République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU

FACULTE DE GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT ELECTRONIQUE

Mémoire de fin d'études

En vue de l'obtention du Diplôme de Master II Académique en Electronique

Option : Télécommunications et Réseaux

Théme :

Mise en place d'une plate-forme pour un système de messagerie interne

Proposé et dirigé par :

M^r^ LAHDIR Mourad

M^r^ BRAHIMI Mouloud

Présenté par :

M^elle^ HANICHE Djouher

M^elle^ LEHARANI Dalila

Année universitaire
2013/2014

Remerciements

Nous remercions en premier lieu Dieu, tout puissant de nous avoir accordé la puissance et la volonté pour terminer ce travail.

Nous tenons à exprimer notre profonde gratitude à notre promoteur Mr. LAHDIR , pour ses orientations et ses conseils précieux.

Un grand merci à Mr. BRAHIMI, ingénieur en Système, Réseau et Sécurité chez Alcôve (société de service en logiciels libres) en France. Qui nous a proposé ce thème, et pour son suivi et son encouragement tout au long de l'élaboration de notre mémoire.

Nous remercions chaleureusement les membres du jury, pour l'honneur qu'ils nous font en acceptant d'examiner et de juger notre travail.

Nous, nous remercions toutes les personnes qui ont contribué de prés ou de loin à la réalisation de ce mémoire.

Dédicaces

Je dédie ce travail à :

Mes très chers parents : Mouloud et Fatma, pour leurs sacrifices et leurs dévouements pour mon bonheur, et leur soutient pendant toute la durée de mes études. « Que Dieu les gardes et les protèges ».

Mon cher frère : Yacine et sa femme Hayat.

Mes chères sœurs : Naima, Nahila, Hassiba et leurs maris : Karim, Djilali et Karim.

Mes chères et adorables nièces et neveux : Fatah et Salim.

Ma chère binôme Djouhar et sa famille surtout son fiancé Mouloud, à qui je souhaite beaucoup de bonheur et de réussite.

Mes chères amies : Djidji, Sousou, Sam, Souhila et Sadjia.

Toute la promotion : 2013/2014 ELN.

Dalila

Dédicaces

Je rends grâce à dieu de m'avoir donné le courage et la volonté ainsi que la conscience d'avoir pu terminer mes études.

Un grand merci à :

Mes très cher parents, pour leurs sacrifices et leurs dévouements pour mon bonheur, et leur soutient pendant touts la durée de mes études.

Que Dieu les gardes et les protèges

Mon cher mari mouloud, pour son aide et son encouragement en derniers années du mes étude, et son support tout en long de préparation de ce mémoire.

Dieu me pouvoir à rendre tout ton bienfait pour moi

Mes chères sœurs : lynda, kahina et leila.

Mes chers frères : azeddine, sofiane et hocine.

Qui remplissent ma vie de bonheur

Mon beau père et sa femme, mes belles sœurs et leurs maris et mes beaux frères et leurs femmes.

Oui ont su croire en moi

Mes chers Amies : samira, malika, noiarra et amira .

Oui ont toujours été la pour moi

Ma chère binôme Dalila et sa famille, à qui je souhaite beaucoup de bonheur et de réussite.

Toute la promotion 2013/2014 ELN.

Enfin à tout ceux qui m'on soutenu de prés ou de loin.

Merci à vous tous.

Djouher

Chapitre I : Généralités sur le système de la messagerie électronique

Chapitre II : Serveurs et protocoles de la messagerie électronique

Chapitre III : Application et tests

Liste des figures

Liste des tableaux

Il ne fait désormais plus aucun doute, que les technologies de l'information et de la communication représentent la révolution la plus importante, et la plus innovante qui a marqué la vie de l'humanité en ce siècle passé. En effet, loin d'être un éphémère phénomène de mode, ou une tendance passagère, ces technologies viennent nous apporter de multiples conforts à notre mode de vie, car ils ont révolutionné le travail des individus par leur capacité de traitement d'information, d'une part, et de rapprochement des dimensions espace/temps, d'une autre.

Parmi ces technologies de l'information et de la communication, la messagerie électronique est rapidement développée dans les organisations, aux cours de ces dix dernières années, par sa facilité d'utilisation et son utilité perçue. Désormais, elle représente l'outil de travail le plus utilisé. En le comparant aux autres façons de communiquer (par écrit, par téléphone, …), on s'aperçoit que les nombreux avantages du courrier électronique surpassent de loin ses inconvénients, parce que c'est un moyen rapide, efficace et peu coûteux, et sa grande force réside dans son médium de transport.

Un nombre grandissant d'organisations utilisent le système de messagerie électronique pour : diffuser des informations générales, faire circuler des rapports, envoyer des notes, échanger des documents officiels, expédier de la correspondance à l'extérieur du réseau local, diffuser des directives et soutenir différents aspects de leurs opérations. Un service de courrier électronique adapté offre la possibilité : d'augmenter la rapidité des communications organisationnelles, de réduire le nombre d'appels internes et externes, de rencontres entre direction et personnel, de diffuser massivement des informations, d'éliminer des opérations de surcharge, de faciliter la prise de décision et d'automatiser certaines tâches courantes, il est aussi un excellent moyen de coordination d'une équipe ou d'un service.

C'est dans ce cadre que s'intègre ce mémoire qui consiste la mise en place d'un système de messagerie interne, qui sera destinée au public. Le but principal de ce service est de garantir l'écriture ou la lecture des courriers, et de permettre aux utilisateurs d'accéder facilement à leurs comptes.

Afin de comprendre ce système et son fonctionnement, nous avons jugé utile de structurer notre mémoire en trois chapitres articulés comme suit :

Dans le premier chapitre, nous donnons les différents éléments théoriques impliqués dans la réalisation d'un système de messagerie électronique.

Dans le deuxième chapitre, nous présentons les différents protocoles et serveurs régulant à la messagerie électronique.

Le troisième chapitre est consacré à la présentation du travail réalisé. Nous présentons le cadre général de notre application, avec un test final qui consiste à créer des comptes mails, envoyer et recevoir des courriers.

Enfin, nous terminons notre mémoire par une conclusion sur les travaux décrits dans ce document, ainsi que des perspectives sur les suites à donner à notre travail.

I.1.Préambule

Le système de la messagerie est aujourd'hui le moyen de communication le plus utilisé sur Internet. C'est également l'un des moins chers à mettre en œuvre, parce que simple, rapide et fiable. En raison de sa popularité, le courrier électronique permet de communiquer avec un vaste auditoire. Il tend à prendre une place de plus en plus prépondérante, par rapport aux moyens de communication traditionnels. Bien qu'il puisse incorporer des graphique, des fichiers sonore et visuels, il sert principalement à l'envoi de textes avec ou sans documents annexés.

La messagerie électronique joue un rôle très important au sein des organisations, elle représente l'outil de travail le plus utilisé. Elle est souvent considérée comme une application stratégique voir critique. Cependant, il est impératif de bien assimiler l'étude théorique et l'aspect technique de l'ensemble des modules constituant un système de messagerie.

I.2.Les premières messageries électroniques

Les premières messageries électroniques datent des années 60. Aujourd'hui, l'e-mail est l'application d'Internet la plus répandue.

- 1967-1968 : la première messagerie collective est crée par l'équipe de Douglas Engelbart, pionnier des interfaces, de l'hypertexte et inventeur de la souris. Son projet appelé NLS était un dispositif intégrant l'hypertexte, les interfaces graphiques et la messagerie collective, c'est-à-dire un espace de travail collaboratif. Le projet NLS est étroitement lié à la naissance du réseau ARPANET en 1969.
- Jusqu'en 1972, les programmes de messagerie fonctionnaient sur des machines à temps partagé, utilisées par plusieurs utilisateurs.
- En mars 1972, deux ans à peine après la création d'ARPANET, premier réseau distribué et ancêtre d'Internet, Ray Tomlinson, ingénieur chez BBN, écrit le premier programme de courrier électronique (E-Mail) entre deux machines, à partir de deux programmes qu'il venait de créer pour le courrier « intra-machine » : SNDMSG (SeND MeSsaGe), pour envoyer les messages et READMAIL, pour lire les messages. La création par Tomlinson, d'un protocole expérimental de transfert de fichier appelé CPYNET, a permit aux messages électroniques de « sortir » pour la première fois des machines locales, pour circuler sur le réseau. Le véritable courrier électronique à distance était né. Dans son programme, Ray Tomlinson voulait un caractère du clavier

qui soit très peu utilisé par les informaticiens, pour séparer nettement l'adresse de l'utilisateur de celle de l'hébergeur et il a choisir l'@, symbole aujourd'hui connu du courrier électronique.

La première adresse de courrier électronique fut *tomlinson@bbn-tenexa*. Tenexa réfère à Tenex, le système d'exploitation utilisé.

I.3.La valeur de la messagerie électronique

I.3.1.Pourquoi le courrier électronique ?

Aujourd'hui tout tourne autour du courrier électronique (communication, inscription, authentification,…etc.). C'est un portail collaboratif et un moyen pratique de communication pour quatre grandes raisons :

- Ø Son fort taux d'utilisation, (qui ne possède pas d'adresse électronique).
- Ø Son accès régulier, (tout le monde consulte son courrier électronique au moins une fois par jour).
- Ø Son universalité, (quel que soit le fournisseur de messagerie, il est compatible avec les autres).
- Ø Sa pérennité, (il y'a peu de risque que le courrier électronique disparaisse dans les années à venir).

Le courrier électronique est un bon outil de signalisation, car il est asynchrone, soit ouvert au reste du monde (Internet), ou fermé (à l'intérieur des groupes de travail professionnels).

I.3.2.Besoins des entreprises en termes de technologie de l'informatique et de la communication

L'évolution des technologies, l'internationalisation des marchés, la concurrence des firmes d'un même secteur, et les exigences toujours plus fortes des consommateurs, sont autant de facteurs qui rendent instable et turbulent l'environnement des organisations. Il est dés lors vital pour les organisations de démontrer leurs aptitudes à réagir et à s'adapter à ces perturbations externes. La messagerie électronique est une solution qui s'est peu à peu imposée dans les organisations, au point d'y être aujourd'hui omniprésente et de constituer une technologie utilisée par les administrateurs.

I.3.3.Apports d'un système de messagerie à une entreprise

Dans le cadre de l'entreprise aujourd'hui, la messagerie électronique offre l'opportunité de prendre contact avec d'autres utilisateurs, clients et dirigeants. Dans les années 80, le dirigeant transmettait les décisions par la voie hiérarchique, en s'assurant que les personnes intéressées avaient bien reçu les informations. De nos jours, le manager rédige ses notes depuis son logiciel de messagerie, vérifie l'orthographe (la plus part du temps elle se fait automatiquement), les relie, puis les envoie. La procédure est simple et fiable. Cependant la rédaction de notes de services n'est pas la seule fonctionnalité qui contribue à l'amélioration des communications interne. On peut citer de nombreuses potentialités techniques et organisationnelles, que la messagerie électronique apporte aux entreprises :

- **La gestion du temps**
  - Améliorer les temps de réponse.
  - Raccourcit les délais de prise de décision.
  - Accélère l'exécution des tâches.
- **La gestion de l'information**
  - Facilite le stockage de l'information.
  - Augmente la circulation des documents.
  - Permet le partage d'information et de documents de natures et de sources différentes.
  - Unifie les dispositifs et procédures de diffusion d'informations.
- **L'exécution des tâches**
  - Améliore la productivité.
  - Allège le travail du manager.
  - Permet de mieux organiser son travail.
- **La communication**
  - Augmente l'accès à l'individu.
  - S'affranchit (en partie) des barrières spatiales et temporelles.
  - Améliore la fréquence de communication.
- **Le travail en équipe**
  - Améliore la constitution des équipes.
  - Favorise le travail collaboratif.
  - Permet de structurer le travail en équipe.
  - Permet une meilleure coordination horizontale.

- **Les relations verticales**
  - Réduit les barrières hiérarchiques.
  - Permet une meilleure implication des collaborateurs.
  - Permet une meilleure responsabilisation des collaborateurs.
  - Peut être utilisé comme levier dans les dispositifs de motivation.

I.4.Définitions

I.4.1.La messagerie électronique

La messagerie électronique appelée parfois courriel, courrier électronique, ou encore e-mail provenant de « electronic-mail », est un service de transmission des messages envoyés électroniquement via un réseau informatique, dans la boite aux lettres électronique d'un ou plusieurs destinataires simultanément. Le message envoyé est un ensemble d'informations constitué d'un texte auquel peuvent être jointes, tous types de fichiers (image, son, vidéo, logiciels, fichiers bureautiques,…etc.).

L'émission et la réception des messages par courrier électronique, nécessitent la mise à disposition d'une adresse électronique et d'un programme d'accès, sous la forme d'un logiciel appelé client de messagerie. L'acheminement des courriels est régi par diverses normes concernant aussi bien le routage que le contenu.

I.4.2.Le réseau informatique

Un réseau informatique est un ensemble d'ordinateurs et périphériques connectés les uns aux autres afin d'assurer des échanges, tels que le transfert de fichiers, le partage de ressources (imprimantes et données), la messagerie électronique ou l'exécution de programmes à distance.

Le terme réseau peut désigner plusieurs choses en fonction de son contexte :

- L'ensemble des machines ou l'infrastructure informatique d'une organisation, avec les protocoles qui sont utilisés.
- Description de la façon dont les machines d'un site sont interconnectées.
- Spécification des protocoles utilisés par les machines pour communiquer.

Mise en réseau (Networking) : Mise en œuvre des outils et des taches permettant de relier des ordinateurs, afin qu'ils puissent partager des ressources.

I.4.3.L'organisation réseau utilisé par la messagerie électronique

Le courrier électronique est l'un des services réseau qui utilise le paradigme (client/serveur).

- **L'environnement (client/serveur)**

Dé nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau), contactent un serveur (une machine généralement très puissante en termes de capacités d'entrée/sortie), qui lui fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion,…etc.

C'est ce type d'architecture que l'on trouve sur les réseaux d'entreprises, qui peut parfaitement supporter plusieurs centaines de clients, voir plusieurs milliers.

Dans un environnement purement client/serveur, les ordinateurs du réseau (les clients) ne peuvent voir que le serveur, c'est l'un des principaux atouts de ce modèle.

- **Fonctionnement d'un système client/serveur**

Un système client/serveur fonctionne selon le schéma suivant :

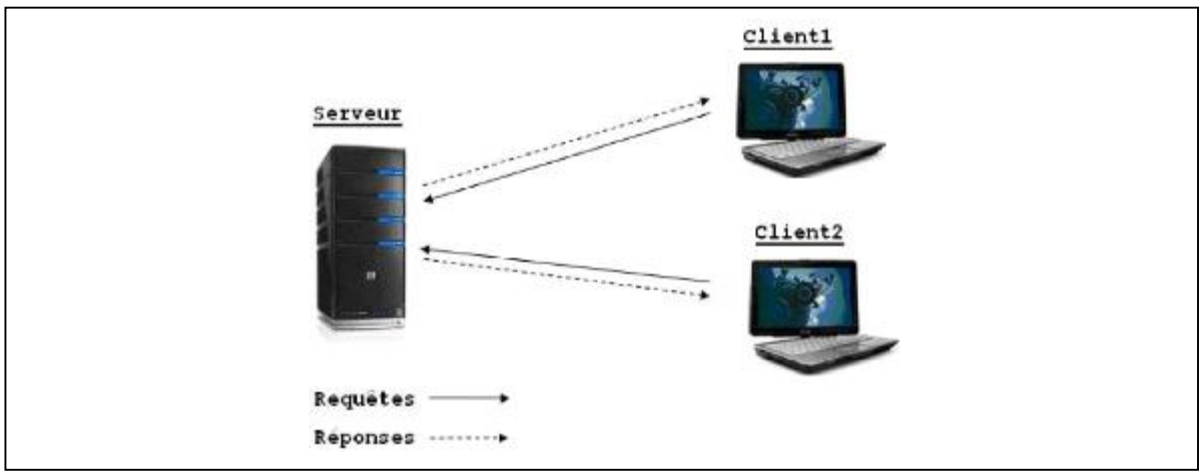


Figure I.1 : Principe de fonctionnement d'un système client/serveur.

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

I.4.4.La boite aux lettres électroniques

Une Boite Aux Lettres ou inbox en anglais, est un espace dédié à un utilisateur, ou sont stockés (dans une pile (stack)) les courriels qui parviennent, en attendant qu'il les lises. La taille des mails stockés est limitée par les serveurs de messagerie électroniques.

Afin d'accéder aux différentes applications proposées, on désigne une adresse à partir de laquelle on peut émettre et recevoir des e-mails. Elle a la forme suivante :

nomd'utilisateur@domaine.extention.

I.4.5.Les éléments d'une adresse électronique

- **Le nom d'utilisateur**

L'utilisateur peut s'inspirer pour cette partie de l'adresse, de son propre nom (« prénom-nom », « prénom.nom », « prénomnom »,…etc.), ou bien adopter un pseudonyme. Le nom d'utilisateur identifie l'utilisateur sur le réseau, le différenciant de tous les autres utilisateurs de ce réseau.

- **L'arobase @**

L'arobase, caractère indispensable de l'adresse électronique, sépare le nom de l'utilisateur du nom de domaine et signifie « chez ».

- **Le nom de domaine**

Le nom de domaine du fournisseur (« provider » en anglais), est en général l'hébergeur ou le nom de site qui fournit le service de messagerie : laposte, gmail, free,…etc.

- **L'extension**

Elle désigne le type de domaine. Il existe des extensions géographique pour tous les pays, par exemple L'extension '.dz' désigne un DNS en Algérie, ou encore '.fr' pour un DNS en France,…etc, ainsi que des extensions qui désignent le domaine d'activité auquel le serveur est rattaché, par exemple, les universités ou une autre institution scolaire ont souvent pour extension '.edu', les entreprises commerciales utilisent l'extension '.com', le '.Org' indique que l'hôte est un organisme non commercial, les organismes gouvernementaux comportent une extension '.gouv', et '.net' est réservé aux organismes comme les fournisseurs de services Internet,…etc.

Notons qu'une adresse électronique peut comporter les caractères suivants : les lettres minuscules de a à z, les chiffres, les caractères « - », « _ » et « . ».

I.5.Structure et format d'un e-mail

I.5.1.Structure d'un e-mail

Un e-mail à une structure similaire à celle d'un courrier classique, il est composé d'une enveloppe (en-tête), comportant les données relatives aux adresses des expéditeurs et des destinataires, ainsi que le sujet du message, la date,…etc. A la suite de l'en-tête séparée par une ligne vide s'ajoute le contenu de l'e-mail (corps du message), comprenant éventuellement des pièces jointes.

L'en-tête contient donc les informations suivantes :

- L'adresse e-mail de l'émetteur du message.
- L'adresse e-mail du (ou des) destinataires.
- Le chemin suivi par le message.
- Le type d'encodage du message.
- Des informations « subsidiaires », comme par exemple le type de logiciel qui a généré le message.

Lors de la lecture d'un e-mail, les champs visibles sont :

- L'expéditeur.
- L'objet.
- Le texte (ou corps) du message.

I.5.2.Le format MIME (Multi-purpose Internet Mail Extention)

Le format MIME a été défini pour permettre la transmission de données non ASCII par courrier électronique. L'extension MIME offre un mécanisme complémentaire au service de courriel utilisant le SMTP.

MIME ajoute des lignes à l'en-tête d'un mail, pour définir le type des données et la méthode de codage utilisé. Un message peut contenir plusieurs types de données différents. Ainsi la structure des messages appelés « RFC 822 » ou « 822 » utilise une ligne blanche, pour séparer l'en-tête et le corps de l'image. MIME apporte à la messagerie les fonctionnalités suivantes :

- Ø Possibilité d'avoir plusieurs objets (pièces jointes) dans un même message.
- Ø Une longueur de message illimité.
- Ø L'utilisation de jeu de caractère alphabet autre que le code ASCII.
- Ø L'utilisation de texte enrichie (mise en forme des messages, police de caractère, couleur,…etc.).
- Ø Des pièces jointe binaire (exécutable, image, fichier audio ou vidéo,…etc.).

v Les directives spécifiques de l'en-tête du MIME

Content type	**Type MIME de base**	- Text/plain, html,rfc822 - Image/gif, jpeg, png… - Audio/basic, wav… - Video/mpeg… - Application/octet-stream,pdf… - Multipart/Mixed, Alternative, parallel,Digest.
Content-transfert-Encoding	**Format de codage**	- 7bits (pour les messages non accentués) - 8bits - Quoted-printable (pour les messages utilisant un alphabet sur plus de 7bits « présence d'accents par exemple » - Based64 (recommandé pour les fichiers binaires en pièce jointe) - Binary (déconseillé)

Tableau I.1 : Directives spécifiques de l'en-tête du MIME.

I.6.Concepts clés de la messagerie électronique

I.6.1.Le serveur de messagerie électronique

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électronique d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise un client de messagerie, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.

La plupart des serveurs de messagerie possèdent ces deux fonctions (envoi/réception), mais elles sont indépendantes et peuvent être dissociées physiquement en utilisant plusieurs serveurs.

I.6.2.Les agents de la messagerie électronique

L'architecture de la messagerie repose sur un ensemble des constituants logiciels distincts, qui travaillent ensemble pour assurer le transfert d'un message d'un utilisateur vers d'autres utilisateurs.

On peut distinguer trois types de constituants : MUA, MTA, MDA.

I.6.2.1.MUA (Mail User Agent ou Agent de Gestion du Courrier « AGC »)

L'Agent de Gestion du Courier, est un logiciel client de messagerie qui fournit l'interface entre l'utilisateur et la messagerie. Il permet à l'utilisateur la gestion des courriels (saisie, suppression, réception,…etc.), il est également capable d'expédiez le message au MTA le plus proche.

On trouve deux MUA distincts : un MUA installé sur le système de l'utilisateur qui est appelé client de messagerie lourd, et un MUA accessible via un navigateur Web appelé client de messagerie léger (Webmail).

- **Client de messagerie lourd**

Est un logiciel installé sur la machine de l'utilisateur, qui sert à lire et à envoyer des courriers électroniques, il permet de stocker tous les messages sur la machine et d'écrire des messages hors connexions, ou de lire ceux qui sont déjà stockés.

Les clients de messageries lourds les plus connus sont : Microsoft Outlook, Lotus Note (IBM), Mail (Apple), Mozilla Thenderbrid, Zimbra Desktop,…etc.

- **Client de messagerie léger**

Est un client de messagerie qui s'exécute sur un serveur Web, il sert d'interface entre un serveur de messagerie et un navigateur Web. Il faut absolument être connecté pour rédiger ou lire les messages.

Les logiciels de Webmail les plus connu sont : MS Outlook, Web Application, Web mail, ajax de zimbra, roundcube,…etc.

I.6.2.2.MTA (Mail Transfer Agent ou Agent de Transfert de Courriers « ATC »)

L'Agent de Transfert de Courriers, est un programme qui permet d'envoyer le message d'un serveur à un autre. Ce logiciel est situé sur chaque serveur de messagerie. Il est composé d'un agent de routage et d'un agent de transmission. Il envoie le message via des protocoles, qui permettent de gérer la transmission du courrier entre les systèmes de messagerie. Le protocole le plus utilisé est le SMTP.

Le transfert des messages entre utilisateurs est assuré par une chaine de MTA, selon la situation des utilisateurs sur le réseau. Cette chaine peut être constituée d'un MTA ou de plusieurs MTA. A titre d'exemple, pour une société équipée d'un seul serveur de messagerie pour des échanges de messages en interne, la chaine est réduite à un seul MTA. Quand la chaine comprend plusieurs MTA, les messages sont « relayés » de MTA en MTA, du MTA d'émission au MTA de réception comme le montre la figure I.2. Le MTA est souvent appelé « relai SMTP ». Il existe plusieurs logiciels serveurs de messageries : Sendmail, MS Exchange, Postfixe,…etc.

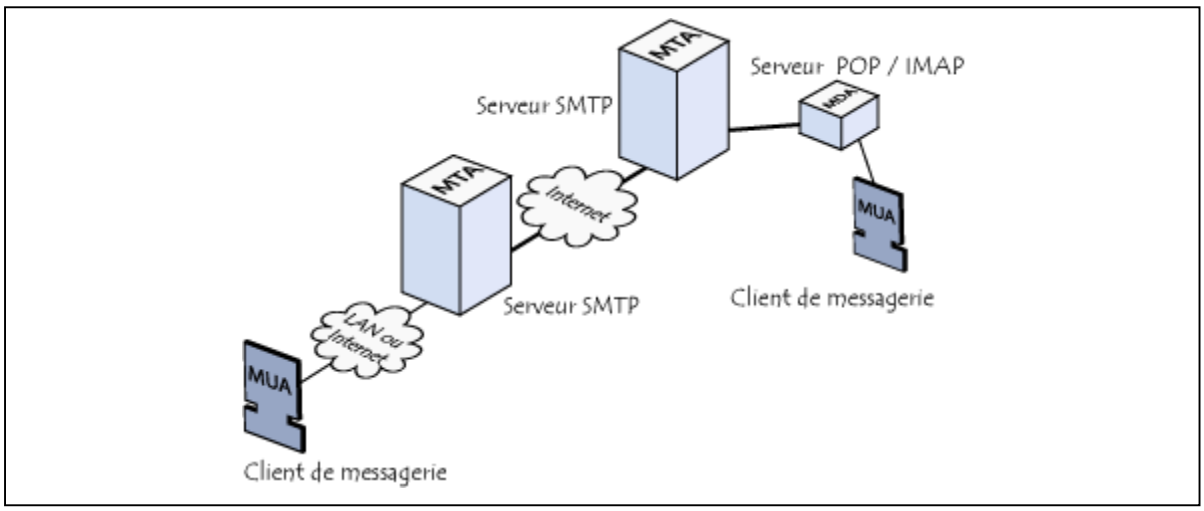


Figure I.2 : Les différents relais de MTA.

I.6.2.3.MDA (Mail Delivery Agent ou Agent de Distribution de Courriers « ADC »)

L'agent de Distribution de Courriers, est un programme utilisé par l'Agent de Transfert de Courriers ATC, pour mettre en charge la gestion des boites aux lettres. Son rôle est de trier les messages en fonction de leurs en-têtes ou de leurs contenus. Il prélève les courriers dans les files d'attentes du MTA, et les dépose dans le répertoire de boites aux lettres de l'utilisateur à l'aide du protocole POP et IMAP, qui viendra les consulter en utilisant le MUA de son poste de travail. Pour cela il est souvent considéré comme le point final d'un système de messagerie. Sous Linux, procmail est très utilisé, et sous Windows on utilise Exchange.

La figure I.3 met l'accent sur la récupération du courrier de la boite aux lettres par le MDA.

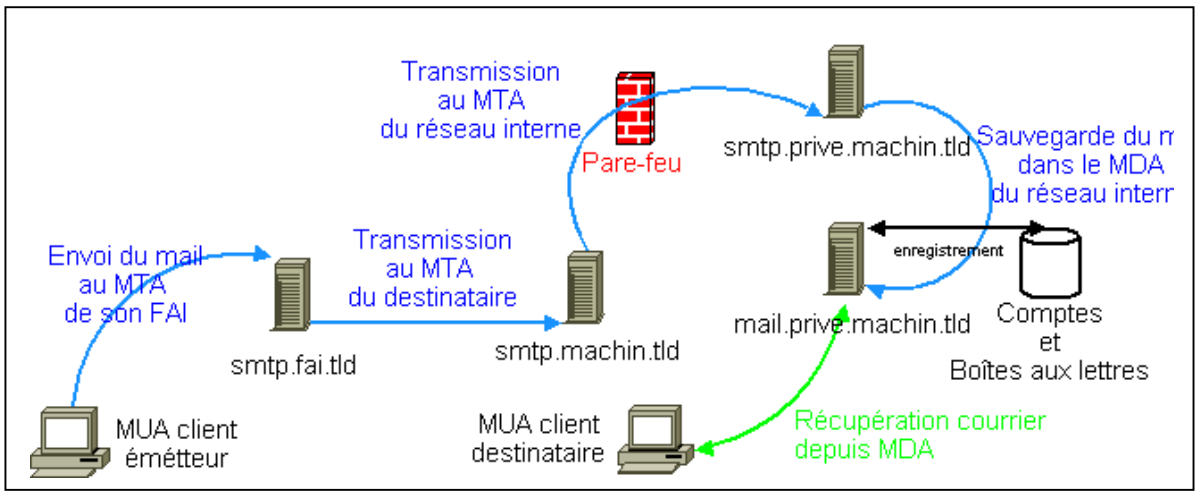


Figure I.3 : Récupération du courrier de la boite aux lettres par le MDA.

I.7.Architecture et principe de fonctionnement

Les différents éléments d'un système de messagerie sont agences selon une architecture logique, pour en assurer le fonctionnement. L'architecture d'un système de messagerie peut être représentée de la sorte :

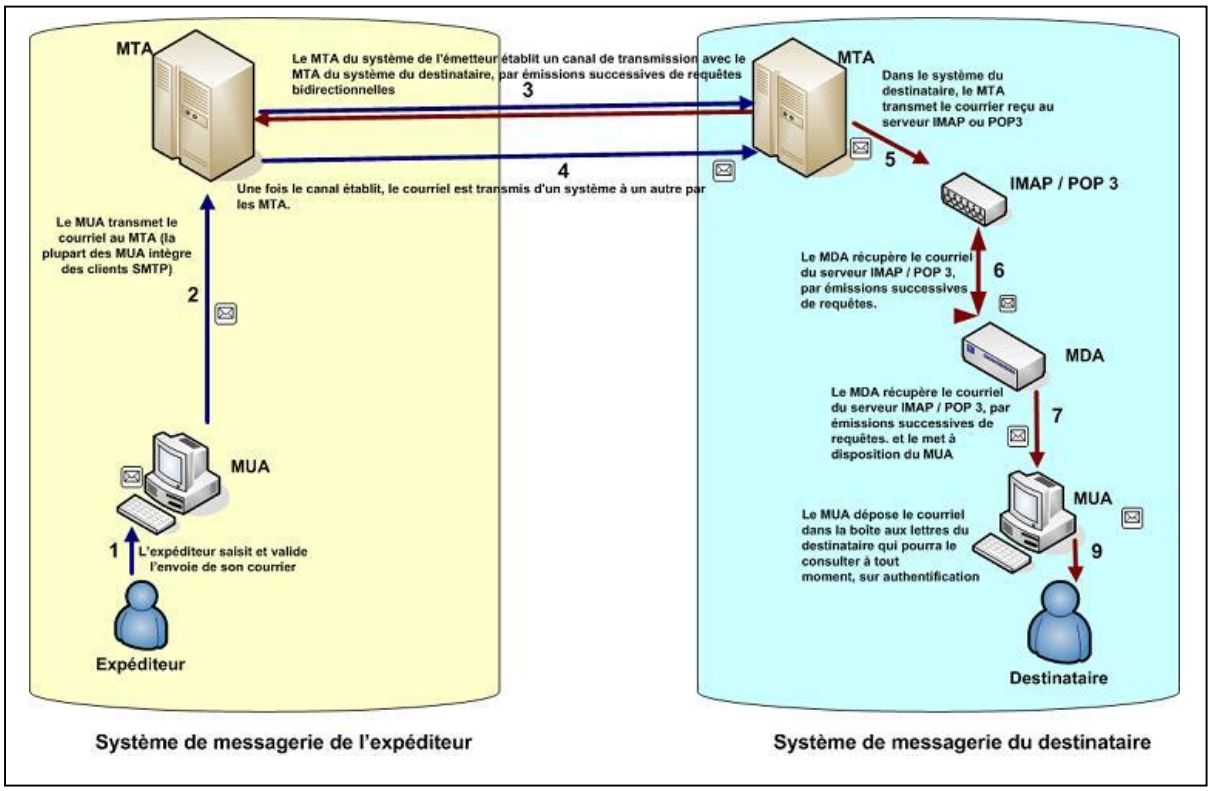


Figure I.4 : Architecteur d'un système de messagerie.

- **Les étapes de fonctionnement de système de messagerie**
  - **Etape 1 :** L'expéditeur saisit et valide l'envoie de son courrier.
  - **Etape 2 :** Le MUA transmet le courriel au MTA, (la plupart de MUA intègre des clients SMTP).
  - **Etape 3 :** Le MTA du système de l'émetteur établit un canal de transmission avec le MTA du système du destinataire, par émission successives de requêtes bidirectionnelles.
  - **Etape 4 :** Une fois le canal établit, le courriel est transmis d'un système à un autre par le MTA.
  - **Etape 5 :** Dans le système du destinataire, le MTA transmet le courrier reçu au serveur IMAP ou POP.
  - **Etape 6 :** Le MDA récupère le courriel du serveur IMAP /POP3 par émission successives de requêtes.
  - **Etape 7 :** Le MDA récupère le courriel du serveur IMAP /POP3 par émission successives de requêtes, et le met à disposition du MUA.
  - **Etape 8 :** Le MUA dépose le courriel dans la boîte aux lettre du destinataire, qui pourra consulter à tout moment authentification.

I.8.Le contexte d'utilisation de la messagerie électronique en entreprise

On distingue trois cas d'utilisation de la messagerie électronique dans une entreprise :

- Une utilisation purement interne, via le réseau privé de l'entreprise, appelée: Intranet.
- Une utilisation étendue à des fournisseurs ou partenaires, appelée: Extranet.
- Une utilisation ouverte vers l'extérieur via des réseaux publics, appelée: Internet.

I.8.1.L'utilisation de l'e-mail au sien d'un Intranet

Un Intranet est un ensemble de services internes à un réseau local, c'est –à-dire accessible uniquement à partir des postes d'un réseau local, ou bien d'un ensemble de réseaux bien définis, et invisible de l'extérieur. Ces services sont basés les même technologies que l'Internet (protocole de communication TCP/IP, messagerie électronique, partage des données, serveur Web interne,…etc.).

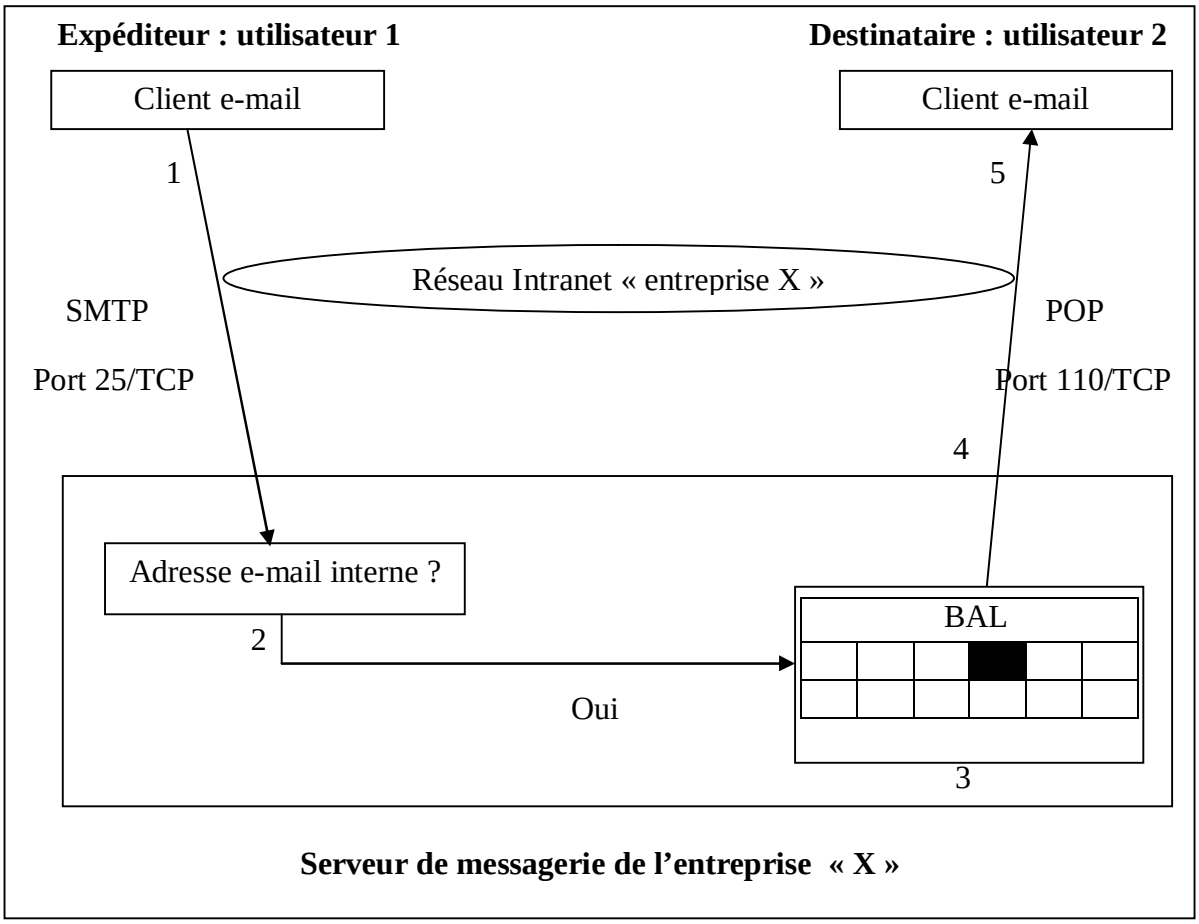


Figure I.5 : Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à la même entreprise (Intranet).

- **Les étapes**

1. L'utilisateur 1 expédie un e-mail, avec comme adresse de destination celle de l'utilisateur 2. Il utilise un client de messagerie configuré pour dialoguer avec le serveur de messagerie de son entreprise « entreprise X ».
2. Le serveur de messagerie analyse l'adresse de destination de cet e-mail, il reconnait que celle–ci correspond à une adresse interne à l'entreprise (utilisateur2@entrepresex.extansion).
3. L'e-mail est donc dépose dans la boîte aux lettres (BAL) assignée à l'utilisateur 2.
4. L'utilisateur 2 destinataire de cet e-mail, doit périodiquement interroger le serveur de messagerie (manuellement ou automatiquement), afin de savoir s'il a du courrier en attente.
5. Dans le cas positif, les e-mails en attente sut le serveur de messagerie peuvent être rapatriés sur le poste de travail du destinataire (utilisateur 2).

I.8.2.L'utilisation de l'e-mail au sien d'un Extranet

Un Extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'Extranet doit être sécurisé dans la mesure, où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe), ou d'une authentification forte (authentification à l'aide d'un certificat). Il est conseillé d'utilises HTTOS pour toutes les pages Web consultées depuis l'extérieur.

De cette façon, un Extranet n'est ni un site Internet, ni un Internet, il s'agit d'un système supplémentaire offrant par exemple aux clients d'une entreprise, à ses partenaires ou à des filiales un accès privilégié à certaines ressources informatiques de l'entreprise par l'intermédiaire d'une interface Web.

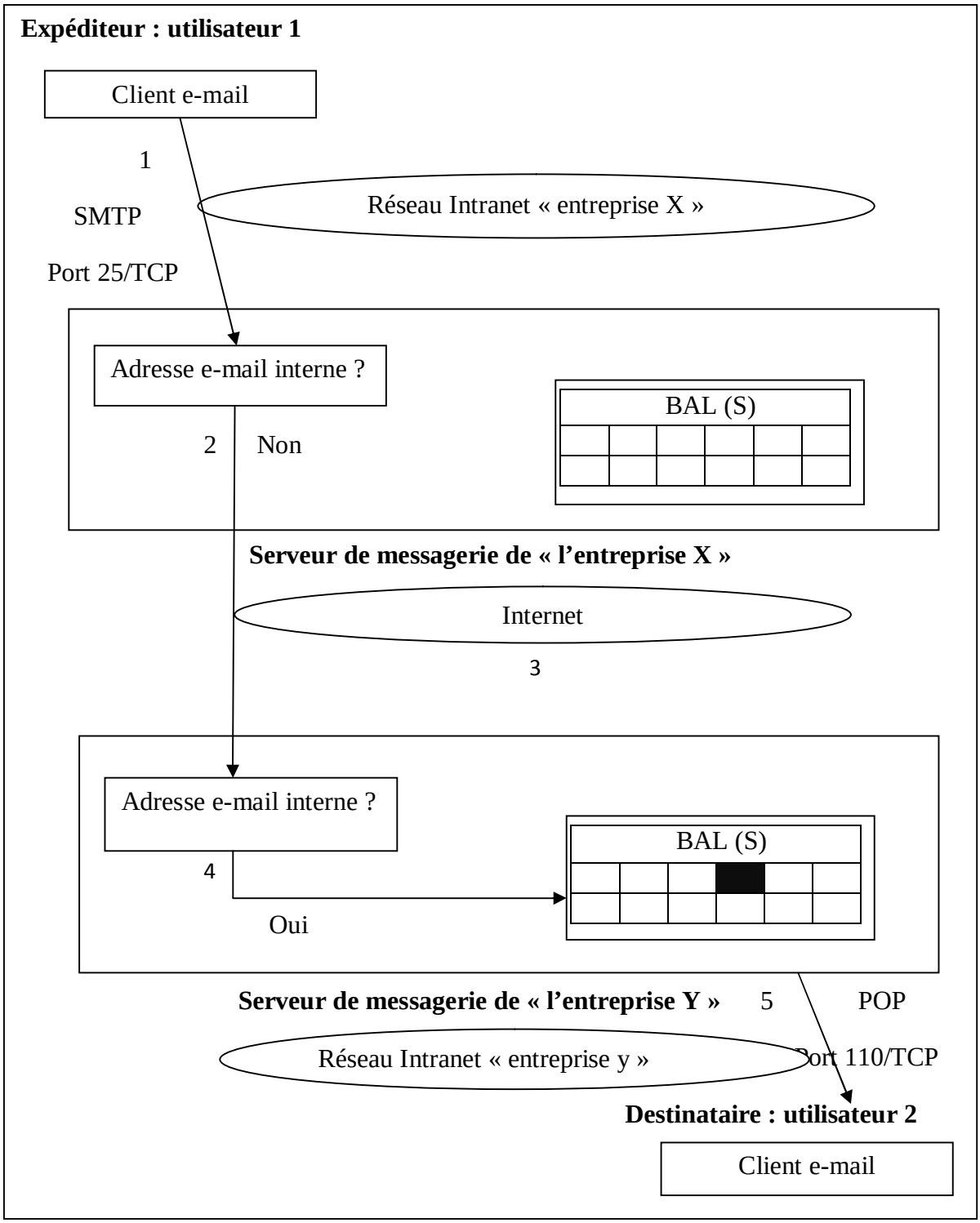


Figure I.6 : Illustration de l'acheminement d'un e-mail entre deux correspondants appartenant à des entreprises différentes (Internet ou Extranet).

- **Les étapes**

1. L'utilisation 1 expédie un e-mail, avec comme adresse de destination celle de l'utilisateur 2 à l'extérieure de l'entreprise. Il utilise un client de messagerie configuré pour dialoguer avec le serveur de messagerie de son entreprise « entreprise X ».
2. Le serveur de messagerie analyse l'adresse de destination.
3. Compte tenu que l'adresse de destination ne corresponde pas à une adresse interne, le serveur de la messagerie « entreprise X » oriente le message via Internet vers le serveur de messagerie de la société « entreprise Y ». Une recherche de l'adresse IP du serveur de messagerie de l'entreprise destinataire est alors nécessaire, il s'agit d'une interrogation du DNS (Domain Name Service). La résolution DNS s'obtient à partir du nom de domaine situé à la droite du signe @ de l'adresse de l'expéditeur « utilisateur2@entreprisey.extension ». Eventuellement, l'email peut transiter par plusieurs serveurs de messagerie intermédiaires.
4. Le serveur de messagerie de la société « entreprise Y » analyse l'adresse de destination de l'e-mail, il constate que cette adresse correspond à une des adresse internes et référencées, il place donc l'e-mail dans la boite aux lettres du destinataire.
5. L'utilisateur 2 destinataire de cet e-mail, doit interroger périodiquement le serveur de messagerie (manuellement ou automatiquement), afin de savoir s'il a du courrier en attente.
6. Les e-mails en attente sur le serveur de messagerie peuvent être rapatriés sur le poste de travail du destinataire (utilisateur2).

I.8.3.L'utilisation de l'e-mail au sein d'un Internet

L'Internet forme une gigantesque toile d'araignée (en anglais « Web ») formant le réseau le plus vaste, puisqu'il contient l'interconnexion des différents réseaux (LAN, MAN et WAN). Sur Internet il existe différents protocoles qui permettent de faire plusieurs applications :

- **IRC (Internet Relay Chat)**

Qui signifie discision relayée par Internet. Elle utilise un protocole qui sert à la communication instantanée (en temps réel) principalement, sous la forme de discussions en groupe par l'intermédiaire de canaux de discussion. IRC correspond en fait à un

serveur de conférence électronique improvisée, qui s'article autour d'un contexte question et réponses. Les paquets IRC arrivent sur le port 6667, (ou un autre situé généralement autour de 7000).

- **HTTP (Hyper Text Transfer Protocol**)

La version du protocole HTTP 0.9 était uniquement destine à transférer des données sur Internet, mais la version 1.0 permet un transfert de fichiers (essentiellement au format HTML) localisés, grâce à une chaîne de caractères appelée URL, entre un navigateur (le client) et un serveur Web, mais également un transfère des messages avec des en-têtes décrivant le contenu du message, en utilisant le codage MIME. Les paquets http arrivent sur le port 80, et sont transmis au navigateur Internet à partir du quel la page à été appelée.

- **FTP (File Transfert protocole)**

Est un protocole de communication dédie à l'échange informatique de fichier sur un réseau TCP/IP. Il permet depuis un ordinateur, de copier des fichiers depuis ou vers un autre ordinateur du réseau, ou encore de supprimer ou modifier des fichiers sur cet ordinateur.

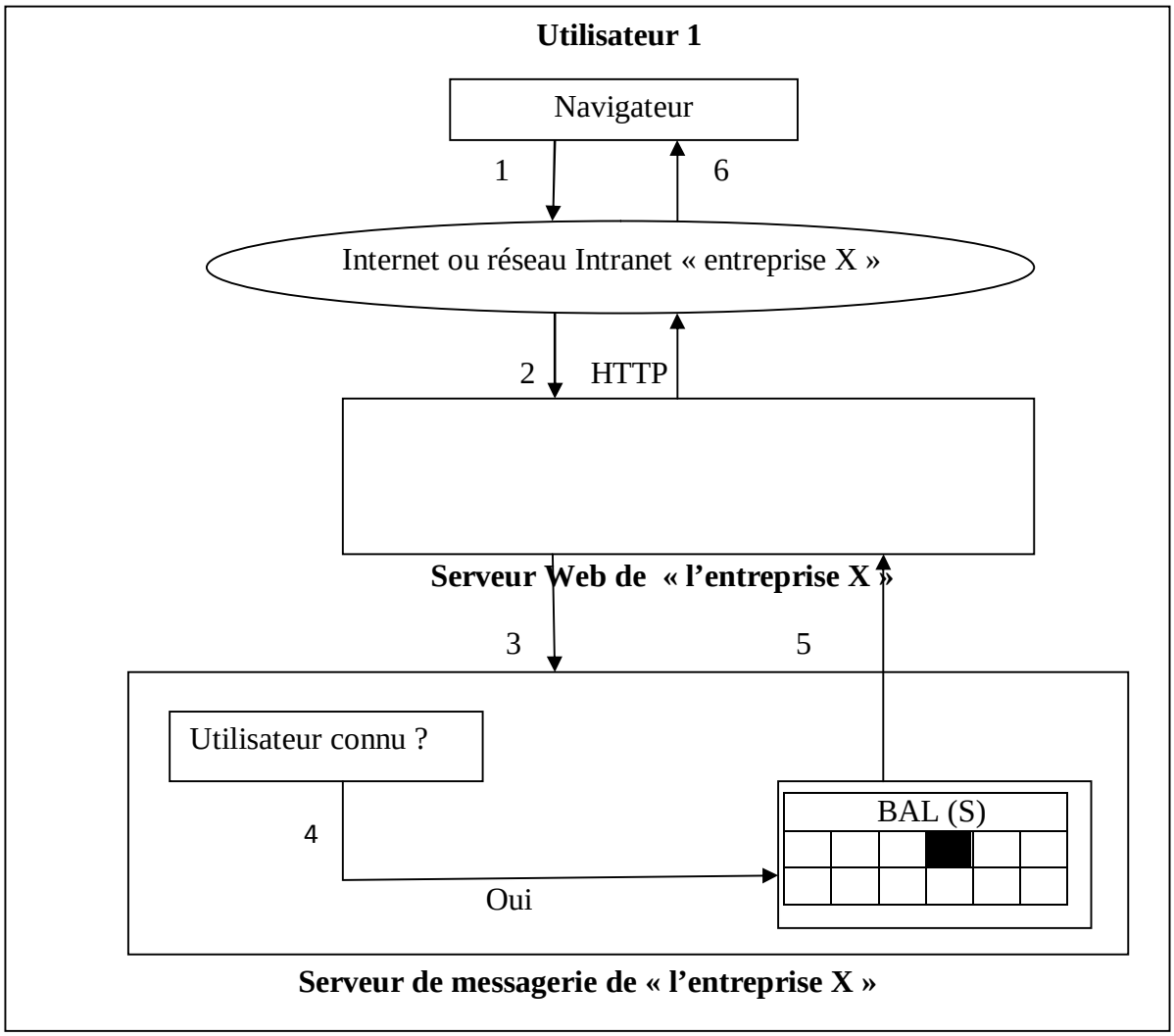


Figure I.7 : Illustration de l'accès à un serveur de messagerie à partir d'un navigateur (Webmail) pour le retrait d'un e-mail.

- **Les étapes**

1. L'utilisateur 1 se connecte au serveur Web de son entreprise à l'aide de son navigateur. Il accède à une page http permettant de solliciter le service Webmail d'accès à sa messagerie. Un dialogue initial permet d'identifier et d'authentifier l'utilisateur.
2. Le serveur Web élabore une requête destinée au serveur de messagerie.
3. La requête est transmise au serveur de messagerie de « l'entreprise X ».
4. Le serveur de messagerie de « l'entreprise X » authentifie le propriétaire de la boîte aux lettres.
5. Tous les messages reçus sont transmis au serveur Web, qui les reformate dans une page Web.

6. Le résultat est transmis en retour au navigateur de l'utilisateur 1, qui peut alors consulter le contenu de ses e-mails.

I.9.Discussion

Nous avons présenté les différents éléments théoriques impliqués dans la réalisation d'un système de messagerie. Nous avons commencé par présenter le format d'un message électronique et le standard MIME, qui normalise la structure et le codage des messages. Nous avons ensuite présenté le service de messagerie électronique, son architecture et les différents agents intervenant dans son fonctionnement.

II.1.Préambule

L'acheminement de l'e-mail se fait en plusieurs étapes. Tout d'abord, le courrier est envoyé à un serveur de mail, qui va se charger de l'acheminement à bon port. Le serveur source transmet le message au serveur destinataire, qui le stocke en attendant que l'utilisateur destinataire le récupère à partir de sa boîte lettres personnelle. Contrairement au courrier postal, l'acheminement d'un message électronique est beaucoup plus rapide, et il peut être distribué automatiquement à plusieurs destinataires à la fois.

Tout au long de ce chapitre nous avons exposé un ensemble des protocoles utilisés par les serveurs pour acheminer le courrier.

II.2.Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers (le FTP), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP),…etc.

II.3.Classification des protocoles

On classe généralement les protocoles en deux catégories, selon le niveau de contrôle des données que l'on désire :

II.3.1.Les protocoles orientés connexion

Il s'agit des protocoles opérant un contrôle de transmission des données (paquets), pendant une communication établie entre deux machines. Dans tel machine réceptrice envoie des accusés de réception lors de la communication, ainsi la machine émettrice est garante de la validité des données qu'elle envoie en assurant l'ordre de remise des paquets, leur retransmission en cas de perte ou d'erreur, et la vérification de l'intégrité de l'en-tête des paquets.

II.3.2.Les protocoles non orientés connexion

Il s'agit d'un mode de communication dans lequel la machine émettrice envoie des données (datagrammes) sans prévenir la machine réceptrice, et la machine réceptrice reçoit les

données sans envoyer d'avis de réception à la première. Ce protocole ne garantit ni la remise ni l'ordre des paquets délivrés.

II.4.Les différents serveurs et protocoles de la messagerie électronique

Le fonctionnement du courrier électronique repose sur une série des protocoles de communication destinés à envoyer les messages, de serveur à serveur, à travers l'Internet. Les principaux protocoles sont les suivants : TELNET, SMTP, POP et IMAP. Ces derniers font partis d'une suite des protocoles et appelée TCP/IP.

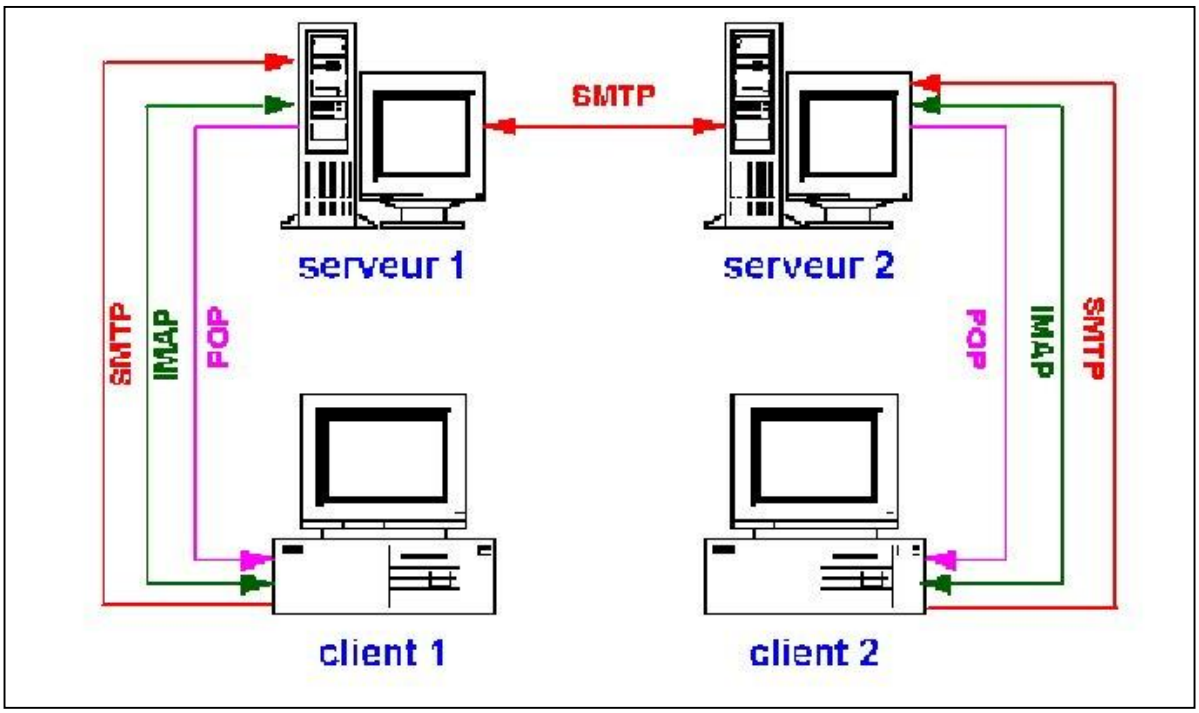


Figure II.1 : Les protocoles de la messagerie électronique.

II.4.1.Le protocole TELNET (TELecommunication NETwork)

Le premier protocole historique est TELNET. C'est un protocole standard permettant à un ordinateur de se connecter à distance à un autre ordinateur, via l'Internet, en mode caractère uniquement : une fois que l'on est connecté la machine distante, les touches tapées au clavier sont directement transmise à celle-ci, et à partir du TELNET la machine nous renvoie les réponses. Généralement, la machine distante commence la communication par nous demandes un mot de passe d'accès, puis nous donne accès à un Shell sur lequel nous pouvons lancer nos commandes.

Le protocole TELNET s'appuie sur une connexion TCP, pour envoyer des données au format ASCII entre lesquelles s'intercalent des séquences de contrôle TELNET ; Il fournit ainsi un système orienté communication, bidirectionnel. C'est un protocole de base, sur lequel s'appuient certains autres protocoles de la suite TCP/IP (FTP, SMTP, POP3, IMAP,…etc.). Ainsi, TELNET permet de transférer des fichiers FTP, de lire le courrier électronique et de visionner des documents HTML.

Le serveur TELNET n'est pas sécurisé, toutes les informations (y compris le compte d'utilisateur et le mot de passe) circulent en clair dans le réseau.

II.4.2.Le protocole SMTP (Simple Mail Transfert Protocole)

Est un protocole de communication utilisé pour transférer le courrier électronique, soit d'un client à un serveur, soit d'un serveur à un autre. L'utilisation de ce protocole est assez simple, il fonctionne en mode commuté dans des trames TCP/IP, grâce à des commandes textuelles, (chaine de caractère ASCII termine par le caractère CR/LF, qui est une séquence de deux octets qui indique la fin de ligne dans un texte).

Dans un dialogue, par exemple entre un client et un serveur de messagerie, chaque commande envoyée du client est suivie d'une réponse du serveur SMTP. Une réponse est composée d'un numéro et d'un message, afin de signaler est prise en compte ou non pas le serveur.

SMTP : EXEMPLE

• Il existe cinq commandes SMTP pour envoyer du courrier :

– HELO, MAIL, RCPT, DATA, QUIT

mail –v djouher@bastos.dz

Subjectif: SMTP Essai

Coucou

.

Cc:

djouher@bastos.dz... Relier à bastos.dz. par esmtp...

220 bastos.dzESMTP Sendmail 8.9.3+Sun/8.9.0; Mon, 27join 2014 13:35:01 +0100 (a RENCONTRÉ)

>>> EHLO djouher@bastos.dz

250 bastos.dz Bonjour djouher@bastos.dz [192.168.1.12], content vous rencontrer

250-8BITMIME

250 SIZE

250-DSN

250-ONEX

250-XUSR

250 HELP

>>> MAIL From:< djouher@bastos.dz > SIZE=60

250 <djouher@bastos.dz>... ok de l'Envoyeur

>>> RCPT To:< djouher@bastos.dz>

250 <djouher@bastos.dz>... ok du Destinataire

>>> DATA

354 entrent le courrier, terminez avec ". " sur une ligne

>>>.

250 Message PAA20253 a accepté pour livraison

djouher@bastos.dz... a Envoyé (le Message PAA20253 a accepté pour livraison)

>>>QUIT

221 bastos.dz qui ferment le rapport 4

Dans cet exemple les numéros apparus sont : 220, 250, 354 et 221 qui signifient respectivement : service prêt, action exécutée, début de saisie de message fin avec un point «.» et fermeture du canal de transmission.

D'autres code de messages de services peuvent être interceptés dans les messages tels que : 211(état de système), 214(message d'information), 251(utilisation non locale),…etc.

Et les codes d'erreurs tels que : 450(requête non prise en compte, boite inaccessible ou occupée), 452(requête non prise en compte, espace mémoire insuffisant), 500(erreur de syntaxe, commande non reconnue, ligne de commande trop langue),…etc.

- **Récapitulatif des principales commandes SMTP**

Commande	Exemple	Description
HELO	HELO 192.168.1.12	Identification à l'aide de l'adresse IP ou du nom de domaine de l'ordinateur expéditeur.
MAIL FROM	MAILFROM : expediteut@domaine.com	Identification de l'adresse de l'expéditeur.
RCPT TO	RCPTTO : destinataire@domaine.com	Identification de l'adresse du destinataire.
DATA	DATA message	Partie de l'entête et corps du mail.
QUIT	QUIT	Permet de quitter la connexion sur le serveur SMTP.
HELP	HELP	Liste des commandes SMTP supportées par le serveur.

Tableau II.1 : Récapitulatif des principales commandes SMTP.

II.4.3.Le protocole ESMTP (Extended Simple Mail Transfert Protocole)

Il est une amélioration du protocole SMTP avec lequel il est compatible, il fournit des options supplémentaires d'authentification et de cryptage. La commande « HELO » est remplacée par la commande « EHLO » (Extended Helo). Le destinataire ne répond plus seulement « OK », mais donne aussi la liste des extensions qu'il est capable de traiter.

Dans le cas où le destinataire ne supporte pas le protocole ESMTP, retourne un message d'erreur. Le poste émetteur envoie alors la commande HELO pour initier une communication SMTP.

- **Récapitulatif des principales commandes ESMTP**

Commande	Description
8BITMIME	Permet au client d'envoyer des messages comportant des caractères 8bits.
DNS	(Delivery Status Notification) : Génère et envoie une notification d'état de remise à l'ordinateur expéditeur en cas de la remise.
SIZE	Indique avant l'envoie par le client, la taille maximale des messages admissibles par le serveur.

Tableau II.2 : Récapitulatif des principales commandes ESMTP.

II.4.4.Le protocole POP (Post Office Protocole)

Est un protocole qui permet de récupérer les courriers électroniques, situés sur un serveur de messagerie électronique. Ce protocole a été réalisé en plusieurs versions respectivement : POP1, POP2, POP3. Actuellement, c'est POP3 (Post Office Protocole Version3) qui utilisé de façon standard.

Tout comme dans le cas de protocole SMTP, le protocole POP (POP2, POP3) fonctionne grâce à des commendes textuelles envoyées au serveur POP. Chacune des commendes envoyées par le client (validée par la séquence CR/LF), est composée d'un mot clé éventuellement accompagné d'un au plusieurs arguments, et est suivie d'une réponse de serveur POP (soit + OK ou - ERR).

v Récapitulatif des principales commandes POP3

Commande	Description
USER identifiant	Cette commande permet de s'authentifier. Elle doit être suivie du nom de l'utilisateur, c'est-à-dire une chaine de caractère identifiant l'utilisateur sur le serveur. La commande USER doit précéder la commande PASS.
PASS mot_de_passe	La commande PASS, permet d'indiquer le mot de passe de l'utilisateur dont le nom a été spécifié lors d'une commande USER préalable
STAT	Information sur les messages contenus sur le serveur.
RETR	Numéro du message à récupérer.
DELE	Numéro du message à supprimer.
LIST [msg]	Numéro du message à afficher.
NOOP	Permet de garder les connexions ouvertes en cas d'inactivité.
TOP <message-ID> <n>	Commande affichant n liges du message, dont le numéro est donné en argument. En cas de réponse positive de serveur, celui-ci revoie les en-têtes du message, puis une ligne vierge et enfin les n premières lignes du message.
UIDEL [msg]	Demande au serveur de renvoyer une ligne contenant des informations sur le message éventuellement donné en argument. Cette ligne contient une chaine de caractère, appelée *listing d'identificateur unique,* permettant d'identifier de façon unique le message sur le serveur, indépendamment de la session. L'argument optionnel est un numéro correspondant à un message existent sur le serveur POP,
QUIT	La commande QUIT de la sortie du serveur POP3.Elle entraine la suppression de tous les messages marqués comme effacés et revoie l'état de cette action.

Tableau II.3 : Récapitulatif des principales commandes POP3.

Le protocole POP3 gère ainsi l'authentification, à l'aide d'un nom d'utilisateur et d'un mot de passe, il n'est pas sécurisé, car les mots de passe au même titre que les mails circulent en clair sur le réseau. D'autre part le protocole POP3 bloque la boite aux lettres lors de la

consultation, ce qui signifie qu'une consultation simultanée par deux utilisateurs d'une même boite aux lettres est impossible.

II.4.5.Le protocole IMAP (Internet Message Access Protocole)

Ce protocole permet de récupérer les courriers électroniques déposés sur des serveurs de messagerie. Son but est similaire à POP3, l'autre principal protocole de relève du courrier. Mais contrairement à ce dernier, il présente les avantages suivants :

- Ø Possibilité de stocker les messages sur le serveur de manière structurée.
- Ø Gestion de plusieurs boites aux lettres.
- Ø Permet l'accès direct à des parties du message, (par exemple les en-têtes sans le corps du message).

Un serveur IMAP, est un système de fichiers dont les répertoires sont des classeurs, chaque classeur contient des messages. A chaque message est associé des informations (en plus de corps et de l'en-tête des messages), tels que :

- Ø Un numéro unique.
- Ø Une série de drapeaux (message lu, réponse envoyée, message à effacer,…etc.).
- Ø Une date de réception du message.

v Récapitulatif des principales commandes IMAP

Commande	Description
LOGIN	Connexion au serveur IMAP.
LIST	List des dossiers.
SELECT	Selection d'un dossier.
SEARCH	Recherche de messages dans un dossier en fonction de critère.
FETCH	Récupération d'un message.
STORE	Association de drapeaux à un message.
LOGOUT	Déconnexion du serveur IMAP.

Tableau II.4 : Récapitulatif des principales commandes IMAP.

II.4.6.Le protocole LDAP (Lightweight Directory Access Protocol)

LDAP (Lightweight Directory Access Protocol, traduisez Protocole d'Accès aux Annuaires Léger), est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau, par l'intermédiaire de protocoles TCP/IP. Les bases d'informations sont généralement relatives à des utilisateurs, mais elles sont parfois utilisées à d'autres fins, comme pour gérer du matériel dans une entreprise.

Le protocole LDAP définit la méthode d'accès aux données sur le serveur au niveau du client, et non la manière de laquelle les informations sont stockées.

Le protocole LDAP en est actuellement à la version 3, et a été normalisé par l'IETF (Internet Engineering Task Force). Ainsi, il existe une RFC pour chaque version de LDAP, constituant un document de référence :

- RFC 1487 pour LDAP v.1 standard.
- RFC 1777 pour LDAP v.2 standard (1994).
- RFC 2251 pour LDAP v.3 standard (1997).

Le protocole LDAP, développé en 1993 par l'université du Michigan, avait pour but de supplanter le protocole DAP (servant à accéder au service d'annuaire X.500 de l'OSI), en l'intégrant à la suite TCP/IP.

Le service d'annuaire X.500 était un standard conçu en 1988, par les opérateurs télécoms prévu pour interconnecter tout type d'annuaire dans un but de normalisation. Celui-ci définit :

- des règles de nommages pour les éléments qu'il contient.
- des protocoles d'accès à l'annuaire (dont DAP).
- des moyens d'authentification de l'utilisateur.

Toutefois, la norme X.500 était basée sur les protocoles ISO, et impliquait donc une mise en place très lourde. Ainsi, en 1993 l'université du Michigan a adapté le protocole DAP de la norme X.500 au protocole TCP/IP, et mis au point LDAP.

A partir de 1995, LDAP est devenu un annuaire natif (LDAP standard), afin de ne plus servir uniquement à accéder à des annuaires de type X.500, c'est-à-dire en gérant sa propre base de

données. LDAP est ainsi une version allégée du protocole DAP, d'où son nom de Lightweight Directory Access Protocol prévu pour fonctionner avec les protocoles TCP/IP.

- **Fonctionnalités**

Le protocole LDAP est uniquement prévu pour gérer l'interfaçage avec les annuaires. Plus exactement il s'agit d'une norme définissant la façon suivant laquelle les informations sont échangées entre le client et le serveur LDAP, ainsi que la manière de laquelle les données sont représentées. Ainsi ce protocole se conforme à quatre modèles de base :

- **un modèle d'information** : définissant le type d'information stocké dans l'annuaire.
- **un modèle de nommage** (parfois appelé modèle de désignation) : définissant la façon de laquelle les informations sont organisées dans l'annuaire et leur désignation.
- **un modèle fonctionnel** (parfois appelé modèle de services) : définissant la manière d'accéder aux informations et éventuellement de les modifier, c'est-à-dire les services offerts par l'annuaire.
- **un modèle de sécurité** : définissant les mécanismes d'authentification et des droits d'accès des utilisateurs à l'annuaire.

De plus, LDAP définit la communication entre :

- **Le client et le serveur**, c'est-à-dire les commandes de connexion et de déconnexion au serveur, de recherche ou de modification des entrées.
- **Les serveurs eux-mêmes**, pour définir d'une part le service de réplication (réplication service), c'est-à-dire un échange de contenu entre serveurs et synchronisation, d'autre part pour créer des liens entre les annuaires.

Le format des données dans le protocole LDAP, n'est pas le format ASCII comme c'est le cas pour la plupart des protocoles, mais une version allégée du Basic Encoding Rules (BER), appelée Lightweight Basic Encoding Rules (LBER).

D'autre part, LDAP fournit un format d'échange (LDIF, Lightweight Data Interchange Format), permettant d'importer et d'exporter les données d'un annuaire avec un simple fichier texte.

Enfin, il existe un certain nombre d'API (Application Programming Interface, c'est-à-dire des interfaces de programmation), permettant de développer des applications clientes,

permettant de se connecter à des serveurs LDAP avec différents langages. Ainsi LDAP fournit à l'utilisateur des méthodes lui permettant de :

- Se connecter.
- Se déconnecter.
- Recherche des informations.
- Comparer des informations.
- Insérer des entrées.
- Modifier des entrées.
- Supprimer des entrées.

D'autre part le protocole LDAP (dans sa version 3), propose des mécanismes de chiffrement (SSL) et d'authentification (SASL), permettant de sécuriser l'accès aux informations stockées dans la base.

De plus, contrairement à la plupart des protocoles, LDAP permet d'effectuer plusieurs requêtes sur le serveur d'annuaire à l'aide d'une seule connexion. En effet, le protocole HTTP ne permet d'effectuer qu'une et une seule requête à chaque connexion au serveur.

- **Extensibilité du protocole LDAP**

Le protocole LDAP version 3, a été conçu de telle façon qu'il soit possible d'y ajouter des fonctionnalités, sans avoir à s'écarter de la norme grâce à trois concepts :

- **opérations étendues LDAP** (LDAP extended operations), permettant de rajouter une opération aux neuf opérations originales.
- **contrôles LDAP** (LDAP controls), permettant d'associer des paramètres supplémentaires à une opération pour en modifier le comportement.
- **SASL** (Simple Authentification and Security Layer), une couche supplémentaire permettant d'utiliser des méthodes d'authentification externes de façon modulaire.

- **Les avantages de LDAP**

  - **Annuaire de recherche / Page blanche :** Un annuaire LDAP est avant tout un annuaire. Il permet donc d'obtenir des informations sur une personne enregistrée, comme son adresse email, son numéro de téléphone, son service, ou n'importe quel

autre renseignement que l'on aura jugé bon de stocker dans la base. La recherche peut se faire selon de multiples critères.

Des applications clientes (clients de messagerie : Outlook, Netscape,…etc.), comme des applications serveurs (serveur de messagerie : Postfix, Sendmail,…etc.).

- **Authentification :** De nombreuses applications nécessitant une authentification sont aujourd'hui capables d'interroger un annuaire LDAP, et d'y vérifier l'identité d'un utilisateur grâce à un couple login / mot de passe.
- **Unification / Centralisation :** De nombreuses applications sont capables d'interroger un même annuaire LDAP : authentification d'utilisateur Unix (pam_ldap) ou Windows (Samba), proxy (Squid), web (Apache : Auth LDAP), POP3, IMAP,…etc.

  Les utilisateurs de tout ces services, ne s'identifient, alors qu'avec un seul identifiant pour tout ces services.
- **Fiabilité :** Des mécanismes de réplication (en cours de standardisation) entre des annuaires maîtres et des réplicas, permettent d'assurer une bonne fiabilité au système.
- **Sécurisation :** Les annuaires supportent pour la plupart des mécanismes de chiffrage des connexions (SSL, TLS).

  Les droits d'accès aux différentes données de l'annuaire, peuvent être précisés finement grâce à des ACL.
- **Support de nombreux environnements de développement :** Des librairies pour accéder à un annuaire LDAP existent dans la plupart des langages (C, C++, Java, Perl, PHP,…etc.).
- **Consulter les données :** LDAP fournit un ensemble des fonctions (procédures), pour effectuer des requêtes sur les données afin de rechercher, modifier, effacer des entrées dans les répertoires.

Voici la liste des principales opérations que LDAP peut effectuer :

Opération	Description
Abandon	Abandonne l'opération précédemment envoyées au serveur.
Add	Ajoute une entrée au répertoire.
Bind	Initie une nouvelle session sur le serveur LDAP.
Compare	Compare les entrées d'un répertoire selon des critères.
Delete	Supprime une entrée d'un répertoire.
Extended	Effectuer des opérations étendues.
Rename	Modifie le nom d'une entrée.
Search	Recherche des entrées d'un répertoire.
Unbind	Termine une session sur le serveur LDAP.

Tableau II.5 : La liste des principales opérations que LDAP peut effectuer.

II.4.7.Le protocole SSH (Secure Shell)

SSH signifie Secure Shell, est un protocole qui facilite les connexions sécurisées entre deux systèmes, à l'aide d'une architecture client/serveur, et permet aux utilisateurs de se connecter à distance à des systèmes hôte de serveur. Toutefois, contrairement à d'autres protocoles de communication à distance, tels que FTP ou TELNET, SSH crypte la session de connexion et empêche ainsi tout agresseur de recueillir des mots de passe non-cryptés.

SSH est conçu pour remplacer les applications de terminal plus anciennes, et moins sécurisées qui sont utilisées pour se connecter à des hôtes distants, comme TELNET ou rsh. Un programme similaire appelé scp, remplace des programmes moins récents conçus pour copier des fichiers entre des hôtes, tels que rcp. Étant donné que ces applications plus anciennes, ne cryptent pas les mots de passe entre le client et le serveur, il est recommandé d'éviter autant que possible de les utiliser. En effet, l'utilisation de méthodes sécurisées pour se connecter à des systèmes distants, réduit les risques aussi bien pour le système client que pour l'hôte distant.

La première version de SSH (SSH-1) a été conçue par Tatu Ylönen, à Espoo, en Finlande en 1995. Il a créé le premier programme utilisant ce protocole et a ensuite créé une entreprise, SSH Communications Security pour exploiter cette innovation. Cette première version utilisait certains logiciels libres comme la bibliothèque Gnu libgmp, mais au fil du temps ces logiciels ont été remplacés par des logiciels propriétaires. SSH Communications Security a vendu sa licence SSH à F-Secure, (anciennement connue sous le nom de Data

Fellows). La version suivante a été nommée (SSH-2). Le groupe de recherche de l'IETF « secsh » a défini en janvier 2006 le standard Internet SSH-2, que l'on retrouve actuellement dans la plupart des implémentations.

- **Fonctionnalités**

- Le principal objectif de SSH était de résoudre le problème de transmission en clair, de toutes les informations sur le réseau LAN ou Internet.
- Le protocole SSH, permet le transfert d'informations de manière sécurisée. Il existe plusieurs commandes utilisant ce protocole : scp et sftp pour le transfert de fichiers sécurisé, et ssh pour ouvrir une session à distance ou exécuter des commandes à distance de manière sécurisée.
- SSH peut également être utilisé pour transférer des ports TCP d'une machine vers une autre, créant ainsi un tunnel. Cette méthode est couramment utilisée afin de sécuriser une connexion, qui ne l'est pas (par exemple le protocole de récupérations de courrier électronique POP3), en la faisant transférer par le biais du tunnel chiffré SSH.
- Habituellement le protocole SSH utilise le port TCP 22. Il est particulièrement utilisé pour ouvrir un Shell sur un ordinateur distant. SSH fait référence pour l'accès distant sur les stations Linux et Unix.
- Il est également possible de faire plusieurs sauts entre consoles SSH, c'est-à-dire ouvrir une console sur un serveur, puis, de là, en ouvrir une autre sur un autre serveur.
- Avec SSH, l'authentification peut se faire sans l'utilisation de mot de passe ou de phrase secrète, en utilisant la cryptographie asymétrique. La clé publique est distribuée sur les systèmes sur lesquels on souhaite se connecter. La clé privée, qu'on prendra le soin de protéger par un mot de passe, reste uniquement sur le poste à partir duquel on se connecte.
- Le protocole SSH (Secure Shell), est utilisé pour établir un accès sécurisé permettant d'effectuer des opérations sensibles sur des machines distantes, et d'effectuer des transferts de fichiers à travers un réseau public, tout en garantissant l'authentification, la confidentialité et l'intégrité des données.

- **Pourquoi utiliser SSH ?**

Les utilisateurs d'ordinateurs malintentionnés disposent d'une variété d'outils pour interrompre, intercepter et réacheminer le trafic réseau afin de s'octroyer l'accès à un système. D'une manière générale, ces menaces peuvent être répertoriées de la manière suivante :

- **Interception d'une communication entre deux systèmes :** dans ce scénario, le pirate peut se trouver quelque part sur le réseau entre les entités qui communiquent, pouvant ainsi copier toute information qui est transmise entre elles. Le pirate peut intercepter et garder les informations, ou peut les modifier avant de les envoyer au destinataire prévu. Cette attaque peut être orchestrée en utilisant un programme renifleur (un utilitaire réseau courant).

- **Usurpation de l'identité d'un hôte :** grâce à cette technique, le système d'un agresseur est configuré de telle manière, qu'il apparaît comme étant le destinataire souhaité d'une transmission. Si cette stratégie fonctionne, le système de l'utilisateur ne détecte pas qu'il communique en fait avec le mauvais hôte. Ce type d'attaque peut être organisé grâce à l'utilisation de techniques appelées : empoisonnements DNS ou usurpation d'adresse IP.

  Ces deux techniques permettent d'intercepter des informations potentiellement confidentielles, et si cette interception est effectuée pour des raisons hostiles, le résultat peut être catastrophique.

L'utilisation du protocole SSH pour effectuer une connexion au Shell à distance, ou pour copier des fichiers permet de réduire considérablement ces menaces au niveau de la sécurité. En effet, le client et serveur SSH utilisent des signatures numériques pour vérifier leur identité respectives. En outre, toute communication entre le système client et le système serveur est cryptée. Toute tentative d'usurpation d'identité à une extrémité ou à une autre de la communication, est difficilement possible puisque chaque paquet est crypté à l'aide d'une clé connue seulement par le système local et le système distant.

II.4.8.Le serveur Slapd

Slapd, est le serveur LDAP de la suite logicielle Openldap. Il répond donc aux requêtes des clients LDAP, quels qu'ils soient, et quelle que soit la librairie LDAP sur laquelle ils sont construits.

Un serveur Slapd est configuré pour n'écouter qu'un seul port, à la différence d'autres serveurs comme Apache. Néanmoins un même serveur Slapd permet de répondre aux requêtes de plusieurs annuaires, c'est à dire d'annuaires qui ont des suffixes différents.

Mais dans ce cas les annuaires servis par une même instance de Slapd, vont partager un certain nombre de caractéristiques (permissions, index,…etc.), ce qui n'est pas toujours souhaitable. Donc si l'on veut qu'une même machine serve plusieurs annuaires, il est parfois nécessaire de faire tourner plusieurs instances du serveur Slapd, chacun écoutant un port différent et chacun ayant son propre fichier de configuration Slapd.conf.

La manière dont sont stockées les données d'un serveur Slapd fait aussi partie des informations de configuration. Le stockage des données est défini par un *backend*. De la même façon qu'une même instance de serveur Slapd peut servir plusieurs annuaires, une même instance de serveur Slapd peut avoir plusieurs *backends*, dans lesquels elle va stocker ses différents annuaires.

Un fichier de configuration d'un serveur Slapd, est logiquement divisé en trois sections :

- Configuration globale.
- Spécifique à un backend.
- Spécifique à un annuaire.

II.4.9.Le serveur Postfix

Postfix, est un serveur de messagerie électronique (MTA), et un logiciel libre, permettant de proposer le service SMTP pour l'envoi des mails par les utilisateurs de la base de données. Il se charge de la livraison de messages électroniques, et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que l'historique Sendmail.

Postfix, est développé par le célèbre spécialiste en sécurité Wietse Venema, et a tout axé sur l'écriture d'un remplaçant performant et sécurisé de Sendmail. Objectif réussi puisque

Postfix est devenu l'une des références, grâce à la qualité du programme et son architecture modulaire.

- **Fonctionnalités**

- Il permet de gérer presque tous les cas d'une utilisation professionnelle, et il remplace idéalement toutes sortes de solutions moins libres.
- Afin d'optimiser l'analyse de courriels, Postfix permet de déléguer la gestion de ceux-ci à un processus externe, qui se chargera de déterminer si le courriel est accepté ou refusé (très utile dans les systèmes anti-pourriel).
- Il est le serveur de courriel par défaut dans plusieurs systèmes de type Unix, comme MacOS X, NetBSD, diverses distributions GNU/Linux,…etc.
- Le MTA est l'agent de transfert des courriers. C'est le cœur du système de messagerie. En tant que MTA, Postfix ne fournit aucune fonctionnalité de récupération des courriers par les utilisateurs, il ne fournit que le protocole SMTP.

II.4.10.Le serveur Cyrus-imap

Cyrus, est un serveur de messagerie électronique (MDA), et un logiciel permettant de proposer le service IMAP, pour la livraison des mails aux utilisateurs de la base de données. Créé dans un objectif de fiabilité et d'extensibilité optimale, utilisé essentiellement pour gérer de très grandes quantités de comptes de courrier électronique.

L'université Carnegie-Mellon a développé, dans les années 1980 pour ses besoins en gestion de courriels, le logiciel AMS (Andrew Mail System) qui s'est révélé décevant en termes de fiabilité et de montée en charge. Cependant, il avait des questions d'extensibilité majeure. Carnegie Mellon voulait déplacer à un système du courrier niveaux-conforme qui a rencontré ou a dépassé le trait mettez d'AMS, et avec une accentuation sur opération hors circuit et extensibilité.

En 1994 la Division des Services de l'Informatique à Carnegie Mellon a adressé ces buts en commençant le Projet Cyrus. En 1998 (classe de 2002), Carnegie Mellon a placé tous ses étudiants de première année nouveaux sur le serveur Cyrus pour la première fois. En décembre 2001, lequel avait été reflété d'AMS à Cyrus, complètement coupez à Cyrus. AMS a été abandonné finalement en mai 2002 progressivement.

- **Fonctionnalités**

- Cyrus est un logiciel libre distribué sous Carnegie Mellon University License.
- Cyrus, répondant aux besoins des grands fournisseurs de services de courriel, est fréquemment utilisé par les fournisseurs de services internet et les universités.
- Cyrus permet de consulter ses emails par POP3, KPOP, IMAP et NNTP, et met en œuvre le langage normalisé Sieve.
- Cyrus est conçu pour être utilisé sur un serveur ou les utilisateurs n'ont pas le droit de se connecter. Cyrus semble aussi être parmi les deux plus populaires serveurs IMAP pour Unix. L'autre est le serveur IMAP de l'Université de Washington.
- Les messages sont stockés chacun dans un fichier séparé, rangés dans un répertoire par utilisateur.
- Les utilisateurs peuvent être enregistrés dans une base de données, un annuaire LDAP et n'ont absolument pas besoin de disposer d'un compte Unix sur la machine serveur.
- Ce serveur est plus souple, plus sûr, offre plus de possibilités et, bien entendu, est beaucoup plus difficile à installer et à configurer.

II.4.11.Le serveur SOGO

SOGO, est un serveur collaboratif libre dont l'architecture est axée sur l'extensibilité (en anglais : « scalability »), qui permet son utilisation simultanée par des dizaines de milliers d'utilisateurs. C'est un cousin d'OpenGroupware.Org (OGO) qui, comme lui, est fondé sur le Skyrix Object Publishing Environment (SOPE). Permet de fournir aux utilisateurs une interface Web conviviale pour gérer leur messagerie.

Le projet SOGO a été initié en 2004 par la société Skyrix, établie en Allemagne. Cette même société est à l'origine du projet OpenGroupware.Org (OGO). Une entreprise montréalaise, a repris le développement depuis 2006 et le poursuit encore aujourd'hui. SOGO est un logiciel libre, distribué sous Licence publique générale GNU.

- **Fonctionnalités**

SOGO possède l'essentiel des fonctionnalités qu'on peut attendre d'un environnement collaboratif. Les modules disponibles ont été choisis en fonction de leur utilité et de leur utilisation de ressources machine et réseau. Son nombre de composantes est donc limité à la gestion de calendriers, de carnet d'adresses et de courrier électronique. Sa philosophie d'intégration tend à éviter la duplication de fonctionnalités lorsque des services adéquats

existent déjà. D'autre part, SOGO est modulaire et permet d'ajouter facilement les fonctionnalités dont le manque se ferait sentir. Un parc-type peut donc utiliser SOGO à côté d'un serveur de fichiers pour le partage de documents, ou d'un serveur jabber pour la messagerie instantanée.

En implémentant des protocoles et des formats de données standardisés, SOGO facilite aussi l'interopérabilité entre différents logiciels ou appareils mobiles. En l'occurrence, SOGO conserve les fiches des carnets d'adresses au format vCard, tandis que les événements et les tâches des calendriers sont au format iCalendar,…etc. Bien que l'utilisation de Thunderbird soit privilégiée, aucun client particulier n'est imposé.

Côté serveur, l'un de ses aspects le plus intéressant est sans doute son intégration à toute infrastructure préexistante. Plutôt que d'imposer une refonte de l'organigramme des services réseau, SOGO est capable d'utiliser virtuellement toute base de données SQL existante ainsi que n'importe quel serveur IMAP. L'identification des utilisateurs se fait en LDAP ou en CAS.

- **Connectivité**

SOGO propose à priori trois modes d'accès à l'utilisateur :

- une interface Web, basée sur AJAX, dont l'aspect et les fonctionnalités se rapprochent de celles offertes par la suite d'applications Mozilla : Thunderbird/Lightning et Sunbird. Ce choix permet à l'utilisateur de bénéficier de nombreuses fonctionnalités au travers d'interfaces cohérentes, simples et rapides. Cette fluidité va en réalité de pair avec la légèreté des requêtes effectuées auprès du serveur et de ses services connexes.
- une interface GroupDAV, CardDAV et CalDAV qui permettent à l'utilisateur d'avoir accès à ses informations via un "client lourd" de son choix, pour autant qu'il supporte ces protocoles.
- la synchronisation des données avec un assistant personnel ou un téléphone mobile par le biais de l'intergiciel Funambol.

Depuis peu, le développement d'un composant SOGO pour le « middleware » OpenChange, permet aux clients Outlook de se connecter à SOGO sans nécessiter de plugin côté client.

- **Partage d'information**

Comme logiciel collaboratif, SOGO permet le partage d'informations entre utilisateurs et par conséquent de contrôler l'accès aux données. Ainsi, un utilisateur peut définir des droits d'accès sur ses ressources avec une certaine finesse. Chaque module fournit son propre ensemble de droits applicables. Par exemple, les « ACL » IMAP sont gérés en conformité avec le RFC 4314.

II.5.Les ports associés aux quelque protocoles

Un port est un numéro associé à un service ou une application réseau. La fonction du port est de déterminer à quel programme la communication est destinée.

De nombreux programmes peuvent être exécutés simultanément sur internet (on peut par exemple naviguer sue des pages web toute en consultant une messagerie électronique). Chacun de ses programmes travaille avec un protocole de communication, toute fois l'ordinateur doit pouvoir distinguer les différentes sources de données.

Ainsi, pour faciliter ce processus, chacune de ces applications se voit attribuer une adresse sur la machine, codée sur 16 bits : la combinaison adresse IP + port de communication et alors une adresse unique au monde, il est appelée socket.

L'adresse IP sert donc à identifier de façon unique un ordinateur sur le réseau local ou sur le réseau internet tandis que le numéro de port indique l'application à laquelle les données sont destinées. De cette manière, lorsque l'ordinateur reçoit des informations destinées à un port de communication, les données sont envoyées vers l'application correspondante. Le tableau suivant montre les ports des protocoles de messagerie.

Protocole (application)	port
TELNET	23
SMTP	25
IMAP	143
POP3	110

Tableau II.6 : Les ports liés à la messagerie électronique.

II.6.Discussion

Nous avons présenté une multitude des serveurs et protocoles, intervenant dans les communications entre les différents agents du service de messagerie. Les e-mails utilisent plusieurs types des serveurs et protocoles, ayant chacun des modes de fonctionnement particuliers.

Dans le prochain chapitre, nous allons mettre en pratique les installations et configurations requises, pour réaliser un système de messagerie interne.

III.1.Préambule

Afin de garantir la réussite et l'efficacité de notre projet, il est recommandé de définir la solution à mettre en place.

Dans ce chapitre, nous présentons l'environnement de l'application, avec un test final qui consiste à créer deux boites mails, envoyer et recevoir des courriers.

III.2.Descriptifs de systèmes à mettre en place

Nous avons réalisé une plate-forme basique d'un système de messagerie interne, on a pris comme exemple notre Université Mouloud Mammeri, Tizi-Oouzou (Bastos).

III.2.1.Présentation du matériel utilisé

- **Un PC portable**

Sur un PC portable, on a installé un système d'exploitation Ubuntu, VirtualBox et les machines Debians, et familiariser avec l'environnement Linux, le Shell et l'éditeur de texte nano ou vi.

- **VirtualBox**

Oracle VM VirtualBox, est un logiciel de virtualisation créé par InnoTek et publié par Oracle Corporation. Ce logiciel permet de créer des machines virtuelles et d'installer sur chacune un système invité, indépendant du système hôte. Vous pourrez donc, par exemple, travailler sous Linux (votre système d'exploitation principal, le système hôte), tout en utilisant une machine virtuelle sous Linux ou Windows (système invité), sous la forme d'une fenêtre.

Et pour objectif :

- de diminuer le nombre de machines physique, ce qui entraine une réduction d'énergie, d'espace et de temps de maintenance.
- de construire des réseaux complexes, développer, tester et déployer de nouvelles applications sur une seule et même machine sans impact sur celle-ci.
- d'effectuer des solutions efficaces pour les tests d'intrusions et failles en sécurité informatique.
- de prendre en charge des applications existantes tout en assurant une migration sécurisée vers un nouveau système d'exploitation.

- de tester les nouveaux systèmes d'exploitation dans des machines virtuelles sécurisées avant tout déploiement.

III.2.2.Présentation de l'architecteur

Le schéma suivant représente l'architecture réseau de la plate-forme de test, de la messagerie interne.

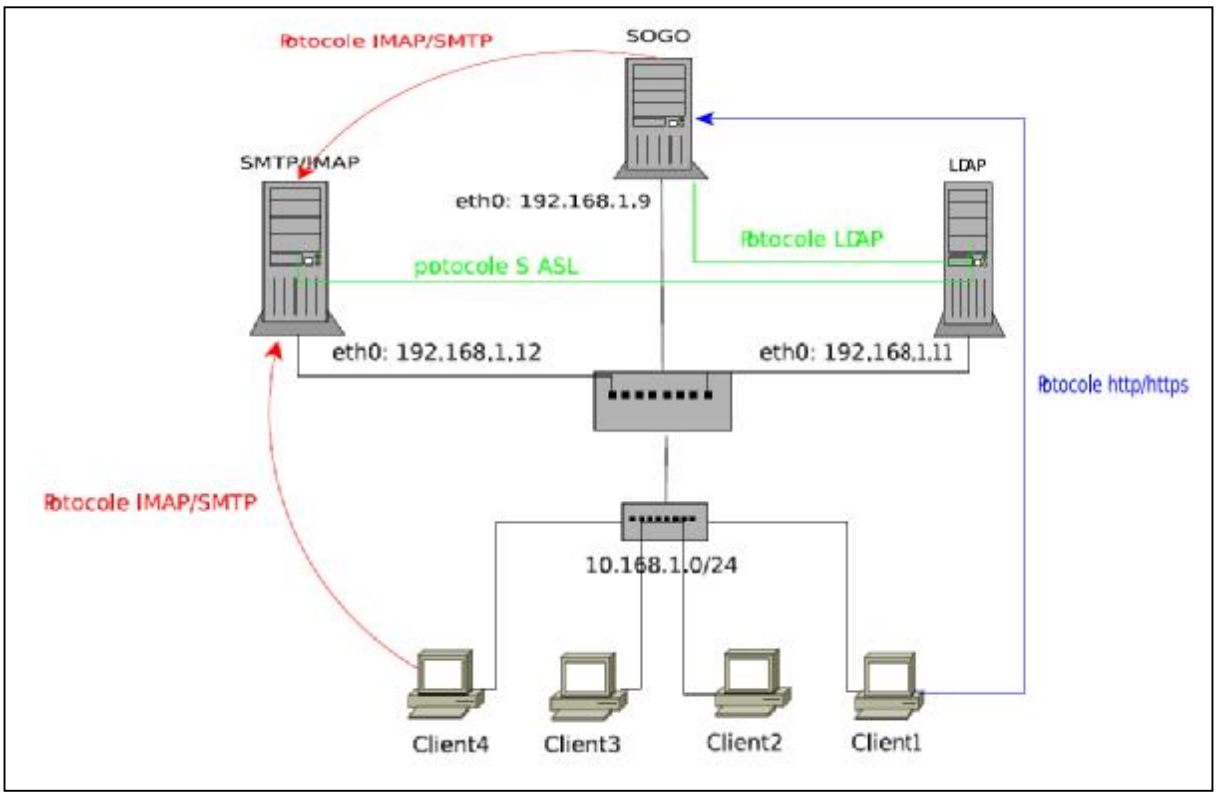


Figure III.1 : La plate-forme de test de la messagerie interne.

La plate-forme de la messagerie, est mise en place sous des systèmes GNU/Linux (Debian), installés sur des machines virtuelles :

- SOGO : serveur SOGO.
- LDAP : serveur LDAP.
- SMTP/IMAP: serveur SMTPIMAP.

III.3.Installation de VirtualBox et création des machines virtuelles

III.3.1.Installation de VirtualBox

Sur une machine Ubuntu, on va installer l'outil de virtualisation VirtualBox. On ouvre le terminal en mode root, et on installe les paquets suivants :

virtualbox virtualbox-dkms virtualbox-qt, en tapant la commande suivante :

```
aptitude install virtualbox virtualbox-dkms virtualbox-qt
```

III.3.2.Création des machines virtuelles

- **Lancez l'application VirtualBox :** Pour lancer VirtualBox, il faut double cliquez sur l'icône :

Et on aura la fenêtre suivante :

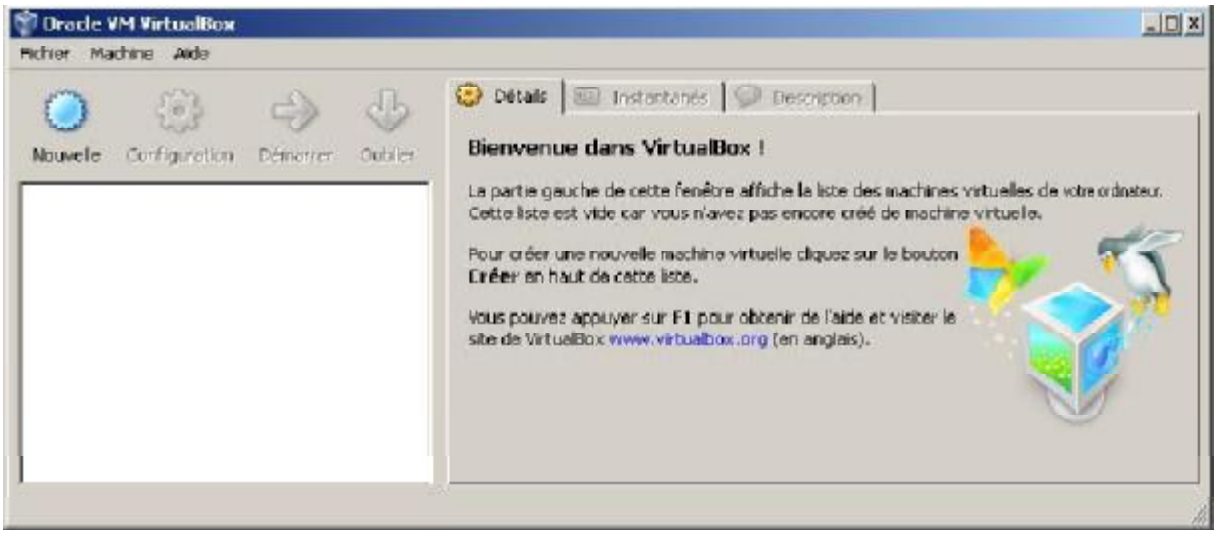


Figure III.2 : Oracle VM VirtualBox.

- **Création d'une machine virtuelle :** Pour Crée une machine virtuelle, il faut cliquez sur l'onglet supérieur de VirtualBox :

L'assistant de création se lance, alors on aura la fenêtre suivante :

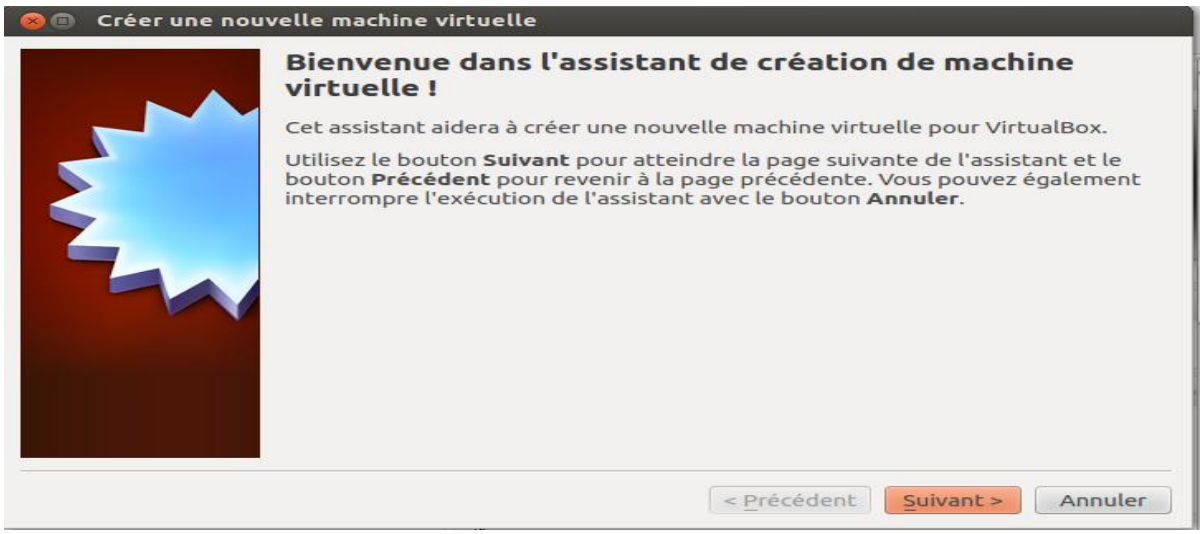


Figure III.3 : L'assistant de création de machine virtuelle.

On clique sur « Suivant » :

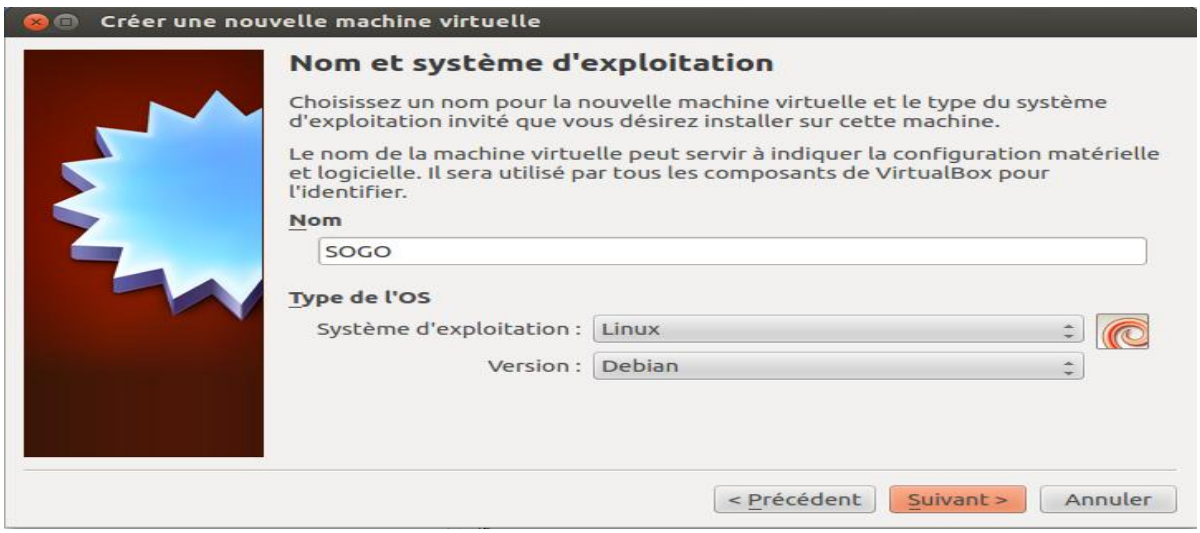


Figure III.4 : Nom et type de système d'exploitation.

La première étape permet de spécifier un nom qui sera attribué à la machine virtuelle. On saisit le nom de notre machine (dans notre cas on nomme SOGO), et par la suite on définit le type et la version de système d'exploitation, que l'on installera.

On clique sur « Suivant » :

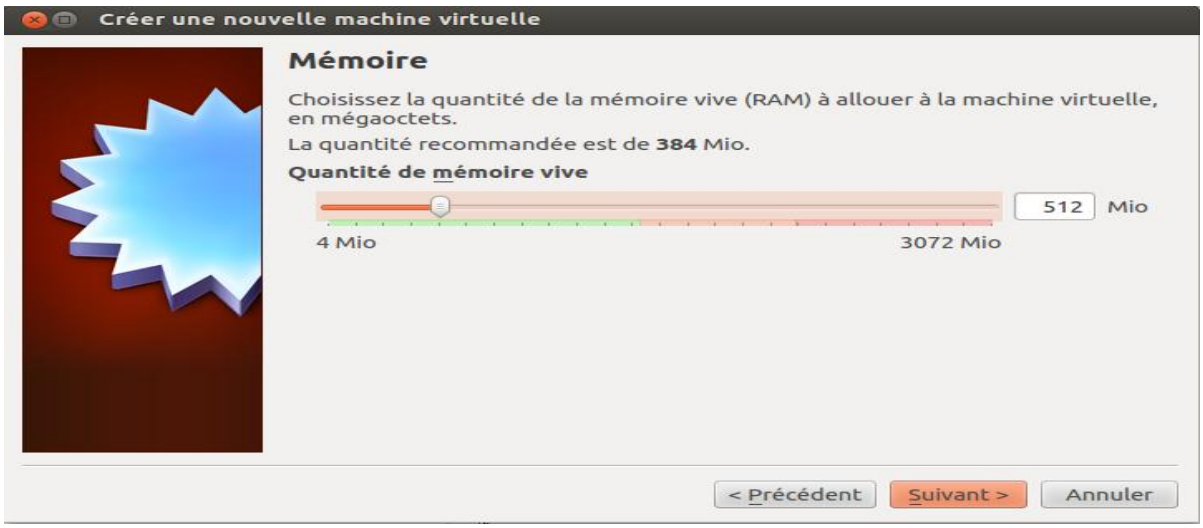


Figure III.5 : Quantité de mémoire vive.

La seconde étape permet de déterminer quelle quantité de mémoire sera attribuée à la machine virtuelle, (VirtualBox recommande des tailles de mémoire vive à allouer en fonction de choix du système à installer).

On va définir 512 Mo de mémoire vive, et on clique sur « Suivant » :

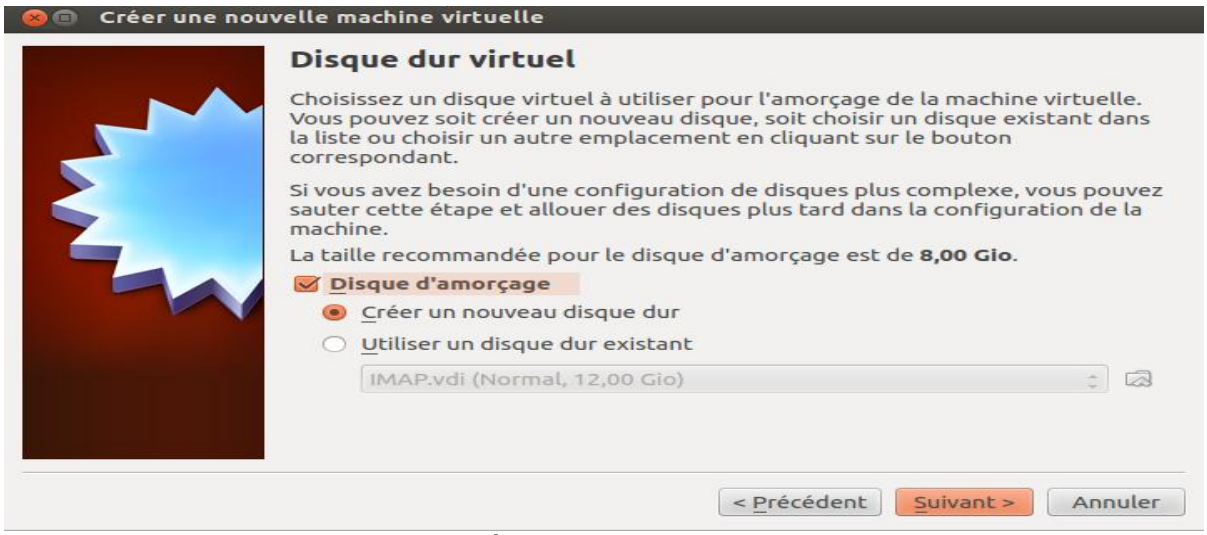


Figure III.6 : Création d'un disque dur d'amorçage.

La troisième étape, création d'un disque d'amorçage pour notre machine virtuelle. C'est sur ce disque virtuel qu'on installe par la suite notre système d'exploitation.

On clique sur « Suivant » :

Figure III.7 : Création d'un disque virtuel.

On choisit le type de fichier de disque, et on clique sur « Suivant » :

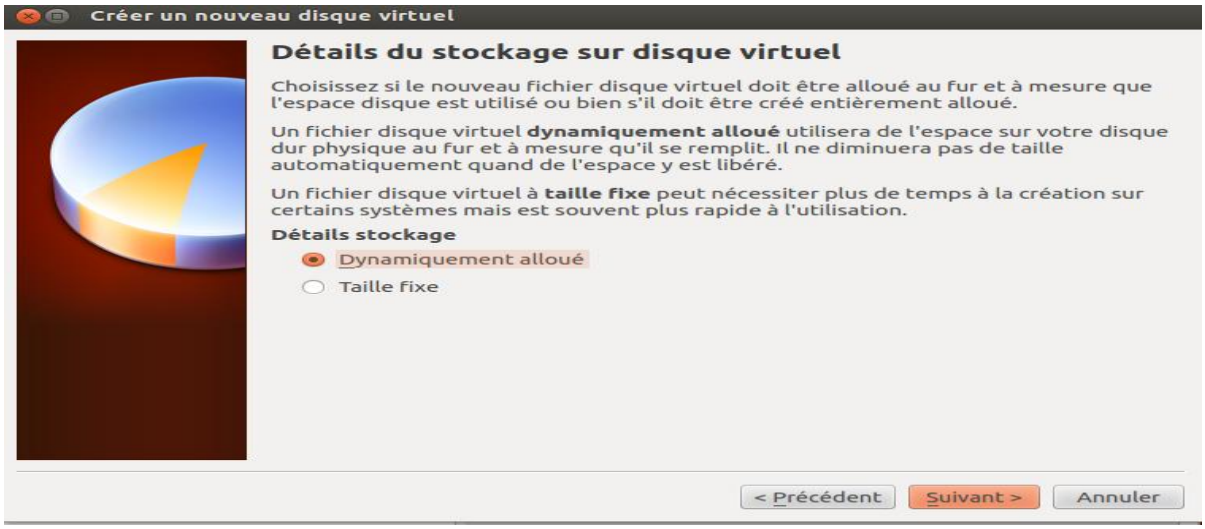


Figure III.8 : Type de disque virtuel.

D'après la nouvelle fenêtre qui apparaît, on a la possibilité de choisir entre deux types de disques virtuels :

- Dynamiquement alloué : la taille allouée à votre machine virtuelle n'est pas définie à l'avance, mais s'adaptera automatiquement à vos besoins.
- Taille fixe : la taille du disque virtuel est fixée dès le départ.

On choisit le type de disque Dynamiquement alloué, afin de ne pas gaspiller inutilement de l'espace disque, et on clique sur « Suivant » :

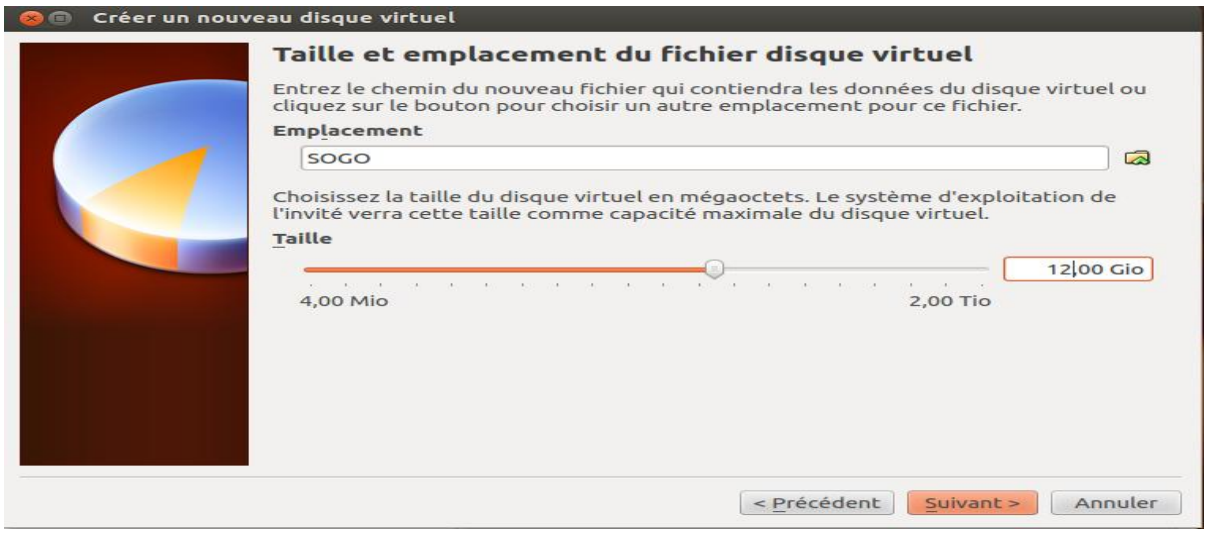


Figure III.9 : Taille et emplacement du fichier disque virtuel.

Puis on paramètre la dimension de notre disque virtuel. On va paramétrer la taille de disque à 12 Go, et on clique sur « Suivant » :

Figure III.10 : Réglage de disque virtuel.

Cette étape récapitule simplement les réglages de notre disque virtuel. Et on clique sur « Créer » afin de le créer :

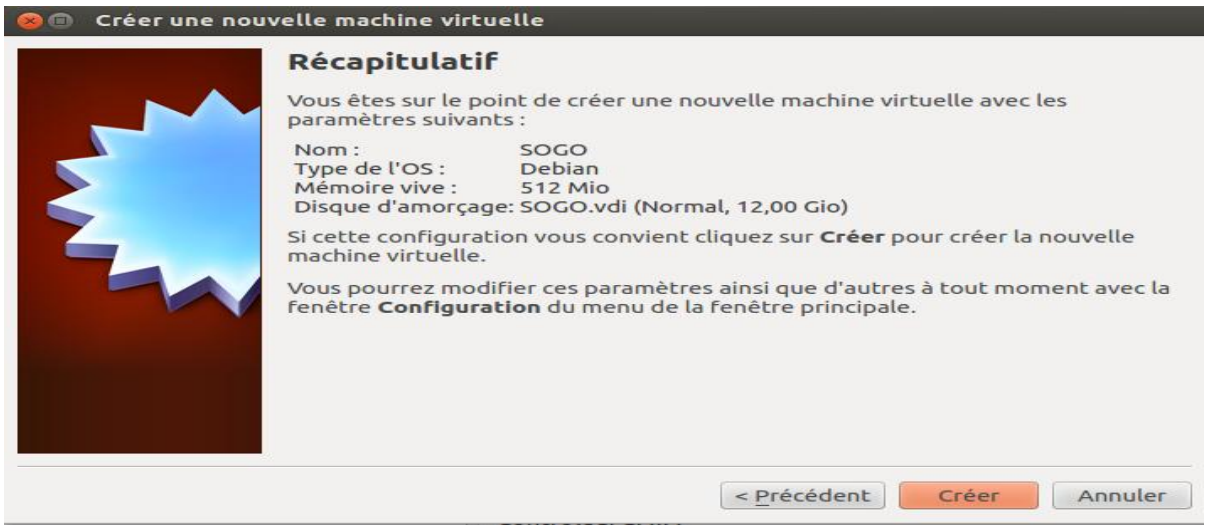


Figure III.11 : Récapitulative des caractéristiques de la machine virtuelle.

Une dernière fenêtre récapitulative apparaît. On clique sur « Créer » :

Donc la fenêtre initiale de VirtualBox, réapparaît avec le nom de la nouvelle machine virtuel.

III.3.3.Configuration de la machine virtuelle sur VirtualBox

On sélectionne la machine virtuelle dans VirtualBox, et on clique sur l'onglet :

On clique sur l'icone « Stockage », pour configurer le contrôleur IDE de notre machine.

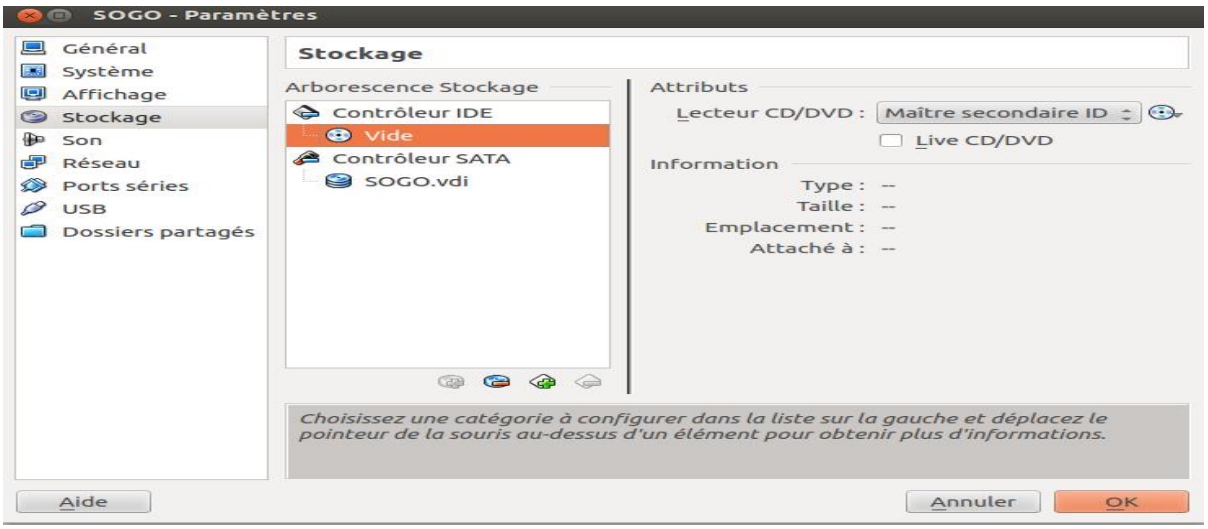


Figure III.12 : Configuration de contrôleur IDE de la machine.

On choisit l'icône du CDROM « Vide ».

Ensuite on clique sur l'icône représentant un CDROM dans le champ « Attributs », pour choisir un disque secondaire IDE sous forme de fichier ou de disque amovible.

Ensuite on clique sur « Choisissez un fichier CD/DVD virtuelle », et renseigne notre système d'exploitation en format ISO.

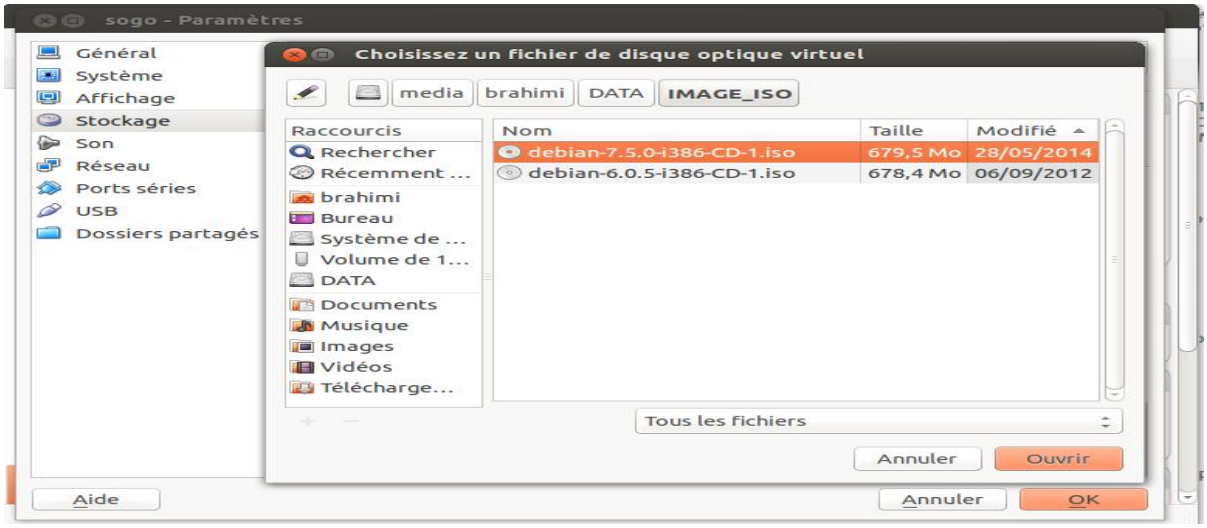


Figure III.13 : Le fichier de disque optique virtuel.

Dans notre cas on choisit le système **debian-7.5.0-i386-CD-1.iso**, et on clique sur « Ouvrir » :

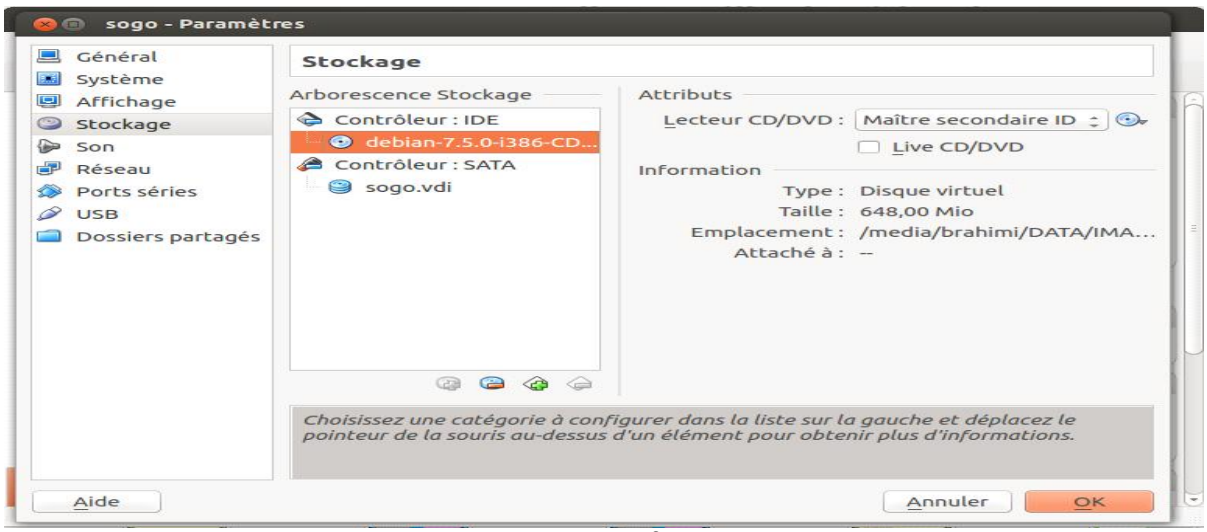


Figure III.14 : Le fichier ISO.

Notre fichier ISO est bien pris en compte. Ensuite on clique sur « OK ».

III.3.4.Installation du système d'exploitation sur une machine virtuelle

Cette étape consiste à démarrer la machine virtuelle, pour installer le système Debian, qu'on a renseigné dans les étapes précédentes.

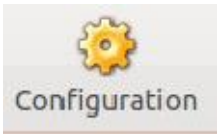
On sélectionne la machine virtuelle dans VirtualBox, et on clique sur l'onglet :

Et on suivre les étapes de l'installation.

Enfin, un système Debian de base est installé sur la machine SOGO, on va cloner cette machine pour créer une machine (SMTPIMAP), et une machine LDAP.

III.3.5.Paramétrage de mode d'accès réseau des machines virtuelles

On sélectionne une machine virtuelle dans VirtualBox, et on clique sur l'onglet :



On clique sur l'icone « Réseau » en mode Pont, pour configurer le réseau de notre machine.

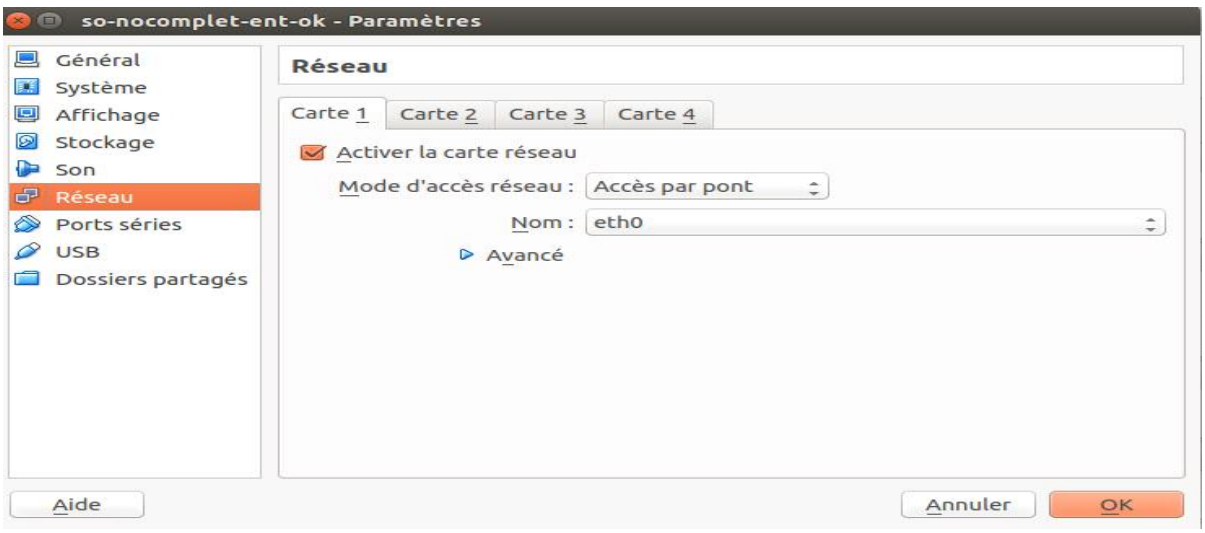


Figure III.15 : Configuration réseau de la machine.

Et on clique sur « OK ».

III.3.6.Configuration réseau des machines virtuelles

On édite le fichier /etc/network/interfaces avec la commande nano**,** pour configurer le réseau.

- **Serveur SOGO**

```
root@SOGO:~# nano  /etc/network/interfaces
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 192.168.1.9
    netmask 255.255.0.0
    gateway  192.168.0.254
```

- **Serveur LDAP**

```
root@LDAP:~# nano  /etc/network/interfaces
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 192.168.1.11
    netmask 255.255.0.0
    gateway  192.168.0.254
```

- **Serveur SMTPIMAP**

```
root@SMTPIMAP:~# nano  /etc/network/interfaces
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet static
    address 192.168.1.12
    netmask 255.255.0.0
    gateway  192.168.0.254
```

Après avoir renseigné ce fichier sur chaque machine, on relance le service réseau, en exécutant le script /etc/init.d/networking en mode sudo comme on le montre dans la commande suivante :

```
#/etc/init.d/networking  restart
```

Ensuite on teste l'interconnexion entre les trois machines avec la commande ping.

Après avoir validé la configuration réseau, on va attaquer le serveur LDAP.

III.4.Le serveur LDAP

III.4.1.Configuration des fichiers /etc/hosts de la machine LDAP

```
127.0.0.1          localhost
127.0.1.1          ldap.bastos.dz ldap
192.168.1.11    ldap.bastos.dz ldap
192.168.1.12    smtpimap.bastos.dz smtpimap
192.168.1.9     sogo.bastos.dz sogo
```

III.4.2.Installation de serveur OpenLDAP

Mise à jour dépôt et installation du serveur OpenLDAP (slapd) avec les commandes suivantes :

```
root@LDAP:~#apt-get update

root@LDAP~# apt-get install slapd ldap-utils
```

III.4.3.Configuration de serveur OpenLDAP

Pour configurer le serveur OpenLDAP, on exécute les commandes suivantes :

```
root@LDAP:~# /etc/init.d/slapd stop

root@LDAP:~# rm -f /var/lib/ldap/*

root@LDAP:~# dpkg-reconfigure slapd
```

Et on répond aux questions posées par le système :

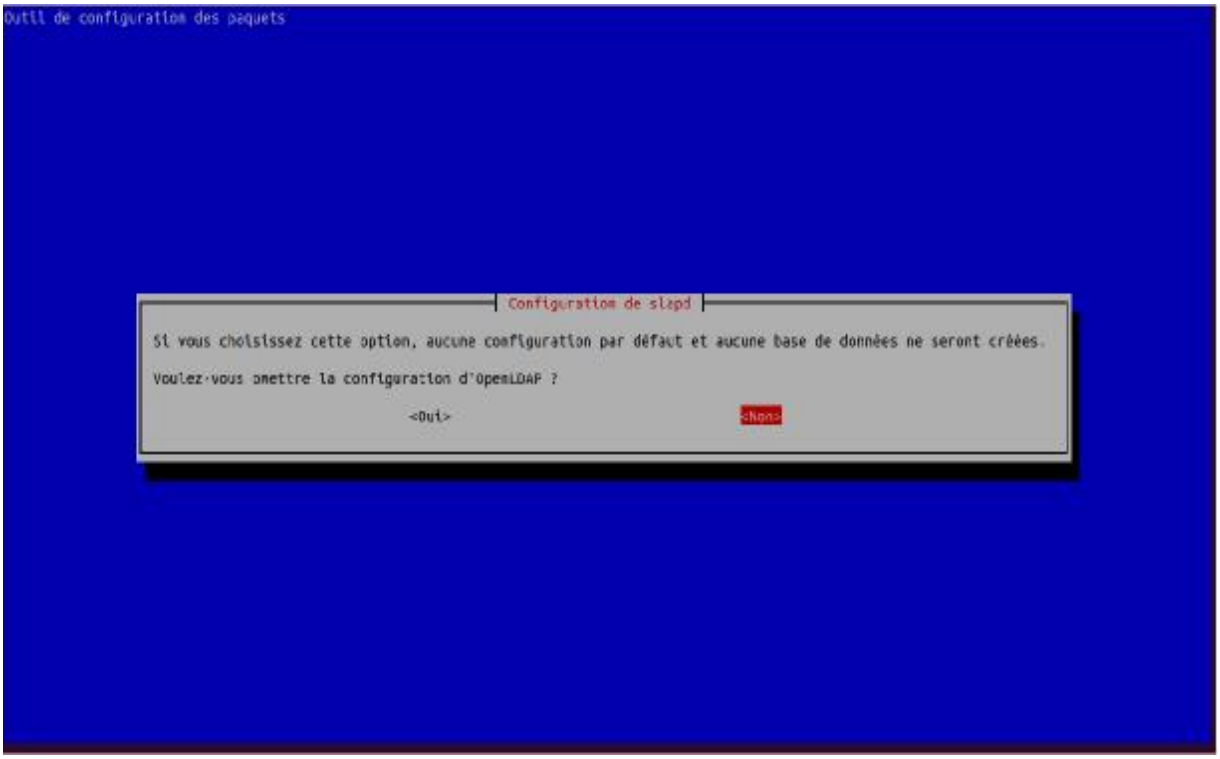


Figure III.16 : Configuration de serveur OpenLDAP.

Pour ne pas omettre la configuration de serveur OpenLDAP, On clique sur « Non »:

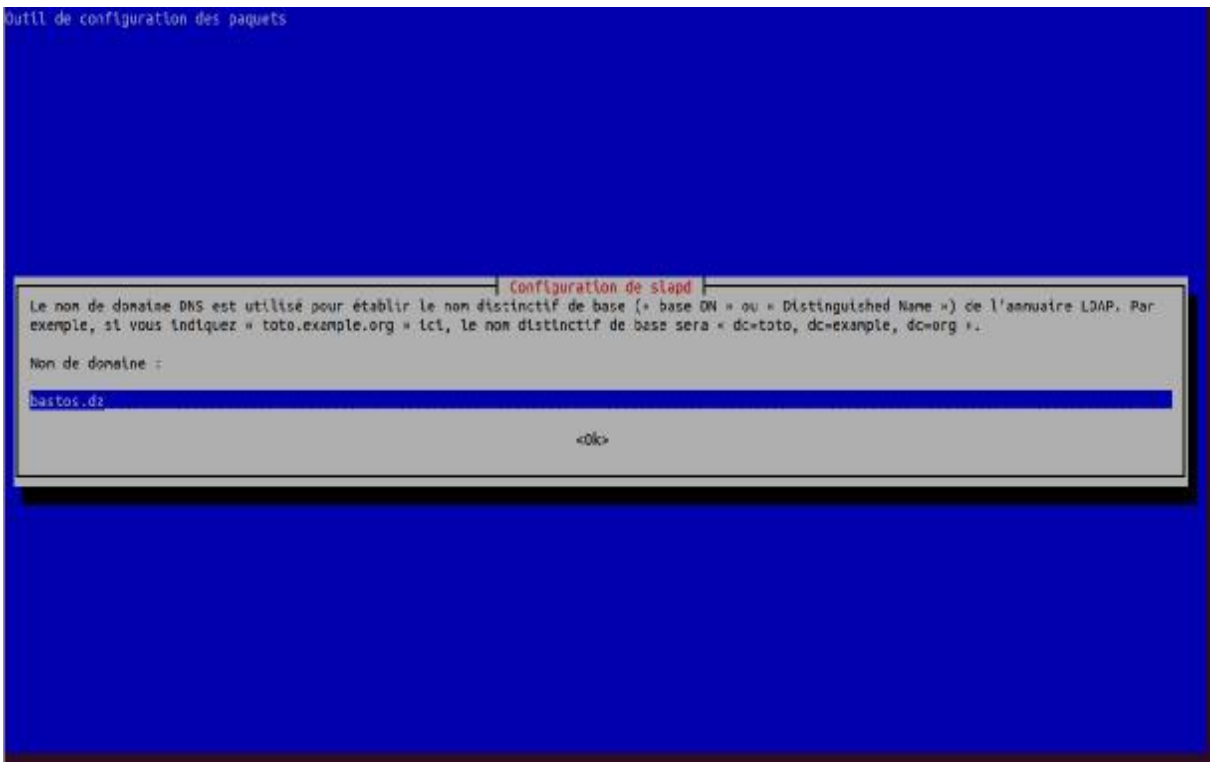


Figure III.17 : Nom de domaine.

On saisit le nom de domaine (bastos.dz), et on clique sur « OK » :

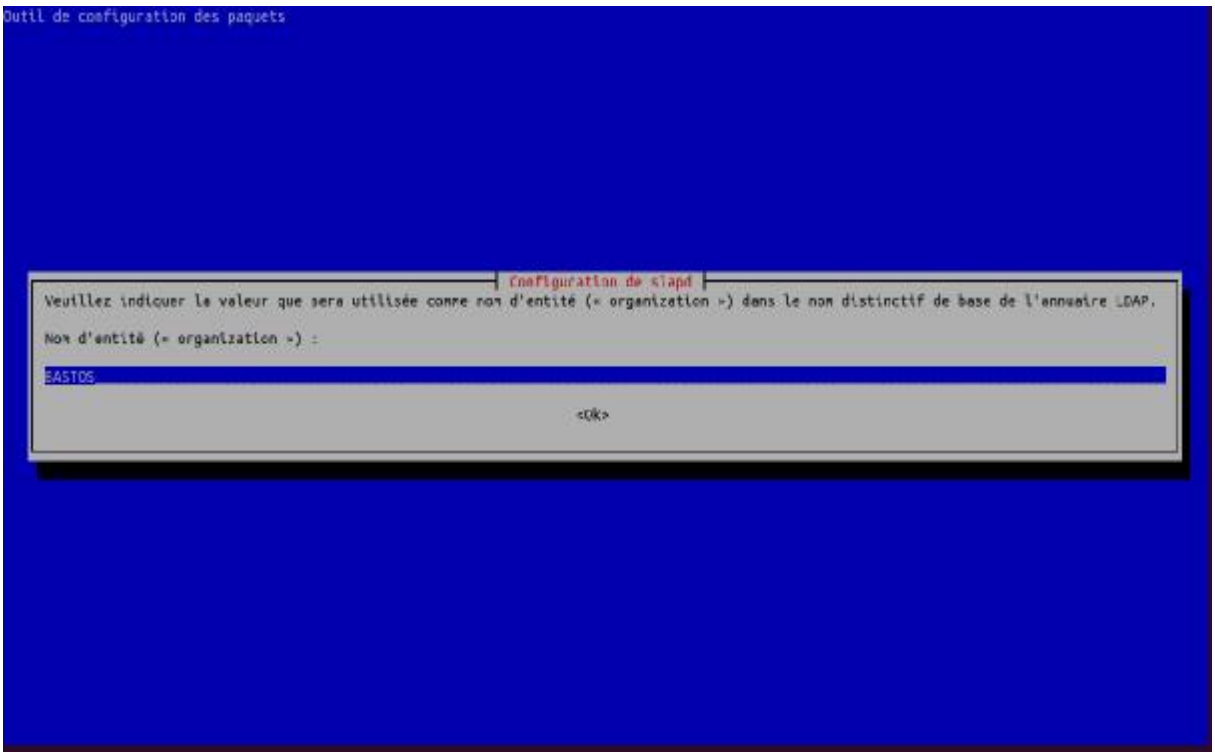


Figure III.18 : Nom d'organisation.

On saisit le nom d'organisation (BASTOS), et on clique sur « OK » :

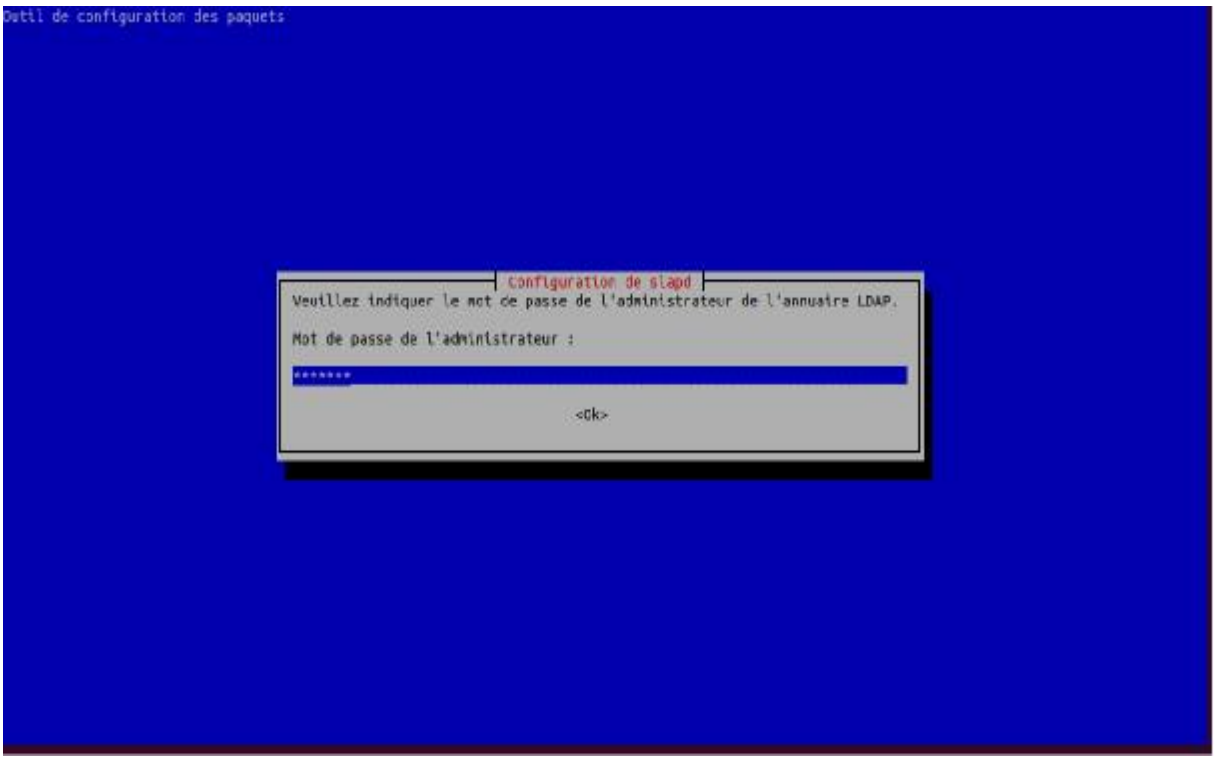


Figure III.19 : Mot de passe de l'administrateur.

On saisit le mot de passe de l'administrateur, et on clique sur « OK » :

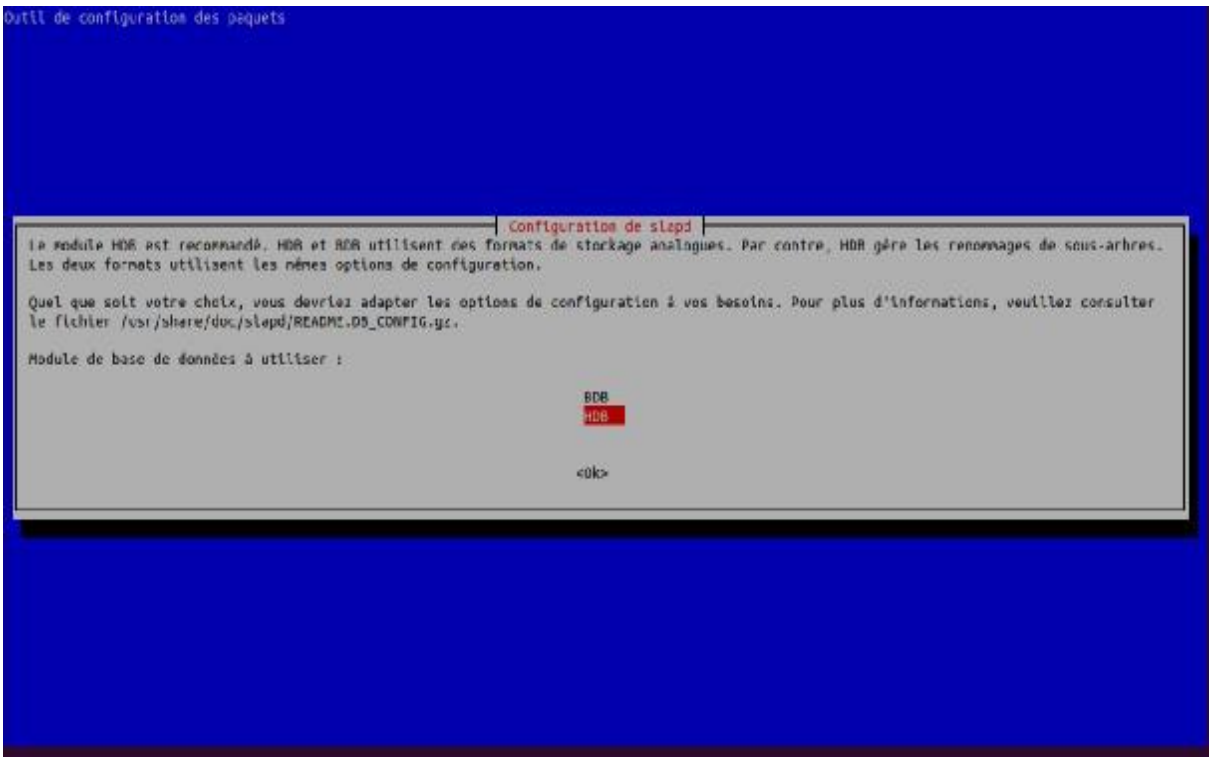


Figure III.20 : Module de base de données à utiliser.

On choisit le module HDB (recommandé), et on clique sur « OK » :

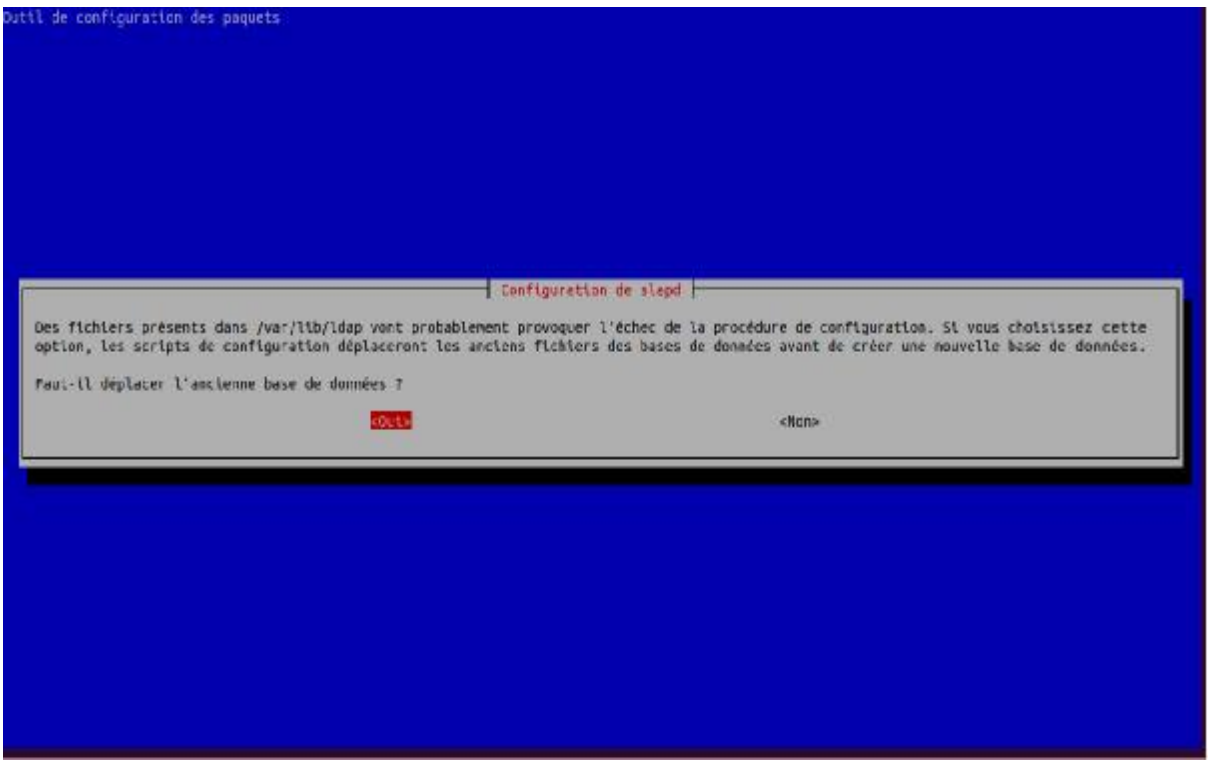


Figure III.21 : Déplacement de l'ancienne base de données.

Avant de créer une nouvelle base de données, on autorise le déplacement de l'ancienne base de données, en cliquant sur « Oui » :

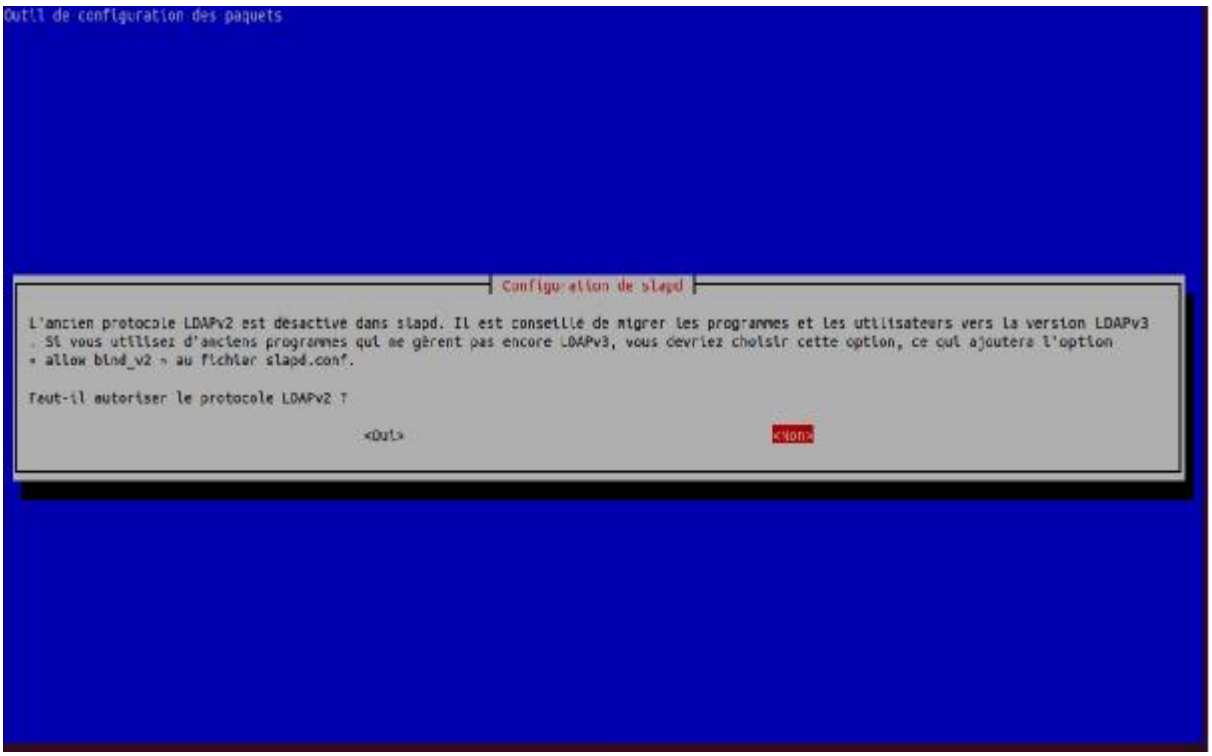


Figure III.22 : Autorisation de protocole LDAPv2.

On désactive le protocole LDAPv2, et on clique sur « Oui ».

III.4.4.Administrer le serveur LDAP avec phpLDAPadmin

III.4.4.1.Installation de phpLDAPadmin

L'installation de phpLDAPadmin require l'installation des paquets suivants : apache2 php5 php5-mysql.

```
root@LDAP:~# apt-get install apache2 php5 php5-mysql
```

Ensuite on installe phpLDAPadmin avec la commande :

```
root@LDAP:~# apt-get install phpldapadmin
```

III.4.4.2.Configuration de phpLDAPadmin

La configuration de phpLDAPadmin se fait au niveau de fichier /etc/phpldapadmin/config.php.

L’accès à l'interface phpLDAPadmin se fait à travers l'url suivante :

http://ldap.bastos.dz/phpldapadmin/

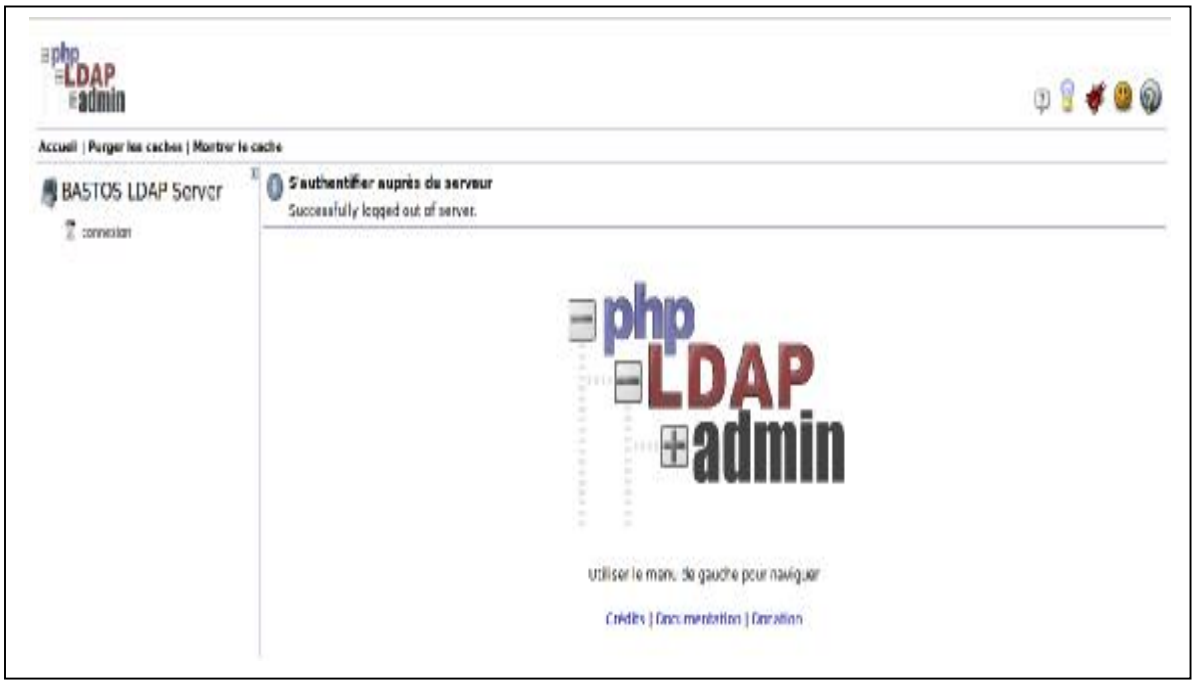


Figure III.23 : L'interface phpLDAPadmin.

Figure III.24 : Authentification de serveur LDAP.

Figure III.25 : Connexion au serveur BASTOS LDAP.

Création d'un objet de type (Générique : Unité Organisationnelle), qu'on nomme « People » qui va contenir les adresses mails.

Figure III.26 : Création d'une nouvelle unité organisationnelle.

Figure III.27 : Validation de la nouvelle unité organisationnelle.

Pour valider la création de la nouvelle unité organisationnelle « people », on clique sur « Valider ».

Et on procède à la création des sous entrées de l'objet « People », en choisissant le modèle adresse mail :

Figure III.28 : Création d'une entrée de modèle mail.

Figure III.29 : Validation de sous entrée.

Pour valider la création de sous entrée « djouher », on clique sur « Valider ».

Figure III.30 : Création d'une nouvelle sous entrée.

De la même façon, on crée les comptes suivants :

Cyrus pour l'authentification Cyrus-imap, et un compte mail pour dalila.

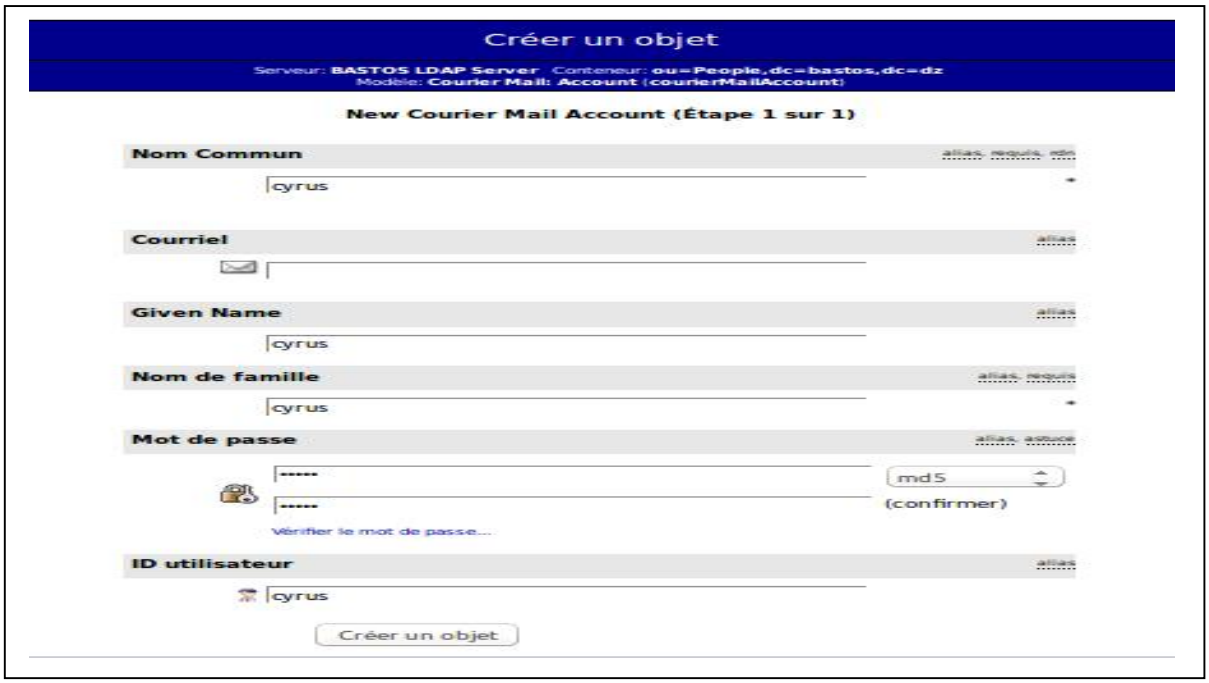


Figure III.31 : Création d'un compte Cyrus.

Figure III.32 : Validation de compte Cyrus.

Pour valider la création de sous entrée « Cyrus », on clique sur « Valider ».

Figure III.33 : L'ensemble des comptes créés.

III.5.Le serveur SMTPIMAP

III.5.1.Configuration de client LDAP

La configuration du client LDAP, se fait au niveau de fichier /etc/ldap/ldap.conf

```
root@SMTPIMAP:~# nano /etc/ldap/ldap.conf
#
# LDAP Defaults
#
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
BASE   ou=People,dc=bastos,dc=dz
URI    ldap://ldap.bastos.dz:389
#SIZELIMIT    12
#TIMELIMIT   15
#DEREF                  never
# TLS certificates (needed for GnuTLS)
TLS_CACERT /etc/ssl/certs/ca-certificates.crt
```

III.5.2.Authentification SASL

Pour mettre en place une authentification SASL, on devrait installer le paquet sasl2-bin:

```
#aptitude install sasl2-bin
```

III.5.3.Configuration de L'authentification SASL

Le fichier /etc/saslauthd.conf (à créer de toute pièce), va permettre à saslauthd d'utiliser l'annuaire LDAP comme base d'utilisateurs et de mot de passe.

```
root@cyrus:~# nano /etc/saslauthd.conf
ldap_servers: ldap://ldap.bastos.dz
ldap_version: 3
LDAP_USE_SASL: no
ldap_auth_method: bind
LDAP_BIND_DN: cn=admin,dc=bastos,dc=dz
# Et le mot de passe
LDAP_BIND_PW: xxxxxx
LDAP_SEARCH_BASE: ou=People,dc=bastos,dc=dz
# Et profondeur (sub / one / base )
LDAP_SCOPE: sub
ldap_filter: uid=%U
ldap_scope: sub
```

Remarque : Ce fichier est créé par défaut en lecture pour tout le monde sous Debian. Il est impératif de changer ses droits pour n'autoriser la lecture qu'à l'utilisateur root.

```
# chmod 600 /etc/saslauthd.conf
```

L'activation de l'authentification SASL et prise en charge ce fichier, se font au niveau de fichier /etc/default/saslauthd.

Activer le démon (START=yes), et spécifier la méthode d'authentification utilisée par saslauthd (LDAP dans notre cas).

```
root@cyrus:~# nano  /etc/default/saslauthd
START=yes
DESC="SASL Authentication Daemon"
NAME="saslauthd"
MECHANISMS="ldap"
PARAMS="-O /etc/saslauthd.conf"
MECH_OPTIONS=""
THREADS=5
OPTIONS="-c -m  /var/run/saslauthd"
```

III.6.Le serveur Cyrus

III.6.1.Installation de serveur Cyrus IMAP

On installe Cyrus IMAP avec la commande suivante :

```
root@SMTPIMAP:~# aptitude install cyrus-admin-2.4 cyrus-common cyrus-common-2.4
cyrus-imapd cyrus-sasl2-dbg  cyrus-sasl2-mit-dbg libcyrus-imap-perl24
Les nouveaux paquets suivants vont être installés :
cyrus-admin-2.4 cyrus-common cyrus-common-2.4 cyrus-imapd-2.4 cyrus-sasl2-dbg
cyrus-sasl2-mit-dbg db4.7-util{a} db4.8-util{a} gawk{a}
imapproxy libcyrus-imap-perl24 libperl5.14{a} libsasl2-modules-gssapi-mit{a}
libsensors4{a} libsigsegv2{a} libsnmp-base{a} libsnmp15{a}
libzephyr4{a}
0 paquets mis à jour, 18 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 18,7 Mo d'archives. Après dépaquetage, 62,3 Mo seront
utilisés.
Voulez-vous continuer ? [Y/n/?] Y
```

III.6.2.Configuration de serveur Cyrus IMAP

La configuration se fait au niveau de fichier imapd.conf.

```
root@SMTPIMAP:~#nano  /etc/imapd.conf
configdirectory: /var/lib/cyrus
proc_path: /var/run/cyrus/proc
mboxname_lockpath: /run/cyrus/lock
defaultpartition: default
partition-default: /var/spool/cyrus/mail
partition-news: /var/spool/cyrus/news
newsspool: /var/spool/news
altnamespace: no
unixhierarchysep: no
lmtp_downcase_rcpt: yes
admins: cyrus
allowanonymouslogin: no
popminpoll: 1
autocreatequota: 0
umask: 077
sieveusehomedir: false
sievedir: /var/spool/sieve
hashimapspool: true
```

```
allowplaintext: yes
sasl_mech_list: PLAIN
sasl_pwcheck_method: saslauthd
sasl_auto_transition: no
tls_ca_path: /etc/ssl/certs
tls_session_timeout: 1440
tls_cipher_list: TLSv1+HIGH:!aNULL:@STRENGTH
lmtpsocket: /var/run/cyrus/socket/lmtp
idlesocket: /var/run/cyrus/socket/idle
notifysocket: /var/run/cyrus/socket/notify
syslog_prefix: cyrus
```

Avec :

- **admins : Cyrus** (Nom de l'administrateur du serveur imapd… Si ! C'est bien l'utilisateur Cyrus que nous avons inséré dans l'annuaire).
- **sasl_pwcheck_method : saslauthd** (à modifier pour préciser la méthode de gestion des mots de passe).

Et on redémarrer le serveur :

```
root@SMTPIMAP:~#/etc/init.d/cyrus-imapd restart
```

Création des comptes IMAP :

```
root@SMTPIMAP:/run/cyrus# cyradm -u cyrus localhost
Password: (mot de passe = cyrus)
localhost>
localhost> cm user.djouher
localhost> cm user.dalila
localhost> lm
user.dalila (\HasNoChildren)   user.djouher (\HasNoChildren)
localhost>
```

III.7.Le serveur Postfix

III.7.1.Installation de serveur Postfix

On installe Postfix et le client postfix-ldap, avec la commande suivante :

```
#aptitude install postfix  postfix-ldap
```

```
Les nouveaux paquetts suivants vont être installés :
postfix{b} postfix-ldap ssl-cert{a}
0 paquets mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de télécharger 1 830 ko d'archives. Après dépaquetage, 3 704 ko seront utilisés.
Les paquets suivants ont des dépendances non satisfaites :
exim4-config : Est en conflit avec: postfix mais 2.9.6-2 doit être installé.
 postfix : Est en conflit avec: mail-transport-agent qui est un paquet virtuel
exim4-daemon-light : Est en conflit avec: mail-transport-agent qui est un paquet virtuel
          Les actions suivantes permettront de résoudre ces dépendances :
Supprimer les paquets suivants :
1)     exim4
2)     exim4-base
3)     exim4-config
4)     exim4-daemon-light
Accepter cette solution ? [Y/n/q/?] Y
```

III.7.2.Configuration de serveur Postfix

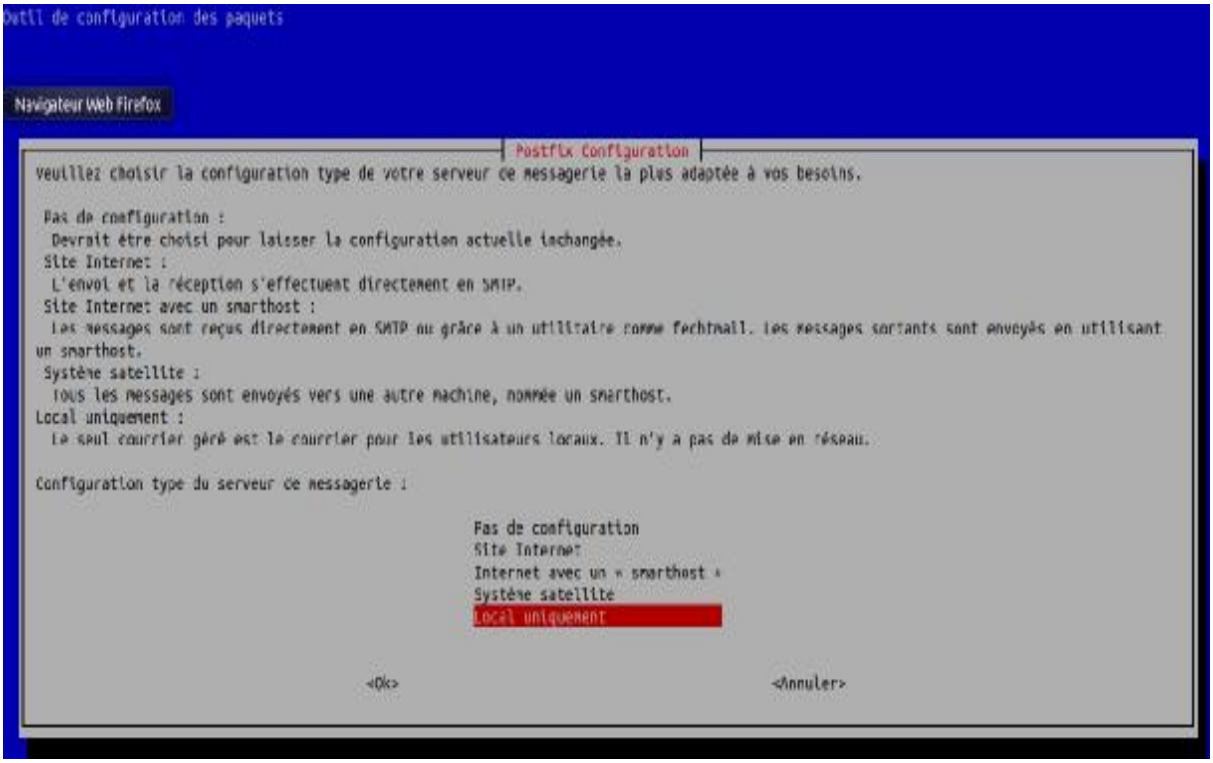


Figure III.34 : Le choix de type du serveur de messagerie.

On choisit le type de configuration local uniquement (le seul courrier géré est le courrier pour les utilisateurs locaux, il n'y a pas de mise en réseau), et on clique sur « OK » :

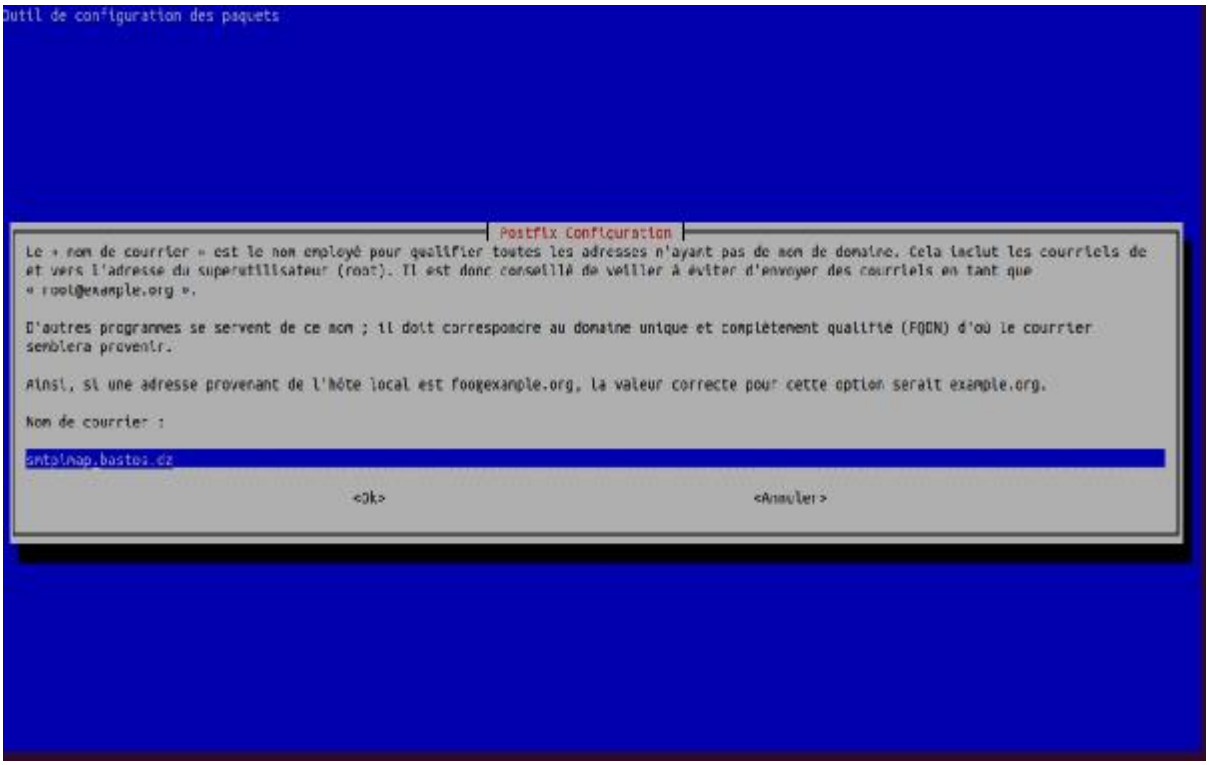


Figure III.35 : Nom de courrier.

On saisit le nom de courrier pour qualifier toutes les adresses n'ayant pas de nom de domaine, et on clique sur « OK ».

La configuration de fichier /etc/postfix/master.cf :

```
root@SMTPIMAP:~# nano  /etc/postfix/master.cf | egrep -v '(^#|^$)'
smtp      inet  n       -       n       -       -       smtpd
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       -       -       -       smtp
relay     unix  -       -       -       -       -       smtp
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
retry     unix  -       -       -       -       -       error
discard   unix  -       -       -       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
cyrus     unix  -       n       n       -       -       pipe
  flags=R user=cyrus argv=/cyrus/bin/deliver -e -m ${extension} ${user}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix  -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user}
${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
```

La suite de la configuration se passe dans le fichier principal de Postfix /etc/postfix/main.cf :

```
root@SMTPIMAP:~# nano  /etc/postfix/main.cf | egrep -v '(^#|^$)'
myorigin = /etc/mailname
mydomain = bastos.dz
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
append_dot_mydomain = no
readme_directory = no
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
myhostname = smtpimap.bastos.dz
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
virtual_mailbox_maps = ldap:/etc/postfix/ldap-accounts.cf
virtual_alias_maps = ldap:/etc/postfix/ldap-aliases.cf
mydestination = localhost, $myhostname, $mydomain
relayhost =
local_recipient_maps =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128  192.168.0.0/16
mailbox_command = procmail -a "$EXTENSION"
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
default_transport = smtp
relay_transport = smtp
mailbox_transport = lmtp:unix:/var/run/cyrus/socket/lmtp
inet_protocols = ipv4
smtpd_recipient_restrictions = reject_unauth_pipelining,
                               reject_non_fqdn_recipient,
                               reject_unauth_destination,
                               permit_mynetworks,
                               permit_sasl_authenticated
smtpd_sender_restrictions =  reject_non_fqdn_sender,
                              reject_unknown_sender_domain,
                              reject_unauth_pipelining,
                              permit_sasl_authenticated,
                              permit_mynetworks
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_type = cyrus
smtpd_sasl_path = smtpd
smtpd_sasl_authenticated_header = yes
inet_interfaces = all
queue_directory = /var/spool/postfix
```

Il faut particulièrement être attentif aux points suivants de la configuration :

- **virtual_mailbox_maps = ldap:/etc/postfix/ldap-accounts.cf** et

  virtual_alias_maps = ldap:/etc/postfix/ldap-aliases.cf, Pour la validation des destinataires par recherche dans le LDAP.

- **mynetworks = 127.0.0.0/8, 192.168.0.0/16** pour n'autoriser que Local host à envoyer ou recevoir des mails (permit_mynetworks), les autres seront authentifiés via saslauthd.
- **smtpd_sasl_auth_enable = yes**, pour activer l'authentification SASL.

Pour l'accès au LDAP, nous faisons référence à deux fichiers : /etc/postfix/ldap-accounts.cf et /etc/postfix/ldap-aliases.cf

```
root@SMTPIMAP:~#nano   /etc/postfix/ldap-accounts.cf
server_host = ldap.bastos.dz
server_port = 389
search_base = ou=People,dc=bastos,dc=dz
query_filter = (&(objectClass=InetOrgPerson)(mail=%s))
result_attribute = cn
bind = yes
bind_dn = cn=admin,dc=bastos, dc=dz
bind_pw = xxxxxx
version = 3
root@SMTPIMAP:~#  nano /etc/postfix/ldap-aliases.cf
server_host = ldap.bastos.dz
server_port = 389
search_base = ou=People,dc=bastos,dc=dz
query_filter = (&(objectClass=InetOrgPerson)(mail=%s))
result_attribute = mail
bind = yes
bind_dn = cn=admin,dc=bastos,dc=dz
bind_pw = xxxxxx
version = 3
```

Remarque : n'oublions pas de gérer les droits de ces 2 fichiers.

En se positionnant sur le répertoire /etc/postfix/, on exécute ses deux commandes :

```
# chown root:sasl ldap*.cf

# chmod 640 ldap*.cf
```

L'attribut en retour ici est mail (result_attribute = mail), mais il peut être très judicieux d'ajouter à l'annuaire LDAP un champ « maildrop » qui sera retourné ici. Ce champ donnera alors une vraie fonctionnalité d'alias, permettant de transférer tout mail à destination de l'utilisateur vers une ou plusieurs autres adresses email.

De plus, il faut noter que dans la configuration actuelle et sans cette notion d'alias, une boîte Cyrus doit être associée à chaque adresse email locale. En effet, Cyrus recherche une boîte dont le nom correspond au préfixe de l'adresse email du destinataire (ce qui est avant le @ en bref).

L'authentification SASL à besoin d'un fichier : /etc/postfix/sasl/smtpd.conf. Attention, sous d'autres distributions, le fichier peut être cherché ailleurs, généralement dans /usr/lib/sasl2/ ou /usr/local/lib/sasl2. Elle a également besoin que l'utilisateur « Postfix » appartienne au groupe SASL.

```
# adduser postfix sasl
#id postfix
uid=106(postfix) gid=109(postfix) groupes=109(postfix),8(mail),45(sasl)
root@SMTPIMAP:~# nano /etc/postfix/sasl/smtpd.conf
pwcheck_method: saslauthd
mech_list: plain  login
```

Remarque :

Afin d'activer le support TLS pour Cyrus-imap, il suffit d'éditer le fichier /etc/imapd.conf et de dé commenter les deux lignes suivantes (le certificat utilisé est le même que pour Postfix). L'utilisateur Cyrus doit appartenir au groupe ssl-cert pour pouvoir lire la clef privée.

```
# adduser cyrus ssl-cert
#cat  /etc/imapd.conf | egrep -v '(^#|^$)'
configdirectory: /var/lib/cyrus
                        ….
                        ….
tls_cert_file: /etc/ssl/certs/ssl-cert-snakeoil.pem
tls_key_file: /etc/ssl/private/ssl-cert-snakeoil.key
                        …..
```

III.8.Le serveur SOGO

III.8.1.Installation de serveur SOGO

Ajouter la ligne suivante : http://inverse.ca/debian-nightlywheezy wheezy dans le fichier source.list.

```
root@SOGO:~# nano  /etc/apt/sources.list
#Dépôt pour sogo
deb http://inverse.ca/debian-nightly wheezy  wheezy
```

Ensuite on exécute la commande suivante pour authentifier les paquets de ce nouveau dépôt :

```
root@SOGO:~# apt-key adv --keyserver keys.gnupg.net --recv-key 0x810273C4
```

On met à jour les dépôts et on installe les paquets sogo et postgresql

```
root@SOGO:~# aptitude update
root@SOGO:~# aptitude install sogo postgresql
                .
                .
                .
Voulez-vous continuer ? [Y/n/?] Y
```

III.8.2.Configuration de serveur SOGO

```
root@SOGO:~# nano /etc/sogo/sogo.conf
{
  /* ********************  Main SOGo configuration file  ********************
   *                                                                        *
   * Since the content of this file is a dictionary in OpenStep plist format,  *
   * the curly braces enclosing the body of the configuration are mandatory.   *
   * See the Installation Guide for details on the format.                     *
   *                                                                        *
   * C and C++ style comments are supported.                                   *
   *                                                                        *

   * This example configuration contains only a subset of all available        *
   * configuration parameters. Please see the installation guide more details. *
   *                                                                        *
   * ~sogo/GNUstep/Defaults/.GNUstepDefaults has precedence over this file,    *
   * make sure to move it away to avoid unwanted parameter overrides.          *
      *                                                                        *
   * ************************************************************************/
/* Database configuration (mysql:// or postgresql://) */
    SOGoProfileURL = "postgresql://sogo:djouher@localhost:5432/sogo/sogo_user_profile";
    OCSFolderInfoURL = "postgresql://sogo:djouher@localhost:5432/sogo/sogo_folder_info";
    OCSEMailAlarmsFolderURL                                                    =
postgresql://sogo:djouher@127.0.0.1:5432/sogo/sogo_alarms_folder;
    OCSSessionsFolderURL                                                       =
"postgresql://sogo:djouher@localhost:5432/sogo/sogo_sessions_folder";
  /* fin de  Database configuration (mysql:// or postgresql://) */
SOGoUserSources = (
        {
          CNFieldName = cn;
          IDFieldName = uid;
          UIDFieldName = uid;
          baseDN = "ou=People,dc=bastos,dc=dz";
          canAuthenticate = YES;
          displayName = "Shared Addresses";
          hostname = "ldap://ldap.bastos.dz:389";
          id = public;
 isAddressBook = YES;
          type = ldap;
        }
    );
```

```
SOGoAppointmentSendEMailNotifications = YES;
    0SOGoSuperUsernames = (service);
    SOGoSieveScriptsEnabled = YES;
    SOGoForwardEnabled = YES;
    SOGoVacationEnabled = YES;
    SOGoEnableEMailAlarms = YES;
    SOGoSupportedLanguages = ( "French", "English", "Spanish" );
    SOGoLanguage = French;
SOGoTimeZone = Europe/Paris;
    SOGoIMAPServer = smtpimap.bastos.dz:143;
    SOGoSieveServer = sieve://smtpimap.bastos.dz:4190;
    SOGoMailingMechanism = smtp;
SOGoSMTPServer = smtpimap.bastos.dz;
SOGoCalendarDefaultRoles = ("PublicDAndTViewer");
SOGoDraftsFolderName = INBOX/Drafts;
SOGoSentFolderName = INBOX/Sent;
SOGoTrashFolderName = INBOX/Trash;
LDAPDebugEnabled = YES;
ImapDebugEnabled = YES;
SOGoDebugRequests = YES;
SoSecurityManagerDebugEnabled = YES;
}
```

v Configuration /etc/apache2/conf.d/Sogo.conf

On renseigne url https://sogo.bastos.dz dans le paramètre (RequestHeader set "x-webobjects-server-url) :

```
# adjust the following to your configuration
  RequestHeader set "x-webobjects-server-port" "443"
  RequestHeader set "x-webobjects-server-name" "yourhostname"
  RequestHeader set "x-webobjects-server-url" "https://sogo.bastos.dz"
```

- **Configuration de fichier /etc/apache2/site-availible/sogo**

```
root@SOGO:~# nano /etc/apache2/sites-available/sogo
<VirtualHost *:80>
        ServerName sogo.bastos.dz
        ServerAdmin rtr+sogo.bastos.dz
        DocumentRoot /var/www
        ErrorLog /var/log/apache2/sogo.bastos.dz-error.log
        CustomLog /var/log/apache2/sogo.bastos.dz-access.log combined
        RedirectMatch ^/$ https://sogo.bastos.dz/SOGo
</VirtualHost>
```

- **Configuration de fichier /etc/apache2/site-availible/sogo-ssl**

```
root@SOGO:~# nano /etc/apache2/sites-available/sogo-ssl
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
        ServerName sogo.bastos.dz
        ServerAdmin sogo@bastos.dz
        #Alias /plugins /srv/sogo-plugins/
        #<Directory /srv/sogo-plugins/>
        #       Options +ExecCGI
        #       AddHandler cgi-script .py
        #</Directory>
        RedirectMatch ^/$ https://sogo.bastos.dz/SOGo
        ErrorLog /var/log/apache2/sogo.bastos.dz-ssl-error.log
        CustomLog /var/log/apache2/sogo.bastos.dz-ssl-access.log combined
        SSLEngine on
        SSLCertificateFile      /etc/apache2/sogo.bastos.dz.crt
        SSLCertificateKeyFile  /etc/apache2/sogo.bastos.dz.key
        SSLVerifyClient None
</VirtualHost>
</IfModule>
```

Activation les sites de SOGO et sogo-ssl et les modules nécessaires pour le bon fonctionnement :

```
root@SOGO:~# a2ensitesogo,
root@SOGO:~#a2ensitesogo-ssl,
root@SOGO:~# a2enmod proxy
root@SOGO:~#a2enmod proxy_http
root@SOGO:~#a2enmod headers
root@SOGO:~# a2enmod rewrite
```

III.9.Test d'envoie et réception d'un mail

Cette partie de notre projet consiste à faire des tests d'envoie et de réception des mails, pour assurer le bon fonctionnement de notre plate-forme.

Pour effectuer ces tests on suit les étapes suivantes :

On ouvre le navigateur Web, puis accéder au serveur SOGO à laide de l'adresse suivant :https://sogo.bastos.dz/SOGo/ :

Figure III.36 : L'interface Web de SOGO.

On saisit le nom d'utilisateur et le mot de passe, et on clique sur « connexion » :

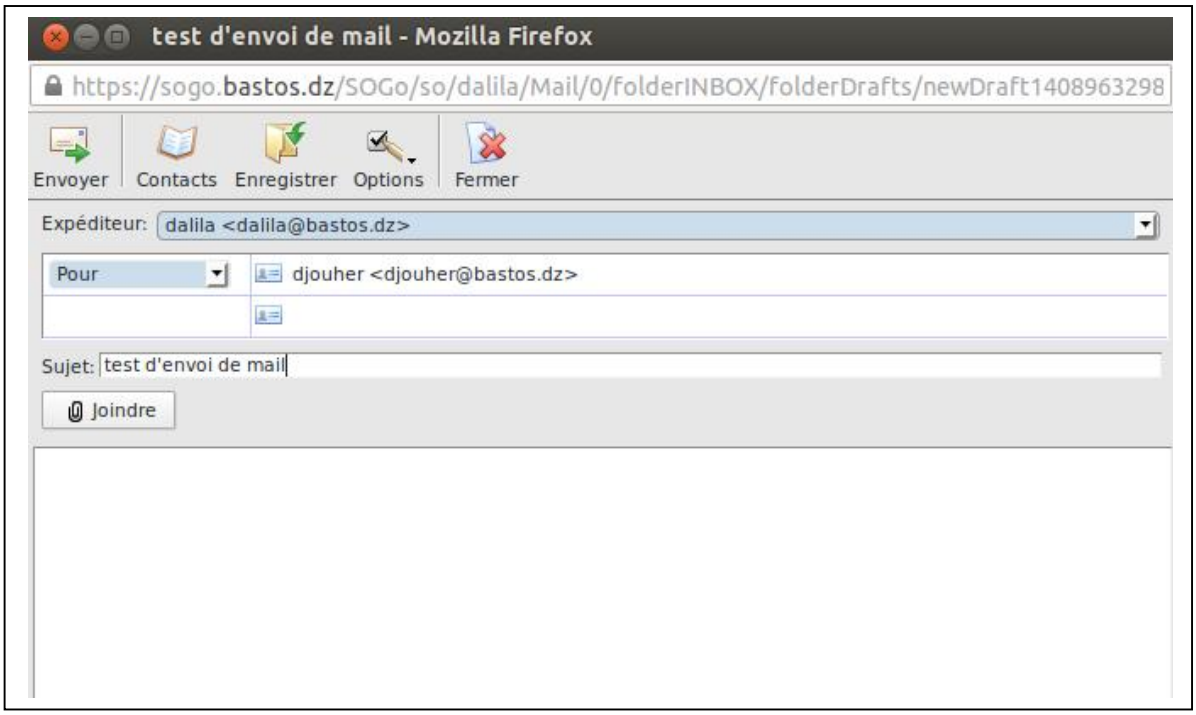


Figure III.37 : Message envoyé.

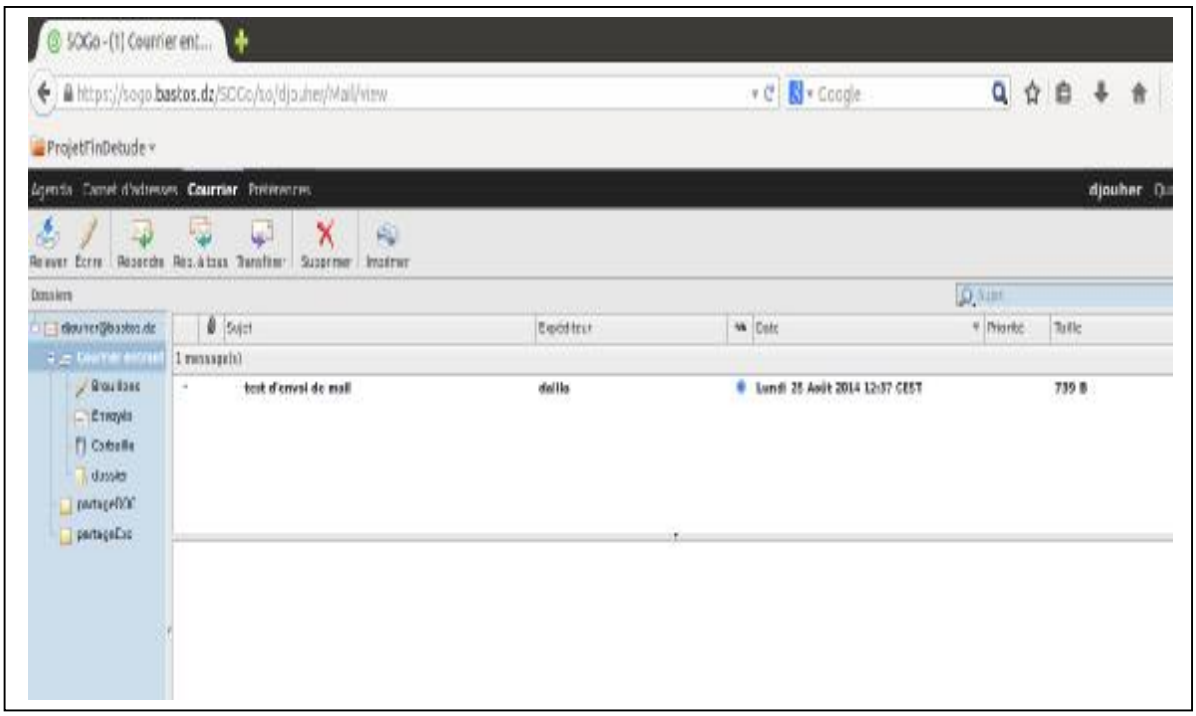


Figure III.38 : Message reçu.

Le message de test envoyé est bien reçu.

III.10.Discussion

Dans ce chapitre, on a montré les différentes étapes nécessaires pour réaliser un système de messagerie interne, commencé par l'installation et la configuration des différents serveurs, création d'utilisateurs dans l'annuaire LDAP, création des boite mails, finir par un test d'envoie et réception d'un mail.

On a constaté que la messagerie électronique est l'un des services les plus utilisé dans les milieux du travail.

Ce mémoire est pour nous l'occasion d'aborder un des systèmes de l'information et de la communication, qui est le système de la messagerie électronique, et d'étendre nos connaissances au monde professionnel qui nous était jusqu'à lors inconnu.

Nous avons constaté à travers notre travail, que la mise en œuvre d'un système de messagerie électronique, devient de plus en plus la solution de communication et d'échange de données au sein des organisations, car elle offre des accès mobiles ou distants dans un environnement simple et rapide.

Afin de répondre à ces objectifs, nous avons porté notre choix sur la mise en place d'une messagerie interne d'un organisme, nous avons effectué des configurations d'un serveur de messagerie simple, mais fonctionnel, des boites aux lettres, et des connecteurs d'envoie et de réception pour l'envoie de mail à partir des clients interne. Néanmoins, une phase de démonstration pratique a été possible, grâce à notre ordinateur personnel configuré comme serveur de messagerie dans le réseau local.

L'élaboration de ce mémoire nous a initiés au monde de la gestion et de l'administration réseaux, ce qui nous a permis de comprendre l'importance de notre domaine d'étude. Il nous a permis d'abord de revoir certaines notions comme par exemple le DNS, les protocoles TCP/IP, les différents agents (MUA, MTA, MDA), et les protocoles de messagerie tels qu'IMAP et SMTP.

Le déroulement de notre travail sous Linux nous permis de se familiariser avec ce système, et de découvrir le monde de l'Open Source.

Nous citons comme perspective à notre travail : réaliser pratiquement ce système de messagerie électronique au sein de notre université (Université Mouloud Mammeri Tizi-Ouzou), afin de répondre aux besoins de communication entre les différents acteurs (administration, enseignant-e-s, étudiant-e-s, …).

Nous souhaitons que ce thème malgré les contraintes temporelles et matérielles soit enrichi et approfondi à l'avenir.

I.1.Préambule

Il est important que tous les termes significatifs soient clairement définis, c'est pour cette raison que nous avons consacré une partie importante aux annexes.

Dans cette annexe, nous avons pris le temps de bien définir les différents protocoles de communication utilisé par les systèmes d'information. La transmission de l'information entre deux programmes informatiques sur deux machines différentes passe par deux modèles de base, le modèle OSI et le modèle TCP/IP.

I.2.Les protocoles réseaux

I.2.1.Le modèle OSI

OSI signifie (Open System Interconnexion, ce qui se traduit par Interconnexion de Systèmes Ouverts). Ce modèle a été mise en place par l'ISO (International Standard Organisation), afin de mettre en place un standard de communication entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre les ordinateurs. En effet, aux origines des réseaux chaque constructeur avait un système propre (on parle de système propriétaire), ainsi de nombreux réseaux incompatibles coexistaient. C'est la raison pour laquelle l'établissement d'une norme a été nécessaire.

Le rôle du modèle OSI consiste à standardiser la communication entre les machines, afin que différents constructeurs puissent mettre au point des produit (logiciels ou matériels) compatibles, (pour peu qu'ils respectent scrupuleusement le modèle OSI).

- **L'intérêt d'un système en couches :** Le but d'un système en couches est de séparer le problème en différentes parties selon leurs niveaux d'abstraction.
  Chaque couche du modèle communique avec une couche adjacente (celle du dessus ou celle du dessous). Chaque couche utilise ainsi les services des couches inférieurs et en fournit à celle de niveau supérieur.
- **Les couches de modèle OSI :** Le modèle OSI est un modèle qui comporte 7 couches, qui sont les suivantes :

Application
Présentation
Session
Transport
Réseau
Liaison de Données
Physique

Figure 1 : Les couches de modèle OSI.

Et les rôles des différentes couches sont les suivants :

- **La couche physique** : définit la façon de laquelle les données sont converties en signaux numériques.
- **La couche liaison de données** : définit l'interface avec la carte réseau.
- **La couche réseau** : permet de gérer les adresses et le routage des données.
- **La couche transport** : elle est chargée du transport des données et de la gestion des erreurs.
- **La couche session** : définit l'ouverture des sessions sur les machines du réseau.
- **La couche présentation :** définit le format des données (leur représentation, éventuellement leur compression et leur cryptage).
- **La couche application :** assure l'interface avec les applications.

I.2.2.Le modèle TCP/IP

TCP/IP est une suite de protocoles. Le signale TCP/IP signifie « Transmission Control Protocol / Internet Protocol ». Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire le protocole TCP et le protocole IP.

TCP/IP représente d'une certaine façon, l'ensemble des règles de communication sur Internet et se base sur l'adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau, afin de pouvoir acheminer des paquets de données. Etant donné que la suite du protocole TCP/IP a été crée a l'origine dans le but militaire, elle est conçue pour répondre à un certain nombre de critères parmi lesquels :

- Le fonctionnement des messages en paquets.
- L'utilisation d'un système d'adresses.
- L'acheminement des données sur le réseau.
- Le contrôle des erreurs de transmission de données.

- **Les couches de modèle TCP/IP :** Le modèle TCP/IP peut en effet être décrit comme une architecture réseau à quatre couches, qui sont les suivantes :

Application
Transport
Inter-réseaux
hôte réseaux

Figure 2 : Les couches de modèle TCP/IP.

Et les rôles des différentes couches sont les suivants :

- **La couche hôte réseaux :** elle spécifie la forme sous laquelle les données doivent être acheminées quelque soit le type du réseau utilisé.
- **La couche Inter-réseaux (IP) :** elle est chargée d'assurer le transport des paquets de données (datagrammes).
- **La couche transport (TCP) :** elle assure l'acheminement des données, ainsi que les mécanismes permettant de connaitre l'état de la transmission.
- **La couche application :** elle englobe les applications standards du réseau (Telnet, SMTP, FTP...)

Remarque : Les données sont transmises vers le bas du modèle lorsqu'il s'agit d'une émission sur le réseau, et vers le haut lors d'une application.

Voici les principaux protocoles faisant partie de la suite TCP/IP :

Application : TELNET, FTP, SMTP, DNS
Transport : TCP, UDP
Internet : IP, ARP, ICMP
Hote réseau Ethernet

Figure 4 : Protocoles et réseaux dans le modèle TCP/IP.

- **Le protocole IP:** Internet Protocol, fait partie de la couche internet, c'est l'un des protocoles les plus importants d'Internet, car il permet l'élaboration et le transport des datagrammes IP, sans toutefois en assurer la livraison. Le protocole IP traite les datagrammes IP indépendamment les un des autres en définissant leur représentation, leur routage et leur expédition.

  Le protocole IP détermine le destinataire du message grâce à trois champs :

  - Adresse IP.
  - Le masque de sous réseau.
  - Passerelle par défaut.
- **Le protocole ARP :** Adresse Résolution Protocol, a un rôle important parmi les protocoles de la couche Internet de la suite TCP/IP ; car il permet de connaitre l'adresse physique d'une carte réseau correspondant à une adresse IP, d'où son nom protocole de résolution d'adresse.
- **Le protocole ICMP :** Internet Control Message Protocol, est un protocole qui permet de gérer les informations relatives aux erreurs des machines connectées. Etant donnée le peu de contrôles que le protocole IP réalise, il permet non pas de corriger ces erreurs mais de faire état de celles-ci aux protocoles des couches voisines. Ainsi, le protocole ICMP est utilisé par tous les routeurs pour rapporter une erreur.
- **Le protocole UDP :** User Datagramme Protocol, est comme le protocole TCP, c'est un protocole de transport de donnée. Cependant, contrairement au TCP, on qualifie l'UDP de transmission « en mode non connecté et non faible » ou encore de protocole « non orienté connexion ».
- **TCP :** Transmission Control Protocol, protocole orienté connexion qui assure le contrôle des erreurs.

- **DNS** : Domain Nam System, détermine les adresses IP à partir des noms de machines.

I.3.Transposition des deux modèles

Le modèle OSI a été mise à coté du modèle TCP, pour faciliter la comparaison entre les deux modèles.

Modèle TCP/IP	Modèle OSI
Application	Application
	Présentation
	Session
Transport	Transport
Inter-réseaux	Réseau
Hôte réseaux	Liaison de Données
	Physique

Figure 3 : Transposition TCP/IP et OSI.

Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de module ou couche), mais en contient uniquement quatre. Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

II.1.Préambule

Nous présentons dans cette annexe certaines informations importantes, qui aideront les lecteurs à comprendre ce travail.

II.2.L'annuaire LDAP

II.2.1.Définition d´un annuaire

Un annuaire est un recueil de données, dont le but est de pouvoir retrouver facilement des ressources (généralement des personnes ou des organisations), à l'aide d'un nombre limité de critères.

Les annuaires électroniques sont un type de base de données spécialisées, permettant de stocker des informations de manière hiérarchique et offrant des mécanismes simples pour rechercher l'information, la trier, l'organiser selon un nombre limité de critères. Ainsi le but d'un annuaire électronique est approximativement le même que celui d'un annuaire papier, si ce n'est qu'il offre une grande panoplie de possibilités que les annuaires papier ne sauraient donner.

L'utilisation d'annuaire ne se limite pas à la recherche de personnes ou de ressources. En effet, un annuaire peut servir à :

- constituer un carnet d'adresse.
- authentifier des utilisateurs (grâce à un mot de passe).
- définir les droits de chaque utilisateur.
- recenser des informations sur un parc matériel (ordinateurs, serveurs, leurs adresses IP et adresses MAC, ...).
- décrire les applications disponibles.

II.2.2.Caractéristiques des annuaires électroniques

Les annuaires électroniques possèdent un grand nombre d'avantages sur leurs "cousins de papier" :

- ils sont **dynamiques** : la mise à jour d'un annuaire électronique est beaucoup plus simple (et nettement moins coûteuse) à réaliser que celle d'un annuaire papier. Ainsi un annuaire en ligne (disponible sur le réseau) sera à jour beaucoup plus rapidement,

d'autant plus que les personnes recensées dans l'annuaire peuvent elles-mêmes modifier les informations les concernant (si elles sont habilitées à le faire).

- Ø ils sont **sûrs** : les annuaires en ligne disposent de mécanismes d'authentification des utilisateurs grâce à un mot de passe et un nom d'utilisateur, ainsi que des règles d'accès permettant de définir les branches de l'annuaire auxquelles l'utilisateur peut accéder.
- Ø ils sont **souples** : ils permettent ainsi de classer l'information selon des critères multiples contrairement aux annuaires papiers, imprimés une fois pour toute pour permettre de rechercher selon un critère figé (en général l'ordre alphabétique selon le nom).

II.2.3.La différence entre annuaire et base de données

Un annuaire est un type de base de données spécifique, c'est-à-dire qu'il s'agit d'une sorte de base de données ayant des caractéristiques particulières :

- Ø un annuaire est prévu pour être plus sollicité en lecture qu'en écriture. Cela signifie qu'un annuaire est conçu pour être plus souvent consulté que mis à jour.
- Ø les données sont stockées de manière hiérarchique dans l'annuaire, tandis que les bases de données dites "relationnelles" stockent les enregistrements de façon tabulaire.
- Ø les annuaires doivent être compacts et reposer sur un protocole réseau léger.
- Ø Un annuaire doit comporter des mécanismes permettant de rechercher facilement une information et d'organiser les résultats.
- Ø les annuaires doivent pouvoir être répartis. Cela signifie qu'un serveur d'annuaire doit comporter des mécanismes permettant de coopérer, c'est-à-dire d'étendre la recherche sur des serveurs tiers si jamais aucun enregistrement n'est trouvé.
- Ø Un annuaire doit être capable de gérer l'authentification des utilisateurs, ainsi que les droits de ceux-ci pour la consultation ou la modification de données.

Ainsi, un annuaire est généralement une application se basant sur une base de données afin d'y stocker des enregistrements, mais surtout un ensemble de services permettant de retrouver facilement les enregistrements à l'aide de requêtes simples. Une base de données par contre n'est pas forcément un annuaire...

II.2.4.Nécessité d'une normalisation

Ainsi un annuaire est un serveur remplissant les conditions décrites ci-dessus, mais l'implémentation peut être totalement différente d'un serveur à un autre, c'est pourquoi il a été nécessaire de définir une interface normalisée permettant d'accéder de façon standard aux différents services de l'annuaire. C'est le rôle du protocole LDAP (Lightweight Directory Access Protocol), dont le rôle est uniquement de fournir un moyen unique (standard ouvert) d'effectuer des requêtes sur un annuaire (compatible LDAP).

Bibliographie

- Alexis de Lattre, Rémy Garrigue, Tanguy Ortolo, Adrien Grand, Loïc Alsfasser, Patrick Burri : « Formation Debian GNU/Linux », 27 janvier 2013.
- BERNIER François : « Installation d'un serveur MAIL sous Ubuntu Server 12.10 », AFPA Formation TSGERI 2012-2013.
- Groupe : « Sécurité de la messagerie », septembre 2005.
- Sébastien ROHAUT : « Maitriser l'administrateur du système LINUX », 2iémé édition.
- Thierry.Charles : « VirtualBox ou comment avoir le beurre et l'argent du beurre… », 26 janvier 2010.
- Tutorial : « Comment créer une machine virtuel ».
- Yoch : « Comprendre la messagerie électronique », 2011.
- Mise en œuvre d'un système de messagerie Exchange sécurisé par la TMG, M^{lle} DAHOUMANE Lynda et M^{lle} CHEHEB Lilia, département électronique UMMTO, 2012/2013.

Sites Internet

- www.commentcamarche.net/contents/courrier-electronique/mime.php3
- www.commentçamarche.com/internet/ldap.htm
- www.Mémoireonligne.com/m_Etude-et-developpement-dune-application-de-messagerie-electronique0.html
- www.Mémoireonligne.com/m_Mise-en-place-dun-systeme-de-messagerie-electronique-Cas-du-fonds-de-prevoyance-militaire8.html
- http://www.virtualbox.org
- http://fr.wikipedia.org/wiki/Client_de_messagerie

A

ACL (**A**ccess **C**ontrol **L**ist) : interviennent après la notion de binding. Il sera possible de donner des droits de lecture, d'écriture (ou d'autres droits divers) sur des branches particulières de l'annuaire au compte connecté.

ADC (**A**gent de **D**istribution de **C**ourrier).

AGC (**A**gent de **G**estion de **C**ourrier).

AMS (**A**ndrew **M**ail **S**ystem).

API (**A**pplication **P**rogramming **I**nterface).

ARP (**A**dresse **R**ésolution **P**rotocol).

ARPANET (**A**dvanced **R**esearch **P**roject **A**gency **NET**work) : premier réseau à commutation de parquets à l'origine d'Internet, développé par le département de la défense américaine.

ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange) : qui signifie en français "code américain normalise pour l'échange d'information". La norme ASCII est largement utilisée en informatique pour coder les caractères.
L'ASCII est la norme de codage la plus répandue, et compatible avec le plus de supports. Il contient l'ensemble des caractères alphanumérique utilisé en anglais. Initialement, il est codé sur 7 bits (plus un code de parité).

ATC (**A**gent de **T**ransfert de **C**ourrier).

B

BAL (**B**oite **A**ux **L**ettres).

BBN (**B**olt **B**eranek and **N**ewman) : est une société américaine créée en 1948 par deux professeurs du Massachusetts Institude of Technologie (MIT) : Richard Bolt et Leo Beranek et d'un ancien étudiant de Richard Bolt : Robert Newman. La société doit son nom à ses fondateurs : ce sont leurs trois initiales.
Cette société a été pionnière dans l'histoire de l'informatique, on lui doit pêle-mêle : le langage Logo, le système d'exploitation TENEX, la mise en place du réseau ARPANET et l'envoi du premier courrier électronique.

BER (**B**asic **E**ncoding **R**ules).

C

CR/LF (**C**arriage **R**eturn / de **L**ine **F**eed) : est une séquence de deux octets, qui indique une fin de la ligne (et surtout une nouvelle ligne) dans un texte. Le sigle CRLF provient de la juxtaposition du sigle de Carriage Return (retour chariot), et de Line Feed (saut de ligne).

D

DAP (**D**irectory **A**ccess **P**rotocol).

Debian GNU / Linux : une distribution de logiciels libres. Populaire pour une utilisation sur les serveurs. Cependant, Debian n'est pas une distribution pour les débutants.

DHCP (Dynamic **H**ost **C**onfiguration **P**rotocol) : est un service qui permet d'attribuer dynamiquement des paramètres TCP/IP, aux clients qui ont font la demande.

DNS (**D**omain **N**ame **S**ystem) : il s'agit d'un service disponible dans un environnement TCP/IP, permettant de résoudre des noms du type www.google.fr en adresse IP.

E

E-Mail (**E**lectronic-**M**ail).

ESMTP (**E**xtended **S**imple **M**ail **T**ransfert **P**rotocol).

F

FTP (**F**ile **T**ransfert **P**rotocol).

G

GID (Group **ID**entifier) : est déterminé l'appartenance, ce qui permet de définir les droits.

GNU (GNU is **N**ot **U**nix) : est un projet qui a apporté des tas d'utilitaires au noyau Linux.

H

HTML (**H**yper **T**ext **M**arkup **L**anguage) : langage de mise en forme de données, utilises pour effectuer des présentations en mode graphique à travers un navigateur Internet.

HTTP (**H**yper **T**ext **T**ransfert **P**rotocol).

Hypertexte : les liens hypertexte (ancrages), sont des éléments d'une page HTML (soulignés lorsqu'il s'agit de texte), permettant aux internautes de navigateur vers une nouvelle adresse, lorsque l'on clique dessus. Ce sont les liens hypertextes qui permettent de lier des pages Web entre elles.

I

ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol).

IDE (**I**ntegrated **D**rive **E**lectronics).

IETF (**I**nternet **E**ngineering **T**ask **F**orce).

IMAP (**I**nternet **M**essage **A**ccess **P**rotocol).

Infrastructure : cette expression désigne l'ensemble des éléments de type matériel et logiciel, composant le système informatique d'une entreprise ou d'une organisation.

Internet : c'est un réseau informatique qui relie les ordinateurs du monde entier. Internet est le plus grand réseau informatique au monde.

IP (**I**nternet **P**rotocol).

IRC (**I**nternet **R**elay **C**hat).

ISO (**I**nternational **S**tandard **O**rganisation).

L

LAN (**L**ocal **A**rea **N**etwork) : il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation, et relies entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répandue étant Ethernet).

LBER (**L**ightweight **B**asic **E**ncoding **R**ules).

LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol).

LDIF (**L**ightweight **D**ata **I**nterchange **F**ormat).

Linux : est un système d'exploitation de type UNIX, multitâches et multiutilisateurs pour machines à processeurs 32 et 64 bits (en particulier les machines de type PC et Powermac), ouvert sur les réseaux et les autres systèmes d'exploitation.

M

Machine virtuelle : c'est l'environnement spécial créé par VirtualBox pour votre système d'exploitation invité qui s'exécute.

MAN (Métropolisation **A**rea **N**etwork) : interconnectent plusieurs LAN géographiquement proches (au maximum quelque dizaines de Km) à des débits importants. Ainsi un MAN permet à deux nœuds distants de communiquer, comme si ils faisaient partie d'un même réseau local. Un MAN est formée de commutateurs ou de routeurs interconnectés par des liens haut débits (en général en fibre optique).

MDA (**M**ail **D**elivery **A**gent).

MIME (**M**ulti-purpose **I**nternet **M**ail **E**xtention).

MTA (**M**ail **T**ransfert **A**gent).

MUA (**M**ail **U**ser **A**gent).

N

NLS (o**N-L**ine **S**ystem).

O

OpenLDAP : est un projet libre diffusé sous licence "OpenLDAP Public License". Il est supporté par la fondation OpenLDAP, créée en 1998 par une société du nom de "Net Boolean", fournisseur de services professionnels liés à la messagerie.

Oracle : logiciel de bases de données de la société Oracle Corporation, qui a acquis en 2009 la société Sun Microsystems qui a elle-même acquis en 2008 la société InnoTek, développeur du logiciel VirtualBox.

OSI (**O**pen **S**ystem **I**nterconnexion).

P

Paquet : est une archive comprenant les fichiers informatiques, les informations et procédures nécessaires a l'installation d'un logiciel sur un système d'exploitation au sein d'un agrégat logiciel, en s'assurant de la cohérence fonctionnelle du système ainsi modifie.

PhpLDAPadmin : est une interface écrite en php, qui permet de modifier facilement et via une interface conviviale un annuaire LDAP (OpenLDAP principalement), sur le même principe que phpMyAdmin pour les bases de données MySQL.
Il permet de gérer plusieurs annuaires LDAP, et implémente plusieurs modes d'authentification. Il est présent sous forme de paquets dans la plupart des distributions récentes.

POP (**P**ost **O**ffice **P**rotocol).

R

Routage : est le mécanisme par lequel des chemins sont sélectionnés dans un réseau, pour acheminer les données d'un expéditeur jusqu'à un ou plusieurs destinataires. Le routage est une tache exécuté dans de nombreux réseaux, tels que le réseau téléphonique, les réseaux de données électroniques comme l'Internet, et les réseaux de transports. Sa performance est importante dans les réseaux décentralisés, c'est-à-dire ou l'information n'est pas distribuée par une seule source, mais échangée entre des agents indépendants.

S

SASL (Simple **A**uthentication and **S**ecurity **L**ayer) : signifiant « Couche d'authentification et de sécurité simple », est un cadre d'authentification et d'autorisation standardisé par l'IETF.

Sendmail : est le doyen de tous les serveurs de messagerie, et fût à une époque le plus répandu sur les réseaux grâce à ses bonnes performances, et une grande publicité par les universités. Malheureusement, il est également le plus connu pour son fichier de configuration compliqué, pour une personne normalement constituée. De nombreuses failles de sécurité criblent malheureusement ce vénérable MTA.

Shell : est un programme qui va faire le lien entre le noyau UNIX et l'utilisateur.

SI (Système d'**I**nformation).

SMTP (**S**imple **M**essage **T**ransfert **P**rotocol).

SNDMSG (**S**e**ND** **M**e**S**sa**G**e) : programme informatique pour envoyer les messages.

SOPE (**S**kyrix **O**bject **P**ublishing **E**nvironment).

SSH (**S**ecure **S**hell).

SSL (**S**ecure **S**ockets **L**ayer).

Système d'exploitation : programme assurant la gestion de l'ordinateur et de ses périphériques. Il sert d'interface entre l'utilisateur et le matériel.

Système d'exploitation hôte : c'est le système d'exploitation de l'ordinateur physique sur lequel VirtualBox a été installé.

Système d'exploitation invité : c'est le système d'exploitation en fonction dans la machine virtuelle.

T

TCP (Transfer**t C**ontrol **P**rotocol).

TELNET (TELecommunication **NET**work).

Transmission asynchrone : l'émetteur et le récepteur n'ont pas à être connectés en même temps.

U

Ubuntu : distribution Sud Africaine, elle dérive de Debian mais est plus facile d'utilisation.

UDP (**U**ser **D**atagramme **P**rotocol).

UID (**U**ser **ID**entifier) : est unique et propre à l'utilisateur.

URL (**U**niform **R**essource **L**ocator) : chemin réseau permettant d'identifier une ressource TCP/IP de manière unique.

W

WAN (**W**ide **A**rea **N**etwork ou réseau étendu) : interconnecte plusieurs LAN à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des routeurs, qui permettent de « choisir » le trajet le plus approprié pour atteindre un nœud du réseau.