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

……

Ecole **S**upérieure d'**I**nformatique
(**E.S.I**)
BP : 1091 Bobo-Dioulasso
TEL : 20 97 27 64
URL:http://esi.univ-bobo.bf

……

Cycle des **I**ngénieurs de **T**ravaux **I**nformatiques
(**CITI)**
Option : **R**éseaux et **M**aintenance **I**nformatiques
(**RéMI**)

BURKINA FASO
Unité-**P**rogrès-**J**ustice

……

Bureau d'Informatique et de Gestion
03 BP : 4075 Bobo-Dioulasso 03
TEL : 20 97 33 24
FAX : 20 98 80 34
Email : big@fasonet.bf

PROJET DE FIN DE CYCLE

Thème :

ETUDE DU SYSTEME INFORMATIQUE DE BIG: SECURITE ET DEPLOIEMENT DE SERVICES RESEAUX

Présenté et soutenu par:

M. NIKIEMA Ousmane
Etudiant en 3éme année de Réseaux et Maintenance Informatiques
Du 5 Septembre au 5 Décembre 2008

Superviseur
M. Pasteur PODA
Enseignant à l'ESI

Maître de Stage
M. Soumaïla SAMADOULOUGOU
Directeur Général de BIG

Année académique 2007-2008

Table des matières

SIGLES ET ABREVIATIONS

ADSL	Asymetric Digital Subscriber Line
AOI	Aide Odontologie Internationale
APT	Advanced Packaging Tools
BIG	Bureau d'Informatique et de Gestion
BIND	Berkeley Internet Name Domain
BIOS	Basic Input Output System
CICI	Cycle des Ingénieurs de Conception Informatique
CITI	Cycle des Ingénieurs de Travaux Informatiques
DMZ	Zone démilitarisée
DNS	Domain Name Server ou Domain Name System
ESI	Ecole Supérieure d'Informatique
FAI	Fournisseur d'Accès à Internet
FQDN	Fully Qualified Domain Name
FTP	File Tranfer Protocol
GNU	Gnu's Not Unix
HP	Hewlett Packard
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
IDR	Institut du Développement Rural
IUT	Institut Universitaire de Technologie
LAN	Local Area Network
LDAP	Lighweight Directory Access Protocol
LS	Ligne Spécialisée
MAC	Media Access Control
ONATEL	Office National des Télécommunications
ONG	Organisation Non Gouvernementale
OSI	Open Systems Interconnection
PC	Personal Computer

PDF Portable Document Format

PHP Hypertext Preprocessor

PME Petites et Moyennes Entreprises

RFC Request For Comment

SE Système d'exploitation

SGBD Système de Gestion des Bases de Données

SOA Start Of Authority

SQL Structured Query Language

SSH Secure Shell

SSL Secure Socket Layer

TCP/IP Transmission Control Protocol/Internet Protocol

TIC Technologies de l'Information et de la Communication

UDP User Datagram Protocol

UPB Université Polytechnique de Bobo-Dioulasso

URL Uniform Resource Locator

TABLE DES ILLUSTRATIONS

AVANT PROPOS

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

Elle comprend 6 écoles et instituts qui sont l'Ecole Supérieure d'Informatique (ESI), l'Institut de développement rural (IDR), l'Institut Universitaire de Technologie (IUT), l'Institut des Sciences Exactes et Appliquées (ISEA), l'Institut des Sciences de la Nature et de la Vie (ISNV), l'Institut des Sciences de la santé (INSSA).

L'Ecole Supérieure d'Informatique (ESI)**,** créée en 1991, a d'abord été implantée à Ouagadougou, ensuite elle a été transférée au sein de l'Université Polytechnique de Bobo-Dioulasso (UPB) en septembre 1995. Elle a pour mission la formation fondamentale, appliquée et/ou professionnelle dans les domaines de l'informatique, la formation continue, la recherche scientifique et technologique ainsi que la valorisation des résultats de la recherche, la diffusion de la culture et de l'information dans les domaines relevant de sa compétence, la collaboration avec d'autres structures de formation et/ou de recherche pour la préparation des diplômés et la participation à des programmes internationaux de formations et de recherche.

L'ESI offre trois cycles de formations. Le premier est le Cycle des Ingénieurs de Travaux en Informatiques (CITI) et comporte deux options : l'Analyse et Programmation (AP), créée en 1990, et le Réseaux et Maintenance Informatiques (RéMI), créée en 2000 ; ce cycle est sanctionné par un diplôme d'ingénieur de travaux informatiques. Le second est le Cycle des Ingénieurs de Conception en Informatique (CICI), sanctionné par un diplôme d'ingénieur de conception en informatique. Et enfin, le troisième cycle est celui du Diplôme d'Etudes Approfondies (DEA) créé en 2003.

Pour compléter leur formation et en vue d'obtenir le diplôme d'Ingénieurs des Travaux Informatiques(CITI) option Réseaux et Maintenance Informatiques (RéMI), les étudiants en fin de cycle à l'Ecole Supérieure d'Informatique(ESI) doivent effectuer un stage pratique de trois(03) mois en entreprise. C'est dans ce cadre que nous avons travaillé au Bureau d'Informatique et de Gestion (BIG) sous le thème : «Etude du système informatique de BIG: sécurité et déploiement de services réseaux».

INTRODUCTION GENERALE

Défini comme la science de traitement automatique de l'information, l'informatique a évolué et continue d'évoluer de façon exponentielle. Cette évolution a permis à l'informatique de s'implanter aujourd'hui dans pratiquement tous les domaines d'activités comme la gestion, la science, etc. Ainsi l'entreprise qui est un domaine en ébullition dans le monde actuel, se retrouve la plus touchée par cette science qui est l'informatique. Ainsi l'informatisation se révèle être le levier de prospérité des entreprises ambitieuses et la solution idoine aux nombreux défis. Dès lors, une entreprise qui se veut concurrente ne saurait se passer de cette science.

Une des branches de cette science, qui est le réseau, a permis l'interconnexion de plusieurs ordinateurs entre eux. Cette interconnexion a apporté plusieurs avantages parmi lesquels on peut citer le partage, la publication et l'accès à distance aux informations. Dès lors, le réseau est devenu nécessaire dans les entreprises car il permet de simplifier beaucoup de tâches, à travers plusieurs possibilités qu'il offre actuellement.

Fruit des trois mois de travail que nous avons effectué au Bureau d'Informatique et de Gestion (BIG), ce document s'articule sur l'étude du système informatique de BIG et nous l'avons subdivisé en quatre grands chapitres. Le premier présentera la structure qui nous a accueilli pour notre stage, à savoir BIG. Le deuxième chapitre est une généralité sur l'informatique, notamment le réseau et la sécurité informatiques Dans la deuxième partie, nous entrerons dans le vif du sujet par une étude critique du patrimoine technologique de BIG. Cela nous permettra d'en ressortir les limites afin de proposer une solution plus adaptée aux besoins de l'entreprise. Quant à la troisième partie qui sera la plus consistante de notre travail, elle nous permettra de mener une étude approfondie des solutions envisageables pour la mise en place du système informatique escompté. Dans cette partie nous aurons deux grands axes: le premier consistera à définir des architectures physique et logique du système futur. Dans le second, nous nous attellerons à étudier les services réseaux qui seront déployés en commençant par le choix dûment justifié du système d'exploitation et des applications serveurs les plus adaptées pour l'implémentation des services définis; ces applications et leur mise en œuvre sécurisée feront également l'objet d'une étude détaillée, avant que nous ne passions aux estimations en termes de temps et de moyens humains et matériels nécessaires à la réalisation effective de notre projet d'étude.

CHAPITRE 1: PRESENTATION DE LA STRUCTURE D'ACCUEIL

1.1 PRESENTATION DE BIG

L'entreprise Bureau d'Informatique et de Gestion (BIG) est une entreprise privée de Bureautique, Informatique et Gestion. Elle a vu le jour le 28 octobre 2001 sous l'initiative de deux associés:

- Soumaïla SAMANDOULOUGOU dit SAM, jeune Burkinabé titulaire d'une MSG (Maîtrise dès Sciences de Gestion) et ex employé des ONG Pharmaciens sans Frontières et Aide Odontologie Internationale (AOI)
- Yves GILLE Médecin bactériologiste exerçant au CHU de Lyon et Fondateur de l'association Aide Bonifiée pour la Création et le Développement de l'entreprise.

La satisfaction de la clientèle, corollaire de sa forte culture d'entreprise, a fait d'elle une entreprise leader dans les domaines de l'informatique, de la Bureautique et de la Gestion à Bobo-Dioulasso capitale économique du BURKINA.

Bien qu'étant une entreprise commerciale, BIG est aussi une entreprise citoyenne et joue à cet effet sa partition dans le développement du Burkina à travers:

- ➔ la création d'emplois,
- ➔ la promotion et la vulgarisation des TIC dans le cadre de la réduction de la fracture numérique,
- ➔ le renforcement des capacités organisationnelles et managériales des entreprises de la place.

Elle a su développer au fil des années un réseau de partenaires tant au niveau national qu'international, ce qui lui permet d'offrir à ses clients des services diversifiés et des produits à la pointe.

Le siège social est situé au 737 de l'avenue Imam Dienepo, secteur 8 à Bobo-Dioulasso entre l'hôtel 421 et la pharmacie du Levant.

1.2 STRUCTURATION

Afin de répondre au mieux aux attentes de la clientèle, BIG est structurée selon la figure 1.1 ci-dessous:

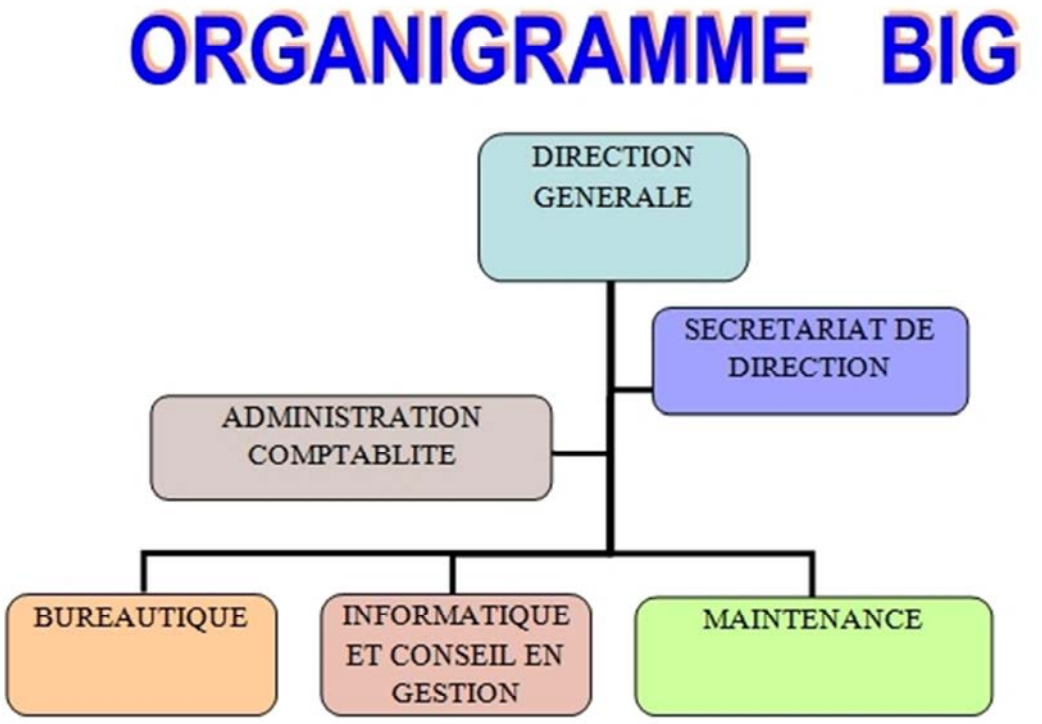


Figure 1.1 : Structuration de la société BIG

1.3 DESCRIPTION

1.3.1 Secrétariat de Direction

Ce service est chargé d'assister le directeur dans ses tâches administratives, de gérer les communications téléphoniques, d'introduire les visiteurs chez le Directeur, de prendre et fixer des rendez –vous, de gérer le courrier, de faire faire les factures et les bordereaux de livraison, de mettre en place un système de classement et de classer les documents, de préparer les réponses aux appels d'offres, de réunir les pièces administratives pour les appels d'offres, de suivre les différents contrats de BIG, de suivre l'exécution des contrats de maintenance, et enfin de coordonner le travail des différents services.

1.3.2 Bureautique et formation

Ce service est chargé de reproduire des documents pour les clients au moyen de photocopieuses, de scanner et de machine à relier, de saisir les documents pour le compte des clients, d'imprimer, mettre sur support informatique ou envoyer par courrier électronique les documents et données pour le compte des clients au moyen de l'outil informatique dont il dispose, de concevoir et reproduire les cartes de visite, de mariage, d'invitation, les brochures, les affiches, etc.…, de former les clients à l'informatique option bureautique, et d'effectuer tous les travaux de bureautique pour le compte de BIG.

1.3.3 Maintenance

Ce service est chargé d'assurer la maintenance préventive du matériel informatique de BIG, de faire la maintenance informatique des clients sous contrats de maintenance, de mettre en place un moyen de suivi des contrats de maintenance, d'exécuter la maintenance préventive et curative du matériel informatique et bureautique des clients, de produire des rapports de maintenance et enfin de Déployer et dépanner des réseaux filaires et sans fil.

1.3.4 Administration Comptabilité

Ce service est chargé d'assurer la tenue de la comptabilité conformément aux dispositions en vigueur en la matière, produire les états comptables périodiques, d'appuyer le Directeur pour la production des états financiers de fin d'exercice, d'effectuer les déclarations fiscales et sociales conformément aux dispositions en vigueur en la matière, d'assurer la tenue du livre du personnel, et d'assurer la gestion des fournitures et consommables.

1.3.5 Informatique et conseils en gestion

Ce service est chargé d'assurer l'assistance comptable chez les clients sous contrat d'assistance comptable, de produire les déclarations fiscales pour les clients sous contrat d'assistance fiscale, de produire les états financiers de fin d'exercice pour les clients sous contrat d'assistance comptable et pour les clients occasionnels, de défendre les clients devant le service des impôts, d'effectuer le diagnostic flash et organisationnel des PME, d' les diagnostics financiers des PME, de concevoir et mettre en place à la demande des systèmes comptables, de concevoir des modules de formation pour la tenue de la comptabilité des associations, des groupements d'intérêt économique, des coopératives et des P.M.E, de commercialiser et installer les logiciels de gestion, de commercialiser les matériels et consommables informatiques et enfin de concevoir et commercialiser les logiciels et

solution informatiques.

1.4 LES PRODUITS ET SERVICES

1.4.1 Les produits

BIG commercialise du matériel informatique et péri informatique de qualité et de marque reconnue par les professionnels du domaine. Les marques de prédilection sont: HP, Toshiba, Sharp, Linksys, Sysco, Canon, APC, MGE….

Il commercialise également:

- ✓ des ordinateurs de bureau,
- ✓ des ordinateurs portables,
- ✓ des imprimantes,
- ✓ des appareils photo numériques,
- ✓ des onduleurs,
- ✓ du matériel pour le réseau filaire et sans fil,
- ✓ des consommables informatiques,
- ✓ des vidéos projecteurs,
- ✓ des photocopieurs et divers autres matériels de Bureau,
- ✓ des logiciels de bureautique,
- ✓ des logiciels de comptabilité,
- ✓ des logiciels antivirus.

1.4.2 Les services

1.4.2.1 La maintenance

BIG offre également des prestations de service après-vente et de maintenance afin de permettre aux entreprises de disposer d'un parc informatique opérationnel et performant.

Ses compétences dans ce domaine sont:

- ◆ L'installation de système d'exploitation et de logiciel Microsoft,
- ◆ L'installation de système d'exploitation et de logiciel libre,
- ◆ Le dépannage logiciel et matériel,
- ◆ L'installation et optimisation des réseaux filaires et sans fil,
- ◆ La maintenance à distance…

1.4.2.2 Le conseil en gestion

BIG dispose d'un éventail de services afin de permettre aux clients de disposer d'un système de gestion performant et fiable à de meilleurs prix.

Ses prestations en gestion sont:

- mise en place de système comptable selon les normes du Syscoa,
- assistance comptable,
- assistance et conseil en fiscalité,
- établissement des états financiers de fin d'exercice,
- diagnostic organisationnel,
- diagnostic financier,
- plan d'affaire,
- montage de dossiers financiers,
- installation de logiciel de gestion…

1.4.2.3 La bureautique

Les prestations dans le domaine de la bureautique concernent :

- La reprographie de documents par l'entremise d'un équipement neuf et performant capable de débiter 3000 copies à l'heure,
- Le secrétariat public pour les saisies et les mises en pages de tout type de document,
- La conception et la plastification de badges, de brochures et de tout autre document nécessitant une protection,
- Le service de télécommunication par le fax et l'Internet.

1.4.2.4 La formation

BIG dispose d'une expertise dans le domaine de la formation. Il offre à cet effet des formations initiales et des formations à la carte dans le domaine de l'informatique bureautique et dans le domaine de la gestion.

Dans le domaine de l'informatique –bureautique, il propose des formations en Word, Excel, Access, Windows,…

Dans le domaine de la gestion, il propose des formations en Comptabilité d'entreprise, en Comptabilité d'association et en Comptabilité agricole.

Il assure également des formations approfondies pour permettre la maîtrise totale des différents

outils de gestion d'entreprise tels que la gestion financière, la gestion de la trésorerie, la gestion de la paye, la gestion des ressources humaines, la fiscalité d'entreprise, etc.…

1.4.2.5 Le placement de personnel

Pour les entreprises et organisations souhaitant recruter une compétence précise pour occuper temporairement ou durablement un poste, BIG offre un lot de candidatures couplés d'une technique de choix collégiale éprouvée permettant de minimiser les risques de déception de l'après recrutement.

Son excellente maîtrise de la législation du travail au Burkina garantit à ceux qui leur font appel un allègement de leurs structures, un gain de productivité et la diminution considérables de risques de conflits sociaux et de leurs corollaires.

1.5 LA CLIENTELE DE BIG

BIG gère un portefeuille hétéroclite de clients qui lui font régulièrement appel pour la qualité de ses produits et services. Ce sont:

- deux (02) Directions régionales de la santé du Burkina,
- AGROZOOTECH Sarl,
- projet PADS,
- ambassade de France,
- sept (07) Districts sanitaires,
- entreprise de construction BCKOF,
- pharmacie Miyougou,
- pharmacie Nazindi,
- GIP ESTHER (France),
- INERA (station de recherche).

1.6 LE PERSONNEL DE BIG

La force d'une entreprise se repose sur la qualité de ses ressources humaines. Consciente de ce fait, BIG a mûri le critère de sélection de son personnel. C'est un personnel qualifié, disponible, qui ne ménage aucun effort pour la satisfaction du client. Personnel très jeune et ambitieux, il se sent appartenir à une Afrique qui gagne.

Il comprend:

- ✓ un agent de liaison,
- ✓ une opératrice de saisie,
- ✓ un formateur en informatique bureautique,
- ✓ deux techniciens de maintenance,
- ✓ un aide comptable,
- ✓ un chef comptable,
- ✓ une assistante de direction,
- ✓ un directeur général.

CHAPITRE 2 : GENERALITES SUR LE RESEAU ET LA SECURITE INFORMATIQUES

2.1 Définition de l'informatique

L'informatique est la technique du traitement logique et automatique du support des connaissances et des communications humaines : l'information. Elle comprend donc, d'une manière indissociable, les méthodes et les moyens de ce traitement, ainsi que l'étude de leur domaine d'application. Mais en fait, plus qu'une simple technique, l'informatique constitue une discipline, une science carrefour, qui couvre un secteur large et disparate, tant technique que scientifique **;** c'est aussi une attitude de l'esprit dans l'approche des problèmes.

2.2 Le réseau informatique : les concepts et principes de base

Un réseau informatique est un ensemble d'équipements interconnectés qui servent à acheminer un flux d'informations. C'est précisément un ensemble de moyens matériels et logiciels mis en œuvre pour assurer les communications entre ordinateurs, stations de travail et terminaux informatiques.

Un réseau est principalement caractérisé par sa taille et sa topologie.

2.2.1 Classification des réseaux selon la taille

Les réseaux informatiques sont classés en trois catégories regroupées dans le tableau 2.1 ci dessous:

Tableau 2.1: classification des réseaux

	LAN (Local Area Network)	**MAN** (Metropolitan Area Network)	**WAN** (Wide Area Network)
Description	Réseau situé dans une zone réduite ou dans un environnement commun, tels qu'un immeuble ou un bloc d'immeubles	Interconnectent plusieurs LAN géographiquement proches. Il permet à deux nœuds distants de communiquer comme si ils faisaient partie d'un même	Interconnectent plusieurs LAN à travers de grandes distances géographiques Des routeurs permettent de "choisir" le trajet le plus approprié pour

		réseau local.	atteindre un nœud du réseau.
Taille géographique	1m à 1000m	100m-100km	Planétaire
Nombre de postes	2-200	2-1000	Plusieurs milliers
Débit	1 à 100Mbits/s	1-100Mbits/s	50bits/s à 2Mbits/s
Medias utilisés	STP, FTP,		
Opérateur	l'utilisateur	groupement d'utilisateurs	Public ou privé différent des utilisateurs
Taux d'erreur	$< 10^{-9}$	$< 10^{-9}$	10^{-3} à 10^{-6}
Délai de transmission de données	de 1 à 100 ms	de 10 à 100 ms	< 0,5 s
Facturation	gratuit	forfait	Volume et durée

2.2.2 Les différentes topologies

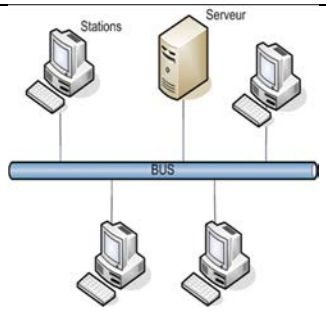
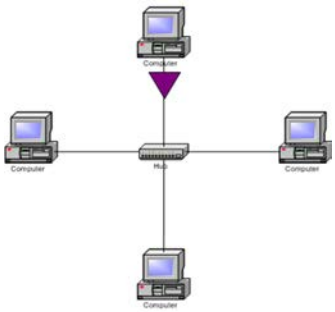
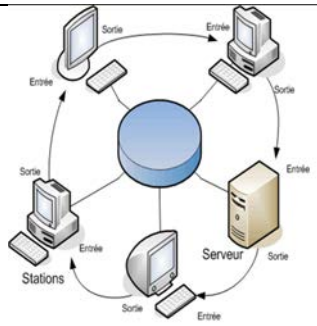
La topologie d'un modèle réseau représente l'agencement des éléments matériels que compose ce réseau.

- **La topologie physique**

La topologie physique est la manière dont sont interconnectés les nœuds et les terminaux des utilisateurs des systèmes informatiques c'est-à-dire la cartographie du réseau. Il n'est pas à confondre à la disposition physique des systèmes. Selon les topologies, on obtient des performances et des caractéristiques différentes (débits, nombre d'utilisateur maximum, temps d'accès, longueur de câblage, etc.) On distingue principalement trois types de topologies physiques (voir tableau 2.2 a la page suivante), l'étoile, le bus et l'anneau, qui peuvent être combinées pour donner naissance à des topologies hybrides (arbre, maillée, etc.).

Tableau 2.2: Les principaux types de topologies physiques

	Le bus	**L'étoile**	**L'anneau**
Description	Il permet une connexion multipoint. Le support physique de transmission est le bus. Tous les matériels connectés au câble reçoivent toutes les données qui sont émises.	Tous les équipements sont reliés au nœud central : hub ou un Switch pour les réseaux Ethernet. La communication est centralisée et se fait par diffusion ou commutation	C'est une topologie de type bus, mais en circuit fermé. Chaque poste doit reconnaître son adresse et se comporter comme un répéteur d'un réseau de type bus.
Medias utilisés	câble coaxial	paire torsadée 10BASE-T, coaxial ; fibre optique	Paire torsadée blindée ou non ; fibre optique
Avantages	-Economie de la longueur du câble ; -Support peu coûteux ; simple, fiable et facile à étendre.	-Chaque station a sa propre ligne, donc les conflits entre postes sont évités. -L'administration du réseau est facilitée par la présence du nœud central.	-Le temps d'accès est déterminé. -Le sens de parcours du réseau est déterminé ; ce qui évite les conflits.
Inconvénients	-nécessité d'un protocole d'accès qui gère le tour de parole des stations afin d'éviter les conflits. -Si le câble est défectueux ou cassé, le	-autant de câbles que de stations à raccorder La longueur de câble nécessaire est importante. -Une anomalie du nœud central peut bloquer tout	-Si un nœud ne fonctionne pas, le réseau est coupé. -Elle est coûteuse en câble et en matériels.

	réseau est paralysé	le réseau	
Schéma illustratif			

Les topologies hybrides

- **Arbre** : C'est un réseau en bus dans lequel une connexion donne naissance à un autre bus. Aussi connu sous le nom de *hiérarchique*, elle est divisée en niveau.
- **Mailée** : Elle est constituée d'une série de liaison point à point reliant différents éléments. Chaque terminal est relié à tous les autres

- **La topologie logique**

La topologie logique, par opposition à la topologie physique, représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI. Le tableau 2.3 suivant donne une brève description de ces différentes topologies.

Tableau 2.3 : les différentes topologies logiques

Topologie Logique	Description	Médias utilisés
	Il est défini par la norme iso IEEE 802.3 et fonctionne à des débits allant de 10 à 1000 Mbits/s. Il existe deux modes de fonctionnement : Ethernet partagé : tout message émis est entendu par	✓ Câble coaxial ✓ Paire torsadée ✓ Fibre optique

Ethernet	l'ensemble des machines raccordées. Ethernet commuté : Le commutateur utilise un mécanisme de filtrage et de commutation. Le message n'est transmis que sur le port adéquat. le mécanisme de détection des collisions est le CSMA/CD (Carrier Sense Multiple Access). Ethernet est une technologie très utilisée car le prix de revient d'un tel réseau n'est pas très élevé.	
Token Ring	Il est défini par la norme iso IEEE 802.5. Contrairement à Ethernet le temps d'émission (de parole) est limité et se fait suivant une procédure définie : Avant d'émettre sur le réseau un ordinateur doit disposer d'un "jeton"(Token).	✓ La paire torsadée blindée ou non ; ✓ Le twinax
FDDI (Fiber Distributed Data Interface).	C'est une amélioration de Token Ring. Elle compte non plus un (1) mais deux (2) anneaux. Elle permet le transport de trafic isochrone (voix vidéo) et de données souvent à des vitesses pouvant atteindre 100 Mbps.	✓ la fibre optique multimode ; ✓ Paire torsadée

Conclusion sur les topologies

Le choix d'une ou l'autre des topologies s'appui sur :

- Le bilan des équipements informatiques existants,
- L'analyse des besoins immédiats,
- La disposition géographique des équipements et des locaux,
- L'expression des besoins futurs,
- Les coûts d'investissement et de maintenance.

2.2.3 Modèles et protocoles

Un protocole de communication est un ensemble de règles et de procédures permettant de définir un type de communication particulier. Les protocoles sont hiérarchisés en couches, pour décomposer et ordonner les différentes tâches.

Un modèle est une suite de protocoles. Comme exemple de modèle on peut citer le modèle OSI (Open System Interconnection) et le TCP/IP. Le tableau 2.4 suivant donne un récapitulatif des modèles et protocoles.

Tableau 2.4: récapitulatif des modèles et protocoles

Couche	Modèle OSI	Modèle TCP/IP	Description	Exemples de protocoles du modèle TCP/IP
7	Couche application	Couche application	Elle assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.	FTP, SSH, SFTP, DNS, HTTP, IMAP, NFS, POP3, Samba, SNMP, RIP, SMTP, Telnet,
6	Couche présentation			
5	Couche session			
4	couche de transport	Couche Transport (TCP)	Elle est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission.	TCP, UDP, RTP
3	couche de réseau	Couche Internet (IP)	Elle permet de gérer l'adressage, l'acheminement des datagrammes (paquets de données) et le routage des données, via le réseau.	IP, ICMP, IGMP, ARP
2	couche de liaison des données	Couche accès réseau ou liaison	Elle spécifie comment les paquets sont transportés sur la couche	Ethernet, ATM, Token ring, SLIP
1	Couche physique	Couche physique	Elle décrit les caractéristiques physiques de la communication comme les types de câbles et de connecteurs utilisés, le niveau des signaux, la longueur d'onde etc.	électronique, radio, laser

2.2.4 Les médias de transmission

On les retrouve au niveau de la première couche du modèle TCP/IP. Le choix du support de transmission doit prendre en compte la distance à parcourir, le coût, le débit, la flexibilité et le déploiement.

Le tableau 2.5 ci-dessous résume les différents câbles et leurs caractéristiques ainsi que les avantages et les inconvénients.

Tableau 2.5: Les différentes sortes de câbles et leurs caractéristiques

Type de câble	**Distance Max (m)**	**Débits Max**	**Avantages**	**Inconvénients**
Câble coaxial fin RG58U 10Base2	200	100 Mbits	Facilité d'installation; Connectique moins coûteuse	faible bande passante ; sensible aux interférences.
Câble coaxial épais 10Basae5	500	100 Mbits	Large bande passante Déploiement sur longue distance	Manque de souplesse ; Coût élevé.
Paire torsadée non blindée (UTP) 10baseT	100	Catégorie3 **:** 10 à 50Mbits Catégorie4 : 50 Mbits Catégorie5e et 6: 100 Mbits et plus.	Coût faible Facile à installer	- Faibles distances (<100m) Sensible aux perturbations
Paire torsadée blindée (STP)-10baseT	100			
Fibre optique (10baseF)	10000	1Gbits	Déploiement sur très longue distance ; Large bande passante	- Coût très élevé Difficulté de connexion

2.2.5 Les équipements d'interconnexion

Les principaux équipements matériels mis en place dans des réseaux locaux sont :

- **Le répéteur** : Il est encore appelé répéteur-régénérateur. C'est un matériel électronique servant à amplifier un signal numérique, et ainsi étendre la distance maximale entre deux nœuds d'un réseau.
- **Le concentrateur** : C'est un élément de connectivité qui établit une connexion commune entre des composants d'un réseau en étoile. Son rôle est de répercuter toutes les informations qu'il reçoit d'un port vers tous les autres ports du concentrateur. *Exemple de concentrateur : le Hub.*

- **Le commutateur** : Il est semblable au concentrateur mais à la différence du fait que les informations venant d'un port donné sont répercutées uniquement vers le port qui en a besoin. *Exemple de commutateur : le Switch*

- **Le pont** : Cet équipement permet de segmenter un réseau. Il filtre les trames et les transmet vers le segment équivalent. Pour cela, il opère sur les adresses physiques (adresse MAC) et maintient une table de correspondance entre adresses MAC et segments auxquels appartiennent ces adresses.

- **La passerelle** : C'est un dispositif permettant de relier deux réseaux informatiques différents, ayant des architectures différentes ou des protocoles différents, ou offrant des services différents.

- **Le routeur**: Il permet de relier de nombreux réseaux locaux de telles façons à permettre la circulation de données d'un réseau à un autre. Leur fonction principale est le routage qui consiste essentiellement à déterminer le prochain nœud du réseau auquel un paquet de données doit être envoyé, afin que ce dernier atteigne sa destination de façon optimale.

2.2.6 Les technologies d'interconnexion des réseaux

Il existe un nombre élevé de moyen d'interconnexion des réseaux. Nous retenons ici quelques technologies courantes.

- **Le VPN (V**irtual **P**rivate **N**etwork**):** Un réseau privé virtuel (VPN) est l'extension d'un réseau privé qui inclut les liaisons avec des réseaux partagés ou publics tels qu'Internet. Avec un réseau VPN, on peut transmettre des données entre deux ordinateurs par le biais d'un réseau partagé ou public en émulant une liaison privée point à point. L'échange des données se fait de façon cryptée.

- **La LS** (Liaison Spécialisée**) :** La LS est un moyen d'interconnexion dédiée entre un opérateur ou fournisseur d'accès à Internet (FAI) et un client. Ce moyen permet d'avoir le débit que l'on souhaite et reste évolutif sans limites si ce n'est celui du fournisseur. Il est plus adapté à un usage professionnel.

- **L'ADSL** (Asymetric Digital Suscriber Line) **:** L'ADSL ou réseau de raccordement numérique asymétrique en français est un service d'accès à l'Internet utilisant les lignes téléphoniques classiques, en utilisant une bande de fréquence plus élevé que celles utilisée pour la téléphonie. Le débit descendant est plus élevé que le débit ascendant. Les débits proposés actuellement peuvent atteindre 2Mbit/s

- **La BLR** (Boucle Locale Radio) : elle est normalisée sous la référence IEEE 802.15. La BLR est une technologie de connexion sans fil, fixe et bidirectionnelle :
  - ✓ Sans fil : utilise les 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.

- **Le WIMAX** (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 sous le nom IEEE-802.16. Le WIMAX, définit les connexions à haut débit par voie hertzienne. Il opère dans la zone de fréquence de 2 à 11GHz pour une portée est de 50km généralement.

- **Le Wifi** (Wireless Fidelity) : c'est une technologie réseau sans fil, répondant à la norme 802.11. Sa spécificité permet à un utilisateur de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu. En plus de la possibilité d'échange de données entre plusieurs postes, il permet le partage de la connexion Internet. La technologie Wifi est basée sur une liaison utilisant les ondes radios électriques (Radio et Infrarouge) en lieu et place des câbles habituels.

2.2.7 Les services réseaux

Les deux dernières couches du modèle TCP/IP sont le domaine des services réseaux. Les services réseaux représentent l'ensemble des applications qui apportent un gain considérable dans les travaux quotidiens des utilisateurs du réseau. Nous donnons ici une brève définition de quelques

services en montrant leur utilité dans un réseau local.

Le Firewall

Un pare-feu ou coupe-feu (firewall en anglais) est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un autre réseau (Internet le plus souvent). Il s'agit d'un système informatique situé à l'entrée du réseau pour le protéger des intrusions éventuelles provenant de l'extérieur. Ainsi, en plus de la sécurité qui sera déployée dans la mise en œuvre de chaque service nous mettrons en place un système de filtrage des accès du réseau de BIG.

Web

Le Web est, de manière simple, un réseau composé de l'ensemble des sites Internet disponibles publiquement. Ils sont reliés entre eux par des hyperliens. Un site Internet (ou site web) est quant à lui un ensemble de pages Web, liées entre elles.

Un site web a une adresse, comme celle du site Ubuntu-fr: http://ubuntu-fr.org. La page Web principale de ce site propose des liens hypertextes vers d'autres pages et d'autres sites, par exemple : http://ubuntu-fr.org/telechargement.

Pour accéder à un site web, il vous faut utiliser un client Web, appelé communément Navigateur, par exemple : firefox, lynx, opera, konqueror, w3m… Vous devez spécifier en plus du nom ou de l'adresse IP, le protocole utilisé. Celui qui nous intéresse est HTTP. Un document Hypertexte est un document contenant des hyperliens. Ceux-ci permettent de lier les pages les unes avec les autres. Ainsi, vous pouvez naviguer grâce à des liens sur les pages. L'ordinateur auquel vous vous connectez pour lire vos documentations, héberge un logiciel qui fournit les pages demandées.

Le serveur Web désigne donc:

- Un ordinateur sur lequel fonctionne un logiciel serveur HTTP.
- Le logiciel serveur HTTP lui-même.
- Un ensemble de serveurs permettant le fonctionnement d'applications Web.

A priori, un serveur Web permet de mettre des pages Web à la disposition des autres ordinateurs du réseau. Cependant, dans une implémentation plus avancée, il facilite l'utilisation de certains services (messagerie électronique par exemple). Il peut permettre également d'administrer les ressources serveurs grâce à l'interface Web (base de données par exemple).

DNS

Le Domain Name System (ou DNS, système de noms de domaine) est un système permettant d'établir une correspondance entre une adresse IP et un nom de domaine. Il en dérive qu'un serveur de résolution de noms ou serveur DNS (Domain Name Server) permet de faire une correspondance entre les adresses IP (utilisées par les ordinateurs d'un réseau TCP/IP pour communiquer) et les noms de machine (qui sont plus mnémoniques pour nous les êtres humains). Les ordinateurs du réseau pourront alors s'identifier par des adresses numériques qu'ils traitent plus facilement pendants que les utilisateurs humains retiendront les noms de machines qui sont plus significatifs. Le système DNS est d'autant plus important dans un réseau qu'il est utilisé par d'autres services pour fonctionner correctement; c'est le cas par exemple du Web et de la messagerie. La preuve c'est qu'il est plus facile et plus commode de demander l'affichage de la page d'accueil du site Web de l'UPB en saisissant l'URL: www.univ-bobo.bf plutôt que 212.52.121.212 par exemple. Pourtant c'est le système DNS qui fait la correspondance entre l'adresse 212.52.121.212 et le nom de domaine www.univ-bobo.bf.

FTP

Un serveur FTP (File Transfer Protocol) comme son nom l'indique permet le transfert de fichiers. Nous l'implémenterons d'une part pour faciliter la mise à jour des sites Web. D'autre part, il permettra le dépôt et la récupération à distance de fichiers dans des répertoires dédiés aux utilisateurs.

DHCP

Un serveur DHCP (*Dynamic Host Configuration Protocol*) qui utilise le protocole de même nom, a pour rôle d'attribuer des adresses IP à des ordinateurs d'un réseau ainsi que tous les paramètres de configuration tels que: serveur DNS, passerelle, nom du réseau, pour une durée déterminée.

L'administrateur du réseau est exempté de la configuration manuelle de chaque poste du réseau qui peut s'avérer très pénible pour un réseau d'une certaine taille. De plus il n'ya pas de risque que plusieurs postes aient la même adresse si leur attribution est gérée par DHCP.

Ainsi donc, un serveur DHCP faciliterait la tâche d'administration du réseau.

Serveur de fichiers

Un serveur de fichiers, permet le partage des ressources entre les utilisateurs. Nous

entendons par ressources, les fichiers, les répertoires, les périphériques, etc. L'accès à ces ressources se fera par identification et authentification des utilisateurs. Dans l'implémention du serveur de fichiers nous laisserons le choix du système d'exploitation client aux utilisateurs pour accéder aux ressources partagées.

2.3 La sécurité informatique

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

2.3.1 Principes de la sécurité

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

Le **risque** en termes de sécurité est généralement caractérisé par l'équation suivante :

Risque = (Menace ***** Vulnérabilité)/Contre-mesure

La **menace** représente le type d'action susceptible de nuire dans l'absolu, tandis que la **vulnérabilité** (appelée parfois *faille* ou *brèche*) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la **contre-mesure** est l'ensemble des actions mises en œuvre en prévention de la menace.

Les contre-mesures à mettre en œuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies. Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

2.3.2 Objectifs de la sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. La sécurité informatique vise généralement cinq principaux objectifs :

- L'**intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;
- La **non répudiation**, permettant de garantir qu'une transaction ne peut être niée ;
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

2.3.3 Mise en place d'une politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés. Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;

- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en termes de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système. A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation. De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient de faire remonter les informations concernant la sécurité à sa direction, éventuellement de conseiller les décideurs sur les stratégies à mettre en œuvre, ainsi que d'être le point d'entrée concernant la communication à destination des utilisateurs sur les problèmes et recommandations en termes de sécurité.

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :

- Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
- Une procédure de management des mises à jour ;
- Une stratégie de sauvegarde correctement planifiée ;
- Un plan de reprise après incident ;
- Un système documenté à jour ;

Pour mettre en place un nouveau système informatique et une stratégie de sécurité plus adaptés aux besoins de communication de BIG, il est nécessaire de faire au préalable une étude détaillée du système informatique déjà existant de l’entreprise.

CHAPITRE 3: ANALYSE DU SYSTEME INFORMATIQUE EXISTANT

Notre étude ne saurait se faire sans prendre connaissance du Système Informatique dont BIG est actuellement dotée. Dans les lignes qui suivent, nous allons dans un premier temps faire une étude de l'existant dans le domaine des Technologies de l'Information et de la Communication (TIC) en mettant l'accent sur les éléments qui pourraient servir de base à la mise en œuvre du projet de notre étude. Ensuite nous ferons une étude critique des moyens déjà déployés. Nous finirons par la proposition d'une solution plus adaptée aux besoins de communication et d'apprentissage à BIG

3.1 ÉTUDE DE L'EXISTANT

3.1.1 Le patrimoine en Technologie de l'Information et de la Communication (TIC) de BIG.

Il est constitué du matériel informatique, des infrastructures réseaux, des logiciels et services réseaux mis en place.

3.1.1.1 Le matériel informatique

Il est reparti de façon suivante selon les différents services que compte BIG:

- ✓ **Secrétariat:**

Le secrétariat de BIG est doté du matériel informatique listé dans le tableau 3.1 ci-dessous.

Tableau 3.1: matériel informatique du secrétariat

Ordinateurs	Caractéristiques	Périphériques
3 Postes COMPAQ	Pentium III 799Mhz RAM: 128 Mo Disque dur: 20 Go SE: Windows XP Pro SP2	Imprimante partagée: HP Laserjet 1000 séries Imprimante réseau: HP Officejet 7313 Tout-en-Un

- ✓ **Formation et Bureautique:**

Le service de Formation et Bureautique est doté du matériel informatique listé dans le tableau 3.2

Tableau 3.2 : matériel informatique de la Formation et Bureautique

Ordinateurs	Caractéristiques	Périphériques
1 poste ASUS	Pentium IV 3 GHz RAM: 768 Mo Disque Dur: 80 Go Lecteur/graveur DVD SE: Windows XP Pro SP2	1 disque dur externe 160 Go 1 Magnétoscope Sharp Hauts parleurs
1 poste COMPAQ	Pentium III 799Mhz RAM: 128 Mo Disque dur: 10 Go SE: Windows XP Pro SP2	
1 Ordinateur portable IBM	Pentium III 732Mhz RAM: 512 Mo Disque dur: 20 Go SE: Windows XP Pro SP2	

- ✓ **Direction Générale:**

  Le tableau 3.3 contient la liste du matériel informatique de la Direction Générale.

Tableau 3.3 : matériel informatique de la Direction Générale.

Ordinateurs	Caractéristiques	Périphériques
1 Ordinateur portable TOSHIBA	Intel(R) CPU T1300 1,66 GHz RAM: 512 Mo Disque dur: 80 Go SE: Windows XP Pro SP2 Lecteur/graveur DVD	Ecran plat HP 1502 Haut parleur Mercury SW1980R

- ✓ **Comptabilité et gestion:**

  Le tableau 3.4 contient la liste du matériel informatique du service de la Comptabilité-Gestion

Tableau 3.4 : matériel informatique de la Comptabilité-Gestion

Ordinateurs	Caractéristiques	Périphériques
1 Poste COMPAQ	Celeron 731Mhz RAM: 128 Mo Disque dur: 10 Go SE: Windows XP Pro SP2	
1 poste	AMD-K6(tm)3D processor RAM: 256 Mo Disque dur: 30 Go SE: Windows XP Pro SP2	

- ✓ **Maintenance:**

  Le tableau 3.5 ci-dessous contient la liste du matériel informatique du service de la Maintenance Informatique.

Tableau 3.5 : matériel informatique du service de la Maintenance

Ordinateurs	Caractéristiques	Périphériques
1 poste CM Mercury	Pentium IV 3 GHz RAM: 1 Go Disque Dur: 280 Go SE: Windows XP Pro SP3 et Ubuntu 8.04	Lecteur/Graveur DVD externe PHILLIPS 16x
1 poste	Pentium IV 2 GHz RAM: 384 Mo Disque Dur: 120 Go SE: Windows XP Pro SP3 et Ubuntu 8.04	

3.1.1.2 Les infrastructures réseaux

L'architecture du réseau actuel de BIG est une architecture d'égal à égal. En effet, les différents ordinateurs des divers services sont reliés entre eux par du câble à paire torsadée de catégories 5e.

Le matériel réseau de BIG se compose donc de:

- 1 modem Speedtouch 350 pour la connexion internet
- 1 hub 16 ports pour connecter les ordinateurs du LAN
- 1 router Linksys pour la connexion sans fil au LAN

Il est à noter que le service de comptabilité et gestion ne fait pas parti du réseau local et n'a par conséquent aucun moyen de communication avec les postes du LAN.

La figure I.6 ci-dessous représente l'architecture du réseau actuel de l'entreprise BIG.

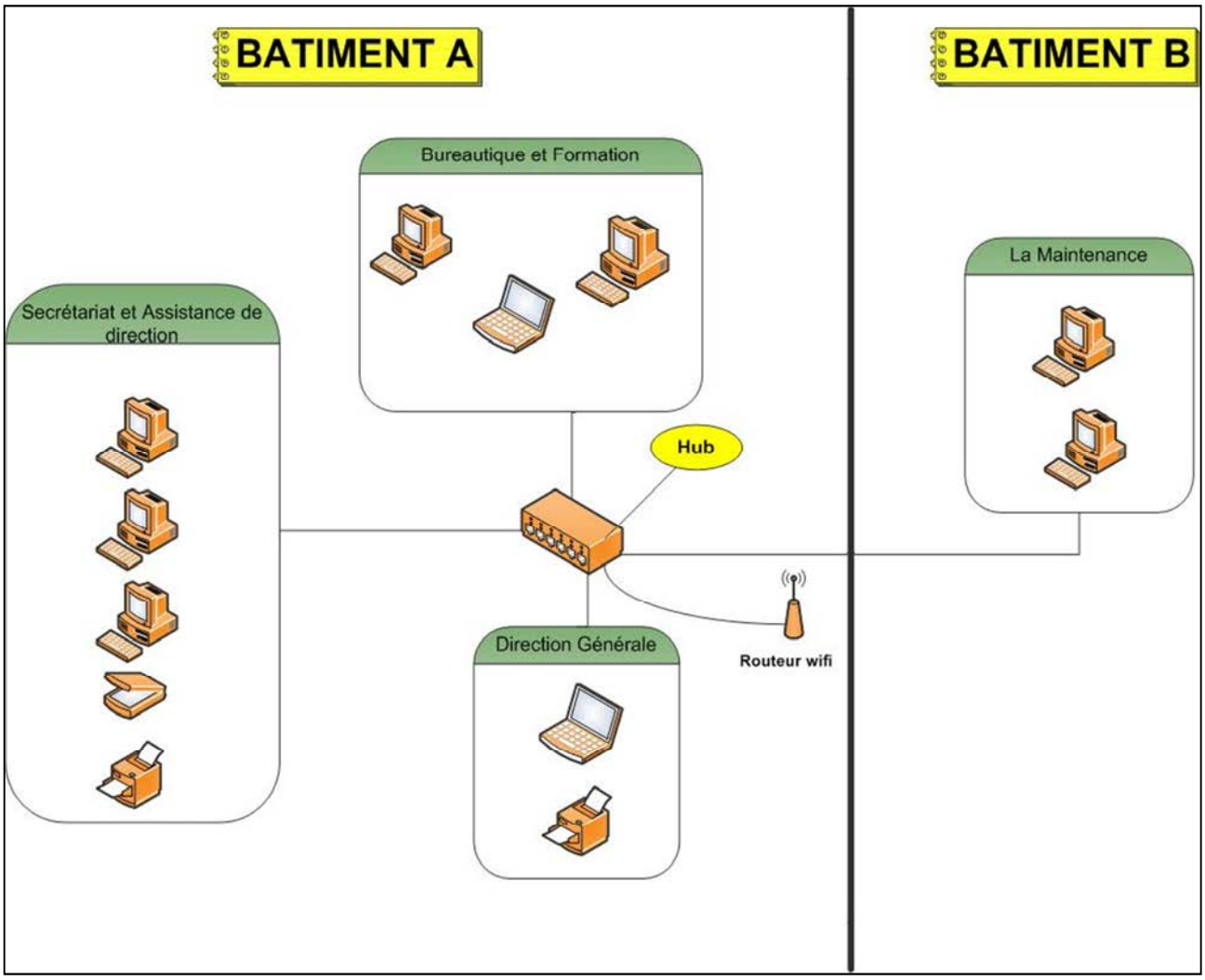


Figure 3.1: Architecture du réseau actuel de BIG

3.1.2 Les logiciels et les services réseaux

Le fonctionnement du matériel informatique de BIG est assuré par une gamme variée de programmes informatiques allant des systèmes d'exploitation aux programmes d'applications diverses.

3.1.2.1 Les systèmes d'exploitation

Le système d'exploitation installé sur la totalité des machines du parc informatique de BIG est Microsoft® Windows® XP Professionnel avec le service pack 2 ou le service pack 3. Mais sur certains postes, en plus de Windows® XP, On trouve aussi le système d'exploitation Linux et plus précisément la distribution Ubuntu dans sa version 8.04.

3.1.2.2 Les logiciels d'application

Les logiciels d'application sont nettement plus variés que les systèmes d'exploitation. Sur la totalité des postes de BIG est installée la suite bureautique Microsoft® Office version 2003 ou 2007. On rencontre divers autres types de programmes selon les utilisateurs des postes sur lesquels ces programmes sont installés. Ainsi on trouve le logiciel EBP Comptabilité pour le service de la comptabilité et gestion, Pinnacle Studio Plus pour le service de la formation et bureautique qui s'occupe aussi de montage vidéo, et sur tous les postes, plein d'utilitaires comme Adobe® Reader® 7 pour la lecture de fichiers au format PDF, WinRAR pour la gestion des fichiers compressés, et bien entendu des antivirus pour la protection contre des attaques virales.

3.1.2.3 Les services réseaux

Grâce au réseau de BIG, ses utilisateurs ont accès à plusieurs services leur permettant d'optimiser leurs travaux.

a) La connexion internet

BIG s'est souscrit à un abonnement ADSL chez l'opérateur ONATEL SA lui permettant d'être connectée au réseau global (internet). Grâce à cette connexion, elle dispose de façon permanente d'un débit de 128 Kbits/s. Tous les services de l'entreprise, à l'exception du service de comptabilité et gestion, ont donc accès à internet grâce au réseau local.

b) Le partage de fichiers et de ressources

Grâce au réseau local de BIG, tous les utilisateurs ont accès aux ressources partagées telles

les imprimantes pour leurs besoins d'impression. De plus, le partage de dossiers et de documents permet d'optimiser les travaux et accélérer les productions.

c) Le site web

BIG dispose aussi d'un site web qui lui permet d'être vu de l'extérieur et ainsi de faire connaître ses produits et ses prestations de service. Ce site est actuellement hébergé en France.

3.2 CRITIQUE DE L'EXISTANT ET PERSPECTIVES

3.2.1 Les limites du système actuel

Avec le système informatique actuel de BIG, il est clair qu'il sera impossible de répondre aux besoins de communication et d'optimisation des travaux de façon optimale. Ainsi nous avons pu relever :

- L'isolement du service de comptabilité et gestion, ce qui fait que ce service n'a pas accès aux fichiers et ressources partagés ainsi qu'à la connexion internet.
- L'architecture du réseau actuel rend difficile la gestion des utilisateurs (qui sont totalement maitres de leurs postes) et des ressources réseaux diminuant ainsi la sécurité des données.
- Un débit internet faible et par conséquent insuffisant pour une entreprise et l'exploitation optimale du futur système.

3.2.2 Proposition de solutions

Il découle des analyses menées plus haut que BIG doit être doté d'un système informatique pouvant répondre aux exigences de l'entreprise de façon optimale ainsi qu'à celles du futur système. Pour cela, il faudra donc:

- ✓ Compléter le câblage du réseau déjà existant afin de prendre en compte le service de comptabilité et de gestion.
- ✓ Mettre en place une nouvelle architecture réseau, cette fois centralisée, qui contrôlera tout accès aux ressources du réseau.
- ✓ Augmenter le débit de la connexion internet à au moins 512 Kbits/s afin de pouvoir tirer pleinement parti des possibilités du système informatique actuel et futur.

3.2.3 Choix d'une architecture centralisée

Une architecture centralisée est une architecture client/serveur, c'est-à-dire que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacité d'entrée-sortie, qui leur fournit des services.

Un système client/serveur fonctionne selon le schéma suivant :

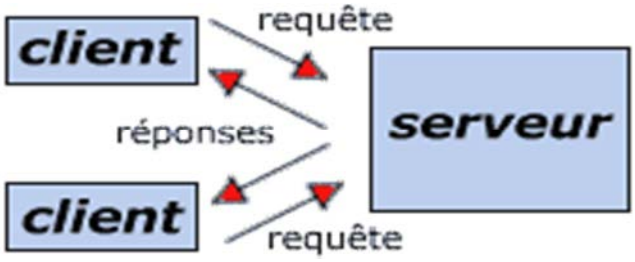


Figure 3.2: fonctionnement d'un système client/serveur

Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur et le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

Le choix d'une architecture client/serveur adaptée dépend de la taille de l'entreprise ainsi que de son chiffre d'affaire. Ainsi pour BIG nous avons la possibilité d'utiliser une architecture dont le serveur est doté d'un DNS fonctionnant avec adresse internet fixe ou une autre dont le serveur est doté d'un DNS fonctionnant avec ADSL dont l'adressage IP est dynamique.

3.2.3.1 Le DNS avec adresse internet fixe

Pour mettre en place cette solution, BIG doit demander auprès de l'opérateur ONATEL SA une adresse internet fixe qui lui sera accordée avec une liaison spécialisée. Cette solution oblige BIG à acquérir au moins 2 serveurs, un pour la DMZ et un autre pour les services fonctionnant dans le réseau local. Les couts (recueillis auprès de l'ONATEL SA) pour cette solution se résument dans le tableau 6 ci-dessous donc:

Tableau 3.6 : Couts pour la mise en place d'une liaison spécialisée avec un débit internet de 512Kbits/s

Acquisitions	**Couts**
Liaison spécialisée	472 000F
2 serveurs HP Proliant ML 570	4 000 000F
Redevances	500 000F/mois pour un débit de 512kbits/s

Les avantages et les inconvénients de cette solution seront donc:

Avantages

- ✓ Sécurité haute et totalement centralisée c'est -à-dire que la mise en place de la sécurité appartient totalement à BIG;
- ✓ garantie de rétablissement et bande passante réservée;
- ✓ L'encombrement des serveurs est moindre et leur capacité de fonctionnement est donc optimum.

Inconvénients

- × Avec une adresse internet fixe, BIG sera une cible facile pour les pirates. Ce qui requiert plus de moyens techniques et financiers pour la mise en place d'une sécurité conséquente;
- × Couts d'acquisition des équipements et de mise en œuvre assez élevé.

Cette architecture est représentée par la figure 3.3 ci-dessous :

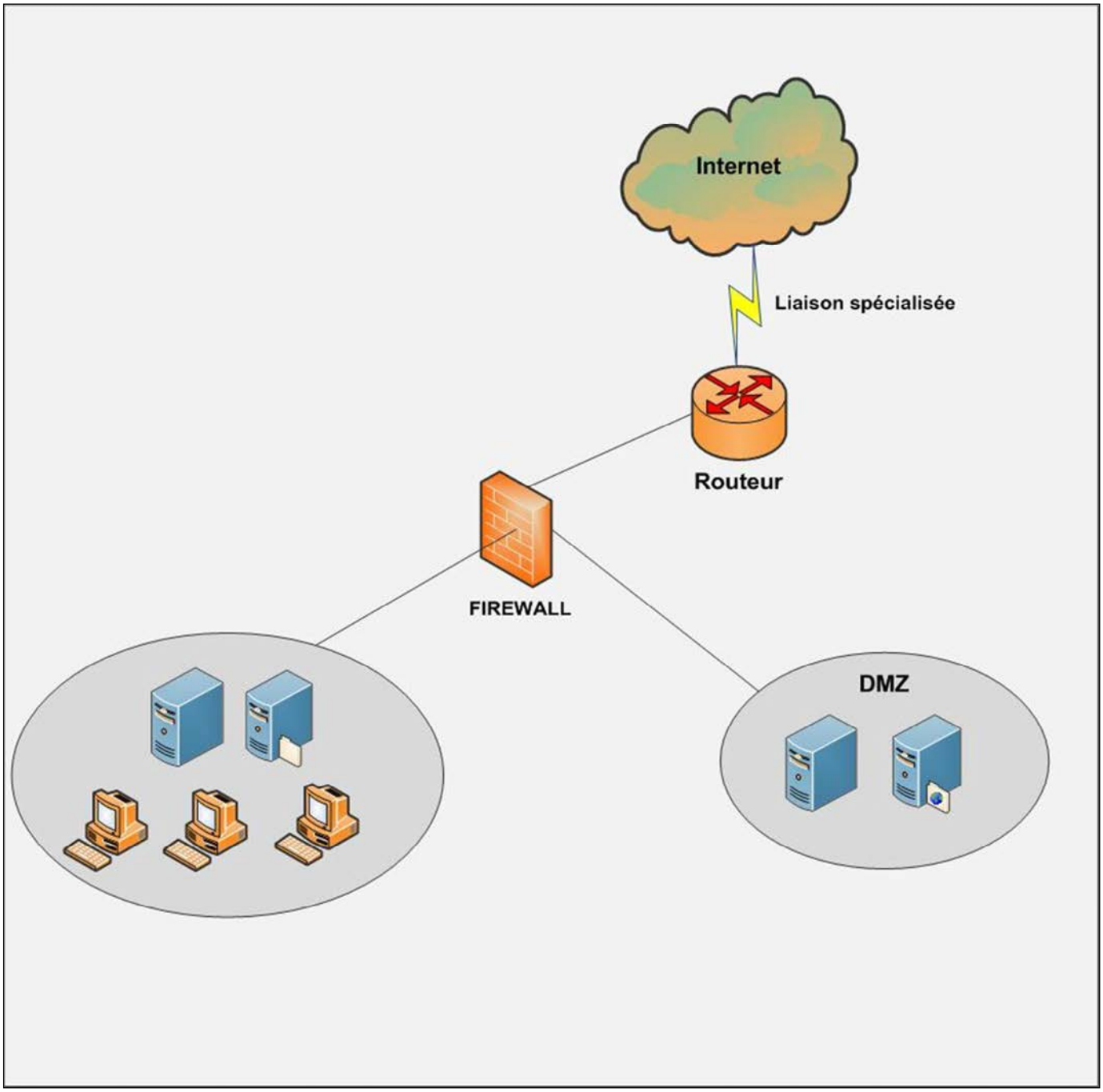


Figure 3.3 : Architecture centralisée avec DMZ

3.2.3.2 Le DNS dynamique

C'est un DNS capable de s'adapter à une adresse IP dynamique. Le DNS Dynamique permet de maintenir le lien entre le nom de domaine et l'adresse IP malgré les changements fréquents de celle-ci. Avec cette solution, BIG n'a pas besoin d'une liaison spécialisée. Elle garde sa connexion ADSL même si elle devra en augmenter le débit à 1 Mbits/s; elle devra alors payer une redevance d'environ 81 900 F chaque mois. De plus, grâce à l'adresse internet changeante de l'ADSL, BIG ne sera donc pas une cible facile pour les pirates car il est beaucoup plus difficile d'attaquer une cible

mouvante. Un seul serveur lui sera amplement suffisant car elle n'aura pas besoin d'une DMZ. Donc Les couts pour la mise en place de cette solution seront relativement faibles.

Mais l'inconvénient majeur de cette solution réside dans le fait que sécurité soit partagée. En effet, BIG est chargé d'une partie de la sécurité au niveau de ses configurations mais une autre partie incombe au service internet chargé de faire la correspondance entre l'adresse IP dynamique et le nom de domaine.

Cette architecture est représentée dans la figure 3.4 ci-dessous :

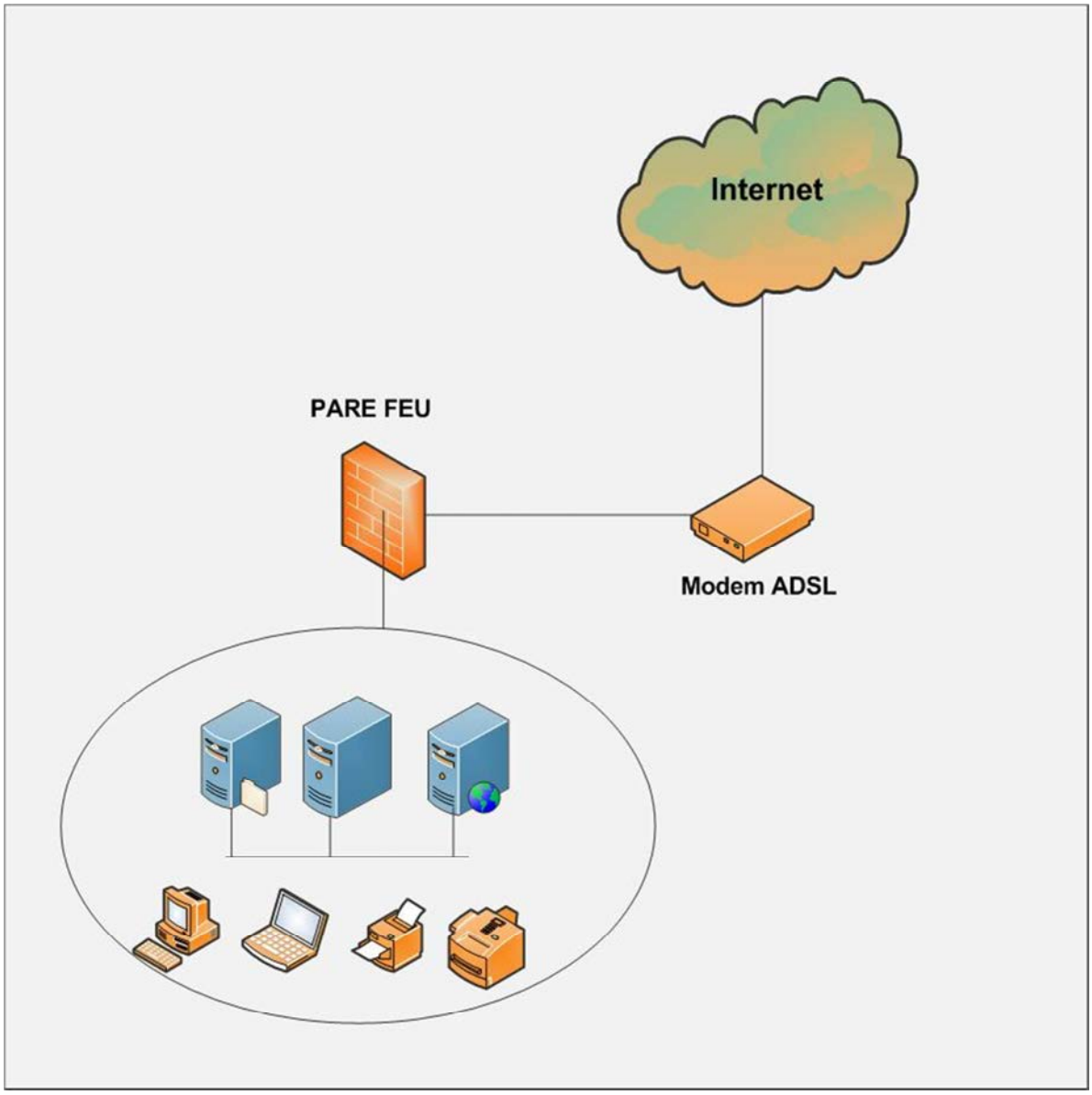


Figure 3.4: Architecture centralisée sans DMZ

3.2.3.3 Choix d'une solution

Au vu des deux solutions proposées plus haut et au regard du chiffre d'affaire de BIG qui s'élève à 80 millions de FCFA, à notre sens, il était donc plus judicieux pour BIG d'opter pour la deuxième solution, c'est-à-dire le DNS dynamique qui présente des caractéristiques tant au niveau de la sécurité qu'au niveau de la mise en œuvre pouvant entrer dans le portefeuille de l'entreprise dont le réseau est d'ailleurs assez limité. En accord avec notre maitre de stage, cette solution fut donc adoptée.

CHAPITRE 4: ÉTUDE DE LA MISE EN PLACE DES SOLUTIONS PROPOSÉES

4.1 DÉFINITION DE L'ARCHITECTURE DU FUTUR SYSTÈME INFORMATIQUE

Il y a deux niveaux d'abstraction dans le domaine des réseaux; *le niveau physique* et *le niveau logique*. Ainsi en parlant d'architecture réseau nous devons tenir compte de l'organisation logique et de celle physique. Pour mener à bien notre étude nous allons suivre une évolution axée sur la progression en couche du **modèle OSI**. Nous concevrons donc notre réseau par l'utilisation des équipements, protocoles et services selon les niveaux du modèle OSI.

4.1.1 Architecture physique

La topologie physique couvre les deux premiers niveaux du modèle OSI. Nous allons concevoir l'architecture physique des infrastructures informatiques de BIG. Pour ce faire, nous étudierons les équipements réseaux et leur interconnexion, relevant des deux premières couches du modèle OSI.

4.1.1.1 Les médias utilisés au sein des bâtiments

Pour l'interconnexion des équipements dans chaque bureau et bâtiment (le service de maintenance et celui de la comptabilité-gestion sont dans un autre bâtiment situé à une quinzaine de mètres des autres services), nous proposons l'utilisation combinée de deux types de supports: Les supports filaire et sans fil.

a) Les supports filaires

A l'intérieur de chaque bâtiment nous choisissons le câble à paire torsadée catégorie 5e avec des prises murales. Les caractéristiques du câble à paire torsadée **catégorie 5e** sont les suivantes: dans les câbles à paire torsadée circulent des signaux électriques. La catégorie 5e (e pour *enhanced*) est un type de câble permettant une bande passante de 100 Mhz (apparu dans la norme TIA/EIA-568A-5).

b) Les supports sans fil

La transmission des données est assurée ici par les ondes radio. Grâce à la technologie, de plus en plus, les ordinateurs portables sont équipés de cartes Wifi. Le Wifi permettra de relier des ordinateurs portables, des machines de bureau, des assistants personnels (PDA) ou même des

périphériques à une liaison haut débit (de 11 Mbit/s en 802.11b à 54 Mbit/s en 802.11a/g et 540 Mbit/s pour 802.11n) sur un rayon de plusieurs dizaines de mètres en intérieur.

4.1.1.2 Les équipements réseaux et leur disposition

Comme équipements réseaux, nous allons utiliser deux concentrateurs, dont un au niveau de chaque bâtiments. Un hub sera donc placé dans le local technique et un autre sera placé dans l'atelier de maintenance.

Précautions à prendre et normes à suivre dans la mise en place

Nous allons nous référer à la norme ANSI/TIA/EIA-569-A, relative aux espaces et aux voies de télécommunication qui sont: câblage horizontal, câblage backbone, poste de travail, armoire de câblage, salle du matériel, salle des terminaux principaux.

- ***Choix du local technique***

Il s'agit de l'endroit où la plupart des câbles et des équipements de réseau seront installés. Les critères de choix de local technique sont les suivants:

- ***Taille:*** Un local technique doit être suffisamment grand pour pouvoir loger tous les équipements et le câblage nécessaires au réseau. De plus, un espace supplémentaire doit être prévu pour la croissance future du réseau. La norme TIA/EIA-569 stipule que chaque étage doit avoir au moins un local technique et qu'un local technique supplémentaire doit être installé tous les 1 000 mètres^2, lorsque la surface de l'étage desservi est supérieure à 1 000 mètres^2 ou que la distance du câblage horizontal est supérieure à 90 mètres.
- ***Environnement:*** Tout emplacement sélectionné pour un local technique doit répondre à certaines conditions d'environnement incluant entre autres l'alimentation électrique, la ventilation et la climatisation. De plus, seules les personnes autorisées ont accès au local qui doit être conforme à toutes les réglementations en vigueur dans les domaines de la sécurité et de la construction. Le local technique doit être conforme aux règles applicables aux éléments suivants :
  - **la température et l'humidité;** Le système de ventilation et de climatisation du local technique doit maintenir une température ambiante à environ 21 °C lorsque les équipements du réseau local fonctionnent. Aucune canalisation d'eau ou de vapeur ne doit passer au-dessus du local ou à l'intérieur de celui-ci, à l'exception d'un système de gicleurs que peuvent exiger la

réglementation locale de prévention des incendies. L'humidité relative doit être maintenue à un niveau compris entre 30 % et 50 %. Si ces normes ne sont pas respectées, les fils de cuivre des câbles à paires torsadées non blindées ou blindées peuvent être détériorés par la corrosion, ce qui dégraderait les performances du réseau.

- **l'accès au local et à l'équipement;** La porte du local technique doit avoir au moins 90 cm de largeur et doit s'ouvrir vers l'extérieur pour permettre aux personnes de sortir facilement du local. Le verrou doit se trouver à l'extérieur de la porte, mais toute personne se trouvant à l'intérieur du local doit pouvoir sortir à tout moment.

Pour remplir ces différentes conditions nous proposons l'aménagement d'une salle au sein du bâtiment principal qui servira de local technique.

- ***Les câbles et supports.***

L'accès aux câbles et leur support. Les câbles hors des bâtiments doivent être couverts et enterrés et ceux dans les bâtiments doivent être mis dans des goulottes. Enfin, toute ouverture dans les murs ou le plafond permettant au conduit ou au mandrin de pénétrer dans le local doit être scellée à l'aide d'un matériau ignifuge conforme à toutes les normes applicables.

- ***L'accès au sans fil***

A l'instar des autres équipements d'interconnexion tels que les commutateurs et les routeurs, les routeurs Wifi devront être disposés dans des locaux dont l'accès fait l'objet d'un contrôle rigoureux.

4.1.2 Architecture logique

La topologie logique couvre le niveau trois du modèle OSI.

Niveau 3: la couche réseau, détermine les routes de transport et s'occupe du traitement et du transfert de messages: gère IP (Internet Protocol) et ICMP (Internet Control Message Protocol). C'est le domaine du routage, la subdivision logique du réseau.

Dans notre cas, nous aurons un réseau local global sans subdivision ayant comme adresse IP 192.168.1.0/24. La figure 4.1 ci-dessous représente notre réseau :

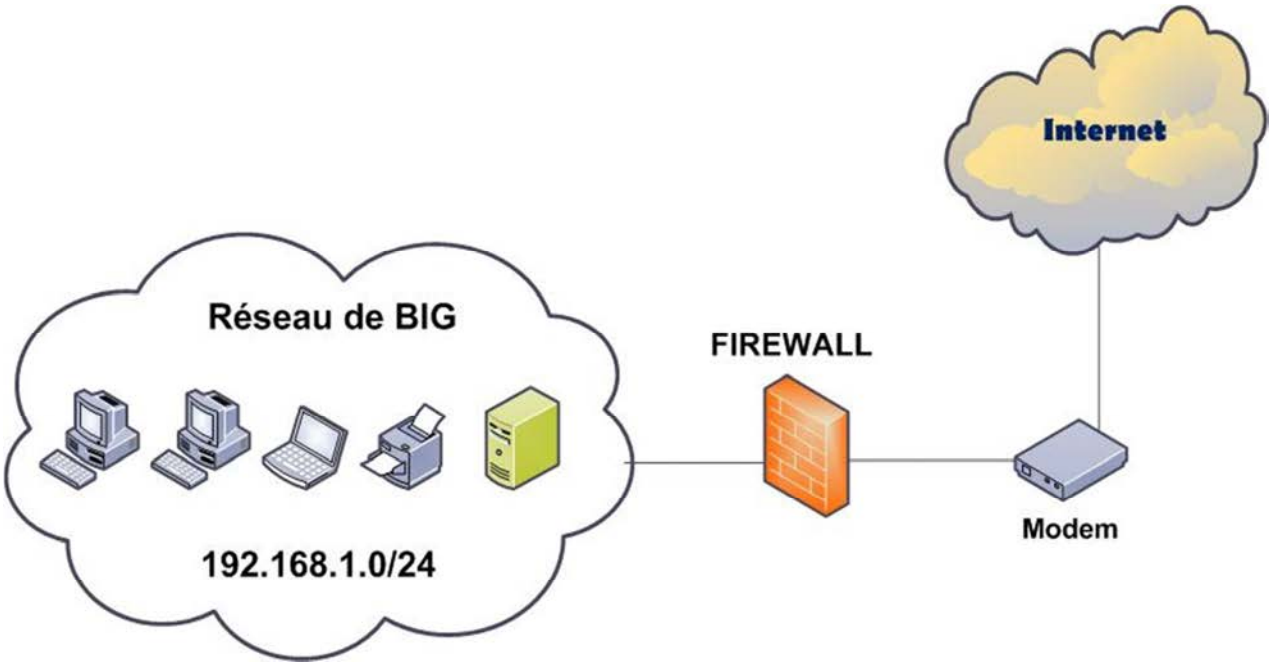


Figure 4.1: Schéma de synthèse de l'architecture logique

En remontant les couches du modèle OSI, nous avons conçu le réseau de BIG. L'organisation logique détermine les règles de dialogue entre les équipements du réseau. Ceci étant, il convient de poursuivre notre progression axée sur le modèle OSI. Nous allons regrouper les quatre dernières couches (Transport, Session, Présentation et Application); c'est le domaine des services réseaux.

4.2 ÉTUDE DES SERVICES À METTRE EN PLACE

Pour concevoir le futur système informatique de BIG, plusieurs services réseaux devront être déployés. Leur disposition est illustrée par la figure 4.2 ci-dessous.

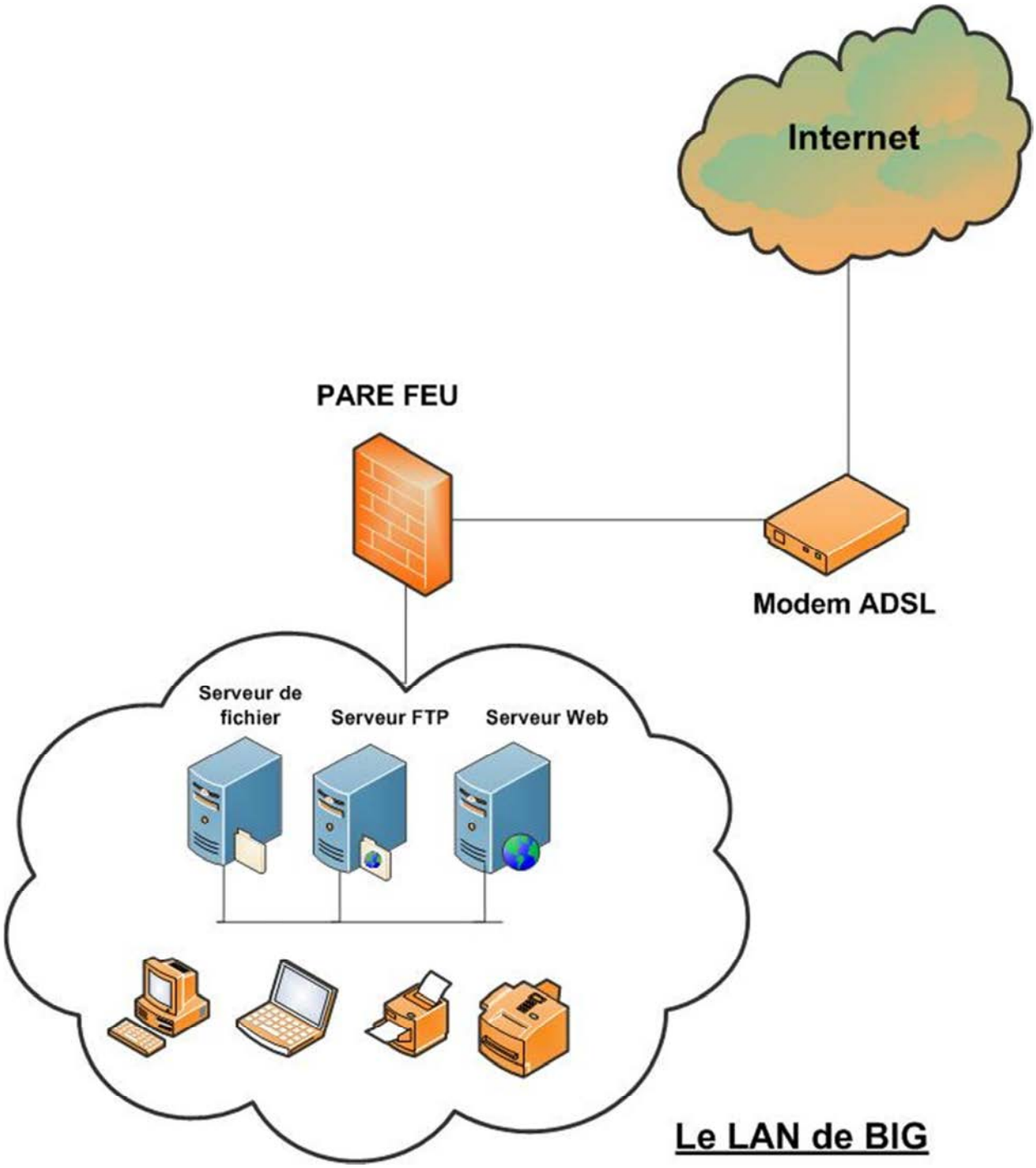


Figure 4.2: Schéma de synthèse de la disposition des services

Cependant, pour que ces derniers puissent bien fonctionner, il est nécessaire qu'un système d'exploitation soit préalablement déployé pour assurer leur communication avec le matériel informatique.

4.2.1 Choix du système d'exploitation et des applications serveurs

La question de savoir quel système d'exploitation convient pour notre étude peut susciter de très vifs débats tant à cause du très grand nombre de systèmes existants que du fanatisme de certains utilisateurs vis-à-vis d'un système donné. Pour nous guider dans notre choix, nous allons dans un premier temps mener une étude comparative des systèmes d'exploitation serveurs les plus utilisés de nos jours. Ensuite nous effectuerons un choix en considérant les critères suivants: ***les compétences humaines disponibles et les différents services à mettre en place.***

Tout d'abord, examinons les tableaux suivants qui présentent les caractéristiques générales et techniques des systèmes d'exploitation serveurs les plus utilisés.

Caractéristiques générales:

Tableau 4.1:Caractéristiques générales des systèmes d'exploitation serveurs

Système d'exploitation	Créateur	Première version publique (date)	Ancêtre	Dernière version	Prix	Licence	Ordinateur cible
AIX	IBM	1986	System V release 3	5.3 (août 2004)	Fourni avec le matériel	Logiciel propriétaire	Serveur, Station de travail
freeBSD	Le projet FreeBSD	Décembre 1993	386BSD	6.2 (15 janvier 2007) et 5.5 (25 mai 2006)	Gratuit	Licence BSD	Serveur, Station de travail
GNU/Linux	Auteurs multiples	17 septembre 1991	Minix	Kernel 2.6.22.4 (21 août 2007), 2.4.35.1 (15 août 2007) et 2.2.26 (5 février 2004)	Gratuit	Normalement GNU GPL (Copyleft)	Serveur, Station de travail, Ordinateur de bureau
Mac OS X	Apple Computer	Mars 2001	UNIX MachBSD, NeXTSTEP, Mac OS	10.4.10 « *Tiger* » (20/06/2007), 10.5.0 « *Leopard* » (26/10/2007)	129$, Familial (5 postes) 199$, Mac OS X Serveur 10 clients 499$, Mac OS X Serveur	Logiciel propriétaire, en partie APSL, GPL, et autres.	Ordinateur personnel, Station de Travail, Serveur

Système d'exploitation	Créateur	Première version publique (date)	Ancêtre	Dernière version	Prix	Licence	Ordinateur cible
					illimité 999$, Étudiant 69$		
NetBSD	Le projet NetBSD	Mai 1993	386BSD	3.1 (9novembre 2006)	Gratuit	Licence BSD	Embarqué, Ordinateur de Bureau, Serveur
HP-UX	Hewlett-Packard (HP)	1983	Unix	11.23 "11i v2" (Décembre 2005)	400$	Logiciel propriétaire	Serveur, Station de travail
NetWare	Novel	1985	S-Net	6.5 SP4 (Septembre 2005)	184$	Logiciel propriétaire	Serveur
OpenBSD	Le projet OpenBSD	Octobre 1995	NetBSD	1.0 4.1 (1er mai 2007)	Gratuit	Licence BSD	Serveur, Station de Travail, Embarqué
OpenVMS	DEC (HP à l'heure actuel)	Février 1978	RSX-11M	8.2-1 (septembre 2005)	Gratuit pour usage non-commercial	Logiciel propriétaire	Serveur
OS/2	IBM/Microsoft	Décembre 1987	MS-DOS	4..52 (décembre 2001)	300$	Logiciel propriétaire	Serveur, Ordinateur personnel

Système d'exploitation	Créateur	Première version publique (date)	Ancêtre	Dernière version	Prix	Licence	Ordinateur cible
Plan 9	Bell Labs	1993	Unix	Quatrième édition	Gratuit	LPL	Station de Travail, Serveur, Embarqué, HPC
Solaris	Sun Microsystems	Juillet 1992	SunOS	10(1ér février 2005)	Gratuit	CDDL	Station de travail, Serveur
Windows Server 2003	Microsoft	Avril 2003	Windows 2000	5.2 SP1 (30 mars 2005)	999$/5 clients	Logiciel propriétaire	Serveur

Caractéristiques techniques:

Tableau 4.2: Caractéristiques techniques des systèmes d'exploitation serveurs

Système d'exploitation	Architectures possibles	Système de fichiers possible	Type de noyau	Environnement graphique intégré	Paquetages	Logiciel de mise à jour	APIs
AIX	POWER, PowerPC JFS,	JFS2, ISO 9660, UDF, NFS, SMBFS, GPFS	Micro-noyau	Non	installp, RPM	Service Update	SysV, POSIX

Système d'exploitation	Architectures possibles	Système de fichiers possible	Type de noyau	Environnement graphique intégré	Paquetages	Logiciel de mise à jour	APIs
						Management Assistant (SUMA)	
FreeBSD	Intel IA32 (x86), AMD64, PC98, SPARC, autres	UFS2, ext2, FAT, ISO 9660, UDF, NFS, autres	Monolithique avec des modules	Non	ports tree, packages	par source (CVSup), freebsdupdate	BSD, POSIX
HP-UX	PA-RISC,IA-64	CFS, HFS, ISO 9660, NFS, SMBFS, UDF, VxFS	Monolithique avec des modules	Non	swinstall	???	SysV, POSIX
GNU/Linux	Presque toutes	Presque tous	Monolithique avec des modules	Non (sauf avec X Window, très répandu)	selon la distribution	selon la distribution	POSIX
Mac OS X	PowerPC, Intel IA32 (s86)	HFS+ (defaut), UFS, AFP, ISO 9660, FAT,	Hybride	Oui	OS X Installer	Software Update	Carbon, Cocoa,

Système d'exploitation	Architectures possibles	Système de fichiers possible	Type de noyau	Environnement graphique intégré	Paquetages	Logiciel de mise à jour	APIs
		UDF, NFS, SMBFS, NTFS (lecture seulement)					BSD/POSIX, X11 (depuis la 10.3)
NetBSD	Intel IA32 (x86), 68k, Alpha, AMD64, PowerPC, SPARC, playstation2, dreamcast(60 plateformes)	UFS, UFS2, ext2, FAT, ISO 9660, NFS, LFS, autres	Monolithique avec des modules	Non	pkgsrc	par source (CVS, CVSup, rsync) ou binaire (utilisant sysinst)	BSD POSIX
NetWare	Intel IA32 (x86)	NSS, NWFS, FAT, NFS, AFP, UDF, ISO 9660	Hybride	Non	NWCONFIG.NLM, RPM	mise à jour binaire, Red Carpet	Propriétaire
OpenBSD	Intel IA32 (x86), 68k, Alpha, AMD64, SPARC, VAX,	UFS, ext2, FAT, ISO 9660, NFS, quelques autres	Monolithique avec des modules	Non	ports tree, packages	apr source	BSD, POSIX

Système d'exploitation	Architectures possibles	Système de fichiers possible	Type de noyau	Environnement graphique intégré	Paquetages	Logiciel de mise à jour	APIs
OpenVMS	VAX, Alpha, IA-64	Files-11, ISO 9660, NFS	Monolithique avec des modules	Non	PCSI, VMSINSTAL	-	Unix-like
OS/2	Intel IA32 (x86)	HPFS, JFS, FAT, ISO 9660, UDF, NFS	Monolithique avec des modules	Oui	Via Install et autres	-	Propriétaire
Plan 9	Intel IA32 (x86), Alpha, MIPS, PowerPC, SPARC, autres 0	fossil/venti, 9P2000, kfs, ext2, FAT, ISO 966	Monolithique avec des modules	Oui	-	replica	Unix-like (et optionnellement POSIX)
Solaris	SPARC, SPARC64, AMD64, Intel IA32 (x86) (pkgadd)	UFS, ZFS, ext2, FAT, ISO 9660, UDF, NFS, quelques autres	Monolithique avec des modules	Non	SysV packages	Sun Update Connection	SysV, POSIX
Windows server 2003	Intel IA32 (x86), AMD64, IA-64	NTFS, FAT, ISO 9660, UDF	Hybride	Oui	MSI, installateurs personnalisés	Windows Update	Win32, Win64

Nous venons de faire le point sur les systèmes d'exploitation serveurs les plus utilisés. Nous pourrions déjà en choisir un en tenant compte des critères tels que les fonctionnalités, le coût, la licence et le type de matériel supporté par ces systèmes. Cependant pour optimiser notre choix, nous allons également prendre en compte des aspects tels que les compétences humaines disponibles et surtout les services à mettre en place.

- **Compétences humaines.**

La mise en place et le suivi d'un système informatique, nécessite un minimum de compétence. Cela est d'autant plus important que si on envisage d'utiliser les logiciels libres (GNU/Linux) auxquels on reconnaît quand même la non facilité d'utilisation. Il est donc primordial que nous possédions de bonnes connaissances du système. Les bases de ces compétences peuvent être acquises par des formations académiques continues. Cela n'est guère une inquiétude dans le cas de notre étude si nous considérons le fait que l'UPB compte parmi ses instituts et écoles, une structure de formation en informatique qui intègre dans ses programmes de formations, des modules liés aux logiciels libres notamment GNU/Linux. De plus, pour le suivi de son système informatique existant, BIG dispose d'un personnel technique qui n'est pas étranger aux systèmes de la famille UNIX.
Aussi, il est indispensable que nous apprécions le système d'exploitation choisi et que nous le pratiquions régulièrement.

En somme, l'inquiétude liée à la difficulté de déploiement et d'utilisation des systèmes UNIX pour la mise en place du système informatique de BIG ne serait pas justifiée.

- **Que voulons-nous faire?**

Un autre critère dont la prise en compte doit être primordiale dans la mise en place d'un système informatique est l'application que l'on veut en faire. En effet, le meilleur système d'exploitation du monde (s'il existait) ne le serait pas forcément dans tous les domaines d'application.

Le choix du système d'exploitation se fait donc en tenant compte également de l'ensemble des services que celui-ci peut nous permettre de configurer. Pour notre étude, nous envisageons de mettre en place notamment:

- **un serveur HTTP,**
- **un serveur FTP,**
- **un serveur de résolution de nom de domaine (DNS),**
- **un serveur de fichiers,**

Dans les lignes qui suivent, nous allons faire l'état sur les applications serveurs les plus utilisées

en vue d'opérer un choix.

Serveur HTTP

Netcraft est une entreprise spécialisée dans les technologies Internet; elle est surtout connue pour mener depuis 1995 des sondages automatisés d'Internet par nom de domaine à la recherche de serveurs HTTP, donc de sites Web. Elle publie mensuellement ses résultats qui sont régulièrement repris par les média informatiques. Le tableau 4.3 ci-dessous est une stastique des serveurs http les plus utilisés en Décembre 2007.

Tableau 4.3: statistique des serveurs HTTP les plus utilisés en Décembre 2007 d'après Netcraft.

Applications serveurs	**Nombre de postes serveurs**	**licence**	**pourcentage d'utilisation**
Apache	76,945,640	GPL	49.57%
Microsoft IIS	55,509,223	propriétaire	35.76%
Google GWS	8,558,256	propriétaire	5.51%
lighttpd	1,521,250	-	0.98%
Sun	588,997	propriétaire	0.38%
autres	12,089,939	-	7,8%

Le tableau ci-dessus nous montre qu'Apache est le serveur HTTP le plus implémenté dans le monde. En plus d'être sous licence GNU GPL (il est libre contrairement à ses deux concurrents directs qui sont propriétaires), il présente de nombreux atouts tels que sa conception modulaire, sa forte documentation, sa robustesse, la sécurité dont il est doté et son support des hôtes virtuels.
Nous pensons donc que c'est le serveur HTTP qui convient pour notre étude.

Serveur FTP

On trouve de nombreux serveur FTP pour Linux/Unix/BSD comme:
Ftpd, glftpd, ProFTPd, Pure-FTPd, VsFTPd, Wu-ftpd, wzdftpd.
Sous Windows, on trouve:
warFTPD Server, FileZilla Server, Pure-FTPd, Typsoft FTP, Server, wzdftpd. Serv-U. Il faut noter

que ce sont tous des logiciels libres.

Notre choix se porte sur vsFTPd, simple et très sécurisé. D'ailleurs, il a été développé dans l'optique de la meilleure sécurité possible afin de combler les innombrables failles de ses concurrents. Bien que très simple, il bénéficie de toutes les options habituelles des serveurs ftp classiques (ProFTPd, Pure-FTPd, ...).

Serveur de fichiers

Étant donné que nous avons un réseau hétérogène il faut permettre aux utilisateurs d'accéder aux données partagées quel que soit le système d'exploitation qu'ils utilisent. Pour les utilisateurs Linux nous configurerons le NFS (Network File System). En ce qui concerne les utilisateurs Windows nous avons le choix entre Samba (logiciel libre sous licence GPL) et Windows 2003 Server.

En la matière, des études ont montré que Samba est trois (3) fois plus rapide d'accès que Windows 2003 serveur. Nous n'avons donc pas l'embarras du choix à ce niveau vu que le plus performant est également gratuit.

Le firewall

Dans le domaine de la protection du réseau nous pourrons remplir des pages avec une liste des pare-feu. Mais parmi ceux-ci, iptables est celui qui offre le plus de flexibilité dans la configuration; c'est l'interface utilisateur de Netfilter qui est en fait un puissant outil réseau qui permet le déploiement d'une très bonne politique de sécurité sur un réseau.

En somme, l'étude préalable au choix du système d'exploitation et des applications serveurs pour la mise en place de notre système informatique nous a permis dans un premier temps de faire la comparaison entre les principaux systèmes serveurs existants. Ensuite, en tenant compte du contexte de notre entreprise et des services à mettre en place, nous avons passé en revue les différentes applications serveurs disponibles pour chaque type de service. En définitive, nous proposons Ubuntu, un système d'exploitation GNU/Linux qui pourra gérer l'ensemble des services dans la stabilité, la fiabilité, et la sécurité. De plus nous choisissons des applications parmi les meilleures qui ont l'avantage de s'intégrer parfaitement à Ubuntu GNU/Linux.
Le tableau 4.4 suivant récapitule nos choix.

Tableau 4.4: Tableau récapitulant le choix du système d'exploitation et des applications serveurs

Objectif	**Choix de l'application ou du système d'exploitation**
Système d'exploitation serveur	Ubuntu server GNU/Linux (version 8.04)
serveur Web	Apache
Anti virus, anti-spam	amavisd, clamav, spamassassin
Serveur FTP	VsFTPD
Serveur de fichier	NFS et Samba
serveur DNS	DNS dynamique sur dyndns.com
serveur DHCP	dhcpd
pare feu (firewall)	Iptables (Netfilter)

4.2.2 Le système d'exploitation Ubuntu et son déploiement

4.2.2.1 Étude de Ubuntu

- Présentation de Ubuntu

Ubuntu Linux est une distribution GNU/Linux non commerciale basée sur Debian et lancée en 2004. Son nom provient d'un ancien mot bantou (langue d'Afrique), Ubuntu, signifiant «*humanité aux autres*» ou encore «j*e suis ce que je suis grâce à ce que nous sommes tous*». Avant sa sortie pour le grand public, le projet très secret avait comme nom de code no-name-yet (pas encore de nom).

Initiée par le milliardaire sud-africain Mark Shuttleworth, et sponsorisée par sa société Cannonical Ltd., Ubuntu Linux est conçue principalement pour les ordinateurs de bureau (PC et Macintosh) avec un objectif de convivialité et d'ergonomie.

Ubuntu repose sur la distribution Debian dont elle reprend l'architecture et le système de procédure d'installation est néanmoins nettement simplifié. Il marque discrètement ses racines africaines par un fond d'écran initial brun (par opposition aux bleus classiques) et de brefs sons

d'instruments de musique africains associés aux événements qui se produisent.

Ubuntu Linux est disponible pour les architectures x86 (Intel et compatibles), AMD64 et PowerPC, soit sous forme de distribution à installer sur le disque dur (install), ou de CD de démonstration (live). Cette version live est un Live CD qui permet d'en tester le fonctionnement sur un ordinateur sans le modifier (par exemple pour vérifier sa compatibilité); cela est très important lorsqu'on désire par exemple tester le comportement d'une version 64 bits de Ubuntu (entre autres le bon fonctionnement des pilotes graphiques, ou l'augmentation de vitesse obtenue (en général 20%)) sans remettre en cause tout de suite son environnement 32 bits existant sur disque dur. La version DVD contient les deux versions, Install et live.

- Pourquoi Ubuntu

Il y a de nombreuses distributions GNU/Linux (telles que RedHat, SuSE, Debian, Mandriva) mais Ubuntu se distingue comme une distribution d'un genre différent. L'objectif de Ubuntu est de créer une distribution GNU/Linux qui fournisse un système à jour et cohérent pour les ordinateurs de bureau et les serveurs

Installation

- Ubuntu s'installe avec un seul CD. Pas besoin de télécharger un DVD ou 3 CD (Mandriva) voire 5 CD (SuSE). Le CD est le même pour une installation serveur ou bureau.
- Ubuntu propose un live-CD avec le même support matériel que le système installé. Très utile pour tester le support matériel sans altérer la configuration de l'ordinateur à installer.
- Ubuntu dispose de versions pour les architectures i386 (Processeurs Pentium / AMD / PC compatibles IBM), AMD-64 (Hammer) et PowerPC (iBook/PowerBook, G3, G4 et G5). C'est moins que Debian (12 architectures) mais plus que SuSE par exemple (PC et PowerPC).
- Savoir si son matériel est compatible est un souci d'Ubuntu. Le projet hwdb (HardWare DataBase) d'Ubuntu acquiert beaucoup de maturité. Chaque utilisateur peut soumettre l'état du support de son matériel simplement; ces données sont envoyées à http://hwdb.ubuntu.com/.

Communautaire

- Ubuntu est communautaire. Bien que sponsorisée par Cannonical, elle n'est pas un produit de Cannonical. D'ailleurs, la fondation Ubuntu a été créée afin d'assurer l'indépendance d'Ubuntu.
- Ubuntu possède un développement ouvert, à l'instar de Debian.

- Avec Launchpad (de Canonical), Ubuntu ne rejette pas les autres distributions mais veut au contraire travailler main dans la main avec elles (notamment pour partager les rapports de bogues, l'aide sur les logiciels et la traduction).
- Comme Debian, Ubuntu est libre et permet d'avoir un système entièrement libre par la séparation des paquets libres et non-libres dans des dépôts distincts. Cependant, afin de garantir une compatibilité maximale, Ubuntu a tout de même choisi d'intégrer un certain nombre de modules pas tout à fait libres dans sa distribution par défaut. C'est aussi ce qui fait sa force!!!

Logiciels

- Ubuntu fait les bons choix par défaut. Vous n'aurez même pas à vous soucier de choisir les logiciels qui s'intègrent le mieux à votre environnement préféré, ni même à les configurer pour que l'utilisation des différentes applications soit harmonieuse. Il n'y a pas de travail d'intégration à faire manuellement. (Contrairement à Debian).
- Ubuntu est construite sur la base solide et reconnue qu'est Debian. Tous les 6 mois, Ubuntu est une 'dérivée périodique', à partir de Debian *unstable* à laquelle Ubuntu applique ses propres patches, choix de paquets et configurations par défaut.
- Ubuntu a choisi de maintenir un dépôt main réduit et un dépôt universe très large. Ce choix assure un très bon support des paquets essentiels tout en ayant la disponibilité de très nombreuses applications. Il est rare d'avoir besoin de dépôt externe (qui est source de dépendances cassées).
- La bibliothèque de logiciels disponibles pour Ubuntu est grande mais reste cohérente. Ainsi on retrouve *j2re, mplayer* dans *universe/multiverse* alors qu'ils ne sont pas intégrés à Debian (par exemple).

Versions prévisibles et fréquentes

- Le projet se consacre au composant main et est donc capable de sortir tous les 6 mois une version contenant le meilleur des logiciels actuels, testés et avec une bonne finition.
- Chaque version sort un mois après GNOME. On a donc une version récente de GNOME mais suffisamment testée et stable. Ce n'est pas le cas de ForeSight Linux, entre autres, qui sort une nouvelle version quelques jours seulement après GNOME.
- La fréquence des versions est très appréciée pour un ordinateur de bureau ou un portable. Sans tomber dans un système en mise-à-jour perpétuelle (comme *unstable* dans Debian ou *cooker* avec Mandriva), l'utilisateur possède un bureau à jour mais stable.

Mes critères personnels

- Le site www.ubuntu-fr.org est un site français richement documenté permettant à un néophyte de se familiariser et de progresser très rapidement dans l'univers de Linux. Ubuntu est à notre connaissance la seule distribution à posséder un site français aussi complet et aussi accessible.
- Un forum très riche en informations, assisté d'une communauté très active, où chacun peut trouver rapidement une réponse à ses questions.
- Contrairement à certaines distributions (Mandriva, SuSE ...) il n'existe pas de version commerciale d'Ubuntu donc pas non plus de version limitée : **tout est accessible à tous.**
- La multiplicité des dépôts assure de trouver facilement la quasi-totalité des applications désirées sans avoir à rechercher d'hypothétiques paquets sur une multitude de sites.

4.2.2.2 Déploiement de Ubuntu serveur

Les caractéristiques matérielles requises pour installer Ubuntu serveur 8.04 se résument au tableau 4.5 suivant :

Tableau 4.5: caractéristiques matérielles requises pour installer Ubuntu serveur

	Minimale	Recommandée
RAM	128 Mo	256 Mo
Disque dur	1 Go	4 Go
Vitesse du processeur	200 Mhz	500 Mhz

En ce qui concerne le matériel, Ubuntu GNU/Linux n'a pas plus d'exigences que le noyau Linux et les outils GNU. Par conséquent, toute architecture ou plateforme, sur laquelle le noyau Linux, la libc, le compilateur gcc, ont été portés, et pour laquelle un portage de Ubuntu GNU/Linux existe, peuvent le faire fonctionner.

Précautions à prendre pour un serveur

Ubuntu est devenu un des systèmes les plus adaptés à la mise en place d'un serveur grâce à la sécurité et la stabilité dont elle est dotée. Mais ces qualités peuvent être compromises au moment même où on installe Ubuntu si certaines précautions ne sont pas prises:

- Ne pas installer un autre système d'exploitation sur la machine serveur,

- Bien partitionner son ou ses disques durs pour l'installation d'Ubuntu.
- Éviter d'installer le mode graphique sur le serveur; utiliser plutôt le mode texte pour ses configurations.

Obtenir le cdrom d'installation

Allez sur le site : http://www.ubuntu.com/getubuntu/download.

Allez dans l'onglet Server Edition. Choisissez la version 8.04.

Choisissez le pays d'ou vous téléchargerez.

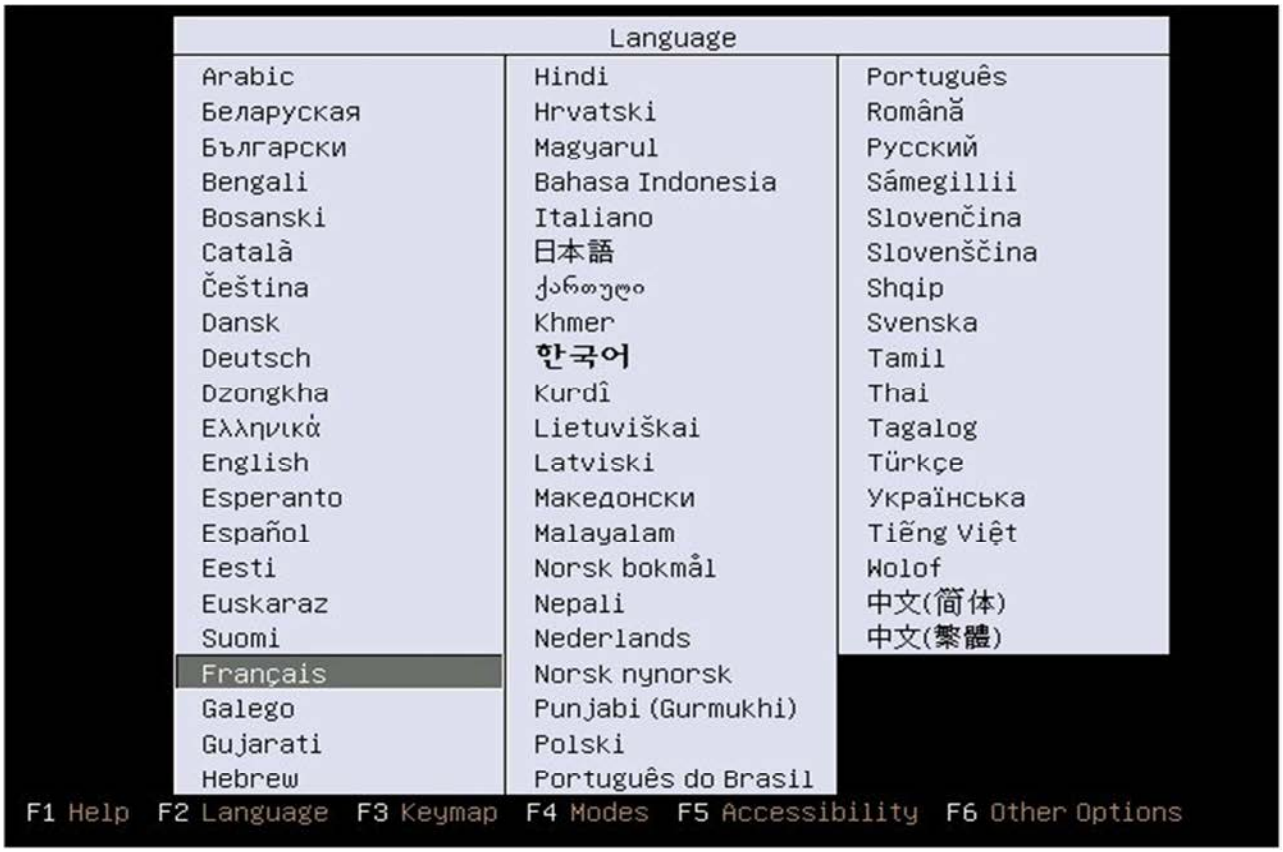
Choisissez la version 32bits ou 64bits suivant votre machine (en cas de doute utilisez la version 32Bits).

Cliquez sur le bouton DOWNLOAD. Le téléchargement débute

Une fois l'image obtenue vous pouvez la graver depuis votre logiciel de gravure préféré.

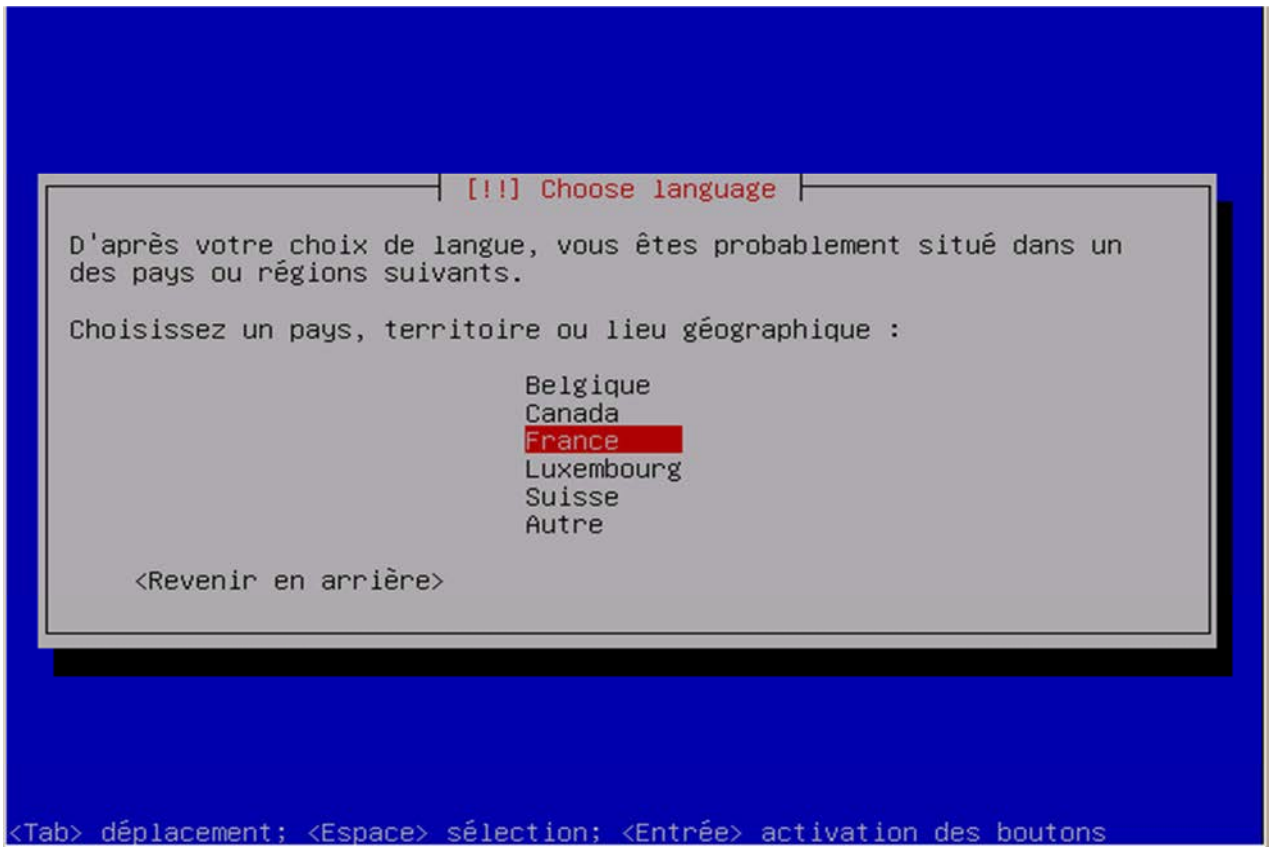
Installation du serveur

1. Insérer le cdrom dans la machine puis rebooter
2. L'écran de démarrage apparait



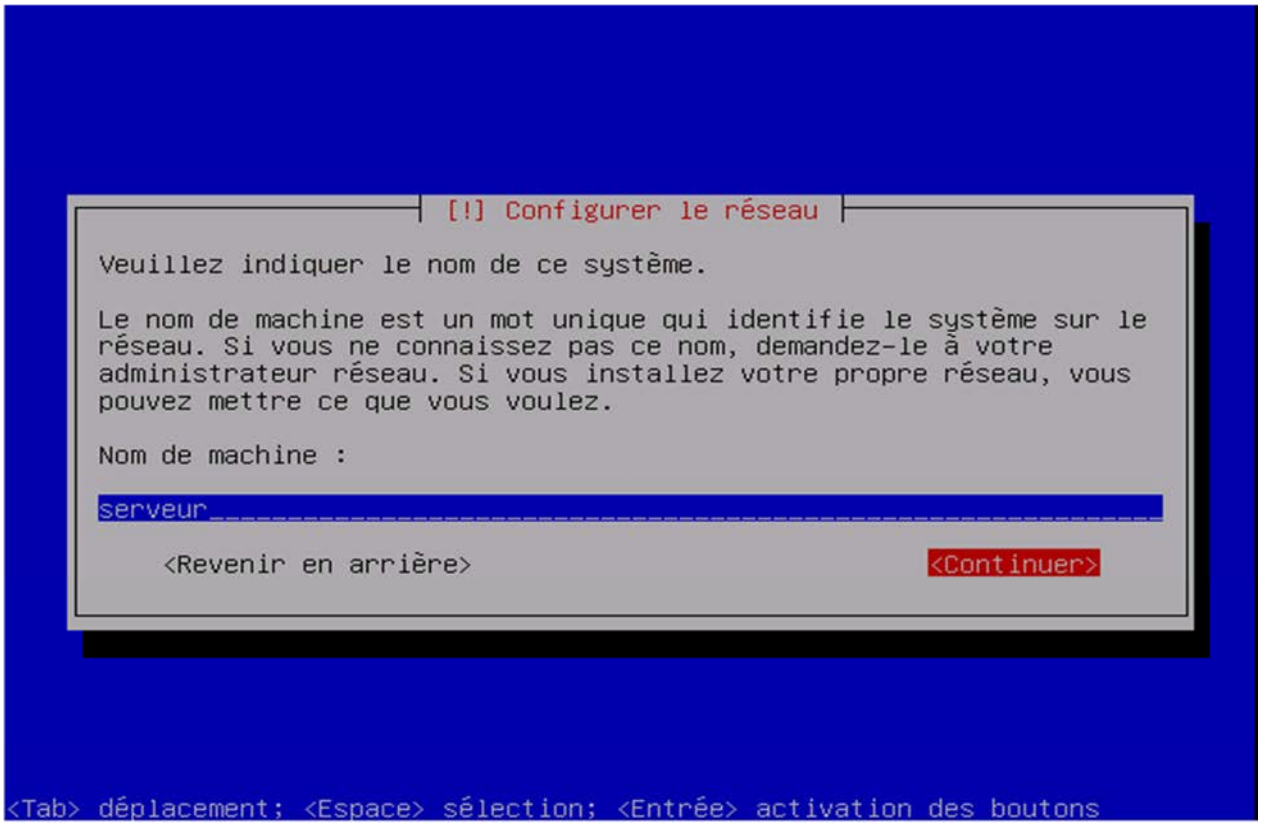
3. Sélectionner "Install Ubuntu Server"

4. Choisir votre pays



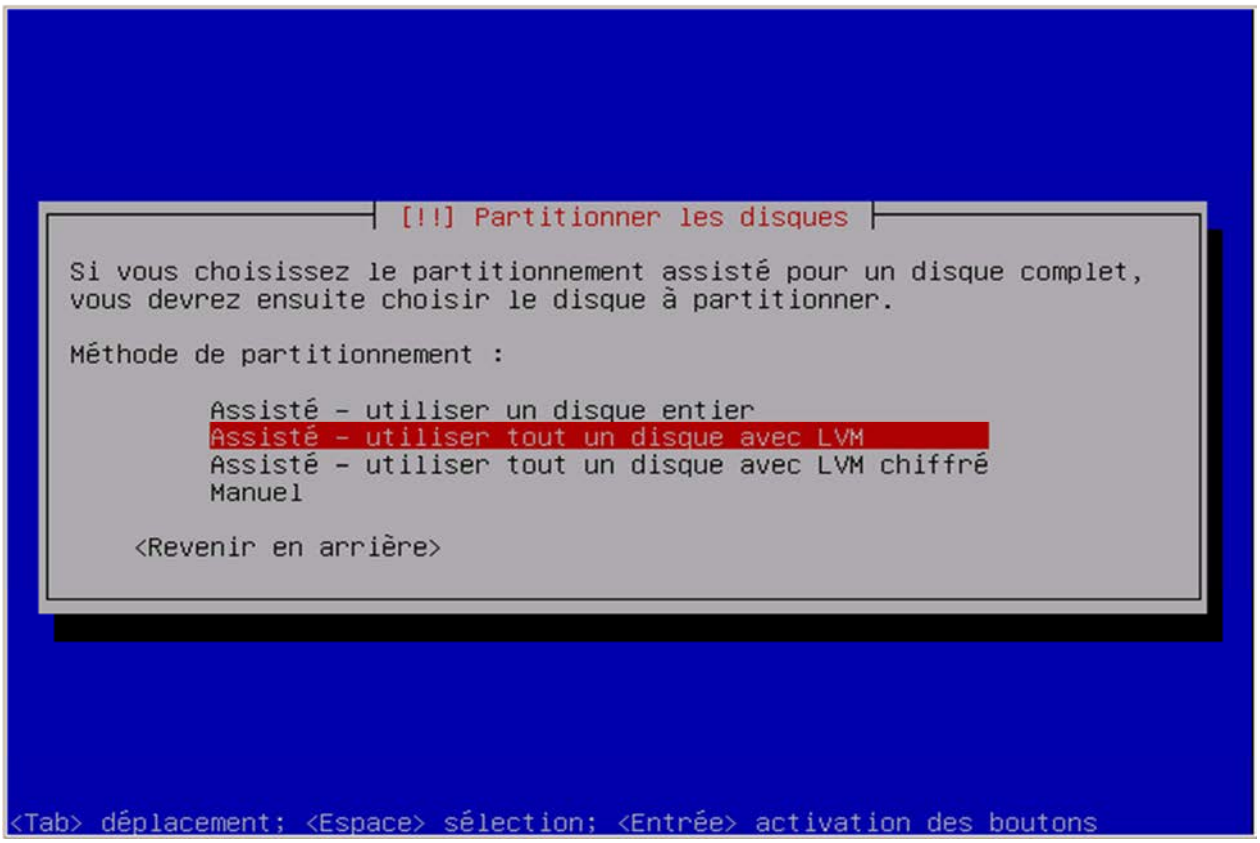
5. Nom de la machine

Ce nom ce doit d'être unique sur votre réseau.

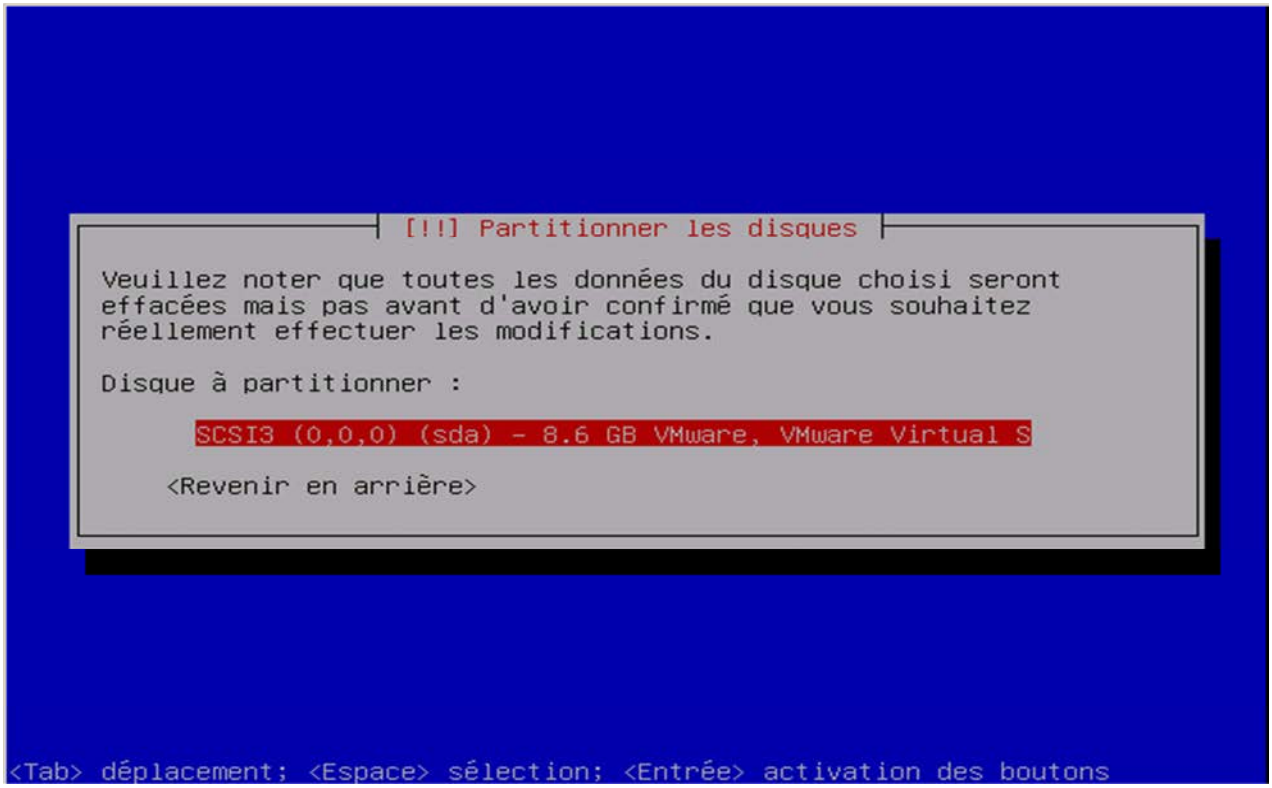


6. Choix du partitionnement

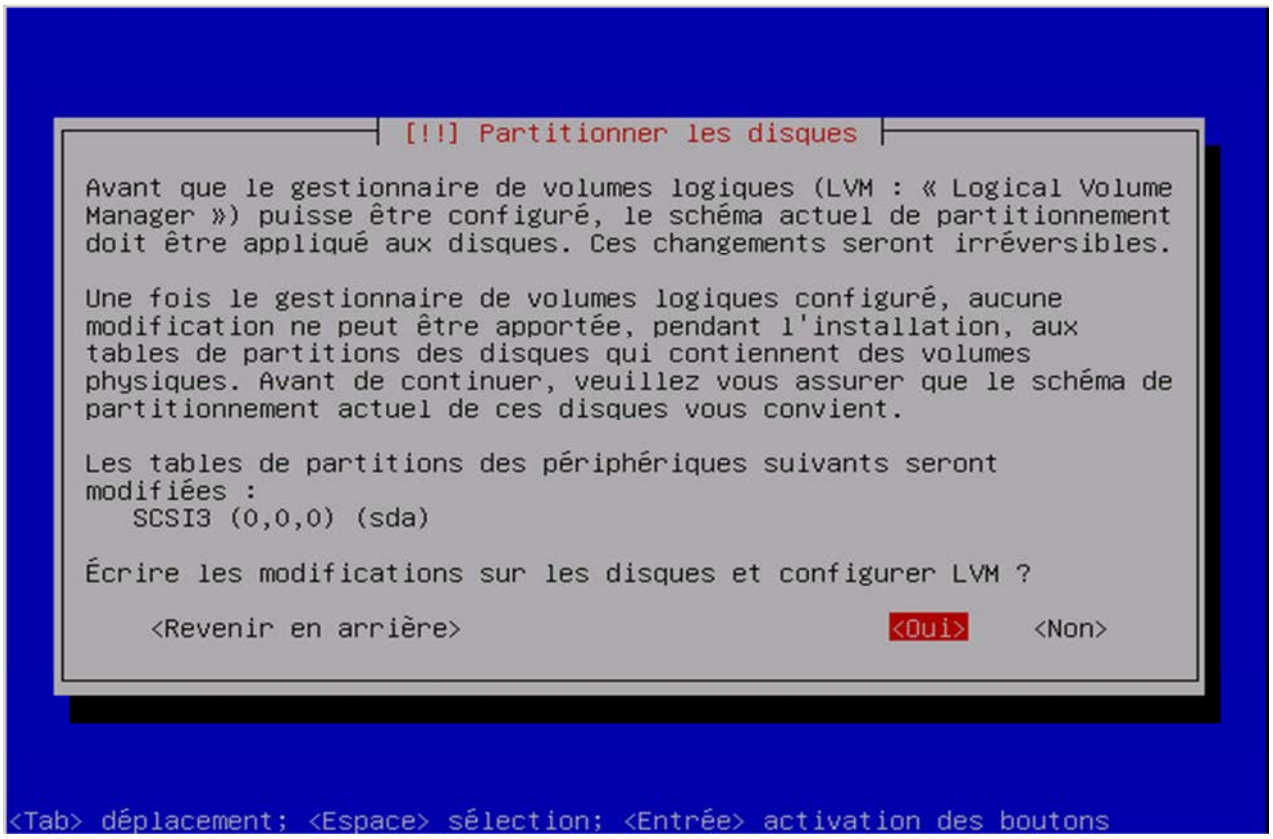
Sauf spécifications particulière utilisez le montage par LVM des partitions. LVM est un outil ajouter, supprimer, modifier des partitions d'un ou de plusieurs disques durs à la volée ou à chaud. Il vous permettra toutes les modifications que vous désirerez par la suite, ainsi que la possibilité de faire des snapshots.

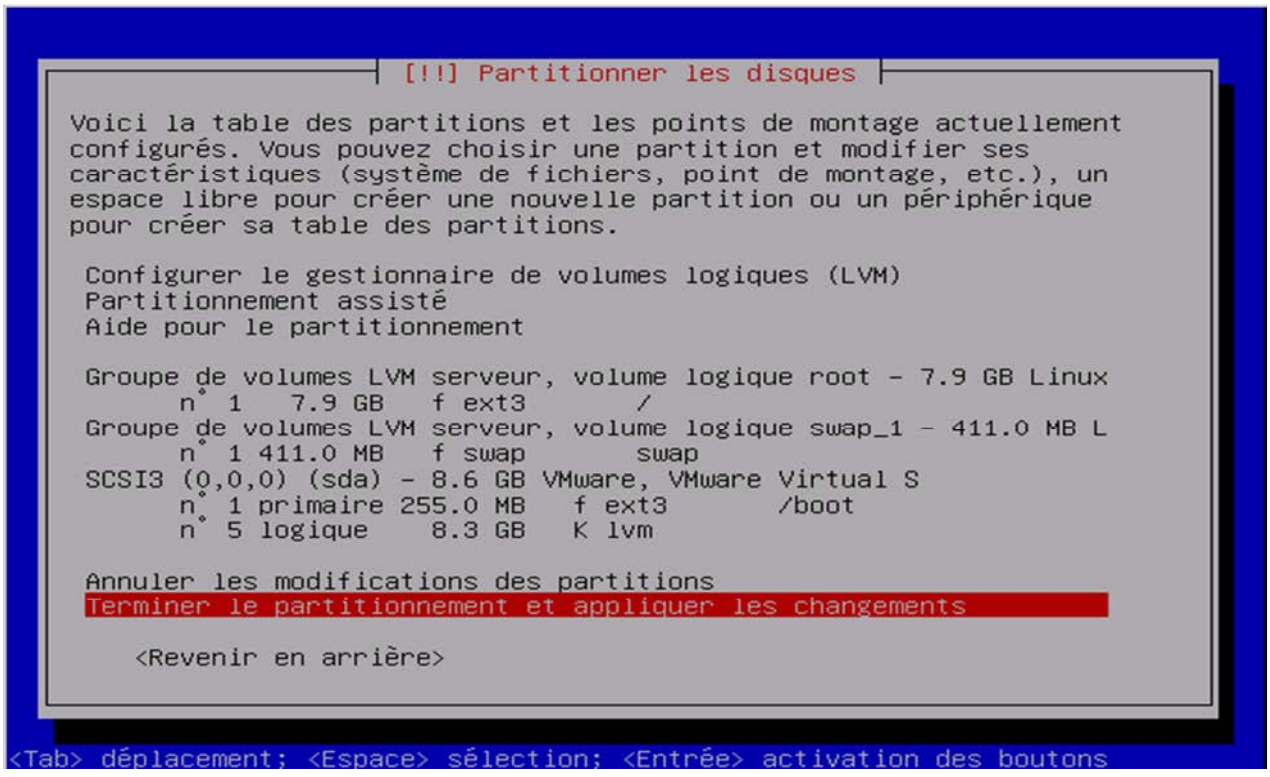


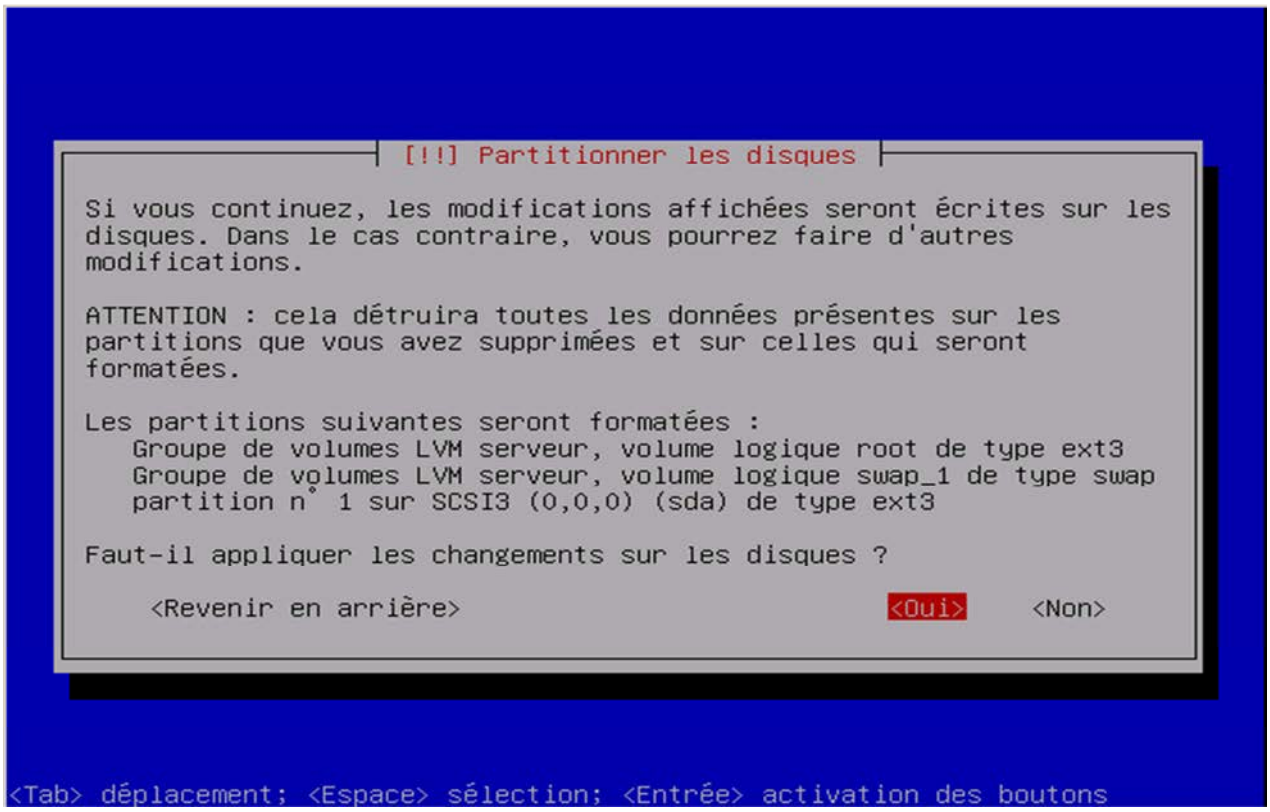
7. Choix du disque à partitionner



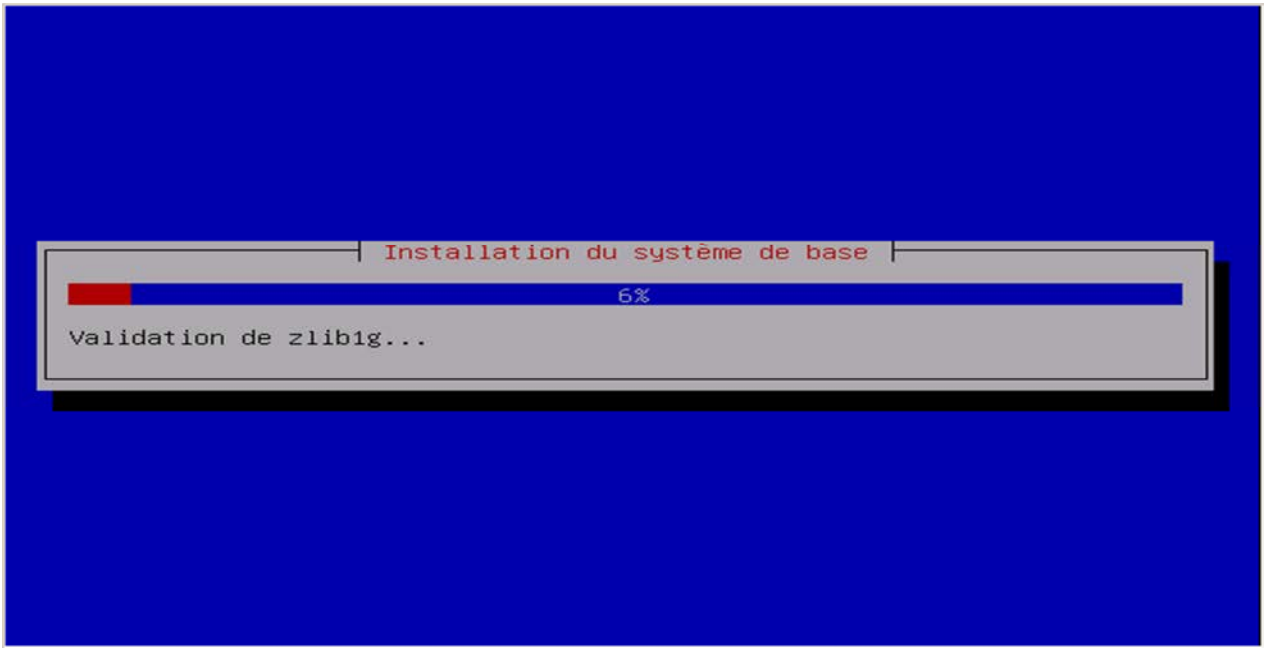
8. Partitionnement


[!!] Partitionner les disques
Avant que le gestionnaire de volumes logiques (LVM : « Logical Volume Manager ») puisse être configuré, le schéma actuel de partitionnement doit être appliqué aux disques. Ces changements seront irréversibles.
Une fois le gestionnaire de volumes logiques configuré, aucune modification ne peut être apportée, pendant l'installation, aux tables de partitions des disques qui contiennent des volumes physiques. Avant de continuer, veuillez vous assurer que le schéma de partitionnement actuel de ces disques vous convient.
Les tables de partitions des périphériques suivants seront modifiées :
SCSI3 (0,0,0) (sda)
Écrire les modifications sur les disques et configurer LVM ?
<Revenir en arrière>
<Oui>
<Non>
<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons


[!!] Partitionner les disques
Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.
Configurer le gestionnaire de volumes logiques (LVM)
Partitionnement assisté
Aide pour le partitionnement
Groupe de volumes LVM serveur, volume logique root - 7.9 GB Linux
n° 1 7.9 GB f ext3 /
Groupe de volumes LVM serveur, volume logique swap_1 - 411.0 MB L
n° 1 411.0 MB f swap swap
SCSI3 (0,0,0) (sda) - 8.6 GB VMware, VMware Virtual S
n° 1 primaire 255.0 MB f ext3 /boot
n° 5 logique 8.3 GB K lvm
Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements
<Revenir en arrière>
<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons



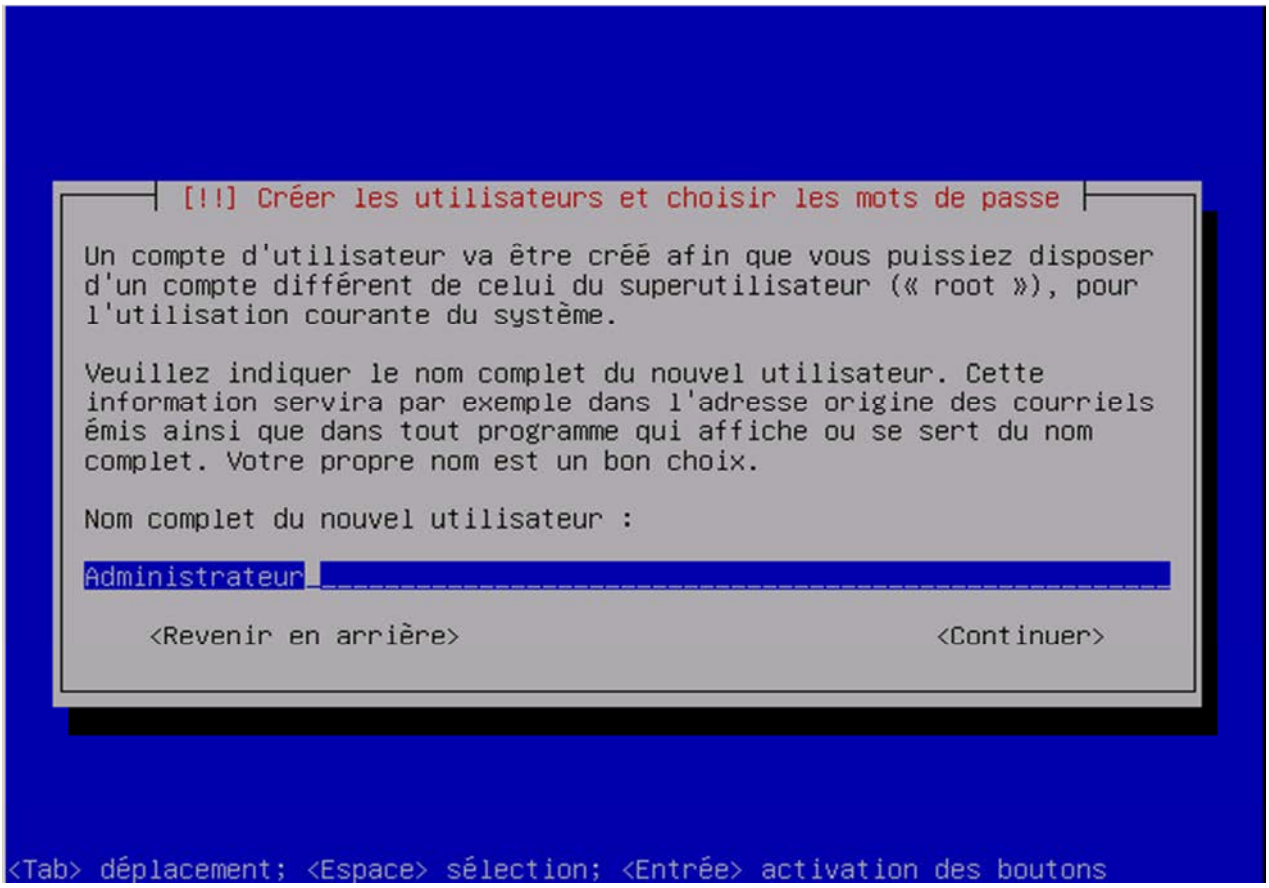
9. Installation du système de base



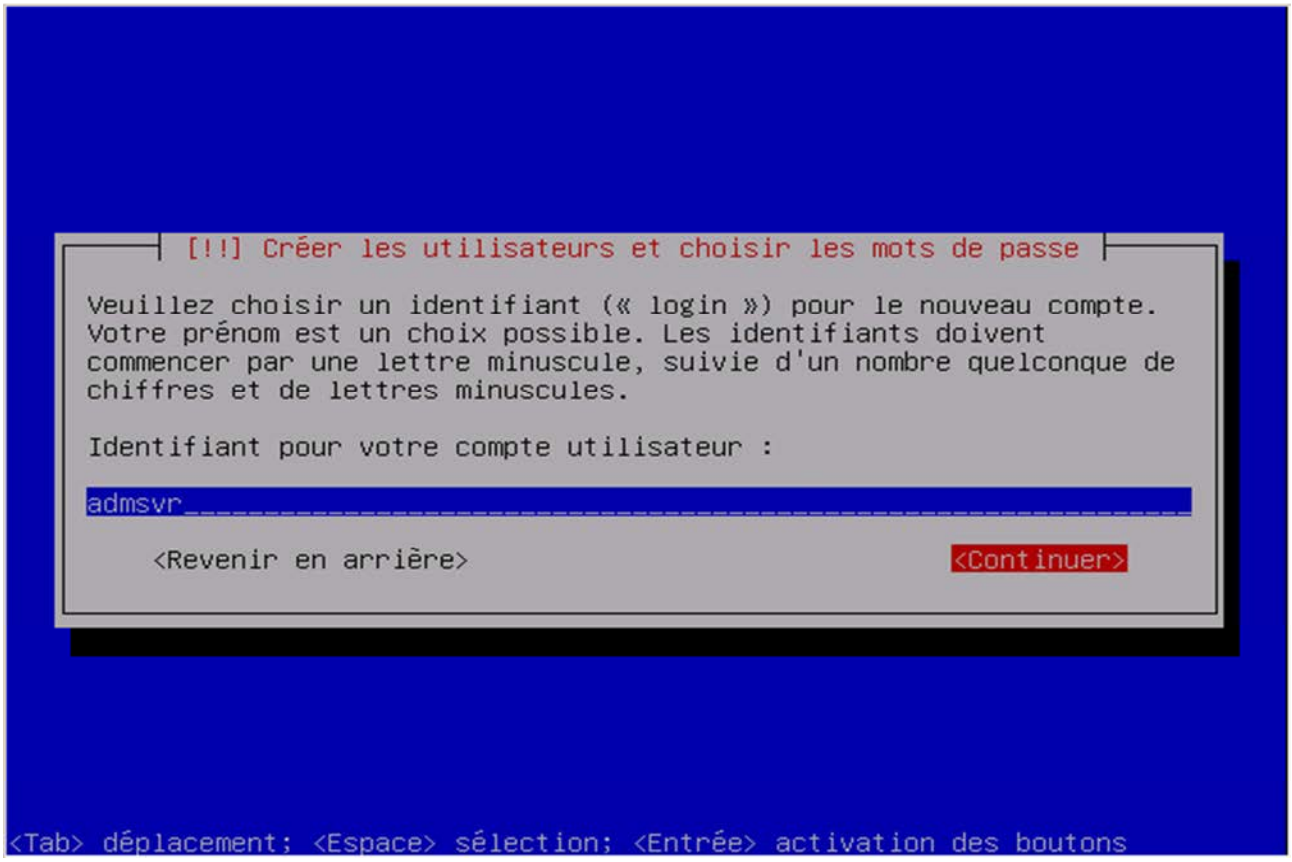
10. Création de l'utilisateur principal.

Sous Ubuntu, l'utilisateur root n'est utilisé que contraint et forcé pour des applications non sécurisées.

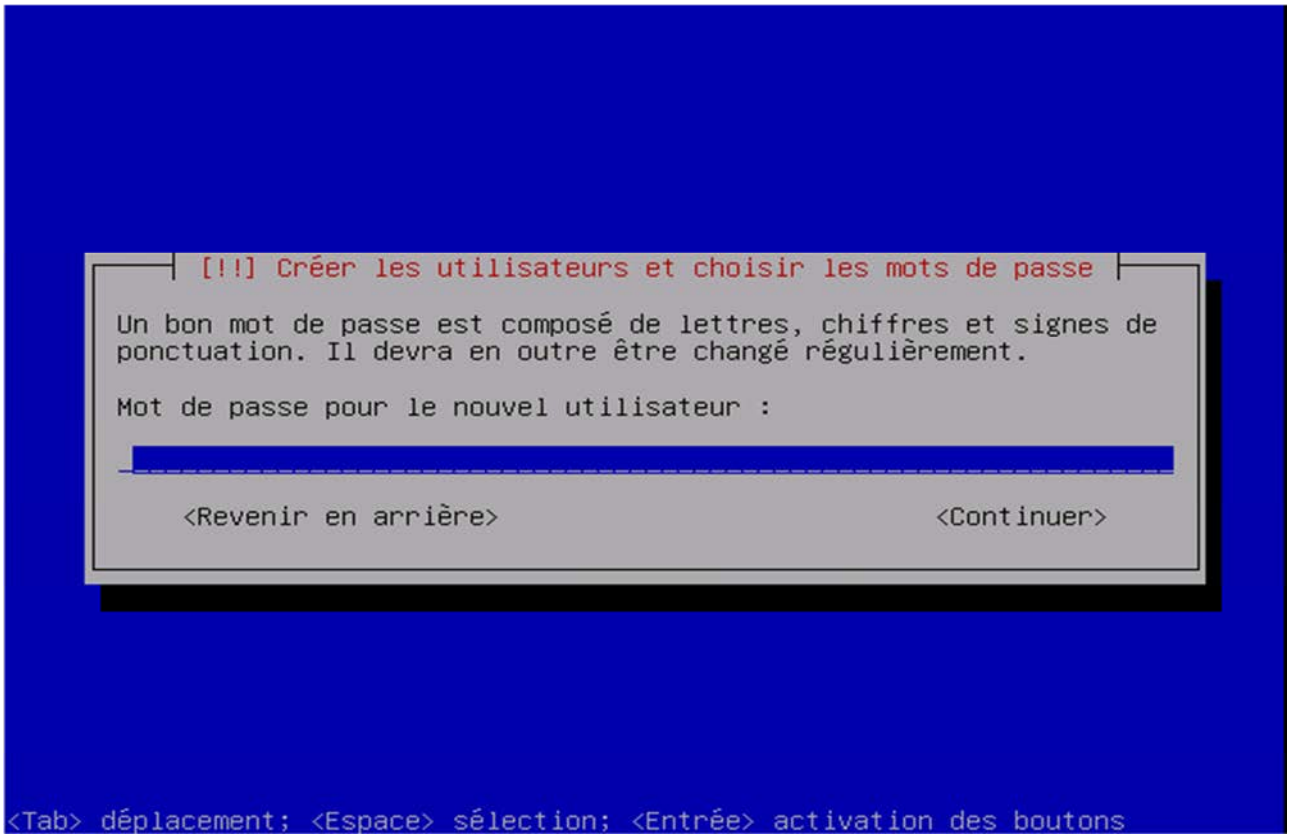
Entrez d'abord le nom complet de l'utilisateur



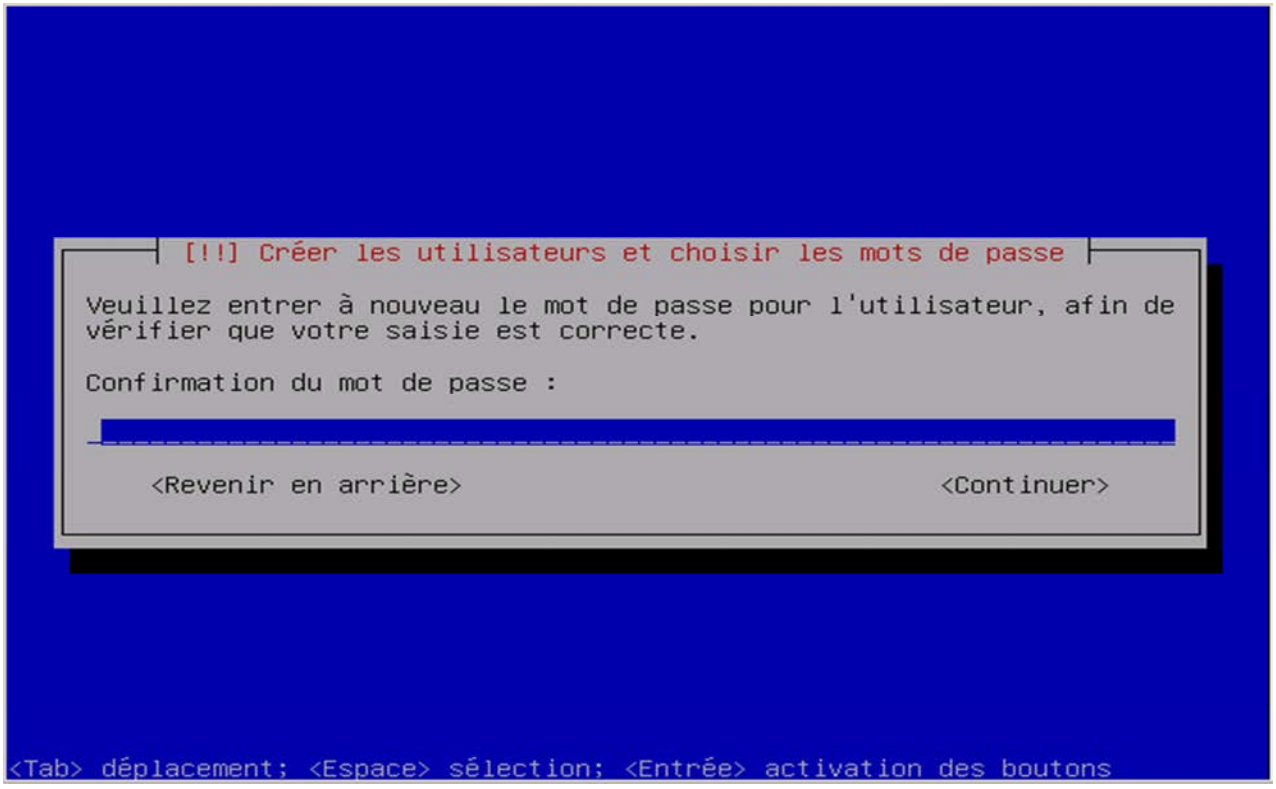
Entrez ensuite l'identifiant de l'utilisateur principal



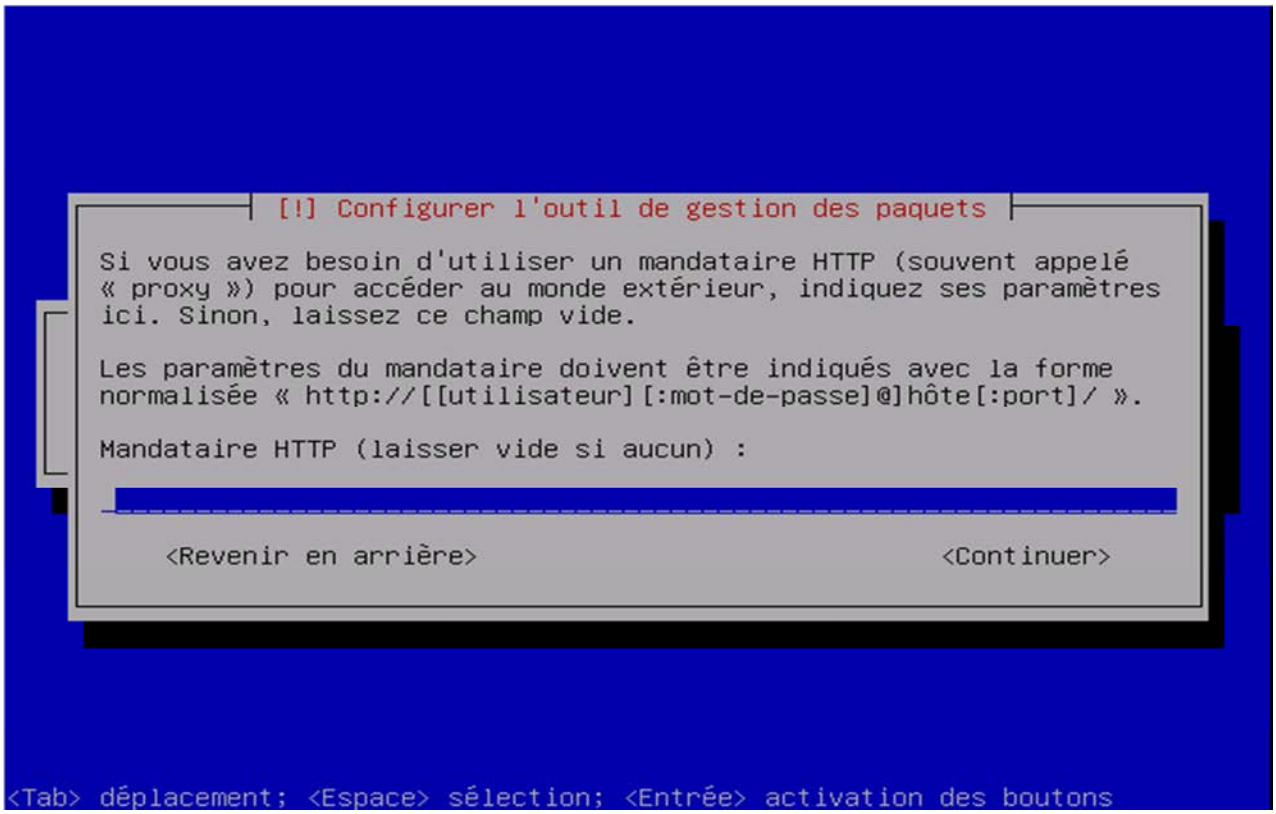
Entrez le mot de passe de l'utilisateur principal



Confirmez votre mot de passe



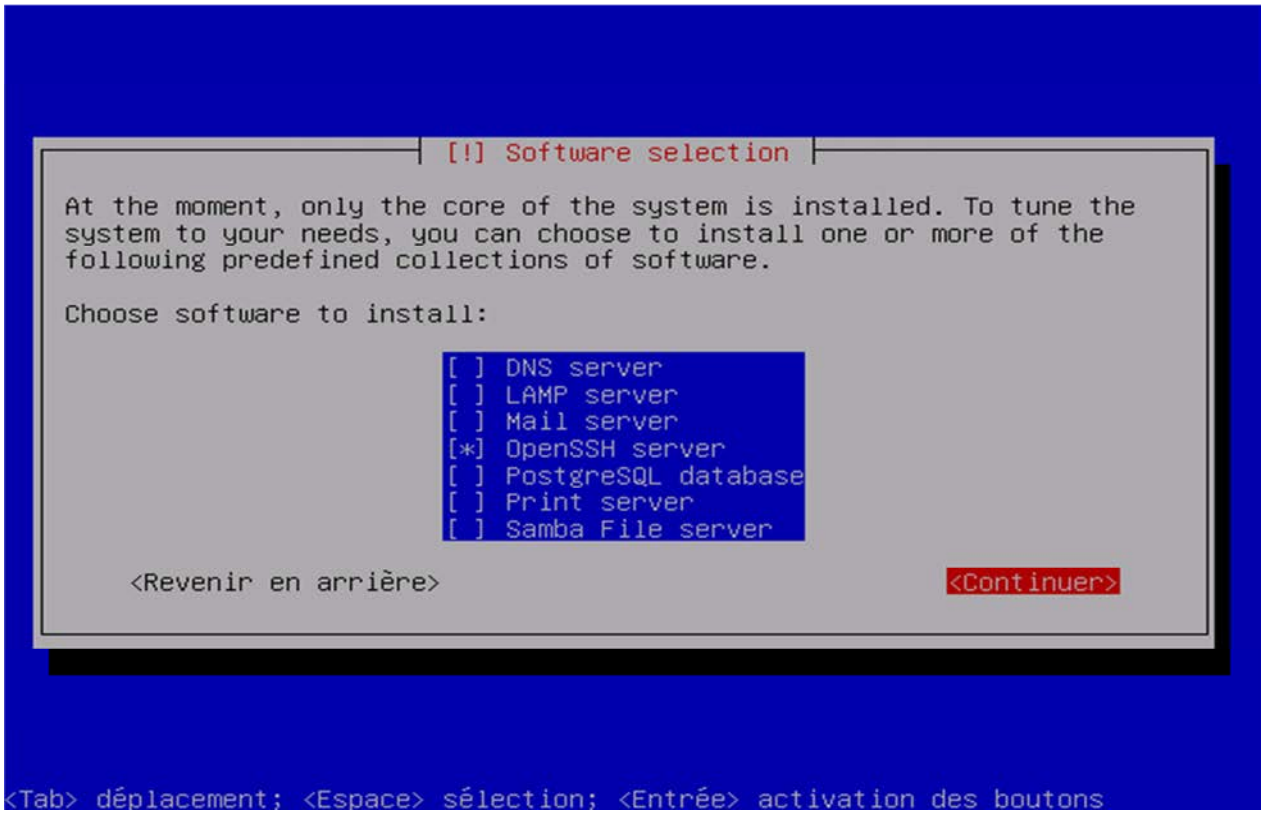
11. Choix du proxy



12. Choix des serveurs applicatifs

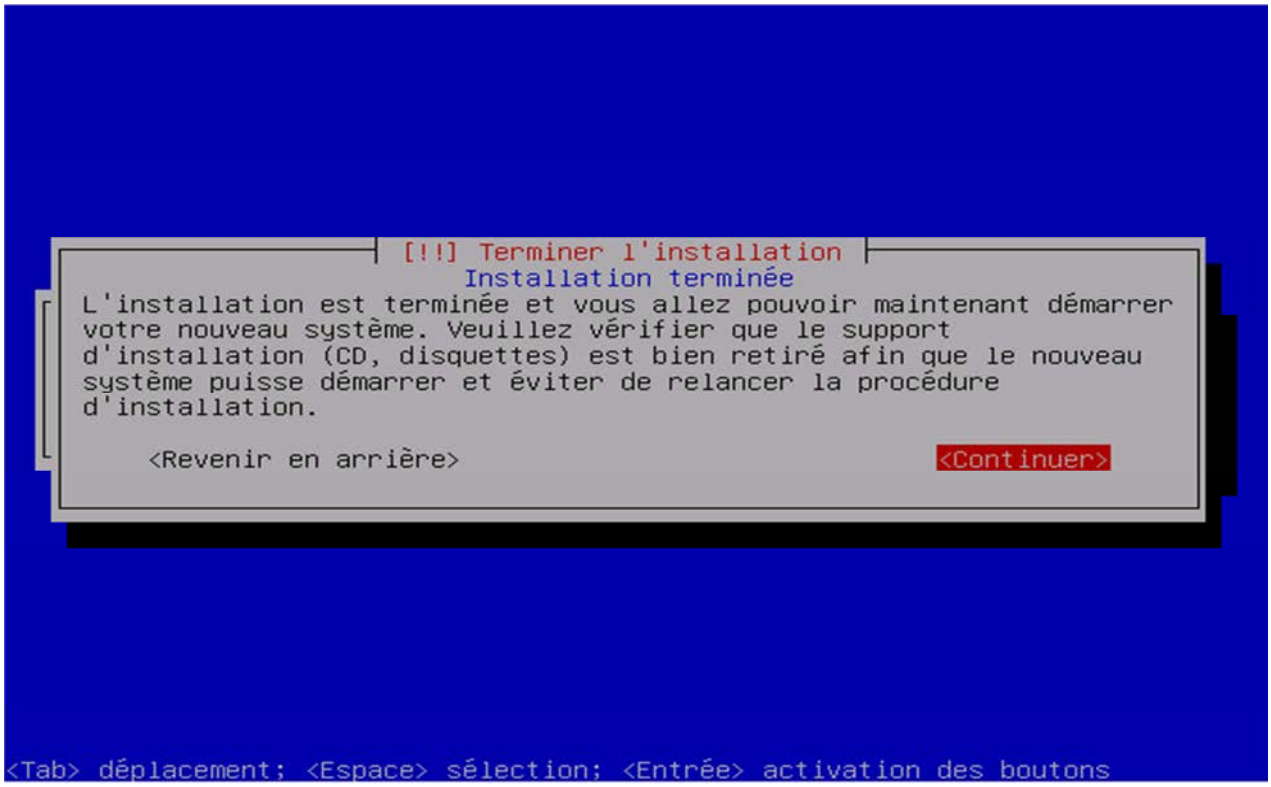
Suivants les utilisations de votre serveur choisissez l'une des options ci-dessous. Ses applicatifs peuvent être installés par la suite

Il est conseillé de monté le serveur openSSH dans tout les cas afin de permettre une prise en main à distance en toute sécurité.



13. Fin de l'installation

Redémarrez le serveur



14. Connexion au serveur

Entrez votre login

```
/dev/mapper/serveur-root: clean, 17620/483328 files, 150641/1933312 blocks
                                                                       [ OK ]
 * Checking file systems...
fsck 1.40.8 (13-Mar-2008)
/dev/sda1: recovering journal
/dev/sda1: clean, 31/62248 files, 33074/248976 blocks
                                                                       [ OK ]
 * Mounting local filesystems...                                      [ OK ]
 * Activating swapfile swap...                                        [ OK ]
$Mounting securityfs on /sys/kernel/security: done.
Loading AppArmor profiles : done.
 * Checking minimum space in /tmp...                                 [ OK ]
 * Skipping firewall: ufw (not enabled)...                           [ OK ]
 * Configuring network interfaces...                                 [ OK ]
 * Setting up console font and keymap...                             [ OK ]
 * Starting system log daemon...                                     [ OK ]
 * Starting kernel log daemon...                                     [ OK ]
 * Starting OpenBSD Secure Shell server sshd                         [ OK ]
 * Starting deferred execution scheduler atd                         [ OK ]
 * Starting periodic command scheduler crond                         [ OK ]
 * Running local boot scripts (/etc/rc.local)                        [ OK ]

Ubuntu 8.04.1 serveur tty1

serveur login: admsrv_
```

Entrez votre mot de passe

```
 * Starting OpenBSD Secure Shell server sshd                         [ OK ]
 * Starting deferred execution scheduler atd                         [ OK ]
 * Starting periodic command scheduler crond                         [ OK ]
 * Running local boot scripts (/etc/rc.local)                        [ OK ]

Ubuntu 8.04.1 serveur tty1

serveur login: admsvr
Password:
Linux serveur 2.6.24-19-server #1 SMP Wed Jun 18 15:18:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

admsvr@serveur:~$  * Reloading OpenBSD Secure Shell server's configuration sshd
_
```

15. Faire les mises à jour

sudo aptitude safe-upgrade

16. Votre serveur est prêt.

4.2.3 Étude des applications serveurs, de leur mise en œuvre et leur sécurisation

4.2.3.1 Serveur Web

a) Concept d'un serveur web

Un serveur Web dans le sens des réseaux actuels, notamment dans l'environnement Linux, ne se limite pas au simple serveur HTTP mais inclut de nombreuses autres applications lui apportant diverses fonctionnalités. Une combinaison très implémentée est LAMP (Linux, Apache, MySQL, PHP) qui combine sous Linux le serveur HTTP Apache avec le SGBD (Système de Gestion de Base de Données) MySQL et la plate-forme PHP pour générer des pages web dynamiques. Pour héberger les sites web de BIG, nous avons opté pour la mise en place d'un LAMP.

b) L'installation des applications pour le serveur Web

- ✓ **Installation de apache 2**

Il nous faut tout d'abord installer le serveur HTTP apache2 qui permettra d'afficher les différentes pages.

 # aptitude install apache2

Pour s'assurer du bon fonctionnement d'Apache, On saisit l'URL suivante dans le navigateur Internet : *http://adresse_du_serveur_Web*. Si Apache a été correctement installé il s'affiche une page Web dans laquelle apparaît l'index du répertoire Web ainsi que le dossier « *apache2-default* »

- ✓ **Installation de php5**

A ce stade, le serveur peut nous afficher des pages statiques au format HTML. Les sites que nous aurons à héberger disposent d'une partie dynamique. C'est pourquoi nous poursuivons par l'installation de PHP sur le serveur.

 # aptitude install php5

Pour vérifier si PHP a été correctement installé nous allons créer un fichier phpinfo.php dans le répertoire ***/var/www***. Pour cela, tapez dans un terminal :

 # echo "<? PHP phpinfo(); ?>" > /var/www/phpinfo.php

En saisissant http://adresse_de_la_machine/phpinfo.php cela nous affiche des informations concernant php5.

✓ **Installation du SGBD MySQL**

PHP est très souvent couplé à un système de gestion de base de données : MySQL dans notre cas. Nous installons donc MySQL-server version 5 étant donné que certains sites à héberger comportent des bases de données.

 # aptitude install mysql-server-5.0

Puis définir le mot de passe root de MySQL. Dans l'écran suivant, il demande s'il faut gérer les connexions d'hôtes qui utilisent Debian Sarge. On répond OUI.

Pour vérifier que MySQL fonctionne bien, saisir: **# mysql -p**

Puis entrer le mot de passe:

Pour quitter on exécute la commande: **>Exit;**

✓ **Installation des librairies php5-mysql :**

L'installation du module PHP-MySQL est nécessaire pour permettre la communication entre PHP et MySQL:

 # aptitude install php5-mysql

✓ **Installation de PhpMyAdmin**

C'est pour l'administration en mode graphique du SGBD MySQL.

La commande est: **# aptitude install phpmyadmin**

Après on redémarre Apache par: **#/etc/init.d/apache2 restart**

On peut se connecter à l'interface d'administration phpmyadmin en saisissant l'URL suivante: http://adresse_de_la_machine/phpmyadmin.

✓ **Installation du ftp (VSFTPD)**

Avoir un site disponible sur le Net, c'est bien. Pouvoir y mettre des fichiers (mise à jour des sites Web), c'est encore mieux. Et c'est le but de VSFTPD qui est un serveur FTP (File Transfer Protocol) très sécurisé. On l'installe par la commande:

 # aptitude install vsftpd

La configuration des applications

- **apache2**

Il faut tout d'abord configurer le serveur Web (apache) lui même. C'est lui qui va permettre l'interprétation des pages HTML, PHP, etc. Il permet de gérer des sites virtuels. Et c'est de cette manière que nous allons le configurer. En effet, le but étant de disposer de plusieurs sites sur notre serveur, il nous faut pouvoir les contacter directement avec une URL propre, notre serveur ne disposant que d'une adresse IP pour tous les sites à héberger.

Nous créerons une entrée pour chaque site hébergé sur notre serveur. C'est là que la gestion des virtualhosts va intervenir. Lorsque la requête atteint le serveur HTTP, celui-ci consulte le fichier de configuration afin de trouver dans quel répertoire la requête doit être dirigée.

Éditons le fichier de configuration principal d'apache2 : **/etc/apache2/apache2.conf**:

On vérifie l'utilisateur et le groupe d'apache (aux environs de la ligne 100) et la présence des lignes d'inclusion des fichiers de configuration des hôtes virtuels.

```
User www-data          # la directive User spécifie l'utilisateur de apache sur le système
Group www-data         # la directive Group pour le groupe de l'utilisateur  apache

# Include the virtual host configurations:

Include /etc/apache2/sites-enabled/   # inclusion du fichier de configuration des VirtualHosts
```

- **Configuration des virtualHosts**

Le Serveur Web Apache2 étant capable de gérer simultanément plusieurs arborescences Web grâce à la notion de VirtualHosts, il nous permettra d'héberger les différents sites qui sont à notre disposition. Les modifications se font dans le fichier ***/etc/apache2/sites-enabled/000-default***. La déclaration d'un VirtualHost se fait selon la syntaxe:

```
NameVirtualHost *
<VirtualHost *>

  directive_1 valeur_1
  directive_2 valeur_2
   ........
 directive_n valeur_n

</VirtualHost>
```

Contenu du fichier ***/etc/apache2/sites-enabled/000-default**:*

```
############################## »SITE DE BIG#################################
NameVirtualHost *                    #début du virtualHost de BIG
<VirtualHost *>
        ServerAdmin machiax@yahoo.fr      # en cas de problème le serveur apache envoie un mail à cette adresse
        ServerName www.big-burkina.homelinx.net          #Fixe le nouveau nom public pour la page d'accueil du site
        DocumentRoot /var/www/site-big/   #Répertoire racine où se trouvent les pages Web.

        <Directory />                                #début du paramétrage des droits d'accès d'apache sur   le  répertoire
                                                     # racine du site
                Options FollowSymLinks
                AllowOverride None
        </Directory>                    #fin du paramétrage des droits d'accès d'apache sur le répertoire racine du site
<Directory  /var/www/site-big>     # début du paramétrage des droits d'accès au répertoire racine du site

                Options Indexes FollowSymLinks MultiViews
                AllowOverride None
                Order allow,deny
                allow from all
</Directory>                                     # fin du paramétrage des droits d'accès au répertoire racine du site

ErrorLog /var/log/apache2/error.log                 # le fichier d'enregistrement des erreurs rencontrées par apache

        # Possible values include: debug, info, notice, warn, error, crit,
        # alert, emerg.
        LogLevel warn
```

```
        CustomLog /var/log/apache2/access.log combined          # le fichier d'enregistrement des accès à apache
        ServerSignature On
</VirtualHost>
```

L'ajout des autres sites se fera de la même façon.

- ✓ **configuration de la base de données MySQL**

La configuration va consister à l'importation des bases de données utilisées par les différents sites. Cela nous est facilité par l'interface d'administration phpmyadmin.

- ✓ **Configuration de VSFTPD en mode "utilisateur virtuel"**

VSFTPD dispose de plusieurs styles de paramétrage de base. Nous utiliserons le paramétrage par utilisateur virtuel. Pour ce faire, nous allons utiliser une base de données de type Berkeley. Il s'agit d'une base de type non-SQL. Elle n'est pas prévue pour être interrogée comme MySQL ou SQL server. En fait, il s'agit d'une table de hachage. Chaque enregistrement ne sera constitué que d'un login et d'un mot de passe.

Pour le principe, nous ne définissons qu'un seul utilisateur Unix à notre serveur FTP. Lorsque l'on se connecte avec un utilisateur virtuel, le programme vérifie dans notre base de données si celui-ci existe, et si le mot de passe correspond. A partir de là, il va chercher les paramètres concernés (chroot, droits spécifiques) et renvoie le répertoire concerné.

Grâce au chroot, il n'y a aucun souci de sécurité, car le répertoire est considéré comme étant un répertoire racine, il n'est donc pas possible de remonter la hiérarchie. Ce point est important pour la sécurité, car chaque connexion FTP utilise exactement le même utilisateur Unix : **www-data**. Il faut commencer par installer la base de données adéquate:

 # aptitude install db4.5-util

Ce type de base de données est extrêmement simple. Elle se base sur un fichier de type texte contenant nos différentes informations, entrées une à une. En fait, il n'y a pas de tables, ni de champs à configurer. On va juste convertir un fichier contenant nos données ayant la forme suivante:

login 1
password 1
login 2
password 2
...
login n
password n

Les fichiers de configuration de base de vsftpd sont placés dans /etc/. Pour gérer notre nouvelle configuration, plus évoluée, nous allons tout d'abord créer un nouveau répertoire qui contiendra tous nos fichiers. **# mkdir /etc/vsftpd**
On sauvegarde les anciens fichiers de configuration:
 # cp /etc/vsftpd.conf /etc/vsftpd.conf.default.old
 # cp /etc/pam.d/vsftpd /etc/pam.d/vsftpd.default.old

On va maintenant modifier notre fichier *vsftpd.conf*.
Contenu de **/etc/vsftpd.conf** :

```
# Ceci configure vsFTPd en mode "standalone"
listen=YES

# Masquer la bannière vsftp par défaut
ftpd_banner="FTP Server"

# On désactive les connexions anonymes
# et on active les non-anonymes (c'est le cas des utilisateurs virtuels):
anonymous_enable=NO
local_enable=YES

# Pour des raisons de sécurité on interdit toute action d'écriture
# et on cache les uids et gids associés aux répertoires/fichiers
write_enable=NO
anon_upload_enable=NO
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
```

```
hide_ids=YES

# 'guest_enable' est très important: cela active les utilisateurs virtuels!
# 'guest_username' fait correspondre tous les utilisateurs virtuels à
# l'utilisateur 'www-data' que nous avons défini plus haut, et au home
# correspondant: '/var/www/'.
guest_enable=YES
guest_username=www-data
# On veut que les utilisateurs virtuels restent chez eux: '/var/www/'
chroot_local_user=YES

# Définir la plage des ports sur laquelle le client pourra se connecter
pasv_max_port=2020
pasv_min_port=2000

# On défini le nombre maximum de sessions à 10(les nouveaux clients recevront
# un message du genre: "erreur: serveur occupé").
# On défini le nombre maximum de sessions par IP à 2
max_clients=10
max_per_ip=2

# Enregistrer les actions des utilisateurs
xferlog_enable=YES
xferlog_file=/var/log/vsftpd.log
log_ftp_protocol=YES

#######################################
# This option should be the name of a directory which is empty.  Also, the
# directory should not be writable by the ftp user. This directory is used
# as a secure chroot() jail at times vsftpd does not require file system
# access.
secure_chroot_dir=/var/run/vsftpd

# Le service PAM doit utiliser le démon vsftpd
```

```
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/vsftpd.pem

# Chaque utilisateur à une configuration propre présente dans le répertoire
# vsftpd_user_conf
user_config_dir=/etc/vsftpd/vsftpd_user_conf
```

- **Création de la base de données des utilisateurs virtuels**

Cette base de données contient les login et mots de passe des utilisateurs virtuels. Ces utilisateurs virtuels auront juste pour but de mettre à jour les sites web. Contenu du fichier ***/etc/vsftpd/login****:*

```
site-big
big-pass (mot de passe)
```

Remarque: il faut être sûr de terminer le fichier par un retour chariot.

On a ainsi un utilisateur, site-big ayant comme password big-pass.

Il faut maintenant convertir le fichier en une base de données:

 # db4.5_load -T -t hash -f /etc/vsftpd/login /etc/vsftpd/login.db
 # chmod 600 /etc/vsftpd/login.db

Et modifier la configuration pam pour utiliser notre base login.db comme source d'authentification de vsftpd. Créer le fichier /etc/vsftpd/vsftpd.pam et ajoutez-y les lignes suivantes:

```
auth required /lib/security/pam_userdb.so db=/etc/vsftpd/login
account required /lib/security/pam_userdb.so db=/etc/vsftpd/login
```

Ensuite, copiez ce fichier dans le dossier de configuration PAM:

 # cp /etc/vsftpd/vsftpd.pam /etc/pam.d/vsftpd

Si le système nous informe que le fichier existe déjà, on l'écrase.

On crée le dossier ***/etc/vsftpd/vsftpd_user_conf*** que l'on a mentionné dans le fichier ci-dessus pour contenir la configuration des utilisateurs virtuels

 # mkdir /etc/vsftpd/vsftpd_user_conf/

- **Les répertoires des utilisateurs virtuels**

Chaque fichier de configuration est désigné par le nom de l'utilisateur virtuel auquel il est associé. Pour l'utilisateur site-big, nous allons accorder tous les droits. On créé le fichier ***/etc/vsftpd/vsftpd_user_conf/site-big*** et on y met les lignes qui spécifient les droits d'accès:

```
anon_world_readable_only=NO
anon_upload_enable=NO
write_enable=YES
anon_mkdir_write_enable=NO
anon_other_write_enable=NO
local_root=site-big
```

Les droits d'accès de l'utilisateur virtuel site-big, pouvant faire la mise à jour du site de BIG par FTP étant définis, le procédé est le même pour fixer les droits d'un utilisateur virtuel chargé de la mise à jour d'un autre site web qui sera hébergé sue ce serveur aussi. Il faut signaler que ces utilisateurs ne peuvent faire que la mise à jour des sites pour lesquels ils ont été créés sur le système. En ligne de commande on utilise:

 # ftp login@adresse**_IP_serveur**

Il existe cependant de nombreux outils graphiques tels que filezilla, gFTP, etc pour se connecter à un serveur par FTP.

En somme nous avons mis en place un serveur Web dans le but d'héberger les sites de BIG grâce au serveur HTTP Apache2. Ces sites Web étant du genre dynamique avec des bases de données, nous avons utilisé le duo PHP et MySQL. Les mises à jour se feront de manière conviviale et très sécurisée par le serveur de transfert de fichiers VSFTPD. Nous pensons que BIG sera ainsi doté d'un serveur Web adapté à ses besoins en communication.

4.2.3.2 Les services internes du réseau

a) Serveur DHCP

L'affectation et la mise à jour d'informations relatives aux adresses IP fixes (cas où il n'ya pas de serveur DHCP) peuvent représenter une lourde tâche. Afin de faciliter ce travail et de simplifier la distribution des adresses IP, le protocole DHCP offre une configuration dynamique des adresses IP et des informations associées.

Le principe du DHCP

Voici le principe de fonctionnement du service DHCP (figure 4.3 ci-dessous):

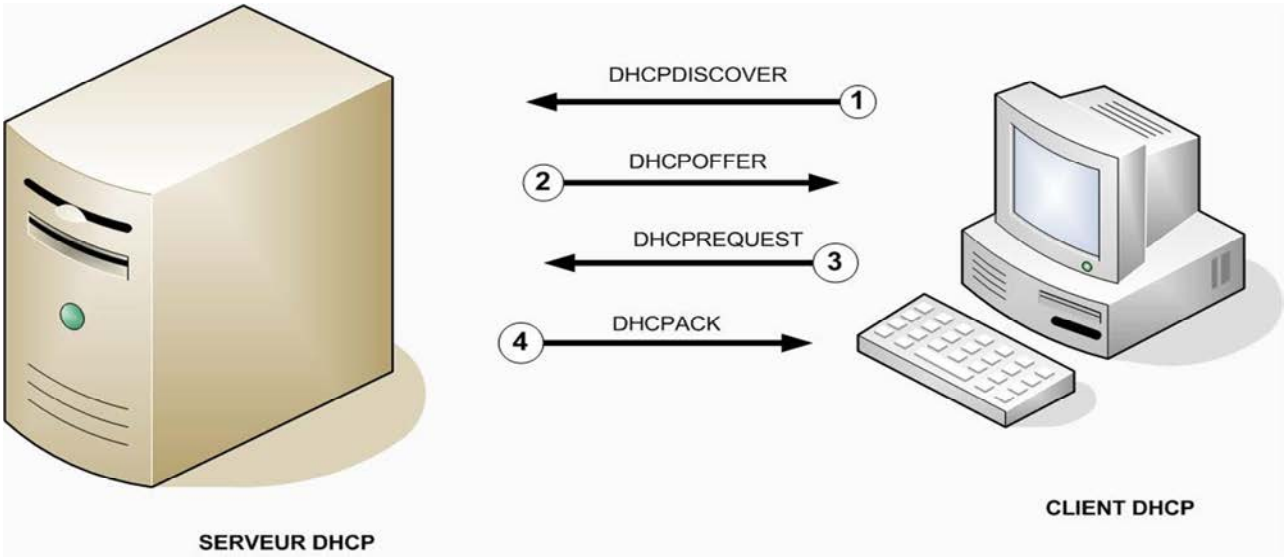


Figure 4.3: Schéma illustrant le principe de fonctionnement du DHCP

- Lorsque le client DHCP démarre, il n'a aucune connaissance du réseau, du moins, en principe. Il envoie donc une trame **"DHCPDISCOVER",** destinée à trouver un serveur DHCP. Cette trame est un "broadcast"(elle est destinée à toutes les machines du réseau), donc elle est envoyée à l'adresse 255.255.255.255. N'ayant pas encore d'adresse IP, il adopte provisoirement l'adresse 0.0.0.0. Comme ce n'est pas avec cette adresse que le DHCP va l'identifier, il fournit aussi son adresse MAC.
- Le, ou les serveurs DHCP du réseau qui vont recevoir cette trame vont se sentir concernés et répondre par un **"DHCPOFFER"** qui est une trame contenant une proposition de bail et l'adresse MAC du client, avec également l'adresse IP du serveur. Tous les serveurs DHCP répondent et le client normalement accepte la première réponse venue.

- Le client répond alors par un **DHCPREQUEST** à tous les serveurs (donc toujours en "Broadcast") pour indiquer quelle offre il accepte.
- Le serveur DHCP choisi répond définitivement par un **DHCPACK** qui constitue une confirmation du bail. L'adresse du client est alors marquée comme utilisée et ne sera plus proposée à un autre client pour toute la durée du bail.

Le bail

Dans le bail, il y a non seulement une adresse IP pour le client, avec une durée de validité, mais également d'autres informations de configuration comme:

- L'adresse d'un ou de plusieurs DNS (pour la résolution de noms)
- L'adresse de la passerelle par défaut (pour sortir de son réseau)
- L'adresse du serveur DHCP.

L'installation

Pour installer le serveur DHCP (appelé **dhcpd**) sous Ubuntu, la commande est la suivante:

 # aptitude install dhcp3-server ou apt-get install dhcp3-server

Configuration

Il y a deux fichiers à renseigner afin de configurer le serveur DHCP:

- le fichier /etc/default/dhcp3-server

Il contient l'interface sur laquelle doit écouter le serveur. On modifie la ligne INTERFACES=" ", qui est d'ailleurs la seule ligne du fichier (à part les lignes de commentaire), en y ajoutant l'interface que l'on veut. Par exemple, si le serveur DHCP doit tourner sur l'interface eth0 la ligne doit correspondre à: INTERFACES="eth0"

- mais le fichier le plus important à modifier est /*etc/dhcp3/dhcpd.conf*

C'est lui qui permet de définir toute la configuration du serveur DHCP. Plus la configuration est avancée et plus ce fichier est complexe.

Voici ce que peut contenir ce fichier dans le cas d'une configuration très simple.

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.10 192.168.1.250;
    option routers 192.168.1.1;
   option broadcast-address 192.168.1.255;
```

```
    option domain-name "big-burkina.biz";
    option domain-name-servers 192.168.1.3;
}

host serverX {
    hardware ethernet 00:C0:9F:AF:83:85;
    fixed-address 192.168.1.2;
}
```

Le serveur DHCP lui-même doit avoir une adresse fixée car il ne s'attribue pas une adresse. Nous déclarons un réseau local en 192.168.1.0/255.255.255.0 dont les adresses seront automatiquement attribuées entre 192.168.1.10 et 192.168.1.250.
De plus, le nom de domaine est précisé par: option domain-name "big-burkina.biz"; et le serveur DNS est déclaré grâce à l'option domain-name-servers 192.168.1.3. L'adresse IP 192.168.1.2 sera associée à l'ordinateur dont l'adresse MAC est 00:C0:9F:AF:83:85 et qui est peut-être une autre machine serveur du réseau.

Dans la plupart des cas, la configuration de ce fichier n'est pas si simple. En effet, il peut être intéressant d'utiliser des pools et des classes (d'adresses) pour créer différents "sous-réseaux" afin de permettre une meilleure localisation des ressources sur le réseau et aussi une meilleure organisation. Il est ainsi possible de distinguer un serveur, d'un poste utilisateur et mieux encore, d'une machine étrangère au réseau; un firewall basé sur cette architecture pourrait interdire ses ressources à des machines étrangères, ou leur interdire d'accéder à Internet.

Vu la simplicité de notre réseau informatique, un seul serveur DHCP sera largement suffisant pour l'attribution d'adresses IP aux postes du réseau ainsi qu'aux postes étrangers susceptibles de se connecter à notre réseau.

```
[....]
# Création d'une classe pour réseau local de BIG
class "Réseau_big" {
    match if substring (option dhcp-client-identifier,0,5) = "BIG";
}
```

```
# Créer le réseau pour les machines étrangères
subnet 192.168.1.0 netmask 255.255.255.0 {
    # Associer la plage [40-60] pour les machines inconnues sur le réseau
    pool {
        deny members of "Réseau_big";
        range 192.168.1.40 192.168.1.60;
    }
    # Associer la plage [10-30] aux machines du réseau BIG
    pool {
        allow members of "Réseau_big";
    }


        # Configuration d'une machine serveur via son adr MAC
        host serveurX {
            hardware ethernet 00:C0:9F:AF:83:85;
            fixed-address 192.168.1.2;
        }
[....]
```

L'option DHCP-client-identifier permet de définir les classes. Pour des clients sous Linux, il faut ajouter cette option dans le ficher **/etc/dhcp3/dhclient.conf** des différents postes clients en fonction de leur groupe. Par exemple, la ligne suivante doit figurer dans le fichier ci-dessus pour les ordinateurs du réseau local BIG:

```
send DHCP-client-identifier "BIG_PCx"
```

Avec **x** le numéro du poste client.

Pour les clients sous Windows, il faut exécuter la commande suivante sous DOS:

 # ipconfig /setclassid "Connexion au sous-réseau" BIG_PC1

Ensuite, pour que le DHCP marche, il est très important de lancer le démon DHCP en exécutant la commande suivante sur le serveur : **# /etc/init.d/dhcp3-server start**

Il faut également le relancer chaque fois qu'on modifie les fichiers de configuration et qu'on veut prendre en compte les modifications.

b) Serveur SAMBA

Le service Samba est une des composantes de notre serveur de fichiers. Un serveur Samba permet dans un réseau, de partager des ressources entre des ordinateurs ayant des systèmes d'exploitation différents (Linux, Windows, MAC/OS, etc.). Il assure donc une certaine hétérogénéité des machines du réseau du point de vu des systèmes d'exploitation utilisés.

Samba utilise le protocole SMB (Server Message Block) dont son nom dérive d'ailleurs et qui s'appuie sur NetBios, un autre protocole de transfert de fichiers plus ancien. Samba met en œuvre deux processus serveurs ou "daemons" : **smbd** pour le partage de ressources proprement dit et **nmbd** qui assure la résolution des noms NetBIOS.

Installation

Elle se fait simplement par la commande : **# apt-get install samba**.

Configuration

- **Le fichier de configuration**

Sous Ubuntu la configuration se fait dans **/etc/samba/smb.conf** qui comprend essentiellement deux parties: une partie "générale" contenant la section **[global]** qui définit le comportement général du serveur et la stratégie adoptée pour les services communs et l'autre partie qui définit les ressources partagées et les permissions d'accès. Dans cette partie, on retrouve la section **[homes**] qui permet de partager les répertoires personnels des utilisateurs Linux, de même que des sections définies pour le partage des imprimantes (**[printers]**), et d'autres répertoires sur le serveur.

Il est toujours possible de modifier et d'ajouter des sections, pour définir de nouvelles ressources à partager. Les sections sont configurées par des paramètres auxquels sont affectées des valeurs.

Les principaux paramètres de configuration Pour la section GLOBAL sont (tableau 4.6 et 4.7 à la page suivante) :

Tableau 4.6: paramètres de configuration de la section globale de SAMBA

Paramètre	**valeur par défaut**	**Description**
workgroup =		le nom du groupe de travail ou du domaine (Windows) des postes clients
NetBIOS name =		le nom du serveur Samba
guest account =	nobody	le compte à utiliser pour les accès invités aux partages
share modes = yes|no	yes	accès multi utilisateur ou non
interfaces =		l'adresse IP de la carte réseau du serveur
printcap =	/etc/printcap	emplacement du fichier printcap, récapitulant toutes les imprimantes installées sur le serveur
load printers = yes|no	yes	partager ou non toutes les imprimantes définies dans le fichier printcap
log file =	/var/log/samba/log.%m	fichier log pour les machines qui se connectent
security = user|share	user	mode de sécurité

Pour les autres sections on a:

Tableau 4.7: paramètres de configuration des sections secondaires de SAMBA

paramètre	**valeur par défaut**	**Description**
path =		chemin du répertoire à partager
comment =		texte visible dans le voisinage réseau client
guest ok = yes|no	no	partage en accès libre sans authentification
valid users =	tous	liste des users autorisés à se connecter à la ressource
printable = true|false	false	partage d'un service d'impression et non de répertoire.
writeable = yes|no	no	permet ou non l'écriture sur le répertoire, contraire de read only
write list =	tous les utilisateurs	liste des users autorisés à écrire
browseable =	yes	visibilité du partage par tous, *même les users non autorisés*
create mode | mask =	0744	droits maximum accordés à un fichier créé dans la ressource; ces droits seront en intersection (and) avec les droits Linux (umask)
directory mode | mask=	0755	droits maximum accordés à un répertoire créé dans la ressource; ces droits seront en intersection (and) avec les droits Linux (umask)
force directory mode =	000	droits imposés lors de la création du répertoire. composé par un opérateur OR avec les droits usuels
force group =		Impose un groupe propriétaire d'un fichier lors de sa création dans le partage
hide dot files =	yes	cache les fichiers cachés au sens Linux, commençant par un point
hosts allow = hosts deny =	toutes les stations aucune	ressource réservée|interdite à la liste des stations (adresses IP)
max connections =	0	nombre de connexions à la ressource illimité, sinon maximum

Ceci est notre fichier ***/etc/samba/smb.conf*** largement commenté.

```
[global]
   # Nom du groupe samba
workgroup = group_samba

   # accès multi utilisateur
share modes = yes ;

   # restreindre par sécurité les sous-réseaux autorisés à se connecter au serveur
   # ici on se limite aux adresses réseau privé 192.168.1.0
   et à l'interface "loopback"
hosts allow = 192.168.1.    127.

   # indique l'adresse IP de l'adaptateur du serveur et le masque de sous réseau
interfaces = 192.168.1.10/255.255.255.0

   # indique l'emplacement du fichier printcap, récapitulant
    toutes les imprimantes installées sur le serveur Linux
printcap = /etc/printcap
   # partage toutes les imprimantes définies dans le fichier printcap
load printers = yes

   # utiliser un fichier de trace pour chaque machine qui se connecte
log file = /var/log/samba/log.%m

   # choisir le mode de sécurité : user ou share
security = user



# Ce paragraphe permet de rendre les répertoires personnels des utilisateurs sur le serveur, accessibles depuis les postes clients

[homes]
```

comment =Répertoire personnel

#Pour que seul le propriétaire ait accès

browsable = no

#L'accès sera total

writable = yes

create mode = 0700

 # Ici nous partageons un répertoire pour tous les utilisateurs

[public]

 # Ce répertoire aura pour nom de partage " public "([public]),

 # la valeur du champ comment apparaîtra dans le voisinage réseau

comment =Répertoire public

path = /home/tmp

 # il pourra être accessible par tous les utilisateurs

public = yes

 # il est accessible en écriture

writeable = yes

 # les fichiers créés sont en lecture seule, sauf pour le propriétaire

create mode = 0755

#configurer un partage de répertoire pour un groupe

 # Ce répertoire aura pour nom de partage stagiaire

[stagiaire]

comment =Partage pour le groupe stagiaire exclusivement

 # Le répertoire à partager est /home/partage

path = /home/partage

 # il ne pourra pas être accessible par tous les utilisateurs

public = no

```
# liste des utilisateurs autorisés
valid users = Main1 Maint2

# les utilisateurs autorisés pourront y écrire
writeable = yes

# permissions par défaut des fichiers créés
create mode = 0640


# Partager des applications sur le serveur

[logiciels]
comment = Applications partagées sur le serveur
path = /appli
public = yes
# le rép. ne doit pas être en lecture seule pour tous
writeable =no
# le groupe admin peut seul installer les applications
write list = @admin

# Partager le lecteur de cd-rom

[cdrom]

# chemin d'accès au pseudo-répertoire de montage du CD
path = /media/cdrom
# accessible à tous les utilisateurs
public = yes
# l'écriture sera interdite
writeable = no
```

- **La création des comptes Samba**

Les comptes systèmes Linux et les comptes Samba sont différents, même si on peut créer un compte Samba associé à chacun des comptes systèmes. Pour créer un compte Samba, on utilise la commande **smbpasswd**. Ces comptes seront utilisés avec le mot de passe associé pour accéder aux ressources depuis les postes clients.

- **Configuration des postes clients et accès aux ressources sur le serveur.**

Sur les postes Windows, il faut s'assurer que les protocoles TCP/IP et NetBIOS sont installés, que les clients sont dans le même réseau que le serveur Linux et que le groupe de travail ou le domaine est celui défini dans le fichier /etc/samba/smb.conf du serveur.

Après un redémarrage aller dans:

- Favoris réseaux,
- Voir les ordinateurs du groupe de travail,
- Réseaux Microsoft Windows,
- Sélectionnez le nom de votre groupe de travail Samba, puis cliquez sur votre serveur.
- Vous devrez alors vous identifier puis vous authentifier avec un des comptes définis sur votre serveur Samba pour accéder aux ressources partagées.

Création des utilisateurs samba et accès aux comptes de ces utilisateurs

- 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.

Et de redémarrer Samba :

 # /etc/init.d/samba restart

c) Serveur NFS

NFS signifie Network File System. C'est, comme son nom l'indique, un système de fichiers en réseau qui permet de partager ses données, principalement entre systèmes UNIX. À la différence de SAMBA, NFS gère les permissions sur les fichiers et on peut donc l'utiliser de manière totalement transparente dans son arborescence Linux.

Installation

 # aptitude install nfs-kernel-server

configuration

- **Le serveur**

Les 3 fichiers de configuration principaux sont */etc/exports*, */etc/hosts.deny* et */etc/hosts.allow.*

/etc/exports

Le fichier */etc/exports* est très simple :

Ses lignes présentent les répertoires partagés selon la syntaxe suivante:

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

- répertoire :
  le répertoire du serveur à partager.
- Machine :
  Une liste de machines séparées par des virgules et autorisées à monter ce répertoire (utilisez des adresses IP plutôt que des noms à cause des problèmes de "*dns spoofing*").
- 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'utilisateur root sur le serveur se font sous l'identité root, au contraire de nobody (par défaut).

Par exemple :

```
/home 192.168.1.10(rw) 192.168.1.25(ro)
```

signifie que l'on autorisera la machine *192.168.1.10* à accéder à notre répertoire /home en lecture et écriture (rw) ainsi que la machine *192.168.1.25* mais uniquement en lecture (ro).

Pour un bon fonctionnement : il faut avoir les mêmes numéros de groupes et d'utilisateurs sur les deux machines. Des systèmes permettent de gérer cela, NIS (assez ancien) ou LDAP (plus récent). Avec peu d'utilisateurs, il faut tout simplement éditer /etc/group et /etc/passwd pour synchroniser ces numéros.

Il n'est pas recommandé d'exporter un système DOS ou VFAT à cause de leurs absences de gestion multiutilisateurs ; ils ne sont pas faits pour être partagés avec NFS.

/etc/hosts.deny

On va interdire toutes les machines qui ne sont pas autorisées explicitement dans le */etc/hosts.allow.*

Pour interdire l'accès à tous les services à partir de toutes les machines la mention "ALL: ALL" suffit. On peut cependant être plus précis en écrivant :

portmap:ALL

lockd:ALL

mountd:ALL

rquotad:ALL

statd:ALL

/etc/hosts.allow

Dans le même esprit que pour le /etc/hosts.deny, ce fichier a l'architecture

[service]: [IP de la machine client]

Donc pour autoriser 192.168.1.34 à se connecter à un partage NFS, on écrira :

portmap:192.168.1.34

lockd:192.168.1.34

mountd:192.168.1.34

rquotad:192.168.1.34

statd:192.168.1.34

- **Le client**

Pour utiliser NFS v4, il faut au minimum la version 2.10m du programme mount. Pour voir sa version, taper : **# mount −V**

Pour monter le partage, on tape:

 # mount mon.serveur.nfs:/home /mnt/home

En principe tout devrait bien se dérouler.

Pour monter ce partage définitivement à chaque démarrage de la machine, éditons notre /etc/fstab:

```
# device mountpoint fs−type options dump fsckorder
master.foo.com:/home /mnt nfs rw 0 0
```

4.2.3.3 Les services à l'entrée du réseau

a) Le serveur DNS

BIND pour *Berkeley Internet Name Domain*, précédemment appelé *Berkeley Internet Name Daemon* est le serveur DNS le plus utilisé sur Internet, spécialement de type Unix et devenu de fait un standard. Le protocole DNS est défini par l'IETF dans une dizaine de RFC (Request For Comment), mais les grands principes sont présentés dans les RFC 1034 et 1035.

Comme souligné précédemment, le système de nom de domaine (DNS) est utilisé pour faire correspondre des noms de domaine et des adresses IP afin de pouvoir localiser des hôtes sur des réseaux distants par le biais de noms, plus facilement mémorisables que les adresses IP. Ce processus s'articule autour d'une relation client / serveur ou le client, nommé «*resolver*» effectue une requête auprès d'un serveur de nom.

Les différents types de serveur de nom.

On distingue 4 types de serveurs de noms regroupés dans le tableau 4.8 ci-dessous.

Tableau 4.8: les déférents types de serveurs DNS

Type	Description
master	Conserve les enregistrements originaux et fait autorité pour un espace de noms.
slave	Reçoit ses informations des serveurs maîtres
caching-only	Ne fait pas autorité, ce type de serveur sert juste de cache afin d'accélérer le temps de réponse.
forwarding	Fait suivre des requêtes à une liste spécifique de serveurs de noms

installation

L'installation se fait par la commande:

 # aptitude install bind9

Le DNS dynamique

Concept:

Si vous avez un serveur web, ou que vous avez régulièrement besoin de connaître l'IP de votre machine pour une autre raison, et que vous n'avez pas l'IP fixe, c'est-à-dire qu'elle change à chaque fois que vous redémarrez votre modem, il peut être pratique d'en faire la relation vers un nom de domaine. On appelle ça un DNS

Comment ça marche :

Le système est simple : Votre IP, à chaque fois qu'elle change, et grâce à un script sur votre machine (nous allons utiliser ddclient), va informer un fournisseur de service (exemple avec dyndns.com), qui va établir la relation entre un (sous-)nom de domaine (que vous aurez choisi parmi les possibilités disponibles). De cette manière, vous n'aurez plus à entrer, ou à donner l'IP de votre machine, mais simplement son (sous-)nom de domaine, beaucoup plus facile à retenir.

1ère étape : création d'un compte sur DynDns

Allez donc sur le Site de DynDns, et créez-vous un compte (Sign Up Now), ceci est totalement gratuit.
Remplissez ce qu'il vous demande en première page.
On va prendre ici comme exemple :

Login: NuXo
Password: toto

Vous confirmez vos renseignements et un mail va vous être envoyé sur votre boîte mail pour confirmer votre inscription puis on va donc l'activer.
Une fois le compte confirmé vous allez pouvoir vous connecter, afin de pouvoir obtenir un petit DNS.
Une fois connecté, dans le menu de gauche, choisissez "**MyServices**" puis "**My Host**", "**Add Host Services**" et pour finir "**Add Host Services**" dans la partie centrale.
Là, vous allez pouvoir choisir votre Dns.
Dans un premier temps, choisissez le nom du début du Dns, dans l'exemple nous

prendrons **NuXo**.

Puis choisissez, la fin parmi ce que vous propose DynDns, ici nous choisissons dyndns.org.

On se retrouve donc avec comme Dns "**NuXo.dyndns.org**".

En dessous vous avez l'IP que DynDns a récupéré du Navigateur, donc logiquement la vôtre !

Tout est bon, on peut le créer, et cela vous amène à un récapitulatif;

Vous pouvez y accéder par la suite par "**Dynamic DNS**" dans "**My Host**".

2ème étape : Installation du client DynDns

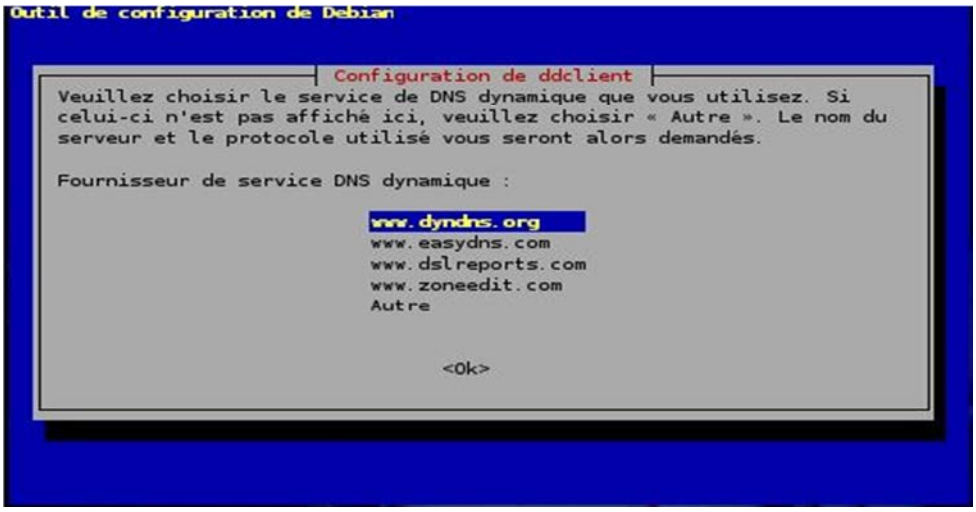
On a bien un Dns **Fixe** qui pointe sur nôtre **IP Dynamique**, mais la ce n'est valable que le temps de vie de notre IP donc à peine 24h, ce n'est pas vraiment ce que nous voulions.

Voilà comment votre petite Ubuntu intervient pour mettre à jour l'IP sur le site de DynDns.

```
BIG@MacServer:~$ su
Password:
MacServer:~# apt-get install ddclient
```

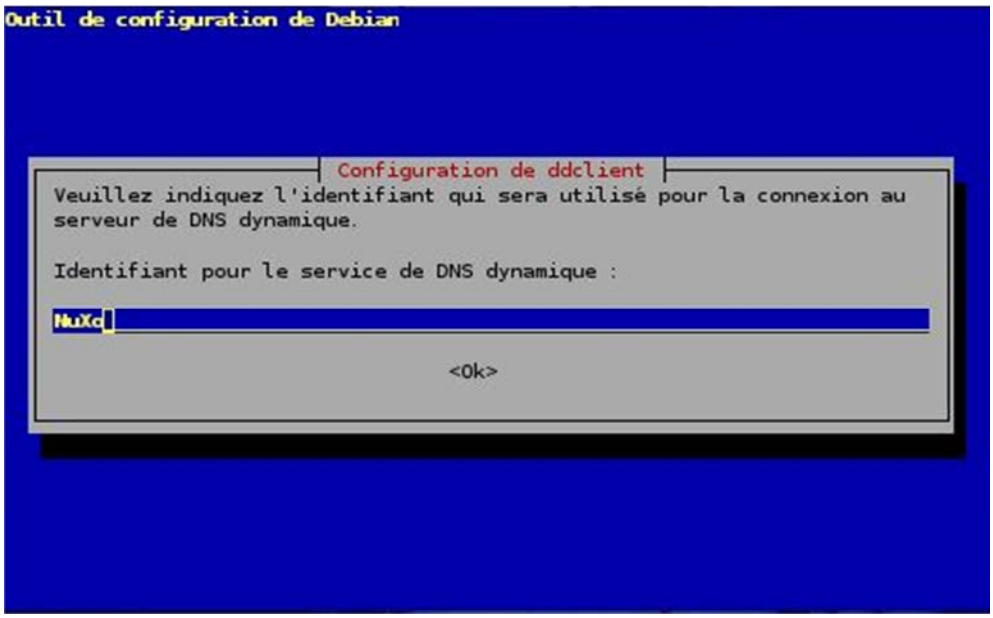
Allez, c'est parti pour une pré configuration de ddclient :

Alors, ici on choisit l'URL où l'on a créé notre compte, et donc, bien sûr**,** www.dyndns.org



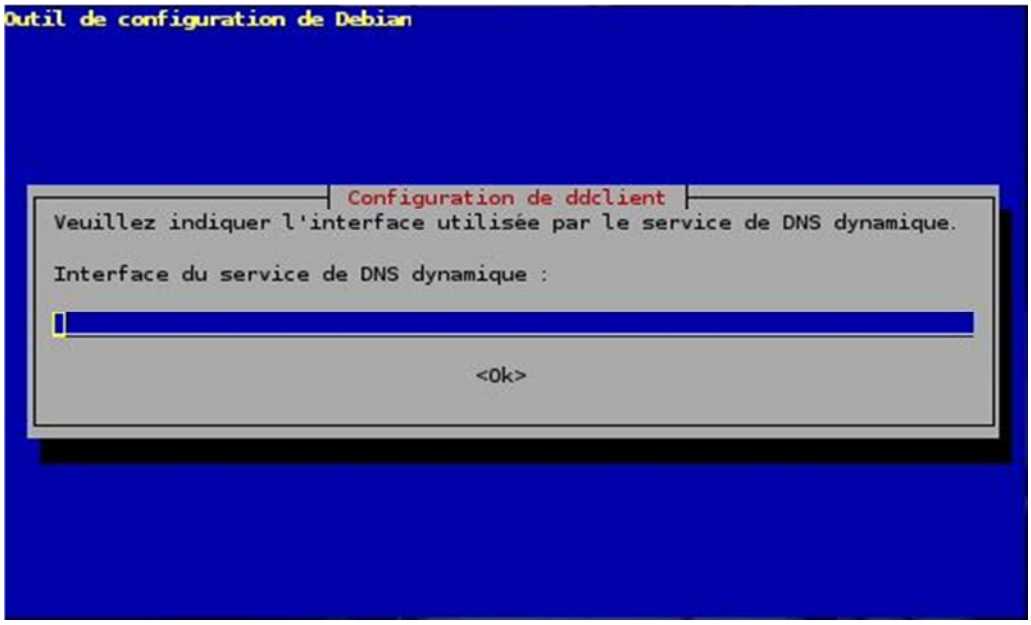
Là, c'est le moment de mettre le nom du Dns que l'on a créé c'est-à-dire NuXo.dyndns.org

Bien sûr, c'est au tour du Login : NuXo



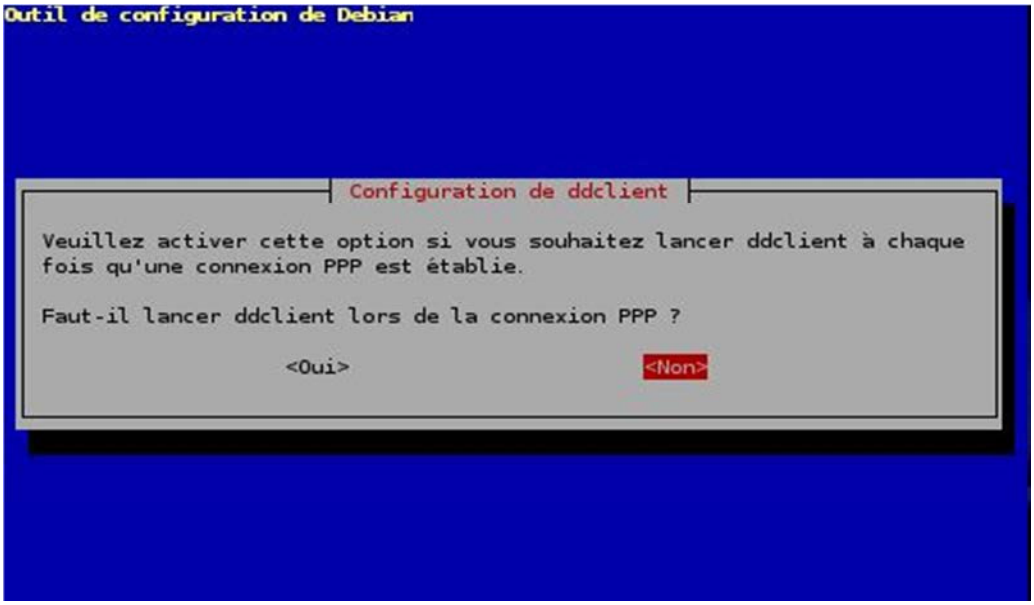
Et bien entendu du Password : toto

Ici, on vous demande quelle interface choisir pour récupérer l'IP, laissez le vide pour le moment.



Alors, si vous vous connectez via un modem, ici il faut répondre Oui.

Par contre si vous êtes derrière un routeur, alors répondez Non.



Si vous voulez qu'il soit lancé à chaque démarrage, appuyez sur Oui, vivement conseillé si vous l'installez sur un serveur

Pour finir, choisissez le temps entre le renouvellement de l'IP, à vous d'adapter ce temps suivant vos besoins.

On a laissé vide l'interface donc DynDns ne va pas encore récupérer votre IP, mais on va voir cela dans la 3ème étape.

3ème étape : Configuration du Client DynDns

Nous voici donc avec un compte créé sur DynDns, le client qui permet la mise à jour de l'IP sur notre compte; il reste à lui envoyer la bonne adresse IP.

Pour cela on va maintenant passé au petit fichier de configuration de **ddclient**:

MacServer:~# nano /etc/ddclient.conf

On se retrouve avec notre config de l'étape 2 :

```
# Configuration file for ddclient generated by debconf
#
# /etc/ddclient.conf

pid=/var/run/ddclient.pid
protocol=dyndns2
use=if, if=
server=members.dyndns.org
login=NuXo
```

```
password=toto
NuXo.dyndns.org
```

La partie qui nous intéresse est le paramètre "use", c'est ce qui détermine sur quoi DynDns doit récupérer l'IP.

Ici, il y a plein de possibilités comme :

Connexion par Modem, Routeur; à travers un Firewall etc ...

A vous donc d'adapter ceci suivant votre configuration.

Pour ceux qui ont un Modem :

```
use=fi # par defaut fi point sur ppp0
```

Pour ceux qui passent par une carte réseau possédant l'IP du FAI sur celle-ci:

use=fi, fi= ethX # X étant le numéro de la carte, en général eth0)

Pour ceux qui possèdent un Routeur, regardez la liste proposée dans la section help de ddclient :

```
MacServer:~# ddclient --help
```

Pour ceux qui ont la flemme de configuration en fonction de leur matériel, et qui ne passent pas à travers un Proxy :

```
use=web # utilise le même principe que tout à l'heure pour l'IP lors de la création de compte.
```

Une dernière chose, en ce qui concerne l'intervalle de temps entre les mises à jour, il existe deux possibilités :

- Soit de le mettre dans le fichier ddclient.conf
- Soit de le passer en paramètre dans la commande ddclient (le cas par défaut).

Nous vous conseillons de le mettre dans le fichier .conf; comme ça, rien à mettre en tête de la commande et cela évite les oublis.

Au final, vous devriez avoir quelque chose ressemblant à cela :

```
# Configuration file for ddclient generated by debconf
#
# /etc/ddclient.conf

deamon=10s
pid=/var/run/ddclient.pid
protocol=dyndns2
use=web
server=members.dyndns.org
login=NuXo
password=toto
NuXo.dyndns.org
```

Il ne reste plus qu'à relancer ddclient pour qu'il prenne en compte vos dernières configurations :

```
/etc/init.d/ddclient restart
```

Configuration du modem

Pour finir, il faut se rendre dans la page de configuration de votre modem qui donne accès à internet (dans notre cas, un SpeedTouch 350) afin de lui demander d'autoriser toute transaction HTTP, SSH(pour une connexion distante), FTP(pour pouvoir mettre à jour votre site web),...entre la machine serveur et votre nom de domaine c'est-à-dire pour notre exemple Nuxo.dyndns.org.

b) Le firewall (pare-feu)

Le firewall a pour but d'accroître la sécurité du réseau local, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet de façon beaucoup plus sûre. De plus, il peut permettre de restreindre l'accès interne vers l'extérieur. Le firewall propose donc un véritable contrôle sur le trafic réseau. Netfilter est le module qui fournit à Linux les fonctionnalités de pare-feu, de traduction d'adresses et d'historisation du trafic réseau.

Architecture et fonctionnement de Netfilter

Netfilter se présente comme une série de cinq (5) « hooks » (points de d'accrochage), sur lesquels des modules de traitement des paquets vont se greffer. Ces points:

- NF_IP_PRE_ROUTING
- NF_IP_LOCAL_IN
- NF_IP_FORWARD
- NF_IP_POSTROUTING
- NF_IP_LOCAL_OUT

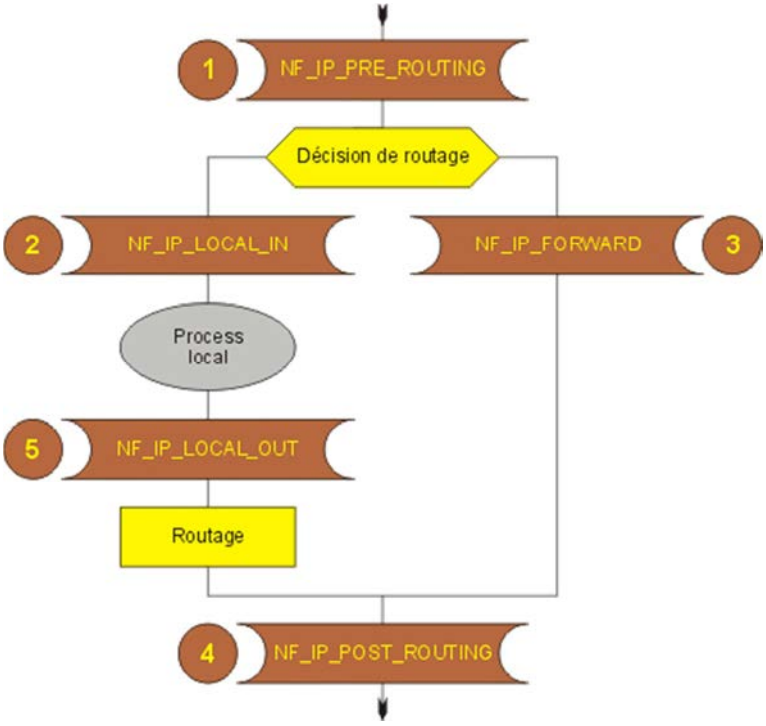


Figure 4.4: Schéma de Netfilter

La branche gauche représente le trajet des paquets qui entrent et qui sortent vers et depuis un processus local.

La branche de droite représente le trajet des paquets qui traversent notre passerelle dans sa fonction de routeur.

A travers ces cinq points d'insertion, Netfilter va être capable :

- D'effectuer des filtrages de paquets, principalement pour assurer des fonctions de Firewall.
- D'effectuer des opérations de NAT (Network Address Translation). Ces fonctions sont particulièrement utiles lorsque l'on veut faire communiquer tout ou partie d'un réseau privé, monté avec des adresses IP privées (192.168.x.x par exemple) avec l'Internet.
- D'effectuer des opérations de marquage des paquets, pour leur appliquer un traitement spécial.

Il y a dans Netfilter trois **tables** qui correspondent aux trois principales fonctions. Chaque table contient des **chaînes**. Les **chaînes** sont des ensembles de règles que nous allons écrire dans chaque table. Ces **chaînes** vont permettre d'identifier des paquets qui correspondent à certains critères.

Les tables et leurs chaines

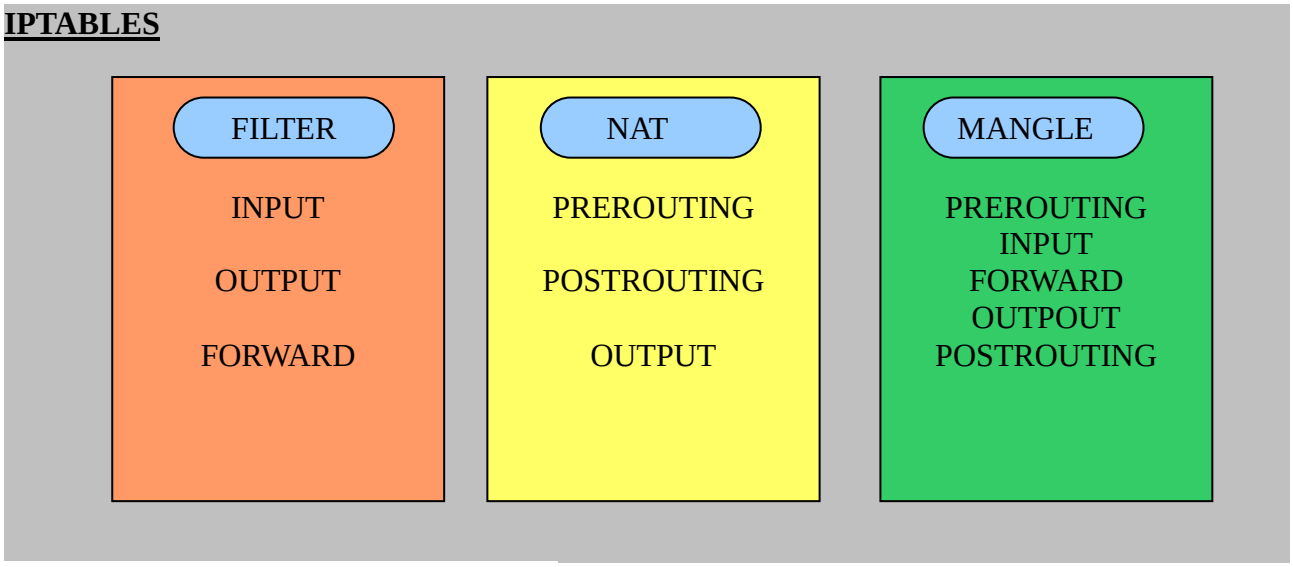


Figure 4.5: schéma des tables de iptables

- PREROUTING: Le paquet est pris en charge par l'interface réseau. Il s'apprête à être routé.
- INPUT: Le paquet est destiné à l'hôte sur lequel nous définissons les règles. Il *nous* est destiné.
- FORWARD: Le paquet ne nous est pas destiné, et nous sommes une passerelle.
- OUTPUT: Le paquet est émis par nous.
- POSTROUTING: Le paquet s'apprête à sortir par l'interface réseau.

Les **cibles** enfin sont des sortes d'aiguillage qui dirigeront les paquets satisfaisant aux critères. Les cibles préconstruites sont :

- ACCEPT: Les paquets qui satisfont aux critères sont acceptés, ils continuent leur chemin dans la pile,
- DROP: Les paquets qui satisfont aux critères sont rejetés, on les oublie, on n'envoie même pas de message ICMP. Un trou noir, quoi.
- LOG: C'est une cible particulière qui permet de tracer au moyen de syslog les paquets qui satisfont aux critères.

Netfilter dispose d'une commande à tout faire : **iptables**. Cette commande va permettre, entre autres, d'écrire des chaînes de règles dans des tables. La syntaxe est la suivante:

#iptables [table] chaîne_spécifiée condition action.

Déploiement de la politique de sécurité

La politique de sécurité qui sera mise en œuvre au niveau de notre pare feu est la suivante :

- Trafic de tout poste du réseau vers les postes du service de Comptabilité-Gestion refusé
- Trafic du poste du Directeur Général vers les postes de la Comptabilité-Gestion accepté
- Trafic des logiciels peer-to-peer du réseau local vers le réseau externe refusé
- Trafic des logiciels non déclarés du LAN vers le réseau externe refusé

4.2.4 Estimations

Dans cette partie, nous allons estimer la durée et le coût que la réalisation de notre projet nécessite.

4.2.4.1 Durée

Notre stage n'a duré que trois mois. Nous avons cependant su mettre ce temps à profit pour mener une étude sur la plupart des services à déployer. Nous avons également pu tester l'ensemble de ces services, dont certains fonctionnent d'ailleurs bien. Cependant, pour réaliser complètement un tel projet, en tenant compte de la sécurité qui est d'une importance capitale, il nous faudrait beaucoup plus de temps. Si nous considérons les résultats que nous avons pu produire durant le temps de notre stage, nous estimons que pour une étude plus complète prenant en compte toutes les données de BIG, il nous faudrait deux (01) mois supplémentaires. La mise en place de ces services nécessiterait également deux (01) mois. Soit au total quatre (02) mois.

4.2.4.2 Coûts

Tableau 4.9: Tableau estimatif des coûts.

Désignation	Caractéristiques	Quantité	Prix unitaire	Montant
Ordinateur firewall	Pentium II 350Mhz	01	85.000	85.000
Ordinateur serveur	HP Proliant ML750	01	2.000.000	2.000.000
Système d'exploitation	Ubuntu serveur version 8.04	-	Gratuit	Gratuit
Nom de domaine	big-burkina.homelinux.net	-	gratuit	gratuit
Serveur HTTP	Apache2	01	Gratuit	Gratuit
Serveur FTP	VsFTPd	01	Gratuit	Gratuit
SGBD	MySQL	01	Gratuit	Gratuit
Antivirus	Clamav, amavisd-new, spamassassin	-	Gratuit	Gratuit
Logiciel firewall	Netfilter (iptables)	-	Gratuit	Gratuit
Mise en œuvre				2.000.000
Coût total	-	-	-	4.085.000

CONCLUSION GENERALE

En définitive, BIG a besoin d'un système informatique qui assurera une gestion centralisée de toutes ses ressources afin de voir son rendement s'accroître sur le plan du travail ainsi que sur le plan financier.

Partie intégrante de la formation des étudiants de l'ESI, ce projet de fin de cycle a permis pour notre part, de mener pendant plus de trois mois, une étude du système informatique de BIG. Cela nous a permis de déployer de nouveaux services réseaux et de mettre en place une nouvelle stratégie de sécurité. Ce stage nous aura permis d'aborder d'un point de vue plus pratique, les enseignements reçus durant tout notre cycle, notamment dans les domaines des réseaux informatiques et des télécommunications. Nous pensons que la réalisation de notre étude permettrait à BIG d'être dotée d'un système informatique qui augmentera son chiffre d'affaire.

Cependant les utilisateurs du nouveau système doivent veiller au bon fonctionnement du système. Une mise à jour régulière du système est nécessaire afin d'évoluer avec l'avancée rapide de la technologie.

BIBLIOGRAPHIE

Craig Hunt, "*Linux Network Servers*", Sybex, 1999, 483 pages

Azzedine RAMRAMI "*La sécurité des réseaux*", 2002, 216 pages

- http://www.dyndns.org
- http://www.ubuntu-fr.org
- http://techniciens.info/index.php?id=2
- http://www.apache.org
- http://www.commentcamarche.net
- http://www.google.com
- http://www.wikipedia.org
- http://www.developpez.com/
- http://www.framasoft.net
- http://www.generation-linux.net
- http://www.labo-linux.org