de service et de capacité.* Ecole Superieure Polytechnique, Services des Télécommunications, de l'Informatique et du Multimédia. Antananarivo: Universite D'Antananarivo.

[25]Frédéric, D. G. (2001, Juillet 15). Méthodologie des systèmes d'information - MERISE. *Cours du cycle B du Cnam.doc*, 1-101.

[26]Fuchs, P., & Poulain, P. (2019). *Programmation en Python pour les sciences de la vie.* Paris, France, France: éditions Dunod.

[27]Gogniat, C. (2010). *Développement d'un logiciel de suivi pour l'élève sur Educlasse.* Généve: Université de GENEVE.

[28]Guibert, O. (2007). *Cours d'Analyse et Conception des Systèmes d'Information (d'Outils et Modèles pour le Génie Logiciel).* Bordeaux: Département Informatique de l'IUT de l'Université Bordeaux 1.

[29]Guibert, O. (2007). *Cours d'Analyse et Conception des Systèmes d'Information (d'Outils et Modèles pour le Génie Logiciel).* Bordeaux: Département Informatique de l'IUT de l'Université Bordeaux 1.

[30]Hamid, K. (2017). Conception et réalisation d'une application web de gestion d'école. *Systémes Intelligents & Réseaux*, 1-93.

[31]Hanen, C. (n.d). *Outils informatiques.*

[32]Jean-Luc, A. (2011). Cours Interconnexion et conception de réseaux informatiques. *L'archive ouverte pluridisciplinaire*, 1-162.

[33]Julien, S. (2016). *Conception et réalisation d'un système d'information sur la formation documentaire : SINFODOC.* Lyon: Science de l'information.

[34]Kenza, K. (2018). *Etude et simulation du standard de transmission de donnéesans fil : WIMAX par OPNET comparé avec WIFI.* Université Mohamed Khider de Biskra.

[35]Leïla, C. (2016). *La technologie WiMAX.* Algerie: Direction de l 'Interconnexion et des Nouvelles Technologies.

[36]Mahdi, M. (2012). *Architectures réseaux pour le partage de contenus multimédias avec garantie de qualité de service.* Toulouse: Université Paul Sabatier.

[37]Mama, S. (2018). Avant projet d'interconnexion satellitaire pour la gestion des urgences du Service d'Aide Médicale des Urgences (SAMU-BENIN) aux autres centres utilisateurs. *Electronique & Télécommunication*, 1-135.

[38]Matta, N. (2011). *Conception et installation d'un système de surveillance dans une menuiserie avec émission d'alarme à distance.* Liban: L'archive ouverte pluridisciplinaire HAL.

[39]Messouci. (2017). *JMERISE.* Marseille: l'Université Aix-Marseille.

[40]Mian, S. (2006). WiMAX ou l'évolution des réseaux sans-fil ? *Lex Electronica, XI*(1), 1-17.

[41]Mohamed, O. B., & Fettah, A. (n.d). *Développement d'un Outil de planification.*

[42]Nampoina, A. N. (2015). Conception Et Mise En Place Du Reseau Hierarchique A Haute Disponibilite Au Sein Du MFB. *Système de traitement d'informations (STI)*, 1-100.

[43]Nampoina, A. N. (2016). *Conception et mise en place du reseau hierarchique à haute disponibilité au sein du MFB.*

[44]Olivier, G. (n.d). *Applications des réseaux informatiques et de l'Internet.* Lyon: Initiation Réseaux.

[45]Ouemba. (2009). *Optimisation d'un réseau WIMAX : Cas de SACONETS S.A.* Cameroun/Yaoundé: ESMT.

[46]Oumar, D. A., & Hamadoun, T. (2010). Etude et mise en place d'un réseau informatique sécurisé à l'HDJ. *reseaux et maintenance informatiques*, 1-75.

[47]Paul, E., & Nabil, D. (2010). *Etude de la technologie WIMAX MOBILE.* Paris: Telecom sudparis.

[48]Peersman, G. (2014). Présentation des méthodes de collecte et d'analyse de données dans l'évaluation d'impact. *Note méthodologique*(10), 1-24.

[49]Pietrosemoli, E., & al. (2009). *Réseaux sans fil dans les pays en développement.* Paris: Hacker Friendly.

[50]Rongere, P. (1971). *Méthodes de science sociale.* Paris: Dalloz.

[51]Sanna, M. (2014). *Etude et dimensionnement d'un réseau WiMAX fixe.* Tlemcen: Université de Tlemcen.

[52]Sébastien, M., & Wattiau, Y. (2005). Installation et configuration d'un serveur FTP (FileZilla Server version FR). *FileZilla Server*, 1-53.

[53]Timnou, J.-P. (2015). Collecte et Analyse des données. *Informatique & Statistiques*, 1-40.

[54]Trabelsi, K., & Amara, H. (2011). Mise en place des réseaux LAN interconnectés en redondance par 2 réseaux WAN. *One TECH Business Solution*, 1-37.

[55]WiMAX Forum. (n.d). *"Technical Information",.*

[56]Wissam, A., & Imane, B. (2013). *Etude et caractérisation de la couche physique du standard IEEE802.16/WIMAX.* Algerie: Universite Abou Bekr Belkaid Tlemcen.

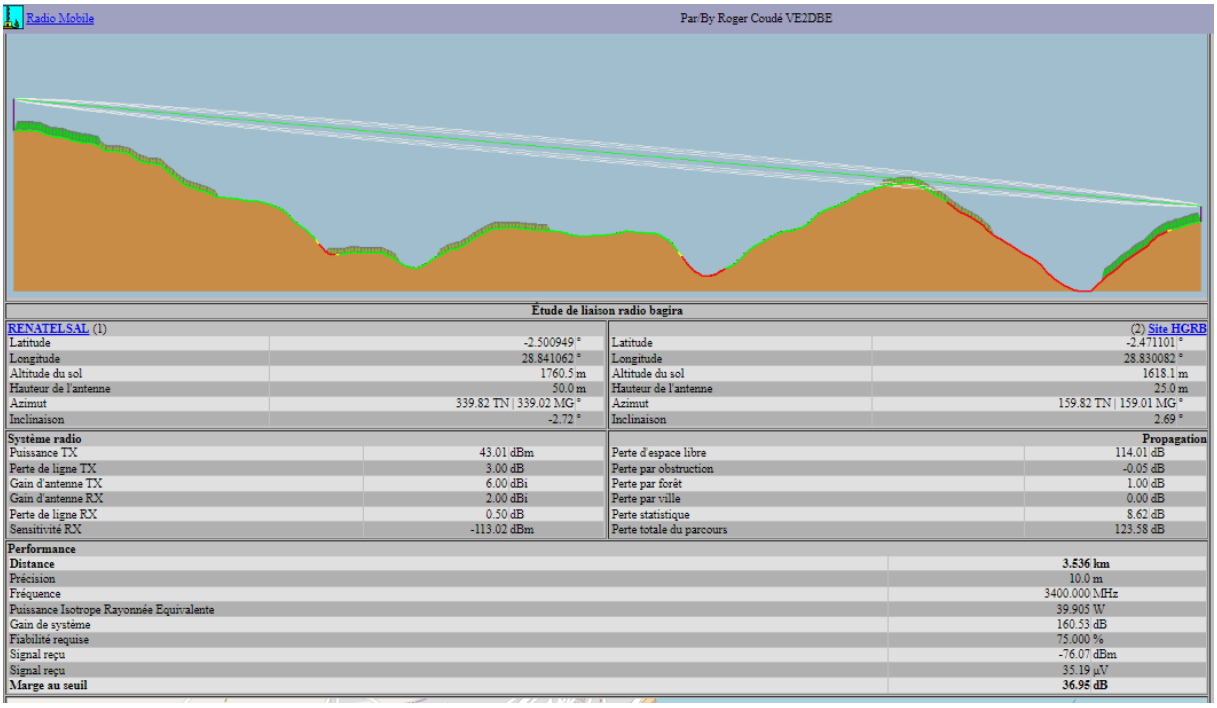
[57]Xiaojun, Y. (2013). Modélisation et simulation des systèmes de production : une approche orientée-objets. *L'archive ouverte pluridisciplinaire*, 1-257.

[58]Zimbardo, P. (2010). Modélisation d'un système d'information dans le cadre de projets de coopération géoterritoriale. *Sciences de l'Homme et Société*, 1-320.

[59]Zouhair, E.-K. (n.d). SFTP & SCPOnly. *Projet Administration Réseaux*(20072486), 1-7.

ANNEXES

ANNEXES 1 : Les liaisons



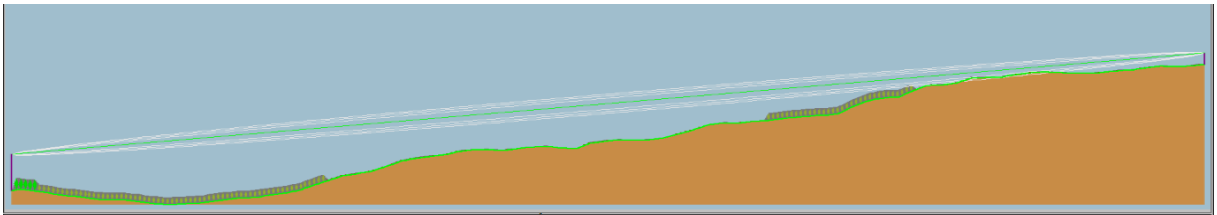
Étude de liaison radio bagira

RENATELSAL (1)		(2) Site HGRB	
Latitude	-2.500949 °	Latitude	-2.471101 °
Longitude	28.841062 °	Longitude	28.830082 °
Altitude du sol	1760.5 m	Altitude du sol	1618.1 m
Hauteur de l'antenne	50.0 m	Hauteur de l'antenne	25.0 m
Azimut	339.82 TN | 339.02 MG °	Azimut	159.82 TN | 159.01 MG °
Inclinaison	-2.72 °	Inclinaison	2.69 °

Système radio		Propagation	
Puissance TX	43.01 dBm	Perte d'espace libre	114.01 dB
Perte de ligne TX	3.00 dB	Perte par obstruction	-0.05 dB
Gain d'antenne TX	6.00 dBi	Perte par forêt	1.00 dB
Gain d'antenne RX	2.00 dBi	Perte par ville	0.00 dB
Perte de ligne RX	0.50 dB	Perte statistique	8.62 dB
Sensitivité RX	-113.02 dBm	Perte totale du parcours	123.58 dB

Performance	
Distance	**3.536 km**
Précision	10.0 m
Fréquence	3400.000 MHz
Puissance Isotrope Rayonnée Equivalente	39.905 W
Gain de système	160.53 dB
Fiabilité requise	75.000 %
Signal reçu	-76.07 dBm
Signal reçu	35.19 µV
Marge au seuil	**36.95 dB**

Figure 32 Liaison RENA-BAGIRA



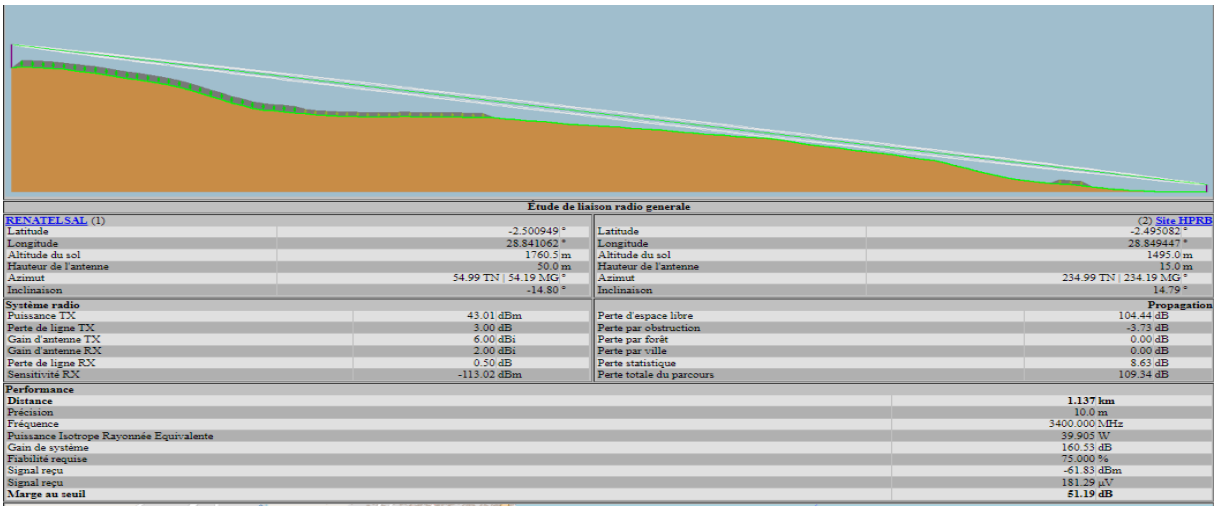
Étude de liaison radio ciriri

RENATELSAL (1)		(2) Site HGRC	
Latitude	-2.500949 °	Latitude	-2.523609 °
Longitude	28.841062 °	Longitude	28.835429 °
Altitude du sol	1760.5 m	Altitude du sol	1932.8 m
Hauteur de l'antenne	50.0 m	Hauteur de l'antenne	15.0 m
Azimut	193.95 TN | 193.14 MG °	Azimut	13.95 TN | 13.15 MG °
Inclinaison	3.02 °	Inclinaison	-3.04 °

Système radio		Propagation	
Puissance TX	43.01 dBm	Perte d'espace libre	111.33 dB
Perte de ligne TX	3.00 dB	Perte par obstruction	-0.49 dB
Gain d'antenne TX	6.00 dBi	Perte par forêt	0.00 dB
Gain d'antenne RX	2.00 dBi	Perte par ville	0.00 dB
Perte de ligne RX	0.50 dB	Perte statistique	8.58 dB
Sensitivité RX	-113.02 dBm	Perte totale du parcours	119.42 dB

Performance	
Distance	**2.596 km**
Précision	10.0 m
Fréquence	3400.000 MHz
Puissance Isotrope Rayonnée Equivalente	39.905 W
Gain de système	160.53 dB
Fiabilité requise	75.000 %
Signal reçu	-71.91 dBm
Signal reçu	56.81 µV
Marge au seuil	**41.11 dB**

Figure 33 Liaison RENA CIRIRI

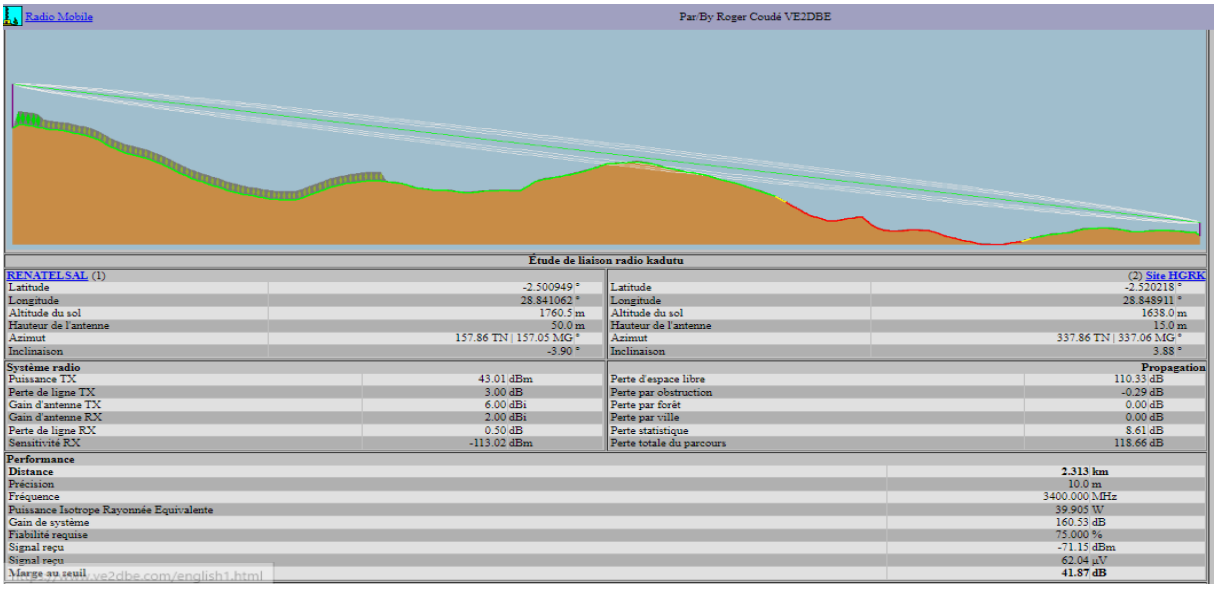


Étude de liaison radio generale

RENATELSAL (1)		(2) Site HPRB	
Latitude	-2.500949 °	Latitude	-2.495082 °
Longitude	28.841062 °	Longitude	28.849447 °
Altitude du sol	1760.5 m	Altitude du sol	1495.0 m
Hauteur de l'antenne	50.0 m	Hauteur de l'antenne	15.0 m
Azimut	54.99 TN | 54.19 MG °	Azimut	234.99 TN | 234.19 MG °
Inclinaison	-14.80 °	Inclinaison	14.79 °
Système radio		**Propagation**	
Puissance TX	43.01 dBm	Perte d'espace libre	104.44 dB
Perte de ligne TX	3.00 dB	Perte par obstruction	-3.73 dB
Gain d'antenne TX	6.00 dBi	Perte par forêt	0.00 dB
Gain d'antenne RX	2.00 dBi	Perte par ville	0.00 dB
Perte de ligne RX	0.50 dB	Perte statistique	8.63 dB
Sensitivité RX	-113.02 dBm	Perte totale du parcours	109.34 dB

Performance	
Distance	**1.137 km**
Précision	10.0 m
Fréquence	3400.000 MHz
Puissance Isotrope Rayonnée Equivalente	39.905 W
Gain de système	160.53 dB
Fiabilité requise	75.000 %
Signal reçu	-61.83 dBm
Signal reçu	181.29 µV
Marge au seuil	**51.19 dB**

Figure 34 Liaison RENA-HPGRB



Étude de liaison radio kadutu

RENATELSAL (1)		(2) Site HGRK	
Latitude	-2.500949 °	Latitude	-2.520218 °
Longitude	28.841062 °	Longitude	28.848911 °
Altitude du sol	1760.5 m	Altitude du sol	1638.0 m
Hauteur de l'antenne	50.0 m	Hauteur de l'antenne	15.0 m
Azimut	157.86 TN | 157.05 MG °	Azimut	337.86 TN | 337.06 MG °
Inclinaison	-3.90 °	Inclinaison	3.88 °
Système radio		**Propagation**	
Puissance TX	43.01 dBm	Perte d'espace libre	110.33 dB
Perte de ligne TX	3.00 dB	Perte par obstruction	-0.29 dB
Gain d'antenne TX	6.00 dBi	Perte par forêt	0.00 dB
Gain d'antenne RX	2.00 dBi	Perte par ville	0.00 dB
Perte de ligne RX	0.50 dB	Perte statistique	8.61 dB
Sensitivité RX	-113.02 dBm	Perte totale du parcours	118.66 dB

Performance	
Distance	**2.313 km**
Précision	10.0 m
Fréquence	3400.000 MHz
Puissance Isotrope Rayonnée Equivalente	39.905 W
Gain de système	160.53 dB
Fiabilité requise	75.000 %
Signal reçu	-71.15 dBm
Signal reçu	62.04 µV
Marge au seuil	**41.87 dB**

Figure 35 Liaison RENA-Hôpital de Kadutu

ANNEXES 2: Les Equipements à installer par Site

N°	Equipements	Qté	Caractéristiques
Site RENATELSAT			
1	Antenne	1	Antenne Nano Omnidirectionnel configuré en point to multipoint avec les autres Antennes
2	Routeur	1	
3	Machine Serveur	1	Système d'exploitation Ubuntu, Minimum 2TB, 8GB RAM, Processeur 2,5GHz
4	Prise Ethernet	1	
5	Câble Ethernet	1	Minimum 80m
6	Alimentation POE	1	
Site HPGRB			
1	Antenne	1	Antenne Nano Station configuré en point to point avec l'antenne RENA
2	Point d'accès Wifi	3	

3	Machine serveur	30	Système d'exploitation Win10, Minimum 500GB, 8GB RAM, Processeur 2,5GHz
4	Prise Ethernet	25	
5	Switch	3	24 ports
6	Câble Ethernet		Minimum 500m
7	Alimentation POE	1	
8	Routeur Cisco	1	
Site HGRB/Hôpital de CIRIRI et Hôpital de Kadutu			
1	Antenne	1	Antenne Nano Station configuré en point to point avec l'antenne RENA
2	Point d'accès Wifi	2	
3	Machine serveur	30	Système d'exploitation Win10, Minimum 500GB, 8GB RAM, Processeur 2,5GHz
4	Prise Ethernet	25	
5	Switch	2	24 ports
6	Câble Ethernet		Minimum 300m
7	Alimentation POE	1	
8	Routeur Cisco	1	

Tableau 9 Les Equipements à installer par Site