

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique



Mémoire de Master

Mention Électronique

Spécialité : Systèmes de Télécommunication

Présenté par

Arbia Youcef

&

Tidafi Adel

Mise en place d'un système de messagerie sous Linux

Proposé par : Dr. Y. KABIR

Année Universitaire 2020-2021

Remerciements

Tout d'abord, nous commençons par remercier Dieu le Tout Puissant de nous avoir donné le courage et la volonté pour réaliser ce travail, et de le finir.

L'opportunité nous est donnée de témoigner notre gratitude et notre reconnaissance à toutes les personnes qui par leur aide et leurs encouragements nous ont permis de réaliser ce travail.

Nous exprimons nos vifs remerciements à nos chers parents, pour leur soutien, sacrifices et prières. C'est grâce à eux qu'on est là aujourd'hui.

Nous tenons à remercier aussi notre promoteur Mr. Kabir qui nous a énormément soutenu et orienté. Ils nous a encouragé par ses orientations sans cesser d'être une grande source de motivation et d'enthousiasme. Nous lui sommes reconnaissant de nous avoir fait bénéficier tout au long de ce travail de sa grande compétence, sa rigueur intellectuelle, son efficacité et de ses précieux conseils.

Nous n'oublions pas de remercier Mr. Moussa et Mr. Mehdi Merouane, les enseignants qui ont contribué par leurs nombreuses remarques et suggestions à améliorer la qualité de ce travail. Nous les remercions sincèrement pour leur disponibilité, leurs qualités humaines d'écoute et leur soutien moral pendant toute cette période.

Nous remercions enfin toutes les personnes qui ont contribué de près ou de loin, en apportant un petit grain supplémentaire de conseil, de savoir et d'enrichissement à ce modeste travail.

Dédicaces

Nous dédions ce travail à
nos chères familles,
nos amis
et à toute personne nous ayant soutenue durant toute cette période,
et à tous ceux qui n'ont jamais cessé de nous épauler.

Adel et Youcef

ملخص: تُعتبر أنظمة البريد الإلكتروني و الرسائل الإلكترونية من أنجح الوسائل التي تستعملها المؤسسات و الجامعات من أجل إضفاء خدمات تواصلية بسيطة و سهلة الاستعمال في ظرف زمني وجيز محافظين بهذا على خصوصية و سرية المعلومات المتبادلة.

الهدف من وراء هذا المشروع هو تحضير خادم للتواصل الإلكتروني بين مجموعة من الطلبة بُغية تسهيل عملية التواصل المباشر و هذا بطرح منهجية عمل للحصول على نتائج.

في بادئ الأمر، تمّ شرح أسس و طرق تطوير الأدوات المُستعملة في هذا العمل.

تمّ هذا العمل باستعمال الخادم المخصّص للمراسلات postfix و roundcube كواجهة بيانية.
كلمات المفاتيح: رسائل الكترونية، postfix، roundcube.

Résumé : La messagerie électronique et le courrier électronique sont des dispositifs de communication et d'échange de messages au sein des entreprises et universités qui visent à fournir un service de communication facile et plus simple dans un laps de temps tout en préservant la confidentialité des informations.

Notre tâche est bien de préparer le serveur de messagerie pour un groupe d'étudiants afin de faciliter la communication directe entre eux en suivant une méthodologie de travail pour obtenir des résultats.

Nous avons commencé par expliquer les bases et les méthodes de développement des outils utilisés avant de les réaliser.

La réalisation est faite en utilisant le serveur de messagerie postfix et roundcube comme interface graphique.

Mots clés : Messagerie électronique, Postfix, Roundcube.

Abstract: Electronic messaging and electronic mailing are communication and message exchange tools within companies and universities which aim to provide an easy and simpler communication service in a short period of time while preserving the confidentiality of information.

Our task is to prepare the mail server for a group of students in order to facilitate direct communication between them following a work methodology to achieve results.

We started by explaining the basics and the developed methods of the tools used before realizing them

The realization is done using the postfix and roundcube mail server as a graphical interface.

Keywords: Electronic messaging, Postfix, Roundcube.

Table des matières

Liste des acronymes	viii
Table des figures	ix
Introduction générale	xi
I Généralités sur les réseaux	3
I.1 Introduction	3
I.2 Réseaux informatiques	3
I.2.1 Définition d'un réseau	3
I.2.2 Topologies des réseaux	3
I.2.3 Taxonomies des réseaux informatiques	5
I.3 Architectures client/serveur	7
I.4 Modèles de communication réseau	8
I.4.1 Modèle OSI	8
I.4.2 Modèle TCP/IP	9
I.5 Mécanisme de routage	10
I.5.1 Éléments du routage	10
I.5.2 Routage statique	11
I.5.3 Routage dynamique	11
I.6 Généralités sur les serveurs	11
I.6.1 Serveur DNS	11
I.6.2 Serveur DHCP	12
I.6.3 Serveur proxy	12
I.7 Sécurité dans les réseaux locaux	13
I.7.1 Réseaux privés virtuels	13
I.7.2 Zones démilitarisées DMZ	13
I.7.3 Pare-feux	14

I.7.4	Table d’adressage réseau	14
I.8	Conclusion	14
II	Serveur de messagerie	17
II.1	Introduction	16
II.2	Protocoles de messagerie	16
II.2.1	Protocole SMTP	16
II.2.2	Protocole POP	17
II.2.3	Protocole IMAP	17
II.3	Système de messagerie électronique	18
II.3.1	Agents MTA	18
II.3.2	Agents MDA	18
II.3.3	Agents MUA	18
II.4	Protocoles de sécurité	18
II.4.1	Protocole SSL	18
II.4.2	Protocole SSH	19
II.5	Clients de messagerie	20
II.5.1	Client léger	20
II.5.2	Client lourd	20
II.5.3	Comparaison entre les clients lourds et les clients légers	20
II.6	Adresses électroniques	21
II.7	Outils de mise en œuvre d’un serveur de messagerie	22
II.7.1	Serveur de messagerie Postfix	22
II.7.2	Gnome sur Ubuntu 20.04 LTS Focal Fossa	22
II.7.3	Définition et rôle de PHP	22
II.7.4	Définition et rôle du MySQL	23
II.7.5	Définition de Certbot	23
II.7.6	Définition et avantages de Dovecot	24
II.7.7	Client Roundcube	24
II.8	Conclusion	24
III	Réalisation et mise en oeuvre	25
III.1	Introduction	25
III.2	Description de l’environnement du travail	25
III.2.1	Matériel et logiciels de base	25

III.2.2 Installation et description des composantes de la messagerie	25
III.3 Installation et configuration du système de messagerie	29
III.4 Conclusion	45
Conclusion générale	47
Bibliographie	48

Liste des acronymes

DMZ	D e M ilitarized Z one
DNS	D omain N ame S ervice
FTP	F ile T ransfer P rotocol
HTTP	H yper T ext T ransfer P rotocol
IMAP	I nternet M essage A ccess P rotocol
IP	I nternet P rotocol
LAN	L ocal A rea N etwork
MAA	M ail A ccess A gent
MAN	M etropolitan A rea N etwork
MDA	M ail D elivery A gent
MTA	M ail T ransfer A gent
MUA	M ail U se A gent
MySQL	M y S tructured Q uery L anguage
NAT	N etwork A ddress T ranslation
OSI	O pen S ystem I nterconnection
PAN	P ersonal A rea N etwork
POP3	P ost O ffice P rotocol version 3
RAN	R egional A rea N etwork
SMTP	S imple M ail T ransfer P rotocol
SSH	S ecure S hell
SSL	S ecure S ocket L ayer
TCP	T ransmission C ontrol P rotocol
VAN	V irtual A rea N etwork

VPN **V**irtual **P**rivate **N**etwork

WAN **W**ide **A**rea **N**etwork

-

Table des figures

I.1	Topologie en bus	4
I.2	Topologie en anneau	4
I.3	Topologie en étoile	5
I.4	Topologie maillée	5
I.5	Classification des réseaux selon la portée	6
I.6	Classification des réseaux selon la fonction	7
I.7	Architecture client/serveur	7
I.8	Modèle OSI	9
I.9	Modèle OSI et modèle TCP/IP	10
I.10	Configuration du serveur proxy	12
I.11	Emplacement du NAT entre deux réseaux	14
II.1	Position du protocole SMTP dans la chaîne de communication	16
III.1	Configuration du serveur Ubuntu - configuration de la connexion réseau .	26
III.2	Configuration du serveur Ubuntu - téléchargement des mises à jour du programme	26
III.3	Configuration du serveur Ubuntu - gestion des disques	27
III.4	Configuration du serveur Ubuntu - configuration du mot de passe pour le super-utilisateur	27
III.5	Configuration du serveur Ubuntu - mise à jour	28
III.6	Configuration du serveur Ubuntu - installation du système	28
III.7	Installation du serveur de messagerie - liaison de l'adresse IP avec le nom de l'hôte	31
III.8	Installation du serveur de messagerie - installation de certbot	33
III.9	Configuration de postfix - redirection	34
III.10	Configuration de postfix - sélection du site internet	34
III.11	Configuration de postfix - fourni du nom de domaine	35

III.12	Configuration de postfix - étapes de la configuration	36
III.13	Configuration de postfix - modification du fichier de configuration	37
III.14	Configuration de postfix - définition du domaine dans le fichier	37
III.15	Configuration de postfix - modification du fichier d'authentification	41
III.16	Configuration de postfix - lignes à ajouter	41
III.17	Configuration de Dovecot - lignes à modifier	42
III.18	Configuration de Dovecot - modification du fichier	42
III.19	Configuration de Roundcube - modification du fichier	43
III.20	Accès à la messagerie web Roundcube - interface de connexion	43
III.21	Accès à la messagerie web Roundcube - interface principale	44
III.22	Accès à la messagerie web Roundcube - envoi de message	44
III.23	Accès à la messagerie web Roundcube - réception de message	45

Introduction Générale

Un serveur de messagerie électronique est un logiciel serveur de courrier électronique. Il a pour vocation de transférer les messages électroniques d'un serveur à un autre. Un utilisateur n'est jamais en contact direct avec ce serveur mais utilise soit un client de messagerie installé sur son terminal (ordinateur ou smartphone), soit une messagerie web, qui se charge de contacter le serveur pour envoyer ou recevoir les messages.

Désormais, il est sûr que les technologies de l'information et de la communication représentent la révolution la plus innovante qui a marqué la vie de l'humanité en ce dernier siècle. En effet, elles viennent nous apporter de multiples comforts à notre mode de vie en révolutionnant le travail des individus par leur capacité de traitement d'information, d'une part, et de rapprochement des distances d'une autre. Parmi ces technologies, la messagerie électronique qui est assez développée dans les organisations aux cours de ces quinze dernières années, grâce à sa facilité d'utilisation et son utilité perçue.

De nos jours, les réseaux de télécommunication constituent une formidable passerelle entre les hommes et les différentes cultures et viennent nous apporter de multiples comforts à notre mode de vie en révolutionnant le travail des individus, d'une part, et en rapprochant les distances d'autre part, mais transporter des informations aussi différentes que la voix, les données et les images nécessite des techniques de plus en plus élaborées et une bonne connaissance des mécanismes de base ainsi qu'une maîtrise des technologies utilisées c'est-à-dire bien connaître les limites technologies pour être capable de concevoir, de spécifier et d'utiliser correctement les moyens mis à notre disposition.

C'est un service gratuit qui constitue un moyen de communication privilégié entre des personnes à travers un réseau informatique. Utiliser pour des applications très variées personnelles, professionnelles, associatives, politiques, etc., celui-ci occupe une place de plus en plus prépondérante par rapport aux moyens de communication traditionnels. Outre son faible coût, l'avantage de la messagerie électronique est d'optimiser la communication et la diffusion d'informations ce qui la rend indispensable au sein d'une entreprise, néanmoins la dépendance du réseau internet touche à la disponibilité de ce service ainsi

qu'à sa sécurité. Ainsi une mise en place d'un serveur de messagerie stable, disponible et sécurisé s'impose.

Dans ce contexte, nous allons montrer comment un système de messagerie interne, de par sa mise en place et sa sécurisation pourrait répondre aux besoins en termes de technologies de l'information et de la communication d'une entreprise.

En plus de l'introduction générale, ce rapport est composé de trois chapitres :

- Chapitre 01 : dans ce chapitre, nous présentons certains concepts de base sur les réseaux et leurs caractéristiques ainsi que leurs architectures. Nous parlons aussi des mécanismes de sécurité d'un réseau local.
- Chapitre 02 : ce chapitre aborde quelques notions théoriques sur les systèmes de messagerie électronique. Nous détaillons ainsi ses éléments de base.
- Chapitre 03 : nous expliquons dans cette partie la méthodologie suivie pour la réalisation d'un serveur de messagerie électronique sécurisé.

Et enfin, nous finalisons le travail par une conclusion générale résumant les grands points qui ont été abordé.

Chapitre I

GÉNÉRALITÉS SUR LES RÉSEAUX

I.1 Introduction

Dans ce chapitre nous allons d'abord définir et présenter le réseau informatique et ses différents concepts. Ensuite, nous allons définir et expliquer le fonctionnement de la messagerie électronique ainsi que ses composantes. Enfin, nous expliquerons les différentes manières pour sécuriser un serveur mail.

I.2 Réseaux informatiques

Nous allons dans cette section, aborder d'une manière générale les notions relatives aux réseaux informatiques.

I.2.1 Définition d'un réseau

Un réseau est un ensemble d'objets interconnectés les uns avec les autres. Il permet de faire circuler des éléments entre chacun de ces objets selon des règles bien définies.

Un réseau informatique particulièrement est une infrastructure constitué d'un ensemble de moyens matériels et logiciels permettant d'interconnecter des terminaux fixes ou mobiles, homogènes ou hétérogènes afin de transporter des informations d'un point A à B.

Un réseau peut avoir une dimension locale, métropolitaine, grande échelle ou planétaire.

I.2.2 Topologies des réseaux

Une topologie est la façon de conception et de construction d'un réseau. Autrement dit, elle désigne le motif ou bien la forme d'établissement des liens entre les différents terminaux et nœuds intermédiaires composants un réseau.

a. Critères de conception d'une topologie

Construire une topologie exige de prendre en compte plusieurs aspects :

- Nombre de stations à connecter ;
- Flux de données circulées ;
- Coût d'établissement des liens ;
- Distances entre les entités communicantes ;
- Résistance aux pannes ;
- Administration et évolution possible du réseau.

Tous ces facteurs doivent être pris en compte pour bien mener à une conception fiable, efficace et qui répond aux différents besoins auxquels on doit répondre lors de la construc-

tion d'un réseau.

Une topologie est censé résoudre les problèmes liés à l'acheminement des messages, le contrôle de flux et la sûreté de fonctionnement du réseau (fiabilité et maintenabilité).

b. Modélisation des topologies

Il existe plusieurs topologies des réseaux. Citons :

1. **Topologie en bus** : chaque poste de travail (ou terminal) est connecté à un câble principal (fig. I.1).

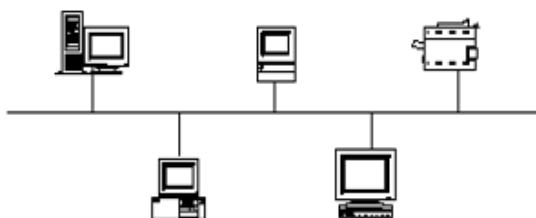


Figure I.1 — Topologie en bus

2. **Topologie en anneau** : comme le montre la figure I.2, les machines du réseau suivant cette topologie, sont câblées en formant un cercle. Ils ont donc deux voisins chacun.

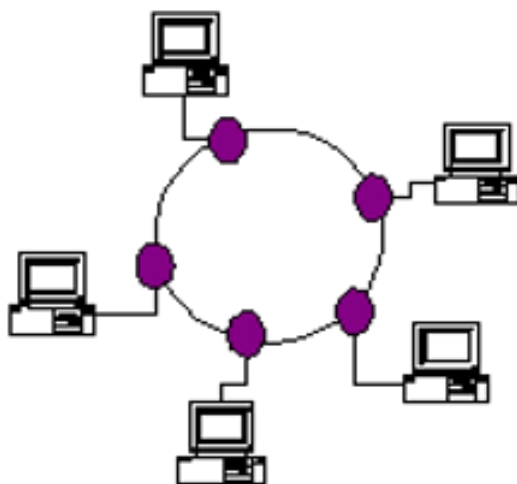


Figure I.2 — Topologie en anneau

3. **Topologie en étoile** : c'est la plus fréquente des topologies. Elle se constitue d'un dispositif central, très souvent un switch ou un hub, reliant les ordinateurs et les autres périphériques du réseau. La figure I.3 montre cette topologie.

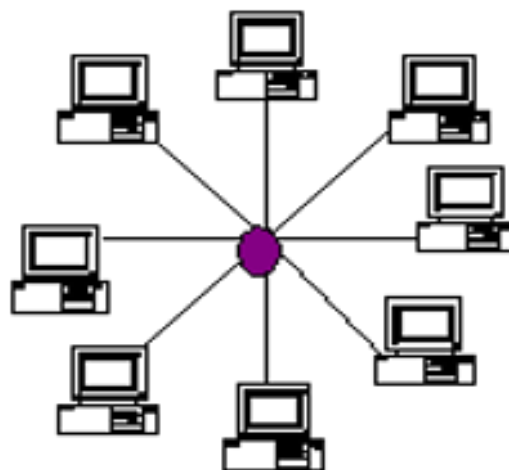


Figure I.3 — Topologie en étoile

4. **Topologie maillée** : chaque périphérique réseau est câblé avec plein d'autres (fig. I.4) ce qui permet d'avoir une redondance et une meilleure fiabilité.

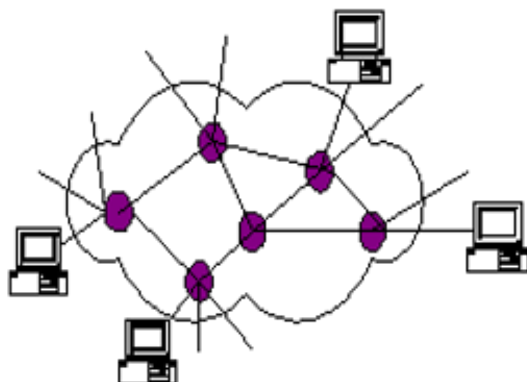


Figure I.4 — Topologie maillée

Il existe d'autres topologies, à savoir :

- **Topologie Radio** : la communication entre deux terminaux ou deux machines fait intervenir une antenne terrestre.
- **Topologie Satellite** : comme son nom l'indique, un satellite est responsable de l'établissement de la communication.

I.2.3 Taxonomies des réseaux informatiques

Un réseau informatique peut être classifié selon plusieurs critères en plusieurs classes.

a. Classification selon la portée

Suivant le critère de l'étendu ou la portée, un réseau peut appartenir à l'une des classes montrées dans la figure I.5.

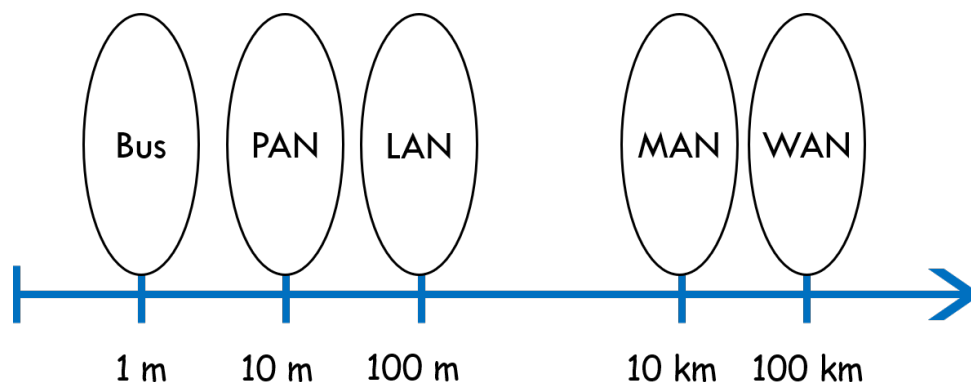


Figure I.5 — Classification des réseaux selon la portée

- **Bus** : ils sont responsables de la communication à l'intérieur d'une machine.
- **PAN** (Personal Area Network) : ce sont les réseaux à très petite échelle (réseaux personnels).
- **LAN** (Local Area Network) : ce sont des réseaux se trouvant dans un espace limité. Ils couvrent un bâtiment ou un ensemble de bâtiments.
- **MAN** (Metropolitan Area Network) : ce sont des réseaux à large échelle moyennement et qui couvrent généralement un quartier ou une cité.
- **WAN** (Wide Area Network) : ce sont les réseaux à large échelle (réseaux étendus). Ils couvrent les grandes villes et même des pays.

b. Classification selon la fonction

La figure I.6 montre que les réseaux informatiques sont répartis en trois grandes familles.

- **Réseaux particuliers ou d'entreprises** : ce sont les réseaux LAN, MAN qui gèrent la communication à une petite échelle (organisation, quartier, etc.).
- **Réseaux d'accès ou de collecte** : ce sont généralement les réseaux mobiles et à domicile. Par exemple : ADSL, GRPS, GSM, 3G, etc.
- **Réseaux de transport de données** : cette catégorie regroupe tous les réseaux responsables de l'échange de messages. (Internet, ATM, IP MPLS, etc.).

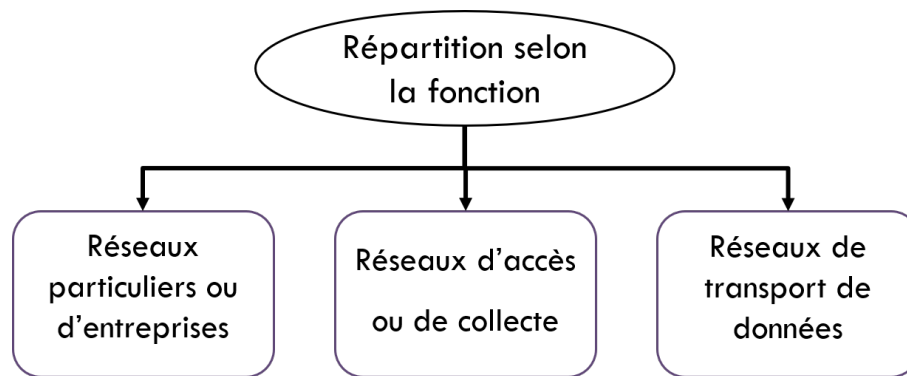


Figure I.6 — Classification des réseaux selon la fonction

I.3 Architectures client/serveur

Dans un réseau qui suit cette architecture (fig. I.7), il existe deux types de machines : [1]

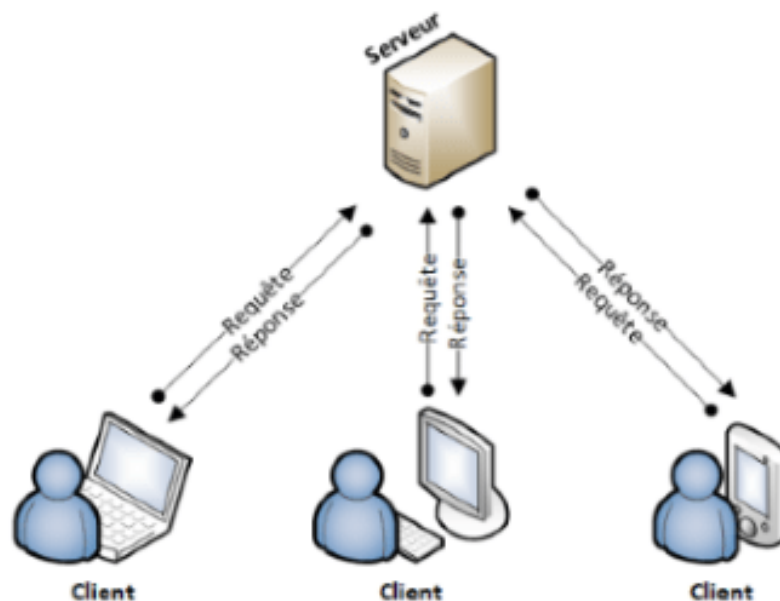


Figure I.7 — Architecture client/serveur

- **Machine client** : ce type de machines ne fait que demander des informations, services et des fichiers dont il a besoin. Cette demande va vers une autre machine **centrale** appelée **serveur**.
- **Machine serveur** : dans un réseau client/serveur, le serveur est unique et il représente le nœud central du réseau, auquel sont liés tous les autres nœuds. Il est appelé souvent **fournisseur**.

a. Fonctionnement de l'architecture

Le client émet une requête vers le serveur grâce à son adresse et à son port, qui désigne un service particulier du serveur.

Le serveur, après réception de la demande, répond le client en lui fournissant les informations voulues. [2]

b. Avantages de l'architecture

- Première infrastructure informatique pour un travail coopératif.
- Centralisation des traitements au niveau du serveur.
- Pas de duplication de données, ce qui permet de gagner en termes de ressources de stockage.

I.4 Modèles de communication réseau

Il existe principalement deux modèles qui définissent la manière de communication entre les nœuds d'un réseau.

I.4.1 Modèle OSI

OSI [3] signifie système ouvert réel dont la communication avec un autre système se fait conformément au modèle OSI. Ce modèle définit un cadre fonctionnel pour l'élaboration de normes d'interconnexion de systèmes. Il ne décrit pas comment ces systèmes fonctionnent en interne ou comment les normes doivent être implantées.

C'est modèle normalisé par l'organisation internationale de la standardisation ISO. Il se comporte comme une pile, c'est-à-dire une architecture en couches où chaque couche fournit des services pour la couche supérieure.

L'architecture OSI considère deux (02) aspects :

- L'organisation des communications en couches
- Le transfert de données grâce à un protocole.

L'architecture du modèle OSI se constitue de sept (07) couches [3] :

1. **Physique** : assurer la transmission de bits entre les entités physiques.
2. **Liaison** : responsable de l'accès entre les nœuds du réseau, la gestion de l'accès au médium et la détection et correction des erreurs.
3. **Réseau** : assurer l'acheminement à travers le réseau des messages en tenant compte des nœuds intermédiaires.



Figure I.8 — Modèle OSI

4. **Transport** : acheminement de bout en bout exclusivement, fiabilité et qualité de service de bout en bout.
5. **Session** : fournir un ensemble de services pour contrôler le dialogue entre les applications.
6. **Présentation** : permettre de manipuler des objets typés plutôt que des bits.
7. **Application** : fournir tous les mécanismes nécessaires au fonctionnement des programmes utilisateurs situés sur des machines distinctes et interconnectées.

I.4.2 Modèle TCP/IP

C'est le premier modèle de protocole en couches pour les communications inter-réseau. Il est créé au début des années 70 et est appelé modèle Internet. [4]

Il définit quatre (04) catégories de fonctions qui doivent s'exécuter pour que les communications réussissent [5].

1. **Accès au réseau** : contrôler les périphériques matériels et les supports qui constituent le réseau.
2. **Internet** : déterminer le meilleur chemin à travers le réseau.

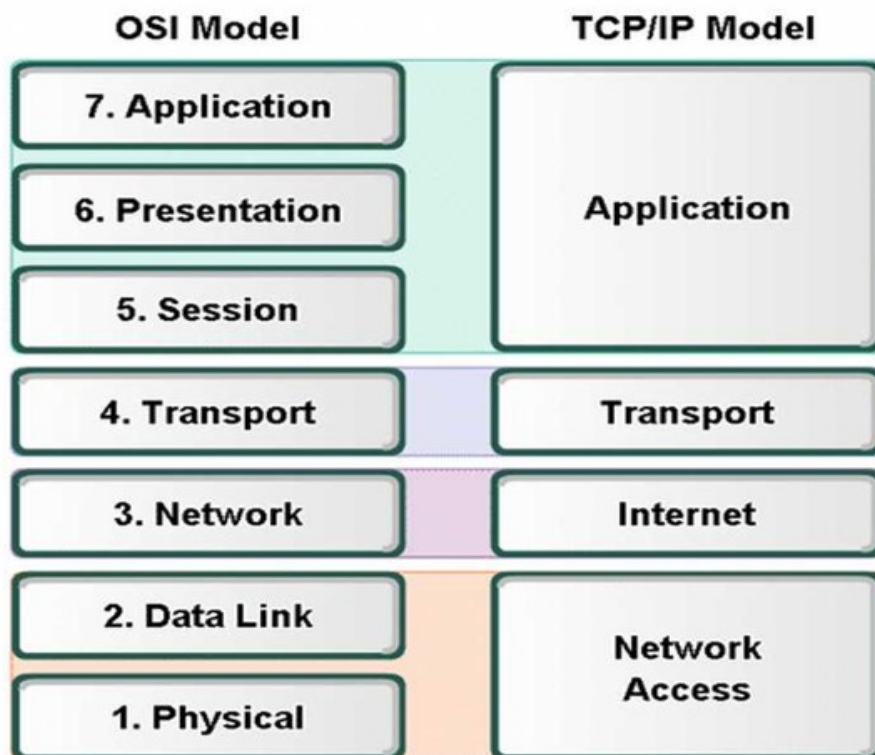


Figure 1.9 — Modèle OSI et modèle TCP/IP

3. **Transport** : prendre en charge la communication entre les différents périphériques à travers divers réseaux.
4. **Application** : représenter des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue.

I.5 Mécanisme de routage

Le 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. [6]

C'est une tâche exécutée au niveau des réseaux de données électroniques comme Internet et les réseaux de transport.

I.5.1 Éléments du routage

Le routage utilise : [6]

- **Table de routage** : située dans chaque nœud : information nécessaire pour atteindre le prochain nœud vers la destination.
- **Algorithme de routage** : fonction distribuée sur chaque nœud qui a pour objectif

de calculer les routes optimales pour atteindre une destination.

- **Protocoles de routage** : ont pour rôle l'échanges des informations de routes calculées par les algorithmes de routage et qui permettent la mise à jour dynamique des tables de routage.

Il en existe deux (02) façons de routage. [7]

I.5.2 Routage statique

Ce type de routage n'entraîne aucun changement dans la table de routage sauf si l'administrateur réseau la modifie manuellement.

Les algorithmes de routage statique fonctionnent bien là où le trafic réseau est prévisible. [6]

C'est une technique simple à concevoir et facile à mettre en œuvre. Il n'y a aucune exigence de protocoles de routage complexes.

I.5.3 Routage dynamique

C'est une technique de mise en réseau qui permet un routage optimal des données.

Contrairement au routage statique, le routage dynamique permet aux routeurs de sélectionner des chemins en fonction des changements de disposition du réseau logique en temps réel. Dans le routage dynamique, le protocole de routage opérant sur le routeur est responsable de la création, la maintenance et de la mise à jour de la table de routage.

Le routage dynamique utilise plusieurs algorithmes et protocoles. Les plus populaires sont RIP (Routing Information Protocol) et OSPF (Open Shortest Path First). [6]

I.6 Généralités sur les serveurs

Nous parlerons dans cette section de différents types de serveurs qui permettent chacun à son rôle de garantir un ensemble de fonctionnalités qui permettent l'échange de messages entre les couches des modèles de communication.

I.6.1 Serveur DNS

DNS [8] est responsable de la résolution des noms de domaine en adresses IP.

Pour les humains, il est facile de se souvenir d'une personne par son nom plutôt que par son numéro de téléphone. De même dans le monde d'Internet, nous nous souvenons des domaines par leurs noms mais l'ordinateur veut que leurs adresses IP communiquent avec eux. C'est donc le DNS qui vous fournit le nom du mappage d'adresse IP. [9]

I.6.2 Serveur DHCP

Il donne au client une adresse IP pour pouvoir communiquer avec d'autres clients dans un réseau local ou sur Internet.

Lorsque vous connectez un téléphone portable ou un PC à Internet via un port Wifi ou Ethernet, la première chose que fait votre appareil est d'obtenir une adresse IP d'un serveur DHCP. Cela implique l'échange de quatre messages entre votre appareil et le serveur, et qui sont : **DHCP Discover**, **DHCP offer**, **DHCP request** et **acknowledgement**. [10]

I.6.3 Serveur proxy

a. Définition et principe

Un serveur proxy (fig. I.10) joue le rôle d'une passerelle entre Internet et le client. C'est un serveur intermédiaire qui sépare les utilisateurs des sites Web sur lesquels ils naviguent. Les serveurs proxy assurent différents niveaux de fonctionnalité, sécurité et de confidentialité, selon le type d'utilisation, les besoins ou la politique de votre entreprise.

Quand utilisé, le trafic Internet passe par ce serveur avant d'atteindre l'adresse demandée. La réponse renvoyée passe par ce même serveur proxy (il y a des exceptions pour cette règle), puis celui-ci transmet au client les données reçues depuis le site Web.



Figure I.10 — Configuration du serveur proxy

b. Pourquoi ne pas communiquer directement avec le site Web ?

Pour assurer la sécurité des données et les performances du réseau, les serveurs proxy modernes font bien plus que transférer des requêtes Web. Ils font office de pare-feu et filtrent le Web, fournissent des connexions réseau partagées et placent les données en cache pour accélérer le traitement des requêtes les plus courantes. [11]

Un bon serveur proxy protège les utilisateurs et le réseau interne des menaces que recèle Internet.

Enfin, les serveurs proxy garantissent un niveau élevé de confidentialité.

I.7 Sécurité dans les réseaux locaux

La sécurité informatique est l'ensemble des moyens outils, techniques et méthodes mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

Elle a principalement trois (03) objectifs à réaliser :

- **Disponibilité** : a pour but de s'assurer qu'un système ou une donnée soit accessible en un temps défini.
- **Confidentialité** : a pour but de s'assurer qu'une information n'est accessible qu'aux personnes autorisées.
- **Intégrité** : a pour but de s'assurer qu'une donnée reste exacte et consistante à travers son cycle de vie.

Plusieurs techniques de sécurité ont été créés dans le but de protéger et minimiser les intrusions et les attaques dans un réseau local LAN.

I.7.1 Réseaux privés virtuels

VPN est une connexion cryptée entre des réseaux privés et un réseau public, similaire à Internet. [12]

Les informations provenant d'un réseau privé sont transportées en toute sécurité vers un réseau public. Cette connexion virtuelle est composée de paquets. Le VPN crée un réseau physiquement public mais virtuellement privé. Il est privé car il garantit la confidentialité à l'intérieur de l'organisation et il est virtuel car il n'utilise pas de véritables WAN privés.

De plus, VPN fournit un mécanisme pour utiliser l'authentification, la protection de l'intégrité, et le cryptage. VPN fournit aussi une connexion hautement sécurisée, cependant, il n'a pas besoin de câblage spécifique dans l'intérêt de l'organisation qui veut l'utiliser. Par conséquent, un VPN fusionne les avantages d'un réseau public avec ceux d'un réseau privé (sécurisé et fiable). [12]

I.7.2 Zones démilitarisées DMZ

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise.

On parle ainsi de « zone démilitarisée » pour désigner cette zone isolée hébergeant des

applications mises à disposition du public. La DMZ fait ainsi office de "zone tampon" entre le réseau à protéger et le réseau hostile. [13]

I.7.3 Pares-feux

Le pare-feu est un système physique (matériel) ou logique (logiciel) servant d'interface entre un ou plusieurs réseaux afin de contrôler et éventuellement bloquer la circulation des paquets de données, en analysant les informations contenues dans les couches 3, 4 et 7 du modèle OSI. [14]

Il s'agit donc d'une machine : machine spécifique dans le cas d'un firewall matériel ou d'un ordinateur sécurisé hébergeant une application particulière de pare-feu.

I.7.4 Table d'adressage réseau

NAT est la traduction d'adresses réseau qui relie deux réseaux et convertit les adresses privées en adresses publiques.

Ici, le terme "adresses privées" signifie que l'adresse de l'hôte appartient à un réseau local et n'est pas assignée par le fournisseur de services et l'adresse publique signifie que l'adresse est une adresse assignée par le fournisseur de service et il représente également une ou plusieurs adresses locales internes au monde extérieur. [15]

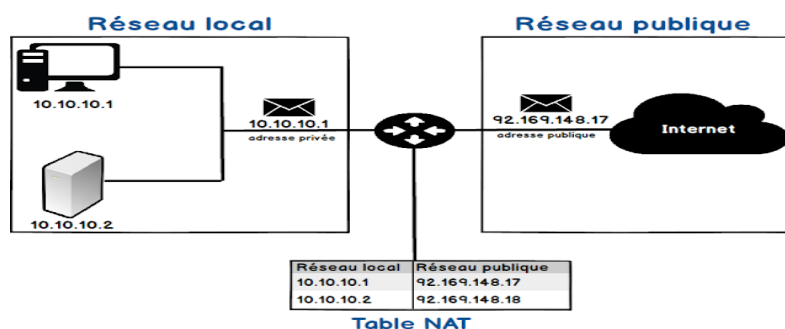


Figure I.11 — Emplacement du NAT entre deux réseaux

I.8 Conclusion

Un réseau est un ensemble d'objets interconnectés. Pour bien gérer l'échange de données entre ces objets, des modèles de communication sont définis. Et pour garantir la sécurité de ces données, diverses techniques sont établies.

Dans ce premier chapitre, nous avons donné des concepts de base liés aux réseaux en général. Nous avons expliqué la notion du réseau et ses topologies. Nous avons, par la

suite, abordé les modèles de communication et le mécanisme du routage. À la fin, nous avons expliqué quelques techniques appliquées pour la sécurité des réseaux.

Chapitre II

SERVEUR DE MESSAGERIE

II.1 Introduction

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

Dans ce chapitre, nous allons détailler cette notion de serveur de messagerie ainsi que les aspects lui sont liés.

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.

II.2 Protocoles de messagerie

Il existe une variété de protocoles qui sont responsables de la tâche de communication ou bien échange de messages entre les divers composants d'un système de messagerie.

II.2.1 Protocole SMTP

C'est un protocole de communication standard pour l'envoi de courriers électroniques sur des réseaux d'entreprise et sur Internet. SMTP (fig. II.1) a été développé au début des années 1980 et reste l'un des protocoles les plus populaires au monde. [16]

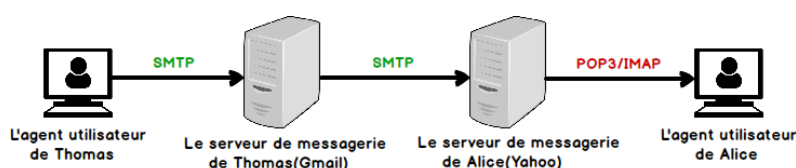


Figure II.1 — Position du protocole SMTP dans la chaîne de communication

Le logiciel de messagerie utilise généralement le protocole SMTP pour l'envoi et le protocole POP3 (Post Office Protocol 3) ou IMAP (Internet Message Access Protocol) pour la réception du courrier.

Jusqu'à présent, Il n'existe pas d'alternative au protocole SMTP. SMTP utilise le port TCP numéro 25 pour la communication standard. [17]

Le protocole SMTP est généralement intégré dans un client de messagerie et est composé de quatre composantes clés :

- Utilisateur local connu sous le nom de "agent de messagerie" (MUA – Mail User Agent),
- Serveur appelé (MSA – Mail Submission Agent),
- Agent de transfert de courrier (MTA – Mail Transfer Agent),
- Agent de distribution de courrier (MDA – Mail Delivery Agent).

SMTP commence d'abord par vérifier l'existence de l'expéditeur et du ou des destinataire(s), indiqués dans l'entête du message, puis il transmet le contenu. La transmission s'effectue sur un canal de communication établi entre l'émetteur et le destinataire par émission bidirectionnelle de requêtes basées sur des commandes. [16]

Autrement dit, SMTP fonctionne en lançant une session entre l'utilisateur et le serveur, alors que MTA et MDA fournissent des services de recherche de domaine et de remise locale. [18]

II.2.2 Protocole POP

POP ou bien Post Office Protocol est un protocole qui permet le téléchargement des courriels auprès d'un serveur de messagerie sur un PC.

Il a été mis à jour deux fois depuis sa première publication en 1984. Post Office v2 (POP2) a été publié en 1985 alors que la version 3 (POP3) a été publié en 1988. Cette version inclut de nouveaux mécanismes d'authentification et permet d'effectuer d'autres actions. [19]

Les messages électroniques entrants sont stockés sur un serveur POP jusqu'à ce que l'utilisateur se connecte (avec un client de messagerie) et télécharge les messages sur sa machine.

Le standard POP n'inclut pas les moyens d'envoyer des messages, et donc pour effectuer cette tâche, le protocole SMTP est utilisé.

II.2.3 Protocole IMAP

IMAP (Internet Messaging Access Protocol) est un standard Internet qui permet de récupérer des messages depuis un serveur de messagerie.

IMAP est un protocole Internet de couche application utilisant les protocoles de couche transport sous-jacents pour établir des services de communication hôte à hôte pour les applications. Cela permet d'utiliser un serveur de messagerie distant. L'adresse de port connue pour IMAP est 143. [20]

II.3 Système de messagerie électronique

Un système de messagerie électronique se compose de :

II.3.1 Agents MTA

Un agent MTA est un agent qui permet d'acheminer le courriel d'un serveur à un autre. Le MTA de l'émetteur route le mail sur le MTA du récepteur [21]. Il implémente toujours un protocole sortant¹.

Le protocole sortant généralement utilisé est SMTP. Il est de la famille des protocoles basés sur TCP/IP et utilise généralement le port 25.

II.3.2 Agents MDA

Il s'agit d'un agent qui est chargé de la gestion des boîtes aux lettres. Il est responsable de la livraison du courriel dans la boîte à messages du destinataire. Pour cela, il est souvent considéré comme le point final d'un système de messagerie. Dans le MDA, on peut filtrer les courriels, supprimer les spams par des anti-spams (comme spam assassin) et contrôler les virus par des antivirus [22].

II.3.3 Agents MUA

Le MUA est un logiciel client de messagerie qui fournit un environnement pour la gestion du courriel (envoi, saisie, réception, suppression, etc.). Il est très proche du MDA [23].

II.4 Protocoles de sécurité

Pour maintenir la sécurité et garantir la confidentialité des messages ou des données échangés, on a recours généralement à un protocole de sécurité.

II.4.1 Protocole SSL

SSL (Secure Socket Layer) est un protocole utilisé pour fournir des connexions sécurisées entre un client et un serveur. Une connexion TCP peut fournir un lien fiable entre un serveur et un client mais ne peut pas fournir des services tels que la confidentialité, l'intégrité et l'authentification du point de terminaison. Ainsi, les prochaines versions

1. Notons que les protocoles sortants permettent de gérer la transmission du courrier entre les systèmes de messagerie

du protocole SSL sont apparues sous le nom TLS.

a. Principe de fonctionnement

SSL, qui est implémenté dans la couche de transport, peut sécuriser un protocole tel que TCP en appliquant diverses mesures de sécurité. Il fournira la confidentialité en utilisant des cryptages pour empêcher quiconque d'espionner. Il utilise à la fois le cryptage asymétrique et symétrique. [24]

Tout d'abord, en utilisant un chiffrement à clé asymétrique, une clé de session symétrique est établie qui sera ensuite utilisée pour chiffrer le trafic.

La cryptographie à clé asymétrique est également utilisée pour les certificats numériques utilisés pour authentifier le serveur. Ensuite, le code d'authentification de message, qui utilise diverses techniques de hachage, est utilisé pour assurer l'intégrité (identifier toute modification non authentifiée apportée aux données réelles).

b. Utilité de SSL

Ainsi, un protocole comme SSL permet de transmettre des informations sensibles telles que les transactions bancaires et les informations de carte de crédit sur Internet. En outre, il est utilisé pour fournir la confidentialité pour des services tels que le courrier électronique, la navigation Web, la messagerie et la voix sur IP.

II.4.2 Protocole SSH

SSH (Secure Shell) est un protocole réseau utilisé pour établir une connexion sécurisée entre deux hôtes distants sur Internet ou au sein d'un réseau. IL utilise un format crypté pour transférer des données entre ordinateurs, de sorte que ce mécanisme crypté assure la confidentialité et l'intégrité des données échangées.

Ce protocole est largement utilisé pour les systèmes de connexion à distance et pour l'exécution de commandes à distance en raison de sa sécurité. En l'utilisant, les utilisateurs peuvent envoyer des données confidentielles telles que nom d'utilisateur, mot de passe et autres commandes de manière sécurisée car toutes ces données sont cryptées et ne peuvent pas être déchiffrées et lues facilement par les pirates.

SSH utilise la cryptographie à clé publique pour l'authentification du système distant. Par défaut, les serveurs SSH écoutent le port 22 sur TCP et peuvent être utilisés dans les réseaux publics. Il fournit donc, une authentification forte et un mécanisme de communication sécurisé sur des canaux non sécurisés. [25]

II.5 Clients de messagerie

Il existe deux types de clients qui manipulent les systèmes de messagerie.

II.5.1 Client léger

Le terme « client léger » (parfois « client pauvre », en anglais « thin client ») désigne une application accessible via une interface web (en HTML) consultable à l'aide d'un navigateur web, où la totalité de la logique métier est traitée du côté du serveur. Pour ces raisons, le navigateur est parfois appelé client universel.

Le fait que l'essentiel des traitements soit réalisé du côté du serveur et que l'interface graphique est envoyée au navigateur à chaque requête, permet une grande souplesse de mise à jour. En contrepartie, l'application doit s'affranchir des différences d'interprétation du code HTML par les différents navigateurs et l'ergonomie de l'application possède un champ réduit.

II.5.2 Client lourd

Le terme « client lourd » (en anglais « fat client » ou « heavy client ») désigne une application cliente graphique exécutée sur le système d'exploitation de l'utilisateur. Il possède généralement des capacités de traitement évoluées. Néanmoins, ceci demande un effort de développement et tend à mêler la logique de présentation (l'interface graphique) avec la logique applicative (les traitements).

Ce type d'application étant généralement installé sur le système d'exploitation de l'utilisateur, une nouvelle version doit être installée afin de la faire évoluer. Pour y remédier, les éditeurs d'applications lourdes les dotent généralement d'une fonctionnalité exécutée au lancement de l'application, permettant de vérifier sur un serveur distant si une version plus récente est disponible et dans le cas échéant, ils proposent à l'utilisateur de la télécharger et de l'installer.

II.5.3 Comparaison entre les clients lourds et les clients légers

Un client lourd exécute des fonctions indépendamment d'un service. Ces fonctions incluent le stockage et la récupération de données et de programmes ou d'applications, ainsi que le traitement local.

Les ordinateurs personnels connectés à un réseau local, à un réseau virtuel, à des serveurs d'informatique en nuage ou à Internet sont un excellent exemple de clients lourds.

Il est important de souligner le fait qu'un ordinateur personnel doit être utilisé principalement dans un environnement en réseau pour qu'il soit considéré comme un client lourd.

La collaboration et les programmes ou applications basés sur un abonnement sont d'autres exemples de clients lourds, en particulier s'ils sont installés et traités sur un périphérique informatique particulier. Microsoft Office 365 et Adobe Creative Cloud sont des exemples de ces applications.

D'autre part, un client léger est un client qui dépend fortement d'un serveur pour accéder aux données ou récupérer des fichiers et pour exécuter ou traiter des programmes ou des applications. Le serveur exécute la majeure partie de la charge de travail critique, notamment le stockage, la récupération et le traitement. En d'autres termes, un client léger dépend de manière critique des ressources matérielles d'un serveur.

Un ordinateur personnel peut également fonctionner en tant que client léger s'il est utilisé pour accéder à des programmes stockés sur un serveur. La plupart des ordinateurs clients légers sont légers en termes de spécifications matérielles.

Les navigateurs Web et les applications Web telles que WordPress, Google Docs et les jeux en ligne sur le Web sont également des exemples de clients légers. Les périphériques utilisés pour la diffusion multimédia en continu, tels que Chromecast et Apple TV, équipés d'applications de diffusion en continu telles que Netflix ou Spotify sont des exemples techniques de clients légers.

Pour concevoir et mettre en œuvre une architecture client-serveur, vous devez choisir entre un client lourd et un client léger ou, en d'autres termes, décider si le client ou le serveur gèrera la majeure partie de la charge de travail.

II.6 Adresses électroniques

Une adresse électronique (ou encore adresse e-mail ou adresse mail) est une chaîne de caractères permettant de recevoir du courrier électronique dans une boîte aux lettres informatique.

Format et codage des adresses électroniques

Les adresses de courrier électronique utilisées sur Internet sont codées dans un nombre très limité de caractères, sous-ensemble de l'ASCII. Un codage spécial appelé UTF-7 permet néanmoins de représenter tous les caractères Unicode en utilisant uniquement les caractères autorisés.

Elles sont constituées des trois éléments suivants, dans cet ordre :

1. Une partie locale, identifiant généralement une personne (lucas, Jean.Dupont, joe123) ou un nom de service (info, vente, postmaster).
2. Le caractère séparateur @ (arobase), signifiant *at* ("à" ou "chez") en anglais.
3. Un nom de domaine identifiant généralement l'entreprise hébergeant la boîte électronique (hotmail.com, live.com, gmail.com, yahoo.com).

II.7 Outils de mise en œuvre d'un serveur de messagerie

Dans cette section, nous définissons quelques outils utilisés dans la mise en œuvre d'un serveur de messagerie.

II.7.1 Serveur de messagerie Postfix

La messagerie électronique (ou E-mail : Électronique mail) est l'un des services les plus importants dans une entreprise. Elle permet aux utilisateurs d'envoyer et de recevoir des messages. Pour ce service, il faut mettre en place un serveur dit de messagerie qui va permettre aux clients de recevoir et gérer leurs comptes de messagerie.

Il existe plusieurs serveurs de messagerie parmi lesquels, on peut citer Postfix qui est beaucoup plus utilisé dans certaines entreprises.

Postfix est un serveur de messagerie électronique et un logiciel libre. Il se charge de la livraison de courriers électroniques (courriels) et a été conçu comme une alternative plus rapide, plus facile à administrer et plus sécurisée que son antécédent Sendmail.

II.7.2 Gnome sur Ubuntu 20.04 LTS Focal Fossa

GNOME (GNU Network Objet Environment) est une interface utilisateur graphique (GUI) sous Linux et, en particulier, dans le système d'exploitation Ubuntu. Il comprend une variété d'applications de bureau et son objectif est de rendre un système Linux facile à utiliser.

II.7.3 Définition et rôle de PHP

Le terme PHP est l'acronyme de "PHP Hypertext Preprocessor" . Le premier P de PHP est en effet lui-même l'abréviation de PHP.

PHP va nous permettre de créer des pages qui vont être générées dynamiquement. En d'autres mots, grâce au PHP, nous allons pouvoir afficher des contenus différents sur une

même page en fonction de certaines variables : l'heure de la journée, le fait que l'utilisateur soit connu et connecté ou pas, etc.

Ici, lorsque l'utilisateur rentre ses informations de connexion, celles-ci vont être traitées et analysées en PHP. On va vérifier si les informations sont bonnes et si c'est le cas récupérer des informations spécifiques à cet utilisateur et générer dynamiquement les pages de son espace client avec ces informations.

Lorsqu'un utilisateur fournit des informations comme une adresse, un numéro de téléphone ou passe une commande, les données sont généralement enregistrées dans ce qu'on appelle une base de données. Le PHP va également nous permettre d'aller récupérer des données dans une base de données pour s'en resservir.

De plus, notez que le PHP va s'exécuter côté serveur. Il fait ainsi partie des langages qu'on nomme "server side" en opposition aux langages "client side" qui s'exécutent côté client.

II.7.4 Définition et rôle du MySQL

MySQL est un système de gestion de bases de données relationnelles. Une base de données est un ensemble structuré de données. Les données vont pouvoir être des informations clients (nom, adresse, mot de passe, etc.), la liste des commentaires, le texte de nos articles, etc.

Le problème ici est qu'on ne va pas directement pouvoir interagir avec les bases de données car les données sont stockées d'une manière illisible pour un humain. Pour manipuler les données stockées dans les bases de données, nous allons devoir utiliser un langage de bases de données.

Le langage de bases de données le plus célèbre est le SQL. SQL est l'acronyme de Structured Query Language (Langage de Requêtes Structurées). Le système de gestion de bases de données MySQL utilise le langage SQL pour la manipulation des données des bases de données.

Grâce à sa simplicité d'utilisation, sa fiabilité et ses performances, MySQL est le langage par excellence pour l'interrogation des bases de données. De plus, on peut l'utiliser conjointement avec PHP.

II.7.5 Définition de Certbot

Certbot est un outil automatique, compatible avec les serveurs web majeurs (dont Apache et Nginx), ainsi qu'avec les OS Linux les plus courants à savoir : Debian, CentOS

et Ubuntu. Il est placé sous l'égide de l'EFF (Electronic Frontier Foundation). Un choix logique, sachant que Certbot pourra gérer des certificats proposés par d'autres autorités de certifications que Let's Encrypt.

II.7.6 Définition et avantages de Dovecot

Dovecot est une application d'agent de distribution des courriels MDA. Autrement, c'est un logiciel, sous licence libre, serveur de distribution de courriels par IMAP et POP3 pour Linux / UNIX, écrit avec comme première préoccupation la sécurité. Il convient tant pour des petites que pour des grandes structures.

Dovecot offre plusieurs avantages :

- Rapide,
- Simple à mettre en œuvre et à installer,
- Consommation faible de mémoire,
- Pas de charge d'administration extraordinaire.

II.7.7 Client Roundcube

Roundcube est un client IMAP multilingue basé sur un navigateur avec une interface utilisateur de type application. Il fournit toutes les fonctionnalités que vous attendez d'un client de messagerie, y compris la prise en charge MIME, le carnet d'adresses, la manipulation de dossiers, la recherche de messages et la vérification orthographique.

II.8 Conclusion

Dans ce second chapitre, nous avons abordé le concept des serveurs de messagerie. Nous avons parlé sur les protocoles de messagerie, l'architecture d'un système de messagerie ainsi que les protocoles gérant la sécurité.

Nous avons cité quelques enjeux liés à l'aspect sécuritaire dans un serveur de messagerie, et nous avons fini par la description des adresses électroniques.

Chapitre III

RÉALISATION ET MISE EN OEUVRE

III.1 Introduction

Après avoir expliqué la partie théorique et les notions de base liées à la thématique, nous passons maintenant à la pratique.

L'objectif de ce chapitre est de décrire la méthodologie de travail pour la mise en place du serveur de messagerie en détaillant les différentes phases de configuration, d'installation et de gestion du système.

III.2 Description de l'environnement du travail

Pour la réalisation de notre application, nous avons eu recours à des moyens matériels (hardware) et moyens logiciels (software).

III.2.1 Matériel et logiciels de base

1. **Matériel** : un PC portable (Dell) dont les caractéristiques sont :
 - CPU : Intel(R) Core(TM) i5-4210U, 1.70 GHz.
 - RAM : 8GO DDR3L.
2. **Logiciel** :
 - Système d'exploitation : Linux (Ubuntu 20.04).
 - Roundcube Webmail 1.4.3.

III.2.2 Installation et description des composantes de la messagerie

Nous avons d'abord réalisé l'installation su serveur Ubuntu 20.04 et son interface graphique à l'aide du Gnome.

a. Installation du serveur Ubuntu 20.04 (64bits)

Cette phase passe par sept (07) étapes :

1. **Choix de la langue** qui est l'anglais.
2. **Configuration de la connexion réseau** (fig. III.1)

Pour commencer à programmer les connexions réseau d'Ubuntu 20.04, Nous avons défini la configuration par défaut en tant que DHCP, attribution automatique des adresses IP, et nous avons pris la première disponible. La plupart des routeurs incluent DHCP.

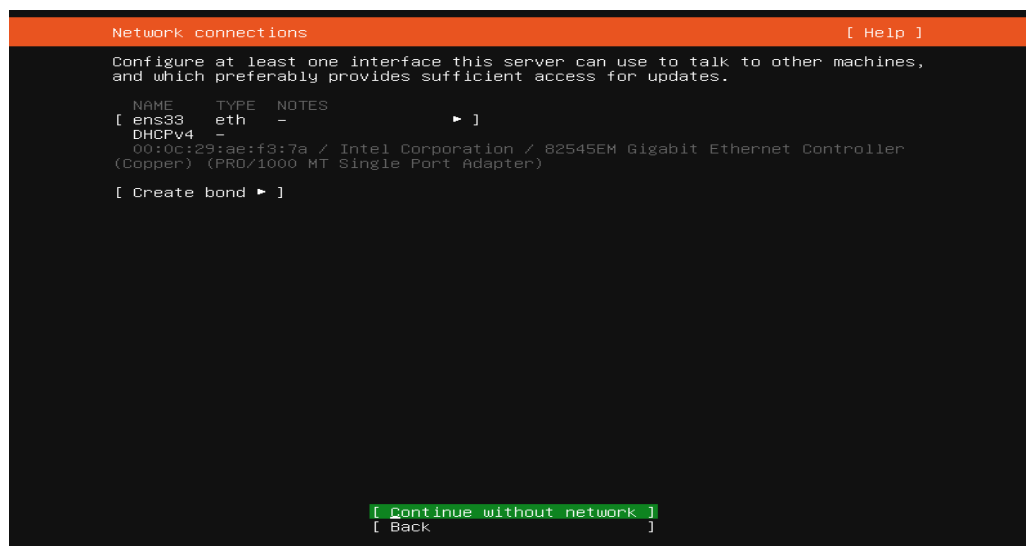


Figure III.1 — Configuration du serveur Ubuntu - configuration de la connexion réseau

3. Téléchargement des mises à jour du programme (fig. III.2) :

Plus tard, il nous a demandé d'où nous allons télécharger les mises à jour du programme d'installation et autres, nous l'avons laissé par défaut et poursuivi l'installation.

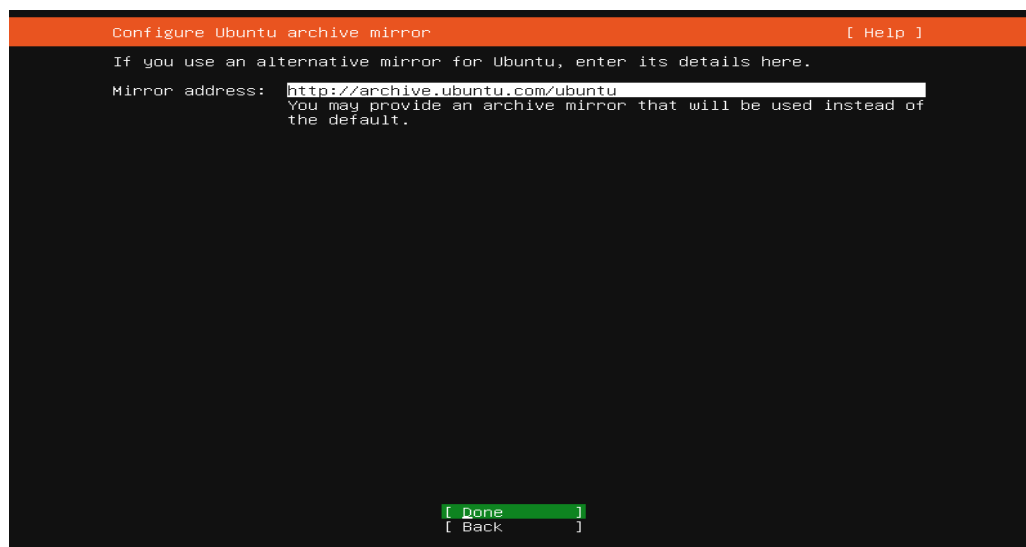


Figure III.2 — Configuration du serveur Ubuntu - téléchargement des mises à jour du programme

4. Gestion des disques (fig. III.3)

L'étape suivante, est l'une des améliorations décrites par Ubuntu dans le serveur 20.04. C'est une tâche rapide et sûre. Pour changer les partitions, nous devons sélectionner l'option "Utiliser un disque entier" pour configurer le disque et cela

en fonction de notre matériel.

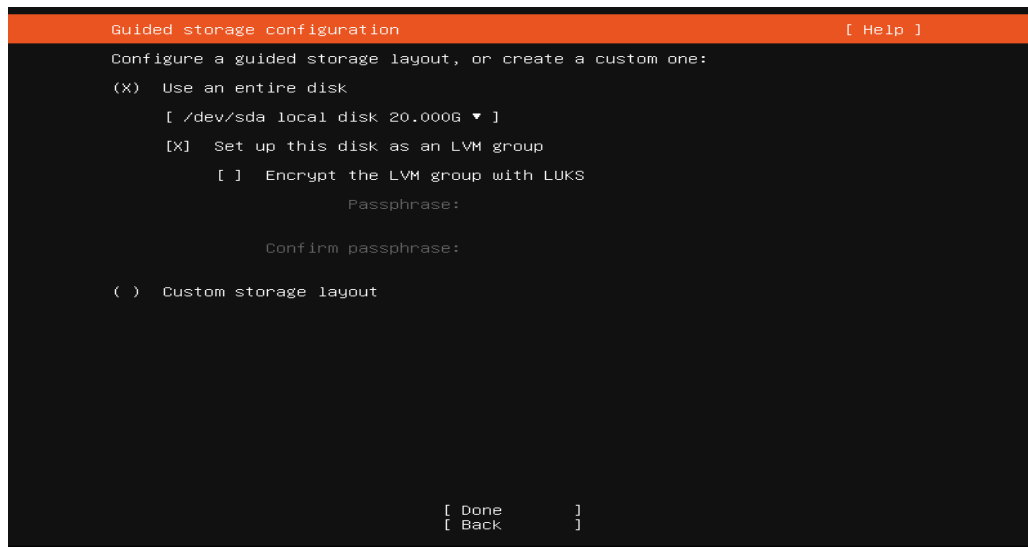


Figure III.3 — Configuration du serveur Ubuntu - gestion des disques

5. Configuration du mot de passe pour le super-utilisateur (fig. III.4)

Il est important de protéger la configuration de notre système d'exploitation par un mot de passe.

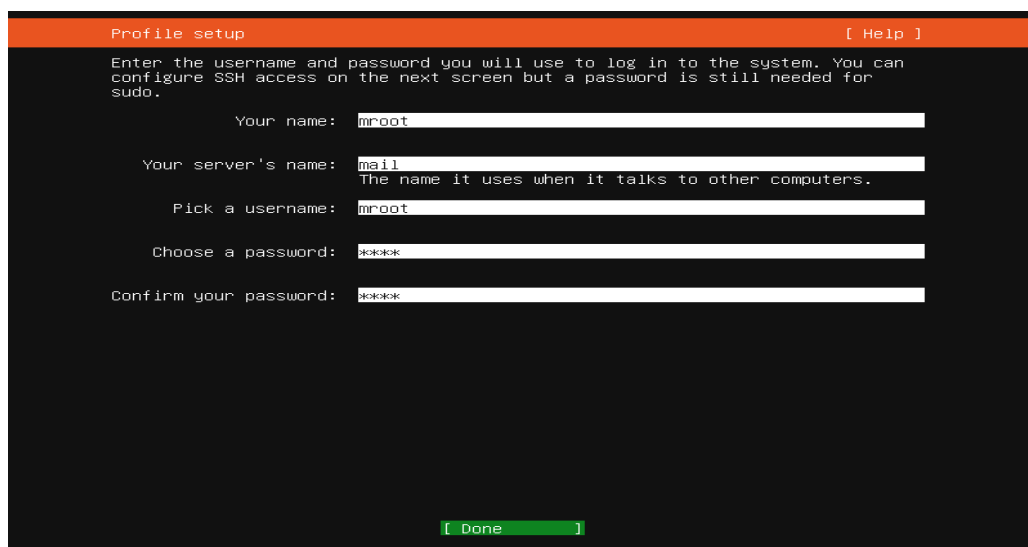


Figure III.4 — Configuration du serveur Ubuntu - configuration du mot de passe pour le super-utilisateur

Ensuite, nous devons définir :

- Nom : mroot descriptif de l'utilisateur que nous allons utiliser dans notre cas, administrateur système.
- Nom du serveur : le nom de la machine, dans notre cas nous allons l'appeler mail.

- Nom d'utilisateur : le nom d'utilisateur, sans espaces ni symboles, nous allons mettre mroot.
- Mot de passe : le mot de passe qui sera utilisé en tant qu'utilisateur root du système, il le demandera à la fois pour entrer et dans les installations ou modifications du système.

6. Mise à jour (fig. III.5)

À cette étape, il est demandé si nous voulons installer le package openssh. Nous dirons non.

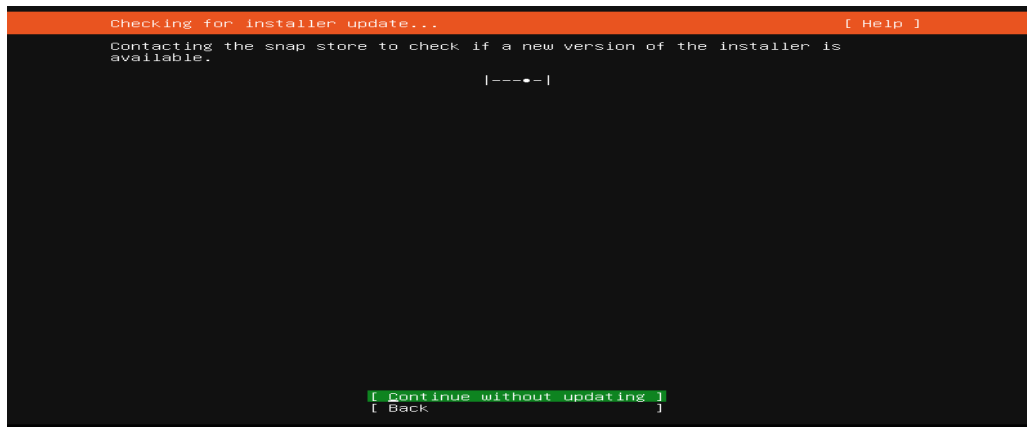


Figure III.5 — Configuration du serveur Ubuntu - mise à jour

7. Installation du système (fig III.6)

En principe, nous n'en sélectionnerons aucun et nous le ferons plus tard dans des installations individuelles.

Une fois l'installation terminée, il installe le système d'exploitation de manière très rapide et il nous demandera de redémarrer en présentant un résumé de l'installation, il nous donnera la possibilité de voir le journal d'installation complet.

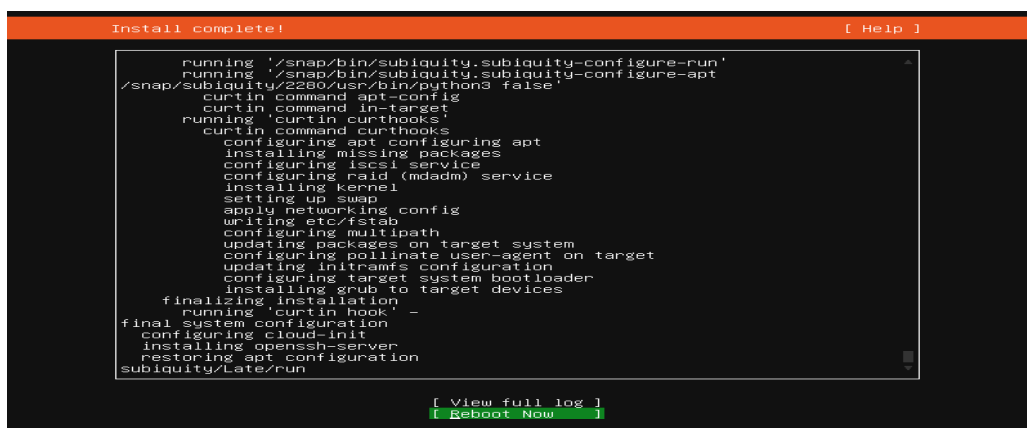


Figure III.6 — Configuration du serveur Ubuntu - installation du système [26]

Si tout s'est bien passé dans l'installation, nous pourrons nous connecter au serveur Ubuntu.

III.2.2.1 Installation du Gnome Vanilla sur Ubuntu 20.04 LTS Focal Fossa

La version Vanilla Gnome est une installation de bureau GNOME propre. Il manque la plupart des logiciels que vous attendez par défaut, mais les besoins en ressources de bureau sont minimales.

Pour installer la version vanille du bureau GNOME, exécutez la commande suivante [27] :

```
sudo apt install gnome-session gdm3
```

La façon la plus simple pour installer le bureau GNOME complet est d'utiliser la *taskel* *command*. Assurez-vous d'abord qu'elle est disponible sur votre système :

```
sudo apt install taskel
```

Ensuite, utilisez la *taskel* *command* pour installer le bureau GNOME :

```
sudo taskel install ubuntu-desktop
```

Une fois terminé, redémarrez le système Ubuntu 20.04 :

```
sudo reboot
```

III.3 Installation et configuration du système de messagerie

L'installation du serveur de messagerie est réalisée en neuf (09) étapes.

1. Création du serveur cloud

Tout d'abord, connectez-vous à votre Projet.dz Cloud Server.

a. Pourquoi cette étape ?

Les ordinateurs et autres appareils du réseau utilisent l'adresse IP pour acheminer une demande vers le site Web auquel le client essaie d'accéder. Cela revient à demander un numéro de téléphone pour appeler la personne que vous essayez d'appeler, mais grâce au DNS, le client ne doit pas garder un répertoire d'adresses IP dans sa poche. Au lieu de cela, il se connecte à un serveur de noms de domaine appelé serveur DNS, ou serveur de

noms, qui exécute une grande base de données liant les noms de domaine a leurs adresses IP.

Que vous essayiez d'accéder a un site Web ou d'envoyer un e-mail, votre ordinateur utilisera le serveur DNS pour rechercher le nom de domaine auquel vous essayez d'accéder. Et le nom correct pour ce processus est : processus de resolution de nom DNS, nous disons donc que le serveur DNS decide d'un nom de domaine pour son adresse IP. Par exemple, lorsque vous saisissez "https://www.mail.projet.dz" dans votre navigateur, une partie du processus de connexion réseau consiste à convertir le nom "mail.projet.dz" en une adresse IP, disons 192.168.43.200 par exemple.

Vous pouvez aussi éviter d'utiliser le DNS en saisissant l'adresse 192.168.43.200 directement dans le navigateur, mais mémoriser mail.projet.dz est bien plus simple que mémoriser une adresse numérique, et cela vous aidera lorsque vous prévoyez de revenir sur le site plus tard, sauf que l'adresse IP peut aussi changer Au fil du temps, il existe certains sites qui allouent plusieurs adresses IP dans un même nom de domaine.

b. Création du serveur

1. Créez un nouveau serveur en choisissant Ubuntu 20.04 comme système d'exploitation avec au moins 2 Go de RAM.
2. Connectez-vous à votre serveur Cloud via SSH et connectez-vous à l'aide des informations d'identification mises en haut de la page.
3. Une fois que vous êtes connecté à votre serveur Ubuntu 20.04, exécutez la commande suivante pour mettre à jour votre système de base avec les derniers packages disponibles.

```
sudo apt-get update -y
```

2. Configuration du nom de l'hôte

Ensuite, vous devrez définir le nom d'hôte de votre serveur. Dans ce cas, nous définirons le nom d'hôte sur mail.projet.dz, comme indiqué ci-dessous :

```
hostnamectl set-hostname mail.projet.dz
```

Ensuite, ouvrez le fichier /etc/hosts et liez l'adresse IP de votre serveur avec le nom d'hôte :

```
nano /etc/hosts
```

Ajoutez les lignes suivantes :

```
GNU nano 4.8 /etc/hosts
127.0.0.1 localhost
127.0.1.1 mail.projet.dz mail
192.168.43.200 mail.projet.dz mail

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Figure III.7 — Installation du serveur de messagerie - liaison de l'adresse IP avec le nom de l'hôte

Enregistrez et fermez le fichier. Ensuite, exécutez la commande suivante pour appliquer les modifications de configuration :

```
hostname -f
```

3. Installation de Apache, MariaDB et PHP

Roundcube nécessite l'installation d'Apache, MariaDB et PHP sur votre serveur.

a. Motivations derrière l'installation de PHP et MySQL

Concrètement, il n'y a pas de raison « absolue » au sens où les alternatives citées sont également des langages performants et qui possèdent certains avantages comme certains inconvénients par rapport au PHP et au MySQL. Cependant, si le couple PHP / MySQL reste de loin le plus célèbre et le choix de référence lorsqu'on veut créer des sites dynamiques et stocker des données, c'est pour de bonnes raisons.

Le premier avantage du PHP concerne la structure de ce langage : c'est un langage à la fois très simple d'accès pour des débutants qui pourront rapidement comprendre sa syntaxe de base et réaliser leurs premiers scripts et qui va également supporter d'un autre côté des structures très complexes.

Ensuite, le PHP est un langage Open Source et donc gratuit. Il est bon de le noter car cela n'est pas forcément automatique même si les utilisateurs du web ont l'habitude du « tout gratuit ». Le PHP est également reconnu et supporté de manière universelle : il va fonctionner quasiment partout et avec l'immense majorité des architectures techniques.

Enfin, le PHP se distingue par ses performances et sa solidité : comme le langage est Open Source, n'importe qui peut contribuer à son évolution, ce qui fait qu'il est sans cesse perfectionné et qu'il ne sera à priori jamais abandonné. En outre, le PHP possède de bonnes performances d'exécution en termes de rapidité et est un langage sûr : les rares failles jamais détectées dans le langage ont toujours été corrigées dans les 24h.

Les systèmes de gestion de base de données sont également nombreux, quoiqu'ils se basent aujourd'hui pour la plupart sur du SQL standard. J'ai choisi dans ce cours d'utiliser le MySQL car c'est encore une fois le choix le plus populaire parmi les développeurs et cela pour de bonnes raisons.

Tout d'abord, il va être totalement compatible avec PHP et utilise une syntaxe SQL standard ce qui facilitera les opérations si un jour vous devez changer de système de gestion de bases de données. Ensuite et enfin le MySQL est à la fois simple d'utilisation, très robuste et offre d'excellente performances que cela soit pour une petite ou pour une grosse structure.

b. Installation de PHP et MySQL

Pour pouvoir installer ces packages, il suffit d'écrire la commande suivante :

```
apt-get install apache2 mariadb-server php libapache2-mod-php php-mysql -y
```

Après avoir installé tous les packages requis, vous devrez activer le module de réécriture Apache pour que Roundcube fonctionne. Vous pouvez l'activer avec la commande suivante :

```
a2enmod rewrite
```

Ensuite, rechargez le service Apache pour appliquer les modifications :

```
sudo system restart apache2
```

4. Installation du certificat SSL de Let's Encrypt

Ensuite, vous devrez installer le certificat SSL de Let's Encrypt Free sur votre serveur pour configurer votre serveur de messagerie avec TLS.

a. Atouts de SSL

Les certificats SSL protègent nos informations confidentielles telles que les informations relatives aux cartes de crédit, les informations de connexion (le nom d'utilisateur, le mot de passe, etc.) Ils permettent également de :

- Sécuriser les données entre les serveurs,
- Améliorer votre classement sur Google,
- Renforcer la confiance des clients,

— Améliorer les taux de conversion.

Toute organisation doit installer le certificat SSL sur son serveur web afin d’initialiser des sessions sécurisées avec les navigateurs. Une fois la connexion sécurisée établie, l’ensemble du trafic entre le serveur et le navigateur sera sécurisé. Il est à noter que quand le certificat est correctement installé sur le serveur, le protocole HTTP devient HTTPS pour signifier ”sécurisé”.

b. Installation de Certbot

Pour installer le client Certbot sur le serveur, il suffit de taper la commande suivante :

```
mroot@mail:~$ sudo apt-get install python3-certbot-apache -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
python3-certbot-apache is already the newest version (0.39.0-1).
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
mroot@mail:~$
```

Figure III.8 — Installation du serveur de messagerie - installation de certbot

c. Installation du certificat SSL

Le téléchargement du certificat SSL gratuit de Let’s Encrypt pour le domaine email.example.com se fait grâce à la commande suivante :

```
sudo certbot certonly --apache -d mail.projet.dz
```

5. Installation et configuration du Postfix

Ensuite, commençons à installer un serveur de messagerie Postfix avec la commande suivante :

```
sudo apt-get install postfix
```

Vous serez redirigé vers l’écran suivant :

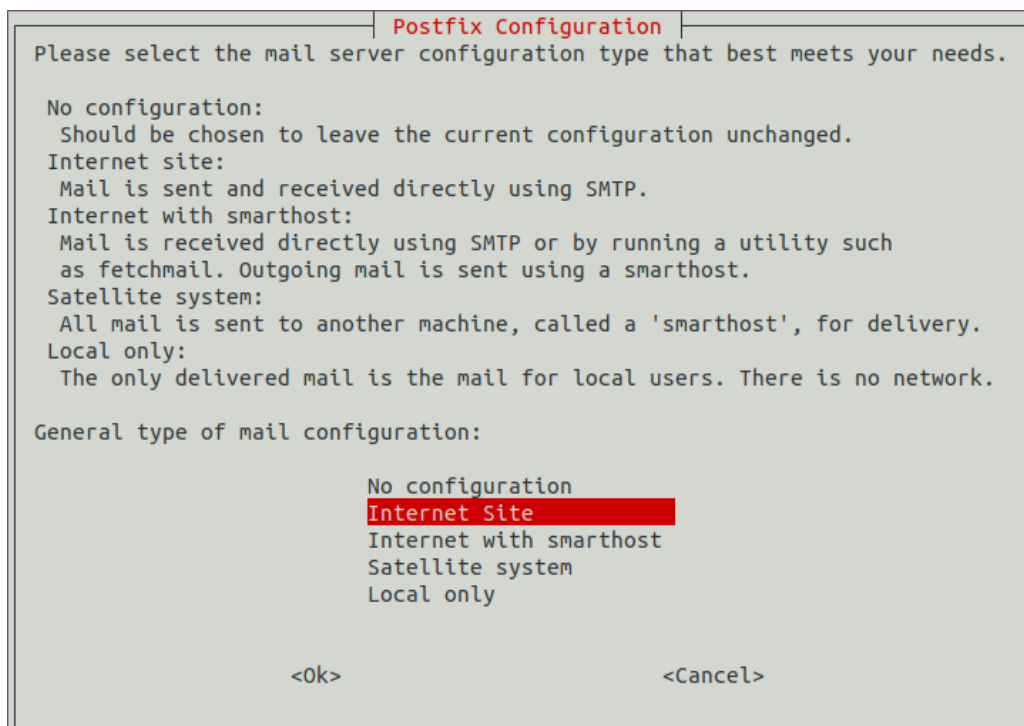


Figure III.9 — Configuration de postfix - redirection

Sélectionnez Site Internet et appuyez sur TAB et Entrée pour continuer. Vous devriez voir l'écran suivant :

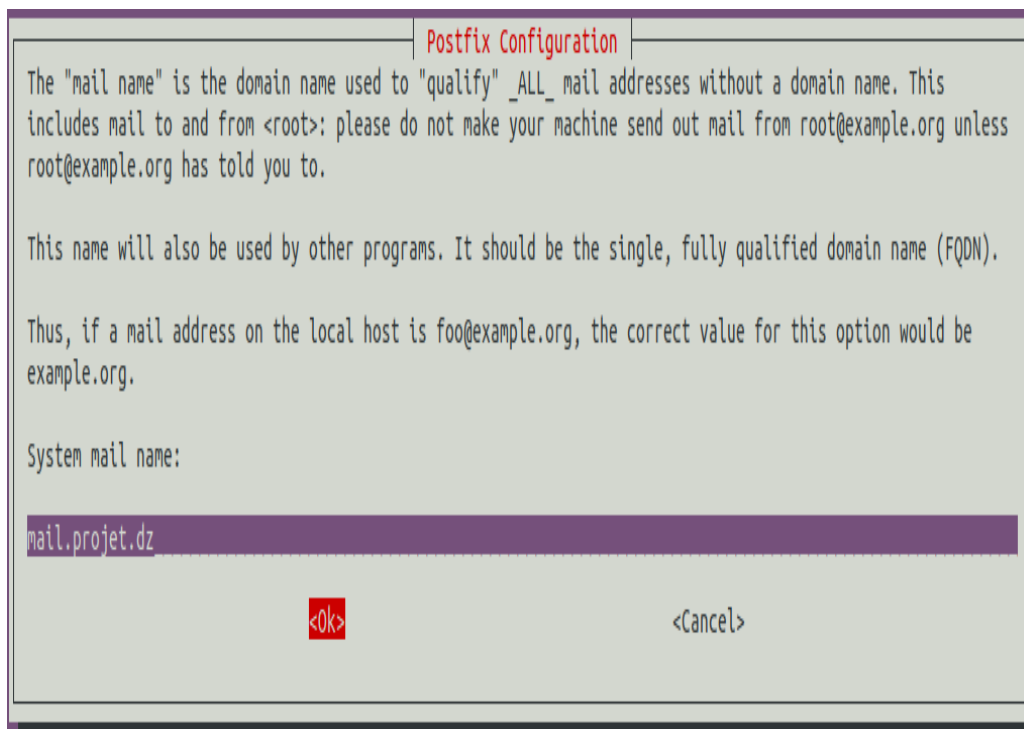


Figure III.10 — Configuration de postfix - sélection du site internet

Fournissez votre nom de domaine et appuyez sur Tab et Entrée pour terminer l'installation.

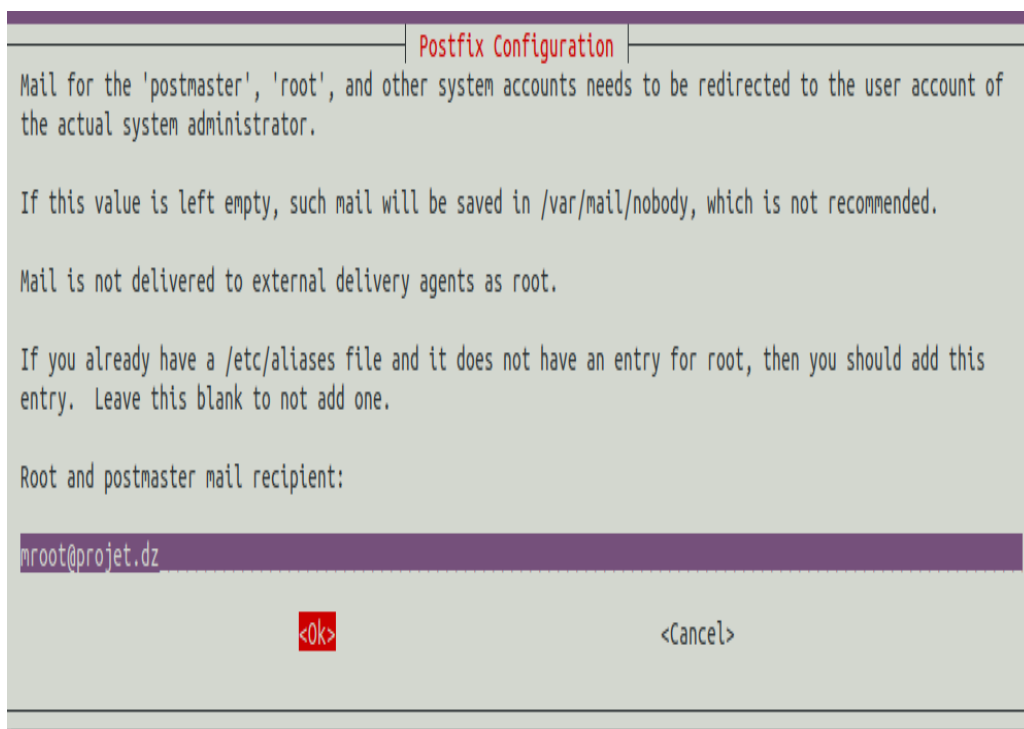
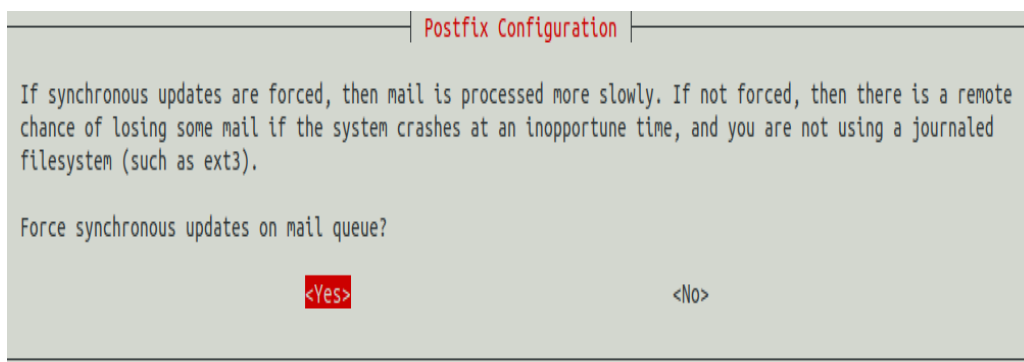
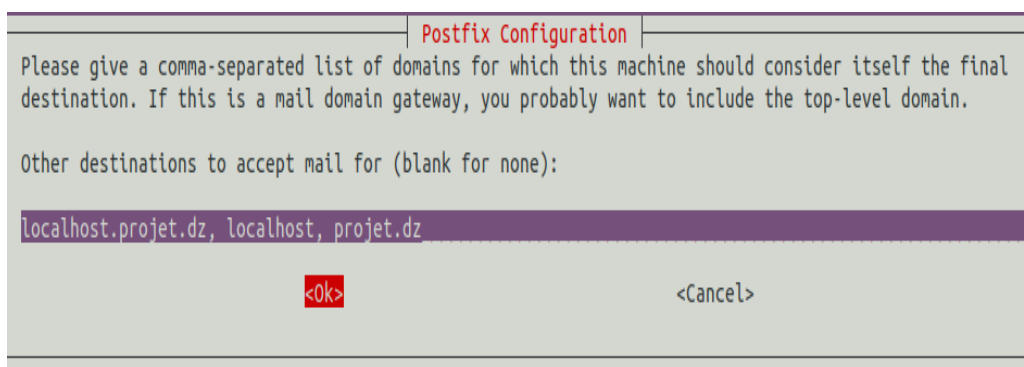


Figure III.11 — Configuration de postfix - fourni du nom de domaine



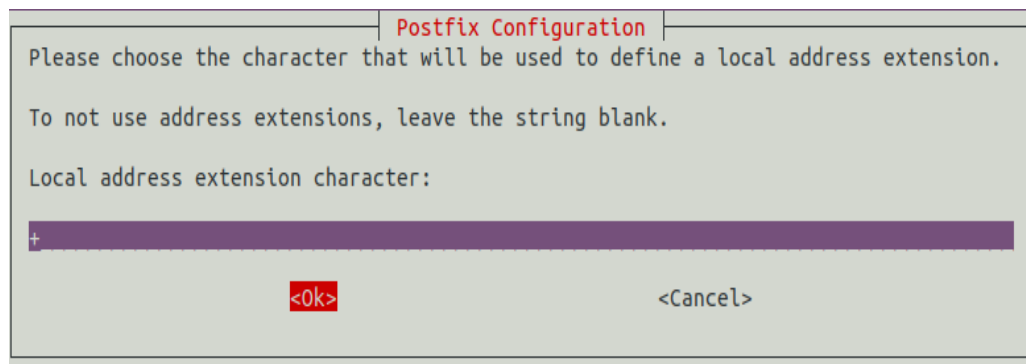
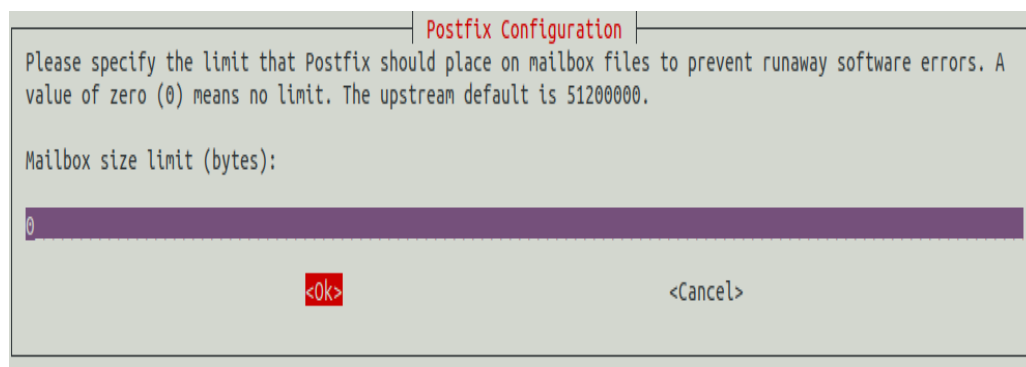
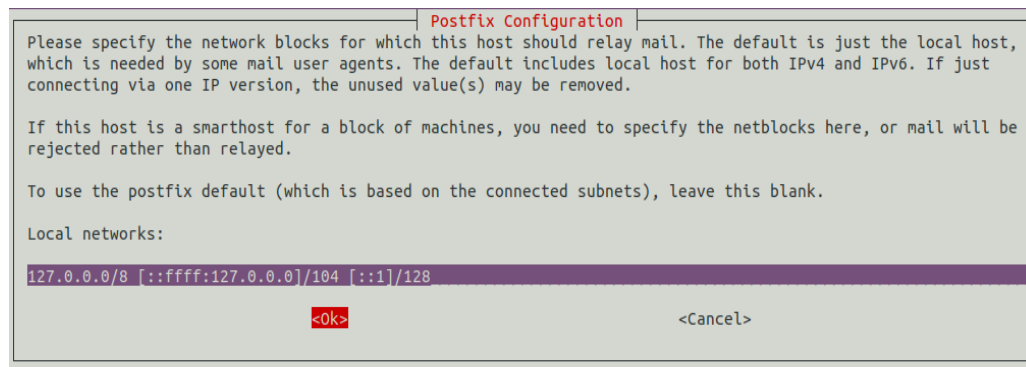


Figure III.12 — Configuration de postfix - étapes de la configuration

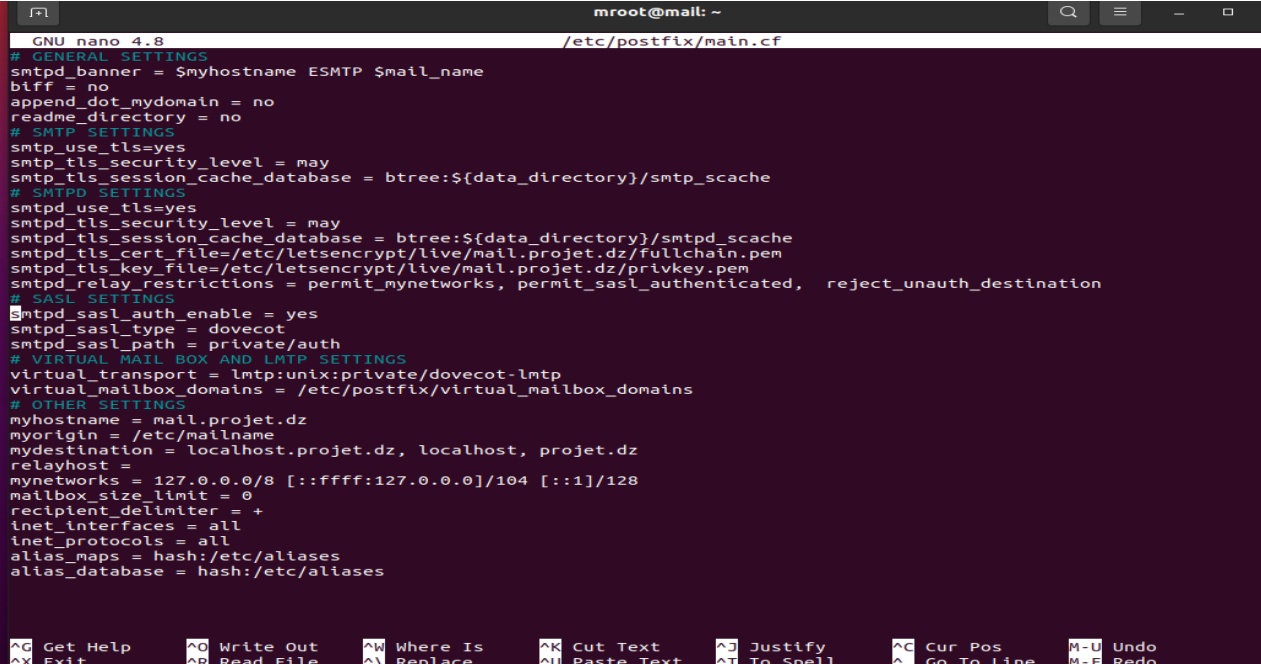
Le fichier de configuration par défaut de Postfix se trouve dans `/etc/postfix/main.cf`. Avant de configurer Postfix, il est recommandé de sauvegarder ce fichier :

```
mv /etc/postfix/main.cf /etc/postfix/main.cf.bak
```

Ensuite, créez un nouveau fichier de configuration Postfix comme indiqué ci-dessous :

```
sudo nano /etc/postfix/main.cf
```

Ajoutez les lignes suivantes :



```

GNU nano 4.8 /etc/postfix/main.cf
# GENERAL SETTINGS
smtpd_banner = $myhostname ESMTP $mail_name
biff = no
append_dot_mydomain = no
readme_directory = no
# SMTP SETTINGS
smtp_use_tls=yes
smtp_tls_security_level = may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
# SMTPD SETTINGS
smtpd_use_tls=yes
smtpd_tls_security_level = may
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtpd_tls_cert_file=/etc/letsencrypt/live/mail.projet.dz/fullchain.pem
smtpd_tls_key_file=/etc/letsencrypt/live/mail.projet.dz/privkey.pem
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, reject_unauth_destination
# SASL SETTINGS
smtpd_sasl_auth_enable = yes
smtpd_sasl_type = dovecot
smtpd_sasl_path = private/auth
# VIRTUAL MAIL BOX AND LMTP SETTINGS
virtual_transport = lmtp:unix:private/dovecot-lmtp
virtual_mailbox_domains = /etc/postfix/virtual_mailbox_domains
# OTHER SETTINGS
myhostname = mail.projet.dz
myorigin = /etc/mailname
mydestination = localhost.projet.dz, localhost, projet.dz
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
^G Get Help      ^O Write Out    ^W Where Is    ^K Cut Text     ^J Justify     ^C Cur Pos     M-U Undo
^X Exit          ^R Read File    ^N Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line   M-E Redo

```

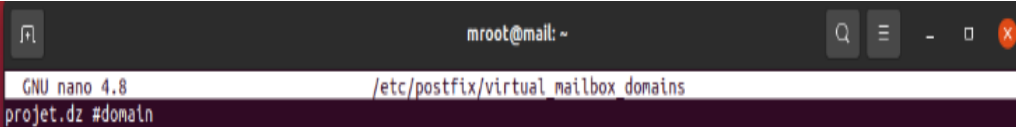
Figure III.13 — Configuration de postfix - modification du fichier de configuration

Enregistrez et fermez le fichier.

Ensuite, vous devrez définir votre domaine dans le fichier `/etc/postfix/virtual_mailbox_domains` :

```
sudo nano /etc/postfix/virtual_mailbox_domains
```

Ajoutez la ligne suivante :



```

GNU nano 4.8 /etc/postfix/virtual_mailbox_domains
projet.dz #domain

```

Figure III.14 — Configuration de postfix - définition du domaine dans le fichier

Enregistrez et fermez le fichier puis convertissez le fichier dans un format que Postfix peut comprendre. Ensuite, modifiez le fichier de configuration principal de Postfix avec la commande suivante :

```
sudo nano /etc/postfix/master.cf
```

Décommentez la ligne suivante **submission inet n**.

Enregistrez et fermez le fichier lorsque vous avez terminé.

6. Installation et configuration de Dovecot

Ensuite, vous devrez installer Dovecot avec les autres packages requis.

L'installation se fait à l'aide de la commande suivante :

```
sudo apt-get install dovecot-care dovecot-imapd dovecot-pop3d dovecot-imtpd -y
```

Ensuite, vous devrez définir l'emplacement du courrier Dovecot pour communiquer avec Postfix et les domaines de boîtes aux lettres virtuelles. Vous pouvez le définir en éditant le fichier `/etc/dovecot/conf.d/10-mail.conf` :

```
sudo nano /etc/dovecot/conf.d/10-mail.conf
```

Trouvez la ligne suivante : `emplacement_mail = mbox : /mail :IN-BOX=/var/mail/%u`

Et remplacez-la par `mail_location = maildir :/var/mail/vhosts/%d/%n`.

Enregistrez et fermez le fichier.

Ensuite, créez le répertoire `vhosts` Dovecot et le sous-répertoire de votre nom de domaine.

```
sudo mkdir /var/mail/vhosts
```

```
sudo mkdir /var/mail/vhosts/projet.dz
```

Ensuite, créez un utilisateur `vmail` et un groupe, et attribuez la propriété des répertoires à l'utilisateur `vmail`.

```
sudo groupadd -g 5000 vmail
```

```
sudo useradd -r -g vmail -u 5000 vmail -d /var/mail/vhosts -c "virtual mail user"
```

```
chown -R vmail :vmail /var/mail/vhosts
```

Ensuite, modifiez le fichier de configuration principal de Dovecot et activez les services sécurisés IMAP et POP3 :

```
sudo nano /etc/dovecot/conf.d/10-master.conf
```

Trouvez les lignes suivantes :

```
inet_listener imaps {
    #port = 993
    #ssl = oui
}
```

Et remplacez-les par les suivantes :

```
inet_listener imaps {
    #port = 993
    #ssl = yes
}
```

Sur le même fichier, cherchez les lignes suivantes :

```
inet_listener pop3s {
    #port = 995
    #ssl = oui
}
```

Et remplacez-les par les suivants :

```
inet_listener pop3s {
    #port = 995
    #ssl = yes
}
```

Ensuite, cherchez les lignes suivantes :

```
service imtp {
    unix_listener lmtp {
        mode = 0666
        ...
    }
}
```

Et remplacez-les par les suivantes :

```
service imtp {
    unix_listener /var/spool/postfix/private/dovecot-lmtp {
        mode = 0600
        ...
    }
}
```

Ensuite, cherchez les lignes suivantes :

```

authentification de service {
  # Postfix smtp-auth
  #unix_listener /var/spool/postfix/private/auth {
    #mode = 0666
  #}
}

```

Et remplacez-les par les suivantes :

```

service imtp {
  unix_listener /var/spool/postfix/private/auth {
    mode = 0666
    ...
  }
}

```

Enregistrez et fermez le fichier lorsque vous avez terminé.

Ensuite, configurez le processus d'authentification Dovecot en éditant le fichier `/etc/dovecot/conf.d/10-auth.conf` :

```
sudo nano /etc/dovecot/conf.d/10-auth.conf
```

Décommentez la ligne suivante (**disable plaintext auth = yes**).

Sur le même fichier, cherchez la ligne suivante (**auth_mechanisms = plain**).

Et remplacez-le par ce qui suit (**auth_mechanisms = plain login**).

Ensuite, commentez la ligne (**include auth-system.conf.ext**) pour désactiver le comportement par défaut de Dovecot pour l'authentification des utilisateurs.

Ensuite, décommentez la ligne (**!include auth-passwdfile.conf.ext**) pour activer la configuration du fichier de mot de passe.

Enregistrez et fermez le fichier lorsque vous avez terminé.

Ensuite, éditez le fichier `/etc/dovecot/conf.d/auth-passwdfile.conf.ext` :

```
sudo nano /etc/dovecot/conf.d/auth-passwdfile.conf.ext
```

Modifiez le fichier comme indiqué ci-dessous :

```

GNU nano 4.8 /etc/dovecot/conf.d/auth-passwdfile
# Authentication for passwd-file users. Included from 10-auth.conf.
#
# passwd-like file with specified location.
# <doc/wiki/AuthDatabase.PasswdFile.txt>

passdb {
  driver = passwd-file
  args = scheme=PLAIN username_format=%u /etc/dovecot/dovecot-users
}
userdb {
  driver = static
  args = uid=vmail gid=vmail home=/var/mail/vhosts/%d/%n
}
  
```

Figure III.15 — Configuration de postfix - modification du fichier d'authentification

Enregistrez et fermez le fichier.

Ensuite, créez un fichier de mot de passe pour l'utilisateur auquel vous souhaitez attribuer un compte de messagerie :

```
sudo nano /etc/dovecot/dovecot-users
```

Ajoutez les lignes suivantes :

```

GNU nano 4.8 /etc/dovecot/dovecot-users
admin@projet.dz:12345
adel@projet.dz:12345
youcef@projet.dz:12345
mroot@projet.dz:0000
  
```

Figure III.16 — Configuration de postfix - lignes à ajouter

Enregistrez et fermez le fichier.

7. Configuration de Dovecot pour l'emploi de SSL

Ensuite, vous devrez configurer Dovecot pour qu'il fonctionne avec SSL. Vous pouvez le faire en éditant le fichier /etc/dovecot/conf.d/10-ssl.conf.

```
sudo nano /etc/dovecot/conf.d/10-ssl.conf
```

Ensuite, recherchez les lignes suivantes :


```
#ssl_cert = </etc/dovecot/dovecot.pem  
#ssl_key = </etc/dovecot/private/dovecot.pem
```

Figure III.17 — Configuration de Dovecot - lignes à modifier

Et remplacez-les par les suivantes :

```
ssl_cert = </etc/dovecot/private/dovecot.pem  
ssl_key = </etc/dovecot/private/dovecot.key
```

Figure III.18 — Configuration de Dovecot - modification du fichier

Enregistrez et fermez le fichier lorsque vous avez terminé, puis redémarrez les services Postfix et Dovecot pour appliquer les modifications de configuration :

```
systemctl restart postfix systemctl restart roundcube
```

8. Installation et configuration de Roundcube

Par défaut, Roundcube est disponible dans le référentiel par défaut Ubuntu 20.04. Vous pouvez l'installer en exécutant simplement la commande suivante :

```
apt-get install roundcube
```

Lors de l'installation, vous serez invité à configurer la base de données. Choisissez l'option souhaitée et appuyez sur Entrée pour terminer l'installation.

Ensuite, vous devrez configurer l'hôte virtuel Apache pour Roundcube. Vous pouvez le faire en éditant le fichier `/etc/apache2/sites-enabled/000-default.conf` :

```
nano /etc/apache2/sites-enabled/000-default.conf
```

Modifiez le fichier comme indiqué ci-dessous :

```
GNU nano 4.8 /etc/apache2/sites-enabled/000-default.conf
<VirtualHost *:80>
  Alias /mail /usr/share/roundcube

  ServerAdmin webmaster@localhost
  DocumentRoot /var/www/html
  ErrorLog ${APACHE_LOG_DIR}/error.log
  CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Figure III.19 — Configuration de Roundcube - modification du fichier

Enregistrez et fermez le fichier, puis redémarrez le service Web Apache pour appliquer les modifications :

```
system restart apache2
```

9. Accès à la messagerie web Roundcube

Maintenant, ouvrez votre navigateur Web et tapez l'URL **http** ://**mail.projet.dz/mail**. Vous serez redirigé vers la page de connexion Roundcube :

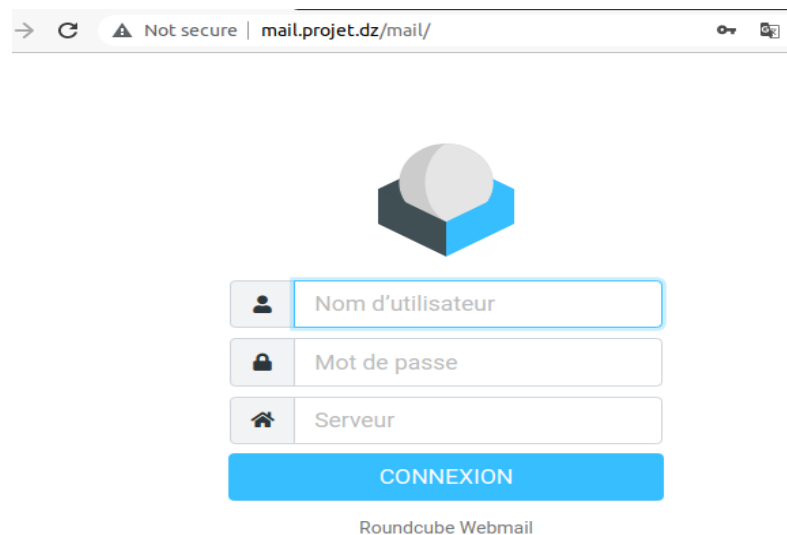


Figure III.20 — Accès à la messagerie web Roundcube - interface de connexion

Fournissez votre nom d'utilisateur et votre mot de passe que vous avez définis dans le

fichier de mots de passe Dovecot et cliquez sur le bouton Connexion. Vous devriez voir le tableau de bord par défaut de Roundcube sur la page suivante :

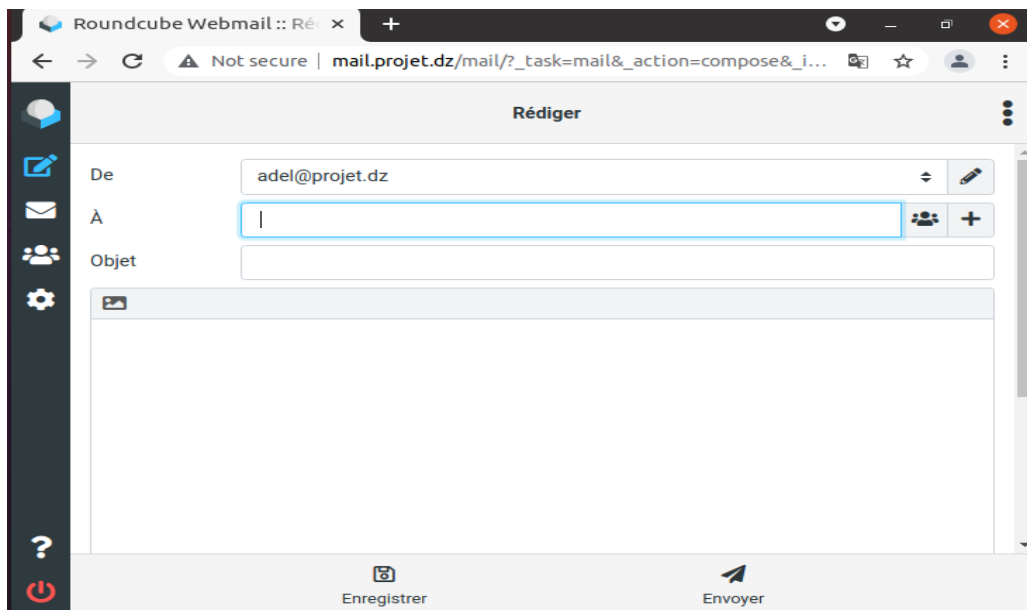


Figure III.21 — Accès à la messagerie web Roundcube - interface principale

Les deux figures suivantes montrent un exemple d'envoi et de réception d'un message en utilisant notre serveur de messagerie.

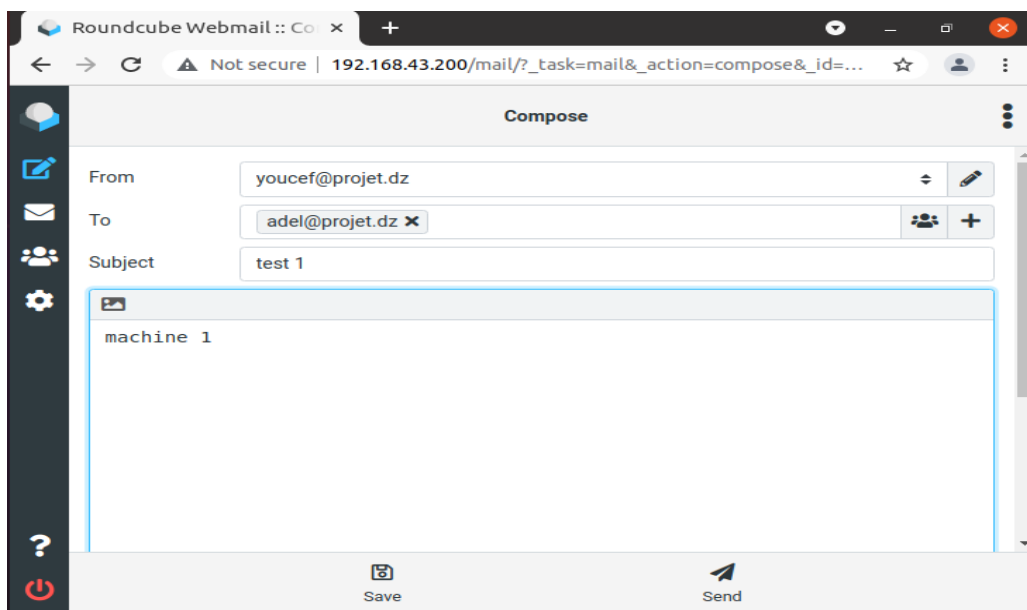


Figure III.22 — Accès à la messagerie web Roundcube - envoi de message

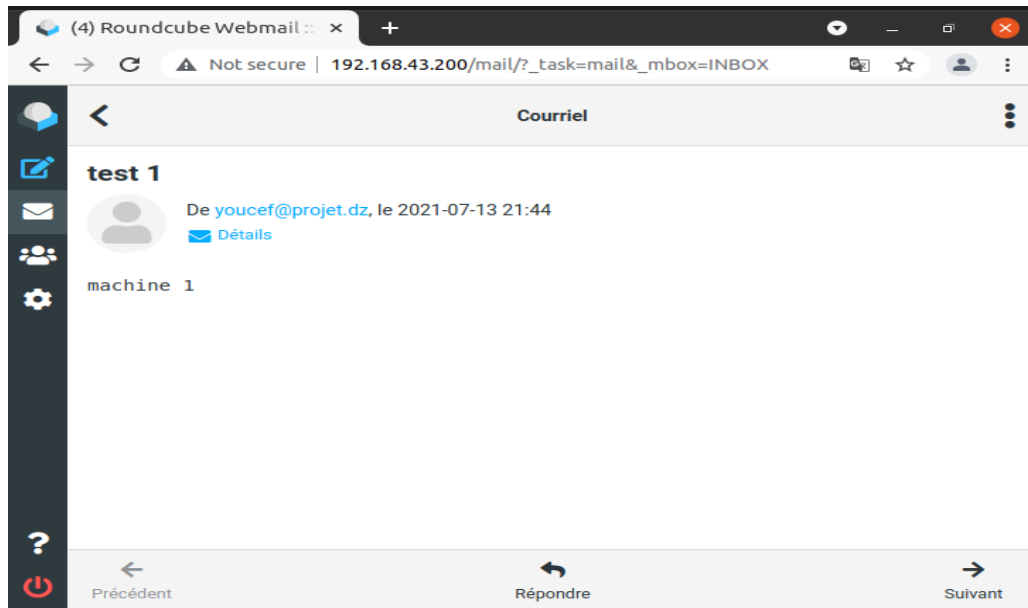


Figure III.23 — Accès à la messagerie web Roundcube - réception de message

III.4 Conclusion

Nous avons dans ce chapitre expliqué les étapes nécessaires pour l'installation et la mise en oeuvre du système de messagerie.

Nous avons dans un premier lieu parlé des outils matériels et logiciels utilisés pour l'établissement du serveur. Ensuite, nous avons détaillé toutes les phases suivies pour sa réalisation.

Conclusion Générale

Nous avons réalisé un système de messagerie qui peut être utilisé dans différents domaines, dans multiples sociétés, ce qui permet de communiquer et de transférer des e-mails, des informations ou des documents, etc. en toute sécurité et confidentialité.

Le système réalisé peut être vu comme un outil de messagerie, dans lequel on peut effectuer un certain nombre d'actions et de tâches :

- Envoi et réception d'e-mails,
- Création d'un calendrier,
- Programmation de réunions et des rendez-vous.

Dans ce mémoire, nous avons commencé d'abord par définir quelques notions relatives aux réseaux, moyens de communication et la sécurité informatique. Deuxièmement, nous avons abordé le concept de serveur de messagerie, nous avons expliqué son architecture et ses composants. Dans un troisième lieu, nous avons expliqué la démarche de mise en œuvre du système.

La démarche que nous avons suivi se constitue de plusieurs étapes dont la première est d'installer et de configurer les agents du serveur ainsi que les outils utilisés.

Ce projet a été une expérience, pour exploiter nos connaissances, nos capacités et pour affronter le domaine professionnel. Par contre, pour maintenir la sécurité d'un système de messagerie il faut être à jour pour couvrir toutes les vulnérabilités qui peuvent avoir lieu.

Le système réalisé est fonctionnel, mais reste perfectible. Nous proposons comme perspectives :

- Mettre le serveur de messagerie comme un relais SMTP.
- Sécuriser l'accès au serveur avec le protocole SSH.

Bibliographie

- [1] S. Tahir, “Client-server architecture,” pp. (15,21–23), Janvier, 2019.
- [2] M. Bertocco, F. Ferraris, C. Offelli, and M. Parvis, “A client-server architecture for distributed measurement systems,” *Instrumentation and Measurement, IEEE Transactions on*, vol. 47, pp. (1143 – 1148), Novembre, 1998.
- [3] A. Miry, *OSI Model*, Octobre, 2018.
- [4] A. Mohammed, *TCP/IP model*, 2014, pp. (19–50).
- [5] M. Aljumaily, “What is the difference between tcp/ip model and osi model?” Mars, 2018.
- [6] S. Fordham, *Routing*, Septembre, 2021, pp. (227–282).
- [7] I. Association and K. Curtin, *Routing*, Janvier, 2013, pp. (39–46).
- [8] M. Radu, “Dns bind server configuration,” *Oeconomics of Knowledge*, vol. 3, 2011.
- [9] L. Wang, X. Zhao, D. Pei, R. Bush, D. Massey, and L. Zhang, “Protecting bgp routes to top-level dns servers,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 14, pp. (851– 860), Octobre, 2003.
- [10] “What is a dhcp server?” <https://www.infoblox.com/glossary/dhcp-server/>, site consulté le 17/08/2021.
- [11] M. Sysel and O. Doležal, “An educational http proxy server,” *Procedia Engineering*, vol. 69, p. (128–132), 2014.
- [12] B. Saugat and N. Sushil, *VPN research (Term Paper)*, 2016.
- [13] V. E. Iskandar Akbar and A. Ansari, “Implementing dmz in improving network security of web testing in stmik akba,” 2019.
- [14] I. Kenneth and F. Stephanie, “Network firewalls,” *IEEE Communications Magazine - IEEE Commun. Mag.*, vol. 32, 1994.
- [15] H. Varsha, “Network address translation,” 2016.

- [16] A. O. M. A. Ramadass Sureswaran, Bazar Hussein and E.-T. Homam, “Active e-mail system smtp protocol monitoring algorithm,” 2009, pp. (257 – 260).
- [17] “What is a dhcp server ?” 2016, <https://www.afternerd.com/blog/smtp> , site consulté le 05/07/2021.
- [18] R. Vladimir, *SMTP (Simple Mail Transfer Protocol)*, 2007, pp. (388–406).
- [19] P. Letta, “Secure transparent authentication for pop3 access,” Février, 2000.
- [20] “What are imap and pop ?” <https://support.microsoft.com/en-us/office/what-are-imap-and-pop>, site consulté le 03/06/2021.
- [21] “Message transfer agent,” 2012, <https://www.techopedia.com/definition/1691/message-transfer-agent-mta>, site consulté le 31/07/2021.
- [22] P. Carlos and C. Ricardo, “A mda approach for agent-oriented development using faml,” 2012, pp. (415–420).
- [23] F. M. Nasrinpour Hamid Reza and M. R., “An agent-based model of message propagation in the facebook electronic social network,” *arXiv :1611.07454 [cs.SI]*, 2016.
- [24] R. Jörg and O. Philipp, “Ssl : a theory of how people learn to select strategies,” *Journal of experimental psychology. General*, vol. 135, pp. (207–236), Juin, 2006.
- [25] K. Philip, *Using SSH*, Aout, 2020, pp. (89–106).
- [26] “Installer ubuntu server,” <https://vivaubuntu.com/installar-ubuntu-server-20-04-lts/>, site consulté le 20/07/2021.
- [27] “Installer gnome sur ubuntu,” <https://goto-linux.com/fr/2020/6/9/comment-installer-gnome-sur-ubuntu-20.04-lts-focal-fossa/>, site consulté le 17/05/2021.

