République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

ATE Department

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

Étude, Analyse, Critique d'un réseau existant et implémentation des solutions proposée sur simulateurs

Préparé par :

- Cheurfa Rana
- Djebari Sara

Dirigé par :

M. Bessaad Omar

M. Slimani Mennad

Examiné par :

M. Bellahsene Président

M. Khiredine Examinateur

Année universitaire : **2023/2024**

Dédicace

Je dédie ce mémoire :

À ***mes très chers parents*** *, aucune dédicace ne saurait exprimer adéquatement mon respect, mon amour éternel et ma profonde reconnaissance pour leur patience, leur amour, leurs encouragements et leurs sacrifices tout au long de mon parcours.*

À mes frères bien-aimés, ***Abdou*** *et* ***Badreddine*** *, je souhaite une vie pleine de réussite et de bonheur.*

À mon précieux soutien, ***Ch. Hakim*** *, pour sa patience lors de mes crises d'angoisse, et pour avoir toujours été à mes côtés pour me soutenir et me donner du courage.*

À ma chère binôme, pour les bons moments partagés durant ces quatre dernières années.

À tous ceux qui ont contribué, de près ou de loin, à la réalisation de ce travail, je vous adresse toute ma gratitude sincère.

RANA

Dédicace

Avec tous mes sentiments de respect et ma plus profonde reconnaissance, je dédie ma remise de diplôme et ma joie :

À celui qui m'a fait devenir la femme que je suis aujourd'hui, à la source de ma vie, à mon soutien constant, toujours à mes côtés pour me soutenir et m'encourager. ***Mon prince, Papa***

À mon paradis, à la lumière de mes yeux, à la source de ma joie et de mon bonheur, pour sa patience infinie et ses précieux conseils qui m'ont guidée tout au long de ma vie. ***Ma reine, Maman.***

À mon frère ***Riad****, pour l'amour qu'il me porte et sa présence rassurante.*

À ma sœur ***Lydia****, pour Sa présence, Son amour et Ses encouragements.*

À mes meilleures amies ***Kenza*** *et* ***Lydia****, pour leur amitié sincère et leur soutien sans faille.*

À ma binôme ***Rana****, avec qui j'ai partagé des moments inoubliables et des réalisations importantes tout au long de ce projet.*

À tous ceux qui ont contribué à ma réussite et à tous ceux qui m'aiment.

Sara

Remerciements

En premier lieu et avant tout, nous exprimons notre profonde gratitude à **Allah** Tout-Puissant, qui nous a donné la force et le courage nécessaires pour mener à bien ce travail.

Nous tenons à remercier notre directeur de mémoire, le professeur **BESSAAD OMAR** , pour son encadrement attentif, ses précieux conseils et son soutien constant tout au long de ce projet.

Nos sincères remerciements vont également aux membres du jury, pour avoir accepté d'évaluer notre mémoire et pour ses retours constructifs.

Nous exprimons notre gratitude au chef de département, le professeur **HADJI SLIMANE**, pour son soutien précieux et son engagement, qui ont grandement facilité la réalisation de ce mémoire.

Un remerciement tout particulier à notre enseignant **BELABBACI EL OUANAS**, dont l'aide exceptionnelle, la disponibilité et les conseils précieux ont été d'une valeur inestimable. Son soutien indéfectible et son implication ont été des piliers essentiels pour la qualité et le succès de notre travail. Son encouragement constant nous a motivés à surmonter les défis et à atteindre nos objectifs.

Nous remercions également tous nos enseignants et les employés du département ATE de l'université A.Mira Béjaia pour leur contribution à notre formation.

Nos remerciements s'adressent aussi aux personnels de l'entreprise CEVITAL-BEJAIA, en particulier à monsieur **SLIMANI MENNAD**, notre encadrant de stage, pour sa patience et son soutien tout au long de notre stage.

Nous tenons à exprimer nos meilleurs remerciements à nos parents, nos frères et sœurs, pour leur amour inconditionnel, leur patience et leur soutien indéfectible. Sans leur soutien moral et financier, ce travail n'aurait pas été possible.

Enfin, nous exprimons notre profonde gratitude à toutes les personnes qui ont contribué, de près ou de loin, à la réalisation de ce mémoire. Ce travail est le fruit de leur soutien et de leurs encouragements continus.

Table des matières

Table des figures

Liste des tableaux

Liste des acronymes

BPDU	*Bridge Protocol Data Units*
CD	*Collision Detection*
CLI	*Commande Langage Interface*
CSMA	*Carrier Sense Multiple Access*
DRH	*Directrice des ressources humaines*
DFC	*Direction Finances Comptabilité*
DG	*Direction générale.*
DHCP	*Dynamique Host Configuration Protocol*
DSI	*Directeur du système d'information*
FDDI	*Fiber Distributed Data Interface*
FTP	*File Transfer Protocole*
HSRP	*Hot Standby Router Protocol.*
HTTP	*Hyper Texte Transfer Protocole*
ID	*Identificateur*
IEEE	*Institute of Electric and Electronic Engeneer*
IP	*Internet Protocol.*
ISO	*International Organization for Standardization*
IT	*Information Technologie*
LAN	*Local Area Network.*
MAN	*Metropolitan Area Network.*

OSI *Open System Interconnexion*

PAN *Personal Area Network*

PC *Personale Computer*

PDU *Protocol Data Unit*

Rj45 *registered jack 45.*

STP *Spanning Tree Protocol.*

TCP *Transmission Control Protocol*

USB *Universal Serial Bus*

VLAN *Virtual Local Area Network.*

VTP *Virtual trunking Protocol.*

WAN *Wide Area Network*

Introduction Générale

Avec l'évolution des technologies informatiques, les réseaux locaux des entreprises se trouvent confrontés à des infrastructures de plus en plus complexes, nécessitant la conformité à diverses normes spécifiques en matière d'interconnexion d'équipements et de prise en charge d'application. Ainsi la mise en place d'un réseau local requiert une approche adaptée à l'architecture propre à chaque organisation, permettant de soutenir sa croissance tous en assurant la sécurité de ses services face aux menaces internes et externes . Au sein du groupe « Cevital-Bejaia ».

lors de notre stage, nous avons exploré les méthodes déployées par l'entreprise pour établir un réseau local répondant aux exigences d'interconnexion de tous les utilisateurs.

Le présent rapport est composé de quatre chapitre :

— **Le premier chapitre,** sera consacré à la présentation générale de l'entreprise Cevital, où notre stage s'est déroulé, ainsi qu'à la problématique de réseau existante qui sera le centre de notre travail.

— **Le second chapitre,** sera dédié aux réseaux informatiques, où nous aborderons les équipements réseaux utilisés dans l'entreprise ainsi que les protocoles mis en œuvre.

— **Le troisième chapitre,** nous étudierons, analyserons et critiquerons l'architecture de réseau existant de « Cevital », en proposant également quelques solutions. Ensuite, nous examinerons le réseau amélioré apporté par l'entreprise. Enfin, nous proposerons trois architectures différentes, en détaillant leurs avantages et inconvénients respectifs, afin de sélectionner la meilleure architecture pour le nouveau réseau de CEVITAL, en utilisant les simulateurs Cisco Packet Tracer.

— **Le quatrième chapitre,** sera consacré à notre proposition de nouvelle topologie de réseau, conçue pour répondre aux besoins de l'entreprise « Cevital

» et soutenir son développement continu, ainsi qu'à un test de validation de la configuration globale.

— **Enfin**, nous terminerons notre travail par une conclusion générale.

Chapitre I

Présentation de l'organisme d'accueil Cevital Agro- industriel

I.1 Introduction

Dans ce chapitre, nous présenterons l'entreprise CEVITAL, en détaillant ses départements et son historique. Nous aborderons également la problématique et les hypothèses qui structureront notre mémoire.

I.2 Présentation de l'entreprise

Cevital Agro-industrie, filiale du groupe Cevital a été créée en 1998 par Mr. Issad Rebrab, implantée au sein du port de Bejaïa c'est une entreprise privée algérienne et un acteur majeur du secteur agro-alimentaire [21]. voir la figure I.1

FIGURE I.1 – L'entreprise Cevital[1]

Le premier projet fut celui d'une raffinerie d'huile végétale, le création de l'entreprise cible volontairement les produits de base et de première nécessité pour le consommateur algérien, comme les huiles de table, la margarine, les graisses végétales, ou le sucre, à l'époque des secteurs largement placés sous monopole d'État, mais ouverts à l'importation [21].

Cevital Agro-industrie dispose de plusieurs unités de production amodernes telles que deux raffineries de sucre, une unité de sucre liquide, une raffinerie d'huile, une margarinerie, une unité de conditionnement d'eau minérale, une unité de fabrication et de conditionnement de boissons rafraîchissantes, une conserverie, une unité de fabrication de chaux calcinée [21].

Cevital Agro-industrie propose des produits haut de gamme à des tarifs concurrentiels, grâce à ses installations de pointe, son expertise reconnue, son engagement envers l'excellence et sa solide infrastructure de distribution. En répondant aux

demandes du marché national, l'entreprise a joué un rôle clé dans la transformation de l'Algérie, passant du statut d'importateur à celui d'exportateur pour les huiles, les margarines et le sucre [21].

Sa gamme de produits est distribuée dans divers pays, incluant l'Europe, le Maghreb, le Moyen-Orient et l'Afrique de l'Ouest [21].

I.3 Historiques du groupe Cevital

Année	**Industrie**
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 and distribution samsung création mfg (verre plat)
2008 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	CEVITAL rachète le Français OXXO, spécialisée dans la menuiserie PVC. Investi dans ALAS (Espagne) : Usine d'aluminium
2014	CEVITAL reprend les activités françaises du groupe FAGOR-Brandt : électroménager français. Investi dans AFFERPI (Italie) : usine de métal.

Table I.1 – Historique de Cevital [21].

I.4 Activités et produits de l'entreprise

I.4.1 Les Activités

I.4.1.1 L'activité de Cevital au niveau de la commune Béjaia

Cevital joue un rôle majeur dans l'économie locale de Bejaia en contribuant au développement de l'industrie agro-alimentaire à travers ses investissements dans des installations de pointe pour la production de margarine, le raffinage du sucre et des huiles, ainsi que le stockage des matières premières. Ces activités créent des milliers d'emplois directs et indirects [21].

Au niveau de Béjaia, Cevital contribue au secteur agro-alimentaire par :

— Production de margarine (120 000 tonnes par an)
— Raffinage du sucre (1 million de tonnes par an)
— Raffinage des huiles alimentaires (600 000 tonnes par an)
— Silos portuaires pour le stockage des matières premières

I.4.2 Les Produits

CEVITAL est concentré sur la fabrication et la commercialisation d'une gamme très diversifiée en matières de produits agro-alimentaires : des huiles végétales, margarine et sucre [23].

FIGURE I.2 – Les Produits de Cevital

1. Les huiles végétales :
   — Fleurial
   — Elio et Fridor
2. Margarinerie et graisses végétales :
   — Matina
   — Rania
   — Fleurial
   — MEDINA « SMEN »
3. Sucre :
   — sucre roux : Le sucre raffiné est conditionné dans des sachets de 50Kg et aussi commercialisé en morceau dans des boites d'1kg.

— sucre liquide

4. Boissons :
   — Eau minérale
   — Jus de fruits
5. Confitures
6. Sauces

I.5 Organigramme du complexe CEVITAL

I.5.1 Organigramme général du complexe CEVITAL

Cevital possède une organisation hiérarchisée avec diverses structures de direction, sous la supervision d'un directeur général. Ce dernier est chargé d'assurer la sécurité et la gestion optimale des ressources de l'entreprise.

Le directeur général et les directions assistantes forment la direction générale du complexe, qui est responsable de la coordination entre les autres directions. la représentation de la structure organisationnelle décomposée de cette direction générale peut être consultée dans la figure I.3 . Direction Commercial e B2B Directeur Commercial B2C [23].

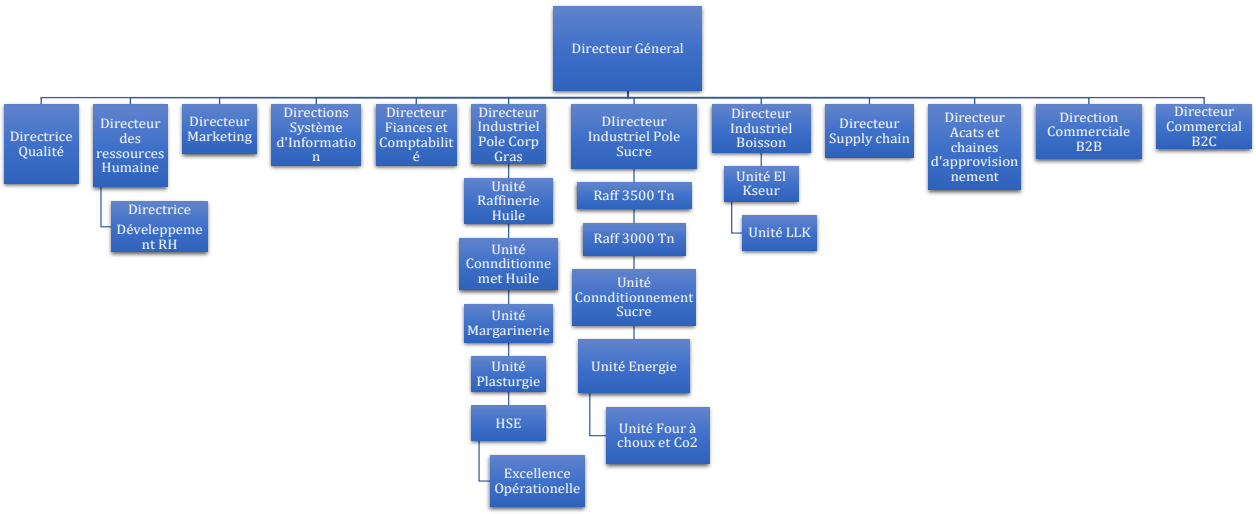


FIGURE I.3 – L'organigramme général de Cevital[2].

I.5.2 Organigramme de la direction système d'information

Cet organigramme permet de décrire de manière concise la structure hiérarchique typique de la DSI 'cevital' avec le directeur du système d'information en

tête, suivi des différents responsables de départements et leurs responsabilités.

La direction des systèmes d'information est chargée de superviser l'ensemble des activités informatiques de l'entreprise.

Elle a pour mission de fournir des solutions technologiques innovantes et fiables pour soutenir les opérations commerciales et stratégiques.

La DSI s'engage à garantir la sécurité et la disponibilité opérationnelle grâce à l'autorisation et à la faciliter l'innovation en collaborant avec les différents départements de l'entreprise.

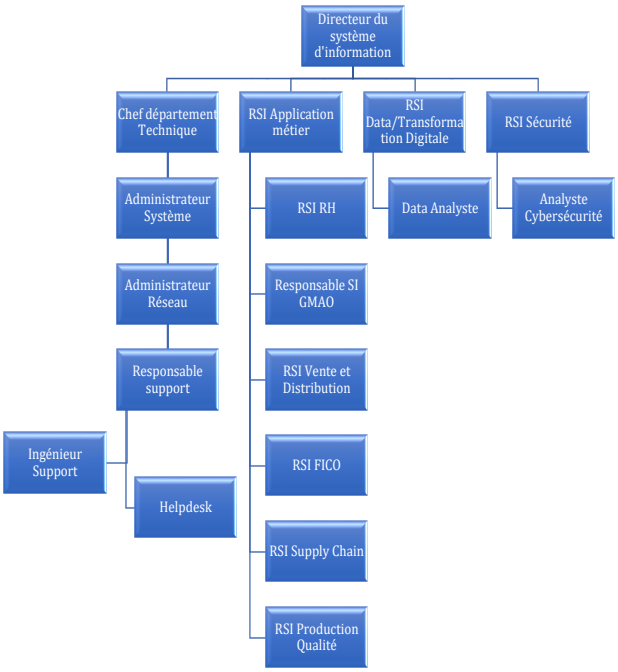


FIGURE I.4 – Organigramme de la direction système d'information[2].

I.6 Situation géographique

Cevital c'est le plus grand complexe privé en Algérie, il s'éntend sur une superficie de 4500 M2.

Il se situé à l'arrière port de Bejaia à une à une distance de 200 ML (Mètre linéaire) du quai à 3km sud-ouest de la ville à proximité de la RN 26 et la RN 09. Ce terrain à l'origine un marécage et une décharge publique a été partiellement récupéré grâce à une technologie avancée de consolidation des sols, comprenant l'installation de 337 Kilomètre de colonnes ballastées de 18 m chacune, ainsi qu'à l'expansion d'une partie sur la mer [24].

FIGURE I.5 – Situation géographique de Cevital[3].

I.7 La Problématique

Les réseaux des grandes entreprises requièrent une infrastructure solide, une administration experte, des mesures de sécurité avancées et une surveillance continue afin d'assurer leur fiabilité et leur efficacité. Une défaillance des réseaux pourrait entrainer une perturbation des activités commerciales, des risques accrus en matière de sécurité des données, une baisse de la productivité, une insatisfaction des clients et une détérioration de la réputation de l'entreprise. La problématique qui se pose est quelle stratégies et technologies pourraient être déployées afin d'assurer la continuité des services et maintenir un fonctionnement optimal du réseau informatique, même en cas de défaillance d'un ou plusieurs composants matériels ou logiciel.

Chapitre II

Définitions et Généralités sur les réseaux informatiques

II.1 Introduction

Les réseaux informatiques jouent un rôle fondamental en facilitant la connectivité et l'échange d'informations à l'échelle mondiale. Dans ce deuxième chapitre, nous allons rappeler brièvement quelques notions de base essentielles pour une meilleure compréhension du sujet. Ces concepts fondamentaux serviront de point de départ pour les analyses plus approfondies qui suivront.

II.2 Qu'est-ce qu'un réseau informatique ?

Un réseau informatique est un ensemble interconnecté d'appareils et de systèmes informatiques qui permettent le partage efficace de ressources et de données entre eux. Les réseaux informatiques sont conçus pour permettre la communication et la collaboration entre les utilisateurs, ainsi que l'accès aux informations et aux services à distance. Ils reposent sur une combinaison de matériel (ordinateurs, commutateurs, routeurs, serveurs, câbles...) et de logiciels (tels que des protocoles de communication et des systèmes d'exploitation réseau) pour assurer un fonctionnement fluide et fiable [25].

1. Objectifs des réseaux informatiques

Les réseaux informatiques ont plusieurs objectifs principaux qui peuvent varier en fonction des besoins spécifiques d'une organisation ou d'un environnement donné [14].

Partage de ressources : Les réseaux informatiques permettent le partage efficace de ressources telles que des imprimantes, des fichiers, des applications et des périphériques entre les utilisateurs du réseau. Cela facilite la collaboration et améliore la productivité au sein d'une organisation.

Communication : Les réseaux informatiques permettent la communication instantanée entre les utilisateurs, que ce soit par le biais de messageries électroniques, de chats en ligne, de vidéoconférences ou d'appels vocaux. Cela favorise la collaboration et la coordination des activités.

Accès à distance : Les réseaux informatiques permettent l'accès à distance aux ressources et aux services, ce qui permet aux utilisateurs de se connecter à partir de différents emplacements géographiques. Cela est particulièrement utile pour les travailleurs à distance, les voyageurs d'affaires et les succursales distantes d'une organisation.

Centralisation des données et des applications : Les réseaux informatiques permettent de centraliser les données et les applications sur des serveurs, ce qui facilite la gestion et la sauvegarde des informations critiques. Cela permet

également une gestion plus efficace des mises à jour logicielles et des correctifs de sécurité.

Économies d'échelle : Les réseaux informatiques permettent de réaliser des économies d'échelle en partageant les ressources et en évitant la duplication des équipements et des données. Cela permet également de réduire les coûts liés à l'administration et à la maintenance des systèmes informatiques.

Sécurité des données Les réseaux informatiques permettent de mettre en œuvre des mesures de sécurité pour protéger les données sensibles contre les accès non autorisés, les altérations et les pertes. Cela comprend la mise en place de pare-feu, de systèmes de détection des intrusions, de cryptage des données et de contrôles d'accès.

Fiabilité et disponibilité : Les réseaux informatiques sont conçus pour être fiables et disponibles, assurant un accès continu aux ressources et aux services même en cas de défaillance matérielle ou de perturbation du réseau. Cela est souvent réalisé par la mise en place de redondances et de mécanismes de sauvegarde.

II.3 Les composants de base d'un réseau

"La mise en œuvre d'une communication entre deux ou plusieurs nœuds dans un réseau nécessite la mise en place de 3 types de composants :

Les supports de transmission : sont tout moyen permettant de transporter des données sous forme de signaux de leur source vers leur destination.

Les équipements d'interconnexion : servent à connecter plusieurs machines entre elles, comme : les cartes réseaux, les switchs, les routeurs, les modems, etc.

Les protocoles de communication : sont des règles établies entre l'émetteur et le récepteur des données [25].

II.4 Les différents types de réseaux :

La diversité des réseaux informatiques est définie par leur taille, le nombre de machines qu'ils connectent, leur vitesse de transfert des données et leur étendue géographique. Cette variété permet de les classer en différentes catégories, chacune adaptée à des besoins spécifiques en termes de connectivité et de performances.

PAN (Personal Area Network)

Le réseau personnel représente une infrastructure de communication restreinte en termes d'équipements. Il est également connu sous d'autres appellations telles que réseau domestique ou réseau individuel. Souvent déployée dans un espace

de quelques mètres (Bluetooth et le Wi-Fi direct), allant jusqu'à une dizaine de mètre (ZigBee), destiné à couvrir de petites zones : les maisons privées, les espaces de travail individuels. Conçu pour faciliter l'échange d'informations entre des périphériques tels qu'un ordinateur portable, un smartphone, une tablette. Ce type de réseau peut être mis en place à l'aide de connexions filaires (USB) ou sans fil (Bluetooth, ZigBee), offrant ainsi une flexibilité accrue en matière de déploiement et d'utilisation[26].

FIGURE II.1 – Réseau PAN[4]

LAN (Local Area Network)

Les réseaux locaux (LAN) sont des infrastructures de communication informatique conçues pour des environnements restreints tels que les domiciles ou les locaux d'entreprise. Leur principal rôle est de permettre aux appareils connectés de partager des ressources et des données de manière efficace. Qu'il s'agisse d'un réseau domestique basique ou d'un réseau d'entreprise complexe, un LAN peut relier au moins deux appareils et jusqu'à plusieurs milliers, offrant ainsi une grande flexibilité d'utilisation. En termes de vitesse, les LAN peuvent fournir des débits de données allant de 10 à 1000 Mbps, adaptés aux besoins variés des utilisateurs[27, 28].

FIGURE II.2 – Réseau LAN[5]

MAN (Metropolitan Area Network)

Les réseaux Metropolitan Area Network (MAN) sont spécifiquement conçus pour couvrir une métropole en reliant plusieurs réseaux locaux (LAN) répartis sur divers sites urbains. Typiquement, la portée géographique de ces réseaux ne dépasse pas 200 kilomètres. Leur objectif principal est de fournir une connectivité à haut débit, avec des débits dépassant souvent les 1000 Mbps. Ces performances sont rendues possibles grâce à l'utilisation de technologies telles que le WiMAX, qui permettent une interconnexion efficace des réseaux dans des environnements urbains dynamiques[29, 30].

FIGURE II.3 – Réseaux Man[6]

WAN (Wide Area Networks)

Les réseaux WAN, étendant leur emprise sur des pays voire des continents, unissent des réseaux LAN et MAN pour connecter des sites éloignés. Leur mission : faciliter un échange sécurisé et fluide de données sur de vastes distances, qu'elles soient transmises par des connexions filaires comme Internet ou sans fil via les technologies 4G/5G[31, 32].

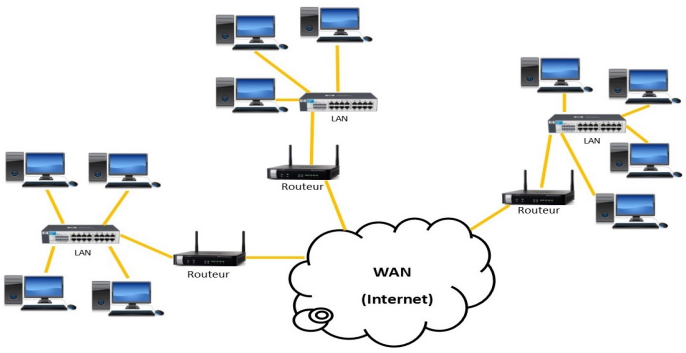


FIGURE II.4 – Réseau WAN[7]

II.5 Les topologies des réseaux informatiques

Une topologie de réseau informatique correspond à l'architecture (physique ou logique) de celui-ci, définissant les liaisons entre les équipements du réseau et une hiérarchie éventuelle entre eux.

Elle peut définir la façon dont les équipements sont interconnectés et la représentation spatiale du réseau (topologie physique). Elle peut aussi définir la façon dont les données transitent dans les lignes de communication (topologies logiques) [33].

II.5.1 Les topologies physiques

Il existe plusieurs topologies physiques, parmi lesquelles on retrouve principalement :

1. **Topologie en bus :** La topologie en bus est une configuration linéaire, dans laquelle tous les ordinateurs sont connectés par un seul câble (bus) par l'intermédiaire d'un connecteur. Le bus est constitué d'un câble coaxial. Il présente une impédance caractéristique de 50Ω. Chaque extrémité du bus est bouclée sur un bouchon" dont l'impédance électrique est égale à l'impédance caractéristique du câble. Sur un bus les signaux sont envoyés à tous les ordinateurs du réseau. Pour éviter que les signaux rebondissent d'un bout à l'autre du câble, on doit placer un bouchon de terminaison à l'extrémité du câble [34].

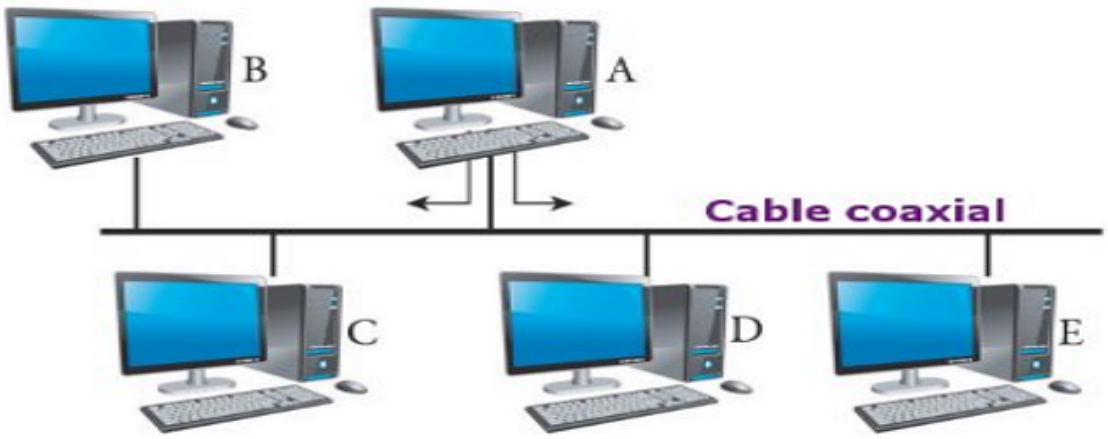


FIGURE II.5 – Topologie en Bus [8].

— **Les Avantages :**
  — la plus facile à mettre en place.
  — Economique en câble et en prix.
  — Simple et fiable
— **Les Inconvénients :**

- Les machines ne peuvent pas communiquer en même temps car il y a risque de collision ou de conflit.
- Si un défaut de connexion survient, tout le réseau tombe en panne.
- En cas de coupure du câble le réseau est interrompu.
- Ralentissement du trafic en cas de nombreuses stationsu.

2. **Topologie en étoile (star) :**La topologie en étoile est la topologie la plus fréquente. Chaque unité (équipement) est reliée à un nœud central (HUB ou SWITCH) par l'intermédiaire d'un câble à paires torsadées. Les connecteurs sont de type RJ45 [34].

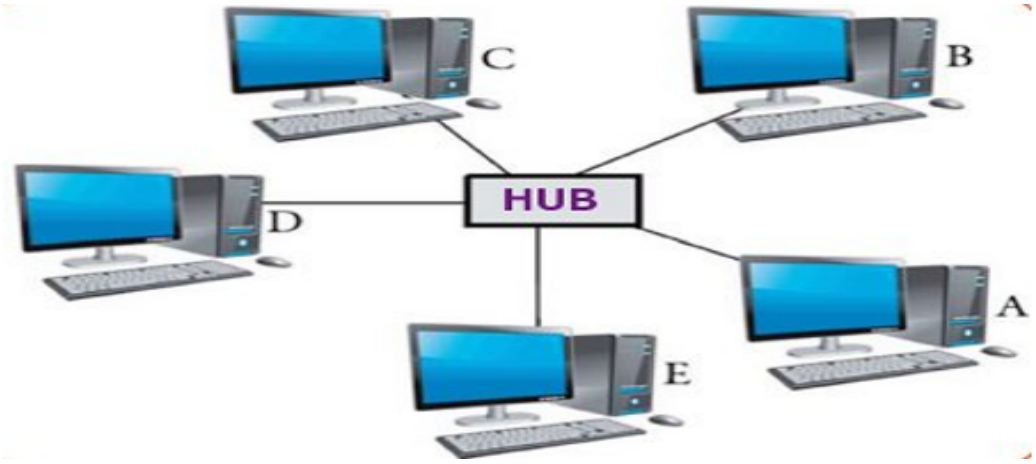


FIGURE II.6 – Topologie en étoile [8].

- **Les Avantages :**
  - Simple dans la réalisation
  - Ajout facile d'équipement
  - Gestion centralisée
  - Une panne d'ordinateur est sans incidence sur le réseau.
- **Les Inconvénients :**
  - Si le site central (hub ou switch) tombe en panne, tout le réseau est mis hors service.
  - Le cout de l'appareil central s'ajoute par rapport à la topologie en bus.
  - Utilisation beaucoup de câble.

3. **Topologie anneau :**Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. Les ordinateurs sont reliés à un seul câble en anneau, les signaux transitent dans une seule direction, chaque ordinateur joue le rôle de répéteur, régénérant le signal. Elle utilise la méthode d'accès à "jeton" (Token ring).

Les données transitent de stations en stations en suivant l'anneau qui chaque fois régénèrent le signal. Le jeton détermine quelle station peut émettre, il est transféré à tour de rôle vers la station suivante [34].

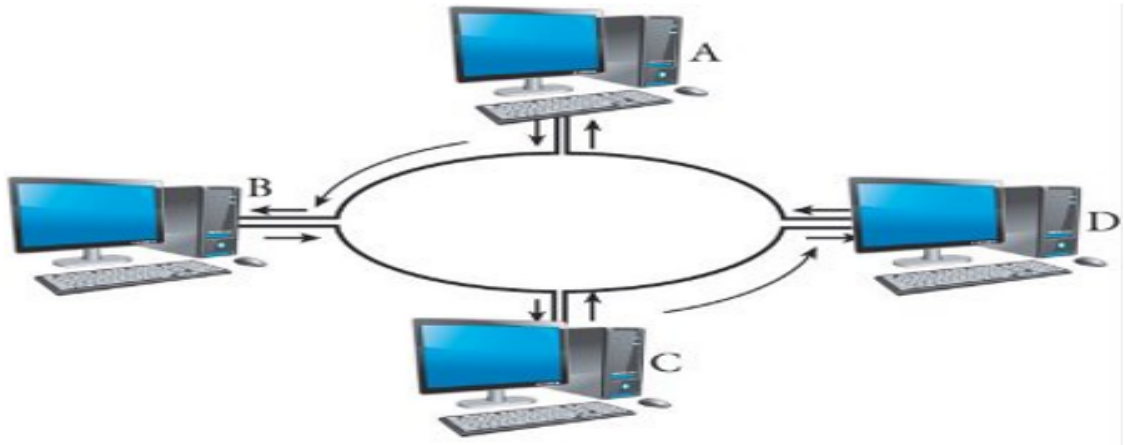


FIGURE II.7 – Topologie en anneau[8].

— **Les Avantages :**
  — Topologie active (chaque station régénère le signal).
  — Accès égalitaire de toutes les stations.
  — Performances régulières même avec un grand nombre de stations .
— **Les Inconvénients :**
  — Une panne d'un ordinateur met le réseau hors service.
  — S'il y a une panne ou une coupure du câble c'est tout le réseau qui est en panne.

4. **Topologie en maille (mesh) :** Internet est une topologie maillée (sur le réseau étendu « WAN », elle garantit la stabilité en cas de panne d'un nœud). Les réseaux maillés utilisent plusieurs chemins de transferts entre les différents nœuds. C'est une structure réseau hybride reprenant un câblage en étoile regroupant différents nœuds de réseaux. Cette méthode garantit le transfert des données en cas de panne d'un nœud [35].

— **Les Avantages :**
  — Garantie d'une meilleure stabilité du réseau en cas d'une panne du nœud
  — Assure la sécurité et la confidentialité.
— **Les Inconvénients :**
  — Difficile à mettre en œuvre et ne peut être utilisé que dans les réseaux internes Ethernet.
  — Très coûteuse en câblage.

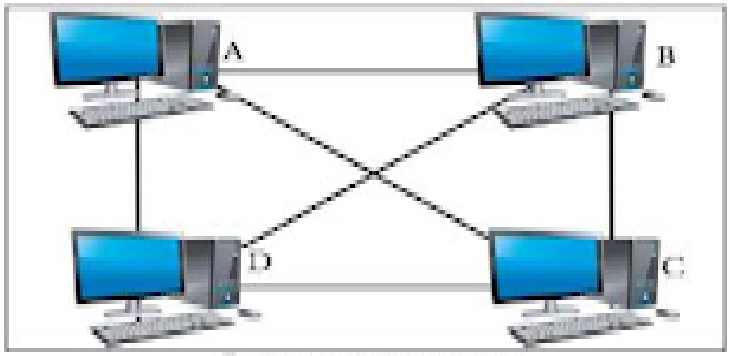


FIGURE II.8 – Topologie en maille [8].

5. **Topologie en arbre :** Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur [18].

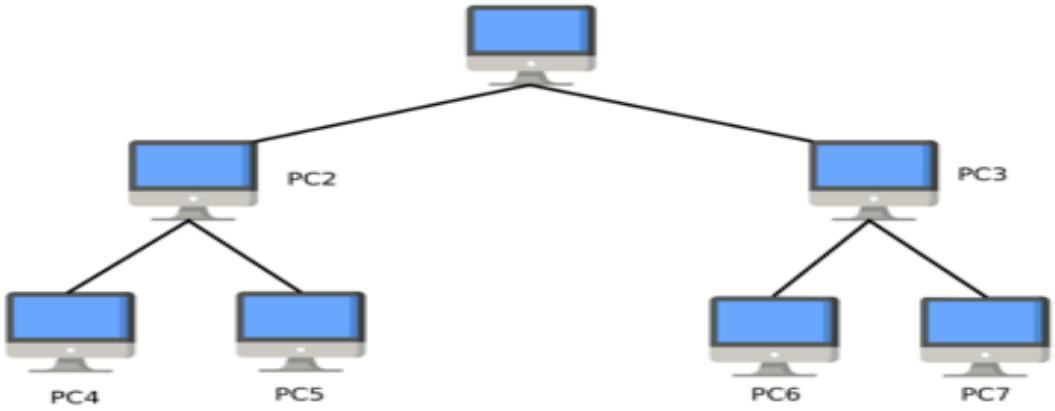


FIGURE II.9 – Topologie en arbre [8].

— **Les Avantages :**
  — La topologie en arbre divise l'ensemble du réseau en plusieurs parties qui sont facilement gérables
  — Elle fournit assez de place pour l'expansion future du réseau.
— **Les Inconvénients :**
  — Un échec de la plate-forme centrale ou de l'échec du câble principal de données principale, peuvent paralyser l'ensemble du réseau .
  — Avec l'augmentation de la taille au-delà d'un point, la gestion devient difficile.

6. **Topologie en hybride :** Une topologie hybride est une topologie de réseau dans laquelle deux topologies différentes ou plus sont combinées pour former un réseau plus vaste. Par exemple, vous pouvez avoir une topologie en étoile

pour chaque service de votre organisation, puis les connecter à une topologie de bus pour former un réseau hybride. La fusion de deux réseaux n'est pas une topologie hybride si les réseaux à fusionner ont le même type de topologie. Par exemple, un réseau qui utilise une topologie en bus est combiné avec un autre réseau qui utilise une topologie en bus, de sorte que la fusion des deux réseaux reste la topologie en bus au lieu de la topologie hybride. La topologie hybride portera les caractéristiques de la topologie d'origine qui l'a construite [34].

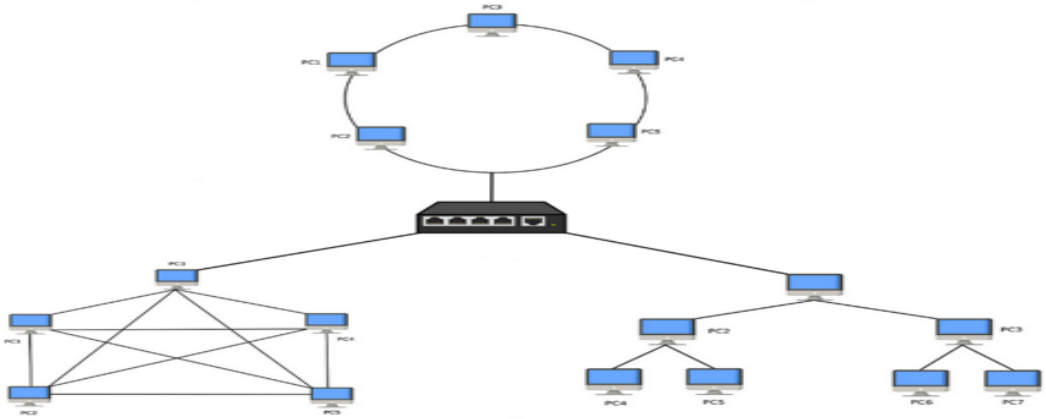


FIGURE II.10 – Topologie en hybride[8].

— **Les Avantages :**
  — Une erreur de réseau ne sera pas affecter les performances du reste du réseau, les défauts sont efficacement diagnostiqués et isolés.
  — Les topologies hybride sont fiables et ont une meilleure tolérance aux pannes que d'autres topologies .
  — possibilité d'utiliser les aspects les plus fortes d'autres réseaux , par exemple , la force du signal.
— **Les Inconvénients :**
  — L'installation et la configuration du réseau sont compliquées, car il doit connecter plusieurs topologies différentes.
  — Les coûts de maintenance du réseau sont également assez chers.

II.5.2 Les topologies logiques

Les topologies logiques les plus courantes sont Ethernet , Token Ring et FDDI.

1. **Ethernet :** Ethernet est une technologie de réseau local très répandue. Elle fait appel au protocole CSMA/CD (Carrier Sense Multiple Access with Collision Detection) entre les clients, et peut être utilisée avec différents types de câbles. Un réseau Ethernet est passif, ce qui signifie qu'il fonctionne sans

alimentation électrique. C'est pourquoi il ne peut tomber en panne que si le câble est coupé physiquement ou que ses terminaisons sont incorrectes. Un réseau Ethernet est connecté au moyen d'une topologie en bus, dans laquelle le câble est terminé aux deux extrémités [36].

— **Méthode d'accès :** La méthode d'accès au réseau utilisée avec Ethernet est appelée CSMA/CD. CSMA/CD est un ensemble de règles qui déterminent la façon dont les périphériques du réseau répondent lorsque deux de ces périphériques tentent de transmettre simultanément des données sur le réseau.

La transmission simultanée de données par plusieurs ordinateurs provoque une collision. Tous les ordinateurs du réseau, clients et serveurs, vérifient le câble sur lequel s'effectue le trafic réseau. Un ordinateur ne transmet des données que lorsqu'il détecte que le câble est libre et exempt de trafic. Une fois que l'ordinateur a transmis des données sur le câble, aucun autre ordinateur ne peut transmettre des données tant que les données d'origine n'ont pas atteint leur destination, libérant ainsi le câble. Lorsqu'il détecte une collision, un périphérique attend pendant un délai aléatoire, puis tente de retransmettre le message. S'il détecte de nouveau une collision, il attendra deux fois plus longtemps avant de retransmettre le message.

— **Vitesse de transfert :**
Le réseau Ethernet standard, appelé 10BaseT, prend en charge des vitesses de transfert de données de 10 Mb/s sur divers types de câbles. Il existe aussi des versions plus rapides d'Ethernet. Fast Ethernet (100BaseT) autorise des vitesses de transfert de données de 100 Mb/s et Gigabit Ethernet de 1 Gb/s, soit 1 000 Mb/s.

2. **Token Ring :**
Les réseaux Token Ring sont implémentés dans une topologie en anneau. La topologie physique d'un réseau Token Ring est la topologie en étoile, dans laquelle tous les ordinateurs du réseau sont physiquement connectés à un concentrateur. La topologie logique représente le chemin, de forme annulaire, parcouru par le jeton entre les ordinateurs [36].

— **Méthode d'accès :**
La méthode d'accès utilisée dans un réseau Token Ring est le passage de jeton. Un ordinateur ne peut transmettre des données sans posséder le jeton. Lorsqu'un ordinateur prend le contrôle du jeton, il envoie une trame de données qui circule sur l'anneau jusqu'à l'ordinateur destinataire. Une fois reçue, la trame est copiée en mémoire par l'ordinateur destinataire, marquée comme reçue, puis renvoyée à l'expéditeur. Enfin,

l'expéditeur retire la trame de l'anneau et envoie un nouveau jeton pour permettre la transmission suivante

— **Vitesse de transfert :** La vitesse de transfert d'un réseau Token Ring est comprise entre 4 et 16 Mb/s.

3. **FDDI (Fiber Distrubuted Data Interface) :**
Un réseau FDDI permet d'établir des connexions rapides pour différents types de réseaux, offrant des vitesses supérieures à Ethernet et Token Ring. Il peut servir de dorsale rapide pour plusieurs réseaux locaux de faible capacité. Un réseau FDDI est composé de deux anneaux, un principal et un secondaire, transmettant dans des directions opposées. En cas de problème avec l'anneau principal, le réseau se reconfigure pour transférer les données sur l'anneau secondaire, assurant ainsi la continuité du service [36].

— **Méthode d'accès :** La méthode d'accès utilisée dans un réseau FDDI est le passage de jeton, où un ordinateur peut transmettre plusieurs paquets dans un délai prédéfini avant de restituer le jeton. Contrairement au réseau Token Ring traditionnel qui ne permet de faire circuler qu'une seule trame à la fois, le FDDI permet à plusieurs paquets de circuler simultanément sur l'anneau.

— **Vitesse de transfert :** La vitesse de transfert d'un réseau FDDI est comprise entre 155 et 622 Mb/s.

II.6 Les modèles de références

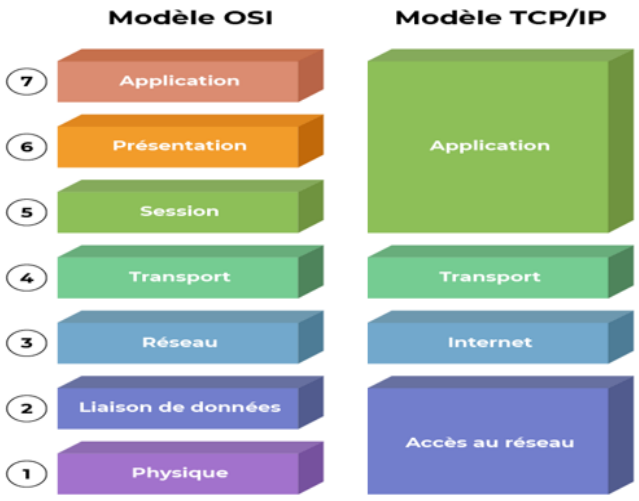


FIGURE II.11 – Comparaison des modèles OSI et TCP/IP [9].

II.6.1 Le modèle OSI

Le modèle OSI, développé par l'ISO, est une architecture qui guide la conception et le fonctionnement des réseaux informatiques. Il divise le processus de communication en sept couches numérotées de 1 à 7, réparties en couches basses (couches 1 à 3) et couches hautes (couches 4 à 7). Les couches sont classées par ordre d'abstraction de la moins logique à la plus logique. Chacune est responsable de fonctions spécifiques. De plus, il existe des unités de données correspondantes à chaque couche appelées PDU (Protocol Data Unit) [25, 15, 37].

— **Couche 1 (Physique) :** La couche physique gère la transmission des données binaires sur les supports physiques comme les signaux électriques, électromagnétiques ou optiques. Elle choisit également le codage et la modulation appropriés. L'unité de données PDU de cette couche est le bit.

— **Couche 2 (Liaison de Données) :** assure le maintien de la connexion logique, gère l'adressage et le transfert de données sous forme de trames, tout en assurant la détection et la correction des erreurs qui peuvent survenir au niveau physique du réseau. La PDU utilisée à cette couche est la trame.

— **Couche 3 (Réseau) :** responsable de l'adressage logique des équipements, gère les communications entre les ordinateurs sur différents réseaux en acheminant les données d'un réseau à un autre via les routeurs et les protocoles de routage. À ce niveau, la PDU utilisée est le paquet.

— **Couche 4 (Transport) :** segmente les données en petits paquets appelés segments, gère les problèmes de transport tels que le renvoi des données manquantes, et assemble tous les segments à la réception pour reconstituer le message original, tout en contrôlant également le flux de données.

— **Couche 5 (Session) :** facilite l'échange de données et la communication entre les applications en fournissant des services de dialogue, de synchronisation et de gestion de session. La PDU associée à cette couche est le "datagramme", qui encapsule les données de la session ainsi que les informations de contrôle nécessaires pour assurer la cohérence et la fiabilité des échanges entre les applications.

— **Couche 6 (Présentation) :** est responsable de garantir la cohérence et la sécurité des données lors de leur transfert entre les applications, en convertissant les formats, en gérant les encodages et en assurant le chiffrement.

— **Couche 7 (Application) :** est le point de départ et d'arrivée de toutes les données à transmettre via le réseau, elle réunit des applications telles que la messagerie électronique, le transfert de fichiers (FTP), la gestion de bases de données et la navigation sur le web (HTTP).

II.6.2 Le modèle TCP/IP

Le modèle de référence TCP/IP (Transmission Control Protocol /Internet Protocol) a été développé par le ministère américain de la Défense pour garantir la résilience d'un réseau, même en cas de guerre nucléaire. L'objectif était d'assurer la connectivité ininterrompue des paquets de données, quelles que soient les circonstances. Ce défi complexe a conduit à la création du modèle TCP/IP, devenu depuis la norme fondamentale d'Internet. Ce modèle se compose de quatre couches distinctes : l'application, le transport, l'Internet et l'accès au réseau. Il est important de noter que certaines couches du modèle TCP/IP partagent des noms avec celles du modèle OSI. Il est crucial de ne pas confondre les fonctions des différentes couches entre ces deux modèles, notamment en ce qui concerne la couche application, qui diffère significativement d'un modèle à l'autre [38].

— **La couche application :**

La couche application dans le modèle TCP/IP gère les protocoles de haut niveau tels que la représentation des données, le codage des données et le contrôle du dialogue entre les applications.

— **La couche transport :**

La couche transport assure la fiabilité, le contrôle de flux et la correction des erreurs. Le protocole TCP fournit des communications réseau fiables et à faible taux d'erreurs. TCP est orienté connexion : il établit un dialogue entre les ordinateurs source et destination. Il prépare les données de la couche application en segments pour une transmission efficace.

— **La couche Internet :**

Le rôle de la couche Internet consiste à envoyer des paquets source à partir d'un réseau quelconque de l'interréseau et à les faire parvenir à destination, indépendamment du trajet et des réseaux traversés pour y arriver. Le protocole qui régit cette couche est appelé protocole IP (Internet Protocol). L'identification du meilleur chemin et la commutation de paquets ont lieu au niveau de cette couche.

— **La couche d'accès au réseau :**

Cette couche se charge de tout ce dont un paquet IP a besoin pour établir une liaison physique, puis une autre liaison physique. Cela comprend les détails sur les technologies LAN et WAN, ainsi que tous les détails dans les couches physique et liaison de données du modèle OSI.

II.7 Les Protocoles Virtuels

II.7.1 Virtual Local Area Network (VLAN)

Le terme "VLAN" se décompose en deux parties : "LAN" qui désigne un réseau local, auquel s'ajoute la lettre "V" pour virtuel. Ainsi, un VLAN représente un concept de réseau local virtuel. C'est une technologie de réseau informatique qui permet de diviser un réseau physique en plusieurs sous-réseaux logiques. Chaque VLAN est identifié par un numéro de VLAN unique. Dans un VLAN donné, la communication est autorisée uniquement entre les machines appartenant à ce VLAN [25, 39, 40].

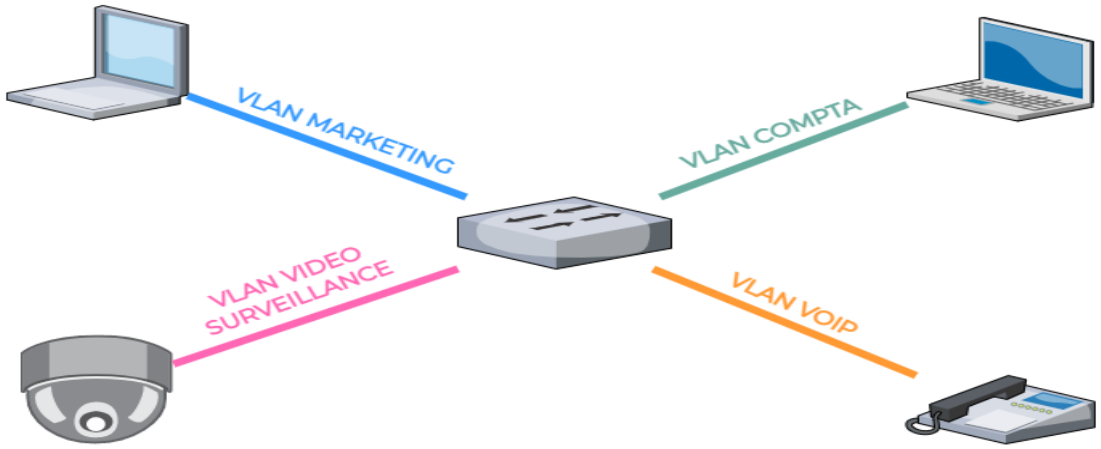


FIGURE II.12 – VLAN[10]

Les avantages des VLANs

1. **Evolutivité et réduction des coûts :** pour s'adapter aux changements de tailles et de structure, et optimiser l'utilisation des ressources existantes.
2. **Sécurité renforcée :** en segmentant le réseau pour limiter l'accès non autorisé aux ressources sensible.
3. **Simplification de la gestion réseau :** en organisant les ressources de manière logique et en facilitant la configuration des paramètres réseau.
4. **Optimisation de la bande passante :** en segmentant le trafic réseau selon les besoins.
5. **La réduction broadcast :** en limitant la propagation des trames de diffusion aux périphériques du même VLAN.
6. **Mobilité accrue :** en permettant aux utilisateurs de se déplacer dans le réseau sans perdre leur connectivité.
7. **Isolation des problèmes :** limitant leur impact et facilitant leur résolution [39, 40].

Les Type de VLAN

1. **VLAN niveau 1 (Port-Based VLAN) :** ces VLAN attribuent des ports physiques sur un commutateurs à un VLAN spécifique.
2. **VLAN niveau 2 (Mac Address-Based VLAN) :** attribuent les trames à un VLAN en fonction de l'adresse MAC source de l'émetteur.
3. **VLAN niveau 3 :** il existe deux types.
   - VLAN par sous-réseau (Network Address-Based VLAN) : segmenter les sous-réseaux selon l'adresse IP source de l'émetteur.
   - VLAN par protocole (Protocole-Based VLAN) : utilisent le type de protocole ou d'encapsulation pour attribuer les trames à un vlan spécifique [25, 37, 39].

II.7.2 VLAN Trunking protocol (VTP)

II.7.2.1 Définition

VLAN Trunking Protocol est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques Cisco. VTP permet d'ajouter, renommer ou supprimer un ou plusieurs réseaux locaux virtuels sur un seul commutateur (le serveur) qui propagera cette nouvelle configuration à l'ensemble des autres commutateurs du réseau (clients). VTP permet ainsi d'éviter toute incohérence de configuration des VLAN sur l'ensemble d'un réseau local [26]. VTP fonctionne sur les commutateurs Cisco dans un de ces 3 modes :

- **VTP server :** commutateurs qui crée les annonces VTP .
- **VTP client :** commutateurs qui reçoit, se synchronise et propage les annonces VTP.
- **VTP transparent :** commutateurs qui ne traite pas les annonces VTP.

Les messages VTP se propagent sur les liens configurés en Trunk (norme 802.1Q) et pas en Access.

VTP ne gère que la plage de VLAN comprise entre 1 et 1005. La plage étendue 1006 à 4096 n'est pas supportée. Pour cela, il faut basculer en mode Transparent sur tous les switchs et créer ses VLANS étendus [26].

II.7.2.2 Concept du protocole VTP

Les administrateurs peuvent changer les informations de VLAN sur les commutateurs fonctionnant en mode serveur uniquement. Une fois que les modifications sont appliquées, elles sont distribuées à tout le domaine VTP au travers des liens « trunk » (Cisco ISL ou IEEE 802.1Q).

En mode transparent, le switch reçoit les mises à jour et les transmet à ses voisins sans les prendre en compte. Il peut créer, modifier ou supprimer ses propres VLAN mais ne les transmet pas. Les switchs en mode client appliquent automatiquement les changements reçus du domaine VTP[41].

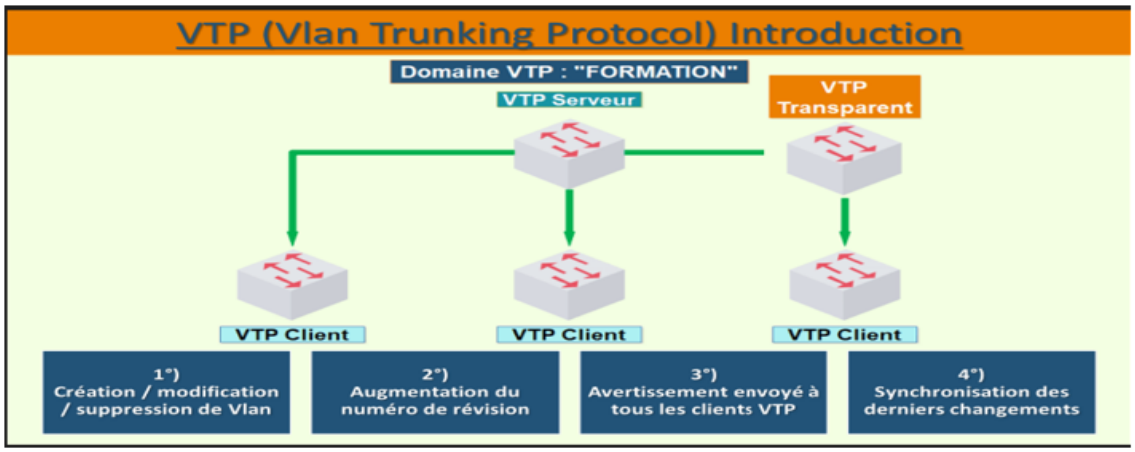


FIGURE II.13 – Concept VTP [11].

II.8 Les protocoles de redondance

II.8.1 STP (Spanning Tree Protocol)

Le protocole Spanning Tree Protocol (STP), défini dans la norme IEEE 802.1D, est un Protocole de la couche 2 utilisé dans les réseaux commutés pour éviter la création des boucles de communication tout en permettant l'utilisation de liens redondants.

Dans un réseau commuté, STP coordonne une série d'élections pour attribuer des rôles à chaque commutateur. Tout d'abord, le commutateur racine, appelé root bridge, est élu en fonction des priorités configurées, avec une préférence pour l'adresse MAC la plus basse en cas d'égalité de priorité. Ensuite, chaque commutateur détermine son port racine (root port) en sélectionnant celui offrant le chemin le plus court vers le root bridge, basé sur le coût du trajet. Chaque commutateur ne peut avoir qu'un seul root port.

Enfin, les ports désignés ((designated port)) sont identifiés en choisissant le port connecté au segment offrant le chemin le plus direct vers le root bridge. Les autres ports sont alors mis en état de blocage pour éviter les boucles de commutation. Chaque commutateur échange des données concernant la sélection du commutateur racine et la configuration réseau ultérieure via des messages BPDU (Bridge Protocol Data Units), comparant les paramètres BPDU émis avec ceux reçus de leurs voisins [42, 43, 44, 45].

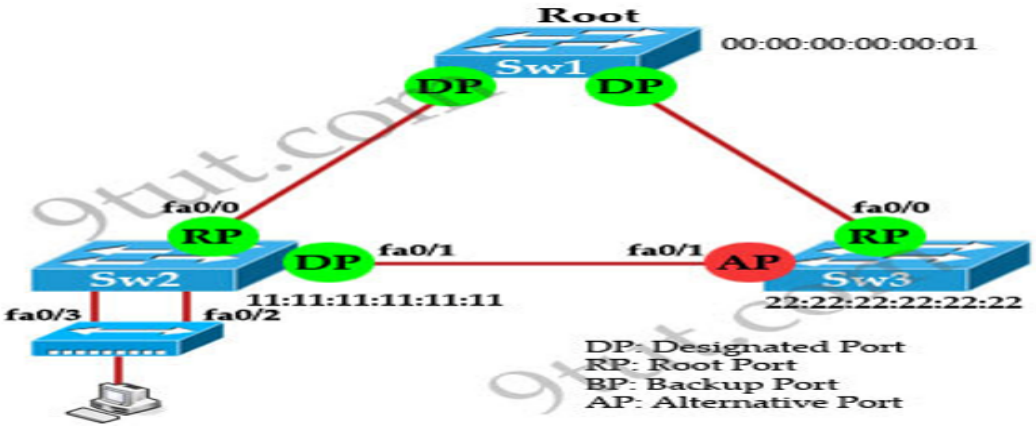


FIGURE II.14 – fonctionnement de STP[12].

II.8.2 HSRP (Hot Standby Router Protocol)

II.8.2.1 Définition

HSRP est un protocole propriétaire de Cisco implémenté sur les routeurs et les commutateurs de niveau 3 .Il permet de gérer la redondance de routeur pour que lorsqu'un routeur (ou un commutateur de niveau 3) tombe en panne un routeur (ou un commutateur de niveau 3) de secours prenne le relais. HSRP permet d'augmenter la tolérance de panne sur un réseau en créant un routeur virtuel à partir de 2 routeurs physiques (ou plus), une élection déterminera le routeur actif et les autres routeurs seront en "attente" (standby). L'élection du routeur actif est réalisée grâce à la priorité configurée sur chaque routeur [46].

II.8.2.2 Fonctionnement de HSRP

En pratique, HSRP permet qu'un routeur de secours (ou Spare) prenne immédiatement, de façon transparente, le relais dès qu'un problème physique apparaît. En partageant une seule et même adresse IP et MAC, plusieurs routeurs peuvent être considérés comme un seul routeur "Virtuel".

Les membres du groupe de ce routeur virtuel sont capables de s'échanger (Multicast) des messages d'état et des informations. Un routeur physique peut donc être "responsable" du routage et un autre en redondance Si le routeur, que nous appellerons primaire, a un problème, le routeur secondaire prendra sa place automatiquement.

Un groupe de routeurs va négocier au sein d'un même groupe HSRP (ou standby group), un routeur primaire (Active router), élu au moyen d'une priorité, pour transmettre les paquets envoyés au routeur virtuel. Un autre routeur, le routeur secondaire (Standby router), sera élu lui aussi afin de remplacer le routeur primaire en cas de problème.

Le secondaire assumera donc la tâche de transmettre les paquets à la place du primaire en cas de défaillance.

Le processus d'élection se déroule pendant la mise en place des liens, une fois ce processus terminé, seul le routeur primaire (Active) va envoyer des messages HSRP multicast en UDP aux autres afin de minimiser Redondance de routeur avec HSRP le trafic réseau. Si ces messages ne sont plus reçus par le routeur secondaire (Standby), c'est que le routeur primaire à un problème et le secondaire devient donc Actif.

L'élection se fait un peu à la manière de spanning-tree, en prenant en compte une priorité. Cette priorité est composée d'un paramètre "priority" compris entre 1 et 255 (255 étant le plus prioritaire) et de l'adresse IP de l'interface. A priorités statiques égales, la plus haute adresse IP sera élue.

Plusieurs groupes HSRP peuvent exister au sein d'un même routeur sans que cela ne pose problème (depuis l'IOS 10.3). Seuls les routeurs du même numéro de groupe s'échangeront les messages HSRP.

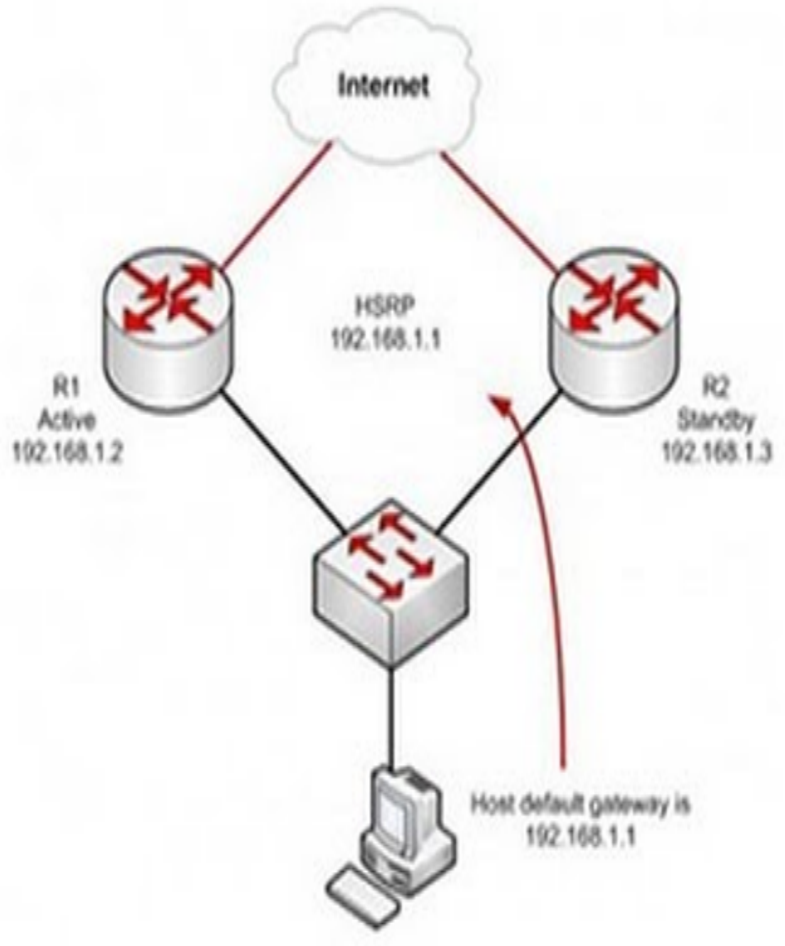


FIGURE II.15 – fonctionnement de HSRP[13].

II.9 Adressage IP et masque de réseau

II.9.1 L'adressage IP

1. **Adresse IP**

   Une adresse IP (Internet Protocol) est un identifiant unique attribué à chaque ordinateur connecté à un réseau. Elle est composée de quatre nombres compris entre 0 et 255, séparés par des points [47].

2. **Parties d'une adresse IP**

   — **ID de Réseau** : Les nombres à gauche de l'adresse IP qui désignent le réseau.

   — **ID Hôte** : Les nombres à droite de l'adresse IP qui désignent l'ordinateur sur ce réseau.

3. **Classes d'adresses IP**

   — Classe A : 0 à 127

   — Classe B : 128 à 191

   — Classe C : 192 à 223

   — Classe D : 224 à 239

   — Classe E : 240 à 255

   Les adresses IP de Classe D et E sont réservées à des utilisations spécifiques et ne sont pas utilisées pour l'identification des ordinateurs sur un réseau local.

4. **Adresse privée**

   — Les adresses IP privées sont des plages d'adresses réservées pour une utilisation interne dans les réseaux locaux. Elles ne sont pas routables sur Internet et ne peuvent pas être utilisées pour communiquer directement avec des ordinateurs en dehors du réseau local [47].

   — Elles sont utilisées pour :

      — éviter les conflits avec les adresses IP publiques sur Internet.

      — permettre une plus grande flexibilité dans la gestion des réseaux locaux [32][33].

5. **Plages d'adresses IP privées**

   — 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

II.9.2 Masque de réseau

Le masque de sous-réseau est utilisé pour séparer la partie réseau de la partie machine d'une adresse IP. Il est composé de quatre octets, comme une adresse IP.

L'utilisation et la maîtrise des masques de sous-réseau doivent pouvoir vous permettre d'une part, de savoir ce que vous manipulez, et d'autre part d'optimiser le fonctionnement de votre réseau. Effectivement, l'utilisation des masques vous permettra de segmenter de la façon la plus correcte l'adressage de votre réseau, et ainsi de séparer les machines sensibles du reste du réseau, limiter les congestions, et prévoir l'évolution de votre réseau [48].

II.10 Conclusion

Ce chapitre a permis de mettre en évidence l'importance des protocoles dans la configuration et le fonctionnement efficace d'un réseau informatique. Nous avons vu que les protocoles jouent un rôle essentiel dans l'établissement de règles et de standards qui assurent une communication fluide entre les différents équipements du réseau.

Chapitre III

Étude, Analyse et Proposition de solutions

III.1 Introduction

Dans ce chapitre, nous allons présenter notre travail en trois parties. Dans la première partie, nous allons d'abord présenter le réseau existant de « Cevital» à Bejaia, identifier les critiques et proposer des solutions pour améliorer le réseau. Ensuite, nous passerons à la deuxième partie pour discuter du réseau amélioré par l'entreprise « Cevital » ces dernières années. Enfin, dans la troisième partie, nous proposerons trois architectes et choisirons la meilleure comme nouvelle architecture de réseau pour «Cevital».

Notre configuration sera réalisée à travers le simulateur «Cisco Packet Tracer», et nous effectuerons les différents tests de configuration en utilisant l'outil de captures d'écran.

III.2 Présentation du simulateur (Cisco Packet Tracer) :

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

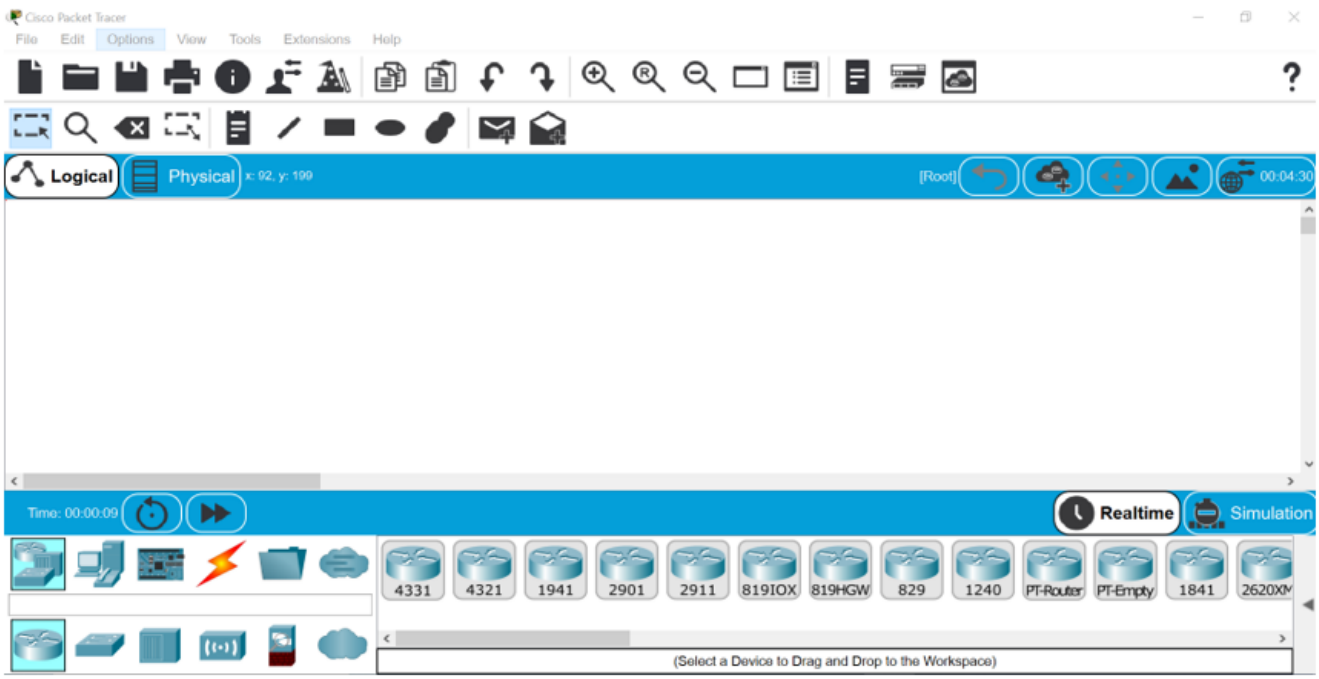


FIGURE III.1 – Interface Cisco Packet Tracer.

III.2.1 Méthode de configuration des équipements

Pour configurer les caractéristiques de modèle, nous utilisant le CLI (Commande Langage Interface).

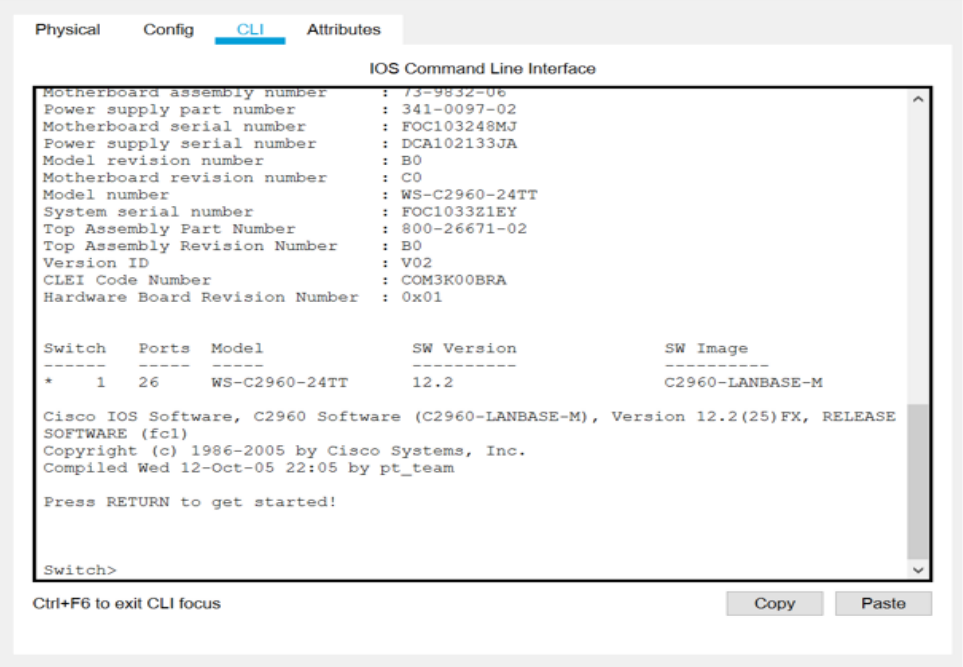


FIGURE III.2 – Interface CLI.

III.3 Etude du réseau existant

Dans ce chapitre, nous allons d'abord présenter le réseau existant de « Cevital » à Bejaia, puis identifier les critiques et proposer des solutions pour améliorer le réseau.

III.3.1 Présentations des équipements utilisés

La topologie de réseau existant utilisée par « Cevital » consiste principalement en deux couches la couche cœur et la couche d'accès et deux serveurs DHCP

1. **Couche Cœur :**
   La couche cœur de réseau, également appelée réseau fédérateur, est une partie critique du réseau local (LAN) qui connecte plusieurs composants du campus. Dans la topologie de réseau existant de « Cevital », Un commutateur (Switch) Cisco Catalyst 3650 est utilisé. Ces commutateurs, issus de la gamme Cisco Catalyst 3560, est un modèle de classe entreprise conçu pour les réseaux locaux d'entreprise et leurs succursales. Il offre une combinaison de ports Ethernet 10/100/1000 et PoE (Power over Ethernet) au standard 802.3af et pré-standard Cisco, ce qui permet des configurations mixtes pour maximiser

la productivité et protéger les investissements. Ce commutateur est idéal pour le déploiement de nouvelles applications telles que la téléphonie IP, le réseau sans fil, la vidéo surveillance, les systèmes de gestion de bâtiment, et les kiosques de vidéo à distance.

Equipements	Type et Marque	Quantité
Switch Cœur	Cisco Catalyst 3560	1

2. **Couche d'Accès :**
   La couche d'accès est la partie la plus externe du réseau, où les utilisateurs finaux se connectent pour accéder aux ressources du réseau. « Cevital » utilise des commutateurs (Switches) Cisco Catalyst 2960 dans son réseau existant connectés entre eux en cascades, Ces commutateurs apportent aux postes de travail une connectivité Fast Ethernet et Gigabit Ethernet optimisent les services de LAN sur les réseaux d'entreprise d'entrée de gamme, intermédiaires et les réseaux de succursale. La gamme Catalyst 2960 offre une sécurité intégrée avec contrôle de l'admission sur le réseau (NAC), qualité de service :

Equipements	Type et Marque	Quantité
Switch d'Accès	Cisco Catalyst C2960	35

3. **Serveur DHCP :**
   Le serveur DHCP gère une plage d'adresses IP et les alloue aux clients de façon permanente ou temporaire, lorsque l'adresse n'est plus utilisée, elle reprend sa place dans le pool d'adresses sous le contrôle du serveur et peut être réallouée à un autre client. Le serveur tient à jour les informations relatives à l'allocation des adresses IP aux clients dans ses tables de réseau DHCP, afin d'éviter tout conflit d'utilisation des adresses.

Equipements	Type et Marque	Quantité
Serveur	DHCP , HPE ProLiant DL380 Gen9	2

III.3.2 Architecture du réseau existant du complexe Cevital

La figure ci-dessous figure III.3 représente la topologie existant du complexe Cevital :

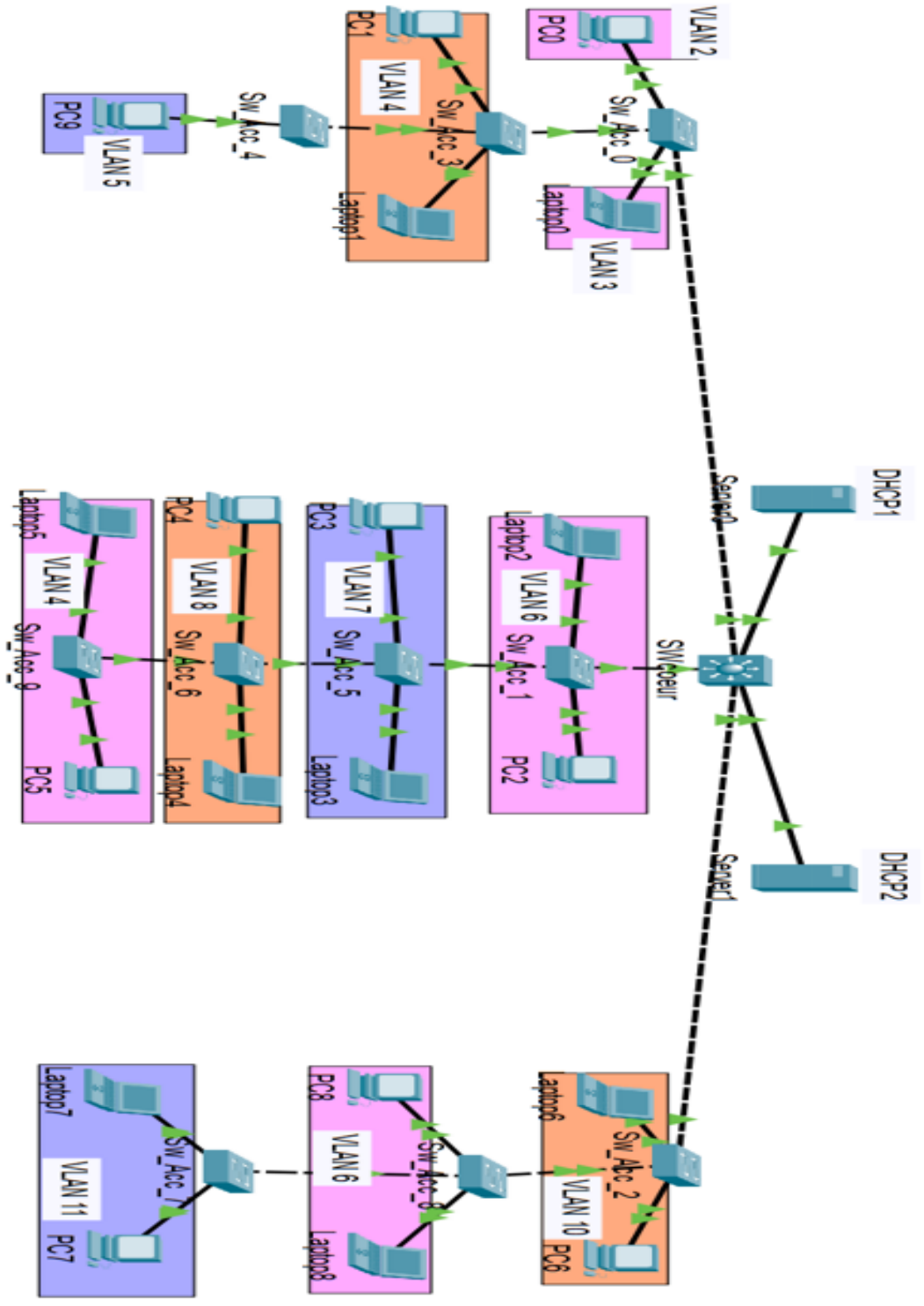


FIGURE III.3 – Architecture du réseau existant.

III.3.3 Désignations des interfaces

Les interfaces sur les équipements seront comme indique le tableau III.1 :

Local Device	Remote Device	Local Interface(s)	Mode De Ports
SW_COEUR	SW_ACC_0	Gig1/0/1	Mode Trunk
SW_COEUR	SW_ACC_1	Gig1/0/2	Mode Trunk
SW_COEUR	SW_ACC_2	Gig1/0/3	Mode Trunk
SW_COEUR	SERVER_0	Gig1/0/4	Mode Access
SW_COEUR	SERVER_1	Gig1/0/5	Mode Access
SW_ACC_0	SW_COEUR	F0/1	Mode Trunk
SW_ACC_0	SW_ACC_3	F0/2	Mode Trunk
SW_ACC_0	PC0	F0/3	Mode Access
SW_ACC_0	Laptop0	F0/4	Mode Access
SW_ACC_1	SW_COEUR	F0/1	Mode Trunk
SW_ACC_1	SW_ACC_5	F0/2	Mode Trunk
SW_ACC_1	PC2	F0/3	Mode Access
SW_ACC_1	Laptop2	F0/4	Mode Access
SW_ACC_2	SW_COEUR	F0/1	Mode Trunk
SW_ACC_2	SW_ACC_8	F0/2	Mode Trunk
SW_ACC_2	PC6	F0/3	Mode Access
SW_ACC_2	Laptop6	F0/4	Mode Access
SW_ACC_3	SW_ACC_0	F0/1	Mode Trunk
SW_ACC_3	SW_ACC_4	F0/4	Mode Trunk
SW_ACC_3	PC1	F0/2	Mode Access
SW_ACC_3	Laptop6	F0/3	Mode Access
SW_ACC_4	SW_ACC_3	F0/1	Mode Trunk
SW_ACC_4	PC9	F0/2	Mode Access
SW_ACC_5	SW_ACC_1	F0/1	Mode Trunk
SW_ACC_5	SW_ACC_6	F0/2	Mode Trunk
SW_ACC_5	PC3	F0/4	Mode Access
SW_ACC_5	Laptop4	F0/3	Mode Access
SW_ACC_6	SW_ACC_5	F0/1	Mode Trunk
SW_ACC_6	SW_ACC_9	F0/2	Mode Trunk
SW_ACC_6	PC3	F0/3	Mode Access
SW_ACC_6	Laptop4	F0/4	Mode Access
SW_ACC_7	SW_ACC_8	F0/1	Mode Trunk
SW_ACC_7	PC7	F0/3	Mode Access
SW_ACC_7	Laptop7	F0/2	Mode Access
SW_ACC_8	SW_ACC_2	F0/1	Mode Trunk
SW_ACC_8	SW_ACC_7	F0/2	Mode Trunk
SW_ACC_8	PC8	F0/3	Mode Access
SW_ACC_8	Laptop8	F0/4	Mode Access
SW_ACC_9	SW_ACC_6	F0/1	Mode Trunk
SW_ACC_9	PC5	F0/3	Mode Access
SW_ACC_9	Laptop5	F0/2	Mode Access

TABLE III.1 – Liste des interfaces.

III.3.4 Vlan de l'entreprise

Cevital utilise dans l'architecteur du réseau de la classe d'adressages "A" divisée en sous réseaux 10.20.0.0/24. L'administrateur réseau a créé un VLAN-Management pour permettre l'administration du réseau distant de la configuration, mise à jour et équipement de sauvegarde.

Le tableau suivant représente la liste des VLAN :

Nom de VLAN	VLAN ID	Adresse sous-réseau	Masque sous-réseau
IT	2	10.20.2.0	255.255.255.0
DFC	3	10.20.3.0	255.255.255.0
DRH	4	10.20.4.0	255.255.255.0
DG	5	10.20.5.0	255.255.255.0
RF HUILE	6	10.20.6.0	255.255.255.0
RF SUCRE	7	10.20.7.0	255.255.255.0
PLANIFICATIO	8	10.20.8.0	255.255.255.0
SEVEUR	9	10.20.9.0	255.255.255.0
SUCRE LIQUIDE	10	10.20.10.0	255.255.255.0
MARGARINE	11	10.20.11.0	255.255.255.0

Table III.2 – Liste des VLAN.

III.4 Implémentation sur simulateur du réseau existant

(voir annexe A)

III.4.1 Configurations des équipements :

- Configuration de Hostname et la Sécurité
- La création des VLANS et ses interfaces
- Configurer le protocole VTP (VLAN Trunking Protocol)
- Configuration Des Ports
- Configuration du serveur
- Configurations des PC
- Tester la connectivité

III.4.2 Remarque

Lorsque nous avons commencé la configuration du réseau existant de l'entreprise « Cevital », nous avons débuté par la recherche des mémoires précédentes pour comprendre comment le réseau avait été étudié. Nous avons remarqué que parmi les mémoires consultées (figure III.4 et figure III.5), les deux serveurs DHCP n'avaient pas été utilisés, alors que la véritable architecture réseau chez « Cevital » repose sur l'utilisation de deux serveurs DHCP relier avec le switch cœur.

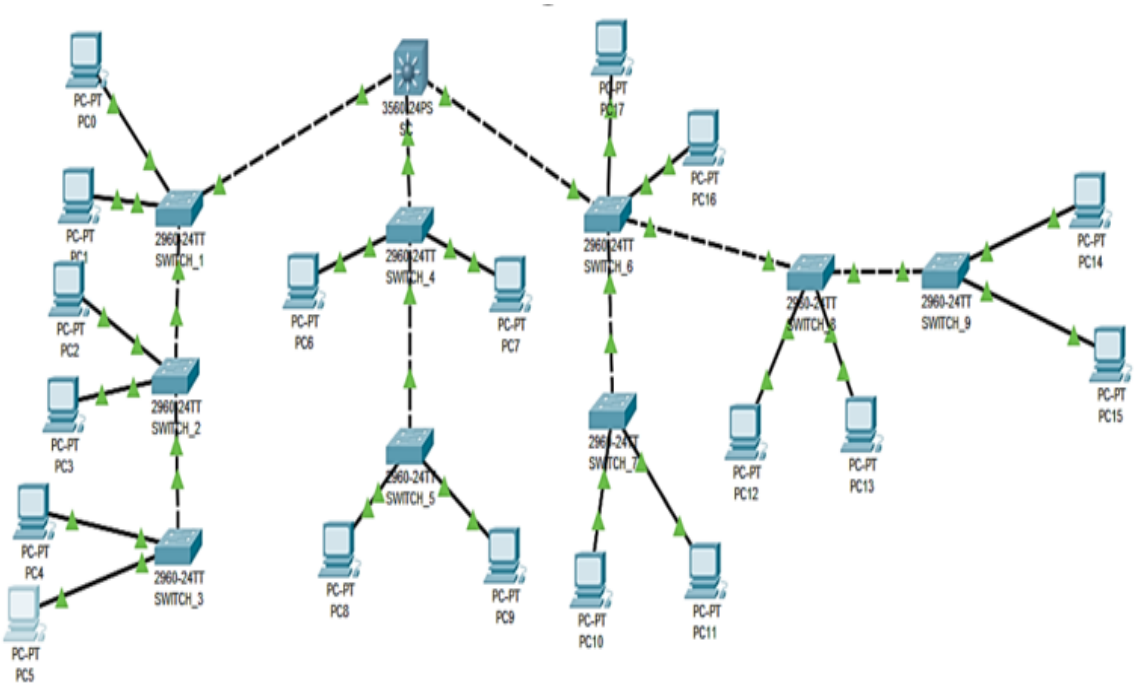


FIGURE III.4 – Topologie 1 [14].

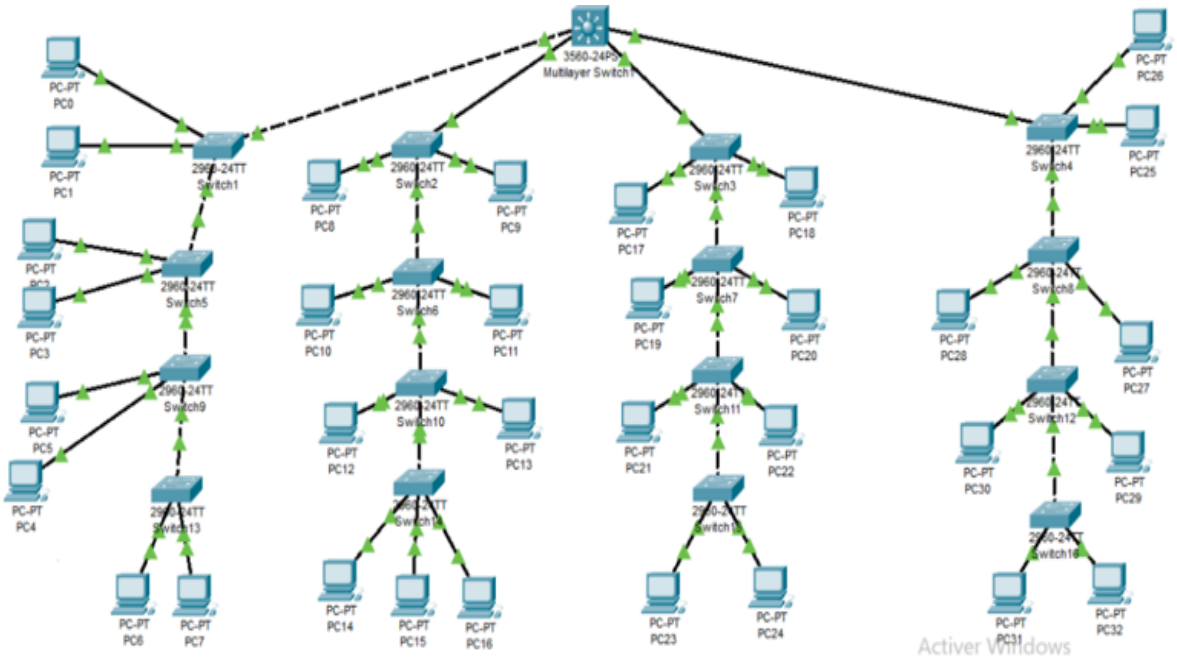


FIGURE III.5 – Topologie 2 [15].

III.4.3 Critique de l'existant

1. Apres l'étude du réseau existant de l'entreprise, Le réseau dispose d'un seul commutateur (switch) cœur, ce qui n'est pas idéal pour des lacunes dans la disponibilité de réseau, ce qui affecte la capacité à maintenir les opérations de l'entreprise sans interruption et des inefficacités dans la répartition de la charge, ce qui entraine des performances inégales et des temps de réponse plus longs pour les utilisateurs.

2. Le réseau comporte également des switches d'Accès connectés en cascades, ce qui crée un grand diamètre de réseau et peut conduire à un réseau plat et non hiérarchique. Il est difficile d'ajouter de nouveaux équipements ou de modifier la configuration du réseau sans affecter la stabilité globale. Les paquets de données doivent traverser plusieurs commutateurs, ce qui peut augmenter les temps de latence et réduire le réseau .

3. La configuration de la surveillance DHCP sur les switches cœur au lieu d'un serveur distinct peut simplifier le processus de configuration du réseau et améliorer les performances du réseau, sans avoir besoin d'un serveur séparé. Cela peut également réduire le risque si il tombe en panne.

• Avant de commencer notre stage (mars 2024) chez « Cevital », ils ont rencontré un problème sur le réseau, le gaz de l'onduleur de climatisation situé dans le data center a été épuisé. La température de l'onduleur a atteint 50°C, ce qui a entraîné l'arrêt du serveur DHCP. En conséquence, lorsque le serveur DHCP est hors service, tout le réseau de « Cevital » s'arrête. Lorsque le réseau s'arrête pendant quelques minutes, toutes les activités peuvent être impactées, entraînant des pertes importantes pour l'entreprise.

4. Les interfaces disponibles sur le Switch sont limitées aux ports Fast Ethernet. Cette limitation de vitesse entrave les performances du réseau surtout à mesure que les besoins en bande passante de l'entreprise augmentent.

• Les ports Fast Ethernet offrent moins de flexibilité que les ports Gigabit Ethernet pour faire évoluer le réseau.

• Si le trafic réseau généré par les utilisateurs et les applications dépasse la capacité des ports Fast Ethernet, cela peut entraîner de la congestion sur le réseau.

5. La présence de switches en fin de vie (Cisco Catalyst 2950/2960) dans le réseau actuel est source d'inquiétude en raison des risques accrus de pannes et de vulnérabilités de sécurité.

6. L'utilisation de switches non-POE (Power over Ethernet) peut présenter des inconvénients dans les contextes où une alimentation électrique dédiée pour chaque appareil connecté n'est pas pratique.

7. La simplicité des mots de passe utilisés. Cette pratique compromet la sécurité globale du réseau, exposant l'entreprise à des risques de piratage et d'accès non autorisé.

8. La sécurité des switches d'accès est critiquée en raison du manque de protection individuelle pour chaque port. Cela expose le réseau à diverses menaces, telle que les attaques par usurpation d'identité et les accès non autorisés.

III.4.4 Les Solutions proposées

• Une conception de réseau hiérarchique avec une couche cœur, une couche de distribution et une couche d'accès est préférable, car elle offre une meilleure évolutivité, des performances améliorées et une sécurité renforcée.

• Pour assurer une haute disponibilité avec redondance matérielle et logicielle, ainsi qu'une solution d'équilibrage de charge, il est recommandé d'avoir au moins deux commutateurs (switches) principaux : En cas de panne d'un switch, le trafic réseau peut être automatiquement basculé vers l'autre. Les deux switches peuvent également partager la charge de trafic, améliorant ainsi les performances globales du réseau.

• Configurer le protocole DHCP dans les Switches cœur plutôt que sur un serveur dédié central, ce qui élimine un point de défaillance potentiel pouvant impacter tout le réseau. La distribution du DHCP sur les Switches cœur rend le système plus résilient.

• Un remplacement progressif des switchs obsolètes par des modèles plus récents mieux pris en charge comme « le Cisco Catalyst 9200/9300 » pour garantir une infrastructure réseau robuste, tout en minimisant les risques de pannes et de failles de sécurité.

• Pour répondre aux besoins actuels et futurs en bande passante, il est recommandé d'envisager une mise à niveau vers des interfaces plus rapide, telles que GigabitEthernet ou 10 GigabitEthernet.

• Pour garantir une protection adéquate, il est impératif de mettre en œuvre des politiques plus sécuriser en matière de complexité des mots de passe et de sensibiliser les employés aux bons pratiques de sécurité informatique.

• Adopté une architecture en étoile pour les switches d'accès, offre une répartition plus équilibrée du trafic et une gestion simplifiée.

• L'implémentation de switches POE (Power over Ethernet), ces switches offrent une solution intégrée en fournissant à la fois des données et de l'alimentation électrique via un seul câble Ethernet. Cette transition réduit la complexité du câblage, facilite l'installation des appareils réseau et diminue les coûts associés aux adaptateurs secteur individuels.

• Pour les switches d'accès, attribuer une adresse MAC unique à chaque port et désactiver les ports non utilisés. Cela limitera l'accès aux seuls périphériques autorisés et réduirait les risques d'intrusion.

III.5 Présentation de l'amélioration réalisée par le D.S.I

III.5.1 Le réseau améliorer par l'entreprise.

Pour comprendre en détail la structure et les composants de la nouvelle topologie réseau de « Cevital », il est essentiel d'examiner de près la manière dont elle est organisée en couches et les équipements clés déployés à chaque niveau.

1. **Couche Cœur :** Dans le réseau existant, un seul switch cœur était responsable de la gestion du trafic entre les différents sous-réseaux de l'entreprise. Cependant, dans la topologie améliorée, cette fonction critique est renforcée par la présence de deux switches cœur. Cette redondance au niveau du cœur du réseau permet d'assurer une disponibilité accrue et une résilience face aux pannes potentielles. En effet, l'introduction de deux switches cœur permet une répartition plus équilibrée du trafic, minimisant ainsi les risques de congestion et garantissant une meilleure fluidité des données à travers l'infrastructure.
2. **Couche distribution :** Dans la topologie précédente de « Cevital », l'absence d'une couche distribution laissait un vide crucial dans la gestion du trafic et la distribution des données au sein du réseau. Cette absence signifiait que les switches cœur étaient responsables à la fois du transfert de données et de la gestion du trafic vers les switches d'accès, ce qui pouvait entraîner une surcharge et une inefficacité opérationnelle. Toutefois, avec l'introduction d'une couche distribution dans la nouvelle topologie, dotée de deux switches distribution, l'entreprise a défini un rôle distinct et dédié à cette couche. Désormais, les switches distribution installés au sein du data center, assurent la connectivité entre les switches cœur et les switches d'accès, permettant ainsi une gestion plus efficace du trafic et une répartition équilibrée des charges.
3. **Couche d'accès :**

   Dans la configuration précédente du réseau de « Cevital », les switches d'accès étaient reliés directement aux switches cœur, formant ainsi une cascade de connexions. Cependant, cette structure présentait des inconvénients en termes de gestion du trafic et de fiabilité. Dans la nouvelle topologie, chaque switch d'accès est désormais connecté aux deux switches distribution. Cette modification permet une répartition équilibrée du trafic et offre une redondance accrue, améliorant ainsi la disponibilité du réseau et sa résilience face aux pannes éventuelles. Cette approche simplifiée et redondante renforce la connectivité des utilisateurs finaux et des périphériques, tout en optimisant les performances globales du réseau.

III.5.2 Architecture du réseau ammélioé par le D.S.I

La figure ci-dessous figure III.6 illustre l'architecture après les améliorations effectuées par le D.S.I :

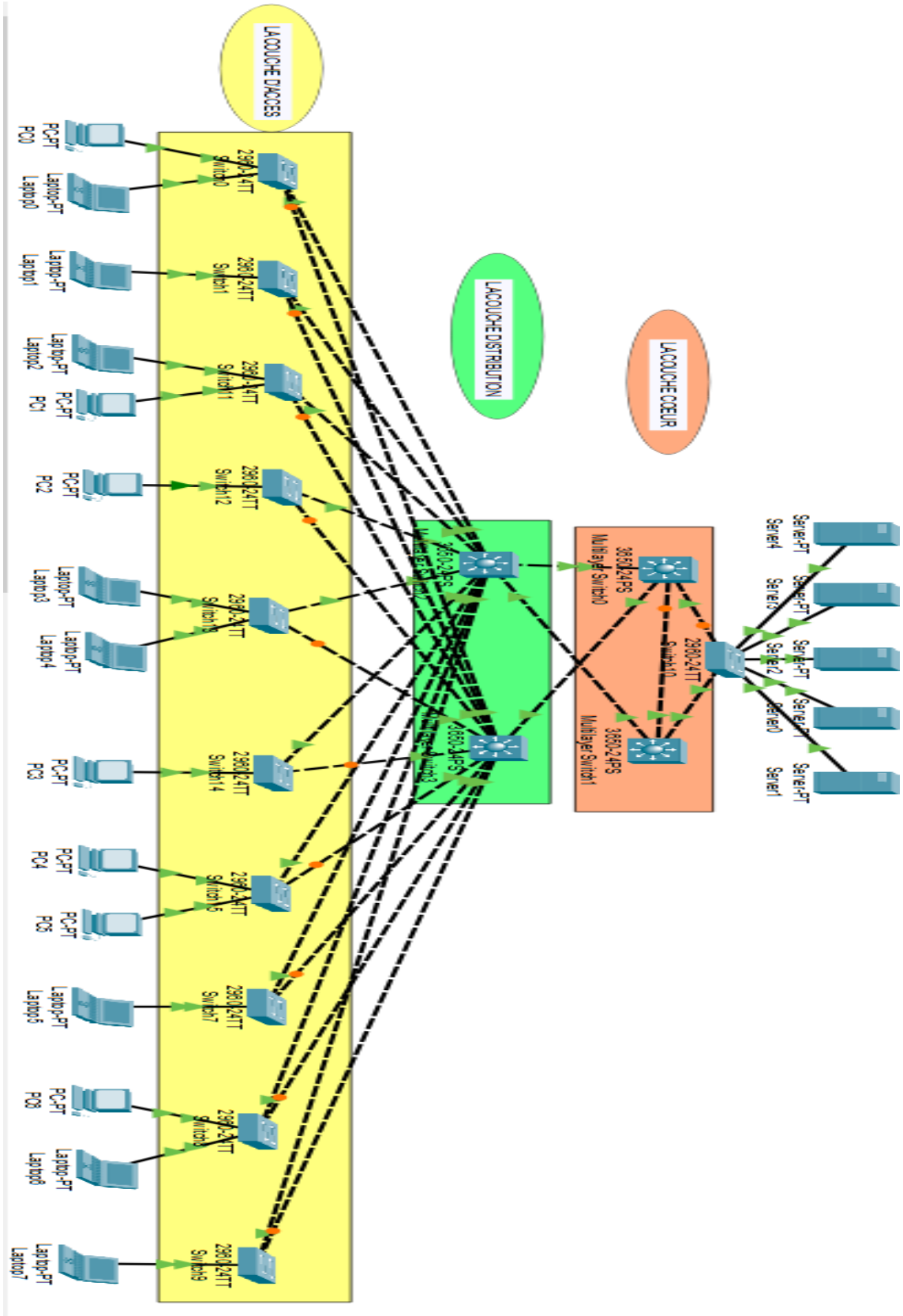


FIGURE III.6 – Architecture du réseau amélioré

III.5.3 La liste des switches Utilisés dans le Réseau amélioré par l'entreprise

Modèle	Nombre
C9200-L-48P-4G	03
WS-C2960X-48FPS-L	06
WS-C2960X-24PS-L	06
WS-C2960X-24PS-L V03	04
WS-C2960X-24PS-L V06	02
WS-C2960-48PST-L	03
WS-C2960-48TC-L	07
WS-C2960-24TC-L	03
WS-C2960-24TC-S	01
WS-C2960-24PC-L	03
WS-C2960C-12PC-L V05	02
WS-C2960-24LT-L	02
WS-C2960C-12PC	02
WS-C2960-8TC-L	01
C2950-I6K2L2Q4-M	01
WS-C2950G-12-EI	02
WS-C3850-24S	02
C6807-XL	02
Nexus 3048	03

-

TABLE III.3 – Modèle des switches[22].

• La couleur « rouge » dans le tableau indique les équipements en fin de vie, signalant ainsi la nécessité de planifier leur remplacement ou leur mise à niveau.

• La couleur « verte » dans le tableau désigne les équipements récemment remplacés.

• La couleur « jeune » indique Les switch à déplacer de l'entreprise de Béjaïa.

III.5.4 Equipements clés dans chaque couche

III.5.4.1 Switch cœur (Cisco Catalyst 6807-XL)

Le commutateur modulaire Cisco Catalyst 6807-XL, tirant parti de l'héritage solide de la série de commutateurs Cisco Catalyst 6500, se positionne comme une solution clé pour répondre aux défis croissants de gestion des infrastructures réseau. Adopté par l'entreprise « Cevital », ce modèle est déployé avec deux switches pour répondre précisément aux besoins évolutifs de son réseau[49].

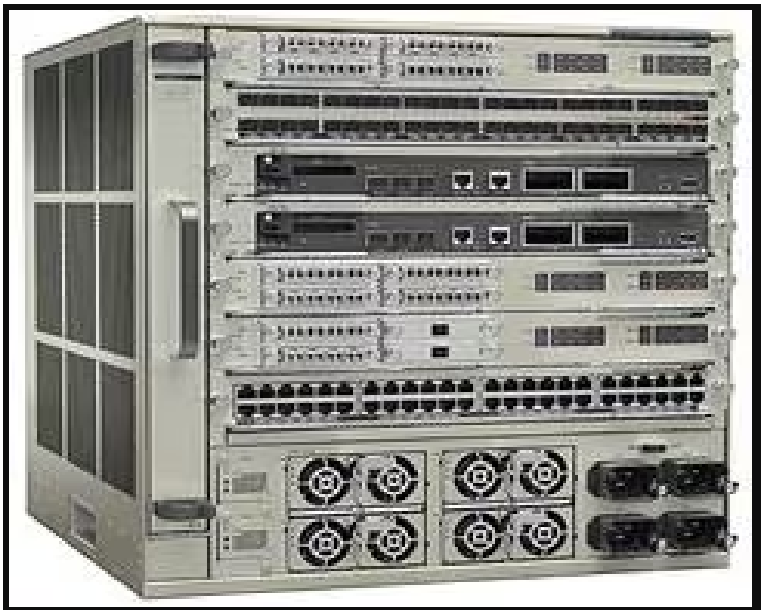


FIGURE III.7 – Cisco Catalyst 6807-XL[16]

- **Caractéristiques :**

- Capacité de Bande Passante : Offre jusqu'à 11,4 Tbps de bande passante système et 440 Gbps par emplacement, avec une capacité de 22,8 Tbps avec VSS.

- Optimisation pour l'Ethernet Haute Densité : Prise en charge de l'Ethernet 10 gigabits haute densité et de l'Ethernet 40 gigabits.

- Protection des Investissements : Compatibilité avec les moteurs de supervision 6T et 2T, ainsi que les cartes de ligne et modules de service associés.

- Résilience Intégrée : Assure une redondance de moteur de supervision 1+1, des ventilateurs et alimentations redondants (N+1) pour minimiser les temps d'arrêt réseau et garantir la productivité et la satisfaction client.

III.5.4.2 Switch Distribution (Cisco WS-C3850-24S)

La gamme Cisco Catalyst® 3850, intégrée au portefeuille Cisco DNA, offre une virtualisation sécurisée, une automatisation améliorée et des données analytiques précieuses, réduisant ainsi les coûts d'installation et d'exploitation pour les entreprises en pleine croissance, comme l'entreprise Cevital qui utilise deux commutateurs de distribution WS-C3850-24S.

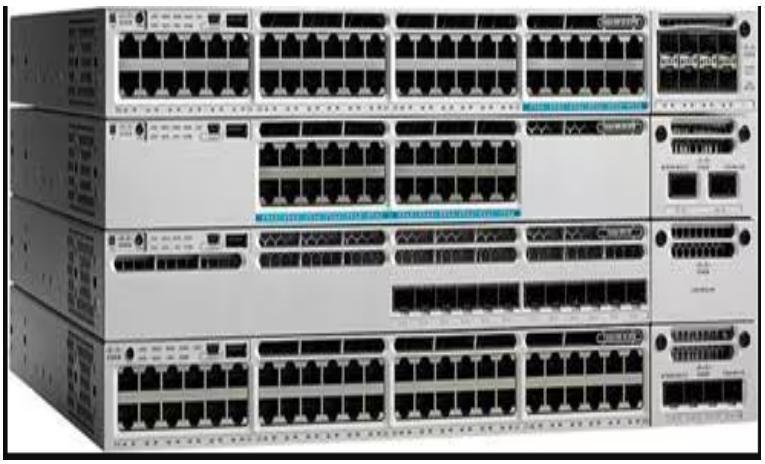


FIGURE III.8 – Cisco WS-C3850-24S[17]

- **Caractéristiques :**

- Capacité du Contrôleur sans Fil Intégré : Jusqu'à 40G de capacité sans fil par commutateur (modèles RJ45 48 ports), avec prise en charge jusqu'à 100 points d'accès et 2000 clients sans fil sur chaque entité de commutation (commutateur ou pile).

- Options de Ports et Technologie Avancée : Disponibles en versions PoE+ et Cisco UPOE avec diverses options de ports, une technologie de pile Cisco StackWise-480 et une technologie Cisco StackPower® pour une redondance d'alimentation.

- Connectivité et Sécurité Renforcée : Prise en charge étendue des normes IEEE pour une connectivité optimale et une sécurité renforcée, avec des fonctionnalités avancées telles que le routage IPv4 et IPv6, la qualité de service modulaire (QoS) et le flux NetFlow flexible (FNF).

- Services Cisco DNA et Garantie Améliorée : Les services Cisco DNA, fournis via le logiciel Cisco ONE™, offrent des solutions simplifiées et à forte valeur ajoutée, avec une garantie à vie limitée améliorée (E-LLW) comprenant un remplacement matériel avancé et un accès de 90 jours au support technique du centre d'assistance technique (TAC) Cisco.

III.5.4.3 Switch d'accès

1. **Cisco Catalyst 9200-L-48P-4G :**

   Les commutateurs de la série Cisco Catalyst 9200 prolongent la puissance des réseaux basés sur l'intention et l'innovation matérielle et logicielle des Catalyst 9000, les rendant accessibles à une gamme plus large de déploiements[50].

FIGURE III.9 – Cisco Catalyst 9200-L-48P-4G[18].

• Le commutateur Cisco Catalyst C9200-L-48P-4G pèse 4,53 kg.
• Le temps moyen entre pannes (MTBF) est de 347 760 heures.
• Il est équipé de 48 ports avec une capacité complète pour le PoE+.
• L'alimentation est assurée par une unité PWR-C5-1KWAC.
• La durée de vie prévue pour ces commutateurs est de 5 ans.
• Les commutateurs de la série Cisco Catalyst 9200 prolongent la puissance des réseaux basés sur l'intention et l'innovation matérielle et logicielle des Catalyst 9000, les rendant accessibles à une gamme plus large de déploiements.
• Le Cisco Catalyst C9200 fournit jusqu'à 48 ports avec une capacité complète Power over Ethernet Plus (PoE+).
• Les options de liaison descendante incluent des connexions pour données, PoE+, UPOE, et UPOE avec mGig pour le Wi-Fi 6/6E.
• Le fond de panier facultatif pour l'empilage supporte une bande passante allant jusqu'à 160 Gbps.

2. **Cisco catalyst 2960 :**
« Cevital » utilise plusieurs types de la catégorie Catalyst 2960, assurant une commutation de couche 2 fiable et sécurisée pour les environnements d'entreprise, tout en offrant des fonctionnalités avancées grâce au logiciel Cisco IOS, notamment Cisco Catalyst SmartOperations, comprnant notamment les modèles suivants :
- WS-C2960X-48FPS-L
- WS-C2960X-24PS-L
- WS-C2960X-24PS-L V03
- WS-C2960X-24PS-L V06
- WS-C2960-48PST-L
- WS-C2960-48TC-L

- WS-C2960-24TC-L
- WS-C2960-24TC-S
- WS-C2960-24PC-L
- WS-C2960C-12PC-L V05
- WS-C2960-24LT-L
- WS-C2960C-12PC
- WS-C2960-8TC-L

FIGURE III.10 – Cisco catalyst 2960[19]

- **Caractéristiques :**

- 24 ou 48 ports Ethernet rapide - Connexions montantes Gigabit Ethernet Small Form-Factor Pluggable (SFP) et 1000BASE-T.
- Alimentation par Ethernet conforme à la norme IEEE 802.3af (PoE).
- Ensemble de fonctionnalités logicielles Cisco IOS® LAN Base ou LAN .
- Outils SmartOperations simplifiant le déploiement et réduisant les coûts d'administration réseau.
- Technologie Cisco EnergyWise pour gérer la consommation d'énergie des périphériques connectés.
- Garantie matérielle à durée de vie limitée améliorée (E-LLW) avec remplacement le jour ouvrable suivant[51].

3. **Cisco catalyst 2950 :** Le commutateur de la gamme Cisco Catalyst 2950 est un commutateur autonome empilable à configuration fixe qui fournit une connectivité Fast Ethernet et Gigabit Ethernet à vitesse filaire, offre de nombreuses fonctionnalités avancées de qualité de service (QoS) et de traitement des flux multicast. Cevital utilise deux types de ce modèle :
   - C2950-I6K2L2Q4-M
   - WS-C2950G-12-EI

FIGURE III.11 – Cisco catalyst 2950

- **Caractéristiques :**

- Performances à vitesse filaire dans la connectivité au réseau local.
- Commutation de couche 2 avec des services intelligents de couche 2 4.
- Gestion de multidiffusion via IGMP Snooping.
- Poids 3 Kg.
- 24 ports 10/100.
- 2 ports 10/100/1000.

4. **Nexus 3048 :** Le Cisco Nexus 3048 est un commutateur Ethernet d'entreprise de la gamme Cisco Nexus 3000, conçu pour des environnements à haute densité et haute performance, tels que les centres de données. Il est idéal pour les applications nécessitant une faible latence et une grande capacité de commutation. Équipé de protocoles de gestion à distance tels que SNMP, RMON, Telnet, et SSH, il permet une administration réseau flexible et sécurisée. Ce modèle prend en charge des protocoles de routage robustes comme BGP et IGMP, et offre une garantie fabricant d'un an, soulignant sa fiabilité. Il propose des caractéristiques avancées, notamment la prise en charge des réseaux locaux virtuels (VLAN), des mécanismes de contrôle des tempêtes pour les Broadcast, Multicast, et Unicast, et des fonctionnalités de QoS. La sécurité est renforcée par le DHCP snooping, et la redondance d'alimentation assure une disponibilité continue. Le commutateur est conforme à diverses normes industrielles, garantissant une compatibilité et des performances optimales dans différents environnements réseau[20].

FIGURE III.12 – Nexus 3048[20]

- **Caractéristiques :**

Dimensions :43.9 cm x 50.5 cm x 4.4 cm
Ports :48 x 10/100/1000 + 4 x 10 Gigabit SFP+
Sous-type 10 igabit Ethernet
Capacité : - Interfaces virtuelles (VLAN) : 4096
- Instances Multiple Spanning Tree Protocol : 64
- Instances Rapid Spanning Tree Protocol : 512 RAM 9 Mo
Mémoire flash :2 Go (maximum)
Poids : 9.3 kg
Taille de la table d'adresses MAC : 128 000 entrées
Performances :
- Capacité de commutation : 176Gbps
- Performances de transfert 132Mpps
Garantie du fabricant : 1 an de garantie
Alimentation :CA 120/230 V (50/60 Hz)

III.5.5 La fréquence des pannes de l'entreprise « Cevital »

La fréquence des pannes dans l'entreprise « Cevital » est d'environ trois incidents par année.

• En 2024, l'entreprise a subi une panne majeure en mars due à l'arrêt des serveurs DHCP dans le data center, suivie d'une défaillance du pare-feu en mai.

• En 2023, une panne a affecté le switch Nexus 3048, ainsi que d'autres switches d'accès en fin de vie.

• La plupart des pannes dans cette entreprise concernent les switches d'accès, souvent en fin de vie, ce qui souligne la nécessité de mettre en œuvre de nouveaux switches pour garantir une meilleure fiabilité du réseau.

III.6 Architecturs proposées comme solution

Nous aborderons dans cette partie les trois propositions que nous avons formulées, en examinant en détail leurs avantages et leurs inconvénients dans le contexte de notre projet.

III.6.1 Architecture 1

a. Description

Dans cette première solution, nous proposons une architecture réseau en trois couches composées de la couche cœur, de la couche de distribution et de la couche d'accès. Chaque switch de distribution, situé dans différents blocs de l'entreprise comme la raffinerie de sucre, l'administration et la raffinerie d'huile, est relié à deux switches cœur situés au data center via des câbles de fibre optique. Cette configuration assure une redondance et une haute disponibilité en cas de défaillance d'un des switches cœur. Les switches d'accès, quant à eux, sont connectés aux switches de distribution de leur bloc respectif et gèrent les connexions des appareils finaux tels que les PC, les laptops et les imprimantes. De plus, deux serveurs DHCP situés dans le data center fournissent des adresses IP dynamiques, tandis que d'autres serveurs offrent divers services nécessaires au fonctionnement de l'entreprise.

b. Les équipements requis

Le tableau suivant présente Les équipements nécessaire , leurs description , les quantités requises , ainsi que les Coûts estimés pour chacun d'eux pour crée le premier réseau proposé :

N°	Equipement	Description	Quantité	Coût Estimé[52]
1	Cisco Catalyst C6807-XL	Switch cœur	2	7 300,00-7 500,00 $US
2	Cisco Catalyst WS-C3850-24S	Switch de distribution	3	3 030,00-6 500,00 $US
3	Cisco Catalyst C9200-L-48P-4G	Switch d'accès	49	3 140,00-3 150,00 $US
4	HPE ProLiant DL380 Gen9	Serveur DHCP	2	3 000,00-5 000,00$US

c. Avantages :

La topologie proposée combine redondance, haute disponibilité, performance optimisée, sécurité renforcée, isolation des pannes et gestion simplifiée. En assurant une continuité opérationnelle même en cas de défaillance, elle garantit des

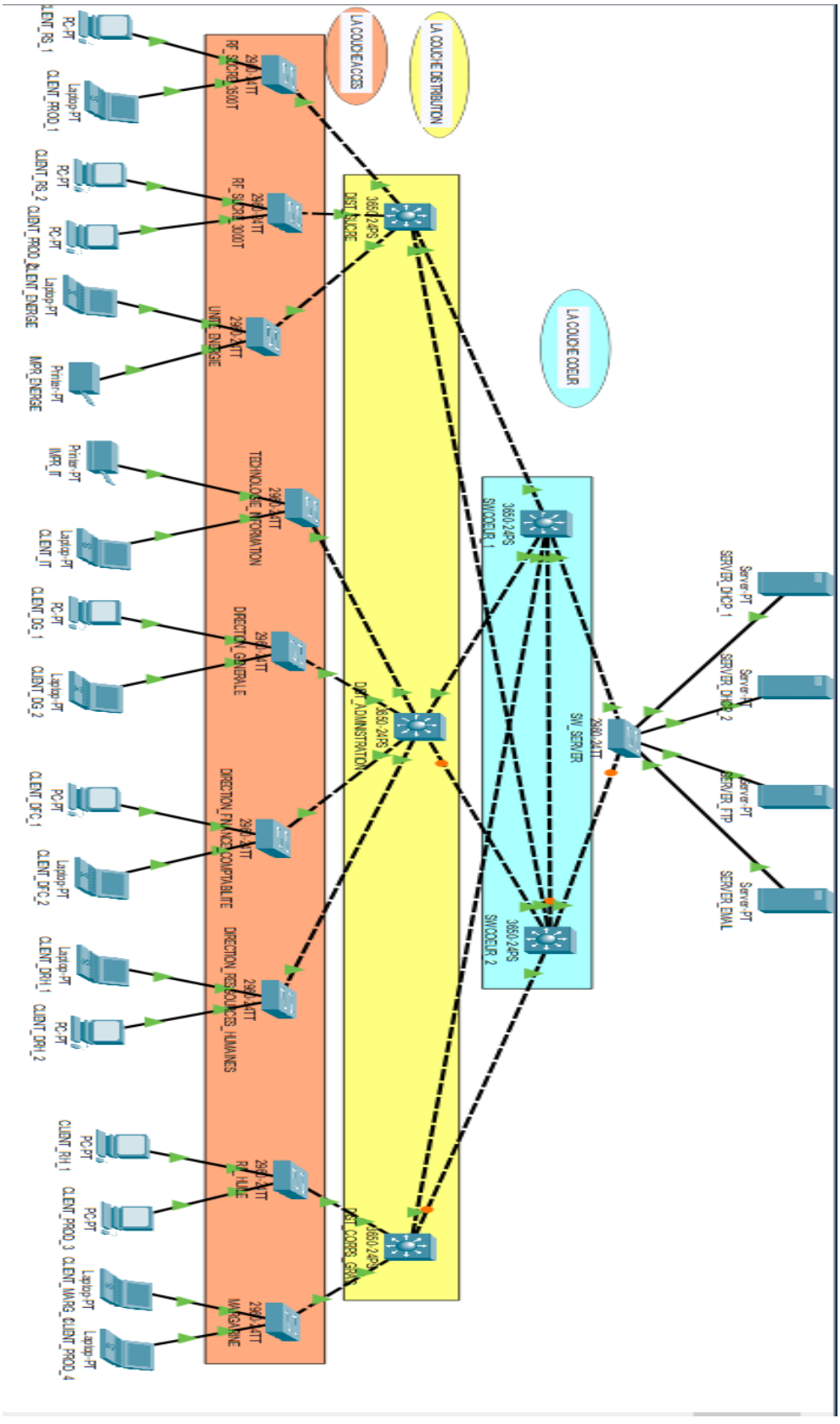
temps de réponse rapides, une protection robuste contre les menaces et une gestion efficace du réseau.

d. Inconvénients :

En configurant le DHCP sur des serveurs, on introduit un point de défaillance unique. Si ces serveurs DHCP tombent en panne ou rencontrent des problèmes, les appareils du réseau peuvent se retrouver incapables d'obtenir des adresses IP dynamiques, ce qui perturberait gravement leur connectivité. En 2024, le réseau de l'entreprise « Cevital » a justement été impacté par une telle panne. Cette défaillance était due à l'arrêt des serveurs DHCP suite à une coupure de gaz dans les onduleurs de climatisation, nécessaire au fonctionnement des équipements. Cet incident souligne la vulnérabilité d'une infrastructure où la gestion des adresses IP repose sur une seule localisation centrale.

e. Schéma de l'architecture

La figure ci-dessous représente l'architecture 1 Proposée :



III.6.2 Architecture 2

a. Description

La topologie réseau présentée est caractérisée par une interconnexion physique précise des équipements réseau. Les commutateurs de niveau trois sont stratégiquement déployés aux niveaux cœur et distribution, tandis que les commutateurs de niveau deux sont assignés à la couche d'accès. Les liaisons entre les commutateurs sont établies via des connexions fibre optique, garantissant ainsi une bande passante élevée et une latence minimale pour un transfert fluide des données. Parallèlement, les connexions reliant les commutateurs d'accès aux périphériques des utilisateurs sont réalisées à l'aide de câbles FTP et de connecteurs RJ45, assurant une connectivité Ethernet fiable. Au niveau des commutateurs cœur, le service DHCP est centralisé, bénéficiant de la redondance fournie par plusieurs serveurs DHCP. Cette approche assure une gestion efficace et une fiabilité accrue des services réseau.

b. Les équipements requis

Le tableau suivant présente Les équipements nécessaire , leurs description , les quantités requises , ainsi que les Coûts estimés pour chacun d'eux pour crée le deuxième réseau proposé :

N°	Equipement	Description	Quantité	Coût Estimé[52]
1	Cisco Catalyst C6807-XL	Switch cœur	2	7 300,00-7 500,00 $US
2	Cisco Catalyst WS-C3850-24S	Switch de distribution	3	3 030,00-6 500,00 $US
3	Cisco Catalyst C9200-L-48P-4G	Switch d'accès	49	3 140,00-3 150,00 $US

c. Avantages :

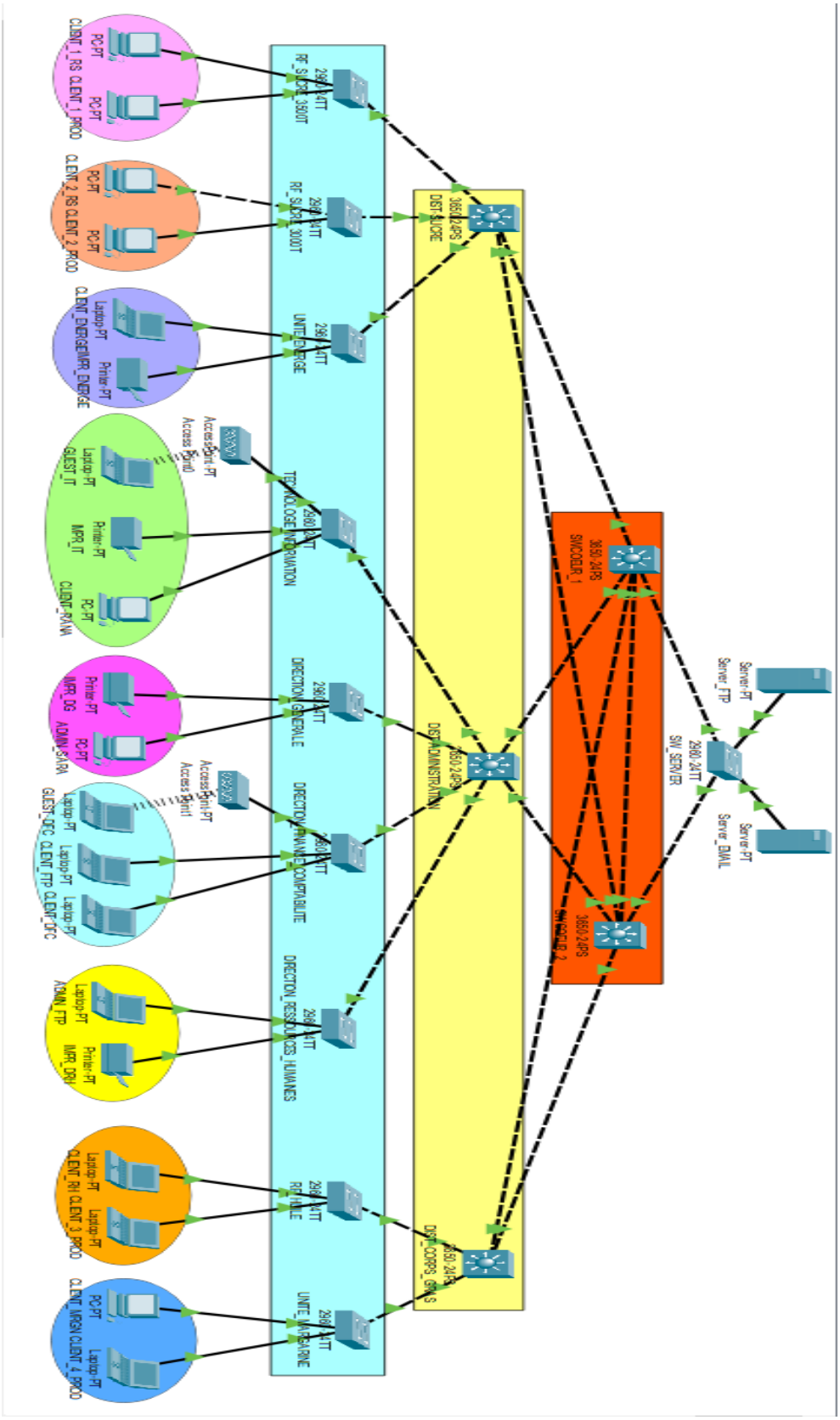
La centralis bation du service DHCP au niveau des commutateurs cœur, associée à la redondance des serveurs DHCP, garantit une disponibilité continue des services réseau, même en cas de défaillance d'un serveur.

d. Inconvénients :

La présence d'un seul commutateur de distribution dans chaque site constitue un inconvénient majeur de cette topologie. En cas de défaillance de ce commutateur, toute la connectivité au sein du site est compromise, donc il est impératif de mettre en place des plans de continuité des activités et des mécanismes de redondance. Ainsi, des solutions de sauvegarde et de redondance doivent être déployée pour garantir une disponibilité continue du réseau .

e. Schéma de l'architecture :

La figure ci-dessous représente l'architecture 2 Proposée :



III.6.3 Architecture 3

a. Description

Cet architecture correspond à un modèle hiérarchique à trois couches, Chaque couche fournit différentes fonctionnalités et capacités du réseau. La couche cœur fournit la connectivité entre tous les périphériques de la couche Distribution, elle transfère de la manière la plus efficiente un gros volume de trafic du réseau. La couche Distribution fournit l'interconnexion entre les couches Access et Cœur. Les commutateurs (Switches) de la couche Distribution doivent être capables de supporter la charge de traitement de tout le trafic venant des périphériques Access. Ces commutateurs (Switches) devraient disposer d'une haute densité de ports à vitesse élevée pour assurer son service d'interconnexion. La couche Access est celle qui connecte les utilisateurs finaux. Chaque Switches de couche Access dispose d'un lien redondant vers chaque commutateur de couche Distribution. Chaque couche devrait contenir une paire de switches, Connecter chaque switches à la couche supérieure avec deux liens pour la redondance et Connecter chaque paire de switches de couche Distribution avec au moins un lien. Cette topologie combine plusieurs éléments de redondance pour offrir une haute disponibilité et une tolérance aux pannes.

b. Les équipements requis

Le tableau suivant présente Les équipements nécessaire , leurs description , les quantités requises , ainsi que les Coûts estimés pour chacun d'eux pour crée le troisième réseau proposé :

N°	Equipement	Description	Quantité	Coût Estimé[52]
1	Cisco Catalyst C6807-XL	Switch cœur	2	7 300,00-7 500,00 $US
2	Cisco Catalyst WS-C3850-24S	Switch de distribution	6	3 030,00-6 500,00 $US
3	Cisco Catalyst C9200-L-48P-4G	Switch d'accès	49	3 140,00-3 150,00 $US

c. Avantages :

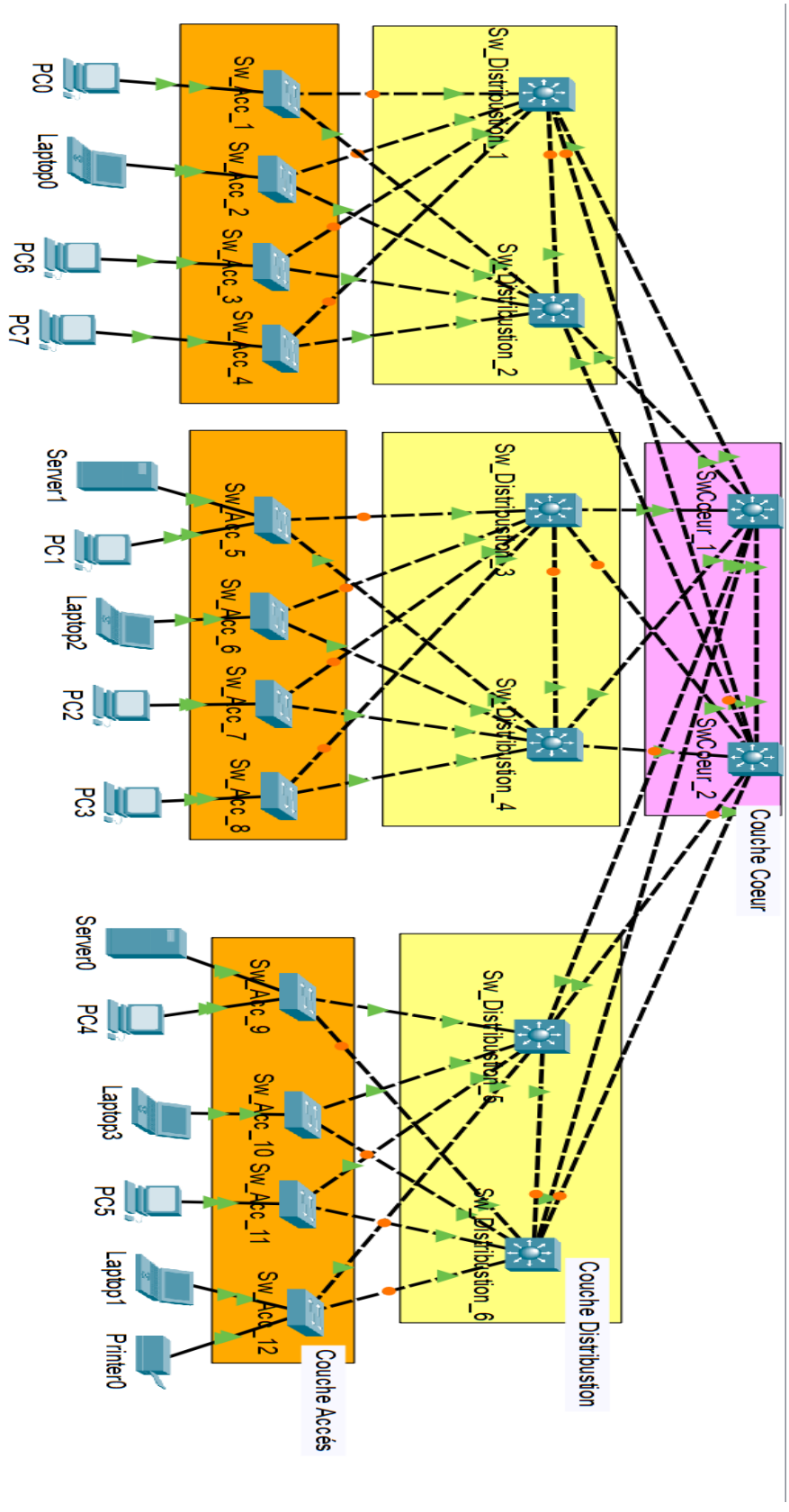
le modèle offre des niveaux fonctionnels : Couches Cœur/Distribution/Access - la redondance entre les couches Cœur-Distribution et Distribution-Accès offre une haute disponibilité, une tolérance aux pannes et une stabilité du réseau local. - Les équipements utilisés, tels que les commutateurs (Switches) sont généralement de haute qualité et de dernière génération.

d. Inconvénients :

Ces équipements (switches) sont trop coûteux.

e. Schéma de l'architecture :

La figure ci-dessous représente l'architecture 3 Proposée :



III.6.4 Solution Retenue

Après avoir étudié la description générale des trois architectes proposés ,leurs avantages et inconvénients . Nous constatons que la première proposition, bien qu'elle présente une bonne conception, une haute disponibilité et des redondances implémentées au niveau de la couche cœur, présente cependant un réseau faible .

En effet, la configuration la surveillance DHCP sur les deux serveurs pose un problème, comme cela a été récemment observé à Cevital en mars 2024. Lorsque le gaz de l'onduleur de climatisation situé dans le data center a été épuisé, la température de l'onduleur a atteint 50°C, ce qui a entraîné l'arrêt du serveur DHCP.

En conséquence, lorsque le serveur DHCP est hors service, tout le réseau de Cevital s'arrête. Cela montre que cette proposition n'est pas suffisamment robuste pour répondre aux besoins de l'entreprise.

En ce qui concerne la troisième proposition, même si l'architecture est également de bonne conception et présente une haute disponibilité. Toutefois l'implémentation de liaisons redondantes peut être coûteuse. Il serait improbable d'implémenter une redondance sur la couche distribution en raison du coût et des fonctionnalités limitées des périphériques finaux. De plus, les commutateurs (switchs) utilisés sont coûteux, ce qui rend cette proposition moins avantageuse.

Enfin, pour la deuxième proposition, l'utilisation d'un seul commutateur de distribution par bloc est suffisante pour répondre aux besoins de chaque bloc, réduisant ainsi les coûts et les complexités. L'implémentation d'une redondance uniquement au niveau de la couche cœur assure une haute disponibilité et une sécurité accrues. De plus, en utilisant des équipements de qualité à un prix raisonnable, nous pouvons répondre aux besoins de l'entreprise sans dépasser les budgets.

En resumé, après la comparaison des trois architecturs avec les cots avontageaux, nous avons choisi la deuxième proposition car elle est la plus avantageuse en termes de coût, de redondance et de haute disponibilité. L'utilisation d'un seul commutateur de distribution par bloc , La configuration de DHCP sur les switchs cœurs au lieu d'un serveur distinct et la redondance au niveau de la couche cœur sont des choix judicieux pour répondre aux besoins de l'entreprise de manière efficace et économique.

III.6.5 Conclusion

Ce chapitre a présenté notre travail en trois parties. Nous avons d'abord décrit le réseau existant de « Cevital » à Bejaïa, identifié les critiques et proposé des solutions pour l'améliorer. Ensuite, nous avons examiné les améliorations apportées par l'entreprise ces dernières années. Enfin, nous avons proposé trois architecturs et choisi la meilleure comme nouvelle architecture proposée de réseau pour Cevital. Cette nouvelle architecture devrait permettre une amélioration significative de la performance et de la fiabilité du réseau, répondant ainsi aux besoins de l'entreprise et des utilisateurs.

Chapitre IV

Analyse et mise en pratique des solutions : simulations et implémentations.

IV.1 Introduction

En tant que stagiaires au sein de l'entreprise algérienne « Cevital », nous avons été chargés d'évaluer et de proposer une nouvelle topologie de réseau pour répondre aux défis actuels et futurs de l'infrastructure réseau de l'entreprise. Avec l'évolution rapide des technologies et l'augmentation des besoins en bande passante, il est crucial de moderniser le réseau existant. Notre proposition vise à améliorer les performances, renforcer la sécurité, assurer une haute fiabilité et garantir l'évolutivité. Ce mémoire présente notre proposition de nouvelle topologie de réseau, qui a pour objectif de répondre efficacement à ces exigences et de soutenir le développement continu de « Cevital ».

IV.2 Vue d'ensemble du réseau

La topologie de réseau proposée repose sur une interconnexion physique méticuleuse des équipements réseau, avec l'utilisation stratégique de commutateurs de niveau 3 pour les couches cœur et distribution, et de commutateurs de niveau 2 pour la couche d'accès. Les liaisons entre les commutateurs cœur et distribution ainsi que celles entre les commutateurs distribution et accès seront établies à l'aide de connexions fibre optique, assurant ainsi une bande passante élevée et une latence minimale pour le transfert efficace des données. De plus, les connexions entre les commutateurs d'accès et les machines des utilisateurs seront établies via des câbles FTP et des connecteurs RJ45, garantissant une connectivité Ethernet robuste et fiable pour les appareils finaux.

IV.3 L'architecture réseau de la solution retenue

La figure ci-dessous représente la topologie réseau de la solution retenue :

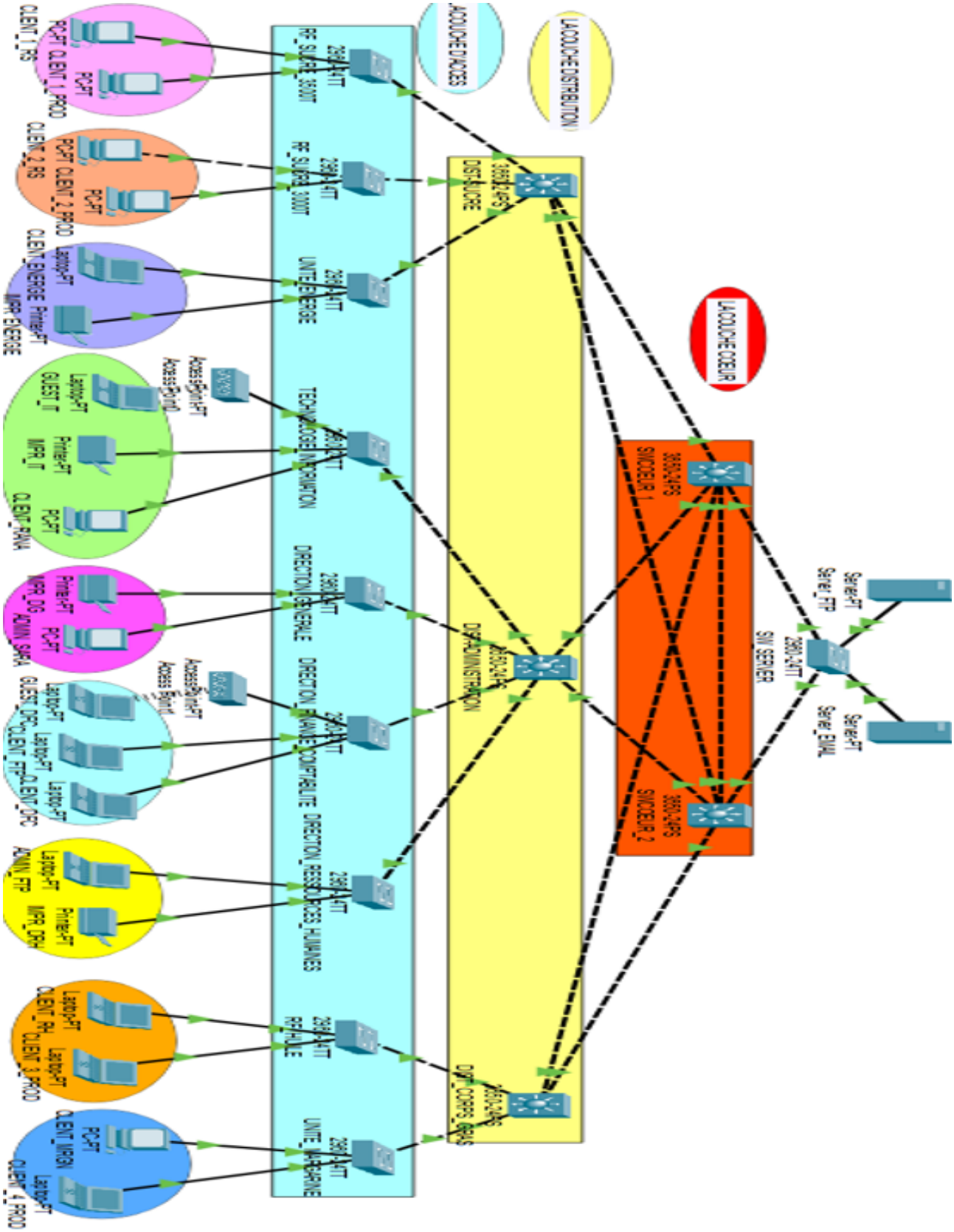


FIGURE IV.1 – architecture réseau de la solution retenue.

IV.4 Applications necessaires et protocoles à mettre en œuvre

- Les Application :
  - Putty
  - MobaXterm
  - HyperTerminal
- Les protocoles :
  - HSRP
  - STP

IV.5 Désignations des interfaces

Les interfaces sur les équipements seront comme indique le tableau IV.1 :

Local Device	Remote Device	Local Interface(s)	Mode De Ports
SWCOEUR_1	SWCOEUR_2	Gig1/0/1	Mode Trunk
SWCOEUR_1	DIST_SUCRE	Gig1/0/2	Mode Trunk
SWCOEUR_1	DIST_ADMINISTRATION	Gig1/0/3	Mode Trunk
SWCOEUR_1	DIST_CORPS_GRAS	Gig1/0/4	Mode Trunk
SWCOEUR_1	SW_SERVER	Gig1/0/5	Mode Trunk
SWCOEUR_2	SWCOEUR_1	Gig1/0/1	Mode Trunk
SWCOEUR_2	DIST_SUCRE	Gig1/0/2	Mode Trunk
SWCOEUR_2	DIST_ADMINISTRATION	Gig1/0/3	Mode Trunk
SWCOEUR_2	DIST_CORPS_GRAS	Gig1/0/4	Mode Trunk
SWCOEUR_2	SW_SERVER	Gig1/0/5	Mode Trunk
DIST_SUCRE	SWCOEUR_1	Gig1/0/1	Mode Trunk
DIST_SUCRE	SWCOEUR_2	Gig1/0/2	Mode Trunk
DIST_SUCRE	RF_SUCRE_3500T	Gig1/0/3	Mode Trunk
DIST_SUCRE	RF_SUCRE_3000T	Gig1/0/4	Mode Trunk
DIST_SUCRE	UNITE_ENERGIE	Gig1/0/5	Mode Trunk
DIST_ADMINISTRATION	SWCOEUR_1	Gig1/0/1	Mode Trunk
DIST_ADMINISTRATION	SWCOEUR_2	Gig1/0/2	Mode Trunk
DIST_ADMINISTRATION	TECHNOLOGIE_INFORMATION	Gig1/0/3	Mode Trunk
DIST_ADMINISTRATION	DIRECTION_GENERALE	Gig1/0/4	Mode Trunk
DIST_ADMINISTRATION	DIRECTION_FINANCE_COMPTABILITE	Gig1/0/5	Mode Trunk
DIST_ADMINISTRATION	DIRECTION_RESSOURCES_HUMAINES	Gig1/0/6	Mode Trunk
DIST_CORPS_GRAS	SWCOEUR_1	Gig1/0/1	Mode Trunk
DIST_CORPS_GRAS	SWCOEUR_2	Gig1/0/2	Mode Trunk
DIST_CORPS_GRAS	RF_HUILE	Gig1/0/3	Mode Trunk
DIST_CORPS_GRAS	UNITE_MARGARINE	Gig1/0/4	Mode Trunk
RF_SUCRE_3500T	DIST_SUCRE	Gig0/1	Mode Trunk
RF_SUCRE_3500T	CLIENT_1_RS	Fa0/1	Mode Access
RF_SUCRE_3500T	CLIENT_1_PROD	Fa0/2	Mode Access
RF_SUCRE_3000T	DIST_SUCRE	Gig0/1	Mode Trunk
RF_SUCRE_3000T	CLIENT_2_RS	Fa0/1	Mode Access
RF_SUCRE_3000T	CLIENT_2_PROD	Fa0/2	Mode Access
UNITE_ENERGIE	DIST_SUCRE	Gig0/1	Mode Trunk
UNITE_ENERGIE	CLIENT_ENERGIE	Fa0/1	Mode Access
UNITE_ENERGIE	IMP_ENERGIE	Fa0/2	Mode Access
TECHNOLOGIE_INFORMATION	DIST_ADMINISTRATION	Gig0/1	Mode Trunk
TECHNOLOGIE_INFORMATION	Access Point0	Fa0/3	Mode Access
TECHNOLOGIE_INFORMATION	IMP_IT	Fa0/2	Mode Access
TECHNOLOGIE_INFORMATION	CLIENT_RANA	Fa0/1	Mode Access
DIRECTION_GENERALE	DIST_ADMINISTRATION	Gig0/1	Mode Trunk
DIRECTION_GENERALE	IMP_DG	Fa0/2	Mode Access
DIRECTION_GENERALE	ADMIN_SARA	Fa0/1	Mode Access
DIRECTION_FINANCE_COMPTABILITE	DIST_ADMINISTRATION	Gig0/1	Mode Trunk
DIRECTION_FINANCE_COMPTABILITE	Access Point1	Fa0/3	Mode Access
DIRECTION_FINANCE_COMPTABILITE	CLIENT_FTP	Fa0/2	Mode Access
DIRECTION_FINANCE_COMPTABILITE	CLIENT_DFC	Fa0/1	Mode Access
DIRECTION_RESSOURCES_HUMAINES	DIST_ADMINISTRATION	Gig0/1	Mode Trunk
DIRECTION_RESSOURCES_HUMAINES	ADMIN_FTP	Fa0/1	Mode Access
DIRECTION_RESSOURCES_HUMAINES	IMP_DRH	Fa0/2	Mode Access
RF_HUILE	DIST_CORPS_GRAS	Gig0/1	Mode Trunk
RF_HUILE	CLIENT_RH	Fa0/1	Mode Access
RF_HUILE	CLIENT_3_PROD	Fa0/2	Mode Access
UNITE_MARGARINE	DIST_CORPS_GRAS	Gig0/1	Mode Trunk
UNITE_MARGARINE	CLIENT_MRGN	Fa0/1	Mode Access
UNITE_MARGARINE	CLIENT_4_PROD	Fa0/2	Mode Access

TABLE IV.1 – Désignations des interfaces.

IV.6 Nomination des VLAN

Le tableau suivant représente la liste des VLAN :

VLAN ID	Nom de VLAN	Descriptionl Description	Adresse sous-réseau	Masque sous réseau
2	IT	Technologie de l'information	10.20.2.0	255.255.255.0
3	DG	Direction générale	10.20.3.0	255.255.255.0
4	DFC	Direction finance et comptabilité	10.20.4.0	255.255.255.0
5	DRH	Direction des ressources humaines	10.20.5.0	255.255.255.0
6	RF_SUCRE	Raffinerie sucre	10.20.6.0	255.255.255.0
7	RF_HUILE	Raffinerie huile	10.20.7.0	255.255.255.0
8	MARGARINERIE	/	10.20.8.0	255.255.255.0
9	SERVER	Serveur	10.20.9.0	255.255.255.0
10	IMPRIMANTE	/	10.20.10.0	255.255.255.0
11	WIFI_GUEST	/	10.20.11.0	255.255.255.0
12	ENERGIE	/	10.20.12.0	255.255.255.0
13	PRODUCTION	/	10.20.13.0	255.255.255.0

Table IV.2 – Nomination des VLAN.

IV.7 Etude de la Solution Retenue

IV.7.1 Couche du réseau de la solution retenue

IV.7.1.1 Couche cœur de la solution retenue

— **Rôle et importance pour « Cevital » :**

Au sein de l'entreprise « Cevital », la couche cœur du réseau revêt une importance capitale en tant qu'élément essentiel de l'infrastructure. En tant que point central, elle assure la transmission sécurisée et efficace des données essentielles entre les différents sites, départements et services de l'entreprise. La haute performance de cette couche est cruciale pour soutenir les opérations critiques telles que le partage de données stratégiques, la communication entre les équipes et la gestion des processus métier. De plus, la couche cœur agit comme un pivot central pour l'intégration des applications et des systèmes, facilitant ainsi la collaboration et la prise de décision à tous les niveaux de l'organisation. En garantissant une connectivité robuste et une

disponibilité continue des services, la couche cœur contribue directement à la compétitivité et à la croissance de « Cevital » sur le marché.

— **Equipements requis :** Dans le cadre de notre proposition pour l'infrastructure réseau de « Cevital », nous avons soigneusement sélectionné et recommandé l'utilisation de deux commutateurs de niveau 3 de la marque « Cisco Catalyst 6807-XL Switch ». Ces commutateurs, situés au cœur de notre réseau et spécifiquement localisés dans « Data Center », sont le résultat de notre analyse approfondie et de notre expertise en matière de réseaux. Ces commutateurs offrent :

1. Jusqu'à 11,4 Tbps de bande passante système et 440 Gbps par emplacement, avec une capacité de 22,8 Tbps avec VSS (Virtual Switching System).
2. Optimisation pour l'Ethernet Haute Densité, avec prise en charge de l'Ethernet 10 gigabits haute densité et de l'Ethernet 40 gigabits.
3. Compatibilité avec les moteurs de supervision 6T et 2T, ainsi que les cartes de ligne et modules de service associés, pour une protection des investissements.
4. Redondance de moteur de supervision 1+1, des ventilateurs et alimentations redondants (N+1) pour minimiser les temps d'arrêt réseau et garantir la productivité et la satisfaction client.

— **Câblage :**

Dans l'architecture réseau proposée, les deux commutateurs cœur sont reliés entre eux par des liaisons en fibre optique, assurant ainsi une connexion hautement fiable et à haut débit entre les cœurs du réseau. De plus, chaque commutateur distribution est connecté aux deux commutateurs cœur via des connexions en fibre optique, ce qui garantit une redondance et une résilience accrues au niveau de la distribution, permettant ainsi de maintenir la connectivité même en cas de défaillance d'un commutateur cœur.

IV.7.1.2 Couche distribution

— **Rôle et importance :**

La couche distribution joue un rôle essentiel dans l'architecture réseau de « Cevital » en assurant une gestion efficace et sécurisée du trafic réseau. Elle agit comme un intermédiaire clé entre la couche cœur et la couche accès, permettant l'agrégation des connexions provenant de divers points d'accès. Cette couche optimise le flux de données et améliore l'efficacité opérationnelle de l'entreprise. De plus, la couche distribution garantit la qualité de service (QoS) en priorisant le trafic critique, comme les applications de voix sur IP

(VoIP) et les services vidéo, essentiels pour les opérations quotidiennes de « Cevital ». Enfin, la redondance et la résilience intégrées dans cette couche assurent la continuité des services réseau, même en cas de défaillance d'un équipement, ce qui est vital pour maintenir la productivité et la satisfaction des clients.

— **Equipements requis :** Dans notre proposition pour la couche distribution, nous avons opté pour l'utilisation de trois commutateurs Cisco Catalyst WS-C3850-24S, soigneusement sélectionnés pour répondre aux besoins spécifiques de « Cevital » en matière de performances et de fonctionnalités avancées :

1. Capacité sans Fil : Jusqu'à 40G par commutateur, avec prise en charge de jusqu'à 100 points d'accès et 2000 clients sans fil.
2. Options de Ports : Disponibles en versions PoE+ et Cisco UPOE avec diverses options de ports.
3. Connectivité et Sécurité : Prise en charge étendue des normes IEEE pour une connectivité optimale, avec des fonctionnalités de routage IPv4 et IPv6, qualité de service modulaire (QoS), et flux NetFlow flexible (FNF).
4. Services Cisco DNA : Offrant des solutions simplifiées et une garantie à vie limitée améliorée (E-LLW) avec accès au support technique.

Contrairement à la configuration antérieure où les commutateurs de distribution étaient localisés au sein du data center, notre nouvelle approche consiste à les placer dans des blocs associés spécifiques. Cette décision découle de plusieurs considérations stratégiques.

Premièrement, en rapprochant les commutateurs de distribution des commutateurs d'accès, nous réduisons l'utilisation de câbles de fibre optique à longue portée. Cette approche permet non seulement de réduire les coûts d'installation, mais également de minimiser les dépenses opérationnelles associées.

Deuxièmement, cette configuration simplifie la gestion de l'infrastructure réseau en réduisant le nombre de câbles s'étendant jusqu'au data center. Cette simplification réduit la complexité du réseau et diminue les risques de pannes potentielles.

Enfin, en positionnant les commutateurs de distribution dans des blocs associés spécifiques, nous renforçons la redondance et la résilience du réseau. En cas de défaillance, les interventions de maintenance sont plus rapides et moins perturbatrices, ce qui minimise les interruptions de service et maintient la productivité de l'entreprise à un niveau optimal.

— **Câblage :**

Dans le cadre du câblage de notre topologie réseau, nous avons établi deux

connexions cruciales : D'une part, les commutateurs de distribution sont reliés par fibre optique aux commutateurs d'accès associés à leur bloc respectif.

D'autre part, chaque commutateur de distribution est également connecté par fibre optique aux deux commutateurs cœur.

Cette architecture de câblage garantit une connectivité fiable et redondante entre les différents niveaux de notre infrastructure réseau, assurant ainsi une performance optimale et une disponibilité continue des services pour les utilisateurs de « Cevital ».

IV.7.1.3 Couche d'accès

— **Rôle et importance :**

La couche d'accès est essentielle dans l'architecture réseau de l'entreprise, en connectant directement les utilisateurs finaux au réseau. Elle permet la connexion des périphériques tels que les ordinateurs, téléphones IP et points d'accès Wi-Fi, tout en assurant la sécurité et la qualité de service. Grâce à l'authentification des utilisateurs et à la segmentation du réseau via VLANs, elle protège contre les accès non autorisés et garantit une expérience utilisateur fluide en priorisant le trafic critique. Flexible et extensible, la couche d'accès permet des ajouts ou modifications rapides de l'infrastructure réseau, répondant ainsi aux besoins évolutifs de l'entreprise.

— **Equipements requis :** Pour la couche d'accès de notre réseau, nous avons sélectionné les commutateurs Cisco Catalyst C9200-L-48P-4G pour leurs performances avancées et leurs fonctionnalités étendues. Voici un aperçu de ces équipements :

1. Les commutateurs de la série Cisco Catalyst 9200 étendent la puissance du réseau basé sur l'intention et l'innovation matérielle et logicielle des Catalyst 9000 à un ensemble plus large de déploiements.
2. Le Cisco Catalyst C9200 offre jusqu'à 48 ports avec une capacité Power over Ethernet Plus (PoE+) complète
3. La résilience est garantie grâce à des unités remplaçables sur site (FRU), une alimentation redondante, des ventilateurs et des liaisons modulaires
4. Les options de source d'alimentation vont de la tension AC de ligne au courant continu haute tension (HVDC), offrant aux clients la possibilité de migrer vers des réseaux micro DC alimentés par des sources d'énergie renouvelable.
5. Les options de liaison descendante incluent des données, PoE+, UPOE et UPOE avec mGig pour le Wi-Fi 6/6E.

6. Le stacking facultatif du fond de panier prend en charge une bande passante d'empilage allant jusqu'à 160 Gbps
7. L'ASIC UADP 2.0 Mini intégré avec un CPU optimise la mise à l'échelle et la structure des coûts.
8. La sécurité est renforcée avec un chiffrement MACsec AES-128 (C9200) ou AES-256 (C9200CX), ainsi que la segmentation basée sur les politiques et des solutions fiables pour la série Catalyst 9200.
9. L'ASIC offre des capacités de micro-ingénierie et de pipeline programmable, ainsi qu'une allocation configurable basée sur des modèles pour les fonctions de transfert de couche 2 et couche 3, les listes de contrôle d'accès (ACL) et la qualité de service (QoS).
10. La surveillance cloud via le tableau de bord Meraki et la certification ENERGY STAR® pour les modèles C9200L complètent les fonctionnalités essentielles de ces commutateurs Cisco Catalyst.

— **Câblage :**

Dans la topologie améliorée par « Cevital » ces dernières années, chaque commutateur d'accès est relié aux deux commutateurs de distribution situés dans le data center. Cette configuration permet une redondance et une disponibilité accrues du réseau. En revanche, dans notre topologie proposée, les commutateurs d'accès associés à un bloc spécifique sont connectés à leur commutateur de distribution dédié dans le même bloc. Cette approche réduit la distance physique entre les commutateurs d'accès et de distribution, minimisant ainsi l'utilisation de câbles longue portée et améliorant la gestion globale du réseau.

IV.7.2 Coût de la solution

Le tableau suivant représente Coût de la Solution Retenue

N°	Désignation	Prix Estimé[52]	Quantité	Coût Estimé
1	6807-xl	7 300,00- 7 500,00 $US	2	14 600,00- 15 000,00 $US
2	WS-C3850-24S	3 030,00- 6 500,00 $US	3	9 090,00- 19 500,00 $US
3	C9200-L-48P-4G	3 140,00- 3 150,00 $US	49	15 3860,00- 15 4350,00 $US
4	Câble fibre optique	3,7653 $US	6 Km	22 591,8 $US
5	Câble FTP	0,5- 1,00 $US	100 m	50 ,00- 100,00 $US
6	Connecteur RJ45	0,1 $US	300	30 $US
Total : 200221.8- 211571,8 $US				

IV.8 Implémentation sur simulateur "Cisco packet Tracer" l'architecture proposée

(Voir annexe B)

IV.8.1 Couche cœur

1. Accès au mode de configuration
2. Nom du switch
3. Configuration de la bannière MOTD
4. Configuration VTP
5. Configuration les VLAN
6. Configuration des interface VLAN.
7. Configuration le DHCP.
8. Configuration des ports
9. Configuration le Protocole STP.
10. Configuration le Protocole HSRP.
11. La sécurité .
12. Enregistrement de la configuration :

IV.8.2 Switch de distribution

1. Accès au mode de configuration
2. Nom de switch
3. Configuration VTP
4. Configuration des modes de ports
5. La sécurité

IV.8.3 Switch d'accès

1. **Accès au mode de configuration globale**
2. Attribution de noms aux switches
3. Configuration VTP
4. Configuration des modes de ports
5. La sécurité

IV.8.4 4.9 Conclusion

Dans ce dernier chapitre, nous avons présenté la solution retenue, en détaillant la configuration des différents protocoles et en effectuant des tests de validation pour vérifier que notre objectif a été atteint.

Conclusion Générale

L'objectif principal de ce projet était d'étudier, de critiquer et d'analyser un réseau local existant, puis d'implémenter des solutions sur un simulateur pour l'améliorer. Nous avons tenté de mettre en place des solutions aidant l'entreprise de mieux comprendre et sécuriser leur réseau.

Dans un premier temps, nous avons présenté un aperçu théorique du complese CEVITAL Bejaia. Ensuite, nous avons défini les concepts clés liés aux équipements de base d'un réseau informatique et aux différents protocoles utilisés pour la configuration et l'administration des réseaux. Cette étape nous a permis de mieux comprendre le réseau de CEVITAL.

Ensuite, nous nous sommes penchés sur la présentation et la conception du réseau local existant de CEVITAL. Nous avons pu schématiser la topologie du réseau étudié et identifier certains manques dans cette architecture non hiérarchique. Nous avons critiqué et analysé en détail les forces et faiblesses de ce réseau et implémenté quelques solutions. Puis nous avons discuté du réseau amélioré par l'entreprise CEVITAL, en citant tous ses équipements et ses fréquences de panne. Nous avons également abordé les trois architectures que nous avons formulées, en examinant en détail leurs avantages ainsi leurs inconvénients, et nous avons sélectioné la meilleure comme nouvelle architecture de réseau pour CEVITAL.

Enfin, le dernier chapitre a été consacré à notre topologie proposée sur un simulateur, Cisco Packet Tracer. Nous avons pu mettre en évidence le rôle majeur des protocoles, tels que VTP, STP et HSRP, dans l'optimisation de la qualité de transmission des données dans un réseau local. De plus, la mise en place d'une architecture hiérarchique a permis de démontrer l'intérêt de la redondance des équipements dans la tolérance aux pannes.

Bibliographie

[1] EL Watan. Tage cevital. https://elwatan-dz.com/tag/cevital, 2023. Consulté le 14 avril 2024.

[2] Source interne de l'entreprise Cevital. Organigramme, 2024. Consulté le 16 avril 2024.

[3] Google Maps. Cevital agroindustrie. https://www.google.com/maps/place/Cevital+AgroIndustrie/@36.7418343,5.0756116,15z/data=!4m6!3m5!1s0x12f2ccc73def0999:0xe69fc2b22167e619!8m2!3d36.7418343!4d5.0756116!16s%2Fg%2F11c2jpn4c6?entry=ttu. Consulté le 18 avril 2024.

[4] Dieng Cyber. Mengenal tentang pan (personal area network) [image]. https://diengcyber.com/mengenal-tentang-panpersonal-area-network/, 2023. Consulté le 22 juin 2024.

[5] Pathshala Nepal. What is local area network (lan) ? what are the advantages & features of lan ? [image]. https://pathshalanepal.com/question/what-is-local-area-network-lan-what-are-the-advantages-features-of-lar#gsc.tab=0, 2020. Consulté le 24 juin 2024.

[6] Kibrispdr. Metropolitan area network diagram [image]. https://www.kibrispdr.org/detail-27/metropolitan-area-network-diagram.html, 2022. Consulté le 22 juin 2024.

[7] Loutrel. Différents types de réseau : Réseau wan [image]. https://www.loutrel.fr/wikisn/doku.php?id=les_exposes:differents_type_reseau, 2020. Consulté le 22 juin 2024.

[8] Shutterstock. Images libres de droits de topologie de réseau. https://www.shutterstock.com/fr/search/topologie-de-r%C3%A9seau. Consulté le 9 juin 2024.

[9] OpenClassrooms. Modèle osi et tcp/ip [image]. https://openclassrooms.com/fr/courses/6944606-concevez-votre-reseau-tcp-ip/7236472-prenez-du-recul-sur-votre-pratique-grace-au-modele-osi, 2024. Consulté le 24 juin 2024.

[10] OpenClassrooms. Configurez des vlan sur un switch cisco [image]. https://openclassrooms.com/fr/courses/2557196-administrez-une-architecture-reseau-avec-cisco/5135441-configurez-des-vlan-sur-un-switch-cisco, 2024. Consulté le 22 juin 2024.

[11] Formip. Vlan trunking protocol : Introduction vtp. https://www.formip.com/pages/blog/vlan-trunking-protocol-introduction-vtp. Consulté le 8 juin 2024.

[12] Google. All about rstp (rapid spanning tree protocol) with configuration. https://www.google.com/search/about-this-image?img=H4sIAAAAAAAA_-MS4Zj95tGxff9bPpULbOn_Om_vxt-NfgBjTwIQFgAAAA%3D%3D&q=https:%2F%2Fgbu-presnenskij.ru%2Felektronnoe-obraschenie%2F%3Fu%3Dall-about-rstp-rapid-spanning-tree-protocol-with-configuration-qq-x5ctx=iv&hl=fr&sa=X&ved=0CA0Qg4ILahcKEwiYssn9ivaGAxUAAAAAHQAAAAAQBA, n.d. Consulté le 22 juin 2024.

[13] SlideShare. Hsrp (hot standby router protocol). https://www.slideshare.net/slideshow/29-hsrp-hot-standby-router-protocol/47547160, 2015. Consulté le 5 mai 2024.

[14] N. Gherbi and Hamchaoui. *Installation, configuration et administration d'un réseau local (Cevital)*. PhD thesis, Université de Béjaïa, 2020. Consulté le 24 avril 2024.

[15] M. Allaoua and M. Saou. Mise en place d'un réseau local et l'interconnexion avec les sites distants, 2022. Consulté le 23 mai 2024.

[16] Cisco Systems. Catalyst 6807-xl switch [image]. https://www.cisco.com/c/dam/en/us/products/collateral/switches/catalyst-6807-xl-switch/datasheet-c78-728229.docx/_jcr_content/renditions/datasheet-c78-728229_0.jpg, 2019. Consulté le 31 mai 2024.

[17] Cisco Systems. Catalyst 3850 series switches [image]. https://www.cisco.com/c/dam/en/us/products/collateral/switches/catalyst-3850-series-switches/datasheet_c78-720918.docx/_jcr_content/renditions/datasheet_c78-720918_0.jpg, 2019. Consulté le 1 juin 2024.

[18] Cisco Systems. Cisco catalyst 9200 [image]. https://www.cisco.com/site/us/en/products/networking/switches/catalyst-9200-series-switches/index.html?dtid=osscdc000283&_gl=1*1j247kw*_gcl_au*NDAwMjk5NTA3LjE3MTU3MjA4NDU.*_

ga*NTMwNzMyNTQwLjE3MTU1MTI1MTM.*_ga_KP8QEFW4ML*MTcxOTIxMDU3NS4xNS4xLjE3
2023. Consulté le 24 juin 2024.

[19] Cisco Systems. Catalyst 2960 series switches [image]. https://www.cisco.com/c/dam/assets/support/product-images/series/switches-catalyst-2960-series-switches.jpg, 2014. Consulté le 1 juin 2024.

[20] Compufirst. Cisco nexus 3048tp-1ge commutateur 48 ports. https://www.compufirst.com/cisco-nexus-3048tp1ge-commutateur-48-ports-gere-montable-sur-rack/fiche_prod.do?prodId=1511984#prod-spec. Consulté le 24 juin 2024.

[21] Source interne de l'entreprise Cevital. Présentation. https://www.cevital.com/presentation, 2024. Consulté le 15 avril 2024.

[22] Source interne de l'entreprise Cevital. Modèle des switches. Consulté le 7 juin 2024.

[23] Cevital. Présentation. https://www.cevital.com/presentation, 2024. Consulté le 16 avril 2024.

[24] M. Brahmi and D. Bouras. *Proposition de plans de distribution de marchandise optimaux : Cas de l'entreprise Cevital*. PhD thesis, Université A. Mira Béjaia, 2018.

[25] N. Khatir and A. Belhadri. Support de cours sur les réseaux informatiques, 2021. Université, Consulté le 24 avril 2024.

[26] Patsh Tecno. Le réseau personnel pan (personal area network). https://patshtecno.com/le-reseau-personnel-pan-personal-area-network/. Consulté le 8 mai 2024.

[27] Cloudflare. Réseau local (lan). https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-a-lan/, 2024. Consulté le 8 mai 2024.

[28] INOS. Lan – local area network : aperçu de la technologie. https://www.ionos.fr/digitalguide/serveur/know-how/lan/, 2020. Consulté le 8 mai 2024.

[29] Cloudflare. What is a metropolitan area network ? https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-a-metropolitan-area-network/. Consulté le 8 mai 2024.

[30] LeMagIT. Réseau métropolitain man. https://www.lemagit.fr/definition/Reseau-metropolitain-MAN. Consulté le 9 mai 2024.

[31] Fortinet. Wan. https://www.fortinet.com/fr/resources/cyberglossary/wan. Consulté le 9 mai 2024.

[32] IONOS. Wan. https://www.ionos.fr/digitalguide/serveur/know-how/wan/. Consulté le 9 mai 2024.

[33] Techopedia. Topologie de réseau. `https://www.techopedia.com/definition/16258/network-topology`. Consulté le 2 mai 2024.

[34] Moulay Ismail. Support de cours - chapitre 2 : Topologies et architectures des réseaux locaux. `https://fad.umi.ac.ma/pluginfile.pdf`. Consulté le 9 juin 2024.

[35] Systèmes d'Information et Numérique. Cours sur la topologie des réseaux. `http://robert.cireddu.free.fr.pdf`. Consulté le 7 juin 2024.

[36] Microsoft. Microsoft training and certification guide, module 4 : Examen d'un réseau, pp. 23-27. `https://elielecatportefoliosio.files.wordpress.com/2016/04/module-4-examen-dun-reseau1.pdf`, 2016. Consulté le 2 mai 2024.

[37] E. Feriel and M. Messaouda. *Simulation et segmentation d'un réseau VLAN*. PhD thesis, 2015. Consulté le 23 mai 2024.

[38] BTS SRI. Notions de base sur les réseaux informatiques, les modèles osi et tcp/ip, pp. 5-7. `https://btssri13.files.wordpress.com/2013/04/les-modc3a8les-osi-et-tcp-ip.pdf`, 2013. Consulté le 9 juin 2024.

[39] K. Kaced and Y. Khelili. *Étude sur la technologie MSAN : Réalisation d'une plate-forme VoIP simulée à base de la solution VLAN et le protocole DHCP*. PhD thesis, Université Mouloud Mammeri de Tizi-Ouzou, 2015. Consulté le 11 mai 2024.

[40] H. Bouida. *Étude et mise en œuvre d'une solution SDN : Application de gestion de VLANs*. PhD thesis, 2017. Consulté le 10 mai 2024.

[41] E. H. El Amri. Campus des réseaux informatiques et télécommunications, cours vtp. `https://fr.slideshare.net/slideshow/cours-vtp/71253063`, 2017. Consulté le 8 juin 2024.

[42] OpenSpace Course. Le protocole stp. `https://openspacecourse.com/le-protocole-stp/`. Consulté le 15 mai 2024.

[43] Cisco. Spanning tree protocol. `https://www.cisco.com/c/fr_ca/support/docs/lan-switching/spanning-tree-protocol/5234-5.html`. Consulté le 22 mai 2024.

[44] Google Scholar. Protocol spanning-tree. `https://scholar.google.com/`. Consulté le 22 mai 2024.

[45] HAL. Protocol spanning-tree. `https://hal.science/hal-00656865v1/document`. Consulté le 22 mai 2024.

[46] N. Salmon. Redondance de routeur avec hsrp. `https://hal-00656865v1.document`, 2011. Consulté le 9 juin 2024.

[47] Z. Belgherbi. *Simulation sous GNS3 d'une Solution Réseau Intégrée*. PhD thesis, Université de 8 Mai 1945 – Guelma, 2020. Consulté le 10 mai 2024.

[48] FrameIP. Masques de sous-réseau. https://www.frameip.com/masques-de-sous-reseau. Consulté le 10 mai 2024.

[49] Cisco Systems. Catalyst 6807-xl switch. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-6807-xl-switch/datasheet-c78-728229.html, 2019. Consulté le 31 mai 2024.

[50] Cisco Systems. Cisco catalyst 9200 [image]. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html?dtid=osscdc000283&_gl=1*23obom*_gcl_au*NDAwMjk5NTA3LjE3MTU3MjA4NDU.*_ga*NTMwNzMyNTQwLjE3MTU1MTI1MTM.*_ga_KP8QEFW4ML*MTcxOTIxMDU3NS4xNS4xLjE3, 2023. Consulté le 24 juin 2024.

[51] Cisco Systems. Catalyst 2960-plus series switches : Data sheet. https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-plus-series-switches/data_sheet_c78-728003.html?dtid=osscdc000283, 2014. Consulté le 1 juin 2024.

[52] Made in China. Prix des équipements réseau cisco. https://fr.made-in-china.com/tag_search_product/Cisco-Network-Equipment_Price_ysesoegn_1.html, 2024. Consulté le 15 juin 2024.

Annexe A

Annexe 1

A.1 Implémentation sur simulateur du réseau existan

- **Configuration de Hostname et la Sécurité**

Nous avons configuré les paramètres de sécurité et les noms d'hôtes pour chaque switch pour garantir la sécurité et la gestion efficace du réseau.

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line console 0
Switch(config-line)#password CEVITAL24
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line vty 0 4
Switch(config-line)#password CEVITAL24
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#enable password CEVITALBEJAIA
Switch(config)#service password-encryption
Switch(config)#hostname SWcoeur
SWcoeur(config)#
```

- **La création des VLANS et ses interfaces**

- **création les VLAN**

```
SWCOEUR_1(config-vlan)#
SWCOEUR_1(config-vlan)#vlan 2
SWCOEUR_1(config-vlan)#name IT
SWCOEUR_1(config-vlan)#vlan 3
SWCOEUR_1(config-vlan)#name DG
SWCOEUR_1(config-vlan)#vlan 4
SWCOEUR_1(config-vlan)#name DFC
SWCOEUR_1(config-vlan)#vlan 5
SWCOEUR_1(config-vlan)#name DRH
SWCOEUR_1(config-vlan)#vlan 6
SWCOEUR_1(config-vlan)#name RF_SUCRE
SWCOEUR_1(config-vlan)#vlan 7
SWCOEUR_1(config-vlan)#name RF_HUILE
SWCOEUR_1(config-vlan)#vlan 8
SWCOEUR_1(config-vlan)#name MARGARINERIE
SWCOEUR_1(config-vlan)#vlan 9
SWCOEUR_1(config-vlan)#name SERVER
SWCOEUR_1(config-vlan)#vlan 10
SWCOEUR_1(config-vlan)#name IMPRIMANTE
SWCOEUR_1(config-vlan)#vlan 11
SWCOEUR_1(config-vlan)#name GUEST_WIFI
SWCOEUR_1(config-vlan)#vlan 12
SWCOEUR_1(config-vlan)#name ENERGIE
SWCOEUR_1(config-vlan)#vlan 13
SWCOEUR_1(config-vlan)#name PRODUCTION
SWCOEUR_1(config-vlan)#
```

Vérification les VLAN avec la commande « SHOW VLAN BRIEF ».

```
SWcoeur#SH VLAN BR

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/6, Gig1/0/7, Gig1/0/8, Gig1/0/9
                                                Gig1/0/10, Gig1/0/11, Gig1/0/12, Gig1/0/13
                                                Gig1/0/14, Gig1/0/15, Gig1/0/16, Gig1/0/17
                                                Gig1/0/18, Gig1/0/19, Gig1/0/20, Gig1/0/21
                                                Gig1/0/22, Gig1/0/23, Gig1/0/24, Gig1/1/1
                                                Gig1/1/2, Gig1/1/3, Gig1/1/4
2    IT                               active
3    DFC                              active
4    DRH                              active
5    DG                               active
6    RF_HUILE                         active
7    RF_SUCRE                         active
8    PLANIFICATION                    active
9    SERVEUR                          active
10   SUCRE_LIQUIDE                    active
11   MARGARINE                        active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
 --More--
```

- **création les interface**

```
SWcoeur(config)#int vlan 2
SWcoeur(config-if)#
%LINK-5-CHANGED: Interface Vlan2, changed state to up

SWcoeur(config-if)#ip add 10.20.2.254 255.255.255.0
SWcoeur(config-if)#exit
SWcoeur(config)#int vlan 3
SWcoeur(config-if)#
%LINK-5-CHANGED: Interface Vlan3, changed state to up

SWcoeur(config-if)#ip add 10.20.3.254 255.255.255.0
SWcoeur(config-if)#exit
SWcoeur(config)#int vlan 4
SWcoeur(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

SWcoeur(config-if)#ip add 10.20.4.254 255.255.255.0
SWcoeur(config-if)#exit
SWcoeur(config)#int vlan 5
SWcoeur(config-if)#
%LINK-5-CHANGED: Interface Vlan5, changed state to up

SWcoeur(config-if)#ip add 10.20.5.254 255.255.255.0
SWcoeur(config-if)#exit
SWcoeur(config)#int vlan 6
SWcoeur(config-if)#
%LINK-5-CHANGED: Interface Vlan6, changed state to up

SWcoeur(config-if)#ip add 10.20.6.254 255.255.255.0
SWcoeur(config-if)#exit
```

- **Configurer le protocole VTP (VLAN Trunking Protocol)**

VTP	MODE	NAME
SWCOEUR	SERVER	CEVITAL.COM
Tous les autres Switchs	CLIENT	CEVITAL.COM

- **Mode Server**

```
SWcoeur#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SWcoeur(config)#vtp mode server
Device mode already VTP SERVER.
SWcoeur(config)#vtp domain CEVITAL.com
Changing VTP domain name from NULL to CEVITAL.com
SWcoeur(config)#vtp password CEVITALBEJAIA
Setting device VLAN database password to CEVITALBEJAIA
SWcoeur(config)#end
SWcoeur#
%SYS-5-CONFIG_I: Configured from console by console
wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
```

Vérification VTP SERVER avec la commande « SHOW VTP STATUS ».

```
SWcoeur#SH 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                       : 0002.175D.4600
Configuration last modified by 0.0.0.0 at 3-1-93 00:00:00
Local updater ID is 10.20.2.254 on interface Vl2 (lowest numbered VLAN interface found)

Feature VLAN :
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs        : 15
Configuration Revision          : 340
MD5 digest                      : 0x26 0x30 0x1C 0x3E 0xC6 0xBF 0x18 0xFB
                                  0x7C 0x2F 0xC4 0xE3 0x45 0xB1 0xCB 0x89
```

- **Mode CLIENT**

```
SW_ACC_0#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
SW_ACC_0(config)#vtp mode client
Device mode already VTP CLIENT.
SW_ACC_0(config)#vtp domain CEVITAL.COM
Domain name already set to CEVITAL.COM.
SW_ACC_0(config)#VTP PASSWORD CEVITALBEJAIA
Password already set to CEVITALBEJAIA
SW_ACC_0(config)#END
SW_ACC_0#
%SYS-5-CONFIG_I: Configured from console by console
WR
```

Vérification VTP CLIENT avec la commande « SHOW VTP STATUS ».

```
SW_ACC_0>EN
Password:
Password:
SW_ACC_0#SH VTP STATUS
VTP Version                     : 2
Configuration Revision          : 280
Maximum VLANs supported locally : 255
Number of existing VLANs        : 15
VTP Operating Mode              : Client
VTP Domain Name                 : CEVITAL.COM
```

- **Cconfigyration Des Ports**
- **Mode Trunk**

```
SWcoeur#config t
Enter configuration commands, one per line.  End with CNTL/Z.
SWcoeur(config)#interface range G1/0/1-3
SWcoeur(config-if-range)#switchport trunk encapsulation dot1q
SWcoeur(config-if-range)#switchport mode trunk
SWcoeur(config-if-range)#end
```

Vérification les interfaces avec la commande « SHOW Interfaces STATUS ».

```
SWcoeur#SH INT STATUS
Port      Name               Status       Vlan       Duplex  Speed Type
Gig1/0/1                     connected    1          auto    auto  10/100BaseTX
Gig1/0/2                     connected    1          auto    auto  10/100BaseTX
Gig1/0/3                     connected    1          auto    auto  10/100BaseTX
Gig1/0/4                     connected    9          auto    auto  10/100BaseTX
Gig1/0/5                     connected    9          auto    auto  10/100BaseTX
Gig1/0/6                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/7                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/8                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/9                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/10                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/11                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/12                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/13                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/14                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/15                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/16                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/17                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/18                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/19                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/20                    notconnect   1          auto    auto  10/100BaseTX
Gig1/0/21                    notconnect   1          auto    auto  10/100BaseTX
 --More--
```

- Mode Access

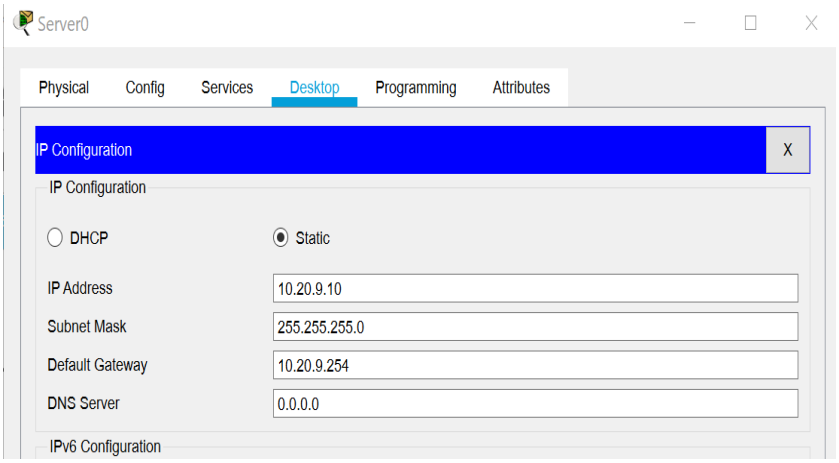
```
SW_ACC_0#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
SW_ACC_0(config)#INT F0/3
SW_ACC_0(config-if)#switchport mode access
SW_ACC_0(config-if)#switchport access vlan 2
SW_ACC_0(config-if)#INT F0/4
SW_ACC_0(config-if)#switchport mode access
SW_ACC_0(config-if)#switchport access vlan 3
SW_ACC_0(config-if)#exit
```

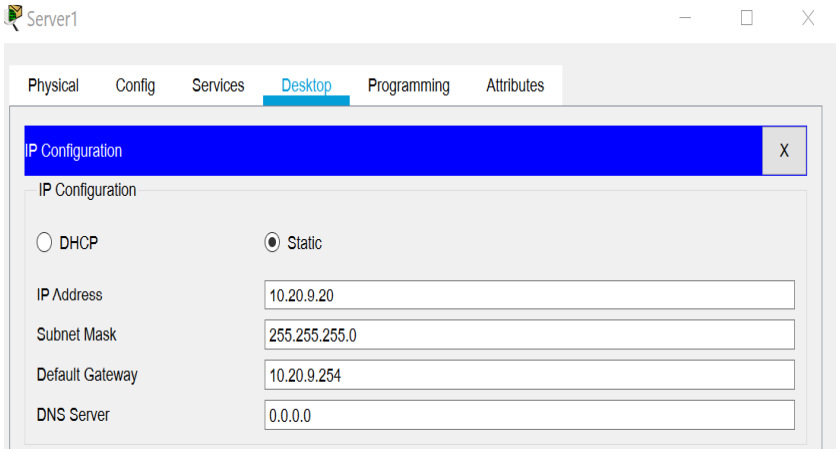
Vérification les interfaces avec la commande « SHOW Interfaces STATUS ».

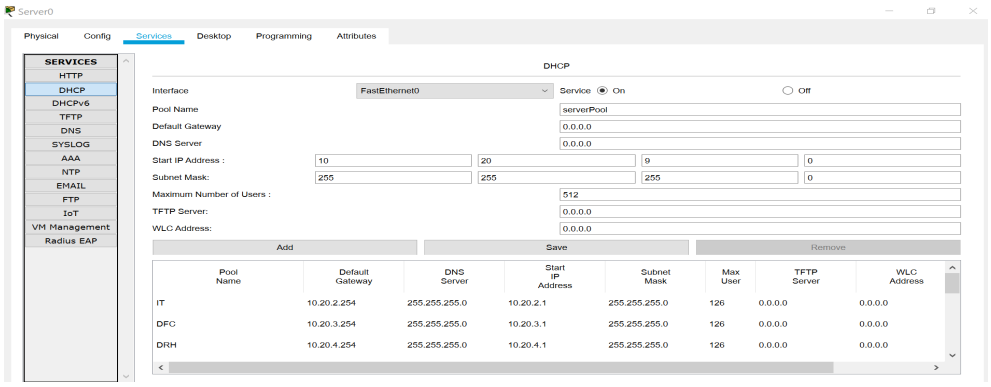
```
SW_ACC_0#SH INT STATUS
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          auto    auto  10/100BaseTX
Fa0/2                        connected    1          auto    auto  10/100BaseTX
Fa0/3                        connected    2          auto    auto  10/100BaseTX
Fa0/4                        connected    3          auto    auto  10/100BaseTX
Fa0/5                        notconnect   1          auto    auto  10/100BaseTX
Fa0/6                        notconnect   1          auto    auto  10/100BaseTX
Fa0/7                        notconnect   1          auto    auto  10/100BaseTX
Fa0/8                        notconnect   1          auto    auto  10/100BaseTX
Fa0/9                        notconnect   1          auto    auto  10/100BaseTX
Fa0/10                       notconnect   1          auto    auto  10/100BaseTX
Fa0/11                       notconnect   1          auto    auto  10/100BaseTX
Fa0/12                       notconnect   1          auto    auto  10/100BaseTX
Fa0/13                       notconnect   1          auto    auto  10/100BaseTX
Fa0/14                       notconnect   1          auto    auto  10/100BaseTX
Fa0/15                       notconnect   1          auto    auto  10/100BaseTX
Fa0/16                       notconnect   1          auto    auto  10/100BaseTX
Fa0/17                       notconnect   1          auto    auto  10/100BaseTX
Fa0/18                       notconnect   1          auto    auto  10/100BaseTX
Fa0/19                       notconnect   1          auto    auto  10/100BaseTX
Fa0/20                       notconnect   1          auto    auto  10/100BaseTX
Fa0/21                       notconnect   1          auto    auto  10/100BaseTX
 --More--
```

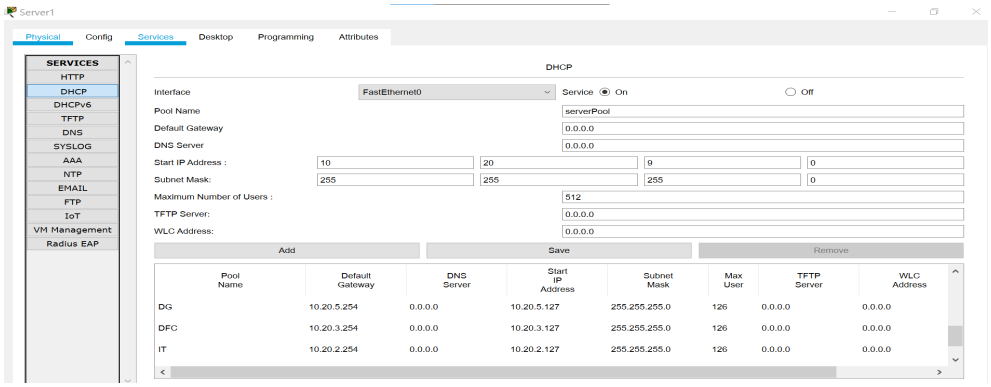
- **Configuration du serveur**

Configuré le protocole DHCP (Dynamic Host Configuration Protocol) sur les deux serveurs pour attribuer automatiquement des adresses IP aux périphériques connectés au VLAN.









- **Ajouter la commande IP helper address**

Ajouter la commande « ip helper address » dans le switch cœur pour permettre l'attribution automatique d'adresses IP aux périphériques connectés aux VLAN via le protocole DHCP.

```
SWcoeur#CONFIG T
Enter configuration commands, one per line.  End with CNTL/Z.
SWcoeur(config)#int vlan 2
SWcoeur(config-if)#ip helper-add 10.20.9.10
SWcoeur(config-if)#int vlan 3
SWcoeur(config-if)#ip helper-add 10.20.9.10
```

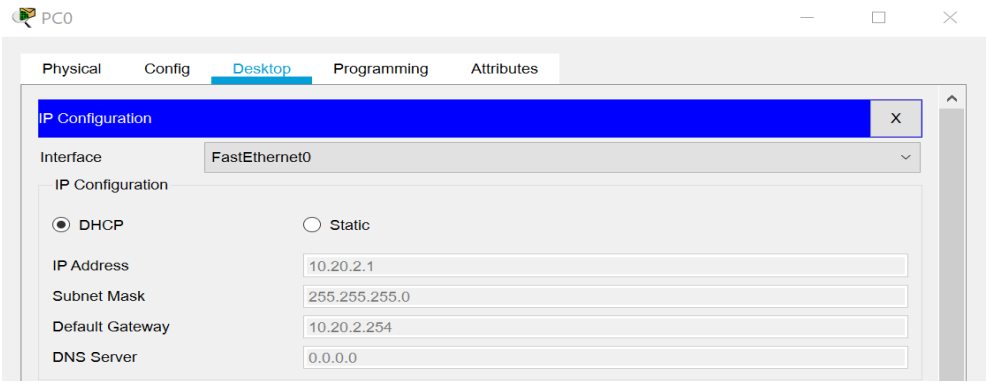
```
SWcoeur(config-if)#int vlan 2
SWcoeur(config-if)#ip helper-add 10.20.9.20
SWcoeur(config-if)#int vlan 3
SWcoeur(config-if)#ip helper-add 10.20.9.20
```

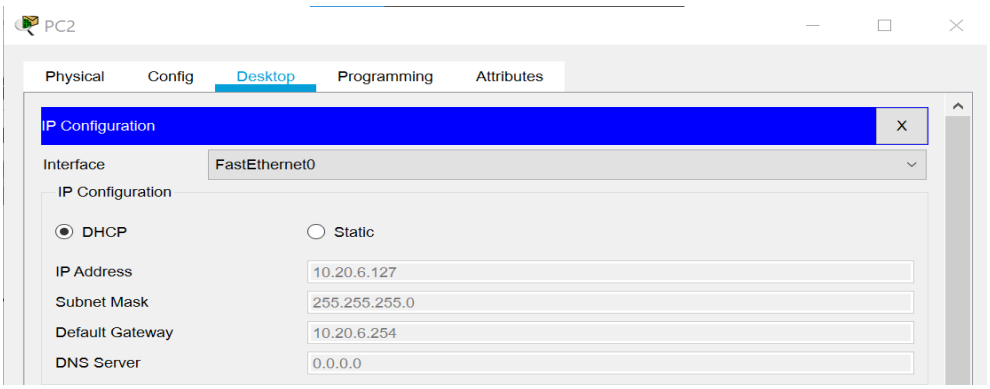
Vérification Avec la commande « Show running-config ».

```
interface Vlan2
 mac-address 0002.17d2.8c01
 ip address 10.20.2.254 255.255.255.0
 ip helper-address 10.20.9.10
 ip helper-address 10.20.9.254
 ip helper-address 10.20.9.20
!
interface Vlan3
 mac-address 0002.17d2.8c02
 ip address 10.20.3.254 255.255.255.0
 ip helper-address 10.20.9.10
 ip helper-address 10.20.9.254
 ip helper-address 10.20.9.20
```

- **Configurations des PC**

Les adresses IP, les masques sous réseaux et les passerelles seront configurées en mode DHCP





- **Tester la connectivité**

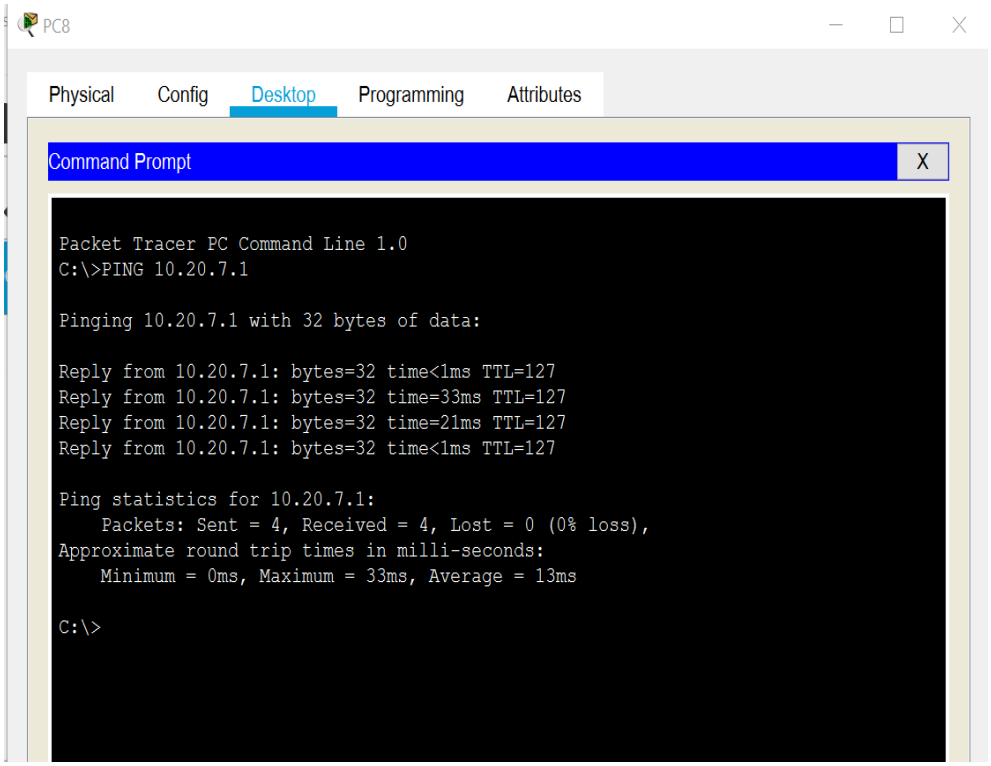


FIGURE A.1 – Test entre PC8 (Vlan 8) et PC3 (Vlan 7)

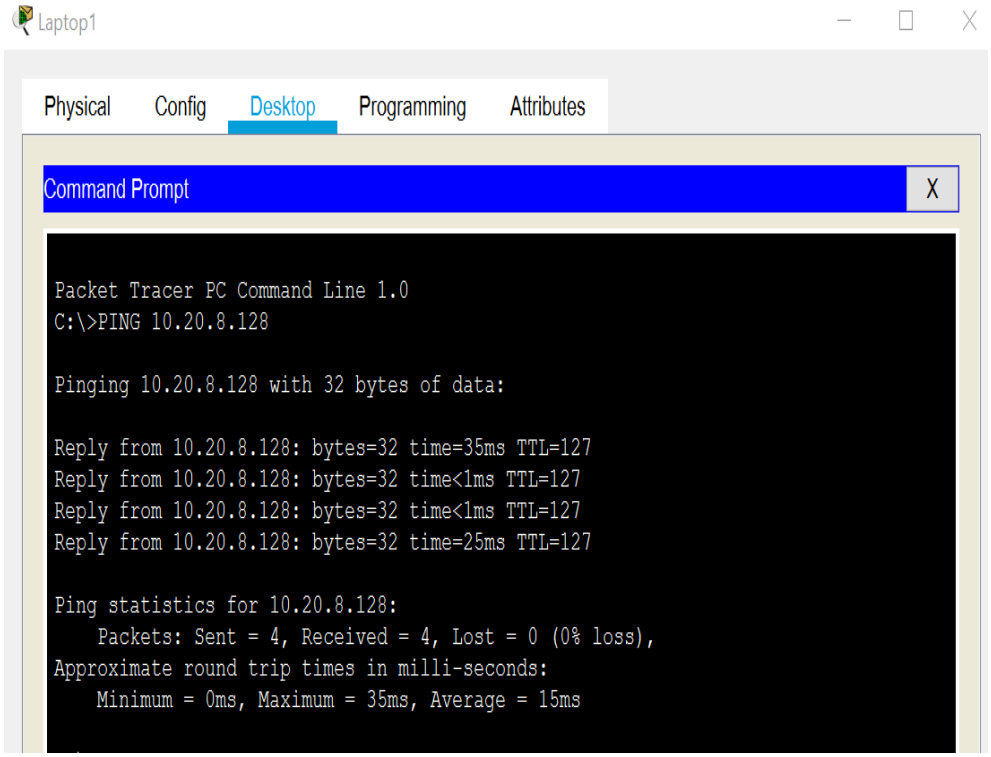


FIGURE A.2 – Test entre Laptop1 (Vlan 4) et Laptop1 (Vlan 8)

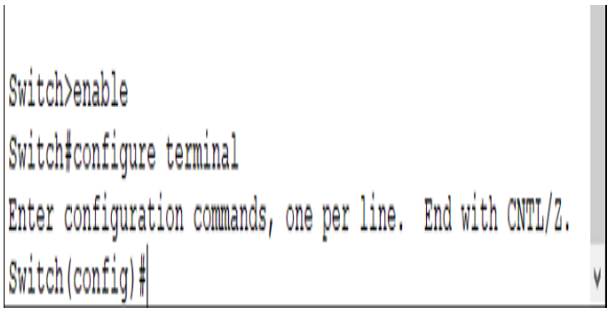
Annexe B

Annexe 2

B.1 Implémentation sur simulateur l'architecture proposée

1. **Couche cœur**

   (a) **Accès au mode de configuration :**
   Une fois les dispositifs connectés physiquement, nous accédons au mode privilégié des équipements pour bénéficier de privilèges étendus. Ensuite, nous entrons dans le mode de configuration pour initialiser les paramètres de base du réseau.



   (b) **Nom du switch :** Nous procédons à la configuration de base de notre topologie réseau. Nous commençons par attribuer des noms d'hôtes aux switches cœurs pour les distinguer des autres équipements du réseau. Cette étape est essentielle pour faciliter l'identification et la gestion de cet appareil .

```
Switch(config)#
Switch(config)#hostname SWCOEUR_1
SWCOEUR_1(config)#
SWCOEUR_1(config)#
SWCOEUR_1(config)#
SWCOEUR_1(config)#
```

```
Switch(config)#
Switch(config)#hostname SWCOEUR_2
SWCOEUR_2(config)#
SWCOEUR 2(config)#
```

(c) **Configuration de la bannière MOTD :** Configuration la bannière Message of the Day (MOTD) pour fournir des informations importantes aux utilisateurs se connectant aux équipements du réseau.

```
SWCOEUR_1(config)#
SWCOEUR_1(config)#banner motd "BIENVENUE SUE LE RESEAU
CEVITAL". Reseau securise et performant pour soutenir nos
operations et nos equipes. pour toute demande d'assistance
technique, veuillez connecter notre equipe IT
SWCOEUR_1(config)#
```

```
SWCOEUR_2(config)#
SWCOEUR_2(config)#banner mot "BIENVENUE SUR LE RESEAU
CEVITAL". Reseau securise et performant pour soutenir nos
operations et nos equipes. Pour toute demande d'assistance
technique, veuillez connecter notre equipe IT.
SWCOEUR_2(config)#
```

(d) **Configuration VTP :**

- **Indiquer le mode VTP.**
- **Attribution du domaine Name VTP.**
- **Activation du mot de passe VTP.**

Pour simplifier la gestion des VLANs dans notre infrastructure réseau, nous mettons en place le protocole VTP (VLAN Trunking Protocol). Nous configurons le switch cœur en tant que serveur VTP et les autres switches en tant que clients VTP pour permettre la distribution automatique des informations VLAN. En spécifiant un domaine VTP et un mot de passe commun et en configurant le mode de transmission approprié (client, serveur ou transparent) sur chaque switch.

```
SWCOEUR_1(config)#
SWCOEUR_1(config)#vtp mode server
Device mode already VTP SERVER.
SWCOEUR_1(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
SWCOEUR_1(config)#vtp password VTP_Res3au@2024
Setting device VLAN database password to VTP_Res3au@2024
SWCOEUR_1(config)#
```

```
SWCOEUR_2(config)#
SWCOEUR_2(config)#vtp mode client
Setting device to VTP CLIENT mode.
SWCOEUR_2(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
SWCOEUR_2(config)#vtp password VTP_Res3au@2024
Setting device VLAN database password to VTP_Res3au@2024
SWCOEUR_2(config)#
```

- Vérification VTP avec la commande « show vtp statuts »

```
SWCOEUR_1#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.C963.B400
Configuration last modified by 0.0.0.0 at 3-1-93 00:10:01
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN :
--------------
VTP Operating Mode                : Server
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 17
Configuration Revision            : 24
MD5 digest                        : 0x36 0x25 0x63 0x1F 0x52
0x00 0xB3 0xA6
                                    0x34 0x49 0x00 0x05 0x83
0xE3 0x8F 0x95
```

```
SWCOEUR_2#
SWCOEUR_2#show vtp status
VTP Version capable             : 1 to 2
VTP version running             : 1
VTP Domain Name                 : cevital.com
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : 0001.6321.EB00
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Feature VLAN :
--------------
VTP Operating Mode                : Client
Maximum VLANs supported locally   : 1005
Number of existing VLANs          : 5
Configuration Revision            : 0
MD5 digest                        : 0xFF 0x2F 0x18 0xF1 0x30
0x32 0xE2 0x44
                                    0x76 0x9E 0x31 0x7E 0x68
0xCE 0xA7 0xFC
```

(e) **Configuration les VLAN :**

- Création des VLANs.

Pour optimiser la segmentation et la gestion du réseau, nous avons configuré la création de 12 VLAN distincts sur le switch cœur 1, permettant ainsi une isolation et une sécurisation accrues des différents segments de réseau.

```
SWCOEUR_1(config-vlan)#
SWCOEUR_1(config-vlan)#vlan 2
SWCOEUR_1(config-vlan)#name IT
SWCOEUR_1(config-vlan)#vlan 3
SWCOEUR_1(config-vlan)#name DG
SWCOEUR_1(config-vlan)#vlan 4
SWCOEUR_1(config-vlan)#name DFC
SWCOEUR_1(config-vlan)#vlan 5
SWCOEUR_1(config-vlan)#name DRH
SWCOEUR_1(config-vlan)#vlan 6
SWCOEUR_1(config-vlan)#name RF_SUCRE
SWCOEUR_1(config-vlan)#vlan 7
SWCOEUR_1(config-vlan)#name RF_HUILE
SWCOEUR_1(config-vlan)#vlan 8
SWCOEUR_1(config-vlan)#name MARGARINERIE
SWCOEUR_1(config-vlan)#vlan 9
SWCOEUR_1(config-vlan)#name SERVER
SWCOEUR_1(config-vlan)#vlan 10
SWCOEUR_1(config-vlan)#name IMPRIMANTE
SWCOEUR_1(config-vlan)#vlan 11
SWCOEUR_1(config-vlan)#name GUEST_WIFI
SWCOEUR_1(config-vlan)#vlan 12
SWCOEUR_1(config-vlan)#name ENERGIE
SWCOEUR_1(config-vlan)#vlan 13
SWCOEUR_1(config-vlan)#name PRODUCTION
SWCOEUR_1(config-vlan)#
```

- Vérification LES VLAN avec la commande « show VLAN BRIEF »

```
Gig1/1/2, Gig1/1/3, Gig1/1/4
2    IT                                active
3    DG                                active
4    DFC                               active
5    DRH                               active
6    RF_SUCRE                          active
7    RF_HUILE                          active
8    MARGARINERIE                      active
9    SERVER                            active
10   IMPRIMANTE                        active
11   GUEST_WIFI                        active
12   ENERGIE                           active
13   PRODUCTION                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
SWCOEUR_1#
SWCOEUR 1#
```

(f) **Configuration des interface VLAN.**

Pour segmenter notre réseau en groupes logiques et isoler le trafic, nous procédons à la configuration de 12 VLANs (Virtual Local Area Networks) sur notre switch cœur. Une fois les VLANs créés, nous attribuons des ports spécifiques à chaque VLAN en les configurant en tant que membres de ces VLANs. nous configurons les interfaces VLAN avec des

adresses IP correspondant aux sous-réseaux associés à chaque VLAN. Nous configurons les passerelles par défaut de manière à répartir la charge entre les deux switchs : le premier switch cœur a comme passerelle 252 et le deuxième a comme passerelle 253.

```
SWCOEUR_1(config-if)#interface vlan2
SWCOEUR_1(config-if)#ip add 10.20.2.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan3
SWCOEUR_1(config-if)#ip add 10.20.3.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan4
SWCOEUR_1(config-if)#ip add 10.20.4.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan5
SWCOEUR_1(config-if)#ip add 10.20.5.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan6
SWCOEUR_1(config-if)#ip add 10.20.6.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan7
SWCOEUR_1(config-if)#ip add 10.20.7.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan8
SWCOEUR_1(config-if)#ip add 10.20.8.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan9
SWCOEUR_1(config-if)#ip add 10.20.9.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan10
SWCOEUR_1(config-if)#ip add 10.20.10.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan11
SWCOEUR_1(config-if)#ip add 10.20.11.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan12
SWCOEUR_1(config-if)#ip add 10.20.12.252 255.255.255.0
SWCOEUR_1(config-if)#interface vlan13
SWCOEUR_1(config-if)#ip add 10.20.13.252 255.255.255.0
SWCOEUR_1(config-if)#
SWCOEUR_1(config-if)#
```

```
SWCOEUR_2(config)#interface vlan2
SWCOEUR_2(config-if)#ip add 10.20.2.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan3
SWCOEUR_2(config-if)#ip add 10.20.3.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan4
SWCOEUR_2(config-if)#ip add 10.20.4.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan5
SWCOEUR_2(config-if)#ip add 10.20.5.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan6
SWCOEUR_2(config-if)#ip add 10.20.6.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan7
SWCOEUR_2(config-if)#ip add 10.20.7.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan8
SWCOEUR_2(config-if)#ip add 10.20.8.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan9
SWCOEUR_2(config-if)#ip add 10.20.9.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan10
SWCOEUR_2(config-if)#ip add 10.20.10.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan11
SWCOEUR_2(config-if)#ip add 10.20.11.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan12
SWCOEUR_2(config-if)#ip add 10.20.12.253 255.255.255.0
SWCOEUR_2(config-if)#interface vlan13
SWCOEUR_2(config-if)#ip add 10.20.13.253 255.255.255.0
SWCOEUR_2(config-if)#
```

- Vérification les Interfaces avec la commande « show running-config »

```
interface Vlan2
 mac-address 00e0.f965.6201
 ip address 10.20.2.252 255.255.255.0
!
interface Vlan3
 mac-address 00e0.f965.6202
 ip address 10.20.3.252 255.255.255.0
!
interface Vlan4
 mac-address 00e0.f965.6203
 ip address 10.20.4.252 255.255.255.0
!
interface Vlan5
 mac-address 00e0.f965.6204
 ip address 10.20.5.252 255.255.255.0
!
interface Vlan6
 mac-address 00e0.f965.6205
 ip address 10.20.6.252 255.255.255.0
!
interface Vlan7
 mac-address 00e0.f965.6206
 ip address 10.20.7.252 255.255.255.0
!
interface Vlan8
 mac-address 00e0.f965.6207
 ip address 10.20.8.252 255.255.255.0
 --More--
```

```
interface Vlan9
 mac-address 00e0.f965.6208
 ip address 10.20.9.252 255.255.255.0
!
interface Vlan10
 mac-address 00e0.f965.6209
 ip address 10.20.10.252 255.255.255.0
!
interface Vlan11
 mac-address 00e0.f965.620a
 ip address 10.20.11.252 255.255.255.0
!
interface Vlan12
 mac-address 00e0.f965.620b
 ip address 10.20.12.252 255.255.255.0
!
interface Vlan13
 mac-address 00e0.f965.620c
 ip address 10.20.13.252 255.255.255.0
!
ip classless
```

```
interface Vlan2
 mac-address 0000.0c4e.4101
 ip address 10.20.2.253 255.255.255.0
!
interface Vlan3
 mac-address 0000.0c4e.4102
 ip address 10.20.3.253 255.255.255.0
!
interface Vlan4
 mac-address 0000.0c4e.4103
 ip address 10.20.4.253 255.255.255.0
!
interface Vlan5
 mac-address 0000.0c4e.4104
 ip address 10.20.5.253 255.255.255.0
!
interface Vlan6
 mac-address 0000.0c4e.4105
 ip address 10.20.6.253 255.255.255.0
!
interface Vlan7
 mac-address 0000.0c4e.4106
 ip address 10.20.7.253 255.255.255.0
!
interface Vlan8
 mac-address 0000.0c4e.4107
 ip address 10.20.8.253 255.255.255.0
```

```
interface Vlan9
 mac-address 0000.0c4e.4108
 ip address 10.20.9.253 255.255.255.0
!
interface Vlan10
 mac-address 0000.0c4e.4109
 ip address 10.20.10.253 255.255.255.0
!
interface Vlan11
 mac-address 0000.0c4e.410a
 ip address 10.20.11.253 255.255.255.0
!
interface Vlan12
 mac-address 0000.0c4e.410b
 ip address 10.20.12.253 255.255.255.0
!
interface Vlan13
 mac-address 0000.0c4e.410c
 ip address 10.20.13.253 255.255.255.0
!
ip classless
```

- Activation du routage IP

Nous activons le routage IP sur notre switch cœur. Cette étape est cruciale pour permettre au réseau de router les paquets entre les différents réseaux virtuels créés par les VLANs. Nous activons le protocole de routage IP en utilisant la commande : "ip routing" pour activer le routage sur le switch. En activant le routage IP, nous permettons au switch de fonctionner comme un routeur, acheminant les paquets entre les différentes interfaces et sous-réseaux.

```
SWCOEUR_1(config)#
SWCOEUR_1(config)#
SWCOEUR_1(config)#ip routing
SWCOEUR_1(config)#
```

```
SWCOEUR_2(config)#
SWCOEUR_2(config)#
SWCOEUR_2(config)#ip routing
SWCOEUR_2(config)#
SWCOEUR_2(config)#
```

(g) **Configuration le DHCP.**

- Configuration des pools DHCP.

- Attribution des options DHCP (passerelle par défaut).

- Exclusion d'adresses IP.

Pour simplifier la gestion des adresses IP au sein de notre réseau, il faut mettre en place un service DHCP sur nos deux switchs cœurs. Nous organisons la configuration de manière à répartir les adresses IP disponibles de manière équilibrée entre les deux switches cœurs. Ainsi, la moitié des adresses IP, allant de 1 à 126, sont configurées sur le premier switch cœur, tandis que l'autre moitié, de 127 à 251, sont attribuées au deuxième switch cœur. De plus, nous configurons les passerelles par défaut 254. Nous définissons ces paramètres dans les pools DHCP correspondants, en spécifiant les plages d'adresses IP et les passerelles par défaut appropriées pour chaque switch. En activant le service DHCP sur les interfaces VLANs correspondantes, nous assurons une distribution automatique et équilibrée des adresses IP aux périphériques connectés à chaque switch cœur.

```
SWCOEUR_1(dhcp-config)#ip dhcp pool IT
SWCOEUR_1(dhcp-config)#network 10.20.2.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.2.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.2.127 10.20.2.251
SWCOEUR_1(config)#ip dhcp pool DG
SWCOEUR_1(dhcp-config)#network 10.20.3.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.3.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.3.127 10.20.3.251
SWCOEUR_1(config)#ip dhcp pool DFC
SWCOEUR_1(dhcp-config)#network 10.20.4.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.4.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.4.127 10.20.4.251
SWCOEUR_1(config)#ip dhcp pool DRH
SWCOEUR_1(dhcp-config)#network 10.20.5.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.5.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.5.127 10.20.5.251
SWCOEUR_1(config)#ip dhcp pool RF_SUCRE
SWCOEUR_1(dhcp-config)#network 10.20.6.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.6.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.6.127 10.20.6.251
SWCOEUR_1(config)#ip dhcp pool RF_HUILE
SWCOEUR_1(dhcp-config)#network 10.20.7.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.7.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.7.127 10.20.7.251
SWCOEUR_1(config)#ip dhcp pool MARGARINERIE
SWCOEUR_1(dhcp-config)#network 10.20.8.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.8.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.8.127 10.20.8.251
SWCOEUR_1(config)#ip dhcp pool SERVER
```

```
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.8.127 10.20.8.251
SWCOEUR_1(config)#ip dhcp pool SERVER
SWCOEUR_1(dhcp-config)#network 10.20.9.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.9.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.9.127 10.20.9.251
SWCOEUR_1(config)#ip dhcp pool IMPRIMANTE
SWCOEUR_1(dhcp-config)#network 10.20.10.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.10.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.10.127 10.20.10.251
SWCOEUR_1(config)#ip dhcp pool GUEST_WIFI
SWCOEUR_1(dhcp-config)#network 10.20.11.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.11.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.11.127 10.20.11.251
SWCOEUR_1(config)#ip dhcp pool ENERGIE
SWCOEUR_1(dhcp-config)#network 10.20.12.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.12.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.12.127 10.20.12.251
SWCOEUR_1(config)#ip dhcp pool PRODUCTION
SWCOEUR_1(dhcp-config)#network 10.20.13.0 255.255.255.0
SWCOEUR_1(dhcp-config)#default-router 10.20.13.254
SWCOEUR_1(dhcp-config)#ip dhcp excluded-add 10.20.13.127 10.20.13.251
SWCOEUR_1(config)#END
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWCOEUR_2(config)#ip dhcp pool IT
SWCOEUR_2(dhcp-config)#network 10.20.2.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.2.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.2.1 10.20.2.126
SWCOEUR_2(config)#ip dhcp pool DG
SWCOEUR_2(dhcp-config)#network 10.20.3.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.3.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.3.1 10.20.3.126
SWCOEUR_2(config)#ip dhcp pool DFC
SWCOEUR_2(dhcp-config)#network 10.20.4.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.4.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.4.1 10.20.4.126
SWCOEUR_2(config)#ip dhcp pool DRH
SWCOEUR_2(dhcp-config)#network 10.20.5.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.5.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.5.1 10.20.5.126
SWCOEUR_2(config)#ip dhcp pool RF_SUCRE
SWCOEUR_2(dhcp-config)#network 10.20.6.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.6.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.6.1 10.20.6.126
SWCOEUR_2(config)#ip dhcp pool RF_HUILE
SWCOEUR_2(dhcp-config)#network 10.20.7.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.7.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.7.1 10.20.7.126
SWCOEUR_2(config)#ip dhcp pool MARGARINERIE
SWCOEUR_2(dhcp-config)#network 10.20.8.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.8.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.8.1 10.20.8.126
```

```
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.8.1 10.20.8.126
SWCOEUR_2(config)#ip dhcp pool SERVER
SWCOEUR_2(dhcp-config)#network 10.20.9.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.9.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.9.1 10.20.9.126
SWCOEUR_2(config)#ip dhcp pool IMPRIMANTE
SWCOEUR_2(dhcp-config)#network 10.20.10.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.10.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.19.1 10.20.10.126
SWCOEUR_2(config)#ip dhcp excluded-add 10.20.10.1 10.20.10.126
SWCOEUR_2(config)#ip dhcp pool GUEST_WIFI
SWCOEUR_2(dhcp-config)#network 10.20.11.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.11.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.11.1 10.20.11.126
SWCOEUR_2(config)#ip dhcp pool ENERGIE
SWCOEUR_2(dhcp-config)#network 10.20.12.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.12.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.12.1 10.20.12.126
SWCOEUR_2(config)#ip dhcp pool PRODUCTION
SWCOEUR_2(dhcp-config)#network 10.20.13.0 255.255.255.0
SWCOEUR_2(dhcp-config)#default-router 10.20.13.254
SWCOEUR_2(dhcp-config)#ip dhcp excluded-add 10.20.13.1 10.20.13.126
SWCOEUR_2(config)#
SWCOEUR_2(config)#
```

- Vérification le DHCP avec la commande « show running-config »

```
ip dhcp excluded-address 10.20.2.127 10.20.2.251
ip dhcp excluded-address 10.20.3.127 10.20.3.251
ip dhcp excluded-address 10.20.4.127 10.20.4.251
ip dhcp excluded-address 10.20.5.127 10.20.5.251
ip dhcp excluded-address 10.20.6.127 10.20.6.251
ip dhcp excluded-address 10.20.7.127 10.20.7.251
ip dhcp excluded-address 10.20.8.127 10.20.8.251
ip dhcp excluded-address 10.20.9.127 10.20.9.251
ip dhcp excluded-address 10.20.10.127 10.20.10.251
ip dhcp excluded-address 10.20.11.127 10.20.11.251
ip dhcp excluded-address 10.20.12.127 10.20.12.251
ip dhcp excluded-address 10.20.13.127 10.20.13.251
!
ip dhcp pool IT
 network 10.20.2.0 255.255.255.0
 default-router 10.20.2.254
ip dhcp pool DG
 network 10.20.3.0 255.255.255.0
 default-router 10.20.3.254
ip dhcp pool DFC
 network 10.20.4.0 255.255.255.0
 default-router 10.20.4.254
ip dhcp pool DRH
 network 10.20.5.0 255.255.255.0
 default-router 10.20.5.254
ip dhcp pool RF_SUCRE
 network 10.20.6.0 255.255.255.0
 default-router 10.20.6.254
ip dhcp pool RF_HUILE
 --More-- |
```

```
.
ip dhcp excluded-address 10.20.2.1 10.20.2.126
ip dhcp excluded-address 10.20.3.1 10.20.3.126
ip dhcp excluded-address 10.20.4.1 10.20.4.126
ip dhcp excluded-address 10.20.5.1 10.20.5.126
ip dhcp excluded-address 10.20.6.1 10.20.6.126
ip dhcp excluded-address 10.20.7.1 10.20.7.126
ip dhcp excluded-address 10.20.8.1 10.20.8.126
ip dhcp excluded-address 10.20.9.1 10.20.9.126
ip dhcp excluded-address 10.20.10.1 10.20.10.126
ip dhcp excluded-address 10.20.11.1 10.20.11.126
ip dhcp excluded-address 10.20.12.1 10.20.12.126
ip dhcp excluded-address 10.20.13.1 10.20.13.126
!
ip dhcp pool IT
 network 10.20.2.0 255.255.255.0
 default-router 10.20.2.254
ip dhcp pool DG
 network 10.20.3.0 255.255.255.0
 default-router 10.20.3.254
ip dhcp pool DFC
 network 10.20.4.0 255.255.255.0
 default-router 10.20.4.254
ip dhcp pool DRH
 network 10.20.5.0 255.255.255.0
 default-router 10.20.5.254
ip dhcp pool RF_SUCRE
 network 10.20.6.0 255.255.255.0
 default-router 10.20.6.254
 --More-- |
```

(h) **Configuration les port**

- Configuration du mode Trunk :

Pour assurer le transport efficace du trafic VLAN entre nos switchs cœurs et les switches de distribution, mon binôme et moi-même configurons les interfaces reliant les switches en mode trunk. Le mode trunk permet le transport simultané de plusieurs VLANs sur une seule interface, ce qui est essentiel pour garantir une connectivité entre les différents segments

de notre réseau.

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWCOEUR_1(config)#interface range g1/0/1-5
SWCOEUR_1(config-if-range)#switchport mode trunk
SWCOEUR_1(config-if-range)#
```

```
SWCOEUR_2(config)#
SWCOEUR_2(config)#interface range g1/0/1-6
SWCOEUR_2(config-if-range)#switchport mode trunk
SWCOEUR_2(config-if-range)#
```

-Vérification mode trunk avec la commande « show interface status »

```
SWCOEUR_1#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Gig1/0/1                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/2                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/3                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/4                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/5                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/6                     notconnect   trunk      auto    auto  10/100BaseTX
Gig1/0/7                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/8                     notconnect   1          auto    auto  10/100BaseTX
```

```
SWCOEUR_2#
SWCOEUR_2#show interface status
Port      Name               Status       Vlan       Duplex  Speed Type
Gig1/0/1                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/2                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/3                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/4                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/5                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/6                     notconnect   trunk      auto    auto  10/100BaseTX
Gig1/0/7                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/8                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/9                     notconnect   1          auto    auto  10/100BaseTX
```

(i) **Configuration le Protocole STP.**

- Activation du STP.
- Configuration des priorités bridge.

Afin d'éviter les boucles de commutation qui pourraient survenir dans notre infrastructure réseau, nous configurons le protocole STP (Spanning Tree Protocol) sur nos switches cœurs.

```
SWCOEUR_1(config)#
SWCOEUR_1(config)#spanning-tree vlan 2-7 priority 4096
SWCOEUR_1(config)#spanning-tree vlan 8-13 priority 8192
SWCOEUR_1(config)#
SWCOEUR_1(config)#
```

```
SWCOEUR_2(config)#
SWCOEUR_2(config)#spanning-tree vlan 2-7 priority 8192
SWCOEUR_2(config)#spanning-tree vlan 8-13 priority 4096
SWCOEUR_2(config)#
```

- Vérification STP avec commande « show spanning-tree ou show running-config. »

```
!
!
!
spanning-tree mode pvst
spanning-tree vlan 2-7 priority 4096
spanning-tree vlan 8-13 priority 8192
!
!
!
```

```
!
!
spanning-tree mode pvst
spanning-tree vlan 8-13 priority 4096
spanning-tree vlan 2-7 priority 8192
!
!
```

(j) **Configuration le Protocole HSRP.**

Pour garantir une haute disponibilité et une redondance au niveau de la passerelle par défaut de notre réseau, nous mettons en place le protocole HSRP (Hot Standby Router Protocol) sur nos switches cœurs. Le protocole HSRP permet de configurer un routeur actif et un rou-

teur de secours, assurant ainsi une commutation transparente en cas de défaillance de l'équipement principal.

```
SWCOEUR_1(config)#interface vlan2
SWCOEUR_1(config-if)#standby 2 ip 10.20.2.254
SWCOEUR_1(config-if)#standby 2 priority 105
SWCOEUR_1(config-if)#standby 2 preempt
%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Standby -> Active

SWCOEUR_1(config-if)#exi
SWCOEUR_1(config)#interface vlan3
SWCOEUR_1(config-if)#standby 3 ip 10.20.3.254
SWCOEUR_1(config-if)#standby 3 priority 105
SWCOEUR_1(config-if)#standby 3 preempt
SWCOEUR_1(config-if)#exit
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan3 Grp 3 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan3 Grp 3 state Standby -> Active

SWCOEUR_1(config)#interface vlan4
SWCOEUR_1(config-if)#standby 4 ip 10.20.4.254
SWCOEUR_1(config-if)#standby 4 priority 105
SWCOEUR_1(config-if)#standby 4 preempt
SWCOEUR_1(config-if)#exit
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan4 Grp 4 state Standby -> Active

SWCOEUR_1(config)#interface vlan5
SWCOEUR_1(config-if)#standby 5 ip 10.20.5.254
SWCOEUR_1(config-if)#standby 5 priority 105
SWCOEUR_1(config-if)#standby 5 preempt
SWCOEUR_1(config-if)#e
```

```
SWCOEUR_1(config)#interface vlan6
SWCOEUR_1(config-if)#standby 6 ip 10.20.6.254
SWCOEUR_1(config-if)#standby 6 priority 105
SWCOEUR_1(config-if)#standby 6 preempt
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan6 Grp 6 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan6 Grp 6 state Standby -> Active

SWCOEUR_1(config)#interface vlan7
SWCOEUR_1(config-if)#standby 7 ip 10.20.7.254
SWCOEUR_1(config-if)#standby 7 priority 105
SWCOEUR_1(config-if)#standby 7 preempt
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan7 Grp 7 state Standby -> Active

SWCOEUR_1(config)#interface vlan8
SWCOEUR_1(config-if)#standby 8 ip 10.20.8.254
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan8 Grp 8 state Speak -> Standby

SWCOEUR_1(config)#interface vlan9
SWCOEUR_1(config-if)#standby 9 ip 10.20.9.254
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan9 Grp 9 state Speak -> Standby
```

```
SWCOEUR_1(config)#interface vlan9
SWCOEUR_1(config-if)#standby 9 ip 10.20.9.254
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan9 Grp 9 state Speak -> Standby

SWCOEUR_1(config)#interface vlan10
SWCOEUR_1(config-if)#standby 10 ip 10.20.10.254
SWCOEUR_1(config-if)#exit
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby

SWCOEUR_1(config)#interface vlan11
SWCOEUR_1(config-if)#standby 11 ip 10.20.11.254
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Speak -> Standby

SWCOEUR_1(config)#interface vlan12
SWCOEUR_1(config-if)#standby 12 ip 10.20.12.254
SWCOEUR_1(config-if)#EXIT
SWCOEUR_1(config)#
%HSRP-6-STATECHANGE: Vlan12 Grp 12 state Speak -> Standby

SWCOEUR_1(config)#interface vlan13
SWCOEUR_1(config-if)#standby 13 ip 10.20.13.254
SWCOEUR_1(config-if)#EXIT
```

```
SWCOEUR_2(config)#interface vlan8
SWCOEUR_2(config-if)#standby 8 ip 10.20.8.254
SWCOEUR_2(config-if)#standby 8 priority 105
SWCOEUR_2(config-if)#standby 8 preempt
SWCOEUR_2(config-if)#exit
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan8 Grp 8 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan8 Grp 8 state Standby -> Active

SWCOEUR_2(config)#interface vlan9
SWCOEUR_2(config-if)#standby 9 ip 10.20.9.254
SWCOEUR_2(config-if)#standby 9 priority 105
SWCOEUR_2(config-if)#standby 9 preempt
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan9 Grp 9 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan9 Grp 9 state Standby -> Active

SWCOEUR_2(config)#interface vlan10
SWCOEUR_2(config-if)#standby 10 ip 10.20.10.254
SWCOEUR_2(config-if)#standby 10 priority 105
SWCOEUR_2(config-if)#standby 10 preempt
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active

SWCOEUR_2(config)#interface vlan11
SWCOEUR_2(config-if)#standby 11 ip 10.20.11.254


SWCOEUR_2(config)#interface vlan11
SWCOEUR_2(config-if)#standby 11 ip 10.20.11.254
SWCOEUR_2(config-if)#standby 11 priority 105
SWCOEUR_2(config-if)#standby 11 preempt
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Speak -> Standby

%HSRP-6-STATECHANGE: Vlan11 Grp 11 state Standby -> Active

SWCOEUR_2(config)#interface vlan12
SWCOEUR_2(config-if)#standby 12 ip 10.20.12.254
SWCOEUR_2(config-if)#standby 12 priority 105
SWCOEUR_2(config-if)#standby 12 preempt
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan12 Grp 12 state Standby -> Active

SWCOEUR_2(config)#interface vlan13
SWCOEUR_2(config-if)#standby 13 ip 10.20.13.254
SWCOEUR_2(config-if)#standby 13 priority 105
SWCOEUR_2(config-if)#standby 13 preempt
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan13 Grp 13 state Standby -> Active

SWCOEUR_2(config)#interface vlan2
SWCOEUR_2(config-if)#standby 2 ip 10.20.2.254
SWCOEUR_2(config-if)#EXIT
```

```
%HSRP-6-STATECHANGE: Vlan2 Grp 2 state Speak -> Standby

SWCOEUR_2(config)#interface vlan3
SWCOEUR_2(config-if)#standby 3 ip 10.20.3.254
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan3 Grp 3 state Speak -> Standby

SWCOEUR_2(config)#interface vlan4
SWCOEUR_2(config-if)#standby 4 ip 10.20.4.254
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan4 Grp 4 state Speak -> Standby

SWCOEUR_2(config)#interface vlan5
SWCOEUR_2(config-if)#standby 5 ip 10.20.5.254
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan5 Grp 5 state Speak -> Standby

SWCOEUR_2(config)#interface vlan6
SWCOEUR_2(config-if)#standby 6 ip 10.20.6.254
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
%HSRP-6-STATECHANGE: Vlan6 Grp 6 state Speak -> Standby

SWCOEUR_2(config)#interface vlan7
SWCOEUR_2(config-if)#standby 7 ip 10.20.7.254
SWCOEUR_2(config-if)#EXIT
SWCOEUR_2(config)#
```

- Vérification HSRP avec commande « show standby brief . »

```
SWCOEUR_1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
Vl2         2    105 P Active   local           10.20.2.253     10.20.2.254
Vl3         3    105 P Active   local           10.20.3.253     10.20.3.254
Vl4         4    105 P Active   local           10.20.4.253     10.20.4.254
Vl5         5    105 P Active   local           10.20.5.253     10.20.5.254
Vl6         6    105 P Active   local           10.20.6.253     10.20.6.254
Vl7         7    105 P Active   local           10.20.7.253     10.20.7.254
Vl8         8    100   Standby  10.20.8.253     local           10.20.8.254
Vl9         9    100   Standby  10.20.9.253     local           10.20.9.254
Vl10        10   100   Standby  10.20.10.253    local           10.20.10.254
Vl11        11   100   Standby  10.20.11.253    local           10.20.11.254
Vl12        12   100   Standby  10.20.12.253    local           10.20.12.254
Vl13        13   100   Standby  10.20.13.253    local           10.20.13.254
SWCOEUR_1#
```

```
SWCOEUR_2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Pri P State    Active          Standby         Virtual IP
V12         2    100   Standby  10.20.2.252     local           10.20.2.254
V13         3    100   Standby  10.20.3.252     local           10.20.3.254
V14         4    100   Standby  10.20.4.252     local           10.20.4.254
V15         5    100   Standby  10.20.5.252     local           10.20.5.254
V16         6    100   Standby  10.20.6.252     local           10.20.6.254
V17         7    100   Standby  10.20.7.252     local           10.20.7.254
V18         8    105 P Active   local           10.20.8.252     10.20.8.254
V19         9    105 P Active   local           10.20.9.252     10.20.9.254
V110        10   105 P Active   local           10.20.10.252    10.20.10.254
V111        11   105 P Active   local           10.20.11.252    10.20.11.254
V112        12   105 P Active   local           10.20.12.252    10.20.12.254
V113        13   105 P Active   local           10.20.13.252    10.20.13.254
SWCOEUR_2#
```

(k) **La sécurité .**

- Activation du mot de passe « enable ».

- Configuration des accès console.

- Configuration des accès vty (Virtual Terminal Lines) pour les administrations à distance.

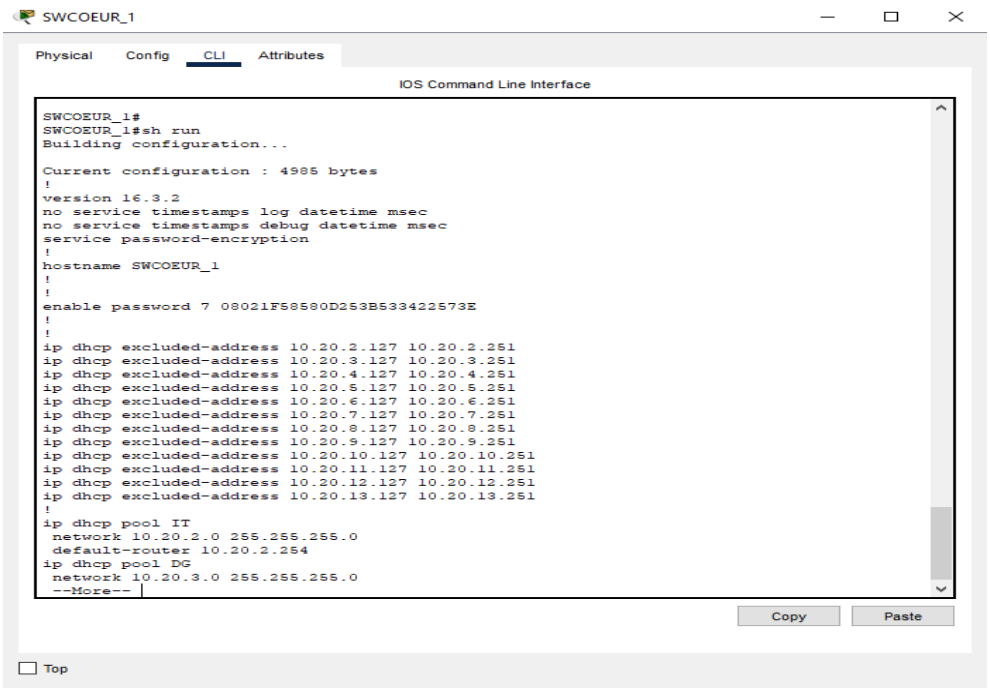
- Chiffrement des mots de passes.

Mettons en place une sécurité renforcée en définissant des mots de passe pour différents accès au switch cœur. Nous commençons par configurer un mot de passe d'activation (enable password) pour limiter l'accès privilégié à l'appareil. Ensuite, nous sécurisons l'accès à la console en attribuant un mot de passe à la ligne de console (line console). Cette mesure protège l'accès direct à l'appareil via le port console. De plus, nous configurons des mots de passe pour les lignes de type VTY (line vty) pour contrôler les connexions distantes au switch. Enfin, nous prenons soin de chiffrer les mots de passe.

```
SWCOEUR_2(config)#line console 0
SWCOEUR_2(config-line)#password C0nsOL3@S3cur3!
SWCOEUR_2(config-line)#login
SWCOEUR_2(config-line)#exit
SWCOEUR_2(config)#line vty 0 15
SWCOEUR_2(config-line)#password VtY_SecuR!te2024
SWCOEUR_2(config-line)#login
SWCOEUR_2(config-line)#exit
SWCOEUR_2(config)#enable password C3v1t@L!_N3t
SWCOEUR_2(config)#service password-encryprtion
                                            ^
% Invalid input detected at '^' marker.

SWCOEUR_2(config)#service password-encryption
SWCOEUR_2(config)#end
```

Vérification la sécurité avec la commande « show running-config »



(l) **Enregistrement de la configuration :**

Pour prévenir toute perte accidentelle de configuration et assurer une gestion efficace de notre infrastructure réseau, nous procédons à l'enregistrement régulier de la configuration sur nos switches. Nous utilisons la commande "copy running-config startup-config" ou l'abréviation "wr " pour sauvegarder la configuration actuelle dans la mémoire permanente du switch, assurant ainsi que les modifications apportées au réseau sont

persistantes même en cas de redémarrage.

```
SWCOEUR_1(config-vlan)#
SWCOEUR_1(config-vlan)#end
SWCOEUR_1#
%SYS-5-CONFIG_I: Configured from console by console

SWCOEUR_1#wr
Building configuration...
Compressed configuration from 7383 bytes to 3601 bytes[OK]
[OK]
SWCOEUR_1#
```

2. **Switch de distribution**

- **Accès au mode de configuration**
- **Nom de switch**

- **Configuration VTP**

Le protocole VTP (VLAN Trunking Protocol) est configuré en mode client sur les switches de distribution pour assurer une gestion centralisée et simplifiée des VLANs. Cela permet aux switches de distribution de recevoir automatiquement les informations de configuration des VLANs depuis les switches de cœur en mode serveur.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z
Switch(config)#hostname DIST_SUCRE
DIST_SUCRE(config)#vtp mode client
Setting device to VTP CLIENT mode.
DIST_SUCRE(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
DIST_SUCRE(config)#vtp password VTP_Res3au@2024
Setting device VLAN database password to VTP_Res3au@2024
DIST_SUCRE(config)#
```

- **Vérifier les VLANs Configurés**

Après avoir configuré les VLANs dans le switch cœur, la prochaine étape consiste à vérifier et à observer ces VLANs sur les switches de distribution.

```
2    IT                                active
3    DG                                active
4    DFC                               active
5    DRH                               active
6    RF_SUCRE                          active
7    RF_HUILE                          active
8    MARGARINERIE                      active
9    SERVER                            active
10   IMPRIMANTE                        active
11   GUEST_WIFI                        active
12   ENERGIE                           active
13   PRODUCTION                        active
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
DIST-SUCRE#
DIST-SUCRE#
```

- **Configuration des modes de ports**

Pour assurer une communication efficace et la transmission de plusieurs VLANs entre les différentes couches du réseau, les ports des switches de distribution sont configurés en mode trunk.

```
DIST_SUCRE(config)#
DIST_SUCRE(config)#interface range g1/0/3-5
DIST_SUCRE(config-if-range)#switchport mode trunk
DIST_SUCRE(config-if-range)#
```

- Verification le mode trunk avec la commande « show interface status »

```
DIST-SUCRE#sh int status
Port      Name               Status       Vlan       Duplex  Speed Type
Gig1/0/1                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/2                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/3                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/4                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/5                     connected    trunk      auto    auto  10/100BaseTX
Gig1/0/6                     notconnect   1          auto    auto  10/100BaseTX
Gig1/0/7                     notconnect   1          auto    auto  10/100BaseTX
```

- **La sécurité**

- Configuration du mot de passe enable.
- Configuration des accès console.
- Configuration des accès vty (Virtual Terminal Lines).
- Chiffrement des mots de passes.

```
DIST_SUCRE(config)#line console 0
DIST_SUCRE(config-line)#password C0ns0L3@S3cur3!
DIST_SUCRE(config-line)#login
DIST_SUCRE(config-line)#exit
DIST_SUCRE(config)#line vty 0 15
DIST_SUCRE(config-line)#password VtY_SecuR!te2024
DIST_SUCRE(config-line)#login
DIST_SUCRE(config-line)#exit
DIST_SUCRE(config)#enable password C3v1t@L!_N3t
DIST_SUCRE(config)#service password-encryption
DIST_SUCRE(config)#
```

Après avoir configuré le switch de distribution DIST-SUCRE et sauvegardé la configuration avec la commande copy running-config startup-config, les mêmes étapes de configuration ont été appliquées aux switches DIST-ADMINISTRATI et DIST-CORPS-GRAS. Cette démarche inclut la configuration des ports en mode trunk pour permettre une propagation efficace des VLANs et la centralisation des données. En outre, des mesures de sécurité ont été mises en place pour protéger les switches contre les accès non autorisés et les attaques potentielles.

3. **Switch d'accès**
   - Accès au mode de configuration globale
   - Attribution de noms aux switches
   - Configuration VTP
   - Configuration des modes de ports

   Dans le switch d'accès de la raffinerie de sucre 3500T, nous configurons les ports en mode accès pour les VLANs 6 et 13. Cette configuration permet de séparer efficacement le trafic entre les différents services ou départements de la raffinerie, assurant ainsi une gestion optimale du réseau.

```
Switch>
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNT
Switch(config)#hostname RF_SUCRE_3500T
RF_SUCRE_3500T(config)#vtp mode client
Setting device to VTP CLIENT mode.
RF_SUCRE_3500T(config)#vtp domain cevital?
WORD
RF_SUCRE_3500T(config)#vtp domain cevital.com
Changing VTP domain name from NULL to cevital.com
RF_SUCRE_3500T(config)#vtp password VTP_Res3au@2024
Setting device VLAN database password to VTP_Res3au@2024
RF_SUCRE_3500T(config)#interface f0/1
RF_SUCRE_3500T(config-if)#switchport mode access
RF_SUCRE_3500T(config-if)#switchport access vlan 6
RF_SUCRE_3500T(config-if)#exit
RF_SUCRE_3500T(config)#interface f0/2
RF_SUCRE_3500T(config-if)#switchport mode access
RF_SUCRE_3500T(config-if)#switchport access vlan 13
RF_SUCRE_3500T(config-if)#
```

- **La sécurité**

- Configuration du mot de passe enable.
- Configuration des accès console.
- Configuration des accès vty (Virtual Terminal Lines) pour les administrations à distance.
- Chiffrement des mots de passes

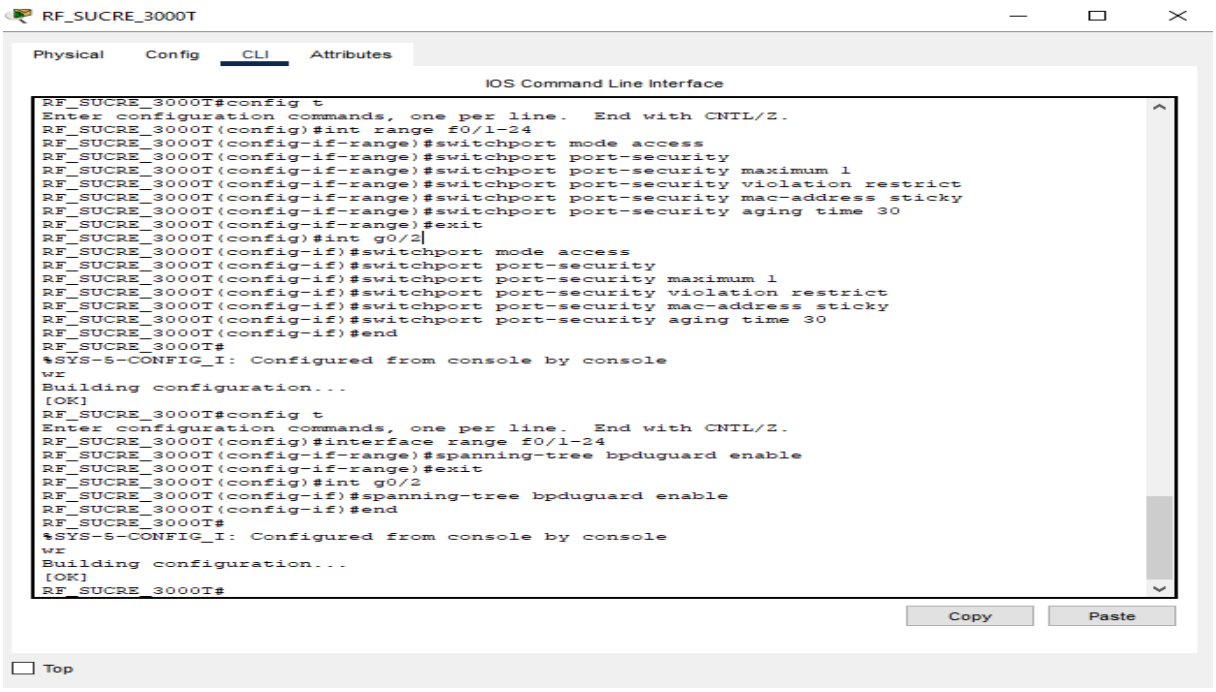
```
RF_SUCRE_3500T(config)#line console 0
RF_SUCRE_3500T(config-line)#password C0ns0L3@S3cur3!
RF_SUCRE_3500T(config-line)#login
RF_SUCRE_3500T(config-line)#exit
RF_SUCRE_3500T(config)#line vty 0 15
RF_SUCRE_3500T(config-line)#password VtY_SecuR!te2024
RF_SUCRE_3500T(config-line)#login
RF_SUCRE_3500T(config-line)#exit
RF_SUCRE_3500T(config)#enable password
% Incomplete command.
RF_SUCRE_3500T(config)#enable password C3v1t@L!_N3t
RF_SUCRE_3500T(config)#service password-encryption
RF_SUCRE_3500T(config)#
```

- Limitation des Adresses MAC Autorisées.

- Configuration de la Fonctionnalité de Sécurité BPDUguard (Bridge Protocol Data Unit Guard)

• BPDU Guard est une fonctionnalité qui désactive automatiquement un port de commutateurs d'accès si des BPDUs sont reçues sur ce port pour empêcher que d'autres commutateurs soient connectés, afin d'éviter des boucles et d'autres problèmes de réseau.

• BPDUs sont des messages échangés entre les commutateurs pour se protéger contre les boucles de communication.



• **Vérification la sécurité avec la commande « show running-config »**

```
interface FastEthernet0/1
 switchport access vlan 6
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security aging time 30
 spanning-tree bpduguard enable
!
interface FastEthernet0/2
 switchport access vlan 13
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security aging time 30
 spanning-tree bpduguard enable
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security violation restrict
 switchport port-security aging time 30
 spanning-tree bpduguard enable
!
interface FastEthernet0/4
```

Tous les switches d'accès suivent les mêmes étapes de configuration que celles appliquées au premier switch d'accès, RF_SUCRE_3000T. Ce switch, configuré pour répondre aux exigences spécifiques de la raffinerie de sucre, assure une connectivité fiable et sécurisée pour les utilisateurs. En standardisant la configuration des switches d'accès, nous garantissons une homogénéité dans la gestion du réseau, ce qui simplifie la maintenance et renforce la performance globale de l'infrastructure.

Les services Email et FTP

Dans notre architecture réseau proposée, le switch situé au niveau du data center, directement connecté aux switches cœur, joue un rôle vital dans la distribution des services aux utilisateurs finaux. Cette connexion privilégiée assure une haute disponibilité et des performances optimales pour les serveurs hébergeant les applications essentielles à l'entreprise.

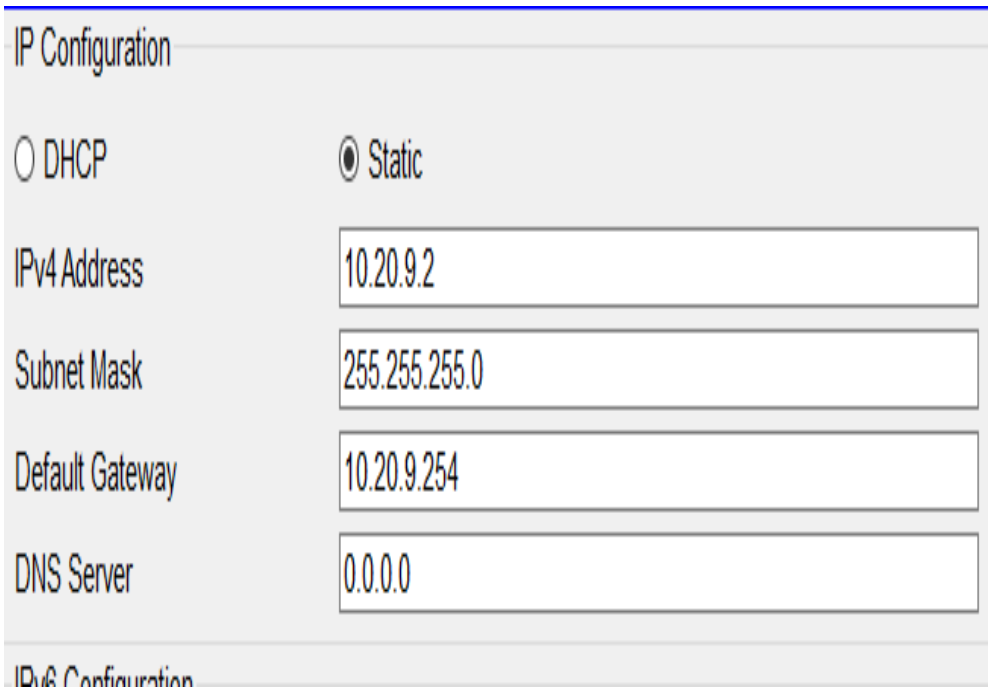
Quant à la configuration des services email et FTP sur les serveurs, elle revêt une importance stratégique. Le service email permet la communication électronique, tandis que le FTP facilite le partage de fichiers. Ces deux services sont essentiels au fonctionnement quotidien de l'entreprise, facilitant la collaboration entre les membres de l'équipe et la distribution d'informations cruciales. La configuration précise de ces services garantit une efficacité maximale et assure la sécurité des données transitant à travers le réseau.

Le serveur FTP

Dans notre topologie réseau proposée, nous avons intégré le service FTP pour faciliter le transfert sécurisé de fichiers entre les utilisateurs et les serveurs. En configurant ce service sur nos serveurs, nous avons permis une gestion centralisée et sécurisée des fichiers, répondant aux besoins spécifiques de notre infrastructure. Suivez les étapes de configuration comme suit :

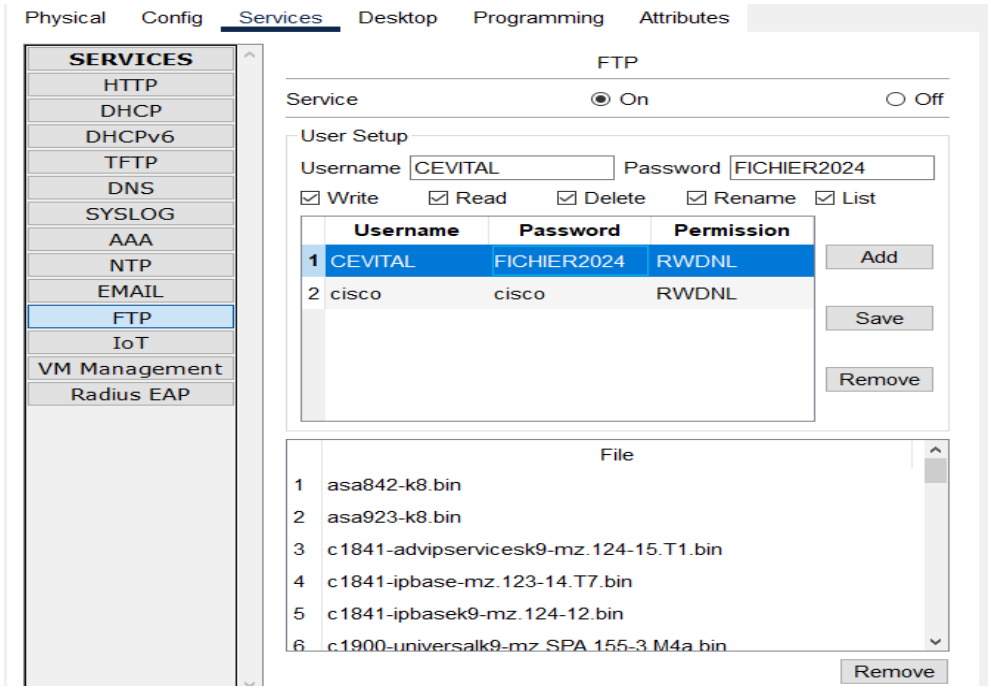
- **Attribuer une Adresse IP au Serveur :**

Pour assurer une connexion stable et constante, l'adresse IP du serveur FTP a été configurée manuellement en attribuant une adresse IP statique. Cela garantit que le serveur conserve la même adresse IP même après un redémarrage, facilitant ainsi l'accès pour les utilisateurs et les clients FTP dans le réseau.



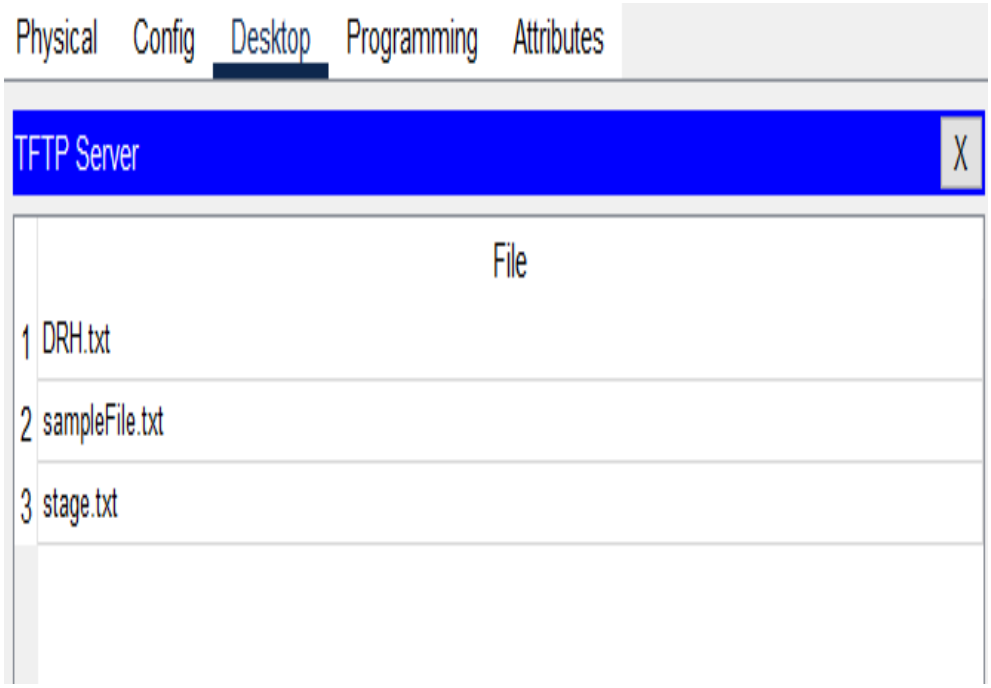
- **Configuration du Service FTP sur le Serveur :**

Pour activer le service FTP sur notre serveur, nous avons accédé à l'interface de gestion du serveur. Ensuite, nous avons navigué jusqu'à l'onglet "Services" et sélectionné l'option FTP pour l'activer. Une fois le service FTP activé, nous avons créé un compte utilisateur en cliquant sur l'option pour ajouter un nouvel utilisateur, puis en entrant un nom d'utilisateur et un mot de passe sécurisé. Après la création du compte, nous avons configuré les autorisations d'accès en sélectionnant les répertoires auxquels l'utilisateur peut accéder et en définissant les permissions de lecture et d'écriture nécessaires.



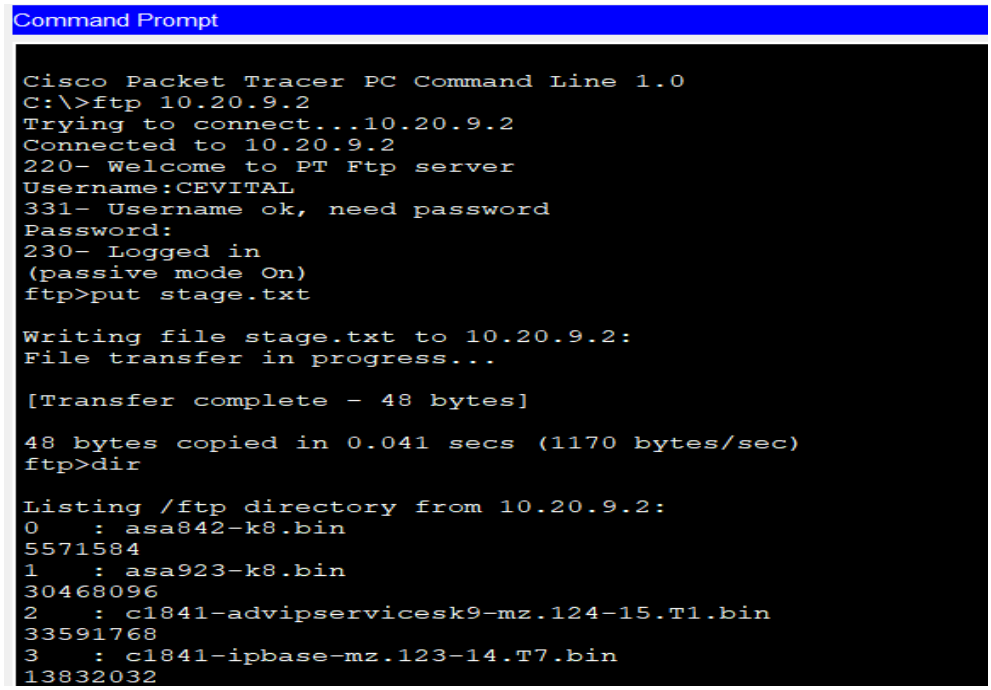
- **Crée un fichier :**

Dans le PC ADMIN_FTP, nous avons créé un fichier nommé « Stage ».



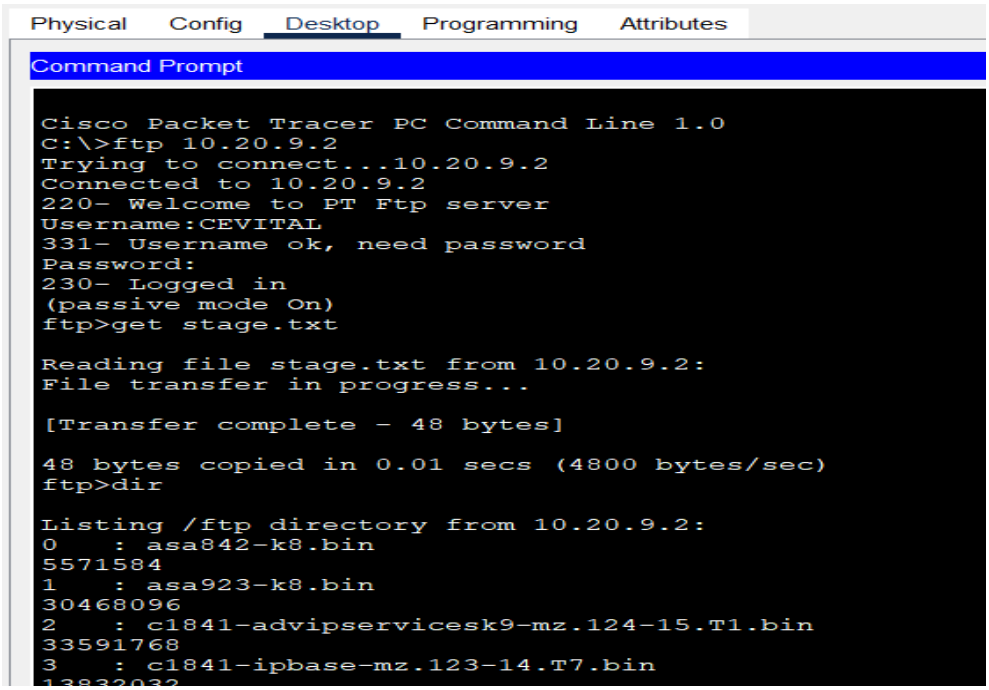
- **Transfert du Fichier vers le Serveur :**

Dans le PC ADMIN_FTP connecté au serveur, nous avons listé les fichiers existants sur le serveur. En utilisant la commande « put », nous avons transféré le fichier nommé « stage » depuis le PC CLIENT_FTP vers le serveur.



- **Téléchargement du Fichier :**

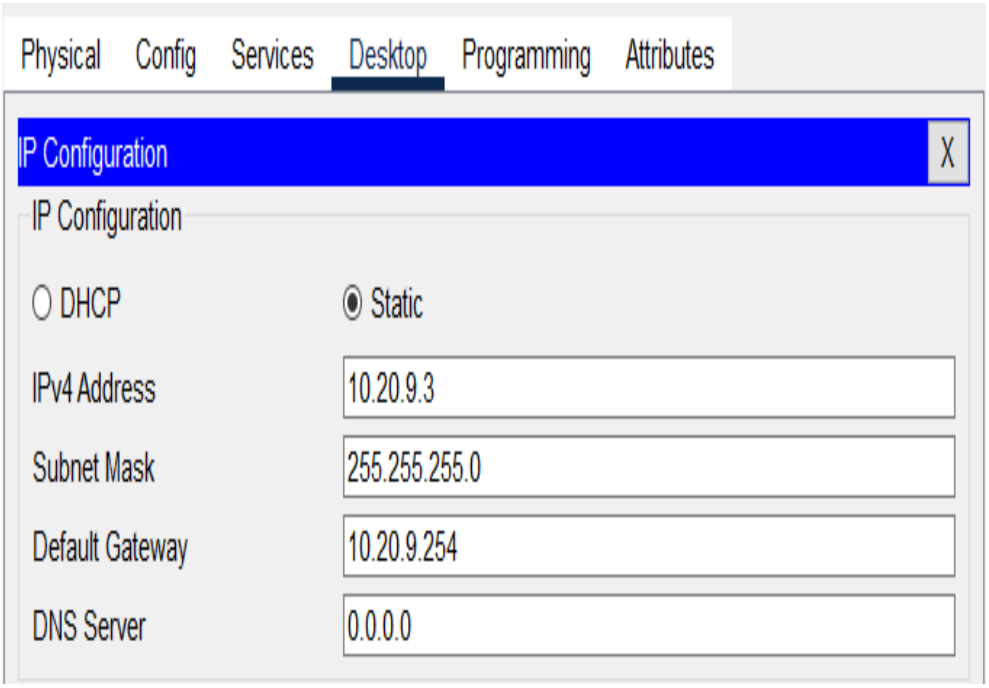
Dans le PC CLIENT_FTP connecté au serveur, nous avons utilisé la commande "get" pour télécharger le fichier "stage" du serveur vers le PC CLIENT_FTP. Ensuite, nous avons listé les fichiers existants sur le serveur pour vérifier que le téléchargement a été effectué avec succès.



Le serveur EMAIL

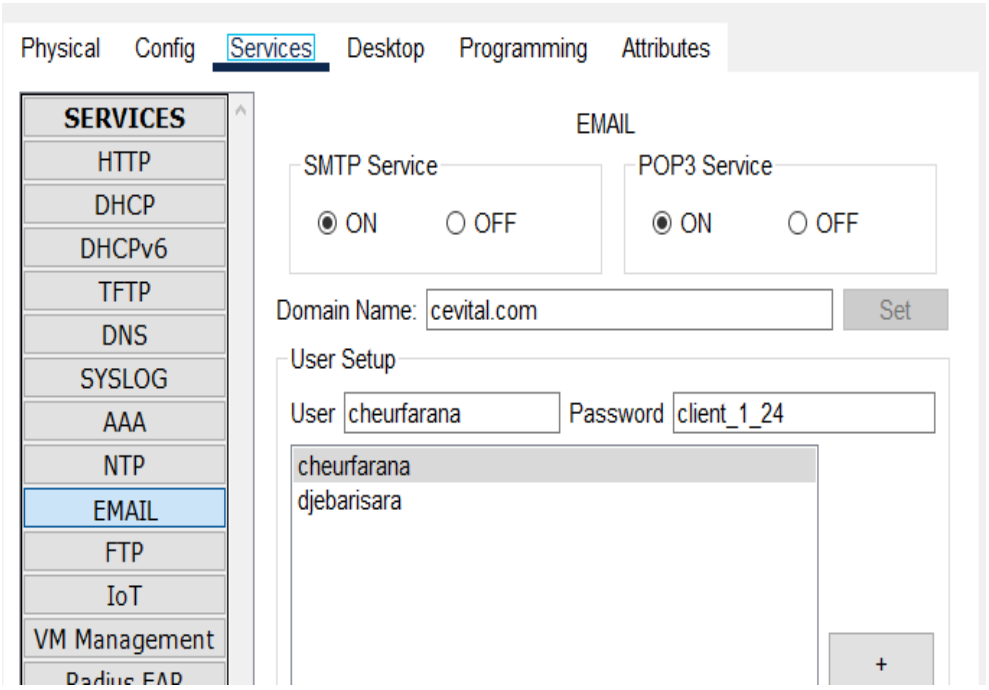
- **Attribuer une adresses IP au serveur :**

La première étape pour configurer le service email consiste à attribuer une adresse IP statique au serveur. Cette configuration manuelle assure que le serveur de messagerie est toujours accessible à la même adresse, facilitant ainsi l'envoi et la réception d'emails sans interruption.



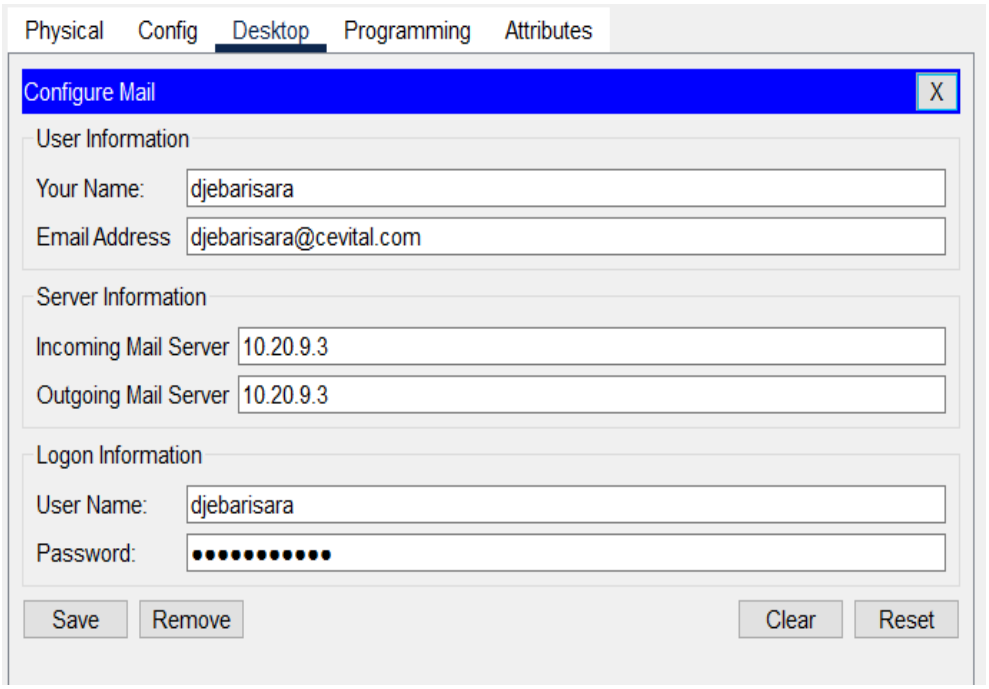
- **Configurer le service EMAIL sur le serveur :**

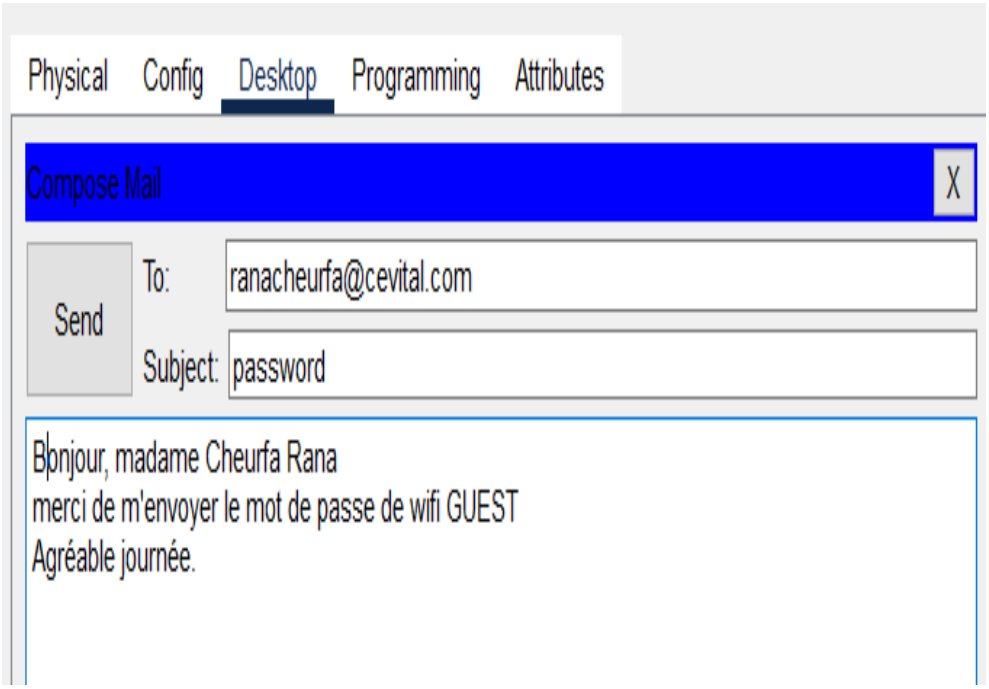
Dans la deuxième étape, nous avons configuré le service email via l'onglet "Services" du serveur. Nous avons commencé par activer le service email et entrer le nom de domaine spécifique pour notre réseau. Ensuite, nous avons créé des comptes utilisateurs en définissant des noms d'utilisateur et des mots de passe pour chaque employé ou membre de l'équipe. Cette configuration a permis de définir les adresses email et d'assurer une gestion efficace des comptes de messagerie pour tous les utilisateurs du réseau.



- **Configuration du PC émetteur :**

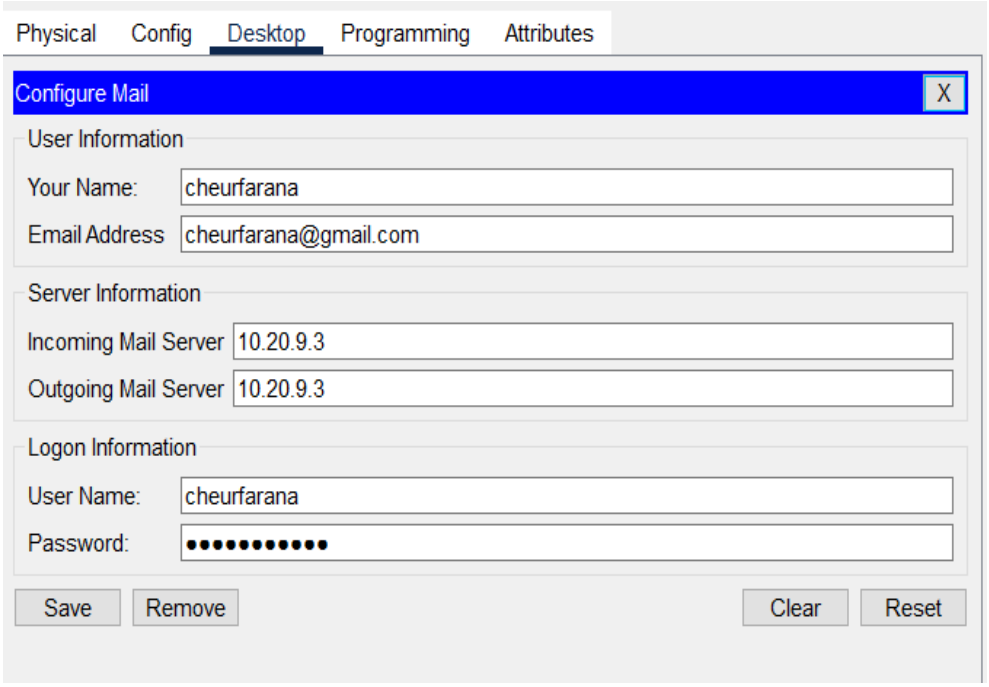
Dans cette étape, nous avons configuré le service email sur le PC émetteur (ADMIN_SARA). Nous avons commencé par ouvrir le client de messagerie et entré les paramètres nécessaires pour se connecter au serveur email. Nous avons ajouté un compte utilisateur en spécifiant l'adresse email et le mot de passe créés précédemment. Après avoir configuré le compte, nous avons rédigé et envoyé un message au récepteur (CLIENT_RANA) pour tester la connectivité et le bon fonctionnement du service email.

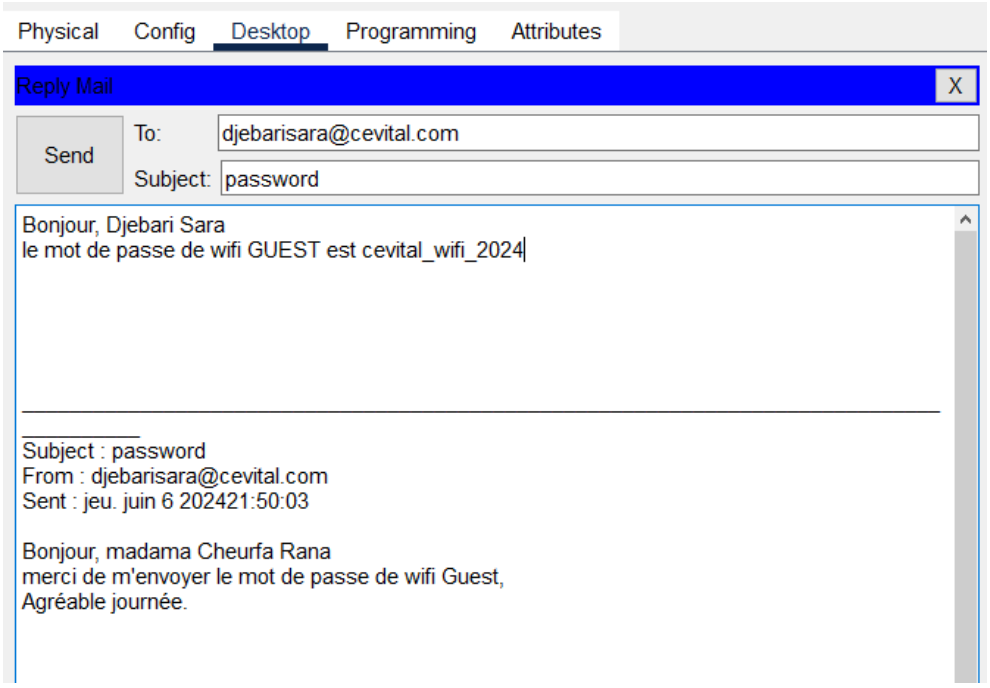




- **Configuration du PC récepteur :**

Sur le PC récepteur (CLIENT_RANA), nous avons configuré le service email pour permettre la réception des messages envoyés par l'administrateur. En utilisant le client de messagerie, nous avons ajouté un utilisateur en entrant l'adresse email et le mot de passe correspondants. Une fois connecté, nous avons vérifié le message envoyé par ADMIN_SARA pour s'assurer de sa bonne réception. Après cette vérification, nous avons rédigé une réponse et renvoyé le message à l'administrateur, confirmant ainsi le bon fonctionnement du service email.

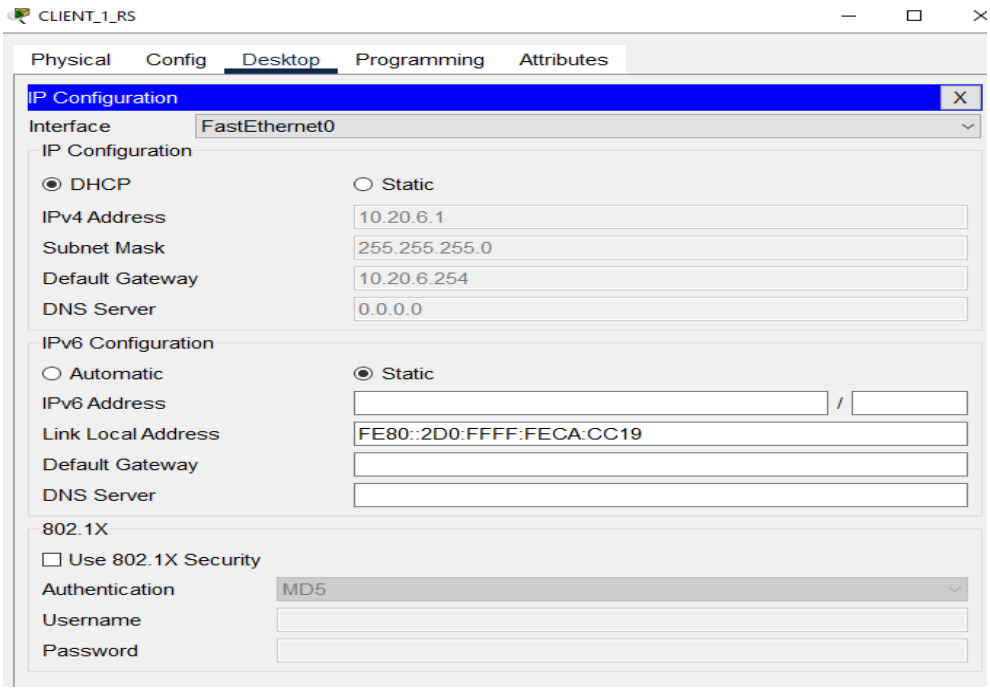




Configuration des Machines Utilisateurs

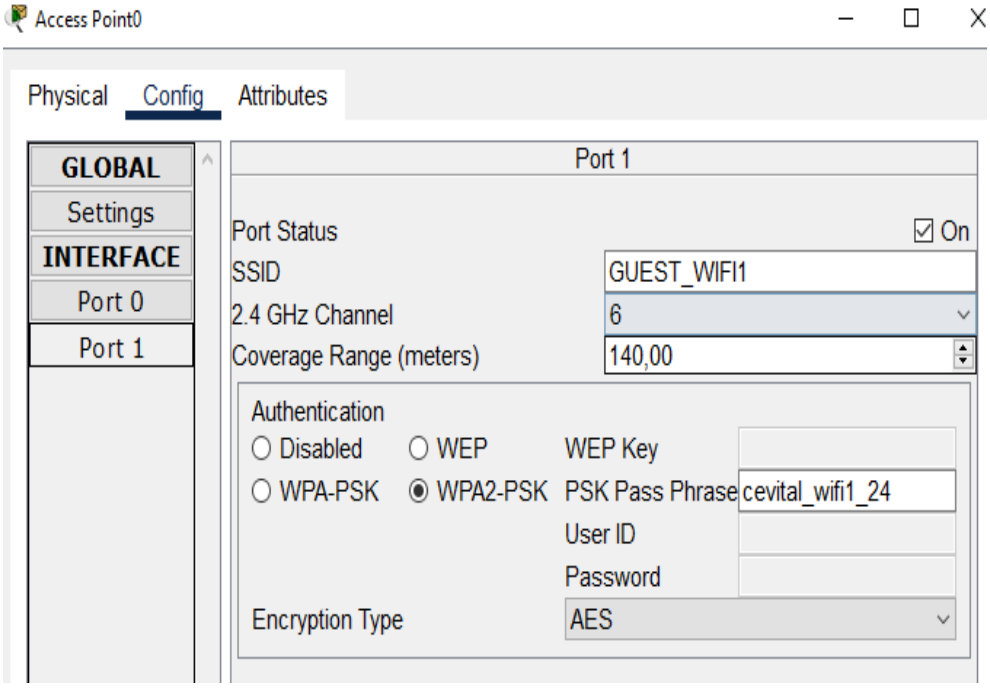
- **Configuration des PC en Mode DHCP :**

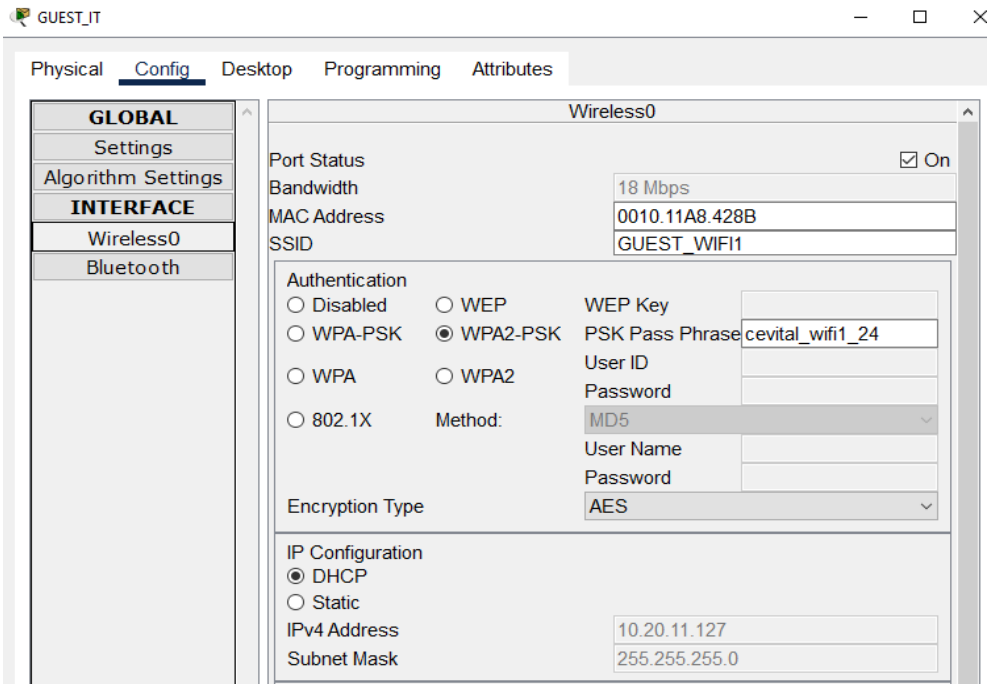
Nous configurerons les PC des utilisateurs pour qu'ils reçoivent automatiquement des adresses IP dynamiques via le DHCP.



- **Connexion des PC Guest aux Points d'Accès Wi-Fi :**

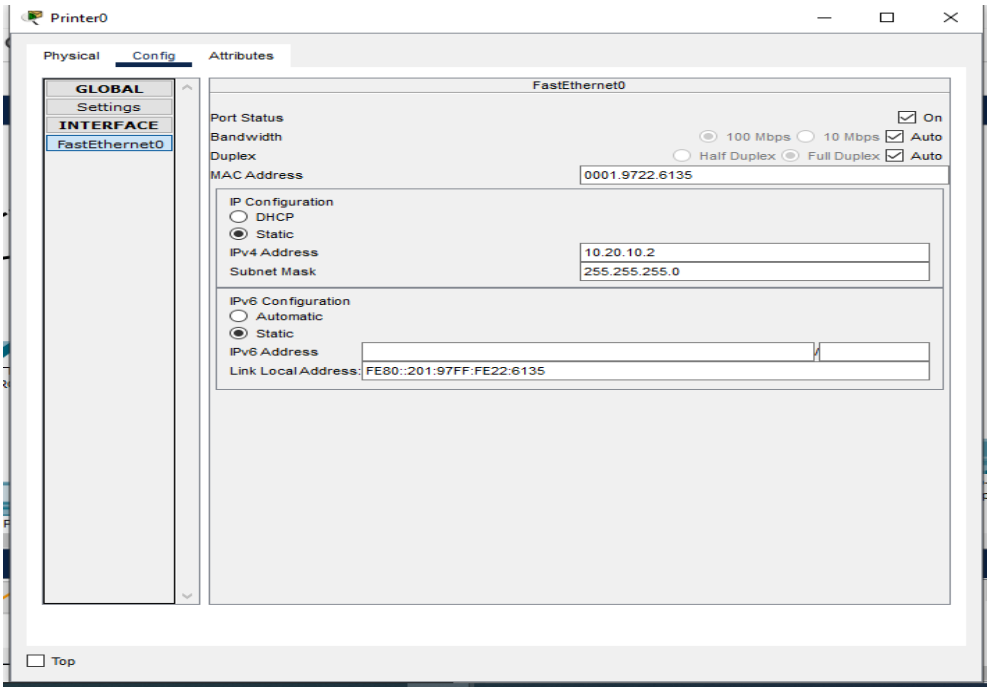
Nous relierons les PC Guest aux points d'accès Wi-Fi et les configurerons pour recevoir des adresses IP dynamiques via le DHCP, assurant ainsi une connectivité sans fil efficace.





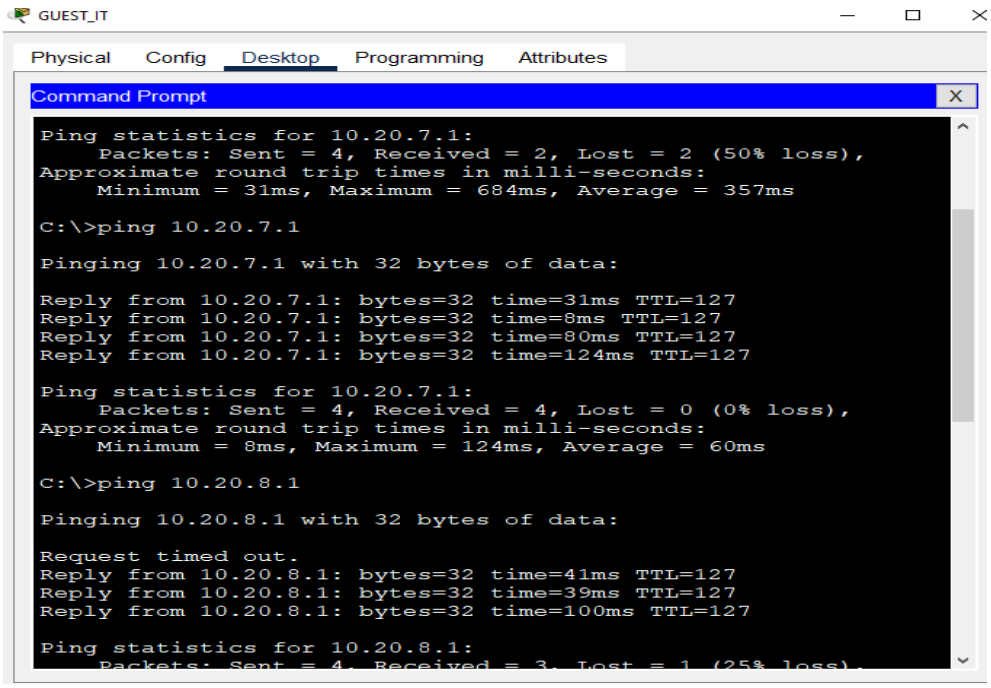
- **Configuration des Imprimantes avec des Adresses IP Statique :**

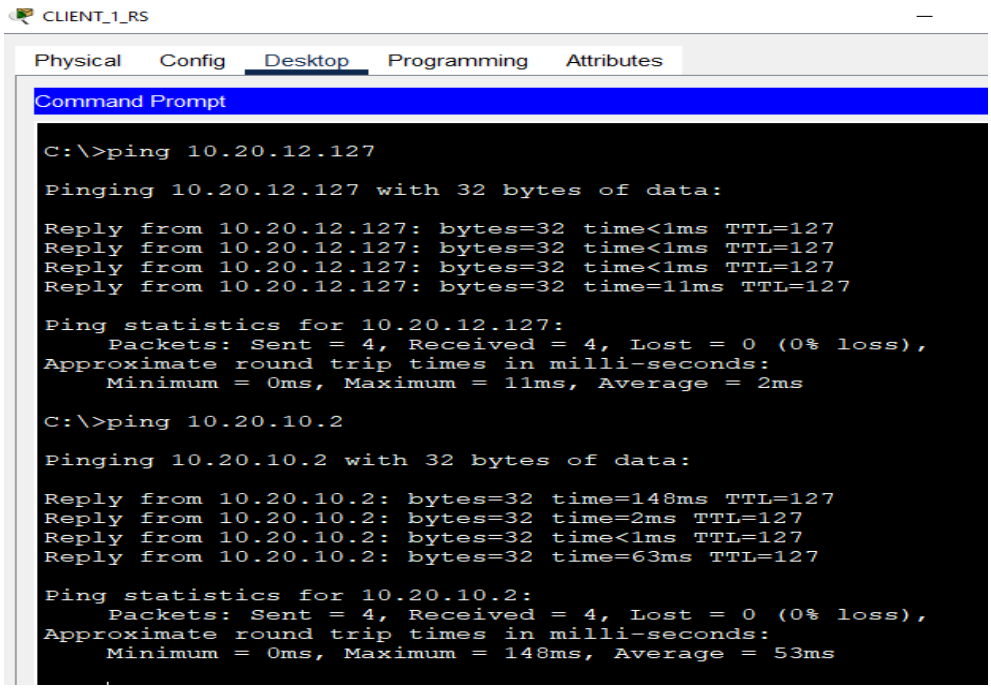
Configurerons les imprimantes manuellement en leur attribuant des adresses IP statiques pour garantir une accessibilité constante.



- **Vérification de la Connectivité :**

Après avoir configuré tous les périphériques, nous effectuons des tests de connectivité pour vérifier que chaque appareil est correctement connecté au réseau et peut accéder aux services nécessaires.


GUEST_IT
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Ping statistics for 10.20.7.1:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 31ms, Maximum = 684ms, Average = 357ms
C:\>ping 10.20.7.1
Pinging 10.20.7.1 with 32 bytes of data:
Reply from 10.20.7.1: bytes=32 time=31ms TTL=127
Reply from 10.20.7.1: bytes=32 time=8ms TTL=127
Reply from 10.20.7.1: bytes=32 time=80ms TTL=127
Reply from 10.20.7.1: bytes=32 time=124ms TTL=127
Ping statistics for 10.20.7.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 8ms, Maximum = 124ms, Average = 60ms
C:\>ping 10.20.8.1
Pinging 10.20.8.1 with 32 bytes of data:
Request timed out.
Reply from 10.20.8.1: bytes=32 time=41ms TTL=127
Reply from 10.20.8.1: bytes=32 time=39ms TTL=127
Reply from 10.20.8.1: bytes=32 time=100ms TTL=127
Ping statistics for 10.20.8.1:


CLIENT_1_RS
Physical
Config
Desktop
Programming
Attributes
Command Prompt
C:\>ping 10.20.12.127
Pinging 10.20.12.127 with 32 bytes of data:
Reply from 10.20.12.127: bytes=32 time<1ms TTL=127
Reply from 10.20.12.127: bytes=32 time<1ms TTL=127
Reply from 10.20.12.127: bytes=32 time<1ms TTL=127
Reply from 10.20.12.127: bytes=32 time=11ms TTL=127
Ping statistics for 10.20.12.127:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 11ms, Average = 2ms
C:\>ping 10.20.10.2
Pinging 10.20.10.2 with 32 bytes of data:
Reply from 10.20.10.2: bytes=32 time=148ms TTL=127
Reply from 10.20.10.2: bytes=32 time=2ms TTL=127
Reply from 10.20.10.2: bytes=32 time<1ms TTL=127
Reply from 10.20.10.2: bytes=32 time=63ms TTL=127
Ping statistics for 10.20.10.2:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 148ms, Average = 53ms

Résumé

Notre projet de fin d'études porte sur la conception et l'optimisation d'un réseau hiérarchique pour l'entreprise « Cevital-Béjaïa ». L'objectif de ce travail consiste à proposer des architectures réseau adaptées pour améliorer les performances, la sécurité et la gestion des ressources de l'entreprise. Pour cela, nous avons étudié le réseau existant et analysé les améliorations apportées par « Cevital » ces dernières années, ce qui nous a permis de suggérer des solutions pour une nouvelle architecture réseau. Cette architecture propose une redondance accrue, une haute disponibilité et un équilibrage de charge optimisé, tout en remplaçant les équipements réseau en fin de vie par des commutateurs plus récents et sécurisés. Nous avons mis en œuvre des protocoles tels que DHCP, VTP, STP et HSRP pour renforcer la sécurité et la fiabilité du réseau. La solution a été testée en utilisant le simulateur « Cisco Packet Tracer », qui nous a permis de créer un réseau virtuel et de simuler le comportement des protocoles afin de valider l'efficacité de la nouvelle architecture.

Mots clés : Cevital, la redondance, la haute disponibilité, équilibrage de charge, commutateurs, DHCP, VTP, STP, HSRP, Cisco Packet Tracer.

Abstract

Our final year project focuses on the design and optimization of a hierarchical network for the company « Cevital-Bejaia ». The objective of this work is to propose suitable network architectures to improve the performance, security, and resource management of the company. For this purpose, we studied the existing network and analyzed the improvements made by « Cevital » in recent years, which allowed us to suggest solutions for a new network architecture. This architecture proposes increased redundancy, high availability, and optimized load balancing, while replacing end-of-life network equipment with newer, more secure switches. We implemented protocols such as DHCP, VTP, STP, and HSRP to enhance network security and reliability. The solution was tested using the « Cisco Packet Tracer » simulator, which enabled us to create a virtual network and simulate the behavior of protocols to validate the effectiveness of the new architecture.

Keywords : Cevital, redundancy, high availability, load balancing, switches, DHCP, VTP, STP, HSRP, Cisco Packet Tracer.