الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث 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

en Télécommunication
Spécialité : Réseaux & Télécommunications

Karadaniz Hassiba

&

Hocine Zhor

Mise en place d'une architecture DMZ sous packet tracer

Proposé par : Mme Amirouche Nesrine

Année Universitaire 2021-2022

Remerciements

Nous remercions tout d'abord, ALLAH pour la volonté, la force, la santé et la patience qu'il nous a donné afin de réaliser ce travail.

Nous tiendrons à adresser nos plus chaleureux remerciements au notre promotrice Mme Amirouche, pour ses conseils, ses remarques pertinentes et ses contributions considérables tout, au long de la réalisation de ce travail.

Nous adressons également nos vifs remerciements à Mr Mehdi Merouane, pour sa confiance et ses encouragements qui nous ont aidés au cours de notre projet.

Nous sommes également très reconnaissants à Mme Amalou, pour ces précieux aides et conseils pour la réalisation de notre projet.

Nous adressons nos remerciements aux membres de jury d'avoir accepté de juger notre travail.

Nos remerciements s'adressent à tous nos enseignants durant toutes les étapes de notre parcours universitaire.

Nous tenons à saisir cette occasion et adresser nos sincères remerciements et nos profondes reconnaissances à nos familles, qui par leur prière et leur encouragement, on a pu surmonter tous les obstacles.

Nos vifs gratitudes adressées à tous ceux qui nous ont aidées de près ou de loin à élaborer notre mémoire de fin d'études.

Dédicace

J'ai l'honneur de dédier ce modeste travail réalisé grâce à l'aide de Dieu tout puissant :

A Mes très chers parents, Pour les sacrifices déployés à mon égard, Pour leur patience leur amour et leur confiance en moi, Ils ont tout fait pour mon bonheur et ma réussite qu'ils trouvent dans ce modeste travail, le témoignage de ma Profonde affection et de mon attachement indéfectible. Nulle dédicace ne puisse exprimer ce que je leur dois que dieu leur réserve la bonne santé et une longue vie.

A mes chers frères et sœurs pour leurs soutiens et attentions. Ils m'ont permis de réaliser que la famille est sacrée. Ils étaient pour moi, une vraie source d'inspiration et ont été toujours à mes côtés durant les moments difficiles.

A ma chère sœur cousine et binôme Hassiba aucune dédicace ne peut exprimer mon amour et ma gratitude de t'avoir comme sœur. Je ne pourrais jamais imaginer la vie sans toi, tu comptes énormément pour moi, tu es la sœur qui assure sone rôle comme il faut, je n'oublierais jamais ton encouragement et ton soutien le long de nos études, je t'estime beaucoup et je t'aime beaucoup. Je te souhaite beaucoup de succès, de prospérité et une vie pleine de joie et de bonheur.

A tous mes cousins et mes cousines maternelles et paternelles.

A ma tout famille Hocine, Saoudi et Karadaniz, avec tous mes sentiments de respect, d'amour, de gratitude et de reconnaissance pour tous les sacrifices déployés pour m'élever dignement et assurer mon éducation dans les meilleures conditions.

Mes mots ne seraient jamais à la hauteur de l'amour et l'affection que vous m'avez témoignée tout au long de mes études. J'aimerais vous exprimer toute ma gratitude et reconnaissance. Cette dédicace serait pour moi, la meilleure façon de vous honorer et vous montrer à quel point vous avez été magnifique.

Zhor

Dédicace

C'est avec profonde gratitude et sincères mots, que je dédie ce modeste travail :

A mes parents, pour l'amour qu'ils m'ont toujours donné, leurs Encouragements, soutien et leurs prières, et toute l'aide qu'ils m'ont apportée durant mes études. Aucun mot, aucune dédicace ne pourrait exprimer mon respect, ma considération, et mon amour pour les sacrifices qu'ils ont consentis pour mon instruction et mon bien-être. J'espère que dieu leur réserve la bonne santé et une longue vie.

A mes frères et sœurs, pour l'amour et l'affection qui nous unissent. Ils ont partagés avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours. Je prie Dieu le tout puissant de préserver notre attachement mutuel, et d'exaucer tous nos rêves.

A ma chère sœur cousine et binôme Zhor, tu es une personne unique, une frangine merveilleuse, une fille magnifique. Merci pour m'avoir toujours supporté dans mes décisions. Merci pour tout votre amour et votre confiance, pour votre énorme support pendant la rédaction de notre projet. Je t'aime beaucoup ma sœur. Je te souhaite plein de bonheur et de réussite dans ta vie professionnelle et personnelle.

A mon fiancé Sidahmed, je ne saurais exprimer ma profonde reconnaissance pour le soutien continu dont tu as toujours fait preuve. Tu m'as toujours encouragé, incité à faire de mon mieux, ton soutien m'a permis de réaliser le rêve tant attendu.

A tous mes chers cousins et chères cousines maternelles et paternelles.
A tout ma famille karadaniz, Saoudi et Hocine aucun langage ne saurait exprimer mon respect et ma considération pour votre soutenir et encouragements. Je vous dédie ce travail en reconnaissance de l'amour que vous m'offrez quotidiennement et votre bonté exceptionnelle.

Des fois, les mots ne suffisent pas pour exprimer tout le bien qu'on ressent, juste

MERCI à vous. ***Hassiba***

ملخص: يعد مجال شبكات الكمبيوتر مجالًا شاسعًا للغاية، وفي الوقت الحاضر ومع استخدام الشبكات المحلية والإنترنت، ترغب جميع الشركات في الحصول على اتصال موثوق به. أفضل طريقة للتواجد لا تكفي أن يكون لديك اتصال داخلي على الشبكة او على الإنترنت فقط ، ولكن أن يكون لديك بنية جيدة تجمع خدمات الإنترنت للشبكة بأكملها (الويب ، بروتوكول نقل الملفات ، البريد ، ...)تحمى بالشبكة المعزولة . يتطلب هذا إنشاء حسابات مخصصة لهذه الخدمات، ويمكن الوصول إلى هذه الحسابات من قبل عدد معين من الأشخاص على الشبكة. جاء هذا المشروع لدراسة هذه الشبكة.

كلمات المفاتيح: الشبكة المعزولة، شبكة الكمبيوتر.

Résumé : Le réseau informatique est un domaine très vaste. De nos jours et avec l'usage des réseaux locaux et d'internet, les entreprises ont toutes envie d'avoir une communication fiable. Le meilleur moyen d'être efficace une bonne architecture qui rassemble les services Internet (web, ftp, mail,...) pour tout le réseau, qui se situe dans un réseau isolé DMZ. Ceci nécessite de créer des comptes dédiés à ces services, ces comptes sont accessibles par un certain nombre de personnes du réseau. Notre projet fin d'étude s'intègre sur ce domaine

Mots clés : la zone démilitarisé ; réseau informatique.

Abstract : The computer network is a very wide field. Nowadays and with the use of local networks and internet, all companies want to have a reliable communication. The best way to be present is not only to have an international communication on the network, or to have an internet connection, but to have a good architecture which can gathering together all the internet services (web, ftp, mail…) the entire network; witch is situated in an isolated network DMZ. This require creating accounts are accessible by a certain number of people on the network

Keywords : Demilitarized zone ; computer network.

Listes des acronymes et abréviations

DMZ	Demilitarized Zone
LAN	Local Area Network
WAN	Wide Area Network
MAN	Metropolitan Area Network
OSI	International Standards Organisation
TCP	Transmission Control Protocol
IP	Internet Protocol
HTML	L'HyperText Markup Language
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
NAT	Network Address Translation
PAT	Port Address Translation
ACL	Access Control List
ACLs	Access Control Lists
UDP	User Datagram Protocol
PC	Personal Computer
NIC	Network Interface Card
Mbit/s	Mégabit par seconde
Kbit/s	Kilobit par seconde
MAU	Multi-station Access Unit
WWW	World Wide Web
Hub	Concentrateur réseau

Table des matières

Introduction générale 1
Chapitre 1 Généralité sur le réseau informatique 2
1.1 Introduction 2
1.2 Définition d'un réseau 2
1.3 Les composants du réseau 3
1.3.1 Les supports physiques de transmission : 3
1.3.2 Les périphériques finaux 4
1.3.3 Les périphériques intermédiaires 5
1.4 Classification des réseaux 6
1.4.1 Classification selon la taille 6
1.4.2 Classification selon l'organisation 8
1.4.3 Classification selon la topologie 9
1.5 La difference entre un intranet et un extranet 13
1.5.1 Le réseau intranet 13
1.5.2 Le réseau extranet 13
1.6 Modèles OSI et TCP/IP 13
1.6.1 Le modèle OSI 13
1.6.2 Le modèle TCP/IP 14
1.7 Les protocoles réseaux 15
1.7.1 Définition 15
1.7.2 Les différents protocoles réseaux 16
1.8 L'adressage IP 17
1.8.1 Principe de l'adressage 17
1.8.2 Adresse IPv4 18
1.9 Conclusion 19
Chapitre 2 Notions fondamentales sur la sécurité informatique 20
2.1 Introduction 20
2.2 Sécurité informatique 20
2.3 L'administration des réseaux informatique 21
2.3.1 L'administration des utilisateurs 21

2.3.2 L'administration des serveurs 22
2.3.3 L'administration de la machine de transport 22
2.4 Techniques de renforcement de sécurité dans un réseau local 23
2.5 La zone démilitarisée (DMZ) 23
2.5.1 Présentation 23
2.5.2 Définition 24
2.5.3 Objectif de la zone démilitarisée 25
2.6 Les serveurs informatiques 25
2.6.1 Serveur web 25
2.6.2 Serveur messagerie 26
2.6.3 Serveur FTP 27
2.6.4 Serveur DHCP 28
2.6.5 Serveur DNS 28
2.6.6 Serveur Proxy 29
2.7 Le routage dans un réseau informatique 29
2.7.1 Fonctionnement de routage 30
2.7.2 Les modes de routage 31
2.8 NAT & PAT 32
2.8.1 NAT (Network Address Translation) 32
2.8.2 PAT (Port Address Translation) 34
2.9 Les listes de contrôle d'accès (ACL) 34
2.9.1 Définition 34
2.9.2 Fonctionnement des listes de contrôle d'accès : 35
2.9.3 Type des ACLs 36
2.10 Présentation du simulateur CISCO Packet Tracer 37
2.10.1 Construire un réseau 38
2.10.2 Configuration d'un équipement 38
2.10.3 Mode simulation 39
2.11 Conclusion 39
Chapitre 3 Conception et résultats de mise en place 41
3.1 Introduction 41

3.2 Analyse des besoins et étude du projet 41
3.2.1 Présentation de l'architecture 41
3.2.2 Planification des tâches 42
3.3 Mise en œuvre de l'architecture 42
3.4 Configuration des équipements 43
3.4.1 Configuration de la zone Inside 43
3.4.2 Configuration de la zone outside 46
3.4.3 Configuration de la zone DMZ 48
3.4.4 Configuration de routage statique 56
3.4.5 Configuration des listes de contrôle d'accès ACLs 57
3.4.6 Configuration de la traduction des adresses avec le PAT 58
3.5 Test et simulation 59
3.5.1 Test de connectivité 59
3.5.2 Test d'empêchements 61
3.5.3 Test d'accès à internet 63
3.5.4 Test de fonctionnement du serveur FTP 65
3.5.5 Test d'échange de courriel 74
3.5.6 Test du traduction des adresse avec le PAT 77
3.6 Conclusion 78
Conclusion générale 79
Bibliographie 81

Liste des figures

Figure 1.1. Réseau informatique. 3
Figure 1.2. La fibre optique. 3
Figure 1.3. Câble coaxial. 4
Figure 1.4. Câble à paire torsadée. 4
Figure 1.5. Classification des réseaux. 6
Figure 1.6. Réseau local (LAN). 7
Figure 1.7. Réseau métropolitain (MAN). 7
Figure 1.8. Réseau étendu (WAN). 8
Figure 1.9. Architecture Peer to Peer. 9
Figure 1.10. Architecture Client/serveur. 9
Figure 1.11. Topologie en bus. 10
Figure 1.12. Topologie en étoile. 10
Figure 1.13. Topologie en anneau. 11
Figure 1.14. Topologie en arbre. 12
Figure 1.15. Topologie en maillée. 12
Figure 1.16. Modèle OSI et TCP/IP. 15
Figure 1.17.Les classes d'adresse IPv4. 18

Figure 2.1. Topologie de l'administration de réseau. 21
Figure 2.2. La zone démilitarisée. 24
Figure 2.3. La DMZ en informatique. 25
Figure 2.4. Le service web. 26
Figure 2.5. L'acheminement d'un courriel. 27
Figure 2.6. Fonctionnement du service FTP. 27
Figure 2.7. Fonctionnement du service DHCP. 28
Figure 2.8. Principe d'une requête DNS. 29
Figure 2.9. Le serveur proxy. 29
Figure 2.10. Fonctionnement d'un routage. 30
Figure 2.11. Exemple de NAT. 33
Figure 2.12. Exemple de PAT. 34
Figure 2.13. L'interface du simulateur Cisco Packet Tracer. 37
Figure 2.14. Type d'équipement Cisco. 38
Figure 2.15. Les différentes connexions. 38
Figure 2.16. Partie simulation. 39

Figure 3.1. Architecture d'un réseau informatique avec DMZ. 42
Figure 3.2. L'architecture de notre réseau. 43

Figure 3.3.Configuration du serveur DHCP. 44
Figure 3.4. Activation du service DHCP. 45
Figure 3.5.L'attribution des adresses. 45
Figure 3.6. Configuration du serveur DHCP. 46
Figure 3.7. Activation du service DHCP. 47
Figure 3.8. L'attribution des adresses. 47
Figure 3.9. Configuration du serveur elearning.univ-blida. 49
Figure 3.10. Configuration du serveur DNS pour un nom (www.elearning.univ-blida.dz). 50
Figure 3.11 Configuration du PC de la cliente ''Zhor''. 51
Figure 3.12. Configuration du PC de la cliente ''Karadaniz'' 52
Figure 3.13. Configuration du PC de la cliente ''Hassiba''. 52
Figure 3.14. Configuration du serveur messagerie pour la cliente ''Zhor''. 53
Figure 3.15. Configuration du serveur messagerie pour la cliente ''Karadaniz'' 54
Figure 3. 16 . Configuration du serveur messagerie pour la cliente ''Hassiba''. 54
Figure 3.17. Configuration du serveur FTP. 55
Figure 3. 18. Configuration du l'interface DMZ. 56
Figure 3.19. La route statique de réseau outside vers le réseau DMZ. 56
Figure 3.20. La route statique de réseau inside vers le réseau DMZ. 57
Figure 3.21. La route statique de réseau inside vers le réseau DMZ. 57
Figure 3.22. Configuration des ACLs pour bloquer l'accès au serveur elearning.univ-blida. 57
Figure 3.23. Configuration des ACLs pour bloquer le pinge entre la zone inside et la zone de DMZ. 58
Figure 3.24. Configuration des ACLs pour bloquer le pinge entre la zone outside et la zone de DMZ. 58
Figure 3.25. Configuration de la traduction des adresses avec le PAT. 59
Figure 3.26. Test de connectivité entre inside et la DMZ. 59
Figure 3.27. Test de connectivité entre inside et outside. 60
Figure 3.28. Test de connectivité entre DMZ et outside. 61
Figure 3.29. Test de l'empêchement de la connectivité entre Inside et DMZ. 62
Figure 3.30. Test de l'empêchement de connectivité entre outside et DMZ. 63
Figure 3.31. Test de blocage l'accès au serveur elearning-univ.blida. 64
Figure 3.32. Test d'accès au serveur elearning.univ-blida. 65
Figure 3.33. Demande d'accès serveur FTP. 66
Figure 3.34. L'accès au serveur FTP. 66
Figure 3.35. Le contenu d'un répertoire du serveur FTP. 67
Figure 3.36. Vérification des fichiers du répertoire du serveur FTP. 68
Figure 3.37. L'enregistrement de fichier. 68
Figure 3.38. Téléchargement de fichier vers le serveur. 69
Figure 3.39. Vérification que le fichier.txt est au répertoire du serveur FTP. 69

Figure 3.40. L’accès au répertoire http. 70
Figure 3.41. Création d’un fichier html. 70
Figure 3.42 .L’enregistrement du fichier html. 71
Figure 3.43. Téléchargement de fichier html vers le serveur. 71
Figure 3.44. Vérification que le fichier html est au répertoire du serveur http. 72
Figure 3.45. Le contenu du fichier test.html. 73
Figure 3.46. L’affichage de la page test.html. 73
Figure 3.47. La composition d’un e-mail. 74
Figure 3.48. La réception de l’email. 75
Figure 3. 49. La composition d’un e-mail. 76
Figure 3.50. La réception de l’email. 76
Figure 3.51. Les résultats de débogage. 77

Liste des tableaux

Tableau 1.1. Les couches de modèle OSI. 14
Tableau 1.2. Les couches de modèle TCP/IP. 15
Tableau 1.3.Les classes de plage d'adressage. 19

Tableau 2.1.La comparaison entre le routage statique et le routage dynamique. 32

Tableau 3.1. Planification des tâches. 42
Tableau 3.2. Matériels utilisés. 43
Tableau 3.3. Les adresses pour chaque serveur. 48
Tableau 3.4. Les adresses des interfaces des routeurs. 56

Introduction générale

Depuis l'existence des êtres humains sur terre, ils n'ont jamais arrêté de trouver des moyens plus développés pour communiquer entre eux (gestes, symboles, dessins…etc.).A travecrs les siècles successifs, l'Homme a fait des efforts afin de trouver des méthodes de communication plus avancées.

De nos jours, la ommunication s'effectue via les réseaux informatiques qui permettent et facilitent les échanges des informations à l'intérieur et à l'extérieur des entreprises à travers les réseaux locaux LAN (Local Area Network) et les réseaux étendus WAN (Wide Area Network) et MAN (Metropolitan Area Network).

Pour garantir la confidentialité et la fiabilité des informations échangées et se prémunir des attaques et intrusions externes, nous allons mettre en place une architecture DMZ (Demilatarizate zone) sous logiciel packet tracer. L'objectif de ce travail est de proposer une architecture qui permette une communication sécurisée entre différents postes, de gérer les équipements hôte à hôte, de filtrer les paquets à travers les ACLs (Access Control List).

Notre mémoire est structuré en trois chapitres, le premier intitulé « généralités sur les réseaux informatiques», a pour but de donner des généralités sur les différents éléments constituant d'un réseau. Le deuxième chapitre présente des « Notions fondamentales sur la sécurité informatique » dans l'objectif de renforcer le niveau de sécurité du réseau local de l'entreprise via l'ensemble des serveurs au niveau de la DMZ. Le troisième chapitre consiste à mettre en place l'architecture DMZ sous PACKET TRACER, il sera entièrement consacré aux solutions envisagées pour l'obtention d'un niveau de sécurité optimale: la DMZ, ACLs, PAT (Port Address Translation); et aussi dédié aux différentes simulations, tests et implémentations, et enfin nous avons une conclusion et des perspectives.

Chapitre 1 Généralité sur le réseau informatique

1.1 Introduction

De nos jours, les réseaux informatiques sont devenus indispensables, pratiquement dans tous les domaines de la vie : banques, assurance, sécurité, internet, santé, administration, transport, ... Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages, partage de ressources (imprimante, disque dur, internet), transfert de fichiers, consultation de bases de données, gestion de transactions, télécopie ...

Dans ce chapitre nous allons présenter différentes généralités sur lesquelles sont basées la réalisation d'un réseau informatique et le bon fonctionnement de ses éléments.

1.2 Définition d'un réseau

Un réseau est un ensemble d'éléments reliés entre eux et réglés de manière qu'ils puissent communiquer. Les équipements interconnectés peuvent être des ordinateurs, des stations de travail, des terminaux ou des appareils de stockage.

Il existe deux types de réseaux :

- Le réseau filaire : c'est un réseau qui utilise une connexion avec fil, il utilise des câbles pour relier des ordinateurs et des périphériques entre eux.
- Le réseau sans fil : c'est un réseau qui n'utilise pas de câbles, c'est une technique qui permet aux particuliers, aux réseaux de télécommunications et aux entreprises de limiter l'utilisation de câbles entre divers localisation. [1]

Figure 1.1. Réseau informatique [28].

1.3 Les composants du réseau

1.3.1 Les supports physiques de transmission :

a Fibre optique

La fibre optique est un fil en verre ou en plastique très pur et transparent, à la fois flexible et très fin. Les câbles à fibre optique transmettent les données sur de plus longues distances et avec une bande passante plus large que n'importe quel autre support réseau. Contrairement aux fils en cuivre, les câbles à fibre optique peuvent transmettre des signaux avec moins d'atténuation, et ils sont entièrement protégés contre les perturbations électromagnétiques et radioélectriques. La fibre optique est couramment utilisée pour relier les périphériques réseau [2].

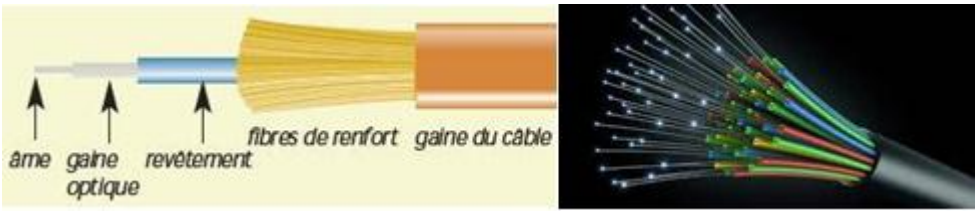

Figure 1.2. La fibre optique [29] [30].

b Câble coaxial

Le câble coaxial est un type de ligne de transmission, utilisé pour transporter des signaux électriques à haute fréquence avec des faibles pertes. Le fil de cuivre est entouré une couche isolante et au pourtour se trouve une couche protectrice, qui

permet de protéger les données transmises contre les bruits extérieurs constitué d'une tresse métallique en cuivre ou en aluminium. L'ensemble : tresse métallique, isolant et câble conducteur sont entourés d'une gaine isolante en matière plastique [3].

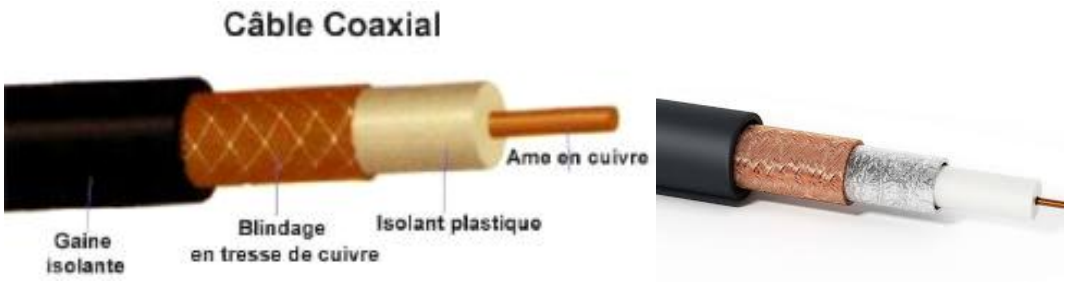

Figure 1.3. Câble coaxial [31] [32].

c Paire torsadé

Le câblage en cuivre est le type de câblage le plus courant dans les réseaux d'aujourd'hui. Il se compose d'une ou plusieurs paires de câble en cuivre fin de 1mm de diamètre entouré d'isolant, et l'ensemble des paires est enfermé dans une gaine protectrice. Les supports en cuivre sont utilisés sur certains réseaux, car ils fonction bien, faciles à installer et qu'ils présentent une faible résistance au courant électrique. Cependant, les supports en cuivre sont limités par la distance et les interférences du signal [4].

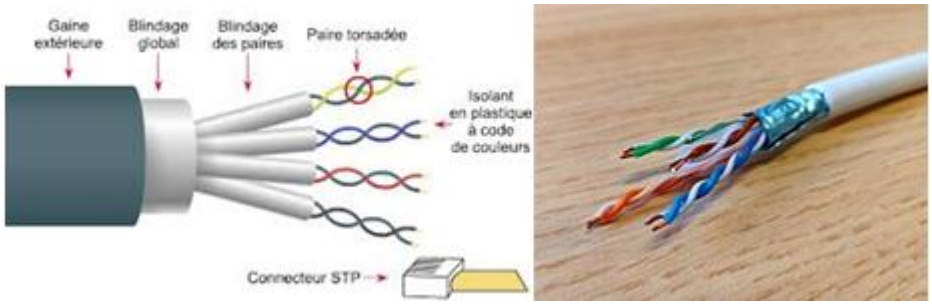

Figure 1.4. Câble à paire torsadée [33] [34].

1.3.2 Les périphériques finaux

a Les Hôtes

Tous les ordinateurs connectés à un réseau et qui participent directement aux communications transmises sur le réseau sont des hôtes. Ces derniers sont également appelés des périphériques finaux ou bien des clients. L'hôte est identifié par une adresse IP et le réseau auquel il est connecté [5].

b Les serveurs

Les serveurs sont des ordinateurs équipés par des logiciels qui permettent de fournir des informations, comme des messages électroniques ou des pages web, à d'autres périphériques finaux sur le réseau. Chaque service nécessite un logiciel serveur distinct. Par exemple, un serveur nécessite un logiciel de serveur web pour pouvoir offrir des services web au réseau. Un ordinateur équipé d'un logiciel serveur peut fournir des services à un ou plusieurs clients en même temps [5].

1.3.3 Les périphériques intermédiaires

a Les routeurs

Le routeur permet d'interconnecter deux réseaux de type différents. Il travaille au niveau de la couche 3 du modèle OSI, et s'occupe du routage des unités de données. C'est l'outil le plus élaboré pour les acheminer entre les réseaux [6].

b Les commutateurs (Switch)

Le commutateur réseau est un équipement qui permet de connecter plusieurs appareils sur un même réseau. Il est capable de connaître l'adresse physique des machines qui sont connectés avec lui, et d'analyser les trames reçues pour les diriger vers la machine de destination, il travaille au niveau 2 du modèle OSI [7].

c Les cartes réseaux

La carte réseau (appelée Network Interface Card en anglais et notée NIC) constitue l'interface (Port) entre l'ordinateur et le réseau. La fonction d'une carte réseau est d'assurer les échanges et les transferts des données entre les appareils présents sur le réseau [6].

d Les passerelles

La passerelle (en anglais Gateway) est un système matériel et logiciel, qui permet de faire la liaison entre plusieurs réseaux de protocoles différents. Elle permet aussi de manipuler les données afin de pouvoir assurer le passage d'un type de réseau à un autre [8].

1.4 Classification des réseaux

Il existe différents types de niveaux de classification des réseaux, on peut les distingue selon : la taille, l'organisation et la méthode d'accès.

1.4.1 Classification selon la taille

La figure (1.5) montre les différents types de réseau selon la taille.

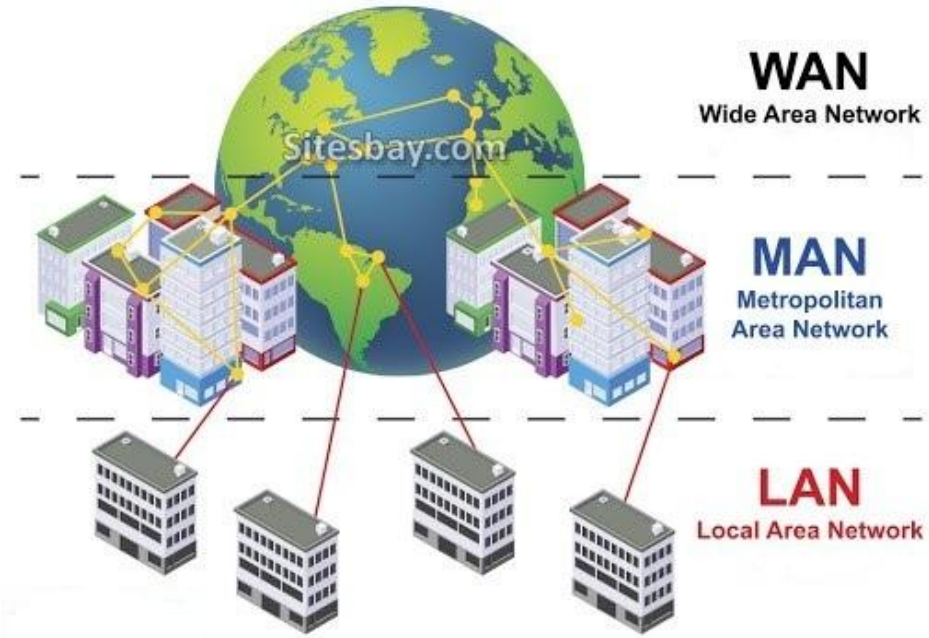

Figure 1.5. Classification des réseaux [35].

On adopte la terminologie suivante :

a LAN (Local Area Network)

Un type de réseau informatique qui traite généralement une petite zone, et principalement limité à un seul endroit avec des débits de quelques dizaines de Mbit/s jusqu'à quelques centaines [9].

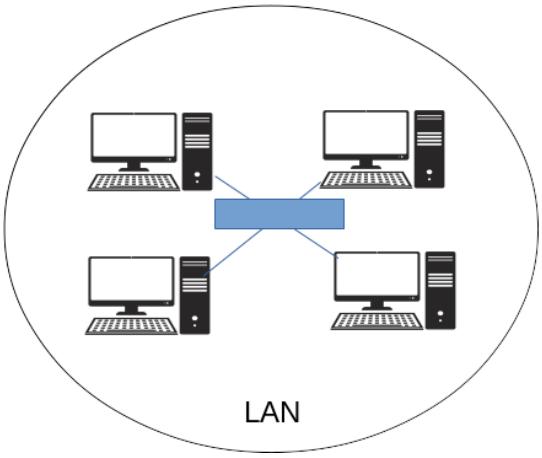

Figure 1.6. Réseau local (LAN) [36].

b MAN (Metropolitan Area Network)

Man est un intermédiaire entre LAN et WAN. Il s'étend sur une centaine de kilomètres, et dispose d'un plus grand nombre d'ordinateurs. Et il peut également être vu comme une combinaison de plusieurs réseaux locaux [10].

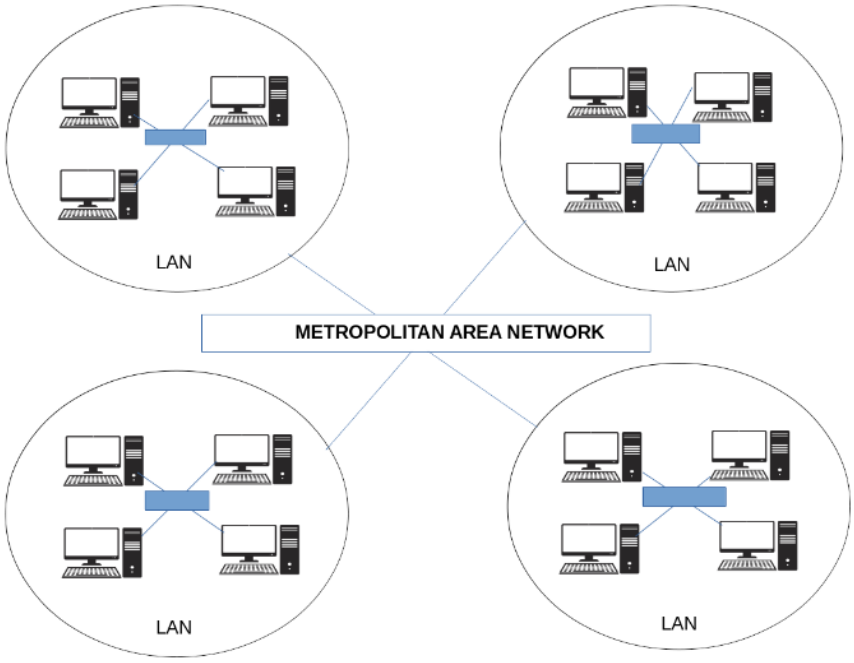

Figure 1.7. Réseau métropolitain (MAN) [36].

c WAN (Wide Area Network)

Ces réseaux assurent généralement le transport de l'information sur une grande distance qui permet de connecter plusieurs LAN éloignées entre eux. Les débits sont très variables de quelques Kbit/s à quelques Mbit/s [10].

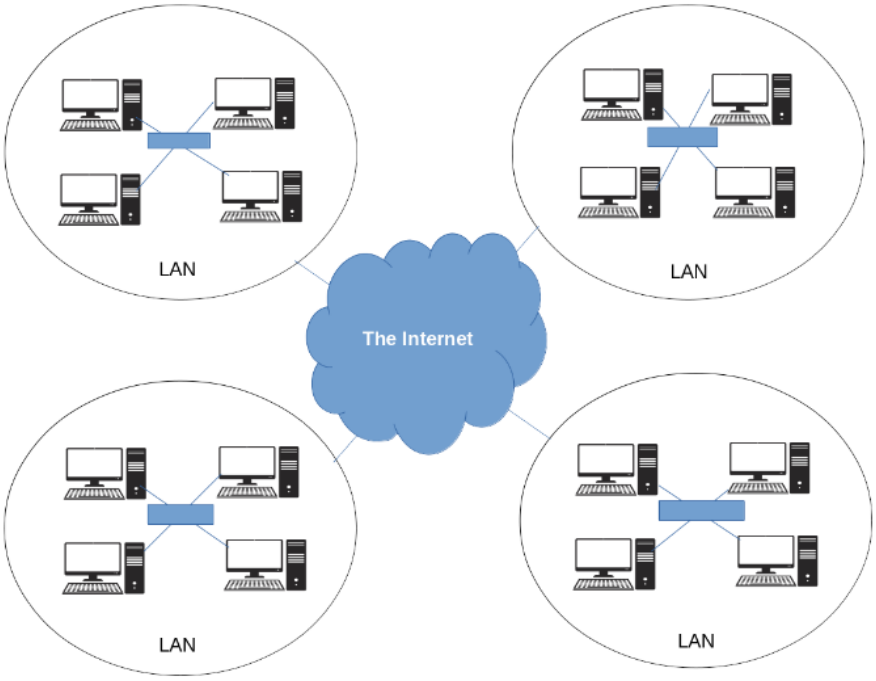

Figure 1.8. Réseau étendu (WAN) [36].

1.4.2 Classification selon l'organisation

a Peer to Peer

Les systèmes pair à pair (en l'anglais "peer-to-peer") sont composés d'un ensemble d'entités partageant un ensemble de ressources, et jouant à la fois le rôle de serveur et de client. Ils permettent une réduction des coûts [11].

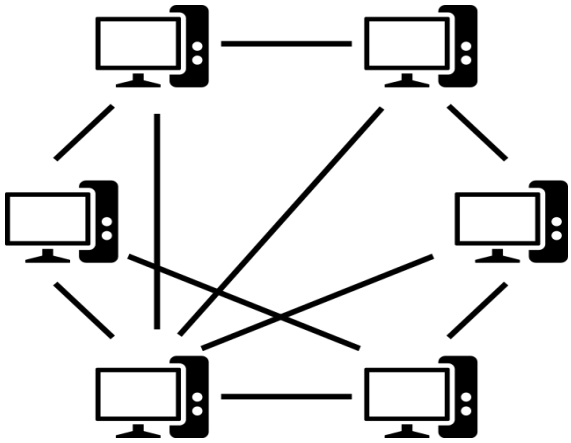

Figure 1.9. Architecture Peer to Peer [37].

b Client-serveur

L'architecture client/serveur désigne un mode de communication entre plusieurs ordinateurs d'un réseau qui distingue un ou plusieurs postes clients du serveur, chaque logiciel client peut envoyer des requêtes à un serveur. Un serveur peut être spécialisé en serveur d'applications, de fichiers, de terminaux, ou encore de messagerie électronique [12].

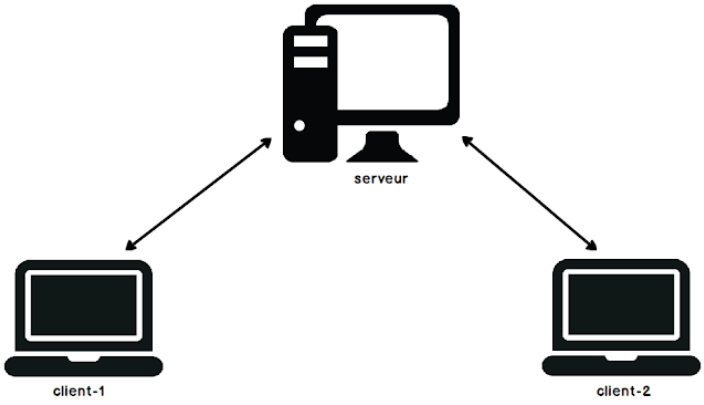

Figure 1.10. Architecture Client/serveur [37].

1.4.3 Classification selon la topologie

Un réseau informatique est constitué de plusieurs ordinateurs reliés entre eux grâce aux matériaux (câblage, cartes réseau, ainsi que d'autres équipements permettant d'assurer la bonne circulation des données). L'arrangement physique de ces éléments est appelé topologie physique. Il existe plusieurs topologies tels que :

a Topologie en bus

Le mot "bus" indique la ligne physique qui relie les périphériques du réseau. Dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission via un câble, généralement câble coaxial [13].

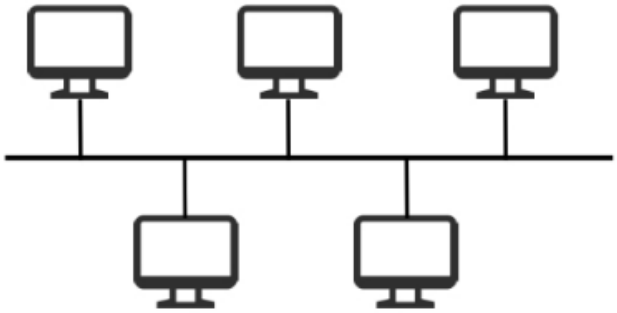

Figure 1.11. Topologie en bus [38].

Cette structure se caractérise par sa facilité de mise en œuvre et son fonctionnement simple et économique en terme. D'autre part, elle n'est pas fiable car si l'une des connexions est défectueuse, alors l'ensemble du réseau sera affecté.

b Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés avec hub ou un concentrateur.

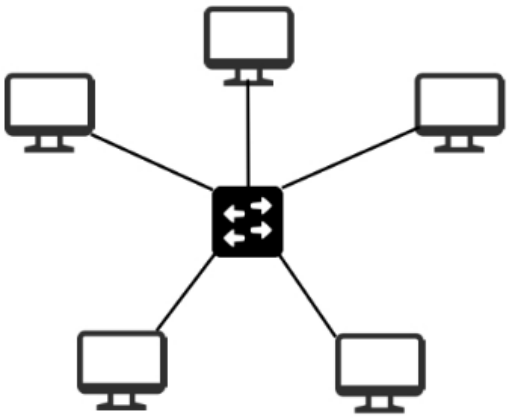

Figure 1.12. Topologie en étoile [38].

Les réseaux qui ont une topologie en étoile sont beaucoup moins vulnérables, car on peut facilement retirer une connexion en la débranchant du concentrateur sans

paralyser le reste du réseau. De plus, les administrations de ce type de réseau sont faciles (grâce au nœud central). En revanche un réseau à topologie en étoile est plus cher que le réseau à topologie en bus car un matériel supplémentaire est nécessaire (le hub) [13].

c Topologie en anneau

Dans un réseau en topologie en anneau, les ordinateurs sont situés sur une boucle fermée et communiquent chacun à leur tour.

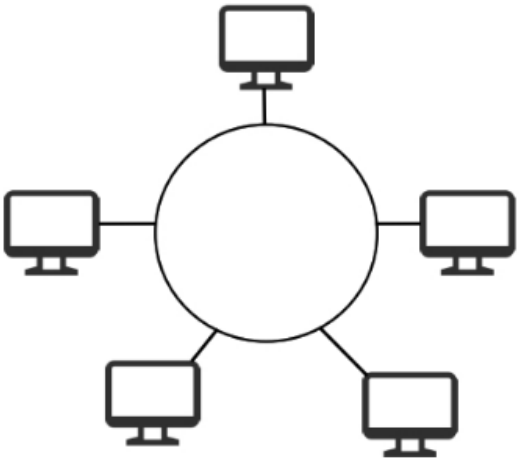

Figure 1.13. Topologie en anneau [38].

En réalité, dans une topologie anneau, les ordinateurs ne sont pas reliés en boucle, mais ils sont reliés à un répartiteur (appelé MAU, Multi-station Access Unit) qui va gérer la communication entre les ordinateurs, qui lui sont reliés en attribuent à chacun d'entre-deux un temps de parole [13].

d Topologie en arbre

Elle est également appelée topologie hiérarchique. Chaque ordinateur est relié à d'autres ordinateurs qui sont aussi des nœuds. Le réseau est donc divisé en niveaux. Le sommet, de haut niveau, est connecté à plusieurs nœuds de niveau inférieur. [13].

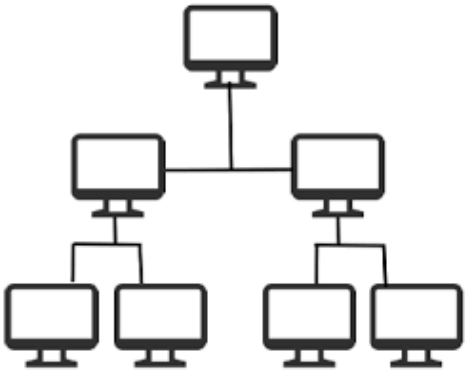

Figure 1.14. Topologie en arbre [38].

e Topologie maillée

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à de nombreuses liaisons point à point. Chaque ordinateur est relié à tous les autres. L'inconvénient est le nombre de liaisons nécessaires qui devient très élevé. Cette structure se retrouve dans les grands réseaux de distribution (Exemple : Internet). L'information peut être envoyée sur le réseau suivant des chemins divers, sous le contrôle de puissants superviseurs de réseau, ou grâce à des méthodes de routage réparties [13].

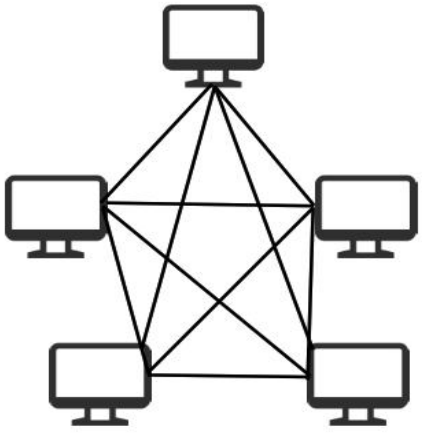

Figure 1.15. Topologie en maillée [38].

1.5 La difference entre un intranet et un extranet

On parle souvent d'internet mais il existe d'autres types de réseaux utilisés au quotidien, à savoir l'intranet et l'extranet. Les principaux utilisateurs de réseaux intranet et extranets sont les organisations professionnelles et plus particulièrement les entreprises [50].

1.5.1 Le réseau intranet

Un réseau intranet est un réseau local interne à une entreprise dont l'utilisation s'apparente à celle d'internet puisqu'il fonctionne avec la même technologie. Son principal intérêt réside dans le partage d'informations et de documents en interne. Il est normalement accessible avec ou sans connexion à internet. Cependant, le réseau reste totalement privé et fermé aux connexions publiques [50].

1.5.2 Le réseau extranet

Un réseau extranet se destine quant à lui au partage d'informations avec des acteurs externes à l'entreprise. Il est accessible depuis n'importe quel appareil connecté à internet. Son utilisation est filtrée grâce à une identification par mot de passe. L'extranet permet d'ouvrir le système d'informations d'une entreprise à des partenaires extérieurs : clients, fournisseurs, filiales… [50].

1.6 Modèles OSI et TCP/IP

1.6.1 Le modèle OSI

Le modèle OSI explique la manière dont les données transitent à travers les différentes couches de et vers les différents d'équipements du réseau. Le modèle OSI comporte sept couches : Physique, Liaison de données, Réseau, Transport, Session, Présentation et Application. Chaque couche est constituée d'éléments matériels et logiciels et offre un service à la couche située immédiatement au-dessous d'elle. Chaque couche ''n'' d'une machine gère la communication avec la couche n d'une autre machine en suivant un protocole de niveau n qui est un ensemble de règles de communication pour le service de niveau n [14].

Couchette du modèle OSI	La dispersion
7- Application	La couche application contient les protocoles utilisés pour les processus de communication.
6- Présentation	La couche de présentation permet une représentation commune des données transférées entre les services de couche d'application.
5- Session	La couche de session fournit des services à la couche de présentation pour organiser son dialogue et gérer l'échange de données.
4- Transport	La couche transport définit les services à segmenter, à transférer et à réassembler les données pour les communications individuelles entre les terminaux.
3- Réseau	La couche réseau fournit des services permettant d'échanger les différents éléments de données individuels sur le réseau entre les dispositifs identifiés.
2- Liaison de donné	Les protocoles de la couche liaison de données compliquées les méthodes d'échange de trames de données entre les appareils sur un support commun
1- Physique	Les protocoles de la couche physique dotés des moyens mécaniques, électriques, fonctionnels et procéduraux pour activer, maintenir et désactiver les connexions physiques pour la transmission d'un bit vers et depuis un appareil réseau.

Tableau 1.1. Les couches de modèle OSI.

1.6.2 Le modèle TCP/IP

TCP/IP signifie Transmission Control Protocol/Internet Protocol (Protocol de contrôle des transmissions/Protocole Internet). TCP/IP est un ensemble de règles normalisées permettant aux ordinateurs de communiquer sur un réseau tel qu'internet. Ce modèle est un protocole, car il décrit les fonctions qui interviennent à chaque couche de protocoles au sein de la suite TCP/IP. Il comporte quatre couches: application, transport, internet, accès réseau [14].

Couches du modèle TCP/IP	La description
4- Application	Représente des données pour l'utilisateur, ainsi que du codage et un contrôle du dialogue.
3- Transport	Prend en charge la communication entre plusieurs périphériques à travers divers réseaux.
2- Internet	Déterminez le meilleur chemin à travers le réseau.
1- Accès réseau	Contrôlez les périphériques matériels et les supports qui constituent le réseau.

Tableau 1.2. Les couches de modèle TCP/IP.

La figure (1.16) montre la différence entre le modèle OSI et TCP/IP :

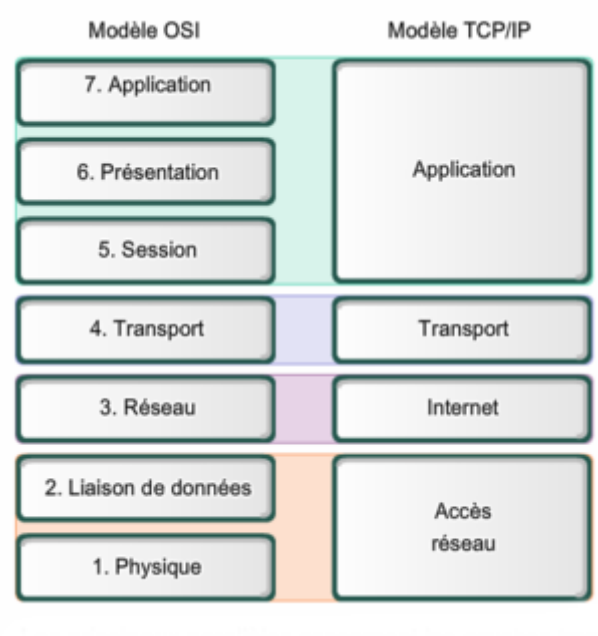

Figure 1.16. Modèle OSI et TCP/IP [39].

1.7 Les protocoles réseaux

1.7.1 Définition

Un protocole informatique est un ensemble de règles et des procédures à respecter pour émettre et recevoir des données sur un réseau. Chaque protocole réseau a sa propre fonction, son format et ses propres règles de communication.

1.7.2 Les différents protocoles réseaux

a Protocole TCP

C'est un protocole fiable qui sécurise l'échange de données : créé dans le but d'établir une communication de haute fiabilité entre différents abonnés à un réseau informatique (protocole orienté connexion) [15].

b Protocole HTTP

Le protocole HTTP (Hyper Text Transfert Protocol) est le protocole de communication du web, l'un les plus utilisé sur Internet car il concerne le World Wide Web. Ce protocole décrit de quelle façon un navigateur peut interroger un serveur Web, et permettant d'échangé des documents hyper textes contenants des données sous la forme de texte, d'images fixes ou animées et de sons. Tout client web communique avec le port 80 d'un serveur http [15].

c Protocole ICMP

ICMP signifie Internet Control Message Protocol est l'un des protocoles fondamentaux constituant la suite de protocoles Internet. ICMP est utilisé pour transporter des messages de contrôle et d'erreur qui fournissent des informations concernant l'état du réseau. La commande la plus connue est la commande « ping » qui a pour objectif d'envoyer une requête ICMP. C'est grâce à ce protocole qu'une machine émettrice peut savoir qu'il y a eu un incident de réseau [16].

d Protocole DHCP

DHCP est l'abréviation de Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement et automatiquement sa configuration IP. Le but principal étant la simplification de l'administration d'un réseau. On voit généralement le protocole DHCP comme distribuant des adresses IP [17].

e Protocole DNS

Le DNS (Domain Name System) est un système essentiel au fonctionnement d'Internet. C'est un annuaire qui permet la conversion de noms de domaine alphanumériques en adresses IP numériques [17].

f Protocole FTP

Le FTP (File Transfer Protocol) est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'administrer un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur [17].

g Protocole SMTP

SMTP est le sigle de Simple Mail Transfer Protocol, littéralement « protocole simple de transfert de courrier ». Il s'agit d'un protocole de communication qui utilise un ensemble de règles pour transférer des emails vers les serveurs de messagerie électronique [17].

h Protocole IP

C'est lui qui gère la fragmentation des données lorsque par exemple une section du réseau admet une taille différente des paquets, mais le rôle le plus important de ce protocole est d'acheminer les données à travers un ensemble de réseaux interconnectés grâce à la gestion des adresses IP [17].

1.8 L'adressage IP

1.8.1 Principe de l'adressage

Un hôte a besoin d'une adresse IP pour participer aux activités sur Internet. L'adresse IP est une série de chiffres et de lettres qui permettent de connecter un dispositif informatique d'un réseau via une méthode de communication spécifique (protocole IP). Elle doit être unique et correctement configurée pour toute communication avec d'autres périphériques sur Internet.

L'adresse IP est attribuée à chaque matériel à l'interface du réseau informatique. Cette connexion se présente généralement sous la forme d'une carte réseau installée dans le périphérique. Les stations de travail, serveurs, imprimantes réseau et téléphones IP sont des exemples des périphériques utilisateurs dotés d'interfaces réseaux.

Chaque paquet transmis par le protocole IP contient l'adresse IP de l'émetteur ainsi que l'adresse IP du destinataire. Les périphériques réseaux ont besoin de ces informations pour garantir que les données arrivent à destination et que toutes les réponses sont renvoyées à la source [18].

1.8.2 Adresse IPv4

Une adresse IP version 4 est constituée de 32 bit structurés en deux parties : identificateur de réseau et identificateur de machine [18].

Les adresses IP sont organisées en cinq classes (A, B, C, D ou E) selon la valeur de son premier octet comme la figure (1.17) montre :

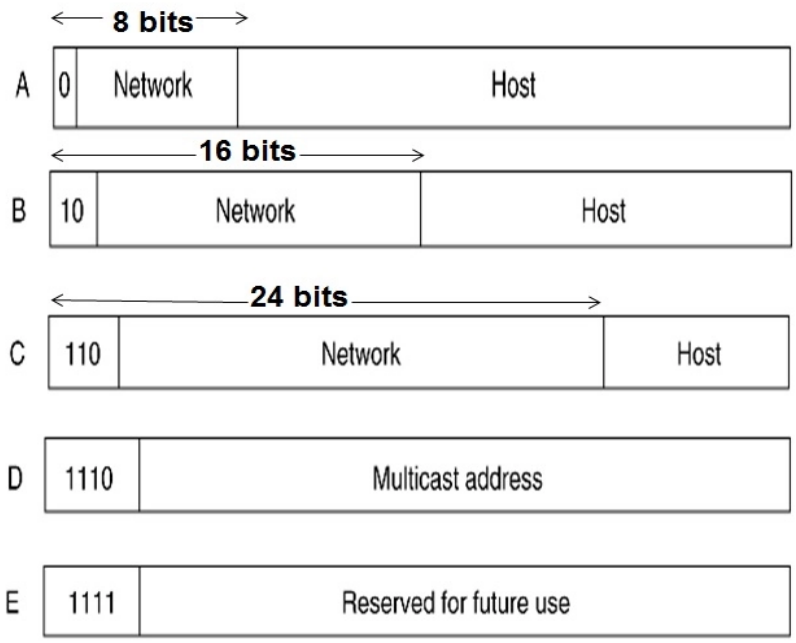

Figure 1.17. Les classes d'adresse IPv4.

Le tableau ci-après donne l'espace d'adresses possibles pour chaque classe :

Les classes	Les adresses
A	0.0.0.0 à 127.255.255.255
B	128.0.0.0 à 191.255.255.255
C	192.0.0.0 à 223.255.255.255
D	224.0.0.0 à 239.255.255.255
E	240.0.0.0 à 247.255.255.255

Tableau 1.3.Les classes de plage d'adressage.

1.9 Conclusion

Les réseaux informatiques sont devenus aujourd'hui une nécessité dans la vie de tous les jours. Ce chapitre nous a permis en premier lieu de découvrir et de mieux comprendre les notions et les aspects élémentaires des réseaux informatiques, à savoir les outils d'interconnexion et les classifications des réseaux. Ainsi il nous a permis de différencier entre le modèle OSI et le modèle TCP/IP qui assurent la fiabilité de communication.

Dans le deuxième chapitre nous allons présenter les techniques telles que la DMZ, et plusieurs solutions que nous proposons pour améliorer le niveau de sécurité sur un réseau informatique.

Chapitre 2 Notions fondamentales sur la sécurité informatique

2.1 Introduction

La sécurité informatique est de nos jours devenue un aspect majeur dans la gestion des réseaux d'entreprise, ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques par l'intermédiaire administrateurs.

Dans ce chapitre nous avons présenté les principaux moyens pour renforcer la sécurité informatique. Ainsi que le simulateur utilisé pour la rédaction de notre mémoire.

2.2 Sécurité informatique

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. L'objectif de la sécurité informatique est de s'assurer que les ressources matérielles et/ou logicielles d'un parc informatique sont uniquement utilisées dans le cadre prévu et par des personnes autorisées. Il convient d'identifier les exigences fondamentales en sécurité informatique, qui caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques au regard de la sécurité [19] :

- **Intégrité :** confirmation que les données qui ont été envoyées, reçue ou stockées sont complètes et n'ont pas été modifiées.
- **Disponibilité :** Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment même en cas

d'événements perturbants tels que des pannes de courant, des catastrophes naturelles, des accidents, ou des attaques.

- **Confidentialité :** Seules les personnes autorisées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- **L'authentification :** Elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

2.3 L'administration des réseaux informatique

L'administration réseau est le processus permettant le contrôle d'un réseau de donnée pour assurer l'efficacité et la productivité. Celle-ci peut se décomposer en trois types d'administration [13]:

Figure 2.1. Topologie de l'administration de réseau.

2.3.1 L'administration des utilisateurs

L'administration des utilisateurs fournit l'ensemble des mécanismes nécessaires pour qu'une personne puisse utiliser le réseau, à savoir [13]:

- *Accessibilité et connectivité aux applications :* l'utilisateur doit pouvoir se connecter aux différentes applications fournit par le réseau, et doit disposer

d'un ensemble d'outils lui assurant une certaine transparence au niveau des méthodes d'accès et connexions aux applications.

- *La confidentialité et la sécurité :* Le système doit fournir l'ensemble des mécanismes qui permettent de garantir la confidentialité des informations de l'utilisateur, de sécuriser son environnement et de prévenir toute perte ou altération des échanges effectués par l'utilisateur.
- *La qualité de service fournit à l'utilisateur :* Il s'agit principalement de la disponibilité et des performances du système et sa capacité à assurer le service attendu.

2.3.2 L'administration des serveurs

L'administration des serveurs fournit tous les mécanismes suivants [13]:

- *La connexion et la distribution des applications sur tout le réseau :* afin de permettre la relation entre les différents services.
- *La gestion et la distribution des données :* comme pour les utilisateurs, doivent garantir la fiabilité de transmission des informations, et offrir des outils permettant le transfert de ces informations. C'est le rôle des outils de transfert de fichiers, qui permettent le partage des capacités de stockage entre plusieurs systèmes.
- *La gestion des applications :* est essentiellement lié au contrôle et à la protection des accès de ces applications par la distribution de droits, et de différents protocoles de contrôle d'utilisation de ressources concernant les applications utilisés.

2.3.3 L'administration de la machine de transport

L'administration de la machine de transport (routeur, switch, câble ….) consiste à fournir [13]:

- Les opérations de réseau : dont le rôle est de permettre l'intervention sur le fonctionnement et la modification du réseau.
- La liste des incidents réseaux par la mise en place de protocoles de détection et de correction, Lorsqu'une alerte est déclenchée, des actions vont être prises

pour résoudre l'incident et de ce fait, réduire son influence et ses perturbations sur l'ensemble du réseau.

- Les performances fournies par le réseau, le but est d'afficher et d'évaluer le système par un ensemble de paramètres comme le temps de réponse ou la charge du système.
- Les coûts, afin de pouvoir les mesurer (dans un réseau, les coûts d'utilisation sont complexes à évaluer puisqu'ils concernent un ensemble de composants distribués).
- La configuration, le but est de déterminer la meilleure configuration du réseau afin d'améliorer les performances du système et la qualité du service.
- L'inventaire, qui a pour rôle de tenir à jour en temps réel la liste des éléments logiciels et matériels qui constituent un réseau.
- L'évolution et les changements, l'objectif est de fournir les informations permettant de déterminer les nouveaux besoins, et les parties du système concernées par ces besoins de changement.

2.4 Techniques de renforcement de sécurité dans un réseau local

Avant la sécurisation du réseau local contre les menace et les attaque provenant de l'extérieure, il faut renforcer le réseau à travers les différentes techniques suivantes :

- La zone démilitarisée (DMZ).
- Les mécanismes de routage.
- Traduire les adresses locales internes en adresse publique similaire par le NAT (Network Address Translation) et le PAT (Port Address Translation).
- Filtrer les accès entre les différents réseaux avec les ACLs (Access Control List).

2.5 La zone démilitarisée (DMZ)

2.5.1 Présentation

La DMZ signifie en anglais Demilitarized Zone. Pour comprendre l'origine de ce terme, il faut s'intéresser à l'histoire, non pas à l'histoire de l'informatique, mais à l'histoire de

la Corée et à la Guerre Froide. La zone démilitarisée Coréenne est une zone tampon (représentée par des terres inhabitées et où l'accès est très limité) qui sert de frontière entre la Corée du Nord et la Corée du Sud.

Sur l'image ci-dessous, on peut voir que la zone démilitarisée crée une véritable séparation entre la Corée du Nord et la Corée du Sud [20].

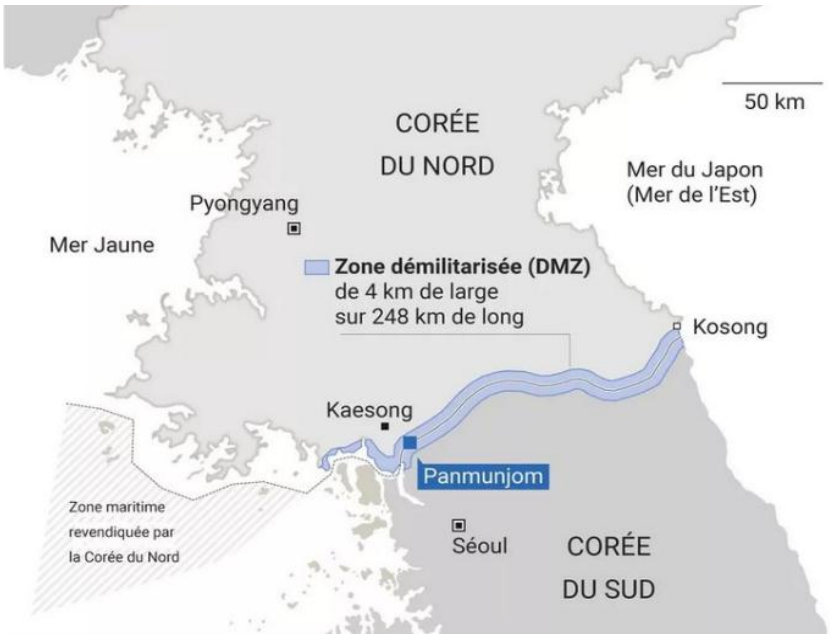

Figure 2.2. La zone démilitarisée [40].

Le rapport entre : la DMZ entre les deux Corée et la DMZ en informatique s'explique par : si l'on compare la situation des deux Corée avec un réseau informatique, on peut voir quelques similitudes et imaginer que [20]:

- La Corée du Nord, c'est le réseau Internet (ou le réseau local).
- La Corée du Sud, c'est le réseau local (ou Internet).
- La zone démilitarisée est une séparation entre les deux qui est là pour des raisons de sécurité.

2.5.2 Définition

Dans le domaine des réseaux informatique, une zone démilitarisée (ou DMZ) fait référence à un sous-réseau physique ou logique qui héberge les services exposés et accessibles de l'extérieur d'une entreprise. Parmi les services les plus souvent rencontrés, on retrouvera : le serveur web, le serveur de messagerie et le serveur FTP.

Cette zone agit comme une zone tampon avec les réseaux non sécurisés tels qu'Internet [21].

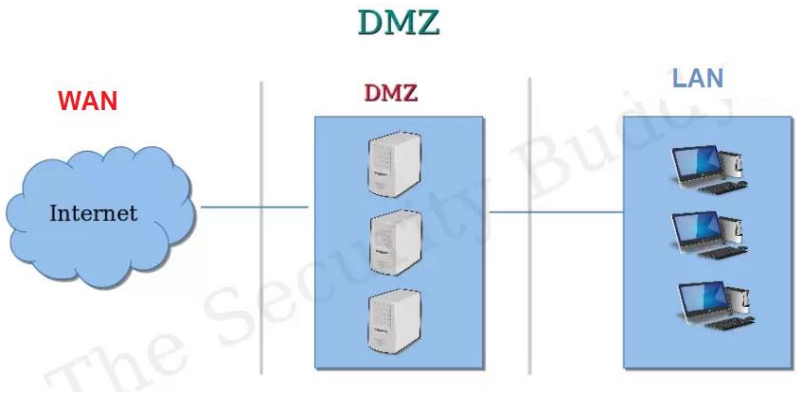

Figure 2.3. La DMZ en informatique [41].

2.5.3 Objectif de la zone démilitarisée

Les DMZ aident les entreprises à détecter et corriger les failles de sécurité avant qu'elles n'atteignent le réseau interne, où sont stockées les ressources les plus précieuses. Les DMZ visent avant tout à protéger les hôtes les plus exposés aux attaques. Parmi ces hôtes, on trouve généralement des services accessibles aux utilisateurs en dehors du réseau local, tels que la messagerie, les serveurs Web, les serveurs FTP et les serveurs DNS. En raison de leur vulnérabilité, ceux-ci sont placés dans un sous-réseau surveillé, afin que le reste du réseau soit protégé en cas d'attaque [21].

2.6 Les serveurs informatiques

Ce dispositif informatique offre des services à un ou plusieurs clients (parfois des milliers). Les services les plus courants sont :

2.6.1 Serveur web

Un serveur web est un ordinateur connecté à Internet et sur lequel sont hébergés des sites web, composés de pages HTML. La transmission est effectuée via le protocole de communication HTTP (le serveur web sera également appelé serveur HTTP). Grâce à un serveur Web, on peut enregistrer des contenus Web et assurer leur accessibilité aux utilisateurs de manière sûre. Lorsque vous chargez une adresse Internet dans votre

navigateur Web, les éléments que vous apercevez d'une page sont toujours envoyés sur votre ordinateur depuis un serveur Web. Pour qu'un site Web soit accessible à tout moment, le serveur Web sur lequel il est hébergé doit être connecté à Internet en permanence [22].

Figure 2.4. Le service web [42].

2.6.2 Serveur messagerie

Un serveur de messagerie (serveur SMTP) est un serveur qui achemine sur Internet des emails d'un expéditeur à un ou plusieurs serveurs destinataires selon les règles du protocole réseau SMTP. Une fonction importante du serveur SMTP est d'éviter le spam au moyen de mécanismes d'authentification, par lesquels il n'est possible d'envoyer des emails qu'aux utilisateurs autorisés. C'est pourquoi les serveurs de messagerie sont généralement construits ou placés dans la DMZ. Ainsi que les messages personnels sont généralement stockés sur des serveurs dépourvus d'accès direct à Internet [22].

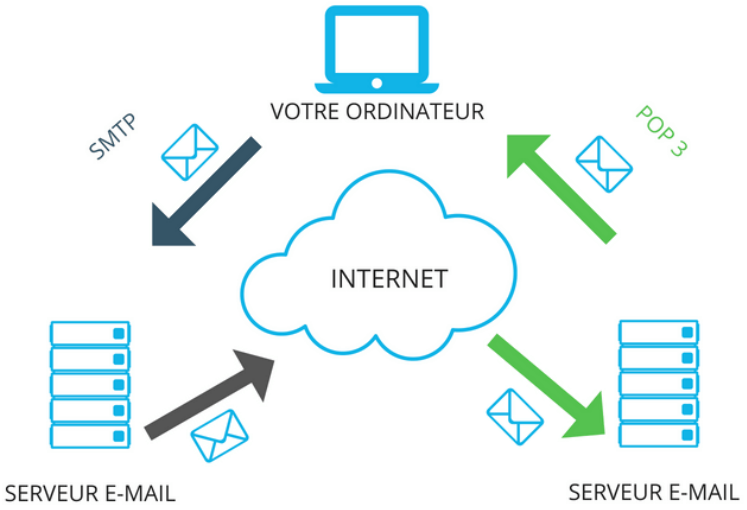

Figure 2.5. L'acheminement d'un courriel [43].

2.6.3 Serveur FTP

Le serveur FTP (File Transfer Protocol) permet de transférer des fichiers par Internet ou par le biais d'un réseau informatique local (intranet). Toute personne en ayant l'autorisation, peut télécharger et envoyer des fichiers sur un ordinateur distant faisant fonctionner un tel serveur. Par défaut le port le plus souvent utilisé est le port 21. Ce type de serveur peut héberger des contenus sensibles sur le site Web d'une entreprise tout en permettant une interaction directe avec les fichiers. Les serveurs FTP doivent donc être partiellement isolés des systèmes internes critiques [21].

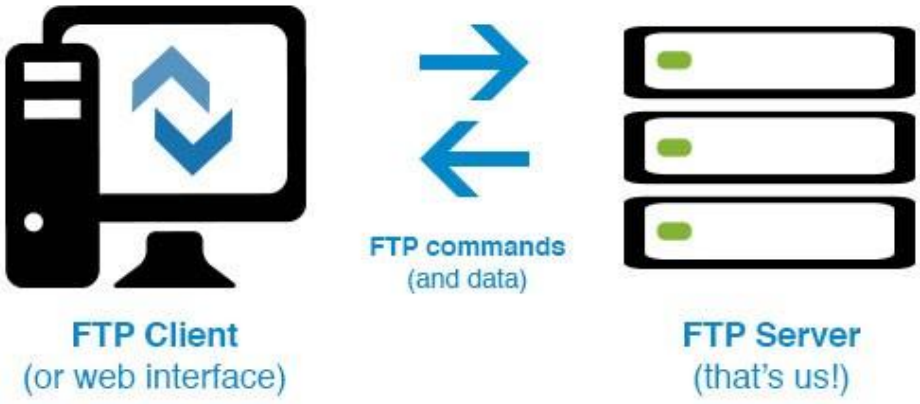

Figure 2.6. Fonctionnement du service FTP [44].

2.6.4 Serveur DHCP

Un serveur DHCP (Dynamic Host Configuration Protocol ou protocole de configuration dynamique) a pour rôle de distribuer des adresses IP à des clients d'une manière dynamique pour une durée déterminée. Au lieu d'affecter manuellement à chaque hôte une adresse statique, ainsi que tous les paramètres tels que (serveur de noms, l'adresse de passerelle par défaut, IP du réseau), un serveur DHCP alloue à un client, un bail d'accès au réseau, pour une durée déterminée (durée du bail). Le serveur passe en paramètres au client toutes les informations dont il a besoin [23].

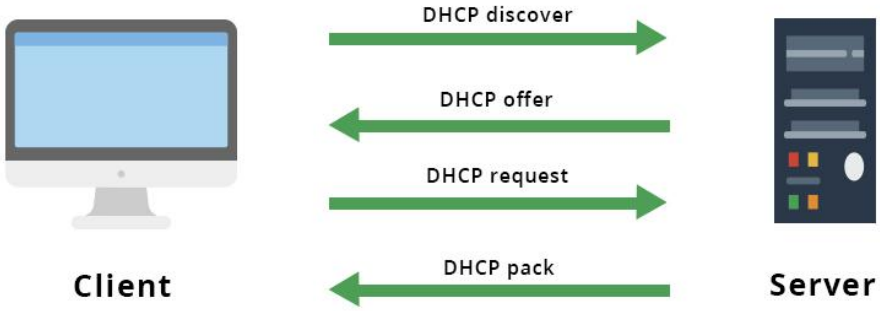

Figure 2.7. Fonctionnement du service DHCP [45].

2.6.5 Serveur DNS

Le service DNS signifiant Domain Name Services est né de la volonté de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques tels que l'Internet. Les machines ne sachant communiquer qu'à travers l'échange d'adresses IP difficiles à mémoriser pour l'homme, le DNS agit comme un annuaire téléphonique en fournissant la correspondance entre le nom de la machine et son adresse IP. Ainsi, lorsque l'on veut se connecter à un ordinateur dont on connaît le nom d'hôte, on interroge un serveur DNS qui nous renvoie l'adresse IP correspondant à ce nom [15].

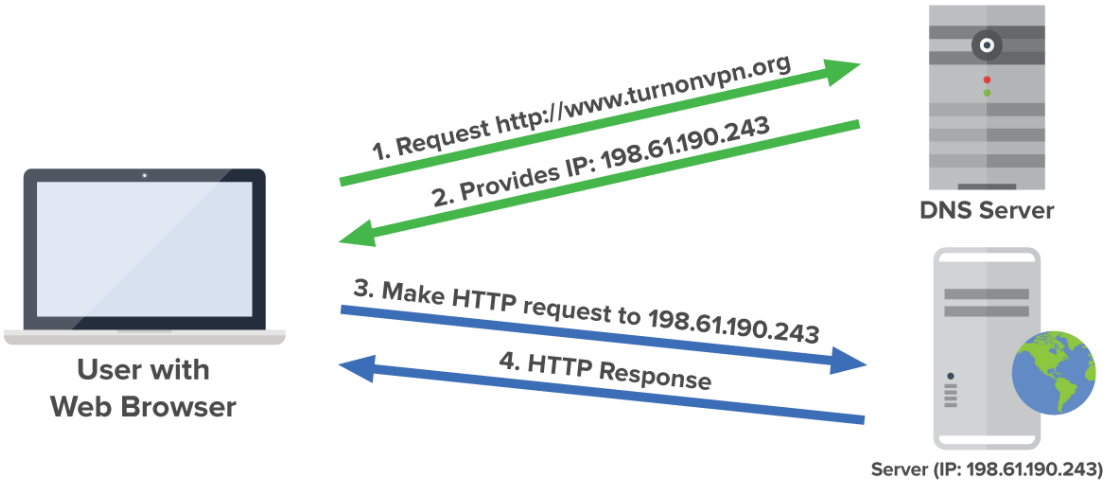

Figure 2.8. Principe d'une requête DNS [46].

2.6.6 Serveur Proxy

Un serveur proxy est un ordinateur intermédiaire installé entre l'ordinateur de l'utilisateur de l'accès Internet. En français, le terme « proxy » désigne un mandataire, une personne que vous avez autorisée à effectuer certaines actions en votre nom, c'est-à-dire au lieu de communiquer directement avec le site Web qui vous intéresse, un proxy se charge de gérer cette relation à votre place [24] [25].

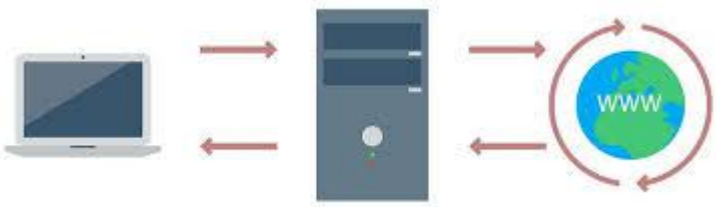

Figure 2.9. Le serveur proxy [47].

2.7 Le routage dans un réseau informatique

Le routage informatique est un processus de sélection des chemins, qui transport les informations aux destinataires d'un réseau au niveau du routeur qui atteint les hôtes, et les périphériques qui ne sont pas dans le même réseau [26].

2.7.1 Fonctionnement de routage

Au centre du réseau informatique se trouve le routeur, qui globalement a pour but de relie plusieurs réseaux. Pour ce faire, il dispose de plusieurs interfaces, chacune appartenant à un réseau IP différent. Lorsqu'un routeur reçoit un paquet IP sur une interface, il détermine quelle interface utiliser pour transférer le paquet vers sa destination grâce à sa table de routage.

Les interfaces de routeur peuvent être classées en deux groupes principaux :

- **Interfaces LAN** : telles qu'Ethernet et FastEthernet : sont utilisées pour connecter le routeur au réseau local, elles utilisent généralement une prise RJ-45 prenant en charge des câbles à paires torsadées non blindées.
- **Interfaces WAN** : telles que les interfaces série, RNIS et Frame Relay : elles permettent de connecter des routeurs à des réseaux externes, généralement sur une distance géographique importante. Chaque interface WAN a sa propre adresse IP et son propre masque de sous-réseau, lui permettant d'être identifiée comme faisant partie d'un réseau donné [26].

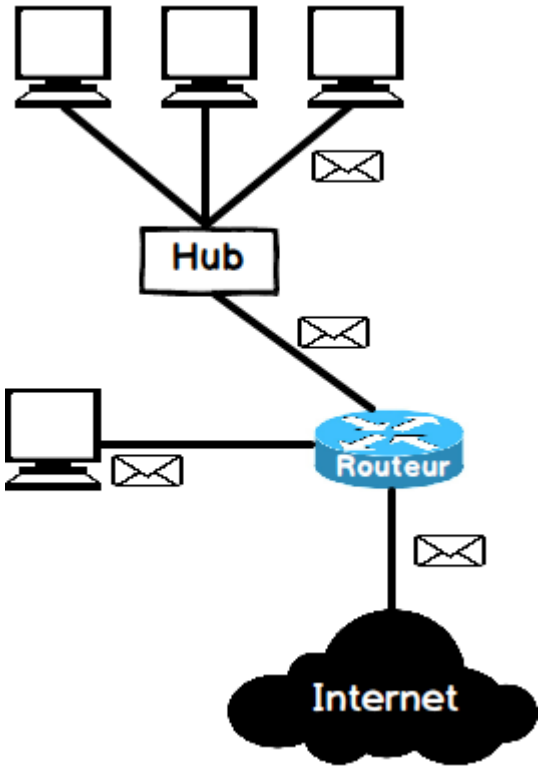

Figure 2.10. Fonctionnement d'un routage [48].

2.7.2 Les modes de routage

Il existe deux modes de routages bien distincts lorsqu'on souhaite aborder la mise en place d'un protocole de routage, il s'agit du routage statique et du routage dynamique.

a Le routage statique

Le routage statique est une technique de routage réseau, et n'est pas un protocole de routage; il s'agit plutôt de la configuration et de la sélection manuelles d'un itinéraire réseau, généralement gérées par l'administrateur réseau. Il est utilisé dans des scénarios où les paramètres du réseau et l'environnement devraient rester constant [26].

b Le routage dynamique

Le routage dynamique 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, de la maintenance et de la mise à jour de la table de routage dynamique. Cela permet de gagner du temps lors de réseau est très grand ou le nombre d'hôtes est très élevé. Inversement dans le routage statique, tous ces travaux sont effectués manuellement par l'administrateur du système car il est implémenté dans un petit réseau [26].

c Comparaison entre routage statique et dynamique

Les différent clé entre le routage statique et dynamique sont représenté sur le tableau suivant :

	Routage statique	Routage dynamique
Mis en œuvre dans des	Petits réseaux	Grands réseaux
Configuration	Manuel	Automatique
Les routes	Défini par l'utilisateur	Les itinéraires sont mis à jour en fonction du changement de topologie.
La construction de la table de routage	Les routes sont remplies à la main	Les routes sont remplies dynamiquement dans la table.
Algorithmes de routage	N'utilise pas d'algorithmes de routage complexes.	Utilise des algorithmes de routage complexes pour effectuer des opérations de routage.
Sécurité	Fournit une haute sécurité.	Moins sécurisé en raison de l'envoi de diffusions et de multidiffusions.
Échec du lien	L'échec de liaison bloque le routage.	L'échec de liaison n'affecte pas le routage.

Tableau 2.1.La comparaison entre le routage statique et le routage dynamique.

2.8 NAT & PAT

Au niveau du routeur, le NAT (Network Address Translation) et le PAT (Port Address Translation) sont les protocoles utilisés pour mapper l'adresse privée (locale) non enregistrée d'un réseau interne vers une adresse publique enregistrée d'un réseau externe avant de transférer le paquet au niveau du routeur. Le mappage permet d'ajouter un niveau de sécurité et de confidentialité au réseau en empêchant les réseaux externes de voir les adresses IPv4 internes [27].

2.8.1 NAT (Network Address Translation)

Le NAT est la traduction d'adresses réseau qui relie deux réseaux et mappe 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 [27].

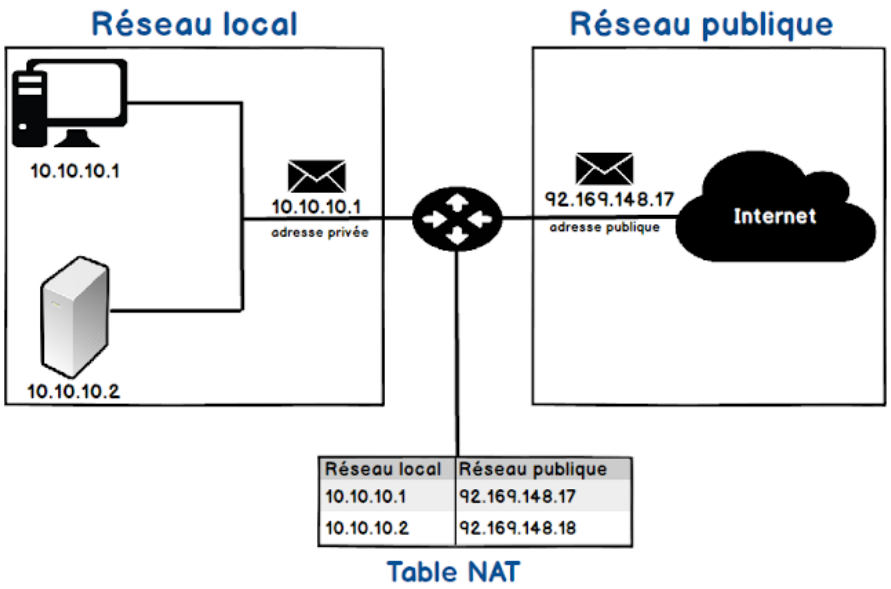

Figure 2.11. Exemple de NAT [49].

De plus, une seule adresse peut être configurée en NAT pour représenter l'ensemble du réseau vers le monde extérieur. Par conséquent, il assure la sécurité car le processus de traduction est transparent. Le NAT peut être utilisé comme un outil pour la migration et la fusion de réseaux, le partage de charge de serveur, la création de serveur virtuel, etc.

On distingue deux types du NAT :

a NAT statique

La NAT statique, se base sur l'association de n adresses privées avec n adresses publiques. C'est à dire qu'à une adresse IP interne, on associe une adresse IP externe. Dans ce cas, la seule action qui sera effectuée par le routeur sera de remplacer l'adresse source ou destination par l'adresse correspondante [27].

b NAT dynamique

Une plage d'adresses publiques est mise au niveau du routeur et lorsqu'une machine du réseau local veut accéder à internet, on lui attribue temporairement et dynamiquement une adresse publique prise dans cette plage [27].

2.8.2 PAT (Port Address Translation)

Le PAT est la traduction d'adresse de port, c'est un type de NAT dynamique grâce auquel la traduction d'adresse peut être configurée au niveau du port, et l'utilisation de l'adresse IP est optimisée. Le PAT met en correspondance plusieurs adresses locales et ports sources avec une adresse IP publique et un port à partir d'une liste d'adresses IP routables sur le réseau de destination. Ici, l'adresse IP de l'interface est utilisée en combinaison avec le numéro de port et plusieurs hôtes peuvent avoir la même adresse IP avec un numéro de port unique.

Il utilise une adresse de port source unique sur l'adresse IP globale interne pour identifier des traductions distinctes. Le nombre total de traductions NAT pouvant être exécutées est 65536 car le numéro de port est codé sur 16 bits [27].

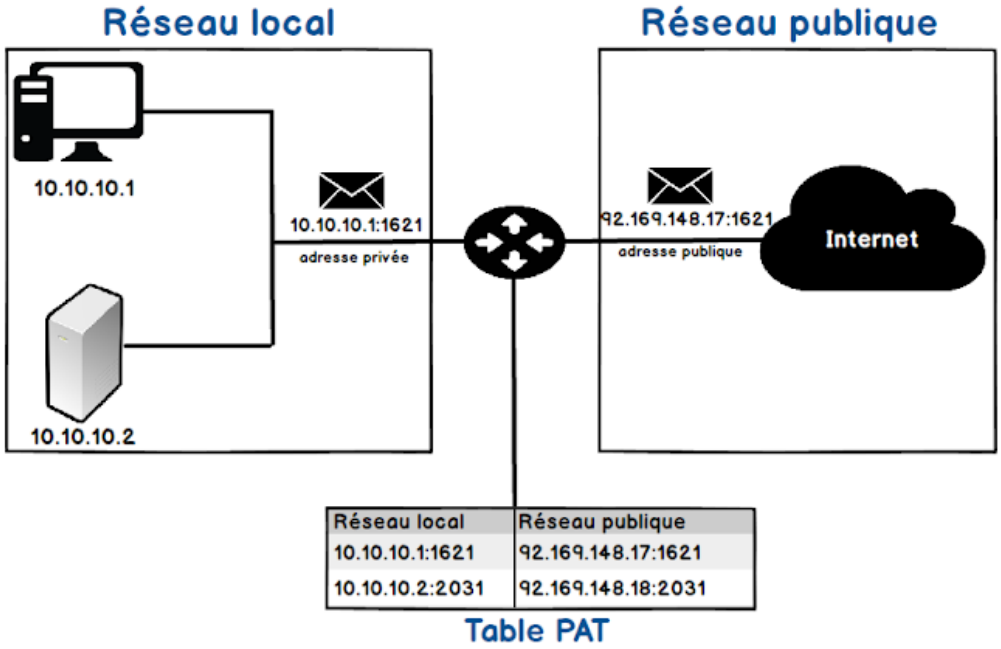

Figure 2.12. Exemple de PAT [49].

2.9 Les listes de contrôle d'accès (ACL)

2.9.1 Définition

Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent aux adresses ou aux protocoles de couche supérieure. Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant

ou sortant d'un réseau. Des listes de contrôle d'accès peuvent être configurées pour tous les protocoles réseau routés.

Une fois configurées, les listes de contrôle d'accès assurent les tâches suivantes :

- ✓ Elles limitent le trafic réseau pour accroître les performances réseau. Ainsi, la charge réseau est nettement réduite et les performances réseau sont sensiblement améliorées.
- ✓ Elles contrôlent le flux de trafic.
- ✓ Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- ✓ Elles filtrent le trafic en fonction de son type.
- ✓ Elles filtrent les hôtes pour autoriser ou refuser l'accès aux services sur le réseau.

2.9.2 Fonctionnement des listes de contrôle d'accès :

Les listes de contrôle d'accès définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie.

Les ACL filtrent le trafic en demandant aux interfaces d'acheminer ou non les paquets qui y transitent. Pour ce faire, le routeur lit l'en-tête de chaque paquet afin de déterminer s'il doit être acheminé ou non, en fonction des conditions définies dans la liste de contrôle d'accès ACLs.

Les listes de contrôle d'accès sont configurées pour s'appliquer au trafic entrant ou sortant :

a Listes de contrôle d'accès entrantes (in)

Les paquets entrants sont traités avant d'être routés vers l'interface de sortie. Une liste de contrôle d'accès entrante est efficace car elle réduit la charge des recherches de routage en cas d'abandon du paquet.

b Listes de contrôle d'accès sortantes (out)

Les paquets entrants sont acheminés vers l'interface de sortie, puis traités par le biais de la liste de contrôle d'accès sortante. Les listes de contrôle d'accès sortantes sont particulièrement efficaces lorsqu'un même filtre est appliqué aux paquets provenant de plusieurs interfaces d'entrée avant de quitter la même interface de sortie.

2.9.3 Type des ACLs

a Listes de contrôle d'accès standard

Les listes de contrôle d'accès standard peuvent être utilisées pour autoriser ou refuser le trafic uniquement depuis des adresses IPv4 source. La destination du paquet et les ports concernés ne sont pas évalués. Elles sont numérotées de 1 à 99 et de 1300 à 1999.

b Listes de contrôle d'accès étendues

Permet de vérifier les adresses des paquets source et de destination. Elles peuvent également cibler des protocoles spécifiques, des numéros de port et d'autres paramètres. Ce qui donne aux administrateurs plus de flexibilité et de contrôle. Elles sont numérotées de 100 à 199 et de 2000 à 2699.

Les listes de contrôle d'accès étendues filtrent les paquets IPv4 en fonction de différents critères :

- Type de protocole.
- Adresse IPv4 source.
- Adresse IPv4 de destination.
- Ports TCP ou UDP source.
- Ports TCP ou UDP de destination.
- Informations facultatives sur le type de protocole pour un contrôle plus précis [28].

2.10 Présentation du simulateur CISCO Packet Tracer

Packet Tracer est un logiciel open source permettent la construction d'un réseau physique virtuel, et de simuler les comportements des protocoles sur une quelconque topologie de réseau. Le simulateur permet aux utilisateurs de créer et de configurer leurs propres réseaux à l'aide des équipements Cisco avant de passer à la configuration réelle.

La figure (2.13), ci-dessous montre un aperçu général de Packet Tracer, dont on définit les zones :

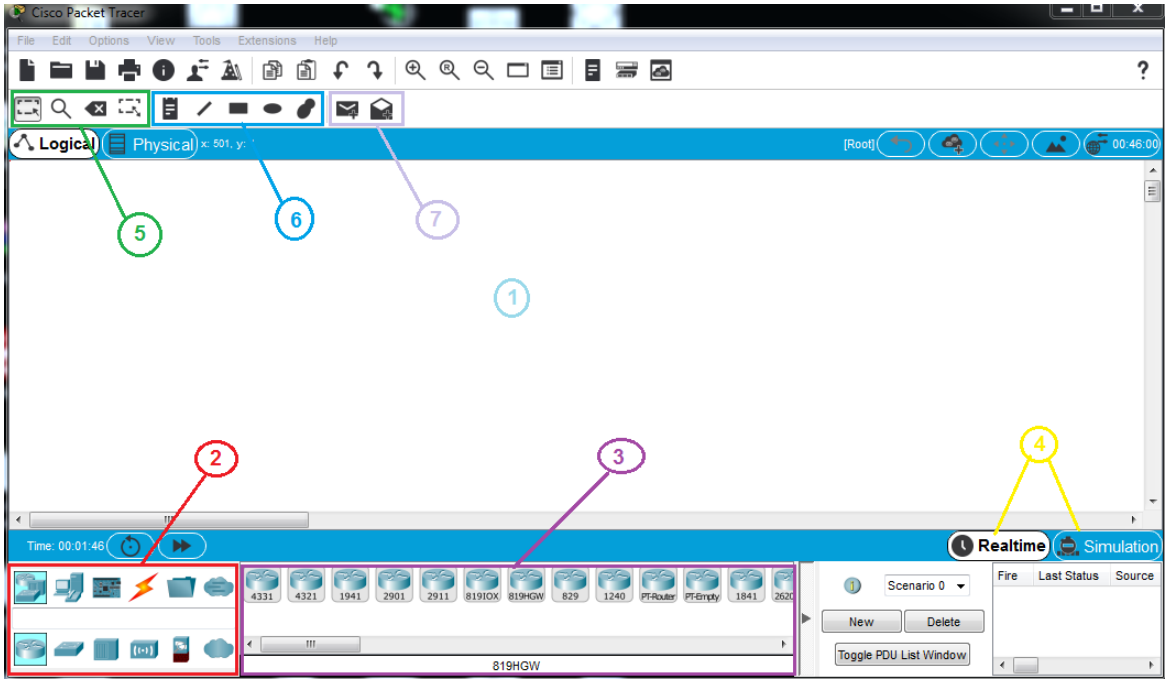

Figure 2.13. L'interface du simulateur Cisco Packet Tracer.

Zone 1 : la partie dans laquelle le réseau est construit ;

Zone 2 : la partie ou le type des équipements sont choisis ;

Zone 3 : les différent modèles de périphériques de type sélectionné dans la zone 2 ;

Zone 4 : elle permet de passer du mode réel au mode simulation ;

Zone 5 : elle contient un ensemble d'outils : sélection, inspection, suppression et redimensionner la forme ;

Zone 6 : elle contient l'annotation du schéma et des palettes de dialogues ;

Zones 7 : concerne les tests de communication (envoie de la trame et personnalisation de la trame).

Pour la simulation et la construction du réseau il faut suivre ces étapes suivant :

2.10.1 Construire un réseau

Pour construire un réseau, l'utilisateur doit choisir parmi les catégories proposées par Packet Tracer : les routeurs, les switchs, les hubs, les équipements sans-fil, les connexions, les équipements dits terminaux (ordinateurs, serveurs), les équipements personnalisés et enfin une connexion multi-utilisateurs. Lorsqu'une catégorie est sélectionnée, l'utilisateur a alors le choix entre plusieurs équipements différents. Pour ajouter un équipement, il suffit de cliquer dessus puis de cliquer à l'endroit choisi.

Figure 2.14. Type d'équipement Cisco.

Pour relier deux équipements, il faut choisir la catégorie "Connections" puis cliquer sur la connexion désirée. La figure (2.15) montre les différentes connexions :

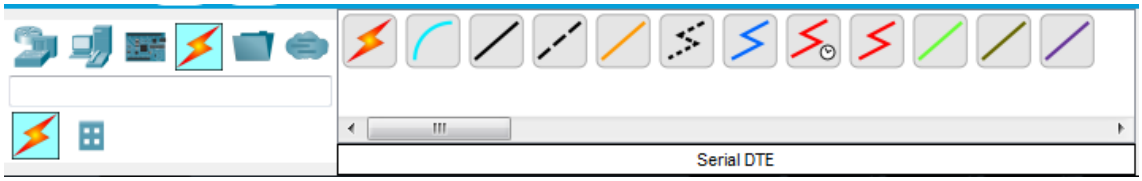

Figure 2.15. Les différentes connexions.

2.10.2 Configuration d'un équipement

Lorsqu'un ordinateur a été ajouté dans le plan de travail, il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau.

2.10.3 Mode simulation

Une fois le réseau créé et prêt à fonctionner, il est possible de passer en mode simulation, ce qui permet de visualiser tous les messages échangés dans le réseau.

En ce mode, la fenêtre principale permettant de gérer le mode simulation : exécution pas-à-pas, vitesse de simulation, protocoles visibles…

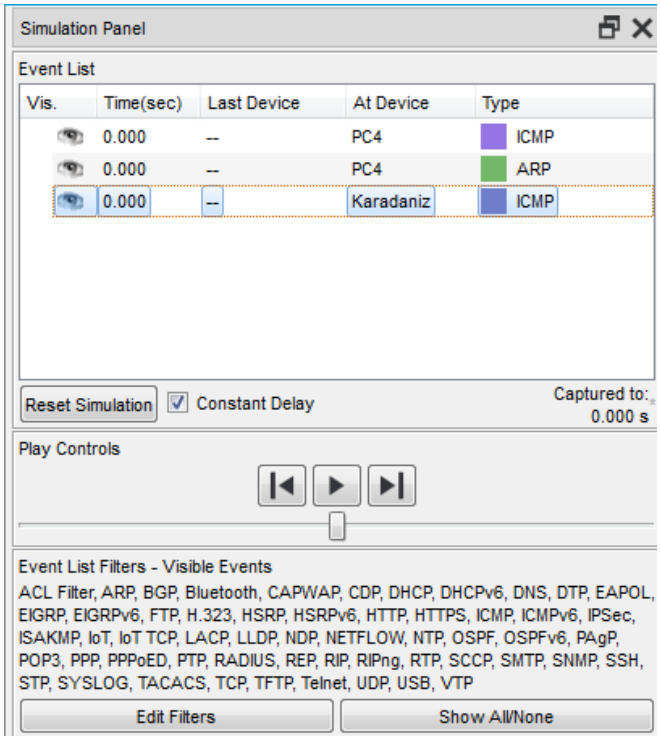

Figure 2.16. Partie simulation.

2.11 Conclusion

Dans ce chapitre, nous avons étudié les notions de base pour la sécurisation d'un réseau informatique. D'abord nous avons présenté la topologie de l'administration de réseau, ensuite nous avons montré les fonctionnalités de renforcement de sécurités existantes dans un réseau que ce soit : la DMZ qui offre plusieurs services tel que serveur DNS, messagerie, WEB et FTP ; le NAT et le PAT pour la traduction des adresses et les ACLs qui représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau informatique. Enfin nous avons présenté un aperçu sur le simulateur Packet Tracer pour créer et configurer un réseau à l'aide des équipements Cisco avant de passer à la configuration réelle.

Dans le chapitre suivant nous allons simuler les différentes étapes qui nous permettront la bonne réalisation d'un réseau informatique.

Chapitre 3 Conception et résultats de mise en place

3.1 Introduction

Dans ce chapitre, nous allons passer à la dernière étape de notre travail qui est la réalisation de notre projet. Cette dernière est cruciale pour la mise en place de tout ce que nous avons fait dans les précédents chapitres. Nous implémenterons les solutions proposées pour renforcer de sécurité d'un réseau. Et pour ce faire, nous commencerons par l'analyse des besoins et l'étude du projet, ensuit nous expliquerons en détail les différentes étapes suivies pour la réalisation des réseaux informatiques au niveau du simulateur Packet Tracer.

3.2 Analyse des besoins et étude du projet

3.2.1 Présentation de l'architecture

Nous avons met en place un réseau informatique qui contient trois zones (inside, DMZ, outside), qui communiquent via un routeur entre eux avec plusieurs fonctionnalité. Nous avons configuré notre réseau de telle manière :

- Gérer les serveurs de la zone démilitarisée pour offrir aux utilisateurs une gestion efficace et simplifiée.
- Filtrer les accès entre les différents réseaux et diriger le trafic entrant et sortant du réseau qui constitue généralement la première ligne de défense lorsque le réseau se connecte à Internet.
- Mapper une adresse privée d'un réseau interne vers une adresse publique d'un réseau externe avant de transférer le paquet.

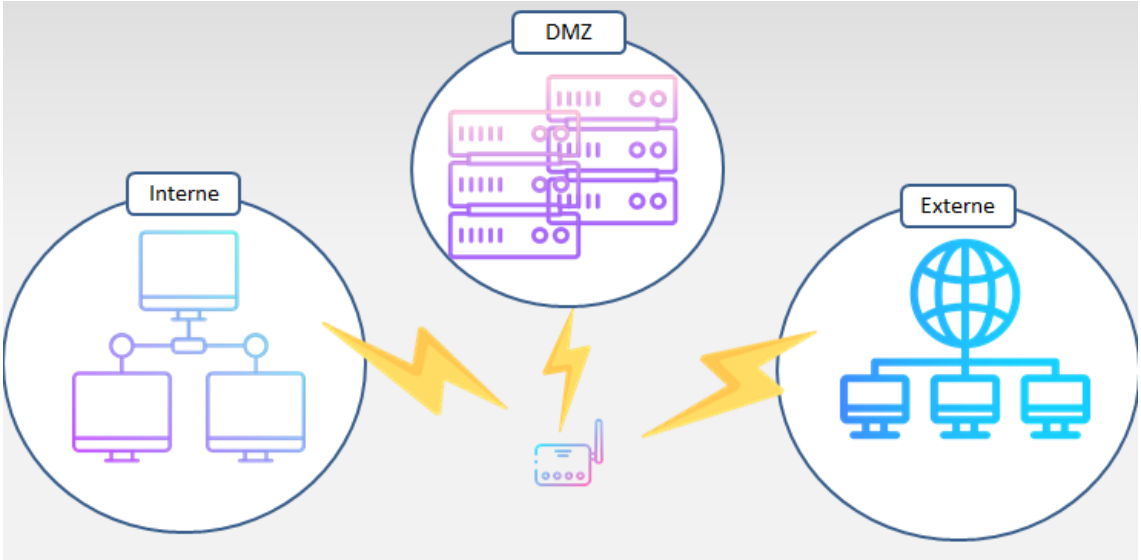

Figure 3.1. Architecture d'un réseau informatique avec DMZ.

3.2.2 Planification des tâches

Avant d'entamer la réalisation du réseau, on a eu recours à une étape de planification où on a regroupé et organisé toutes les étapes de configurations nécessaires. Le tableau suivant présente ces différentes tâches par ordre chronologique.

Ordre	Intitulé
1	Création des Zones réseaux (Inside & Outside)
2	Création d'un réseau isolé (DMZ) entre Inside et Outside
3	Configuration des chemins par le routage statique
4	Ajout des règles d'accès de base (ACL)
5	Mapper les adresses privées en adresses publiques le PAT

Tableau 3.1. Planification des tâches.

3.3 Mise en œuvre de l'architecture

L'architecture que nous avons choisi de mettre en place pour la création de notre réseau est l'architecture client/serveur. Dans cette architecture les trois zones proposées (Inside, Outside, DMZ) sont reliées entre eux avec les routeurs (par exemple

université Blida et l'extérieur de l'université Blida), et les équipements de chaque zone sont reliées avec un switch celui-ci est la topologie étoile.

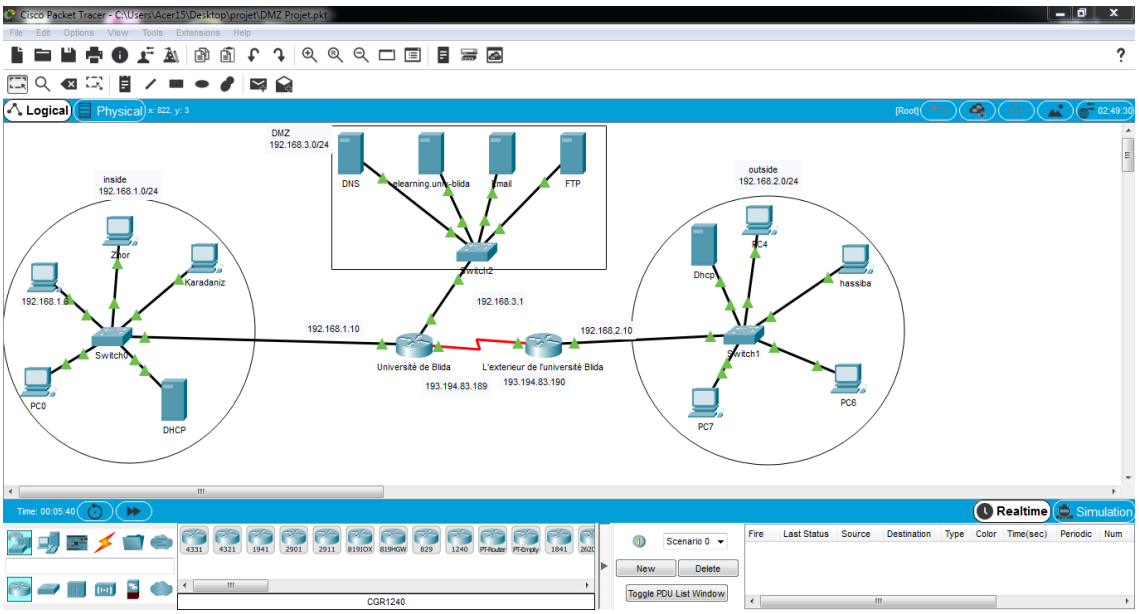

Figure 3.2. L'architecture de notre réseau.

Le tableau suivant montre les matériels utilisés pour chaque zone :

Matériels utilisés pour chaque zone		
Zone inside	**zone démilitarisé DMZ**	**Zone outside**
- Quatre postes clients - Un poste serveur DHCP - Un switch	- Un poste serveur DNS - Un poste serveur HTTP - Un poste serveur FTP - Un poste serveur messagerie	- Quatre postes clients - Un poste serveur DHCP - Un switch

Tableau 3.2. Matériels utilisés.

3.4 Configuration des équipements

3.4.1 Configuration de la zone Inside

On a quatre postes clients et un serveur DHCP reliée entre eux avec un Switch. Nous avons configuré le serveur DHCP pour attribué automatiquement les adresses IP de sous réseau (192.168.1.0), masque de sous réseau (255.255.255.0), la passerelle (192.168.1.10) et le DNS (192.168.3.2) pour chaque client.

Pour ce qui concerne la configuration d'un serveur DHCP, on clique sur **« Desktop »** puis **« IP configuration »,** ensuit nous fixons une adresse IP de façon statique et nous remplissons les adresses pour IP Address, Subnet Mask, Default Getway et DNS server comme montre la figure (3.3) ci-dessous :

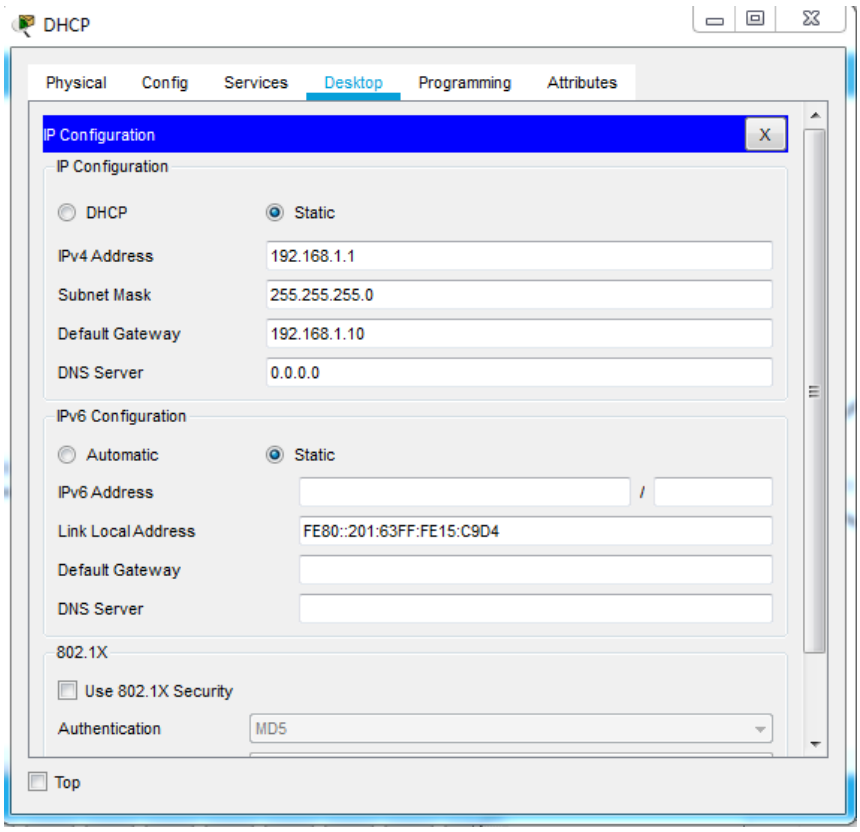

Figure 3.3.Configuration du serveur DHCP.

Pour activer le service DHCP sur ce serveur, sur le même menu on tape sur **« services »** puis **« DHCP » .**Nous avons activé le bouton **« On »** pour que le réseau soit actif et nous avons rempli le default Gateway et Dns Server de la même manière que précédemment.

Ensuite dans **« Start IP adress »** nous avons mis la première adresse que notre machine aura dans la plage et nous avons défini le nombre maximal des machines de ce réseau dans **« Maximum Number of User »**, dans notre réseau nous avons choisi 9 machines. Comme montre la figure ci-dessous :

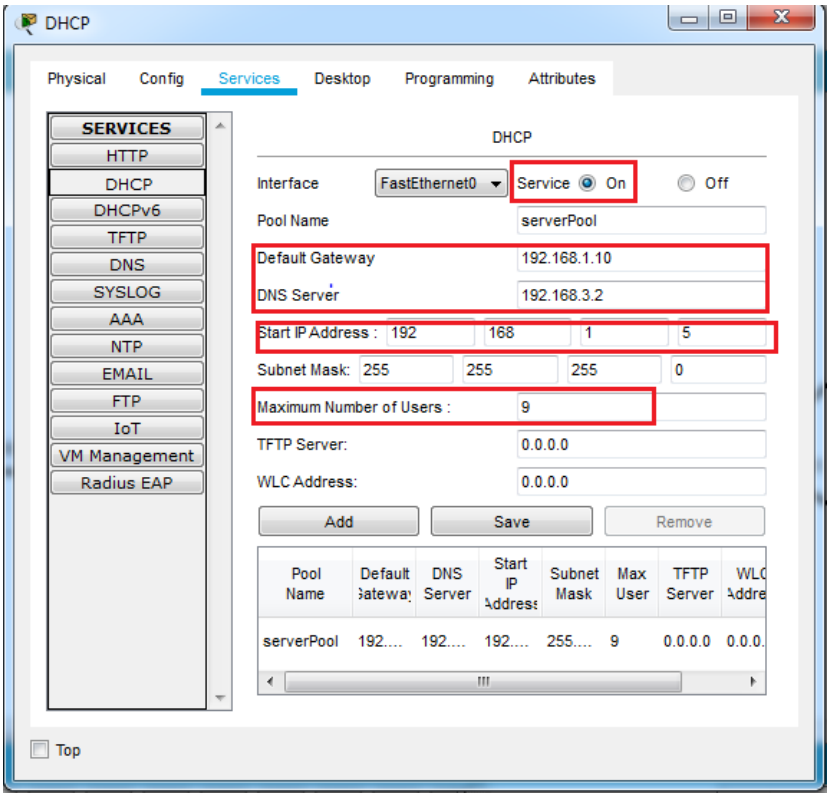

Figure 3.4. Activation du service DHCP.

Pour obtenir la configuration IP automatiquement pour chaque client (PC), on passe du mode **statique** au mode **DHCP**.

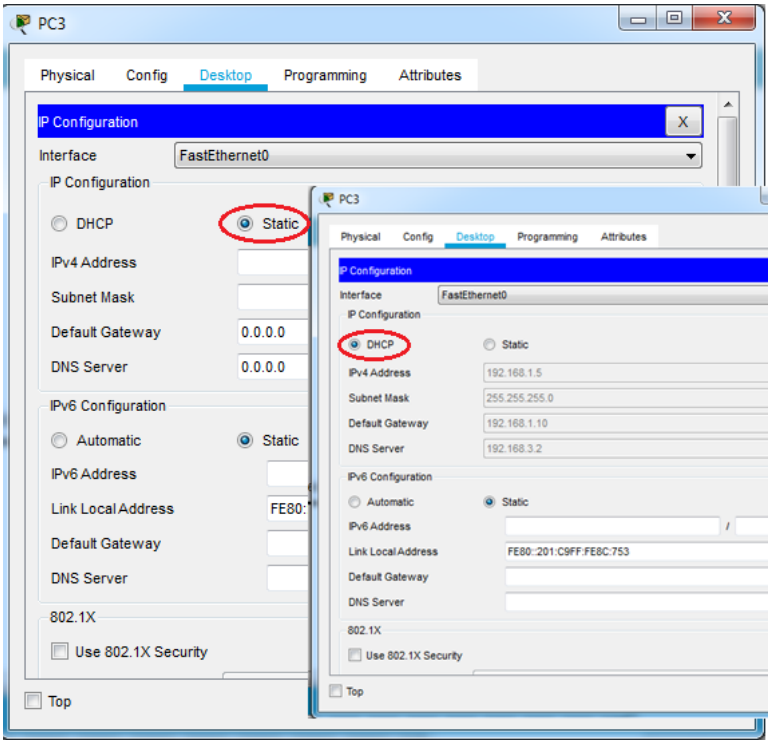

Figure 3.5.L'attribution des adresses.

3.4.2 Configuration de la zone outside

Pour la configuration de cette zone nous avons suivi le même principe que celui de la zone Inside sauf que l'adresse de sous-réseau change et devenir (192.168.2.0) :

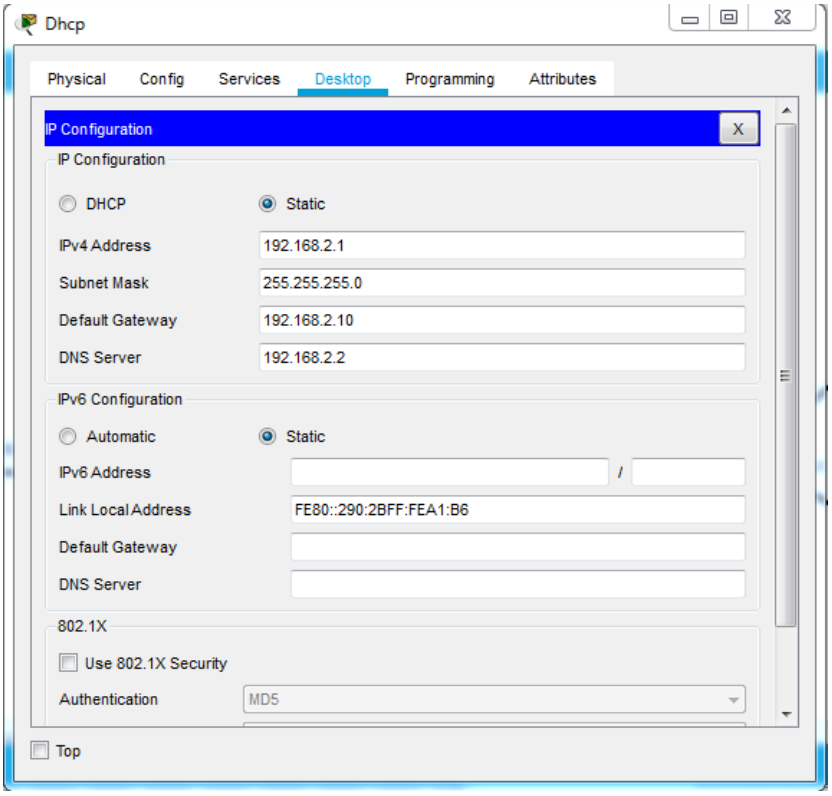

Figure 3.6. Configuration du serveur DHCP.

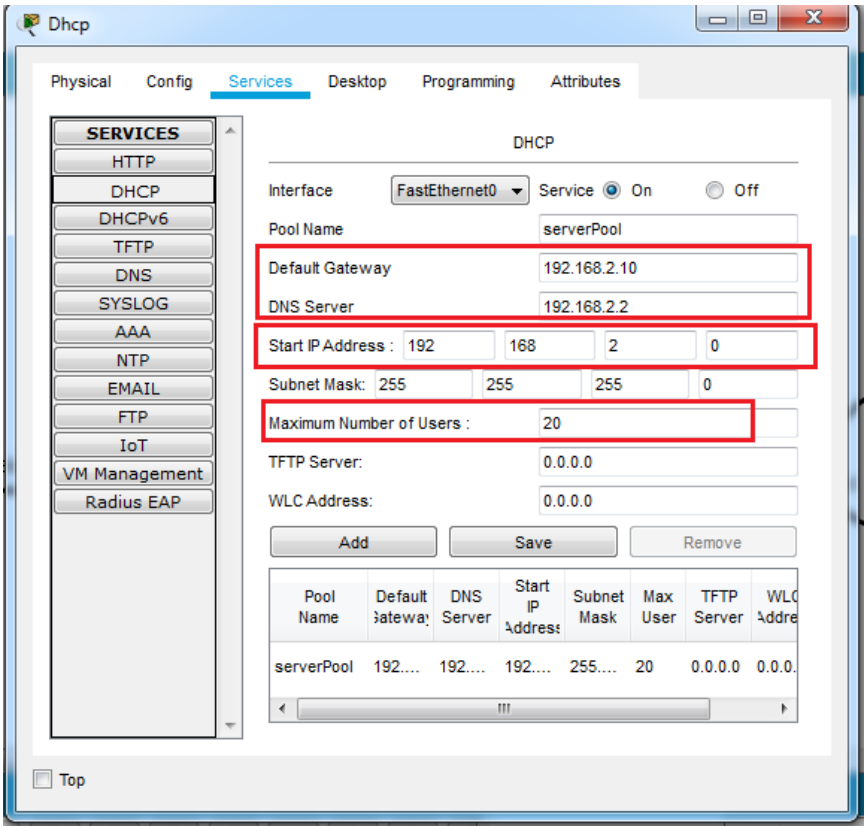

Figure 3.7. Activation du service DHCP***.***

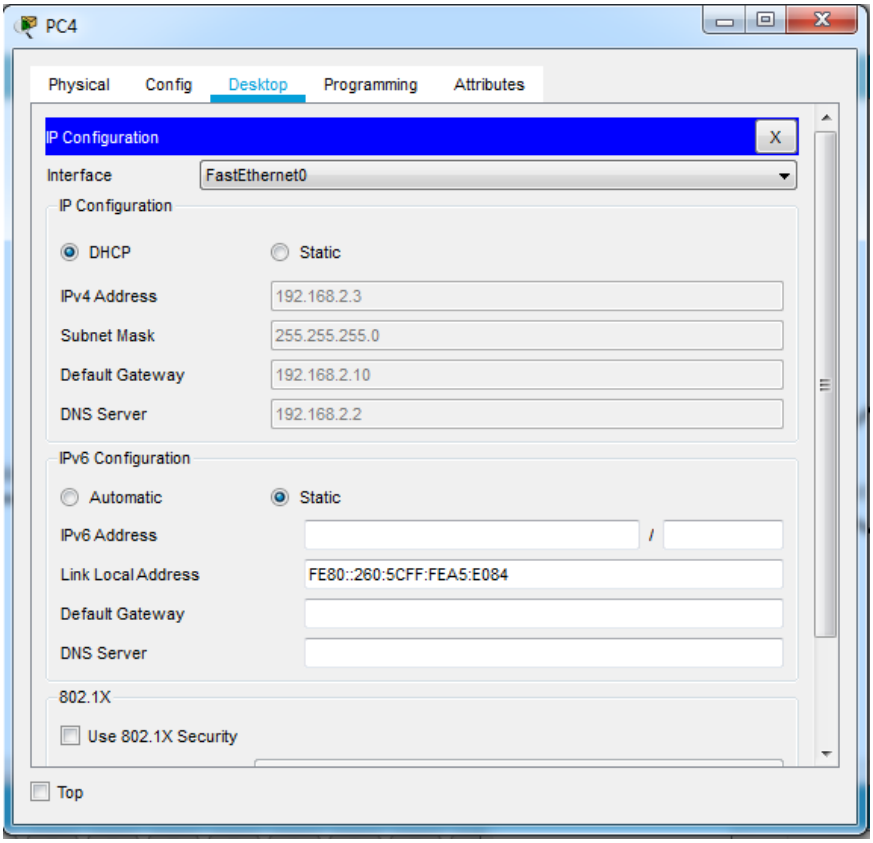

Figure 3.8. L'attribution des adresses.

3.4.3 Configuration de la zone DMZ

Dans cette partie, nous allons configurer les serveurs de DMZ qui devra offrir cinq services (serveur elearning.univ-blida, serveur DNS, serveur Email et le serveur FTP). Le tableau suivant indique les adresses pour chaque serveur :

	Serveur elearning.univ-blida	**Serveur DNS**	**Serveur Email**	**Serveur FTP**
Adresse IP	192.168.3.3	192.168.3.2	192.168.3.20	192.168.3.25
Masque de sous réseau	255.255.255.0			
Passerelle	192.168.3.1			
Adresse de serveur DNS	192.168.3.2			

Tableau 3.3. Les adresses pour chaque serveur.

a Le serveur Web (elearning.univ-blida)

Le serveur *elearning.univ-blida* c'est un serveur web (HTTP), qui répond à des requêtes du World Wide Web sur un réseau, en utilisant principalement le protocole HTTP.

Tout d'abord pour passer à la configuration du service *elearning.univ-blida*, nous cliquons sur le serveur puis nous tapons sur **« Services »** ensuit **« HTTP »** et activer le bouton **« ON »** :

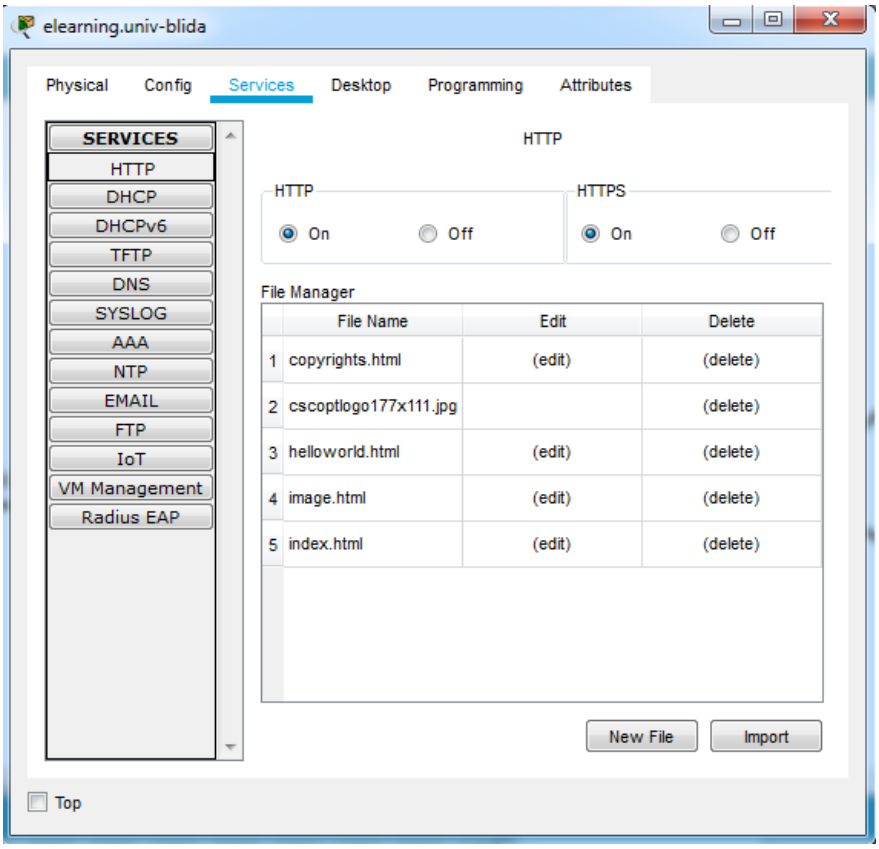

Figure 3.9. Configuration du serveur elearning.univ-blida.

Pour associer un nom compréhensible, à une adresse IP de ce serveur on passe au serveur DNS.

b Le serveur DNS

Pour faciliter la recherche d'un site donné sur Internet, le système de noms de domaine (DNS) a été inventé. Le DNS permet d'associer un nom compréhensible, à une adresse IP.

Pour ce faire, dans le serveur DNS nous cliquons sur l'angle **« service »**, nous commençons toujours par activer le bouton **« On ».** Il est crucial de le faire pour amorcer notre configuration. Car sans cela notre réseau ne pourra pas fonctionner. Maintenant dans la partie Name, nous allons mettre le nom de notre domaine précéder par **www** et suivi de l'extension **.com**, **.fr**, **.dz**. … Ensuite, nous donnons l'adresse de notre nom de domaine, et en dernier nous cliquons sur **« save »** pour sauvegarder.

La figure suivante montre comment nous avons fait la configuration de ce serveur :

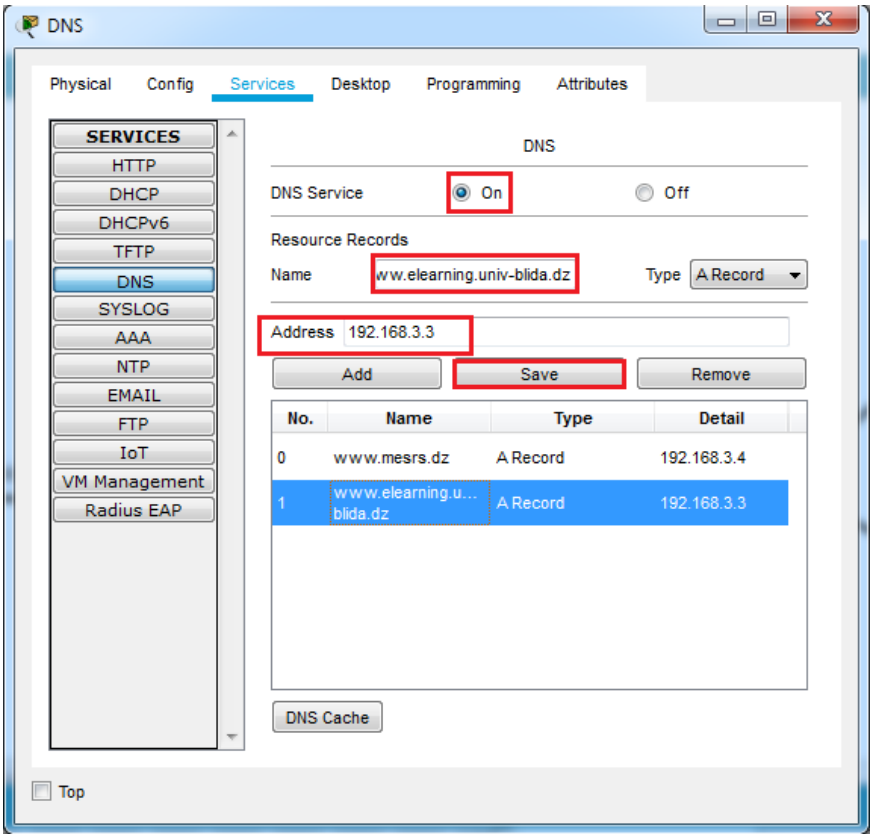

Figure 3.10. Configuration du serveur DNS pour un nom (www.elearning.univ-blida.dz).

c Serveur messagerie (Email)

Tout d'abord, nous avons commencé par la configuration des clients de messagerie du réseau Inside.

Nous sélectionnons sur le PC de la cliente ''Zhor''. Puis nous Accédons à son onglet **« Desktop »** et nous cliquons sur **« Email ».** Pour configurer le client de messagerie nous remplissons les informations d'utilisateur, de serveur et de connexion et nous cliquons sur **« save »**. Comme montre la figure ci-dessous :

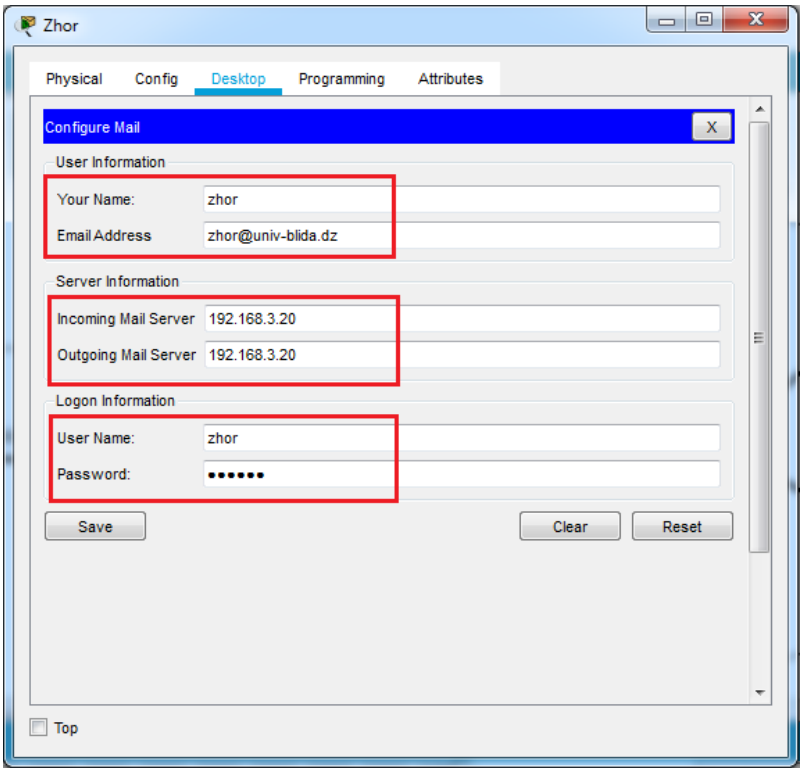

Figure 3.11 Configuration du PC de la cliente ‘’Zhor’’.

Nous configurons le PC de la cliente de messagerie ‘’Karadaniz’’ de la même manière que nous l'avons fait pour PC ‘’Zhor’’.

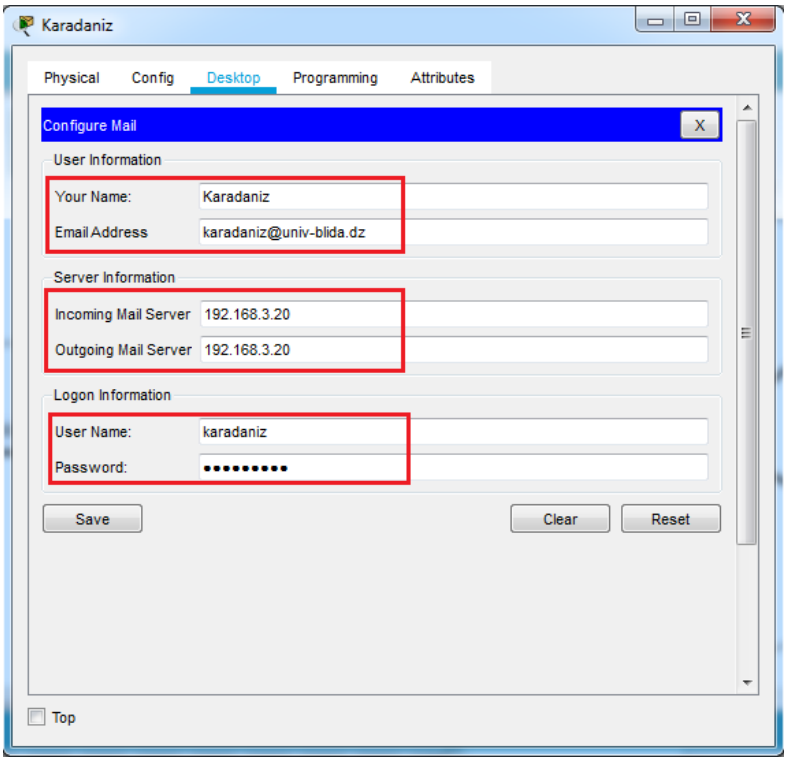

Figure 3.12. Configuration du PC de la cliente ''Karadaniz''.

Ensuite, nous avons configuré le PC de la cliente de messagerie ''Hassiba'' du réseau outside. Afin que cette cliente de ce réseau peut communiquer avec les clients de réseau Inside.

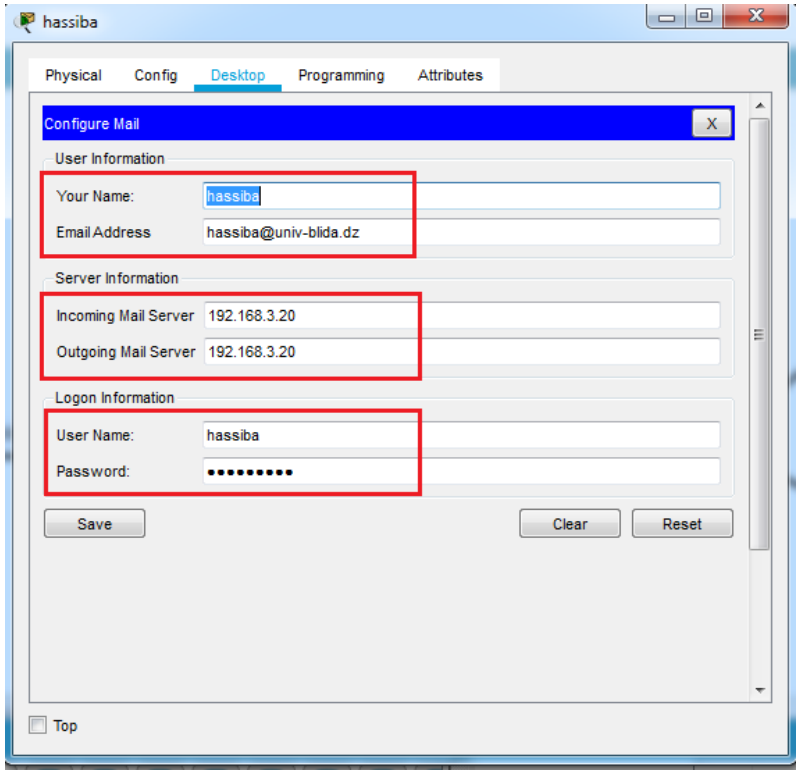

Figure 3.13. Configuration du PC de la cliente ''Hassiba''.

Puis, nous avons configuré le serveur de messagerie.

Pour ce faire, nous cliquons sur le serveur, puis sur l'onglet **« Services »,** et nous choisissons le serveur **« EMAIL »**. Nous indiquons le nom de domaine du serveur puis cliquons sur **« set »** pour le définir. Dans cet exemple, nous avons utilisé le nom 'univ-blida.com'. Nous continuons d'ajouter des utilisateurs et fournissons leurs mots de passe. Nous avons deux clients de messagerie (utilisateurs) avec les noms d'utilisateur ''Zhor'' et ''karadaniz '' dans le réseau Inside et un autre client de messagerie avec le nom d'utilisateur ''Hassiba'' dans le réseau outside. Après avoir entré un nom d'utilisateur et un mot de passe, nous cliquons sur **« + »** pour ajouter l'utilisateur au serveur. Nous pouvons éventuellement supprimer un utilisateur en cliquant sur **«-».** Les figures (3.14), (3.15) et (3.16) ci-dessous montrent la configuration du serveur messagerie pour les trois utilisateurs :

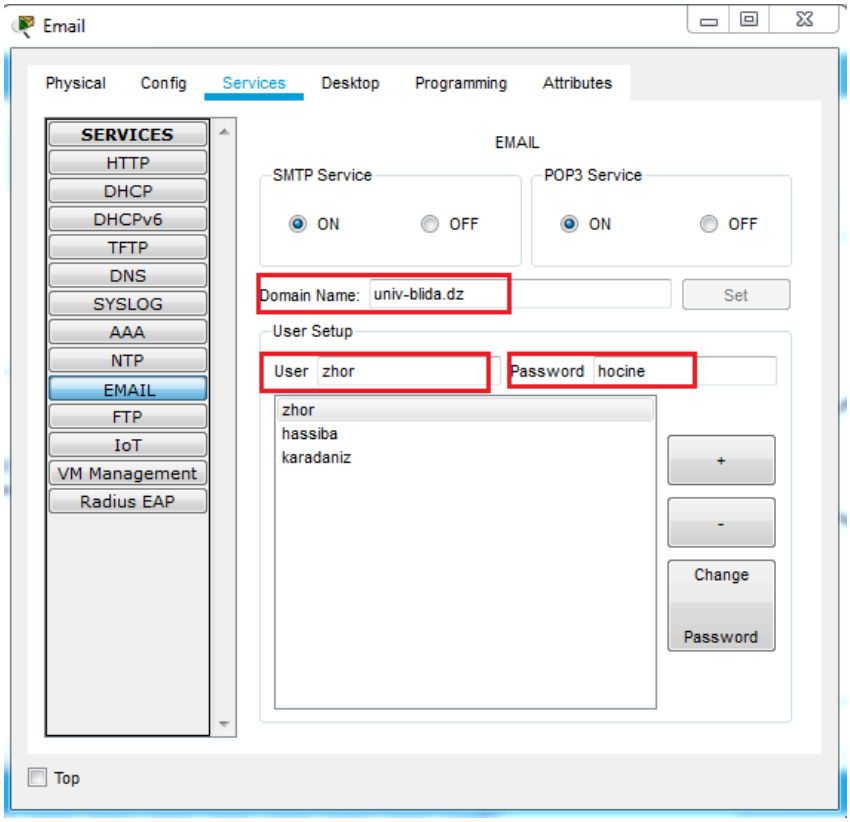

Figure 3.14. Configuration du serveur messagerie pour la cliente ''Zhor''.

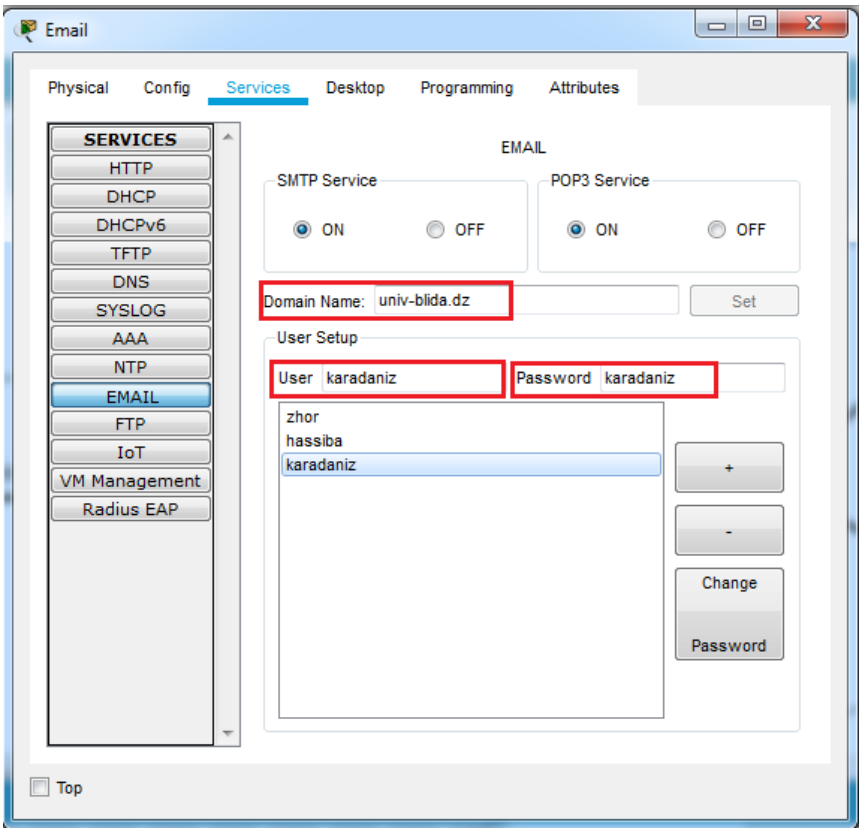

Figure 3.15. Configuration du serveur messagerie pour la cliente ‘’Karadaniz’’.

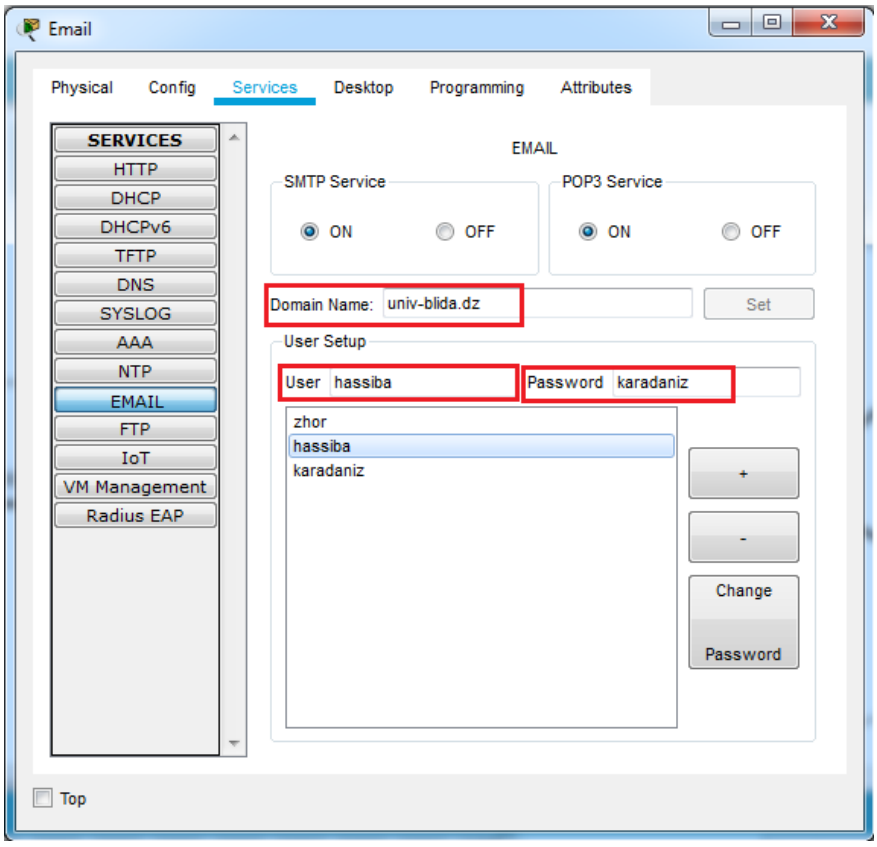

Figure 3. 16 . Configuration du serveur messagerie pour la cliente ‘’Hassiba’’.

d Serveur FTP

Le serveur FTP est un moyen de transférer des fichiers, il peut être utilisé pour lire et écrire des fichiers de configuration. De plus, le serveur FTP prend également en charge les opérations sur les fichiers telles que renommer, supprimer et répertorier les fichiers.

Dans la configuration de ce serveur nous avons créé un utilisateur (Zhor) sécurisé avec un mot de passe (Hassiba), pour que les clients puissent accéder aux fichiers de serveur FTP.

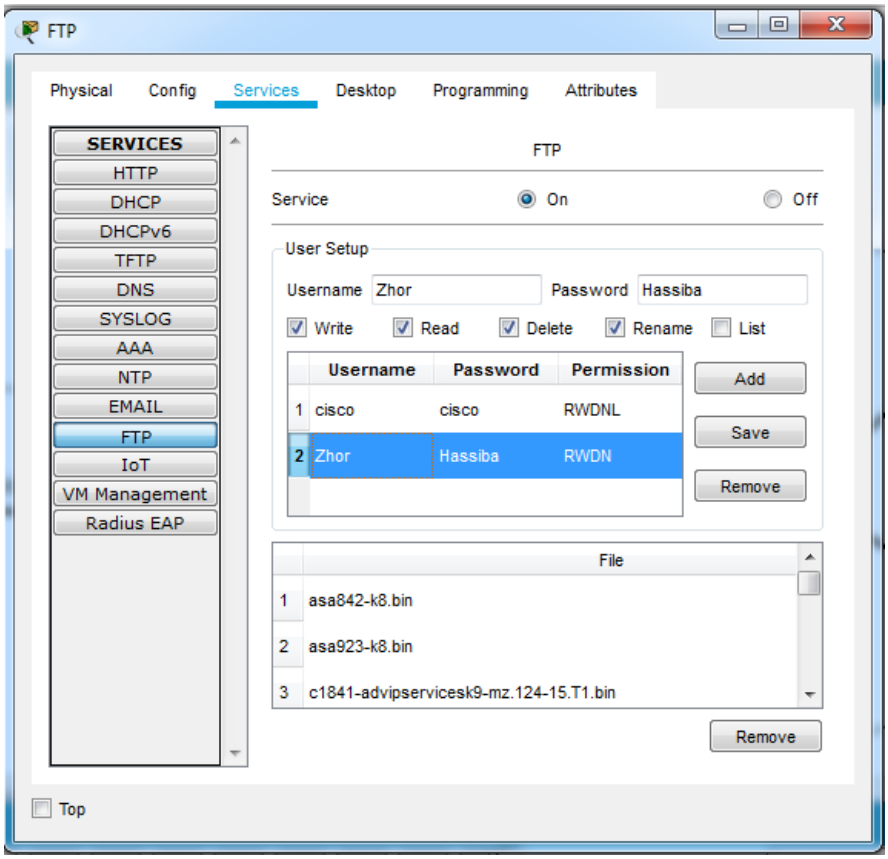

Figure 3.17. Configuration du serveur FTP.

Une fois que les clients connaissent le nom de l'utilisateur et leur mot de passe ils peuvent accéder aux fichiers de serveur FTP.

3.4.4 Configuration de routage statique

Un routeur est un équipement réseau informatique assurant le routage des paquets. Son rôle est de faire transiter des paquets d'une interface réseau vers une autre, selon un ensemble des règles. Pour acheminer les paquets, il faut introduire les adresses IP pour les interfaces, ensuite ajouté des routes statiques. Le tableau ci-dessus montre les adresses pour chaque interface.

Routeur 1 (l'extérieur de l'université Blida)		Routeur 2 (Université Blida)	
Interface	Adresse	Interface	Adresse
Fa0/0	192.168.2.10	Fa0/0	192.168.1.10
Se0/1/0	193.194.83.190	Fa0/1	192.168.3.1
		Se0/0/0	193.194.83.189

Tableau 3.4. Les adresses des interfaces des routeurs.

La figure ci-dessus montre la méthode que nous avons utilisée pour configuré l'interface de la DMZ dans le routeur université Blida:

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#interface fa0/1
Router(config-if)#ip add 192.168.3.1 255.255.255.0
Router(config-if)#no shutdown
```

Figure 3. 18. Configuration du l'interface DMZ.

Ces lignes de commande sont réalisées pour la configuration des autres interfaces.

Et voilà comment nous avons fait pour configurer des routes statiques pour chaque routeur :

a Routeur 1 (l'extérieur de l'université Blida)

Nous avons ajouté une route de réseau outside vers le réseau DMZ 192.168.3.0/24 et qu'il passe par la passerelle 193.194.8.3.189, la commande est la suivante :

```
Router(config)#ip route 0.0.0.0 0.0.0.0 193.194.83.190
```

Figure 3.19. La route statique de réseau outside vers le réseau DMZ.

b Routeur 2 (Université Blida)

Nous avons ajouté une route de réseau inside vers le réseau DMZ 192.168.3.0/24 et qu'il passe par la passerelle Fa0/0 (192.168.1.10), la commande est la suivante :

```
Router(config)#ip route 192.168.1.0 255.255.255.0 FastEthernet0/1
```

Figure 3.20. La route statique de réseau inside vers le réseau DMZ.

Et aussi nous avons ajouté une route de réseau inside (192.168.1.0) vers le réseau outside (192.168.2.0) avec la passerelle (193.194.83.190) :

```
Router(config)#ip route 192.168.2.0 255.255.255.0 193.194.83.190
```

Figure 3.21. La route statique de réseau inside vers le réseau DMZ.

3.4.5 Configuration des listes de contrôle d'accès ACLs

- Dans le routeur de l'université Blida, nous avons créé les ACLs étendues pour filtrées le trafic des paquets TCP, et pour bloquer l'accès du « PC » avec l'adresse 192.168.1.7 d'accéder vers le serveur web (elearning.univ-blida) avec l'adresse 192.168.3.3 et le port 80. Nous avons suivi la commande ci-dessus.

Access-list **numéro de la List {permit/deny} protocole** host **adresse IP source** host **adresse IP destination {opérateur (port)}**

Donc, la commande sera la suivante :

```
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 101 deny tcp host 192.168.1.7 host
192.168.3.3 eq 80
Router(config)#int fa0/0
Router(config-if)#ip access-group 101 in
Router(config-if)#exit
```

Figure 3.22. Configuration des ACLs pour bloquer l'accès au serveur elearning.univ-blida.

- Et pour que les serveurs ne soient pas saturé, nous avons créé des ACLs pour filtrées le trafic des paquets ICMP qui bloque le « ping » entre Inside et DMZ et entre outside et DMZ :

Nous avons bloqué le « ping » entre la zone Inside (192.168.1.0) et la zone DMZ (192.168.3.0) comme montre la première (1) commande de la figure (3.23), la deuxième (2) commande va permettre d'autoriser tout le reste du trafic, et pour appliquer l'ACL à l'interface fa0/1 nous avons configuré par la troisième (3) commande.

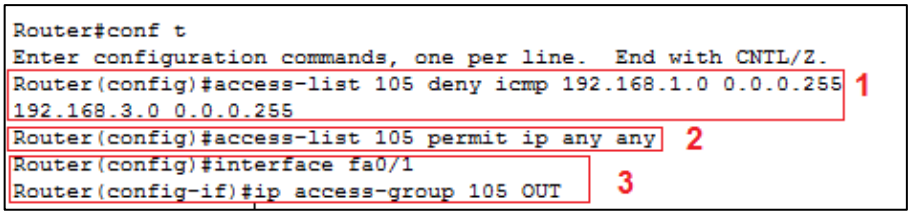

Figure 3.23. Configuration des ACLs pour bloquer le pinge entre la zone inside et la zone de DMZ.

Puis nous avons bloqué le « ping » entre la zone outside (192.168.2.0) et la zone DMZ (192.168.3.0) de la même manière présidente :

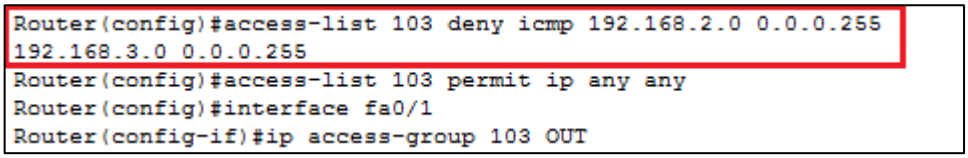

Figure 3.24. Configuration des ACLs pour bloquer le pinge entre la zone outside et la zone de DMZ.

3.4.6 Configuration de la traduction des adresses avec le PAT

Pour que les postes du réseau LAN puissent se connecter à l'extérieure il leurs faut une adresse IP routable. Nous avons appliqué le PAT pour résoudre ce problème, d'abord nous avons définis une liste d'accès qui inclura l'adresse privé du sous réseau Inside, ensuite nous avons activé le PAT et faites référence à l'ACLs créé à l'étape président et à l'interface dans l'adresse IP sera utilisé pour la traduction avec les commandes de la figure suivante :

```
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#access-list 5 permit 192.168.1.0 0.0.0.255
Router(config)#ip nat pool P2 193.194.83.91 193.194.83.99 netmask
255.255.255.0
Router(config)#ip nat inside source list 5 pool P2 overload
```

Figure 3.25. Configuration de la traduction des adresses avec le PAT.

3.5 Test et simulation

3.5.1 Test de connectivité

Pour tester si notre configuration est correcte, nous allons tester les communications avec les équipements qui appartiennent au réseau local (inside) et les serveurs qui appartiennent au réseau (DMZ) ainsi que le réseau externe (outside). Le meilleur moyen pour tester la communication est l'utilisation de la fonction ping, en envoyant des paquets de demande d'écho ICMP à l'hôte cible, puis en attendant une réponse ICMP. Il peut enregistrer le temps aller-retour et toute perte de paquets ou boucles de routage.

a Test de connectivité entre inside et la DMZ

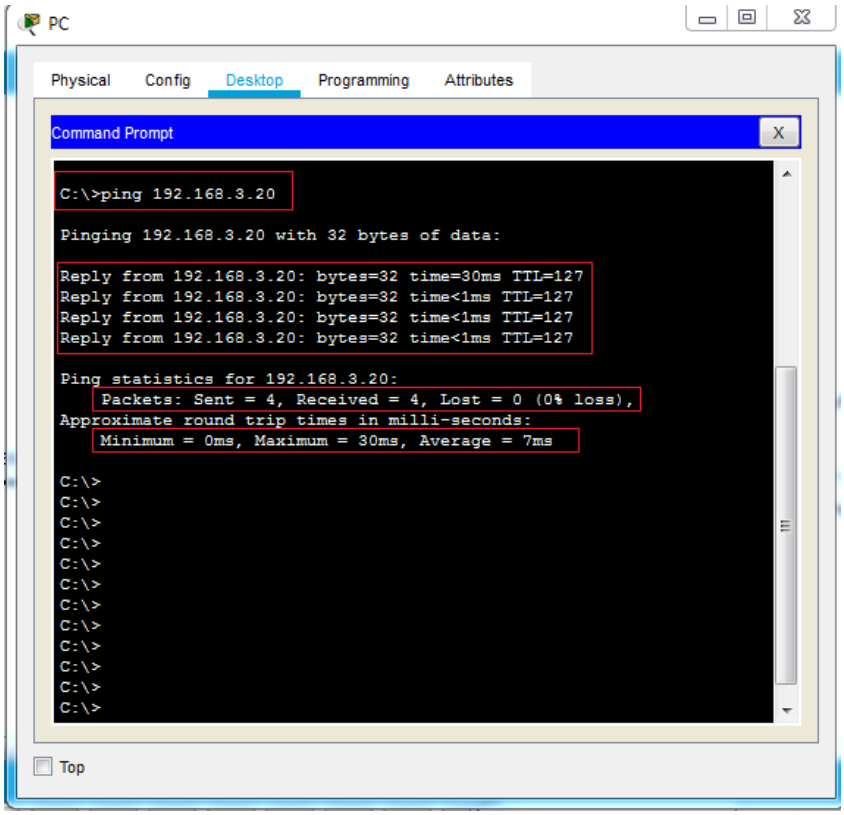

Figure 3.26. Test de connectivité entre inside et la DMZ.

Dans la vérification de la connectivité entre le réseau Inside et la DMZ, on à quatre requêtes ICMP de 32 octets chacune ont été envoyées. Les réponses ont été reçues en moins d'une milliseconde sans perte de paquets. Le temps de transmission et de réponse peut augmenter à mesure que les demandes et les réponses ICMP sont traitées par plus d'appareils pendant le trajet vers et depuis la destination.

Nous avons fait la même chose pour tester la connectivité entre Inside et outside et entre la DMZ et outside. Nous avons remarqué que les requêtes ont été bien reçues.

b Test de connectivité entre Inside et outside

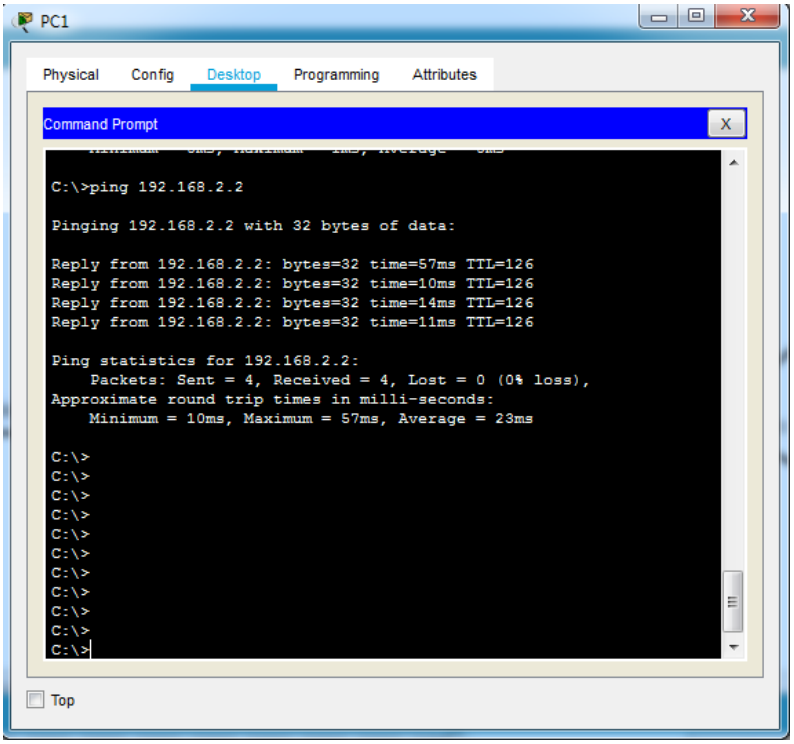

Figure 3.27. Test de connectivité entre inside et outside.

c Test de connectivité entre la DMZ et outside

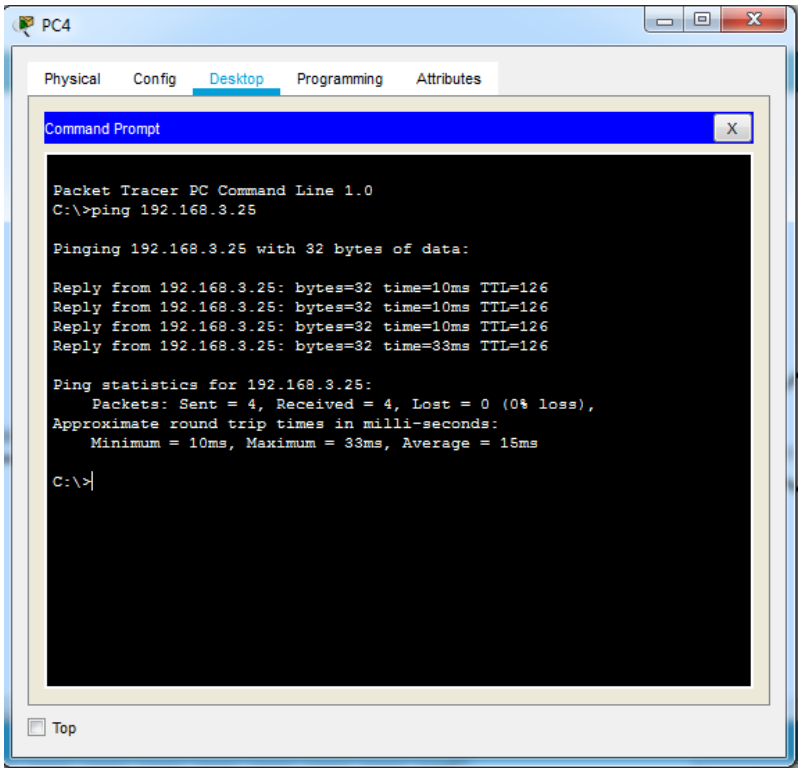

Figure 3.28. Test de connectivité entre DMZ et outside.

3.5.2 Test d'empêchements

a Test de l'empêchement de la connectivité entre Inside et DMZ

Nous avons testé l'empêchement de connectivité de réseaux Inside et outside de ne pouvoir pas envoyer des « ping » dans le réseau DMZ.

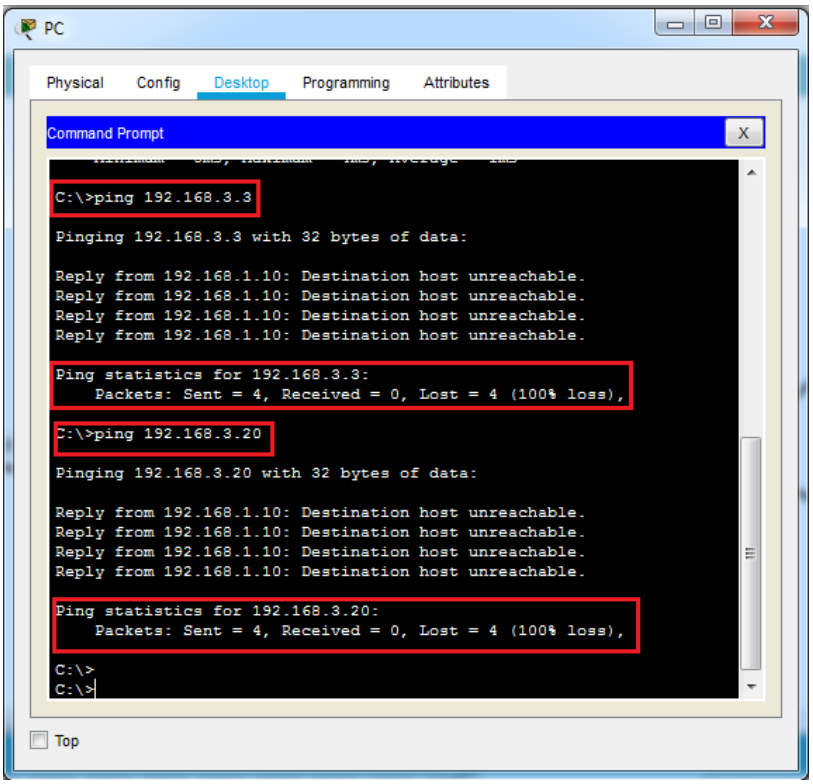

Figure 3.29. Test de l'empêchement de la connectivité entre Inside et DMZ.

Dans la vérification de l'empêchement de connectivité entre le réseau Inside et la DMZ, on à quatre requêtes ICMP de 32 octets chacune ont été envoyées mais les réponses ont été échouées.

Nous avons fait la même chose pour tester l'empêchement de connectivité entre la DMZ et outside. Nous avons remarqué que tous les requêtes ont été échouées.

b Test de l'empêchement de la connectivité entre Outside et DMZ

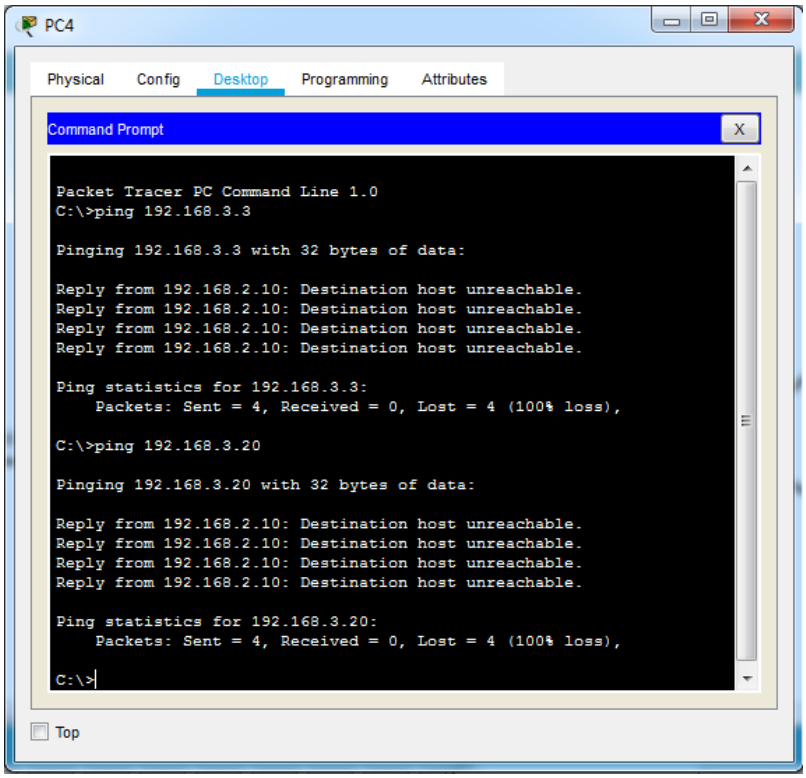

Figure 3.30. Test de l'empêchement de connectivité entre outside et DMZ.

3.5.3 Test d'accès à internet

Pour tester le bon fonctionnement de la liste de contrôle 101 crée, et le système de nom de domaine DNS, tout d'abord nous allons au réseau local, puis nous cliquons sur le PC qui a l'adresse **192.168.1.7** , ensuite sur **« Desktop »**, après sur **« web browser »** et enfin nous avons tapé l'adresse suivante: **elearning.univ-blida** au lieu **192.168.3.3** . Car, il est plus facile de se rappeler d'un nom que d'un numéro. C'est pourquoi en utilise le service DNS qui assure une correspondance entre les adresses IP des ordinateurs et les noms des domaines qu'ils les hébergent.

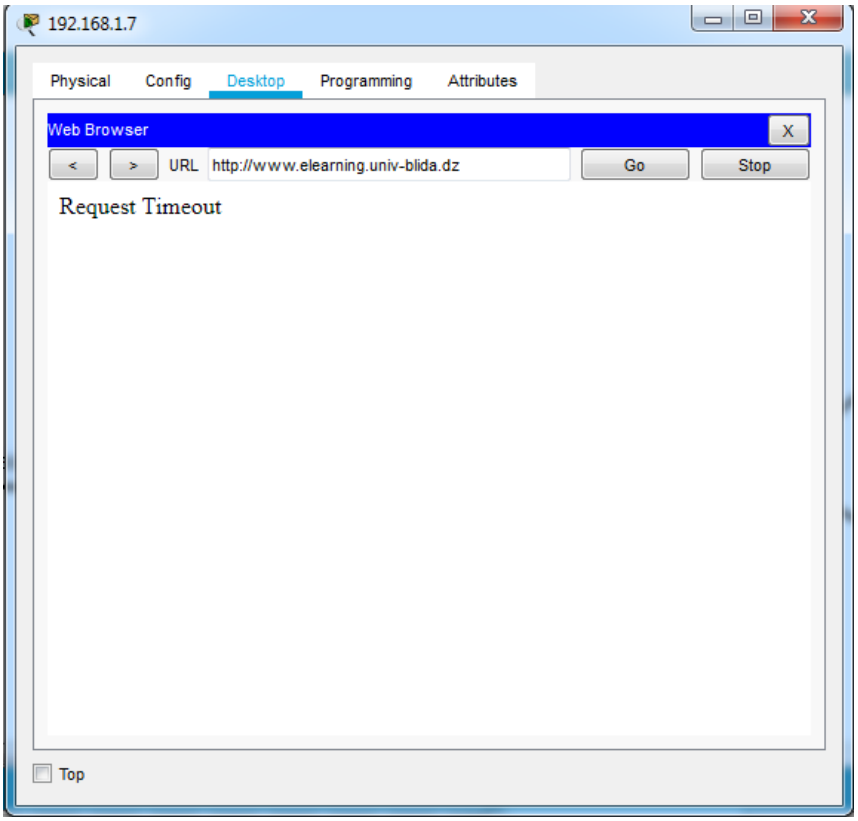

Figure 3.31. Test de blocage l'accès au serveur elearning-univ.blida.

Nous avons remarqué que le PC qui a l'adresse **192.168.1.7** est automatiquement refusé lors de l'accès à **elearning-univ.blida,** cela revient au choix de notre configuration.

Mais nous pouvons accéder à un serveur **elearning-univ.blida** par un autre PC qui a l'adresse 192.168.1.6, comme montre la figure suivante :

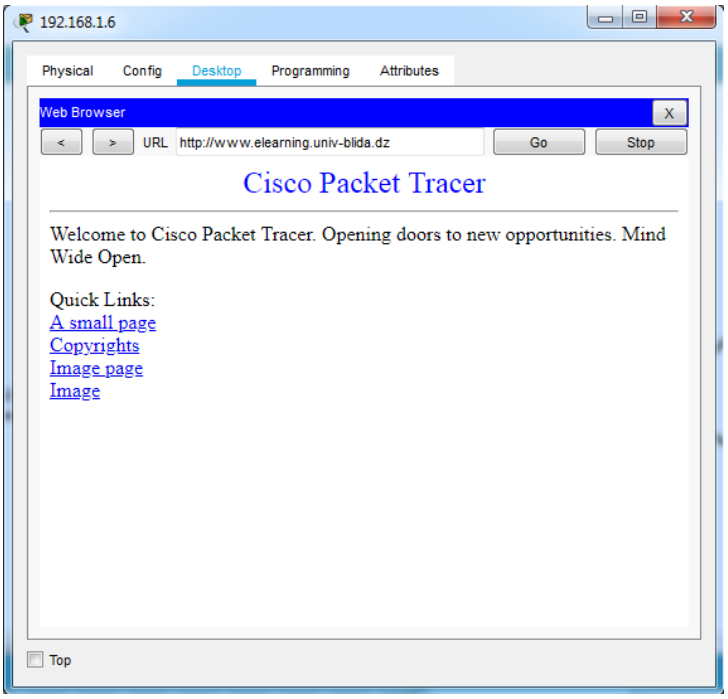

Figure 3.32. Test d'accès au serveur elearning.univ-blida.

Donc nous en concluons que si on active les ACLs étendues sur les interfaces pour les paquets entrants ou sortants, le routeur de l'université Blida cherche dans la liste de manière séquentielle. C'est pour ça l'accès aux serveurs de la zone démilitarisé peut être bloqué ou autorisé.

3.5.4 Test de fonctionnement du serveur FTP

- Tous d'abord on tape sur n'importe quel PC qui appartient au notre réseau pour envoyer des fichiers à un serveur FTP configuré dans le serveur, à partir de **« command prompt »** de PC0, nous avons utilisé l'adresse IP du serveur en tapant *ftp 192.168.3.25* comme montre la figure suivante :

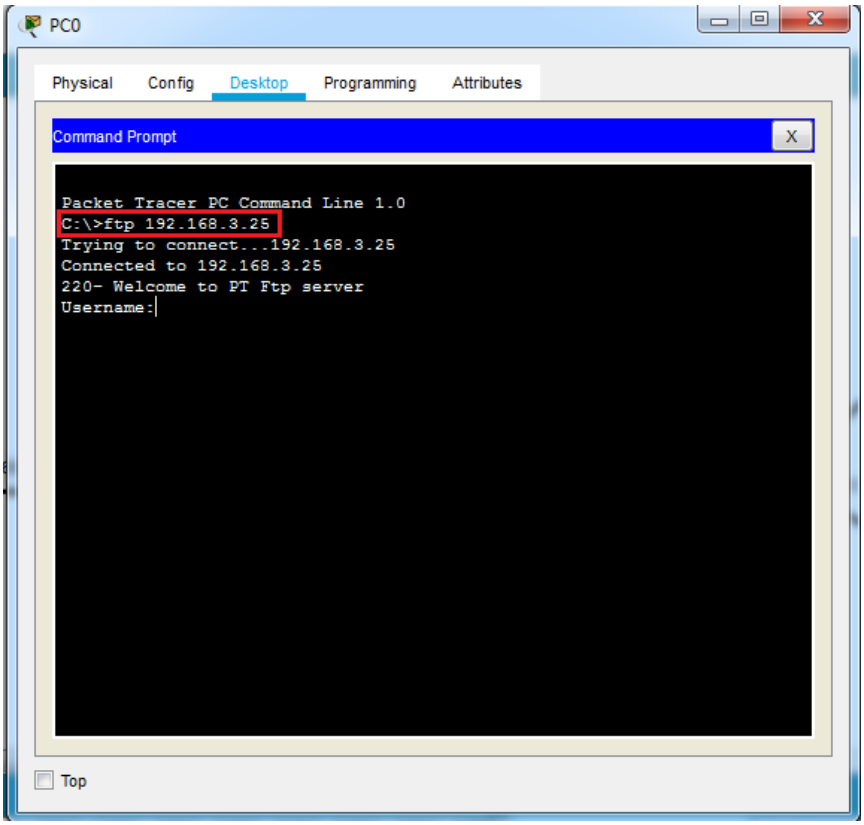

Figure 3.33. Demande d'accès serveur FTP.

- Nous avons fourni le nom d'utilisateur **« Zhor »** et le mot de passe **« Hassiba »** pour la connexion ftp :

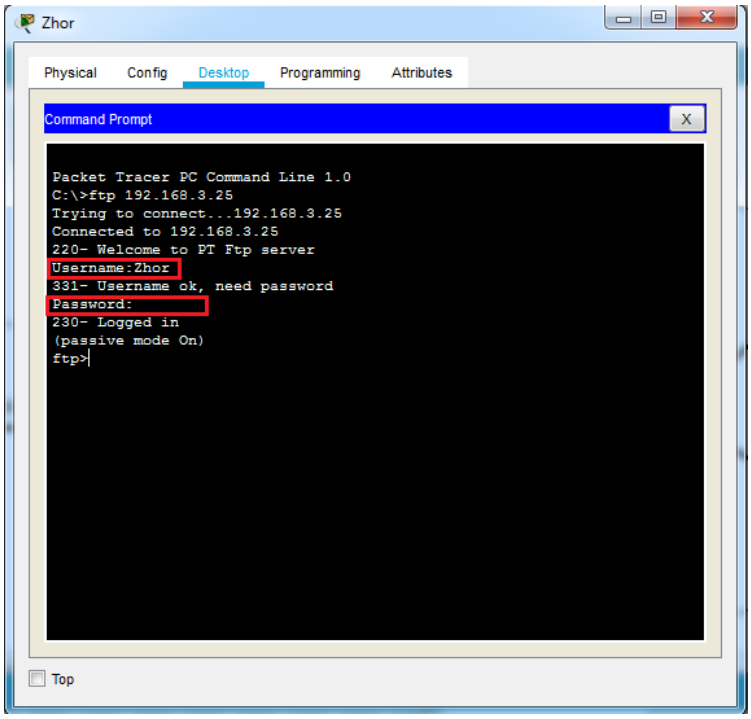

Figure 3.34. L'accès au serveur FTP.

Le PC0 dispose d'un client FTP qui peut être utilisé pour lire, écrire, supprimer et renommer les fichiers présents sur le serveur FTP.

- Nous avons testé l'accès aux fichiers, nous fessons ceci :

Nous avons tapé la commande « **dir** » qui permet d'afficher le contenu d'un répertoire du serveur FTP comme montre la figure suivant :

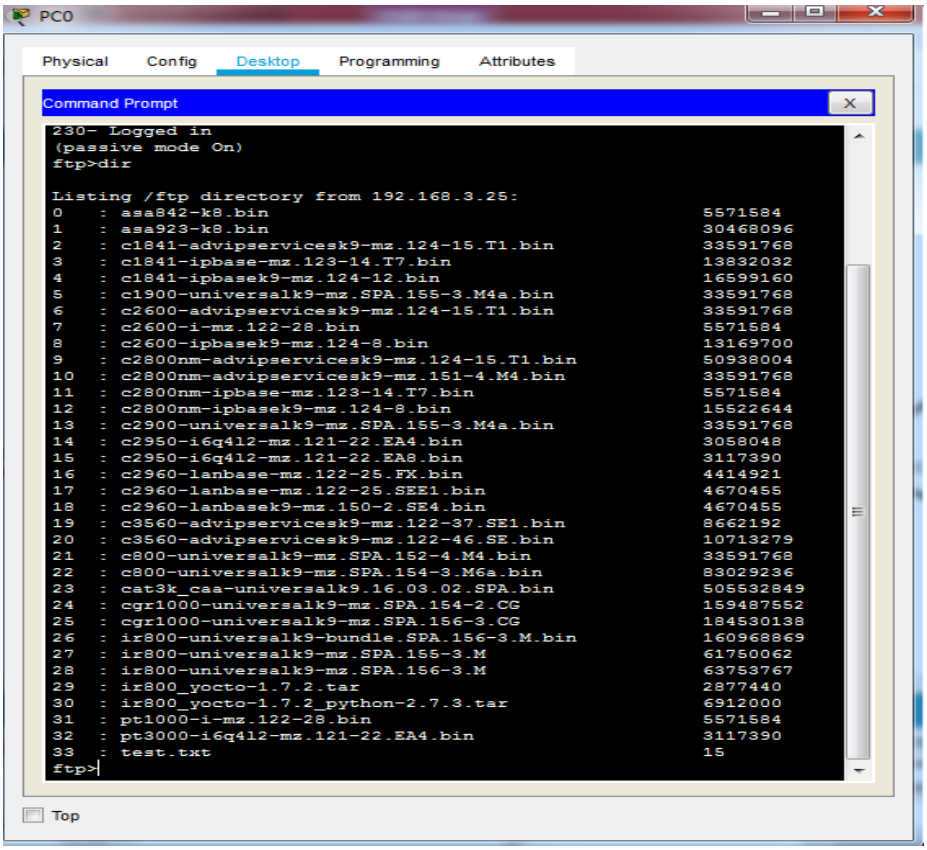

Figure 3.35. Le contenu d'un répertoire du serveur FTP.

- Nous avons comparé les fichiers du répertoire du serveur FTP affichés avec les fichiers dans le serveur lui-même :

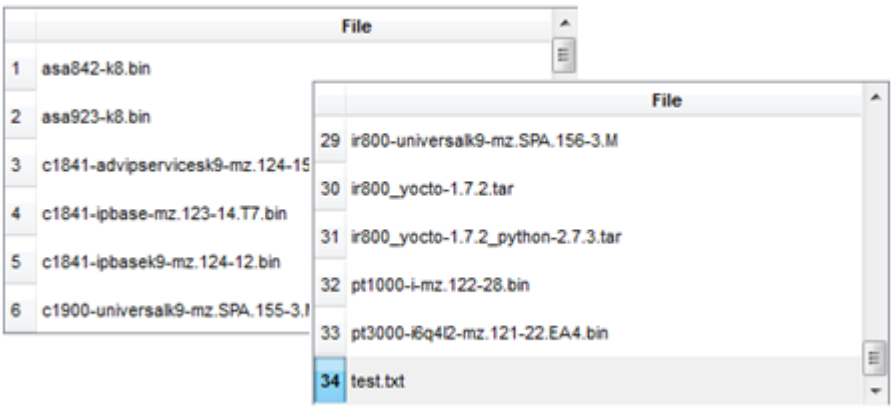

Figure 3.36. Vérification des fichiers du répertoire du serveur FTP.

Nous avons remarqué que sont les mêmes fichiers.

- Nous avons créé un fichier dans le PC0, puis l'avons téléchargé sur le serveur FTP. Pour ce faire, nous avons cliqué sur **« Text Editor »**, puis nous avons tapé n'importe quel texte dans l'éditeur par exemple **« Hello »**, l'avons nommé **« fichier.txt »** et nous l'avons enregistré :

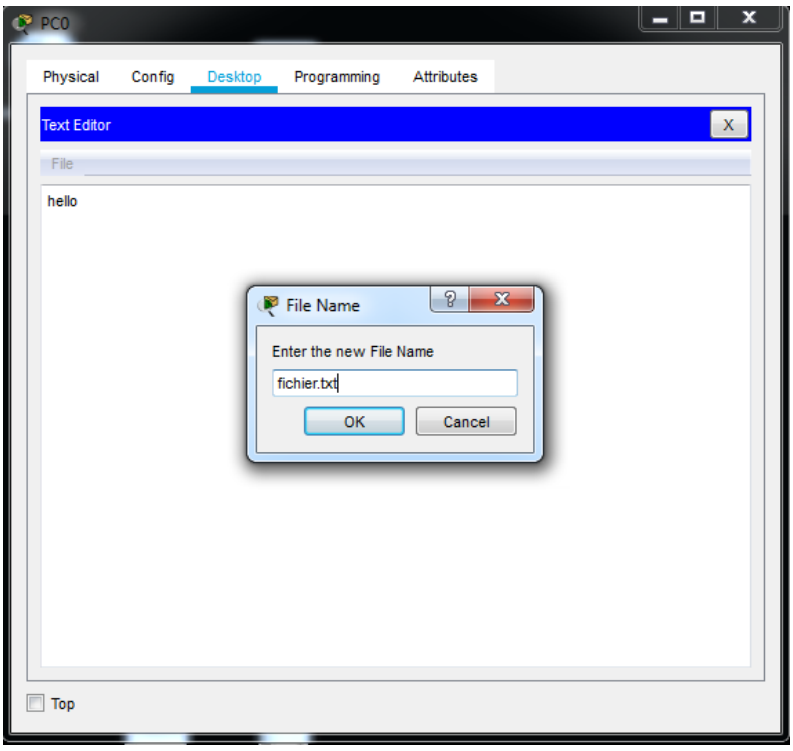

Figure 3.37. L'enregistrement de fichier.

Et pour télécharger ce fichier de PC0 vers le serveur nous avons utilisé la commande **« put ».**

```
ftp>put fichier.txt

Writing file fichier.txt to 192.168.3.25:
File transfer in progress...

[Transfer complete - 5 bytes]

5 bytes copied in 0.086 secs (58 bytes/sec)
ftp>
```

Figure 3.38. Téléchargement de fichier vers le serveur.

Une fois le téléchargement du fichier réussi, nous avons accédé au **« File FTP »** du serveur pour vérifier si le fichier envoyé a bien été reçu. Pour ce faire, nous allons dans **« Serveur FTP », « Services »** et **« FTP »**

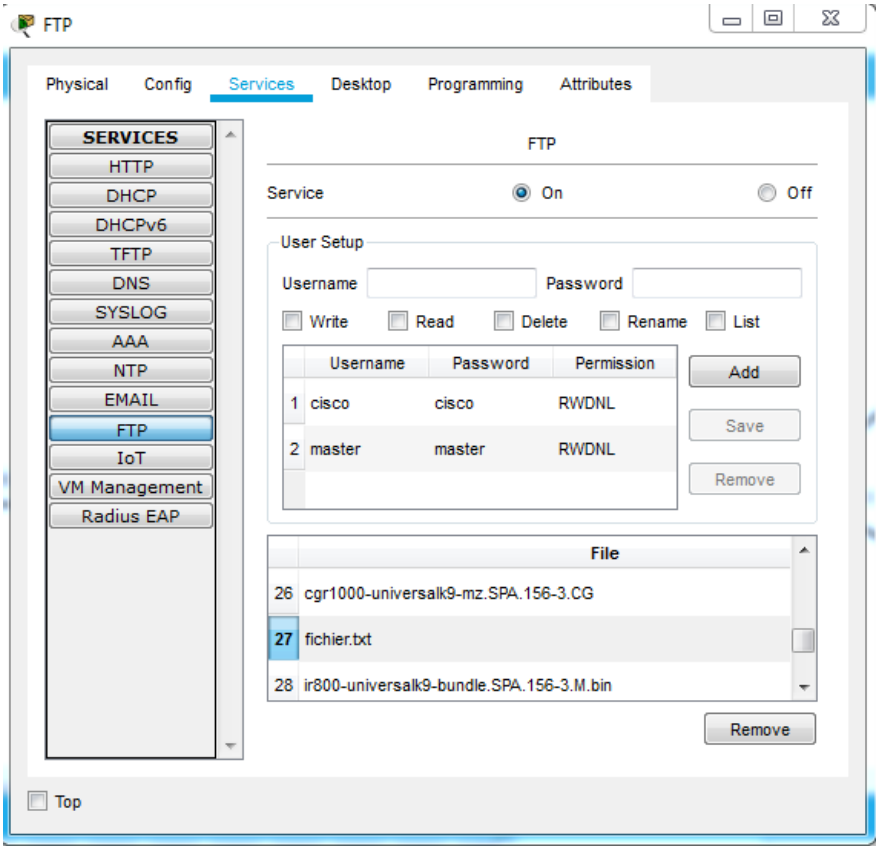

Figure 3.39. Vérification que le fichier.txt est au répertoire du serveur FTP.

Donc nous avons remarqué que le fichier envoyé par le PC0 a bien été reçu.

- Nous avons ouvrir un répertoire HTTP sur le serveur en tapant : **« cd /http »** dans la **« Command Prompt »** du PC client. Cela changera le répertoire actuel du répertoire FTP au répertoire http.

```
ftp>cd /http
ftp>
Working directory changed to /http successfully
```

Figure 3.40. L'accès au répertoire http.

Une fois le répertoire http ouvert, nous pouvons télécharger un fichier sur le serveur HTTP. Tout d'abord, nous allons créer un fichier html sur le PC0 comme montre la figure (3.41) suivante :

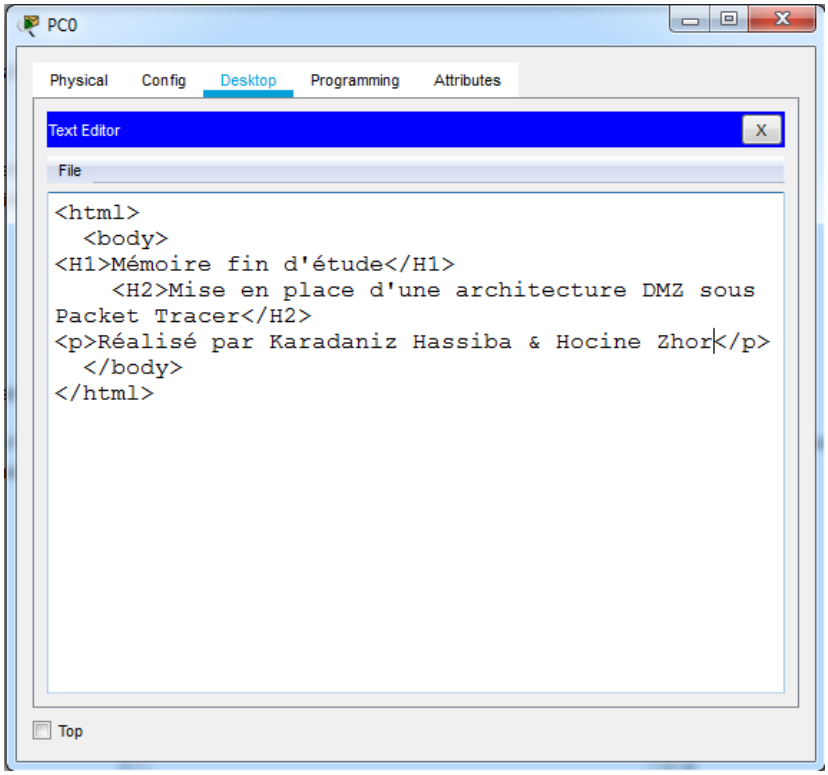

Figure 3.41. Création d'un fichier html.

Puis nous enregistrons notre fichier en tant que fichier html comme ceci :

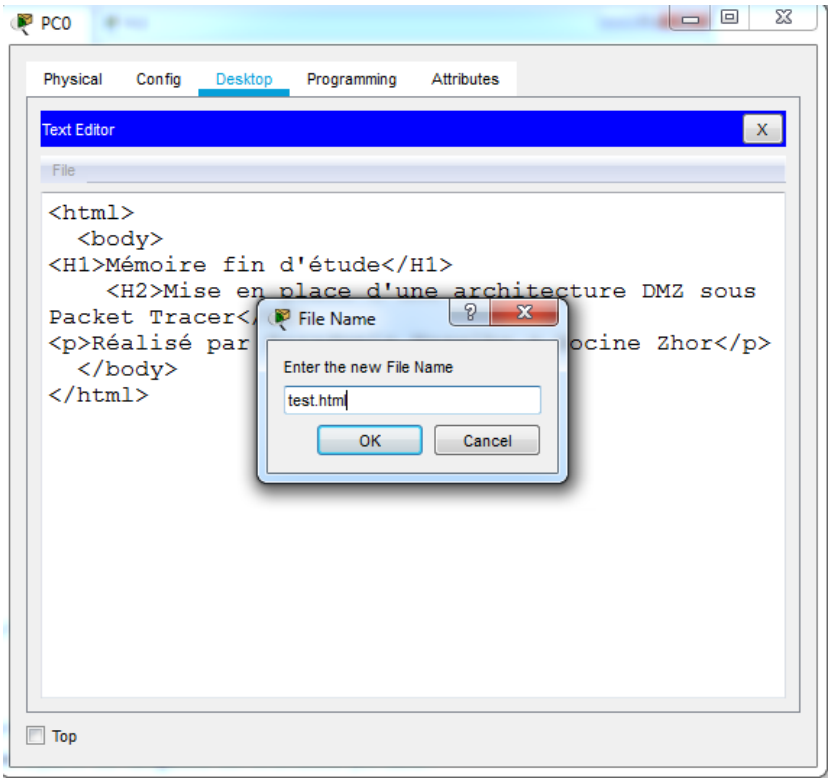

Figure 3.42 **.**L'enregistrement du fichier html.

Après, nous avons téléchargé ce fichier dans le dossier HTTP en utilisant la commande **put test.html** comme montre la figure suivant :

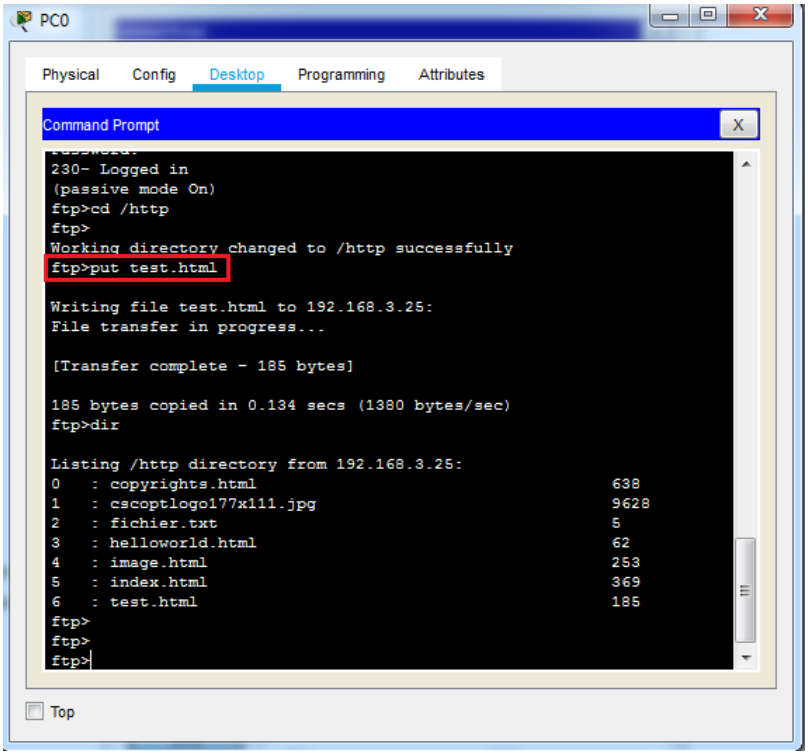

Figure 3.43. Téléchargement de fichier html vers le serveur.

Alors, nous pouvons vérifier dans le **« File http »** du serveur que le fichier téléchargé depuis le PC0 test.html est bien reçu :

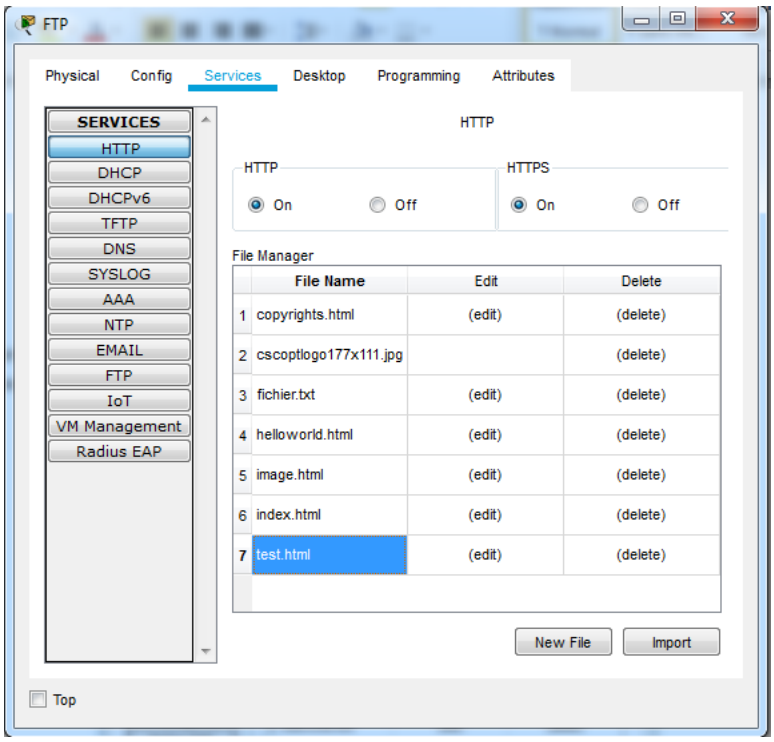

Figure 3.44. Vérification que le fichier html est au répertoire du serveur http.

Notons que nous avons téléchargé des fichiers dans un répertoire du serveur HTTP à l'aide du protocole de transfert de fichiers (FTP). Cela rendra test.html accessible depuis le navigateur des PC du réseau local, et on peut l'édité au niveau du serveur.

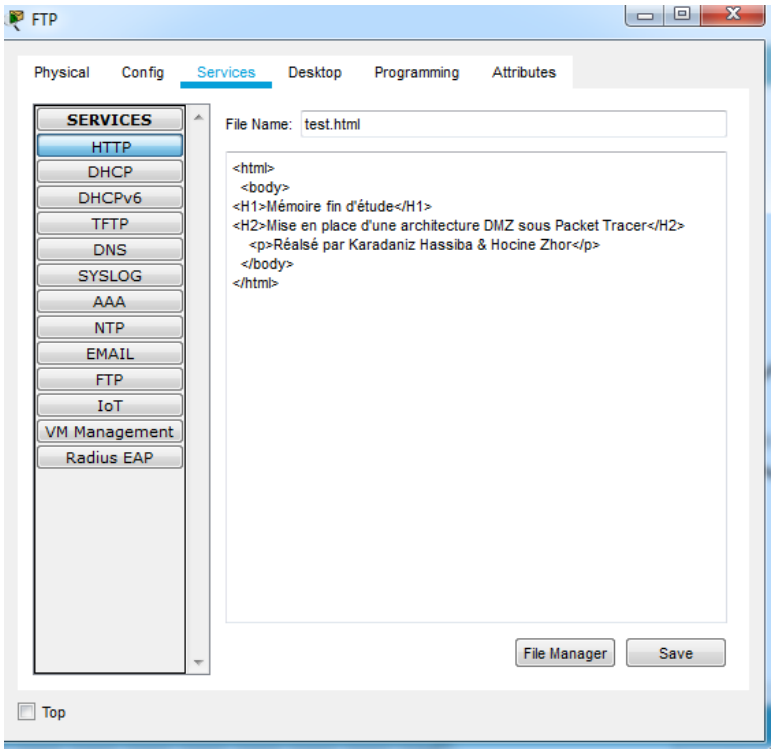

Figure 3.45. Le contenu du fichier test.html.

Enfin, nous avons essayé d'accéder au fichier à partir du navigateur de PC0 :

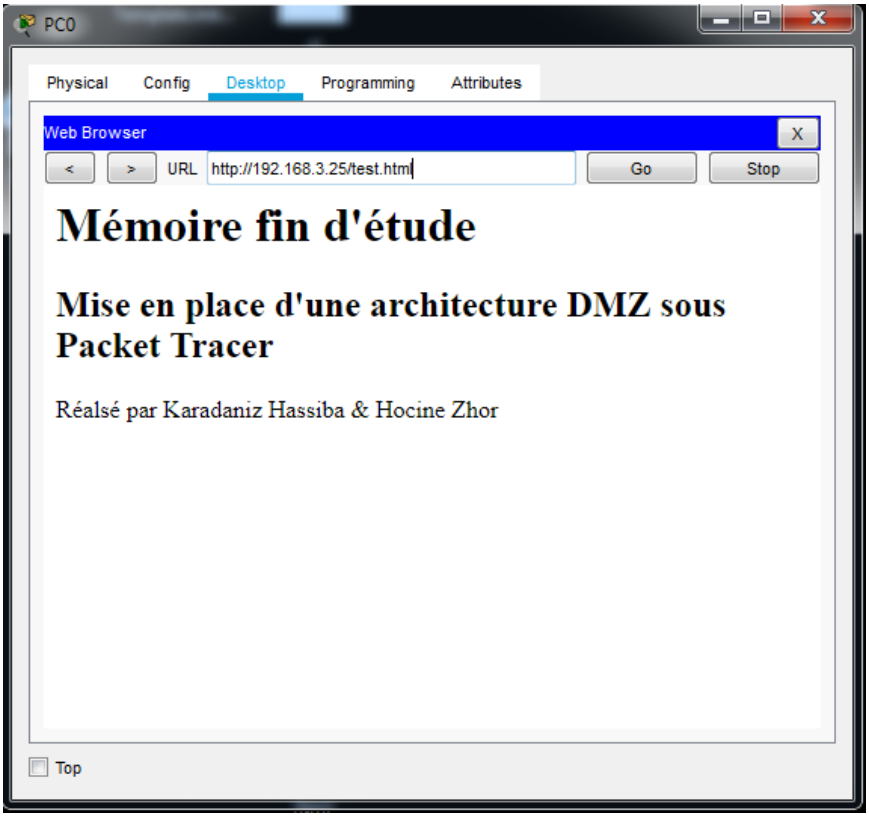

Figure 3.46. L'affichage de la page test.html.

Donc le navigateur envoie une requête http au serveur, puis Le serveur répondra à notre PC0 et affiche le fichier que nous avons créé.

3.5.5 Test d'échange de courriel

Pour tester le service de messagerie dans le réseau local. Nous avons accédé à la cliente de messagerie PC ''Karadaniz'', puis nous avons écrié un email et nous l'avons envoyé à l'adresse email PC ''Zhor'':

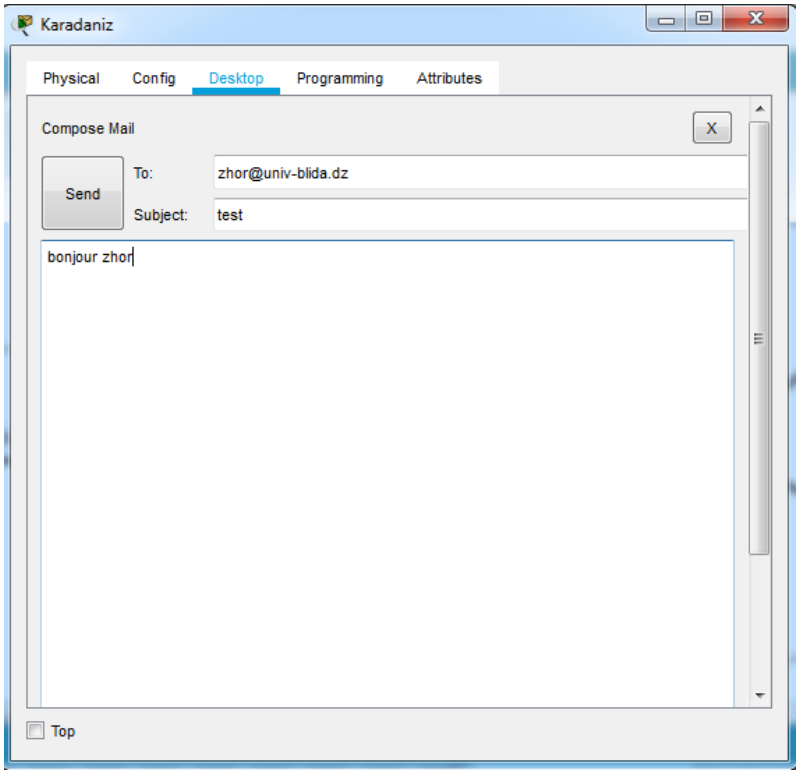

Figure 3.47. La composition d'un e-mail.

Ensuite nous avons essayé de voir si l'email de PC Karadaniz est reçu. Sur la cliente de messagerie Zhor, nous avons cliqué sur **« Receive » :**

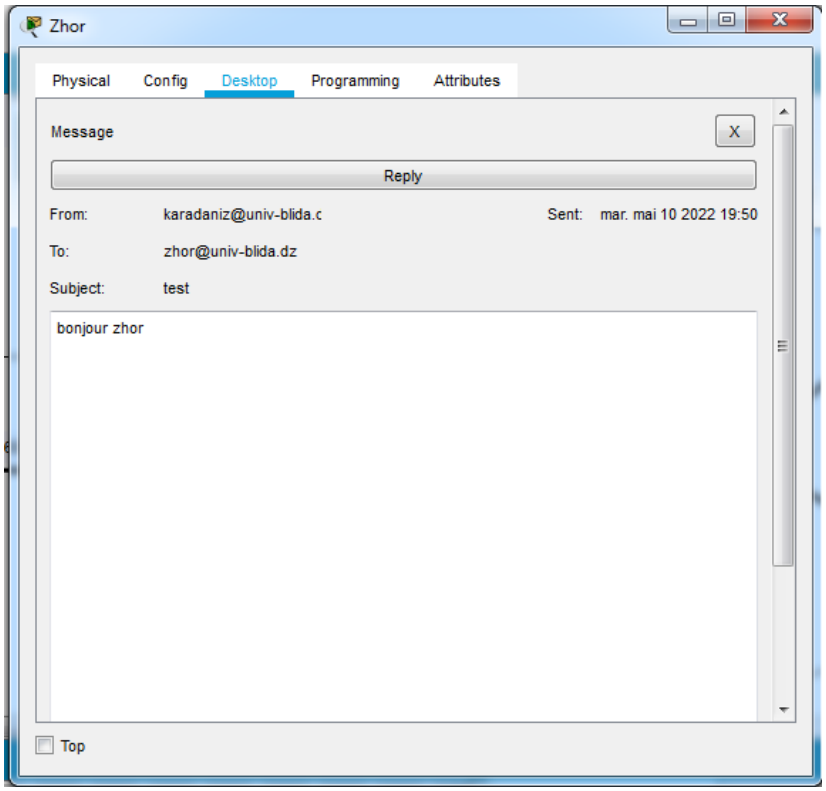

Figure 3.48. La réception de l'email.

Nous avons remarqué que tout est bien configuré, le mail de PC Karadaniz sera bien reçu sur PC Zhor**.**

Puis nous avons testé l'échange de courriel échangé du réseau outside vers le réseau inside. Nous avons accédé à la cliente de messagerie Hassiba**,** puis nous avons écrié un email et l'envoyé à la cliente Zhor

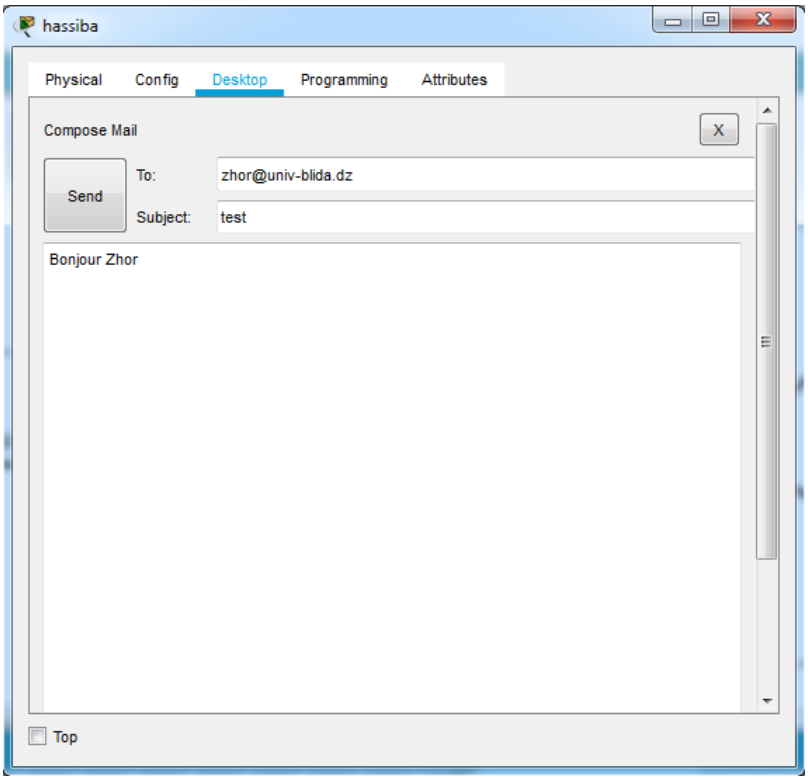

Figure 3. 49. La composition d'un e-mail.

Ensuite nous avons essayé de voir si l'email de La cliente Hassiba est reçu. Sur la cliente de messagerie Zhor, nous avons cliqué sur **« Receive » :**

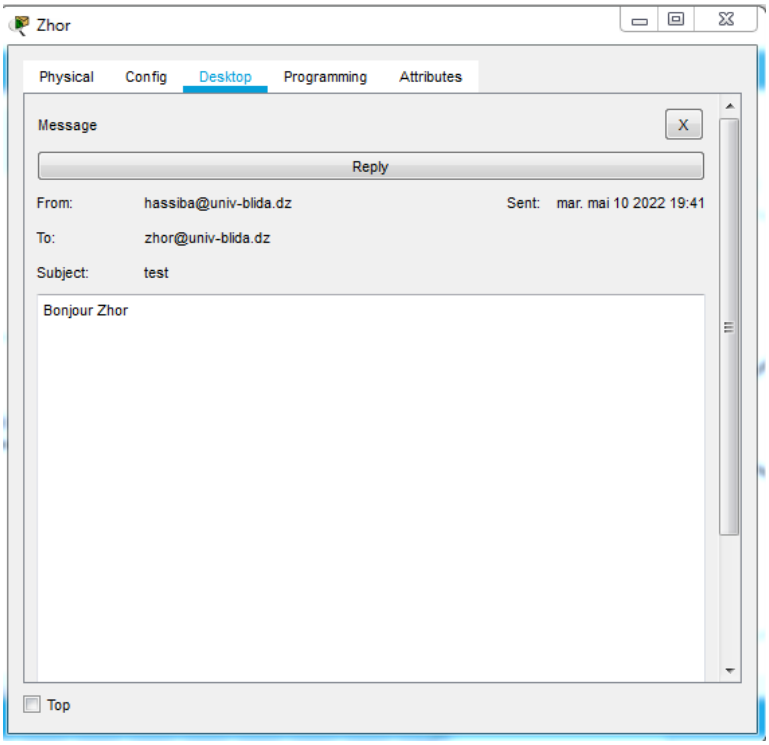

Figure 3.50. La réception de l'email.

Nous avons remarqué que tout est bien configuré, le mail de la cliente Hassiba est bien reçu sur PC Zhor.

3.5.6 Test du traduction des adresse avec le PAT

Pour tester la configuration de la traduction des adresses avec le PAT, nous avons utilisé la commande **do debug ip nat** dans le routeur de l'université blida pendant que nous avons envoyé un **ping** provenant de 192.168.1.7 (Inside) destiné à 192.168.2.4 (outside). Et de 192.168.1.5 (Inside) destiné à 192.168.2.4 (outside). Les résultats du débogage sont ci-dessous :

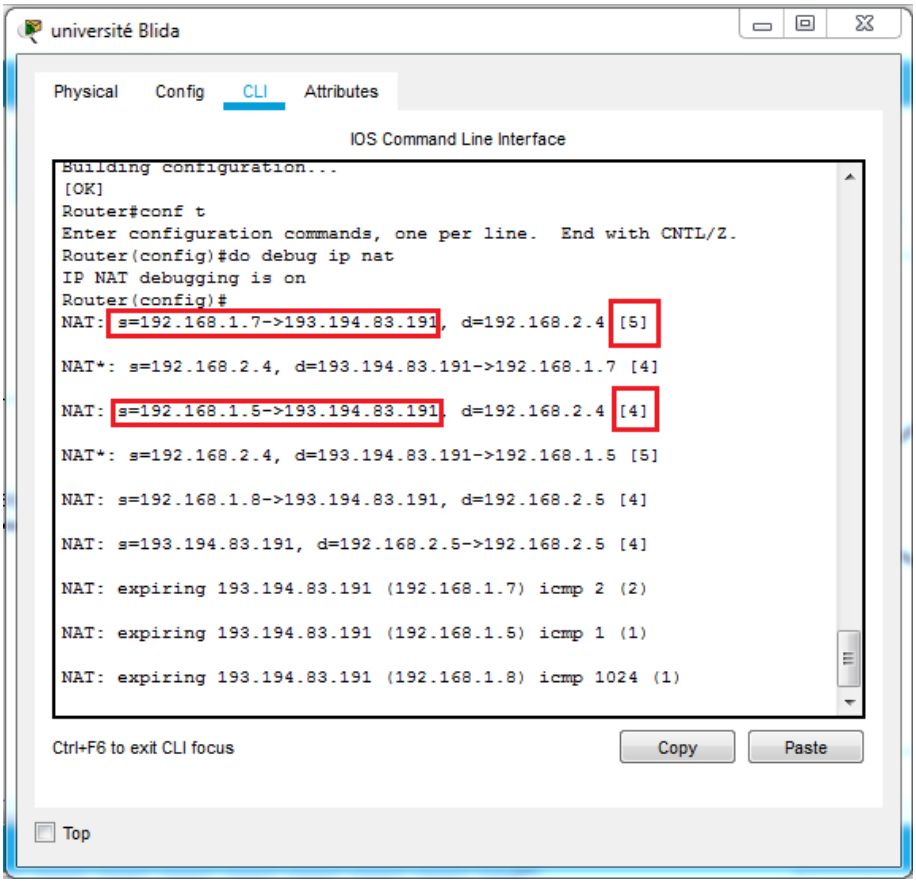

Figure 3.51. Les résultats de débogage.

Nous remarquons sur la figure (3.51) que la même adresse IP (193.194.83.191) a été utilisée pour traduire les adresses IP privées (192.168.1.7, 192.168.1.5). Ainsi, lorsque le routeur de l'université Blida répond à (192.168.2.4, 192.168.2.3), il examine sa table de traductions NAT et il transmet la réponse (192.168.1.7, 192.168.1.5). Cela nous indique que le routeur traduit les paquets dans les deux sens.

Donc avec la traduction d'adresse du port (PAT), une seule adresse IP publique est utilisée pour toutes les adresses IP privées internes, mais un port différent est attribué à chaque adresse IP privée.

3.6 Conclusion

Pour la mise en place de notre projet nous avons commencé par présenter une analyse des besoins et nous avons étudié l'architecture de notre réseau. Ensuit nous avons utilisé Packet Tracer pour simuler et configurer notre architecture réseau, qui contient plusieurs fonctionnalité tel que DMZ, ACLs, PAT,… Autrement dit, nous avons présenté l'implémentation et la mise en œuvre de l'architecture déployée sur le simulateur afin de tester les fonctionnalités mise en place.

Conclusion générale

Notre projet s'inscrit dans la continuité de notre formation, et répond à une des problématiques les plus importantes des réseaux informatique, qui est la sécurité.

Après avoir exposer certaines généralités sur les réseaux informatiques, nous nous somme intéressé à un point important et crucial aussi bien pour les entreprises que pour les particuliers, qui est la sécurité des réseaux informatiques et les moyens de l'assurer.

Nous avons étudié les différentes techniques de renforcement de la sécurité dans un réseau informatique. Afin de tester ces différentes, nous avons choisis un réseau d'une architecture client/serveur constitué de trois zones (deux réseaux locaux et un réseau DMZ) reliés entre eux par un routeur de sécurité qui permet la communication entre les réseaux, grâce à leur interface connectée en direct sur chacun des réseaux. La DMZ est considérée comme une zone tampon entre le réseau Internet et le réseau interne d'une entreprise ou d'un particulier, elle permet de fournir des services exposés et accessible depuis l'extérieur afin d'offrir aux utilisateurs une gestion efficace et simplifie pour la récupération des données. Comme le serveur web qui se charge sur la diffusion du contenu des sites Web, le serveur de messagerie qui achemine des emails d'un expéditeur à un ou plusieurs serveurs destinataires, le serveur FTP agit d'un moyen codifié d'échange des fichiers entre plusieurs ordinateurs et le serveur DNS Permet d'associer un nom compréhensible, à une adresse IP.

Nous avons aussi utilisé certaines fonctionnalités de renforcement de sécurité sur le routeur tel que l'ACLs pour bloquer et autoriser les ports d'entrée du réseau et filtrer le trafic, ainsi que le pat pour traduire les adresses privées d'un réseau interne vers des adresses publiques d'un réseau externe, selon les exigences et la politique adopté par cette étude. Pour mettre notre solution en pratique nous avons utilisé le simulateur «

PACKET TRACER » qui permet aux utilisateurs de construire un propre réseau physique virtuel à l'aide des équipements Cisco avant de passer à la configuration réelle.

Ce travail nous a permis de mettre en pratiques les connaissances acquises durant notre cursus universitaire, de les approfondir et de les mettre en pratique.

Nous avons suivi les différentes étapes de réalisation d'un projet, ainsi que les techniques développées par les spécialistes du domaine pour assurer l'efficacité et la bonne réalisation des travaux en se limitant aux ressources et à des durées de temps exactes. Nous avons pu voir la complexité de la mise en route d'un nouveau projet et de sa rapide évolution qui nous a appris à mieux nous organiser afin d'être capable de finaliser notre travail.

Nous espérons que notre travail permette à de futures étudiantes et étudiants de mieux comprendre les aspects aborder.

Nous proposons comme perspectives à ce travail de compléter par l'ajout de Firewall pour la protection des ressources logiciels et matériel aussi bien des entreprises que des particuliers.

Bibliographie

[1] Philippe Atelin « Réseaux informatiques - Notions fondamentales », Eni éditions, 12 janvier 2009.

[2] Cisco Networking Academy, « Câblage à fibre optique », cour CCNA1-P6 version7.02, rubrique4.5.1, 7avril 2022, Récupéré par : https://www.netacad.com/ .

[3] Nahin, Paul J. (2002). Oliver Heaviside : La vie, le travail et les temps d'un génie électrique de l'ère victorienne. ISBN 0-8018-6909-9.

[4] Cisco Networking Academy, « Câblage à paire torsadée », cour CCNA1-P6 version7.02, rubrique4.4.1, 7avril 2022, Récupéré par : https://www.netacad.com/ .

[5] Cisco Networking Academy, « composants réseau », cour CCNA1-P6 version7.02, rubrique1.2.1, 7avril 2022, Récupéré par : https://www.netacad.com/ .

[6] Cour « Formation réseaux informatiques, internet », Récupéré par : https://www.informatique-bureautique.com/moodle/mod/page/view.php?id=189&forceview=1 .

[7] https://fr.wikipedia.org/wiki/Commutateur_r%C3%A9seau

[8] https://web.maths.unsw.edu.au/~lafaye/CCM/lan/gateway.htm

[9] S.ALICHE, A.HADDAD « Implémentation d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de TIZI OUZOU », mémoire de fin d'étude Master électronique, UMMTO, 2011.

[10] Ramandaniainy Oliva Michaël « Mise en place d'un serveur proxy et système de sécurisation des réseaux sous linux », Ecole supérieure polytechnique d'Antananarivo département, 16 juin 2011.

[11] Algorithmique des réseaux et des télécoms, Chapitre 2 : Réseaux Pair à Pair, Notes de cours (ENS Lyon, M1), 2006.

[12]https://www.technoscience.net/definition/3743.html?fbclid=IwAR3NF_knNyrtLdVbwDmB6JLQIVgLmzKZ83ameAeQm054PSAYzzIAV3Wpw3o

[13] H.ZENTICI, Y.BEDDAICH, « Etude et Simulation d'une architecture réseau mixte sécurisée d'une Carte d'itinéraire IPSEC VPN et NAT », mémoire de fin d'étude de master académique, 2019.

[14] Verlain Lelo Nzita, « Etude et déploiement des stratégies sécuritaires couvertes d'une infrastructure réseau dans un environnement public », 2012. Récupéré par : https://www.memoireonline.com/ .

[15] B.Belhadj, Y.Hamadouche « Etude et sécurisation d'une infrastructure DMZ avec ASA CISCO551 » Université Mouloud Mammeri de Tizi-ouzou, 2015.

[16] https://www.editions-eni.fr/ .

[17] « Glossaire des protocoles réseau », édition livres pour tous, Mai 2009. Récupéré par : http://www.livrespourtous.com/ .

[18] Cours d'adressage IPv4, 2 éme année LMD, Université Mohamed Khider – Biskra, 2021/2022.

[19] Raphael Yende « Support de cours de sécurité informatique et crypto » Master, Congo-Kinshasa, 2018. Récupéré par : https://hal.archives-ouvertes.fr/cel 01965300/document

[20] Florian burnel, Cours - Tutoriels, Administration Réseau « Informatique : c'est quoi une DMZ ? » 07/12/2021. Récupéré par : https://www.it-connect.fr/.

[21] Barracuda Networks « Réseau DMZ », 2003, Récupéré par : https://fr.barracuda.com/.

[22] https://www.ionos.fr/digitalguide/.

[23] Haddache, « le protocol DHCP-dynamic-host-configuration », 2010/2011.

[24] Asma Rachid, « Mise en place d'un Serveur Proxy « Wingate » sous Windows », 2016/2017.

[25] https://www.avast.com/c-academy.

[26] Mickael Dorigny, « Routage statique et routage dynamique », 02/01/2014. Récupéré par : https://www.it-connect.fr/.

[27] WayToLearnX Réseau, « Différence entre NAT et PAT », 29 juillet 2018.

[28] https://www.solutions-numeriques.com/dossiers/lintegration-imprime-son-rythme-au-datacenter/?fbclid=IwAR1woJWo9PwoRA-zZ85Xx2W5fOkPWJD7z7wJLKzTYBUE7Kuw8ZPMVM9z1X0 consulté le 09/05/2022

[29] https://www.blackbox.be/wa-be/page/27215/Resources/Technical-Resources/Black-Box-Explains/fibre-optic-cable/fibre-optic-cable-construction?fbclid=IwAR11EQbPTTJp2MNWKu-JMw2PXVpmLHCj0W0KSiBCYqYH6J-t2IOVEw4qvwM consulté le 09/05/2022

[30] https://www.fast-com.ca/quest-ce-que-la-fibre-optique/ consulté le 09/05/2022

[31] https://www.futura-sciences.com/tech/definitions/electronique-cable-coaxial-4388/?fbclid=IwAR0cps2IGc6Y1mO-x6StaEBHVNJ1kUP98iWJRoePmLUSjwAjCqXue0Rmosc consulté le 09/05/2022

[32] https://techno-skills.com/reseaux/les-fondamentaux/comparaison-des-types-de-cablage-et-dinterface-physique/?fbclid=IwAR1biwdHBSqw2PE9PNd7L5MTqocQeJIxGAYeChgaUc3EPhXHOLamaCc2EII consulté le 09/05/2022

[33]https://fr.wikipedia.org/wiki/Paire_torsad%C3%A9e?fbclid=IwAR3j24OeQPnqmfuFk8CJ76zh8UOVRlY46GG5DpaF6XFEM3hF9K4rJazTOho consulté le 09/05/2022

[34] Chouraqui, « Complément réseau », USTO-MB, 2014/2015

[35] https://n0tes.fr/2022/03/10/LAN-MAN-WAN-et-le-reste/ consulté le 10/05/2022

[36] https://geekflare.com/fr/computer-networking-basics/ consulté le 10/05/2022

[37] https://waytolearnx.com/2018/07/difference-entre-les-reseaux-client-serveur-et-peer-to-peer.html consulté le 10/05/2022

[38] https://www.proconcept-service.com/installation-reseau/ consulté le 10/05/2022

[39]https://fr.wikipedia.org/wiki/Couche_transport?fbclid=IwAR06cLvNoJWPAWAuCJKPvq54_Lo96-ToMKrjYpkjfNTPFTKMdJ9OPHf7xSw consulté le 10/05/2022

[40] https://www.lefigaro.fr/international/la-dmz-coreenne-la-derniere-frontiere-de-la-guerre-froide-20190630?fbclid=IwAR3Rinst1jkY0F2W2r8963l00M3IXJLkymqZCCku0DYit4vf13f22dBeZ4E consulté le 15/05/2022

[41] https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-dmz-in-computer-networking/ consulté le 15/05/2022

[42] https://waytolearnx.com/2019/07/a-quoi-sert-un-service web.html?fbclid=IwAR3n7r5bEltjE6eZMAXJDLCmh10szlHdIt-BeJver_RPHycHY3DRoQMAAxA consulté le 16/05/2022

[43] https://www.hosteur.com/ressources/articles/serveur-de-messagerie?fbclid=IwAR1dYaFRpTn6H1NCt4f3ldpDnOa-Cx_MGV7v-XXblEBX5RaG4lvbdNCA6oY consulté le 15/05/2022

[44] https://www.websiterating.com/web-hosting/glossary/what-is-ftp/?fbclid=IwAR1CWoXUE7YlXi3QVvD8F-0MmguHFfZxU7h5NJ8fa66penek7HO8v3lpqxM consulté le 20/05/2022

[45] https://blog.labvl.net/dhcp/install-dhcp-server/?fbclid=IwAR0iJw58-bBh9n1I6z2N7ri_QZfBdU0EivFjnxu8HijnN38VsE3_eJXz0AU consulté le 20/05/2022

[46] https://www.android-dz.com/ar/how-to-channge-dns/?fbclid=IwAR0iJw58-bBh9n1I6z2N7ri_QZfBdU0EivFjnxu8HijnN38VsE3_eJXz0AU consulté le 22/05/2022

[47] https://www.futura-sciences.com/tech/definitions/internet-proxy-488/?fbclid=IwAR1FajHnV6MI7QMaNbsAg9x-KCq66U8zcCdG3qnvRwauFHL9lXdfa-OZ6SY consulté le 22/05/2022

[48] https://waytolearnx.com/2019/06/qu-est-ce-qu-un-routeur.html?fbclid=IwAR1Di30s9n-nYd1Oji_UIIZcObQC5SMYgivGUFXtK6_qyDM4lXC-PTytMCI consulté le 20/05/2022

[49] https://waytolearnx.com/2018/07/difference-entre-nat-et-pat.html?fbclid=IwAR0xrvpEbbP6tsWxzWLf0LN5-IuWnRXLNVFuKfJ0t5DeQZqTwr9Uqv40yQA consulté le 18/05/2022

[50] https://www.noodo-wifi.com/faq/difference-entre-intranet-et-extranet/