Ministère des **E**nseignements **S**econdaire et **S**upérieur
(**MESS**)

Secrétariat Général

Université **P**olytechnique de **B**obo-Dioulasso (**U.P.B.**)

Ecole **S**upérieure d'**I**nformatique (**E.S.I**)

Cycle des **I**ngénieurs de **T**ravaux **I**nformatiques (**C.I.T.I**)
Option : **R**éseau et **M**aintenance **I**nformatique **(ReMI)**

Rapport de fin de cycle

THEME : « INTERCONNEXION DES SITES DE LA SONABEL : CAS DE LA DIRECTION REGIONALE DE L'OUEST»

Période du 15 Octobre 2013 au 15 janvier 2014

Auteurs : Arnaud TAMINI & Somaye OUATTARA

Maître de stage

Mr Souleymane ZONGO

Responsable de la Division Informatique de BOBO

Superviseur

Dr. Telesphore TIENDREBEOGO

Enseignant chercheur à l'Université Polytechnique de Bobo-Dioulasso

Année académique : 2012-2013

TABLE DES MATIERES

DEDICACES

Nous aimerons dédier ce travail à tous ceux qui ont une place particulière aussi bien dans nos esprits que dans nos cœurs.

Nous pensons avant tout à ces intarissables puits de sagesse, d'affection et dévouement qui sont nos parents.

A nos chers Frères et Sœurs, pour tout ce qu'on a vécu, et que nous espérons nous restons proche et solidaires.

A nos meilleurs amis.

REMERCIEMENTS

Nous voudrions remercier notre encadreur, Mr ZONGO Souleymane pour son soutien et ses recommandations judicieuses. Aussi nous présentons nos remerciements les plus sincères à tous les agents et employés de la société nationale d'électricité du Burkina de la région de l'ouest pour leur volonté, la pertinence de leur remarque et la subtilité de leur conseil qui ont été pour nous des atouts importants dans l'élaboration de notre stage.

Nous adressons nos reconnaissances à Dr. TIENDREBEOGO B. Telesphore pour sa patience lors de nos nombreuses discussions techniques, pour l'aide qu'il nous a apporté et pour nous avoir sensibilisés à la clarté et la rigueur dans l'écriture.

Nous devons chaque brique de notre connaissance à nos enseignants de l'école supérieure informatique de l'université polytechnique de Bobo-Dioulasso qui ont su bien mené leur noble quête d'enseigner tous ce qu'il faut. Nous les remercions non seulement pour leur savoir qu'ils nous ont transmis, mais aussi pour la fierté et l'ambition que leur personne nous aspire.

Non loin de tout projet ambitieux, il existe des personnes qui partagent sans jamais se lasser ses meilleurs et ses pires moments. Ce sont des personnes qui nous ont soutenu dans chacun de nos instants de faiblesses, et qui, sans leurs extrêmes attention et gentillesses, nous ne serons pas ce que nous sommes devenus aujourd'hui. En tête de liste de ces gens nous placerons nos familles bien aimées qui n'ont jamais hésité à nous offrir le meilleur qu'elles pouvaient. Viennent alors nos camarades de promotions ainsi que tous nos amis qui nous ont aidés de façon directe ou tout simplement par leur présence et leur soutien moral.

Finalement nous tenons à remercier l'école supérieure d'informatique de l'Université Polytechnique de Bobo-Dioulasso qui nous a donné l'occasion de s'intégrer dans la vie professionnelle durant trois mois. Et nous espérons que ce travail sera convainquant et satisfaisant.

LISTE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ANNEXES

LES SIGLES

ADSL	Asymetric Digital Subscriber Line
AH	Authentication Header
AK	Authorization Key
AOF	Afrique Occidentale Française
AP	Analyse Programmation
ASA	Advanced Security Appliant
ATM	Asynchrnous Transfer Mode
BLR	Boucle Local Radio
BTS	Base Transceiver Station
CDMA	Code division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
CICI	Cycle d'Ingénieur de Conception Informatique
CNR	Conseil National de Révolution
DES	Data Encryption Standard
DHCP	Protocole de Configuration dynamique Host
DNS	Domain Name Server
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EIK	EAP Integrity Key
ESI	Ecole Supérieure d'Informatique
ESP	Encapsulating security Payload
FAI	Fournisseur d'Accès en Internet
FDDI	Fiber Distributed Data Interface
FDMA	Frequency Division Multiple Access
FHSS	Frequency Hopping Spread Spectrum

GRE	Geneic Routing Encapsulation
GSM	Global System for Mobile
HP	Hewlett Packarda
HTTP	Hyper Text Transfer Protocol
IBM	International Business Machines
IDU	In Door Unit
IEEE	Institue of Electrical and Electronic Engeneer
IETF	Internet Engineerring Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	Internet Protocol Security
ISA	Internet Security Association
ISAKMP	Internet Security Association and Key Managemant Protocol
L2F	Layer two forwarding
L2TP	Layer two Tunneling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network
LMD	Licence Master Doctorat
LNS	L2TP Network Server
LOS	Line Of Sight
LS	Liaison Spécialisée
MAC	Medium Access Control
MAN	Metropolitan Area Network
MPPC	Microsoft Point to Point Compression
MPPE	Microsoft Point to Point Encryption

MPLS	Multi-Protocol Label Switching
MS	Mobil Station
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol
MSK	Master Session Key
NAS	Network Access Server
ODU	Out Door Unit
OFDMA	Orthogonal Frequency Division Multiple Access
ONATEL	Office National des Telecommunications
ONEA	Office National des Eaux et de l'Assainissement
PAP	Password Authentication Protocol
PMP	Point Multi Point
PPP	Point to Point Protocol
PPTP	Point to Point Tunneling Protocol
QoS	Quality of Service
RAID	Redundant Array of Independant Disk
RéMI	Réseau Maintenance Informatique
RFC	Request For Comment
RLI	Réseau Local Interne
RSA	Rivest Shamir Adlman
SA	Association de Sécurité
SAD	Security Association Data
SAFELEC	Société Africaine d'Electricité
SONABEL	Société Nationale d'électricité Burkinabé
SPAP	Shiva Password Authentication Protocol
SPD	Données de Politique de Sécurité

SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TDMA	Time Division Multiple Access
UO	Université de Ouagadougou
UPB	Université Polytechnique de Bobo-Dioulasso
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VOLTELEC	Société Voltaique d'Electricité
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
W-OFDM	Wide-Orthogonal Frequency Division Multiplexing
WAN	Wide Area Network
WIMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network

PREAMBULE

Dans le but de décentraliser la formation universitaire qui était centrée à l'Université de Ouagadougou (UO), un centre universitaire fut créé en 1995 à Bobo-Dioulasso. Ce centre devient une université en 1997 sous le nom de «Université Polytechnique de Bobo-Dioulasso (UPB) ». Elle a pour objectif de donner une formation professionnelle aux étudiants. Avec le système Licence Master Doctorat (LMD), L'UPB a subi des modifications et comprend actuellement :

1. l'Ecole Supérieure d'Informatique (ESI) ;
2. les instituts :
   - ❖ l'Institut de Développement Rural (IDR) ;
   - ❖ l'Institut Nationale des Sciences de la Santé (INSSA) ;
   - ❖ l'Institut Universitaire de Technologie (IUT) ;
3. les Unités de Formations et de Recherches :
   - ❖ Science Juridique et Politique (SJP) ;
   - ❖ Science Juridique Politique Economique et Gestion (SJPEG) ;
   - ❖ Science et Technologie (Génie Biologie, Maths Informatique, Science Biologie) ;

L'Ecole Supérieure d'Informatique (ESI) dès sa création en 1990 a d'abord été implantée à l'U.O, et fut transférée ensuite au sein de l'UPB en septembre 1995. Sa mission première est d'accompagner le pays dans son ambition de s'approprier les technologies de l'information et de la communication. Elle a pour mission la formation fondamentale, appliquée et/ou professionnelle dans les domaines de l'informatique, la formation continue.

L'ESI offre :

- ✓ Le Cycle des Ingénieurs des Travaux Informatique (CITI) ;
- ✓ Le Cycle des Ingénieurs de Conception en Informatique (CICI) ;
- ✓ Le cycle du Diplôme d'Etudes Approfondies (DEA) créé en 2003.

Le Cycle des Ingénieurs de Travaux en Informatique (CITI) comprend deux filières :

- ➢ L'Analyse et Programme (AP) qui existe depuis la création de l'ESI ;
- ➢ Le Réseau et Maintenance Informatique (RéMI) créé en octobre 2000 avec le soutien de la coopération Française.

Pour consolider en qualité, la formation suivant le système Licence Master Doctorat, il a été prévu dans le semestre six un stage pratique de trois mois en entreprise et donc l'obtention du diplôme sera sanctionné par une soutenance publique. C'est dans ce cadre que nous avons été admis à la SONABEL/BOBO pour effectuer notre stage du 1er octobre au 31 décembre 2013.

INTRODUCTION GENERALE

Parmi les facteurs nécessaires au fonctionnement de toute entreprise, s'inscrit fortement le système d'information dont la gestion optimale est un moyen incontournable pour une entreprise possédant plusieurs succursales. Cette gestion du système d'information, qui constitue l'ensemble des équipements nécessaire à l'automatisation de l'information, passe au préalable, par le choix d'une technologie de télécommunication adaptée. C'est le cas notamment de la centralisation des bases de données du paysage d'un grand nombre d'entreprise.

La SONABEL/BOBO, société dans laquelle nous avons été admis à effectuer notre stage s'inscrit dans cette logique d'interconnexion de ces sites rattachés. Seulement, jusqu'à ce jour, le système d'information de la DRO/SONABEL souffre d'un manque de moyen de télécommunication permettant de relier ces différents sites. Les principaux moyens utilisés sont le téléphone et les E-mails, ce qui ne va pas sans problème tant pour la société que pour la clientèle : problème de gestion du personnel, de gestion de stock, lenteur du service etc.

C'est en observant tous ces dysfonctionnements dans le système de communication que nous avons opté de proposer une amélioration, d'où le thème de notre rapport : « INTERCONNEXION DES SITES DE LA SONABEL : CAS DE LA DIRECTION REGIONALE DE L'OUEST».

Ainsi, pour une meilleure compréhension de notre travail, ce document est organisé autour de quatre grandes parties structurées en chapitres. La première partie, présentation de la structure d'accueil, décrit de manière succincte la SONABEL. La seconde partie, problématique, met en relief le problème observé en entreprise. Les technologies d'interconnexions, qui constitue la troisième partie, où nous faisons une étude comparative des différentes technologies d'interconnections envisageables. La dernière partie intitulée étude et mise en œuvre de la technologie choisie, vient présenter la technologie choisie et sa mise en œuvre.

PREMIERE PARTIE I : PRESENTATION DE LA STRUCTURE D'ACCUEIL

CHAPITRE I

PRESENTATION DE LA SONABEL

I.1 HISTORIQUE DE LA SONABEL

En février 1954 à Ouagadougou la société nationale d'électricité du BURKINA a entrepris ses activités et en octobre de la même année à Bobo-Dioulasso sous le nom d'Energie Afrique Occidentale Française (AOF). Société française à l 'époque au capital de 150.000.000 F CFA, la SONABEL a connu de nombreuses transformations tant au niveau de sa structure financière (capital) que de sa dénomination avant de prendre sa forme actuelle.

En effet, elle s'est vue confié en plus de sa mission primaire en 1956, la distribution d'eau dans les villes de OUAGADOUGOU et BOBO-DIOULASSO jusqu'en 1970 ou cette tache fut assignée à l'Office National des Eaux et de l'Assainissement (ONEA).

Au lendemain des indépendances la société ENERGIE AOF est rénovée en une société d'économie mixte multinationale dénommée société Africaine d'électricité (SAFELEC) avec un capital de 50 millions de francs CFA.

Exprimant le souci de contrôler les activités économiques sur son territoire, la société est transformée en une société de droit Voltaïque sous le nom de Société Voltaïque d'Electricité (VOLTELEC) en 1968 au capital de un milliard (1.000.000.000) de francs CFA. Suite au changement du nom du pays le 04 août 1984, avec l'avènement du Conseil National de la révolution (CNR), la VOLTELEC a pris la dénomination de Société Nationale d'Electricité du Burkina en abrégé SONABEL avec un capital de 1.387.628.180 f CFA. Suite au changement du nom du pays le 04 août 1984, avec l'avènement du Conseil National de la révolution (CNR), la VOLTELEC a pris la dénomination de Société Nationale d'Electricité du Burkina en abrégé SONABEL avec un capital de 1.387.628.180 f CFA.

Par décret n° 095/160/PRES/MICM/TPHU du 14 avril 1995, la SONABEL a changé de statut juridique. Elle est passée de forme d'Etablissement publique à caractère industriel et commercial à celle de société d'Etat.

Par décret n° 97-599/PRES/PM/MEM/MCIA DU 31 décembre 1997, le statut de la SONABEL comme société d'Etat ont été approuvés.

Depuis 1998, l'Etat a procédé à l'ouverture du sous-secteur d'électricité au privé. Jusqu'à ce jour aucune société privée n'a encore pu s'investir dans la production d'électricité au Burkina.

La loi n° 012/2001/AN du 04 juillet 2001 portant autorisation de privatisation de la SONABEL a été votée par l'Assemblée Nationale. Le processus de privatisation est donc engagé

De nos jours la société fonctionne avec un capital de 46.000.000.000 de francs CFA, et avec la politique de l'électricité rurale, la société ne détient plus le monopole de la production et de la distribution de l'électricité au Burkina.

I.2 OBJECTIF DE LA SONABEL

Aujourd'hui, la SONABEL mène des actions concrètes surtout à l'encontre de la clientèle afin de pouvoir s'adapter à cette nouvelle réalité. Ainsi la Société Nationale d'Electricité du Burkina a des projets de grande envergure à savoir:

- L'extension des réseaux de distribution des centres électrifiés;
- La poursuite de l'électricité rurale;
- Respecter les engagements contractuels de fourniture d'électricité en tant que société d'Etat ;
- Améliorer la productivité en créant des conditions axée sur la responsabilisation des cadres et le contrôle des résultats ;
- Assurer une évolution harmonieuse de l'entreprise face aux enjeux et aux changements du secteur énergétique au BURKINA FASO.

I.3 MISSIONS DE LA SONABEL

Elle a pour mission principale la production et/ou l'importation, le transport et la distribution de l'énergie électrique sur tout le territoire burkinabè. Une partie de son énergie lui vient de la Côte d'Ivoire et du Ghana. L'autre partie est produite au Burkina par les centrales thermiques et hydrauliques.

I.4 ORGANISATION INTERNE DE LA SONABEL

Pour un succès de sa mission, la SONABEL s'est dotée d'une structure cohérente et adaptée. Tout en faisant une relecture de son organigramme en juillet 2012 avec pour conséquence la modification de son organisation. Le nouvel organigramme a pris effet depuis le 1er janvier 2013.

I.4.1 PRESENTATION DE LA DIRECTION GENERALE

La SONABEL est administrée par une Direction Générale installée à Ouagadougou, siège social de la Société qui regroupe les Directions Centrales et les Départements suivants :

- ✓ **D**irection des **E**tudes, de la **P**lanification et de l'**E**quipement **(DEPE) ;**
- ✓ **D**irection du **T**ransport **(DT) ;**
- ✓ **D**irection **C**ommerciale et de la **C**lientèle **(DCC) ;**
- ✓ **D**irection de la **P**roduction **(DP) ;**
- ✓ **D**irection de la **D**istribution **(DD) ;**
- ✓ **D**irection des **F**inances et de la Comptabilité **(DFC) ;**
- ✓ **D**irection des **M**archés et du **P**atrimoine **(DMP) ;**
- ✓ **D**irection des **R**essources **H**umaines **(DRH) ;**
- ✓ **D**épartement **N**ormalisation – **E**nvironnement – **S**écurité **(DNES) ;**
- ✓ **D**épartement **A**udit et **C**ontrôle de **G**estion **(DACG) ;**
- ✓ **D**épartement de la **C**ommunication, des **A**rchives et de la **D**ocumentation **(DCAD) ;**
- ✓ **D**épartement **I**nformatique **(DI) ;**

- ✓ **D**épartement **J**uridique et du **C**ontentieux **(DJC)** ;

A la Direction commerciale et de la clientèle sont rattachées :

- ✓ **D**irection **R**égionale du Kadiogo ;
- ✓ **D**irection **R**égionale de l'**O**uest ;
- ✓ **D**irection **R**égionale du **C**entre ;
- ✓ **D**irection **R**égionale du **C**entre-Ouest ;
- ✓ **D**irection **R**égionale du **C**entre-Est ;
- ✓ **D**irection **R**égionale du **N**ord

Figure 1 : Organigramme de la Direction Générale (confère le papier A3).

I.4.2 PRESENTATION DE LA DIRECTION REGIONALE DE L'OUEST

Elle a en charge les principales missions ci-après :

- ✓ assurer la représentation de la Direction générale dans sa zone géographique ;
- ✓ assurer le recouvrement des revenus liés aux ventes d'électricité et aux produits divers de leur zone géographique ;
- ✓ planifier et organiser les travaux de branchement de la clientèle de leur zone géographique ;

La Direction régionale de l'Ouest dispose de quatre (04) services, de trois (03) divisions et d'un (01) secrétariat de direction :

- ✓ le Service Gestion Clientèle (SGC) ;
- ✓ le Service Moyens Généraux (SMG) ;
- ✓ le Service Centre de Banfora (SC/Banfora) ;
- ✓ le Service Centres Rattachés (SCR) ;
- ✓ la Division Contrôle Budgétaire (DCB) ;
- ✓ la Division Etalonnage et Mesure ;
- ✓ la Division Contrôle Abonnés et Branchements ;
- ✓ le Secrétariat de la Direction Régionale.

Figure 2 : Organigramme de la Direction Régionale de l'Ouest (confère le papier A3).

CHAPITRE II

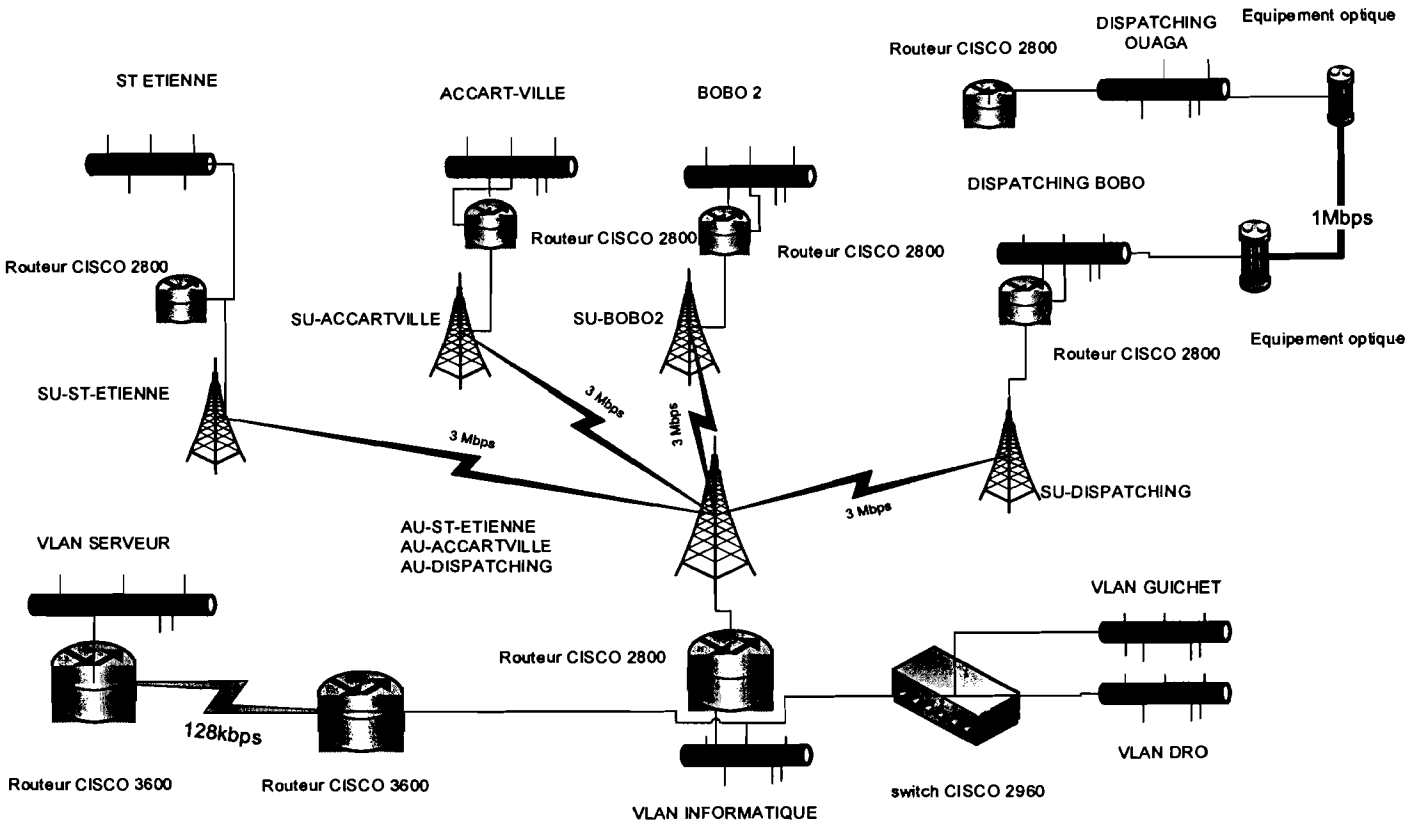
ETUDE DE L'EXISTANT ET CRITIQUE DU RESEAU

II.1 ETUDE DE L'EXISTANT

La SONABEL est une société qui comporte un nombre important de service déployé sur l'ensemble de la région. La DRO a comme but de gérer, de fournir les outils et informations nécessaires de tous les centres qui lui sont rattachés. Ainsi les centres rattachés ont chacun un serveur servant à abriter des systèmes informatiques comme le stockage. Tous les serveurs dans les centres rattachés ne sont pas interconnectés par un réseau local ce qui ne permet pas de communiquer de manière rapide et sure. Dans la DRO il y'a une équipe qui administre les serveurs, qui contrôle et fait le suivi de l'état des serveurs dans tous les centres qui lui sont rattachés.

II.1.1 PRESENTATION DE L'ARCHITECTURE DU RESEAU INFORMATIQUE DE LA DRO/SONABEL.

Toute révision, modification ou action visant à apporter des améliorations de l'architecture du réseau informatique de la DRO/SONABEL doit passer par une connaissance préalable de l'ensemble des différents éléments constituant l'architecture de son réseau informatique existant. La Direction Régionale de l'Ouest a été judicieusement centralisée dans la ville de BOBO-DIOULASSO. Il faut noter que l'interconnexion BOBO-OUAGA est réalisée par fibre optique. L'intranet de la SONABEL/BOBO a accès à la connexion internet à travers la liaison spécialisée. En effet le Réseau informatique de Ouagadougou dispose d'une liaison spécialisée de 2Mb/s qu'il partage avec les autres directions régionale ; ce qui fait un débit de 512kb/s pour les quatre régions. A cet effet la ville de BOBO-DIOULASSO a donc été interconnectée par une technologie sans fils à savoir la Boucle Locale Radio (BLR). Celle-ci est composée de cinq sites à savoir le site de la direction régionale, le site de la DCET situé à Accart-ville, le site de Saint-Etienne, le site de Kodéni (Dispashing) et le site de BOBO 2. Chaque site est composé d'une technologie LAN.



Source: Réalisé par la SONABEL

Figure 3 : Architecture du Réseau actuel de la ville de BOBO

II.1.2 PRESENTATION DE L'INTRANET DE LA DRO/SONABEL

➢ NOTION DE L'INTRANET

Un intranet est une configuration de réseau local très répandue. Les serveurs Web intranet diffèrent des serveurs Web publics en ce que le public doit posséder les autorisations et mots de passe appropriés pour accéder à l'intranet d'une organisation. Les intranets sont conçus pour autoriser les utilisateurs qui ont des privilèges d'accès à accéder au réseau local interne de l'organisation. Au sein d'un intranet, les serveurs Web sont installés dans le réseau. La technologie de navigateur sert de frontal commun pour accéder aux informations, telles que les données financières, graphiques ou textuelles.

➢ NOTION DU LAN

Les réseaux locaux permettent aux entreprises de partager localement des fichiers et des imprimantes de manière efficace et rendent possibles les communications internes. Le courrier électronique est un bon exemple de cette technologie. Les réseaux locaux gèrent les données, les communications locales et l'équipement informatique. Les réseaux locaux

comprennent les éléments suivant : Ordinateurs ; Cartes réseau ; Équipements périphériques ; Médias réseau et Équipements de réseau

Quelques technologies courantes de réseau local:

- Ethernet ;
- Token Ring ;
- FDDI.

Cependant l'intranet de la DRO/SONABEL est un réseau Ethernet, basé sur la topologie étoile. Ce réseau est obtenu par la réalisation d'un MAN de cinq sites. Dans chaque site est installé un réseau local de type Ethernet, câblés selon les normes 802.3, avec pour support la paire torsadée non blindée (UTP) de catégorie 5e.

Au niveau siège est réalisé quatre LAN logiques appelés VLAN à savoir :

- VLAN serveur ;
- VLAN Informatique ;
- VLAN Guichet ;
- VLAN DRO.

Le principe des VLAN consiste à regrouper des machines quelles que soient leur emplacement physique. Cette technologie permet de créer un regroupement logique des machines.

Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.

Cet intranet est connecté à internet via la liaison spécialisé de l'ONATEL (Office Nationale de Télécommunication).

Ces réseaux locaux sont interconnectés par la technologie BLR (Boucle Local Radio). Les sites SONABEL de la ville de BOBO-DIOULASSO abritent des réseaux locaux disposant d'une alimentation électrique sécurisée par un onduleur et un groupe électrogène.

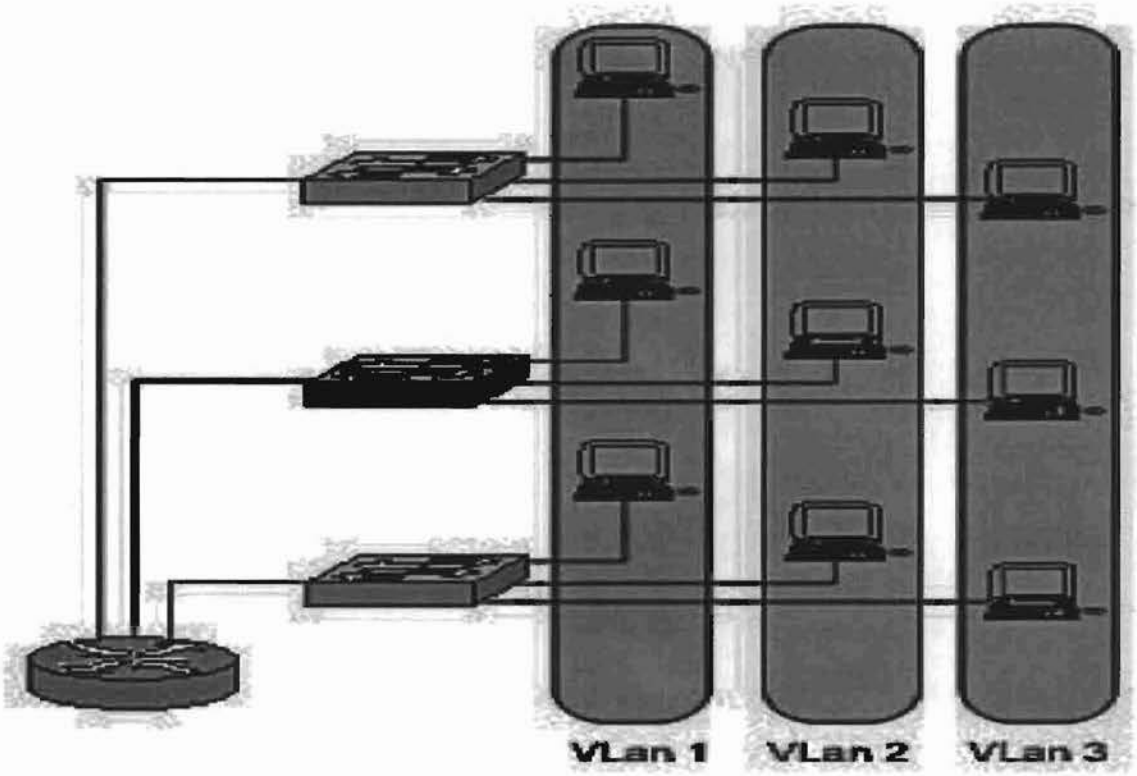


Figure 4 : Regroupement Logique des utilisateurs

II.1.3 LES RESSOURCES DE MISE EN PLACE DE L'INTRANET

II.1.3.1 LES RESSOURCES MATERIELLES

La SONABEL/Bobo dispose d'une gamme variée de matériels parmi lesquelles on trouve:

- Environ une centaine de micro-ordinateurs de marques Compaq aux écrans cathodique et des marques HP avec des écrans plats ;
- Des serveurs IBM X séries 235, 236 et 3400 pour les bases de données au siège et dans les différents centres rattachés;
- Six routeurs CISCO dont un cisco 2800 sur le site de St-Etienne, un Cisco 2800 sur le site d'Accart-ville, un Cisco 2800 sur le site de BOBO 2 et un Cisco 2800 sur le site du Dispatching et un Cisco 2800 au siège. En plus du cisco2800 du siège, il y a un Cisco 3600 ;
- Un Modem Nokia pour la liaison spécialisée au siège;
- Des Switch pour les différents LAN ou VLAN dans les différentes divisions;
- Des imprimantes pour les brouillards, les factures ordinaires et les factures doubles tarif, etc ;
- Des imprimantes ordinaires, et ou des télécopieurs pour les impressions sur papier;
- Un onduleur de 30 KVa pour la protection de l'intranet…

Le tableau ci-dessous donne un aperçu des ressources matérielles de l'intranet existant dans la ville de BOBO-DIOULASSO.

Tableau 1: Ressources matérielles de l'intranet de la ville de BOBO.

EQUIPEMENTS	CARACTERISTIQUES	QUANTITE
SERVEURS	IBM Série 235-236	03
MICRO ORDINATEURS	COMPAQ ET HP	Une centaine
MODEM		01
ROUTEUR	CISCO 2800	06
SWITCH	DLINK DES1024D 10/100Mbps 24 ports	03
HUB Switch nway	10/100Mbps 24 ports	02
IDU		05
ODU		05

II.1.3.2 LES RESSOURCES LOGICIELLES

II.1.3.2.1 LES SYSTEMES D'EXPLOITATION UTILISES

Comme systèmes d'exploitation La SONABEL/Bobo utilise les systèmes suivants :

- Linux Red Hat version 4 pour les serveurs de l'entreprise;
- Windows 98, Windows XP et Windows 7 pour les ordinateurs clients.

II.1.3.2.2 LES APPLICATIONS

Pour faciliter les tâches de comptabilités la SONABEL/Bobo dispose d'importantes ressources logicielles que nous allons noter comme suit :

- GesPha pour la gestion des frais pharmaceutique ;
- GesCli BT/MT pour la gestion de la clientèle ;
- Un système de notation et d'avancement du personnel (pour le payement du personnel) ;
- Quicken 2001 pour la comptabilité des fournisseurs ;
- Un logiciel pour la gestion des missions ;
- Oracle application 3/3 pour la production ;
- Eclipse pour les factures cash power.

Il existe des applications développées à l'interne bien sûr parmi les applications ci-dessus citées.

La gestion des bases de données est assurée par Oracle 10g et le développement par le logiciel Développer 2000.

II.1.4 PRESENTATION DE L'ARCHITECHTURE DES SITES HORS DE BOBO-DIOULASSO.

L'architecture des sites rattachés à la SONABEL/BOBO est également un réseau LAN (Local Area Network), Ethernet, basé sur la topologie étoile par l'ADSL et par clé de connexion (CDMA). Chaque LAN est de type Ethernet, câblés selon les normes 802.3, avec pour support la paire torsadée non blindée (UTP) de catégorie 5e. Les localités telles que BANFORA, GAOUA, ORODARA et DIEBOUGOU utilisent l'ADSL et les localités telles que DANO, DISSIN, HOUNDE et NIANGOLOKO utilisent le CDMA pour avoir accès à l'internet. Il faut aussi préciser que les localités que nous venons d'énumérer disposent chacune d'un serveur et comportent des villes ou villages satellitaires qui aussi disposent de leur serveur (des ordinateurs juste pour l'enregistrement des payements juste pour les jours de marchés pour les villages).

Le tableau ci-dessous vous donne un aperçu sur les villes disposant d'un serveur et les villages satellitaires ainsi que le nombre de poste utilisés par localité.

Tableau 2 : Les sites hors de la ville de Bobo-Dioulasso et leur existant.

LOCALITES	Technologie d'interconnexion	NOMBRDE DE POSTES
BANFORA	ADSL	08
DANO	Clé de connexion	03
DIEBOUGOU	ADSL	02
DISSIN	Clé de connexion	01
GAOUA	ADSL	04
HOUNDE	Clé de connexion	03
NIANGOLOKO	Clé de connexion	02
ORODARA	ADSL	03

Le tableau ci-dessous donne un aperçu sur les centres serveurs et leurs villages satellitaires

Tableau 3: Les localités avec server et leurs villages satellitaires.

LOCALITE AVEC SERVEURS	LOCALITES SATELLITAIRES ET DISTANCES PAR RAPPORT AU SERVEUR
BANFORA	BEREGADOUGOU / 15 km
	SIDERA /30 km
	TOUSIANA / 25 km
	TIEFORA /30 km
DANO	FOUNZA/25 km
	ORONKWA /35 km
GAOUA	BOUFFOUN-BOUFOUN/30 km
ORODARA	TOURNI /25 km
HOUNDE	KOUMBIA / 33 km
	BONI/30 km
	PA /30 km
DIEBOUGOU	HAMELE/ WESSA
	DISSINE /33 km

NIANGOLOKO	KOUTOURA /10 km
	SINIENA /15 km
	DIARABAKOKO /20 km
BOBO	MATROUKOU /10 km
	DARSALAMI /13 km DE BOBO
	PENI 40 km

II.2 CRITIQUE

Apres une analyse objective de l'intranet de la SONABEL/BOBO, on peut apporter des appréciations dans son installation matérielle. L'environnement serveur est assuré par deux serveurs à savoir un serveur de données et un serveur de sauvegarde ; les deux configuré selon la technologie RAID de niveau 5. Cependant sa connexion à internet est vraiment limitée à un débit de 512 kb/s pour tous les sites de la ville de BOBO. Par conséquent son exploitation est relativement restreinte si bien qu'on ne peut pas l'utiliser pour les téléchargements pour les fins de simulation. Le but du projet est d'interconnecté les différents centres rattachés permettant à la DRO de fournir les outils et les informations nécessaires à ces différents centre pour accroitre son activité et facilité le retour d'information de ses centres et de suspendre certains coût.

PARTIE II : PROBLEMATIQUE

La résolution d'un problème passe sans doute par sa compréhension. Cette partie énonce clairement le problème tel que posé à notre arrivée en entreprise, l'explique de façon schématique et présente les données à étudier.

CHAPITRE I

SCHEMATISATION DU PROBLEME ENONCE

I.1 DEROULEMENT DU STAGE

La journée de travail commence à 7h30 et se termine à 18h00 avec une pause de 12h à 15h. A la SONABEL/BOBO les activités techniques sont nombreuses parmi lesquelles on cite les tâches de maintenance logiciel et dépannages des ordinateurs, d'installation de logiciels d'application et d'exploitation ; d'installation et de configuration en réseau des imprimantes, l'installation et la configuration d'un nouveau matériel tel les ordinateurs de bureau.

I.2 ENONCE DU PROBLEME

La SONABEL voit le nombre des sites évolué de façon significative. Il devient nécessaire de mettre de nouvelles technologies en place.

La DRO/SONABEL d'aujourd'hui ne dispose pas d'un moyen réseau informatique permettant de partager et de réunir les informations en temps réel. Le partage des fichiers se fait traditionnellement par des agents de liaison en d'autres termes, les données sont collectées dans des clés USB pour être expédier et sauvegarder au niveau du serveur central qui se trouve dans la ville de BOBO.

La SONABEL/BOBO nous recommande de travailler sur le thème et de trouver une technique d'interconnexion qui réussira à centraliser la base de données afin que le client soit à mesure de régler sa facture d'électricité partout où il se trouve dans la région et que cette solution réduise du même coût les risques de pertes de données et de traitement multiples; tenant compte des aspects tels l'aspect fiabilité, l'aspect sécuritaire et l'aspect coût de celle-ci.

I.3 SCHEMA DU PROBLEME

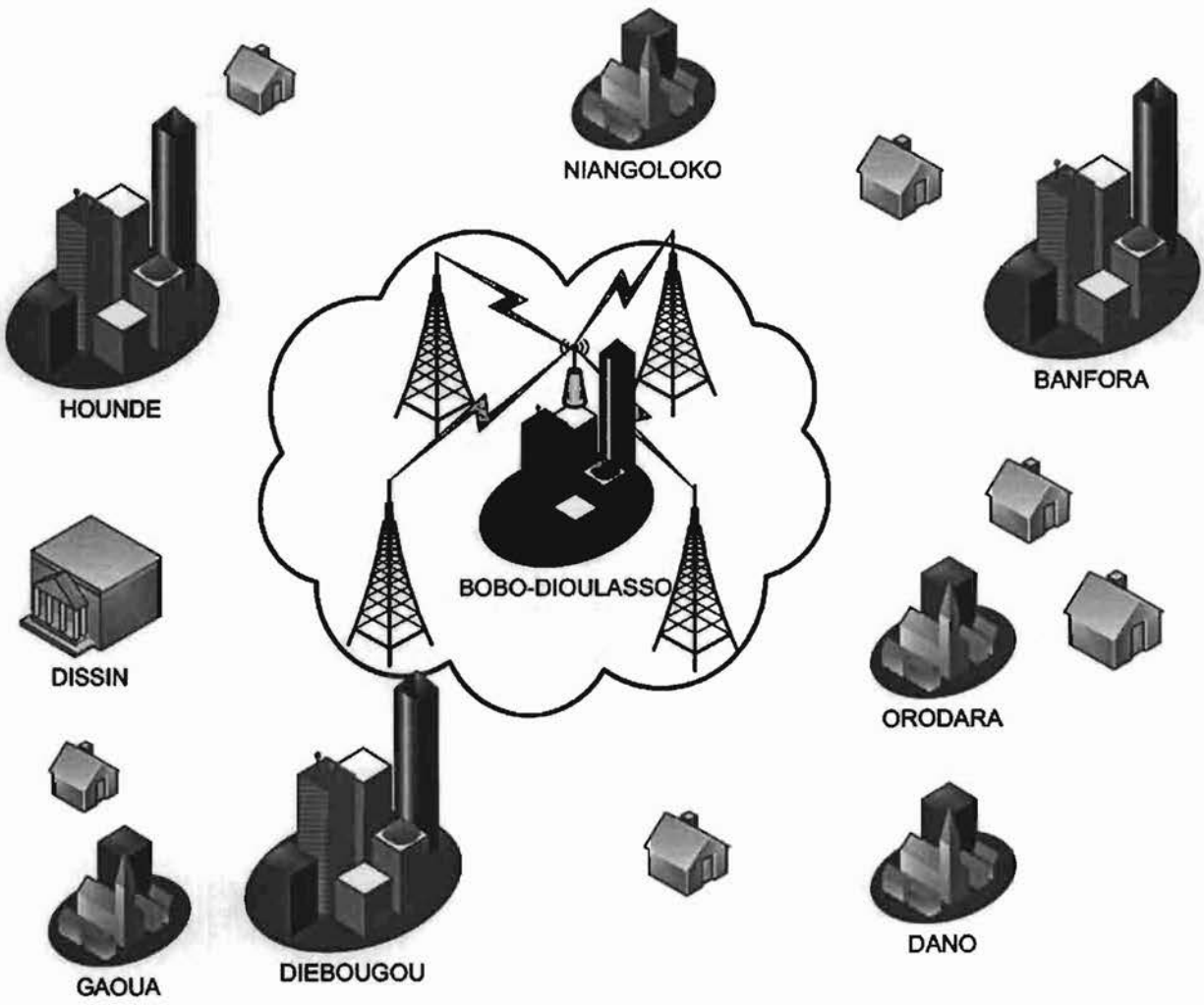


Figure 5 : Schéma du problème

TROISIEME PARTIE: LES TECHNOLOGIES D'INTERCONNEXION POSSIBLES

La partie précédente a consisté à dégager la préoccupation principale de nos travaux et les différentes questions qui s'y rattachent. Nous Vous proposons dans cette section d'étudier les différentes technologies envisageables.

CHAPITRE I

LA FIBRE OPTIQUE

I.1 DEFINITION

La fibre optique est un fil en verre ou en plastique très fin qui a la propriété de conduire de la lumière et sert dans les transmissions aériennes, terrestres et océaniques de données. Elle offre un débit d'informations nettement supérieur à celui des câbles coaxiaux et supporte un réseau large bande par lequel peuvent transiter aussi bien la télévision, le téléphone, la visioconférence ou les données informatiques.

I.2 PRINCIPE DE FONCTIONNEMENT

À la base une fibre optique est un guide-onde. C'est donc l'onde qui se propage dans la fibre optique qui est modulée pour contenir une information. Le signal lumineux est codé en variation d'intensité. Pour les courtes distances, et une optique à bas coût, une simple DEL peut jouer le rôle de source émettrice tandis que sur des réseaux hauts débits et à longue distance, c'est un laser qui est de préférence utilisé. Il existe principalement deux types de fibres optiques :

- **Les fibres plastiques**, en polystyrène (PS) ou en poly méthacrylate de méthyle (PMMA), sont économiques, légères et souples, mais leur atténuation est élevée ; on les utilise surtout pour les transmissions à courte distance.

- **Les fibres silice-silicone** sont constituées d'un cœur de silice pure et d'une gaine de silicone. Elles présentent une faible atténuation, mais sont plus rigides et plus onéreuses que les fibres plastiques et sont utilisées pour les transmissions longue distance.

Lorsqu'un rayon lumineux entre dans une fibre optique à l'une de ses extrémités avec un angle adéquat, il subit de multiples réflexions totales internes. Ce rayon se propage alors jusqu'à l'autre extrémité de la fibre optique sans perte, en empruntant un parcours en zigzag. La propagation de la lumière dans la fibre peut se faire avec très peu de pertes même lorsque la fibre est courbée.

I.3 LES DIFFERENTES CATEGORIES DE FIBRE OPTIQUE

On peut distinguer deux catégories de fibres optiques selon le diamètre de leur cœur et la longueur d'onde utilisée:

- Les fibres optiques multimodes, les premières sur le marché, les fibres multimodes ont pour caractéristiques de transporter plusieurs modes (trajets lumineux). Elles sont caractérisées par un diamètre de cœur de plusieurs dizaines à plusieurs centaines de micromètres et permettent d'atteindre le Gbit/s sur des distances de l'ordre du km. Elles sont réservées aux réseaux informatiques à courtes distances.

Dans cette famille, nous trouvons deux sous catégories:

a)La fibre multimode à saut d'indice ;

b) La fibre multimode à gradient d'indice.

- La fibre optique monomode c'est le top. Pour de plus longues distances et/ ou de plus hauts débits, on préfère utiliser des fibres monomodes (dites SMF, pour Single Mode Fiber), qui sont technologiquement plus avancées car plus fines. Leur cœur très fin n'admet ainsi qu'un mode de propagation, le plus direct possible c'est-à-dire dans l'axe de la fibre. Elles sont installées pour les réseaux à très longues distances tel que les lignes intercontinentales. Il n'y a pas de miracle, c'est la solution la meilleure, mais aussi la plus onéreuse.

I .4 AVANTAGES ET INCONVENIENTS DE LA FIBRE OPTIQUE

LES AVANTAGES

- Débit très élevé, d'une grosse centaine de Mégas bit par seconde : 10,2 Tbit/s (10 200 Gbit/s), sur une distance de 100 kilomètres ;
- Transmission longue distance ;
- Sécurité élevée ;
- Durée de vie de la fibre est de 20 ans, ce qui représente une valeur sûre, durable et économique pour les entreprises ;
- Insensibilité aux interférences extérieures.

LES INCONVENIENTS

- Coût de déploiement élevé. La fibre optique, par apport au câble en cuivre coûte moins cher. En revanche, la connectique et les convertisseurs d'énergie électrique/lumineuse et réciproquement à placer aux extrémités coûtent cher, très cher même, suivant les technologies mises en œuvre;
- La silice qui est le matériau au centre de la fibre est fragile. Il est important que cette silice soit bien protégée ;
- Maintenance difficile.

La fibre optique représente assurément le meilleur moyen actuel pour transporter de très hauts débits d'informations numériques, et les besoins dans ce domaine vont probablement augmenter très fortement dans un avenir proche. Est-ce que la politique financière de la SONABEL/BOBO lui permet-elle de supporter le coût de mise en œuvre d'une telle architecture réseau à base de fibre optique ? Assurément pas. Passons à la deuxième possibilité d'interconnexion qui est notre chapitre suivant.

CHAPITRE II

LIAISON SPECIALISEE ET VPN

II.1 LIAISON SPECIALISEE

Les lignes louées ou spécialisées permettent la transmission de données à moyens et hauts débits (2,4 Kbps à 140 Mbps) en liaison point à point ou multipoints (service Transfix). La ligne spécialisée est tirée directement entre les locaux du client et le fournisseur d'accès. Au Burkina Faso le débit d'une liaison varie entre 64Kb/s et 2Mb/s et le coût est fonction du débit demandé.

II.2 AVANTAGES ET INCONVENIENTS DE LA LS

➢ AVANTAGES

- C'est une liaison qui offre des débits de connexion symétriques, garantis en émission et en réception de données et allant de 64 Kbpsjusqu'à des dizaines de Mbps ;

- Par le biais d'un canal unique exclusivement réservé à votre entreprise, une liaison spécialisée vous offre la possibilité d'échanger tous types de données ;
- Toutes vos communications sont sécurisées et offrent ainsi une fiabilité et une confidentialité totales.

➢ INCONVENIENTS

- Cette solution est dépendante de L'ONATEL ;
- Au Burkina L'ONATEL fournit une connexion instable et le coût de la redevance mensuelle est très élevé : 472.000 F pour les frais d'accès et 1.180.000 F pour la redevance mensuelle d'un débit de 1 Mb/s.

II.3 VIRTUAL PRIVATE NETWORK (VPN)

Le but de la solution VPN (Virtual Private Network) est de pouvoir faire communiquer à distance les employés distants et partenaires de l'entreprise de façon confidentielle, et ceci en utilisant internet. Il s'agit de créer un canal de communication protégé traversant un espace public non protégé. Chacun des membres du réseau VPN peut être un réseau local (LAN) ou un ordinateur individuel.

Un VPN fonctionne en encapsulant les données d'un réseau à l'intérieur d'un paquet IP ordinaire et en le transportant vers un autre réseau. Quand le paquet arrive au réseau de destination, il est décapsulé et délivré à la machine approprié de ce réseau. En encapsulant les données et en utilisant les techniques de cryptographie, les données sont protégées de l'écoute et de modification pendant leur transport au travers du réseau public.

II.4 AVANTAGES ET INCONVENIENTS DU VPN

➢ AVANTAGES

- Favorise l'évolutivité et offre de vastes possibilités grâce à l'internet. Le VPN permet l'ouverture du réseau selon les besoins ou les nécessités, en y ajoutant une grande souplesse et une grande réactivité ;
- Réduction des ressources humaines et financières de l'entreprise affectées à l'utilisation du VPN. D'où une baisse du coût global, en particulier pour les entreprises possédant un réseau avec une configuration complexe ;
- Solution très avantageuse économiquement parlant. Internet VPN a été conçu pour relier à un moindre cout les employés distants et les partenaires de l'entreprise, puisque l'entreprise ne paye que l'accès à internet.
- Solution sécurisée puisque le VPN est un réseau privé reposant sur deux éléments :

L'authentification et l'encryptage.

➢ **INCONVENIENTS**

- Le VPN doit être établit entre chaque station. En effet une station ne possédant pas l'application VPN ne pourra pas communiquer avec les autres, et la sécurisation entre cette station et l'entrée du VPN ne sera pas activée. Pour les clients nomades, il faut installer un logiciel sur les pc portable et maintenir le parc à niveau de régulière. Il faut savoir plus le nombre de sites est important, plus la stabilité de la solution s'amoindrie et plus le VPN est lourd à déployer ;
- Désavantages liés à l'encryptage généré par le VPN : le branchement est légèrement plus lent, l'ordinateur consomme plus ressource, et il faut ajouter une étape pour se brancher au point de destination ;
- Nécessité de respecter les règlementations nationales en vigueur sur le chiffrement, sans compter que la gestion des clés est assez complexe. De même, la qualité des services est difficilement gérable et la mise en place du QoS est très limitée ;
- Coût des passerelles VPN relativement élevé. En effet, le matériel nécessaire à la mise en place de VPN est relativement cher, même si par la suite cette solution permet à l'entreprise de nombreuses économies tant dans la gestion que dans la maintenance du réseau VPN.

CHAPITRE III

INTERCONNEXION PAR VSAT

III.1 DEFINITION

Un satellite de télécommunications est un engin spatial en orbite autour de la Terre, qui assure des communications à distance en relayant des signaux par ondes radio, entre deux ou plusieurs stations terrestres dotées d'antenne VSAT (Very Small Aperture Terminal), qui est un terminal d'émission/réception généralement équipé d'une antenne de 1 à 3,7 m. Il peut gérer, au niveau réseau, des applications haut débit pouvant atteindre des vitesses de transmission de 20 Mbps en voie descendante et de 76,8 Kbps en voie montante. Les réseaux VSAT relient les entreprises à leur maison mère, des magasins de distribution avec leurs grossistes et les institutions financières à leurs agences. Au milieu des années quatre-vingt, ils ont initialement été utilisés par les grands groupes pour la transmission de leurs services voix, données et vidéo. Depuis quelques années, les petites entreprises et les particuliers ont rejoint les légions d'acheteurs de petites stations terrestres. Avec les réseaux VSAT, pas de numéro à composer, pas de délai d'attente, pas d'interruptions. L'accès est immédiat, et la qualité de la communication garantie. Et comme ils sont adaptés à n'importe quel type de transmission (données, voix, télécopie ou vidéo), ils offrent la souplesse opérationnelle voulue pour tous transferts d'information, avec une installation très simple.

III.2 NATURE DES EQUIPEMENTS

III.2.1 DANS L'ESPACE

Un satellite de télécommunications comprend une plate-forme qui gère le contrôle thermique, l'alimentation électrique et la stabilité, cette dernière étant assurée par des propulseurs à poudre. Il comporte également une charge utile, composée d'antennes et de dispositifs électroniques. Des batteries, ainsi que des cellules à énergie solaire montées sur de grands panneaux fixés au satellite, alimentent les différents équipements. Afin d'éviter les interférences, les signaux captés sont réémis sur une fréquence différente, en général plus basse. Ce changement de fréquence entre les antennes de réception et d'émission est assuré par des appareils appelés répéteurs, chargés également d'amplifier massivement le signal.

III.2.2 SUR TERRE

Un système complet de télécommunications par satellites comporte un certain nombre d'équipements au sol tel que : un Hub central pour la station terrestre principale; une ou plusieurs antennes VSAT pour les stations distantes; une tête satellite contenant un système électronique pour gérer les signaux en émission et en réception; un boîtier intérieur pour gérer les connexions entre les équipements. D'une part, il possède, comme pour tout satellite artificiel, des stations de poursuite, de télémesure et de télécommande qui contrôlent le suivi de la trajectoire. D'autre part, il est doté de stations d'émission qui assurent les liaisons montantes vers le satellite, et de stations de réception qui établissent les liaisons descendantes;

de manière générale, les stations jouent les deux rôles simultanément (antenne satellite VSAT).

Le schéma de principe ci-dessous illustre de manière simple le fonctionnement d'une architecture réseau basé sur la technologie VSAT.

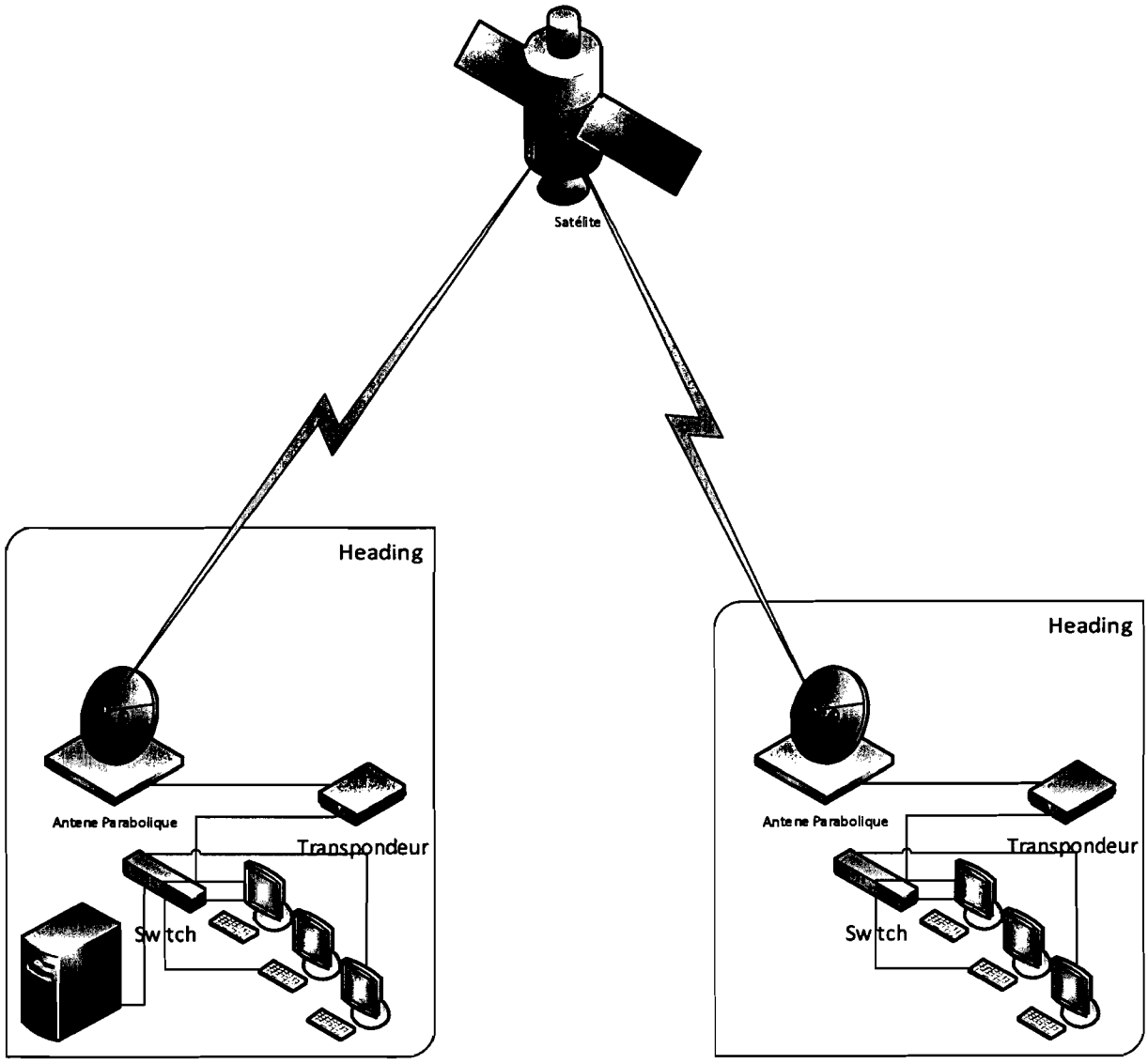


Figure 6 : Schéma illustratif du VSAT

III.3 AVANTAGES ET INCONVENIENTS

- **LES AVANTAGES**
- ❖ Très grande surface de couverture ;
- ❖ Le VSAT est un système qui permet de connectés 1.000 points simultanément ;
- ❖ Couverture des sites isolés (îles, bateaux…) ;

- ❖ Couverture des zones géographiques dépourvues d'infrastructures (forêt équatoriale…).

➢ **LES INCONVENIENTS**

- ❖ Durée de vie restreinte (car leurs propulseurs de stabilité ont une réserve en carburant limitée) ;
- ❖ Le hub qui est l'élément central du réseau impose un investissement de base important: environ 1 M€ soit 655millions FCFA ;
- ❖ Coût du déploiement très élevé.

Au vu de cette étude nous pouvons dire que cette solution ne saurait être prise en compte financièrement par l'entreprise SONABEL pour cause de son cout de déploiement très élevé.

CHAPITRE IV

LA BOUCLE LOCALE RADIO (BLR) ET LE WIMAX

IV.1 BOUCLE LOCALE RADIO

La boucle locale correspond à l'ensemble des moyens mis en œuvre par un opérateur pour collecter le trafic des utilisateurs. Une définition plus restrictive limite l'utilisation du terme « boucle locale » au seul câble de raccordement usager/réseau. Pour des raisons historiques, l'infrastructure du réseau de boucle locale correspond à celle de la distribution des services voix. Cette infrastructure est aujourd'hui partagée entre les accès aux réseaux voix et les accès aux réseaux de données.

IV.1.1 PRINCIPE DE FONCTIONNEMENT

La boucle locale radio est un moyen pour un opérateur de télécommunication de relier directement l'abonné à ses équipements en passant par une liaison radio (faisceau hertzien) au lieu d'utiliser les fils de cuivre. La B.L.R. est une technologie de connexion sans fil, fixe et bidirectionnelle:

- sans fil: utilise des ondes radio comme moyen de transmission ;
- fixe: le récepteur doit être fixe, il ne peut être mobile comme dans le cas du GSM ;
- bidirectionnelle: la liaison se fait dans les deux sens opérateur-client et client-opérateur.

  Les avantages de la B.L.R. sont nombreux. On peut citer la rapidité d'être "raccordé", le coût de raccordement moins élevé (pas besoin de travaux pour installer de la filaire). Concrètement, une connexion par B.L.R. nécessite chez le client une petite antenne plate visant directement ou non (selon la bande de fréquence et la technologie utilisées) l'antenne de l'opérateur, appelée station de base. Ensuite un câble relie l'antenne à un boîtier sur lequel se trouvent différents connecteurs: prises téléphoniques, alimentation électrique. On peut connecter un modem ou un routeur RNIS sur l'une des prises téléphoniques pour obtenir une connexion à internet en utilisant la B.L.R. WLL est l'équivalent aux Etats-Unis et en Australie, il signifie « Wireless Local Loop ».

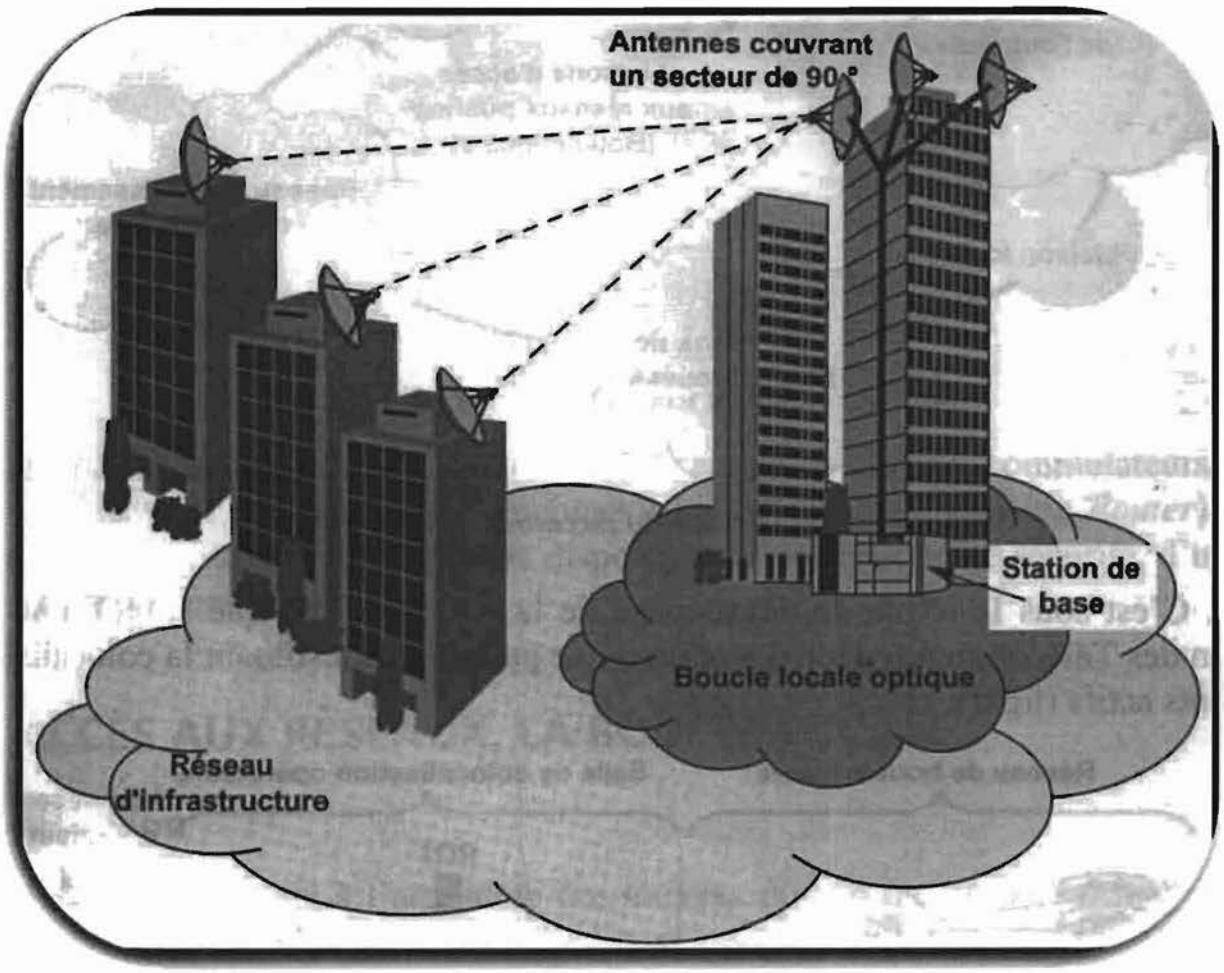


Figure 7 : Représentation de la BLR

IV.1.2 AVANTAGES ET INCONVENIENTS

➢ **AVANTAGES**

- débit constant : chaque internaute dispose de son propre canal de communication ;
- connexion permanente ;
- raccordement provisoires et rapides possibles (expositions, catastrophes,...) ;
- l'opérateur évite d'avoir à tirer une ligne de cuivre du commutateur d'abonnés jusqu'au foyer de l'abonné (économie de coût, pas de travaux de génie civil) ;
- facilité, flexibilité et rapidité du déploiement du réseau (pas de travaux génie civil,) ;
- coûts d'infrastructure et de fonctionnement moins élevés, proportionnels et progressifs ;
- parfaitement adapté aux régions rurales, à faible densité de population ou la desserte des zones reculées (dans les pays à faible taux de pénétration téléphonique).

➢ **INCONVENIENTS**

- sensibilité aux conditions météorologiques : chute de débit de 30% ;
- nécessité de vue directe entre les antennes (20-40% des habitations situées dans des zones d'ombres ne seraient pas couvertes) ;
- les signaux ne peuvent pas traverser les obstacles entre les antennes émettrices et réceptrices.

IV.2 Le WIMAX

WIMAX est abbreviation pours Worldwide Interoperability for Microwave Access. Il s'agit d'un standard de réseau sans fil métropolitain créé par les sociétés Intel et Alvarion en 2002 et ratifié par l'IEEE Institute (Institue of Electrical and Electronics Engineer) sous le nom IEEE- 802.16. Plus exactement, WIMAX est le label commercial délivré par le WiMax Forum aux équipements conformes à la norme IEEE 802.16, afin de garantir un haut niveau d'interopérabilité entre ces différents équipements. Ainsi il permet d'obtenir des débits montants et descendants de 70 Mbit/s avec une portée de 50 Km.

IV.2.1 FONCTIONNEMENT

Le fonctionnement d'un réseau WIMAX est principalement basé sur la communication entre les stations de base (Base Transceiver Station ou BTS) et les divers équipements certifiés WiMax qui y sont reliés. Les stations de base correspondent aux antennes placées sur les points hauts de la ville et à tous les équipements qui y sont reliés, chargés d'émettre et de recevoir les données sous forme d'ondes radio. La station de base est reliée au centre de l'opérateur et prend en charge les transmissions avec les abonnés. Chez le client, une petite antenne doit être placée sur le toit du domicile et orientée vers la station de base (LOS). Celle-ci est reliée par un câble à un boîtier périphérique de l'ordinateur, qui joue le rôle d'interface et d'alimentation de l'ODU (Out Door Unit). Les évolutions technologiques permettent désormais de connecter des antennes clients sans que celles-ci ne soient en vue des stations de base (NLOS). La figure illustre clairement le principe de fonctionnement du WIMAX.

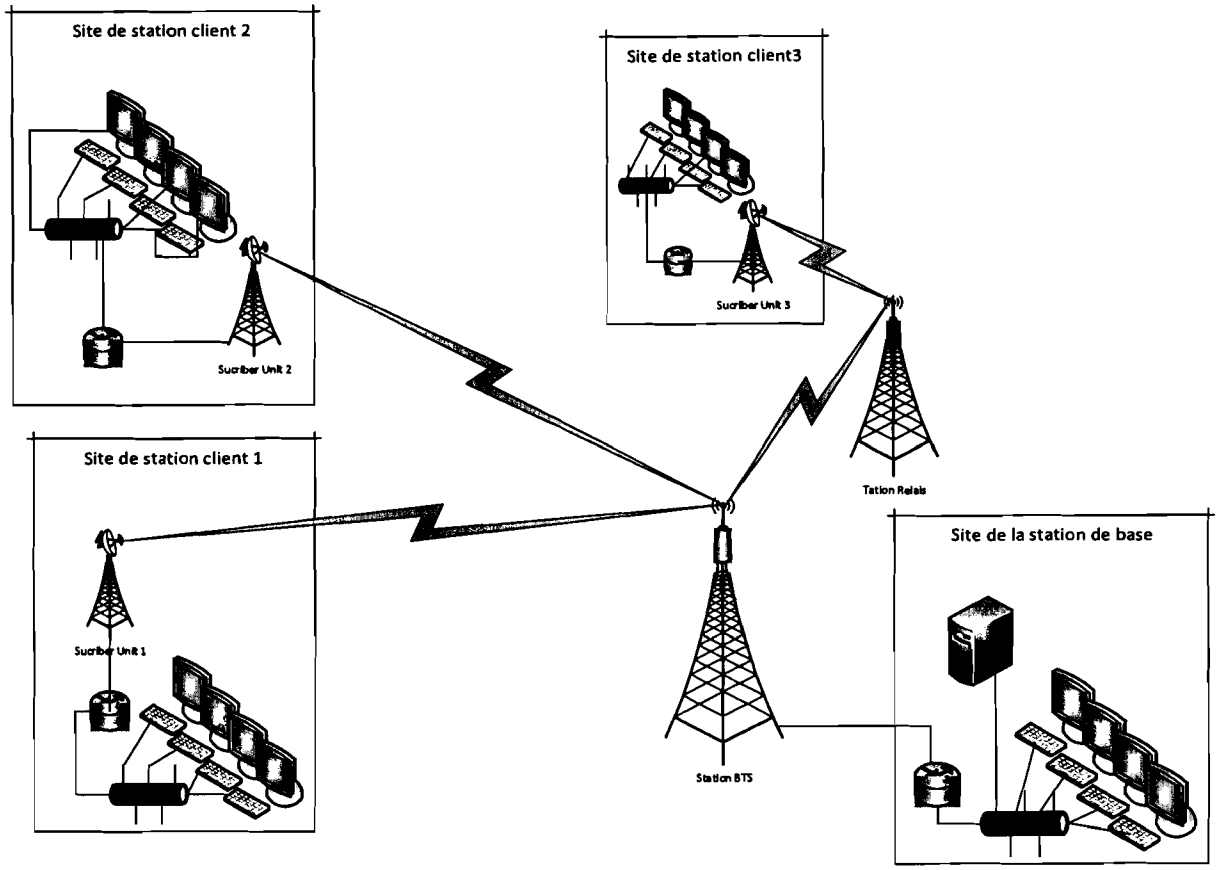


Figure 8: Représentation du WIMAX

IV.2.2 AVANTAGES ET INCONVENIENTS DU WIMAX

➢ LES AVANTAGES :

- Facilité de mise en œuvre ;
- Large zone de couverture ;
- Facilité de maintenance et d'administration ;
- Possibilité d'investissement progressif en fonction de la demande ;
- Faible coût de déploiement par rapport au réseau filaire.

➢ LES INCONVENIENTS :

- Faible tolérance aux perturbations en milieu urbain;
- Sensibilité aux conditions météorologiques ;
- Nécessité de disposer d'un point haut.

L'investissement de départ d'un WIMAX est important, essentiellement du côté du fournisseur qui développer son réseau d'antenne afin de couvrir un territoire le plus large

possible. En plus il y'a des équipements qui ne suivent pas la technologie (antennes sur laptop pas assez puissantes).

En réalité, le WIMAX ne pourra franchir que de petits obstacles comme un arbre ou une maison mais le signal est incapable de passer au travers de collines ou d'immeubles importants. Le débit en présence d'obstacle est fortement diminué (on parle de 20 Mbit/s/sec).

Après une étude des différentes solutions possibles, le tableau nous donne une synthèse sur ces solutions.

Tableau 4: Comparaisons des solutions possible.

Solution	Fibre Optique	LS	VPN	BLR	VSAT	WIMAX
Autonomie	OUI	NON	NON	OUI	NON	OUI
Coût	Très élevé	Moyen	Moyen	Moyen	Elevé	Moyen
Implantation	Complexe	Facile	Facile	Facile	Facile	Facile
Durée D'implantions	Très élevée	Peu élevée	Peu élevée	Assez élevée	Peu élevée	Assez élevée

IV.3 SOLUTIONS CHOISIES

Au regard de toutes ces solutions qui se présentent, il nous appartient d'opérer un choix judicieux et optimal pour l'interconnexion des sites de la région de l'ouest. Ainsi pour respecter l'objectif recherché, nous nous sommes donnés à une solution hétérogène. Après l'analyse des différentes solutions, le tableau précédent nous permet de choisir : Le VPN et Le WIMAX.

QUATRIEME PARTIE: ETUDE ET MISE EN ŒUVRE DES SOLUTIONS CHOISIES

La partie précédente a mis en relief les différentes possibilités envisageables pour interconnecter les sites de la direction régionale de la SONABEL. Au regard du problème posé, nous sommes en obligation de faire une proposition de solution hétérogène afin de lever avec succès les soucis de la DRO/SONABEL. Par conséquent nous proposons une solution qui prend en compte de manière simple la mise en œuvre d'une technologie WIMAX et d'un réseau VPN.

CHAPITRE I

PRESENTATION GENERALE DU VPN

I.1 DEFINITION

Le terme VPN (Virtual Private Network) ou réseau privé virtuel, est devenu un terme courant dans l'informatique d'entreprise et le domaine des réseaux. Néanmoins, beaucoup de petites entreprises ont du mal à comprendre le concept et le bénéfice que cela peut leurs apporter.

La méthode la plus simple pour définir un VPN est de simplement décomposer l'expression comme suit :

Network : C'est un réseau, qui peut être constitué de plusieurs machines pouvant communiquer entre elles d'une façon ou d'une autre. Ces machines peuvent être dans un même endroit physiquement ou non et les méthodes de communication sont diverses.

Privat : pour privé cela veut dire que les communications entre deux ou plusieurs machines sont secrètes. Ainsi, une machine ne participant pas à la communication privée ne saura même pas que celle-ci a lieu.

Virtual : Le concept de virtuel est un peu plus compliqué à définir. Ce terme est souvent utilisé pour parler d'objet artificiel par exemple la mémoire virtuelle opposée à la mémoire physique d'un ordinateur ; en d'autre terme c'est l'émulation de la fonction d'un objet qui n'est pas vraiment là.

En combinant ces termes, on comprend que le VPN est un réseau privé obtenu en émulant, une fonction à l'opposé d'un réseau rendu par câblage direct entre les différentes machines. Les termes ci-dessus nous permettent de définir le concept de VPN comme étant un réseau privé construit au sein d'une infrastructure informatique public, telle qu'internet.

I.2 PRINCIPE DE FONCTIONNEMENT

Le VPN repose sur un protocole appelé «protocole de tunneling », c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre en toute sécurité grâce à des algorithmes de cryptographie. On emploie le terme « tunnel » pour symboliser le fait que les données soient cryptées et de ce fait incompréhensible pour tous les autres utilisateurs du réseau public (ceux qui ne se trouvent pas aux extrémités du VPN). Ainsi les utilisateurs ont l'impression d'être connecter directement sur le réseau de leur entreprise. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de

l'organisation. De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffré es, puis transmises à l'utilisateur. Pour émuler une liaison point à point, les données sont encapsulées, ou enrobées, à l'aide d'un en-tête qui contient les informations de routage pour leur permettre de traverser le réseau partagé ou public jusqu'à leur destination finale. Le principe de tunneling consiste donc à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les données à transmettre peuvent être prises en charge par un protocole différent du protocole IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête.

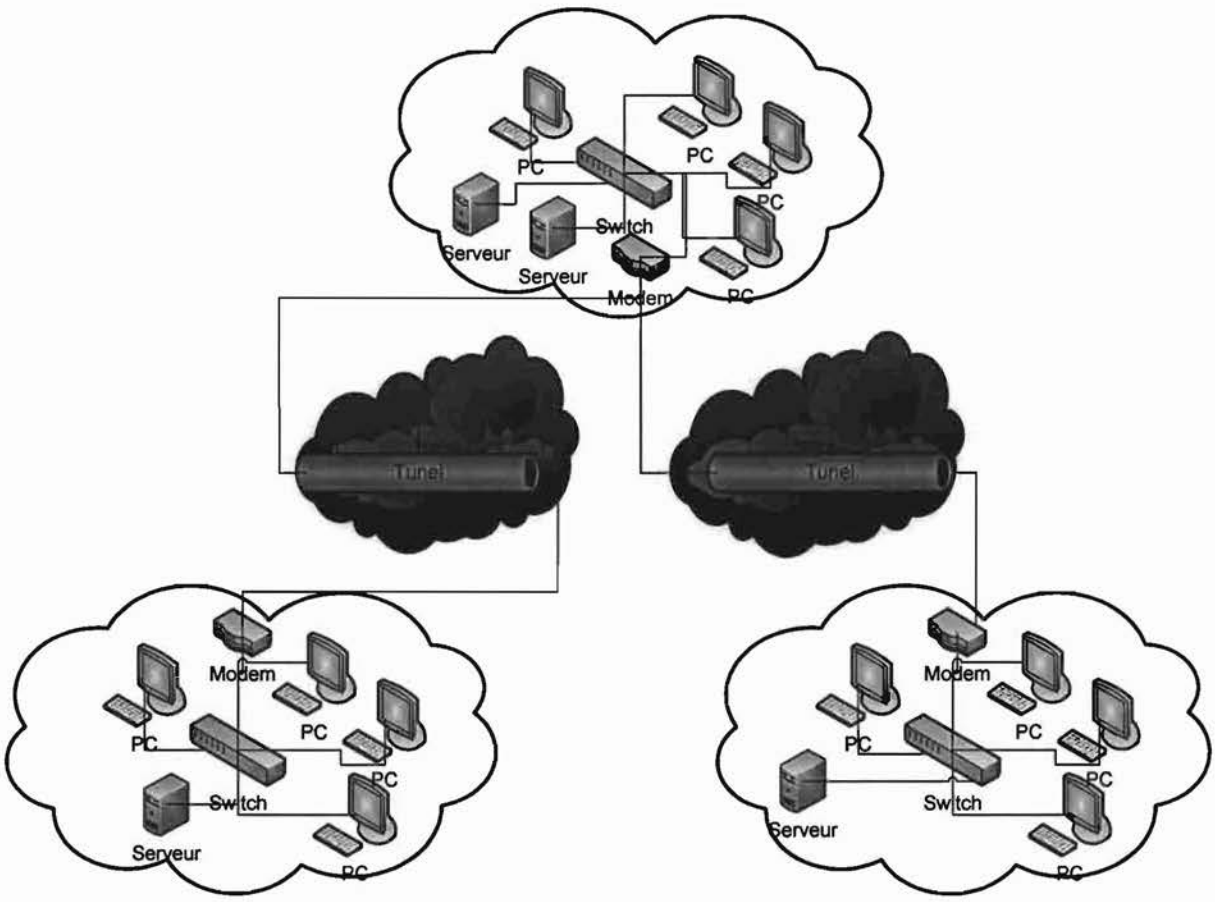


Figure 9 : Schéma de Principe

Le tunneling est un ensemble de processus d'encapsulation (la charge utile est mise dans un en-tête supplémentaire), de transmission (acheminement des paquets par un réseau intermédiaire) et de desencapsulation (récupération de la charge utile). Pour des besoins de facilité d'administration et de configuration de la solution, nous nous s'orienterons vers une architecture centralisée, où les différents points VPN se relient à un site central, pour lequel il faudra augmenter le débit de la ligne. Dans le cas d'un site éclaté, des ajustements peuvent

être faits en termes de débits mais le nombre d'équipements et la complexité de l'administration augmente au fur et à mesure que les liens VPN se multiplient.

I.3 CARACTERISTIQUES D'UN VPN

Le VPN est une généralisation du concept de tunnel. Il s'agit de faire circuler dans le tunnel non seulement les informations des applications, mais également tout ce qui concerne les couches réseau et transport. En effet, on crée un nouveau réseau à l'intérieur du tunnel. Vous imaginerez facilement les avantages d'un VPN en considérant 2 réseaux locaux ayant besoin d'être reliés via un réseau peu sûr comme internet. Les 2 LAN se relient par un tunnel traversant Iternet et formant un nouveau LAN virtuel et sûr : le VPN.

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Son principe est celui d'être transparent pour les utilisateurs et pour les applications ayant accès. Il se caractérise par les fonctionnalités suivantes :

Authentification des entités communicantes: le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa ;

Authentification des utilisateurs : seules les personnes autorisées doivent y accédés ;

Gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveaux clients en obtenir une facilement. Cette adresse privée doit rester confidentielle ;

Cryptage des données: les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa ;

Gestion des clés: les clés de cryptage pour le client et le server doivent être générées et régénérées souvent (automatiquement) ;

Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux public en particulier IP fin a de réaliser un vrai tunnel comme s'il y'avait réellement un câble entre les deux réseaux.

Le VPN est un principe, un concept : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

I.4 INTERET D'UN RESEAU VPN

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local. Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail et SONABEL/BOBO ne faillira pas à la tradition et aspire à une extension de son réseau local. On peut facilement imaginer un grand nombre d'applications possibles.

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades ;
- Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante ;
- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet ;
- Les connexions VPN permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée ;
- Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante.

Il n'en demeure pas moins qu'un VPN présente des limites parmi lesquelles : la connexion internet qui en plus d'être un avantage économique pour les entreprises dans le sens où elle lui évite des coûts liées à la ligne dédié ; mais sans elle le VPN n'est pas possible. La connexion doit à tout moment être disponible pour les utilisateurs et entreprises utilisant cette technologie.

I.5 LES DIFFERENTS TYPES DE VPN

On peut dénombrer deux grands types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie :

I.5.1 LE VPN D'ACCES

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée. Il existe deux cas :

L'utilisateur demande au FAI de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du FAI.

L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune des avantages et des inconvénients :

La première méthode permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un FAI proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée; ce qui peut poser des problèmes.

La deuxième méthode permet de résoudre ce problème puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel lui permettant d'établir une communication cryptée. Nous verrons que pour pallier à ce problème, certaines entreprises mettent en place des VPN à base de SSL (Secure Socket Layer), technologie implémentée dans la majorité des navigateurs internet du marché. Quel que soit la méthode de connexion utilisée, ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification login/mot de passe, par un algorithme dit Tokens sécurisés (utilisation de mots de passe aléatoires) ou par certificats numériques.

I.5.2 LE VPN LAN TO LAN

Ici on a deux sous-catégories :

L'EXTRANET VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors une partie de son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seule une partie des ressources sera partagée, ce qui nécessite une gestion des espaces d'échange.

L'INTRANET VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données client, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source, ainsi que leur non répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutés aux paquets. La confidentialité des données est elle aussi basée sur des algorithmes de cryptographie.

CHAPITRE II

SECURISATION D'UN VPN

Lors de l'utilisation de serveurs VPN sur un réseau, il est conseillé de s'attarder de façon rigoureuse sur la sécurité. Pour éviter d'être exposé aux différentes attaques des hackers. Le VPN utilise un ensemble de technologies pour sécuriser les données qui voyagent d'un bout à l'autre d'internet. Les concepts les plus importants sont ceux de firewall, d'authentification, protocole de tunnels et du chiffrement de données que nous allons présenter.

II.1 LES FIREWALLS

Un firewall (pare-feu) internet a le même but qu'une porte coupe-feu dans un immeuble : protéger une certaine zone de l'avancée des flammes ou d'une explosion qu'elles pourraient engendrer. L'avancée des flammes dans un immeuble est contrôlée en plaçant de solides murs à des endroits stratégiques qui aident à contenir les flammes et à réduire les dégâts occasionnés. Un pare-feu Internet a le même rôle en utilisant des techniques telles que l'examen de l'adresse IP du paquet qu'il reçoit ou le port sur lequel arrive une connexion il décide de laisser passer ou de bloquer le trafic entrant.

Bien que le VPN n'implémente pas de firewall standard par défaut, les pare-feu font partie intégrante d'un VPN. L'idée est qu'ils doivent être utilisés pour garder les utilisateurs non désirables hors du réseau tout en acceptant les utilisateurs du VPN. Le pare-feu le plus classique est un pare-feu filtrant les paquets, qui bloquera l'accès à certains services(en fonction des ports) au niveau de la passerelle (routeur). De nombreux routeurs supportant les technologies VPN, tel que le routeur Cisco Privat Internet Exchange (PIX), gère en natif ce type de filtrage et ASA(Advanced Security Appliant). Un serveur proxy est aussi une solution possible pour protéger un réseau en laissant accès aux services VPN. Ce type de serveur tourne généralement sur des systèmes d'exploitation tels que Linux, Open BSD, Windows ou Novell Netware.

II.2 LES TECHNIQUES D'AUTHENTIFICATION

Les techniques d'authentification sont essentielles au bon fonctionnement d'un VPN puisqu'elles assurent aux utilisateurs d'un VPN qu'ils effectuent un échange de données avec le bon partenaire. L'authentification dans un VPN est semblable à l'authentification sur un système à l'aide d'un nom d'utilisateur et d'un mot de passe. Cependant les méthodes d'authentification des VPN sont souvent bien plus rigoureuses et compliquées. Chaque hôte possède un jeu de clefs, composé d'une clef publique et d'une clef privée. Les clefs parcourent un algorithme de hachage qui produit une valeur haché de ces dernières. A l'autre bout de la connexion, l'hôte possédant les mêmes clefs réalise un hachage identique, récupère

et compare la valeur de hachage retournée à celle qu'il a reçue. Ceci est possible grâce à certains protocoles :

- Protocole PAP (Password Authentication Protocol) est un protocole d'authentification non sécurisé car les identifiants et les mots de passe sont envoyés en clair (c'est-à-dire sans cryptage) entre le client et le serveur d'accès distant ;
- Protocol CHAP (Challenge Handshake Authentication Protocol) est une méthode d'authentification qui autorise le cryptage des mots de passe envoyés du client vers le serveur d'accès distant ;
- Protocole SPAP (Shiva Password Authentication Protocol) est un protocole d'authentification qui permet aux machines clients équipées avec du matériel de marque Shiva de se connecter au serveur d'accès distant. Les mots de passe sont protégés par un cryptage réversible (faible sécurité) ;
- Protocol MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) est un protocole propriétaire de Microsoft basé sur CHAP. Il utilise le protocole de cryptage MPPE (Microsoft Point-to-Point Encryptions) et est supporté depuis Windows 95 ;
- Protocol MS-CHAP v2 (Microsoft Challenge Handshake Authentification Protocol) est une amélioration du protocole de cryptage MS-CHAP avec des clés de cryptages plus fortes et une Authentification mutuelle entre le client et le serveur d'accès distant. Il a été implémenté à partir de Windows 98 ;

II.3 LE CHIFFREMENT

Utilisé pour que les données traversant le réseau ne puissent pas être lues par une autre personne. Pour cela, la première étape consiste à s'assurer que les deux équipements en bout de ligne disposent des mêmes algorithmes de chiffrement. On utilise pour cela notre baguage mathématique et surtout arithmétique. Les deux principaux types de cryptage utilisés sont :

Le chiffrement symétrique: le chiffrage symétrique utilise la même clé pour chiffrer et pour déchiffrer. L'inconvénient, est clair : chaque partie de la communication devra avoir la même clé, et la communiquer à la partie adverse sans que les autres puissent la récupérer. Plusieurs algorithmes de cryptage peuvent être utilisés DES: (Data Encryption Standard), AES (Advanced Encryption Standard).

Le chiffrement asymétrique: le cryptage asymétrique n'a pas cet inconvénient-là: deux clés sont utilisées : une clé publique et une clé privée. La clé publique est disponible par tout le monde. Elle sert à crypter des données. Si on veut communiquer avec un autre, on doit récupérer sa clé publique et seul lui pourra la décrypter avec sa clé privé. Bien sur le cryptage et le décryptage se font de manière précise suivant la méthode utilisée. La plus connue est la méthode RSA, acronyme des chercheurs qui ont publiés cette méthode : Rivest, Shamir et Adleman. Le chiffrement est utilisé dans le contexte du VPN pour garantir la confidentialité des données circulant sur le réseau public. En effet, le réseau VPN n'est que virtuellement coupé du réseau public.

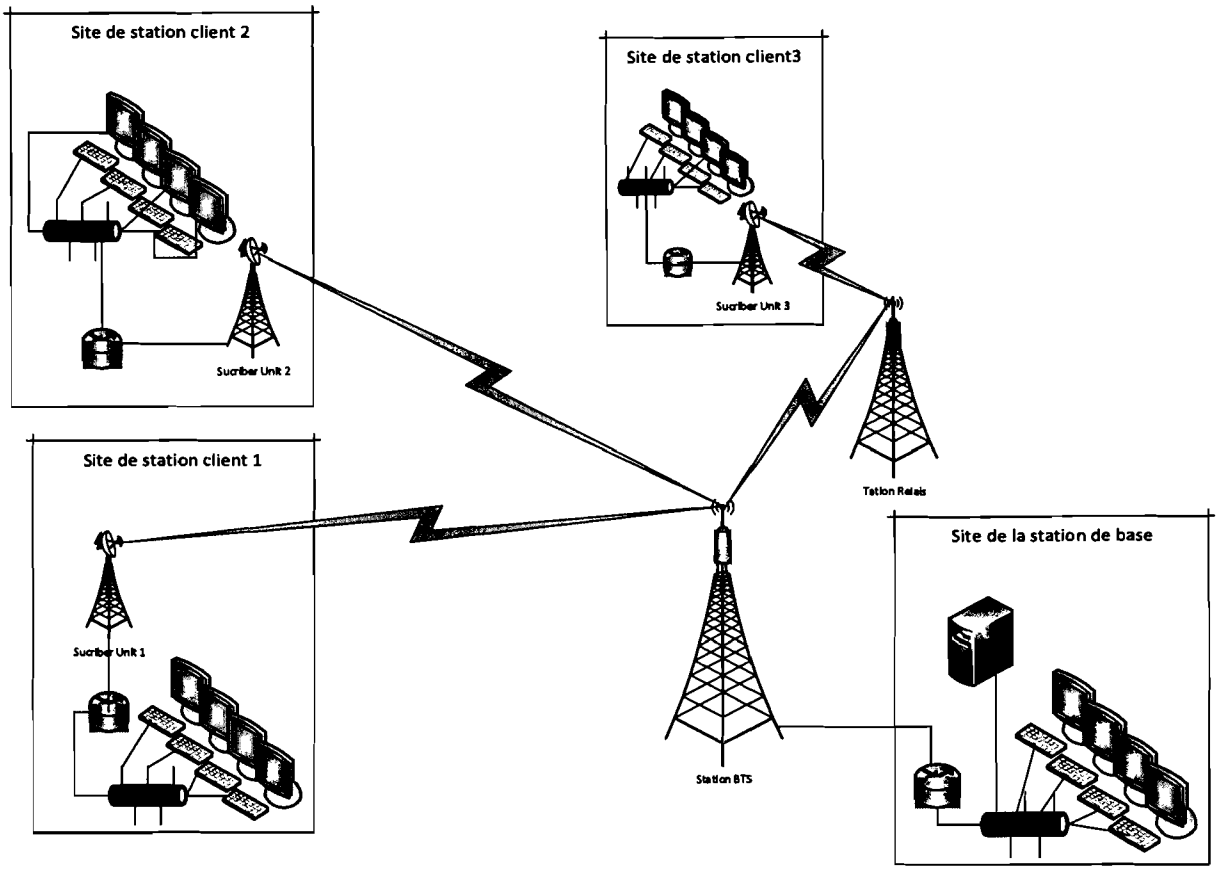


Figure 8: Représentation du WIMAX

IV.2.2 AVANTAGES ET INCONVENIENTS DU WIMAX

➢ LES AVANTAGES :

- Facilité de mise en œuvre ;
- Large zone de couverture ;
- Facilité de maintenance et d'administration ;
- Possibilité d'investissement progressif en fonction de la demande ;
- Faible coût de déploiement par rapport au réseau filaire.

➢ LES INCONVENIENTS :

- Faible tolérance aux perturbations en milieu urbain;
- Sensibilité aux conditions météorologiques ;
- Nécessité de disposer d'un point haut.

L'investissement de départ d'un WIMAX est important, essentiellement du côté du fournisseur qui développer son réseau d'antenne afin de couvrir un territoire le plus large

possible. En plus il y'a des équipements qui ne suivent pas la technologie (antennes sur laptop pas assez puissantes).

En réalité, le WIMAX ne pourra franchir que de petits obstacles comme un arbre ou une maison mais le signal est incapable de passer au travers de collines ou d'immeubles importants. Le débit en présence d'obstacle est fortement diminué (on parle de 20 Mbit/s/sec).

Après une étude des différentes solutions possibles, le tableau nous donne une synthèse sur ces solutions.

Tableau 4: Comparaisons des solutions possible.

Solution	Fibre Optique	LS	VPN	BLR	VSAT	WIMAX
Autonomie	OUI	NON	NON	OUI	NON	OUI
Coût	Très élevé	Moyen	Moyen	Moyen	Elevé	Moyen
Implantation	Complexe	Facile	Facile	Facile	Facile	Facile
Durée D'implantions	Très élevée	Peu élevée	Peu élevée	Assez élevée	Peu élevée	Assez élevée

IV.3 SOLUTIONS CHOISIES

Au regard de toutes ces solutions qui se présentent, il nous appartient d'opérer un choix judicieux et optimal pour l'interconnexion des sites de la région de l'ouest. Ainsi pour respecter l'objectif recherché, nous nous sommes donnés à une solution hétérogène. Après l'analyse des différentes solutions, le tableau précédent nous permet de choisir : Le VPN et Le WIMAX.

QUATRIEME PARTIE: ETUDE ET MISE EN ŒUVRE DES SOLUTIONS CHOISIES

La partie précédente a mis en relief les différentes possibilités envisageables pour interconnecter les sites de la direction régionale de la SONABEL. Au regard du problème posé, nous sommes en obligation de faire une proposition de solution hétérogène afin de lever avec succès les soucis de la DRO/SONABEL. Par conséquent nous proposons une solution qui prend en compte de manière simple la mise en œuvre d'une technologie WIMAX et d'un réseau VPN.

CHAPITRE I

PRESENTATION GENERALE DU VPN

I.1 DEFINITION

Le terme VPN (Virtual Private Network) ou réseau privé virtuel, est devenu un terme courant dans l'informatique d'entreprise et le domaine des réseaux. Néanmoins, beaucoup de petites entreprises ont du mal à comprendre le concept et le bénéfice que cela peut leurs apporter.

La méthode la plus simple pour définir un VPN est de simplement décomposer l'expression comme suit :

Network : C'est un réseau, qui peut être constitué de plusieurs machines pouvant communiquer entre elles d'une façon ou d'une autre. Ces machines peuvent être dans un même endroit physiquement ou non et les méthodes de communication sont diverses.

Privat : pour privé cela veut dire que les communications entre deux ou plusieurs machines sont secrètes. Ainsi, une machine ne participant pas à la communication privée ne saura même pas que celle-ci a lieu.

Virtual : Le concept de virtuel est un peu plus compliqué à définir. Ce terme est souvent utilisé pour parler d'objet artificiel par exemple la mémoire virtuelle opposée à la mémoire physique d'un ordinateur ; en d'autre terme c'est l'émulation de la fonction d'un objet qui n'est pas vraiment là.

En combinant ces termes, on comprend que le VPN est un réseau privé obtenu en émulant, une fonction à l'opposé d'un réseau rendu par câblage direct entre les différentes machines. Les termes ci-dessus nous permettent de définir le concept de VPN comme étant un réseau privé construit au sein d'une infrastructure informatique public, telle qu'internet.

I.2 PRINCIPE DE FONCTIONNEMENT

Le VPN repose sur un protocole appelé «protocole de tunneling », c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre en toute sécurité grâce à des algorithmes de cryptographie. On emploie le terme « tunnel » pour symboliser le fait que les données soient cryptées et de ce fait incompréhensible pour tous les autres utilisateurs du réseau public (ceux qui ne se trouvent pas aux extrémités du VPN). Ainsi les utilisateurs ont l'impression d'être connecter directement sur le réseau de leur entreprise. Dans le cas d'un VPN établi entre deux machines, on appelle client VPN l'élément permettant de chiffrer et de déchiffrer les données du côté utilisateur (client) et serveur VPN (ou plus généralement serveur d'accès distant) l'élément chiffrant et déchiffrant les données du côté de

l'organisation. De cette façon, lorsqu'un utilisateur nécessite d'accéder au réseau privé virtuel, sa requête va être transmise en clair au système passerelle, qui va se connecter au réseau distant par l'intermédiaire d'une infrastructure de réseau public, puis va transmettre la requête de façon chiffrée. L'ordinateur distant va alors fournir les données au serveur VPN de son réseau local qui va transmettre la réponse de façon chiffrée. A la réception sur le client VPN de l'utilisateur, les données seront déchiffré es, puis transmises à l'utilisateur. Pour émuler une liaison point à point, les données sont encapsulées, ou enrobées, à l'aide d'un en-tête qui contient les informations de routage pour leur permettre de traverser le réseau partagé ou public jusqu'à leur destination finale. Le principe de tunneling consiste donc à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les données à transmettre peuvent être prises en charge par un protocole différent du protocole IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un en-tête.

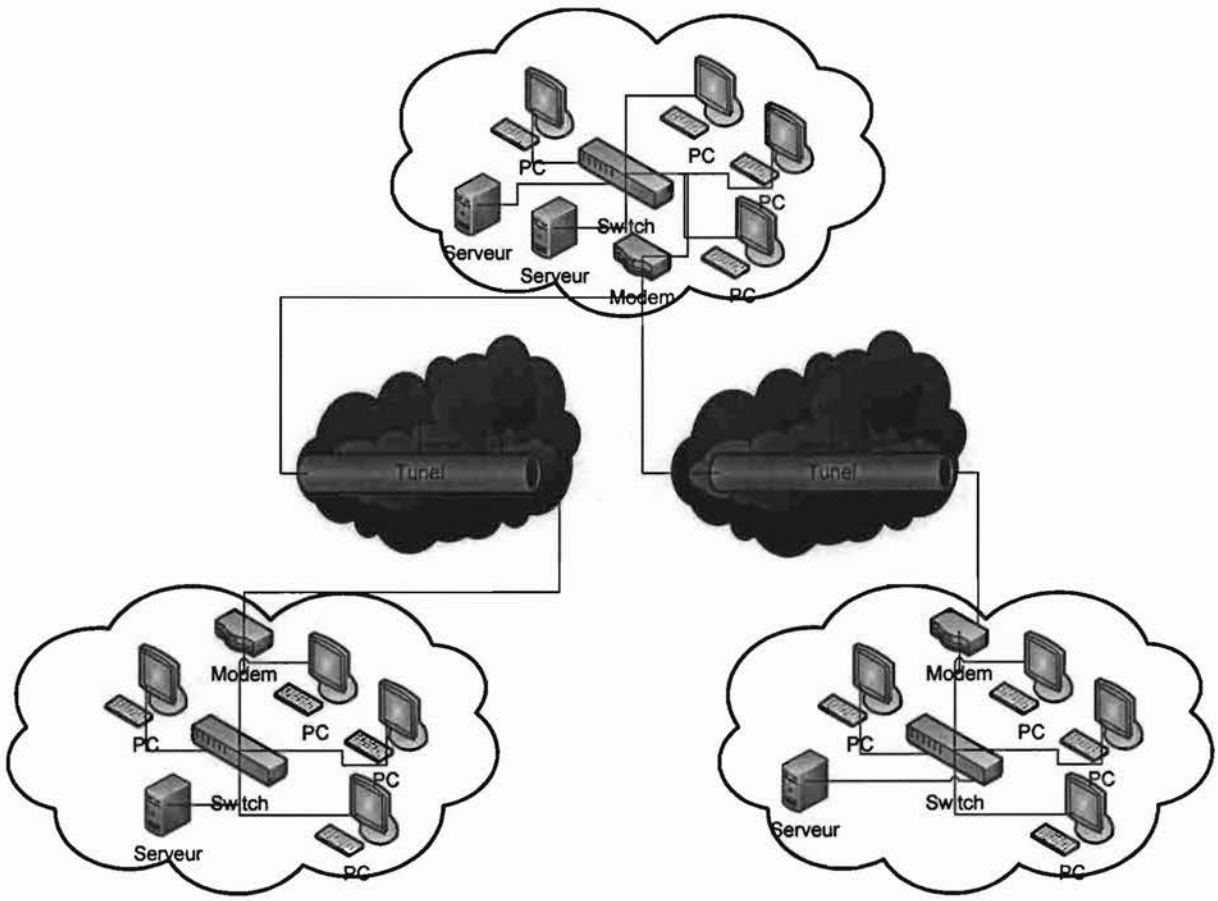


Figure 9 : Schéma de Principe

Le tunneling est un ensemble de processus d'encapsulation (la charge utile est mise dans un en-tête supplémentaire), de transmission (acheminement des paquets par un réseau intermédiaire) et de desencapsulation (récupération de la charge utile). Pour des besoins de facilité d'administration et de configuration de la solution, nous nous s'orienterons vers une architecture centralisée, où les différents points VPN se relient à un site central, pour lequel il faudra augmenter le débit de la ligne. Dans le cas d'un site éclaté, des ajustements peuvent

être faits en termes de débits mais le nombre d'équipements et la complexité de l'administration augmente au fur et à mesure que les liens VPN se multiplient.

I.3 CARACTERISTIQUES D'UN VPN

Le VPN est une généralisation du concept de tunnel. Il s'agit de faire circuler dans le tunnel non seulement les informations des applications, mais également tout ce qui concerne les couches réseau et transport. En effet, on crée un nouveau réseau à l'intérieur du tunnel. Vous imaginerez facilement les avantages d'un VPN en considérant 2 réseaux locaux ayant besoin d'être reliés via un réseau peu sûr comme internet. Les 2 LAN se relient par un tunnel traversant Iternet et formant un nouveau LAN virtuel et sûr : le VPN.

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Son principe est celui d'être transparent pour les utilisateurs et pour les applications ayant accès. Il se caractérise par les fonctionnalités suivantes :

Authentification des entités communicantes: le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa ;

Authentification des utilisateurs : seules les personnes autorisées doivent y accédés ;

Gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveaux clients en obtenir une facilement. Cette adresse privée doit rester confidentielle ;

Cryptage des données: les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa ;

Gestion des clés: les clés de cryptage pour le client et le server doivent être générées et régénérées souvent (automatiquement) ;

Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux public en particulier IP fin a de réaliser un vrai tunnel comme s'il y'avait réellement un câble entre les deux réseaux.

Le VPN est un principe, un concept : il ne décrit pas l'implémentation effective de ces caractéristiques. C'est pourquoi il existe plusieurs produits différents sur le marché dont certains sont devenus standard, et même considérés comme des normes.

I.4 INTERET D'UN RESEAU VPN

La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local. Ce procédé est utilisé par de nombreuses entreprises afin de permettre à leurs utilisateurs de se connecter au réseau d'entreprise hors de leur lieu de travail et SONABEL/BOBO ne faillira pas à la tradition et aspire à une extension de son réseau local. On peut facilement imaginer un grand nombre d'applications possibles.

- Les connexions VPN offrent un accès au réseau local (d'entreprise) à distance et de façon sécurisée pour les travailleurs nomades ;
- Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante ;
- Les connexions VPN permettent aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public, telle qu'Internet ;
- Les connexions VPN permettent également aux entreprises de disposer de connexions routées partagées avec d'autres entreprises sur un réseau public, et de continuer à disposer de communications sécurisées, pour relier, par exemple des bureaux éloignés géographiquement. Une connexion VPN routée via Internet fonctionne logiquement comme une liaison de réseau étendu (WAN, Wide Area Network) dédiée ;
- Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisés entre une machine locale et une machine distante.

Il n'en demeure pas moins qu'un VPN présente des limites parmi lesquelles : la connexion internet qui en plus d'être un avantage économique pour les entreprises dans le sens où elle lui évite des coûts liées à la ligne dédié ; mais sans elle le VPN n'est pas possible. La connexion doit à tout moment être disponible pour les utilisateurs et entreprises utilisant cette technologie.

I.5 LES DIFFERENTS TYPES DE VPN

On peut dénombrer deux grands types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie :

I.5.1 LE VPN D'ACCES

Il est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau de leur entreprise. L'utilisateur se sert d'une connexion internet afin d'établir une liaison sécurisée. Il existe deux cas :

L'utilisateur demande au FAI de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS (Network Access Server) du FAI.

L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune des avantages et des inconvénients :

La première méthode permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un FAI proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée; ce qui peut poser des problèmes.

La deuxième méthode permet de résoudre ce problème puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel lui permettant d'établir une communication cryptée. Nous verrons que pour pallier à ce problème, certaines entreprises mettent en place des VPN à base de SSL (Secure Socket Layer), technologie implémentée dans la majorité des navigateurs internet du marché. Quel que soit la méthode de connexion utilisée, ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs. Cette authentification peut se faire par une vérification login/mot de passe, par un algorithme dit Tokens sécurisés (utilisation de mots de passe aléatoires) ou par certificats numériques.

I.5.2 LE VPN LAN TO LAN

Ici on a deux sous-catégories :

L'EXTRANET VPN

Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors une partie de son réseau local à ces derniers. Dans ce cas, il est nécessaire d'avoir une authentification forte des utilisateurs, ainsi qu'une trace des différents accès. De plus, seule une partie des ressources sera partagée, ce qui nécessite une gestion des espaces d'échange.

L'INTRANET VPN

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données client, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source, ainsi que leur non répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutés aux paquets. La confidentialité des données est elle aussi basée sur des algorithmes de cryptographie.

CHAPITRE II

SECURISATION D'UN VPN

Lors de l'utilisation de serveurs VPN sur un réseau, il est conseillé de s'attarder de façon rigoureuse sur la sécurité. Pour éviter d'être exposé aux différentes attaques des hackers. Le VPN utilise un ensemble de technologies pour sécuriser les données qui voyagent d'un bout à l'autre d'internet. Les concepts les plus importants sont ceux de firewall, d'authentification, protocole de tunnels et du chiffrement de données que nous allons présenter.

II.1 LES FIREWALLS

Un firewall (pare-feu) internet a le même but qu'une porte coupe-feu dans un immeuble : protéger une certaine zone de l'avancée des flammes ou d'une explosion qu'elles pourraient engendrer. L'avancée des flammes dans un immeuble est contrôlée en plaçant de solides murs à des endroits stratégiques qui aident à contenir les flammes et à réduire les dégâts occasionnés. Un pare-feu Internet a le même rôle en utilisant des techniques telles que l'examen de l'adresse IP du paquet qu'il reçoit ou le port sur lequel arrive une connexion il décide de laisser passer ou de bloquer le trafic entrant.

Bien que le VPN n'implémente pas de firewall standard par défaut, les pare-feu font partie intégrante d'un VPN. L'idée est qu'ils doivent être utilisés pour garder les utilisateurs non désirables hors du réseau tout en acceptant les utilisateurs du VPN. Le pare-feu le plus classique est un pare-feu filtrant les paquets, qui bloquera l'accès à certains services(en fonction des ports) au niveau de la passerelle (routeur). De nombreux routeurs supportant les technologies VPN, tel que le routeur Cisco Privat Internet Exchange (PIX), gère en natif ce type de filtrage et ASA(Advanced Security Appliant). Un serveur proxy est aussi une solution possible pour protéger un réseau en laissant accès aux services VPN. Ce type de serveur tourne généralement sur des systèmes d'exploitation tels que Linux, Open BSD, Windows ou Novell Netware.

II.2 LES TECHNIQUES D'AUTHENTIFICATION

Les techniques d'authentification sont essentielles au bon fonctionnement d'un VPN puisqu'elles assurent aux utilisateurs d'un VPN qu'ils effectuent un échange de données avec le bon partenaire. L'authentification dans un VPN est semblable à l'authentification sur un système à l'aide d'un nom d'utilisateur et d'un mot de passe. Cependant les méthodes d'authentification des VPN sont souvent bien plus rigoureuses et compliquées. Chaque hôte possède un jeu de clefs, composé d'une clef publique et d'une clef privée. Les clefs parcourent un algorithme de hachage qui produit une valeur haché de ces dernières. A l'autre bout de la connexion, l'hôte possédant les mêmes clefs réalise un hachage identique, récupère

et compare la valeur de hachage retournée à celle qu'il a reçue. Ceci est possible grâce à certains protocoles :

- Protocole PAP (Password Authentication Protocol) est un protocole d'authentification non sécurisé car les identifiants et les mots de passe sont envoyés en clair (c'est-à-dire sans cryptage) entre le client et le serveur d'accès distant ;
- Protocol CHAP (Challenge Handshake Authentication Protocol) est une méthode d'authentification qui autorise le cryptage des mots de passe envoyés du client vers le serveur d'accès distant ;
- Protocole SPAP (Shiva Password Authentication Protocol) est un protocole d'authentification qui permet aux machines clients équipées avec du matériel de marque Shiva de se connecter au serveur d'accès distant. Les mots de passe sont protégés par un cryptage réversible (faible sécurité) ;
- Protocol MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) est un protocole propriétaire de Microsoft basé sur CHAP. Il utilise le protocole de cryptage MPPE (Microsoft Point-to-Point Encryptions) et est supporté depuis Windows 95 ;
- Protocol MS-CHAP v2 (Microsoft Challenge Handshake Authentification Protocol) est une amélioration du protocole de cryptage MS-CHAP avec des clés de cryptages plus fortes et une Authentification mutuelle entre le client et le serveur d'accès distant. Il a été implémenté à partir de Windows 98 ;

II.3 LE CHIFFREMENT

Utilisé pour que les données traversant le réseau ne puissent pas être lues par une autre personne. Pour cela, la première étape consiste à s'assurer que les deux équipements en bout de ligne disposent des mêmes algorithmes de chiffrement. On utilise pour cela notre baguage mathématique et surtout arithmétique. Les deux principaux types de cryptage utilisés sont :

Le chiffrement symétrique: le chiffrage symétrique utilise la même clé pour chiffrer et pour déchiffrer. L'inconvénient, est clair : chaque partie de la communication devra avoir la même clé, et la communiquer à la partie adverse sans que les autres puissent la récupérer. Plusieurs algorithmes de cryptage peuvent être utilisés DES: (Data Encryption Standard), AES (Advanced Encryption Standard).

Le chiffrement asymétrique: le cryptage asymétrique n'a pas cet inconvénient-là: deux clés sont utilisées : une clé publique et une clé privée. La clé publique est disponible par tout le monde. Elle sert à crypter des données. Si on veut communiquer avec un autre, on doit récupérer sa clé publique et seul lui pourra la décrypter avec sa clé privé. Bien sur le cryptage et le décryptage se font de manière précise suivant la méthode utilisée. La plus connue est la méthode RSA, acronyme des chercheurs qui ont publiés cette méthode : Rivest, Shamir et Adleman. Le chiffrement est utilisé dans le contexte du VPN pour garantir la confidentialité des données circulant sur le réseau public. En effet, le réseau VPN n'est que virtuellement coupé du réseau public.

II.4 LES PROTOCOLES DE TUNNELISATION

II.4.1 CATEGORIES DE PROTOCOLES

II.4.1.1 CLASSEMENT PAR NIVEAU OSI

Il existe deux catégories de protocoles VPN :

✓ Les protocoles nécessitant parfois/souvent du matériel particulier :

Les protocoles de niveau 2 (Couche Liaison) dans la pile TCP/IP : PPTP, L2F et L2TP

Les protocoles de niveau 3 (Couche Réseau) dans la pile TCP/IP : IPSec ou

MPLS

✓ Les protocoles ne nécessitant qu'une couche logicielle :

Les protocoles de niveau 4 (Couche Transport) : OpenVPN en SSL

II.4.1.2 CLASSEMENT PAR SYSTEME D'EXPLOITATION

Voici les protocoles classés par OS :

✓ Disponibles nativement sous Windows:

PPTP et IPSec/L2TP

✓ Protocoles disponibles sous Linux et Windows par logiciel annexe :

OpenVPN

✓ Disponibles sous Linux:

Tous

II.4.2 LES PRINCIPAUX PROTOCOLES DE VPN

Les principaux protocoles de tunneling VPN sont les suivants :

- PPTP (Point-to-Point Tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics ;
- L2F (Layer Two Forwarding) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète ;

- L2TP (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 2661) pour faire converger les fonctionnalités de PPTP et L2F. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP ;
- IPSec est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

CHAPITRE III

GENERALITES ET ANALYSE DU WIMAX

III.1 PRESENTATION DU WIMAX

III.1.1 GENERALITE

Le WIMAX est un nom commercial pour désigner une future norme dans les domaines des réseaux sans fils et signifie en anglais: World Interoperability for Microware Access». Cette norme a été créée en 2002 par les sociétés Intel et Alvarion. Il s'agit d'une nouvelle technique de transmission de données à longue distance par voie hertzienne, destinée à être employé pour l'internet haut débit. En résumé, on peut dire que le WIMAX est une sorte d'extension du WIFI. On peut même considéré que le WIMAX est une amélioration significative du wifi. Son objectif avoué est de remplacer à terme les réseaux filaires de types ADSL. Le WIMAX répond parfaitement aux caractéristiques d'une liaison haut débit :

- Vitesse, avec une rapidité de transmission dans les deux sens (montant et descendant) ;
- Permanence, avec une connexion permanente même en cas d'inactivité du réseau ;
- Continuité, le réseau local de l'entreprise se prolonge par l'internet ;
- Temps de latence faible, pour les applications ;
- Stabilité des débits, pour un confort d'utilisation ;
- Sécurité, le réseau ne doit pas être exposé de manière exagérée aux attaques.

III .1.2 LE WIMAX CONTRE LA FRACTURE NUMERIQUE

Le WIMAX a été créé à la base pour régler les problèmes d'éligibilité d'une ligne haut débit pour les particuliers habitant de la zone rurale non couvertes ou ayant une atténuation trop élevée sur leur ligne téléphonique. De plus suivant son lieu de résidence, tout le monde n'a pas accès aux offres dégroupées des fournisseurs des accès internet. Tous ces foyers représentent un marché potentiel énorme avec un bénéfice évident à en retirer. Etant donné que la transmission des données se fait par voie hertzienne, la différence d'atténuation, entre un point éloigné de l'antenne émettrice et un autre proche, n'est pas aussi flagrante que dans le cas d'un réseau filaire. Tant que l'abonné est situé dans la zone couverte par l'antenne il est en mesure de bénéficié d'une bonne connexion. Surfant sur la vague du succès du wifi, le WIMAX est probablement destiné à un grand avenir sur le moyen terme. Le WIMAX dispose de quelques avantages jouant en sa faveur pour atteindre ce but : avec un débit théorique de 75 Mbits/s et une zone de couverture de 50 km, il surpasse largement l'offre ADSL filaire

atteignant au 24 Mbits/s pour une zone de 10 km, tout en offrant les avantages d'une connexion Wireless.

III.1.3 L'INTERET DU WIMAX

- L'offre triple *play*

Actuellement, les offres triples *play* (Internet, télévision et téléphonie) sont très prisées du grand public. Le standard WIMAX intègre la notion de Qualité de Service (souvent notée QoS pour Quality of Service), c'est à dire la capacité o garantir le fonctionnement d'un service à un utilisateur. Ce qui est indispensable pour une offre triple *play*.

Concrètement, le WIMAX permet ainsi de réserver une bande passante pour un usage donné. En effet certain usages ne peuvent pas tolérer de goulots d'étranglement. C'est le cas notamment de la voix sur IP (VOIP) car la communication orale ne peut pas tolérer de coupure de la seconde. La télévision numérique aussi requiert une transmission de donnée en même cas de mobilité de l'antenne.

- Un débit alléchant

Le débit théorique affiché de 75 Mbit/s sera ce qui se fait de mieux en matière d'offre grand public tout en couvrant une plus large partie de la population.

- Le *wireless*

Le mode de transmission sans fil permet de profiter de sa connexion haut débit même en dehors de sa résidence (il faut de même se situé dans la zone de couverture de l'antenne de base).

- Compatibilité

Le WIMAX s'intègre partiellement dans les architectures réseau déjà existantes.

III.2 ANALYSE TECHNIQUE DU WIMAX

III.2.1 LA NORME 802.16

Le WIMAX fait partie de la norme 802.16. Celle-ci a été publiée et validée par l'IEEE (*Institute of Electrical and Electronics Engineers*) pour la première fois en 2002. Elle définit les réseaux métropolitains sans fil à large bande.

Tableau 5: Norme 802.16

STANDARD	DESCRIPTION	PUBLIE
IEEE std 802.16-2001	Définit des réseaux métropolitains sans fil utilisant des fréquences supérieures à 10GHz (jusqu'à 66GHz)	8 avril 2002
IEEE std 802.16c-2002	Définit les options possibles pour les réseaux utilisant les fréquences entre 10 et 66 GHz	15 janvier 2003
IEE 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 désignant 802.16d)	Il s'agit de l'actualisation (la révision) des standard de base 802.16, 802.16a, 802.16c.	1er octobre 2004
IEEE 802.16e (également désigné IEEE std 802.16e-2005)	Apporte les possibilités d'utilisation en situation mobile du standard, jusqu'à 60 km/h.	7 décembre 2005
IEEE 802.16f	Spécifie la MIB (Management Informatique Base) pour les couches MAC et Physique	22 septembre 2005

III.2.2 CARACTERISTIQUES TECHNIQUES

Nous nous intéressons dans cette partie au contenu technique du WIMAX. Comme nous avons pu le voir précédemment, la technologie WIMAX repose sur un ensemble de norme ayant deux objectifs :

- Atteindre une très grande distance;
- Pouvoir livrer en bande large à des millions de débits par seconde ;

Ces caractéristiques imposent des techniques de modulation particulières en matière de traitement numérique du signal car nous avons une très longue portée et un débit important.

Or plus la distance de transmission est élevée, plus le débit est faible ; la technologie sans fil wifi a montré ses limites sur ce point. Le WIMAX reprend en grande partie plusieurs techniques de modulation du wifi mais avec des spécifications différentes pour permettre un meilleur rendement. Les différents types de modulation du signal sont les suivants:

- CDMA, Code Division Multiple Access
- FDMA, Frequency Division Multiple Access
- DSSS, Direct Sequence Spread Spectrum
- FHSS, Frequency Hopping Spread Spectrum
- TDMA, Time Division Multiple Access
- W-OFDM, Wide Orthogonal Frequency Division Multiplexing
- OFDMA, Orthogonal Frequency Division Multiple Access

DSSS (Direct Sequence Spread Spectrum) : Utilisé également dans le Wifi, on retrouve cette technique de modulation dans le WIMAX. DSSS convient généralement pour tous les réseaux sans fil, il consiste à diviser la porteuse en sous- canaux. Le signal occupe la totalité de la bande.

OFDM (Orthogonal Frequency Division Multiplexing) : Pour émettre un signal, l'OFDM divise une plage de fréquence en plusieurs sous-canaux espacés par des zones libres de tailles fixes. Par la suite, un algorithme, le Fast Fourier Transform (FFT), véhicule le signal par le biais des recompositions du message chez le récepteur. L'objectif permet ainsi d'exploiter au maximum la plage de fréquence allouée tout en minimisant l'impact du bruit grâce aux espaces libres séparant chaque canal.

FHSS (Frequency Hopping Spread Spectrum) : La bande de fréquence est divisée 75 sous-canaux de 1 Mhz chacun. A chaque message correspond une séquence de sauts qui indique quels sont les schémas de fréquences que doit emprunter le signal durant son trajet. Cette séquence de saut est transmise au récepteur du message avant le début de l'émission. L'objectif du FHSS est d'améliorer des informations transmises.

Tableau 6: Autre technique de modulation

LES AUTRES TECHNIQUES DE MODULATION			
SIGLES	**SIGNIFICATION**	**COMMENTAIRE**	**SECURITE**
FDMA	Frequency Division Multiple Access	Technologie utilisée pour les communications en analogie. Divise le spectre alloué à l'opérateur en fréquence individuelles. Ecoute facile	-
TDMA	Time Division Multiple Access	Technologie utilisée pour les communications digitales. Chaque fréquence est divisée en 6 sessions voix/données distinctes, ce qui rend leur interception plus difficile	+
CDMA	Code Division Multiple Access	Chaque paquet de signaux est codé de manière aléatoire. De plus, cette technologie utilise un spectre très large de fréquence, rendant l'interception des données beaucoup plus complexe.	+++

III.3 SECURITIE DU WIMAX

Le standard 802.16e s'avère très riche sur plusieurs aspects à savoir la flexibilité du traitement des canaux de communication, les solutions adaptatives pour le codage et les fréquences... Cependant, l'aspect sécurité fut reconnu comme une des principales faiblesses des premières versions. La sous-couche sécurité protège fortement les utilisateurs contre le détournement du service. La station émettrice (BS – Base Station) se protège des accès illicites en sécurisant les flux de service associés dans le réseau. La sous-couche sécurité introduit également des mécanismes d'authentification dans le protocole client/serveur de gestion des clés, par lequel la BS contrôle la distribution des éléments de chiffrement aux stations mobiles (MS – Mobile Station). En plus, les mécanismes de sécurité de base sont renforcés en ajoutant une authentification des équipements basée sur un certificat numérique.

III.3.1 PROTOCOLE DE GESTION DES CLÉS PKM V2

Le protocole (Privacy Key Management) de gestion des clés PKM permet à la fois l'authentification mutuelle et l'authentification unilatérale. Celui-ci utilise dans son processus d'authentification :

- Des certificats numériques X. 509 [IETF RFC 3280] associés à un algorithme de chiffrement à clés publiques RSA [PKCS # 1].
- Le protocole EAP [IETF RFC 3748], en processus simple ou double.

III.3.2 PROCESSUS D'AUTHENTIFICATION

➢ CERTIFICAT NUMÉRIQUE MUTUEL RSA – X. 509.

Le protocole d'authentification RSA utilise des certificats numériques X. 509 [IETF RFC 3280] et l'algorithme de chiffrement sur clé publique RSA [PKCS # 1] qui lie les clés publiques de chiffrement RSA aux adresses MAC des stations mobiles. Un mobile MS initialise le processus d'autorisation en envoyant un message Authentication Information à sa station émettrice (BS). Ce message contient le certificat X. 509 délivré par le constructeur du mobile ou par une Autorité externe. Le message Authentication Information est purement informatif, la BS peut décider de l'ignorer. Cependant, il fournit à la BS un moyen de connaître le certificat constructeur du mobile client. Le mobile envoie un message Authorisation Request à sa BS, immédiatement après avoir envoyé le message Authentication Information. Ceci est une demande de clé d'authentification AK. Ce message est signé par la clé privée du mobile suivant un échange RSA. A la réception, la BS va utiliser la clé publique du certificat pour vérifier la signature du message. Le message Authorisation Request contient:

Un certificat X. 509, avec la clé publique du mobile que la BS va utiliser ensuite pour vérifier la signature du message.

Une description des possibilités cryptographiques que supporte le mobile. Celles-ci sont présentées à la BS sous la forme d'une liste d'identifiants, chacun indiquant les algorithmes de chiffrement et les algorithmes d'authentification que supporte le mobile.

Un nombre aléatoire de 64 bits pour caractériser chaque parcelle du message.

Message d'authentification/autorisation avec signature RSA : quand la BS reçoit ce message, elle procède à une vérification du code MAC avec la clé publique du certificat du mobile. Si correct, la BS utilise la clé publique du mobile pour chiffrer une clé Pre-PAK aléatoire (Pre-Primary AK, clé qui est utilisée ensuite pour obtenir la clé d'authentification AK). Cette Pre PAK est envoyée avec le certificat X. 509 de la BS, encapsulée dans un message RSA Autorisation Reply. Tous les attributs de ce message sont signés avec la clé privée de la BS, suivant un chiffrement RSA. A la réception, le mobile fait une vérification MAC avec la clé publique de la BS qui vient d'être envoyée dans le message RSA Autorisation Reply et, si tout est correct, le mobile utilise sa propre clé privée pour déchiffrer le Pre-PAK (chiffré auparavant avec la clé publique du mobile).

Message Authorisation Reply avec signature RSA : Le processus se termine quand le mobile envoie le message RSA Authorisation ACK. Ce message indique si l'authentification a été concluante ou non et, en cas d'erreur, la cause d'échec. Ce message est de nouveau signé RSA avec la clé privée du mobile, comme le RSA Autorisation Request.

Message RSA Autorisation ACK avec signature RSA: Grâce à cet échange de messages, les deux extrémités ont la Pre-PAK. Celle-ci est utilisée pour obtenir l'AK finale (qui sera utilisée

ensuite dans les signatures HMAC des procédures TEK d'échange et de transport de messages).

- PROTOCOLE EAP [IETF RFC 3748]

L'authentification EAP de la PKM utilise l'Extensible Authentication Protocol [IETF RFC 3748] conjointement à un mode d'EAP choisi par l'opérateur, par exemple EAP-TLS [IETF RFC 2716]. Le mode d'EAP va utiliser un type particulier de certificat, comme un certificat X. 509 pour EAP-TLS ou le Subscriber Identity Module pour EAP- SIM. Les références particulières et modes d'EAP utilisés (dont la description est en dehors du cadre de ce document) doivent satisfaire les « critères obligatoires ». L'utilisation d'un type d'EAP qui ne satisferait pas ces critères introduirait des vulnérabilités de sécurité dans le réseau. Le produit de la transaction EAP (d'un type qui garantit l'authentification mutuelle) qui est transmis à la couche 802.16 est la Master Session KEY (MSK) de 512 bits. Une clé servant à l'authentification est dérivée de la clé maître MSK Le mobile et le processus d'authentification en déduisent une PMK (Pairwise Master Key) et une EIK (EAP Integrity Key) optionnelle en tronquant la MSK à 2*160 bits. Après authentification réussie par EAP, si le mobile ou la BS négocient une règle d'autorisation comme « authentification EAP après EAP », une seconde authentification EAP intervient. La première authentification EAP s'est déroulée sans vérification de signature HMAC mais néanmoins, la seconde authentification va utiliser les procédures HMAC avec l'EIK (EAP Integrity Key) qui résulte de l'authentification EAP précédente.

- AUTHENTIFICATION RSA PLUS EAP

Si RSA plus EAP est choisi, la première authentification RSA intervient dans les mêmes conditions que ci-dessus. L'authentification EAP qui suit utilise un type qui satisfait les « critères obligatoires » mais les messages EAP sont protégés avec les procédures HMAC en utilisant l'EIK issu de la précédente authentification.

III.3.3 INTEGRITE : MAC/CMAC/SIGNATURES

Pour garantir l'intégrité des messages, WIMAX préconise l'utilisation de procédures HMAC/CMAC/signatures. L'algorithme de hachage HMAC utilisé est défini dans l'IETF RFC 2104 et utilise SHA-1 (FIPSb180-1) comme fonction logique. Le tableau suivant précise les clés HMAC/signature dans le processus d'authentification.

Tableau 7: Clés HMAC

Type d'Authent.	Signature		
RSA	OUI	NON	MS ou BS Publique/Privée
EAP	NON	NON	-
RSA	OUI	NON	MS ou BS

+			Publique/Privée
EAP	NON	OUI	EIK issu de RSA
EAP	NON	NON	-
+	NON	OUI	EIK issu d'EAP
RSA			

De tels mécanismes pour valider l'authenticité des messages ne sont pas seulement utilisés pendant le processus d'authentification, mais ils le sont aussi pendant l'échange de messages de distribution de clés et pendant l'échange de messages normaux de transport. Après le processus d'authentification (RSA, EAP, RSA + EAP) les deux extrémités (BS et mobile) ont reçu la clé d'authentification AK. A partir de celle-ci, la BS et le mobile vont tous deux obtenir trois autres clés :

CMAC/HMAC_KEY_U : clé utilisée dans les procédures HMC/CMAC pour les messages montants (uplink) Excepté la réauthentification. Dans ce cas, l'AK issue de l'authentification précédente est utilisé comme clé HMAC

CMAC/HMAC_KEY_D : clé utilisée dans les procédures HMC/CMAC pour les messages descendants (downlink)

KEK (Key Encryption Key) : c'est la clé qui est utilisée pour chiffrer la TEK (Traffic Encryption Key). La TEK doit être connu du mobile pour pouvoir décoder les messages. Ainsi cette clé doit elle-même être transportée sur l'interface air, mais ceci ne pouvant se faire en clair, la KEK est utilisée pour la chiffrer.

CHAPITRE IV

MISE EN ŒUVRE

Beaucoup d'entreprise comme la SONABEL sont réparties sur différents sites géographiques. Elles pourraient facilement utiliser une configuration VPN pour partager des informations ou même pour réduire leurs factures téléphoniques en implémentant un réseau sur cette liaison VPN. La mise en œuvre d'une solution VPN et donc les moyens utilisés dépendent étroitement du type de VPN dont il s'agit, ainsi que de la fréquence d'utilisation. La mise en œuvre d'un VPN nécessite systématiquement l'utilisation d'un serveur qui aura en charge la partie authentification, cryptage et décryptage, et d'un client assurant la partie cryptage/décryptage et qui assurera la partie connexion, sauf en cas de connexion vers un serveur. De plus, le client aura souvent la charge d'initialiser la connexion, sauf en cas de connexion permanente.

IV.1 ETUDE DE FAISABILITE

Etant donné que la SONABEL à plusieurs sites distants, et que suivant ses activités, celles-ci ont besoin d'un échange fréquent d'informations. Cependant la communication entre les sites doit garantir une sécurité optimale au trafic des informations ; et en plus des informations nous constatons que même les ressources de l'entreprise devront être mutualisées. Vue toutes ces doléances, l'accès internet illimité disponible en son sein doit être exploité en compensation des nombreux investissements qu'elle entraine, afin d'atteindre notre objectif. La mise en œuvre de cette architecture réseau passe d'abord au préalable par une étude de faisabilité.

IV.1.1 FAISABILITE TECHNIQUE

Le bilan des ressources disponibles effectué plus haut dans la partie problématique, nous montre clairement que nous possédons l'ensemble du matériel nécessaire à la mise en œuvre de notre projet dans les trois sites dans la mise en du VPN. Mais dans la mise en œuvre du WIMAX, la majorité du matériel est manquant.

IV.1.2 FAISABITE ECONOMIQUE

- Contrairement aux autres solutions d'interconnexions des sites distants (VSAT ou la fibre optique), le VPN est non seulement pratique, mais économique, car on utilise un réseau publique (internet) pour relier les trois sites ;

- Les coûts liés aux anciennes techniques de transferts et de stockage des données sont suspendus, et de plus les ressources sont partagées de part et d'autre de l'entreprise ce qui réduit les dépenses.

IV.1.3 FAISABILITE TEMPORELLE

Le VPN est évolutif car il permet de connecter plusieurs sites distants entre eux. De même, plusieurs utilisateurs distants et itinérants pourront accéder au serveur distant de l'entreprise grâce à cette technologie.

IV.2 MISE EN PLACE D'UN RESEAU HETEROGENE GERE PAR UN SERVEUR LINUX

De nos jours, il existe plusieurs systèmes d'exploitation qui jouent le rôle de gestion de réseau (LanManager), par exemple Windows_NT, NOVELL, UNIX, LINUX etc....
Dans la suite, on va se limiter à expliquer les serveurs samba, NFS, NIS et le DHCP.

IV.2.1 MISE EN PLACE RESEAU UNIX / WINDOWS

Nous allons installer un serveur Unix et le configurer pour qu'il soit un contrôleur de domaine des postes Windows. Pour plus d'information sur l'implémentation vous pouvez consulter l'Annexe. Dans cette section nous étudions les outils utilisés afin de réaliser ce type de réseau.

IV.2.1.1 QU'EST-CE QUE LE SAMBA

Samba est un outil qui permet de faire communiquer les systèmes Unix et Windows. Le logiciel est développé sous la licence publique GNU. Samba va permettre à votre serveur Unix d'être vu comme s'il était une machine Windows. Cela signifie que toute personne utilisant une machine Windows sera capable d'utiliser des ressources sur un serveur Unix de la même façon que s'il était un pur server NT ou LanManager. Actuellement cela ne peut se faire que via le protocole TCP/IP. Samba est une implémentation du protocole SMB (Server Message Block) pour Unix. Le protocole SMB est le cœur de Net Bios ou de LanManager. Il va vous permettre de partager de partager vos répertoires et imprimantes Unix avec Windows NT, Windows 2000/XP etc... Il nécessitera que juste que TCP/IP soit configuré sur chaque machine devant accéder Samba ou pouvant être accédée par Samba. Samba peut aussi être activé en tant que Contrôleur de Domaine Principal (PDC Primary Domain Controller) qui validera des connections depuis un PC client, permettre à un script d'être exécuté et aussi à un profil (paramètre et préférences d'un utilisateur ou n group) d'être stocké sur le serveur et accédé depuis n'importe quelle place sur le réseau. Alors, Samba gère lui-même la liste de tous les utilisateurs. Finalement, Samba peut être compilé sur une grande variété de version Unix.

IV.2.1.2 MODE DE FONCTIONNEMENT DE SAMBA

Toutes les fonctionnalités Samba résident dans deux daemons : smbd et nmbd. Le premier est le serveur lui-même, réalisant les authentifications, donnant accès aux partages et/ou imprimante, jouant le rôle de contrôleur de domaine, … et la seconde facilite toutes les opérations de résolution de noms. Les daemon de Samba reçoivent toutes leurs directives de fichier smb.conf. Ce fichier possède une structure simple et la syntaxe employée est claire. Il contient de nombreux paramètres et certains sont dépendants des autres.

IV.2.1.3 SYNTAXE DE FICHIER SMB.CONF

La structure de fichier smb.conf et simple. En voici les grandes lignes :

- Le fichier est divisé en deux parties. Chaque partie renferme des paramètres qui définissent les ressources devant être exportées par Samba et les options pour chacun de celle-ci ;
- Une section globale rassemble les paramètres contrôlant les caractéristiques générales de Samba ;
- En plus de section globale, on trouve une section pour chaque service spécifique. Chaque section commence par un nom entouré par un crochet ([home]).
- Chaque paramètre est défini selon la syntaxe : nom=valeur. La valeur se compose d'un ou plusieurs mots séparés par des espaces. La valeur peut être de type booléen (true, false, yes, no) numérique ou une chaîne de caractères ;
- Chaque ligne commence par un point-virgule (;) ou par le symbole dièse(#) est considéré comme un commentaire et n'a aucun effet sur la configuration.

IV.2.1.4 ADMINISTRATION SAMBA AVEC SWAT

SWAT est l'acronyme de Samba Web Administration tool ou outil d'administration Web de Samba. Ce programme va nous permettre d'utiliser notre web browser préféré pour configurer et gérer fichier smb.conf. SWAT est un outil livré en standard avec toute distribution Samba (source ou exécutable). Si vous compilez vous-même Samba, ce programme sera automatiquement compilé. Un des gros avantages de SWAT sur les autres programmes de configuration est qu'il est écrit par le Samba Team et donc il connait toujours tous les paramètres correspondant à une version donnée.

IV.2.2MISE EN PLACE RESEAU Unix/Unix

IV.2 .2.1 CREATION DE SERVEUR NFS

- Présentation du NFS

  NFS signifie Network Files System, c'est comme son nom l'indique, un système de fichier en réseau qui permet de partager ses données principalement entre systèmes Unix. A la différence de Samba, NFS gère les permissions sur les fichiers et on peut donc l'utilisé de manière totalement transparente dans son arborescence linux.
- Installer un serveur NFS

Les trois fichiers de configurations principaux sont : /etc/export,/etc/hosts.deny et /etc /hosts.allow.

- /etc /export

La syntaxe fichier /etc /export est très simple :

Répertoire machine1 (option11, option12) machine2 (option21, option22)

Par exemple :

/home 192.168.1.10 (rw) 192.168.1.25 (ro)

Signifie que l'on autorise la machine 192.168.1.10 à accéder à notre répertoire /home en lecture et écriture ainsi que la machine 192.168.1.25 mais uniquement lecture.

- ❖ Répertoire : Le répertoire du serveur à partager
- ❖ Machine : Une liste de machine séparée par des virgules et autorisées à monter ce répertoire (utiliser des adresses IP).
- ❖ Options :

ro : c'est la valeur par défaut, lecture seule

rw : la machine à un accès en lecture/écriture au répertoire

no_root_squash : Les accès par l'utilisateurs root sur le serveur se font sous l'identité root

- /etc /hosts.deny

On va interdire toutes les machines qui ne sont pas autorisées explicitement dans le /etc /hosts.allow. Un bon vieux ALL:ALL interdira l'accès à tous les services à partir de toutes les machines. On peut cependant être plus précis en écrivant :

Portmap: ALL

Lockd : ALL

Mountd: ALL

Rquotad: ALL

Statd: ALL

- /etc /hosts.allow

Ce fichier a l'architecture suivante : service:IP de la machine client

Donc pour autoriser 192.168.1.6 à se connecter à un partage NFS, on écrira :

Portmap: 192.168.1.6

Lockd: 192.168.1.6

Mountd: 192.168.1.6

Rquotad: 192.168.1.6

Statd: 192.168.1.6

La commande exportfs est utilisée pour la mise à jour de la liste des répertoires exportés.

Options :

-a : pour exporter tous les répertoires

-u : pour ne pas exporter

Lancement du serveur NFS se fait par la commande : /etc /rcd.d /NFS start ou bien service NFS start

Le serveur est prêt et il reste le coté client !

Pour utiliser NFS, il faut le programme mount. On va maintenant pouvoir monter notre partage ! En principe tout devrait bien se dérouler. Pour monter ce partage définitivement à chaque démarrage de la machine, éditons votre /etc /fstab : 192. 168.1.1:/home /home NFS default 0 0

IV.2.2.2 CREATION DE SERVEUR NIS

- Présentation de NIS

Lorsque votre réseau comporte plus de deux ou trois ordinateurs Linux ou Unix, la gestion des utilisateurs et leur fichier se complique, la vie de l'utilisateur aussi. La solution : le système d'information sur le réseau ou NIS (Network Infomation Systèm). Les informations susceptibles d'être distribuée par NIS sont par exemple

/etc /password : nom login, mot de passe et répertoire d'ouverture

/etc /group : renseignement sur les groupes d'utilisateurs

Par exemple si votre mot de passe et les informations s'y rattachant sont enregistrées dans la base de donnée NIS, alors vous pouvez loguer sur toutes les machines du réseau sur lesquelles un client NIS est lancé.

- Fonctionnement

Le serveur NIS contient des fichiers de données appelés Tables NIS. Les clients s'effectuent des requêtes sur ses tables. Ils sont en contact permanent avec le serveur NIS pour trouver les informations dans sa base de données

- Installation un serveur NIS

- Configuration d'un serveur Maître

  - Commencer par créer un nouvel environnement NIS en définissant le nom du domaine :

#nisdomainname MONDOMAINE

Ou en modifiant le fichier /etc / sysconfig /network en ajoutant la ligne suivante : NISDOMAIN=MONDOMAINE

  - L'installation d'un serveur NIS se fait généralement grâce à un script : /usr /sbin /ypinit avec l'option (-m) pour un serveur maitre.

  - Lancer ensuite 'ypserv' qui permet au système d'agir en tant que serveur NIS : #/etc /rc.d /init.d / ypserv start ou bien ypserv start

- Configuration d'un client

L'installation de NIS sur une machine cliente comporte deux étapes :

- ❖ Modifier les fichiers d'administration du client de sorte que le client puisse profiter des avantages NIS ;
- ❖ Lancer ypbind qui permettra au client d'effectuer ses requêtes NIS.

IV.2.3 DHCP

Un serveur DHCP (protocole de configuration dynamique de l'hôte) permet aux ordinateurs clients d'obtenir dynamiquement les informations de configuration du réseau à chaque fois qu'ils se connectent à celui-ci. Un serveur DHCP attribue des adresses IP aux clients à partir d'un pool d'adresses définit pas l'administrateur. Les adresses attribuées sont généralement temporaires, mais peuvent être allouées de façon permanente à certains postes du réseau. L'adressage dynamique offre plusieurs avantages par rapport à l'adressage statique:

- Il est plus facile pour un nouvel utilisateur de configurer une connexion Internet sans avoir à se soucier de l'adresses IP, masque du réseau, les adresses DNS et d'autres détails techniques ;
- L'affectation, la gestion des adresses IP et des informations liées au réseau sont centralisées sur un serveur. L'administrateur système peut alors adresser des centaines de systèmes qui se connectent au réseau à partir d'un point central en utilisant le protocole DHCP ;
- Le bail d'adresse facilite la réutilisation d'une même adresse par plusieurs postes différents. Toute fois une adresse IP ne être utiliser que par un seul système à la fois.

Fonctionnement

- Le client dépourvu d'adresse IP, envoie en diffusion Broadcast un datagramme (DHCP DISCOVER) au port 67. Ce datagramme comporte entre autres l'adresse physique (MAC) du client.
- Tout serveur DHCP autoritaire ayant reçu ce datagramme, envoie une offre DHCP (DHCP OFFER) à l'attention du client (sur son port 68), identifié par son adresse physique. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous-réseau qu'il propose au client ;
- Le client retient la première qui lui parvient, et diffuse sur le réseau un datagramme de requête DHCP (DHCP REQUEST). Ce datagramme comporte l'adresse IP du serveur et celle qui vient d'être proposée au client. Elle a pour effet de demander au serveur choisi l'assignation de cette adresse, l'envoi éventuel des valeurs des paramètres, et d'informer les autres serveurs qui ont fait une offre qu'elle n'a pas été retenue ;
- Le serveur DHCP élabore un datagramme d'accusé de réception DHCP ACK qui assigne au client l'adresse IP et son masque de sous-réseau, la durée du bail de cette adresse et éventuellement d'autres paramètres comme l'adresse IP de la passerelle par défaut, l'adresse IP des serveurs DNS, l'adresses IP des serveurs NTP etc...

Les serveurs DHCP doivent être pourvus d'une adresse IP statique comprise dans la même classe d'adresses que l'adresse de réseau couverte par l'étendue DHCP.

IV.3 ARCHITECTURE DU RESEAU FUTUR

Le réseau de la SONABEL de la région de l'ouest sera constitué des sites de WIMAX. En effet les centres qui seront dans un rayon de 50 km constitueront une zone WIMAX à établir. Ces différentes zones de WIMAX seront interconnectées à la direction régionale via VPN.

Tableau 8 : Les stations de base WIMAX et leurs stations clients

STATION DE BASE WIMAX	STATION CLIENT WIMAX	DISTANCE (KM)
BANFORA	BEREGADOUGOU	15
	NIANGOLOKO	45
	ORODARA	42
	TOUSSIANA	25
	TIEFORA	30
DIEBOUGOU	DANO	29
	DISSINE	33
	ORONKWA	28
	FOUNZA	39
	WESSA/HAMELE	39
HOUNDE	KOUMBIA	33
	PA	30
	BONI	30
GAOUA	BOUFOUN-BOUFOUN	30

IV.4.1 SCHEMA DU RESEAU FUTUR

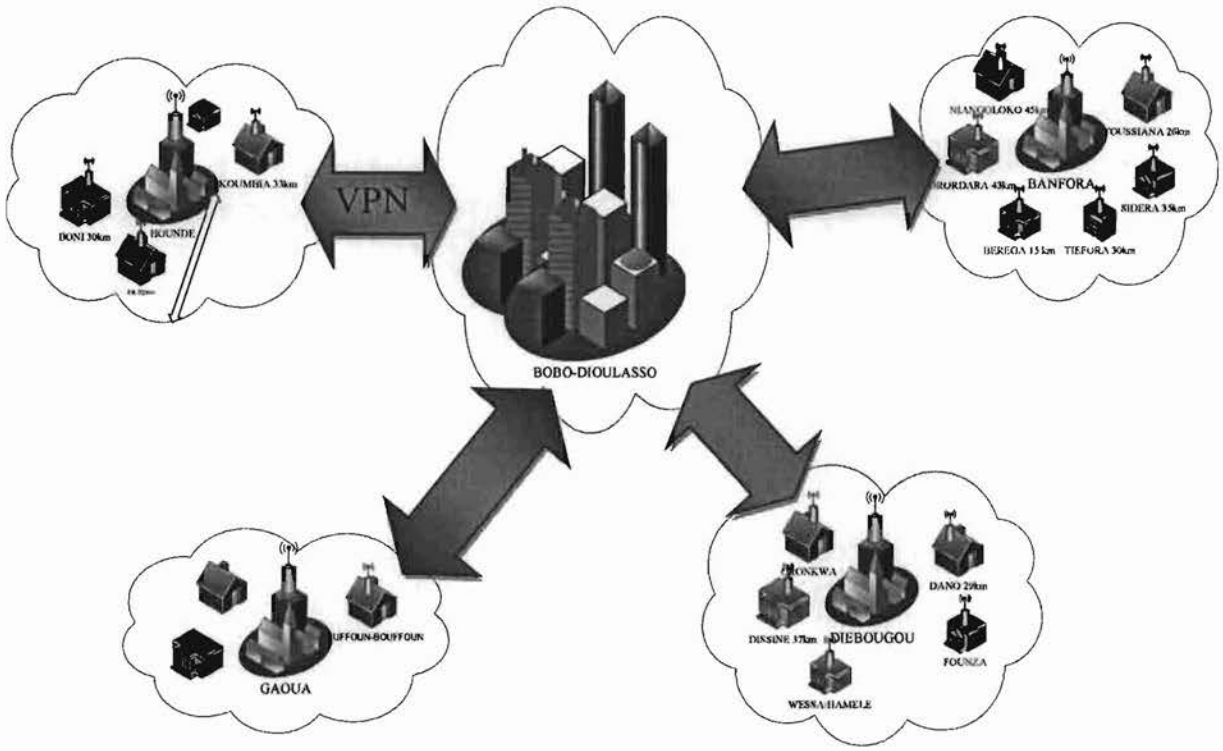


Figure 10 : Schéma du réseau futur

IV.4.2 MATÉRIELS ET ÉQUIPEMENTS UTILES

Tableau 9 : Matériels nécessaires

DESIGNATION	CARACTERISTIQUES	QUANTITE
Station de Base		3
SU + Modem	SU-31, SU-6, SU-54	16
Rouleau de câble	STP cat. 5	12
Connecteur	RJ45 Blindé	6
Capuchon	Pour RJ45	500
Pylône	15 m de haut	3
Tube de fer	fer de 5 m	21
Baliseur Nocturne	Ampoule économique d'une moyenne de 15000h- 15Watt- 220V	4
Routeur	D-Link routeur Ethernet de 4 ports DIR-100	13

CHAPITRE V

GESTION DU PROJET

Réaliser un projet d'interconnexion de sites, est une opération pleine de pièges. Ce chapitre vise à faire une étude sur les éléments permettant de maitriser le déroulement du projet informatiques en matière du temps qui sera mis pour la réalisation du projet, des moyens financiers qui seront déployés pour la réalisation et de la qualité du projet

V.1 GESTION DU DELAIS

L'évaluation de la durée du projet s'est fait en tenant compte de la durée d'implémentation des pylônes, la fixation et la configuration des antennes, et la mise en place des services réseaux

Tableau 10 : Estimation de la durée du projet

TACHE	TEMPS ESTIMATIF
Interconnexion et mise en place des services réseaux	15 mois
Formation des Agents	1 mois
Suivi	2 mois
Total	18 mois

V.2 GESTION DES COUTS

Le déploiement des solutions retenues, n'utilisant que des logiciels gratuits et libres, nécessite une étude théorique et une implémentation dont le coût est estimé comme suit :

Tableau 11 : Devis du projet

DESIGNATION		CARACTERISTIQUES	QUANTITE	PRIX UNITAIRE (FCFA)	MONTANT HT (FCFA)
Coté Interconnexion					
Station de Base	ODU		13	800.000	10.400.000
	IDU		13	4.200.000	54.600.000
SU + Modem		SU-31, SU-6, SU-54	8	400.000	3.200.000

Rouleau de câble	STP cat. 5	12	50.000	600.000
Paquet de connecteur	RJ45 Blindé	6	25.000	150.000
Capuchon	Pour RJ45	500	50	25.000
Pylône		13	400.000	5.200.000
Tube de Fer	Fer de 5m	21	25.000	525.000
Sac de ciment		10	8.000	80.000
Baliseur Nocturne	Ampoule économique d'une moyenne de 15000h- 15Watt- 220V	4	250.000	1.000.000
Routeur	D-Link routeur Ethernet de 4 ports DIR-100	13	20.000	260.000
Ordinateur	2.80 Ghz-4 Go de RAM	1	250.000	250.000
Coté Serveur				
Système d'exploitation	Linux/Unix		Gratuit	Gratuit
Serveur de fichier	Samba		Gratuit	Gratuit
Serveur d'information	NIS		Gratuit	Gratuit
Logiciel Firewall	Netfilter		Gratuit	Gratuit
Coût du Matériel	76.290.000			
Main d'œuvre	12.000.000			
Coût Total TTC	88.290.000			

V.3 GESTION DES RESOURCES HUMAINES

Le management des ressources humaines de notre projet sera constitué comme suit :

- Deux ingénieurs de travaux informatiques qui assureront la planification des ressources à savoir la formation, la direction des équipes, la configuration des différentes installations et le suivi des travaux ;
- Des techniciens pour le montage des pylônes et les différents câblages ;
- Des ouvriers pour les travaux divers.

V.4 GESTION DES RISQUES

On distingue cinq manières de gérer le risque, par ordre croissant de coût :

- **La prévention :**

  Des mesures peuvent être prises pour limiter l'apparition de l'événement redouté. Cette stratégie est le plus souvent appliquée en premier lieu et surtout lorsque le danger est dramatique (brûlure grave, chute de grande hauteur, coupure, pouvant entrainer la mort). La prévention peut aussi se faire par « évitement », c'est-à-dire, l'activité présentant un risque peut être suspendue ;

- **L'étude de danger**

  L'étude de dangers est un principe de la sécurité, dont un préalable est l'inventaire des objets et activités avec leur dangers intrinsèques, suivi de l'analyse des risques (scénarios pouvant aboutir à des événements non souhaités), en vue de maîtriser au mieux ces risques par des mesures de prévention.

- **L'acceptation :**

  L'acceptation d'un risque fait suite à une étude de danger. Cette étude permet d'évaluer les dommages pouvant être causés à des personnes exposées si l'événement redouté a lieu. Ainsi, un risque sans gravité conséquente peut être accepté par les travailleurs au compte de l'entreprise. L'acceptation est aussi valable lorsque le moyen de protection coûte trop cher ou gêne énormément l'ouvrier dans sa tâche. Cette approche ne permet pas de protéger les personnels ni l'outil de production tant qu'aucune volonté de réduction du risque ne se manifeste.

- **La réduction du risque :**

  Veille, identification des risques par l'audit, analyse par la recherche des facteurs de risques et des vulnérabilités, maîtrise des risques par les mesures de prévention et de protection : c'est la démarche classique de gestion des risques.

- **Le transfert :**

  A titre financier, le transfert de risque s'établit lorsqu'une assurance ou toute autre forme de couverture de risque financier ou garantie financière est contractée par le dirigeant confronté au risque. Ces garanties ne sont pas exhaustives pour couvrir le risque économique et financier. En cas de risque pénal pris par le dirigeant, ce transfert peut être réduit à néant.

V. 5 PLANNING DU PROJET

Le planning correspond aux dates pour réaliser les activités, identifier les jalons et atteindre les objectifs du projet; ce qui explique le tableau suivant :

Tableau 12 : Planning du Projet

TACHES	RESPONSABLES	RESULTATS ATTENDUS	CONTROL	DUREE
Commande du matériel et inspection des différents sites	Ingénieurs chargés des travaux	Détermination exacte d'implantation des pylônes	Informaticien de la SONABEL	3 mois
Implantation des pylônes et configuration de WiMax	Techniciens (aidés aussi par les ouvriers)		Ingénieurs chargés des travaux	9 mois
Configuration des serveurs, clients et installation des services	Ingénieurs chargés des travaux		Informaticien de la SONABEL	3 mois
Formation des agents	Ingénieurs chargés des travaux	Compréhension du nouveau système	Informaticien de la SONABEL	1 mois
Suivi	Ingénieurs chargés des travaux	Stabilité du bon fonctionnement	Informaticien de la SONABEL	2 mois

V.5 ACTIVITES MENEES DURANT LE STAGE

Tableau 13 : Activité menée durant le stage

INTERVENTIONS	DESCRIPTIONS
Configuration	l'Administrateur lors de la réinstallation d'Active directory sur Windows server 2003
Microsoft Office	Assistance du personnel pour la maîtrise des services Microsoft office
Maintenance des Imprimantes	Bourrage, changement de cartouche, partage,

	réparation.
Maintenance des Ordinateurs	Désinfection, réinstallation, installation des cartes d'extensions, réparation, changement d'ordinateur.
Réception de matériels informatiques	Vérification de la bonne marche du matériel et des caractéristiques demandées (ordinateur, Imprimante, Photocopieurs)
Technicien lors des dons de matériel	Mise en marche du matériel et explication des performances
Câblage	Ajout de prise murale et changement de switch
Gestion du système informatique pendant les absences (missions) de notre maître de stage	

V.6 ANALYSE CRITIQUE ET SUGGESTION

Au cours de notre séjour à la SONABEL, nous avons eu à remarquer un ensemble de choses bénéfiques ou préjudiciables à l'entreprise. De ces remarques ont découlés quelques suggestions.

V.6.1 CRITIQUES

Malgré l'organisation comme nous l'avons présenté dans la première partie, il n'en demeure pas moins que cette entreprise présente un certain nombre de faiblesses parmi lesquelles :

- l'utilisation des emails pour l'échange des données de l'entreprise, est un grand risque pour la sécurité de l'entreprise ;
- La mise à jour des serveurs et leurs maintenances dans chaque localité ;
- Un informaticien pour toute la région de l'ouest ;
- Le débit de la connexion à internet est très faible ;
- Il y a un manque d'outil informatiques ;
- Usage des ordinateurs obsolètes ;
- Usage des systèmes d'exploitation dépassés comme Windows 98.

V.6.2 SUGGESTIONS

Vue toutes ces dépenses qui incombe la société et le niveau de travail effectué, nous avons suggéré à l'entreprise :

De procéder à l'interconnexion de ses agences par le VPN pour permettre de sécuriser les informations de l'entreprise qui utilise la connexion internet afin de diminuer les couts de transport pour aller vers les différents clients et aussi par le WIMAX vue les conditions c'est-à-dire que l'ONATEL ne trouve pas dans certaines de ces zones donc pas accès à l'internet. De plus nous suggérons à la direction régionale dans la mesure du possible de remplacer les matériels obsolètes et enfin d'y remédier au manque des outils informatiques et de prévoir des matériels à la disposition de ses stagiaires.

CONCLUSION

Arrivé au terme de notre rapport de stage académique, et sans prétendre avoir cerné tous les contours du problème, il est judicieux de rappeler que notre travail portait sur le thème : « INTERCONNEXION DES SITES DE LA SONABEL : CAS DE LA DIRECTION REGIONALE DE L'OUEST». Nous avons dans les prémices de notre travail, effectué un tour d'horizon sur les besoins de l'entreprise, afin de mieux comprendre le problème posé et répondre aux attentes de l'entreprise, tout en respectant sa politique financière. Par la suite, nous avons fait une étude comparative des différentes technologies d'interconnexions envisageables, dans le but de choisir celle qui pourra être la mieux adapté à une société comme la SONABEL. A l'issu de cette étude, nous avons choisi les technologies VPN et WIMAX pour de nombreux avantages : économique, sécuritaire, évolutif et technique qu'elles offrent. Même si le fonctionnement du VPN reste dépendant de la connexion internet et de la bande passante allouée, cette nouvelle architecture réseau a été proposée aux dirigeants de SONABEL par le biais de la division informatique, et est actuellement en étude.

Nous tenons à souligner à quel point ce stage a été motivant et passionnant. Son principal atout a été sa richesse ; il nous a permis d'aborder plusieurs thèmes. La configuration d'un concentrateur VPN et celle du WIMAX ne nous était pas familière. Il nous a permis de toucher le monde des télécommunications. Nous avons notamment essuyé quelques moments de doute lors de la configuration du concentrateur VPN. Mais la réussite aidant, ces moments de flottements ont vite été oubliés. L'ambiance de travail a énormément contribuée à notre réussite, puisque intégré à l'équipe de division informatique de la SONABEL de la DRO, nous avons beaucoup bénéficié de l'expérience et du savoir-faire des professionnels.

Au point de vue personnel, ce stage nous a donc permis de mettre un pieds dans le monde du travail et de parfaire nos connaissances. Nous en sortons très heureux du travail que nous avons accompli et de tous les bénéfices que nous avons su en tirer.

BIBLIOGRAPHIE

APPLICATIONS :

Collection Microsoft Encarta 2009

Jargon informatique

LIENS :

http://Les Réseaux Privés Virtuels - Vpn.mht

http://la technologie VSAT · tout sur l'informatique.mht

http://technologie wimax (images) - Recherche Google.mht&biw=0&bih=0
http://neosmart.net/blog/feed/

http://chap-8-Les VPN.pdf http://www.commentcamarche.net/forum/affich-213673-projet-de-mise-en-reseau-d-entreprise
http://www.linuxfrance.org/~amascret/prj/edu/archinet/systeme/ch14s02.html
http://www.google.cm/#hl=fr&source=hp&q=VPN&lr=&aq=f&aqi=&aql=&oq=&gs_rfai=&f p=3e87d3dbfaac5c54 http://www.commentcamarche.net/forum/affich-767635-avantages-inconvenients

http://Les équipements de télécommunication VSAT &Fibre optique - foudaloic_over-blog_com.mht

http://www.xs4all.nl/~yskes/howto/linux_ipip_tunnel.htm

http://www.routage.org/gre.html

http://www.generation-nt.com/dossiers-39.html

http://www.commentcamarche.net/pratique/vpn-xp.php3

http://support.microsoft.com/default.aspx?scid=kb;fr;324747&Product=winsvr2003

http://www.securite.org/db/reseau/tunnel

http://free.korben.info/index.php/VPN

ANNEXES

ANNEXE 1 : PRINCIPAUX PROTOCOLES DU VPN

PROTOCOLE PPP

PPP (Point to Point Protocol) permet d'établir une connexion entre deux machines. Il est surtout utilisé pour les connexions modem. Il est full duplex et garantit l'ordre d'arrivée des paquets. Il encapsule PPP est employé généralement entre un client d'accès à distance et un serveur d'accès réseau. Il n'est pas sécurisé mais sert de support aux protocoles PPTP ou L2TP.

PROTOCOLE PPTP

Le principe du protocole PPTP (RFC2637) (Point To Point Tunneling Protocol) est de créer des trames avec le protocole PPP et de les crypter puis de les encapsuler dans un paquet IP. Cela permet de relier les deux réseaux par une connexion point-à-point virtuelle acheminée par une connexion IP sur Internet.

Il permet les opérations suivantes :

·L'authentification se fait par le protocole MS-CHAP (Challenge Handshake Authentification Protocol) version 2 ou avec le protocole PAP (Password Authentification Protocol)

·L'encryptage se fait par le protocole MPPE (Microsoft Point-to-Point Encryption). Cela crée un tunnel de niveau 3 (Réseau) géré par le protocole GRE (Generic Routing Encapsulation).

·La compression peut se faire avec le protocole MPPC (Microsoft Point to Point Compression)

On peut ajouter autant de protocole que l'on veut dans le protocole PPTP pour l'encryptions et la compression des données. Ces divers protocoles permettent de réaliser une connexion VPN complète, mais les protocoles suivants permettent un niveau de performance et de fiabilité bien meilleur.

PROTOCOLE L2TP

L2TP, définit par la référence RFC 2661, est issu de la convergence des protocoles PPTP et L2F (Layer 2 Forwading). Il a été développé conjointement par Cisco System, Microsoft, Ascend, 3Com ainsi que d'autres acteurs clés du marché des réseaux. Il permet l'encapsulation des paquets PPP au niveau des couches 2 (Frame Relay et ATM) et 3 (IP). Lorsqu'il est configuré pour transporter les données sur IP, L2TP peut être utilisé pour faire du tunneling sur Internet. Il repose sur deux concepts : les concentrateurs d'accès L2TP (LAC : L2TP Access Concentrator) et les serveurs réseau L2TP (LNS : L2TP Network Server).

L2TP n'intègre pas directement de protocole pour le chiffrement des données. C'est pourquoi L'IETF (Internet Engineering Task Force) préconise l'utilisation conjointe d'IPSEC et L2TP.

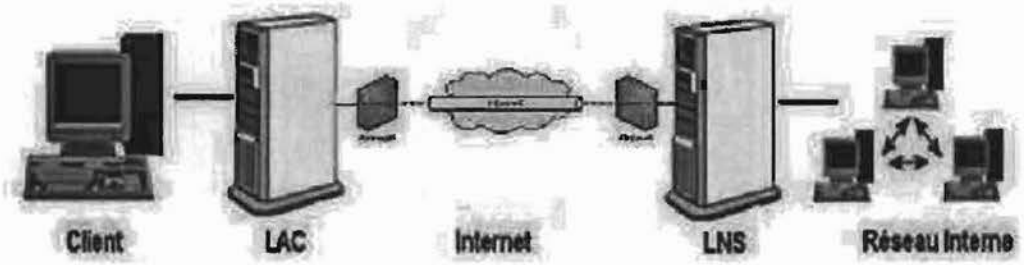


Figure 11 : Protocole L2TP

Concentrateurs d'accès L2TP (Lac : L2TP Access Concentrator)

Les périphériques LAC fournissent un support physique aux connexions L2TP. Le trafic étant alors transféré sur les serveurs réseau L2TP. Ces servers peuvent s'intégrer à la structure d'un réseau commuté RTC ou alors à un système d'extrémité PPP prenant en charge le protocole L2TP. Ils assurent le fractionnement en canaux de tous les protocoles basés sur PPP. Le LAC est l'émetteur des appels entrants et le destinataire des appels sortants.

Serveur réseau L2TP (LNS : L2TP Network Server)

Les serveurs réseau L2TP ou LNS peuvent fonctionner sur toute plate-forme prenant en charge la terminaison PPP. Le LNS gère le protocole L2TP côté serveur. Le protocole L2TP n'utilise qu'un seul support, sur lequel arrivent les canaux L2TP côté serveur. C'est pourquoi, les serveurs réseau LNS, ne peuvent avoir qu'une seule interface de réseau local (LAN) ou étendu (WAN). Ils sont cependant capables de terminer les appels en sortants et le destinataire des appels entrants. C'est le LNS qui sera responsable de l'authentification de tunnel.

PROTOCOLE IPSec

IPSec, définit par la référence RFC 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau IPv4 est largement déployé et la migration vers IPv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à IPv4 et IPv6. Ces mécanismes sont couramment désignés par le terme IPSec pour IP Security Protocol. IPSec est basé sur deux mécanismes et un protocole :

Le premier AH, pour Authentication Header vise à assurer l'intégrité et l'authentification des datagrammes IP. Il ne fournit pas, par contre aucune confidentialité : les données fournies et transmises par ce protocole ne sont pas encodées ;

Le second ESP, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement.

Enfin, le protocole IKE permet de gérer les échanges ou les associations notre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans IPSec.

a) Vue d'ensemble

Les mécanismes mentionnés ci-dessus font bien sûr appel à la cryptographie et utilisent donc un certain nombre de paramètres (algorithmes de chiffrement utilisés, clefs, mécanisme sélectionnés...) sur lesquels les tiers communicants doivent se mettre d'accord. Afin de gérer ces paramètres, IPSec a recours à la notion d'association de sécurité(SA). Une association de sécurité IPSec est une connexion simple qui fournit des services de sécurité au trafic qu'elle transporte. On peut aussi la considérer comme une structure de données servant à stocker l'ensemble des paramètres associés à une communication donnée. Une SA est unidirectionnelle ; en conséquence, protéger les deux sens d'une communication classique requiert deux associations, une dans chaque sens. Les services de sécurité sont fournis par l'utilisation soit de AH soit de ESP. Si AH et ESP sont tous deux appliqués au trafic en question, deux SA sont créés. Pour gérer les associations de sécurités actives, on utilise une base de données des associations de sécurités (Security Association Data, SAD). Elle contient tous les paramètres relatifs à chaque SA et sera consulter pour savoir comment traiter chaque paquet reçu ou à émettre. Les protections offertes par IPSec sont basées sur des choix définis dans une base de données de politique de sécurité(SPD). Cette base de données est établie et maintenue par un utilisateur, un administrateur système ou une application mise en place par ceux-ci. Elle permet de décider, pour chaque paquet, s'il se verra apporter des services de sécurité, s'il sera autorisé à passer ou à rejeter. Dans le cas où le paquet reçu est un paquet IP classique, la SPD permet de savoir s'il a néanmoins le droit de passer. Par exemple les paquets IKE sont une exception. Ils sont traités par IKE, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

b) L'Authentification Header (AH)

Est conçu pour assurer l'intégrité et l'authentification des datagrammes IP sans chiffrement des données. Le principe d'AH est d'adjoindre au datagramme IP classique un champ supplémentaire permettant à la réception de vérifier l'authenticité des données inclue dans le datagramme, en fonction du mode de fonctionnement utilisé

c) L'Encapsulating Security Payload (ESP)

ESP permet de combiner, à volonté, plusieurs services de sécurité. A savoir, la confidentialité des données par l'utilisation d'un système de chiffrement; l'authentification du paquet et de son émetteur (l'adresse source du paquet est celle de l'émetteur) ; l'intégrité des données (aucune altération volontaire ou non du paquet durant le transport) et l'unicité du paquet.

d) Principe de fonctionnement d'IPSec

On distingue deux situations :

- Trafic sortant

Lorsque la "couche" IPSec reçoit des données à envoyer, elle commence par consulter la base de données des politiques de sécurité (SPD) pour savoir comment traiter ces données. Si cette base lui indique que le trafic doit se voir appliquer des mécanismes de sécurité, elle récupère les caractéristiques requises pour la SA correspondante et va consulter la base des SA (SAD).

Si la SA nécessaire existe déjà, elle est utilisée pour traiter le trafic en question. Dans le cas contraire, IPSec fait appel à IKE pour établir une nouvelle SA avec les caractéristiques requises.

- Trafic entrant

Lorsque la couche IPSec reçoit un paquet en provenance du réseau, elle examine l'en-tête pour savoir si Ce paquet s'est vu appliquer un ou plusieurs services IPSec et si oui, quelles sont les références de la SA. Elle consulte alors la SAD pour connaître les paramètres à utiliser pour la vérification et/ou le déchiffrement du paquet. Une fois le paquet vérifié et/ou déchiffré, la Spd est consultée pour savoir si l'association de sécurité appliquée au paquet correspondait bien à celle requise par les politiques de sécurité.

Dans le cas où le paquet reçu est un paquet IP classique, la Spd permet de savoir s'il a néanmoins le droit de passer. Par exemple, les paquets IKE sont une exception. Ils sont traités par Ike, qui peut envoyer des alertes administratives en cas de tentative de connexion infructueuse.

e) La gestion des clefs pour IPSec : ISAKMP ET IKE

Les protocoles de sécurités présentés dans les paragraphes précédents ont recours à des algorithmes cryptographiques et ont donc besoin de clefs. Un des problèmes fondamentaux d'utilisation de la cryptographie est la gestion de ces clefs. Le terme gestion regroupe la génération, la distribution, le stockage et la suppression des clefs.

IKE (Internet Key Exchange) est un système développé spécifiquement pour IPSec qui vise à fournir des mécanismes d'authentification et d'échange de clef adaptés à l'ensemble des situations qui peuvent se présenter sur l'internet. IKE utilise ISAKMP pour construire un protocole pratique.

ISAKMP (Internet Security Association and Key Management Protocol) a pour rôle la négociation, l'établissement, la modification et la suppression des associations de sécurité et de leurs attributs. Il pose les bases permettant de construire divers protocoles de gestion des clefs (et plus généralement des associations de sécurité).

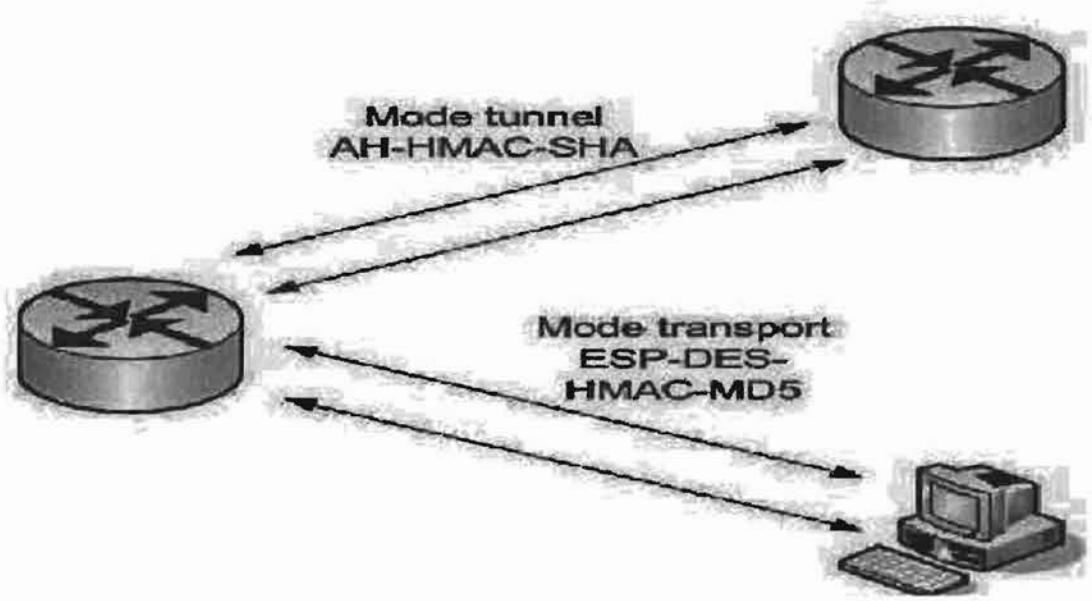
f) Modes de fonctionnement d'IPSec

On distingue trois modes :

Le mode transport ou transparent: Ce mode est utilisé pour créer une communication entre deux hôtes qui supportent IPSec. Une SA est établie entre les deux hôtes. Les entêtes IP ne sont pas modifiées et les protocoles AH et ESP sont intégrés entre cet entête et l'entête du protocole transporté. Ce modeste souvent utilisé pour sécuriser une connexion Point-To-Point.

Le mode tunnel : il est utilisé entre deux équipements dont au moins un n'est pas un équipement terminal ; les données peuvent être chiffrés (modes ESP) ou pas (mode AH). Il crée des tunnels en encapsulant chaque trame dans une enveloppe qui protège tous champs de trames.

Le mode Nesting : Le mode de Nesting utilise à la fois le mode transport et le mode tunnel : Un paquet IPSec et encapsule dans un paquet IPSec.



Source: tunnel_et _ vpn.pd

Figure 12 : Mode de fonctionnement d'IPSec

PROTOCOLE SSL (Secure Socket Layer)

SSL est un protocole de couche 4 (niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application. SSL a deux grandes fonctionnalités : l'authentification du serveur et du client à l'établissement de la connexion et le chiffrement des données durant la connexion.

SSL est le dernier arrivé dans le monde des VPN, mais il présente un gros avantage dans la mesure où côté client, il ne nécessite qu'un navigateur Internet standard. Ce protocole est celui qui est utilisé en standard pour les transactions sécurisées sur Internet.

PROTOCOLE MPLS (Multi-Protocol Label Switching)

Il se présente comme une solution aux problèmes de routage des datagrammes IP véhiculés sur Internet. Pour satisfaire les besoins des opérateurs de services VPN, la gestion de VPN-IP à l'aide des protocoles MPLS a été définie dans une spécification référencéeRFC 2547.

Des tunnels sont donc crées entre des routeurs MPLS et des périphériques appartenant à l'opérateur, et dédiés à des groupes fermés d'usagers particuliers, qui constituent des VPN. Dans l'optique MPLS/VPN, un VPN est un ensemble de sites placés sous la même autorité administrative, ou groupés suivant un intérêt particulier.

ANNEXE 2 : CONFIGURATION DU SERVEUR VPN

Nous allons voir comment mettre en place un serveur VPN PPTP sous Debian et Ubuntu avec authentification des utilisateurs via un AD (ou pas).

Cela va se passer en trois étapes:

1. Intégration de notre machine dans un domaine Active Directory
2. Installation et configuration du serveur VPN
3. Configuration de notre client VPN

Si vous souhaitez mettre en place un serveur VPN sans authentification Active Directory passez directement à la seconde étape.

1) Intégration de notre machine dans le domaine active directory

On installe ce qu'il faut:

```
apt-get install winbind samba smbclient krb5-user ntpdate
```

On met à l'heure le serveur:

```
ntpdate IP_de_votre_contrôleur_de_domaine
```

On configure SAMBA (Voir annexe 2)

On test l'intégration dans le demaine:

```
kinit compte_admin_du_domaine@DOMAINE.LAN (en majuscule)
```

Si il l'y a pas d'erreur c'est que c'est bon

On rajoute la machine dans le domaine:

```
net ads join -S serveur.domaine.lan -U compte_admin_du_domaine
```

On test avec la commande:

```
wbinfo -u
```

Si ça ne fonctionne pas refaites un:

```
/etc/init.d/smb restart
/etc/init.d/winbind restart
```

Voilà la machine est dans le domaine.

On configure l'authentification:
on édite le fichier « /etc/nsswitch.conf »

```
vim /etc/nsswitch.conf
```

Et on met ça dedans:

```
passwd:         compat winbind
group:          compat winbind
shadow:         compat

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

puis le fichier « /etc/pam.d/common-account »

```
vim /etc/pam.d/common-account
```

On met ça dedans:

```
account sufficient  pam_windind.so
account required    pam_unix.so
```

et encore le fichier « /etc/pam.d/common-auth » :

```
vim /etc/pam.d/common-auth
```

On met ça dedans:

```
auth    sufficient  pam_winbind.so krb5_auth krb5_ccache_type=FILE
auth    sufficient  pam_unix.so nullok_secure use_first_pass
auth    required    pam_deny.so
```

Puis le dernier « /etc/pam.d/common-session » :

```
vim /etc/pam.d/common-session
```

On met ça dedans:

```
session required    pam_unix.so
session required    pam_mkhomedir.so umask=0022 skel=/etc/skel
```

Et on reboot les services.

```
/etc/init.d/smb restart
/etc/init.d/winbind restart
```

2) Installation et configuration du serveur VPN

On installe le paquet pptpd

```
apt-get install pptpd
```

On édite le fichier « /etc/pptpd.conf »

```
vim /etc/pptpd.conf
```

On met ceci à la fin :

```
#La plage d'adresse ip fournis par le VPN sera de la forme 10.0.5.0
localip 10.0.5.0
#La plage d'adresse fournie sera de 10.0.5.2 à 10.0.5.10
remoteip 10.0.5.2-10
```

Vous pouvez bien sur configurer ce fichier comme bon vous semble

Puis on édite le fichier « /etc/ppp/pptpd-options »

```
vim /etc/ppp/pptpd-options
```

On s'assure que la configuration soit comme ceci :

```
name pptpd
refuse-pap
refuse-chap
refuse-mschap
require-mschap-v2
require-mppe-128
ms-dns adresse_du_DNS_fournis_par_le_vpn # dans mon cas IP de l'AD
proxyarp
nodefaultroute
```

Si vous ne souhaitez pas mettre en place une authentification via un Active Directory, éditez le « /etc/ppp/chap-secrets »

```
vim /etc/ppp/chap-secrets
```

Et rentrez les utilisateurs de la façon suivante:

```
#username pptpd password *
user1 pptpd userpass *
```

Si vous voulez permettre aux utilisateurs de votre Active Directory de se connecter avec leurs identifiants, rajoutez les lignes suivantes à la fin du fichier « /etc/ppp/pptpd-options ».

```
#Authentification avec les users de l'AD
plugin winbind.so
ntlm_auth-helper "/usr/bin/ntlm_auth --helper-protocol=ntlm-server-1"
```

Et pour finir, on redémarre les services pptpd

```
/etc/init.d/pptpd restart
```

Et voilà votre serveur VPN est configuré ;

3) Configuration d'un client

Adresse internet : IP sur serveur VPN
Nom : VPN
Nom d'utilisateur : « Username du fichier chap-secret ou de l'AD »
Mot de passe : « Mot de passe du fichier chap-secret ou de l'AD »
Domaine : DOMAINE.LAN

ANNEXE 3: CONFIGURATION DE SAMBA

Installation des paquetages nécessaires au serveur samba

Avant toute chose s'assurer que les paquetages nécessaires sont installer sinon les installer en tapant mcc (Centre de Contrôle Mandrake) en ligne de commande dans le terminal en se loggant en tant que root (taper su puis le mot de passe du root), aller dans Gestionnaire de Logiciels puis dans Installer, sélectionner les trois paquetages suivants (dans tous les paquetages, classement alphabétiques) :

```
samba-client-3.0.2a-3mdk
samba-common-3.0.2a-3mdk
samba-server-3.0.2a-3mdk
```

Puis cliquer sur Installer.

Premier démarrage de Samba

Après installation, le serveur de Samba devrait normalement être apte à démarrer (sans aucun partage de fichiers ou d'imprimante) en lançant la commande suivante:

```
/etc/rc.d/init.d/smb start
Starting SMB services: [OK]
Starting NMB services: [OK]
```

La commande suivante permet de contrôler que les deux démons sont correctement lancés `/etc/rc.d/init.d/smb status` (ou service smb status)

```
smbd (pid 1054) is running...
nmbd (pid 1056) is running...
```

Les commandes utiles

(à partir du terminal en root)

- `testparm /etc/samba/smb.conf`
  - Test de syntaxe d'écriture du fichier smb.conf
- `/etc/rc.d/init.d/smb stop`
  - Stop les services Samba
- `/etc/rc.d/init.d/smb start`
  - Démarre le serveur Samba
- `/etc/rc.d/init.d/smb restart`
  - Redémarrage de Samba
- `/smbstatus`
  - Affiche les connexions actives via Samba

Configuration du fichier smb.conf

La configuration de Samba est effectuée par l'intermédiaire d'un fichier de configuration unique: smb.conf. Ce fichier est située dans le répertoire /etc/samba/
Remarque : à chaque modification du fichier smb.conf à l'aide d'un éditeur de texte, l'enregistrer puis taper en ligne de commande :
`/etc/rc.d/init.d/smb restart` (afin de redémarrer le serveur samba et par la même occasion prendre en compte les modifications du fichier smb.conf).

Ce fichier décrit les ressources que l'on désire partager, ainsi que les permissions/restrictions qui leur sont associées. Le fichier smb.conf se découpe selon des rubriques (chacune référencé par une ligne contenant le nom de la section entre crochets) comprenant chacune un ensemble de lignes de paramètres du type attribut = valeur. Une ligne commençant par un # est une ligne de commentaires et une ligne commençant par ; est inactive.
Il existe 3 sections principales:

- La section [global]
  - définit des paramètres généraux sur le serveur
- La section [homes]
  - définit le partage d'un répertoire personnel
- La section [printers]
  - définit les imprimantes partagées par le serveur

Section "global"

Voici un exemple (l'exemple est celui du réseau R2D4) de section [global] :
[global]

même nom de groupe que celui sous Windows (Voisinage réseau)
```
workgroup = DRO_SONABEL
```

nom sous lequel apparaîtra le serveur dans le voisinage réseau
```
netbios = samba server
```

ce qui apparaîtra dans la rubrique détail du voisinage réseau, %v fait
apparaître le n° de version de samba
```
server string = Samba Server %v
```

les mots de passe transitent cryptés
```
encrypt passwords = Yes
smb passwd file = /etc/samba/smbpasswd
```

lieux de stockage du journal des événements
```
log file = /var/log/samba/log.%m
```

taille maximum du journal
```
max log size = 50
```

aucun compte invité (facultatif)
```
guest account = nobody
```

accès multi-utilisateur (facultatif)
```
Share modes = yes
```

emplacement du fichier printcap (imprimantes sur le serveur Linux)
```
printcap = /etc/printcap
```

partage de toutes les imprimantes définies dans printcap
```
printcap name = cups
```

```
load printers = yes
printing = cups
printer adm = @adm

# fichier journal de Samba
log level = 1
log file = /var/log/samba/log.%m

# mode de sécurité : (user / share / server)
security = user

# Autoriser l'accès à certains réseaux (le point final est important)
hosts allow = 192.168.1.

# Vous pouvez autoriser toutes les machines de ce réseau sauf 192.168.1.10
hosts allow = 192.168.1. EXCEPT 192.168.1.10

# Mettre les adresses IP des machines auxquelles vous souhaitez interdire l'accès
# au serveur samba par exemple : ALL, pour interdire tout le monde sauf les
# machines autorisées par <hosts allow>.
Hosts deny = ALL

# pas de proxy dns
dns proxy = No

# Laisser ce champs par défaut
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

# active le fonction de serveur de temps
time server = yes

# le script de connexion porte le nom du groupe, %g est la variable samba pour le
# groupe primaire
logon script = %g.bat

# autorise la connexion des utilisateurs sur le domaine
domain logons = yes

# Si on veut que le serveur soit le maître du domaine
domain master = yes

# dans le cas de la présence de plusieurs contrôleurs de domaine, c'est le
# serveur qui est le favori
preferred master = yes

# En cas de serveur maître permet de gagner l'élection contre les autres machines
# windows os level = 255
# on donne l'accès au répertoire netlogon qui contient les scripts de démarrage
[netlogon]
path = /home/net
#chemin d'accès du répertoire
logon
```

seuls les utilisateurs spécifiés peuvent utiliser ce répertoire
```
public = no
```

on ne peut pas écrire dans ce répertoire
```
writable = no
```

le répertoire n'apparaît pas dans l'arborescence
```
browseable = no
```

#liste des utilisateurs ayant les droits root sur ce répertoire
```
admin users = sonabel
```

Section "homes"

Partage du répertoire personnel
La section [homes] permet de définir l'accès au répertoire personnel de chaque utilisateur.
Voici un exemple de section:

[HOMES]
commentaire visible depuis le voisinage réseau
```
comment = Home Directories
```

affichage de la ressource pour tous
```
browseable = no
```

possibilité d'écrire sur la ressource
```
writable = yes
```

Section "documents"

Partager un répertoire quelconque
Il est possible de définir un accès personnalisé à n'importe quel répertoire de la machine en créant une section portant le nom que le veut donner à la ressource. Celui-ci contiendra entre autres un paramètre path donnant le chemin d'accès à la ressource.
Ce répertoire sera consultable en lecture et en écriture sur la station Windows suivant l'utilisateur loggé.
Voici un exemple de section personnalisée:

[DOCUMENTS]
commentaire visible depuis le voisinage réseau
```
comment = /home/Répertoire_quelconque
```

chemin d'accès à la ressource
Attention à la casse !!
```
path = /home/Répertoire_quelconque
```

affichage de la ressource pour tous
```
browseable = no
guest ok = yes
```

mettre les noms d'utilisateurs qui seront validés, la procédure pour les
insérer sera expliquée ultérieurement
```
valid users = noms_utilisateurs
```

chemin d'acces a la ressource
#etant donné que des utilisateurs insérés pourront y accéder il faut mettre no
```
public = no
```

utilisateurs ayant les droits root sur ce répertoire
```
admin users = noms_utilisateurs
```

possibilité d'écrire sur la ressource
```
writable = yes
```
Section "cdrom"

Partage d'un lecteur de CD-ROM
Il est ainsi possible de partager un lecteur de CD-ROM (celui-ci devant être préalablement monté), en créant par exemple une section [cd-rom] comme suit:

[CD-ROM]
commentaire visible depuis le voisinage réseau
```
comment = lecteur de CD-ROM
```

chemin d'accès au lecteur
```
path = /mnt/cdrom
```

accessible à tous
```
public = yes
```

impossibilité d'écrire sur la ressource
```
writable = no
```

```
create mask = 0750
```
Accéder à une ressource Samba sous linux

Le client Samba (smbclient) permet de fournir une interface en ligne de commande pour accéder aux ressources Samba à partir d'une machine de type Unix.
smbclient permet en premier lieu de vérifier l'existence d'une serveur Samba sur le réseau et de lister les ressources qu'il partage grâce à la commande:
smbclient nom_serveur_smb
Une fois les ressources identifiées, il est possible d'accèder à chacune d'entre elles par la commande:
```
smbclient \\\\nom_serveur_smb\\ressource -U nom_utilisateur
```
Un mot de passe devrait être demandé à l'utilisateur. Il suffit ensuite d'envoyer des commandes FTP afin d'envoyer/recevoir des fichiers ou bien de parcourir les répertoires de la ressource.
L'accès à une imprimante se fait par la commande
```
smbclient \\\\nom_serveur_smb\\ressource -P
```
l'impression du fichier /usr/local/samba/lib/etc.conf se fait par la commande:
```
print /usr/local/samba/lib/etc.conf
```
la visualisation de la queue d'impression:
```
queue
```
l'arrêt de smbclient:
```
exit
```

Remarque : Pour accéder au voisinage réseau sous Linux, ouvrir Konqueror et taper dans la barre d'URL : smb:/

Création des utilisateurs Samba et accès aux comptes de ces utilisateurs

Créer un utilisateur sur la machine serveur Samba sous Linux Mandrake version 10 (serveur) :

Graphiquement

En ligne de commande taper mcc en se loggant en tant que root (ou passer par le menu « configure your computer »), nous voilà dans le Centre de Contrôle Mandrake , ensuite aller dans « système » puis « Utilisateurs et groupes » enfin « ajouter utilisateur ».

En ligne de commande taper

```
adduser Nom_Utilisateur
```

Ensuite entrer le mot de passe de l'utilisateur dans le fichier smbpasswd dans le répertoire /etc/samba de la manière suivante (en ligne de commande):

```
smbpasswd -a Nom-Utilisateur
```

En réponse :
New SMB password : Donner le même mot de passe que lors de l'ajout de l'utilisateur
Retype new SMB password :idem

Créer le même utilisateur avec le même passe sur la machine Windows (Client) :

Aller dans « panneau de configuration » puis dans compte utilisateur pour créer un utilisateur avec les droits « administrateur »

Renouveler autant de fois l'opération précédente qu'il y a d'utilisateur à créer.

Remarque : En cas d'utilisateurs déjà existant sur la machine Windows, le recréer uniquement sur le serveur Linux et surtout ne pas renommer un utilisateur, soit il est déjà existant soit il faut le créer. A chaque création d'utilisateur sous windows, redémarrage de la station.

Le partage de répertoires

Il y a le partage du répertoire personnel, qui affiche les répertoires selon l'utilisateur logué et il y a le partage d'un répertoire commun.
Attention, si on partage un répertoire ne se trouvant pas dans l'arborescence « Home », tout accès sera refusé, donc le répertoire « Home » ou un de ses sous-répertoires doit contenir ce répertoire commun pour un usage optimal de celui-ci.

Les messages d'erreurs

Des messages d'erreurs du type suivant peuvent provenir :

Problèmes : Réseau introuvable (sous Windows)
ou encore :
Internal Error
Please send a full bug at http://kde.org
Unknown error condition in stat : Network is unreahable (sous Linux)
Ce type d'erreur signifie que vous n'êtes pas connecté à un réseau, branchement, câbles réseau à vérifier, configuration réseau et fichier /etc/samba/smb.conf à vérifier également.

Si un message d'erreur tel que :

Impossible de se connecter au serveur samba est affiché, dans ce cas vérifier la configuration du fichier /etc/samba/smb.conf.
Le serveur Samba s'affiche au sein du domaine mais affiche le message d'erreur suscité lorsque l'on clique dessus, dans ce cas vérifier le chemin du répertoire de partage quelconque ou personnel dans le fichier smb.conf.

ANNEXE 4: CONFIGURATION DE NIS

Installation

Sur le serveur maître lancez cette commande pour installer les paquets nécessaires au fonctionnement de NIS:

```
# yum install yp-tools ypbind ypserv portmap
```

Les paquets sont désormais installés, passons à la configuration du serveur NIS.

Configuration

Tout d'abord nous devons inclure le serveur maître dans le domaine NIS, pour cela éditons le fichier /etc/sysconfig/network:

```
# vi /etc/sysconfig/network
```

Ajoutons cette ligne à la fin du fichier:

```
NISDOMAIN="mydomain.com"
```

Nous déclarons le serveur maître comme client NIS lui-même en éditant le fichier /etc/yp.conf:

```
# vi /etc/yp.conf
```

Nous ajoutons à ce fichier cette ligne, 127.0.0.1 correspondant à la boucle locale:

```
ypserver 127.0.0.1
```

Cette partie étant configurée, nous pouvons démarrer les services portmap (convertit les numéros de programmes RPC en numéros de port logiciel DARPA), yppasswdd (démon permettant de changer le mot de passe d'un utilisateur sur le serveur maître NIS depuis le client NIS) et ypserv (démon principal du serveur NIS).

```
    # service portmap start
# service yppasswdd start
# service ypserv start
```

N'oublions pas d'ajouter ces services au démarrage de la machine:

```
# chkconfig portmap on
# chkconfig yppasswdd on
on
# chkconfig ypserv on
```

Pour vérifier que les services fonctionnent correctement, lancez la commande rpcinfo et vérifiez que chaque processus y est listé :

```
# rpcinfo -p localhost
program vers proto   port
 100000    2   tcp    111  portmapper
 100000    2   udp    111  portmapper
 100009    1   udp    681  yppasswdd
 100004    2   udp    698  ypserv
 100004    1   udp    698  ypserv
 100004    2   tcp    701  ypserv
 100004    1   tcp    701  ypserv
```

Attention! ypbind et ypxfrd ne fonctionnent pas tant que le domain NIS n'est pas correctement configuré.

Maintenant initialisons notre domaine NIS en exécutant l'utilitaire ypinit:

```
    # /usr/lib64/yp/ypinit -m
At this point, we have to construct a list of the hosts which will run NIS
servers. centos-nis-1 is in the list of NIS server hosts.  Please continue
to add
the names for the other hosts, one per line.  When you are done with the
list, type a "">.
        next host to add:  centos-nis-1
        next host to add:
The current list of NIS servers looks like this:

centos-nis-1

Is this correct?  [y/n: y]  y
We need a few minutes to build the databases...
Building /var/yp/mydomain.com/ypservers...
Running /var/yp/Makefile...
gmake[1]: Entering directory `/var/yp/mydomain.com'
Updating passwd.byname...
Updating passwd.byuid...
Updating group.byname...
Updating group.bygid...
Updating hosts.byname...
Updating hosts.byaddr...
Updating rpc.byname...
Updating rpc.bynumber...
Updating services.byname...
Updating services.byservicename...
```

```
Updating netid.byname...
Updating protocols.bynumber...
Updating protocols.byname...
Updating mail.aliases...
gmake[1]: Leaving directory `/var/yp/mydomain.com'

centos-nis-1 has been set up as a NIS master server.

Now you can run ypinit -s centos-nis-1 on all slave server.
```

Notre domaine NIS est configuré, démarrons les services ypbind (démon client NIS) et ypxfrd (démon permettant l'accélération du transfert des cartes NIS volumineuses):

```
 # service ypbind start
# service ypxfrd start
```

Ajoutons les services au démarrage de la machine :

```
 # chkconfig ypbind on
# chkconfig ypxfrd on
```

Une fois de plus, vérifions que les services fonctionnent correctement :

```
  # rpcinfo -p localhost
  program vers proto   port
   100000    2   tcp    111  portmapper
   100000    2   udp    111  portmapper
   100003    2   udp   2049  nfs
   100003    3   udp   2049  nfs
   100021    1   udp   1024  nlockmgr
   100021    3   udp   1024  nlockmgr
   100021    4   udp   1024  nlockmgr
   100004    2   udp    784  ypserv
   100004    1   udp    784  ypserv
   100004    2   tcp    787  ypserv
   100004    1   tcp    787  ypserv
   100009    1   udp    798  yppasswdd
600100069    1   udp    850  fypxfrd
600100069    1   tcp    852  fypxfrd
   100007    2   udp    924  ypbind
   100007    1   udp    924  ypbind
   100007    2   tcp    927  ypbind
   100007    1   tcp    927  ypbind
```

Le serveur maître NIS est maintenant installé et configuré, installons un serveur esclave NIS (facultatif, tout dépend de votre architecture réseau).

Installation

Lancez cette commande pour installer les paquets nécessaires au fonctionnement du serveur esclave NIS:

```
# yum install yp-tools ypbind ypserv portmap
```

Les paquets sont désormais installés, passons à la configuration du serveur esclave NIS.

Configuration

Modifions les fichiers hosts afin d'avoir une entrée entre chaque noeud NIS.

Sur le serveur maître NIS (centos-nis-22 n'est qu'un exemple, nous n'avons dans le tutorial qu'un serveur esclave):

```
# vi /etc/hosts
192.168.0.201   centos-nis-2 #the NIS slave server number 1
192.168.0.221   centos-nis-22 #the NIS slave server number 22
```

Sur le serveur esclave NIS:

```
# vi /etc/hosts
192.168.0.200   centos-nis-1 #the NIS master server
```

Revenons à la configuration propre au serveur esclave, lui aussi doit être déclaré lui-même comme client NIS:

```
# vi /etc/yp.conf
ypserver 127.0.0.1
```

Comme pour le serveur maître, nous intégrons le serveur esclave dans le domaine NIS:

```
# vi /etc/sysconfig/network
NISDOMAIN="mydomain.com"
```

Démarrons les services portmap, ypbind et ypxfrd sur le serveur esclave:

```
# service portmap start
# service ypbind start
# service ypxfrd start
```

Et ajoutons les au démarrage de la machine:

```
# chkconfig portmap on
# chkconfig ypbind on
# chkconfig ypxfrd on
```

Pour vérifier que la configuration fonctionne correctement, nous allons interroger le serveur maître pour savoir quel serveur est le serveur maître, via l'outil ypwhich:

```
# ypwhich -m
mail.aliases centos-nis-1
group.bygid centos-nis-1
passwd.byuid centos-nis-1
rpc.bynumber centos-nis-1
...
...
```

Nous procédons maintenant à un téléchargement initial de la base de données NIS (stockée sur le serveur maître):

```
# /usr/lib64/yp/ypinit -s centos-nis-1
We will need a few minutes to copy the data from centos-nis-1.
Transferring services.byservicename...
Trying ypxfrd ... success

Transferring group.byname...
Trying ypxfrd ... success
...
...

centos-nis-2's NIS data base has been set up.
If there were warnings, please figure out what went wrong, and fix it.

At this point, make sure that /etc/passwd and /etc/group have
been edited so that when the NIS is activated, the data bases you
have just created will be used, instead of the /etc ASCII files.
```

Nous avons désormais téléchargé la carte NIS, nous pouvons démarrer le service qui répondra aux clients NIS, sur le serveur esclave, et l'ajouter au démarrage:

```
# service ypserv start
Starting YP server services:
# chkconfig ypxfrd on
```

Sur le serveur maître, nous enregistrons les serveurs esclaves dans le fichier ypservers:

```
# vi ypservers
```

```
#
# File: /var/yp/ypservers
#
centos-nis-1
centos-nis-22
```

Toujours sur le serveur maître, nous configurons le fichier Makefile pour qu'il pousse sa carte NIS aux serveurs esclaves. Mais n'oublions pas de sauvegarder le fichier Makefile au préalable:

```
# cp /var/yp/Makefile /var/yp/Makefile.bak
# vi /var/yp/Makefile
NOPUSH=false
```

Nous poussons maintenant la carte aux serveurs listés dans /var/yp/ypservers:

```
# make
gmake[1]: Entering directory `/var/yp/mydomain.com'
Updating ypservers...
YPPUSH: gethostbyname(): Success
YPPUSH: using not FQDN name
gmake[1]: Leaving directory `/var/yp/mydomain.com '
gmake[1]: Entering directory `/var/yp/mydomain.com'
Updating netid.byname...
YPPUSH: gethostbyname(): Success
YPPUSH: using not FQDN name
gmake[1]: Leaving directory `/var/yp/mydomain.com'
```

Afin d'éviter un oubli de mise à jour, nous allons ajouter 3 scripts qui vont périodiquement télécharger la base de données depuis le serveur maître, ajoutons donc ceci sur les serveurs esclaves:

```
# vi /etc/cron.d/nis_sync
```

```
#
# File: /etc/cron.d/nis_sync
#
20 *    * * *    /usr/lib64/yp/ypxfr_1perhour
40 6    * * *    /usr/lib64/yp/ypxfr_1perday
55 6,18 * * *    /usr/lib64/yp/ypxfr_2perday
```

Redémarrons cron:

```
# service crond restart
```

Les serveurs maître et esclave sont maintenant configurés, nous pouvons passer à la configuration des clients NIS.

Installation

Tout d'abord, installons les paquets nécessaires sur la machine cliente:

```
# yum install yp-tools ypbind portmap
```

Les paquets sont désormais installés, passons à la configuration de NIS sur la machine cliente.

Configuration

Lançons la commande authconfig. Cette commande va configurer le système pour utiliser le service NIS. Remplacez les arguments nisdomain, nisserver par les valeurs propres à votre infrastructure. Si je souhaite associer ma machine au serveur NIS esclave, j'indique alors l'adresse IP sur serveur esclave pour l'argument nisserver.

```
# authconfig --enableshadow --enablenis --nisdomain=mydomain.com --
nisserver=192.168.0.200 -update
```

Démarrons les services portmap et ypbind sans oublier de les ajouter au démarrage de la machine:

```
# service portmap start
Starting portmapper: [  OK  ]
# service ypbind start
Binding to the NIS domain:
Listening for an NIS domain server.
# chkconfig ypbind on
# chkconfig portmap on
```

Pour vérifier l'accès au serveur NIS, lançons la commande ypcat passwd, qui va lister les entrées passwd du serveur maître. Les utilisateurs test, test2, test3, test4 ont été créés sur le serveur maître spécifiquement pour vérifier que le client les liste:

```
# ypcat passwd
test:$1$TqofoiOE$TwWUHrJDTFHcaSAg2qFQC0:500:500::/home/test:/bin/bash
test2:$1$sLUwtdB6$32n6IK2OqY1dbFCdW7BU21:501:501::/home/test2:/bin/bash
test3:$1$.XHW.qNf$3R0QIk48Sdrtou5c4RU/t/:502:502::/home/test3:/bin/bash
test4:$1$R/vbkqcX$YeGEGm3mocjTfm3Y./07T0:503:503::/home/test4:/bin/bash
```

Maintenant vous pouvez vous authentifier à la machine cliente via SSH (par exemple) en utilisant les comptes utilisateurs créés sur le serveur maître NIS. Attention toutefois, vous n'aurez pas de dossier /home pour votre utilisateur sur les machines clientes (sauf dans le cas d'une intégration de partages NFS), vous pouvez y rémédier avec les commandes suivantes lancées sur la machine cliente, mais les dossiers ne seront pas synchronisés:

```
# mkdir /home/test4
# chmod 700 /home/test4/
# ll /home
total 2
drwx------    2 test4 users    1024 Aug  4 08:05 test4
# cp /etc/skel/.* /home/test4/
cp: omitting directory `/etc/skel/.'
cp: omitting directory `/etc/skel/..'
cp: omitting directory `/etc/skel/.kde'
# chown -R test4:users /home/test4
```

Vous pouvez également essayer de pinger une machine inscrite sur le fichier hosts du serveur maître NIS:

```
# ping centos-nis-4
PING centos-nis-4.mydomain.com (192.168.0.203) 56(84) bytes of data.
64 bytes from centos-nis-4.mydomain.com (192.168.0.203): icmp_seq=1 ttl=64
time=0.643 ms
--- centos-nis-4.mydomain.com ping statistics ---
1 packet transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.512/0.652/0.735/0.091 ms
```

Le client NIS est maintenant configuré.

Ce qui suit est une fiche permettant l'exploitation et le diagnostic du service NIS.

Les fichiers de configuration

/etc/sysconfig/network : Ce fichier doit contenir une association au domain NIS que vous avez créé. Voici un exemple:

```
NISDOMAIN="mydomain.com"
```

/etc/yp.conf : Ce fichier contient le nom du serveur à partir duquel cette machine obtient ses information NIS.

Exemple sur un serveur maître ou esclave (le serveur NIS est donc lui-même):

```
ypserver 127.0.0.1
```

Exemple sur un client (le serveur NIS est un serveur maître ou esclave):

```
domain interact-iv.com server 192.168.0.200
```

/etc/nsswitch.conf : Ce fichier contient l'ordre dans lequel certaines sources de données doivent être interrogées. Ce fichier est utilisé pour les résolutions de noms, les authentifications, ... Nous devons retrouver "nis" au moins pour les lignes passwd, shadow,

group et hosts. On peut le placer avant "files" en fonction de la priorité que vous souhaitez attribuer à NIS.

```
passwd:     files nis
shadow:     files nis
group:      files nis

hosts:      files nis dns
```

/etc/hosts : Ce fichier contient des informations différentes en fonction du rôle de la machine.

Le client NIS doit retrouver une référence au serveur NIS (maître ou esclave) dans ce fichier:

```
192.168.0.200   centos-nis-1
```

Le serveur esclave NIS doit retrouver une référence au serveur maître NIS dans ce fichier:

```
192.168.0.200   centos-nis-1
```

Le serveur maître NIS doit retrouver une référence à tous ses serveurs esclaves NIS dans ce fichier:

```
192.168.0.201   centos-nis-2
192.168.0.221   centos-nis-22
```

/var/yp/Makefile : Ce fichier définit comment le serveur NIS va construire sa base de données, sa carte NIS et comment le serveur maître va se lier aux serveurs esclaves. Dans notre tutorial nous allons garder la configuration par défaut, à l'exception de l'argument "NOPUSH" qui sera désactivé afin de pousser les données vers les serveur esclaves:

```
#
# File: /var/yp/Makefile
#


#
# Allow the master to do database pushes to the slave
#
NOPUSH=false
```

/etc/cron.d/nis_sync : Ce fichier a été créé durant l'installation. Il est seulement présent sur les serveurs esclaves pour se lancer périodiquement et télécharger la base de données NIS depuis le serveur maître. Le script est dans notre cas lancé chaque heure et une et deux fois par jour:

```
#
# File: /etc/cron.d/nis_sync
```

```
#
20 *     * * *     /usr/lib/yp/ypxfr_1perhour
40 6     * * *     /usr/lib/yp/ypxfr_1perday
55 6,18 * * *     /usr/lib/yp/ypxfr_2perday
```

Diagnostic

Processus-clés:

portmap : le démon RPC à partir duquel NIS fonctionne. Lancé sur client, serveurs maître et esclave NIS.

yppasswdd : le démon permettant de changer les mots de passe utilisateur sur le serveur NIS maître depuis le client NIS. Lancé sur serveur maître NIS.

ypserv : le démon serveur NIS principal. Lancé sur serveurs maître et esclave NIS.

ypbind : le démon client NIS. Lancé sur client, serveurs maître et esclave NIS.

ypxfrd : démon utilisé pour accélérer le transfert des cartes NIS très volumineuses. Lancé sur serveurs maître et esclave NIS.

Diagnostic RPC:

Avec cette table, vous pouvez vérifier si les processus NIS sont lancés et écoutent correctement. La commande fonctionne sur une machine cliente ou serveur:

```
[root@centos-nis-1 tmp]# rpcinfo -p localhost
   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100009    1   udp    681  yppasswdd
    100004    2   udp    698  ypserv
    100004    1   udp    698  ypserv
    100004    2   tcp    701  ypserv
    100004    1   tcp    701  ypserv
```

Test de connexion à distance:

Vous pouvez tester l'authentification via NIS en vous connectant par SSH ou Telnet sur une machine cliente. N'oubliez pas qu'une erreur de connexion peut souvent être liée à une règle de pare-feu manquante! NIS fonctionne via RPC, qui écoute sur le port 111.

Connexion via Telnet:

```
[root@centos-nis-1 tmp]# telnet 192.168.0.202
Trying 192.168.1.202...
Connected to 192.168.1.202.
```

```
Escape character is '^]'.
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6 on an i686
login: test4
Password:
Last login: Fri Aug 6 16:13:32 from 192-168-0-200.mydomain.com
```

Connexion via SSH

```
[root@ tmp]# ssh -l test4 192.168.0.202
test4@192.168.0.202's password:
[test4@centos-nis-3 test4]$
```

Fichiers de log:

NIS écrit des logs par défaut dans /var/log/messages ou /var/log/syslog, en fonction de votre configuration syslog. N'oubliez pas de vérifier ces fichiers en cas de souci!

Gestion des utilisateurs

Changement de mot de passe:

Voici la procédure pour changer le mot de passe d'un utilisateur.

Connectez-vous sur une machine cliente (ne surtout pas modifier le mot de passe sur le serveur maître directement!):

```
[test4@centos-nis-1 test4]$ yppasswd -p test4
Changing NIS account information for test4 on centos-nis-1.mydomain.com.
Please enter old password:
Changing NIS password for test4 on centos-nis-1.mydomain.com.
Please enter new password:
Please retype new password:

The NIS password has been changed on centos-nis-1.mydomain.com.

[test4@centos-nis-1 test4]$
```

Ajout d'un utilisateur:

Voici la procédure pour ajouter un utilisateur. Sur le serveur maître:

```
[root@centos-nis-1 tmp]# useradd -g users test5
[root@centos-nis-1 tmp]# passwd test5
Changing password for user test5.
New password:
```

```
Retype new password:
passwd: all authentication tokens updated successfully.
[root@centos-nis-1 tmp]# cd /var/yp
[root@centos-nis-1 yp]# make
gmake[1]: Entering directory `/var/yp/mydomain.com'
Updating passwd.byname...
Updating passwd.byuid...
Updating netid.byname...
gmake[1]: Leaving directory `/var/yp/mydomain.com'
[root@centos-nis-1 yp]#
```

Vous pouvez vérifier que l'authentification de l'utilisateur a été mise à jour en utilisant la commande "ypmatch" qui va retourner la chaîne contenant le mot de passe chiffré de l'utilisateur:

```
[root@centos-nis-1 yp]# ypmatch test5 passwd
test5:$1$d6E2i79Q$wp3Eo0Qw9nFD/::504:100::/home/test5:/bin/bash
```

Vous pouvez également utiliser la commande "gentent" qui a une syntaxe similaire. Contrairement à ypmatch, gentent ne fournit pas le mot de passe chiffré lorsqu'il est lancé sur le serveur NIS. Il fournit juste l'entrée de l'utilisateur dans le fichier /etc/passwd. Sur un client NIS, le résultat est identique, les deux commandes montrant le mot de passe chiffré.

```
[root@centos-nis-1 yp]# getent passwd test5
test5:x:504:100::/home/test5:/bin/bash
```

Résolution de problèmes

- Pendant "ypinit", si vous obtenez l'erreur suivante:

  ```
  failed to send 'clear' to local ypserv: RPC: Port mapper failure
  Updating group.bygid...
  ```

- Supprimez le dossier /var/yp/mydomain.com et redémarrez portmap, yppasswdd et ypserv sur le serveur maître.

- Sur le serveur esclave, pendant "ypinit", si votre base de données est corrompue ou que votre fichier /etc/hosts est incorrect, vous obtiendrez une erreur d'énumération de la carte "Can't enumerate maps from centos-nis-1. Please check that it is running.". Utilisez la commande "make" dans /var/yp sur le serveur maître pour reconstruire la base de données NIS.
- Lancer la commande yppasswdd sur le mauvais client ou serveur (en fonction de la configuration de vos serveurs maître et esclave), peut causer des erreurs de segmentation. Voici des exemples de commandes qui retournent ces erreurs:

  ```
  [nisuser@centos-nis-3 test4]$ yppasswd
  Segmentation fault
  ```

```
[root@centos-nis-3 root]# yppasswd -p test4
Segmentation fault
```

- Le démon yppasswdd doit être lancé sur le client et le serveur pour lors des changements de mots de passe pour fonctionner correctement. Si le démon n'est pas démarré d'un côté ou de l'autre, vous obtiendrez cette erreur:

```
        [root@centos-nis-3 etc]# yppasswd -p test4
yppasswd: yppasswdd not running on NIS master host ("centos-nis-1").
```

- Utilisez toujours les commandes ypmatch, ypwhich, getent pour vérifier la connectivité NIS. Si une erreur survient, vérifiez les étapes de ce tutorial et cette page de diagnostic, vous devriez trouver d'où vient la source de votre problème.
- N'oubliez pas de créer un dossier home à chaque utilisateur, définissez ses permissions et copiez le fichier /etc/skel. Si vous oubliez, vos utilisateurs n'auront pas la possibilité de créer des fichiers dans leur dossier home et vous risquez d'obtenir des erreurs à l'authentification.
- Et comme rappelé plus haut, n'oubliez pas de vérifier vos fichiers de logs, ils contiennent souvent l'information qui vous permettra de résoudre votre problème!

ANNEXE 5: CONFIGURATION DU DHCP

Installation du serveur

Les paquets sont déjà installés.

Attention : vous pouvez avoir sur votre distribution, plusieurs serveurs DHCP.

dhcpxd est conforme à la RFC 2131. Il fournit un exemple de configuration assez détaillé.

dhcp3, intègre l'inscription auprès d'un DNS Dynamique. Par contre si vous n'avez pas de DNS dynamique sur le réseau, vous devrez mettre en entête du fichier `dhcpd.conf`, la ligne :

```
ddns-update-style none;
```

Configuration du serveur

La configuration consiste à créer 2 fichiers :

- `/etc/dhcp3/dhcpd.conf`, ce fichier sert à la configuration même du serveur (plage d'adresses, paramètres distribués),
- `/var/lib/dhcp3/dhcpd.leases`, ce fichier va servir à l'inscription des clients. Chaque client DHCP, génère l'écriture d'un enregistrement dans ce fichier. Cela permet le suivi, les statistiques de l'activité du serveur.

Le fichier de configuration dhcpd.conf

Vous pouvez créer ce fichier avec un éditeur.

```
$>more dhcpd.conf

# ici il s'agit du réseau 192.168.0.0
subnet 192.168.0.0 netmask 255.255.255.0 {

#La plage d'adresse disponible pour les clients
range 192.168.0.10 192.168.0.20;

# Les clients auront cette adresse comme passerelle par défaut
option routers     192.168.0.254;

# Ici c'est le serveur de noms, on peut en mettre plusieurs
option domain-name-servers    192.168.0.1;

# Enfin on leur donne le nom du domaine
option domain-name    "freeduc-sup.org";

# Et l'adresse utilisée pour la diffusion
option broadcast-address 192.168.0.255;

# Le bail à une durée de 86400 s par défaut, soit 24 h
# On peut configurer les clients pour qu'ils puissent demander
# une durée de bail spécifique
default-lease-time  86400;

# On le laisse avec un maximum de 7 jours
```

```
max-lease-time 604800;

#Ici on désire réserver des adresses à des machines
group {
#use-host-decl-names indique que toutes les machines dans l'instruction «
group »
# auront comme nom, celui déclaré dans l'instruction host.
use-host-decl-names true ;

# ici définir les machines
host m1 {
hardware ethernet 00:80:23:a8:a7:24;
fixed-address 192.168.0.125;
} # End m1

host m2 {
hardware ethernet a0:81:24:a8:e8:3b;
fixed-address 192.168.0.126;
} # End m2

    } # End Group
}     # End dhcp.conf
```

Création d'un fichier d'inscription

Ce fichier doit parfois être créé, sans quoi le serveur DHCP ne pourra pas démarrer. Il suffit de créer un fichier vide. Pour cela, saisissez la commande:

`touch /var/lib/dhcp3/dhcpd.leases`. Le fichier est créé. Voici ce qu'il peut contenir après l'inscription du premier client :

```
[root@master /etc]# more /var/lib/dhcp3/dhcpd.leases

lease 192.168.0.10 {

 starts 1 2002/12/14 18:33:45;

 ends 1 2002/12/14 18:34:22;

 hardware ethernet 00:40:33:2d:b5:dd;

 uid 01:00:40:33:2d:b5:dd;

 client-hostname "CHA100";

}
```

On distingue les informations suivantes : Début du bail, Fin du bail, adresse MAC du client, le nom d'hôte du client. Attention ce nom est différent du nom Netbios utilisé sur les réseaux Microsoft.

Activation du serveur

Le serveur est configuré, il n'y a plus qu'à le mettre en route. Utilisez la commande suivante pour arrêter ou activer le service : **`/etc/init.d/dhcpd3 start | stop`**.

Le script lance le serveur en mode daemon. Vous pouvez le lancer en avant plan avec la commande `dhcpd3 -d`. Cela permet de voir les messages et déterminer s'il y a des disfonctionnement éventuels.

```
root@master:/etc/dhcp3# dhcpd3 -d

Internet Software Consortium DHCP Server V3.0.1rc9

Copyright 1995-2001 Internet Software Consortium.

All rights reserved.

For info, please visit http://www.isc.org/products/DHCP

Wrote 1 leases to leases file.

Listening on LPF/eth0/00:d0:59:82:2b:86/192.168.0.0/24

Sending on   LPF/eth0/00:d0:59:82:2b:86/192.168.0.0/24

Sending on   Socket/fallback/fallback-net
```

CTRL C pour arrêter.

Installation des clients

Le client sous Windows

L'installation est assez simple si vous avez déjà une carte réseau et le protocole TCP/IP installé. Utilisez les commandes suivantes: Panneau de configuration/Réseau/Protocole TCP IP/Propriétés/Onglet "adresse ip"/ Cochez Obtenir automatiquement une adresse IP

La configuration est terminée, vous pouvez relancer la machine. Le client interrogera un serveur DHCP pour qu'il lui délivre un bail (sorte d'autorisation de séjour sur le réseau) contenant au minimum une adresse IP et le masque correspondant.

Le client sous Linux

Vous allez réaliser une configuration manuelle

Allez dans le répertoire `/etc/network`, ouvrez le fichier **interfaces**. C'est ici qu'est la configuration des cartes installées sur la machine. Remplacez `static` par `dhcp` dans la configuration de l'interface `eth0`. Mettez tous les paramètres de cette interface (address, netmask, network....) en commentaire.

La configuration de la carte est terminée, vous pouvez tester en relançant le service réseau.

Vous pouvez egalement tester dynamiquement en ligne de commande:

```
root@m1:# dhclient eth0
```

Procédure de test

Sur Windows vous allez pouvoir utiliser (selon les versions) les commandes `IPCONFIG` et `Winipcfg`.

Utilisez `ipconfig /?` pour voir comment utiliser la commande

Vous pouvez utiliser l'interface graphique `winipcfg` sous Windows 9x uniquement. Allez dans Démarrer puis Exécuter et saisissez `winipcfg`. Une fois la fenêtre activée vous pouvez utiliser les fonctions de libération et de renouvellement de bail. Si vous avez plusieurs cartes sur la station, la liste déroulante " Cartes Ethernet Informations " vous permet d'en sélectionner une.