République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Abderrahmane Mira

Faculté de la Technologie

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : télécommunications.

Spécialité : Réseaux et Télécommunications.

Thème

Conception et implémentation d'une architecture réseau

« Cas Cevital »

Préparé par :

Melle AGHBARI Imene

Melle BIZRICHE Kamilia

Dirigé par :

Mr. MOKETFI Mohand

Mr. M.Arab.Younes

Examiné par :

Mr. KASMI.R

Mr. AZNI .S

Année universitaire : 2022/2023

Dédicace :

Au nom d'Allah et la paix au NABIYA Allah je dédie ce modeste travail à :

Mes très chers parents Zahir et Fatiha

Qui ont œuvré pour ma réussite, par leur amour, leur soutien, leur encouragement, tous leurs sacrifices consentis.

Recevez à travers ce modeste travail l'expression de mon éternelle gratitude ;

Au formidable frère que j'ai Anis

Qui n'a cessé d'être pour moi un exemple de persévérance, de courage et de générosité ;

À ma très chère sœur kenza

Qui m'a encouragée à chaque fois, qui m'a soutenue et qui était toujours à mes côtés.

A toute ma famille

Mes tantes et leurs maris, à mes cousins et cousines

Ainsi, à mes grands-parents,

Que dieu les accueille dans son vaste paradis ;

A tous mes ami(e)s,

De groupe de réseaux Télécommunications, et tous ceux du système et télécommunication;

Et enfin une spéciale dédicace à tous les professeurs de l'ATE.

AGHBARI Imene

Dédicace :

Dieu le tout puissant

De m'avoir prêté longue vie Pour arriver au terme de ce projet.

Mes très chers parents Noureddine et Fatiha

Qui ont veillez sur moi avec leur suivis, supports, et encouragements pour que je retrouve là où je suis aujourd'hui.

Mon petit cher frère Aymen

Qui a était un frère à mes côtés.

Mes chères sœurs Amel et Imen

Qui m'ont encouragé et soutenue durant toute ma vie.

Ma chère grand-mère Fatma et Mes grands Parents

Que dieu vous protège et à ma grand-mère que dieu t'accueilles dans son vaste paradis

Toute ma famille et mes proches

Mes cousins, cousines mes tantes et à toute la famille BIZIRCHE et MANSOURI

Ma chère amie Malika

Et enfin une spéciale dédicace à tous les professeurs de l'ATE.

BIZRICHE Kamilia

Remerciements

Je remercie d'abord le Bon dieu de nous avoir donné le courage, la patience et la volonté fine pour accomplir notre parcours.

Nous tenons à remercier particulièrement nos promoteurs Mr : M.Arab.Younes et Mr Moketfi Mohand pour leurs qualité d'encadrement et pour leurs suivi, leurs orientation, leurs remarque de patiente et précieuses durant la réalisation de notre projet.

De nous avoir fait confiance et encouragées tout au long de ce projet.

Un grand merci à tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Enfin, nos remerciements s'adressent aux membres du jury qui vont nous faire l'honneur de juger notre travail.

Table des matières

Table des matières

Liste des figures

Liste des figures

Liste des tableaux

Liste des tableaux

Liste des abréviations

Liste des abréviations

A

ARP Address Resolution Protocol

C

CARP Common Address Redundancy Protocol

CEVITAL Conglomérat Algérien de L'industrie Agroalimentaire

Cisco City Group for Small Companies

CLI Command-Line Interface

D

DEL Diode Electro luminescente

DHCP Dynamic Host Configuration Protocol

DMZ DeMilitarized Zone

DNS Domaine Name Service

DSI Direction des Systèmes d'Information

E

EIGRP Enhanced Interior Gateway Protocol

ESRP Extreme Standby Router Protocol

E/S Entrée Sortie

Ethernet Ether milieu mythique net réseau

F

FHRP First Hop Redundancy Protocol

G

GLBP Gateway Load Balancing Protocol

H

HSRP Hot Standby Router Protocol

HUB Has Unit Broadcast

I

IANA Internet Assigned Numbers Authority

IBM International Business Machines

ICMP Internet Control Message Protocol

IEEE Institute of Electrical and Electronics Engineers

ISO International Standard Organization

IP Internet Protocol

IPsec Internet Protocol Security

IPSG Internet Protocol Source Guard

IPv4 Internet Protocol version 4

IPv6 Internet Protocol version 6

ISO International Standard Organization

L

LAN Local Area Network

LED Light Emitting Diode

M

MAN Metropolitan Area Network

MAC Man And Machine

MIME Multipurpose Internet Mail Extensions

ML Mètre Linéaire

MPLS Multiple Label Switching

N

NIC Network Interface Card

NSRP NetScreen Redundancy Protocol

O

OSI Open Systems Interconnection

OSPF Open Shortest Path First

P

PAN Personal Area Network

R

Rj45 Registered Jack-45

RIP Routing Information Protocol

RMS Royal Mail Ship

RN 9 Revenu National 9

R-SMLT Routed Split Mutli-link Trunking

S

S-HTTP Secure Hyper Text Transfer Protocol

STA Spanning-Tree Algorithm

STP Spanning-Tree Protocol Switch

SDN Software Defined Networking

T

TCP Transmission Control Protocol

TDMA Time Division Multiple Access

U

UDP User Datagram Protocol

V

VLAN Virtual LAN

VRRP Virtual Router Redundancy Protocol

VSAT Very Small Aperture Terminal

VTP VLAN Trunking Protocol

W

WAN Wide Area Network

Wi-Fi Wireless Fidelity

Introduction

Introduction

De nos jours, l'informatique joue un rôle important dans l'évolution de nos sociétés et du développement mondial. Elle est utilisée au sein des entreprises pour stocker des données parfois sensibles, de ce fait il est important d'en assurer la protection que ce soit lors du stockage ou dans leur mise à disponibilité.

Le réseau informatique est devenu une ressource vitale et déterminante pour le bon fonctionnement de l'entreprise.

En effet, chaque société dispose d'un réseau informatique particulier et propre à elle, avec ses propres caractéristiques et fonctionnalités, dans lequel chaque réseau illustre une architecture réseau unique et particulière.

Le groupe CEVITAL (Conglomérat Algérien de L'industrie Agroalimentaire) répondu par la variété de ses activités, la diversité de ses départements et par conséquent par la complexité de ses réseaux locaux, ce qui rend l'activité de son réseau informatique très particulière mais surtout qui nécessite une bonne disponibilité.

De ce fait, assurer et garantir un bon fonctionnement de ce réseau en toute circonstance même dans le cas d'un dysfonctionnement ou d'une panne devient primordial. Une interrogation mérite d'être posée afin de solutionner ce problème, par quel biais doit-on assurer le bon fonctionnement ainsi de maintenir l'efficacité du réseau au sein du groupe, quelle structure topologique, et comment faire face au dysfonctionnement des équipements matériels et logiciels ?

Pour cet effet, et durant notre stage au sein du groupe, nous allons mener une étude dans le but de proposer une nouvelle architecture, plus sécurisée, plus fiable en cas de dysfonctionnement du réseau de l'entreprise.

Nous visons par ce modeste travail à analyser l'architecture actuelle du réseau du groupe CEVITAL, tirer les divers problèmes liés aux collisions et congestions dans le trafic de l'information, puis proposer une nouvelle architecture plus sécurisée en cas de pannes ou d'interruption.

Ce mémoire est divisé en trois chapitres :

Chapitre 01 : "Principes fondamentaux des réseaux informatiques" - Ce chapitre présente une introduction générale aux réseaux informatiques, en abordant les différents types de réseaux, leurs modèles et les protocoles associés.

Chapitre 02 : "Présentation de l'organisme d'accueil" - Ce chapitre fournit une vue d'ensemble du groupe CEVITAL, en détaillant ses départements, ses équipements et ses ressources informatiques utilisées. Il expose également la problématique soulevée et propose une solution appropriée en réponse à celle-ci.

Chapitre 03 : "Conception et réalisation" - Ce chapitre se concentre sur la partie pratique du travail, en utilisant le simulateur "Cisco Packet Tracer". Il commence par présenter le réseau existant, sa configuration et sa segmentation en VLAN (Virtual Local Area Network) en fonction des différents départements administratifs. Ensuite, une nouvelle architecture est proposée pour éviter les pannes et améliorer le fonctionnement du réseau.

En conclusion, le mémoire se clôture par un résumé des connaissances acquises lors de la réalisation du projet de fin d'études, ainsi que quelques perspectives pour l'avenir.

Chapitre 1

Chapitre 1 : Principes fondamentaux des réseaux informatiques

1.1. Introduction

Un réseau est un moyen de communication qui permet à des individus ou à des groupes, d'échanger des informations et des services. Les technologies de mise en réseau informatique sont un ensemble d'outils, qui permettent aux ordinateurs de partager des informations et des ressources. Et aussi, ils permettaient à l'origine de connecter de simples terminaux à un grand ordinateur central, mais connectent aujourd'hui toutes sortes d'ordinateurs, y compris de gros serveurs, des postes de travail, des ordinateurs personnels ou même de simples terminaux graphiques.

Dans ce premier chapitre, nous passons en revue quelques concepts de base qui nous semblent nécessaires pour un rappel rapide afin de mieux comprendre l'avancée du sujet présenté.

1.2. Le réseau informatique

Un réseau informatique est un ensemble de dispositifs matériels et logiciels interconnectés dans le but de partager des données.

1.3. Objectif d'un réseau informatique

- **Partage des ressources**

Un réseau permet d'accéder à un ensemble de ressources (logiciels, bases de données, imprimantes, etc.) quelle que soit la localisation géographique de l'utilisateur. Un exemple de ceci est le partage de données commerciales d'entreprise. Tous les employés d'une entreprise multinationale ont accès au dernier compte de résultat de l'entreprise.

- **Augmentation de la fiabilité et des performances**

Les réseaux permettent par exemple de dupliquer en plusieurs endroits les fichiers vitaux d'un projet, d'une entreprise ; en cas de problème, la copie de sauvegarde est immédiatement disponible.

- **Réduction des coûts**

Les ordinateurs individuels PC (Personal Computer) ont un meilleur rapport prix/performances que les gros systèmes centralisés. Aujourd'hui, nous trouvons surtout des architectures client/serveur plus économiques, plus souple et permettant un déploiement incrémental aisé.

1.4. Classification des réseaux informatiques

Il existe différents types de réseaux, selon leur taille, leur l'architecteur ainsi que leur topologie.

1.4.1 Classification selon leur taille

On peut classifier les réseaux informatiques selon leurs tailles, comme l'indique la figure (1.1)

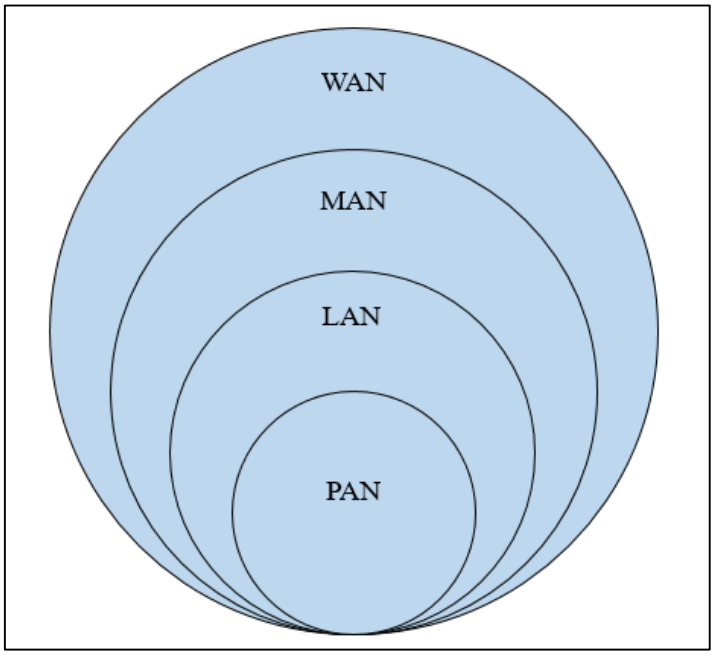

Figure 1. 1 : Topologies des réseaux.

- **Le réseau personnel :** PAN (Personnal Area Network), Il interconnecte des équipements personnels comme un ordinateur portable avec une imprimante ou scanner, etc. la figure (1.2)

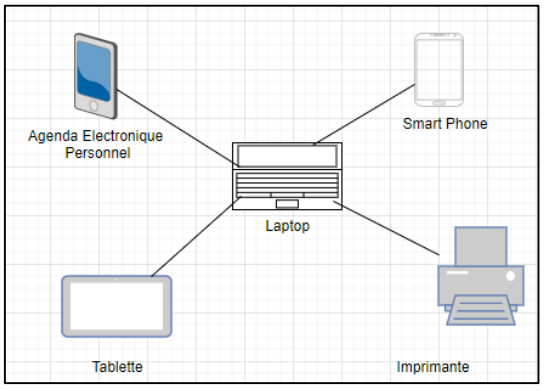

Figure 1. 2 : Le réseau personnel (PAN).

- **Les réseaux locaux :** LAN (Local Area Network), c'est des réseaux informatiques locaux couvrant une petite zone géographique où sont installés des ordinateurs, des serveurs et des périphériques. Très souvent, les connexions entre les serveurs sont

établies à l'aide de câbles Ethernet et les terminaux communiquent entre eux via une connexion sans fil, c'est-à-dire Wifi (Wireless Fidelity). La figure (1.3)

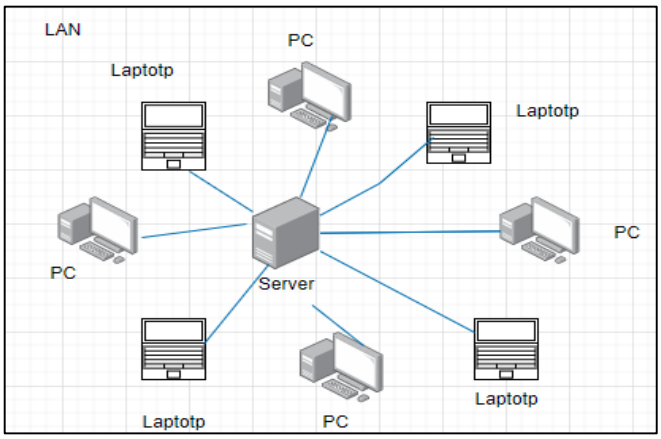

Figure 1. 3 : Réseau local (LAN).

- **Les réseaux métropolitains :** MAN (Metropolitan Area Network), Sont des réseaux qui couvrent une métropole (ville), interconnectant plusieurs LAN géographiquement. La figure (1.4)

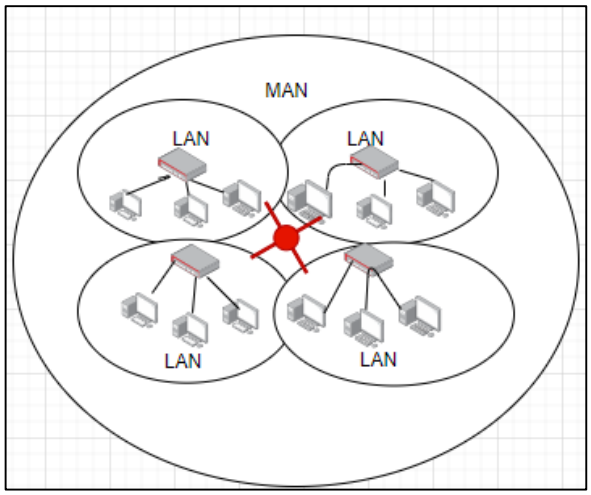

Figure 1. 4 : Réseau local(MAN).

- **Les réseaux étendus :** WAN (Wide Area Network), sont destinés à transporter des données numériques sur des distances à l'échelle d'un pays, voire d'un continent ou de plusieurs continents. Le réseau est soit terrestre, il utilise en ce cas des infrastructures au niveau du sol, essentiellement les grands réseaux de fibre optique, soit hertzien, comme les réseaux satellite, mais seulement pour des applications particulières à débit faible [1]. La figure (1.5)

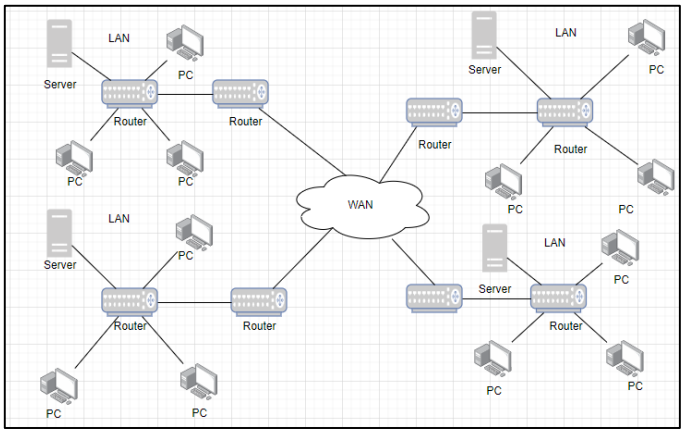

Figure 1. 5 : Les réseaux étendus (WAN).

1.4.2 Classification selon leur l'architecteur

- **Architecture poste à poste**

L'architecture poste à poste appelée aussi égale à égale (en anglais peer to peer), permet de mettre en place un réseau à moindre cout, son principe s'agit de relier les postes entre eux en utilisant une topologie physique, sachant que chaque utilisateur du réseau est libre de partager ces ressources et les données ne sont pas centralisées [2] voir la figure (1.6)

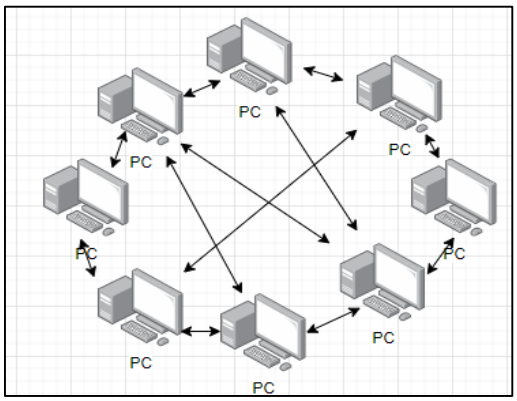

Figure 1. 6 : Architecture poste à poste.

L'architecture poste à poste a tout de même quelque avantage parmi lesquels :

- Une simplicité à toute épreuve.
- Chaque utilisateur peut décider de partager l'une de ses ressources avec les autres postes.

Le réseau poste à poste a énormément d'inconvénient :

- Si un poste est éteint ou il se plante, ses ressources ne sont plus accessibles.
- Ce système n'est pas centralisé, ce qu'il le rend difficile à administrer.
- La sécurité est peu présentée.

- **Architecture client/serveur**

Une architecture client-serveur, représente l'environnement dans lequel des applications de machines clientes communiquent avec des applications de machines de type serveurs. (Figure 1.7)

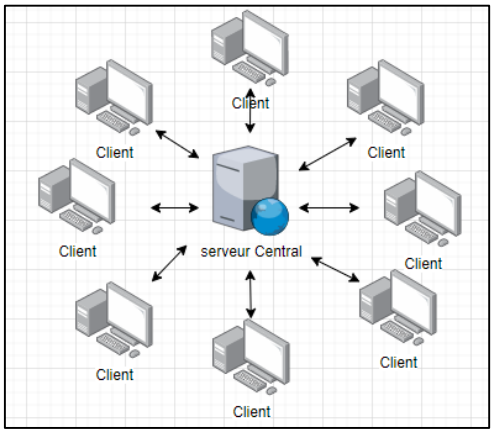

Figure 1. 7 : Architecture client/serveur.

L'architecture client-serveur a tout de même quelques inconvénients parmi lesquels [3] :

- Si trop de clients veulent communiquer sur le serveur en même temps, ce dernier risque de ne pas supporter la charge.
- Si le serveur n'est plus disponible, plus aucun des clients ne fonctionne (le réseau pair à pair continue à fonctionner, même si plusieurs participants quittent le réseau).
- Les coûts de mise en place et de maintenance sont élevés. En aucun cas les clients ne peuvent pas communiquer entre eux, entraînant une asymétrie de l'information au profit des serveurs.

1.4.3 Classification selon leur topologie

Il existe deux types de topologies : physique et logique.

- **Les topologies physiques**

Une topologie physique est en fait la structure physique de votre réseau. C'est donc la forme, l'apparence du réseau.

Il existe plusieurs topologies physiques : le bus, l'étoile (la plus utilisée), le mesh (topologie maillée), l'anneau, topologie en arbre (hiérarchique), etc. Cependant nous n'allons parler que des plus utilisées.

- **Topologie en bus**

Le bus, segment central où circulent les informations, s'étend sur toute la longueur du réseau et les machines vont s'y accrocher. Lorsqu'une station envoie des données, elle parcourt toute la longueur du bus et la station de destination peut obtenir ces données. Une seule station peut émettre à la fois. En bout de bus, une "prise" permet d'effacer définitivement l'information pour qu'une autre station puisse émettre. (Figure 1.8)

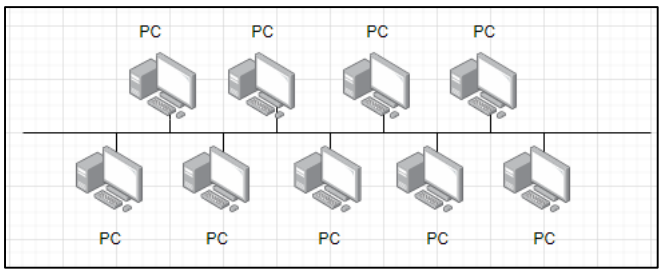

Figure 1. 8 : la topologie en bus.

- **Topologie en anneau**

La topologie en anneau est également l'une des topologies les plus anciennes, développée par IBM (International Business Machines), principalement utilisée par les réseaux Token Ring utilisant la technique d'accès par jeton. Les données circulent autour de l'anneau d'un nœud à un autre, la station avec le jeton qui envoie les données fait le tour de l'anneau, la station qui l'a envoyé le rejette et transmet le jeton à ses voisins, et ainsi de suite. (Figure 1.9)

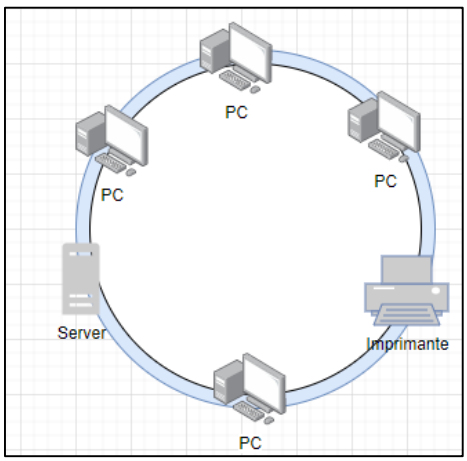

Figure 1. 9 : Topologie en anneau.

- **La topologie en étoile**

La topologie en étoile est la topologie la plus courante, notamment avec les réseaux locaux Ethernet. Les câbles sont raccordés à un point central switch ou hub (Has Unit Uroadcast). (Figure 1.10)

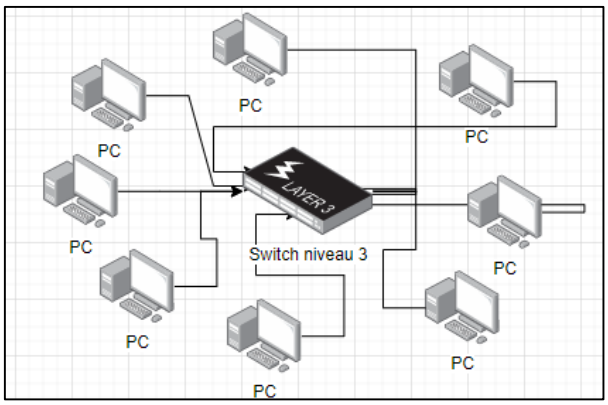

Figure 1. 10 : Topologie en étoile.

- **La topologie en arbre (hiérarchique)**

C'est une arborescence hiérarchique. Le réseau arborescent est formé par un ensemble de réseaux en étoile reliés entre eux par des centres à un nœud central unique. Cette structure est largement utilisée dans les réseaux locaux. (Figure 1.11)

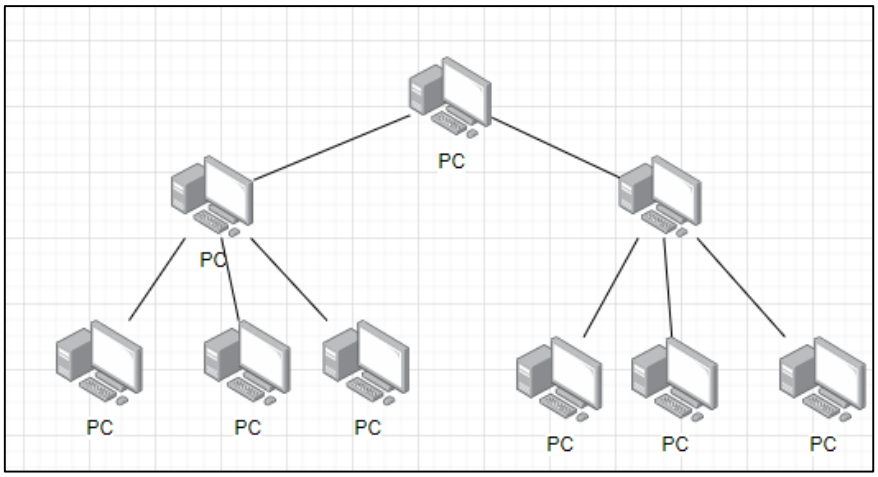

Figure 1. 11 : Topologie en hiérarchique.

- **La topologie complète (maillée)**

Pour des raisons d'erreur, le réseau est maillé dans lequel chaque nœud est caractérisé par sa connectivité, c'est-à-dire que pour accéder à un même nœud, il existe plusieurs chemins, cette structure a optimisé l'utilisation des ressources en répartissant la charge entre différents chemins. (Figure 1.12)

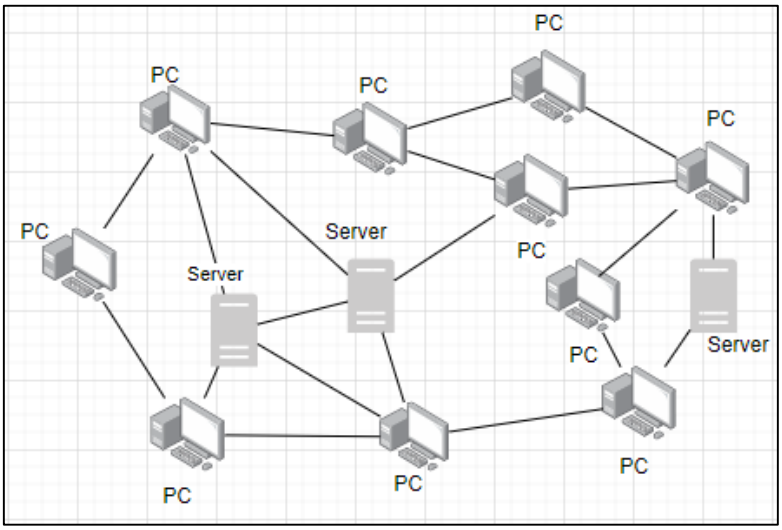

Figure 1. 12 : Topologie maillée.

➢ **Les topologies logiques**

- **Token Ring**

Token Ring est un protocole LAN qui fonctionne au niveau de la couche Liaison du modèle OSI (Open Systems Interconnection). Il utilise une trame spéciale de trois octets, appelée jeton.

- **Ethernet**

Ethernet est la technologie de base des réseaux LAN la plus utilisée actuellement. Le principe repose sur le fait que toutes les machines sont reliées à une même ligne de communication. L'institut IEEE (Institute of Electrical and Electronics Engineers) l'a normalisé et adapté dans son modèle IEEE 802.3. Il y a deux types d'Ethernet sont l'Ethernet commuté et l'Ethernet partagé [4].

Ethernet commuté :

Ethernet commuté est une technologie mure qui présente de nombreux avantages. Sa connaissance nous permet également de réutiliser des outils de maintenance déjà développés pour d'autres applications.

Ethernet partagé :

Ethernet partagé est l'utilisation de la stratégie Time Division Multiple Access (TDMA), pour laquelle chaque station bénéficie d'un temps d'accès pré alloué.

Quelques normes pour les différentes technologies Ethernet : (Tableau 1.1)

Norme	Appellation	Débit	Média utilisé
802.3	Ethernet	10 Mbps	Coaxial / UTP / fibre optique
802.3u	Fast Ethernet	100 Mbps	UTP / Fibre optique
802.3z	Gigabit Ethernet	1000 Mbps	Fibre optique
802.3ab	Gigabit Ethernet	1000 Mbps	Câble UTP
802.2ae	10 gigabit Ethernet	10 000 Mbps	Fibre optique

Tableau 1. 1 : les normes d'ethernet.

1.5. Les équipements d'interconnexion

1.5.1. La carte réseau

Une carte réseau (appelée Network Interface Card en anglais et notée NIC) c'est un périphérique informatique constitué d'éléments électroniques soudés à un circuit imprimé. Il reçoit les données envoyées par l'ordinateur et les retransmet à un autre appareil du réseau, il reçoit également des données du web et les transcrit sur votre ordinateur pour lecture et traitement. Par conséquent, il assure l'échange et la transmission de données entre votre ordinateur et d'autres appareils sur le réseau. (Figure 1.13)

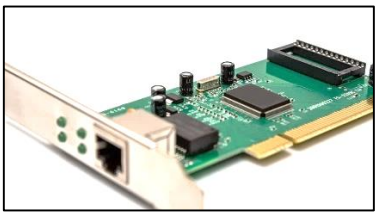

Figure 1. 13 : Carte réseau.

1.5.2. Le répéteur

Les répéteurs réalisent une connexion physique entre deux segments d'un même réseau logique. Agissant au niveau physique, les réseaux interconnectés doivent être homogènes. Le répéteur régénère les signaux reçus sur son interface d'entrée et les transfère sur son interface de sortie au format de celle-ci [5]. (Figure 1.14)

Figure 1. 14 : Répéteur WIFI.

1.5.3. Le concentrateur (HUB)

Un concentrateur est un répéteur qui envoie un signal via plusieurs ports d'E/S (entrée / sortie). Lorsqu'il reçoit un signal électrique sur une de ces interfaces, il le répètera en l'envoyant à toutes ses interfaces sauf celle qui a reçu ce signal. (Figure 1.15)

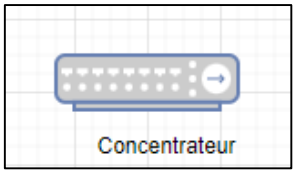

Figure 1. 15 : Un concentrateur.

1.5.4. Le commutateur (Switch)

Un switch réseau est un appareil qui permet de connecter plusieurs appareils segments sur le même réseau. Sa seule différence avec le Hub est qu'il peut connaître l'adresse physique des machines qui lui sont connectées et analyser les trames reçues pour les diriger vers la machine cible, il fonctionne au niveau 2 du modèle OSI (Open Systems Interconnection). (Figure 1.16)

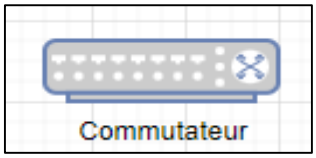

Figure 1. 16: Le commutateur.

1.5.5. Le pont (bridge)

Le pont appelé aussi bridge représente un élément réseau permet d'assurer la mise en relation d'un port d'entrée et un port de sortie avec une autorisation de la diffusion des messages de type broadcaste et Multicaste.

Le pont est utilisé pour connecter deux ou plusieurs segments d'un réseau local de même type, il travaille au niveau de la couche 2 du modèle OSI (couche liaison de données). (Figure 1.17)

Figure 1. 17 : Le pont.

1.5.6. Le routeur

Le routeur travaille au niveau de la couche 3 du modèle OSI, et s'occupe du routage des unités de données. Il permet d'interconnecter deux réseaux de type différents. C'est l'outil le plus élaboré pour acheminer les données [6]. (Figure 1.18)

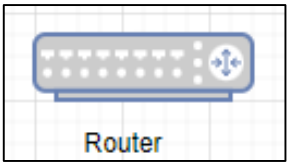

Figure 1. 18 : le routeur.

1.6. Les Supports de transmission

C'est un moyen avec lequel les différentes topologies qu'on vient de citer sont reliées entre eux :

1.6.1. Les câbles à paires torsadées

La paire torsadée ou symétrique est constituée de deux conducteurs identiques torsadés. Les torsades réduisent l'inductance de la ligne (*L*). Généralement plusieurs paires sont regroupées sous une enveloppe protectrice appelée gaine pour former un câble. Les câbles contiennent une paire (desserte téléphonique), quatre paires (réseaux locaux), où plusieurs dizaines de paires (câble téléphonique) [7]. (Figure 1.19)

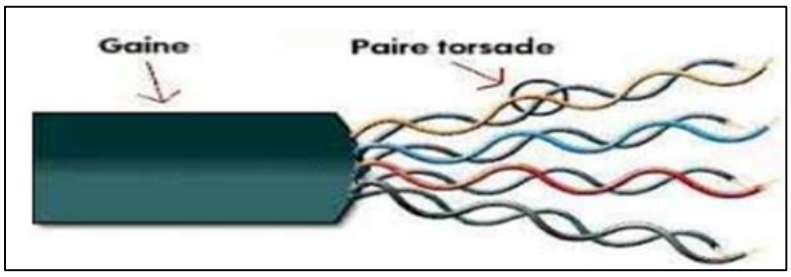

Figure 1. 19 : le câble paire torsadée.

1.6.2. Les câbles coaxiaux

Un câble coaxial se compose de deux conducteurs concentriques qui sont séparés par un diélectrique et un blidage l'un de l'autre. Les câbles coaxiaux sont utilisés dans la technique vidéo et dans la technique de mesure électrique, mais aussi dans les domaines oú des signaux radio doivent être transférés sans perte. (Figure 1.20)

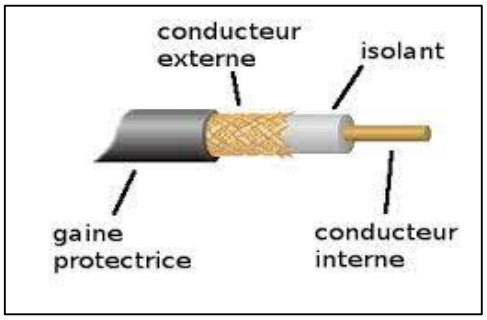

Figure 1. 20 : le câble coaxial.

1.6.3. Les câbles à fibre optique

L'intégration de la fibre optique dans le système de câble est liée au fait qu'elle résout les problèmes environnementaux dus à sa résistance aux interférences électromagnétiques et à l'absence de rayonnement radioélectrique. (Figure 1.21)

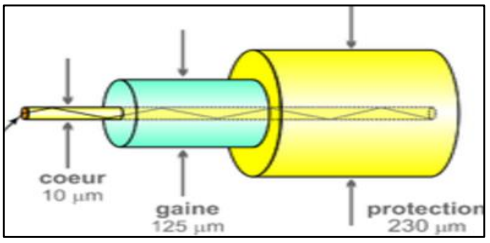

Figure 1. 21 : La fibre optique.

Principalement il y a deux types de fibre optique multimode et monomode [4] :

- **Fibre optique Multimode**

Dans une fibre multimode les sources qui diffusent la lumière ne sont pas la fibre monomode. En effet, elle utilise la LED (Light Emitting Diode), en français c'est DEL (Diode Electro luminescente), les rayons émis par ce type de fibre sont courts par rapport à la monomode .les fibres multimodes sont les fibres les plus utilisées dans l'entreprise. (Figure 1.22)

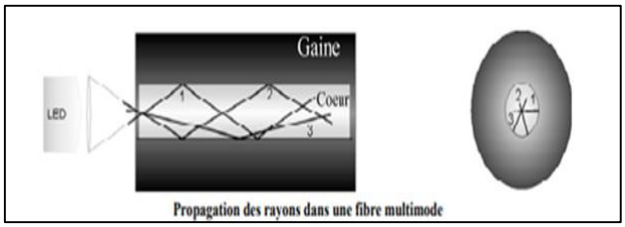

Figure 1. 22 : Fibre optique multimode.

- **Fibre optique monomode**

Une fibre optique monomode généralement utilise le laser. Le laser émet des rayons avec des grandes longueurs .leur utilisation est fréquemment destiné aux liaisons WAN, entre différents bâtiments. (Figure 1.23)

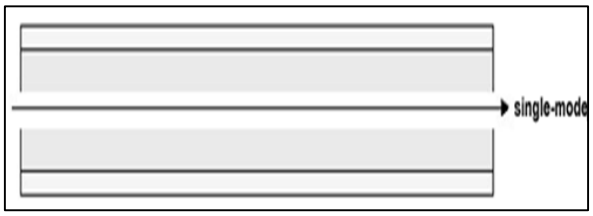

Figure 1. 23 : Fibre optique Monomode.

1.6.4. Transmission sans fil

Le Wi-Fi est un ensemble de protocoles de communication sans fil régis par les normes du groupe IEEE 802.11 (Institute of Electrical and Electronics Engineers 802.11). Un réseau Wi-Fi permet de relier par ondes radio plusieurs appareils informatiques (ordinateur, routeur, smartphone, décodeur Internet, etc.) au sein d'un réseau informatique afin de permettre la transmission de données entre eux.

1.7. Les Modèles généraux de communication

1.7.1. Modelé OSI

Le modèle OSI (Open Systems Interconnection) a été développé en 1978 par l'ISO (International Standard Organization) afin qu'il soit défini un standard, utilisé dans le développement des Systèmes ouverts. Le modèle OSI comprend sept couches, les couches basses (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les couches hautes (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs. Les couches 4 à 7 sont au contraire des couches qui n'interviennent qu'entre hôtes distants [9]. (Tableau 1.2)

Numéro	Nom de couche	Définition
Couche 7	Application	C'est la couche la plus proche de l'utilisateur, elle assure l'interface avec les applications
Couche 6	Présentation	La couche présentation spécifie les formats des données des applications (encodage MIME, compression, encryptions)
Couche 5	Session	Cette couche permet d'établir, gérer et fermer les sessions de communications entre les applications.
Couche 4	Transport	La couche transport c'est une couche de niveau 4 qui permet d'assurer la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission.
Couche 3	Réseau	Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.
Couche 2	Liaisons de données	La couche de liaison de donnée s'occupe de l'envoi de la donnée sur le média.
Couche 1	Physique	La couche physique définit les spécifications du média (câblage, connecteur, Voltage, bande passante….)

Tableau 1. 2: Les couches OSI.

1.7.2. Modelé TCP/IP (Le protocole de contrôle de transmission/protocole Internet)

Même si le modèle OSI est le plus rencontré dans la littérature courante, les applications réseaux actuelles utilisent le modèle TCP/IP, notamment parce que les applications informatiques courantes sont souvent reprises à cheval sur les 3 couches supérieures de l'OSI. Le modèle TCP/IP repose sur 4 couches [10]. (Tableau 1.3)

Numéro	Nom de Couche	Définition de la couche
Couche 4	Application	Définit les protocoles d'application TCP/IP et explique comment l'hôte programme l'interface avec les services de couches de transport pour utiliser le réseau.
Couche 3	Transport	La couche transport c'est une couche de niveau 2 permet à deux machines de communiquer (communication de bout en bout), Propose la gestion des sessions de communication entre les ordinateurs hôtes. Définit le niveau de service et l'état de la connexion utilisés lors du transport des données.
Couche 2	Internet	Cette couche gère la circulation des paquets à travers le réseau en assurant leur routage, aussi elle Regroupe les données en datagrammes IP qui contiennent des informations sur les adresses de source et de destination utilisées pour transmettre les datagrammes entre les hôtes et à travers les réseaux. Effectue le routage des datagrammes IP.
Couche 1	Accès Réseau	Donne des détails sur le mode d'envoi physique des données à travers le réseau, y compris sur la façon dont les bits sont électriquement signalés par les périphériques matériels jouant directement le rôle d'interface avec un support réseau, comme un câble coaxial, une fibre optique ou un fil de cuivre à paire torsadée.

Tableau 1. 3 : Les couches TCP/IP.

1.7.3. La différence entre le modèle de référence OSI et le modèle de couche TCP / IP

TCP/IP et OSI sont les deux modèles de réseau les plus utilisés pour la communication. Il y a quelques différences entre les deux. L'une des principales différences est que TCP/IP est utilisé pour les connexions et la communication sur les réseaux, tandis qu'OSI est un modèle conceptuel rarement utilisé pour la communication.

Voici une figure 1.24 qui illustre Comparaison entre le modèle OSI et le modèle TCP/IP

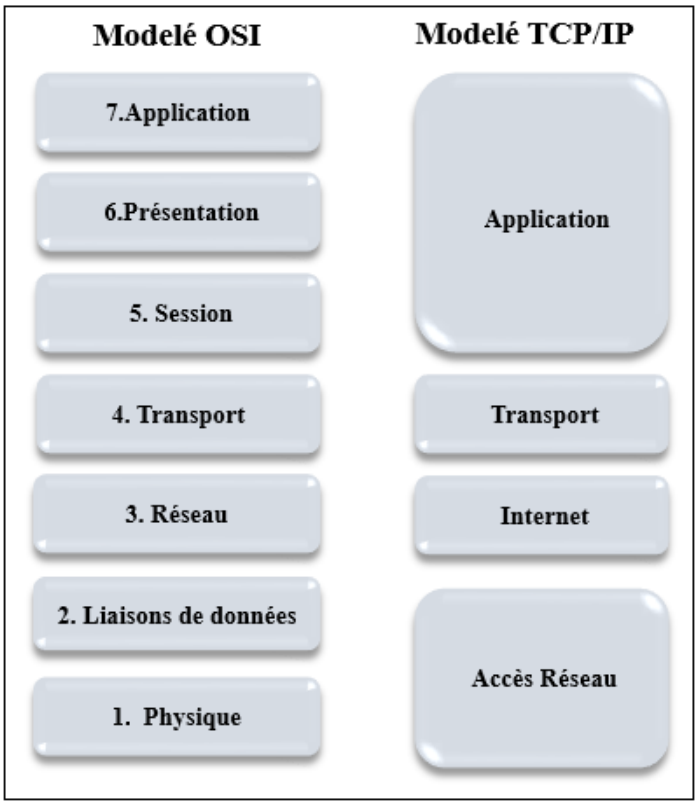

Figure 1. 24 : Modèles OSI - TCP/IP.

1.8. Les protocols réseaux

Un protocole réseau c'est un protocole de communication, qui s'exécute sur des réseaux informatiques ou bien sur des réseaux télécommunication. Il s'agit d'un ensemble de règles et de procédures de communication utilisées bilatéralement par toutes les stations échangeant des données sur le réseau. Il existe de nombreux protocoles réseau (NETWORK PROTOCOLS).

a. Protocole IPsec (Internet Protocol Security)

IPSec est un protocole de sécurité au sein de la couche réseau, ainsi que c'est un protocole de la couche 3 du modèle OSI, tout comme IP ; il fut à l'origine développé dans le cadre de la version future de ce dernier protocole, à savoir IPv6 (Internet Protocol version 6).

b. Protocole ICMP (Internet Control Message Protocol)

Le protocole ICMP permet de gérer les informations relatives aux erreurs du protocole IP. Il ne permet pas de corriger ces erreurs, mais d'en informer les différents émetteurs des datagrammes en erreurs. Utilisé pour les tests et les diagnostics (ping), Ce protocole est considéré comme faisant partie de l'ensemble des protocoles TCP/IP.

c. Protocole IP (Internet Protocol)

Le protocole IP est un protocole, ou un ensemble de règles, faisant partie de la couche Internet de la famille de protocoles TCP/IP, qui achemine et adresse les paquets de données afin qu'ils puissent traverser le réseau et atteindre la bonne destination. En fait, le protocole IP gère les datagrammes IP indépendamment en définissant leur représentation, leur routage et leur transmission.

d. Protocol ARP (Address Resolution Protocol)

Il s'agit d'un protocole qui se situe entre la couche liaison de données et la couche réseau, et résout le problème de résolution d'adresse, selon lequel un protocole de couche réseau doit envoyer un message à une destination et n'a que l'adresse de couche réseau(IP) de destination.

ARP est Protocole de résolution d'adresse permettant de faire le lien, entre les adresses de niveau (IP) et de niveau 2 (MACMedia Access Control) [11].

e. Protocole DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) est un protocole de configuration dynamique, utilisé pour assurer une gestion automatique et consiste en la distribution d'adresses IP au sein d`un réseau, et aussi c`un protocole peut configurer tout à la fois.

f. Protocole TCP (Transmission Control Protocol)

Protocole de niveau 4 qui fonctionne en mode connecté. Dans le cas d'une connexion TCP entre deux machines, les messages (ou paquets TCP) sont acquittés et délivrés en séquence.

Etablissement d'une connexion (circuit virtuel) entre 2 hosts pour échanger des données acquittées et garanties en séquence (compteurs).

g. Protocole DNS (Domaine Name Service)

Est une base de données utilisée sur les réseaux IP pour transposer les noms d'ordinateurs en adresse IP.

h. Protocole TCP/IP

Le protocole de contrôle de transmission et le protocole Internet, sont les protocoles de base pour la gestion des communications. Ces protocoles veillent à ce que deux ordinateurs en viennent à une entente sur les règles de base d'échange des données, et garantissent que les messages sont bien conditionnés et transmis sur le réseau [12].

1.9. L'adressage IP (Internet Protocol)

Les adresses IP permettent aux ordinateurs et aux appareils de communiquer entre eux sur Internet. Sans eux, personne ne saurait qui dit quoi ou à qui. Mais il en existe deux types: IPv4 (le protocole internet version 4) et IPv6 (Le protocole internet version 6).

1.9.1. Le protocole internet version 4 (IPV4)

IPv4 dénote la quatrième version du protocole IP (Internet Protocol), cette version du Protocole Internet qui a été largement développée, et il forme la base des communications sur Internet, elle permet d'identifier les machines connectées sur un réseau informatique.

Cette adresse est composée de quatre octets, chacun ayant leur valeur en décimale de 0 jusqu'à 255, séparés avec des points, Par exemple : 192.168.2.68. Le nombre maximal des adresses possibles est de 2^32 ce qui est équivalent à 4 294 967 296 adresses possibles et ces adresses IP sont des adresses IPv4.

- ✓ **La conception de l'adresse IP et son évolution**

Plusieurs groupes d'adresses ont été définis à l'origine pour optimiser le routage (ou routage) des paquets entre différents réseaux. Les adresses IP sont classées selon le nombre d'octets qui représentent le réseau. Ces classes correspondent à un regroupement en réseaux de même taille, et les réseaux partageant la même classe ont le même nombre maximum d'hôtes.

Il existe 4 classes : classe A ; classe B ; classe E ; classe C ; classe D. (Tableau 1.4)

Classe	Masque réseau	Adresses réseau
A	255.0.0.0	1.0.0.0 - 126.255.255.255
B	255.255.0.0	128.0.0.0- 191.255.255.255
C	255.255.255.0	192.0.0.0 – 223.255.255.255
D	240.0.0.0	240.0.0.0.0 -255.255.255255
E	Non défini	240.0.0.0.0 -255.255.255255

Tableau 1. 4 : Classe d'adressage IPv4 [13].

- Classe A : 128 réseaux et 16 777 214 hôtes (7 bits pour les réseaux et 24 pour les hôtes), la classe A défini une fourchette de réseaux d'adresses IP allant de 1.0.0.0 à 126.255.255.255.
- Classe B : 16 384 réseaux et 65 534 hôtes (14 bits pour les réseaux et 16 pour les hôtes), la classe B définit une fourchette de réseaux d'adresses IP allant de 128.0.0.0 à 191.255.255.255.
- Classe C : 2 097 152 réseaux et 254 hôtes (21 bits pour les réseaux et 8 pour les hôtes). La classe C définit une fourchette de réseaux d'adresse IP allant de 192.0.0.0 à 223.255.255.255.
- Classe D : ne désignent pas une machine particulière sur le réseau, mais un ensemble de machines voulant partager la même adresse et ainsi participer à un même groupe : adresses de groupe de diffusion (multicast).
- Classe E : le premier octet a une valeur comprise entre 240 et 255. Il s'agit d'une zone d'adresses réservées par IANA à un usage non déterminé. Ces adresses ne doivent pas être utilisées pour adresser des hôtes ou des groupes d'hôtes.

Les autres adresses sont particulières ou réservées :

- 0.0.0.0 : est une adresse non encore connue, utilisée par les machines ne connaissant pas leur adresse IP au démarrage.
- L'adresse dont la partie hôte est constituée de bits à 0 est une adresse réseau ou sous-réseau, 210.24.25.0 pour une classe C par exemple.
- L'adresse dont la partie hôte est constituée de bits à 1 est une adresse de diffusion (broadcast), 130.24.255.255 pour une classe B.
- 127.0.0.1 : une adresse de bouclage (loopback en anglais) est une adresse utilisée par une interface pour s'envoyer un message à elle-même. Cette adresse sert à tester le fonctionnement de carte réseau. Un Ping 127.0.0.1 doit retourner un message correct.

Pour chaque classe, certaines plages d'adresses sont réservées à un usage privé :

- classe A : 10.0.0.0.à 10.255.255.255
- classe B : 172.16.0.0 à 172.31.255.255
- classe C : 192.168.0.0 à 192.168.255.255

✓ **Notions de sous-réseaux et masque.**

- **Les Sous-réseaux**

Un sous-réseau est un réseau qui fait partie d'un autre réseau (de classe A, B ou C). Les sous-réseaux sont créés en utilisant un ou plusieurs bits de la partie hôte de classe A, B ou C pour étendre l'identifiant de réseau. Par conséquent, plutôt que d'avoir un identifiant de réseau standard de 8, 16 ou 24 bits, un sous-réseau peut avoir un identifiant de n'importe quelle longueur. Plus précisément, lorsqu'une segmentation en sous-réseaux est nécessaire, la partie hôtes de l'adresse IP peut être découpée en deux parties :

- Partie sous-réseau ;
- Partie hôte dans le sous-réseau.

- **Masques de sous-réseaux**

Un masque de sous-réseau a le même format qu'une adresse IPv4. Les bits à « 1 » désignent la partie réseaux et sous-réseau de l'adresse, et les bits à « 0 » désignent la partie machine sur le sous-réseau.

En l'absence de segmentation en sous-réseau, les masques sont ceux par défaut des classes standards :

- classe A : 255.0.0.0
- classe B : 255.255.0.0
- classe C : 255.255.255.0

1.9.2. Le protocole internet version 6 (IPV6)

Très pénalisante en termes de performance réseau, la notion de broadcast dispara11. Elle est remplacée par une généralisation des adresses multicast.

1Pv6 distingue trois types d'adresse :

- **Les adresses unicast (one-to-one)** : une adresse unicast désigne une interface, elle peut être utilisée pour identifier un groupe d'interfaces lorsque ces interfaces constituent une agrégation de liens et qu'ils doivent être vus comme une seule interface ;
- **Les adresses multicast (one-to-any)** : ces adresses désignent un ensemble d'interfaces dont la localisation n'est pas nécessairement sur le même réseau physique. Un datagramme adressé à une adresse multicast est acheminé à toutes les interfaces du groupe ;

- **Les adresses anycast (one-to-nearest)** : ces adresses introduites par 1Pv6 correspondent à une restriction des adresses de multicast. Elles désignent un ensemble d'interfaces partageant un même préfix réseau. Cependant, lorsqu'un datagramme est adressé à une adresse anycast, il n'est délivré qu'à une seule interface du groupe, celle dont la métrique, au sens routage du terme, est la plus proche du nœud source.

1.10. La sécurité des réseaux

1.10.1. Définition

De nos jours, la majorité des entreprises possèdent des réseaux locaux qui sont connectés à Internet. Cette ouverture vers l'extérieur est à la fois dangereuse et indispensable en même temps. En effet, ces réseaux peuvent être ouverts vers le monde étranger pour essayer de pénétrer le réseau local de l'entreprise. Pour cela la sécurité réseaux a pour objectif de sécuriser les réseaux informatiques de tous risques, attaques et vulnérabilité.

1.10.2. Objectifs de la sécurité réseau

Le système en réseau informatique est visé à pirater par les attaques dans le but d'avoir les informations sensibles ou altérer les services existent à tous les niveaux. La majorité des entreprises ont connu une attaque. Donc pour cela toutes les politique de sécurité sont mises en place dont le but d'avoir un réseau informatique sécurisée et performant afin de garantir les quatre objectifs de sécurité l'intégrité, la confidentialité, la non-répudiation et la disponibilité [14].

1.10.3. Les attaques

Les attaques peuvent être classées en deux grandes catégories : les techniques d'intrusion a pour objectif de s'introduire sur un réseau pour modifier et découvrir les données. Les dénis de service qui ont objectif d'empêcher un service ou une application de fonctionner. Une autre classification existante distingue les attaques passives basées sur l'interception et l'écoute qui concernent la confidentialité seulement et les attaques passives qui altèrent les servies et également les données qui concernent la disponibilité [14].

1.10.4. Le Mécanisme de sécurisation

Les mécanismes mis en œuvre pour garantir la confidentialité, l'intégrité, l'authentification, le non-désaveu et la disponibilité du système peuvent de répartir en deux techniques : celles qui tendent à protéger les données et celles qui tendent à protéger les systèmes [15].

La protection des données :

- Cryptographie : C'est un chiffrement utilisé pour sécuriser les données informatiques à l'aide d'une clé de chiffrement, une clé pour chiffrement et une autre pour le déchiffrement.
- Sécurisation des échanges sur le web : S-http introduit la cryptographie au niveau http dont elle constitue une extension. S-HTTP c'est la version du http sécurisé.
- IP Security : IPsec Internet Protocol Security Standard fournit une sécurisation au niveau IP. Développé à l'origine le cadre d'IPv6 et adapté à IPv4, il offre les services de contrôle d'accès, d'authentification, d'intégrité et confidentialité.

1.11. Conclusion

Au cours de ce chapitre, nous avons parcouru des généralités sur les réseaux informatiques ainsi sa sécurité du réseau, leurs notions et leurs aspects élémentaires, à savoir les outils d'interconnexion, les classifications des réseaux, ainsi il nous a permis de différencier entre le modèle OSI et le modèle TCP/IP.

Le prochain chapitre, sera consacré à la présentation de l'organisme d'accueil et nous allons proposer des solutions pour subvenir aux besoins de ce dernier.

Chapitre 2

Chapitre 2 : Présentation de l'organisme d'accueil

2.1. Introduction

Un réseau d'entreprise peut connecter tous les ordinateurs via un serveur qui contrôle les droit d'accès à Internet, aux e-mails se taux documents et travaux partagés. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe authentifié par le serveur. Les utilisateurs peuvent accéder à leurs données et partagent les fichiers.

Ce chapitre présente un bref historique de CEVITAL Bejaia, et un aperçu des différentes divisions qui composent l'entreprise. De plus, nous analysons les sujets sur lesquels se déroule principalement le projet.

2.2. Organisme d'accueil

2.2.1. Présentation de l'entreprise et son historique

Dans cette partie, nous allons présenter le groupe CEVITAL, sa nature, son rôle national et son image à l'international, tout en citant les divers départements qui le forment.

- **Présentation du groupe CEVITAL**

Premier groupe privé algérien, créé en 1998 par l'entrepreneur **ISAAD Rabrab**, leader du secteur agroalimentaire en Algérie, Société par action implantée au sein du port de la wilaya de Bejaia.

Ce groupe familial a pu couvrir les besoins nationaux et réussir à mettre l'Algérie sur la liste des pays exportateurs des huiles, des margarines ainsi que le sucre ; et ce grâce à l'ultra modernité de ses unités de production, au contrôle étroit de qualité, l'élargissement ainsi qu'à l'excellence de son service de logistique.

- **Historique**

Aujourd'hui, CEVITAL agroalimentaire est le plus grand complexe privé en Algérie. Il est devenu le leader du secteur agroalimentaire en Afrique. CEVITAL a traversé d'importantes étapes historiques pour atteindre sa taille et sa notoriété actuelle [17]. Ci-après, quelques dates qui ont marqué l'histoire de CEVITAL :

- **1971** : lancement de la construction métallique
- **1988** : création de metal sider (sidérurgie)
- **1991** : reprise des activités i.b.m en algérie / création du quotidien liberté
- **1997** : création de hyundai motors algérie
- **1998** : création de cevital spa industries agroalimentaires
- **2006** : création de numidis et immobis; acquisition de cojek
- **2007**: samha – production & distribution samsung / création mfg (verre plat)
- **2008** : nolis - transport maritime /commercialisation du verre plat en europe /création de numilog
- **2009** : augmentation de la production de sucre de 1 m t/an
- **2013** : oxxo (france) / alas (espagne)
- **2014** : brandt (france) / afferpi (italie) ex lucchini piombino

2.2.2. Situation géographique

L'entreprise CEVITAL se situe à l'arrière port de la wilaya de Bejaia à 200 ML (mètre linéaire) du quai à 3km Sud-ouest de la ville, à proximité de la RN 26 et la RN 9. Cette situation géographique de l'entreprise lui prote bien étant donné qu'elle lui confère l'avantage de la proximité économique. Le complexe s'étend sur une superficie de 45 000m^2 (le plus grand complexe privé en Algérie), il a une capacité de stockage de 182 000 tonnes/an (silos portuaire), et un terminal de déchargement portuaire de 200 000 tonnes/heure (réception de matière première). Elle possède un réseau de distribution de plus de 52 000 points de vente sur tout le territoire national également. (Figure 2.1)

Figure 2. 1 : Image satellitaire de CEVITAL Bejaia.

2.2.3. Activité de l'entreprise CEVITAL

CEVITAL Agro-industrie dispose de plusieurs unités de production ultramodernes :

- 2 raffineries de sucre ;
- 1 unité de sucre liquide ;
- 1 raffinerie d'huile ;
- 1 margarinerie ;
- 1 unité de conditionnement d'eau minérale ;
- 1 unité de fabrication et de conditionnement de boissons rafraîchissantes ;
- 1 conserverie ;
- 1 unité de fabrication de chaux calcinée.

2.2.4. Organigramme générale du groupe CEVITAL

Ce qui caractérise CEVITAL c'est la stratégie ainsi que la diversification des directions qu'elle a mise en place pour déterminer les différentes fonctionnalités dans le but de répondre au besoin du marché national et même international.

La figure 2.2 ci-dessous présente l'organigramme général de l'organisation administrative de l'entreprise CEVITAL site de Bejaia.

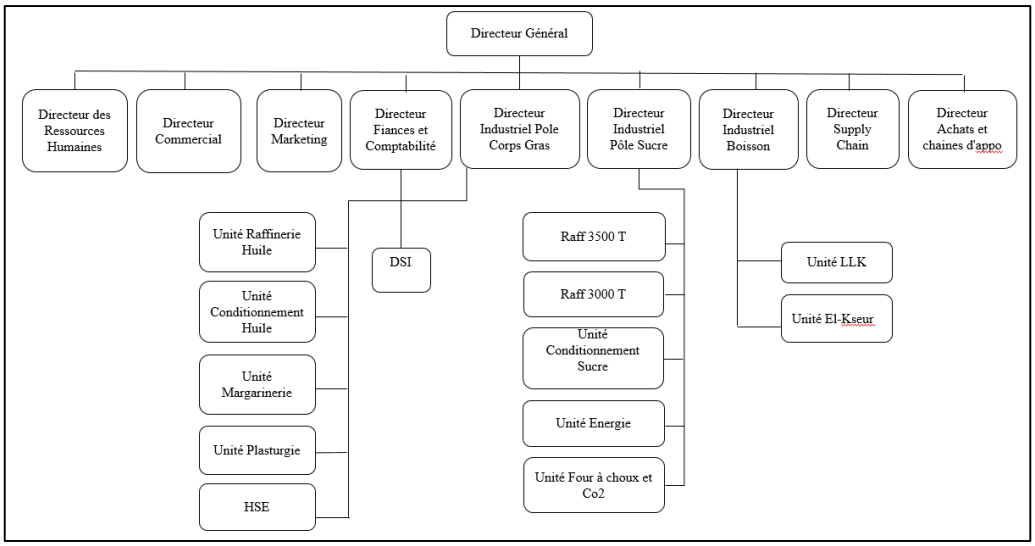

Figure 2. 2 : Organigramme générale du groupe CEVITAL.

2.2.5. Présentation de la Direction du système d'informatique CEVITAL

Nous avons effectué un stage au niveau de la division Réseaux et Télécoms de la Direction des Systèmes d'Information (DSI). Ce dernier assure la mise en place des mesures et technologies de l'information nécessaires à l'amélioration des activités, de la stratégie et des performances de l'entreprise. Par conséquent, la cohérence des ressources informatiques et de télécommunications mises à la disposition des utilisateurs, la compétence technique des utilisateurs, la disponibilité et la facilité d'utilisation constantes, ainsi que la sécurité globale doivent être garantie. L'organigramme du système d'information est présenté dans la figure suivante (Figure 2.3).

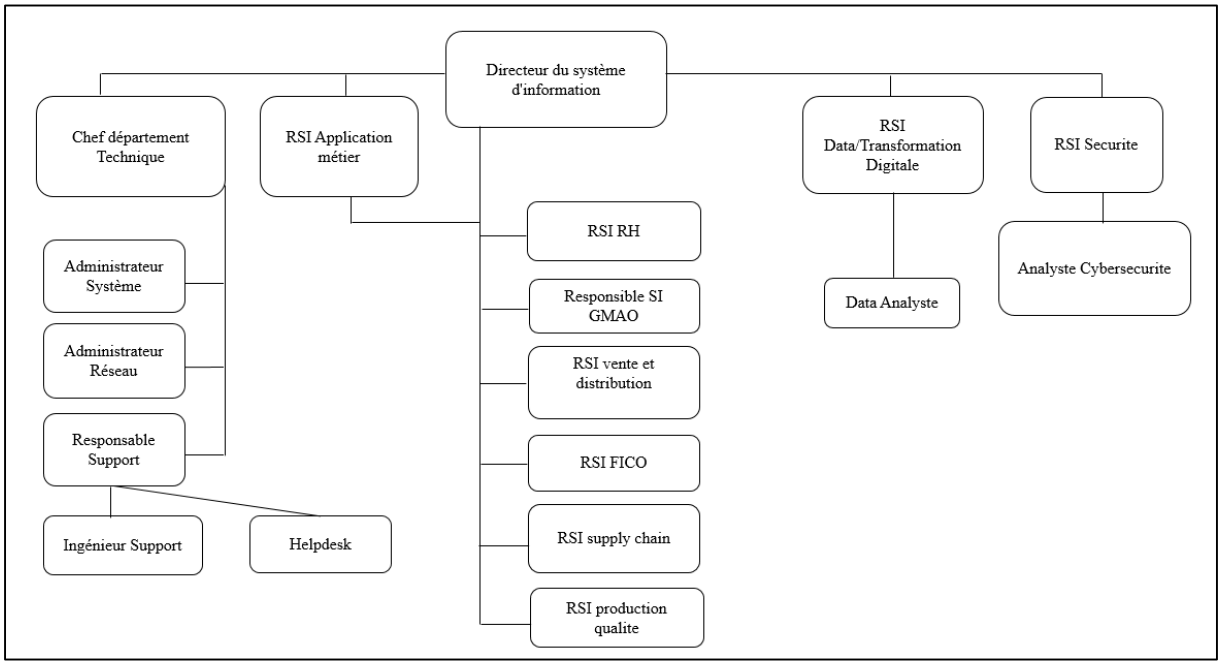

Figure 2. 3 : Organigramme de la direction système d'information.

La direction du système d'informatique CEVITAL est suivie par des responsables spécialistes cités ci-dessous :

- **Directeur du système d'information :** Il est chargé de régler les problèmes à moindre coût et dans les plus brefs délais et opter pour des solutions informatiques améliorant la productivité de l'entreprise.
- **Administrateur système :** Il conçoit, installe et veille au bon fonctionnement d'une infrastructure informatique et réseau d'une entreprise, il assure également la gestion et la maintenance de système opérant sur le réseau.
- **Administrateur réseau :** Il permet d'administrer le réseau et d'assurer la bonne circulation de l'information dans l'entreprise en veillant à la qualité, continuité et la performance des équipements et du réseau, tout en répondant aux besoins des utilisateurs.

- **Responsable support :** Il permet d'assurer un contrôle à distance des postes, apporter aux utilisateurs une aide pour la prise en main de leur équipement et assurer un support téléphonique interne.

2.2.6. Architecture du réseau CEVITAL

CEVITAL dispose d'un réseau interne assez étendu qui relie les différents bâtiments, unités de production et de gestion du complexe. Nous pouvons le diviser en plusieurs parties : Le backbone du réseau, pare-feu, DMZ (DeMilitarized Zone), point d'accès Wi-Fi, routeur et enfin le centre de données data-center où se trouvent les serveurs de l'entreprise. Le réseau est composé de plusieurs équipements, dont la plupart sont des équipements Cisco, qui sont interconnectés par fibre optique (Switch, Catalyst, Router) ou paires torsadées en cuivre. Nous tenons à souligner que tout au long de ce manuscrit, l'unité CEVITAL fait référence à l'emplacement de Bejaia pour la plupart des citations. (Figure 2.4)

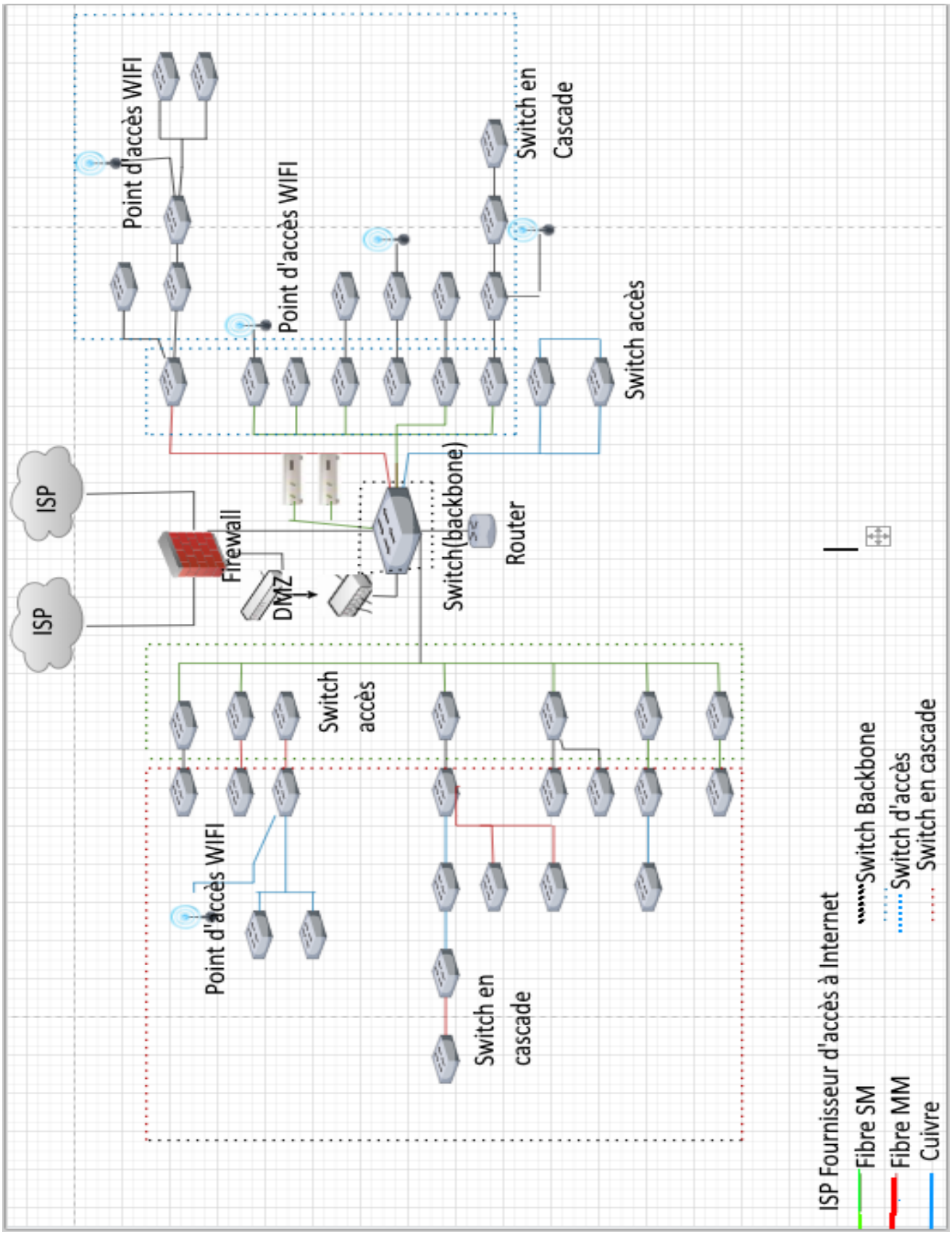

Figure 2. 4 : Architecture du réseau informatique du site CEVITAL-Bejaia.

2.2.7. Câblage informatique

Le système de câblage informatique installé est conçu pour fonctionner de façon idéale pour permettre des améliorations futures. Tout dispositif informatique existant dans l'entreprise sont interconnectés via le câblage de type fibre optique. Les boitiers des prises muraux sont repérés par des étiquettes portant un numéro unique sur le réseau et qui est repéré facilement dans le panneau de brassage pour l'interconnexion avec les commutateurs « prise Rj45 »

2.2.8. Les liaisons inter-sites

Dans le but de partager les différentes informations internes ainsi que les ressources au sein de la société, le groupe CEVITAL a mis en place deux liaisons afin de relier le complexe de Bejaia aux différentes annexes : (Figure 2.5)

- Une liaison fibre optique point à point entre Bejaïa et Alger.
- Une Liaison par satellite (Vsat) entre Bejaïa et les sites d'EL Kser (Cojek), site de TiziOuzou (Lala Khadija) et El Khroub

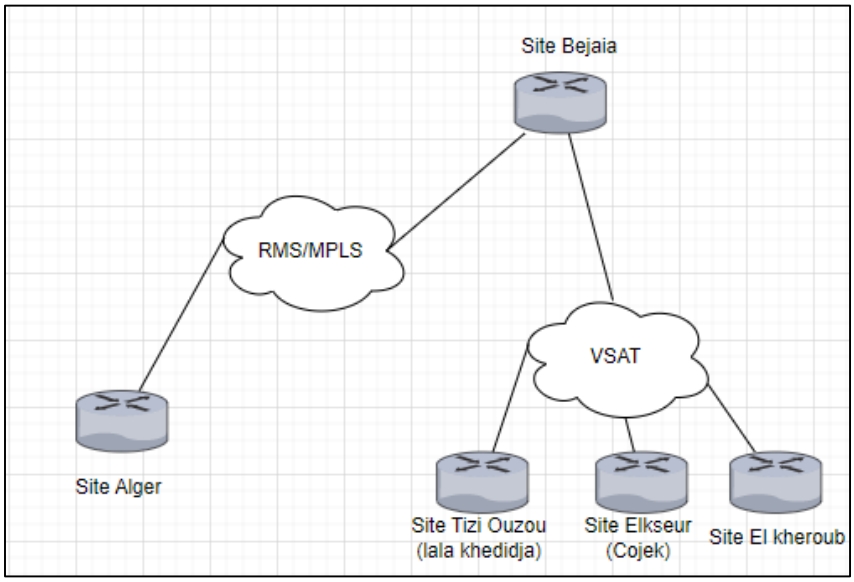

Figure 2. 5 : Connexion inter-sites du site CEVITAL Bejaia.

2.2.9. VLAN de l'entreprise

Un administrateur réseau a divisé le réseau en plusieurs VLAN selon différents départements. VLAN Management a été créé pour permettre la gestion du réseau à distance (configuration, mises à jour et sauvegarde des équipements).

L'adressage utilisé dans l'architecture est de classe A, divisé en sous-réseaux 10.10.0.0/24. (Tableau 2.1) suivant présente la liste des VLAN

Direction	VLAN
DRH	VLAN10
Direction des Appro	VLAN11
DSI	VLAN12
Raff Huile	VLAN13
Raff sucre 3000T	VLAN14
Division utilités	VLAN15
Supply-chain	VLAN16
Unité margarinerie	VLAN17
Printer	VLAN18
Téléphone	VLAN20
Voice	VLAN21
Direction R&D	VLAN22
Performance industriel	VLAN23
Unité Cdt Huile	VLAN24
Management switch	VLAN 25
DFC	VLAN26
Commercial	VLAN27
Direction générale	VLAN28
Direction qualité et management système	VLAN29
Raff sucre 3500T	VLAN30
Cdt sucre	VLAN31
Caméra	VLAN32
Projets	VLAN33
Trituration	VLAN36

Tableau 2. 1 : Liste des VLANs de l'entreprise**.**

2.2.10. Points forts de l'existant

Le réseau de CEVITAL présente un ensemble de points forts qu'il faut préservé à citer:

- Présence d'un firewall qui protège le réseau informatique interne de l'entreprise, analyse le trafic entrant en fonction de règles préétablies et filtre les données provenant de sources non sécurisées ou suspectes pour prévenir les attaques.
- Tenir compte de la protection contre les risques physiques (les dégâts d'eau, de feu ou d'électricité).
- Existence d'un système de gestion et de surveillance du réseau monitoring (recevoir des notifications en cas de panne du périphérique, et mettre des alertes par courrier électronique).

2.2.11. Critique de l'existant

Après analyse du réseau CEVITAL (en particulier le réseau informatique existant), un certain nombre de lacune sont été découvertes. Cela nous a permis de définir un grand nombre de limites de fonctionnalités, qui pourraient dégrader considérablement les performances des réseaux existants. Voir aussi les dysfonctionnements courants. Les conclusions concernant les réseaux existants comprennent :

- De plus, Un unique backbone centralise le réseau, Cela signifie que tous la charge réseau et sur lui. ce qui implique que le backbone et en surcharge.
- Les commutateurs en cascade limitent la bande passante,ralentissant davantage les applications et les ressources existantes.Une simple panne logicielle ou matérielle dans l'un des commutateurs perturbera la connectivité de tous les utilisateurs au réseau.
- Utilisation d'un seul domaine de diffusion ce qu'implique la surcharge de réseau.
- Absence un serveur redondant afin d'assurer la tolérance en cas de la panne ainsi que la redondance des liens et des équipements causant des défaillances dans l'architecture de réseau.

2.2.12. Problématique

De nos jours le système informatique est devenu indispensable au bon fonctionnement de l'entreprise en particulier les grandes entreprises, dont il joue un rôle primordial en assurant des services de collecte, stockage, traitement et diffusion de l'information non seulement entre le personnel de l'entreprise qui représente un effectif important mais aussi qui est répartis sur plusieurs unités.

Cependant, dans le cas où le système informatique manque de pertinence et d'efficacité, cela engendrera un ralentissement ou totalement un arrêt des activités de l'entreprise et affectera d'une façon négative le rendement des équipes ainsi que la production.

De ce fait, l'infrastructure du réseau d'une entreprise devient une base indispensable, ceci dit, par quel biais doit-on assurer le bon fonctionnement ainsi de maintenir l'efficacité du réseau au sein du groupe, quelle structure topologique, et comment faire face au dysfonctionnement des équipements matériels et logiciels ?

2.2.13. Propositions

Afin de répliquer à la problématique posée ci-dessus, nous tenons à mettre en avant des solutions dont une étude sera menée pour but de les affirmer ou les confirmer :

- ✓ Mettre en place une architecture redondance tout en se basant sur deux backbones interconnectés en redondances avec un protocole de routage au niveau du cœur du réseau afin de réduire le nombre des switches branchés en cascade.
- ✓ Se baser sur un protocole de haute disponibilité pour but de régler le souci de défaillance des équipements.

2.2.14. Solution optée

Nous étions satisfais qu'après l'analyse des examens cités précédemment, que la solution la plus appropriée serait d'utiliser une architecture de réseaux qui sera composée de quatre switches de niveau 3 avec un protocole de routage OSPF et aussi des protocoles à haute disponibilité au niveau de la couche de distribution. Pour cela, nous avons opté pour le HSRP comme un protocole de redondance. De plus, nous avons décidé de minimiser le nombre de switches interconnectés en cascade et qui rassure et la connectivité de plus grand nombre possible de switches aux backbones dans distribution.

- Après tout analyse des problématiques et de solution optée nous avons proposé d'utiliser le simulateur Cisco Packet Tracer pour l'élaboration de notre projet et de montrer le bon fonctionnement de la nouvelle architecture. malgré qu'il existe plusieurs moyens et méthode pour réaliser ce denier comme l'algorithme SDN (Software-Defined Networking) qui sert a dissocie le plan de contrôle logiciel du matériel réseau.

2.3. La Haute Disponibilité d'un Réseau Informatique

Après avoir présenté l'organisme de l'entreprise et les différents problèmes prisant sur leur réseau, nous allons à présent dans ce chapitre élaborer une étude descriptible de la haute disponibilité, ainsi qu'une présentation de différents protocoles assurant cette dernière.

2.3.1. Définition de la haute disponibilité

La forte densité du réseau et sa redondance permettent également la mise en place d'une confiance entre les acteurs, indispensable pour acquérir des informations parfois stratégiques pour l'entreprise [18].

Ce que les entreprises recherchent aujourd'hui, c'est un réseau fiable et toujours disponible. Une telle solution n'est pas forcément très simple à mettre en place, de plus, elle peut être relativement coûteuse pour l'entreprise. Il est préférable d'avoir un réseau qui prend en placé les charges sans interruption d'utilisation et sans redondance des pannes. Cela signifie que plusieurs appareils remplissent la même fonction, tout en étant aussi transparent que possible pour l'utilisateur.

2.3.2. Évaluation des risques

La panne d'un système informatique peut causer une perte de productivité et d'argent, voire des pertes matérielles ou humaines dans certains cas critiques. Il est ainsi essentiel d'évaluer les risques liés à un dysfonctionnement d'une des composantes du système d'information et de prévoir des moyens et mesures permettant d'éviter ou de rétablir dans des temps acceptables tout incident. Comme chacun le sait, les risques de pannes d'un système informatique en réseau sont nombreux. L'origine des fautes peut être schématisée de la manière suivante [19].

- Origines opérationnelles ;
- Origines humaines ;
- Origines physiques.

2.3.3. Comment assurer la haute disponibilité d'une infrastructure informatique

La redondance des appareils garantit une haute disponibilité de l'infrastructure informatique.

La redondance vous donne non seulement accès à votre solution de sauvegarde en cas de panne informatique, mais elle maximise également la capacité et les performances du système. La redondance augmente l'efficacité globale, comme une équipe de composants disparates travaillant ensemble pour résoudre les problèmes plus rapidement et plus efficacement.

Pour assurer la haute disponibilité de son infrastructure informatique, une entreprise peut d'abord compter sur l'équilibrage de charge de ses serveurs Web. Cette opération toute simple

permet en outre de distribuer les tâches ou les communications au sein d'un réseau sur deux serveurs distincts ou plus, notamment pour en améliorer la performance.

Cette méthode permet d'assurer la disponibilité des services informatiques d'une entreprise même lorsqu'ils sont fortement achalandés. Ainsi, par le biais de celui-ci, les utilisateurs sont répartis entre les différents serveurs à l'aide d'un équilibreur de charge, c'est-à-dire un dispositif qui trie intelligemment les requêtes des utilisateurs selon l'espace disponible sur les serveurs [20].

2.3.4. Les protocole FHRP (First Hop Redundancy Protocol)

Le protocole de redondance du premier saut est un protocole basé sur un réseau informatique conçu pour permettre la redondance de la passerelle. Il est implémenté dans un réseau pour définir un chemin de secours en cas de perturbation. FHRP est configuré en définissant un routeur actif et un ou plusieurs routeurs de secours dans le réseau. Une adresse IP virtuelle est attribuée dans le processus. Il existe plusieurs types de protocoles de redondance Fast Hop tels que le protocole HSRP (Hot Standby Router Protocol), le protocole VRRP (Virtual Router Redundancy Protocol), le protocole GLBP (Gateway Load Balancing Protocol), le protocole CARP (Common Address Redundancy Protocol), le protocole ESRP (Extreme Standby Router Protocol), Routed Split multi-link trunking (R-SMLT), NetScreen Redundancy Protocol (NSRP) [21].

a. Protocol HSRP (Hot Standby Router Protocol)

HSRP est un protocole Cisco permettant d'assurer une haute disponibilité des passerelles réseau, qui peut être implémenté sur des routeurs ou des commutateurs de couche 3. L'objectif est qu'une défaillance potentielle du routeur ne perturbe pas le routeur. Il est construit en regroupant les opérations de plusieurs routeurs physiques (au moins 2) qui se supportent automatiquement, c'est-à-dire d'un routeur à l'autre.

- **Fonctionnement de HSRP**

Cela se fait par la mise en commun du fonctionnement de plusieurs routeurs physiques (au minimum deux) qui, de manière automatique, assurerons la relève entre eux d'un routeur à un autre. Le protocole HSRP présente aussi son semblable normalisé qui se nomme VRRP. Celui-ci étant normalisé, il est disponible sur les routeurs d'autres marques que Cisco. Plus précisément, la technologie HSRP permettra aux routeurs situés dans un même groupe (que l'on nomme « standby group ») de former un routeur virtuel qui sera l'unique passerelle des hôtes du réseau local. En se « cachant » derrière ce routeur virtuel aux yeux des hôtes. Les routeurs garantissent en fait qu'il y est toujours un routeur qui assure le travail de l'ensemble du groupe. Un routeur dans ce groupe est donc désigné comme « actif » et ce sera lui qui fera passer les requêtes d'un réseau à un autre.

Pendant que le routeur actif travail, il envoie également des messages aux autres routeurs indiquant qu'il est toujours « vivant » et opérationnel. Si le routeur principal (élu actif) vient à tomber.

Il sera automatiquement remplacé par un routeur qui était alors jusque-là « passif » et lui aussi membre du groupe HSRP. Aux yeux des utilisateurs toutefois, cette réélection et ce changement de passerelle sera totalement invisible car ils auront toujours pour unique passerelle le routeur virtuel que forment les routeurs membres du groupe HSRP. Le routeur virtuel aura donc toujours la même IP et adresse MAC aux yeux des hôtes du réseau même si en réalité il y a un changement du chemin par lequel transitent les paquets [22].

Pour illustrer cela, nous pouvons schématiser la vision que les hôtes auront du réseau ainsi que l'état réel du réseau :

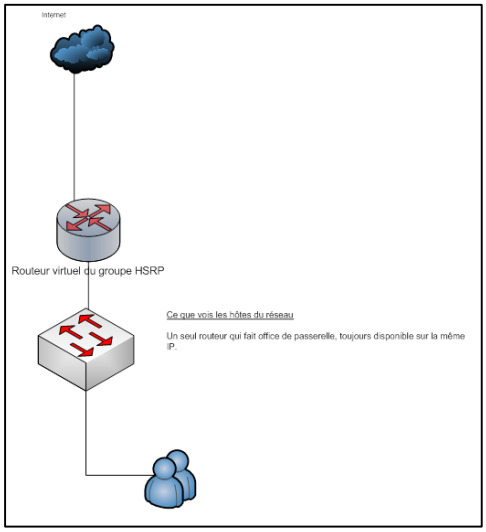

Figure 2. 6 : Le protocole HSRP vue d'un hôte du réseau.

L'état réel du réseau :

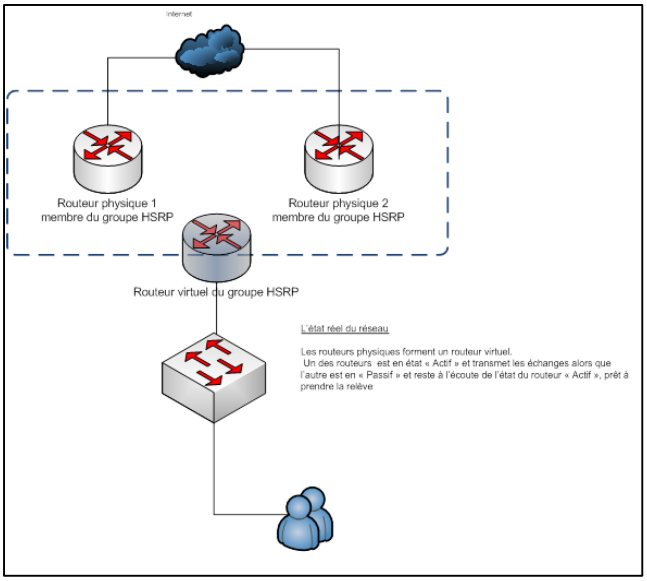

Figure 2. 7 : Le schéma physique et virtuel d'un réseau HSRP.

b. Protocol VRRP (Virtual Router Redundancy Protocol)

VRRP spécifie un protocole d'élection pour fournir le routeur virtuel fonction décrite précédemment. Tous les messages de protocole sont exécutés en utilisant des datagrammes IP multicast, ainsi le protocole peut fonctionner sur une variété de technologies LAN multi-accès prenant en charge la multidiffusion IP. Chaque routeur virtuel VRRP a une seule adresse MAC bien connue qui lui sont alloués [23].

c. Protocol GLBP (Gateway Load Balancing Protocol)

Gateway Load Balancing Protocol (GLBP) est de conception Cisco, avec partage de charge, brevet encore en instance. Il permet de faire de la redondance ainsi que de la répartition de charge sur plusieurs routeurs utilisant une seule adresse IP virtuelle, mais plusieurs adresses MAC virtuelles [23].

2.3.5. Les protocoles de routage

a. Le protocole RIP (Routing Information Protocol)

Il s'agit d'un protocole de routage IP de type vecteur de distance qui permet à chaque routeur de communiquer avec ses routeurs voisins. Le nombre de sauts est utilisé pour calculer une valeur métrique qui détermine le meilleur chemin pour atteindre le réseau.

b. Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol)

C'est un protocole propriétaire Cisco. Est une version améliorée d'IGRP qui utilise la même technologie à vecteur de distance. Les améliorations portent principalement sur les propriétés de converge et l'efficacité des opérations du protocole.

c. Le protocole OSFP (Open Shosrtest Path First)

C'est un protocole est basé sur la technologie d'état de liaison (Il est plus performant que le protocole RIP). Contrairement à lui, ce protocole n'envoie pas aux routeurs adjacents le nombre de saut qui les séparent mais l'état de la liaison qui les sépare. L'OSPF sert à déterminer le meilleur chemin que peuvent emprunter les paquets ce qui permet d'avoir une meilleure bande passante utile qu'avec RIP.

2.3.6. STP (Spanning-Tree Protocol)

C'est un protocole de gestion de couche 2, qui fournit des chemins redondants dans un réseau tout en évitant les boucles de routages. Tous les protocoles STP utilisent un algorithme STA (Spanning-Tree Algorithme) qui calcule le meilleur chemin sans boucle à travers le réseau. (Figure 2.8)

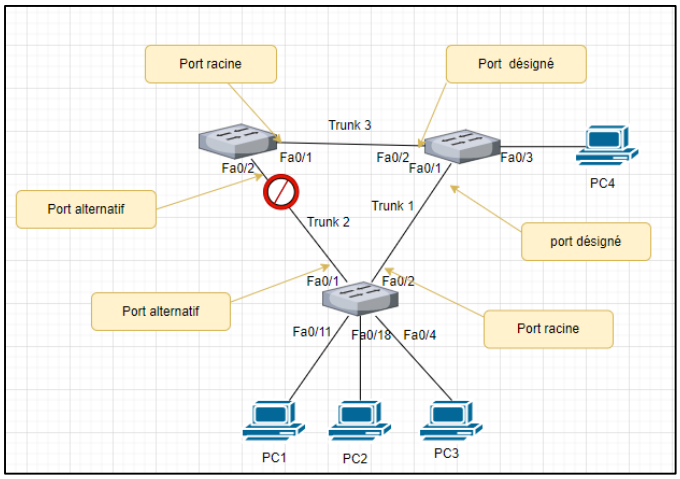

Figure 2. 8 : Description de l'algorithme STP.

2.3.7. VTP (VLAN Trunking Protocol)

VTP (VLAN Trunking Protocol), protocole propriétaire Cisco permet, aux commutateurs qui l'implémentent, d'échanger des informations de configuration des VLAN. Il permet donc de redistribuer une configuration à d'autres commutateurs, évitant par la même occasion à l'administrateur de faire des erreurs, en se trompant par exemple de nom de VLAN. VTP diffuse ses mises à jour au sein du domaine VTP toutes les 5 min ou lorsqu'une modification a lieu [25].

Dans un domaine VTP, on distingue une hiérarchie comprenant trois modes de fonctionnement : (Figure 2.9)

- VTP **serveur**
- VTP **client**
- VTP **transparent**

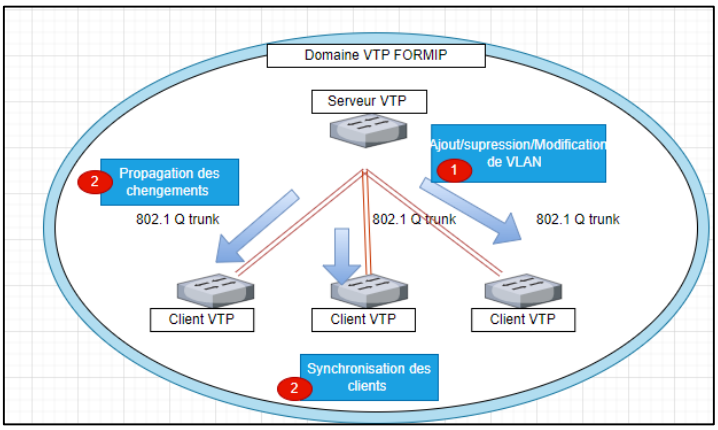

Figure 2. 9 : Domaine VTP.

2.3.8. EtherChannel

La technologie EtherChannel a initialement été développée par Cisco comme une technique de réseau local entre deux commutateurs permettant d'assembler plusieurs liens physiques Ethernet identiques en un seul lien logique. Cette technologie a pour but d'augmenter la bande passante et d'améliorer la tolérance aux pannes entre les commutateurs, les routeurs et les serveurs. (Figure 2.10)

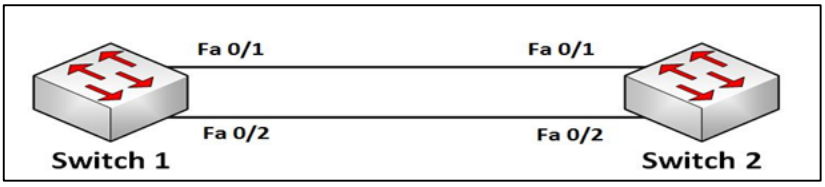

Figure 2. 10 : Schéma illustre l'interconnexion de deux switch avec Etherchannel.

2.4. Conclusion

Ce chapitre porte généralement sur la présentation de l'organisme d'accueil, en l'occurrence le site CEVITAL Bejaia. Cependant, la première partie de ce chapitre a pu donner un aperçu de CEVITAL et mettre en évidence les problèmes qui ont conduit à proposer des solutions. Cette dernière revient essentiellement à proposer de nouvelles architectures et à mettre en place de la haute disponibilité.

La partie 2 de ce chapitre est consacrée à la définition des différents protocoles utilisés dans le projet et à la compréhension du processus et des bénéfices qu'il apporte au réseau.

Chapitre 3

Chapitre 3 : Conception et réalisation d'une architecture réseau

3.1. Introduction

Dans ce chapitre, nous allons présenter les différentes configurations nécessaires à la mise en œuvre d'un nouveau réseau LAN, basé sur le simulateur Cisco Packet Tracer (Figure 3.1).

Pour bien présenter les différentes étapes de configurations mises en place sur les équipements réseau, nous avons fait usage de l'outil de captures d'écran.

3.2. Présentation du simulateur

Cisco Packet Tracer est un simulateur de matériel réseau très puissant permettant de construire un réseau physique virtuel et de simuler le comportement des protocoles réseaux sur ce réseau. L'utilisateur construit son réseau à l'aide d'équipements tels que les routeurs, les commutateurs ou des ordinateurs. Ces équipements doivent ensuite être reliés via des connexions (câbles divers, fibre optique). Une fois l'ensemble des équipements reliés, il est possible pour chacun d'entre eux, de configurer les adresses IP, les services disponibles, etc. (Figure 3.1)

Figure 3.1 : Capture de simulateur Cisco Packet Tracer 8.2.1.0118

Une fois nous ouvrons Cisco Packet tracer, l'interface ci-dessous va être affiché d'où y' on trouve : La zone (1) indique l'espace de travail dans lequel on construira notre réseau, regardera des simulations et affichera de nombreux types d'informations et de statistiques. Les équipements sont regroupés en catégories accessibles dans la zone (2). Une fois la catégorie sélectionnée, le type d'équipement peut être sélectionné dans la zone (3).La zone (9) signifie la barre de menu, la zone (8) indique la barre d'outils principale et La zone (6) contient un ensemble d'outils : – Select : pour déplacer ou éditer des équipements – Move Layout : permet de déplacer le plan de travail – Place Note : pour placer des notes sur le réseau – Delete : pour supprimer un équipement ou une note – Inspect : permet d'ouvrir une fenêtre d'inspection sur un équipement (table ARP, routage). La zone (5) permet d'ajouter des indications dans le réseau. La zone (4) permet de passer du mode temps réel au mode simulation, et enfin la zone (7) permet la gestion des paquets dans les scénarios de simulation. (Figure 3.2)

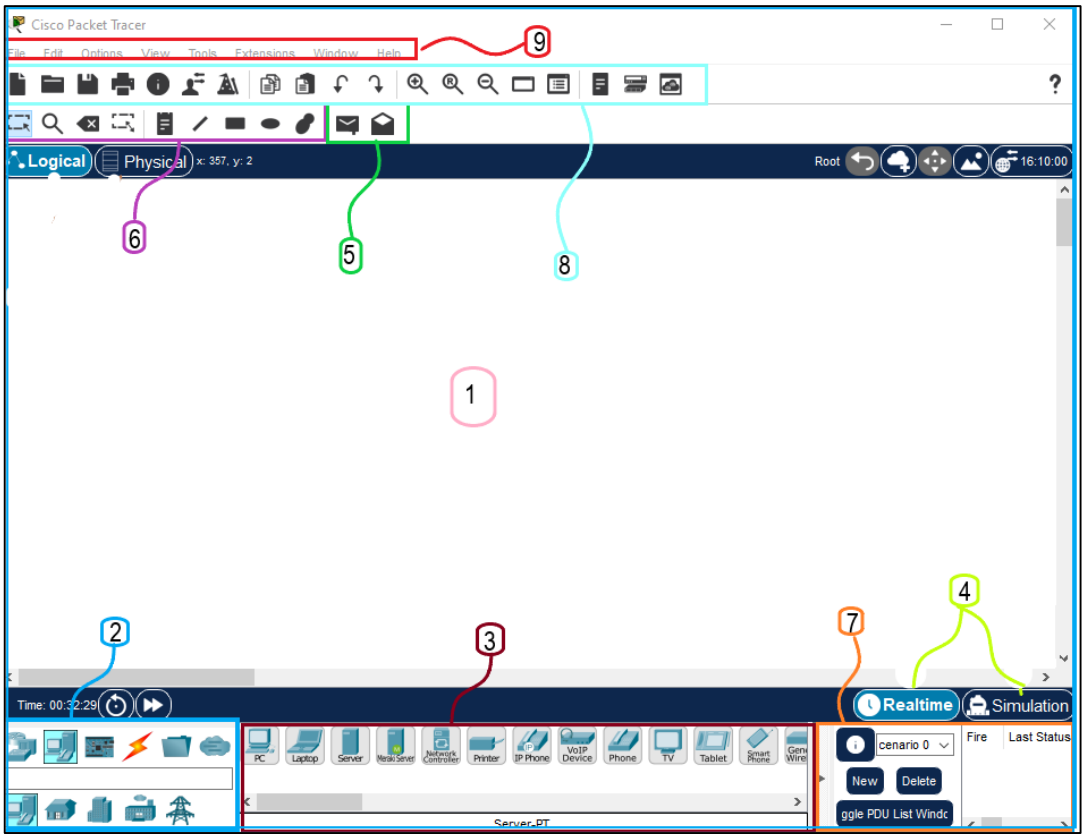

Figure 3.2 : Capture de l'interface Cisco Packet 8.2.1.0118

3.3. Présentation du réseau de l'entreprise

Dans cette partie nous allons présenter le réseau d'entreprise en se concentrant sur la configuration des deux architectures réseau.

3.3.1. Segmentation du réseau en VLAN

Le réseau a été divisé en plusieurs sections, chacune représente un VLAN [26]. Par conséquent, il y'aura naissance de 19 VLANs à savoir :

VLAN		Description
ID	NOM	
10	DRH	Direction Ressource Humaine
11	Direction des Appro	Direction des Approvisionnement
12	DSI	Direction Systèmes Informatique
13	Raff Huile	Raffinerie Huile
14	Raff sucre 3000T	Raffinerie de sucre
15	Division utilités	/
16	Supply-chain	/
17	Unité margarinerie	/
18	Printer	Imprimantes
20	Téléphone	/
21	Voice	/
22	Direction R&D	/
23	Performance industriel	/
24	Unité Cdt Huile	Unité Conditionnement d'Huile
25	Management switch	Switch Management
26	DFC	Direction Finances et Comptabilité
27	Commercial	Direction commercial
28	DG	Direction Générale
29	DQMS	Direction Qualité et Management Système
30	Raff sucre 3500T	Raffinerie de Sucre
31	Cdt sucre	Conditionnement sucre
32	Caméra	/
33	Projets	/
36	Trituration	/

Tableau 3. 1 : Nomination des Vlans de l'entreprise.

3.3.2. Adressage des VLANs

L'administrateur réseau à diviser le réseau en plusieurs VLANs en fonction des différents départements, L'adressage utilisé dans l'architecture est de classe à segmenter en plusieurs sous réseaux 10.10.0.0/24, chaque vlan a une adresse de sous réseau. (Tableau 3.2)

Direction	VLAN	DHCP	Passerelle
DRH	VLAN10	Dynamique	10.10.10.254
Direction des Appro	VLAN11	Dynamique	10.10.11.254
DSI	VLAN12	Dynamique	10.10.12.254
Raff Huile	VLAN13	Dynamique	10.10.13.254
Raff sucre 3000T	VLAN14	Dynamique	10.10.14.254
Division utilités	VLAN15	Dynamique	10.10.15.254
Supply-chain	VLAN16	Dynamique	10.10.16.254
Unité margarinerie	VLAN17	Dynamique	10.10.17.254
Printer	VLAN18	Statique	10.10.18.254
Téléphone	VLAN20	Dynamique	10.10.20.254
Voice	VLAN21	Dynamique	10.10.21.254
Direction R&D	VLAN22	Dynamique	10.10.22.254
Performance industriel	VLAN23	Dynamique	10.10.23.254
Unité Cdt Huile	VLAN24	Dynamique	10.10.24.254
Management switch	VLAN 25	Statique	10.10.25.254
DFC	VLAN26	Dynamique	10.10.26.254
Commercial	VLAN27	Dynamique	10.10.27.254
Direction générale	VLAN28	Dynamique	10.10.28.254
Direction qualité et management système	VLAN29	Dynamique	10.10.29.254
Raff sucre 3500T	VLAN30	Dynamique	10.10.30.254
Cdt sucre	VLAN31	Dynamique	10.10.31.254
Caméra	VLAN32	Statique	10.10.32.254
Projets	VLAN33	Dynamique	10.10.33.254
Trituration	VLAN36	Dynamique	10.10.36.254

Tableau 3.2 : Liste des noms VLANs du réseau et leur plan d'adressage.

3.4. Réseau existant

Dans cette partie nous illustrons brièvement les configurations déjà en place :

- La création des vlan et ses interfaces ;
- La configuration du protocole DHCP ;
- La configuration de lien Trunk **;**
- La configuration de VTP.

3.4.1. Architecture de mise en œuvre

Voici l'architecture du réseau local existant ou nival du CEVITAL. (Figure 3.3)

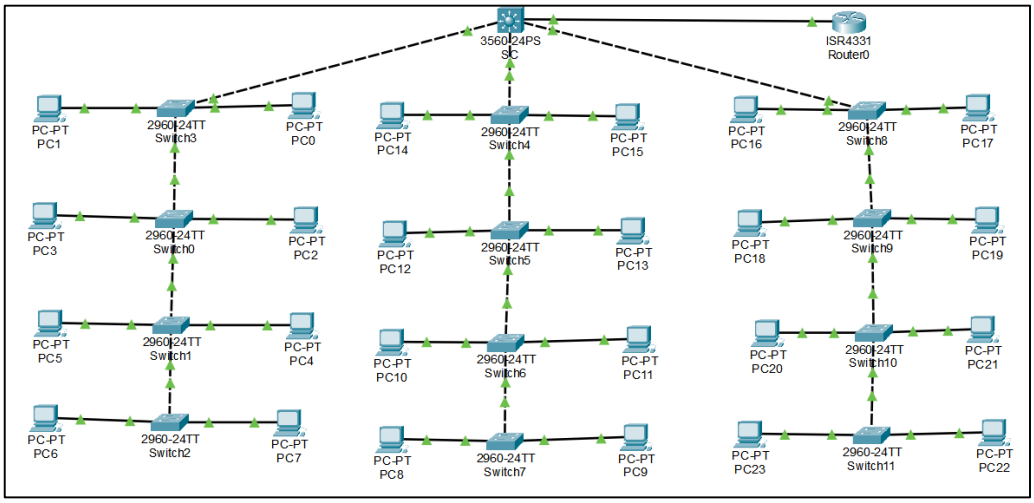

Figure 3.3 : Architecture du réseau local existant.

3.4.2. Configuration des équipements

La configuration des équipements du réseau se fera au niveau des Switches de niveau 2, niveau 3 et des PCs.

Lorsqu'un équipement est ajouté, il est possible de le configurer en cliquant dessus, une fois ajouté dans le réseau. Une nouvelle fenêtre s'ouvre comportant différents onglets : Physical, config, desktop, CLI … etc.

Généralement pour les ordinateurs, on utilise l'onglet config pour configurer l'adresse IP, mais pour le switch, il est préférable d'utiliser l'onglet CLI car il permet de configurer le switch avec les commandes nécessaires.

Un exemple de configuration de chaque équipement sera donné dans la suite de ce chapitre.

I. Switch Cœur

a. Configuration des Hostname et sécurité

Cette configuration consiste à renommer les équipements par des noms significatifs, prenons comme exemple la nomination d'un switch cœur ainsi que le sécuriser avec un mot de passe et le crypter afin de limiter l'accès aux personne étrangères. La figure 3.4 ci-dessous l'explique.

```
Switch(config)#hostname SWC
SWC(config)#enable password cevital
SWC(config)#exit
```

Figure 3.4 : Configuration du Hostname et mot de passe.

b. Création des VLANs

La création des VLANs se fait au niveau du switch Multilayer (SWC) comme le montre (Figure 3.5) suivante sur la création de certains VLANs mis en place.

```
SWC(config)#Vlan 10
SWC(config-vlan)#Name DRH
SWC(config-vlan)#Vlan 11
SWC(config-vlan)#Name Direction-des-Appro
SWC(config-vlan)#Vlan 12
SWC(config-vlan)#Name DSI
SWC(config-vlan)#Vlan 13
SWC(config-vlan)#Name Raff-Huile
SWC(config-vlan)#Vlan 14
SWC(config-vlan)#Name Raff-sucre-3000T
SWC(config-vlan)#Vlan 15
SWC(config-vlan)#Name Division-utilits
SWC(config-vlan)#Vlan 16
SWC(config-vlan)#Name Supply-chain
SWC(config-vlan)#Vlan 17
SWC(config-vlan)#Name Unit-margarinerie
SWC(config-vlan)#Vlan 18
SWC(config-vlan)#Name Printer
SWC(config-vlan)#Vlan 20
SWC(config-vlan)#Name Tlphone
SWC(config-vlan)#Vlan 21
SWC(config-vlan)#Name Voice
SWC(config-vlan)#Vlan 22
SWC(config-vlan)#Name Direction-R&D
```

Figure 3.5 : Création des VLANs.

c. Configuration des interfaces VLANs

La configuration des interfaces virtuelles de VLANs est faite au niveau de Switch Cœur (SWC) en attribuant une adresse IP à chaque interface. (Figure 3.6)

Illustre le principe de configuration de ces interfaces pour quelques VLANs.

```
SWC(config)#Int vlan 10
SWC(config-if)#Ip add 10.10.10.254 255.255.255.0
SWC(config-if)#Int vlan 11
SWC(config-if)#Ip add 10.10.11.254 255.255.255.0
SWC(config-if)#Int vlan 12
SWC(config-if)#Ip add 10.10.12.254 255.255.255.0
SWC(config-if)#Int vlan 13
SWC(config-if)#Ip add 10.10.13.254 255.255.255.0
SWC(config-if)#Int vlan 14
SWC(config-if)#Ip add 10.10.14.254 255.255.255.0
SWC(config-if)#Int vlan 15
SWC(config-if)#Ip add 10.10.15.254 255.255.255.0
SWC(config-if)#Int vlan 16
SWC(config-if)#Ip add 10.10.16.254 255.255.255.0
SWC(config-if)#Int vlan 17
SWC(config-if)#Ip add 10.10.17.254 255.255.255.0
SWC(config-if)#Int vlan 18
SWC(config-if)#Ip add 10.10.18.254 255.255.255.0
SWC(config-if)#Int vlan 20
SWC(config-if)#Ip add 10.10.20.254 255.255.255.0
```

Figure 3.6 : Configuration des interfaces VLANs.

d. Configuration des liens Trunk

Le lien Trunk est un mode d'accès qui permet à plusieurs VLANs de passer par une seule liaison physique. En effet, la plupart des liaisons entre l'ensemble des switches d'accès et le switch cœur sont en mode Trunk, (Figure 3.7) qui montre comme configure.

```
SC#Conf ter
Enter configuration commands, one per line.  End with CNTL/
Z.
SC(config)#int range f0/1-3
SC(config-if-range)#switchport trunk encapsulation dot1q
SC(config-if-range)#switchport mode trunk
SC(config-if-range)#switchport trunk allowed vlan all
SC(config-if-range)#exit
SC(config)#
```

Figure 3.7 : Configuration des interfaces du switch Core en mode Trunk.

e. Configuration du protocole VTP

Le Switch-Cœur (SWC) sera configurer comme VTP serveur, c'est lui qui va gérer l'administration de l'ensemble des VLANs. (Figure 3.8), illustre la configuration du protocole VTP au niveau de SWC.

```
Switch(config)#vtp mode server
Setting device to VTP SERVER mode.
Switch(config)#vtp domain cevital.com
Domain name already set to cevital.com.
Switch(config)#vtp password cevital
Password already set to cevital
Switch(config)#vtp version 2
VTP mode already in V2.
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 3.8 : Configuration du VTP server.

f. Configuration du DHCP

Le DHCP consiste à attribuer dynamiquement les adresses IP aux hôtes connectés, au lieu de les configurer manuellement sur chaque poste utilisateur. (Figure 3.9) et la (Figure 3.10), montre les commandes permettant d'activer ce protocole.

```
SWC(config)#ip dhcp pool VLANDRH
SWC(dhcp-config)#network 10.10.10.0 255.255.255.0
SWC(dhcp-config)#default-router 10.10.10.254
SWC(dhcp-config)#exit
SWC(config)#ip dhcp pool VLANDirection-des-Appro
SWC(dhcp-config)#network 10.10.11.0 255.255.255.0
SWC(dhcp-config)#default-router 10.10.11.254
SWC(dhcp-config)#exit
SWC(config)#ip dhcp pool VLANDSI
SWC(dhcp-config)#network 10.10.12.0 255.255.255.0
SWC(dhcp-config)#default-router 10.10.12.254
SWC(dhcp-config)#exit
SWC(config)#ip dhcp pool VLANRaff-Huile
SWC(dhcp-config)#network 10.10.13.0 255.255.255.0
SWC(dhcp-config)#default-router 10.10.13.254
SWC(dhcp-config)#exit
SWC(config)#ip dhcp pool VLANRaff-sucre-3000T
SWC(dhcp-config)#network 10.10.14.0 255.255.255.0
SWC(dhcp-config)#default-router 10.10.14.254
SWC(dhcp-config)#exit
```

Figure 3.9 : Configuration du DHCP.

```
SWC(config)#ip dhcp excluded-address 10.10.10.254
SWC(config)#ip dhcp excluded-address 10.10.11.254
SWC(config)#ip dhcp excluded-address 10.10.12.254
SWC(config)#ip dhcp excluded-address 10.10.13.254
SWC(config)#ip dhcp excluded-address 10.10.14.254
SWC(config)#ip dhcp excluded-address 10.10.15.254
SWC(config)#ip dhcp excluded-address 10.10.16.254
SWC(config)#ip dhcp excluded-address 10.10.17.254
SWC(config)#ip dhcp excluded-address 10.10.20.254
SWC(config)#ip dhcp excluded-address 10.10.21.254
```

Figure 3.10 : Adresses exclues.

Tout de même, nous pouvons vérifier la configuration de DHCP avec la commande, **show running-config**.

```
SWC#show running-config
Building configuration...

Current configuration : 7269 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname SWC
!
!
enable password cevital
!
!
ip dhcp excluded-address 10.10.10.254
ip dhcp excluded-address 10.10.11.254
ip dhcp excluded-address 10.10.12.254
ip dhcp excluded-address 10.10.13.254
ip dhcp excluded-address 10.10.14.254
ip dhcp excluded-address 10.10.15.254
ip dhcp excluded-address 10.10.16.254
ip dhcp excluded-address 10.10.17.254
ip dhcp excluded-address 10.10.20.254
ip dhcp excluded-address 10.10.21.254
ip dhcp excluded-address 10.10.22.254
ip dhcp excluded-address 10.10.23.254
ip dhcp excluded-address 10.10.24.254
ip dhcp excluded-address 10.10.26.254
ip dhcp excluded-address 10.10.27.254
ip dhcp excluded-address 10.10.28.254
ip dhcp excluded-address 10.10.29.254
ip dhcp excluded-address 10.10.30.254
ip dhcp excluded-address 10.10.31.254
ip dhcp excluded-address 10.10.33.254
ip dhcp excluded-address 10.10.36.254
ip dhcp pool VLANDRH
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.254
ip dhcp pool VLANDirection-des-Appro
 network 10.10.11.0 255.255.255.0
 default-router 10.10.11.254
ip dhcp pool VLANDSI
 network 10.10.12.0 255.255.255.0
 default-router 10.10.12.254
ip dhcp pool VLANRaff-Huile
 network 10.10.13.0 255.255.255.0
 default-router 10.10.13.254
ip dhcp pool VLANRaff-sucre-3000T
 network 10.10.14.0 255.255.255.0
 default-router 10.10.14.254
ip dhcp pool VLANDivision-utilits
 network 10.10.15.0 255.255.255.0
 default-router 10.10.15.254
ip dhcp pool VLANSupply-chain
 network 10.10.16.0 255.255.255.0
 default-router 10.10.16.254
ip dhcp pool VLANUnit-margarinerie
 network 10.10.17.0 255.255.255.0
 default-router 10.10.17.254
ip dhcp pool VLANTlphone
 network 10.10.20.0 255.255.255.0
 default-router 10.10.20.254
ip dhcp pool VLANVoice
 network 10.10.21.0 255.255.255.0
 default-router 10.10.21.254
ip dhcp pool VLANDirection-R&D
 network 10.10.22.0 255.255.255.0
 default-router 10.10.22.254
ip dhcp pool VLANPerformance-industriel
 network 10.10.23.0 255.255.255.0
 default-router 10.10.23.254
ip dhcp pool VLANUnit-Cdt-Huile
 network 10.10.24.0 255.255.255.0
 default-router 10.10.24.254
```

Figure 3.11 : Vérification de l'activation du DHCP.

g. Configuration du protocole STP

Le Root Bridge est en quelque sorte le chef de la topologie Spanning Tree. Une fois le Root Bridge élu, les switchs vont rechercher le meilleur chemin vers le Root Bridge, les switches vont chercher le port avec la métrique la plus faible vers le Root Bridge, puis ils vont couper les autres ports.

On va configurer le STP au niveau de Le Switch-Cœur (SWC). (Figure 3.12)

```
SC#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SC(config)#spanning-tree vlan 10-36 root primary
SC(config)#exit
SC#
%SYS-5-CONFIG_I: Configured from console by console
```

Figure 3.12 : Configuration du protocole STP.

h. Assigne d'une adresse IP et activation du routage ainsi l'OSPF

OSPF est meilleur pour la répartition de charge et aussi son rôle de choisir le meilleur chemin basé sur le coût (la bande passante inversée). Cette métrique peut être définie manuellement sur les interfaces. (Figure 3.13), illustre la configuration du protocole OSPF.

```
SWC(config)#int f0/4
SWC(config-if)#no switchport
SWC(config-if)#ip add 192.168.16.2 255.255.255.252
SWC(config-if)#exit
SWC(config)#ip routing
SWC(config)#router ospf 1
SWC(config-router)#network 10.10.10.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.11.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.12.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.13.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.14.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.15.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.16.0 0.0.0.255 area 0
SWC(config-router)#network 10.10.16.0 0.0.0.255 area 0
```

Figure 3.13 : Configuration du protocole OSPF.

II. Switch accès

a. Configuration des ports en mode trunk et en mode accès

Cette opération se fait au niveau des switches d'accès, chaque port appartiendra à un VLAN donné. Les commandes suivantes nous permettent d'associer les ports aux VLANs en mode Access, et le mode trunk est utilisé dans le cas ou plusieurs vlans doivent circuler sur un même lien. (Figure 3.14)

```
SWAC(config)#int range f0/3-4
SWAC(config-if-range)#switchport mode trunk
SWAC(config-if-range)#switchport trunk allowed vlan all
SWAC(config-if-range)#exit
```

```
SWAC(config)#int f0/1
SWAC(config-if)#switchport mode access
SWAC(config-if)#switchport access vlan 10
SWAC(config-if)#no sh
SWAC(config-if)# int f0/2
SWAC(config-if)#switchport mode access
SWAC(config-if)#switchport access vlan 11
SWAC(config-if)#no sh
SWAC(config-if)#exit
```

Figure 3.14 : Configuration des interfaces du switch en mode et Access et en mode trunk.

b. Configuration du protocole VTP sur le switch d'accès

Le switch d'accès sera configuré comme VTP client, tel qu'il est donné par (Figure 3.15).

```
SWAC(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWAC(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
SWAC(config)#vtp password cevital
Setting device VLAN database password to cevital
SWAC(config)#vtp version 2
Cannot modify version in VTP client mode
```

Figure 3.15: Configuration du VTP client.

III. Router

Lors de la configuration au niveau du retour, une adresse IP doit être attribuée au niveau de son interface ainsi que le protocole OSPF devait être configuré. (Figure 3.16)

```
Router(config)#int g0/0/0
Router(config-if)#ip add 192.168.16.1 255.255.255.252
Router(config-if)#no sh
Router(config-if)#exit
Router(config)#ip routing
Router(config)#router ospf 1
Router(config-router)#network 192.168.16.0  0.0.0.3 area 0
```

Figure 3.16 : Configuration du protocole OSPF.

3.4.3. Vérification des adressages IP attribuées par le DHCP

La vérification s'effectue pour tous les ordinateurs, (Figure 3.17) ci-dessous nous montre un exemple :

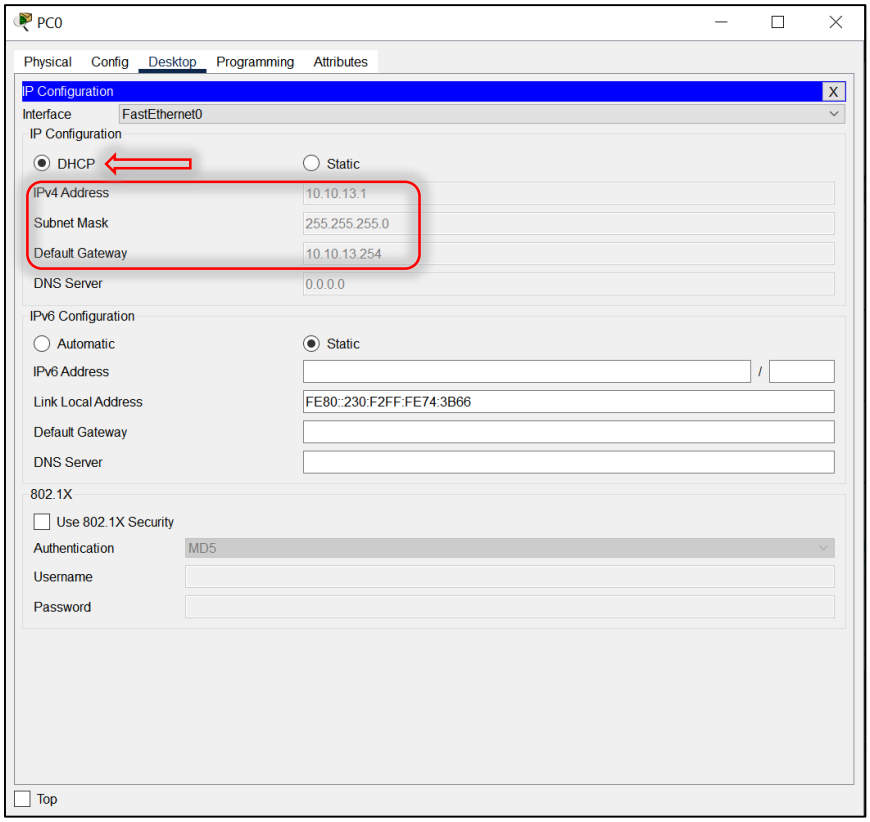

Figure 3.17 : Adressage IP attribué automatiquement.

3.4.4. Vérification de la connectivité

a. Test inter-VLANs

Ce test consiste d'envoyer des paquets qui appartiennent à des VLANs différents. Pour tester la connectivité, nous pouvons envoyer un Ping entre le PC1 d'adresse : 10.10.11.1 et le PC 4 avec l'adresse : 10.10.15.1 (Figure 3.18)

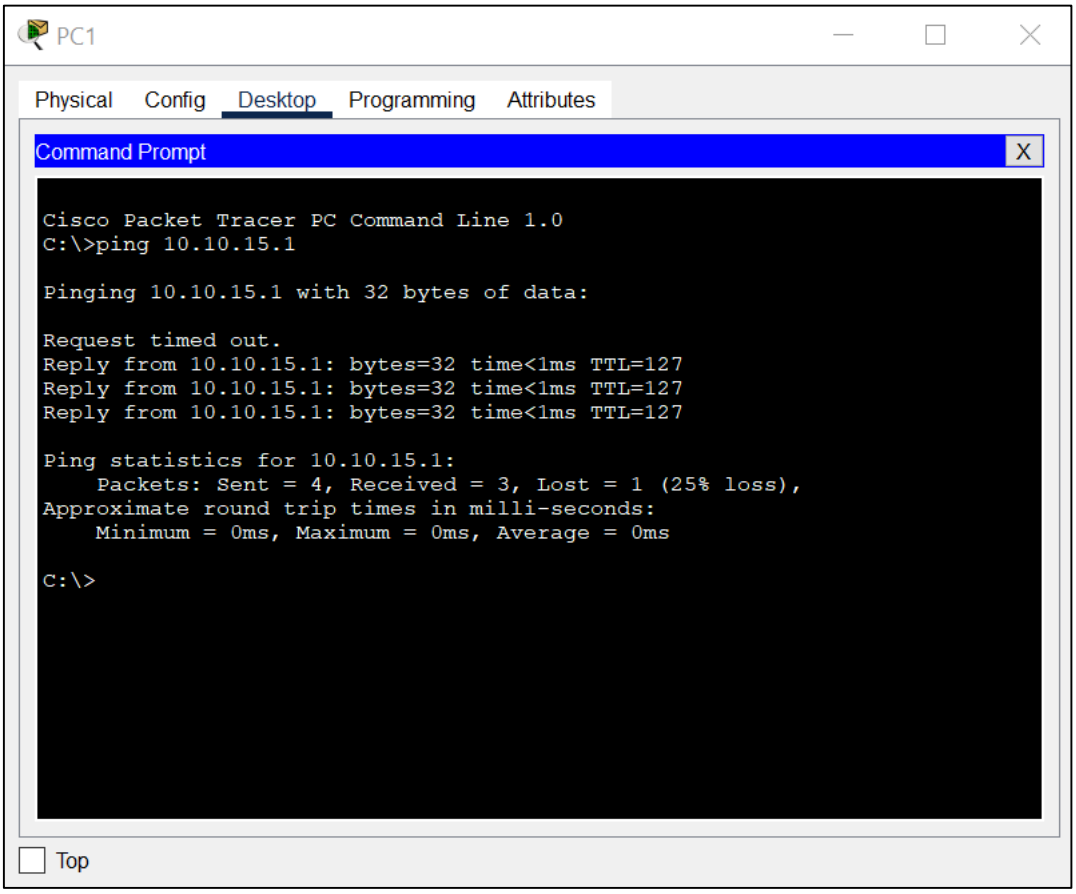

Figure 3.18 : Test entre le PC 1 et le PC 4.

b. Test intra-VLANs

Nous avons pris un PC du VLAN 10 et nous allons faire un Ping continu vers un autre PC du même (VLAN 10) après on va simuler une panne au niveau de l'interface, et cette panne consiste à simuler la rupture de la liaison entre le switch d'accès et le switch de cœur.

Premièrement nous effectuons un autre Ping entre l'adresse IP du PC8. Est : 10.10.10.2 et l'adresse IP du PC 9 est : 10.10.10.1, En premier lieu nous avons constaté que le ping fonctionne parfaitement et sans problème, comme la figure 3.19 l'explique.

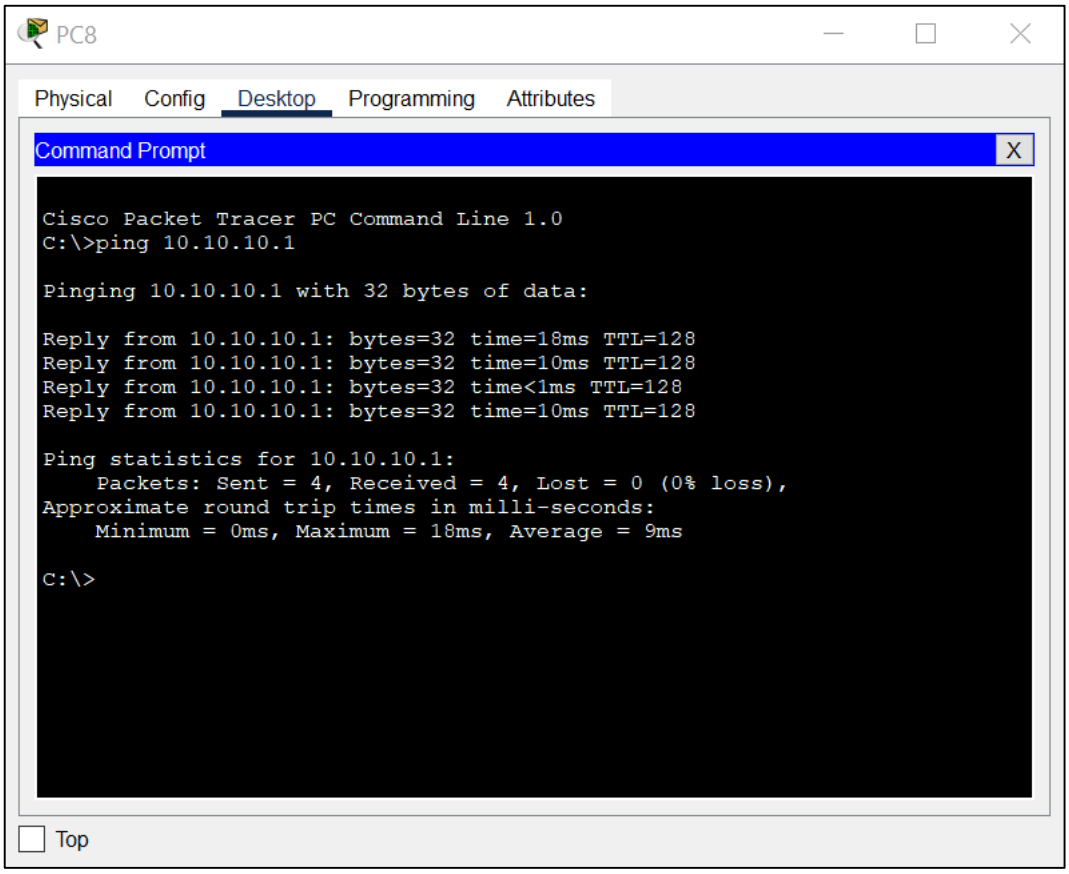

Figure 3.19 : Test entre le PC 8 et le PC 9.

En deuxième lieu nous allons simuler une panne comme la figure 3.20 l'explique nous allons constater directement que le ping s'arrête.

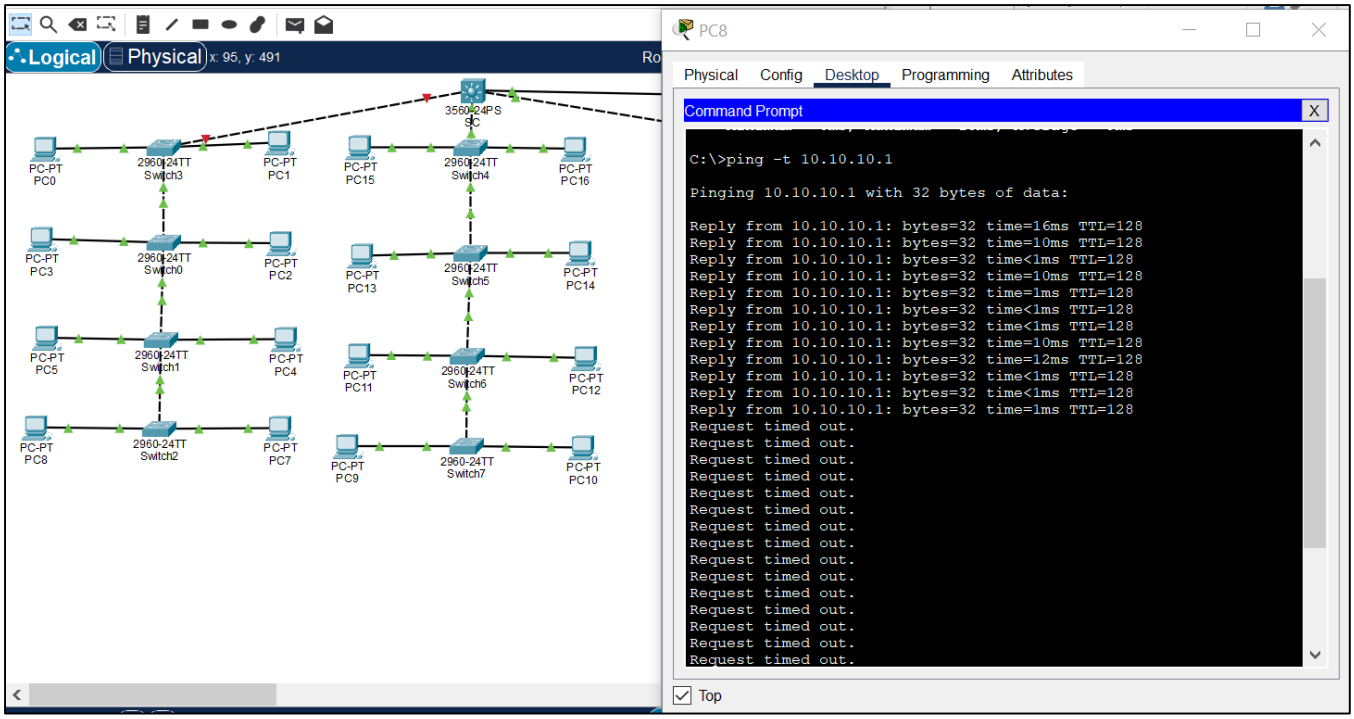

Figure 3.20 : Test de panne.

D'après ces tests, on remarque qu'un dysfonctionnement a eu lieu suite à l'absence de la couche de distribution au sein de l'architecture du groupe CEVITAL, de ce fait, nous avons proposé une architecture plus potentielle qui répond à ce point faible.

3.5. Nouvelle architecture proposée au réseau CEVITAL

Dans cette partie, nous allons décortiquer la nouvelle topologie globale de l'entreprise CEVITAL de Bejaia.

3.5.1. Amélioration de l'architecture

Afin de tester notre solution choisie nous étions dans l'obligation de porter des modifications matérielles sur l'ancienne architecture et ceci en ajoutant deux backbones pour la partie Coeur celle qui reliera le réseau vers les autres sites et comprendra en elle avec la partie distribution le protocole de routage choisi (OSPF), nous avons aussi mis en œuvre deux backbones dans la partie distribution afin de configurer le protocole de la haute disponibilité HSRP sur ces deux backbones qui eux même sont reliés en EtherChannel pour une meilleure connectivité et un débit plus haut. Afin que cette architecture soit hautement disponible, on doit aussi brancher tous les switches d'accès au premier backbone que nous avons nommé SWD1 ainsi qu'au deuxième que nous avons nommé SWD2.

3.5.2. Nouvelle architecture du réseau CEVITAL

Voici donc le modèle d'architecture adopté pour le réseau de CEVITAL , il se décompose en trois couches, une couche Cœur de deux switches niveau 3, une couche distribution avec deux switches aussi niveau 3, une couche accès là ou tous les switches d'accès y sont, un protocole de haute disponibilité HSRP sera configuré à la partie distribution qui assure la continuité de service, un protocole OSPF sera configuré entre la partie Cœur et distribution qui vas assurer le bon routage du réseau, et tout ça sera un mi- travaille sans que les périphériques de la couche accès soient interconnectés aux deux switches en redondance pour qu'ils assurent la haute disponibilité dans le cas où l'un des switches de distribution subit un dysfonctionnement ou une coupure d'un des liens d'interconnexion.

La figure 3.21, illustre la nouvelle architecture mise en place

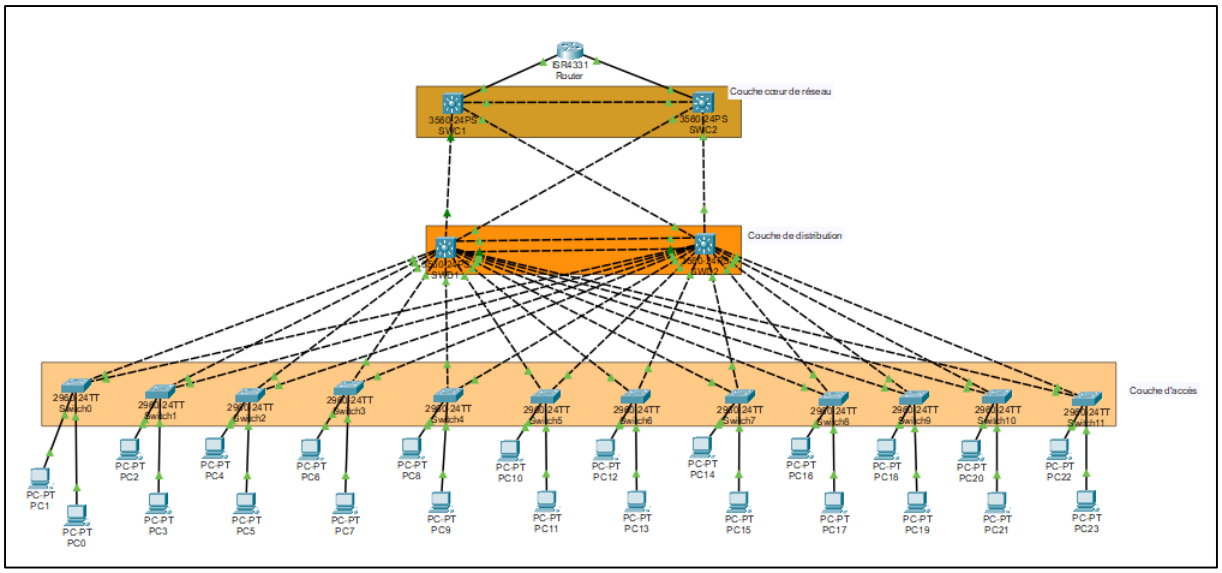

Figure 3.21 : Modèle d'architecture réseau CEVITAL.

3.5.3. Présentation des équipements utilisés

Au sein de CEVITAL, les différents équipements utilisés sont tous de même marque, ce qui évite tout problème de compatibilité entre les protocoles propriétaires. Les équipements réseau sont illustrés dans le tableau 3.3:

Equipement du modèle type	Nombre	Type et marque de Switch
Switch Coeur	02	Cisco Catalyst C6807-XL
Switch Distribution	02	Cisco Catalyst C3850-24S
Switch d'Accès	24	Cisco Catalyst C2960

Tableau 3.3 : Représentation de la liste des équipements utilisés.

3.5.4. Désignation des interfaces

Le tableau suivant (Tableau 3.4) indique la répartition des interfaces sur les différents équipements.

Appareil Local	**Appareil distant**	**Interface(s) locale(s)**	**Interface(s) distante(s)**
Router	SWC1	Gig0/0	Fa0/4
Router	SWC2	Gig0/1	Fa0/4
SWC1	SWC2	Fa0/3	Fa0/3
SWC1	SWD1	Fa0/1	Fa0/14
SWC1	SWD2	Fa0/2	Fa0/13
SWC2	SWD1	Fa0/2	Fa0/13
SWC2	SWD2	Fa0/1	Fa0/14
SWD1	SWC1	F0/14	Fa0/1
SWD1	SWC2	F0/13	Fa0/2
SWD1	SWD2	Gig0/1-Gig0/2	Gig0/2-Gig0/1
SWD1	DRH	Fa0/1	F0/3
SWD1	Direction des Appro	F0/5	F0/3
SWD1	DSI	F0/6	F0/3
SWD1	Raff Huile	F0/7	F0/3
SWD1	Raff sucre 3000T	F0/8	F0/3
SWD1	Division utilités	F0/9	F0/3
SWD1	Supply-chain	F0/10	F0/3
SWD1	Unité margarinerie	F0/11	F0/3
SWD1	Printer	F0/12	F0/3
SWD1	Téléphone	F0/13	F0/3

SWD1	Voice	F0/14	F0/3
SWD1	Direction R&D	F0/15	F0/3
SWD1	Performance industriel	F0/16	F0/3
SWD2	Unité Cdt Huile	Fa0/1	F0/4
SWD2	Management switch	F0/2	F0/4
SWD2	DFC	F0/3	F0/4
SWD2	Commercial	F0/4	F0/4
SWD2	Direction générale	F0/5	F0/4
SWD2	Direction qualité et management système	F0/6	F0/4
SWD2	Raff sucre 3500T	F0/7	F0/4
SWD2	Cdt sucre	F0/8	F0/4
SWD2	Caméra	F0/9	F0/4
SWD2	Projets	F0/10	F0/4
SWD2	Trituration	F0/11	F0/4

Tableau 3.4 : Désignation des interfaces des différents équipements.

3.5.4. Configuration des équipements

Nous avons quatre (04) switches de niveau 3 qui sont interconnectés entre eux, avec deux de la couche Coeur et deux autres pour la couche de distribution, ainsi que dix (10) switches de niveau 2 pour assurer la couche d'accès, et des PCs hôtes répartis sur les différentes directions.

Les premières étapes de la configuration sont similaires à la partie précédente. Toutefois, quelques exemples de configuration de chaque équipement seront ajoutés pour bien montrer les taches réalisées.

3.5.5. Configuration de base

La même configuration de base sera effectuée pour le routeur, les Switches Cœurs, les Switches de distribution SWD1 et SWD2 ainsi que les Switches d'accès.

Comme premier pas dans notre travail, nous allons changer le nom de chaque équipement en donnant des noms significatifs et facile à reconnaitre. Voici un exemple illustratif la nomination de l'un des Switches de distribution SWD1.

```
Switch(config)#
Switch(config)#hostname SWD1
```

Figure 3.22 : Exemple de configuration de Hostname.

Nous avons attribué un mot de passe chiffré « Cevital » pour l'accès au mode privilégié.

```
SWD1(config)#enable password cevital
```

Figure 3.23 : Sécurisation en mode privilégié.

Les mots de passe apparaissent en clair lors de l'affichage du fichier de configuration. Nous allons donc activer le service **password-encryption** afin de sécuriser les équipements.

```
SWD1(config)#service password-encryption
SWD1(config)#
```

Figure 3. 24 : Exemple de sécurisation du SWD1.

Pour Vérifier les configurations de base pratiquées on tapera la commande show running-config, la figure ci-dessous :

```
SWD2>en
Password:                    Mot de passe du mode privilégie.
SWD2#show running-config
Building configuration...

Current configuration : 11392 bytes
!
version 12.2(37)SE1
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname SWD2                Nomination des switch distridution.
!
!
enable password 7 08224958000D041B   Securitation des MDP.
!
```

Figure 3.25 : Vérification des configurations de base sur SWD2.

3.5.6. Configuration des VLANs

1. Création des VLANs

La création des VLANs est faite au niveau des switchs de distribution comme le montre la figure 3.26.

```
SWD1(config)#Vlan 10
SWD1(config-vlan)#Name DRH
SWD1(config-vlan)#Vlan 11
SWD1(config-vlan)#Name Direction-des-Appro
SWD1(config-vlan)#Vlan 12
SWD1(config-vlan)#Name DSI
SWD1(config-vlan)#Vlan 13
SWD1(config-vlan)#Name Raff-Huile
SWD1(config-vlan)#Vlan 14
SWD1(config-vlan)#Name Raff-sucre-3000T
SWD1(config-vlan)#Vlan 15
SWD1(config-vlan)#Name Division-utilits
SWD1(config-vlan)#Vlan 16
SWD1(config-vlan)#Name Supply-chain
SWD1(config-vlan)#Vlan 17
SWD1(config-vlan)#Name Unit-margarinerie
SWD1(config-vlan)#Vlan 18
SWD1(config-vlan)#Name Printer
```

Figure 3.26 : Création des VLANs SWD1.

Ensuite, nous allons vérifier leurs créations avec la commande **show vlan brief**.

```
SWD1#show vlan brief

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/15, Fa0/16, Fa0/17, Fa0/18
                                                   Fa0/19, Fa0/20, Fa0/21, Fa0/22
                                                   Fa0/23, Fa0/24
10   DRH                                 active
11   Direction-des-Appro                active
12   DSI                                 active
13   Raff-Huile                          active
14   Raff-sucre-3000T                    active
15   Division-utilits                    active
16   Supply-chain                        active
17   Unit-margarinerie                   active
18   Printer                             active
20   Tlphone                             active
21   Voice                               active
22   Direction-R&D                       active
23   Performance-industriel              active
24   Unit-Cdt-Huile                      active
25   Management-switch                   active
26   DFC                                 active
27   Commercial                          active
28   Direction-gnrale                    active
29   Direction-qualit-et-management-systme active
30   Raff-sucre-3500T                    active
31   Cdt-sucre                           active
32   Camra                               active
33   Projets                             active
36   Trituration                         active
1002 fddi-default                        active
1003 token-ring-default                  active
 --More--
```

Figure 3.27 : Vérification des VLANs SWD1.

2. Configuration de VTP (VLAN Trunking protocol)

Afin de profiter des services VTP, nous allons configurer le switch de distributions SWD1 en mode serveur et lui attribuer un nom de domaine ainsi un mot de passe, le reste des switches en mode client afin que les VLANs se propagent de SWD1 vers les autres switchs.

Pour cela nous allons procéder comme suite :

```
SWD1(config)#vtp mode server
Device mode already VTP SERVER.
SWD1(config)#vtp domain cevital.com
Domain name already set to cevital.com.
SWD1(config)#vtp password cevital
Setting device VLAN database password to cevital
SWD1(config)#vtp version 2
SWD1(config)#exit
```

Figure 3.28 : Configuration du VTP serveur.

```
SWD2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWD2(config)#vtp domain cevital.com
Domain name already set to cevital.com.
SWD2(config)#vtp password cevital
Setting device VLAN database password to cevital
SWD2(config)#vtp version 2
Cannot modify version in VTP client mode
SWD2(config)#exit
```

Figure 3.29 : Configuration du VTP client.

Nous allons vérifier cette configuration avec la commande **show vtp status** :

```
SWD1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 000A.F3A3.9100
Configuration last modified by 10.10.10.252 at 3-1-93 01:18:44
Local updater ID is 10.10.10.252 on interface Vl10 (lowest numbered VLAN
interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 29
Configuration Revision          : 361
MD5 digest                      : 0x39 0xAD 0xB7 0x34 0xE9 0xC3 0x01
0x61
                                  0xB1 0x6E 0x37 0x10 0x9F 0xF2 0xF8
0xFB
```

Figure 3.30 : Vérification de la configuration du VTP serveur.

```
Switch#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 2
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0060.5C8A.5A00
Configuration last modified by 10.10.10.252 at 3-1-93
01:18:44

Feature VLAN :
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 29
Configuration Revision          : 361
MD5 digest                      : 0x39 0xAD 0xB7 0x34
0xE9 0xC3 0x01 0x61
                                  0xB1 0x6E 0x37 0x10
0x9F 0xF2 0xF8 0xFB
```

Figure 3.31 : Vérification de la configuration du VTP client.

3. Configuration des interfaces VLAN

En outre, nous avons configuré les interfaces des switchs de distribution de chaque VLAN, autrement dit, nous allons attribuer une adresse IP pour chaque VLAN sur les deux switches. Cela nous permettra de faire un routage inter-VLAN, mais ce dernier ne sera pas fonctionnel avant son activation avec la commande ip routing. Durant cette étape, nous allons attribuer les adresses aux interfaces virtuelles des switchs de distribution, ou le 252 sera sur la partie machine de chaque

VLAN de SWD1 (Figure 3.32). Tandis que, sur le SWD2, nous allons attribuer le 253 sur la partie machine de chaque VLAN (Figure 3.33), est donnée pour bien illustrer cette étape.

Direction	VLAN	DHCP	Root	IP SWD1	IP SWD2	Passerelle
DRH	VLAN10	Dynamique	SWD1	10.10.10.252	10.10.10.253	10.10.10.254
Direction des Appro	VLAN11	Dynamique	SWD1	10.10.11.252	10.10.11.253	10.10.11.254
DSI	VLAN12	Dynamique	SWD1	10.10.12.252	10.10.12.253	10.10.12.254
Raff Huile	VLAN13	Dynamique	SWD1	10.10.13.252	10.10.13.253	10.10.13.254
Raff sucre 3000T	VLAN14	Dynamique	SWD1	10.10.14.252	10.10.14.253	10.10.14.254
Division utilités	VLAN15	Dynamique	SWD1	10.10.15.252	10.10.15.253	10.10.15.254
Supply-chain	VLAN16	Dynamique	SWD1	10.10.16.252	10.10.16.253	10.10.16.254
Unité margarinerie	VLAN17	Dynamique	SWD1	10.10.17.252	10.10.17.253	10.10.17.254
Printer	VLAN18	Statique	SWD1	10.10.18.252	10.10.18.253	10.10.18.254
Téléphone	VLAN20	Dynamique	SWD1	10.10.20.252	10.10.20.253	10.10.20.254
Voice	VLAN21	Dynamique	SWD1	10.10.21.252	10.10.21.253	10.10.21.254
Direction R&D	VLAN22	Dynamique	SWD1	10.10.22.252	10.10.22.253	10.10.22.254
Performance industriel	VLAN23	Dynamique	SWD2	10.10.23.252	10.10.23.253	10.10.23.254
Unité Cdt Huile	VLAN24	Dynamique	SWD2	10.10.24.252	10.10.24.253	10.10.24.254
Management switch	VLAN 25	Statique	SWD2	10.10.25.252	10.10.25.253	10.10.25.254
DFC	VLAN26	Dynamique	SWD2	10.10.26.252	10.10.26.253	10.10.26.254
Commercial	VLAN27	Dynamique	SWD2	10.10.27.252	10.10.27.253	10.10.27.254
Direction générale	VLAN28	Dynamique	SWD2	10.10.28.252	10.10.28.253	10.10.28.254
Direction qualité et management système	VLAN29	Dynamique	SWD2	10.10.29.252	10.10.29.253	10.10.29.254
Raff sucre 3500T	VLAN30	Dynamique	SWD2	10.10.30.252	10.10.30.253	10.10.30.254
Cdt sucre	VLAN31	Dynamique	SWD2	10.10.31.252	10.10.31.253	10.10.31.254
Caméra	VLAN32	Statique	SWD2	10.10.32.252	10.10.32.253	10.10.32.254
Projets	VLAN33	Dynamique	SWD2	10.10.33.252	10.10.33.253	10.10.33.254
Trituration	VLAN36	Dynamique	SWD2	10.10.36.252	10.10.36.253	10.10.36.254

Tableau 3.5 : Plan d'adressage pour la nouvelle topologie.

```
SWD1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#Int vlan 10
SWD1(config-if)#Ip add 10.10.10.252 255.255.255.0
SWD1(config-if)#Int vlan 11
SWD1(config-if)#Ip add 10.10.11.252 255.255.255.0
SWD1(config-if)#Int vlan 12
SWD1(config-if)#Ip add 10.10.12.252 255.255.255.0
SWD1(config-if)#Int vlan 13
SWD1(config-if)#Ip add 10.10.13.252 255.255.255.0
SWD1(config-if)#Int vlan 14
SWD1(config-if)#Ip add 10.10.14.252 255.255.255.0
SWD1(config-if)#Int vlan 15
SWD1(config-if)#Ip add 10.10.15.252 255.255.255.0
SWD1(config-if)#Int vlan 16
SWD1(config-if)#Ip add 10.10.16.252 255.255.255.0
SWD1(config-if)#Int vlan 17
SWD1(config-if)#Ip add 10.10.17.252 255.255.255.0
SWD1(config-if)#Int vlan 18
SWD1(config-if)#Ip add 10.10.18.252 255.255.255.0
SWD1(config-if)#Int vlan 20
SWD1(config-if)#Ip add 10.10.20.252 255.255.255.0
SWD1(config-if)#Int vlan 21
SWD1(config-if)#Ip add 10.10.21.252 255.255.255.0
SWD1(config-if)#Int vlan 22
SWD1(config-if)#Ip add 10.10.22.252 255.255.255.0
SWD1(config-if)#Int vlan 23
SWD1(config-if)#Ip add 10.10.23.252 255.255.255.0
SWD1(config-if)#Int vlan 24
SWD1(config-if)#Ip add 10.10.24.252 255.255.255.0
SWD1(config-if)#Int vlan 25
SWD1(config-if)#Ip add 10.10.25.252 255.255.255.0
SWD1(config-if)#Int vlan 26
SWD1(config-if)#Ip add 10.10.26.252 255.255.255.0
SWD1(config-if)#Int vlan 27
SWD1(config-if)#Ip add 10.10.27.252 255.255.255.0
SWD1(config-if)#Int vlan 28
SWD1(config-if)#Ip add 10.10.28.252 255.255.255.0
SWD1(config-if)#Int vlan 29
SWD1(config-if)#Ip add 10.10.29.252 255.255.255.0
SWD1(config-if)#Int vlan 30
SWD1(config-if)#Ip add 10.10.30.252 255.255.255.0
```

```
SWD1(config-if)#Int vlan 31
SWD1(config-if)#Ip add 10.10.31.252 255.255.255.0
SWD1(config-if)#Int vlan 32
SWD1(config-if)#Ip add 10.10.32.252 255.255.255.0
SWD1(config-if)#Int vlan 33
SWD1(config-if)#Ip add 10.10.33.252 255.255.255.0
SWD1(config-if)#Int vlan 36
SWD1(config-if)#Ip add 10.10.36.252 255.255.255.0
SWD1(config-if)#Exit
```

Figure 3.32: Configuration des interfaces VLANs sur SWD1.

```
SWD2(config)#Int vlan 10
SWD2(config-if)#Ip add 10.10.10.253 255.255.255.0
SWD2(config-if)#Int vlan 11
SWD2(config-if)#Ip add 10.10.11.253 255.255.255.0
SWD2(config-if)#Int vlan 12
SWD2(config-if)#Ip add 10.10.12.253 255.255.255.0
SWD2(config-if)#Int vlan 13
SWD2(config-if)#Ip add 10.10.13.253 255.255.255.0
SWD2(config-if)#Int vlan 14
SWD2(config-if)#Ip add 10.10.14.253 255.255.255.0
SWD2(config-if)#Int vlan 15
SWD2(config-if)#Ip add 10.10.15.253 255.255.255.0
SWD2(config-if)#Int vlan 16
SWD2(config-if)#Ip add 10.10.16.253 255.255.255.0
SWD2(config-if)#Int vlan 17
SWD2(config-if)#Ip add 10.10.17.253 255.255.255.0
SWD2(config-if)#Int vlan 18
SWD2(config-if)#Ip add 10.10.18.253 255.255.255.0
SWD2(config-if)#Int vlan 20
SWD2(config-if)#Ip add 10.10.20.253 255.255.255.0
SWD2(config-if)#Int vlan 21
SWD2(config-if)#Ip add 10.10.21.253 255.255.255.0
SWD2(config-if)#Int vlan 22
SWD2(config-if)#Ip add 10.10.22.253 255.255.255.0
SWD2(config-if)#Int vlan 23
SWD2(config-if)#Ip add 10.10.23.253 255.255.255.0
SWD2(config-if)#Int vlan 24
SWD2(config-if)#Ip add 10.10.24.253 255.255.255.0
SWD2(config-if)#Int vlan 25
SWD2(config-if)#Ip add 10.10.25.253 255.255.255.0
SWD2(config-if)#Int vlan 26
SWD2(config-if)#Ip add 10.10.26.253 255.255.255.0
SWD2(config-if)#Int vlan 27
SWD2(config-if)#Ip add 10.10.27.253 255.255.255.0
SWD2(config-if)#Int vlan 28
SWD2(config-if)#Ip add 10.10.28.253 255.255.255.0
SWD2(config-if)#Int vlan 29
SWD2(config-if)#Ip add 10.10.29.253 255.255.255.0
SWD2(config-if)#Int vlan 30
SWD2(config-if)#Ip add 10.10.30.253 255.255.255.0
```

```
SWD2(config-if)#Int vlan 30
SWD2(config-if)#Ip add 10.10.30.253 255.255.255.0
SWD2(config-if)#Int vlan 31
SWD2(config-if)#Ip add 10.10.31.253 255.255.255.0
SWD2(config-if)#Int vlan 32
SWD2(config-if)#Ip add 10.10.32.253 255.255.255.0
SWD2(config-if)#Int vlan 33
SWD2(config-if)#Ip add 10.10.33.253 255.255.255.0
SWD2(config-if)#Int vlan 36
SWD2(config-if)#Ip add 10.10.36.253 255.255.255.0
SWD2(config-if)#Exit
```

Figure 3.33 : Configuration des interfaces VLANs sur SWD2.

Après avoir configuré les interfaces des switches de chaque VLAN, nous allons vérifier avec la commande, **show running-config**, les configurations mises en place.

```
interface Vlan10
 mac-address 0040.0b1d.3801
 ip address 10.10.10.252 255.255.255.0
```

Figure 3.34 : Vérification des interfaces VLANs de SWD1.

3.5.7. Configuration des interfaces Mode TRUNK

Le mode trunk est utilisé dans le cas ou plusieurs vlans doivent circuler sur un même lien. Nous allons associer des ports à ces VLANs en mode Trunk :

- ✓ Sur le Switch distribution SWD2

```
SWD2#Conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SWD2(config)#int range f0/1-12
SWD2(config-if-range)#switchport trunk encapsulation dot1q
SWD2(config-if-range)#switchport mode trunk
SWD2(config-if-range)#switchport trunk allowed vlan all
SWD2(config-if-range)#exit
SWD2(config)#int range g0/1-2
SWD2(config-if-range)#switchport trunk encapsulation dot1q
SWD2(config-if-range)#switchport mode trunk
SWD2(config-if-range)#switchport trunk allowed vlan all
SWD2(config-if-range)#exit
```

Figure 3.35 : Configuration des liens Trunk sur SWD2.

Nous allons vérifier avec la commande **show running-config** :

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface GigabitEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-group 1 mode on
!
interface GigabitEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

Figure 3.36 : Vérification des liens trunks sur SWD2.

- ✓ Sur le Switch distribution SWD1

```
SWD1#Conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#int range f0/1-12
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#switchport trunk allowed vlan all
SWD1(config-if-range)#exit
SWD1(config)#int range g0/1-2
SWD1(config-if-range)#switchport trunk encapsulation dot1q
SWD1(config-if-range)#switchport mode trunk
SWD1(config-if-range)#switchport trunk allowed vlan all
SWD1(config-if-range)#exit
```

Figure 3.37 : Configuration des liens Trunk sur SWD1.

✓ Sur les Switch niveau accès

```
SWac#Conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SWac(config)#int range f0/3-4
SWac(config-if-range)#switchport mode trunk
SWac(config-if-range)#switchport trunk allowed vlan all
SWac(config-if-range)#exit
```

Figure 3.38 : Exemple de configuration des liens trunk sur DRH.

3.5.8. Configuration Dynamic Host Configuration Protocol DHCP

Afin de faciliter la gestion et l'attribution des adresses IP pour chaque hôte du réseau, nous allons utiliser le protocole DHCP, ce dernier permet de configurer les paramètres de chaque hôte et le laissera profiter d'un adressage dynamique. La configuration se fera au niveau des switches de distribution SWD1 et SWD2.

Afin de réussir ce protocole, et de permettre aux deux Switches de distribution d'attribuer des adresses au même temps sans conflit, nous allons exclure les adresses de 128 à 254 sur le SWD1, c'est-à-dire le SWD1 va attribuer les adresses allant de 1 jusqu'à 127.

```
SWD1(config)#Ip dhcp excluded-address 10.30.10.128 10.30.10.254
SWD1(config)#Ip dhcp excluded-address 10.30.11.128 10.30.11.254
SWD1(config)#Ip dhcp excluded-address 10.30.12.128 10.30.12.254
SWD1(config)#Ip dhcp excluded-address 10.30.13.128 10.30.13.254
SWD1(config)#Ip dhcp excluded-address 10.30.14.128 10.30.14.254
SWD1(config)#Ip dhcp excluded-address 10.30.15.128 10.30.15.254
SWD1(config)#Ip dhcp excluded-address 10.30.16.128 10.30.16.254
SWD1(config)#Ip dhcp excluded-address 10.30.17.128 10.30.17.254
SWD1(config)#Ip dhcp excluded-address 10.30.18.128 10.30.18.254
SWD1(config)#Ip dhcp excluded-address 10.30.20.128 10.30.20.254
SWD1(config)#Ip dhcp excluded-address 10.30.21.128 10.30.21.254
SWD1(config)#Ip dhcp excluded-address 10.30.22.128 10.30.22.254
SWD1(config)#Ip dhcp excluded-address 10.30.23.128 10.30.23.254
SWD1(config)#Ip dhcp excluded-address 10.30.24.128 10.30.24.254
SWD1(config)#Ip dhcp excluded-address 10.30.25.128 10.30.25.254
SWD1(config)#Ip dhcp excluded-address 10.30.26.128 10.30.26.254
SWD1(config)#Ip dhcp excluded-address 10.30.27.128 10.30.27.254
SWD1(config)#Ip dhcp excluded-address 10.30.28.128 10.30.28.254
SWD1(config)#Ip dhcp excluded-address 10.30.29.128 10.30.29.254
SWD1(config)#Ip dhcp excluded-address 10.30.30.128 10.30.30.254
SWD1(config)#Ip dhcp excluded-address 10.30.31.128 10.30.31.254
SWD1(config)#Ip dhcp excluded-address 10.30.32.128 10.30.32.254
SWD1(config)#Ip dhcp excluded-address 10.30.33.128 10.30.33.254
SWD1(config)#Ip dhcp excluded-address 10.30.36.128 10.30.36.254
```

Figure 3.39 : Les adresses exclues 128-254 sur SWD1**.**

Aussi nous allons exclure les adresses 1 à 127 et 252 à 254 sur SWD2 c'est-à-dire le SWD2 va attribuer les adresses allant de 128 à 251.

```
SWD2(config)#Ip dhcp excluded-address 10.30.10.1 10.30.10.127
SWD2(config)#Ip dhcp excluded-address 10.30.11.1 10.30.11.127
SWD2(config)#Ip dhcp excluded-address 10.30.12.1 10.30.12.127
SWD2(config)#Ip dhcp excluded-address 10.30.13.1 10.30.13.127
SWD2(config)#Ip dhcp excluded-address 10.30.14.1 10.30.14.127
SWD2(config)#Ip dhcp excluded-address 10.30.15.1 10.30.15.127
SWD2(config)#Ip dhcp excluded-address 10.30.16.1 10.30.16.127
SWD2(config)#Ip dhcp excluded-address 10.30.17.1 10.30.17.127
SWD2(config)#Ip dhcp excluded-address 10.30.18.1 10.30.18.127
SWD2(config)#Ip dhcp excluded-address 10.30.20.1 10.30.20.127
SWD2(config)#Ip dhcp excluded-address 10.30.21.1 10.30.21.127
SWD2(config)#Ip dhcp excluded-address 10.30.22.1 10.30.22.127
SWD2(config)#Ip dhcp excluded-address 10.30.23.1 10.30.23.127
SWD2(config)#Ip dhcp excluded-address 10.30.24.1 10.30.24.127
SWD2(config)#Ip dhcp excluded-address 10.30.25.1 10.30.25.127
SWD2(config)#Ip dhcp excluded-address 10.30.26.1 10.30.26.127
SWD2(config)#Ip dhcp excluded-address 10.30.27.1 10.30.27.127
SWD2(config)#Ip dhcp excluded-address 10.30.28.1 10.30.28.127
SWD2(config)#Ip dhcp excluded-address 10.30.29.1 10.30.29.127
SWD2(config)#Ip dhcp excluded-address 10.30.30.1 10.30.30.127
SWD2(config)#Ip dhcp excluded-address 10.30.31.1 10.30.31.127
SWD2(config)#Ip dhcp excluded-address 10.30.32.1 10.30.32.127
SWD2(config)#Ip dhcp excluded-address 10.30.33.1 10.30.33.127
SWD2(config)#Ip dhcp excluded-address 10.30.36.1 10.30.36.127
```

Figure 3.40 : Les adresses exclues 1-127 sur SWD2.

```
SWD2(config)#Ip dhcp excluded-address 10.30.10.252 10.30.10.254
SWD2(config)#Ip dhcp excluded-address 10.30.11.252 10.30.11.254
SWD2(config)#Ip dhcp excluded-address 10.30.12.252 10.30.12.254
SWD2(config)#Ip dhcp excluded-address 10.30.13.252 10.30.13.254
SWD2(config)#Ip dhcp excluded-address 10.30.14.252 10.30.14.254
SWD2(config)#Ip dhcp excluded-address 10.30.15.252 10.30.15.254
SWD2(config)#Ip dhcp excluded-address 10.30.16.252 10.30.16.254
SWD2(config)#Ip dhcp excluded-address 10.30.17.252 10.30.17.254
SWD2(config)#Ip dhcp excluded-address 10.30.18.252 10.30.18.254
SWD2(config)#Ip dhcp excluded-address 10.30.20.252 10.30.20.254
SWD2(config)#Ip dhcp excluded-address 10.30.21.252 10.30.21.254
SWD2(config)#Ip dhcp excluded-address 10.30.22.252 10.30.22.254
SWD2(config)#Ip dhcp excluded-address 10.30.23.252 10.30.23.254
SWD2(config)#Ip dhcp excluded-address 10.30.24.252 10.30.24.254
SWD2(config)#Ip dhcp excluded-address 10.30.25.252 10.30.25.254
SWD2(config)#Ip dhcp excluded-address 10.30.26.252 10.30.26.254
SWD2(config)#Ip dhcp excluded-address 10.30.27.252 10.30.27.254
SWD2(config)#Ip dhcp excluded-address 10.30.28.252 10.30.28.254
SWD2(config)#Ip dhcp excluded-address 10.30.29.252 10.30.29.254
SWD2(config)#Ip dhcp excluded-address 10.30.30.252 10.30.30.254
SWD2(config)#Ip dhcp excluded-address 10.30.31.252 10.30.31.254
SWD2(config)#Ip dhcp excluded-address 10.30.32.252 10.30.32.254
SWD2(config)#Ip dhcp excluded-address 10.30.33.252 10.30.33.254
SWD2(config)#Ip dhcp excluded-address 10.30.36.252 10.30.36.254
```

Figure 3.41 : Les adresses exclues 252-254 sur SWD2.

Avec la commande **show running-config** nous pouvons vérifier les adresses exclues sur le Switch SWD1 comme la figure 3.42 le montre :

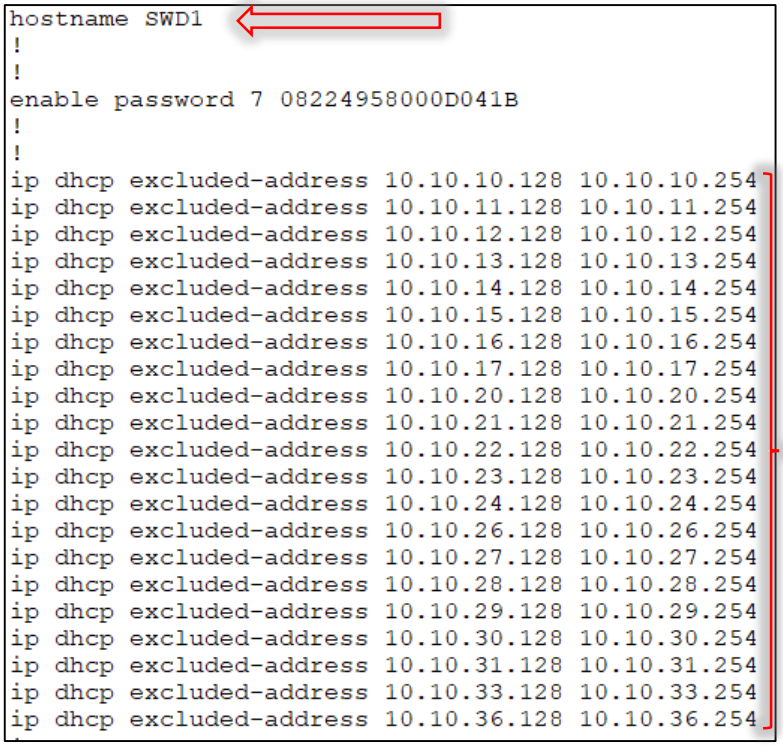

Figure 3.42 : Vérification des adresses exclues sur SWD1.

Avec la même commande nous vérifions aussi les adresses exclues sur le switch SWD2 comme la figure 3.43 le montre :

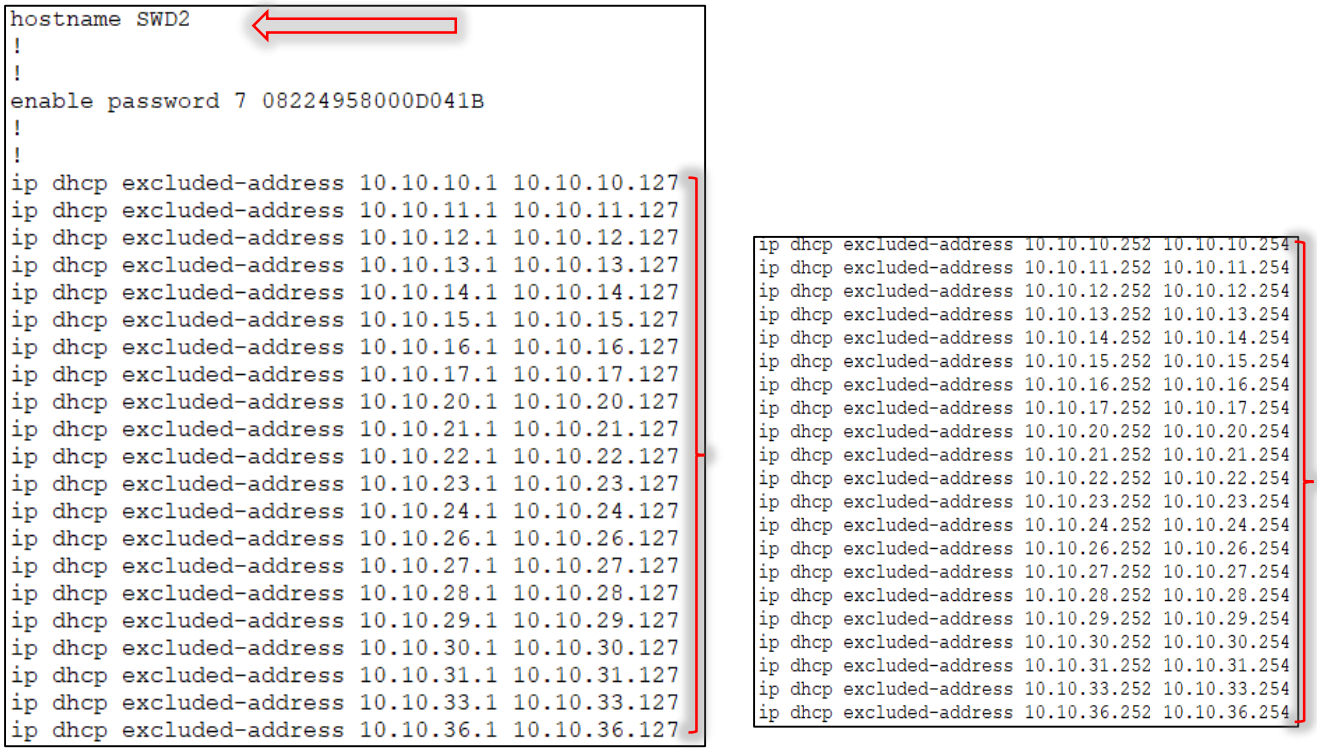

Figure 3.43 : Vérification des adresses exclues sur SWD2.

Nous allons créer maintenant un pool d'adresse pour chaque vlan à l'exception du vlan 18 (printer), vlan 20 (téléphone) vlan 21(Voice), vlan 25 (Management), et vlan 32(Camera), par la suite on définira la passerelle par défaut du sous réseau.

```
SWD1(config)#Ip dhcp pool vlan10
SWD1(dhcp-config)#Network  10.30.10.0 255.255.255.0
SWD1(dhcp-config)#Default-router 10.30.10.254
SWD1(dhcp-config)#Exit
```

Figure 3.44 : Exemple de création d'un pool pour le Vlan 10 sur le SWD1.

Nous allons vérifier la création de nos pools DHCP avec la commande show running-config. (Figure 3.45)

```
ip dhcp pool vlan10
 network 10.30.10.0 255.255.255.0
 default-router 10.30.10.254
ip dhcp pool vlan11
 network 10.30.11.0 255.255.255.0
 default-router 10.30.11.254
ip dhcp pool vlan12
 network 10.30.12.0 255.255.255.0
 default-router 10.30.12.254
ip dhcp pool vlan13
 network 10.30.13.0 255.255.255.0
 default-router 10.30.13.254
ip dhcp pool vlan14
 network 10.30.14.0 255.255.255.0
 default-router 10.30.14.254
ip dhcp pool vlan15
 network 10.30.15.0 255.255.255.0
 default-router 10.30.15.254
ip dhcp pool vlan16
 network 10.30.16.0 255.255.255.0
 default-router 10.30.16.254
ip dhcp pool vlan17
 network 10.30.17.0 255.255.255.0
 default-router 10.30.17.254
ip dhcp pool vlan18
 network 10.30.18.0 255.255.255.0
 default-router 10.30.18.254
ip dhcp pool vlan20
 network 10.30.20.0 255.255.255.0
 default-router 10.30.20.254
ip dhcp pool vlan21
 network 10.30.21.0 255.255.255.0
 default-router 10.30.21.254
```

```
ip dhcp pool vlan23
 network 10.30.23.0 255.255.255.0
 default-router 10.30.23.254
ip dhcp pool vlan24
 network 10.30.24.0 255.255.255.0
 default-router 10.30.24.254
ip dhcp pool vlan25
 network 10.30.25.0 255.255.255.0
 default-router 10.30.25.254
ip dhcp pool vlan26
 network 10.30.26.0 255.255.255.0
 default-router 10.30.26.254
ip dhcp pool vlan27
 network 10.30.27.0 255.255.255.0
 default-router 10.30.27.254
ip dhcp pool vlan28
 network 10.30.28.0 255.255.255.0
 default-router 10.30.28.254
ip dhcp pool vlan29
 network 10.30.29.0 255.255.255.0
 default-router 10.30.29.254
ip dhcp pool vlan30
 network 10.30.30.0 255.255.255.0
 default-router 10.30.30.254
ip dhcp pool vlan31
 network 10.30.31.0 255.255.255.0
 default-router 10.30.31.254
ip dhcp pool vlan32
 network 10.30.32.0 255.255.255.0
 default-router 10.30.32.254
ip dhcp pool vlan33
 network 10.30.33.0 255.255.255.0
 default-router 10.30.33.254
ip dhcp pool vlan36
 network 10.30.36.0 255.255.255.0
 default-router 10.30.36.254
```

Figure 3.45 : Vérification de la création des pools DHCP.

Après la configuration du DHCP, nous allons configurer les PCs en mode DHCP afin qu'ils reçoivent la configuration du réseau dynamiquement.

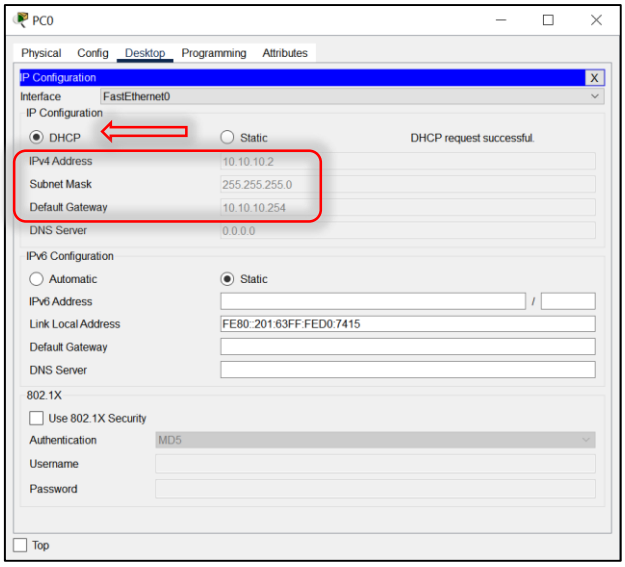

Figure 3.46 : Configurer le DHCP sur le pc et vérifier son fonctionnement.

3.6. Configurations de Protocole OSPF (Open Shortest Path First)

Ici pour l'OSPF, nous allons configurer ce Protocol au niveau des switches de distribution et ceux du Cœur. Nous allons tout d'abord convertir les ports de couche 2 en des ports de couche 3 et les faire fonctionner comme des interfaces de routeur plutôt que comme des ports de commutateur en utilisant la commande « no switchport », puis on attribue une adresse IP et un masque de réseau pour chacun des ports routés.

Les figures ci-dessous montrent la configuration des ports routés :

- ✓ Ou niveau 2 (pour les deux Switch SWD1 SWD2) :

```
SWD1(config)#Int range f0/1-4
SWD1(config-if-range)#no switchport
SWD1(config-if-range)#Exit
SWD1(config)#Int f0/4
SWD1(config-if)#Ip add 192.168.6.2 255.255.255.252
SWD1(config-if)#Int f0/3
SWD1(config-if)#Ip add 192.168.5.2 255.255.255.252
SWD1(config-if)#Int f0/2
SWD1(config-if)#Ip add 192.168.4.2 255.255.255.252
SWD1(config-if)#Int f0/1
SWD1(config-if)#Ip add 192.168.1.2 255.255.255.252
```

```
SWD2(config)#Int range f0/1-4
SWD2(config-if-range)#no switchport
SWD2(config-if-range)#Exit
SWD2(config)#Int f0/4
SWD2(config-if)#Ip add 192.168.7.2 255.255.255.252
SWD2(config-if)#Int f0/3
SWD2(config-if)#Ip add 192.168.5.1 255.255.255.252
SWD2(config-if)#Int f0/2
SWD2(config-if)#Ip add 192.168.3.1 255.255.255.252
SWD2(config-if)#Int f0/1
SWD2(config-if)#Ip add 192.168.2.1 255.255.255.252
```

Figure 3.47 : Configuration des ports routés sur SWD1 et SWD2.

- ✓ Ou niveau 3 (pour les deux Switch cœur et pour le Routeur) :

```
SWC1(config)#Int range f0/1-4
SWC1(config-if-range)#no switchport
SWC1(config-if-range)#Int f0/4
SWC1(config-if)#Ip add 192.168.6.2 255.255.255.252
SWC1(config-if)#Int f0/3
SWC1(config-if)#Ip add 192.168.5.2 255.255.255.252
SWC1(config-if)#Int f0/2
SWC1(config-if)#Ip add 192.168.4.2 255.255.255.252
SWC1(config-if)#Int f0/1
SWC1(config-if)#Ip add 192.168.1.2 255.255.255.252
SWC1(config-if)#Exit
```

```
SWC2(config)#Int range f0/1-4
SWC2(config-if-range)#no switchport
SWC2(config-if-range)#Int f0/4
SWC2(config-if)#Ip add 192.168.7.2 255.255.255.252
SWC2(config-if)#Int f0/3
SWC2(config-if)#Ip add 192.168.5.1 255.255.255.252
SWC2(config-if)#Int f0/2
SWC2(config-if)#Ip add 192.168.3.1 255.255.255.252
SWC2(config-if)#Int f0/1
SWC2(config-if)#Ip add 192.168.2.1 255.255.255.252
SWC2(config-if)#Exit
```

Figure 3.48 : Configuration des ports routés sur SWC1 et SWC2.

```
Router(config)#Int gig0/0/0
Router(config-if)#Ip add 192.168.6.1 255.255.255.252
Router(config-if)#No sh
Router(config-if)#Ex
Router(config)#Int gig0/0/1
Router(config-if)#Ip add 192.168.7.1 255.255.255.252
Router(config-if)#No sh
```

Figure 3.49 : Configuration des ports routés sur Router.

Ensuite nous allons activer le routage OSPF, on attribue un groupe 1 par exemple et nous allons saisir tous les réseaux directement connectés dans chaque switch.

Pour les Vlans, nous allons saisir le réseau 10.30.X.0 avec un masque inversé 0.0.0.255 comme suit :

✓ **Ou niveaux 2 :**

Sur SWD1

```
SWD1(config)#Ip routing
SWD1(config)#Router ospf 1
SWD1(config-router)#Network 192.168.1.0 0.0.0.3 area 0
SWD1(config-router)#Network 192.168.3.0 0.0.0.3 area 0
SWD1(config-router)#Network 10.10.10.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.11.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.12.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.13.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.14.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.15.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.16.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.17.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.18.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.20.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.21.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.22.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.23.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.24.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.25.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.26.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.27.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.28.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.29.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.30.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.31.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.32.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.33.0 0.0.0.255 area 0
SWD1(config-router)#Network 10.10.36.0 0.0.0.255 area 0
SWD1(config-router)#exit
```

Figure 3.50 : Configuration de l'OSPF sur SWD1.

Sur SWD2

```
SWD2(config)#Ip routing
SWD2(config)#Router ospf 1
SWD2(config-router)#Network 192.168.2.0 0.0.0.3 area 0
SWD2(config-router)#Network 192.168.4.0 0.0.0.3 area 0
SWD2(config-router)#Network 10.10.10.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.11.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.12.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.13.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.14.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.15.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.16.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.17.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.18.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.20.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.21.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.22.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.23.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.24.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.25.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.26.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.27.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.28.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.29.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.30.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.31.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.32.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.33.0 0.0.0.255 area 0
SWD2(config-router)#Network 10.10.36.0 0.0.0.255 area 0
```

Figure 3.51 : Configuration de l'OSPF sur SWD2.

✓ **Nous allons procéder la même chose Ou niveaux 3 :**

Sur SWC1 et SWC2 :

```
SWC1(config)#Ip routing
SWC1(config)#Router ospf 1
SWC1(config-router)#Network 192.168.6.0 0.0.0.3 area 0
SWC1(config-router)#Network 192.168.5.0 0.0.0.3 area 0
SWC1(config-router)#Network 192.168.4.0 0.0.0.3 area 0
SWC1(config-router)#Network 192.168.1.0 0.0.0.3 area 0
SWC1(config-router)#exit
```

```
SWC2(config)#Ip routing
SWC2(config)#Router ospf 1
SWC2(config-router)#Network 192.168.7.0 0.0.0.3 area 0
SWC2(config-router)#Network 192.168.5.0 0.0.0.3 area 0
SWC2(config-router)#Network 192.168.3.0 0.0.0.3 area 0
SWC2(config-router)#Network 192.168.2.0 0.0.0.3 area 0
SWC2(config-router)#exit
```

Figure 3.52 : Configuration de l'OSPF sur SWC1 et SWC2.

Sur Routeur :

```
Router(config)#Ip routing
Router(config)#Router ospf 1
Router(config-router)#Network 192.168.7.0 0.0.0.3 area 0
Router(config-router)#Network 192.168.6.0 0.0.0.3 area 0
```

Figure 3.53 : Configuration de l'OSPF sur Router.

Et nous pouvons vérifier avec la commande Show IP route.

```
Router#Show IP route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/24 is subnetted, 24 subnets
O       10.10.10.0/24 [110/3] via 192.168.6.2, 02:13:33, GigabitEthernet0/0/0
                      [110/3] via 192.168.7.2, 02:13:33, GigabitEthernet0/0/1
O       10.10.11.0/24 [110/3] via 192.168.6.2, 02:13:33, GigabitEthernet0/0/0
                      [110/3] via 192.168.7.2, 02:13:33, GigabitEthernet0/0/1
O       10.10.12.0/24 [110/3] via 192.168.6.2, 02:13:33, GigabitEthernet0/0/0
                      [110/3] via 192.168.7.2, 02:13:33, GigabitEthernet0/0/1
O       10.10.13.0/24 [110/3] via 192.168.6.2, 02:13:33, GigabitEthernet0/0/0
                      [110/3] via 192.168.7.2, 02:13:33, GigabitEthernet0/0/1
O       10.10.14.0/24 [110/3] via 192.168.6.2, 02:13:33, GigabitEthernet0/0/0
                      [110/3] via 192.168.7.2, 02:13:33, GigabitEthernet0/0/1
```

Figure 3.54 : Vérification de l'OSPF.

3.7. Configuration du Spanning Tree Protocol (STP)

Pour faciliter la mise en place d'un chemin logique sans boucle sur l'ensemble du domaine de diffusion nous allons configurer le protocole STP.

Le commutateur SWD1 d'être le root bridge de Vlan 10 jusqu'à vlan 22 et le root bridge de secours de Vlan 23 jusqu'à vlan 36.

```
SWD1(config)#spanning-tree vlan 10-22 root primary
SWD1(config)#spanning-tree vlan 23-36 root secondary
SWD1(config)#exit
```

Figure 3.55 : Configuration du STP sur SWD1.

Nous avons procédé de la même façon pour le SWD2 qui est le root bridge de Vlan 23 jusqu'à vlan 36 et le root bridge de secours de vlan 10 jusqu'à vlan 22.

```
SWD2(config)#spanning-tree vlan 23-36 root primary
SWD2(config)#spanning-tree vlan 10-22 root secondary
SWD2(config)#exit
```

Figure 3.56 : Configuration de STP sur SWD2.

Et nous allons vérifier cette configuration avec la commande Show running-config :

```
spanning-tree mode pvst
spanning-tree vlan 10-22 priority 24576
spanning-tree vlan 23-36 priority 28672
```

Figure 3.57 : Vérification du STP sur SWD1.

```
spanning-tree mode pvst
spanning-tree vlan 23-36 priority 24576
spanning-tree vlan 10-22 priority 28672
```

Figure 3.58 : Vérification du STP sur SWD2.

Pour voir la configuration de chaque instance Spanning-tree, on tape la commande show spanning-tree.

```
VLAN0011
  Spanning tree enabled protocol ieee
  Root ID     Priority    24587
              Address     0040.0B1D.3858
              This bridge is the root
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID   Priority    24587  (priority 24576 sys-id-ext 11)
              Address     0040.0B1D.3858
              Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
              Aging Time  20
```

Figure 3.59 : Instance STP, exemple Vlan 11.

3.8. Configuration de protocole de la haute disponibilité (HSRP)

1. Configuration des SVI (Switch Virtual Interface)

Durant cette étape nous allons configurer les SVI de chaque vlan, autrement dit, nous allons attribuer une adresses IP virtuel pour chaque vlan sur les deux switches de distribution SWD1 et SWD2, cela va nous permettre de faire un routage inter-vlan, mais ce dernier ne se fera pas sauf si on active la fonction de routage avec la commande ip routing.

```
SWD1(config)#ip routing
SWD1(config)#
```

Figure 3.60 : Configuration d'ip routing.

2. Configuration de protocole HSRP

Maintenant nous allons configurer le protocole HSRP au niveau des deux switches de distribution SWD1 et SWD2, on définit un groupe HSRP, une priorité « standbay priority » la plus élevée qui décide le commutateur "active", et de la préemption « standby preempt » comme suite :

✓ pour les VLANs 10 à 22 en mode « Active » :

```
SWD1(config)#int vlan 10
SWD1(config-if)#standby 10 ip 10.10.10.254
SWD1(config-if)#standby 10 priority 200
SWD1(config-if)#standby 10 preempt
SWD1(config-if)#
SWD1(config-if)#int vlan 11
SWD1(config-if)#standby 11 ip 10.10.11.254
SWD1(config-if)#standby 11 priority 200
SWD1(config-if)#standby 11 preempt
SWD1(config-if)#
SWD1(config-if)#int vlan 12
SWD1(config-if)#standby 12 ip 10.10.12.254
SWD1(config-if)#standby 12 priority 200
SWD1(config-if)#standby 12 preempt
```

Figure 3.61 : Configuration du HSRP sur SWD1 (VLAN 10-22).

✓ Pour les VLANs 23 à 36 en mode « Standby » :

```
SWD1(config-if)#int vlan 23
SWD1(config-if)#standby 23 ip 10.10.23.254
SWD1(config-if)#standby 23 priority 150
SWD1(config-if)#standby 23 preempt
SWD1(config-if)#
SWD1(config-if)#
SWD1(config-if)#int vlan 24
SWD1(config-if)#standby 24 ip 10.10.24.254
SWD1(config-if)#standby 24 priority 150
SWD1(config-if)#standby 24 preempt
SWD1(config-if)#
SWD1(config-if)#int vlan 25
SWD1(config-if)#standby 25 ip 10.10.25.254
SWD1(config-if)#standby 25 priority 150
SWD1(config-if)#standby 25 preempt
```

Figure 3.62 : Configuration du HSRP sur SWD1 (VLAN 23-36).

On procédera de même pour le SWD2 :

- ✓ pour les VLANs 23 à 36 en mode « **Active** » :

```
SWD2(config-if)#int vlan 23
SWD2(config-if)#standby 23 ip 10.10.23.254
SWD2(config-if)#standby 23 priority 200
SWD2(config-if)#standby 23 preempt
SWD2(config-if)#
SWD2(config-if)#
SWD2(config-if)#int vlan 24
SWD2(config-if)#standby 24 ip 10.10.24.254
SWD2(config-if)#standby 24 priority 200
SWD2(config-if)#standby 24 preempt
SWD2(config-if)#
SWD2(config-if)#int vlan 25
SWD2(config-if)#standby 25 ip 10.10.25.254
SWD2(config-if)#standby 25 priority 200
SWD2(config-if)#standby 25 preempt
SWD2(config-if)#
SWD2(config-if)#int vlan 26
SWD2(config-if)#standby 26 ip 10.10.26.254
SWD2(config-if)#standby 26 priority 200
SWD2(config-if)#standby 26 preempt
```

Figure 3.63 : Configuration du HSRP sur SWD2 (VLAN 23-36).

- ✓ Pour les VLANs de 10 à 22 en mode « Standby » :

```
SWD2(config)#int vlan 10
SWD2(config-if)#standby 10 ip 10.10.10.254
SWD2(config-if)#standby 10 priority 150
SWD2(config-if)#standby 10 preempt
SWD2(config-if)#standby 10 preempt
SWD2(config-if)#
SWD2(config-if)#int vlan 11
SWD2(config-if)#standby 11 ip 10.10.11.254
SWD2(config-if)#standby 11 priority 150
SWD2(config-if)#standby 11 preempt
SWD2(config-if)#
SWD2(config-if)#int vlan 12
SWD2(config-if)#standby 12 ip 10.10.12.254
SWD2(config-if)#standby 12 priority 150
SWD2(config-if)#standby 12 preempt
```

Figure 3.1 : Configuration du HSRP sur SWD2 (VLAN 10-22).

Nous allons vérifier cette configuration avec la commande Show standby brief sur les deux switches

✓ Sur SWD1 :

```
Show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   200 P Active   local           10.10.10.253    10.10.10.254
Vl11        11   200 P Active   local           10.10.11.253    10.10.11.254
Vl12        12   200 P Active   local           10.10.12.253    10.10.12.254
Vl13        13   200 P Active   local           10.10.13.253    10.10.13.254
Vl14        14   200 P Active   local           10.10.14.253    10.10.14.254
Vl15        15   200 P Active   local           10.10.15.253    10.10.15.254
Vl16        16   200 P Active   local           10.10.16.253    10.10.16.254
Vl17        17   200 P Active   local           10.10.17.253    10.10.17.254
Vl18        18   200 P Active   local           10.10.18.253    10.10.18.254
Vl20        20   200 P Active   local           10.10.20.253    10.10.20.254
Vl21        21   200 P Active   local           10.10.21.253    10.10.21.254
Vl22        22   200 P Active   local           10.10.22.253    10.10.22.254
Vl23        23   150 P Standby  10.10.23.253    local           10.10.23.254
Vl24        24   150 P Standby  10.10.24.253    local           10.10.24.254
Vl25        25   150 P Standby  10.10.25.253    local           10.10.25.254
Vl26        26   150 P Standby  10.10.26.253    local           10.10.26.254
Vl27        27   150 P Standby  10.10.27.253    local           10.10.27.254
Vl28        28   150 P Standby  10.10.28.253    local           10.10.28.254
Vl29        29   150 P Standby  10.10.29.253    local           10.10.29.254
Vl30        30   150 P Standby  10.10.30.253    local           10.10.30.254
Vl31        31   150 P Standby  10.10.31.253    local           10.10.31.254
Vl32        32   150 P Standby  10.10.32.253    local           10.10.32.254
Vl33        33   150 P Standby  10.10.33.253    local           10.10.33.254
Vl36        36   150 P Standby  10.10.36.253    local           10.10.36.254
```

Figure 3. 64 : Vérification du HSRP sur SWD1.

✓ Sur SWD :

```
SWD2#Show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl10        10   150 P Standby  10.10.10.252    local           10.10.10.254
Vl11        11   150 P Standby  10.10.11.252    local           10.10.11.254
Vl12        12   150 P Standby  10.10.12.252    local           10.10.12.254
Vl13        13   150 P Standby  10.10.13.252    local           10.10.13.254
Vl14        14   150 P Standby  10.10.14.252    local           10.10.14.254
Vl15        15   150 P Standby  10.10.15.252    local           10.10.15.254
Vl16        16   150 P Standby  10.10.16.252    local           10.10.16.254
Vl17        17   150 P Standby  10.10.17.252    local           10.10.17.254
Vl18        18   150 P Standby  10.10.18.252    local           10.10.18.254
Vl20        20   150 P Standby  10.10.20.252    local           10.10.20.254
Vl21        21   150 P Standby  10.10.21.252    local           10.10.21.254
Vl22        22   150 P Standby  10.10.22.252    local           10.10.22.254
Vl23        23   200 P Active   local           10.10.23.252    10.10.23.254
Vl24        24   200 P Active   local           10.10.24.252    10.10.24.254
Vl25        25   200 P Active   local           10.10.25.252    10.10.25.254
Vl26        26   200 P Active   local           10.10.26.252    10.10.26.254
Vl27        27   200 P Active   local           10.10.27.252    10.10.27.254
Vl28        28   200 P Active   local           10.10.28.252    10.10.28.254
Vl29        29   200 P Active   local           10.10.29.252    10.10.29.254
Vl30        30   200 P Active   local           10.10.30.252    10.10.30.254
Vl31        31   200 P Active   local           10.10.31.252    10.10.31.254
Vl32        32   200 P Active   local           10.10.32.252    10.10.32.254
Vl33        33   200 P Active   local           10.10.33.252    10.10.33.254
Vl36        36   200 P Active   local           10.10.36.252    10.10.36.254
```

Figure 3.65 : Vérification du HSRP sur SWD2.

3.9. Agrégation des liens EtherChannel

Donc dans notre architecture, nous avons opté pour une agrégation des liens Faste Ethernet entre les deux switchs de distribution SWD1 et SWD2 on a donc mis les deux ports fastEthernet dans un groupe en précisant le mode ON, peut on les a mis en mode trunk, et nous allons la configurer comme l'indique la figure 3.66 ci-dessous.

```
SWD1#conf ter
Enter configuration commands, one per line.  End with CNTL/Z.
SWD1(config)#int range g0/1-2
SWD1(config-if-range)#channel-group 1 mode on
SWD1(config-if-range)#exit
SWD1(config)#int port-channel 1
SWD1(config-if)#switchport trunk encapsulation dot1q
SWD1(config-if)#switchport mode trunk
SWD1(config-if)#exit
SWD1(config)#
Creating a port-channel interface Port-channel 1
```

Figure 3.66 : Configuration d'EtherChannel sur SWD1.

Pour vérifier la configuration en mode trunk sur l'un des switchs d'accès, en utilisant la commande show interface trunk.

```
DRH#show interface trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/3       on           802.1q         trunking      1
Fa0/4       on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/3       1-1005
Fa0/4       1-1005

Port        Vlans allowed and active in management domain
Fa0/3       1,10,11,12,13,14,15,16,17,18,20,21,22,23,24,25,26,27,28,29,30,31,32,33,36
Fa0/4       1,10,11,12,13,14,15,16,17,18,20,21,22,23,24,25,26,27,28,29,30,31,32,33,36

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/3       10,11,12,13,14,15,16,17,18,20,21,22
Fa0/4       1,23,24,25,26,27,28,29,30,31,32,33,36
```

Figure 3.67 : Vérification de la configuration du mode trunk sur Switch accès.

3.10. Vérification de la communication

Afin de tester le bon fonctionnement de notre réseau et de s'assurer qu'il est opérationnel, nous allons simuler un Ping continue d'un des Vlans vers une autre interface. Puis, nous allons simuler une panne en mettant la route principale en « shutdown ». Ensuite, nous allons vérifier si le Ping change facilement de route, après nous allons à nouveaux rallumer la route principale afin de vérifier le « preempt » du HSRP qui va à nouveau reprendre sa route principale.

- ✓ **Test entre pc de différents Vlans au niveau de la couche distribution :**

Premièrement nous avons pris un PC du VLAN 10 (10.30.10.1) et nous allons faire un ping continu vers VLAN 23 (10.30.23.128), En premier lieu nous avons constaté que le ping fonctionne parfaitement et sans problème, comme Figure 3.68 l'explique :

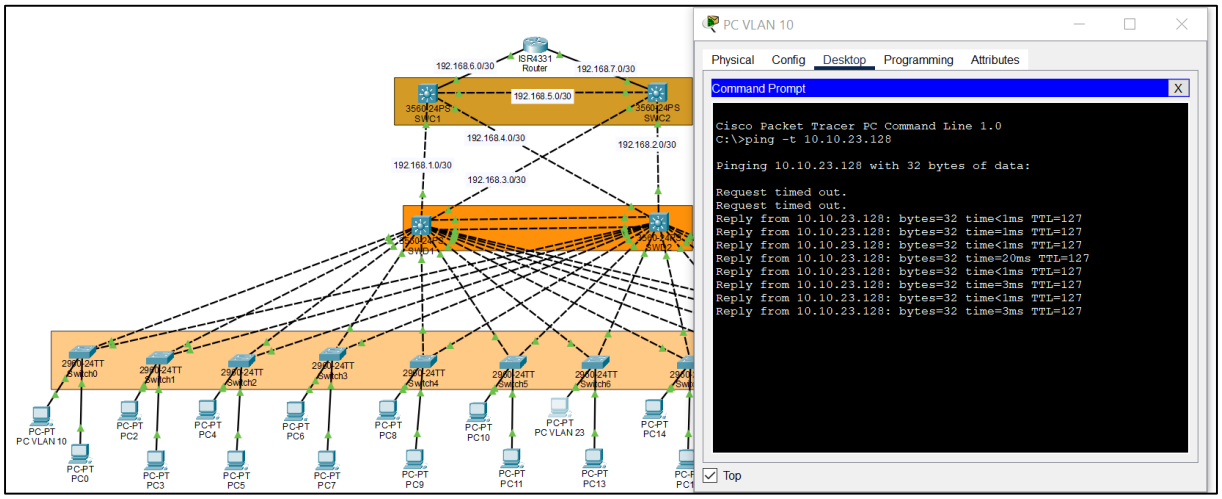

Figure 3.68 : Capture explicative du ping au niveau de la couche distribution.

Ensuite nous allons simuler une panne, celle d'éteindre la route principale de ce vlan (la ligne rouge sur Figure 3.69), nous allons constater directement que le ping s'arrête, Juste après 5 ou 6 arrêts le protocole HSRP discute avec le SWD2 et active automatiquement la route qui est en standby en active, nous allons constater directement que le ping reprend, ce qui prouve que la route a bien été basculée vers le SWD2, comme est visible sur Figure 3.69 :

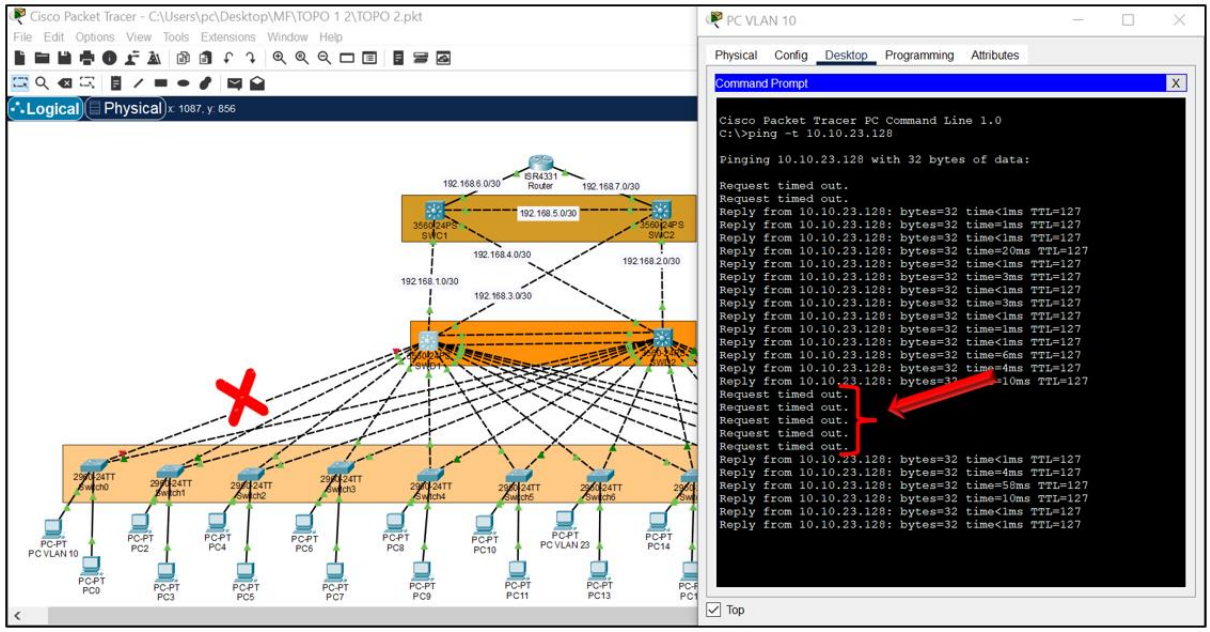

Figure 3.69: Capture explicative du Ping au niveau de la couche distribution

Maintenant, nous allons réactiver l'interface principale sur le SDW1 afin de s'assurer qu'il va reprendre sa route principale et vérifier que le preempt du HSRP fonctionne parfaitement.

Dès qu'on active l'interface, on constate qu'il y a encore un arrêt dans le ping et aussi environ 4 ou 5 arrêts le temps que les deux switches discutent les priorités, il reprend facilement sa route et le ping reprend comme si rien n'était Figure 3.70 :

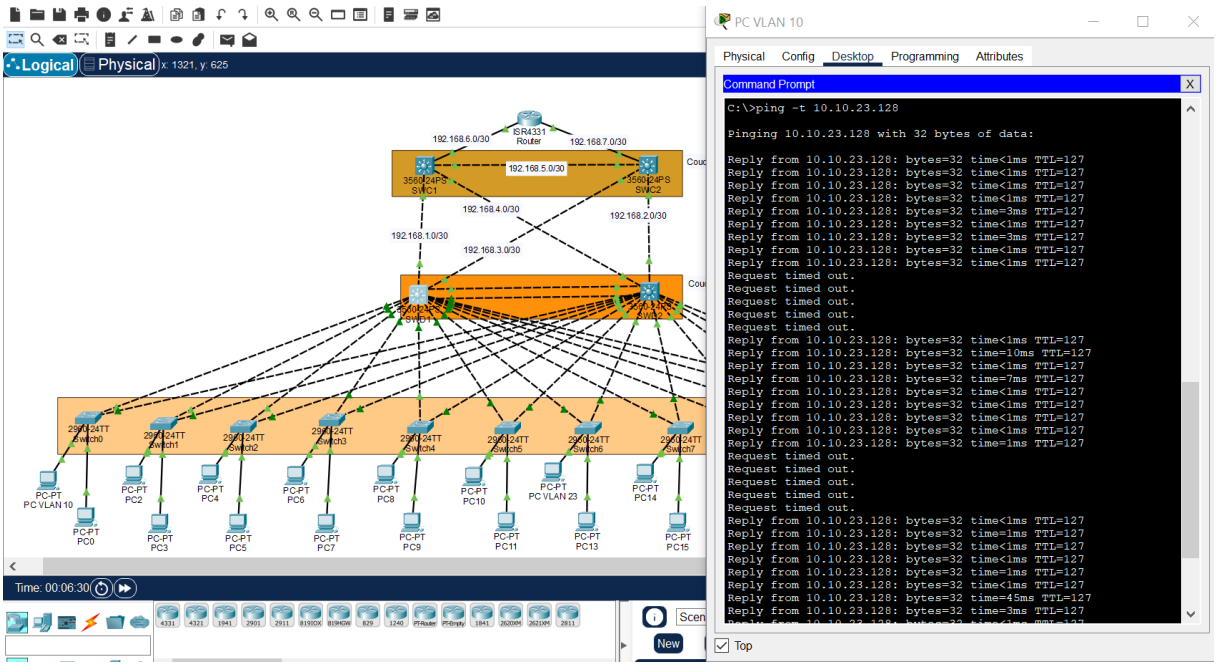

Figure 3.70: Capture explicative du Ping au niveau de la couche distribution

✓ **Test de haute disponibilité du Réseau LAN de CEVITAL (niveau2 et niveau3) :**

Suivant la même méthode nous allons tester la haute disponibilité de tout le réseau local de CEVITAL. Nous avons simulé ici la défaillance de l'un des switches de distribution et les interfaces amenant au routeur.

Premièrement, nous avons pris un PC du VLAN 10 et nous allons faire un Ping continue vers l'adresse **192.168.7.1** afin de vérifier non seulement le HSRP mais aussi l'OSPF comme l'explique la figure 3.71.

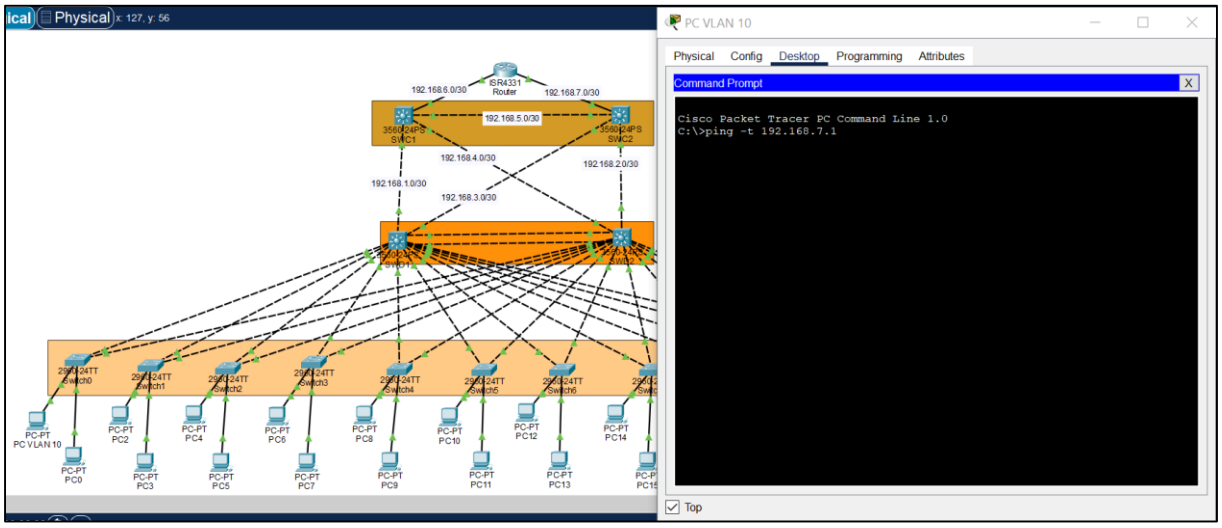

Figure 3.71 : Capture explicative du Ping.

En premier lieu nous avons constaté que le Ping fonctionne parfaitement et sans problème, comme le montre la figure 3.61. Ensuite, nous allons simuler une panne, celle d'éteindre la route principale de ce VLAN, présenté par la ligne rouge sur la figure 3.72. En effet, nous allons constater directement que le Ping s'arrête et ne passe pas.

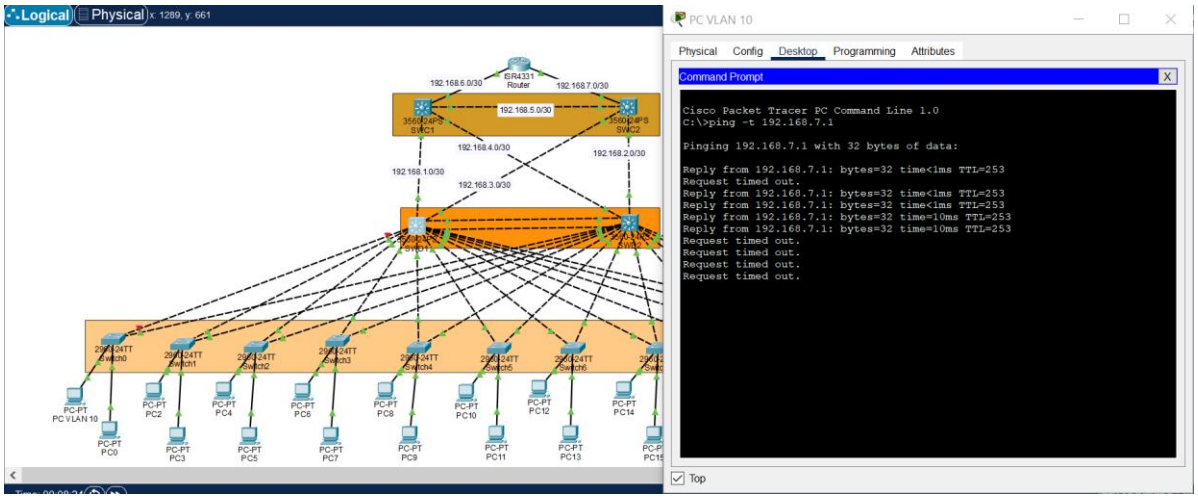

Figure 3.72 : Ping lors de désactivation du port vers SWD1.

Après quelques arrêts le protocole HSRP communique avec le SWD2 et active automatiquement la route qui est en standby en active, nous allons constater directement que le Ping reprend. Ce qui prouve que la route est converti vers SWD2, comme est visible sur la figure 3.73 :

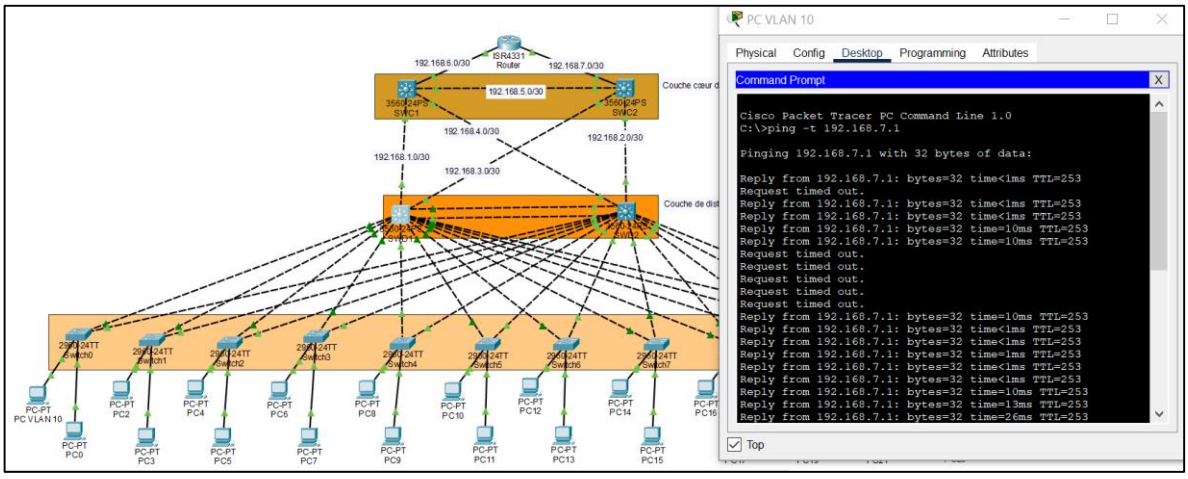

Figure 3.73 : Reprise du Ping après discussion avec SWD2.

Maintenant, nous allons réactiver l'interface principale sur le SWD1, afin de s'assurer qu'il va reprendre sa route principale et vérifier que le **preempt** du HSRP fonctionne parfaitement.

Dès qu'on active l'interface, on constate qu'il y a encore un arrêt dans le Ping et aussi environ 4 à 5 arrêts le temps que les deux switches discutent les priorités il reprend facilement sa route et le Ping reprend comme si rien n'était :

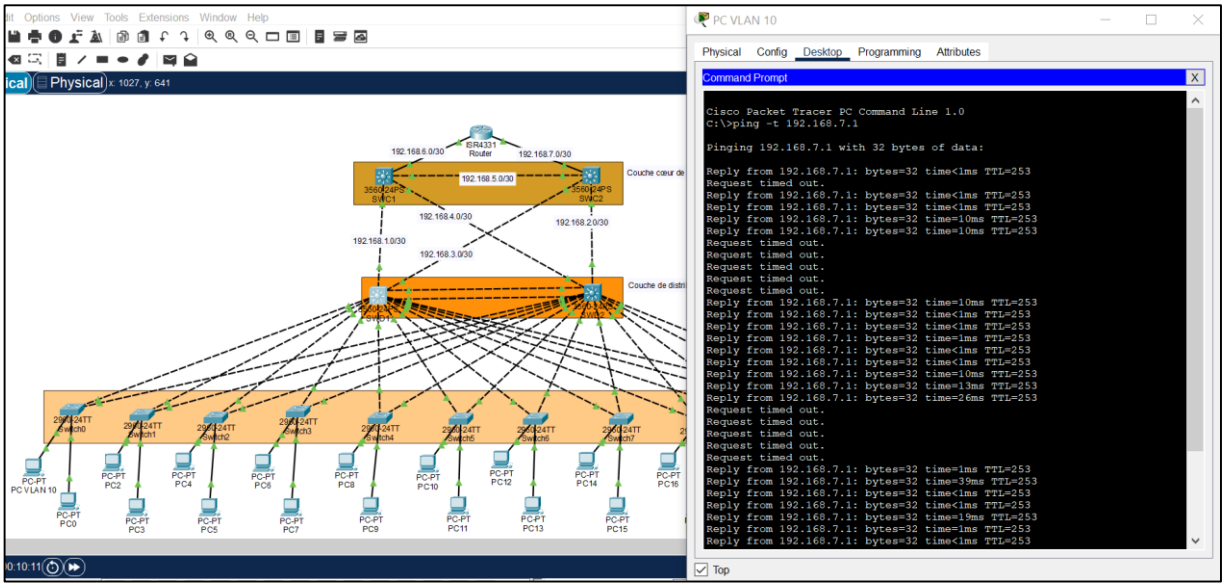

Figure 3.74 : Ping lors de la réactivation du port vers SWD1.

- **Pour bien confirme le bon fonctionnement des protocoles, une autre simulation a été faite :**

Nous avons pris un PC du VLAN 10 (10.10.10.1) et nous allons envoyer un ping continu vers l'adresse 192.168.7.1. Puis on a simulé une panne au niveau du Switch de distribution SWD1 (root bridge de Vlan 10) ainsi au niveau de l'un des liens de Switch SWD2 (interface Fa0/13) et

switch cœur 1 (interface Fa0/4) afin de vérifier non seulement le HSRP mais aussi l'OSPF comme Figure 3.75 l'explique :

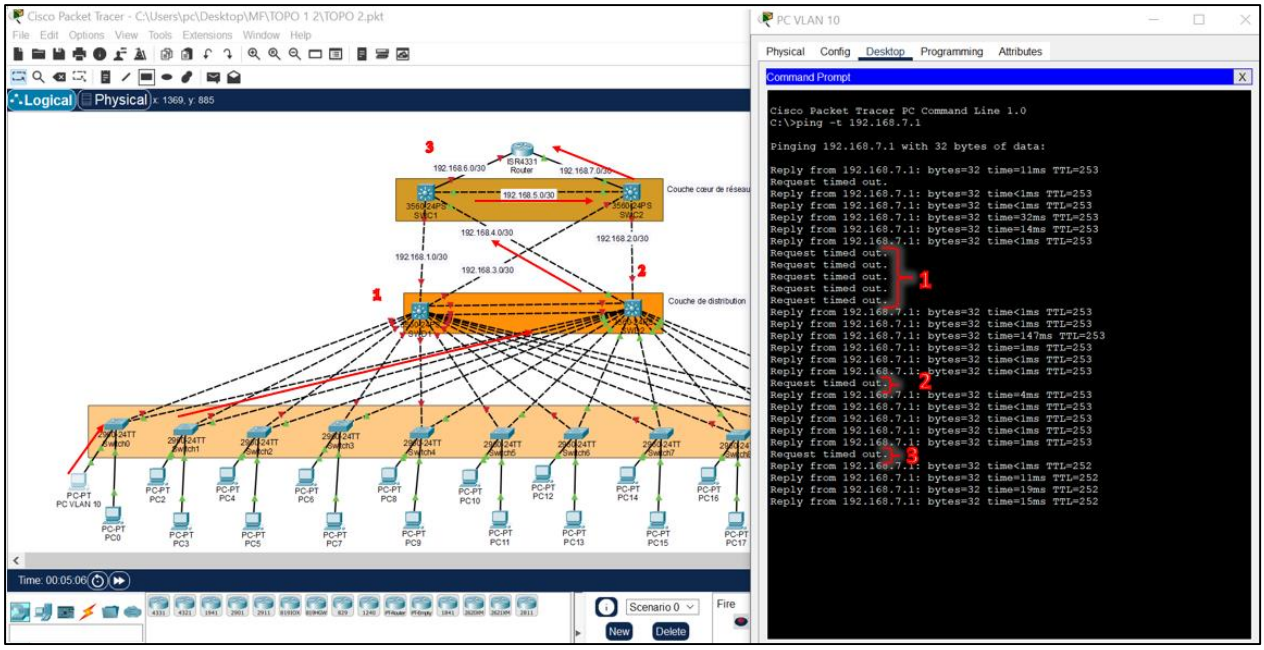

Figure 3.75 : Capture explicative de test de la haute disponibilité LAN.

Désormais le protocole HSRP que nous avons configuré, ainsi que le protocole de routage OSPF fonctionnent parfaitement et ne signalent aucun problème.

3.11. Conclusion

Dans ce chapitre, nous avons commencé par la présentation du simulateur Packet Tracer. Par conséquent, au cours des deux parties, nous avons pu décrire toutes les configurations effectuées au niveau du réseau local concernant les VLAN, DHCP, VTP, STP, OSPF, ainsi que le HSRP. Les résultats obtenus par cette simulation montrent que la segmentation du réseau en VLAN apporte une sécurisation des données échangées entre les différents services de l'entreprise site CEVITAL Bejaia, améliore la gestion de manière dynamique tout en évitant des collisions, ainsi qu'une meilleure régulation du réseau (réduire la congestion).

Conclusion

Conclusion

L'informatique ne cesse de se développer au fil des années, et avec la mondialisation, le secteur de technologie de l'information a facilité le transfert des données.

Ce présent travail a été élaboré dans le cadre d'un projet de fin d'étude pour l'obtention du diplôme master Académique en Réseaux et télécommunications dont le stage pratique a été effectué au sein du groupe CEVITAL.

Afin de bien mener notre projet, et atteindre les résultats attendus tout en répondant à la problématique en question, nous avons décidé de nous servir du simulateur Cisco Packet Tracer dans l'intention de bénéficier des différents avantages qu'il présente en matière des composants de l'architecture d'un réseau déjà créé.

Pour bien Etaler sur les problèmes du réseau existant nous trouvons que le réseau d'entreprise dispose de plusieurs lacunes comme la d'insatisfaction du débit, la limitation de la bande passante et sur tout de la surcharge au niveau du switch centrale (backbone). Ce qui a permet de rendre le réseau non performant, non redondant et qui a causé aussi une défaillance dans l'architecture réseau.

De ce fait, nous avons devisé notre travail en trois grands chapitres, dont le premier a mis en avant les principes fondamentaux des réseaux informatiques. Le deuxième été consacré sur la présentation de l'organisme d'accueil CEVITAL, ses différentes directions ainsi que son système informatique, dont on a constaté un problème au niveau de son architecture actuelle, ce qui nous a poussés à leur proposer nos solutions. Enfin, le troisième chapitre, qui été dédié au cas pratique de notre thème, quant au premier lieu, nous avons décortiqué le réseau déjà existant du groupe afin que nous puissions signaler les problèmes rencontrés, pour qu'en second lieu, nous arriverons à leurs proposer une architecture meilleure pour un excellent fonctionnement.

Grace à notre projet, nous avons pu approfondir nos connaissances déjà acquises et à les mettre en place durant la pratique de notre stage afin d'installer, configurer et administrer une architecture réseau locale pour le groupe CEVITAL.

Ce que nous pouvons tirer lors de notre projet, est que les protocoles présentent un élément primordial et ils jouent un rôle majeur dans l'optimisation de la qualité de transfert de l'information dans le réseau local de l'entreprise, et qu'une simple panne peut interrompre la transmission de données et donc elle peut engendrer un dysfonctionnement total du réseau, ce qui explique la complexité des réseaux informatiques et surtout de la sécurité.

Pour conclure, la transmission des données nécessite une haute sécurité, qui reste à nos jours un sujet très complexe et un domaine assez vaste qui exige plus de détails techniques et de savoir-faire.

Bibliographie

Les livres

[1] Pujolle, G. (2014). Les réseaux .Editions Eyrolles.

[4] Cauchie N. Dzodic, V. & Vernerie. M. (2005). CCNA 1-Essentiel Théorie des réseaux. Laboratoire SUPINFO des Technologies Cisco.

[5] Servin, C. (2013). Réseaux et Telecoms (4e édition). Dunod.

[7] Bedra, R. (2019). Supports de cours « Supports de transmission ». Université Mousfa-Benboulaid- Batna 2.

[9] GERET.30 septembre 2003.Architecure de réseau.

[10]Laurent HAUGEARD. (2007). Architecture et Interconnexion Internet. GNU Free Documentation License.

[11] ANSSI. (2016). Recommandations pour la sécurisation d'un commutateur de desserte.

[12] Peters, C. (1997). Document de travail pour le Comité directeur d'Internet du Conseil consultatif sur l'autoroute de l'information.

[14] Lohier, S. (2010). Le réseau Internet : des services aux infrastructures.Dunod

[15] Servin, C. (2020).réseaux et télécoms (2e édition).Dunod

[18] Simon, F., & Tellier, A. (2008). Créativité et réseaux sociaux dans l'organisation ambidextre. Revue française de gestion.

[19] Pillou, J.-F., & Bay, J.-P. (2020). Tout sur la sécurité informatique (5e édition). Dunod.

[20] Shahriar, F., et al. (2018). Designing a reliable and redundant network for multiple VLANs with Spanning Tree Protocol (STP) and Fast Hop Redundancy Protocol (FHRP). Proceedings of the International Conference on Industrial Engineering and Operations Management.

[23] Andrianina, R. J. (2013).réseaux et Télécoms (2e édition).

[25] TOURRES, G.BODIN, L.VERNERIE, M. (2005-2007) .Cisco CCNA 3 Commutation et routage intermédiaire Essentiel.

[26] Document délivré par l'organisme d'accueil Cevital Agro-industrie de l'entreprise.

Mémoires et thèses :

[2] Badéche, A. (2012). Classification selon l'architecture (Mémoire de master). Université de Bejaia.

[3] Talbi, B. (2012). Configuration du réseau local de l'entreprise NAFTAL Bejaia en vue de partage des ressources informatiques via active directory (Mémoire de master). Université Abderahmane Mira Béjaia.

[19] Boulila, N., & Boulila, R. (2020). Mise en réseau d'une Infrastructure Hyper-Converg

Les sites internet

[6]https://www.informatique-bureautique.com/moodle/mod/page/view.php?id=189 consulté le 15/06/2023.

[13]http://projet.eu.org/pedago/sin/term/8-adressage_IP.pdf consulté le 15/06/2023.

[17]https://www.cevital.com/lhistoire-du-groupe/ consulté le 15/06/2023.

[20]https://www.groupesl.com/nouvelles/comment-assurer-disponibilite-informatique-entreprise/ consulté le 15/06/2023.

[22]https://www.it-connect.fr/mise-en-place-du-protocole-hsrp/ consulté le 15/06/2023.

Résumé

L'objectif de notre projet consiste à répondre aux problèmes de partage des ressources informatiques au sein de l'entreprise CEVITAL, on a proposé une solution permettant de centraliser les équipements et les ressources utilisées par les utilisateurs au sein de l'entreprise. Afin de lui fournir un partage efficace de données en utilisant les protocoles de redondances, ainsi que les VTPs qui permet de gérer de façon centralisé les VLANs. Pour mettre notre solution en pratique nous avons utilisé le simulateur « PACKET TRACER », qui offre la possibilité d'implémenter un réseau physique virtuel et de simuler le comportement des protocoles sur ce réseau.

Mots clés : VTP, VLAN, PACKET TRACER.

Abstract

The objective of our project is to respond to the problems of sharing IT resources within the company CEVITAL, we have proposed a solution to centralize the equipment and resources used by users within the company. In order to provide it with efficient data sharing using redundancy protocols, as well as VTPs which allows VLANs to be managed centrally. To put our solution into practice we used the "PACKET TRACER" simulator, which offers the possibility of implementing a virtual physical network and simulating the behavior of protocols on this network.

Keywords: VTP, VLAN, PACKET TRACER

ملخص

الهدف من مشروعنا هو الاستجابة لمشاكل مشاركة موارد تكنولوجيا المعلومات داخل شركة CEVITAL، وقد اقترحنا حلاً لمركزية المعدات والموارد المستخدمة من قبل المستخدمين داخل الشركة. من أجل تزويدها بمشاركة فعالة للبيانات باستخدام بروتوكولات التكرار ، بالإضافة إلى VTPs التي تسمح بإدارة شبكات VLAN مركزياً. لوضع حلنا موضع التنفيذ، استخدمنا محاكي "PACKET TRACER" ، والذي يوفر إمكانية تنفيذ شبكة فعلية افتراضية ومحاكاة سلوك البروتوكولات على هذه الشبكة.

الكلمات الرئيسية: VTP، VLAN، PACKET TRACER

.