République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Configuration et sécurisation de réseau de l'entreprise Général Emballage à base des Liaisons Virtuelles

---

Réalisé par :

Mlle. CHERAFT Célina et Mlle. TINOUILINE Ghada .

Evalué le 26/06/2023 devant le jury composé de :

Président	**Dr.ACHROUFENE Achour**	**U. A/Mira Béjaïa.**
Examinateur	**Dr. BOUZIDI Zair**	**U. A/Mira Béjaïa.**
Encadrant	**Dr. BOUDRIES Abdelmalek**	**U. A/Mira Béjaïa.**

Année universitaire 2022/2023

Dédicaces

Avec tous mes sentiments de respect, avec l'expérience de ma reconnaissance,

je dédie ma remise de diplôme et ma joie

À mon paradis, à la prunelle de mes yeux, à la source de ma joie et de mon bonheur, ma lune et le fil d'espoir qui illumine mon chemin, ma moitié,

Maman.

À celui qui m'a fait une femme, ma source de vie, d'amour et de paix,
À mon support qui était toujours à mes côtés pour me soutenir et m'encourager, à mon cher Papa, que Dieu l'accueille en son vaste paradis.

Papa.

À Mon frère d'amour 'Nabil' que j'aime beaucoup et à qui je souhaite une bonne réussite dans sa vie.

À mon cher mari.

À Mon exemple dans la vie, ma très chère cousine 'Wahiba'.

À Ma belle-mère, que Dieu la protège et lui donne une longue vie.

À toute ma famille et ma belle-famille.

À ma binôme Célina, avec qui j'ai partagé de belles années d'études.

Mes chers copines et amis.

Ghada.

Dédicaces

Avec une profonde estime et une gratitude infinie, Je dédie ce moment sacré

de ma remise de diplôme et de ma joie à ceux qui ont joué un rôle essentiel dans ma vie.

À toi, ma mère bien-aimée, mon refuge sacré, l'éclat dans mes yeux, la source intarissable de ma joie et de mon bonheur.
Tu es ma lune éclairant mon chemin, ma moitié précieuse.

chère maman.

À toi, mon père, celui qui m'a façonnée en tant que femme, ma source de vie, d'amour et de paix. Tu as été mon soutien constant, toujours à mes côtés pour me soutenir et m'encourager.

cher papa.

À mes frères chéris Tahar, Salah, Bilal, et Idir,et ma unique soeur d'amour , que j'aime énormément et à qui je souhaite une réussite éclatante dans leur vie.

À mon cher oncle, que Dieu l'accueille dans son vaste paradis, je dédie une pensée spéciale.
Ta bienveillance et ton soutien inconditionnel ont marqué ma vie à jamais.
Djaafar.

À mes cousines adorées Célina, Sofia, Ouassila et Zahoua,
votre présence colorée dans ma vie est une source d'inspiration constante. Vous êtes des piliers solides et je vous suis reconnaissante pour votre amour inébranlable.

À toute ma famille et mes chères amies Sabrina, Yasmine, Sabiha et Siham, je vous adresse cette dédicace. Votre amour et votre soutien indéfectibles ont été des piliers solides dans ma vie.

À ma binôme Ghada, avec qui j'ai partagé de merveilleuses années d'études, je te suis reconnaissante pour notre amitié sincère et notre collaboration précieuse.

Enfin, à tous mes chers amis, je vous adresse ma profonde gratitude. Votre amitié sincère et votre soutien inébranlable ont illuminé ma vie de joie et de rires.

Célina.

Remerciements

Avant d'entamer ce projet de fin de cyc, nous tenons à exprimer notre sincère gratitude envers notre promoteur Monsieur BOUDRIES Abdelmalek, pour ses précieux conseils, son orientation éclairée et son assistance précieuse tout au long de notre projet de fin de cycle .

Nous souhaitons également adresser nos remerciements les plus chaleureux au président et aux membres du jury pour avoir accepté de consacrer leur temps et leur expertise pour évaluer notre travail en profondeur.

Nous aimerions également exprimer notre profonde reconnaissance envers l'ensemble des enseignants et professeurs qui nous ont prodigué leur aide précieuse, sans oublier de remercier sincèrement tous ceux qui ont contribué, de près ou de loin, à la réalisation de notre mémoire .

Nous tenons également à exprimer notre gratitude envers le personnel de l'entreprise Général Emballage pour leur accueil chaleureux lors de notre stage pratique, qui nous a permis d'acquérir une expérience concrète et de mettre en pratique les connaissances acquises au cours de notre parcours universitaire.

Et enfin, que nos chers parents et familles, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleures conditions.

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

Liste des abréviations

ACK	ACKnowledged
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
DMZ	DeMilitarized Zone
DNS	Domain Name System
FDDI	Fiber Distributed Data Interface
FAI	Fournisseur d'Accès Internet
GNS3	Graphical Network Simulator
GLBP	(Gateway Load Balancing Protocol
HTTP	Hypertext Transfer Protocol
HSRP	Host Standby Router Protocol
IDS	Intrusion detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LAN	Local Area Network
MAN	Metropolitan Area Network
MAC	Media Access Control
NAT	Network Address Translation
OSI	Open Systems Interconnection
PAN	Personal Area Network
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
VRRP	Virtual Redondancy Protocol
VTP	VLAN Trunking Protocol
WAN	Wide Area Network

Introduction générale

Les entreprises dépendent de plus en plus de la connectivité réseau pour leurs opérations quotidiennes, qu'il s'agisse de la communication entre les employés, de l'accès à distance aux données et aux applications, ou de l'échange d'informations sensibles avec des partenaires commerciaux.

Dans un monde de plus en plus connecté, les réseaux d'entreprise doivent être flexibles, évolutifs et sécurisés pour répondre aux besoins croissants des entreprises.
La sécurité informatique est un élément crucial pour protéger les informations et les systèmes d'une entreprise et une branche de la technologie de l'information qui étudie et met en œuvre les menaces et les vulnérabilités des systèmes informatiques, en particulier dans le réseau, comme les virus, les vers, les chevaux de Troie, les cyberattaques , les attaques par invasion, le vol de données et l'intrusions.

Le présent mémoire de fin de cycle a pour objectif d'étudier le réseau de l'entreprise Générale Emballage, en effectuant une analyse de sa configuration actuelle et en proposant des solutions pour renforcer sa politique de sécurité.

Le réseau local de Générale Emballage joue un rôle essentiel dans les opérations quotidiennes de l'entreprise en permettant la communication et le partage d'informations entre les utilisateurs. Cependant, il est primordial de garantir la sécurité et la confidentialité des données échangées au sein du réseau.
Dans ce mémoire, nous proposerons une solution basée sur les liaisons virtuelles, telles que les VLAN (Virtual Local Area Network), les VPN (Virtual Private Network), l'agrégation des liens et la redondance. Ces technologies permettront d'améliorer l'exploitation et l'attribution du réseau, tout en assurant une communication sûre et confidentielle entre les utilisateurs de l'entreprise.

Nous procéderons à une évaluation approfondie du réseau actuel, en identifiant les faiblesses potentielles sur le plan de la sécurité et en proposant des mesures correctives appropriées. Nous aborderons également les meilleures pratiques en matière de configuration

des VLAN, des VPN, de l'agrégation des liens et de la redondance, afin de garantir une infrastructure réseau robuste et résiliente.

Notre projet comporte les chapitres suivants :

Le premier chapitre est consacré à la présentation de quelques généralités sur les réseaux informatiques .
Le chapitre suivant contient deux parties , la première présente une introduction à la sécurité informatique , les principales notions ainsi que les stratégies de sécurité. Dans la deuxième contient une présentation de l'organisme d'accueil Générale Emballage et les problématiques rencontrées lors de notre stage.
Au troisième, nous concentrons notre attention sur les concepts de bases des réseaux virtuels, nous mettons en outre l'accent sur les VLANs,VPNs. l'agrégation des liens et de la redondance .
Dans le dernier chapitre, nous avons présenté le principe de configuration du réseau de l'entreprise Générale Emballage, où nous avons proposé une solution et l'avons mise en œuvre.
Nous clôturons notre travail par une conclusion générale, qui résumera les connaissances acquises durant la réalisation du projet et proposera quelques perspectives futures.

CHAPITRE 1

GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES

1.1 Introduction

Un réseau peut être défini comme un ensemble de dispositifs inter-connectés qui peuvent communiquer et partager des ressources entre eux.

Dans ce chapitre, nous abordons les notions fondamentales des réseaux, notamment la classification des réseaux, les topologies, les périphériques réseau, les modèles OSI(Open Systems Interconnection)et TCP/IP (Transmission Control Protocol / Internet Protocol), ainsi que l'adressage. Ce qui nous permet de mieux cibler notre domaine de travail et d'approfondir nos connaissances de manière précise.

1.2 Définition d'un réseau et son intérêt

a)Définition d'un réseau informatique

Réseau informatique est Une série d'ordinateurs et de terminaux reliés entre eux qui partagent des données et des ressources et échangent des informations numériques. (Remarque : si vous avez deux ordinateurs connectés, vous disposez déjà d'un réseau. [**1**]

b)L'intérêt des réseaux informatiques

Parmi les objectifs et les intérêts des réseaux les plus remarquables, on peut noter les suivants :

- Partage de ressources : apporte un gain en matière de coût, du fait qu'il est possible de partager ce qui existe au lieu d'en acheter.

- Duplication d'information : Le partage d'information permet des duplications et des sauvegardes sur plusieurs sites.

- Tolérance aux pannes : un système centralisé se concentre sur une seule machine, dés qu'elle tombe en panne tout le système d'information se trouve paralysé.

Comme le réseau est constitué de plusieurs machines qui forment un système ce dernier n'est plus paralysé par la panne De l'une d'entre -elles. Services offerts par le réseau :

- Échange d'information.

- Communication (téléphone, mail...).

- Exécution à distance.

- Vidéo conférence.[**2**]

1.3 Classification des réseaux informatiques

On peut classer les réseaux selon superficie pouvant être couverte par le réseau c'est-à-dire :en fonction de la localisation, la distance et le débit.[**3**]

Donc nous pouvons classifier les réseaux informatiques de la manière présenté sur la figure 1.1 :

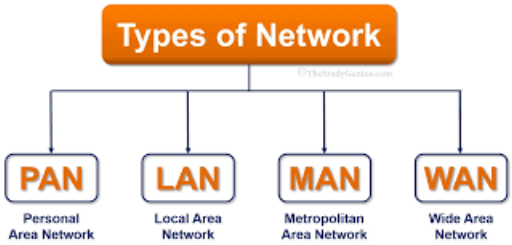

FIGURE 1.1 – Classification des réseaux informatiques.

a)LAN (Local Area Network ou Réseau Local) : Un LAN est un réseau situé généralement dans la même entité géographique (entreprise, campus,...) permettant de relier des ordinateurs et des périphériques situés à proximité les uns des autres destination comme illustré dans la figure 1.2[**3**].

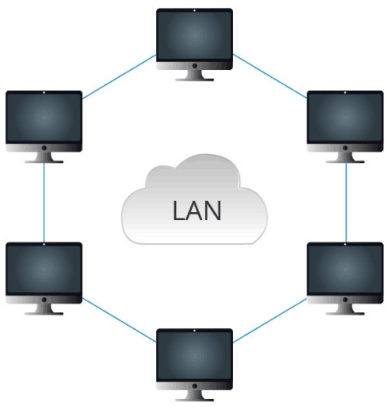

FIGURE 1.2 – Réseau local.

b) MAN (Metropolitan Area Network ou Réseau Métropolitain) : MAN est une série de réseaux locaux permettant de relier plusieurs LAN géographiquement à proximité.Tel qu'indiqué dans la représentation graphique de la figure 1.3[**3**]

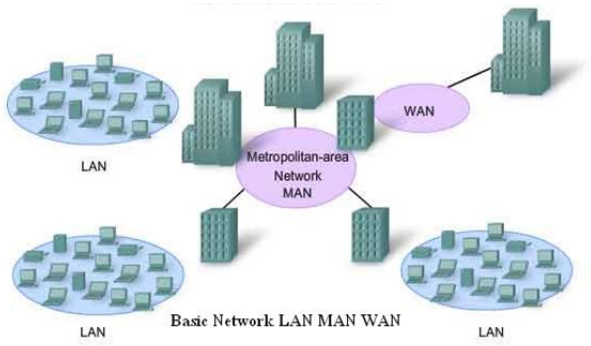

FIGURE 1.3 – Réseau Man.

c) WAN (Wide Area Network ou Réseau Etendu) : WAN comme le montre clairement la figure 1.4 [**3**], est un réseau étendu couvrant des vastes zones géographiques à l'échelle d'un pays ou d'un continent par exemple[**3**].

FIGURE 1.4 – Réseau Wan.

d) PAN (Personale Area Network) En examinant attentivement la figure 1.5 [**3**], on remarque que ce type de réseau est généralement de petite taille et est communément appelé réseau individuel ou réseau domestique[**3**].

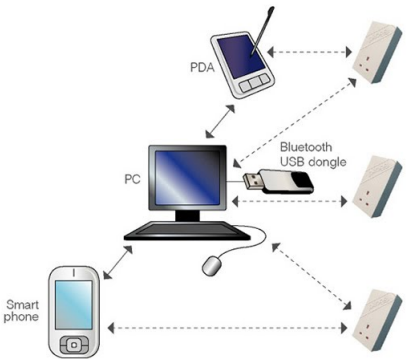

FIGURE 1.5 – Réseau Pan.

1.4 Topologies des réseaux informatiques

Il existe deux types de topologies : topologie logique et topologie physique .
La topologie physique concerne la manière dont les dispositifs sont connectés physiquement sur le réseau, tandis que la topologie logique concerne la manière dont les données circulent sur le réseau. Les deux sont importants pour comprendre et concevoir un réseau informatique efficace et fiable[**6**].

1.4.1 Topologies physiques

La topologie physique est la façon dont les équipements sont connectés physiquement les uns aux autres grâce à des lignes de communication (câbles réseaux) et des éléments matériel (cartes réseau, etc.) La topologie dans réseau informatique est choisie selon l'environnement, l'architecture (bâtiments,...) et les besoins techniques de débit pour l'entreprise.
Selon la représentation graphique présentée dans la figure 1.6 [**7**].Il existe 3 grande topologies dans le monde des réseaux câblés (wired).La topologie Bus, Anneau et celle en Étoile[**7**].

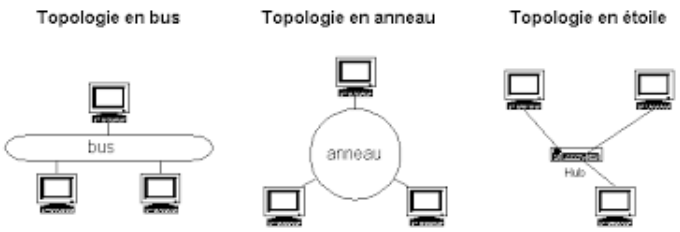

FIGURE 1.6 – Topologie physique .

a) Topologie en bus :

La topologie en bus est une forme simple d'organisation d'un réseau où tous les ordinateurs sont connectés à une seule ligne de transmission via un câble, généralement coaxial. Le terme "bus" fait référence à la ligne physique reliant les machines du réseau. Cette configuration présente l'avantage d'être facile à mettre en place et de fonctionner de manière simple. Cependant, elle est très vulnérable, car si l'une des connexions est défectueuse, l'intégralité du réseau est impactée ,la figure 1.7 [**4**] démontre comment les ordinateurs sont connectés [**4**]

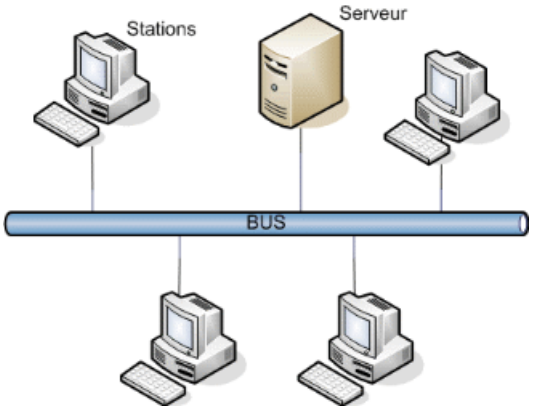

FIGURE 1.7 – Topologie en bus.

b) Topologie en Anneau

Cette topologie repose sur une boucle fermée, en anneau (ring), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud, qui ce comporte comme un répéteur (élément actif). Les concentrateurs en anneau permettent l'insertion de stations dans un réseau. Ils contiennent non seulement des ports pour ces dernières, mais Éga-

lement deux connecteur hermaphrodites nommés R/I (Ring In) et R/O (Ring Out) pour faire les boucles entre éléments. Ils acceptent des connexions de câble cuivre (RJ45) ou de fibres. On différencie le MAU (Multistation Access Unit), passif, du CAU (Controlled Access Unit), actif. L'exploitation du MAU dans un réseau crée une topologie physique en Étoile, alors que la topologie logique associée est en anneau(la figure 1.8)[**5**].

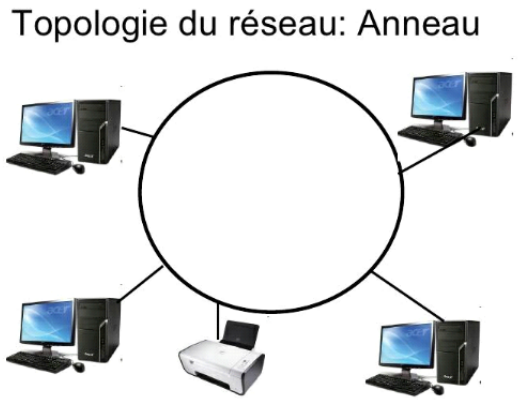

FIGURE 1.8 – Topologie en anneau.

c) Topologie en Étoile

Comme nous montre la figure 1.9[**7**], est une topologie de réseau dans laquelle chaque élément individuel d'un réseau est connecté à un nœud central (souvent appelé concentrateur ou commutateur) qui va diriger toutes les connexions. La fixation de ces éléments de réseau au composant central est représentée visuellement sous une forme similaire à une étoile[**7**].

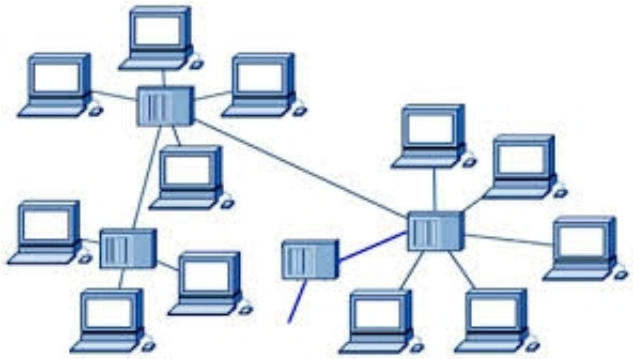

FIGURE 1.9 – Topologie en étoile.

1.4.2 Topologies logiques

Se réfère à la façon dont les données circulent sur un réseau informatique. Elle est définie par les protocoles de communication et les chemins que les données empruntent pour atteindre leur destination. Voici les topologies logiques les plus courantes Ethernet, token ring et FDDI.

a) Ethernet :

Ethernet est un protocole de réseau local basé sur la commutation de paquets. Depuis les années 1990, Ethernet est couramment utilisé pour connecter les postes clients à l'aide de paires torsadées, tandis que des versions sur fibre optique sont utilisées pour le cœur du réseau. Le principe de transmission d'Ethernet consiste à relier les ordinateurs d'un réseau à une même ligne de transmission, et à utiliser le protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detect). Ce protocole permet à n'importe quelle machine de transmettre des données sur la ligne à tout moment, sans notion de priorité entre les machines[**8**].

b) Token ring :

L'Anneau à jeton, plus connu internationalement sous le terme de Token Ring, est un protocole de réseau local qui fonctionne sur la couche Liaison du modèle OSI. Il utilise une trame spéciale de trois octets, appelée jeton, qui circule dans une seule direction autour d'un anneau. Les trames Token Ring parcourent l'anneau dans un sens qui est toujours le même[**8**].

c) FDDI :

Fiber Distributed Data Interface (FDDI) est un type de réseau informatique LAN ou MAN permettant d'interconnecter plusieurs LAN à une vitesse de 100 Mbit/s sur de la fibre optique (ce qui lui permet d'atteindre une distance maximale de 200 km. FDDI est un protocole utilisant un anneau à jeton à détection et correction d'erreurs[**8**].

1.5 Alternatives de raccordemont des réseaux

1.5.1 Supports de transmission

Les supports physiques de transmission peuvent être très hétérogènes, aussi bien au niveau du transfert de données (circulation de données sous forme d'impulsions électriques, sous forme de lumière ou bien sous forme d'ondes électromagnétiques) qu'au niveau du type de support (paires torsadées, câble coaxial, fibre optique, ondes radio, ...)[**5**].

➢ **Le câble coaxial :** Il est composé d'un fil, entouré d'une couche d'isolant, elle-même entourée d'une couche de conducteur (couche de blindage), et le tout est enroulé par une couche de protection isolante. Ces câbles réseau sont très puissants. Leurs débits vont de 56 kilobits à plusieurs gigabits. Ils sont utilisés aussi bien dans les réseaux locaux que dans les liaisons longues distance. Par exemple, le câble réseau reliant votre ordinateur et votre box Internet est de ce genre. Mais le câble qui relie votre prise téléphonique à l'équipement de votre opérateur est également coaxial (du moins, si vous n'avez pas de fibre optique). Comme mentionné précédemment, ces câbles transportent à la fois des signaux analogiques et numériques. Le câble coaxial est largement utilisé pour connecter une antenne parabolique ou une antenne parabolique à un décodeur ou à un téléviseur. Il est également utilisé sur les réseaux câblés pour transporter la télévision ou Internet, et comme connecteur pour les équipements audio et vidéo[**5**]. La figure 1.10 montre un modèle de câble coaxial [**5**]

FIGURE 1.10 – Le câble coaxial.

➢ **Le câble à paire torsadée :** C'est l'un des supports de transmission les plus anciens et il est toujours d'actualité. Comme illustré dans la figure 1.11[**5**]une paire torsadée est constituée de deux fils de cuivre isolés d'environ 1 mm d'épaisseur. Ces fils sont enroulés les uns autour des autres de manière hélicoïdale, tout comme une molécule d'ADN. Cela permet de réduire les rayonnements électromagnétiques parasites, puisque les ondes rayonnant de chaque torsade s'annulent [**5**].

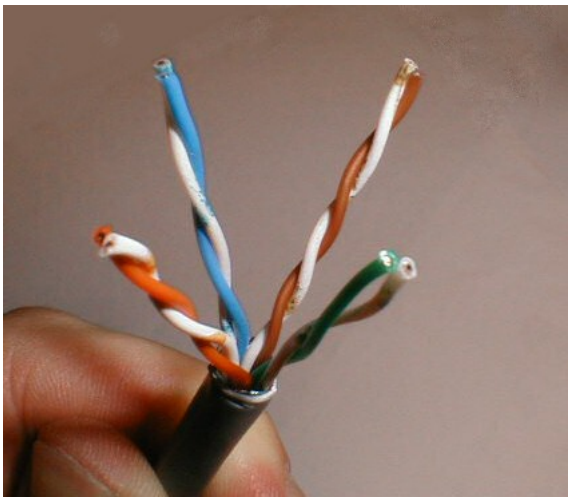

FIGURE 1.11 – Le câble à paire torsadée .

➢ **La fibre optique :** Une fibre optique est un fil de verre extrêmement fin, puisqu'il mesure environ un dixième d'un cheveu humain. Il a la capacité de conduire la lumière et est utilisé pour transmettre des données numériques ou pour des explorations visuelles dans le milieu médical. Un exemple est illustré dans l'image 1.12 [**5**]

FIGURE 1.12 – La fibre optique .

➢ **Transmission sans fil :** Aucun support filaire n'est utilisé, il s'agit des réseaux sans fil. Des ondes sont utilisées pour transporter l'information[**5**].

1.5.2 Equipements d'interconnexion

staff.univ-batna2.dz

Sont des périphériques physiques nécessaires à la communication et l'interconnexion entre les appareils d'un réseau, nous en distinguons :[**10**]

- **Le concentrateur(HUB) :** Le hub constitue un « répéteur multiport » car tout signal reçu sur un port est répété (diffusé) sur tous les autres ports. Les données binaires émises par une station sont reçues par toutes les autres stations. Ainsi seule la destination tient compte des données binaires, les autres stations les ignorent[**10**].
- **Le répeteur :** Le répeteur est une appareil qui fonctionne seulement au niveau physique (couche 1 du modèle OSI), a pour rôle de faire suivre le signal transmis sur un réseau local en empêchant toute perte de signal. Parmi ses caractéristiques : - Amplification et régénération du signal origine pour lui permettre de voyager sur de plus longues distances dans le support, - Possibilité de changer de support (passer d'un câble coaxial à une paire torsadée)[**10**].
- **Le commutateur (Switch) :** Le commutateur est une appareil multiport (il peut connecter plusieurs stations entre elles dans le même réseau local) fonctionne au niveau de liaison de données (couche 2 du modèle OSI), c'est à dire il exploite sa table de correspondance entre l'adresses physique d'une station et son port de sortie qui la relie à cette station afin d'adresser la trame reçue directement vers la station concernée.[**10**]
- **Le pont (Bridge) :** Le pont est comme le Switch. La différence, c'est que le Bridge ne comporte que deux prises (ports).il sert à relier deux réseaux de même adresse[**10**].
- **Le routeur (Gateway) :** Le routeur est un équipement possédant plusieurs interfaces, chacune est connectée à un réseau, le routeur relie ainsi plusieurs réseaux entre eux. Il fonctionne au niveau réseau (couche 3 du modèle OSI), c'est à dire il exploite sa table de routage dans laquelle est indiqué l'interface à utiliser pour que le paquet transmis arrive au réseau de destination[**10**].
- **La passerelle :** Une passerelle est un équipement recouvrant les 7 couches du mo-

dèle OSI, qui permet de relier des réseaux de types différents n'utilisant pas les mêmes protocoles[**10**].

1.5.3 Terminaux

- **La carte réseau :** La carte réseau est l'interface entre votre ordinateur et le réseau. Elle reçoit les données émises par l'ordinateur et les transfère vers un autre appareil présent sur le réseau, contrôle l'ensemble de ces données et les flux échangés. Elle reçoit également des informations depuis le réseau et les transcrit pour que celles-ci soient lues et traitées par votre ordinateur. Elle assure donc les échanges et les transferts entre votre PC et les autres appareils présents sur le réseau[**11**].
- **L'adresse Mac :** Une adresse MAC (Media Access Control) est un identifiant unique attribué à l'interface réseau d'un périphérique, tel qu'une carte réseau ou une carte Wi-Fi. Elle permet d'identifier de manière unique chaque périphérique connecté à un réseau local (LAN) et est utilisée au niveau de la couche de liaison de données pour l'échange de données entre les périphériques[**12**].

1.6 Modèles d'architecture réseau

Il existe deux types de base de modèles de réseau : le modèle de référence (OSI) et le modèle d'Application (TCP/IP)[**13**]

1.6.1 Modèle de référence OSI

Le modèle OSI, qui signifie Open Systems Interconnection, est une norme établie par l'ISO (Organisation internationale de normalisation) pour faciliter l'interconnexion des systèmes ouverts. Il propose une architecture réseau spécifiant un ensemble de règles pour permettre la connexion de divers équipements hétérogènes. Le modèle OSI standardise la manière dont les matériels et les logiciels collaborent pour assurer la communication au sein d'un réseau. Il est structuré en sept couches successives[**4**] .

Pour mieux comprendre les services offerts par chaque couche, nous allons les présenter individuellement dans l'ordre suivant :

- **La couche Physique :** Les protocoles de la couche physique décrivent les moyens mécaniques, électriques, fonctionnels et méthodologiques permettant d'activer, de gérer et de désactiver des connexions physiques pour la transmission de bits vers et depuis un périphérique réseau.
- **La couche Liaison :** Les protocoles de la couche liaison de données décrivent des méthodes d'échanges de trames de données entre des périphériques sur un support commun.
- **La couche réseau :** La couche réseau fournit des services pour échanger les parties de données individuelles sur le réseau entre des périphériques terminaux identifiés.
- **La couche Transport :** Cette couche est responsable du bon acheminement des messages complets au destinataire. Le rôle principal de la couche transport est de prendre les messages de la couche session, de les découper s'il le faut en unités plus petites et de les passer à la couche réseau, tout en s'assurant que les morceaux arrivent correctement de l'autre côté. Cette couche effectue donc aussi le réassemblage du message à la réception des morceaux.
- **La Couche Session :** La couche session fournit des services à la couche présentation pour organiser son dialogue et gérer l'échange de données.
- **La couche Présentation :** Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises : c'est elle qui traite l'information de manière à la rendre compatible entre tâches communicantes. Elle va assurer l'indépendance entre l'utilisateur et le transport de l'information. Typiquement, cette couche peut convertir les données, les reformater, les crypter et les compresser.
- **La couche Application :** Cette couche est le point de contact entre l'utilisateur et le réseau. C'est donc elle qui va apporter à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichier, la messagerie...

1.6.2 Modèle TCP/IP :

La pile protocolaire TCP/IP : comporte quatre couches : accès réseau, Internet, transport et application. Ensemble, ces couches composent une suite de protocoles. Le modèle TCP/IP fait transiter les données par ces couches dans un ordre bien défini lorsque l'utilisateur envoie une information, puis dans l'ordre inverse lorsque des données arrivent[**5**].

- **La couche d'accès réseau :** La couche d'accès réseau, aussi appelée couche de liaison de données, gère l'infrastructure physique qui permet aux ordinateurs de communiquer entre eux via Internet. Cette infrastructure comprend les câbles Ethernet, les réseaux sans fil, les cartes réseau, les pilotes de périphérique de votre ordinateur, etc[**5**].
- **La couche Internet :** La couche Internet, aussi appelée couche réseau, contrôle le flux ou le routage des paquets sur le réseau afin que les données soient envoyées rapidement et à la bonne destination. Cette couche est également chargée de réassembler le paquet de données côté destination. Si le trafic Internet est important, la couche Internet peut avoir besoin d'un peu plus de temps pour envoyer un fichier, mais les risques qu'une erreur vienne endommager ce fichier sont réduits[**5**]
- **La couche transport :** La couche transport fournit une connexion des données fiable entre deux appareils qui communiquent entre eux. C'est comme si vous envoyiez un colis avec une assurance. La couche de transport décompose les données en paquets, accuse réception des paquets qu'elle a reçus de l'expéditeur et s'assure que le destinataire accuse réception des paquets qu'il reçoit[**5**].
- **La couche application :** La couche application est le groupe d'applications qui permettent à l'utilisateur d'accéder au réseau. Pour la plupart d'entre nous, il s'agit des e-mails, des applications de messagerie et des programmes de stockage dans le cloud. C'est ce que l'utilisateur final voit et utilise lorsqu'il envoie et reçoit des données[**5**].

La figure 1.13 présente une comparaison entre le deux modèle

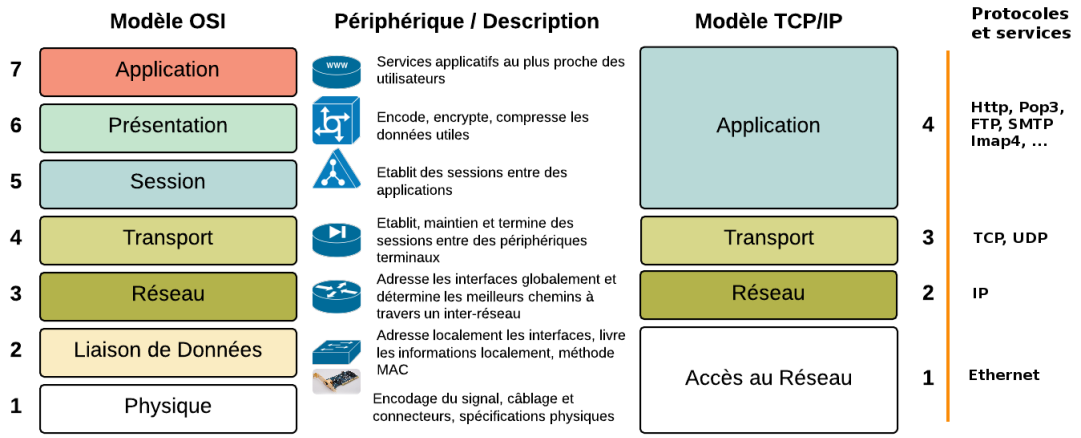

FIGURE 1.13 – comparaison entre les deux modèles OSI et TCP/IP .

[5]

1.7 L'adressage IP

Nous sommes conscients que l'objectif principal d'un réseau est d'établir des connexions entre des machines et de permettre ainsi l'échange d'informations entre elles. Pour atteindre cet objectif, il est nécessaire que ces machines disposent d'un moyen de s'identifier mutuellement, ce qui est réalisé grâce aux adresses IP. Il existe deux formats d'adresses IP : le format IPV4 et le format IPV6.

1.7.1 Le format IPV4

Format IPV4 Il s'agit d'une adresse de 32 bits divisée en 4 fois 8 bits (octets). cette adresse est un identifiant réseau qui peut être décomposé en deux parties : Section réseau et hôte. Le premier identifie le réseau sur lequel se trouve la machine Le second identifie la machine elle-même. A fin d'Identifier les deux parties Chaque adresse est liée à un masque de sous-réseau pour qu'il soit possible de définir C'est sur quel réseau elle se trouve.

Le format binaire d'une adresse IP est le suivant : xxxxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx ET (x=0 ou x=1). les masques de réseau sont utilisés pour séparer les parties réseau et hôtes d'une adresse. On trouve l'adresse réseau : En effectuant un ET logique entre l'adresse IPv4

classe	Bits de départ	Plage d'adresses	Masque de sous-réseau
A	0	0.0.0.0 à 127.255.255.255	255.0.0.0 (/8)
B	10	128.0.0.0 à 191.255.255.255	255.255.0.0 (/16)
C	110	192.0.0.0 à 223.255.255.255	255.255.255.0 (/24)
D	1110	239.0.0.0 à 127.255.255.255	Non définie
E	1111	240.0.0.0 à 255.255.255.255	Non définie

TABLE 1.1 – Les Classes d'adresses IP.

d'un périphérique et le masque de sous-réseau

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

On distingue deux types d'adresse spécifiques : les adresses privées et les adresses de diffusions.

➢ **Les adresses privées :**

Il existe des adresses privées, dans chaque classe :

A : 10.0.0.0 à 10.255.255.255

B : 172.16.0.0 à 172.31.255.255

C : 192.168.0.0 à 192.168.255.255

➢ **Adresse de diffusion :**

L'adresse de diffusion est utilisée pour envoyer des messages à toutes les machines d'un réseau. Il est obtenu en mettant tous les bits d'host-id à 1. Il y a aussi l'adresse de diffusion "broadcast ", qui permet d'envoyer Envoyez un message à toutes les machines sur tous les réseaux connectés.

1.7.2 Le format IPV6

Le format IPv6, également connu sous le nom d'Internet Protocol version 6, est un protocole de communication utilisé pour l'adressage des dispositifs sur Internet. Contrairement à IPv4, qui utilise des adresses de 32 bits, IPv6 utilise des adresses de 128 bits, offrant ainsi

un espace d'adressage beaucoup plus vaste.

Le format IPv6 est généralement représenté sous la forme de huit groupes de quatre chiffres hexadécimaux séparés par des deux-points (:). Par exemple, une adresse IPv6 valide pourrait ressembler à ceci : 2001 :0db8 :85a3 :0000 :0000 :8a2e :0370 :7334.

1.8 Conclusion

En résumé, ce chapitre nous a permis de développer une base solide de connaissances sur les principes fondamentaux de la communication et de la connectivité dans les réseaux informatiques. Cette base sera essentielle à mesure que nous progresserons vers le deuxième chapitre, qui se consacre à la sécurité informatique.

CHAPITRE 2

NOTIONS DE BASE SUR LA SÉCURITÉ DES RÉSEAUX INFORMATIQUES ET PRÉSENTATION DE L'ORGANISME D'ACCUEIL

2.1 Introduction

La sécurité des réseaux informatiques est devenue une préoccupation majeure en raison de ce développement rapide de la technologie et de l'augmentation des risques qui en résulte. Dans ce chapitre, nous donnerons un aperçu de la sécurité des réseaux informatiques et de ses concepts de base.Nous passons ensuite à la présentation de l'organisme d'accueil,afin d'identifier clairement le domaine dans lequel nous souhaitons travailler.

2.2 Notions de base sur la sécurité des réseaux informatiques

2.2.1 Définition de la sécurité des réseaux

La sécurité des réseaux est la protection des données, des applications, des appareils et des systèmes connectés à un réseau contre les menaces en ligne telles que les virus, les logiciels malveillants, les pirates, les attaques et les accès non autorisés grâce à un ensemble de mesures, de processus et de techniques. La sécurité du réseau vise à assurer la confidentialité, l'intégrité et la disponibilité des données transmises et stockées dans le réseau.

2.2.2 Propriétés de sécurité informatique

Les propriétés de sécurité informatique sont des caractéristiques qui décrivent différents aspects et objectif de la sécurité du système informatique.
Voici les principales propriétés de sécurité informatique :

- **Confidentialité** Demande que l'information sur le système ne puisse être lue que par les personnes autorisées[**14**].
- **Disponibilité** Demande que l'information sur le système soit disponible aux personnes autorisées.

- **Intégrité** Demande que l'information sur le système ne puisse être modifiée que par les personnes autorisées.
- **Non répudiation** Permettant de garantir qu'une transaction ne peut être niée.
- **Authentification** Consistant à assurer que seules les personnes autorisées aient accès aux ressources. Elle est la propriété qui garantit que l'identité de l'utilisateur ou de l'entité avec laquelle vous communiquez est bien celle qu'elle prétend être.
- **Traçabilité**

  La traçabilité est la propriété qui permet de retracer les actions effectuées sur les systèmes informatiques. Elle est importante pour l'audit, la conformité aux réglementations et la détection d'activités suspectes.

2.3 Intérêt de sécurité

La sécurité informatique est devenue un enjeu majeur dans notre monde de plus en plus connecté. Elle vise à protéger les données, les réseaux et les systèmes informatiques contre les attaques, les piratages et les perturbations.

2.3.1 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini que nous utilisons dans nos articles. De manière à bien comprendre ces articles, il est nécessaire de définir certains termes :

- **Vulnérabilité** Ce sont les failles de sécurité dans un ou plusieurs systèmes il s'agir plus généralement d'une faiblesse dans le réseau.
- **Attaques** Elles représentent les moyens d'exploiter une vulnérabilité, et Obtenir un accès non autorisé à l'information c'est-à-dire, violer secret ou confidentialité. Il existe deux types d'attaque : attaque passive et attaque active.

a)Attaque passive : L'attaquant intercepte l'information transmit avec l'intention de lire et d'analyser l'information pour ne pas la modifier.

b)Attaque active : L'attaquant intercepte la connexion et modifie les informations [**15**].

- ➢ **Menace** Ce sont des adversaires résolus qui ont la capacité de lancer une attaque en exploitant une vulnérabilité.
- ➢ **Contre-mesures** Il s'agit de procédures ou de techniques qui résoudre une vulnérabilité ou contrent une attaque spécifique [**16**]

2.3.2 Politique de sécurité

Une politique de sécurité informatique représente un plan d'actions élaboré dans le but de maintenir un niveau de sécurité informatique déterminé. Elle constitue une stratégie visant à optimiser la sécurité informatique au sein d'une entreprise, reflétant ainsi la vision stratégique de la direction concernant la sécurité des systèmes informatiques. La mise en œuvre d'une politique de sécurité informatique s'avère essentielle pour protéger les systèmes informatiques contre les menaces, en assurant l'intégrité, la confidentialité, la disponibilité, la non-répudiation et l'authenticité des données et des systèmes. Les meilleures pratiques relatives à l'implémentation d'une politique de sécurité informatique incluent l'établissement d'objectifs de sécurité, l'identification des risques, l'adoption de mesures de sécurité adaptées, la sensibilisation des employés, la création de politiques de sécurité, la réalisation de vérifications de sécurité régulières et la mise en place d'un plan de continuité des activités[**17**].

2.3.3 Vulnérabilités

Dans la cybersécurité il existe trois familles de vulnérabilités [**17**]

a)Vulnérabilités liées aux domaines physiques

• Le vol et le manque de redondance de matériel informatique, tels que des serveurs, des routeurs, des commutateurs, des ordinateurs portables, etc.

• Accès aux salles de serveurs, Accès physique non autorisé

b)Vulnérabilités liées aux domaines organisationnels

• Ces vulnérabilités résultent des actions ou des erreurs des utilisateurs ou des administrateurs du réseau. (personnels non qualifiés)

• Absence de documents de procédures adaptés à l'entreprise

c)Vulnérabilités liées aux domaines technologiques

• Failles nombreuses dans Les protocoles de communication tels que TCP/IP, DNS, SNMP, FTP, SMTP, etc et dans les applications web.

• Vulnérabilités dans les systèmes d'exploitation : Les systèmes d'exploitation tels que Windows, Linux, macOS, etc.

• Absence de Contrôle suffisant sur les logiciels malveillants.[**17**]

2.3.4 Attaques

Il existe plusieurs types d'attaques à savoir :

- ➢ **Virus** Est tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire.
- ➢ **Ver** Sont des virus capables de se propager à travers un réseau .
- ➢ **Cheval de troie (trojan horse)** Est un programme informatique ouvrant une porte dérobée (backdoor) dans un système pour y faire entrer un hacker ou d'autres programmes indésirables. [**18**]
- ➢ **Logiciel espion (spyware)** Est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur dans lequel il est installé (on appelle donc parfois mouchard) afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes (on parle de profilage) [**18**] .

2.3.5 Solution de défense

2.3.5.1 IPS (Intrusion Prevention System)

Le système de prévention d'intrusion (IPS) analyse directement les données en temps réel, ce qui est différent de l'IDS qui n'analyse qu'une seule donnée. Un IPS répond en bloquant

le port source du trafic suspect. Semblable à l'IDS, il existe deux types d'IPS : NIPS (Network IPS), qui analyse le trafic réseau à l'aide d'une base de données de signatures d'attaque et bloque le trafic malveillant lorsqu'il est détecté ; HIPS (Host IPS), qui analyse en surveillant différents éléments de la machine qui hébergent et bloquent activité suspecte[**18**].

2.3.5.2 IDS (Intrusion Detection System)

Les outils de détection d'intrusion viennent compléter les fonctions du pare-feu .au travers d'une surveillance de l'identité des requêtes en circulation sur le réseau c'est outils sont à même de repère les requêtes malintentionnées, de repérer les intrus dans le flot du trafic courant transitant par les ports de communication laissés ouverts par le pare-feu. Les systèmes de détection sont conçus pour informer des accès non autorisés ou des intrusions dans les réseaux. Les pare-feu qui opèrent avec les systèmes de détection sont capables de détecter automatiquement les menaces venant de l'extérieur plus rapidement qu'une vérification par un opérateur Il existe 2 types de détection du d'intrusion 1. Le premier système basé sur l'hôte doit être installé sur chaque machine à protéger il est en général intégré au système d'exploitation qu'il protège. Ces types de d'IDS Sont prévus Pour la détection de menaces à un haut niveau de sécurité. 2. Le 2nd système basé sur le réseau est implémenté en En tant que analyseur intelligent de protocole. Ses composants surveiller le trafic réseau au niveau physique[**16**]

2.3.5.3 Pare-feu

Un pare-feu également connu sous le terme anglais "firewall est un dispositif ou un logiciel qui surveille et contrôle le trafic réseau, agissant comme une première ligne de défense pour protéger un réseau ou un système informatique contre les attaques et les intrusions non autorisées.

Le rôle principal d'un pare-feu est de filtrer le trafic réseau en autorisant ou en bloquant le trafic en fonction de règles définies. Ces règles déterminent les connexions réseau autorisées via le pare-feu en fonction de critères tels que les adresses IP source et de destination, les

numéros de port et les protocoles de communication. En plus du filtrage du trafic, les pare-feu peuvent fournir d'autres fonctionnalités de sécurité, telles que la traduction d'adresses réseau (NAT), qui masque les adresses IP internes pour préserver la confidentialité, et les systèmes de détection d'intrusion (IDS), qui détectent les activités suspectes [**16**]

2.3.5.4 Proxy

Un serveur proxy est un intermédiaire essentiel qui facilite les communications entre un client et un serveur, il offre des avantages tels que l'amélioration des performances, la sécurité et la confidentialité, en filtrant certains contenus web et logiciels malveillants. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...) [**19**]

2.3.5.5 Vlan

Un VLAN en français Réseau Local Virtuel est un réseau local regroupant un ensemble de machines de façon logique et non physique au plus c'est un sous-réseau logique d'appareils dans un domaine de diffusion, divisé par des commutateurs réseau et/ou un logiciel de gestion de réseau, et peut fonctionner indépendamment comme un seul LAN.[**19**]

2.3.5.6 VPN

Un réseau privé virtuel (Virtual Private Network) est un service qui permet de créer une connexion sécurisée et chiffrée entre votre appareil (comme un ordinateur, un smartphone ou une tablette) et un serveur distant. Il s'agit d'une technologie qui utilise un tunnel virtuel pour faire transiter vos données de manière confidentielle sur Internet.

2.4 Présentation de l'organisme d'accueil

Général Emballage est une société par action au capital de deux (02) milliards de Dinars Algériens et est une entreprise papetière algérienne spécialisée dans la fabrication et la trans-

formation de carton ondulé. Créée en 2000, par Ramdane Batouche qui assure aujourd'hui la présidence du Conseil d'administration. Général Emballage est le plus grand producteur de carton ondulé en Afrique,l'entreprise dispose actuellement d'un siège social et de deux unités de production implantées à Akbou, Oran et Sétif, et Voici le logo de l'entreprise présenté dans la figure 2.1 [**23**] :

FIGURE 2.1 – Logo-GE.

2.4.1 Historique

En 2000

☐ 1er Août Création de la SARL Général Emballage avec un capital de 32 millions de dinars dans la Zone d'activités de Taharacht (Akbou.W. de Bejaia) (décision APSI N°13051 du 06 juin 1998).

En 2002

☐ Entrée en production de l'usine d'Akbou avec un effectif de 83 employé.

En 2006

☐ Le capital est porté à 150 millions de dinars

☐ Effectif : 318 employés.

En 2007

☐ Le capital est porté à 1,23 milliards de dinars.

☐ Effectif : 425 employés.

☐ Trophée de la Production (Euro-Développement PME).

☐ Entrée en production de l'usine de Sétif.

En 2008

☐ Début d'exportation vers la Tunisie.

☐ Entrée en exploitation de l'unité d'Oran.

En 2009

☐ 03 Juin : Augmentation du capital à 2 milliards de DA et entrée de MAGHREB PRIVATE EQUITY FUND II « Cyprus II» (MPEF II) avec une participation de 40% . Général Emballage devient une société de capitaux (Société par actions)

☐ Effectif : 597 employés.

En 2010

☐ Effectif : 630 employés

En 2011

☐ Effectif : 699 employés

☐ Novembre : Cotation COFACE « @@@ »

En 2012

☐ Mars : Les capacités de production sont portées à 130.000 tonnes.

☐ Juin : L'usine d'Oran est transférée à la ZI Hassi-Ameur.

☐ Juin : Production des premiers ouvrages en Haute résolution.

☐ Juillet 02 : Signature d'une Convention cadre de partenariat avec l'Université de Béjaia.

☐ Décembre 17 : Notation COFACE « @@@ ».

☐ Effectif : 830 employés.

De 2013 jusqu'à 2019

☐ Effectif : 1201

☐ Distinguée comme entreprise « inspirante » pour l'Afrique dans le Rapport « Compagnies to inspire Africa 2019 » du London Stock Exchange Group (Bourse de Londres).

☐ Avril 21 : Première expédition sur la Belgique.

☐ Juin 13 : Prix spécial du jury du Trophée Export 2018 (World Trade Center (WTCA).

☐ Juin 19 : Première exportation sur la France.

En 2020

☐ Effectif : 1222.

☐ Janvier 25 : Certifications ISO 14001 :2015 et ISO 45001 :2018.

☐ Juillet 23 : Notation COFACE @@@ [**23**].

2.4.2 Localisation

La Spa Général Emballage est implantée au niveau de la Zone d'activités de Taharacht, située à 2.5 km au Nord-est du chef-lieu de la commune d'Akbou. D'une superficie de 24HA, elle est un véritable carrefour économique vu le nombre d'unités industrielles qui exercent dans différents domaines [**24**]. La figure 2.2 présente la position géographique de l'entreprise[**23**].

FIGURE 2.2 – Localisation de l'entreprise Général Emballage .

2.4.3 Mission

La mission de Général Emballage est de satisfaire sa clientèle de plus en plus exigeante en matiére d'emballage et de plaques en carton ondulé. Parmi ses produits fabriqués on trouve :

— Plaque de carton ondulé.

— Caisse à fond automatique.

— Caisse télescopique.

— Barquette à découpe spéciale [**23**].

2.4.4 Activités

Général Emballage opère sur les domaines d'activités stratégiques suivantes :

— La production de feuilles en carton ondulé pour les transformateurs et certaines activités logistiques.

— La transformation de carton ondulé en emballages, barquette et PAV à travers des process d'impression et de découpe.

— Récupération et collection et revalorisation de papiers et carton à recycler (PCR) .

2.4.5 Organisation de la Spa Général Emballage

L'entreprise a adopté une démarche marketing et commerciale, qui est focalisée autour de la demande; c'est-a-dire la satisfaction et la fidélisation de la clientèle en recherchant l'excellence de la qualité des produits. L'organisation de l'entreprise est présentée selon l'organigramme illustré par la figure 2.3[**23**] :

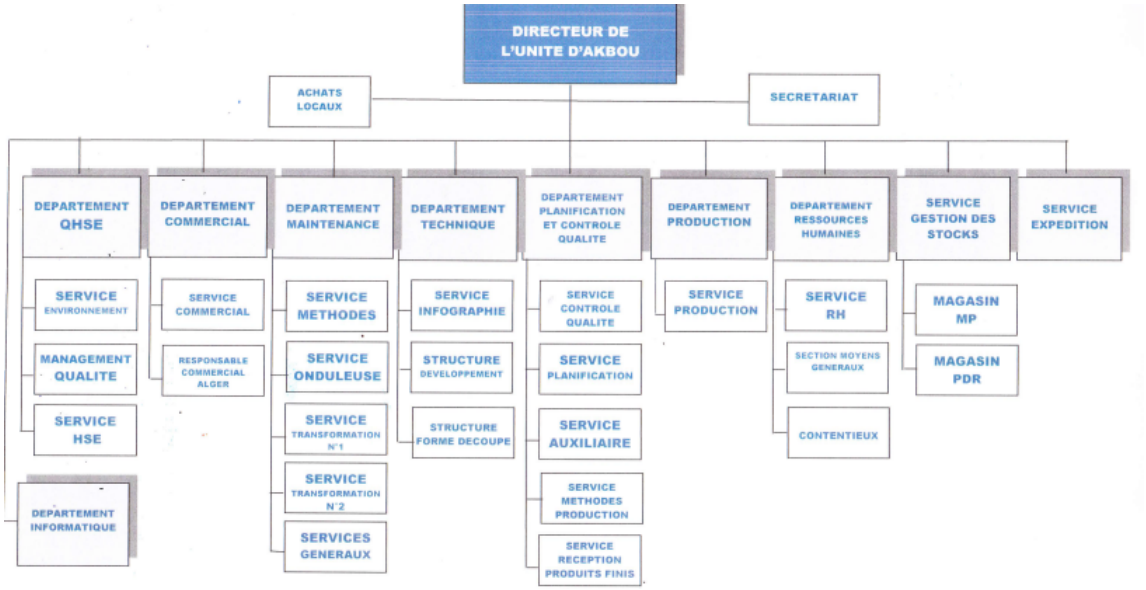

FIGURE 2.3 – L'organigrame de l'entreprise Général Emballage .

2.4.6 Présentation du l'architecture Réseau de Général Emballage

La figre 2.4 présente l'architecture du réseau de Génaral Emballage [**24**]

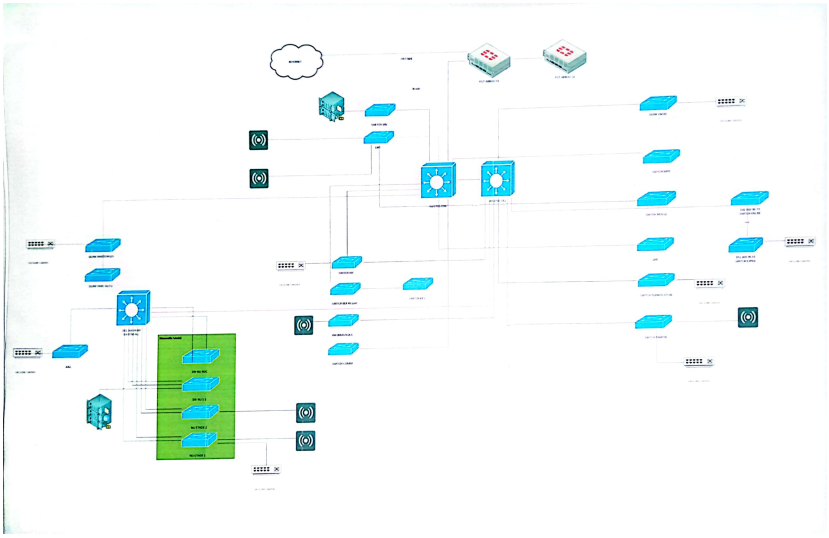

FIGURE 2.4 – Architecture du réseau .

2.4.7 Problématiques

Lors de notre stage à Général Emballage à Béjaia, nous avons remarqué que l'entreprise dispose d'un réseau local comprenant plusieurs plates-formes et offrant différents services. Au cours de nos discussions avec le responsable de stage, nous avons relevé des problèmes de fonctionnement du réseau et avons identifié certaines pannes réseau, notamment :

- ➢ La plupart des ports de commutateur se trouvent sur le VLAN Physique, ce qui risque d'augmenter les domaines de diffusion et de compromettre la sécurité. Contredit, l'objectif de l'utilisation des VLAN, qui est de micro-segmenter le réseau en petits domaines de diffusion.
- ➢ Les adresses IP changées entre les sites de l'entreprises ne sont pas masquées.
- ➢ La société s'étend à des sites distants et à plusieurs centres de distribution. Il dispose donc d'un réseau important et nécessite une interconnexion permanente fiable et privée entre ces différents sites.

- ➢ Absence de point de centralisation et de gestion des comptes et droit des accès systèmes.
- ➢ Absence de contrôle d'accès pour certains sites Web gourmands en bande passante qui réduit la vitesse à la quelle les employés travaillent (YouTube, Face book, etc.).
- ➢ Pas d'accès à distance sécurisé aux équipements depuis l'intranet et l'extranet de l'infrastructure réseau de général emballage.
- ➢ Manque des solutions de haute disponibilité et équilibrage de charge.

2.4.8 Solutions proposées et objectifs

Le principal défi d'une architecture de réseau sécurisée est de pouvoir réguler l'accès aux ressources réseau à partir du réseau local et de l'extérieur, tout en limitant autant que possible les vulnérabilités aux éventuelles attaques ou vol d'informations afin d'améliorer la sécurité du réseau local.

Pour résoudre ces problèmes, nous avons eu des discussions avec le responsable de stage et avons finalement choisi les solutions suivantes :

- ➢ Amélioration de configuration pour les VLANs afin de renforcée la sécurité du réseau et réduire les tempêtes de diffusion ARP.
- ➢ Mise en place d'un canal sécurisé de bout en bout entre le site de Bejaia et les autres sites en utilisant le protocole IPSec (IP sécurisé) pour avoir la confidentialité, l'intégrité et l'authentification des données circulant sur le réseau internet.
- ➢ Mise en place d'un firewall afin de contrôler, gérer et sécuriser les ports logiques ouverts sur le réseau externe.
- ➢ Mise en place du protocole SSH et VPN SSL pour sécuriser les accès à distance aux équipements d'interconnexion depuis l'accès internet
- ➢ Mise en place de l'agrégation des liens et équilibrage de charge en utilisant le protocole standard LACP
- ➢ Mise en place d'un cluster et de la redondance à premier saut pour garantir la haute disponibilité niveau trois.

➢ Mise en place d'une zone DMZ(zone démilitarisée) pour isoler le réseau extranet et intranet .

2.5 Conclusion

En conclusion, l'étude de la sécurité des réseaux informatiques nous a fourni une compréhension approfondie des principes fondamentaux, des objectifs et des menaces qui affectent la sécurité des réseaux. Et l'analyse de notre organisme d'accueil nous a permis d'identifier les mesures nécessaires pour renforcer la sécurité de nos réseaux.Ces principes seront d'une grande utilité à mesure que nous aborderons le prochain chapitre, où nous explorerons en détail la sécurité basée sur les liaisons virtuelles.

CHAPITRE 3

SÉCURITÉ À BASE DES LIAISONS VIRTUELLES

3.1 Introduction

Les réseaux virtuels (Virtual LAN) sont apparus comme une nouvelle fonctionnalité dans l'administration réseau avec le développement des commutateurs. La notion de VLAN est un concept qui permet de réaliser des réseaux de façon indépendante du système de câblage. Ces réseaux permettent de définir des domaines de diffusions restreints, cela signifie qu'un message émis par une station du VLAN ne pourra être reçu que par les stations de ce même VLAN.

Dans ce chapitre, nous allons présenter les principales notions d'un réseau local virtuel après nous allons parler sur le protocole de transport (la norme 802.1Q) et le protocole d'administration et nous allons présenter les réseaux privés virtuels. Finalement nous allons mettre la lumière sur l'agrégation des liens et la redondance.

3.2 Les réseaux locaux virtuels (VLAN)

Un VLAN permet de créer des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérés logiquement.
Leur fonctionnement repose sur la segmentation logique du réseau, ce qui permet de créer des groupes virtuels isolés au sein d'un même réseau physique.

3.2.1 Le fonctionnement des VLANs

Voici un bref aperçu de leur fonctionnement :

Les VLAN permettent de diviser un réseau physique en plusieurs segments logiques indépendants. Chaque VLAN fonctionne comme un réseau LAN distinct, même s'il partage le même réseau physique.

Les ports du commutateur réseau sont associés à des VLAN spécifiques. Les dispositifs connectés à un port particulier appartiendront au VLAN attribué à ce port.
Les VLAN assurent l'isolation entre les dispositifs appartenant à des VLAN différents. Cela signifie que les dispositifs d'un VLAN ne peuvent pas communiquer directement avec ceux d'un autre VLAN, à moins qu'il n'y ait des mécanismes de communication inter-VLAN en place.
Pour permettre la communication entre les VLAN, des routeurs ou des commutateurs de niveau 3 (commutateurs capables de faire du routage) peuvent être utilisés. Ils agissent comme des passerelles entre les VLAN en acheminant les paquets de données entre eux.
Les VLAN offrent des avantages en termes de sécurité et de gestion du réseau. Ils permettent de restreindre l'accès des dispositifs à certains segments du réseau, ce qui peut contribuer à une meilleure sécurité des données et à une meilleure organisation du réseau.

3.2.2 Classification des VLAN

Les vlan peuvent être placés en trois niveaux : niveau 1 (aussi appelé VLAN par port), niveau 2 (VLAN par adresse MAC) et niveau 3 (VLAN par adresse IP).

1) Les VlANs par ports (niveau 1) :

On affecte chaque port des commutateurs à un VLAN. L'appartenance d'une trame à un VLAN est alors déterminée par la connexion de la carte réseau à un port du commutateur. Les ports sont donc affectés statiquement à un VLAN. Si on déplace physiquement une station il faut désaffecter son port du Vlan puis affecter le nouveau port de connexion de la station au bon Vlan. Si on déplace logiquement une station (on veut la changer de Vlan) il faut modifier l'affectation du port au Vlan.Comme illustré dans la figure 3.1 :

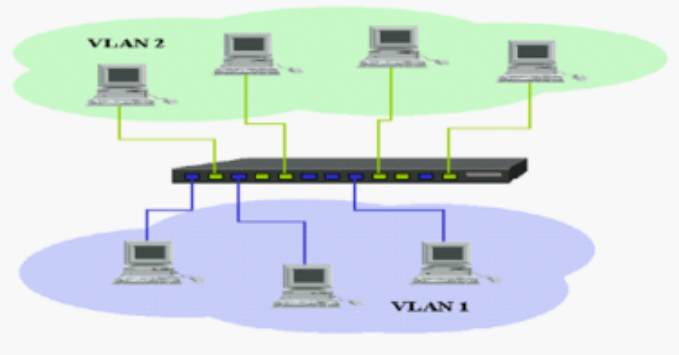

FIGURE 3.1 – construction des VLANs par port .

2) Les VlANs par adresse MAC (Vlan de niveau 2)

D'après la figure 3.2 ,on affecte chaque adresse MAC à un VLAN. L'appartenance d'une trame à un VLAN est déterminée par son adresse MAC. En fait il s'agit, à partir de l'association Mac/VLAN, d'affecter dynamiquement les ports des commutateurs à chacun des VLANs en fonction de l'adresse MAC de l'hôte qui émet sur ce port. L'intérêt principal de ce type de VLAN est l'indépendance vis-à-vis de la localisation géographique. Si une station est déplacée sur le réseau physique, son adresse physique ne changeant pas, elle continue d'appartenir au même VLAN (ce fonctionnement est bien adapté à l'utilisation de machines portables). Si on veut changer de Vlan il faut modifier l'association Mac / Vlan.

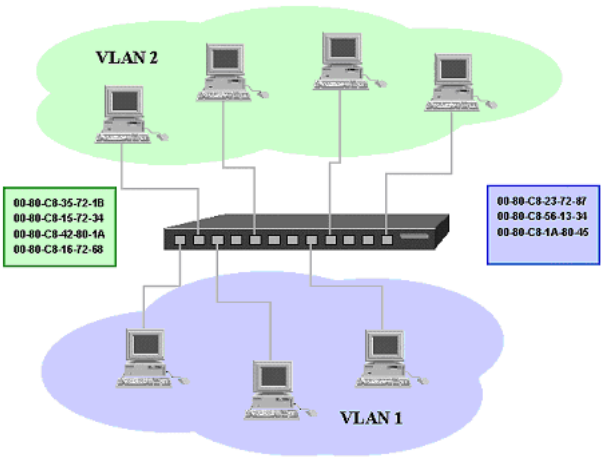

FIGURE 3.2 – construction des VLANs par adresse Mac .

3) Les VLANs par sous réseau et protocole (VLAN de niveau 3 et plus)

Par sous-réseau : Cette méthode de création de VLAN regroupe plusieurs machines en fonction du sous-réseau auquel elles appartiennent. Chaque VLAN est associé à une adresse de sous-réseau spécifique. Ainsi, les machines partageant le même sous-réseau sont regroupées dans le même VLAN. Par exemple, vous pouvez avoir un VLAN pour le sous-réseau 192.168.1.0/24 et un autre VLAN pour le sous-réseau 192.168.2.0/24.(voir la figure 3.3)

Par protocole : Cette méthode permet de créer des VLAN virtuels en fonction du type de protocole utilisé par les machines. Chaque protocole est associé à un VLAN spécifique. Par exemple, vous pouvez avoir un VLAN pour les machines utilisant le protocole HTTP (VLAN 2) et un autre VLAN pour les machines utilisant le protocole SMTP (VLAN 3). Cela permet de regrouper les machines qui utilisent le même protocole au sein d'un même réseau virtuel

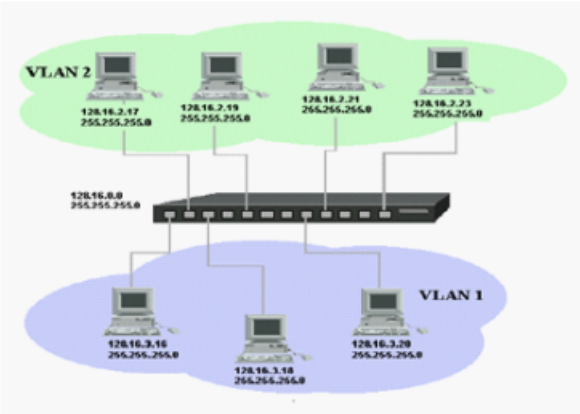

FIGURE 3.3 – construction des VLANs par sous-réseau .

3.2.3 Types de VLANs

Il existe différents types de VLAN utilisés dans les réseaux modernes. Certains types de VLAN sont définis par les classes de trafic. D'autres types de VLAN sont définis par leur fonction spécifique [**20**].

a)VLAN de données

Un VLAN de données est un réseau local virtuel configuré pour transmettre le trafic généré par l'utilisateur. Un VLAN acheminant du trafic de voix ou de gestion ne peut pas faire partie

d'un VLAN de données. Il est d'usage de séparer le trafic de voix et de gestion du trafic de données. Un VLAN de données est parfois appelé un VLAN utilisateur. Les VLAN de données sont utilisés pour diviser un réseau en groupes d'utilisateurs ou de périphériques[**20**].

b)VLAN de gestion

Un VLAN de gestion est un réseau local virtuel configuré pour accéder aux fonctionnalités de gestion d'un commutateur. la configuration de la gestion du VLAN se fait en lui attribuant une adresse IP est un masque sous réseau, généralement le VLAN de gestion par défaut est le VLAN 1.

c)VLAN de voix

Un Voice VLAN est un VLAN (réseau local virtuel) qui est spécifiquement alloué aux flux de données vocales de l'utilisateur. Il assure la qualité du trafic vocal en améliorant la priorité de transmission de celui-ci lorsqu'il est transmis avec d'autres trafics. Autrement dit, lorsque d'autres services (données, vidéo, etc.) sont transmis simultanément, le service vocal sera priorisé et transmis avec une priorité d'acheminement plus élevée[**20**].

d)VLAN par défaut

Tous les ports de commutateur font partie du VLAN par défaut après le démarrage initial d'un commutateur chargeant la configuration par défaut. Les ports de commutateur qui participent au VLAN par défaut appartiennent au même domaine de diffusion. Cela permet à n'importe quel périphérique connecté à n'importe quel port du commutateur de communiquer avec d'autres périphériques sur d'autres ports du commutateur[**20**].

e)VLAN natif

Un réseau local virtuel natif est affecté à un port trunk 802.1Q. Les ports trunk sont les liaisons entre les commutateurs qui prennent en charge la transmission du trafic associée à plusieurs VLAN. Un port trunk 802.1Q prend en charge le trafic provenant de nombreux VLAN (trafic étiqueté ou « tagged Traffic »), ainsi que le trafic qui ne provient pas d'un VLAN (trafic non étiqueté ou « untagged Traffic »).

3.2.4 VLANs privés

Le VLAN privé (PVLAN), également connu sous le nom d'isolation de port, est une technologie de segmentation de réseau pour les réseaux de couche 2, permettant l'isolation des ports ou la segmentation du trafic sous le même segment IP. En appliquant le VLAN privé dans un environnement de réseau partagé, cela permet d'économiser des adresses IP et d'améliorer la sécurité des ports de commutation dans la couche 2[**20**].

3.2.4.1 Types de VLAN privé

Au sein d'un réseau VLAN privé, les VLAN sont accessibles sous trois modalités, selon les informations illustrées dans la figure 3.5 :

a) VLAN primaire :

Ce type de VLAN fait référence au VLAN d'origine, qui peut descendre des trames vers tous ses sous-VLAN (VLAN secondaires) à partir des ports promiscuous vers tous les ports connectés à l'hôte.

b)VLAN isolé :

En tant que VLAN secondaire, le VLAN isolé ne peut prendre en charge que les ports de commutation (ports isolés) au sein du VLAN isolé qui transmettent des données aux ports promiscuous du VLAN primaire. Même dans un même VLAN isolé, les ports isolés ne peuvent pas communiquer entre eux.

c)VLAN communautaire :

Le VLAN communautaire est également un type de VLAN secondaire. Les ports de commutation (ports communautaires) au sein d'un même VLAN communautaire peuvent communiquer entre eux ainsi qu'avec les ports du VLAN primaire. Mais un tel type de VLAN est également incapable de communiquer avec d'autres VLAN secondaires, y compris d'autres VLAN communautaires.

3.2.4.2 Types de port du PVLAN

Il existe trois types de port VLAN :

a)Port promiscuous :

ce type de port est capable d'envoyer et de recevoir des trames de n'importe quel autre port du VLAN. Il se connecte généralement à un commutateur de couche 3, un routeur ou d'autres dispositifs de passerelle.

b)Port isolé :

Existant dans un sous-VLAN, le port isolé se connecte à un hôte et ne peut communiquer qu'avec des ports promiscuous.

c)Port communautaire :

Le port communautaire réside également dans un sous-VLAN et se connecte à un hôte. Cependant, il ne peut dialoguer qu'avec les ports promiscuous et les autres ports communautaires du même sous-réseau.

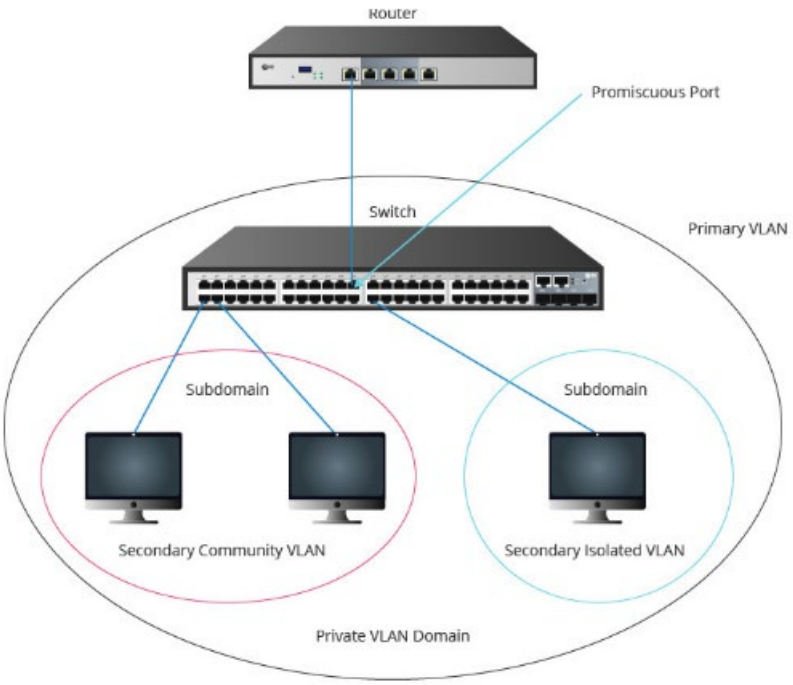

FIGURE 3.4 – VLAN privé .

3.2.4.3 Fonctionnement de PVLAN

Le VLAN privé traverse généralement les étapes suivantes :

1. Le VLAN primaire délivre les trames en aval du port promiscuous à tous les hôtes mappés.

2. Le VLAN isolé transporte les trames depuis les hôtes stub en amont vers le port promiscuous uniquement.

3. Les VLAN communautaires permettent l'échange bidirectionnel de trames au sein d'un même groupe communautaire. En même temps, il remontera les données vers les ports promiscuous.

4. La procédure d'apprentissage et de transfert de l'adresse MAC Ethernet reste la même, ainsi que la procédure d'inondation de diffusion/multicast dans les limites des VLAN primaires/secondaires.

3.2.5 VLANs ACL

Une liste de contrôle d'accès VLAN (VLAN Access Control List) est une liste de contrôle d'accès qui est appliquée à un VLAN. Elle permet de filtrer le trafic entrant et sortant d'un VLAN. Les ACLs VLAN sont utilisées pour contrôler le trafic entre les VLANs et pour protéger les ressources du réseau contre les accès non autorisés[1].

Les ACLs sont créées en deux parties :

• La première partie consiste à créer l'ACL elle-même, c'est-à-dire un nom d'ACL autorisant ou interdisant un réseau.

• La deuxième partie consiste à associer l'ACL à une interface d'un routeur, en entrée ou en sortie[2].

3.2.6 Avantages des VLANs

* La réduction des messages de diffusion (notamment les requêtes ARP) limités à l'intérieur d'un VLAN.

* Ainsi les diffusions d'un serveur peuvent être limités aux clients de ce serveur.

* La création de groupes de travail indépendants de l'infrastructure physique; possibilité de déplacer la station sans changer de réseau virtuel.

* L'amélioration de la sécurité par le contrôle des échanges inter-VLAN utilisant des routeurs (filtrage possible du trafic échangé entre les VLANs).

3.3 Protocoles de transport des VLANs

3.3.1 La norme 802.1Q

L'idée ici est de permettre à certains ports du commutateur d'être assignés à plusieurs VLAN, ce qui permet d'économiser du câblage et des ports sur le commutateur. Pour réaliser cela, on ajoute un marqueur dans l'en-tête de la trame Ethernet qui identifie le VLAN auquel la trame appartient. Au fil du temps, différentes solutions propriétaires ont été développées pour cela, mais un besoin de normalisation s'est fait sentir, ce qui a conduit à la création de la norme 802.1q en 1998. Cette norme a été mise en place pour normaliser le transport des VLANs et offrir une compatibilité entre les équipements réseau provenant de différents fabricants.

Cette figure 3.6 démontre la modification de la trame Ethernet conformément à la norme 802.1Q, qui inclut l'ajout d'un champ de 4 octets :[**22**]

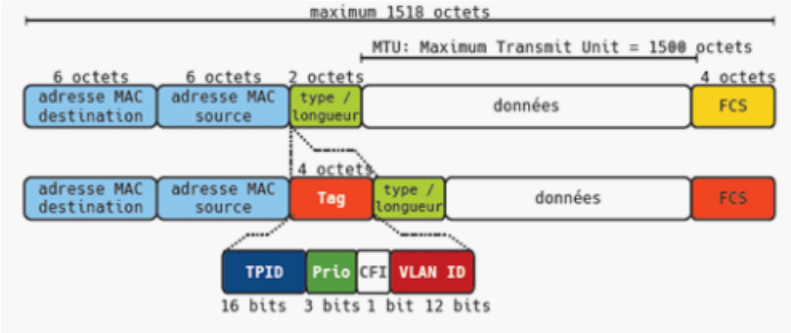

FIGURE 3.5 – Extension de la trame Ethernet modifiée par la norme 802.1 Q .

[22]

La figure 3.7 montre la norme 802.1

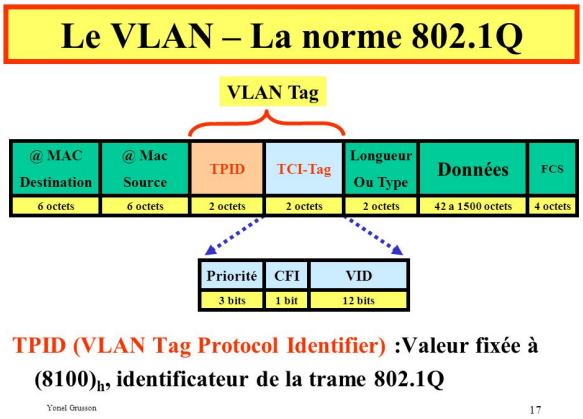

FIGURE 3.6 – La norme 802.1q.

3.3.2 Le protocole VTP

Le protocole VTP (Virtual Trunk Protocol) est un protocole développé par Cisco Systems pour faciliter la gestion des VLAN (Virtual Local Area Networks) sur un réseau étendu. Il permet aux administrateurs de gérer de manière centralisée les VLAN et d'automatiser leur distribution sur les commutateurs (switches) du réseau.

3.3.2.1 Fonctionnement du Protocole VTP

Le protocole VTP fonctionne en propageant les informations sur les VLANs à travers un réseau de switches. Ces informations incluent les ajouts, les suppressions et les modifications de VLAN. Pour ce faire, le VTP utilise un mécanisme de publicité qui envoie des mises à jour VTP appelées « VTP advertisements » à tous les switches du réseau. Ces mises à jour sont transmises sur les liens de trunk entre les switches, qui sont des liens utilisés pour transporter plusieurs VLAN simultanément. En plus du protocole VTP, d'autres protocoles tels que le Spanning Tree Protocol (STP) sont essentiels pour optimiser la gestion de votre réseau local. Le STP permet de prévenir les boucles de réseau qui pourraient survenir lors de l'utilisation de VLAN.[**22**]

Le VTP utilise trois modes de fonctionnement pour les switchesla (figure 3.8) :

a) Serveur VTP : Les switches configurés en mode serveur VTP peuvent créer, modifier et supprimer des VLAN. Ils propagent également les informations sur les VLANs à d'autres switches du réseau. En général, un ou plusieurs switches sont configurés en mode serveur pour gérer les VLAN de manière centralisée.

b)Client VTP

Les switches en mode client VTP ne peuvent pas créer, modifier ou supprimer des VLAN. Ils reçoivent les informations sur les VLANs du serveur VTP et les appliquent automatiquement. Ce mode permet d'automatiser la distribution des VLAN sur l'ensemble du réseau.

c)Transparent VTP

Les switches en mode transparent VTP ne participent pas activement au processus de propagation des VLAN. Ils ne mettent pas à jour leur propre base de données de VLAN en fonction des informations reçues, mais ils transmettent les annonces VTP aux autres switches du réseau. Ce mode est utile lorsque vous souhaitez isoler certains switches de la gestion centralisée des VLANs.

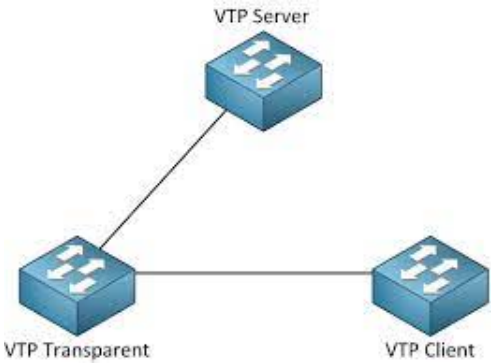

FIGURE 3.7 – Le protocole VTP.

3.3.2.2 Avantages du Protocole VTP

Le protocole VTP présente plusieurs avantages pour les administrateurs réseau :

- ➢ Gestion centralisée des VLAN : Avec le VTP, les administrateurs réseau peuvent gérer les VLAN à partir d'un ou plusieurs switches serveurs, simplifiant ainsi la gestion des VLAN sur un réseau étendu et évitant les erreurs de configuration.

- ➢ Automatisation de la distribution des VLAN : Les switches clients VTP reçoivent et appliquent automatiquement les informations sur les VLANs, ce qui réduit le temps et les efforts nécessaires pour déployer et maintenir les VLAN sur un grand réseau.

- ➢ Consistance des informations sur les VLANs : Grâce à la propagation des mises à jour VTP, les switches du réseau ont des informations cohérentes sur les VLANs, ce qui limite les problèmes de communication entre les différentes parties du réseau.

3.3.2.3 Inconvénients du Protocole VTP

Malgré ses avantages, le protocole VTP présente également des inconvénients :

→ Risque de propagation d'erreurs : Une erreur de configuration sur un switch serveur VTP peut être rapidement propagée à l'ensemble du réseau, entraînant des problèmes de communication ou des interruptions de service.

→ Limitations aux équipements Cisco : Le VTP étant une technologie propriétaire de Cisco, il n'est pas compatible avec les équipements d'autres fabricants. Ceci peut limiter son utilisation dans des réseaux multi-fabricants.

→ Risque de sécurité : Les attaques VTP peuvent être menées pour perturber la gestion des VLAN et compromettre la sécurité du réseau. Il est donc essentiel de sécuriser correctement le protocole VTP.
Cependant, d'autres mesures de sécurité sont également importantes, comme l'Inspection ARP Dynamique, qui est un outil incontournable pour la sécurité du réseau.

3.3.2.4 Meilleures pratiques pour optimiser et sécuriser le Protocole VTP

Pour tirer le meilleur parti du protocole VTP et minimiser ses inconvénients, voici quelques meilleures pratiques à mettre en œuvre :

— Utiliser des versions récentes du VTP : Les versions plus récentes du protocole VTP, telles que VTPv3, offrent des fonctionnalités supplémentaires et une meilleure sécurité. Il est donc recommandé d'utiliser la version la plus récente prise en charge par vos équipements.

— Mettre en place un mot de passe VTP : La configuration d'un mot de passe VTP sur tous les switches participant au domaine VTP permet d'authentifier les annonces VTP et d'empêcher les attaques malveillantes.

— Utiliser le mode Transparent lorsque nécessaire : Si certains switches ne doivent pas participer activement à la gestion des VLAN, configurez-les en mode Transparent pour éviter la propagation d'erreurs ou des problèmes de sécurité.

— Surveiller et auditer régulièrement la configuration VTP : Pour détecter rapidement les erreurs de configuration ou les anomalies, il est important de surveiller régulièrement les logs et l'état des switches VTP.

— Former les administrateurs réseau : La compréhension du fonctionnement du protocole VTP et des bonnes pratiques de gestion des VLAN est essentielle pour éviter les erreurs et les problèmes de sécurité.

— Assurez-vous que les membres de votre équipe réseau sont formés et à jour sur les meilleures pratiques. Lorsqu'il s'agit de la gestion des dates pour vos applications réseau, Java LocalDate est un outil puissant que vous devriez connaître. Il peut aider à gérer les horodatages, ce qui peut être utile pour le suivi et la résolution des problèmes de réseau[**22**].

3.3.3 EtherChannel

Dans le contexte d'une croissance constante des besoins en bande passante, des méthodes sont nécessaires pour améliorer les performances du réseau. Cisco a introduit une technique appelée EtherChannel, qui permet de regrouper plusieurs liens physiques en un seul lien logique. Cela permet d'augmenter la bande passante globale et de contourner les limitations imposées par le protocole STP (Spanning Tree Protocol).

L'EtherChannel fonctionne en combinant plusieurs ports actifs en un seul lien logique. Cela permet d'obtenir une bande passante plus élevée et d'améliorer les performances du réseau. Il est important de noter que les ports inclus dans un EtherChannel doivent être identiques et qu'un maximum de 8 ports peuvent être regroupés. Chaque switch peut prendre

en charge jusqu'à 6 EtherChannels.

En plus d'augmenter la bande passante, l'EtherChannel offre également une redondance. Si l'un des liens physiques inclus dans l'EtherChannel tombe en panne, la topologie du réseau reseau reste intacte tant qu'il reste au moins un lien physique fonctionnel. Cependant, la bande passante disponible sera réduite en cas de défaillance d'un lien.

Il existe deux méthodes pour configurer l'EtherChannel : le mode "ON", qui force l'interface à devenir membre de l'EtherChannel sans négociation, et l'utilisation de protocoles de négociation d'EtherChannel. Il existe deux protocoles de négociation couramment utilisés, dont je vais vous donner une brève explication.[**18**]

➢ **PAgP (Port Aggregation Protocol)**

est l'un des protocoles de négociation utilisés pour configurer l'EtherChannel dans les équipements Cisco. PAgP permet aux ports de négocier leur agrégation automatiquement, en identifiant les ports compatibles et en formant un EtherChannel. possède deux statuts :

1. **auto :** le port attend une requête du port voisin, si celui-ci est en mode Desirable une agrégation est créée, s'il est en mode Auto alors aucune agrégation n'est créée.
2. **Desirable :** le port configuré en mode Desirable négocie avec le port voisin, dans les deux cas : qu'il soit en mode Desirable également ou en mode Auto une agrégation est créée.

➢ **LACP (Link Aggregation Control Protocol)**

est un protocole de négociation utilisé pour configurer l'agrégation de liens, telle que l'EtherChannel, dans les réseaux informatiques. LACP permet aux équipements réseau de détecter automatiquement les ports compatibles et de les regrouper pour former un lien agrégé.et dont les statuts de port peuvent être :[**18**]

1. **Passive :** le port attend les paquets LACP du port voisin pour y répondre, et créer une agrégation si le port voisin est en mode Active.
2. **Active :** le port négocie avec le port voisin et établie une agrégation que ce dernier soit en mode active ou en mode passive[**18**].

3.4 Les réseaux privés virtuels (VPN)

3.4.1 Le fonctionnement d'un VPN

Un VPN utilise un protocole de tunnelisation pour établir un tunnel sécurisé entre l'utilisateur et le serveur VPN. Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu couteux aux intranets et aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme internet. Assurant ainsi la sécurité de la communication et la confidentialité des informations échangées sur Internet.[**16**]

3.4.2 Type de VPN

Il existe trois catégories de VPN :

a) **VPN site à site**

VPN de site à site, figure 3.9, également appelé VPN intranet ou extranet, permet de connecter deux sites d'une même entreprise (VPN intranet) ou de relier le site d'une entreprise à celui d'un fournisseur ou d'un client (VPN extranet). Pour ce faire, des équipements matériels tels que des routeurs, des pare-feu, etc., sont généralement interconnectés aux frontières des réseaux internes et publics de chaque site.

FIGURE 3.8 – VPN site à site .

b) **VPN Poste à site** La figure 3.10 présente une illustration de VPN Poste à Site qui per-

met aux utilisateurs distants de se connecter de manière sécurisée à un réseau d'entreprise sur Internet. Leur trafic est encapsulé et chiffré pour garantir la confidentialité et la sécurité des données pendant la transmission. Cela permet aux employés de se connecter aux ressources internes de l'entreprise, comme les applications, les fichiers partagés ou les bases de données, tout en bénéficiant de la sécurité offerte par le réseau privé virtuel. [**21**]

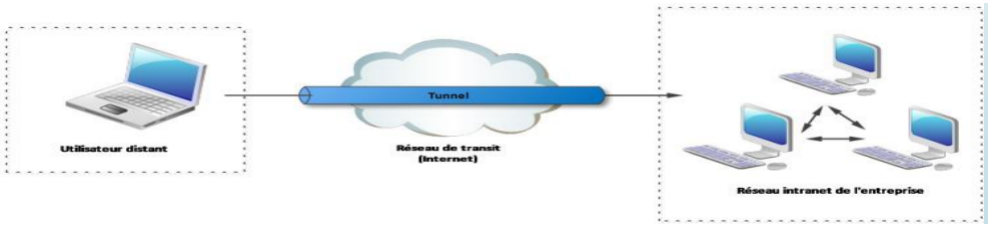

FIGURE 3.9 – VPN poste à site .

c) **VPN poste à poste**

Dans ce type de VPN, l'objectif est de créer une connexion sécurisée de bout en bout entre deux appareils, ou plus fréquemment entre un appareil et un serveur. Ces deux appareils peuvent être situés sur le même réseau ou sur des réseaux distincts qui sont interconnectés par un VPN de site à site.[**21**]

3.4.3 Avantages de VPN

- ➢ VPN Assurera Votre Sécurité (La sécurité en ligne et la protection de la vie privée).
- ➢ Garantir votre anonymat.
- ➢ Empêcher le suivi par les FAI et protéger vos données.
- ➢ La possibilité de télécharger et de streamer en toute sécurité.
- ➢ La suppression des restrictions géographiques de certains sites

3.5 Agrégation des liens (Norme 802.3 ad)

Agrégation des liens est une technique qui permet de combiner plusieurs connexions pour réseau physiques en une seule connexion logique, pour améliorer la bande passante ,la fiabilité et assurant la redondance de liens entre les équipements.[**22**]
Cela offre plusieurs avantages, notamment :

- ➢ Amélioration de la fiabilité et de la disponibilité : si l'une des connexion physiques d'une agrégation de liens tombe en panne , le trafic automatiquement réacheminé de manière dynamique et transparent vers les autres connexions disponibles
- ➢ Une meilleure utilisation des ressources physiques : Le trafic peut être réparti de manière équilibrée sur les différentes connexions physiques, permettant une utilisation optimale des ressources.
- ➢ Augmentation de la bande passante : L'agrégation de liens combine les capacités des connexions physiques agrégées, offrant ainsi une bande passante globale supérieure à celle de chaque connexion individuelle.
- ➢ Rentabilité : L'ajout de nouvelles connexions physiques peut être coûteux, notamment en termes de câblage. L'agrégation de liens permet d'augmenter la bande passante sans nécessiter l'acquisition de nouveaux équipements.[**22**]

3.6 Protocole de tunnelisation IP sec

Protocole IP sec (Internet Protocol Security) est un ensemble de protocoles utilisé pour sécuriser les communications sur les réseaux IP. Il fournit des mécanismes de confidentialité, d'intégrité des données et d'authentification entre les différents nœuds d'un réseau. IP sec est généralement utilisé pour sécuriser les connexions VPN (Virtual Private Network) utilisées par les organisations pour établir des connexions sécurisées entre des sites distants ou pour permettre aux utilisateurs distants de se connecter au réseau de l'entreprise de manière sécurisée.

Mode utilisation de IP sec :

Le protocole IP sec peut être utilisé de deux manières principales : en mode de transport et en mode tunnel. En mode de transport, IP sec sécurise uniquement la partie transport des paquets IP. Cela signifie que seules les données elles-mêmes sont protégées, tandis que les en-têtes IP d'origine sont laissés intacts. Le mode de transport est généralement utilisé pour sécuriser les connexions entre deux hôtes finaux. En mode tunnel, IPsec encapsule les paquets IP d'origine dans de nouveaux paquets IPsec. Les en-têtes IP d'origine sont protégés et les paquets IPsec sont acheminés de manière sécurisée entre les passerelles ou les équipements réseau. Le mode tunnel est couramment utilisé pour sécuriser les connexions VPN entre les sites distants.[**22**]

3.7 Redondance au premier saut

Comme nous montre la figure 3.11 ,l'un des moyens permettant d'éliminer un point de défaillance unique au niveau de la passerelle par défaut consiste à implémenter un routeur virtuel. Pour implémenter ce type de redondance de routeur, plusieurs routeurs sont configurés pour un fonctionnement conjoint, de manière à présenter l'illusion d'un routeur unique au regard des hôtes du LAN, comme illustré dans la figure. En partageant une adresse IP et une adresse MAC, plusieurs routeurs peuvent jouer le rôle d'un routeur virtuel unique. L'adresse IP du routeur virtuel est configurée comme passerelle par défaut pour les stations de travail sur un segment IP spécifique. Lorsque les trames sont envoyées par les périphériques hôtes vers la passerelle par défaut, ces hôtes utilisent le protocole ARP pour résoudre l'adresse MAC associée à l'adresse IP de la passerelle par défaut. La résolution ARP renvoie l'adresse MAC du routeur virtuel.Plusieurs protocoles offrent ce service :

- **HSRP (Host Standby Router Protocol)**

  est un protocole de routage de premier saut (First Hop Redundancy Protocol) utilisé dans les réseaux informatiques pour fournir une redondance et une haute disponibilité pour les passerelles par défaut. Son objectif principal est de permettre à plusieurs

routeurs de fonctionner ensemble en tant qu'unité virtuelle, fournissant ainsi une passerelle par défaut commune aux hôtes du réseau. [**18**]

- **GLBP (Gateway Load Balancing Protocol) :**

  Qui est un protocole de redondance du premier saut propriétaire Cisco, où dans une telle topologie, le trafic vers la passerelle est partagé entre les routeurs réels, offrant ainsi un équilibrage de charge. Il existe deux versions : GLBP pour IPv4 et GLBP pour IPv6.[**18**]

- **VRRP (Virtual Redondancy Protocol) :**

  Qui est défini par le standard IETF, VRRP élit un routeur principal qui achemine le trafic et des routeurs de secondaire ; le routeur virtuel se verra attribuer une adresse IP et une adresse MAC virtuelles constituant la passerelle. Il existe en deux versions VRRPv2 pour IPv4 et VRRPv3 pour IPv4 et IPv6[**18**]

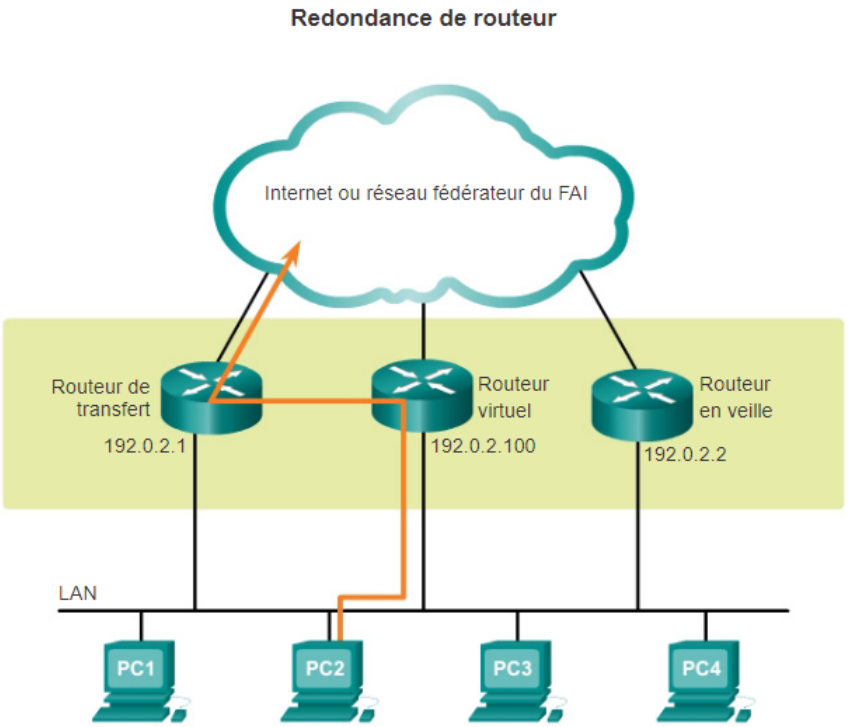

FIGURE 3.10 – Redondance de routeur .

Un protocole de redondance offre le mécanisme nécessaire pour déterminer quel routeur

doit être actif dans le réacheminement du trafic. Il détermine également quand le rôle de réacheminement doit être repris par un routeur en veille. La transition d'un routeur de transfert à un autre est transparente pour les périphériques finaux.

3.8 Load Balancing

L'équilibrage de charge, ou load balancing en anglais, fait référence à la répartition du trafic réseau entrant sur plusieurs serveurs ou ressources afin d'optimiser les performances, maximiser l'utilisation des ressources et assurer une disponibilité élevée. Cela est couramment utilisé dans les réseaux informatiques, les applications web et les clusters de serveurs. Le but du load balancing est d'optimiser la performance globale de l'infrastructure, son efficacité et sa capacité réseau..

- **Son fonctionnement :**

  La répartition de charge est effectuée par un algorithme, s'appuyant sur le DNS (Domain Name System). L'utilisateur accède aux sites internet via une URL, liée à une adresse IP. Cette dernière contacte le répartiteur de charge, qui transmet la demande au serveur. La répartition dépendra alors du type d'algorithme utilisé. Les quatre plus connus sont : Round Robin, Weighted Round Robin, Least Connections et Weighted Least Connections.

- **Avantages et importance du load balancer :**

  Le principal avantage d'un load balancer est de réduire le temps de réponse d'un site suite aux requêtes des utilisateurs. En effet, optimiser la charge de travail des serveurs limite les risques de pannes liés à une surcharge. Si une machine devient indisponible, les utilisateurs seront redirigés vers un autre serveur et auront toujours accès aux pages. Vous leur assurez donc une expérience optimale, grâce à une qualité de service constante : hébergement flexible, haute disponibilité, évolutivité, etc. Le load balancer reste particulièrement adapté au e-commerce, où des fluctuations de trafic importantes peuvent entraîner des surcharges. Il vous permet de maintenir des fonctionnalités homogènes sur vos sites, d'entretenir votre image en ligne, ainsi que de ras-

surer vos clients. Concrètement, il n'y aura pas de paniers perdus ou d'opérations de paiement interrompues.

3.9 Active Directory

Active Directory est un service de gestion d'annuaire développé par Microsoft. Il est utilisé principalement dans les environnements Windows pour gérer et organiser les ressources réseau, telles que les utilisateurs, les ordinateurs, les groupes et les stratégies de sécurité.

➢ **Avantages d'Active Directory**

Active Directory simplifie la vie des administrateurs et des utilisateurs finaux tout en renforçant la sécurité des organisations. Les administrateurs bénéficient d'une gestion centralisée des utilisateurs et des droits d'accès, ainsi que d'un contrôle centralisé de la configuration des ordinateurs et des utilisateurs grâce à la fonctionnalité Stratégie de groupe AD. Il suffit aux utilisateurs de s'authentifier une fois pour accéder facilement à toutes les ressources du domaine pour lequel ils disposent d'autorisations (authentification unique). Par ailleurs, les fichiers sont stockés dans un espace de stockage central où ils peuvent être partagés avec d'autres utilisateurs pour faciliter la collaboration, mais aussi sauvegardés en bonne et due forme par les équipes informatiques qui veillent à la continuité de l'activité.

➢ **Fonctionnement du Active Directory**

Le service Active Directory principal est un service de domaine Active Directory (Active Directory Domain Services, AD DS), qui fait partie du système d'exploitation Windows Server. Les serveurs qui exécutent AD DS sont des contrôleurs de domaine. En règle générale, les organisations disposent de plusieurs contrôleurs de domaine, et chacun d'entre eux possède une copie de l'annuaire pour la totalité du domaine. Les modifications apportées à l'annuaire sur l'un des contrôleurs de domaine (la mise à jour d'un mot de passe ou la suppression d'un compte d'utilisateur, par exemple) sont répliquées sur les autres contrôleurs de domaine afin que tous restent à jour. Un serveur de catalogue global est un contrôleur de domaine qui stocke une copie complète de

tous les objets dans l'annuaire de son domaine et une copie partielle des objets de tous les autres domaines dans la forêt. Ainsi, les utilisateurs et les applications peuvent trouver des objets dans n'importe quel domaine de leur forêt. Les ordinateurs de bureau, les ordinateurs portables et les autres appareils sous Windows (autre que Windows Server) peuvent intégrer un environnement Active Directory, mais ils n'exécutent pas AD DS. AD DS s'appuie sur plusieurs protocoles et normes établis, y compris les protocoles LDAP (Lightweight Directory Access Protocol), Kerberos et DNS (Domain Name System).

Il est important de noter qu'Active Directory s'adresse exclusivement aux environnements Microsoft sur site. Les environnements Microsoft qui se trouvent dans le Cloud utilisent Azure Active Directory, qui remplit les mêmes fonctions que son alter ego local. Bien qu'AD et Azure AD soient des outils distincts, ils peuvent, dans une certaine mesure, fonctionner de concert si votre organisation dispose d'environnements informatiques sur site et dans le Cloud (un déploiement hybride).

3.10 Conclusion

En résumé, ce chapitre nous a permis d'explorer divers aspects des liaisons virtuelles, tels que les VLANs, les VPNs, l'agrégation des liens, la redondance, ainsi que de mettre en évidence le fonctionnement et les avantages de l'Active Directory. La compréhension de ces concepts et technologies est cruciale pour améliorer la gestion et la sécurité des réseaux informatiques. Dans le chapitre suivant, nous passerons de la théorie à la pratique en abordant la configuration des liaisons virtuelles.

CHAPITRE 4

CONFIGURATION DES LIAISONS VIRTUELLES (VLANS , VPNS, REDONDANCE ET AGRÉGATION DES LIENS)

4.1 Introduction

Dans le cadre de notre projet visant à mettre en place des solutions pour le réseau de l'entreprise Générale Emballage, nous allons entamer la phase de déploiement de nos propositions. Tout d'abord, nous allons présenter les logiciels que nous utiliserons pour la réalisation du projet. Ensuite, nous détaillerons les étapes essentielles pour sa mise en œuvre, en mettant en avant les tests que nous avons effectués et les résultats que nous avons obtenus.

4.2 Outils de réalisation

1.GNS3

GNS3 (Graphical Network Simulator) est un logiciel de simulation et d'émulation de réseaux qui se concentre principalement sur les équipements Cisco tels que les routeurs et les commutateurs. Il offre la possibilité de créer des topologies réseaux virtuelles, d'émuler les systèmes d'exploitation des équipements Cisco, et de reproduire fidèlement leur comportement dans un environnement virtuel. Cela permet aux utilisateurs de tester, configurer et dépanner des réseaux complexes, en offrant une expérience réaliste et pratique pour travailler avec les équipements Cisco.
La Figure 4.1 permet de visualiser l'illustration correspondante au logo de logiciel [**empty citation**].

FIGURE 4.1 – Logo GNS3.

2.VMware

VMware est un logiciel développé par VMware Inc, qui permet la virtualisation des ma-

chines. Il offre la possibilité d'exécuter plusieurs instances d'un même système d'exploitation ou d'exécuter simultanément plusieurs systèmes d'exploitation différents sur une seule machine . Il est compatible avec une variété de systèmes d'exploitation et peut être utilisé sur un PC Windows ou Linux. En plus de cela, VMware propose des outils de déploiement tels que VMware ACE, qui permet de stocker le bureau d'un utilisateur sur une clé USB pour faciliter la mobilité. Le logiciel permet également de créer des environnements virtuels complets incluant des serveurs, du stockage et des réseaux.
Veuillez vous référer à la Figure 4.2 pour visualiser l'illustration[**24**].

FIGURE 4.2 – Logo VMWARE .

3.Windows 10

Windows 10 est un système d'exploitation développé par Microsoft,succédant à Windows 8. Windows 10 a été conçu pour offrir une expérience utilisateur améliorée, combinant les fonctionnalités appréciées de Windows 7 avec les nouveautés introduites dans Windows 8.veuillez consulter la Figure 4.3 pour visualiser l'illustration[**24**].

FIGURE 4.3 – Logo Windows .

4. Wireshark

Wireshark est un analyseur de protocole réseau gratuit et open source qui permet aux utilisateurs de visualiser de manière interactive le trafic de données sur un réseau informatique.

5.Windows Server 2022

Server 2022 est une version du système d'exploitation serveur développé par Microsoft. Windows Server 2022 est une plate-forme conçue pour prendre en charge les besoins de gestion et de traitement des données des entreprises.

4.3 Environement de travail

4.3.1 Installation de GNS3 sous windows

Une fois le fichier GNS3 téléchargé, nous procéderons à son exécution et suivrons les étapes d'installation jusqu'à leur terme, comme illustré dans les figures 4.4.

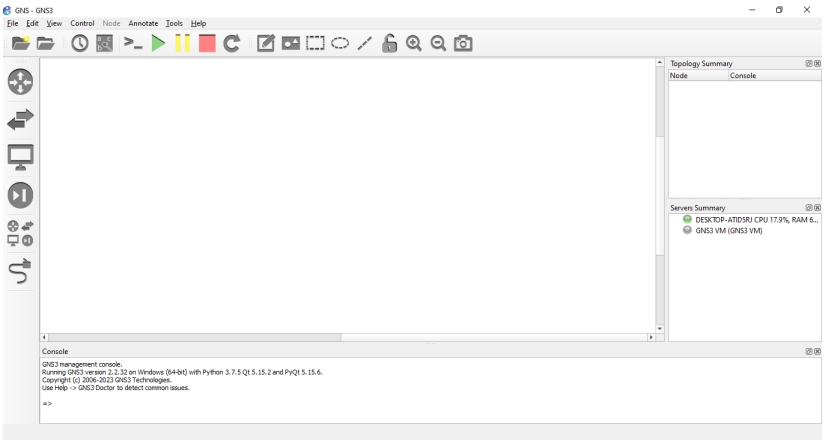

FIGURE 4.4 – Installation de GNS3 sous windows .

4.3.2 Installation de VMWare sous windows

Afin de créer des machines virtuelles, nous devrons procéder à l'installation de VMware Workstation en suivant les illustrations 4.5 :

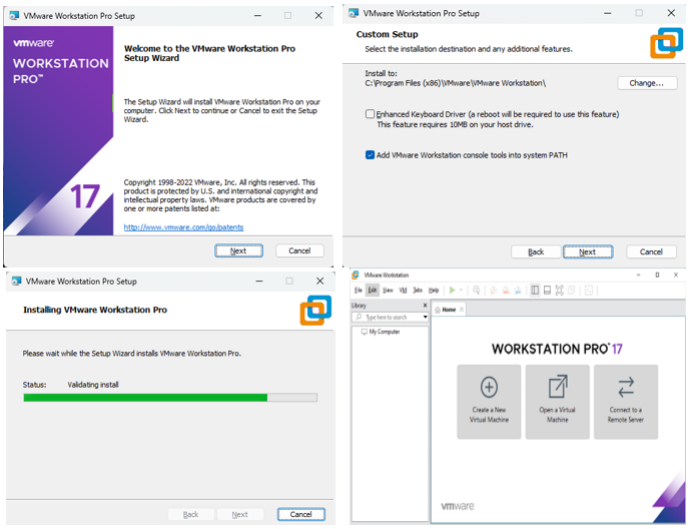

FIGURE 4.5 – Installation de VMWare sous windows .

4.4 Création et déploiement de machines virtuelles

4.4.1 Création du client windows 10

Pour créer une nouvelle machine virtuelle, nous commençons par cliquer sur "File" puis "Nouvelle machine virtuelle" dans le menu. Ensuite, nous suivons les étapes indiquées pour configurer les paramètres de la machine virtuelle.

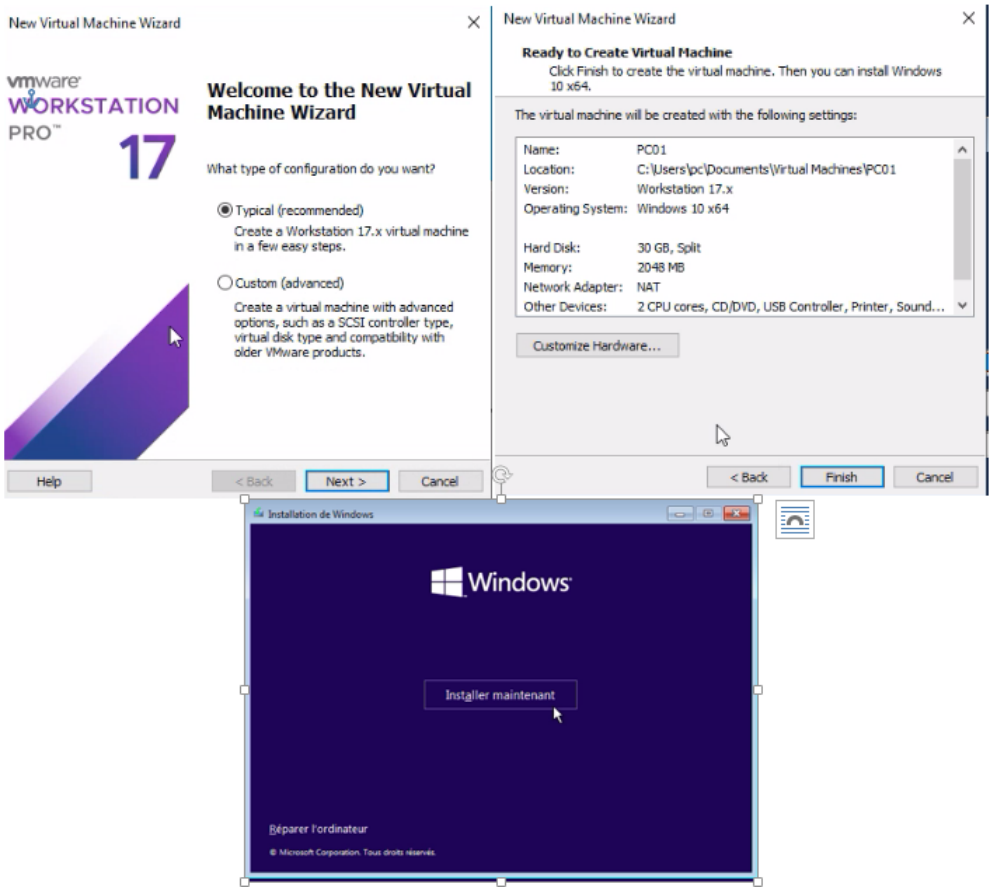

FIGURE 4.6 – Étapes d'Installation du client windows 10 .

Une fois la création terminée, nous procédons à l'installation de l'OS. Après avoir installé la machine virtuelle du PC01, nous devrons créer deux autre machine cliente (PC02,PC03) en les clonant à partir de la première. Pour ce faire, nous effectuons une clique droite sur la fenêtre machine PC01 >Manage>clone.

4.4.2 Création de windows serveur 2022

Pour créer et installer une machine virtuelle Windows serveur 2022, nous suivons les mêmes étapes que pour la création des machines virtuelles clientes précédentes

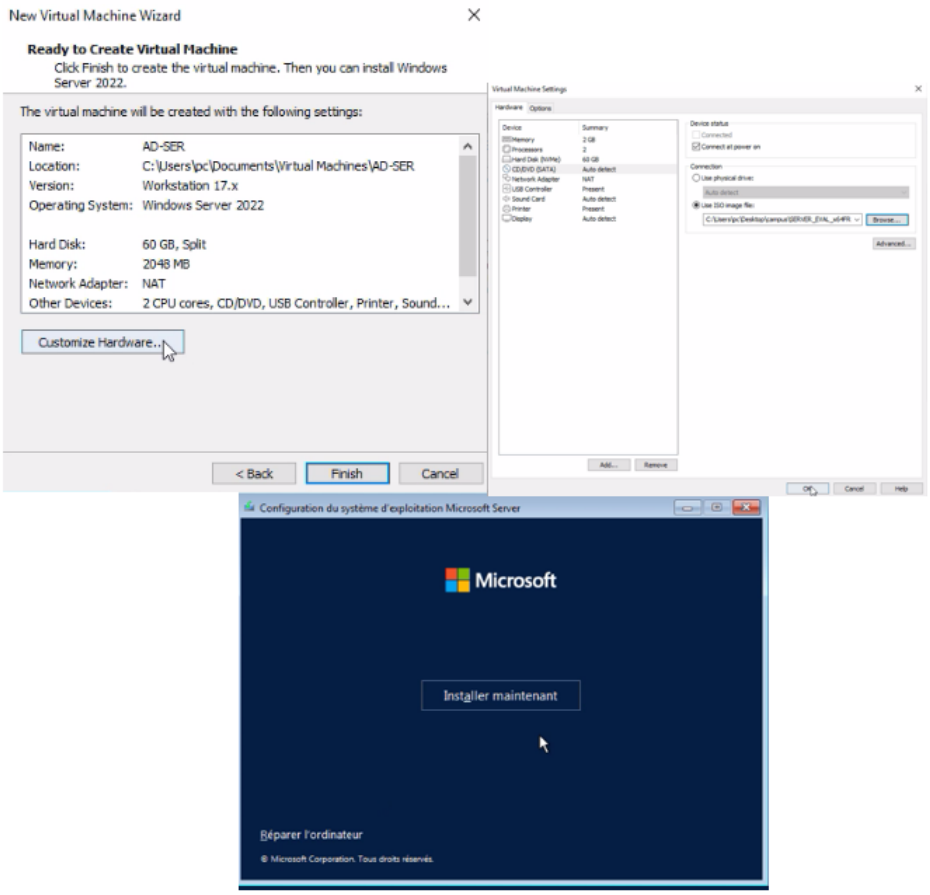

FIGURE 4.7 – Étapes de création du serveur windows 2022 .

4.4.2.1 Configuration de serveur Active directory

Après la création et l'installation d'une machine virtuelle Windows server 2019 nous avons suivi les étapes indiqué dans la figure 4.8 afin de configurer le serveur Active directory

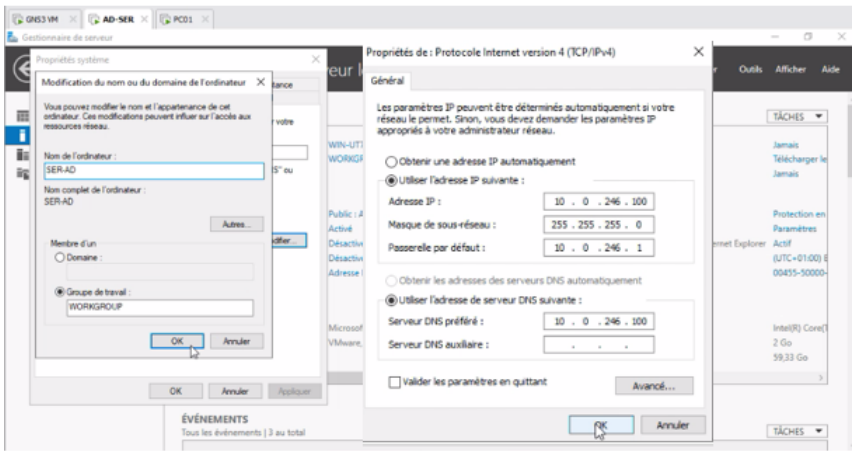

FIGURE 4.8 – Étapes de configuration du serveur Active Directory .

4.4.2.2 Ajouts des rôles et fonctionnalités

Après avoir installé le serveur windows serveur 2022 on peut maintenant ajouter des rôles et des serveur dans notre cas nous avons installé le serveur DNS et le nouveau domaine comme nous montre la figure 4.9 :

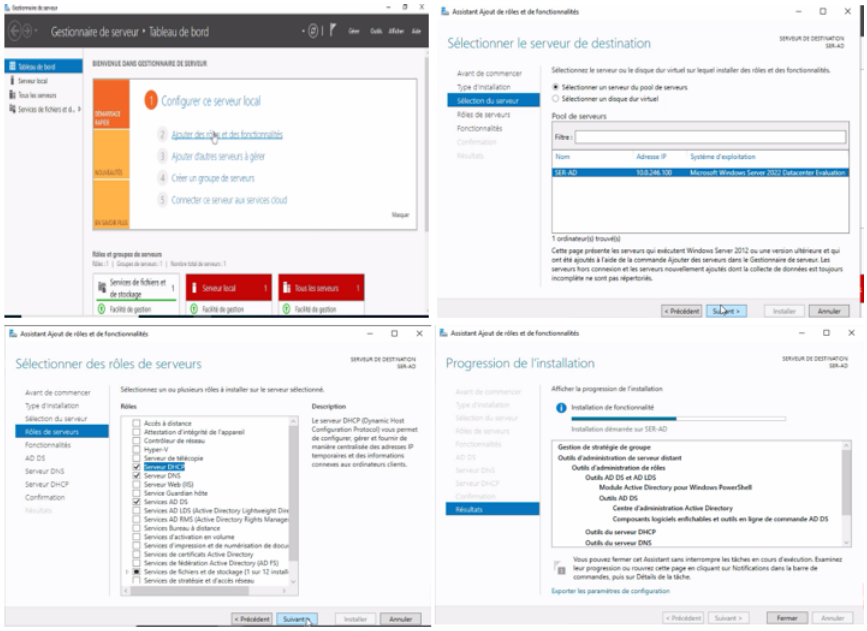

FIGURE 4.9 – Ajouts des rôles et fonctionnalités au serveur Active Directory .

4.4.2.3 Test du serveur Active Directory

Afin d'assurer la bon fonctionnement de notre serveur nous avons exécuter la commande "PING" comme illustré dans la figure 4.10

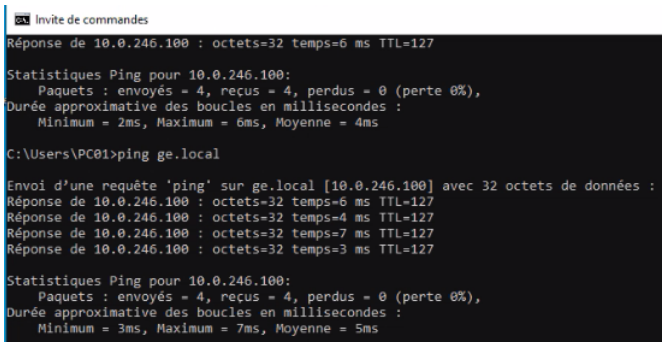

FIGURE 4.10 – Test DNS.

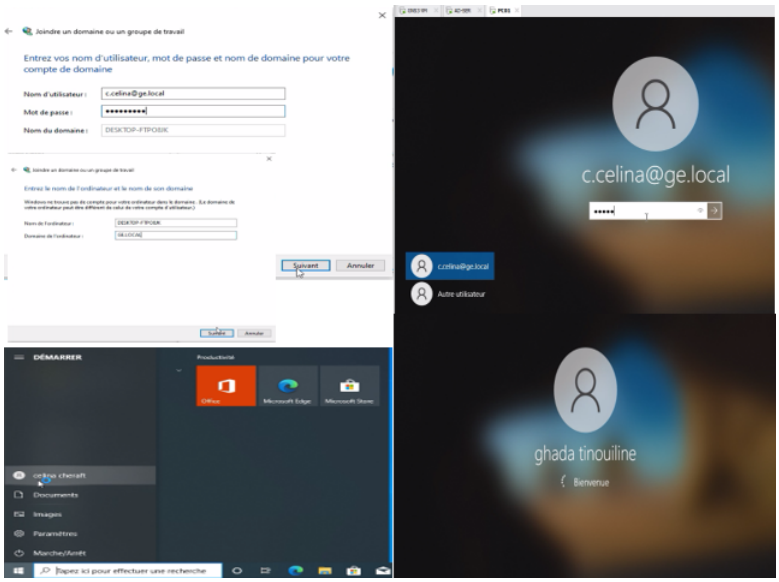

FIGURE 4.11 – Test Active Directory.

4.4.3 Installation des cisco IOU (Switch et Routeur)

Nous allons voir comment importer une image IOS Cisco dans un élément réseau (routeur, switch) d'un réseau virtuel GNS3.

Pour démarrer un élément actif comme un routeur Cisco dans GNS3, il faut cependant que celui-ci ait une véritable image d'un IOS Cisco à disposition, comme c'est le cas d'ailleurs

sur un routeur réel. On doit pour cela passer dès le début de notre prise en main de GNS3 par cette phase d'importation d'une image IOS Cisco dans GNS3. C'est une procédure relativement simple, mais qui comporte tout de même quelques subtilités qu'il faut connaître pour utiliser pleinement les fonctionnalités de GNS3.

La Figure 4. 12 montre comment télécharger et importer des images IOS Cisco.

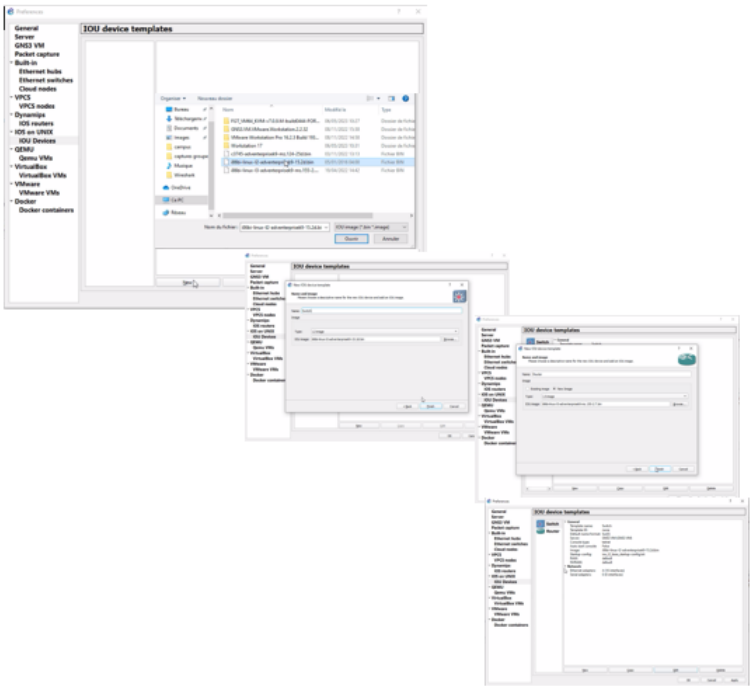

FIGURE 4.12 – Étapes d'installation des images IOU cisco (Switch et Routeur) .

4.4.4 Installation des Firewalls Fortigate

Les étapes à suivre pour procéder à l'installation des firewalls sont présentées dans la figure 4.13.

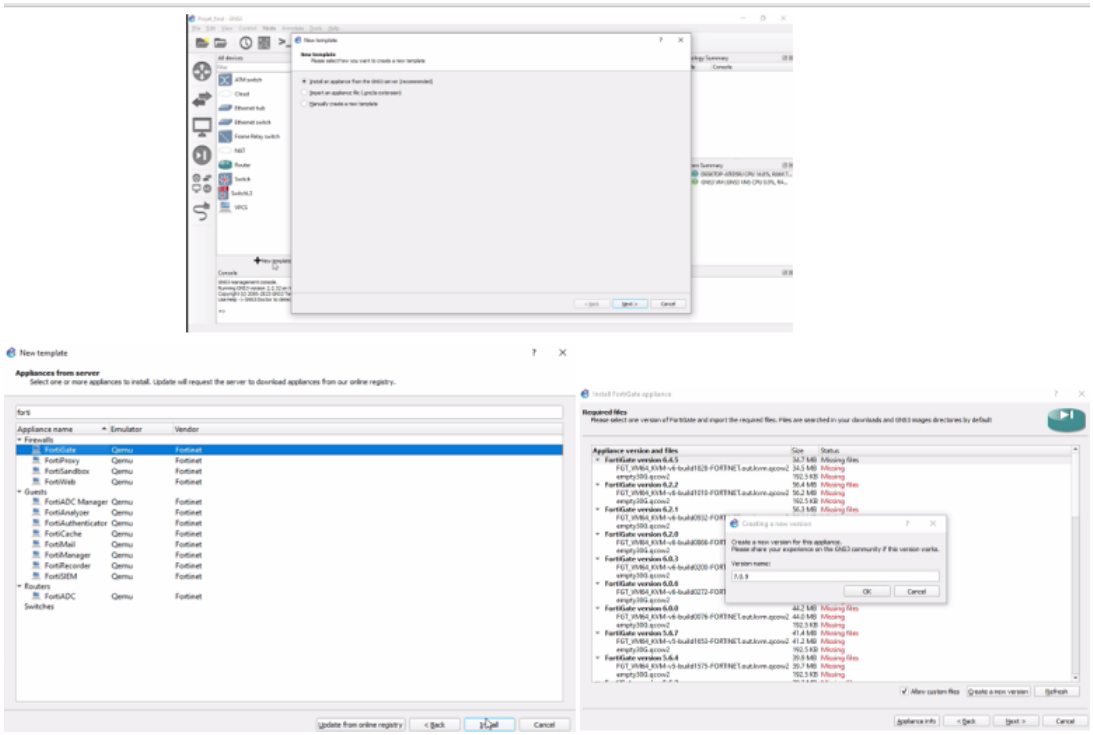

FIGURE 4.13 – Étapes d'installation des Firwalls .

4.5 Création et Configuration des Cartes réseaux virtuelles

Pour créer les cartes réseaux, nous allons cliquer sur Edit >Prefrences>VMWare VMS >Adva-ced local settings , puis suivre les étapes indiquées dans la figure 4.15 .

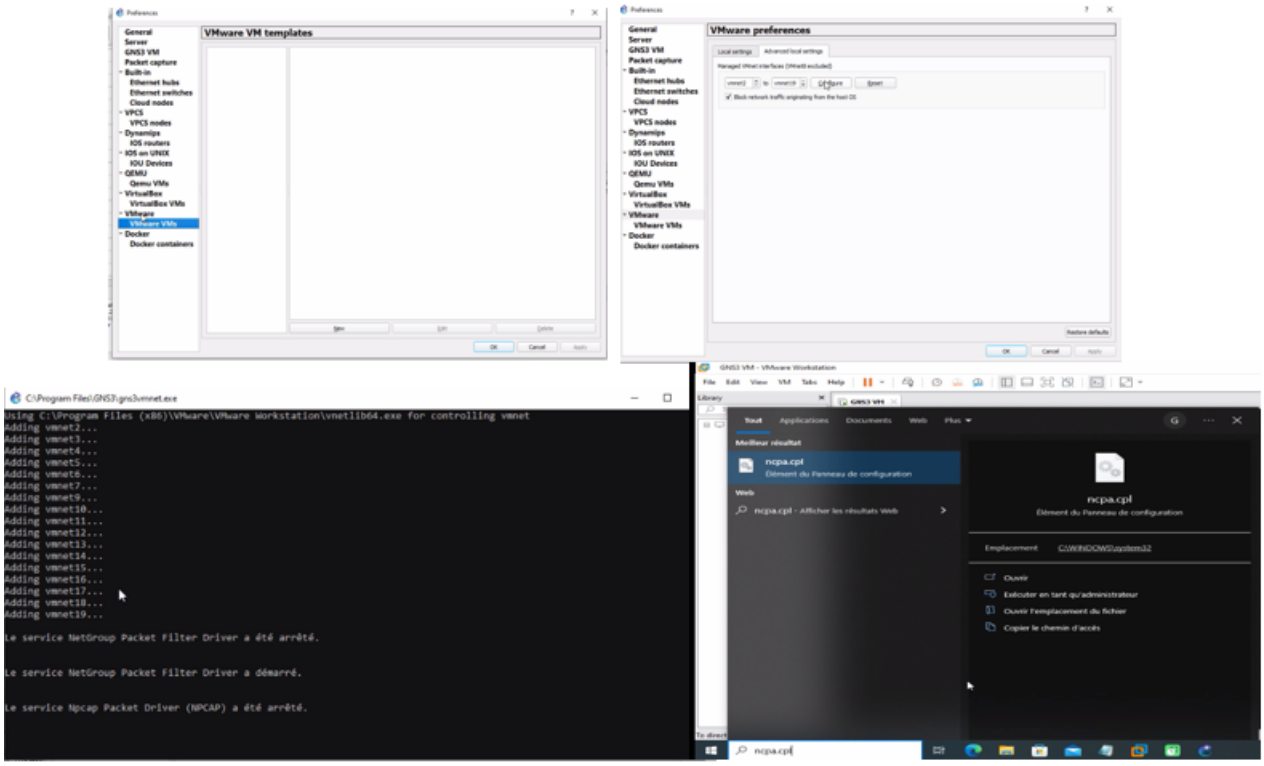

FIGURE 4.14 – Étapes de création des cartes réseaux virtuelle .

4.6 Architecture proposée

L'architecture proposée est illustrée dans la figure 4.15 est un découpage de l'architecture réseau en trois couches distinctes est en grande partie basé sur la répartition des rôles entre routage et commutation.

La première partie : La première couche, également appelée couche d'accès, est le niveau où l'on assure la redondance des passerelles réseau par défaut des hôtes. Cette couche doit être riche en fonctionnalités diverses et ne se limite plus à simplement fournir des ports de commutation pour les postes de travail fixes. Elle prend en charge des systèmes variés.

La deuxième partie : La deuxième couche, la couche de distribution, est responsable de garantir la haute disponibilité et de relier la couche d'accès à la couche cœur.

La troisième partie : La troisième couche, correspondant à la couche cœur, constitue la

partie principale du réseau de l'entreprise, interconnectant les blocs fonctionnels d'équipements. Les objectifs majeurs à ce niveau sont les performances, la stabilité et la minimisation de la complexité. C'est pourquoi, généralement, on ne trouve que deux routeurs redondants à ce niveau.

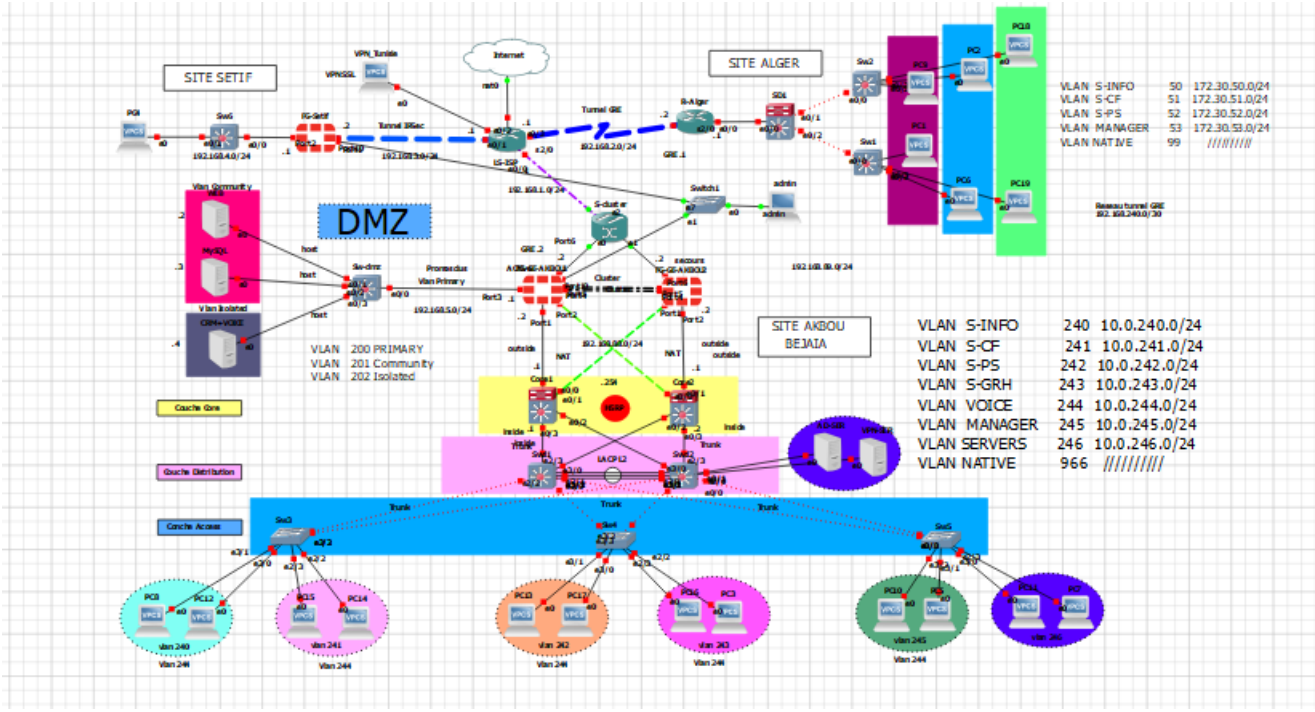

FIGURE 4.15 – Architecture réseau .

4.7 Plan d'adressage

4.7.1 Tableaud'adressage général

Le tableau 4.1 présenter le tableau d'adressage général utiliser .

4.7.2 Tableau d'adressage de routage intre-VLAN et HSRP

Le tableau 4.2 présenter le tableau d'adressage de routage intre-VLAN et HSRP utiliser .

Nom du équipement	Interface	Adressage	Masque
FG-Setif	Port 10	192.168.89.10	255.255.255.0
	Port 1	192.168.3.2	//
FG-Akbou2	Port 10	192.168.89.11	//
	Port 6	192.168.1.2	//
LS-ISP	Ethernet0/1	192.168.3.1	//
	Ethernet 0/0	192.168.1.1	//
	Ethernet 0/3	192.168.146.131	//
Core2	Ethernet 0/1	192.168.88.1	//
Core1	Ethernet 0/0	192.168.88.1	//

TABLE 4.1 – Tableau d'adressage général.

Nom du routeur	Interface	Adressage	Passerelle	address virtuelle
Core 1	L'encapsulation dot1q Ethernet 0/3.240	10.0.240.1	10.0.240.1	
	L'encapsulation dot1q Ethernet 0/3.241	10.0.241.1	10.0.240.1	10.0.241.254
	L'encapsulation dot1q Ethernet 0/3.242	10.0.242.1	10.0.240.1	10.0.242.254
	L'encapsulation dot1q Ethernet 0/3.243	10.0.243.1	10.0.240.1	10.0.243.254
	L'encapsulation dot1q Ethernet 0/3.244	10.0.244.1	10.0.240.1	10.0.244.254
	L'encapsulation dot1q Ethernet 0/3.245	10.0.245.1	10.0.240.1	10.0.245.254
	L'encapsulation dot1q Ethernet 0/3.246	10.0.246.1	10.0.240.1	10.0.246.254
Core 2	L'encapsulation dot1q Ethernet 0/3.240	10.0.240.2	10.0.240.2	10.0.241.254
	L'encapsulation dot1q Ethernet 0/3.241	10.0.241.1	10.0.240.2	10.0.242.254
	L'encapsulation dot1q Ethernet 0/3.245	10.0.245.1	10.0.240.2	10.0.245.254
	L'encapsulation dot1q Ethernet 0/3.246	10.0.246.1	10.0.240.2	10.0.246.254
R-alger	Ethernet 0/0.50	172.30.50.1	192.168.88.254	//
	Ethernet 0/0.51	172.30.51.1	192.168.88.254	//
	Ethernet0/0.52	172.30.52.1	192.168.88.254	//
	Ethernet 0/0.53	172.30.53.1	192.168.88.254	//
	Serial 2/0	192.168.2.2	192.168.2.1	//

TABLE 4.2 – Tableau d'adressage de routage intre-VLAN et HSRP .

Nom du VLAN	ID du VLAN	Adresse du sous-réseau	Passerelle du sous-réseau
VLAN S-INFO	240	10.0.240.0 /24	10.0.240.254
VLANS- CF	241	10.0.241.0 /24	10.0.241.254
VLAN S-PS	242	10.0.242.0 /24	10.0.242.254
VLAN S-GRH	243	10.0.243.0 /24	10.0.243.254
VLAN VOICE	244	10.0.244.0 /24	10.0.244.254
VLAN Manger	245	10.0.245.0 /24	10.0.245.254
VLAN SERVERS	246	10.0.246.0 /24	10.0.246.254
VLAN NATIVE	966	/	/

TABLE 4.3 – Tableau d'adressage de VLANs

Nom du PVLAN	ID du pVLAN	Adresse du sous-réseau	Passerelle du sous-réseau
Primary	200	192.168.5.1	192.168.5.1
Community	201	192.168.5.2/24	192.168.5.1
	//	192.168.5.3/24	192.168.5.1
Isolated	202	192.168.5.4/24	192.168.5.1

TABLE 4.4 – Tableau d'adressage du Private VLANs

4.7.3 Tableau d'adressage de VLANs

Le tableau 4.3 présenter le tableau d'adressage de VLANs utiliser .

4.7.4 Tableau d'adressage de routage Private-VLAN

Le tableau 4.4 présenter le tableau d'adressage de routage Private-VLAN utiliser .

4.8 Configurations des commutateurs

Pour commencer,nous allons configurer les commutateurs pour permettre l'interconnexion des différents segments.

4.8.1 Configuration des interfaces trunk

Pour cela nous avons utilisé la configuration suivante sur les deux switches distribution(Swd1,Swd2,SD1), ainsi que les switches Access(Sw3,Sw4,Sw5,Sw1,Sw2).

```
Swd1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Swd1(config)#in
Swd1(config)#interface ran
Swd1(config)#interface range eth
Swd1(config)#interface range ethernet 2/0-2, ethernet 3/1-3
Swd1(config-if-range)#sw
Swd1(config-if-range)#switchport tr
Swd1(config-if-range)#switchport trunk en
Swd1(config-if-range)#switchport trunk encapsulation do
Swd1(config-if-range)#switchport trunk encapsulation dot1q
Swd1(config-if-range)#sw
Swd1(config-if-range)#switchport mo
Swd1(config-if-range)#switchport mode  tr
Swd1(config-if-range)#switchport mode  trunk
```

FIGURE 4.16 – Configuration du Trunk sur Swd1.

```
SD1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SD1(config)#in
SD1(config)#interface  ran
SD1(config)#interface  range  eth
SD1(config)#interface  range  ethernet 0/1-2
SD1(config-if-range)#sw
SD1(config-if-range)#switchport tr
SD1(config-if-range)#switchport trunk en
SD1(config-if-range)#switchport trunk encapsulation do
SD1(config-if-range)#switchport trunk encapsulation do
SD1(config-if-range)#switchport trunk encapsulation do
SD1(config-if-range)#switchport trunk encapsulation do
SD1(config-if-range)#switchport trunk encapsulation dot1q
SD1(config-if-range)#sw
SD1(config-if-range)#switchport mo
SD1(config-if-range)#switchport mode  tr
SD1(config-if-range)#switchport mode  trunk
SD1(config-if-range)#
SD1(config-if-range)#sw
SD1(config-if-range)#switchport tr
SD1(config-if-range)#switchport trunk n
SD1(config-if-range)#switchport trunk native v
SD1(config-if-range)#switchport trunk native vlan 99
```

FIGURE 4.17 – Configuration du Trunk sur SD1.

4.8.2 Configuration du VLAN native

Configuration du switch access Sw3 plus le VLAN nativ comme illustré dans la figure 4.18 et 4.19

```
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#in
Sw3(config)#interface  ran
Sw3(config)#interface  range eth
Sw3(config)#interface  range ethernet 3/2-3
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport tr
Sw3(config-if-range)#switchport trunk en
Sw3(config-if-range)#switchport trunk encapsulation do
Sw3(config-if-range)#switchport trunk encapsulation dot1q
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport mo
Sw3(config-if-range)#switchport mode  tr
Sw3(config-if-range)#switchport mode  trunk
```

FIGURE 4.18 – Configuration du Trunk sur Sw3.

```
Sw3(config-if-range)#switchport trunk native vlan 966
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport tr
Sw3(config-if-range)#switchport trunk all
Sw3(config-if-range)#switchport trunk allowed vl
Sw3(config-if-range)#switchport trunk allowed vlan  240-245,966
```

FIGURE 4.19 – Configuration du VLAV nativ sur Sw3.

```
Swd1#show  interfaces tr
Swd1#show  interfaces trunk

Port        Mode             Encapsulation  Status        Native vlan
Et2/0       on               802.1q         trunking      966
Et2/1       on               802.1q         trunking      966
Et2/2       on               802.1q         trunking      966
Et3/1       on               802.1q         trunking      966
Et3/2       on               802.1q         trunking      966
Et3/3       on               802.1q         trunking      966

Port        Vlans allowed on trunk
Et2/0       240-245,966
Et2/1       240-245,966
Et2/2       240-245,966
Et3/1       240-245,966
Et3/2       240-245,966
```

FIGURE 4.20 – Vérification interface Trunk.

4.8.3 Configuratuion du VTP

Dans le but d'ajouter, renommer ou supprimer un ou plusieurs VLANs et de faire en sorte que la nouvelle configuration soit propagée aux autres commutateurs du réseau, nous allons configurer le mode VTP Serveur sur les commutateurs de distribution et le mode VTP Client sur les commutateurs d'accès. Ainsi, un seul commutateur sera responsable de la propagation de la configuration mise à jour à l'ensemble du réseau.Comme illustré dans les figures 4.21, 4.22, 4.23.

```
Swd1(config)#vtp mode server
Device mode already VTP Server for VLANS.
Swd1(config)#vtp dom
Swd1(config)#vtp domain ge.vtp
Changing VTP domain name from NULL to ge.vtp
Swd1(config)#vtp pass
Swd1(config)#vtp password gevtp23
Setting device VTP password to gevtp23
Swd1(config)#vtp ve
Swd1(config)#vtp version 2
Swd1(config)#vtp pru
Swd1(config)#vtp pruning
Pruning switched on
```

FIGURE 4.21 – configuration le mode VTP Serveur .

```
Sw3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Sw3(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
Sw3(config)#vtp password gevtp23
Setting device VTP password to gevtp23
Sw3(config)#vtp domain ge.vtp
Changing VTP domain name from NULL to ge.vtp
Sw3(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
Sw3(config)#do wr
```

FIGURE 4.22 – configuration le mode VTP Client .

```
Swd1#show  vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : ge.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0400
Configuration last modified by 0.0.0.0 at 5-6-23 12:26:57
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 2
MD5 digest                      : 0x39 0xA7 0xF6 0x7A 0x16 0xA4 0x42 0x95
                                  0x76 0x18 0xB1 0x44 0x64 0x8C 0xD1 0xA2
```

```
Sw3#show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 2
VTP Domain Name                 : ge.vtp
VTP Pruning Mode                : Enabled
VTP Traps Generation            : Disabled
Device ID                       : aabb.cc80.0600
Configuration last modified by 0.0.0.0 at 5-6-23 12:26:57

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 5
Configuration Revision          : 2
MD5 digest                      : 0x39 0xA7 0xF6 0x7A 0x
                                  0x76 0x18 0xB1 0x44 0x
```

FIGURE 4.23 – Test VTP .

4.8.4 Création des VLANs

Nous allons à présents créer les VLANs à savoir :

```
Swd1(config)#vlan 240
Swd1(config-vlan)#name S-INFO
Swd1(config-vlan)#end
```

FIGURE 4.24 – Création du VLAN S-INFO .

```
Swd1(config)#vlan 241
Swd1(config-vlan)#name S-CF
Swd1(config-vlan)#vlan 242
Swd1(config-vlan)#name S-PS
Swd1(config-vlan)#vlan 243
Swd1(config-vlan)#name S-GRH
Swd1(config-vlan)#vlan 344
Swd1(config-vlan)#NO vlan 344
Swd1(config)#vlan 244
Swd1(config-vlan)#name Voice
Swd1(config-vlan)#vlan 245
Swd1(config-vlan)#name MANAGER
Swd1(config-vlan)#vlan 966
Swd1(config-vlan)#name Native
Swd1(config-vlan)#end
```

FIGURE 4.25 – Création du VLANs .

```
Swd1(config)#vlan 246
Swd1(config-vlan)#name SERVERUS
Swd1(config-vlan)#end
```

FIGURE 4.26 – Création du VLAN Serveur .

4.8.5 Affectations des ports mode Access

```
Sw3(config)#interface range ethernet 3/0-1
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport mo
Sw3(config-if-range)#switchport mo acc
Sw3(config-if-range)#switchport mod
Sw3(config-if-range)#switchport mode acc
Sw3(config-if-range)#switchport mode access
Sw3(config-if-range)#
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport acc
Sw3(config-if-range)#switchport access vl
Sw3(config-if-range)#switchport access vlan  240
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport voi
Sw3(config-if-range)#switchport voice vl
Sw3(config-if-range)#switchport voice vlan 244
Sw3(config-if-range)#
Sw3(config-if-range)#end
```

```
Sw3(config)#interface  range ethernet 2/2-3
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport mo
Sw3(config-if-range)#switchport mo
Sw3(config-if-range)#switchport mode acc
Sw3(config-if-range)#switchport mode access
Sw3(config-if-range)#
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport acc
Sw3(config-if-range)#switchport access vl
Sw3(config-if-range)#switchport access vlan 241
Sw3(config-if-range)#sw
Sw3(config-if-range)#switchport voi
Sw3(config-if-range)#switchport voice vl
Sw3(config-if-range)#switchport voice vlan  244
Sw3(config-if-range)#end
```

```
Sw4(config)#interface  range ethernet 3/0-1
Sw4(config-if-range)#sw
Sw4(config-if-range)#switchport mo
Sw4(config-if-range)#switchport mode  acc
Sw4(config-if-range)#switchport mode  access
Sw4(config-if-range)#
Sw4(config-if-range)#sw
Sw4(config-if-range)#switchport acc
Sw4(config-if-range)#switchport access vl
Sw4(config-if-range)#switchport access vlan 242
Sw4(config-if-range)#sw
Sw4(config-if-range)#switchport vl
Sw4(config-if-range)#switchport v
Sw4(config-if-range)#switchport voice vl
Sw4(config-if-range)#switchport voice vlan 244
Sw4(config-if-range)#end
```

```
Sw4(config)#interface  range ethernet 2/2-3
Sw4(config-if-range)#sw
Sw4(config-if-range)#switchport mo
Sw4(config-if-range)#switchport mode  acc
Sw4(config-if-range)#switchport mode  access
Sw4(config-if-range)#
Sw4(config-if-range)#sw
Sw4(config-if-range)#switchport acc
Sw4(config-if-range)#switchport access vm
Sw4(config-if-range)#switchport access vl
Sw4(config-if-range)#switchport access vlan 243
Sw4(config-if-range)#sw
Sw4(config-if-range)#switchport vo
Sw4(config-if-range)#switchport voice vl
Sw4(config-if-range)#switchport voice vlan 244
Sw4(config-if-range)#
Sw4(config-if-range)#end
```

FIGURE 4.27 – Affectations des ports mode Access .

```
Sw4#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et0/0, Et0/1, Et0/2, Et0/3
                                                 Et1/0, Et1/1, Et1/2, Et1/3
                                                 Et2/0, Et2/1
240  S-INFO                            active
241  S-CF                              active
242  S-PS                              active    Et3/0, Et3/1
243  S-GRH                             active    Et2/2, Et2/3
244  Voice                             active    Et2/2, Et2/3, Et3/0, Et3/1
245  MANAGER                           active
246  SERVEURS                          active
966  Native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

FIGURE 4.28 – Vérification des VLANs .

4.8.6 Configuration des ports EtherChannel(Agrégation des liens)

Nous avons effectuer une Agrégation des liens sur les switch distributeurs avec la configuration illustré dans les figures 4.29

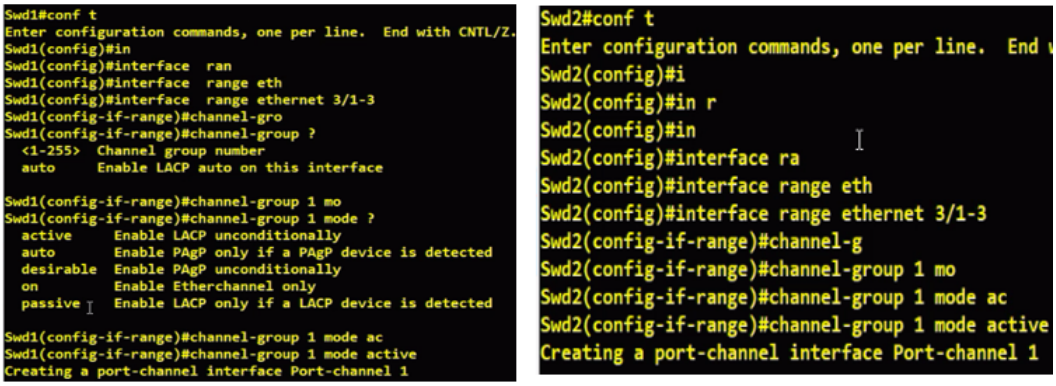

FIGURE 4.29 – Agrégation des liens sur Swd1 et Swd2 .

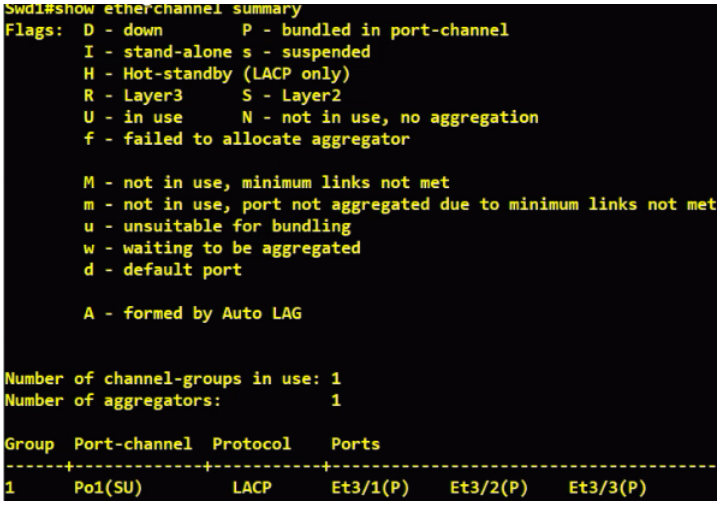

FIGURE 4.30 – Vérification des ports EtherChannel .

4.8.7 Configuration de Load Balancing

L'objectif du load balancing est d'améliorer les performances, d'assurer une meilleure réactivité du système et de prévenir les points de congestion ou les goulots d'étranglement. Pour répartissant équitablement la charge de travail,nous avons configuré le système de la manière suivante(voir la figure 4.31) :

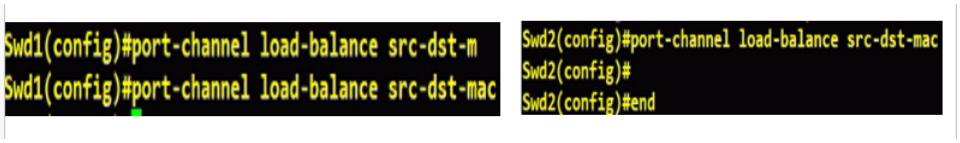

FIGURE 4.31 – Load Balancing .

4.9 Configuration des routeurs

4.9.1 Routage Inter-VLAN

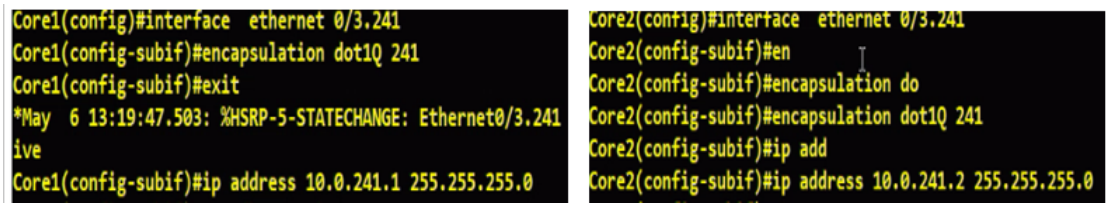

FIGURE 4.32 – Routage Inter-VLAN .

4.9.2 Configuration de la route statique

Pour configurer la route des routeurs Core 1 et Core 2 nous utilisons la configuration de la figure 4.33.

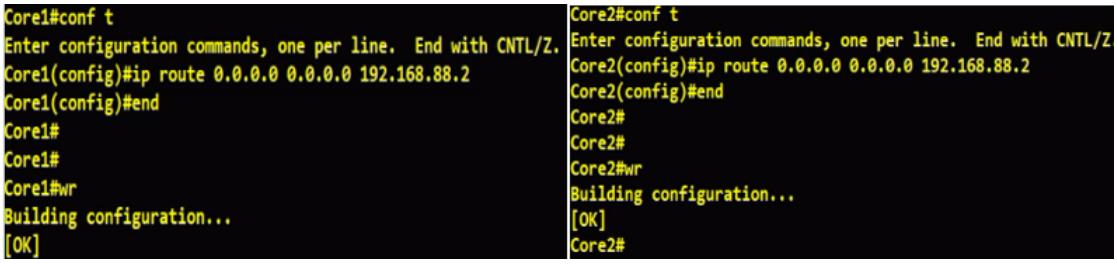

FIGURE 4.33 – Routage statique .

4.9.3 Configuration du protocole HSRP

Nous allons finaliser la configuration de nos routeurs par la mise en place du protocole HSRP, où nous allons définir sur les deux routeurs une adresse IP qui sera celle du routeur virtuel. Core1 sera en mode active tandis que Core2 sera en mode standby, c'est-à-dire que Core1 assurera le rôle de passerelle par défaut et basculera vers Core2 uniquement en cas de panne du routeur actif

```
Core1(config-subif)#standby 241 ip 10.0.241.254
Core1(config-subif)#standby 241 priority 150
Core1(config-subif)#st
Core1(config-subif)#standby ve
Core1(config-subif)#standby version 2
Core1(config-subif)#st
Core1(config-subif)#standby
*May  6 13:20:32.513: %HSRP-5-STATECHANGE: Ethernet0/3.241 Grp
Core1(config-subif)#standby 241 pre
Core1(config-subif)#standby 241 preempt
```

```
Core2(config-subif)#standby 241 ip 10.0.241.254
Core2(config-subif)#st
Core2(config-subif)#st
Core2(config-subif)#standby ve
Core2(config-subif)#standby version 2
```

FIGURE 4.34 – Configuration du protocole HSRP .

Nous avons réalisé un test de redondance au premier saut en éteignant le routeur principal. Après avoir effectué ce test, nous avons éteint le routeur CORE1. En conséquence, le routeur CORE2 a basculé du mode standby au mode actif, démontrant ainsi que la redondance au premier saut a été correctement configurée la figure 4.35 présente les résultats de ce test.

```
core2#show  standby  brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/3.240   240  100   Standby 10.0.240.1      local           10.0.240.254
Et0/3.241   241  100   Standby 10.0.241.1      local           10.0.241.254
Et0/3.242   242  100   Standby 10.0.242.1      local           10.0.242.254
Et0/3.243   243  100   Standby 10.0.243.1      local           10.0.243.254
Et0/3.244   244  100   Standby 10.0.244.1      local           10.0.244.254
Et0/3.245   245  100   Standby 10.0.245.1      local           10.0.245.254
Et0/3.246   246  100   Standby 10.0.246.1      local           10.0.246.254
Core1#show  standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State   Active          Standby         Virtual IP
Et0/3.240   240  150 P Active  local           10.0.240.2      10.0.240.254
Et0/3.241   241  150 P Active  local           10.0.241.2      10.0.241.254
Et0/3.242   242  150 P Active  local           10.0.242.2      10.0.242.254
Et0/3.243   243  150 P Active  local           10.0.243.2      10.0.243.254
Et0/3.244   244  150 P Active  local           10.0.244.2      10.0.244.254
Et0/3.245   245  150 P Active  local           10.0.245.2      10.0.245.254
Et0/3.246   246  150 P Active  local           10.0.246.2      10.0.246.254
```

FIGURE 4.35 – Test du Redondance 1 .

Lors du test de redondance au premier saut, après avoir éteint le routeur, nous avons observé que le routeur est passé de l'état standby à l'état actif, et l'envoi de trames s'est poursuivi de manière fluide comme illustré dans la figure 4.36.

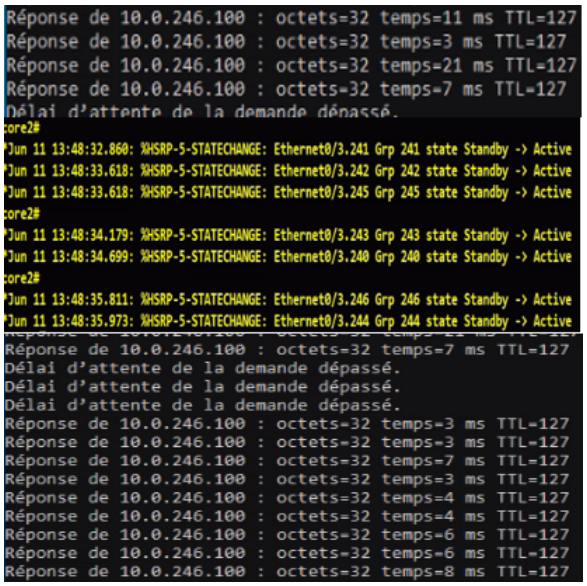

FIGURE 4.36 – Test du Redondance 2 .

4.9.4 Test du routage inter VLAN

Maintenant pour vérifier la connectivité entre des équipements se trouvant dans des VLANs différents, nous avons effectué un test de ping entre la machine virtuelle et les autres VLANs

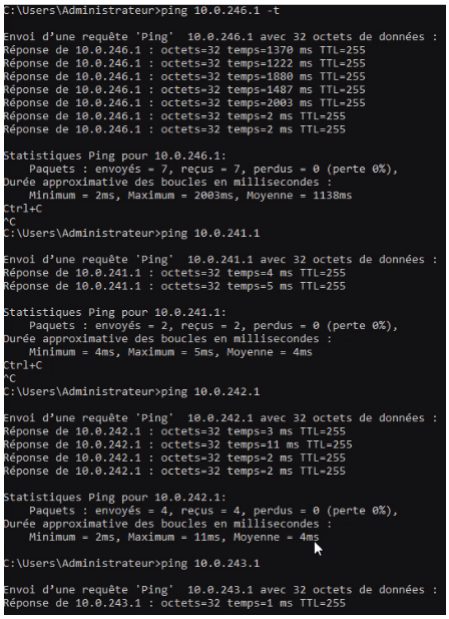

FIGURE 4.37 – Test routage inter VLAN .

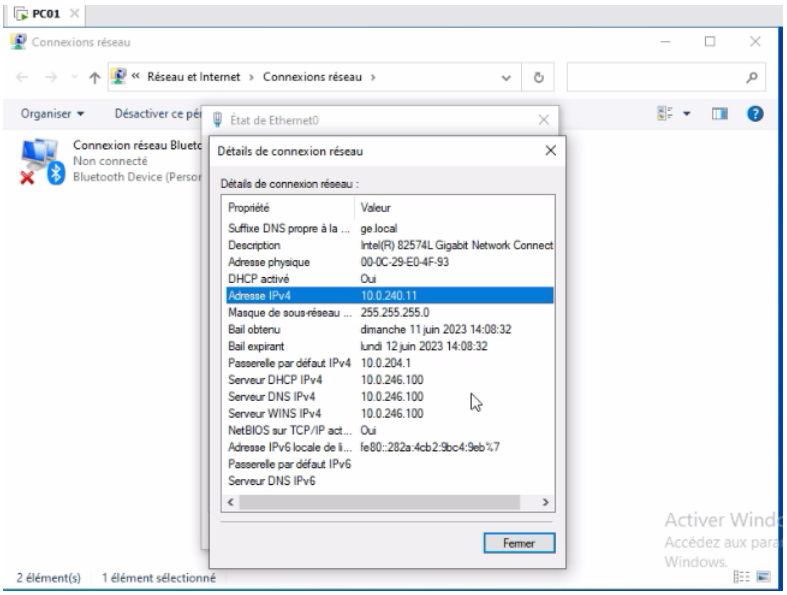

FIGURE 4.38 – Test DHCP .

4.10 Configuration des Private-VLAN

Nous allons procéder à la configuration de la DMZ en créant plusieurs VLANs. Pour commencer, nous configurerons le switch DMZ en mode transparent pour qu'il ne participe pas au processus VTP.comme nous montre la figure 4.39

```
Sw-dmz(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
```

FIGURE 4.39 – Configuration de switch sw-dmz1 .

Aprés nous allons procéder à la création des VLANs, en commençant par le VLAN privé de type "Community", où les équipements pourront communiquer entre eux. Ensuite, nous créerons le VLAN privé de type "Isolated", où les équipements de ce VLAN ne pourront pas communiquer entre eux. Enfin, nous créerons le VLAN privé de type "Primary" qui regroupera les deux VLANs précédents et permettra la communication avec eux. Consulter la figure 4.40 associée.

```
Sw-dmz(config)#vlan 201
Sw-dmz(config-vlan)#pri
Sw-dmz(config-vlan)#private-vlan co
Sw-dmz(config-vlan)#private-vlan community
Sw-dmz(config-vlan)#exit
```

```
Sw-dmz(config)#vlan 202
Sw-dmz(config-vlan)#pri
Sw-dmz(config-vlan)#private-vlan is
Sw-dmz(config-vlan)#private-vlan isolated
Sw-dmz(config-vlan)#exit
```

```
Sw-dmz(config)#vlan 200
Sw-dmz(config-vlan)#pri
Sw-dmz(config-vlan)#private-vlan pri
Sw-dmz(config-vlan)#private-vlan primary
Sw-dmz(config-vlan)#pri
Sw-dmz(config-vlan)#private-vlan as
Sw-dmz(config-vlan)#private-vlan association 201,202
Sw-dmz(config-vlan)#exit
```

FIGURE 4.40 – Création des VLAN privés .

Après cela nous allons associer chaque port au VLAN approprié,comme illustré dans la figure 4.41

```
Sw-dmz(config)#interface ethernet 0/0
Sw-dmz(config-if)#sw
Sw-dmz(config-if)#switchport mo
Sw-dmz(config-if)#switchport mode  pri
Sw-dmz(config-if)#switchport mode  private-vlan p
Sw-dmz(config-if)#switchport mode  private-vlan promiscuous
Sw-dmz(config-if)#sw
Sw-dmz(config-if)#switchport
*May 11 14:49:02.348: %LINEPROTO-5-UPDOWN: Line protocol on In
ged state to down
Sw-dmz(config-if)#switchport pri
Sw-dmz(config-if)#switchport private-vlan m
Sw-dmz(config-if)#switchport private-vlan mapping 200 201,202
Sw-dmz(config-if)#exit
```

```
Sw-dmz(config)#interface  range ethernet 0/1-2
Sw-dmz(config-if-range)#sw
Sw-dmz(config-if-range)#switchport mo
Sw-dmz(config-if-range)#switchport mode pri
Sw-dmz(config-if-range)#switchport mode private-vlan h
Sw-dmz(config-if-range)#switchport mode private-vlan host
Sw-dmz(config-if-range)#sw
Sw-dmz(config-if-range)#switchport
*May 11 14:49:52.664: %LINEPROTO-5-UPDOWN: Line protocol on Interface Eth
ged state to down
*May 11 14:49:52.664: %LINEPROTO-5-UPDOWN: Line protocol on Interface Eth
ged state to down
Sw-dmz(config-if-range)#switchport pri
Sw-dmz(config-if-range)#switchport private-vlan h
Sw-dmz(config-if-range)#switchport private-vlan host-association 200 201
Sw-dmz(config-if-range)#exit
```

```
Sw-dmz(config)#interface  ethernet 0/3
Sw-dmz(config-if)#sw
Sw-dmz(config-if)#switchport mo
Sw-dmz(config-if)#switchport mode  pri
Sw-dmz(config-if)#switchport mode  private-vlan h
Sw-dmz(config-if)#switchport mode  private-vlan host
Sw-dmz(config-if)#sw
Sw-dmz(config-if)#switchport
*May 11 14:50:19.203: %LINEPROTO-5-UPDOWN: Line protocol on Interface
ged state to down
Sw-dmz(config-if)#switchport pri
Sw-dmz(config-if)#switchport private-vlan ho
Sw-dmz(config-if)#switchport private-vlan host-association 200 202
Sw-dmz(config-if)#end
Sw-dmz#
Sw-dmz#wr
```

FIGURE 4.41 – Association des ports aux VLAN Privés .

4.11 Configuration du Fire-Wall Fortigate

Pour configurer les Fortigate à Akbou et Sétif, nous allons suivre les mêmes étapes, qui sont les suivantes : la configuration du mot de passe, le nom et l'adresse. Comme illustré dans les figures 4.42 et 4.43

```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
New passwords don't match.
New Password:
Confirm Password:
Welcome!

FortiGate-VM64-KVM #
```

```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname FG-GE-AKBOU

FortiGate-VM64-KVM (global) # end
```

```
FG-GE-AKBOU # config system  interface

FG-GE-AKBOU (interface) # edit port10

FG-GE-AKBOU (port10) # set mode st

FG-GE-AKBOU (port10) # set ip 192.168.89.11/24

FG-GE-AKBOU (port10) # set allowaccess ping https http  ssh

FG-GE-AKBOU (port10) # end
```

FIGURE 4.42 – Configuration Fortigate Akbou .

```
FortiGate-VM64-KVM # config system global

FortiGate-VM64-KVM (global) # set hostname FG-Setif

FortiGate-VM64-KVM (global) # end
FG-Setif # config system interface

FG-Setif (interface) # edit port10

FG-Setif (port10) # set mode static
FG-Setif (port10) # set ip 192.168.89.10/24

FG-Setif (port10) # set allowaccess ping https http ssh

FG-Setif (port10) # end
```

FIGURE 4.43 – Configuration Fortigate Sétif .

Une fois la configuration de base effectuée c'est-à-dire le nom d'utilisateur, le mot de passe.

La page d'accueil sera comme suit(la figure 4.44 et 4.45) :

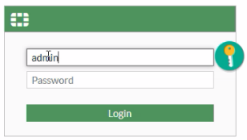

FIGURE 4.44 – Configuration Fortigate Sétif .

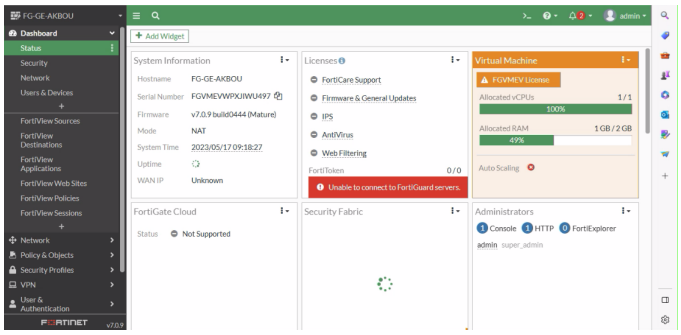

FIGURE 4.45 – La page d'accueil du Fire wall.

Après cela, nous allons procéder à la configuration des interfaces graphiques des firewall en suivant les étapes indiquées dans la figure 4.46 .

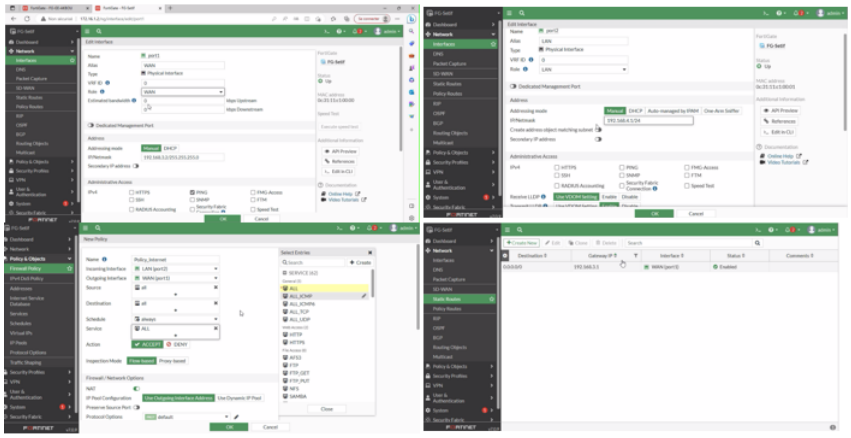

FIGURE 4.46 – Configuration du l'interface graphique .

Avons la configuration de Nat ,nous configurons tour d'abord les interfaces (0/0-1) sur les routeur Core1 et Core2(figure 4.47)

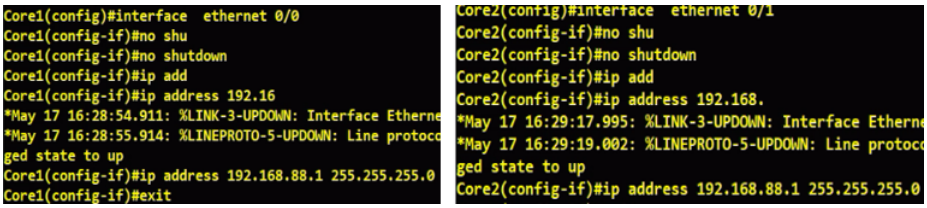

FIGURE 4.47 – Configuration des interfaces 0/0 et 0/1 .

Pour configurer le Nat , nous avons utilisé la configuration suivante

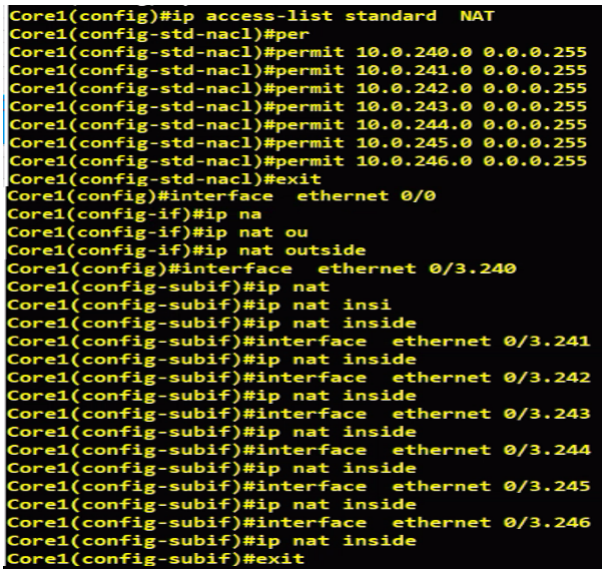

FIGURE 4.48 – Configuration du Nat .

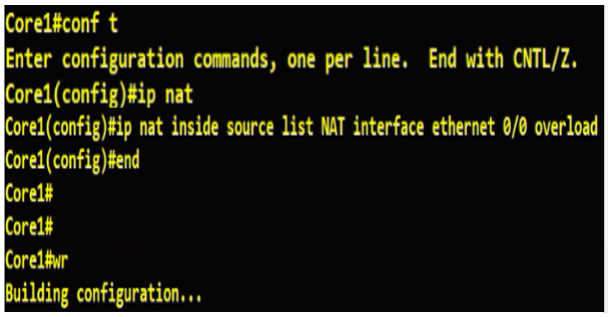

FIGURE 4.49 – Configuration du Nat suite .

4.12 Tunnel IPsec

4.12.1 Création du tunnel IPsec

Nous testons le ping avant la création du tunnel

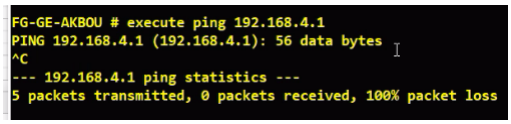

FIGURE 4.50 – Test avant la création du tunnel .

Afin de crée un tunnel IPsec en allant sur notre pare-feu et en cliquant sur VPN> IPsec Tunnels>Creat New> IPsec Tunnelle puis en suivant les étapes indiquées, tel qu'il est illustré dans les Figures 4.51 et 4.52 :

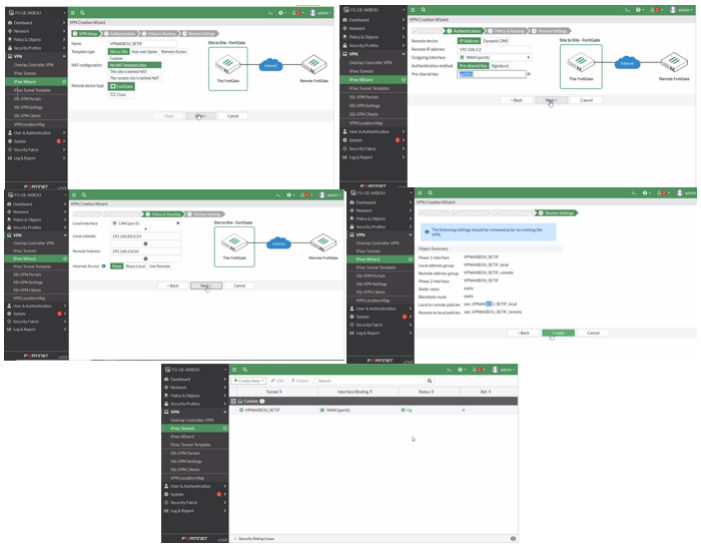

FIGURE 4.51 – Création du tunnel IPsec .

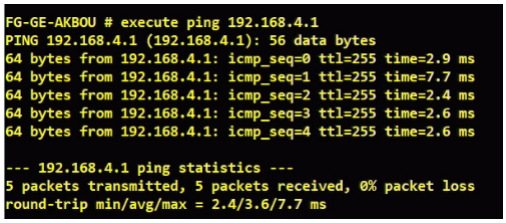

FIGURE 4.52 – Test après la création du tunnel .

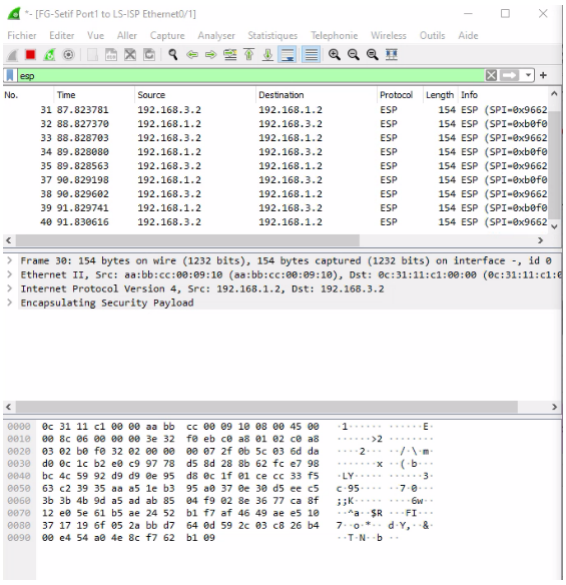

FIGURE 4.53 – Test après la création du tunnel 2 .

4.12.2 Configuration des routeur

Avant de configurer le tunnel nous allons tout d'abord configurer le routeur R- alger plus le Nat tel qu'il est illustré dans la Figure 4.54 et 4.55 :

```
R-Alger#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-Alger(config)#in
R-Alger(config)#interface  se
R-Alger(config)#interface  serial 2/0
R-Alger(config-if)#no shu
R-Alger(config-if)#no shutdown
R-Alger(config-if)#ip add
R-Alger(config-if)#ip address 19
*May 17 17:09:10.774: %LINK-3-UPDOWN: Interface Serial2/0, char
*May 17 17:09:11.774: %LINEPROTO-5-UPDOWN: Line protocol on Int
d state to up
R-Alger(config-if)#ip address 192.168.2.2 255.255.255.0
R-Alger(config-if)#exit
R-Alger(config)#
*May 17 17:09:37.956: %LINEPROTO-5-UPDOWN: Line protocol on Int
d state to down
R-Alger(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1
R-Alger(config)#exit
```

FIGURE 4.54 – Configuration du R-alger.

FIGURE 4.55 – Configuration du Nat .

Après nous allons configurer le prochaine saut LS-ISP(La Figure 4.56)

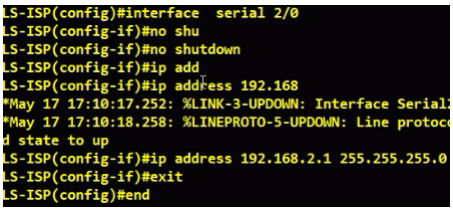

FIGURE 4.56 – Configuration du LS-ISP .

4.12.3 Configuration du Tunnel GRE

Pour configurer le tunnel GRE nous avons appliqué les commandes présentées dans la figure 4.57 et le teste est présenter dans la figure 4.58

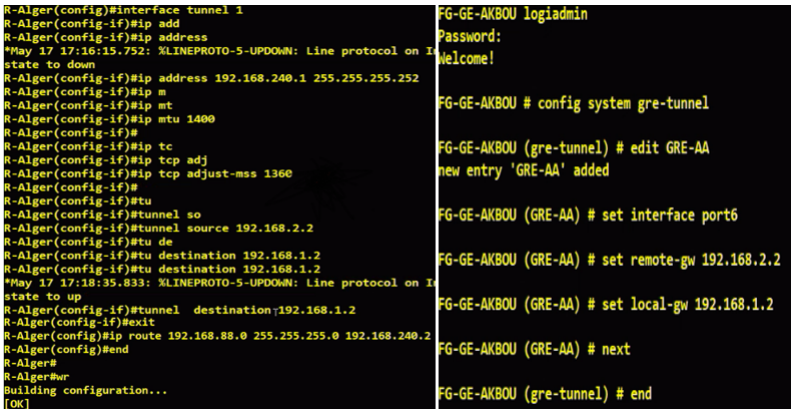

FIGURE 4.57 – Configuration du Tunnel GRE .

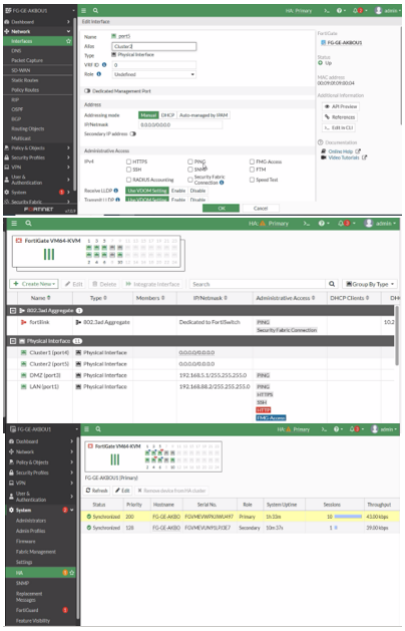

FIGURE 4.58 – Configuration Closturing .

4.13 Conclusion

En conclusion, notre projet de configuration et de sécurisation d'un réseau d'entreprise à base de liaisons virtuelles a été une expérience enrichissante. Nous avons acquis une compréhension approfondie des réseaux informatiques et de la sécurité, ainsi que des compétences pratiques pour mettre en place des solutions de sécurité avancées. Dans ce chapitre, nous avons appris comment configurer ces différents aspects, en mettant l'accent sur les pa-

ramètres, les protocoles et les bonnes pratiques pour assurer des performances optimales et une gestion efficace des réseaux.

Conclusion générale

En appliquant les meilleures pratiques de configuration et de sécurité pour le réseau local de l'entreprise Générale Emballage, nous avons réussi à mettre en place des VLANs, des VPNs, l'agrégation de liens, ainsi qu'une architecture redondante sur leur site principal. Cette approche a permis de créer un environnement réseau robuste, parfaitement adapté à leurs besoins opérationnels, tout en préservant la confidentialité, l'intégrité et la disponibilité des données.

Notre travail se divise en deux parties distinctes. La première partie est axée sur l'aspect théorique et se compose de trois chapitres. Le premier chapitre explore les concepts fondamentaux des réseaux informatiques, le deuxième se penche sur la sécurité des réseaux informatiques, tandis que le troisième chapitre approfondit les liaisons virtuelles.

La deuxième partie est consacrée à la configuration des liaisons virtuelles, telles que les VPNs, les VLANs, l'agrégation des liens et la redondance.

La réalisation de ce travail a été à la fois enrichissante et bénéfique d'un côté, mais également exigeante du point de vue de la conception. En effet, pour simuler notre réseau, il a fallu comprendre le fonctionnement des équipements utilisés, maîtriser leurs fonctionnalités, assimiler les concepts complexes liés aux VLANs, VPNs, agrégation des liens et redondance, et apprendre à les simuler avec le logiciel GNS3.

BIBLIOGRAPHIE

[1] *https ://homepages.laas.fr / NOTIONS DE RESEAUX INFORMATIQUES[Consulté 08/06/2023].*

[2] *Support de Cours Communication de Données et Réseaux pour Etudiants Master en Informatique élaboré par : A. Bilami - Département d'Informatique. Université de Batna 2[Consulté 08/06/2023].*

[3] *http ://sciences-ingenieur.genevoix-signoret-vinci.fr internet/co/01Les reseaux[Consulté 08/06/2023].*

[4] *W. R. Stevens, G. Pujolle, P. Rolin, « Réseaux et principes fondamentaux », Cours Master Informatique 2ème Année, Université d'Angers, France, A.U : 1999-2000*

[5] *J. DORDOIGNE,«Réseaux informatiques Notions fondamentales (Protocoles, Architectures, Réseaux sans fil, Sécurité, IP v6,. . .)». Editions ENI, Janvier 2013*

[6] *G. PUJOLLE. Initiation aux réseaux. Edition eyrolles, 2014.*

[7] *www.rezalfr.org cours réseaux et administration systéme les topologies - 2004.[Consulté 13/06/2023]*

[8] *http ://eventus-networks.blogspot.com/2013[Consulté 08/06/2023].*

[9] *cours master 1 et master 2 Introduction à la Sécurité Informatique, Département Informatique, Université de Bejaia.*

[10] *C. Severin, Réseaux Télécom, 2 ème édition. Paris : Edition DUNOD, 2006*

[11] *waytolearnx.com/2 [Consulté 08/06/2023]*

[12] *www.ionos.fr3[Consulté 08/06/2023]*

[13] *P. JAQUET, « Les Réseaux Informatiques », cours, 2015.*

[14] *Cours master 2 ,« Les*$_s$*ystèmes*$_d$*e*$_s$*écurité* $-$ *CH*5», 2023

[15] *Introduction à la sécurité informatique ,Laurent Poinsot UMR 7030 - Université Paris 13 - ,Institut Galilée Cours " Sécrypt "*

[16] *J. François CAREPENTIER, «La sécurité informatique dans la petite entreprise»,2ème édition*

[17] *https ://www.deessi.si/[Consulté 08/06/2023]*

[18] *F. Goffinet. (2021). [En ligne]. https : //cisco.goffinet.org [Consulté 18/06/2023]*

[19] *J. François PILLOU ,jean-philipeBAY , «tout sur la sécurité informatique»,3 éme édition*

[20] *cisco.ofppt.info/ccna2/course/module3[Consulté 10/05/2023]*

[21] *V. Remazeilles,« La sécurité des réseaux avec Cisco ». Editions ENI, 2009*

[22] *Le grand livre de sécurité info, "http ://www.securiteinfo.com", février 2004*

[23] *https ://www.generalemballage.com/[Consulté 08/04/2023]*

[24] *https ://www.gns3.com [Consulté 10/06/2023]*

Résumé

De nos jours, la sécurité informatique est essentielle pour assurer le bon fonctionnement des réseaux informatiques. Les ingénieurs réseau doivent donc mettre en place des mécanismes et des protocoles de gestion et de sécurité plus solides et efficaces pour protéger leurs réseaux. Dans le cadre de notre travail pour Générale Emballage, notre objectif était d'améliorer l'architecture du réseau afin de gérer et sécuriser efficacement le transfert de données entre les services locaux et les sites distants.
Afin de améliorer l'architecture réseau de l'entreprise Générale Emballage, nous avons mis en place des VLANs, un VPN sécurisé,entre les deux sites locaux d'Akbou et Sétif, l'agrégation des liens et la redondance avec GNS3. Ces mesures ont renforcé la sécurité, optimisé les transferts de données et amélioré la gestion des ressources réseau. Grâce à ces améliorations, nous avons augmenté la performance et la fiabilité des services réseau de l'entreprise.

Mots-clés : VLAN, VPN, l'agrégation des liens et la redondance, GNS3

abstract

In today's modern times, computer security is essential for the proper functioning of any computer network due to its utmost importance. This is why enterprise network engineers must devise more robust and effective management and security mechanisms and protocols to protect their networks. The objective of our work was to implement an improvement in the network architecture of Générale Emballage in order to effectively manage and secure the transfer of data between local network services and remote sites.
To achieve this goal, we established VLANs, a secure VPN between the two local networks of Akbou and Sétif, and implemented link aggregation and redundancy using GNS3. These measures enhanced security, optimized data transfers, and improved network resource management. As a result, we increased the performance and reliability of the company's network services.

Keywords : VLAN, VPN, link aggregation and redundancy, GNS3