الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire
وزارة التعليم العالي والبحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique
جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA
كلية التكنولوجيا
Faculté de Technologie
قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière : Électronique

Spécialité : Systèmes des télécommunications

Présenté par :

Allal Naziha

&

Ykrelef Madina

Thème

Mise en Place d'une Solution Sécurisée pour un Réseau d'Entreprise

Proposé par : Dr MEHDI Merouan

Encadré par : Mme AIT MESSAOUD Lysa

Année Universitaire 2023-2024

Remerciements

En prélude à ce mémoire, nous remercions ALLAH tout-puissant qui nous aidées et nous a données patience et courage durant ces longues année d'étude.

Nous exprimons notre profonde gratitude à notre enseignant Dr. MEHDI Merouan, pour avoir proposé ce thème, son écoute et sa disponibilité. Sans son expertise, nous n'aurions jamais terminé ce travail.

Nous remercions également notre promotrice Mme. AIT MESSAOUD Lysa, pour son aide et ses conseils.

Nous tenons à remercier également le corps professoral et le personnel administratif du département d'ELECTRONIQUE pour la richesse et la qualité de l'enseignement.

Enfin, nous tenons à exprimer nos sincères remerciements à tous les membres de nos familles et à nos amis qui nous ont toujours encouragées tout au long de la rédaction de ce mémoire.

Merci à toutes et à tous.

Dédicace

Je dédie cet humble et modeste travail grand amour, sincérité et fierté :

A mes chers parents, source de tendresse, de noblesse et d'affectation. Puisse cette étape constituer pour vous un motif de satisfaction.

A mes frères et ma sœur, en témoignage de la fraternité, avec mes souhaits de bonheur, de santé et de succès.

A la femme de mon frère.

A ma chère binôme MADINA, gratitude pour tout ce que nous avons accompli et tout ce qui reste à venir.

Et à tous les membres de ma famille.

A tous mes amis, tous mes professeurs.

Et à tout qui compulse ce modeste travail.

Naziha

Dédicace

Je dédie ce modeste travail :

À mes très chers parents,

AMAR et KHEIRA

Source de vie, d'amour et d'affection.

À mes chers frères (BADRO, MANSOUR, HAMZA et MOHAMMED)

Et leurs femmes et leurs enfants,

Source de joie.

À mes chères sœurs (FATIHA, KHADIDJA, FATOUMA et MERIEM)

Et leurs hommes et leurs enfants,

Source de bonheur.

A mes chères FARAH et NOUSSAIBA,

Source de tendresse.

À ma chère binôme NAZIHA,

Source de dévouement.

À toute ma famille et mes amies, source d'espoir et motivation.

Madina

ملخص

أصبح من الضروري الآن ضمان أمان شبكات الشركات لحماية البيانات من الهجمات الخارجية .ما تم عرضه في هذا العمل يعد جزءًا من تأمين هذا النوع من البنى التحتية، من خلال تقسيم الشبكات المحلية لتجميع وعزل المستخدمين. هذا الأمر ساعد في تحقيق رقابة أفضل على الوصول إلى الخدمات المستضافة خارجيًا. أولاً، تم تنفيذ بروتوكول NAT لتأمين عنوان .IP ومن ثم نشر جدران الحماية، وإنشاء منطقة DMZ والتحكم في تدفقات البيانات الواردة والصادرة. كما تم إنشاء واجهة عامة آمنة باستخدام خدمات وبروتوكولات أمان .وأخيرًا، تم تنفيذ هذه الاستراتيجية الأمنية على برنامج Packet Tracer للتحقق من فعاليتها.

كلمات المفتاح: شبكات الشركات، أمان الشبكات، بروتوكولNAT، Packet Tracer، جدران الحماية (الجدران النارية)، منطقة DMZ

Résumé

Il est devenu essentiel d'assurer la sécurité des réseaux d'entreprise afin de protéger les données contre les attaques extérieures.

Ce qui a été présenté dans ce travail fait partie de la sécurisation de ce type d'infrastructures, en segmentant les réseaux locaux pour regrouper et isoler les utilisateurs. Ce qui a permis un meilleur contrôle de l'accès aux services hébergés en externe. D'abord, une mise en œuvre d'un protocole NAT pour sécuriser l'adresse IP. S'en suit un déploiement de pare-feux, création de DMZ et contrôle des flux entrants et sortants. Aussi, une interface publique sécurisée avec des services et des protocoles de sécurité a été créée.

Enfin, une implémentation sur Packet Tracer a été effectuée, afin de vérifier l'efficacité de la stratégie de sécurité proposée.

Mots clés : réseaux d'entreprises, sécurité des réseaux, NAT Protocol, pare-feu, Packet Tracer, DMZ.

Abstract

It has become essential to ensure the security of company's networks to protect data from external attacks.

What presented in this study is part of securing this type of infrastructure, by segmenting local networks to group and isolate users. This allowed better control of access to externally hosted services. First, a NAT protocol to secure the IP address was implemented. This is followed by the deployment of firewalls, creation of DMZs and control of incoming and outgoing flows. Also, a secure public interface with security services and protocols was created.

Finally, an implementation on Packet Tracer was carried out, in order to verify the effectiveness of the proposed security strategy.

Keywords: company networks, network security, NAT protocol, firewall, Packet Tracer, DMZ.

Table des matières

Liste des figures

Liste des tableaux

Liste des abréviations

ACL:	Access Control Lists.
ASA:	Adaptive Security Appliance
BGP:	Border Gateway Protocol.
CFI:	Common Format Identifier.
CISCO:	Computer Information System Company
COS:	Class of Service.
DHCP:	Dynamic Host Configuration Protocol.
DMZ :	La Zone Démilitarisée.
DNS :	Domain Name System.
DOD:	Department Of Defense.
DOS:	Disk Operating System.
FAI :	Fournisseur Access Internet.
FTP :	File Transfert Protocol.
HTTP:	HyperText Transfert Protocol.
IANA:	Internet Assigned Numbers Agency.
ICANN:	Internet Corporation for Assigned Names and Numbers
ICMP:	Internet Control Message Protocol.
IEEE:	Institute of Electrical and Electronics Engineers.
IOT:	Internet of Things
IPv4:	Internet Protocol version 4
IPv6:	Internet Protocol version 6
ISP:	Internet Service Provider.
ISR:	Integrated Services Routers

MAC:	Media Access Control.
NAT:	Network Address Translation.
OSPF:	Open Shortest Path First.
OSI	Open Systems Interconnection
RIF :	Rule Interchange Format.
RIP :	Routing Information Protocol.
SGBD :	Système de Gestion de Base de Données.
SMTP :	Simple Mail Transfer Protocol
TCI :	Information de contrôle du tag
TCP/IP:	Transmission Control Protocol / Internet Protocol.
UDP:	User Datagram Protocol.
UTP:	Unshielded Twisted Pair
VLAN:	Virtual Local Area Network.

Introduction générale

Introduction générale

Les réseaux informatiques consistent en des appareils informatiques interconnectés qui peuvent échanger des données et partager des ressources entre eux

Particulièrement, par ‘’réseau d'entreprise’’ on désigne l'infrastructure informatique que les moyennes et grandes organisations utilisent pour fournir une connectivité entre les utilisateurs, les appareils et les applications. L’objectif étant de rallier efficacité et fiabilité dans services numériques offerts aux travailleurs, aux partenaires, aux clients et, de plus en plus, aux objets.

Les réseaux d’entreprise, qui peuvent se trouver sur plusieurs sites, sont déployés avec des connexions généralement ouvertes. Ce qui les met en danger, tant au niveau interne qu’externe.

De plus en plus souvent, les entreprises sont confrontées à de nouvelles formes d’attaques et de menaces, ce qui nécessite que leurs réseaux mettent en place tous les dispositifs de sécurité pour se protéger.

Ainsi, notre intérêt se porte sur la création et la mise en place d’une infrastructure d’un réseau d’entreprise qui inclut la sécurité, la surveillance et les pares-feux pour se protéger contre les attaques et les menaces.

La première ligne de défense pour mettre en œuvre la sécurité est la protection physique du réseau. La pratique actuelle montre que la sécurité du réseau commence par la sécurisation de la base de données et de la topologie. Les réseaux d’entreprise sont souvent caractérisés par une infrastructure hétérogène et un grand nombre d’appareils répartis sur plusieurs sites à connecter à un réseau commun sécurisé.

L’objectif principal de ce travail est d’établir le réseau d’entreprise dans des endroits éloignés, de fournir un accès à l’infrastructure en même temps de garantir la sécurité des connexions réseau. Nous avons introduit une technique de réseau local (ou VLAN : Virtual Local Area Network) pour séparer les groupes d’accès et isoler les utilisateurs tout en les gérant efficacement.

Ce travail se concentre sur gestion des VLAN, et l’utilisation des protocoles de sécurité tel que le NAT modifier la sécurité des ports, et fournir un accès à distance plus sécurisé aux administrateurs.

Pour mieux contrôler l'accès aux services extérieurs, nous avons installé un pare-feu dans les unités de distribution et de base dans les zones désignées, et mis en œuvre la zone militaire (DMZ).

Nous avons également mis en place des solutions pour les équipements (pare-feu, routeurs et serveurs) et les réseaux (canal Ethernet) pour assurer une tolérance aux pannes. Pour simuler tout cela, nous avons implémenté notre architecture sur Packet Tracer, testé ses fonctionnalités et la mise en œuvre les services.

Ce document est organisé en trois chapitres :

Le premier chapitre, intitulé "Généralités sur les réseaux d'entreprises", présente les concepts fondamentaux ainsi que les technologies de base (équipements, topologies …) des réseaux informatiques.

Le second chapitre examine les architectures et les stratégies et techniques de sécurisation.

L'architecture sécurisée effectuée est exposée dans le troisième chapitre, d'abord par la conception de l'architecture de sécurité, puis l'implémentation sur Packet Tracer de toutes les fonctionnalités de sécurité imposée par le cahier de charge.

Finalement, ce présent mémoire se termine par une conclusion générale.

Chapitre I *Généralités sur les réseaux*

I.1. Introduction

Aujourd'hui et sûrement moins que demain, il y'a un besoin accru de communication entre êtres humains, mais aussi entre différents dispositifs : ordinateurs, machines…

Que ce soit pour socialiser ou pour collaborer afin de réaliser des tâches, cet échange d'informations nécessite un système de communication dit réseau informatique.

Qu'il soit domestique ou d'entreprise (industrie, services, administration …), le réseau permet le partage de ressources humaines et/ou matérielles (calculateurs, logiciels, bases de données, …). Sans oublier l'accès à internet (le réseau des réseaux), et les dispositifs IoT (Internet of Things : Internet des Objets) qui se connectent et échangent des données avec d'autres appareils et systèmes sur Internet.

La mise en réseau permet d'allier fiabilité notamment en sécurisant les données échangées, et efficacité en assurant un partage des ressources couteuses et éloignées géographiquement.

Ce chapitre introductif décrit les concepts de base et les généralités relatifs aux réseaux, leurs objectifs, leur classification et bien d'autres notions…

I.2. Définition d'un réseau informatique

Un réseau informatique est un ensemble de composants matériels ou logiciels reliés entre eux grâce à des lignes de communication (câbles réseaux, liaisons sans fils, etc.) dans le but de permettre aux utilisateurs de partager des ressources et d'échanger des informations sous forme de données numériques [2].

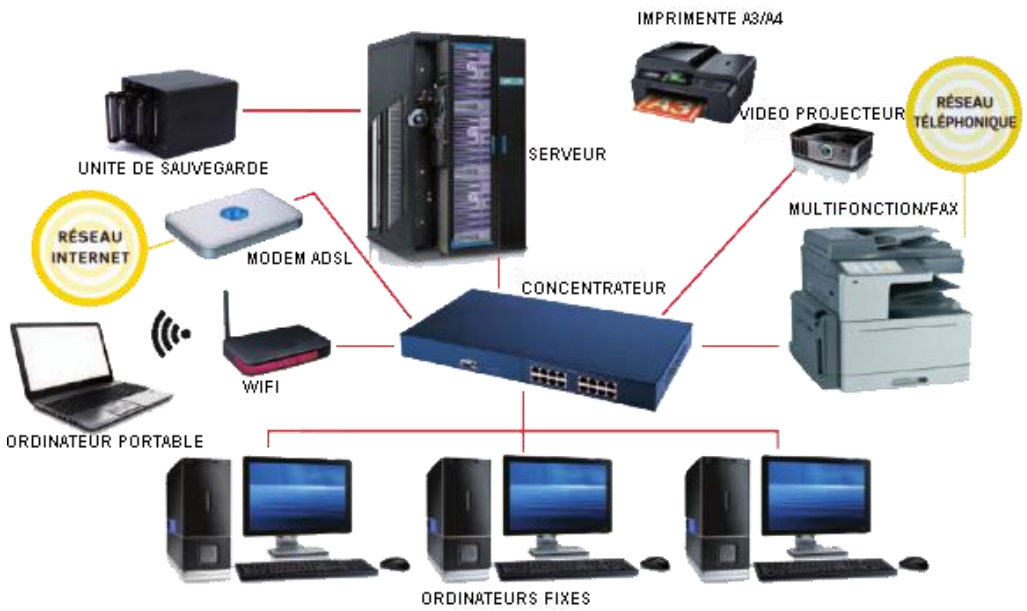

Figure I.1 : Exemple d'un réseau informatique

I.3. Classification des réseaux informatiques

On distingue généralement quatre catégories de réseaux informatiques, différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- **Les réseaux domestiques ou PAN (*Personal Area Network*)** Ils relient des appareils électroniques personnels (ordinateurs portables et imprimantes sans fil, smartphones et oreillettes Bluetooth®, tablettes et enceintes sans fil...) [3].
- **Les réseaux locaux ou LAN (*Local Area Network*)** Peuvent s'étendre de quelques mètres à quelques kilomètres. Ce sont des réseaux locaux au sein d'une maison, d'une entreprise, d'un établissement scolaire. . . Ils permettent l'échange de données informatiques ou le partage de ressources (Ethernet, *token ring*...). Ils connaissent une utilisation importante dans le cadre des jeux vidéo en réseau avec les *LAN gaming*. [3]
- **Les réseaux métropolitains ou MAN (*Metropolitan Area Network*)** c'est des réseaux qui s'étendent à une zone métropolitaine telle qu'une ville. Ces réseaux permettent par exemple de relier plusieurs bâtiments d'une commune ou d'un pôle universitaire. Ce sont des interconnexions de plusieurs sites (ou *LAN*) à l'échelle d'une ville [3].
- **Les réseaux longs distances ou WAN (*Wide Area Network*)** permettent de communiquer à l'échelle d'un pays, ou de la planète entière. Le plus connu de ces réseaux est Internet. Le support de transmission peut être terrestre (réseau maillé de type téléphonique ou ligne spécialisée) ou hertzien (transmission par satellite). L'ADSL est un exemple de type de réseaux.

Dans une grande entreprise, un réseau est généralement une combinaison plus ou moins complexe de LAN et de WAN. Il est possible « d'émuler » un réseau LAN à travers un WAN en utilisant un VPN (*Virtual Private Network*) [3].

La figure suivante illustre sommairement ces grandes catégories de réseaux :

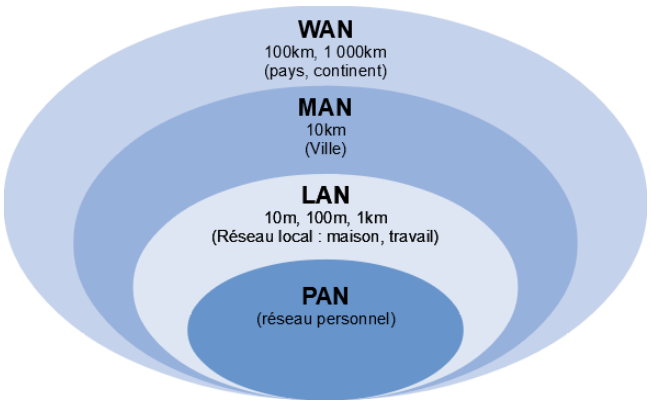

Figure I.2 : Les grandes catégories de réseaux

I.4. Modèles de communication réseau

La communication réseau nécessite l'existence d'un émetteur, d'un récepteur, d'un support de transmission et d'un langage compréhensible par tous ces protagonistes, indépendamment du matériel mis en œuvre dans la communication. Les modèles OSI et TCP/IP sont des modèles de référence imposant des normes à respecter lors de toute communication réseau.

I.4.1. Le modèle OSI

Le modèle OSI (Open Systems Interconnection) a été établi par l'ISO (International Standards Organization). Ce modèle est une norme qui recommande la manière dont les ordinateurs doivent communiquer entre eux. Le modèle OSI est un modèle à 7 couches, et chaque couche ne peut communiquer qu'avec les couches adjacentes.

Les différentes couches du modèle OSI sont définies dans la figure suivante :

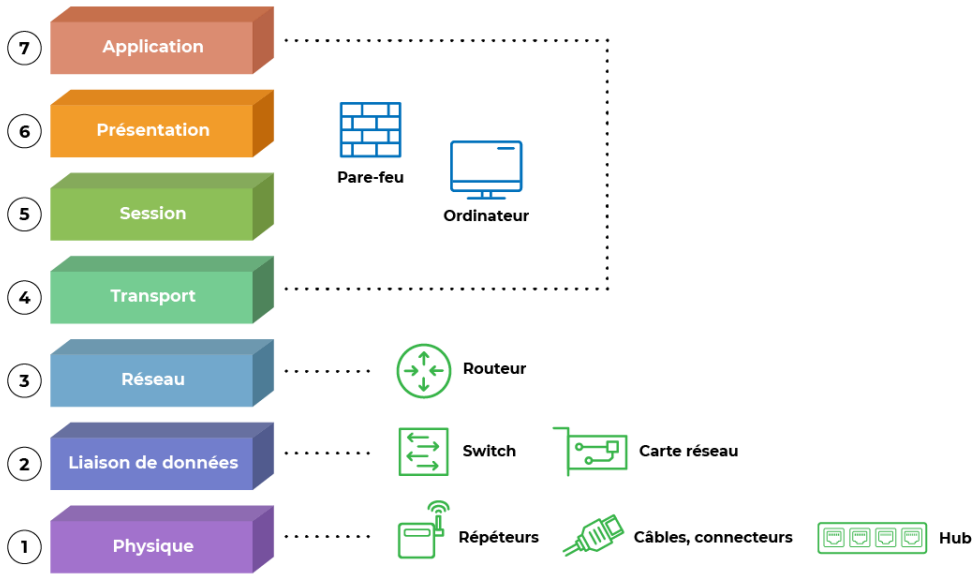

Figure I.3 : Les couches du modèle OSI

Le modèle OSI est donc arrangé en couches superposée explicitées comme suit :

- **La couche physique** Permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau. L'unité de données s'appelle le paquet.
- **La couche liaison de données** Cette couche permet le transfert de l'information sous forme de trames, détection et correction d'erreurs et le partage du média de transmission. L'unité de donnée à ce niveau est la trame.

- **La couche réseau** Permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau. L'unité de données s'appelle le paquet.

- **La couche transport** Assure le transport de données entre les entités de session, la procédure de connexion et déconnexion et le contrôle de flux. L'unité de donnée à ce niveau est le message.
- **La couche session** Assure l'ouverture et la fermeture de sessions de communication entre les machines du réseau.
- **La couche présentation** Cette couche met en forme les informations échangées pour les rendre compatibles avec l'application destinataire (traduction des formats, compression, encryptage, etc.). Elle s'intéresse à la syntaxe des informations.
- **La couche application** C'est la couche OSI la plus près de l'utilisateur, elle fournit des services réseau aux applications de l'utilisateur (exemple : navigateur).

I.4.2. Le modèle TCP/IP

Dans les années 70, le département de la défense américain DOD (Department Of Defense) décide devant le foisonnement de machines utilisant des protocoles de communication différents et incompatibles, de définir sa propre architecture. Cette architecture, dite TCP/IP (Transmission Control Protocol/Internet Protocol), est à la source du réseau Internet [4].

Le modèle TCP/IP est un modèle qui comporte 4 couches :

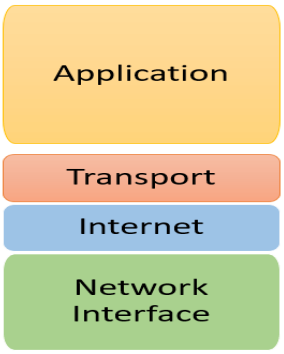

Figure I.4 : Les couches du modèle TCP/IP

I.5. Différence entre le modèle TCP / IP et le modèle OSI

TCP / IP et OSI sont les deux modèles de réseaux les plus utilisés pour la communication. Il y a quelques différences entre les deux. L'une des différences majeures est que l'OSI est un modèle

conceptuel qui n'est pratiquement pas utilisé pour la communication, tandis que TCP / IP est utilisé en pratique.

Tableau I.1 : Comparaison entre le modèle OSI et TCP/IP

	Modéle TCP/IP	Modèle OSI
Signification	Transmission Control Protocol/ Internet Protocol.	Open system interconnect
Définition	C'est un modèle serveur/client utilisé pour la transmission de données sur internet.	C'est un modèle théorique qui utilisé pour le système informatique
Nombre de couches	4 Couches	7 couches
Développé par	Département de la Défense (DoD)	ISO (Organisation Internationale de Normalisation)
Usage	Principalement utilisé	Jamais utilisé

La Figure I.5 illustre l'équivalence entre les sept (07) couches du modèle OSI et le quatre (04) couches du modèle TCP/IP :

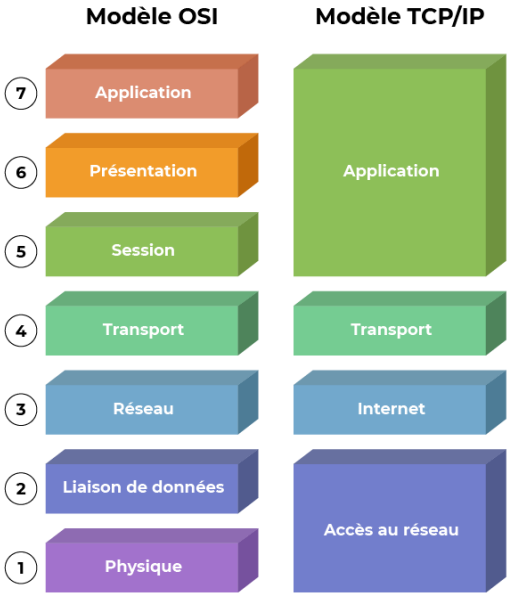

Figure I.5 : Les couches du modèle OSI et TCP/IP

Il faut mentionner également que :

- TCP / IP est un modèle client-serveur, c'est-à-dire lorsque le client demande un service, il est fourni par le serveur. Tandis que le modèle OSI est un modèle conceptuel.

- TCP / IP est un protocole standard utilisé pour tous les réseaux, y compris Internet, tandis que OSI n'est pas un protocole mais un modèle de référence utilisé pour comprendre et concevoir l'architecture du système.
- TCP / IP suit l'approche verticale, alors que le modèle OSI prend en charge l'approche horizontale.
- TCP / IP suit une approche de haut en bas, tandis que le modèle OSI suit une approche ascendante.

TCP / IP est utilisé pour la connexion de bout en bout afin de transmettre les données sur Internet. TCP / IP est robuste, flexible, réel et suggère également comment les données doivent être envoyées sur le Web. La couche de transport du modèle TCP / IP vérifie si les données sont arrivées dans l'ordre, s'il y a une erreur ou non, si les paquets perdus sont envoyés ou non, si l'accusé de réception est reçu ou non, etc.

I.6. Les protocoles utilisés par le modèle TCP/IP

Un protocole est un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Sur internet, les protocoles utilisés font partie d'une suite de protocoles, c'est- à-dire un ensemble de protocoles qui fonctionnent ensemble. La suite de protocole TCP/ IP, contient entre autres les protocoles suivants :

I.6.1. Le protocole IP

Sur internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol) décrit dans la RFC 791, ce dernier utilise des adresses numériques, appelées adresses IP. C'est l'ICANN (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, Internet Assigned Numbers Agency, de- puis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public Internet. Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur le réseau.

a. L'adressage IPV4

Une adresse IPV4 est une adresse 32 bits, arrangée sous forme de quatre (04) octets. Chacun des octets peut être représenté par un nombre de 0 à 255, ce format est appelé la notation décimale pointée. L'adresse est constituée de deux parties :

- Un identificateur de réseau (NET-ID): tous les systèmes du même réseau physique doivent posséder le même identificateur de réseau, lequel doit être unique sur l'ensemble des réseaux gérés.

- Un identificateur d'hôte (HOST-ID) : un nœud sur un réseau TCP/IP est appelé hôte, il identifie une station de travail, un serveur, un routeur ou tout autre périphérique TCP/IP au sein du réseau.

La concaténation de ces deux champs constitue une adresse IP unique sur le réseau. La séparation entre l'identificateur du réseau et celui de la machine se fait avec le masque de sous réseau.

b. Classes d'adresses IPV4

A été défini trois classes d'adresses selon la taille du réseau en question :

- Classe A : les réseaux de grande taille.
- Classe B : les réseaux de taille moyenne.
- Classe C : les réseaux de petite taille.

Tableau I.2 : Comparaison entre le modèle OSI et TCP/IP

Classe	Début en binaire	Valeur	Identificateur de réseau	Identificateur d'hôte
A	0…	1 à 126	a	b, c, d
B	10…	128 à 191	a, b	c, d
C	110…	192 à 223	a, b, c	d
D	1110…	224 à 239	Multicast	a, b, c, d
E	11110…	240 à 255	Réservées	Expérimental

La taille du réseau est exprimée en nombre d'hôtes potentiellement connectés. Le premier octet d'une adresse IP permet de déterminer la classe de cette adresse. Les adresses disponibles (de 0.0.0.0 à 255.255.255.255) ont donc été découpées en plages réservées à plusieurs catégories de réseaux.

c. L'adressage IPv6

Une adresse IPv6 est longue de 128 bits et se compose de huit champs de 16 bits, chacun étant délimité par deux points (:). Chaque champ doit contenir un nombre hexadécimal, à la différence de la notation en format décimal avec points des adresses IPv4 [5].

Il existe trois types d'adresse IPv6 :

- Unicast : Utilisé pour les connexions point à point.
- Multicast : Identifie un groupe d'interfaces.
- Anycast : Adresses virtuelles pointant vers une ou plusieurs adresses physiques.

d. Masque de sous-réseau

On appelle masque de sous-réseau (subnet mask), la séparation entre l'identificateur du réseau et celui de la machine dans une adresse IP. Le masque est précisé en binaire par des 1 pour la partie réseau et des 0 pour la partie ordinatrice.

Tableau I.3 : Le masques de sous-réseau

Lasse	Masque en Décimal	Masque en binaire
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

e. Les adresses "privées"

Les adresses suivantes peuvent également être librement utilisées pour monter un réseau privé :

- A : 10.0.0.0 10.255.255.255 255.0.0.0
- B : 172.16.0.0 à 172.31.255.255 255.240.0.0
- C : 192.168.0.0 à 192.168.255.255 255.255.0.0

Le protocole IPV4 permet d'utiliser un peu plus de quatre milliards d'adresses différentes pour connecter les ordinateurs et les autres appareils reliés au réseau. Du temps des débuts d'internet, cela paraissait plus que suffisant, il était pratiquement impossible d'imaginer qu'il y aurait un jour suffisamment de machines sur un unique réseau pour que l'on commence à manquer d'adresses disponibles [4]. Cette limite conduit à la transition d'IPV4 vers l'IPV6, actuellement en cours de déploiement, qui devrait progressivement le remplacer.

I.6.2. Le protocole TCP

Le protocole TCP (Transmission Control Protocol) décrit dans la RFC 793 est l'un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle. Lorsque les données sont fournies au protocole IP celui-ci les encapsule dans des datagrammes IP. TCP est un protocole fiable créant une connexion bidirectionnelle entre 2 ordinateurs. L'expéditeur s'attend à une confirmation du destinataire sur réception.

I.6.3. Le protocole FTP

Le protocole FTP (File Transfert Protocol) est un protocole de transfert de fichiers, il a été développé dans le cadre d'internet pour garantir une qualité de service, c'est-à-dire le fichier arrive correctement et en entier au récepteur. L'application FTP est de type client-serveur avec un

Client FTP et un serveur FTP. Le logiciel propose un mode avec connexion, de telle sorte que l'émetteur et le récepteur se mettent d'accord sur les caractéristiques de la transmission.

I.6.4. Le protocole SMTP

Le courrier électronique au sein d'internet est géré par le protocole SMTP bâtis sur TCP. Il permet l'échange de message entre un émetteur et un ou plusieurs récepteurs pourvus que leurs adresses soient connues.

I.6.5. Le protocole HTTP

Le protocole HTTP (Hyper Text Transfert Protocol) décrit dans la RFC 2616, est le protocole définit pour le web, c'est un protocole de gestion du transfert de fichier hypertexte entre serveur et client Web.

I.6.6. Le protocole ICMP

Le protocole ICMP (Internet Control Message Protocol) est un protocole de notification d'erreurs (réseau coupé, échéances temporelles) permettant d'informer l'expéditeur en cas d'anomalies de fonctionnement.

I.6.7 Les adresses MAC

L'adresse physique encore appelée adresse MAC (Media Access Control) est un identifiant physique stocké dans une carte réseau ou une interface réseau similaire et utilisée pour attribuer mondialement une adresse unique au niveau de la couche 2 du modèle OSI.

Une adresse MAC est constituée de 48 bits (6 octets) et est généralement représentée sous la forme hexadécimale en séparant les octets par un double point ou un tiret.

Par exemple 5E:FF:56:A2:AF:15.

I.7 Équipement d'interconnexion

Un réseau est constitué d'ordinateurs (ou tout autre dispositif apte à communiquer) reliés par un ensemble d'éléments matériels et logiciels. Les éléments matériels permettant d'interconnecter les ordinateurs sont les suivants :

I.7.1 La carte réseau

La carte réseau (coupleur) est une carte connectée sur la carte mère de l'ordinateur ou partie intégrante de la carte mère qui relie à l'aide d'un câble ou d'ondes radios un ordinateur au reste du réseau.

I.7.2 Les répéteurs

Un répéteur est un dispositif qui augmente la portée du signal sur la ligne de transmission en transmettant un nouveau signal à partir du signal reçu. Le but de cette fonctionnalité est d'augmenter la taille du réseau. La réplication ne fonctionne qu'au niveau de la couche physique (couche 1 du modèle OSI), ce qui signifie qu'elle ne fonctionne que sur les deux couches de données de la ligne de transmission et ne peut pas « interpréter » les données. L'avantage de ces outils est qu'ils ne nécessitent aucune (ou très peu) administration. En revanche, il ne réduit pas la charge du réseau, ne filtre pas les collisions, n'augmente pas la bande passante et ne peut pas fournir un véritable réseau.

I.7.3 Le pont

Un pont est un périphérique matériel utilisé pour connecter des réseaux entre eux en utilisant le même protocole. Ainsi, contrairement au répéteur, qui fonctionne au niveau physique, le pont fonctionne également au niveau logique (couche 2 du modèle OSI), ce qui signifie qu'il peut filtrer les trames autorisant uniquement les trames dont l'adresse correspond à une machine à côté du pont. Le filtre est aussi appelé répéteur ou pont. Ils envoient trames de données en fonction de l'adresse MAC, lisent l'adresse MAC et envoient les informations des paquets reçus aux ports d'entrée pour découvrir les appareils de chaque segment. L'adresse MAC est ensuite utilisée pour créer une table de commutation qui permet aux nœuds de bloquer les paquets qui n'ont pas besoin d'être envoyés vers la zone locale.

I.7.4 Le Switch (commutateur)

Les switches rassemblent les meilleures fonctionnalités des hubs et des ponts dans un seul dispositif intelligent. Un switch réseau connecte les appareils d'un réseau les uns aux autres, leur permettant de communiquer en échangeant des paquets de données. Ces dispositifs peuvent être des périphériques matériels qui gèrent des réseaux physiques ou des périphériques virtuels logiciels.

Un switch réseau fonctionne sur la couche liaison de données, ou couche 2, du modèle OSI. Dans un réseau local (LAN) utilisant Ethernet, il détermine où envoyer chaque trame de message entrant en examinant l'adresse MAC du récepteur contenue dans la trame et ouvre un seul circuit virtuel entre les nœuds émetteur et récepteur, ce qui restreindra la communication entre ces deux ports concernés, mais n’affectera pas le trafic en provenance d’autres ports.

I.7.5 Le hub (concentrateur)

Un hub est un appareil utilisé pour connecter le trafic et mettre à jour les signaux de plusieurs hôtes. C'est un répéteur qui transmet des signaux via un seul port de sortie. Lorsqu'il reçoit un signal d'un port, il le retransmet à tous les autres ports. Le routeur, comme le répéteur, fonctionne au niveau 1 du modèle OSI, il est donc également appelé répéteur, est utilisé du côté du réseau et doit être connecté à un maximum de 4 points entre deux postes de travail. Cela présente des inconvénients tels que la répétition.

I.7.6 Les routeurs

Le routeur est un élément matériel qui connecte les réseaux et permet de relier des paquets entre deux ou plusieurs réseaux afin de déterminer leurs directions. Un routeur dispos de plusieurs

canaux, chacun est connecté à un réseau différent. Il y a donc plusieurs adresses IP car différents réseaux sont connectés. Cette fonctionnalité est utile car elle permet de choisir un itinéraire alternatif dans le cas d'échec d'une connexion ou d'un routeur sur une route bloquée par des paquets.

I.7.7 Un Gateway (Passerelle)

Une passerelle est un nœud de réseau qui connecte deux réseaux utilisant des protocoles différents. Il fait également office de porte d'entrée entre deux réseaux. Il peut s'agir d'un routeur, d'un pare-feu, d'un serveur ou d'un autre périphérique permettant au trafic d'entrer et de sortir du réseau. Une passerelle est aussi appelée convertisseur de protocole.

I.7.8 Un firewall

Le firewall (pare-feu) est un mur sécurisé entre les réseaux privé et publique qui protège le réseau interne de l'extérieur.

Fondamentalement, le pare-feu peut être configuré de telle manière que le réseau public ne puisse pas accéder au réseau privé et/ou que le réseau privé ne puisse pas accéder à certaines ressources du réseau public. Le pare-feu est essentiellement placé dans le Gateway.

Le pare-feu protège le réseau interne par trois outils différents :

- Dissimulation de l'adresse IP.
- Filtrage des ports.
- Filtrage de paquets.

I.7.9 Les équipements physiques

Un réseau informatique est typiquement représenté sous forme de **nœuds** reliés par des **arcs**, voir Figure I.6

Un **arc** représente tout support d'interconnexion : câble réseau, Wifi, fibre optique, …

Un **nœud** représente tout :

- Equipement de communication : PC, Smartphone, capteur, puce, …
- Equipement d'interconnections : répéteur, Hub, Switch, routeur, point d'accès Wifi, ….

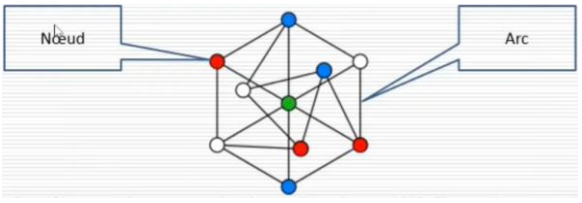

Figure I.6 : Représentation d'un réseau informatique

Pour que les équipements du réseau puissent communiquer entre eux, il faut qu'ils soient reliés par un moyen de transport de l'information. Ce moyen est dit support de transmission ou support d'interconnexion, ce dernier est souvent un simple câble réseau, composé d'un fil de cuivre ou de fibre optique. La transmission peut être aussi sans fils, avec des technologies à base d'infrarouges, d'ondes radio ou de micro-ondes. On pourrait notamment citer le WIFI, le Bluetooth, …

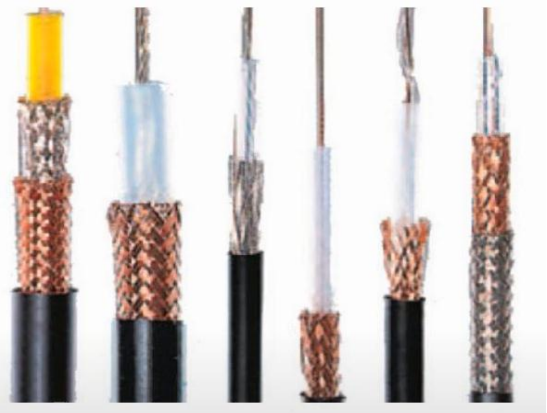

Figure I.7: Exemples de câbles coaxiaux

- **Le câble coaxial**

Les câbles coaxiaux sont composés d'un fil conducteur, entouré d'un isolant, lui-même entouré d'une couche de conducteurs (le blindage), le tout étant enroulé d'une protection isolante.

Les câbles coaxiaux sont identifiés par deux lettres RG suivies d'un nombre, ceux utilisés pour les applications de mises en réseaux sont les RG-8, RG-62 et RG-58, ils sont différenciés notamment par l'impédance, la taille le connecteur et l'utilisation.

Un autre moyen d'identifier les câbles coaxiaux est d'utiliser un code : 10BASE2 (RG-58) ou 10BASE5 (RG-8). Développé par le comité IEEE 802.3 ce code 10BASE5(2) est dérivé de plusieurs caractéristiques du support physique. Le 10 fait référence à sa vitesse de transmission qui est de 10 Mbits/s, BASE est l'abréviation de signalisation digitale en bande de base, et le 5 représente la longueur maximale du segment de 500 mètres, pareillement le 2 dans 10BASE2 fait référence à une longueur de câble de 200 mètres.

Il convient de noter que le 10BASE5 a été remplacé par des alternatives beaucoup moins coûteuses et plus pratiques, notamment le 10BASE2 basé sur un câble coaxial plus fin. En

général les câbles coaxiaux ont tendance à être remplacés par les câbles Ethernet à paire torsadée.

- **Le câble à paires torsadées**

Le câblage à paire torsadée est un type de câble de communication dans lequel deux conducteurs d'un même circuit sont torsadés ensemble dans le but d'améliorer la compatibilité électromagnétique.

Les câbles à paires torsadées les plus courants sont les câbles UTP : Unshielded Twisted Pair, Paire torsadée non blindée. Les câbles UTP modernes contiennent quatre (04) paires de fils en cuivre, chaque paire forme un circuit électrique.

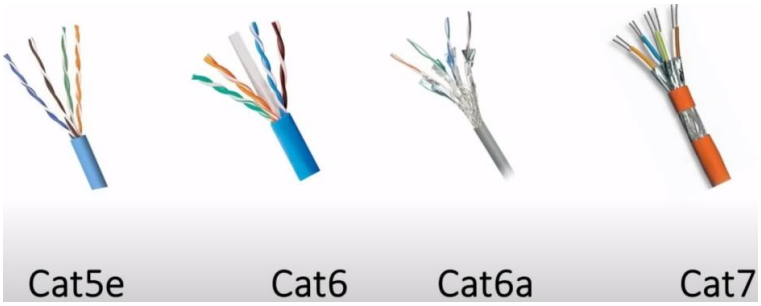

Figure I.8: Différentes catégories de câbles UTP

La figure I.8 illustre les différentes catégories des câbles UTP, le préfixe Cat signifie catégorie, cette dernière définie entre autres le nombre de paires torsadées, l'épaisseur du fil, la vitesse et la distance de transmission…

A titre d'exemples, un câble Cat5 permet une transmission de 100Mbits/s, pour une transmission de l'ordre de 1Gbits/s un Cat5e est nécessaire. Un câble Cat6 permet un débit de10Gbits/s mais sur une distance maximale de 55m, ce même débit peut être obtenu sur une distance de 100m avec un câble Cat6a.

Le câble UTP a un connecteur à chacune des deux extrémités, appelé connecteur RJ45 (Figure I.9), c'est la partie que à connecter à la carte réseau ou au port du Switch.

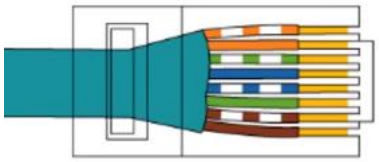

Figure I.9: Le connecteur RJ45

Ce connecteur possède huit broches qui s'alignent avec les huit fils à l'intérieur du câble UTP, l'alignement doit se faire correctement d'où le code couleur des fils (voir la Figure I.9).

La figure I.9 montre la connexion d'un câble UTP de type 1000BASE-T, TX et RX symbolisent La figure I.8 illustre les différentes catégories des câbles UTP, le préfixe Cat signifie catégorie, cette dernière définie entre autres le nombre de paires torsadées, l'épaisseur du fil, la vitesse et la distance de transmission…

A titre d'exemples, un câble Cat5 permet une transmission de 100Mbits/s, pour une transmission de l'ordre de 1Gbits/s un Cat5e est nécessaire. Un câble Cat6 permet un débit de10Gbits/s mais sur une distance maximale de 55m, ce même débit peut être obtenu sur une distance de 100m avec un câble Cat6a.

Le câble UTP a un connecteur à chacune des deux extrémités, appelé connecteur RJ45 (Figure I.9), c'est la partie que à connecter à la carte réseau ou au port du Switch.

Ce connecteur possède huit broches qui s'alignent avec les huit fils à l'intérieur du câble UTP, l'alignement doit se faire correctement d'où le code couleur des fils.

- La gaine de protection de la fibre.
- La fibre de renfort en Kevlar.
- Le revêtement protège mécaniquement la fibre.
- La gaine aide à la propagation du signal.
- Le cœur sert à confiner le signal lumineux et à le propager.

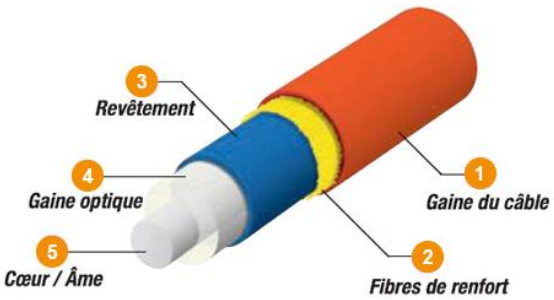

Figure I.10: Composition d'une fibre

Il existe principalement deux types de fibre optique :

La fibre MULTIMODE

La fibre multimode a un cœur de grand diamètre. Elle permet le passage de plusieurs longueurs d'ondes lumineuses, elle est utilisée sur de courtes distances.

La fibre MONOMODE

La fibre monomode n'autorise qu'un seul mode de propagation. La longueur d'onde traverse le centre de la fibre et la lumière est réalignée vers le centre au lieu de rebondir sur son bord comme la fibre multimode. Cette fibre est utilisée pour des longues distances.

Les câbles à fibre optique, utilisés dans les réseaux de communication, sont disponibles dans une variété de diamètres. La Figure I.12 illustre la norme pour le diamètre de la fibre, il s'agit d'expliciter le diamètre du cœur et celui de la gaine optique.

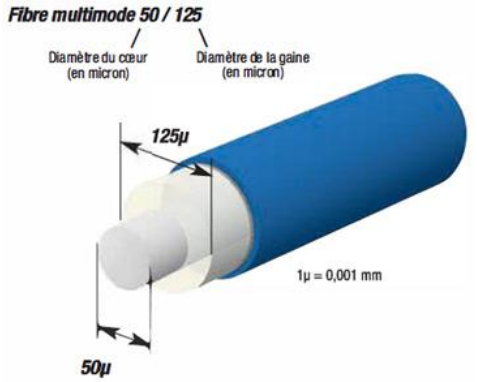

Figure I.11 : Norme pour le diamètre de la fibre

Enfin le Tableau I.4 résume les différents types de câble à fibres optique selon leurs caractéristiques principales, diamètres et utilisations.

Tableau I.4: Norme pour le diamètre de la fibre

Type de fibre	OS1/OS2	OM1	OM2	OM3	OM4
Type de fibre	Monomode	Multimode	Multimode	Multimode	Multimode
Domaine d'application principal	Liaisons bâtiments	Déport vidéosurveillance et réseau	Déport vidéosurveillance et réseau	Déport Gigabit & Datacenter	Datacenter
Débit courant	Illimité	100 Mb/s	100 Mb/s & 1 Gb/s	10 Gb/s	10 Gb/s & 40 Gb/s
Diamètre de la fibre	9/125µ	62,5/125µ	50/125µ	50/125µ	50/125µ
Déport*	Très longue distance > 5 km	Longue distance > 5 km	Longue distance > 550 m	Moyenne distance réseau < 300 m	Moyenne distance réseau < 150 m
Bande passante	Illimité	200 MHz.km (850 nm)	500 MHz.km	1500 MHz.km(850 nm)	3500 MHz.km(850 nm)

Quant à la Figure I.13, elle énumère Les différents connecteurs utilisés pour les câbles en fibre optique.

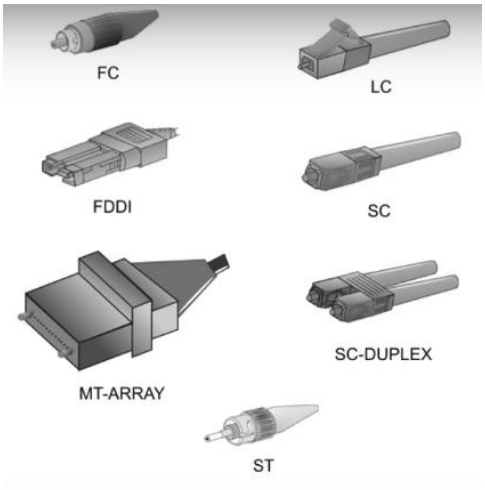

Figure I.12 : Les différents connecteurs utilisés pour les câbles en fibre optique

I.8 Les topologies physiques

La topologie d'un réseau est son arrangement géométrique. Il existe de nombreuses topologies pratiques : topologie en bus, topologie en étoile, topologie en anneau et topologie maillée.

I.8.1 Topologie en bus

Une topologie en bus relie tous les périphériques réseau à une seule ligne qui s'étend d'un bout à l'autre de la ligne. Elle est également appelée topologie de base. Le flux de données dans le système se déplace dans une direction, en suivant le chemin du câble [6].

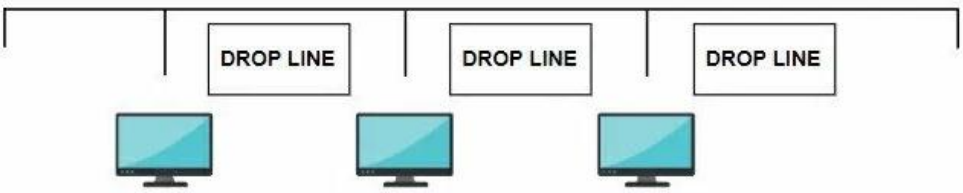

Figure I.13: Topologie en BUS

I.8.2 Topologie en étoile

La topologie la plus populaire est la topologie en étoile, conçue pour connecter chaque appareil du réseau à un point unique avec un câble. Ce nœud central contrôle le transfert de données. Les données de chaque connexion sur le réseau doivent passer par cette connexion pour atteindre leur destination [7].

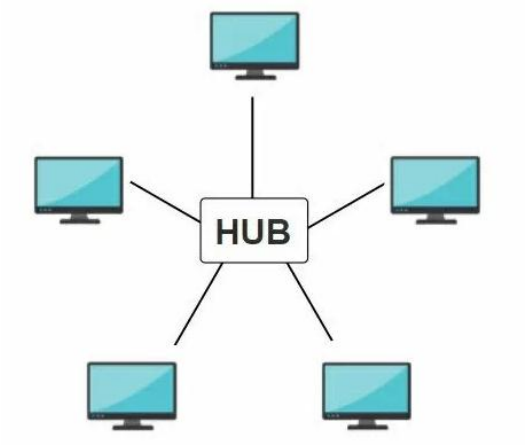

Figure I.14: Topologie en étoile

I.8.3 Topologie en anneau

La topologie en anneau est la disposition des nœuds du réseau en cercle. Les données peuvent se déplacer dans un sens ou dans les deux sens [7].

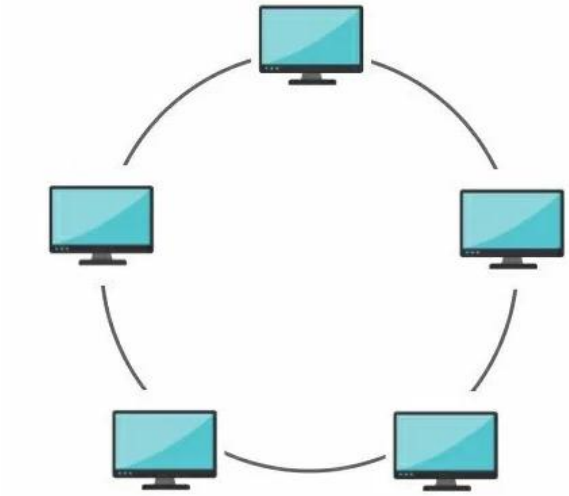

Figure I.15: Topologie en anneau

I.8.4 Topologie en maille

Dans une topologie maillée, chaque ordinateur est connecté à chacun des autres ordinateurs par un câble séparé. Cette configuration fournit des itinéraires de routage redondants sur le réseau pour qu'en cas de défaillance d'un câble, un autre prenne le trafic en charge et que le réseau continu à fonctionner [8].

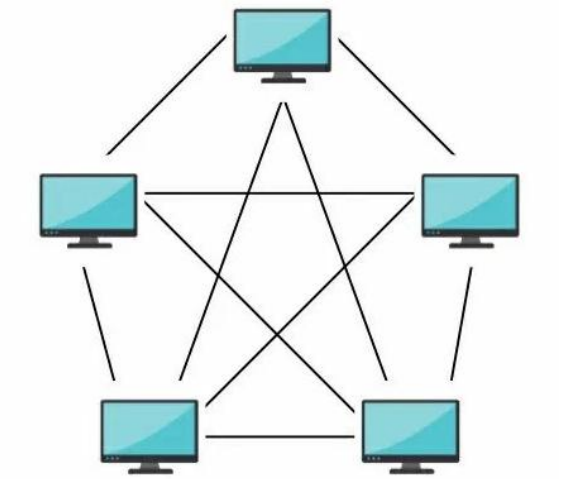

Figure I.16: Topologie en Maille

I.9 Architecture réseau

Une architecture réseau est un ensemble fonctionnel qui comprend des équipements de transmission, des logiciels et des protocoles de communication, ainsi qu'une infrastructure filaire ou radioélectrique qui permet la transmission des données entre les différents éléments.

Le serveur: est un processus accomplissant une opération sur demande d'un client en lui transmettant la réponse. Le serveur est fournisseur de services aux clients qui sont des consommateurs.

Le client: est un processus qui demande l'exécution d'une tâche a un processus serveur par l'envoie d'un requête contenant le descriptif de l'opération à exécuter.

La requête: désigne le message envoyé du client au serveur décrivant l'opération à exécuter.

La réponse: désigne le message transmis par le serveur à un client suite à l'exécution d'une opération contenant le résultat de l'opération.

Le service : c'est le travail fourni par le serveur suite à la requête du client.

I.9.1 L'architecture Client/serveur

L'architecture client/serveur désigne un mode de communication entre un client et un serveur où le client est un processus qui demande l'exécution d'un service au serveur, qui accompli ces services, et envoie en retour des réponses. Ces services sont des programmes fournissant des données.

Un système client/serveur fonctionne selon le schéma suivant :

- Le client émet une requête vers le serveur duquel il demande un service.
- Le serveur reçoit la demande, la traite et renvoie la réponse au client.

La figure suivante illustre ce fonctionnement **:**

Figure I.17: Communication Client/serveur

On note les différentes architectures Client/serveur suivantes :

- **L'architecture client/serveur à 2-tiers**

Cette architecture caractérise les systèmes clients/serveurs pour lesquels le client demande une ressource et le serveur la lui fournit directement, en utilisant ses propres ressources, sans faire appel à d'autres intermédiaires.

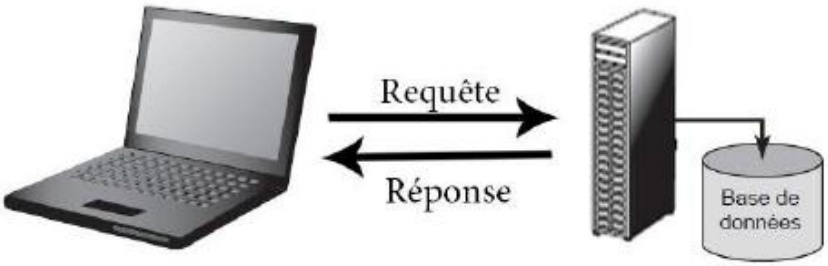

Figure I.18: Architecture client/serveur à 2-tiers

- **L'architecture client/serveur à 3-tiers**

Dans cette architecture un niveau intermédiaire se fait place entre les deux niveaux de l'architecture précédente :

- Le client (niveau 1) : demandeur de ressource.

- Le serveur d'application (niveau 2) : est chargé de fournir la ressource au client mais qui fait appel à un autre serveur pour certaines demandes de ressources. Le niveau deux lui-même est le client d'un serveur de base de données.
- Le serveur de base de données (niveau 3) : fournit les ressources au serveur d'application.

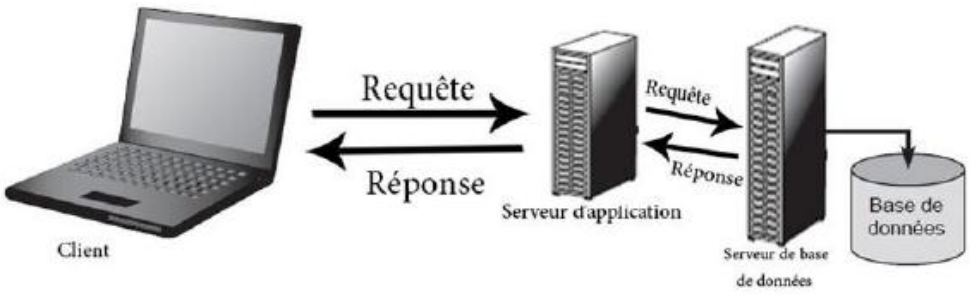

Figure I.19: Architecture client/serveur à 3-tiers

- **L'architecture client/serveur à n-tiers**

Une architecture à n-tiers va plus loin dans le découpage de l'application sur différents serveurs. Elle est également appelée architecture distribuée du fait de la distribuions des traitements et des données sur différents serveurs. Le découpage de base du système reste toujours le même, toutefois les deux parties développées côté serveur vont pouvoir être déployées chacune sur plusieurs serveurs.

L'objectif général de ce type d'architecture est de permettre l'évolutivité du système sous plusieurs aspects : la quantité de données stockée et la disponibilité du serveur

I.9.2 Les différents types de serveur

Les serveurs jouent de nombreux rôles dans l'environnement client/serveur dont certains sont configurés pour l'authentification, certains pour exécuter des appli- cations et d'autres fournissent des services aux utilisateurs. En tant qu'administrateur système, la connaissance des principaux types de serveurs et les fonctions qu'ils exécutent sur le réseau est une chose indispensable.

Il existe plusieurs types de serveurs dont les plus utilisés sont les suivants :

a. Serveurs DNS

Les serveurs DNS (pour Domain Name System) sont des serveurs d'applications utilisés pour résoudre les noms de domaines des ordinateurs clients, c'est-à-dire traduire des noms conçus pour être compris de l'homme en adresses IP exploitables par une machine. Le système DNS est une base de données largement répandue qui contient des noms et d'autres serveurs DNS dont chacun peut servir à demander le nom d'un ordinateur qui, autrement, resterait inconnu. Quand

un client a besoin de l'adresse d'un système, il envoie à un serveur DNS une requête DNS portant le nom de la ressource visée. Le serveur DNS répond en lui fournissant l'adresse IP nécessaire, qu'il trouvera au sein de sa table de noms [9].

b. Serveurs web

Un serveur Web est un programme qui utilise le protocole HTTP pour fournir les fichiers qui constituent les pages Web que les utilisateurs ont demandées via des requêtes transmises par les clients HTTP de leurs ordinateurs [10].

c. Serveur de Messagerie

Un serveur de messagerie électronique permet à ses utilisateurs d'envoyer et de recevoir des courriers électroniques, l'utilisateur a recours à un logiciel client capable de gérer l'envoie et la réception des courriels.

d. Serveurs Proxy

Un serveur proxy est un serveur intermédiaire qui fait office de pont entre l'ordinateur client et le serveur. Il permet aux utilisateurs de naviguer sur Internet en masquant leur adresse IP et en protégeant leur vie privée. Les serveurs proxy peuvent également être utilisés pour filtrer le contenu, restreindre l'accès à certains contenus en ligne et accélérer les connexions en mémorisant les informations les plus fréquemment demandées.

e. Serveurs FTP

Le serveur FTP est un service qui permet de transférer des fichiers entre un ordinateur distant et un serveur, comme un routeur ou un pare-feu. Il est largement utilisé par les administrateurs réseau pour gérer à distance les configurations et les fichiers des équipements Cisco [11].

I.10 Conclusion

La mise en place d'un réseau d'entreprise efficace repose sur l'utilisation de technologies, d'architectures réseaux et de services. Une fois que ce réseau a été créé, il est important de prendre en compte sa sécurité en évitant toute vulnérabilité dans-il. C'est pourquoi nous essayerons dans le prochain chapitre d'examiner la sécurité des architectures réseaux.

Chapitre II *Les architectures réseaux*

II.1 Introduction

Une architecture correspond à l'organisation des différents éléments d`une entité. En ce qui concerne un réseau d`information, il s`agit d`organiser et d`utiliser ce réseau de façon à pouvoir le gérer et repérer les activités inattendues, indésirables et malveillantes. Il existe des outils appropriés et des mécanismes pour assurer une telle protection des architectures réseaux, elles seront abordées dans ce deuxième chapitre.

II.2 Les Architectures des réseaux

L'architecture réseau est la conception d'un réseau informatique. Il s'agit de spécifier les composants physiques du réseau, son organisation ainsi que ses configurations fonctionnelles. On parle alors des procédures de fonctionnement, ainsi que des protocoles de communication utilisés.

I.2.1 Les réseaux locaux

Un réseau local est un système de communication qui permet de relier des ordinateurs et d`autres équipements informatiques dans une zone géographique restreinte. Il fait appel à différents supports physiques tels qu'un câble coaxial, une fibre optique, des ondes électromagnétiques.

Les principales caractéristiques physiques qui permettent de définir un réseau local au sein d'une entreprise sont :

a. La topologie

La structure des réseaux informatiques détermine la façon dont les machines sont reliées les unes aux autres. Deux types de topologies des réseaux sont identifiés en informatique : la topologie physique et la topologie logique.

La topologie physique

Également appelée architecture physique, établit la façon dont le câblage réseau relie les nœuds entre eux.

L'architecture logique (topologie logique)

La topologie logique établit la façon dont les informations se déplacent dans le réseau. Les bits envoyés en mode série sur un support sont utilisés pour transmettre les informations sur un réseau local.

b. La Méthode d'accès au Support

Il est essentiel de définir une politique d'accès au support. Pour éviter les collisions entre les trames émises. Souvent, elle dépend de la topologie employée

c. La Technique de transmission

Il existe principalement deux moyens de transmission :

- La méthode Large Bande (Signal Analogique).
- La méthode Bande de Base (Signal Numérique).

Dans la réalité, la méthode large bande employée. Les informations où transmises en série et en format numérique via le dispositif de transmission. Les données sont toujours transmises de manière codée sur le support pour des raisons liées à la synchronisation du récepteur et à la largeur de bande du signal à transmettre.

d. Les Supports de transmissions

Il existe de nombreux supports de transmission. Les paires torsadées et les câbles coaxiaux sont les supports métalliques les plus anciens et les plus couramment employés pour le transport de courants électriques. La lumière est transmise par des supports en verre, tels que les fibres optiques, tandis que les supports immatériels des communications sans fil propagent des ondes électromagnétiques et sont en plein essor.

II.2.2 Les VLANs

Un VLAN (Virtual Local Area Network) est une solution virtuelle qui permet de diviser un réseau Ethernet physique en plusieurs sous-réseaux.

Un réseau local virtuel peut donc être défini comme un ensemble virtuel d'au moins deux périphériques dans un réseau. Les machines peuvent être regroupées virtuellement au-delà de plusieurs commutateurs. Les périphériques sont classés en fonction de plusieurs éléments en fonction de la configuration du réseau. Le VLAN offre la possibilité de gérer et de maintenir plusieurs réseaux locaux (LAN), soit séparés par des routes, sur une seule et même infrastructure physique commutée.

Le VLAN permet de créer un réseau supplémentaire au-dessus du réseau physique, ce qui présente les bénéfices suivants :

- Une flexibilité accrue pour l'administration et les modifications du réseau, car toute l'architecture peut être ajustée en paramétrant simplement les commutateurs.

- Amélioration de la sécurité car les données sont protégées dans un niveau supplémentaire et éventuellement analysées
- Réduction de la propagation du trafic sur le réseau.

Ainsi, le but principal d'un VLAN est de rendre la fonction d'un réseau local autonome par rapport à l'architecture physique.

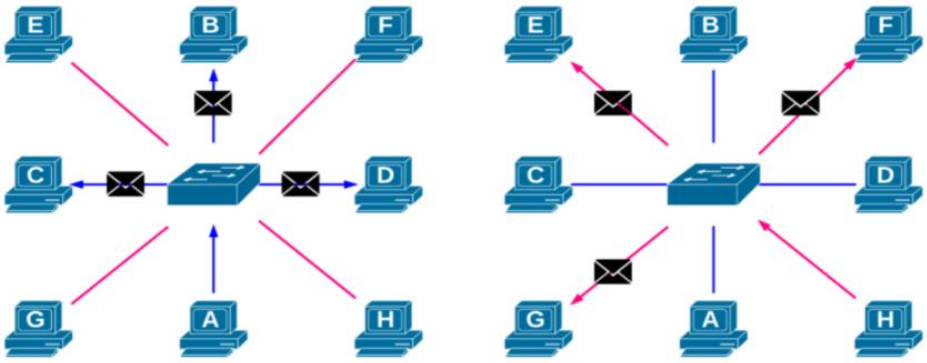

Figure II.1 : Réseau local virtuel VLAN

Selon la Figure 1, les hôtes A, B, C et D font partie du VLAN 66 tandis que les hôtes E, F, G et H font partie du VLAN 33. Ainsi, la Figure 1 présente le flux de diffusion d'A à D et de E à H.

En réalité, les ports du commutateur sont identifiés par un VLAN. Le domaine de diffusion est défini par cet identifiant logique : le trafic de diffusion transmis que sur les ports ayant le même identifiant, les flux de diffusion provenant d'un port du VLAN 66 ne seront transmis que sur les ports dédiés à ce réseau**.**

a. La nécessité de création d'un réseau virtuel

L'architecture physique régit la communication entre les différentes machines dans un réseau local. Pour s'affranchir des contraintes de l'architecture physique, les réseaux virtuels (VLAN) permettent de définir une segmentation logique basée sur un regroupement de machines en utilisant des critères (adresses MAC, numéros de port, protocole, adressage,...).

b. Principes de fonctionnement des VLANs

Le fonctionnement des VLAN se caractérise généralement par deux approches pour le regroupement des utilisateurs connectés dans le réseau local en VLAN.

Le filtrage des trames

- L'analyse de chaque trame permet de créer une table de filtrage pour chaque commutateur, ce qui permet de prendre les décisions adéquates.
- L'utilisation d'une table de filtrage par commutateur entraîne des temps de mise en œuvre lents et des difficultés d'évolution.

La reconnaissance des trames

- Chaque trame possède un code d'identification VLAN (TCI=Information de contrôle du tag) établi par la norme IEEE 802.1q.
- L'identifiant est employé lors de la transmission des paquets sur le réseau.
- Lorsque le paquet quitte le réseau afin d'atteindre les hôtes ou les routeurs, il est retiré.

Cette dernière approche est actuellement la plus répandue sur les VLAN, un exemple est donné par la figure ci-dessous, il s'agit de la Trame 802.1q :

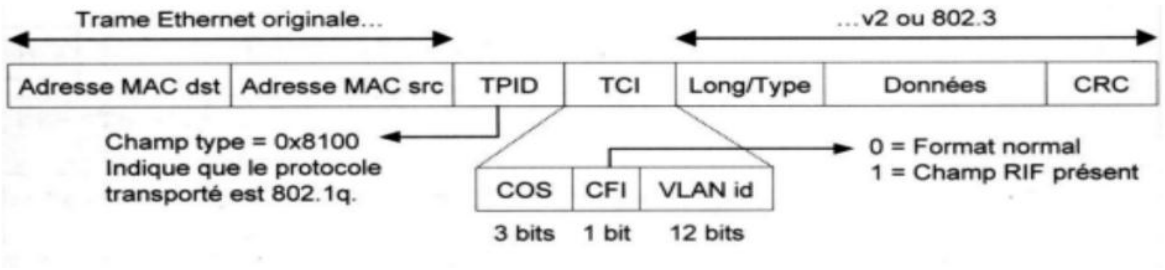

Figure II.2 : Trame 802.1q

TPID (Tag Protocol Identifier) : correspond au champ type d'une trame Ethernet v2

TCI (Tag Control Information) : le label 802.1q inséré dans la trame Ethernet v2

COS (Class Of Service) : utilisé par la norme 802.1q

CFI (Common Format Identifier) : permet de transporter le champ RIF dans le cas d'un tunnel source routing.

VLAN id (numéro de VLA) 4 096 possibilités.

c. Le routage inter-VLAN

Le routage inter-VLAN est essentiel pour interconnecter des réseaux virtuels tout en maintenant une bonne sécurité et une gestion optimale du trafic. Sa mise en place nécessite la configuration d'un périphérique de couche 3 comme un routeur ou un commutateur multicouche.

Les principales raisons d'utiliser le routage inter-VLAN :

- **Sécurité** : Les VLAN permettent d'isoler les données sensibles sur des réseaux séparés. Le routage inter-VLAN autorise l'accès à ces ressources par les appareils autorisés.

- **Partage de ressources :** Le routage inter-VLAN permet aux appareils de différents VLAN d'accéder efficacement aux ressources partagées comme des imprimantes, des serveurs de fichiers, etc.
- **Évolutivité et croissance :** Lorsque le réseau s'agrandit, le routage inter-VLAN facilite la communication entre les nouveaux VLAN sans avoir à reconfigurer physiquement le réseau.
- **Gestion et optimisation du trafic :** Le routage inter-VLAN donne un meilleur contrôle sur la circulation du trafic, permettant d'optimiser les performances du réseau [12].

II.2.3 Les sous réseaux et adressage dans IP

Au commencement de l'informatique, tous les fabricants d'ordinateurs utilisaient leurs propres normes. L'interconnexion de machines de différentes marques était virtuellement impossible, ou très difficile. Donc, afin de résoudre ce problème, des pays ou des organisations ou Donc, afin de résoudre ce problème, des pays ou des organisations ont choisi de mettre en place un protocole qui permet l'interconnexion de toutes ces machines. C'est pourquoi l'émergence du protocole TCP/IP et d'Internet.

a. Adressage IP

Une adresse IP correspond à une adresse logique assignée à un dispositif. Son utilisation permet de l'identifier de manière distincte dans un réseau logique. Cette adresse sert de fondement à la transmission des données de l'expéditeur au destinataire approprié. En réalité, c'est simplement un numéro qui doit être unique sur tout le réseau.

Pour éviter toute défaillance, un réseau TCP/IP sera divisé en sous-réseaux. Elle sera donc composée de deux composantes : un composant réseau au début de l'adresse et une composante hôte à la fin de celle-ci.

Les types d'adresse

- **Adresses unicast**

Il s'agit d'une adresse "normale". Elle désigne une seule machine.

- **Adresses anycast**

Une adresse anycast représente un ensemble de machines. Lorsqu'un message sera envoyé sur cette adresse, la machine la plus proche le recevra.

- **Adresses multicast**

Comme pour les adresses anycast, une adresse multicast représente un ensemble de machines. Toutefois, lorsqu'un message sera envoyé sur cette adresse, toutes les machines du groupe le recevront.

b. Les sous-réseaux

Comme nous l'avons mentionné précédemment, l'adresse IP comprend une partie réseau ainsi qu'une partie hôte.

En ce qui concerne la version 4 de l'IP, les adresses possèdent une partie réseau de 8, 16 ou 24 bits en fonction de la classe d'adresse.

Ces masques standards ne sont pas toujours adaptés aux besoins spécifiques de chacun. C'est la raison pour laquelle il est envisageable de diviser les réseaux par défaut en utilisant un masque de sous-réseau.

Un masque de sous-réseau est un nombre de la même taille que l'adresse. Les premiers bits sont à 1 et désignent la partie réseau. Les derniers bits sont à 0 et désignent la partie hôte.

Exemples : 111111...111111000000...000000

Notation

- En IP v4, les masques de réseau peuvent se représentés comme une adresse réseau.
- En IPv4, on peut écrire 11111111111111111111111111100000 de manière 255.255.255.224.
- Une autre méthode utilisée en IPv4 consiste à faire suivre l'adresse IP d'une barre oblique, puis du nombre de bit du masque IP.

Subdivision de réseaux

Quand il s'agit de subdiviser des réseaux, il existe deux méthodes envisageables. Nous pouvons soit chercher à établir le nombre de sous-réseaux que nous souhaitons obtenir, soit chercher à établir le nombre de machines par sous-réseaux.

Subdivision sur base du nombre de sous-réseaux

Dans cette situation, nous procéderons à une augmentation du masque réseau (bits à 1) d'autant de bits qu'il est requis pour obtenir le nombre de subdivisions désiré. Dans le tableau ci-dessous, nous avons sélectionné quelques exemples qui illustrent le nombre de subdivisions souhaitées en fonction du nombre de bits enregistrés**.**

Tableau II.1 : Subdivisions sur base du nombre de sous-réseaux

Nombre de subdivisions	Nombre de bits
2	1
3 à 4	2
5 à 8	3
9 à 16	4
17 à 32	5

Subdivision sur base du nombre d'hôtes

Dans cette situation, nous pourrons conserver autant de bits pour la partie machine (bits à 0) afin d'obtenir le nombre de machines moins deux (l'adresse réseau et l'adresse de diffusion).

Tableau II.2 : Subdivisions sur base du nombre d'hôtes

Nombre de subdivisions	Nombre de bits
2	2
3 à 6	3
7 à 14	4
15 à 30	5
31 à 62	6

II.2.4 L'interconnexion de réseaux et le routage dans IP

a. L'interconnexion de réseaux

L'interconnexion de réseaux permet de relier plusieurs sous-réseaux initialement isolés afin de les faire communiquer entre eux [13]. Les principaux points à retenir sont :

- Les équipements spécifiques, tels que les routeurs, sont utilisés pour établir l'interconnexion au niveau de la couche réseau (couche 3 du modèle OSI) [14]. Les informations sont transmises à travers les réseaux interconnectés.
- Quand deux réseaux utilisent des protocoles distincts, l'interconnexion nécessite des équipements capables de traduire entre ces protocoles. Par exemple, un routeur peut interconnecter un réseau Ethernet et un réseau X.25 (est un protocole de transmission de données)
- Le routage IP joue un rôle crucial dans l'interconnexion. Les routeurs font appel à des tables de routage afin d'identifier la meilleure voie à emprunter pour acheminer les paquets entre les divers sous-réseaux [14].
- Les routeurs peuvent utiliser des protocoles de routage internes tels que RIP et OSPF pour apprendre de manière dynamique les chemins vers les sous-réseaux et mettre à jour leurs tables en conséquence [14].
- À l'échelle mondiale, Internet est un réseau interconnecté qui utilise le protocole IP. Chaque réseau est connecté à d'autres réseaux, ce qui donne finalement la possibilité à n'importe quel hôte de communiquer avec n'importe quel autre à travers l'infrastructure Internet [13].

Donc, Il est possible d'interconnecter des réseaux grâce à l'utilisation de routeurs et de protocoles de routage qui permettent de faire communiquer des sous-réseaux initialement isolés, tant au niveau local qu'à l'échelle mondiale, avec Internet.

b. Le routage dans IP

Le routage dans IP désigne la manière dont les paquets de données sont transportés d'un hôte à un autre à travers un réseau, en utilisant des routeurs pour déterminer la meilleure voie à emprunter. Voici quelques éléments importants concernant le routage dans IP en se basant sur les sources fournies :

- La technique du routage IP consiste à utiliser des tables de routage qui renferment des données sur les réseaux et les hôtes de destination, ainsi que sur la façon la plus efficace d'atteindre ces destinations. Il est possible de mettre à jour ces tables de manière statique ou dynamique en utilisant des protocoles de routage tels que RIP, OSPF ou BGP.
- La table de routage de chaque nœud du réseau permet de rediriger les paquets vers le prochain routeur en fonction de l'adresse IP de destination. De la source jusqu'à la destination, le routage se déroule de manière progressive, en utilisant plusieurs routeurs intermédiaires.

- Selon le type de réseau et sa taille, les protocoles de routage diffèrent. Le routage entre systèmes autonomes peut être effectué en utilisant des protocoles à vecteur de distances tels que RIP, des protocoles à état de liens tels que OSPF, et le protocole à vecteur de chemin BGP.

c. les différents types de routage IP

En général, les diverses formes de routage IP sont divisées en deux catégories principales : le routage statique et le routage dynamique. Voici un aperçu qui repose sur les données des sources fournies :

- **Routage statique**

Les protocoles de routage statique nécessitent que l'administrateur ajuste de manière manuelle les chemins routiers sur les routeurs. Cela permet d'augmenter la sécurité du réseau en évitant les mises à jour automatiques qui pourraient potentiellement causer des accidents.

- **Routage dynamique**

Les routeurs peuvent intégrer automatiquement des informations à leurs tables de routage à partir des routeurs connectés grâce aux protocoles de routage dynamique. Cela s'effectue automatiquement sans intervention humaine**.**

Les algorithmes utilisés dans ces protocoles permettent de sélectionner les routes optimales en prenant en compte différents critères tels que la distance, la charge du réseau, etc.

En résumé, le routage dans IP est un processus essentiel qui permet de diriger efficacement les paquets de données à travers un réseau en utilisant des routeurs et des tables de routage pour assurer une communication fiable et optimale entre les différents hôtes et réseaux.

II.3 Les architectures sécurisées de réseaux

L'architecture sécurisée de réseau sont de conception et de stratégie structurée visant à assurer la protection des réseaux informatiques contre les menaces et les attaques potentielles. Elles intègrent plusieurs éléments et principes pour renforcer la sécurité globale du réseau

II.3.1Le Pare-Feu (Firewall)

Un pare-feu, appelé aussi coupe-feu ou firewall à pour but de contrôler et de filtrer l'accès entre un réseau d'entreprise et un autre réseau. Le firewall peut être soit un objet matériel ou un programme fonctionnant sur un ordinateur [14].

Il s'agit donc d'une passerelle filtrante qui comprend au moins les interfaces réseau suivantes :

- Une interface pour le réseau à protéger (réseau interne)
- Une interface pour le réseau externe.

Figure II.3 : Pare-Feu ou Firewall

a. Emplacement de Pare-feu dans un réseau

L'emplacement des pare-feu est essentiel pour une gestion efficace des flux de trafic provenant de l'extérieur et de l'intérieur. La position stratégique des pare-feu dans le réseau est essentielle pour qu'ils puissent pleinement jouer leur rôle**.**

b. Un pare-feu unique

Une méthode de configuration réseau plus économique implique l'utilisation d'un pare-feu unique comprenant au moins trois interfaces réseau. Ainsi, la zone démilitarisée sera intégrée à ce pare-feu. Le mécanisme de pare-feu est le suivant : le périphérique réseau externe établit la connexion à partir du FAI (Fournisseur Access Internet), le deuxième périphérique connecte le réseau interne, puis le troisième périphérique du pare-feu connecte la DMZ si elle est présente dans le réseau de l'entreprise.

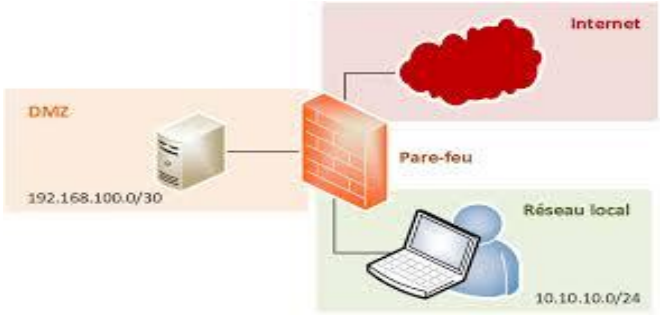

Figure II.4 : Emplacement d'un pare-Feu Unique

c. Deux ou plusieurs pare-feu

La méthode la plus sûre pour protéger un réseau est d'utiliser deux pare-feu afin de créer la DMZ. Le pare-feu initial (connu sous le nom de pare-feu « frontal ») est configuré de manière à ne permettre que le trafic destiné à la DMZ. Le pare-feu secondaire (connu sous le nom de pare-feu « principal ») est exclusivement chargé de gérer le trafic entre la DMZ et le réseau interne. Afin d'améliorer la protection, il est envisageable d'utiliser des pare-feu conçus par deux fournisseurs différents, permettant ainsi de réduire le risque de présenter les mêmes failles.

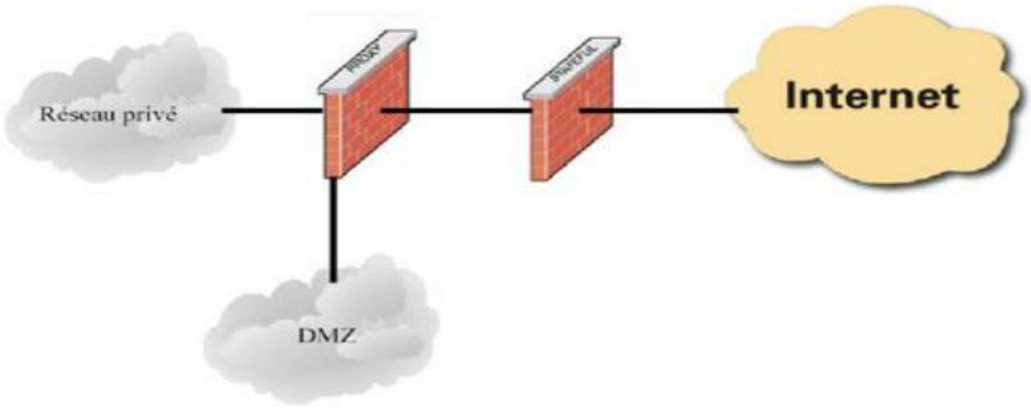

Figure II.5 : emplacement de deux pare-feu

d. Fonctionnement d'un système de Pare-Feu

Un pare-feu est constitué d'une série de règles préétablies qui permettent :

- d'autoriser la connexion (allow)
- de bloquer la connexion (deny)
- de rejeter la demande de connexion sans prévenir l'émetteur.

Toutes ces règles permettent d'appliquer une méthode de filtrage qui dépend de la politique de sécurité qu'adopte l'administrateur du réseau. Deux types de politiques de sécurité sont généralement distingués :

- Soit de ne permettre que les communications qui ont été explicitement autorisées (c'est le Principe du moindre privilège).
- Soit d'interdire les échanges qui ont été explicitement interdits.

Afin d'assurer un bon fonctionnement d'un pare-feu, on observe diverses formes de filtrage au niveau du pare-feu :

e. Le Filtrage simple de paquets (stateless)

Le système de pare-feu repose sur le principe du filtrage simple de paquets. Il examine les données de chaque paquet de données qui est échangé entre une machine du réseau interne et une machine externe.

Les paquets de données qui sont échangés entre une machine du réseau externe et une machine du réseau interne traversent le pare-feu et ont les en-têtes suivants, qui sont systématiquement analysés par le pare-feu :

- Adresse IP source et destination.
- Numéro de port (rappel : un port est un numéro associé à un service ou une application réseau).
- Le protocole de niveaux 3 et 4.

f. le filtrage de paquet avec état (Stateful)

L'amélioration par rapport au filtrage classique consiste à conserver la trace des sessions et des connexions dans des tables d'états internes au pare-feu. Le pare-feu prend alors ses décisions en fonction des états de connexions et peut réagir en cas de situations protocolaires anormales. Ce filtrage permet également de se protéger contre certains types d'attaques DOS.

En ce qui concerne le protocole FTP (et les protocoles similaires), il est plus complexe car il sera nécessaire de gérer l'état de deux connexions. Effectivement, le protocole FTP assure la gestion d'un canal de contrôle créé par le client et d'un canal de données créé par le serveur. Cela signifie que le pare-feu est familiarisé avec le protocole FTP, ainsi que tous les protocoles qui font appel au même principe. On appelle cette méthode le filtrage dynamique (Stateful Inspection) et elle a été créée par Checkpoint. Cependant, cette méthode est désormais gérée par d'autres fabricants.

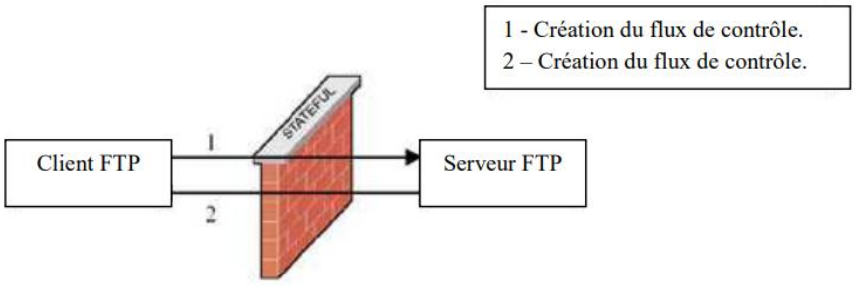

Figure II.6 : filtrage de paquet avec état (FTP)

g. le filtrage applicatif (ou pare-feu de type proxy ou proxying applicatif)

Le filtrage applicatif est effectué, comme son nom l'indique, dans la couche Application. Cela nécessite évidemment la capacité d'extraire les données du protocole de niveau 7 afin de les analyser. On traite les requêtes à l'aide de processus spécifiques, comme par exemple une requête HTTP sera filtrée par un processus proxy HTTP. Le pare-feu refusera toutes les demandes qui ne respectent pas les modalités du protocole. Cela signifie que le pare-feu proxy doit être au courant de toutes les règles protocolaires des protocoles qu'il doit filtrer.

h. Les différents types de pare-feu

Le choix du bon type de pare-feu dépend de la structure de votre réseau et des exigences de sécurité pour fournir une protection efficace contre les menaces potentielles.

- **Les pare-feu bridge**

Les pare-feu bridge (ou transparents) sont une catégorie de pare-feu qui fonctionnent comme de véritables câbles réseau, mais qui sont également équipés d'une fonction de filtrage.

Les pare-feu bridge offrent la possibilité de connecter un pare-feu entre deux segments du réseau sans avoir à modifier la configuration des autres équipements. Ils sont fréquemment employés afin de contrôler le trafic entre le réseau à grande échelle et le réseau interne, ou entre divers segments locaux.

- **Les firewalls matériels**

On les retrouve fréquemment sur des routeurs achetés dans le commerce par des fabricants de renom tels que Cisco ou Nortel. Ils sont intégrés directement dans la machine, servant de « boîte noire » et s'intègrent parfaitement au matériel. Il est fréquent de les configurer de manière assez complexe, mais leur principal avantage réside dans leur facilité d'interaction avec les autres fonctionnalités du routeur en raison de leur présence sur le même logiciel réseau. Leur configuration est souvent assez rigide, ce qui les rend peu vulnérables aux attaques.

- **Les firewalls logiciels**

Ils sont fréquemment destinés au commerce et visent à protéger un ordinateur spécifique plutôt qu'un ensemble d'ordinateurs. Fréquemment coûteux, ils peuvent être rigides et parfois très peu sécurisés. Ils se concentrent en effet davantage sur la facilité d'utilisation plutôt que sur l'exhaustivité, dans le but de rester accessibles à l'utilisateur final.

II.3.2 La Zone démilitarisée (DMZ)

Dans le domaine de la sécurité informatique, une zone démilitarisée (DMZ) désigne un sous-réseau comprenant les services exposés et accessibles de l'extérieur d'une entreprise. Son rôle est de faire office de zone tampon avec les réseaux non sécurisés comme Internet.

Son but est de renforcer la sécurité du réseau local de l'entreprise grâce aux DMZ. Au sein de ce système de réseau, un point de connexion protégé et surveillé, orienté vers l'extérieur, a la possibilité d'accéder aux éléments exposés dans la zone dématérialisée, tandis que le reste du réseau est protégé par un pare-feu.

Les DMZ, une fois mises en place correctement, permettent aux entreprises de repérer et de corriger les vulnérabilités de sécurité avant qu'elles ne pénètrent dans le réseau interne, où les ressources les plus précieuses sont stockées.

a. Objectif des zones démilitarisées

L'objectif principal des DMZ est de préserver les hôtes les plus vulnérables aux attaques. Des services accessibles aux utilisateurs en dehors du réseau local sont généralement disponibles parmi ces hôtes, comme la messagerie, les serveurs Web et les serveurs DNS. Ils sont placés dans un sous-réseau surveillé, car ils sont vulnérables, ce qui permet de protéger le reste du réseau en cas d'attaque.

Les hôtes logés dans la DMZ ne peuvent accéder aux autres services du réseau interne qu'avec des autorisations d'accès très limitées, car le niveau de sécurité des données transmises dans cette zone est parfois inexistant. D'autre part, les échanges entre les hôtes logés dans la DMZ et le réseau externe sont également restreints pour qu'il soit possible d'étendre cette zone tampon. Les hôtes du réseau protégé peuvent interagir avec les réseaux interne et externe grâce à cette pratique, tandis que le pare-feu assure la répartition et la gestion du trafic partagé entre la DMZ et le réseau interne. Un pare-feu supplémentaire sera généralement employé afin de préserver la DMZ de toute menace provenant du réseau externe.

Il sera nécessaire de placer tous les services accessibles aux utilisateurs depuis un réseau externe dans la zone DMZ. Les services les plus fréquemment utilisés comprennent : les serveurs Web, les serveurs DNS, les serveurs de messagerie, les serveurs FTP, etc.

b. Type de DMZ

Afin d'améliorer la sécurité du réseau, il existe deux types de DMZ, dont chaque type est connecté à un pare-feu, ou les deux sont connectés à un même pare-feu pour filtrer les paquets entrants ou sortants. Une DMZ privée et une DMZ publique sont disponibles.

- La DMZ privée doit inclure tous les services qui peuvent être connectés depuis le réseau LAN, tels que DNS, DHCP, SQL.
- La DMZ publique implique la mise en place de tous les services qui peuvent être connectés depuis internet ou le réseau WAN.

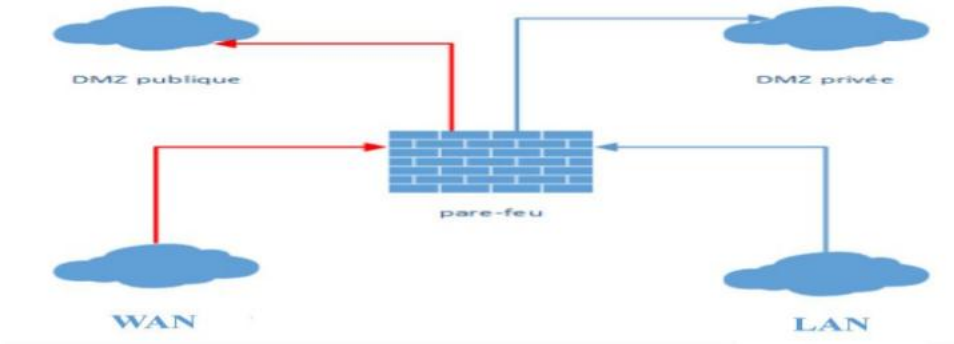

Figure II.7 : Les types de DMZ

c. Emplacement des zones démilitarisées

Dans un réseau d'entreprise, la localisation de la zone démilitarisée peut parfois être influencée par le nombre de pare-feu qui sont présents dans le réseau afin de filtrer les flux entre le réseau local et Internet. Deux emplacements principaux des DMZ sont généralement identifiés :

- **DMZ avec un Pare-Feu**

Un seul pare-feu performant (par exemple un routeur avec pare-feu) avec trois connexions réseaux distinctes : une pour Internet, une pour le réseau local et une troisième pour la zone démilitarisée est plus avantageux. Quant aux DMZ protégées, toutes les connexions sont surveillées par le même pare-feu indépendamment les unes des autres, ce qui peut entraîner un seul point de défaillance dans le réseau. De plus, dans une telle configuration, le pare-feu doit être capable de gérer à la fois le trafic provenant d'Internet et les accès provenant du réseau local.

Un pare-feu surveille les connexions réseau et contrôle le trafic Internet et l'accès au réseau local grâce à une zone démilitarisée protégée.

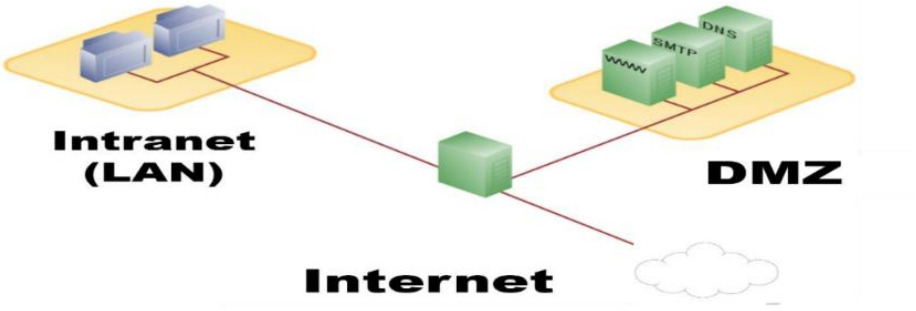

Figure II.8 : Zone démilitarisée avec un Pare-Feu

Un pare-feu unique surveille les connexions réseau et contrôle le trafic Internet et l'accès au réseau local grâce à une zone démilitarisée protégée.

- **DMZ avec deux Pare-feu**

Il est nécessaire de mettre en place des concepts de zones démilitarisées afin de protéger les réseaux d'entreprises contre les intrusions provenant du réseau public (WAN). Il est possible que ce soit des éléments matériels autonomes ou un logiciel de pare-feu sur un routeur. La zone démilitarisée du réseau public est protégée par le pare-feu externe, tandis que le pare-feu interne est connecté entre le DMZ et le réseau de l'entreprise.

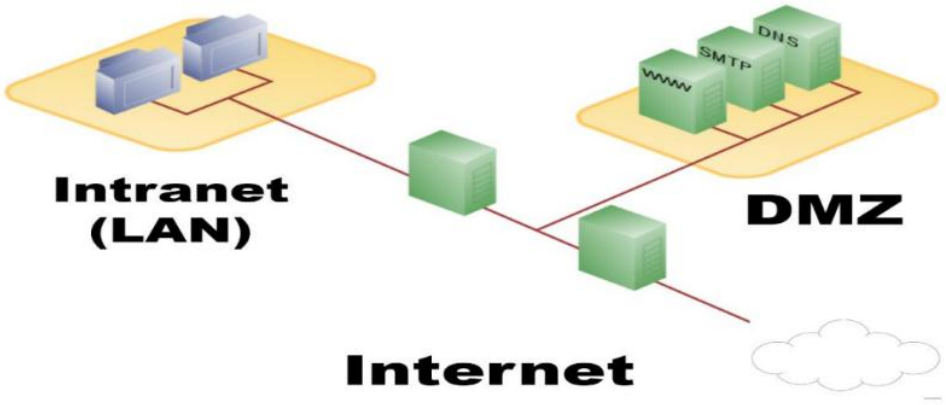

Figure II.9: Zone démilitarisée avec deux Pare-Feu

Afin de protéger les machines de la DMZ contre les attaques d'un serveur compromis, il est envisageable de les éloigner en utilisant d'autres logiciels pare-feu ou en segmentant le VLAN.

II.4 Conclution

Il est essentiel de tenir compte de la sécurité pour les équipements réseaux., ne pas ignorer les risques accourus et être capable de mettre en oeuvre une architecture de sécurité répondant aux exigences de l'entreprise. Ceci en faisant appel aux équipements de sécurité (Porxy, Pare-feu, etc.) et aussi les réseaux virtuels . Ayant présenté les méthodes de la sécurité des architectures réseau, nous allons dans le chapitre suivant les implémenter en déployant une architecture sécurisée d'un réseau d'entreprise.

Chapitre III *Simulation et résultat*

III.1 Introduction

Dans ce chapitre, nous passerons à la dernière étape, la mise en œuvre. Nous présentons la solution précédemment proposée, pour cela nous commencerons par arborer le simulateur utilisé, puis nous expliquerons en détail les différentes étapes de notre architecture.

III.2 Logiciel de simulation

III.2.1 Présentation du système Cisco

Cisco system est une société informatique américaine spécialisée dans le matériel réseau (les routeurs et les commutateurs Ethernet). Fondée en 1984 par Leonard Bosack et Sandra Lerner, elle est basée à San Jose, en Californie [15].

Figure III.1 : Société de Cisco system

III.2.2 Presentation du Packet Tracer 8.2.1

Packet Tracer est un logiciel de CISCO permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles [16].

Figure III.2: Logo du logiciel Cisco Packet Tracer

III.2.3 Description des différentes rubriques

Voici une description des principales rubriques et fonctionnalité de Cisco Packet Tracer 8.2.1 :

Figure III.3 : Interface graphique de Packet Tracer

Partie 1 : la barre de menu

Dans cette zone on retrouve les fonctions standards présentent dans n'importe quel logiciel.

On retrouve la fonction « sauvegarder », « ouvrir un fichier », « nouveau fichier » et d'autres fonctions de base.

Partie 2 : zone de travail

La zone de travail est l'endroit où nous placerons les équipements pour les connecter entre eux et les configurer pour créer le réseau souhaité.

Partie 3 : types d'équipements

Dans cette zone il y a toutes les catégories d'équipements disponibles dans le logiciel.

Partie 4 : choix d'équipements

Une fois la catégorie d'équipement choisit la zone 4 nous permet de choisir notre modèle souhaité en fonction des besoins nécessaires à la création de notre réseau.

Partie 5 : affichage des paquets

Dans cette fenêtre on peut voir les paquets qui sont utilisés lors des simulations du réseau.

Partie 6 : temps réel/simulation

Cette fonction sert à passer du temps réel au mode simulation. En temps réel on configure nos équipements et on les tests. Le mode simulation est un mode pas à pas qui permet d'étudier plus en détails les échanges fait entre les équipements.

III.3 Schématisation d'un réseau sécurisé d'entreprise

Ce schéma repose sur deux dispositifs de sécurité essentiels : Le pare-feu ASA (Adaptive Security Appliance) et le NAT (Network Address Translation). Le pare-feu ASA est utilisé pour contrôler et sécuriser les flux de données entrants et sortants du réseau, tandis que le NAT permet de traduire les adresses IP privées en adresses IP publiques, facilitant ainsi la communication avec l'extérieur tout en masquant l'infrastructure interne du réseau.

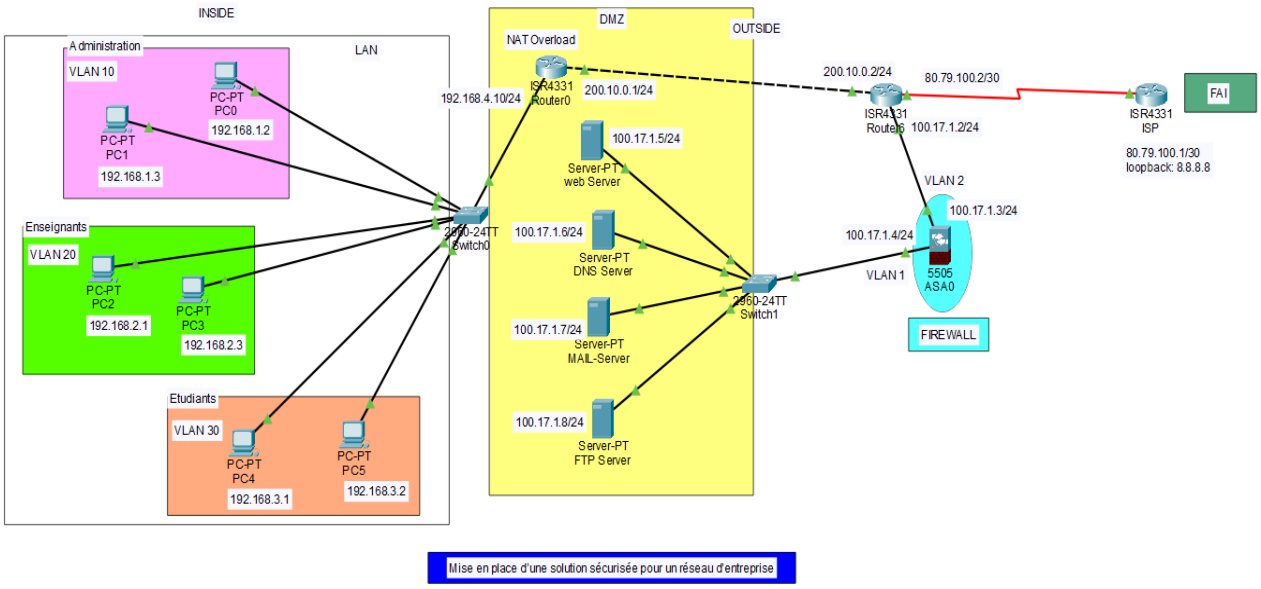

Figure III.4 : l'architecture de réseau

III.3.1 Composition du schéma de simulation

Notre architecture de simulation propose une représentation réaliste d'une architecture de réseau d'entreprise. Elle est composée des structures suivantes :

- Un réseau local (Locale Interne « INSIDE ») qui possède six pcs (PC-PT) et un switch (2960-24TT) de Cisco.
- Un réseau externe (Local Externe « OUTSIDE ») qui contient 02 routeurs (ISR 4331), une DMZ contenant quatre serveurs (server-PT) avec quatre services.
- Le Firewall ASA 5505.

- Un réseau public (Globale Interne et externe) simulé par le routeur ISP (ISR 4331).

Cette simulation permet de tester et d'optimiser les performances, la sécurité, et la résilience du réseau d'entreprise dans un environnement contrôlé avant de déployer les modifications dans le réseau réel.

III.3.2 Table d'adressage des équipements

L'affectation des adresses IP pour cette simulation sont affectées de la manière suivante :

Tableau III.1: D'adressage des équipements

Equipement	Interface	Adresse IP	Le masque de sous réseau
PC0	Fast Ethernet 0	192.168.1.2	255.255.255.0
PC1	Fast Ethernet 0	192.168.1.3	255.255.255.0
PC2	Fast Ethernet 0	192.168.2.1	255.255.255.0
PC3	Fast Ethernet 0	192.168.2.3	255.255.255.0
PC4	Fast Ethernet 0	192.168.3.1	255.255.255.0
PC5	Fast Ethernet 0	192.168.3.2	255.255.255.0
Routeur0 (NAT)	Gig 0/0/1	192.168.4.1	255.255.255.0
	Gig 0/0/0	200.10.0.1	255.255.255.0
Routeur6	Gig 0/0/0	200.10.0.2	255.255.255.0
	Gig 0/0/1	100.17.1.2	255.255.255.0
	Se 0/2/0	80.79.100.2	255.255.255.252
Routeur ISP	Se 0/2/1	80.79.100.1	255.255.255.252
ASA Firewall	VLAN 1	100.17.1.4	255.255.255.0
	VLAN 2	100.17.1.3	255.255.255.0
DMZ	Fast Ethernet 0	100.17.1.5	255.255.255.0
	Fast Ethernet 0	100.17.1.6	255.255.255.0
	Fast Ethernet 0	100.17.1.7	255.255.255.0
	Fast Ethernet 0	100.17.1.8	255.255.255.0

III.4 Configuration des équipements

La configuration de base des périphériques dans Packet Tracer implique la définition de paramètres réseau de base tels que l'adresse IP, le mot de passe et le nom d'hôte. La configuration peut ensuite être sauvegardée de différentes manières pour une restauration ultérieure.

III.4.1 Configuration des PCs

La configuration des PCs consiste à donner les adresses IP avec le masque de sous réseau pour chaque interface.

Pour configurer une machine il suffit de cliquer sur le PC après on choisit ‘’Desktop’’ dans le menu, on sélectionne la case IP configuration, cela nous permet de saisir les paramètres IP (adresse, masque, passerelle, DNS).

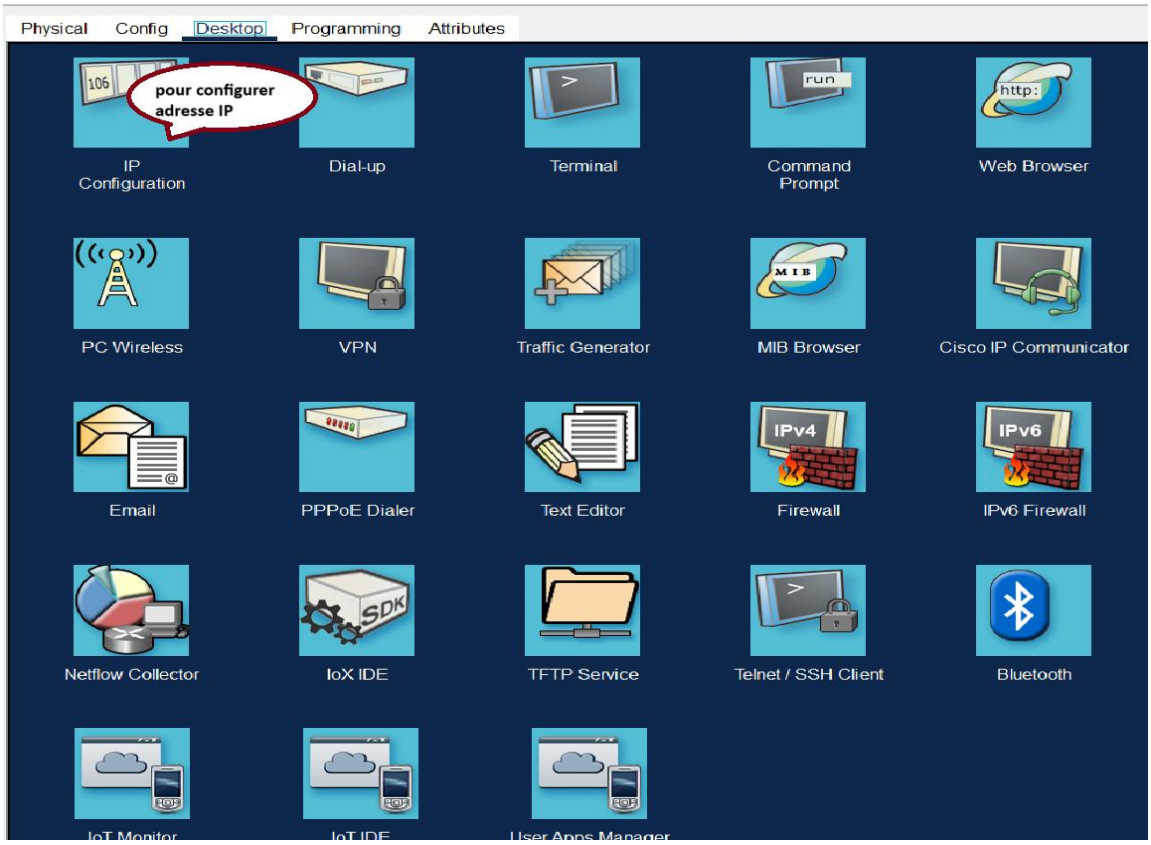

Figure III.5: Interface de configuration des PCs

Voici la case ‘’ IP configuration ’’ :

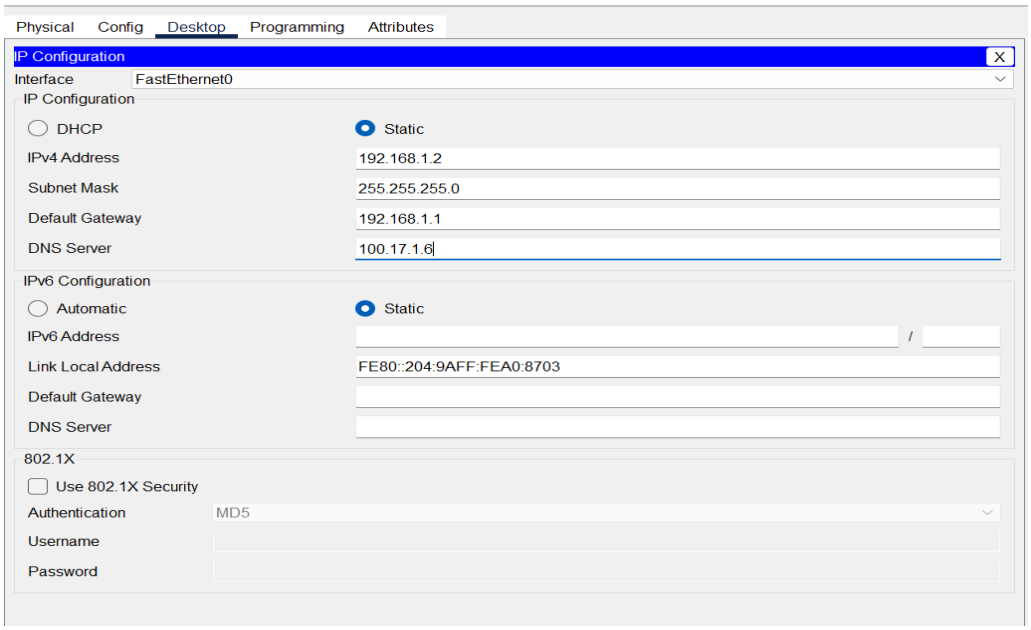

Figure III.6 : IP configuration

PC0 :

Ici la configuration de PC0 :

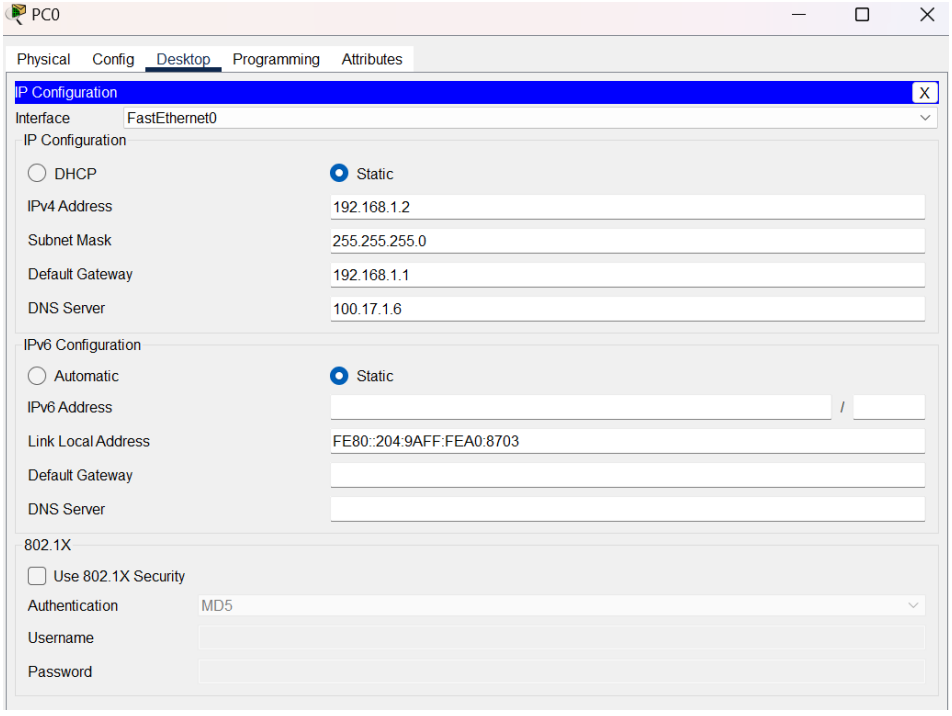

Figure III.7: La configuration PC0

La configuration des autres PCs est de même manière.

III.4.2 Configuration d'un Switch0

Dans la simulation d'un switch sous Packet Tracer, il suffit de suivre les étapes suivantes :

- On entre dans le mode privilège puis dans le mode de configuration.
- On commence par créer des VLANs 10, 20, 30 :

Tableau III.2 : les VLANs de Switch0

VLAN 10	PC0 192.168.1.2
	PC1 192.168.1.3
VLAN 20	PC2 192.168.2.1
	PC3 192.168.2.3
VLAN 30	PC4 192.168.3.1
	PC5 192.168.3.2

- On passe à la configuration de l'interface VLAN en utilisant la commande << range >>.
  Les ports associes aux VLAN sont toujours configures en mode accès.

Figure III.8 : Création des VLANs et attribution des ports aux VLANs

a. Test de simulation

On utilise deux manières de test ICMP pour vérifier visuellement la connectivité réseau entre deux PCs : test ICMP visuel (enveloppe) et la commande PING.

Nous choisissons deux PCs concernant au même VLAN :

PC0 (192.168.1.2) appartient à VLAN 10.

PC1 (192.168.1.3) appartient à VLAN 10.

- **Test ICMP visuel :**

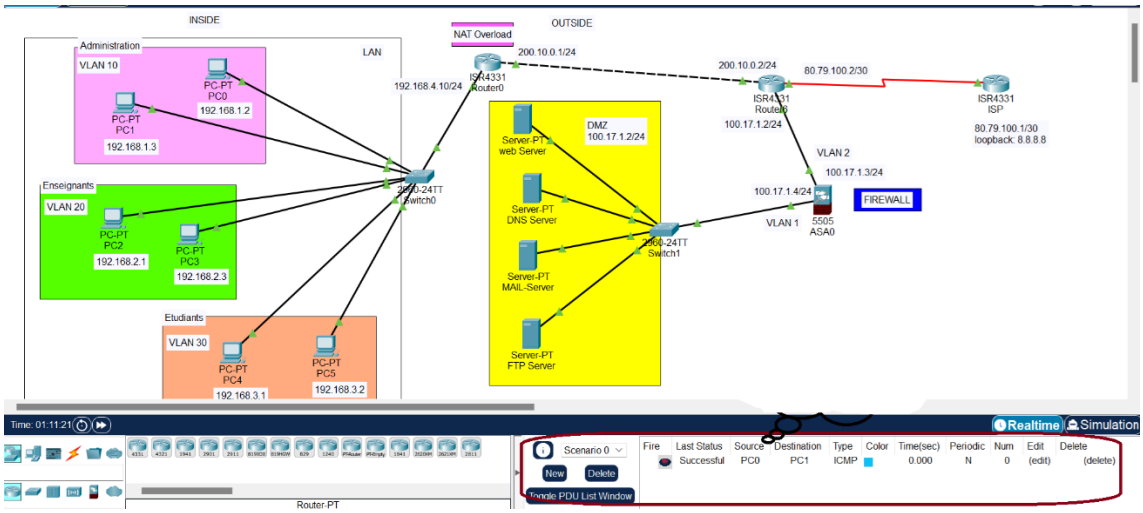

Figure III.9 : ICMP visuel

- **La commande PING :**

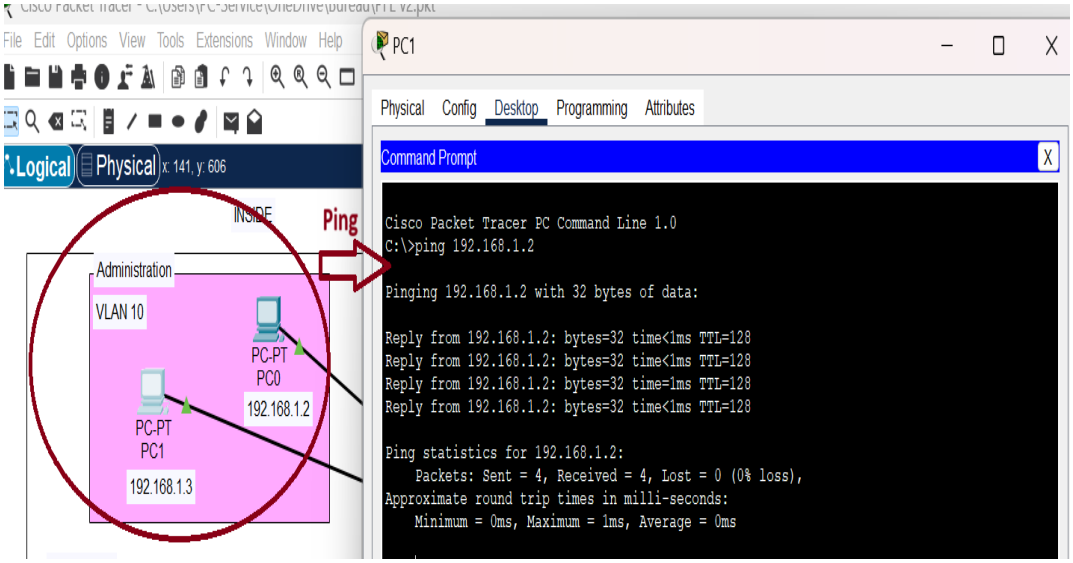

Figure III.10 : PING

Donc la connectivité de réseau entre PC0 et PC1 est validé.

Entre deux PCs les VLANs différents :

Nous choisissons PC0 (VLAN 10) et PC4 (VLAN 30). Les deux VLANs sont séparés et deux réseaux différents donc on va tester cette séparation est-ce que c'est validé.

- **Test ICMP visuel :**

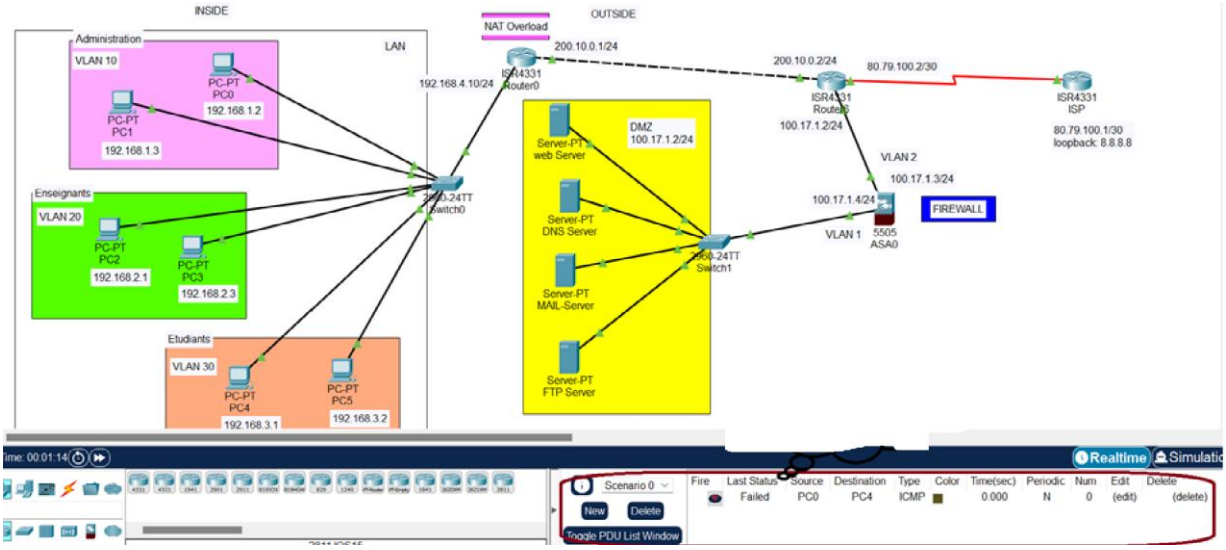

Figure III.11 : ICMP visuel

- **Test PING :**

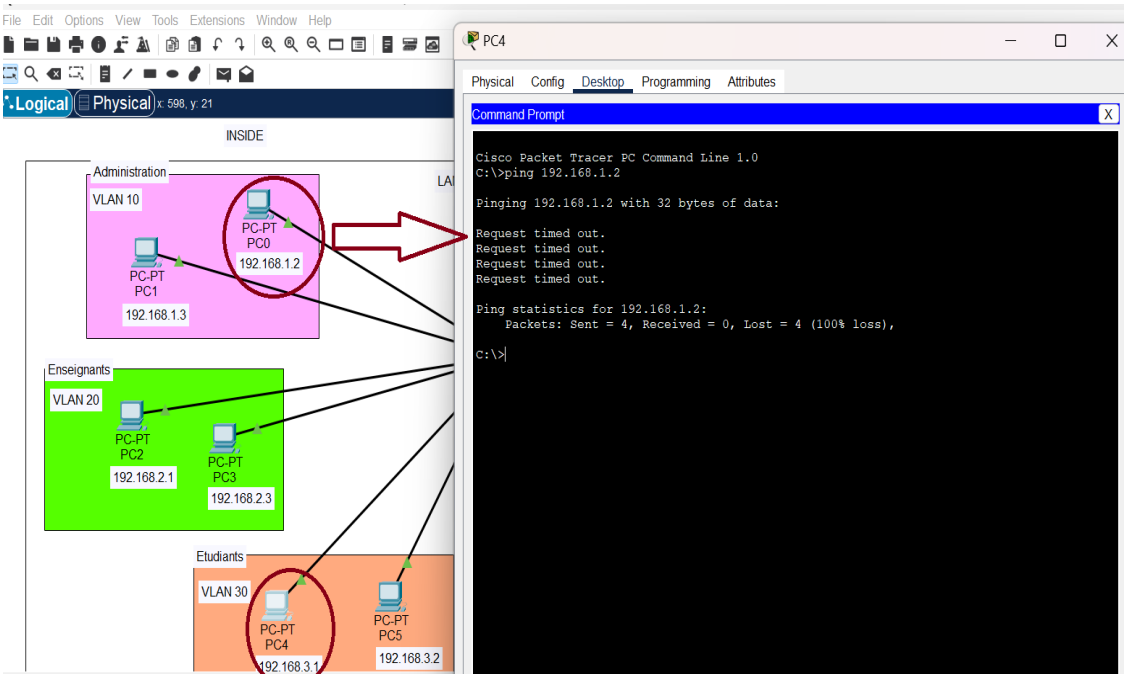

Figure III.12 : PING

Donc cette séparation de deux VLANs est valide.

b. Résultats

D'après les résultats obtenus, il est évident que seuls les ordinateurs qui partagent le même VLAN peuvent interagir.

III.4.3 Configuration de Routeur0

a. Adressage IP d'une interface d'un routeur Cisco :

Tableau III.3 : La configuration IP choisie pour les interfaces Routeur0

Configuration IP / Interfaces	Adresse IP	Masque de sous réseau
GigabitEthernet 0/0/1	192.168.4.10	255.255.255.0
GigabitEthernet 0/0/0	200.10.0.1	255.255.255.0

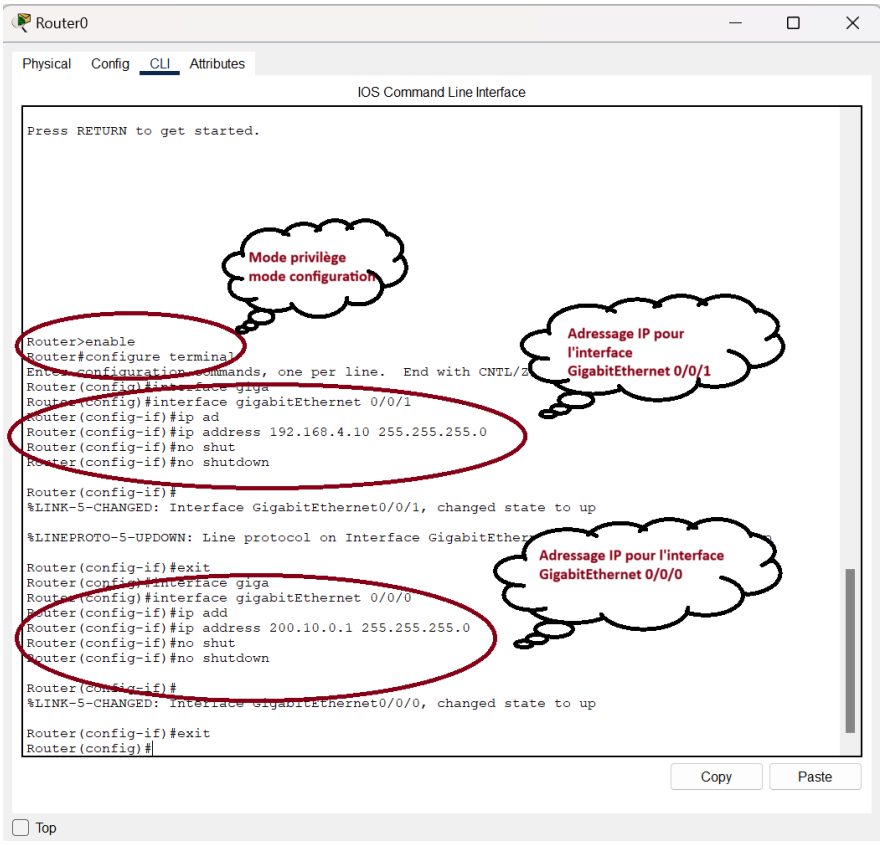

Figure III.13 : La configuration IP d'un Routeur0

b. Configuration de routage statique

Pour référencer un chemin pour le Routeur0, il est nécessaire de fournir une route par défaut. Cette route lui permet de trouver un chemin de dernière option.

```
Router(config)#ip route 0.0.0.0 0.0.0.0 200.10.0.2
```

Figure III.14: Configuration de la passerelle

c. Configuration de routage inter VLAN

On configure chaque VLAN avec sa propre interface virtuelle, pour contrôler le trafic réseau et améliorer la sécurité.

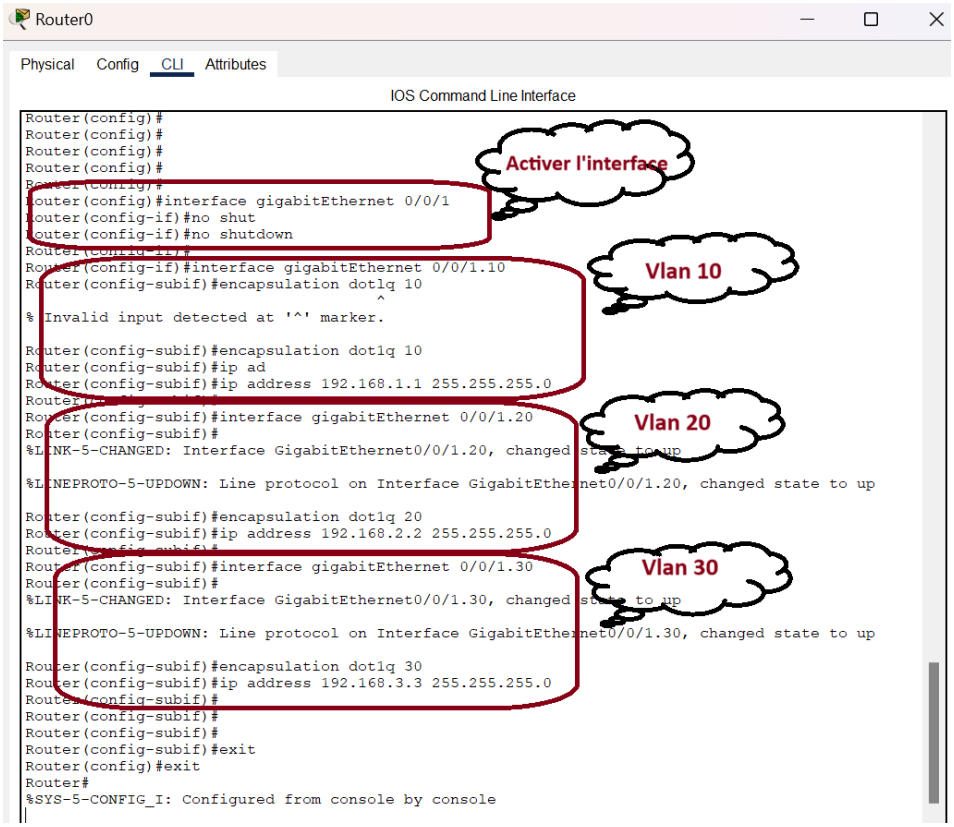

Figure III.15: Configuration inter VLAN de Routeur0

- **Vérification des sous-interfaces crée**

On utilise la commande suivante :

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   200.10.0.1      YES manual up                    up
GigabitEthernet0/0/1   192.168.4.1     YES manual up                    up
GigabitEthernet0/0/1.10192.168.1.1     YES manual up                    up
GigabitEthernet0/0/1.20192.168.2.2     YES manual up                    up
GigabitEthernet0/0/1.30192.168.3.3     YES manual up                    up
GigabitEthernet0/0/2   unassigned      YES unset  administratively down down
Vlan1                  unassigned      YES unset  administratively down down
Router#
Router#
```

Figure III.16: les interfaces inter VLAN

III.4.4 Configuration de Routeur6

a. Adressage IP d'une interface d'un routeur Cisco

Tableau III.4: La configuration IP choisie pour les interfaces Routeur6

Configuration / Interfaces / IP	Adresse IP	Masque de sous réseau
GigaEthernet 0/0/0	200.10.0.2	255.255.255.0
GigaEthernet 0/0/1	100.17.1.2	255.255.255.0
Serial 0/2/0	80.79.100.2	255.255.255.252

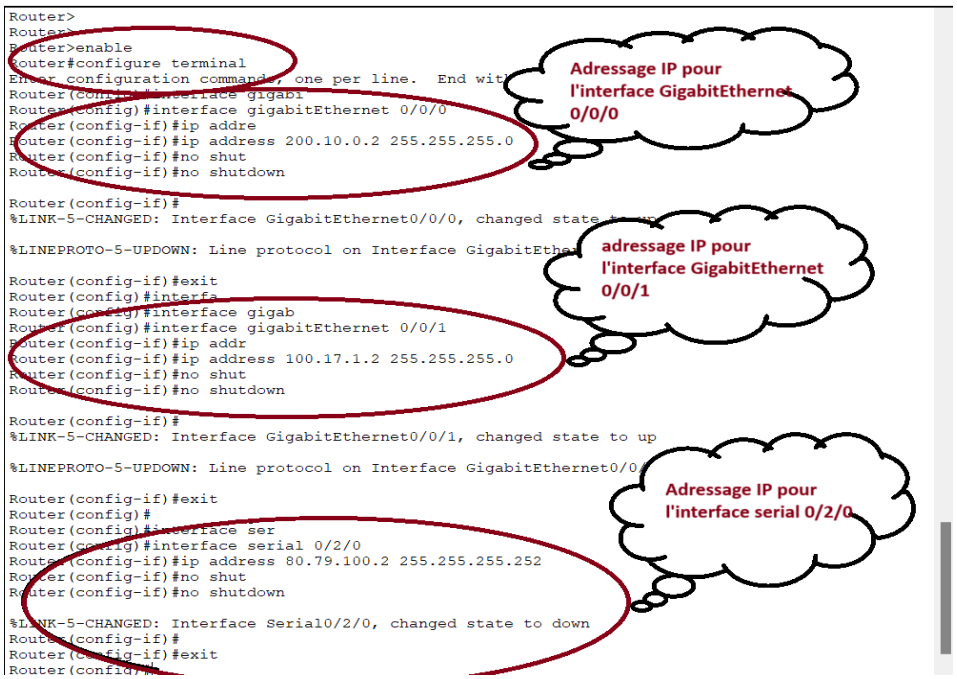

Figure III.17 : La configuration IP d'un Routeur6

b. Configuration de routage statique

Afin de relier les deux sites, il faut donner une route sur laquelle ils peuvent connecter entre eux. Donc on a configuré la route vers Routeur0.

```
Router(config)#
Router(config)#ip route 0.0.0.0 0.0.0.0 200.10.0.1
```

Figure III.18: Configuration de routage vers Routeur0

Et vers le routeur ISP :

```
Enter configuration commands, one per line.  End wit
Router(config)#ip route 0.0.0.0 0.0.0.0 80.79.100.1
Router(config)#exit
```

Figure III.19: Configuration de routage vers routeur ISP

c. Vérification de la connexion

PING de PC0 à Routeur0 (200.10.0.1) et à Routeur6 (200.10.0.2). On exécute :

```
C:\>ping 200.10.0.1

Pinging 200.10.0.1 with 32 bytes of data:

Reply from 200.10.0.1: bytes=32 time<1ms TTL=255
Reply from 200.10.0.1: bytes=32 time<1ms TTL=255
Reply from 200.10.0.1: bytes=32 time=1ms TTL=255
Reply from 200.10.0.1: bytes=32 time<1ms TTL=255

Ping statistics for 200.10.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 200.10.0.2

Pinging 200.10.0.2 with 32 bytes of data:

Reply from 200.10.0.2: bytes=32 time<1ms TTL=254
Reply from 200.10.0.2: bytes=32 time<1ms TTL=254
Reply from 200.10.0.2: bytes=32 time<1ms TTL=254
Reply from 200.10.0.2: bytes=32 time<1ms TTL=254

Ping statistics for 200.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure III.20 : PING de PC0 à Routeur0 et à Routeur6

Après un test de PING, nous pouvons confirmer que les deux routeurs peuvent communiquer.

III.5 Configuration de la DMZ

Au niveau de la simulation nous avons mise en place une zone DMZ constitué de plusieurs services :

1- Nat Overload.

2- WEB.

3- DNS.
4- MAIL.
5- FTP.

On va essayer de voir en détail ses services :

III.5.1 Implémentation de NAT (Routeur)

Grâce à cette configuration, plusieurs hôtes internes peuvent partager une adresse IP publique unique en traduisant leurs ports de source. La table NAT du routeur conserve la trace de ces traductions de ports [3].

La DMZ dispose d'une plage d'adresse publique. Pour que les postes du réseau LAN puissent se connecter à Internet il leur faut une adresse IP routable, Ce qui signifie l'utilisation d'un NAT dynamique (Overload).

```
Router(config)#
Router(config)#access-list 1 permit 192.168.4.0 0.0.0.255
Router(config)#ip nat inside source list 1 interface gigabi
Router(config)#ip nat inside source list 1 interface gigabitEthernet 0/0/0 overload
Router(config)#
Router(config)#interface giga
Router(config)#interface gigabitEthernet 0/0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#interface gigabit
Router(config)#interface gigabitEthernet 0/0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#
Router(config)#
Router(config)#
Router(config)#exit
```

adresse interne : 192.168.4.1

adresse externe : 200.10.0.1

Figure III.21 : Configuration NAT Overload

III.5.2 Configuration de service WEB (HTTP)

a. On entre dans « Desktop » ensuite « IP Configuration ».

b. On attribue l'adresse IP et le masque de sous réseau et DNS server.

c. On passe à l'onglet services après HTTP (déjà activé par défaut) puis on supprime langage HTML et on remplace par << Hi cisco website >>.

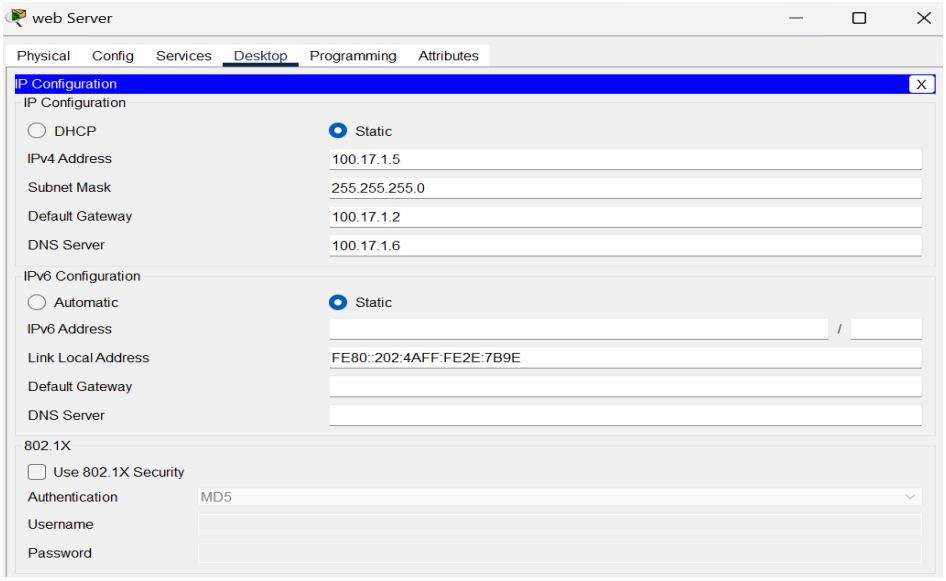

Figure III.22 : La configuration de serveur WEB

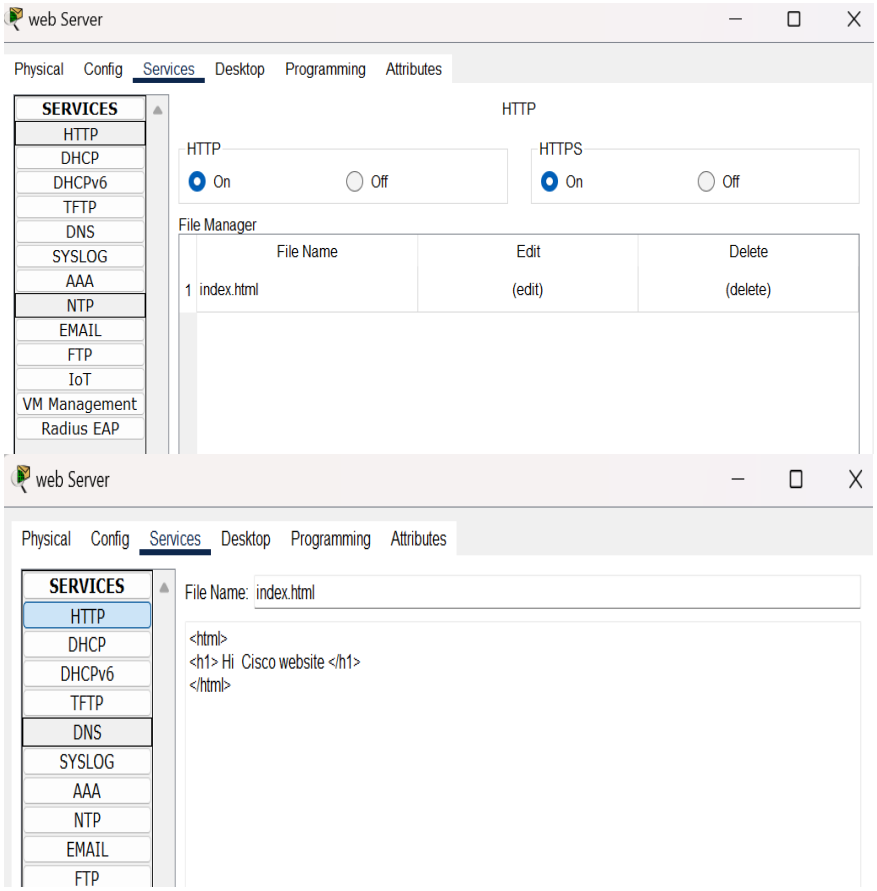

Figure III.23: Service HTTP

- **Résultats**

Test de connectivité

PING entre PC1(192.168.1.3) et le service WEB (100.17.1.5) :

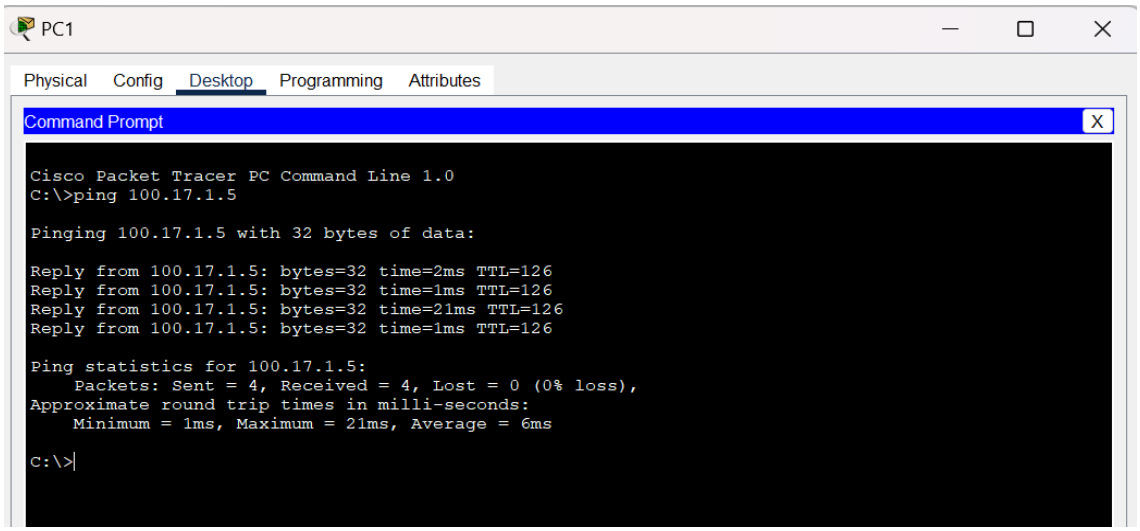

Figure III.24: Test PING

Test HTTP

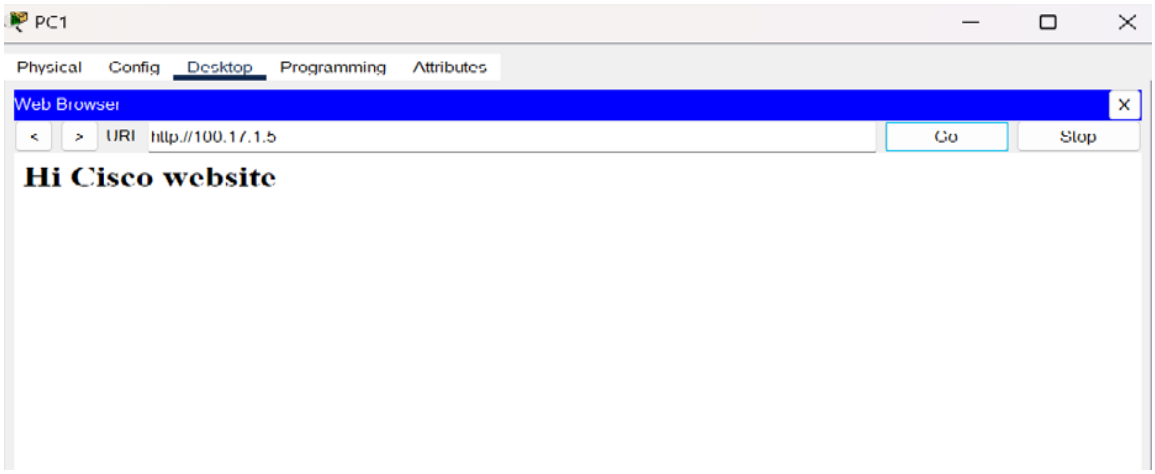

Figure III.25: Test HTTP

Selon les résultats, nous pouvons voir que les deux équipements peuvent communiquer.

III.5.3 Configuration de service DNS

a. On entre dans « Desktop » ensuite « IP Configuration ».

b. On attribue l'adresse IP et le masque de sous réseau et DNS server.

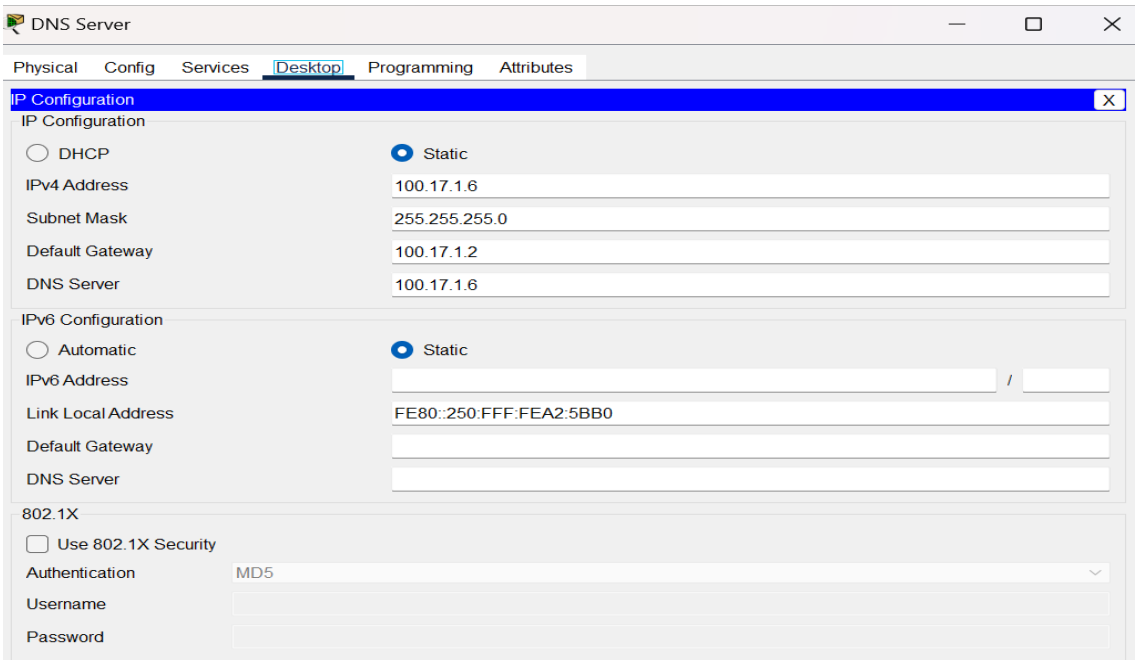

Figure III.26: La configuration de serveur DNS

c. On passe à l'onglet « services » après DNS.

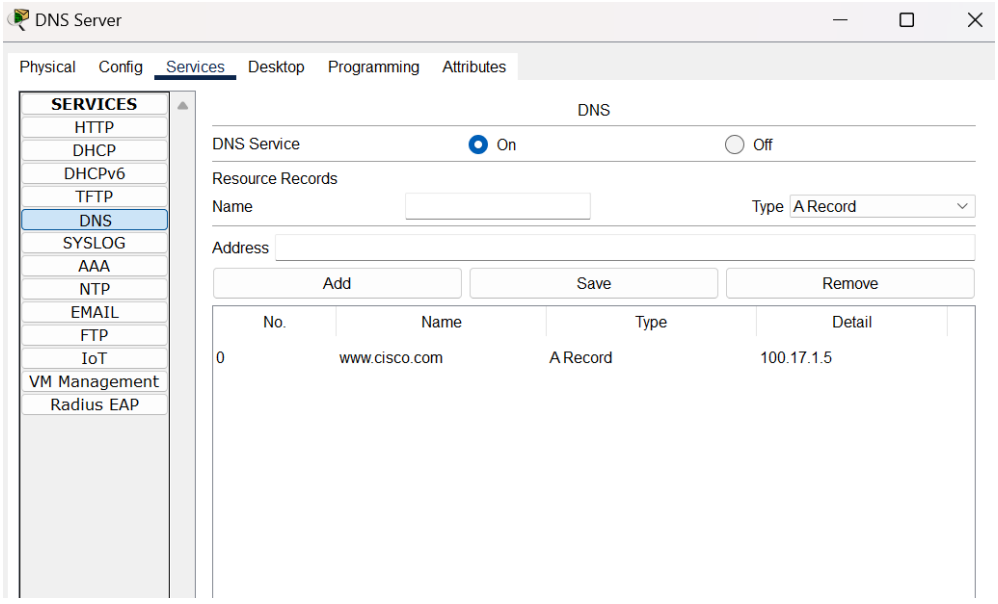

Figure III.27: Service DNS

- **Test de connectivité**

PING entre PC1 et le serveur DNS (100.17.1.6) :

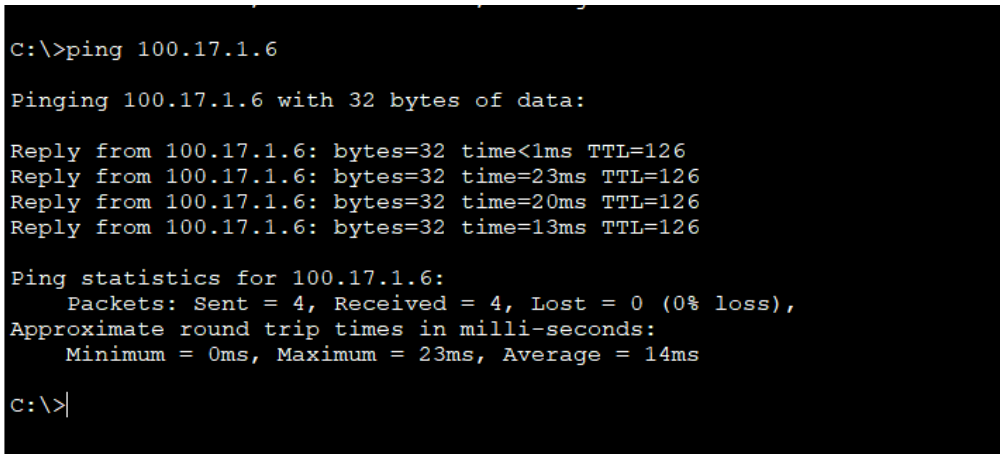

Figure III.28: Test PING

- **Résultats**

D'après les résultats, il est évident que les équipements ont la capacité de communiquer entre eux.

III.5.4 Configuration de service MAIL

a. On donne une adresse IP statique, le masque de sous réseau et DNS server.

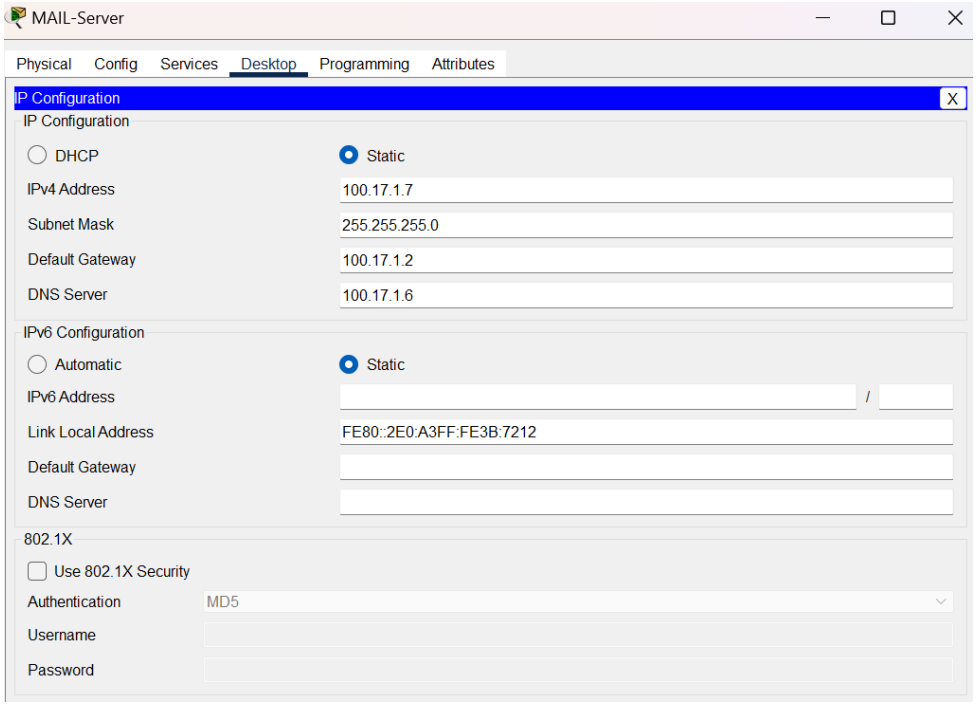

Figure III.29: La configuration d'un serveur MAIL

b. On configure le service EMAIL.

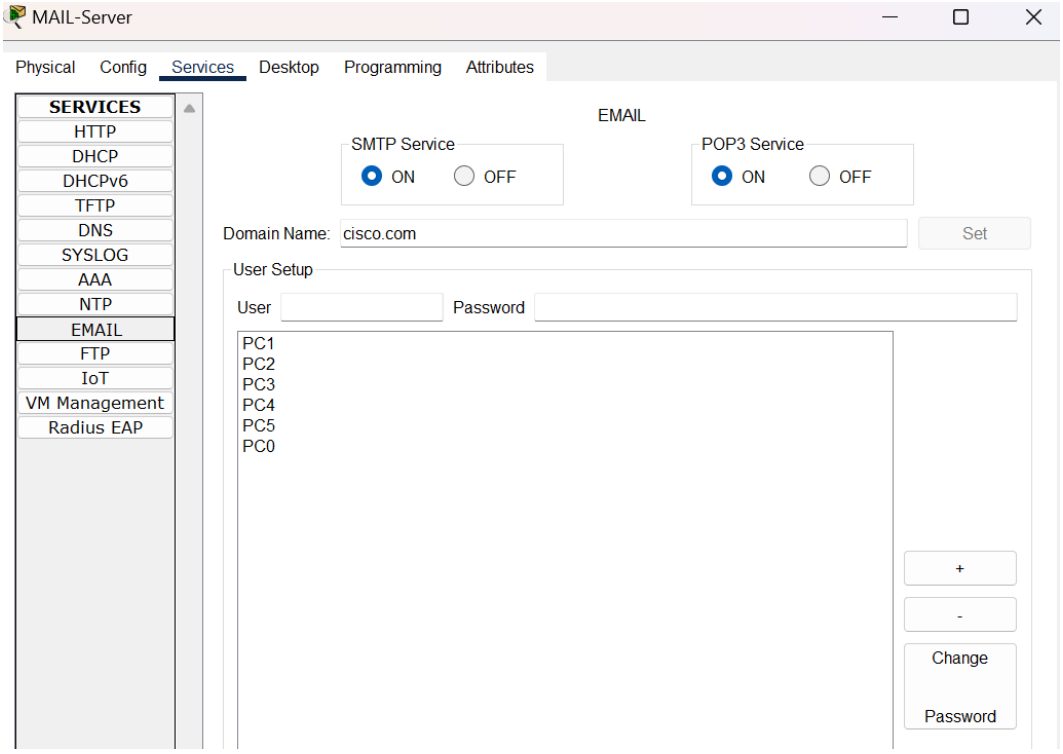

Figure III.30: La configuration d'un service MAIL

c. On configure le service MAIL pour le client PC1 (PC1@cisco.com).

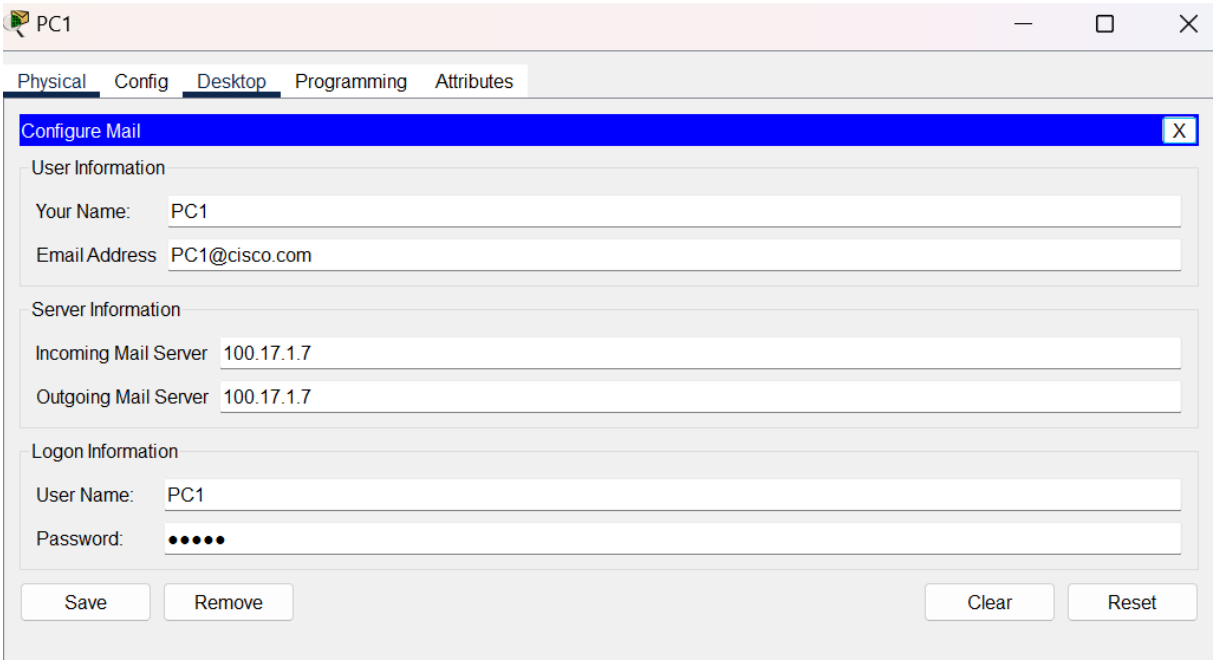

Figure III.31: La configuration MAIL pour PC1

Et PC0 (PC0@cisco.com).

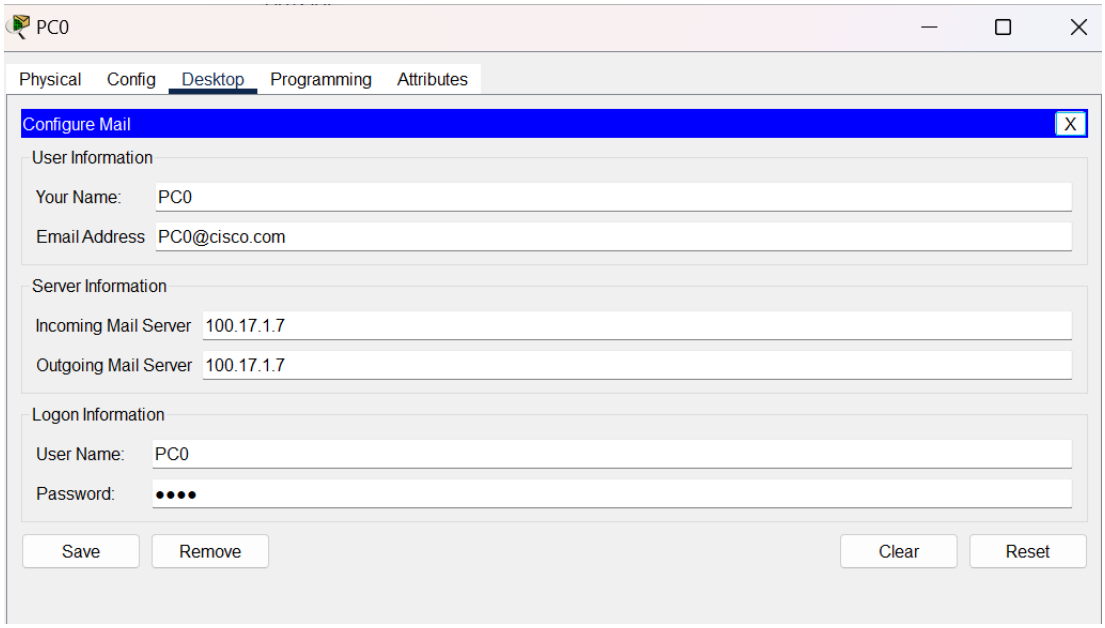

Figure III.32: La configuration MAIL pour PC0

- **Vérification de connectivité**

Pour ce test nous envoyons un email à partir de PC0 à PC1 la figure dessus :

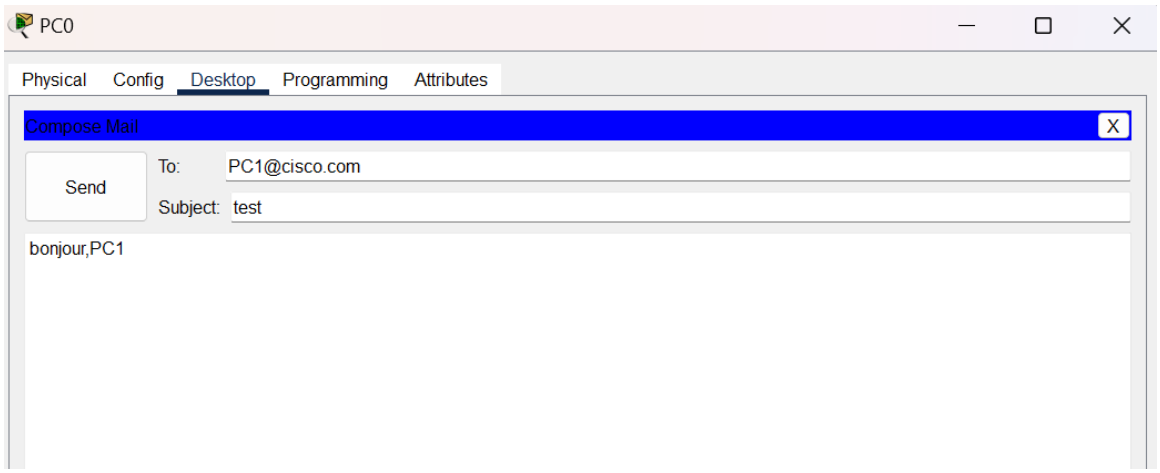

Figure III.33: Compose Mail par SMTP

Comme le montre la figure ci-dessous notre serveur de messagerie a bien fonctionné.

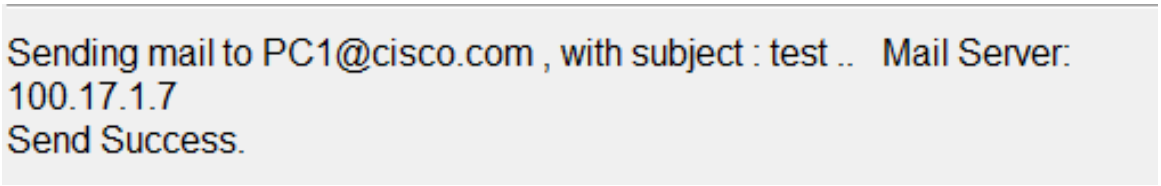

Figure III.34: Confirmation de l'envoi de l'email

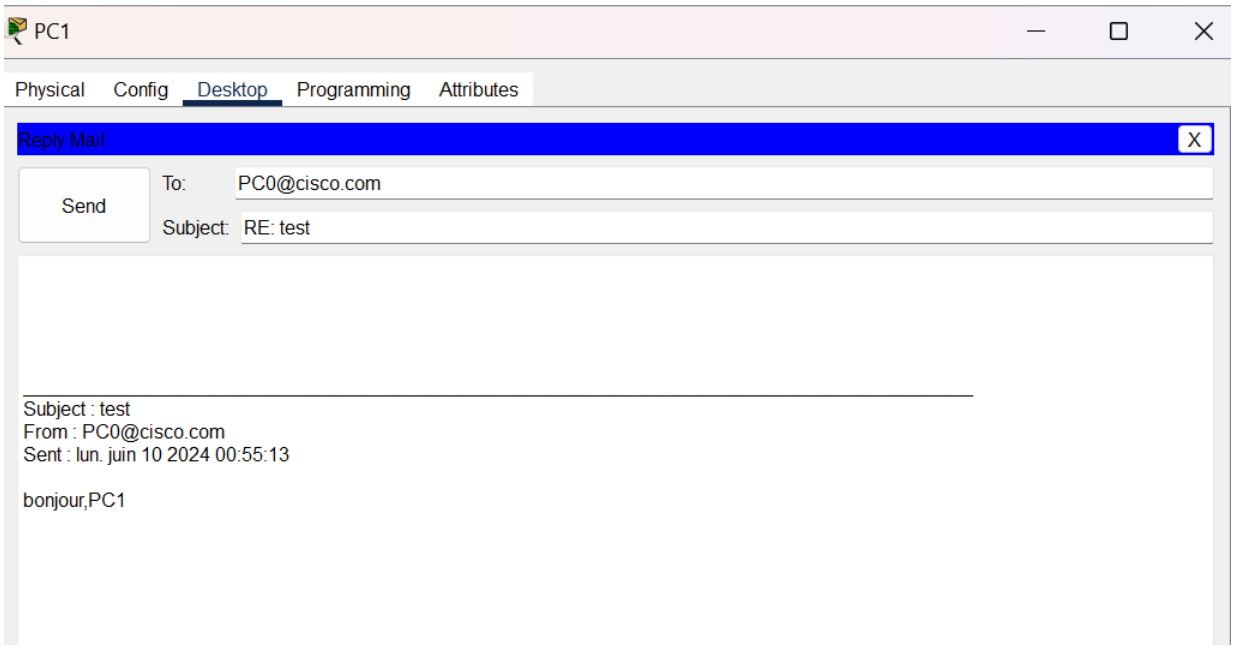

Figure III.35: Réception d'email par POP3

III.5.5 Configuration de service FTP

a. On donne une adresse IP et le masque de sous réseau.

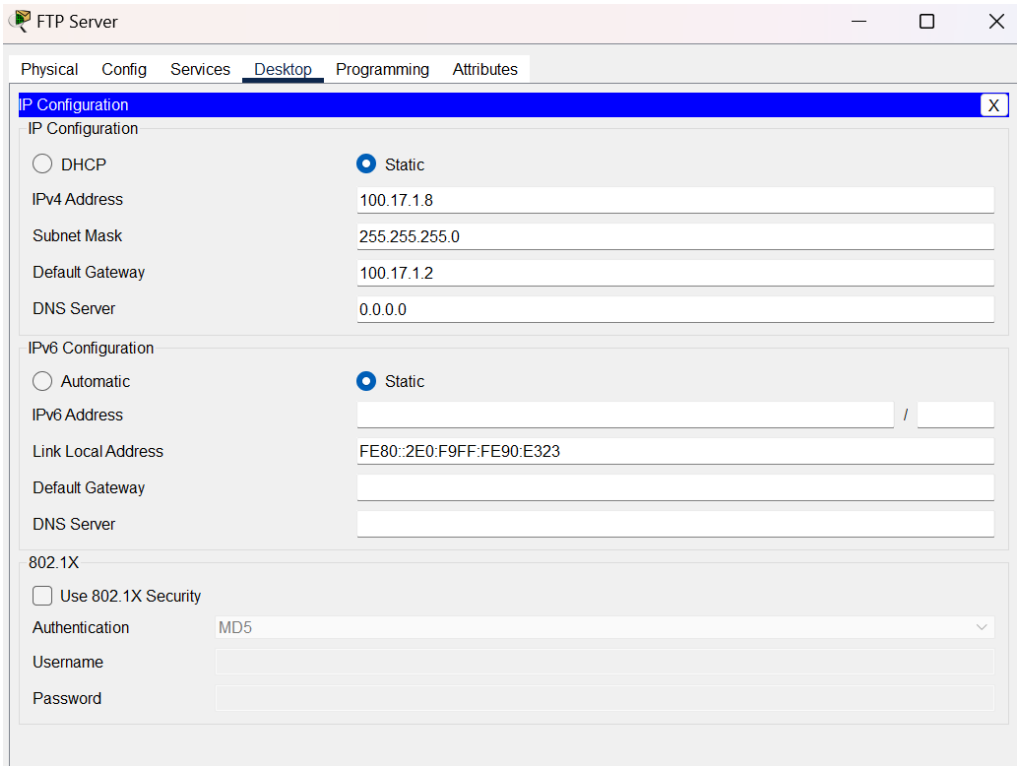

Figure III.36: La configuration d'un serveur FTP

b. On désactive tous les services sauf le service FTP.

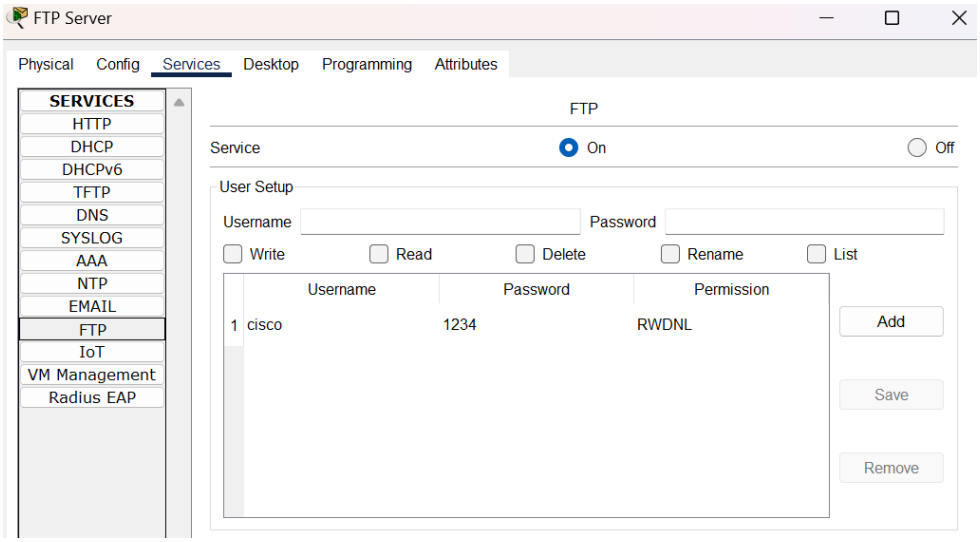

Figure III.37: Le service FTP

- **Test de connectivite**

PING : entre PC0 et le serveur FTP (100.17.1.8).

```
C:\>ping 100.17.1.8

Pinging 100.17.1.8 with 32 bytes of data:

Reply from 100.17.1.8: bytes=32 time<1ms TTL=126
Reply from 100.17.1.8: bytes=32 time=11ms TTL=126
Reply from 100.17.1.8: bytes=32 time=11ms TTL=126
Reply from 100.17.1.8: bytes=32 time=11ms TTL=126

Ping statistics for 100.17.1.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 11ms, Average = 8ms
```

Figure III.38: Test PING

Selon le test PING, les équipements peuvent communiquer entre eux.

Test FTP :

```
C:\>ftp 100.17.1.8
Trying to connect...100.17.1.8
Connected to 100.17.1.8
220- Welcome to PT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put hello.txt

Writing file hello.txt to 100.17.1.8:
File transfer in progress...

[Transfer complete - 6 bytes]

6 bytes copied in 0.021 secs (285 bytes/sec)
ftp>
```

Figure III.39: Test FTP de PC0

On va afficher les fichiers existants :

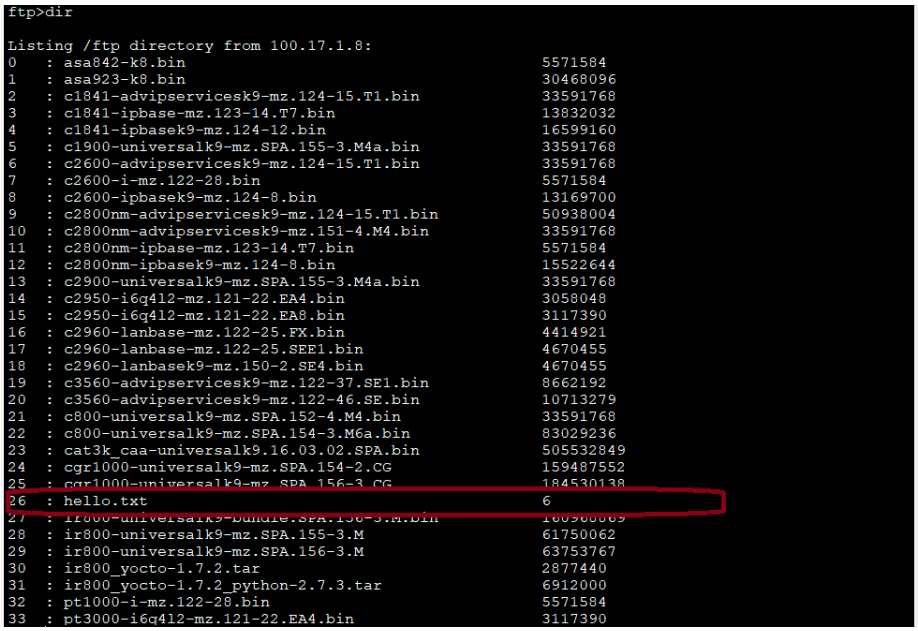

Figure III.40: Visualisation du fichier déposé

PING/test FTP : entre PC1 et le service FTP (100.17.1.8).

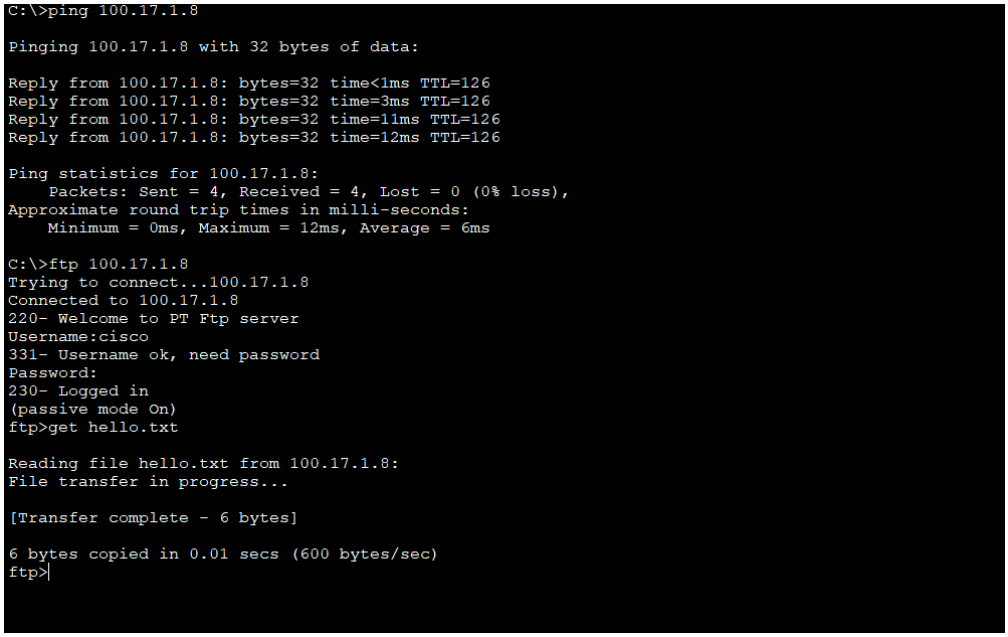

Figure III.41: Test PING et FTP

- **Résultats**

Nous pouvons dire alors que l'interconnexion entre eux est réussie.

III.6 La sécurité (FIREWALL)

III.6.1 ASA 5505

C'est un Dispositif de sécurité conçu pour les petites entreprises. Il fournit des capacités robustes de pare-feu, de VPN et plusieurs services réseaux dans un seul appareil facile à gérer. Ainsi, à chaque interface est associé un nom et un niveau de sécurité, qui déterminent les politiques de sécurité associées. Les niveaux de sécurité vont de 0 à 100. Le niveau de sécurité 100 (Inside) correspond à une confiance totale et un besoin accru de protéger ce réseau. Le niveau de sécurité 0 (Outside) le plus bas est généralement attribué aux interfaces les moins fiables, telles que celles reliées à Internet.

Figure III.42: ASA (Adaptative Security Appliance)

III.6.2 Configuration de ASA 5505

On attribue les adresses IP et niveau de sécurité de chaque interface en précisant la nature de l'interface Inside ou Outside. Pour l'Inside (DMZ), son niveau de sécurité est de 100 (pour donner le pouvoir d'accès) et l'Outside est de 0.

```
ciscoasa#configure terminal
ciscoasa(config)#interface vlan 1
ciscoasa(config-if)#ip address 100.17.1.4 255.255.255.0

ciscoasa(config-if)#nameif DMZ
ciscoasa(config-if)#security
ciscoasa(config-if)#security-level 100
ciscoasa(config-if)#exit
ciscoasa(config)#
ciscoasa(config)#
ciscoasa(config)#interface vlan 2
ciscoasa(config-if)#ip address 100.17.1.3 255.255.255.0
ciscoasa(config-if)#nameif OUTSIDE
ciscoasa(config-if)#secu
ciscoasa(config-if)#security-level 0
ciscoasa(config-if)#
ciscoasa(config-if)#exit
```

Figure III.43: La configuration de ASA

On utilise la commande << show run >> pour afficher les VLANs internes et externes de l'ASA et afficher les ports attribuer.

```
interface Vlan1
 nameif DMZ
 security-level 100
 ip address 100.17.1.4 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 100.17.1.3 255.255.255.0
!
```

Figure III.44: Les interfaces de l'ASA

On configure le protocole de routage pour permettre au réseau d'assurer la connexion.

```
ciscoasa#config ter
ciscoasa(config)#route outside 0.0.0.0 0.0.0.0 100.17.1.2 1
```

Figure III.45: Le routage statique

- **Test de connectivité**

PING vers le Routeur6 (100.17.1.3) pour confirmer la connexion :

```
ciscoasa#ping 100.17.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 100.17.1.2, timeout is 2 seconds:
!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms
```

Figure III.46: PING vers le Routeur6

III.7 Le routeur ISP (Internet Service Provider)

En français FAI (Fournisseur d'accès à Internet), C'est un équipement réseau de l'infrastructure d'un fournisseur de services Internet. Il offre une connexion Internet aux utilisateurs finaux, qu'ils soient des entreprises ou des particuliers.il est responsable de routage du trafic Internet entre le réseau local de l'utilisateur et le réseau global d'Internet.

La configuration de ISP

- On configure la liaison série vers Routeur6.

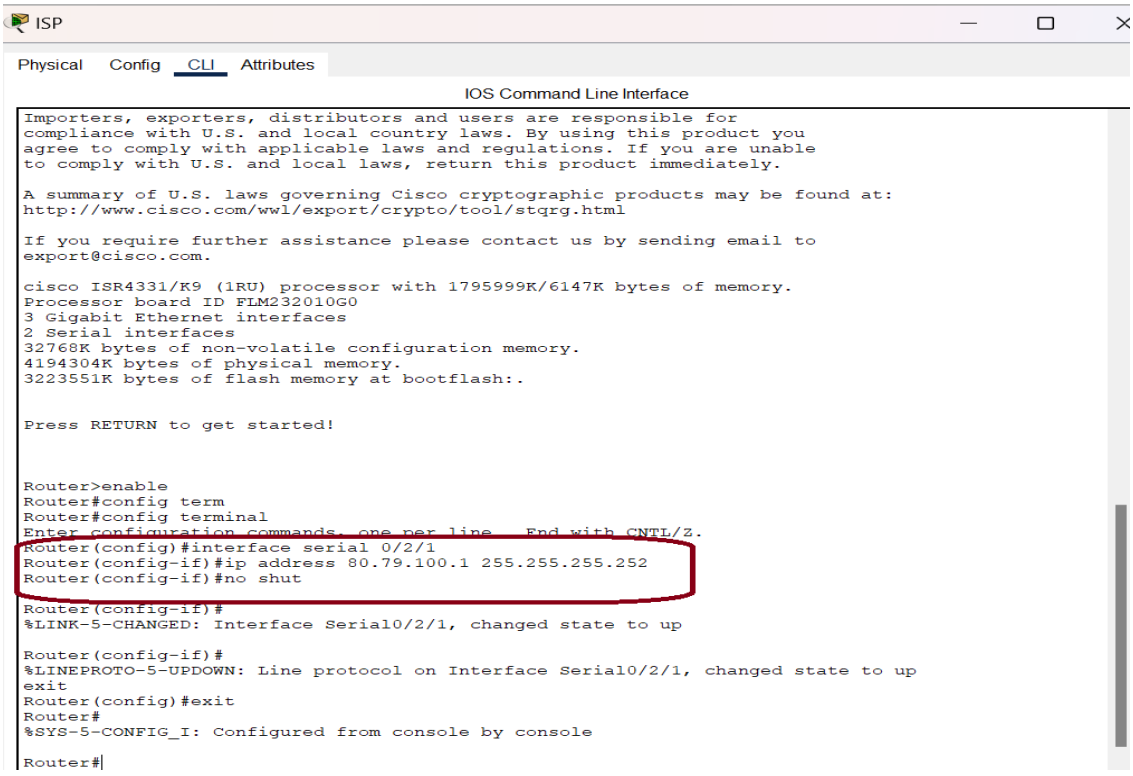

Figure III.47: La configuration du routeur ISP

- Pour émuler le réseau Internet on a utilisé un loopback dans le routeur ISP.

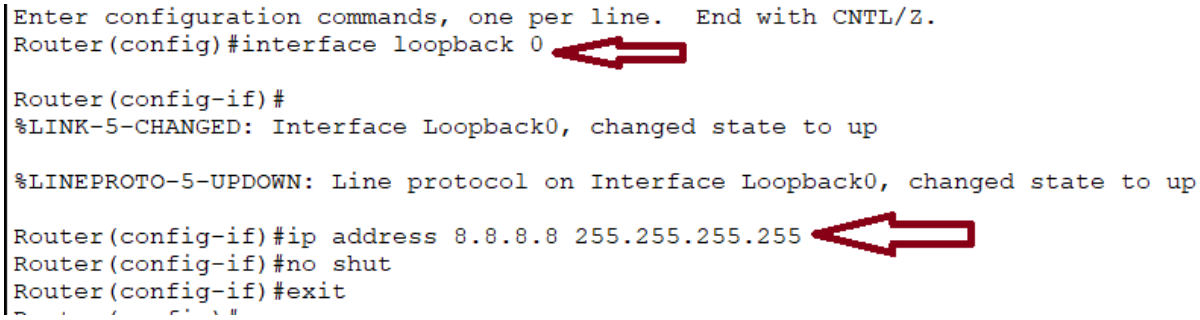

Figure III.48: La configuration de loopback

- On configure la route vers le routeur6.

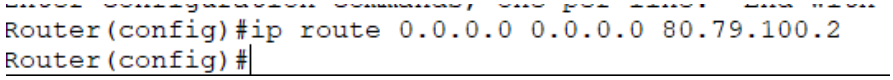

Figure III.49: Le routage vers Routeur6

Vérification

Pour confirmer le routage on fait un PING entre Routeur6 vers routeur ISP.

```
Router>ping 80.79.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 80.79.100.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms

Router>
```

Figure III.50: Test PING

III.8 Conclusion

Suite à la simulation effectuée, nous avons pu mettre en place quatre services sécurisés et une mise en œuvre d'une stratégie de sécurité en se basent sur le pare-feu ASA. Les résultats obtenus sous le logiciel Cisco Packet Tracer confirment la validité de l'étude et la connexion est bien établit.

Conclusion générale

Conclusion générale

La sécurité réseau est le domaine de la cybersécurité qui se concentre sur la protection des réseaux informatiques contre les cybermenaces. Il est primordial donc d'assurer la protection des données face aux attaques des cybercriminels.

Dans notre projet de fin d'étude, nous avons implémenté et testé une solution de sécurité complète pour l'entreprise via son implémentation sur le logiciel « Pcket Tracer ».

Ce travail nous a permis d'améliorer nos connaissances dans le domaine de la sécurité des réseaux notamment le pare feu « FIREWALL » ainsi son fonctionnement et son rôle dans la sécurité des réseaux d'entreprise. Il nous a également permis de découvrir le logiciel de simulation « Packet Tracer ».

Et ce à travers :

- La mise en place et la configuration d'une architecture d'entreprise sécurisée à base de pare-feu ASA, avec configurations et tests de connexion effectués sous le logiciel Cisco Packet Tracer.
- La mise en place le Network Address Translation (NAT) pour masquer les adresses IP internes et permettre une communication sécurisée avec l'extérieur.
- La mise en place d'une DMZ dans le logiciel.

La perspective principale est d'implémenter ce système dans un réseau réel.

Bibliographie

[1] Centre de ressources virtuel des Rivières du sud https://rivieresdusud.uasz.sn/handle/123456789/1432, 2021.

[2] Danièle Dromard & Dominique Seret. L'architecture des ré- seaux, collection synthex, 2éme édition. 2009.

[3] Les différents types de réseaux https://turgotlimoges.scenaricommunity.org/STI2D/2_TSTI2D/1_MEI/COURS_MEI/TD_IMPRIMANTE_web/co/Types_de_reseaux.html, 23 févr.2023.

[4] Lagraña Fernando. E-mail and Behavioral Changes: Uses and Misuses of Electronic Communications. Wiley-ISTE, 1ére édition, 2016.

[5] Groupe de travail du réseau R. Hinden https://www.ietf.org/rfc/rfc2374.txt?number=2374, juillet 1998.

[6] R. Morimoto & D. Présent. Réseaux et transmissions : Protocoles, infrastructures et services. Pearson Education, 2016.

[7] GitMind https://gitmind.com/fr/topologie-reseau.html, 17 novm.2022.

[8] Scribd https://fr.scribd.com/document/466220848/2-Topologies-des-reseaux-pdf, 19 juin.2020.

[9] Paesslar the monitoring experts https://www.paessler.com/fr/it-explained/server, 28 févr.2021.

[10] LeMagIT https://www.lemagit.fr/definition/Serveur-Web, août 2016.

[11] Comprendre la sauvegarde et la restauration des fichiers de configuration https://www.cisco.com/c/fr_ca/support/docs/ios-nx-os-software/ios-software-releases-122-mainline/46741-backup-config.html ,2 févr 2024.

[12] Routage inter VLAN : expliqué https://www.nwkings.com/inter-vlan-routing ,17oct 2023

[13] RÉSEAUX INFORMATIQUES https://www.universalis.fr/encyclopedie/reseaux-informatiques/4-interconnexion-de-reseaux/, 25 mars 2009.

[14] TCP/IP Les interconnexions de réseaux Compilation par Pierre-Alain Muller, Janvier 1996

[15] Z. HASNIA, B. YASMINE « Etude et Simulation d'une architecture réseau mixte sécurisée d'une Carte d'itinéraire IPSEC VPN et NAT » Mémoire de fin d'étude Systèmes des Télécommunications, Université Abdelhamid Ibn Badis de Mostaganem, 2019/2020.

[16] IUT Nice Côte d'Azur Réseaux LPSIL ADMIN https://webusers.i3s.unice.fr/~map/Cours/LPSILADMIN/UtilisationPacketTracer.pdf , 2012/2013

[17] Configuration De La Surcharge NAT Sur Un Routeur Cisco https://www.firewall.cx/cisco/cisco-routers/cisco-router-nat-overload.html, 2017