REPUBLIQUE ALGERIENNE DEMOCRATIQUçE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par

Fekir Ikhlas

Latreche Meriem

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Administration et sécurisation d'un réseau LAN

Soutenu le /09 /2020 devant le jury composé de:

Messaoudi	Nouredine	MCA	UMBB	Président
Merayhi	Yacin	MCA	UMBB	Examinateur
FELLAG	Sidali	Pr	UMBB	Rapporteur
BERRACHED	Facyl	ING	ATM MOBILIS	Membre invité

Année Universitaire : 2019/2020

Remerciement :

Nos remerciements s'adressent en premier lieu à l'éternel Dieu tout puissant de nous avoir accordé la capacité, le courage et la volonté afin de pouvoir réaliser ce travail.

Nous avons l'honneur et le plaisir de présenter notre remerciement à notre promotor **Mr FELLAG** pour ses orientations et ses conseils éclairés.

Au terme de ce travail, nous tenons à exprimer notre profonde gratitude et nos sincères remerciements à **M^{r} BERRACHED FACYAL** Ingénieur en réseaux et télécommunications nous avoir encadré pour le suivi théorique et pratique de ce projet, pour son appui, son aide précieux et sa patience durant toute la période de ce travail.

Au terme de ce travail, nous tenons à exprimer nos sincères gratitudes à nos familles.

Nous tenons à remercier infiniment les membres de jury d'avoir accepté d'examiner notre travail.

Nous exprimons nos reconnaissances à **Mr MASOUDI** Chef département réseaux et télécommunications, pour nous avoir acceptés entant que stagiaires au sein de son unité, et pour avoir mis à notre disposition les moyens nécessaires à ce travail.

Nos plus sincères remerciements s'adressent à toute l'équipe de laboratoire pour leurs accueils chaleureux, leurs gentillesses et leurs sympathies.

Notre gratitude s'adresse également à tous nos amis pour leurs précieuses disponibilités et pour les années inoubliables que nous avons passés ensemble et surtout pour le temps et la patience qu'ils nous ont volontiers consacré à la réalisation de ce mémoire.

Nous tenons à remercier également tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Dédécace

Je dédie ce travail de fin d'étude à:

Mes chers parents, ma raison d'être, pour leurs encouragements, leurs sacrifice set tout l'aide qu'ils m'ont apportée durant mes études, et sans leurs soutiens je ne serais pas arrivé à ce que je suis, que dieu les protège;

Mes sœurs Imane et nada , et mes frères Kamal et Bachir qui ont été toujours à mes côtés, pour leurs soutiens moral, et leurs encouragements ;

Ma chère binôme meriem, pour sa patience et sa compréhension tout au long de ce projet,

Mes chers amis et tous ceux qui m'ont aidé de prés ou de loin à la réalisation de ce travail,

Tous ceux qui me sont chers.

Dédécace

Je dédie ce modeste travail qui n'aura jamais pu voir le jour sans le soutiens indéfectible et sans limite de mes chers parents qui ne cessent de me donner avec amour le nécessaire pour que je puisse arriver à ce que je suis aujourd'hui que dieu vous protège et que la réussite soit toujours à ma portée pour que je puisse vous combler de bonheur.

Je dédie aussi ce travail à :

- *mes chers frères mouhamed et sofiane et sœur sihem et amel qui m'ont encouragé et soutenu durant tout mon cursus.Je vous aime énormément.*
- *mon cher binôme à ikhlas qui je souhaite un avenir radieux plein de réussite.*
- *tous mes amis, mes collègues et tous ceux qui m'estiment.*

Sommaire

Sommaire

Table des matières

Sommaire

Partie II : Sécurité des réseaux locaux (informatique)

Sommaire

Sommaire

Chapitre IV: Réalisation

Liste des tableaux

Listes des figures

Liste des tableaux

Liste des tableaux

Liste des abréviations

Liste des abréviations :

A

ACK ACKnowledgment (Acquittement)

ACL Access Control List

ARP Adresse Resolution Protocol

B

BOOTP Bootstrap Protocol

C

CFI Canonical Format Identifier

D

DHCP Domain Host Configuration Protocol

DMZ Délimitarised Zone

DNS Domain Name System

E

EBCDIC Extended binary coded decimal interchange code

F

FDDI Fiber Distributed Data Interface

FTP File Transfer Protocol

Fw firewall

G

GIF Graphics interchange format

H

Host-ID Host Identification.

HTTP HyperText Transfer Protocol

HTTPS HyperText Transfer Protocol Secure sockets

I

ICMP Internet Control Message Protocol

ICMPV4 Internet Control Message Protocol version 4

Liste des abréviations

ICMPV6 Internet Control Message Protocol version 6

IGMP Internet Group Management Protocol

IETF Internet Engineering Task Force

IMAP Internet Message Access Protocol.

IP Internet Protocol

IPSec Internet Protocole Sécurité

IPv4 Internet Protocole Version 4

IPv6 Internet Protocole Version 6

IPX Internet work Packet Exchange

ISL Inter Switch Link Protocol

J

JPEG Joint Photographic Experts Group.

L

LAN Local Area Network

LLC Logical Link Layer

M

MAC Medium Access Layer

MAN Métropolitain Area Network

MAU *Multistation Access Unit*

MDA Mail Delivery Agent.

MIDI Musical instrument digital interface

MPEG transport stream

MTA Mail Transport Agent.

MUA Mail User Agent.

N

Net-ID Network Identification.

NFS Network File System

O

OSI Open Systems Interconnection

Liste des abréviations

P

PAN Personale Area Network

PC Personnel Computer

POP Post Office Protocol

Ppp point-to-point protocol

POS Personal Operating Space

R

RPC Remote procedure call.

S

SA association de sécurité

SADB association de sécurité de base de donne

SMTP Simple Mail Transport Protocol

SPX Sequenced packet eXchange

SQL Sigle de structured query language

STP Shielde Twisted Paire

SYN Numéro de Séquence

T

TCI Tag Control Information

TCP Transmission Control Protocol

Telnet TELE communication NET work

TFTP Trivial file transfer protocol

TIFF Tagged image file format

TLS Transport Layer Security

TCP Transmission Control Protocol

TPID Tag Protocol Identifier

U

UDP User Datagram Protocol

V

VID VLAN ID

Liste des abréviations

VLAN Virtual Local Area Network

VPN Virtual Private Network

VTP Vlan Truking Protocol

W

WAN Wide Area Network

WWW World Wide Web

Résumé

L'ouverture des systèmes informatiques des entreprises engendre plusieurs problèmes de sécurité, de ce fait la présence d'une politique qui protège les données du réseau local contre les menaces qui provient soit de l'intérieur soit de l'extérieur est devenue indispensable.
Notre travail consiste à définir quelque technique de sécurité telle que les VLANs, les VPNs, la DMZ et le pare-feu. Après la localisation des problèmes de sécurité dans l'entreprise
ATM mobilis nous avons proposé une architecture dont laquelle on va exploiter les techniques de sécurité citées.
Pour mettre notre solution en pratique nous avons utilisé le
Simulateur packet tracer qui offre la possibilité d'implémenter des machines virtuelles d'où être prêt de réseau physique.

Abstract
The opening of the information processing systems of the companies generates several Problems of safety, on this fact the presence of a policy which protects the data of the local area network against the threats which come either from the interior or of outside became essential.
Our work consists of defining some technics of safety such as VLANs, VPNs, DMZ and the firewall. After the localization of the problems of safety in the company of AM mobilis we propose an architecture on which one will exploit the quoted technics of safety. To put our Solution on the real seedling we use the simulator packet tracer which makes it possible to implement Virtual machines from where to be ready of physical network.

Introduction générale

Introduction générale

L'information était toujours un élément essentiel durant l'évolution de l'humanité. En effet, une meilleure gestion de toute activité (économique, social, politique, militaire,..) dépend essentiellement d'une meilleure maitrise de l'information. Etant un facteur précieux et surtout sensible, le besoin de sa disponibilité et de sa fiabilité en tout lieux et à tout moment est devenue une obsession face au défit du monde moderne [54].

Afin de satisfaire ces besoins et autres, l'Homme a eu recours a l'outil informatique, en inventant les réseaux qui ont pour but de garantir une meilleure circulation de l'information. L'univers des systèmes d'information compose de réseau et de systèmes informatiques prend un rôle et une place chaque jour plus important dans les entreprises [54].

A l'heure actuelle, les entreprises doivent faire face à un nombre croissant d'utilisateurs, cela est du à leurs extensions et/ou à la forte demande de ses services ou produits, engendrant un besoin d'accès à leurs informations, ou que résident celles-ci et quelles que soit les méthodes pour récupérer ces informations, satisfaisant une liaison sécurisée, fiable et un prix faible [54].

En effet la mobilité étant un argument dans le monde professionnel, il est nécessaire de pouvoir travailler pour son entreprise à n'importe quel endroit du monde. Pour cause de sécurité les informations indispensables à une entreprise ne peuvent pas être stockées sur un serveur accessible publiquement depuis Internet, elles ne sont donc théoriquement pas accessibles depuis un réseau extérieur à celui de l'entreprise.

Ce mémoire s'articule autour de quatre chapitres : Le premier chapitre présente l'entreprise ATM Mobilis, qui est devenu le premier opérateur mobile en Algérie.

Le deuxième chapitre intitulé " Généralités sur les réseaux et la sécurité des réseaux locaux", nous allons entamer la définition des techniques de sécurité, les protocoles utilisés dans chacune de ces techniques en détaillant les protocoles utilisés dans la phase de la réalisation.

En troisième chapitre présente Les VLANS et la sécurité des VLANs nous définirons en premier lieu ce qu'est un réseau virtuel, ensuite nous parlerons de son fonctionnement et de ses objectifs. Nous finirons par citer les différents protocoles de mise en place, principalement VTP, sa compréhension nous aidera dans la réalisation.

En dernier lieu, le quatrième chapitre présente l'évaluation de l'expérimentation et les résultats obtenus.

Chapitre I :

Présentation de l’entreprise

CHAPITRE I : présentation de l'entreprise

I .1L'introduction générale de l'organisme d'accueil :

A propos d'ATM Mobilis :

Filiale d'Algérie Télécom, Mobilis est le premier opérateur mobile en Algérie, devenu autonome en août 2003.

Depuis sa création, Mobilis s'est fixé des objectifs principaux qui sont :la satisfaction client, la fidélisation client, l'innovation et le progrès technologique, qu'ils lui ont permis de faire des profits et d'acquérir près de 10 million d'abonnés en un temps record.

Optant pour une politique de changement et d'innovation, Mobilis travaille en permanence sur son image de marque et veille constamment à offrir le meilleur à ses clients.

En déployant un réseau de haute qualité, en assurant un service client satisfaisant, et en créant des produits et services innovants, Mobilis est positionné comme étant un opérateur proche de ses partenaires et de ses clients, renforcé par sa signature institutionnelle : « partout avec vous ». Son slogan est une promesse d'écoute et un signe de son engagement à assumer son rôle dans le développement durable grâce à sa participation dans le progrès économique, son respect de la diversité culturelle, son engagement d'assumer son rôle social et sa participation à la protection de l'environnement.

Se munissant des valeurs : Transparence, Loyauté, Dynamisme et Innovation. Mobilis optimise sa qualité de service et veille à fidéliser ses clients.

Mobilis c'est aussi :

- Une couverture réseau totale de la population.
- Un réseau commercial en progression atteignant ainsi les 143 agences Mobilis.
- Plus de 60.000 points de vente indirecte.
- De plus de 4500 stations de base radio (BTS).

Plateformes de service des plus performantes.

I .2 Historique et présentation de l'organisme d'accueil :

Mobilis, filiale d'Algérie Télécom, est le premier opérateur de téléphonie mobile en Algérie. Devenu autonome en août 2003, elle subit une réorganisation en juin 2004 et une deuxième réorganisation en 2006 ou on voit la naissance des divisions.

L'organisation d'ATM Mobilis s'est renforcée avec la création du poste de divisionnaire principale en 2010.

En décembre 2004 Mobilis a lancé le premier réseau de UMTS (Universel Mobile Télécommunication Système) en Algérie intégrant ainsi le club des quarante opérateurs dans le monde qui maîtrisent cette technologie. Devenu un véritable opérateur multimédia en Algérie, il propose à ces clients une large gamme de produits et de services innovants et de haute qualité.

Mobilis propose à ses clients une large gamme de produits et de services de haute qualité « offre post et prépayées vers tous les opérateurs en Algérie à l'étranger ».

I .3 Les services Mobilis :

Mobilis offre a ses clients post et prépayés une large gamme de service :

- Consultation de la facture sur internet.
- MMS : envoi et réception de photos, fichiers musicaux.
- Un portail Wap.
- Notification gratuite du solde après chaque appel*
- SMS vers tous les opérateurs en Algérie et à l'étranger.
- Roaming à l'international.
- Messagerie vocal.
- Tarification des appels à la seconde après la première minute.
- Double appel…

I .4Les produits Mobilis :

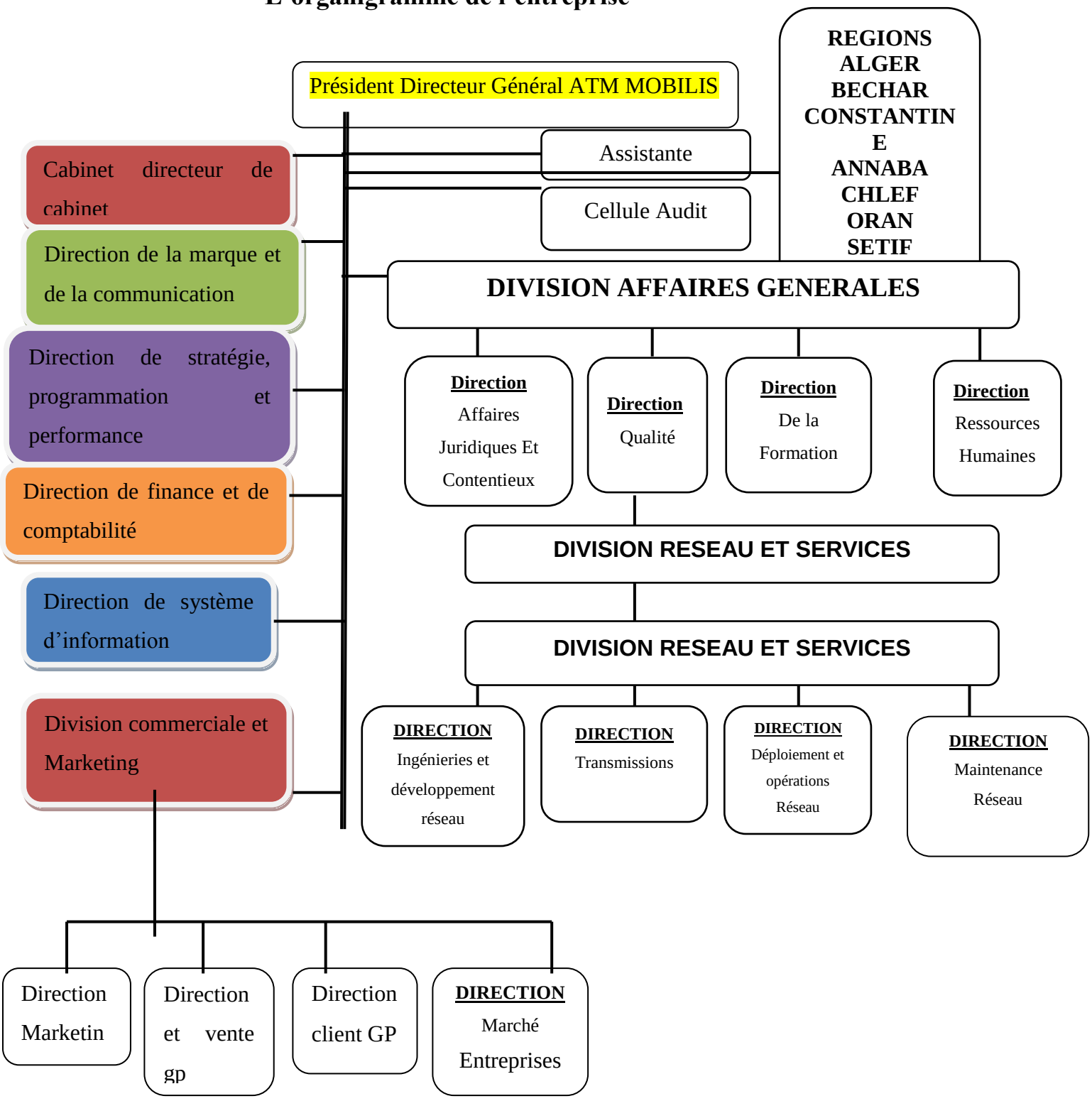
Cinq produits phares adaptés à tous les budgets et à tous les usages :

- L'offre « Mobilis, la carte, Mobiposte, Mobilight ».
- L'offre « Forfait ».
- L'offre « Résidentiel ».
- L'offre « Flotte ».
- L'offre « Mobi+» (**GPRS-MMS**).

I .5 Les ambitions de Mobilis :

- Reprendre rapidement ses parts de marché.
- S'inscrire à l'avant –garde de l'innovation.
- Développer l'expertise et la performance.
- Etre constamment compétitif (qualité, prix, et services).
- Générer des profits et de la croissance.
- Participer au développement national.

L'organigramme de l'entreprise



Chapitre II :
Généralité sur les réseaux et la sécurité des réseaux locaux

CHAPITRE II : Généralités sur les réseaux et la sécurité des réseaux locaux

Introduction

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants et favoriser ainsi l'échange de données qui au fil du temps ces derniers, sont devenues de plus en plus sensibles aux attaques (piratage …etc).

Ce chapitre est scindé en deux parties : la première partie décrira quelques notions sur les réseaux informatiques, tan disque la deuxième sera consacrée à leur sécurité.

Partie I : Réseaux informatiques

I.1.Définition d'un réseau [2]

Un réseau informatique est un ensemble d'éléments, matériels et logiciels reliés entre eux pour permettre aux utilisateurs de partager des ressources et d'échanger des données sous format numérique.

Un réseau a pour fonction de transporter les données d'une machine terminale vers une autre machine terminale. Pour ce faire, une série d'équipements et de processus sont nécessaires, allant de l'environnement matériel, utilisant des câbles terrestres ou des ondes radio, jusqu'à l'environnement logiciel constitué de protocoles, c'est-à-dire de règles permettant de décider de la façon de traiter les données transportées.

I.2 Définition d'un réseau informatique [47]

Un réseau informatique est un réseau dont chaque nœud est un système informatique autonome, ces nœuds sont reliés par des supports matériels (Switch, routeurs ….) et logiciels (protocoles), et ont aussi la possibilité de communiquer entre eux directement ou indirectement. En pratique, deux ordinateurs suffisent pour constituer un réseau informatique. La fig.1.1 montre un exemple d'un réseau.

Figure1.1 : exemple d'un réseau.

I.3 Types des réseaux informatiques [1, 48,49]

Suivant la distance qui sépare les hôtes et selon la taille de réseau, ainsi que la vitesse de transfert des données, on distingue quatre type de réseaux :

- **Réseau personnels ou PAN (Personale Area Network)**

La plus petite étendue de réseau est nommée en anglais Personal Area Network (PAN), Centrée sur l'utilisateur, elle désigne une interconnexion d'équipements informatiques dans un espace d'une dizaine de mètres autour de celui-ci, le Personal Operating Space (POS). Deux autres appellations de ce type de réseau sont : réseau individuel et réseau domestique.

- **Réseau local ou LAN (Local Area Network)**

Il s'agit d'un ensemble d'ordinateurs, appartenant à une même organisation et, reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet).

La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10 Mbit/s et 1Gbit/s [49].

La taille d'un réseau local peut atteindre jusqu'à 100, voire 1000 utilisateurs [49].

- **Réseau métropolitain ou MAN (Metropolitan Area Network)**

Interconnecte plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants, supérieur à 100 Mbits/s. Ainsi un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

- **Réseau étendu ou WAN (Wide Area Network)**

Interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un nœud du réseau. Le plus connu des WAN est internet.

La figure 1.2 montre la topologie des réseaux.

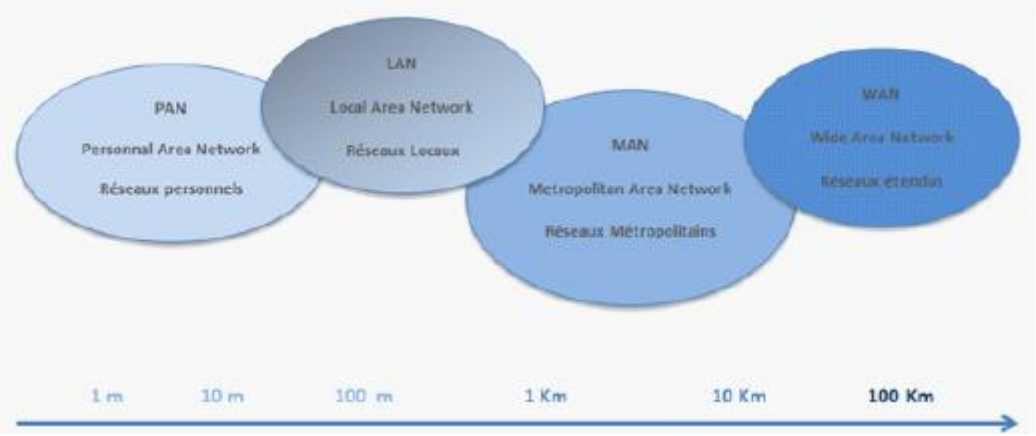


Figure 1.2 : la typologie des réseaux [1].

I.4 Architectures des réseaux informatiques [3, 4,53]

Le type d'architecture de réseau à installer dépend des critères suivants:

– Taille de l'entreprise.

– Niveau de sécurité nécessaire.

– Type d'activité.

– Niveau de compétence d'administration disponible.

On distingue généralement deux types d'architecture de réseaux bien différents, ayant tout de même des similitudes :

I.4.1 Les réseaux poste à poste (Peer to Peer/ égal à égal) :

Les réseaux poste à poste ne comportent en général que peu de postes, moins d'une dizaine de postes, parce que chaque utilisateur fait office d'administrateur de sa propre machine, il n'y a pas d'administrateur central, ni de super utilisateur, ni de hiérarchie entre les postes, ni entre les utilisateurs.

I.4.2 Les réseaux organisés autour de serveurs (client/serveur):

Les réseaux client/serveur comportent, en général, plus de dix postes. La plupart des stations sont des "postes clients". C'est-à-dire des ordinateurs dont se servent les utilisateurs, les autres stations sont dédiées à une ou plusieurs tâches spécialisées, on dit alors qu'ils sont des serveur.

La figure 1.3 montre l'architecture des réseaux.

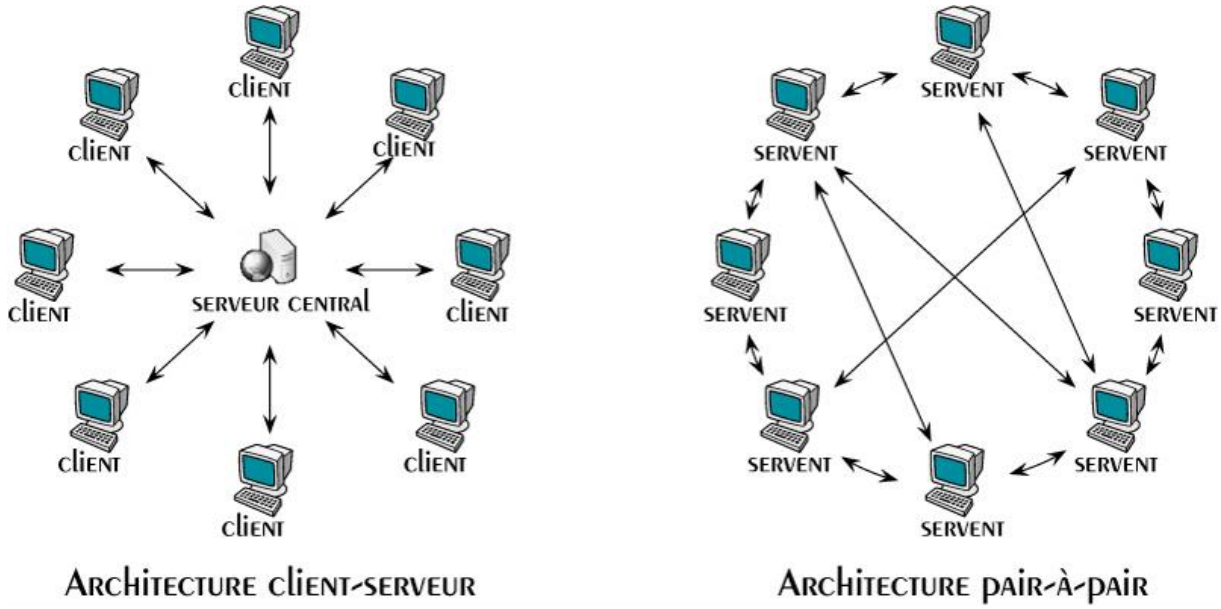


Figure 1.3 :Architecture des reseaux [53].

I.5 Adressage dans les réseaux informatiques [5, 6,50]

I.5.1 Plages d'adressages

I.5.1.1 Définition d'une adresse IP :

L'adresse IP est une adresse de 32 bits, répartie en 4 fois 8 bits (octet). Cette adresse est un identifiant réseau. On peut ensuite, la diviser en 2 portions : la portion du réseau et la portion hôte. La première identifie le réseau sur lequel est la machine et la deuxième identifie les machines en elles-mêmes. Pour identifier ces deux parties chaque adresse est liée à un masque de sous-réseau ce qui permet de définir sur quel réseau elle se trouve.

Le format binaire d'une adresse IP est comme suit :

xxxxxxxx . xxxxxxxx .xxxxxxxx. xxxxxxxx (tel que x=0 ou x=1).

I.5.1.2Les classes des adresses IP :

Le but de la division des adresses IP en classes, est de faciliter la recherche d'un ordinateur sur le réseau. En effet, avec cette notation il est possible de rechercher dans un premier temps le réseau à atteindre puis de chercher un ordinateur sur celui-ci. Ainsi, l'attribution des adresses IP se fait selon la taille du réseau.

En effet, il existe 5 classes des adresses IP, à savoir : classe A, classe B, classe C, classe D et classe E, telles que, chaque classe a un format spécial de son adresse IP. « Adresse réseau et adresse machine ».

Classe A :

Le premier octet est utilisé pour l'adresse *Net-ID*[5], il varie de 1 à 126. Les deuxième, troisième et quatrième octets sont utilisés pour le *Host-ID*[6].

Une adresse de classe A a la forme : R1 .m1 .m2 .m3 (R : Net-ID, m : Host-ID)

Bits de R1 : 0xxxxxxx ou X=0 ou X=1 00000000<=R1<= 01111111

0<=R1<=127 0<=mi<=255

Classe B :

Les premiers et deuxièmes octets sont utilisés pour l'adresse Net-ID, ils varient de 128.0 à 191.255. Les troisièmes et quatrièmes octets sont utilisés pour les adresses Host-ID.

L'adresse de cette classe est comme suit : R1 .R2 .m1 .m2

Bits de R1 : 10xxxxxx ou X=0 ou X=1 10000000<=R1<= 10111111

128<=R1<=191 0<=mi<=255

Classe C :

Les premiers, deuxièmes et troisièmes octets sont utilisés pour l'adresse Net-ID, ils varient de 192.0.0 à 223.255.255. Le quatrième est utilisé pour l'adresse Host-ID.

L'adresse IP de classe C a le format : R1 .R2 .R3 .m1

Bits de R1 : 110xxxxx ou X=0 ou X=1 11000000<=R1<= 11011111

192<=R1<=223 0<=m1<=255

Classe D :

La classe D est ce qu'on appelle Multicast, c'est-à-dire qu'elle est destinée à faire de la diffusion d'information sur plusieurs Hôtes (groupe d'Hôtes) simultanément. Le premier octet a une valeur comprise entre :

224= (11100000) et 239=(11101111).

Classe E :

La classe E n'est pas utilisée pour adresser des hôtes ou des groupes d'Hôtes. Le premier octet a une valeur comprise entre :

240= (11110000) et 255=(11111111).

La figure 1.4 éclaircie les différentes caractéristiques des classes d'adresses IP.

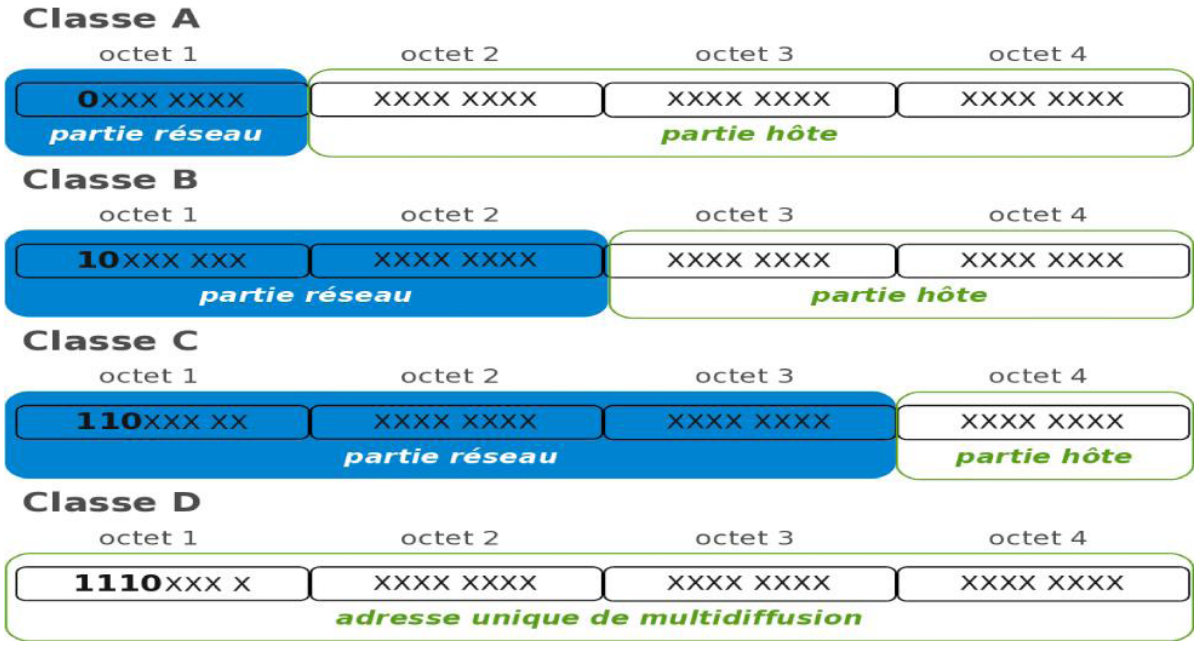


Figure 1.4 : Caractéristiques des classes des adresses IP [5].

I.5.2 Serveur DNS (Domain Name System)

Un serveur DNS est un annuaire pour ordinateur. Lorsque vous voulez accéder à un ordinateur dans le réseau, votre ordinateur va interroger le serveur DNS pour récupérer l'adresse de l'ordinateur que vous voulez joindre. Une fois, que votre ordinateur aura récupéré l'adresse du destinataire, il pourra le joindre directement avec son adresse IP.
le serveur DNS va permettre de faire la relation entre nom d'ordinateur et adresse IP.

I.5.3 Serveur DHCP (Domain Host Configuration Protocol)

DHCP signifie Dynamic Host Configuration Protocol. Il s'agit d'un protocole qui permet à un ordinateur qui se connecte sur un réseau local d'obtenir dynamiquement (c'est-à-dire sans intervention particulière) sa configuration (principalement sa configuration réseau). Vous n'avez qu'à spécifier à l'ordinateur de trouver une adresse IP tout seul par DHCP. Le but principal étant la simplification de l'administration d'un réseau.

Le protocole DHCP sert principalement à distribuer des adresses IP sur un réseau, mais il a été conçu au départ comme complément au protocole BOOTP (Bootstrap Protocol)[50] qui est utilisé par exemple lorsque on installe une machine à travers un réseau. BOOTP est utilisé en étroite collaboration avec un serveur TFTP sur lequel le client va trouver les fichiers à charger et à copier sur le disque dur.

Un serveur DHCP peut renvoyer des paramètres BOOTP ou de configurer propres à un hôte donné[50].

I.6 Étude de réseau LAN :

Précisément on a cité 4 types de réseaux mais le plus pratiqué c'est le réseau LAN. On s'intéresse à l'étude de réseau LAN car le plus utilisé dans les sociétés qui sont constitué généralement de plusieurs départements qui nécessitent un échange d'information.

I.6.1Les caractéristiques des réseaux locaux [7]

Un réseau local se caractérise principalement par sa topologie (physique et logique) : les média, ainsi que le mode transmission.

I.6.1.1 Media de transmission

Dans les réseaux locaux, nous pouvons trouver plusieurs medias de transport/transmission, et parmi ces medias nous citons :

- Le câble coaxial.
- La paire torsadée.
- La fibre optique.
- Les ondes hertziennes.

I.6.1.2 Mode de transmission :

Selon le sens des échanges, nous distinguons trois modes de transmission :

- La liaison simplex.
- La liaison half-duplex.
- La liaison full-duplex.

I.7Les topologies d'un réseau [8]

Pour pouvoir utiliser un réseau, Il faut définir, en plus du type de réseau, une méthode d'accès entre les ordinateurs, ce qui nous permettra de connaître la manière dont les informations sont échangées.

Il existe deux types de topologies : topologie logique et topologie physique.

I.7.1 La topologie logique

Elle représente la façon dont les données transitent dans les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token ring et FDDI.

I.7.2La topologie physique

La topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux, etc.) et des éléments matériels (cartes réseau, etc.)

Nous distinguons principalement trois grandes topologies physiques dans les réseaux locaux, la topologie en bus, en étoile, et en anneau qui peuvent être combinées pour obtenir des topologies hybrides.

- ✓ **Topologie en bus :**Une topologie en bus (Figure 1.5**)** est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. Le mot "bus" désigne la ligne physique qui relie les machines du réseau.

Figure 1.5: Topologie en bus[8].

Cette topologie a pour avantage d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, c'est l'ensemble du réseau qui sera affecté.

- ✓ **Topologie en étoile :**Dans une topologie en étoile (Figure1.6), les ordinateurs du réseau sont reliés à un système matériel appelé *hub* ou *concentrateur*. Il s'agit d'une boîte comprenant un certain nombre de jonctions auxquelles nous pouvons connecter les câbles en provenance des ordinateurs. Celui-ci a pour rôle d'assurer la communication entre les différentes jonctions.

Figure 1.6: Topologie en étoile[8].

Contrairement aux réseaux construits sur une topologie en bus, les réseaux à topologie en étoile sont beaucoup moins vulnérables car nous pouvons aisément retirer une des connexions en la débranchant du concentrateur sans pour autant paralyser le reste du réseau. En revanche,

un réseau à topologie en étoile est plus coûteux qu'un réseau à topologie en bus car un matériel supplémentaire est nécessaire à savoir le hub.

- ✓ **Topologie en anneau :** Dans un réseau en topologie en anneau (Figure 1.7**)**, les ordinateurs communiquent chacun à leur tour, nous avons donc une boucle d'ordinateurs sur laquelle chacun d'entre-eux va avoir la parole successivement.

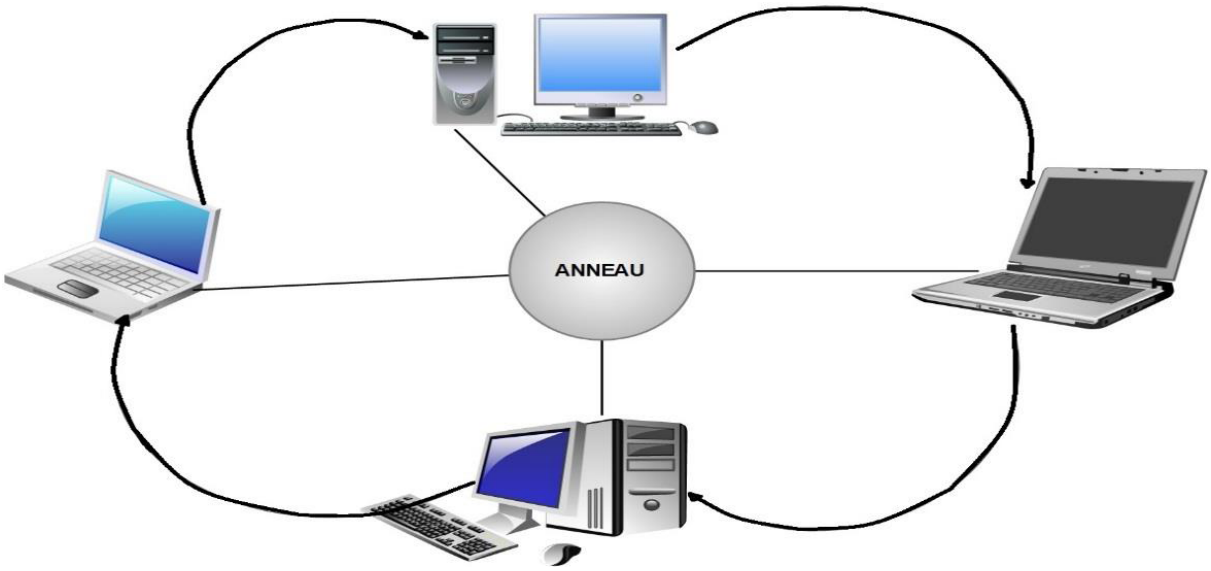


Figure 1.7: Topologie en anneau [8].

En réalité les ordinateurs d'un réseau en topologie anneau ne sont pas reliés en boucle, mais sont reliés à un répartiteur appelé MAU (*Multistation Access Unit*) qui gère la communication entre les ordinateurs qui lui sont reliés en accordant à chacun d'entre eux un temps de parole.

I.8 Les modèles [9,10]:

Pour faciliter la communication entre hotes dans les LAN on utilise des modèles.

On distingue généralement deux type de modèle dans les réseaux est particulièrement dans le réseaux LAN :

I.8.1 Le modèle OSI :

Le modèle OSI (Open Systems Interconnexion) est une architecture abstraite de communication, élaboré par l'ISO (International Standards Organisation). Il définit le fonctionnement d'un réseau informatique suivant sept (07) couches de protocole chacune remplissant une partie bien définie des fonctions et de protocoles.

- **Protocole :**

Un protocole est un ensemble de règles qui régit la communication entre deux entités. Ces règles prennent aussi en compte le format des données échangées entre ces entités. Son objectif est d'assurer que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficace.

I.8.1.1Architecture en couches du modèle OSI

Dans le modèle OSI possède 7 couches qui sont les suivant

A. La couche Physique :

La couche Physique est la première couche du modèle OSI. Quelques fonctionnalités de base de la couche Physique du modèle OSI sont les suivantes :

- Elle est responsable de la transmission bit à bit sur le canal de transmission
- Cette couche gère les signaux électriques, signaux lumineux et les signaux ondes radios

B. La couche Liaison de données :

C'est la deuxième couche du modèle OSI. Voici une vue sur les différentes fonctionnalités de cette couche:

- Elle est responsable du codage/décodage des signaux électriques/bits ;
- Cette couche gère les erreurs de données provenant de la couche Physique ;
- La couche Liaison convertit les signaux électriques en trames de niveau 2 ;
- Elle est subdivisée en deux sous-couches, à savoir ;
- La couche d'accès média– MAC (Medium Access Layer) ;
- La couche LLC (Logical Link Layer) ;
- La sous-couche MAC gère le contrôle d'un nœud du réseau (le nœud peut être un ordinateur) par rapport à l'accès et à la permission de transmettre des données sur le

support physique du réseau ;

 La couche LLC gère la synchronisation des trames, le contrôle de flux et effectue un contrôle d'erreurs ;

 Les équipements réseaux tels que les Switch/Commutateurs agissent à ce niveau (2) du modèle OSI .

C. La couche Réseau :

C'est la troisième couche du modèle OSI. Parmi ces différentes fonctionnalités, on peut citer:

 Les mécanismes de routage sont implémentés à ce niveau ;

 Elle gère le routage des données depuis la source vers la destination ;

 Cette couche gère l'interconnexion entre réseaux hétérogènes ;

 Elle gère les congestions, le séquencèrent des paquets et les erreurs ;

 Les équipementsréseaux tels que les routeurs fonctionnent à ce niveau du modèle OSI ;

 Les protocoles de niveau 3: IP, IPX, AppleTalk, etc.

D. La couche Transport :

C'est la quatrième couche du modèle OSI. En voici les fonctionnalités:

 Cette couche gère la transmission point à point des données de façon transparente pour les utilisateurs finaux ;

 Elle gère les erreurs de transmission point à point et effectue un contrôle de flux ;

 Les protocoles de niveau 4: TCP, UDP, SPX, etc.

E. La couche Session :

C'est la cinquième couche du modèle OSI. Voici les fonctionnalités fondamentales offertes par cette couche:

 Elle est responsable de la gestion de l'établissement, du maintien et de la rupture des connexions ou sessions entre applications ;

 La couche session initialise, coordonne et met un terme aux conversations, échanges, et dialogues entre applications à chaque extrême ;

 Les protocoles de niveau 5: NFS (Network File System), noms NetBIOS, RPC, SQL, etc.

F. La couche présentation :

C'est la sixième couche du modèle OSI dont les fonctionnalités de base sont:

- Elle est responsable de la représentation des données sur votre écran ;
- Chiffrement et déchiffrement des données ;
- Elle gère la syntaxe et la sémantique des données ;
- Exemple de représentations/protocole de niveau 6: ASCII, EBCDIC, TIFF, GIF, JPEG, MPEG, MIDI, etc.

G. La couche Application :

C'est la septième et dernière couche du modèle OSI dont les fonctionnalités de bases sont:

- Cette couche supporte les processus des utilisateurs finaux ;
- Elle gère tous les services des utilisateurs tels que le transfert de fichier, le web, l'email, etc. ;
- Protocoles: Telnet, FTP, SMTP, HTTP, etc.

La figure 1.8 montre Les couches du Modèle OSI**.**

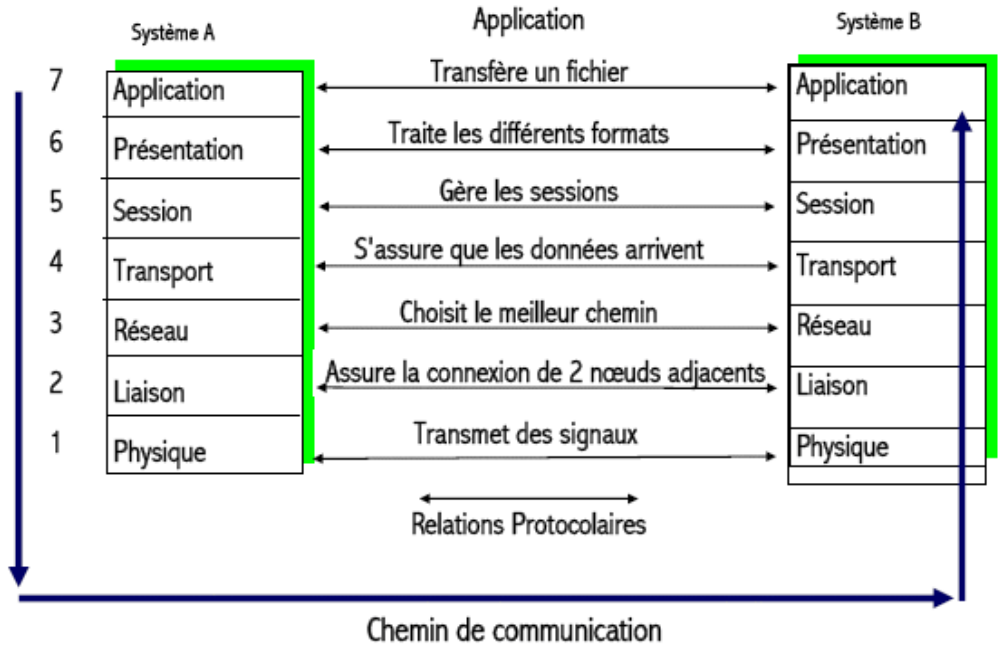


Figure 1.8 : Les couches du Modèle OSI [10].

I.8.2 Le modèle TCP/IP :

TCP/IP ou « *Transmission Control Protocol/Internet Protocol* » est un protocole de transport fiable, en mode connecté, c'est-à-dire qu'il permet l'établissement d'une session de communication entre deux parties qui veulent échanger des données.

La suite TCP/IP est l'ensemble des protocoles utilisés pour le transfert des données sur internet. Elle est souvent appelée TCP/IP, d'après le nom de ses deux premiers protocoles : TCP (Transmission Control Protocol) et IP (Internet Protocol).
TCP/IP Comporte plusieurs protocoles et définit un modèle en 4 couches.

I.8.2.1 Architecture en couches du modèle TCP/IP

A. Accès Réseaux :

 La couche accès réseaux correspond en gros auxcouches 1 et 2 de l'OSI. La couche d'accès réseau a pour rôle de transmettre les données sur le média physique utilisé. En fonction du type de réseau, des protocoles différents peuvent être utilisés à ce niveau.

B. Couche Internet (IP) :

 La couche internet (IP) correspond au niveau 3 de l'OSI. Cette couche a pour rôle de transmettre les données à travers une série de réseaux physiques différents qui relient un hôte source avec un hôte destination. Les protocoles de routage sont étroitement associés à ce niveau. IP est le protocole routé de base sur l'Internet.

C. Couche Transport (TCP) :

 La couche TCP correspond à la couche 4 de l'OSI (transport de bout en bout) prend en charge la gestion de connexion, le contrôle de flux, la retransmission des données perdues et d'autres modes de gestion des flux. Les protocoles TCP et UDP sont dédiés à ces fonctions de transport.

D. Couche Application :

 Enfin, la couche application (équivalente aux couches 5, 6 et 7 de l'OSI), La couche application sert à l'exécution des protocoles de niveau utilisateur tels que les échanges de courrier électronique (SMTP), le transfert de fichiers (FTP) ou les connexions distantes (Telnet).

 Chaque couche de la pile ajoute des informations de contrôle de manière à garantir une transmission de données correcte.

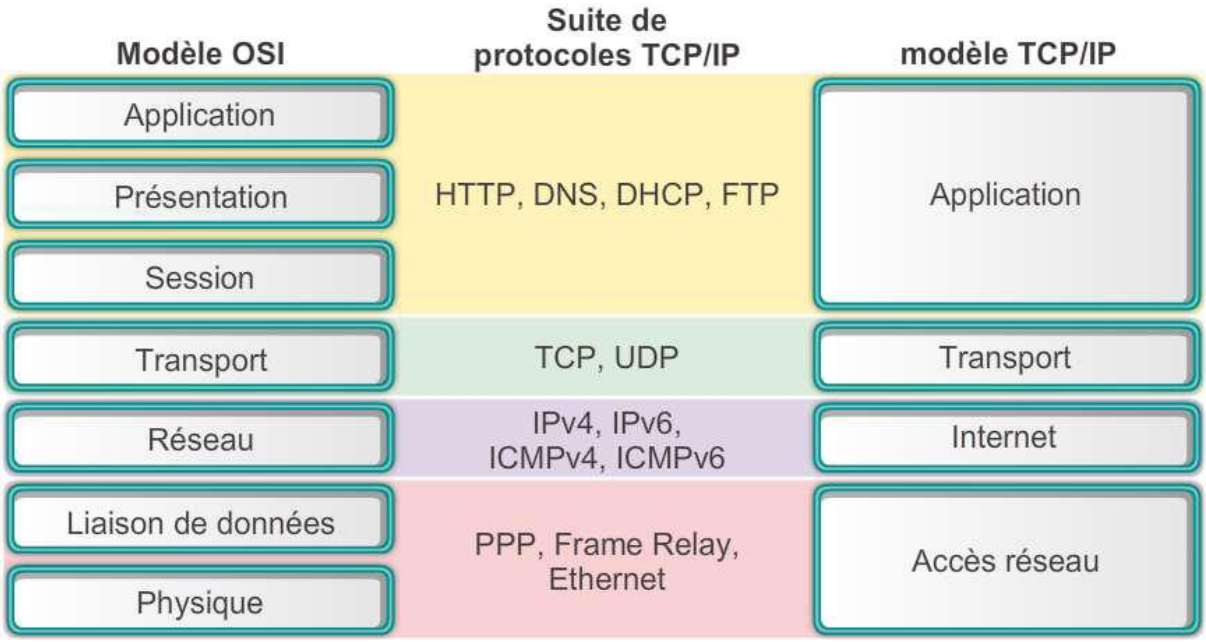


Figure 1.9 : Comparaison entre le modèle TCP/IP et le modèle OSI [9].

Partie II : Sécurité des réseaux locaux (informatique)

II.1 Définition de la sécurité d'un réseau informatique [11]

La sécurité des réseaux informatiques est nécessaire pour protéger le réseau d'une entreprise et de se prémunir contre tout type d'attaques pouvant perturber le réseau. La sécurité informatique (SI) est l'ensemble des moyens (méthodes, techniques et outils) mises en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.

II.2 Objectifs de la sécurité informatique [12]

La sécurité informatique vise généralement cinq principaux objectifs:

- **La disponibilité** : permettre de maintenir le bon fonctionnement du système informatique.
- **L'intégrité** : les données ne doivent pas être altérées de façon illicite ou malveillante. En clair, les éléments considères doivent être exacts et complets.
- L**a confidentialité´** : seule les personnes autorisées ont accès aux informations qui leur sont destinées. Toute accès indésirable doit être empêché.
- **L'authentification** : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
- **La non-répudiation** : aucun utilisateur ne doit pouvoir contester les Operations qui a réalisées dans le cadre de ses actions autorisées.

II.3Terminologie de la sécurité informatique [13]

Ensemble des termes utilisés dans le domaine de la sécurité informatique peut se résumer ainsi :

- **Vulnérabilité :** Une vulnérabilité ou une faille est une faiblesse dans un système ou un logiciel permettant à un attaquant de porter atteinte à la sécurité d'une information ou d'un système d'information.

- **Menace :** Ce sont les actions potentiellement nuisibles à un système informatique. Les menaces peuvent être le résultat de plusieurs actions en provenance de plusieurs origines.
- **Risque :** Un risque désigne la probabilité d'un événement dommageable ainsi que les coûts qui s'en suivent, Le risque dépend également des montants des valeurs à protéger.

La vulnérabilité, menace et risque donnent l'occasion au hacker de lancer des attaques.

II.4 Attaques [14,15]

Une attaque est l'exploitation d'une faille d'un système informatique à des fins non connues par l'exploitant des systèmes et généralement préjudiciables. Parmi les différentes attaques qui existent, nous pouvons citer : IP spoofing, Le Sniffing, lesVirus, les Ver, les attaques DoS, et Man in the middle.

Les attaques représentent un risque pour chaque système de sécurité vulnérable, Pour pouvoir faire face à ces attaques nous devrons d'abord définir ces attaques et connaitre quelles sont les composantes matérielles et logiciels qu'elles visent.

L'attaque peut venir de la part de n'importe qui des utilisateurs, car le réseau de l'entreprise est ouvert sur internet, mais ceci ne veut pas dire que les attaques viennent juste de l'extérieur, car selon les statistiques 70% viennent du réseau interne [14].

Les attaques que peut subir un réseau d'entreprise sont nombreuses et dans ce qui suit nous allons décrire quelques attaques pour lesquelles nous allons illustrer des politiques de sécurité appropriées.

II .4.1 Attaque par inondation [14, 15]

L'inondation est l'une des attaques qui empêche un réseau ou un système d'assurer sa mission. Le principe de cette attaque consiste à :

- Inonder la cible (serveur par exemple) avec des paquets IP jusqu'à saturer sa bande passante.
- Suite à la saturation de la bande passante les autres machines ne peuvent pas se communiquer d'où une situation de déni de service est provoquée.

Inonder le serveur par des demandes de connexion TCP

a) Ouverture d'une session TCP (cas normal) : Dans une connexion TCP, l'ouverture de la session se déroule par l'échange des messages SYN (numéro de séquence) et ACK (acquittement).

Dans le cas normale le déroulement se fait comme suit :

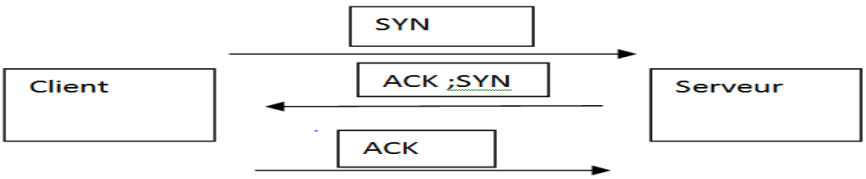


Figure 2.1 : Ouverture d'une session TCP.

Le client doit envoyer un message SYN au serveur puis ce dernier répond par l'envoie d'un message SYN, ACK au client, Dans ce cas, le serveur attend le message ACK qui indique que le client a bien reçu le message ACK, SYN et il reste en attente de réponse jusqu'à l'expiration d'un Timeout.

b) Fonctionnement de l'attaque par inondation SYN (syn flooding)[15]:

Le pirate peut lancer une attaque en essayant d'ouvrir des sessions TCP mais en suivant une technique différente de celle décrite dans le cas normal. Cette technique se résume ainsi :

- Ecrire un programme qui n'envoi jamais de paquets ACK à la réception de paquet SYN

de la part du serveur,

- Par la suite inonder le serveur par des demandes de connexion TCP, ce qui entraine

le serveur à allouer de plus en plus de ressources pour ces demandes de connexion qui reste en attente,

- Le serveur dans ce cas perd ses capacités et les autres machines ne peuvent plus accéder

au serveur, ce qui génère une situation de déni de service.

c) outil de défiance :

Le firewall peut être utilisé comme un moyen de protection contre ce type d'attaque en détectant puis en bloquant la requête après N paquets SYN consécutifs issus du même client ou à destination du même serveur.

II .4.2 Attaque par inondation Attaque "man in the middle" sur le chiffrement SSL

Dans une attaque sur le chiffrement SSL, le trafic vers le port SSL est dérouté de manière transparente vers la machine du pirate, cette dernière assurant les fonctions d'un serveur HTTPS (HyperText Transfer Protocol Secure sockets).

a) **Principe de fonctionnement de l'attaque :** Dans ce type d'attaque, si une machine A souhaite communiquer avec une machine B, la procédure se déroule comme suit :

– La machine A se connecte à la machine pirate C qui est pour lui un serveur HTTPS,

– La machine pirate C lui fournit un certificat puisqu'il assure les fonctions d'un serveur HTTPS,

– La machine B croit que le certificat a été délivré par une autorité de confiance alors que ce n'est pas le cas,

– La machine pirate C reçoit des messages chiffrés avec le certificat qu'il a délivré, de ce fait il peut les déchiffré,

– La machine pirate C déchiffre le message et le réachemine à la machine destination B qui est le serveur HTTPS de confiance,

– Le tunnel de sécurité SSH est donc découpé en deux, l'un entre la machine client A et La machine pirate C et l'autre entre la machine pirate C et le serveur HTTPS B,

– Le relais pirate peut recopier ou modifier les données en transit malgré la sensation de chiffrement qu'a le client A.

La figure 2.2 représente l'attaque min in the middle .

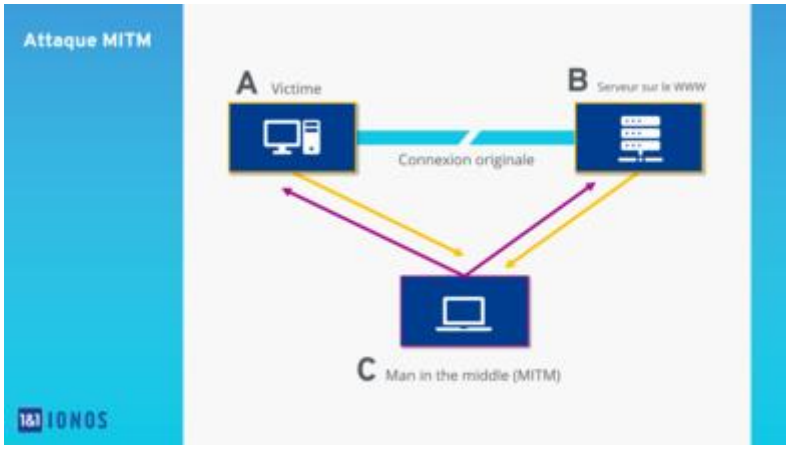


Figure 2.2 : l'attaque Main in the middle [29].

b) Outil de défense : Pour faire face à ce type d'attaque, il faut utiliser le VPN qui utilise IPsec comme un protocole de chiffrement.

II.4.3 Attaque ARP Spoofing

a) Description du fonctionnement du protocole ARP (Address Resolution Protocol) :

– ARP est un protocole qui implémente le mécanisme de résolution des adresses IP (32 bits en IPv4) en adresse MAC (42 bit).

– Les paquets ARP sont envoyés entre les systèmes du réseau local, donc chaque système possède localement une table de correspondance entre l'adresse IP et l'adresse MAC.

La figure 2.3 explique le fonctionnement du protocole ARP

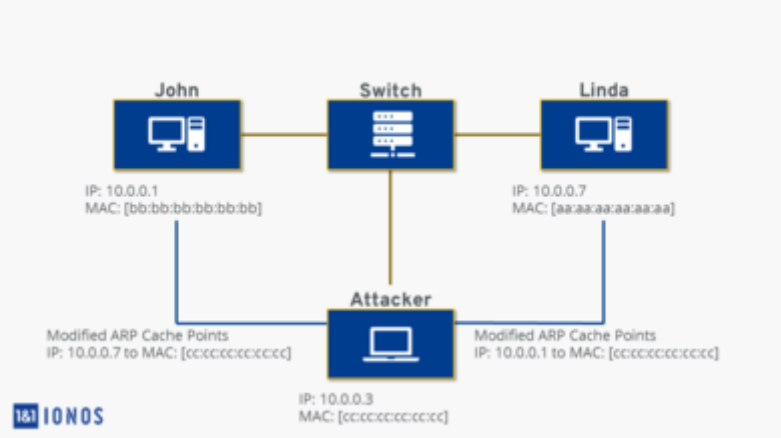


Figure 2.3 : fonctionnement du protocole ARP [52].

b) Principe d'attaque ARP spoofing [14] :

– Le système pirate envoie des paquets ARP vers le système cible indiquant que la nouvelle adresse MAC correspond à une adresse IP d'une passerelle est la sienne,

– Le système cible envoi tout son trafic au système pirate,

– Le système pirate peut donc écouter et modifier passivement le trafic puis le dérouté vers sa véritable destination.

La figure 2.3.1 illustre les étapes de déroulement de l'attaque ARP .

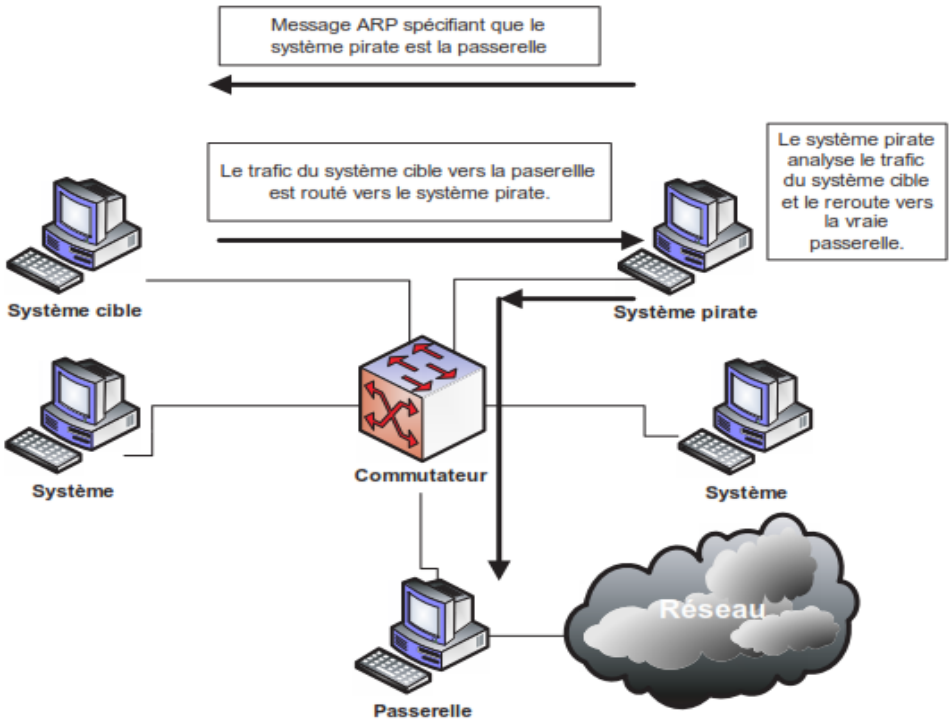


Figure 2.3.1 : Attaque ARP spoofing .

c) Outil de défense : Pour faire face à ce type d'attaque, on doit segmenter le réseau avec des VLANS [16].

II.5 Techniques de sécurité dans un réseau local

II.5.1 Pare-feu (firewall FW) et DMZ

II.5.1.1 Pare-feu (firewall FW) [17]

Définition :

Un pare-feu ou firewall est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à internet par exemple, ou protection d'un réseau d'entreprise).

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

Les firewalls ont obtenu une grande renommée en matière de sécurité sur Internet.

Figure 2.4 : Firewall.

La figure 2.4 explique le principe de firewall

II.5.1.2 Objectif des firewalls [18, 19, 20, 21]

Ils ont deux principaux objectifs:

- Protéger le réseau interne contre les tentatives d'intrusion provenant de l'extérieur, (extérieur vers intérieur).
- Limiter et vérifier les connexions provenant du réseau interne vers l'extérieur. (Intérieur vers extérieur).

II.5.1.2.1 Fonctionnement du Firewall

Le fonctionnement d'un pare-feu (FW) repose sur un ensemble de règles prédéfinies permettant :

– D'autoriser la connexion (allow),

– De bloquer la connexion (deny).

(Voir la figure 2.4.1)

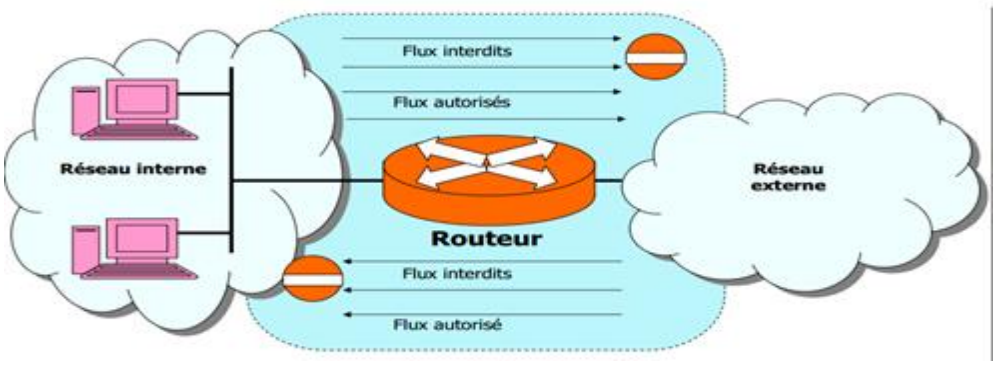


Figure 2.4.1 :Pare-feu.

II.5.1.2.2 Principale différence entre un FW et un routeur IP

Le FW ressemble beaucoup a un routeur la déférence réside dans le suivant :
Le routeur prend en charge les paquets jusqu'à la couche IP. Le routeur transmet chaque paquet en fonction de l'adresse de destination du paquet et de la route vers la destination précisée dans la table de routage. Par contre, le firewall ne transmet pas les paquets. Le pare feu accepte les paquets et les prend en charge jusqu'à la couche application.

II.5.1.2.3 Types de firewall [18, 22,23]

- **Pare-feu filtrage:**

Il existe 3 types de filtrages :

✓ Le filtrage simple de paquet qui travaille au niveau de la couche 3 du modèle OSI. Le pare-feu analyse les en-têtes de chaque paquet de données échangé entre une machine interne et externe afin d'étudier les adresses IP émettrices et réceptrices, les types de paquets et les numéros de port.

✓ Le filtrage dynamique travaille au niveau des couches 3 et 4 du modèle OSI. Le pare-feu Peut ainsi prévoir les ports à autoriser ou à interdire.

✓ Le filtrage applicatif permet de filtrer les communications application par application au Niveau de la couche 7 du modèle OSI. Ce type de filtrage impose la connaissance des protocoles utilisés par chaque application.

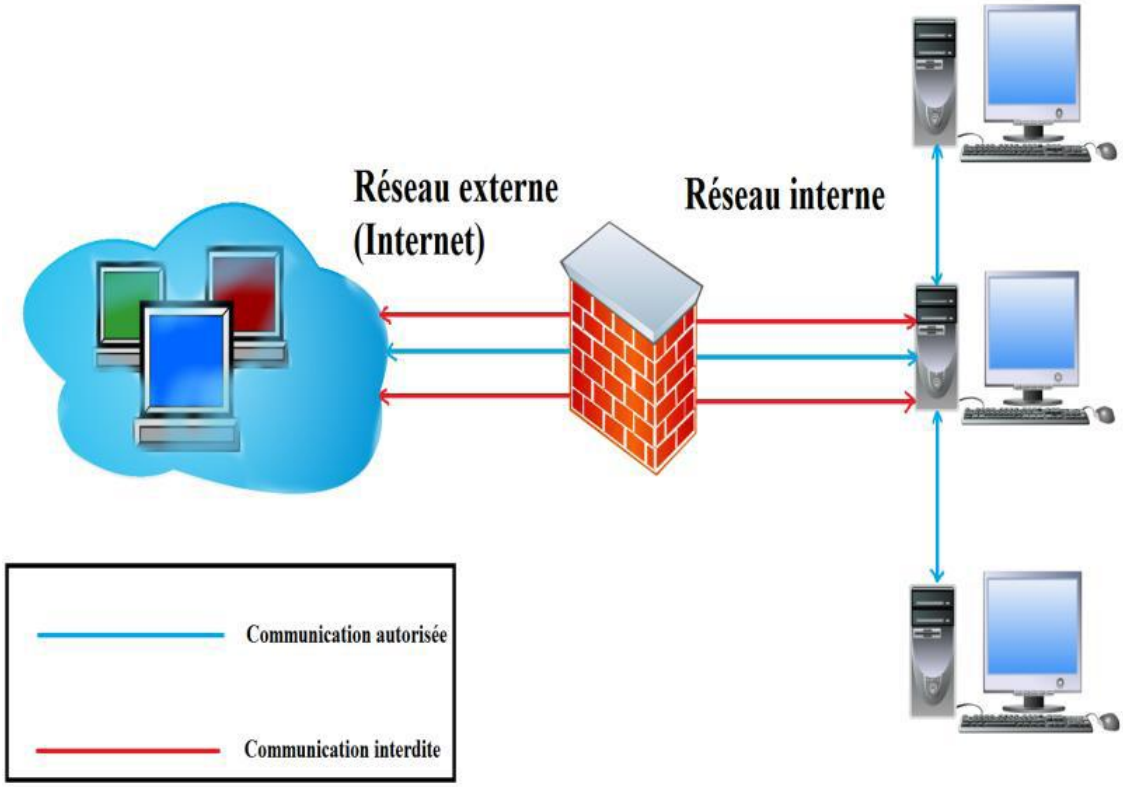


Figure 2.5: Pare-feu [18].

La figure 2.5 représente pare-feu

- **Proxys** [22]**:**

Un proxy est un serveur qui fait la fonction d'Intermédiaire entres les ordinateurs d'un réseau local et internet. Le proxy est un serveur mandaté par une application pour effectuer une requête sur Internet à sa place.

Le proxy assure une fonction de cache, les pages les plus souvent visitées sont stockées sur le serveur.

Il peut également assurer un suivi des connexions (logs utilisateurs) et filtrer les connexions à internet en analysant les requêtes des clients et les réponses des serveurs pour les comparer à la liste blanche (liste de requête autorisées) ou à la liste noire (liste de requête interdites).

Il peut aussi assurer l'authentification des utilisateurs pour gérer l'accès aux ressources externes.

La figure 2.5.1 explique un proxy

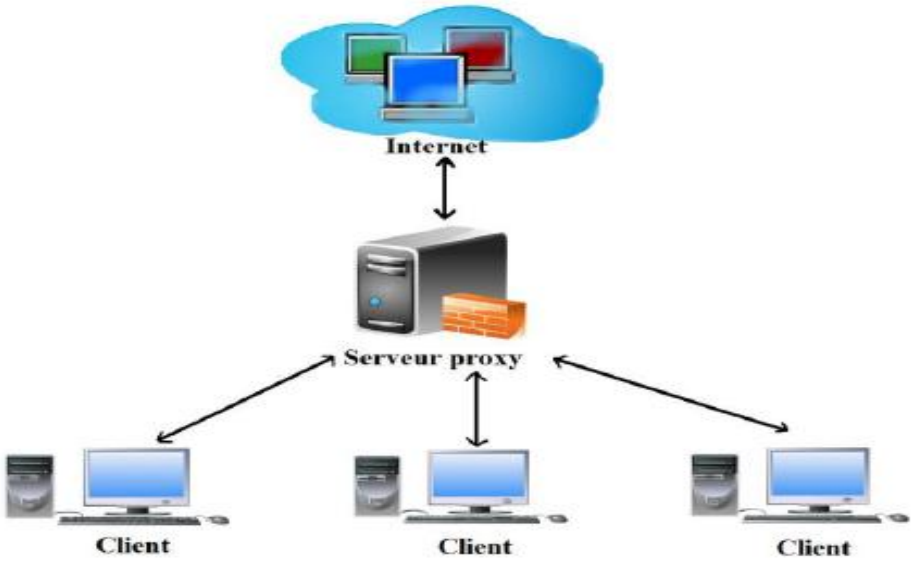


Figure 2.5.1: Proxy [23].

II.5.1.2 DMZ (Délimitarised Zone)

II.5.1.2.1 Définition de DMZ [24,25]

Une DMZ (voir la figure) : en anglais De-Militarized Zone, est une partie du réseau local dont l'objectif est d'être accessible depuis l'extérieur du réseau local, avec ou sans authentification préalable. En effet, pour des raisons à la fois techniques et stratégiques, les réseaux IP locaux (LANs) sont (paradoxalement) devenus des zones inaccessibles depuis internet.

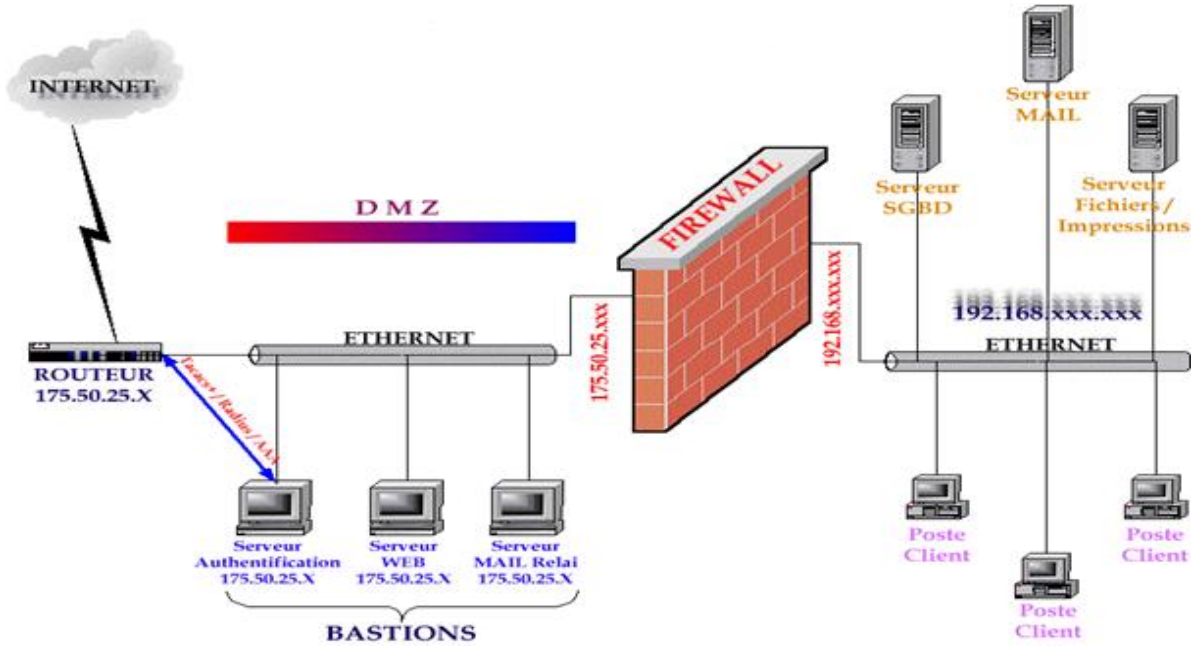


Figure 2.6 – DMZ et Firewall.

La figure 2.6 représente une DMZ et Firewall

II.5.1.2.2 Serveurs installés sur la DMZ

Le DMZ permet de fournir des services au réseau externe, tout en protégeant le réseau interne contre des intrusions possibles sur ces serveurs :

– Les serveurs Web (http),

– Les serveurs de fichiers (ftp),

– Les serveurs d'e-mails (SMTP),

– Les serveurs de noms (DNS).

II.6 VPN [26,27]

Les VPNS (Virtual private Network) ou réseau virtuel privé est une technique qui permet à un ou plusieurs postes distants de se communiquer de manière sécurisée tout en empruntant les infrastructures publiques. Il existe deux types de VPN, les VPNs d'entreprise et les VPNS d'opérateur.

Dans notre étude nous allons s intéresser aux VPNS d'entreprise qui sont utilisées dans les réseaux LAN.

II.6.1 Mode de fonctionnement des VPNS d'entreprise [26, 27] :

Un réseau VPN repose sur un protocole appelé " protocole de tunneling ", ce protocole permet de faire circuler les informations échangés de bout à un autre bout du tunnel d'une façon crypté (chiffrement des données et encapsulation des entêtes). Ainsi les utilisateurs ont l'impression (ou plutôt le fait) de se connecter directement sur le réseau de leurs entreprise. Les données transmises avec un tunnel VPN seront sécurisées.

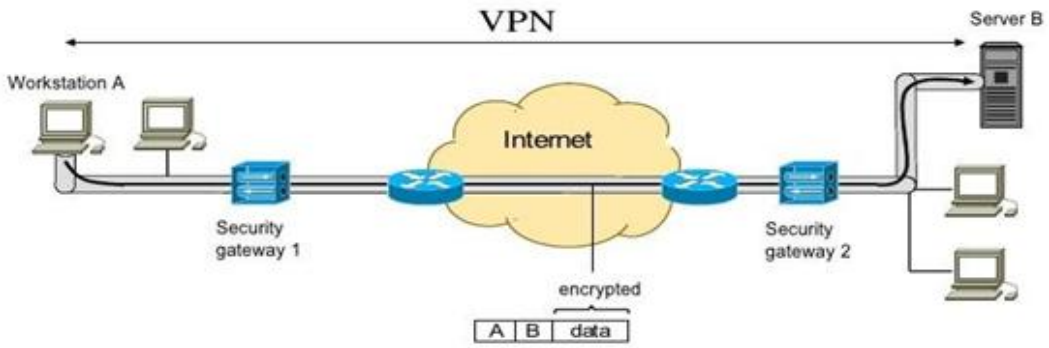


Figure 2.7 : Mode de fonctionnement d'un réseau VPN.

La figure 2.7 illustre le mode de fonctionnement d'un réseau VPN.

II.6.2 Avantages et inconvénients des VPNs d'entreprise [26, 27] :

- **Avantages**: les principaux avantages des VPNs d'entreprise sont :

  - Pas de contrat de négociation,
  - Pas de frais mensuels autre que ceux de l'abonnement Internet servant de support à ces VPN,
  - Le déplacement des tunnels, le chargement des périmètres et le contrôle du trafic circulant s'effectuent avec une grande souplesse,
  - Maitrise des protocoles de sécurité,

- **Inconvénients et limites** [26,27] **:**

Il est évident que les VPN d'entreprise représente quelque inconvénients et limites que l'on cite dans ce qui suit :

- Adresses IP fixes recommandées au moins pour les sites principaux,
- Nécessité d'avoir une personne compétente dans le réseau interne,
- Pas de garantie de temps de rétablissement en cas de défaillance,
- Pas de garantie de performance, car les VPNs ont comme support un lien Internet.

II.6.3 Type de VPN d'entreprise [27]:

Il existe trois types de VPN d'entreprise selon la nature des deux extrémités :

- **VPN site à site :** Autrement dit Intranet VPN, c'est une solution utilisée pour relier deux ou plusieurs sites distants d'une entreprise entre eux via un support internet avec une relation sécurisée, ce cas d'utilisation est l'un des cas les plus fréquents dans le réseau d'entreprise. Pour réaliser cette solution on aura besoin d'un routeur ou d'un pare-feu situé aux frontières.

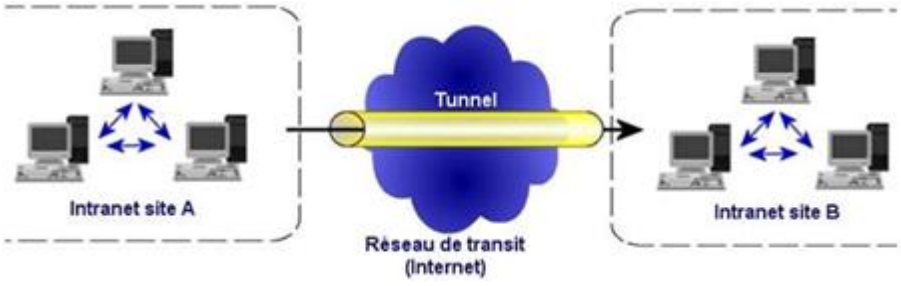


Figure 2.8 – VPN site à site.

La figure 2.8 explique le VPN site à site.

- **VPN poste à site :** Autrement dit VPN d'accès, ce type de VPN est aussi l'une des solutions les plus fréquemment utilisées. Elle consiste à permettre aux utilisateurs distants

de se communiquer et d'accéder aux ressources de leurs réseaux d'entreprise avec un tunnel sécurisé.

Afin de mettre en place cette solution on a besoin :

– Du coté site central : mise en place d'un router, pare-feu ou d'un concentrateur SSL implémenté au frontière du réseau local.

– Du coté poste de travail distant : installation d'un logiciel qui gère le type de protocole choisi et qui doit être compatible avec le matériel implémenté dans le site central.

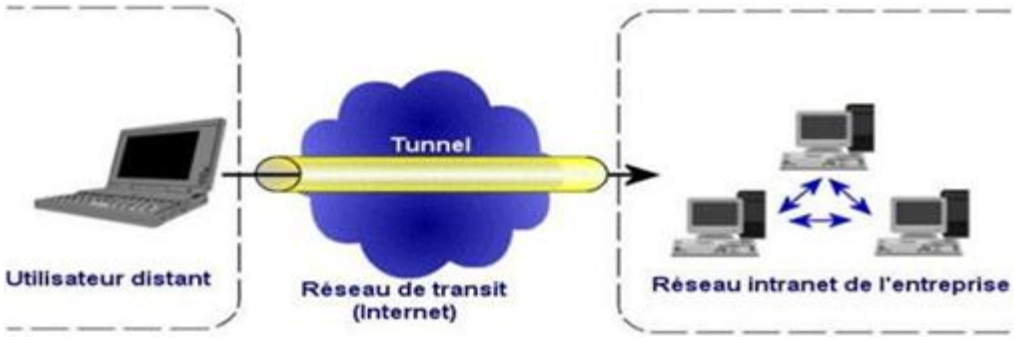


Figure 2.9 : VPN poste à site.

La figure 2.9 explique le VPN poste à site.

- **VPN poste à poste :** C'est le cas le plus simple, il s'agit de relier deux poste (dans le cas Le plus général un poste et un serveur) et ceci se fait dans le cas où les deux postes se trouvent dans le même réseau local ou entre deux postes distant reliés eu même par un VPN site à site.

Cette solution est utilisée dans des relations très sensibles entre deux postes, car elle garantit la protection de la conversation de bout en bout.

Pour réaliser cette solution, il suffit d'installer un composant logiciel dans les deux extrémités de la conversation.

II.7 Cryptographie [31, 32,51] :

Définition :

La cryptographie est la science qui utilise les mathématiques pour le cryptage (chiffrement) et le décryptage (déchiffrement) de données. Elle nous permet ainsi de stocker des informations confidentielles ou de les transmettre sur des réseaux non sécurisés (tels que l'Internet), afin qu'aucune personne autre que le destinataire ne puisse les lire.
La cryptographie est divisée en deux types :

a. cryptographie Symétrique : En cryptographie conventionnelle, également appelée cryptage de clé secrète ou de clé symétrique, une seule clé suffit pour le cryptage et le décryptage. La norme de cryptage de données (DES) est un exemple de système de cryptographie conventionnelle largement utilisé par le gouvernement fédéral des Etats-Unis.
La Figure I.9 est une illustration du processus de cryptage symétrique.

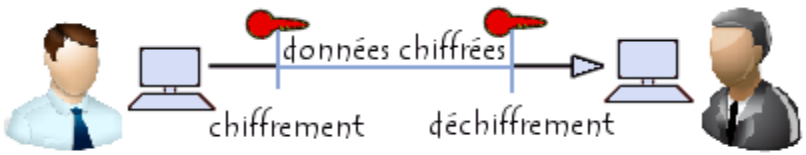


Figure 2.10 : Cryptographie Symétrique.

b. Cryptographie Asymétrique : La Cryptographie asymétrique (Figure 2.17) ou à clé publique est un procédé asymétrique utilisant une paire de clés pour le cryptage : une clé publique qui crypte des données et une clé privée ou secrète correspondante pour le décryptage. Nous pouvons ainsi publier notre clé publique tout en conservant notre clé privée secrète. Tout utilisateur possédant une copie de notre clé publique peut ensuite crypter des informations que nous seuls pouvons lire.
D'un point de vue informatique, il est impossible de deviner la clé privée à partir de la clé publique. Tout utilisateur possédant une clé publique peut crypter des informations, mais est dans l'impossibilité de les décrypter. Seule la personne disposant de la clé privée correspondante peut les décrypter.

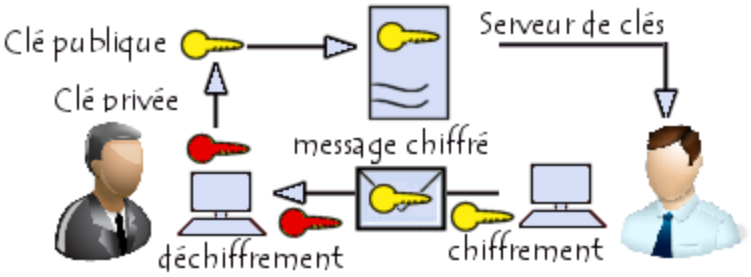


Figure 2.11 : Cryptographie Asymétrique.

c. Signature numérique : Les signatures numériques permettent au destinataire de vérifier authenticité des données, leur origine, mais également de s'assurer qu'elles sont intactes. Ainsi, les signatures numériques garantissent l'authentification et l'intégrité des données. Elles fournissent également une fonctionnalité de non répudiation. Ces fonctions jouent un rôle tout aussi important pour la cryptographie que la confidentialité, sinon plus. Une signature numérique a la même utilité qu'une signature manuscrite. Cependant, une signature manuscrite peut être facilement imitée, alors qu'une signature numérique est pratiquement infalsifiable. De plus, elle atteste du contenu des informations, ainsi que de l'identification du signataire.

d. Hachage : Ce type de fonction est très utilisé en cryptographier, principalement dans le but de réduire la taille des données à traiter par la fonction de cryptage. En effet, la caractéristique principale d'une fonction de hachage est de produire un haché des données, c'est-à-dire un condensé de ces données. Ce condensé est de taille fixe, dont la valeur diffère suivant la fonction utilisée (MD5, SHA).

Conclusion

Ce chapitre nous a permis en premier lieu de définir les notions élémentaires sur les réseaux informatiques telles que leurs types, leurs architectures et le mode d'adressage, pour évoquer en second lieu les enjeux de la sécurité des réseaux affin de mettre en évidence la nécessité d'élaborer des politiques de sécurité complètes et cohérentes pour faire face aux types d'attaques citées en faisant usage des mesures et des techniques de défense telles que l'utilisation des protocoles de sécurité la cryptographie.

Le chapitre suivant sera consacré à l'une des principales solutions d'accès sécurisées ayant eu le plus recours par les entreprises pour la connexion de bureaux distants, d'utilisateurs distants et de partenaires professionnels, via le biais d'un accès Internet tiers et peu couteux qui est le VPN (Virtuel Private Network).

Chapitre III :

Les VLANs et la sécurité des VLANs

CHAPITRE III : Les VLANS et la sécurité des VLANs

III .VLANS et sécurité [28, 30,34 , 35,36 , 37 ,38,39 ,40,41, 50]

Introduction :

De nos jours, il est pratiquement devenu indispensable pour toute entreprise de posséder son propre parc de réseau informatique interne, permettant ainsi la communication de données ou tout simplement d'informations d'un pôle d'une entreprise à un autre, et se présentant sous la forme d'un ensemble de matériels réseaux (commutateurs, routeurs, etc.) reliés entre eux. Cependant, il est parfois nécessaire de segmenter le réseau de façon logique pour des raisons sécuritaires principalement, et ce par la segmentation du réseau en plusieurs réseaux virtuels lesquels nous allons discuter dans ce chapitre (les différents types, raisons de leur utilisation, etc.).

III .1 Définition d'un VLAN :

Un VLAN (*Virtual Local Area Network* ou *Virtual LAN*, en français *Réseau Local Virtuel*) est un réseau local regroupant de façon logique et non physique un ensemble de machines.

Les VLANs permettent de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.)

III .2 Les types du VLAN:

Les VLANs sont diffèrent selon les informations utilisées pour regrouper les stations. Il en existe généralement quatre modèles, respectivement basés sur le port, sur l'adresse Mac, sur le protocole et l'adresse réseau.

- **Un VLAN de niveau 1 :** (aussi appelés VLAN par port, en anglais port-based VLAN) définit un réseau virtuel en fonction des ports de raccordement sur les commutateurs.

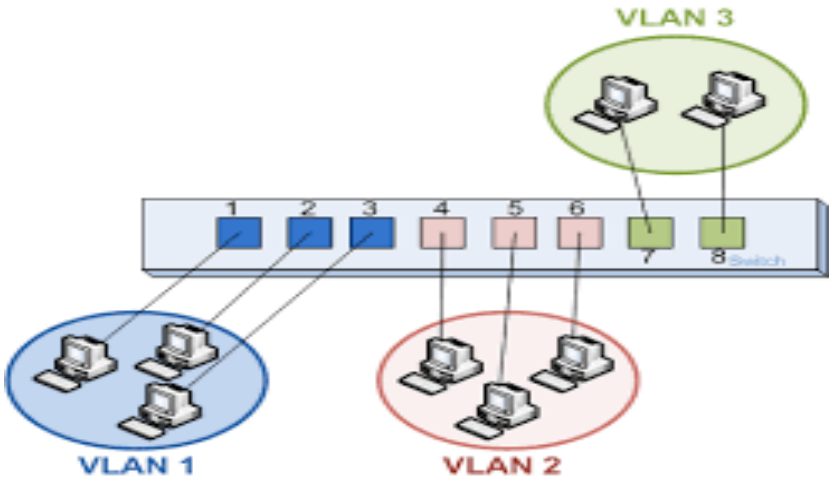


Figure 3.1: VLAN par port[30] .

- **Un VLAN de niveau 2** : (VLAN MAC, VLAN par adresse *IEEE*) consiste à définir un réseau virtuel en fonction des adresses MAC (*Media Access Control*) des stations . Ce type de VLAN est beaucoup plus souple que le VLAN par port car peu importe le port sur lequel la machine sera connectée, cette dernière fera partie du VLAN dans lequel son adresse MAC sera configurée.

  L'un des problèmes que posent les réseaux VLAN basés sur les ports est que si le périphérique d'origine est retiré du port pour être remplacé par un autre périphérique, le nouveau périphérique appartiendra au même réseau VLAN que son prédécesseur.

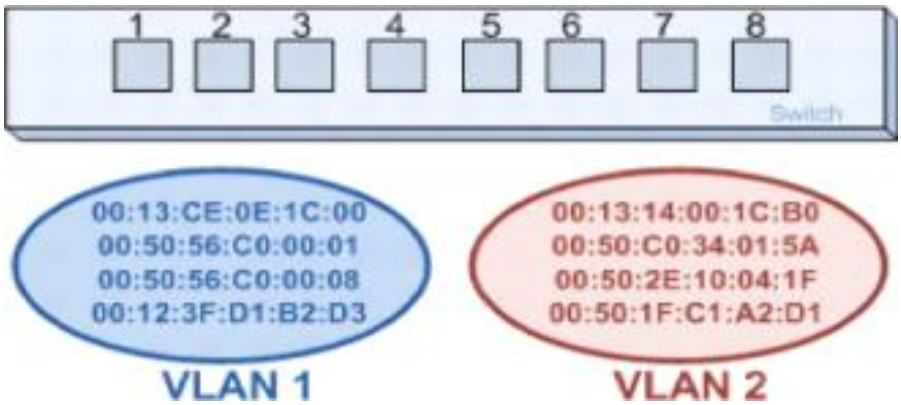


Figure 3.2 : VLAN par adresse MAC[34] .

Un VLAN de niveau 3 : On distingue plusieurs types de VLAN de niveau 3 :

- **Le VLAN** par sous-**réseau** : Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station. En contrepartie une légère dégradation de performances peut se faire sentir dans la mesure où les informations contenues dans les paquets doivent être analysées plus finement.
- **Le VLAN par protocole** : permet de créer un réseau virtuel par type de Protocol (TCP/IP, IPX (*Internetwork Packet Exchange*), AppleTalk, etc.), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau.

III .3 L'intérêt d'avoir des VLANs[35,36] :

Il existe plusieurs intérêts à avoir des VLAN dans un réseau, voici quelques exemples de besoins qui nécessitent l'utilisation des réseaux virtuels:

 La sécurité : Les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.

 Réduction des coûts : Des économies sont réalisées grâce à l'utilisation plus efficace de la bande passante et des liaisons ascendantes existante.

 Meilleures performances : Le fait de diviser des réseaux linéaires de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit la quantité de trafic inutile sur le réseau et augmente les performances.

 Efficacité accrue du personnel informatique : Les VLAN facilitent la gestion du réseau, car les utilisateurs ayant des besoins réseau similaires partagent le même VLAN.

 Gestion simplifiée de projets ou d'applications : La séparation des fonctions facilite la gestion d'un projet ou l'utilisation d'une application.

III .4 Routage inter-VLAN [39] :

- Quand un hôte d'un VLAN veut communiquer avec un hôte d'un autre VLAN, un routeur ou Switch niveau 3 est nécessaire.

- Le Switch de niveau 3 fonctionne en l'occurrence comme un routeur en rendant possible la communication ou l'échange d'information entre les différents VLANs.
- Le routeur (Switch niveau 3) est configuré pour effectuer le routage entre réseaux locaux virtuels.

La figure 3.4 représenté le routage inter-VLANS sur le Switch de niveau 3.

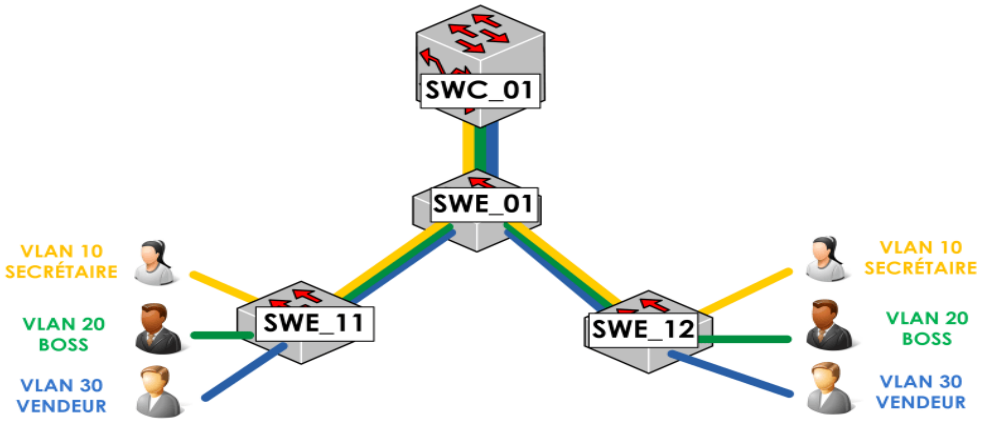


Figure 3.3 : Exemple d'un routage inter-VLANs sur le Switch N3[39] **.**

III.5 Les protocoles de transport des VLANs [37] :

Afin d'assurer le transport des VLANs, certains protocoles ont été mis en place :

III .5.1 Le Protocol ISL (Inter Switch Link Protocol) :

Pour étendre les réseaux virtuels sur plus d'un commutateur, CISCO a mis au point son propre protocole ISL. Ce protocole achemine les informations d'appartenance aux réseaux virtuels. ISL représente en fait une structure de trame et un protocole qui, en plus de transport des informations d'appartenance aux réseaux virtuels, permet à ces réseaux d'échanger des trames

a) Présentation générale de ISL :

Pour identifier les réseaux virtuels, ISL utilise un mécanisme de marquage explicite des paquets. Un commutateur qui utilise ce marquage encapsule la trame reçue dans un paquet

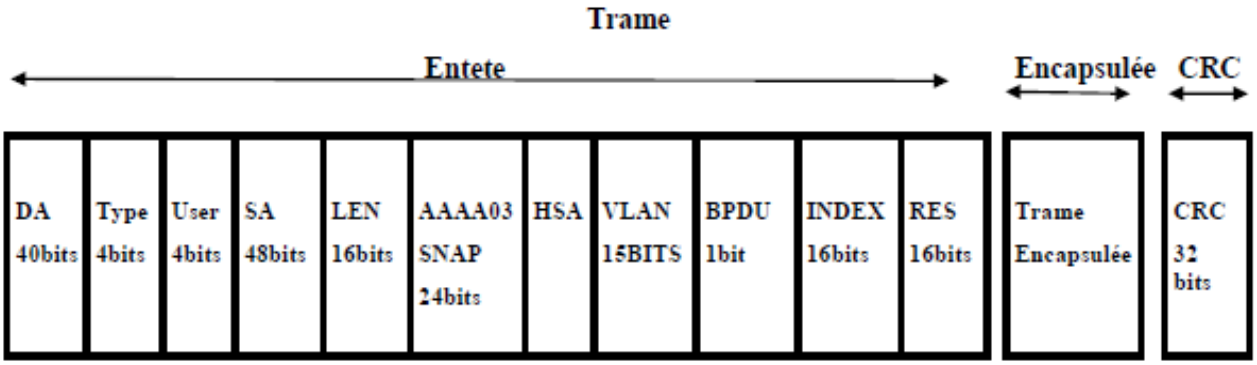
dont l'en-tête contient un champ d'appartenance aux VLAN et l'adresse MAC de la trame, permettant d'acheminer le paquet vers le routeur et les commutateurs appropries.
Lorsqu'elle atteint le réseau destination, on supprime l'en-tête, et la trame est acheminée vers l'équipement récepteur.

b) Structure des trames ISL :

Les trames ISL comprennent trois champs principaux :

- Un en-tête qui est constitué de plusieurs champs.
- Trame encapsulée dont la longueur est comprise entre 1 et 24575 octets.
- Champ CRC, ce champ qui est ajouté à la fin du paquet ISL, porte sur l'intégrité du paquet.

Le tableau 1.1 ci-après illustre la structure d'une trame ISL :



Figue 3.4 : structure de la trame ISL [37].

III .6 Modes de connexion des VLANs [38,40] :

Il existe deux modes pour faire transiter les VLANs :

- Mode *Access*.
- Mode *Trunk*.

III .6 .1Mode Access :

Un lien d'*accès* est un lien qui fait partie d'un seul VLAN, et les liens d'accès sont normalement destinés aux périphériques finaux. Aucun périphérique connecté à un lien d'accès n'est au courant de l'appartenance à un VLAN. Une connexion de liaison d'accès ne

peut comprendre que les trames Ethernet standard. Les commutateurs suppriment toutes les informations VLAN de la trame avant de les envoyer à un périphérique à liaison d'accès.

III .6 .2 Mode Trunk [38] :

Un trunk est une connexion physique unique sur laquelle on transmet le trafic de plusieurs réseaux virtuels. Les trames qui traversent le trunk sont complétéesavec un identificateur de réseau local virtuel (VLAN Id). Grâce à cette identification, les trames sont conservées dans un même VLAN ou domaine de diffusion.

Le réseau local est distribué entre différents équipements via des liaisons dédiées ou tout simplement trunks :

- **Entre deux commutateurs :** C'est le mode de distribution des réseaux locaux le plus courant.

- **Entre un commutateur et un hôte** : C'est le mode de fonctionnement à surveiller étroitement. Un hôte qui supporte le trunking a la possibilité d'analyser le trafic de tous les réseaux locaux virtuels.

- **Entre un commutateur et un routeur :** C'est le mode de fonctionnement qui permet d'accéder aux fonctions de routage ; donc à l'interconnexion des réseaux virtuels par routage inter-VLAN.

Ce schéma ci-dessous (Figure 3.4.), nous illustre la liaison de Trunk entre des commutateurs :

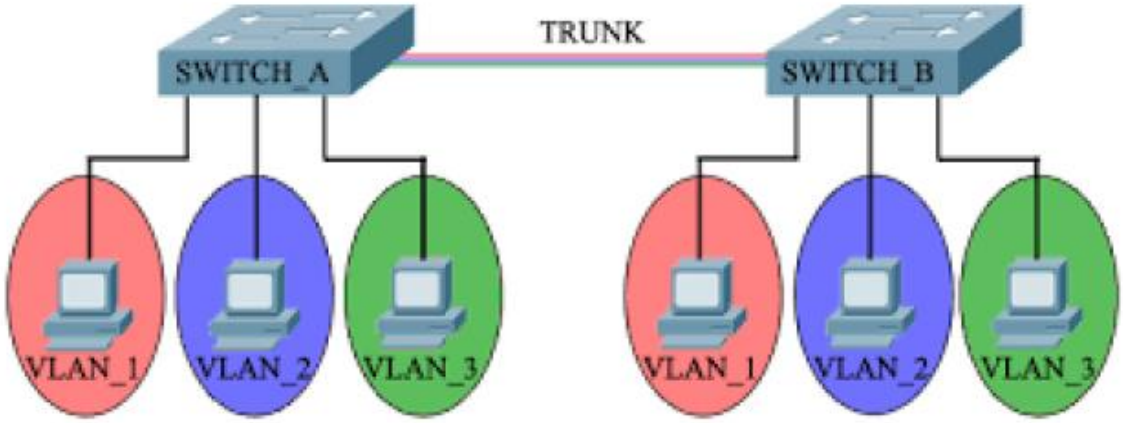


Figure 3.5 : Utilisation de trunk entre deux commutateurs [38].

III.7 Le protocole DHCP [28,50] :

Pour la conception de VLAN on à besoin de protocole DHCP qui est comme il a été mentionné dans le chapitre II un protocol qui permet à un ordinateur de se connecter sur un réseau local et d'obtenir dynamiquement sa configuration et de trouver une adresse IP.
On mentionne que :

- Le protocole DHCP (*Dynamic Host Configuration Protocol*) est un standard TCP/IP conçu pour simplifier la gestion de la configuration d'IP hôte.
- DHCP permet d'affecter de manière dynamique une adresse IP à un client, à partir de la base de données des adresses IP, gérée par le serveur DHCP du réseau local :
  - ✓ Dans un réseau TCP/IP chaque ordinateur doit disposer d'un nom d'ordinateur et d'une adresse IP unique (avec son masque de sous-réseau associé).
  - ✓ Quand on déplace un ordinateur vers un autre sous-réseau, l'adresse IP doit alors être modifiée.
  - ✓ Une adresse IP proposée par un serveur DHCP a une durée de vie limitée appelé bail. lorsque le client aura atteint 50% de sa durée, il enverra un DHCP REQUEST à son serveur DHCP afin de le renouveler.
  - ✓ Lorsqu'on rallume l'ordinateur, celui-ci a gardé, dans son registre, son adresse IP. Il envoie un message au serveur DHCP demandant s'il peut réutiliser cette adresse.

III.7.1 Le fonctionnement de DHCP :

Quand une machine vient de démarrer, elle n'a pas de configuration réseau (même pas de configuration par défaut) et pourtant elle doit arriver à émettre un message sur le réseau pour qu'on lui donne une vraie configuration. La technique utilisée est le broadcast, pour trouver et dialoguer avec un serveur DHCP.

Le message particulier va être reçu par toutes les machines connectées au réseau.

Lorsque le serveur DHCP le reçoit, il répond par un autre message de broadcast contenant toutes les informations requises pour la configuration.

III.8 Quelques protocoles d'administration et de gestion des VLANs [37] :

Il est possible de configurer les protocoles à la main pour permettre le transport des VLANs. Pour cela, il faut configurer chaque port se trouvant sur le chemin d'un port tagué d'un VLAN à un autre. Il faut de plus répéter l'opération pour chaque lien défini.

On peut comprendre que le processus s'avère long et fastidieux. La norme prévoit donc des mécanismes pour taguer les ports automatiquement et administrer les VLAN d'une manière plus simple, plus abrégée. Pour cela plusieurs protocoles ont été défini tels que le VTP, GVRP, DTP,802.1q.

Dans ce qui suit, nous n'allons définir que le protocole VTP propriétaire CISCO, lequel nous allons utiliser par la suite dans le chapitre réalisation.

III.8.1 Le protocole VTP (VLAN Trunking Protocol) [41] :

Le VTP (*Vlan Trunk Protocol*) est un protocole de niveau 2 utilisé pour configurer et administrer les VLANs sur les périphériques (commutateurs de N2 et 3) Cisco. Il permet d'ajouter, renommer ou supprimer un ou plusieurs VLANs sur le seul switch maître et dans un domaine VTP, Celui-ci propagera la modification de la configuration aux Switchs clients du réseau.

VTP permet ainsi d'éviter toute incohérence de configuration des VLANs sur l'ensemble d'un réseau local et il ne peut apprendre que les VLANs à plage normale et les stocke dans le fichier de base de données VLAN, Il ne prend donc pas en compte les VLANs à plage étendue.

III.8.1.1 Les modes de VTP [42] :

Les dispositifs de VTP peuvent être configurés pour fonctionner suivant les trois modes suivants :

A. **Mode serveur**, dans lequel le commutateur est chargé de diffuser la configuration aux commutateurs du domaine VTP.
B. **Mode client VTP**, dans lequel le commutateur applique la configuration émise par un commutateur en mode serveur.
C. **Mode transparent**, dans lequel le commutateur ne fait que diffuser, sans prendre en compte, la configuration du domaine VTP auquel il appartient.

III .8.2 VTP pruning [42] :

Un commutateur doit alors être déclare en serveur, on lui attribue également un nom de domaine VTP. C'est sur ce commutateur que chaque nouveau VLAN devra être défini, modifié ou supprimé. Ainsi chaque commutateur client présent dans le domaine héritera automatiquement des nouveaux VLANs crées sur le commutateur serveur.

La mise en place d'un domaine VTP permet de centraliser la gestion des VLANs, ce qui peut s'avérer plus que plaisant dans un environnement abondamment commuté et comprenant de multiples VLANs.

III 8.2.1 Exemple d'utilisation des VTP [37] :

Pour comprendre le fonctionnement des VTP, nous allons l'illustrer dans cet exemple ci-dessous (Figure 3.5**)**.

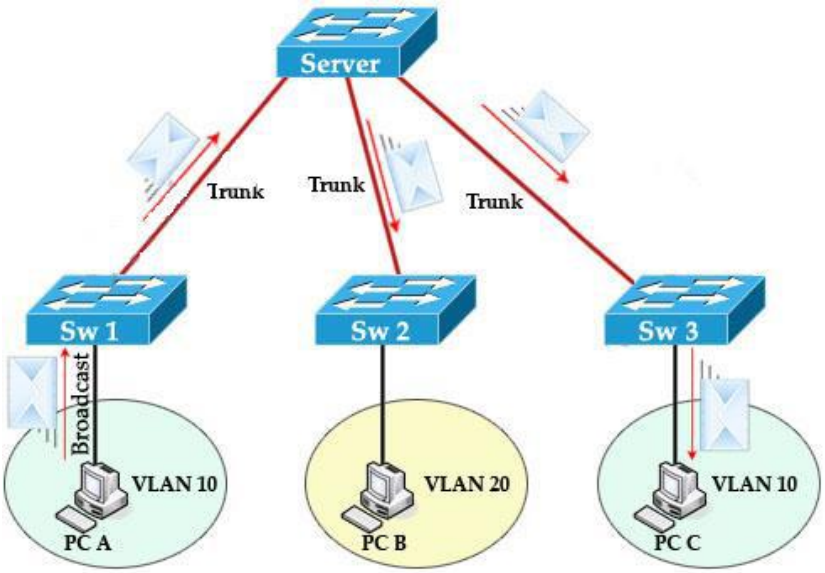


Figure 3.6 : Fonctionnement du protocole VTP[37].

Les administrateurs peuvent changer les informations des VLAN sur les switchs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens "trunk". En mode transparent, les modifications sont locales mais non distribuées. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP.

Les configurations VTP successives du réseau ont un numéro de révision. Si le numéro de révision reçu par un switch client est plus grand que celui en cours, la nouvelle configuration est appliquée. Sinon, elle est ignorée. Quand un nouveau switch est ajouté au domaine VTP, le numéro de révision de celui-ci doit être réinitialisé pour éviter les conflits.

III.9 les avantages de vlan [43] :

Les VLANs ont comme objectif principale la segmentation du réseau selon des critères logiques (les services, les accès...) afin d'atteindre les avantages suivants :

- **Simplification de la gestion :** l'ajout de nouveaux éléments ou le déplacement d'élément existant peut être réalisé rapidement et simplement sans devoir manipuler les connexions physiques dans le local technique.

- **Flexibilité de segmentation du réseau :** le regroupement des ressources et des utilisateurs sans devoir prendre en considération leur localisation physique.

- **Meilleure utilisation des serveurs réseaux :** quand un serveur possède une infrastructure compatible avec les VLANs, le serveur peut appartenir à plusieurs VLANs en même temps, ce qui permet de réduire le trafic qui doit être routé.

- **Renforcement de la sécurité du réseau :** les frontières virtuelles créées par les VLAN ne pouvant être franchies que par le biais de fonctionnalités de routage, la sécurité des communications est renforcée.

- **Technologie évolutive et à faible coût :** la simplicité de la méthode d'accès et la facilité de l'interconnexion avec les autres technologies ont fait d'Ethernet une technologie évolutive à faible coût quelles que soient les catégories d'utilisateurs.

- **Régulation de la bande passante :** un des concepts fondamentaux des réseaux ethernet est la notion d'émission d'un message réseau vers l'ensemble (broadcast ou multicast) des eléments connectés au même commutateur (hub/Switch).

Malheureusement, ce type d'émission augmente sérieusement le trafic réseau au sein du composant de connexion. Même si les vitesses de transmission ne cessent d'augmenter, il est important de pouvoir contrôler ce gaspillage de capacité de trafic (bande passante). Ici encore, le VLAN offre à l'administrateur les moyens de régler l'utilisation de la capacité de trafic disponible au sein de l'infrastructure.

III.10 Politique de sécurité du réseau LAN [44] :

Quelle que soit la nature des biens produit par l'entreprise, sa politique de sécurité réseau vise à satisfaire les critères suivants :

- Identification : information permettant d'indiquer qui vous prétendez être.
- Authentification : information permettant de valider l'identité pour vérifier que vous êtes celui que vous prétendez être.

- Autorisation : information permettant de déterminer quelles sont les ressources de l'entreprise auxquelles l'utilisateur identifié aura accès ainsi que les actions autorisées sur ces ressources.
- Confidentialité : ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire.
- Intégrité : ensemble des mécanismes garantissant qu'une information n'a pas été modifiée.
- Disponibilité : ensemble des mécanismes garantissant que les ressources de l'entreprise sont accessibles.
- Non-répudiation : mécanisme permettant de trouver qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.
- Traçabilité : ensemble des mécanismes permettant de retrouver les opérations réalisées sur les ressources de l'entreprise.
- Continuité : a pour but de garantir la survie de l'entreprise après un sinistre important touchant Le système informatique. Il s'agit de redémarrer l'activité le plus rapidement possible avec le minimum de perte de données.

III.10.1 La sécurisation des ports d'un commutateur [45] **:**

Avec les Switch Cisco, il est possible de faire un contrôle sur les ports en limitant l'accès à certaines adresses MAC, cela permet de sécuriser l'accès. Pour cela, il faut utiliser l'option " Port-Security ".

Il y a deux méthodes, la première consiste à enregistrer manuellement l'adresse MAC autorisée et la seconde consiste à prendre comme adresse MAC autorisée celle de l'hôte qui va se connecter et envoyer une trame en premier à ce port du Switch Cisco.

III.10.2 Les ACLs (Les listes de contrôles d'accès) [46] :

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonctions d'un certain nombre de critères, tels que :

- L'adresse d'origine.
- L'adresse de destinataire.
- Le numéro de port.
- Les protocoles de conches supérieures.

- Autres paramètres (exemple Horaire).

Les listes de contrôle d'accès permettent à un administrateur de gérer le trafic et d'analyser des paquets particuliers. Elles sont ainsi associées à une interface du routeur, et tout trafic acheminé par cette interface est vérifié afin d'y déceler certains conditions faisant partie de la liste de contrôle d'accès.

III.10.2.1 Fonctionnement [46] :

Les ACL permettent de filtrer les paquets, ce filtrage se faire en fonction de certains critères : adresse IP source, adresse IP de destination, port source, port destination, ou bien par des protocoles des couches supérieures.

Leur fonctionnement peut se résumer de la manière suivante:

- Le paquet est vérifié par rapport au premier critère.
- S'il vérifiée critère, l'action définie est appliquée.
- Sinon le paquet est comparé successivement par rapport au ACL suivants.
- S'il satisfait aucun critère, l'action «deny »est appliquée. Les critères sont définit dans les en-têtes IP, TCP ou UDP.

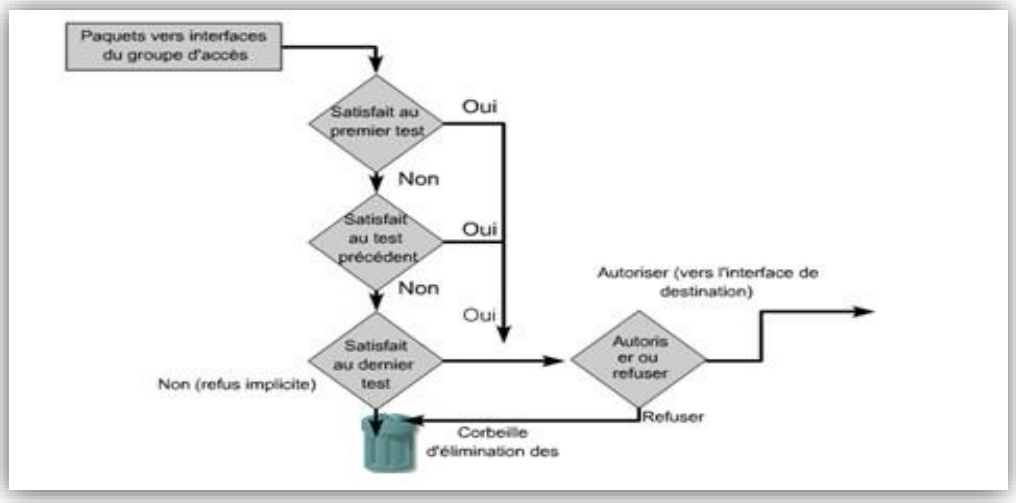


Figure 3.7 : organigramme qui résumée fonctionnement des ACL [46]**.**

III.10.3.2 Les type des ACLS [46] :

Il existe trois types de liste de contrôle d'accès :

- ✓ **Listes de contrôle d'accès standard :** Utilisent des spécifications d'adresses simplifiées et autorisent ou refusent un ensemble de protocole. Les ACLs standards sont à appliquer le plus proche possible de la destination raison de leur fiable précision.

- ✓ **Listes de contrôle d'accès étendues :** Utilisent des spécifications d'adresses plus complexes et autorisent ou refusent des protocoles précis. Les ACLs étendues sont à appliquer le plus proche possible de la source.

- ✓ **Listes de contrôle d'accès nommées :** Peuvent être soit standard, soit étendues, elle n'a pour but que de faciliter la compréhension et de connaitre la finalité de l'ACL.

III.10.2.3 Les listes de contrôles d'accès (ACL) [33] :

Les listes de contrôle d'accès sont des listes de conditions qui sont appliquées généralement au trafic circulant via une interface de routeur. La figure 3.7 montre un Organigramme qui résume le fonctionnement des ACL. Ces listes indiquent au routeur les types de paquets à accepter ou à rejeter. L'acceptation et le refus peuvent être basés sur des conditions précises.

Les ACLs permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie. Des listes de contrôle d'accès peuvent être créées pour tous les protocoles routés, tels que les protocoles IP (Internet Protocol) et IPX (Internet work Packet Exchange). Des listes de contrôle d'accès peuvent également être configurées au niveau du routeur en vue de contrôler l'accès à un réseau ou à un sous-réseau.

La figure 3.8 explique architecteur d'utilisation d'ACL.

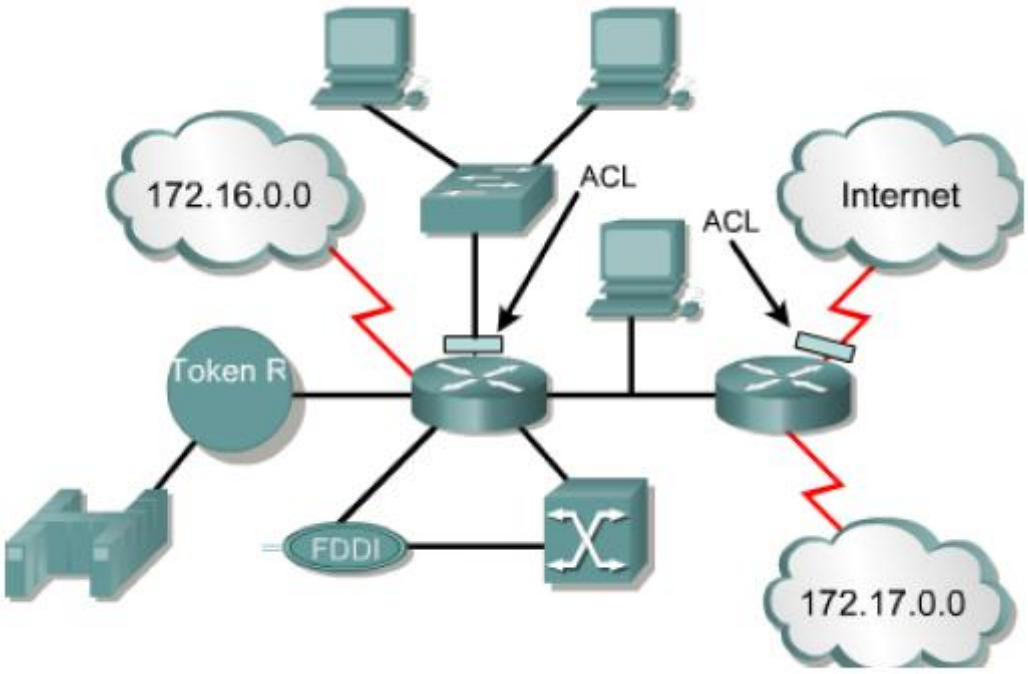


Figure 3 .8 : architecteur d'utilisation de l'ACL [33].

III.10.3.4 L'intérêt d'utiliser des ACL:

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès :

- Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances
- Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée
- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces du routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.

 Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

Conclusion :

Dans ce chapitre on a présenté les réseaux VLANs et leur intérêt de point de vue sécurité. On a présenté aussi les différents types des VLANs. Enfin on a introduit quelques protocoles d'administration et de gestion des VLANs et Les listes de contrôles d'accès qui vont nous aider à concevoir notre propre VLAN dans le chapitre qui suit.

Chapitre IV :

Simulation et réalisation

Chapitre IV: Simulation et réalisation

Introduction

Dans ce chapitre, nous allons passer à la dernière étape qui est la réalisation. Cette phase est cruciale pour la mise en place de tout ce que nous avons vu et fait auparavant, nous implémenterons la solution précédemment proposée et conçu, pour ce faire nous commencerons par la présentation du simulateur utilisé, puis nous expliquerons en détail les différentes étapes suivies pour la réalisation de l'architecture LAN et la création des VLANs.

IV.1. Présentation du simulateur Cisco « Packet Tracer » :

Packet tracer est un simulateur de réseau puissant développé par Cisco Systems pour faire des plans d'infrastructure de réseau en temps réel. il offre la possibilité de créer, visualiser et de simuler les réseaux informatiques. L'objectif principal de simulateur est de schématiser, configurer et de voir toutes les possibilités d'une future mise en œuvre réseau.

Cisco Packet Tracer est un moyen d'apprentissage de la réalisation de divers réseaux et découvrir le fonctionnement des différents éléments constituant un réseau informatique [44].

La figure 4.1 est une image montrant l'interface principale du simulateur Cisco Packet Tracer:

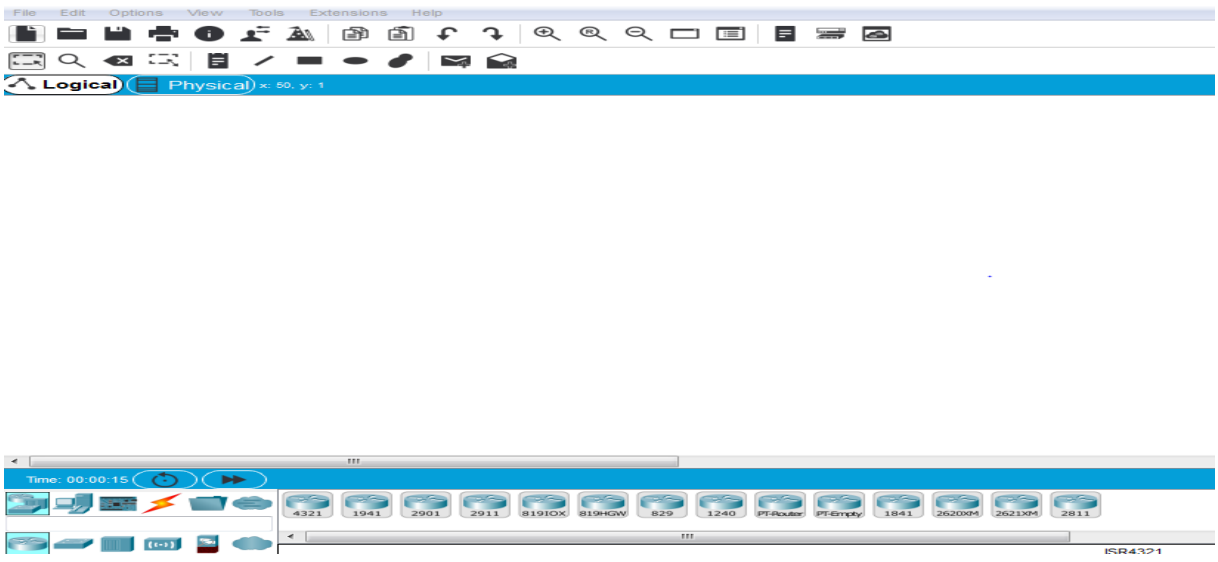


Figure 4.1 : L'interface de simulateur "Cisco Packet Tracer".

IV.2 Schéma d'architecteur :

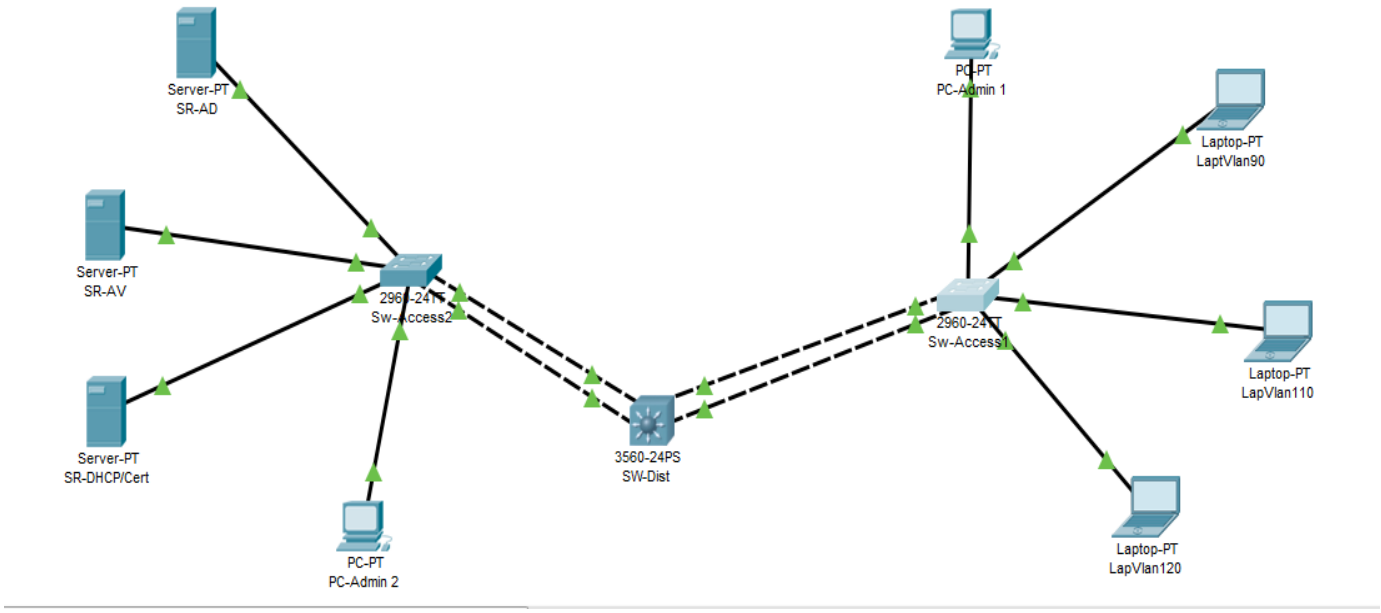


Figure 4.2 : Architecteur de réseau.

IV.3 La réalisation :

IV.3.1Configuration des adresses IP :

- Adresse IP du serveur DHCP :

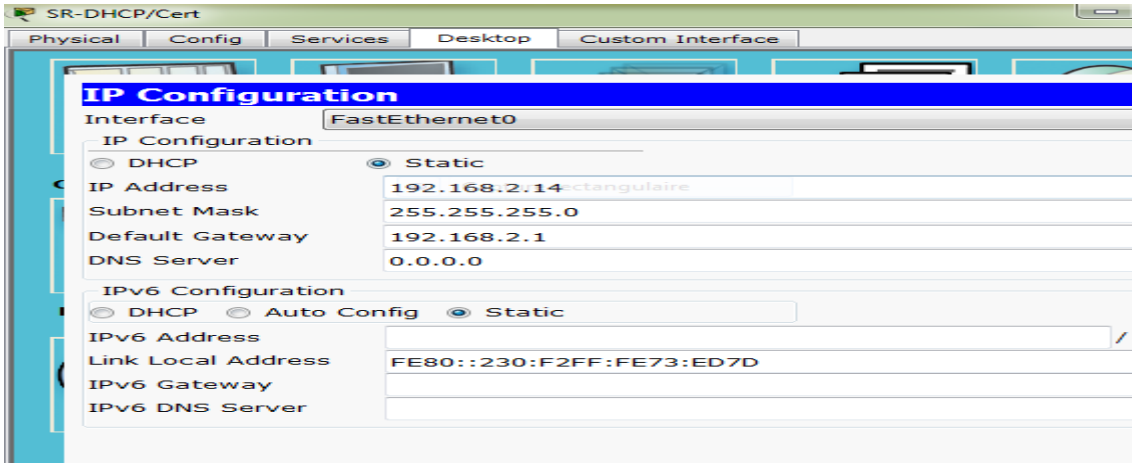


Figure 4.3 : adresse IP du serveur DHCP.

- Adresse ip du serveur Anti-virus :
  - On attribue l'adresse IP : 192.168.2.152/24 au server ANTI-VIRUS.

- Adresse ip du serveur d'AD :
  - On attribue l'adresse IP : 192.168.2.210/24.

- Adresse ip du PC administrateur 1 :
  - On attribue l'adresse IP : 192.168.213.15/24.
- Adresse ip du PC administrateur 2 :
  - On attribue l'adresse IP : 192.168.213.25/24.

IV.3.2 Configuration des interfaces en mode Trunk :

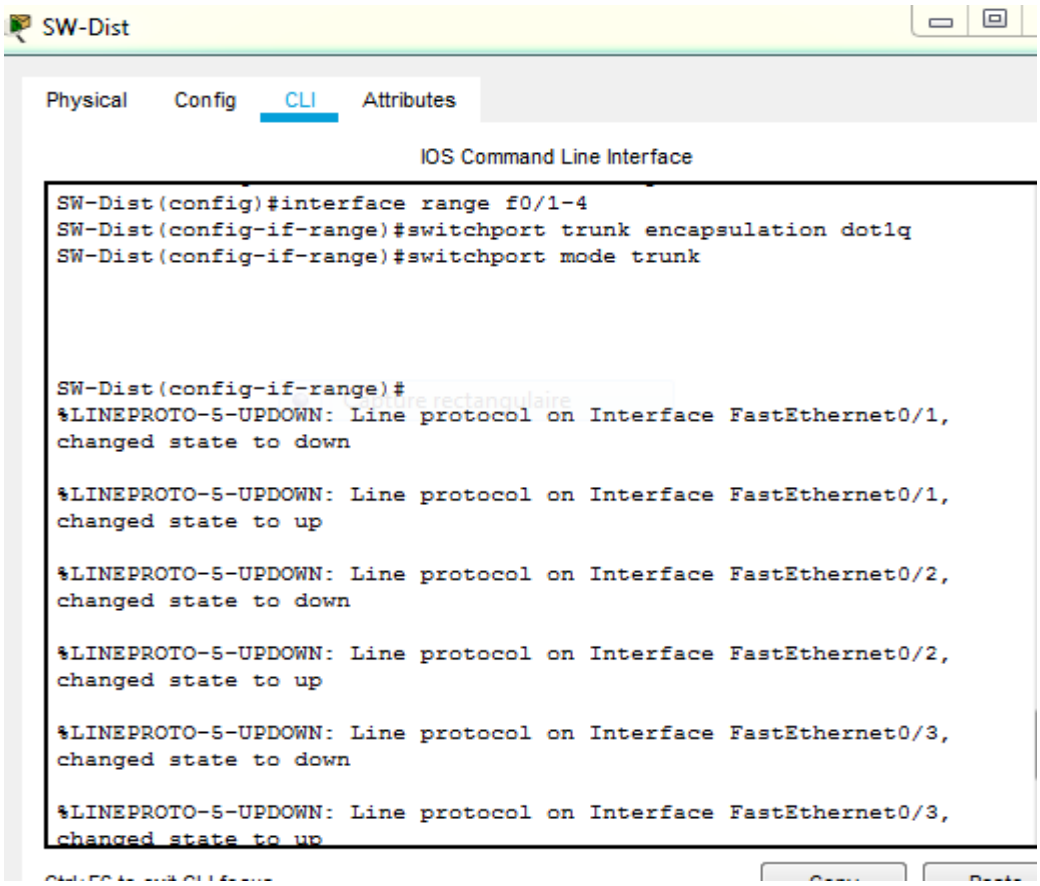


Figure 4.4 : Configuration des interfaces en mode Trunk .

IV.3.3 Configuration du protocole VTP server :

```
SW-Dist(config)#vtp domain stage
Changing VTP domain name from NULL to stage
SW-Dist(config)#vtp password stage
Setting device VLAN database password to stage
SW-Dist(config)#vtp mode server
Device mode already VTP SERVER.
SW-Dist(config)#vtp version 2
```

Figure 4.5: Configuration du protocole VTP server .

IV.3.4 : création des VLANs :

- Création des VLANs et l'attribution des adresses IP aux interfaces VLANs :
  - Vlan 2 et 6 :

```
SW-Dist#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW-Dist(config)#vlan 2
SW-Dist(config-vlan)#name DHCP
SW-Dist(config-vlan)#interface vlan 2
SW-Dist(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan2, changed state
to up

SW-Dist(config-if)#ip address 192.168.2.1 255.255.255.0
SW-Dist(config-if)#no sh
SW-Dist(config-if)#ex
SW-Dist(config)#vlan 6
SW-Dist(config-vlan)#name mgmt-SW
SW-Dist(config-vlan)#interface vlan 2
SW-Dist(config-if)#ip address 192.168.213.1 255.255.255.0
SW-Dist(config-if)#no sh
```

Figure 4.6: Attribution des adresses IP aux Vlan 2 et 6.

- Vlan 90 et 110 :

```
SW-Dist(config-if)#ip address 192.168.90.1 255.255.255.0
SW-Dist(config-if)#NO SH
SW-Dist(config-if)#EXIT
SW-Dist(config)#vlan 90
SW-Dist(config-vlan)#name DRH-DFO
SW-Dist(config-vlan)#interface vlan 90
SW-Dist(config-if)#ip address 192.168.90.1 255.255.255.0
SW-Dist(config-if)#ip helper-address 192.168.2.14
SW-Dist(config-if)#NO SH
SW-Dist(config-if)#EXIT
SW-Dist(config)#vlan 110
SW-Dist(config-vlan)#name DSI
SW-Dist(config-vlan)#interface vlan 110
SW-Dist(config-if)#
%LINK-5-CHANGED: Interface Vlan110, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan110, changed state to
up

SW-Dist(config-if)#ip address 192.168.110.1 255.255.255.0
SW-Dist(config-if)#ip helper-address 192.168.2.14
SW-Dist(config-if)#no sh
SW-Dist(config-if)#exit
```

Figure 4.7: Attribution des adresses IP aux Vlan 90 et 110.

- Vlan 120 :

```
SW-Dist(config-vlan)#exit
SW-Dist(config)#vlan 120
SW-Dist(config-vlan)#name DAL
SW-Dist(config-vlan)#interface vlan 120
SW-Dist(config-if)#
%LINK-5-CHANGED: Interface Vlan120, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan120, changed state to
up

SW-Dist(config-if)#ip address 192.168.120.1 255.255.255.0
SW-Dist(config-if)#NO SH
SW-Dist(config-if)#EXIT
```

Figure 4.8: Attribution d'adresses IP au Vlan 120.

- L'application de la commande **IP routing :**
  - Pour activer le routage :

```
SW-Dist(config)#ip routing
```

Figure 4.9 : La commande d'activation du routage.

IV.3.5 La configuration du Telnet :

```
SW-Dist(config)#line vty 0 15
SW-Dist(config-line)#password mobilis1
SW-Dist(config-line)#login
SW-Dist(config-line)#exit
```

Figure 4.10: configuration du Telnet.

IV.4 Configuration du lien Trunk sur Switch Access 1:

```
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname SW-access1
SW-access1(config)#interface range g0/1-2
SW-access1(config-if-range)#switchport mode trunk
SW-access1(config-if-range)#no sh
SW-access1(config-if-range)#ex
```

Figure 4.11: Configuration du lien Trunk sur Switch Access 1.

IV.4.1Configuration du protocole VTP Client sur Switch Access 1 :

- le même domaine du VTP server et le même mot de passe configuré sur Sw-Dis.

```
SW-Access1(config)#vtp domain stage
Domain name already set to stage.
SW-Access1(config)#vtp password stage
Setting device VLAN database password to stage
SW-Access1(config)#vtp mode client
Setting device to VTP CLIENT mode.
```

Figure 4.12 : Configuration du protocole VTP Client.

- La vérification des VLANs :

```
SW-Access1(config)#do sh vlan

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3,
Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7,
Fa0/8
                                                Fa0/9, Fa0/10,
Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14,
Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18,
Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22,
Fa0/23, Fa0/24
                                                Gig0/2
2    DHCP                             active
6    mgmt-sw                          active
90   DRH-DFO                          active
110  DSI                              active
120  DAL                              active
```

Figure 4.13 : Les VLANs du Switch Access 1.

IV.4.2 Attribution des interfaces VLANs :

- Attribution d'adresse a l'interface Vlan 6:
  - On donne l'adresse IP : 192.168.213.2 à l'interface VLAN 6 pour que le SW-Access1 puisse communiquer avec le SW-Dist.
- Attribution des interfaces aux différents VLANs et les configurés en mode Access :

- Pour le vlan 90 :

```
SW-access1(config)#interface f0/4
SW-access1(config-if)#switchport mode access
SW-access1(config-if)#switchport access vlan 90
SW-access1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/4 but will only
have effect when the interface is in a non-trunking mode.
SW-access1(config-if)#no sh
SW-access1(config-if)#exit
```

Figure 4.14 : Attribution d'interface au VLAN 90et le configuré en mode Access.

❖ La même attribution des interfaces vlan 110 et 120 appliquée sur vlan 90.

➢ Utilisation de la commande **IP default-gateway :**

```
SW-Access1(config)#ip default-gateway 192.168.213.1
```

Figure 4.15 : Gateway du SW-Dis pour le Switch Access 1.

IV.4.3 Configuration du Vty:

```
SW-Access1(config)#enable password mobilis2
SW-Access1(config)#line vty 0 15
SW-Access1(config-line)#password mobilis2
SW-Access1(config-line)#login
```

Figure 4.16: configuration du Vty.

- Configuration d'interface pc administrateur1 en mode Access:

```
SW-access1(config-if)#switchport mode access
SW-access1(config-if)#switchport access vlan 6
SW-access1(config-if)#spanning-tree portfast
%Warning: portfast should only be enabled on ports connected to a
single
host. Connecting hubs, concentrators, switches, bridges, etc... to
this
interface  when portfast is enabled, can cause temporary bridging
loops.
Use with CAUTION

%Portfast has been configured on FastEthernet0/3 but will only
have effect when the interface is in a non-trunking mode.
SW-access1(config-if)#no sh
SW-access1(config-if)#exit
```

Figure 4.17: Configuration d'interface pc administrateur1 en mode Access.

IV.5 Configuration des interfaces en Mode Trunk sur switch access 2 :

- On configure les interfaces g0/1-2 entre le Switch access2 et le Switch distributeur comme dans le Switch Access 1.

- Vérification :

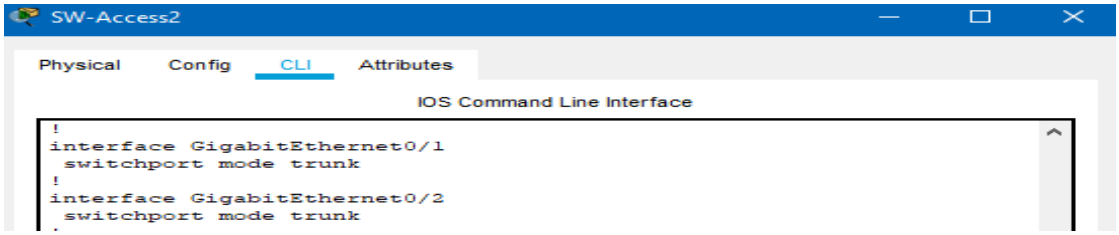


Figure 4.18: vérification du mode trunk.

IV.5.1 Configuration du protocole VTP Client sur Switch Access 2:

- le même domaine créer dans le Switch distributeur et le même mot de passe.

IV.5.2 Attribution des interfaces VLANs :

- Attribution de l'interface 0/2 au vlan 2.
- Attribution d'adresse IP a l'interface vlan 6.

```
SW-Access2(config)#interface vlan 6
SW-Access2(config-if)#
%LINK-5-CHANGED: Interface Vlan6, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan6, changed state
to up

SW-Access2(config-if)#
SW-Access2(config-if)#ip address 192.168.213.3 255.255.255.0
SW-Access2(config-if)#no sh
SW-Access2(config-if)#exit
```

Figure 4.19: Attribution d'adresse a l'interface vlan 6.

- Utilisation de la commande **IP default-Gateway :**

```
SW-Access2(config)#ip default-gateway 192.168.213.1
```

Figure 4.20: Gateway du SW-DIS sur le Switch Access.

IV.5.3 Configuration du Telnet sur Switch Access 2:

```
SW-Access2(config)#line vty 0 15
SW-Access2(config-line)#password mobilis3
SW-Access2(config-line)#login
SW-Access2(config-line)#exit
SW-Access2(config)#enable password mobilis3
```

Figure 4.21 : configuration de Telnet.

- Configuration d'interface du pc administrateur 2 en mode Access :
  - Même configuration appliquer sur pc administrateur (on configure l'interface f0/1 du pc administrateur 2 en mode Access et en lui attribue le vlan 6).

IV.6 Configuration du server DHCP :

- On utilise cette commande pour tout les VLANS dans SW-Dist

```
SW-Dist(dhcp-config)#ip dhcp pool DAL
SW-Dist(dhcp-config)#network 192.168.120.2 255.255.255.0
SW-Dist(dhcp-config)#default-router 192.168.120.1
```

Figure 4.22 : Configuration le pool d'adresses sur SW-Dist.

- **Configuration des pc en mode DHCP :**
  - Pc du vlan 90 :

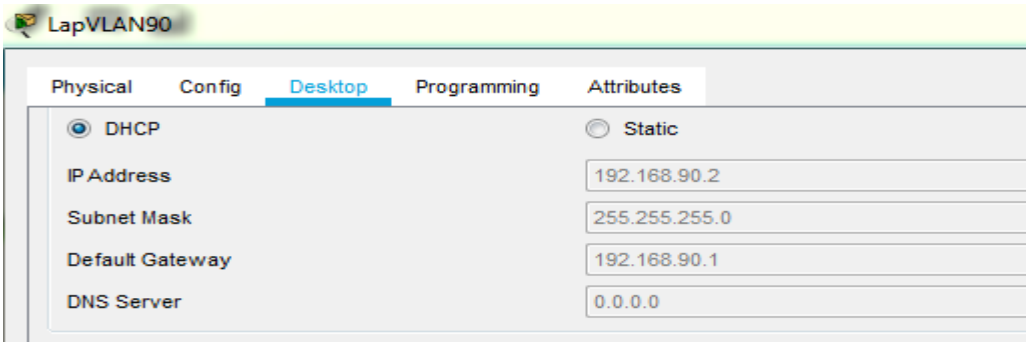


Figure 4.23: Adresse attribuer par DHCP pour pc vlan 90.

  - Pc du vlan 110 :

Figure 4.24 : Adresse attribuer par DHCP pour pc vlan 110.

- Pc du vlan 120 :

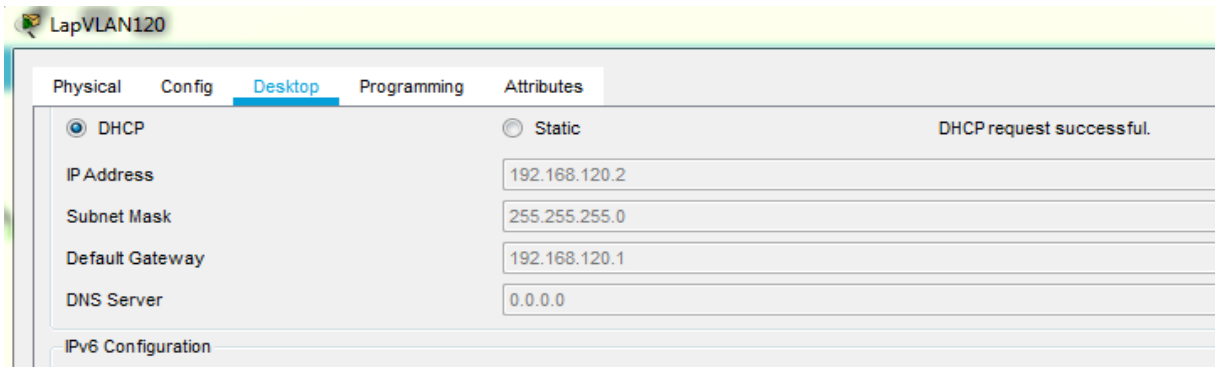


Figure 4.25 : Adresse attribuer par DHCP pour pc vlan 120.

IV.7La configuration d'EtherChannel :

❖ Sur Switch distributeur :

- Coté Switch Access 1 :

```
SW-Dist(config)#interface range f0/1-4
SW-Dist(config-if-range)#channel-protocol pagp
SW-Dist(config-if-range)#channel-group 1 mode desirable
SW-Dist(config-if-range)#no sh
SW-Dist(config-if-range)#exit
```

Figure 4.26: le mode de négociation et l'interface Etherchannel sur SW-Dist.

- Configuration de l'interface précédemment créé

```
SW-Dist(config)#interface port-channel 1
SW-Dist(config-if)#switchport trunk encapsulation dot1q
SW-Dist(config-if)#switchport mode trunk
SW-Dist(config-if)#no sh
SW-Dist(config-if)#exit
```

Figure 4.27: configuration de l'interface Etherchannel sur SW-Dist.

➢ Coté Switch Access 2 :

```
SW-Dist(config-if-range)#interface range f0/1-6
SW-Dist(config-if-range)#channel-protocol pagp
SW-Dist(config-if-range)#channel-group 2 mode desirable

SW-Dist(config-if-range)#no sh
```

Figure 4.28: Le mode de négociation et l'interfaces EtherChannel sur Switch Access.

- Configuration de l'interface précédemment créé:

```
SW-Dist(config)#interface port-channel 2
SW-Dist(config-if)#switchport trunk encapsulation dot1q
SW-Dist(config-if)#switchport mode access
SW-Dist(config-if)#no sh
SW-Dist(config-if)#exit
```

Figure 4.29 : configuration de l'interface EtherChannel sur SW-Dist.

❖ **Sur Switch access 1 :**

```
SW-access1(config)#interface range g0/1-2
SW-access1(config-if-range)#channel-protocol pagp
SW-access1(config-if-range)#channel-group 1 mode desirable
SW-access1(config-if-range)#
Creating a port-channel interface Port-channel 1

SW-access1(config-if-range)#no sh
SW-access1(config-if-range)#exit
```

Figure 4.30 : Le mode de négociation et l'interfaces EtherChannel sur Switch Access1.

- Configuration de l'interface précédemment créé:

```
SW-access1(config)#interface port-channel 1
SW-access1(config-if)#switchport mode trunk
SW-access1(config-if)#no sh
SW-access1(config-if)#exit
```

Figure 4.31 : configuration de l'interface EtherChannel sur Switch Access 1.

❖ **Sur Switch accès 2 :**

➢ la même configuration appliquée sur Switch access1.

IV.7.1Vérification de la configuration d'EtherChannel :

- **Sur Switch accès 2 :**
  - Affichage de la ligne d'information pour chaque groupe de canaux sur switch access2 :

```
SW-Access2#sh etherchannel summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------
+-----------------------------------------------

2      Po2(SD)           PAgP   Gig0/1(D) Gig0/2(D)
SW-Access2#
```

Figure 4.32 : la ligne d'information de groupe de canaux d'EtherChannel sur Switch Access 2.

  - Affichage des informations concernant l'interface port-channel1 sur Switch Access 2 :

```
SW-Access2#sh etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 2
----------
                Port-channels in the group:
                ---------------------------

Port-channel: Po2
------------

Age of the Port-channel   = 00d:00h:05m:29s
Logical slot/port   = 2/2       Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel
Protocol            =   PAGP
Port Security       = Disabled
```

Figure 4.33: les informations concernant l'interface port-channel1sur Switch access2.

- **Sur Switch accès 1:**
  - le même affichage appliqué sur Switch access2.

IV .8 Sécurisation des ports des Switch :

- Configuration des accès aux ports :
  - On active la sécurité des ports sur les interfaces f0/1 du Switch Access 1 et 2 :

```
SW-access1(config-if)#interface f0/1
SW-access1(config-if)#switchport mode access
SW-access1(config-if)#switchport port-security
SW-access1(config-if)#switchport port-security mac-address
000C.CFA3.9A01
SW-access1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to
administratively down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down

SW-access1(config-if)#NO SH

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to down
SW-access1(config-if)#EXIT
```

Figure 4.34 : Activation de la sécurité des ports sur Switch Access 1.

```
SW-Access2(config)#interface f0/1
SW-Access2(config-if)#switchport mode access
SW-Access2(config-if)#switchport port-security
SW-Access2(config-if)#switchport port-security mac-address
0001.97DB.D101
SW-Access2(config-if)#NO SH
SW-Access2(config-if)#EXIT
```

Figure 4.35: Activation de la sécurité des ports sur Switch Access 2.

- la sécurité des adresses mac :

❖ Sur switch access1

```
SW-access1(config-if-range)#interface range f0/2-6
SW-access1(config-if-range)#switchport mode access
SW-access1(config-if-range)#switchport port-security
SW-access1(config-if-range)#switchport port-security maximum 1
SW-access1(config-if-range)#switchport port-security mac-address
sticky
SW-access1(config-if-range)#switchport port-security violation
restrict
SW-access1(config-if-range)#no sh
SW-access1(config-if-range)#exit
```

Figure 4.36: sécurité d'interface utilisée par un seul périphérique sur Switch Access 1.

❖ Sur switch access2 :

- La même sécurité appliquée sur switch access 1

IV.9 La configuration des ACL :

IV.9.1 Création de listes d'ACL :

```
SW-Dist(config)#ip access-list extended ACL_VLAN
SW-Dist(config-ext-nacl)#permit icmp 192.168.90.0 0.0.0.255
192.168.2.0 0.0.0.255 echo-reply
SW-Dist(config-ext-nacl)#permit icmp 192.168.90.0 0.0.0.255
192.168.110.0 0.0.0.0.255 echo-reply

^
% Invalid input detected at '^' marker.

SW-Dist(config-ext-nacl)#permit icmp 192.168.90.0 0.0.0.255
192.168.110.0 0.0.0.255 echo-reply
SW-Dist(config-ext-nacl)#permit icmp 192.168.90.0 0.0.0.255
192.168.213.0 0.0.0.255 echo-reply
SW-Dist(config-ext-nacl)#deny ip 192.168.90.0 0.0.0.255 192.168.2.0
0.0.0.255
SW-Dist(config-ext-nacl)#deny ip 192.168.90.0 0.0.0.255 192.168.110.0
0.0.0.255
SW-Dist(config-ext-nacl)#deny ip 192.168.90.0 0.0.0.255 192.168.213.0
0.0.0.255
SW-Dist(config-ext-nacl)#permit ip any any
SW-Dist(config-ext-nacl)#exit
```

Figure 4.37: La liste d'ACL appliqué.

IV.9.2 L'application des ACLs sur l'interface VLAN 90 :

```
SW-Dist(config)#interface vlan 90
SW-Dist(config-if)#ip access-group ACL_VLAN in
SW-Dist(config-if)#no sh
SW-Dist(config-if)#exit
```

Figure 4.38: application des ACLs sur l'interface VLAN 90.

IV.10 Test des Ping :

- test du Ping depuis le pc administrateur1 par Telnet
  - Entre Switch distributeur et le Switch Access 1 et 2 :

```
SW-Dist#ping 192.168.213.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.213.2, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/1/3 ms

SW-Dist#ping 192.168.213.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.213.3, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/1/3 ms
```

Figure 4.39 : Le Ping au Switch Access 1 et 2 depuis le SW-Dist.

- Entre Switch distributeur et les pc 1 /2/3 :

```
SW-Dist#ping 192.168.90.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.90.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 3/3/3 ms

SW-Dist#ping 192.168.110.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/4 ms

SW-Dist#ping 192.168.120.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.120.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/2/3 ms
```

Figure 4.40 : Le Ping les pc du vlan 90, 110,120 depuis le SW-Dist.

- Entre Switch Access 1 et le Switch distributeur :

```
SW-access1#ping 192.168.213.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.213.1, timeout is 2
seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/1 ms

SW-access1#
```

Figure 4.41: Le Ping au SW-Dist depuis Switch Access 1.

- Test du Ping entre Switch Access 1 et les pc 1/2/3 :

```
SW-access1#ping 192.168.90.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.90.2, timeout is 2 seconds:
..!!!
Success rate is 60 percent (3/5), round-trip min/avg/max = 0/0/0 ms

SW-access1#ping 192.168.110.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.110.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-access1#ping 192.168.120.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.120.2, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Figure 4.42 : Le Ping au pc du vlan 90, 110,120 depuis le Switch Access 1.

- Entre le Switch Access 1 et le server DHCP :

```
SW-access1>en
Password:
SW-access1#ping 192.168.2.14

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.14, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

SW-access1#
```

Figure 4.43: Ping entre le Switch Access 1 et le server DHCP.

- Test du Ping pour tester la liste d'ACL appliqué :
  - Ping au Switch Access 1 :192.168.213.2 depuis le pc du vlan 90.

```
C:\>ping 192.168.213.2

Pinging 192.168.213.2 with 32 bytes of data:

Reply from 192.168.90.1: Destination host unreachable.
Reply from 192.168.90.1: Destination host unreachable.
Reply from 192.168.90.1: Destination host unreachable.
Reply from 192.168.90.1: Destination host unreachable.

Ping statistics for 192.168.213.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 4.44 : Ping au Switch Access 1 depuis le pc du vlan 90.

- Ping au pc du vlan 110 depuis le pc du vlan 90:

```
C:\> ping 192.168.110.2

Pinging 192.168.110.2 with 32 bytes of data:

Reply from 192.168.90.1: Destination host unreachable.
Reply from 192.168.90.1: Destination host unreachable.
Reply from 192.168.90.1: Destination host unreachable.
Reply from 192.168.90.1: Destination host unreachable.

Ping statistics for 192.168.110.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Figure 4.45 : Ping au pc du vlan 110 depuis le pc vlan 90.

- Ping au pc du vlan 90 depuis le pc de vlan 110 :

```
Pinging 192.168.90.2 with 32 bytes of data:

Reply from 192.168.90.2: bytes=32 time=21ms TTL=127
Reply from 192.168.90.2: bytes=32 time<1ms TTL=127
Reply from 192.168.90.2: bytes=32 time<1ms TTL=127
Reply from 192.168.90.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.90.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 21ms, Average = 5ms
```

Figure 4.46 : Ping du pc vlan 110 vers le pc vlan 90.

- Ping au pc administrateur 1 depuis le switch access 1 :

```
SW-access1#ping 192.168.213.15

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.213.15, timeout is 2
seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Figure 4.47 : Ping du Switch Access 1 vers le pc administrateur 1.

- Ping au pc vlan 90 depuis le pc vlan 120 :

```
C:\>ping 192.168.90.2

Pinging 192.168.90.2 with 32 bytes of data:

Reply from 192.168.90.2: bytes=32 time=16ms TTL=127
Reply from 192.168.90.2: bytes=32 time<1ms TTL=127
Reply from 192.168.90.2: bytes=32 time<1ms TTL=127
Reply from 192.168.90.2: bytes=32 time=10ms TTL=127

Ping statistics for 192.168.90.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 16ms, Average = 6ms
```

Figure 4.48: Ping du pc vlan 120 vers pc vlan 90.

- Ping au pc vlan 110 depuis pc vlan 120 :

```
C:\>ping 192.168.110.2

Pinging 192.168.110.2 with 32 bytes of data:

Reply from 192.168.110.2: bytes=32 time<1ms TTL=127
Reply from 192.168.110.2: bytes=32 time<1ms TTL=127
Reply from 192.168.110.2: bytes=32 time<1ms TTL=127
Reply from 192.168.110.2: bytes=32 time<1ms TTL=127

Ping statistics for 192.168.110.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure 4.49 : Ping du pc Vlan 120 vers pc vlan 110.

Conclusion :

Au cours de ce chapitre nous avons pu décrire la procédure de configuration concernant les VLANS et la sécurité des ports, sur le réseau local de Mobilis.

Et on a utilisé le Protocol d'agrégation des liens qui permet d'augmenter la vitesse et la tolérance aux pannes entre commutateurs et les ACLs qui servent a filtré le trafic du réseau.

Conclusion général :

La sécurité des réseaux informatiques et particulièrement celle des réseaux locaux est en évolution ceci est dut à l'ouverture des systèmes informatiques sur internet. Les menaces peuvent se produire au niveau externe comme au niveau interne, de ce fait les entreprises doivent protéger leurs réseaux en implémentant le maximum des techniques de sécurités.

Notre travail s'est porté sur les différentes techniques de sécurité dans un réseau local, soit celles qui existe dans le réseau d'ATM Mobilis ou celles proposés afin de régler quelques problèmes de sécurité.

Les techniques de sécurité que nous avons configurée répondent à un pourcentage important aux exigences de sécurité, d'où la protection du réseau des menaces interne ou externe.

Ce projet de fin d'étude nous a permis d'enrichir nos connaissances et de perfectionner nos acquis notamment dans le domaine des réseaux informatiques.
L'étude et la présentation de ce modeste travail, nous a permis de mettre en pratique nos connaissances théoriques et éventuellement d'enrichir d'autre.
Les attaques peuvent se produire à l'intérieur de l'entreprise (écoute sur le canal ou sur les ports), pour remédier à ce type d'attaque nous avons segmenté le réseau avec des VLANs .

Pour finir, en espérant avoir bien choisi le sujet et qu'il servira de base pour une éventuelle étude complémentaire et apportera un plus aux étudiants qui nous relèverons.

Bibliographie :

[1] :José.DORDOIGNE, Réseaux informatiques Notions fondamentales (Protocoles, Architectures, Réseaux sans fil, Virtualisation, Sécurité, IP v6,. . .). Editions ENI, Janvier 2013.

[2] : J.DORDOIGNE, réseau informatique, notion fondamentales, 4eme édition ENI, février 2011.

[3] :Https//www.ladissertation.com/Sciences-et-Technologies/Informatique-Internet/Reseaux-Informatiques-81608.html, consulté le 20 Avril 2016.

[4] : germain AFFRO Essan, Le réseau informatique dans la chaine de production d'une société de presse, 2010.

[5] : BAPTISTE Wicht, *Introduction au réseau*, source < http://baptiste-wicht.developpez.com/tutoriel/reseau/introduction/>,03 Mars 2007, consulté le 02 Avril 2012.

[6] : https://www.culture-informatique.net, dernier accès Avril 2017.

[7] : JF.PILLOU, Fabrice LEMAINAQUE, Tout sur les réseaux et internet, 4eme édition dunod, 3 juin 2015

[8] : G. PUJOLLE, Initiation aux réseaux, Édition eyrolles , 27 février 2014.

[9] : Philippe Atelin. Réseaux informatique notion fondamentales (normes, Architecture, model OSI, TCP/IP, Ethernet, wifi,...).Edition ENI ,2009

[10] :http://blog.devarieux.net/2009/08/qrqvb-le-modele-osi/

[11] :Khelalfa, Halim M, Introduction à la sécurité Informatique, SECINFO04,2000.

[12] : https://www.securiteinfo.com/conseils/introsecu.shtml, "Objectifs de la Sécurité informatique", dernier accès avril 2017.

[13] : https://www.securiteinfo.com Sécurité Dernier accès juin 2016.

[14] :C. L lorens L. Levier D. Valois. Tableaux de bord de la sécurité. Groupe Eyrolles, 2003-2006, ISBN : 2-212-11973-9.

[15] : J. DORDOIGNE. Réseaux informatiques, édition eni 4. Paris, 2011,482p.

[16] :C. Duret N. Gaillar. Les attaques internet et les moyens de s'en protéger. 2002.

[17] :http ://www.futura-sciences.com/magazines/high-tech/infos/dico/d/internet-firewall 474.

[18] : G.DESGEORGE. La sécurité des réseaux ,3eme édition Dunod ,2012

[19] :Cisco Systems. Cisco PIX Firewall and VPN Configuration Guide Version 6.3. Inc.170West Tasman Drive San Jose, CA 95134-1706 USA, 2001-2003.

[20] :http ://www.altern.org/trom tromh@yahoo.com.

[21] : G. Florin. Cours de sécurité Pare-feu ('Firewalls'). CNAM-Laboratoire CEDRIC, 2000.

[22] :Cyrille DUFRESNES. Pare-feu-Proxy-DMZ. in http ://notionsinformatique.free.fr, 08/06/2008.

[23] : S. GHERNAOUTI-HELIE, Sécurité informatique et réseaux, DUNOD, Paris, 2011.

[24] :MEDEF (Mouvement des Entreprises de France). GUIDE SSI Etablir une barrière de sécurité entre les données externes et internes, mai 2005.

[25] : https ://www.google.dz/DMZ/Images.

[26] :S. KEBAILI S. MEJBRI F. MKACHER M. BEN AMMAR I. KABOUBI et O.NEJI. SECURIDAY 2013 Cyber War. 2013.

[27] : J. ARCHIER, Les vpn, Édition eni, 2010,552P.

[28] : http://mariepascal.delamare.free.fr/IMG/pdf/cours DHCP.pdf.

[29]:Hhttps://www.ionos.fr/digitalguide/fileadmin/digitalGuide/schaubilder/attaque-mitm.png

[30]: https://avibasangi.files.wordpress.com/2015/03/les-diffc3a9rents-type-de-vlan.pdf

[31] : A. Mokhetari, La sécurité dans les Echanges et la Sauvegarde des Données, Université de Versailles.2000-2001.

[32] : JA. BUCHMANN, introduction à la cryptographie, 2eme édition Dunod ,2006.

[33] : mariepascal.delamare.free.fr/IMG/pdf/1_coursVlan_11.pdf

[34] : https://www.commentcamarche.net/contents/543-vlan-reseaux-virtuels

[35] : T.LAMMEL, CCNA CISCO certified network associate study guide ,6éme édition, 2007.

[36] : https://aresu.dsi.cnrs.fr Vlan Dernier accès juin 2016.

[37] : http : //www-igm.univ-mlv.fr type de vlan Dernier accès juin 2016.

[38] :F.NOLOT, cours les Virtual LAN, Université de Reims Champagne. Ardenne, "http://www.nolot.eu/Downlaod/Cours/rezo/AdminRS-Cours2-VLAN.pdf".

[39] : https://www.supinfo.com/.../733-configuration-routage-inter-vlan-layer-3-switch-cisc.

[40] :http://www.omnisecu.com/cisco-certified-network-associate-ccna/types-of-vlan-connection-trunk-links-and-access-links.php

[41] :"http://nobileteric.weebly.com/uploads/2/9/6/6/29668301/proc%C3%A9dure-vtp.pdf".

[42] : Florent Nolot, Des protocoles de Spanning Tree, Master2 informatique, Université de Reims, 2008.

[43] : T. KOUASSI, Etude et optimisation du réseau locale de inova si, Centre d'expertise et de Perfectionnement en informatique, Abidjan - Ingénieur, 2007.

[44] :COLLEGE Lionel-Groulx. Publication, politique de sécurité informatique, Page 5.

[45] : *Mémoire De Fin de cycle de Bejaïa* Thème Etude et amélioration de l'architecture et sécurité du réseau de l'EPB 2015/2016.

[46] :S.BOUBALOU et M.YOUSFI, Proposition d'une configuration sécurisée d'un réseau Local Cas d'étude : Entreprise NAFTAL, 2015/2016.

[47] : Réseaux informatiques, modèle OSI, protocole TCP/IP, 20/05/2010, 58pages.

[48] : T. Dean, Réseaux Informatique, 2ème édition, les Editions RYNALD GOULET, 2001.

[49] : LEMAINQUE Fabrice PILLOU Jean-François, Tout sur les Réseaux et Internet, 3eme édition, Dunod, 2012.

[50] : Collectif, Dictionnaire Hachette encyclopédie illustré, Paris, Ed. Hachette livre, 1998.

[51] : M.Badra, Le transport et la sécurisation des échanges sur les réseaux sans fil, thèse de doctorat, l'Ecole Nationnale Supérieure des Télécommunications, 2004.

[52] :Hhttps://www.ionos.fr/digitalguide/fileadmin/digitalGuide/screenshots/arp_spoofing-example.pn

[53] : Http//mtyas.com/2009/05/11/pourquoi-le-web-30-sera-p2p-ou-ne-sera-pas.consulté-le-02/05/2016.

[54] : *Mémoire De Fin de cycle de Bejaïa* Thème Administration et sécurisation d'un réseau LAN et mise en place d'une passerelle d'interconnexion sécurisée pour l'entreprise RAMINA 2016/2017.